Soluzioni cloud pubbliche e ibride NetApp

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

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

Sommario

Soluzioni cloud pubbliche e ibride NetApp . . . 1
Novità nelle soluzioni cloud pubbliche e ibride NetApp . . . 2
Soluzioni NetApp Hybrid Multicloud con VMware . . . 3
VMware per il cloud pubblico . . . 3
Panoramica di NetApp Hybrid Multicloud con VMware . . . 3
Soluzioni NetApp per VMware negli Hyperscaler . . . 6
Configurazioni supportate per NetApp Hybrid Multicloud con VMware . . . 9
VMware nella configurazione degli hyperscaler . . . 10
Storage NetApp nei cloud pubblici . . . 34
Riepilogo e conclusione: perché NetApp Hybrid Multicloud con VMware . . . 135
Casi d'uso del cloud ibrido VMware . . . 137
Casi d'uso per NetApp Hybrid Multicloud con VMware . . . 137
Soluzioni NetApp per VMware negli Hyperscaler . . . 138
Soluzioni NetApp per Amazon VMware Managed Cloud (VMC) . . . 138
Soluzioni NetApp per Azure VMware Solution (AVS) . . . 139
Soluzioni NetApp per Google Cloud VMware Engine (GCVE) . . . 140
NetApp per AWS/VMC . . . 140
Funzionalità NetApp per AWS VMC . . . 140
Proteggi i carichi di lavoro su AWS/VMC . . . 141
Migrazione dei carichi di lavoro su AWS/VMC . . . 256
NetApp per AWS / EVS . . . 271
Monta FSx ONTAP come datastore esterno per EVS . . . 271
Proteggi il datastore FSx ONTAP per EVS . . . 295
NetApp per Azure / AVS . . . 328
Funzionalità NetApp per Azure AVS . . . 329
Proteggi i carichi di lavoro su Azure/AVS . . . 330
Migrazione dei carichi di lavoro su Azure/AVS . . . 397
NetApp per GCP/GCVE . . . 411
Funzionalità NetApp per Google Cloud Platform GCVE . . . 411
Proteggi i carichi di lavoro su GCP/GCVE . . . 412
Migrazione dei carichi di lavoro su GCP/GCVE . . . 443
Proteggi i dati con Google Cloud NetApp Volumes in Google Cloud . . . 460
NetApp Disaster Recovery . . . 528
Protezione dei dati 3-2-1 per VMware con SnapCenter Plug-in e NetApp Backup and Recovery per proteggere i carichi di lavoro VMware . . . 528
NetApp Disaster Recovery . . . 562
Multicloud ibrido NetApp con carichi di lavoro containerizzati Red Hat OpenShift . . . 604
Iniziare . . . 604
Soluzioni NetApp Hybrid Multicloud per carichi di lavoro Red Hat OpenShift Container . . . 604
Proposte di valore delle soluzioni NetApp Hybrid Multicloud per i carichi di lavoro dei container Red Hat OpenShift . . . 606
Soluzioni supportate di NetApp Hybrid Multicloud per carichi di lavoro di Red Hat OpenShift Container . . . 607
Versioni di vari componenti utilizzati nella convalida della soluzione . . . 610

Integrazioni di NetApp Storage supportate con Red Hat OpenShift Containers . . . 611
Documentazione aggiuntiva . . . 615
Openshift per ambienti on-premise . . . 615
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware . . . 615
Distribuisci e configura la piattaforma Red Hat OpenShift Container su VMware . . . 616
Protezione dei dati tramite Trident Protect . . . 618
Cloud ibrido con componenti autogestiti . . . 619
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido 619
Distribuisci e configura la piattaforma Red Hat OpenShift Container su AWS . . . 621
Distribuisci e configura la piattaforma container Red Hat OpenShift su Google Cloud . . . 623
Distribuisci e configura la piattaforma Red Hat OpenShift Container su Azure . . . 625
Protezione dei dati tramite Trident Protect . . . 628
Cloud ibrido con componenti gestiti dal provider . . . 628
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift gestiti . . . 628
Distribuisci e configura la piattaforma Managed Red Hat OpenShift Container su AWS . . . 629
Distribuisci e configura OpenShift Dedicated su Google Cloud con Google Cloud NetApp Volumes . . . 632
Protezione dei dati . . . 634
Ulteriori soluzioni NetApp Hybrid Multicloud per carichi di lavoro Red Hat OpenShift . . . 634
Proteggi i dati utilizzando Trident Protect . . . 634
Protezione dei dati per le app container in OpenShift Container Platform utilizzando Trident Protect . . . 634
Proteggi le VM in Red Hat OpenShift Virtualization utilizzando Trident Protect . . . 646
Proteggere le app contenitore utilizzando strumenti di terze parti . . . 666
Protezione dei dati per le app container nella piattaforma container OpenShift tramite OpenShift API for Data Protection (OADP) . . . 666
Installazione dell'operatore OpenShift API for Data Protection (OADP) . . . 668
Creazione di backup su richiesta per le app in OpenShift Container Platform . . . 677
Migrare un'app da un cluster a un altro . . . 680
Ripristinare un'app da un backup . . . 684
Eliminazione di backup e ripristini utilizzando Velero . . . 691
Guarda video e demo sulle soluzioni multicloud ibride con NetApp . . . 693
Guarda i video sulle soluzioni multicloud ibride per Amazon Web Services con NetApp . . . 693
Archiviazione connessa agli ospiti . . . 693
TCO e datastore supplementari . . . 693
Flussi di lavoro di migrazione (HCX) . . . 693
Guarda i video sulle soluzioni multicloud ibride per il cloud Azure VMware con NetApp . . . 693
Datastore supplementari . . . 693
Ripristino dopo un disastro . . . 693
Flussi di lavoro di migrazione (HCX) . . . 694
Guarda i video sulle soluzioni multicloud ibride per Red Hat OpenShift con NetApp . . . 694
Istantanee e ripristino . . . 694
Integrazione dello storage . . . 694
Failover e fail-back . . . 694
Automazione delle soluzioni . . . 694
Leggi i blog sulle soluzioni cloud degli esperti NetApp . . . 695
Integrazione VMware con AWS e Amazon FSx per ONTAP . . . 695

Soluzione Azure VMware . . . 695
Motore VMware di Google Cloud . . . 695
Protezione e gestione dei dati . . . 695
NetApp per carichi di lavoro dei container OpenShift . . . 695
VMware Sovereign Cloud . . . 695
Note legali . . . 696
Copyright . . . 696
Marchi . . . 696
Brevetti . . . 696
Politica sulla riservatezza . . . 696

Soluzioni cloud pubbliche e ibride NetApp

Novità nelle soluzioni cloud pubbliche e ibride NetApp

Scopri le novità nelle soluzioni cloud pubbliche e ibride.

[[18-august-2025]]
== 18 agosto 2025

Il sito NetApp Solutions è ora il"Famiglia di soluzioni NetApp" , che comprende i seguenti siti:

- "Soluzioni di intelligenza artificiale NetApp"
- "Soluzioni container NetApp"
- "Soluzioni di gestione dei dati NetApp"
- "Soluzioni di database NetApp"
- Soluzioni cloud pubbliche e ibride NetApp
- "Soluzioni NetApp per SAP"
- "Soluzioni di virtualizzazione NetApp"

Soluzioni NetApp Hybrid Multicloud con VMware

VMware per il cloud pubblico

Panoramica di NetApp Hybrid Multicloud con VMware

La maggior parte delle organizzazioni IT segue l'approccio cloud-first ibrido. Queste organizzazioni si trovano in una fase di trasformazione e i clienti stanno valutando il loro attuale panorama IT e poi migrando i loro carichi di lavoro sul cloud in base all'esercizio di valutazione e individuazione.

I fattori che spingono i clienti a migrare verso il cloud possono includere elasticità e burst, uscita dal data center, consolidamento del data center, scenari di fine vita, fusioni, acquisizioni e così via. Il motivo di questa migrazione può variare in base a ciascuna organizzazione e alle rispettive priorità aziendali. Quando si passa al cloud ibrido, è molto importante scegliere lo storage giusto nel cloud per sfruttare al massimo la potenza e l'elasticità dell'implementazione del cloud.

Opzioni VMware Cloud nel cloud pubblico

Questa sezione descrive in che modo 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 Azure VMware

Azure VMware Solution è un servizio cloud ibrido che consente di avere VMware SDDC completamente funzionanti all'interno del cloud pubblico Microsoft Azure. Azure VMware Solution è una soluzione proprietaria completamente gestita e supportata da Microsoft, verificata da VMware, che sfrutta l'infrastruttura di Azure. Ciò significa che quando viene distribuita la soluzione Azure VMware, i clienti ottengono ESXi di VMware per la virtualizzazione del calcolo, vSAN per l'archiviazione iperconvergente e NSX per la rete e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture dei data center leader del settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure nativi.

VMware Cloud su AWS

VMware Cloud on AWS porta il software SDDC di classe enterprise di VMware su AWS Cloud con accesso ottimizzato ai servizi AWS nativi. Basato su VMware Cloud Foundation, VMware Cloud on AWS integra i prodotti di virtualizzazione di rete, storage ed elaborazione di VMware (VMware vSphere, VMware vSAN e VMware NSX) insieme alla gestione di VMware vCenter Server, ottimizzati per l'esecuzione su infrastrutture AWS dedicate, elastiche e bare-metal.

Motore VMware di Google Cloud

Google Cloud VMware Engine è un'offerta Infrastructure-as-a-Service (IaaS) basata sull'infrastruttura scalabile ad alte prestazioni di Google Cloud e sullo stack VMware Cloud Foundation: VMware vSphere, vCenter, vSAN e NSX-T. Questo servizio consente un rapido accesso al cloud, migrando o estendendo senza problemi i carichi di lavoro VMware esistenti dagli ambienti on-premise a Google Cloud Platform, senza i costi, gli sforzi o i rischi di riprogettare le applicazioni o riorganizzare le operazioni. Si tratta di un servizio venduto e supportato da Google, in stretta collaborazione con VMware.



Il cloud privato SDDC e la colocation NetApp Cloud Volumes garantiscono le migliori prestazioni con una latenza di rete minima.

Lo sapevate?

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

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

Configurazione di archiviazione

Per i clienti che intendono ospitare carichi di lavoro ad alta intensità di storage e scalare su qualsiasi soluzione VMware ospitata nel cloud, l'infrastruttura iperconvergente predefinita impone che l'espansione riguardi sia le risorse di elaborazione che quelle di storage.

Grazie all'integrazione con NetApp Cloud Volumes, come Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponibile in tutti e tre i principali hyperscaler) e Google Cloud NetApp Volumes per Google Cloud, i clienti hanno ora la possibilità di scalare separatamente e in modo indipendente il proprio storage e di aggiungere nodi di elaborazione al cluster SDDC solo quando necessario.

Note:

- VMware sconsiglia configurazioni di cluster sbilanciate, pertanto espandere lo storage significa aggiungere più host, il che implica un TCO maggiore.
- È possibile un solo ambiente vSAN. Pertanto, tutto il traffico di archiviazione sarà in diretta competizione con i carichi di lavoro di produzione.
- Non è possibile fornire più livelli di prestazioni per allineare requisiti, prestazioni e costi delle applicazioni.
- È molto facile raggiungere i limiti della capacità di archiviazione di vSAN costruito sugli host del cluster. Utilizza NetApp Cloud Volumes per scalare lo storage in modo da ospitare set di dati attivi o suddividere i dati più freddi in storage persistente.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponibile in tutti e tre i principali hyperscaler) e Google Cloud NetApp Volumes per Google Cloud possono essere utilizzati insieme alle VM guest. Questa architettura di storage ibrida è costituita da un datastore vSAN che contiene il sistema operativo guest e i dati binari dell'applicazione. I dati dell'applicazione vengono collegati alla VM tramite un iniziatore iSCSI basato su guest o tramite i mount NFS/SMB che comunicano direttamente rispettivamente con Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files e Google Cloud NetApp Volumes per Google Cloud. Questa configurazione consente di superare facilmente le sfide relative alla capacità di archiviazione, poiché con vSAN lo spazio libero disponibile dipende dallo spazio libero e dai criteri di archiviazione utilizzati.

Consideriamo un cluster SDDC a tre nodi su VMware Cloud on AWS:

- La capacità grezza totale per un SDDC a tre nodi è pari a 31,1 TB (circa 10 TB per ciascun nodo).
- Lo spazio libero da mantenere prima di aggiungere host aggiuntivi = 25% = (0,25 x 31,1 TB) = 7,7 TB.
- Capacità raw utilizzabile dopo la deduzione dello spazio libero = 23,4 TB
- Lo spazio libero effettivo disponibile dipende dalla politica di archiviazione applicata.

  Per 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 a ottimizzare il TCO, soddisfacendo al contempo i requisiti di prestazioni e protezione dei dati.

Al momento della stesura del presente documento, l'unica opzione disponibile era l'archiviazione interna.

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 eventuali requisiti di latenza specifici, poiché fanno parte dell'host stesso e si trovano nelle vicinanze. Utilizzare meccanismi in-guest per tutte le VM del carico di lavoro per le quali le latenze transazionali sono accettabili.
- Usa la tecnologia NetApp SnapMirror per replicare i dati del carico di lavoro dal sistema ONTAP on-premises a Cloud Volumes ONTAP o Amazon FSx ONTAP e semplificare la migrazione utilizzando meccanismi a livello di blocco. Questo non si applica ad Azure NetApp Files e Google Cloud NetApp Volumes. Per migrare i dati ad Azure NetApp Files o Google Cloud NetApp Volumes, usa NetApp XCP, NetApp Copy and Sync, rysnc o robocopy, a seconda del protocollo di 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 mappa lo storage.
- Per montare l'archiviazione connessa agli ospiti durante il failover di prova 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 Microsoft Multipath I/O (MPIO) in-guest, del firewall e del timeout del disco siano configurate correttamente all'interno della VM.

Questo vale solo per l'archiviazione connessa agli ospiti.

Vantaggi dello storage cloud NetApp

Lo storage cloud NetApp offre i seguenti vantaggi:

- Migliora la densità di elaborazione-archiviazione ridimensionando l'archiviazione indipendentemente dall'elaborazione.
- Consente di ridurre il numero di host, riducendo così il TCO complessivo.
- Un errore del nodo di elaborazione non influisce sulle prestazioni di archiviazione.
- La riorganizzazione del volume e la funzionalità di livello di servizio dinamico di Azure NetApp Files consentono di ottimizzare i costi dimensionando i carichi di lavoro in stato stazionario, evitando così il provisioning eccessivo.
- L'efficienza di archiviazione, il cloud tiering e le capacità di modifica del tipo di istanza di Cloud Volumes ONTAP consentono di aggiungere e ridimensionare in modo ottimale lo storage.
- Impedisce il provisioning eccessivo: le risorse di storage vengono aggiunte solo quando necessario.
- Le copie e i cloni Snapshot efficienti consentono di creare rapidamente copie senza alcun impatto sulle prestazioni.
- Aiuta a contrastare gli attacchi ransomware utilizzando il ripristino rapido dalle copie Snapshot.

- Fornisce un efficiente disaster recovery regionale basato sul trasferimento incrementale dei blocchi e un backup integrato a livello di blocco tra le regioni che garantisce RPO e RTO migliori.

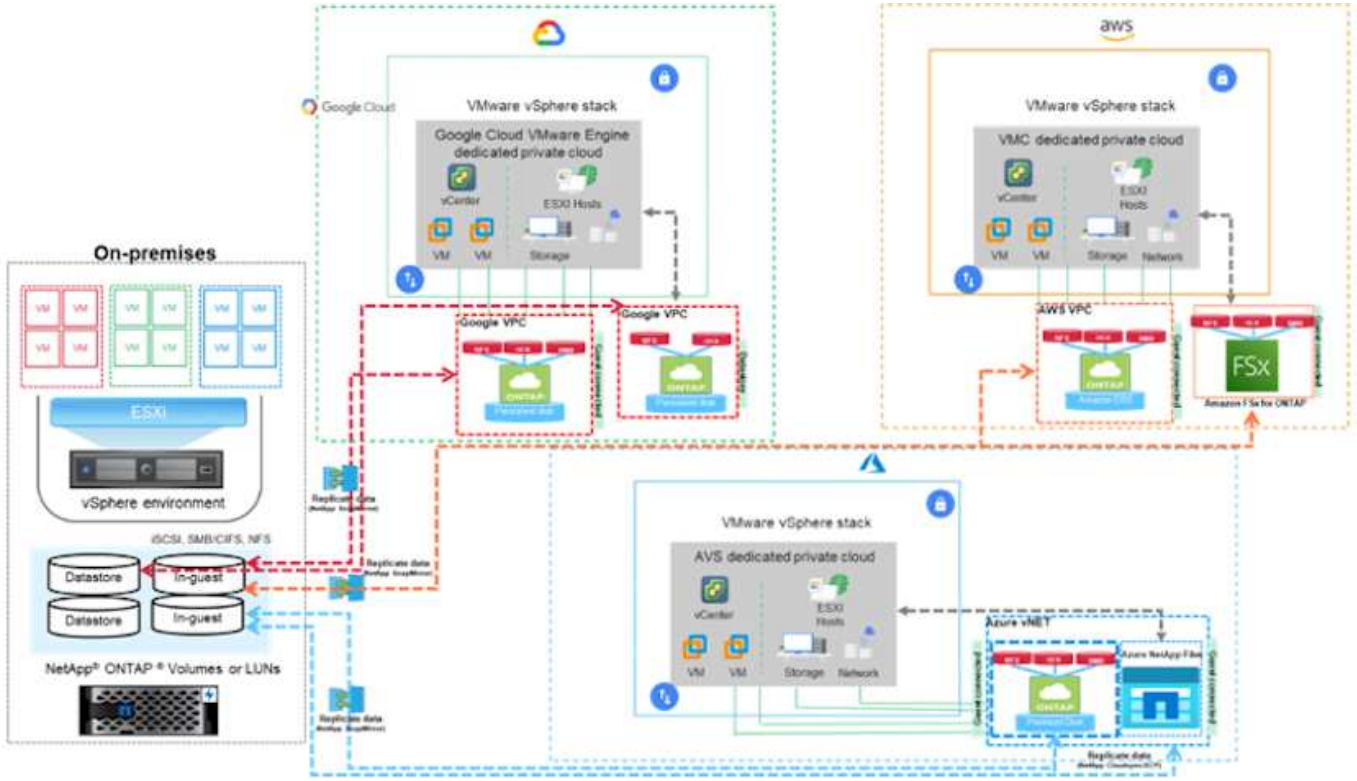
Ipotesi

- Sono abilitati la tecnologia SnapMirror o altri meccanismi di migrazione dei dati pertinenti. Sono disponibili numerose opzioni di connettività, da quelle on-premise a qualsiasi cloud hyperscaler. Utilizzare il percorso appropriato e collaborare con i team di networking competenti.
- Al momento della stesura del presente documento, l'unica opzione disponibile era l'archiviazione interna.

> Coinvolgere gli architetti delle soluzioni NetApp e i rispettivi architetti cloud hyperscaler per la pianificazione e il dimensionamento dello storage e il numero richiesto di host. NetApp consiglia di identificare i requisiti di prestazioni di storage prima di utilizzare il dimensionatore Cloud Volumes ONTAP per finalizzare il tipo di istanza di storage o il livello di servizio appropriato con la giusta velocità effettiva.

Architettura dettagliata

Da una prospettiva di alto livello, questa architettura (mostrata nella figura seguente) illustra come ottenere connettività multicloud ibrida e portabilità delle app su più provider cloud utilizzando NetApp Cloud Volumes ONTAP, Google Cloud NetApp Volumes per Google Cloud e Azure NetApp Files come opzione di archiviazione in-guest aggiuntiva.



Soluzioni NetApp per VMware negli Hyperscaler

Scopri di più sulle funzionalità che NetApp offre ai tre (3) hyperscaler principali: da NetApp come dispositivo di storage connesso guest o datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/espansione 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 quell'hyperscaler.

Passa alla sezione del contenuto desiderato selezionando tra le seguenti opzioni:

- "VMware nella configurazione Hyperscaler"
- "Opzioni di archiviazione NetApp"
- "Soluzioni cloud NetApp /VMware"

VMware nella configurazione Hyperscaler

Come per l'ambiente on-premise, la pianificazione di un ambiente di virtualizzazione basato su cloud è fondamentale per un ambiente di produzione di successo per la creazione di VM 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 .

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

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura VMware Cloud per AWS
- Connetti VMware Cloud a FSx ONTAP

Visualizza il dettaglio"passaggi di configurazione per VMC" .

Azzurro / AVS

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad Azure VMware Solution.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Registra il fornitore di risorse e crea un cloud privato
- Connettiti a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalida la connettività di rete e accedi al cloud privato

Visualizza il dettaglio"passaggi di configurazione per AVS" .

GCP / GCVE

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Google Cloud NetApp Volumes a GCVE.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura GCVE
- Abilita l'accesso privato a GCVE

Visualizza il dettaglio"passaggi di configurazione per GCVE" .

Opzioni di archiviazione NetApp

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

Per favore visita"Opzioni di archiviazione NetApp supportate" per maggiori informazioni.

AWS / VMC

AWS supporta l'archiviazione NetApp nelle seguenti configurazioni:

- FSx ONTAP come storage connesso agli ospiti
- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- FSx ONTAP come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione di connessione guest per VMC" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per VMC" .

Azzurro / AVS

Azure supporta l'archiviazione NetApp nelle seguenti configurazioni:

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

Visualizza il dettaglio"opzioni di archiviazione di connessione ospite per AVS" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per AVS" .

GCP / GCVE

Google Cloud supporta l'archiviazione NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione per la connessione degli ospiti per GCVE" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per GCVE" .

Per saperne di più"Supporto del datastore Google Cloud NetApp Volumes per Google Cloud VMware Engine (blog NetApp)" O"Come utilizzare Google Cloud NetApp Volumes come datastore per Google Cloud VMware Engine (blog di Google)"

Soluzioni cloud NetApp /VMware

Grazie alle soluzioni cloud NetApp e VMware, molti casi d'uso sono semplici da implementare nell'hyperscaler di tua scelta. VMware definisce i principali casi d'uso del carico di lavoro cloud come:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Migrare
- Estendere

AWS / VMC

"Esplora le soluzioni NetApp per AWS / VMC"

Azzurro / 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 Multicloud con VMware

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

	Ospite connesso	Datastore NFS supplementare
AWS	CVO FSx ONTAP"Dettagli"	FSx ONTAP"Dettagli"

Azzurro	CVO ANF"Dettagli"	ANF"Dettagli"
GCP	Volumi CVO NetApp"Dettagli"	Volumi NetApp"Dettagli"

VMware nella configurazione degli hyperscaler

Configurazione dell'ambiente di virtualizzazione nel provider cloud

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura VMware Cloud per AWS
- Connetti VMware Cloud a FSx ONTAP

Visualizza il dettaglio"passaggi di configurazione per VMC" .

Azzurro / AVS

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad Azure VMware Solution.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Registra il fornitore di risorse e crea un cloud privato
- Connettiti a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalida la connettività di rete e accedi al cloud privato

Visualizza il dettaglio"passaggi di configurazione per AVS" .

GCP / GCVE

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Google Cloud NetApp Volumes a GCVE.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura GCVE
- Abilita l'accesso privato a GCVE

Visualizza il dettaglio"passaggi di configurazione per GCVE" .

Distribuisci e configura l'ambiente di virtualizzazione su AWS

Come per le soluzioni on-premise, la pianificazione di VMware Cloud su AWS è fondamentale per un ambiente di produzione di successo per la creazione di VM 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 .

Attualmente, l'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP (CVO) ad AWS VMC.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Distribuisci e configura VMware Cloud per AWS**

"VMware Cloud su AWS"fornisce un'esperienza cloud nativa 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 software-defined vSAN e uno o più host ESXi che forniscono risorse di elaborazione e storage ai carichi di lavoro.

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

Attualmente, l'archiviazione in-guest è 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**

Registrati per un"Account Amazon Web Services" .

Per iniziare è necessario un account AWS, sempre che non ne sia già stato creato uno. Nuovo o esistente, per molti passaggi di questa procedura è necessario disporre di privilegi amministrativi nell'account. Vedi questo"collegamento" per maggiori informazioni sulle credenziali AWS.

▼ **Registrati per un account My VMware**

Registrati per un"Il mio VMware" account.

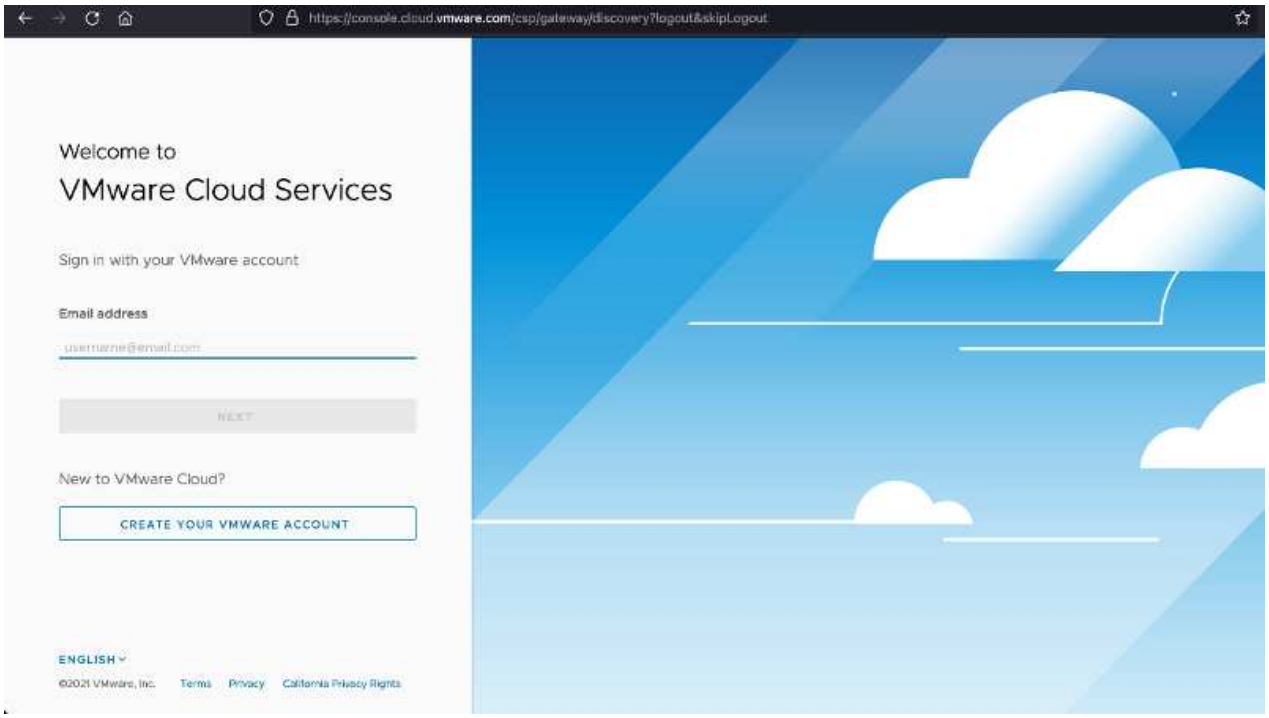
Per accedere al portfolio cloud di VMware (incluso VMware Cloud su AWS), è necessario un account cliente VMware o un account My VMware. Se non l'hai ancora fatto, crea un account VMware"Qui" .

▼ **Provisioning SDDC in VMware Cloud**

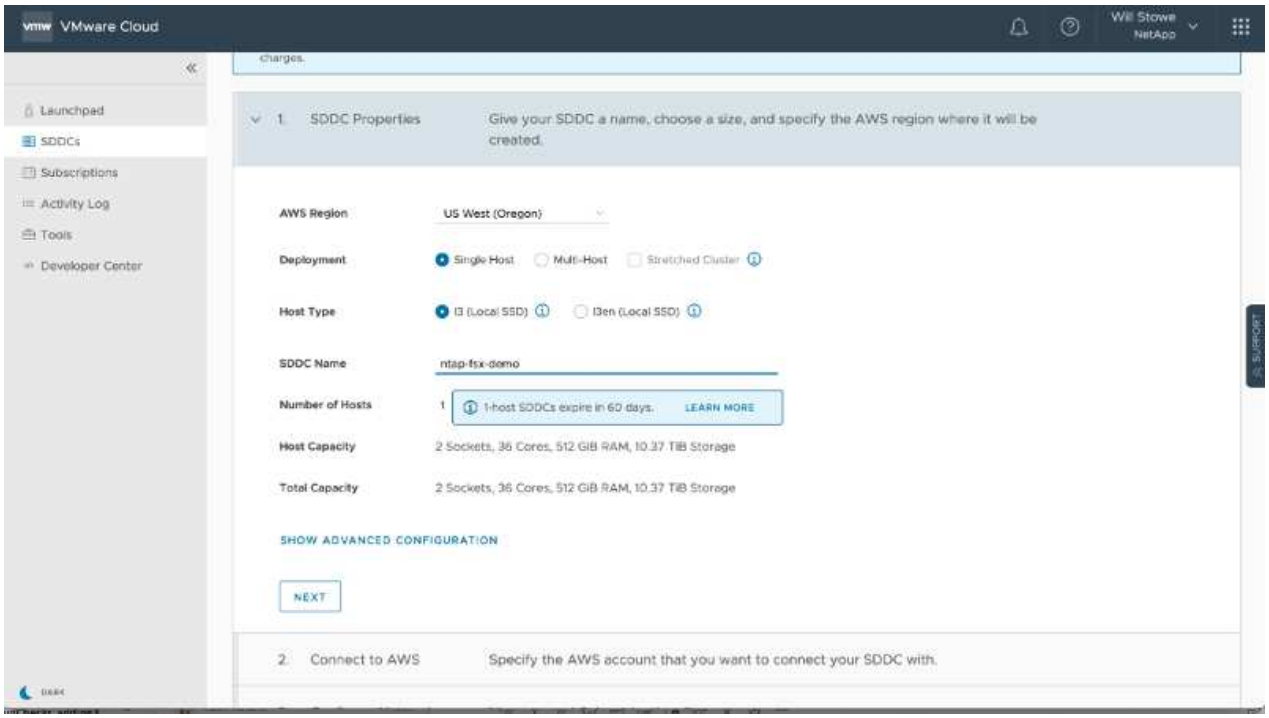
Dopo aver configurato l'account VMware e aver eseguito il dimensionamento corretto, il passo successivo ovvio per utilizzare il servizio VMware Cloud on AWS è l'implementazione di un Software-Defined Data Center. Per creare un SDDC, seleziona una regione AWS in cui ospitarlo, assegna un

nome all'SDDC e specifica quanti host ESXi desideri che contenga. Se non si dispone ancora di un account AWS, è comunque possibile creare una configurazione SDDC iniziale che contenga un singolo host ESXi.

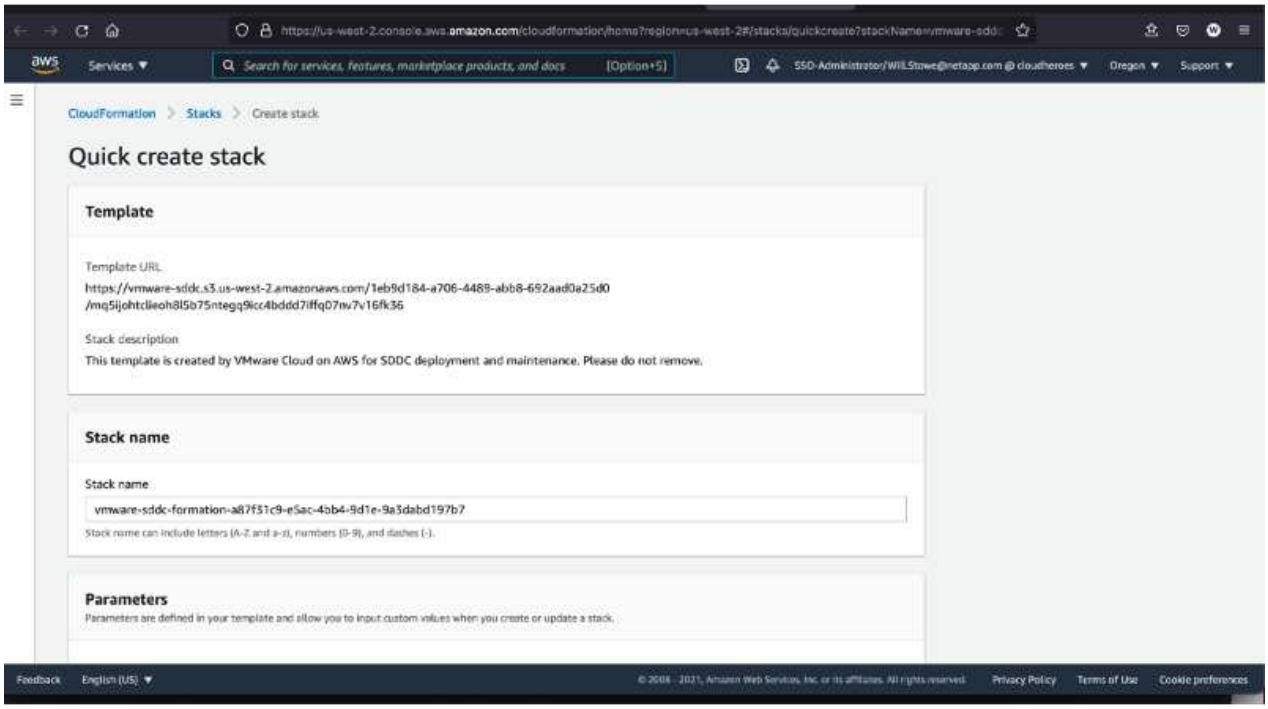
1. Accedi alla VMware Cloud Console utilizzando le tue credenziali VMware esistenti o quelle appena create.

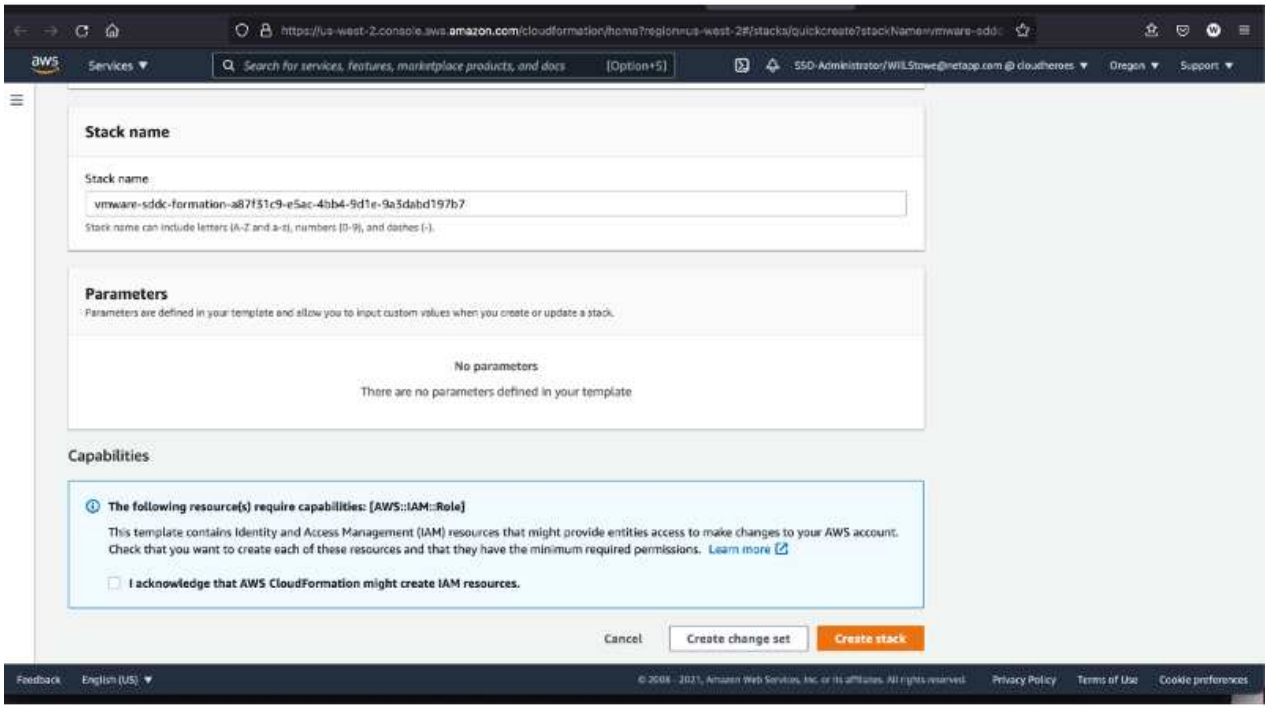


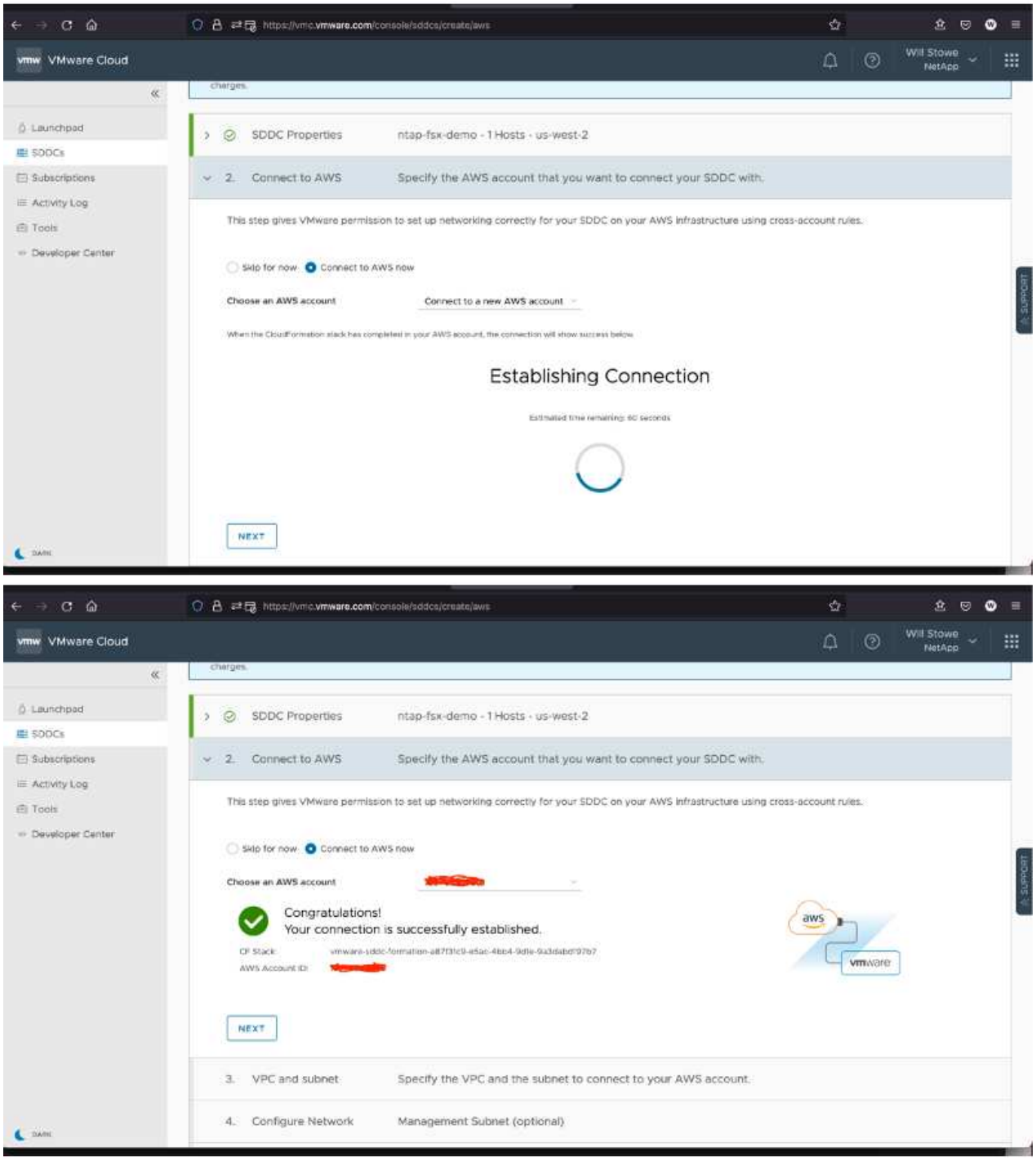
2. Configurare la regione AWS, la distribuzione, il tipo di host e il nome SDDC:



3. Connettiti all'account AWS desiderato ed esegui lo stack AWS Cloud Formation.

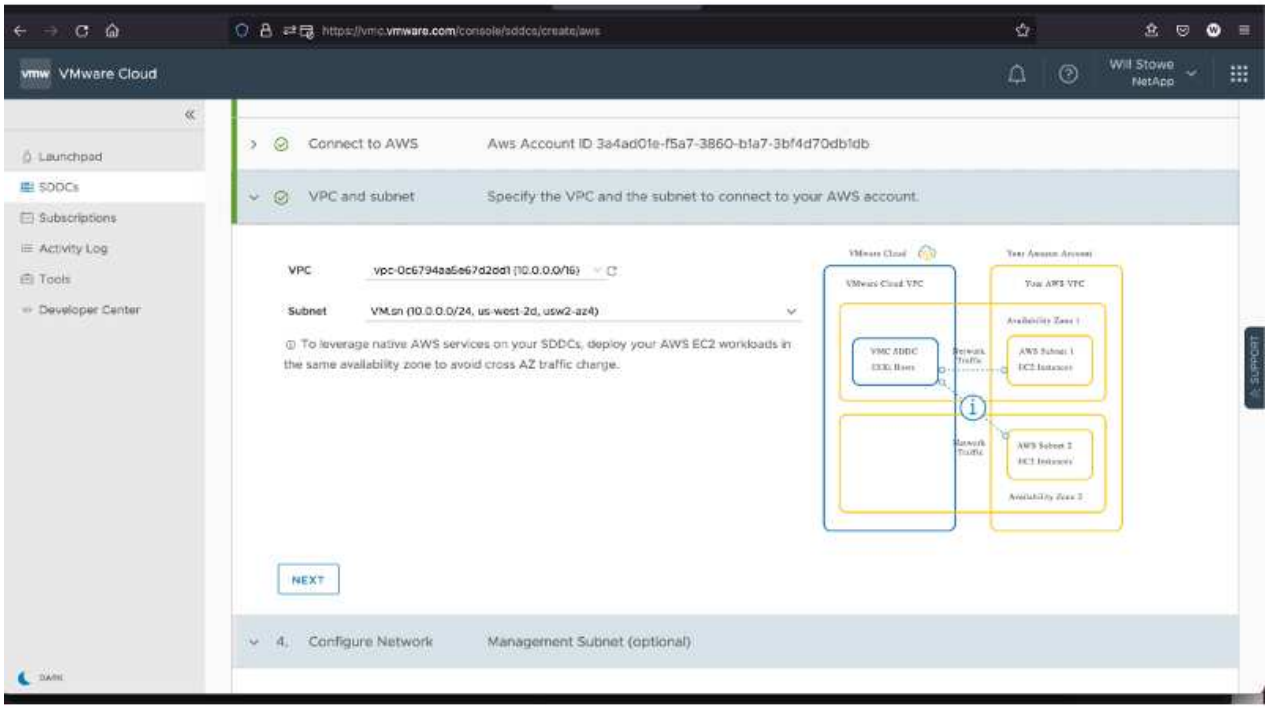

Services
Search for services, features, marketplace products, and docs [Option+S]
Oregon
Support
CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ljohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences


Services
Search for services, features, marketplace products, and docs [Option+S]
Oregon
Support
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

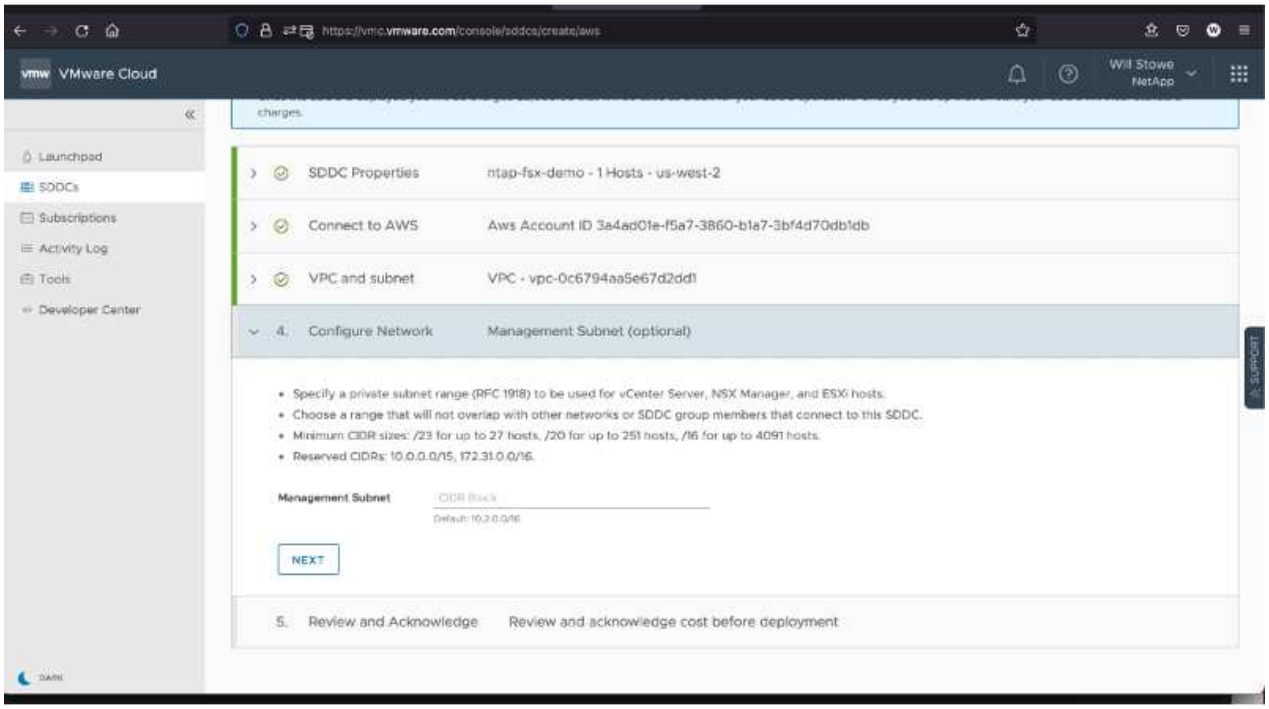


In questa convalida viene utilizzata la configurazione a host singolo.

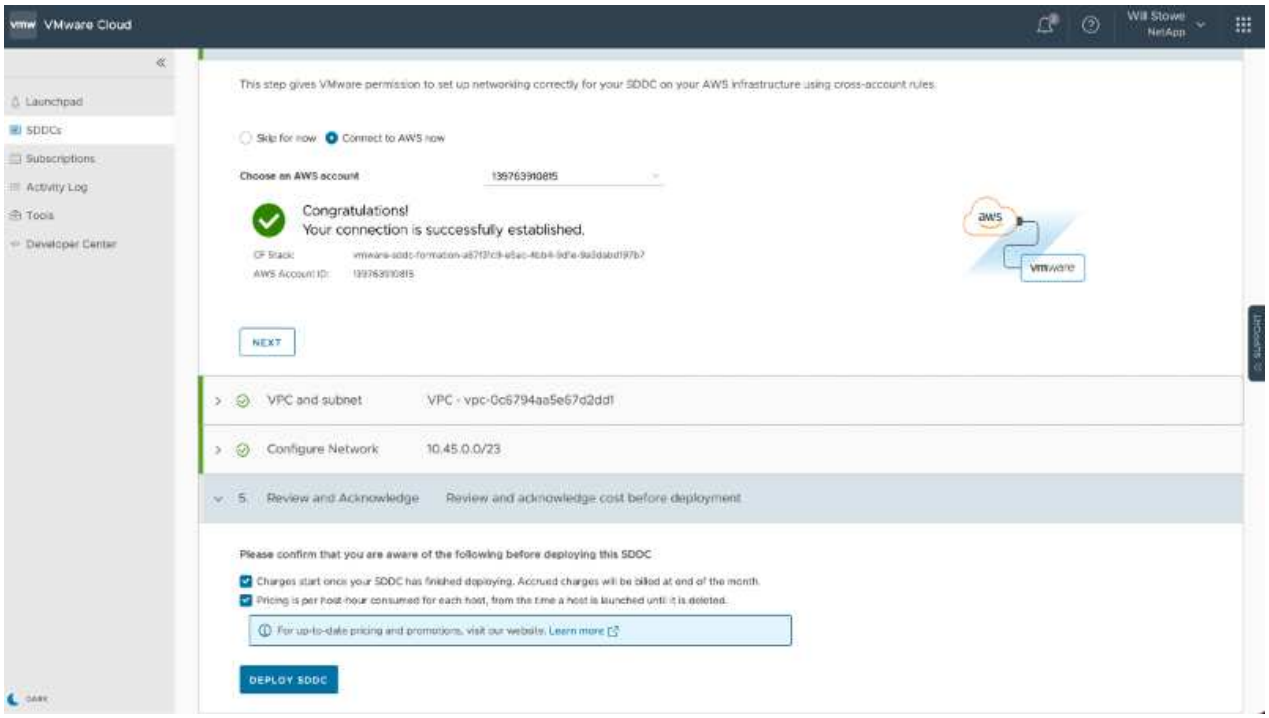
4. Selezionare l'AWS VPC desiderato a cui connettere l'ambiente VMC.



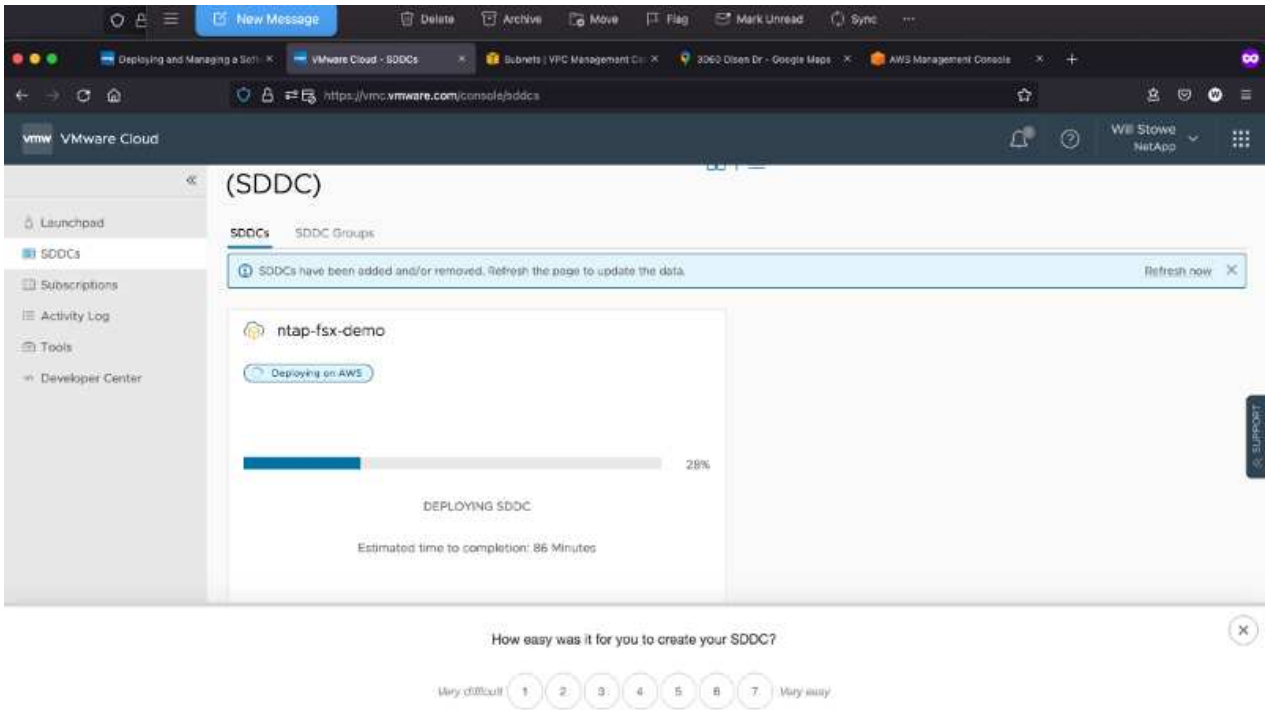
5. Configurare la subnet di gestione VMC; questa subnet contiene i servizi gestiti da VMC come vCenter, NSX e così via. Non scegliere uno spazio di indirizzamento sovrapposto ad altre reti che necessitano di connettività all'ambiente SDDC. Infine, seguire le raccomandazioni per le dimensioni CIDR riportate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



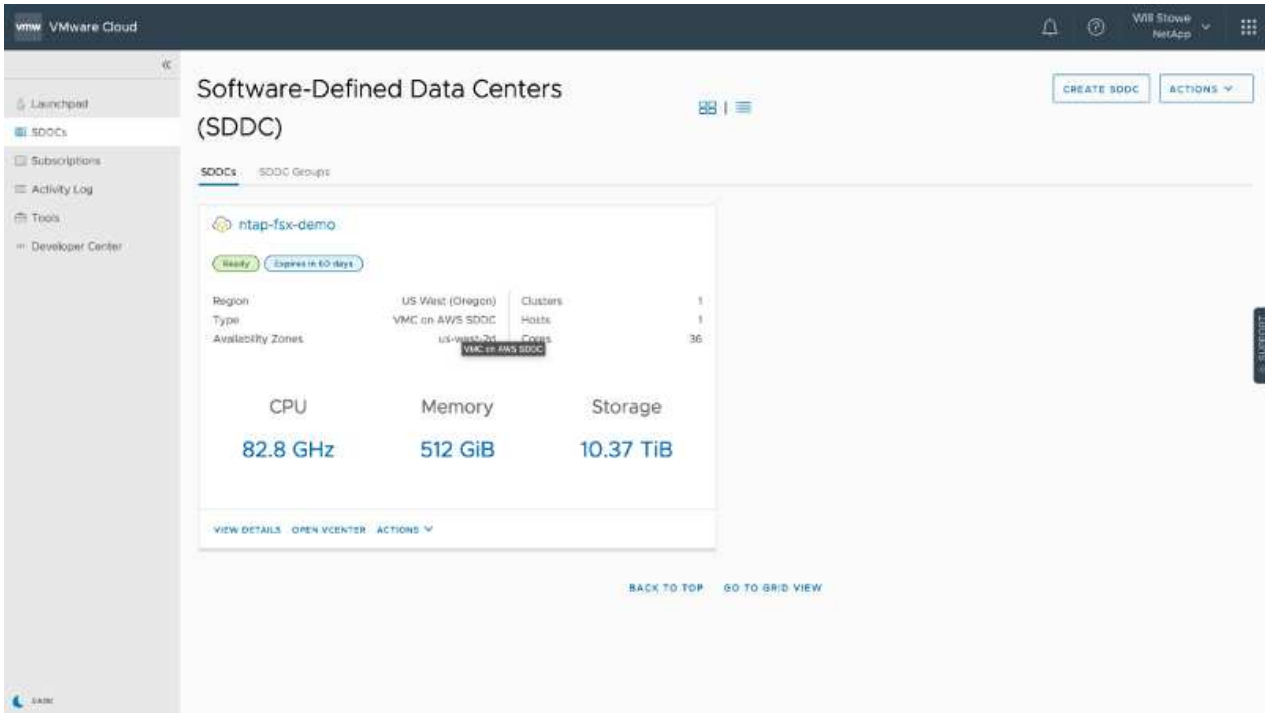
6. Esaminare e confermare la configurazione SDDC, quindi fare clic su Distribuisci SDDC.



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



7. Una volta completato, l'SDDC è pronto per l'uso.

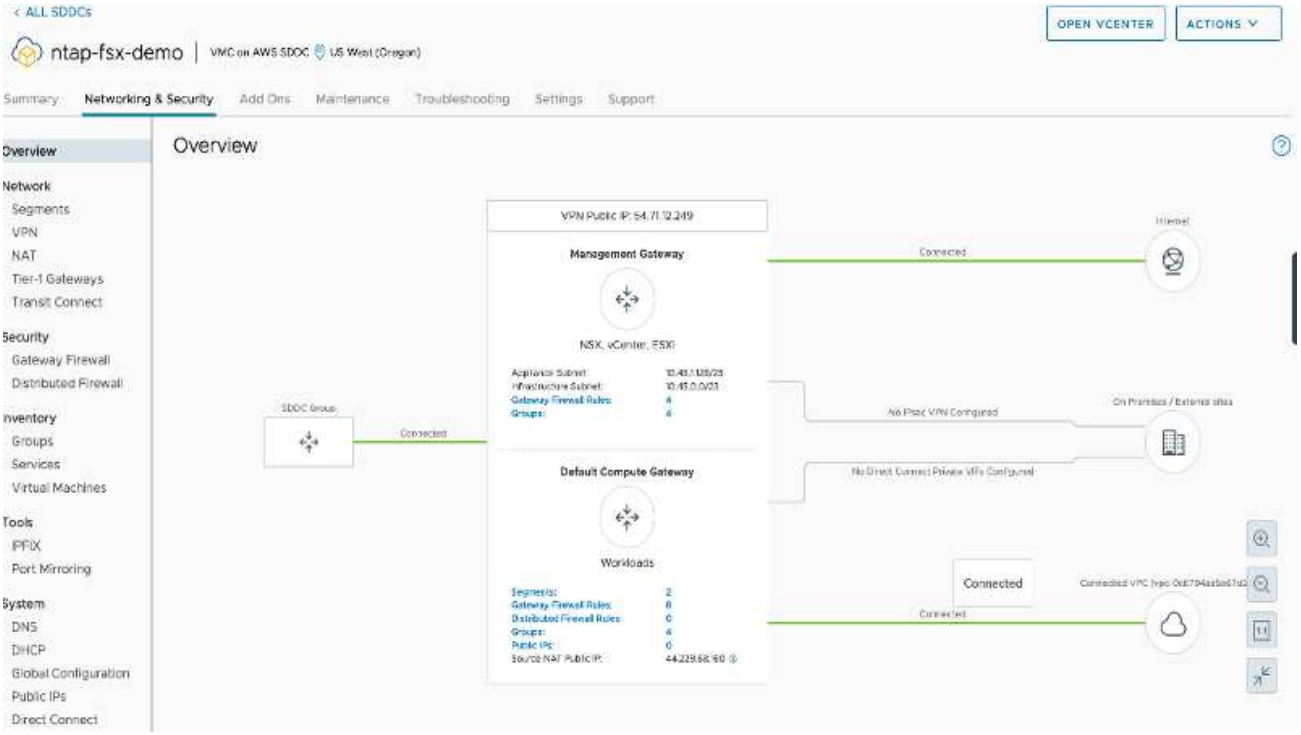


Per una guida dettagliata sulla distribuzione SDDC, vedere"Distribuire un SDDC dalla console VMC" .

▼ **Connetti VMware Cloud a FSx ONTAP**

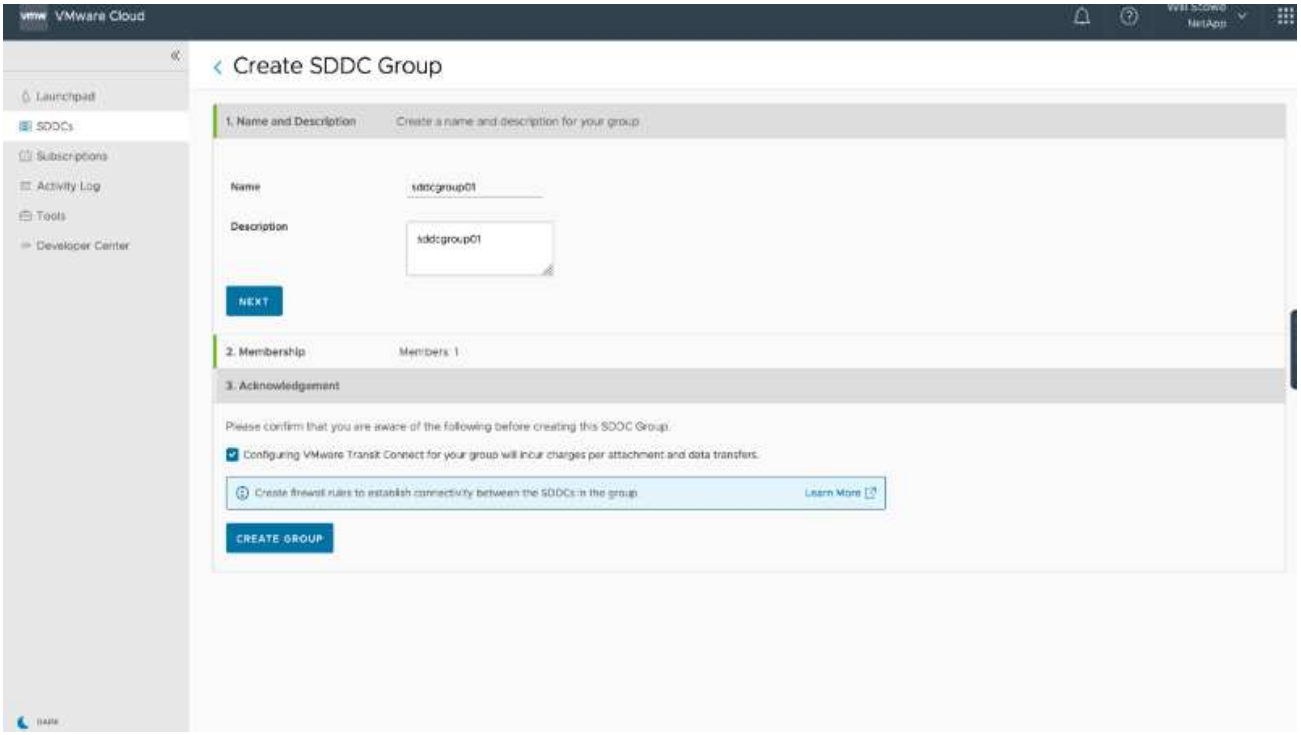
Per connettere VMware Cloud a FSx ONTAP, completare i seguenti passaggi:

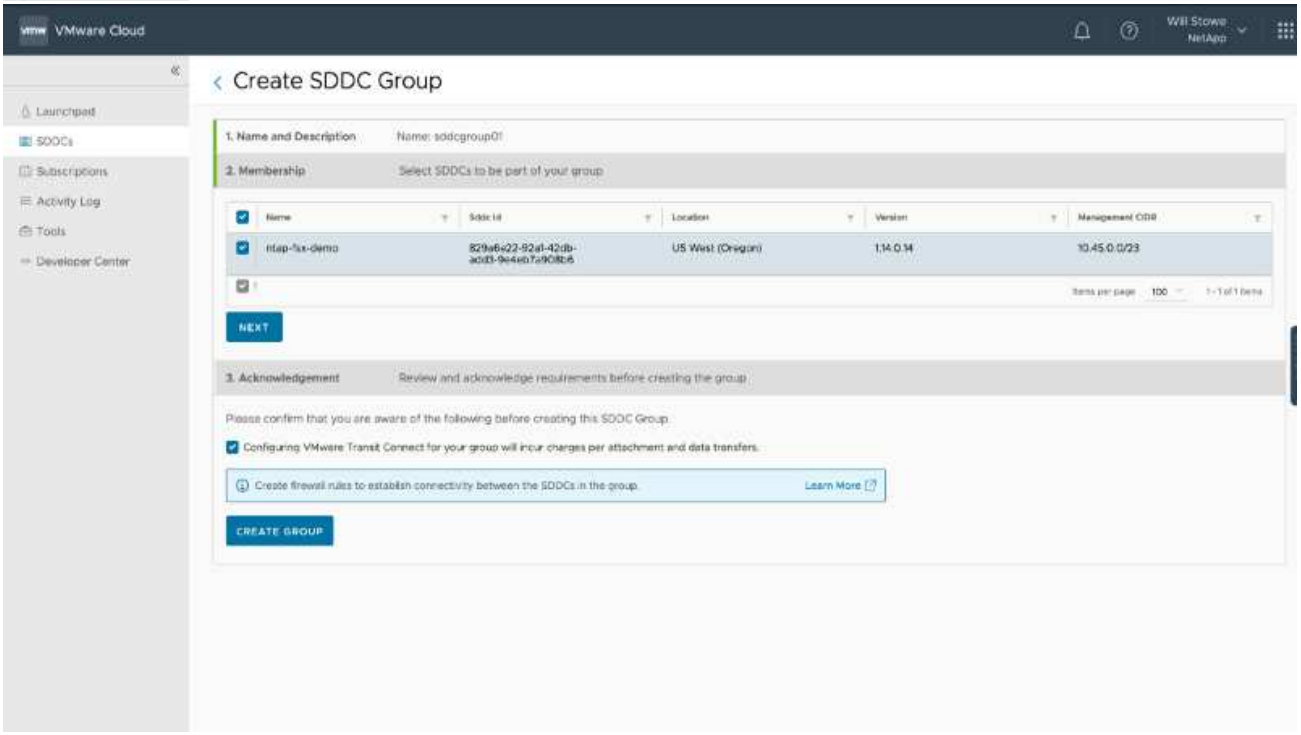
1. Una volta completata la distribuzione di VMware Cloud e connessa ad AWS VPC, è necessario distribuire Amazon FSx ONTAP in una nuova VPC anziché nella VPC connessa originale (vedere lo screenshot qui sotto). FSx (NFS e IP mobili SMB) non è accessibile se distribuito nella VPC connessa. Tieni presente che gli endpoint ISCSI come Cloud Volumes ONTAP funzionano perfettamente dalla VPC connessa.

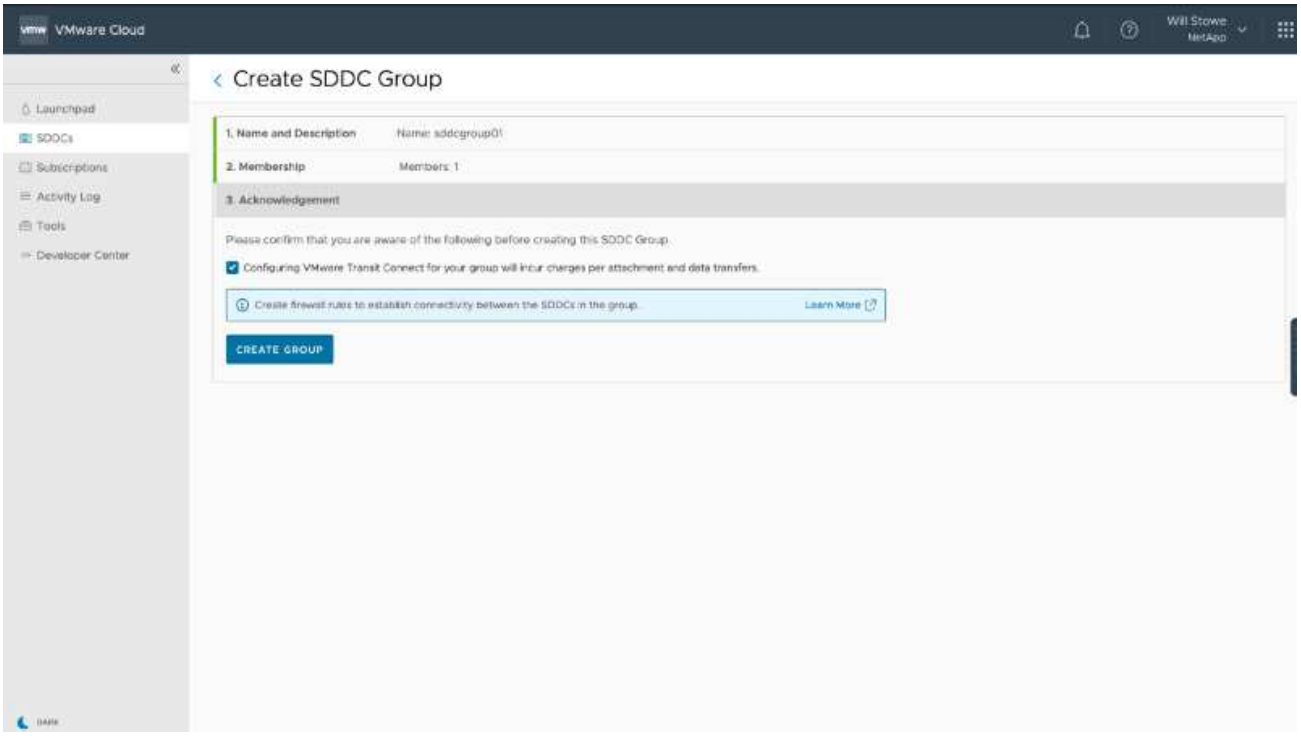


2. Distribuisci un’ulteriore VPC nella stessa regione, quindi distribuisci Amazon FSx ONTAP nella nuova VPC.

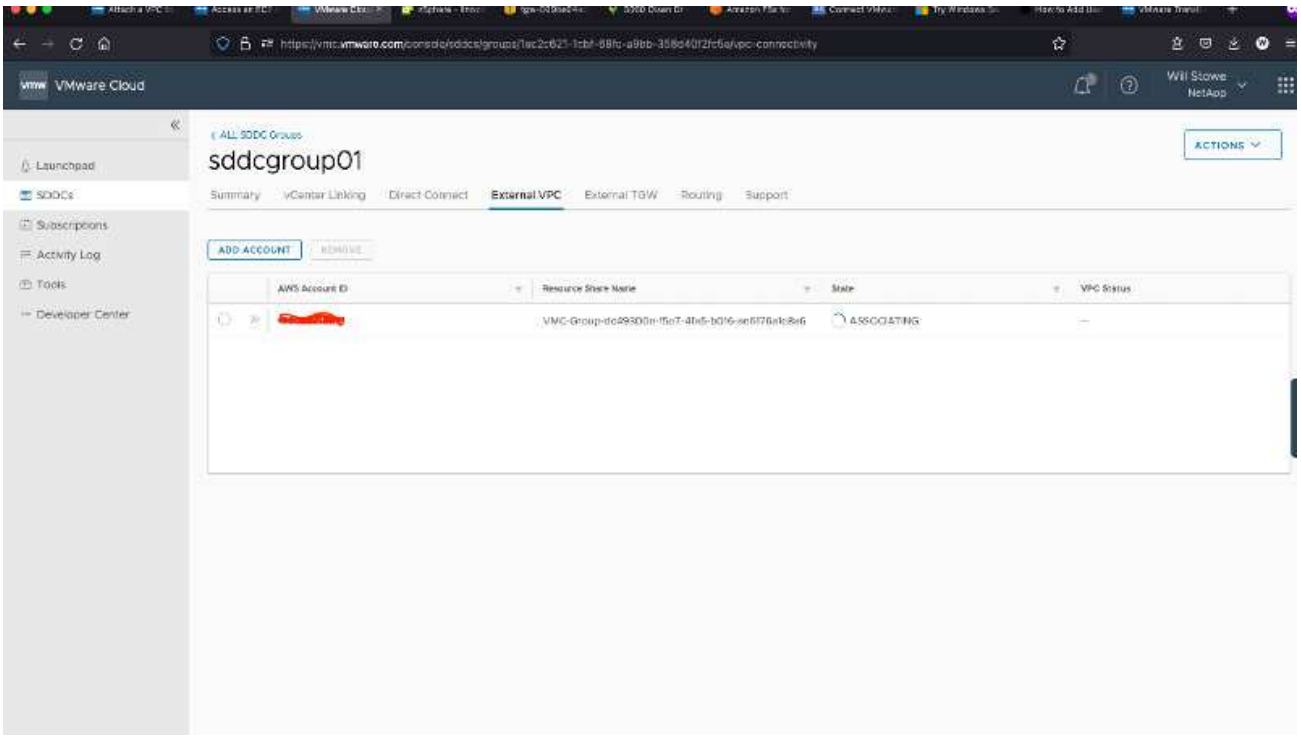
   La configurazione di un gruppo SDDC nella console VMware Cloud abilita le opzioni di configurazione di rete necessarie per connettersi alla nuova VPC in cui è distribuito FSx. Nel passaggio 3, verificare che sia selezionata l’opzione "La configurazione di VMware Transit Connect per il gruppo comporterà addebiti per allegato e trasferimenti di dati", quindi scegliere Crea gruppo. Il completamento del processo potrebbe richiedere alcuni minuti.

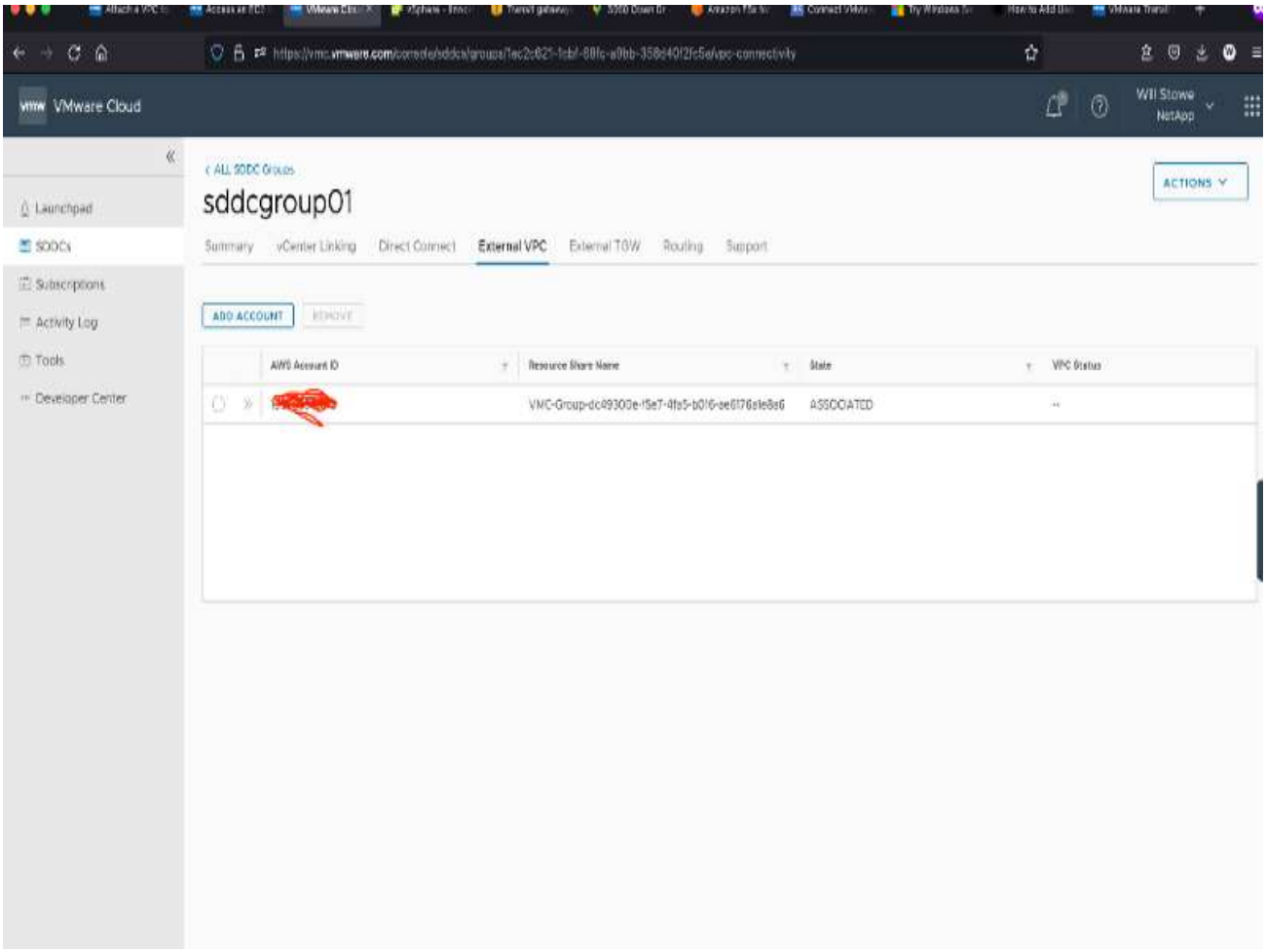




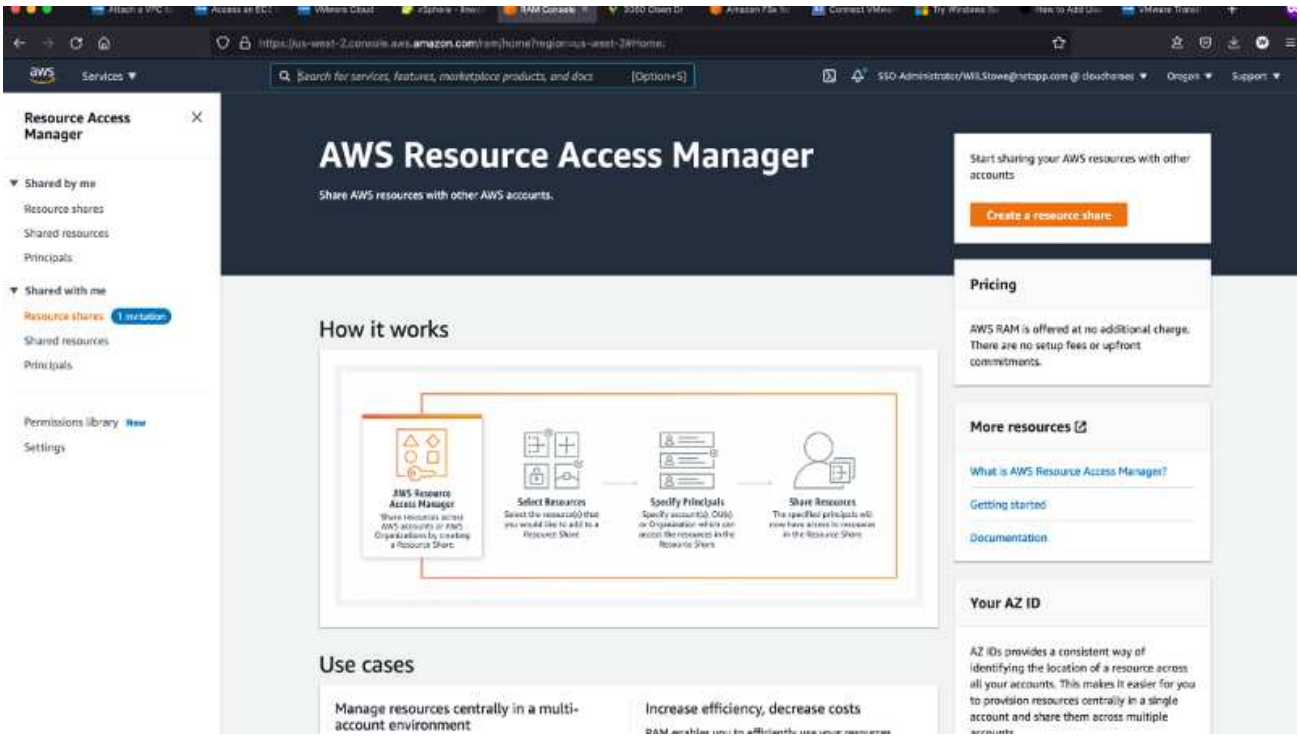


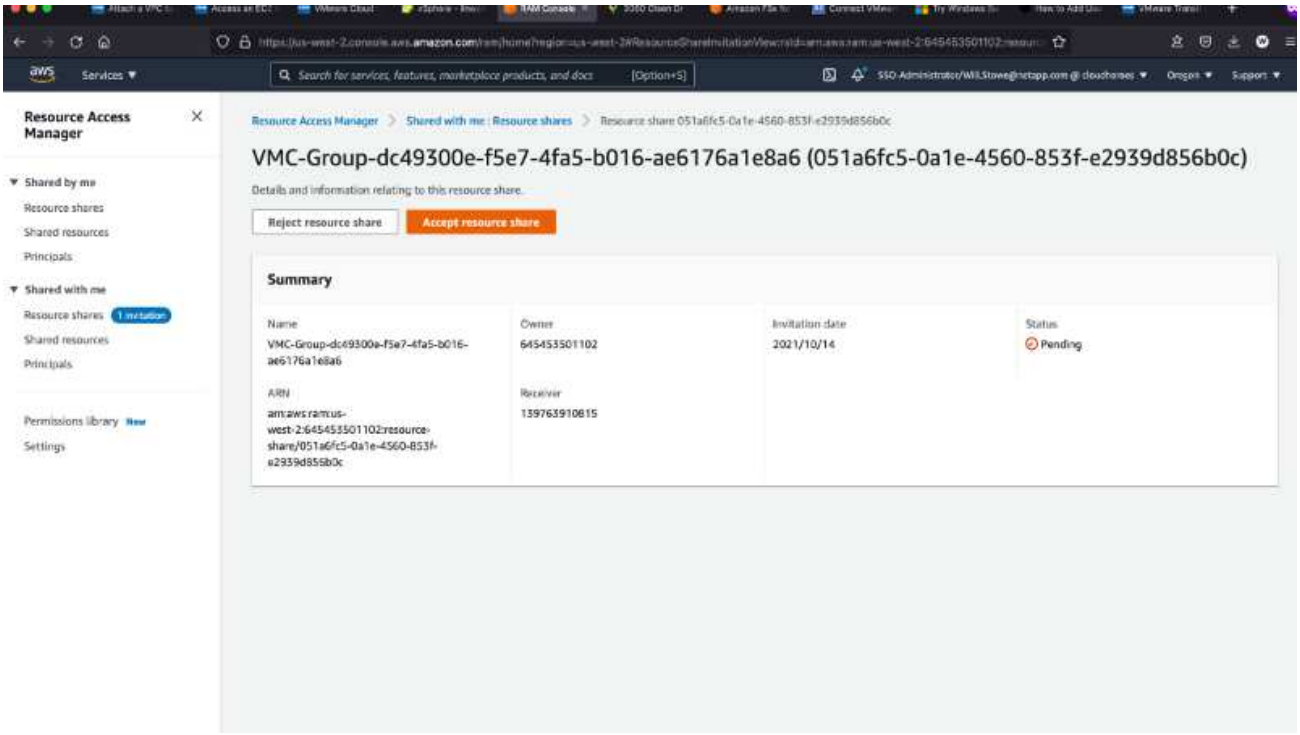
3. Collegare la VPC appena creata al gruppo SDDC appena creato. Selezionare la scheda VPC esterna e seguire le istruzioni"istruzioni per collegare una VPC esterna" al gruppo. Il completamento di questo processo può richiedere dai 10 ai 15 minuti.



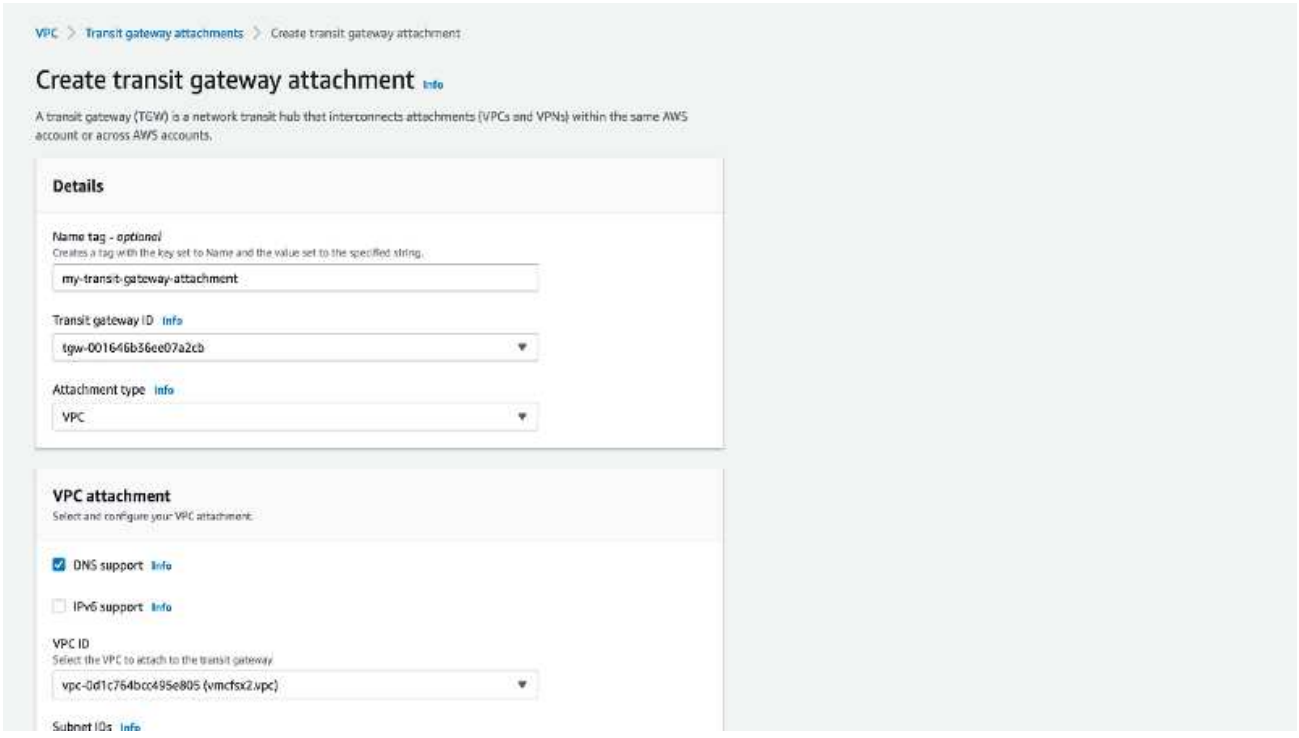


4. Come parte del processo VPC esterno, tramite la console AWS ti verrà richiesto di accedere a una nuova risorsa condivisa tramite Resource Access Manager. La risorsa condivisa è la"Gateway di transito AWS" gestito da VMware Transit Connect.

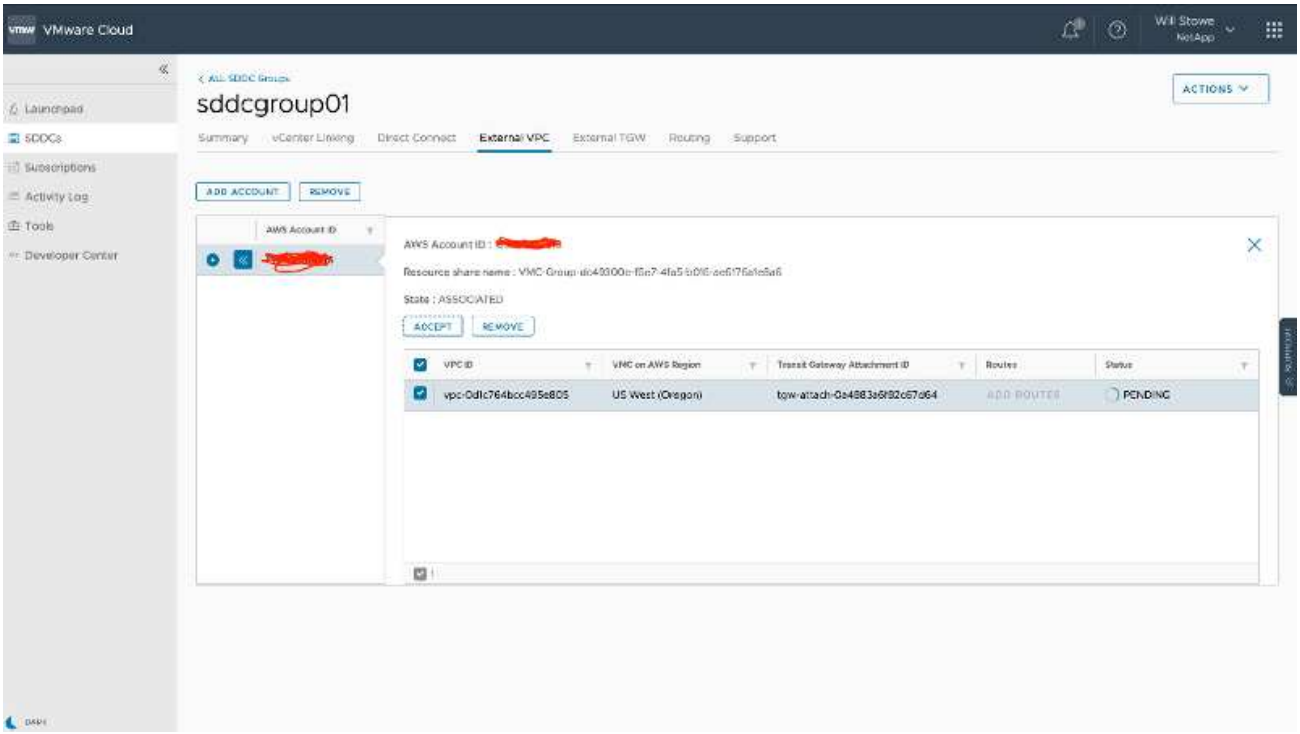




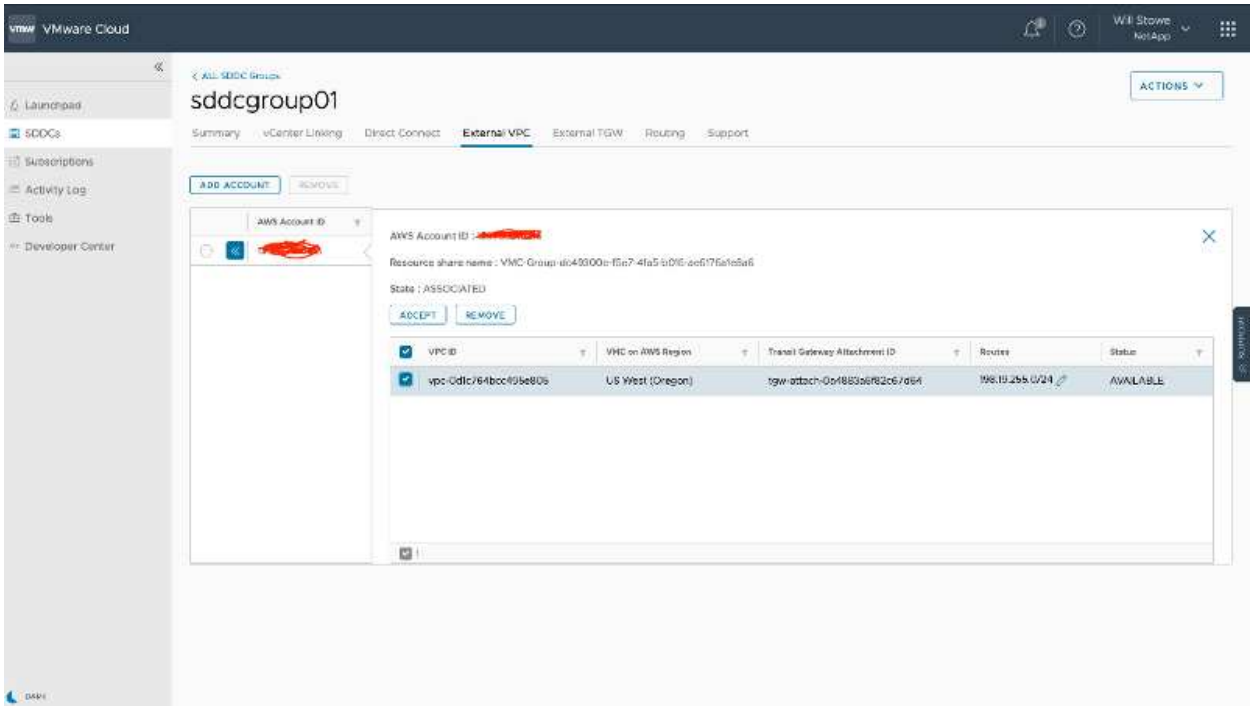
5. Creare l'allegato Transit Gateway.



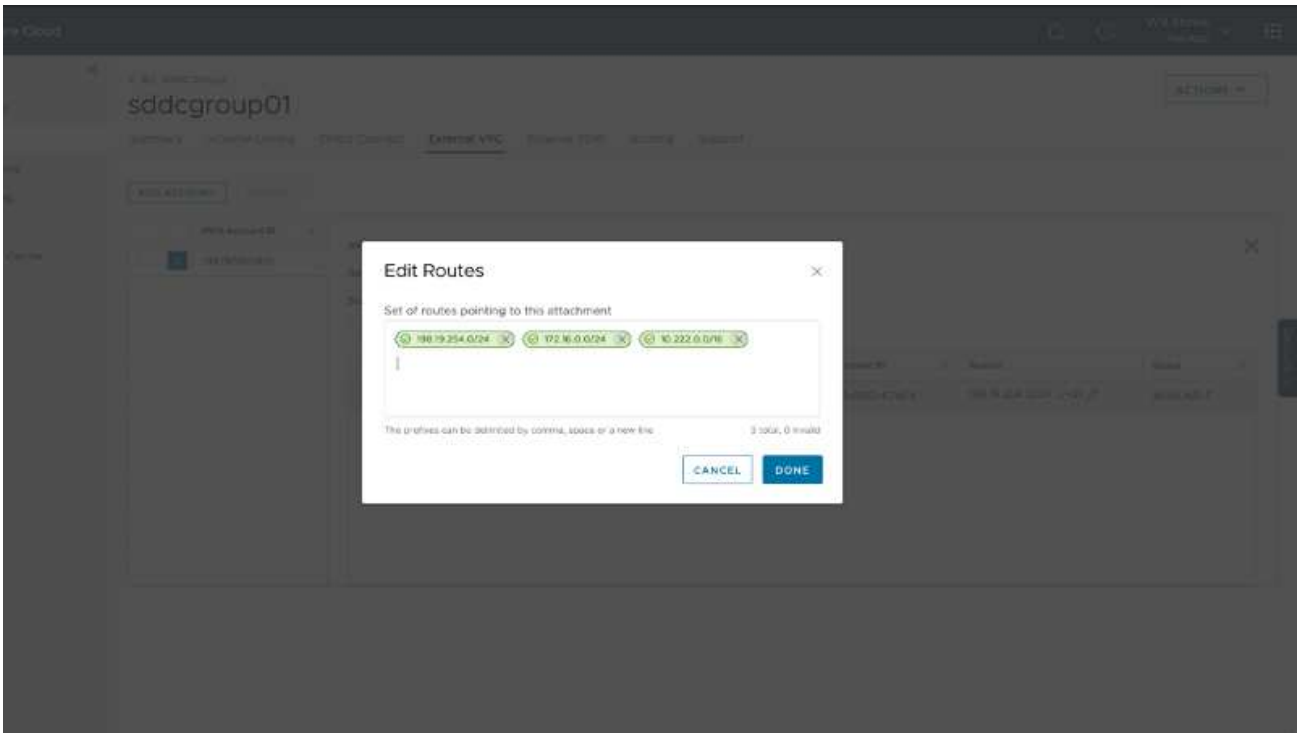
6. Torna alla console VMC e accetta l'allegato VPC. Il completamento di questo processo può richiedere circa 10 minuti.



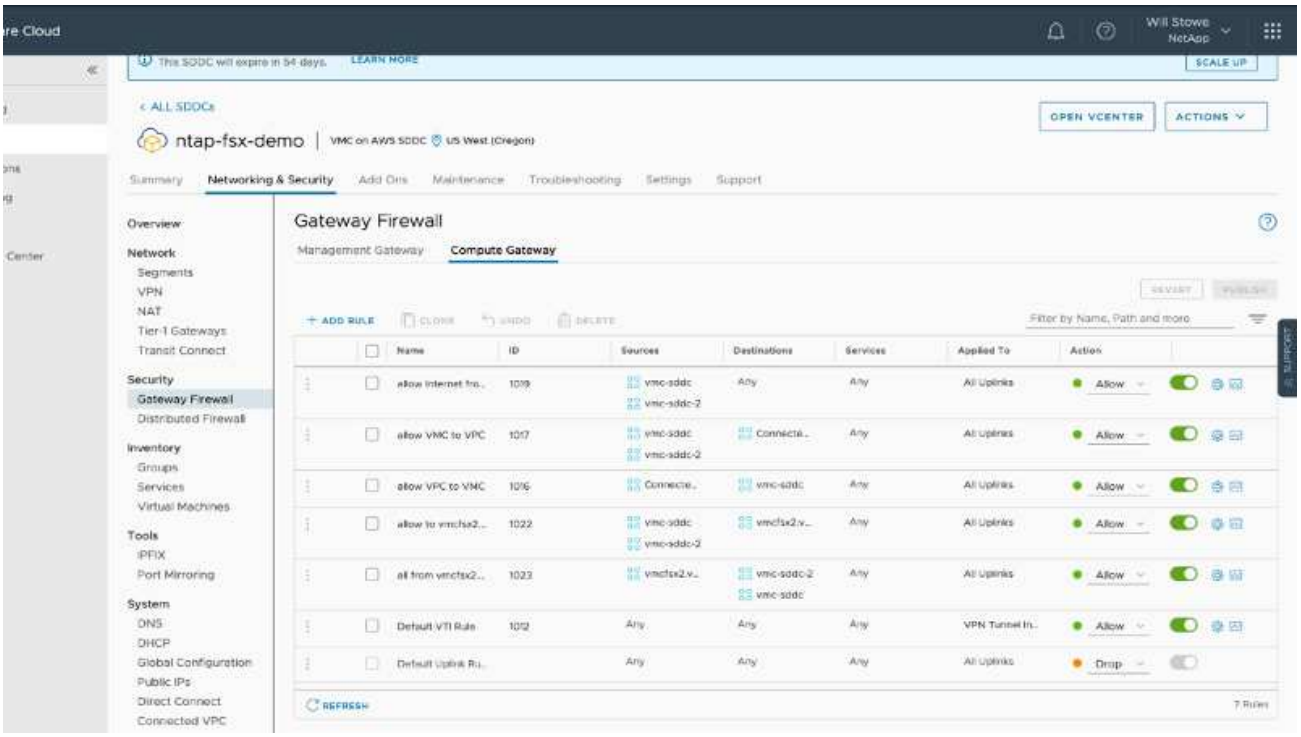
7. Nella scheda VPC esterna, fare clic sull'icona di modifica nella colonna Percorsi e aggiungere i seguenti percorsi richiesti:
   - Un percorso per l'intervallo IP mobile per Amazon FSx ONTAP"IP flottanti" .
   - Un percorso per l'intervallo IP mobile per Cloud Volumes ONTAP (se applicabile).
   - Un percorso per lo spazio di indirizzamento VPC esterno appena creato.



8. Infine, consentire il traffico bidirezionale"regole del firewall" per accedere a FSx/CVO. Segui questi"passaggi dettagliati" per le regole del firewall del gateway di elaborazione per la connettività del carico di lavoro SDDC.



9. Dopo aver configurato i gruppi firewall per il gateway di gestione e di elaborazione, è possibile accedere a vCenter come segue:



Il passaggio successivo consiste nel verificare che Amazon FSx ONTAP o Cloud Volumes ONTAP siano configurati in base alle proprie esigenze e che i volumi siano predisposti per scaricare i componenti di storage da vSAN per ottimizzare la distribuzione.

Distribuire e configurare l'ambiente di virtualizzazione su Azure

Come per le soluzioni on-premise, la pianificazione di Azure VMware Solution è fondamentale per un ambiente di produzione di successo per la creazione di VM e la migrazione.

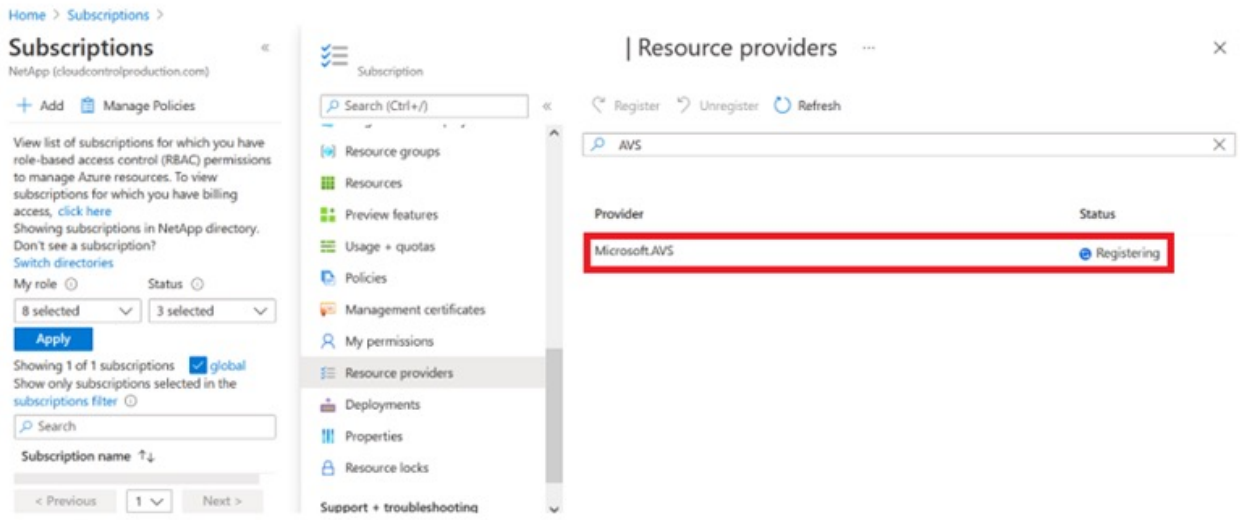
Questa sezione descrive come configurare e gestire Azure VMware Solution e come utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Registra il fornitore di risorse e crea un cloud privato**

Per utilizzare Azure VMware Solution, registrare prima il provider di risorse all'interno della sottoscrizione identificata:

1. Sign in al portale di Azure.
2. Nel menu del portale di Azure, seleziona Tutti i servizi.
3. Nella finestra di dialogo Tutti i servizi, immettere l'abbonamento e quindi selezionare Abbonamenti.
4. Per visualizzarlo, seleziona l'abbonamento dall'elenco degli abbonamenti.
5. Selezionare Provider di risorse e immettere Microsoft.AVS nella ricerca.
6. Se il fornitore di risorse non è registrato, selezionare Registra.

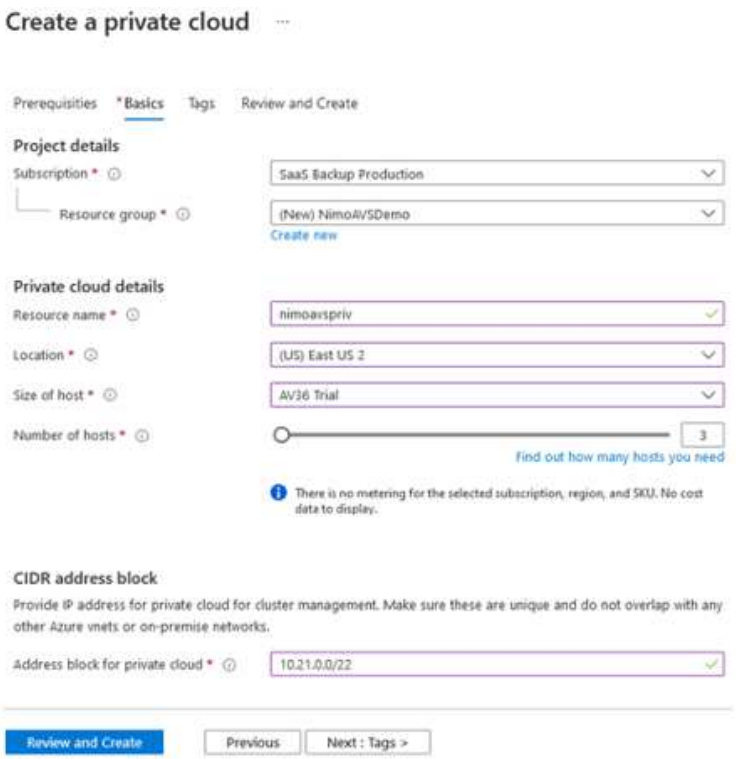




7. Dopo aver registrato il provider di risorse, creare un cloud privato Azure VMware Solution utilizzando il portale di Azure.
8. Sign in al portale di Azure.
9. Seleziona Crea una nuova risorsa.
10. Nella casella di testo Cerca nel Marketplace, immetti Azure VMware Solution e selezionalo dai risultati.
11. Nella pagina Soluzione Azure VMware, seleziona Crea.
12. Dalla scheda Nozioni di base, immettere i valori nei campi e selezionare Revisione + Crea.

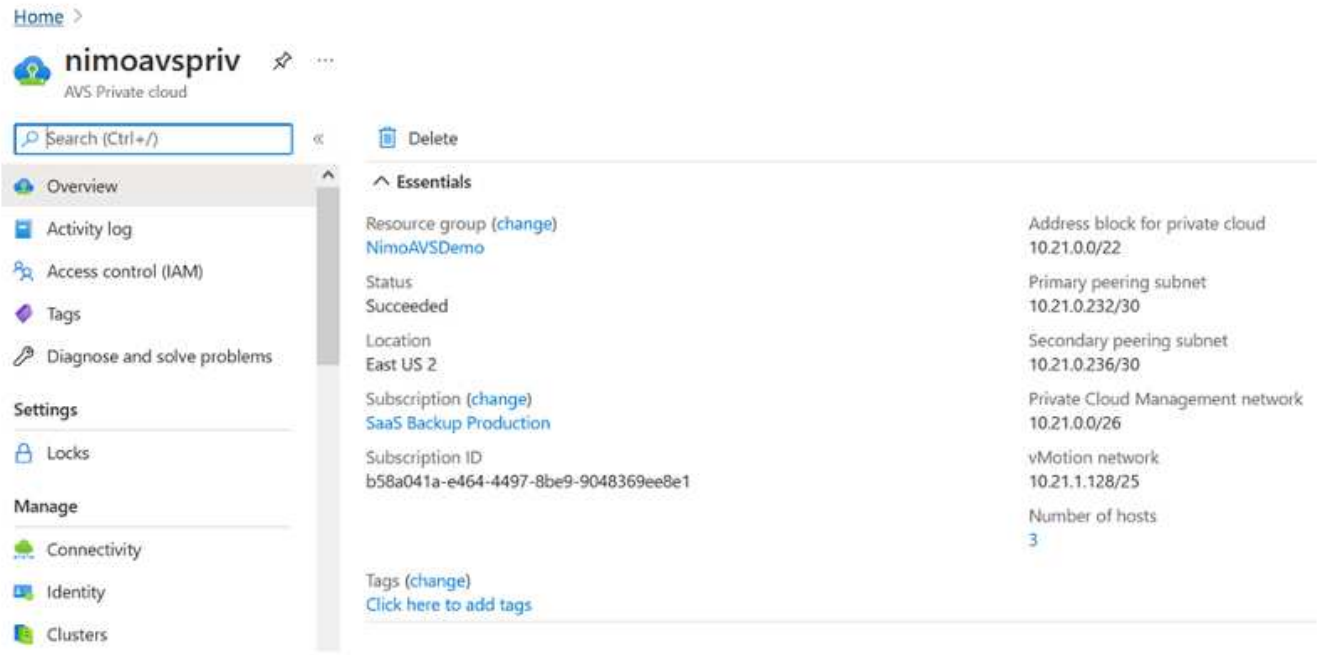
Note:

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



Il processo di provisioning dura circa 4-5 ore. Una volta completato il processo, verifica che la distribuzione sia avvenuta correttamente accedendo al cloud privato dal portale di Azure. Al termine della distribuzione viene visualizzato lo stato Riuscito.

Un cloud privato Azure VMware Solution richiede una rete virtuale Azure. Poiché Azure VMware Solution non supporta vCenter in locale, sono necessari passaggi aggiuntivi per l'integrazione con un ambiente locale esistente. È inoltre necessario configurare un circuito ExpressRoute e un gateway di rete virtuale. In attesa del completamento del provisioning del cluster, crea una nuova rete virtuale o usane una esistente per connetterti ad Azure VMware Solution.



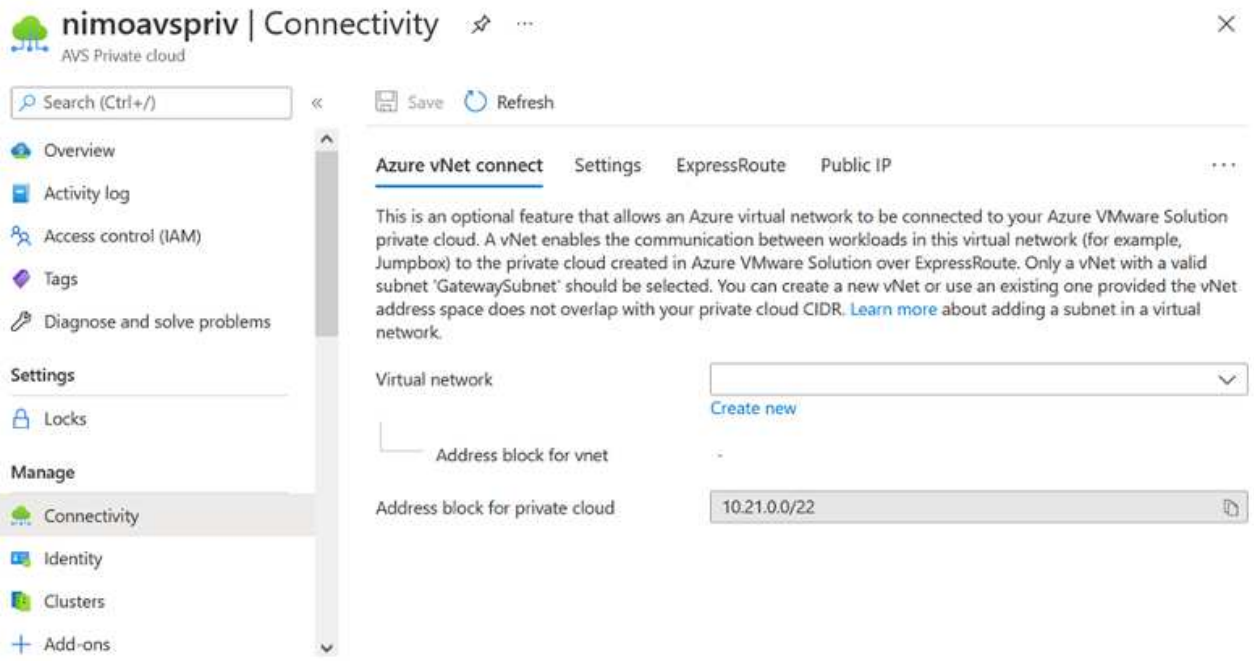
▼ **Connettiti a un gateway di rete virtuale ExpressRoute nuovo o esistente**

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

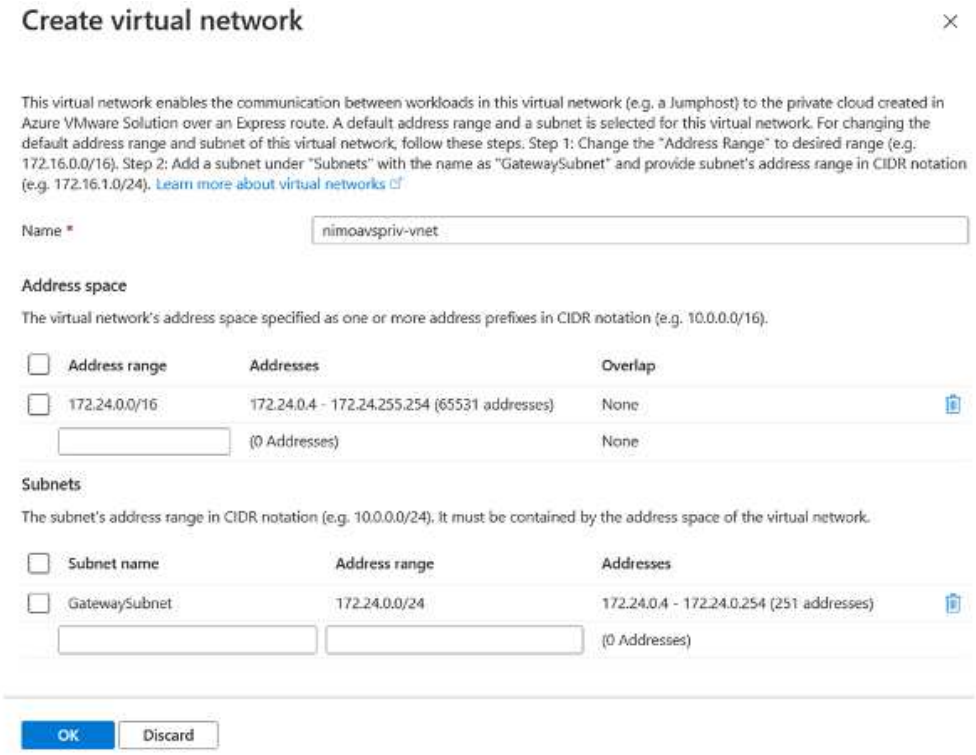
1. Vai al cloud privato Azure VMware Solution e accedi a Connettività nell'opzione Gestisci.
2. Selezionare Azure VNet Connect.
3. Per creare una nuova VNet, selezionare l'opzione Crea nuovo.

   Questa funzionalità consente di connettere una rete virtuale al cloud privato della soluzione Azure VMware. La VNet consente la comunicazione tra 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) nel cloud privato creato in Azure VMware Solution tramite ExpressRoute.

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



4. Fornire o aggiornare le informazioni per la nuova VNet e selezionare OK.



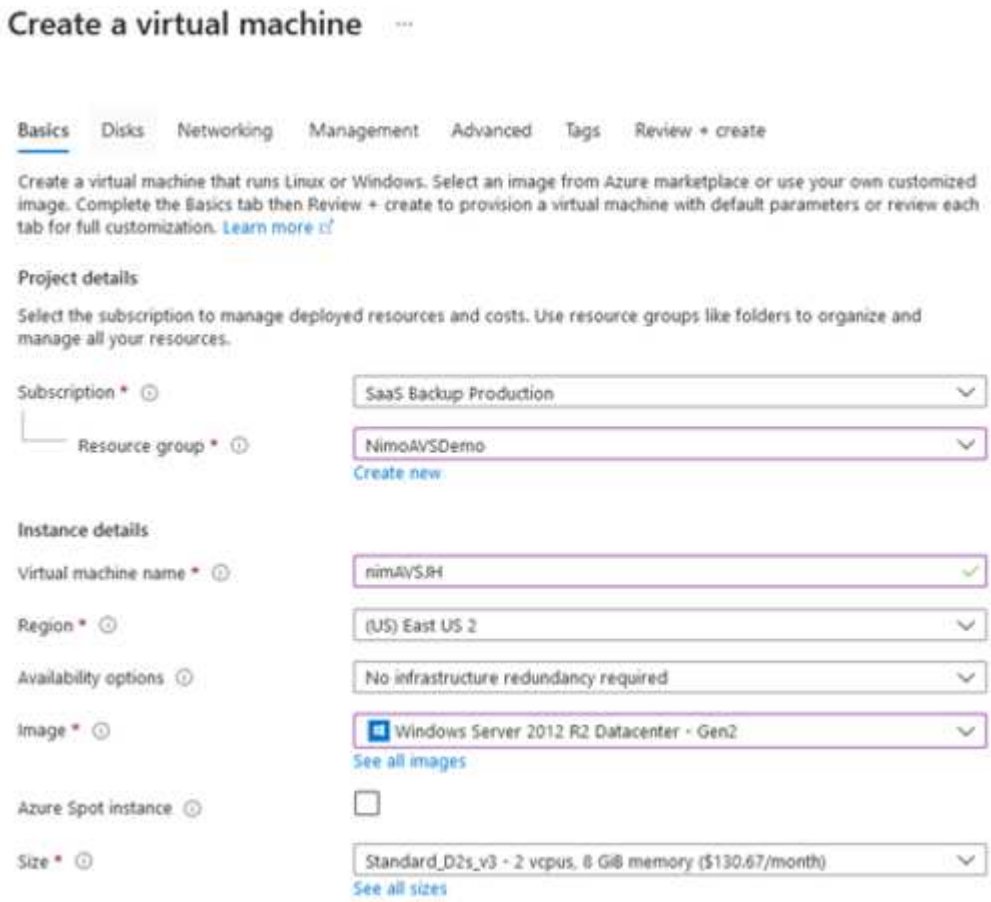
La rete virtuale con l'intervallo di indirizzi e la subnet del gateway specificati viene creata nella sottoscrizione e nel gruppo di risorse designati.

Se si crea una VNet manualmente, creare un gateway di rete virtuale con lo SKU appropriato ed ExpressRoute come tipo di gateway. Una volta completata la distribuzione, collegare la connessione ExpressRoute al gateway di rete virtuale contenente il cloud privato Azure VMware Solution utilizzando la chiave di autorizzazione. Per ulteriori informazioni, consultare

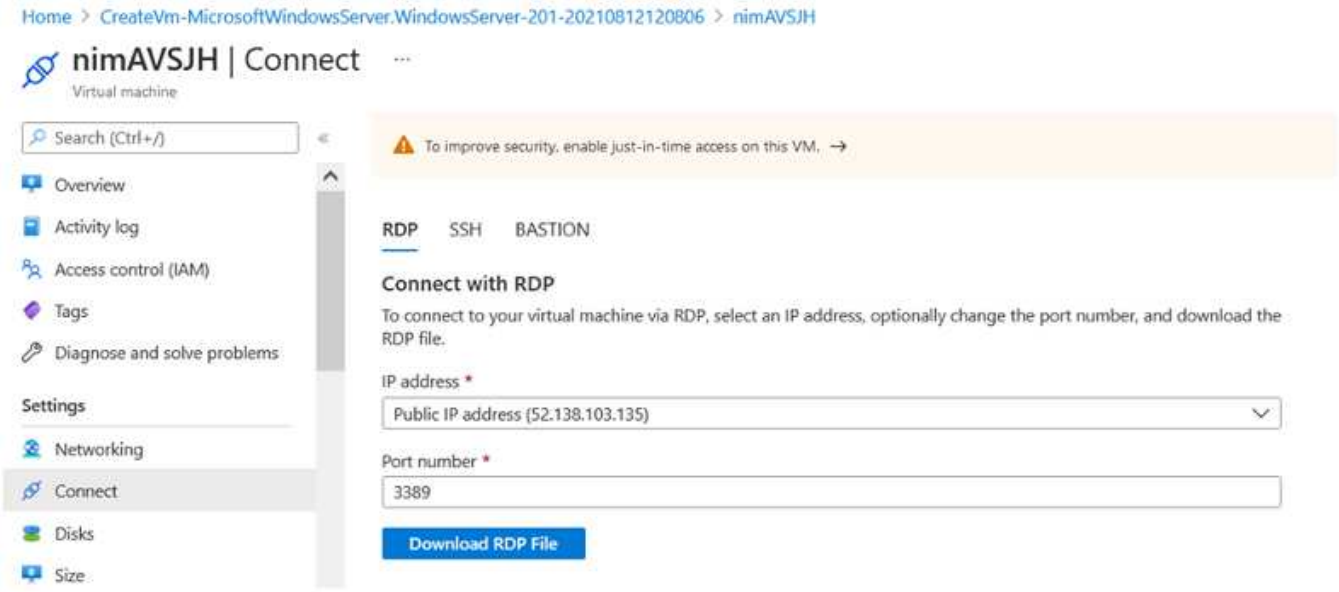
"Configura la rete per il tuo cloud privato VMware in Azure" .

▼ **Convalida la connessione di rete e l'accesso al cloud privato di Azure VMware Solution**

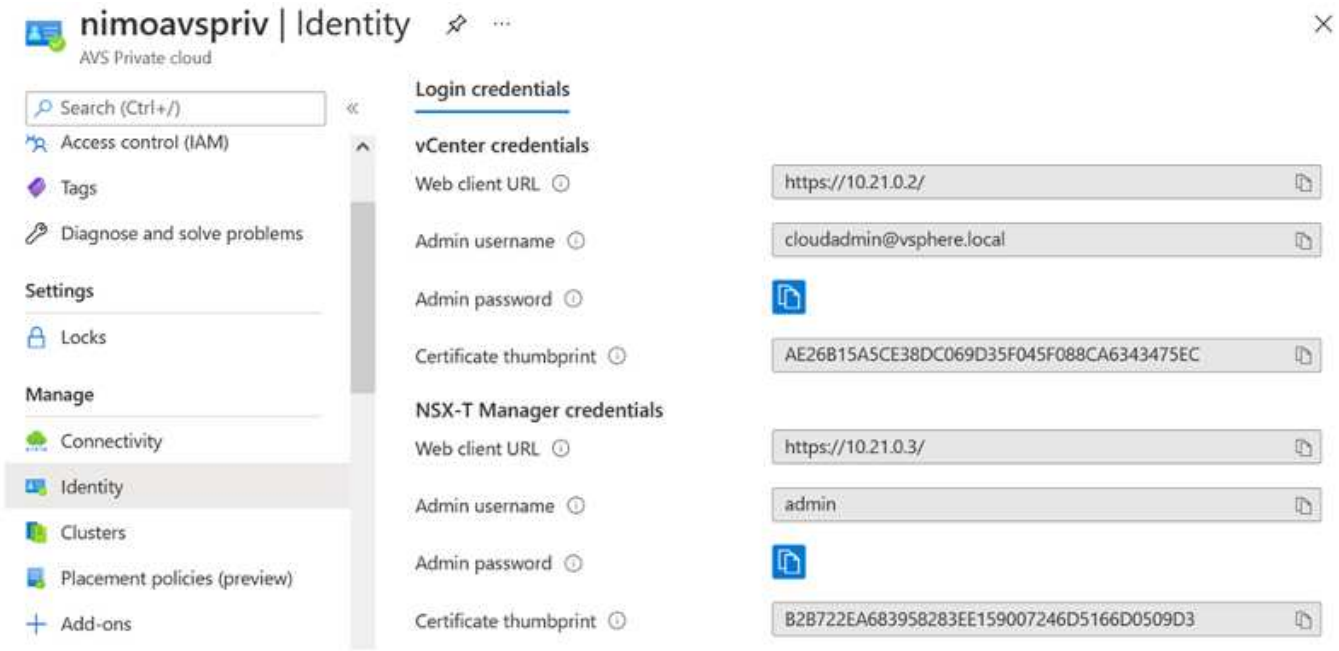
Azure VMware Solution non consente di gestire un cloud privato con VMware vCenter locale. Al contrario, è necessario un host jump per connettersi all'istanza vCenter di Azure VMware Solution. Creare un jump host nel gruppo di risorse designato e accedere ad Azure VMware Solution vCenter. Questo jump host dovrebbe essere una VM Windows sulla stessa rete virtuale creata per la connettività e dovrebbe fornire accesso sia a vCenter che a NSX Manager.



Dopo aver eseguito il provisioning della macchina virtuale, utilizzare l'opzione Connetti per accedere a RDP.



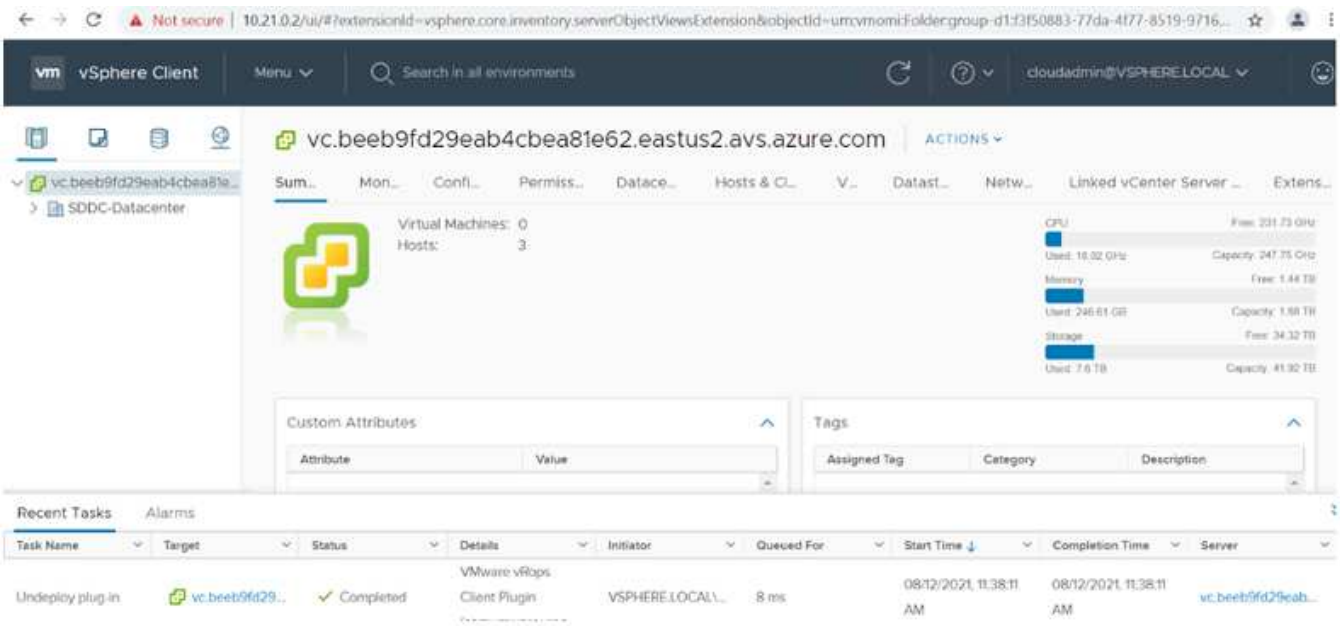
Sign in a vCenter da questa macchina virtuale jump host appena creata utilizzando l'utente cloud admin. Per accedere alle credenziali, vai al portale di Azure e seleziona Identità (sotto l'opzione Gestisci nel cloud privato). Gli URL e le credenziali utente per il cloud privato vCenter e NSX-T Manager possono essere copiati da qui.



Nella macchina virtuale Windows, apri un browser e vai all'URL del client web vCenter(`"https://10.21.0.2/"`) e utilizzare il nome utente amministratore come **cloudadmin@vsphere.local** e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche tramite l'URL del client Web(`"https://10.21.0.3/"`) e utilizzare il nome utente amministratore e incollare la password copiata per creare nuovi segmenti o modificare i gateway di livello esistenti.

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





L'SDDC della soluzione Azure VMware è ora distribuito e configurato. Sfrutta ExpressRoute Global Reach per connettere l'ambiente on-premise al cloud privato Azure VMware Solution. Per ulteriori informazioni, consultare "Connetti gli ambienti locali alla soluzione Azure VMware" .

Distribuisci e configura l'ambiente di virtualizzazione su Google Cloud Platform (GCP)

Come per gli ambienti on-premise, la pianificazione di Google Cloud VMware Engine (GCVE) è fondamentale per un ambiente di produzione di successo per la creazione di VM e la migrazione.

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

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

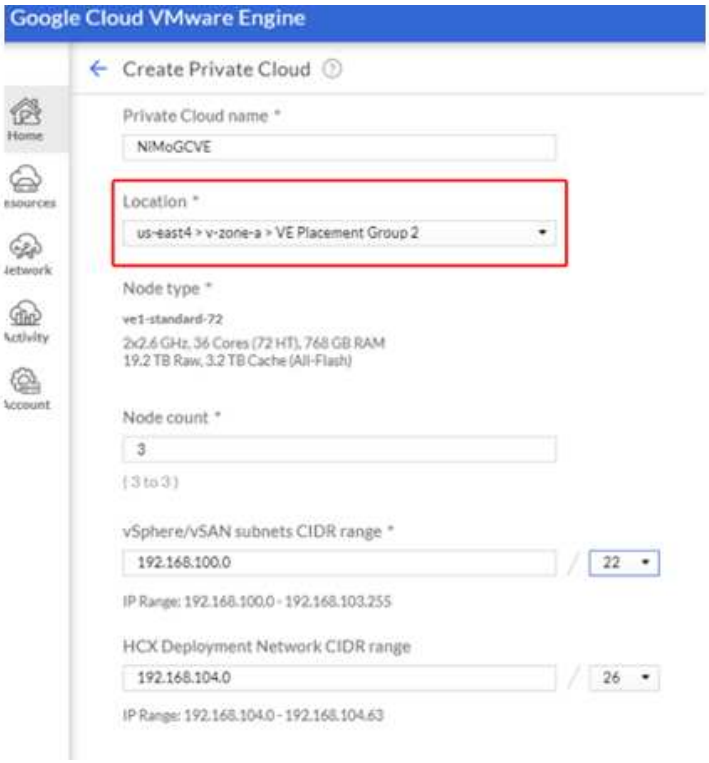
▼ Distribuisci e configura GCVE

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

Fare clic sul pulsante "Nuovo cloud privato" e immettere la configurazione desiderata per il cloud privato GCVE. In "Posizione", assicurati di distribuire il cloud privato nella stessa regione/zona in cui è distribuito NetApp Volumes/CVO, per garantire le migliori prestazioni e la latenza più bassa.

Prerequisiti:

- Imposta il ruolo IAM di amministratore del servizio VMware Engine
- "Abilita l'accesso all'API di VMWare Engine e la quota del nodo"
- Assicurati che l'intervallo CIDR non si sovrapponga ad alcuna delle tue subnet locali o cloud. L'intervallo CIDR deve essere /27 o superiore.



Nota: la creazione di un cloud privato può richiedere dai 30 minuti alle 2 ore.

▼ Abilita l'accesso privato a GCVE

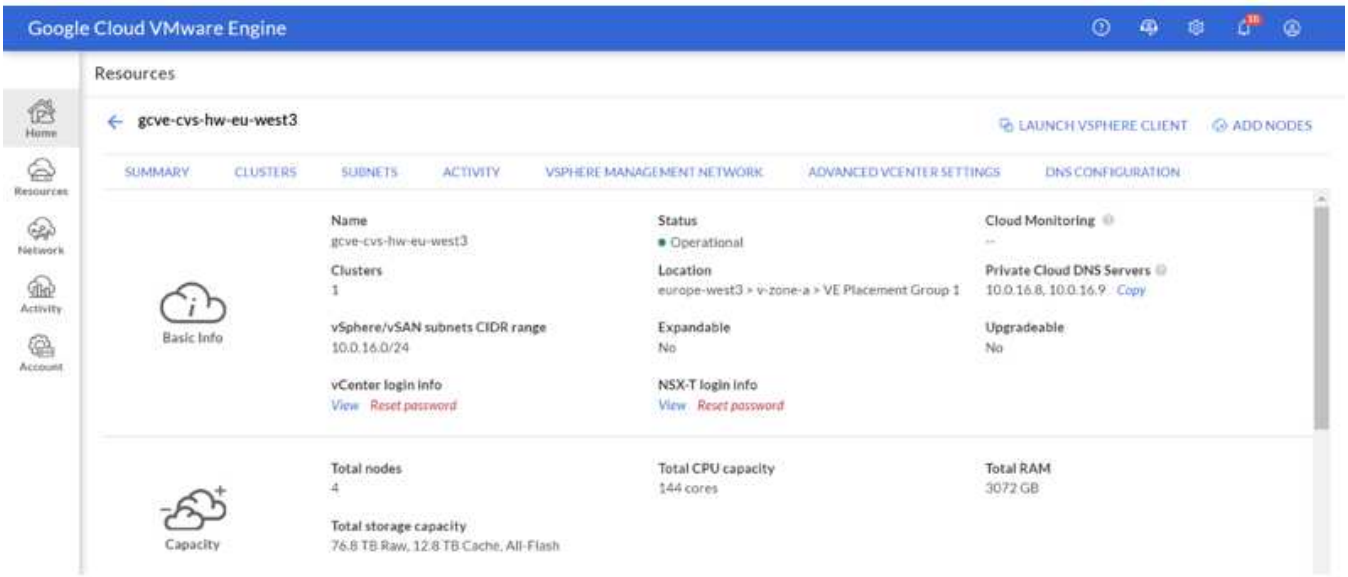
Una volta eseguito il provisioning del Private Cloud, configurare l'accesso privato al Private Cloud per una connessione al percorso dati ad alta velocità e bassa latenza.

In questo modo, la rete VPC in cui sono in esecuzione le istanze di Cloud Volumes ONTAP potrà comunicare con il GCVE Private Cloud. Per farlo, segui "Documentazione GCP". Per Cloud Volume Service, stabilisci una connessione tra VMware Engine e Google Cloud NetApp Volumes eseguendo un peering una tantum tra i progetti host del tenant. Per i passaggi dettagliati, segui "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

Sign in a vcenter utilizzando l'utente CloudOwner@gve.local. Per accedere alle credenziali, vai al portale

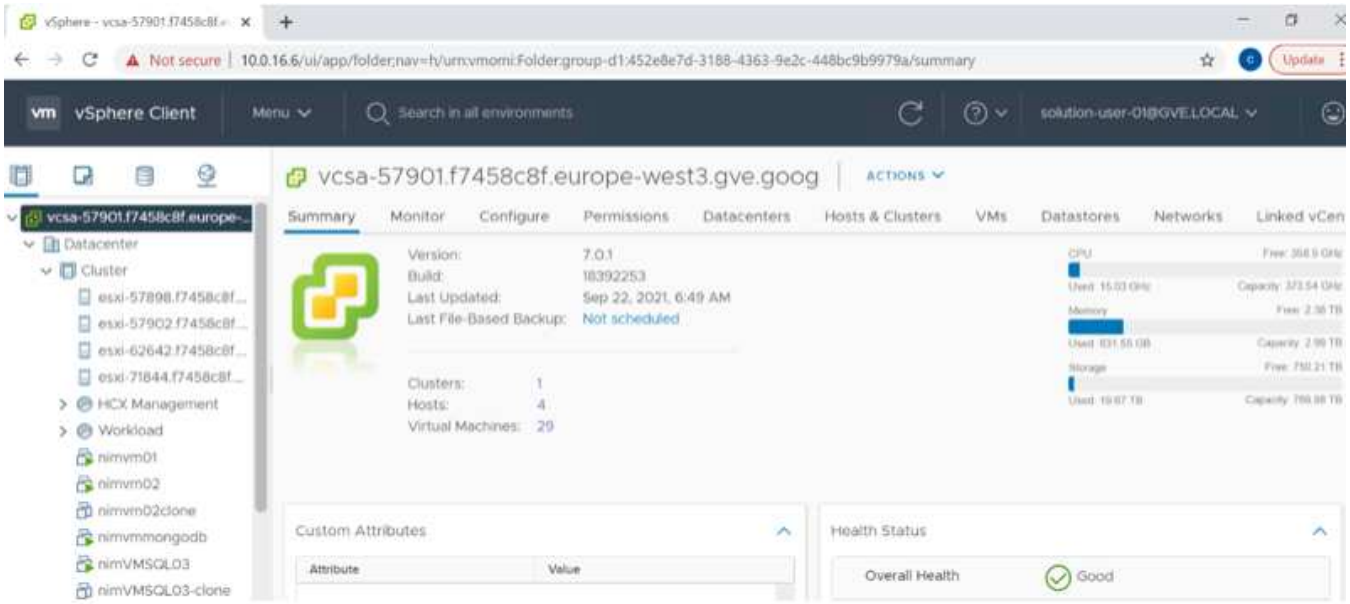
VMware Engine, vai a Risorse e seleziona il cloud privato appropriato. Nella sezione Informazioni di base, fare clic sul collegamento Visualizza per le informazioni di accesso a vCenter (vCenter Server, HCX Manager) o alle informazioni di accesso a NSX-T (NSX Manager).



In una macchina virtuale Windows, apri un browser e vai all'URL del client web vCenter(`"https://10.0.16.6/"`) e utilizzare il nome utente amministratore come CloudOwner@gve.local e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche tramite l'URL del client Web(`"https://10.0.16.11/"`) e utilizzare il nome utente amministratore e incollare la password copiata per creare nuovi segmenti o modificare i gateway di livello esistenti.

Per connettersi da una rete locale al cloud privato VMware Engine, sfruttare la VPN cloud o Cloud Interconnect per una connettività appropriata e assicurarsi che le porte richieste siano aperte. Per i passaggi dettagliati, seguire questo"collegamento" .





▼ **Distribuisci il datastore supplementare Google Cloud NetApp Volumes su GCVE**

Fare riferimento"Procedura per distribuire un datastore NFS supplementare con NetApp Volumes su GCVE"

Storage NetApp nei cloud pubblici

Opzioni di archiviazione NetApp per i provider di cloud pubblico

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

AWS / VMC

AWS supporta l'archiviazione NetApp nelle seguenti configurazioni:

- FSx ONTAP come storage connesso agli ospiti
- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- FSx ONTAP come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione di connessione guest per VMC" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per VMC" .

Azzurro / AVS

Azure supporta l'archiviazione NetApp nelle seguenti configurazioni:

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

Visualizza il dettaglio"opzioni di archiviazione di connessione ospite per AVS" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per AVS" .

GCP / GCVE

Google Cloud supporta l'archiviazione NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione per la connessione degli ospiti per GCVE" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per GCVE" .

Per saperne di più"Supporto del datastore Google Cloud NetApp Volumes per Google Cloud VMware Engine (blog NetApp)" O"Come utilizzare Google Cloud NetApp Volumes come datastore per Google Cloud VMware Engine (blog di Google)"

Amazon Web Services: opzioni per l'utilizzo dello storage NetApp

Lo storage NetApp può essere collegato ad Amazon Web Services come storage guest connesso o supplementare.

Amazon FSx for NetApp ONTAP (FSx ONTAP) come datastore NFS supplementare

Amazon FSx ONTAP offre eccellenti opzioni per distribuire e gestire carichi di lavoro applicativi insieme ai servizi file, riducendo al contempo il TCO rendendo i requisiti dei dati uniformi al livello applicativo. Qualunque sia il caso d'uso, scegli VMware Cloud on AWS insieme ad Amazon FSx ONTAP per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti da locale ad AWS, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per collegare l'archiviazione.

Per maggiori informazioni, visitare:

- "FSx ONTAP come datastore NFS supplementare: panoramica"
- "Amazon FSx per ONTAP come datastore supplementare"

Amazon FSx for NetApp ONTAP come storage connesso agli ospiti

Amazon FSx ONTAP è un servizio completamente gestito che fornisce un archivio file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità, basato sul famoso file system ONTAP di NetApp. FSx ONTAP combina le caratteristiche, le prestazioni, le capacità e le operazioni API note dei file system NetApp con l'agilità, la scalabilità e la semplicità di un servizio AWS completamente gestito.

FSx ONTAP offre uno storage di file condiviso ricco di funzionalità, veloce e flessibile, ampiamente accessibile da istanze di elaborazione Linux, Windows e macOS in esecuzione su AWS o in locale. FSx ONTAP offre storage su unità a stato solido (SSD) ad alte prestazioni con latenze inferiori al millisecondo. Con FSx ONTAP puoi raggiungere livelli di prestazioni SSD per il tuo carico di lavoro, pagando per l'archiviazione SSD solo una piccola parte dei tuoi dati.

Gestire i dati con FSx ONTAP è più semplice perché puoi creare snapshot, clonare e replicare i tuoi file con un semplice clic. Inoltre, FSx ONTAP suddivide automaticamente i dati in livelli di storage più economici ed elastici, riducendo la necessità di provisioning o gestione della capacità.

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

Per maggiori informazioni, visitare"FSx ONTAP come storage connesso agli ospiti"

Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Per maggiori informazioni, visitare"CVO come Guest Connected Storage" .

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

Questo documento descrive come montare Amazon FSx ONTAP come datastore NFS con VMware Cloud su AWS.

Introduzione

Ogni organizzazione di successo è in cammino verso la trasformazione e la modernizzazione. Come parte di questo processo, le aziende solitamente sfruttano i propri investimenti VMware esistenti per sfruttare i vantaggi del cloud e valutare come migrare, espandere, estendere e fornire il disaster recovery per i processi nel modo più fluido possibile. I clienti che migrano verso il cloud devono valutare i casi d'uso per elasticità e burst, uscita dal data center, consolidamento del data center, scenari di fine vita, fusioni, acquisizioni e così via.

Sebbene VMware Cloud su AWS sia l'opzione preferita dalla maggior parte dei clienti perché offre funzionalità ibride uniche, le limitate opzioni di storage nativo ne hanno limitato l'utilità per le organizzazioni con carichi di lavoro ad alta intensità di storage. Poiché lo storage è direttamente collegato agli host, l'unico modo per scalare lo storage è aggiungere più host, il che può aumentare i costi del 35-40% o più per carichi di lavoro ad alta intensità di storage. Questi carichi di lavoro necessitano di spazio di archiviazione aggiuntivo e prestazioni separate, non di potenza aggiuntiva, ma ciò significa pagare per host aggiuntivi. Questo è dove il "integrazione recente" di FSx ONTAP risulta utile per carichi di lavoro che richiedono elevate prestazioni e storage con VMware Cloud su AWS.

Consideriamo il seguente scenario: un cliente necessita di otto host per la potenza (vCPU/vMem), ma ha anche un fabbisogno sostanziale di spazio di archiviazione. In base alla loro valutazione, per soddisfare i requisiti di archiviazione sono necessari 16 host. Ciò aumenta il TCO complessivo perché devono acquistare tutta quella potenza aggiuntiva quando in realtà hanno bisogno solo di più spazio di archiviazione. Ciò è applicabile a qualsiasi caso d'uso, tra cui migrazione, disaster recovery, bursting, sviluppo/test e così via.

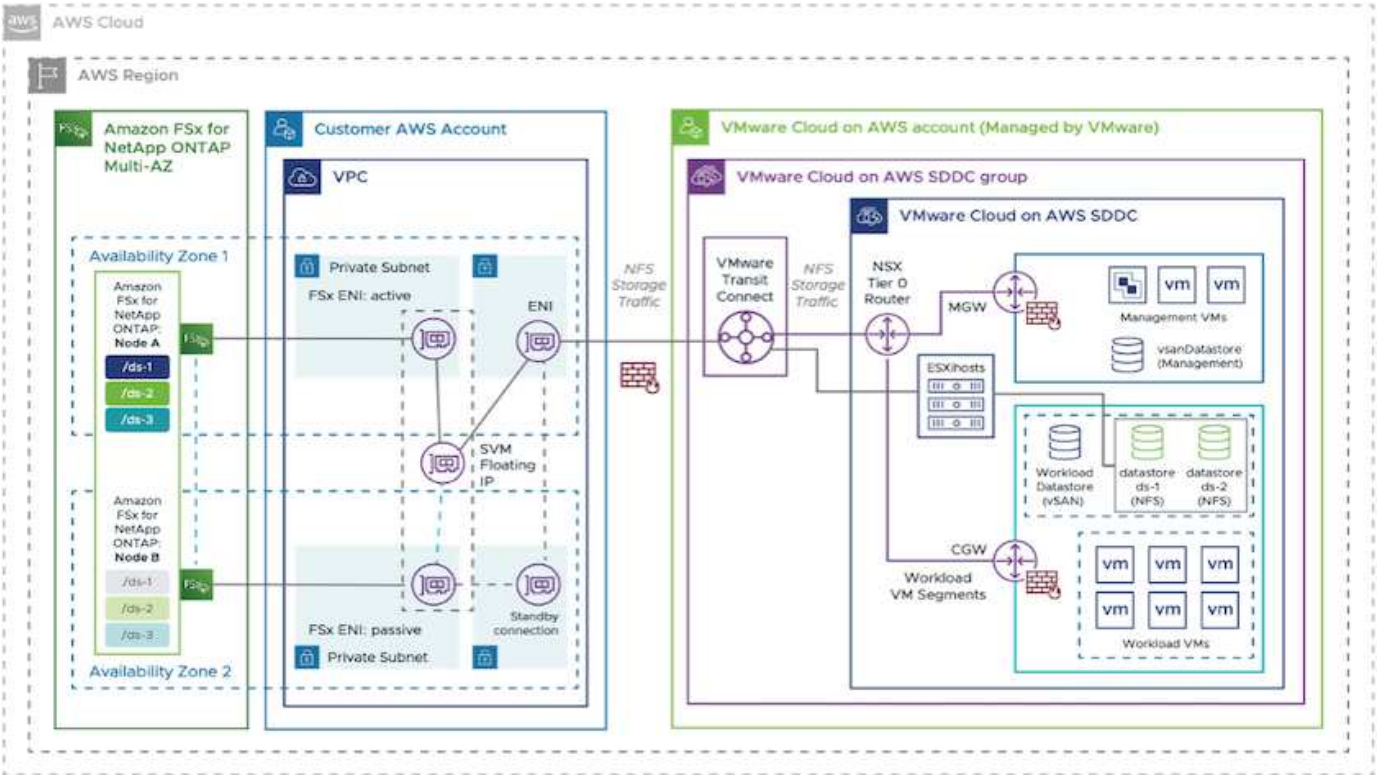
Questo documento illustra i passaggi necessari per predisporre e collegare FSx ONTAP come datastore NFS per VMware Cloud su AWS.

Questa soluzione è disponibile anche da VMware. Si prega di visitare il"Documentazione di VMware Cloud su AWS" per maggiori informazioni.

Opzioni di connettività

VMware Cloud on AWS supporta sia le distribuzioni multi-AZ che single-AZ di FSx ONTAP.

Questa sezione descrive l'architettura di connettività di alto livello insieme ai passaggi necessari per implementare la soluzione per espandere lo storage in un cluster SDDC senza la necessità di aggiungere host aggiuntivi.



I passaggi di distribuzione di alto livello sono i seguenti:

1. Creare Amazon FSx ONTAP in una nuova VPC designata.
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 effettuare il provisioning e collegare FSx ONTAP come datastore NFS, è necessario innanzitutto configurare un ambiente VMware on Cloud SDDC o aggiornare un SDDC esistente alla versione 1.20 o successiva. Per ulteriori informazioni, consultare il sito "Introduzione a VMware Cloud su AWS" .

FSx ONTAP non è attualmente supportato con i cluster estesi.

Conclusione

Questo documento illustra i passaggi necessari per configurare Amazon FSx ONTAP con VMware Cloud su AWS. Amazon FSx ONTAP offre eccellenti opzioni per distribuire e gestire carichi di lavoro applicativi insieme ai servizi file, riducendo al contempo il TCO rendendo i requisiti dei dati uniformi al livello applicativo. Qualunque sia il caso d'uso, scegli VMware Cloud on AWS insieme ad Amazon FSx ONTAP per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti da locale ad AWS, portabilità

bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per collegare l'archiviazione. Ricorda che è cambiata solo la posizione dei dati e i nuovi nomi; gli strumenti e i processi sono rimasti gli stessi e Amazon FSx ONTAP aiuta a ottimizzare la distribuzione complessiva.

Per saperne di più su questo processo, non esitate a seguire il video tutorial dettagliato.

Amazon FSx ONTAP VMware Cloud

Creazione di un datastore NFS supplementare in AWS

Dopo che VMware Cloud è pronto e connesso ad AWS VPC, è necessario distribuire Amazon FSx ONTAP in una VPC appena designata anziché nella VPC predefinita connessa o esistente.

Per iniziare, distribuisci un VPC aggiuntivo nella stessa regione e zona di disponibilità in cui risiede SDDC, quindi distribuisci Amazon FSx ONTAP nel nuovo VPC. "Configurazione di un gruppo SDDC nel VMware Cloud" La console abilita le opzioni di configurazione di rete necessarie per connettersi alla VPC appena designata in cui verrà distribuito FSx ONTAP .

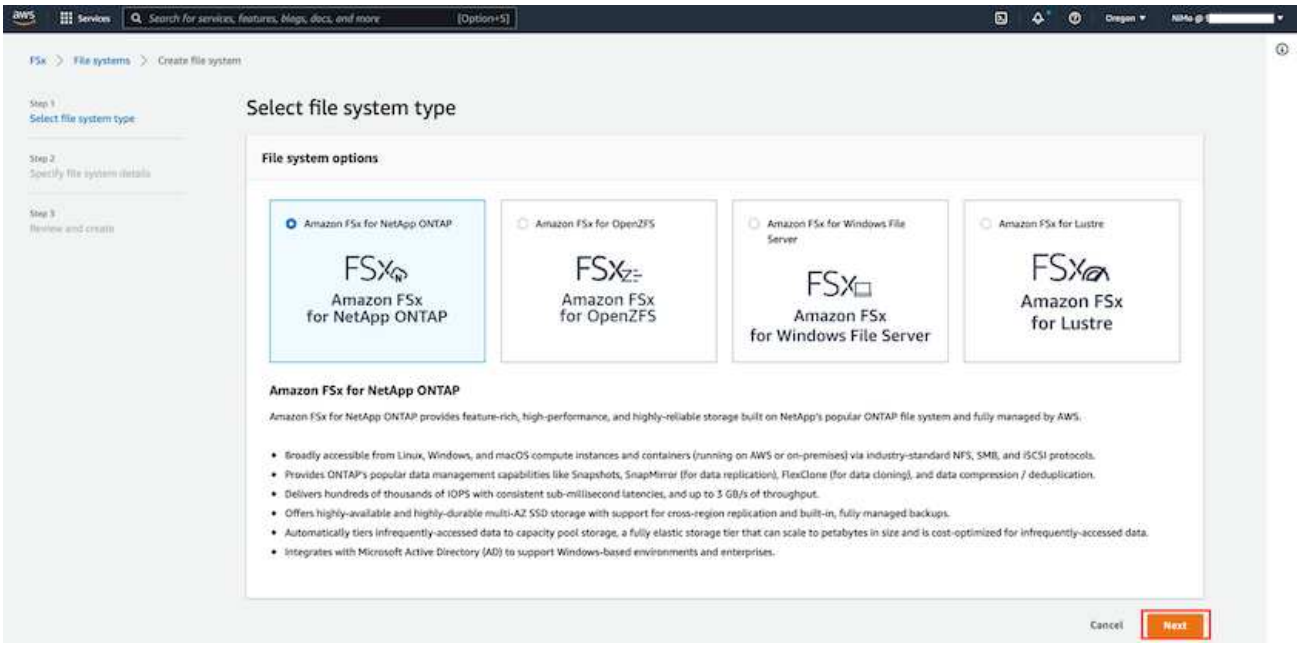
Distribuisci FSx ONTAP nella stessa zona di disponibilità di VMware Cloud su AWS SDDC.

Non è possibile distribuire FSx ONTAP nella VPC connessa. In alternativa, è necessario distribuirlo in una nuova VPC designata e quindi connettere la VPC a un VMware Managed Transit Gateway (vTGW) tramite gruppi SDDC.

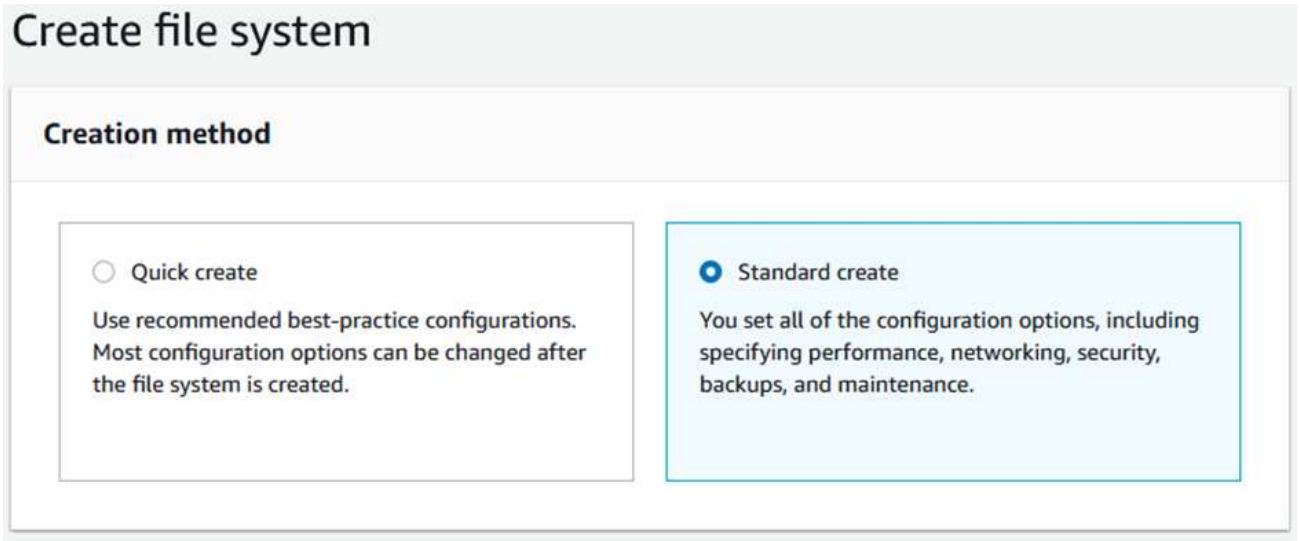
▼ **Passaggio 1: creare Amazon FSx ONTAP in una nuova VPC designata**

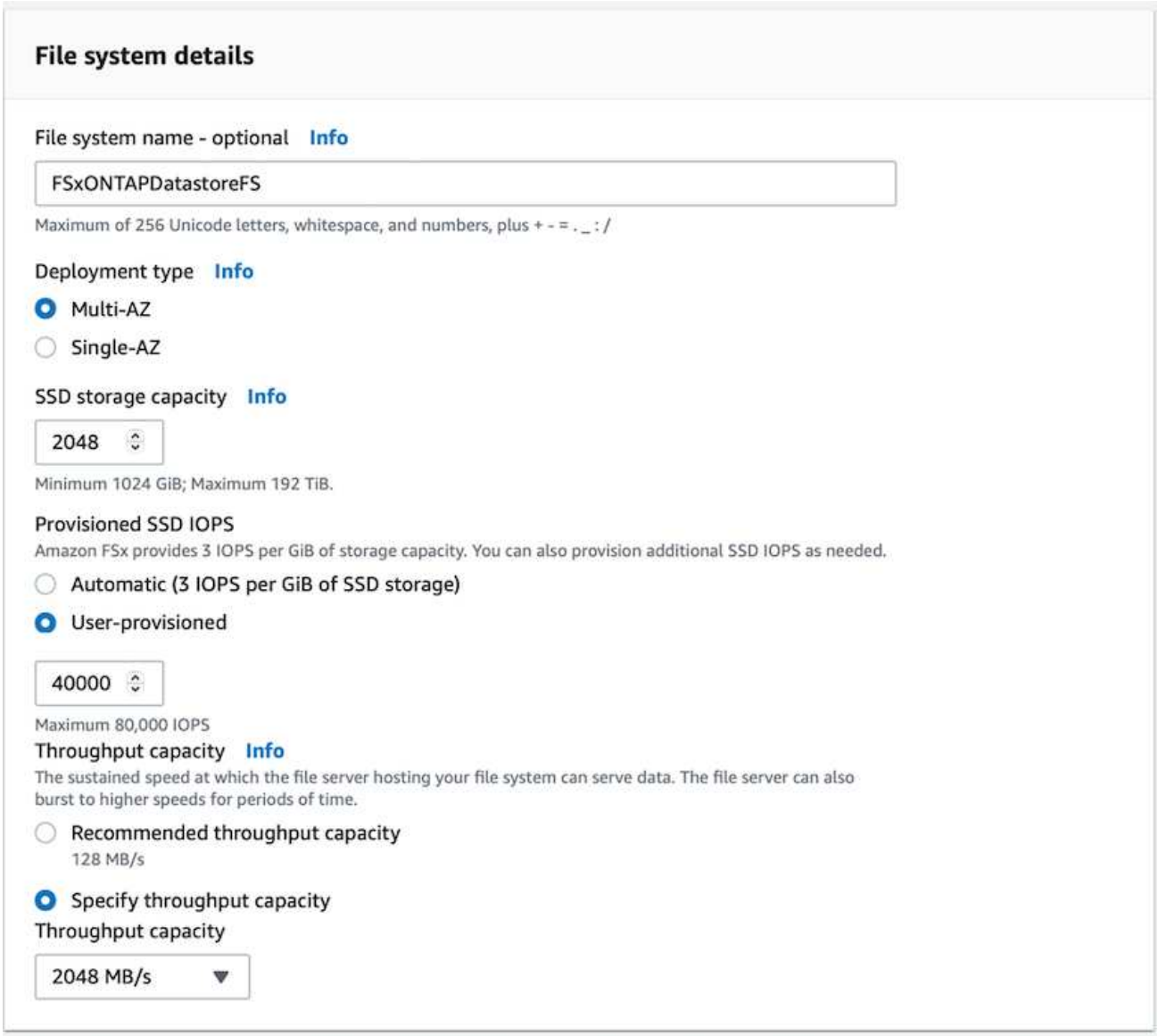
Per creare e montare il file system Amazon FSx ONTAP , completare i seguenti passaggi:

1. Aprire la console Amazon FSx all'indirizzo `https://console.aws.amazon.com/fsx/` e seleziona **Crea file system** per avviare la procedura guidata **Creazione file system**.
2. Nella pagina Seleziona tipo di file system, seleziona * Amazon FSx ONTAP* e poi fai clic su **Avanti**. Viene visualizzata la pagina **Crea file system**.



3. Per il metodo di creazione, seleziona **Creazione standard**.





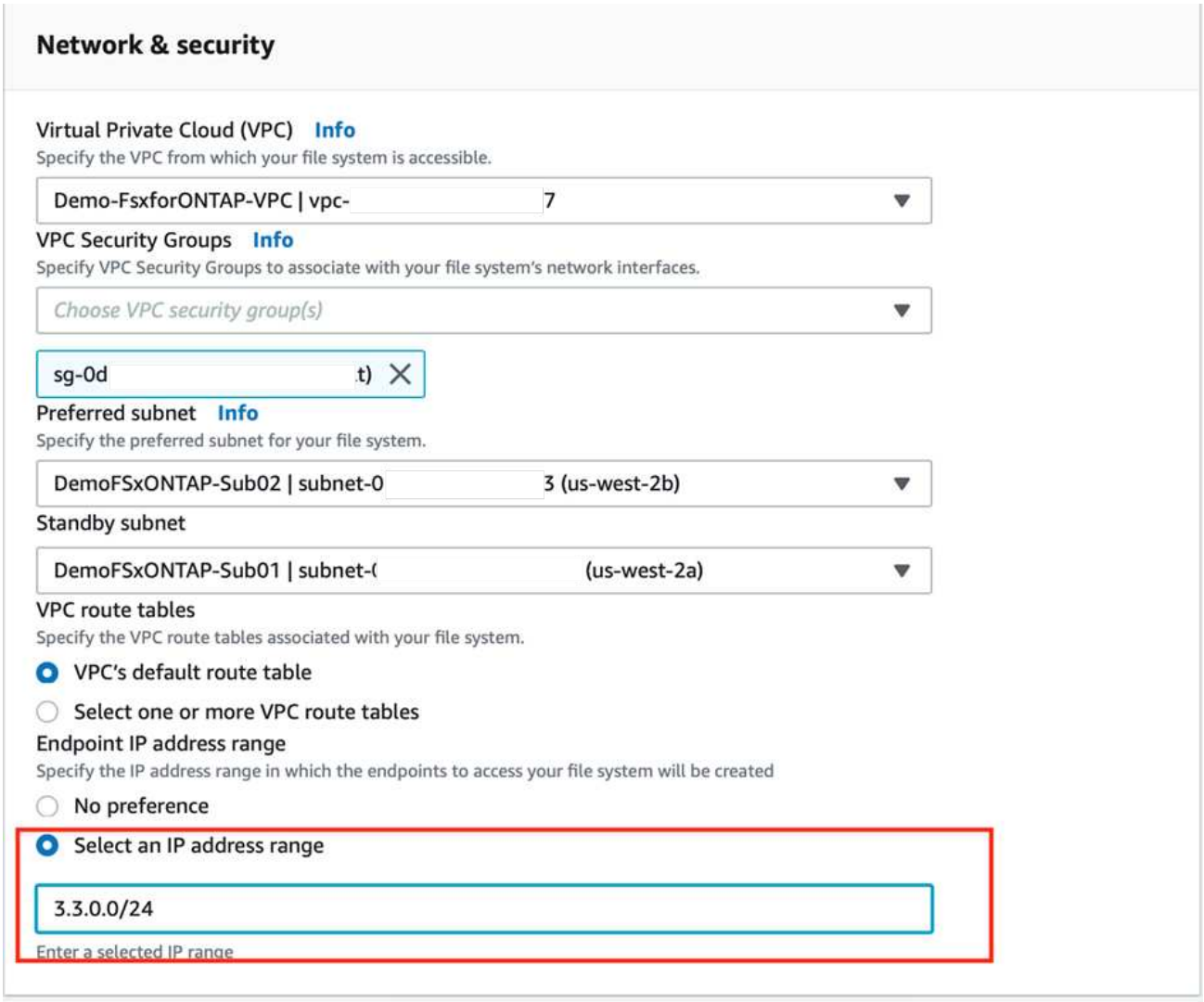
Le dimensioni del datastore variano notevolmente da cliente a cliente. Sebbene il numero consigliato di macchine virtuali per datastore NFS sia soggettivo, molti fattori determinano il numero ottimale di VM che possono essere posizionate su ciascun datastore. Sebbene la maggior parte degli amministratori consideri solo la capacità, la quantità di I/O simultanei inviati ai VMDK è uno dei fattori più importanti per le prestazioni complessive. Utilizzare le statistiche sulle prestazioni locali per dimensionare di conseguenza i volumi del datastore.

4. Nella sezione **Networking** per Virtual Private Cloud (VPC), seleziona la VPC appropriata e le subnet preferite insieme alla tabella di routing. In questo caso, dal menu a discesa viene selezionato Demo-FSxforONTAP-VPC.

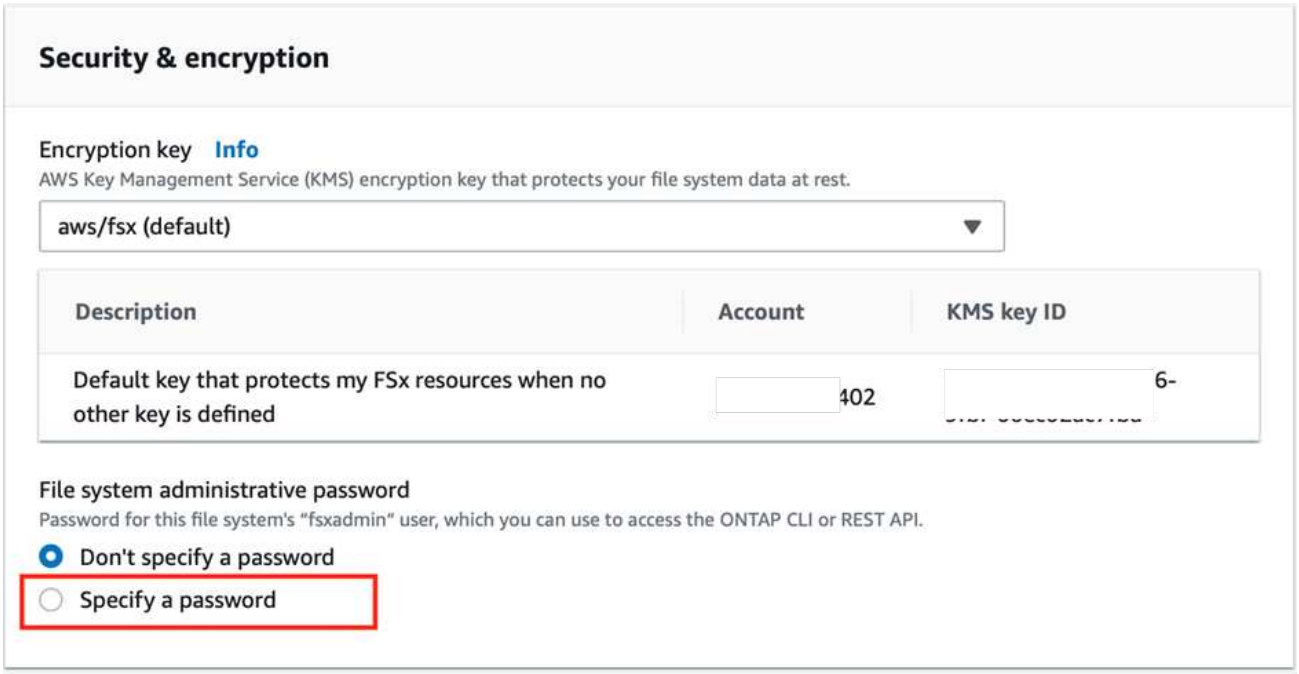
Assicurarsi che si tratti di una nuova VPC designata e non della VPC connessa.

Per impostazione predefinita, FSx ONTAP utilizza 198.19.0.0/16 come intervallo di indirizzi IP endpoint predefinito per il file system. Assicurarsi che l'intervallo di indirizzi IP dell'endpoint non sia in conflitto con la VMC sull'AWS SDDC, le subnet VPC associate e l'infrastruttura locale. In caso di dubbi, utilizzare un intervallo non sovrapposto e senza

conflitti.

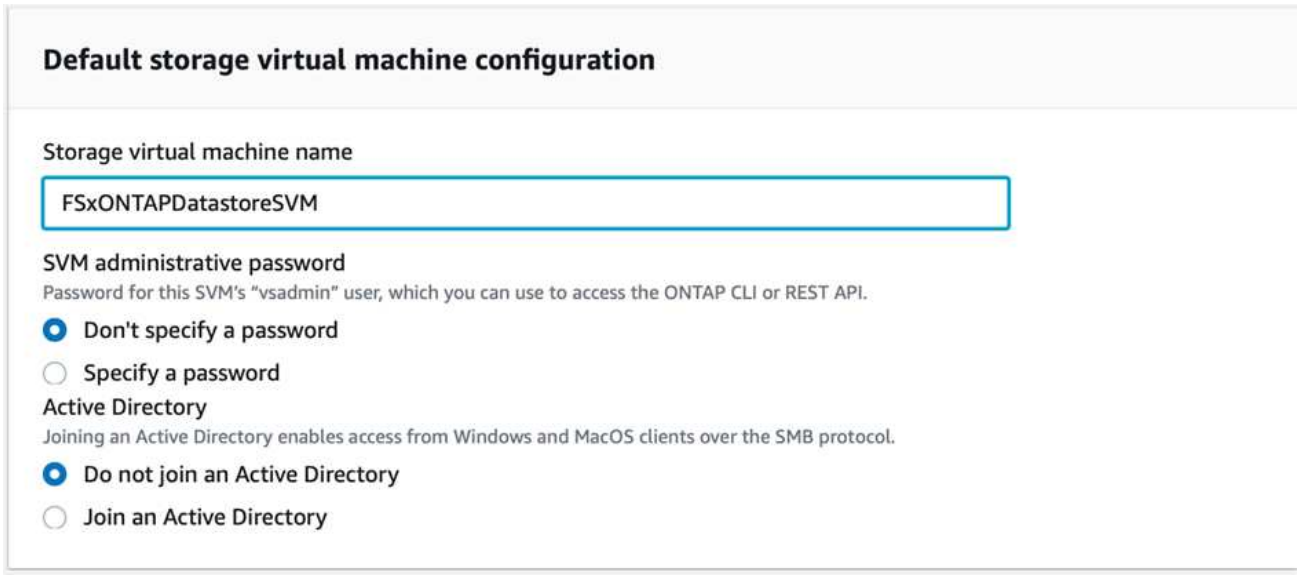


5. Nella sezione **Sicurezza e crittografia** per la chiave di crittografia, seleziona la chiave di crittografia AWS Key Management Service (AWS KMS) che protegge i dati inattivi del file system. Per la **Password amministrativa del file system**, immettere una password sicura per l'utente fsxadmin.



6. Nella sezione **Configurazione macchina virtuale di archiviazione predefinita**, specificare il nome della SVM.

> A partire da GA, sono supportati quattro datastore NFS.



7. Nella sezione **Configurazione volume predefinita**, specificare il nome del volume e le dimensioni richieste per il datastore e fare clic su **Avanti**. Dovrebbe essere un volume NFSv3. Per **Efficienza di archiviazione**, selezionare **Abilitato** per attivare le funzionalità di efficienza di archiviazione ONTAP (compressione, deduplicazione e compattazione). Dopo la creazione, utilizzare la shell per modificare i parametri del volume utilizzando ***volume modify*** come segue:

Collocamento	Configurazione
Garanzia di volume (stile di garanzia spaziale)	Nessuno (thin provisioning) – impostato per impostazione predefinita

Collocamento	Configurazione
fractional_reserve (riserva frazionaria)	0% – impostato di default
snap_reserve (percentuale-spazio-snapshot)	0%
Autosize (modalità autosize)	crescere_ridurre
Efficienza di archiviazione	Abilitato – impostato di default
Eliminazione automatica	volume / più vecchio_primo
Politica di suddivisione in livelli del volume	Solo snapshot: impostato di default
prova_prima	Crescita automatica
Politica di snapshot	Nessuno

Utilizzare il seguente comando SSH per creare e modificare i volumi:

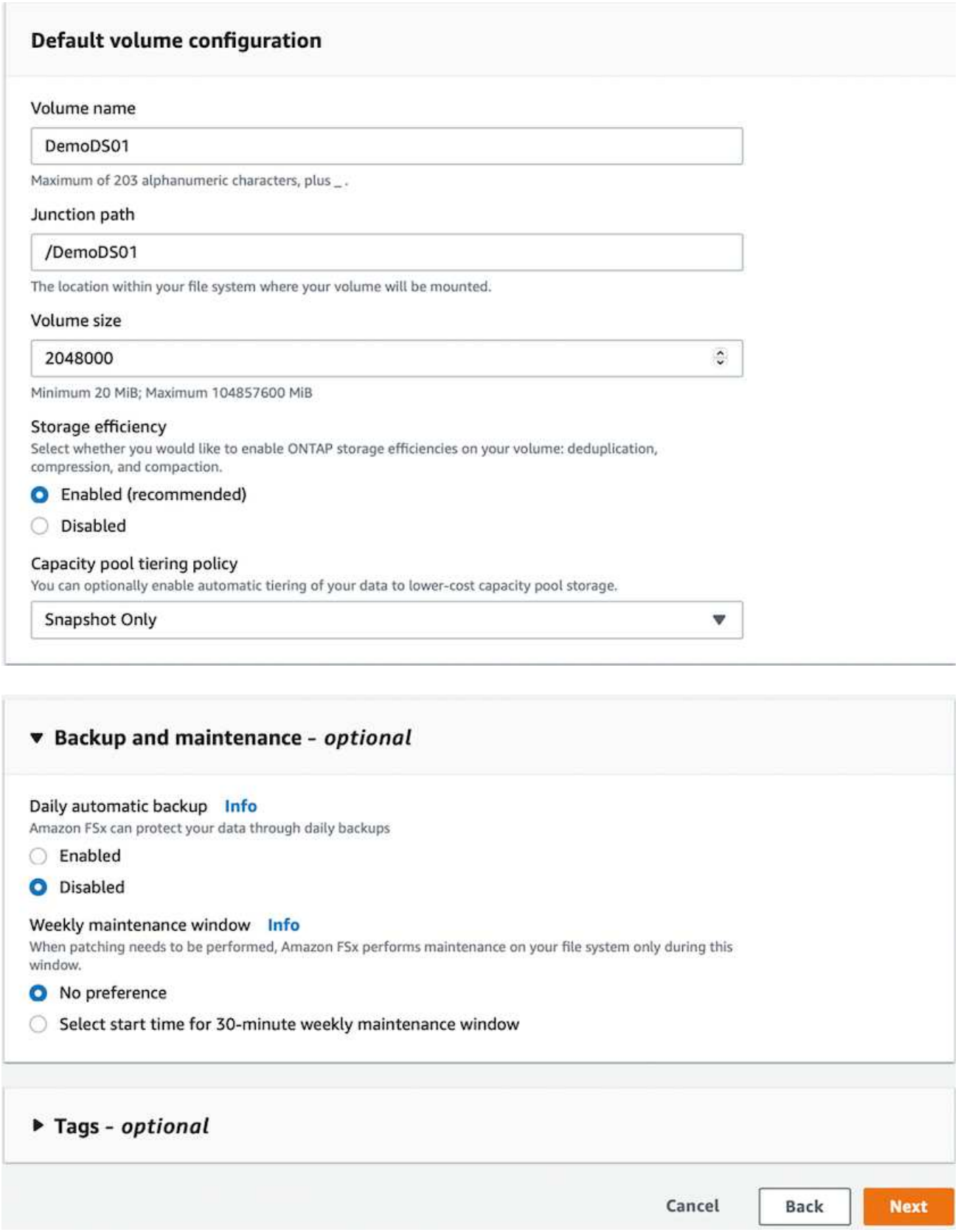
Comando per creare un nuovo volume di archivio dati dalla shell:

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

Nota: i volumi creati tramite shell impiegheranno alcuni minuti prima di essere visualizzati nella console AWS.

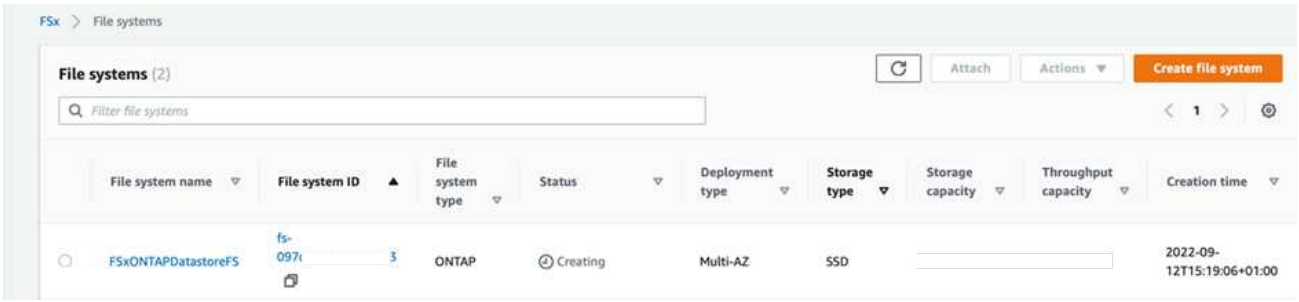
Comando per modificare i parametri del volume che non sono impostati di default:

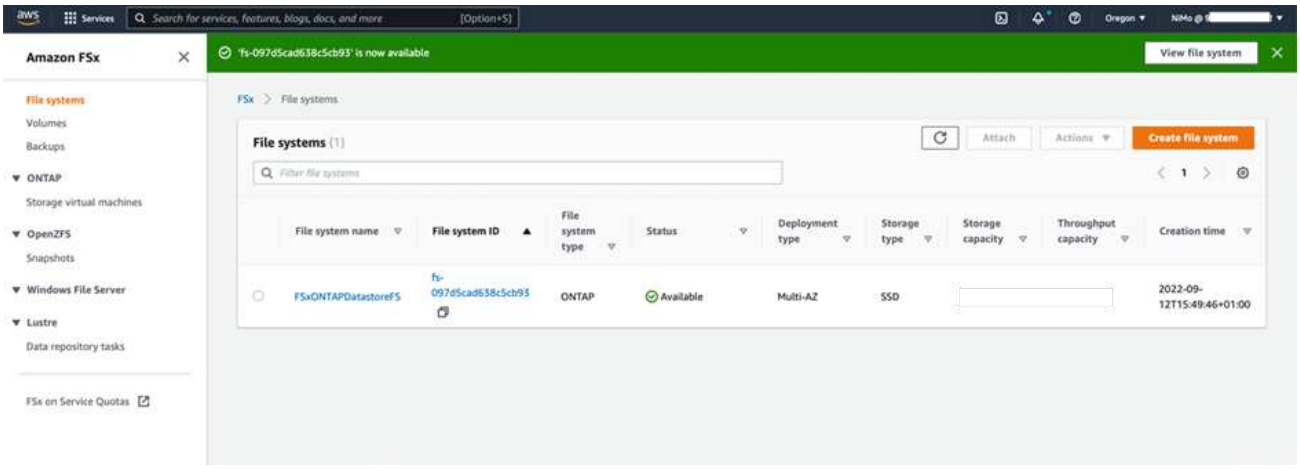
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



Durante lo scenario di migrazione iniziale, il criterio di snapshot predefinito può causare problemi di capacità del datastore completa. Per superare questo problema, modificare la policy degli snapshot in base alle proprie esigenze.

8. Esaminare la configurazione del file system mostrata nella pagina **Crea file system**.
9. Fare clic su **Crea file system**.





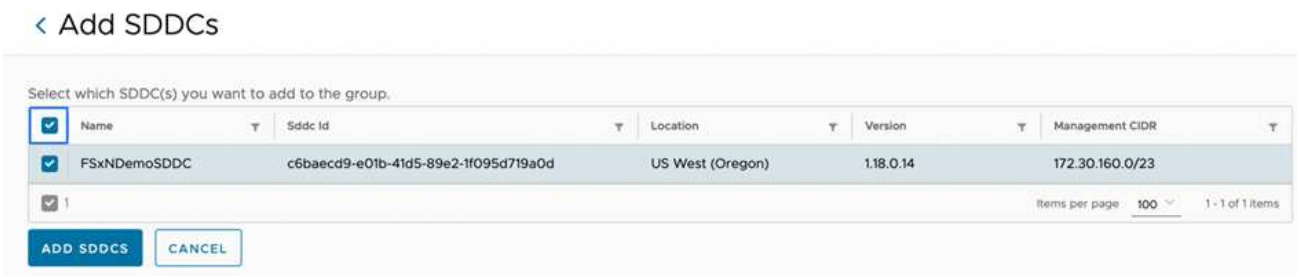
Ripetere i passaggi precedenti per creare più macchine virtuali di archiviazione o file system e volumi di datastore in base ai requisiti di capacità e prestazioni.

Per ulteriori informazioni sulle prestazioni Amazon FSx ONTAP , vedere "Prestazioni Amazon FSx ONTAP" .

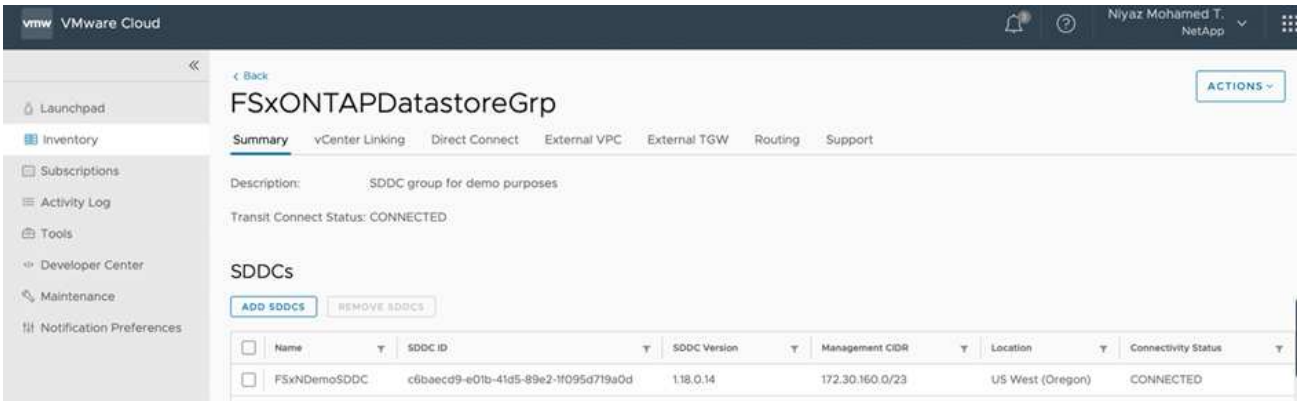
▼ Passaggio 2: creare un gruppo SDDC

Dopo aver creato i file system e le SVM, utilizzare VMware Console per creare un gruppo SDDC e configurare VMware Transit Connect. Per farlo, completa i seguenti passaggi e ricorda che devi passare dalla VMware Cloud Console alla AWS Console.

1. Accedi alla console VMC all'indirizzo `https://vmc.vmware.com` .
2. Nella pagina **Inventario**, fare clic su **Gruppi SDDC**.
3. Nella scheda **Gruppi SDDC**, fare clic su **AZIONI** e selezionare **Crea gruppo SDDC**. A scopo dimostrativo, il gruppo SDDC è chiamato `FSxONTAPDatastoreGrp` .
4. Nella griglia Appartenenza, seleziona gli SDDC da includere come membri del gruppo.

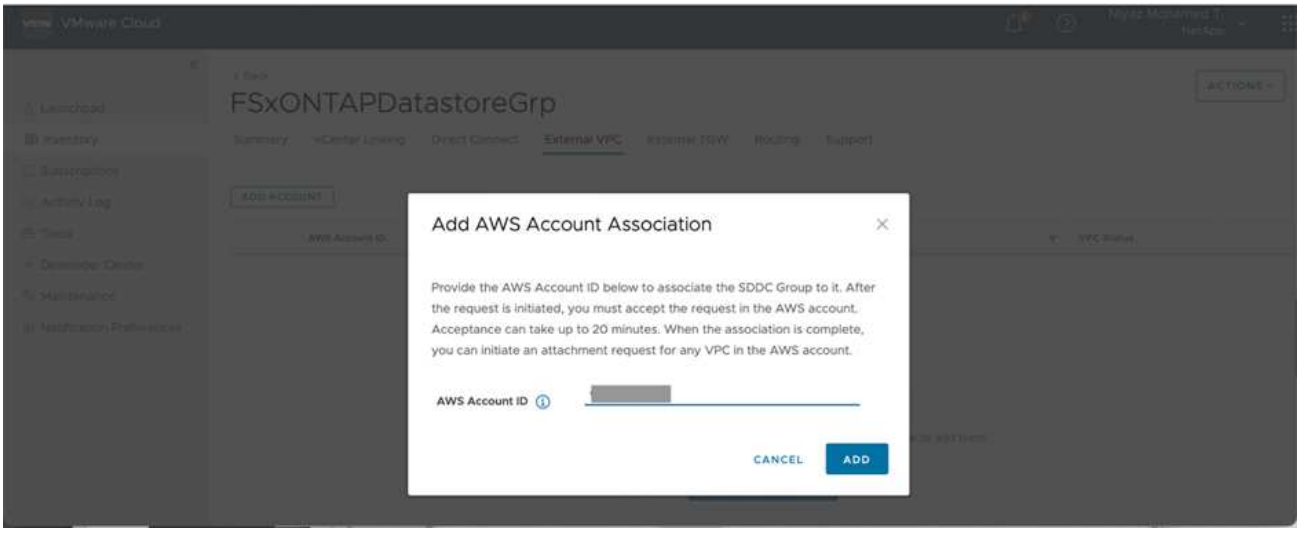


5. Verificare che sia selezionata l'opzione "La configurazione di VMware Transit Connect per il gruppo comporterà addebiti per allegato e trasferimenti di dati", quindi selezionare **Crea gruppo**. Il completamento del processo potrebbe richiedere alcuni minuti.

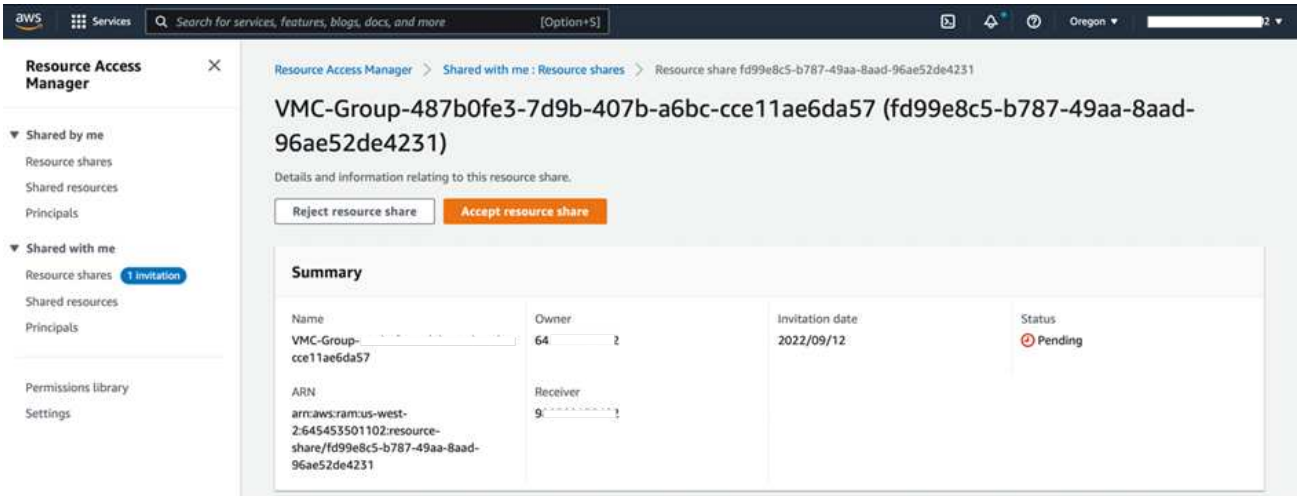


▼ **Passaggio 3: configurare VMware Transit Connect**

1. Collegare la VPC designata appena creata al gruppo SDDC. Selezionare la scheda **VPC esterna** e seguire le istruzioni "istruzioni per collegare una VPC esterna al gruppo" . Questo processo può richiedere dai 10 ai 15 minuti.

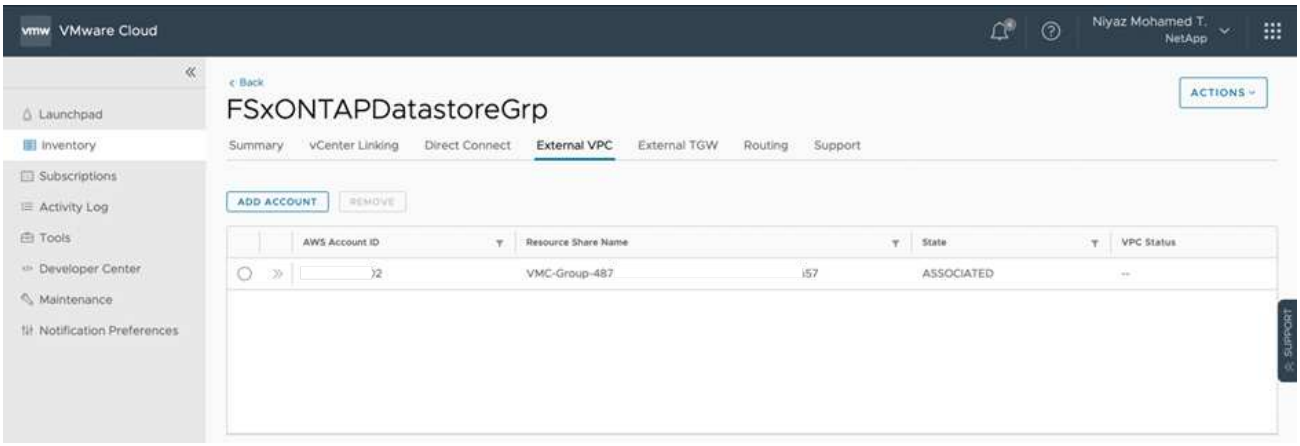


2. Fare clic su **Aggiungi account**.
   a. Fornire l'account AWS utilizzato per il provisioning del file system FSx ONTAP .
   b. Fare clic su **Aggiungi**.
3. Torna alla console AWS, accedi allo stesso account AWS e vai alla pagina del servizio **Resource Access Manager**. C'è un pulsante per accettare la condivisione delle risorse.



Come parte del processo VPC esterno, ti verrà 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.

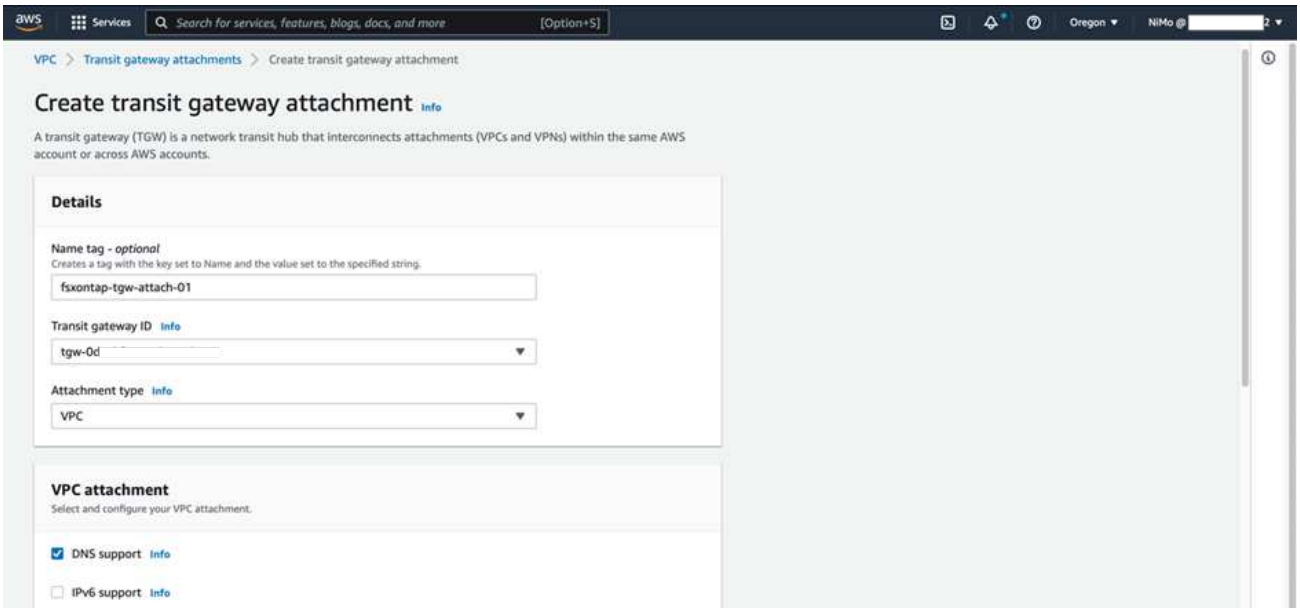
4. Fare clic su **Accetta condivisione risorse**.



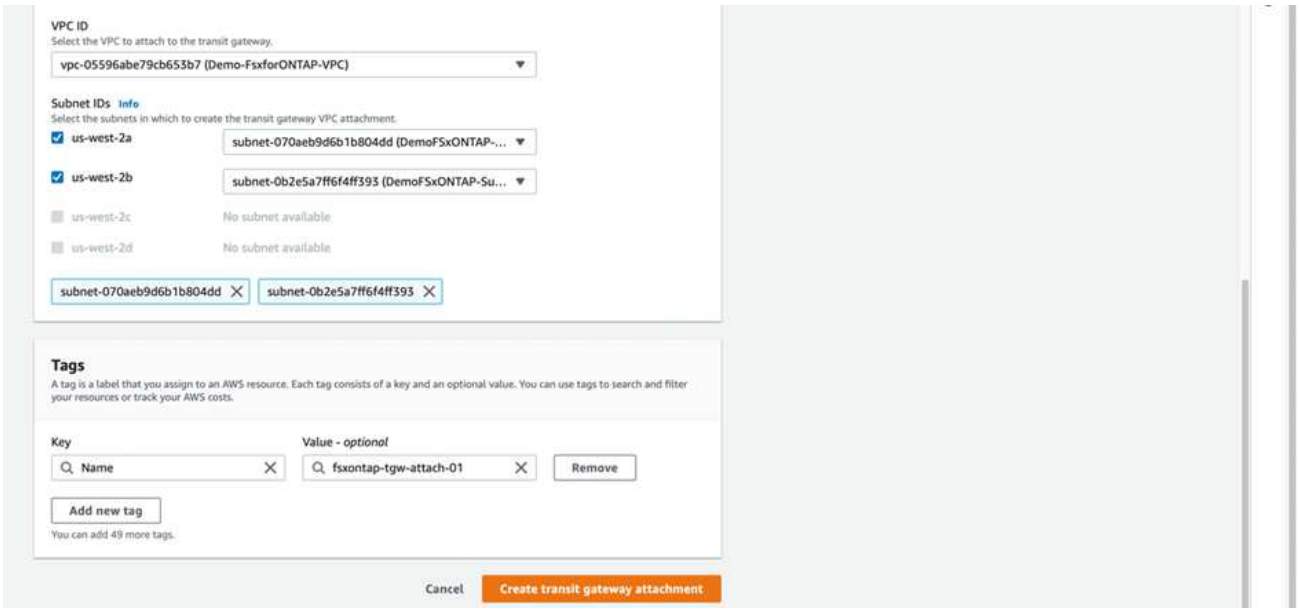
5. Tornando alla console VMC, ora puoi vedere che la VPC esterna è in uno stato associato. Potrebbero volerci diversi minuti prima che venga visualizzato.

▼ **Passaggio 4: creare un allegato al gateway di transito**

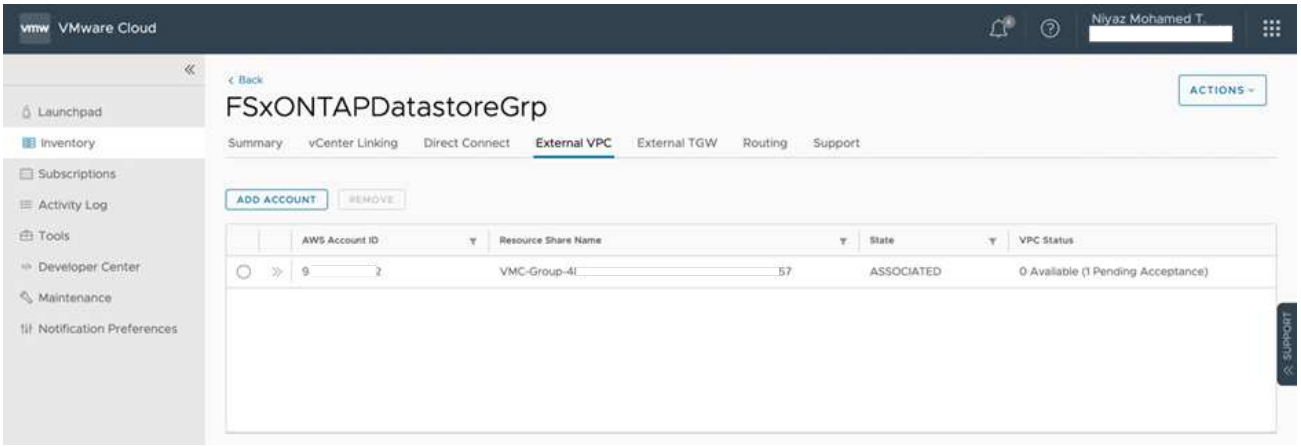
1. Nella console AWS, vai alla pagina del servizio VPC e accedi alla VPC utilizzata per il provisioning del file system FSx. Qui puoi creare un allegato al gateway di transito cliccando su **Allegato al gateway di transito** nel riquadro di navigazione a destra.
2. In **Allegato VPC**, assicurati che l'opzione Supporto DNS sia selezionata e seleziona la VPC in cui è stato distribuito FSx ONTAP .

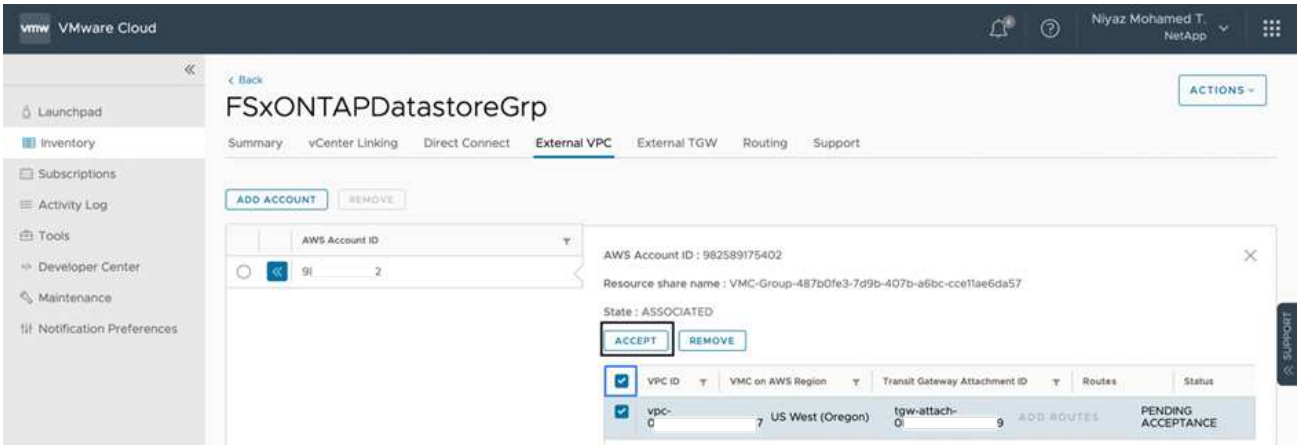


3. Fare clic su **Crea allegato al gateway di transito**.



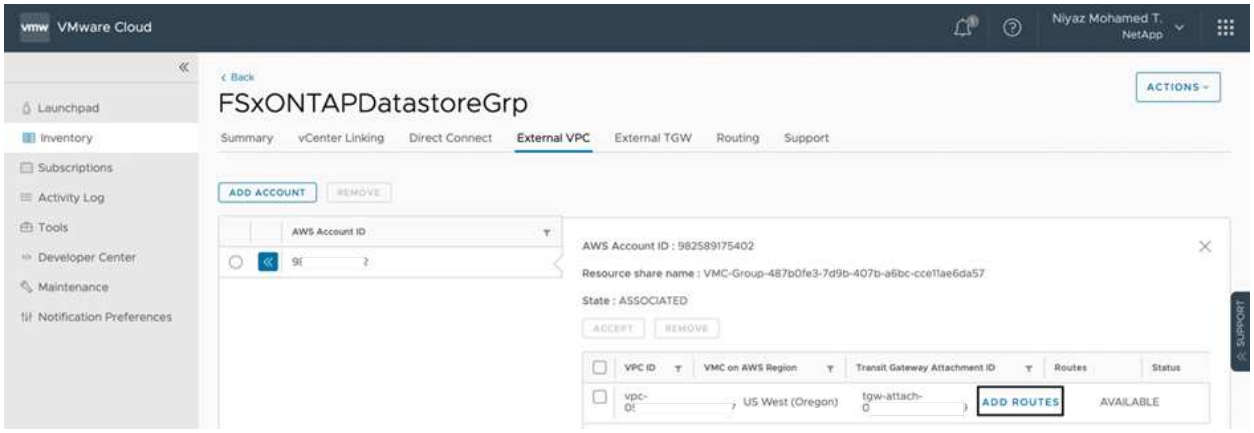
4. Tornando alla VMware Cloud Console, tornare alla scheda SDDC Group > External VPC. Selezionare l'ID account AWS utilizzato per FSx, fare clic sulla VPC e quindi su **Accetta**.

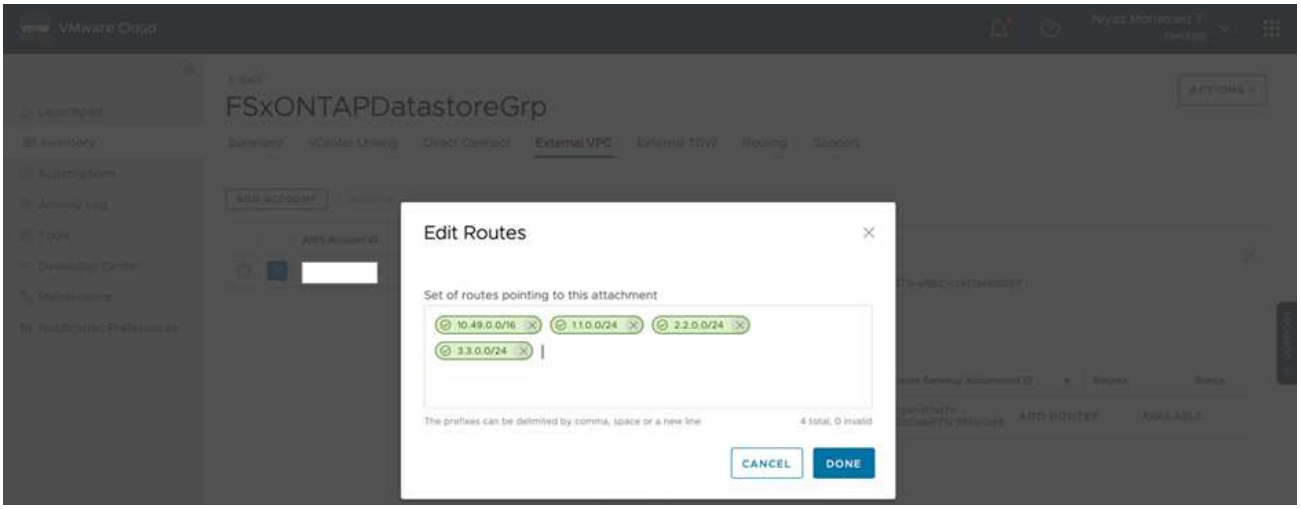




Potrebbero volerci alcuni minuti prima che questa opzione venga visualizzata.

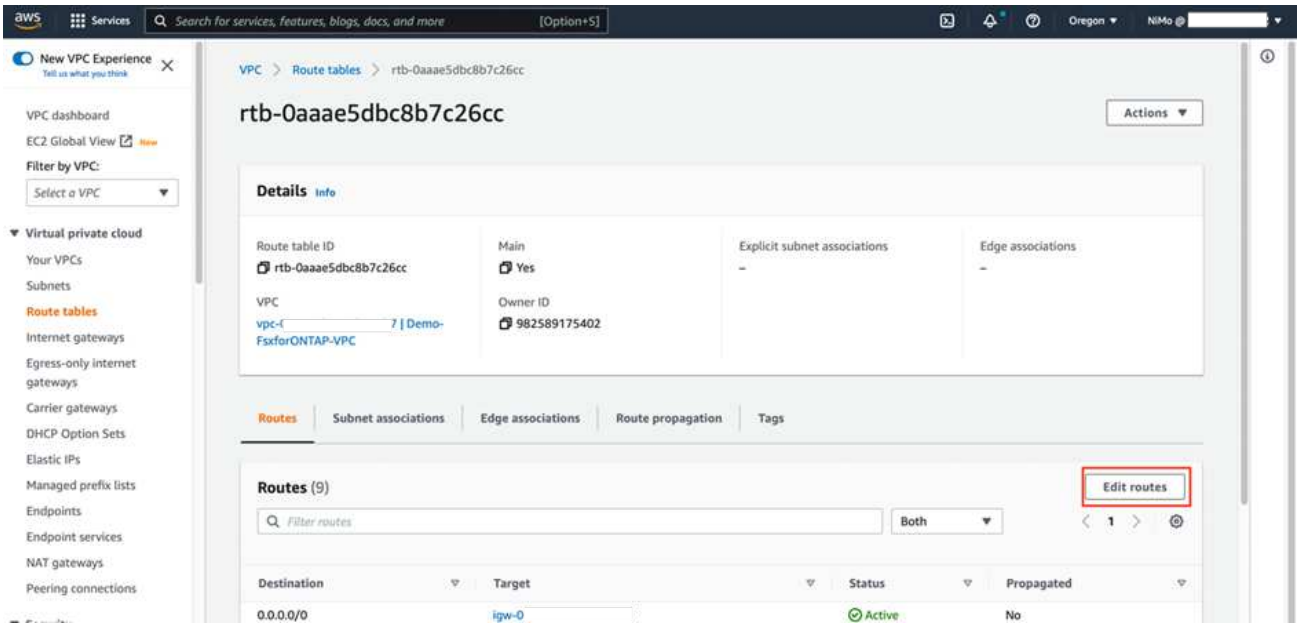
5. Quindi nella scheda **VPC esterna** nella colonna **Percorsi**, fare clic sull'opzione **Aggiungi percorsi** e aggiungere i percorsi richiesti:
   - Un percorso per l'intervallo di IP mobili per gli IP mobili Amazon FSx ONTAP .
   - Un percorso per lo spazio di indirizzamento VPC esterno appena creato.



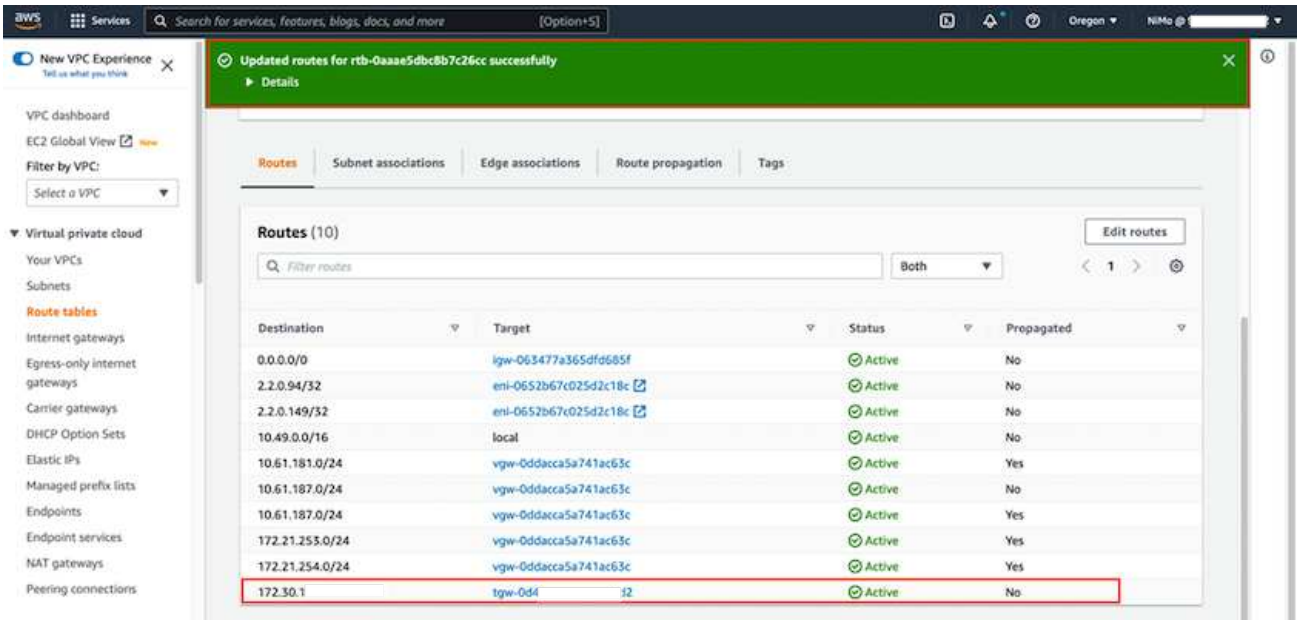


▼ **Passaggio 5: configurare il routing (AWS VPC e SDDC) e i gruppi di sicurezza**

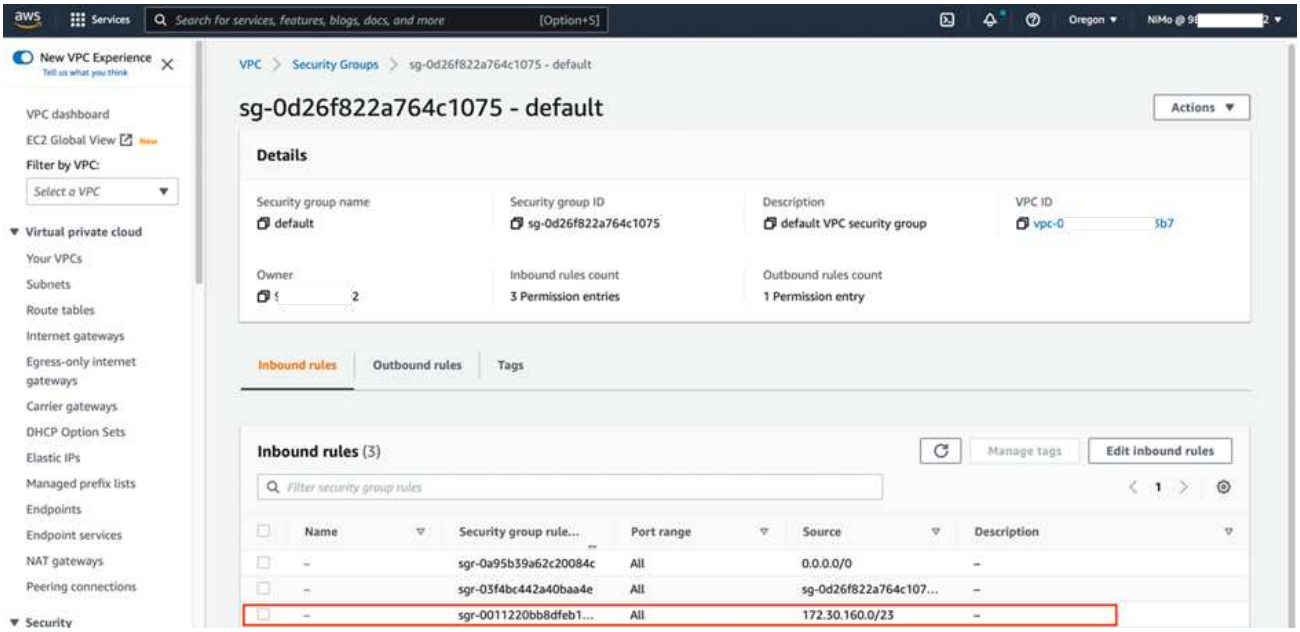
1. Nella console AWS, crea il percorso di ritorno all'SDDC individuando la VPC nella pagina del servizio VPC e selezionando la tabella di routing **principale** per la VPC.
2. Passare alla tabella dei percorsi nel pannello inferiore e fare clic su **Modifica percorsi**.



3. Nel pannello **Modifica percorsi**, fare clic su **Aggiungi percorso** e immettere il CIDR per l'infrastruttura SDDC selezionando **Transit Gateway** e l'ID TGW associato. Fare clic su **Salva modifiche**.



4. Il passaggio successivo consiste nel verificare che il gruppo di sicurezza nella VPC associata sia aggiornato con le regole in ingresso corrette per il CIDR del gruppo SDDC.
5. Aggiornare la regola in entrata con il blocco CIDR dell'infrastruttura SDDC.



Verificare che la tabella di routing VPC (dove risiede FSx ONTAP) sia aggiornata per evitare problemi di connettività.

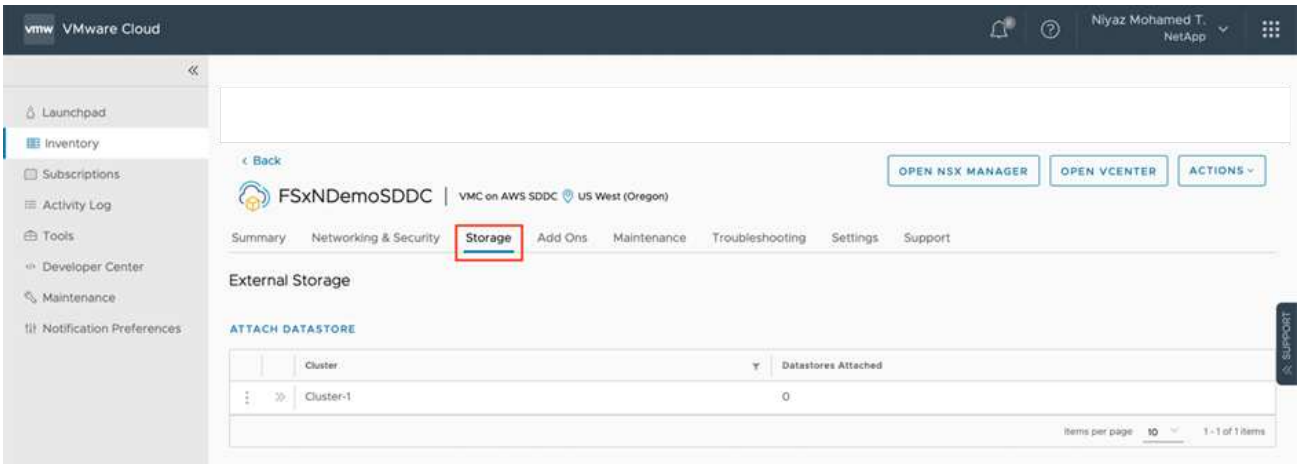
Aggiornare il gruppo di sicurezza per accettare il traffico NFS.

Questo è il passaggio finale nella preparazione della connettività all'SDDC appropriato. Dopo aver configurato il file system, aggiunto i percorsi e aggiornato i gruppi di sicurezza, è il momento di montare i datastore.

▼ Passaggio 6: collegare il volume NFS come datastore al cluster SDDC

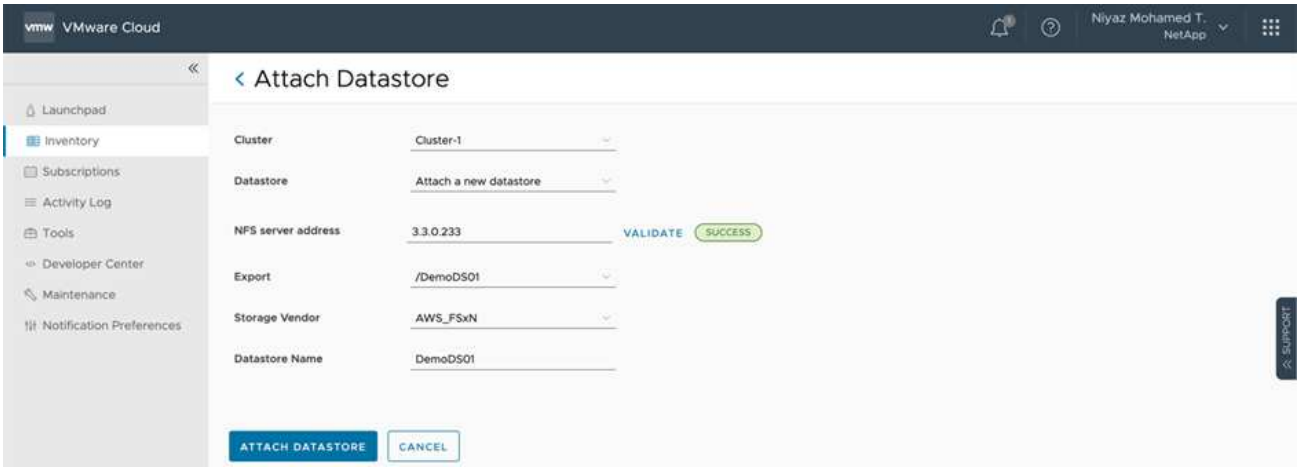
Dopo aver eseguito il provisioning del file system e aver predisposto la connettività, accedere a VMware Cloud Console per montare il datastore NFS.

1. Nella console VMC, aprire la scheda **Archiviazione** dell'SDDC.

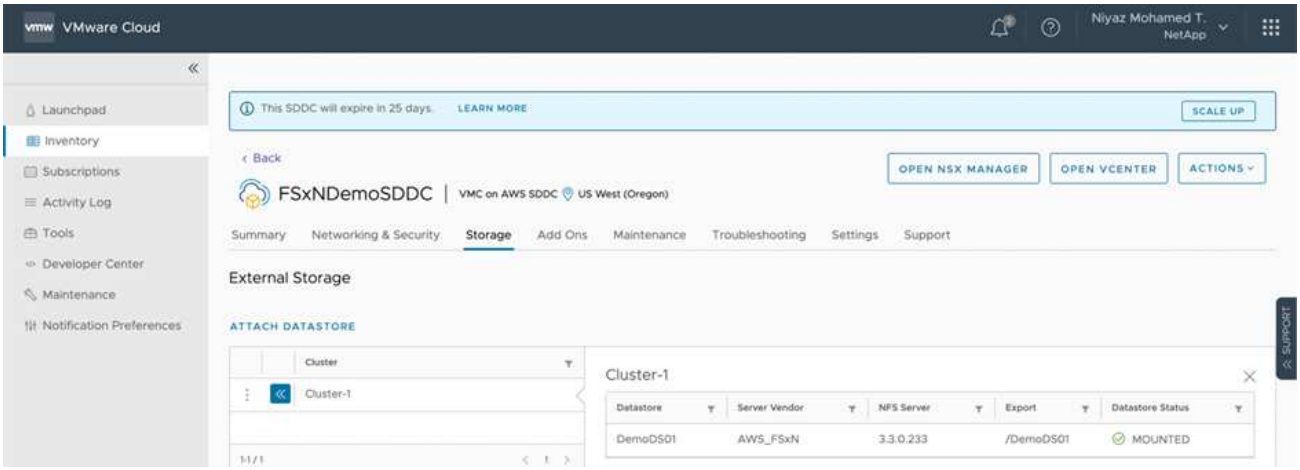


2. Fare clic su **ALLEGA DATASTORE** e compilare i valori richiesti.

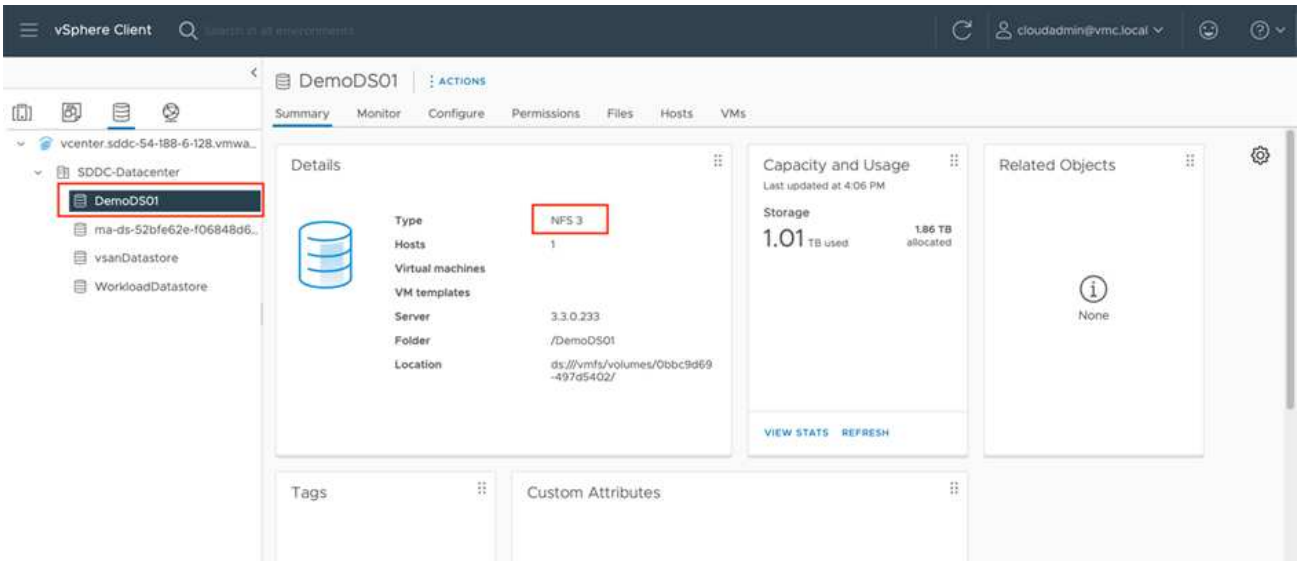
> L'indirizzo del server NFS è l'indirizzo IP NFS che si trova nella scheda FSx > Macchine virtuali di archiviazione > Endpoint nella console AWS.



3. Fare clic su **ALLEGA DATASTORE** per allegare il datastore al cluster.



4. Convalidare il datastore NFS accedendo a vCenter come mostrato di seguito:



Opzioni di storage connesso agli ospiti NetApp per AWS

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

FSx ONTAP

Amazon FSx ONTAP è un servizio completamente gestito che fornisce un archivio file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità, basato sul famoso file system ONTAP di NetApp. FSx ONTAP combina le caratteristiche, le prestazioni, le capacità e le operazioni API note dei file system NetApp con l'agilità, la scalabilità e la semplicità di un servizio AWS completamente gestito.

FSx ONTAP offre uno storage di file condiviso ricco di funzionalità, veloce e flessibile, ampiamente accessibile da istanze di elaborazione Linux, Windows e macOS in esecuzione su AWS o in locale. FSx ONTAP offre storage su unità a stato solido (SSD) ad alte prestazioni con latenze inferiori al millisecondo. Con FSx ONTAP puoi raggiungere livelli di prestazioni SSD per il tuo carico di lavoro, pagando per l'archiviazione SSD solo una piccola parte dei tuoi dati.

Gestire i dati con FSx ONTAP è più semplice perché puoi creare snapshot, clonare e replicare i tuoi file con un semplice clic. Inoltre, FSx ONTAP suddivide automaticamente i dati in livelli di storage più economici ed

elastici, riducendo la necessità di provisioning o gestione della capacità.

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

FSx ONTAP come storage connesso agli ospiti

▼ Configurare Amazon FSx ONTAP con VMware Cloud su AWS

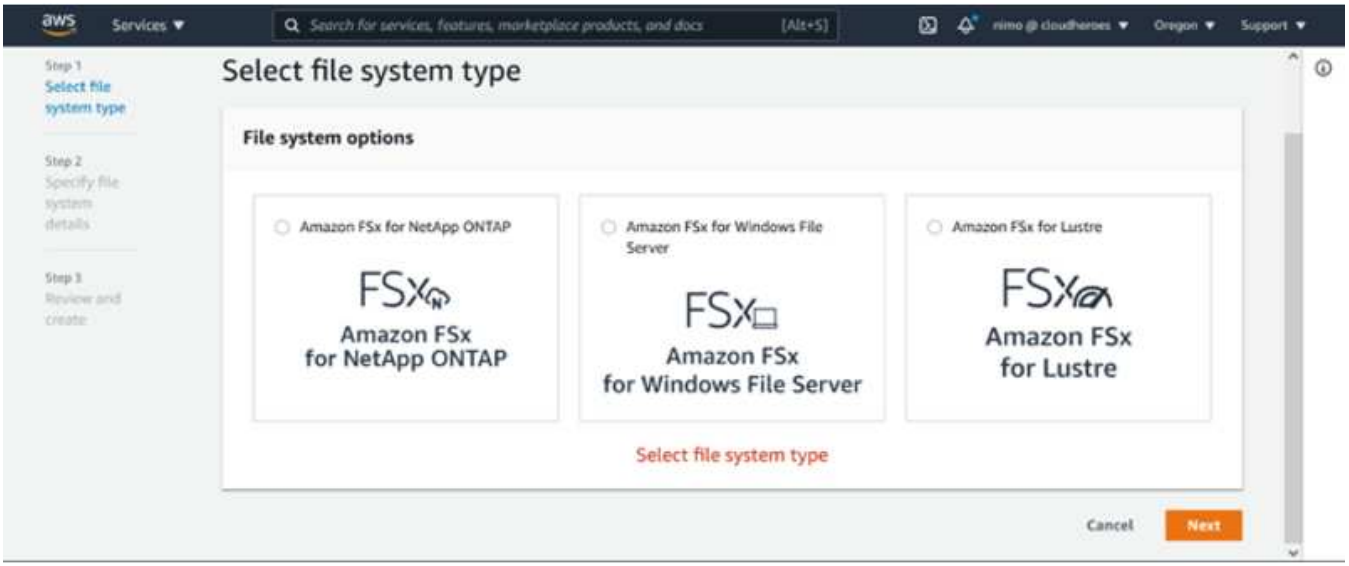
Le condivisioni di file e le LUN Amazon FSx ONTAP possono essere montate da VM create nell'ambiente VMware SDDC su VMware Cloud presso AWS. I volumi possono anche essere montati sul client Linux e mappati sul client Windows utilizzando il protocollo NFS o SMB, ed è possibile accedere ai LUN sui client Linux o Windows come dispositivi a blocchi quando montati su iSCSI. È possibile configurare rapidamente Amazon FSx per il file system NetApp ONTAP seguendo i passaggi seguenti.

> Amazon FSx ONTAP e VMware Cloud on AWS devono trovarsi nella stessa zona di disponibilità per ottenere prestazioni migliori ed evitare costi di trasferimento dati tra zone di disponibilità.

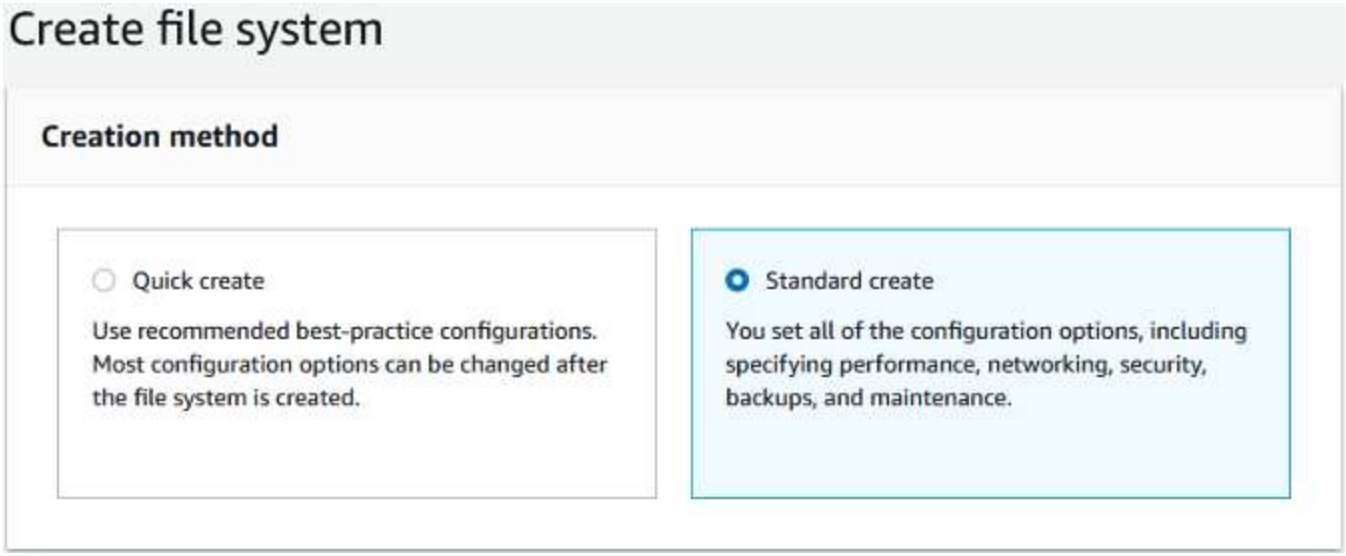
▼ Crea e monta volumi Amazon FSx ONTAP

Per creare e montare il file system Amazon FSx ONTAP , completare i seguenti passaggi:

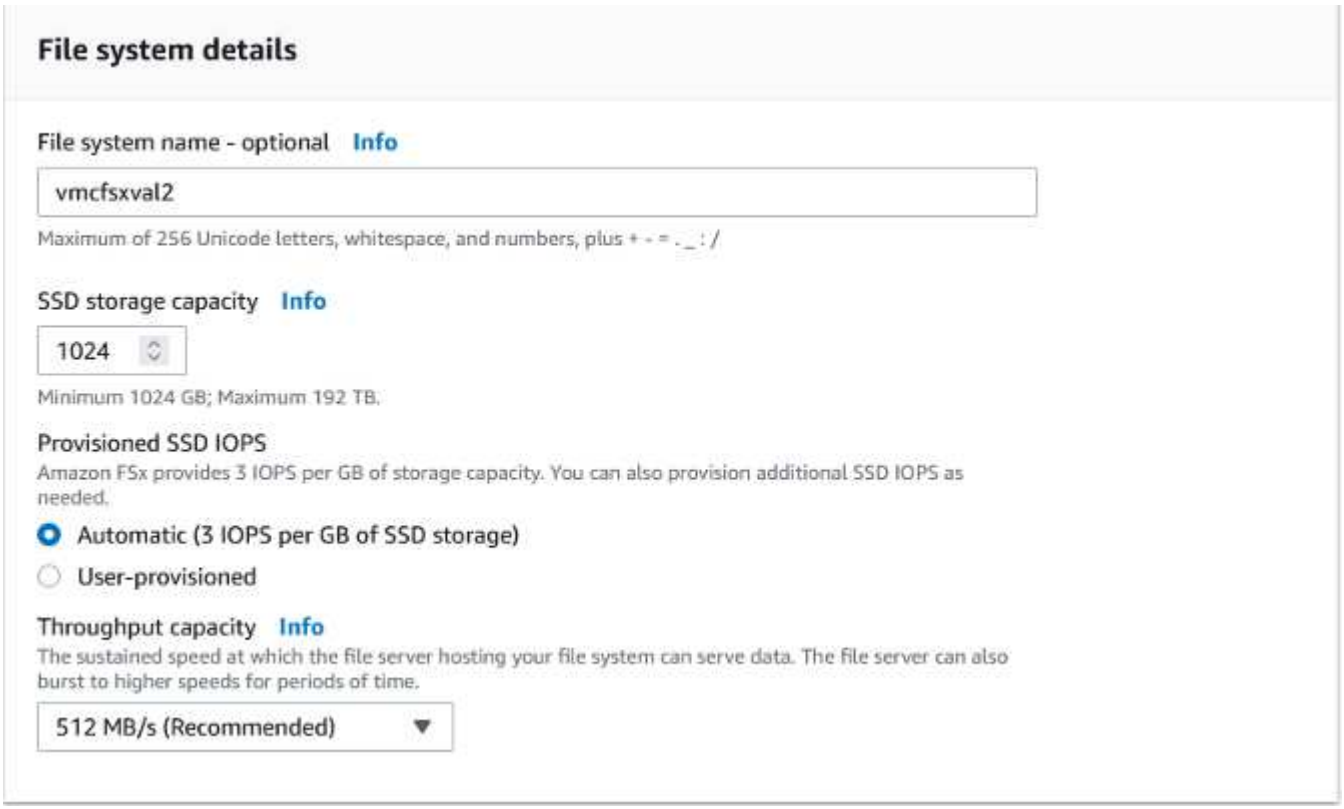
1. Apri il"Console Amazon FSx" e seleziona Crea file system per avviare la procedura guidata di creazione del file system.
2. Nella pagina Seleziona tipo di file system, seleziona Amazon FSx ONTAP, quindi seleziona Avanti. Viene visualizzata la pagina Crea file system.



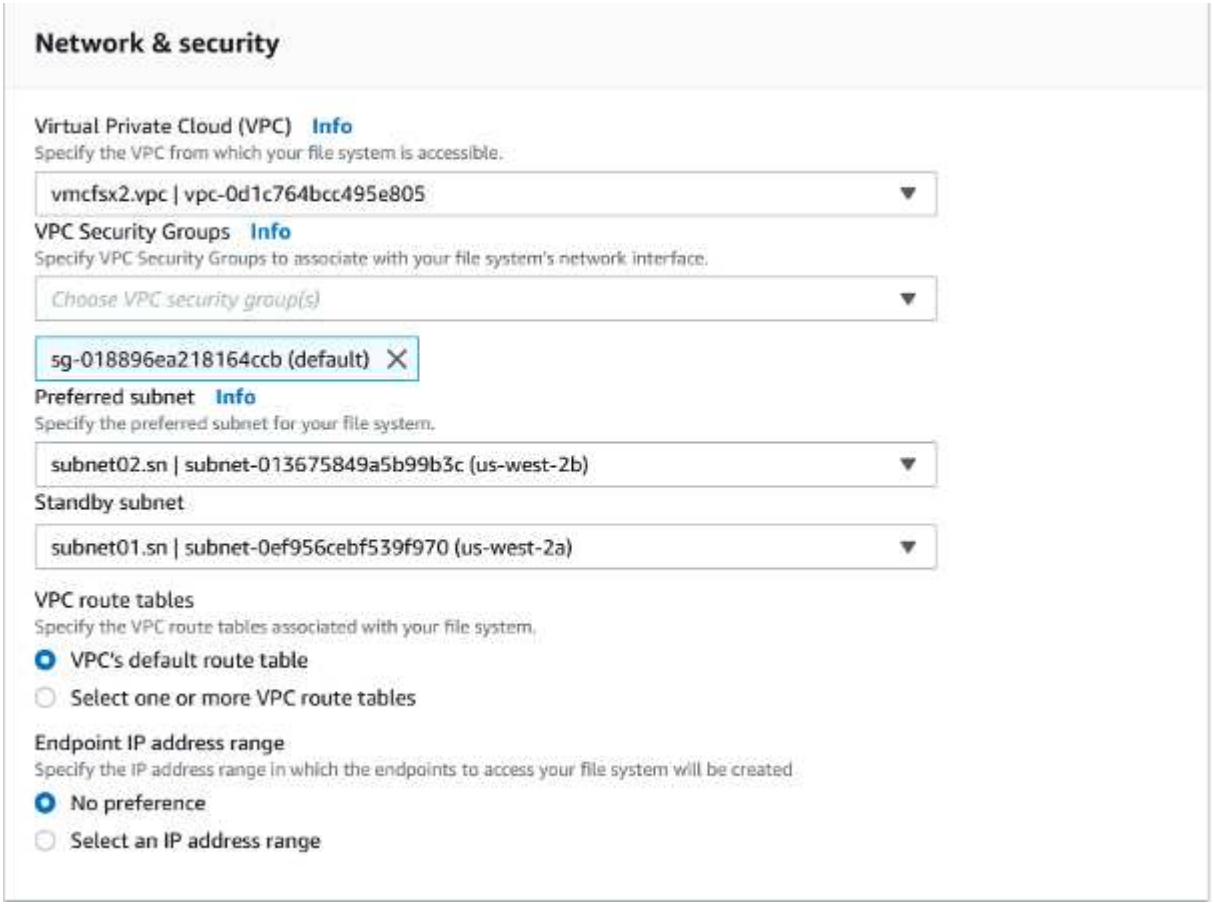
1. Nella sezione Networking, per Virtual Private Cloud (VPC), seleziona la VPC appropriata e le subnet preferite insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.



1. Per il metodo di creazione, seleziona Creazione standard. È anche possibile scegliere Creazione rapida, ma questo documento utilizza l'opzione di creazione Standard.

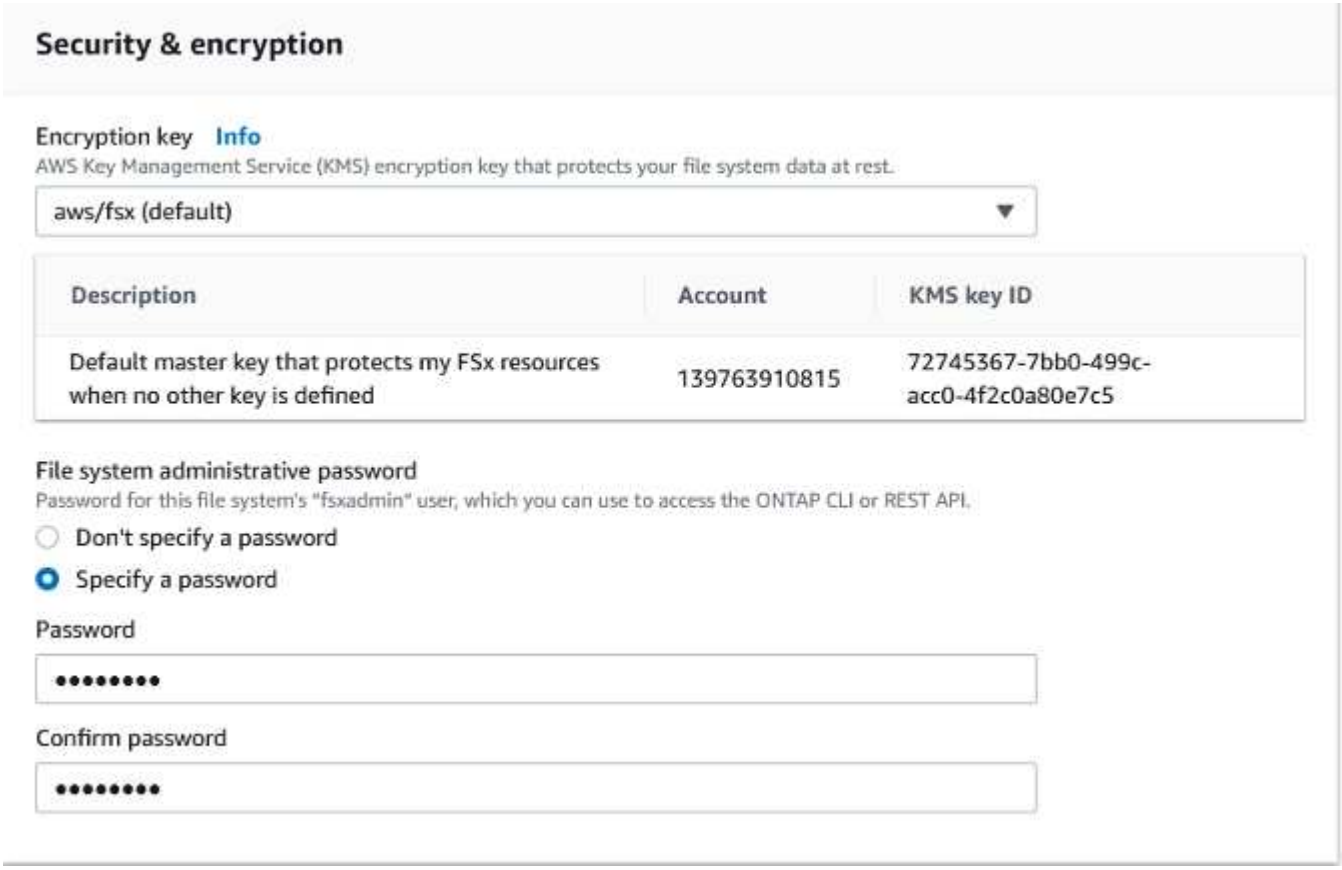


1. Nella sezione Networking, per Virtual Private Cloud (VPC), seleziona la VPC appropriata e le subnet preferite insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.

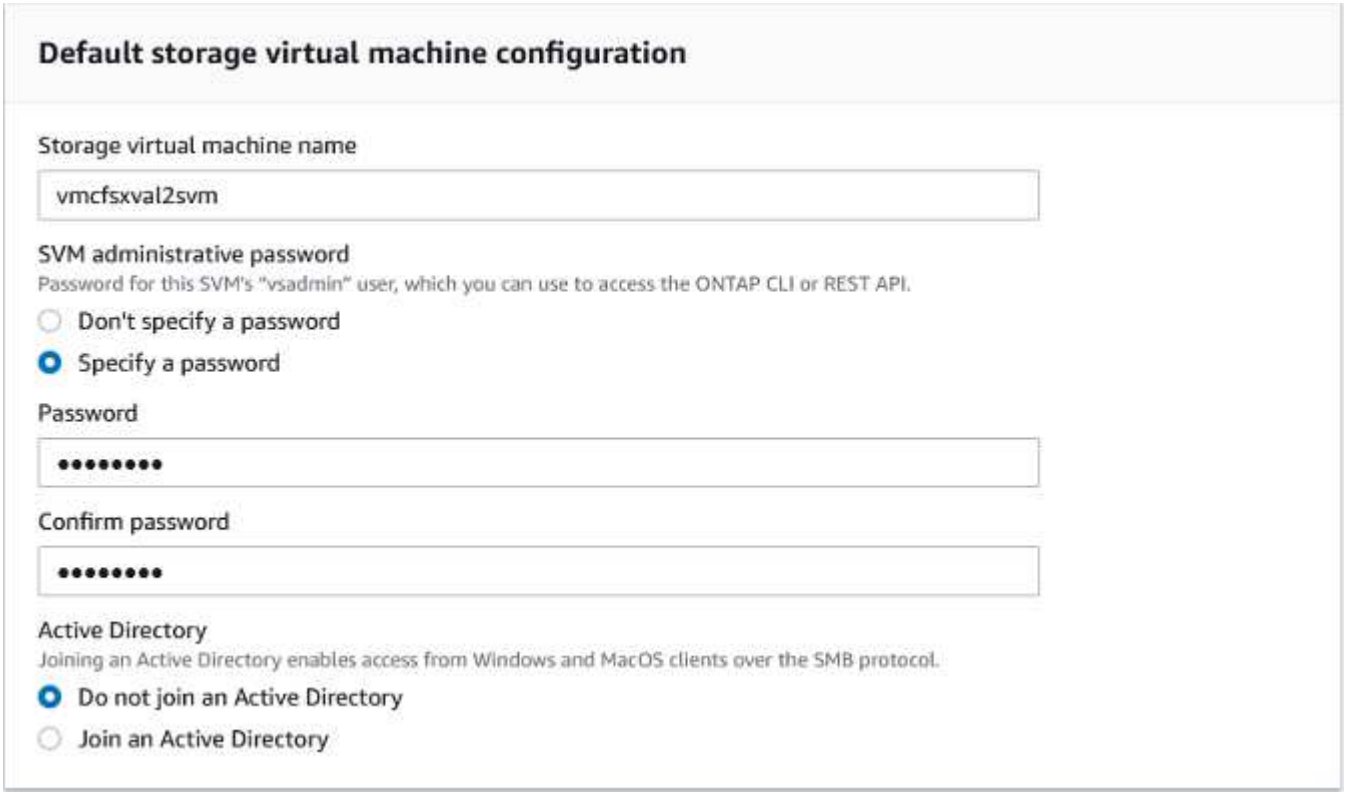


Nella sezione Networking, per Virtual Private Cloud (VPC), seleziona la VPC appropriata e le subnet preferite insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.

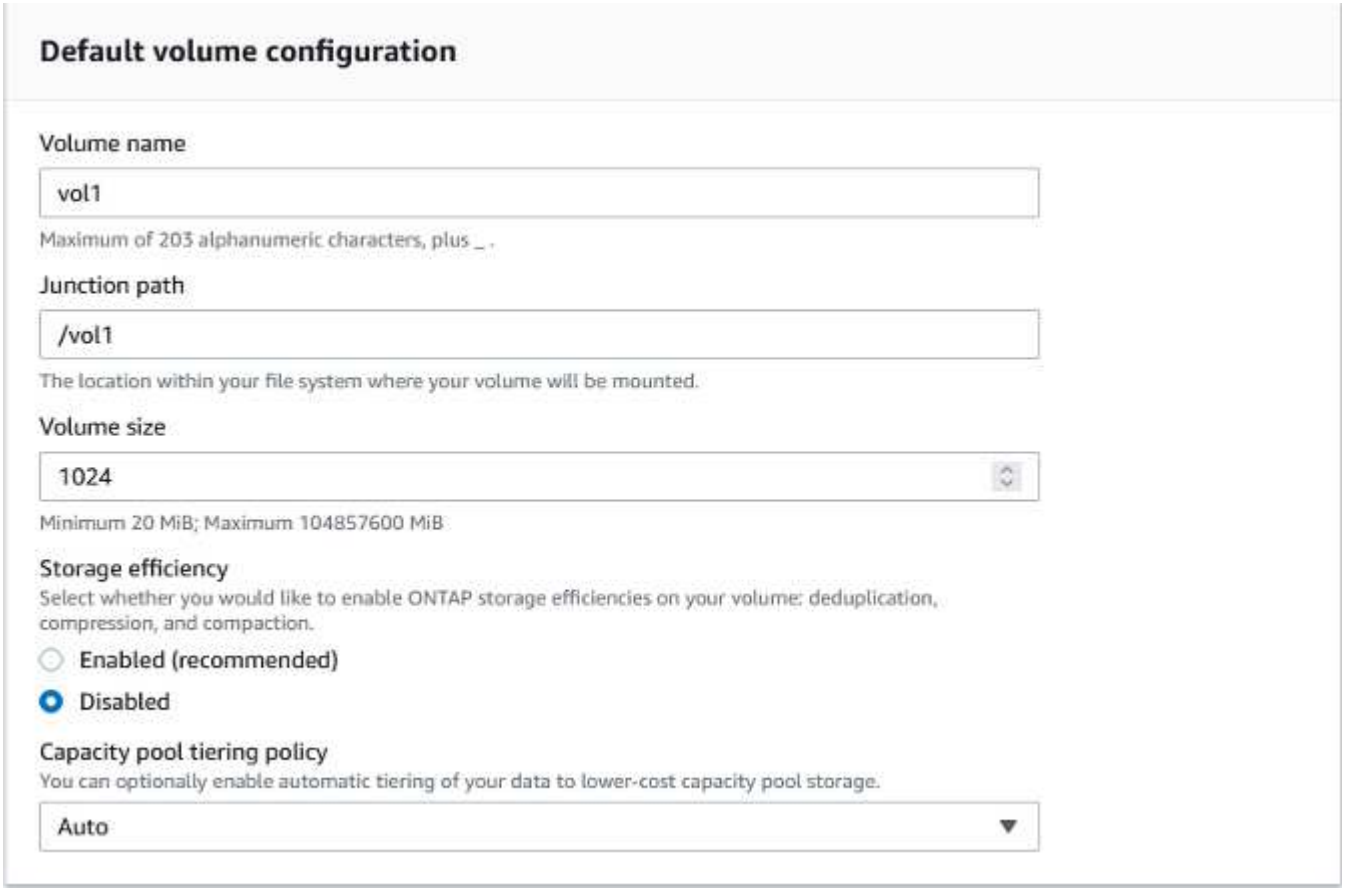
1. Nella sezione Sicurezza e crittografia, per Chiave di crittografia, seleziona la chiave di crittografia AWS Key Management Service (AWS KMS) che protegge i dati inattivi del file system. Per la password amministrativa del file system, immettere una password sicura per l'utente fsxadmin.



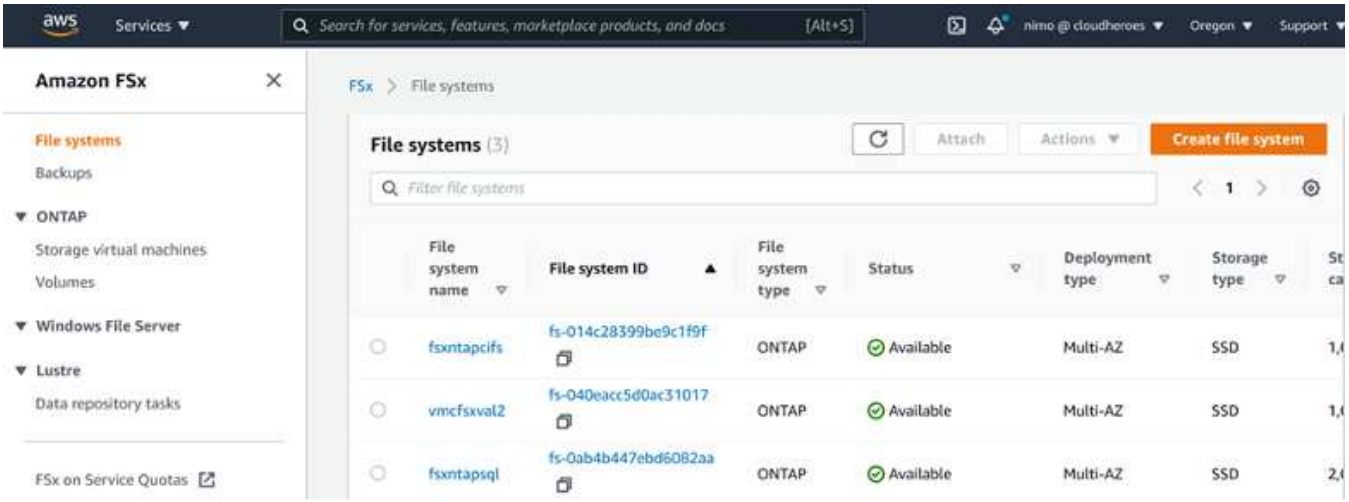
1. Nella macchina virtuale specificare la password da utilizzare con vsadmin per amministrare ONTAP tramite API REST o CLI. Se non viene specificata alcuna password, è possibile utilizzare un utente fsxadmin per amministrare l'SVM. Nella sezione Active Directory, assicurati di unire Active Directory all'SVM per il provisioning delle condivisioni SMB. Nella sezione Configurazione macchina virtuale di archiviazione predefinita, specificare un nome per l'archiviazione in questa convalida; le condivisioni SMB vengono fornite utilizzando un dominio Active Directory autogestito.

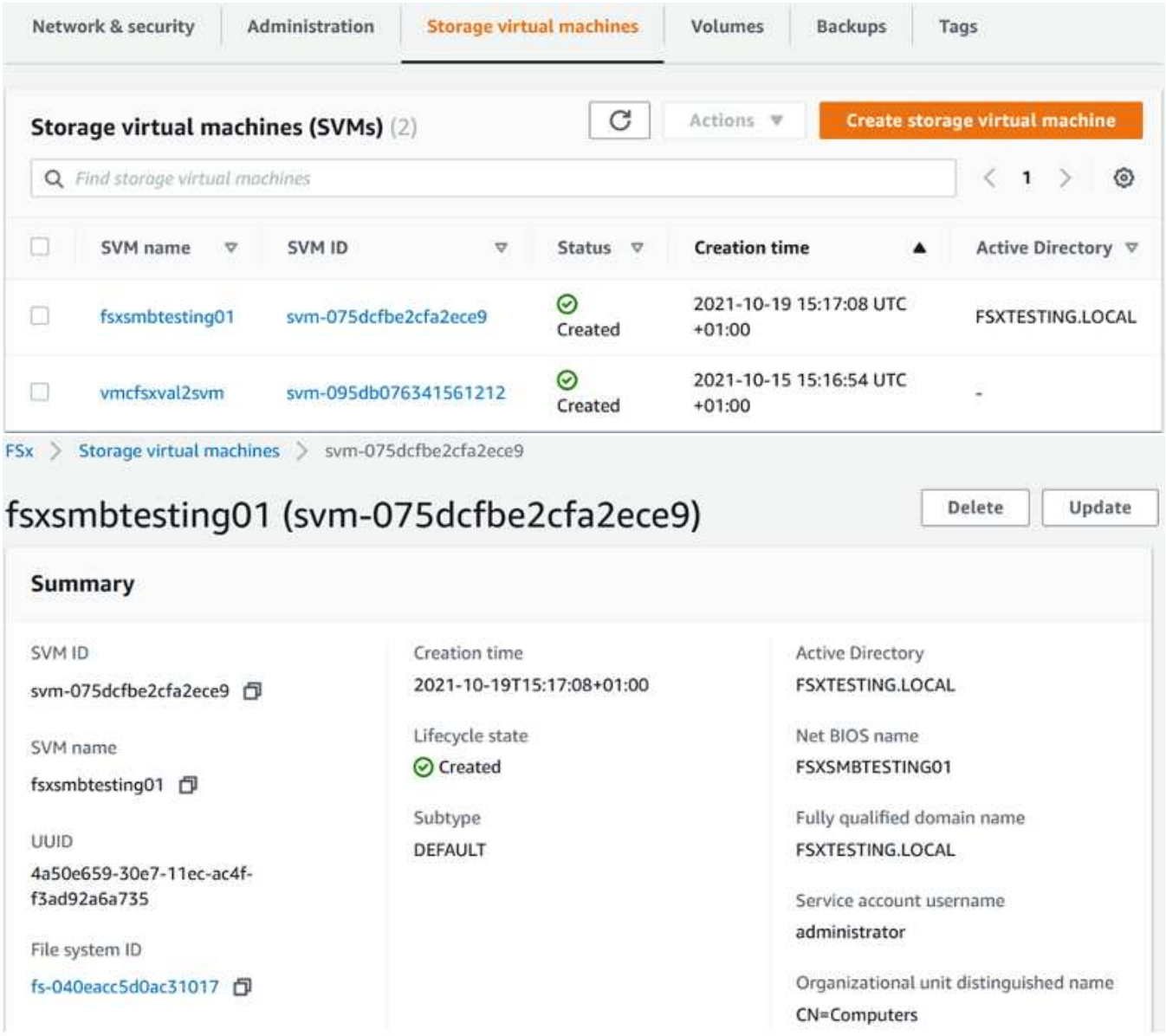


1. Nella sezione Configurazione volume predefinita, specificare il nome e la dimensione del volume. Questo è un volume NFS. Per Efficienza di archiviazione, selezionare Abilitato per attivare le funzionalità di efficienza di archiviazione ONTAP (compressione, deduplicazione e compattazione) oppure Disabilitato per disattivarle.



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





Per informazioni più dettagliate, vedere"Introduzione ad Amazon FSx ONTAP" .

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

1. Apri il"Console Amazon FSx" .
2. Nel riquadro di navigazione a sinistra, seleziona File system, quindi seleziona il file system ONTAP per cui desideri creare un volume.
3. Selezionare la scheda Volumi.
4. Selezionare la scheda Crea volume.
5. Viene visualizzata la finestra di dialogo Crea volume.

A scopo dimostrativo, in questa sezione viene creato un volume NFS che può essere facilmente montato su VM 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 VM Linux all'interno di VMC su AWS SDDC, completare i seguenti passaggi:

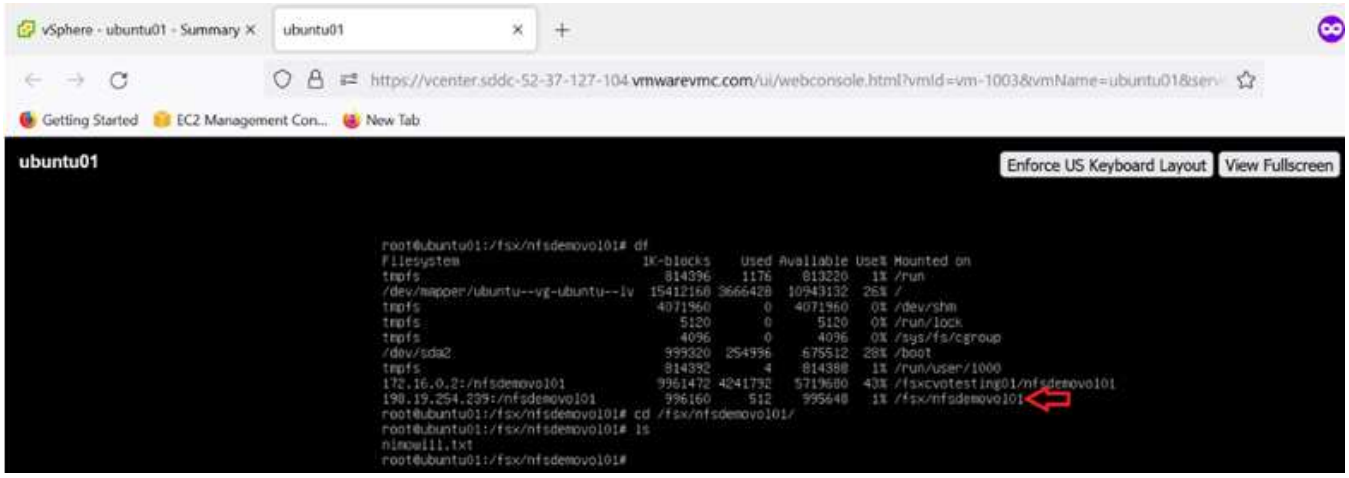
1. Connettersi all'istanza Linux designata.
2. Aprire un terminale sull'istanza utilizzando Secure Shell (SSH) ed effettuare l'accesso con le credenziali appropriate.
3. Creare una directory per il punto di montaggio del volume con il seguente comando:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Montare il volume Amazon FSx ONTAP NFS 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 montaggio.



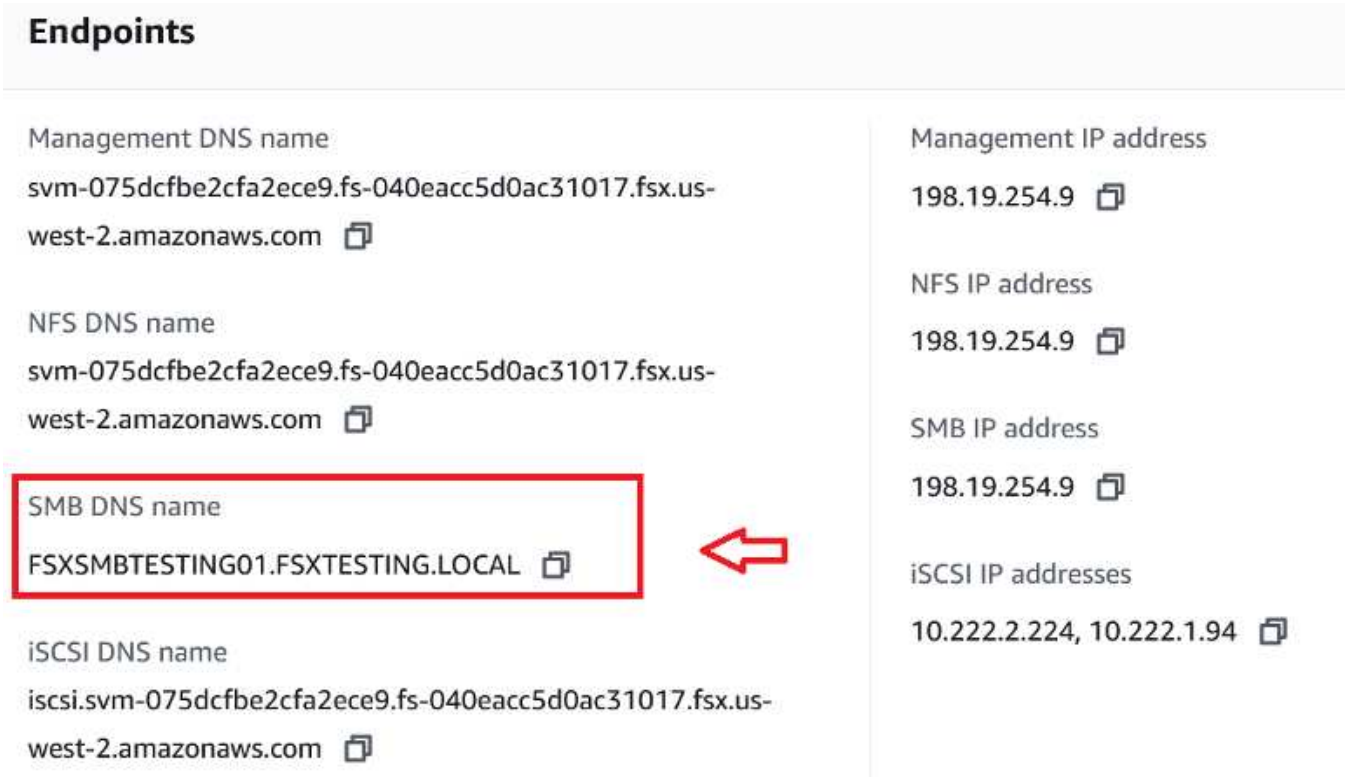
Montare il volume FSx ONTAP sul client Linux

▼ **Collegare volumi FSx ONTAP ai client Microsoft Windows**

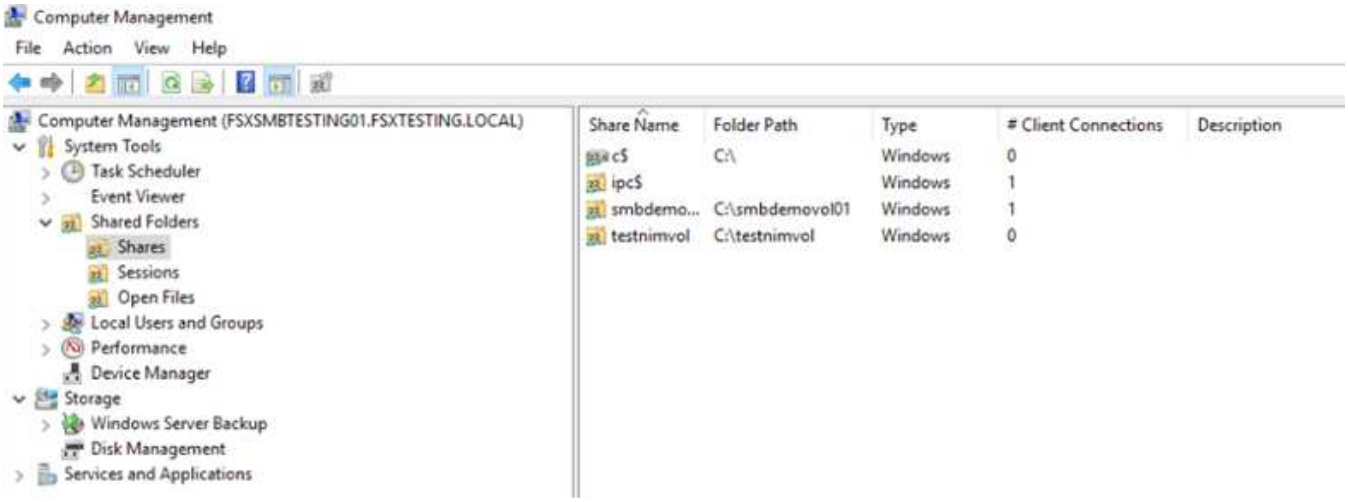
Per gestire e mappare le condivisioni di file su un file system Amazon FSx , è necessario utilizzare l'interfaccia utente grafica delle cartelle condivise.

1. Aprire il menu Start ed eseguire fsmgmt.msc utilizzando Esegui come amministratore. In questo modo si apre lo strumento GUI 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 per la macchina virtuale di archiviazione (SVM). Ad esempio, in questo esempio viene utilizzato FSXSMBTESTING01.FSXTESTING.LOCAL.

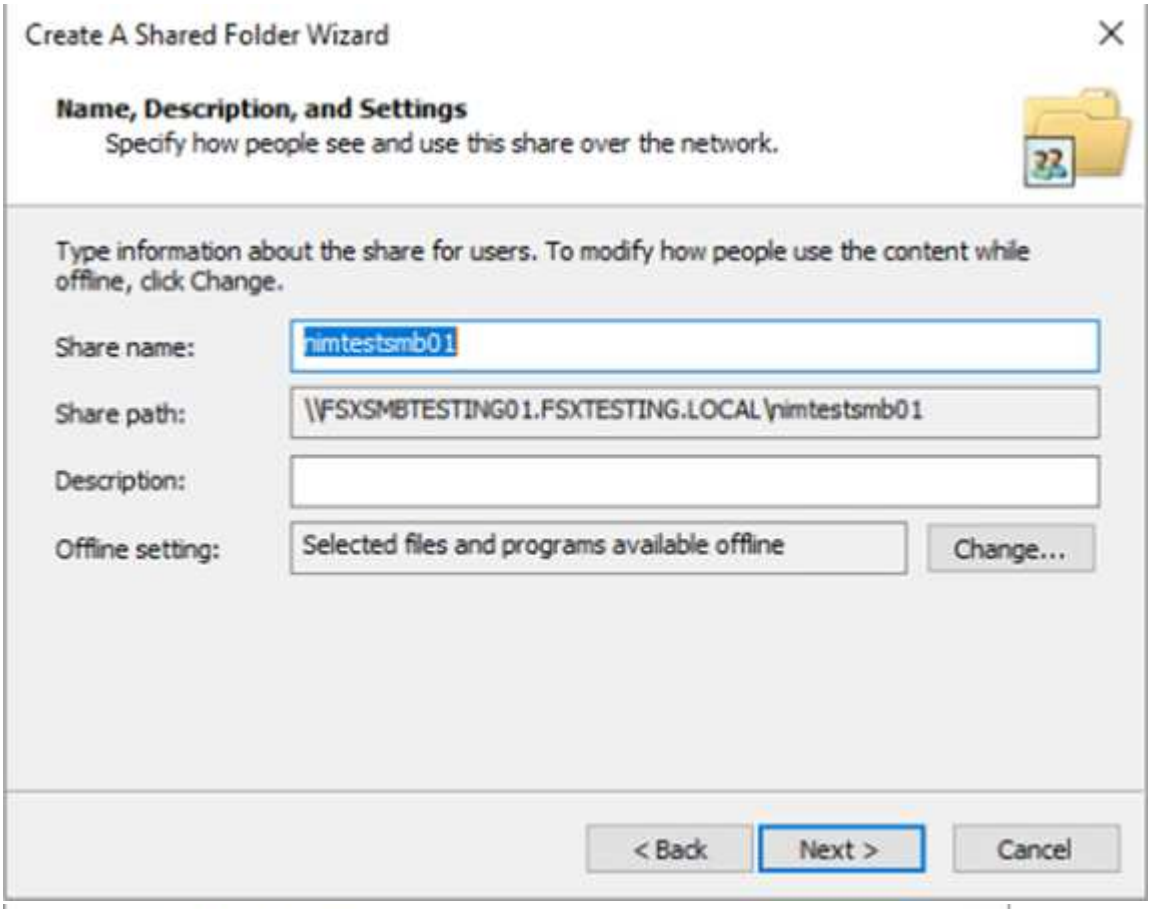
> ⓘ Per trovare il nome DNS dell'SVM nella console Amazon FSx , seleziona Storage Virtual Machines, seleziona SVM e scorri verso il basso fino a Endpoint per trovare il nome DNS SMB. Fare clic su OK. Il file system Amazon FSx viene visualizzato nell'elenco delle cartelle condivise.



1. Nello strumento Cartelle condivise, seleziona Condivisioni nel riquadro a sinistra per visualizzare le condivisioni attive per il file system Amazon FSx .



1. Ora scegli una nuova condivisione e completa la procedura guidata Crea una cartella condivisa.

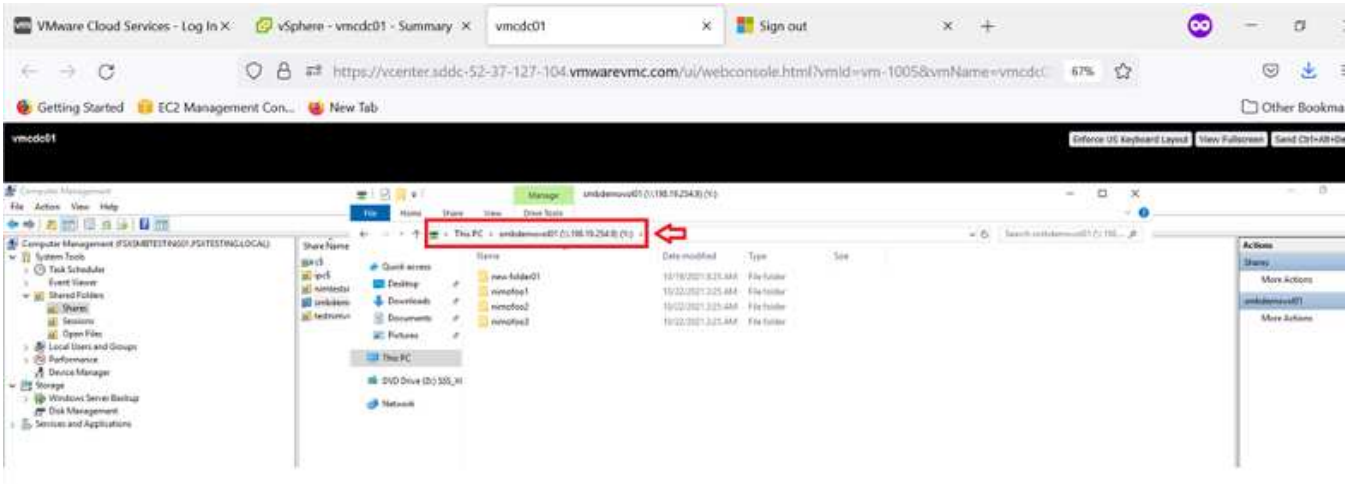




Per saperne di più sulla creazione e la gestione delle condivisioni SMB su un file system Amazon FSx , vedere"Creazione di condivisioni SMB" .

1. Una volta stabilita la connettività, la condivisione SMB può essere collegata e utilizzata per i dati

dell'applicazione. Per fare ciò, copia il percorso di condivisione e utilizza l'opzione Connetti unità di rete per montare il volume sulla VM in esecuzione su VMware Cloud sull'AWS SDDC.



▼ **Collegare un LUN FSx ONTAP a un host tramite iSCSI**

Collegare un LUN FSx ONTAP a un host tramite iSCSI

Il traffico iSCSI per FSx attraversa VMware Transit Connect/AWS Transit Gateway tramite i percorsi forniti nella sezione precedente. Per configurare una LUN in Amazon FSx ONTAP, seguire la documentazione disponibile"Qui" .

Sui client Linux, assicurarsi che il demone iSCSI sia in esecuzione. Dopo aver eseguito il provisioning dei LUN, fare riferimento alla guida dettagliata sulla configurazione iSCSI con Ubuntu (come esempio)"Qui" .

In questo documento viene illustrato come collegare l'iSCSI LUN a un host Windows:

▼ **Fornire una LUN in FSx ONTAP:**

1. Accedere alla CLI NetApp ONTAP utilizzando la porta di gestione del file system FSx per ONTAP .
2. Creare i 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, abbiamo creato una LUN di dimensione 5g (5368709120).

1. Creare gli igroup necessari per controllare quali host hanno accesso a LUN specifici.

```
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. Mappare i LUN sugli igroup 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.

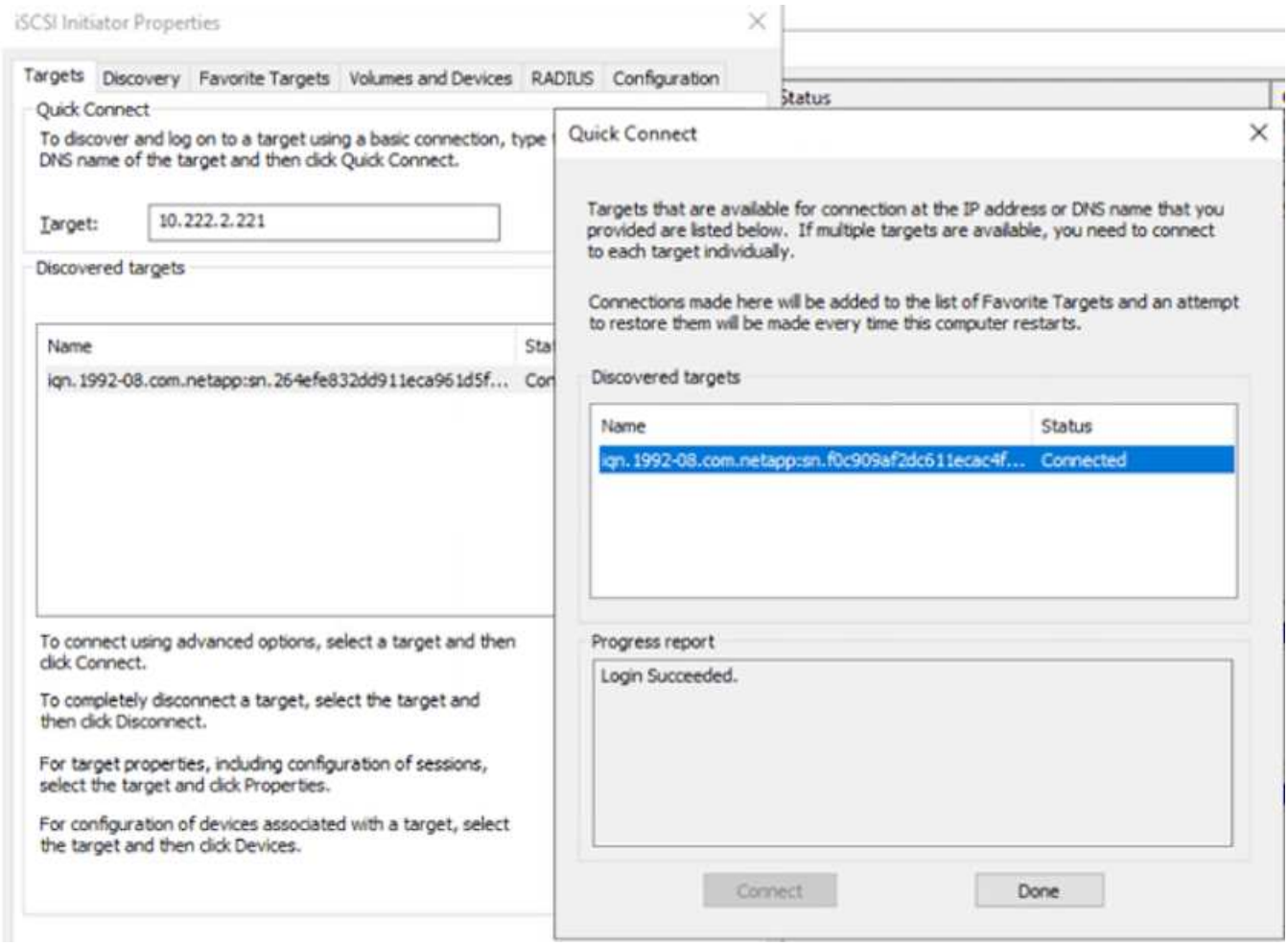
1. Collegare la LUN appena fornita a una VM Windows:

Per connettere il nuovo LUN a un host Windows residente sul cloud VMware su AWS SDDC, completare i seguenti passaggi:

1. RDP alla VM Windows ospitata su VMware Cloud su AWS SDDC.

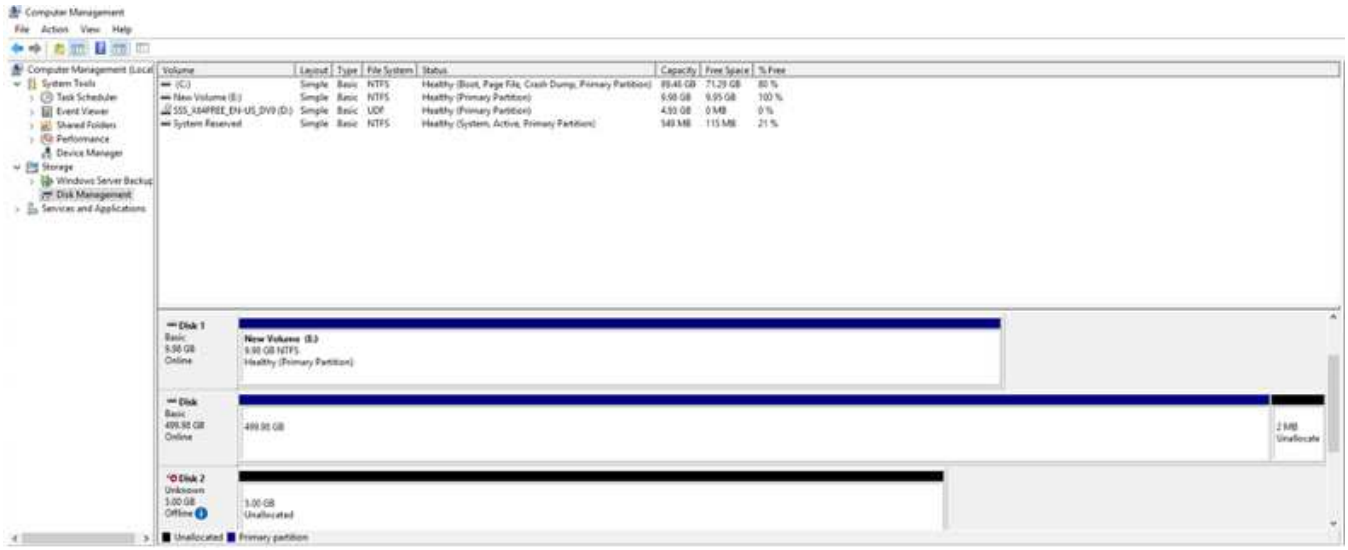
2. Passare a Server Manager > Dashboard > Strumenti > Iniziatore iSCSI per aprire la finestra di dialogo Proprietà dell'iniziatore iSCSI.
3. Dalla scheda Individuazione, fare clic su Individua portale o Aggiungi portale, quindi immettere l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Destinazioni, seleziona la destinazione rilevata e poi fai clic su Accedi o Connetti.
5. Selezionare Abilita Multipath, quindi selezionare "Ripristina automaticamente questa connessione all'avvio del computer" oppure "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.



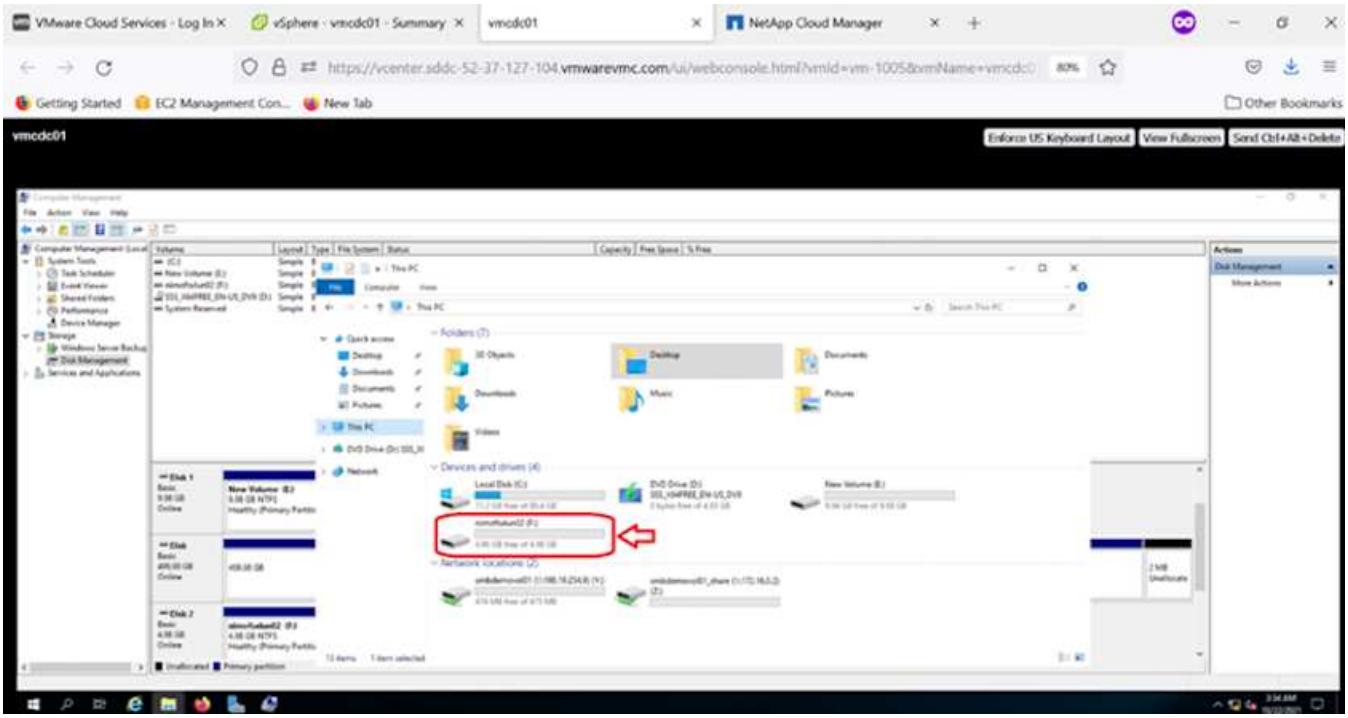
Le LUN sulla macchina virtuale di archiviazione (SVM) vengono visualizzate come dischi dall'host Windows. Tutti i nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Avviare una nuova scansione manuale per rilevare i dischi completando i seguenti passaggi:

1. Aprire l'utilità Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Archiviazione nell'albero di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Azione > Ripeti analisi dischi.



Quando l'host Windows accede per la prima volta a un nuovo LUN, questo non ha alcuna partizione o file system. Inizializzare la LUN e, facoltativamente, formattarla con un file system completando i seguenti passaggi:

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, è montata l'unità F:.



Cloud Volumes ONTAP (CVO)

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti

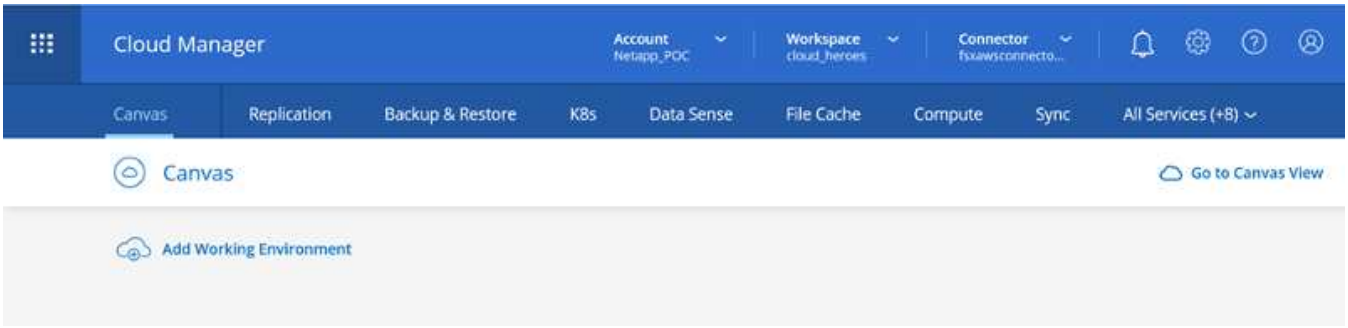
▼ **Distribuisci una nuova istanza Cloud Volumes ONTAP in AWS (fai da te)**

Le condivisioni Cloud Volumes ONTAP possono essere montate da VM create nell'ambiente VMware Cloud on AWS SDDC. I volumi possono anche essere montati su client Linux Windows VM AWS nativi, ed è possibile accedere ai LUN su client Linux o Windows come dispositivi a blocchi quando montati su iSCSI, poiché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

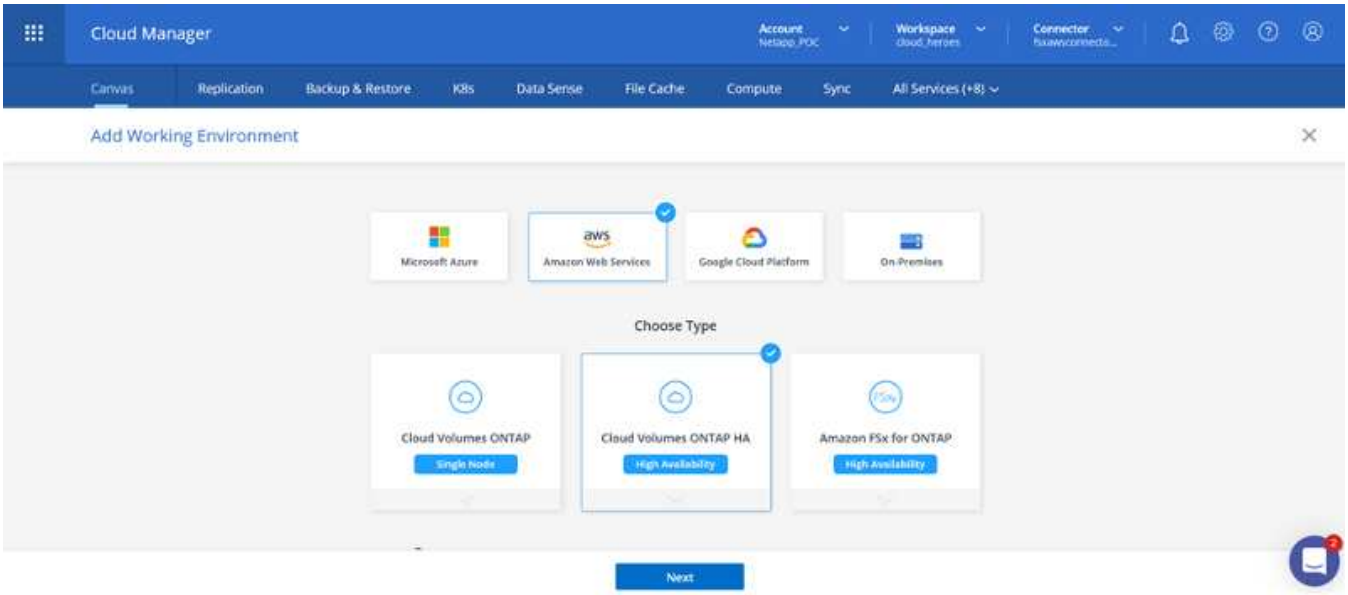
Per replicare volumi da un ambiente locale al cloud per scopi di disaster recovery o migrazione, stabilire la connettività di rete ad AWS, utilizzando una VPN da sito a sito o DirectConnect. La replica dei dati da locale a Cloud Volumes ONTAP esula dall'ambito del presente documento. Per replicare i dati tra i sistemi locali e Cloud Volumes ONTAP , vedere"Impostazione della replica dei dati tra i sistemi" .

Utilizza "Dimensionatore Cloud Volumes ONTAP" per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Monitora inoltre le prestazioni on-premises da usare come input nello strumento di dimensionamento di Cloud Volumes ONTAP.

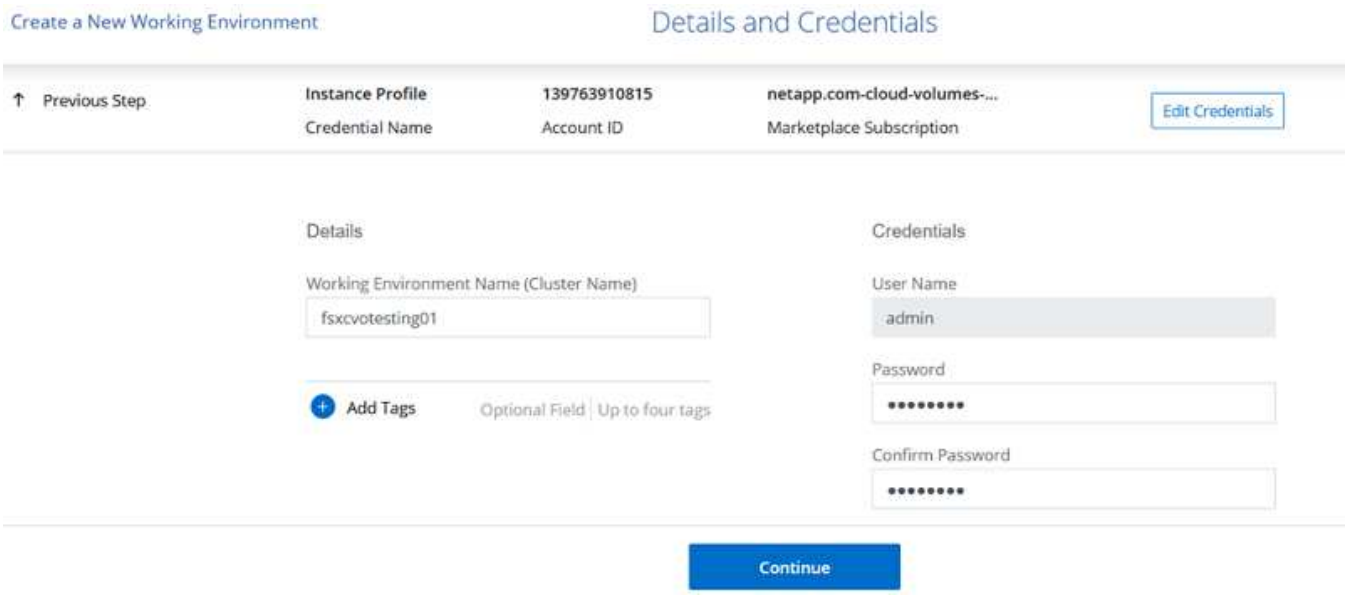
1. Accedi a NetApp Cloud Central; verrà visualizzata la schermata Fabric View. Individua la scheda Cloud Volumes ONTAP e seleziona Vai a Cloud Manager. Dopo aver effettuato l'accesso, verrà visualizzata la schermata Canvas.



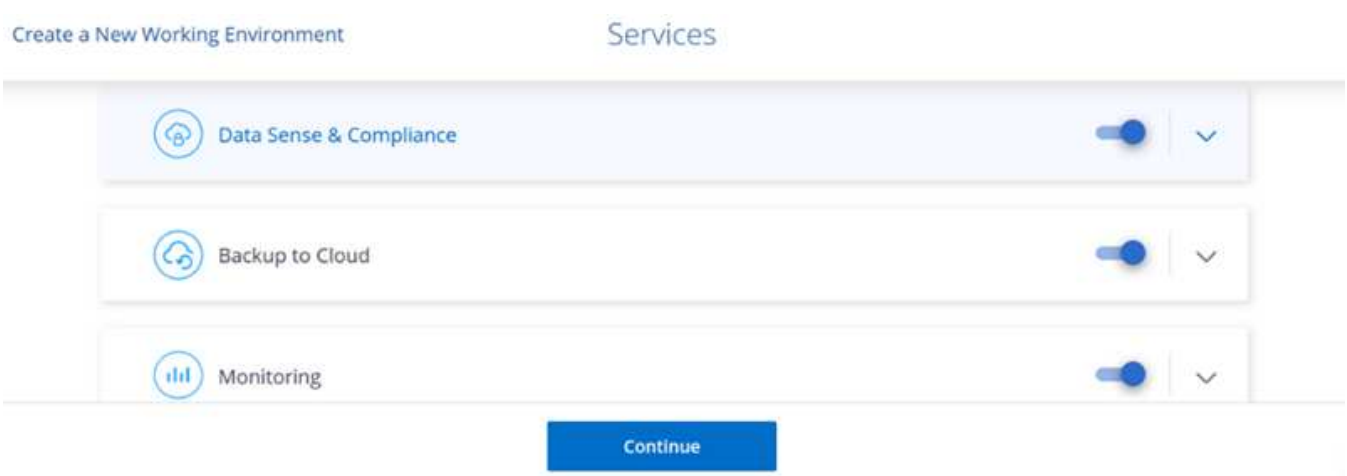
1. Nella home page di Cloud Manager, fai clic su Aggiungi un ambiente di lavoro, quindi seleziona AWS come cloud e il tipo di configurazione del sistema.



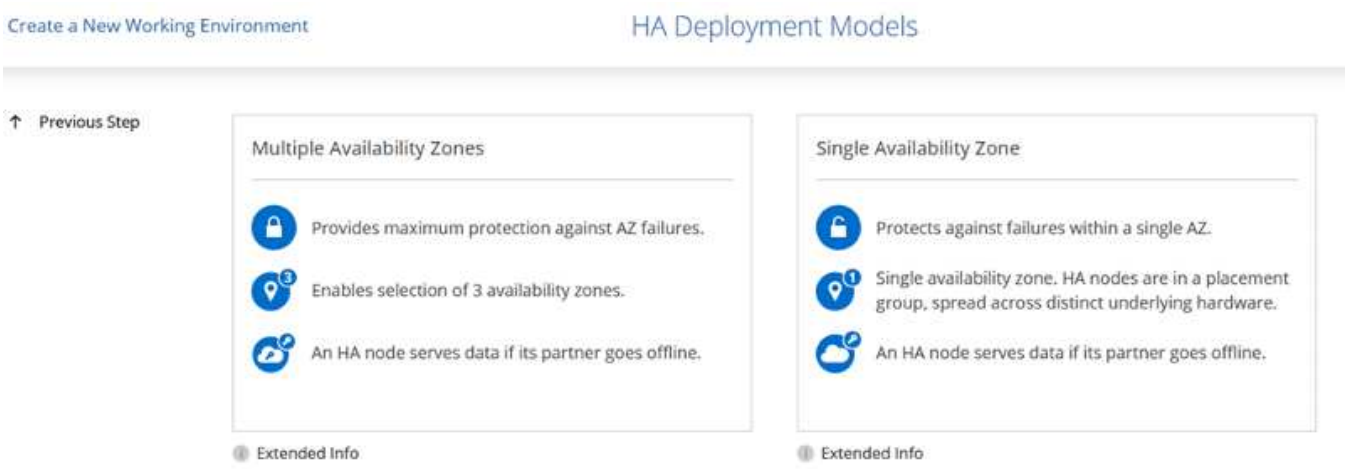
1. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Fare clic su Continua.



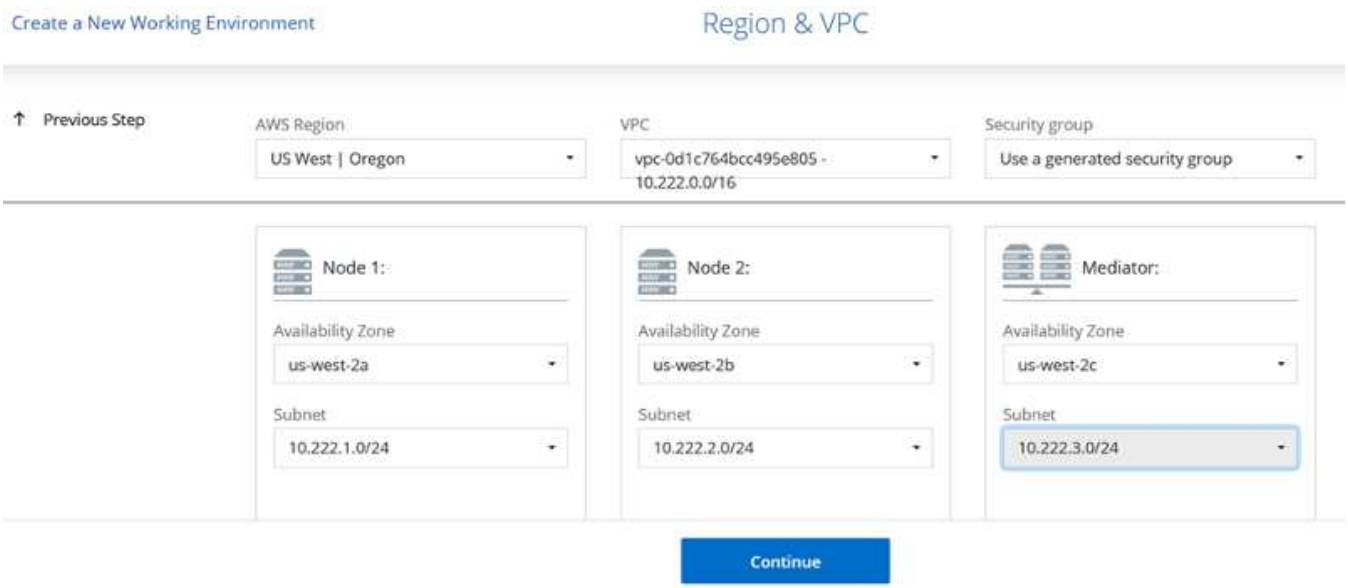
1. Seleziona i servizi aggiuntivi per la distribuzione di Cloud Volumes ONTAP, inclusi NetApp Data Classification, NetApp Backup and Recovery e Data Infrastructure Insights. Fai clic su Continue.



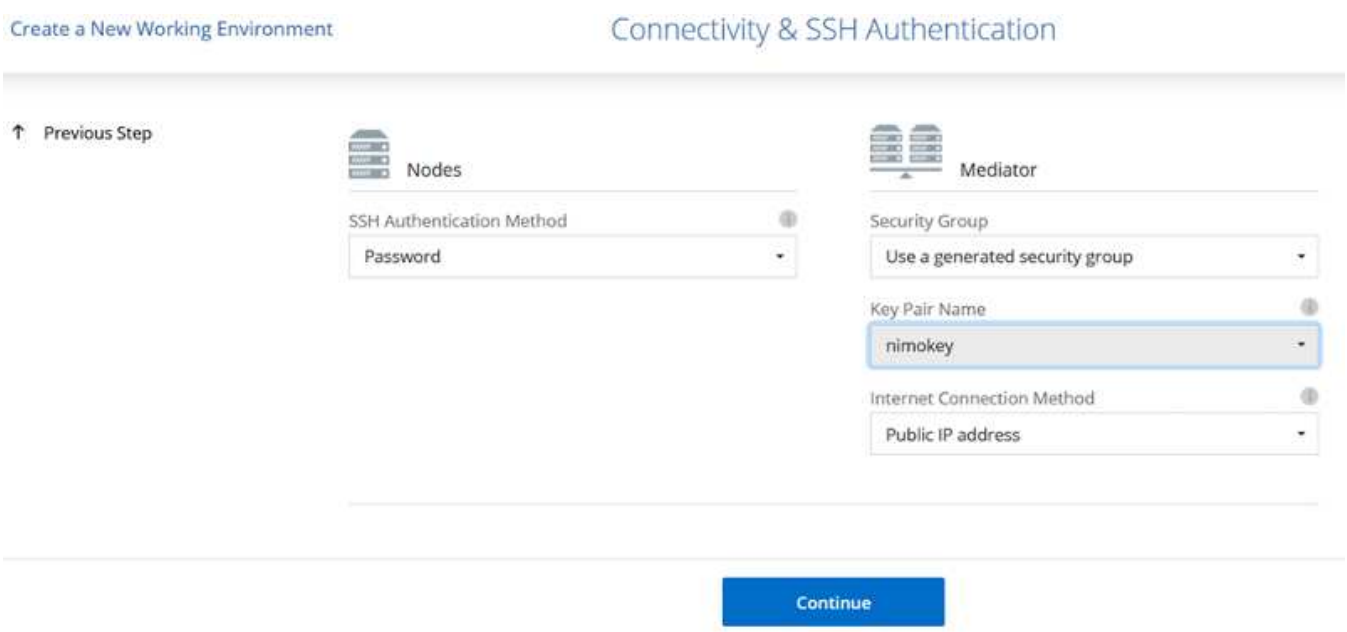
1. Nella pagina Modelli di distribuzione HA, selezionare la configurazione Zone di disponibilità multiple.



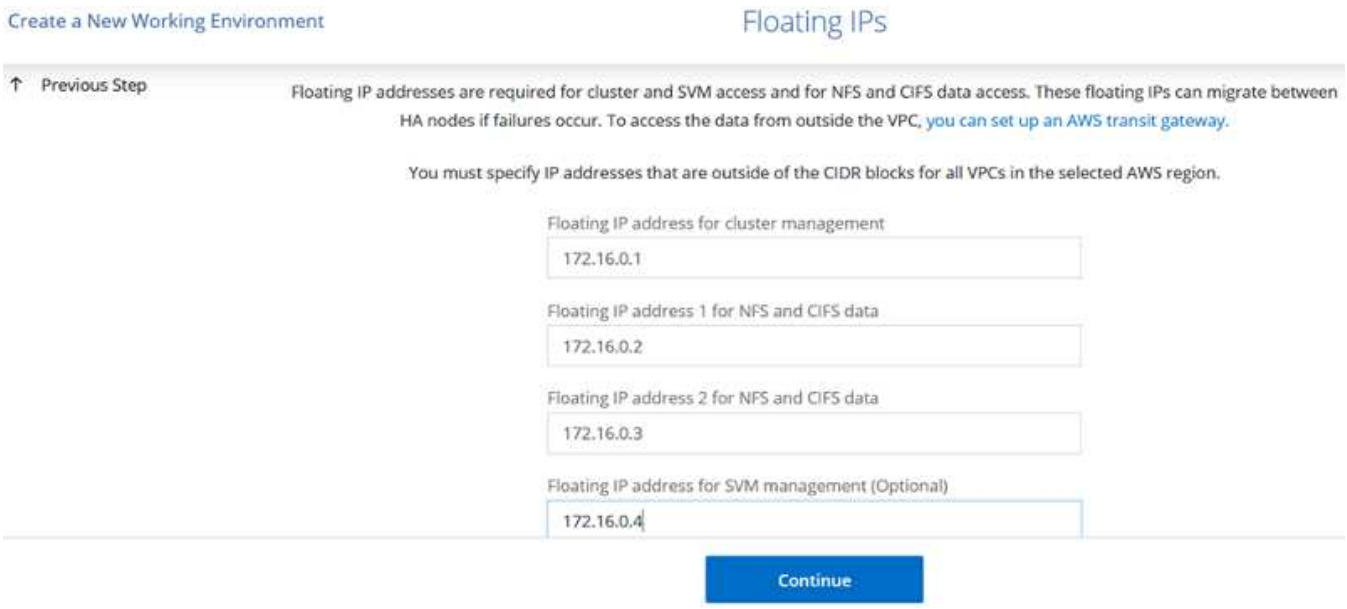
1. Nella pagina Regione e VPC, inserisci le informazioni di rete e poi fai clic su Continua.



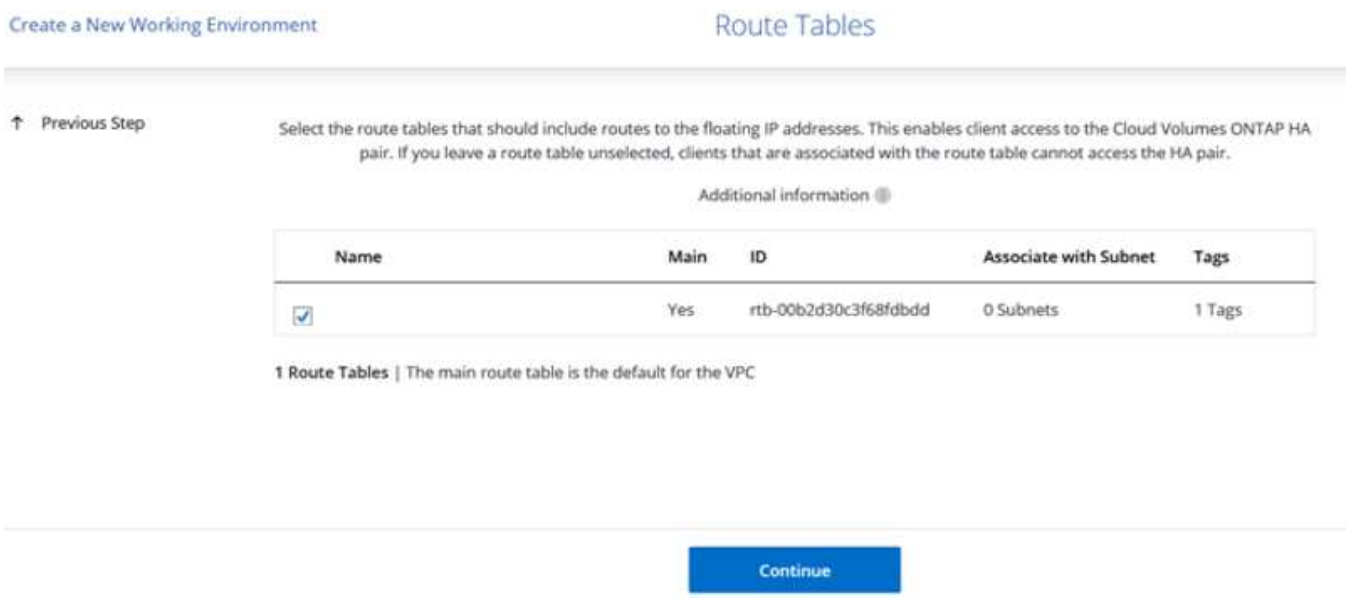
1. Nella pagina Connettività e autenticazione SSH, scegliere i metodi di connessione per la coppia HA e il mediatore.



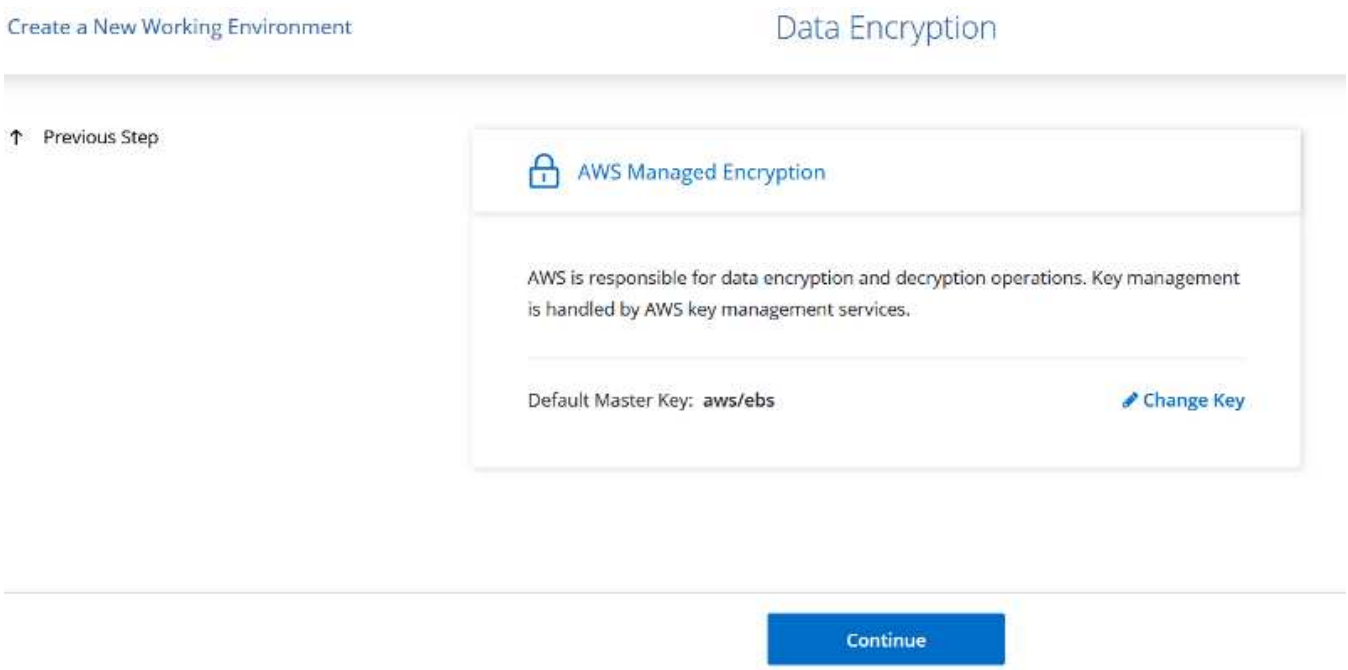
1. Specificare gli indirizzi IP mobili e quindi fare clic su Continua.



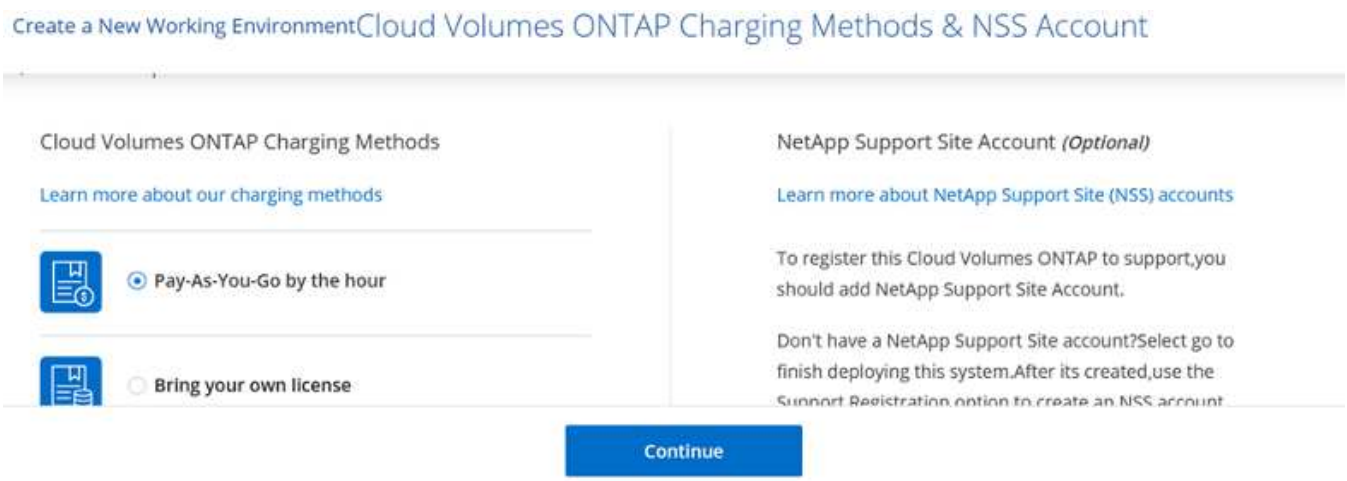
1. Selezionare le tabelle di routing appropriate per includere i percorsi verso gli indirizzi IP mobili, quindi fare clic su Continua.



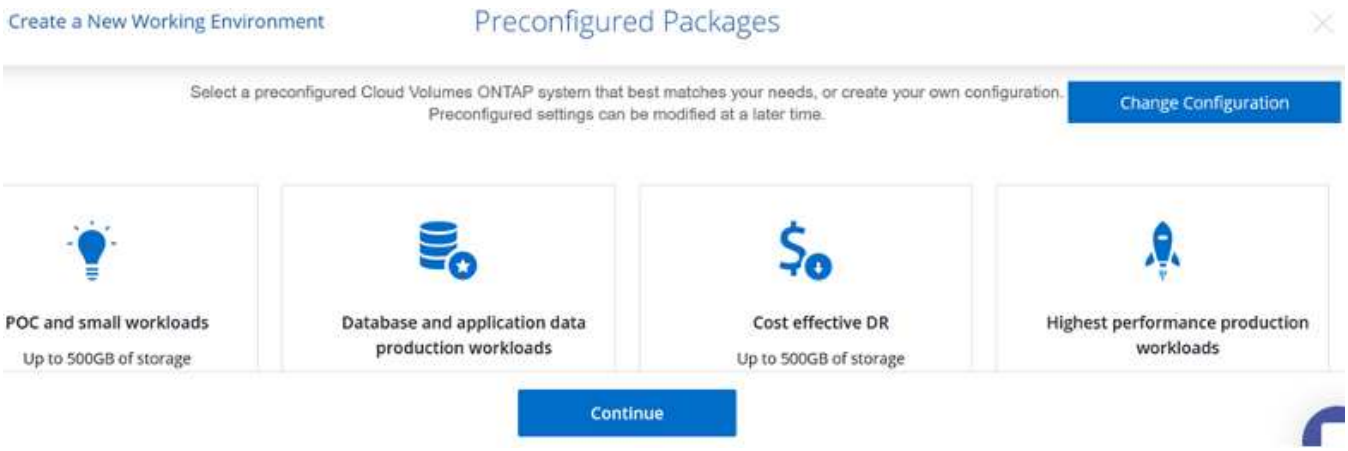
1. Nella pagina Crittografia dati, seleziona Crittografia gestita da AWS.



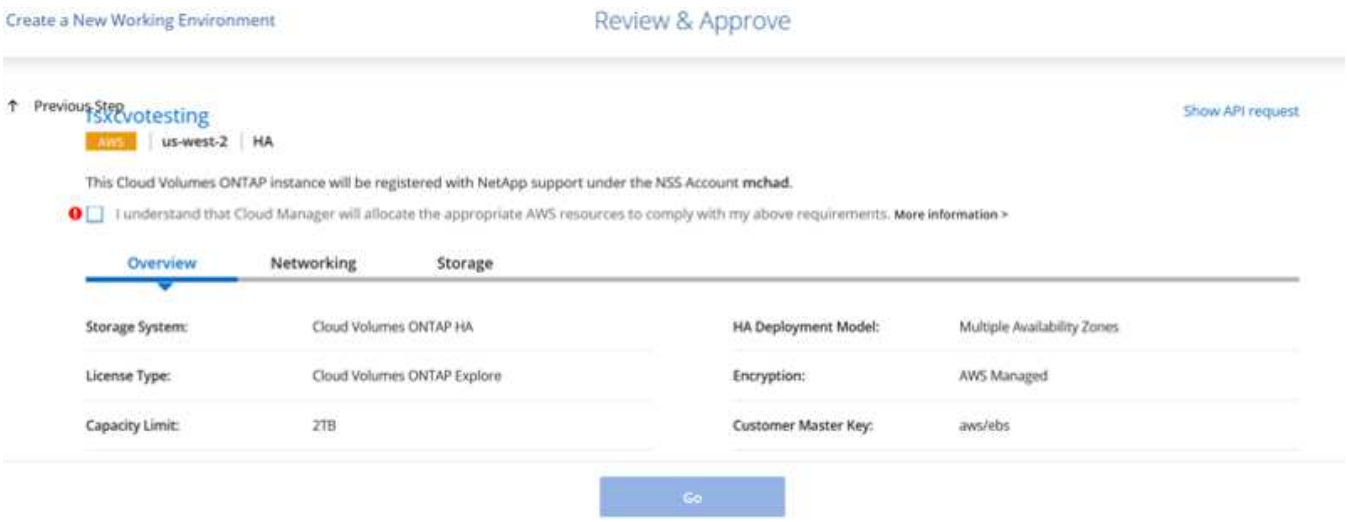
1. Selezionare l’opzione di licenza: Pay-As-You-Go o BYOL per utilizzare una licenza esistente. In questo esempio viene utilizzata l’opzione Pay-As-You-Go.



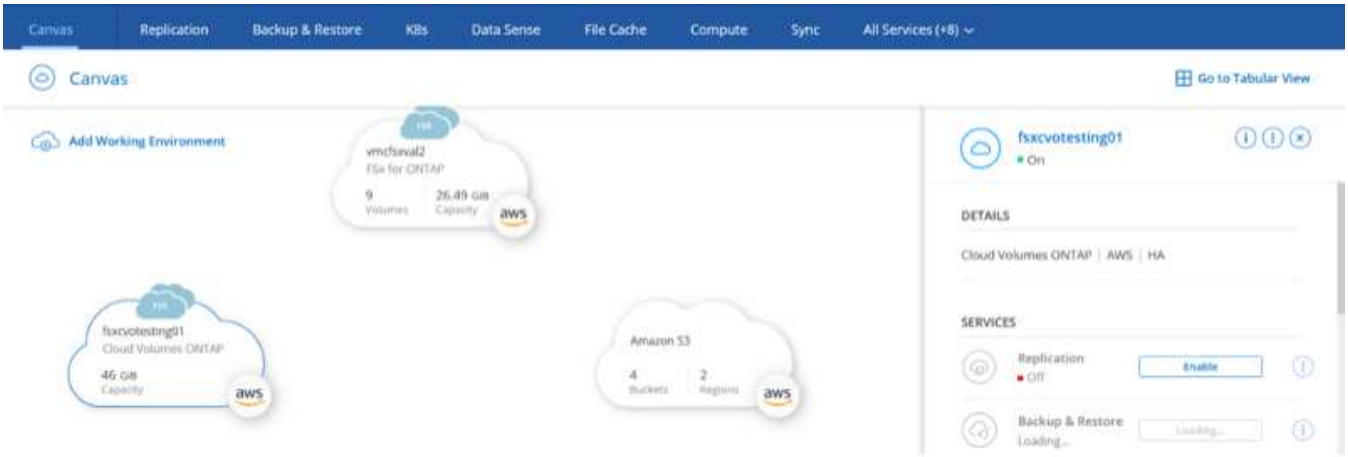
1. Seleziona tra diversi pacchetti preconfigurati disponibili in base al tipo di carico di lavoro da distribuire sulle VM in esecuzione sul cloud VMware su AWS SDDC.



1. Nella pagina Revisione e approvazione, rivedere e confermare le selezioni. Per creare l'istanza Cloud Volumes ONTAP , fare clic su Vai.

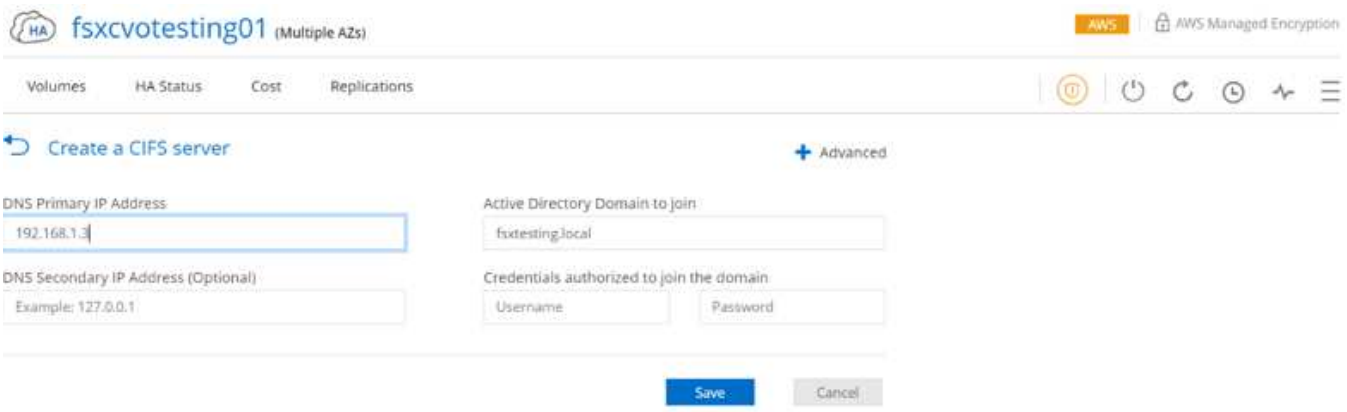


1. Dopo aver eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.

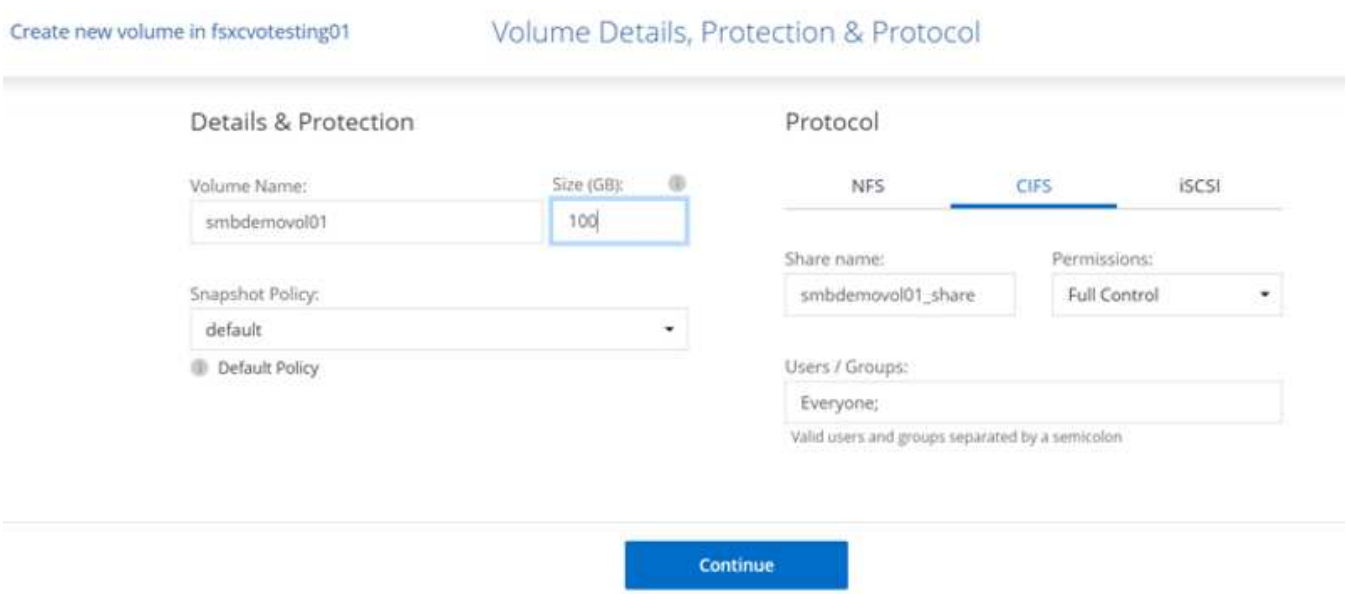


▼ **Configurazioni aggiuntive per volumi SMB**

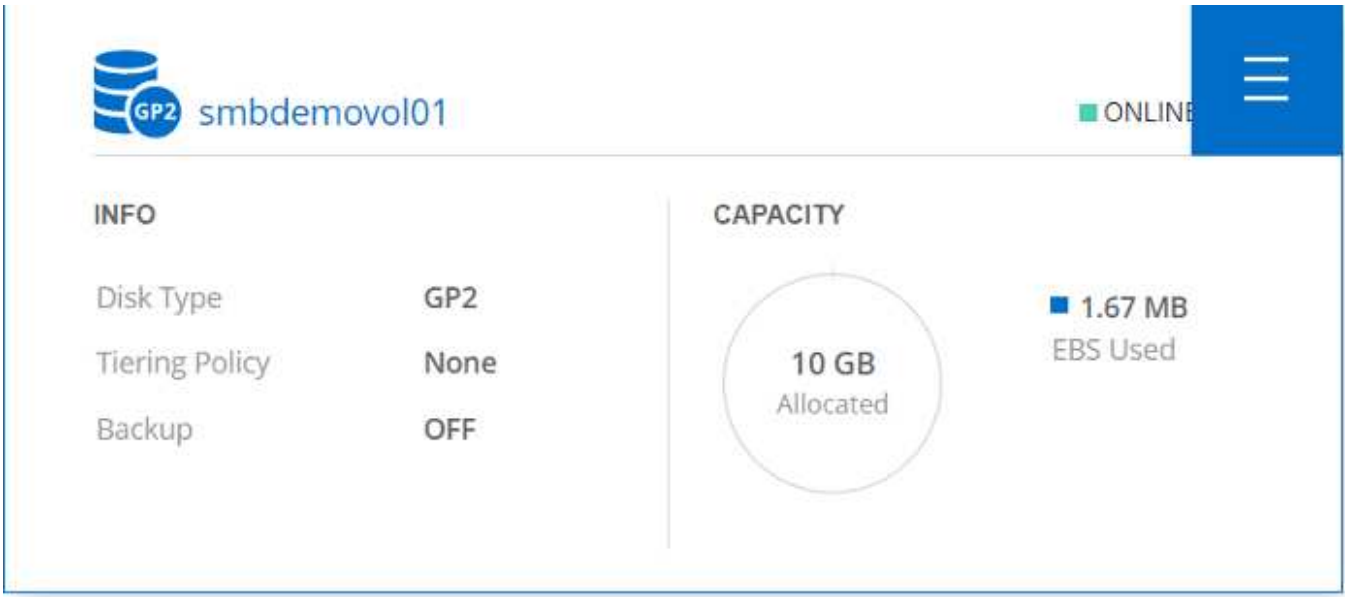
1. Una volta che l'ambiente di lavoro è pronto, assicurarsi che il server CIFS sia configurato con i parametri di configurazione DNS e Active Directory appropriati. Questo passaggio è necessario prima di poter creare il volume SMB.



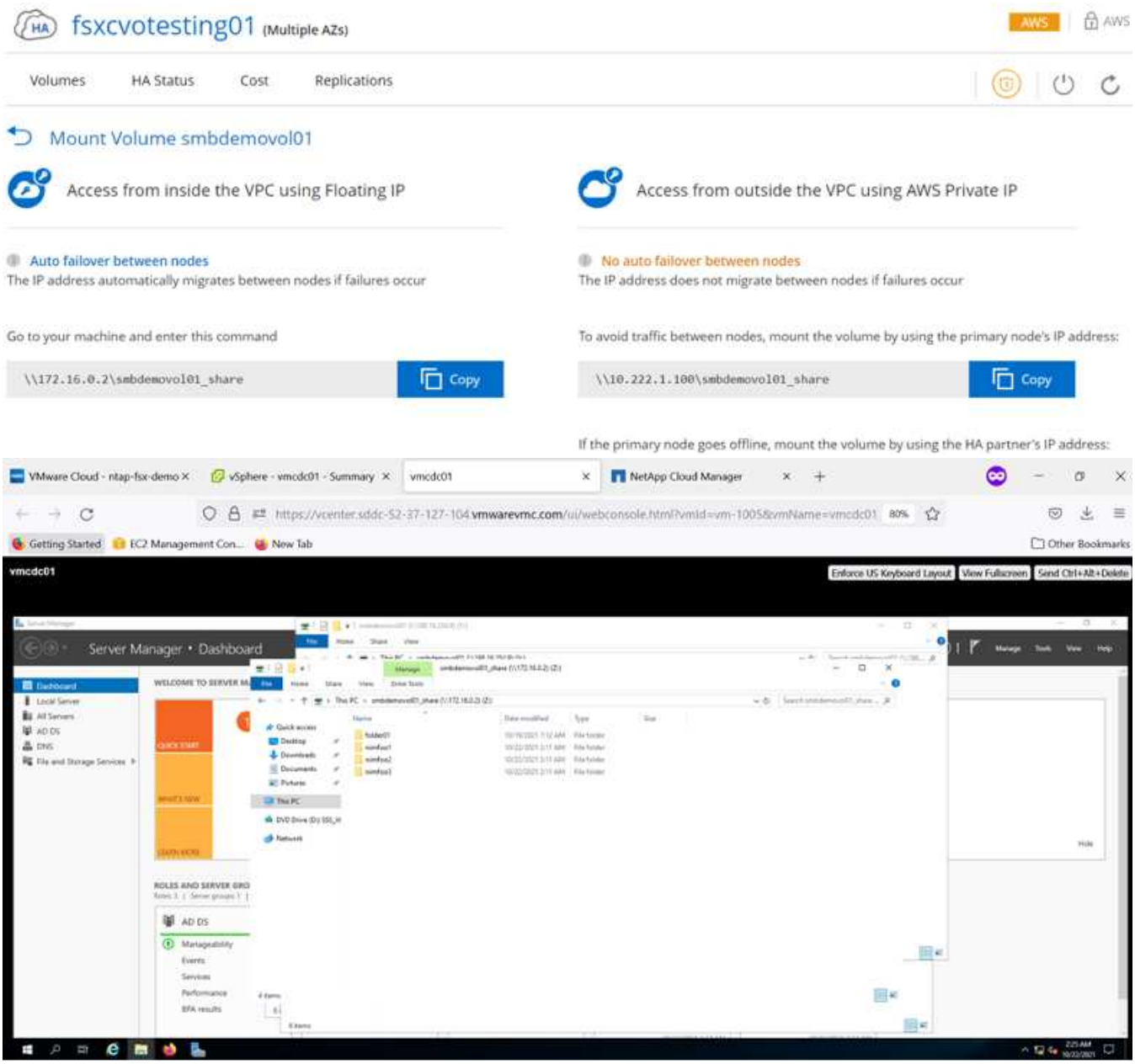
1. Selezionare l'istanza CVO per creare il volume e fare clic sull'opzione Crea volume. Scegli la dimensione appropriata e il gestore cloud sceglierà l'aggregato contenente oppure utilizzerà un meccanismo di allocazione avanzato per posizionarlo su un aggregato specifico. Per questa demo, è stato selezionato SMB come protocollo.



1. Dopo aver eseguito il provisioning, il volume sarà disponibile nel riquadro Volumi. Poiché è stata predisposta una condivisione CIFS, è necessario concedere agli utenti o ai gruppi l'autorizzazione per accedere ai file e alle cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.



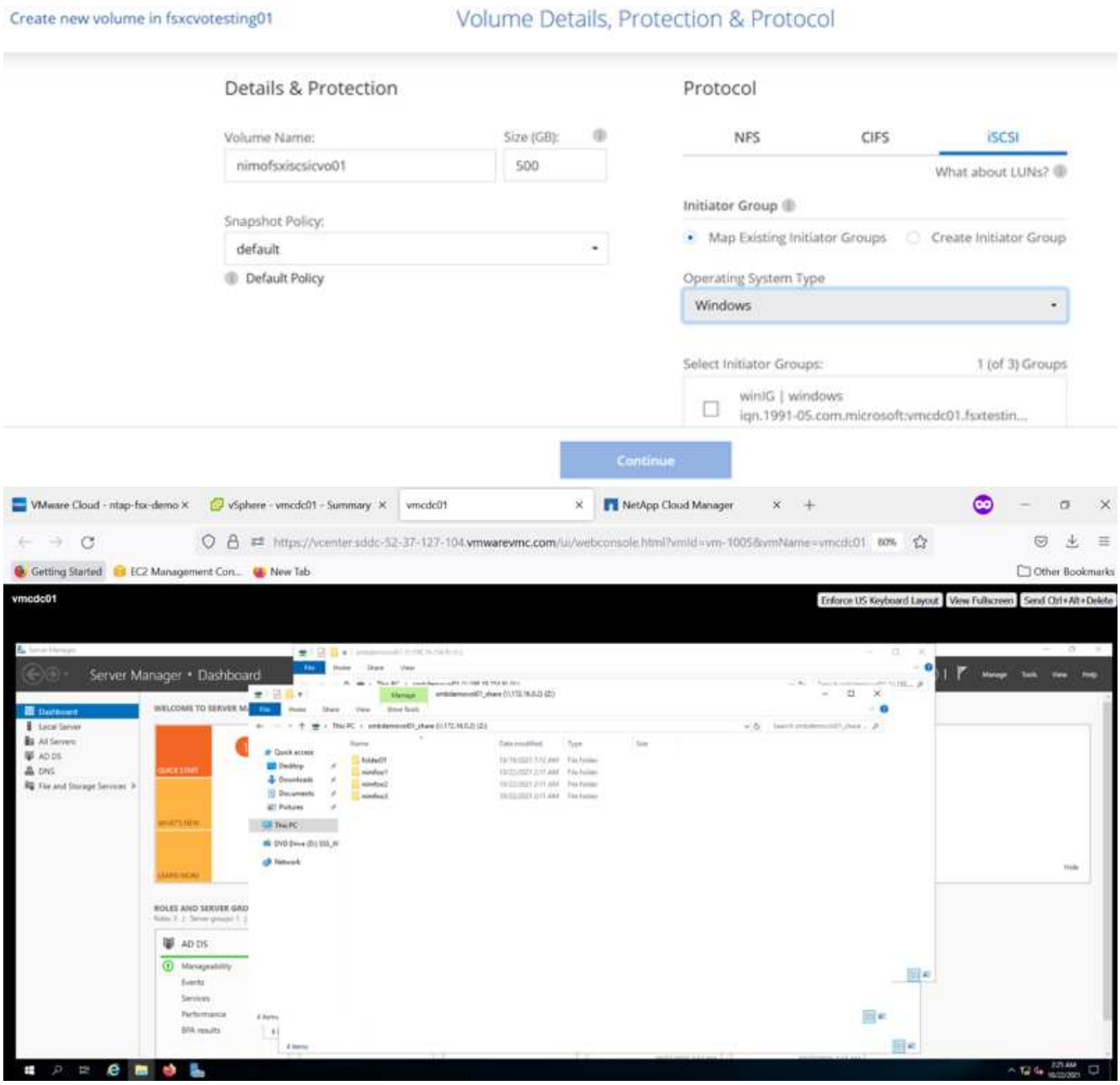
1. Dopo aver creato il volume, utilizzare il comando mount per connettersi alla condivisione dalla VM in esecuzione su VMware Cloud negli host AWS SDDC.
2. Copia il percorso seguente e utilizza l'opzione Connetti unità di rete per montare il volume sulla VM in esecuzione su VMware Cloud in AWS SDDC.



▼ **Collegare la LUN a un host**

Per connettere il LUN Cloud Volumes ONTAP a un host, completare i seguenti passaggi:

1. Nella pagina Cloud Manager Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Aggiungi volume > Nuovo volume, selezionare iSCSI e fare clic su Crea gruppo iniziatori. Fare clic su Continua.



1. Dopo aver eseguito il provisioning del volume, selezionarlo e fare clic su Target IQN. Per copiare il nome qualificato iSCSI (IQN), fare clic su Copia. Impostare una connessione iSCSI dall'host al LUN.

Per ottenere lo stesso risultato per l'host residente su VMware Cloud on AWS SDDC, completare i seguenti passaggi:

1. RDP alla VM ospitata sul cloud VMware su AWS.
2. Aprire la finestra di dialogo Proprietà dell'iniziatore iSCSI: Server Manager > Dashboard > Strumenti > Iniziatore iSCSI.
3. Dalla scheda Individuazione, fare clic su Individua portale o Aggiungi portale, quindi immettere l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Destinazioni, seleziona la destinazione rilevata e poi fai clic su Accedi o Connetti.
5. Selezionare Abilita multipath, quindi selezionare Ripristina automaticamente questa connessione all'avvio del computer o Aggiungi questa connessione all'elenco delle destinazioni preferite. Fare clic su

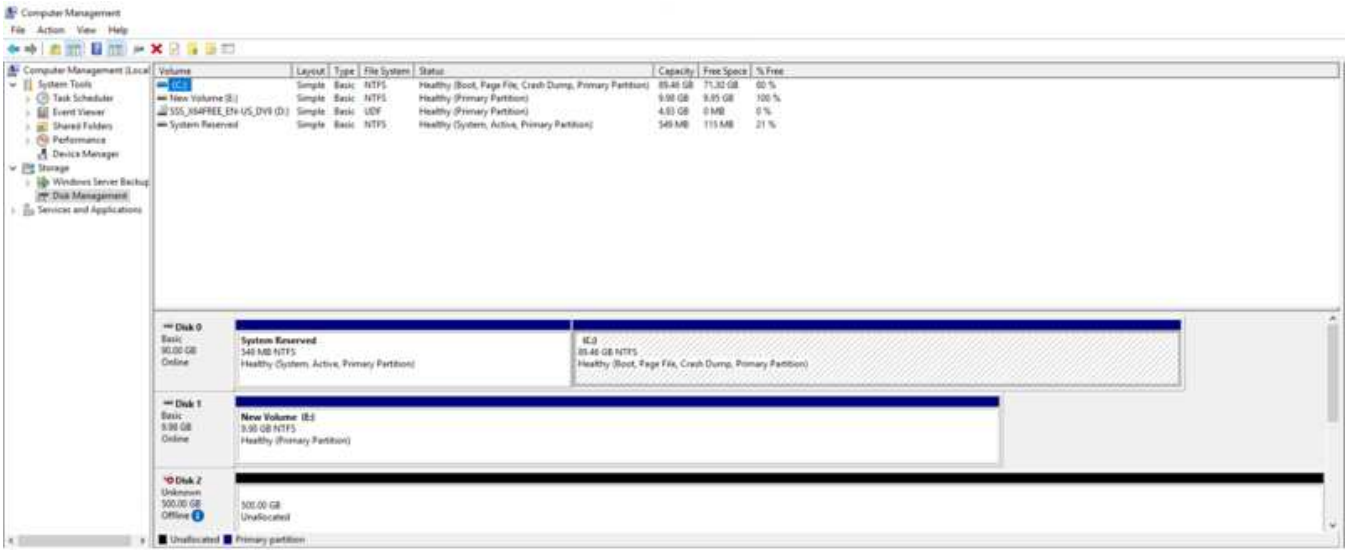
Avanzate.

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



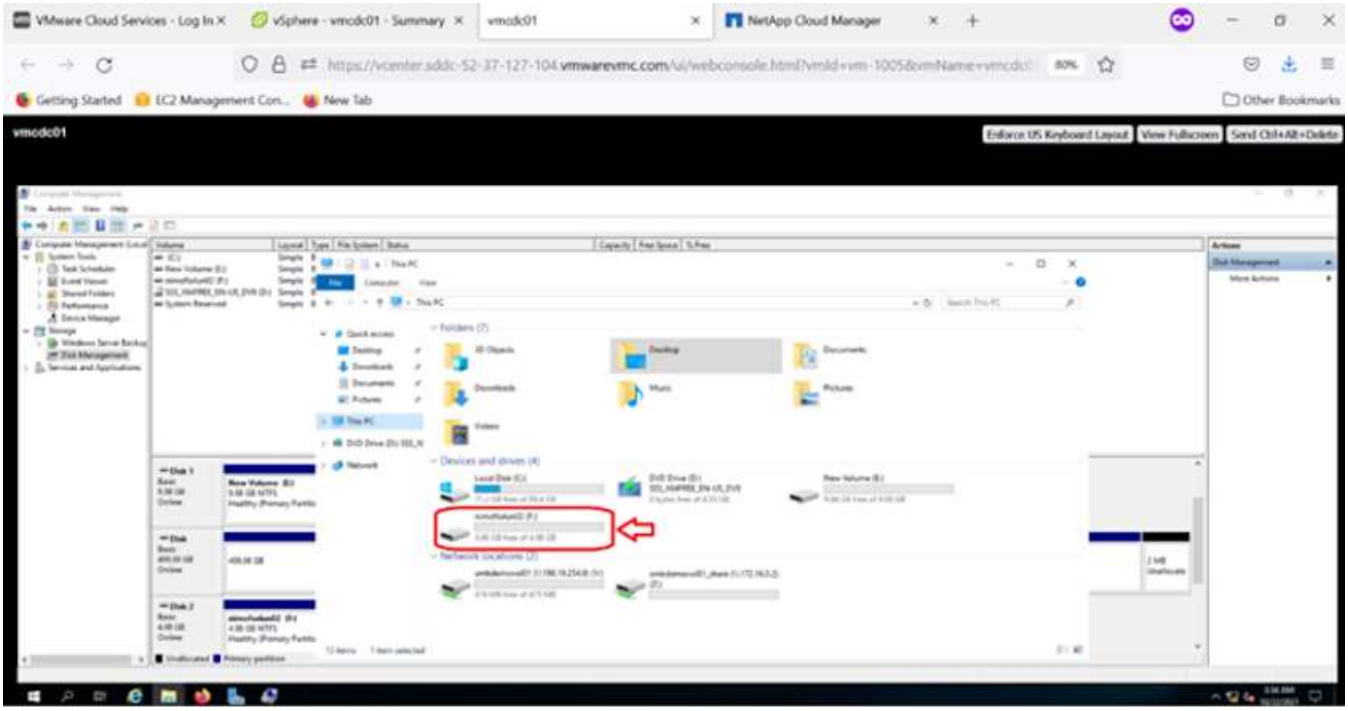
Le LUN dell'SVM vengono visualizzate come dischi sull'host Windows. Tutti i nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Avviare una nuova scansione manuale per rilevare i dischi completando i seguenti passaggi:

1. Aprire l'utilità Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Archiviazione nell'albero di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Azione > Ripeti analisi dischi.



Quando l'host Windows accede per la prima volta a un nuovo LUN, questo non ha alcuna partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando i seguenti passaggi:

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, è montata l'unità F:.



Sui client Linux, assicurarsi che il demone iSCSI sia in esecuzione. Dopo aver eseguito il provisioning dei LUN, fare riferimento alle istruzioni dettagliate sulla configurazione iSCSI per la propria distribuzione Linux. Ad esempio, la configurazione iSCSI di Ubuntu può essere trovata"Qui" . Per verificare, eseguire lsblk cmd dalla shell.

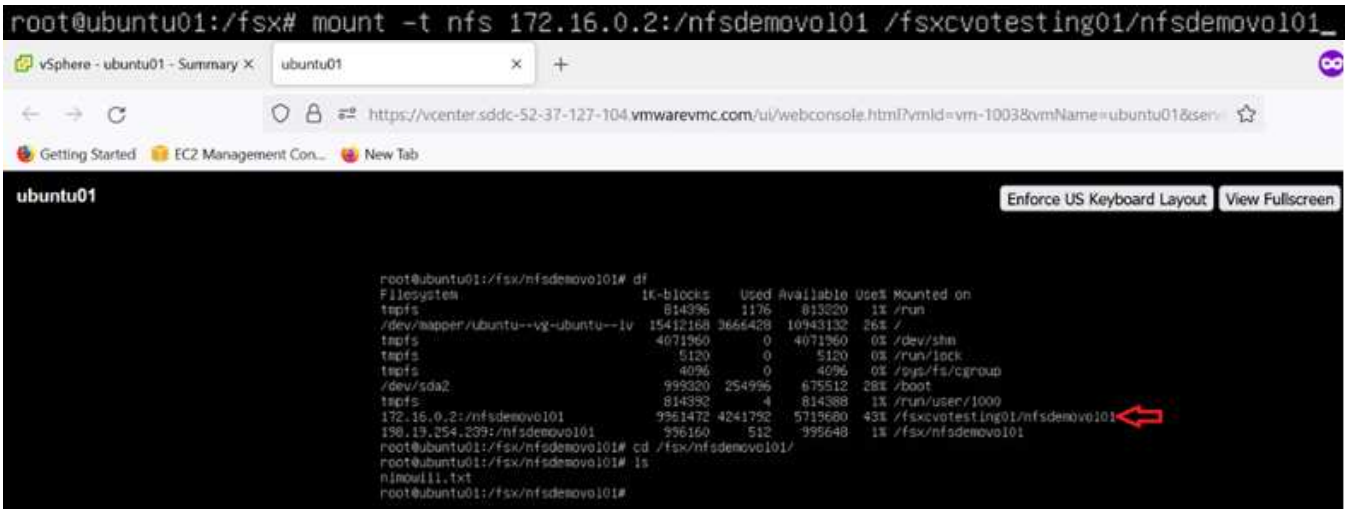
▼ Montare il volume Cloud Volumes ONTAP NFS sul client Linux

Per montare il file system Cloud Volumes ONTAP (DIY) dalle VM 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) ed effettuare l'accesso 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 Amazon FSx ONTAP NFS nella directory creata nel
passaggio precedente.
```

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



Servizio di virtualizzazione di Azure: opzioni per l'utilizzo dell'archiviazione NetApp

Lo storage NetApp può essere collegato al servizio Azure VMware come storage connesso come guest o come storage supplementare.

Azure NetApp Files (ANF) come datastore NFS supplementare

Il supporto per i datastore NFS è stato introdotto con ESXi versione 3 nelle distribuzioni on-premise, ampliando notevolmente le capacità di archiviazione di vSphere.

L'esecuzione di vSphere su NFS è un'opzione ampiamente adottata per le distribuzioni di virtualizzazione in locale perché offre prestazioni e stabilità elevate. Se disponi di un'ampia quantità di storage collegato alla rete (NAS) in un data center locale, dovresti prendere in considerazione l'implementazione di una soluzione SDDC di Azure VMware in Azure con datastore di file Azure NetApp per superare le sfide di capacità e prestazioni.

Azure NetApp Files è basato sul software di gestione dati NetApp ONTAP , leader del settore e altamente disponibile. I servizi Microsoft Azure sono raggruppati in tre categorie: fondamentali, tradizionali e specializzati. Azure NetApp Files rientra nella categoria specializzata ed è supportato da hardware già distribuito in molte

regioni. Grazie all'elevata disponibilità (HA) integrata, Azure NetApp Files protegge i tuoi dati dalla maggior parte delle interruzioni e ti offre un SLA leader del settore con un tempo di attività del 99,99%^.

Per maggiori informazioni su ANF come datastore NFS supplementare, visitare:

- "ANF come datastore NFS supplementare: panoramica"
- "Opzione NFS Datastore supplementare in Azure"

Azure NetApp Files (ANF) come storage connesso guest

Azure NetApp Files offre gestione e archiviazione dei dati di livello aziendale in Azure, consentendoti di gestire con facilità i tuoi carichi di lavoro e le tue applicazioni. Migra i tuoi carichi di lavoro sul cloud ed eseguili senza sacrificare le prestazioni.

Azure NetApp Files rimuove gli ostacoli, così puoi spostare tutte le tue applicazioni basate su file nel cloud. Per la prima volta, non è necessario riprogettare le applicazioni e si ottiene uno storage persistente per le applicazioni senza complessità.

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

Per maggiori informazioni, visitare"ANF come Guest Connected Storage" .

Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Per maggiori informazioni, visitare"CVO come Guest Connected Storage" .

Panoramica delle soluzioni ANF Datastore

Ogni organizzazione di successo è in cammino verso la trasformazione e la modernizzazione. Come parte di questo processo, le aziende in genere sfruttano i propri investimenti VMware esistenti, sfruttando al contempo i vantaggi del cloud e cercando di rendere i processi di migrazione, burst, estensione e disaster recovery il più fluidi possibile. I clienti che migrano verso il cloud devono valutare le problematiche di elasticità 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 aziendali. Quando si scelgono operazioni basate sul cloud, un obiettivo fondamentale è selezionare un modello a basso costo con prestazioni adeguate e ostacoli minimi. Oltre alla scelta della piattaforma giusta, l'orchestrazione dello storage e del flusso di lavoro è particolarmente importante per sfruttare al meglio la potenza e l'elasticità dell'implementazione cloud.

Casi d'uso

Sebbene la soluzione Azure VMware offra ai clienti funzionalità ibride uniche, le limitate opzioni di archiviazione nativa ne hanno limitato l'utilità per le organizzazioni con carichi di lavoro ad alta intensità di archiviazione. Poiché lo storage è direttamente collegato agli host, l'unico modo per scalare lo storage è aggiungere più host, il che può aumentare i costi del 35-40% o più per carichi di lavoro ad alta intensità di storage. Questi carichi di lavoro necessitano di spazio di archiviazione aggiuntivo, non di potenza aggiuntiva, ma ciò significa pagare per host aggiuntivi.

Consideriamo il seguente scenario: un cliente necessita di sei host per la potenza (vCPU/vMem), ma ha anche un fabbisogno sostanziale di spazio di archiviazione. In base alla loro valutazione, per soddisfare i requisiti di archiviazione sono necessari 12 host. Ciò aumenta il TCO complessivo perché devono acquistare tutta quella potenza aggiuntiva quando in realtà hanno bisogno solo di più spazio di archiviazione. Ciò è applicabile a qualsiasi caso d'uso, tra cui migrazione, disaster recovery, bursting, sviluppo/test e così via.

Un altro caso d'uso comune per Azure VMware Solution è il disaster recovery (DR). La maggior parte delle organizzazioni non dispone di una strategia di ripristino di emergenza infallibile oppure potrebbe avere difficoltà a giustificare l'esecuzione di un data center fantasma solo per il ripristino di emergenza. Gli amministratori potrebbero valutare opzioni di ripristino di emergenza a impatto zero con un cluster pilota o un cluster on-demand. Potrebbero quindi scalare lo storage senza aggiungere host aggiuntivi, un'opzione potenzialmente interessante.

Quindi, riassumendo, i casi d'uso possono essere classificati in due modi:

- Scalabilità della capacità di archiviazione utilizzando datastore ANF
- Utilizzo di datastore ANF come destinazione di disaster recovery per un flusso di lavoro di ripristino ottimizzato in termini di costi da locale o all'interno di regioni di Azure tra i data center definiti dal software (SDDC). Questa guida fornisce informazioni sull'utilizzo di Azure NetApp Files per fornire storage ottimizzato per datastore (attualmente in anteprima pubblica) insieme alle migliori funzionalità di protezione dei dati e DR in una soluzione Azure VMware, che consente di scaricare la capacità di storage dall'archiviazione vSAN.



Per ulteriori informazioni sull'utilizzo dei datastore ANF, contattare gli architetti di soluzioni NetApp o Microsoft nella propria area geografica.

Opzioni VMware Cloud in Azure

Soluzione Azure VMware

Azure VMware Solution (AVS) è un servizio cloud ibrido che fornisce VMware SDDC completamente funzionanti all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione proprietaria 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 l'archiviazione iperconvergente e NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture dei data center leader del settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure nativi. La combinazione

di Azure VMware Solution SDDC e Azure NetApp Files garantisce le migliori prestazioni con una latenza di rete minima.

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

- VMware ESXi ospita per la virtualizzazione del calcolo 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 e sicurezza virtuali con un cluster NSX Manager per la gestione.

Conclusione

Che si punti a un cloud all-cloud o ibrido, i file di Azure NetApp offrono ottime opzioni per distribuire e gestire i carichi di lavoro delle applicazioni insieme ai servizi file, riducendo al contempo il TCO rendendo i requisiti dei dati uniformi al livello dell'applicazione. Qualunque sia il caso d'uso, scegli Azure VMware Solution insieme ad Azure NetApp Files per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti in locale e su più cloud, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per collegare l'archiviazione. Ricorda che è cambiata solo la posizione dei dati e i nuovi nomi; gli strumenti e i processi sono rimasti gli stessi e Azure NetApp Files aiuta a ottimizzare la distribuzione complessiva.

Da asporto

I punti chiave di questo documento includono:

- Ora è possibile utilizzare Azure NetApp Files come archivio dati su AVS SDDC.
- Aumenta i tempi di risposta delle applicazioni e garantisci una maggiore disponibilità per consentire l'accesso ai dati del carico di lavoro quando e dove necessario.
- Semplifica la complessità complessiva dello storage vSAN con funzionalità di ridimensionamento semplici e immediate.
- Prestazioni garantite per carichi di lavoro mission-critical grazie alle funzionalità di rimodellamento dinamico.
- Se la destinazione è Azure VMware Solution Cloud, Azure NetApp Files è la soluzione di archiviazione ideale per una distribuzione ottimizzata.

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, fare riferimento ai seguenti link del sito web:

- Documentazione della soluzione Azure VMware

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

- Documentazione Azure NetApp Files

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

- Collegare gli archivi dati di Azure NetApp Files agli host della soluzione Azure VMware (anteprima)

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

Creazione di un datastore NFS supplementare in Azure

Il supporto per i datastore NFS è stato introdotto con ESXi versione 3 nelle distribuzioni on-premise, ampliando notevolmente le capacità di archiviazione di vSphere.

L'esecuzione di vSphere su NFS è un'opzione ampiamente adottata per le distribuzioni di virtualizzazione in locale perché offre prestazioni e stabilità elevate. Se disponi di un'ampia quantità di storage collegato alla rete (NAS) in un data center locale, dovresti prendere in considerazione l'implementazione di una soluzione SDDC di Azure VMware in Azure con datastore di file Azure NetApp per superare le sfide di capacità e prestazioni.

Azure NetApp Files è basato sul software di gestione dati NetApp ONTAP , leader del settore e altamente disponibile. I servizi Microsoft Azure sono raggruppati in tre categorie: fondamentali, tradizionali e specializzati. Azure NetApp Files rientra nella categoria specializzata ed è supportato da hardware già distribuito in molte regioni. Grazie all'elevata disponibilità (HA) integrata, Azure NetApp Files protegge i tuoi dati dalla maggior parte delle interruzioni e ti offre un SLA leader del settore di "99,99%" tempo di attività.

Prima dell'introduzione della funzionalità di datastore Azure NetApp Files , l'operazione di scalabilità orizzontale per i clienti che pianificavano di ospitare carichi di lavoro ad alta intensità di prestazioni e di archiviazione richiedeva l'espansione sia delle capacità di elaborazione che di archiviazione.

Tieni presente i seguenti aspetti:

- Le configurazioni di cluster non bilanciate non sono consigliate in un cluster SDDC. Pertanto, espandere lo storage significa aggiungere più host, il che implica un TCO maggiore.
- È possibile un solo ambiente vSAN. Pertanto, tutto il traffico di archiviazione compete direttamente con i carichi di lavoro di produzione.
- Non è possibile fornire più livelli di prestazioni per allineare requisiti, prestazioni e costi delle applicazioni.
- È facile raggiungere i limiti della capacità di archiviazione per vSAN basati su host cluster. Integrando le offerte PaaS (Platform-as-a-Service) native di Azure, come Azure NetApp Files , come datastore, i clienti hanno la possibilità di ridimensionare in modo indipendente il proprio storage separatamente e di aggiungere nodi di elaborazione al cluster SDDC solo quando necessario. Questa capacità supera le sfide sopra menzionate.

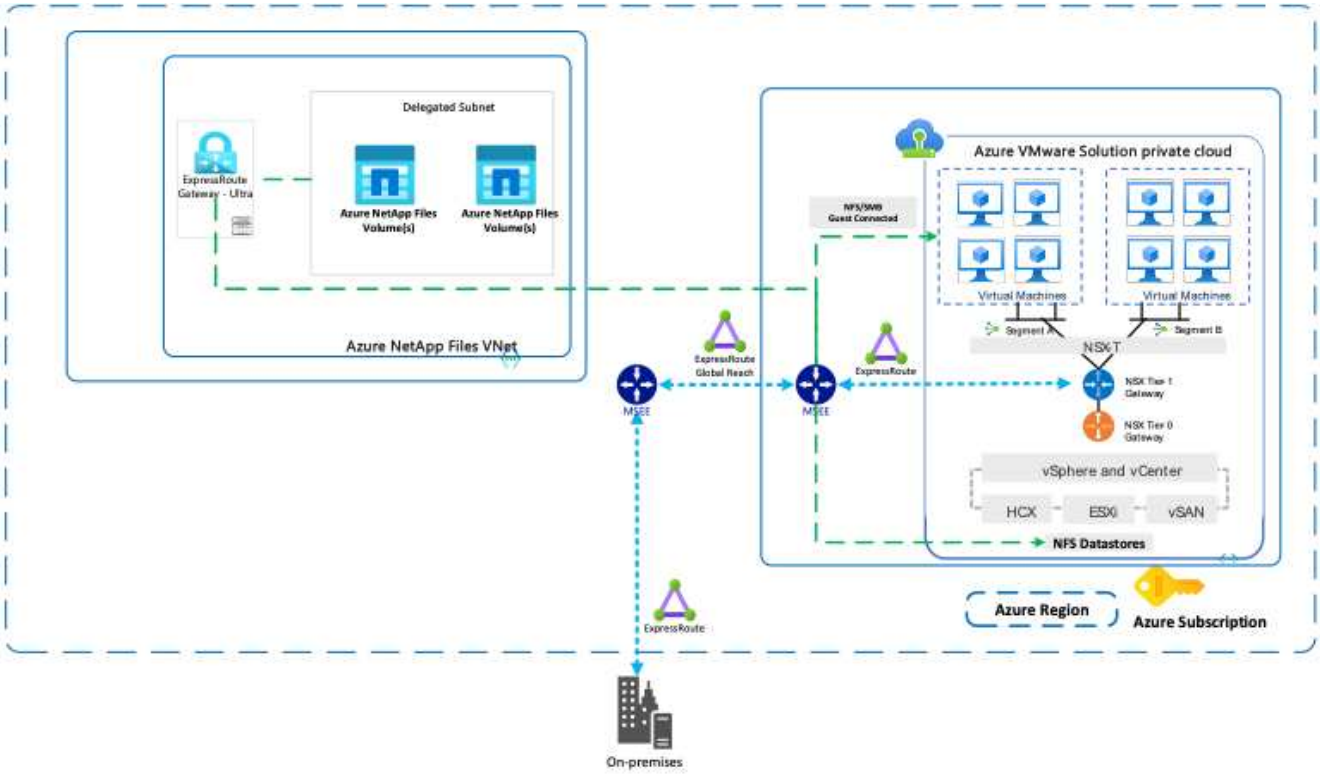
Azure NetApp Files consente inoltre di distribuire più datastore, il che aiuta a imitare un modello di distribuzione locale posizionando le macchine virtuali nel datastore appropriato e assegnando il livello di servizio richiesto per soddisfare i requisiti di prestazioni del carico di lavoro. Grazie alla capacità unica del supporto multiprotocollo, l'archiviazione guest è un'opzione aggiuntiva per carichi di lavoro di database come SQL e Oracle, sfruttando anche la capacità supplementare del datastore NFS per ospitare i VMDK rimanenti. Oltre a ciò, la funzionalità nativa di snapshot consente di eseguire backup rapidi e ripristini granulari.



Contattare Azure e NetApp Solution Architects per la pianificazione e il dimensionamento dello storage e per determinare il numero necessario di host. NetApp consiglia di identificare i requisiti di prestazioni di storage prima di finalizzare il layout del datastore per distribuzioni di test, POC e produzione.

Architettura dettagliata

Da una prospettiva di alto livello, questa architettura descrive come ottenere connettività cloud ibrida e portabilità delle app tra ambienti locali e Azure. Descrive inoltre l'utilizzo di Azure NetApp Files come datastore NFS supplementare e come opzione di archiviazione in-guest per macchine virtuali guest ospitate sulla soluzione Azure VMware.



Dimensionamento

L'aspetto più importante nella migrazione o nel ripristino di emergenza è determinare la dimensione corretta per l'ambiente di destinazione. È molto importante capire quanti nodi sono necessari per eseguire un'operazione di trasferimento da un ambiente locale alla soluzione Azure VMware.

Per il dimensionamento, utilizzare i dati storici dell'ambiente locale tramite RVTools (preferito) o altri strumenti come Live Optics o Azure Migrate. RVTools è uno strumento ideale per acquisire vCPU, vMem, vDisk e tutte le informazioni necessarie, comprese le VM accese o spente, per caratterizzare l'ambiente di destinazione.

Per eseguire RVtools, completare i seguenti passaggi:

1. Scarica e installa RVTools.
2. Esegui RVTools, inserisci le informazioni richieste per connetterti al tuo vCenter Server locale e premi Accedi.
3. Esportare l'inventario in un foglio di calcolo Excel.
4. Modifica il foglio di calcolo e rimuovi dalla scheda vInfo tutte le VM che non sono candidate ideali. Questo approccio fornisce un output chiaro sui requisiti di archiviazione che può essere utilizzato per dimensionare correttamente il cluster Azure VMware SDDC con il numero richiesto di host.

> Le VM guest utilizzate con storage interno devono essere calcolate separatamente; tuttavia, Azure NetApp Files può facilmente coprire la capacità di storage aggiuntiva, mantenendo così basso il TCO complessivo.

Distribuzione e configurazione della soluzione Azure VMware

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

Questa sezione descrive come configurare e gestire AVS per l'utilizzo in combinazione con Azure NetApp Files come archivio dati con archiviazione interna.

Il processo di configurazione può essere suddiviso in tre parti:

- Registra il fornitore di risorse e crea un cloud privato.
- Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente.
- Convalida la connettività di rete e accedi al cloud privato. Fare riferimento a questo"collegamento" per una guida dettagliata al processo di provisioning SDDC della soluzione Azure VMware.

Configurare Azure NetApp Files con Azure VMware Solution

La nuova integrazione tra Azure NetApp Files consente di creare datastore NFS tramite le API/CLI del provider di risorse della soluzione Azure VMware con volumi Azure NetApp Files e di montare i datastore sui cluster desiderati in un cloud privato. Oltre a ospitare i VMDK delle VM e delle app, i volumi di file di Azure NetApp possono anche essere montati dalle VM create nell'ambiente SDDC della soluzione Azure VMware. I volumi possono essere montati sul client Linux e mappati su un client Windows, perché Azure NetApp Files supporta i protocolli Server Message Block (SMB) e Network File System (NFS).

> Per prestazioni ottimali, distribuire Azure NetApp Files nella stessa zona di disponibilità del cloud privato. La collocazione con il percorso rapido Express Route garantisce le migliori prestazioni, con una latenza di rete minima.

Per collegare un volume di file Azure NetApp come datastore VMware di un cloud privato di Azure VMware Solution, assicurarsi che siano soddisfatti i seguenti prerequisiti.

▼ Prerequisiti

1. Utilizzare az login e verificare che l'abbonamento sia registrato nella funzionalità CloudSanExperience nello spazio dei nomi Microsoft.AVS.

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

1. Se non è registrato, registralo.

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

> La registrazione può richiedere circa 15 minuti.

1. Per verificare lo stato della registrazione, eseguire il seguente comando.

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

1. Se la registrazione rimane bloccata in uno stato intermedio per più di 15 minuti, annullare la registrazione e poi registrare nuovamente il flag.

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

1. Verificare che l'abbonamento sia registrato nella funzionalità AnfDatastoreExperience nello spazio dei nomi Microsoft.AVS.

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

1. Verificare che l'estensione VMware sia installata.

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

1. Se l'estensione è già installata, verificare che la versione sia 3.0.0. Se è installata una versione precedente, aggiornare l'estensione.

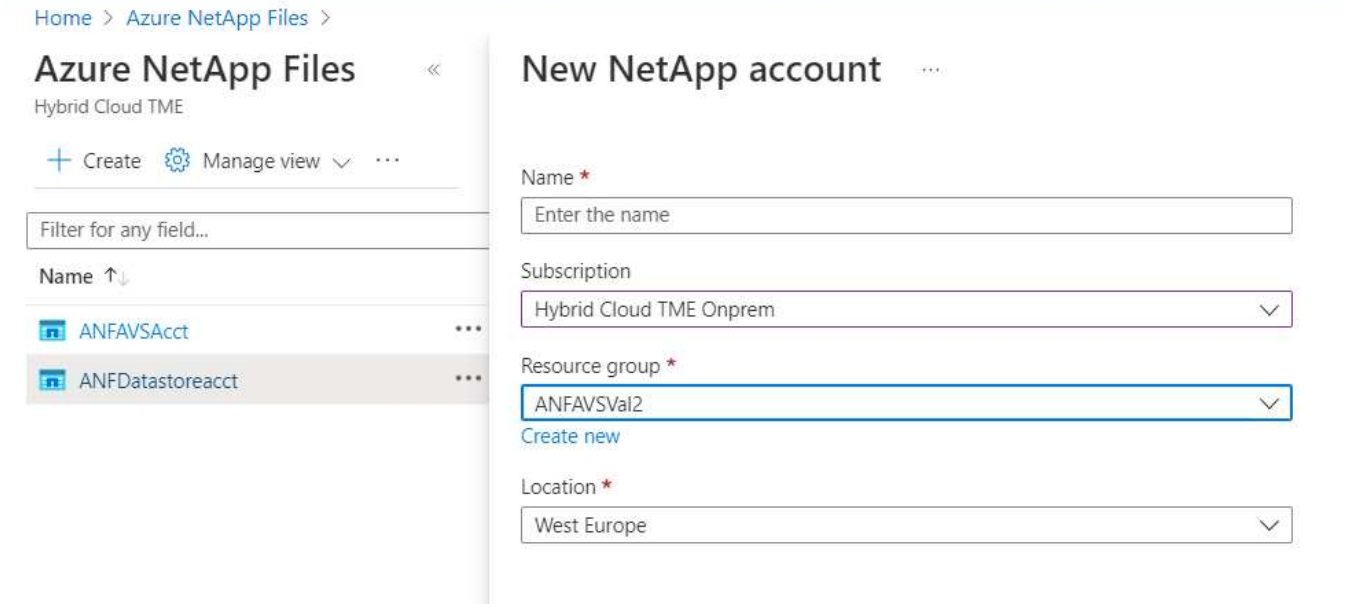
```
az extension update --name vmware
```

1. Se l'estensione non è già installata, installala.

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

▼ Creare e montare volumi Azure NetApp Files

1. Accedi al portale di Azure e accedi ad Azure NetApp Files. Verificare l'accesso al servizio Azure NetApp Files e registrare il provider di risorse Azure NetApp Files utilizzando `az provider register --namespace Microsoft.NetApp –wait` comando. Dopo la registrazione, crea un account NetApp . Fare riferimento a questo "collegamento" per i passaggi dettagliati.



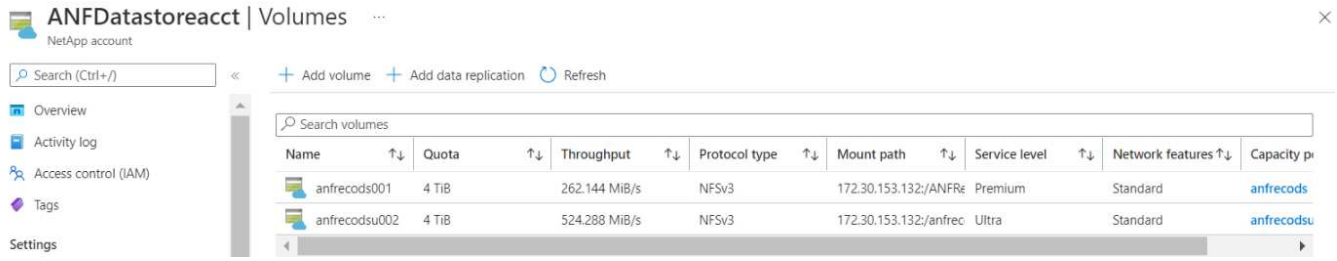
1. Dopo aver creato un account NetApp , impostare i pool di capacità con il livello di servizio e le dimensioni richiesti. Per informazioni dettagliate, fare riferimento a questo "collegamento" .



Punti da ricordare

- NFSv3 è supportato per gli archivi dati su Azure NetApp Files.
- Utilizzare il livello Premium o standard per carichi di lavoro con capacità limitata e il livello Ultra per carichi di lavoro con prestazioni limitate, ove necessario, integrando al contempo l'archiviazione vSAN predefinita.

1. Configurare una subnet delegata per Azure NetApp Files e specificare questa subnet durante la creazione dei volumi. Per i passaggi dettagliati per creare una subnet delegata, fare riferimento a questo "collegamento" .
2. Aggiungere un volume NFS per il datastore utilizzando la lama Volumi sotto la lama Pool di capacità.



Per informazioni sulle prestazioni del volume Azure NetApp Files in base alle dimensioni o alla quota,

vedere"Considerazioni sulle prestazioni per Azure NetApp Files" .

▼ **Aggiungi il datastore dei file Azure NetApp al cloud privato**

Il volume Azure NetApp Files può essere collegato al cloud privato tramite il portale di Azure. Segui questo"collegamento da Microsoft" per un approccio passo passo all'utilizzo del portale di Azure per montare un archivio dati di file Azure NetApp .

Per aggiungere un datastore di file Azure NetApp a un cloud privato, completare i seguenti passaggi:

1. Dopo aver registrato le funzionalità richieste, collegare un datastore NFS al cluster cloud privato della soluzione Azure VMware eseguendo il comando appropriato.
2. Creare un datastore utilizzando un volume ANF esistente nel cluster cloud privato della soluzione Azure VMware.

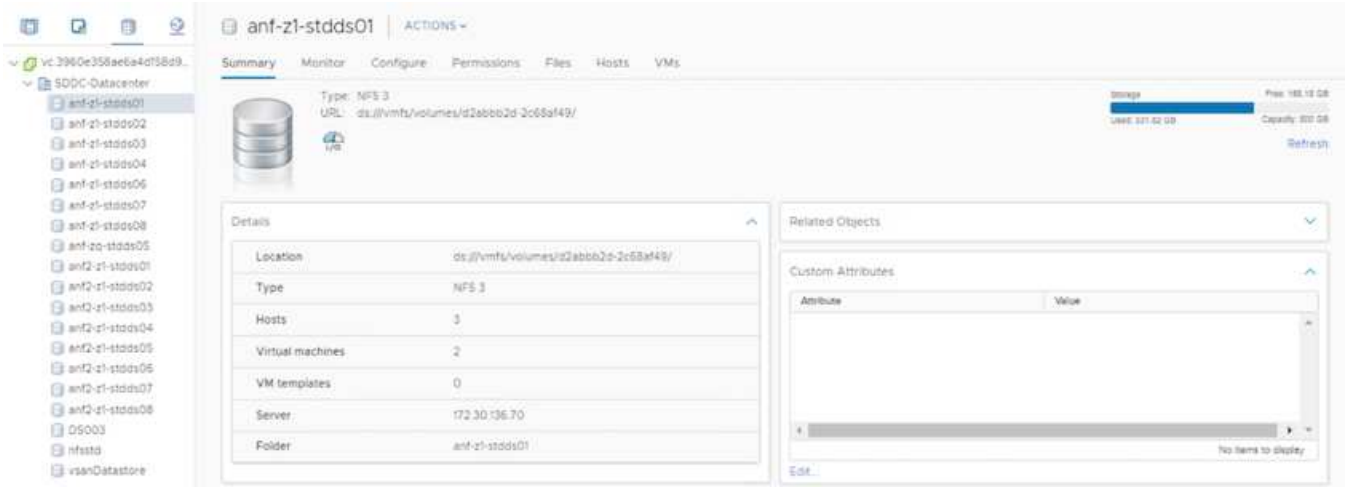
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002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

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

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

917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "Riuscito", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

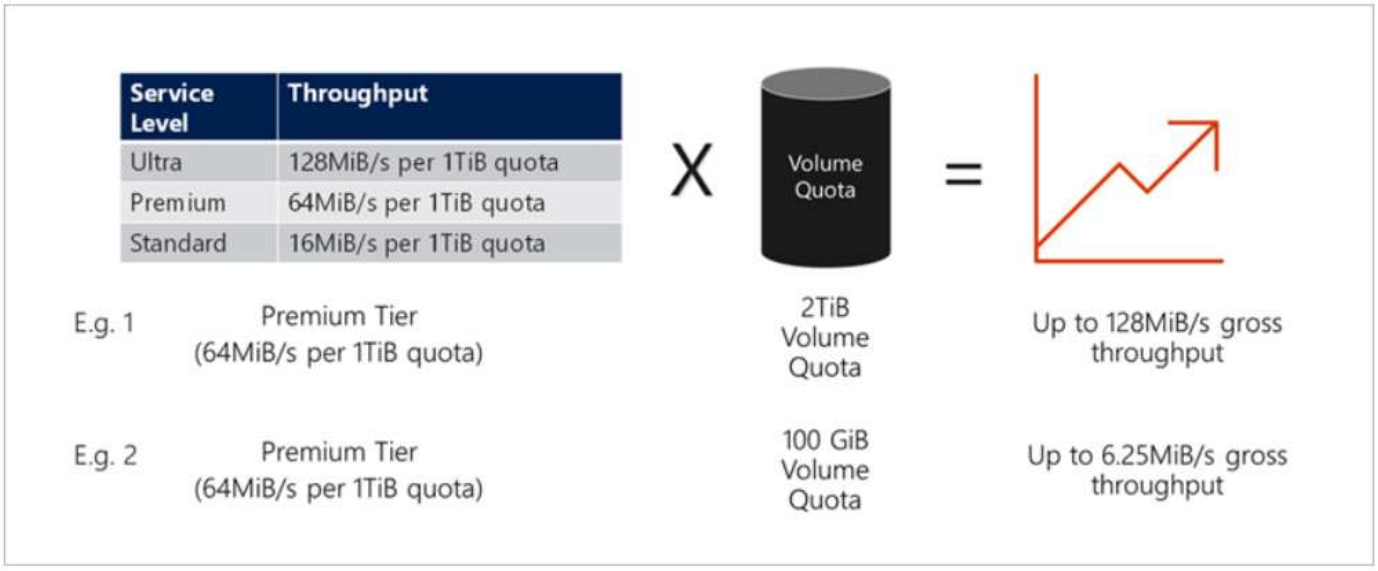
1. Una volta stabilita la connettività necessaria, i volumi vengono montati come datastore.



Ottimizzazione delle dimensioni e delle prestazioni

Azure NetApp Files supporta tre livelli di servizio: Standard (16 MBps per terabyte), Premium (64 MBps per terabyte) e Ultra (128 MBps per terabyte). Per ottenere prestazioni ottimali del carico di lavoro del database è importante predisporre il volume della giusta dimensione. Con Azure NetApp Files, le prestazioni del volume e il limite di velocità effettiva vengono determinati in base ai seguenti fattori:

- Il livello di servizio del pool di capacità a cui appartiene il volume
- La quota assegnata al volume
- Il tipo di qualità del servizio (QoS) (automatico o manuale) del pool di capacità



Per ulteriori informazioni, vedere "Livelli di servizio per Azure NetApp Files" .

Fare riferimento a questo"collegamento da Microsoft" per benchmark dettagliati delle prestazioni che possono essere utilizzati durante un esercizio di dimensionamento.

Punti da ricordare
• Per ottenere capacità e prestazioni ottimali, utilizzare il livello Premium o Standard per i volumi del datastore. Se sono richieste prestazioni elevate, è possibile utilizzare il livello Ultra. • Per i requisiti di montaggio guest, utilizzare il livello Premium o Ultra e per i requisiti di condivisione file per le VM guest, utilizzare i volumi di livello Standard o Premium.

Considerazioni sulle prestazioni

È importante comprendere che con NFS versione 3 è presente un solo canale attivo per la connessione tra l'host ESXi e una singola destinazione di archiviazione. Ciò significa che, sebbene possano essere disponibili connessioni alternative per il failover, la larghezza di banda per un singolo datastore e l'archiviazione sottostante sono limitate a ciò che una singola connessione può fornire.

Per sfruttare una maggiore larghezza di banda disponibile con i volumi Azure NetApp Files , un host ESXi deve disporre di più connessioni alle destinazioni di archiviazione. Per risolvere questo problema, è possibile configurare più datastore, ognuno dei quali utilizza connessioni separate tra l'host ESXi e lo storage.

Per una larghezza di banda maggiore, come best practice, creare più datastore utilizzando più volumi ANF, creare VMDK e suddividere i volumi logici tra i VMDK.

Fare riferimento a questo"collegamento da Microsoft" per benchmark dettagliati delle prestazioni che possono essere utilizzati durante un esercizio di dimensionamento.

Punti da ricordare
• Per impostazione predefinita, la soluzione Azure VMware consente otto datastore NFS. È possibile aumentare tale valore tramite una richiesta di supporto. • Sfrutta ER Fastpath insieme a Ultra SKU per una maggiore larghezza di banda e una minore latenza. Ulteriori informazioni • Con le funzionalità di rete "Base" nei file di Azure NetApp , la connettività dalla soluzione Azure VMware è vincolata dalla larghezza di banda del circuito ExpressRoute e del gateway ExpressRoute. • Per i volumi Azure NetApp Files con funzionalità di rete "Standard", è supportato ExpressRoute FastPath. Se abilitato, FastPath invia il traffico di rete direttamente ai volumi Azure NetApp Files , bypassando il gateway e garantendo una maggiore larghezza di banda e una minore latenza.

Aumento delle dimensioni del datastore

La riorganizzazione del volume e le modifiche dinamiche del livello di servizio sono completamente trasparenti per l'SDDC. In Azure NetApp Files, queste funzionalità garantiscono ottimizzazioni continue di prestazioni, capacità e costi. Aumentare le dimensioni dei datastore NFS ridimensionando il volume dal portale di Azure o utilizzando l'interfaccia della riga di comando. Al termine, accedi a vCenter, vai alla scheda del datastore, fai clic con il pulsante destro del mouse sul datastore appropriato e seleziona Aggiorna informazioni sulla capacità. Questo approccio può essere utilizzato per aumentare la capacità del datastore e per aumentarne le prestazioni in modo dinamico, senza tempi di inattività. Questo processo è inoltre completamente trasparente per le applicazioni.

Punti da ricordare
• La riorganizzazione del volume e la capacità di livello di servizio dinamico consentono di ottimizzare i costi dimensionandoli per carichi di lavoro stabili, evitando così l'eccesso di risorse. • VAAI non è abilitato.

Carichi di lavoro

▼ **Migrazione**

Uno dei casi d'uso più comuni è la migrazione. Utilizzare VMware HCX o vMotion per spostare le VM in sede. In alternativa, è possibile utilizzare Rivermeadow per migrare le VM nei datastore Azure NetApp Files .

▼ **Protezione dei dati**

Tra i grandi punti di forza dei datastore ANF rientrano il backup delle VM e il loro rapido ripristino. Utilizza le copie snapshot per creare copie rapide della tua VM o del tuo datastore senza compromettere le prestazioni, quindi inviale all'archiviazione di Azure per una protezione dei dati a lungo termine o a un'area secondaria utilizzando la replica tra aree per scopi di disaster recovery. Questo approccio riduce al minimo lo spazio di archiviazione e la larghezza di banda della rete memorizzando solo le informazioni modificate.

Utilizzare copie snapshot Azure NetApp Files per la protezione generale e utilizzare strumenti applicativi per proteggere i dati transazionali, ad esempio SQL Server o Oracle, residenti nelle VM guest. Queste copie Snapshot sono diverse dagli snapshot VMware (di coerenza) e sono adatte per una protezione a lungo termine.



Con i datastore ANF, l'opzione Ripristina su nuovo volume può essere utilizzata per clonare un intero volume di datastore e il volume ripristinato può essere montato come un altro datastore sugli host all'interno di AVS SDDC. Dopo aver montato un datastore, le VM al suo interno possono essere registrate, riconfigurate e personalizzate come se fossero VM clonate singolarmente.

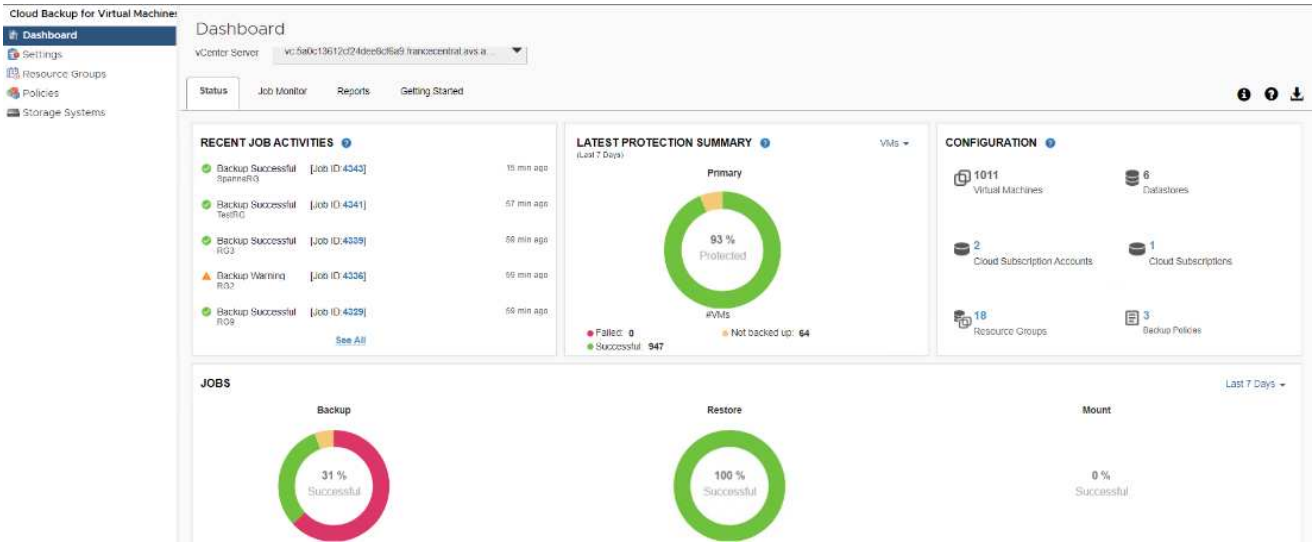
▼ **NetApp Backup and Recovery for Virtual Machines**

NetApp Backup and Recovery for Virtual Machines fornisce una GUI del client web vSphere su vCenter per proteggere le macchine virtuali di Azure VMware Solution e i datastore di Azure NetApp files tramite policy di backup. Queste policy possono definire pianificazione, periodo di conservazione e altre funzionalità. La funzionalità di NetApp Backup and Recovery for Virtual Machine può essere distribuita utilizzando il comando Run.

È possibile installare i criteri di configurazione e protezione completando i seguenti passaggi:

1. Installa NetApp Backup and Recovery for Virtual Machine nel cloud privato Azure VMware Solution usando il comando Run.
2. Aggiungere le credenziali di abbonamento cloud (valore client e segreto), quindi aggiungere un account di abbonamento cloud (account NetApp e gruppo di risorse associato) che contenga le risorse che si desidera proteggere.
3. Creare una o più policy di backup che gestiscano la conservazione, la frequenza e altre impostazioni per i backup dei gruppi di risorse.
4. Crea un contenitore per aggiungere una o più risorse che devono essere protette con criteri di backup.
5. In caso di errore, ripristinare l'intera VM o singoli VMDK specifici nella stessa posizione.

Grazie alla tecnologia Azure NetApp Files Snapshot, i backup e i ripristini sono molto rapidi.



▼ **Ripristino di emergenza con Azure NetApp Files, JetStream DR e Azure VMware Solution**

Il disaster recovery sul cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware). Utilizzando il framework VMware VAIO, i carichi di lavoro VMware locali possono essere replicati nell'archiviazione BLOB di Azure e ripristinati, consentendo una perdita di dati minima o quasi nulla e un RTO prossimo allo zero. JetStream DR può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale ad AVS e in particolare ad Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime nel sito DR e un archivio cloud conveniente. JetStream DR automatizza il ripristino nei datastore ANF tramite Azure Blob Storage. JetStream DR recupera VM indipendenti o gruppi di VM correlate nell'infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino puntuale per la protezione dal ransomware.

"Soluzione DR con ANF, JetStream e AVS" .

Opzioni di archiviazione connessa agli ospiti NetApp per Azure

Azure supporta l'archiviazione NetApp connessa agli ospiti con il servizio nativo Azure NetApp Files (ANF) o con Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure NetApp Files offre gestione e archiviazione dei dati di livello aziendale in Azure, consentendoti di gestire con facilità i tuoi carichi di lavoro e le tue applicazioni. Migra i tuoi carichi di lavoro sul cloud ed eseguili senza sacrificare le prestazioni.

Azure NetApp Files elimina gli ostacoli, così puoi spostare tutte le tue applicazioni basate su file nel cloud. Per la prima volta, non è necessario riprogettare le applicazioni e si ottiene uno storage persistente per le applicazioni senza complessità.

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

Azure NetApp Files (ANF) come storage connesso guest

▼ Configurare Azure NetApp Files con Azure VMware Solution (AVS)

Le condivisioni Azure NetApp Files possono essere montate da VM create nell'ambiente SDDC della soluzione Azure VMware. 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.

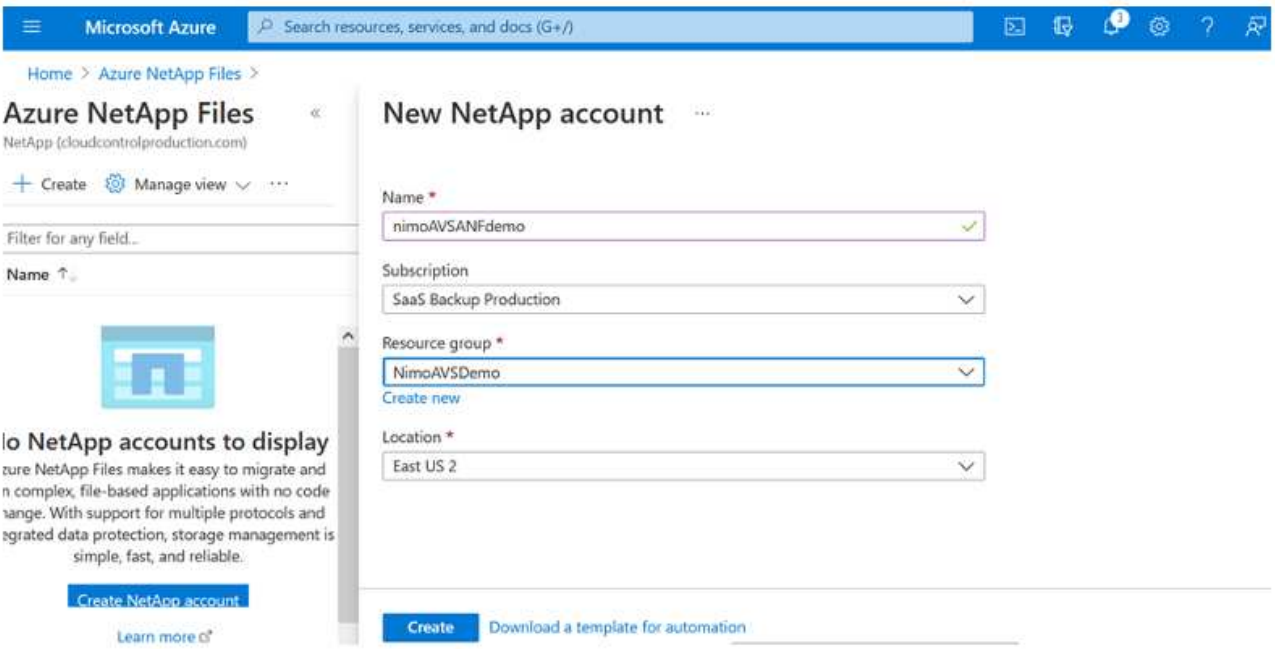
Azure NetApp Files e Azure VMware Solution devono trovarsi nella stessa area di Azure.

▼ Creare e montare volumi Azure NetApp Files

Per creare e montare volumi Azure NetApp Files , completare i passaggi seguenti:

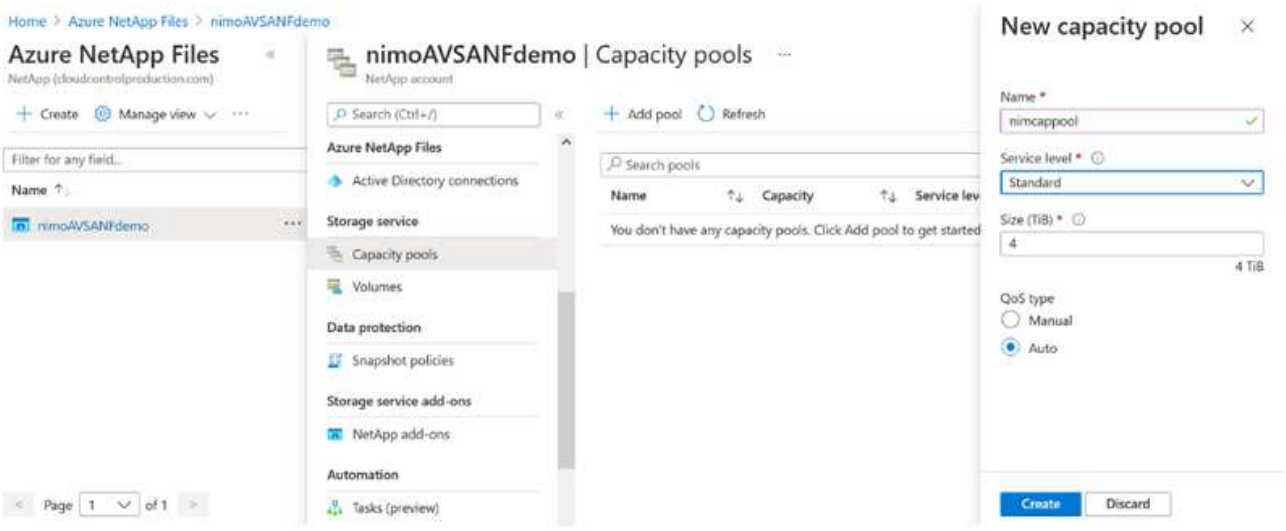
1. Accedi al portale di Azure e accedi ad Azure NetApp Files. Verificare l'accesso al servizio Azure NetApp Files e registrare il provider di risorse Azure NetApp Files utilizzando il comando *az provider register --namespace NetApp –wait*. Una volta completata la registrazione, crea un account NetApp .

   Per i passaggi dettagliati, vedere"Condivisioni Azure NetApp Files" . Questa pagina ti guiderà passo dopo passo attraverso il processo.

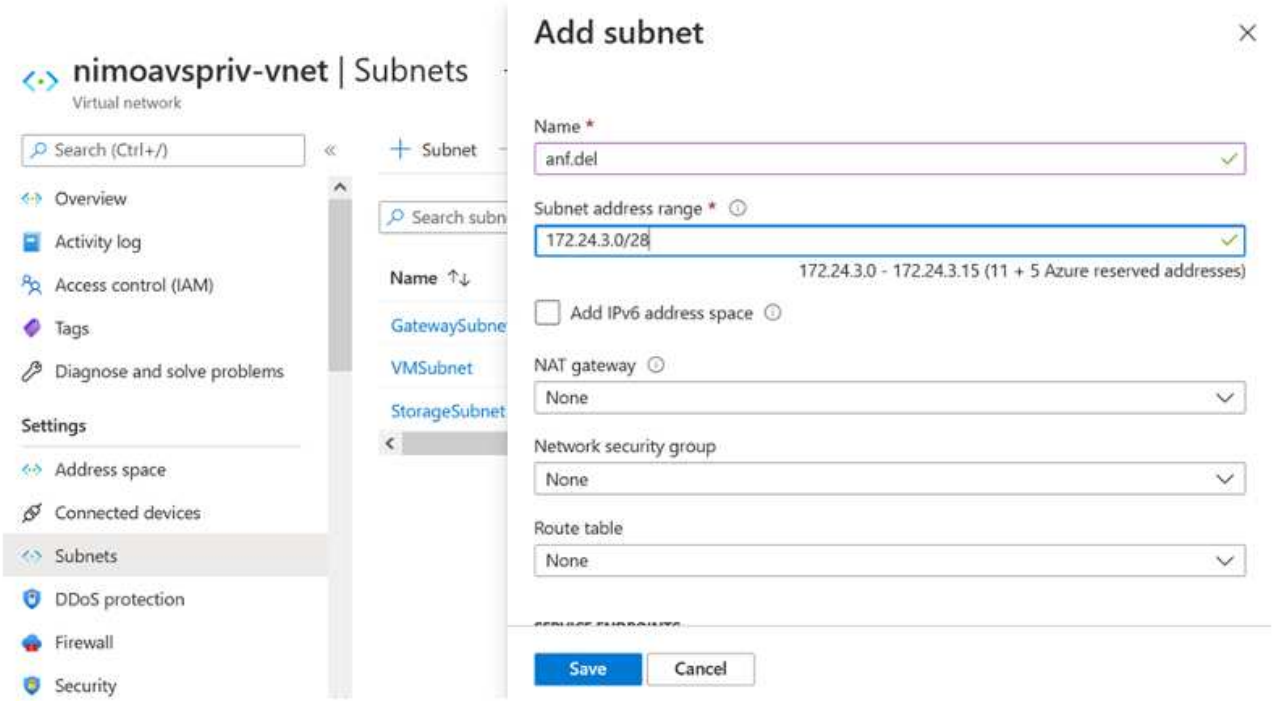


2. Dopo aver creato l'account NetApp , impostare i pool di capacità con il livello di servizio e le dimensioni richiesti.

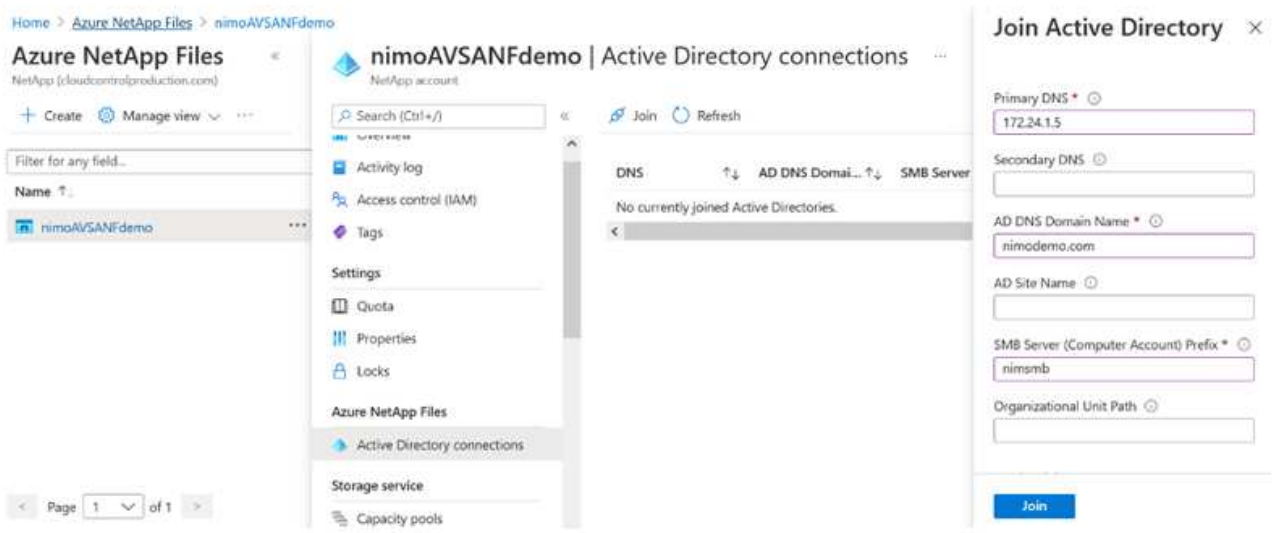
   Per ulteriori informazioni, consultare "Impostare un pool di capacità" .



3. Configurare la subnet delegata per Azure NetApp Files e specificare questa subnet durante la creazione dei volumi. Per i passaggi dettagliati per creare una subnet delegata, vedere"Delegare una subnet ad Azure NetApp Files" .

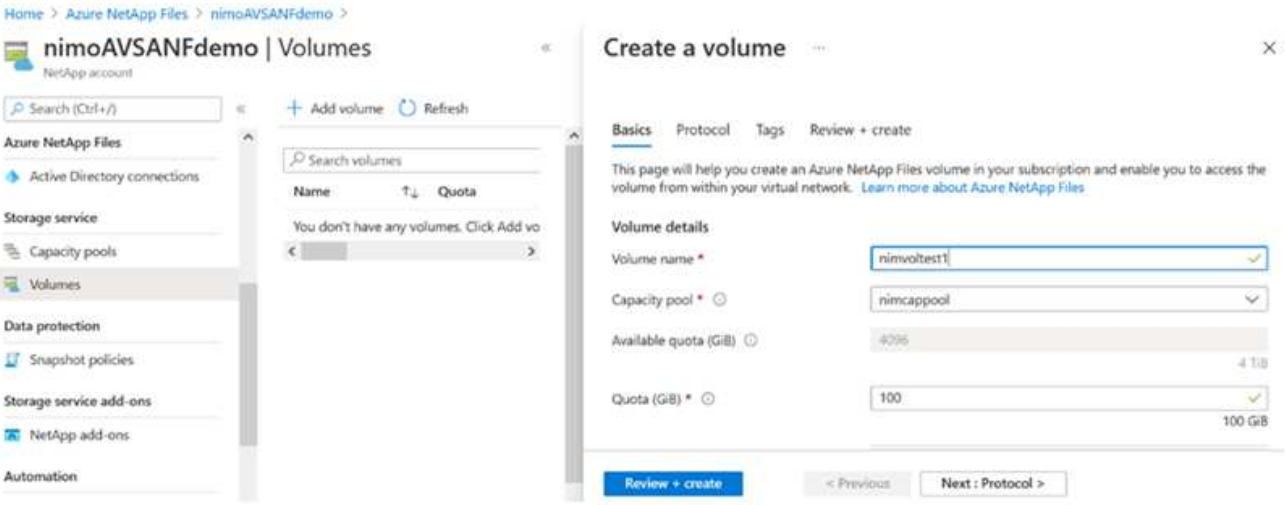


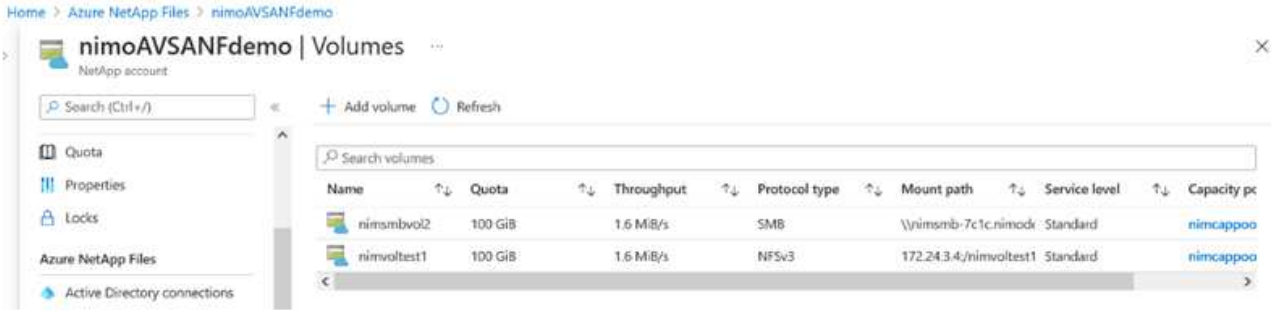
4. Aggiungere un volume SMB utilizzando la lama Volumi sotto la lama Pool di capacità. Assicurarsi che il connettore Active Directory sia configurato prima di creare il volume SMB.



5. Fare clic su Revisiona + Crea per creare il volume SMB.

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

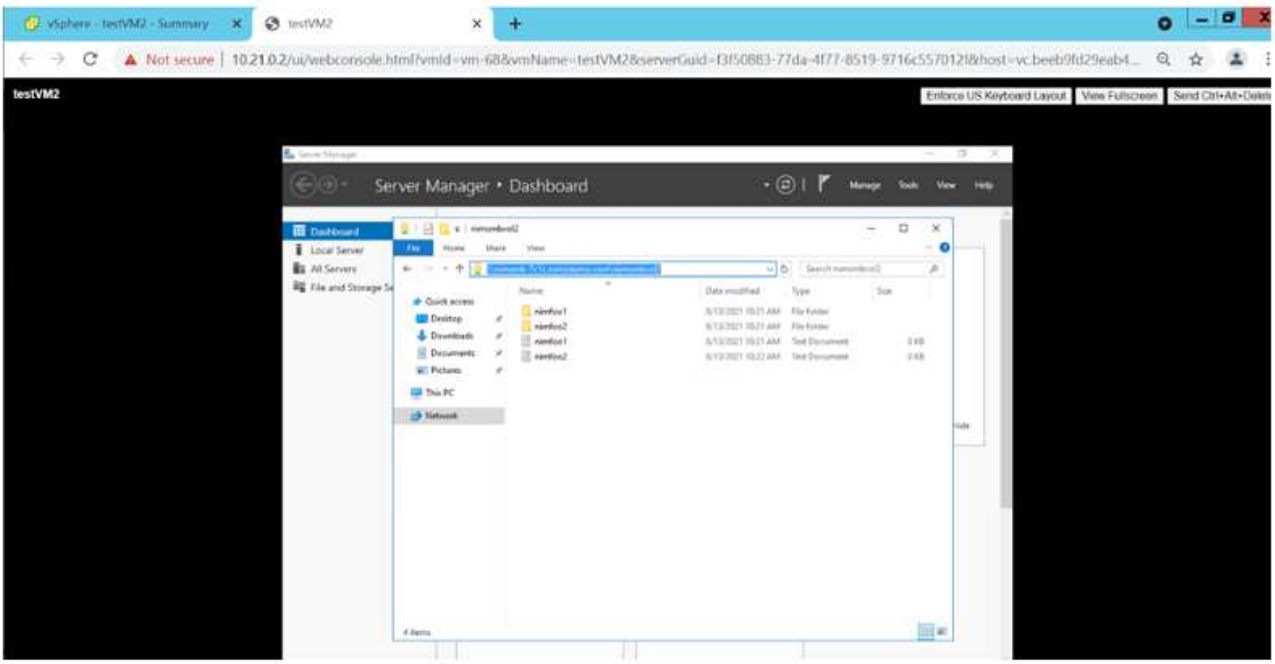


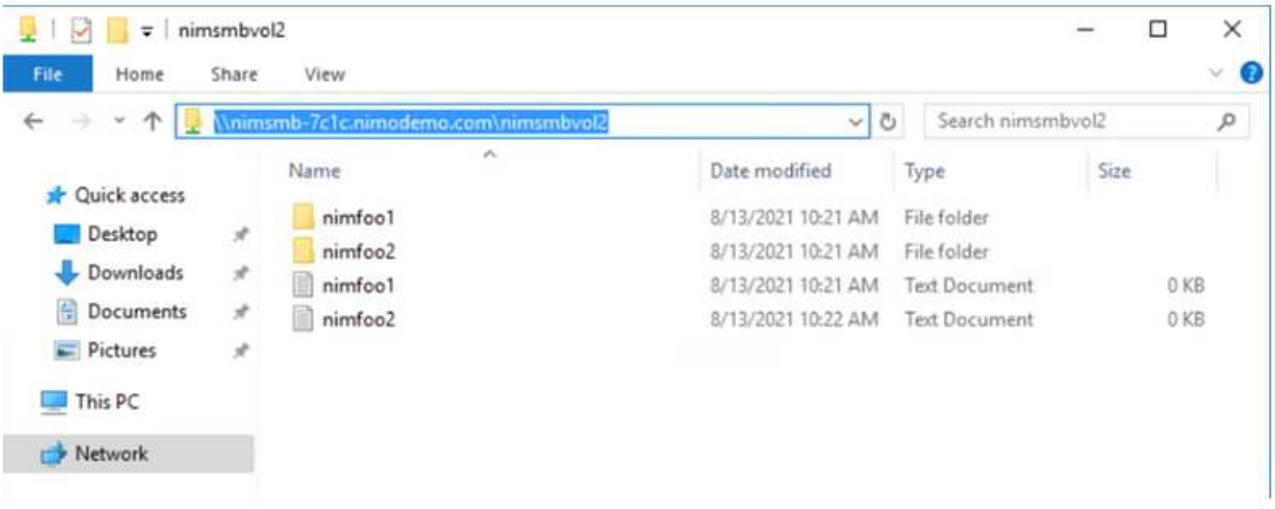


Per ulteriori informazioni sulle prestazioni del volume Azure NetApp Files in base alle dimensioni o alla quota, vedere"Considerazioni sulle prestazioni per Azure NetApp Files" .

6. Una volta stabilita la connettività, il volume può essere montato e utilizzato per i dati dell'applicazione.

   Per fare ciò, dal portale di Azure fare clic sul pannello Volumi, quindi selezionare il volume da montare e accedere alle istruzioni di montaggio. Copiare il percorso e utilizzare l'opzione Connetti unità di rete per montare il volume sulla macchina virtuale in esecuzione su Azure VMware Solution SDDC.





7. Per montare volumi NFS su macchine virtuali Linux in esecuzione su Azure VMware Solution SDDC, utilizzare lo stesso processo. Utilizzare la riorganizzazione del volume o la capacità di livello di servizio dinamico per soddisfare le esigenze del carico 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, consultare "Modificare dinamicamente il livello di servizio di un volume" .

Cloud Volumes ONTAP (CVO)

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti

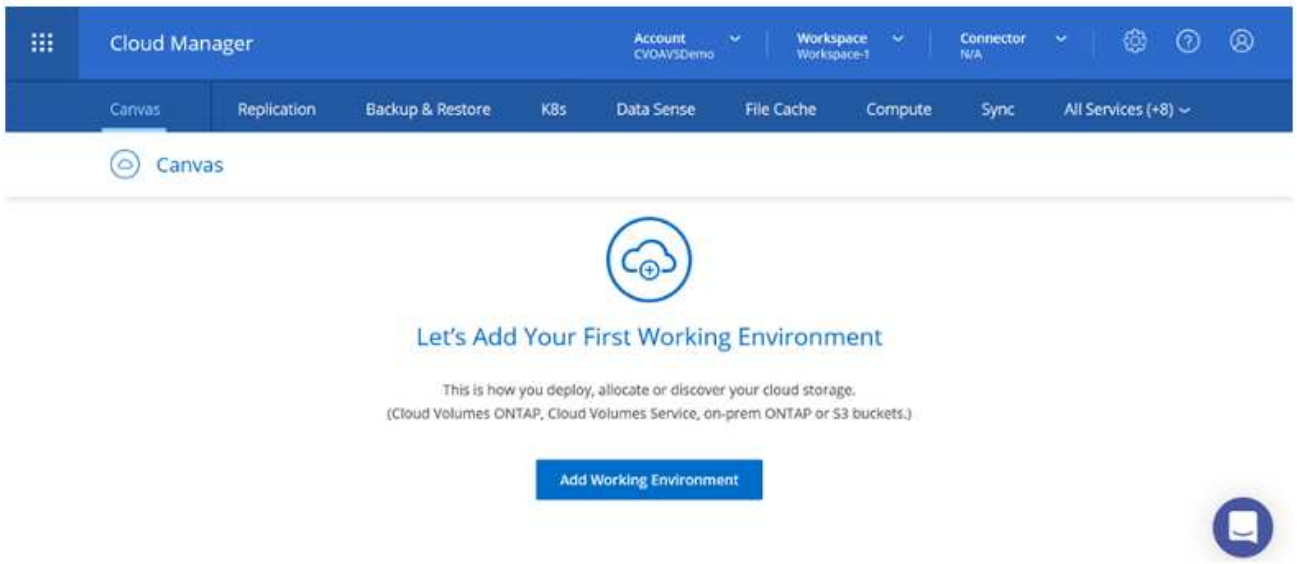
▼ **Distribuisci il nuovo Cloud Volumes ONTAP in Azure**

Le condivisioni Cloud Volumes ONTAP possono essere montate da VM create nell'ambiente SDDC di Azure VMware Solution. I volumi possono essere montati anche sul client Linux e sul client Windows perché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

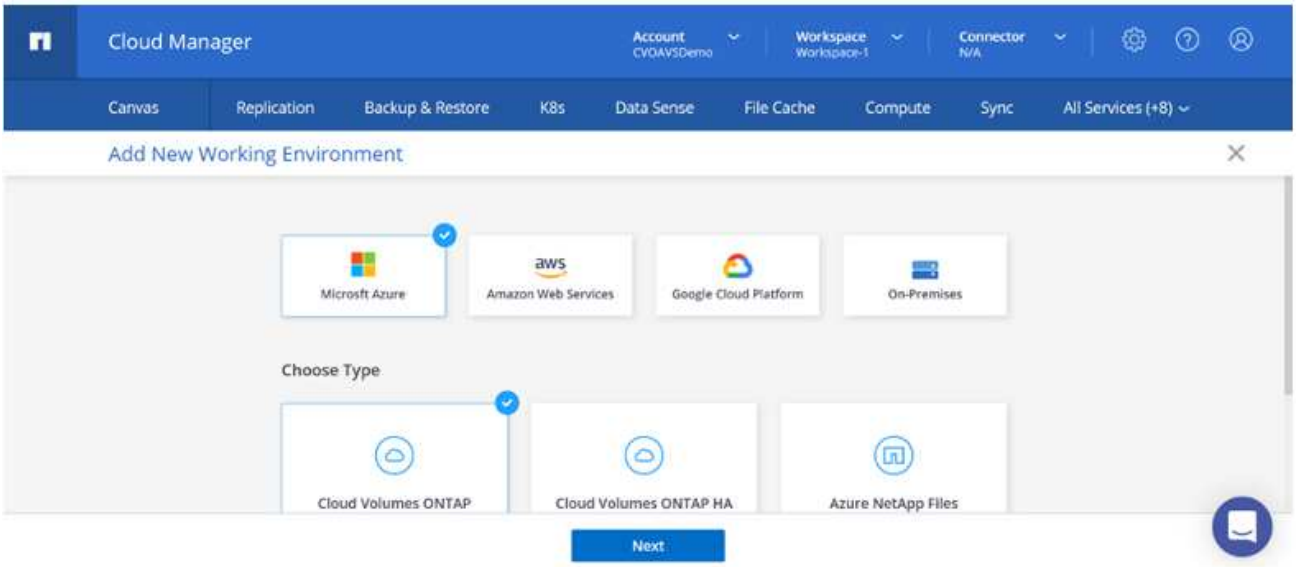
Per replicare volumi da un ambiente locale al cloud per scopi di ripristino di emergenza o migrazione, stabilire la connettività di rete ad Azure, utilizzando una VPN da sito a sito o ExpressRoute. La replica dei dati da locale a Cloud Volumes ONTAP esula dall'ambito del presente documento. Per replicare i dati tra i sistemi locali e Cloud Volumes ONTAP , vedere"Impostazione della replica dei dati tra i sistemi" .

Usa "Dimensionatore Cloud Volumes ONTAP" per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Monitora anche le prestazioni on-premises da usare come input nello strumento di dimensionamento di Cloud Volumes ONTAP.

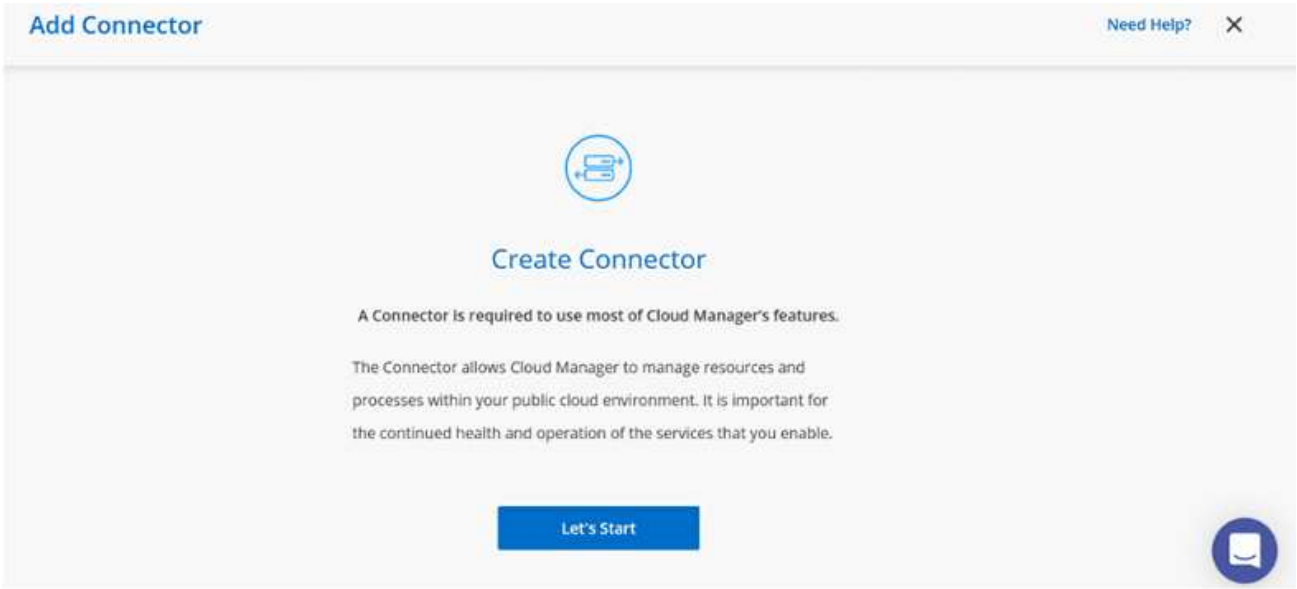
1. Accedi a NetApp Cloud Central: verrà visualizzata la schermata Fabric View. Individua la scheda Cloud Volumes ONTAP e seleziona Vai a Cloud Manager. Dopo aver effettuato l'accesso, verrà visualizzata la schermata Canvas.



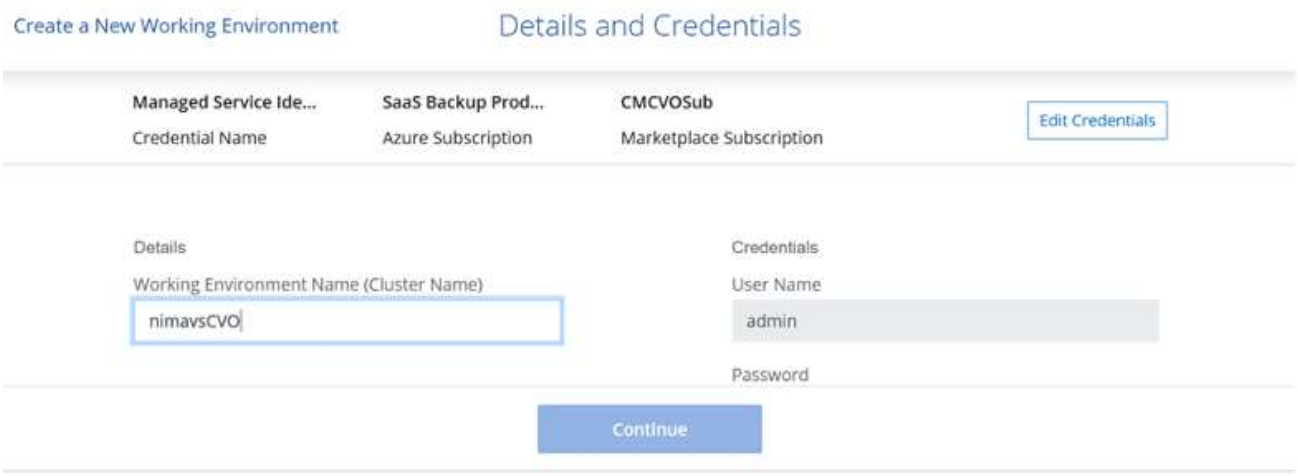
2. Nella home page di Cloud Manager, fare clic su Aggiungi un ambiente di lavoro, quindi selezionare Microsoft Azure come cloud e il tipo di configurazione del sistema.



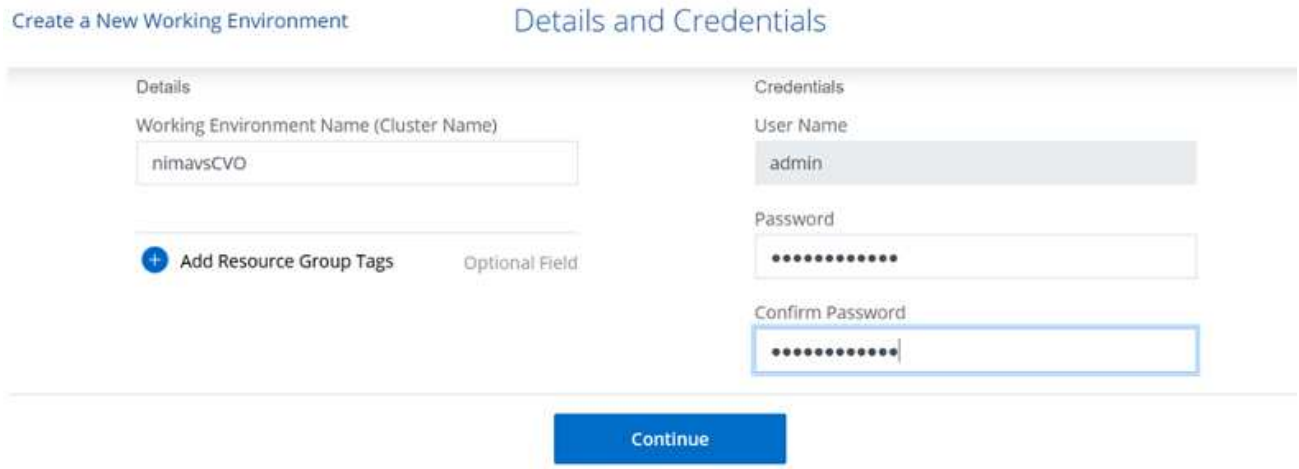
3. Quando si crea il primo ambiente di lavoro Cloud Volumes ONTAP , Cloud Manager richiede di distribuire un connettore.



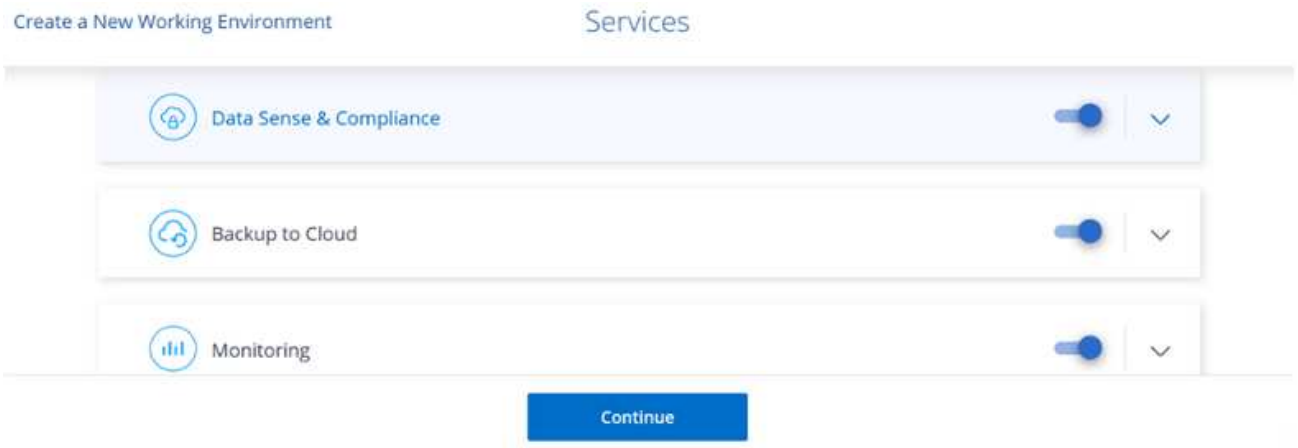
4. Dopo aver creato il connettore, aggiornare i campi Dettagli e Credenziali.



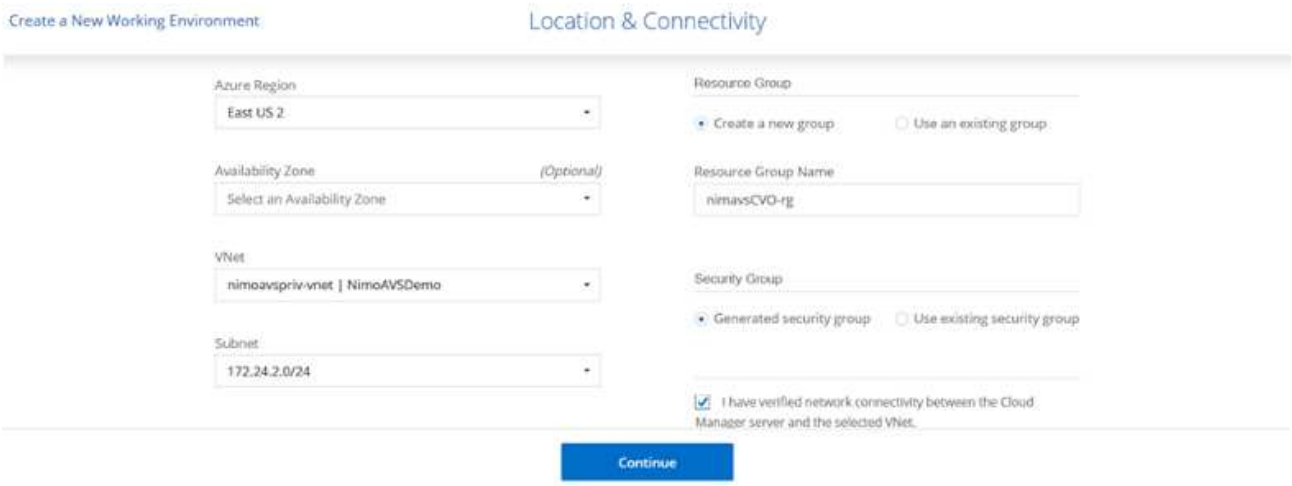
5. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Aggiungere i tag del gruppo di risorse per l'ambiente Azure come parametro facoltativo. Una volta terminato, fare clic su Continua.



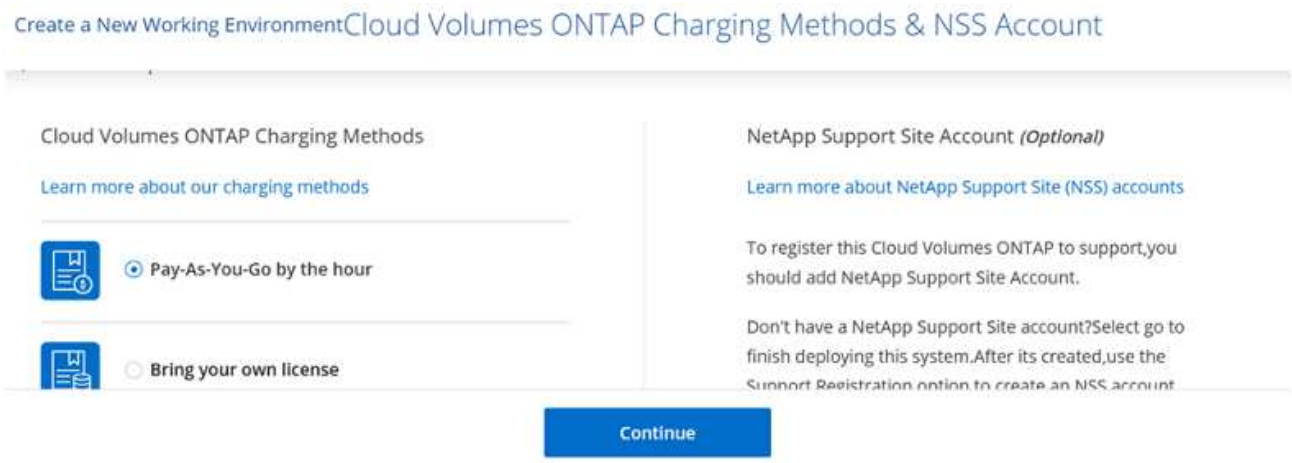
6. Seleziona i servizi aggiuntivi per la distribuzione di Cloud Volumes ONTAP, inclusi NetApp Data Classification, NetApp Backup and Recovery e Data Infrastructure Insights. Seleziona i servizi, quindi fai clic su Continue.



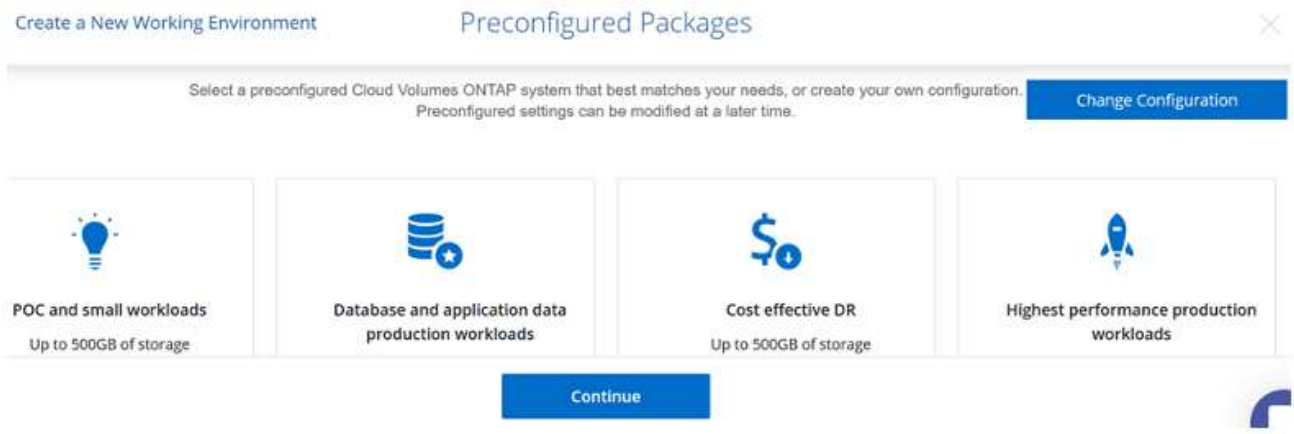
7. Configurare la posizione e la connettività di Azure. Selezionare la regione di Azure, il gruppo di risorse, la rete virtuale e la subnet da utilizzare.



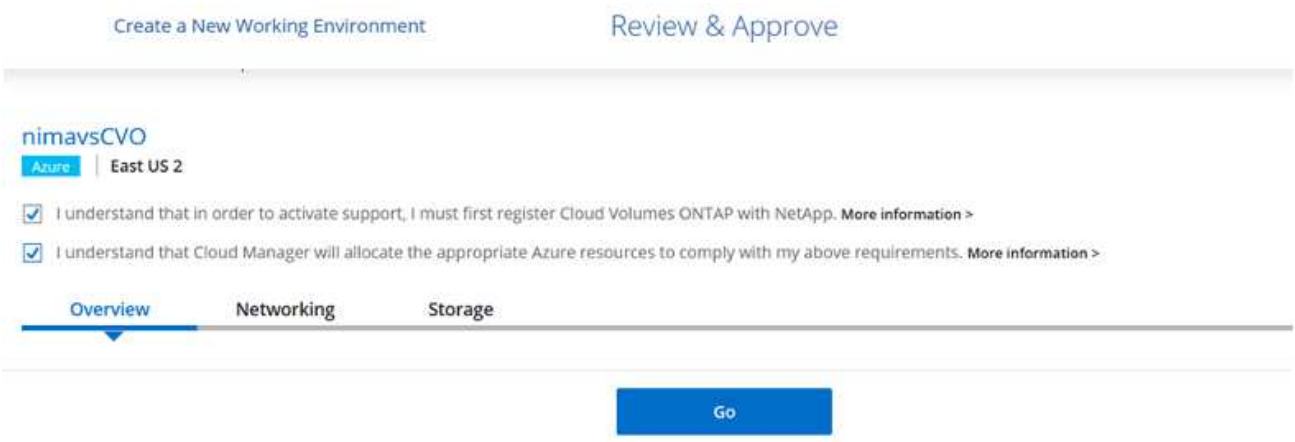
8. Selezionare l'opzione di licenza: Pay-As-You-Go o BYOL per utilizzare la licenza esistente. In questo esempio viene utilizzata l'opzione Pay-As-You-Go.



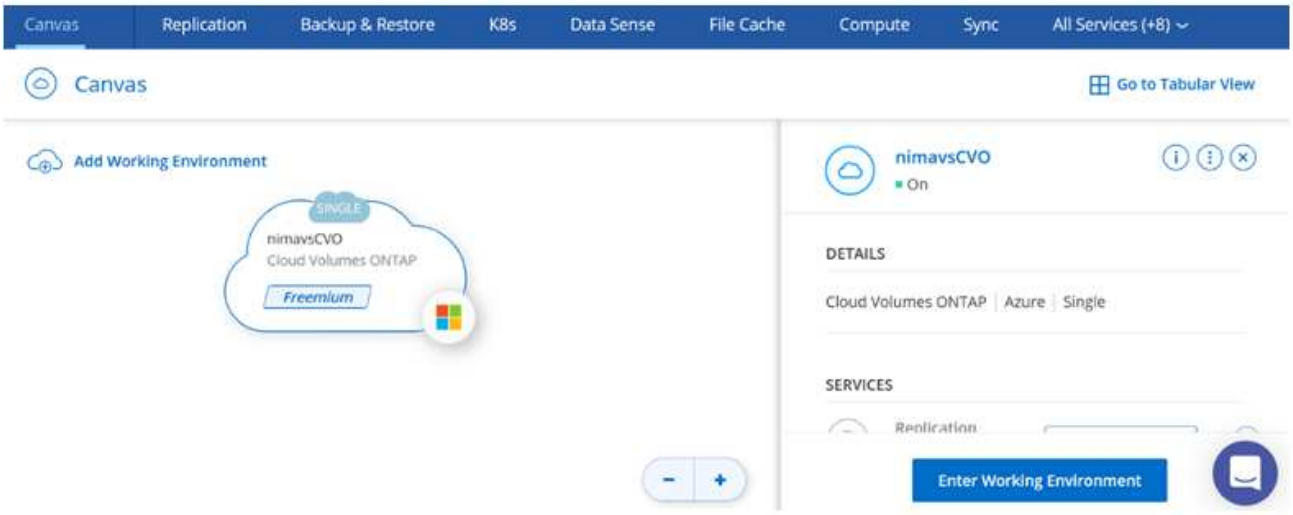
9. Scegli tra diversi pacchetti preconfigurati disponibili per i vari tipi di carichi di lavoro.



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

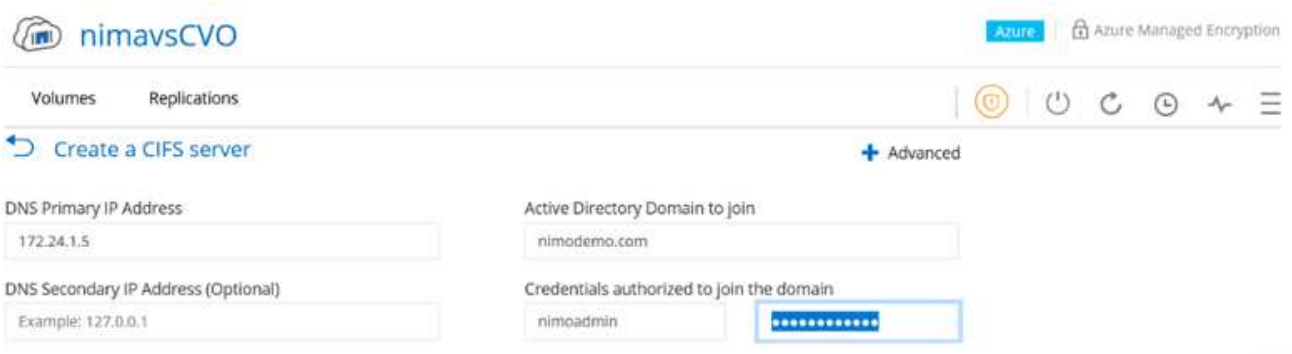


11. Dopo aver eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.



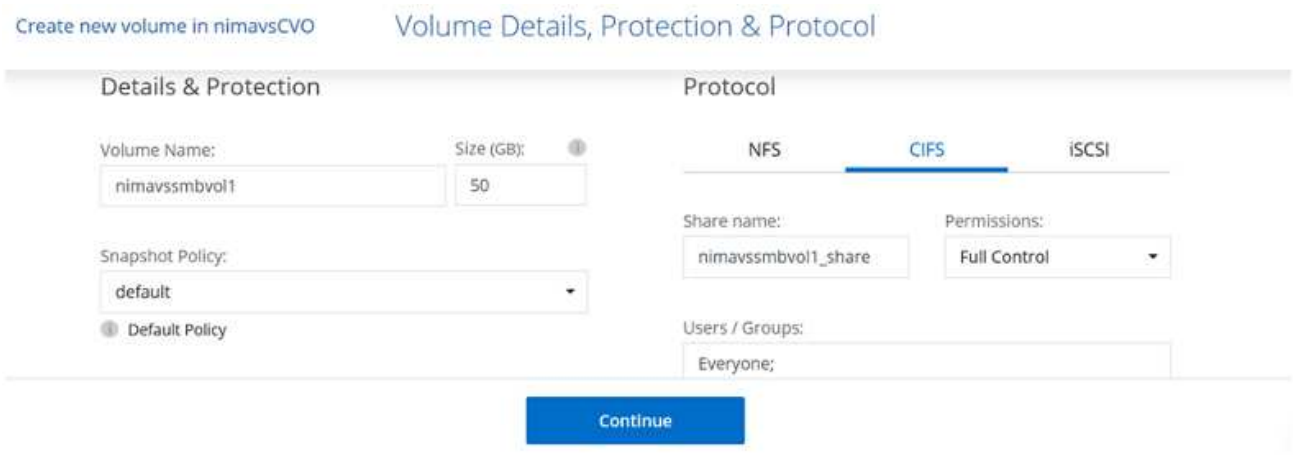
▼ **Configurazioni aggiuntive per volumi SMB**

1. Una volta che l'ambiente di lavoro è pronto, 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.

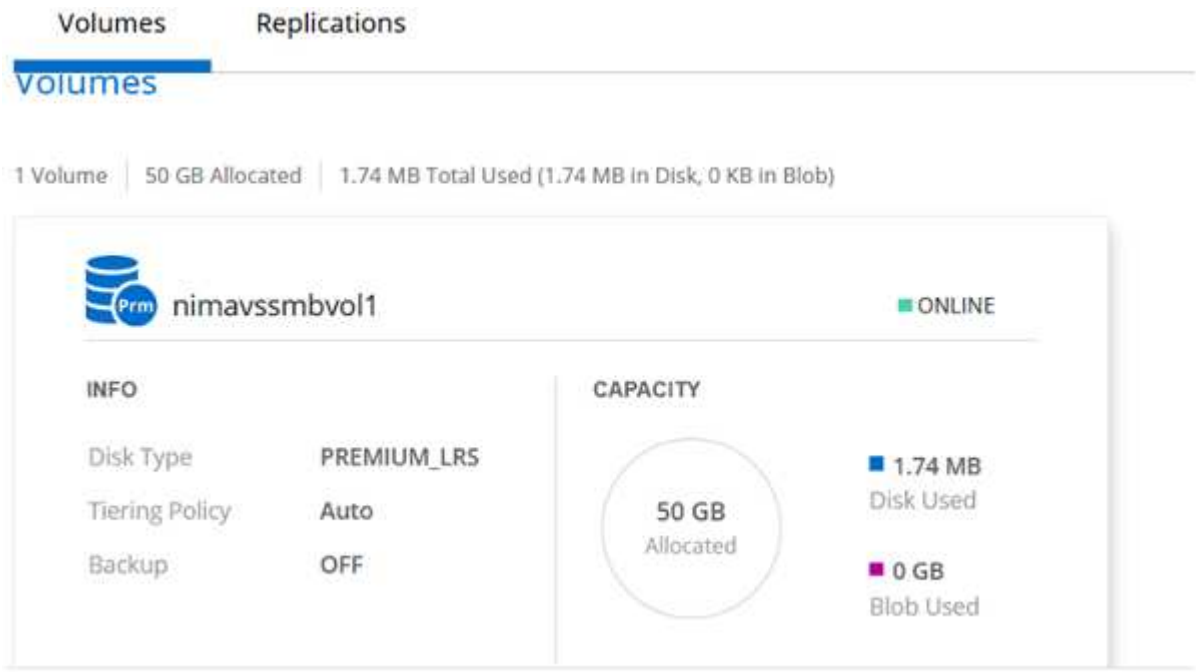


2. La creazione del volume SMB è un processo semplice. Selezionare l'istanza CVO per creare il volume e fare clic sull'opzione Crea volume. Scegli la dimensione appropriata e il gestore cloud sceglierà l'aggregato contenente oppure utilizzerà un meccanismo di allocazione avanzato per posizionarlo su un

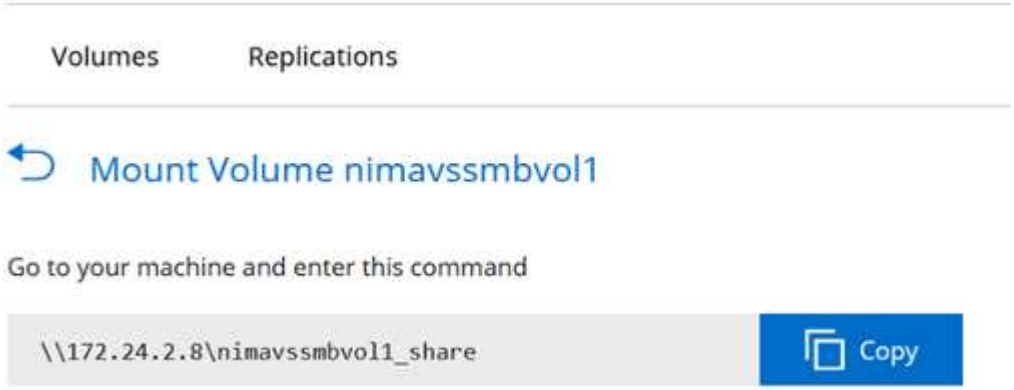
aggregato specifico. Per questa demo, è stato selezionato SMB come protocollo.

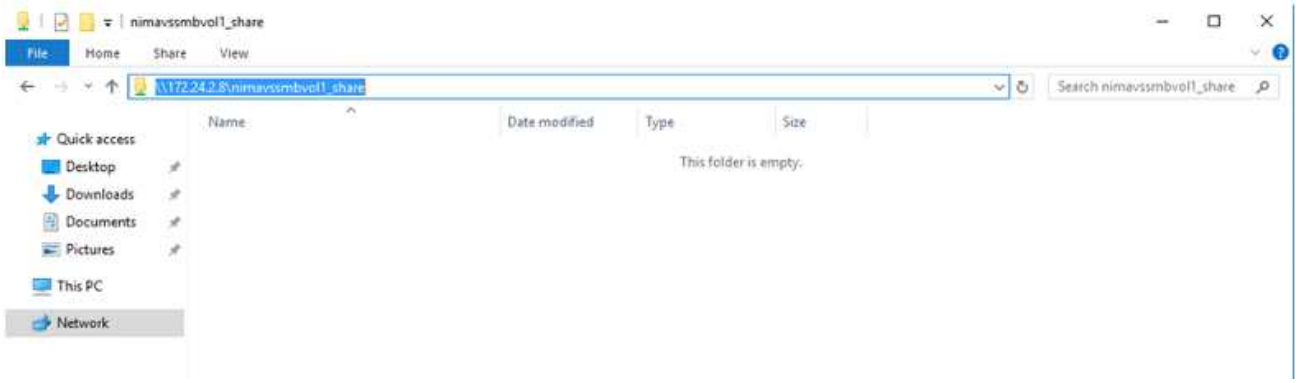


3. Dopo aver eseguito il provisioning, il volume sarà disponibile nel riquadro Volumi. Poiché è stata predisposta una condivisione CIFS, concedere agli utenti o ai gruppi l'autorizzazione per accedere ai file e alle cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file. Questo passaggio non è necessario se il volume viene replicato da un ambiente locale, perché tutte le autorizzazioni per file e cartelle vengono mantenute come parte della replica SnapMirror .



4. Dopo aver creato il volume, utilizzare il comando mount per connettersi alla condivisione dalla macchina virtuale in esecuzione sugli host SDDC di Azure VMware Solution.
5. Copiare il percorso seguente e utilizzare l'opzione Connetti unità di rete per montare il volume sulla macchina virtuale in esecuzione su Azure VMware Solution SDDC.

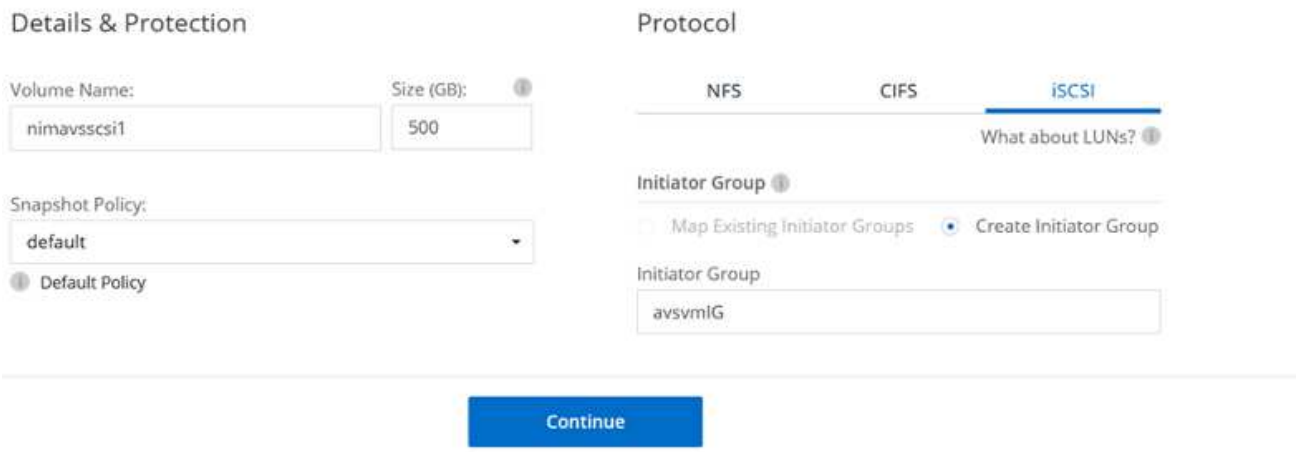




▼ **Collegare la LUN a un host**

Per connettere la LUN a un host, completare i seguenti passaggi:

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Aggiungi volume > Nuovo volume, selezionare iSCSI e fare clic su Crea gruppo iniziatori. Fare clic su Continua.



3. Dopo aver eseguito il provisioning del volume, selezionarlo e fare clic su Target IQN. Per copiare il nome qualificato iSCSI (IQN), fare clic su 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 alla VM ospitata su Azure VMware Solution SDDC.

b. Aprire la finestra di dialogo Proprietà dell'iniziatore iSCSI: Server Manager > Dashboard > Strumenti > Iniziatore iSCSI.

c. Dalla scheda Individuazione, fare clic su Individua portale o Aggiungi portale, quindi immettere l'indirizzo IP della porta di destinazione iSCSI.

d. Dalla scheda Destinazioni, seleziona la destinazione rilevata e poi fai clic su Accedi o Connetti.

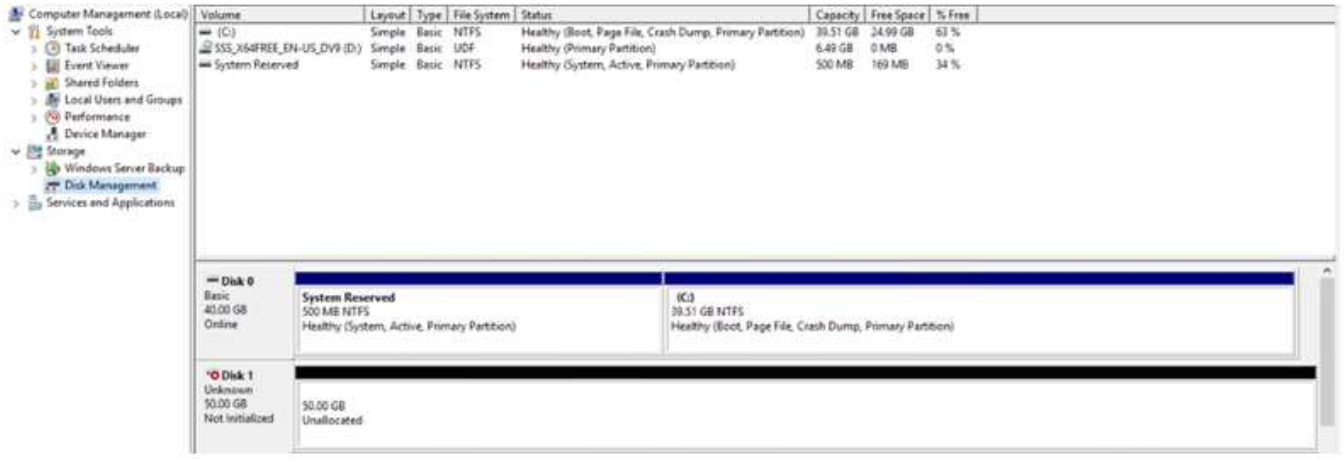
e. Selezionare Abilita multipath, quindi selezionare Ripristina automaticamente questa connessione all'avvio del computer o Aggiungi questa connessione all'elenco delle destinazioni preferite. Fare clic su Avanzate.

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



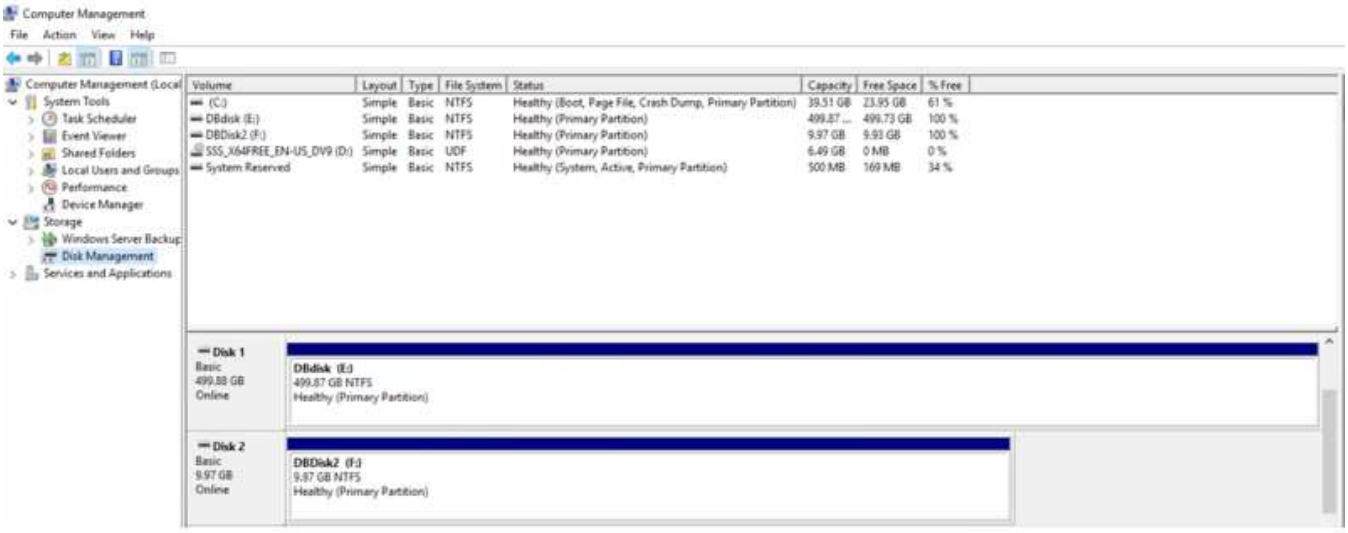
Le LUN sulla macchina virtuale di archiviazione (SVM) vengono visualizzate come dischi sull'host Windows. Tutti i nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Avviare una nuova scansione manuale per rilevare i dischi completando i seguenti passaggi:

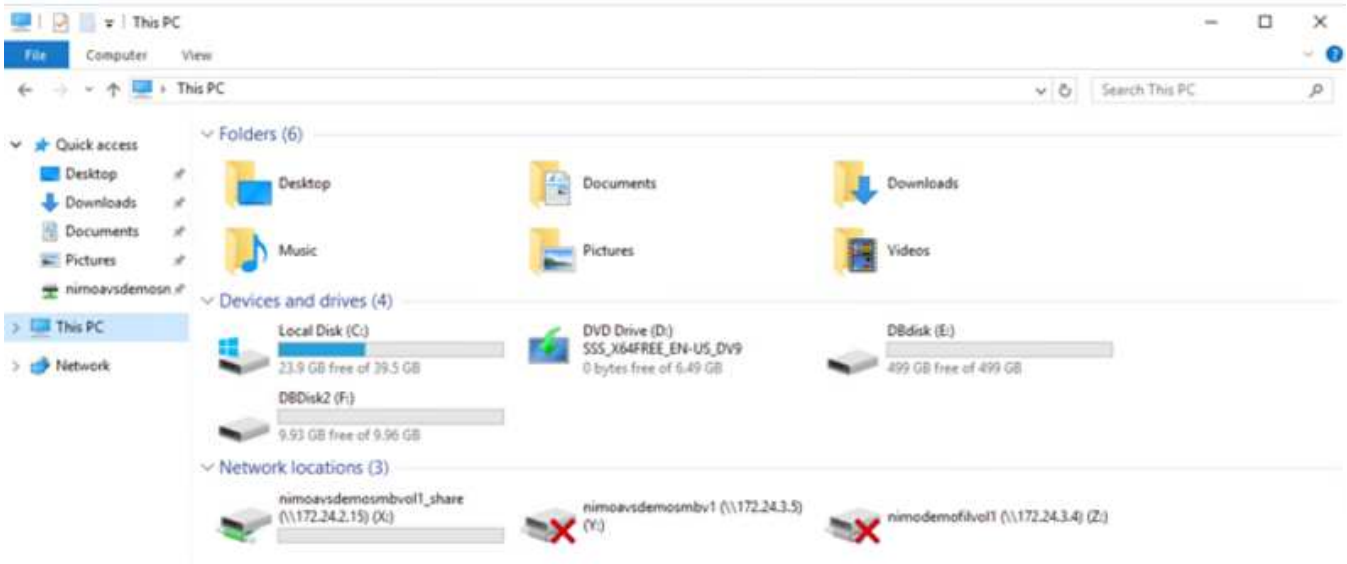
1. Aprire l'utilità Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Archiviazione nell'albero di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Azione > Ripeti analisi dischi.



Quando l'host Windows accede per la prima volta a un nuovo LUN, questo non ha alcuna partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando i seguenti passaggi:

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, l'unità E: è montata





Google Cloud VMware Engine: opzioni per l'utilizzo dello storage NetApp

Lo storage NetApp può essere collegato a Google Cloud Virtualization Engine come storage guest connesso o supplementare.

Google Cloud NetApp Volumes (NetApp Volumes) come datastore NFS supplementare

I clienti che necessitano di capacità di archiviazione aggiuntiva sul proprio ambiente Google Cloud VMware Engine (GCVE) possono utilizzare Google Cloud NetApp Volumes per il montaggio come datastore NFS supplementare. L'archiviazione dei dati su Google Cloud NetApp Volumes consente ai clienti di replicarli tra regioni per proteggersi da eventuali disastri.

Per maggiori informazioni, visitare"Google Cloud NetApp Volumes (NetApp Volumes) come datastore NFS supplementare"

NetApp CVO come storage connesso agli ospiti

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Per maggiori informazioni, visitare"NetApp CVO come storage connesso agli ospiti"

Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti

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

Google Cloud NetApp Volumes e il cloud privato Google Cloud VMware Engine devono trovarsi nella stessa regione.

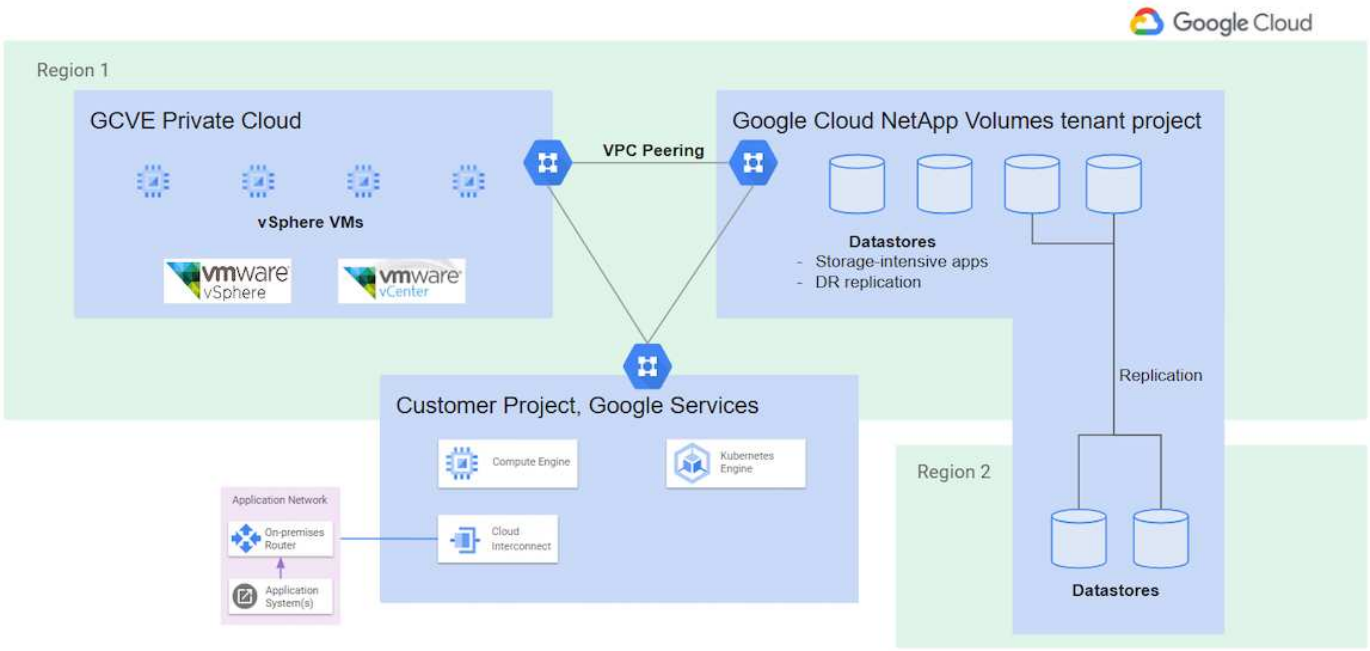
Per maggiori informazioni, visitare"Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti"

Datastore NFS supplementare di Google Cloud VMware Engine con Google Cloud NetApp Volumes

I clienti possono espandere la capacità di archiviazione su Google Cloud VMware Engine utilizzando il datastore supplementare NFS con Google Cloud NetApp Volumes.

Panoramica

I clienti che necessitano di capacità di archiviazione aggiuntiva sul proprio ambiente Google Cloud VMware Engine (GCVE) possono utilizzare Netapp Cloud Volume Service per il montaggio come datastore NFS supplementare. L'archiviazione dei dati su Google Cloud NetApp Volumes consente ai clienti di replicarli tra regioni diverse per proteggersi da eventuali disastri.



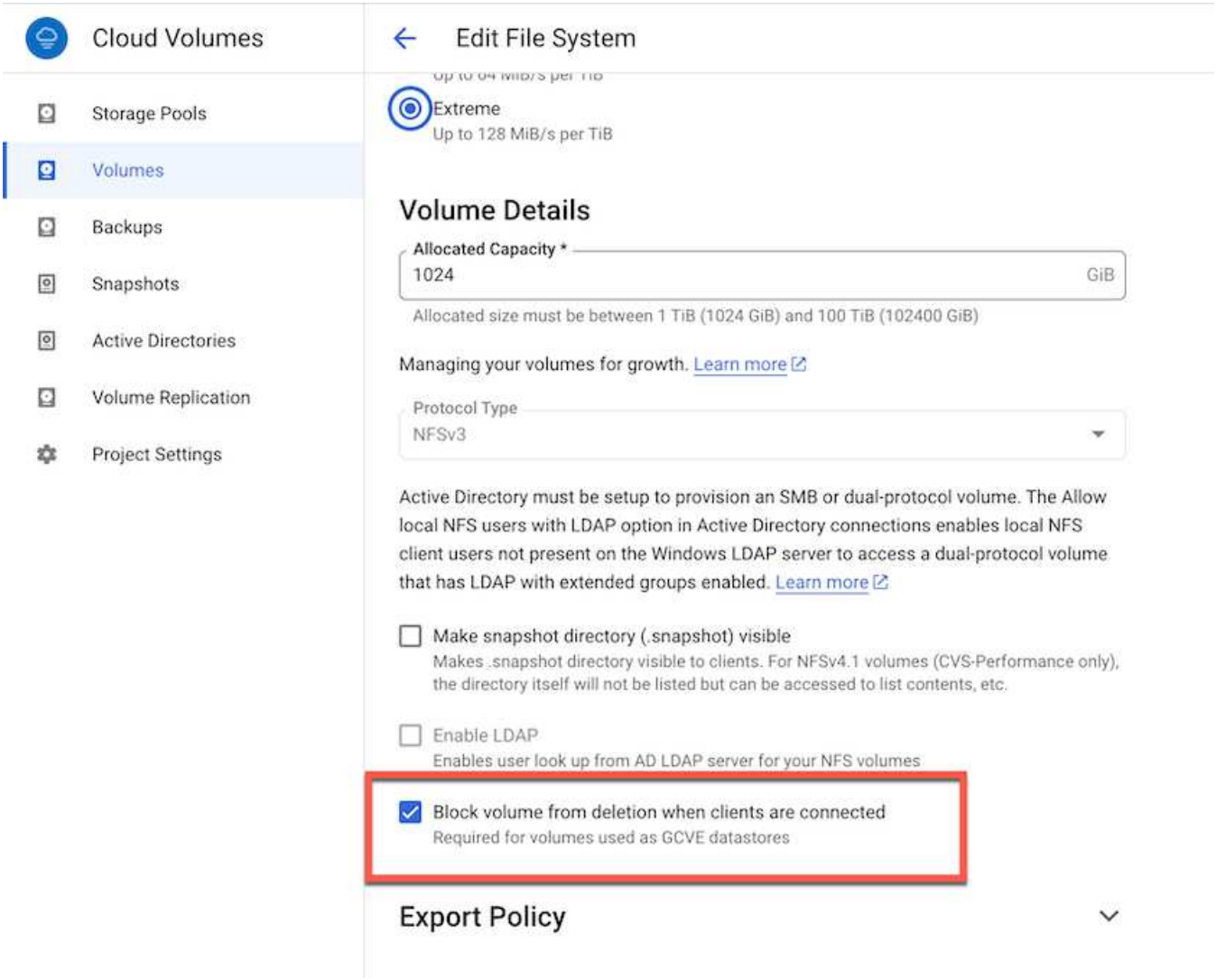
Passaggi di distribuzione per montare il datastore NFS da Google Cloud NetApp Volumes (NetApp Volumes) su GCVE

▼ **Provisioning NetApp Volumes-Performance Volume**

Il volume Google Cloud NetApp Volumes può essere provisionato da "Utilizzo di Google Cloud Console" "Utilizzo di Google Cloud CLI o API"

▼ **Contrassegna il volume NetApp Volumes come non eliminabile**

Per evitare l'eliminazione accidentale del volume mentre la VM è in esecuzione, assicurati che il volume sia contrassegnato come non eliminabile, come mostrato nello screenshot seguente.



Per ulteriori informazioni, consulta "Creazione di un volume NFS" la documentazione.

▼ **Assicurarsi che esista una connessione privata su GCVE per NetApp Volumes Tenant VPC.**

Per montare NFS Datastore, deve esistere una connessione privata tra GCVE e il progetto NetApp Volumes. Per maggiori informazioni, fare riferimento"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 Volumes"

Poiché gli host vSphere sono gestiti da Google, non hai accesso per installare NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). Se hai bisogno di supporto per i volumi virtuali (vVol), faccelo sapere. Se preferisci utilizzare i Jumbo Frame, fai riferimento"Dimensioni MTU massime supportate su GCP"

Risparmi con Google Cloud NetApp Volumes

Per saperne di più sui potenziali risparmi che puoi ottenere con Google Cloud NetApp Volumes per le tue esigenze di archiviazione su GCVE, consulta "Calcolatore del ROI NetApp"

Link di riferimento

- "Blog di Google - Come utilizzare NetApp Volumes come datastore per Google Cloud VMware Engine"
- "Blog NetApp : un modo migliore per migrare le tue app ad alto contenuto di storage su Google Cloud"

Opzioni di archiviazione NetApp per GCP

GCP supporta l'archiviazione NetApp connessa agli ospiti con Cloud Volumes ONTAP (CVO) o Google Cloud NetApp Volumes (NetApp Volumes).

Cloud Volumes ONTAP (CVO)

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

Si tratta di una versione software-defined di ONTAP che utilizza storage cloud-native, consentendo di avere lo stesso software di storage nel cloud e in locale, riducendo la necessità di riqualificare il personale IT su metodi completamente nuovi per gestire i dati.

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

Grazie alla sua progettazione, CVO offre prestazioni estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud.

Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti

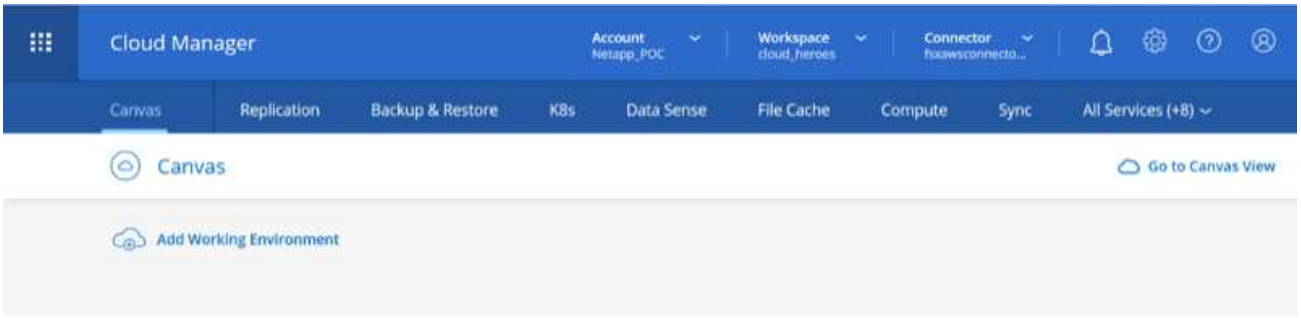
▼ **Distribuisci Cloud Volumes ONTAP in Google Cloud (fai da te)**

Le condivisioni Cloud Volumes ONTAP possono essere montate da VM create nell'ambiente cloud privato GCVE. I volumi possono essere montati anche sul client Linux e sul client Windows, mentre è possibile accedere ai LUN sui client Linux o Windows come dispositivi a blocchi quando montati su iSCSI, poiché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

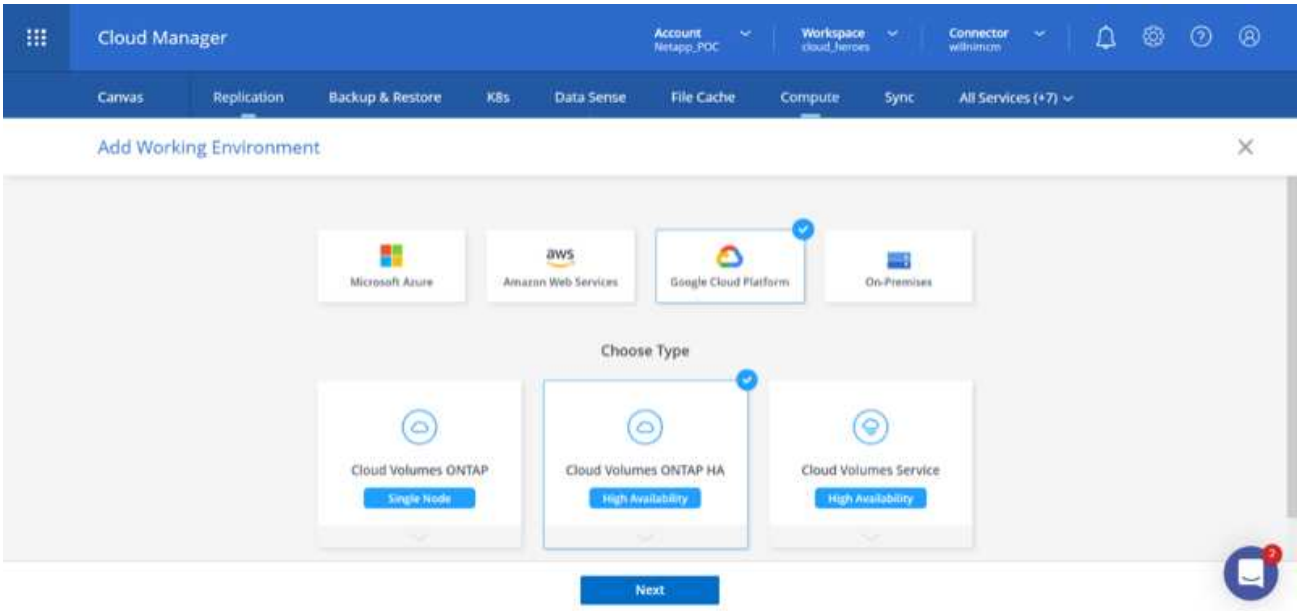
Per replicare volumi da un ambiente on-premise al cloud per scopi di disaster recovery o migrazione, stabilire la connettività di rete a Google Cloud, utilizzando una VPN da sito a sito o Cloud Interconnect. La replica dei dati da locale a Cloud Volumes ONTAP esula dall'ambito del presente documento. Per replicare i dati tra i sistemi locali e Cloud Volumes ONTAP , vedere"Impostazione della replica dei dati tra i sistemi" .

> Usa "Dimensionatore Cloud Volumes ONTAP" per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Monitora anche le prestazioni on-premises da usare come input nello strumento di dimensionamento di Cloud Volumes ONTAP.

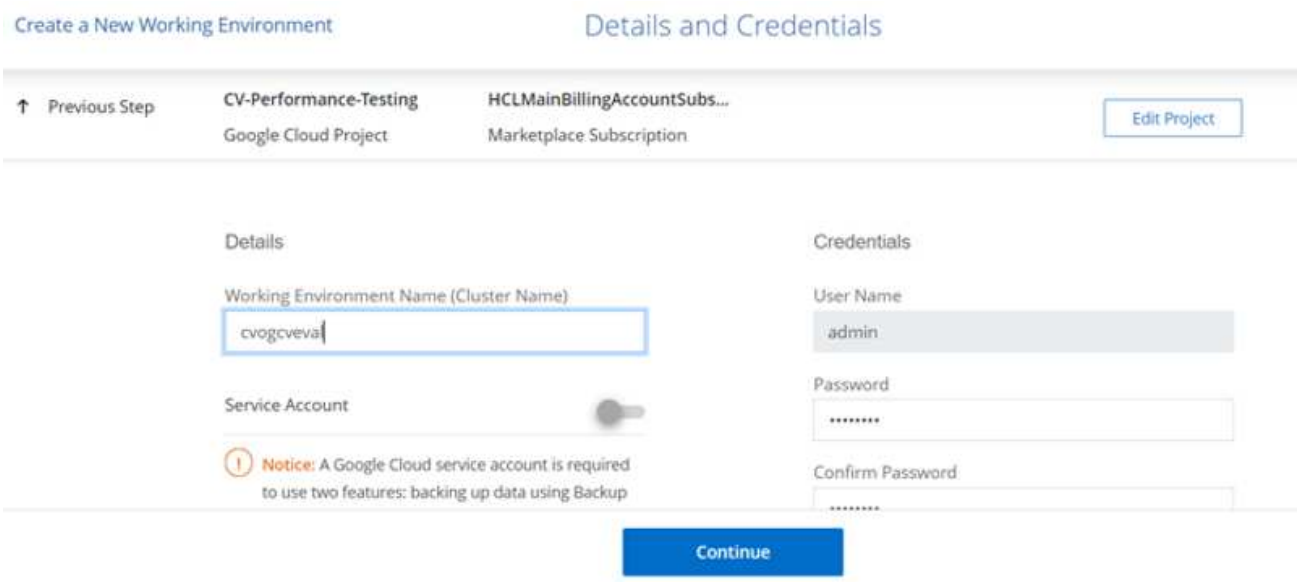
1. Accedi a NetApp Cloud Central: verrà visualizzata la schermata Fabric View. Individua la scheda Cloud Volumes ONTAP e seleziona Vai a Cloud Manager. Dopo aver effettuato l'accesso, verrà visualizzata la schermata Canvas.



2. Nella scheda Cloud Manager Canvas, fare clic su Aggiungi un ambiente di lavoro, quindi selezionare Google Cloud Platform come cloud e il tipo di configurazione del sistema. Quindi, fare clic su Avanti.



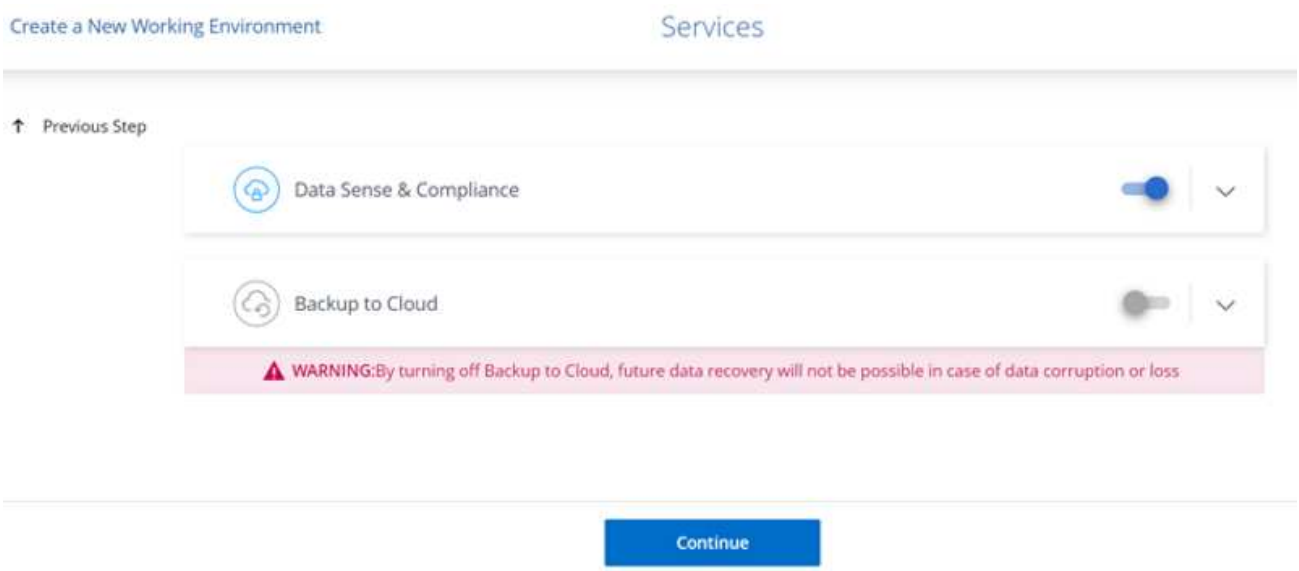
3. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Una volta terminato, fare clic su Continua.



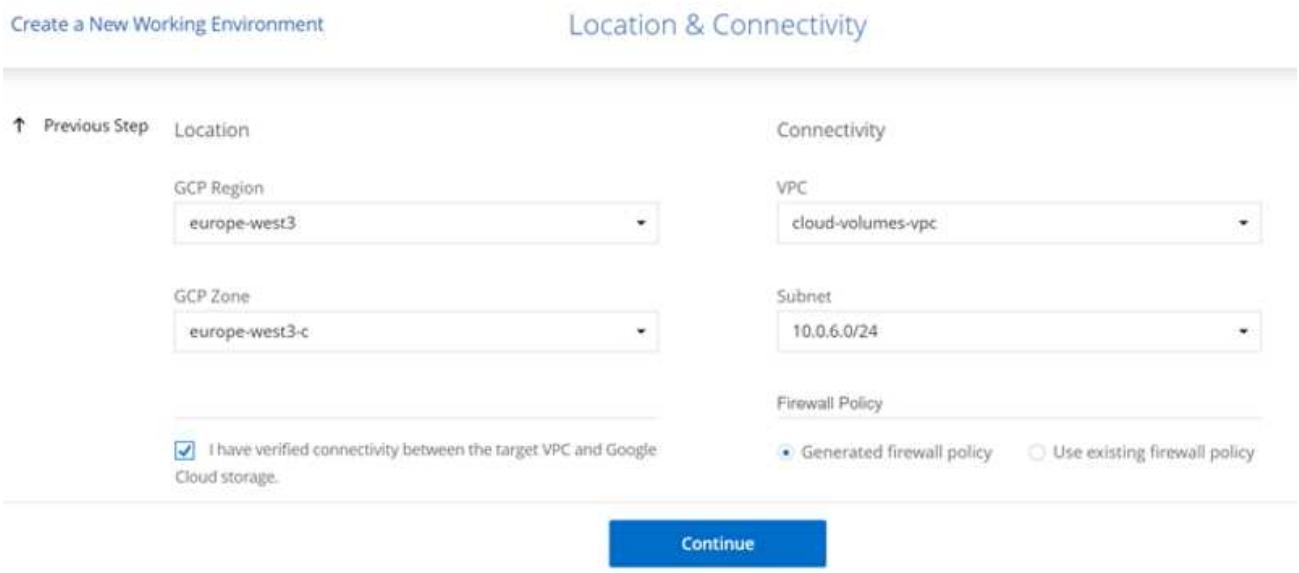
4. Selezionare o deselezionare i servizi aggiuntivi per la distribuzione Cloud Volumes ONTAP , tra cui Data

Sense & Compliance o Backup to Cloud. Quindi, fare clic su Continua.

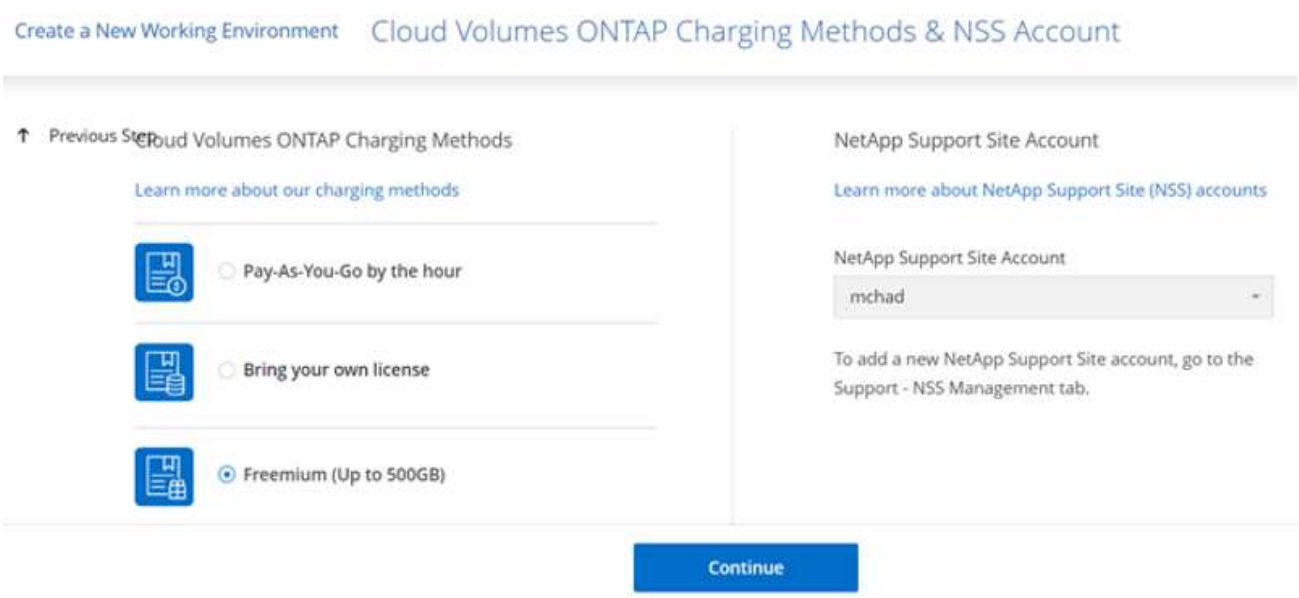
SUGGERIMENTO: quando si disattivano i servizi aggiuntivi verrà visualizzato un messaggio pop-up di verifica. I servizi aggiuntivi possono essere aggiunti/rimossi dopo l'implementazione di CVO; se non sono necessari fin dall'inizio, si consiglia di deselezionarli per evitare costi.



5. Seleziona una posizione, scegli un criterio firewall e seleziona la casella di controllo per confermare la connettività di rete allo storage Google Cloud.

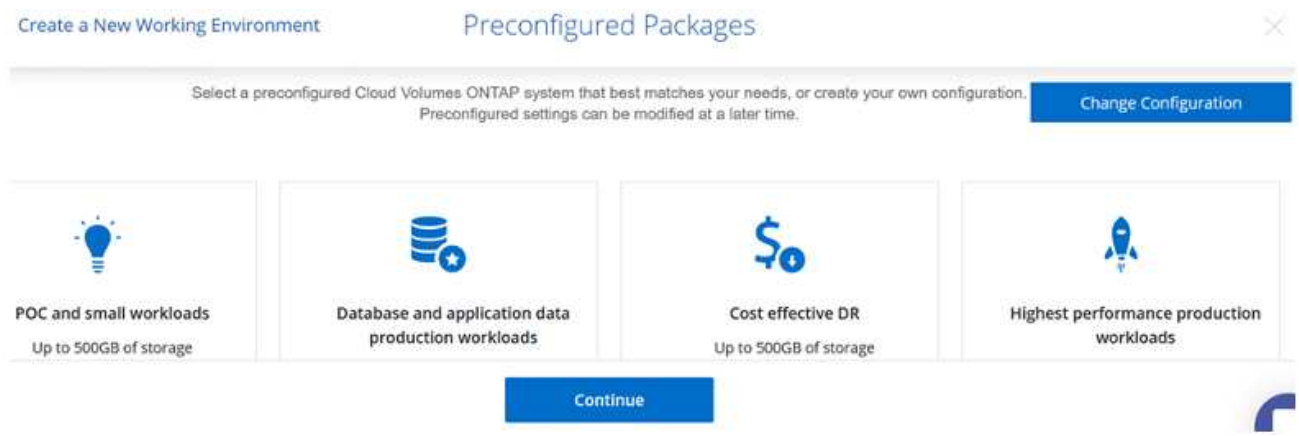


6. Selezionare l'opzione di licenza: Pay-As-You-Go o BYOL per utilizzare la licenza esistente. In questo esempio viene utilizzata l'opzione Freemium. Quindi, fare clic su Continua.

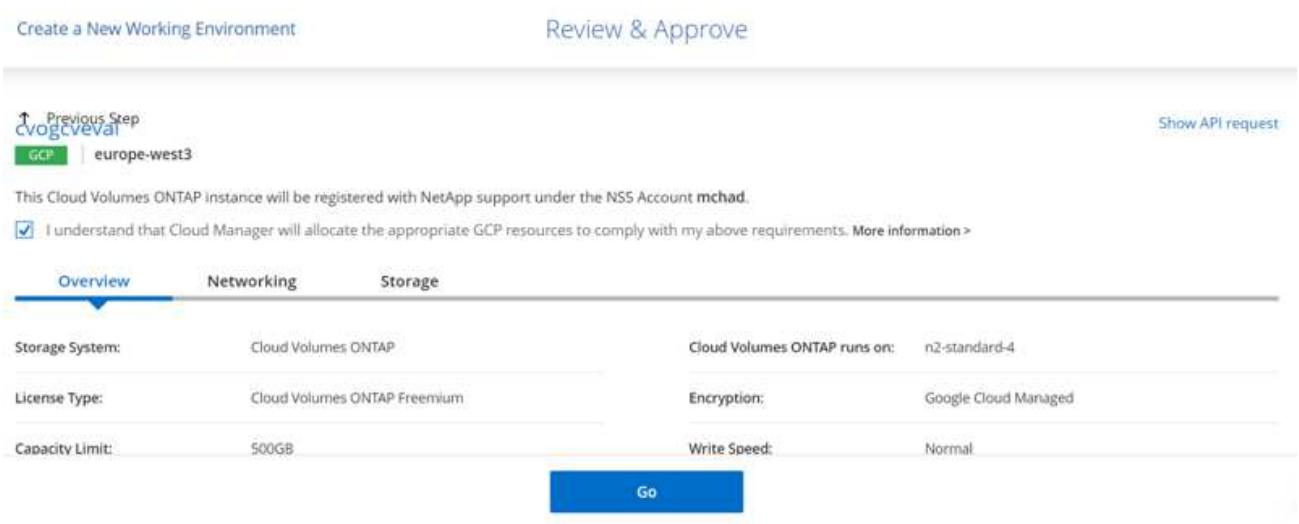


7. Seleziona tra diversi pacchetti preconfigurati disponibili in base al tipo di carico di lavoro che verrà distribuito sulle VM in esecuzione sul cloud VMware su AWS SDDC.

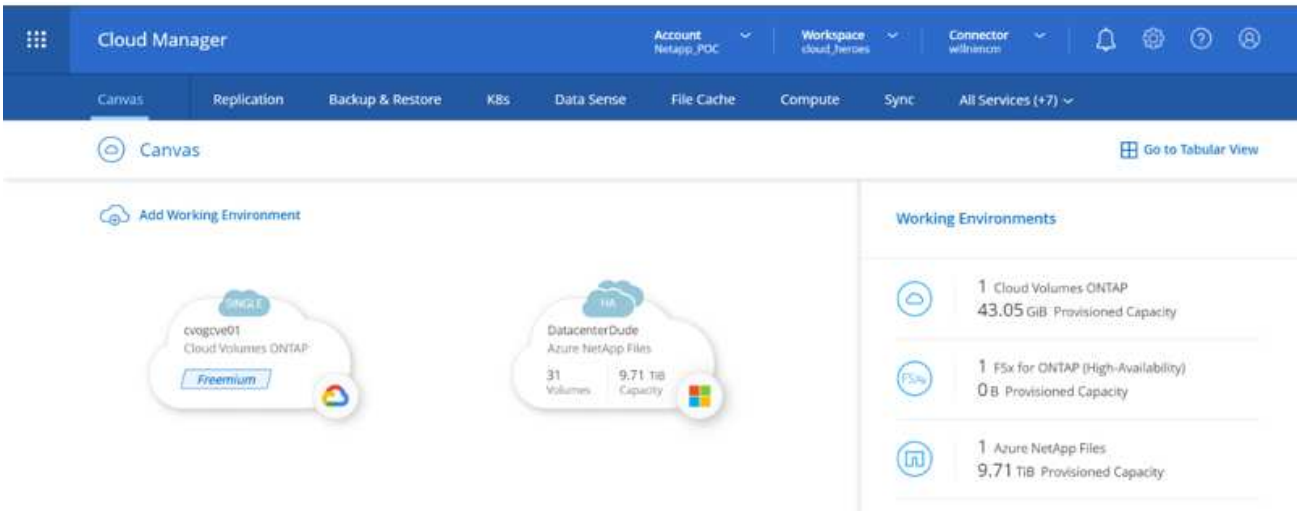
   SUGGERIMENTO: passa il mouse sui riquadri per i dettagli o personalizza i componenti CVO e la versione ONTAP cliccando su Modifica configurazione.



8. Nella pagina Revisione e approvazione, rivedere e confermare le selezioni. Per creare l'istanza Cloud Volumes ONTAP , fare clic su Vai.



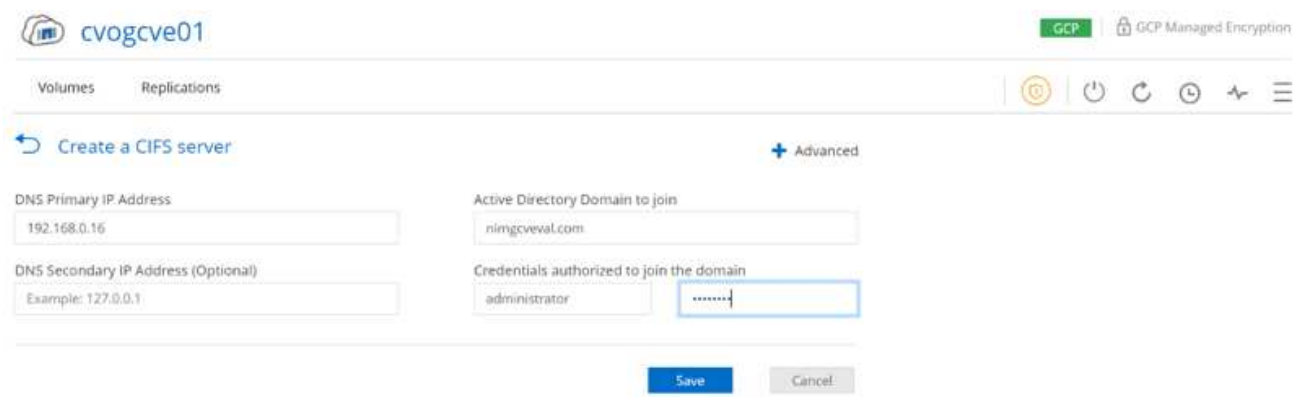
9. Dopo aver eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.



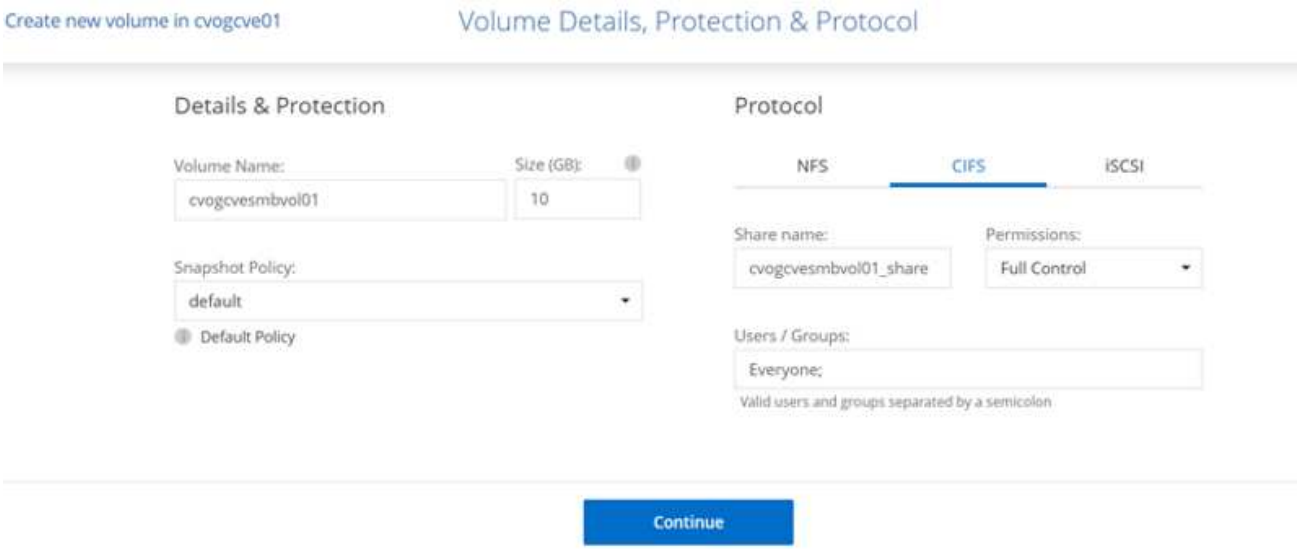
▼ Configurazioni aggiuntive per volumi SMB

1. Una volta che l'ambiente di lavoro è pronto, 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 del menu (º), selezionare Avanzate per visualizzare più opzioni e selezionare 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 la dimensione appropriata e il gestore cloud sceglierà l'aggregato contenente oppure utilizzerà un meccanismo di allocazione avanzato per posizionarlo su un aggregato specifico. Per questa demo, è stato selezionato CIFS/SMB come protocollo.



3. Dopo aver eseguito il provisioning, il volume sarà disponibile nel riquadro Volumi. Poiché è stata predisposta una condivisione CIFS, concedere agli utenti o ai gruppi l'autorizzazione per accedere ai file e alle 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 locale, perché tutte le autorizzazioni per file e cartelle vengono mantenute come parte della replica SnapMirror .

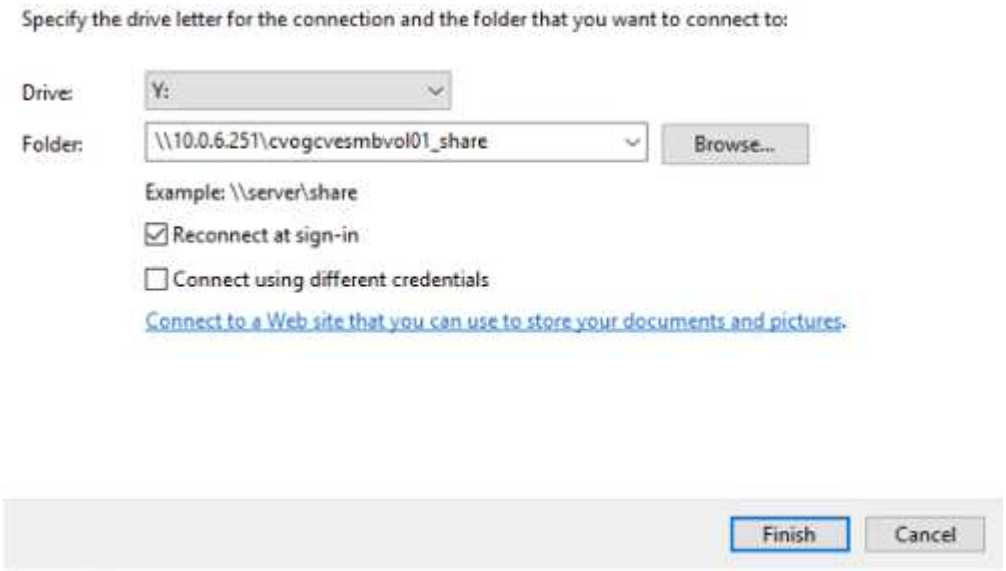
   SUGGERIMENTO: fare clic sul menu del volume (º) per visualizzarne le opzioni.



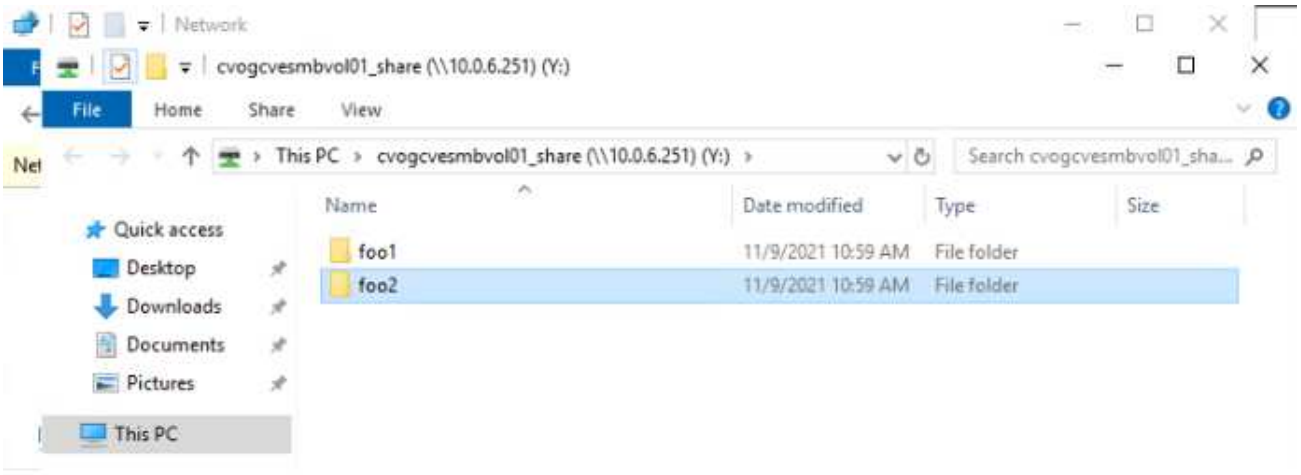
4. Dopo aver creato il volume, utilizzare il comando mount per visualizzare le istruzioni di connessione al volume, quindi connettersi alla condivisione dalle VM su Google Cloud VMware Engine.



5. Copia il percorso seguente e utilizza l'opzione Connetti unità di rete per montare il volume sulla VM in esecuzione su Google Cloud VMware Engine.



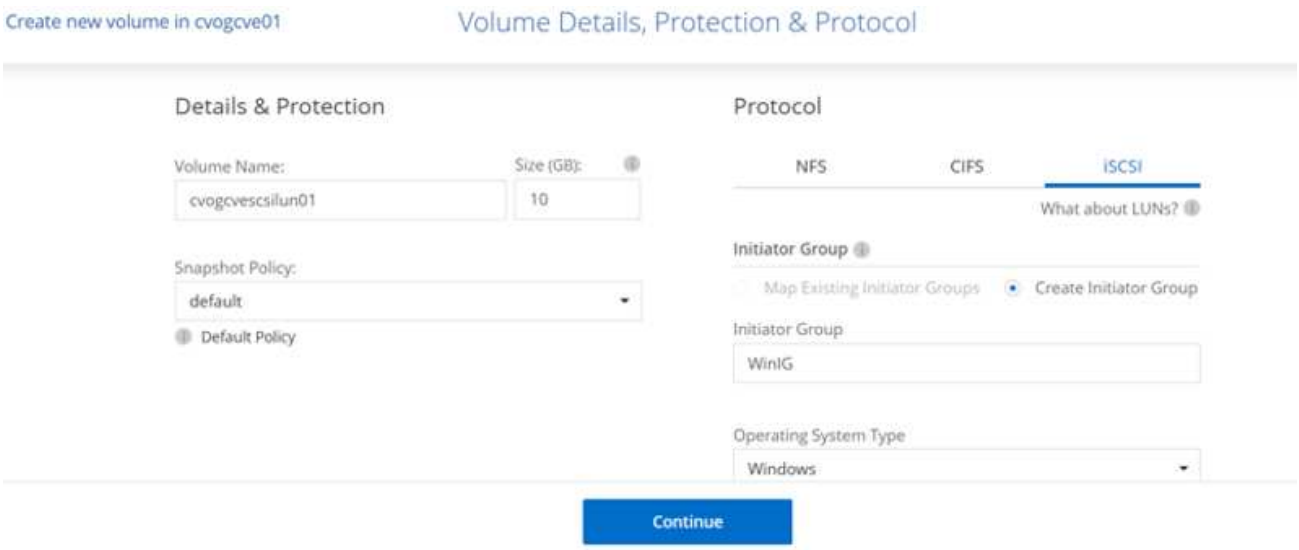
Una volta mappato, è possibile accedervi facilmente e impostare di conseguenza le autorizzazioni NTFS.

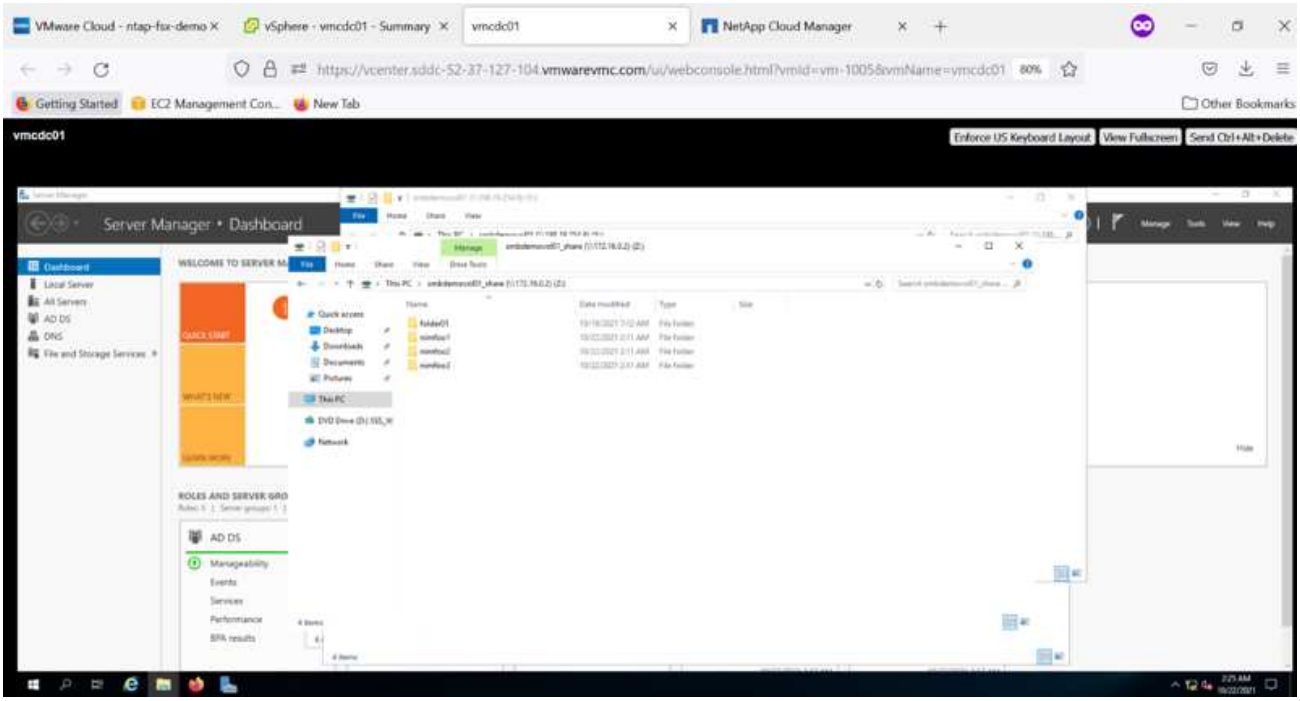


▼ Collegare il LUN su Cloud Volumes ONTAP a un host

Per connettere il LUN ONTAP dei volumi cloud a un host, completare i seguenti passaggi:

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Aggiungi volume > Nuovo volume, selezionare iSCSI e fare clic su Crea gruppo iniziatori. Fare clic su Continua.





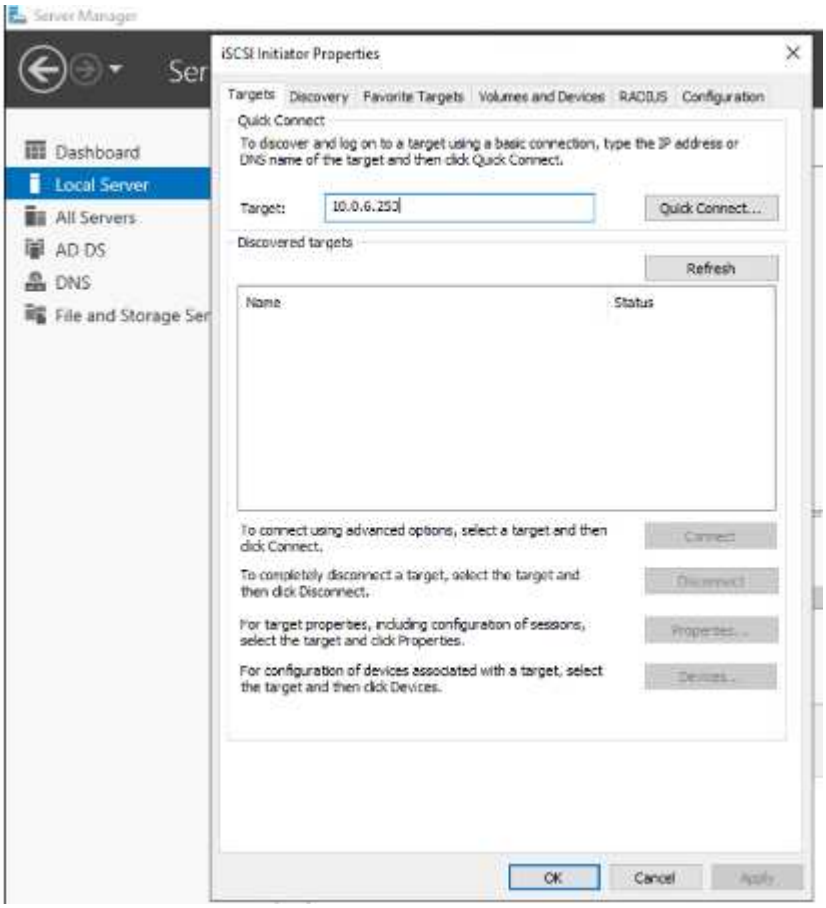
3. Dopo aver eseguito il provisioning del volume, selezionare il menu del volume (º), quindi fare clic su Target iQN. Per copiare il nome qualificato iSCSI (iQN), fare clic su Copia. Impostare una connessione iSCSI dall'host al LUN.

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

1. RDP alla VM ospitata su Google Cloud VMware Engine.
2. Aprire la finestra di dialogo Proprietà dell'iniziatore iSCSI: Server Manager > Dashboard > Strumenti > Iniziatore iSCSI.

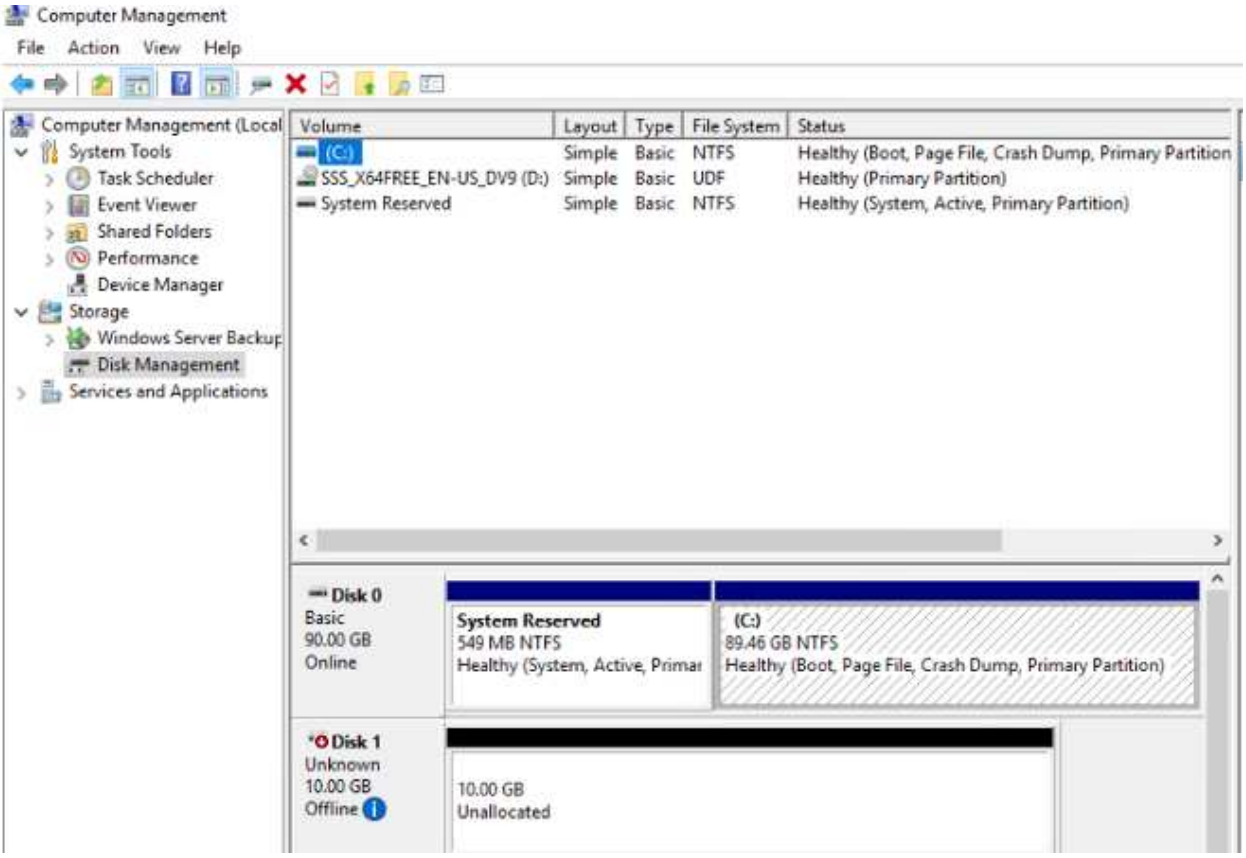
3. Dalla scheda Individuazione, fare clic su Individua portale o Aggiungi portale, quindi immettere l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Destinazioni, seleziona la destinazione rilevata e poi fai clic su Accedi o Connetti.
5. Selezionare Abilita multipath, quindi selezionare Ripristina automaticamente questa 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.



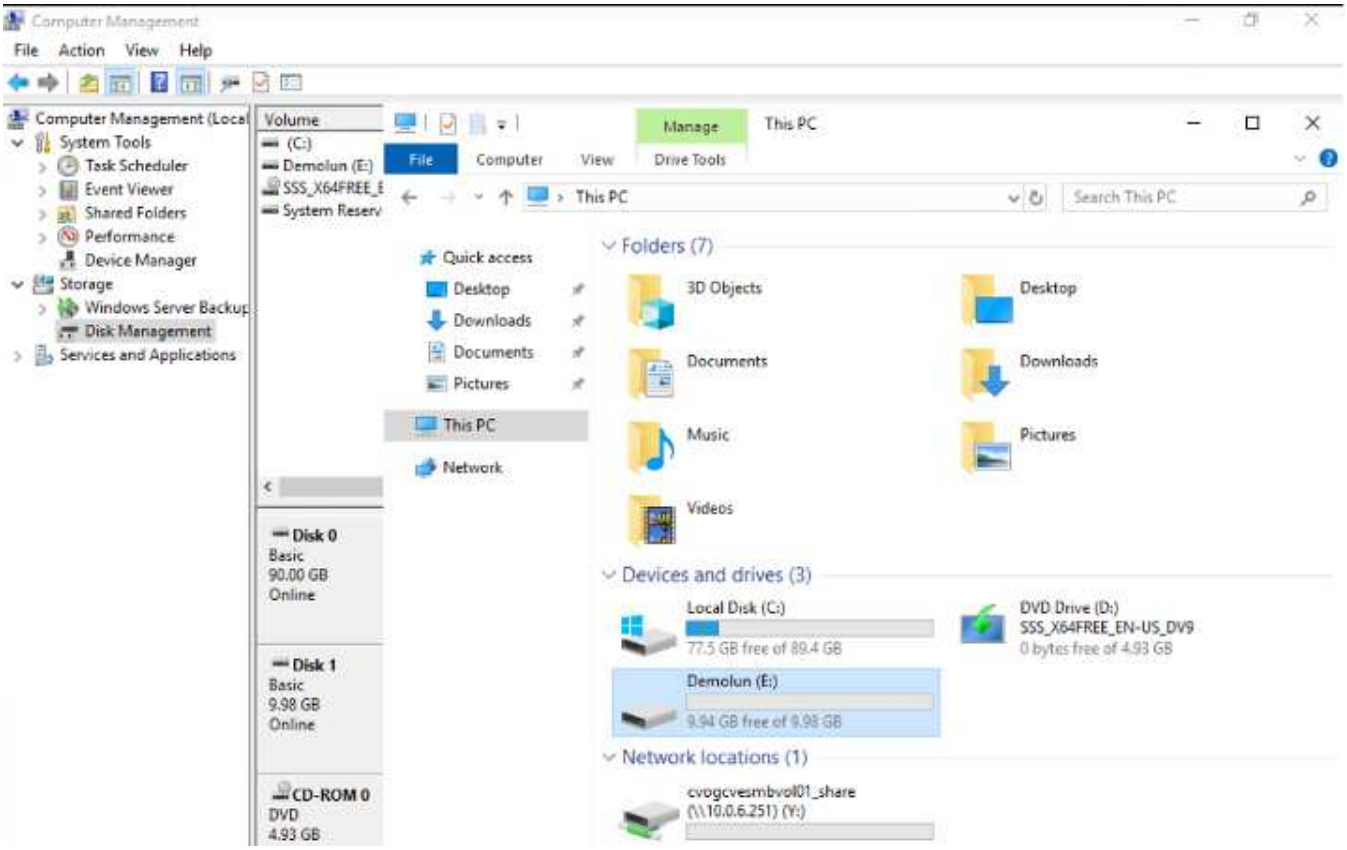
Le LUN sulla macchina virtuale di archiviazione (SVM) vengono visualizzate come dischi sull'host Windows. Tutti i nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Avviare una nuova scansione manuale per rilevare i dischi completando i seguenti passaggi:

a. Aprire l'utilità Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
b. Espandere il nodo Archiviazione nell'albero di navigazione.
c. Fare clic su Gestione disco.
d. Fare clic su Azione > Ripeti analisi dischi.



Quando l'host Windows accede per la prima volta a un nuovo LUN, questo non ha alcuna partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando i seguenti passaggi:

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, è montata l'unità F:.



Sui client Linux, assicurarsi che il demone iSCSI sia in esecuzione. Una volta predisposti i LUN, fare riferimento alle istruzioni dettagliate 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
```

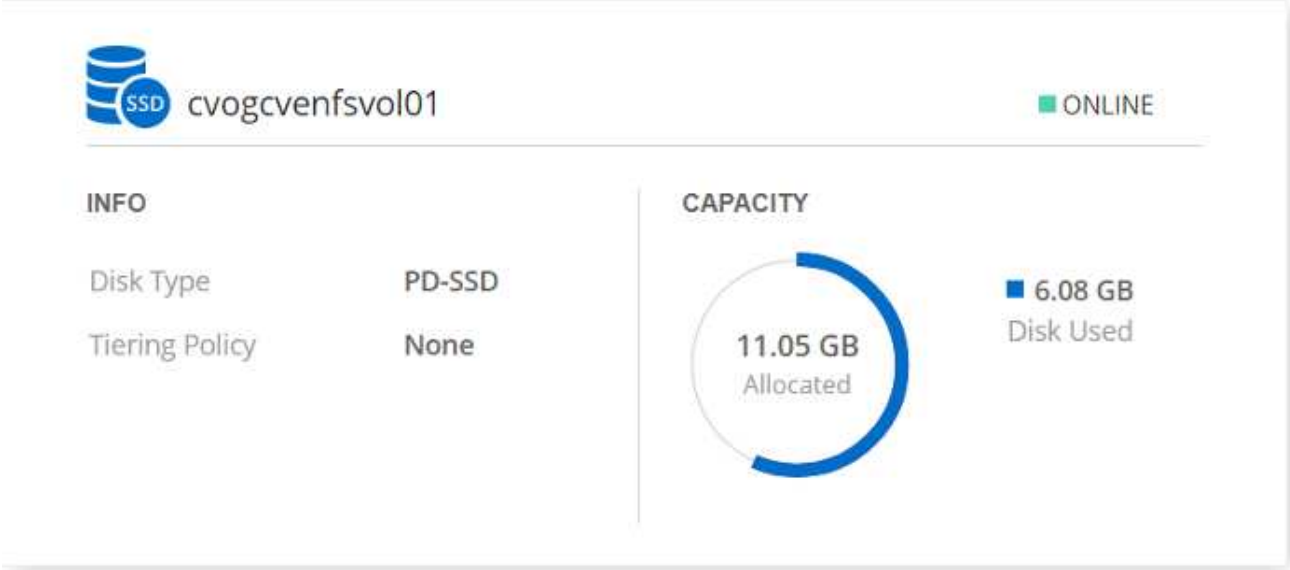
```
nlyaz@nlnubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ **Montare il volume Cloud Volumes ONTAP NFS sul client Linux**

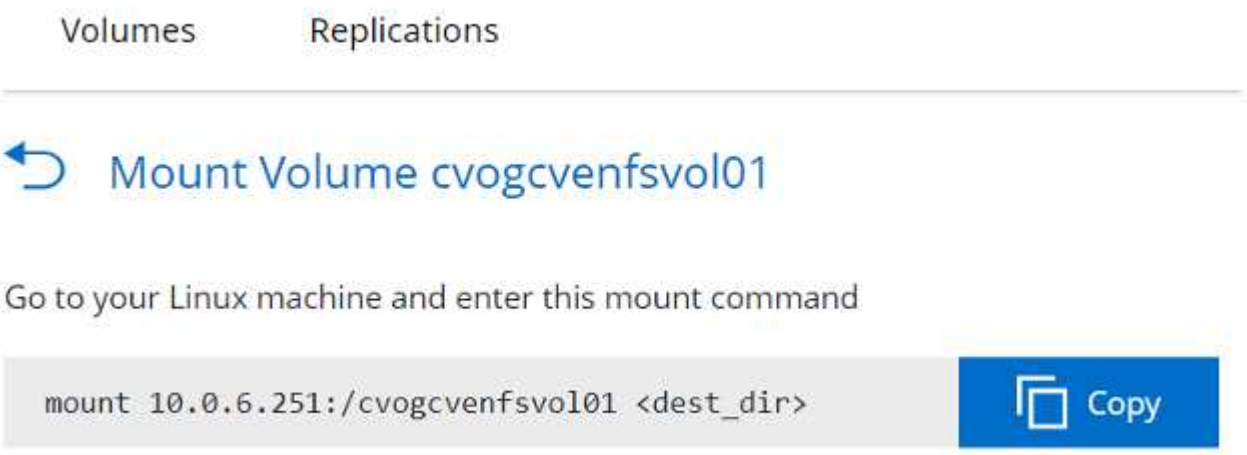
Per montare il file system Cloud Volumes ONTAP (DIY) dalle VM all'interno di Google Cloud VMware Engine, seguire i passaggi seguenti:

Fornire il volume seguendo i passaggi seguenti

1. Nella scheda Volumi, fare clic su Crea nuovo volume.
2. Nella pagina Crea nuovo volume, seleziona un tipo di volume:



3. Nella scheda Volumi, posiziona il cursore del mouse sul volume, seleziona l'icona del menu (º) e quindi fai clic su Comando di montaggio.



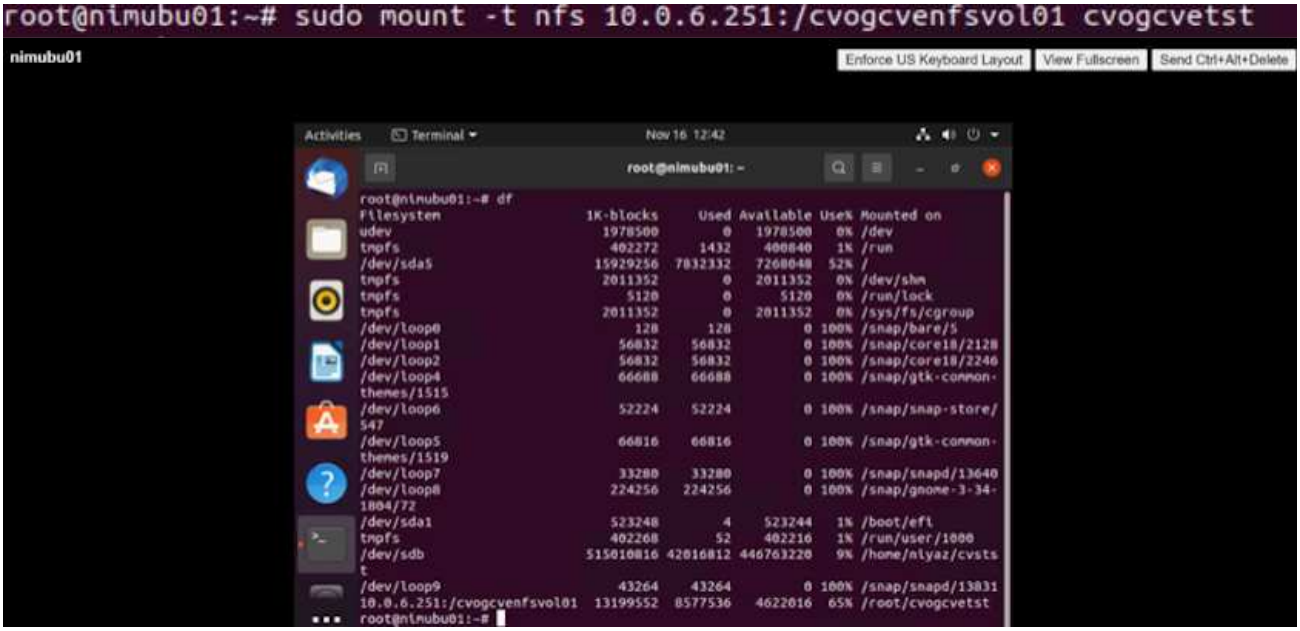
4. Fare clic su Copia.
5. Connettersi all'istanza Linux designata.
6. Aprire un terminale sull'istanza utilizzando Secure Shell (SSH) ed effettuare l'accesso con le credenziali appropriate.
7. Creare una directory per il punto di montaggio del volume con il seguente comando.

```
$ sudo mkdir /cvogcvetst
```

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

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

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



Google Cloud NetApp Volumes (NetApp Volumes)

Google Cloud NetApp Volumes (NetApp Volumes) è un portafoglio completo di servizi dati per fornire soluzioni cloud avanzate. NetApp Volumes supporta più protocolli di accesso ai file per i principali provider cloud (supporto NFS e SMB).

Altri vantaggi e caratteristiche includono: protezione e ripristino dei dati con Snapshot; funzionalità speciali per replicare, sincronizzare e migrare destinazioni di dati in locale o nel cloud; e prestazioni elevate e costanti a livello di un sistema di archiviazione flash dedicato.

Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti

▼ Configurare i volumi NetApp con VMware Engine

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

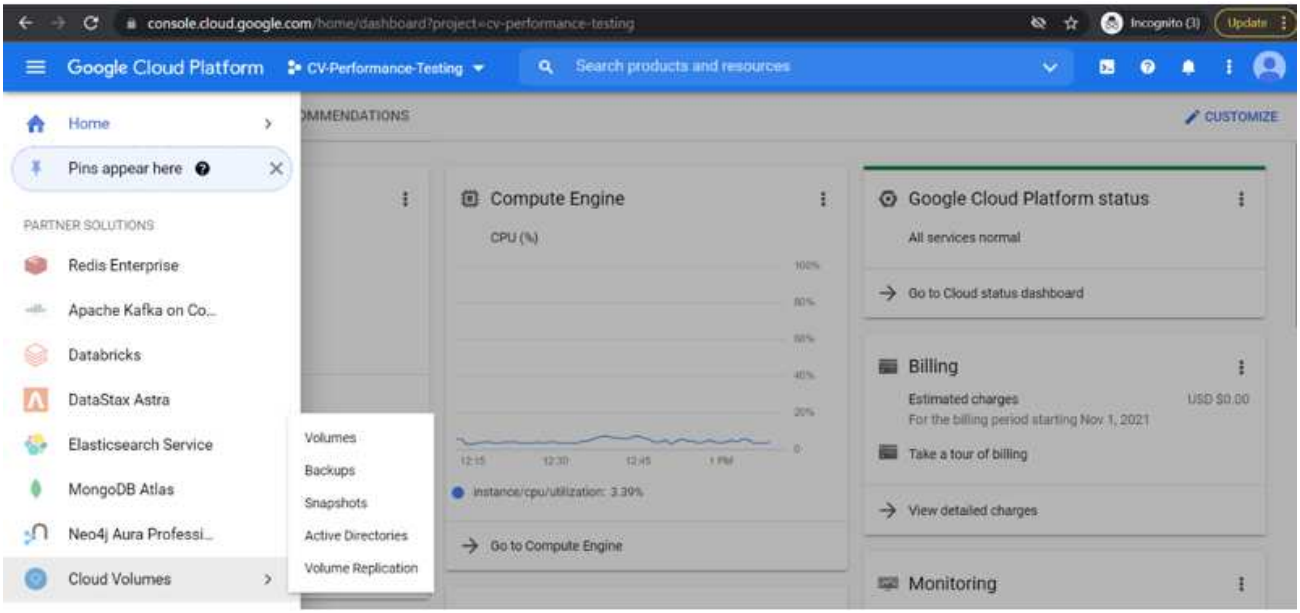
Google Cloud NetApp Volumes e il cloud privato Google Cloud VMware Engine devono trovarsi nella stessa regione.

Per acquistare, abilitare e configurare Google Cloud NetApp Volumes per Google Cloud da Google Cloud Marketplace, segui queste istruzioni dettagliate"guida" .

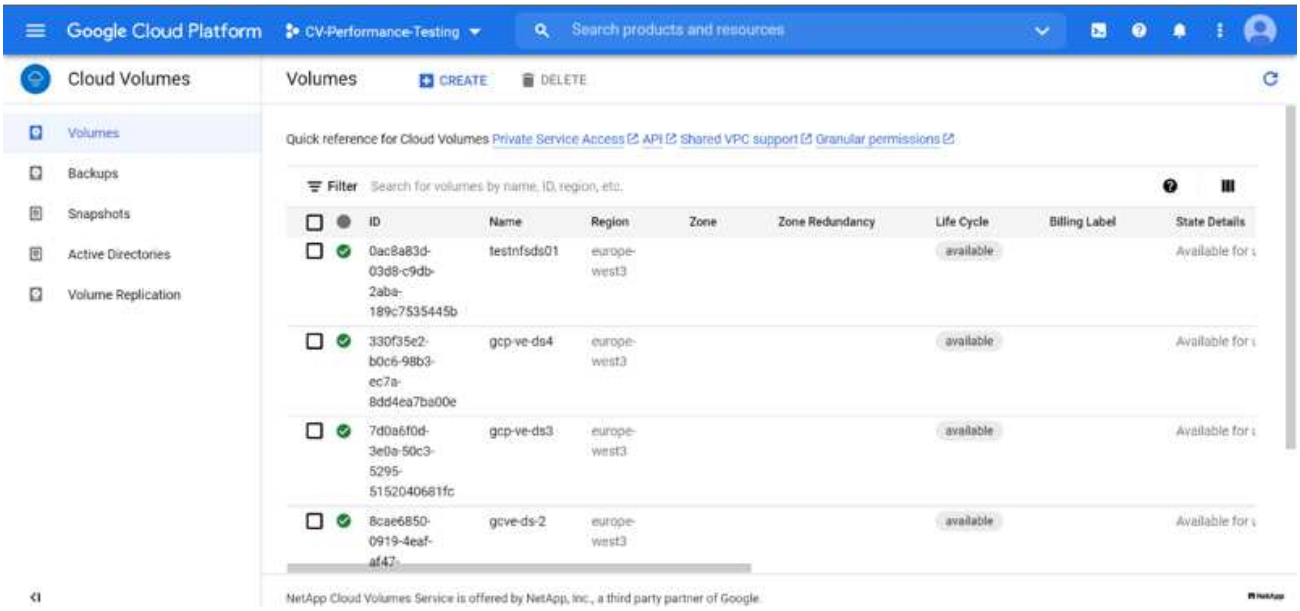
▼ Crea un volume NFS NetApp Volumes nel cloud privato GCVE

Per creare e montare volumi NFS, completare i seguenti passaggi:

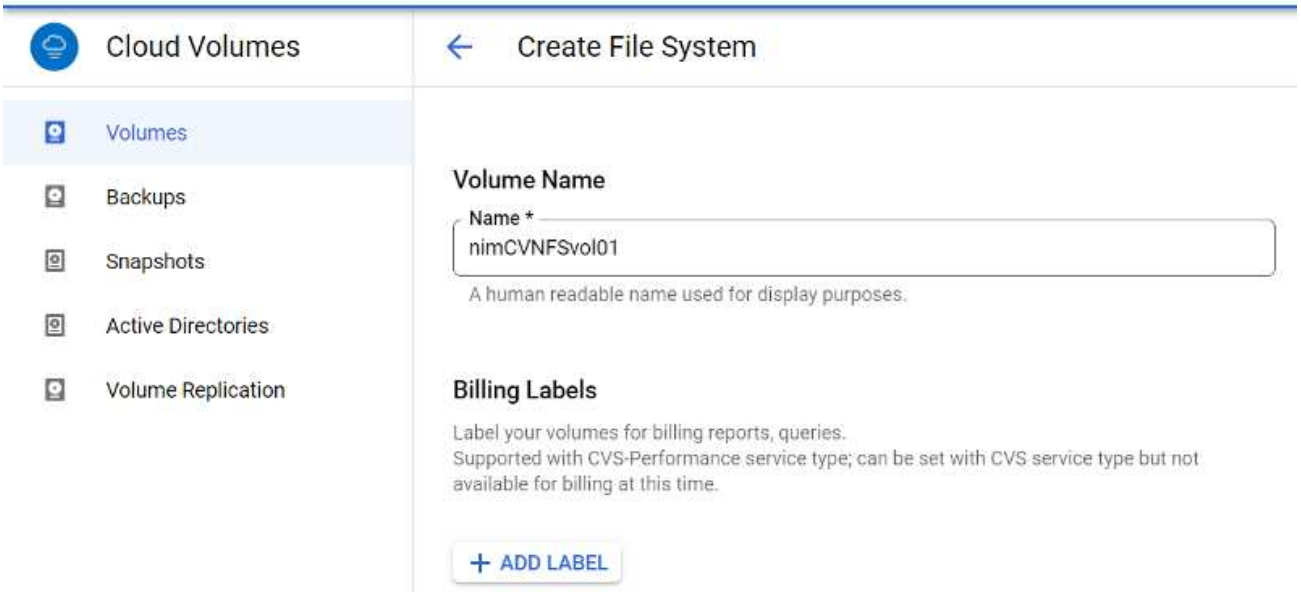
1. Accedi a Cloud Volumes da Partner Solutions all'interno della console Google Cloud.



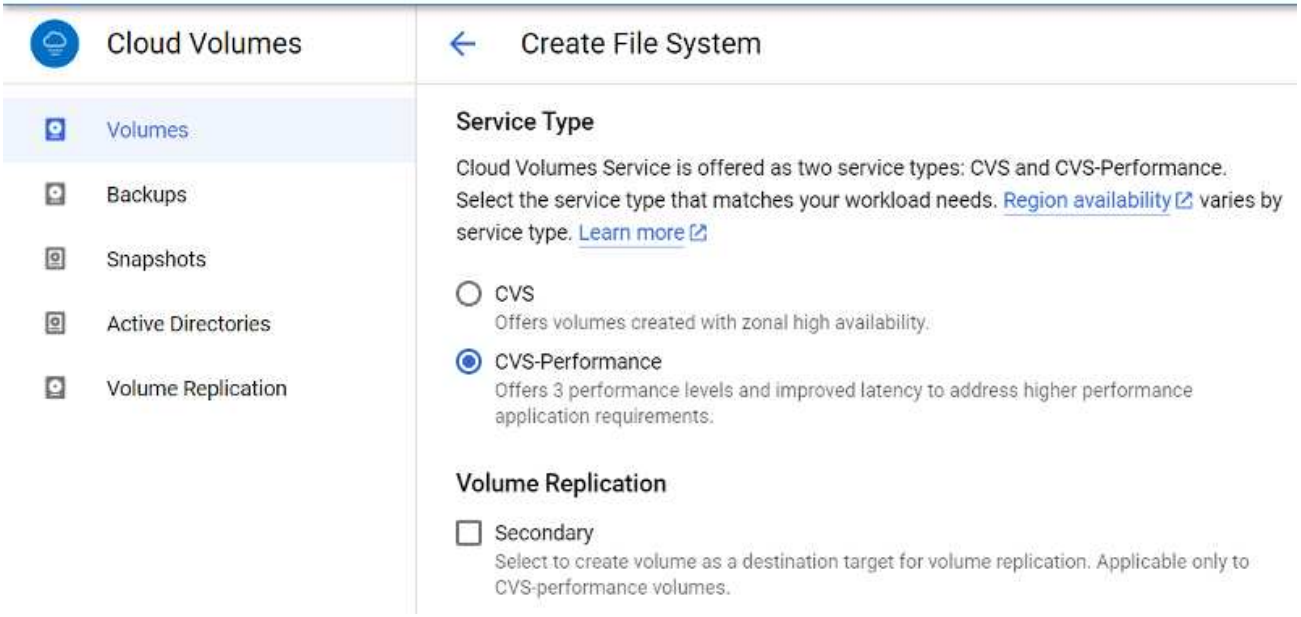
2. Nella console Cloud Volumes, vai alla pagina Volumi e fai clic su Crea.



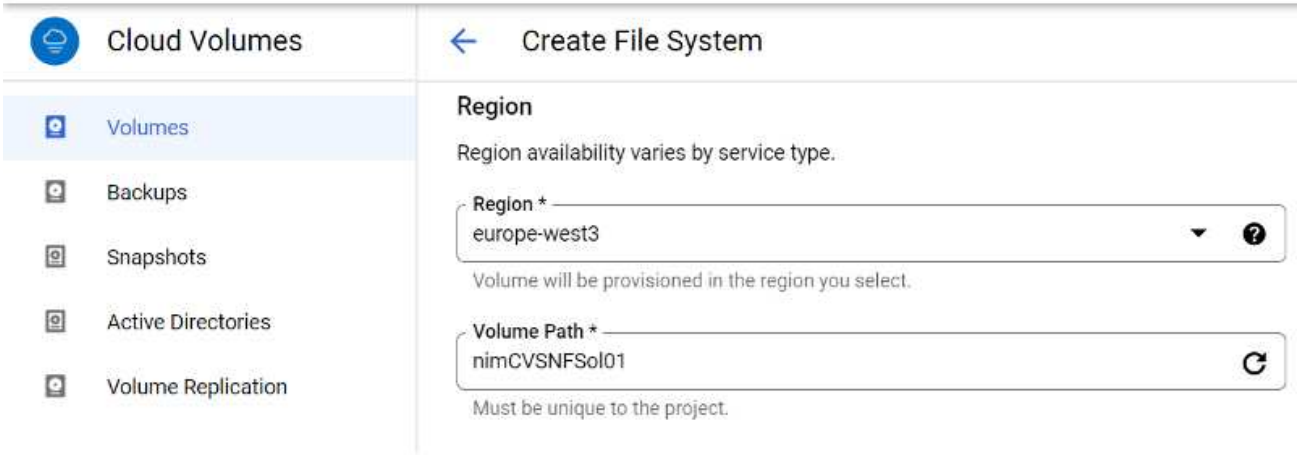
3. Nella pagina Crea file system, specificare il nome del volume e le etichette di fatturazione come richiesto per i meccanismi di addebito.



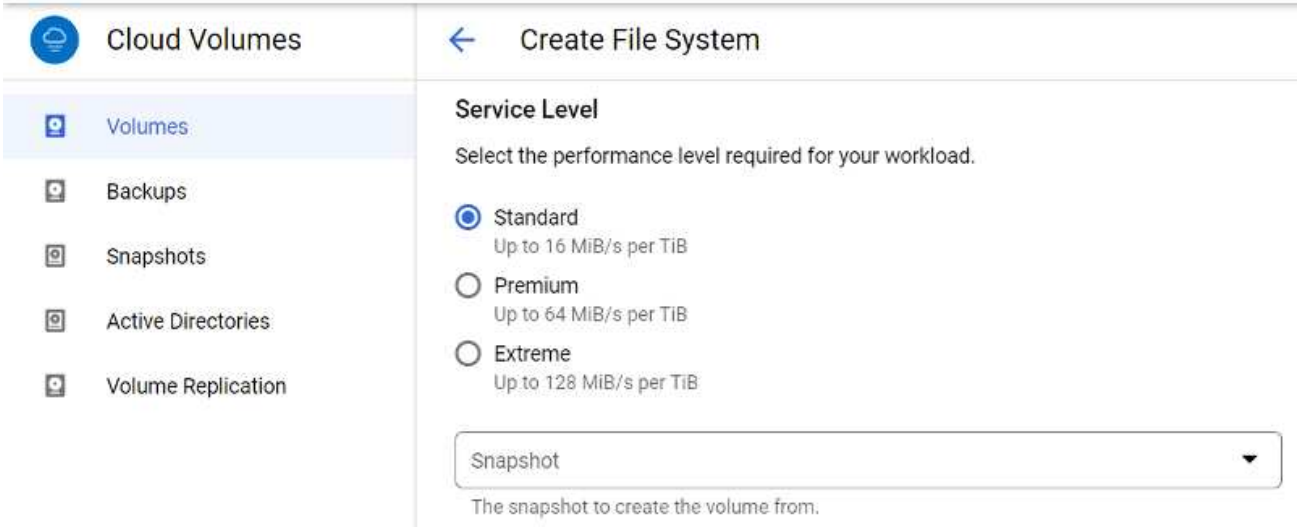
4. Seleziona il servizio appropriato. Per GCVE, scegli NetApp Volumes-Performance e il livello di servizio desiderato per una latenza migliorata e prestazioni più elevate in base ai requisiti del carico di lavoro dell'applicazione.



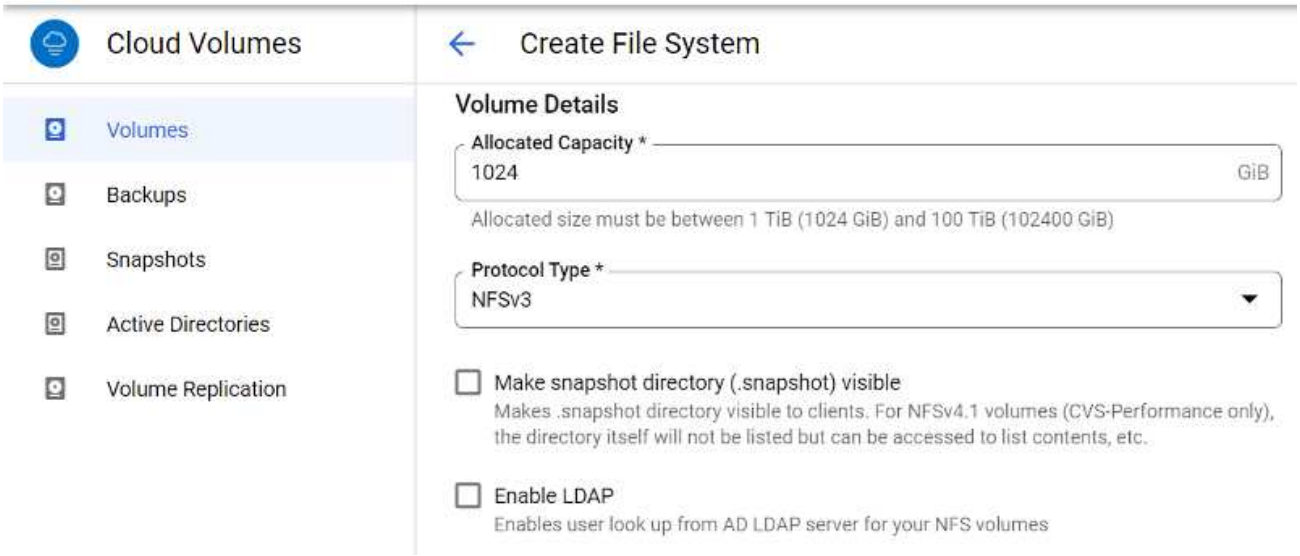
5. Specificare la regione Google Cloud per il volume e il percorso del volume (il percorso del volume deve essere univoco in tutti i volumi cloud nel progetto)



6. Seleziona il livello di prestazioni per il volume.

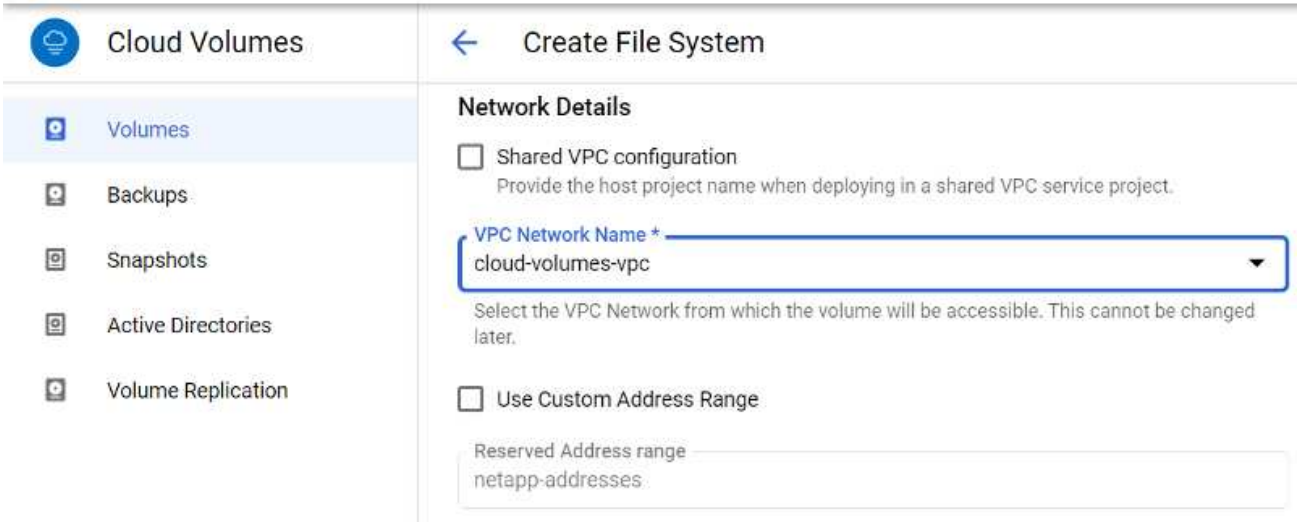


7. Specificare la dimensione del volume e il tipo di protocollo. In questo test viene utilizzato NFSv3.



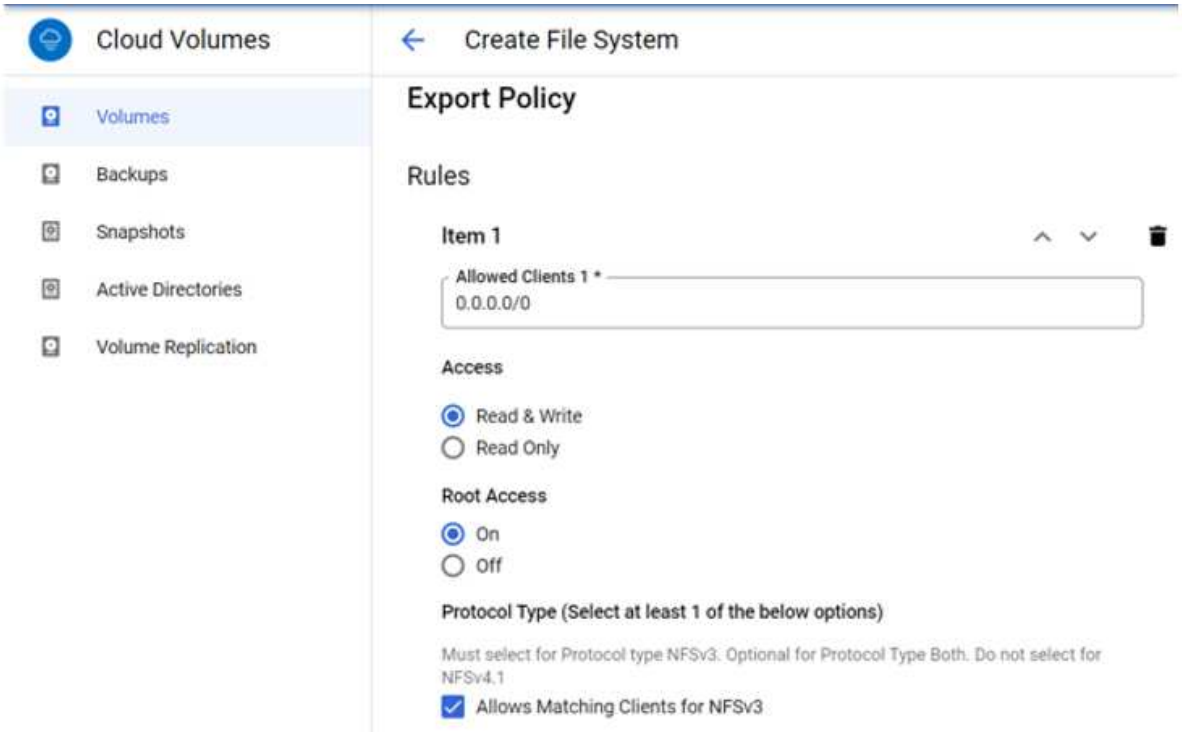
8. In questo passaggio, seleziona la rete VPC da cui sarà accessibile il volume. Assicurarsi che il peering VPC sia attivo.

   SUGGERIMENTO: se il peering VPC non è stato eseguito, verrà visualizzato un pulsante pop-up che ti guiderà attraverso i comandi di peering. Apri una sessione di Cloud Shell ed esegui i comandi appropriati per collegare la tua VPC al produttore di Google Cloud NetApp Volumes . Se decidi di preparare in anticipo il peering VPC, fai riferimento a queste istruzioni.



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

   Nota: l'accesso ai volumi NFS non sarà possibile a meno che non venga aggiunto un criterio di esportazione.



10. Fare clic su Salva per creare il volume.



▼ **Montaggio delle esportazioni NFS su VM in esecuzione su VMware Engine**

Prima di preparare il montaggio del volume NFS, assicurarsi che lo stato di peering della connessione privata sia elencato 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, vai a Cloud Volumes > Volumi.
2. Vai alla pagina dei Volumi
3. Fare clic sul volume NFS per il quale si desidera montare le esportazioni NFS.
4. Scorri verso destra, sotto Mostra altro, fai clic su Istruzioni di montaggio.

Per eseguire il processo di montaggio dall'interno del sistema operativo guest della VM VMware, seguire i passaggi seguenti:

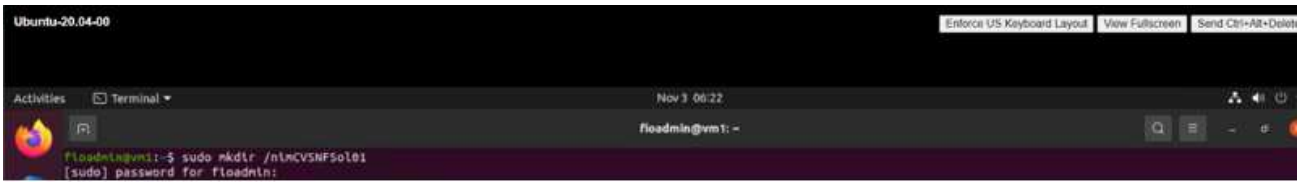
1. Utilizzare il client SSH e SSH per connettersi alla macchina virtuale.
2. Installare il client NFS sull'istanza.
   a. Su istanza Red Hat Enterprise Linux o SuSE Linux:

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

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

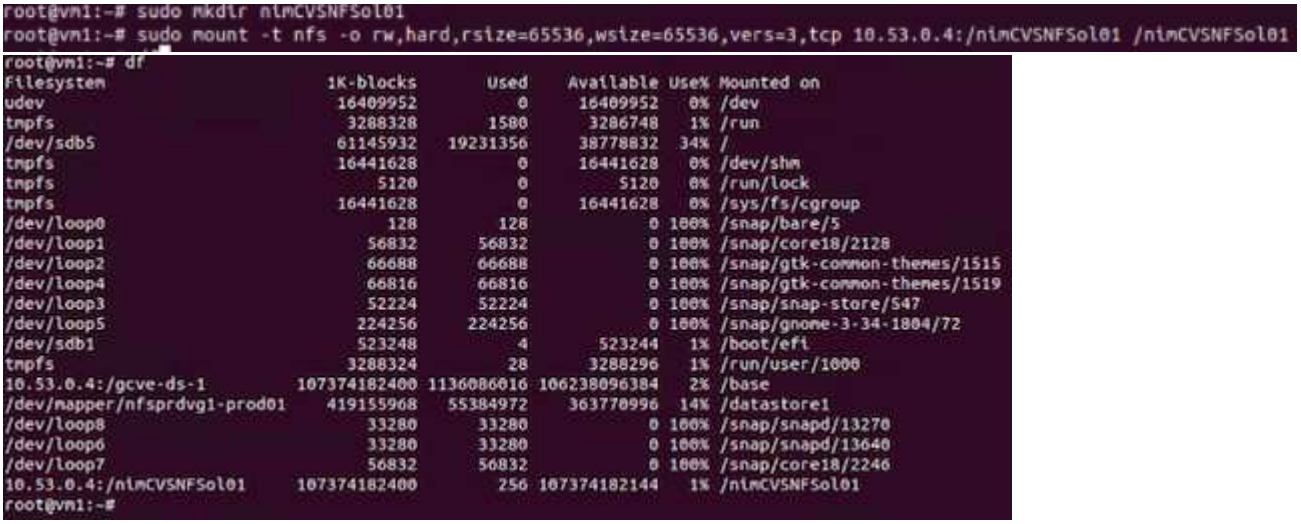
3. Crea una nuova directory sull'istanza, ad esempio "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```



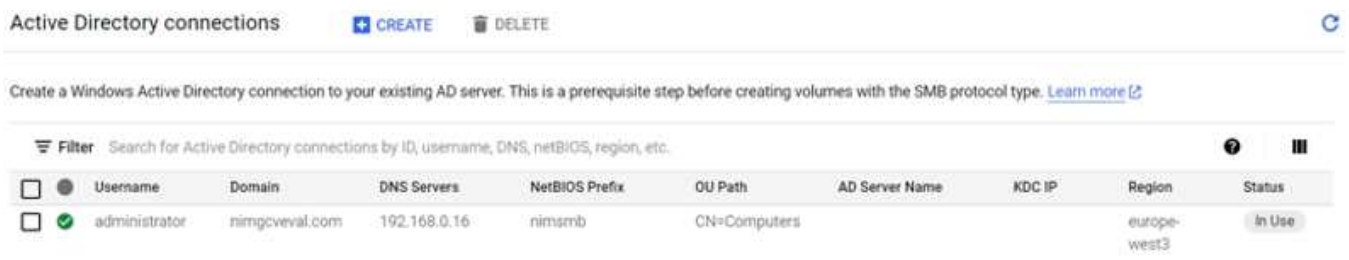
4. Montare il volume utilizzando il comando appropriato. Di seguito è riportato un esempio di comando dal laboratorio:

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



▼ **Creazione e montaggio di condivisioni SMB su VM in esecuzione su VMware Engine**

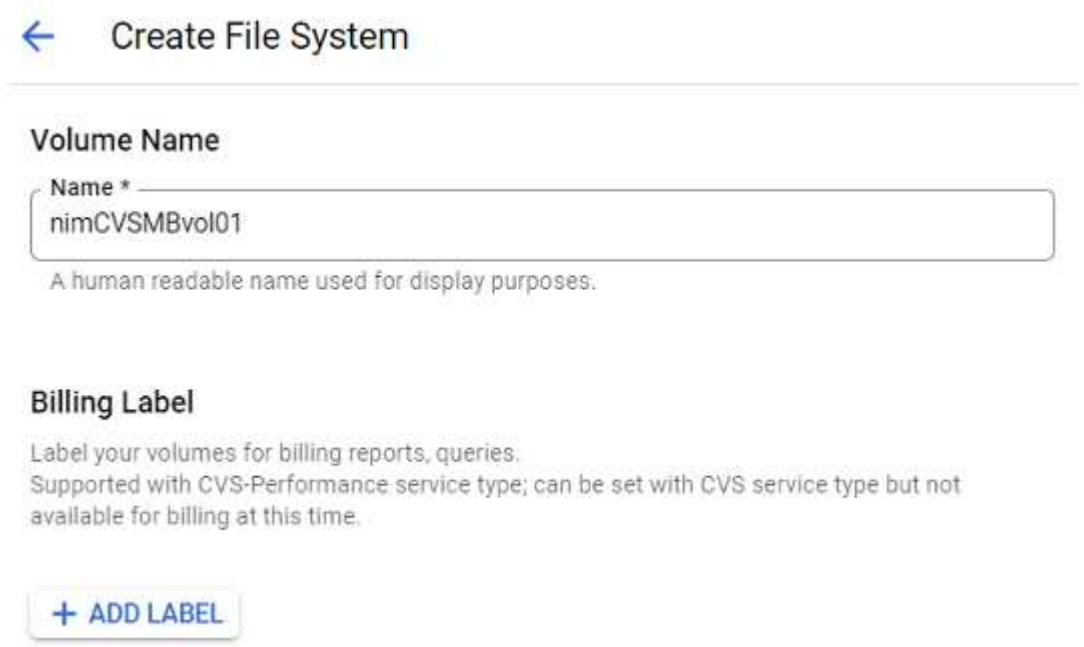
Per i volumi SMB, assicurarsi che le connessioni Active Directory siano configurate prima di creare il volume SMB.



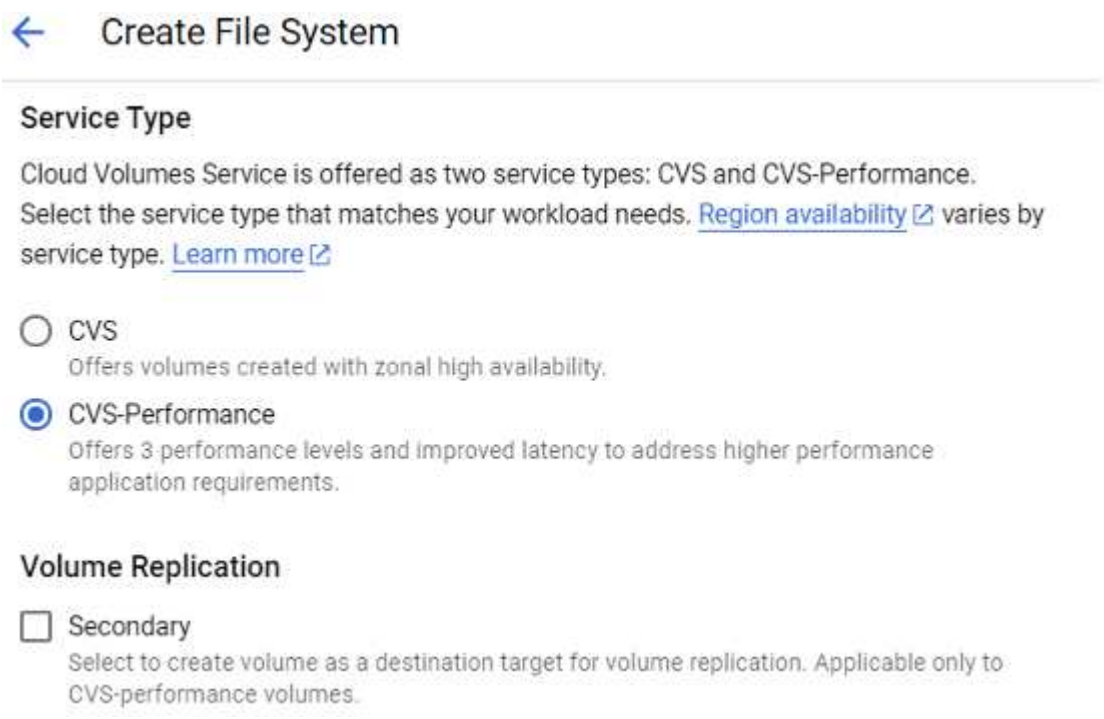
Una volta stabilita la connessione AD, creare il volume con il livello di servizio desiderato. I passaggi sono simili alla creazione di un volume NFS, con la differenza che è necessario selezionare il protocollo

appropriato.

1. Nella console Cloud Volumes, vai alla pagina Volumi e fai clic su Crea.
2. Nella pagina Crea file system, specificare il nome del volume e le etichette di fatturazione come richiesto per i meccanismi di addebito.



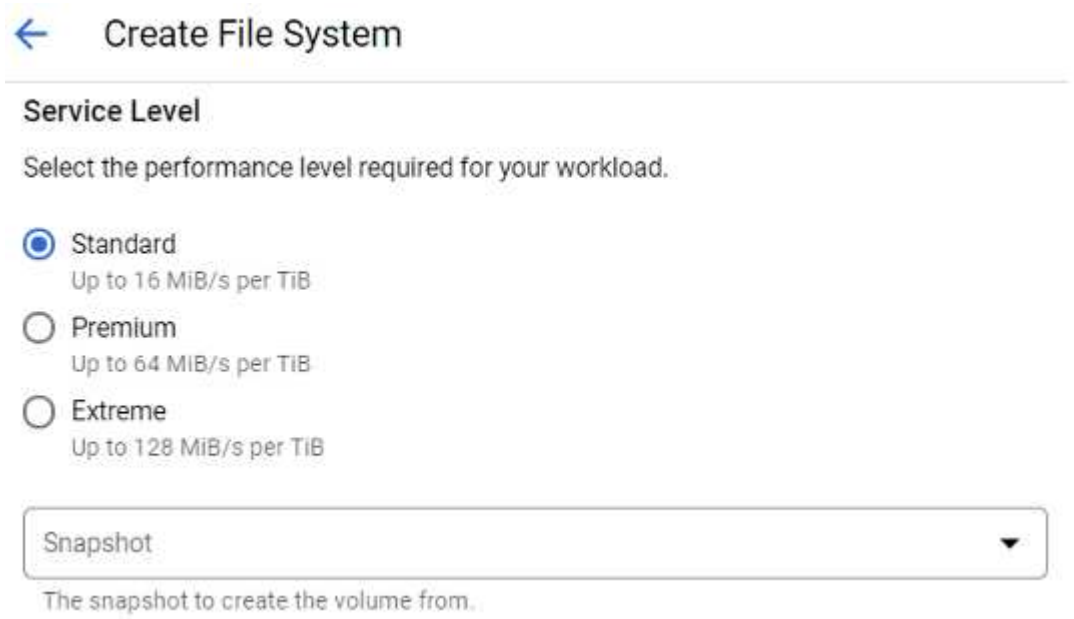
3. Seleziona il servizio appropriato. Per GCVE, scegli NetApp Volumes-Performance e il livello di servizio desiderato per una latenza migliorata e prestazioni più elevate in base ai requisiti del carico di lavoro.



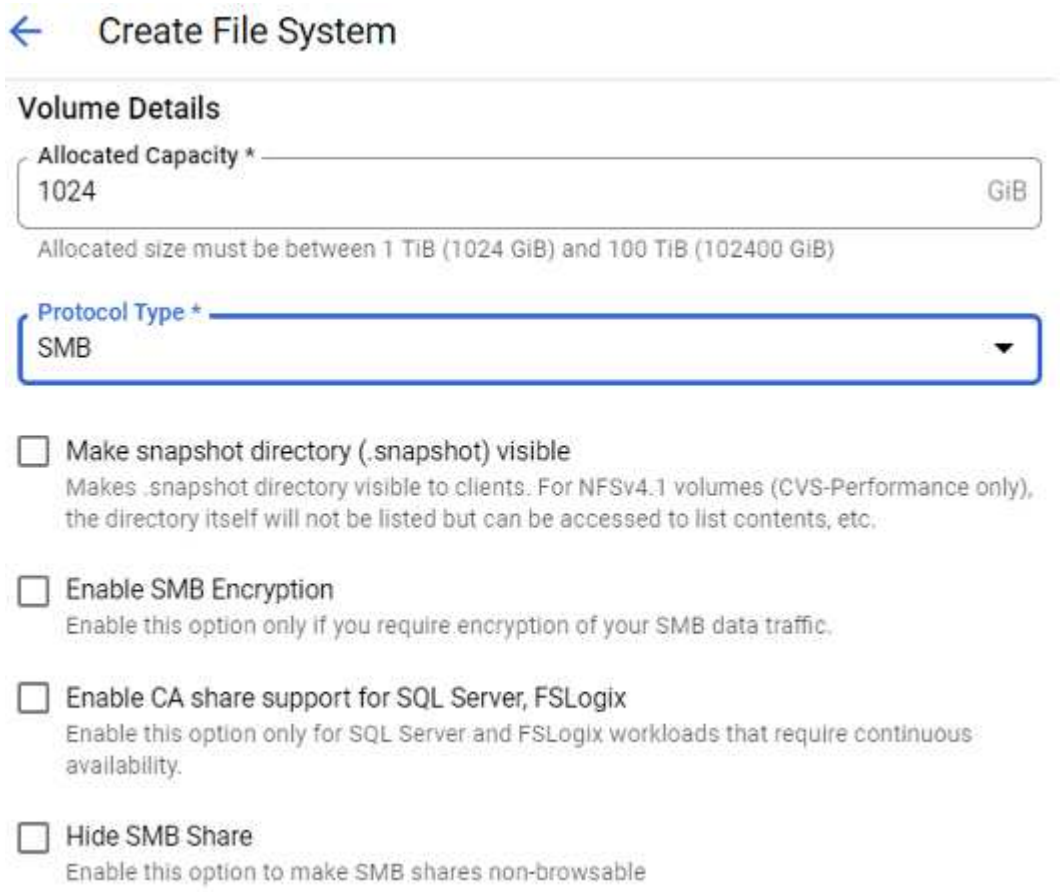
4. Specificare la regione Google Cloud per il volume e il percorso del volume (il percorso del volume deve essere univoco in tutti i volumi cloud nel progetto)



5. Seleziona il livello di prestazioni per il volume.

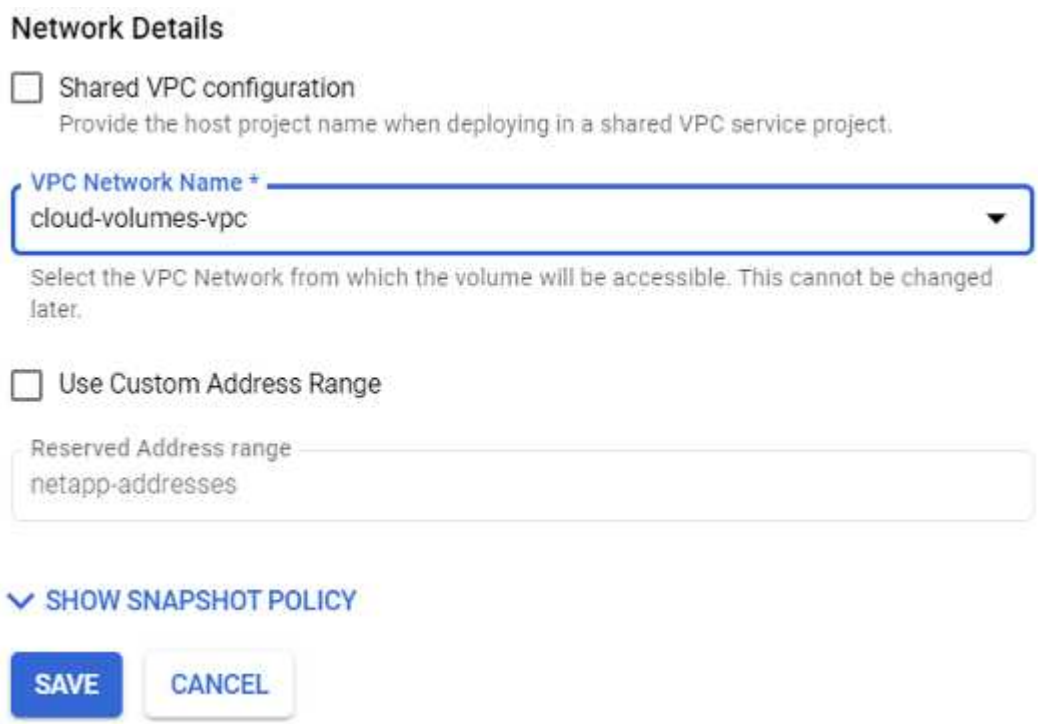


6. Specificare la dimensione del volume e il tipo di protocollo. In questo test viene utilizzato SMB.



7. In questo passaggio, seleziona la rete VPC da cui sarà accessibile il volume. Assicurarsi che il peering VPC sia attivo.

   SUGGERIMENTO: Se il peering VPC non è stato eseguito, verrà visualizzato un pulsante a comparsa che ti guiderà nei comandi di peering. Apri una sessione di Cloud Shell ed esegui i comandi appropriati per eseguire il peering del tuo VPC con il producer di Google Cloud NetApp Volumes. Nel caso in cui tu decida di preparare in anticipo il peering VPC, fai riferimento a questi "istruzioni".



8. Fare clic su Salva per creare il volume.



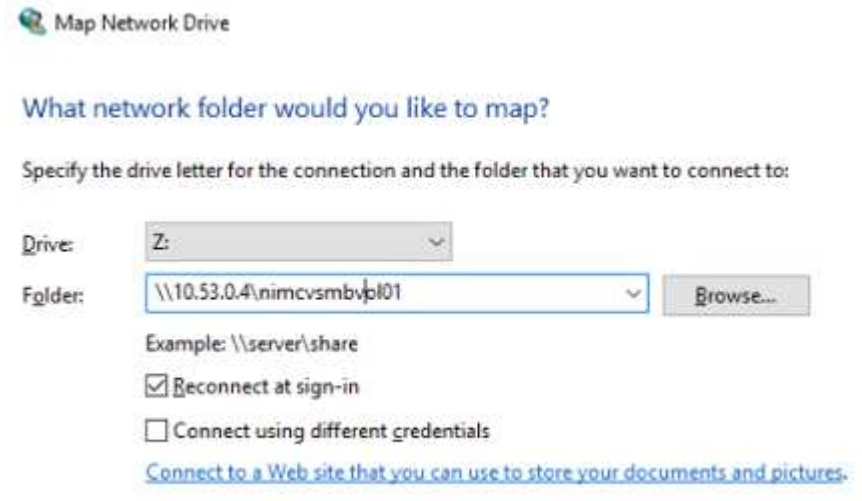
Per montare il volume SMB, procedere come segue:

1. Nella Cloud Console, vai a Cloud Volumes > Volumi.
2. Vai alla pagina dei Volumi
3. Fare clic sul volume SMB per il quale si desidera mappare una condivisione SMB.
4. Scorri verso destra, sotto Mostra altro, fai clic su Istruzioni di montaggio.

Per eseguire il processo di montaggio dall'interno del sistema operativo guest Windows della VM VMware, seguire i passaggi seguenti:

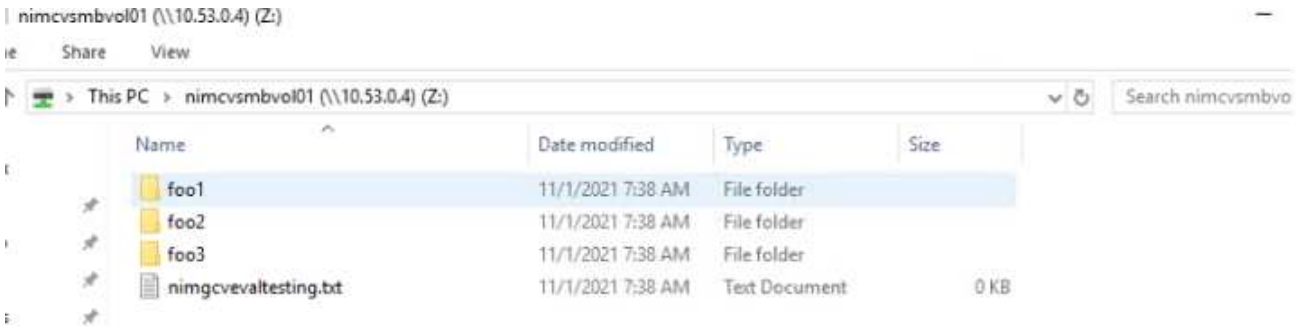
1. Fare clic sul pulsante Start e quindi su Computer.
2. Fare clic su Connetti unità di rete.
3. Nell'elenco Unità, fare clic su una qualsiasi lettera di unità disponibile.
4. Nella casella della cartella, digitare:

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



Per connetterti ogni volta che accedi al computer, seleziona la casella di controllo Riconnetti all'accesso.

5. Fare clic su Fine.



Riepilogo e conclusione: perché NetApp Hybrid Multicloud con VMware

NetApp Cloud Volumes, insieme alle soluzioni VMware per i principali hyperscaler, offre un grande potenziale alle organizzazioni che desiderano sfruttare il cloud ibrido. Il resto di questa sezione illustra i casi d'uso che dimostrano come l'integrazione NetApp Cloud Volumes consenta vere e proprie funzionalità multicloud ibride.

Caso d'uso n. 1: ottimizzazione dello storage

Quando si esegue un esercizio di dimensionamento utilizzando l'output di RVtools, è sempre evidente che la scala della potenza (vCPU/vMem) è parallela allo storage. Spesso le organizzazioni si trovano in una situazione in cui lo spazio di archiviazione richiede unità di dimensioni pari a quelle del cluster, ben oltre la potenza necessaria.

Integrando NetApp Cloud Volumes, le organizzazioni possono realizzare una soluzione cloud basata su vSphere con un semplice approccio di migrazione, senza dover riorganizzare la piattaforma, modificare l'IP o apportare modifiche all'architettura. Inoltre, questa ottimizzazione consente di ridimensionare l'ingombro dello storage mantenendo il numero di host al minimo richiesto in vSphere, senza apportare alcuna modifica alla gerarchia di storage, alla sicurezza o ai file resi disponibili. Ciò consente di ottimizzare l'implementazione e di ridurre il TCO complessivo del 35-45%. Questa integrazione consente inoltre di scalare lo storage da un livello di warm storage a prestazioni di livello di produzione in pochi secondi.

Caso d’uso n. 2: migrazione nel cloud

Le organizzazioni sono sotto pressione per migrare le applicazioni dai data center locali al cloud pubblico per molteplici motivi: l’imminente scadenza di un contratto di locazione; una direttiva finanziaria per passare dalla spesa in conto capitale (capex) alla spesa in spese operative (opex); o semplicemente un mandato dall’alto verso il basso per spostare tutto sul cloud.

Quando la velocità è fondamentale, è possibile adottare solo un approccio di migrazione semplificato, perché la riorganizzazione e il refactoring delle applicazioni per adattarle alla specifica piattaforma IaaS del cloud sono operazioni lente e costose, che spesso richiedono mesi. Combinando NetApp Cloud Volumes con la replica SnapMirror a banda larga efficiente per l’archiviazione connessa agli ospiti (inclusi RDM in combinazione con copie Snapshot coerenti con l’applicazione e HCX, migrazione specifica del cloud (ad esempio Azure Migrate) o prodotti di terze parti per la replica delle VM), questa transizione è ancora più semplice rispetto all’affidarsi a meccanismi di filtri I/O che richiedono molto tempo.

Caso d’uso n. 3: espansione del data center

Quando un data center raggiunge i limiti di capacità a causa di picchi di domanda stagionali o semplicemente di una crescita organica costante, passare a VMware ospitato nel cloud insieme a NetApp Cloud Volumes è una soluzione semplice. Sfruttando NetApp Cloud Volumes è possibile creare, replicare ed espandere lo storage con estrema facilità, garantendo elevata disponibilità in tutte le zone di disponibilità e capacità di scalabilità dinamica. Sfruttando NetApp Cloud Volumes è possibile ridurre al minimo la capacità del cluster host, eliminando la necessità di cluster estesi.

Caso d’uso n. 4: ripristino di emergenza sul cloud

In un approccio tradizionale, se si verifica un disastro, le VM replicate sul cloud richiederebbero la conversione alla piattaforma hypervisor del cloud stesso prima di poter essere ripristinate: un’attività non gestibile durante una crisi.

Utilizzando NetApp Cloud Volumes per l’archiviazione connessa agli ospiti tramite la replica SnapCenter e SnapMirror da locale insieme a soluzioni di virtualizzazione cloud pubblico, è possibile ideare un approccio migliore per il disaster recovery che consenta il ripristino delle repliche delle VM su un’infrastruttura VMware SDDC completamente coerente insieme a strumenti di ripristino specifici per il cloud (ad esempio Azure Site Recovery) o strumenti di terze parti equivalenti come Veeam. Questo approccio consente inoltre di eseguire rapidamente esercitazioni di disaster recovery e di ripristino da ransomware. Ciò consente inoltre di passare alla produzione completa per i test o in caso di emergenza, aggiungendo host su richiesta.

Caso d’uso n. 5: modernizzazione delle applicazioni

Una volta che le applicazioni saranno nel cloud pubblico, le organizzazioni vorranno sfruttare le centinaia di potenti servizi cloud per modernizzarle ed estenderle. Utilizzando NetApp Cloud Volumes, la modernizzazione è un processo semplice perché i dati dell’applicazione non sono bloccati in vSAN e consentono la mobilità dei dati per un’ampia gamma di casi d’uso, tra cui Kubernetes.

Conclusione

Che si punti a un cloud all-cloud o ibrido, NetApp Cloud Volumes offre eccellenti opzioni per distribuire e gestire i carichi di lavoro delle applicazioni insieme ai servizi file e ai protocolli a blocchi, riducendo al contempo il TCO rendendo i requisiti dei dati uniformi al livello dell’applicazione.

Qualunque sia il caso d’uso, scegli il tuo cloud/hyperscaler preferito insieme a NetApp Cloud Volumes per ottenere rapidamente i vantaggi del cloud, un’infrastruttura e operazioni coerenti su cloud locali e multipli, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale.

Si tratta dello stesso processo e delle stesse procedure note utilizzate per collegare l'archiviazione. Ricorda che è solo la posizione dei dati a essere cambiata con i nuovi nomi; gli strumenti e i processi rimangono gli stessi e NetApp Cloud Volumes aiuta a ottimizzare l'implementazione complessiva.

Casi d'uso del cloud ibrido VMware

Casi d'uso per NetApp Hybrid Multicloud con VMware

Una panoramica dei casi d'uso importanti per l'organizzazione IT quando si pianificano implementazioni cloud ibride o cloud-first.

Casi d'uso popolari

I casi d'uso includono:

- Recupero dopo un disastro,
- Hosting di carichi di lavoro durante la manutenzione del data center, * burst rapidi in cui sono richieste risorse aggiuntive oltre a quelle fornite nel data center locale,
- Espansione del sito VMware,
- Migrazione rapida verso il cloud,
- Sviluppo/test e
- Modernizzazione delle app sfruttando le tecnologie supplementari del cloud.

In questa documentazione, i riferimenti ai carichi di lavoro cloud saranno dettagliati utilizzando i casi d'uso VMware. Questi casi d'uso sono:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Migrare
- Estendere

All'interno del percorso IT

La maggior parte delle organizzazioni è impegnata in un percorso di trasformazione e modernizzazione. Nell'ambito di questo processo, le aziende stanno cercando di utilizzare i propri investimenti VMware esistenti, sfruttando al contempo i vantaggi del cloud ed esplorando modi per rendere il processo di migrazione il più fluido possibile. Questo approccio renderebbe i loro sforzi di modernizzazione molto più semplici, perché i dati sono già nel cloud.

La risposta più semplice a questo scenario è l'offerta VMware in ogni hyperscaler. Analogamente a NetApp Cloud Volumes, VMware offre un modo per spostare o estendere gli ambienti VMware on-premise su qualsiasi cloud, consentendo di mantenere le risorse, le competenze e gli strumenti on-premise esistenti eseguendo i carichi di lavoro in modo nativo nel cloud. Ciò riduce i rischi perché non ci saranno interruzioni del servizio né necessità di modifiche IP e offre al team IT la possibilità di operare come fa in sede utilizzando le competenze e gli strumenti esistenti. Ciò può portare a migrazioni cloud accelerate e a una transizione molto più fluida verso un'architettura Multicloud ibrida.

Comprendere l'importanza delle opzioni di archiviazione NFS supplementari

Sebbene VMware in qualsiasi cloud offra funzionalità ibride uniche a ogni cliente, le limitate opzioni di archiviazione NFS supplementari ne hanno limitato l'utilità per le organizzazioni con carichi di lavoro ad alta

intensità di storage. Poiché lo storage è direttamente collegato agli host, l'unico modo per scalare lo storage è aggiungere più host, ma ciò può aumentare i costi del 35-40 percento o più per i carichi di lavoro che richiedono un utilizzo intensivo dello storage. Questi carichi di lavoro necessitano solo di spazio di archiviazione aggiuntivo, non di potenza aggiuntiva. Ma questo significa pagare per host aggiuntivi.

Consideriamo questo scenario:

Un cliente necessita solo di cinque host per CPU e memoria, ma ha molte esigenze di archiviazione e necessita di 12 host per soddisfare i requisiti di archiviazione. Questa esigenza finisce per far pendere davvero la bilancia finanziaria, costringendo ad acquistare potenza aggiuntiva quando in realtà serve solo ad aumentare lo spazio di archiviazione.

Quando si pianifica l'adozione e la migrazione al cloud, è sempre importante valutare l'approccio migliore e intraprendere la strada più semplice che riduca gli investimenti totali. L'approccio più comune e semplice per qualsiasi migrazione di applicazioni è il rehosting (noto anche come lift and shift), in cui non è prevista alcuna conversione di macchine virtuali (VM) o dati. L'utilizzo di NetApp Cloud Volumes con VMware Software-Defined Data Center (SDDC), integrando al contempo vSAN, offre una semplice opzione di trasferimento dati.

Soluzioni NetApp per VMware negli Hyperscaler

Scopri di più sulle soluzioni che NetApp offre all'ambiente VMware in ciascuno degli hyperscaler: dalla migrazione dei flussi di lavoro, all'estensione/bursting nel cloud, al backup/ripristino e al disaster recovery.

Soluzioni NetApp per ambienti VMware

Che si operi in un modello di cloud ibrido o in un modello "cloud first", NetApp offre un'ampia gamma di soluzioni per soddisfare i casi d'uso più comuni per la gestione dei carichi di lavoro in un modello cloud o cloud ibrido.

NetApp offre anche soluzioni per l'archiviazione fornita come archiviazione in-guest (connessa all'ospite) o come datastore NFS supplementare in ciascuno degli hyperscaler. Tutte le soluzioni sono categorizzate in base alla classificazione VMware dei carichi di lavoro cloud. Tali classificazioni includono:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Migrare
- Estendere

Per maggiori dettagli sulle soluzioni disponibili per ciascun hyperscaler, visitare:

- "Soluzioni per AWS / VMC"
- "Soluzioni per Azure / AVS"
- "Soluzioni per GCP / GCVE"

Soluzioni NetApp per Amazon VMware Managed Cloud (VMC)

Scopri di più sulle soluzioni che NetApp porta su AWS.

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

- Protezione (inclusi sia Disaster Recovery che Backup/Ripristino)

- Migrare
- Estendere

Esplora le soluzioni disponibili nelle sezioni seguenti.

Proteggere

- "Disaster Recovery con VMC su AWS (connessi tramite guest)"
- "Veeam Backup Restore in VMC con FSx ONTAP"
- "Disaster Recovery (DRO) con FSx ONTAP e VMC"
- "Utilizzo di Veeam Replication e FSx ONTAP per il disaster recovery su VMware Cloud su AWS"

Migrare

- "Migrazione dei carichi di lavoro sul datastore FSx ONTAP utilizzando VMware HCX"

Estendere

PROSSIMAMENTE!!

Soluzioni NetApp per Azure VMware Solution (AVS)

Scopri di più sulle soluzioni che NetApp porta in Azure.

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

- Protezione (inclusi sia Disaster Recovery che Backup/Ripristino)
- Migrare
- Estendere

Esplora le soluzioni disponibili nelle sezioni seguenti.

Proteggere

- "Disaster Recovery con ANF e JetStream (datastore NFS supplementare)"
- "Disaster Recovery con ANF e CVO (archiviazione connessa agli ospiti)"
- "Disaster Recovery (DRO) con ANF e AVS"
- "Utilizzo di Veeam Replication e del datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware"

Migrare

- "Migrazione dei carichi di lavoro al datastore di Azure NetApp Files utilizzando VMware HCX"

Estendere

PROSSIMAMENTE!!

Soluzioni NetApp per Google Cloud VMware Engine (GCVE)

Scopri di più sulle soluzioni che NetApp porta a GCP.

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

- Protezione (inclusi sia Disaster Recovery che Backup/Ripristino)
- Migrare
- Estendere

Esplora le soluzioni disponibili nelle sezioni seguenti.

Proteggere

- "Disaster recovery delle applicazioni con SnapCenter, Cloud Volumes ONTAP e Veeam Replication"
- "Ripristino di emergenza coerente con le applicazioni con NetApp SnapCenter e Veeam Replication su volumi NetApp su GCVE"

Migrare

- "Migrazione del carico di lavoro tramite VMware HCX nel datastore NFS Google Cloud NetApp Volumes"
- "Replica VM tramite Veeam su Google Cloud NetApp Volumes NFS datastore"

Estendere

PROSSIMAMENTE!!

NetApp per AWS/VMC

Funzionalità NetApp per AWS VMC

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

Passa alla sezione del contenuto desiderato selezionando tra le seguenti opzioni:

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

Configurazione di VMC in AWS

Come per l'ambiente on-premise, la pianificazione di un ambiente di virtualizzazione basato su cloud è fondamentale per un ambiente di produzione di successo per la creazione di VM 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 .

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

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura VMware Cloud per AWS
- Connetti VMware Cloud a FSx ONTAP

Visualizza il dettaglio"passaggi di configurazione per VMC" .

Opzioni di archiviazione NetApp per VMC

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

Per favore visita"Opzioni di archiviazione NetApp supportate" per maggiori informazioni.

AWS supporta l'archiviazione NetApp nelle seguenti configurazioni:

- FSx ONTAP come storage connesso agli ospiti
- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- FSx ONTAP come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione di connessione guest per VMC" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per VMC" .

Casi d'uso della soluzione

Grazie alle soluzioni cloud NetApp e VMware, molti casi d'uso sono semplici da implementare nel tuo AWS VMC. Per ciascuna delle aree cloud definite da VMware vengono definiti i casi d'uso:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Estendere
- Migrare

"Esplora le soluzioni NetApp per AWS VMC"

Proteggi i carichi di lavoro su AWS/VMC

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

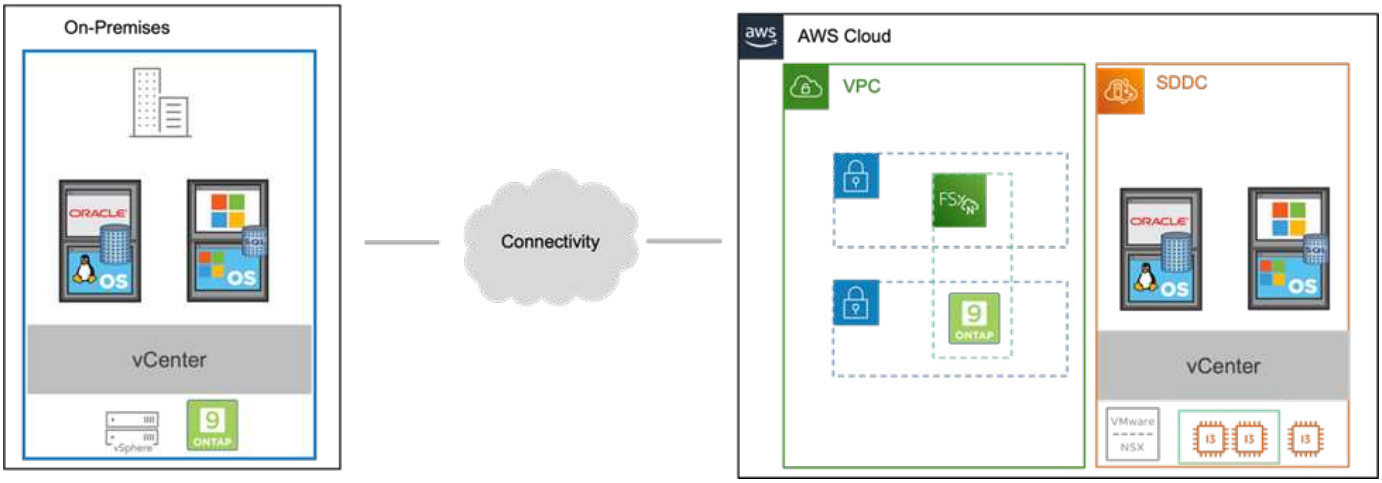
Un ambiente e un piano di disaster recovery (DR) collaudati sono essenziali per le organizzazioni, per garantire che le applicazioni aziendali critiche possano essere ripristinate rapidamente in caso di un'interruzione importante. Questa soluzione si concentra sulla dimostrazione di casi d'uso DR con particolare attenzione alle tecnologie VMware e NetApp , sia in locale che con VMware Cloud su AWS.

Panoramica

NetApp vanta una lunga tradizione 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 anche con le opzioni connesse agli ospiti nel cloud e con le recenti integrazioni con i datastore NFS. Questa soluzione si concentra sul caso d'uso comunemente denominato storage connesso agli ospiti.

Nello storage connesso agli ospiti, il VMDK ospite viene distribuito su un datastore fornito da VMware e i dati dell'applicazione sono ospitati su iSCSI o NFS e mappati direttamente sulla VM. Per illustrare uno scenario DR, come mostrato nella figura seguente, vengono utilizzate le applicazioni Oracle e MS SQL.



Presupposti, prerequisiti e panoramica dei componenti

Prima di distribuire questa soluzione, rivedere la panoramica dei componenti, i prerequisiti richiesti per distribuire la soluzione e le ipotesi formulate nella documentazione di questa soluzione.

"Requisiti, prerequisiti e pianificazione della soluzione DR"

Esecuzione di 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 , garantisce la replicazione dei dati ad alta velocità tra il nostro cluster AFF locale e FSx ONTAP . Inoltre, Veeam Backup & Replication offre funzionalità di backup e ripristino per le nostre macchine virtuali.

In questa sezione, illustreremo la configurazione di SnapCenter, SnapMirror e Veeam sia per il backup che per il ripristino.

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

Configurare le relazioni e le pianificazioni di conservazione SnapMirror

SnapCenter può aggiornare le relazioni SnapMirror all'interno del sistema di archiviazione primario (primario > mirror) e nei sistemi di archiviazione secondari (primario > vault) allo scopo di archiviazione e conservazione a lungo termine. Per fare ciò, 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 peering tramite peering Amazon VPC, un gateway di transito, AWS Direct Connect o una VPN AWS.

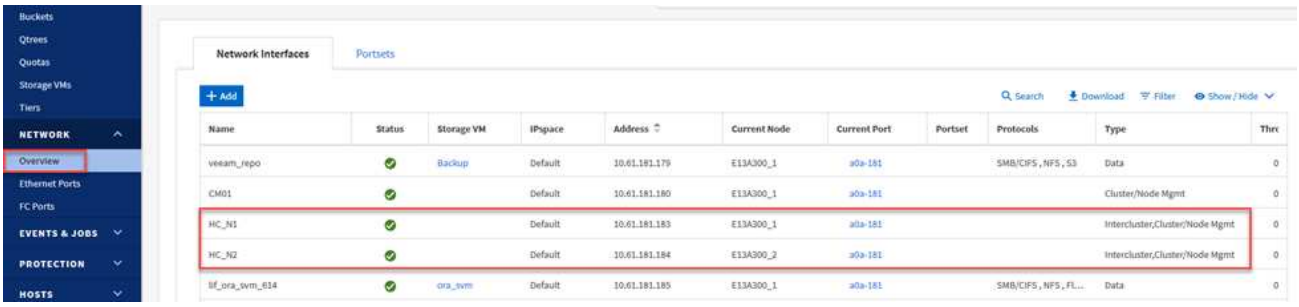
Per impostare le relazioni SnapMirror tra un sistema ONTAP locale e FSx ONTAP sono necessari i seguenti passaggi:

Fare riferimento al "FSx ONTAP – Guida utente ONTAP" per ulteriori informazioni sulla creazione di relazioni SnapMirror con FSx.

▼ Registra le interfacce logiche Intercluster di origine e destinazione

Per il sistema ONTAP di origine residente in locale, è possibile recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

1. In ONTAP System Manager, vai alla pagina Panoramica di rete e recupera gli indirizzi IP di tipo: Intercluster configurati per comunicare con l'AWS VPC in cui è installato FSx.



2. Per recuperare gli indirizzi IP 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

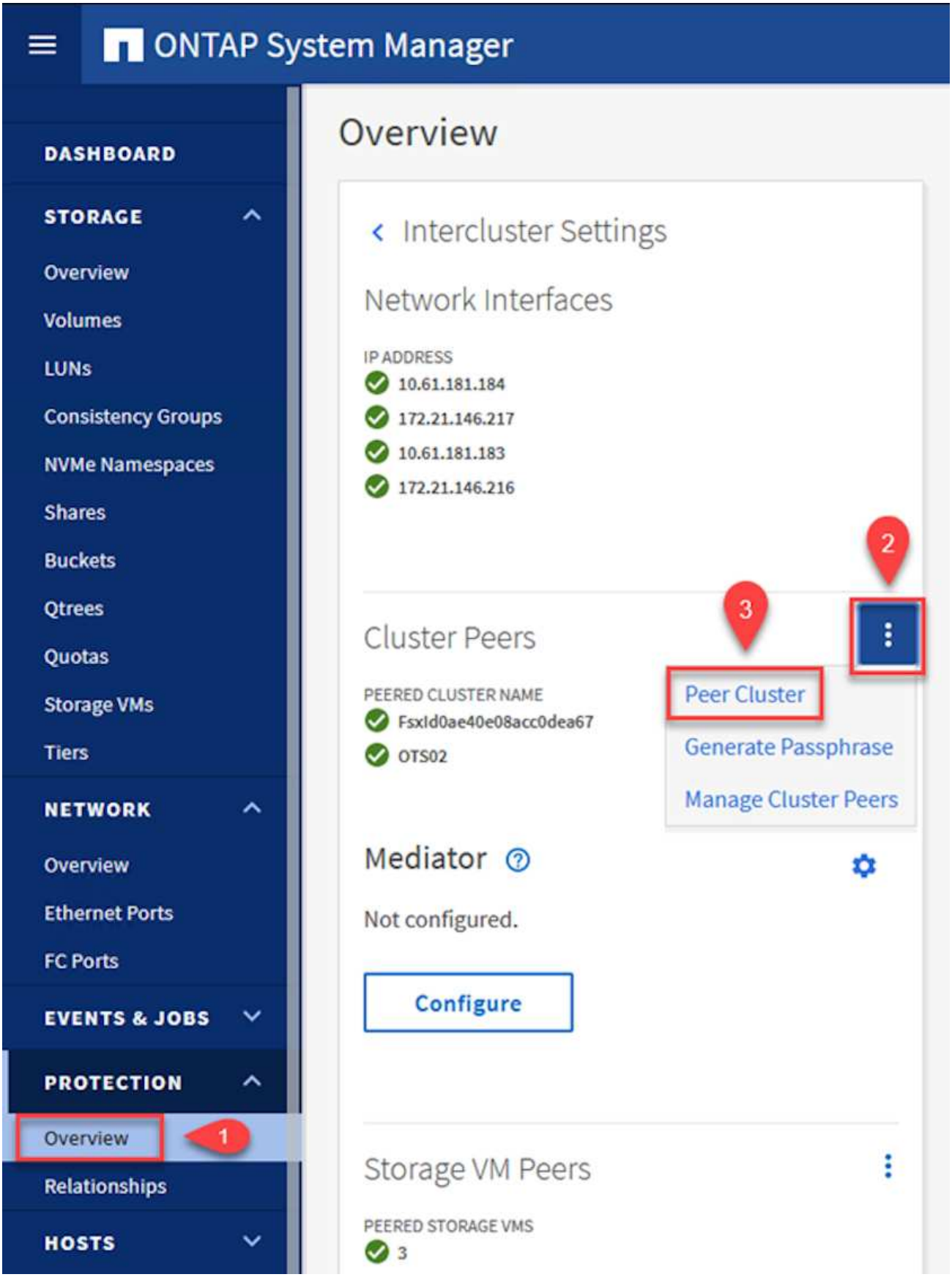
Per stabilire il peering tra cluster ONTAP , è necessario che una passphrase univoca immessa nel cluster ONTAP di avvio venga confermata nell'altro cluster peer.

1. Impostare il peering sul cluster FSx di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca che verrà utilizzata in seguito sul cluster di origine per finalizzare 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 ONTAP System Manager o la CLI. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer

Cluster.



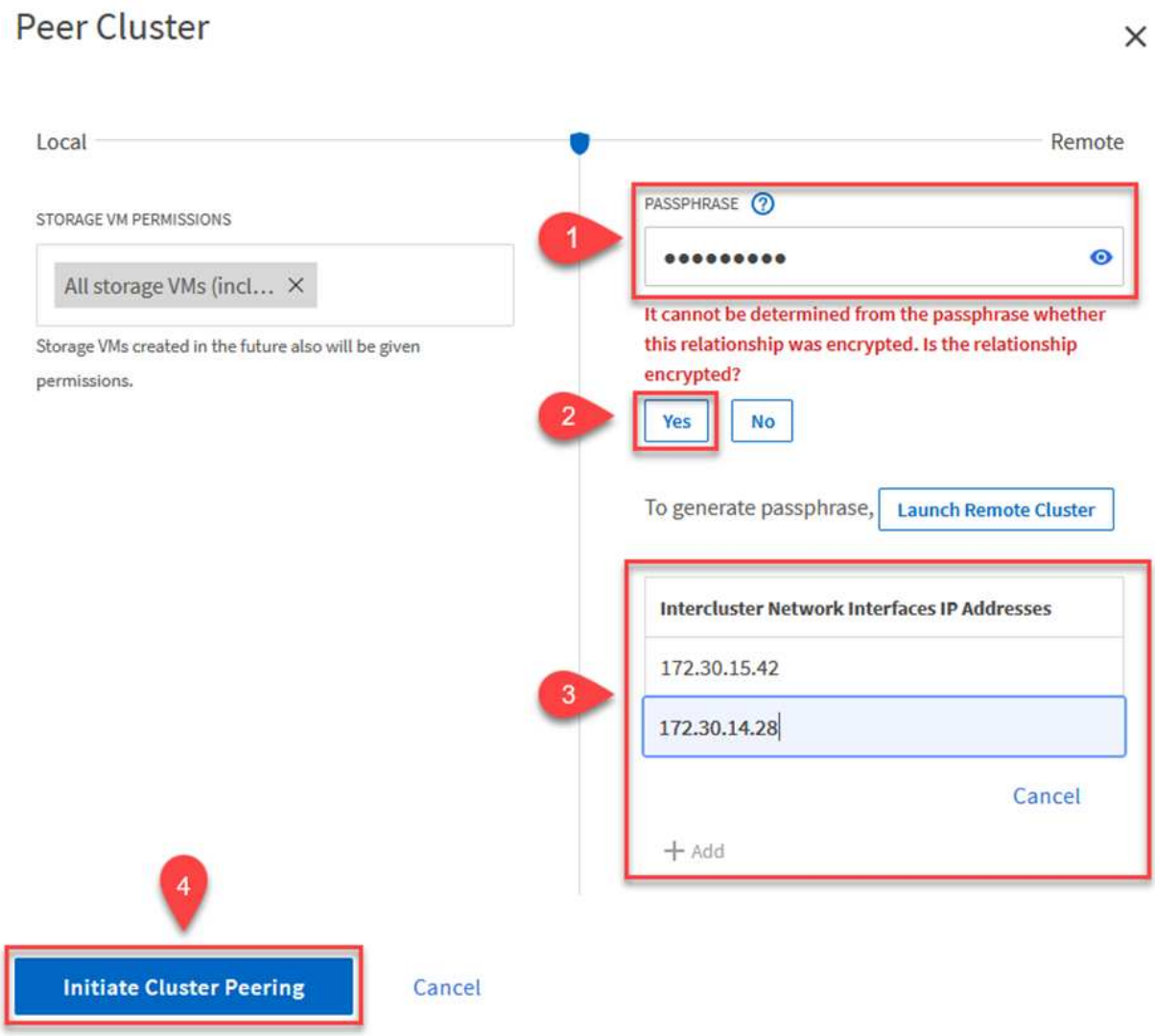
3. Nella finestra di dialogo Peer Cluster, compilare le informazioni richieste:

a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer sul cluster FSx di destinazione.

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

c. Immettere l'indirizzo/gli indirizzi IP LIF intercluster del cluster FSx di destinazione.

d. Fare clic su Avvia peering cluster per finalizzare 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
```

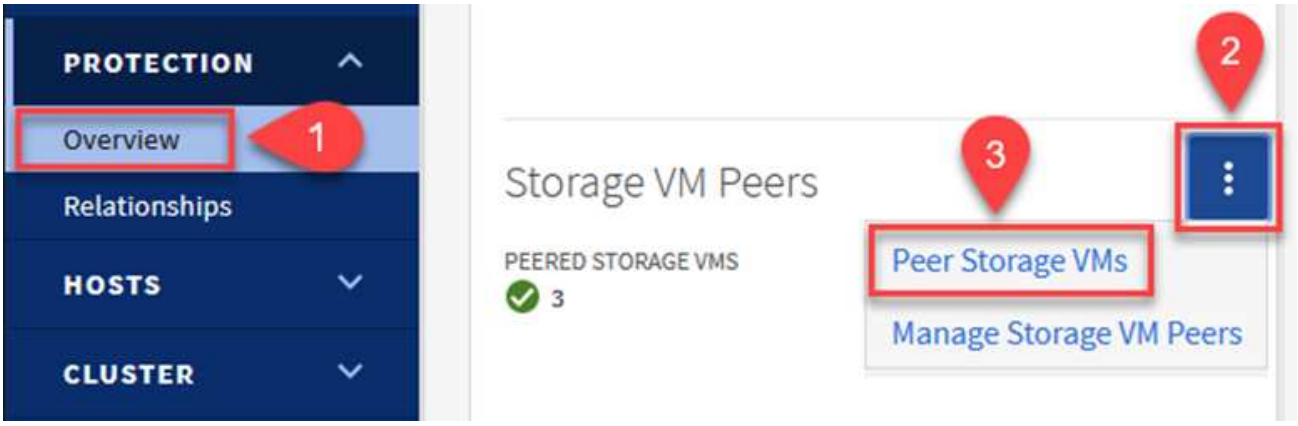
▼ Stabilire una relazione di peering SVM

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

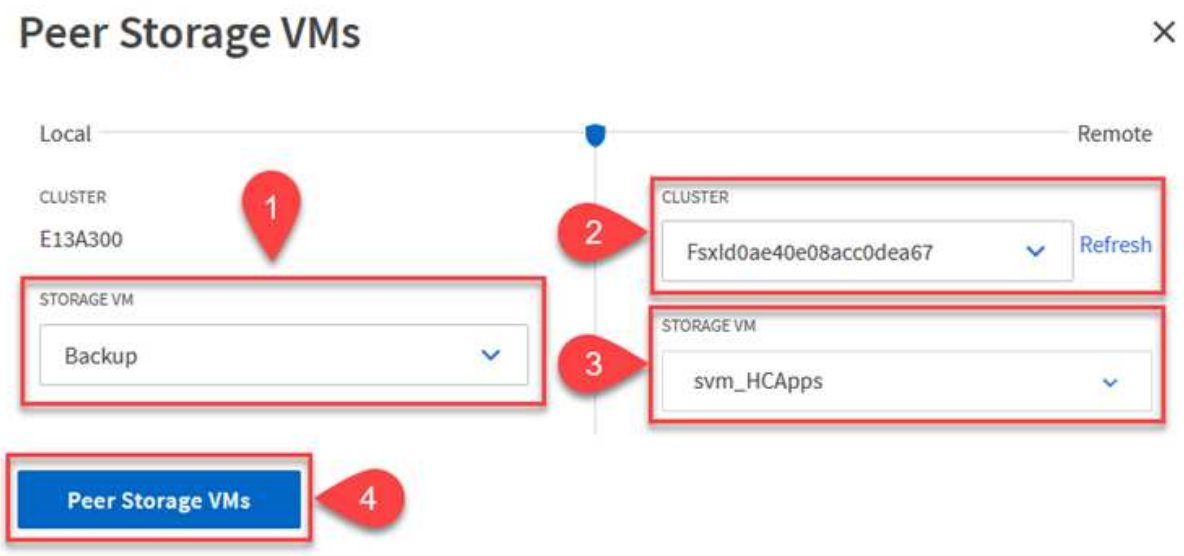
1. Dal cluster FSx di origine, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

```
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 ONTAP System Manager o con la CLI.
3. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Storage VM in Storage VM Peer.



4. Nella finestra di dialogo della VM di archiviazione peer, compilare i campi obbligatori:
   - La VM di archiviazione di origine
   - Il cluster di destinazione
   - La VM di archiviazione di destinazione



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

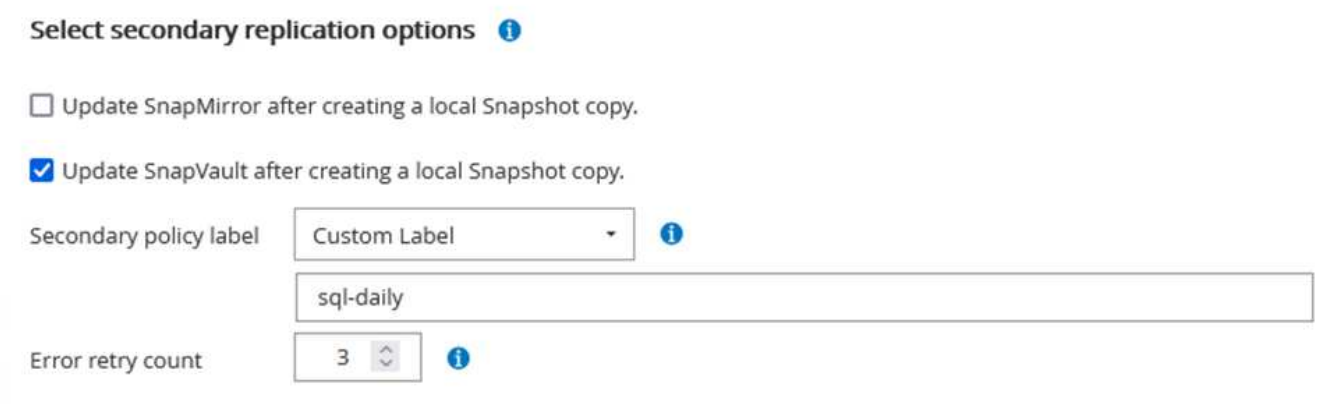
▼ **Creare un criterio di conservazione degli snapshot**

SnapCenter gestisce le pianificazioni di conservazione per i backup presenti come copie snapshot sul sistema di archiviazione primario. Ciò viene stabilito durante la creazione di una policy in SnapCenter. SnapCenter non gestisce i criteri di conservazione per i backup conservati su sistemi di archiviazione secondari. Queste policy vengono gestite separatamente tramite una policy SnapMirror creata sul cluster FSx secondario e associata 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 .

ⓘ Nell'archiviazione secondaria, queste etichette vengono abbinate alle regole dei criteri associati al volume di destinazione allo scopo di imporre la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutti gli snapshot generati come parte di un criterio utilizzato per i backup giornalieri del database SQL Server e dei volumi di registro.



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

Per prima cosa devi creare un criterio SnapMirror con regole che stabiliscano il numero di copie snapshot da conservare.

1. Creare la policy SnapMirror sul cluster FSx.

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

2. Aggiungere regole alla policy con etichette SnapMirror che corrispondono alle etichette della policy secondaria specificate nelle policy SnapCenter .

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

Lo script seguente fornisce un esempio di regola che potrebbe essere aggiunta a una policy:

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

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

▼ **Crea volumi di destinazione**

Per creare un volume di destinazione su FSx che sarà il destinatario delle copie snapshot dai nostri 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 SnapMirror tra i volumi di origine e di destinazione**

Per creare una relazione SnapMirror tra un volume di origine e uno 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
```

▼ **Inizializza le relazioni SnapMirror**

Inizializza 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
```

Distribuisci e configura il server Windows SnapCenter in locale.

▼ **Distribuisci Windows SnapCenter Server in locale**

Questa soluzione utilizza NetApp SnapCenter per eseguire backup coerenti con le applicazioni dei database SQL Server e Oracle. In combinazione con Veeam Backup & Replication per il backup dei VMDK delle macchine virtuali, si ottiene una soluzione completa di disaster recovery per data center on-premise e basati su cloud.

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

Il SnapCenter software può essere ottenuto presso "questo collegamento" .

Dopo l'installazione, è possibile accedere alla console SnapCenter da un browser Web utilizzando *https://Virtual_Cluster_IP_or_FQDN:8146*.

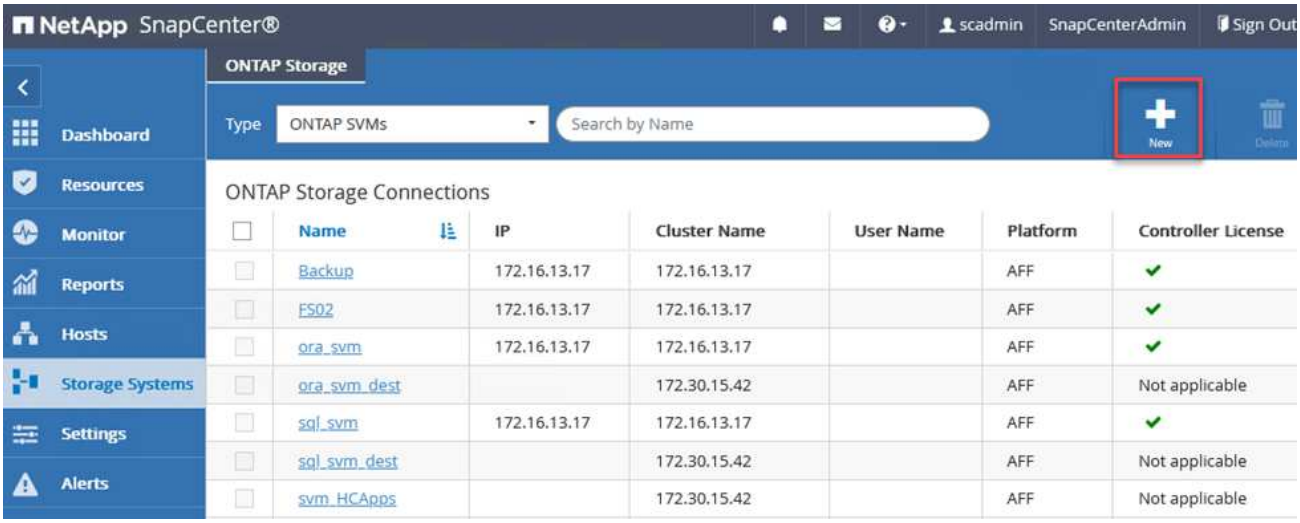
Dopo aver effettuato l'accesso alla console, è necessario configurare SnapCenter per il backup dei

database SQL Server e Oracle.

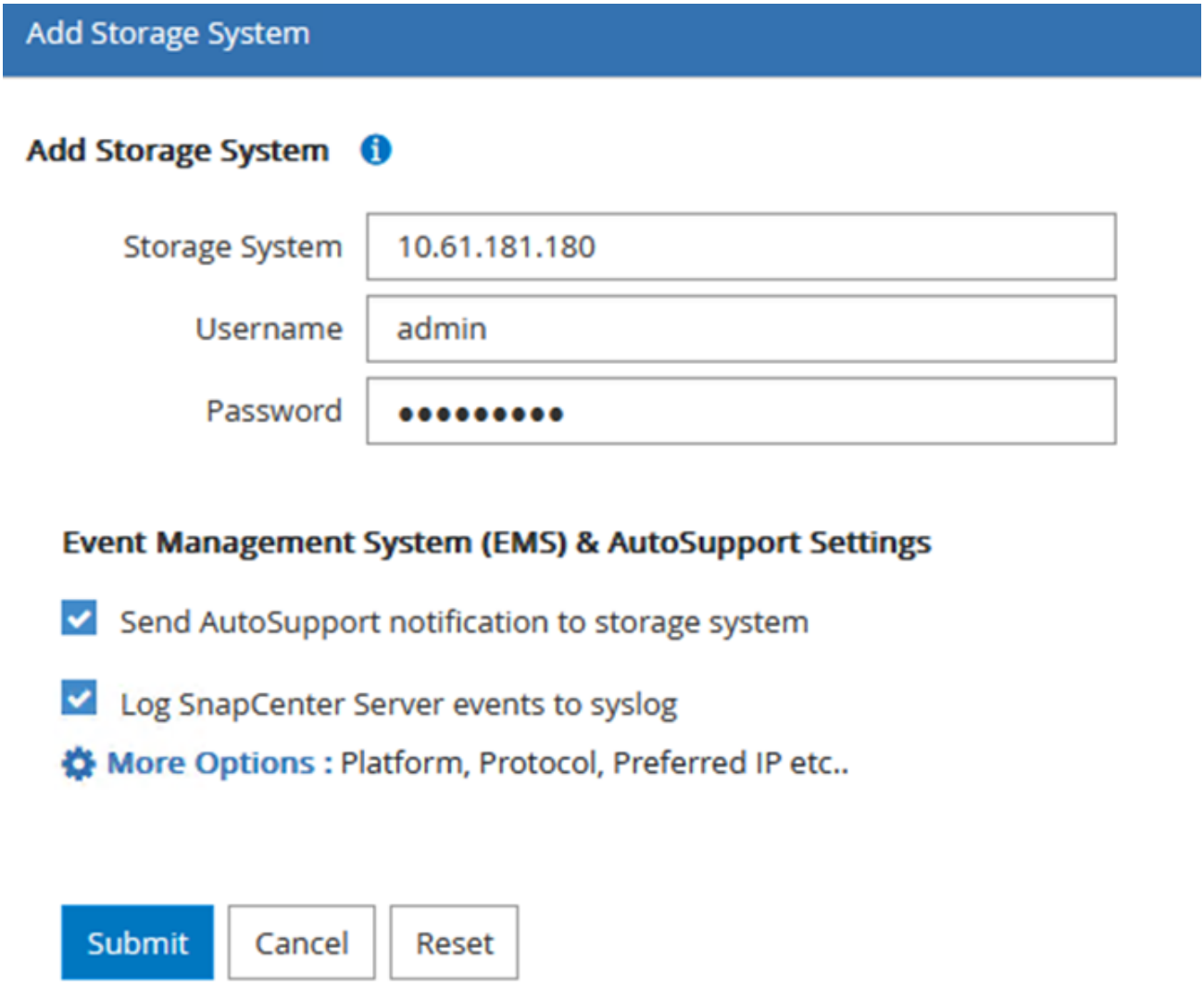
▼ **Aggiungere controller di archiviazione a SnapCenter**

Per aggiungere controller di archiviazione a SnapCenter, completare i seguenti passaggi:

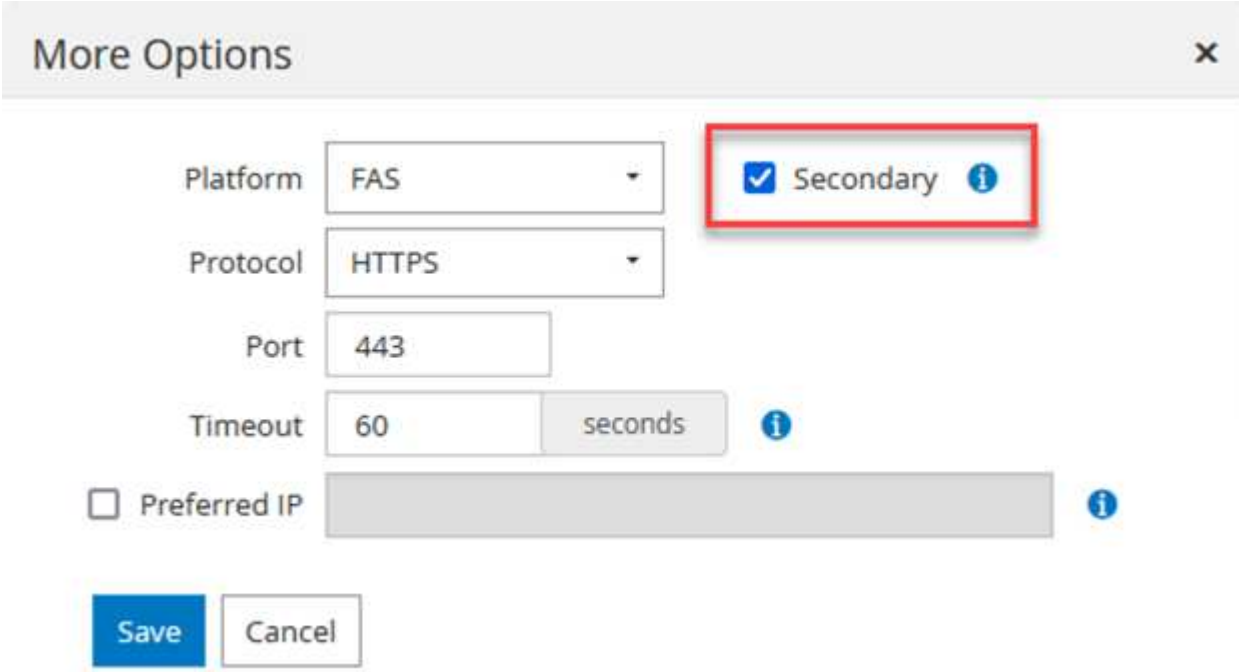
1. Dal menu a sinistra, seleziona Sistemi di archiviazione e poi fai clic su Nuovo per iniziare il processo di aggiunta dei controller di archiviazione a SnapCenter.



2. Nella finestra di dialogo Aggiungi sistema di archiviazione, aggiungere l'indirizzo IP di gestione per il cluster ONTAP locale, nonché il nome utente e la password. Quindi fare clic su Invia per iniziare l'individuazione del sistema di archiviazione.



3. Ripetere questa procedura per aggiungere il sistema FSx ONTAP a SnapCenter. In questo caso, seleziona Altre opzioni nella parte inferiore della finestra Aggiungi sistema di archiviazione e fai clic sulla casella di controllo Secondario per designare il sistema FSx come sistema di archiviazione secondario aggiornato con copie SnapMirror o con i nostri snapshot di backup primari.

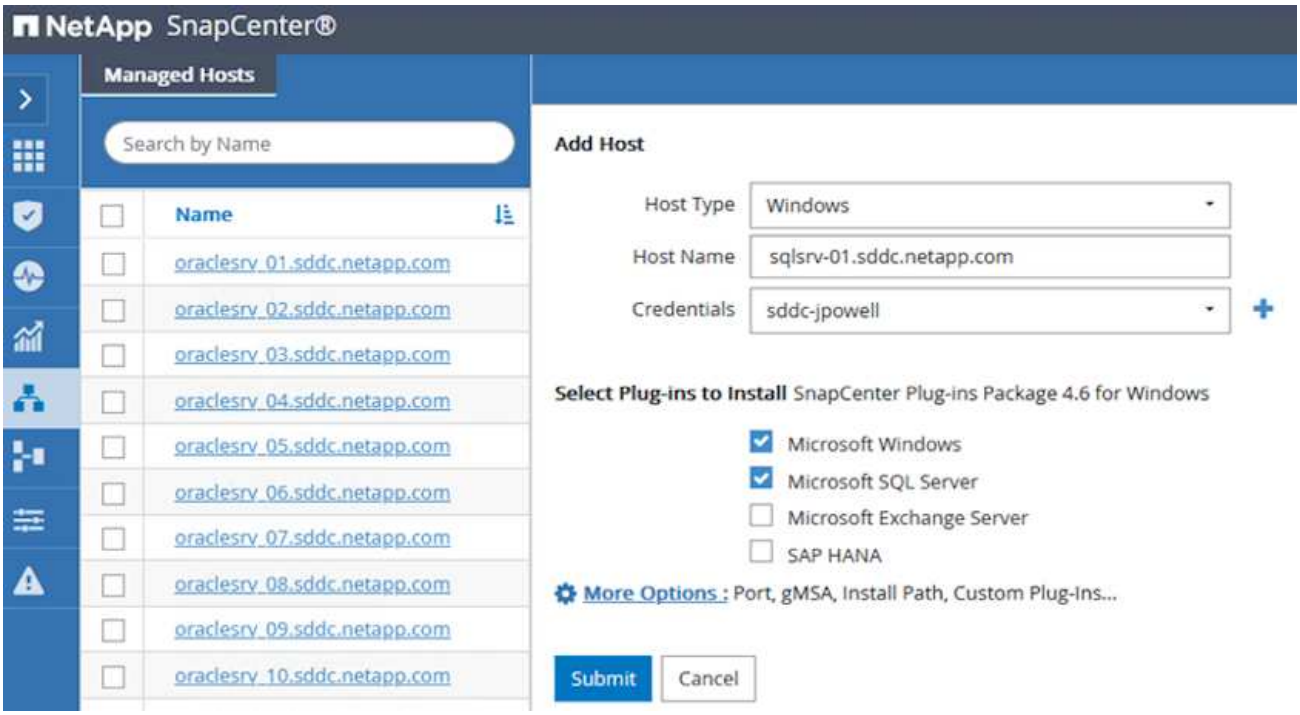


Per ulteriori informazioni relative all'aggiunta di sistemi di archiviazione a SnapCenter, consultare la documentazione all'indirizzo "questo collegamento" .

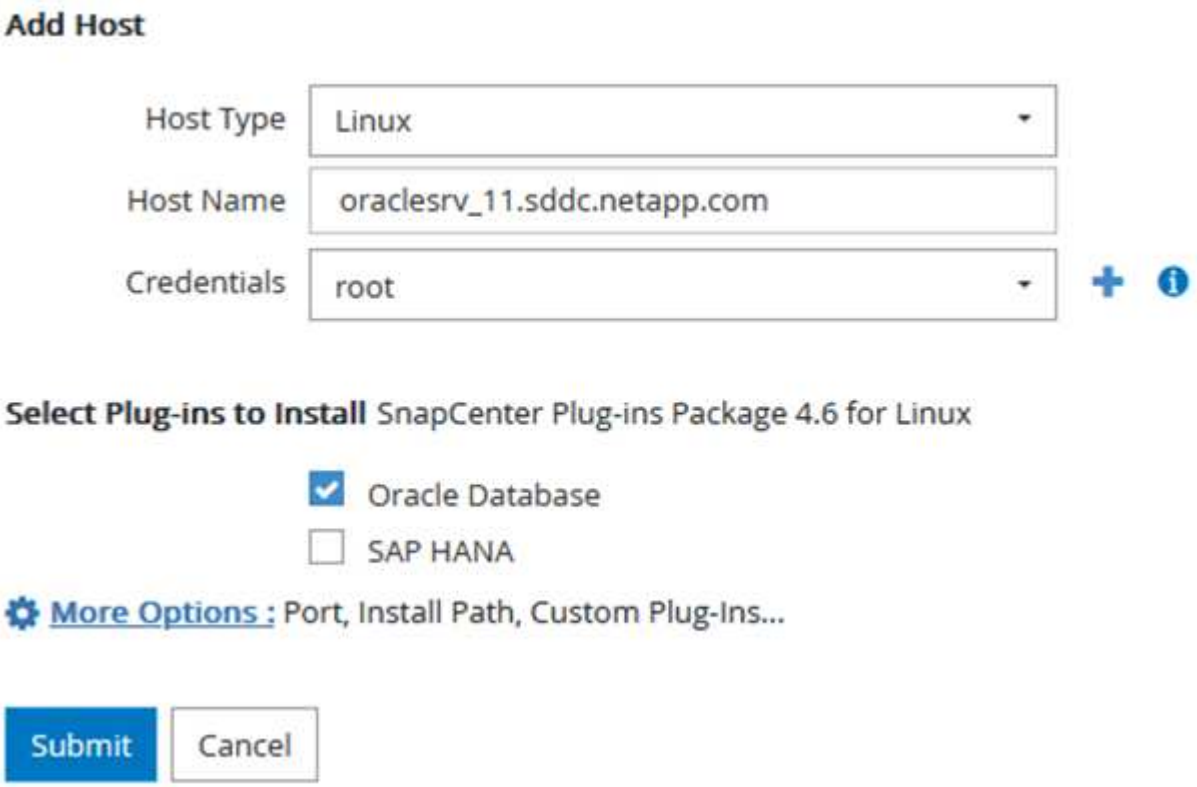
▼ **Aggiungi host a SnapCenter**

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

1. Dal menu a sinistra, seleziona Host e poi fai clic su Aggiungi per iniziare il processo di aggiunta dei controller di archiviazione a SnapCenter.
2. Nella finestra Aggiungi host, aggiungi il tipo di host, il nome host e le credenziali del sistema host. Seleziona il tipo di plug-in. Per SQL Server, selezionare il plug-in Microsoft Windows e Microsoft SQL Server.



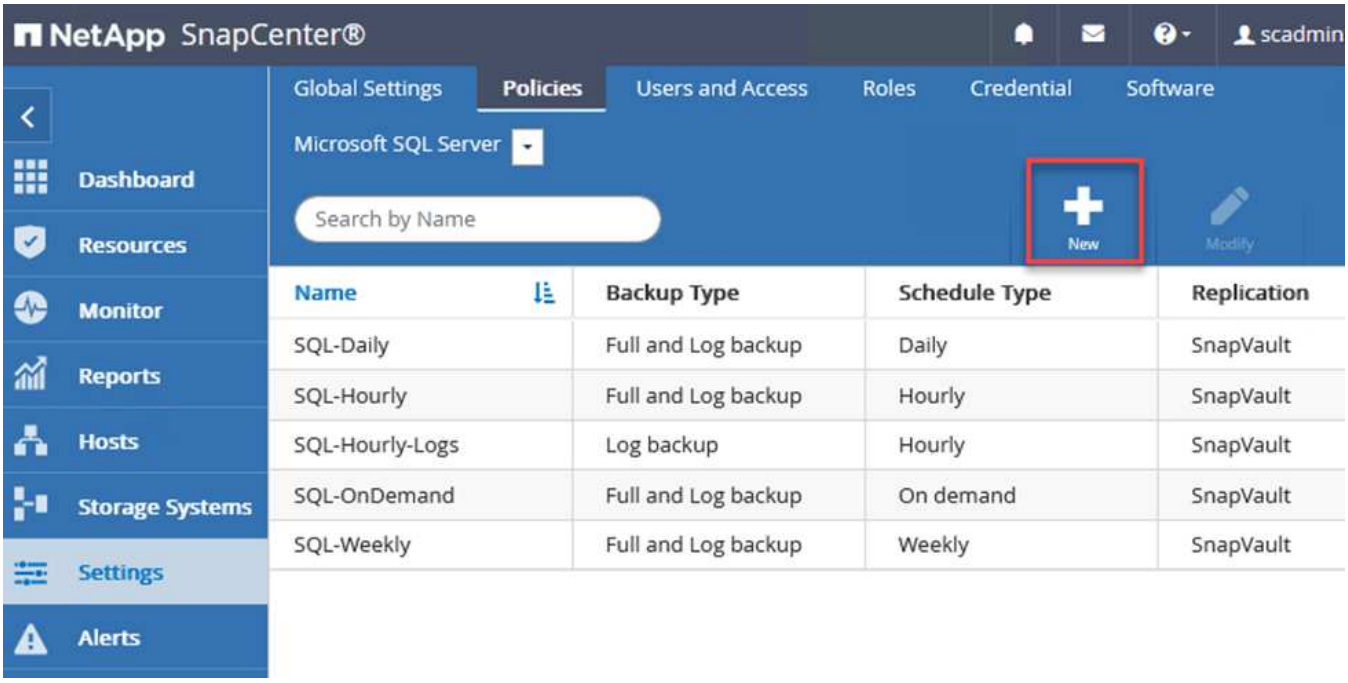
3. Per Oracle, compilare i campi obbligatori nella finestra di dialogo Aggiungi host e selezionare la casella di controllo per il plug-in Oracle Database. Quindi fare clic su Invia per avviare il processo di individuazione e aggiungere l'host a SnapCenter.



▼ **Crea criteri SnapCenter**

Le policy 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 registri delle transazioni.

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



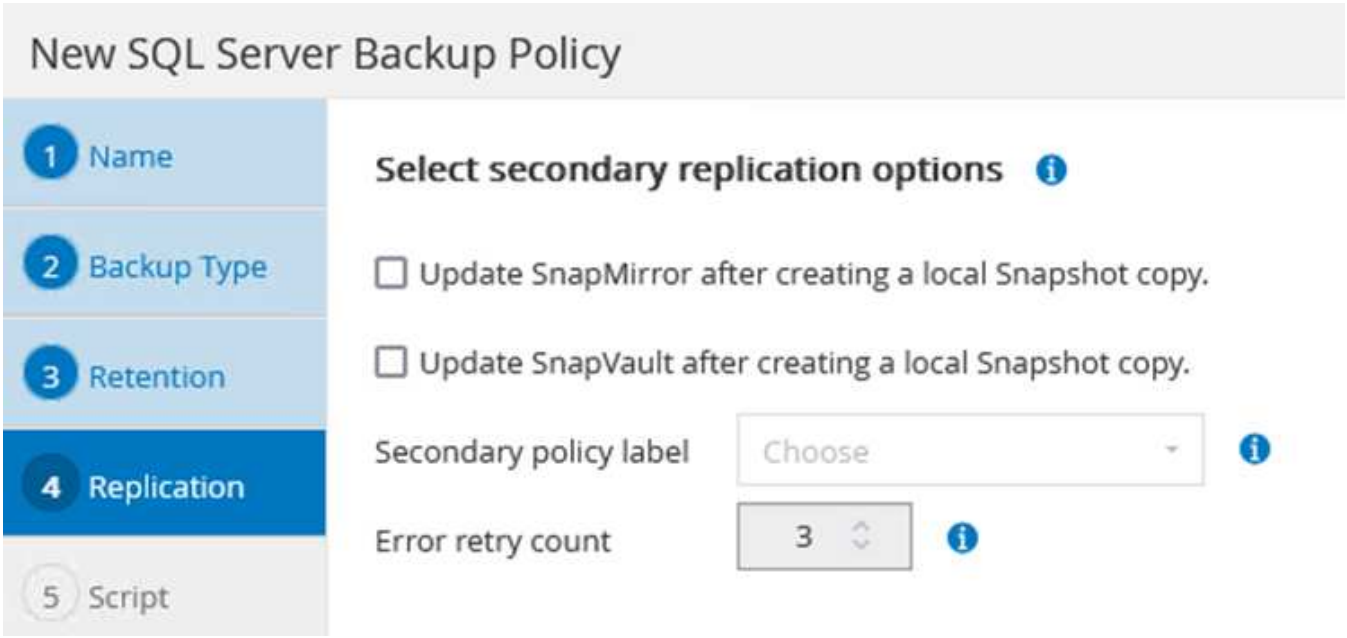
Per informazioni complete sulla creazione di criteri per i backup di SQL Server, vedere "Documentazione SnapCenter" .

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

Note:

- Durante la procedura guidata di creazione dei criteri, prestare particolare attenzione alla sezione Replica. In questa sezione puoi specificare i tipi di copie secondarie SnapMirror che desideri vengano eseguite durante il processo di backup.
- L'impostazione "Aggiorna SnapMirror dopo aver creato una copia Snapshot locale" si riferisce all'aggiornamento di una relazione SnapMirror quando tale relazione esiste tra due macchine virtuali di archiviazione che risiedono sullo stesso cluster.
- L'impostazione "Aggiorna SnapVault dopo aver creato una copia SnapShot locale" viene utilizzata per aggiornare una relazione SnapMirror esistente tra due cluster separati e tra un sistema ONTAP locale e Cloud Volumes ONTAP o FSx ONTAP.

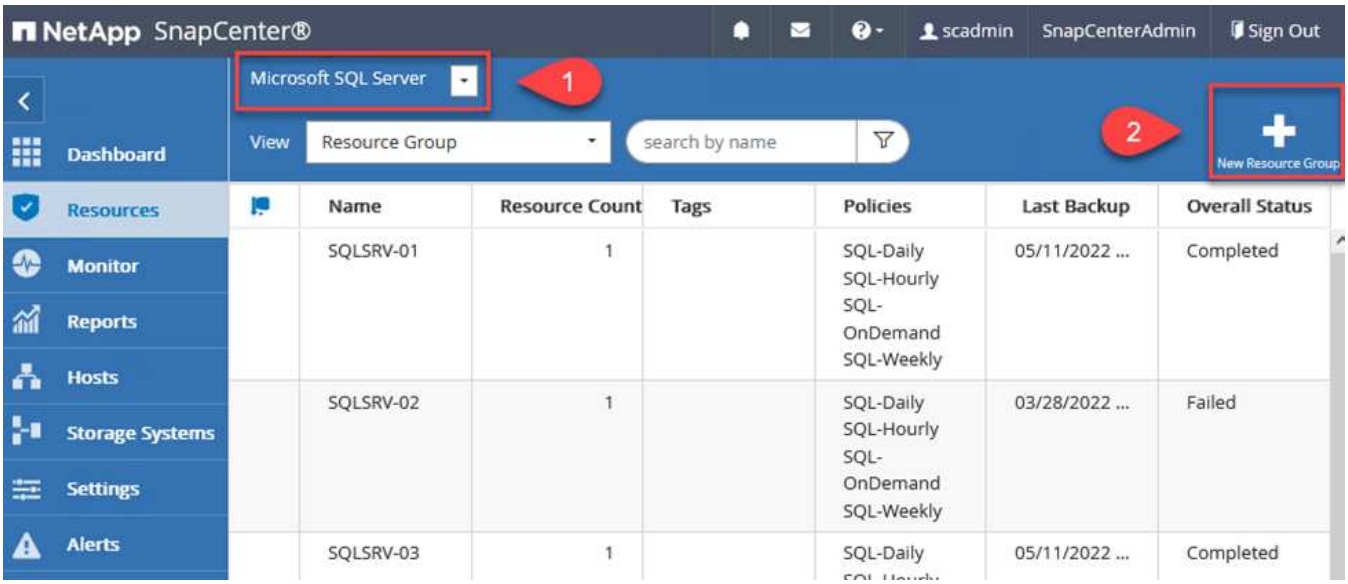
L'immagine seguente mostra le opzioni precedenti e il loro aspetto nella procedura guidata dei criteri di backup.



▼ **Crea gruppi di risorse SnapCenter**

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

1. Vai alla sezione Risorse nel menu a sinistra.
2. Nella parte superiore della finestra, seleziona il tipo di risorsa con cui lavorare (in questo caso Microsoft SQL Server), quindi fai clic su Nuovo gruppo di risorse.



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

Per eseguire il backup delle risorse SQL, seguire "questo collegamento" .

Per il backup delle risorse Oracle, seguire "questo collegamento" .

Distribuisci e configura Veeam Backup Server

Nella soluzione viene utilizzato il software Veeam Backup & Replication per eseguire il backup delle macchine virtuali delle nostre applicazioni e archiviare una copia dei backup in un bucket Amazon S3 utilizzando un repository di backup scale-out (SOBR) Veeam. In questa soluzione Veeam è distribuito su un server Windows. Per indicazioni specifiche sulla distribuzione di Veeam, vedere "Centro assistenza Veeam Documentazione tecnica" .

▼ Configurare il repository di backup scalabile Veeam

Dopo aver distribuito e ottenuto la licenza del software, è possibile creare un repository di backup scalabile (SOBR) come archivio di destinazione per i processi di backup. Dovresti anche includere un bucket S3 come backup dei dati della VM fuori sede per il ripristino di emergenza.

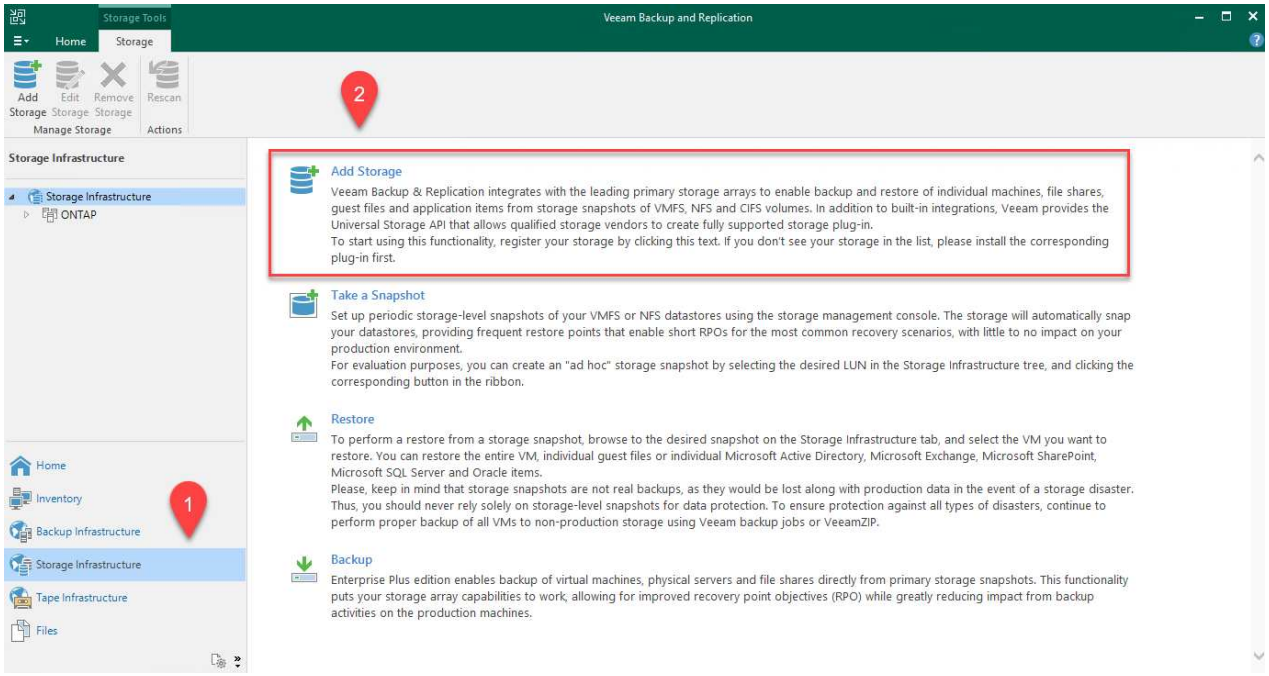
Prima di iniziare, consultare i seguenti prerequisiti.

1. Crea una condivisione file SMB sul tuo sistema ONTAP locale come archivio di destinazione per i backup.
2. Creare un bucket Amazon S3 da includere nel SOBR. Questo è un repository per i backup fuori sede.

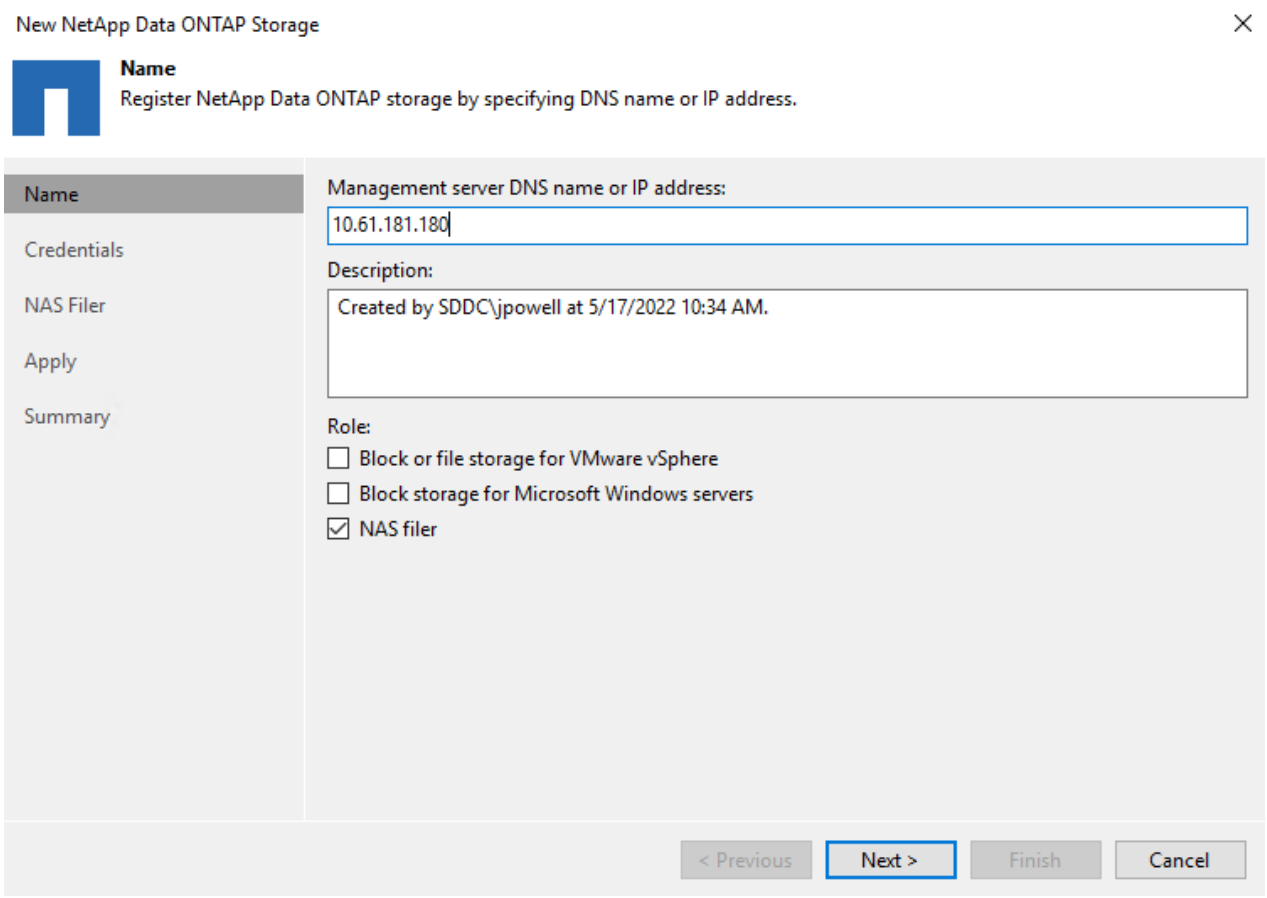
▼ Aggiungi ONTAP Storage a Veeam

Per prima cosa, aggiungi il cluster di storage ONTAP e il file system SMB/NFS associato come infrastruttura di storage in Veeam.

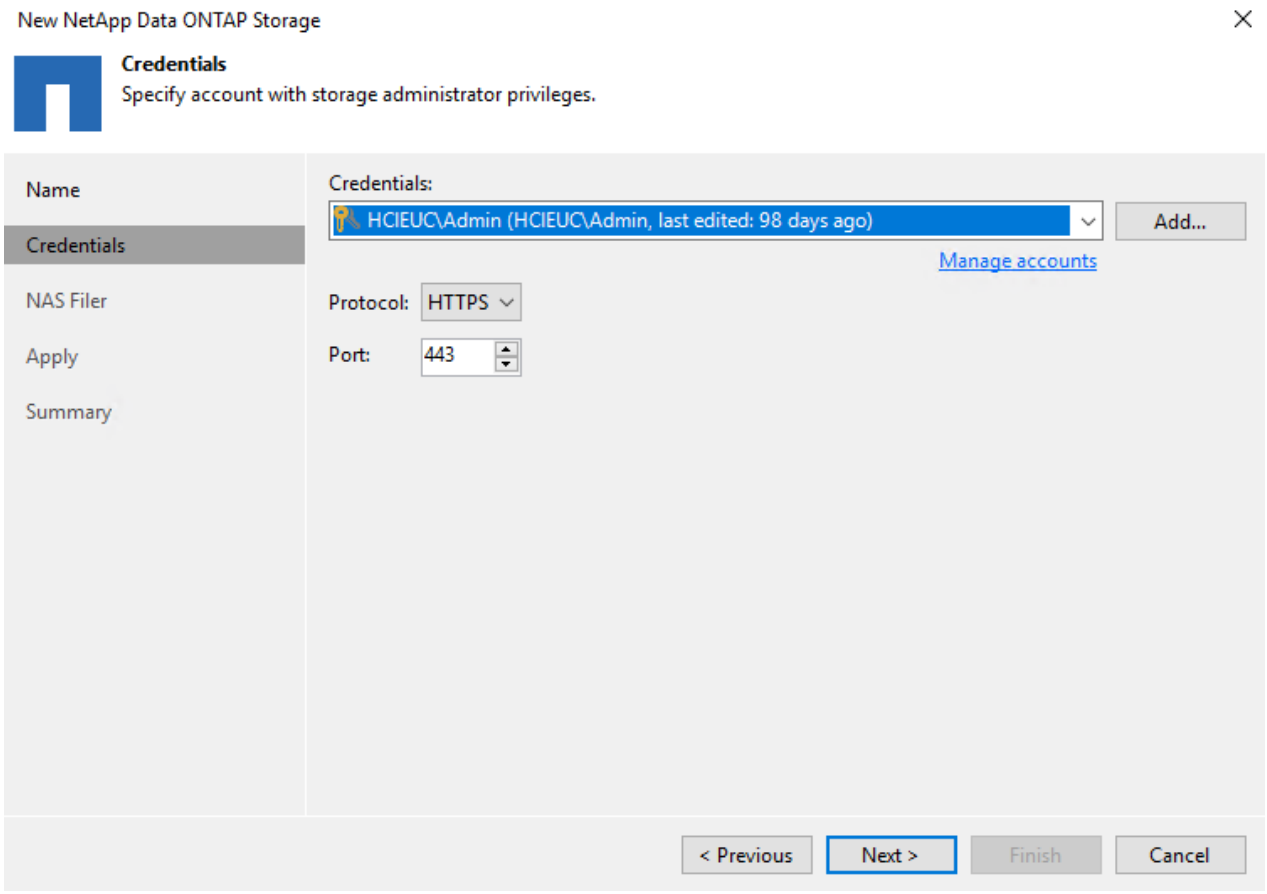
1. Apri la console Veeam ed effettua l'accesso. Vai su Infrastruttura di storage e seleziona Aggiungi storage.



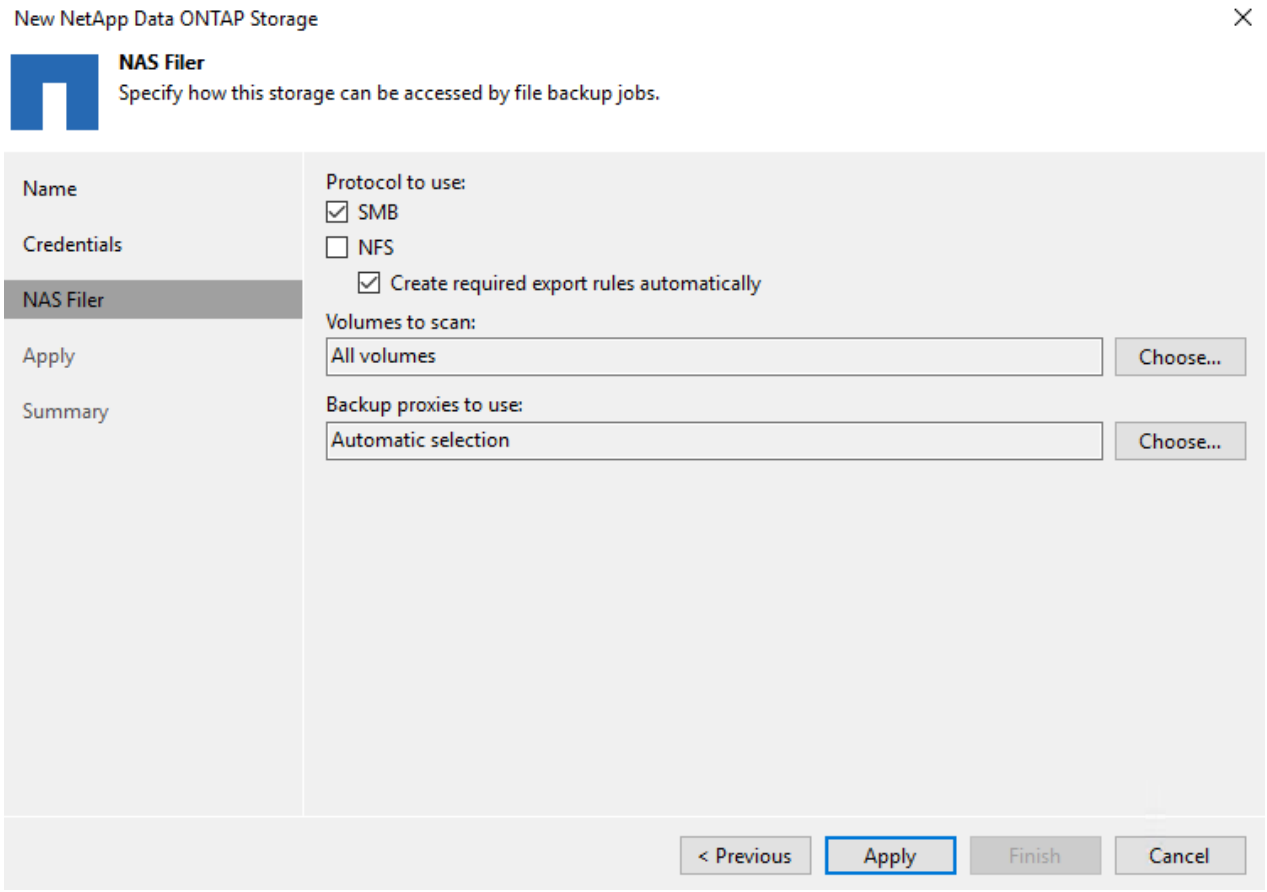
2. Nella procedura guidata Aggiungi storage, seleziona NetApp come fornitore di storage, quindi seleziona Data ONTAP.
3. Immettere l'indirizzo IP di gestione e selezionare la casella NAS Filer. Fare clic su Avanti.



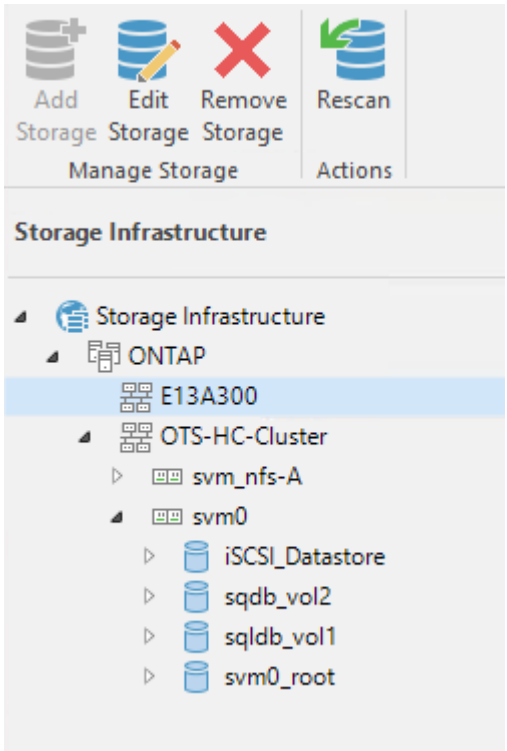
4. Aggiungi le tue credenziali per accedere al cluster ONTAP .



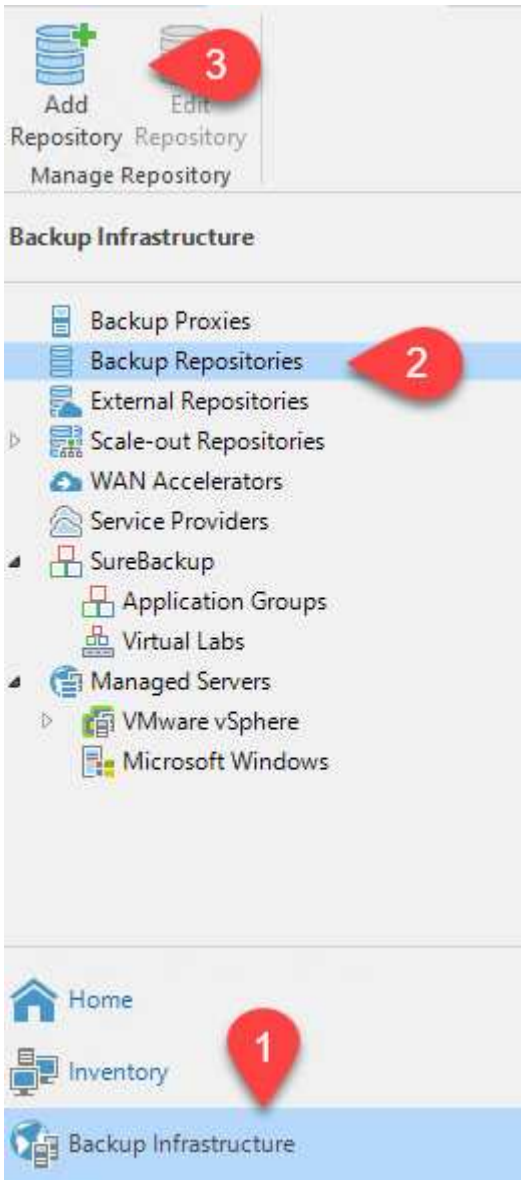
5. Nella pagina NAS Filer, selezionare i protocolli desiderati da analizzare e selezionare Avanti.



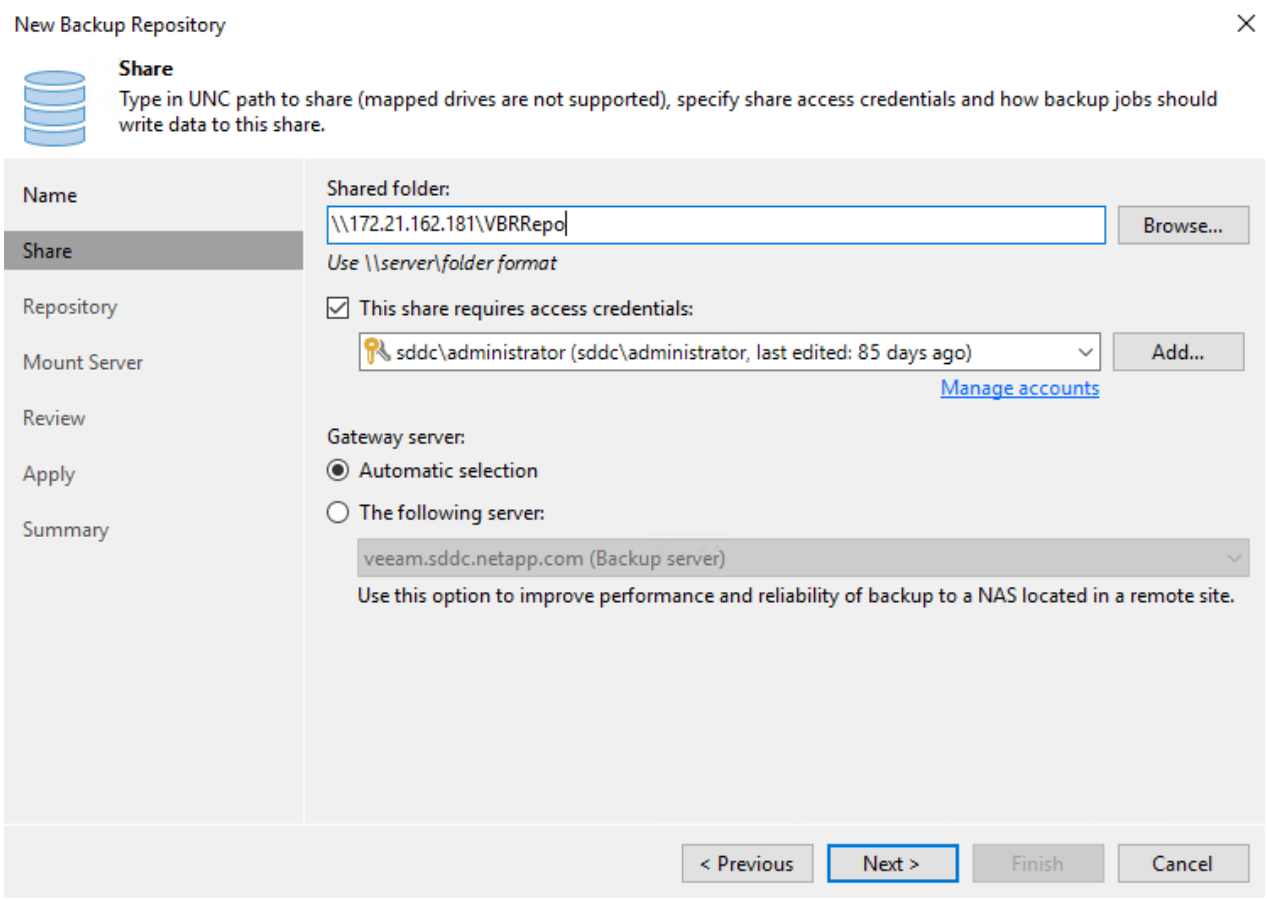
6. Completare le pagine Applica e Riepilogo della procedura guidata e fare clic su Fine per avviare il processo di individuazione dell'archiviazione. Una volta completata la scansione, il cluster ONTAP viene aggiunto insieme ai filer NAS come risorse disponibili.



7. Creare un repository di backup utilizzando le condivisioni NAS appena scoperte. Da Backup Infrastructure, seleziona Backup Repository e fai clic sulla voce di menu Aggiungi repository.



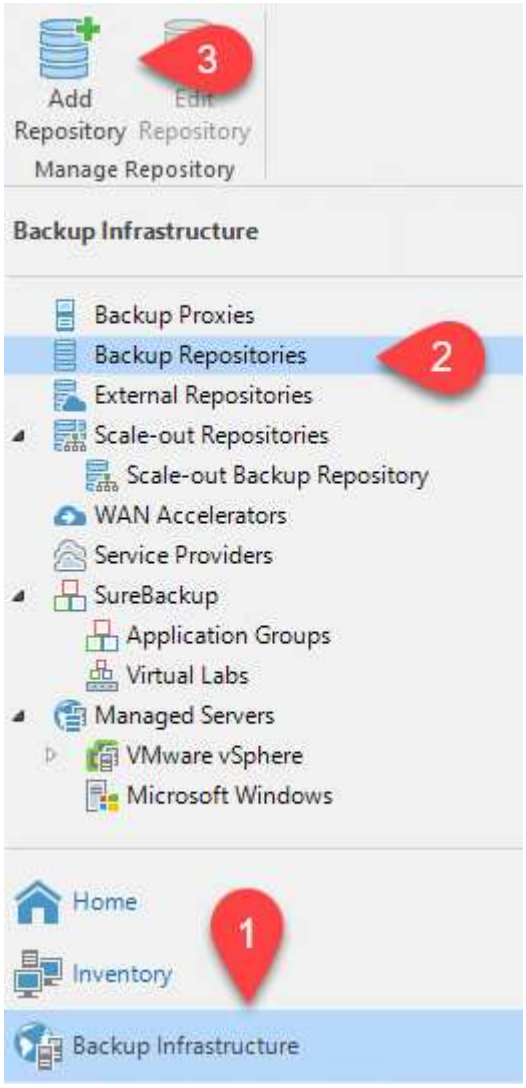
8. Seguire tutti i passaggi della procedura guidata Nuovo repository di backup per creare il repository. Per informazioni dettagliate sulla creazione di repository di backup Veeam, vedere "Documentazione Veeam" .



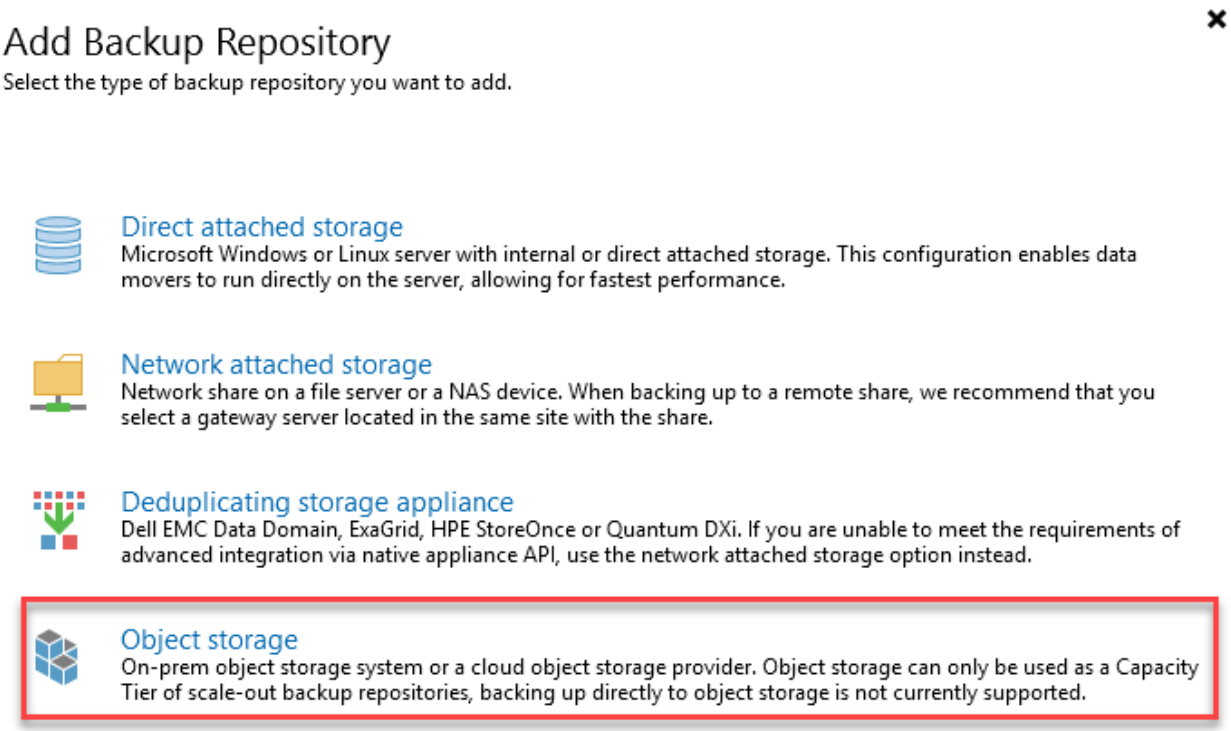
▼ **Aggiungi il bucket Amazon S3 come repository di backup**

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

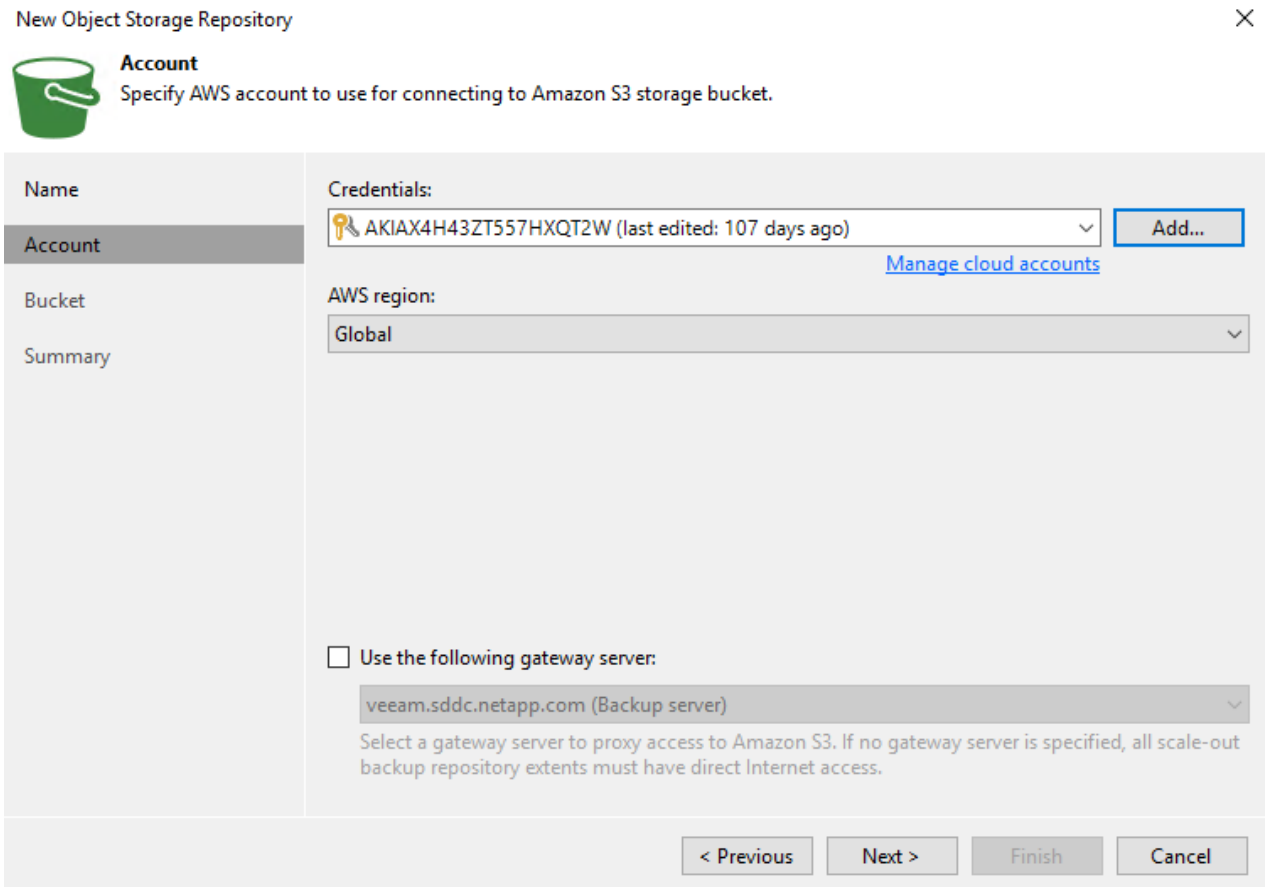
1. Passare a Infrastruttura di backup > Repository di backup. Fare clic su Aggiungi repository.



2. Nella procedura guidata Aggiungi repository di backup, seleziona Object Storage e quindi Amazon S3. Verrà avviata la procedura guidata Nuovo repository di archiviazione oggetti.



3. Specifica un nome per il repository di archiviazione degli oggetti e fai clic su Avanti.
4. Nella sezione successiva, fornisci le tue credenziali. Sono necessarie una chiave di accesso AWS e una chiave segreta.

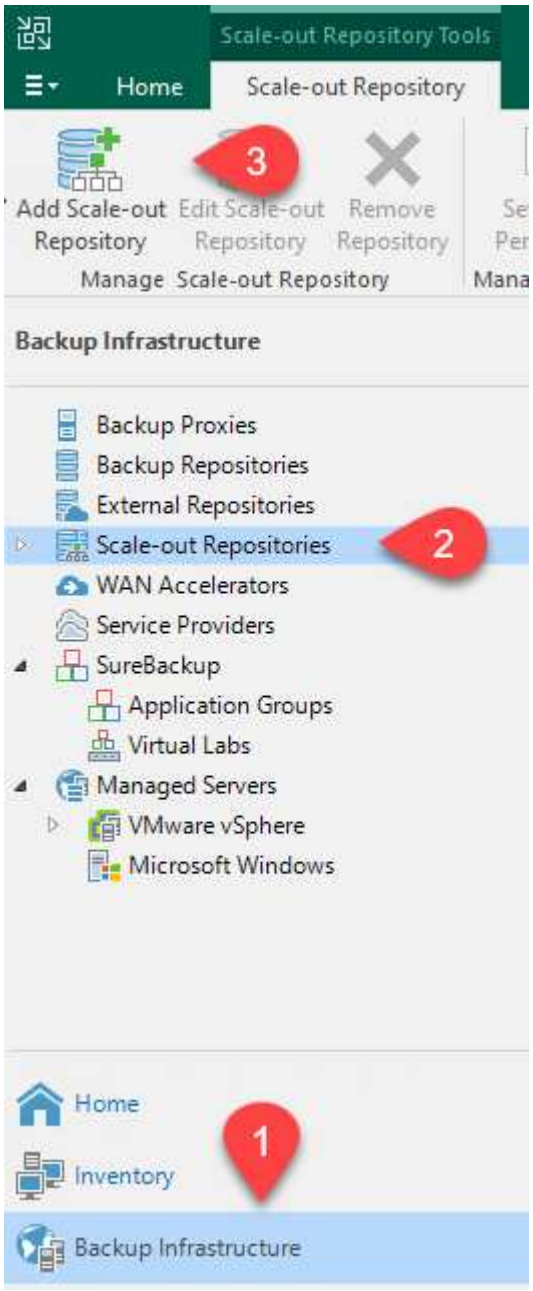


5. Dopo aver caricato la configurazione di Amazon, seleziona il data center, il bucket e la cartella e fai clic su Applica. Infine, fare clic su Fine per chiudere la procedura guidata.

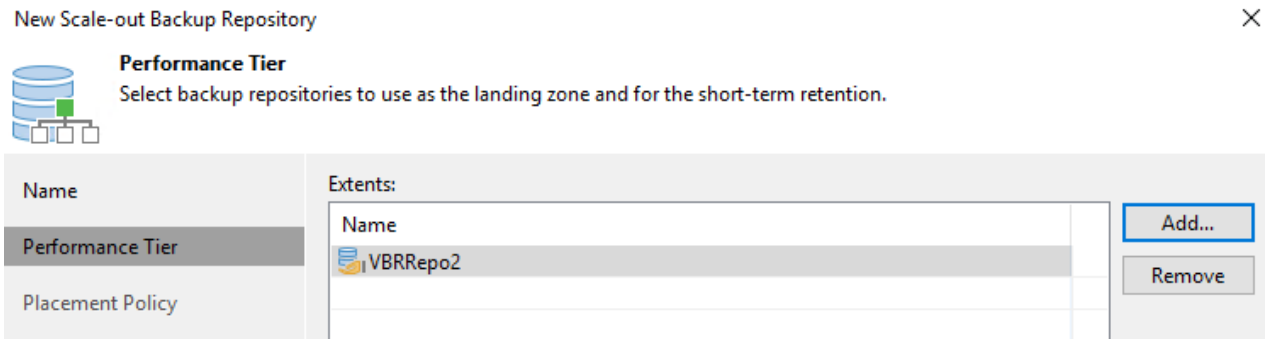
▼ **Crea un repository di backup scalabile**

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

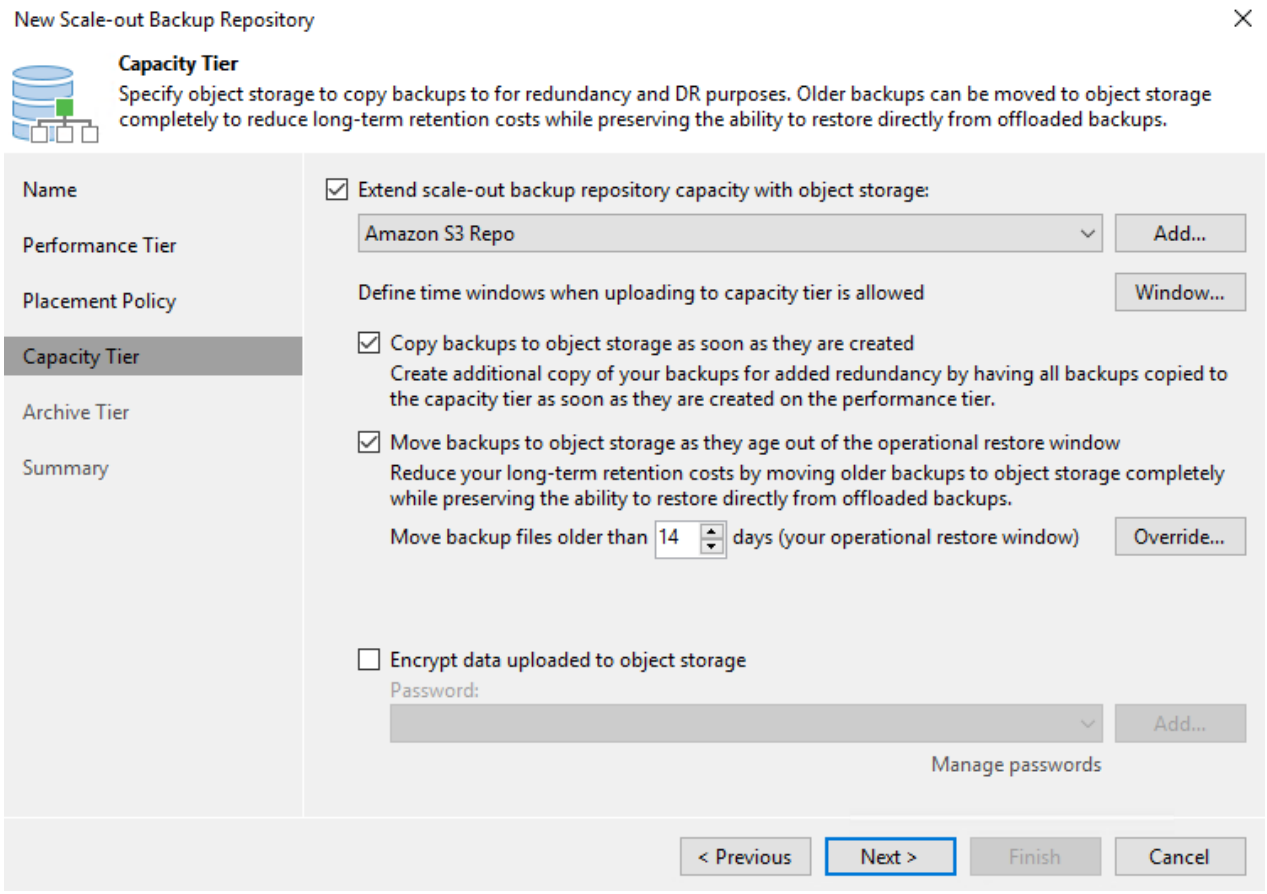
1. Da Backup Infrastructure, seleziona Scale-out Repositories e quindi fai clic sulla voce di menu Aggiungi Scale-out Repository.



2. Nel Nuovo repository di backup scalabile, immettere un nome per SOBR e fare clic su Avanti.
3. Per il livello di prestazioni, seleziona il repository di backup che contiene la condivisione SMB residente sul tuo cluster ONTAP locale.



4. Per la politica di posizionamento, scegli Località dei dati o Prestazioni in base alle tue esigenze. Seleziona Avanti.
5. Per Capacity Tier estendiamo SOBR con l'archiviazione di oggetti Amazon S3. Ai fini del ripristino di emergenza, selezionare Copia backup in Object Storage non appena vengono creati per garantire la consegna tempestiva dei nostri backup secondari.



6. Infine, seleziona Applica e Fine per finalizzare la creazione del SOBR.

▼ Creare i processi di repository di backup scalabili

Il passaggio finale per configurare Veeam consiste nel creare processi di backup utilizzando il SOBR appena creato come destinazione di backup. La creazione di processi di backup è una normale attività del repertorio di qualsiasi amministratore di storage e in questa sede non verranno illustrati i passaggi dettagliati. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam" .

NetApp Backup and Recovery: strumenti e configurazione

Per eseguire un failover delle VM delle applicazioni e dei volumi del database sui servizi VMware Cloud Volume in esecuzione su AWS, è necessario installare e configurare un'istanza in esecuzione sia di SnapCenter Server che di Veeam Backup and Replication Server. Una volta completato il failover, è necessario configurare questi strumenti anche per riprendere le normali operazioni di backup finché non viene pianificato ed eseguito un failback nel data center locale.

▼ **Distribuisci il server Windows SnapCenter secondario**

SnapCenter Server viene distribuito nel VMware Cloud SDDC o installato su un'istanza EC2 residente in una VPC con connettività di rete all'ambiente VMware Cloud.

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

Puoi trovare il SnapCenter software su "questo collegamento" .

▼ **Configurare il server secondario Windows SnapCenter**

Per eseguire un ripristino dei dati dell'applicazione sottoposti a mirroring su FSx ONTAP, è necessario prima eseguire un ripristino completo del database SnapCenter locale. Una volta completato questo processo, la comunicazione con le VM viene ristabilita e i backup delle applicazioni possono ora riprendere utilizzando FSx ONTAP come storage primario.

Per raggiungere questo obiettivo, è necessario completare le seguenti operazioni sul server SnapCenter :

1. Configurare il nome del computer in modo che sia identico al server SnapCenter locale originale.
2. Configurare la rete per comunicare con VMware Cloud e l'istanza FSx ONTAP .
3. Completare la procedura per ripristinare il database SnapCenter .
4. Verificare che SnapCenter sia in modalità Disaster Recovery per assicurarsi che FSx sia ora l'archivio primario per i backup.
5. Verificare che la comunicazione con le macchine virtuali ripristinate sia stata ristabilita.

▼ **Distribuisci il server Veeam Backup & Replication secondario**

È possibile installare il server Veeam Backup & Replication su un server Windows nel VMware Cloud su AWS o su un'istanza EC2. Per una guida dettagliata all'implementazione, vedere "Documentazione tecnica del Centro assistenza Veeam" .

▼ **Configurare il server Veeam Backup & Replication secondario**

Per eseguire un ripristino di macchine virtuali di cui è stato eseguito il backup nello 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 VM dopo il loro ripristino.

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

1. Configurare la rete per comunicare con VMware Cloud, FSx ONTAP e il bucket S3 contenente il repository di backup originale.
2. Configurare una condivisione SMB su FSx ONTAP come nuovo repository di backup.
3. Montare il bucket S3 originale utilizzato come parte del repository di backup scalabile in locale.

4. Dopo aver ripristinato la VM, stabilire nuovi processi di backup per proteggere le VM SQL e Oracle.

Per ulteriori informazioni sul ripristino delle VM tramite Veeam, consultare la sezione"Ripristina le VM delle applicazioni con Veeam Full Restore" .

Backup del database SnapCenter per il ripristino di emergenza

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 SnapCenter su un'istanza AWS EC2 residente nella nostra VPC. Per ulteriori informazioni sul ripristino di emergenza di SnapCenter, vedere "questo collegamento" .

▼ **Prerequisiti per il backup SnapCenter**

Per il backup SnapCenter sono richiesti i seguenti prerequisiti:

- Un volume e una condivisione SMB creati sul sistema ONTAP locale per individuare il database sottoposto a backup e i file di configurazione.
- Una relazione SnapMirror tra il sistema ONTAP locale e FSx o CVO nell'account AWS. Questa relazione viene utilizzata per trasportare lo snapshot contenente il database SnapCenter sottoposto a 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 Windows EC2 o sulla VM in VMware Cloud.

▼ **Riepilogo del processo di backup e ripristino SnapCenter**

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

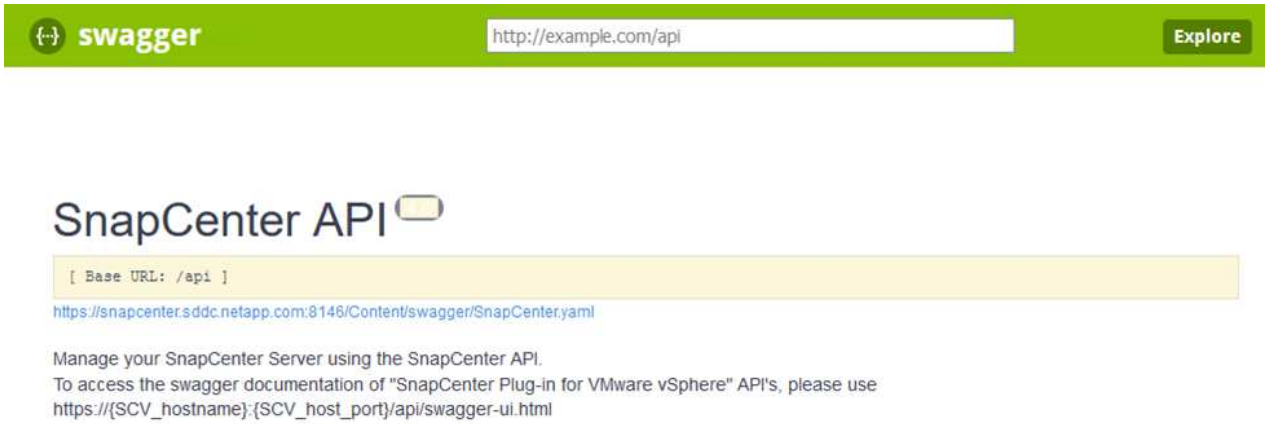
▼ **Eseguire il backup del database e della configurazione SnapCenter**

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

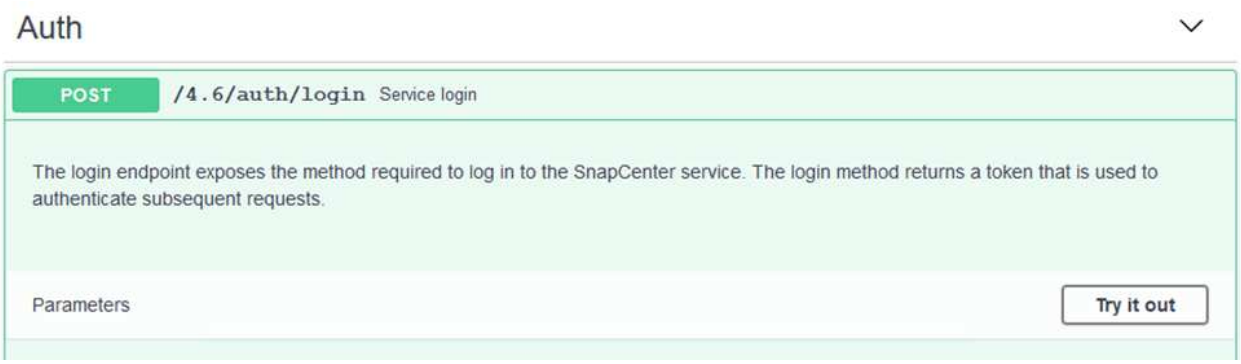
▼ **Accedi a Swagger e ottieni il token di autorizzazione**

Dopo aver navigato fino alla pagina Swagger, è necessario recuperare un token di autorizzazione per avviare il processo di ripristino del database.

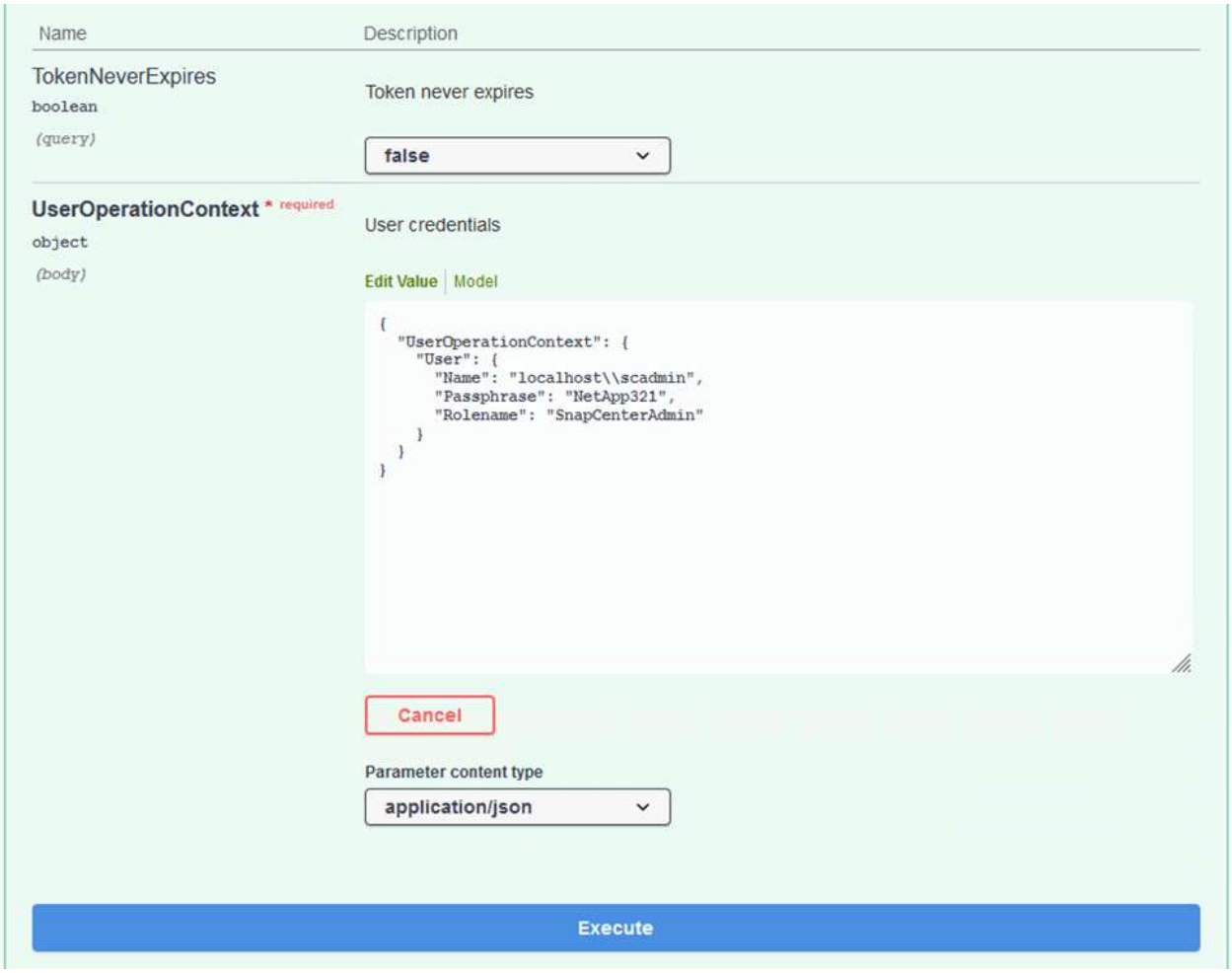
1. Accedi alla pagina web dell'API SnapCenter Swagger all'indirizzo *https://< SnapCenter Server IP>:8146/swagger/*.



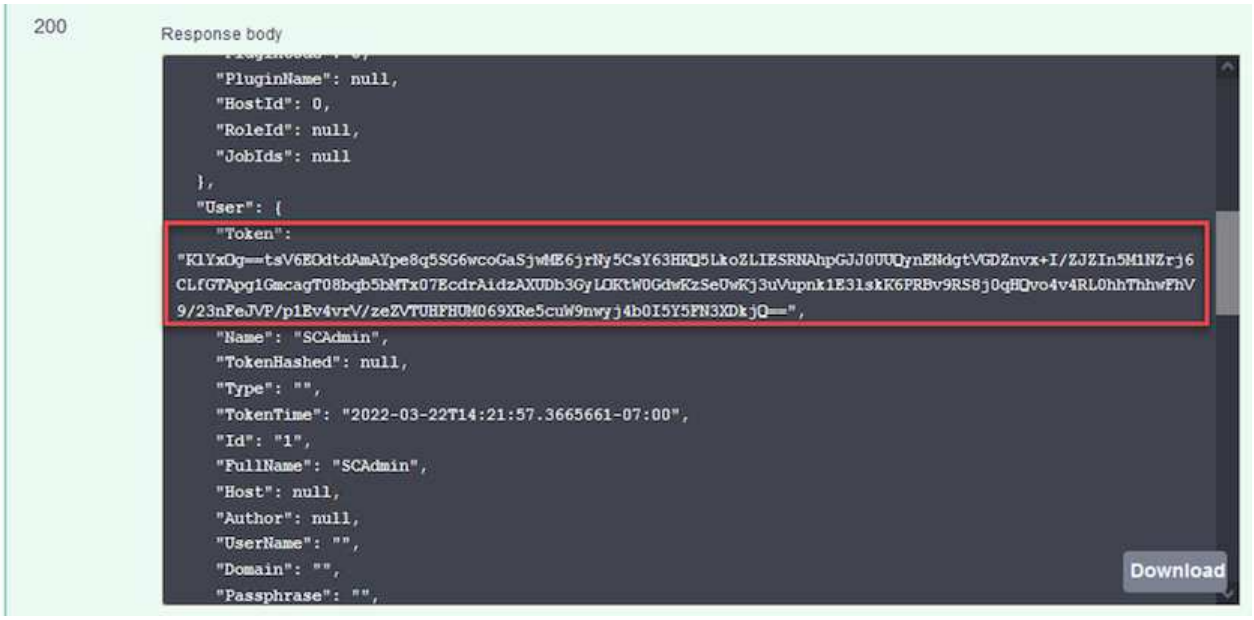
2. Espandi la sezione Autenticazione e fai clic su Provalo.



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



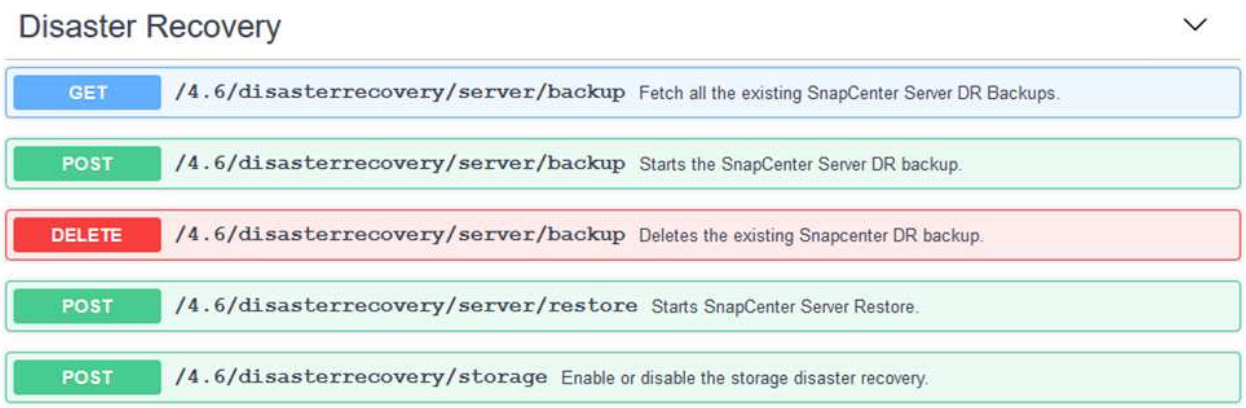
4. Nel corpo della risposta qui sotto puoi vedere il token. Copiare il testo del token per l'autenticazione durante l'esecuzione del processo di backup.



▼ **Eseguire un backup del database SnapCenter**

Successivamente, vai all'area Disaster Recovery nella pagina Swagger per avviare il processo di backup SnapCenter .

1. Espandi l'area Disaster Recovery cliccandoci sopra.

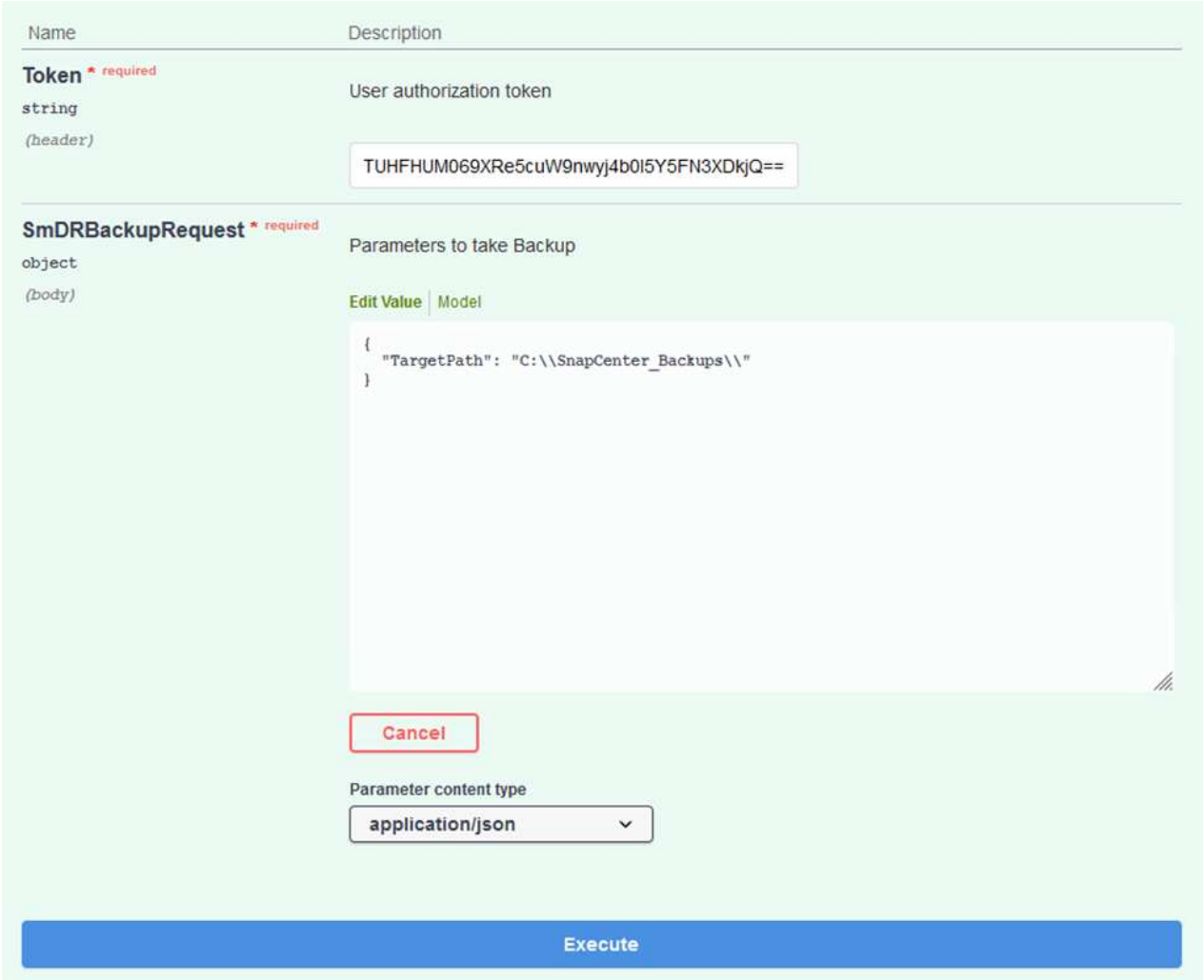


2. Espandi il `/4.6/disasterrecovery/server/backup` sezione e clicca su Provalo.



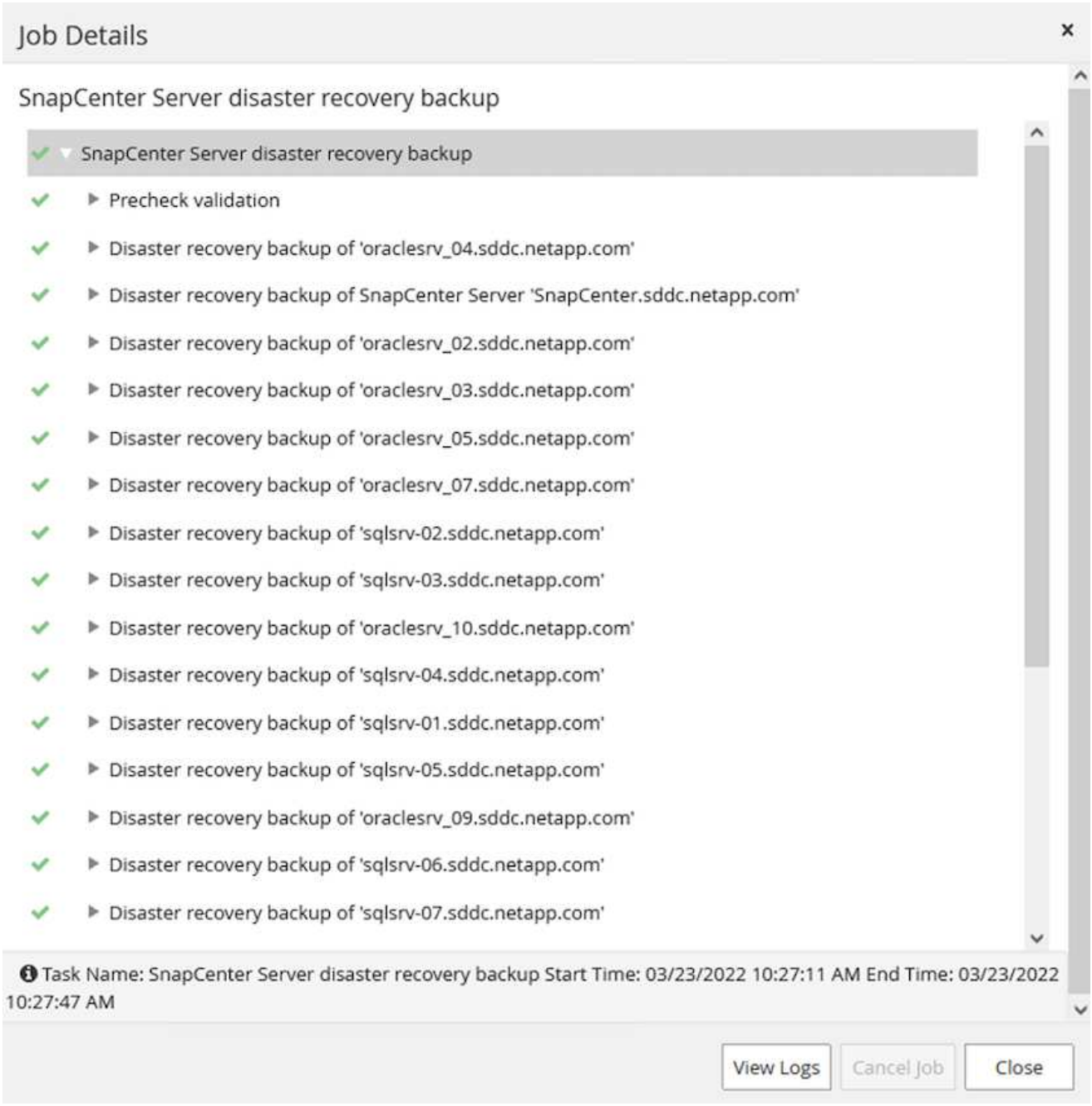
3. Nella sezione SmDRBackupRequest, aggiungere il percorso di destinazione locale corretto e selezionare Esegui per avviare il backup del database e della configurazione SnapCenter .

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



▼ **Monitorare il processo di backup da SnapCenter**

Accedi a SnapCenter per rivedere i file di registro quando avvii il processo di ripristino del database. Nella sezione Monitor è possibile visualizzare i dettagli del backup di ripristino di emergenza del server SnapCenter .



▼ **Utilizzare l'utilità XCOPY per copiare il file di backup del database nella condivisione SMB**

Successivamente è necessario spostare il backup dall'unità locale sul server SnapCenter alla condivisione CIFS utilizzata per copiare i dati SnapMirror nella posizione secondaria situata sull'istanza FSx in AWS. Utilizzare xcopy con opzioni specifiche che mantengano le autorizzazioni 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 principale in sede, il nostro scenario prevede il failover su un sito secondario residente sull'infrastruttura Amazon Web Services tramite VMware Cloud su AWS. Supponiamo che le macchine virtuali e il nostro cluster ONTAP locale non siano più accessibili. Inoltre, le macchine virtuali SnapCenter e Veeam non sono più accessibili e devono essere ricostruite presso il nostro sito secondario.

Questa sezione affronta il failover della nostra infrastruttura sul cloud e tratta i seguenti argomenti:

- Ripristino del database SnapCenter . Dopo aver stabilito un nuovo server SnapCenter , ripristinare il database MySQL e i file di configurazione e attivare la modalità di ripristino di emergenza del database per consentire allo storage FSx secondario di diventare il dispositivo di storage primario.
- Ripristinare le macchine virtuali dell'applicazione utilizzando Veeam Backup & Replication. Collegare l'archiviazione S3 che contiene i backup delle VM, 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 suo database MySQL e dei file di configurazione. Ciò consente a un amministratore di mantenere backup regolari del database SnapCenter nel data center locale e di ripristinare successivamente tale database in un database SnapCenter secondario.

Per accedere ai file di backup SnapCenter sul server SnapCenter remoto, completare i seguenti passaggi:

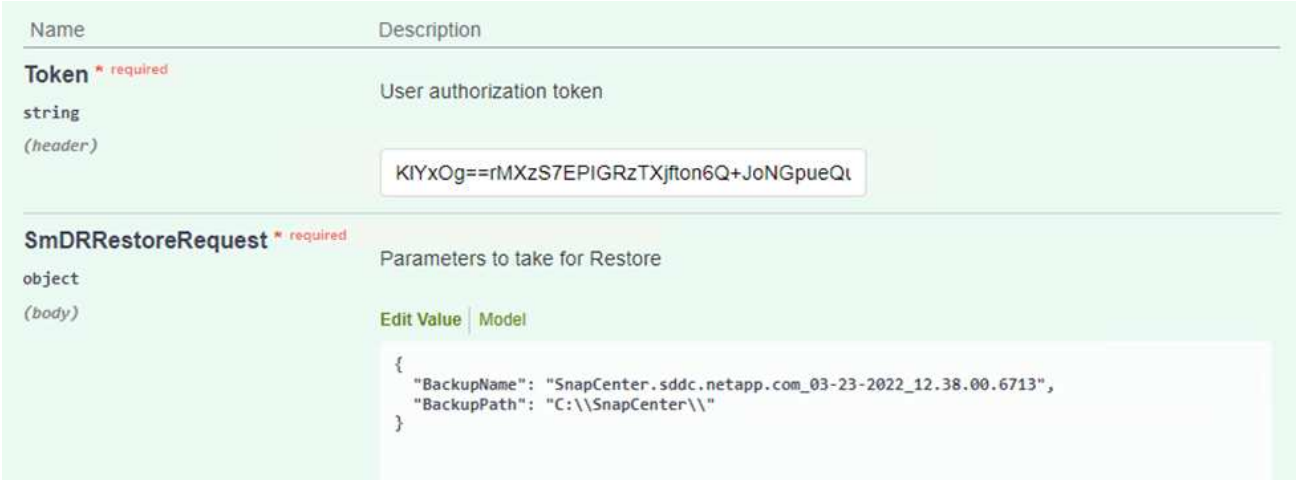
1. Interrompere la relazione SnapMirror dal cluster FSx, rendendo il volume di lettura/scrittura.
2. Creare un server CIFS (se necessario) e creare una condivisione CIFS che punti al percorso di giunzione del volume clonato.
3. Utilizzare xcopy per copiare i file di backup in una directory locale sul sistema SnapCenter secondario.
4. Installa SnapCenter v4.6.
5. Assicurarsi che il server SnapCenter abbia lo stesso FQDN del server originale. Ciò è necessario affinché il ripristino del database abbia esito positivo.

Per avviare il processo di ripristino, completare i seguenti passaggi:

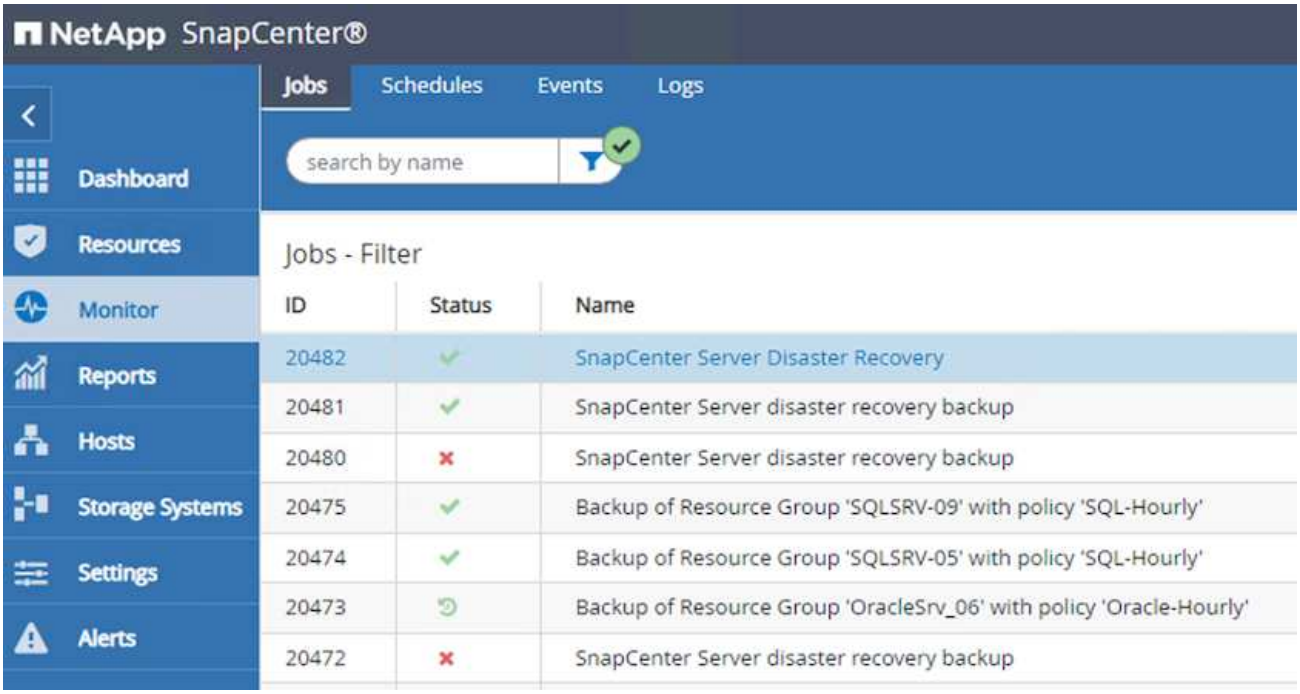
1. Accedere alla pagina web dell'API Swagger per il server SnapCenter secondario e seguire le istruzioni precedenti per ottenere un token di autorizzazione.
2. Vai alla sezione Disaster Recovery della pagina Swagger, seleziona `/4.6/disasterrecovery/server/restore` e fai clic su Provalo.

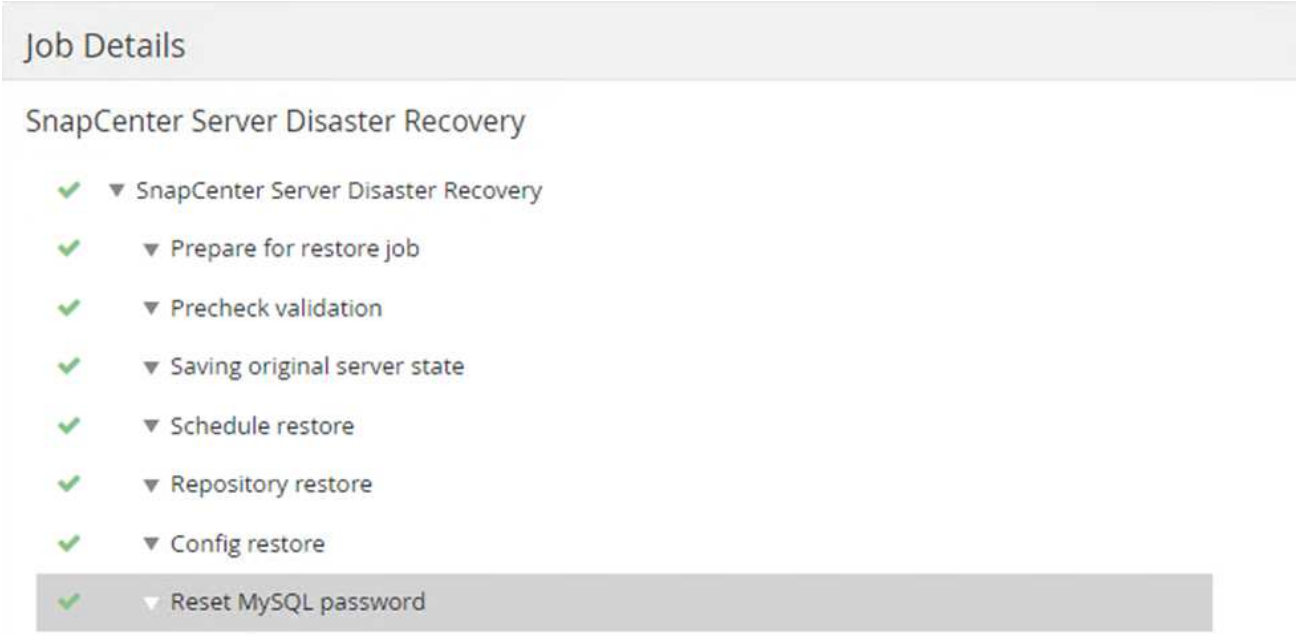


3. Incolla il token di autorizzazione e, nella sezione SmDRResterRequest, incolla il nome del backup e la directory locale sul server SnapCenter secondario.



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





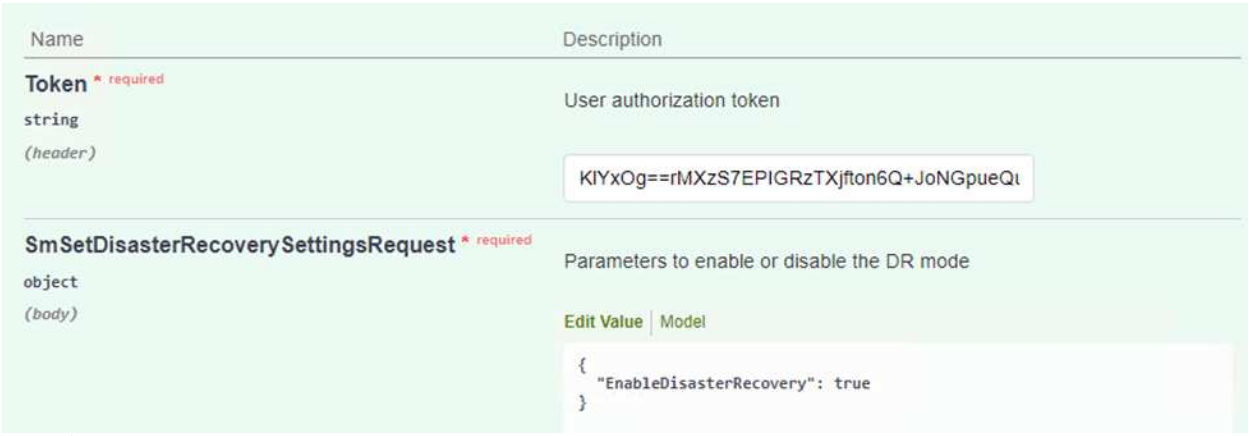
6. Per abilitare i ripristini di SQL Server dall'archiviazione secondaria, è necessario impostare il database SnapCenter in modalità Disaster Recovery. Questa operazione viene eseguita separatamente e avviata sulla pagina web dell'API Swagger.

   a. Passare alla sezione Disaster Recovery e fare clic su `/4.6/disasterrecovery/storage` .

   b. Incolla il token di autorizzazione dell'utente.

   c. Nella sezione SmSetDisasterRecoverySettingsRequest, modificare `EnableDisasterRecover` A `true` .

   d. Fare clic su Esegui per abilitare la modalità di ripristino di emergenza per SQL Server.



Vedere i commenti relativi alle procedure aggiuntive.

Ripristina le VM delle applicazioni con il ripristino completo di Veeam

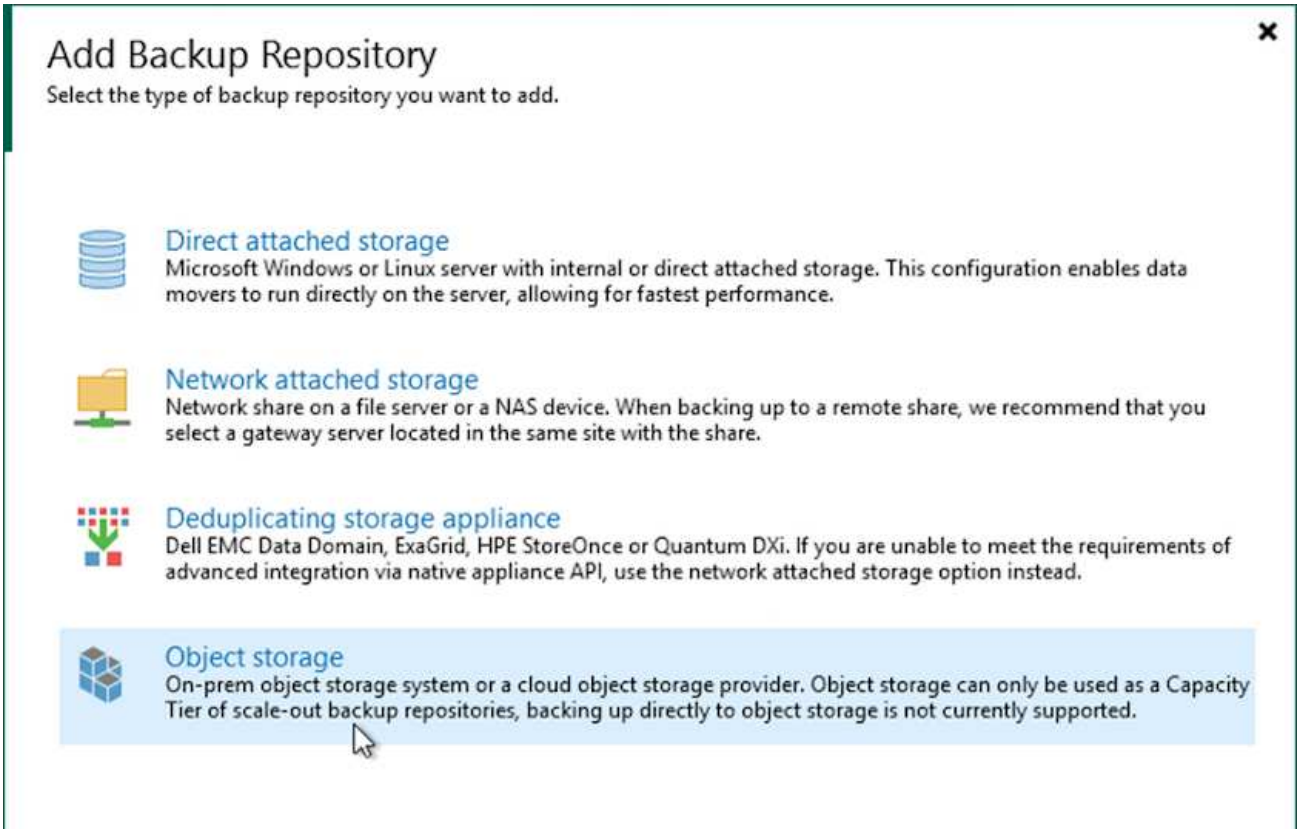
▼ Crea un repository di backup e importa i backup da S3

Dal server Veeam secondario, importa i backup dallo storage S3 e ripristina le VM SQL Server e Oracle nel tuo cluster VMware Cloud.

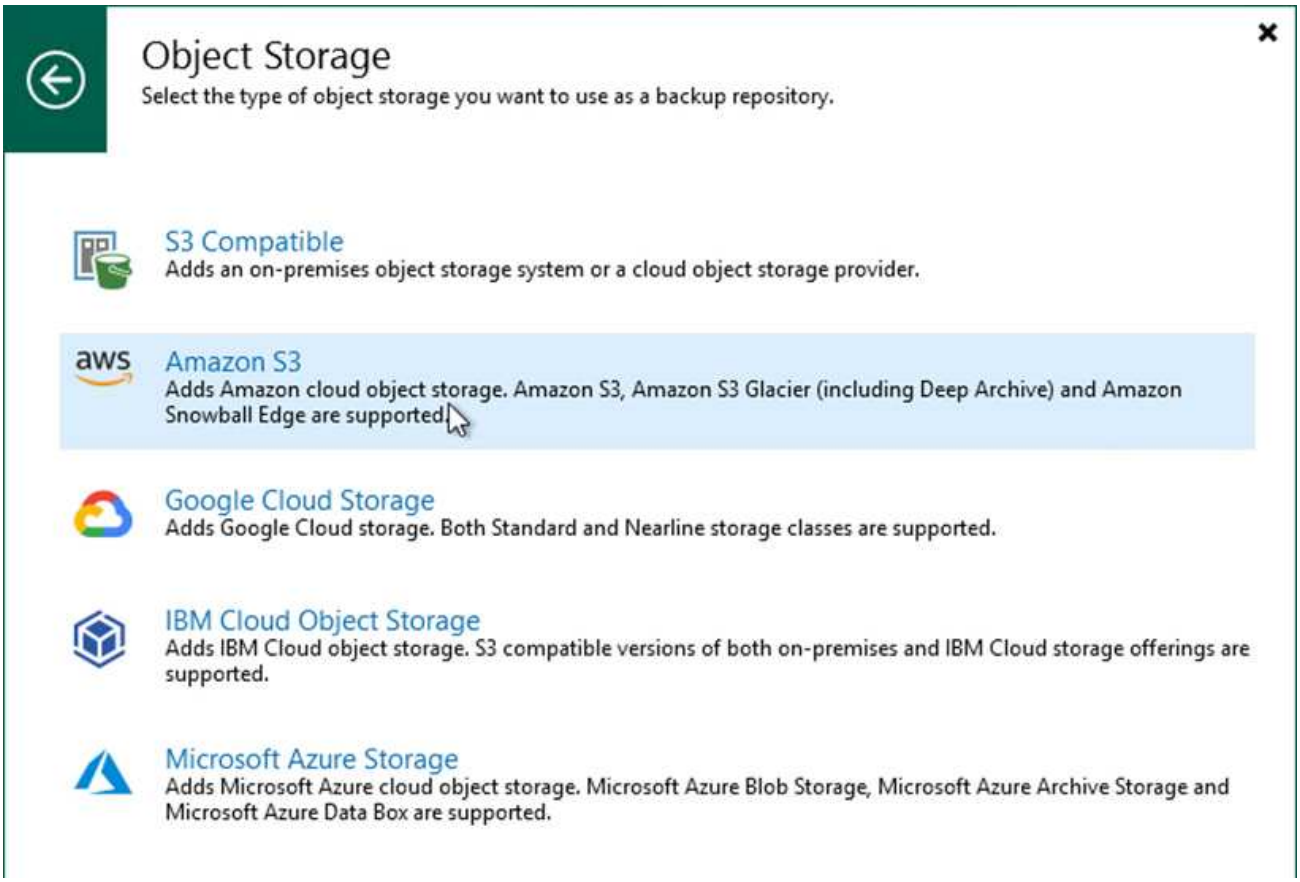
Per importare i backup dall'oggetto S3 che faceva parte del repository di backup scalabile in locale,

completare i seguenti passaggi:

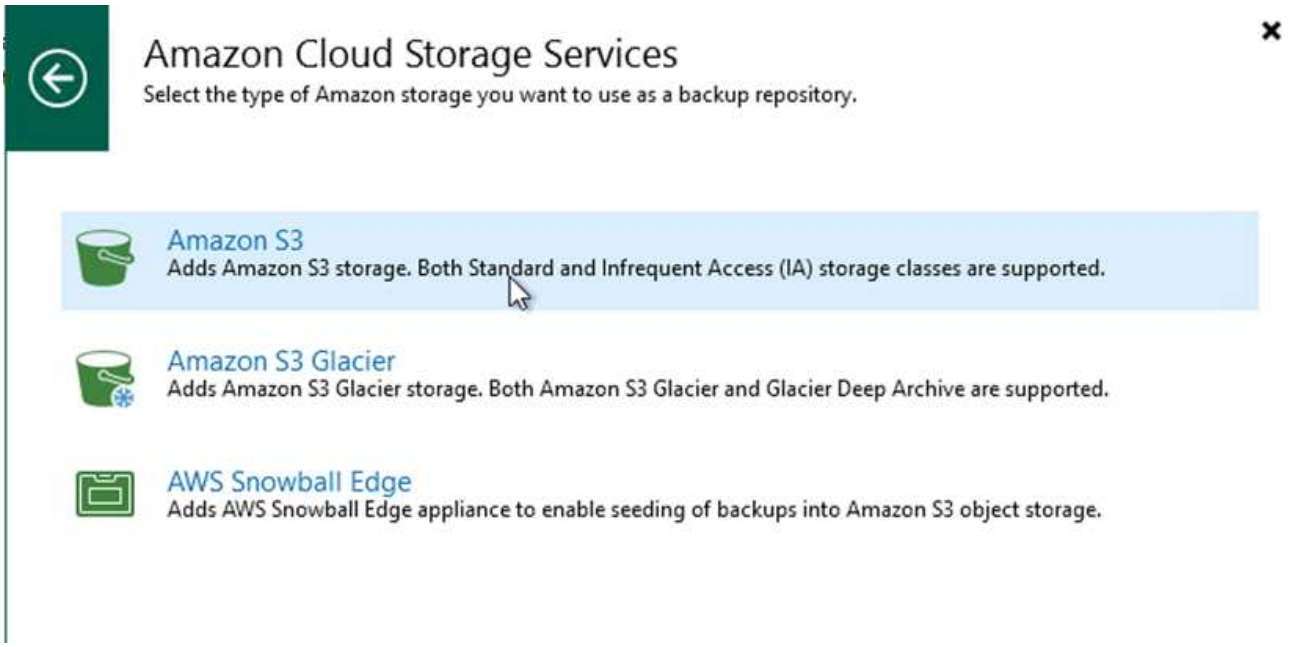
1. Vai a Backup Repositories e fai clic su Aggiungi repository nel menu in alto per avviare la procedura guidata Aggiungi repository di backup. Nella prima pagina della procedura guidata, seleziona Object Storage come tipo di repository di backup.



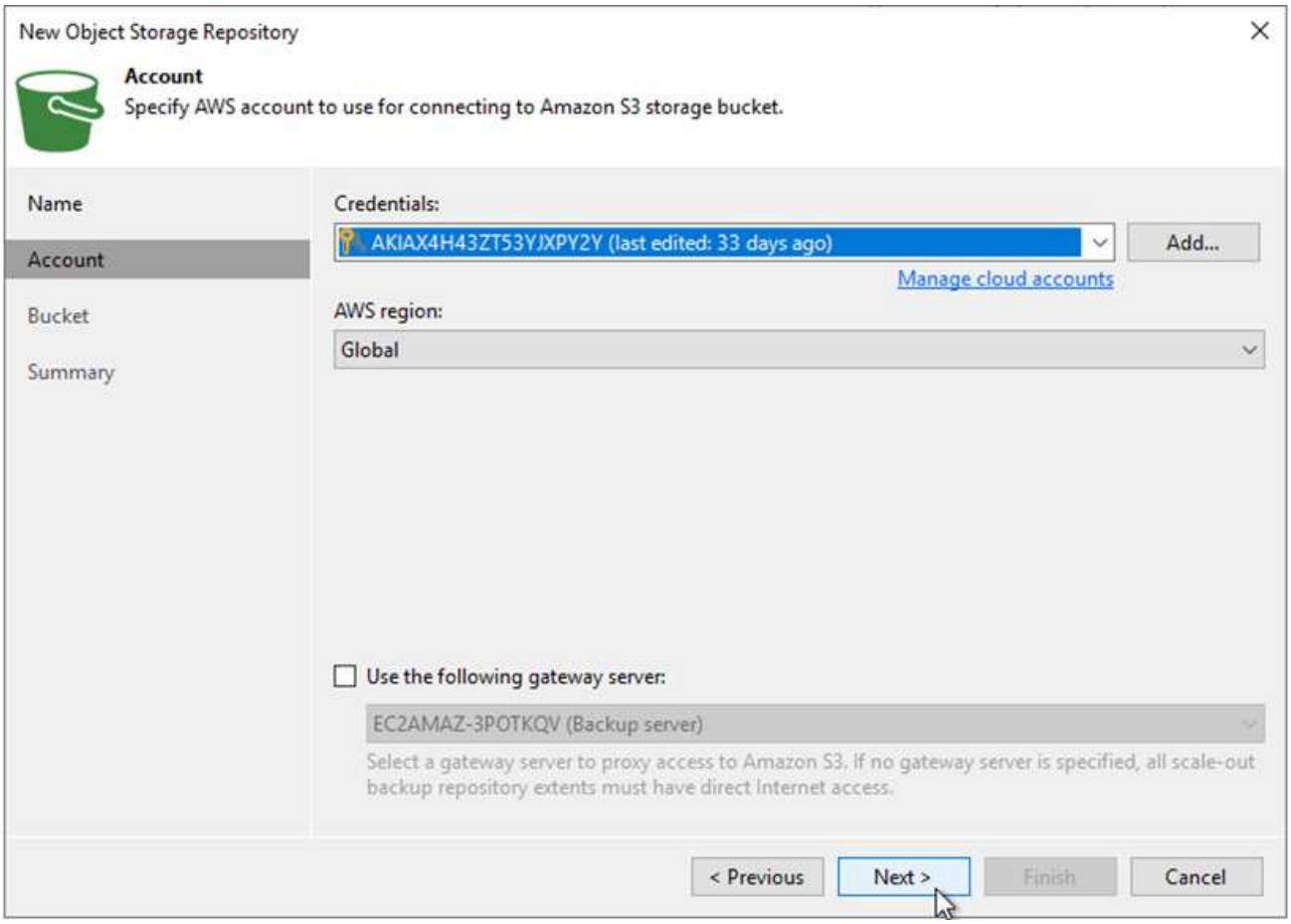
2. Selezionare Amazon S3 come tipo di Object Storage.



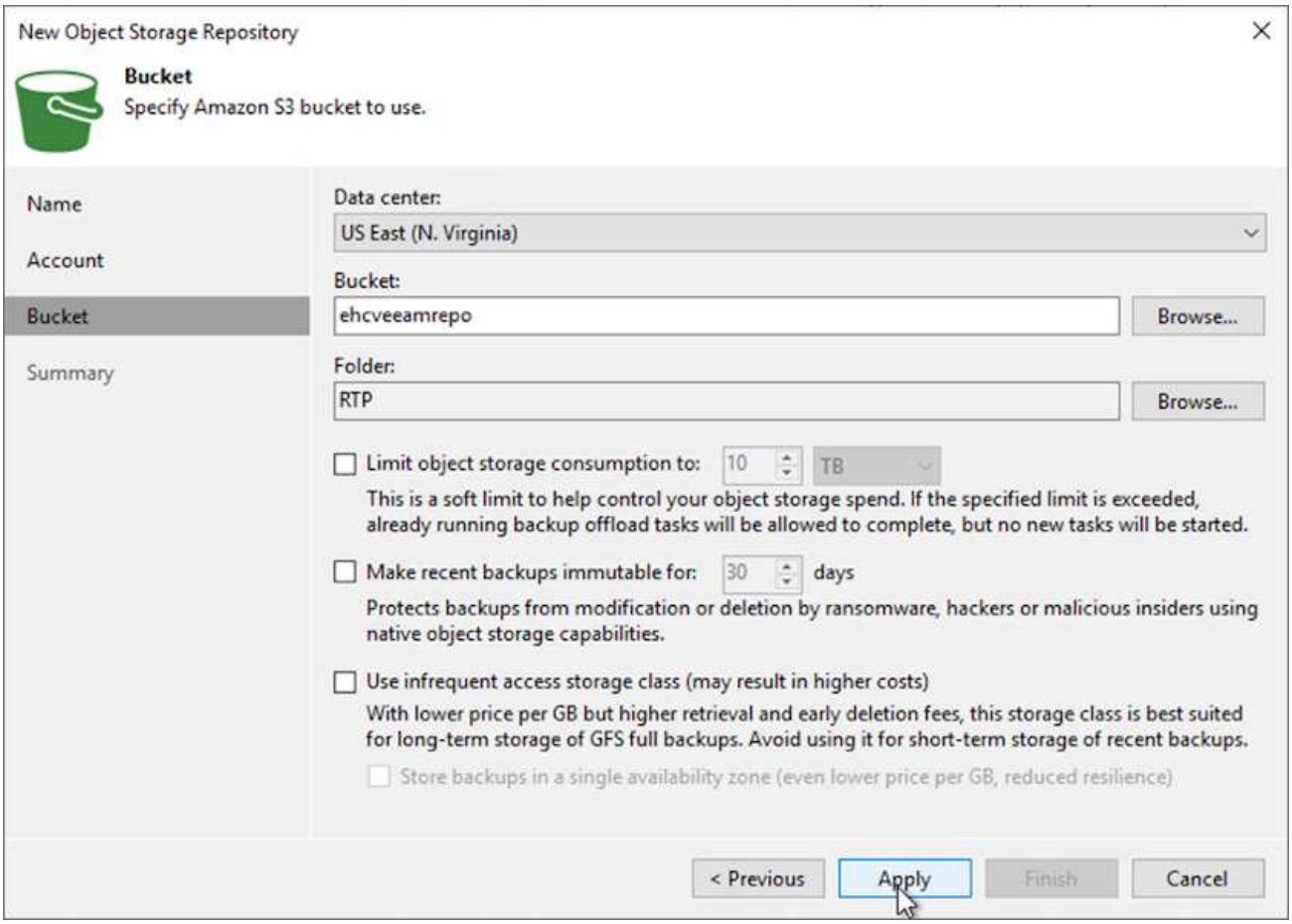
3. Dall'elenco dei servizi di archiviazione cloud Amazon, seleziona Amazon S3.



4. Seleziona le credenziali pre-immesse dall'elenco a discesa oppure aggiungi una nuova credenziale per accedere alla risorsa di archiviazione cloud. Fare clic su Avanti per continuare.



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

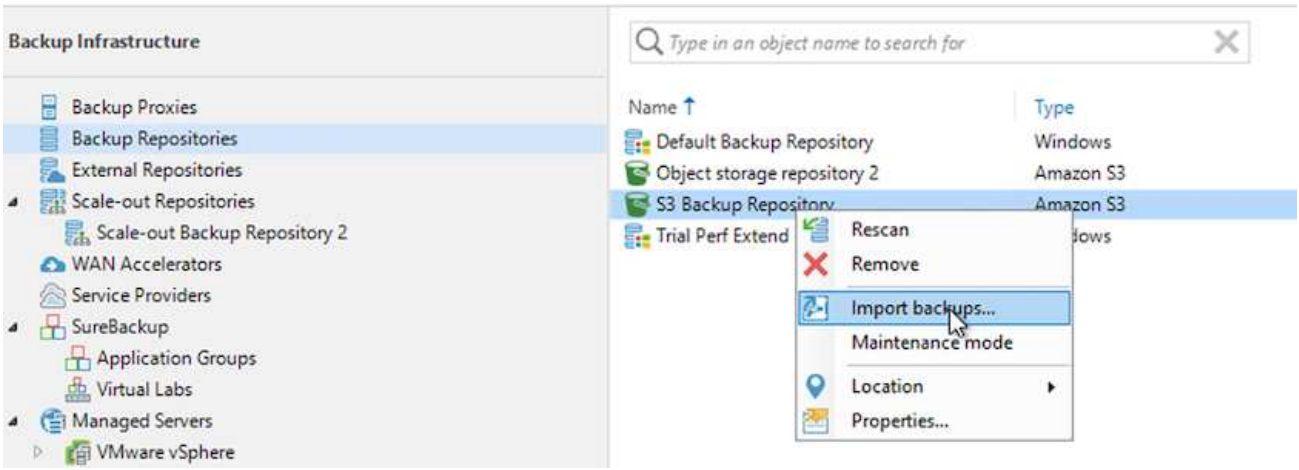


6. Infine, seleziona Fine per completare il processo e aggiungere il repository.

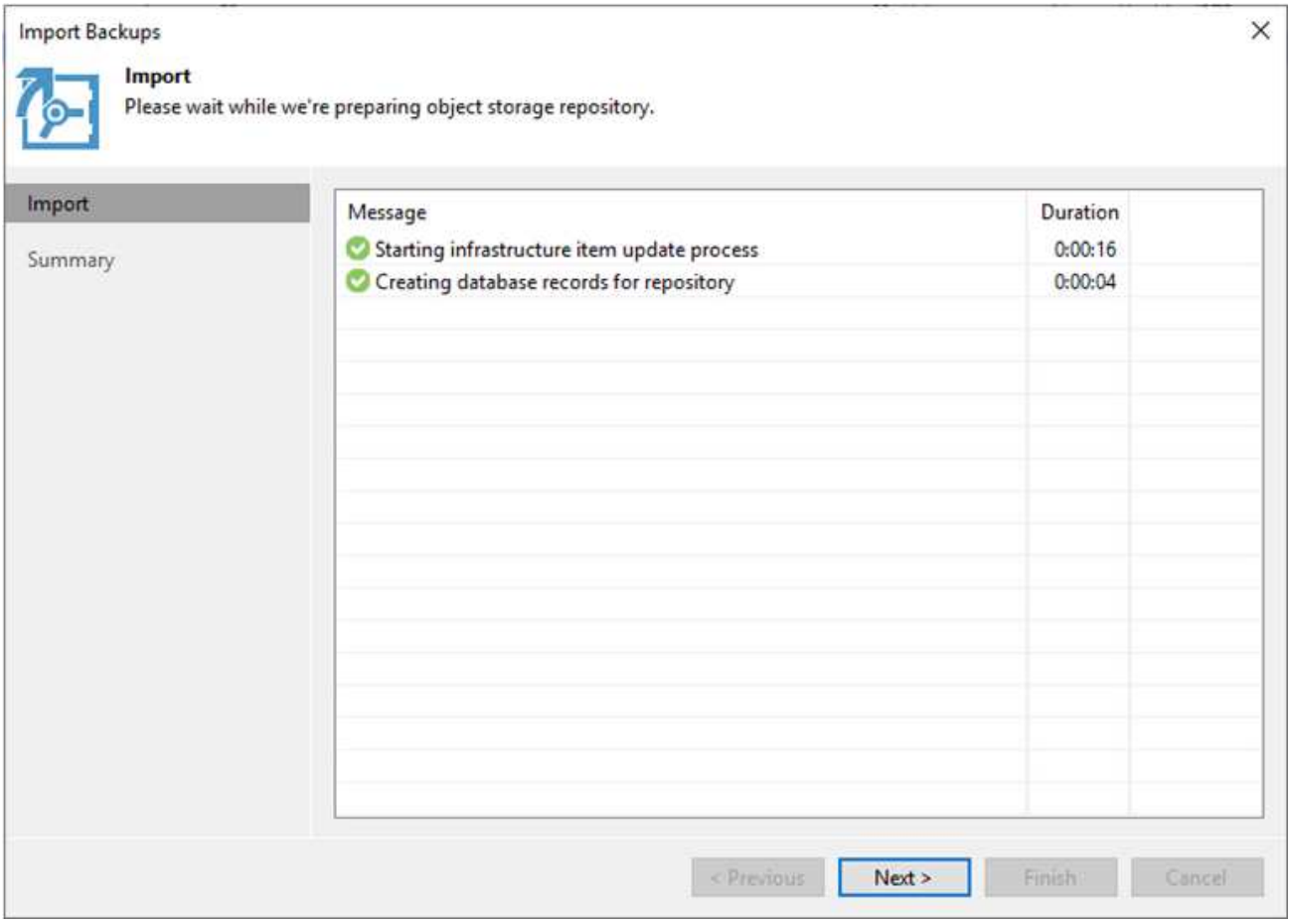
▼ **Importa backup dall'archiviazione di oggetti S3**

Per importare i backup dal repository S3 aggiunto nella sezione precedente, completare i passaggi seguenti.

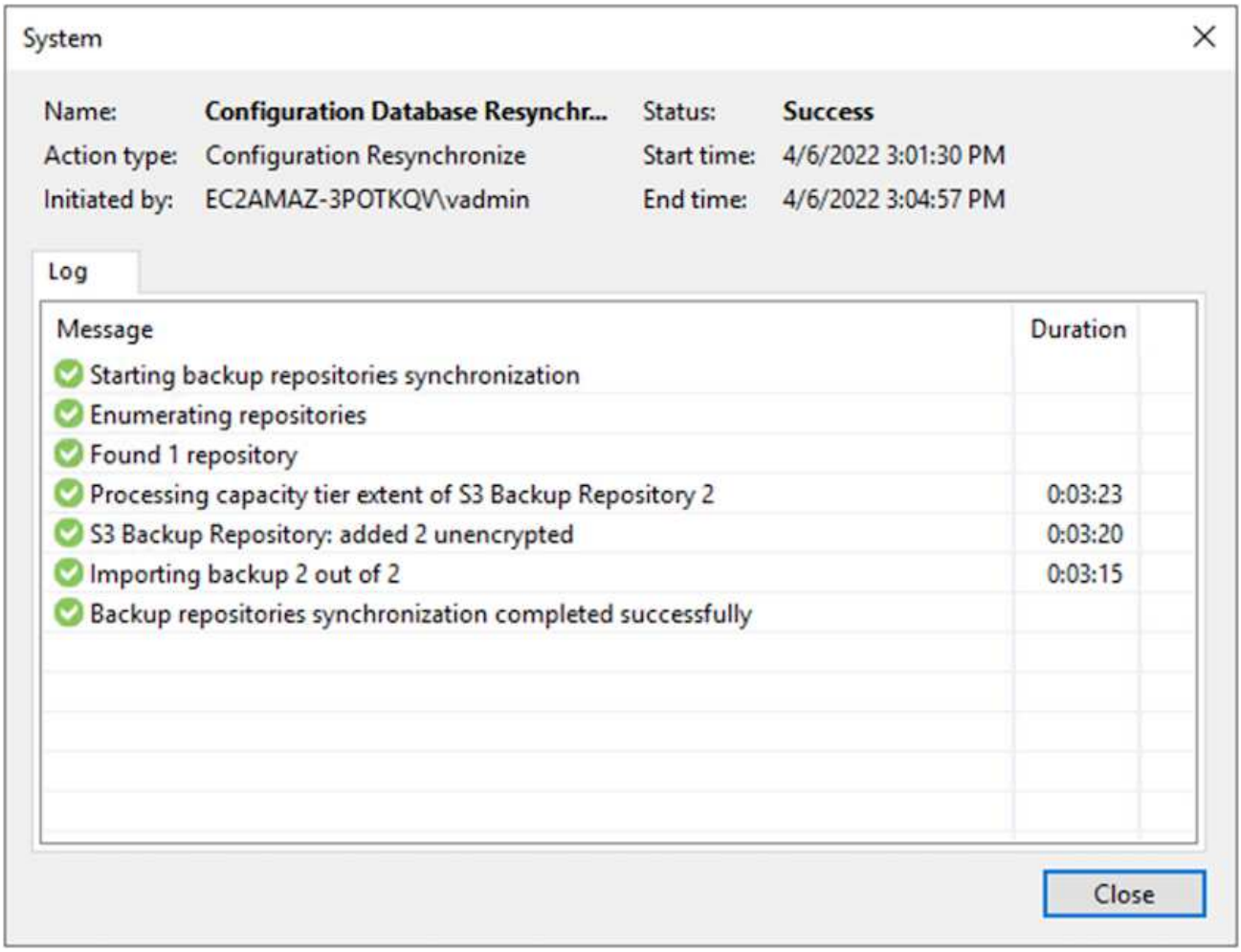
1. Dal repository di backup S3, seleziona Importa backup per avviare la procedura guidata Importa backup.



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



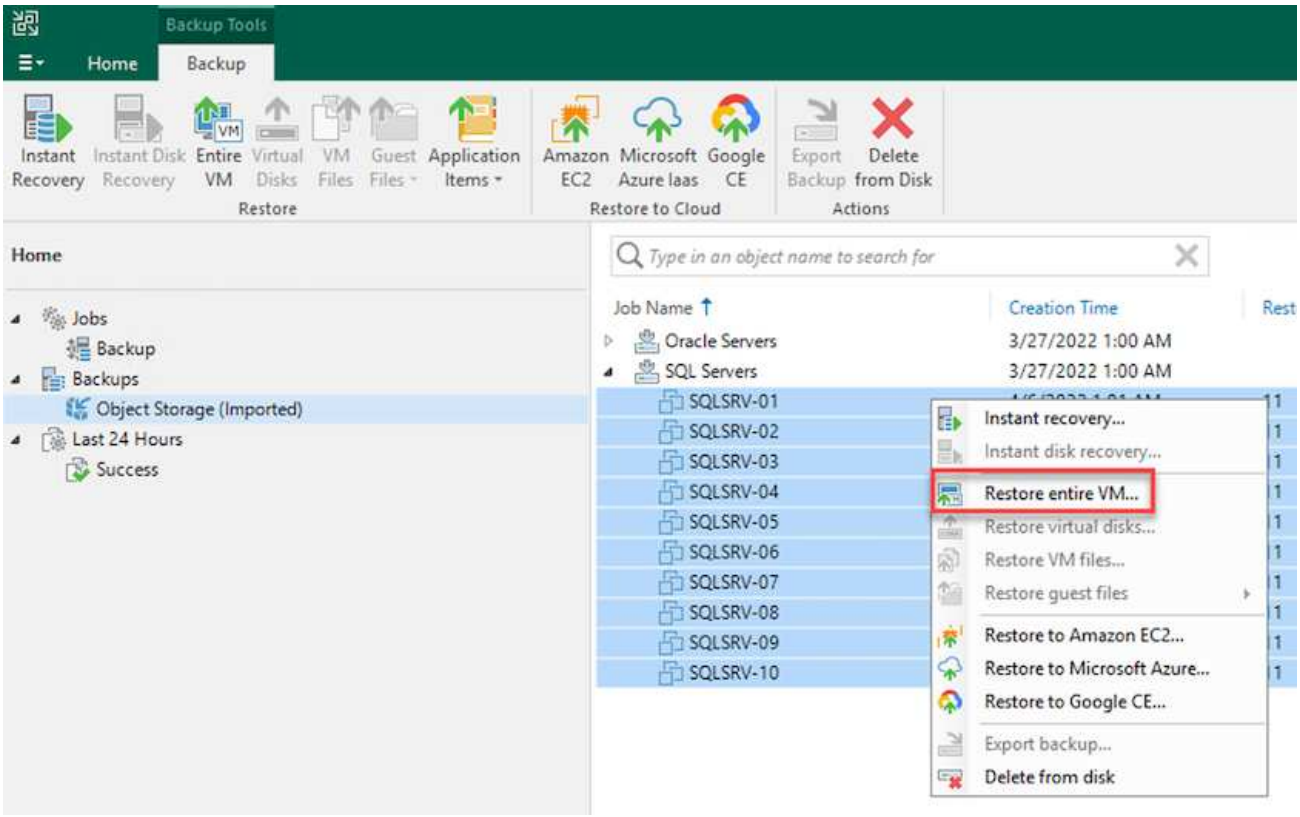
3. Una volta completata l'importazione, è possibile ripristinare le VM nel cluster VMware Cloud.



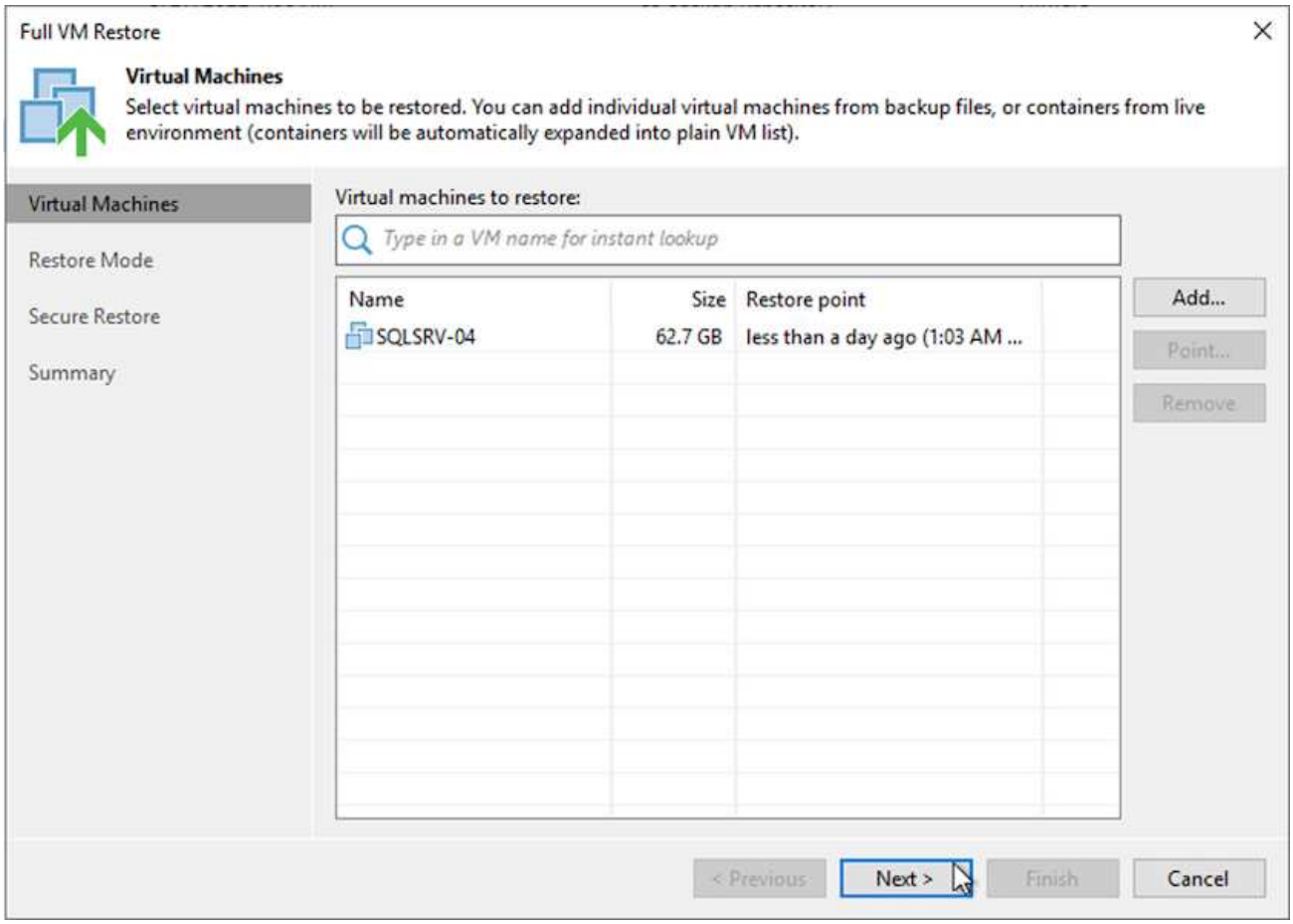
▼ **Ripristina le VM delle applicazioni con il ripristino completo di Veeam su VMware Cloud**

Per ripristinare le macchine virtuali SQL e Oracle nel dominio/cluster del carico di lavoro VMware Cloud on AWS, completare i seguenti passaggi.

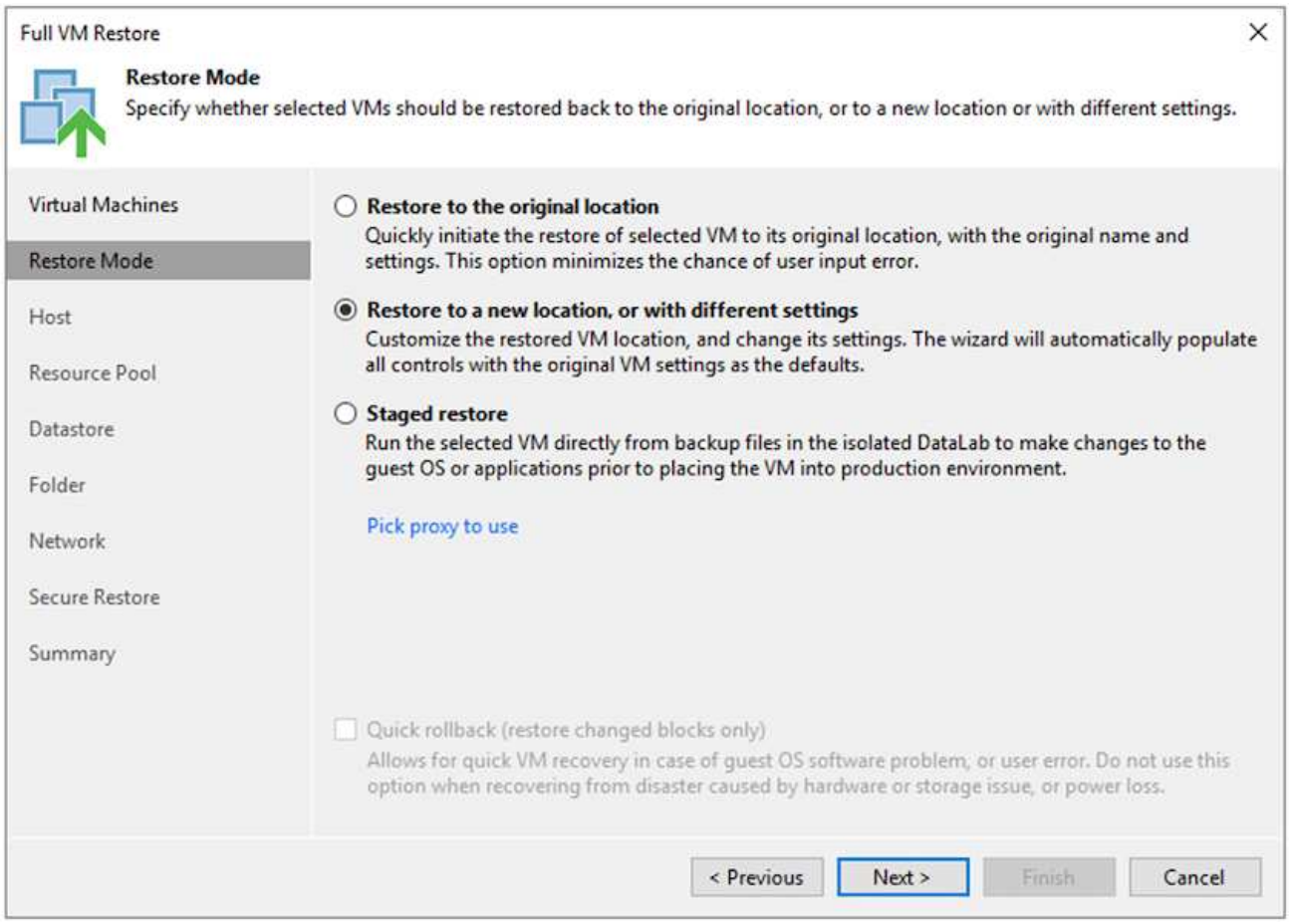
1. Dalla home page di Veeam, seleziona l'archivio oggetti contenente i backup importati, seleziona le VM da ripristinare, quindi fai clic con il pulsante destro del mouse e seleziona Ripristina intera VM.



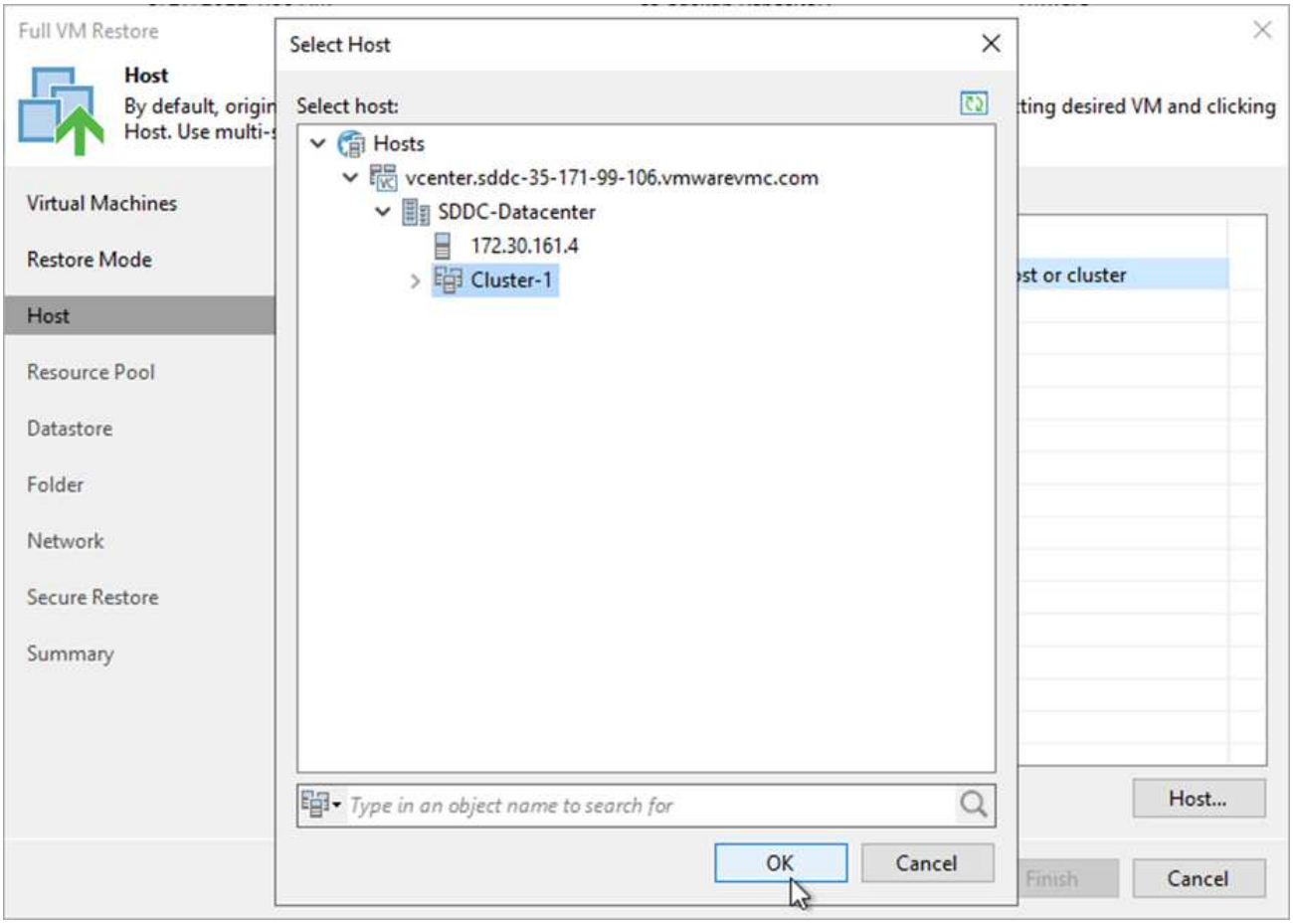
2. Nella prima pagina della procedura guidata Ripristino completo della VM, modificare le VM da sottoporre a backup, se desiderato, e selezionare Avanti.



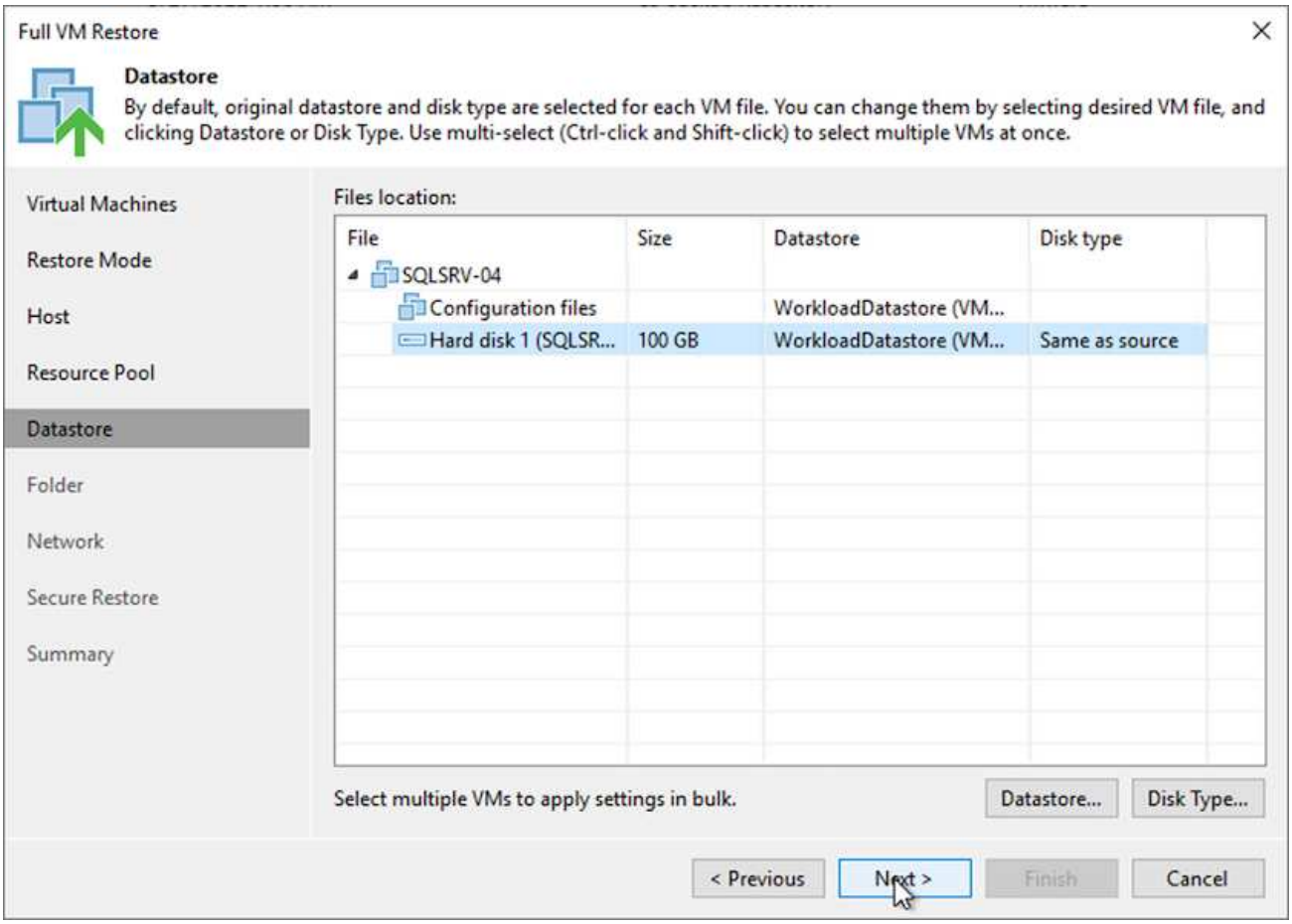
3. Nella pagina Modalità di ripristino, seleziona Ripristina in una nuova posizione o con impostazioni diverse.



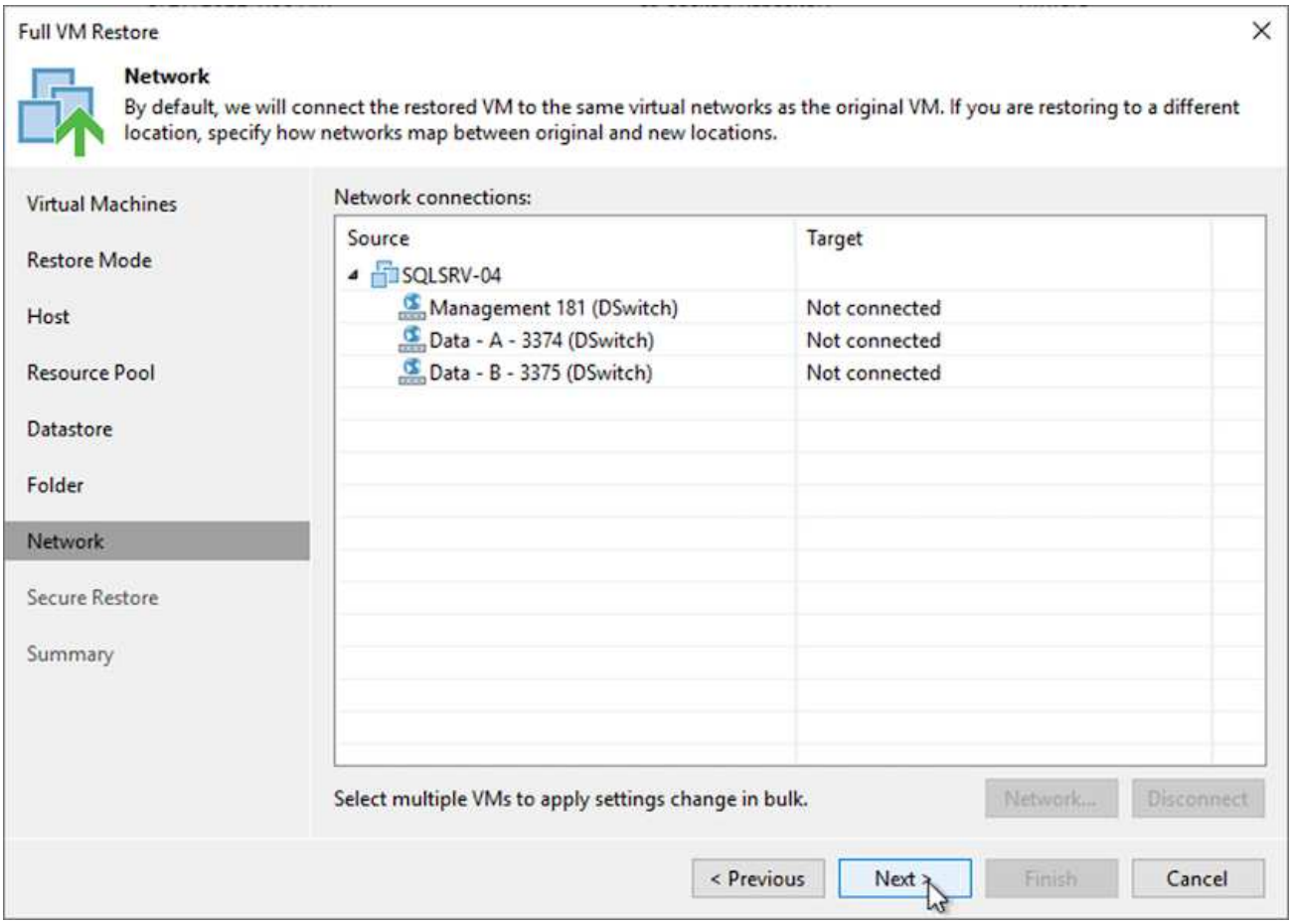
4. Nella pagina host, seleziona l'host o il cluster ESXi di destinazione su cui ripristinare la VM.

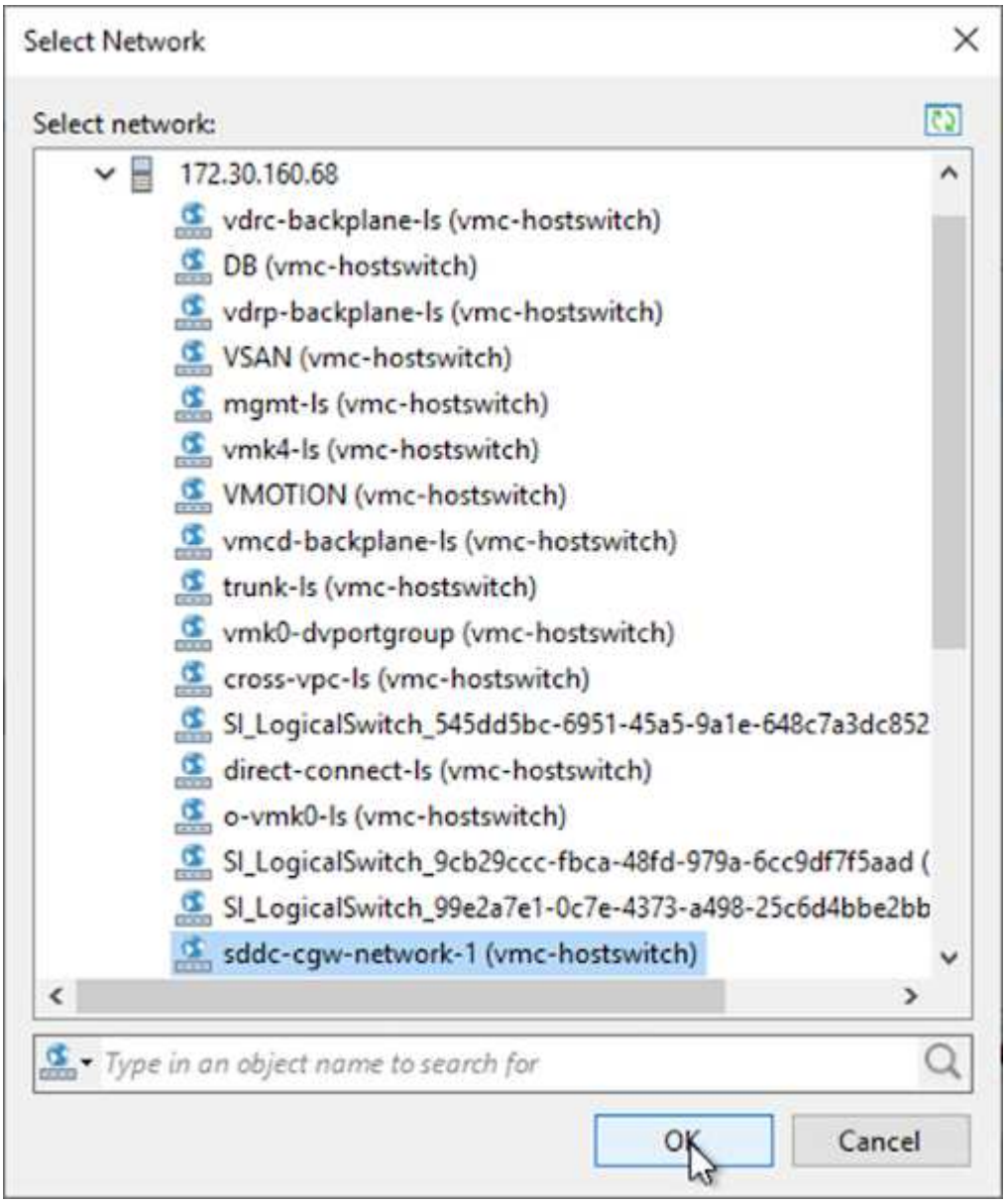


5. Nella pagina Datastore, selezionare la posizione del datastore di destinazione sia per i file di configurazione che per il disco rigido.



6. Nella pagina Rete, mappare le reti originali sulla VM 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 VM ripristinata per rilevare eventuali malware, rivedere la pagina di riepilogo e fare clic su Fine per avviare il ripristino.

Ripristinare i dati dell'applicazione SQL Server

La seguente procedura fornisce istruzioni su come ripristinare un SQL Server in VMware Cloud Services in AWS in caso di un disastro che renda inutilizzabile il sito locale.

Per poter proseguire con le fasi di ripristino si presuppone che siano soddisfatti i seguenti prerequisiti:

1. La VM Windows Server è stata ripristinata su VMware Cloud SDDC tramite Veeam Full Restore.
2. È stato stabilito un server SnapCenter secondario e il ripristino e la configurazione del database SnapCenter sono stati completati utilizzando i passaggi descritti nella sezione"Riepilogo del processo di backup e ripristino SnapCenter ."

▼ **VM: configurazione post-ripristino per VM SQL Server**

Una volta completato il ripristino della VM, è necessario configurare la rete e altri elementi in preparazione per il nuovo rilevamento della VM host in SnapCenter.

1. Assegnare nuovi indirizzi IP per la gestione e iSCSI o NFS.
2. Aggiungere 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 SnapCenter SMCore, Plug-in per Windows e Plug-in per SQL Server.

Per riscoprire automaticamente le VM ripristinate in SnapCenter, il nome di dominio completo (FQDN) deve essere identico alla VM originariamente aggiunta a SnapCenter in locale.

▼ Configurare l'archiviazione FSx per il ripristino di SQL Server

Per completare il processo di ripristino di emergenza per una macchina virtuale di SQL Server, è necessario interrompere la relazione SnapMirror esistente dal cluster FSx e concedere l'accesso al volume. Per farlo, completa i seguenti passaggi.

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

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

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

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

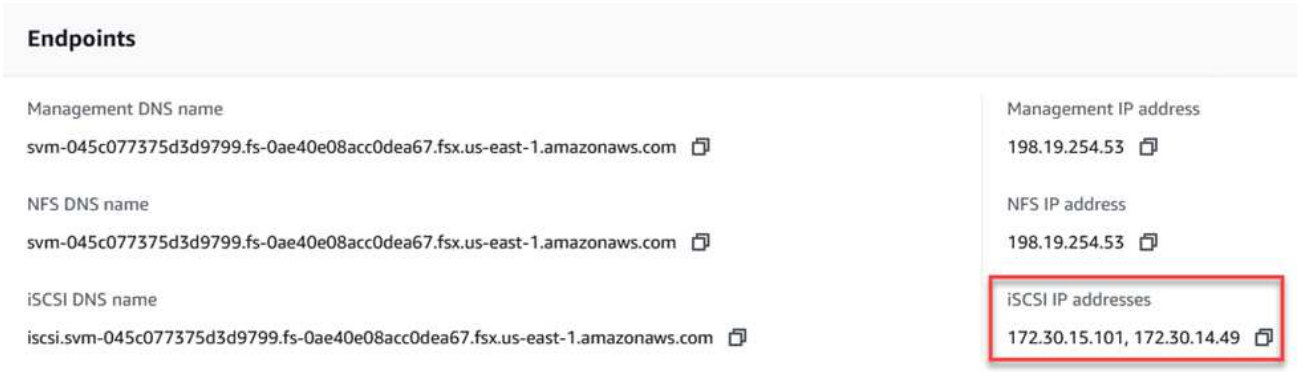
3. Infine, mappa i LUN al gruppo di iniziatori appena creato:

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

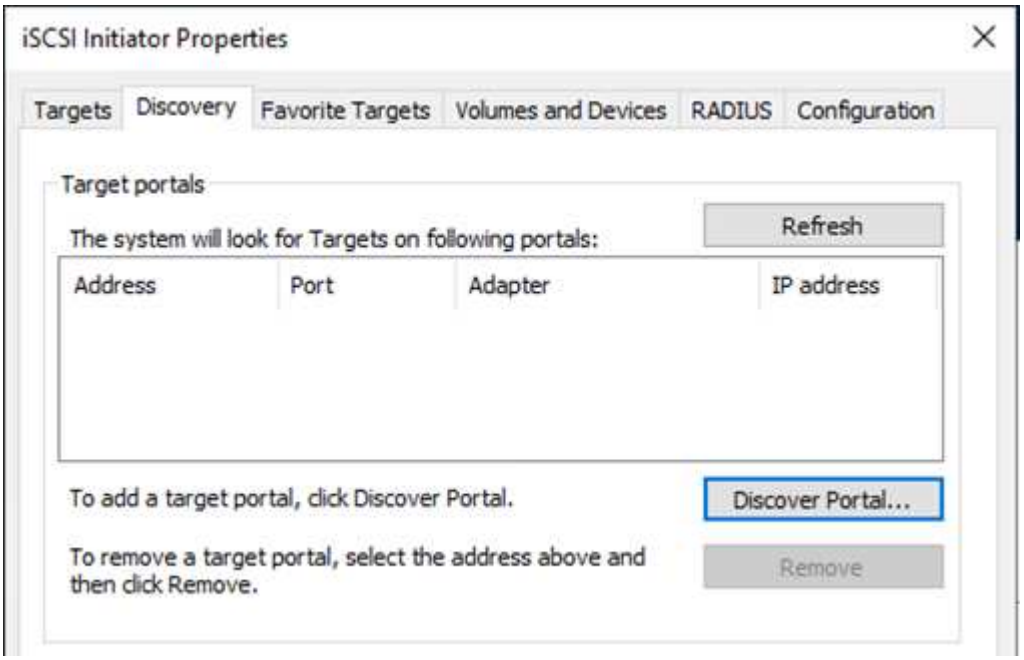
4. Per trovare il nome del percorso, eseguire il comando `lun show` comando.

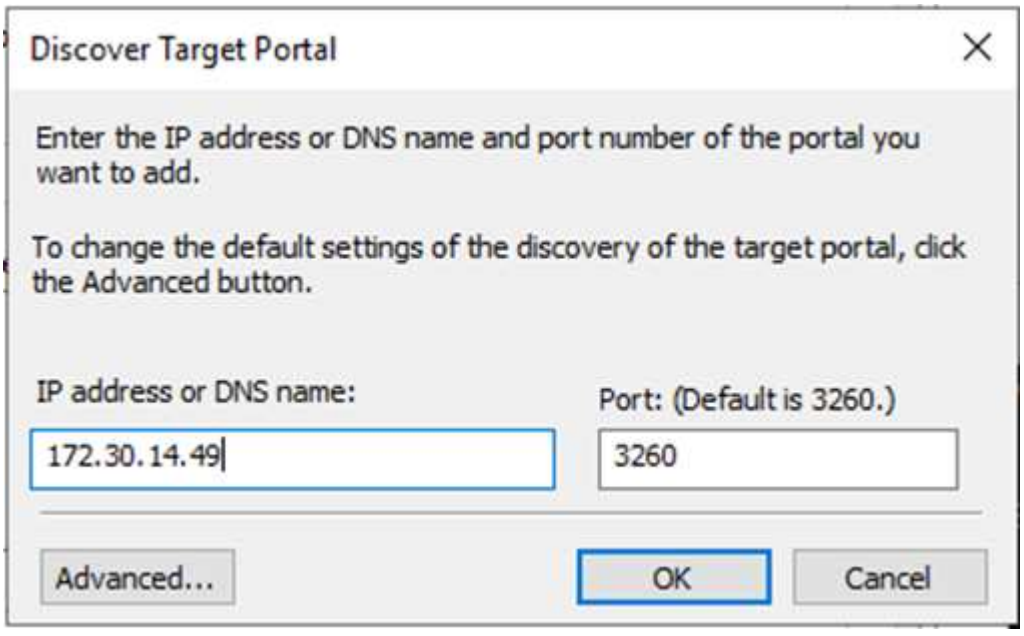
▼ Configurare la VM Windows per l'accesso iSCSI e scoprire i file system

1. Dalla VM di SQL Server, configura la scheda di rete iSCSI per comunicare sul gruppo di porte VMware stabilito con connettività alle interfacce di destinazione iSCSI sulla tua istanza FSx.
2. Aprire l'utilità Proprietà dell'iniziatore iSCSI e cancellare le vecchie impostazioni di connettività nelle schede Rilevamento, Destinazioni preferite e Destinazioni.
3. Individuare l'indirizzo/gli indirizzi IP per accedere all'interfaccia logica iSCSI sull'istanza/cluster FSx. Questa opzione è disponibile nella console AWS in Amazon FSx > ONTAP > Storage Virtual Machines.

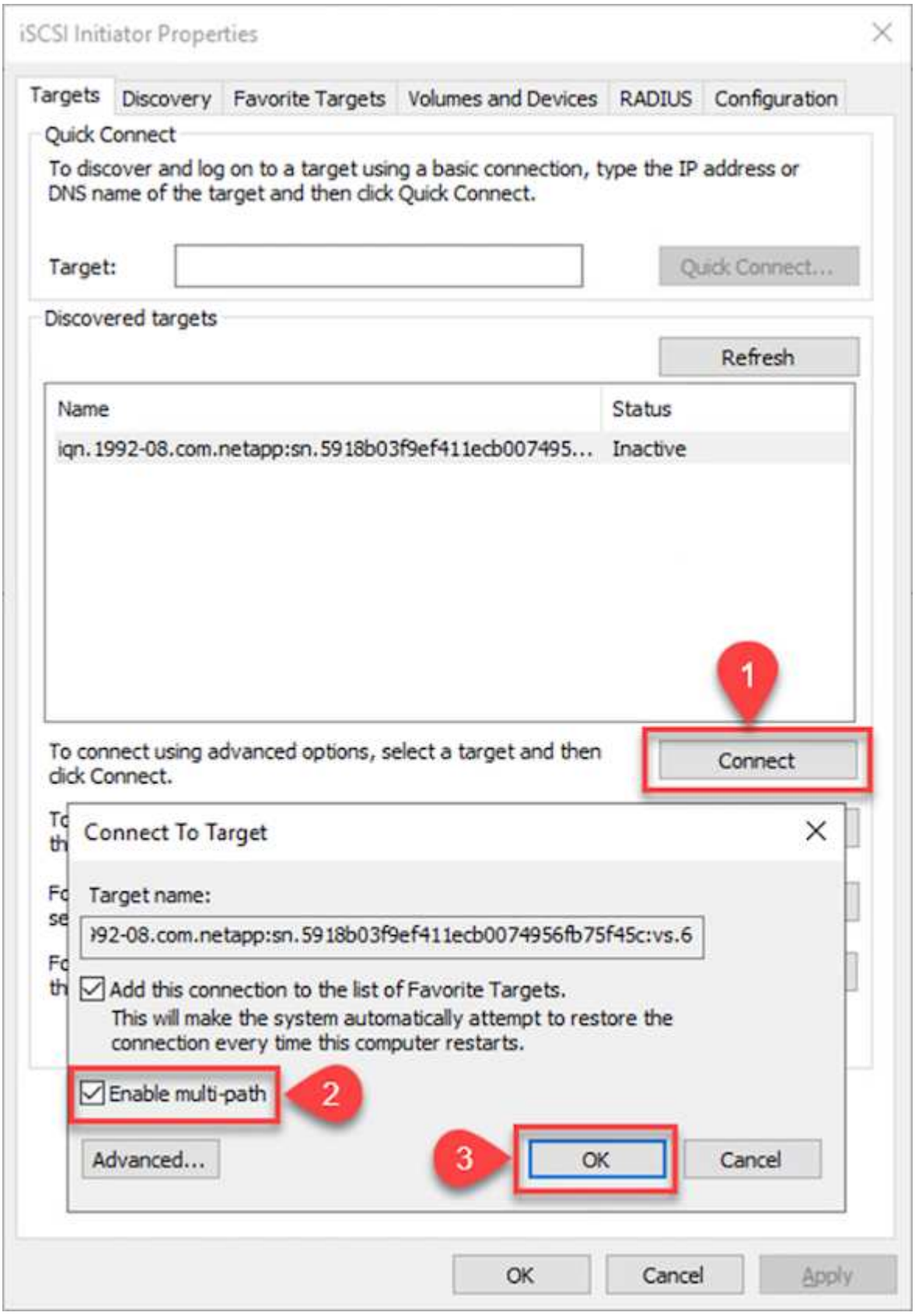


4. Dalla scheda Discovery, fare clic su Discover Portal e immettere gli indirizzi IP per le destinazioni iSCSI FSx.



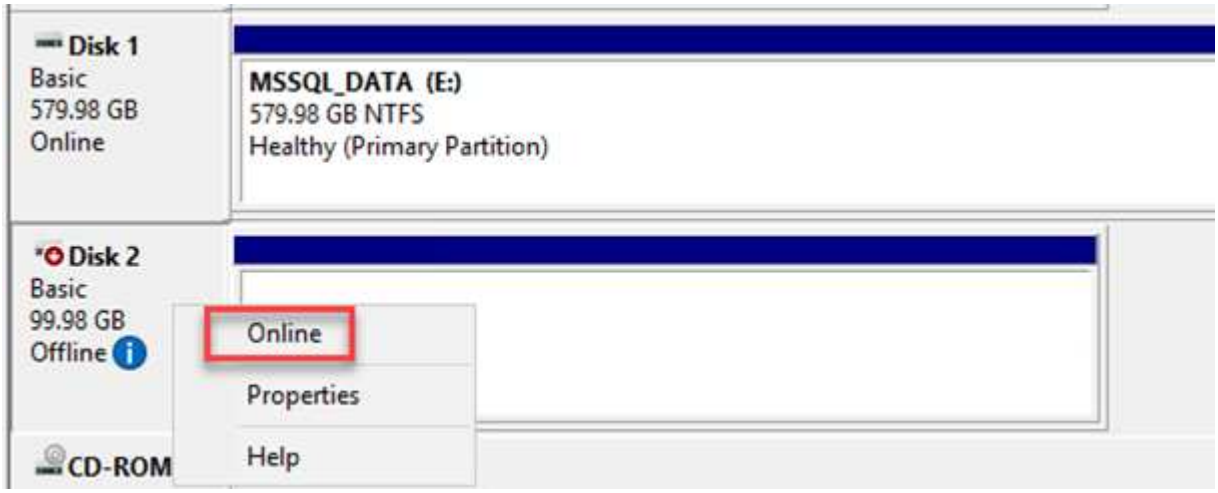


5. Nella scheda Destinazione, fare clic su Connetti, selezionare Abilita multipercorso se appropriato per la configurazione, quindi fare clic su OK per connettersi alla destinazione.



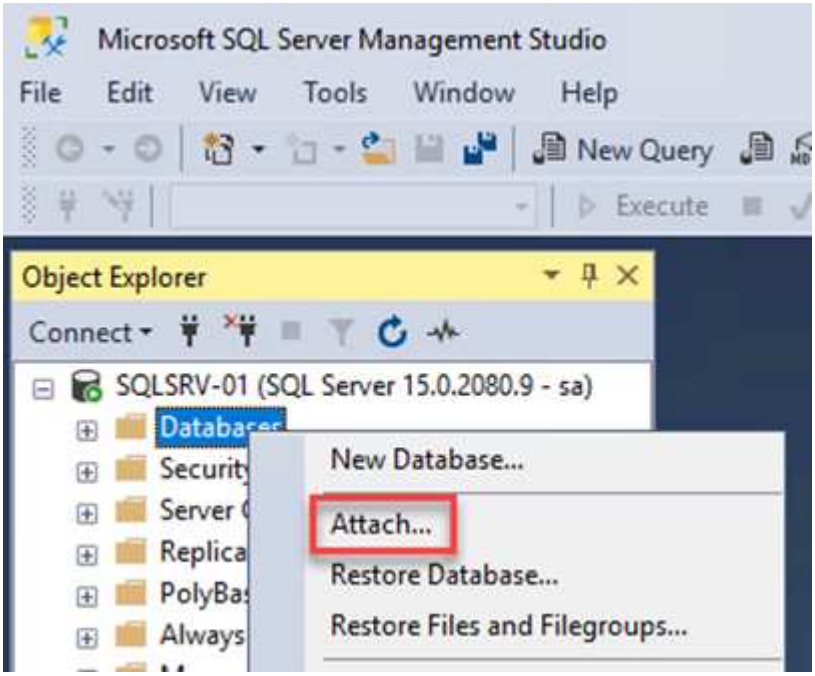
6. Aprire l'utilità Gestione computer e portare i dischi online. Verificare che mantengano le stesse lettere di

unità assegnate in precedenza.

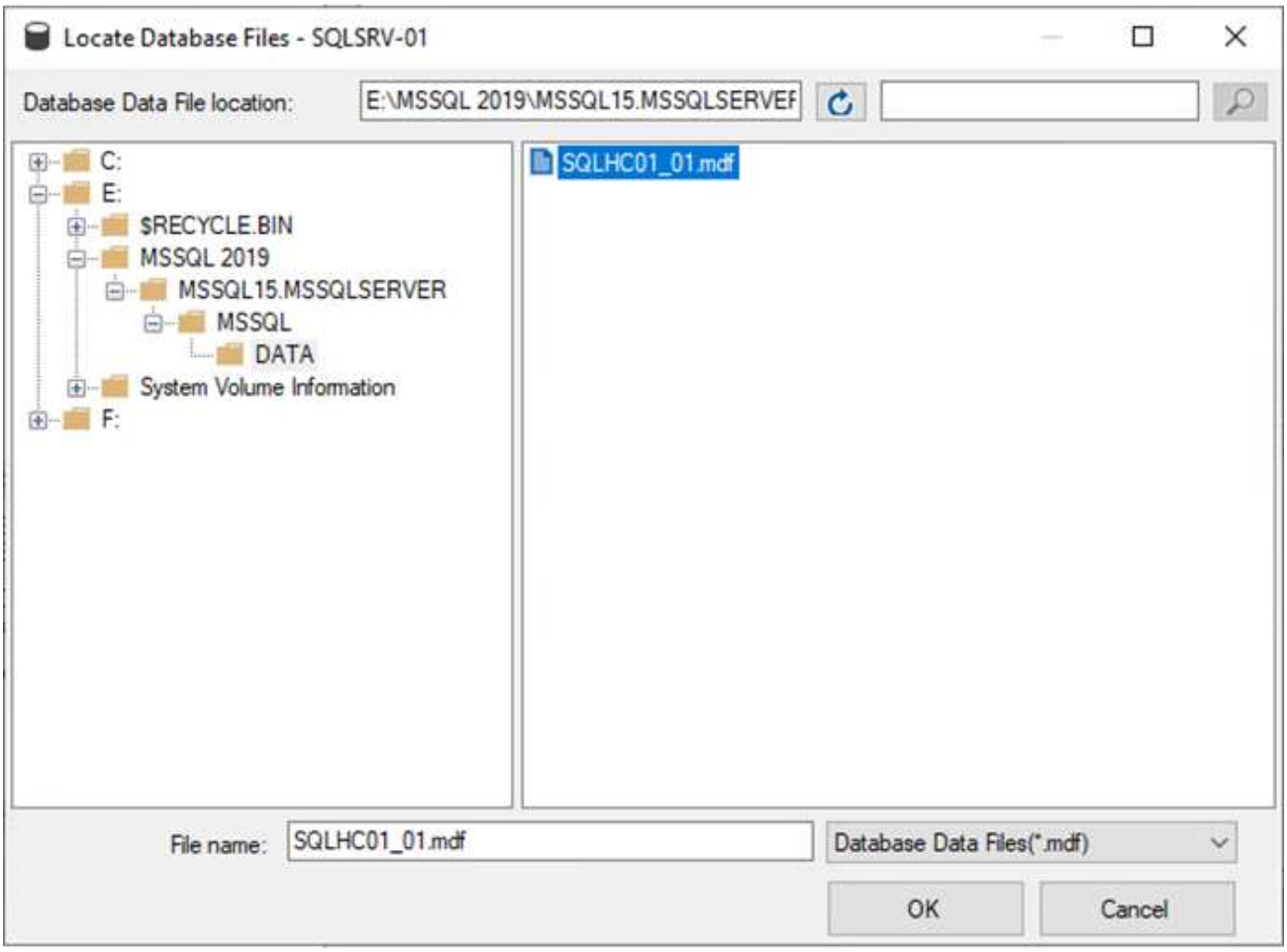


▼ **Collegare i database di SQL Server**

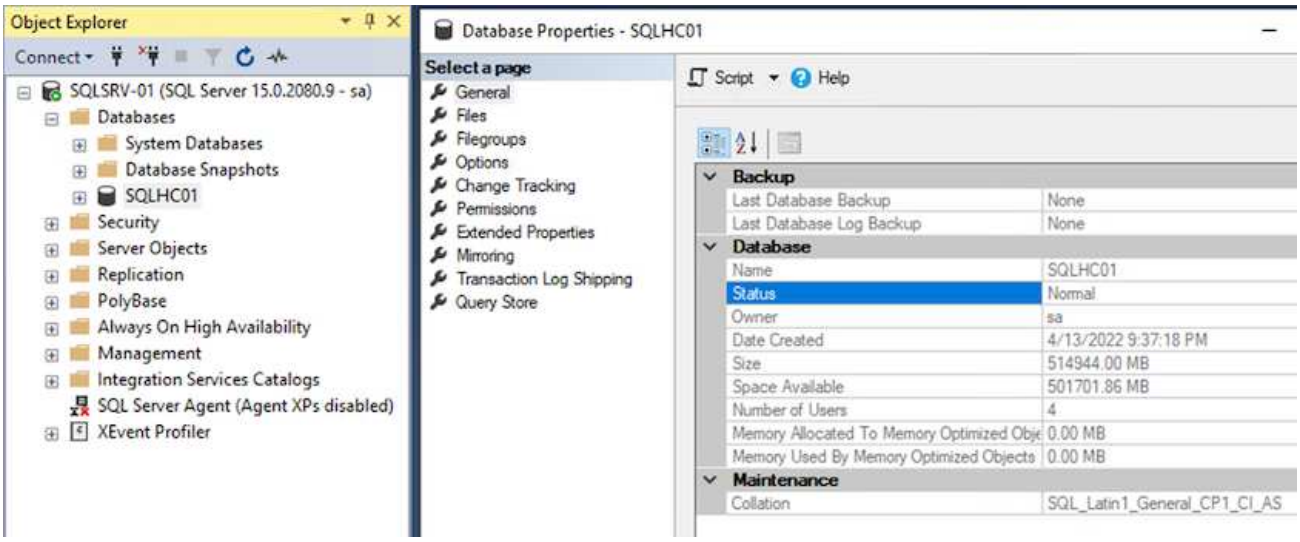
1. Dalla VM di SQL Server, aprire Microsoft SQL Server Management Studio e selezionare Collega per avviare il processo di connessione al database.



2. Fare clic su Aggiungi e andare alla cartella contenente il file del database primario di SQL Server, selezionarlo e fare clic su OK.



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

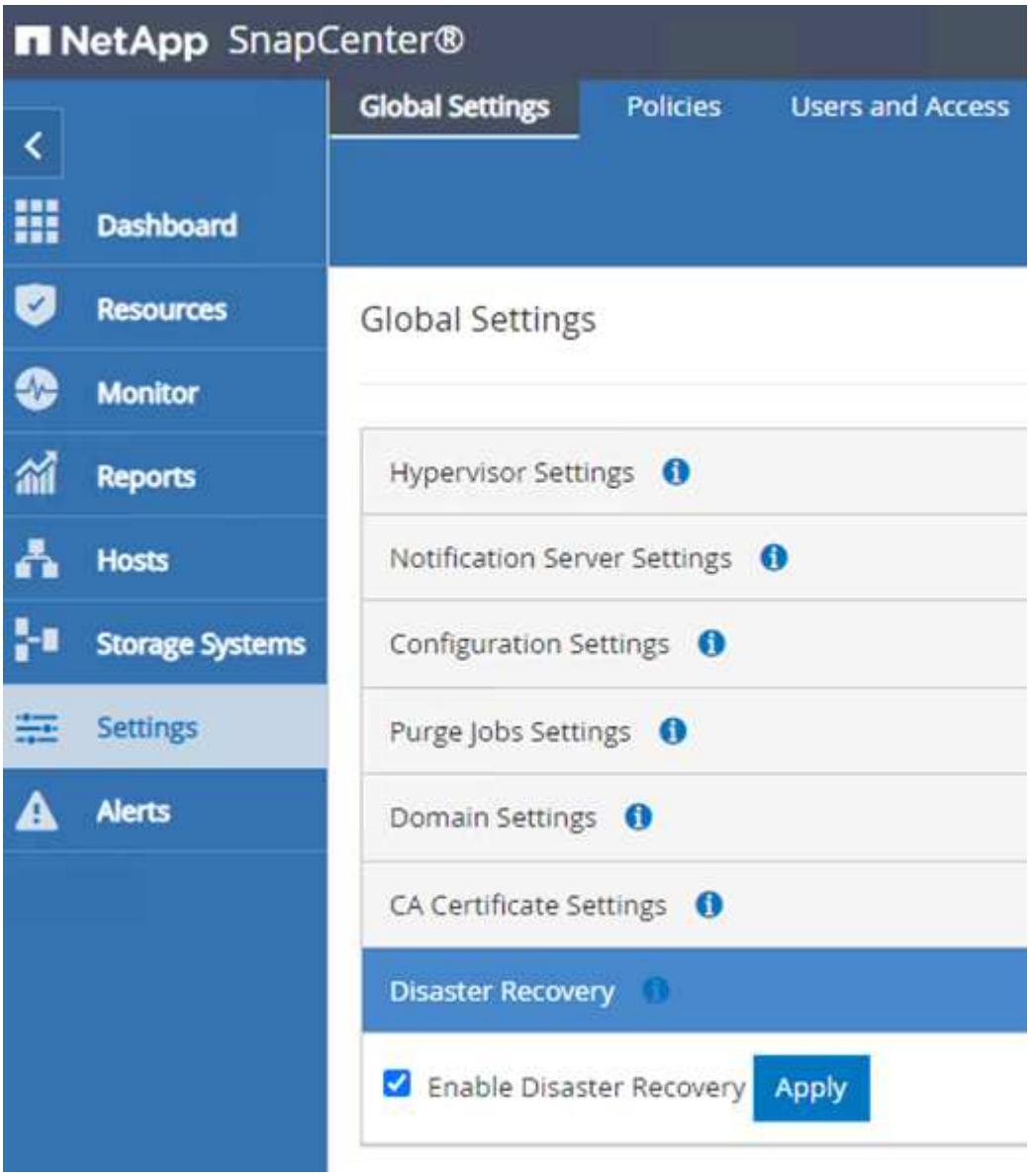


▼ **Conferma la comunicazione SnapCenter con il plug-in di SQL Server**

Una volta ripristinato lo stato precedente del database SnapCenter , gli host di SQL Server vengono automaticamente rilevati. Per far funzionare tutto correttamente, tieni presente i seguenti prerequisiti:

- SnapCenter deve essere impostato in modalità Disaster Recover. Questa operazione può essere eseguita tramite l'API Swagger o nelle Impostazioni globali in Disaster Recovery.
- Il nome di dominio completo (FQDN) di SQL Server deve essere identico all'istanza in esecuzione nel data center locale.
- La relazione SnapMirror originale deve essere interrotta.
- I LUN contenenti il database devono essere montati sull'istanza di SQL Server e il database deve essere collegato.

Per confermare che SnapCenter è in modalità Disaster Recovery, accedere a Impostazioni dal client Web SnapCenter . Vai alla scheda Impostazioni globali e poi fai clic su Ripristino di emergenza. Assicurarsi che la casella di controllo Abilita ripristino di emergenza sia abilitata.



Ripristinare i dati dell'applicazione Oracle

La seguente procedura fornisce istruzioni su come ripristinare i dati delle applicazioni Oracle in VMware Cloud Services in AWS in caso di un disastro che renda inutilizzabile il sito locale.

Per proseguire con i passaggi di ripristino, è necessario soddisfare i seguenti prerequisiti:

1. La VM del server Oracle Linux è stata ripristinata su VMware Cloud SDDC utilizzando Veeam Full Restore.
2. È stato stabilito un server SnapCenter secondario e il database SnapCenter e i file di configurazione sono stati ripristinati utilizzando i passaggi descritti in questa sezione"Riepilogo del processo di backup e ripristino SnapCenter ."

▼ **Configurare FSx per il ripristino di Oracle: interrompere la relazione SnapMirror**

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

1. Dopo aver effettuato l'accesso alla CLI di FSx, eseguire il comando seguente per visualizzare i volumi filtrati in base al nome corretto.

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

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

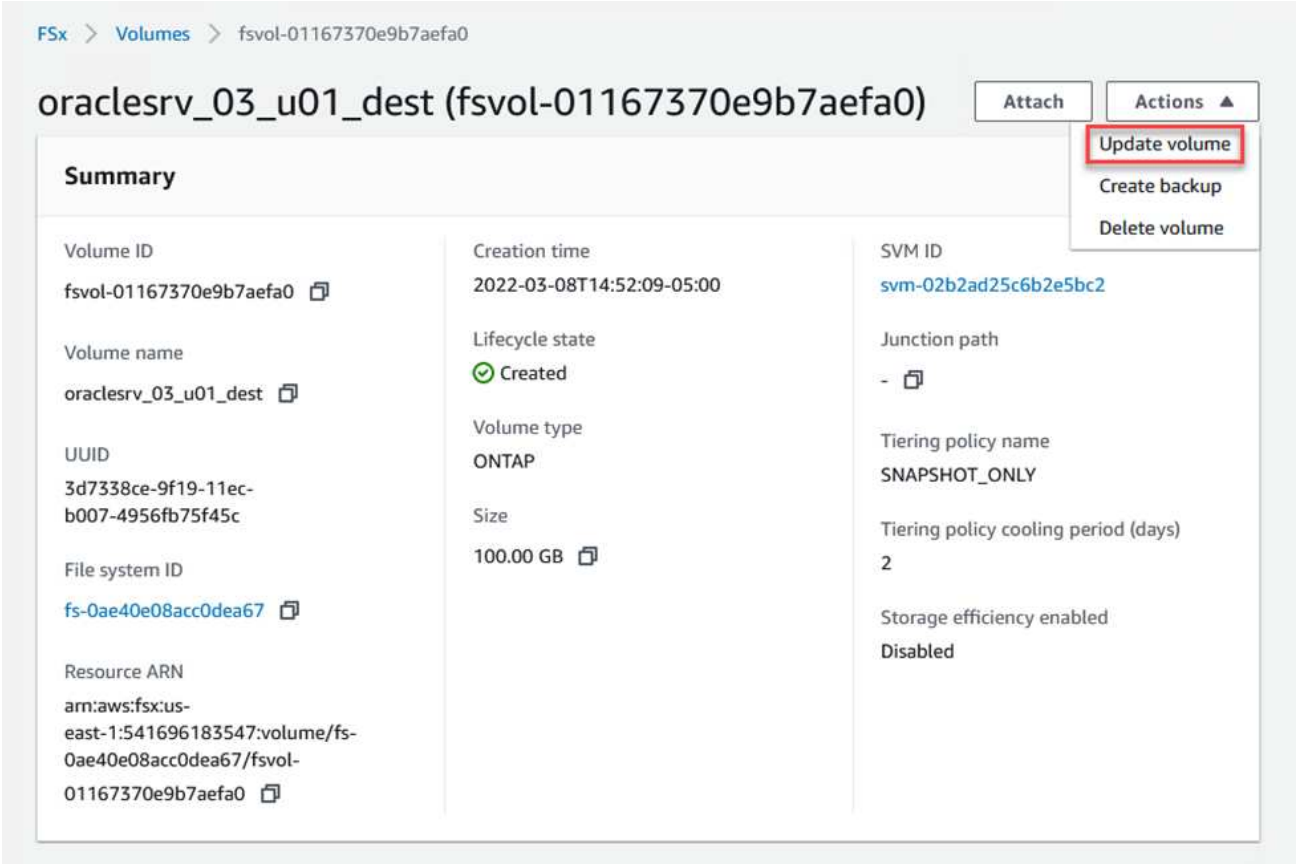
2. Eseguire il comando seguente per interrompere le relazioni SnapMirror esistenti.

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

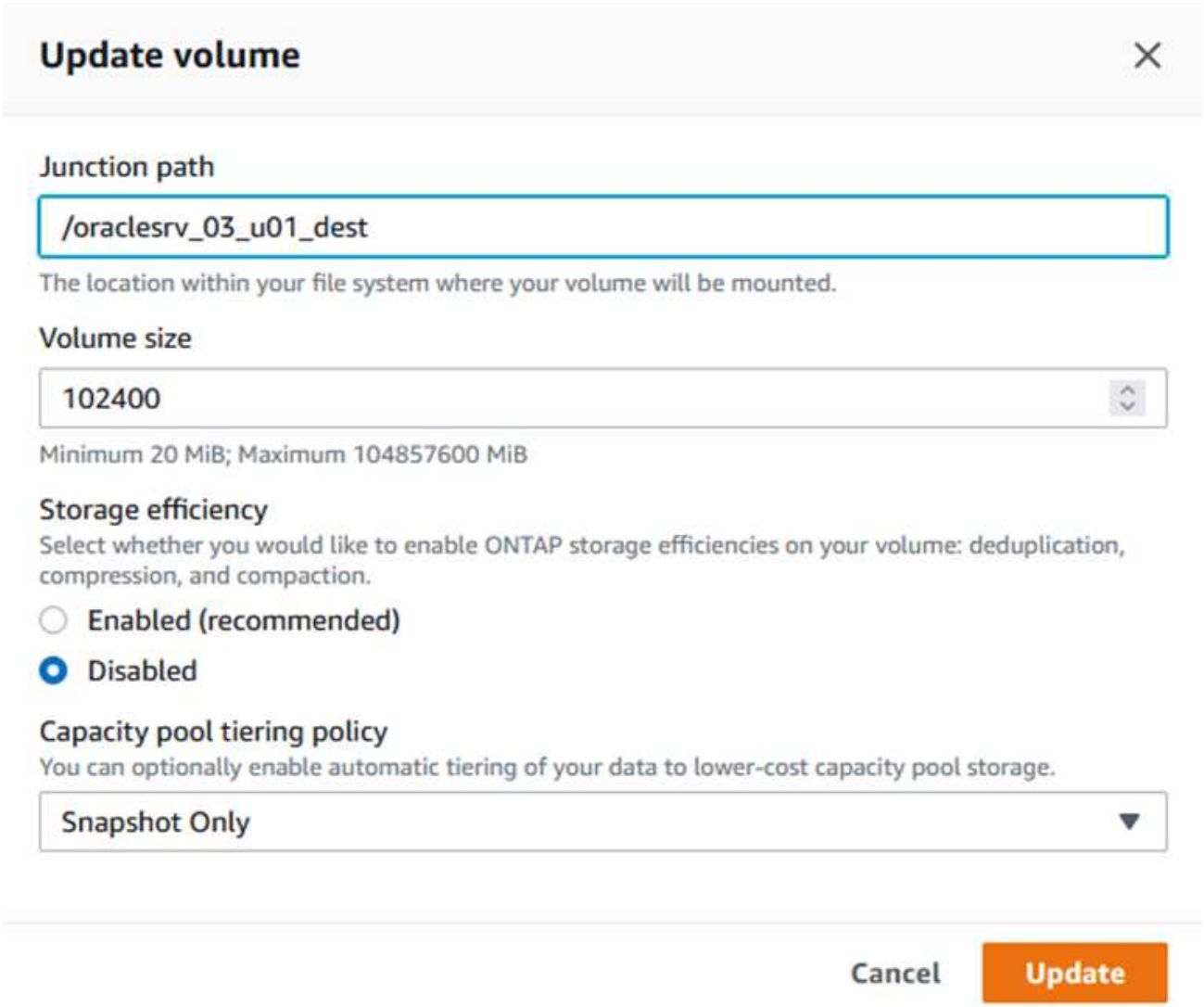
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Aggiorna il percorso di giunzione nel client Web Amazon FSx :



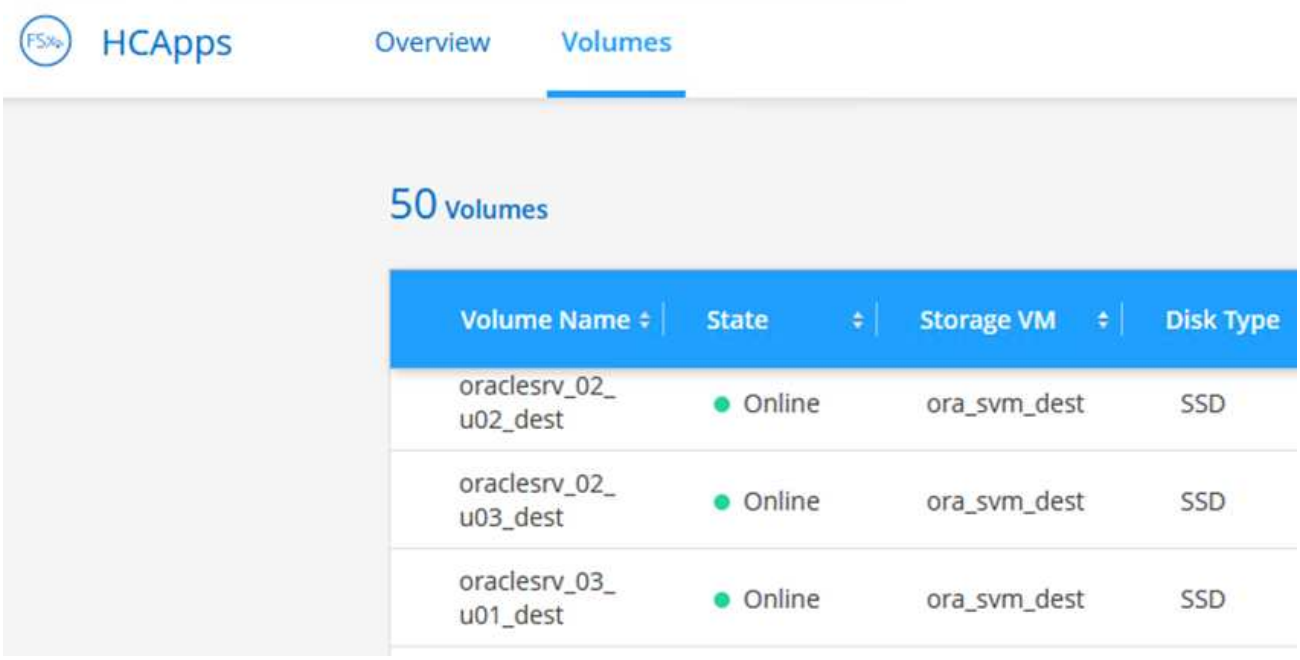
4. Aggiungere il nome del percorso di giunzione e fare clic su Aggiorna. Specificare questo percorso di giunzione quando si monta il volume NFS dal server Oracle.



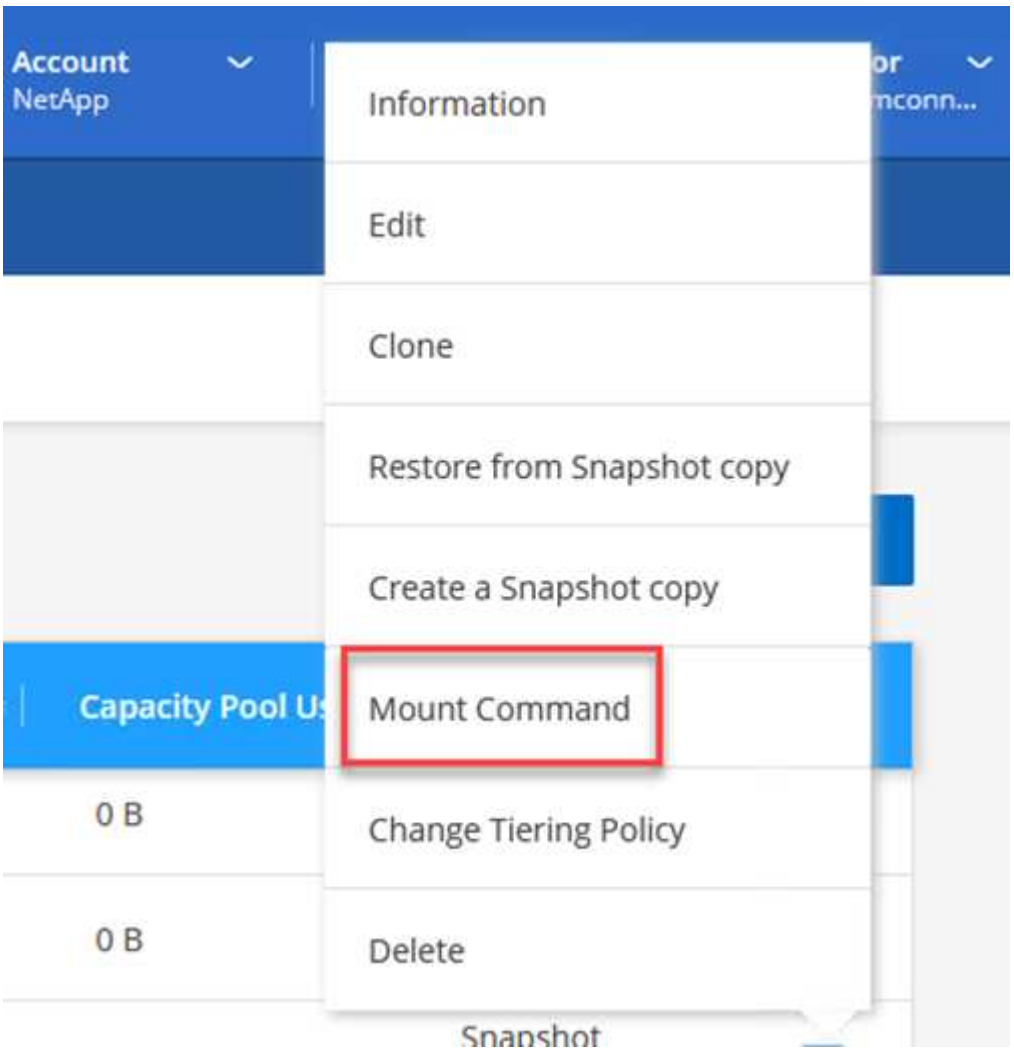
▼ **Montare volumi NFS su Oracle Server**

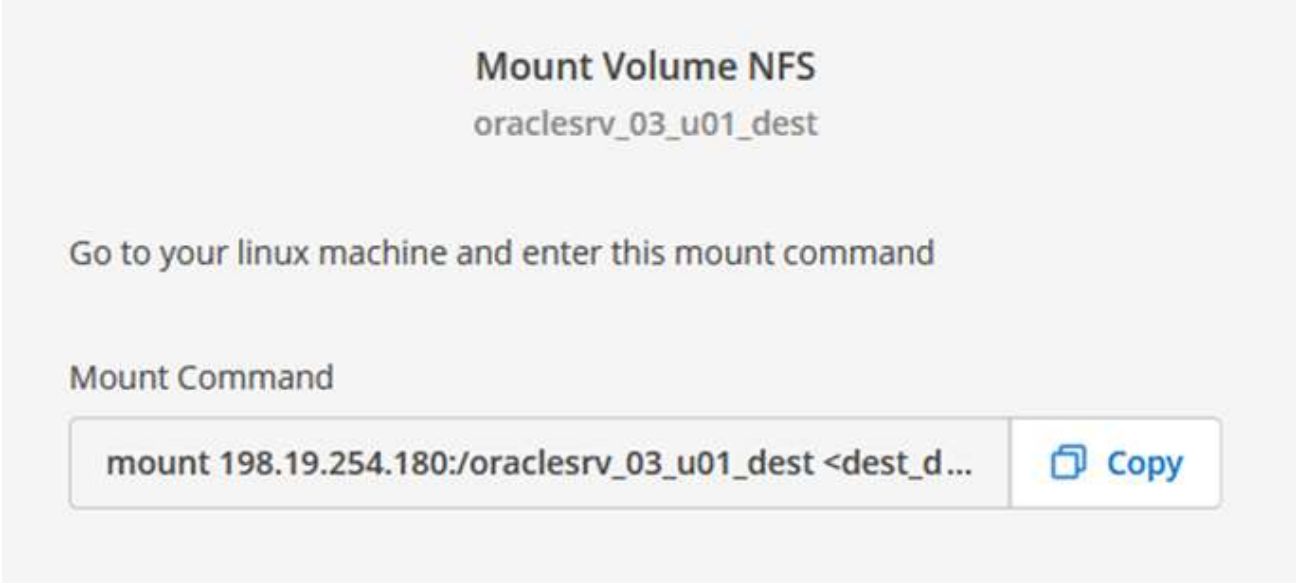
In Cloud Manager, è possibile ottenere il comando mount con l'indirizzo IP LIF NFS corretto per montare i volumi NFS che contengono i file e i log del database Oracle.

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



2. Dal menu Azione, seleziona Comando di montaggio per visualizzare e copiare il comando di montaggio da utilizzare sul nostro 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` file per includere i comandi di montaggio.

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

Rifasamento

Una volta completato con successo il processo di failover descritto in questa soluzione, SnapCenter e Veeam riprendono le loro funzioni di backup in esecuzione su AWS e FSx ONTAP viene ora designato come storage primario senza alcuna relazione SnapMirror esistente con il data center locale originale. Dopo aver ripreso il normale funzionamento in sede, è possibile utilizzare un processo identico a quello descritto in questa documentazione per eseguire il mirroring dei dati sul sistema di archiviazione ONTAP in sede.

Come descritto anche in questa documentazione, è possibile configurare SnapCenter per eseguire il mirroring dei volumi di dati dell'applicazione da FSx ONTAP a un sistema di archiviazione ONTAP residente in locale. Allo stesso modo, è possibile configurare Veeam per replicare le copie di backup su Amazon S3 utilizzando un repository di backup scalabile, in modo che tali backup siano accessibili a un server di backup Veeam residente nel data center locale.

Il failback esula dall'ambito di questa documentazione, ma differisce poco dal processo dettagliato qui descritto.

Conclusione

Il caso d'uso 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 forniscono tecnologie di data-mirroring comprovate che consentono alle organizzazioni di progettare soluzioni di disaster recovery che abbracciano tecnologie locali e ONTAP residenti presso i principali provider cloud.

FSx ONTAP su AWS è una di queste soluzioni che consente un'integrazione perfetta con SnapCenter e SyncMirror per replicare i dati delle applicazioni sul cloud. Veeam Backup & Replication è un'altra tecnologia ben nota che si integra bene con i sistemi di storage NetApp ONTAP e può fornire il failover allo storage nativo di vSphere.

Questa soluzione presentava una soluzione di disaster recovery che utilizzava l'archiviazione guest connect da un sistema ONTAP che ospitava dati di applicazioni SQL Server e Oracle. SnapCenter con SnapMirror fornisce una soluzione facile da gestire per proteggere i volumi delle applicazioni sui sistemi ONTAP e replicarli su FSx o CVO residenti nel cloud. SnapCenter è una soluzione abilitata al DR per il failover di tutti i dati delle applicazioni su VMware Cloud su AWS.

Veeam Backup & Restore in VMware Cloud, con Amazon FSx ONTAP

Veeam Backup & Replication è una soluzione efficace e affidabile per la protezione dei dati nel cloud VMware. Questa soluzione illustra la corretta configurazione e impostazione per l'utilizzo di Veeam Backup and Replication per eseguire il backup e il ripristino delle VM delle applicazioni residenti nei datastore NFS FSx ONTAP in VMware Cloud.

Panoramica

VMware Cloud (in AWS) supporta l'uso di datastore NFS come storage supplementare e FSx ONTAP è una soluzione sicura per i clienti che hanno bisogno di archiviare 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 tradizionali funzionalità NetApp ONTAP .

Casi d'uso

Questa soluzione affronta i seguenti casi d'uso:

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

Datastore NFS che utilizzano Amazon FSx ONTAP

Tutte le macchine virtuali in questa soluzione risiedono su datastore NFS supplementari FSx ONTAP . L'utilizzo di FSx ONTAP come datastore NFS supplementare presenta numerosi vantaggi. Ad esempio, consente di:

- Crea un file system scalabile e altamente disponibile nel cloud, senza dover eseguire complesse operazioni di configurazione e gestione.
- Integralo con il tuo ambiente VMware esistente, consentendoti di utilizzare strumenti e processi familiari per gestire le tue 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 sulla distribuzione della soluzione**

Questo elenco fornisce i passaggi di alto livello necessari per configurare Veeam Backup & Replication, eseguire processi di backup e ripristino utilizzando FSx ONTAP come repository di backup ed eseguire ripristini di VM e database SQL Server e Oracle:

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

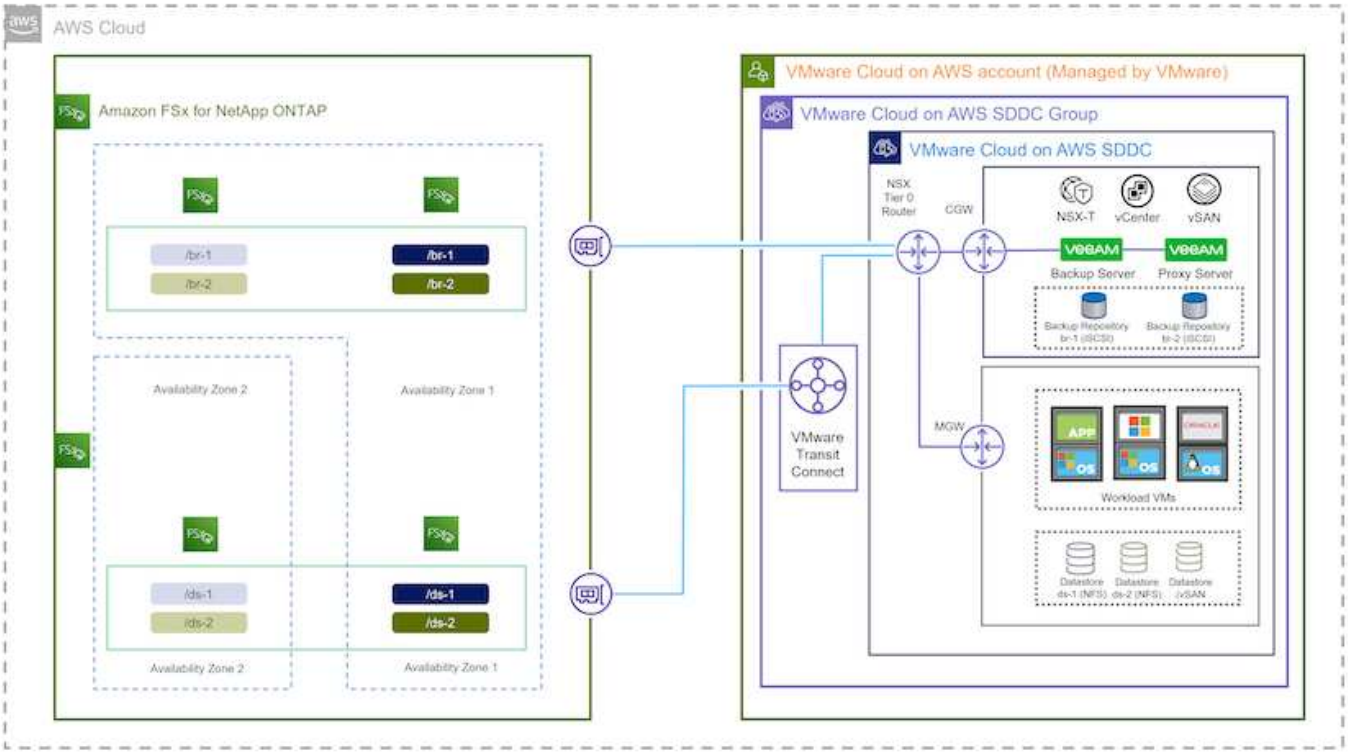
▼ **Prerequisiti**

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

1. File system FSx 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 tramite il suo indirizzo IP o nome di dominio completo.
3. VM Microsoft Windows Server da installare con i componenti Veeam Backup Proxy durante l'implementazione della soluzione.
4. Macchine virtuali Microsoft SQL Server con VMDK e dati applicativi residenti su datastore NFS FSx ONTAP . Per questa soluzione avevamo due database SQL su due VMDK separati.
   - Nota: come buona pratica, i file del database e del registro delle transazioni vengono posizionati su unità separate, poiché ciò migliorerà le prestazioni e l'affidabilità. Ciò è dovuto in parte al fatto che i registri delle transazioni vengono scritti in sequenza, mentre i file del database vengono scritti in modo casuale.
5. VM di Oracle Database con VMDK e dati applicativi residenti su datastore NFS FSx ONTAP .
6. VM di file server Linux e Windows con VMDK residenti su datastore NFS FSx 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, fare riferimento alla sezione Porte del "Guida utente di Veeam Backup and Replication per VMware vSphere" .

Architettura di alto livello

Il test/la convalida di questa soluzione sono stati eseguiti in un laboratorio che potrebbe corrispondere o meno all'ambiente di distribuzione finale. Per ulteriori informazioni, consultare le sezioni seguenti.



▼ **Componenti hardware/software**

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

- VM Microsoft Windows situate su un datastore NFS FSx ONTAP
- VM Linux (CentOS) situate su un datastore NFS FSx ONTAP
- VM di Microsoft SQL Server situate su un datastore NFS FSx ONTAP
  - Due database ospitati su VMDK separati
- VM Oracle situate su un datastore NFS FSx ONTAP

Distribuzione della soluzione

In questa soluzione forniamo istruzioni dettagliate per distribuire e convalidare una soluzione che utilizza il software Veeam Backup and Replication 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 in questa soluzione risiedono su un datastore NFS supplementare ospitato da FSx ONTAP. Inoltre, viene utilizzato un file system FSx ONTAP separato per ospitare i volumi iSCSI che verranno utilizzati per i repository di backup Veeam.

Esamineremo la creazione del file system FSx ONTAP , il montaggio dei volumi iSCSI da utilizzare come repository di backup, la creazione e l'esecuzione di processi di backup e l'esecuzione di ripristini di VM e database.

Per informazioni dettagliate su FSx ONTAP fare riferimento a "Guida utente FSx ONTAP" .

Per informazioni dettagliate su Veeam Backup and Replication fare riferimento a "Documentazione tecnica del Centro assistenza Veeam" sito.

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

Distribuisci 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 del backup o della replica. Il server proxy aiuta a ottimizzare e accelerare il trasferimento dei dati durante i processi di backup elaborando i dati localmente e può utilizzare diverse modalità di trasporto per accedere ai dati tramite le API VMware vStorage per la protezione dei dati o tramite l'accesso diretto all'archiviazione.

Quando si sceglie un design per 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 per i relativi requisiti di sistema, fare riferimento a "Guida alle best practice di Veeam VMware vSphere" .

Veeam Data Mover è un componente di Veeam Proxy Server e utilizza una modalità di trasporto come metodo per ottenere i dati della VM 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 dai datastore NFS utilizzando l'accesso diretto all'archiviazione.

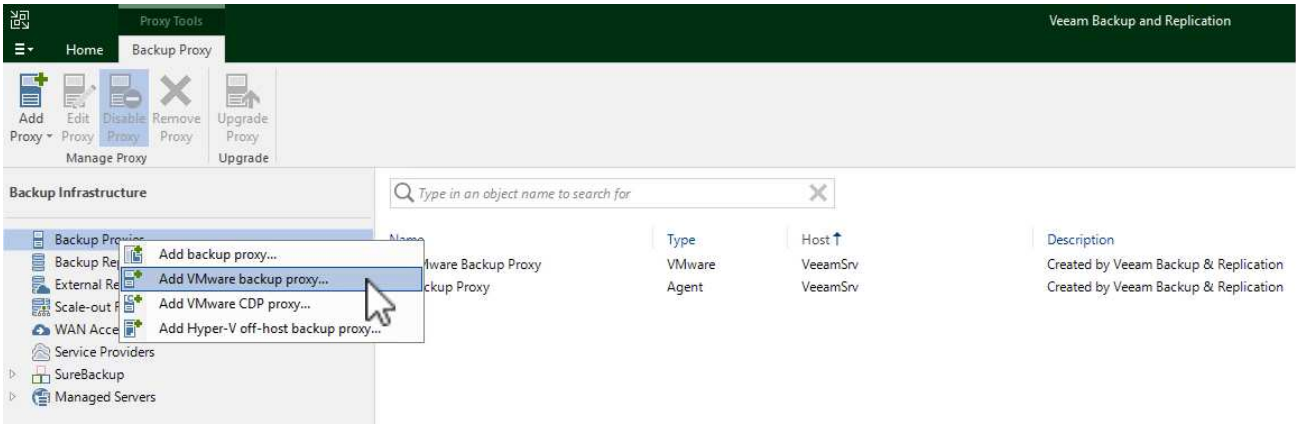
Per maggiori informazioni sulle modalità di trasporto fare riferimento a "Guida utente di Veeam Backup and Replication per VMware vSphere" .

Nel passaggio seguente illustreremo la distribuzione del Veeam Proxy Server su una VM Windows nel VMware Cloud SDDC.

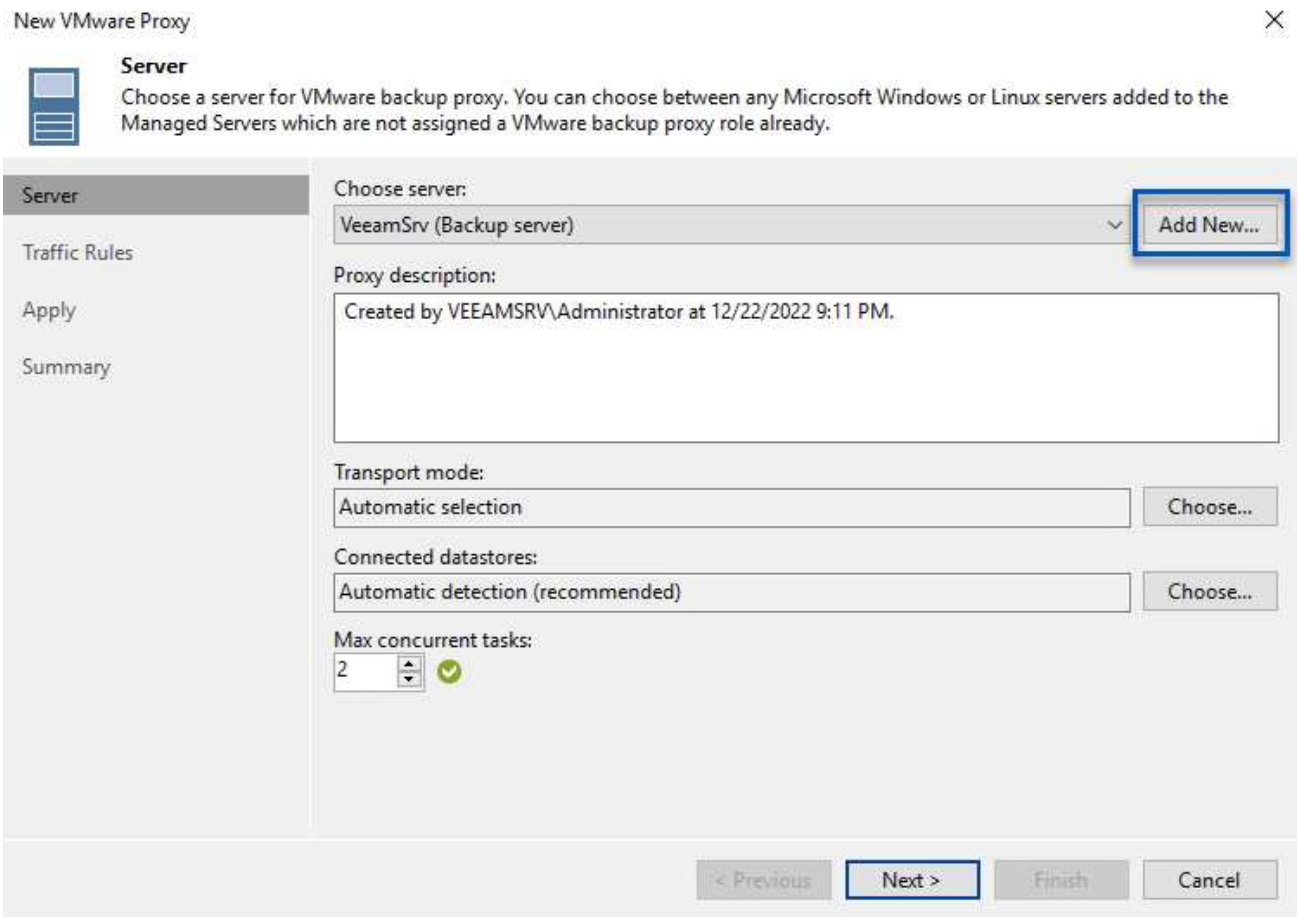
▼ **Distribuisci Veeam Proxy per distribuire i carichi di lavoro di backup**

In questa fase, Veeam Proxy viene distribuito su una VM Windows esistente. Ciò consente di distribuire i processi di backup tra il Veeam Backup Server primario e il Veeam Proxy.

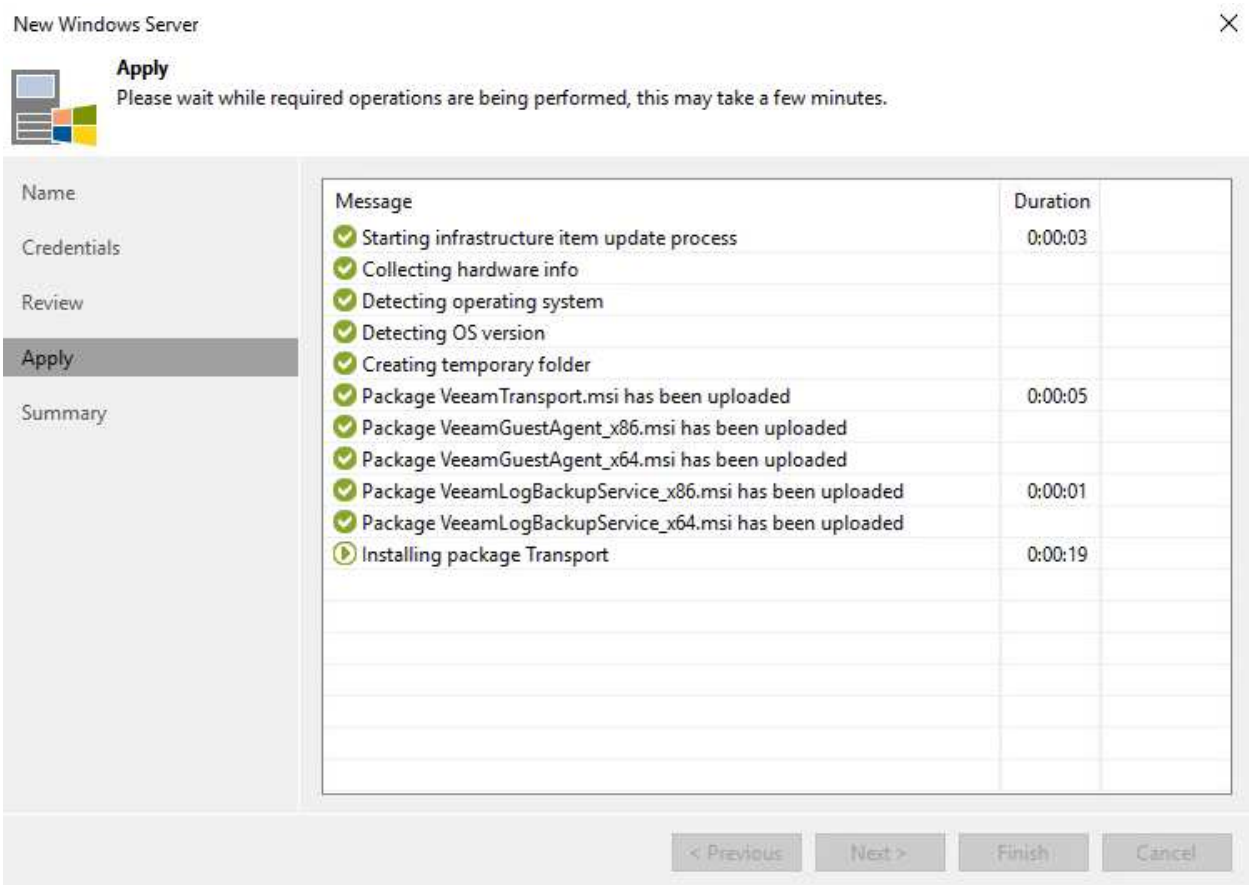
1. Sul server Veeam Backup and Replication, aprire la console di amministrazione e selezionare **Infrastruttura di backup** nel menu in basso a sinistra.
2. Fare clic con il pulsante destro del mouse su **Proxy di backup** e fare clic su **Aggiungi proxy di backup VMware…** per aprire la procedura guidata.



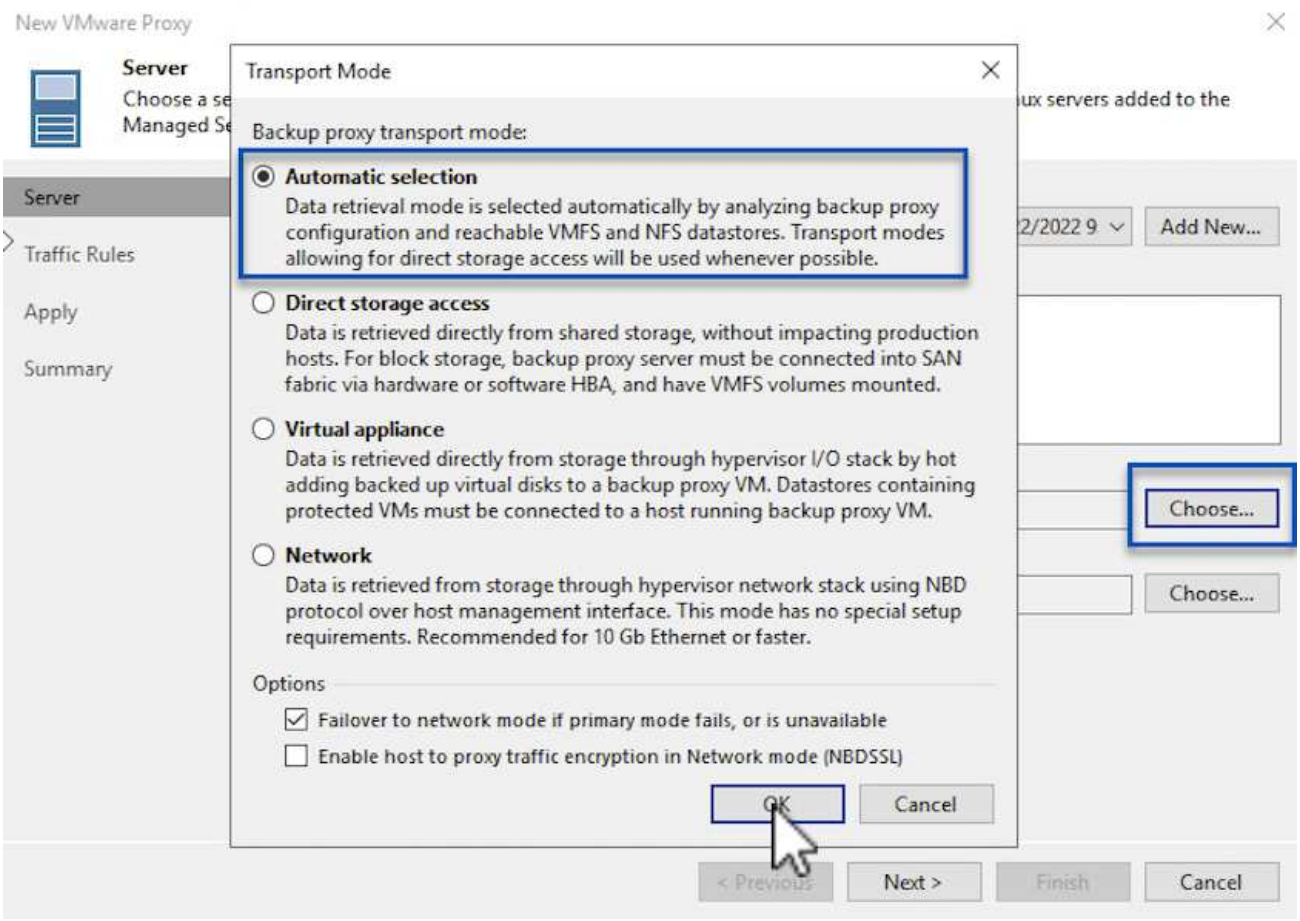
3. Nella procedura guidata **Aggiungi proxy VMware** fare clic sul pulsante **Aggiungi nuovo…** per aggiungere un nuovo server proxy.



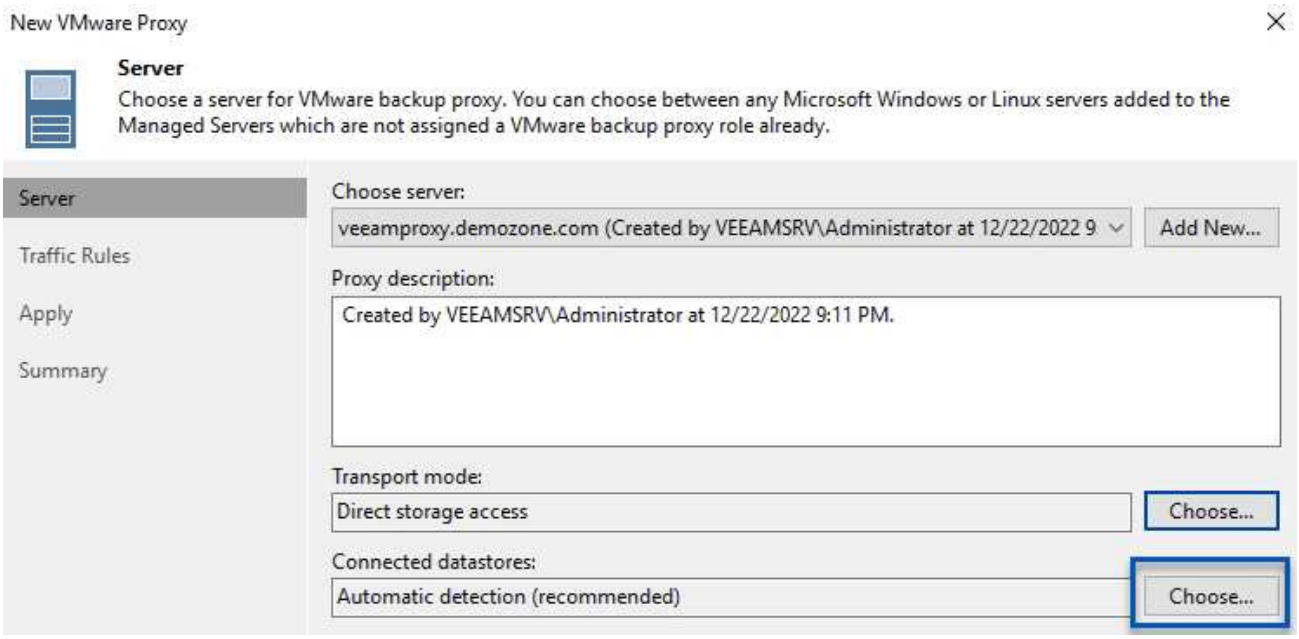
4. Selezionare per aggiungere Microsoft Windows e seguire le istruzioni per aggiungere il server:
   - Compila il nome DNS o l'indirizzo IP
   - Seleziona un account da utilizzare per le credenziali sul nuovo sistema o aggiungi nuove credenziali
   - Rivedi i componenti da installare e poi clicca su **Applica** per iniziare la distribuzione

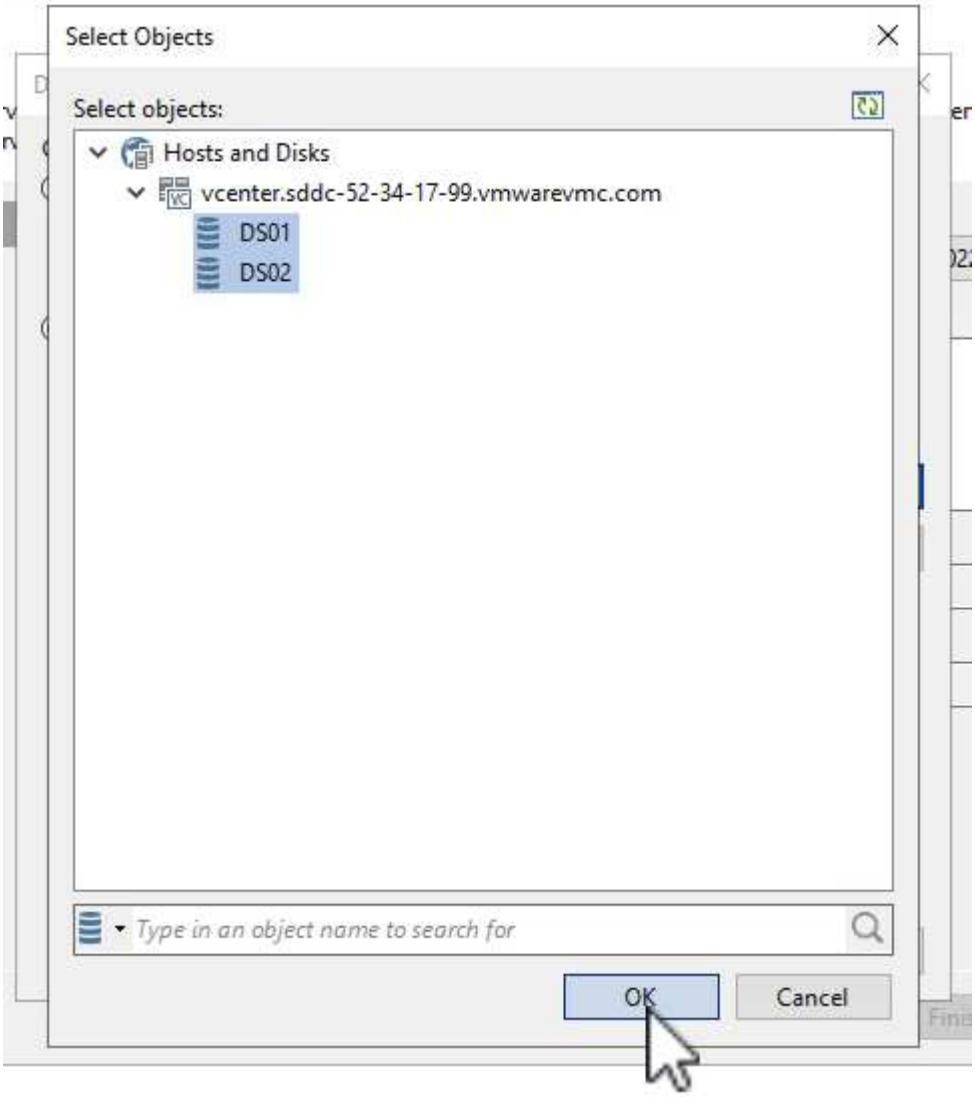


5. Tornando alla procedura guidata **Nuovo proxy VMware**, seleziona una modalità di trasporto. Nel nostro caso abbiamo scelto **Selezione automatica**.

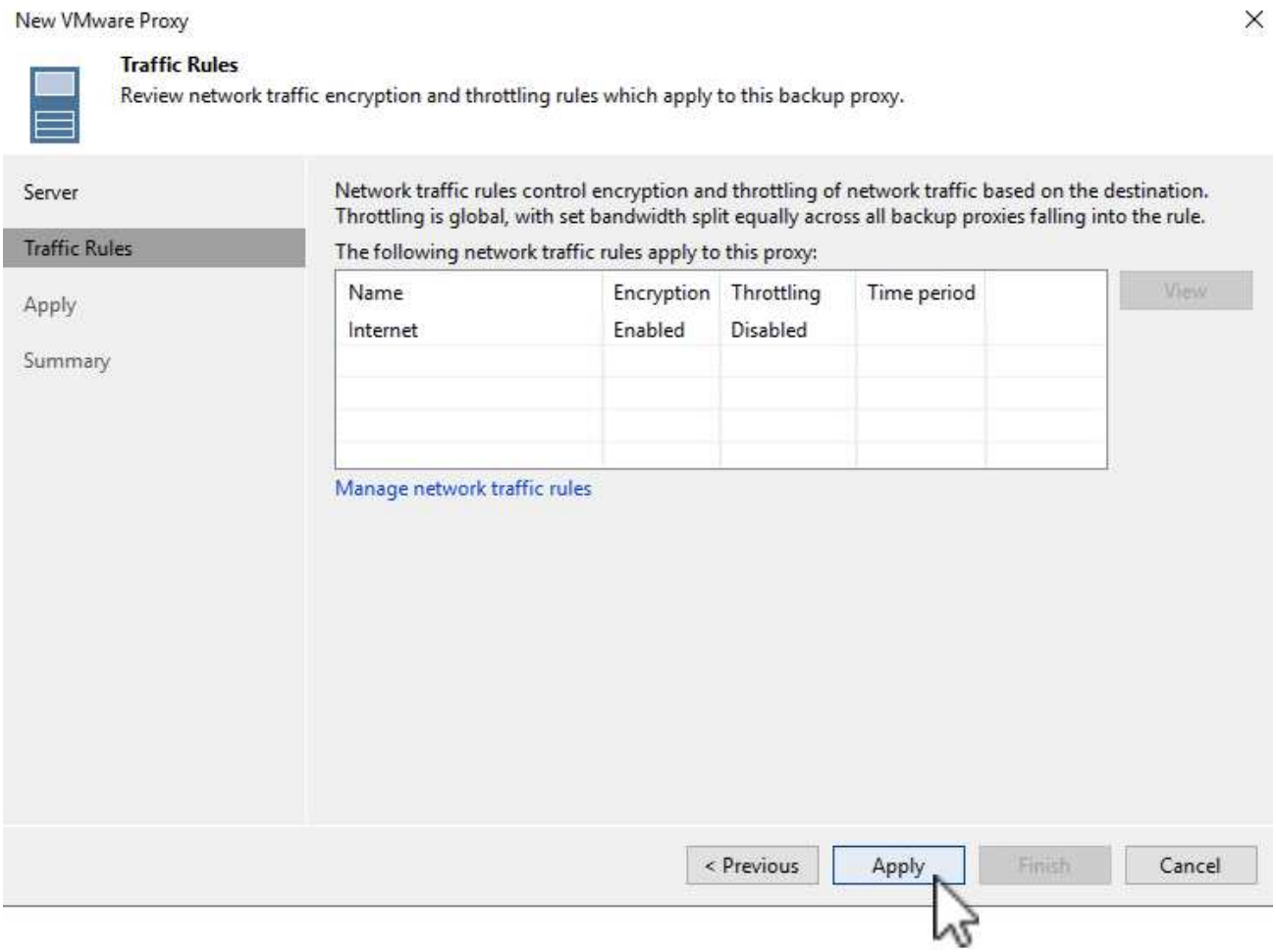


6. Selezionare i datastore connessi a cui si desidera che il proxy VMware abbia accesso diretto.





7. Configurare e applicare tutte le regole specifiche desiderate per il traffico di rete, come la crittografia o la limitazione. Al termine, fare clic sul pulsante **Applica** per completare la distribuzione.



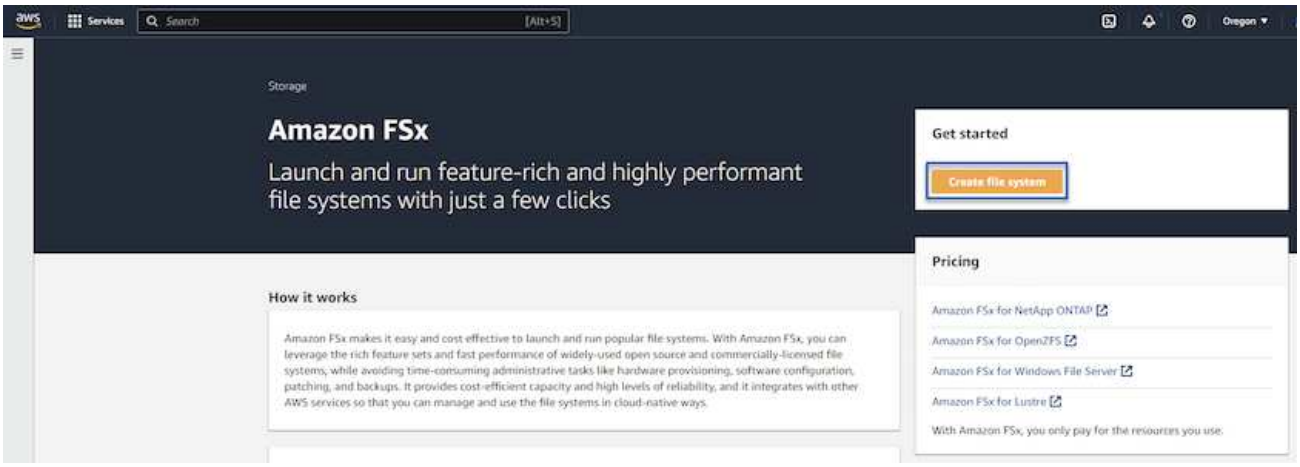
Configurare l'archiviazione e i repository di backup

Il server Veeam Backup primario e il server Veeam Proxy hanno accesso a un repository di backup sotto forma di storage connesso direttamente. In questa sezione illustreremo come creare un file system FSx ONTAP , montare iSCSI LUN sui server Veeam e creare repository di backup.

▼ **Crea il file system FSx ONTAP**

Creare un file system FSx ONTAP che verrà utilizzato per ospitare i volumi iSCSI per i Veeam Backup Repository.

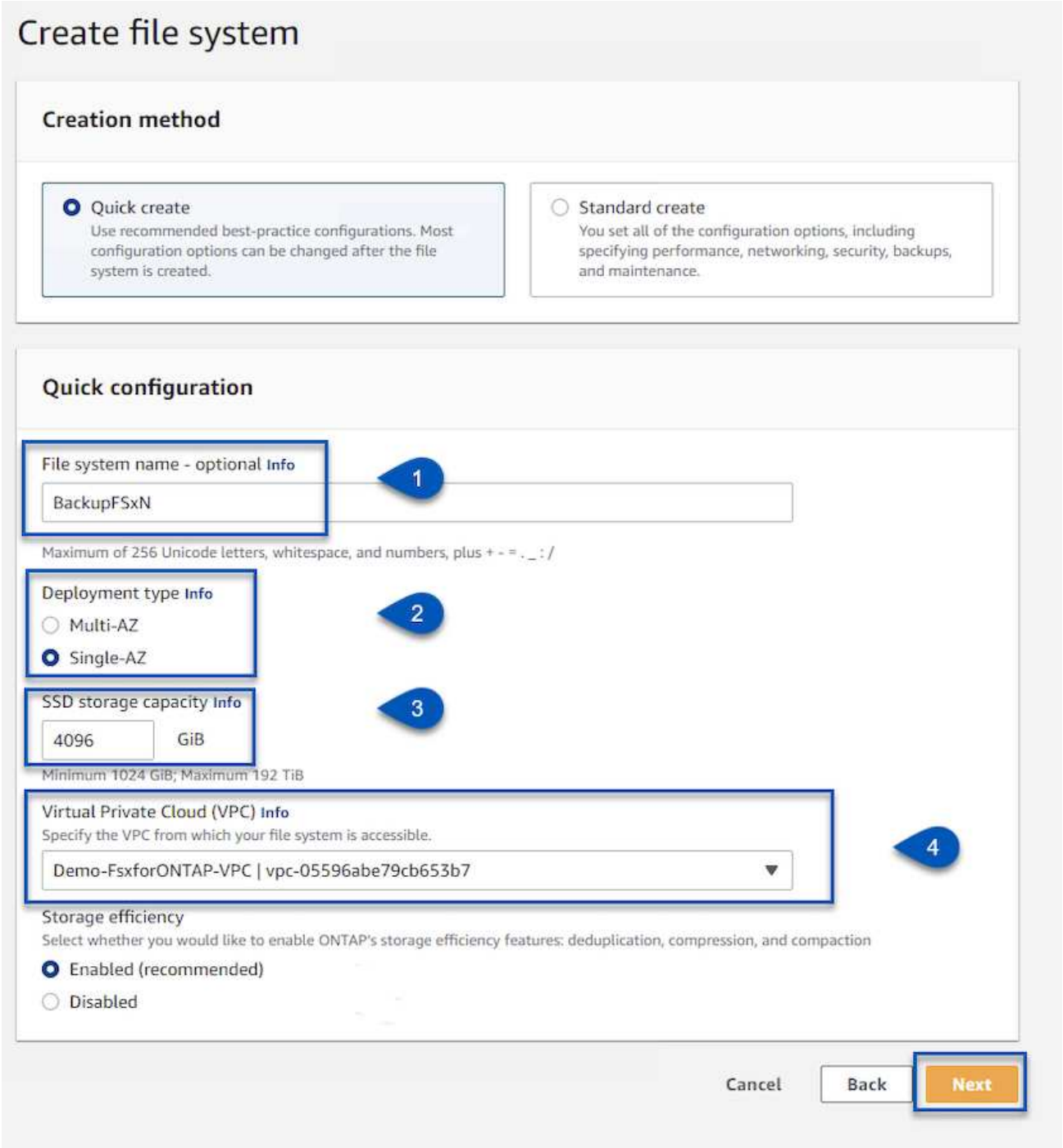
1. Nella console AWS, vai su FSx e poi **Crea file system**



2. Selezionare * Amazon FSx ONTAP* e poi **Avanti** per continuare.



3. Inserire il nome del file system, il tipo di distribuzione, la capacità di archiviazione SSD e la VPC in cui risiederà il cluster FSx ONTAP . Deve trattarsi di una VPC configurata per comunicare con la rete della macchina virtuale in VMware Cloud. Fare clic su **Avanti**.



4. Rivedere i passaggi di distribuzione e fare clic su **Crea file system** per avviare il processo di creazione del file system.

▼ Configurare e montare i LUN iSCSI

Crea e configura i LUN iSCSI su FSx ONTAP e montali sui server di backup e proxy Veeam. Questi LUN verranno successivamente utilizzati per creare repository di backup Veeam.

ⓘ La creazione di un LUN iSCSI su FSx ONTAP è un processo che prevede più fasi. Il primo passaggio per la creazione dei volumi può essere eseguito nella console Amazon FSx o con NetApp ONTAP CLI.

Per ulteriori informazioni sull'utilizzo di FSx ONTAP, vedere "Guida utente FSx ONTAP" .

1. Dalla CLI 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. Concedi l'accesso alle LUN creando un gruppo di iniziatori contenente l'IQN iSCSI dei server di backup e proxy Veeam:

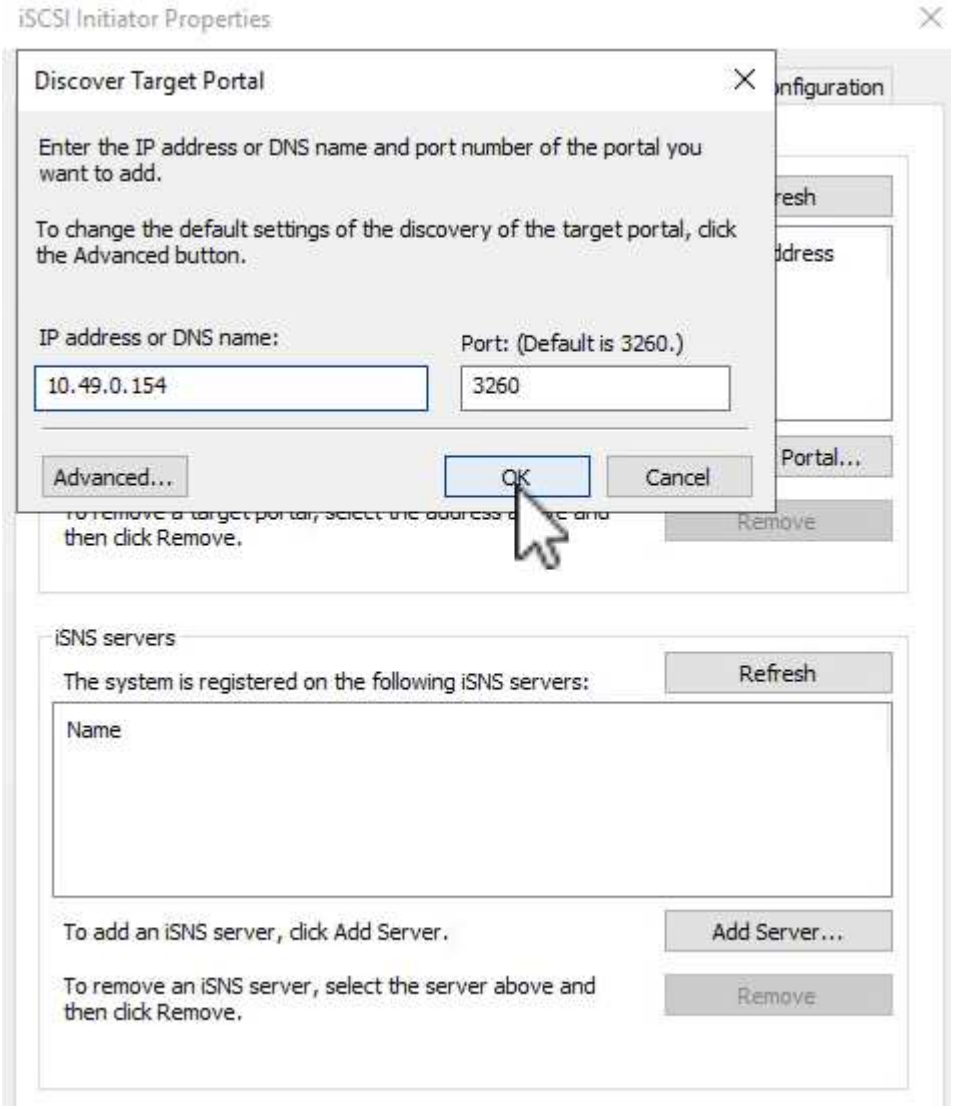
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

Per completare il passaggio precedente, è necessario innanzitutto recuperare l'IQN dalle proprietà dell'iniziatore iSCSI sui server Windows.

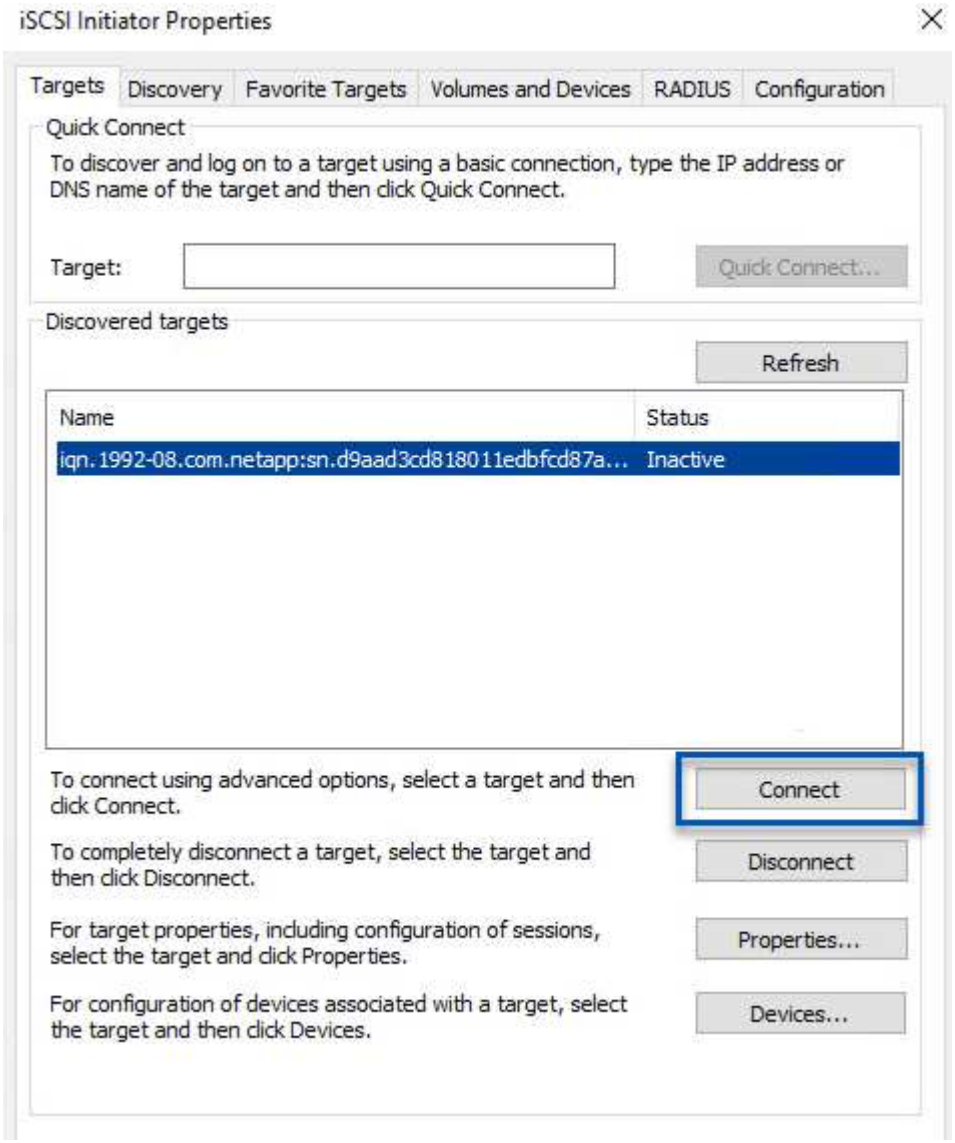
4. Infine, mappa i LUN al gruppo di iniziatori appena creato:

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

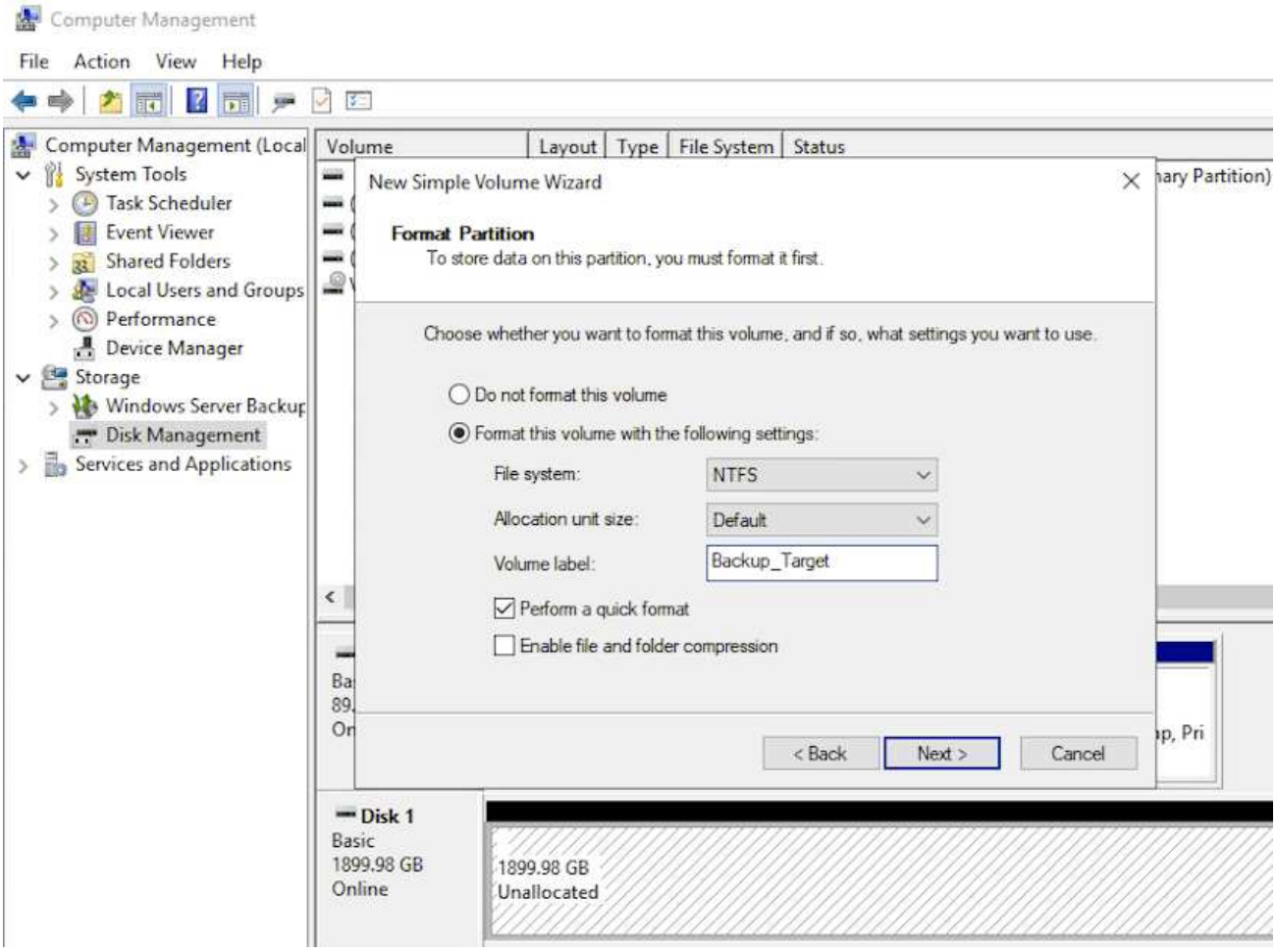
5. Per montare le LUN iSCSI, accedere al Veeam Backup & Replication Server e aprire le Proprietà dell'iniziatore iSCSI. Vai alla scheda **Scopri** e inserisci l'indirizzo IP di destinazione iSCSI.



6. Nella scheda **Destinazioni**, evidenziare la LUN inattiva e fare clic su **Connetti**. Selezionare la casella **Abilita multi-path** e fare clic su **OK** per connettersi al LUN.



7. Nell'utilità Gestione disco inizializzare il nuovo LUN e creare un volume con il nome e la lettera di unità desiderati. Selezionare la casella **Abilita multi-path** e fare clic su **OK** per connettersi al LUN.

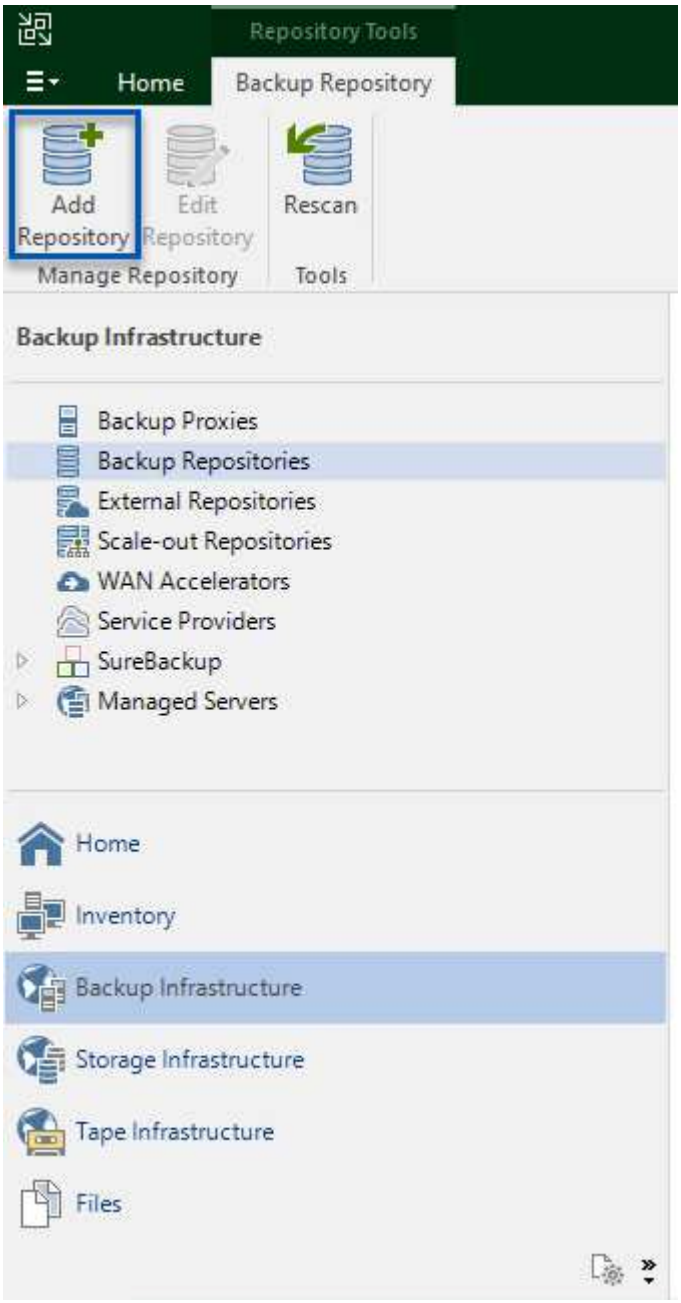


8. Ripetere questi passaggi per montare i volumi iSCSI sul server Veeam Proxy.

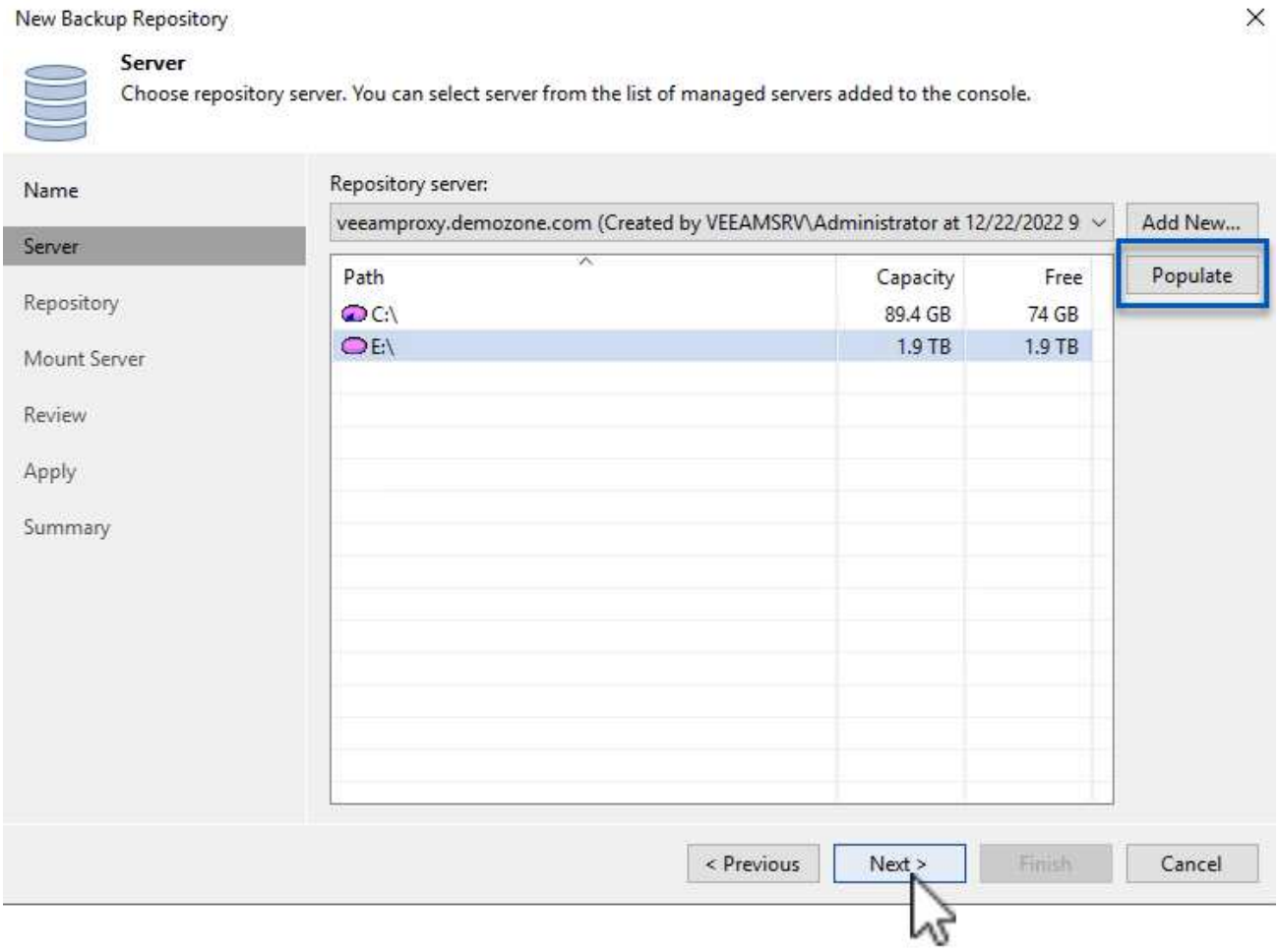
▼ **Crea repository di backup Veeam**

Nella console Veeam Backup and Replication, 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.

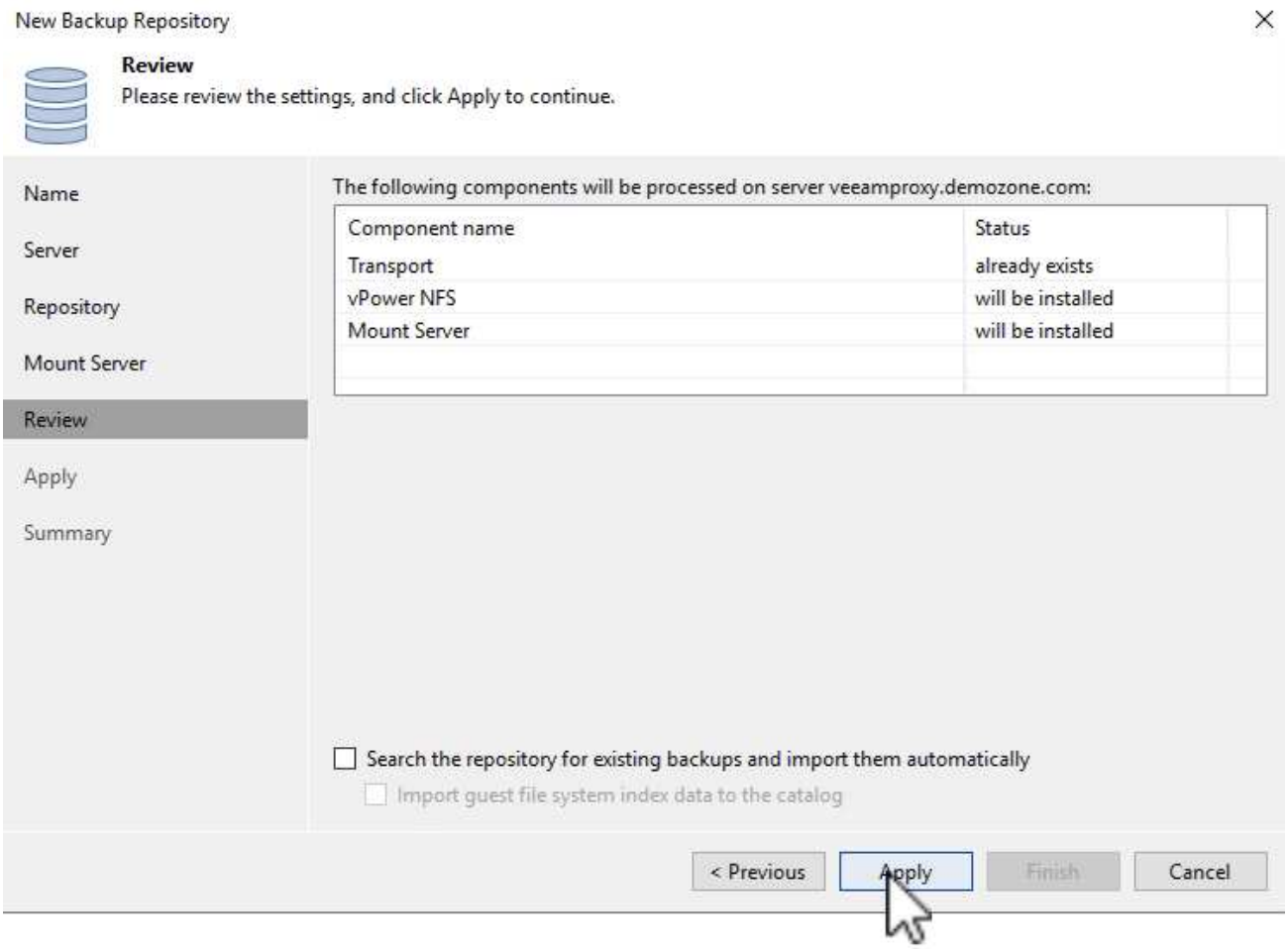
1. Nella console di Veeam Backup and Replication fare clic su **Backup Infrastructure** in basso a sinistra e quindi selezionare **Aggiungi repository**



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 che verrà utilizzato.



3. Nella pagina successiva, seleziona un server di montaggio che verrà utilizzato per montare i backup durante l'esecuzione di ripristini avanzati. Per impostazione predefinita, si tratta dello stesso server a cui è connesso l'archivio del repository.
4. Rivedi le tue selezioni e clicca su **Applica** per avviare la creazione del repository di backup.



5. Ripetere questi passaggi per tutti gli altri server proxy.

Configurare i processi di backup Veeam

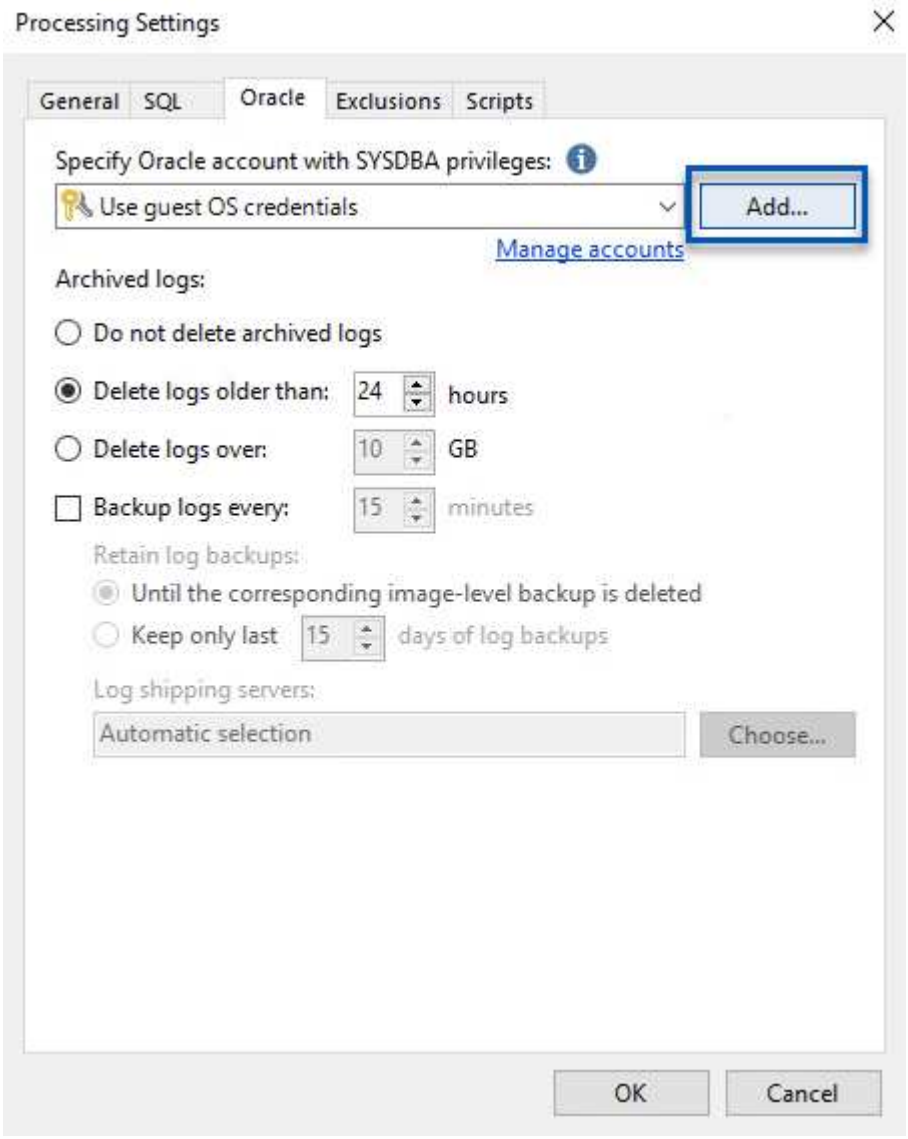
I processi di backup devono essere creati utilizzando i repository di backup descritti nella sezione precedente. La creazione di processi di backup è una parte normale del repertorio di qualsiasi amministratore di storage e in questa sede non verranno trattati tutti i passaggi. Per informazioni più complete 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:

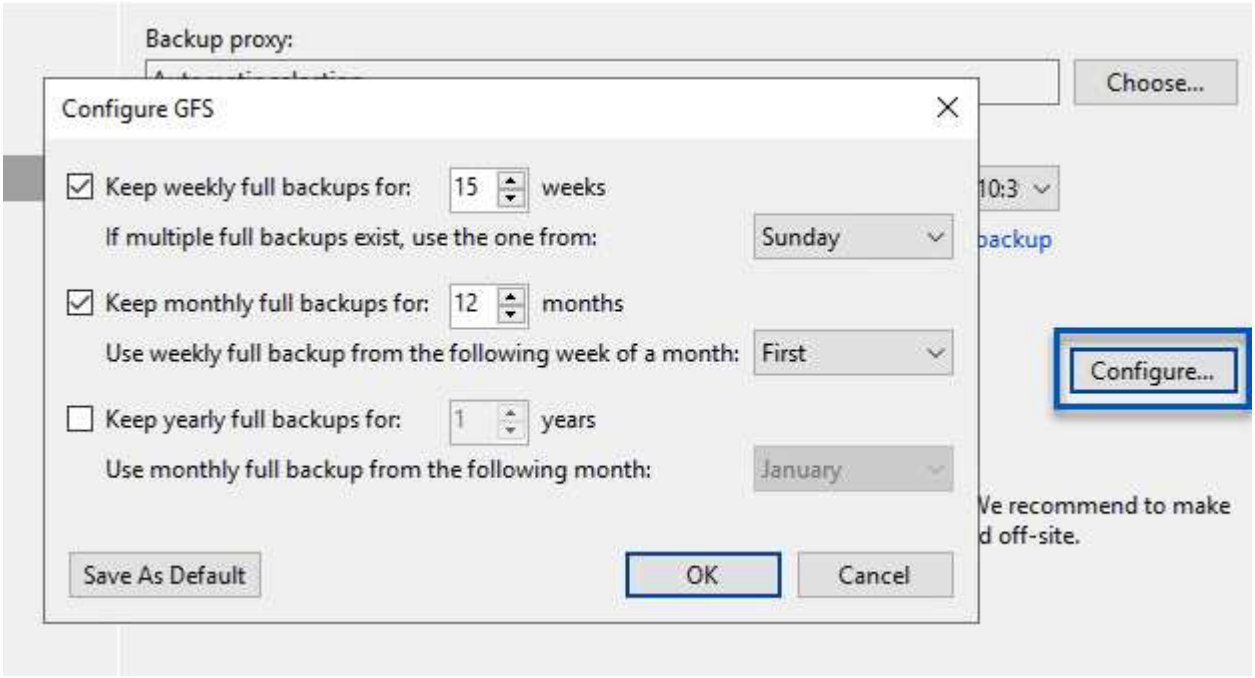
- Server Microsoft Windows SQL
- Server di database Oracle
- Server di file Windows
- Server di file Linux

▼ Considerazioni generali sulla configurazione dei processi di backup Veeam

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



3. Per gestire i criteri di conservazione per il backup, selezionare **Conserva determinati backup completi più a lungo per scopi di archiviazione** e fare clic sul pulsante **Configura…** per configurare i criteri.



Ripristina le VM delle applicazioni con il ripristino completo di Veeam

Eseguire un ripristino completo con Veeam è il primo passo per eseguire il ripristino di un'applicazione. Abbiamo verificato che i ripristini completi delle nostre VM erano attivi e che tutti i servizi funzionavano normalmente.

Il ripristino dei server è una parte normale del repertorio di qualsiasi amministratore di storage e in questa sede non verranno trattati tutti i passaggi. Per informazioni più complete sull'esecuzione di ripristini completi in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam" .

Ripristinare i database di SQL Server

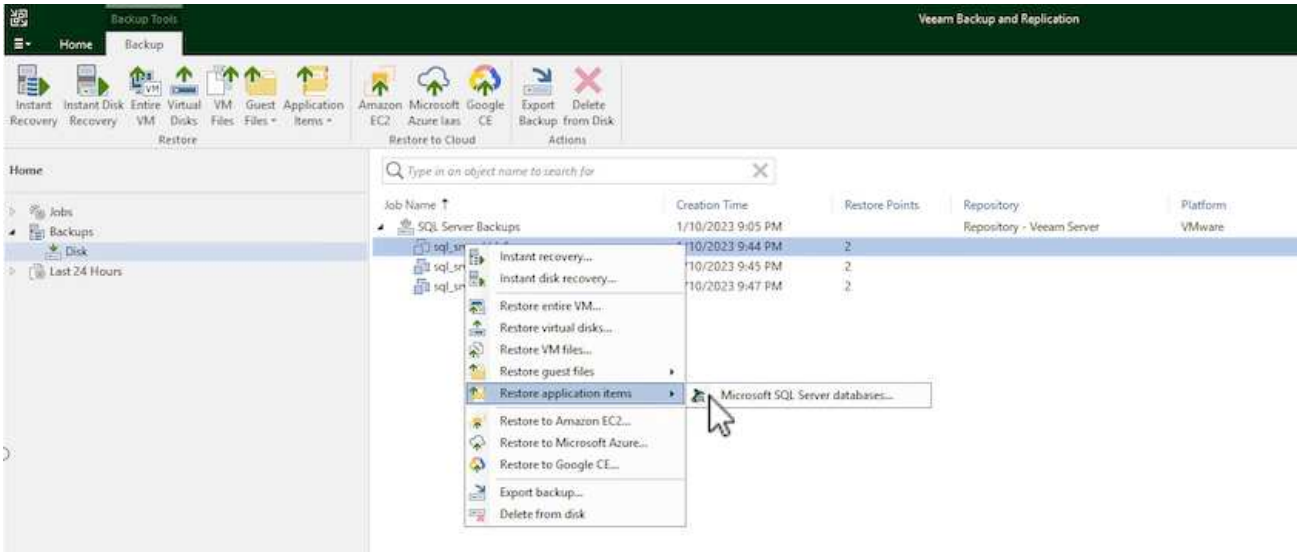
Veeam Backup & Replication offre diverse opzioni per il ripristino dei database SQL Server. Per questa convalida abbiamo utilizzato Veeam Explorer per SQL Server con Instant Recovery per eseguire i ripristini dei nostri database SQL Server. SQL Server Instant Recovery è una funzionalità che consente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

- Veeam 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 degli utenti** a questo database, garantendo che gli utenti possano continuare ad accedere ai dati e a lavorarci.
- 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 degli utenti al database originale** e rimuove il database temporaneo.

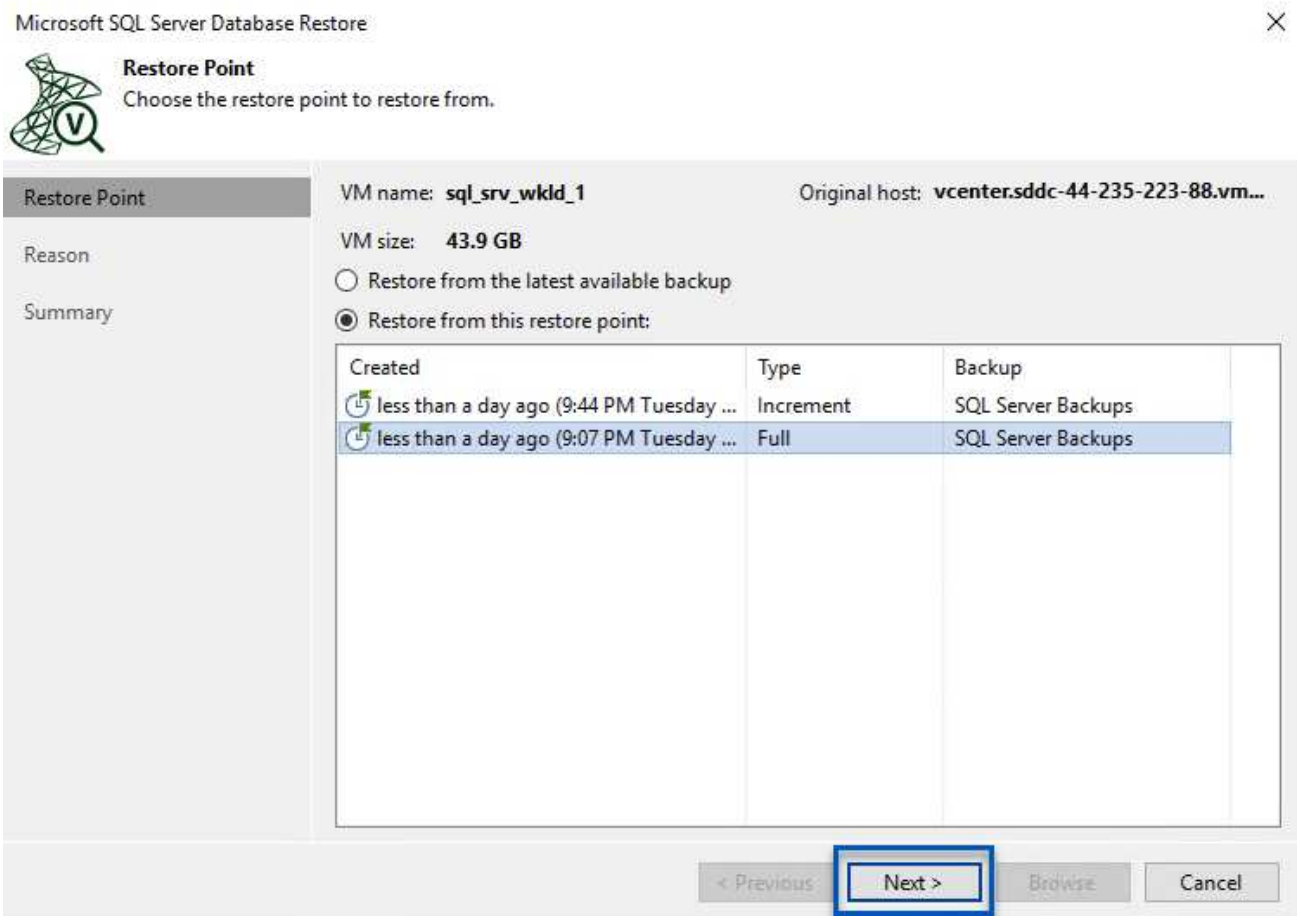
▼ Ripristina il database SQL Server con Veeam Explorer Instant Recovery

1. Nella console di Veeam Backup and Replication, accedere all'elenco dei backup di SQL Server, fare clic con il pulsante destro del mouse su un server e selezionare **Ripristina elementi applicazione**, quindi

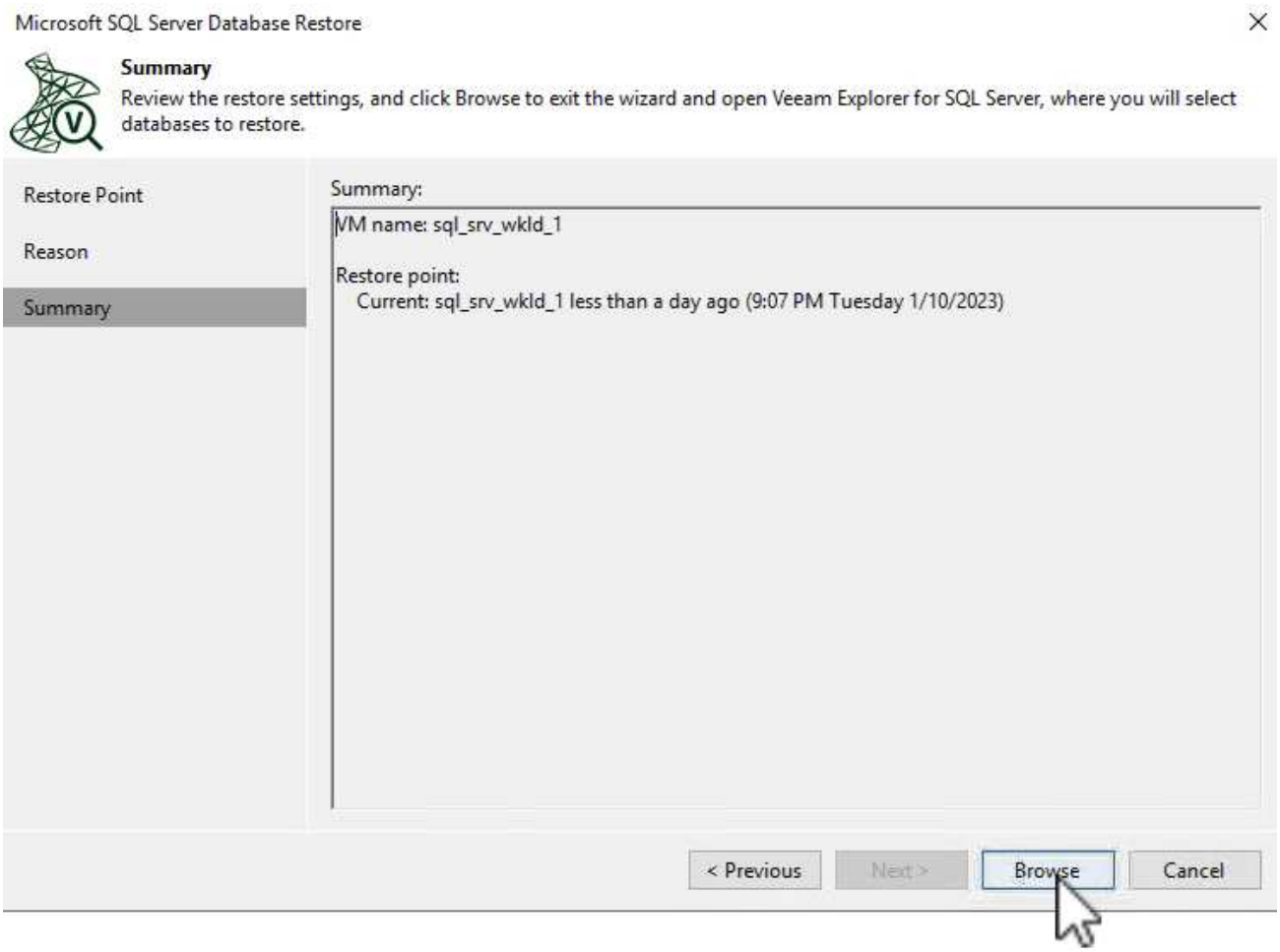
Database di Microsoft SQL Server….



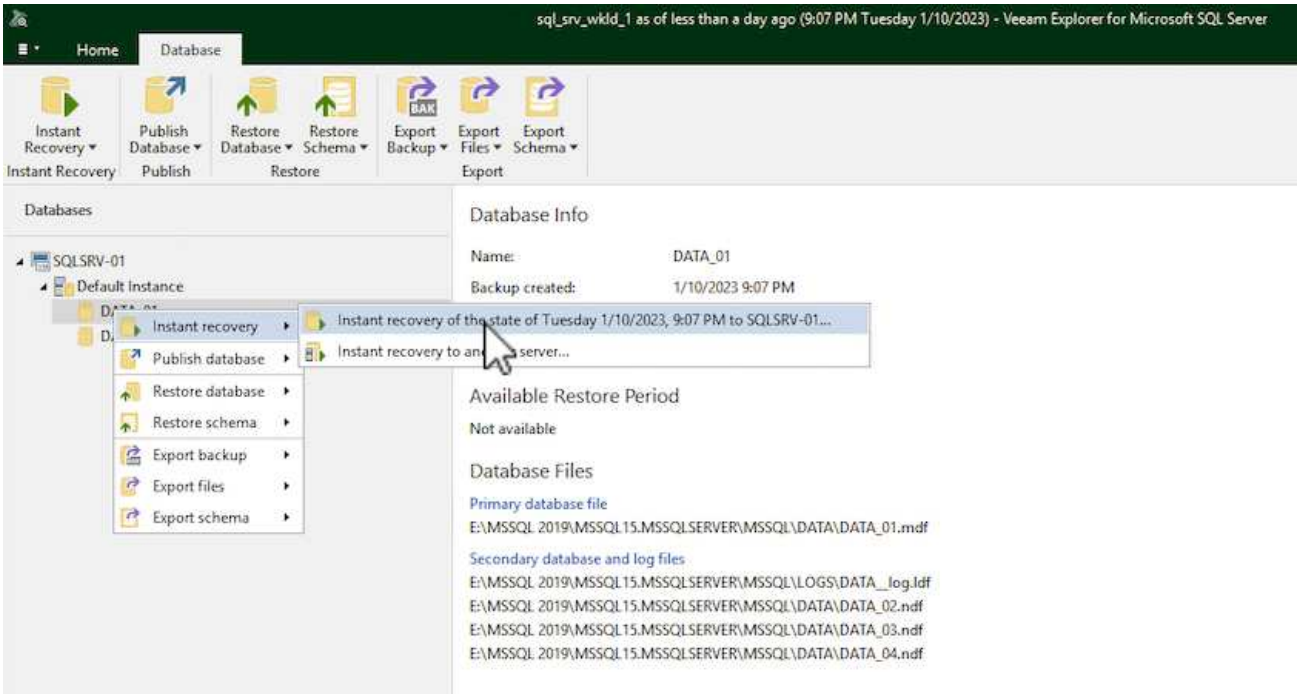
2. Nella procedura guidata di ripristino del database di Microsoft SQL Server, selezionare un punto di ripristino dall'elenco e fare clic su **Avanti**.



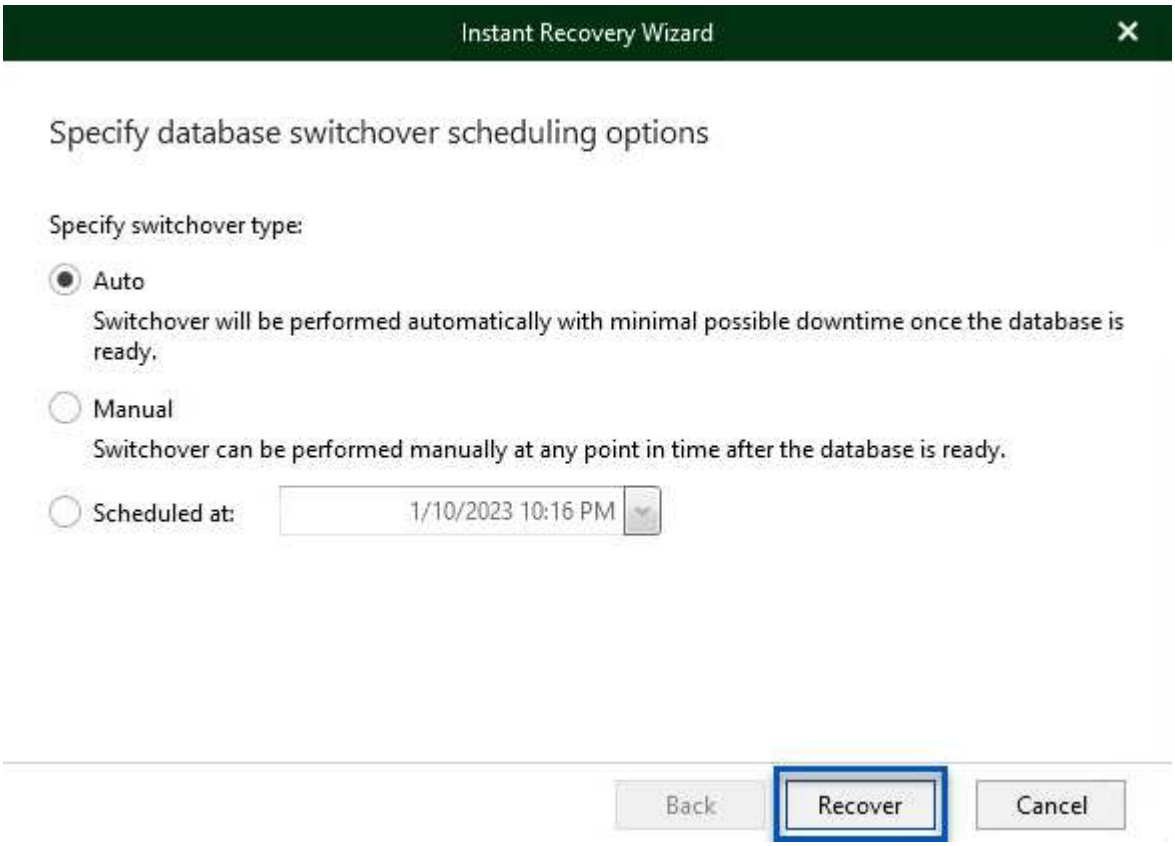
3. Se lo si desidera, immettere un **Motivo di ripristino** e quindi, nella pagina Riepilogo, fare clic sul pulsante **Sfoglia** per avviare Veeam Explorer per Microsoft SQL Server.



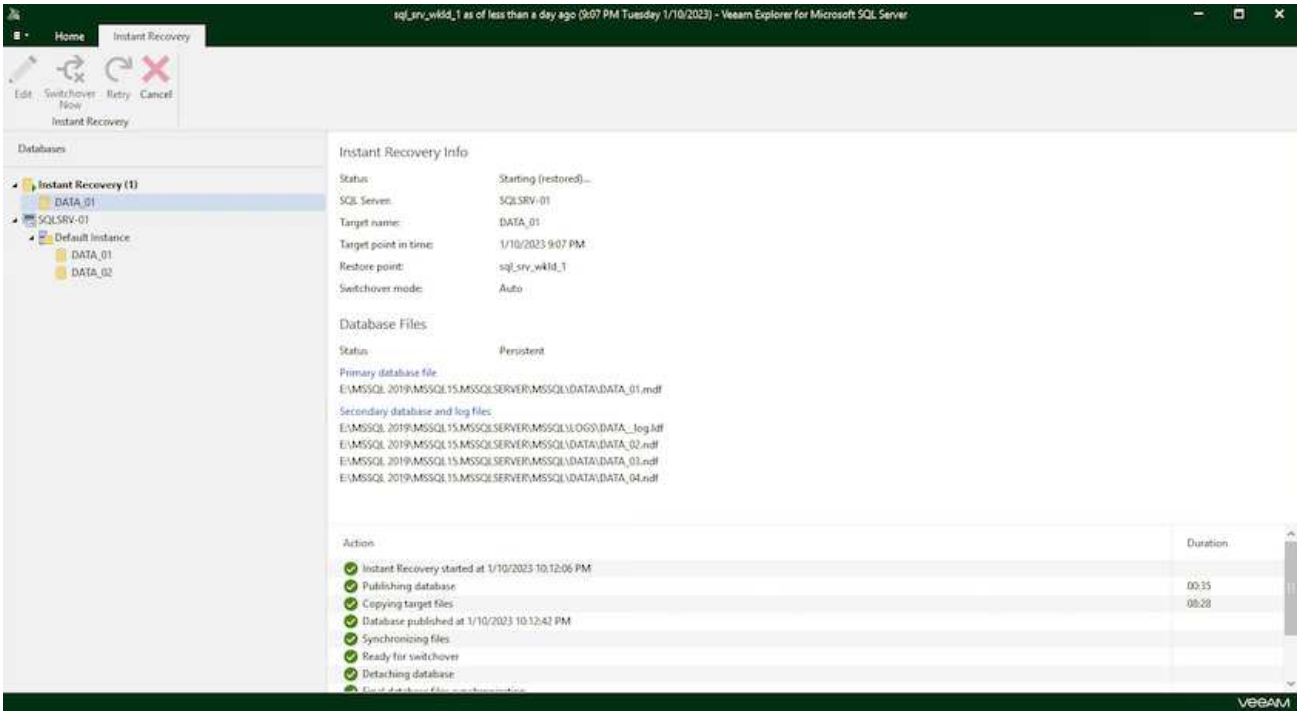
4. In Veeam Explorer espandere l'elenco delle istanze del database, fare clic con il pulsante destro del mouse e selezionare **Ripristino immediato**, quindi il punto di ripristino specifico su cui eseguire il ripristino.



5. Nella procedura guidata di ripristino immediato specificare il tipo di switchover. Ciò può avvenire automaticamente con tempi di inattività minimi, manualmente o in un momento specifico. Quindi fare clic sul pulsante **Recupera** per avviare il processo di ripristino.



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



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

fare riferimento alla sezione Microsoft SQL Server nel "Guida utente di Veeam Explorers" .

Ripristinare i database Oracle con Veeam Explorer

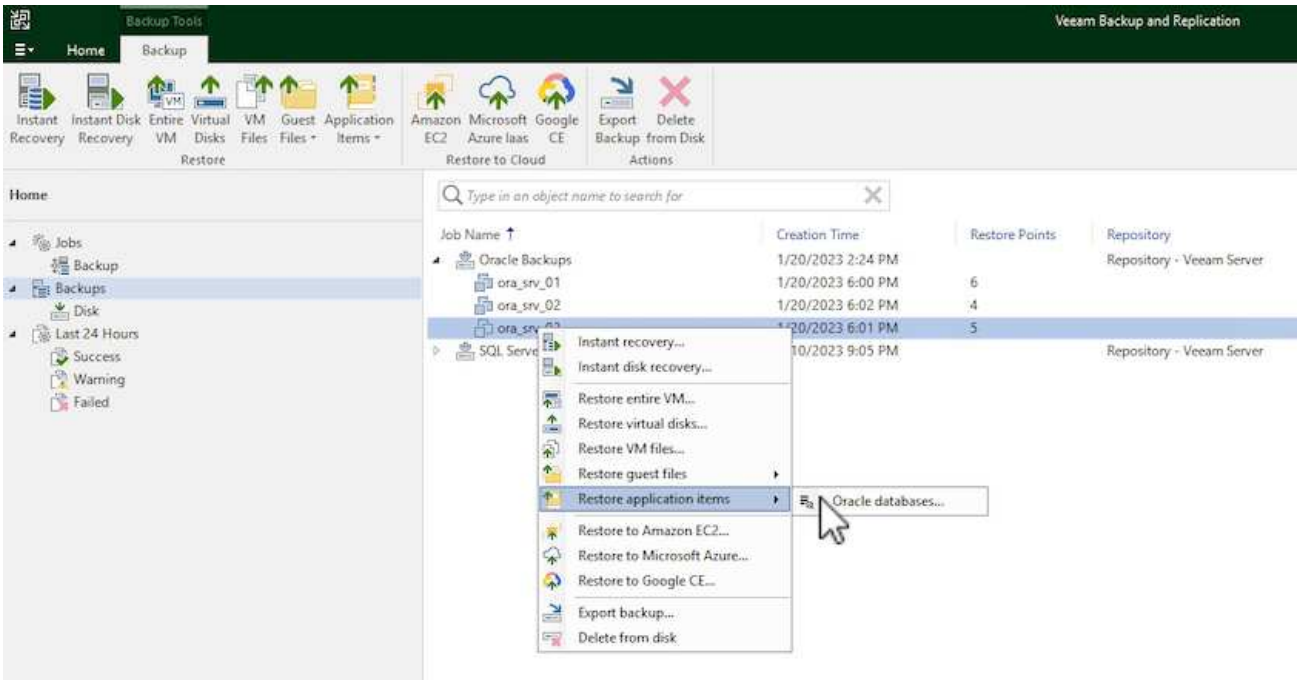
Veeam Explorer per il database Oracle offre la possibilità di eseguire un ripristino standard del database Oracle o un ripristino ininterrotto utilizzando Instant Recovery. Supporta inoltre la pubblicazione di database per un accesso rapido, il ripristino di database Data Guard e il ripristino da backup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

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

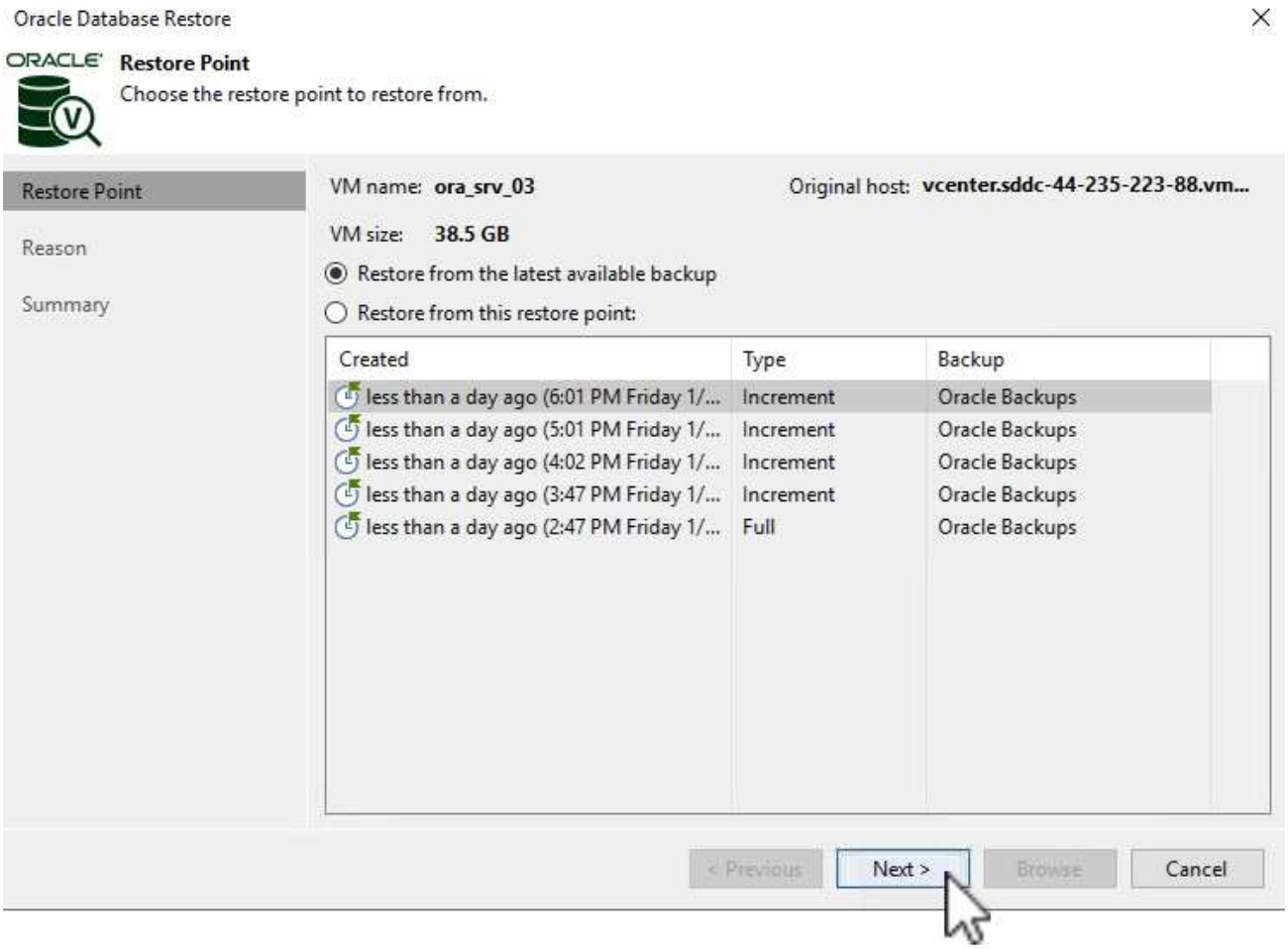
▼ **Ripristina il database Oracle con Veeam Explorer**

In questa sezione viene illustrato il ripristino di un database Oracle su un server diverso utilizzando Veeam Explorer.

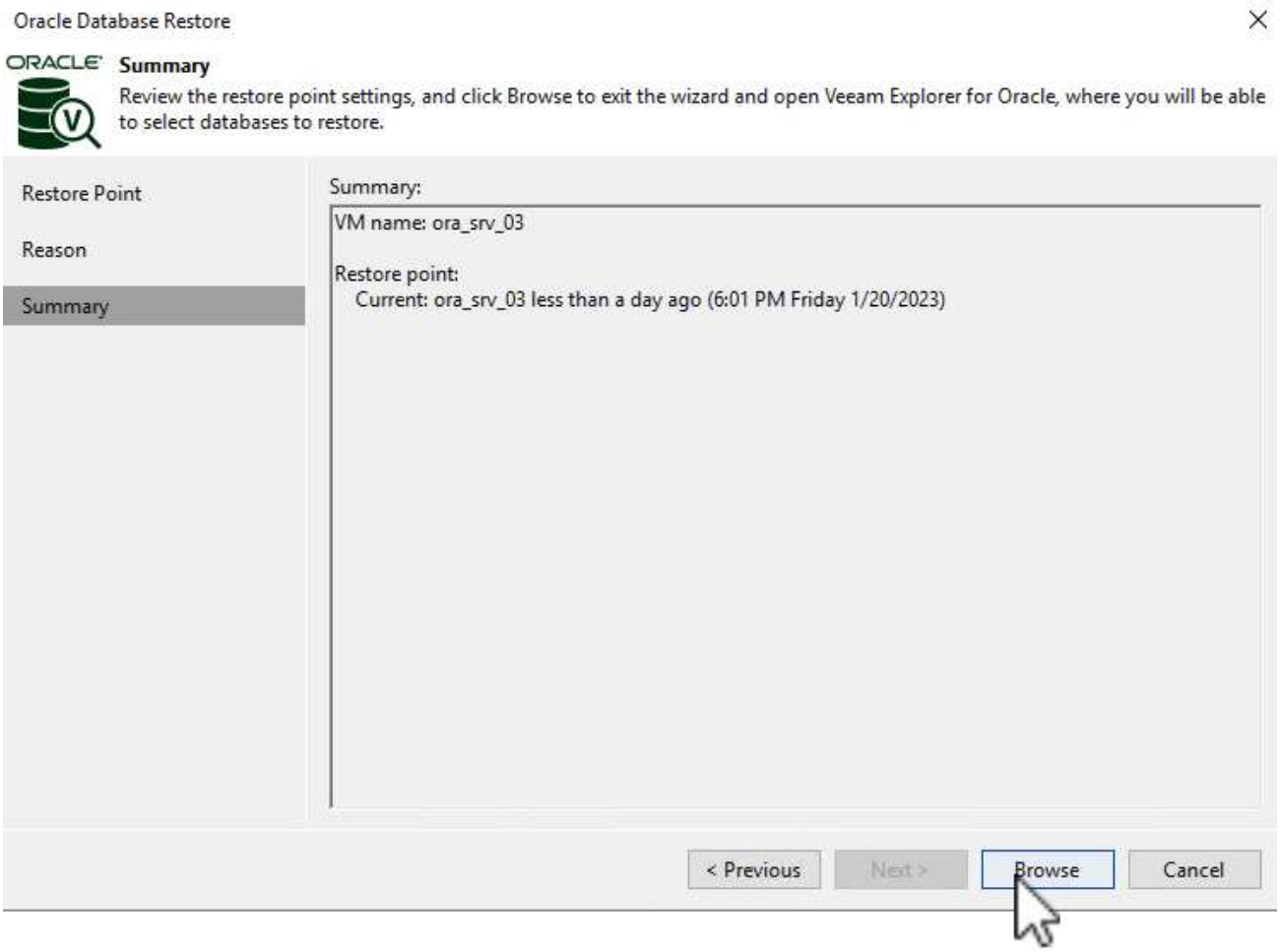
1. Nella console di Veeam Backup and Replication, accedere all'elenco dei backup di Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Ripristina elementi applicazione**, quindi **Database Oracle…**.



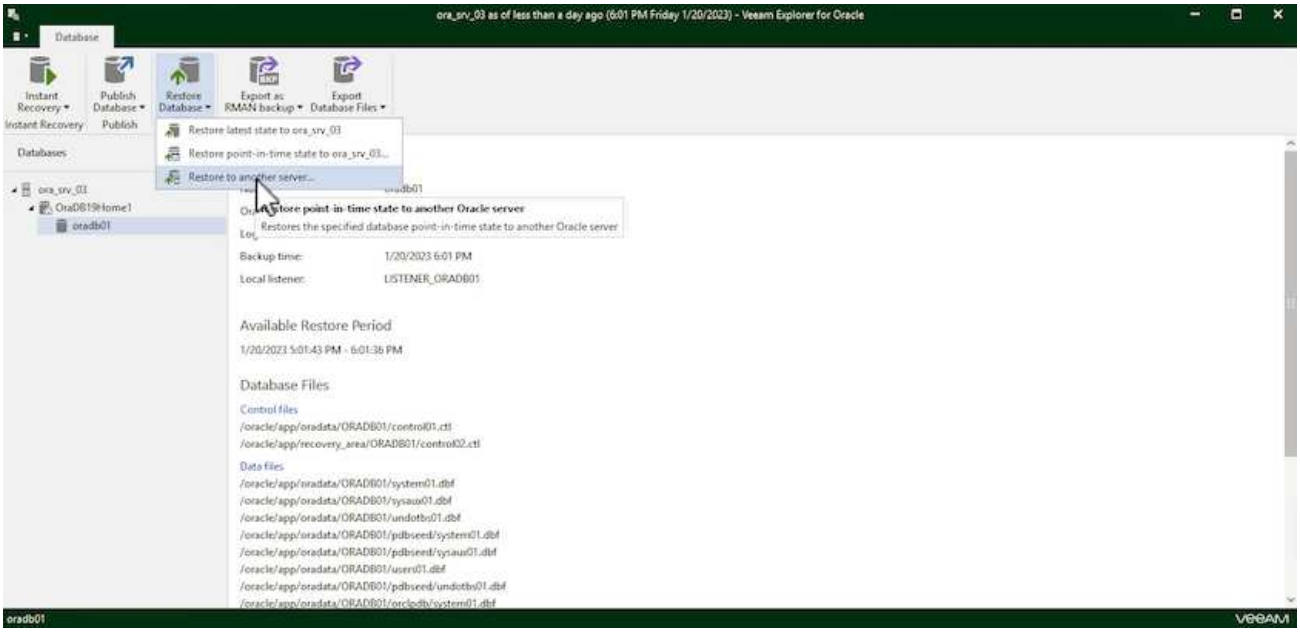
2. Nella procedura guidata di ripristino del database Oracle, selezionare un punto di ripristino dall'elenco e fare clic su **Avanti**.



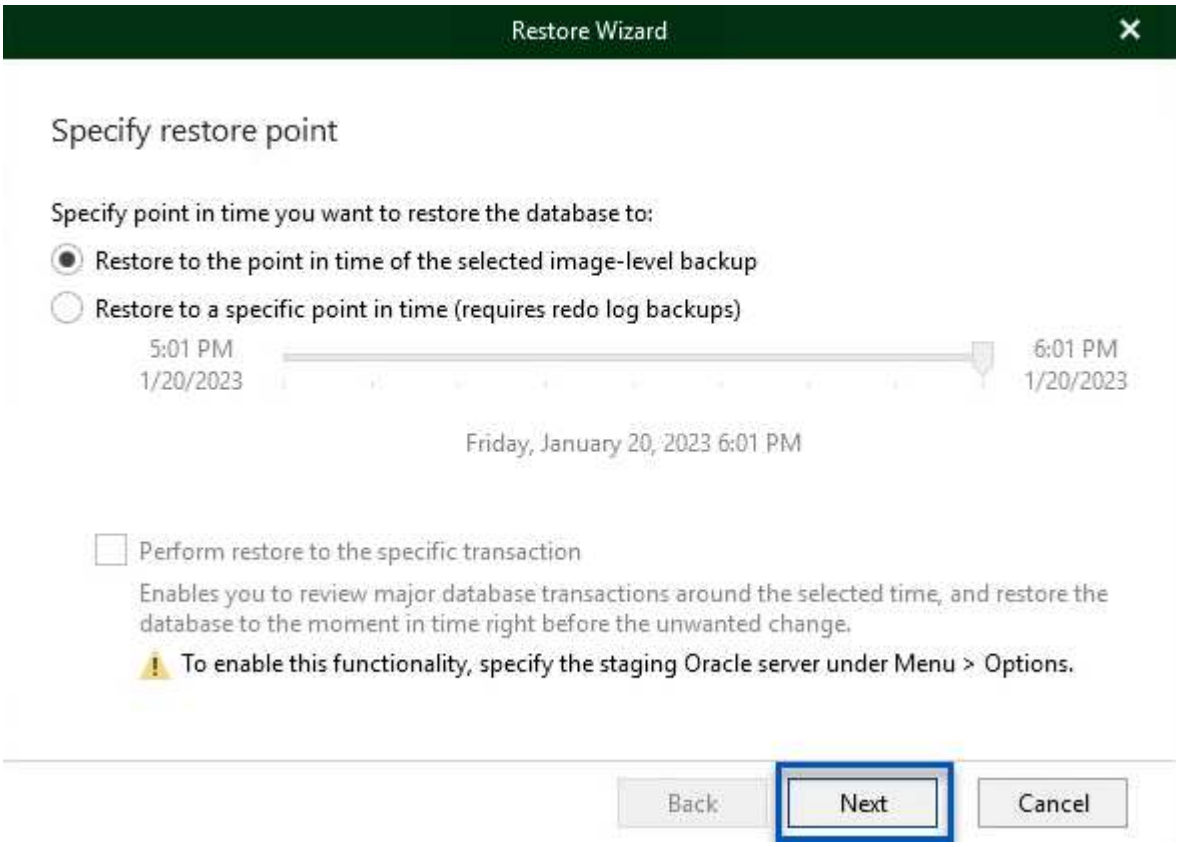
3. Se lo si desidera, immettere un **Motivo di ripristino** e quindi, nella pagina Riepilogo, fare clic sul pulsante **Sfoglia** per avviare Veeam Explorer per Oracle.



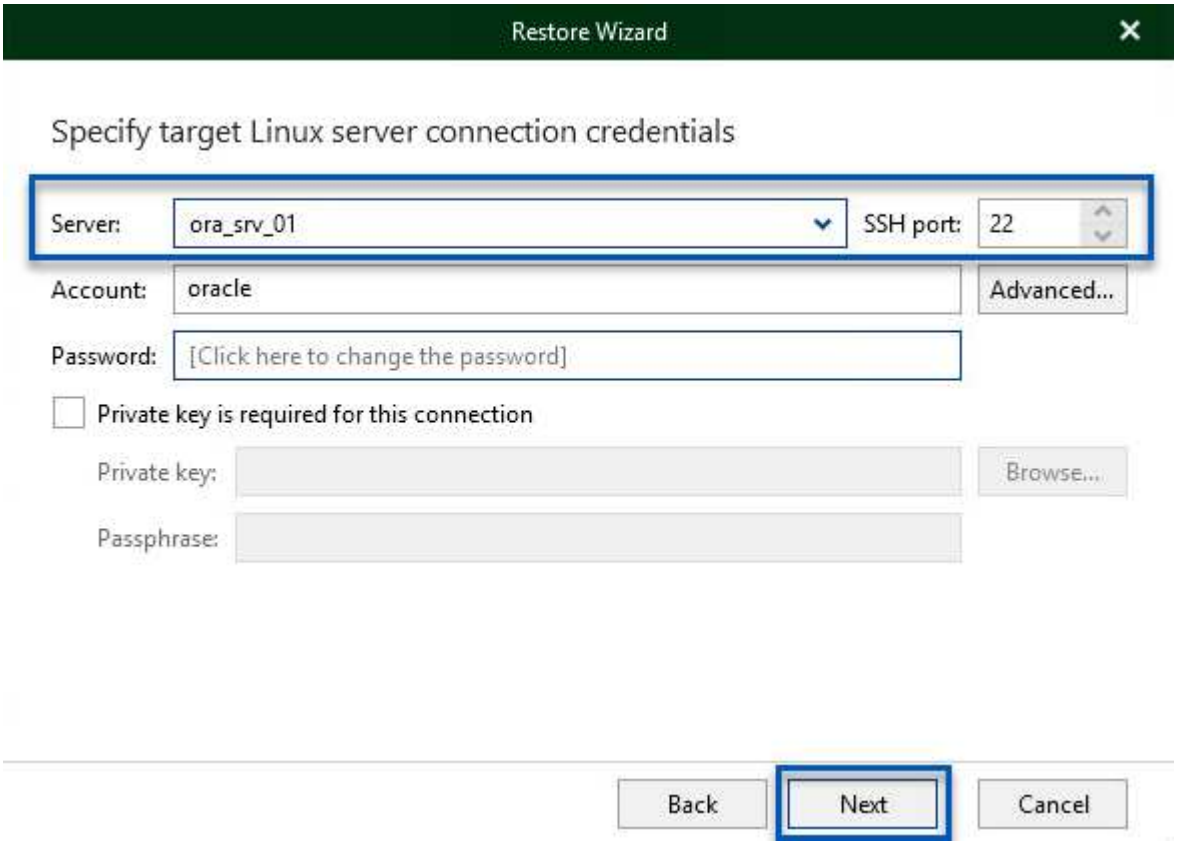
4. In Veeam Explorer espandere l'elenco delle istanze del database, fare clic sul database da ripristinare e quindi dal menu a discesa **Ripristina database** in alto selezionare **Ripristina su un altro server…**.



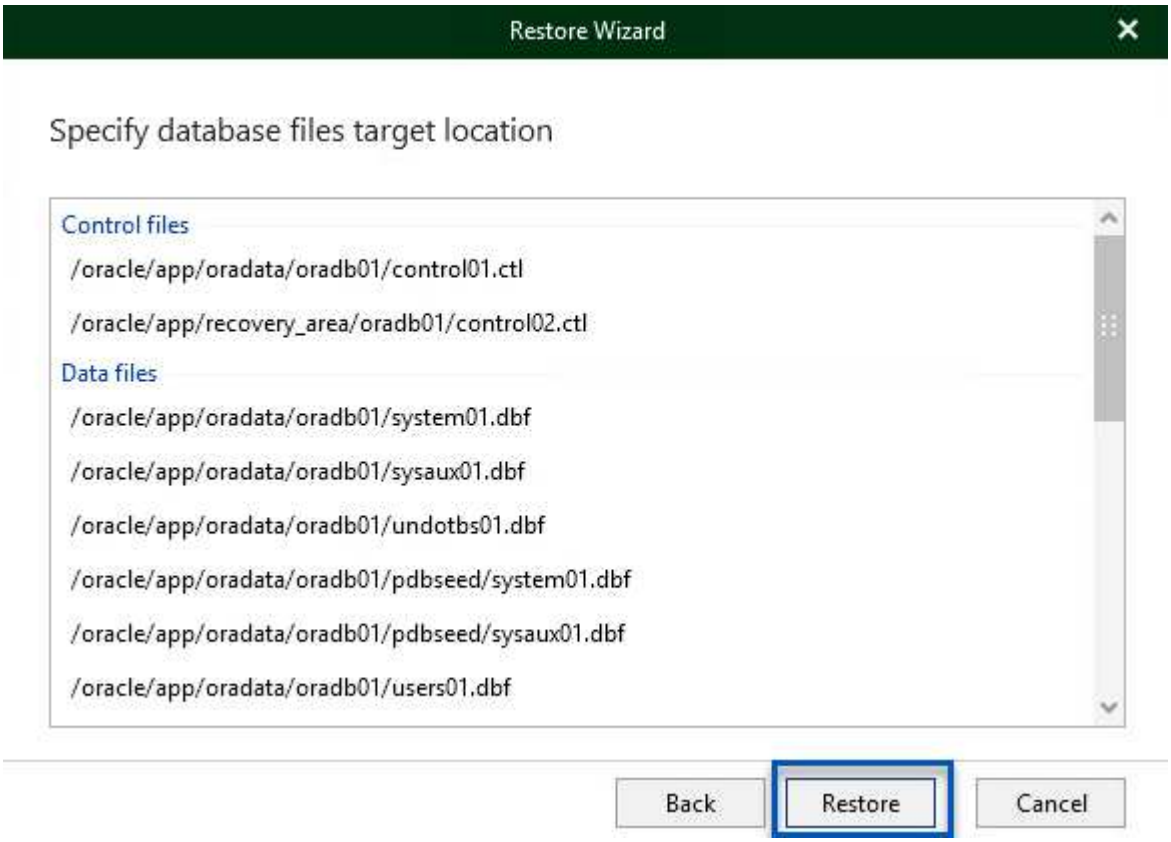
5. Nella procedura guidata di ripristino specificare il punto di ripristino da cui effettuare il ripristino e fare clic su **Avanti**.



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



7. Infine, specificare la posizione di destinazione dei file del database e fare clic sul pulsante **Ripristina** per avviare il processo di ripristino.

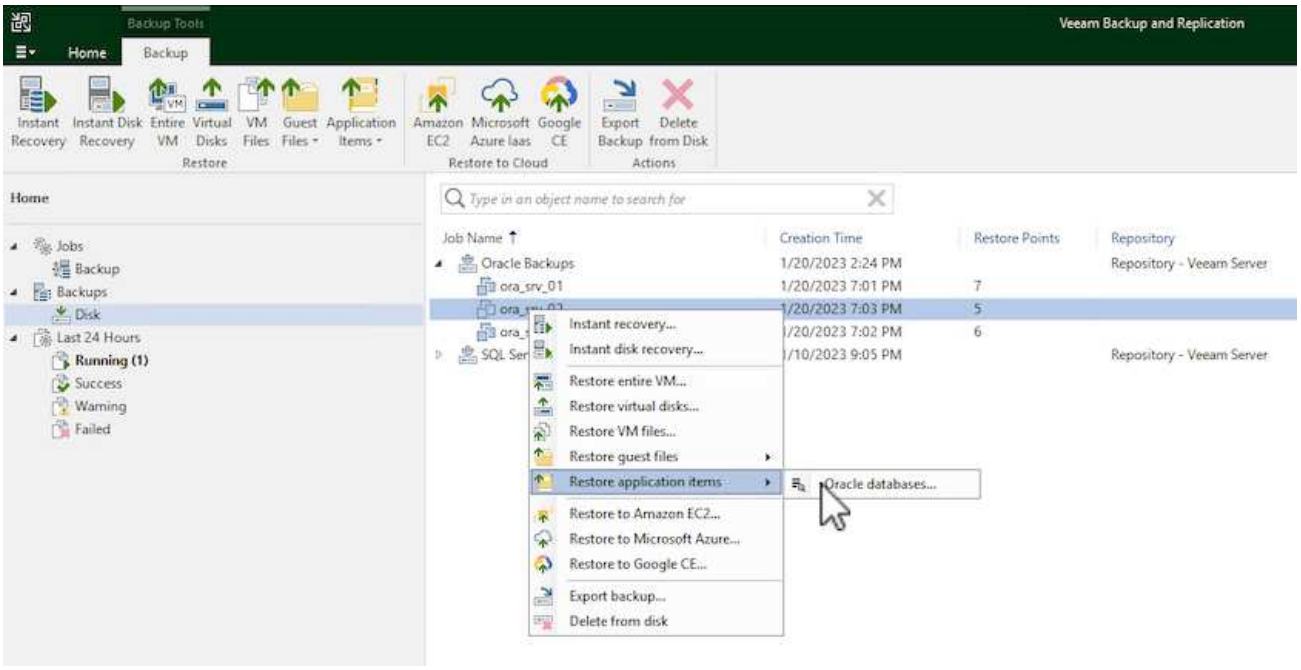


8. Una volta completato il ripristino del database, verificare che il database Oracle venga avviato correttamente sul server.

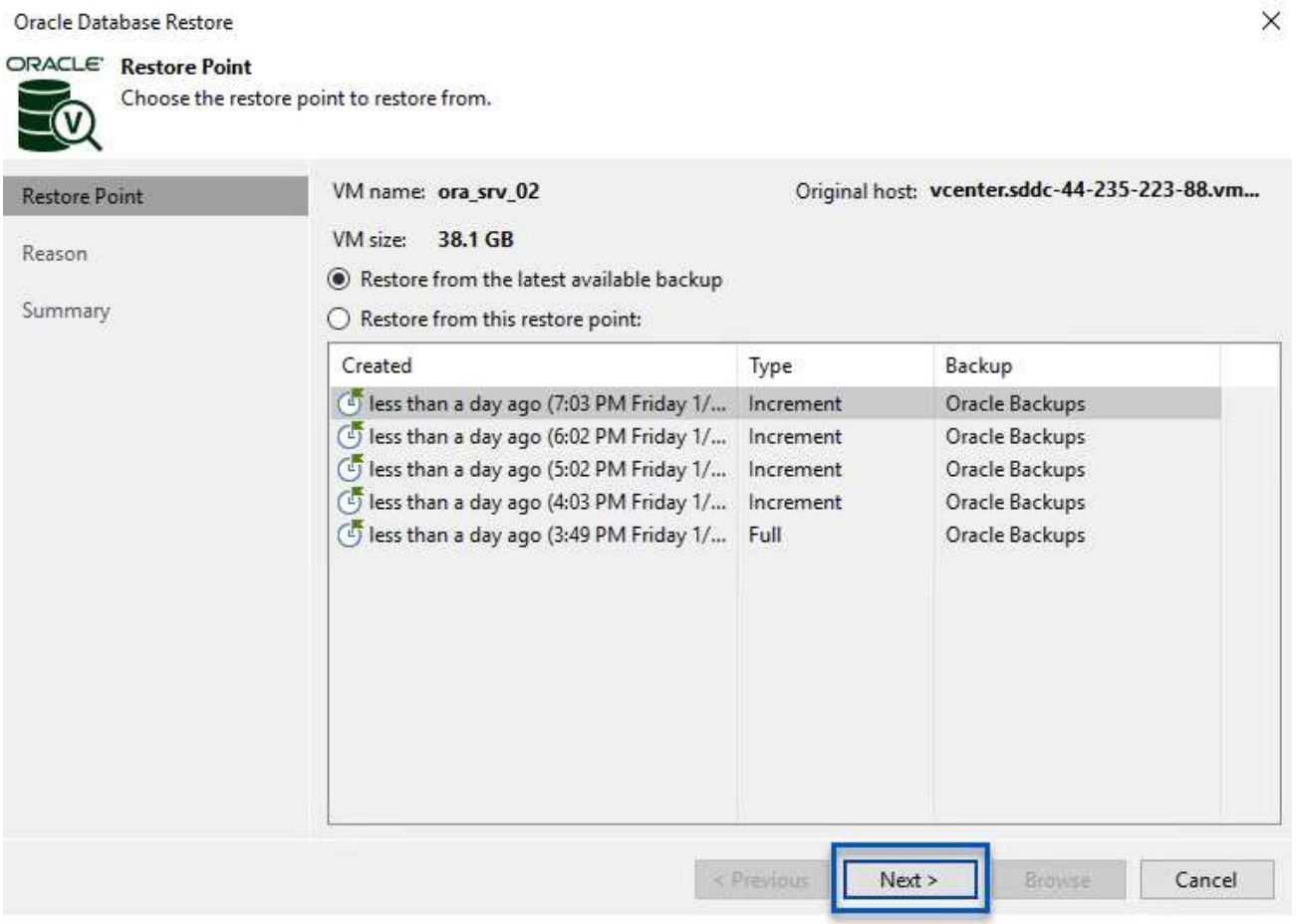
▼ **Pubblica il database Oracle su un server alternativo**

In questa sezione un database viene pubblicato su un server alternativo per un accesso rapido senza dover avviare un ripristino completo.

1. Nella console di Veeam Backup and Replication, accedere all'elenco dei backup di Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Ripristina elementi applicazione**, quindi **Database Oracle…**.

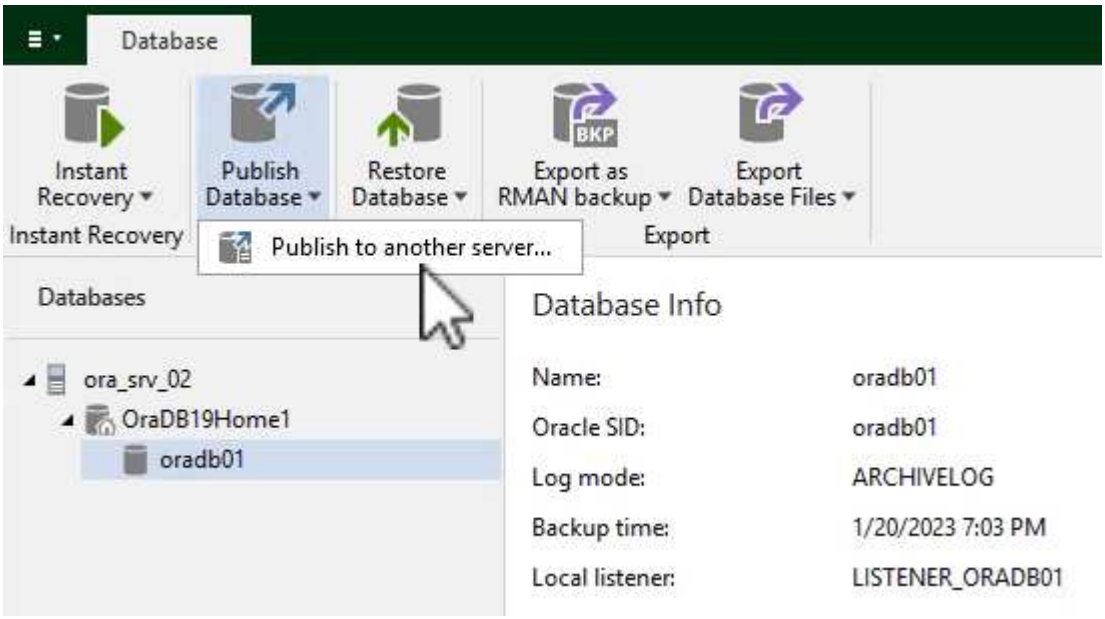


2. Nella procedura guidata di ripristino del database Oracle, selezionare un punto di ripristino dall'elenco e fare clic su **Avanti**.

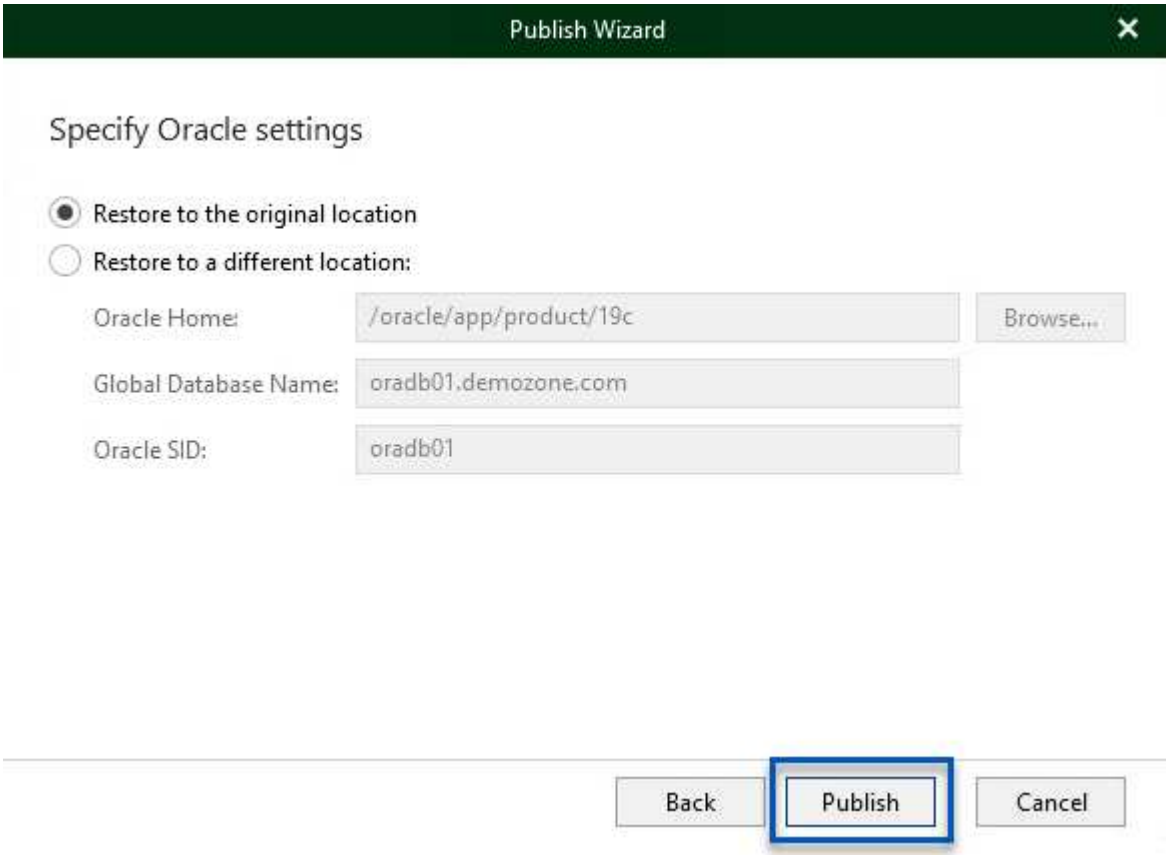


3. Se lo si desidera, immettere un **Motivo di ripristino** e quindi, nella pagina Riepilogo, fare clic sul pulsante **Sfoglia** per avviare Veeam Explorer per Oracle.

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



5. Nella procedura guidata Pubblica, specificare il punto di ripristino da cui pubblicare il database e fare clic su **Avanti**.
6. Infine, specifica la posizione del file system Linux di destinazione e fai clic su **Pubblica** per avviare il processo di ripristino.

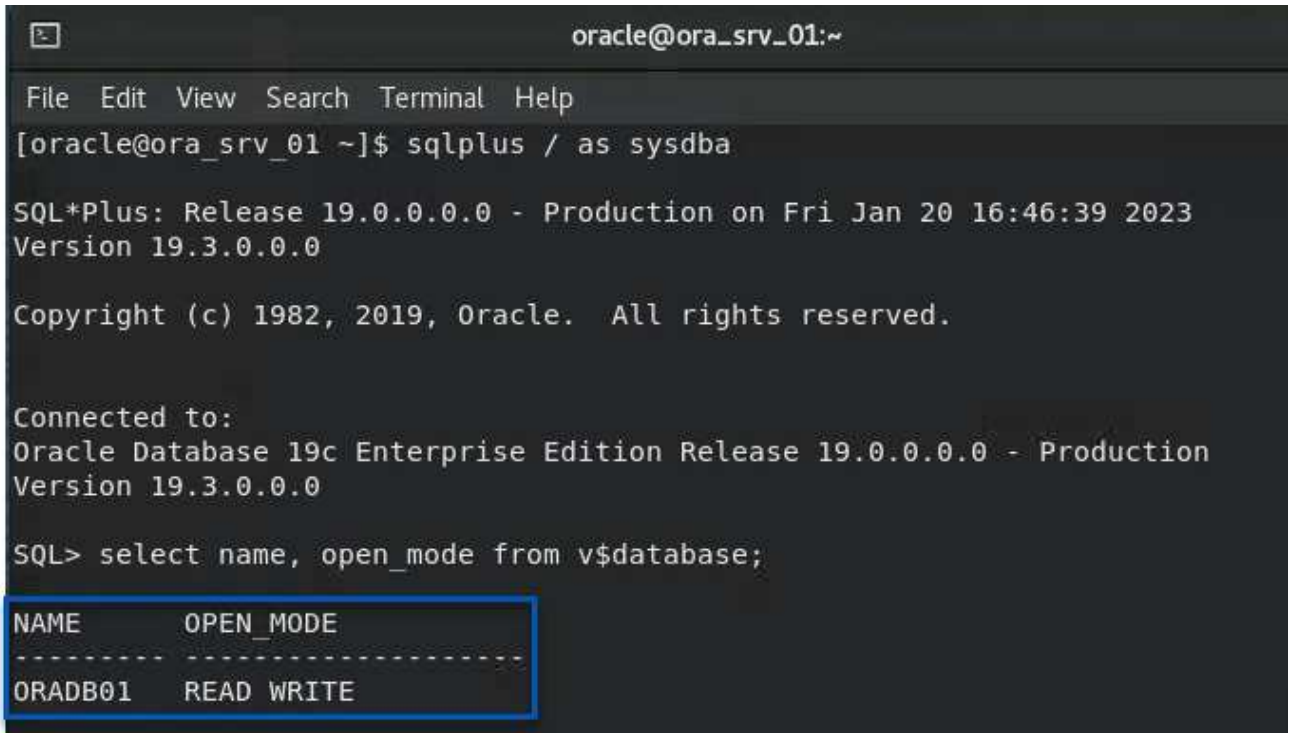


7. Una volta completata la pubblicazione, accedi al server di destinazione ed esegui i seguenti comandi

per assicurarti 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 piattaforma potente per l'esecuzione di applicazioni aziendali critiche e l'archiviazione di dati sensibili. Una soluzione di protezione dei dati sicura è essenziale per le aziende che si affidano a VMware Cloud per garantire la continuità aziendale e contribuire a proteggersi dalle minacce informatiche e dalla perdita di dati. Scegliendo una soluzione di protezione dei dati affidabile e solida, le aziende possono avere la certezza che i loro dati critici siano al sicuro e protetti, qualunque cosa accada.

Il caso d'uso presentato in questa documentazione si concentra su tecnologie di protezione dei dati comprovate che evidenziano l'integrazione tra NetApp, VMware e Veeam. FSx ONTAP è supportato come datastore NFS supplementare 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 semplificare i processi di backup e ripristino. Veeam viene utilizzato insieme ai volumi di destinazione del backup iSCSI, ospitati su FSx ONTAP, per fornire una soluzione di protezione dei dati sicura e facile da gestire per i dati delle applicazioni residenti in VMware Cloud.

Informazioni aggiuntive

Per saperne di più sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Guida utente FSx ONTAP"

- "Documentazione tecnica del Centro assistenza Veeam"
- "Supporto VMware Cloud su AWS. Considerazioni e limitazioni"

TR-4955: Disaster Recovery con FSx ONTAP e VMC (AWS VMware Cloud)

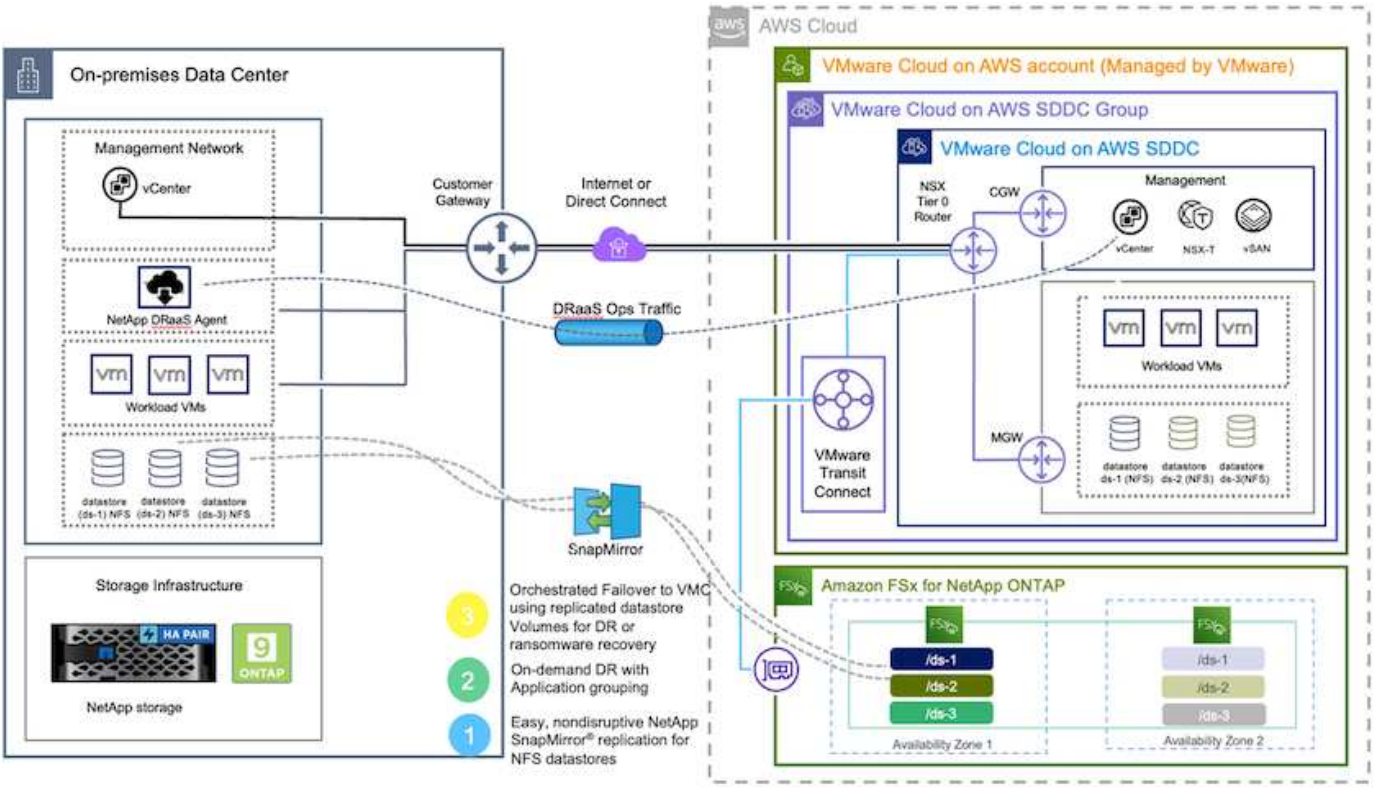
Disaster Recovery Orchestrator (DRO; una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale a FSx ONTAP. DRO automatizza il ripristino dal livello SnapMirror , tramite la registrazione della VM su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzionalità è inclusa in tutti gli ambienti VMC.

Niyaz Mohamed, NetApp

Panoramica

Il disaster recovery nel cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware). Grazie alla tecnologia NetApp SnapMirror , i carichi di lavoro VMware on-premise possono essere replicati su FSx ONTAP in esecuzione su AWS.

Disaster Recovery Orchestrator (DRO; una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale a FSx ONTAP. DRO automatizza il ripristino dal livello SnapMirror , tramite la registrazione della VM su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzionalità è inclusa in tutti gli ambienti VMC.



Iniziare

Distribuisci e configura VMware Cloud su AWS

"VMware Cloud su AWS"fornisce un'esperienza cloud-native per 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 software-defined vSAN e uno o più host ESXi che forniscono risorse di elaborazione e storage ai carichi di lavoro. Per configurare un ambiente VMC su AWS, seguire i passaggi riportati di seguito"collegamento" . Per scopi DR è possibile utilizzare anche un gruppo di spie luminose.

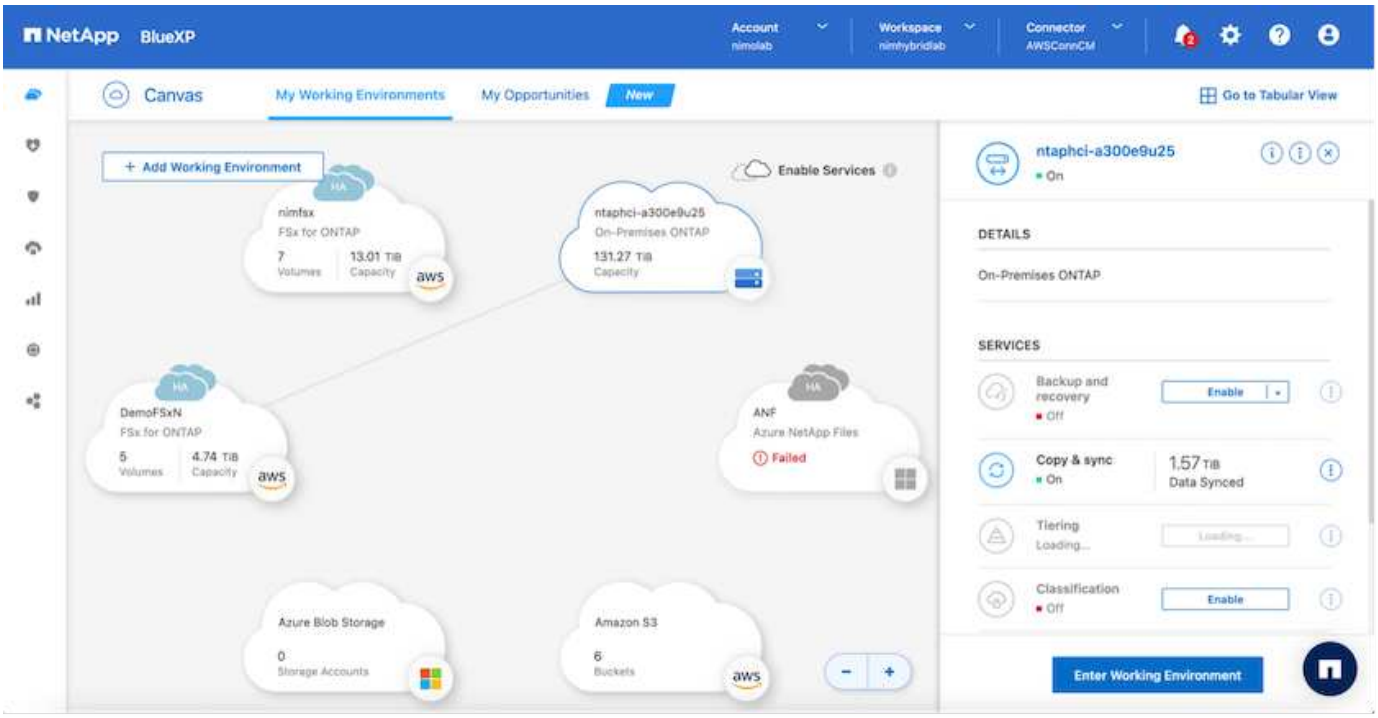
Nella versione iniziale, DRO supporta un cluster di spie luminose esistente. La creazione di SDDC su richiesta sarà disponibile in una prossima versione.

Fornire e configurare FSx ONTAP

Amazon FSx ONTAP è un servizio completamente gestito che fornisce un archivio file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità, basato sul famoso file system NetApp ONTAP . Segui i passaggi qui"collegamento" per fornire e configurare FSx ONTAP.

Distribuisci e configura SnapMirror su FSx ONTAP

Il passaggio successivo consiste nell'utilizzare NetApp Console e individuare l'istanza FSx ONTAP predisposta su AWS, quindi replicare i volumi del datastore desiderati da un ambiente on-premises a FSx ONTAP con la frequenza appropriata e la conservazione delle copie Snapshot di NetApp:



Segui i passaggi in questo link per configurare DRO. Puoi anche utilizzare la NetApp ONTAP CLI per pianificare la replica seguendo questo link.

Una relazione SnapMirror è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a usare DRO, utilizza il sistema operativo Ubuntu su un'istanza EC2 o una macchina virtuale designata per assicurarti di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti

- Assicurarsi che esista la connettività con i sistemi vCenter e di storage di origine e di destinazione.
- Se si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, è necessario utilizzare indirizzi IP per i sistemi vCenter e di storage.
- Creare un utente con permessi di root. È possibile utilizzare sudo anche con un'istanza EC2.

Requisiti OS

- Ubuntu 20.04 (LTS) con un minimo di 2 GB e 4 vCPU
- I seguenti pacchetti devono essere installati sulla VM dell'agente designata:
  - Docker
  - Docker-compose
  - Jq

Cambia i permessi su `docker.sock` : `sudo chmod 666 /var/run/docker.sock` .

IL `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

Installa 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 in locale o all'interno di una VPC AWS.

2. Decomprimi il pacchetto, esegui lo script di distribuzione e inserisci l'IP dell'host (ad esempio, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Passare alla directory ed eseguire lo script di distribuzione come segue:

```
sudo sh deploy.sh
```

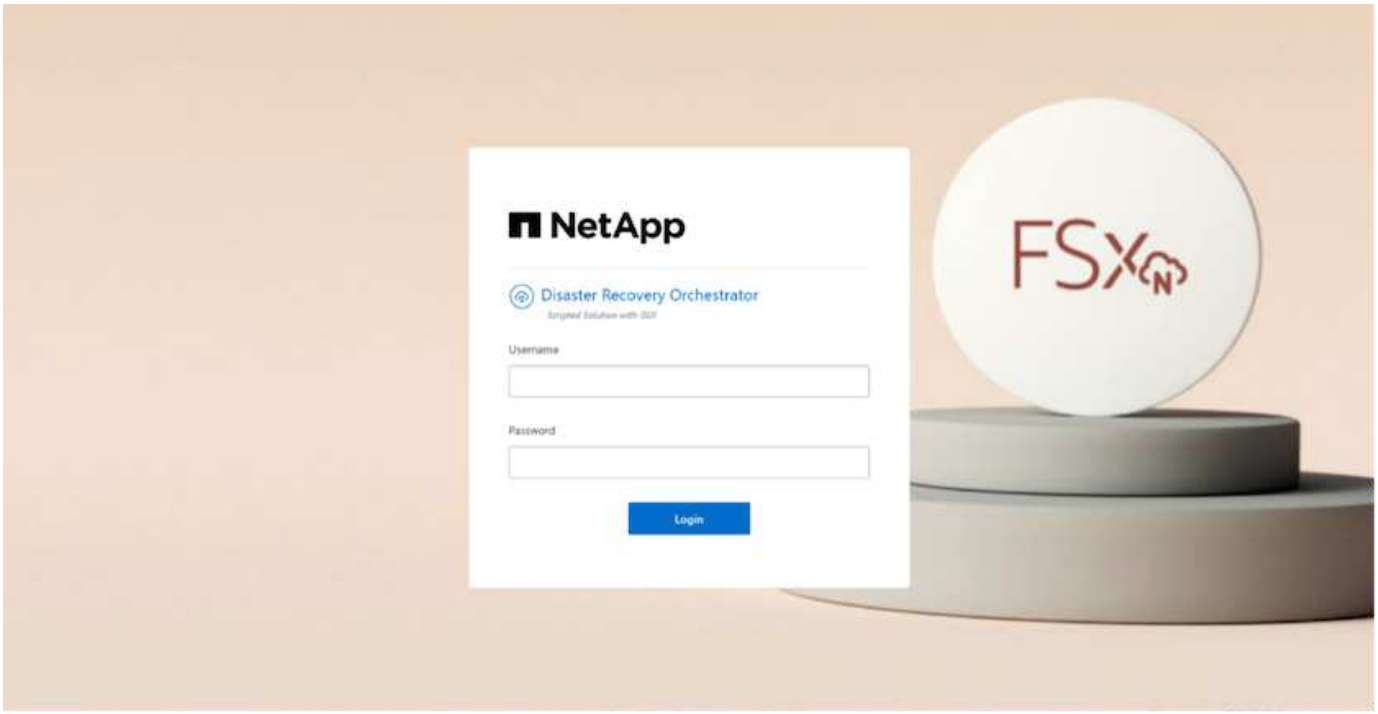
4. Accedi all'interfaccia utente tramite:

```
https://<host-ip-address>
```

con le seguenti credenziali predefinite:

```
Username: admin
Password: admin
```

La password può essere modificata utilizzando l'opzione "Cambia password".



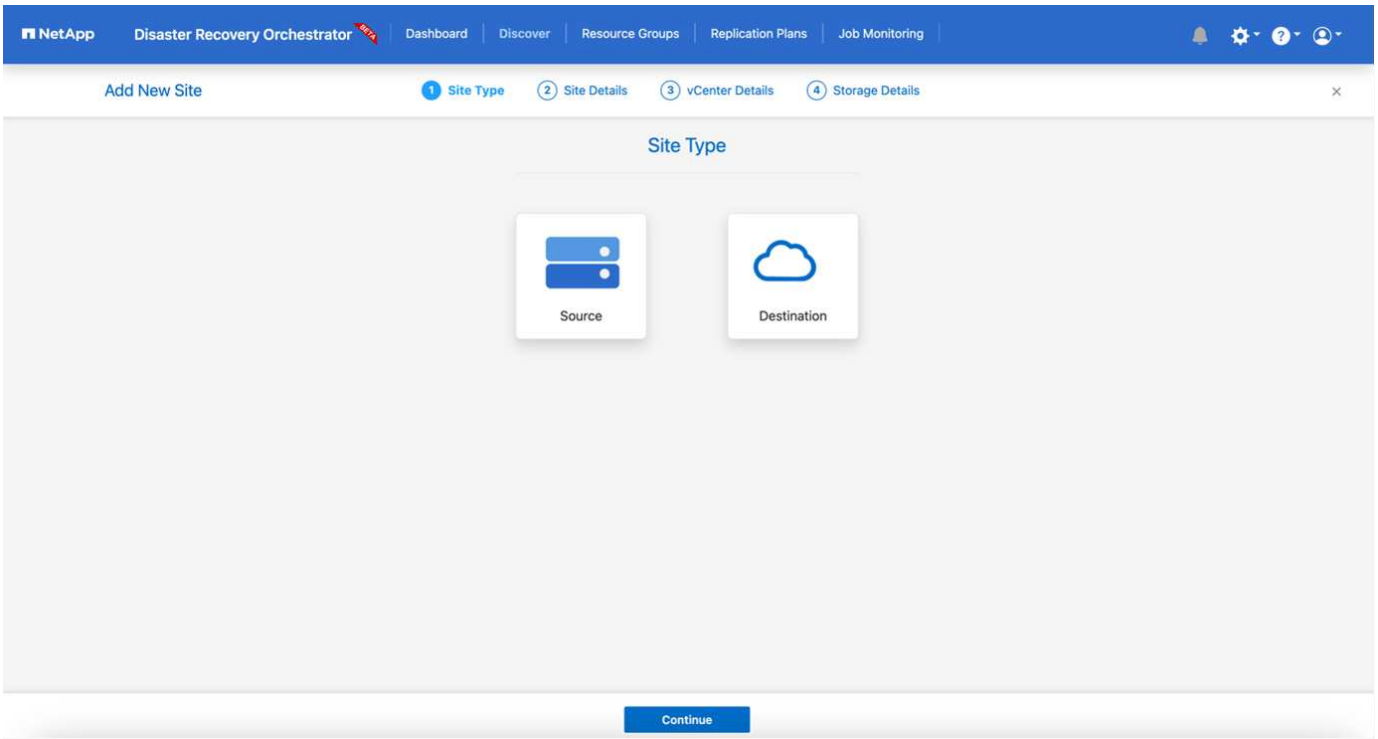
Configurazione DRO

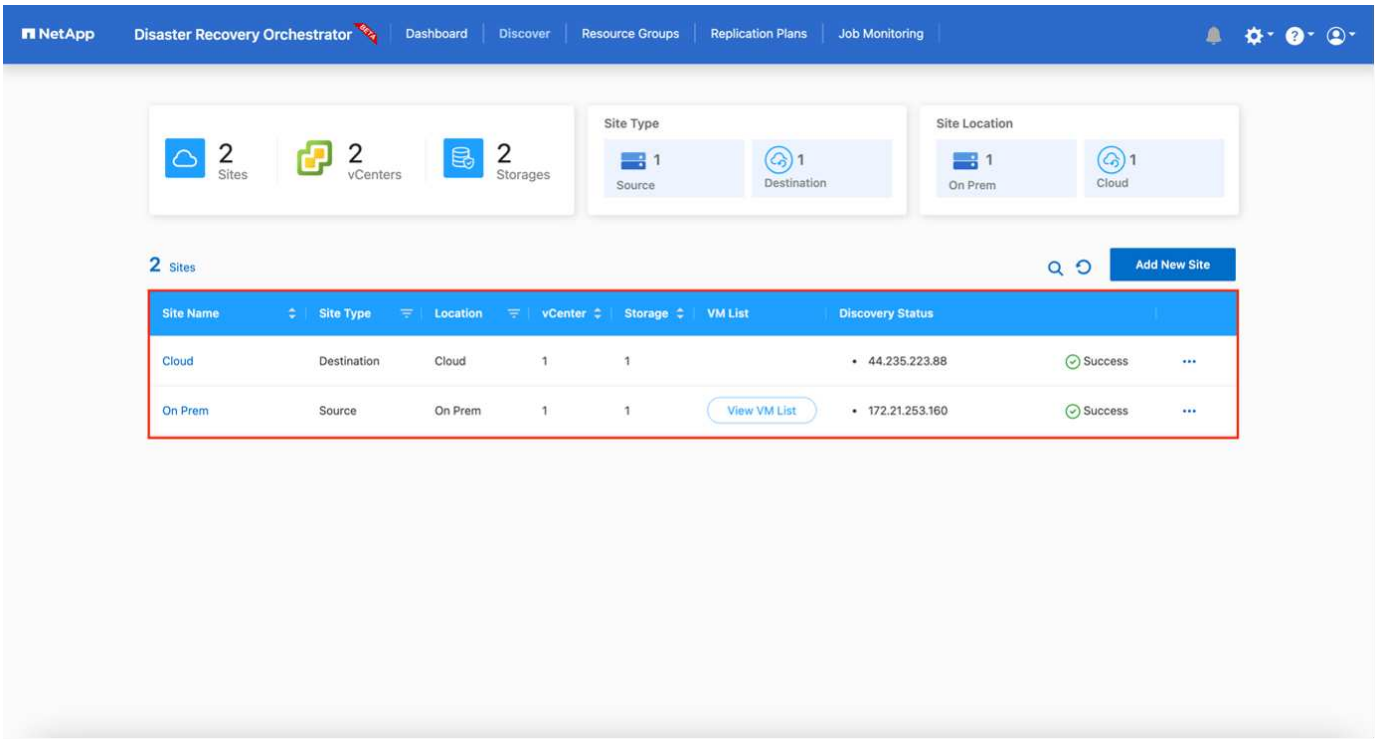
Dopo aver configurato correttamente FSx ONTAP e VMC, è possibile iniziare a configurare DRO per automatizzare il ripristino dei carichi di lavoro locali su VMC utilizzando le copie SnapMirror di sola lettura su FSx ONTAP.

NetApp consiglia di distribuire l'agente DRO in AWS e anche nella stessa VPC in cui è distribuito FSx ONTAP (può anche essere connessa tramite peer), in modo che l'agente DRO possa comunicare tramite la rete con i componenti locali e con le risorse FSx ONTAP e VMC.

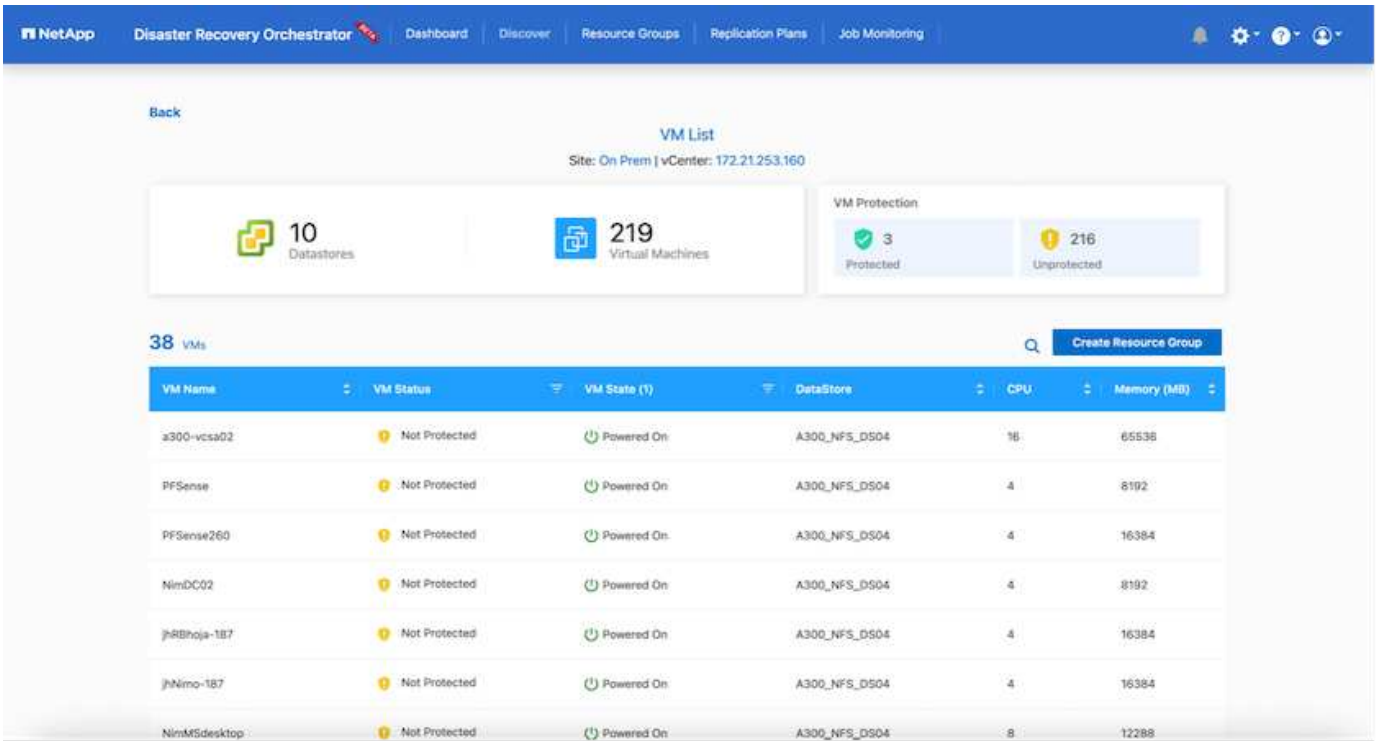
Il primo passo è individuare e aggiungere le risorse on-premise e cloud (sia vCenter che storage) a DRO. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (admin/admin) e Aggiungi siti. È possibile aggiungere siti anche tramite l'opzione Scopri. Aggiungere le seguenti piattaforme:

- In sede
  - vCenter locale
  - Sistema di archiviazione ONTAP
- Nuvola
  - VMC vCenter
  - FSx ONTAP





Una volta aggiunto, DRO esegue la rilevazione automatica e visualizza le VM che dispongono delle repliche SnapMirror corrispondenti dall'archiviazione di origine a FSx ONTAP. DRO rileva automaticamente le reti e i gruppi di porte utilizzati dalle VM e li popola.



Il passaggio successivo consiste nel raggruppare le VM necessarie in gruppi funzionali che fungeranno da gruppi di risorse.

Raggruppamenti di risorse

Dopo aver aggiunto le piattaforme, è possibile raggruppare le VM che si desidera ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

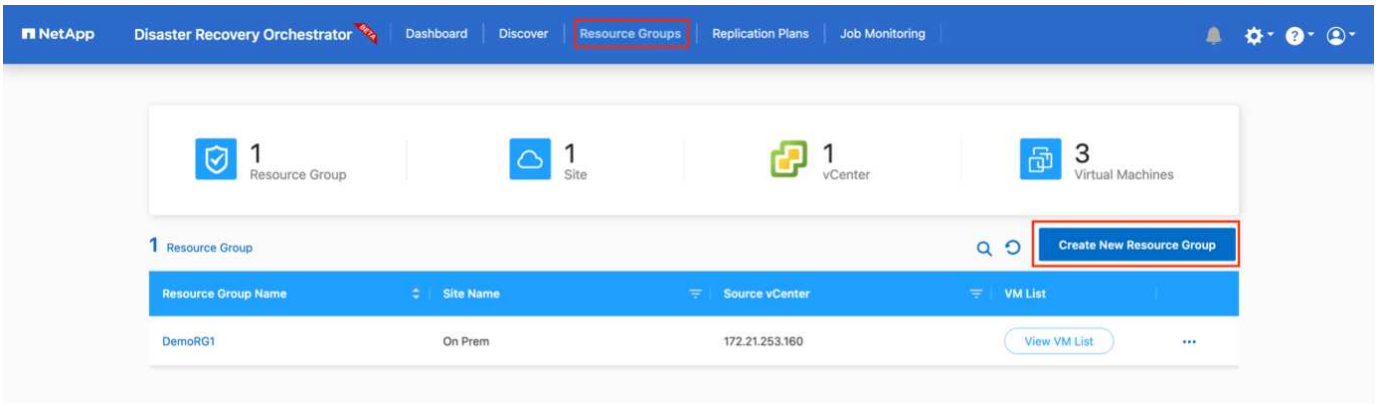
Per iniziare a creare gruppi di risorse, completare i seguenti passaggi:

1. Accedi a **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.
2. In **Nuovo gruppo di risorse**, seleziona il sito di origine dal menu a discesa e fai clic su **Crea**.
3. Fornisci **Dettagli del gruppo di risorse** e fai clic su **Continua**.
4. Selezionare le VM appropriate utilizzando l'opzione di ricerca.
5. Selezionare l'ordine di avvio e il ritardo di avvio (secondi) per le VM selezionate. Imposta l'ordine della sequenza di accensione selezionando ogni VM e impostandone la priorità. Tre è il valore predefinito per tutte le VM.

   Le opzioni sono le seguenti:

   1 – La prima macchina virtuale ad accendersi 3 – Predefinito 5 – L'ultima macchina virtuale ad accendersi

6. Fare clic su **Crea gruppo di risorse**.

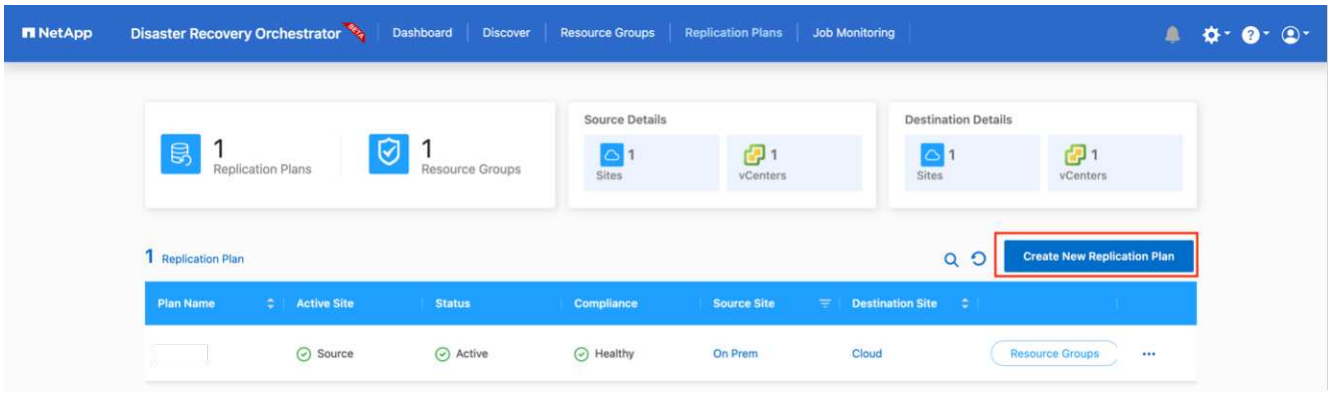


Piani di replicazione

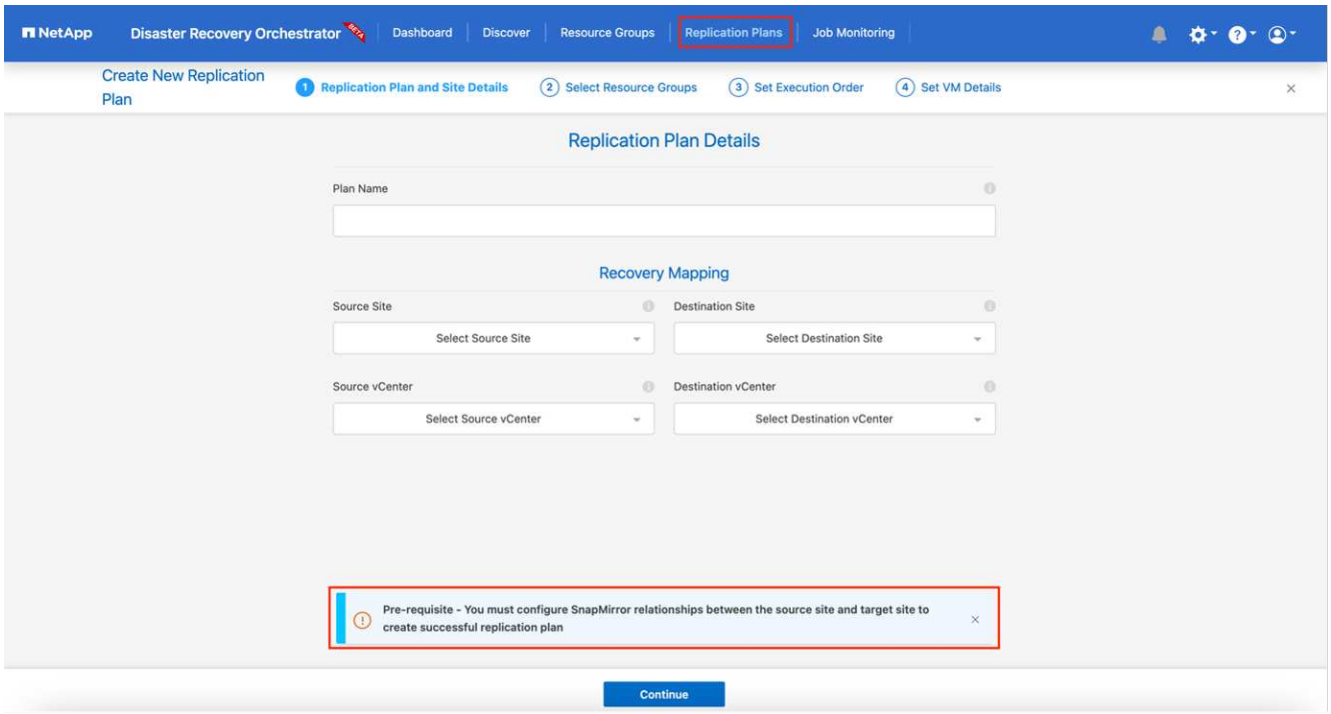
È necessario un piano per ripristinare le applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere in questo piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, quindi livello 1, quindi livello 2 e così via). Tali piani sono talvolta chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Nuovo piano di replica**.

Per iniziare a creare un piano di replicazione, completare i seguenti passaggi:

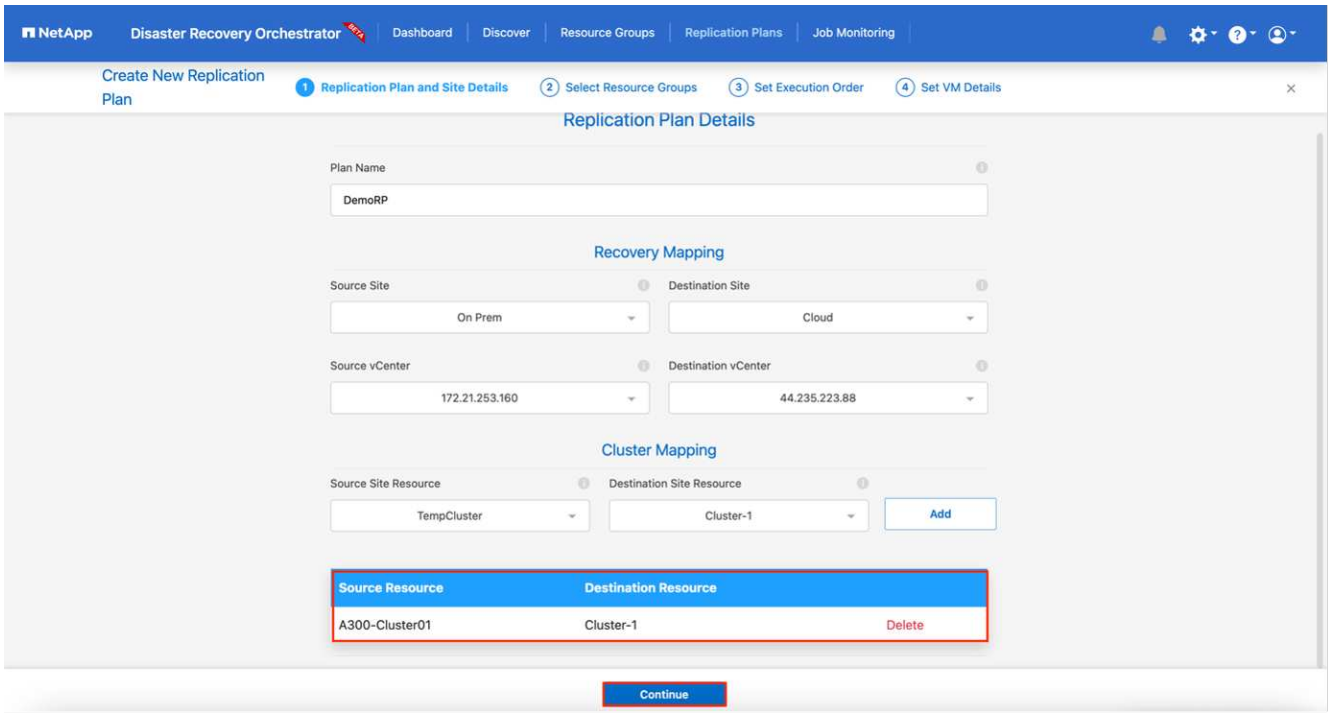
1. Accedi a **Piani di replicazione** e fai clic su **Crea nuovo piano di replicazione**.



2. In **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.

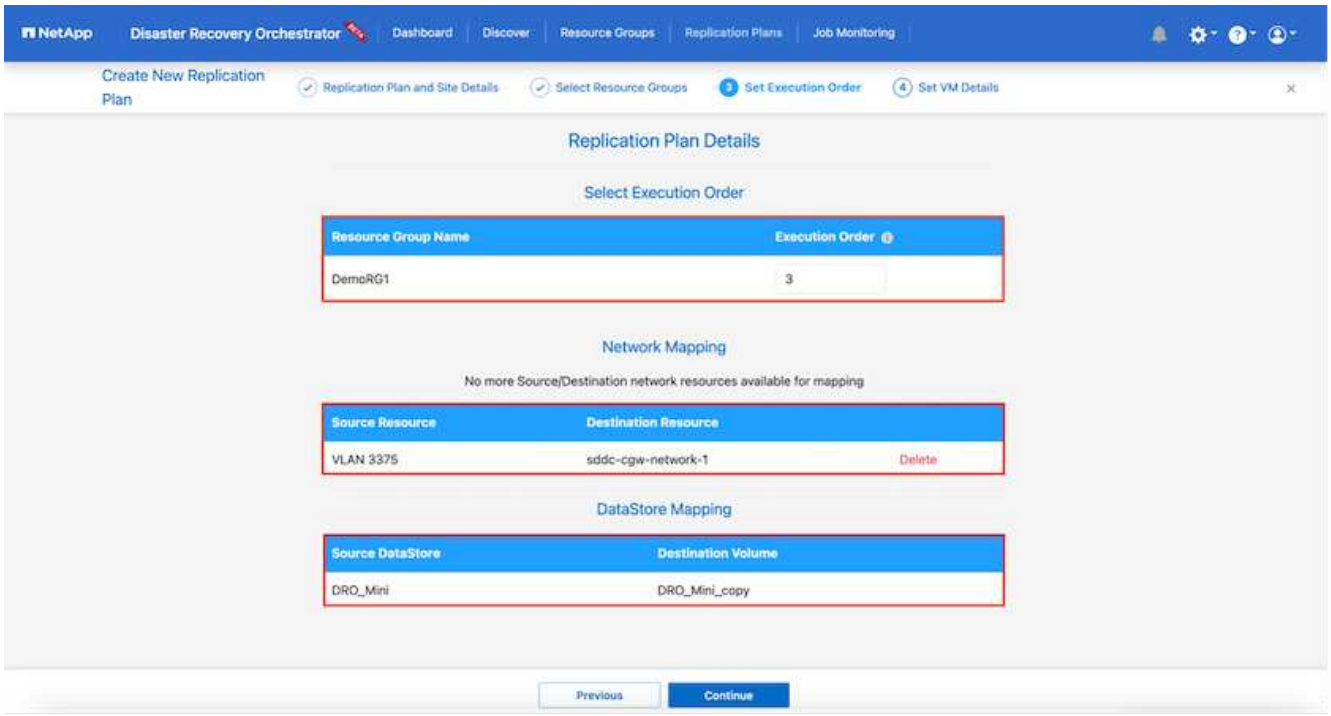


3. Una volta completata la mappatura del ripristino, selezionare la mappatura del cluster.

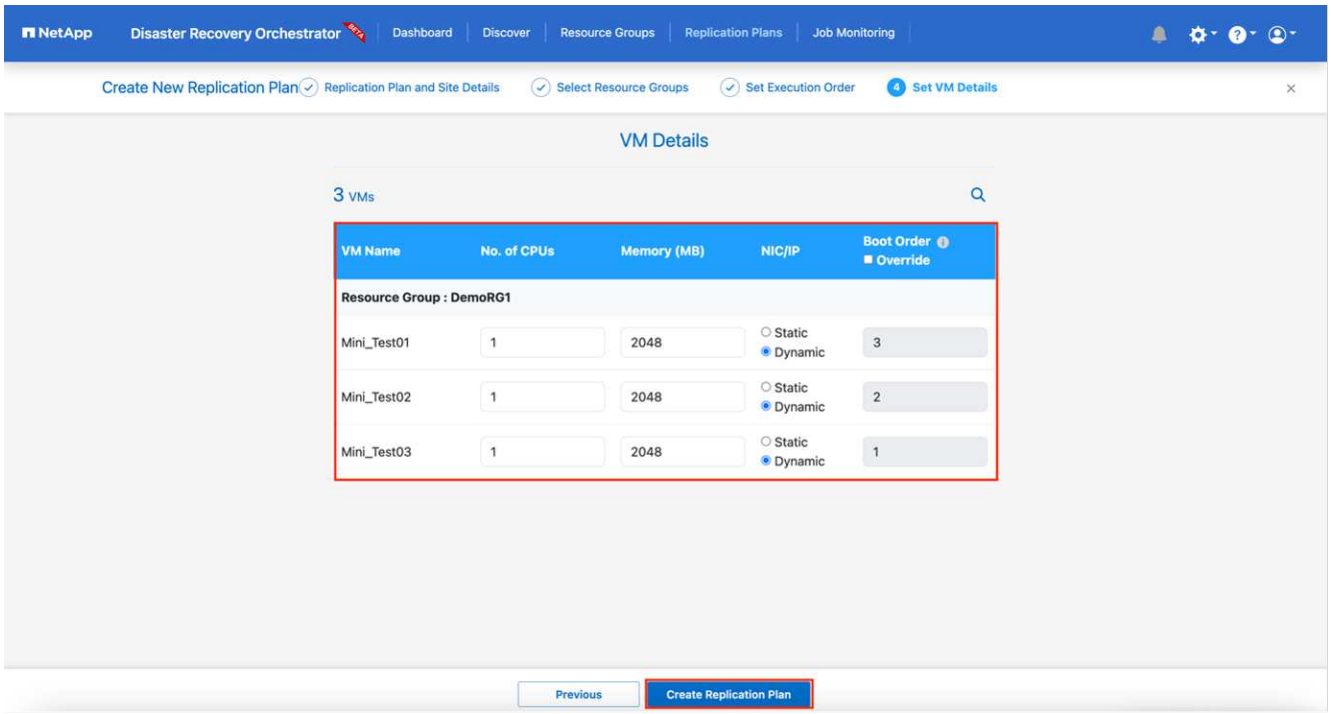


4. Selezionare **Dettagli gruppo di risorse** e fare clic su **Continua**.
5. Imposta l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza delle operazioni quando sono presenti più gruppi di risorse.
6. Una volta terminato, seleziona la mappatura di rete sul segmento appropriato. I segmenti dovrebbero essere già predisposti in VMC, quindi seleziona il segmento appropriato per mappare la VM.
7. In base alla selezione delle VM, vengono selezionate automaticamente le mappature dei datastore.

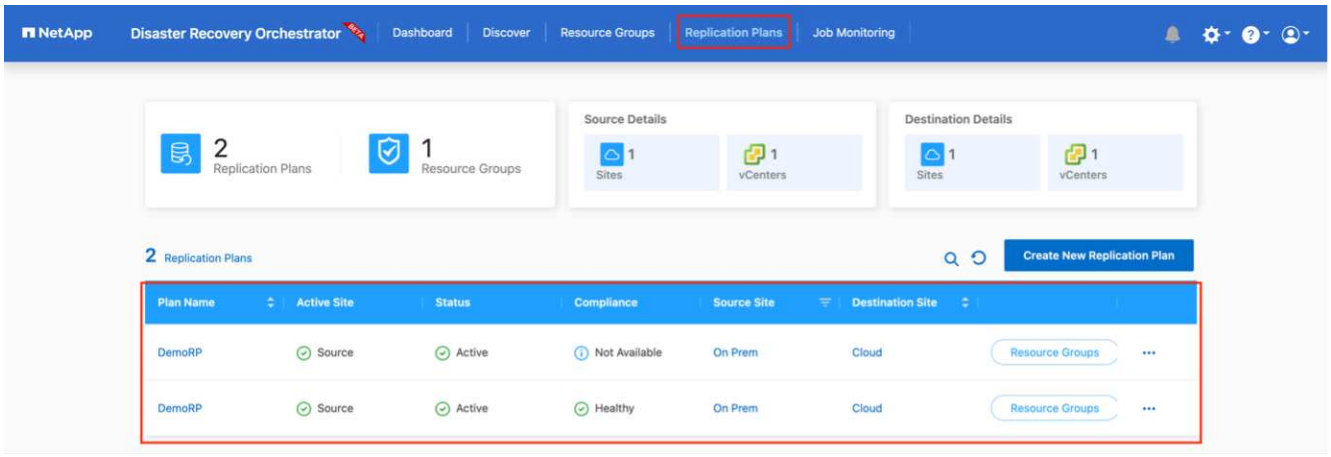
SnapMirror è al livello del volume. Pertanto, tutte le VM vengono replicate nella destinazione di replica. Assicurati di selezionare tutte le VM che fanno parte del datastore. Se non vengono selezionate, vengono elaborate solo le VM che fanno parte del piano di replica.



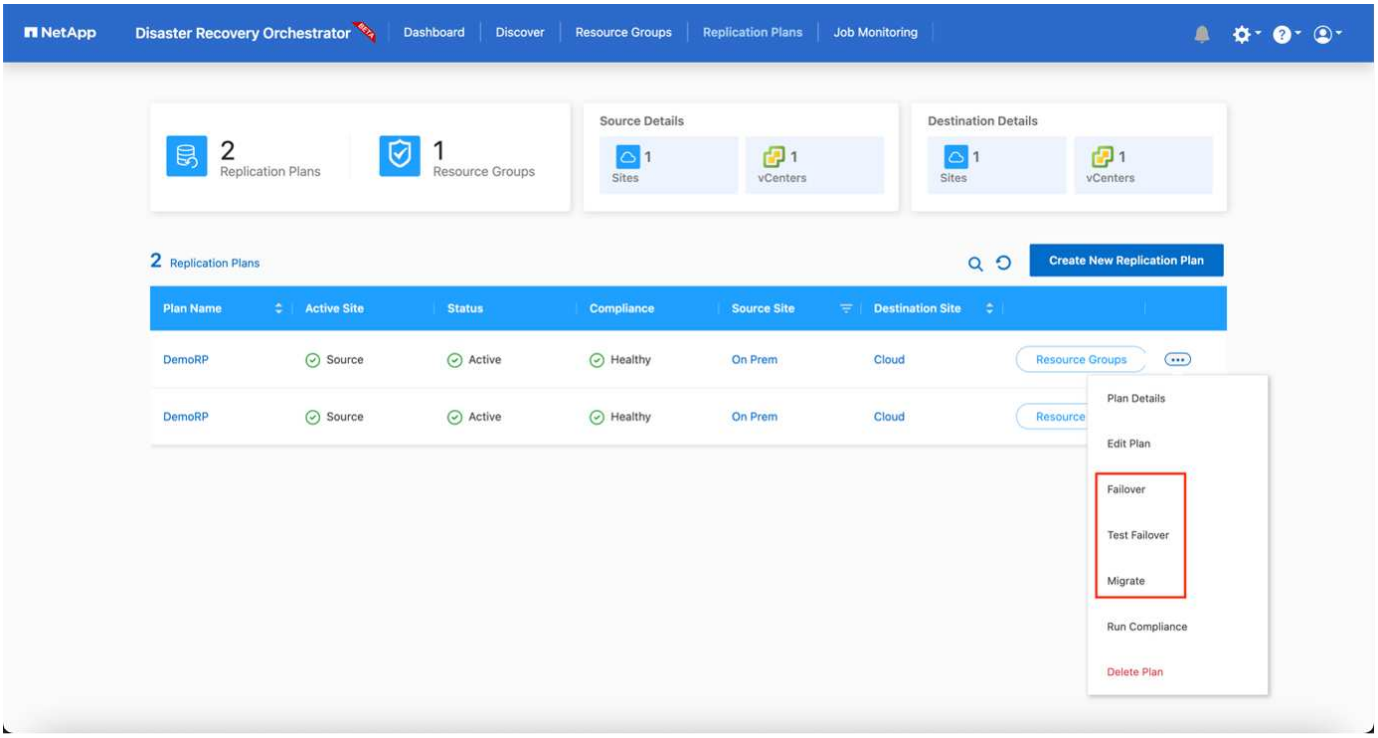
8. Nei dettagli della VM è possibile ridimensionare facoltativamente i parametri CPU e RAM della VM; questa opzione può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o per eseguire test DR senza dover predisporre un'infrastruttura VMware fisica uno a uno. Inoltre, è possibile modificare l'ordine di avvio e il ritardo di avvio (secondi) per tutte le VM selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche rispetto a 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, è possibile apportare modifiche in questa fase.

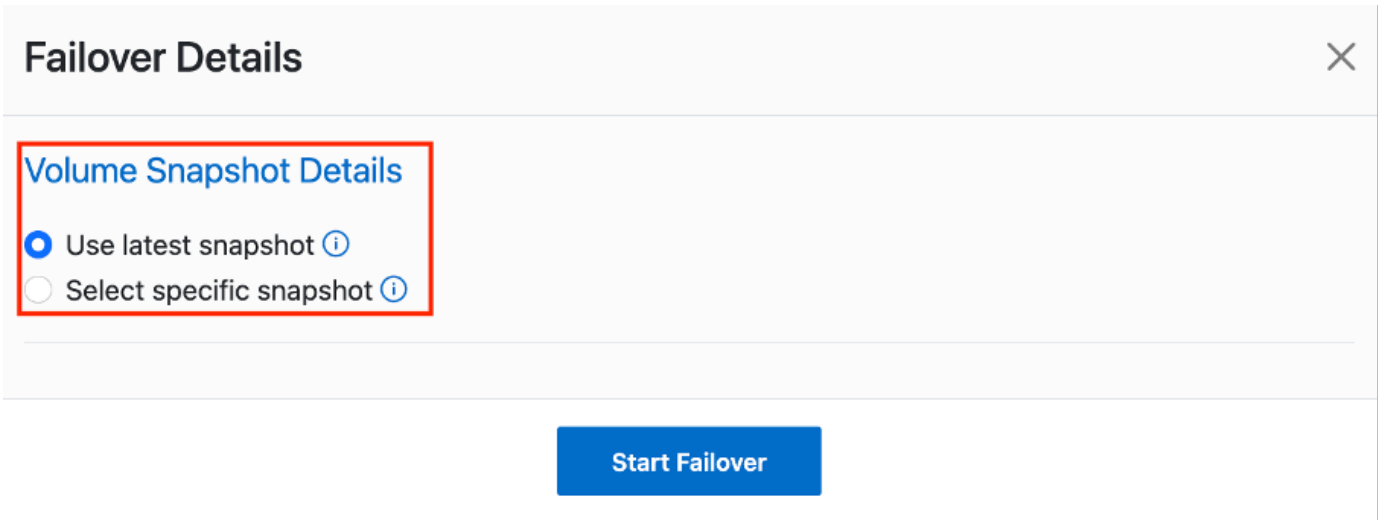


9. Fare clic su **Crea piano di replicazione**.

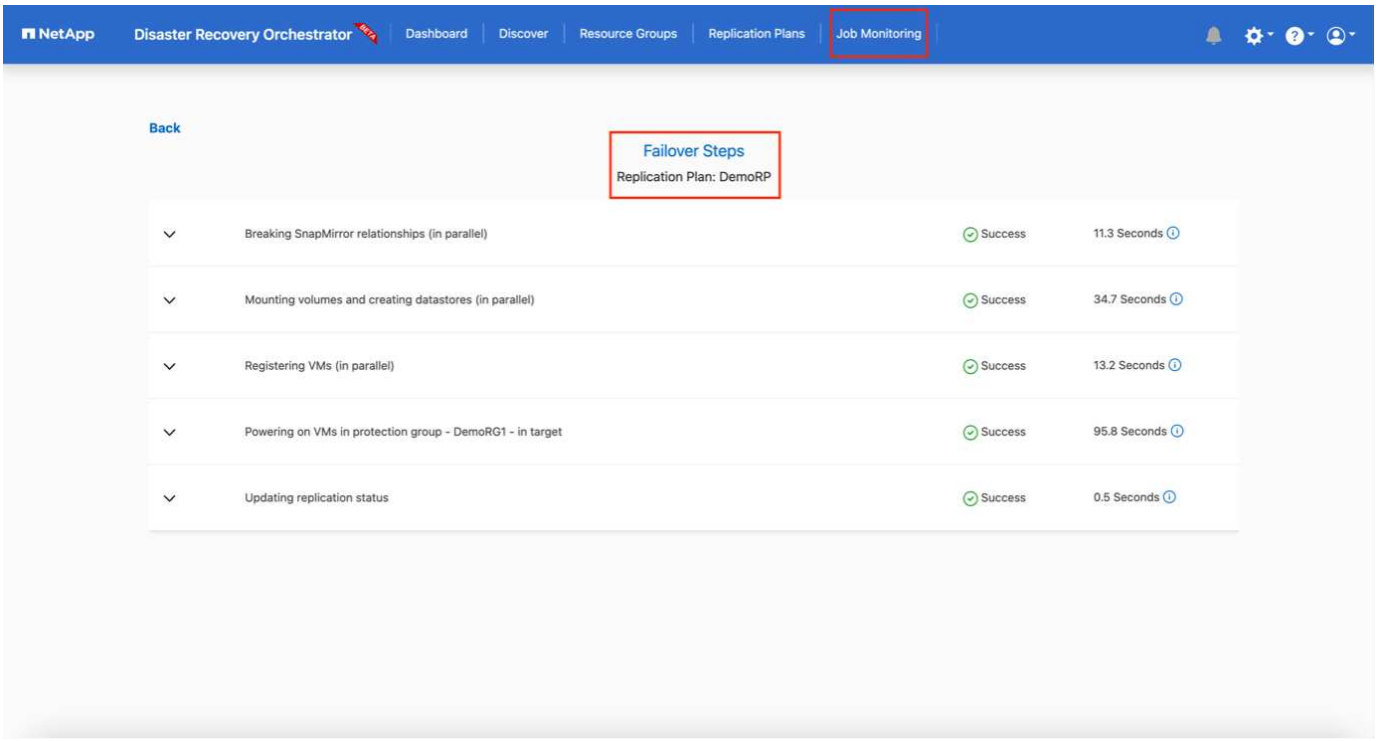


Dopo aver creato il piano di replicazione, è possibile utilizzare l'opzione failover, l'opzione test-failover o l'opzione migrazione, a seconda dei requisiti. Durante le opzioni di failover e test-failover, viene utilizzata la copia Snapshot SnapMirror più recente oppure è possibile selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (in base ai criteri di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come un 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 il failover di prova con la configurazione specificata nel piano di replica, è possibile fare clic su **Failover** o **Failover di prova**.

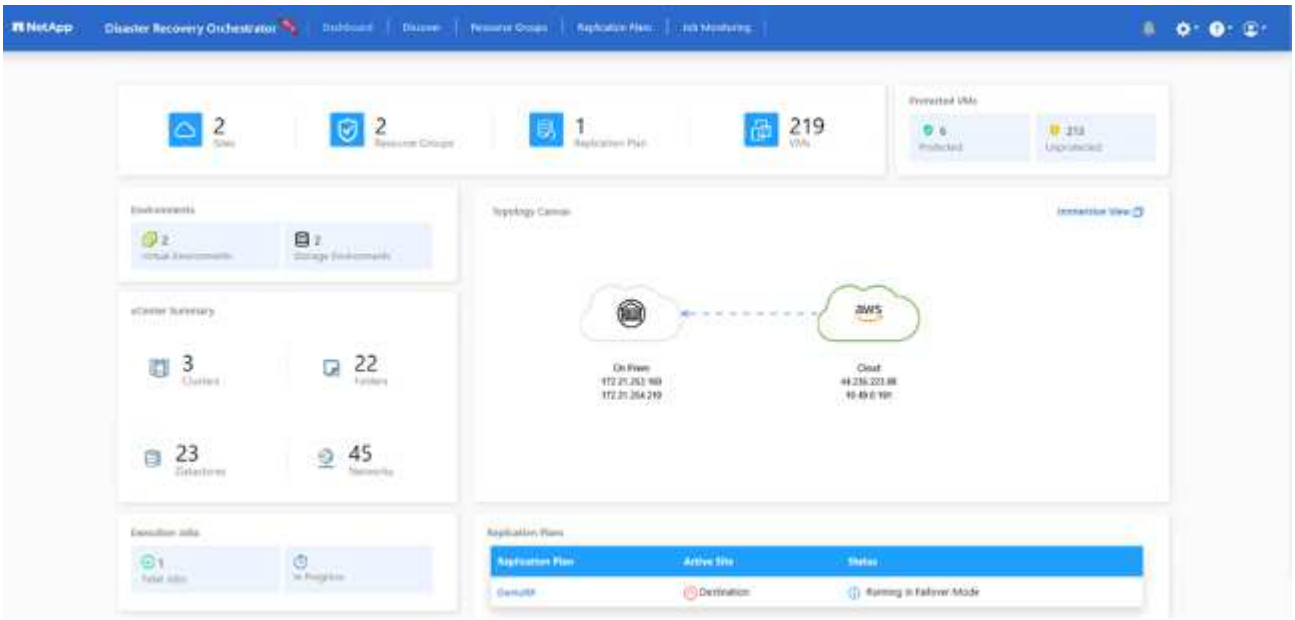




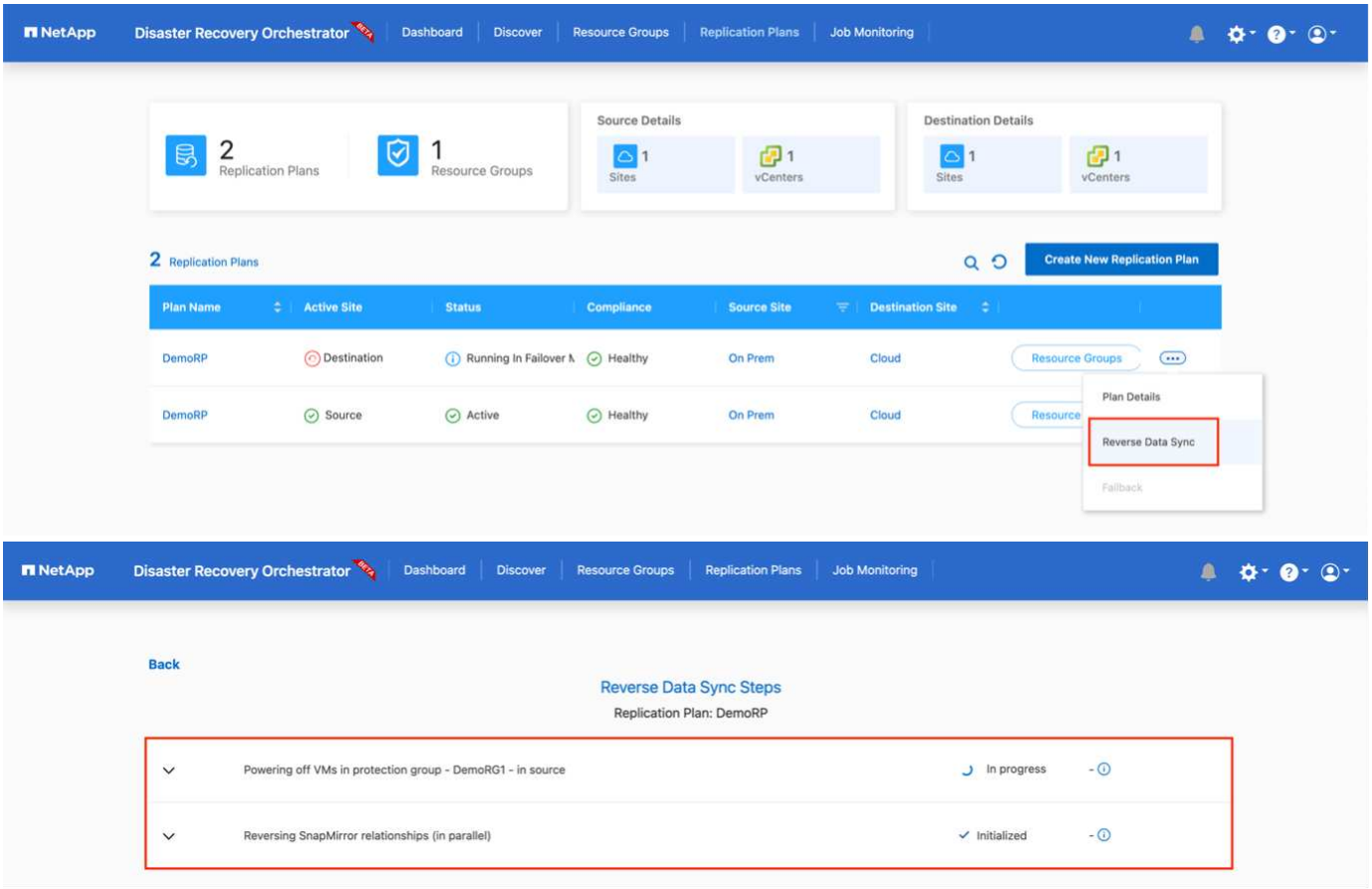
Il piano di replicazione può essere monitorato nel menu delle attività:



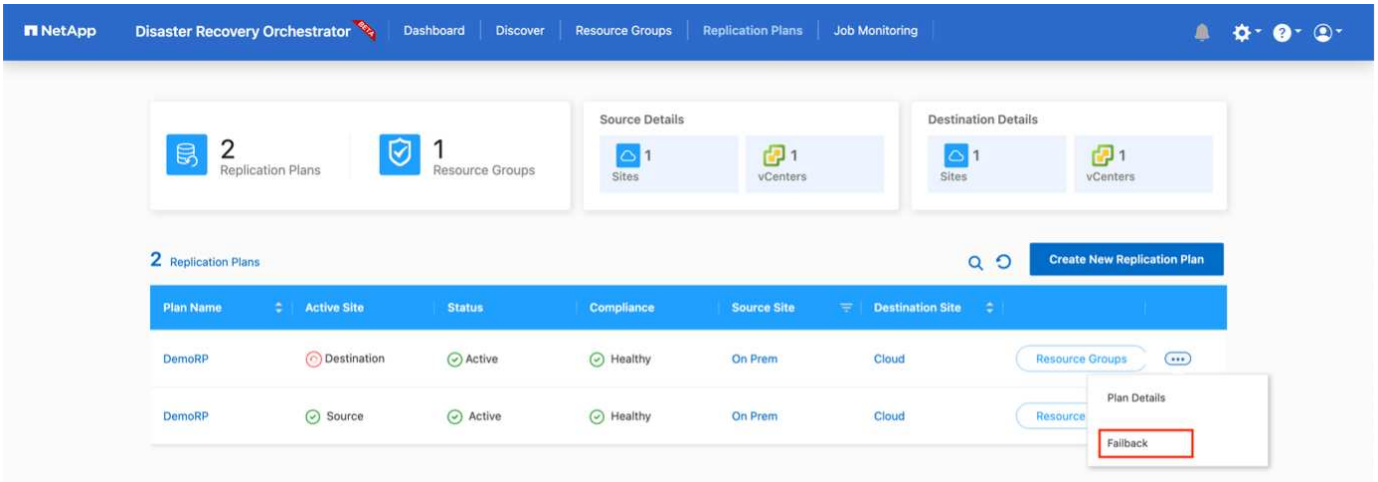
Dopo l'attivazione del failover, gli elementi recuperati possono essere visualizzati nel VMC vCenter (VM, reti, datastore). Per impostazione predefinita, le VM vengono ripristinate nella cartella Workload.

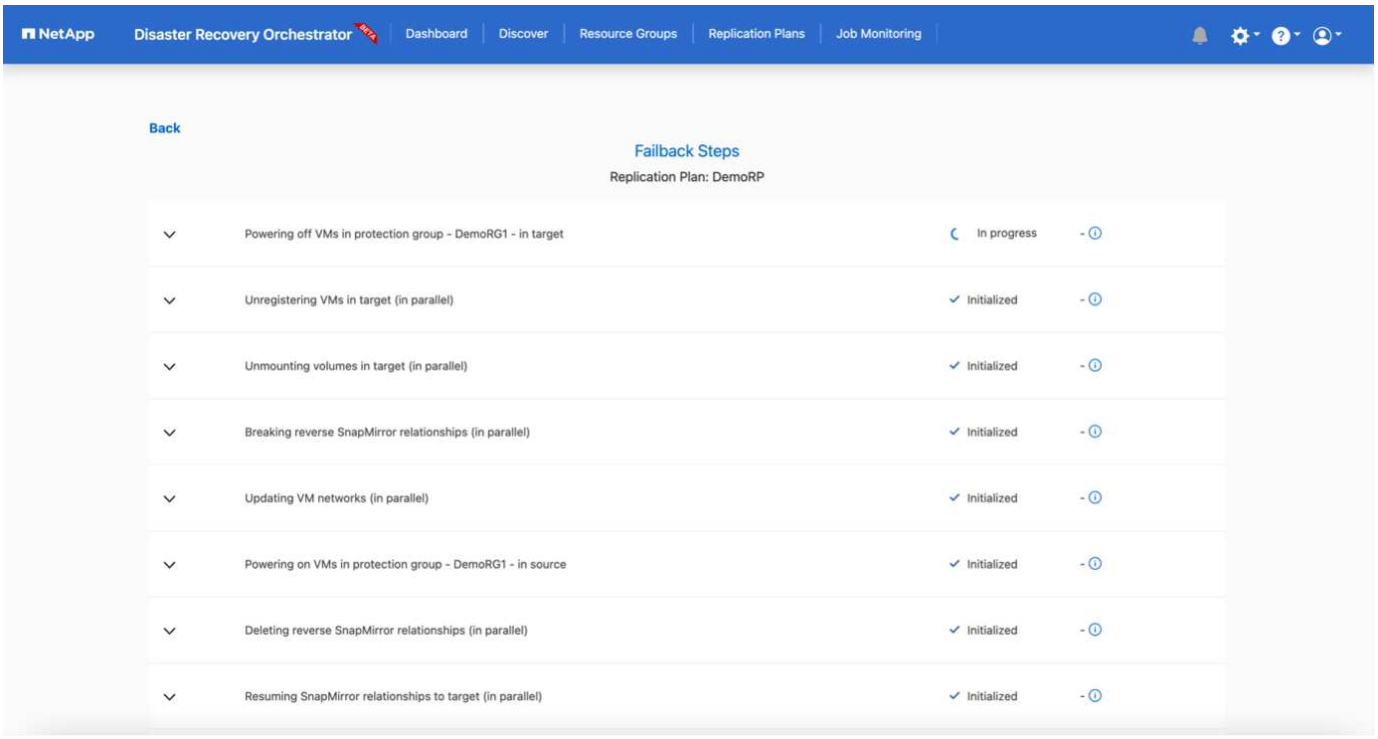


Il failback può essere attivato a livello del piano di replicazione. Per un failover di test, è possibile utilizzare l'opzione tear-down per annullare le modifiche e rimuovere la relazione FlexClone . Il failback correlato al failover è un processo in due fasi. Selezionare il piano di replicazione e selezionare **Sincronizzazione dati inversa**.

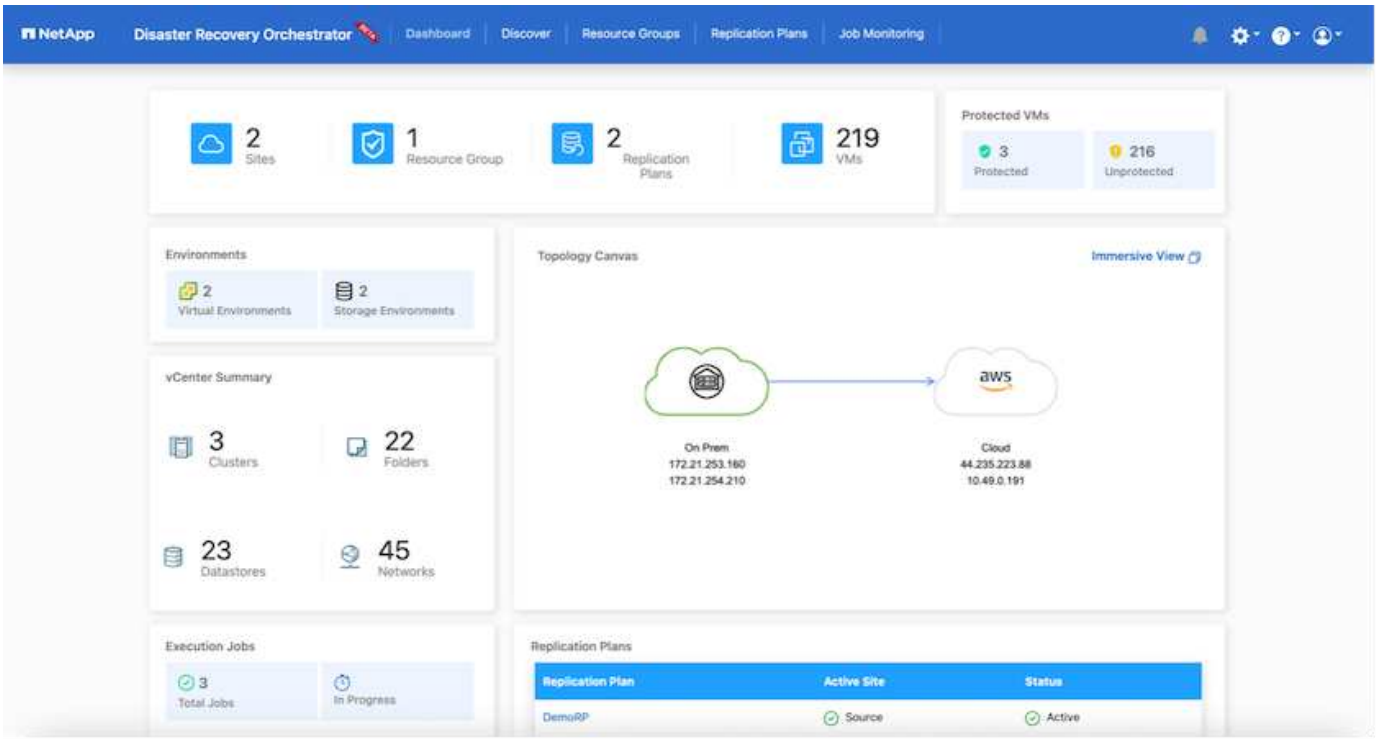


Una volta completato, è possibile attivare il failback per tornare al sito di produzione originale.





Da NetApp Console, puoi vedere che lo stato di integrità della replica si è interrotto per i volumi appropriati (quelli mappati a VMC come volumi in lettura-scrittura). Durante il failover di prova, DRO non mappa il volume di destinazione o quello di replica. Crea invece una copia FlexClone dell'istanza SnapMirror (o Snapshot) richiesta ed espone l'istanza FlexClone, che non consuma capacità fisica aggiuntiva per FSx ONTAP. Questo processo garantisce che il volume non venga modificato e che i processi di replica possano continuare anche durante i test DR o i workflow di triage. Inoltre, questo processo garantisce che, se si verificano errori o vengono recuperati dati corrotti, il recovery possa essere ripulito senza il rischio di distruggere la replica.



Recupero da ransomware

Recuperare i dati da un ransomware può essere un compito arduo. Nello specifico, può essere difficile per le organizzazioni IT individuare con precisione il punto di ritorno sicuro e, una volta determinato, proteggere i carichi di lavoro recuperati da attacchi ricorrenti, ad esempio da malware inattivi o applicazioni vulnerabili.

DRO risolve questi problemi consentendoti di ripristinare il tuo sistema da qualsiasi momento disponibile. È anche 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 siano esposte al traffico nord-sud. In questo modo, il tuo team addetto alla sicurezza avrà a disposizione un luogo sicuro in cui svolgere analisi forensi e assicurarsi che non vi siano malware nascosti o inattivi.

Benefici

- Utilizzo della replica efficiente e resiliente SnapMirror .
- Ripristino in qualsiasi momento disponibile con conservazione della copia Snapshot.
- Automazione completa di tutti i passaggi necessari per ripristinare centinaia o migliaia di VM dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- Ripristino del carico di lavoro con la tecnologia ONTAP FlexClone utilizzando un metodo che non modifica il volume replicato.
  - Evita il rischio di danneggiamento dei dati per volumi o copie Snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.
  - Potenziale utilizzo dei dati DR con risorse di cloud computing per flussi di lavoro che vanno oltre il DR, come DevTest, test di sicurezza, test di patch o aggiornamento e test di correzione.
- Ottimizzazione di CPU e RAM per contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

Utilizzo di Veeam Replication e FSx ONTAP per il disaster recovery su VMware Cloud su AWS

L'integrazione Amazon FSx ONTAP con VMware Cloud su AWS è un datastore NFS esterno gestito da AWS basato sul file system ONTAP di NetApp che può essere collegato a un cluster nell'SDDC. Fornisce ai clienti un'infrastruttura di storage virtualizzata flessibile e ad alte prestazioni, che si adatta in modo indipendente alle risorse di elaborazione.

Panoramica

Per i clienti che desiderano utilizzare VMware Cloud su AWS SDDC come destinazione di disaster recovery, i datastore FSx ONTAP possono essere utilizzati per replicare i dati da locali utilizzando qualsiasi soluzione di terze parti convalidata che fornisca funzionalità di replicazione delle VM. Aggiungendo il datastore FSx ONTAP , sarà possibile ottimizzare i costi di distribuzione rispetto alla creazione di VMware Cloud su AWS SDDC con un'enorme quantità di host ESXi solo per ospitare lo storage.

Questo approccio aiuta inoltre i clienti a utilizzare il cluster di luci pilota in VMC insieme ai datastore FSx ONTAP per ospitare le repliche delle VM. Lo stesso processo può essere esteso anche come opzione di migrazione a VMware Cloud su AWS eseguendo il failover del piano di replica.

Dichiarazione del problema

Questo documento descrive come utilizzare il datastore FSx ONTAP e Veeam Backup and Replication per configurare il disaster recovery per le VM VMware on-premise su VMware Cloud on AWS utilizzando la

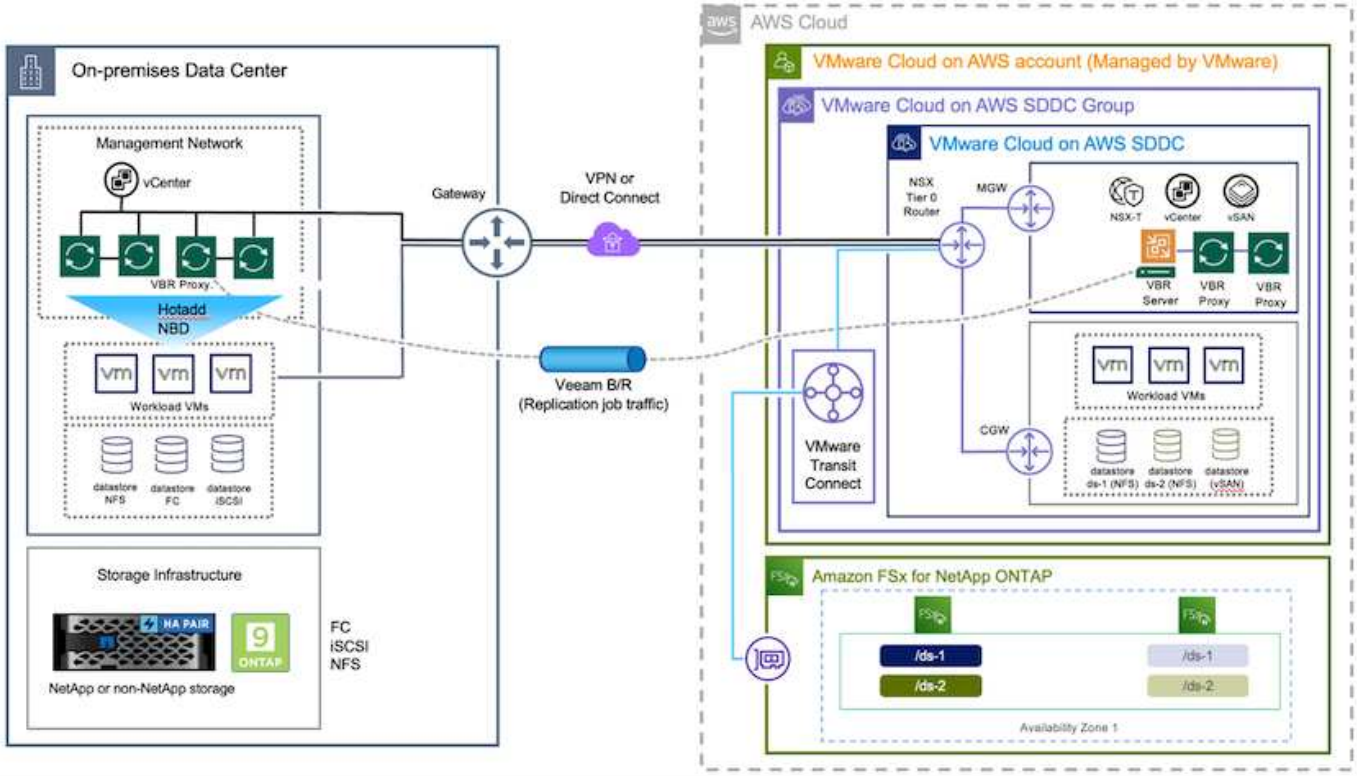
funzionalità di replica delle VM.

Veeam Backup & Replication consente la replica in loco e da remoto per il disaster recovery (DR). Quando le macchine virtuali vengono replicate, Veeam Backup & Replication crea una copia esatta delle VM nel formato nativo VMware vSphere sul cluster VMware Cloud on AWS SDDC di destinazione e mantiene la copia sincronizzata con la VM originale.

La replica fornisce i migliori valori di Recovery Time Objective (RTO) poiché è presente una copia di una VM nello stato pronto per l'avvio. Questo meccanismo di replicazione garantisce che i carichi di lavoro possano essere avviati rapidamente in VMware Cloud su AWS SDDC in caso di disastro. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e connessioni lente. Inoltre, filtra i blocchi di dati duplicati, i blocchi di dati zero, i file di swap e i file del sistema operativo guest della VM esclusi e comprime il traffico di replica.

Per evitare che i processi di replicazione consumino l'intera larghezza di banda della rete, è possibile implementare acceleratori WAN e regole di limitazione della rete. Il processo di replica in Veeam Backup & Replication è guidato dai processi, ovvero la replica viene eseguita configurando i processi di replica. In caso di disastro, è possibile attivare il failover per ripristinare le VM eseguendo il failover sulla relativa copia replica.

Quando viene eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito sullo stato più recente di una replica o su uno qualsiasi dei suoi punti di ripristino noti. Ciò consente il ripristino da ransomware o test isolati, a seconda delle necessità. 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.



Distribuzione della soluzione

Gradini di alto livello

1. Il software Veeam Backup and Replication è in esecuzione in un ambiente locale con connettività di rete adeguata.

2. Configura VMware Cloud su AWS; consulta l'articolo di VMware Cloud Tech Zone "Guida alla distribuzione dell'integrazione di VMware Cloud su AWS con Amazon FSx ONTAP" per distribuire e configurare VMware Cloud su AWS SDDC e FSx ONTAP come datastore NFS. (Per il DR, puoi usare un ambiente pilot-light configurato al minimo. Le VM eseguiranno il failover su questo cluster in caso di incidente e potrai aggiungere altri nodi).
3. Imposta processi di replica per creare repliche di VM utilizzando Veeam Backup and Replication.
4. Creare un piano di failover ed eseguire il failover.
5. Una volta completato l'evento disastroso e quando il sito primario è attivo, tornare alle VM di produzione.

Prerequisiti per Veeam VM Replication su VMC e datastore FSx ONTAP

1. Assicurarsi che la VM 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 vCenter di origine e di destinazione.
3. Il datastore FSx ONTAP di destinazione deve disporre di spazio libero sufficiente per archiviare i VMDK delle VM replicate

Per ulteriori informazioni, fare riferimento alla sezione "Considerazioni e limitazioni" trattata"Qui" .

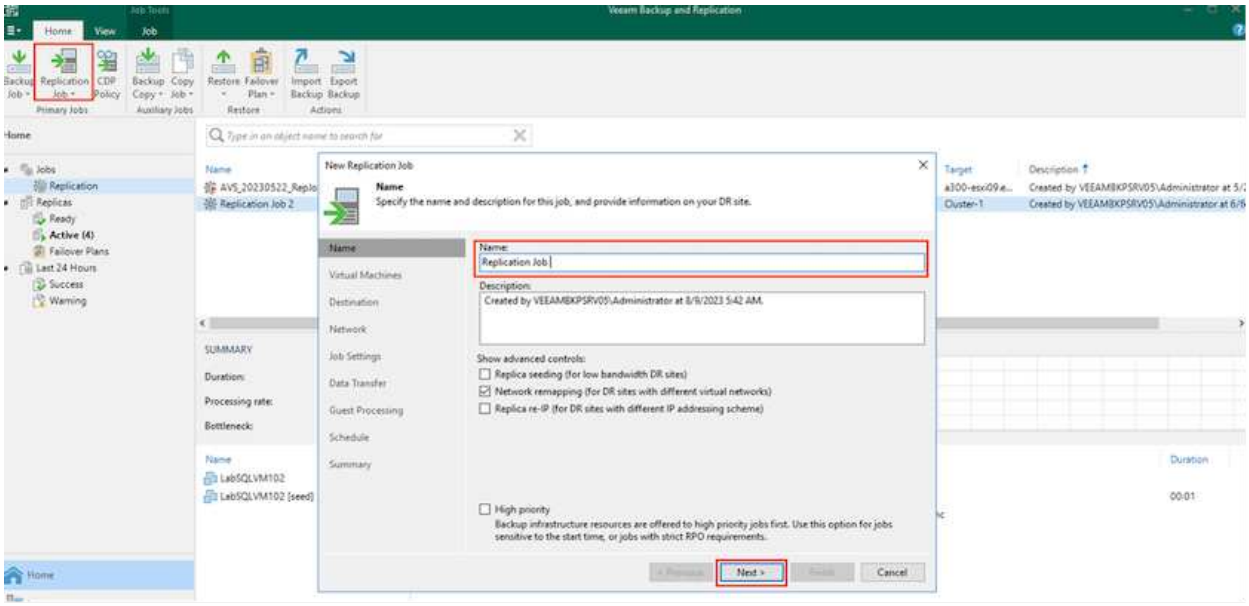
Dettagli di distribuzione

▼ **Passaggio 1: replicare le VM**

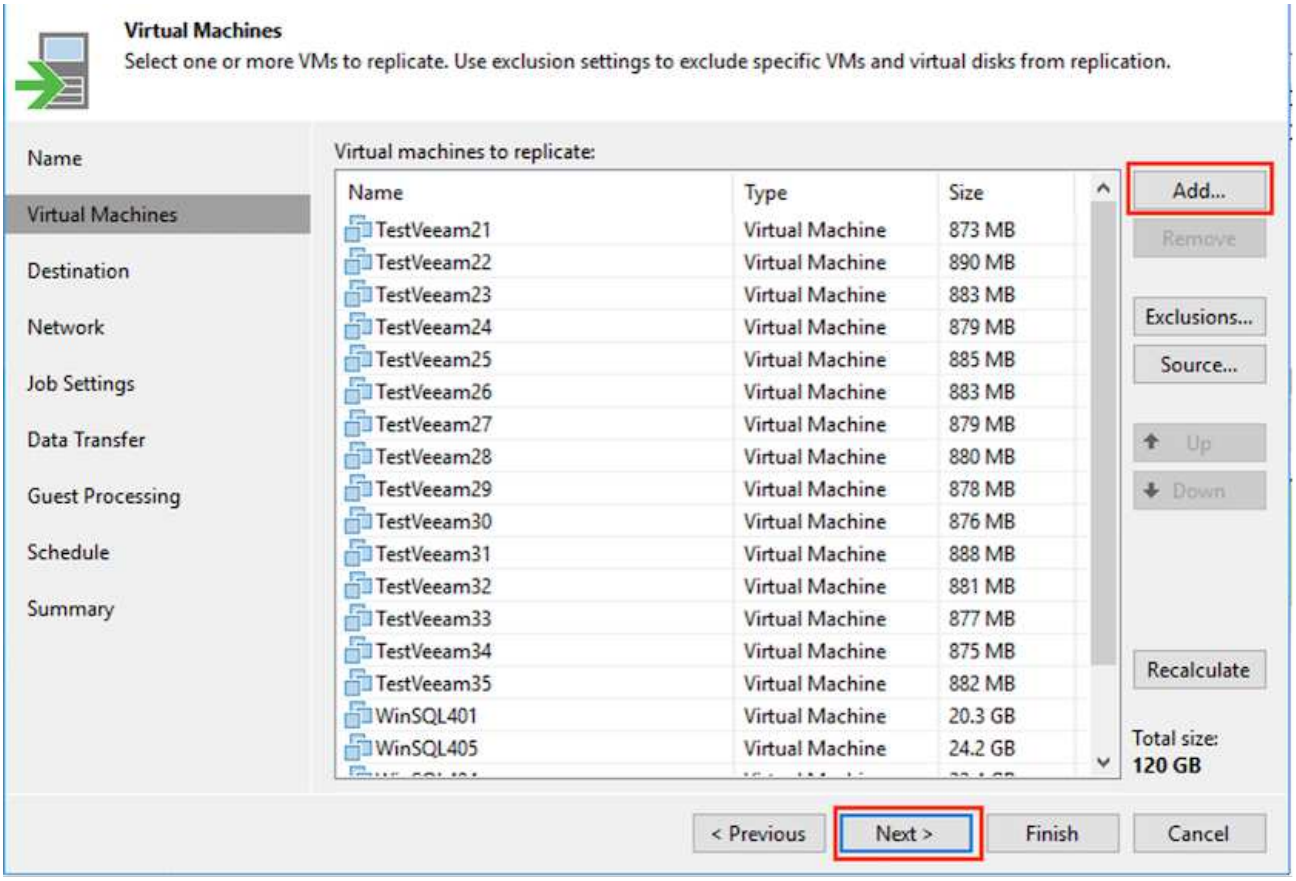
Veeam Backup & Replication sfrutta le funzionalità di snapshot di VMware vSphere e, durante la replica, Veeam Backup & Replication richiede a VMware vSphere di creare uno snapshot della VM. Lo snapshot della VM è la copia di una VM in un dato momento che include dischi virtuali, stato del sistema, configurazione e così via. Veeam Backup & Replication utilizza lo snapshot come origine dei dati per la replica.

Per replicare le VM, seguire i passaggi seguenti:

1. Aprire la console Veeam Backup & Replication.
2. Nella vista Home, seleziona Processo di replica > Macchina virtuale > VMware vSphere.
3. Specificare un nome per il lavoro e selezionare la casella di controllo avanzata appropriata. Fare clic su Avanti.
   - Selezionare la casella di controllo Replica seeding se la connettività tra locale e AWS ha una larghezza di banda limitata.
   - Selezionare la casella di controllo Rimappatura di rete (per siti AWS VMC con reti diverse) se i segmenti su VMware Cloud on AWS SDDC non corrispondono a quelli delle reti dei siti locali.
   - Se lo schema di indirizzamento IP nel sito di produzione locale è diverso dallo schema nel sito AWS VMC, selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso).

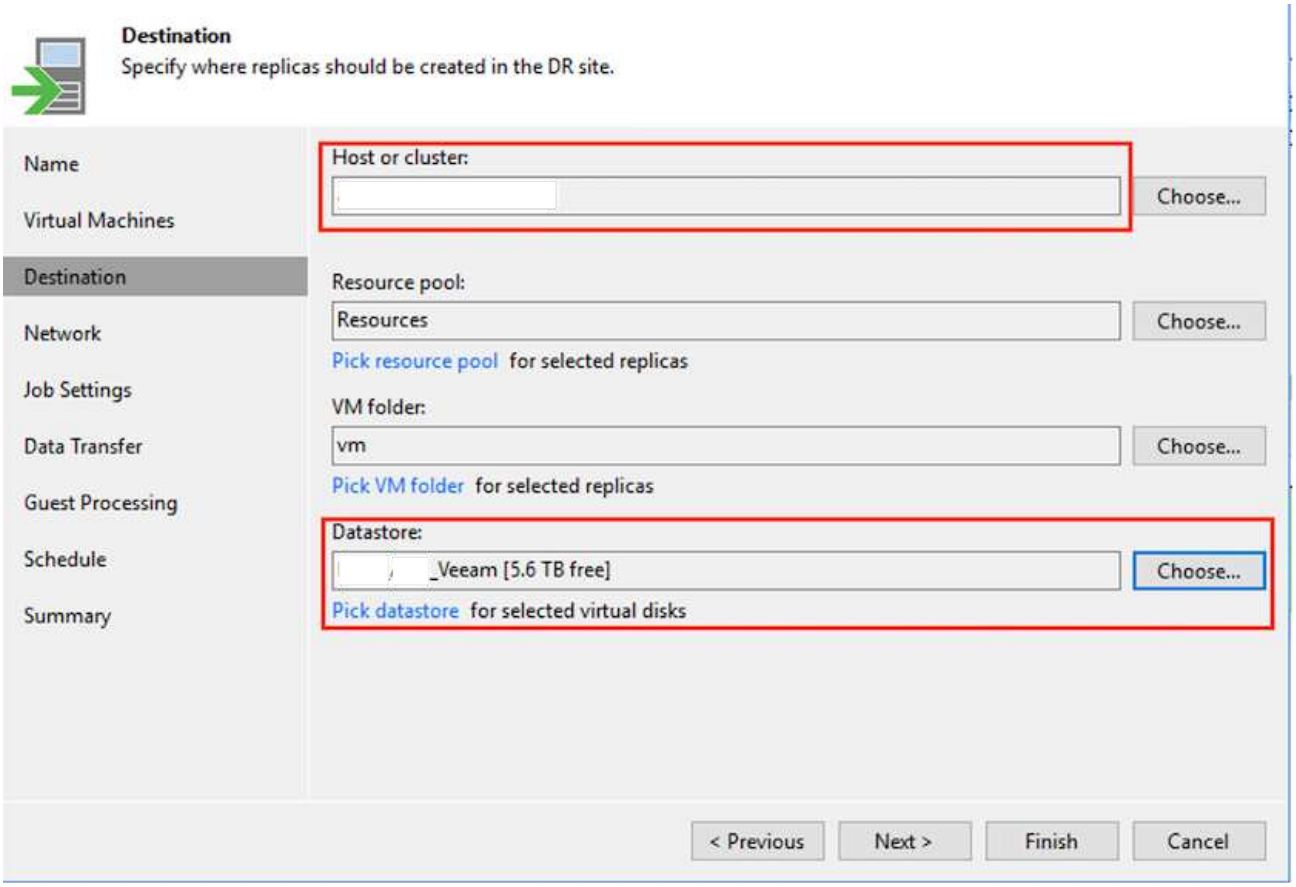


4. Selezionare le VM che devono essere replicate nel datastore FSx ONTAP collegato a VMware Cloud on AWS SDDC nel passaggio **Macchine virtuali**. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità disponibile del datastore vSAN. In un cluster di luci pilota, la capacità utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere replicato negli archivi dati FSx 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**.

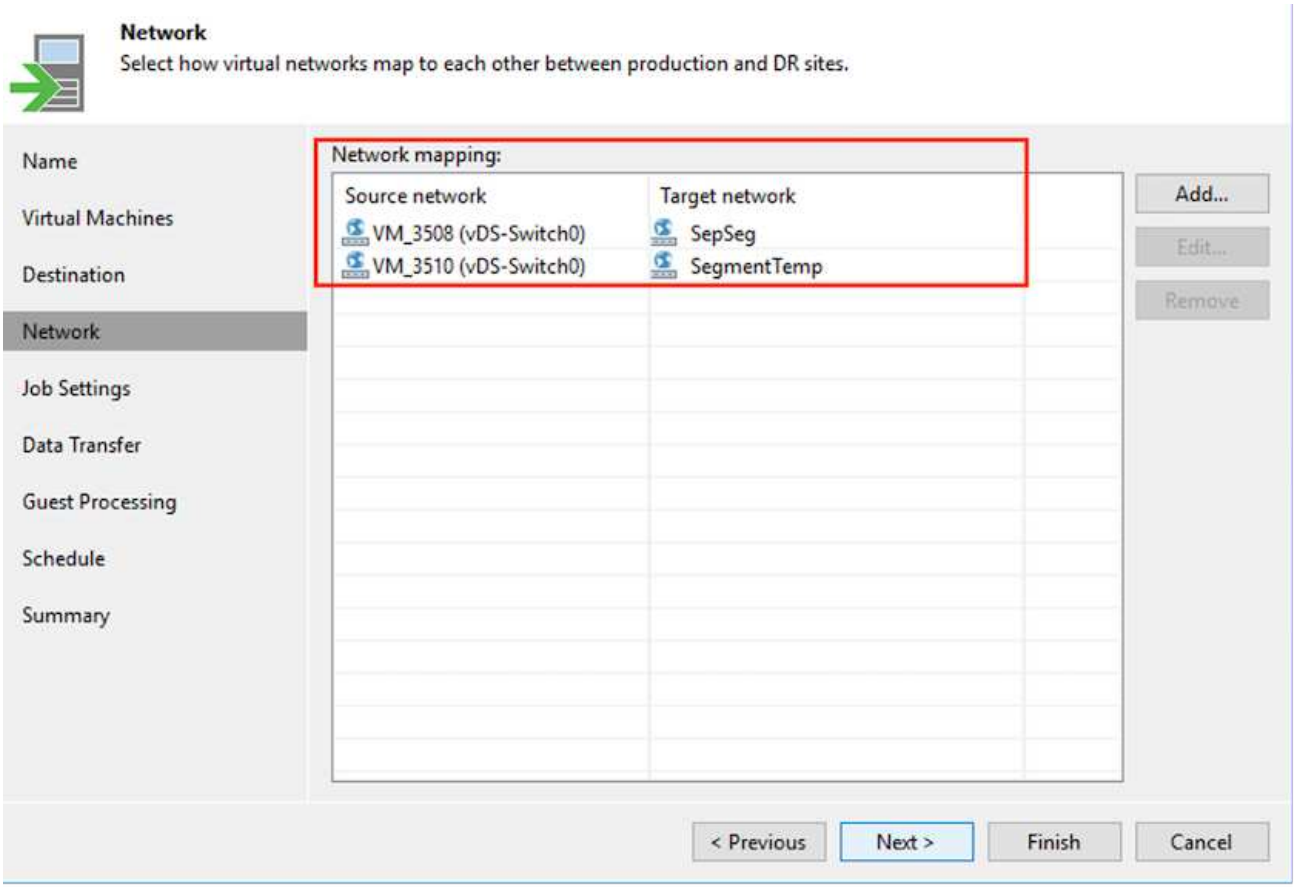


5. Successivamente, seleziona la destinazione come cluster/host VMware Cloud on AWS SDDC e il pool di risorse appropriato, la cartella VM e il datastore FSx ONTAP per le repliche VM. Quindi fare clic su

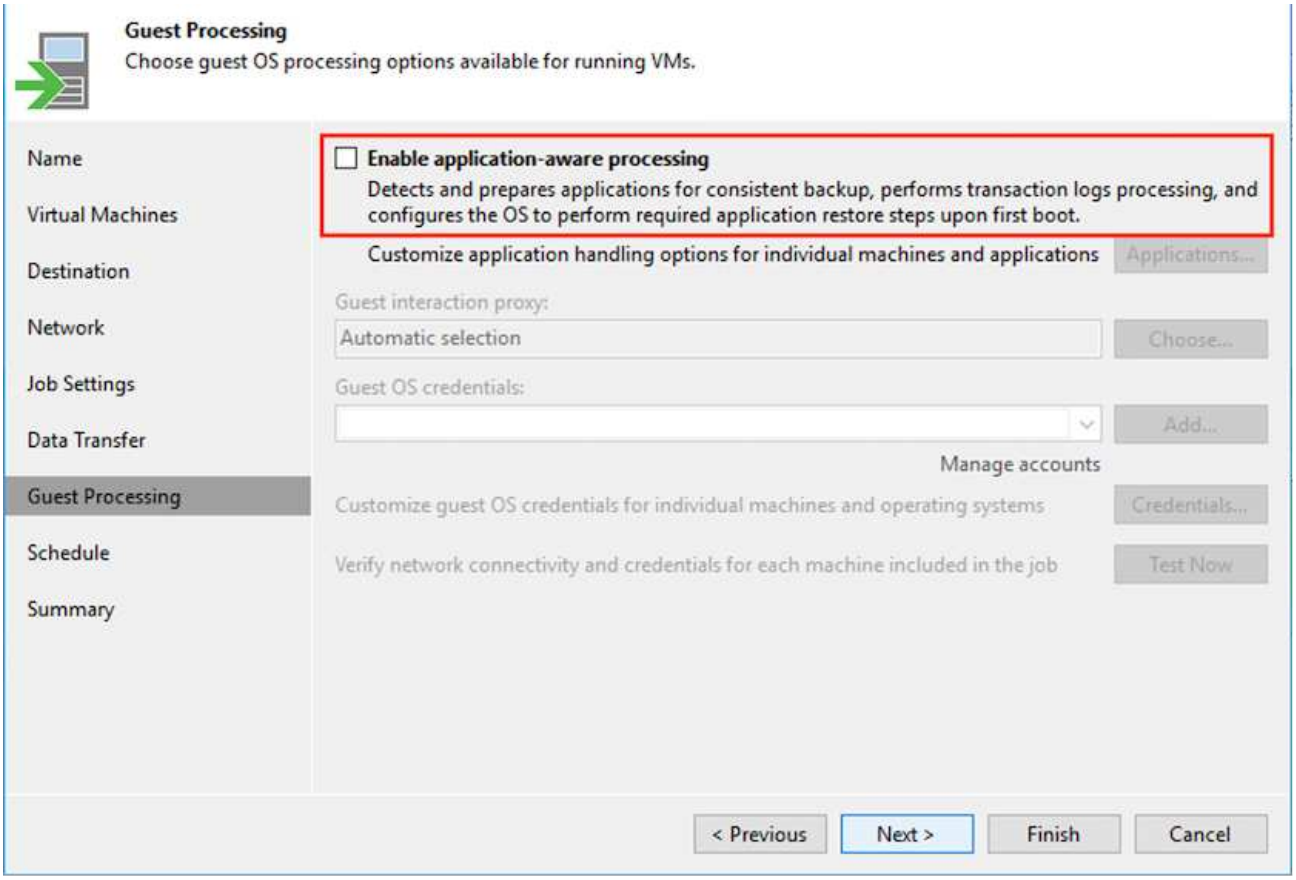
Avanti.



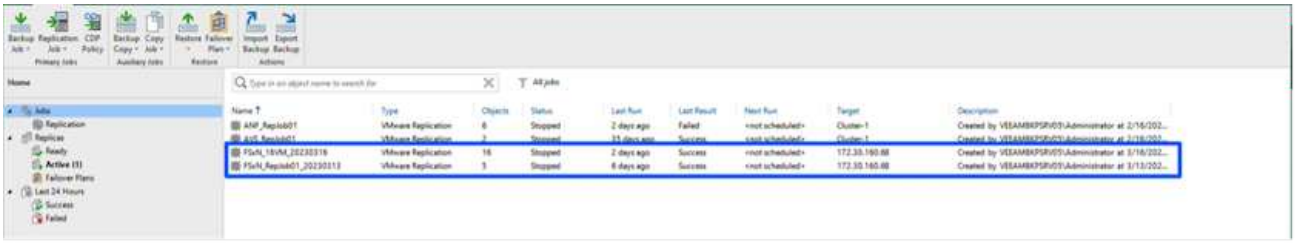
6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e quella di destinazione in base alle esigenze.



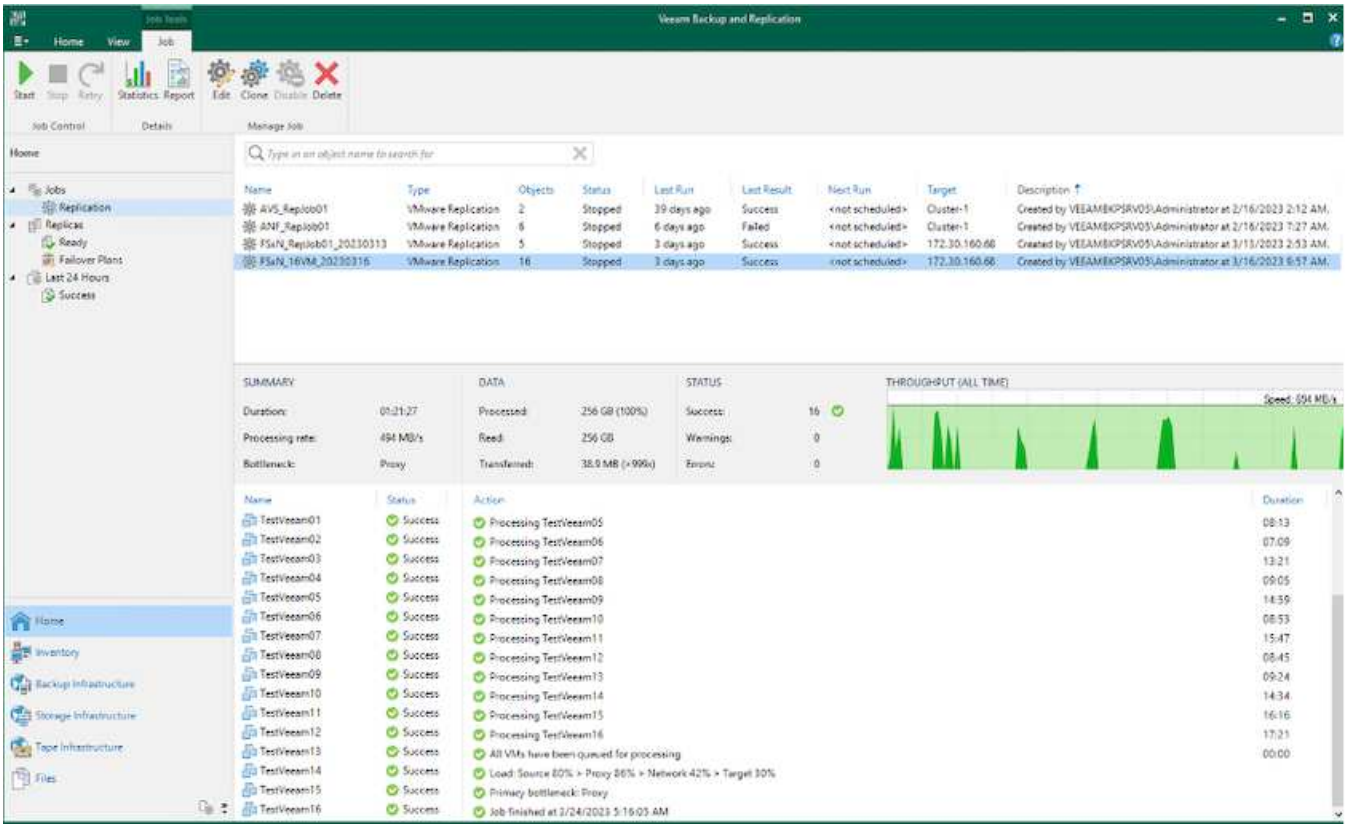
7. Nel passaggio **Impostazioni processo**, specificare il repository di backup in cui verranno archiviati i metadati per le repliche delle VM, i criteri di conservazione e così via.
8. Aggiorna i server proxy **Origine** e **Destinazione** nel passaggio **Trasferimento dati** e lascia la selezione **Automatica** (predefinita), mantieni selezionata l'opzione **Diretta** e fai clic su **Avanti**.
9. Nella fase **Elaborazione guest**, selezionare l'opzione **Abilita elaborazione basata sull'applicazione** in base alle esigenze. Fare clic su **Avanti**.



10. Selezionare la pianificazione della replica per eseguire il processo di replica regolarmente.
11. Nella fase **Riepilogo** della procedura guidata, rivedere i dettagli del processo di replica. Per avviare il processo subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il processo quando faccio clic su Fine**, altrimenti lasciare la casella di controllo deselezionata. Quindi fare clic su **Fine** per chiudere la procedura guidata.



Una volta avviato il processo di replica, le VM con il suffisso specificato verranno popolate sul cluster/host VMC SDDC di destinazione.



Per ulteriori informazioni sulla replica Veeam, fare riferimento a"Come funziona la replicazione" .

▼ Passaggio 2: creare un piano di failover

Una volta completata la replicazione o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire il failover per le VM dipendenti una alla volta o come gruppo automaticamente. Il piano di failover è il modello per l'ordine in cui vengono elaborate le VM, inclusi i ritardi di avvio. Il piano di failover aiuta anche a garantire che le VM dipendenti critiche siano già in esecuzione.

Per creare il piano, vai alla nuova sottosezione denominata Repliche e seleziona Piano di failover. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo momento e li utilizzerà per avviare le repliche delle VM.

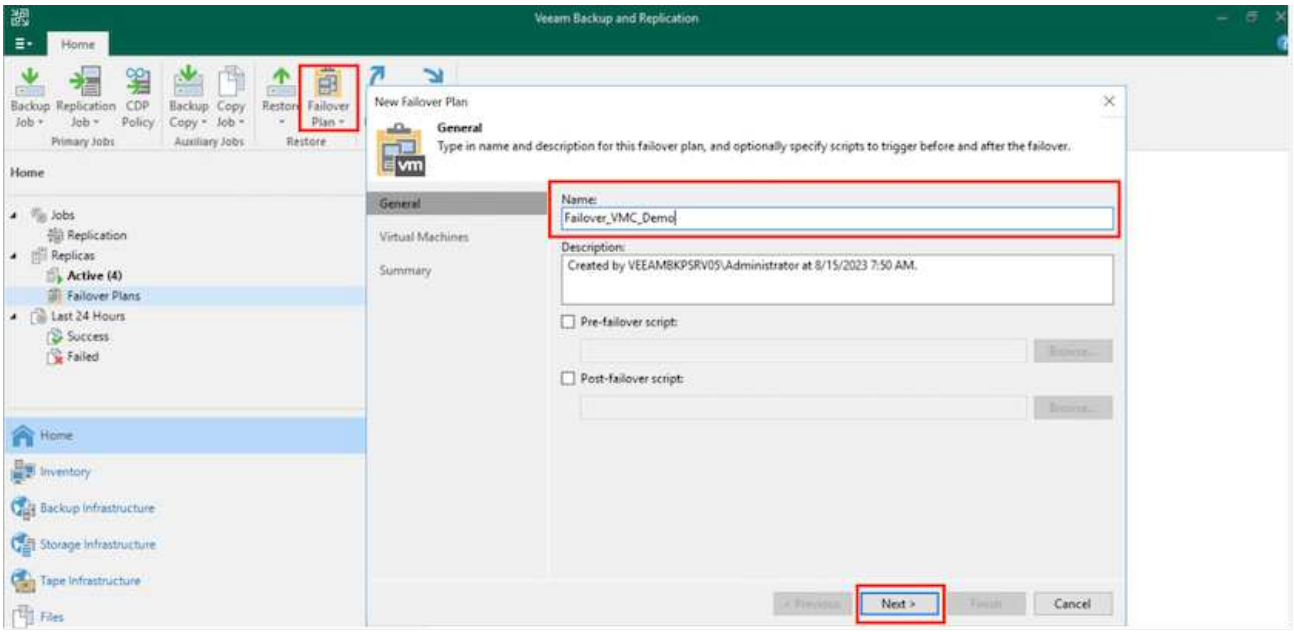
> ⓘ Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e quando le repliche delle VM sono nello stato Pronto.

> ⓘ Il numero massimo di VM che possono essere avviate simultaneamente durante l'esecuzione di un piano di failover è 10.

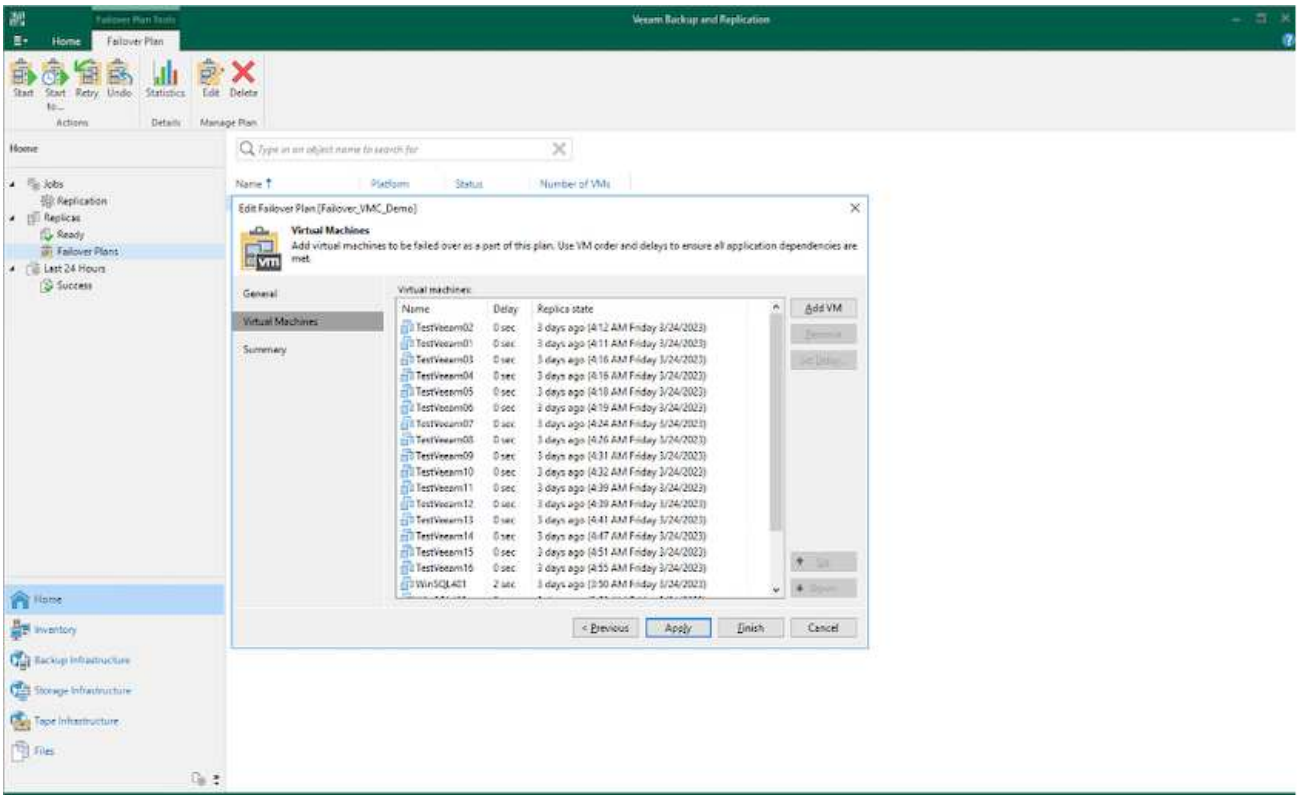
> ⓘ Durante il processo di failover, le VM di origine non verranno spente.

Per creare il **Piano di failover**, procedere come segue:

1. Nella vista Home, seleziona **Piano di failover > VMware vSphere**.
2. Successivamente, fornisci un nome e una descrizione al piano. È possibile aggiungere script pre e post-failover in base alle esigenze. Ad esempio, eseguire uno script per arrestare le VM prima di avviare le VM replicate.



3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze dell'applicazione.



Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento"Creazione di processi di replicazione" .

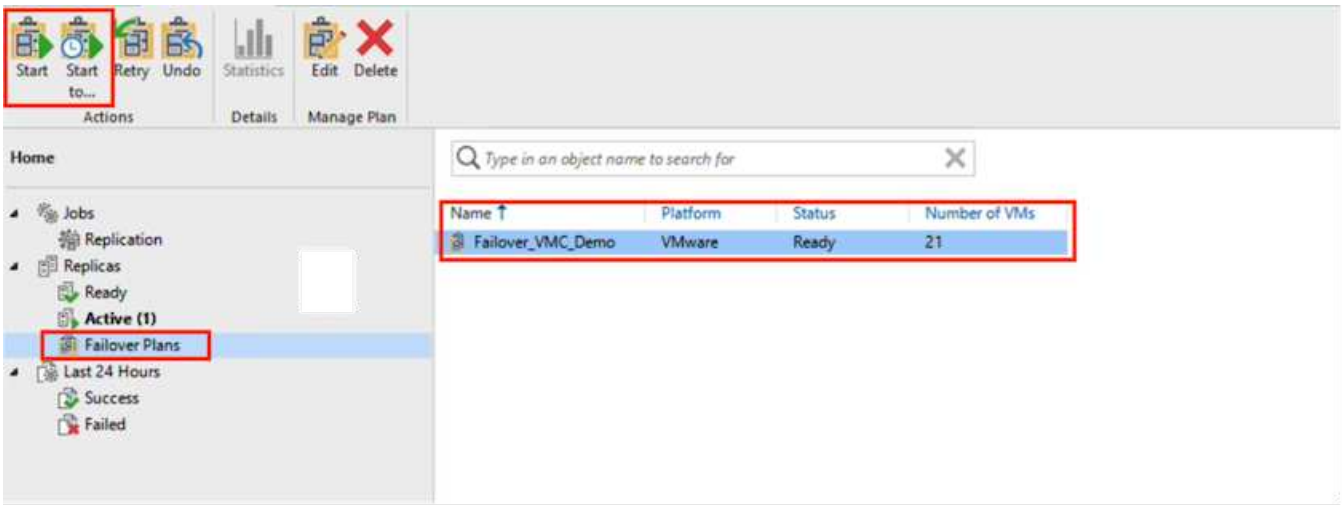
▼ **Passaggio 3: eseguire il piano di failover**

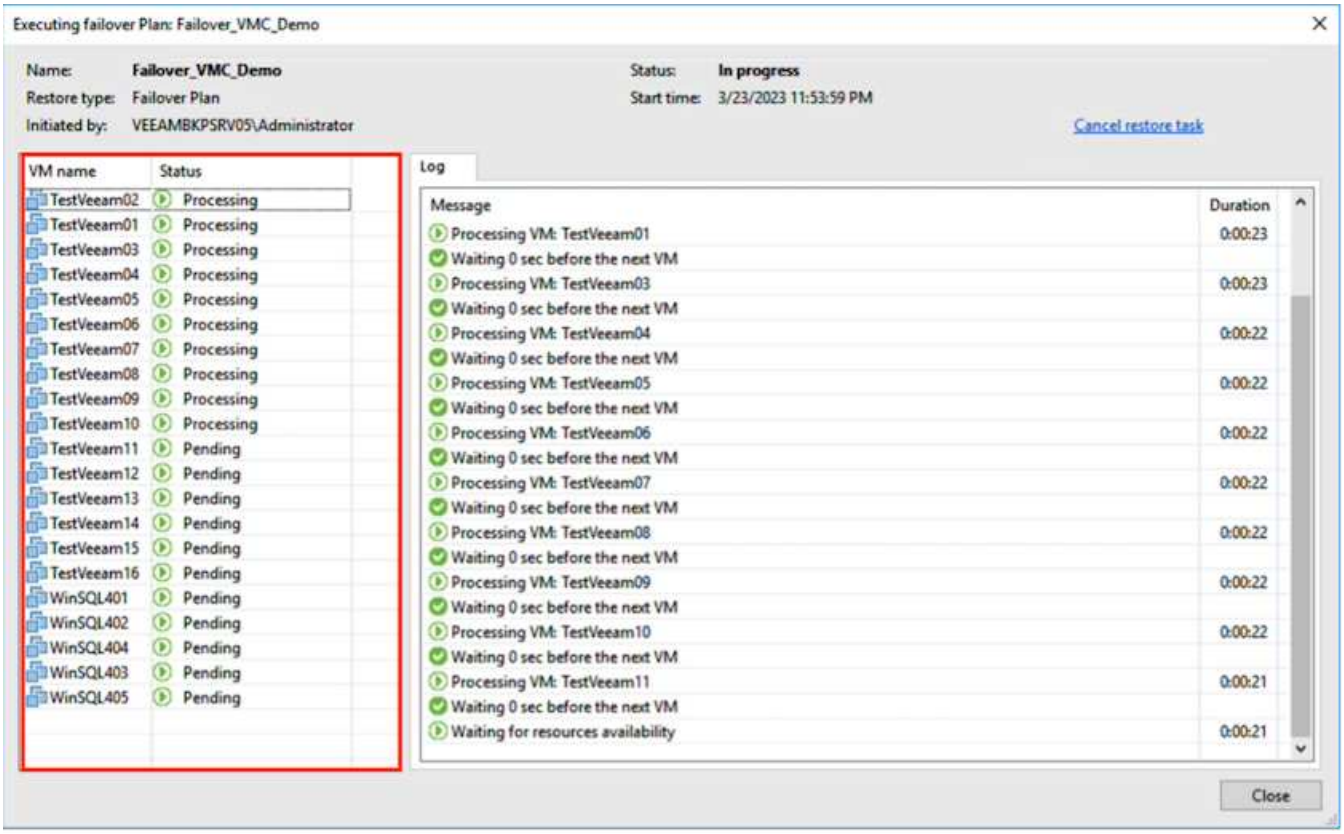
Durante il failover, la VM di origine nel sito di produzione viene commutata sulla sua replica nel sito di disaster recovery. Come parte del processo di failover, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e sposta tutte le attività di I/O dalla VM di origine alla sua replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni 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 alle normali operazioni.

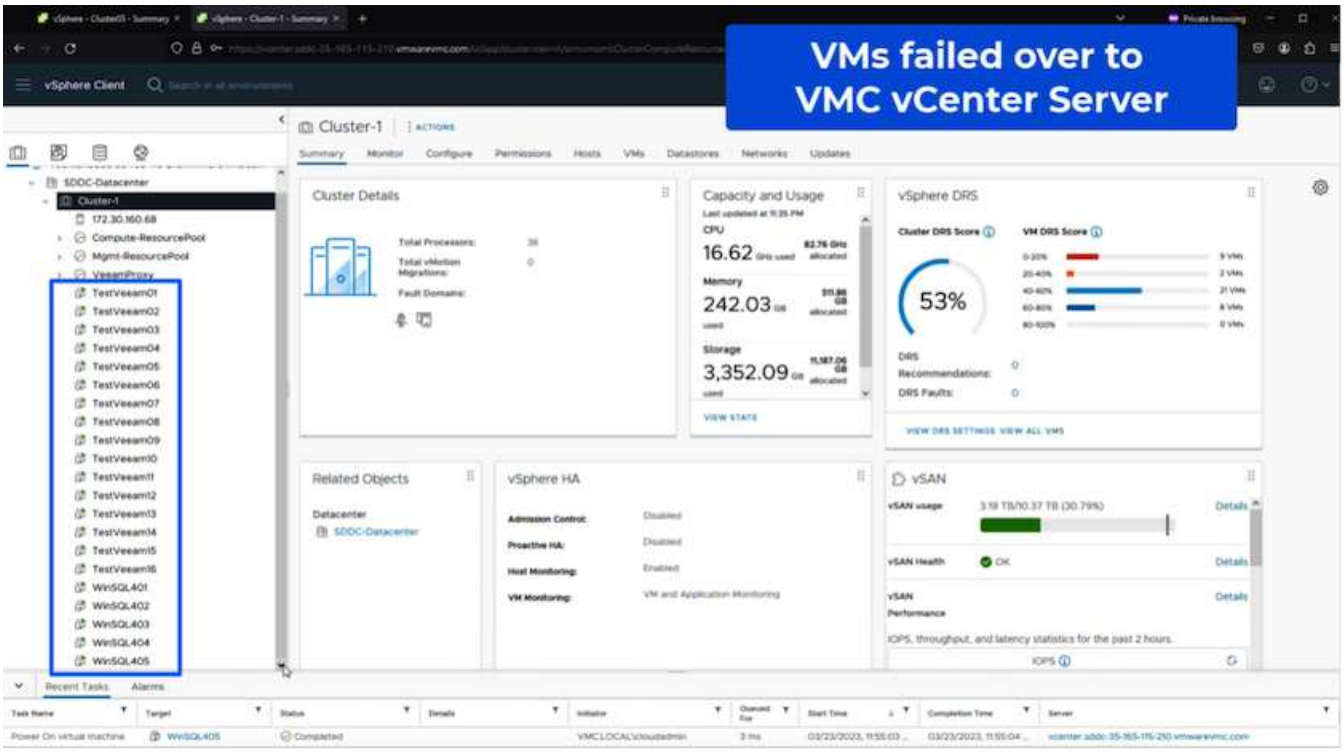
Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante le esercitazioni DR.

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 **Avvia**. Verrà eseguito il failover utilizzando i punti di ripristino più recenti delle repliche delle VM. Per eseguire il failover su punti di ripristino specifici delle repliche delle VM, selezionare **Avvia su**.

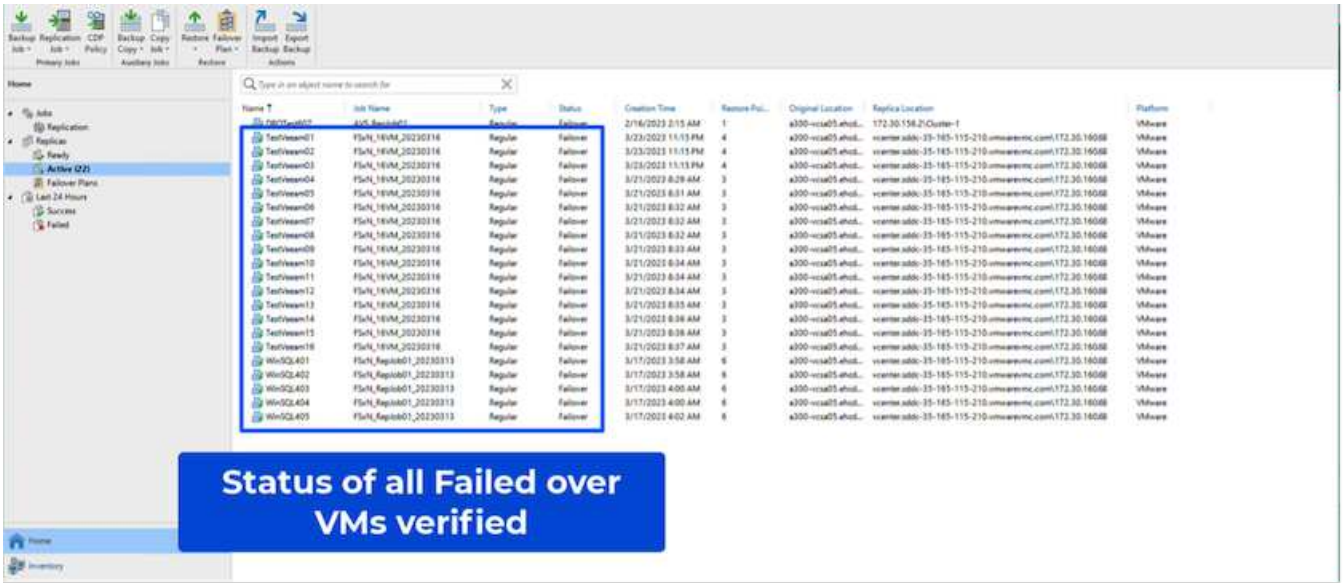




Lo stato della replica della VM cambia da Pronto a Failover e le VM verranno avviate sul cluster/host VMware Cloud on AWS SDDC di destinazione.



Una volta completato il failover, lo stato delle VM cambierà in "Failover".



Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine finché la sua replica non torna allo stato Pronto.

Per informazioni dettagliate sui piani di failover, fare riferimento a"Piani di failover" .

▼ **Fase 4: failback al sito di produzione**

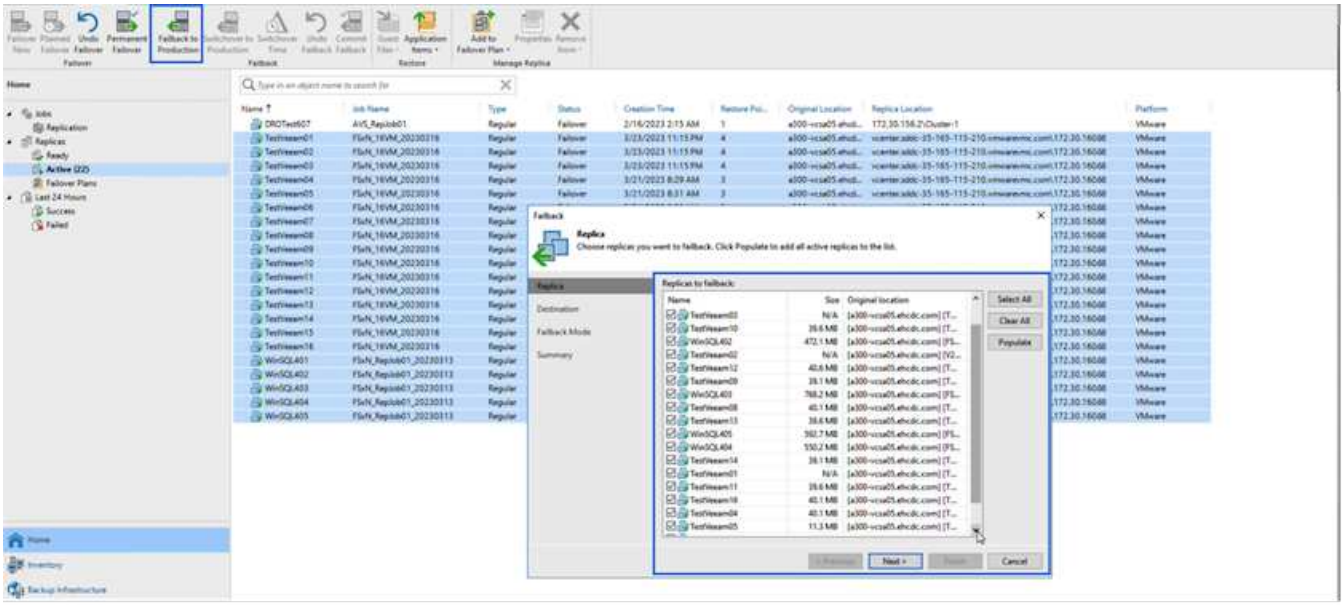
Quando il piano di failover è in esecuzione, viene considerato un passaggio intermedio e deve essere finalizzato in base ai requisiti. Le opzioni includono quanto segue:

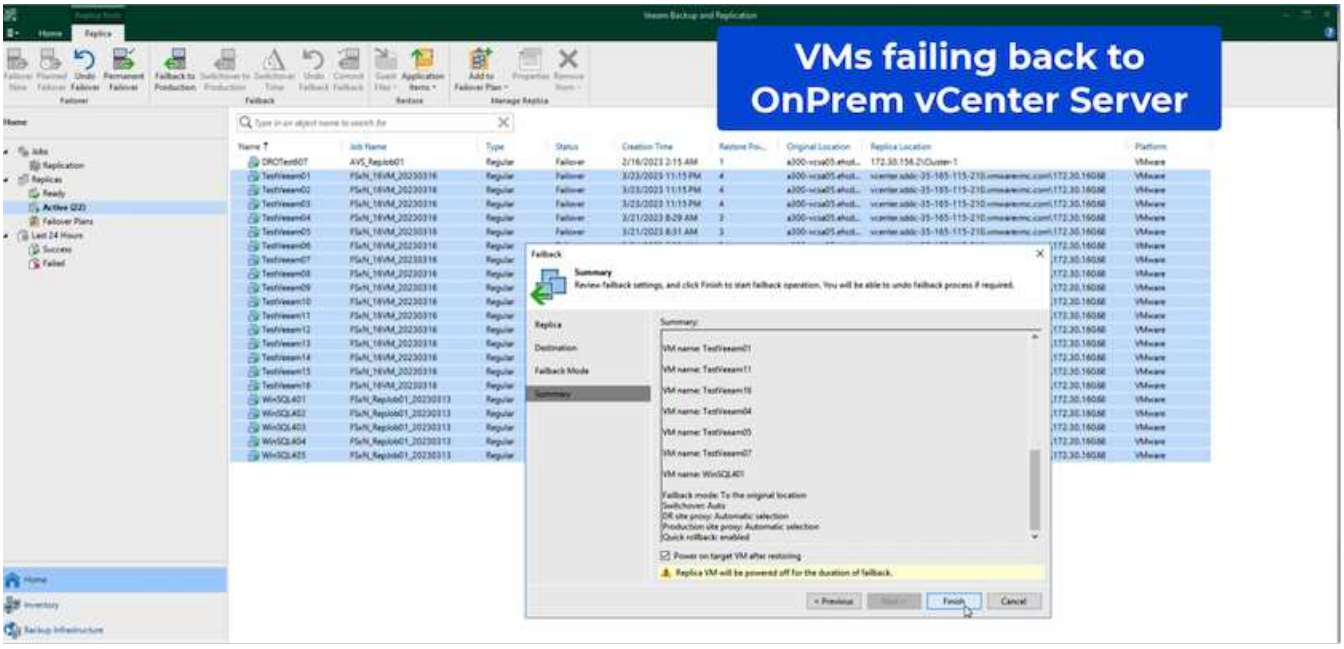
- **Failback in produzione**: torna alla VM originale e trasferisci tutte le modifiche apportate mentre la replica della VM era in esecuzione alla VM originale.

Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Selezionare **Commit failback** (una volta confermato che la VM originale funziona come previsto) oppure **Undo failback** per tornare alla replica della VM se la VM originale non funziona come previsto.

- **Annulla failover**: torna alla VM originale e ignora tutte le modifiche apportate alla replica della VM mentre era in esecuzione.
- **Failover permanente**: passa in modo permanente dalla VM originale a una replica della VM e utilizza questa replica come VM originale.

In questa demo è stato scelto il failback in produzione. Durante il passaggio Destinazione della procedura guidata è stato selezionato il failback sulla macchina virtuale originale ed è stata abilitata la casella di controllo "Accendi macchina virtuale dopo il ripristino".

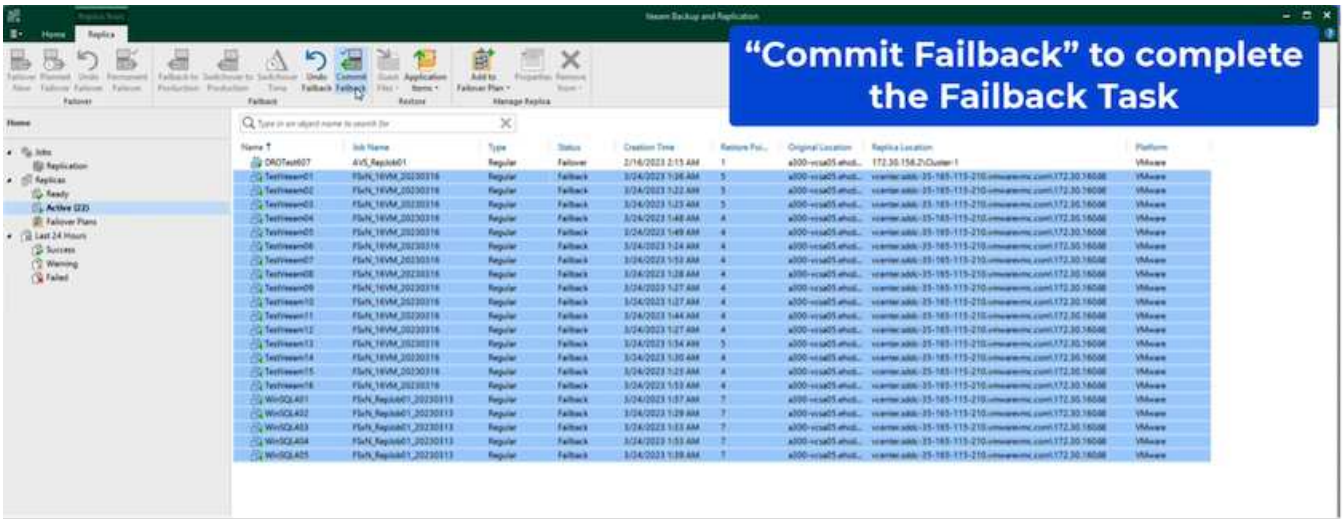


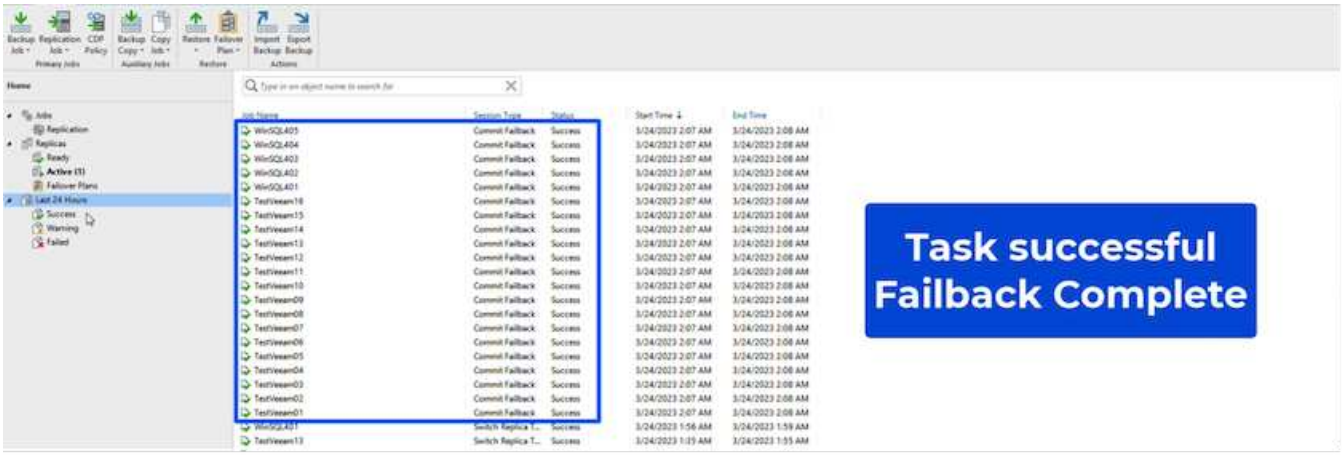


Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene

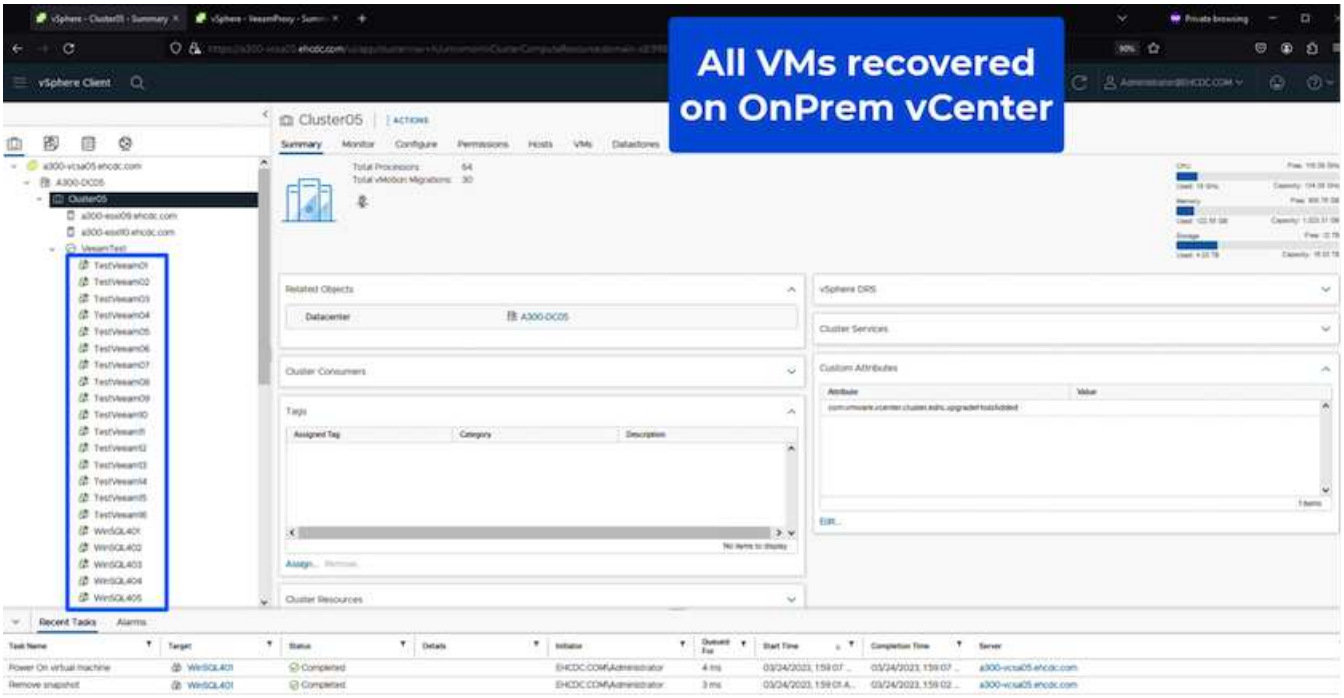
eseguito, conferma che le modifiche inviate alla VM sottoposta a failback (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività di replica per la VM di produzione.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per"Failover e failback per la replica" .





Una volta completato il failback in produzione, tutte le VM vengono ripristinate nel sito di produzione originale.



Conclusione

La funzionalità del datastore FSx ONTAP consente a Veeam o a qualsiasi strumento di terze parti convalidato di fornire una soluzione DR a basso costo utilizzando il cluster Pilot Light e senza dover creare un gran numero di host nel cluster solo per ospitare la copia della replica della VM. Ciò fornisce una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura e consente inoltre di riutilizzare i prodotti di backup esistenti internamente per soddisfare le esigenze di disaster recovery, consentendo così il disaster recovery basato su cloud tramite l'uscita dai data center di disaster recovery in sede. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, non esitate a seguire il video tutorial 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 utilizzando VMware HCX

Un caso d'uso comune per VMware Cloud (VMC) su Amazon Web Services (AWS), con il suo datastore NFS supplementare su Amazon FSx ONTAP, è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e fornisce vari metodi di migrazione per spostare macchine virtuali (VM) locali e i relativi dati, in esecuzione su qualsiasi datastore supportato da VMware, su datastore VMC, che includono datastore NFS supplementari su FSx ONTAP.

Panoramica: migrazione di macchine virtuali con VMware HCX, datastore supplementari FSx ONTAP e VMware Cloud

VMware HCX è principalmente una piattaforma di mobilità progettata per semplificare la migrazione dei carichi di lavoro, il ribilanciamento dei carichi di lavoro e la continuità aziendale tra i cloud. È incluso come parte di VMware Cloud su AWS e offre numerose modalità per migrare i carichi di lavoro e può essere utilizzato per operazioni di disaster recovery (DR).

Questo documento fornisce una guida dettagliata per l'implementazione e la configurazione di VMware HCX, inclusi tutti i suoi componenti principali, sia in locale che sul lato data center cloud, che consente vari meccanismi di migrazione delle VM.

Per maggiori informazioni, vedere "Guida utente VMware HCX" E "Checklist di installazione B - HCX con un ambiente di destinazione SDDC VMware Cloud su AWS" .

▼ gradini di alto livello

Questo elenco fornisce i passaggi principali 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 distribuire il programma di installazione OVA di HCX Connector nel vCenter Server locale.
3. Attiva HCX con una chiave di licenza.
4. Abbina VMware HCX Connector in locale a VMC HCX Cloud Manager.
5. Configurare il profilo di rete, il profilo di elaborazione e il service mesh.
6. (Facoltativo) Eseguire l'estensione di rete per estendere la rete ed evitare il re-IP.
7. Convalidare lo stato dell'appliance e assicurarsi che la migrazione sia possibile.
8. Migrare i carichi di lavoro delle VM.

▼ Prerequisiti

Prima di iniziare, assicurati che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, vedere "Preparazione per l'installazione" . Dopo aver soddisfatto i prerequisiti, inclusa la connettività, configurare e attivare HCX generando una chiave di licenza dalla VMware HCX Console in VMC. Dopo l'attivazione di HCX, il plug-in vCenter viene distribuito e può essere utilizzato per la gestione tramite vCenter Console.

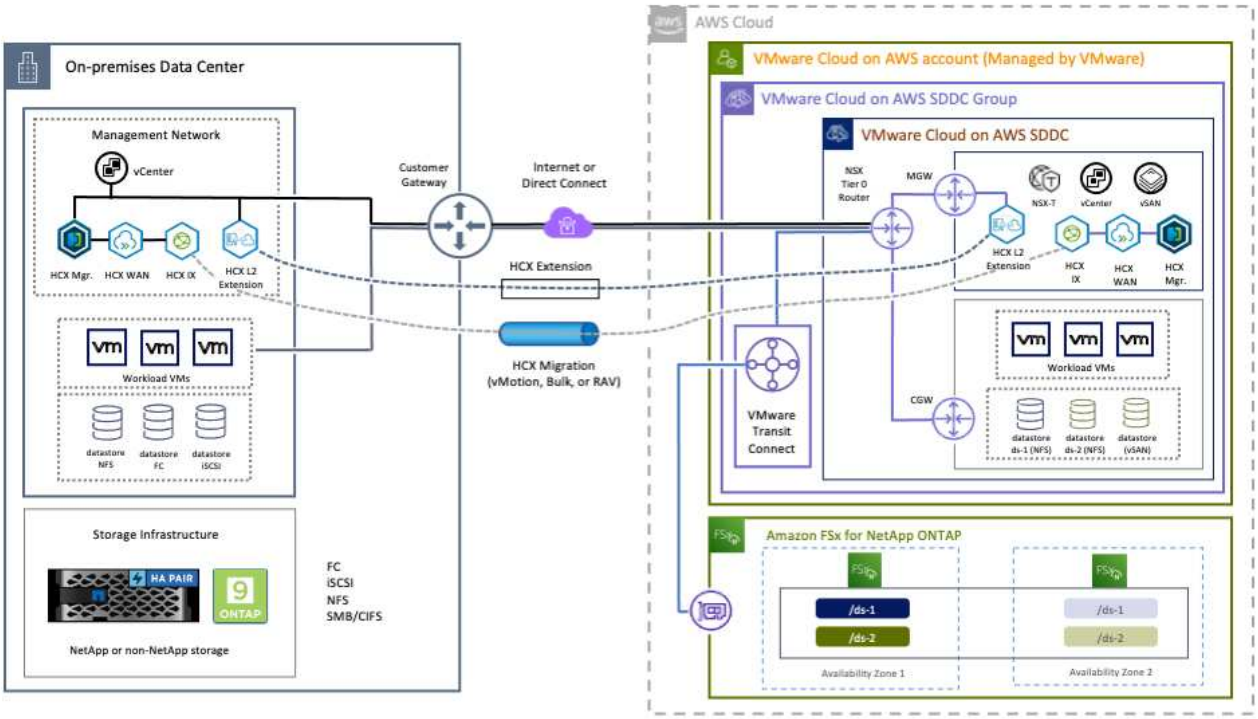
Prima di procedere con l'attivazione e la distribuzione di HCX, è necessario completare i seguenti passaggi di installazione:

1. Utilizzare un VMC SDDC esistente o crearne uno nuovo seguendo questa procedura"Collegamento NetApp" o questo "Collegamento VMware" .
2. Il percorso di rete dall'ambiente vCenter locale al VMC SDDC deve supportare la migrazione delle VM tramite vMotion.
3. Assicurati che il necessario "regole e porte del firewall" sono consentiti per il traffico vMotion tra il vCenter Server locale e il vCenter SDDC.
4. Il volume NFS FSx ONTAP deve essere montato come datastore supplementare nel VMC SDDC. Per collegare i datastore NFS al cluster appropriato, seguire i passaggi descritti in questo"Collegamento NetApp" o questo "Collegamento VMware" .

▼ Architettura di alto livello

A scopo di test, l'ambiente di laboratorio locale utilizzato per questa convalida è stato connesso tramite una VPN da sito a sito ad AWS VPC, che ha consentito la connettività locale ad AWS e a VMware cloud SDDC tramite gateway di transito esterno. Flussi di traffico di migrazione HCX ed estensione di rete su Internet tra l'ambiente locale e la destinazione cloud VMware SDDC. Questa architettura può essere modificata per utilizzare interfacce virtuali private Direct Connect.

L'immagine seguente illustra l'architettura di alto livello.



Distribuzione della soluzione

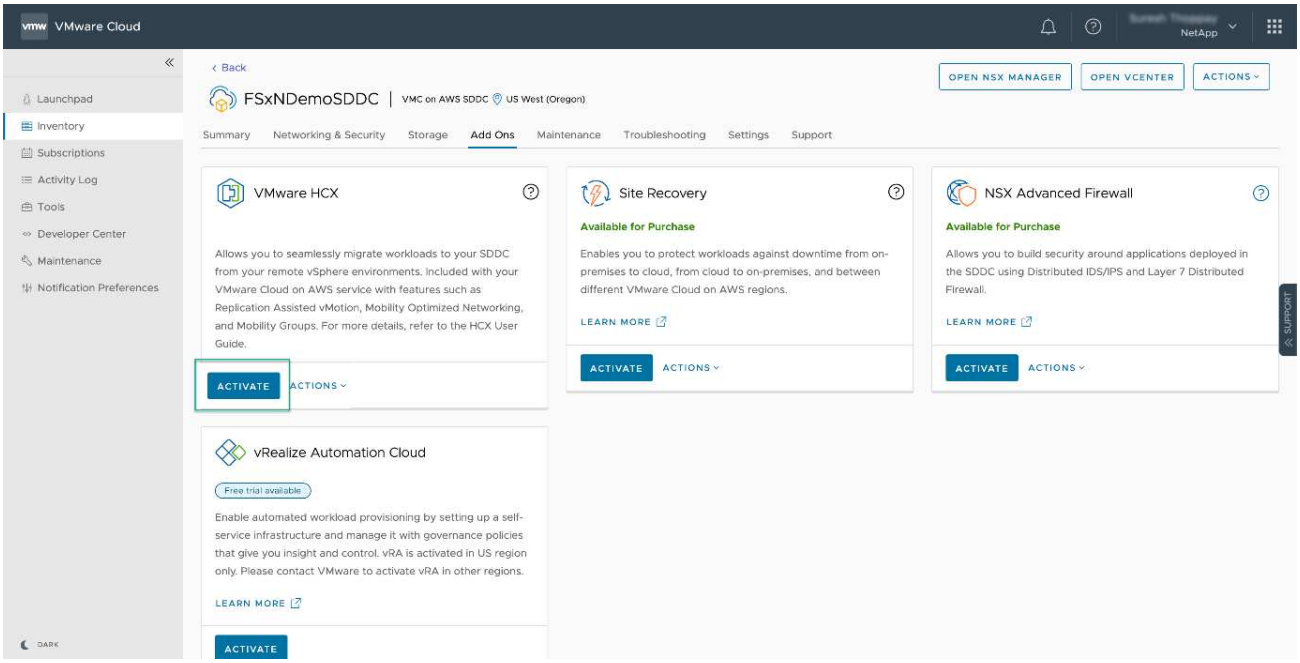
Per completare l'implementazione di questa soluzione, seguire la serie di passaggi:

▼ **Passaggio 1: attivare HCX tramite VMC SDDC utilizzando l'opzione Componenti aggiuntivi**

Per eseguire l'installazione, completare i seguenti passaggi:

1. Accedi 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 Visualizza dettagli su SDDC e selezionare la scheda Componenti aggiuntivi.
3. Fare clic su Attiva per VMware HCX.

Questo passaggio richiede fino a 25 minuti per essere completato.

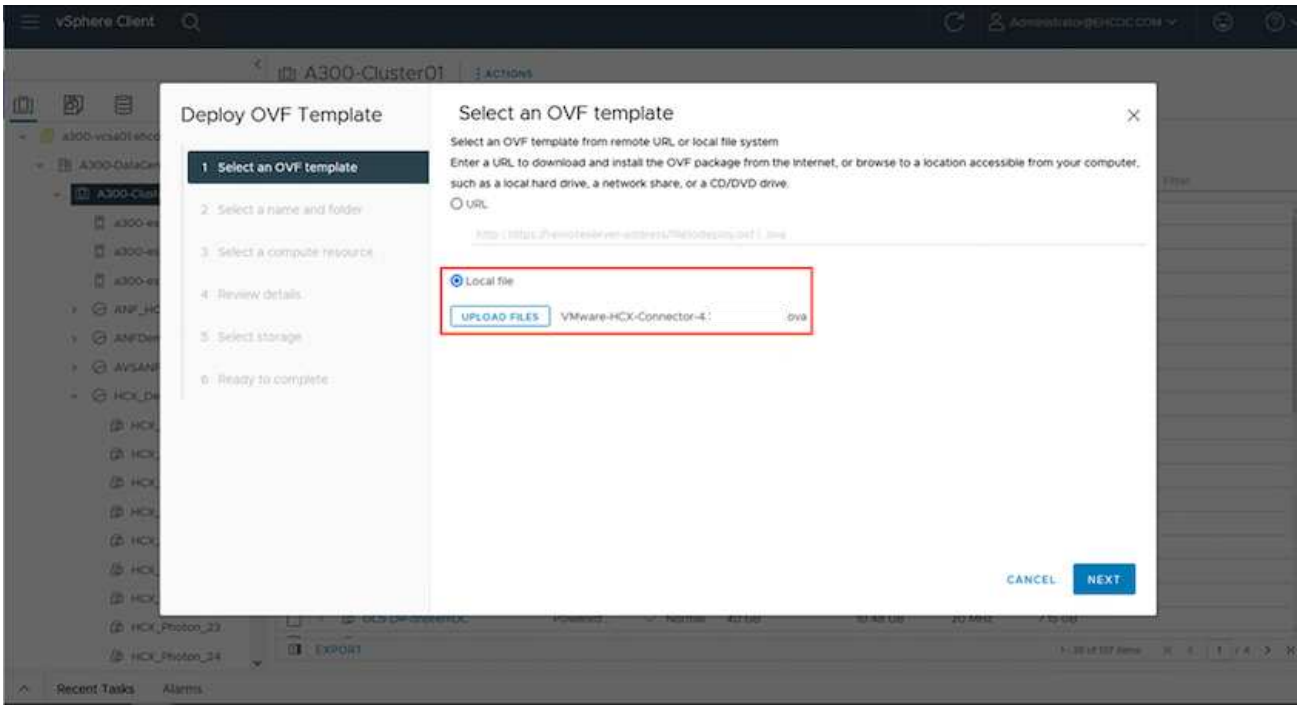


4. Una volta completata la distribuzione, convalidarla verificando che HCX Manager e i plug-in associati siano disponibili in vCenter Console.
5. Creare i firewall Management Gateway appropriati per aprire le porte necessarie per accedere a HCX Cloud Manager. HCX Cloud Manager è ora pronto per le operazioni HCX.

▼ **Passaggio 2: distribuire l'OVA del programma di installazione nel vCenter Server locale**

Per consentire al connettore locale di comunicare con HCX Manager in VMC, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente locale.

1. Dalla console VMC, accedere alla dashboard HCX, andare ad Amministrazione e selezionare la scheda Aggiornamento sistemi. Fare clic su Richiedi un collegamento per il download dell'immagine OVA del connettore HCX.
2. Dopo aver scaricato HCX Connector, distribuire l'OVA nel vCenter Server locale. Fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Distribuisci modello OVF.

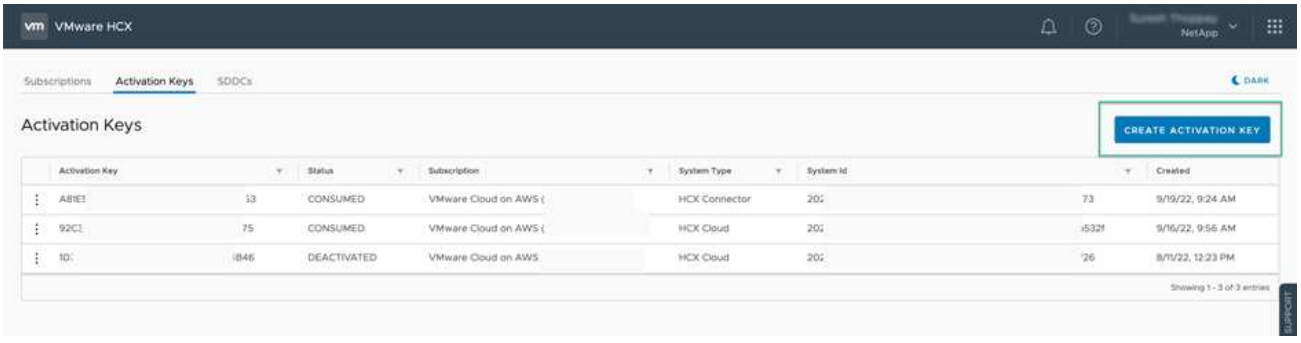


3. Immettere le informazioni richieste nella procedura guidata Distribuisci modello OVF, fare clic su Avanti e quindi su Fine per distribuire VMware HCX Connector OVA.
4. Accendere manualmente l'appliance virtuale. Per istruzioni dettagliate, consultare "Guida utente VMware HCX" .

▼ **Passaggio 3: Attiva HCX Connector con la chiave di licenza**

Dopo aver distribuito VMware HCX Connector OVA in locale e avviato l'appliance, completare i seguenti passaggi per attivare HCX Connector. Generare la chiave di licenza dalla VMware HCX Console su VMC e immettere la licenza durante la configurazione di VMware HCX Connector.

1. Dalla VMware Cloud Console, vai su Inventario, seleziona SDDC e fai clic su Visualizza dettagli. Nella scheda Componenti aggiuntivi, nel riquadro VMware HCX, fare clic su Apri HCX.
2. Nella scheda Chiavi di attivazione, fare clic su Crea chiave di attivazione. Selezionare HCX Connector come Tipo di sistema e fare clic su Conferma per generare la chiave. Copia la chiave di attivazione.



Per ogni HCX Connector distribuito in locale è richiesta una chiave separata.

3. Accedi al VMware HCX Connector locale all'indirizzo `"https://hcxconnectorIP:9443"` utilizzando le credenziali di amministratore.

Utilizzare la password definita durante la distribuzione OVA.

4. Nella sezione Licenze, inserisci la chiave di attivazione copiata dal passaggio 2 e fai clic su Attiva.

Affinché l'attivazione venga completata correttamente, l'HCX Connector locale deve disporre di accesso a Internet.

5. In Posizione datacenter, specificare la posizione desiderata per l'installazione di VMware HCX Manager in locale. Fare clic su Continua.
6. In Nome sistema, aggiorna il nome e fai clic su Continua.
7. Selezionare Sì e poi Continua.
8. In Connetti il tuo vCenter, fornisci l'indirizzo IP o il nome di dominio completo (FQDN) e le credenziali per il vCenter Server, quindi fai clic su Continua.

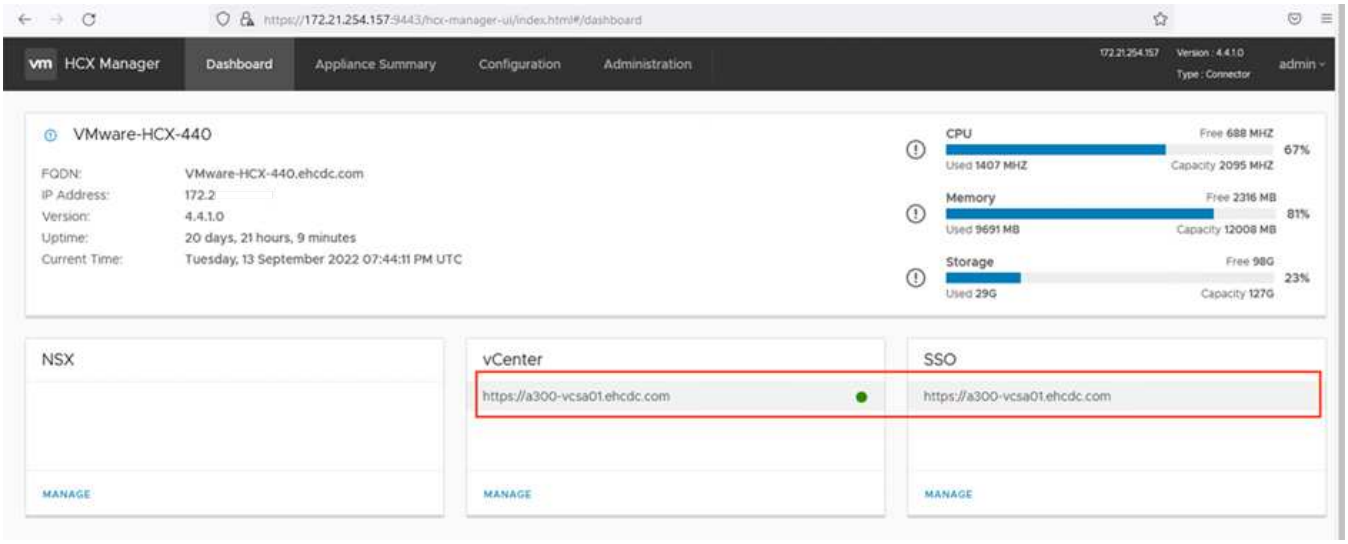
Utilizzare l'FQDN per evitare problemi di comunicazione in seguito.

9. In Configura SSO/PSC, fornisci l'FQDN o l'indirizzo IP del Platform Services Controller e fai clic su Continua.

Immettere l'indirizzo IP o il nome di dominio completo (FQDN) del vCenter Server.

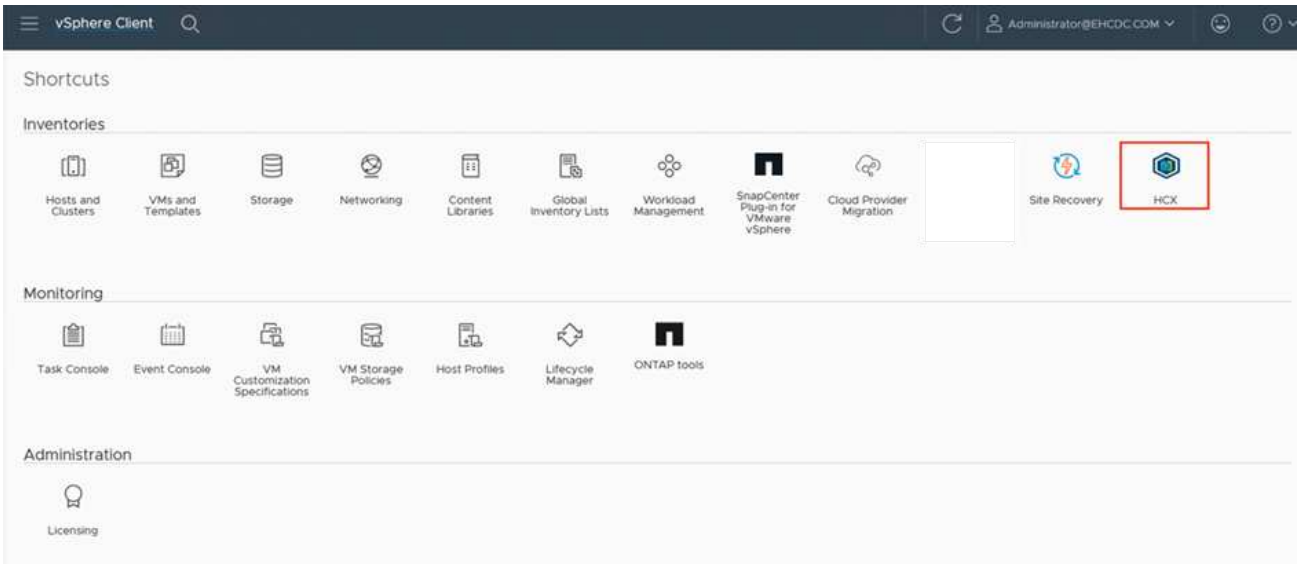
10. Verificare che le informazioni siano state immesse correttamente e fare clic su Riavvia.
11. Al termine, vCenter Server viene visualizzato in verde. Sia vCenter Server che SSO devono avere i parametri di configurazione corretti, che dovrebbero essere gli stessi della pagina precedente.

Questo processo dovrebbe richiedere circa 10-20 minuti affinché il plug-in venga aggiunto al vCenter Server.

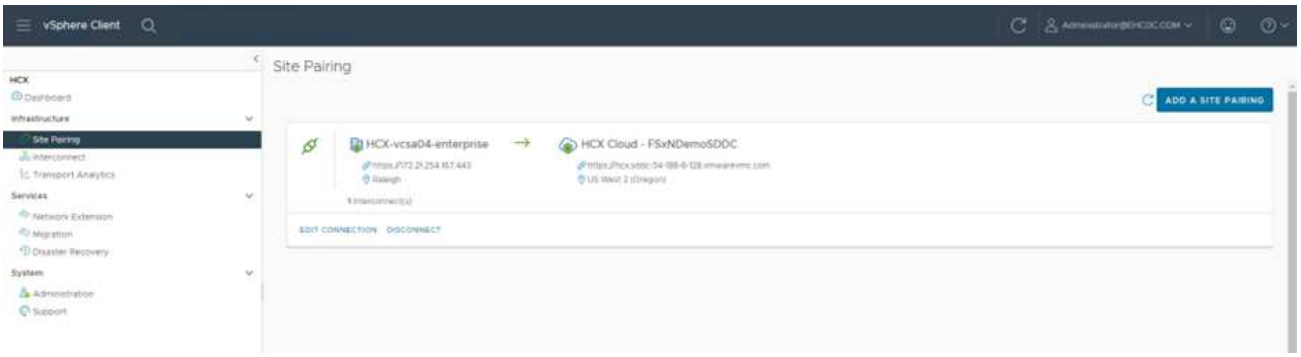


▼ **Passaggio 4: associare VMware HCX Connector on-premise a VMC HCX Cloud Manager**

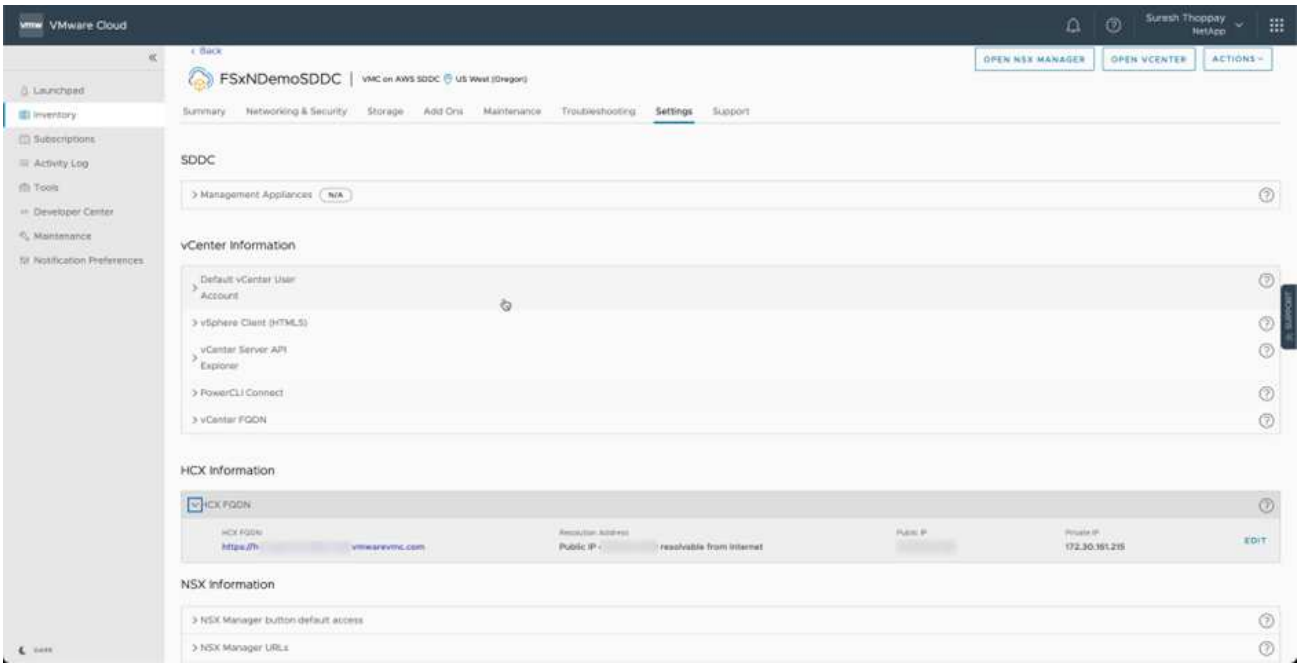
1. Per creare una coppia di siti tra il vCenter Server locale e il VMC SDDC, accedere al vCenter Server locale e accedere al plug-in HCX vSphere Web Client.

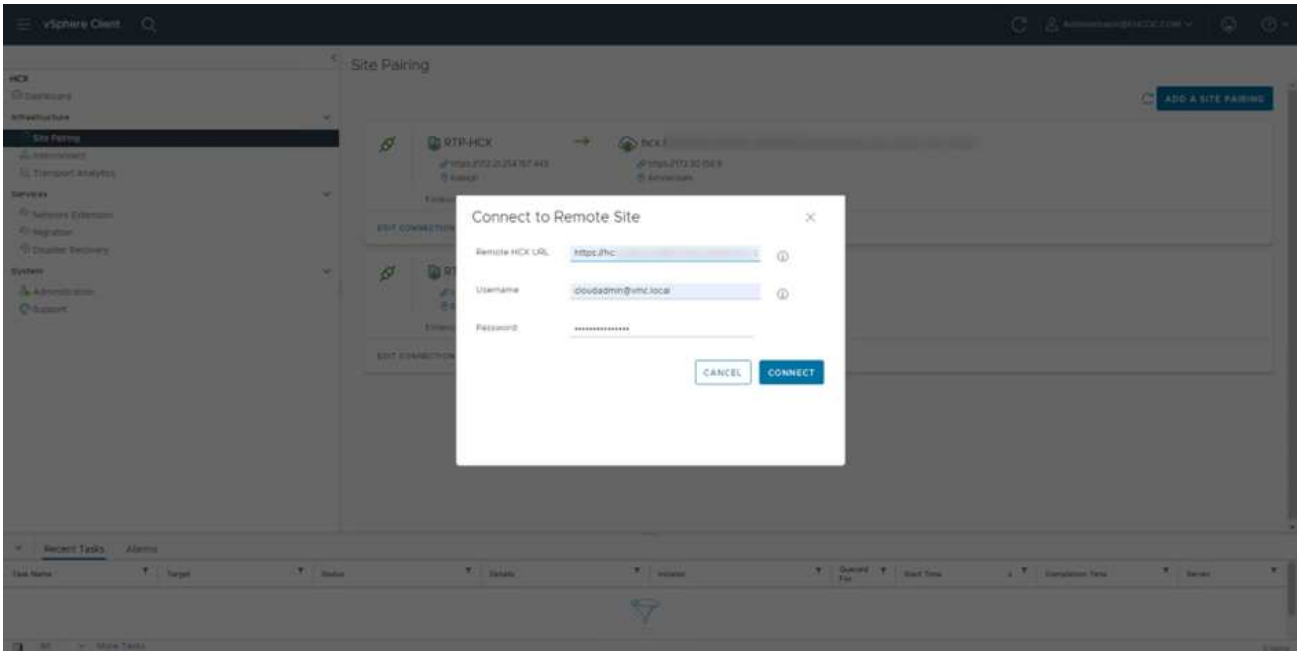


2. In Infrastruttura, fare clic su Aggiungi un'associazione di siti. Per autenticare il sito remoto, immettere l'URL o l'indirizzo IP di VMC HCX Cloud Manager e le credenziali per il ruolo CloudAdmin.



Le informazioni HCX possono essere recuperate dalla pagina Impostazioni SDDC.





3. Per avviare l'associazione del sito, fare clic su Connetti.

> VMware HCX Connector deve essere in grado di comunicare con l'IP di HCX Cloud Manager tramite la porta 443.

4. Dopo aver creato l'associazione, l'associazione del sito appena configurata è disponibile sulla dashboard HCX.

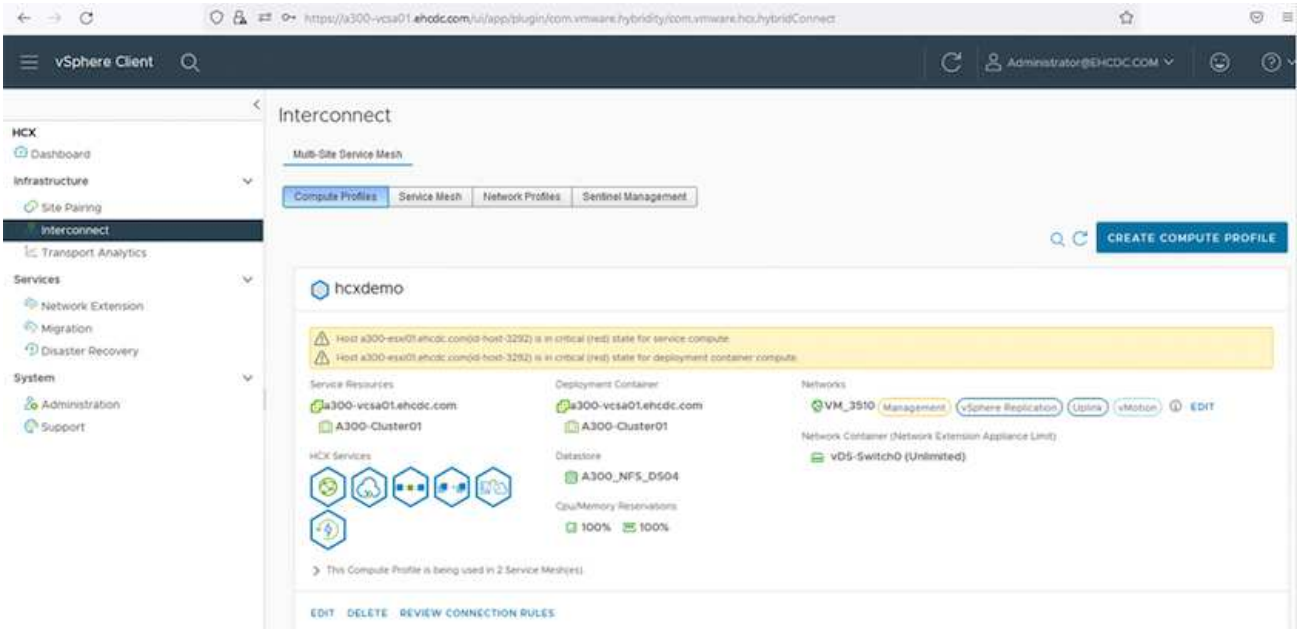
▼ **Passaggio 5: configurare il profilo di rete, il profilo di elaborazione e il service mesh**

L'appliance VMware HCX Interconnect (HCX-IX) fornisce funzionalità di tunneling sicuro su Internet e connessioni private al sito di destinazione che consentono funzionalità di replica e basate su vMotion. L'interconnessione fornisce crittografia, ingegneria del traffico e una SD-WAN. Per creare l'appliance di interconnessione HCI-IX, completare i seguenti passaggi:

1. In Infrastruttura, seleziona Interconnessione > Multi-Site Service Mesh > Profili di calcolo > Crea profilo di calcolo.

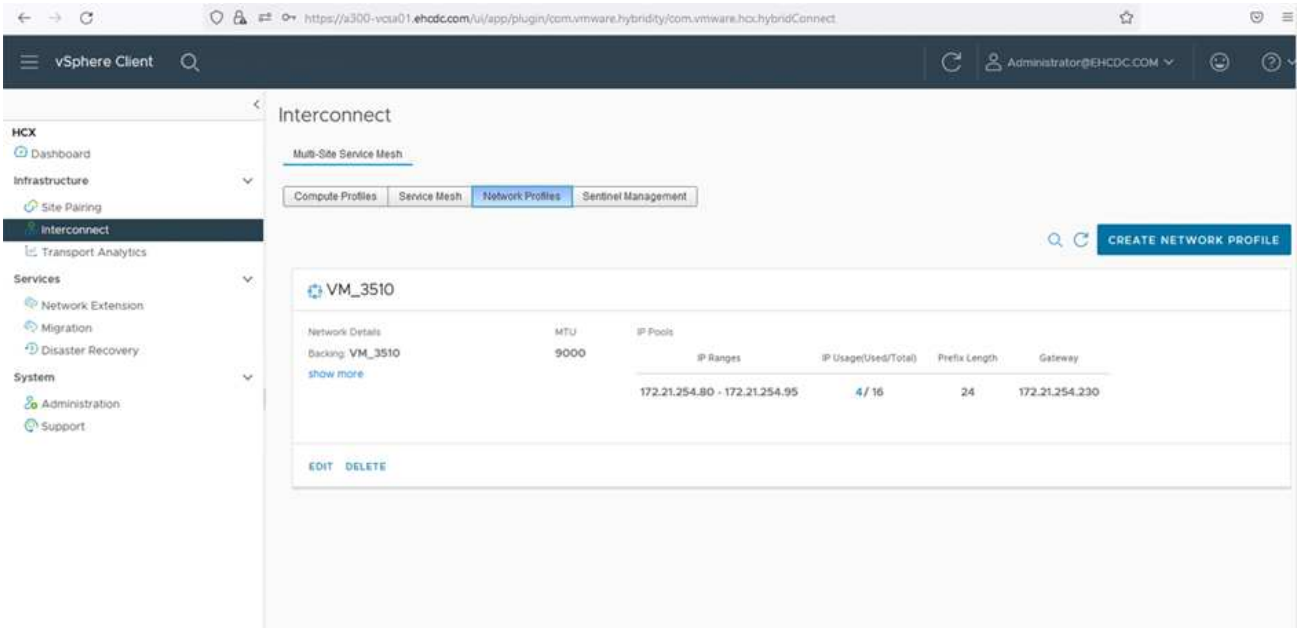
> I profili di calcolo contengono i parametri di calcolo, archiviazione e distribuzione di rete necessari per distribuire un'appliance virtuale di interconnessione. Specificano inoltre quale parte del data center VMware sarà accessibile al servizio HCX.

Per istruzioni dettagliate, vedere "Creazione di un profilo di calcolo" .



2. Dopo aver creato il profilo di calcolo, creare il profilo di rete selezionando Multi-Site Service Mesh > 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 i suoi dispositivi virtuali.

> Per farlo saranno necessari due o più indirizzi IP. Questi indirizzi IP verranno assegnati dalla rete di gestione agli appliance virtuali.



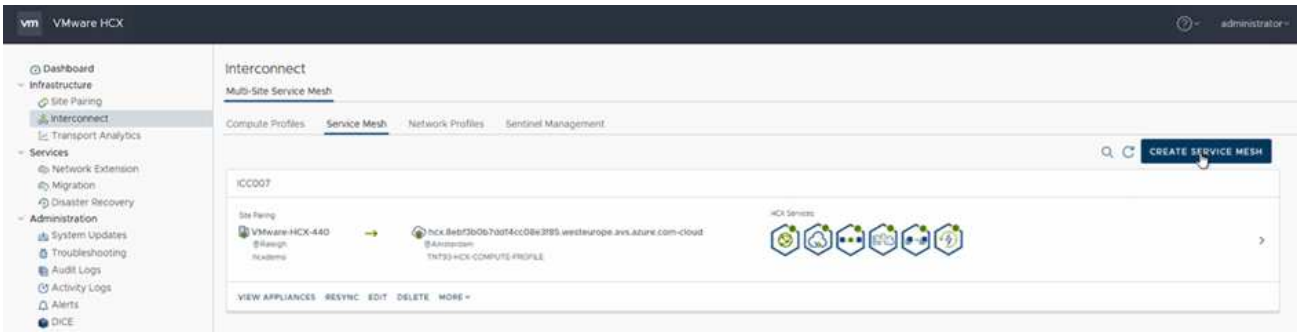
Per istruzioni dettagliate, vedere "Creazione di un profilo di rete" .

> Se ci si connette tramite una SD-WAN tramite Internet, è necessario riservare IP pubblici nella sezione Rete e sicurezza.

4. Per creare una service mesh, seleziona la scheda Service Mesh nell'opzione Interconnessione e

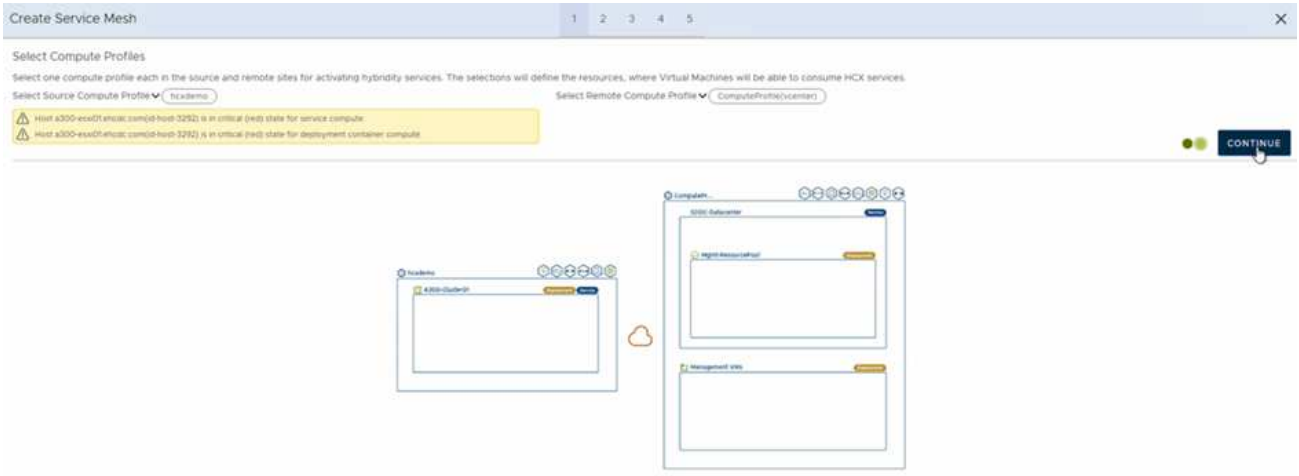
seleziona i siti SDDC locali e VMC.

Il service mesh stabilisce una coppia di profili di rete e di elaborazione locale e remota.

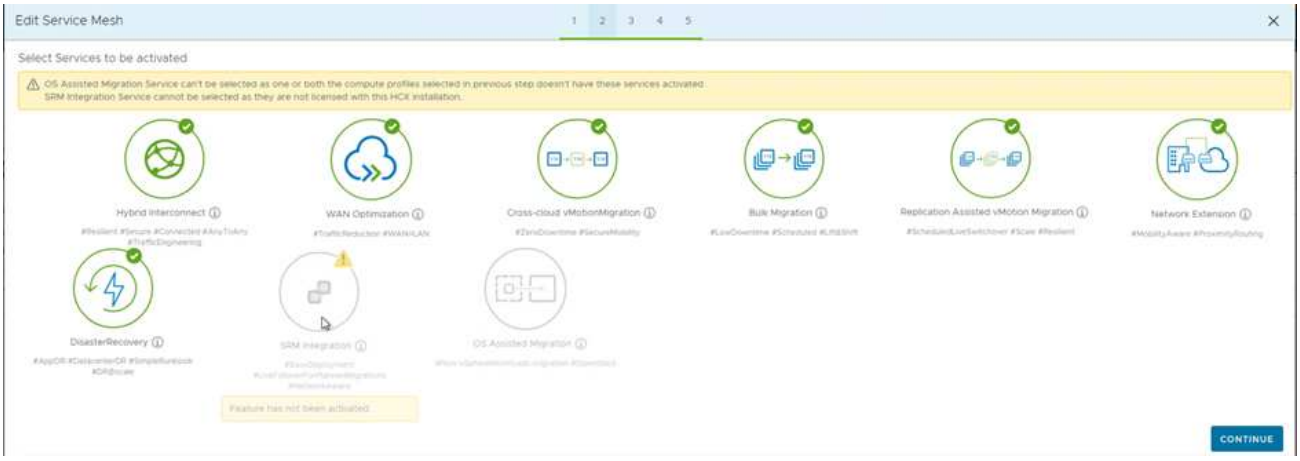


Parte di questo processo prevede l'implementazione di appliance HCX che verranno configurate automaticamente sia sul sito di origine che su quello di destinazione, creando un fabric di trasporto sicuro.

5. Selezionare i profili di origine e di elaborazione remota e fare clic su Continua.

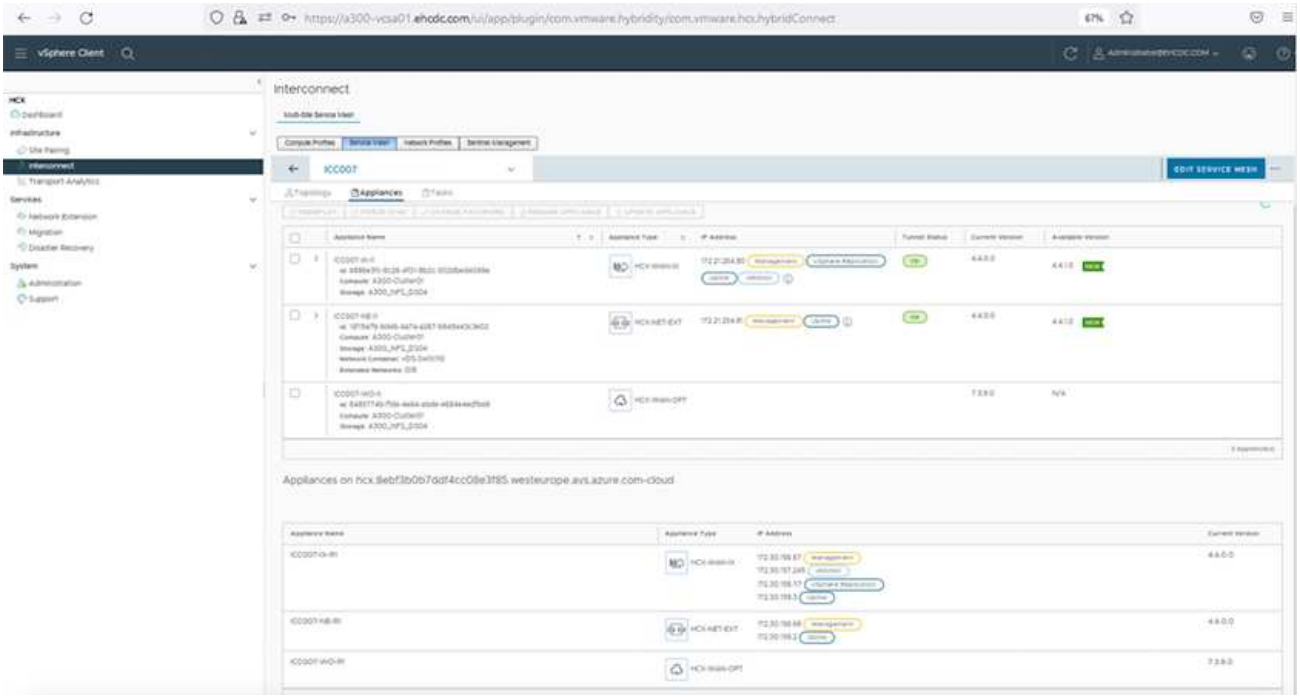


6. Seleziona il servizio da attivare e clicca su Continua.



Per Replication Assisted vMotion Migration, SRM Integration e OS Assisted Migration è richiesta una licenza HCX Enterprise.

7. Crea un nome per il service mesh e fai clic su Fine per iniziare il processo di creazione. L'implementazione dovrebbe richiedere circa 30 minuti. Dopo aver configurato il service mesh, sono state create l'infrastruttura virtuale e la rete necessarie per migrare le VM del carico di lavoro.



▼ Fase 6: Migrazione dei carichi di lavoro

HCX fornisce servizi di migrazione bidirezionale tra due o più ambienti distinti, ad esempio SDDC locali e VMC. I carichi di lavoro delle applicazioni possono essere migrati da e verso i siti attivati da HCX utilizzando una varietà di tecnologie di migrazione, quali migrazione in blocco HCX, HCX vMotion, migrazione a freddo HCX, HCX Replication Assisted vMotion (disponibile con l'edizione HCX Enterprise) e migrazione assistita del sistema operativo HCX (disponibile con l'edizione HCX Enterprise).

Per saperne di più sulle tecnologie di migrazione HCX disponibili, 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 nel vCenter Server. Le risorse di processore, memoria, storage e rete visualizzate su questo oggetto non rappresentano il consumo effettivo sull'hypervisor fisico che ospita l'appliance IX.



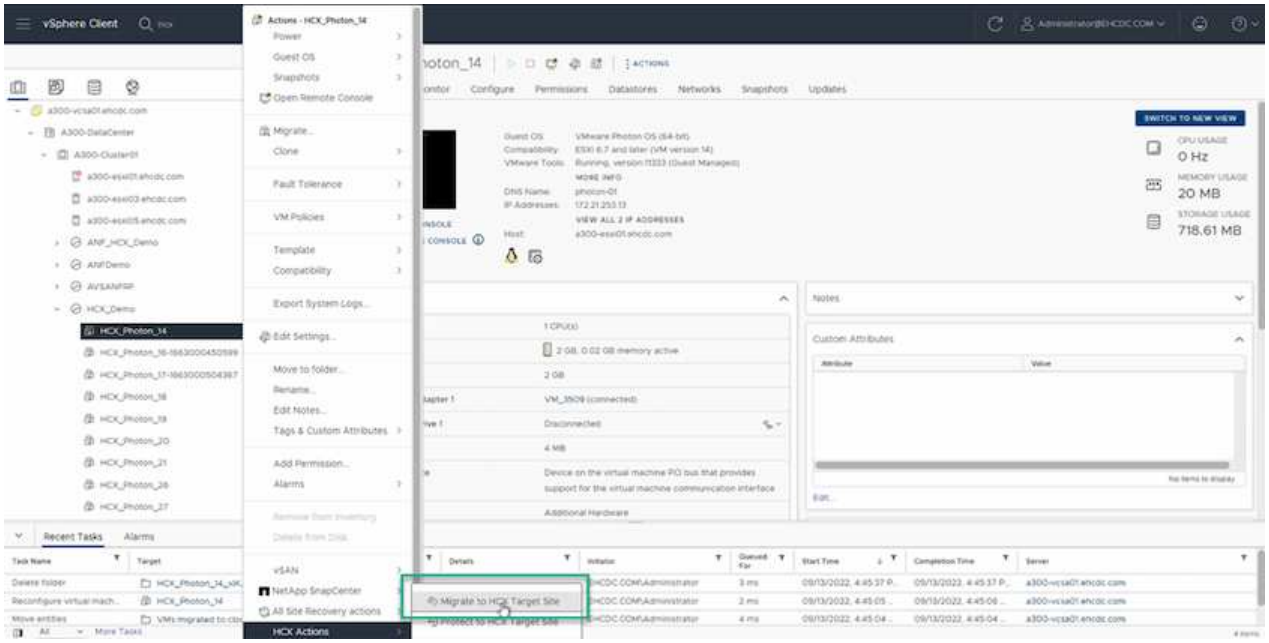
▼ VMware HCX vMotion

Questa sezione descrive il meccanismo HCX vMotion. Questa tecnologia di migrazione utilizza il

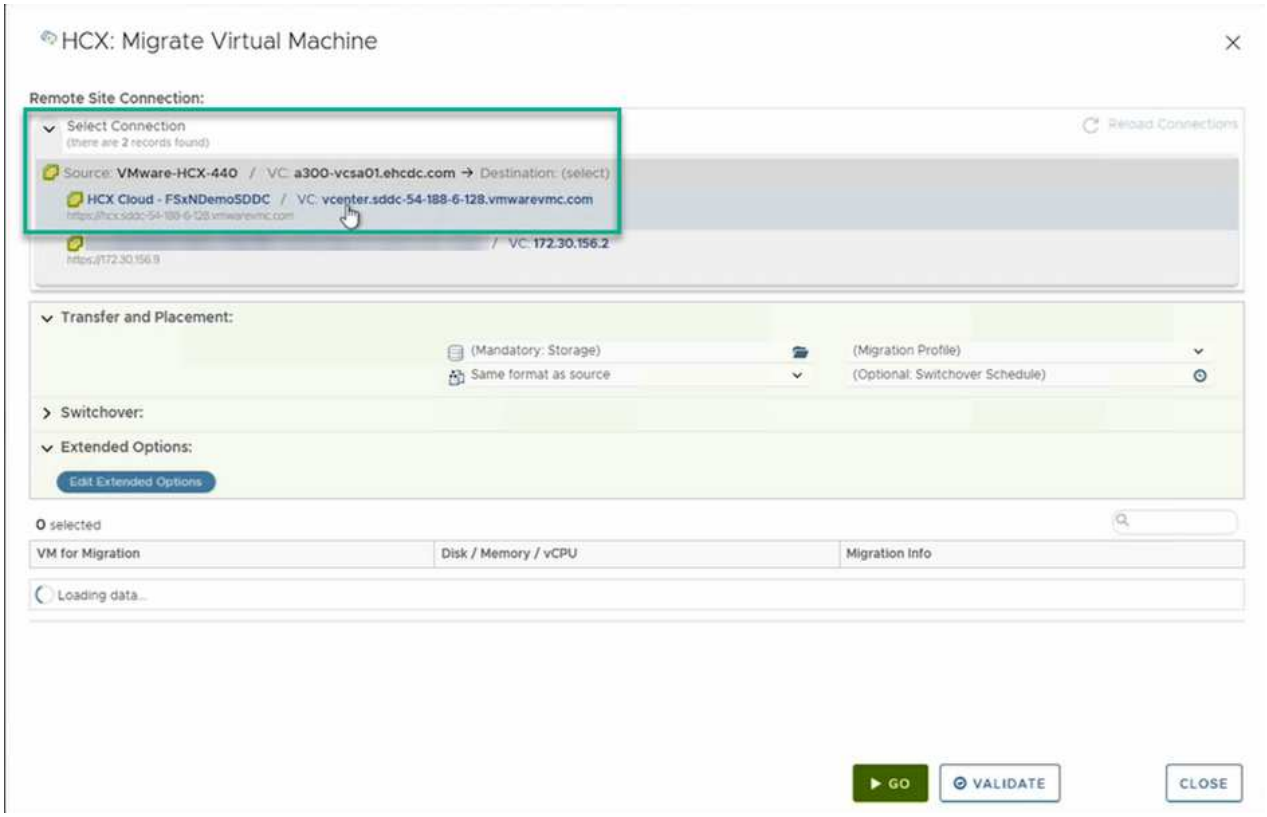
protocollo VMware vMotion per migrare una VM su VMC SDDC. L'opzione di migrazione vMotion viene utilizzata per migrare lo stato di una singola VM alla volta. Durante questo metodo di migrazione non si verifica alcuna interruzione del servizio.

È necessario che sia presente un'estensione di rete (per il gruppo di porte a cui è collegata la VM) per poter migrare la VM senza dover modificare l'indirizzo IP.

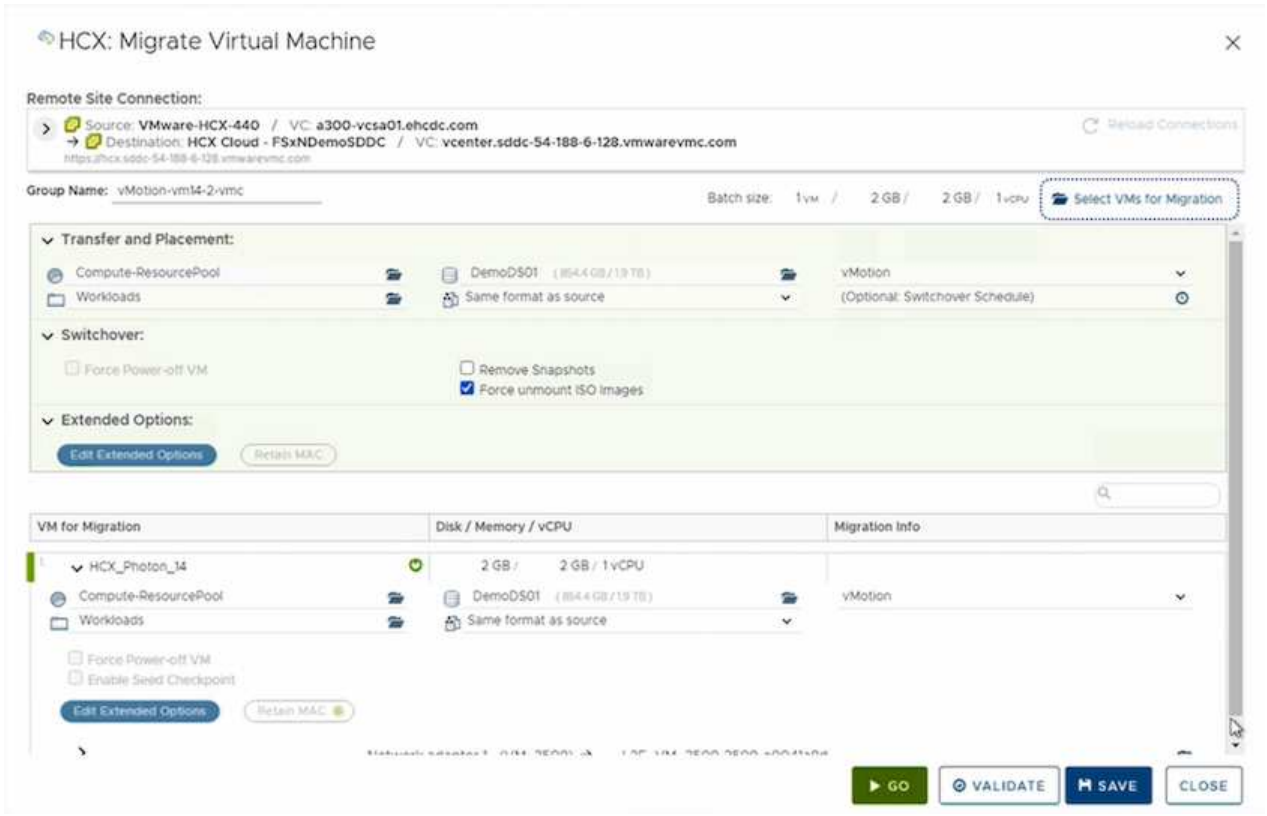
1. Dal client vSphere on-premise, vai su Inventario, fai clic con il pulsante destro del mouse sulla VM da migrare e seleziona Azioni HCX > Migra al sito di destinazione HCX.



2. Nella procedura guidata Migra macchina virtuale, selezionare Connessione sito remoto (destinazione VMC SDDC).



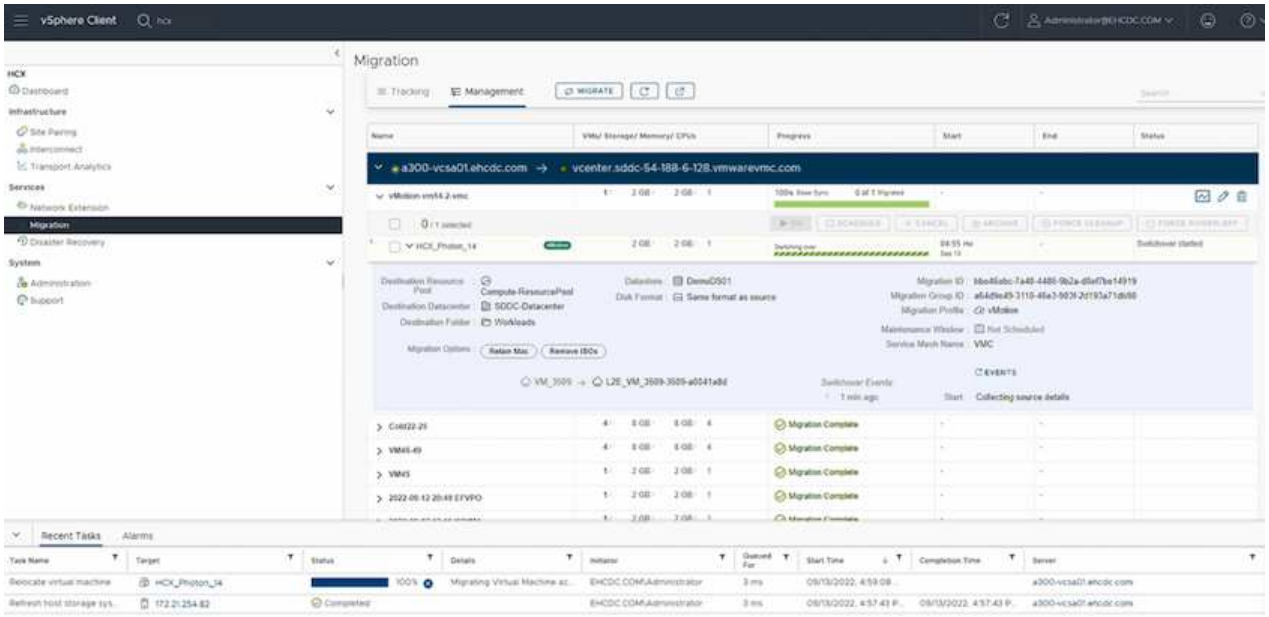
3. Aggiungere un nome di gruppo e in Trasferimento e posizionamento aggiornare i campi obbligatori (Cluster, Archiviazione e Rete di destinazione), quindi fare clic su Convalida.



4. Una volta completati i controlli di convalida, fare clic su Vai per avviare la migrazione.

Il trasferimento vMotion cattura la memoria attiva della VM, il suo stato di esecuzione, il suo indirizzo IP e il suo indirizzo MAC. Per ulteriori informazioni sui requisiti e le limitazioni di HCX vMotion, vedere "Informazioni su VMware HCX vMotion e sulla migrazione a freddo" .

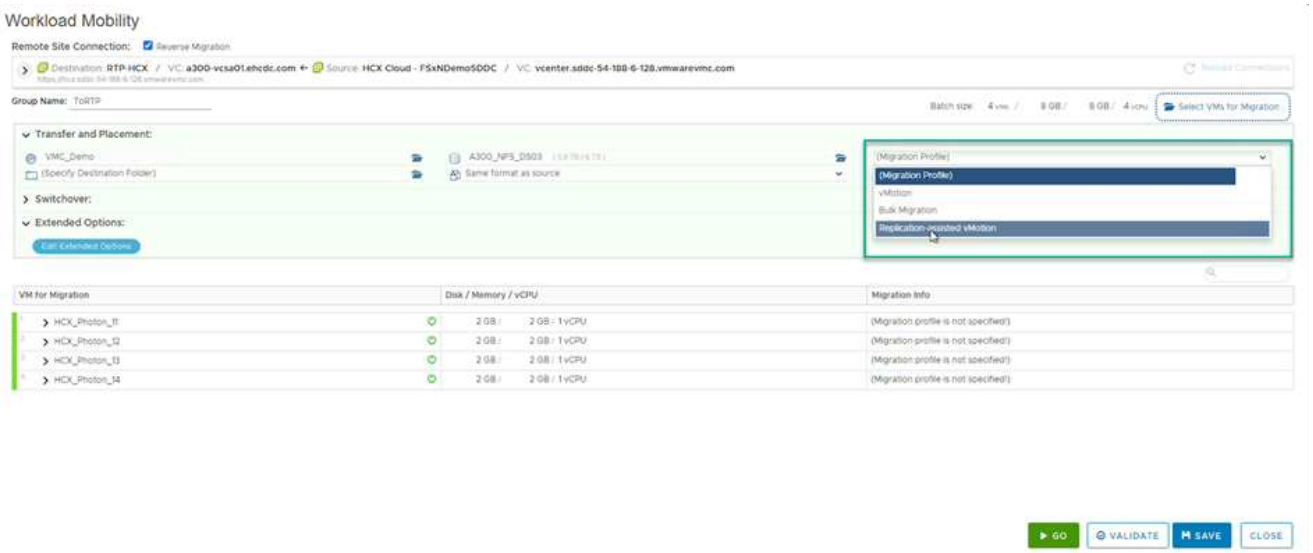
5. È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migrazione.



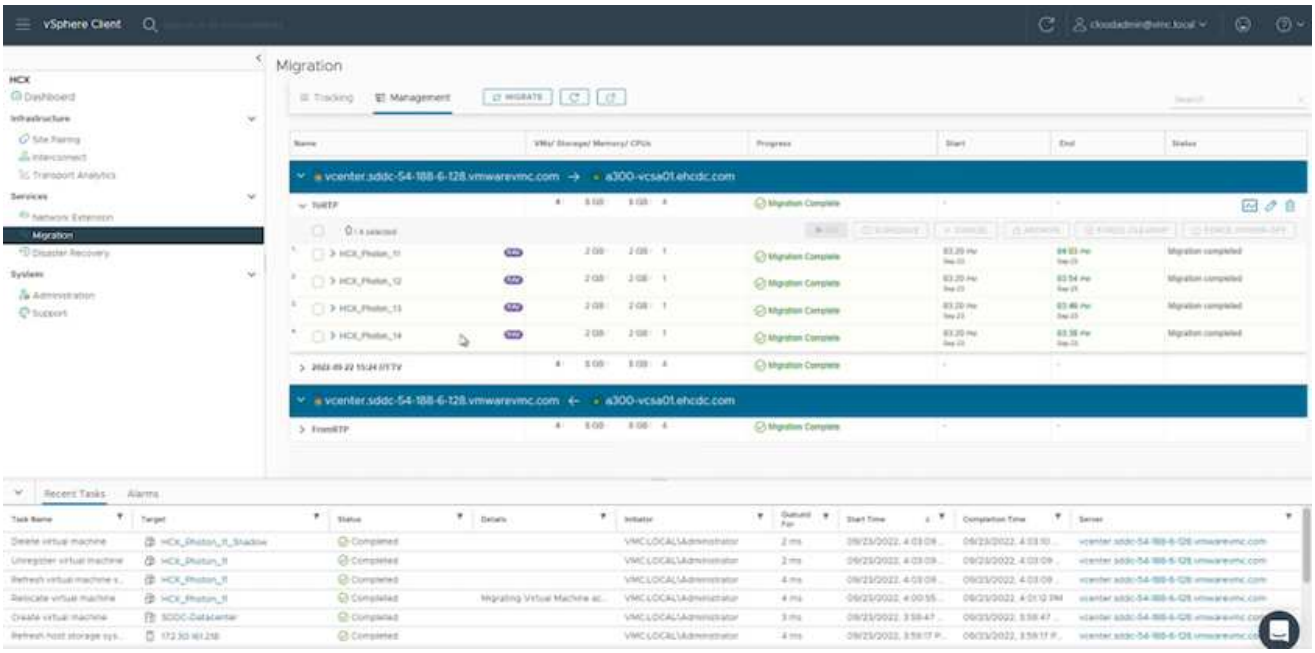
▼ **VMware Replication Assisted vMotion**

Come avrai notato dalla documentazione VMware, VMware HCX Replication Assisted vMotion (RAV) combina i vantaggi della migrazione in blocco e di vMotion. La migrazione in blocco utilizza vSphere Replication per migrare più VM in parallelo: la VM viene riavviata durante il passaggio. HCX vMotion esegue la migrazione senza tempi di inattività, ma la migrazione viene eseguita in serie, una VM alla volta in un gruppo di replica. RAV replica la VM in parallelo e la mantiene sincronizzata fino alla finestra di switchover. Durante il processo di switchover, viene migrata una VM alla volta senza tempi di inattività per la VM.

La seguente schermata mostra il profilo di migrazione come Replication Assisted vMotion.



La durata della replica potrebbe essere più lunga rispetto al vMotion di un numero limitato di VM. Con RAV, sincronizza solo i delta e includi il contenuto della memoria. Di seguito è riportato uno screenshot dello stato della migrazione: mostra come l'ora di inizio della migrazione sia la stessa e l'ora di fine sia diversa per ogni VM.



Per ulteriori informazioni sulle opzioni di migrazione HCX e su come migrare i carichi di lavoro da locale a VMware Cloud su AWS utilizzando HCX, vedere "Guida utente VMware HCX" .

VMware HCX vMotion richiede una capacità di throughput di 100 Mbps o superiore.

Il datastore VMC FSx ONTAP di destinazione deve disporre di spazio sufficiente per supportare la migrazione.

Conclusione

Che si punti a un cloud completamente cloud o ibrido e che i dati risiedano su qualsiasi tipo/fornitore di storage in locale, Amazon FSx ONTAP insieme a HCX offrono eccellenti opzioni per distribuire e migrare i carichi di lavoro, riducendo al contempo il TCO rendendo i requisiti dei dati uniformi al livello applicativo. Qualunque sia il caso d'uso, scegli VMC insieme al datastore FSx ONTAP per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti su cloud locali e multipli, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per connettere lo storage e migrare le VM utilizzando la replica VMware vSphere, VMware vMotion o persino la copia NFC.

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 locale a VMC in esecuzione con datastore FSx ONTAP
- È possibile espandere e ridurre facilmente il datastore FSx ONTAP per soddisfare i requisiti di capacità e prestazioni durante l'attività di migrazione.

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, fare riferimento ai seguenti link del sito web:

- Documentazione VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentazione Amazon FSx ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guida utente VMware HCX

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

NetApp per AWS / EVS

Monta FSx ONTAP come datastore esterno per EVS

Come montare Amazon FSx for NetApp ONTAP come datastore esterno per Amazon Elastic VMware Service

In questo documento verranno illustrati i passaggi dettagliati per creare un file system FSx per ONTAP e collegarlo per l'utilizzo come datastore Internet Small Computer System Interface (iSCSI) o Network File System (NFS) da utilizzare con Amazon EVS.

Introduzione

Le organizzazioni con investimenti VMware on-premise esistenti alla ricerca di modi efficienti e convenienti per modernizzare le proprie distribuzioni migrando, suddividendo, estendendo o proteggendo (backup, disaster recovery) le copie su AWS hanno dovuto affrontare diverse sfide. Con il rilascio di Amazon Elastic VMware Service (Amazon EVS) è ora disponibile un servizio AWS nativo che consente di eseguire VMware Cloud Foundation (VCF) direttamente in un Amazon Virtual Private Cloud (VPC).

Amazon EVS consente di estendere le distribuzioni VCF esistenti ad AWS, di espandersi in AWS per aumentare le prestazioni durante i picchi di utilizzo e di eseguire interamente carichi di lavoro VCF su AWS per facilitare modernizzazioni, uscite dai data center, consolidamenti e altri casi d'uso.

Sebbene Amazon EVS offra notevoli vantaggi, l'architettura iperconvergente predefinita abbina elaborazione e archiviazione, impedendo la scalabilità indipendente dell'uno o dell'altro in base alle esigenze aziendali. Nel mondo odierno incentrato sui dati, le esigenze di storage in molte organizzazioni sono superiori a quelle di elaborazione. Tuttavia, con l'architettura iperconvergente VMware, le risorse di storage sono abbinate alle risorse di elaborazione. Ciò significa che è possibile ridimensionare lo storage solo aggiungendo host di elaborazione che non verranno mai utilizzati. Si tratta di una situazione che può aumentare notevolmente i costi, soprattutto in caso di carichi di lavoro che richiedono molta memoria.

Per risolvere questo problema, AWS e NetApp offrono Amazon FSx for NetApp ONTAP (FSx for ONTAP) come servizio di archiviazione esterno per Amazon EVS. FSx for ONTAP è un servizio di storage nativo di AWS che offre le elevate prestazioni, la resilienza dei dati e la convenienza del software NetApp ONTAP . Utilizzando FSx per ONTAP come storage esterno, gli utenti di Amazon EVS possono scalare le risorse di elaborazione e storage in modo indipendente, consentendo un costo totale di proprietà (TCO) ottimale.

Panoramica

In questo documento verranno illustrati i passaggi dettagliati per creare un file system FSx per ONTAP e collegarlo per l'utilizzo come datastore Internet Small Computer System Interface (iSCSI) o Network File System (NFS) da utilizzare con Amazon EVS.

Scopo di questa guida

Questa guida fornisce istruzioni su come configurare un datastore FSx for ONTAP per Amazon EVS, nonché best practice, requisiti di supporto, considerazioni sul dimensionamento e altre informazioni per aiutarti a pianificare, progettare e implementare l'integrazione.

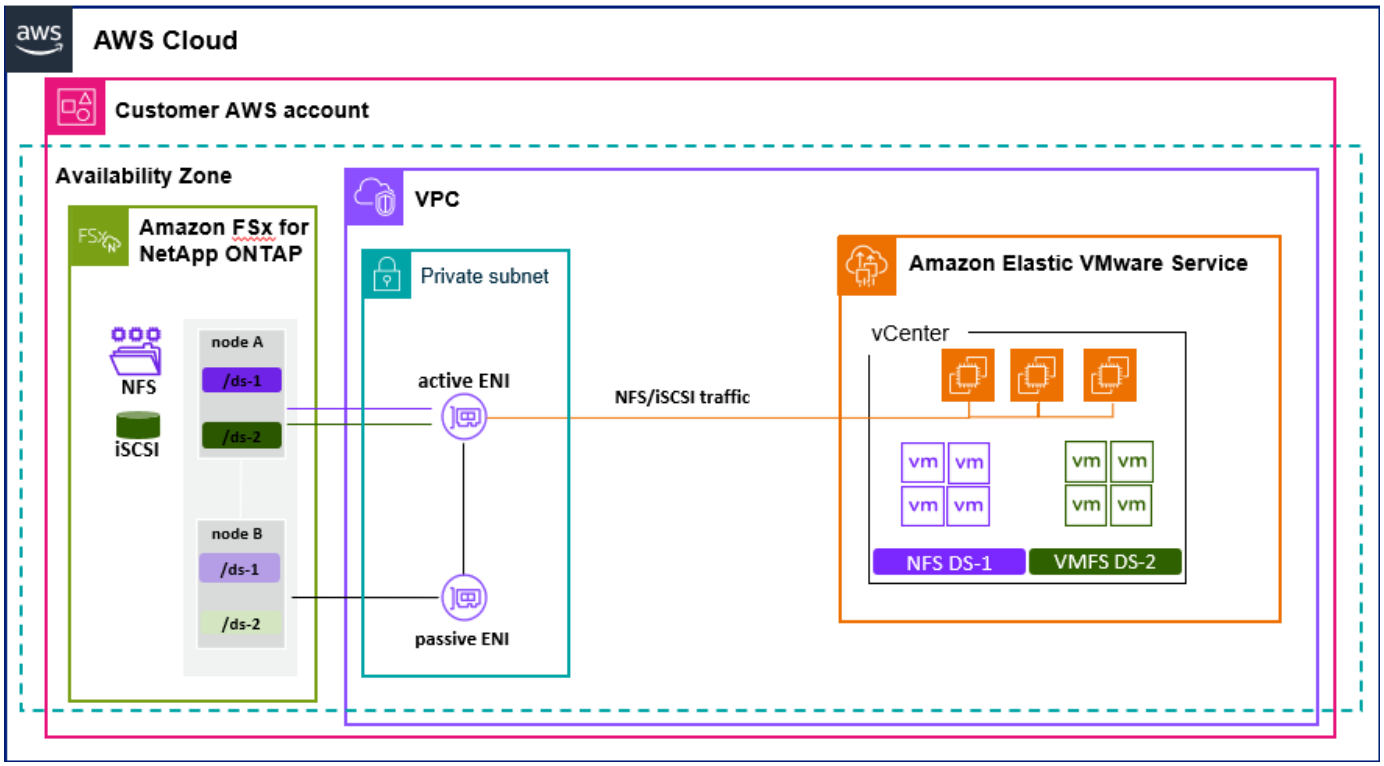
Pubblico

Questo tutorial è destinato ad architetti e amministratori cloud che hanno familiarità con VMware vSphere, Amazon EVS, AWS Console e FSx per ONTAP.

Architettura di alto livello

In questa sezione forniremo una panoramica dell'architettura della soluzione per l'utilizzo di FSx for ONTAP come datastore per Amazon EVS.

Di seguito è possibile visualizzare una panoramica generale dell'architettura del datastore FSx for ONTAP con un ambiente Amazon EVS all'interno di un AWS VPC.



Procedura di distribuzione per l'utilizzo di FSx per ONTAP come datastore NFS

In questa sezione verranno illustrati i passaggi per distribuire FSx per ONTAP come datastore NFS. I passaggi per la distribuzione di un datastore iSCSI sono descritti in dettaglio nella sezione successiva.

Fasi di distribuzione di alto livello

L'implementazione del file system FSx for ONTAP da utilizzare come datastore NFS per Amazon EVS e la creazione della connettività tra i due servizi includeranno i seguenti passaggi:

- Configurazione di un file system FSx per ONTAP nella stessa VPC in cui si trova l'ambiente Amazon EVS VCF.
- Convalida dei gruppi di sicurezza e della tabella di routing.
- Collegamento di un volume di archiviazione FSx for ONTAP da utilizzare come datastore NFS per Amazon EVS.

Prerequisiti

Prima di iniziare il processo di configurazione di un FSx per ONTAP come datastore NFS per Amazon EVS, è necessario soddisfare i seguenti prerequisiti:

- Un ambiente di virtualizzazione Amazon EVS. Per maggiori informazioni su come farlo, vedere la documentazione su"Guida introduttiva ad Amazon EVS" .
- Creare una zona di disponibilità singola (AZ) FSx per ONTAP con capacità di archiviazione SSD adeguata, IOPS e throughput forniti.
- Per prestazioni ottimali, posizionare il file system FSx for ONTAP all'interno della stessa VPC dell'istanza Amazon EVS. Si noti che il peering VPC è supportato anche nel caso in cui FSx per ONTAP venga distribuito in una VPC diversa.
- In base ai requisiti di prestazioni, selezionare gli IOPS e la velocità effettiva corretti necessari per un file system FSx Single-AZ per ONTAP . Vedere"dettagli delle specifiche delle prestazioni per FSx per ONTAP" per comprendere la produttività e gli IOPS forniti da ciascuna opzione disponibile.

> In questa guida distribuiremo il file system FSx for ONTAP nella stessa subnet della subnet di accesso al servizio.

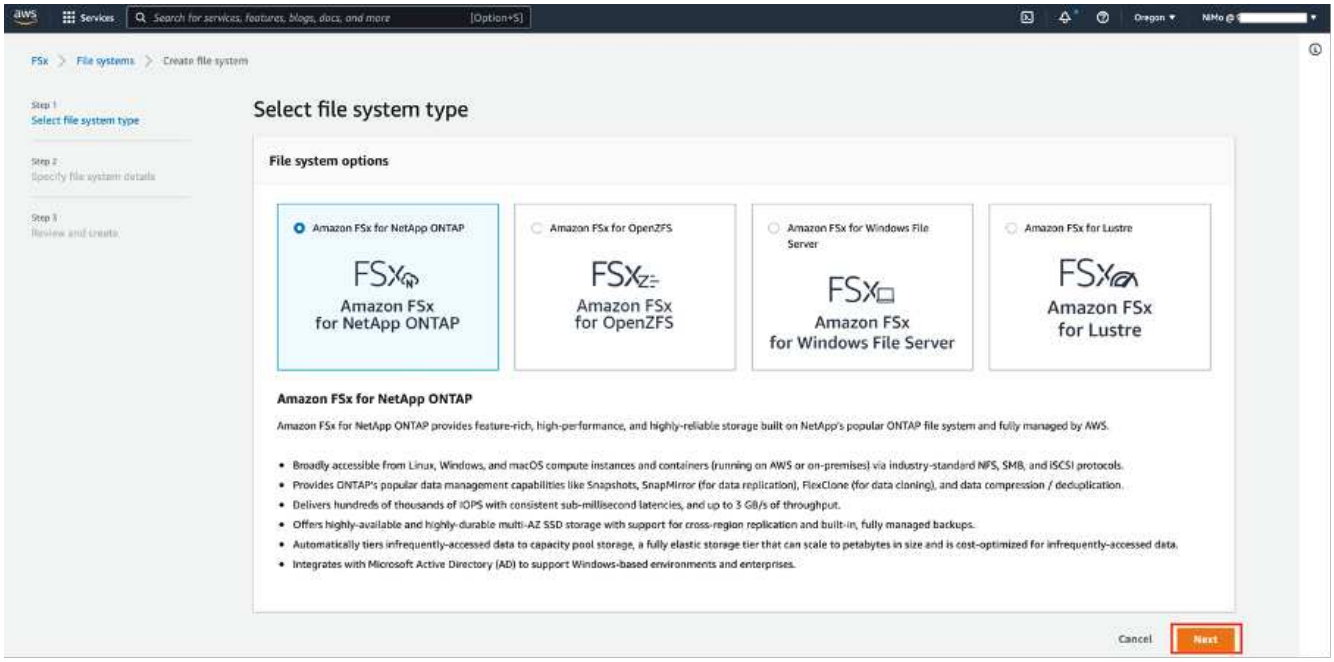
Una volta distribuito l'ambiente di virtualizzazione Amazon EVS nella VPC, è possibile procedere con la configurazione del file system Single-AZ FSx per ONTAP che verrà utilizzato come datastore NFS.

> Il file system FSx for ONTAP deve essere distribuito nella stessa zona di disponibilità dell'Amazon EVS SDDC.

Creare un file system FSx per ONTAP

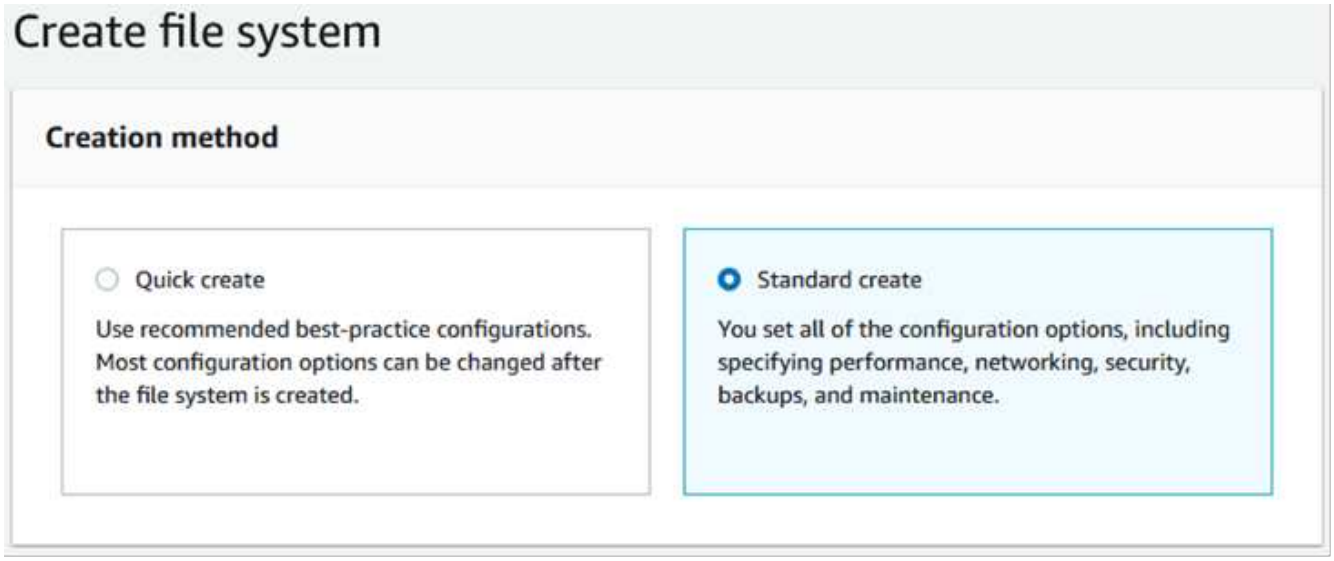
I seguenti passaggi ti mostreranno come effettuare il provisioning e montare un file system FSx per ONTAP :

1. Vai alla console Amazon FSx all'indirizzo `https://console.aws.amazon.com/fsx/` utilizzando il tuo browser Internet ed effettua l'accesso con le tue credenziali.
2. Nella console, seleziona Crea file system. Verrà avviata la procedura guidata di configurazione per creare un file system FSx per ONTAP .
3. Per prima cosa, seleziona il tipo di file system. Dalle opzioni del file system disponibili, seleziona "Amazon FSx for NetApp ONTAP" e procedi cliccando sul pulsante "Avanti".

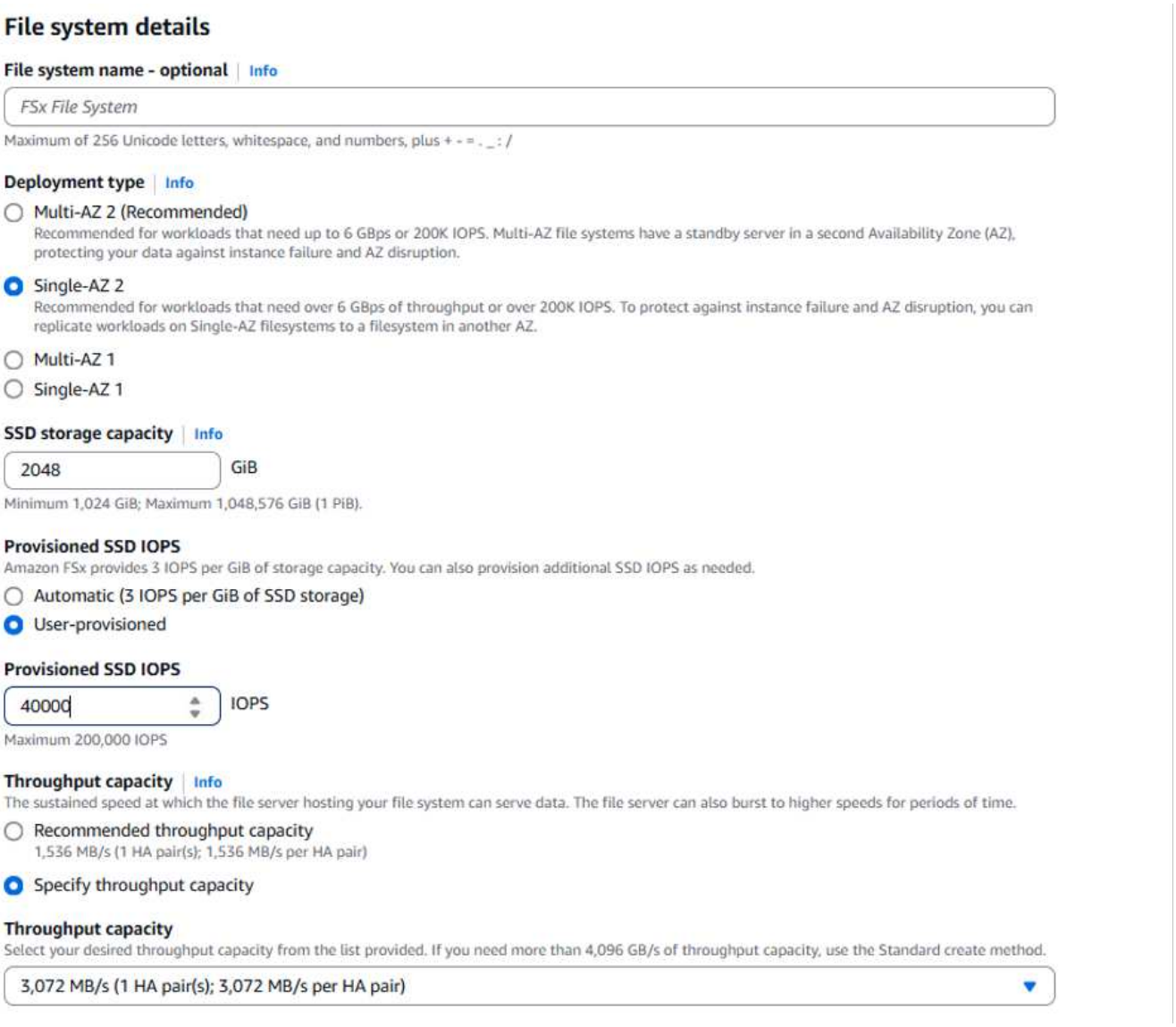


4. Ti verrà chiesto di scegliere tra le opzioni Creazione rapida e Creazione standard. La creazione rapida offre configurazioni predefinite, mentre la creazione standard consente di definire configurazioni personalizzate.

   Selezionare l'opzione "Creazione standard".

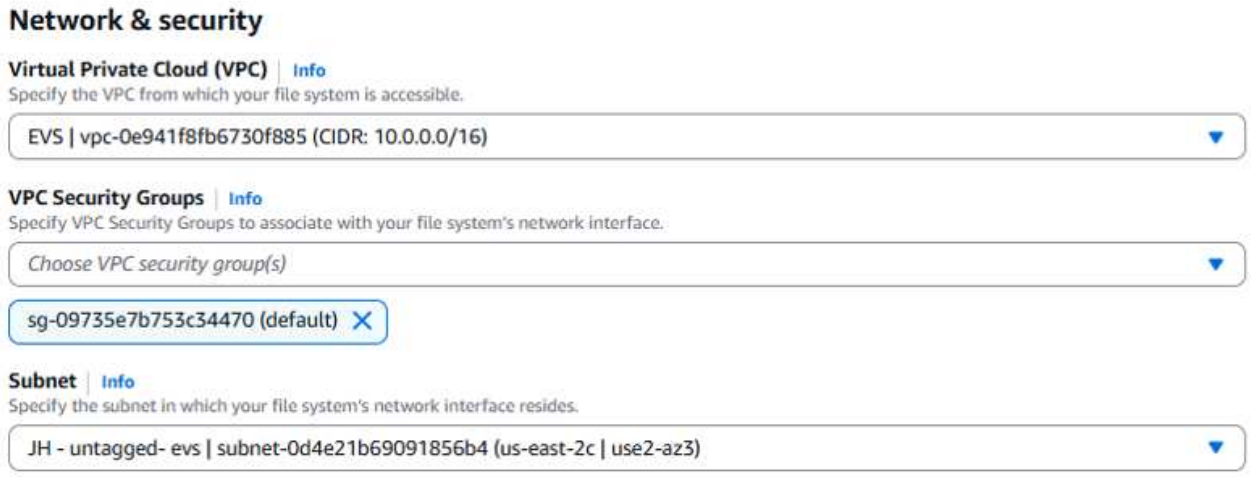


   Ora ti troverai nella procedura guidata di configurazione del file system di creazione standard. Nella pagina dei dettagli del file system, seleziona e inserisci le stesse informazioni mostrate nell'immagine sottostante:



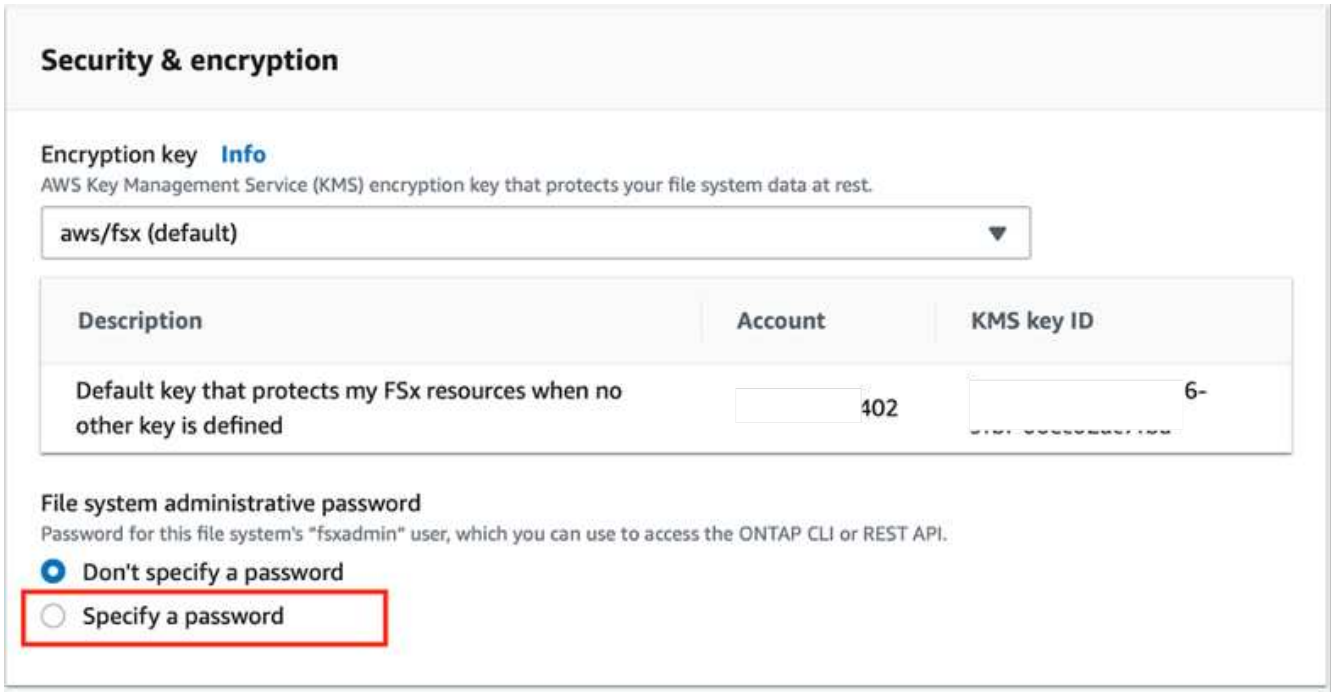
5. Scorri verso il basso fino a trovare la sezione denominata "Rete e sicurezza". In questa sezione imposterai i dettagli per la subnet e la VPC. Ai fini di questa guida, abbiamo selezionato "EVS-VPC" dal menu a discesa e selezionato la subnet di accesso al servizio (VLAN senza tag) come subnet per l'ambiente virtuale EVS.

> La subnet può essere qualsiasi subnet privata senza tag nella VPC. Può anche trovarsi in una VPC/subnet diversa connessa tramite VPC Peering, a condizione che sia stato configurato il routing corretto.

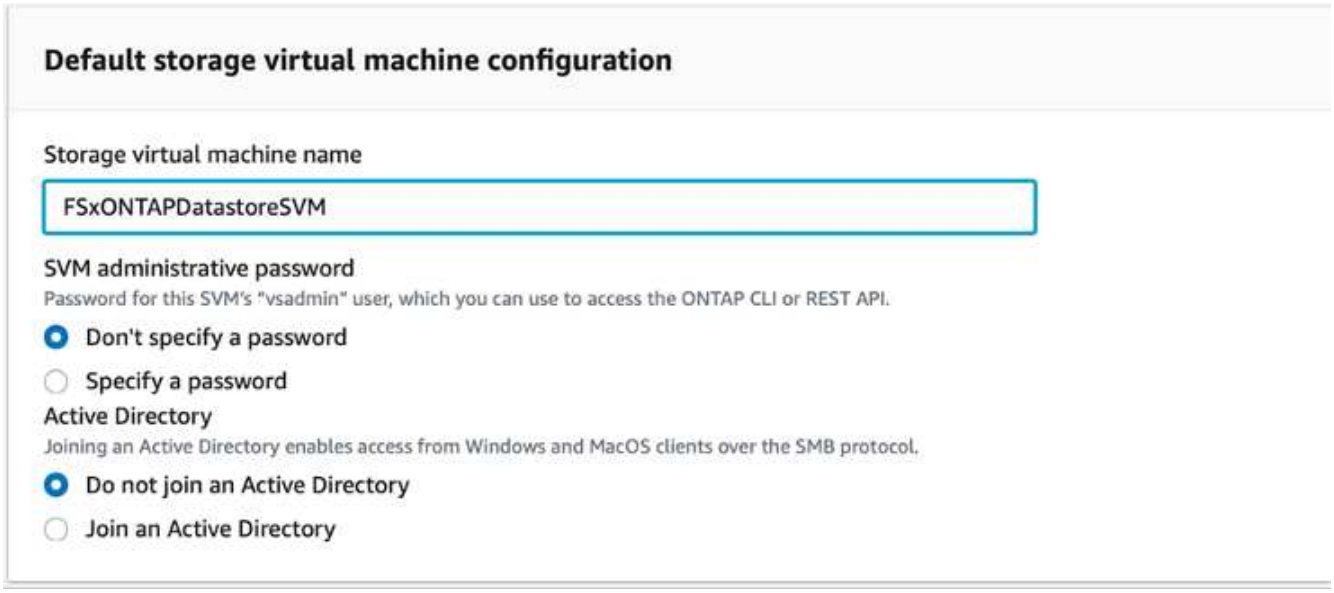


6. Scorrendo verso il basso troverai la sezione "Sicurezza e crittografia". Qui, seleziona la chiave di crittografia dal menu a discesa. Queste chiavi sono fornite da AWS Key Management Service (AWS KMS) e proteggeranno i dati inattivi nel file system FSx for ONTAP .

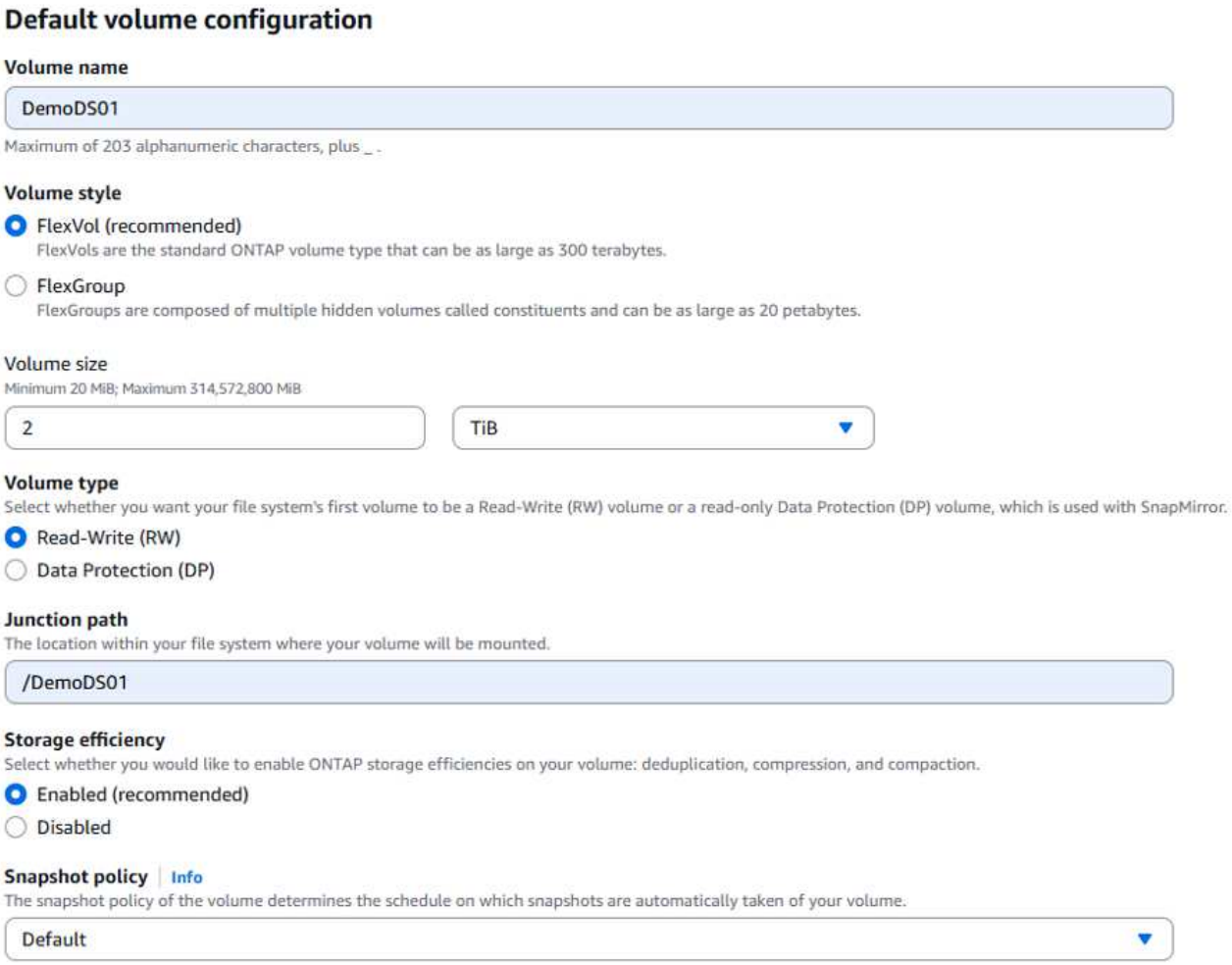
   Successivamente, nell'impostazione "Password amministrativa del file system", specificare una password univoca per l'utente fsxadmin che amministrerà il file system.



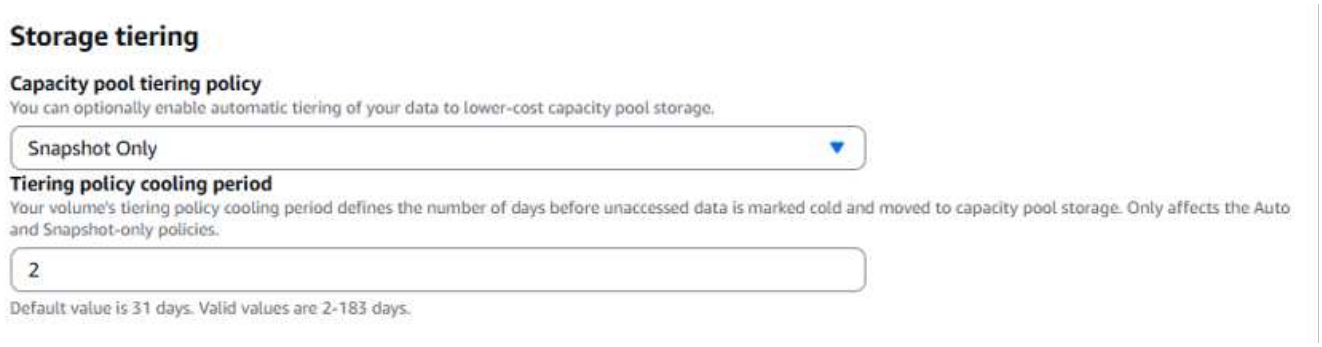
7. Successivamente, scorrerai verso il basso fino a una sezione intitolata "Configurazione predefinita della macchina virtuale di archiviazione". Qui dovrai fornire un nome per la macchina virtuale di archiviazione (SVM).



8. Quindi, scorri verso il basso fino alla sezione intitolata "Configurazione del volume predefinito". Qui potrai fornire un nome per il volume e impostarne la dimensione. Il protocollo del volume dovrebbe essere NFS v3 (abilitato per impostazione predefinita). Fare clic sull'opzione per abilitare le funzionalità di efficienza dell'archiviazione (compressione, deduplicazione e compattazione) per ridurre l'utilizzo complessivo dell'archiviazione e i costi.



9. Per l’opzione di suddivisione in livelli di archiviazione, seleziona "Solo snapshot" dal menu a discesa e imposta un periodo di raffreddamento per la politica di suddivisione in livelli. L’impostazione predefinita è 31 giorni, ma in questo esempio abbiamo impostato un periodo di raffreddamento di due giorni.

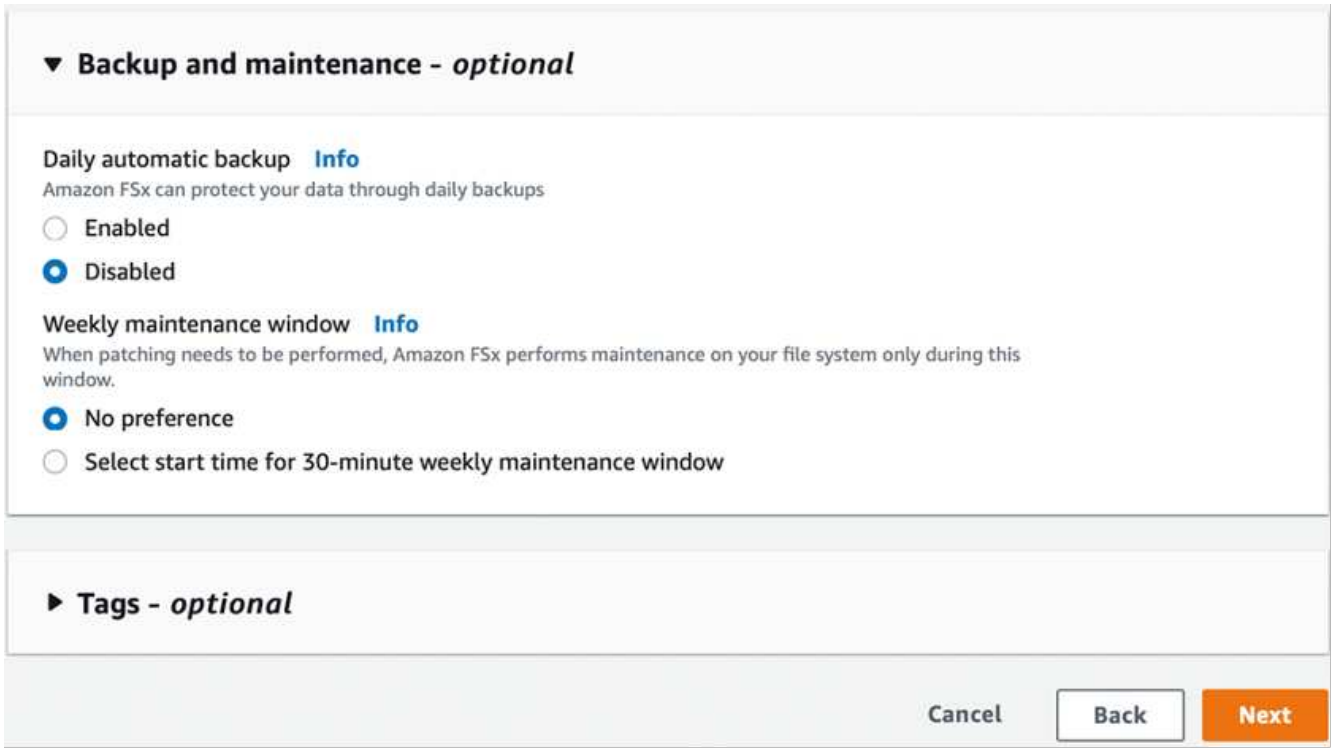


10. Dopo aver creato il volume, modificare i seguenti parametri utilizzando l’interfaccia della riga di comando ONTAP (ONTAP CLI):

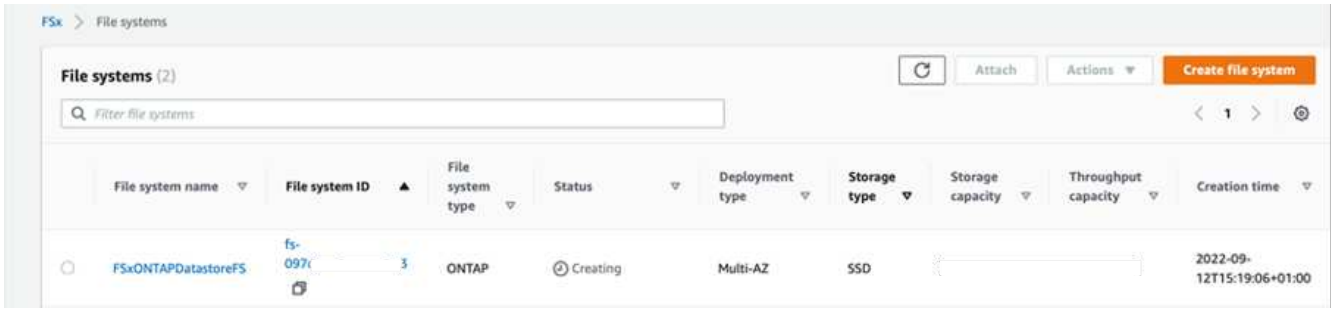
Collocamento	Configurazione
Garanzia di volume	Nessuno (thin provisioning)
riserva frazionaria	0%
snap_reserve	0%
Autodimensionamento	crescere_ridurre
Efficienza di archiviazione	Abilitato
Politica di suddivisione in livelli del volume	Solo istantanea
Aggiornamento dell’ora di accesso (-atime-update)	Falso
Lettura minima anticipata (-min-readahead)	Falso
Politica di snapshot	Nessuno

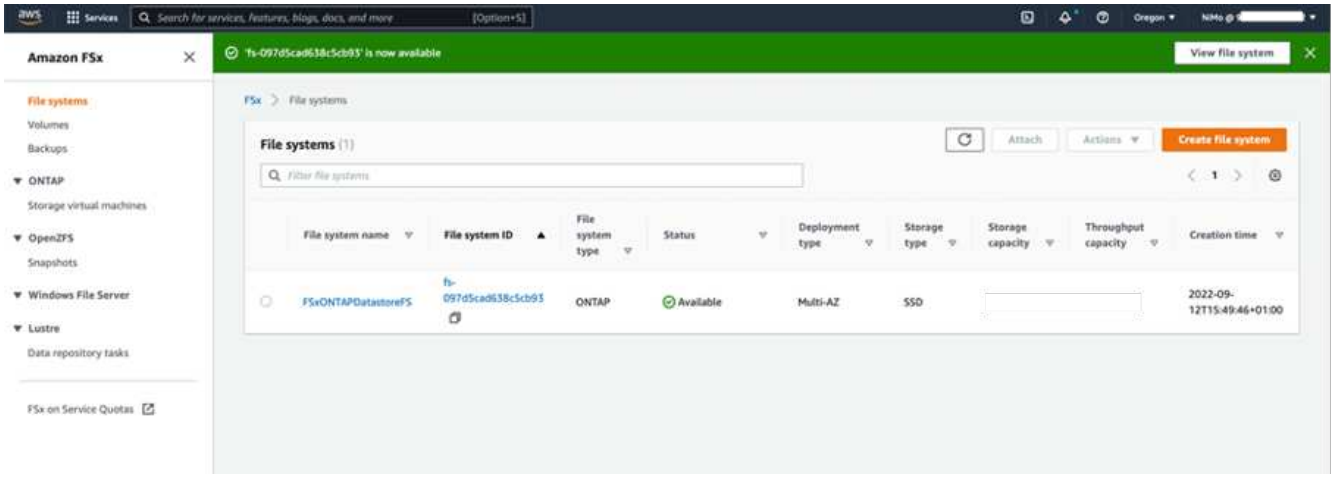
11. Nel passaggio facoltativo "Backup e manutenzione", disabilitare i backup automatici giornalieri e selezionare "Nessuna preferenza" per la finestra di manutenzione settimanale.

    Al termine, fare clic su "Avanti".



12. Ora ti verrà fornita una panoramica dell'intera configurazione del file system che hai impostato seguendo i passaggi precedenti. Verificare che tutti i parametri siano corretti, quindi fare clic sul pulsante "Crea file system" per completare la configurazione.





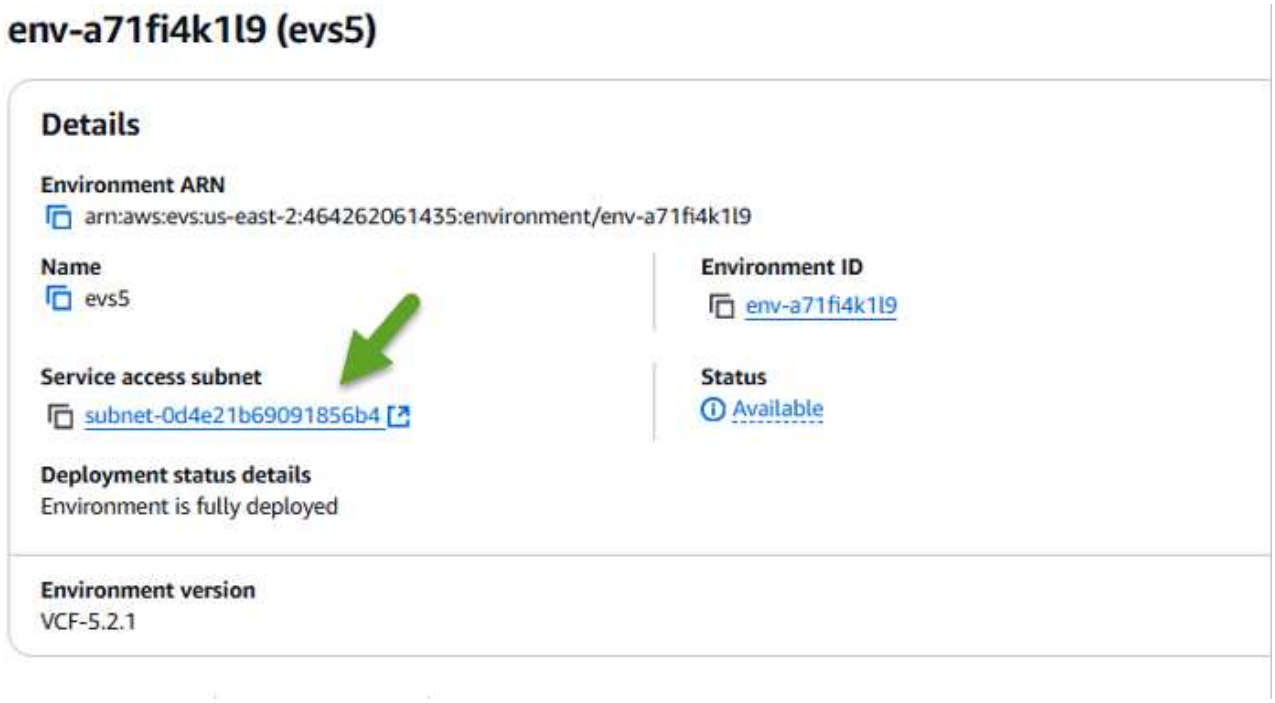
Per creare file system FSx aggiuntivi per ONTAP , è possibile seguire i passaggi descritti sopra, regolando i valori che influiscono sulle prestazioni e sulla capacità del disco secondo necessità. Per saperne di più sulle opzioni di prestazioni per FSx per ONTAP, vedere"questa

pagina di documentazione" .

Convalida dei gruppi di routing e sicurezza dell'ambiente VPC e virtualizzato

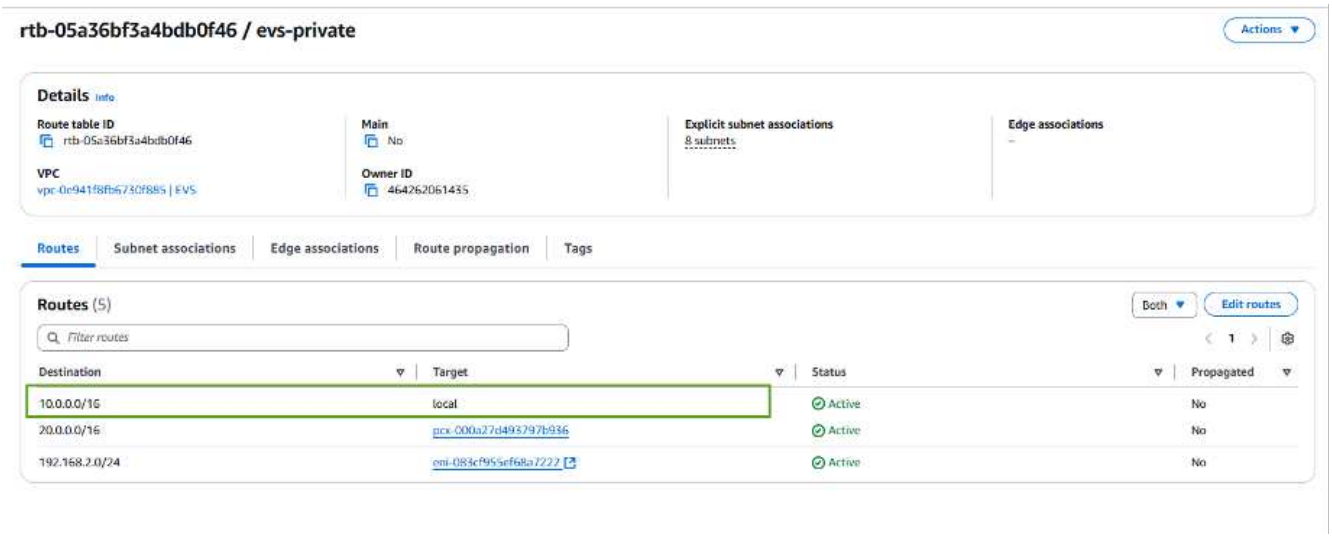
La convalida dei gruppi di routing e sicurezza VPC e SDDC è importante per garantire che l'ambiente di virtualizzazione Amazon EVS e i componenti del file system FSx for ONTAP possano funzionare correttamente insieme.

1. Passare a Elastic VMware Service > Virtualization Environments > [ambiente Amazon EVS] e selezionare la subnet di accesso al servizio, come indicato dalla freccia verde qui sotto:



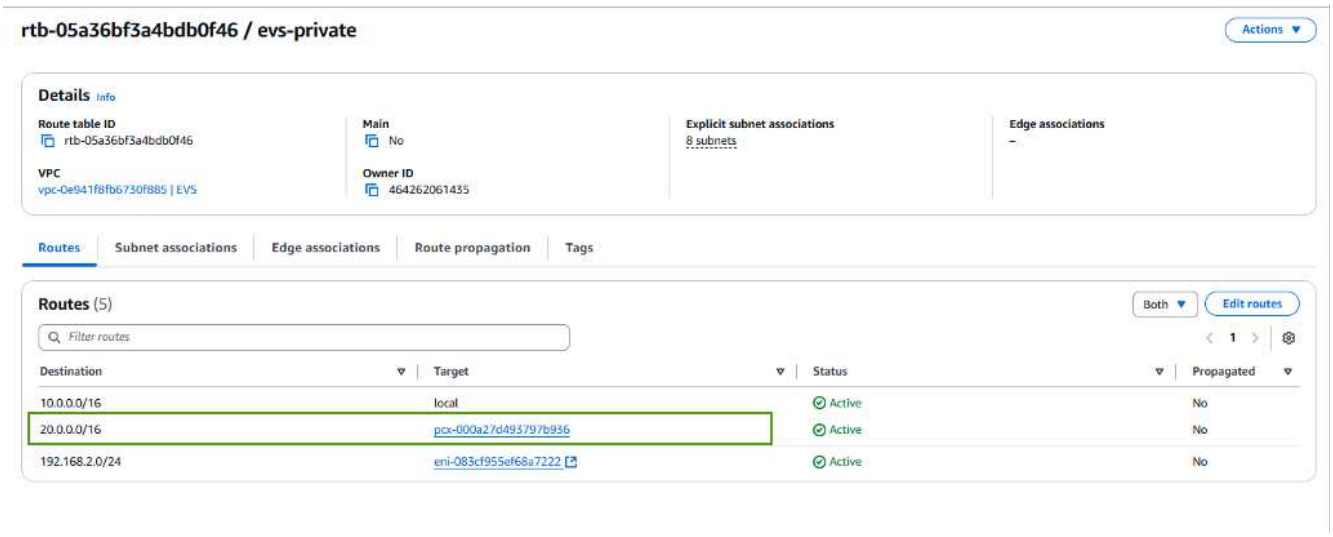
2. Verrà aperto il pannello della subnet. Trova la tabella Percorsi in questo pannello e cliccaci sopra.

   In questo esempio il file system FSxN ONTAP si trova nella stessa VPC dell'ambiente Amazon EVS VCF, quindi i percorsi predefiniti sono sufficienti.



   Se il file system FSx per ONTAP si trova in una VPC diversa, verificare che siano stati aggiunti i percorsi

verso tale VPC. In questo esempio sono stati aggiunti percorsi per il peering VPC alla VPC in cui risiede il sistema FSx for ONTAP .

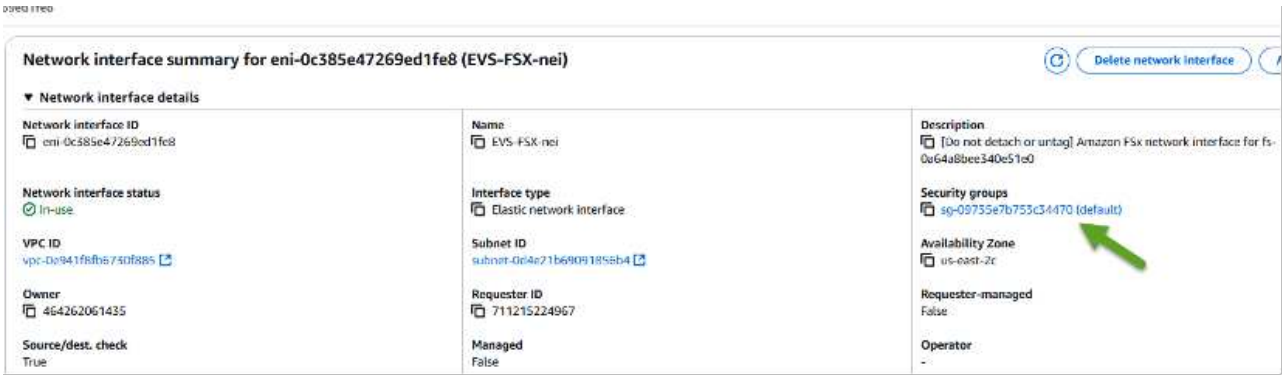


3. Successivamente, sarà necessario verificare che il gruppo di sicurezza connesso al file system FSx for ONTAP (ovvero quello connesso all'interfaccia di rete elastica (ENI) consenta l'accesso alle porte NFS).

   Per un elenco completo delle porte dei protocolli NFS e iSCSI, fare riferimento al collegamento: https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]Documentazione sul controllo degli accessi al file system con Amazon VPC].

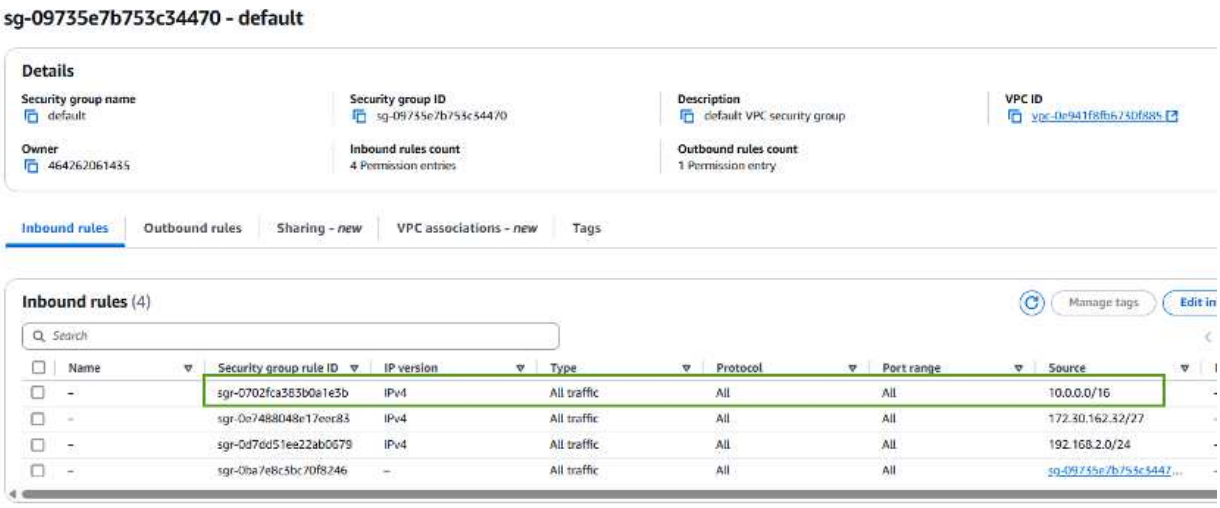
   Per verificare che il file system FSx for ONTAP sia associato al gruppo di sicurezza:

   a. Nella console AWS, vai su FSx > File System > [il tuo file system FSx per ONTAP].
   b. Nella scheda Rete e sicurezza, fare clic su ENI.
   c. Trova il gruppo di sicurezza elencato nei dettagli dell'interfaccia di rete associato all'ENI (indicato dalla freccia verde nell'immagine sottostante).



   d. Convalidare le porte. Nell'esempio mostrato nella schermata seguente, è consentito tutto il traffico. Tuttavia, è possibile limitarli alle sole porte NFS. Ecco l'elenco dei porti:
      - Porta 111 TCP: Portmapper, utilizzato per negoziare quali porte vengono utilizzate nelle richieste NFS.
      - Porta 635 TCP: Mountd, che serve per ricevere le richieste di montaggio in arrivo.
      - Porta 2049 TCP: NFS, che gestisce il traffico NFS.

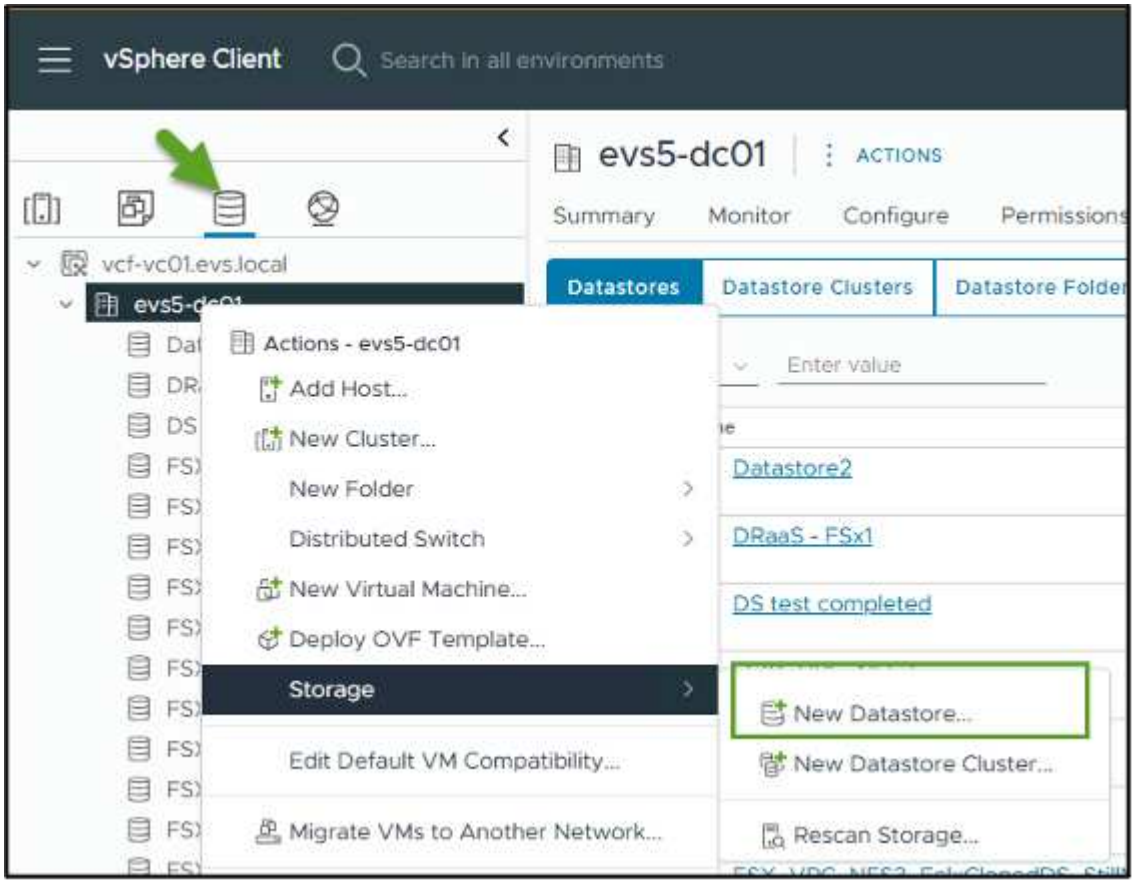
- Porta 4045 TCP: Network Lock Manager (NLM), che gestisce le richieste di blocco.
- Porta 4046 TCP: Network Status Monitor (NSM), che invia notifiche ai client NFS quando il server si riavvia per la gestione dei blocchi.



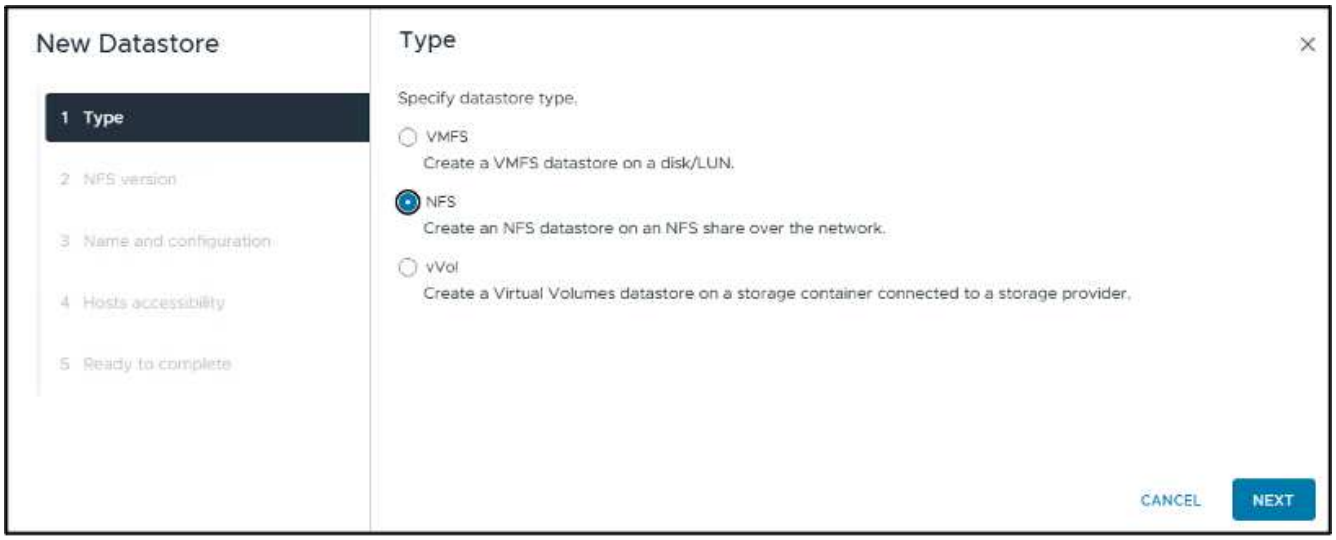
Collegamento di un volume NFS FSx for ONTAP ad Amazon EVS per l'utilizzo come datastore

Ora che il file system FSx for ONTAP è stato predisposto e tutti i parametri di connettività corretti sono stati convalidati, è il momento di collegare un volume di storage FSx for ONTAP ad Amazon EVS. I passaggi seguenti mostrano come accedere a vCenter e montare il volume FSx for ONTAP come datastore NFS:

1. Nel client vSphere, vai alla scheda "Datastore". Trova il Datacenter e vai su Storage > Nuovo Datastore, come mostrato di seguito:

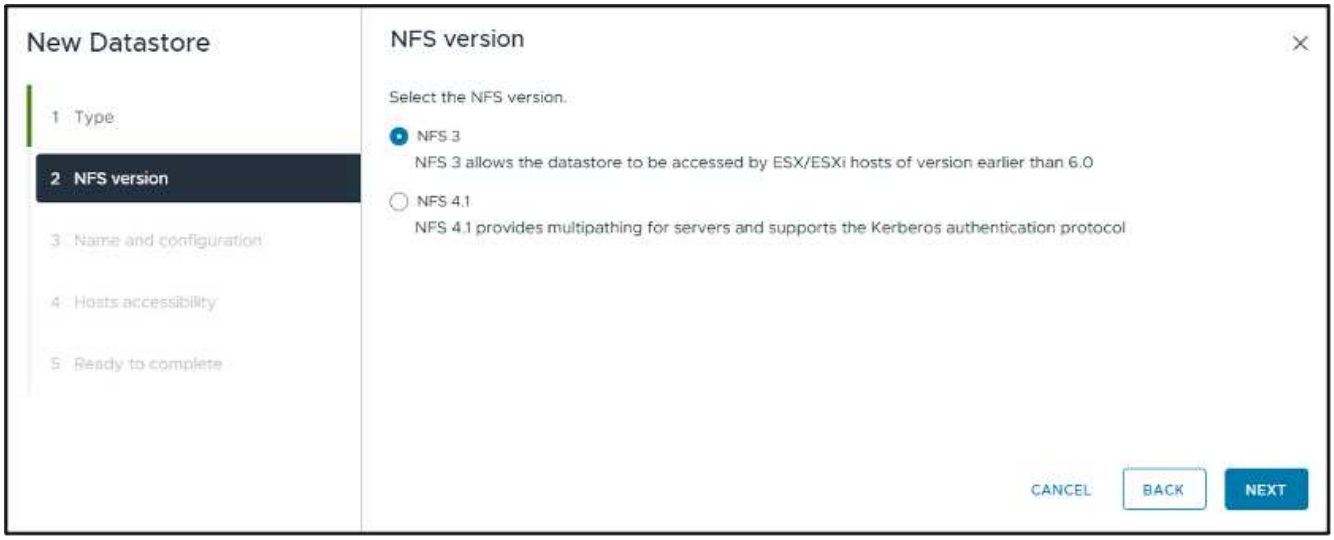


2. Ora ti troverai nella procedura guidata Nuovo Datastore. Nel passaggio "Tipo" dovrai scegliere un tipo di datastore. Selezionare "NFS" e fare clic su "AVANTI" per procedere.



3. Nel passaggio "Versione NFS" selezionerai una versione NFS.

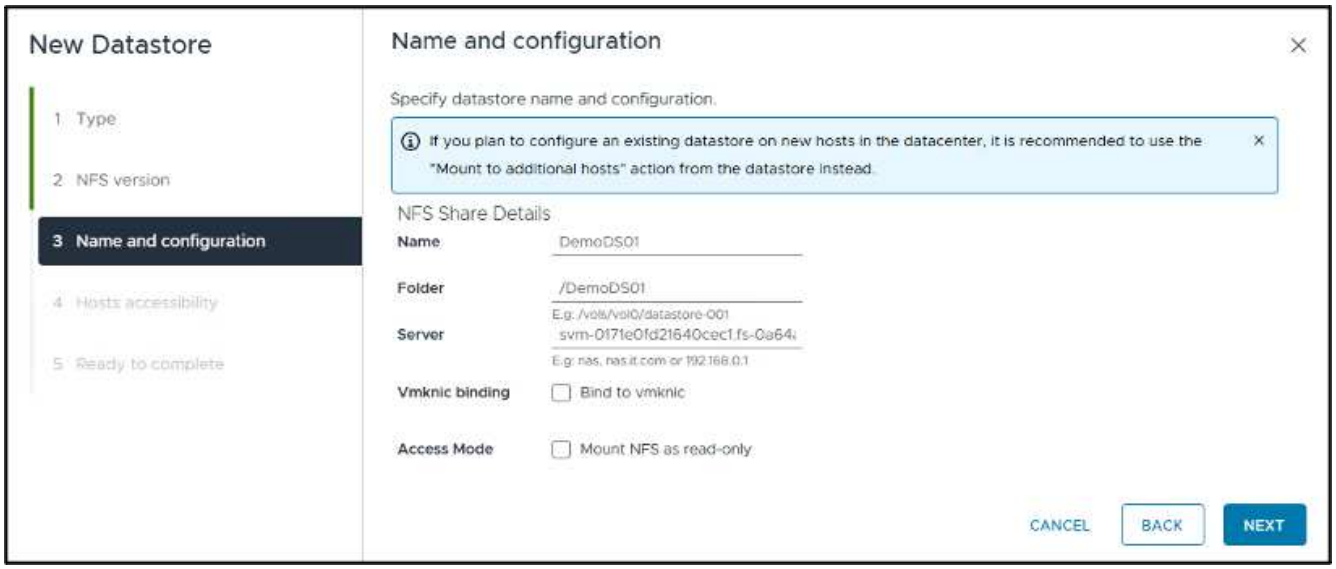
   Ai fini di questo esempio, sceglieremo "NFS 3", ma è importante notare che è possibile utilizzare anche NFS v4.1.



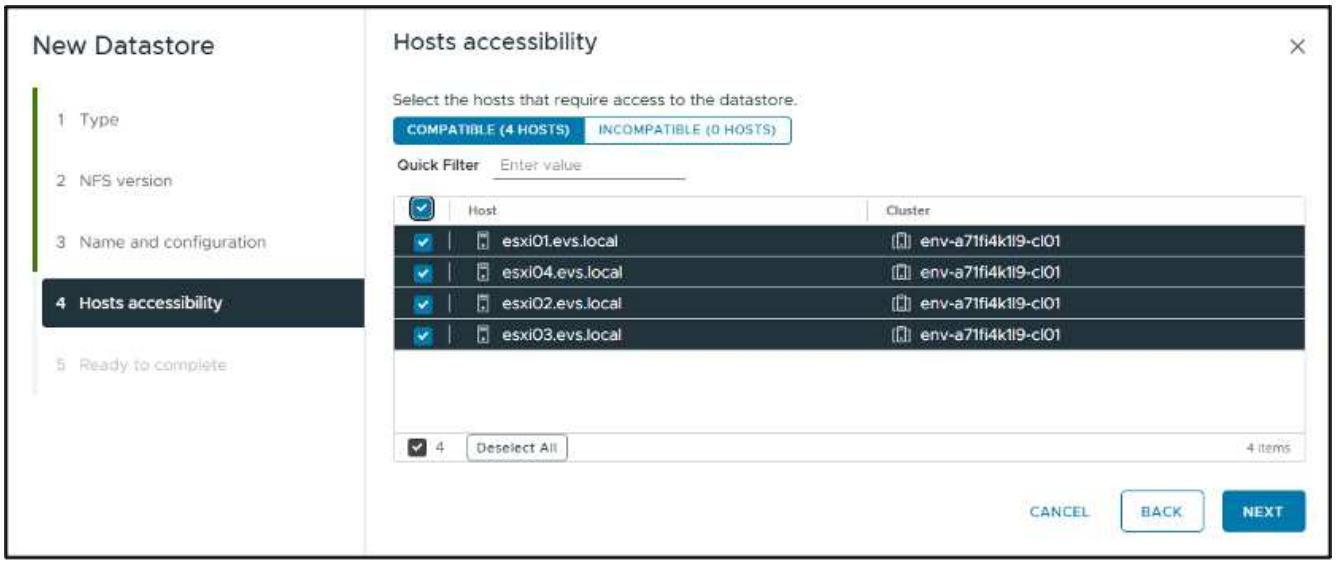
4. Nella fase "Nome e configurazione" dovrai:

   a. Assegna un nome al datastore.
   b. Assegna un nome alla cartella. Utilizzare il percorso di giunzione per il volume NFS.
   c. Assegna un nome al server. Utilizzare il nome DNS NFS della SVM oppure l'indirizzo IP dell'NFS.

      Fare clic su "AVANTI" per continuare.



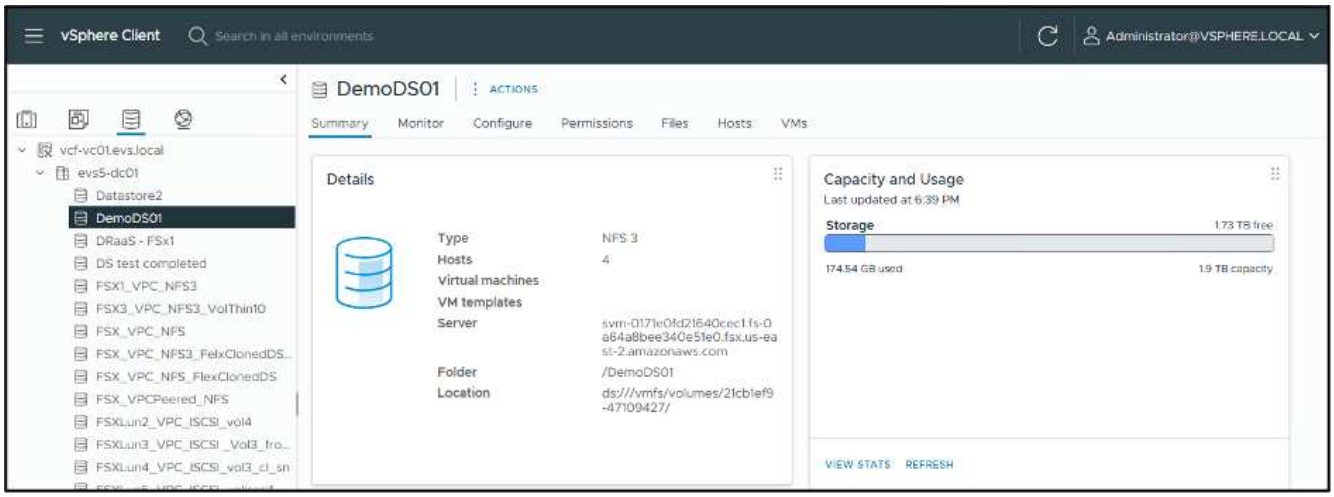
5. Nel passaggio "Accessibilità host", seleziona tutti gli host che richiedono l'accesso al datastore, quindi fai clic su "AVANTI" per continuare.



6. Nella fase "Pronto per il completamento", rivedere i dati e fare clic su "FINISH" per completare la configurazione.



7. Verificare che il datastore NFS sia stato connesso accedendo a vCenter, come mostrato di seguito:



Procedura di distribuzione per l'utilizzo di FSx per ONTAP come datastore iSCSI

Questa sezione illustra i passaggi per configurare un datastore iSCSI utilizzando FSx per ONTAP.

Prerequisiti

Prima di effettuare il provisioning e collegare FSx per ONTAP come datastore iSCSI, è necessario innanzitutto distribuire un ambiente di virtualizzazione Amazon EVS. Per ulteriori informazioni, consultare la documentazione nella guida introduttiva ad Amazon EVS. Questa sezione presuppone inoltre che sia stato distribuito un file system FSx per ONTAP ; consultare la sezione Approccio dettagliato sopra per i passaggi appropriati.

Fasi di distribuzione di alto livello

L'implementazione del file system FSx for ONTAP da utilizzare come datastore iSCSI per Amazon EVS e la creazione della connettività tra i due servizi includeranno i seguenti passaggi:

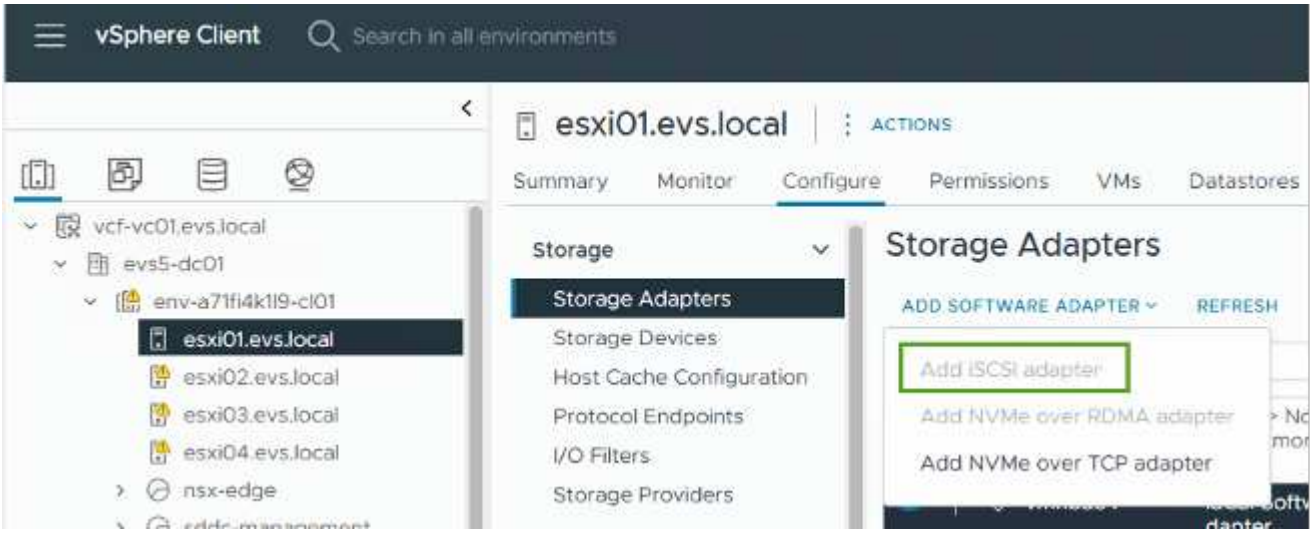
- Configurazione di una scheda di rete iSCSI per ciascun host ESXi.

- Creazione e configurazione del file system FSx per ONTAP , volume, LUN, ecc.
- Connessione degli host ESXi al server del file system FSx for ONTAP .
- Creazione di un file system di macchina virtuale (VMFS) per datastore iSCSI.

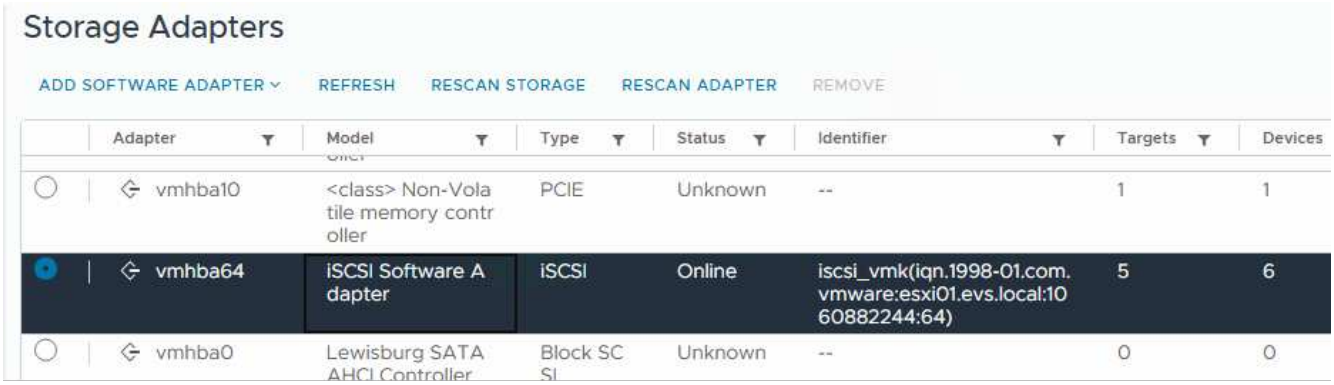
Aggiungi adattatore di rete iSCSI

I seguenti passaggi devono essere eseguiti su ciascun host ESXi nel tuo ambiente.

1. Accedere al client vSphere e selezionare l'host ESXi. Nella scheda Configura, seleziona "Aggiungi adattatore software", quindi seleziona "Aggiungi adattatore iSCSI" dal menu a discesa, come mostrato qui:

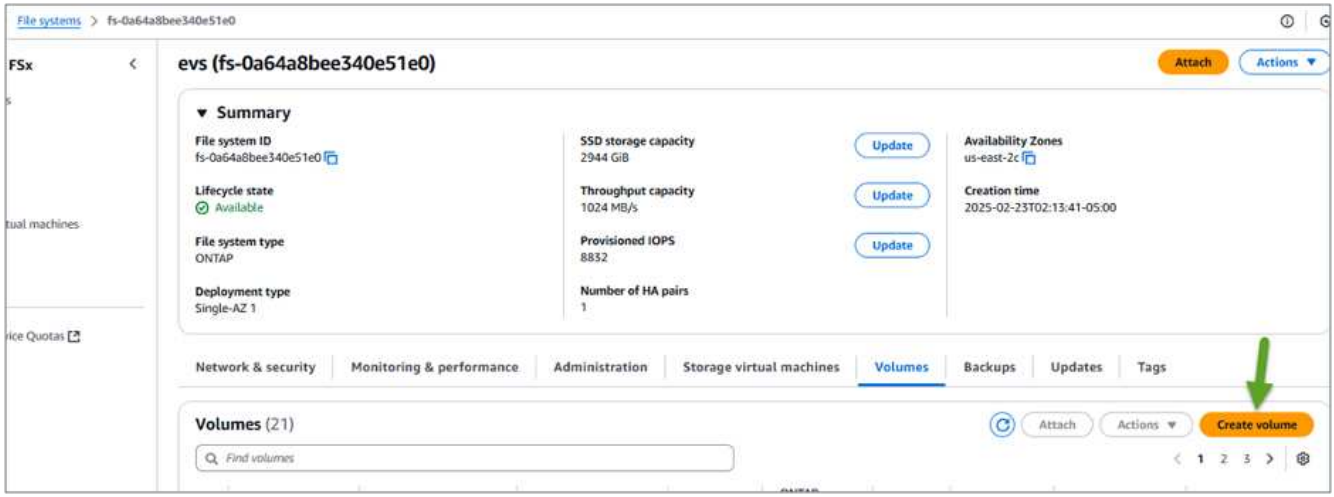


2. Una volta completata l'installazione, ti troverai nella schermata Schede di archiviazione. Selezionare "Riscansiona adattatore" dalla barra dei menu. Registrare l'IQN dell'adattatore iSCSI: iqn.xxxx. Questo valore verrà utilizzato in seguito nella fase di mappatura LUN.



Creare un volume FSx per ONTAP

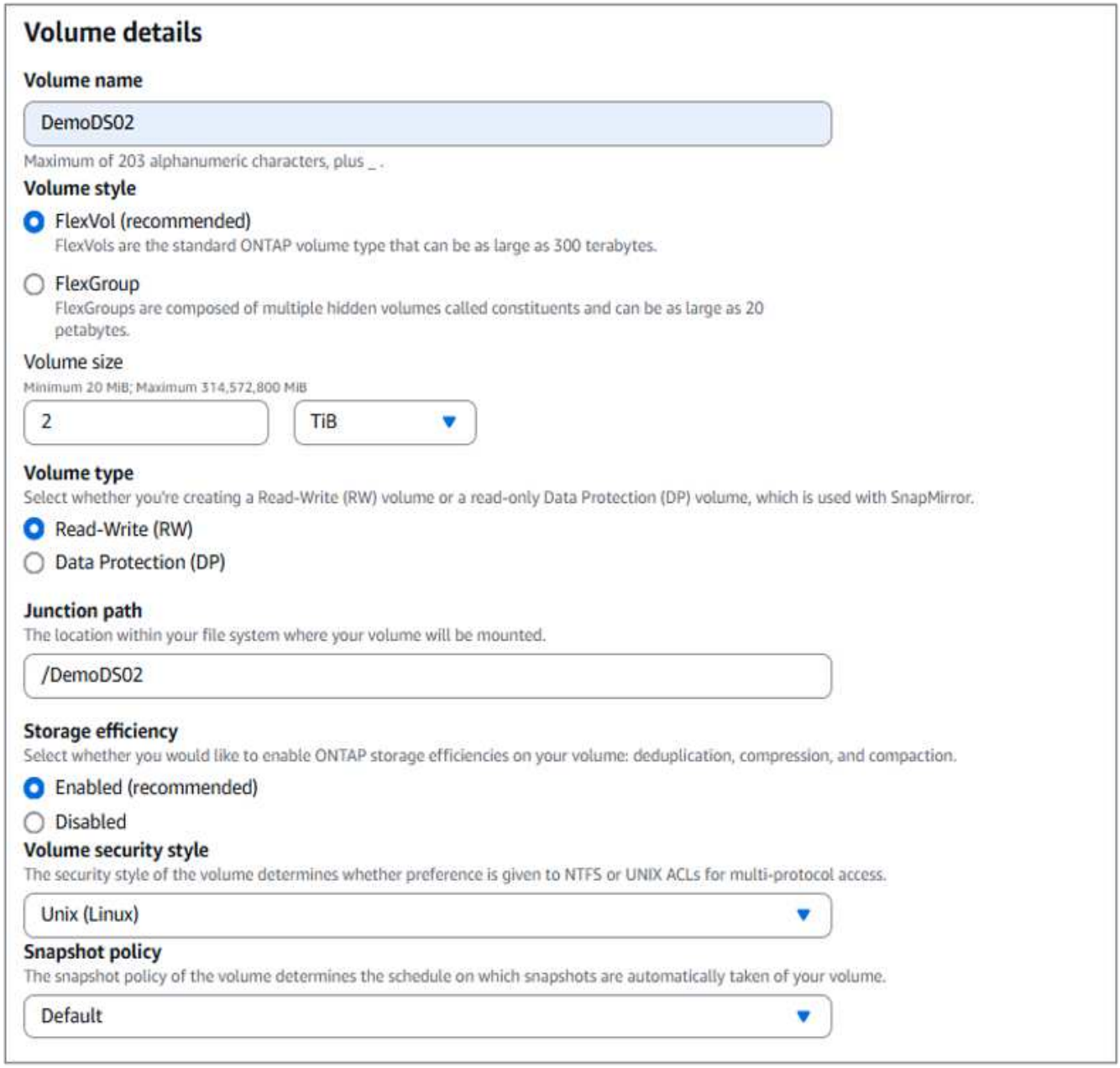
1. Vai alla console AWS, accedi alla pagina del tuo file system FSx for ONTAP e fai clic su "Crea volume".



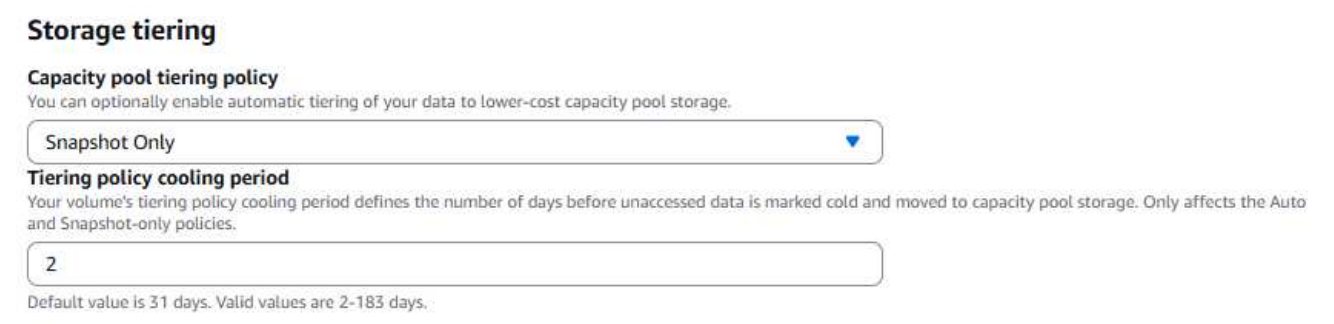
2. Selezionare l'SVM in cui si desidera creare il volume.



3. Nella pagina "Dettagli volume", inserisci i dettagli come mostrato nello screenshot qui sotto. Una volta terminato, fare clic su "Crea" per impostare il volume. Selezionare "Abilitato" per attivare le funzionalità di efficienza di archiviazione ONTAP (compressione, deduplicazione e compattazione).



4. Per l'opzione di suddivisione in livelli di archiviazione, seleziona "Solo snapshot" dal menu a discesa e imposta un periodo di raffreddamento per la politica di suddivisione in livelli. L'impostazione predefinita è 31 giorni, ma in questo esempio abbiamo impostato un periodo di raffreddamento di due giorni.



5. Una volta creato il volume, utilizzare ONTAP CLI per impostare i seguenti valori:

Collocamento	Configurazione
Garanzia di volume	Nessuno (thin provisioning)
riserva frazionaria	0%
snap_reserve	0%
Autodimensionamento	crescere_ridurre
Efficienza di archiviazione	Abilitato
Politica di suddivisione in livelli del volume	Solo istantanea
Aggiornamento dell'ora di accesso (-atime-update)	Falso
Lettura minima anticipata (-min-readahead)	Falso
Politica di snapshot	Nessuno
Prenotazione dello spazio LUN	Disabili
Assegnazione dello spazio LUN	Abilitato

Creare un LUN, un igroup e mappare il LUN

In questa sezione mostreremo come creare la LUN che apparirà come disco in vSphere. Mostreremo anche come creare un gruppo di iniziatori (igroup), ovvero l'elenco degli iniziatori che hanno accesso alla LUN. L'igroup consentirà l'accesso alla LUN dagli host vSphere ESXi. Infine, mostreremo come mappare l'igroup sulla LUN.

1. Per accedere alla CLI ONTAP , stabilire una sessione SSH sulla porta di gestione del file system FSx for ONTAP o SVM eseguendo il seguente comando:

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. Creare il LUN. Assicurati di abilitare l'allocazione e la prenotazione dello spazio. La dimensione dovrebbe essere fino al 90% della dimensione del volume:

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. Creare l'igroup e aggiungere l'IQN di tutti gli host ESXi all'interno del cluster.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. Mappare la LUN con il seguente codice:

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. Esaminare la mappatura LUN e verificare che lo stato sia stato modificato in "mappato". Si tratta di un doppio controllo necessario per assicurarsi che la LUN sia in uno stato mappato:

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

Ottenere informazioni sulla configurazione iSCSI dall'SVM

1. Eseguire iSCSI Show e registrare il nome della destinazione. Verrà utilizzato nella scoperta vSphere dei dischi FSx for ONTAP (Nota: questo nome di destinazione è univoco per la tua SVM):

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. Registrare gli indirizzi IP iSCSI:

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

Scopri il server iSCSI FSx per ONTAP

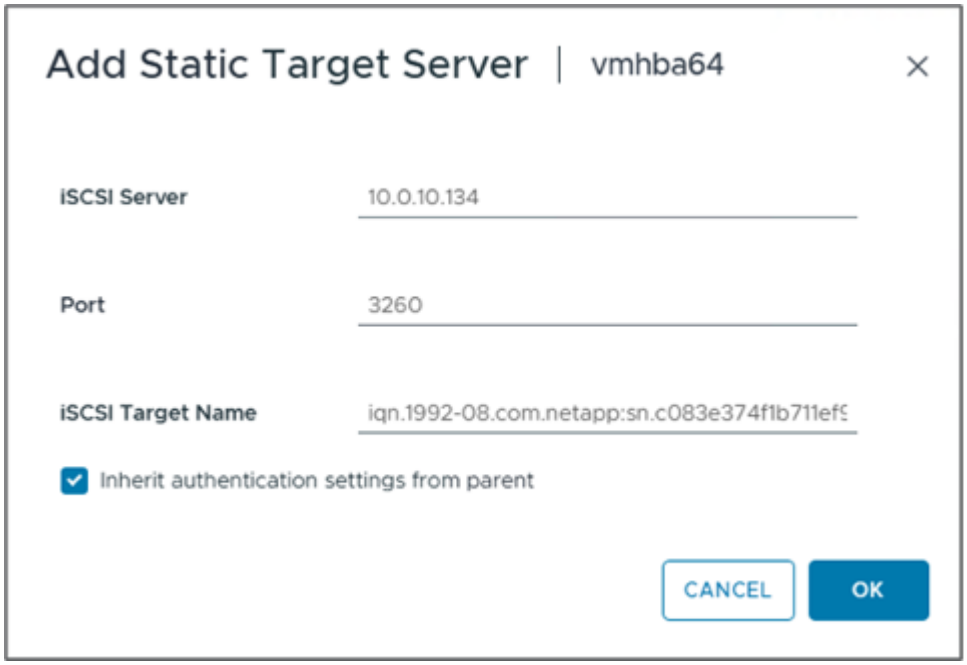
Ora che abbiamo mappato la LUN, possiamo individuare il server iSCSI FSx for ONTAP per l'SVM. Tieni presente che per ogni host ESXi presente nel tuo SDDC dovrai ripetere i passaggi elencati qui.

1. Innanzitutto, assicurarsi che il gruppo di sicurezza collegato al file system FSx for ONTAP (ovvero quello collegato all'ENI) consenta le porte iSCSI.

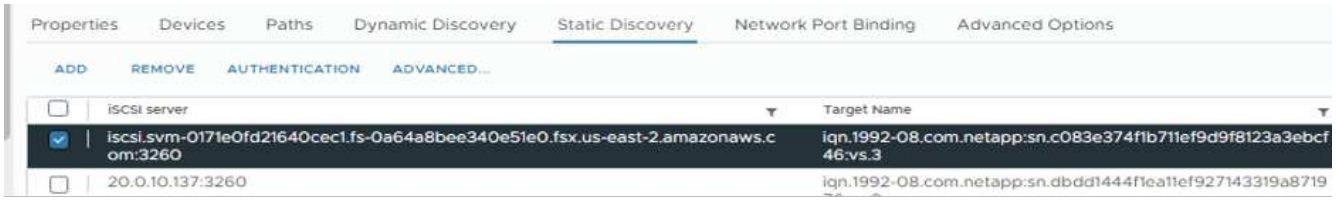
   Per un elenco completo delle porte del protocollo iSCSI e come applicarle, fare riferimento a"Controllo

degli accessi al file system con Amazon VPC" .

2. Nel client vSphere, vai su Host ESXi > Schede di archiviazione > Rilevamento statico e fai clic su "Aggiungi".
3. Immettere l'indirizzo IP del server iSCSI indicato sopra (la porta è 3260). Il nome della destinazione iSCSI è l'IQN del comando iSCSI show. Fare clic su "OK" per procedere.



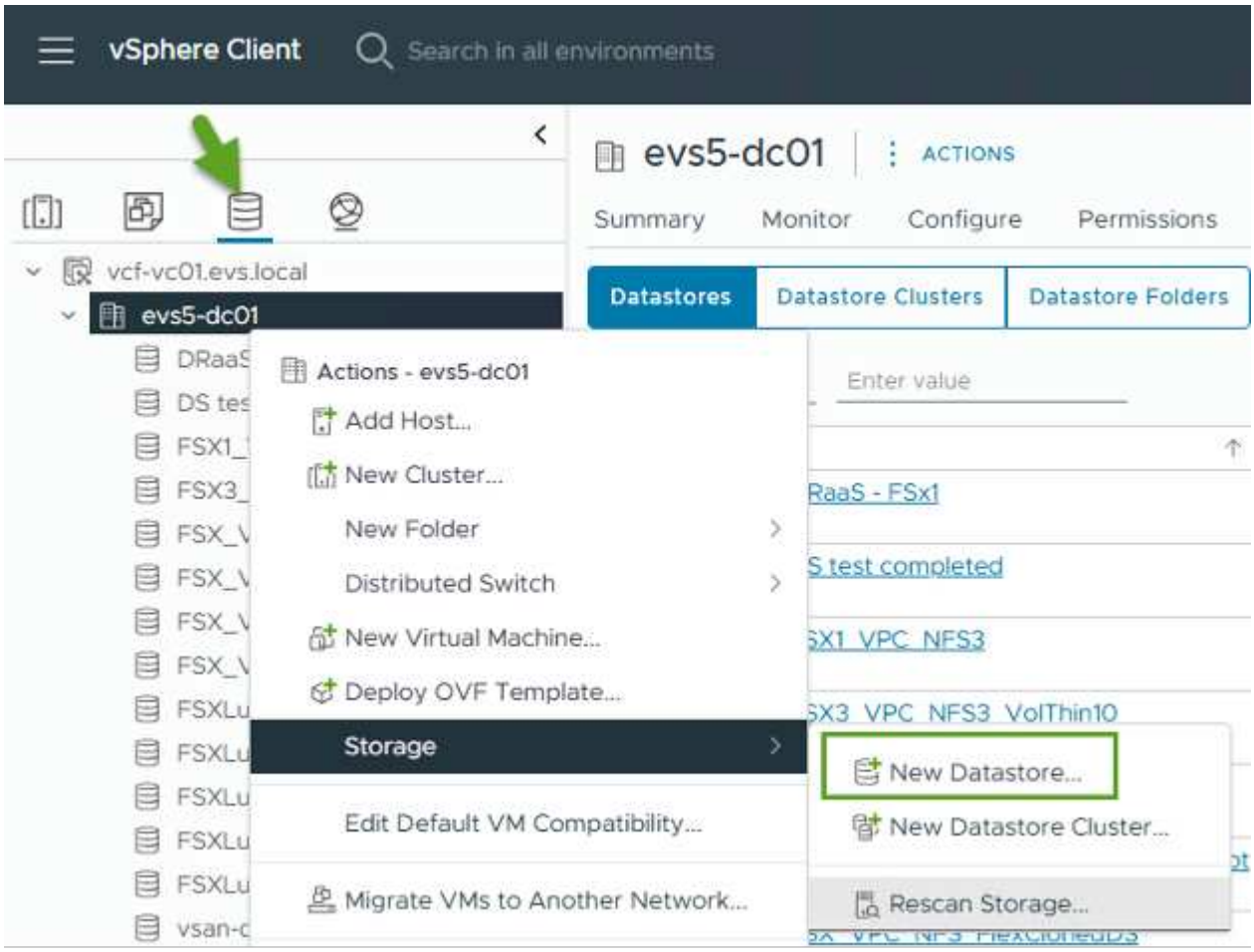
4. La procedura guidata si chiuderà e verrà visualizzata la schermata Datastore Static Discovery. Nella tabella presente in questa pagina potrai verificare che l'obiettivo sia stato scoperto.



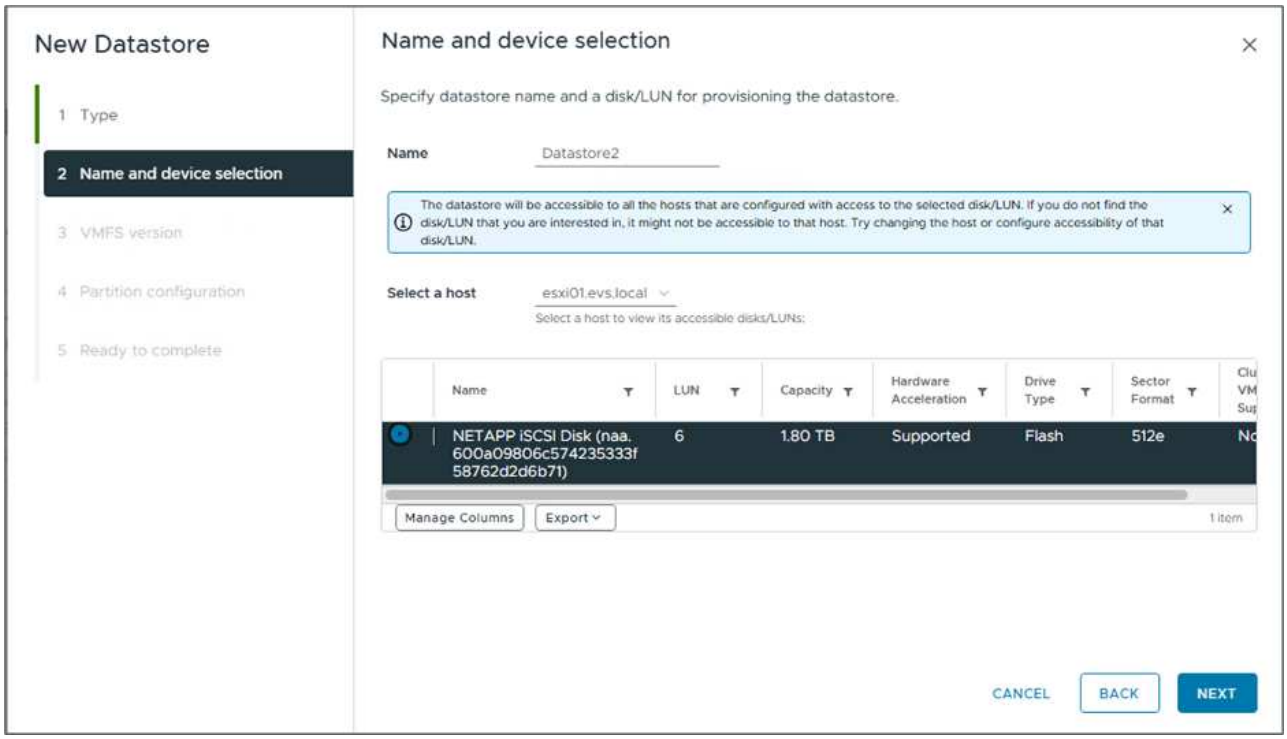
Creare un datastore iSCSI

Ora che abbiamo individuato il server iSCSI, possiamo creare un datastore iSCSI.

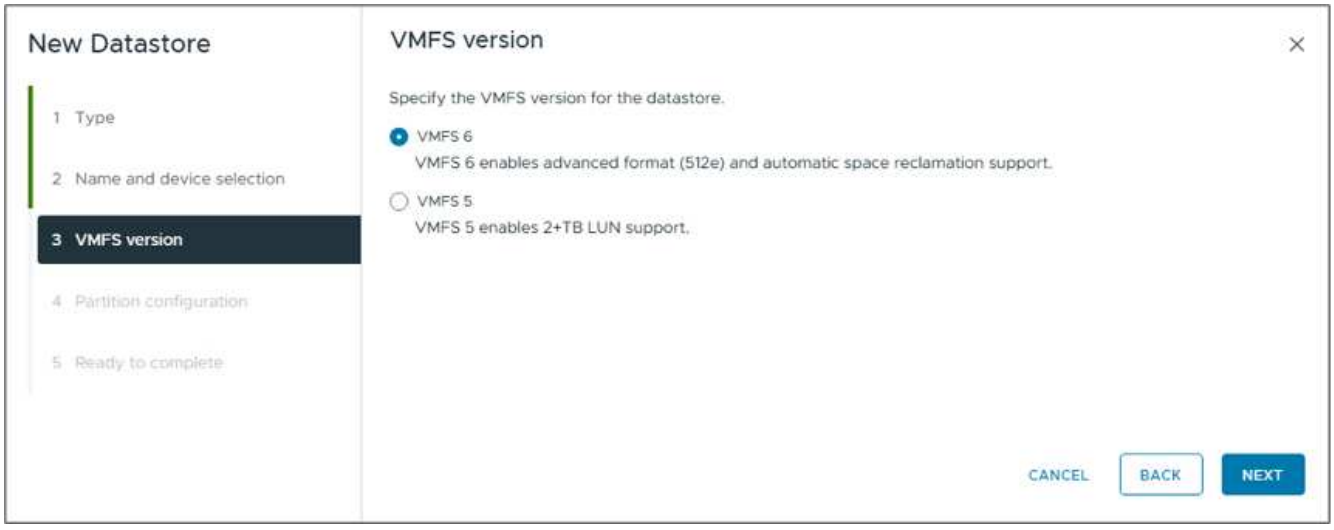
1. Nel client vSphere, vai alla scheda Datastore e seleziona l'SDDC in cui desideri distribuire il datastore. Fare clic con il pulsante destro del mouse e selezionare l'icona Archiviazione (indicata dalla freccia verde nello screenshot qui sotto), quindi selezionare "Nuovo Datastore" dal menu a discesa:



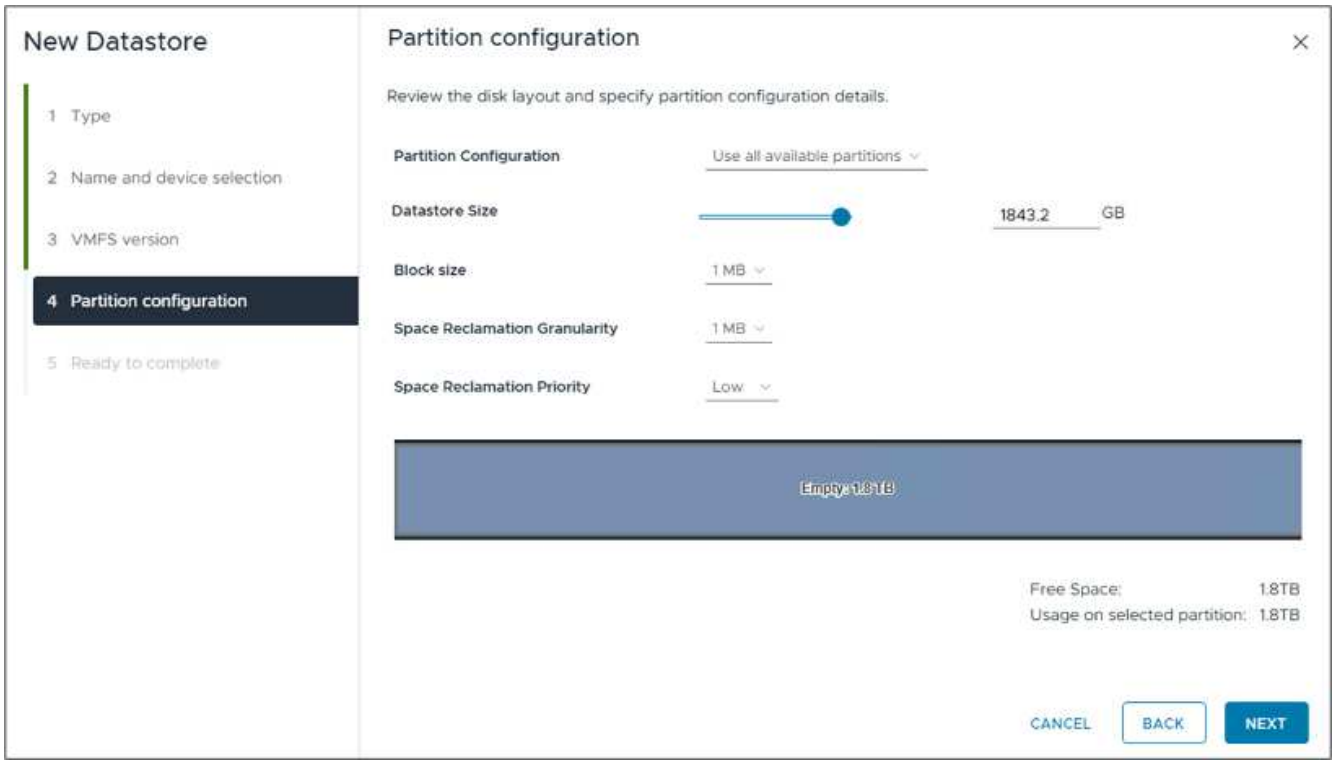
2. Ora ti troverai nella procedura guidata Nuovo Datastore. Nel passaggio "Tipo", selezionare l'opzione VMFS.
3. Nella fase "Selezione nome e dispositivo":
   a. Fornisci un nome per il tuo datastore.
   b. Seleziona l'host ESXi a cui vuoi connetterti al datastore.
   c. Selezionare il disco rilevato (LUN) e fare clic su "Avanti".



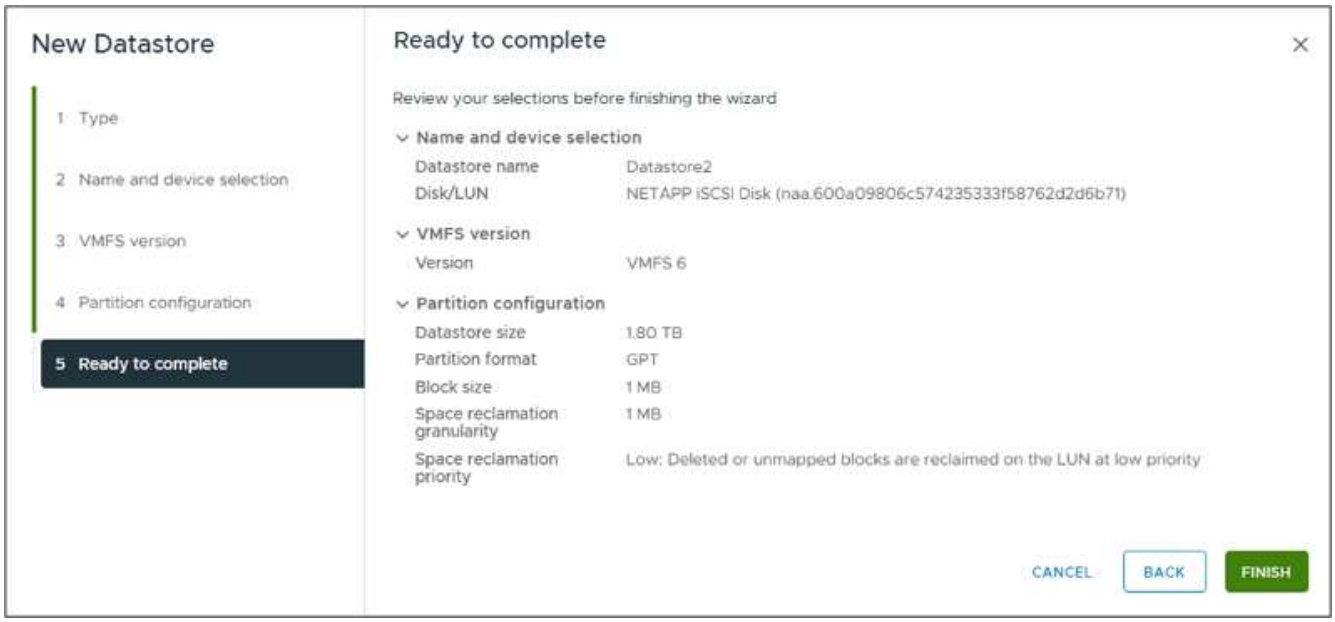
4. Nel passaggio "Versione VMFS", seleziona "VMFS 6".



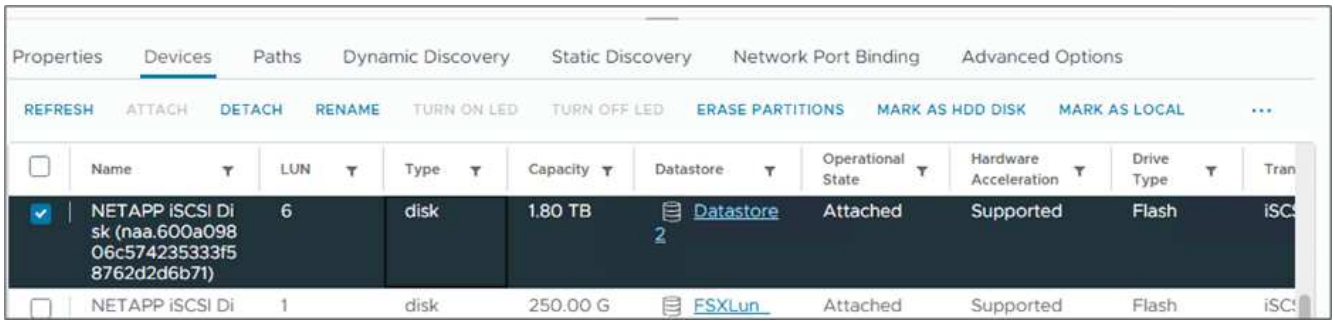
5. Nel passaggio "Configurazione partizione", lasciare invariate le impostazioni predefinite, inclusa l'opzione "Usa tutte le partizioni disponibili". Fare clic su "Avanti" per procedere.



6. Nella fase "Pronto per il completamento", assicurati che le impostazioni siano corrette. Una volta terminato, clicca su "FINISH" per completare la configurazione.



7. Torna alla pagina Dispositivi e verifica che il datastore sia stato collegato.



Conclusione

In questo documento sono fornite istruzioni su come configurare FSx per ONTAP come storage esterno per Amazon EVS da utilizzare con i protocolli NFS e iSCSI.

L'utilizzo di FSx per ONTAP come storage esterno per Amazon EVS offre chiari valori operativi e aziendali. Fornisce una migliore resilienza dei dati, protezione, replicazione ed efficienza dei costi tramite la tecnologia ONTAP e mantiene il TCO ottimizzato grazie al disaccoppiamento dell'architettura iperconvergente VMware. Con FSx per ONTAP, gli utenti di Amazon EVS possono scalare lo storage senza aggiungere risorse di elaborazione e senza aumentare i costi. Ciò consente di sfruttare appieno il potenziale di elasticità e scalabilità offerto dal cloud AWS.

Per saperne di più, leggi l'annuncio delle novità di Amazon:"Amazon EVS ora si integra con FSx per ONTAP" e il blog NetApp :"Amazon EVS annuncia il supporto per FSx per ONTAP" .

Proteggi il datastore FSx ONTAP per EVS

Come proteggere Amazon FSx for NetApp ONTAP datastores con Amazon Elastic VMware Service utilizzando NetApp SnapCenter Plug-in for VMware

Questa guida illustrerà un semplice approccio di distribuzione per la protezione di FSx for ONTAP Network File System (NFS) e iSCSI Amazon EVS datastore e delle relative VM utilizzando la soluzione di backup e recovery NetApp SnapCenter® Plug-in for VMware vSphere (SCV) per VM.

Introduzione

Amazon FSx for NetApp ONTAP (FSx for ONTAP)-based archivi dati supplementari per Amazon Elastic VMware Service (Amazon EVS) offrono un'eccellente soluzione per l'esecuzione sia di carichi di lavoro che richiedono prestazioni elevate—come lo sfruttamento di nConnect, il peering di Amazon Virtual Private Cloud (Amazon VPC) e l'utilizzo di più connessioni di rete per ogni montaggio dell'archivio dati—sia di carichi di lavoro che richiedono un uso intensivo di storage.

Questa funzionalità consente ai clienti di superare i limiti dello storage locale dell'istanza fornito da una virtual storage area network (vSAN), di scalare lo storage indipendentemente dal compute e di ridurre il costo totale di proprietà. Oltre ai vantaggi in termini di total cost of ownership (TCO), FSx for ONTAP offre ad Amazon EVS funzionalità enterprise-grade familiari ai clienti di ONTAP on-premises®, contribuendo a ottimizzare e semplificare le distribuzioni. L'utilizzo di FSx for ONTAP consente di accedere alle tecnologie NetApp® Snapshot™, SnapMirror® e SnapVault® che supportano operazioni di backup e ripristino per macchine virtuali (VM), datastore e dischi di macchine virtuali (VMDK). Una delle funzionalità chiave è la protezione basata su Snapshot.

Panoramica

Con la crescita e il consolidamento degli ambienti aziendali, la necessità di proteggere i carichi di lavoro e lo storage sottostante diventa sempre più importante. SCV può essere utilizzato per eseguire il backup di datastore e macchine virtuali direttamente dal client Amazon EVS vSphere.

Scopo di questa guida

Questa guida fornisce istruzioni su come proteggere un datastore Amazon FSx for NetApp ONTAP per Amazon EVS utilizzando SCV. Vengono forniti esempi di scenari di protezione di VM e database, nonché di restore.

Pubblico

Questo tutorial è destinato ad architetti e amministratori cloud che hanno familiarità con VMware vSphere, Amazon EVS, AWS Console e FSx per ONTAP.

Passaggi high-level per la distribuzione e la configurazione

Di seguito sono riportati i high-level passaggi per distribuire e configurare SCV per proteggere le VM e i datastore su Amazon EVS:

1. Scarica l'SCV Open Virtual Appliance (OVA).
2. Accedi con le credenziali vSphere Client ad Amazon EVS.
3. Distribuire un modello Open Virtualization Format (OVF) per avviare la procedura guidata di distribuzione VMware.
4. Per accedere al plug-in, selezionare SnapCenter Plug-in for VMware dal menu.
5. Aggiungi storage.
6. Crea policy di backup.
7. Crea gruppi di risorse.
8. Eseguire il backup dei gruppi di risorse.
9. Ripristina l'intera macchina virtuale o un disco virtuale specifico o i file guest.

Procedura di installazione per SnapCenter Plug-in per VMware

Questa sezione illustra i passaggi per configurare il SnapCenter Plug-in per VMware.

Prerequisiti

Prima di iniziare sono richiesti i seguenti prerequisiti:

1. Per registrare il server vCenter durante la distribuzione dell'OVA, specificare il fully qualified domain name (FQDN) o l'indirizzo IP del vCenter.
2. Per le credenziali vCenter, utilizzare un account con i privilegi minimi richiesti
3. Aprire le porte del firewall per l'accesso al server vCenter.
4. Aggiorna il gruppo di sicurezza dell'Amazon VPC in cui FSx for ONTAP è in esecuzione per consentire l'accesso SCV a FSx for ONTAP.



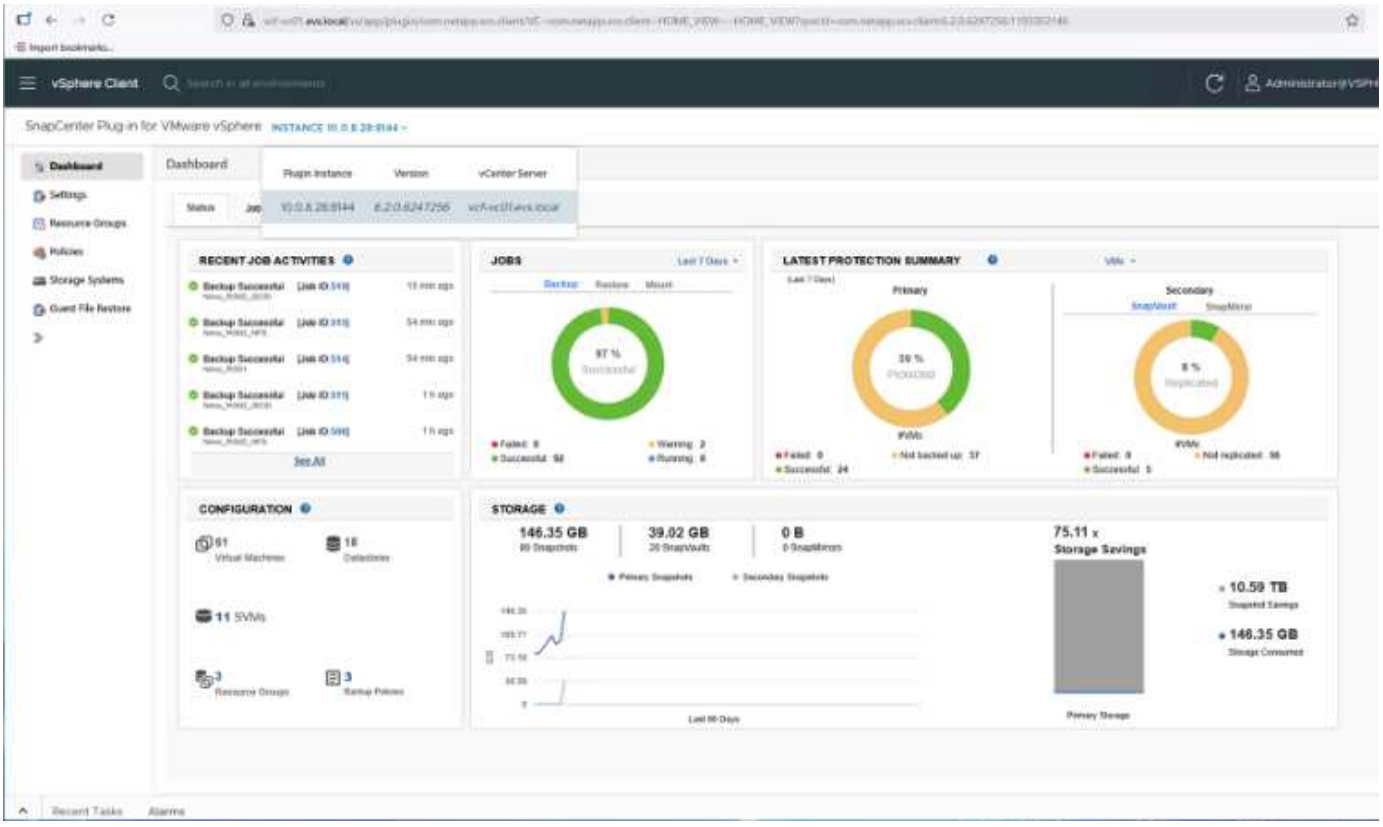
SCV è disponibile gratuitamente.

Configurazione del SnapCenter Plug-in per VMware

Per proteggere le VM e i datastore basati su NFS/iSCSI che le ospitano, è necessario implementare SCV. Si tratta di una semplice importazione OVF.

I passaggi per la distribuzione sono i seguenti:

1. Scarica l'OVA da "Sito di supporto NetApp".
2. Accedi ad Amazon EVS vCenter.
3. All'interno di vCenter, fai clic con il pulsante destro del mouse su qualsiasi oggetto dell'inventario, come un data center, una cartella, un cluster o un host e seleziona "Distribuisci modello OVF".
4. Seleziona le impostazioni corrette, inclusi archiviazione, segmentazione e personalizzazione del modello per aggiornare il vCenter e le sue credenziali, creare le credenziali SCV e i dettagli IP. Una volta verificato, seleziona "Fine".
5. Attendere il completamento delle attività di importazione e distribuzione OVF.
6. Una volta che SCV è stato distribuito correttamente, verrà registrato all'interno di vCenter.
7. Per accedere al plug-in, vai alla barra laterale sinistra della pagina del client web vCenter e seleziona ""SnapCenter Plug-in for VMware".



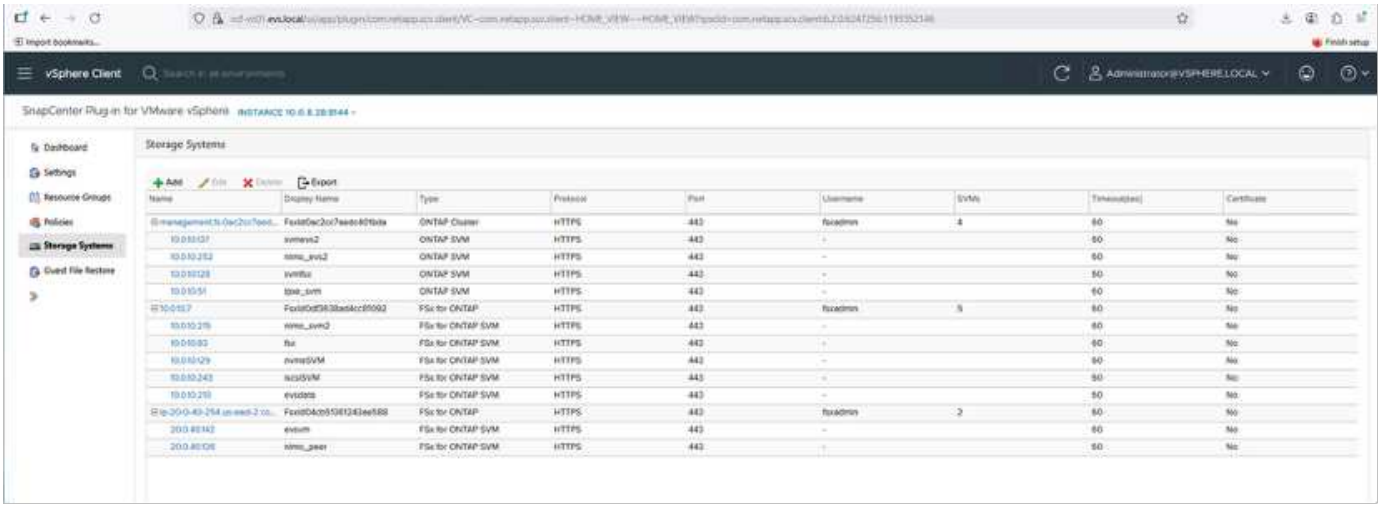
Procedura di configurazione per SnapCenter Plug-in per VMware

Questa sezione illustra i passaggi per configurare il SnapCenter Plug-in for VMware. Le sezioni seguenti spiegheranno in dettaglio come aggiungere storage, creare una policy di backup e come creare gruppi di risorse.

Aggiunta del sistema storage

Il passaggio successivo nella protezione dei carichi di lavoro con SVC è aggiungere il "sistema storage". L'aggiunta dello storage consente a SCV di rilevare e gestire le operazioni di backup e ripristino all'interno di vCenter. Includere l'endpoint di gestione FSx for NetApp ONTAP o l'IP dell'endpoint di amministrazione della storage virtual machine (SVM) come sistema storage per abilitare backup e ripristino.

1. Dal menu di navigazione a sinistra dell'EVS vCenter, selezionare "SnapCenter Plug-in for VMware".
2. Selezionare "Storage System".
3. Selezionare "Aggiungi" per aggiungere i dettagli FSx for ONTAP.
4. Utilizza il metodo "Credenziali come autenticazione" e inserisci FSxadmin come nome utente e password. Quindi seleziona "Aggiungi" per salvare le impostazioni.



Tutte le SVM vengono aggiunte automaticamente quando il file system viene aggiunto.

Se la versione SCV è 6.2, vai su "la pagina di supporto SCV" e scarica la release SCV 6.2P1.

Crea una policy di backup

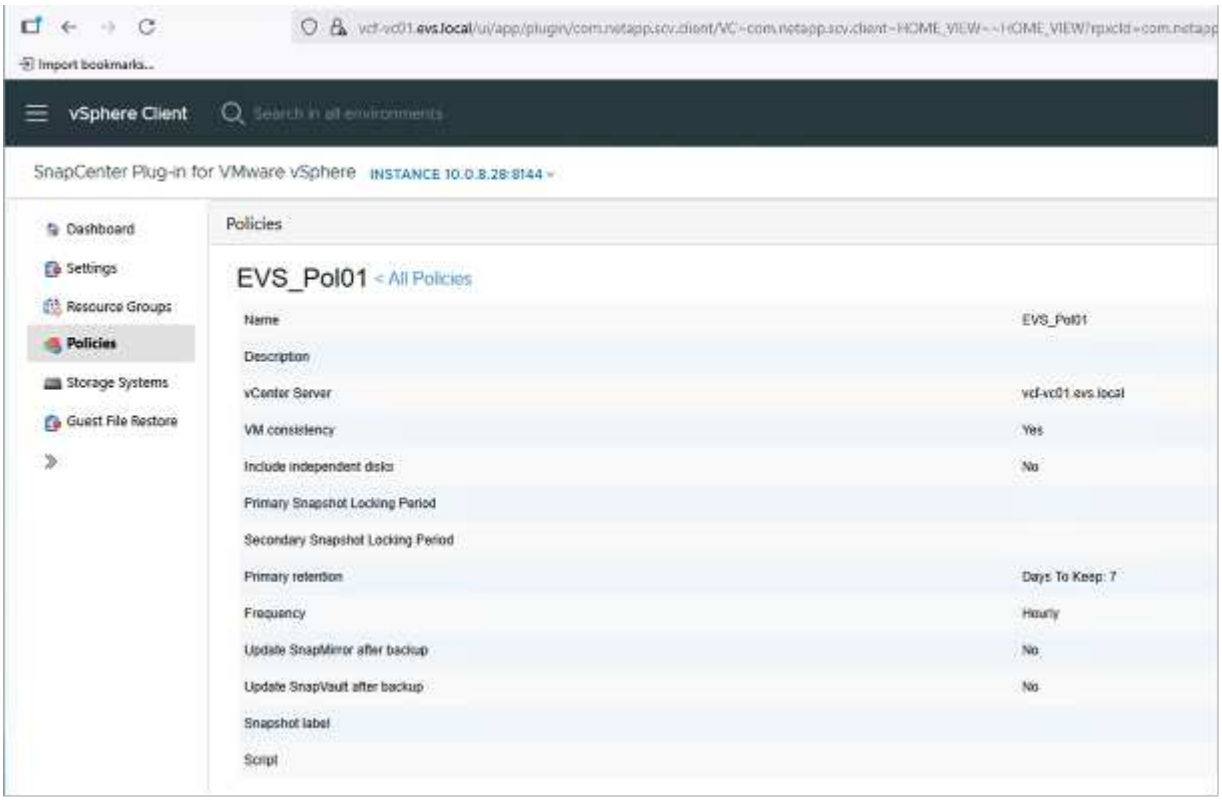
Una solida strategia di backup dovrebbe definire fattori chiave come la pianificazione dei backup, i dati da sottoporre a backup e il periodo di conservazione dei backup. Le copie Snapshot possono essere pianificate su base oraria o giornaliera per proteggere interi datastore. Pianificare i backup in questo modo non solo protegge i datastore, ma supporta anche le operazioni di backup e ripristino per le VM e i VMDK contenuti in tali datastore.

Prima di avviare i backup per VM e datastore, crea "policy di backup" e un gruppo di risorse. La policy di backup specifica parametri come la pianificazione dei backup e le impostazioni di conservazione.

Ecco i passaggi per creare una policy di backup:

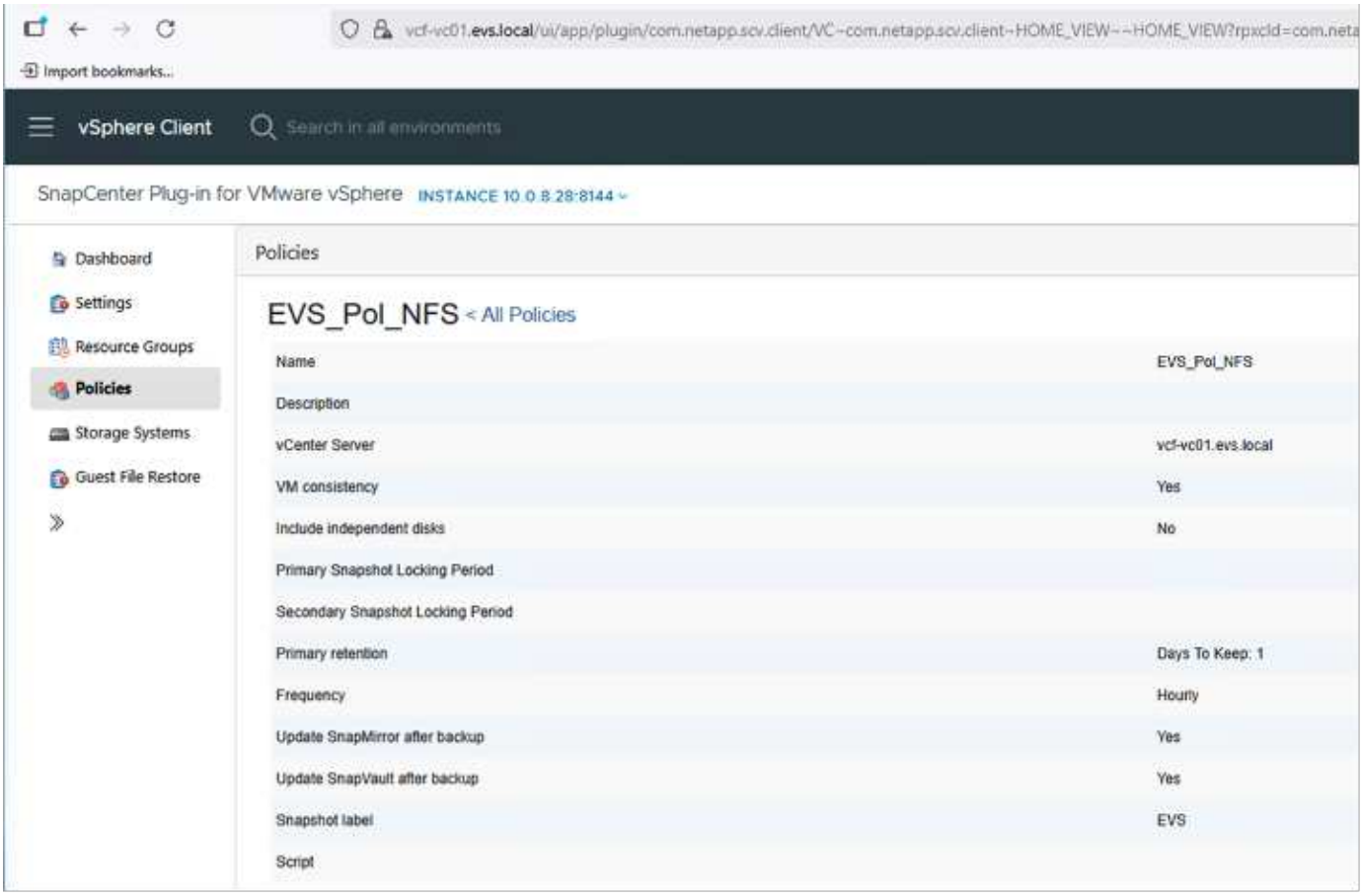
1. Vai al menu di navigazione a sinistra in SCV e seleziona "Policies".
2. Nella pagina Policies, seleziona "Create" per avviare la procedura guidata.
3. Nella pagina "New Backup Policy page", immettere un nome per la policy.
4. Specificare il periodo di conservazione, la frequenza di backup e le impostazioni di replica.
5. Seleziona la casella di controllo "Locking Period" per abilitare il blocco degli Snapshot. Puoi selezionare i periodi di blocco degli Snapshot primario e secondario come Giorni/Mesi/Anni.

Indipendentemente dal valore di conservazione definito nella policy SnapMirror, la copia Snapshot secondaria rimane intatta fino alla scadenza del periodo di blocco dello snapshot secondario specificato.



Per abilitare i backup coerenti con la VM, VMware tools devono essere installati e in esecuzione. Quando la casella di coerenza VM è selezionata, le VM vengono prima messe in quiescenza, quindi VMware esegue uno snapshot coerente con la VM (escludendo la memoria), poi SCV esegue la sua operazione di backup e infine le operazioni della VM vengono riprese.

Per replicare le copie Snapshot su un mirror secondario o su un file system di vault, le relazioni devono essere configurate in anticipo.



Una volta creata la policy, il passaggio successivo consiste nel creare il gruppo di risorse che definirà i datastore NFS o iSCSI e le VM appropriate di cui eseguire il backup.

Crea un gruppo di risorse

Un gruppo di risorse funge da container per le VM e i datastore che necessitano di protezione. Le risorse possono essere aggiunte o rimosse da un gruppo di risorse in qualsiasi momento, garantendo flessibilità nella gestione delle configurazioni di backup.

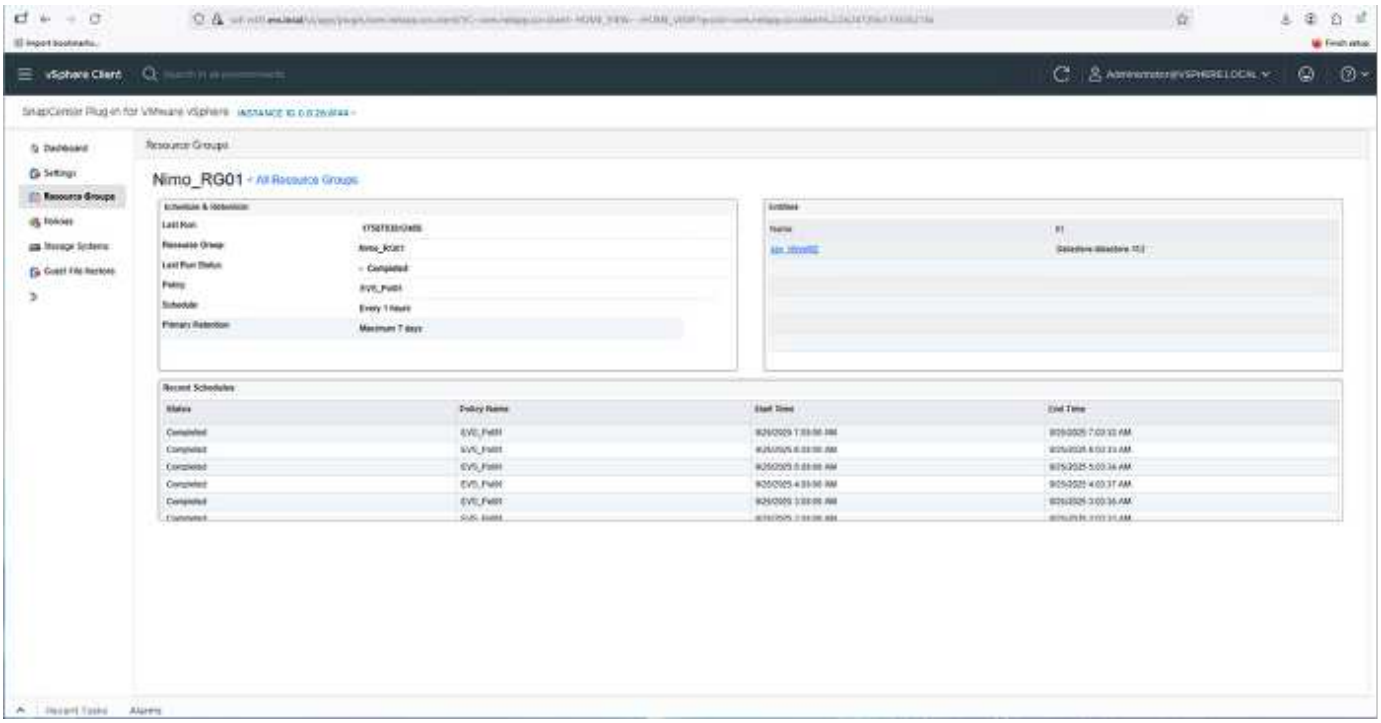
Puoi creare un "gruppo di risorse" utilizzando i seguenti passaggi:

1. Vai al riquadro di navigazione a sinistra in SCV e seleziona "Resource Groups".
2. Nella pagina Resource Groups, seleziona "Create" per avviare la procedura guidata di creazione del resource group.

> Un'altra opzione per creare gruppi di risorse è selezionare una singola VM o un singolo datastore e creare un gruppo di risorse che contenga solo quella risorsa.

3. Nella pagina "Risorse", seleziona l'ambito (VMs o datastores) e il data center.
4. Nella pagina "Spanning disks", seleziona l'opzione "Virtual Machines with multiple VMDKs across multiple datastores".
5. Successivamente, associa una policy di backup. Seleziona una policy di backup esistente o creane una nuova.
6. Nella pagina "Pianificazioni", configura la pianificazione del backup per ogni policy selezionata.

7. Dopo aver effettuato le selezioni appropriate, seleziona "Fine". Questo creerà un nuovo gruppo di risorse e lo aggiungerà all'elenco dei gruppi di risorse.



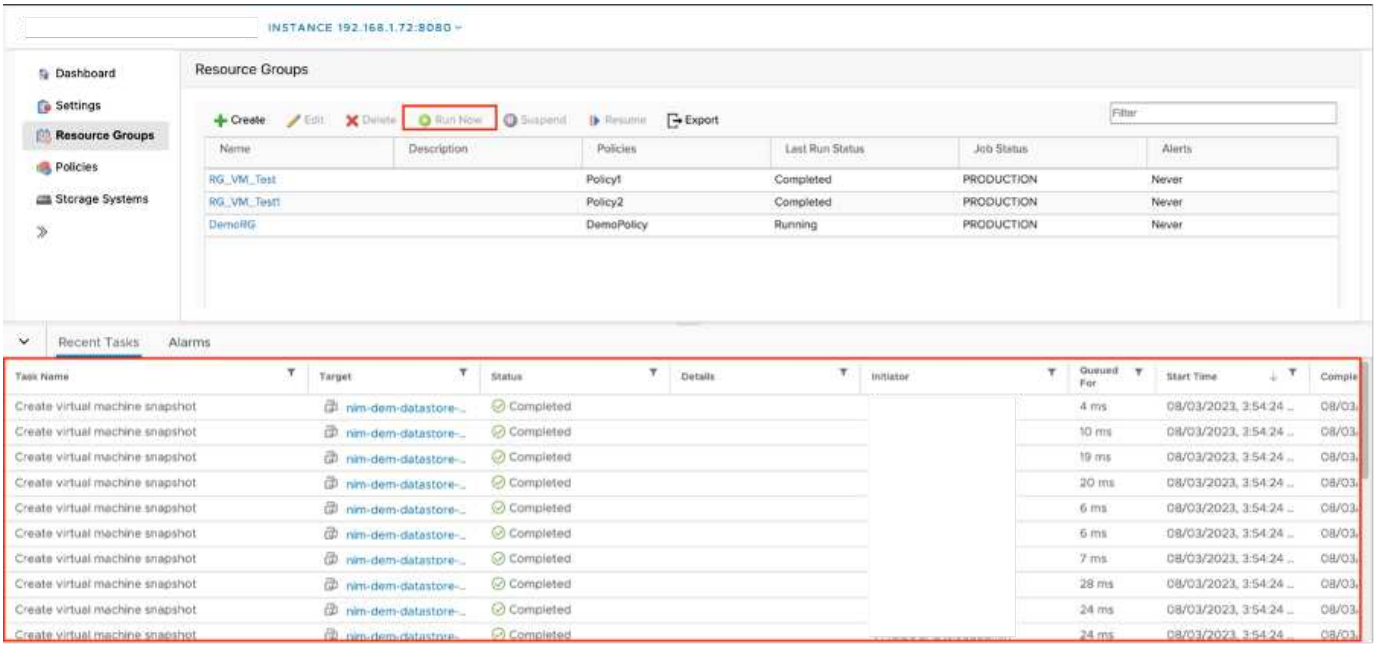
Backup dei gruppi di risorse

Le operazioni di backup vengono eseguite su tutte le risorse definite all'interno di un gruppo di risorse. Se a un gruppo di risorse è associata una policy e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

1. Nella barra di navigazione a sinistra della pagina del client web vCenter, seleziona "SnapCenter Plug-in for VMware" e poi "Resource Groups".
2. Nella pagina Resource Groups, trova il resource group designato e seleziona "Run Now" per avviare il backup manuale.



3. Se per il gruppo di risorse sono configurate più policy, selezionare la policy per l'operazione di backup nella finestra di dialogo "Backup Now".
4. Seleziona "OK" per avviare il backup.

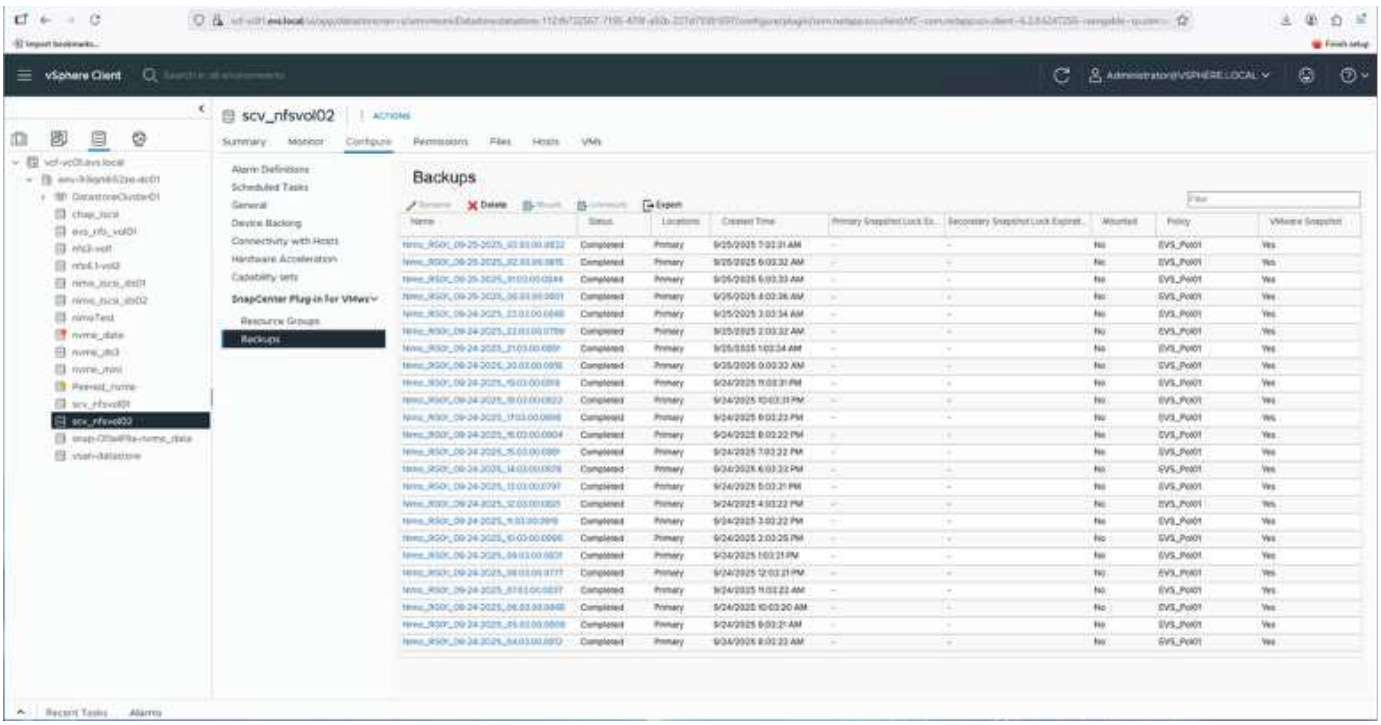


Monitora l'andamento dell'operazione selezionando "Recent Tasks" nella parte inferiore della finestra oppure, per maggiori dettagli, selezionando "Job Monitor" nella dashboard.

Il processo per la creazione di policy di backup, la configurazione di gruppi di risorse e l'esecuzione di operazioni di backup è coerente tra i diversi protocolli di storage, inclusi NFS e iSCSI.

I backup vengono eseguiti secondo la pianificazione definita nella policy.

Dopo il completamento del backup, può essere visualizzato a livello di datastore o per singole VM selezionando "SnapCenter Plug-in for VMware vSphere" dall'elenco a discesa e quindi scegliendo "Ripristina".



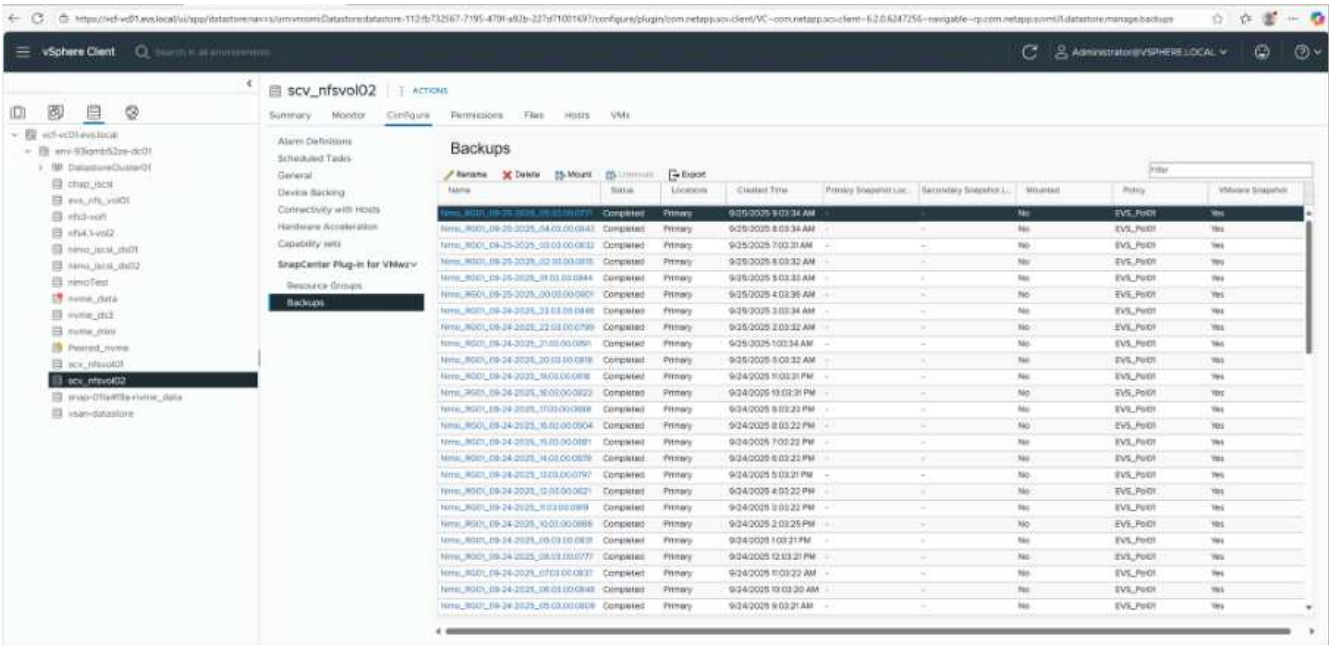
Procedura di ripristino per le VM protette da SnapCenter Plug-in for VMware

Questa sezione illustra i passaggi per ripristinare le VM dai backup. SCV può essere utilizzato per ripristinare le VM all'interno di vCenter, consentendo di recuperarle nel datastore originale sull'host ESXi originale (sovrascrivendo il contenuto esistente), per ripristinare VM eliminate o rinominate da una copia di backup, in un datastore diverso sull'host ESXi originale, nel datastore originale su un host ESXi diverso gestito dallo stesso vCenter, o in un datastore diverso su un altro host ESXi all'interno dello stesso ambiente vCenter.

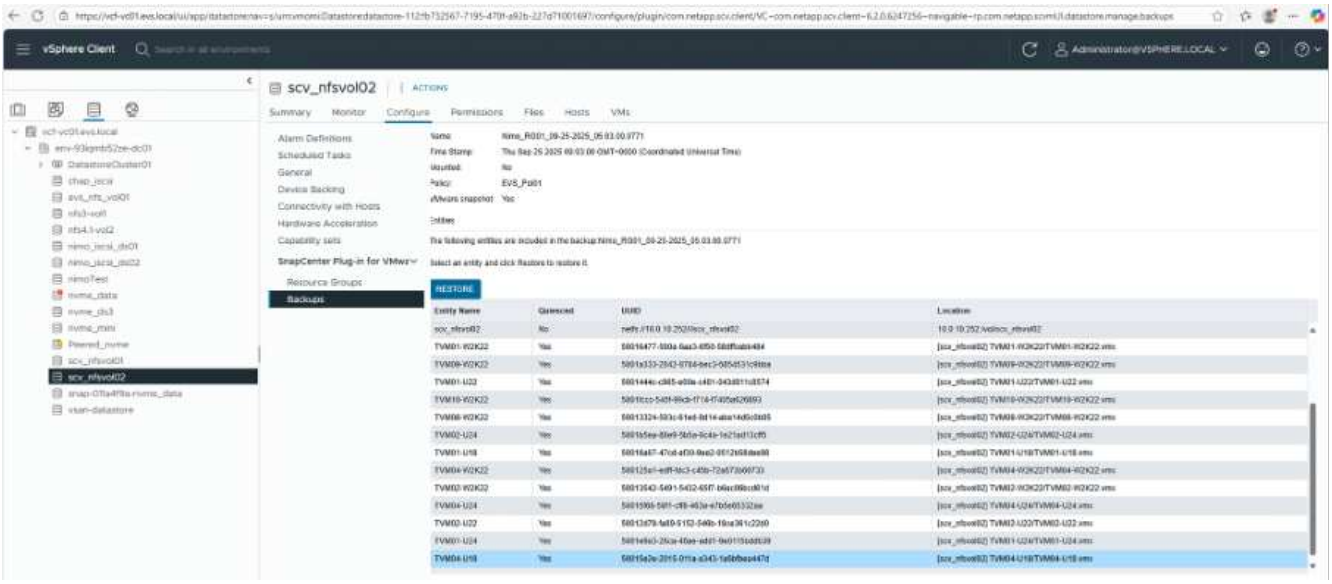
Passaggi per eseguire l'operazione di ripristino

Per eseguire l'operazione di ripristino, seguire questi passaggi:

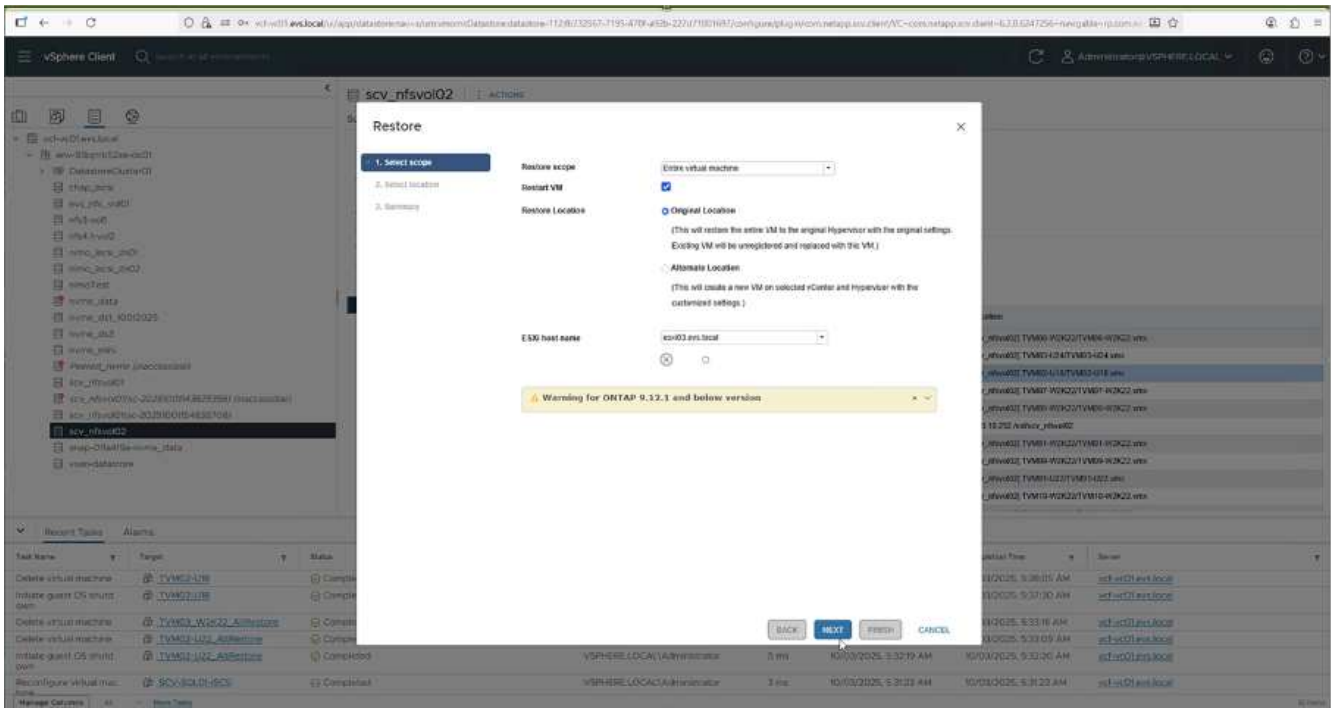
1. Nell'interfaccia grafica utente del client web EVS vSphere, vai su **Inventory › Datastores** e seleziona il datastore desiderato. Quindi vai su **Configure › Backups** nella sezione "SnapCenter Plug-in for VMware vSphere".



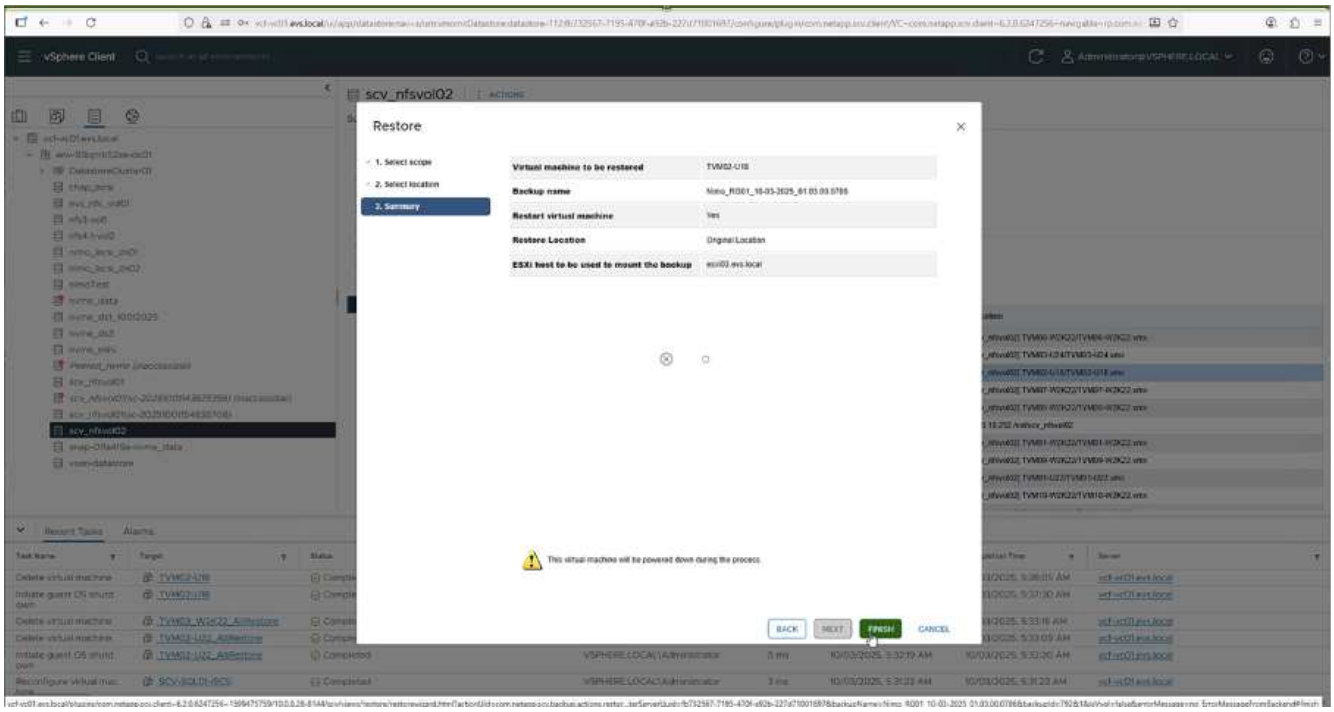
2. Fare doppio clic su un backup per visualizzare tutte le VM incluse in quel backup. Individuare la VM da ripristinare nell'elenco e selezionare "Ripristina".



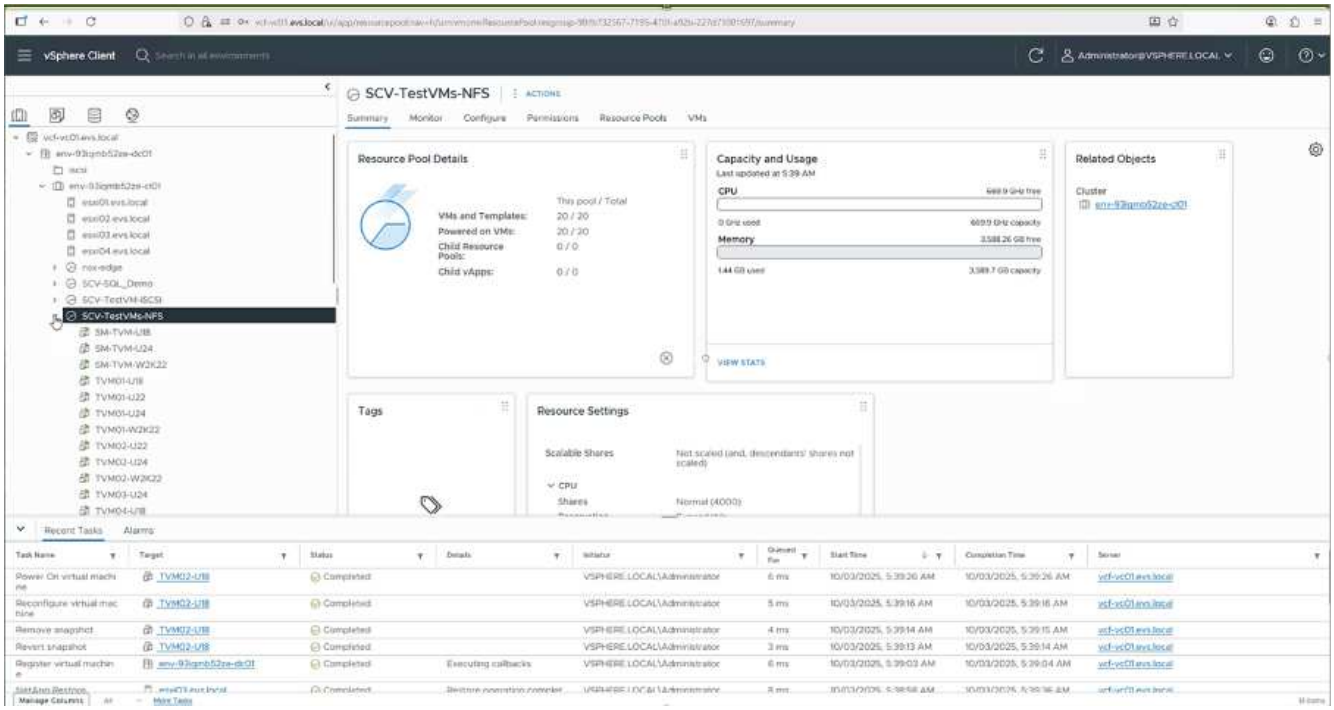
3. Nella pagina "Select Scope page", seleziona "Entire Virtual Machine" nel campo "Restore scope", quindi seleziona "Restore location" e inserisci le informazioni ESXi di destinazione in cui il backup deve essere montato.
4. Abilita la casella di controllo "Riavvia VM" se la VM deve essere accesa dopo l'operazione di ripristino.
5. Nella pagina "Select Location", seleziona una posizione principale.



6. Rivedi la pagina "Summary" e poi seleziona "Finish".



7. Monitora l'operazione in corso selezionando "Recent Tasks" nella parte inferiore dello schermo.



Sebbene le VM vengano ripristinate, non vengono aggiunte automaticamente ai loro precedenti gruppi di risorse. Se si desidera proteggere tali VM, aggiungerle manualmente ai gruppi di risorse appropriati.

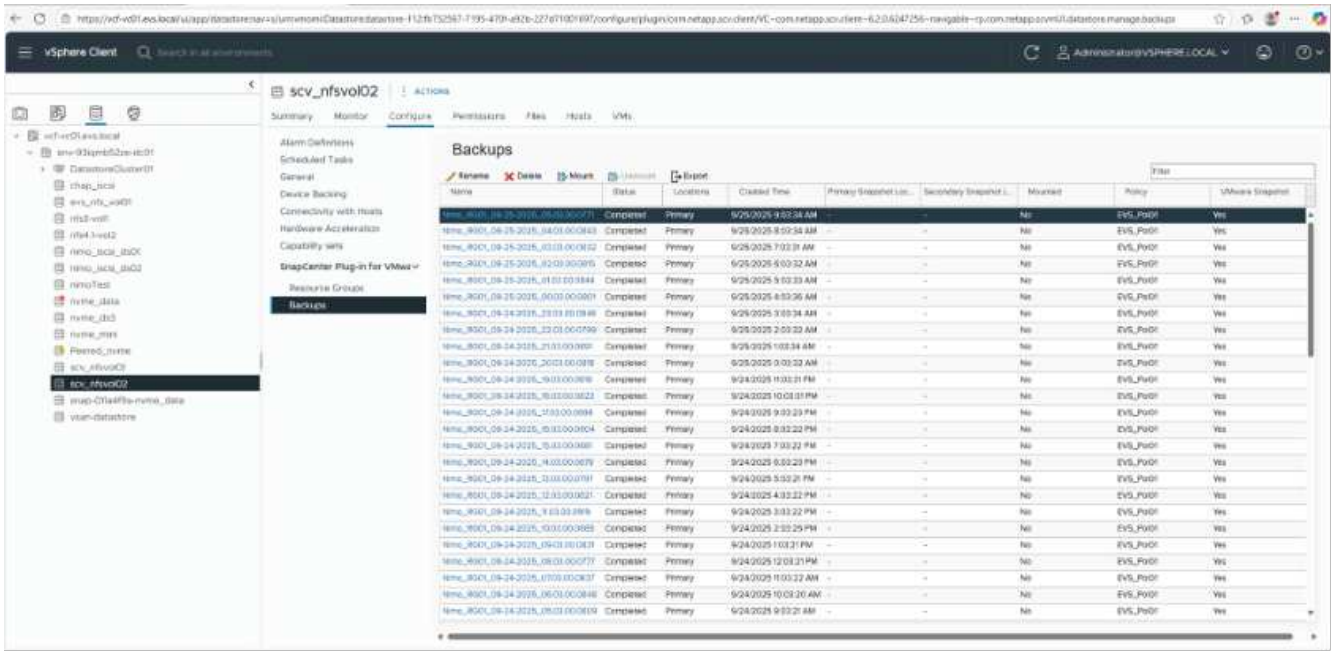
L'operazione di ripristino può essere attivata anche a livello di singola VM.

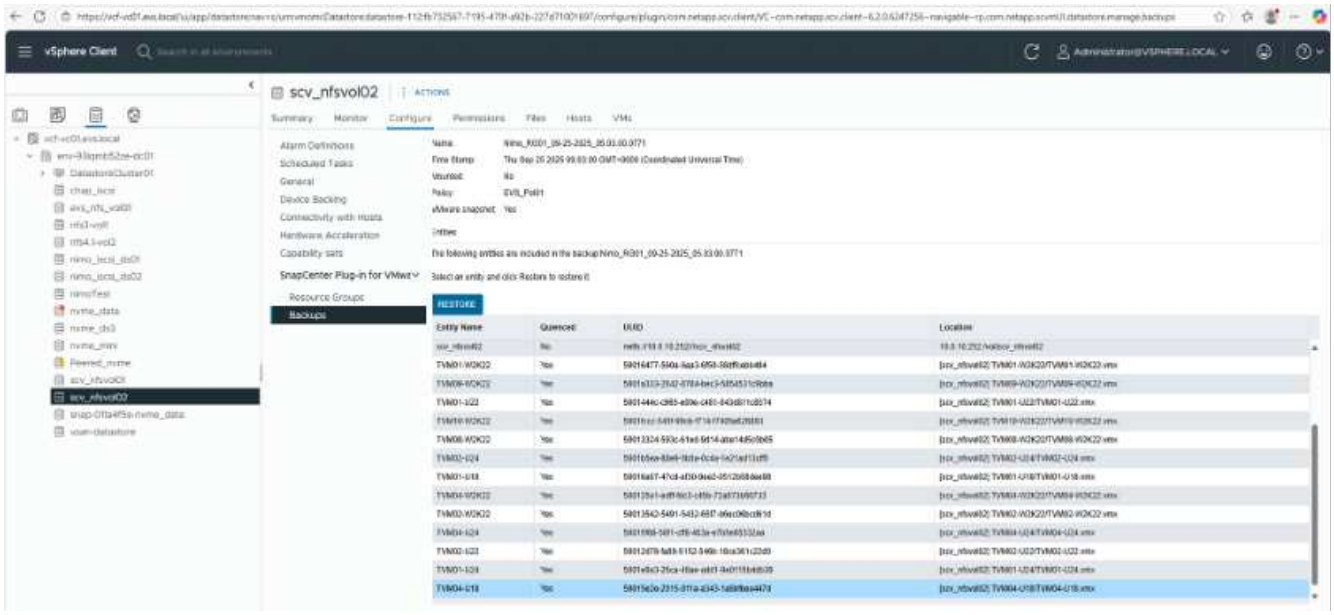
Passaggi per ripristinare una VM eliminata

Il ripristino di una VM eliminata è un processo semplice con SCV.

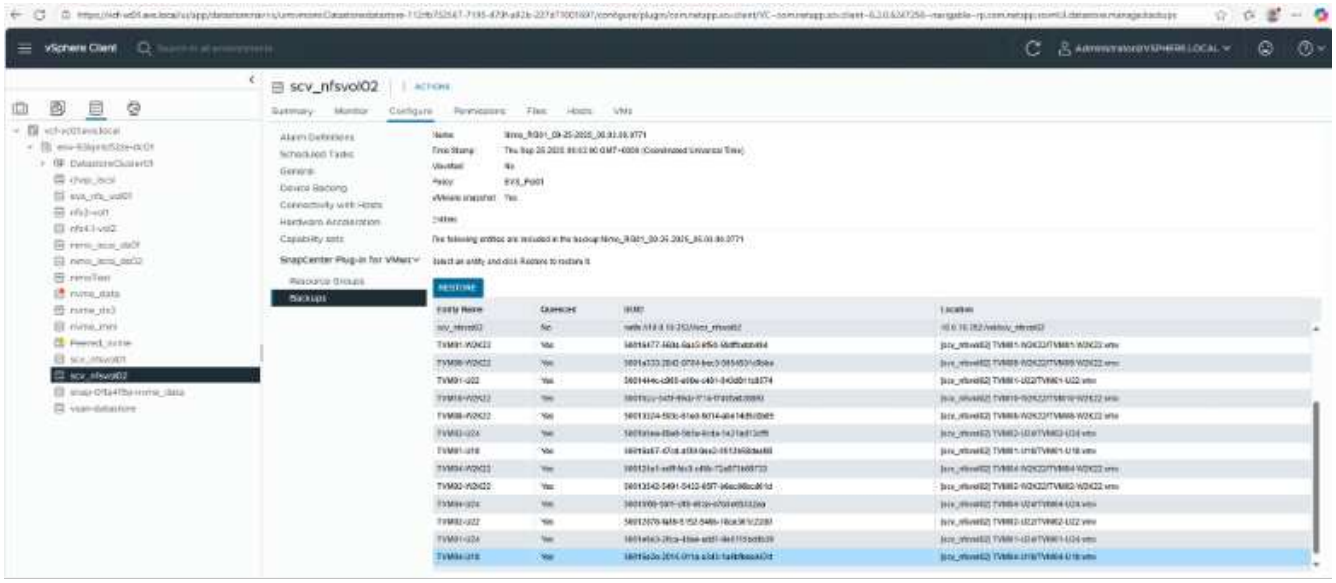
L'operazione di ripristino per una VM eliminata può essere eseguita dal livello del datastore.

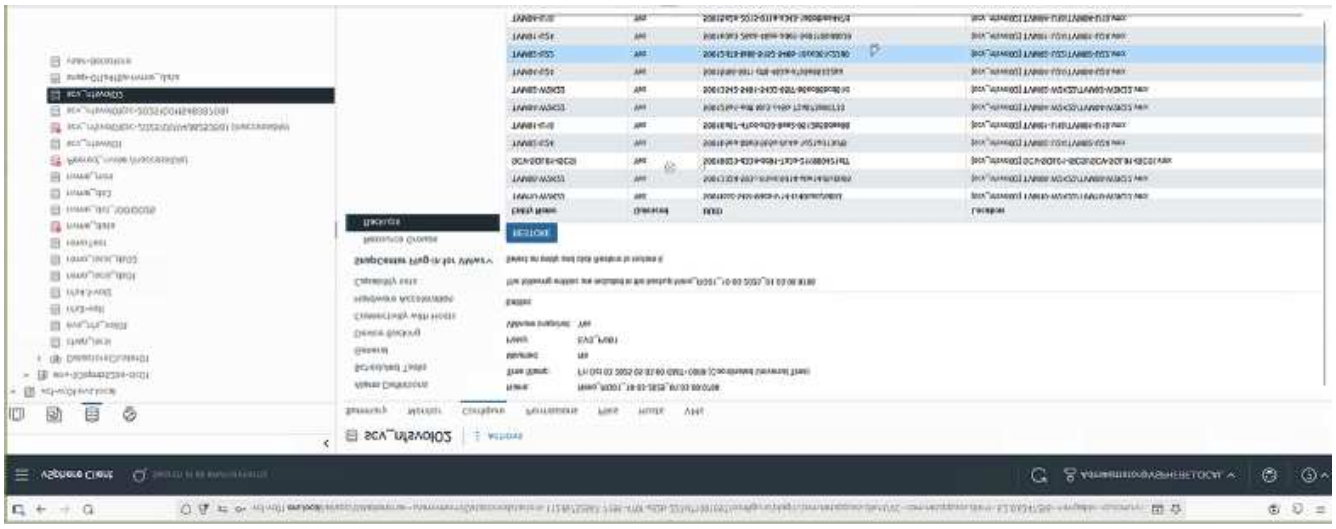
1. Vai al rispettivo Datastore > Configura > Backups. Lì, seleziona la VM eliminata e seleziona "Restore".

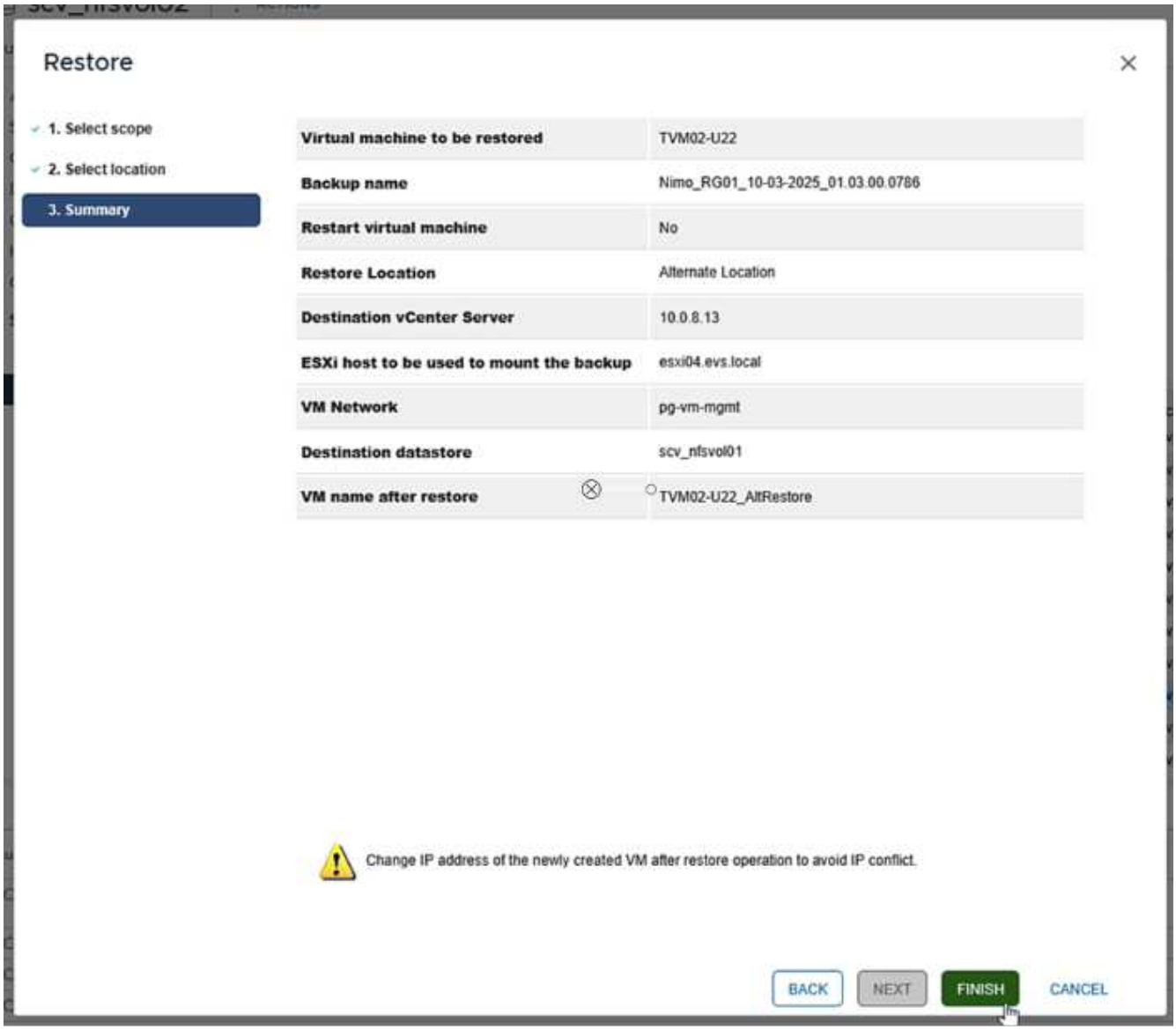


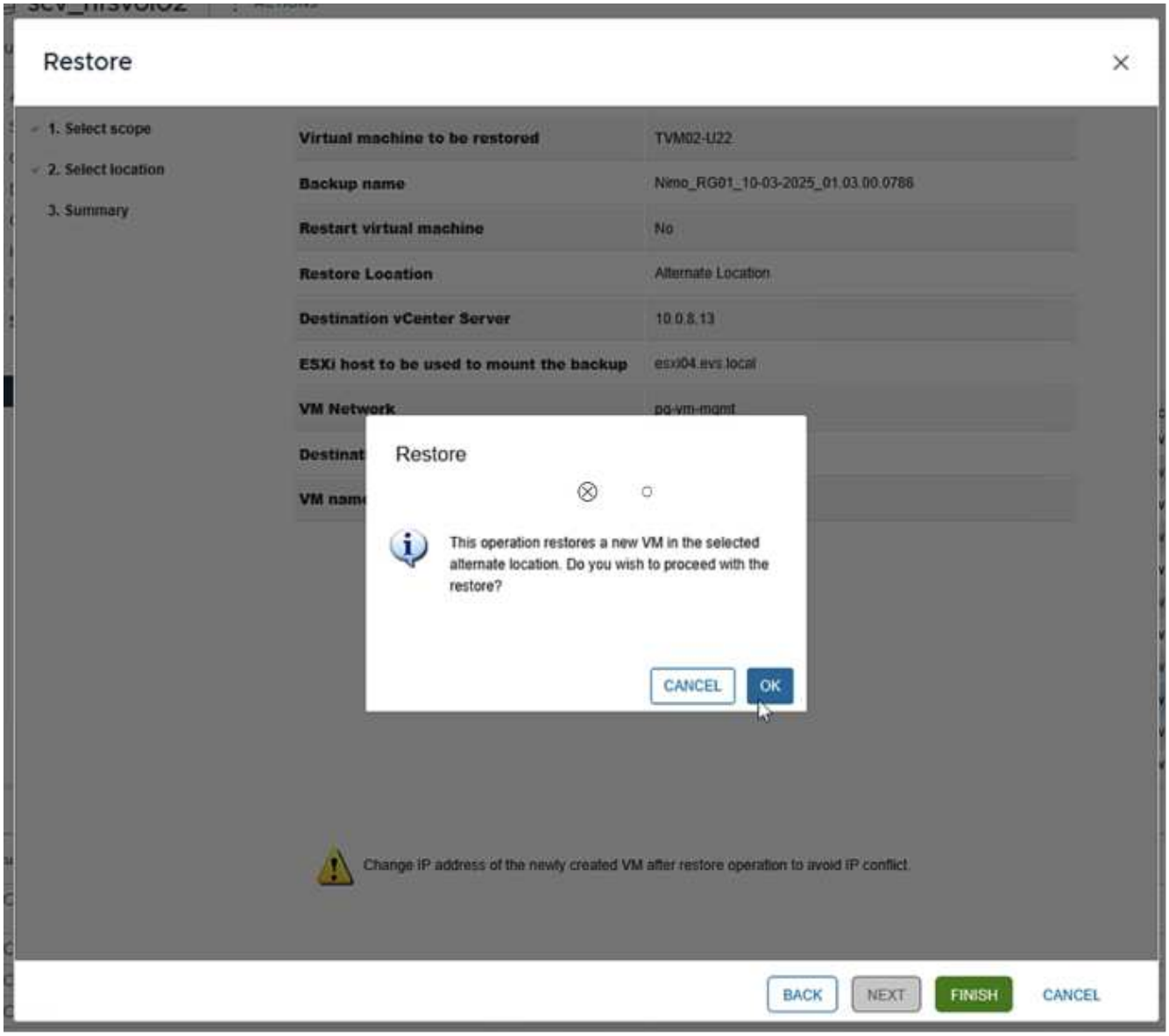


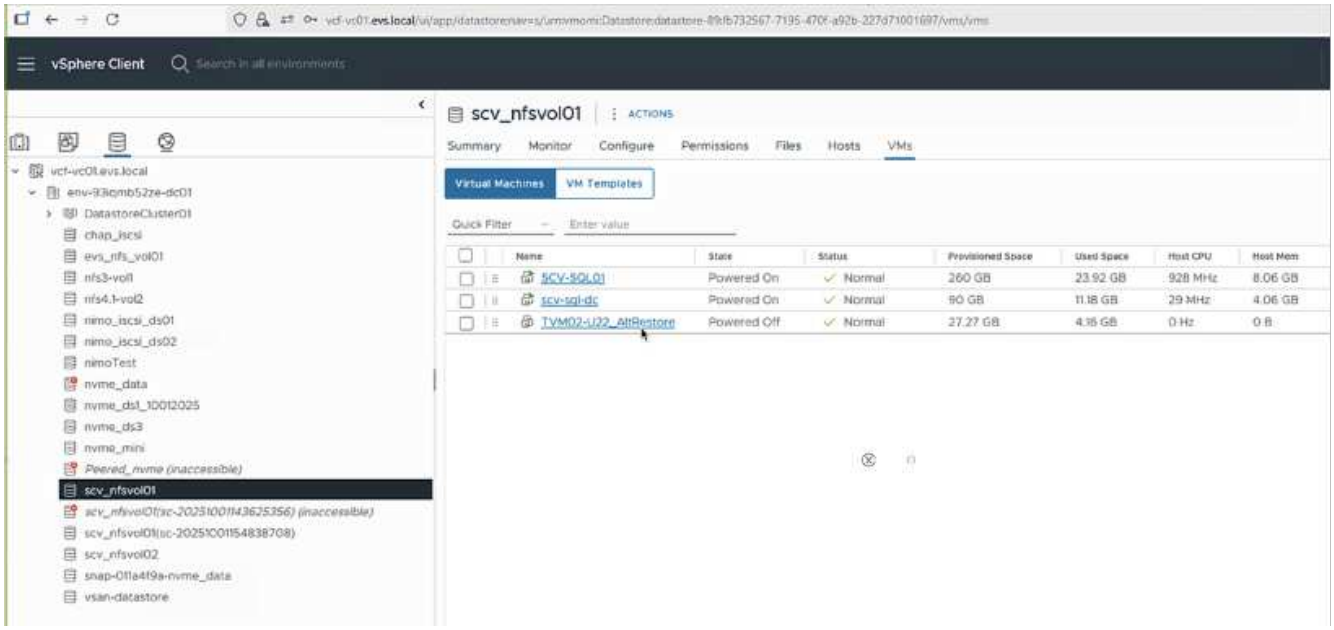
2. Il flusso di screenshot che segue copre il ripristino di una VM su un host ESXi alternativo e un datastore diverso.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity with Hosts
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE




Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

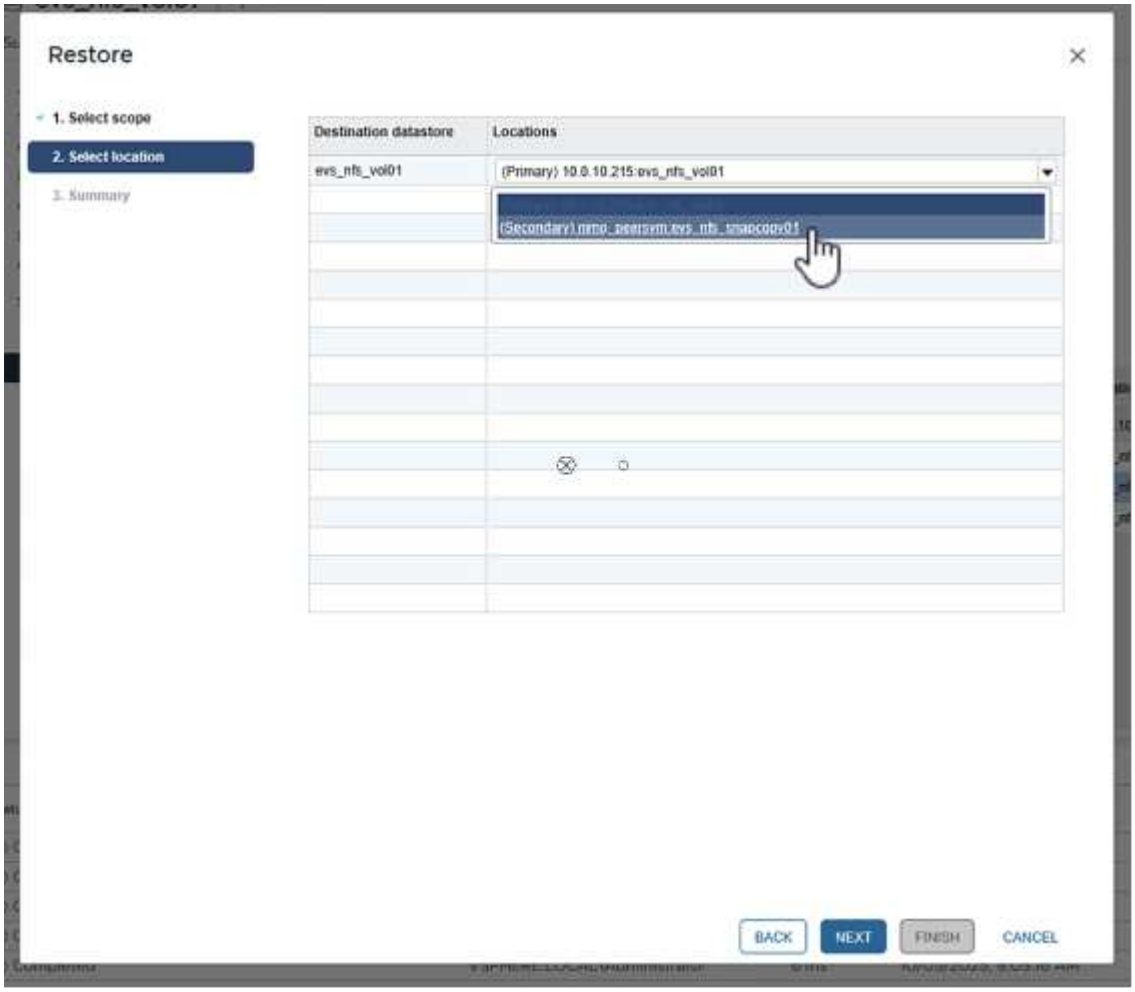

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001143625356) (inaccessible)
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

Il datastore di destinazione deve disporre di spazio libero adeguato e il vCenter specificato nel campo "Ripristina in posizione alternativa" deve essere risolvibile tramite DNS.

Per una migliore efficienza di ripristino negli ambienti NFS, attiva l'API VMware vStorage for Array Integration (VAAI).

I ripristini possono essere eseguiti anche da posizioni secondarie, come una destinazione di SnapMirror.



+

Procedura di ripristino per file e cartelle guest protetti da SnapCenter Plug-in for VMware

La sezione seguente mostra come ripristinare file e cartelle guest dai VMDK.

SnapCenter supporta il ripristino di file e cartelle da VMDK solo quando il sistema operativo guest è Windows.

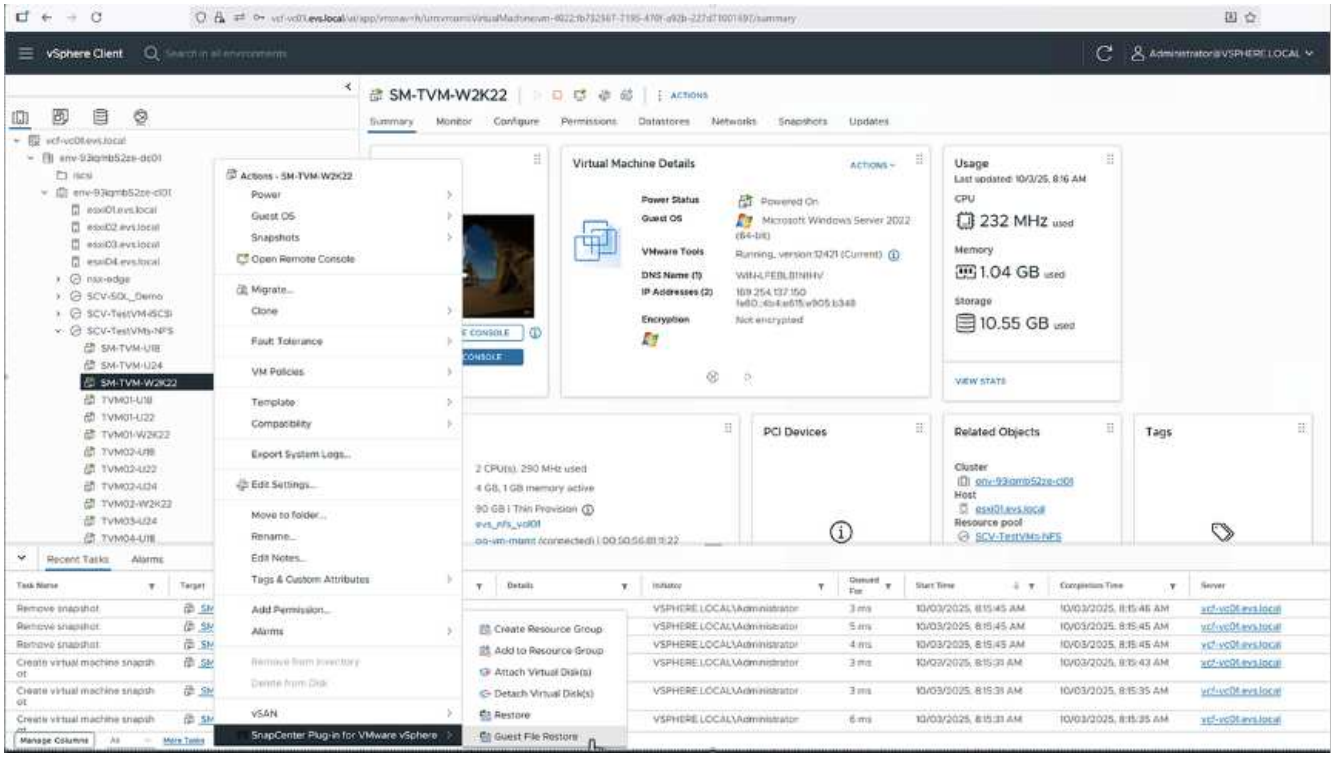
Considerazioni per il ripristino di file e cartelle guest con SCV:

- VMware tools devono essere in esecuzione sulla VM.
- Il VMDK allegato è accessibile per 24 ore per impostazione predefinita.
- Su una macchina virtuale è possibile eseguire una sola operazione di ripristino o di attach alla volta.

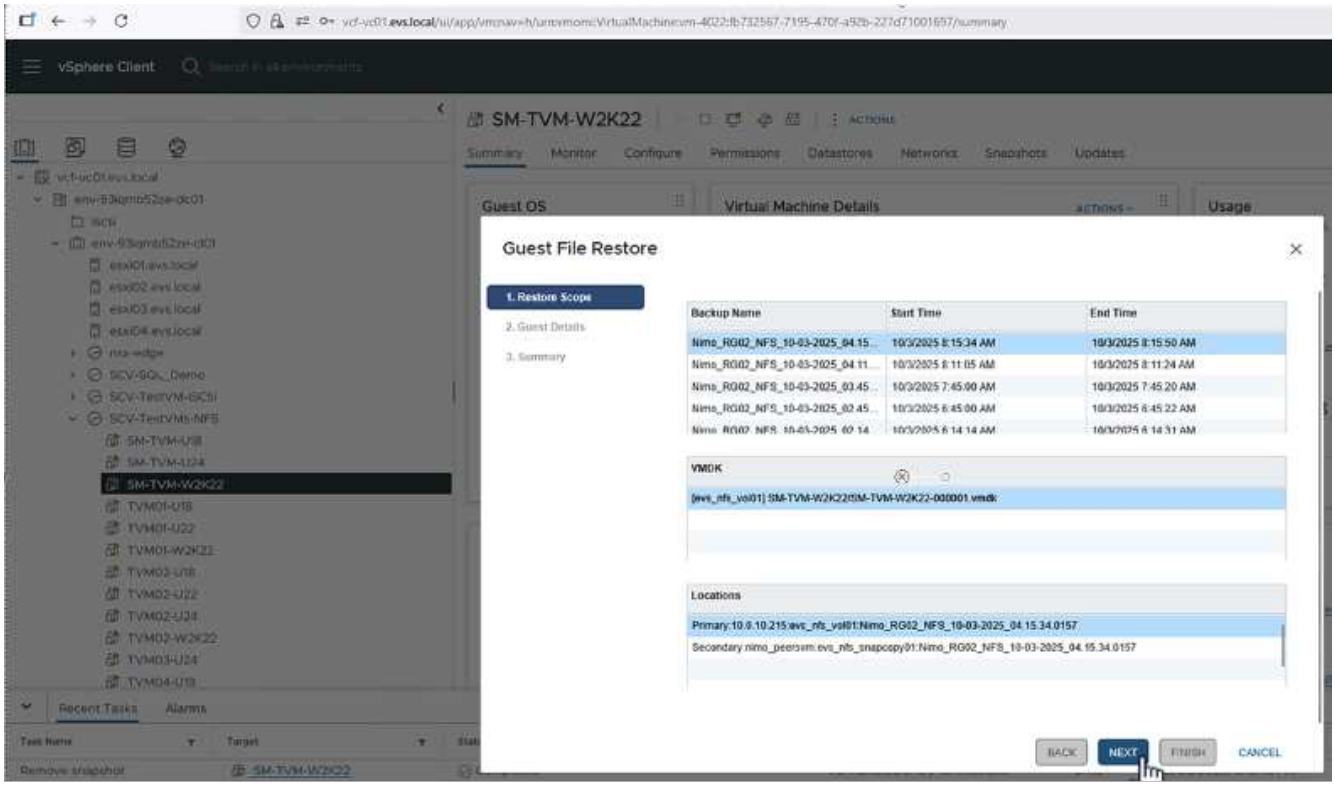
- È possibile ripristinare i file di sistema, nascosti e crittografati; tuttavia, i loro attributi originali non saranno preservati.
- Evitare di ripristinare i file crittografati in cartelle crittografate o di sovrascrivere i file di sistema.

Passaggi per il ripristino di file e cartelle guest:

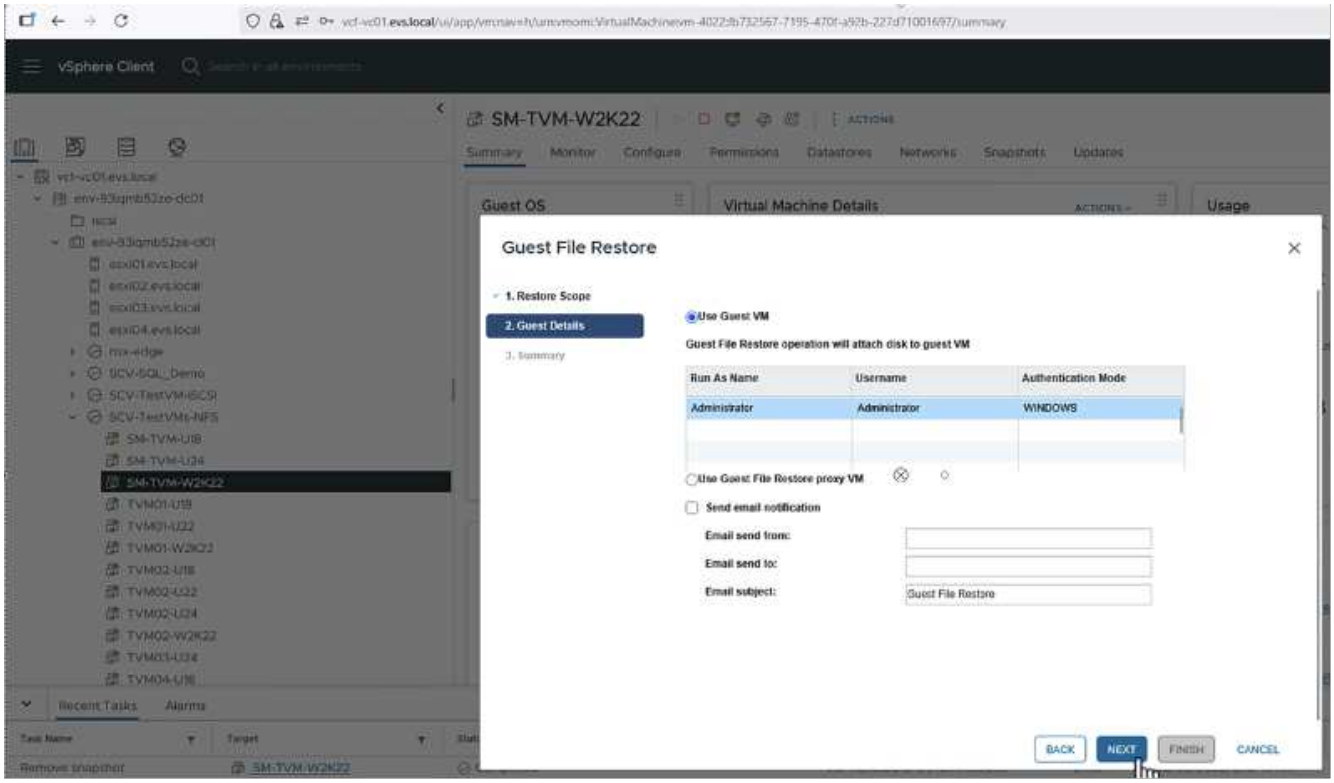
1. Fare clic con il pulsante destro del mouse sulla VM di destinazione e selezionare "**NetApp SnapCenter › Ripristino file guest**.



2. Selezionare il backup contenente il VMDK richiesto. Specificare il VMDK e la sua posizione (primaria o secondaria).



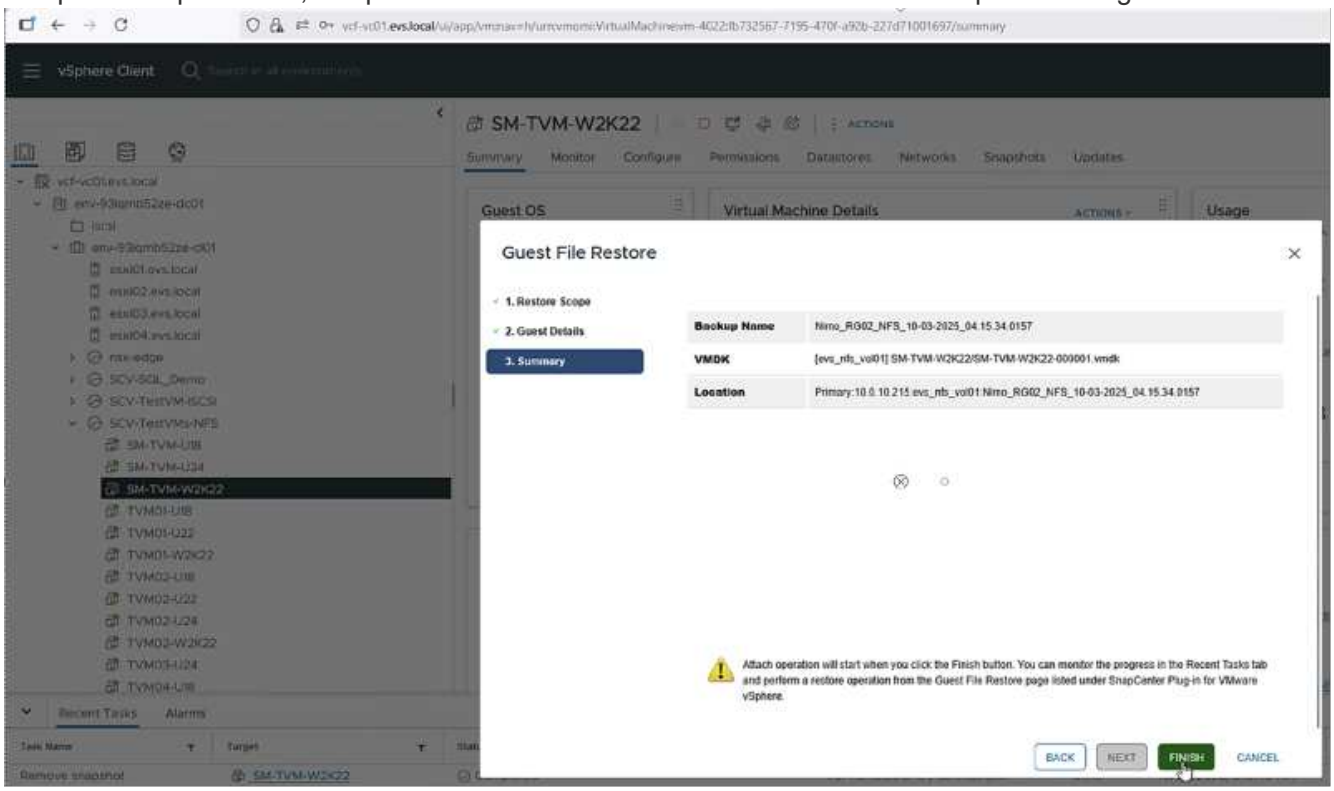
3. Scegliere "Disk Attachment Method".

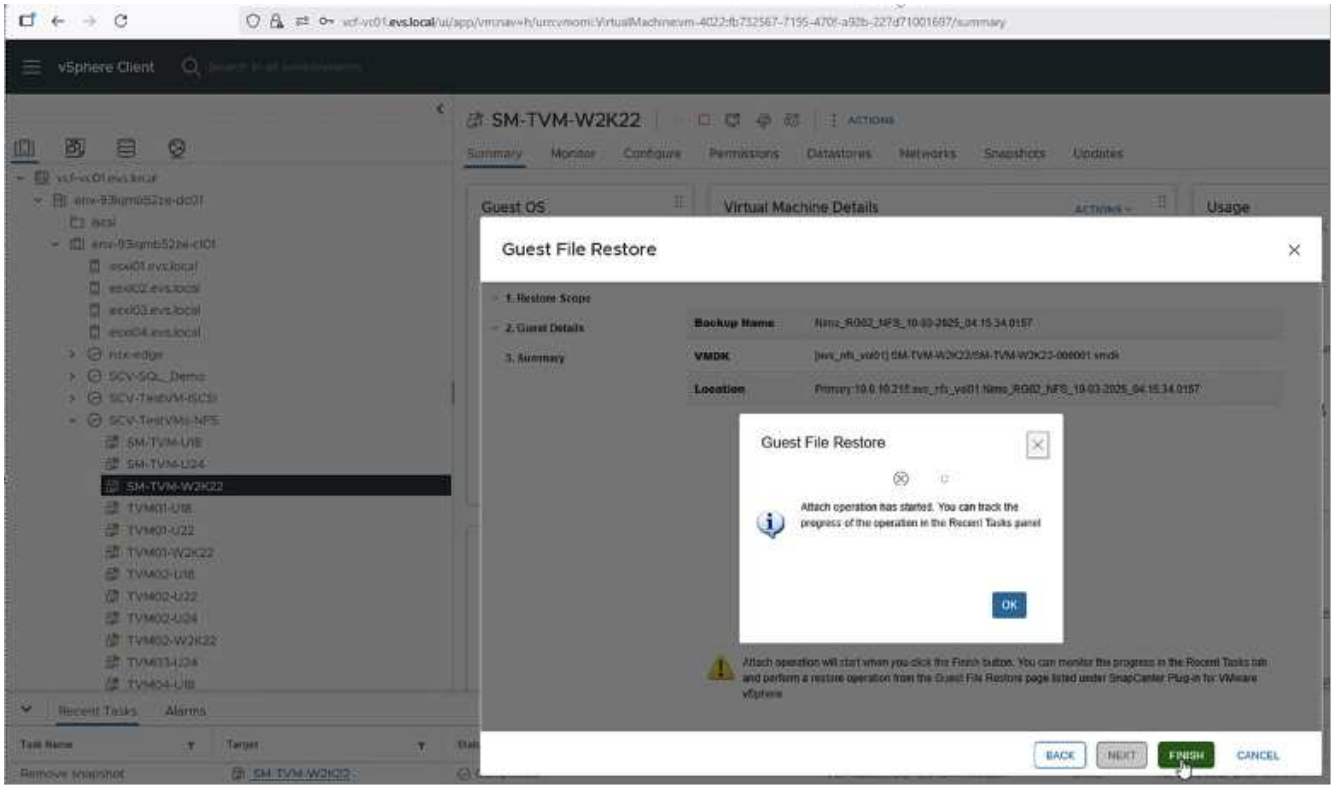


- Opzione VM guest: collega il disco alla VM originale (richiede credenziali preconfigurate). Questa è l'opzione utilizzata in questa dimostrazione.
- Opzione proxy VM: collega il disco a una proxy VM designata (deve essere configurata in anticipo).

4. Attendere il completamento dell'operazione di collegamento prima di esplorare e ripristinare i file. Una volta

completata l'operazione, SnapCenter crea automaticamente una sessione di ripristino file guest.





5. Passare al VMDK nella sessione Guest File Restore, selezionare i file o le cartelle richiesti e ripristinarli nella posizione specificata.

Procedure di protezione per database in esecuzione su VMware VMDK con SnapCenter per SQL (SCSQL)

La sezione seguente mostra come proteggere i database in esecuzione su VMware VMDK con SnapCenter for SQL (SCSQL).

Impostazione di SCSQL

La configurazione per l'utilizzo di SCSQL per proteggere i database sui VMDK è la seguente:

1. "Installa e configura" Server SnapCenter.
2. Accedi a SnapCenter.
3. Configurare l'ambiente SnapCenter:
   - "Aggiungi o assegna" connessioni del sistema storage.
   - "Crea" credenziali.
4. Per i database Microsoft SQL Server su VMware VMDK:
   - "Distribuisci SCV" (già trattato nella sezione di configurazione).
   - Registrare il plug-in con SnapCenter.
5. Aggiungi "Host SQL Server e installazione dei plug-in":
   - "Configurare i plug-in SQL".
   - "Configura il piano di protezione e le pianificazioni per database e log".

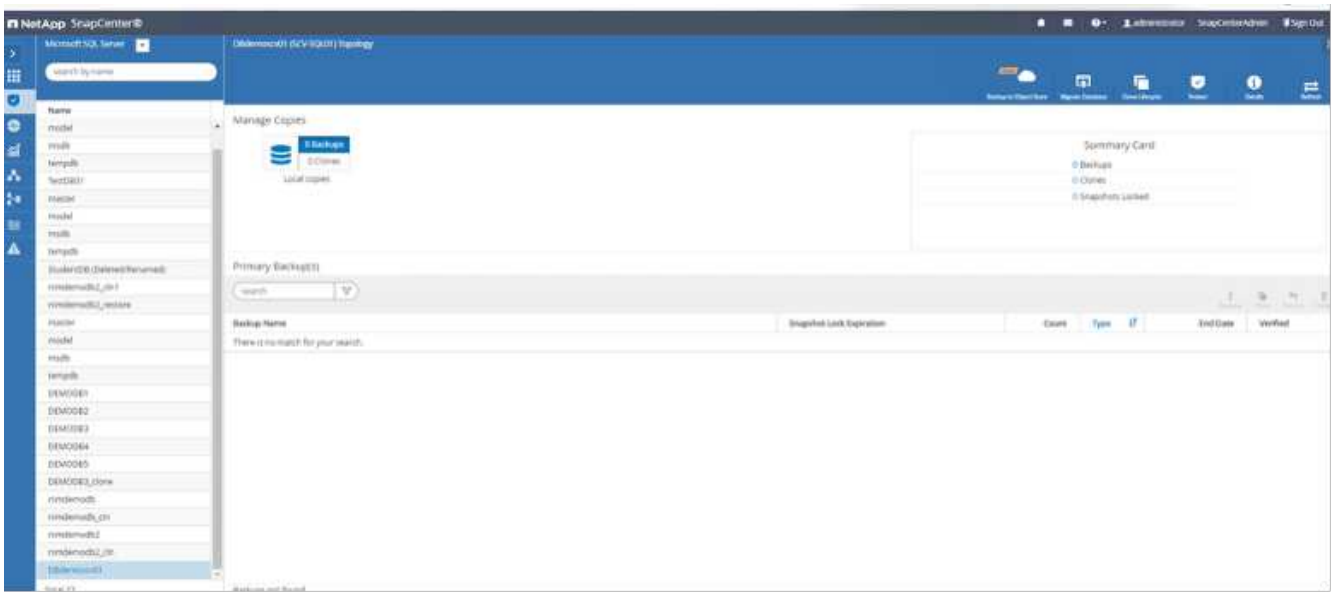


Impostazione di una policy di backup

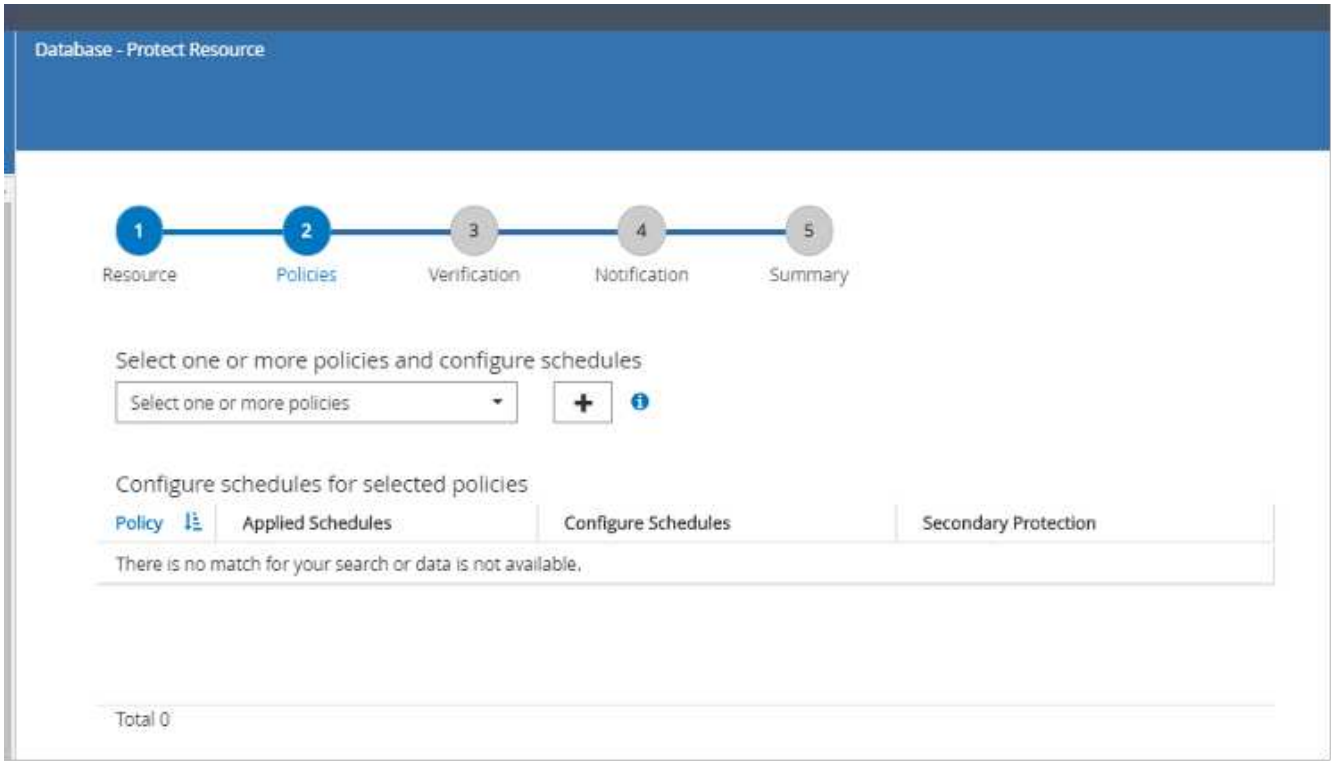
I passaggi seguenti mostreranno come impostare una policy di backup.

1. Selezionare il database dalla scheda Risorse e selezionare "Protect" nell'angolo in alto a destra.

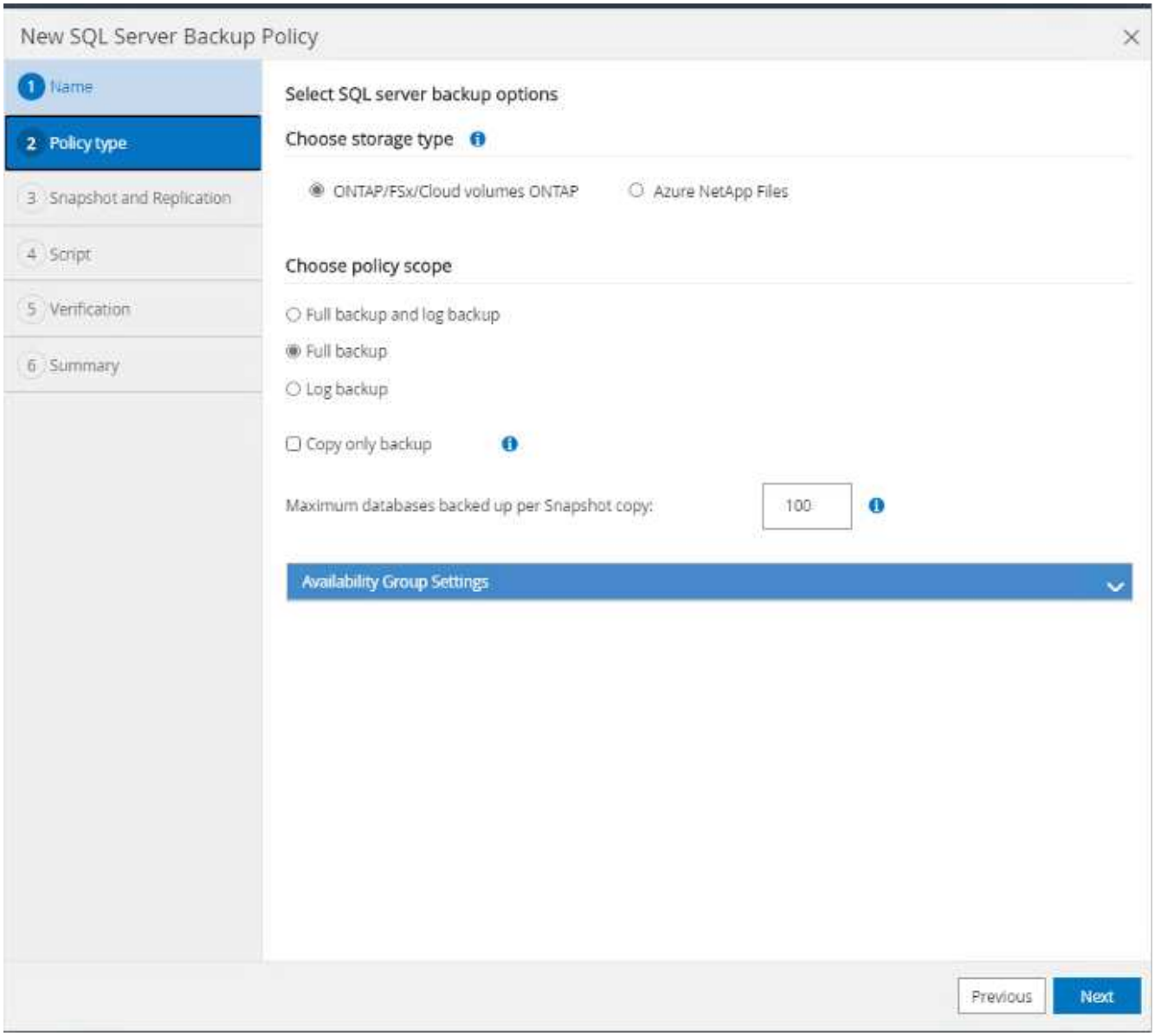
   Le convalide vengono eseguite su un database SQL Server in esecuzione sulla VM guest.



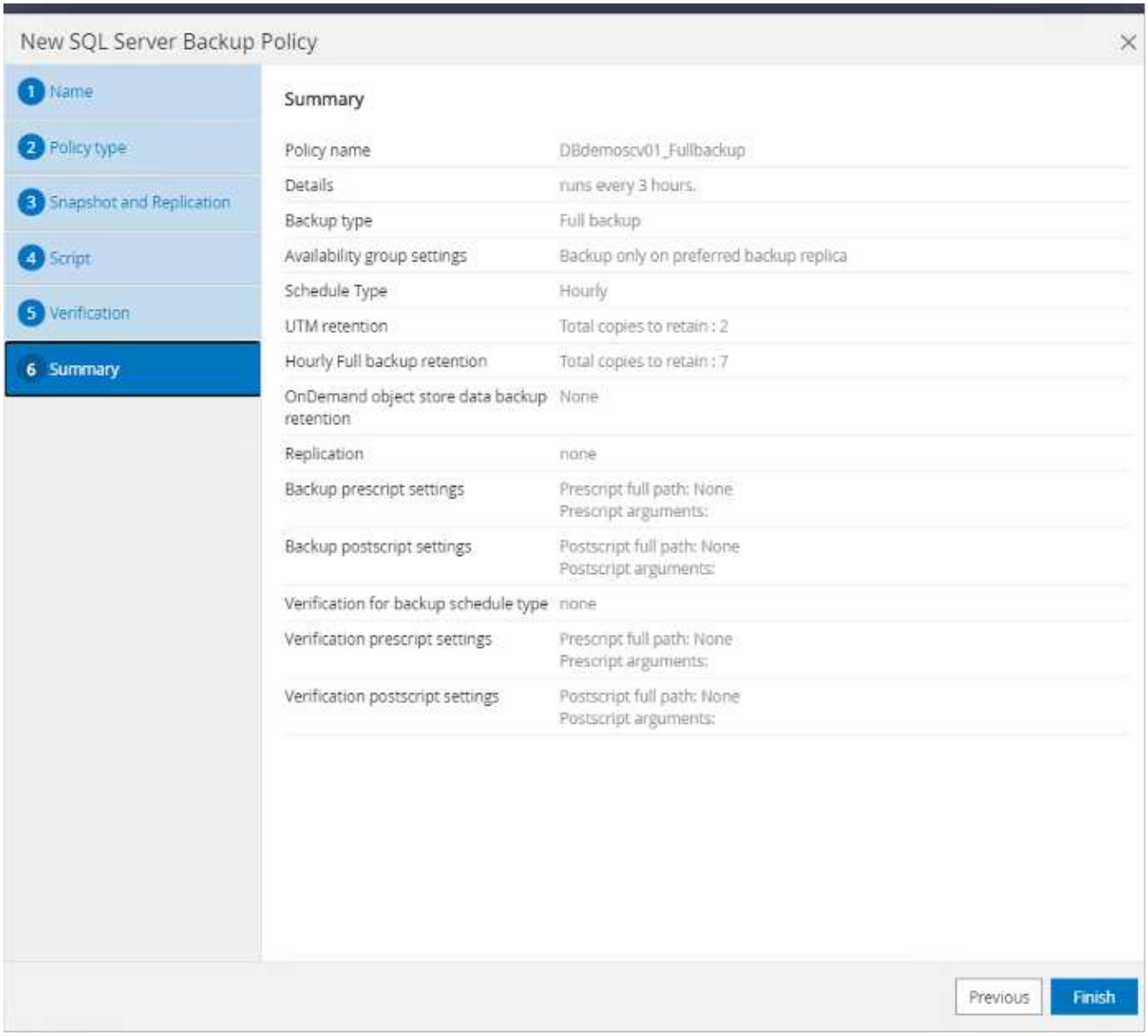
2. Fare clic sull'icona del segno più per configurare una policy di backup di SQL Server.



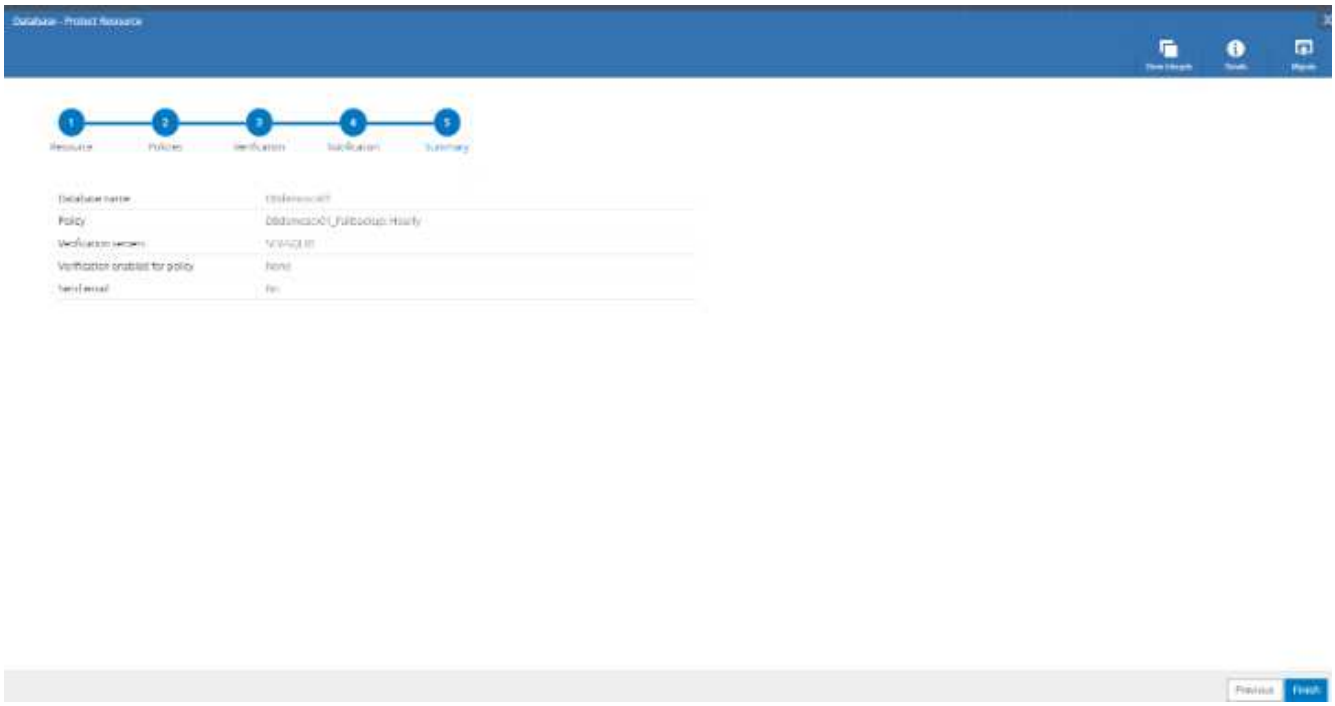
3. In questa demo, "Backup completo" è selezionato. Selezionare "Avanti" per continuare.



4. Nella pagina Summary, seleziona "Finish".



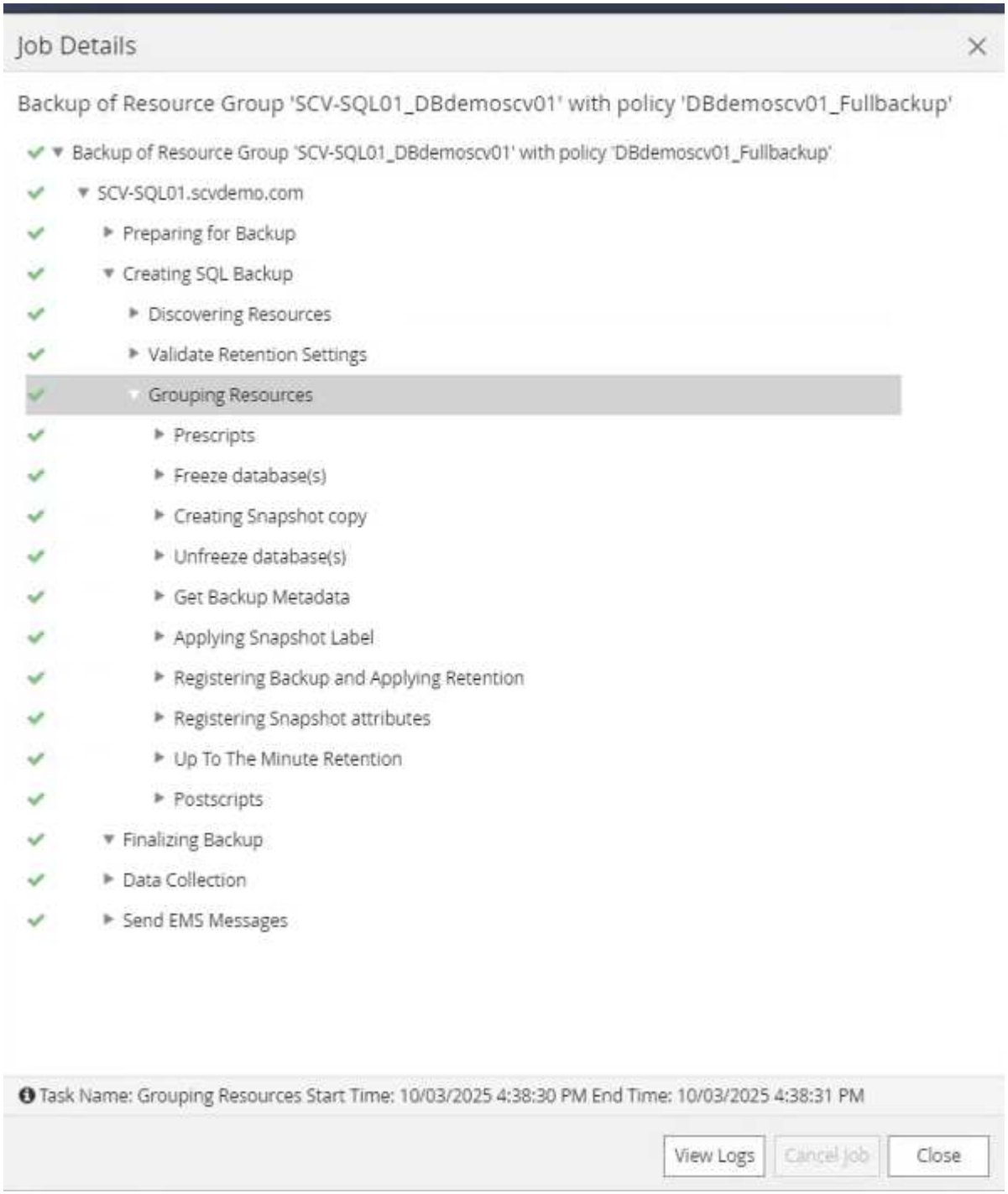
5. Procedi su "Fine".



Monitoraggio di un backup

Una volta impostata una policy di backup, puoi monitorare le operazioni di backup mentre avvengono. Puoi farlo cliccando su Backup now per avviare un'operazione di backup su richiesta oppure attendendo che la tua policy di backup pianificata entri in funzione.

1. Monitorare l'avanzamento del lavoro utilizzando **Monitor › Jobs**.
2. Seleziona il processo di backup, quindi fai clic su "Dettagli" per visualizzare i dettagli del processo come di seguito.

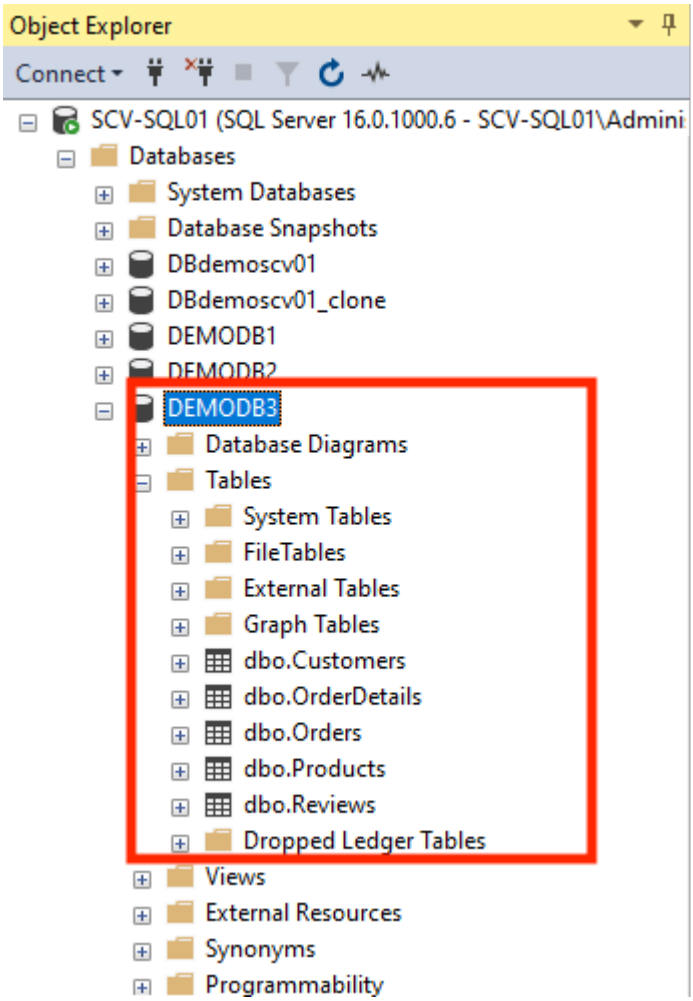


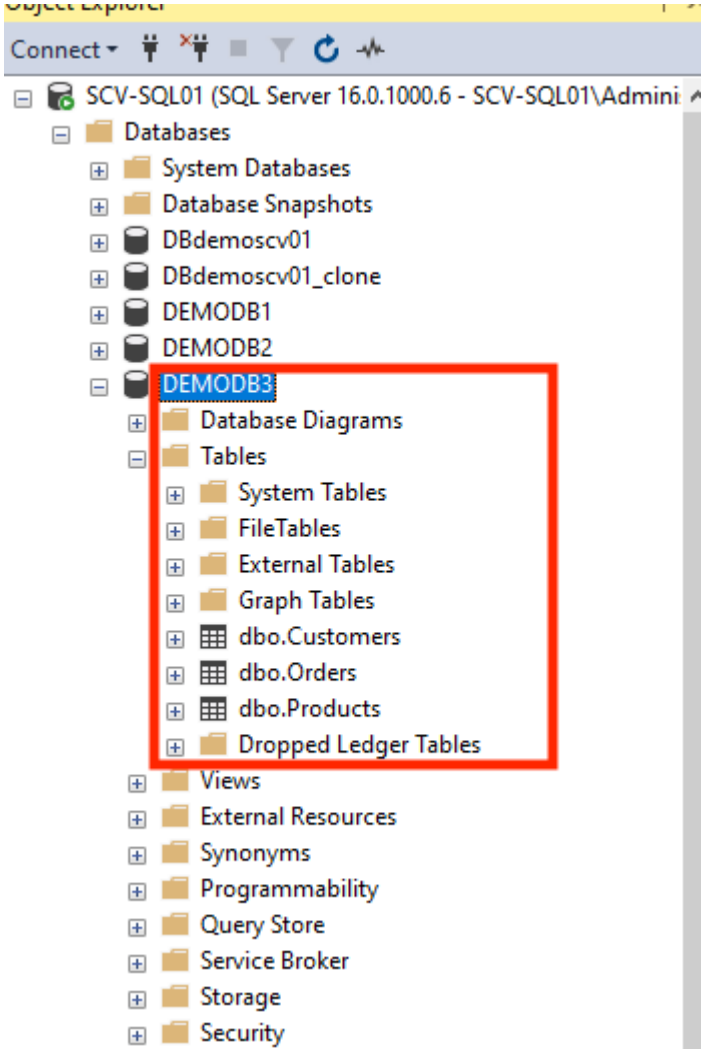
Ripristino dei database residenti sui VMDK

Il database sul VMDK può essere ripristinato a un punto specifico nel tempo.

Possiamo simulare l'importanza di questo eliminando alcune tabelle nel tuo database, che verranno poi corrette eseguendo un rispristino point-in-time.

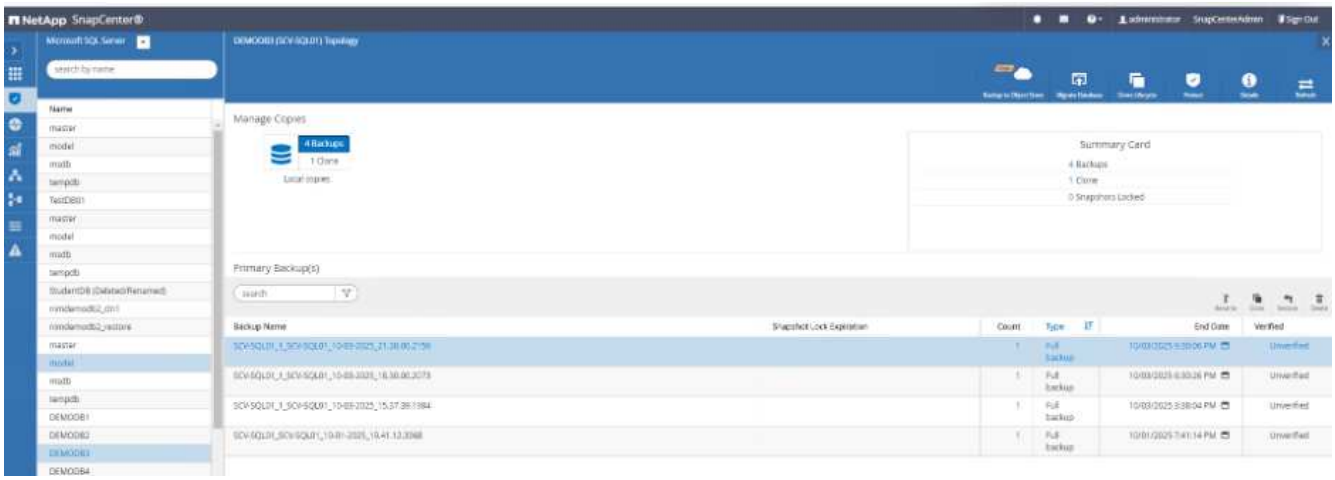
Qui sotto puoi vedere che diverse tabelle del nostro database mostrate nel primo screenshot sono state eliminate nel secondo screenshot:


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

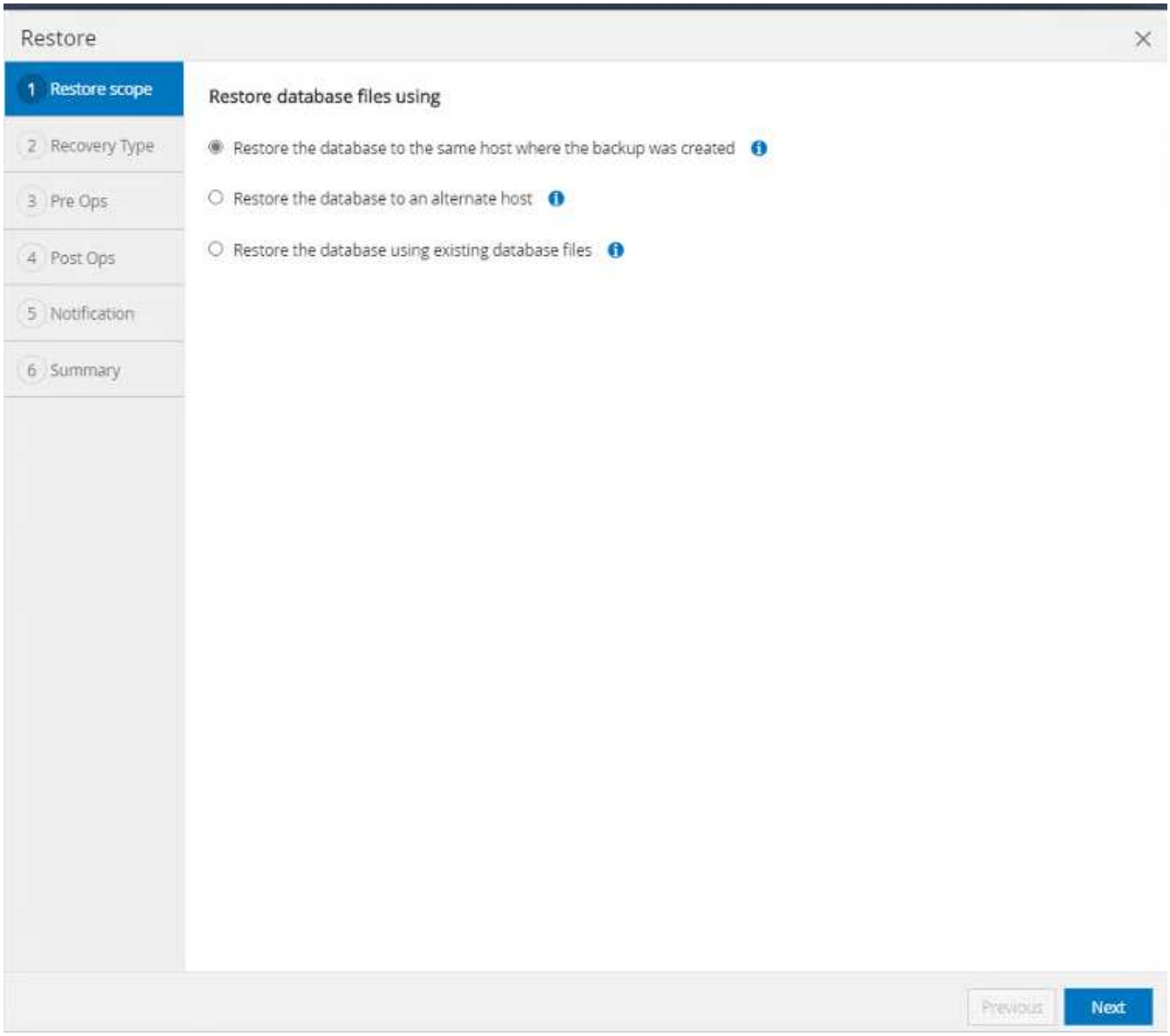


I passaggi seguenti mostrano come eseguire un ripristino per recuperare le tabelle eliminate:

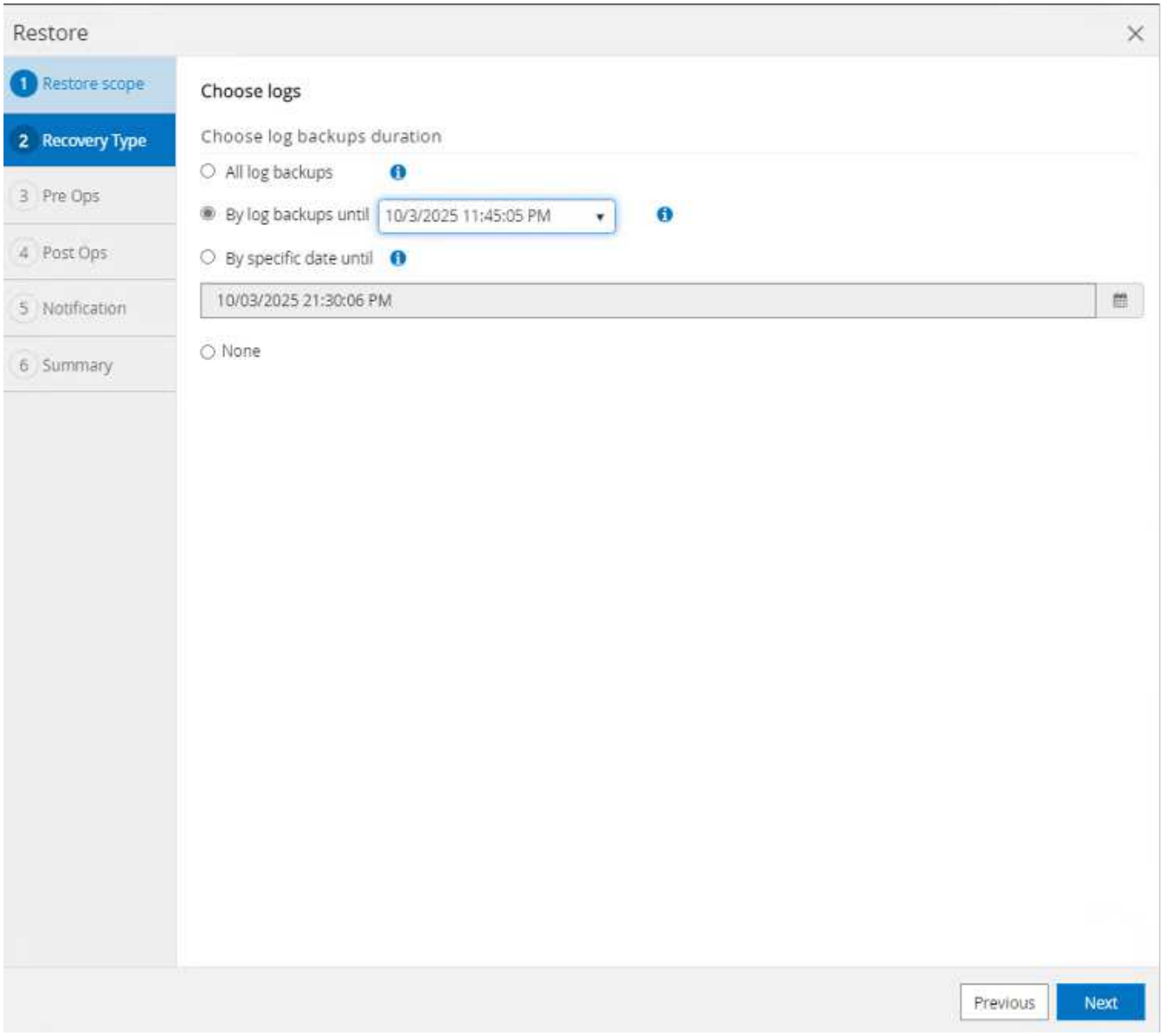
1. Seleziona il database dal gruppo di risorse.



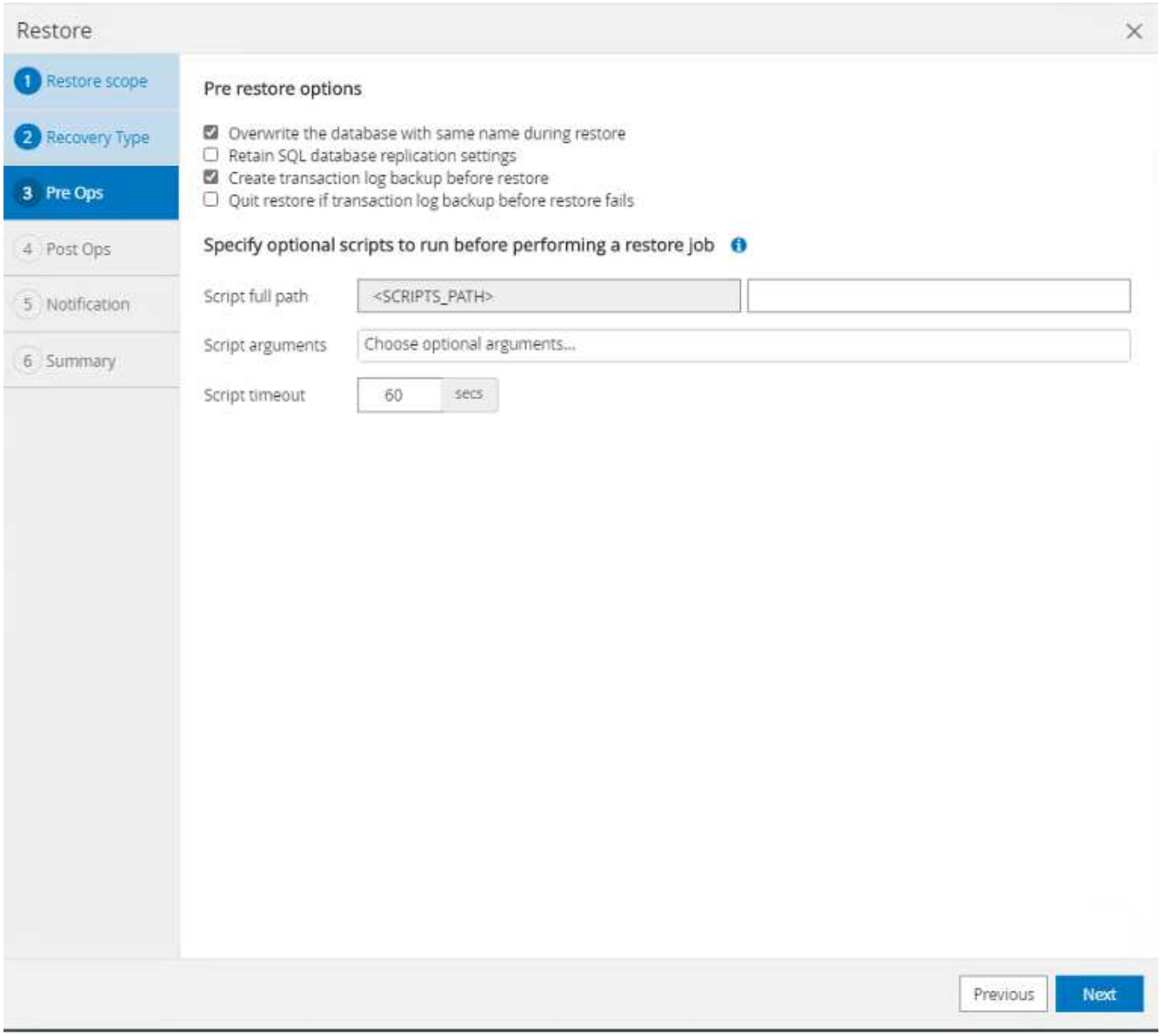
2. Nella pagina Restore, seleziona l'opzione "Restore the database to the same host where the backup was created".



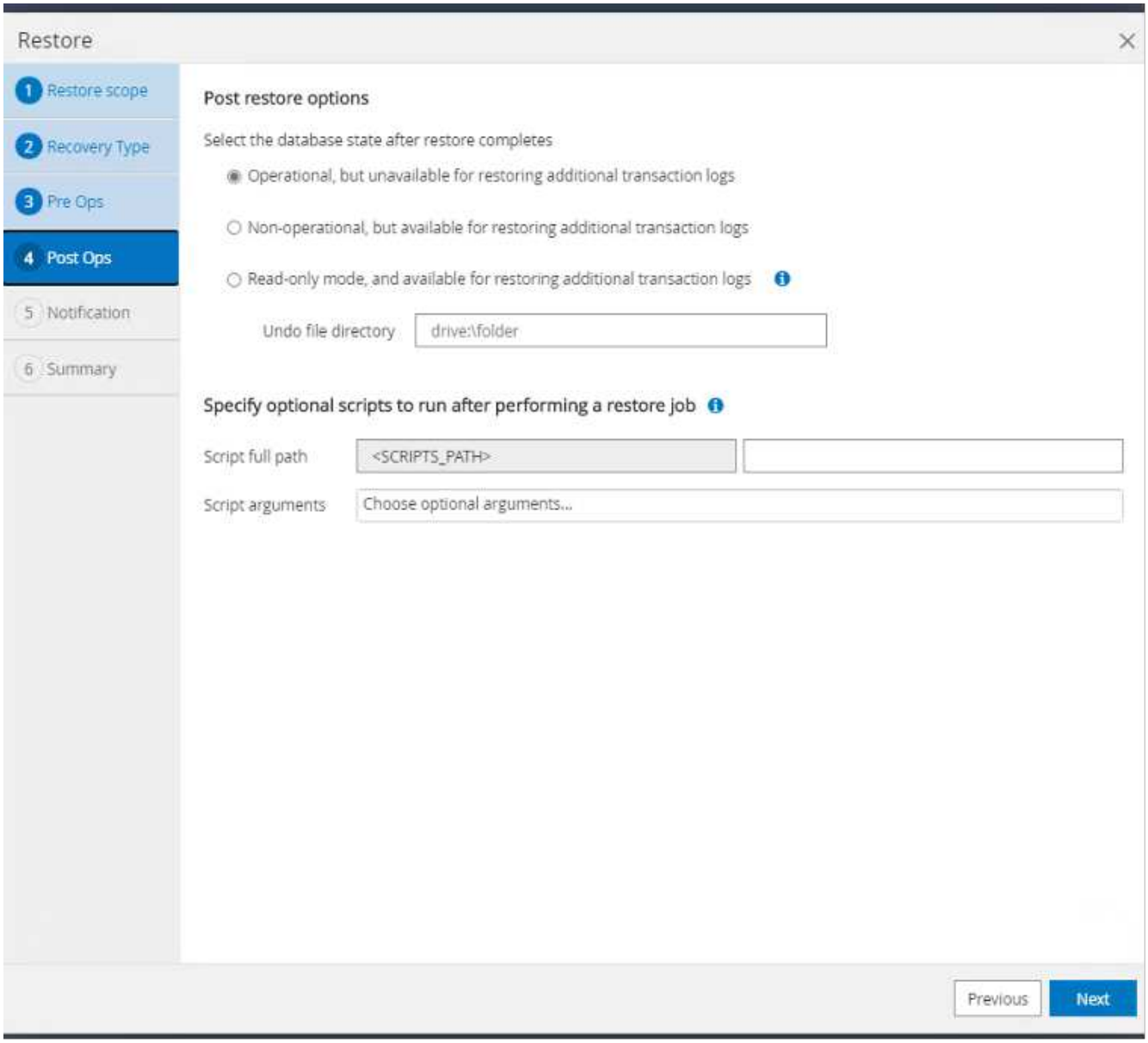
3. Selezionare l'opzione per utilizzare un backup del log fino a un punto nel tempo.



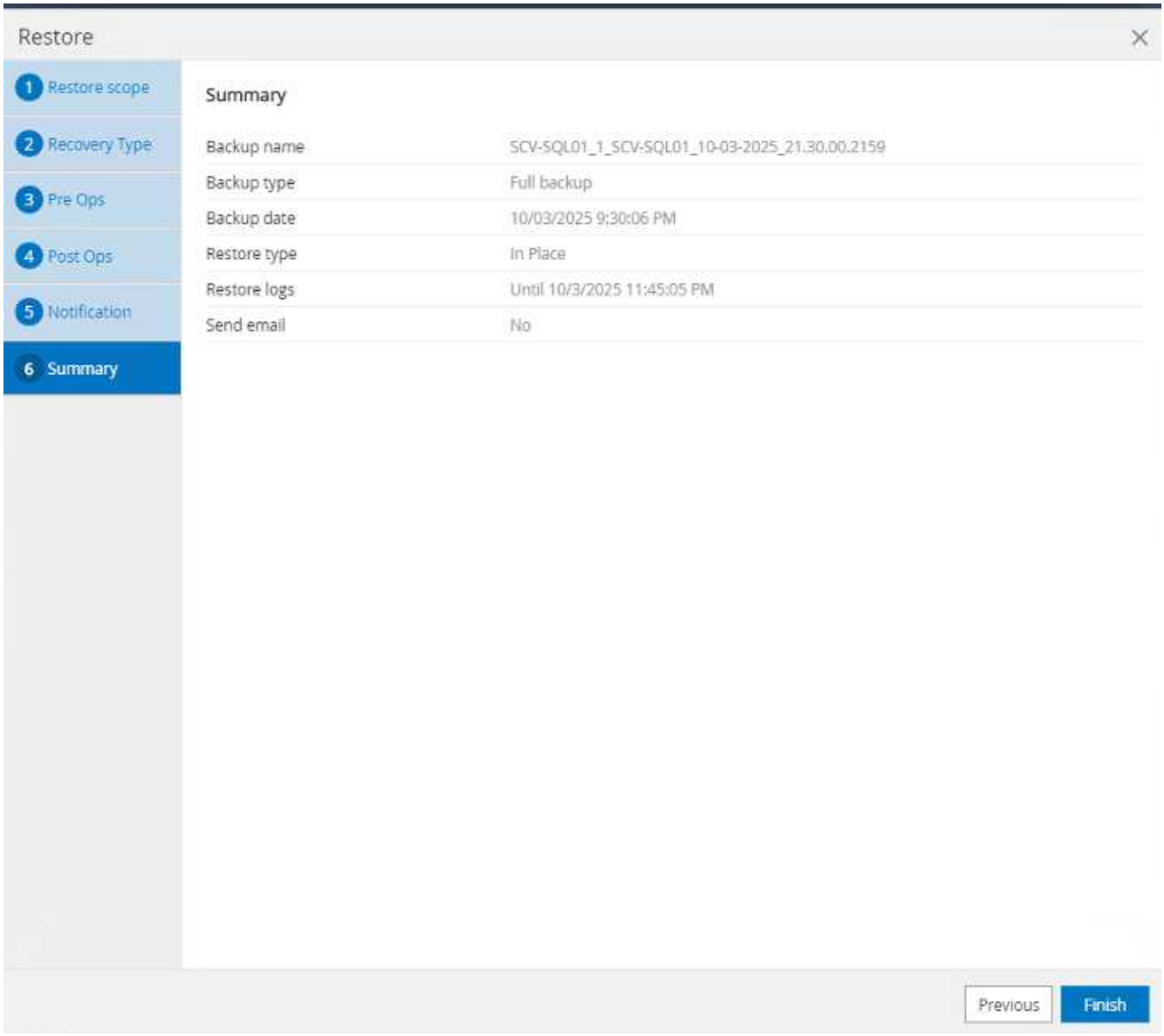
4. Selezionare "Sovrascrivi database con lo stesso nome durante il restore, crea un backup del transaction log prima del restore" e selezionare "Next".



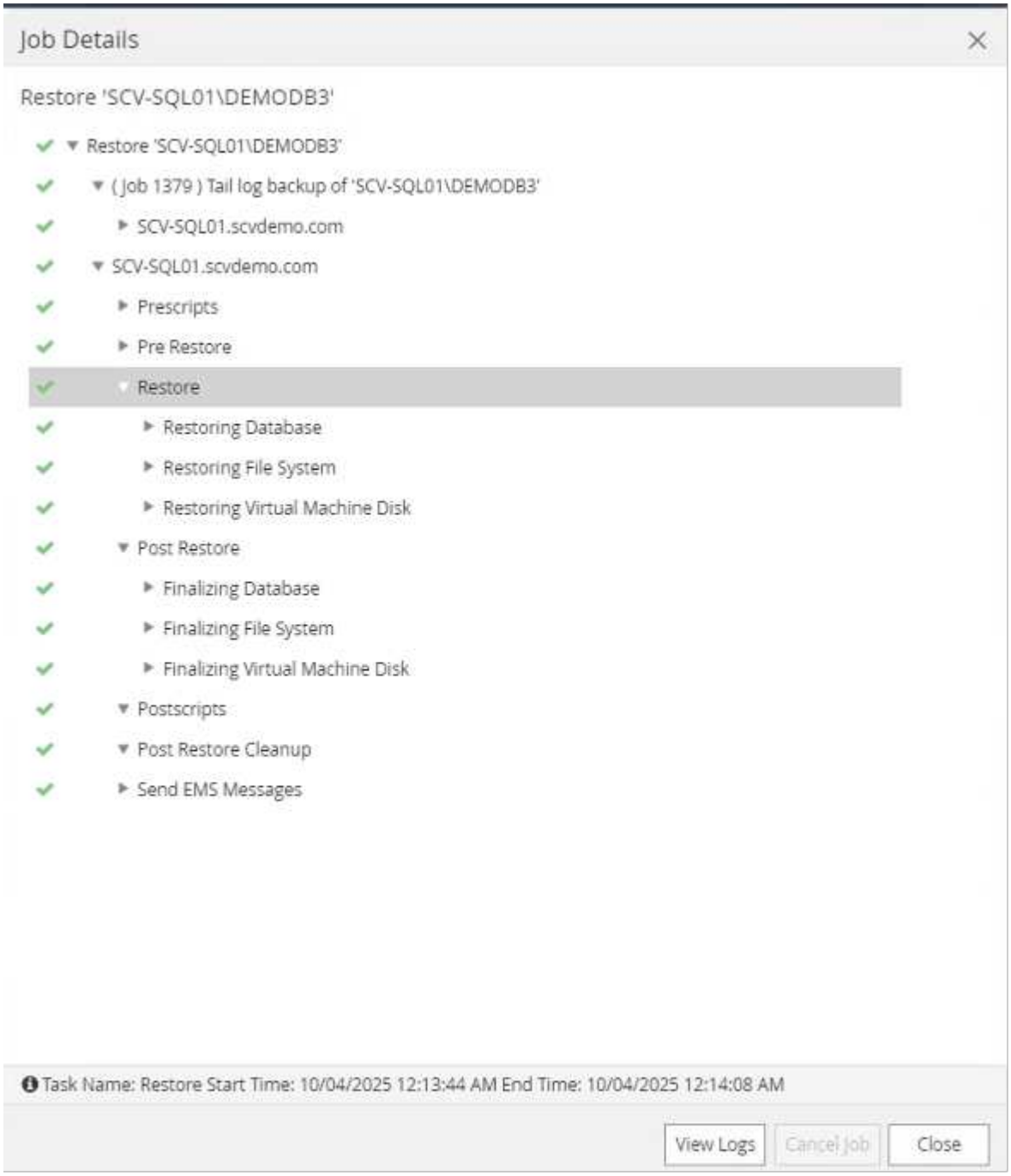
5. Selezionare lo stato post-ripristino che si desidera venga assunto dal database dall'elenco delle opzioni e selezionare "Avanti".



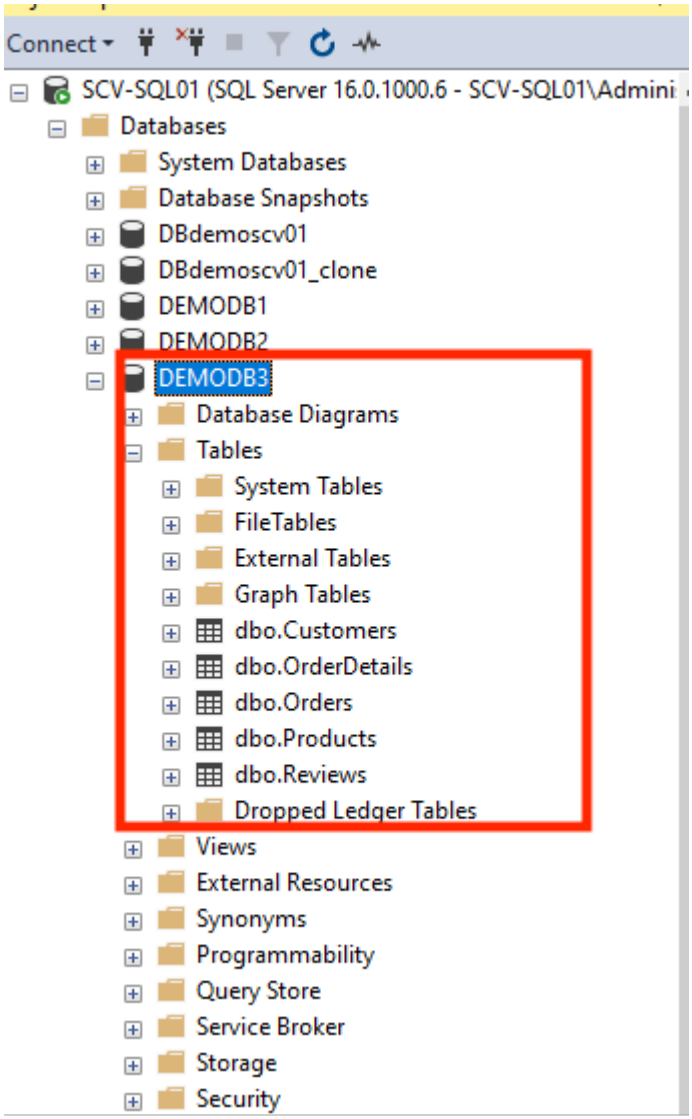
6. Nella pagina di riepilogo, seleziona "Finish".



7. Monitora il lavoro fino al completamento.



8. Verificare che le tabelle eliminate siano state ripristinate correttamente.



Conclusione

In questo documento, abbiamo fornito una guida dettagliata passo dopo passo per distribuire, configurare e utilizzare SCV e "SnapCenter Plug-in per SQL Server (SCSQL)" durante l'utilizzo di FSx for ONTAP come datastore supplementare con i cluster Amazon EVS.

Conclusione

In sintesi, quando si utilizza FSx for ONTAP per ottimizzare il TCO di un'implementazione Amazon EVS, SCV offre un metodo semplice ed efficiente per il backup delle VM. Può eseguire il backup e il ripristino delle VM in modo fluido e rapido, poiché si basa su Snapshot, il cui completamento richiede letteralmente pochi secondi.

"Prova il plug-in SnapCenter per VMware ora gratuitamente".

NetApp per Azure / AVS

Funzionalità NetApp per Azure AVS

Scopri di più sulle funzionalità che NetApp apporta ad Azure VMware Solution (AVS): da NetApp come dispositivo di archiviazione connesso guest o come datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/bursting nel cloud, al backup/ripristino e al disaster recovery.

Passa alla sezione del contenuto desiderato selezionando tra le seguenti opzioni:

- "Configurazione di AVS in Azure"
- "Opzioni di archiviazione NetApp per AVS"
- "Soluzioni cloud NetApp /VMware"

Configurazione di AVS in Azure

Come per l'ambiente on-premise, la pianificazione di un ambiente di virtualizzazione basato su cloud è fondamentale per un ambiente di produzione di successo per la creazione di VM e la migrazione.

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

> L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad Azure VMware Solution.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Registra il fornitore di risorse e crea un cloud privato
- Connettiti a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalida la connettività di rete e accedi al cloud privato

Visualizza il dettaglio"passaggi di configurazione per AVS" .

Opzioni di archiviazione NetApp per AVS

Lo storage NetApp può essere utilizzato in diversi modi, come connessione Guess o come datastore NFS supplementare, all'interno di Azure AVS.

Per favore visita"Opzioni di archiviazione NetApp supportate" per maggiori informazioni.

Azure supporta l'archiviazione NetApp nelle seguenti configurazioni:

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

Visualizza il dettaglio"opzioni di archiviazione di connessione ospite per AVS" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per AVS" .

Casi d’uso della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi d’uso sono semplici da implementare in Azure AVS. Questi casi sono definiti per ciascuna delle aree cloud definite da VMware:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Estendere
- Migrare

"Esplora le soluzioni NetApp per Azure AVS"

Proteggi i carichi di lavoro su Azure/AVS

Disaster Recovery con ANF e JetStream

Il disaster recovery nel cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware). Utilizzando il framework VMware VAIO, i carichi di lavoro VMware locali possono essere replicati nell’archiviazione BLOB di Azure e ripristinati, consentendo una perdita di dati minima o quasi nulla e un RTO prossimo allo zero.

JetStream DR può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da locale ad AVS e in particolare ad Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime nel sito DR e un archivio cloud conveniente. JetStream DR automatizza il ripristino nei datastore ANF tramite Azure Blob Storage. JetStream DR recupera VM indipendenti o gruppi di VM correlate nell’infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino puntuale per la protezione dal ransomware.

Questo documento fornisce una comprensione dei principi operativi di JetStream DR e dei suoi componenti principali.

▼ Panoramica della distribuzione della soluzione

1. Installare il software JetStream DR nel data center locale.
    a. Scarica il pacchetto software JetStream DR da Azure Marketplace (ZIP) e distribuisci JetStream DR MSA (OVA) nel cluster designato.
    b. Configurare il cluster con il pacchetto filtro I/O (installare JetStream VIB).
    c. Eseguire il provisioning di Azure Blob (account di archiviazione di Azure) nella stessa area del cluster DR AVS.
    d. Distribuisci appliance DRVA e assegna volumi di log di replicazione (VMDK da datastore esistente o storage iSCSI condiviso).
    e. Creare domini protetti (gruppi di VM correlate) e assegnare DRVA e Azure Blob Storage/ANF.
    f. Protezione iniziale.
2. Installare il software JetStream DR nel cloud privato Azure VMware Solution.
    a. Utilizzare il comando Esegui per installare e configurare JetStream DR.
    b. Aggiungere lo stesso contenitore BLOB di Azure e individuare i domini utilizzando l’opzione Scansiona domini.
    c. Distribuire gli apparecchi DRVA richiesti.

d. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.

e. Importa domini protetti e configura RocVA (VA di ripristino) per utilizzare il datastore ANF per i posizionamenti delle VM.

f. Selezionare l'opzione di failover appropriata e avviare la reidratazione continua per domini o VM con RTO prossimo allo zero.

3. Durante un evento di emergenza, attiva il failover nei datastore di Azure NetApp Files nel sito AVS DR designato.
4. Richiamare il failback al sito protetto dopo che il sito protetto è stato ripristinato. Prima di iniziare, assicurarsi che i prerequisiti siano soddisfatti come indicato in questo "collegamento" ed eseguire anche lo strumento di test della larghezza di banda (BWT) fornito da JetStream Software per valutare le potenziali prestazioni dell'archiviazione BLOB di Azure e la sua larghezza di banda di replica quando utilizzato con il software JetStream DR. Dopo aver soddisfatto i prerequisiti, inclusa la connettività, configurare e abbonarsi a JetStream DR per AVS da "Azure Marketplace" . Dopo aver scaricato il pacchetto software, procedere con il processo di installazione descritto sopra.

Quando si pianifica e si avvia la protezione per un numero elevato di VM (ad esempio, più di 100), utilizzare lo strumento di pianificazione della capacità (CPT) di JetStream DR Automation Toolkit. Fornire un elenco delle VM da proteggere insieme alle relative preferenze RTO e gruppo di ripristino, quindi eseguire CPT.

Il CPT svolge le seguenti funzioni:

- Combinazione di VM in domini di protezione in base al loro RTO.
- Definizione del numero ottimale di DRVA e delle relative risorse.
- Stima della larghezza di banda di replicazione richiesta.
- Identificazione delle caratteristiche del volume del registro di replicazione (capacità, larghezza di banda e così via).
- Stima della capacità di archiviazione degli oggetti richiesta e altro ancora.



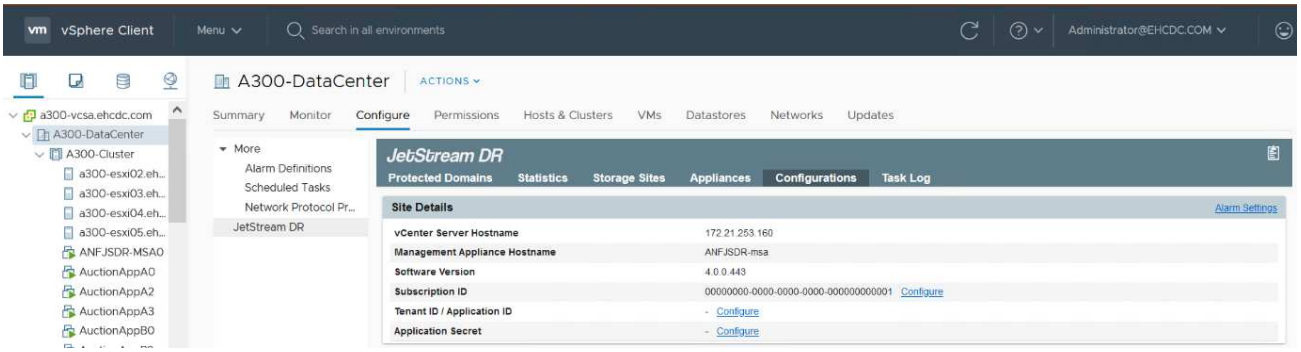
Il numero e il contenuto dei domini prescritti dipendono da varie caratteristiche della VM, come IOPS medi, capacità totale, priorità (che definisce l'ordine di failover), RTO e altro.

Installa JetStream DR nel data center locale

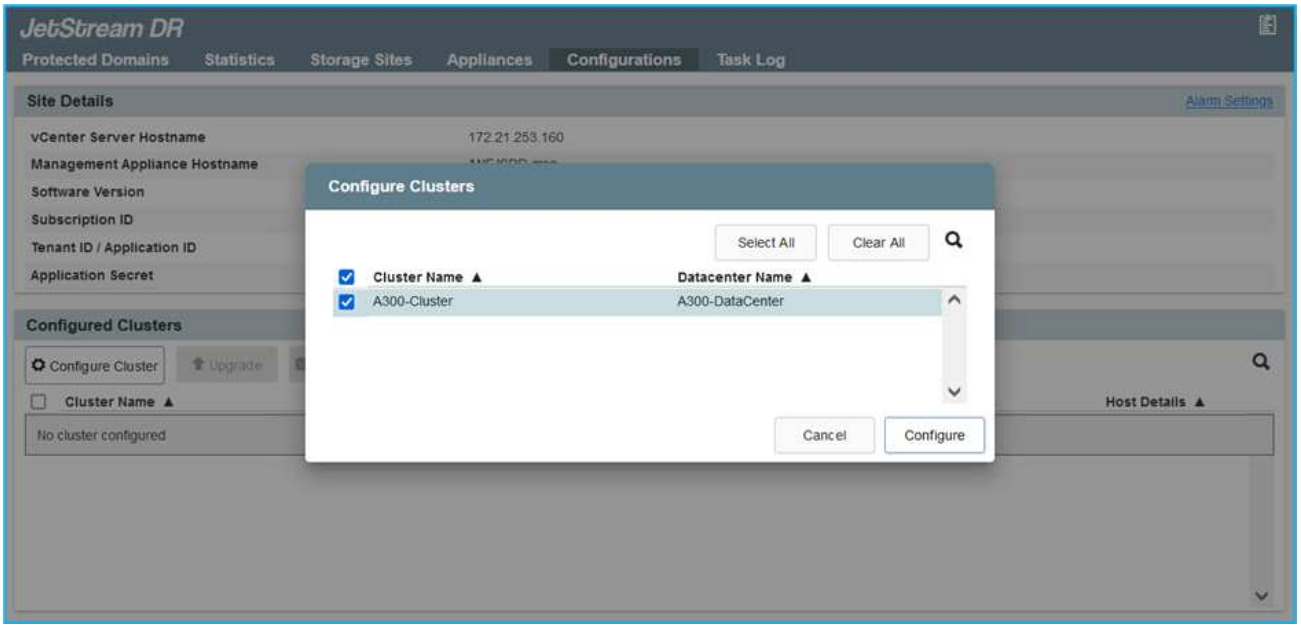
Il software JetStream DR è costituito da tre componenti principali: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) e componenti host (pacchetti di filtri I/O). MSA viene utilizzato per installare e configurare i componenti host sul cluster di elaborazione e quindi per amministrare il software JetStream DR. L'elenco seguente fornisce una descrizione di alto livello del processo di installazione:

▼ Come installare JetStream DR per ambienti locali

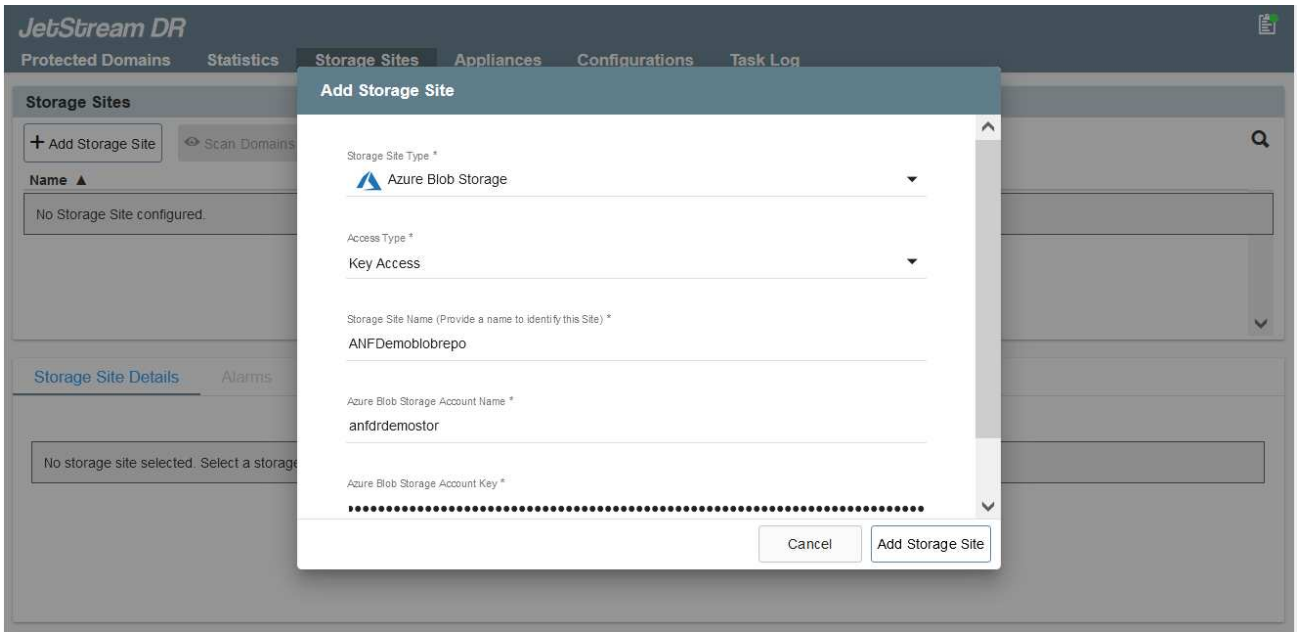
1. Verificare i prerequisiti.
2. Eseguire lo strumento di pianificazione della capacità per ottenere consigli su risorse e configurazione (facoltativo ma consigliato per le prove di proof-of-concept).
3. Distribuire JetStream DR MSA su un host vSphere nel cluster designato.
4. Avviare l'MSA utilizzando il suo nome DNS in un browser.
5. Registrare il server vCenter con MSA. Per eseguire l'installazione, completare i seguenti passaggi dettagliati:
6. Dopo aver distribuito JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR tramite vSphere Web Client. Per farlo, andare su Datacenter > Configura > JetStream DR.



7. Dall'interfaccia JetStream DR, selezionare il cluster appropriato.



8. Configurare il cluster con il pacchetto filtro I/O.

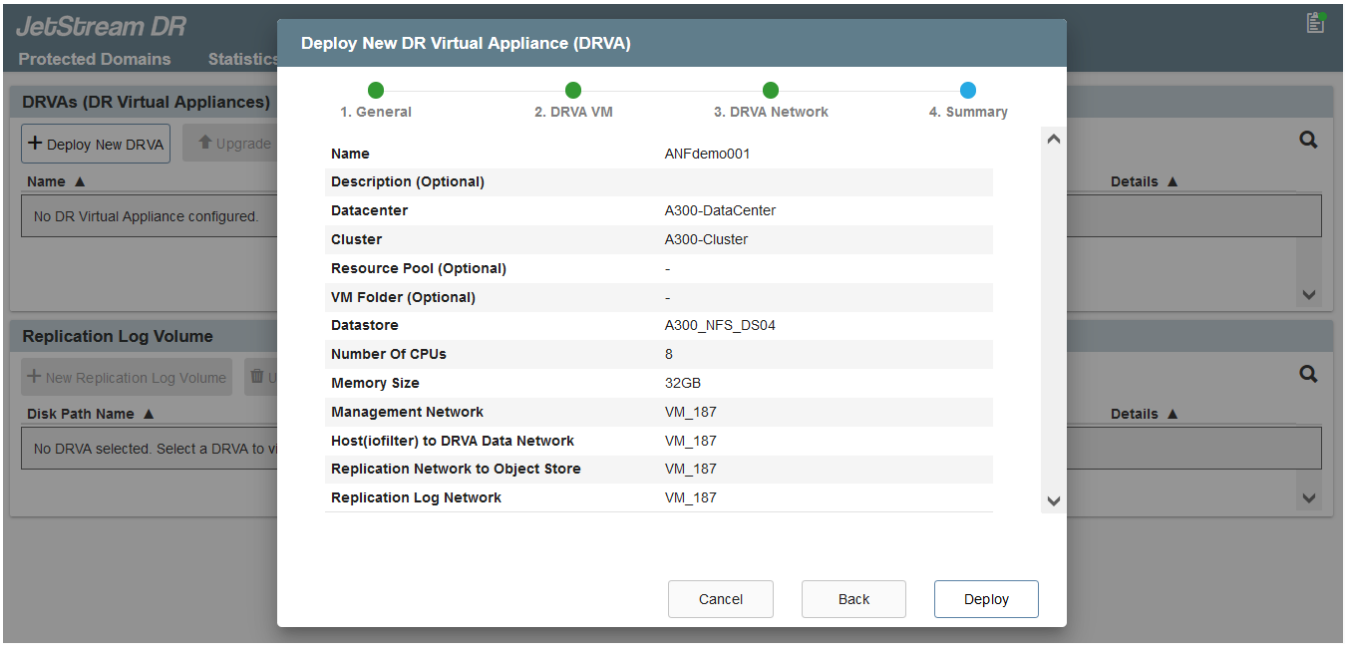


9. Aggiungere Azure Blob Storage situato nel sito di ripristino.

10. Distribuire un DR Virtual Appliance (DRVA) dalla scheda Appliance.

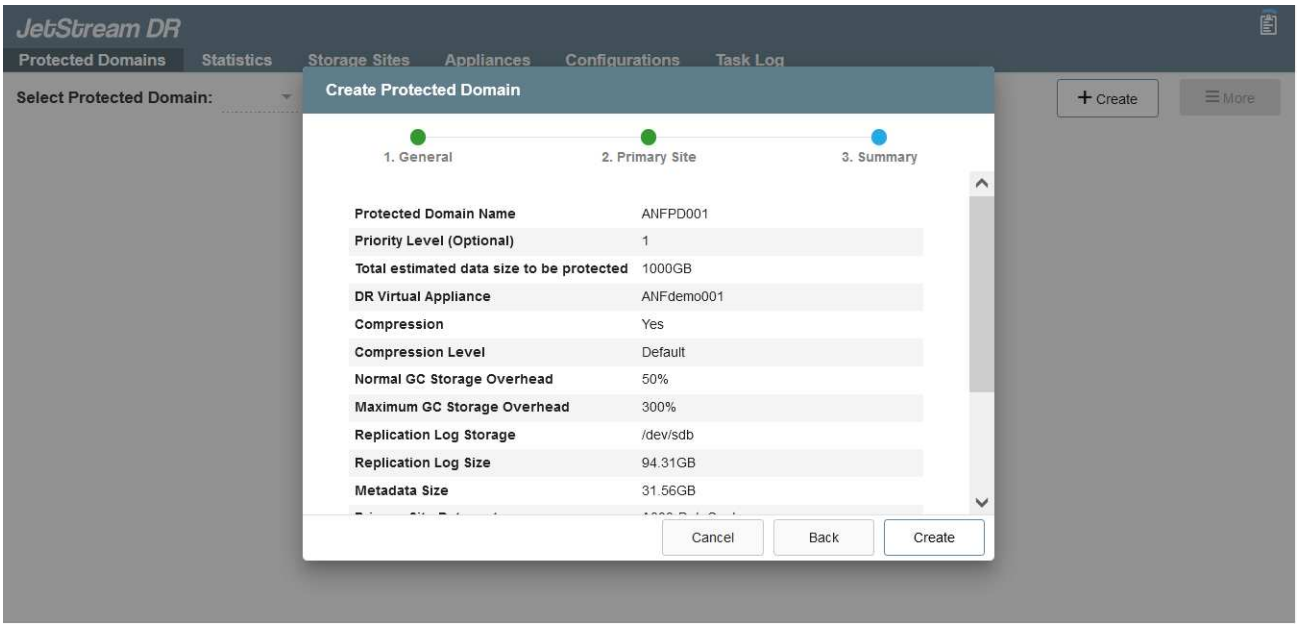
> I DRVA possono essere creati automaticamente da CPT, ma per le prove POC consigliamo di configurare ed eseguire manualmente il ciclo DR (avvio protezione > failover > failback).

JetStream DRVA è un dispositivo virtuale che semplifica le funzioni chiave nel processo di replicazione dei dati. Un cluster protetto deve contenere almeno un DRVA e in genere ne viene configurato uno per host. Ogni DRVA può gestire più domini protetti.



In questo esempio sono stati creati quattro DRVA per 80 macchine virtuali.

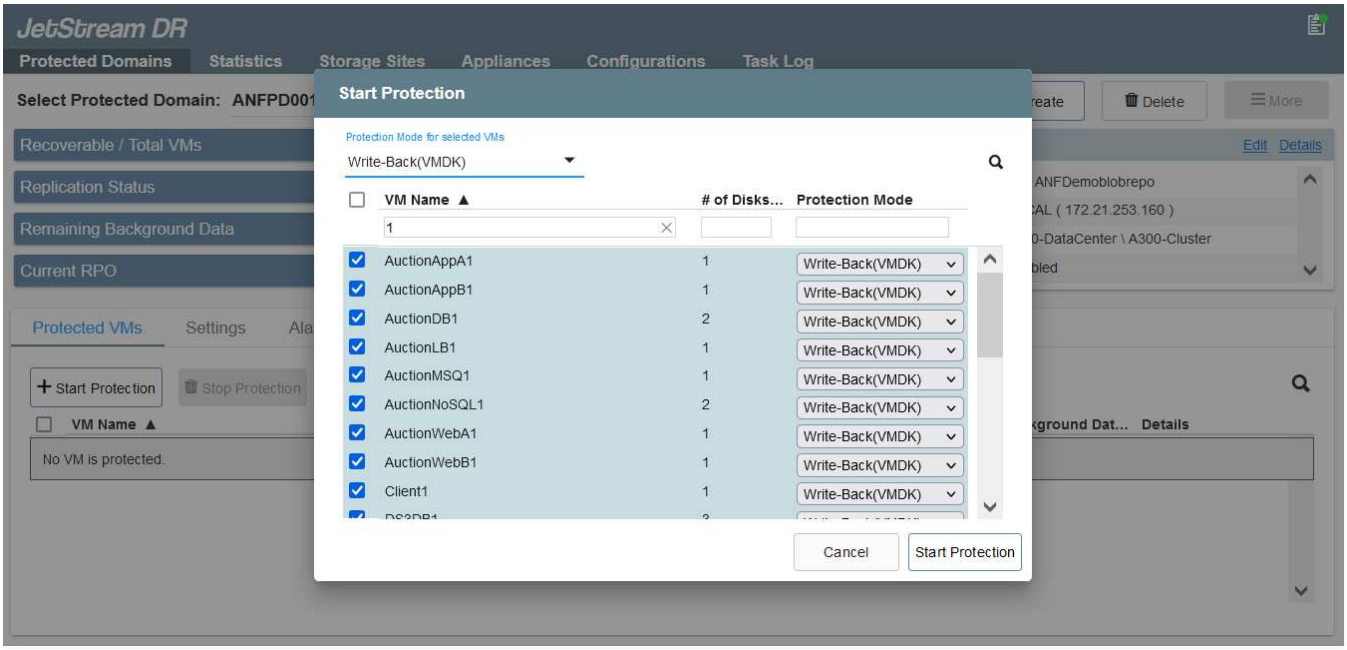
1. Creare volumi di registro di replica per ogni DRVA utilizzando VMDK dai datastore disponibili o da pool di storage iSCSI condivisi indipendenti.
2. Dalla scheda Domini protetti, creare il numero richiesto di domini protetti utilizzando le informazioni sul sito di Azure Blob Storage, l'istanza DRVA e il registro di replica. Un dominio protetto definisce una VM specifica o un set di VM all'interno del cluster, protette insieme e a cui viene assegnato un ordine di priorità per le operazioni di failover/failback.



3. Selezionare le VM che si desidera proteggere e avviare la protezione delle VM del dominio protetto. In questo modo viene avviata la replica dei dati nel Blob Store designato.

Verificare che venga utilizzata la stessa modalità di protezione per tutte le VM in un dominio protetto.

La modalità Write-Back (VMDK) può offrire prestazioni più elevate.



Verificare che i volumi del registro di replica siano posizionati su un archivio ad alte prestazioni.

I run book di failover possono essere configurati per raggruppare le VM (denominate Recovery Group), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

Installa JetStream DR per AVS in un cloud privato di Azure VMware Solution utilizzando il comando Esegui

Una buona pratica per un sito di ripristino (AVS) è quella di creare in anticipo un cluster di luci 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 di volumi ANF come datastore e altro ancoraJetStream DR supporta la modalità RTO prossima allo zero per domini mission-critical. Per questi domini, lo storage di destinazione dovrebbe essere preinstallato. In questo caso, l'ANF è il tipo di archiviazione consigliato.

> La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS in modo da soddisfare i requisiti locali.

A seconda dei requisiti SLA e RTO, è possibile utilizzare la modalità failover continuo o failover regolare (standard). Per un RTO prossimo allo zero, la reidratazione continua deve essere avviata nel sito di recupero.

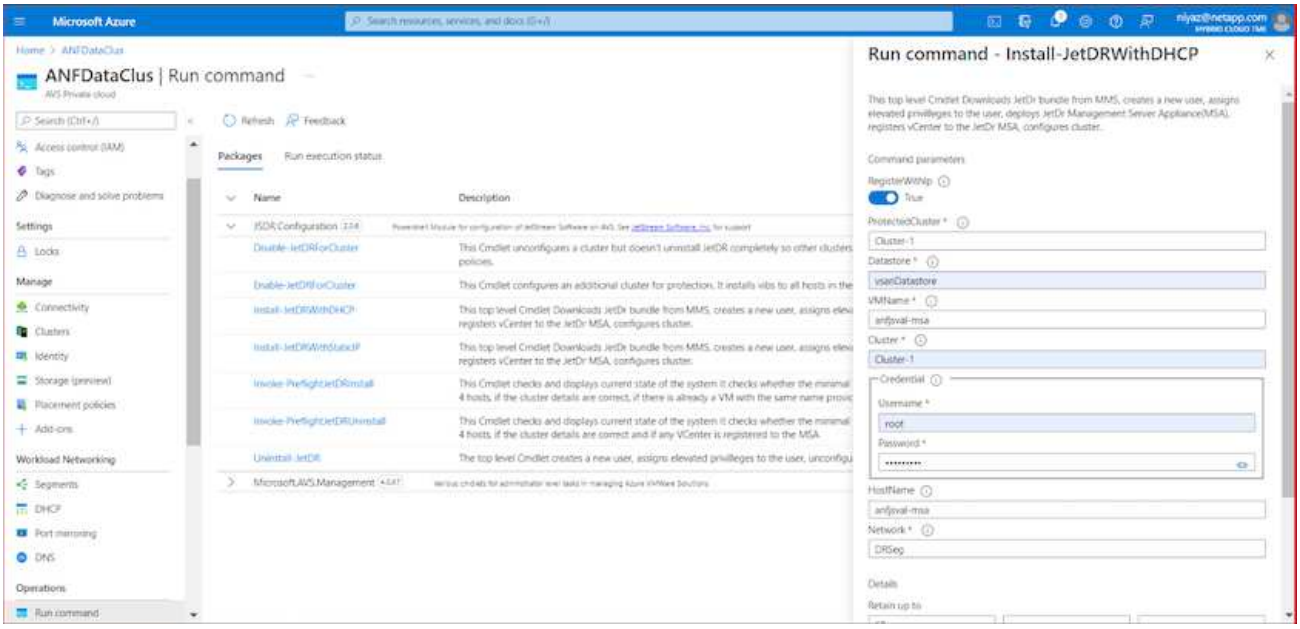
▼ **Come installare JetStream DR per AVS in un cloud privato**

Per installare JetStream DR per AVS su un cloud privato di Azure VMware Solution, completare i seguenti passaggi:

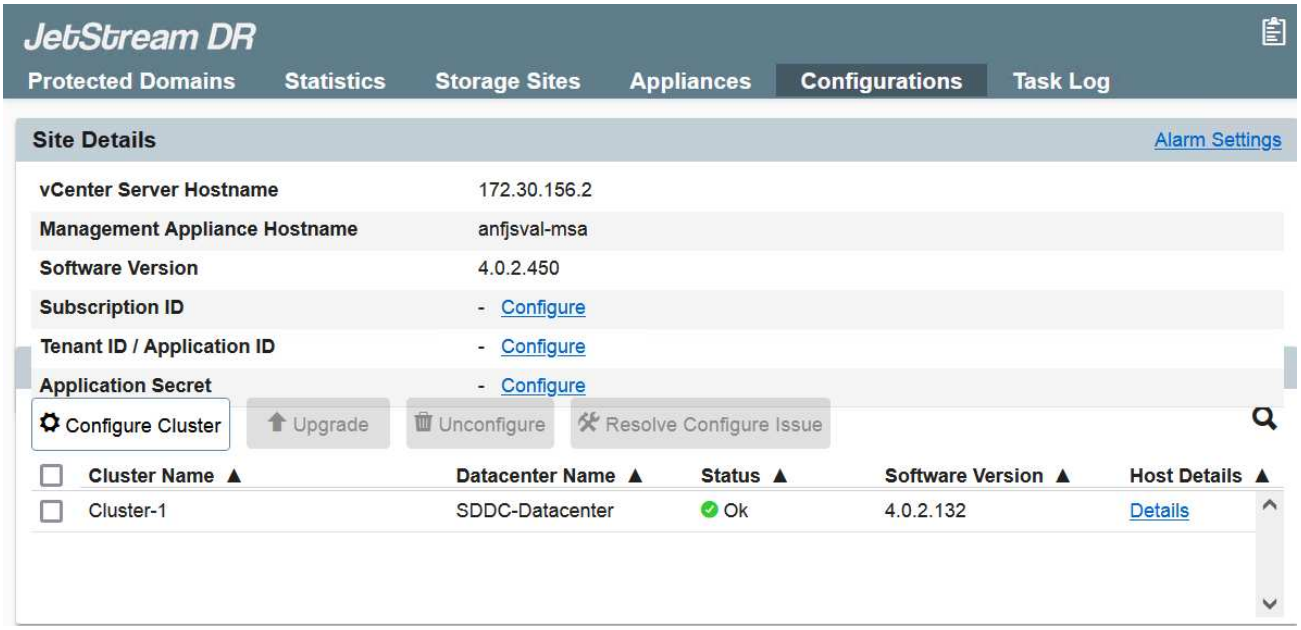
1. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato e seleziona Esegui comando > Pacchetti > JSDR.Configuration.

> L'utente CloudAdmin predefinito in Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente l'installazione semplificata e automatizzata di JetStream DR richiamando il comando Esegui di Azure VMware Solution per JetStream DR.

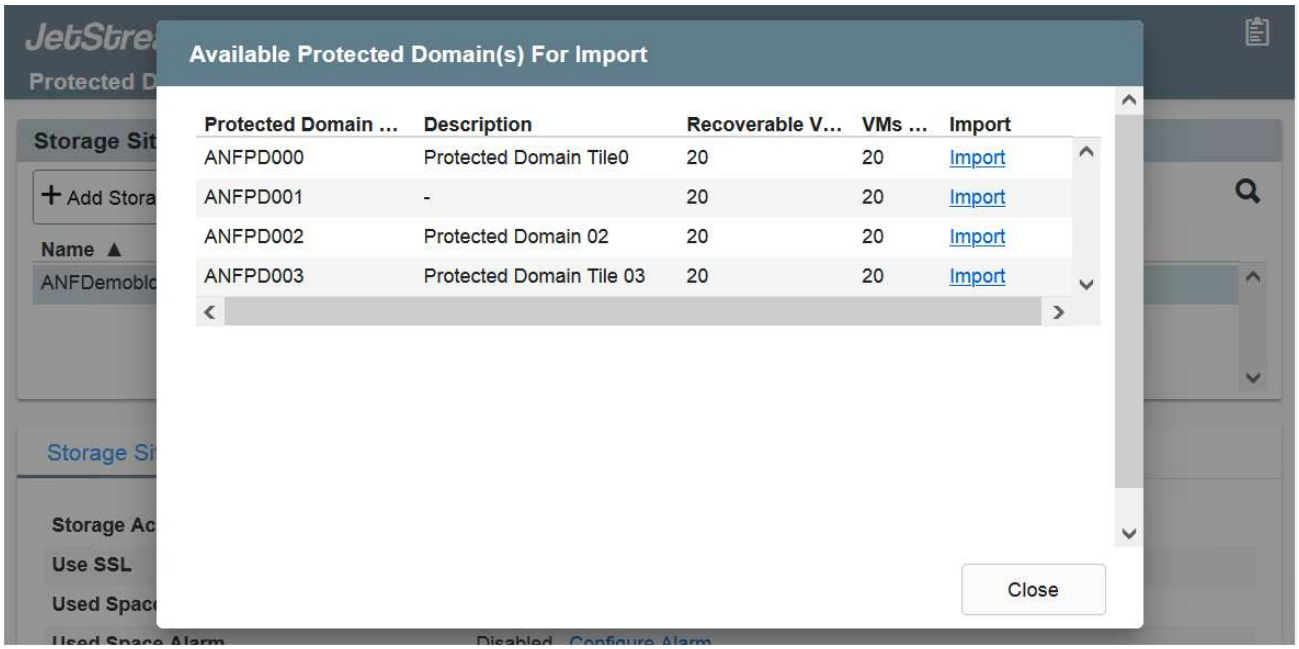
La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente di JetStream DR, andare su SDDC Datacenter > Configura > JetStream DR.



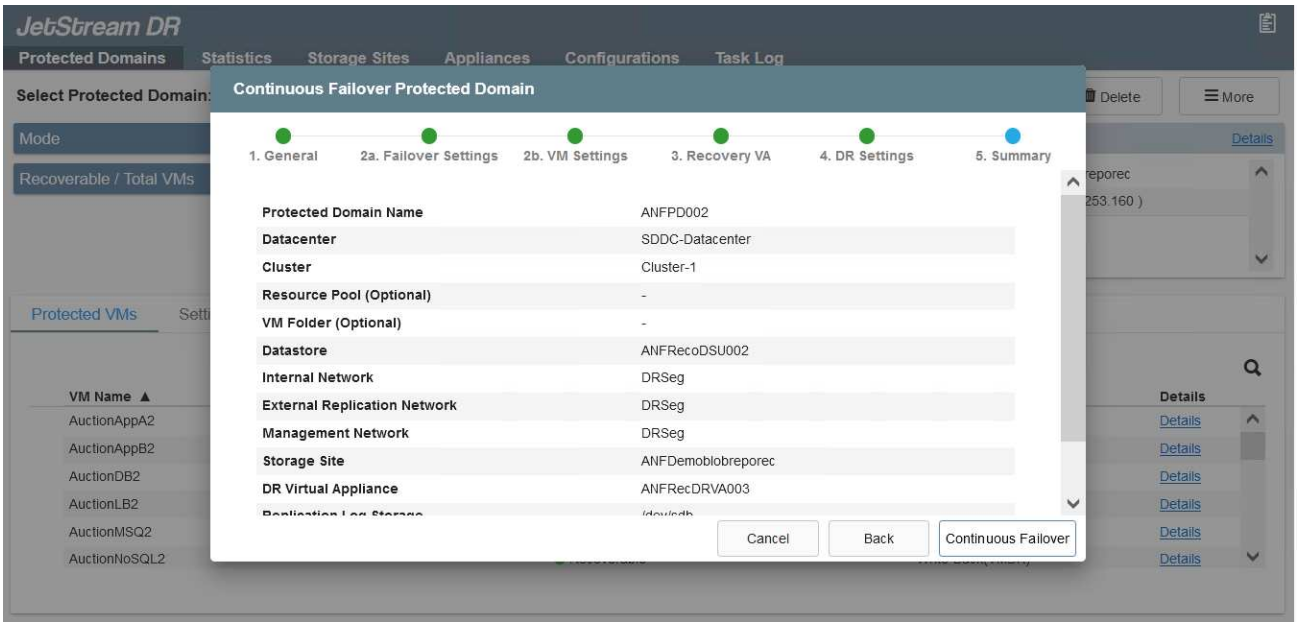
3. Dall'interfaccia JetStream DR, aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster locale come sito di archiviazione, quindi eseguire l'opzione Scansiona domini.



4. Dopo aver importato i domini protetti, distribuire gli appliance DRVA. In questo esempio, la reidratazione continua viene avviata manualmente dal sito di ripristino tramite l'interfaccia utente di JetStream DR.

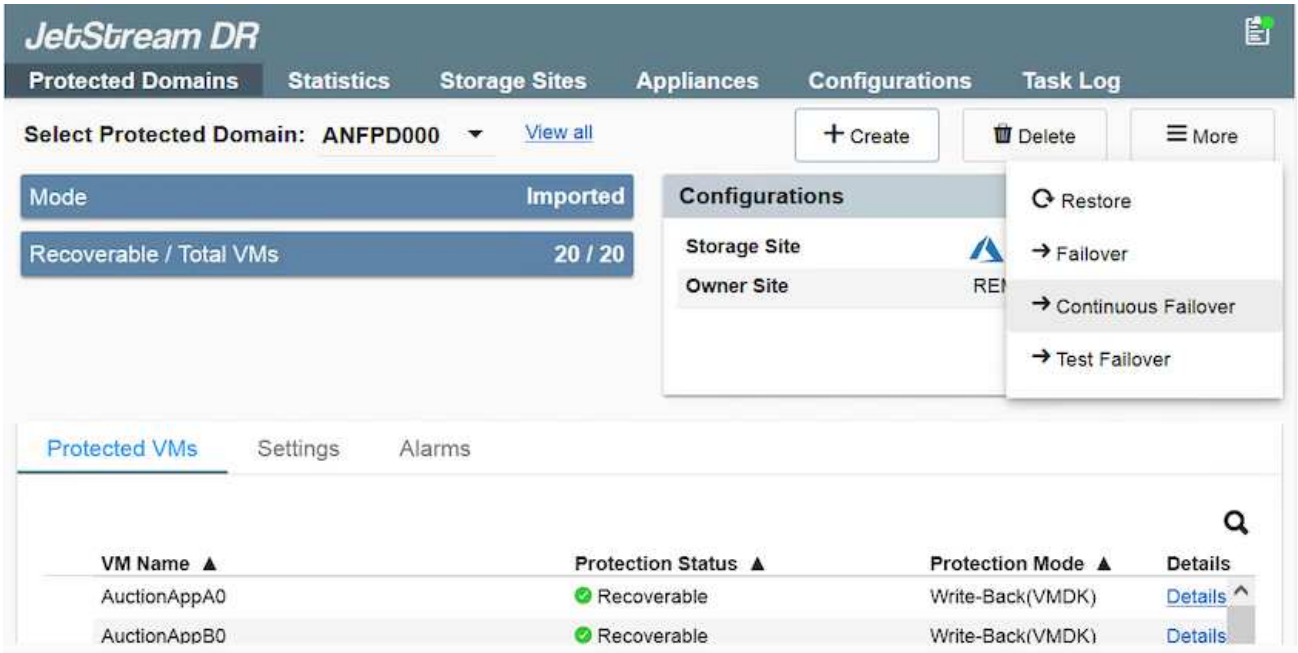
> Questi passaggi possono anche essere automatizzati utilizzando i piani creati da CPT.

5. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.
6. Importare i domini protetti e configurare Recovery VA per utilizzare il datastore ANF per i posizionamenti delle VM.



Assicurarsi che DHCP sia abilitato sul segmento selezionato e che siano disponibili sufficienti IP. Gli IP dinamici vengono utilizzati temporaneamente mentre i domini sono in fase di ripristino. Ogni VM in fase 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 continuo o failover). In questo esempio è stata selezionata la reidratazione continua (failover continuo).



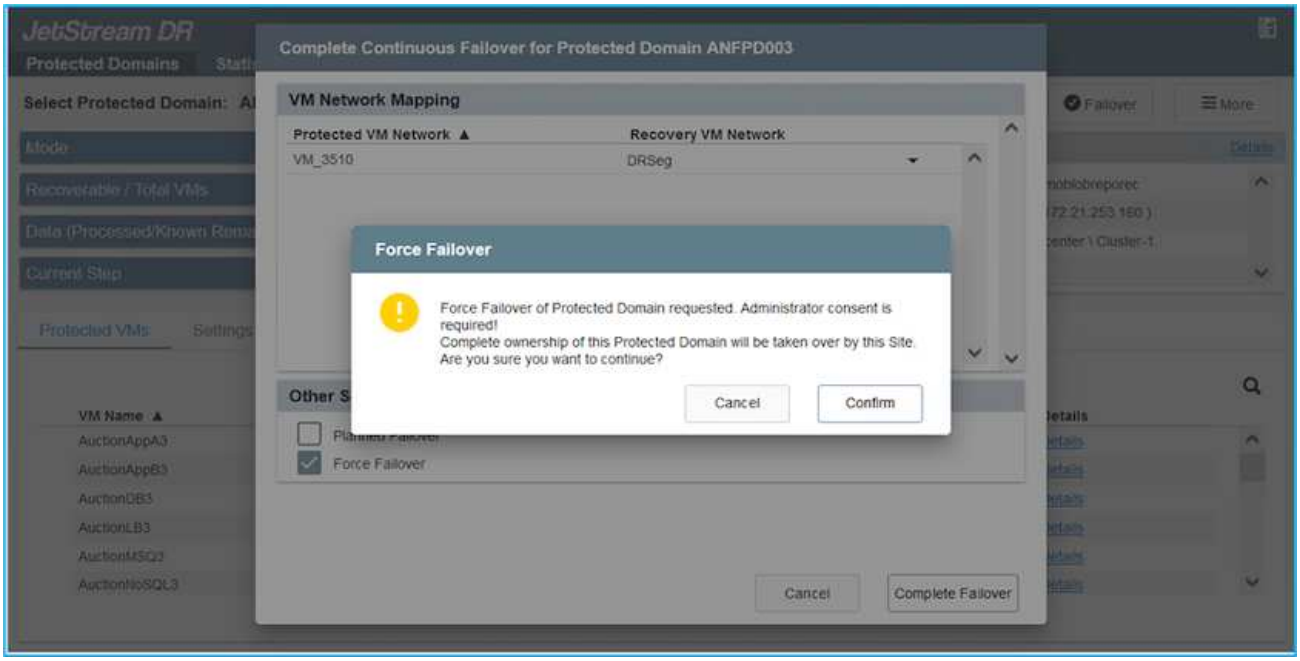
Esecuzione di failover/failback

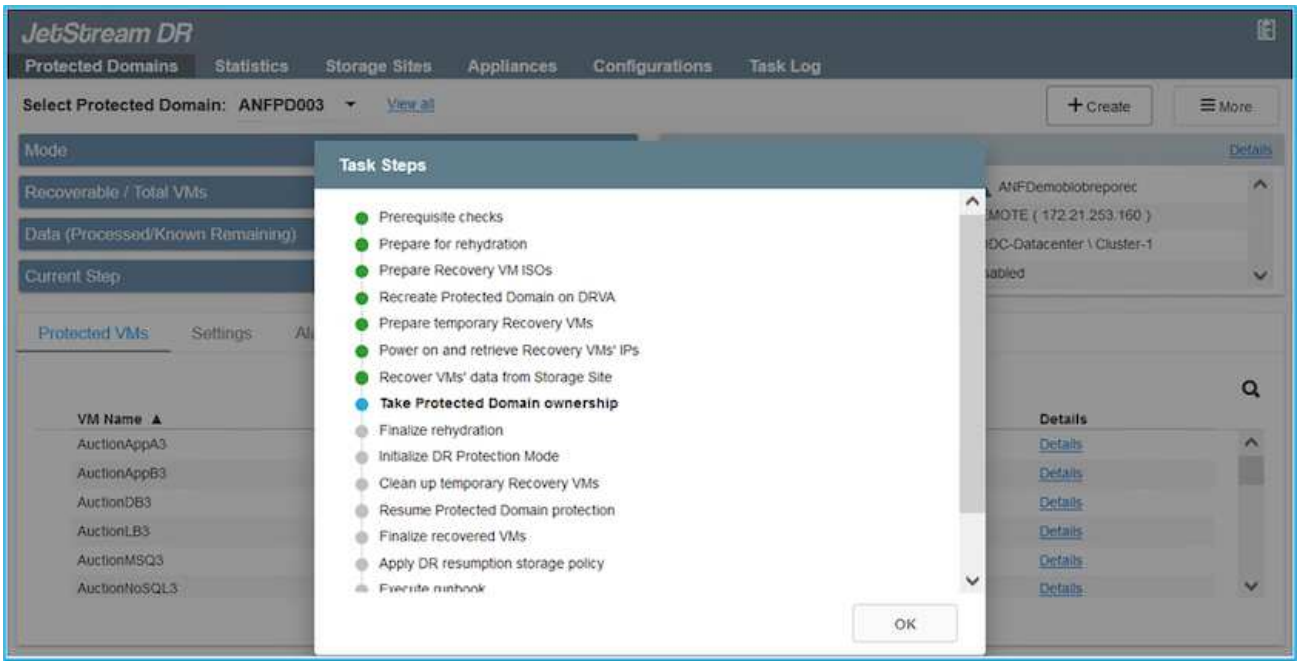
▼ Come eseguire un Failover/Failback

1. Dopo che si è verificato un disastro nel cluster protetto dell'ambiente on-premise (guasto parziale o totale), attivare il failover.

CPT può essere utilizzato per eseguire il piano di failover per ripristinare le VM da Azure Blob Storage nel sito di ripristino del cluster AVS.

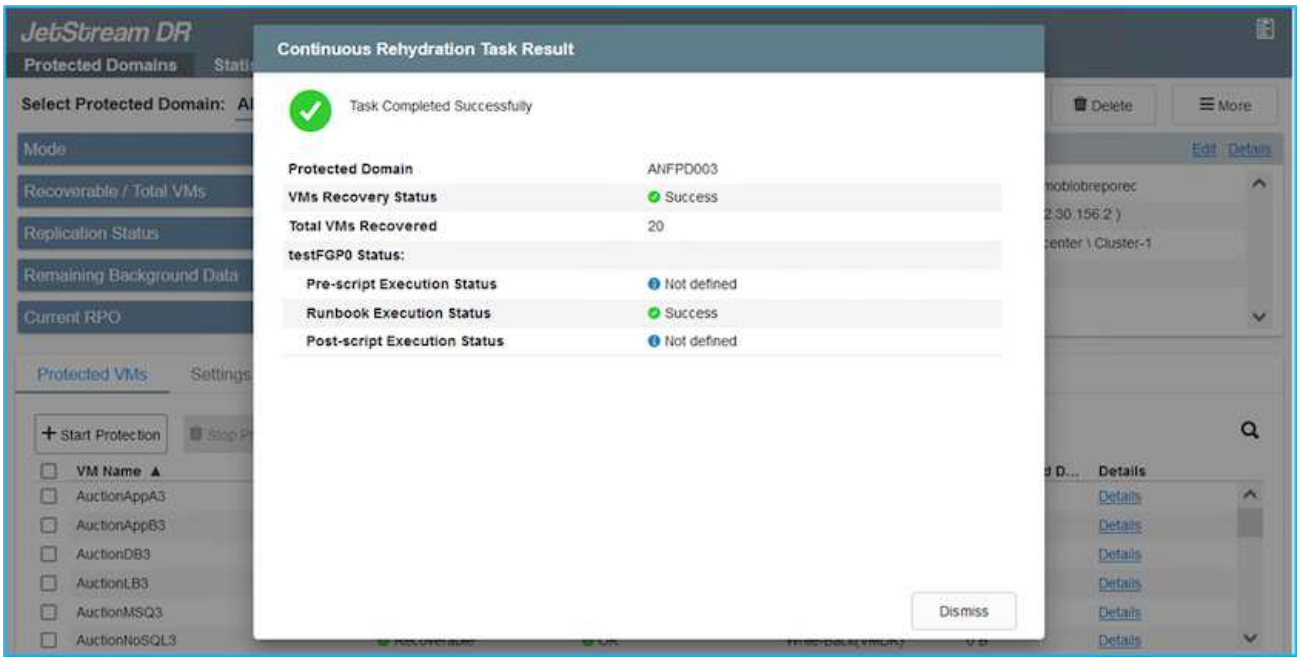
Dopo il failover (per la reidratazione continua o standard), quando le VM protette sono state avviate in AVS, la protezione viene automaticamente ripresa e JetStream DR continua a replicare i dati nei contenitori appropriati/originali in Azure Blob Storage.





La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

2. Una volta completata l'attività, accedi alle VM recuperate e le attività riprenderanno normalmente.

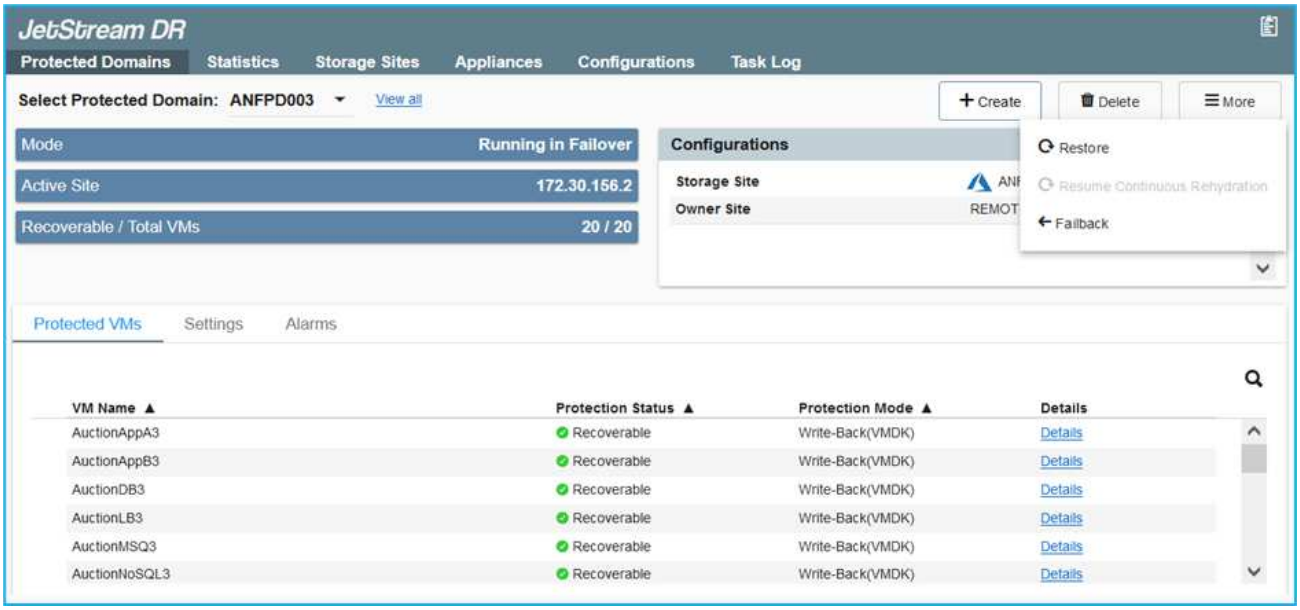


Una volta che il sito primario è di nuovo attivo e funzionante, è possibile eseguire il failback. La protezione della VM è ripristinata e occorre verificare la coerenza dei dati.

3. Ripristinare l'ambiente locale. A seconda del tipo di incidente di emergenza, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software JetStream DR.

> Nota: Il `recovery_utility_prepare_failback` Lo script fornito nell'Automation Toolkit può essere utilizzato per pulire il sito protetto originale da eventuali VM obsolete, informazioni di dominio e così via.

4. Accedere all'ambiente locale ripristinato, andare all'interfaccia utente di Jetstream DR e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione Failback nell'interfaccia utente.



Il piano di failback generato da CPT può essere utilizzato anche per avviare il ritorno delle VM e dei relativi dati dall'archivio oggetti all'ambiente VMware originale.

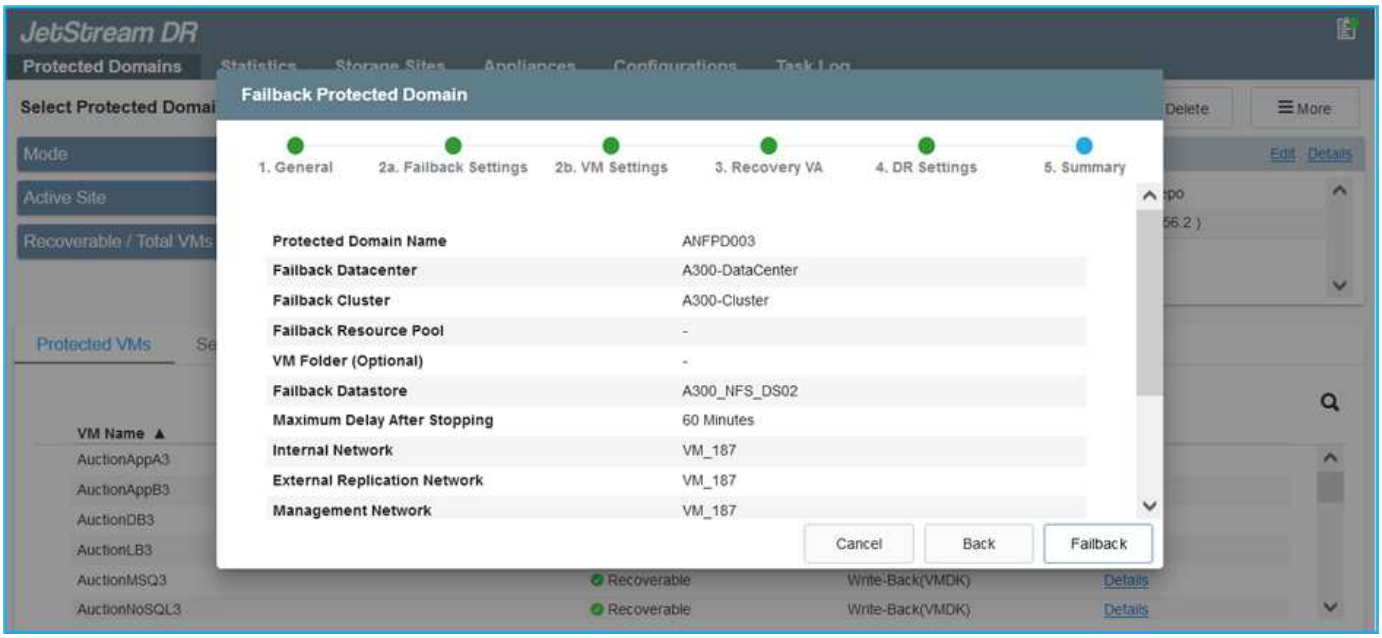
Specificare il ritardo massimo dopo la sospensione delle VM nel sito di ripristino e il riavvio nel sito protetto. Questo tempo include il completamento della replica dopo l'arresto delle VM di failover, il tempo per pulire il sito di ripristino e il tempo per ricreare le VM nel sito protetto. Il valore consigliato NetApp è 10 minuti.

Completare il processo di failback, quindi confermare la ripresa della protezione della VM e la coerenza dei dati.

Recupero da ransomware

Recuperare i dati da un ransomware può essere un compito arduo. Nello specifico, 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 ricorrenti (da malware inattivi o tramite applicazioni vulnerabili).

JetStream DR per AVS insieme ai datastore Azure NetApp Files possono risolvere questi problemi consentendo alle organizzazioni di eseguire il ripristino da punti temporali disponibili, in modo che i carichi di lavoro vengano ripristinati su una rete funzionale e isolata, se necessario. Il ripristino consente alle applicazioni di funzionare e comunicare tra loro senza esporle al traffico nord-sud, offrendo così ai team di sicurezza un luogo sicuro in cui eseguire analisi forensi e altre azioni correttive necessarie.

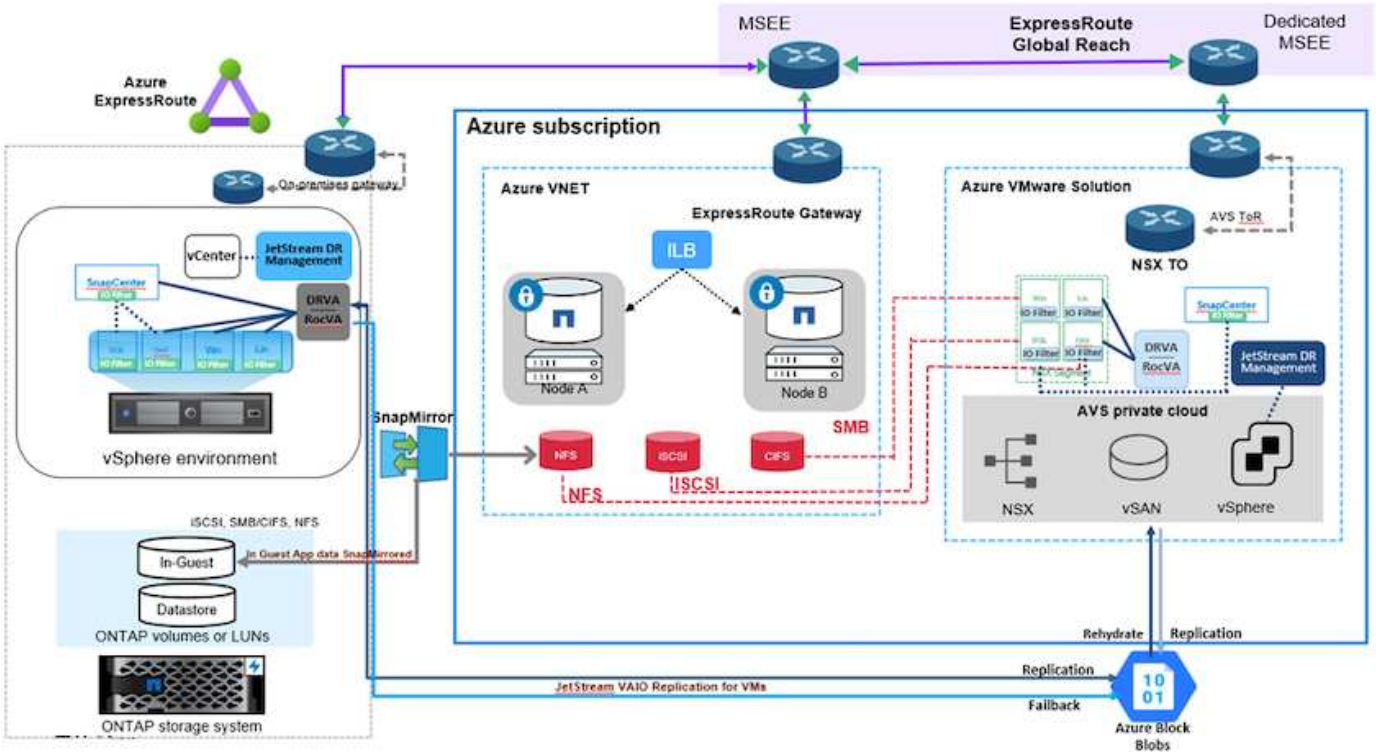


Disaster Recovery con CVO e AVS (archiviazione connessa agli ospiti)

Il disaster recovery sul cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati come il ransomware. Con NetApp SnapMirror, i carichi di lavoro VMware locali che utilizzano storage connesso agli ospiti possono essere replicati su NetApp Cloud Volumes ONTAP in esecuzione in Azure.

Panoramica

This covers application data; however, what about the actual VMs themselves. Disaster recovery should cover all dependent components, including virtual machines, VMDKs, application data, and more. To accomplish this, SnapMirror along with Jetstream can be used to seamlessly recover workloads replicated from on-premises to Cloud Volumes ONTAP while using vSAN storage for VM VMDKs.
Questo documento fornisce un approccio dettagliato per la configurazione e l'esecuzione del disaster recovery utilizzando NetApp SnapMirror, JetStream e Azure VMware Solution (AVS).



Ipotesi

Questo documento si concentra sull'archiviazione in-guest per i dati delle applicazioni (nota anche come guest connected) e presuppone che l'ambiente locale utilizzi SnapCenter per backup coerenti con le applicazioni.

> Il presente documento si applica 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 aziendali.

Per la connettività tra l'ambiente locale e la rete virtuale di Azure, utilizzare la portata globale del percorso espresso o una WAN virtuale con un gateway VPN. I segmenti devono essere creati in base alla progettazione della VLAN locale.

> Esistono diverse opzioni per connettere i data center locali ad Azure, il che ci impedisce di

descrivere un flusso di lavoro specifico in questo documento. Per il metodo di connettività locale-Azure appropriato, fare riferimento alla documentazione di Azure.

Distribuzione della soluzione DR

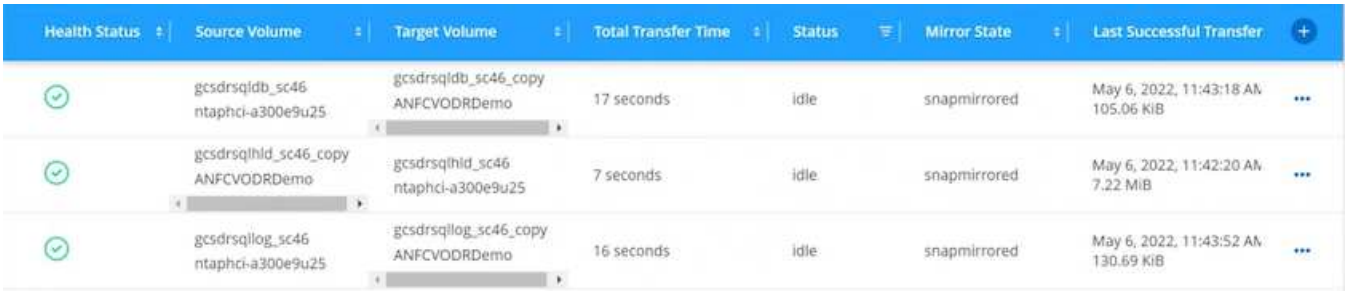
Panoramica sulla distribuzione della soluzione

1. Assicurarsi che i dati dell'applicazione vengano sottoposti a backup tramite SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning Cloud Volumes ONTAP con la dimensione corretta dell'istanza utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
   a. Configurare SnapMirror per i volumi applicativi pertinenti.
   b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti SnapMirror dopo i processi pianificati.
3. Installare il software JetStream DR nel data center locale e avviare la protezione per le macchine virtuali.
4. Installare il software JetStream DR nel cloud privato Azure VMware Solution.
5. Durante un evento di emergenza, interrompere la relazione SnapMirror tramite Cloud Manager e attivare il failover delle macchine virtuali su Azure NetApp Files o sui datastore vSAN nel sito AVS DR designato.
   a. Ricollegare i LUN ISCSI e i mount NFS per le VM dell'applicazione.
6. Richiamare il failback sul sito protetto tramite la risincronizzazione inversa SnapMirror dopo il ripristino del sito primario.

Dettagli di distribuzione

▼ 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 e le conservazioni degli snapshot desiderate.



▼ Configurare gli host AVS e l'accesso ai dati CVO

Due fattori importanti da considerare quando si distribuisce l'SDDC sono le dimensioni del cluster SDDC nella soluzione Azure VMware e per quanto tempo mantenere in servizio l'SDDC. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. L'SDDC può essere composto da un minimo di tre host, fino a diventare un cluster multi-host in una distribuzione su larga scala.

La decisione di implementare un cluster AVS si basa principalmente sui requisiti RPO/RTO. Grazie alla soluzione Azure VMware, l'SDDC può essere predisposto just in time in preparazione per i test o per un evento di emergenza effettivo. Un SDDC distribuito just-in-time consente di risparmiare sui costi di hosting ESXi quando non si è alle prese con un disastro. Tuttavia, questa forma di distribuzione influisce sull'RTO di alcune ore durante il provisioning di SDDC.

L’opzione più comunemente implementata è quella di far funzionare l’SDDC in modalità di funzionamento sempre acceso, con spia luminosa. Questa opzione occupa poco spazio, con tre host sempre disponibili, e velocizza le operazioni di ripristino, fornendo una baseline funzionante per le attività di simulazione e i controlli di conformità, evitando così il rischio di discrepanze operative tra i siti di produzione e di ripristino di emergenza. Il gruppo di spie luminose può essere rapidamente ampliato fino al livello desiderato quando necessario per gestire un evento DR effettivo.

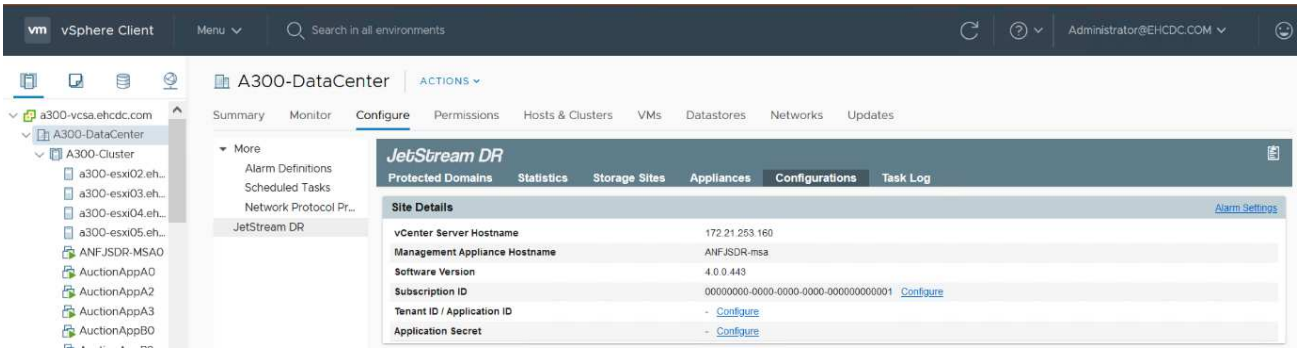
Per configurare AVS SDDC (sia su richiesta che in modalità pilota), vedere"Distribuire e configurare l’ambiente di virtualizzazione su Azure" . Come prerequisito, verificare che le VM guest residenti sugli host AVS siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e AVS, iniziare a configurare Jetstream per automatizzare il ripristino dei carichi di lavoro locali su AVS (VM con VMDK applicativi e VM con storage interno) utilizzando il meccanismo VAIO e sfruttando SnapMirror per le copie dei volumi applicativi su Cloud Volumes ONTAP.

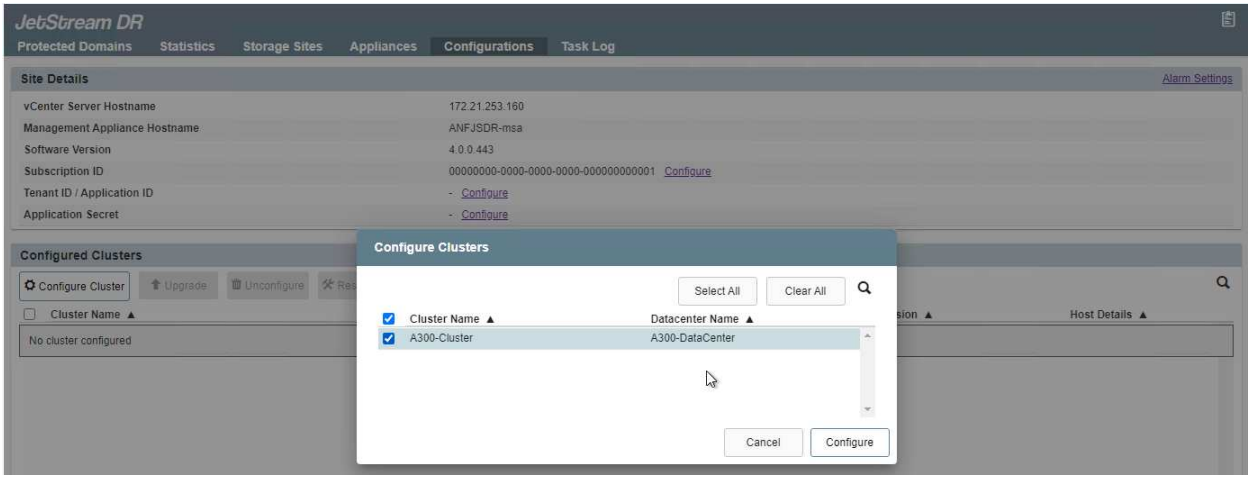
▼ Installa JetStream DR nel data center locale

Il software JetStream DR è costituito da tre componenti principali: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) e componenti host (pacchetti di filtri I/O). L’MSA viene utilizzato per installare e configurare i componenti host sul cluster di elaborazione e quindi per amministrare il software JetStream DR. Il processo di installazione è il seguente:

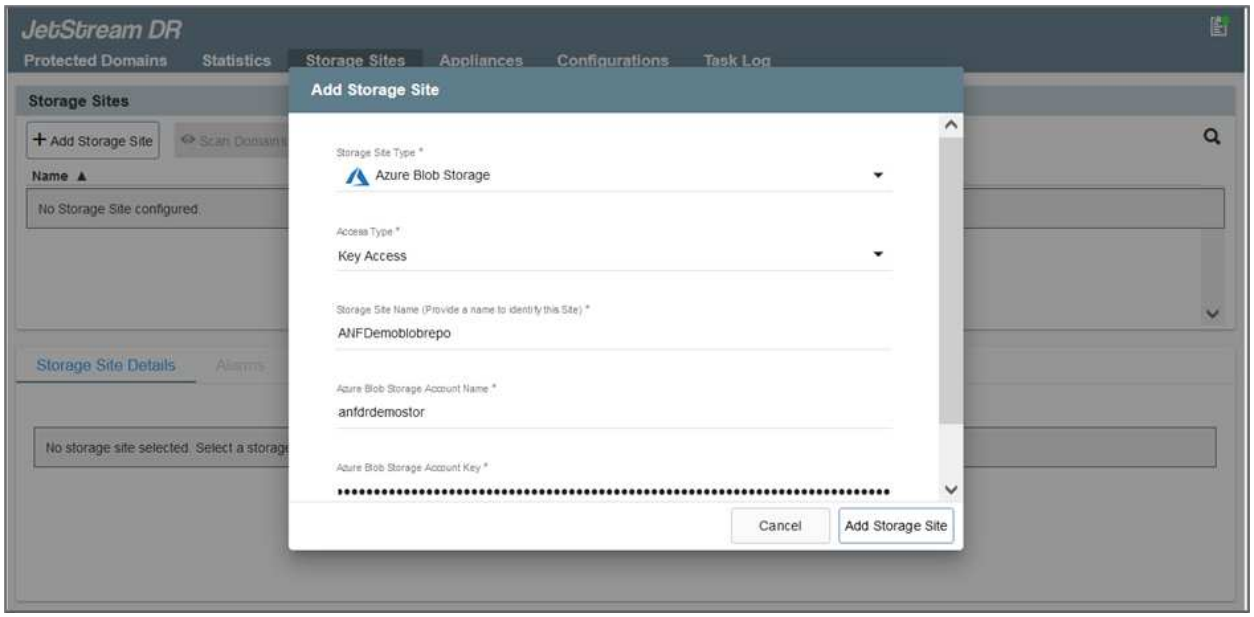
1. Verificare i prerequisiti.
2. Eseguire lo strumento di pianificazione della capacità per ottenere consigli su risorse e configurazioni.
3. Distribuire JetStream DR MSA su ciascun host vSphere nel cluster designato.
4. Avviare l’MSA utilizzando il suo nome DNS in un browser.
5. Registrare il server vCenter con MSA.
6. Dopo aver distribuito JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR con vSphere Web Client. Per farlo, andare su Datacenter > Configura > JetStream DR.



7. Dall’interfaccia JetStream DR, completare le seguenti attività:
   a. Configurare il cluster con il pacchetto filtro I/O.



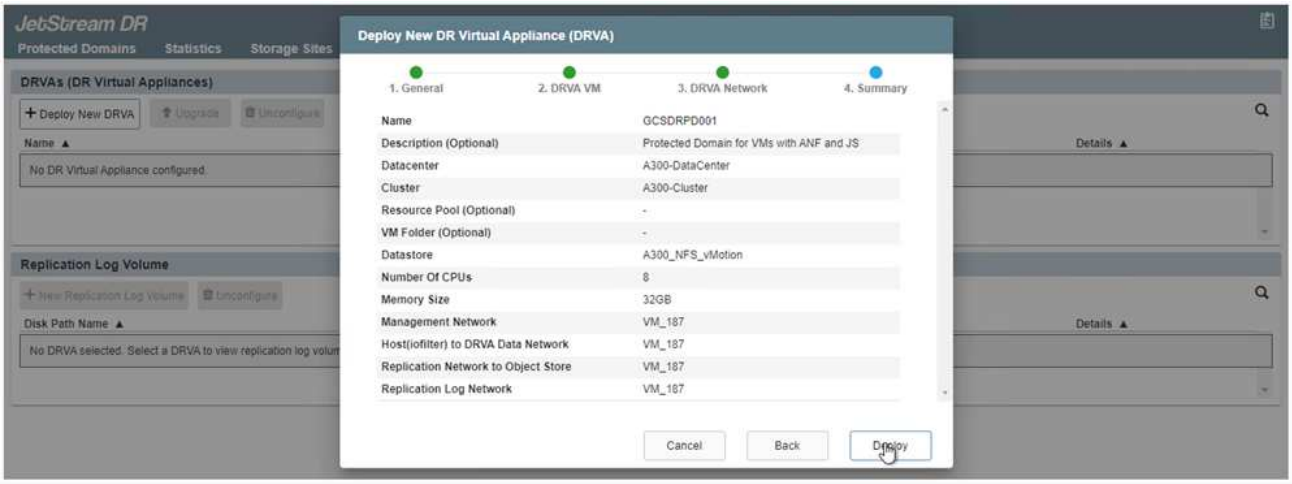
b. Aggiungere l'archiviazione BLOB di Azure situata nel sito di ripristino.



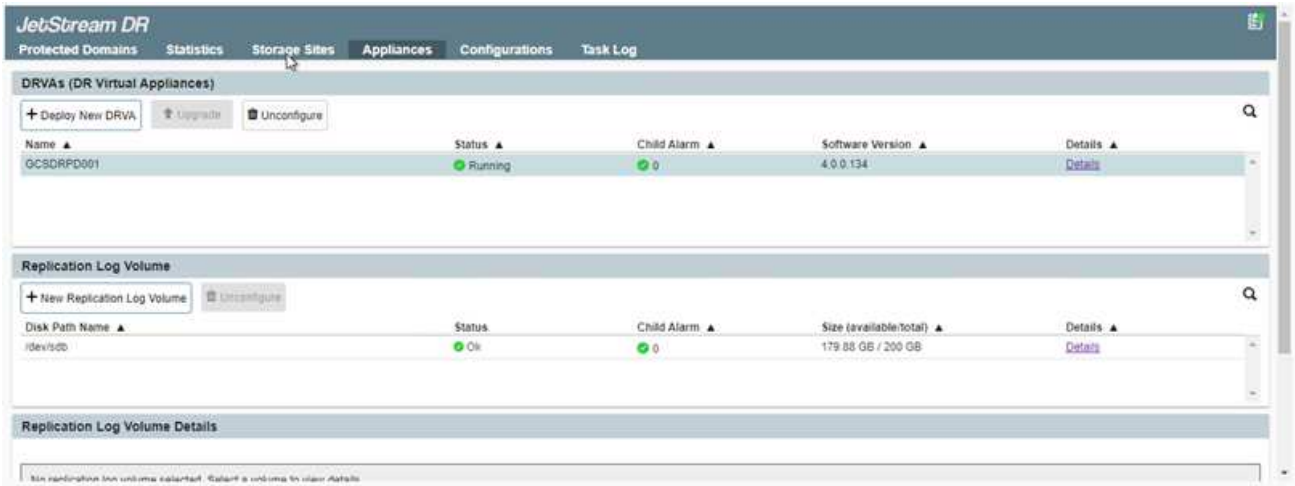
8. Distribuire il numero richiesto di DR Virtual Appliance (DRVA) dalla scheda Appliance.

Utilizzare lo strumento di pianificazione della capacità per stimare il numero di DRVA necessari.

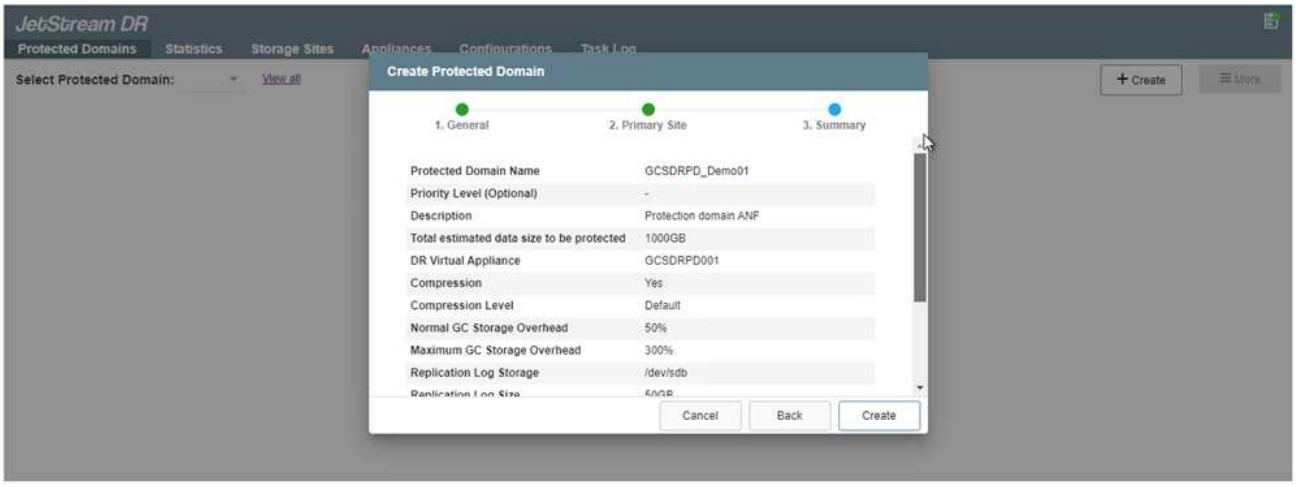


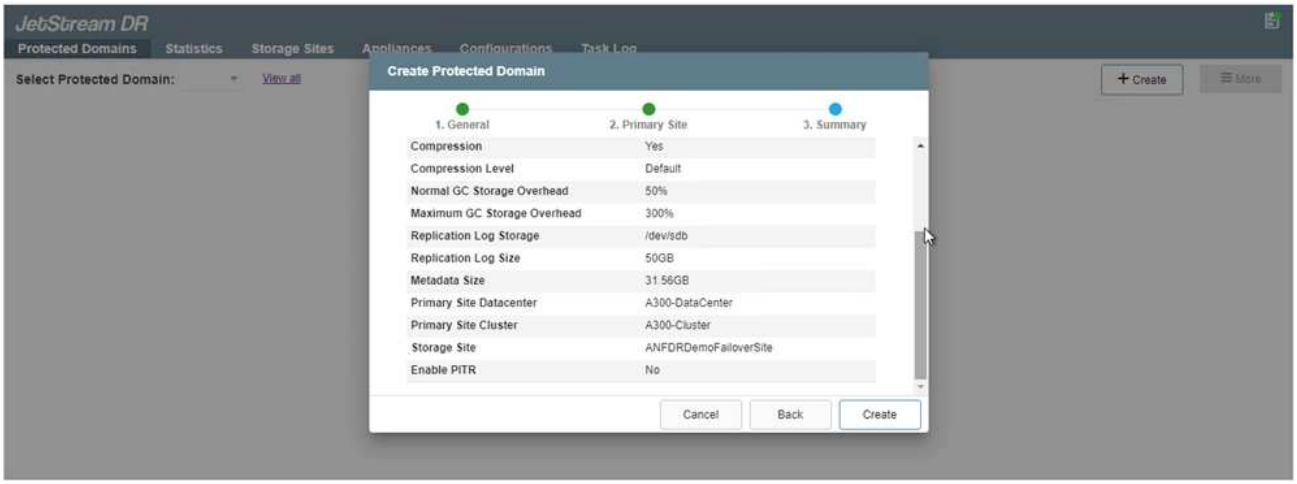


9. Creare volumi di registro di replica per ogni DRVA utilizzando il VMDK dagli archivi dati disponibili o dal pool di archiviazione iSCSI condiviso indipendente.



10. Dalla scheda Domini protetti, creare il numero richiesto di domini protetti utilizzando le informazioni sul sito di Azure Blob Storage, l'istanza DRVA e il registro di replica. Un dominio protetto definisce una VM specifica o un set di VM applicative all'interno del cluster, protette insieme e a cui viene assegnato un ordine di priorità per le operazioni di failover/failback.

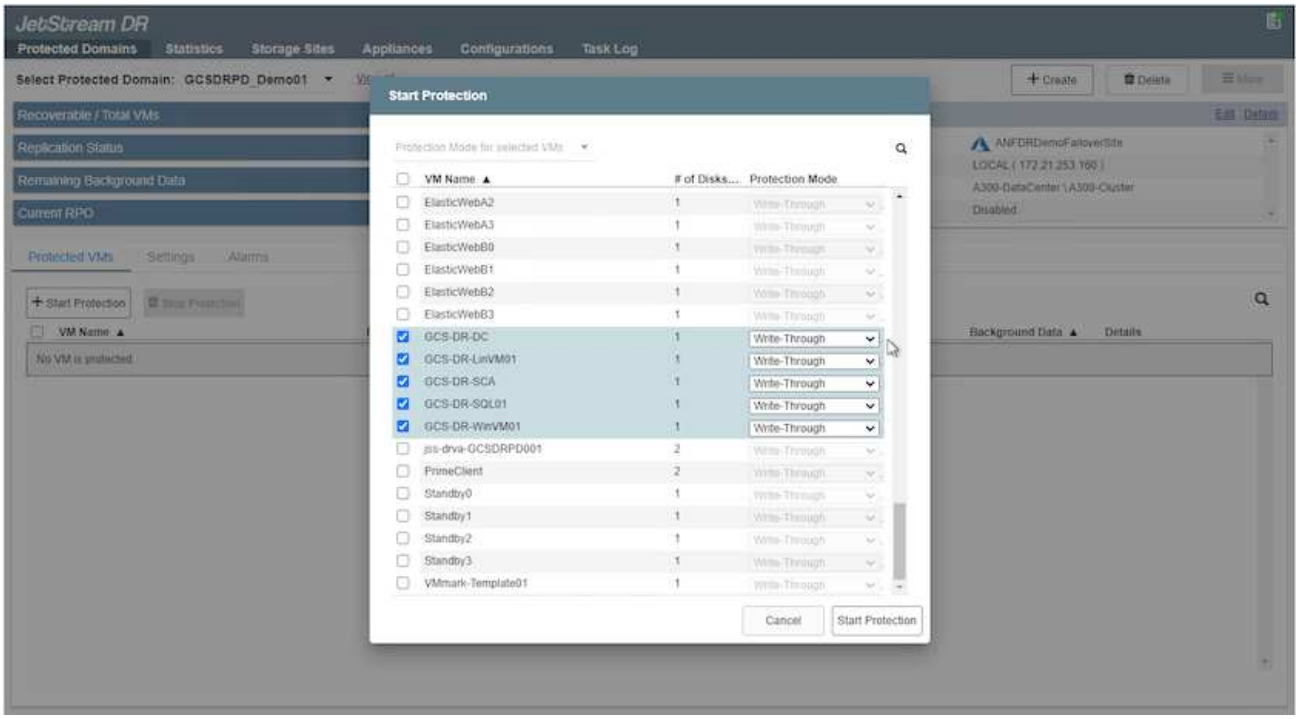




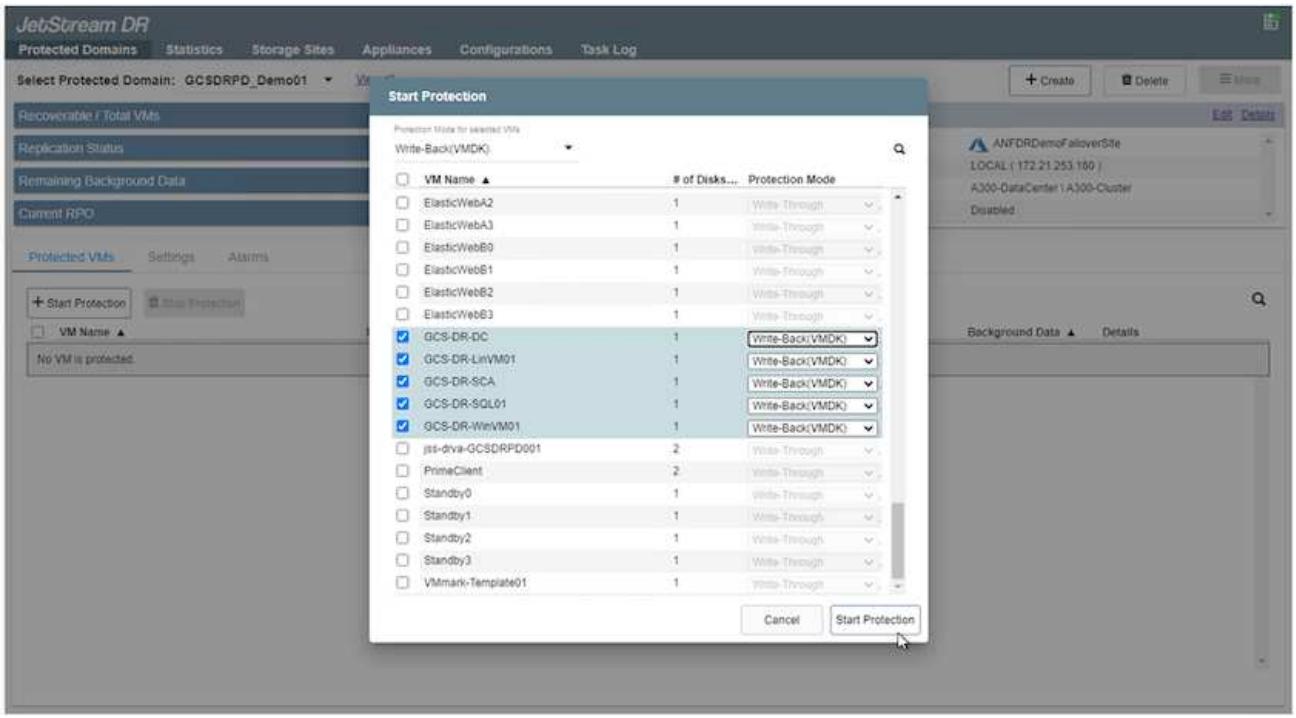
11. Selezionare le VM da proteggere e raggrupparle in gruppi di applicazioni in base alla dipendenza. Le definizioni delle applicazioni consentono di raggruppare set di VM in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

> Assicurarsi che venga utilizzata la stessa modalità di protezione per tutte le VM in un dominio protetto.

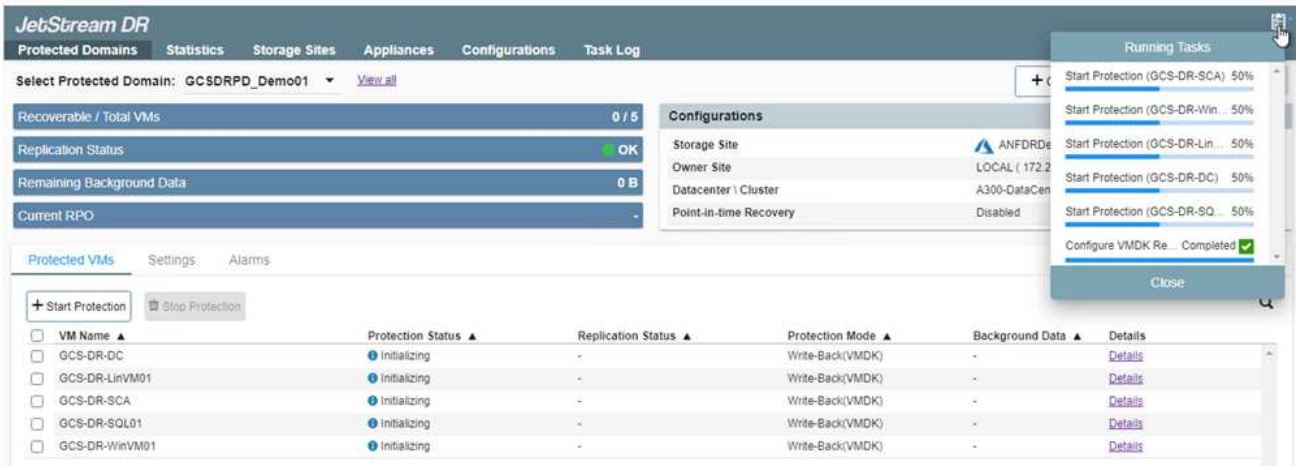
> La modalità Write-Back (VMDK) offre prestazioni più elevate.



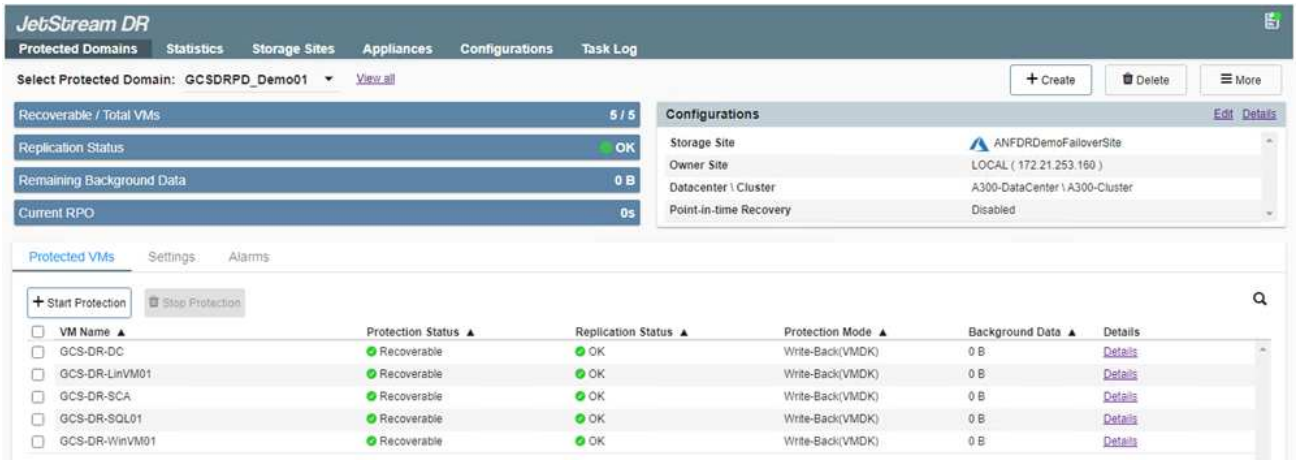
12. Assicurarsi che i volumi del registro di replica siano posizionati su un archivio ad alte prestazioni.



13. Al termine, fare clic su Avvia protezione per il dominio protetto. In questo modo viene avviata la replica dei dati per le VM selezionate nell'archivio BLOB designato.



14. Una volta completata la replica, lo stato di protezione della VM viene contrassegnato come Recuperabile.



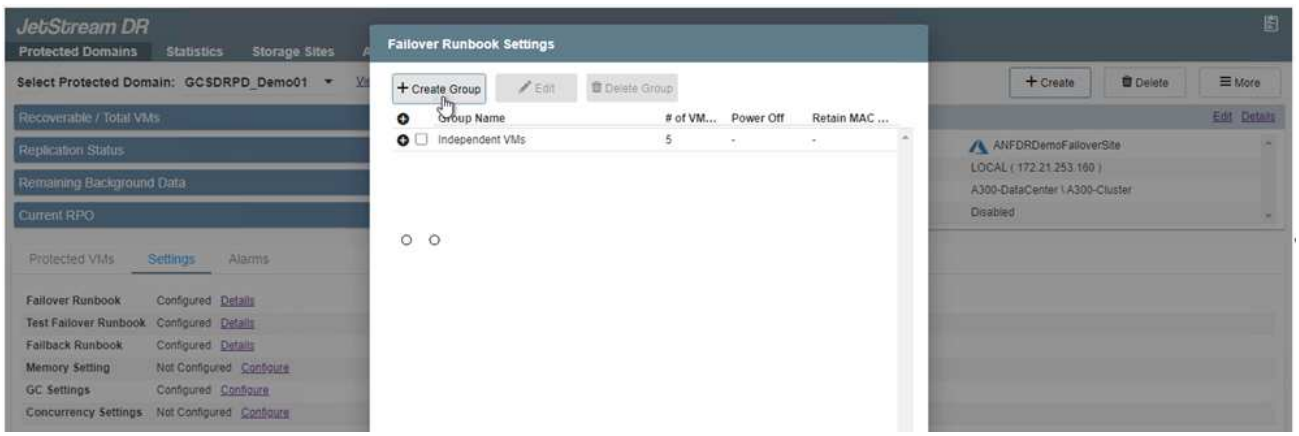
I runbook di failover possono essere configurati per raggruppare le VM (denominate gruppo di ripristino), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

15. Fare clic su Impostazioni e quindi sul collegamento Configura runbook per configurare il gruppo runbook.

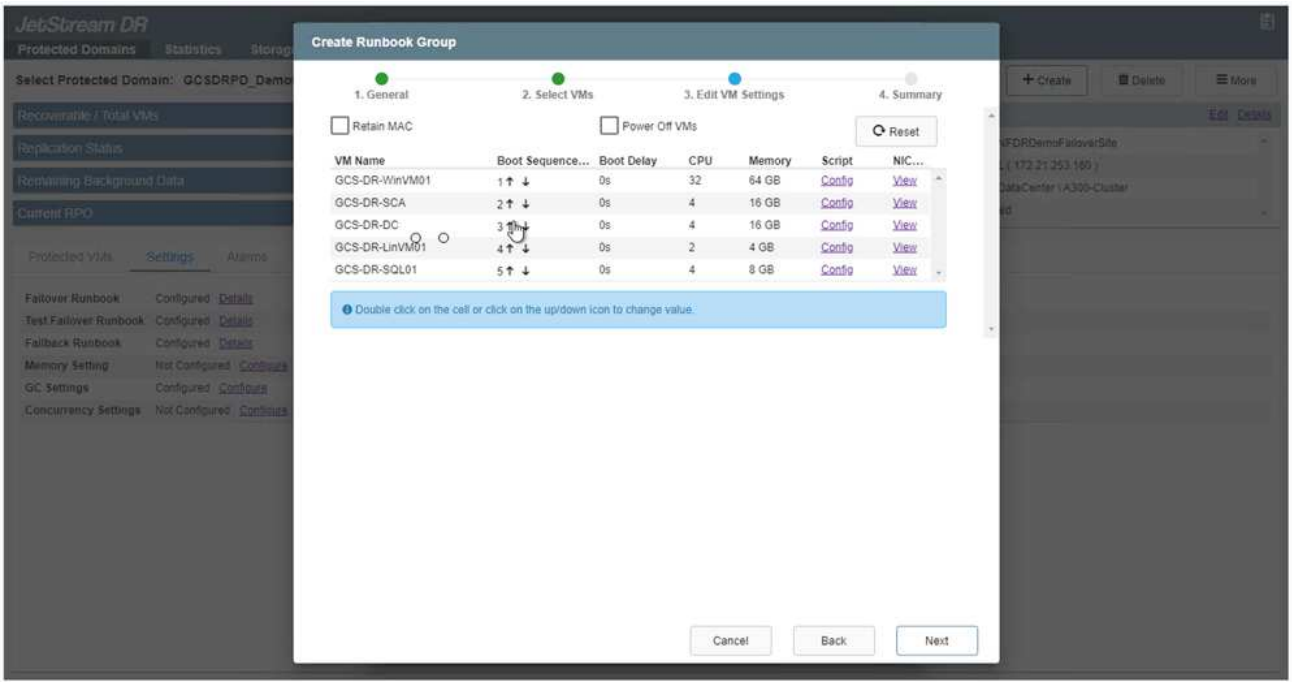


16. Fare clic sul pulsante Crea gruppo per iniziare a creare un nuovo gruppo di runbook.

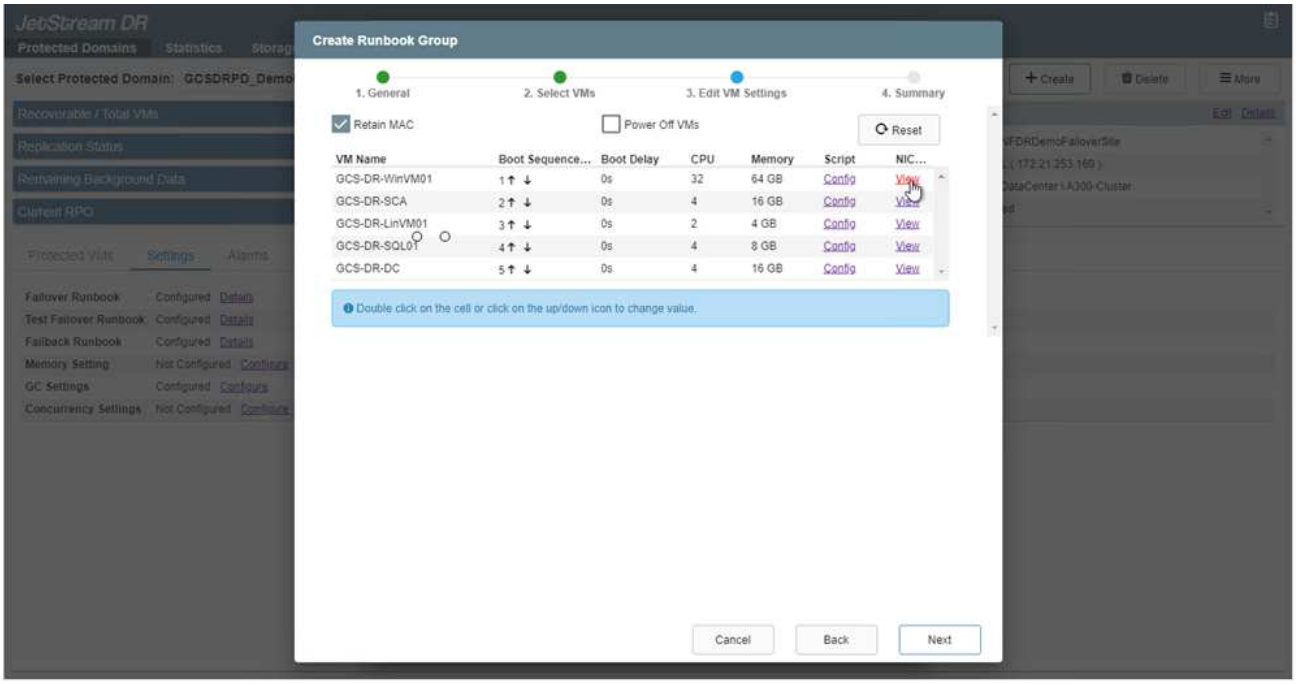
Se necessario, nella parte inferiore dello schermo, è possibile applicare pre-script e post-script personalizzati da eseguire automaticamente prima e dopo l'operazione del gruppo di runbook. Assicurarsi che gli script Runbook risiedano sul server di gestione.



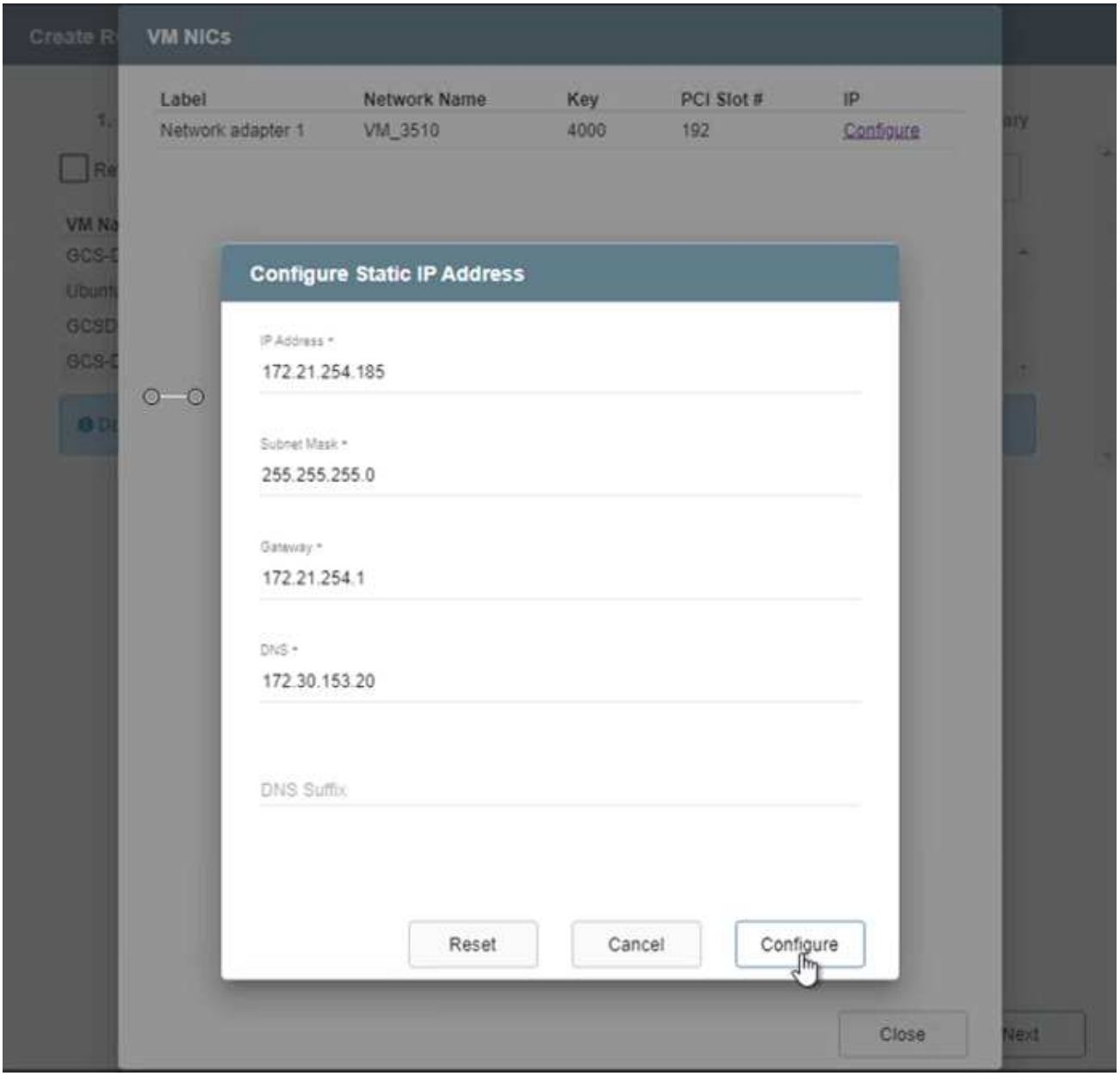
17. Modificare le impostazioni della VM secondo necessità. Specificare i parametri per il ripristino delle VM, tra cui la sequenza di avvio, il ritardo di avvio (specificato in secondi), il numero di CPU e la quantità di memoria da allocare. Modificare la sequenza di avvio delle VM facendo clic sulle frecce su o giù. Sono disponibili anche opzioni per conservare MAC.

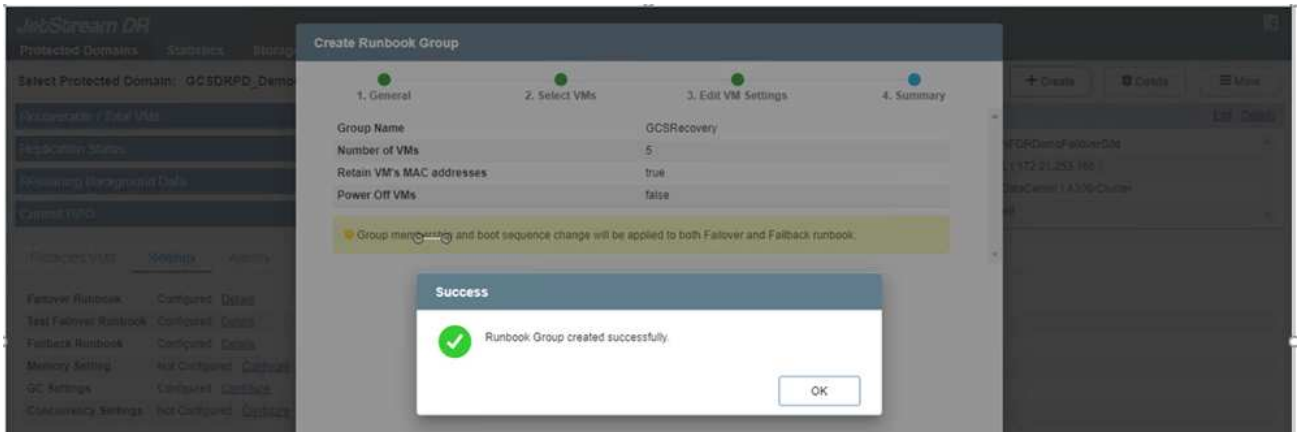


18. Gli indirizzi IP statici possono essere configurati manualmente per le singole VM del gruppo. Fare clic sul collegamento Visualizzazione NIC di una VM per configurare manualmente le impostazioni del suo indirizzo IP.



19. Fare clic sul pulsante Configura per salvare le impostazioni NIC per le rispettive VM.





Lo stato dei runbook di failover e failback è ora elencato come Configurato. I gruppi di runbook di failover e failback vengono creati in coppia utilizzando lo stesso gruppo iniziale di VM e impostazioni. Se necessario, è possibile personalizzare singolarmente le impostazioni di qualsiasi gruppo di runbook facendo clic sul rispettivo collegamento Dettagli e apportando le modifiche.

▼ Installa JetStream DR per AVS nel cloud privato

Una buona pratica per un sito di ripristino (AVS) è quella di creare in anticipo un cluster di luci 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 altro ancora

JetStream DR supporta una modalità RTO prossima allo zero per i domini mission-critical. Per questi domini, lo storage di destinazione dovrebbe essere preinstallato. In questo caso, l'ANF è il tipo di archiviazione consigliato.

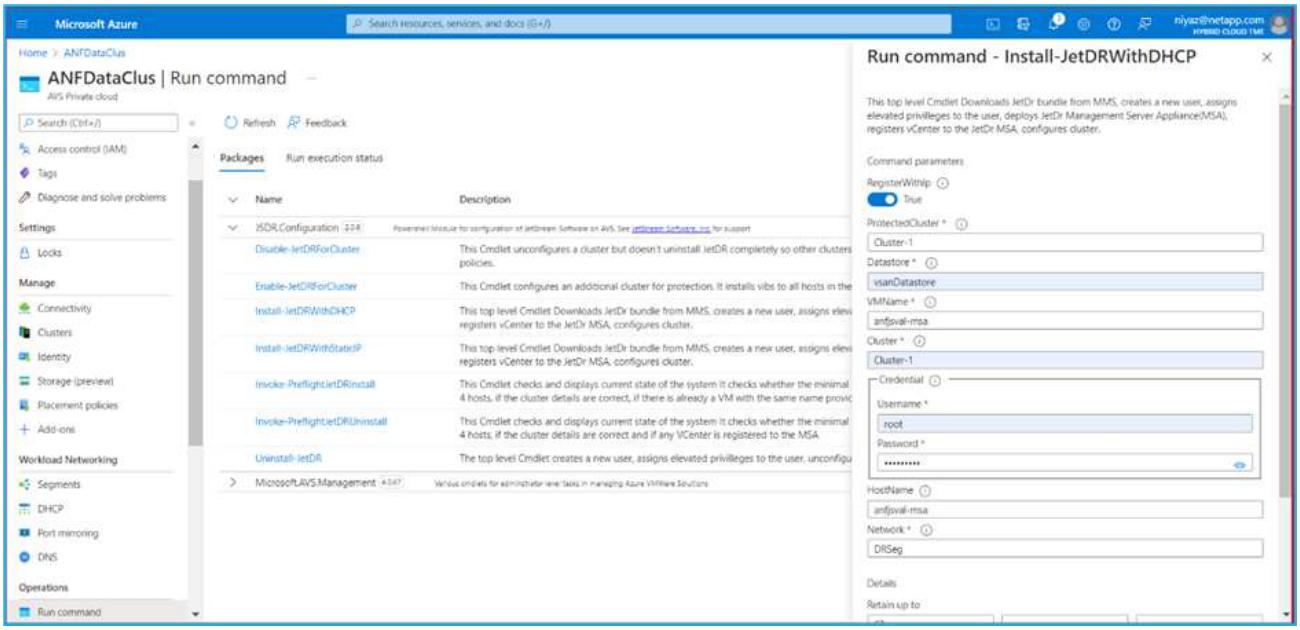
> La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS in modo da soddisfare i requisiti locali.

> A seconda dei requisiti SLA e RTO, è possibile utilizzare la modalità failover continuo o failover regolare (standard). Per un RTO prossimo allo zero, è necessario iniziare la reidratazione continua nel sito di recupero.

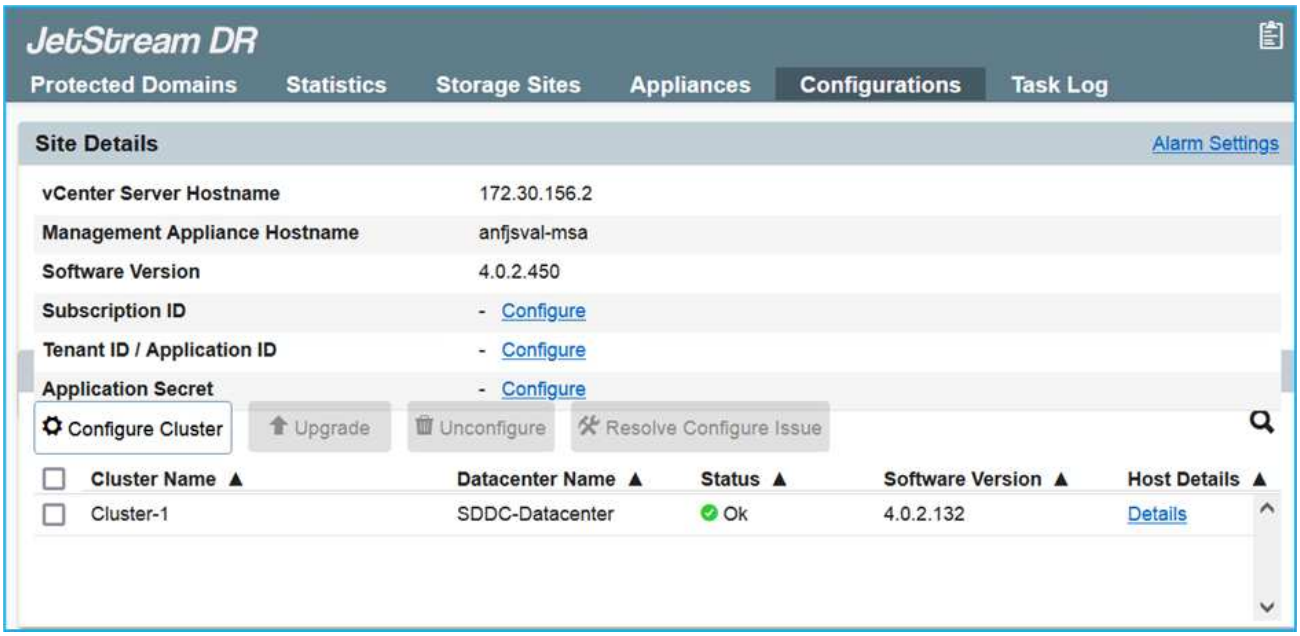
1. Per installare JetStream DR per AVS su un cloud privato di Azure VMware Solution, utilizzare il comando Esegui. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato e seleziona Esegui comando > Pacchetti > JSDR.Configuration.

> L'utente CloudAdmin predefinito della soluzione Azure VMware non dispone di privilegi sufficienti per installare JetStream DR per AVS. La soluzione Azure VMware consente l'installazione semplificata e automatizzata di JetStream DR richiamando il comando Esegui della soluzione Azure VMware per JetStream DR.

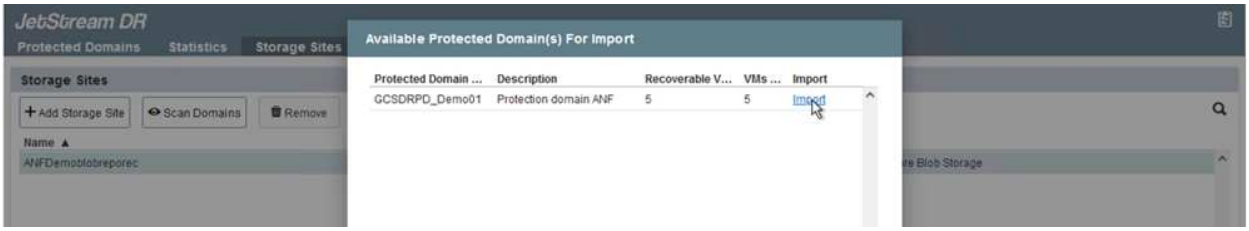
La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



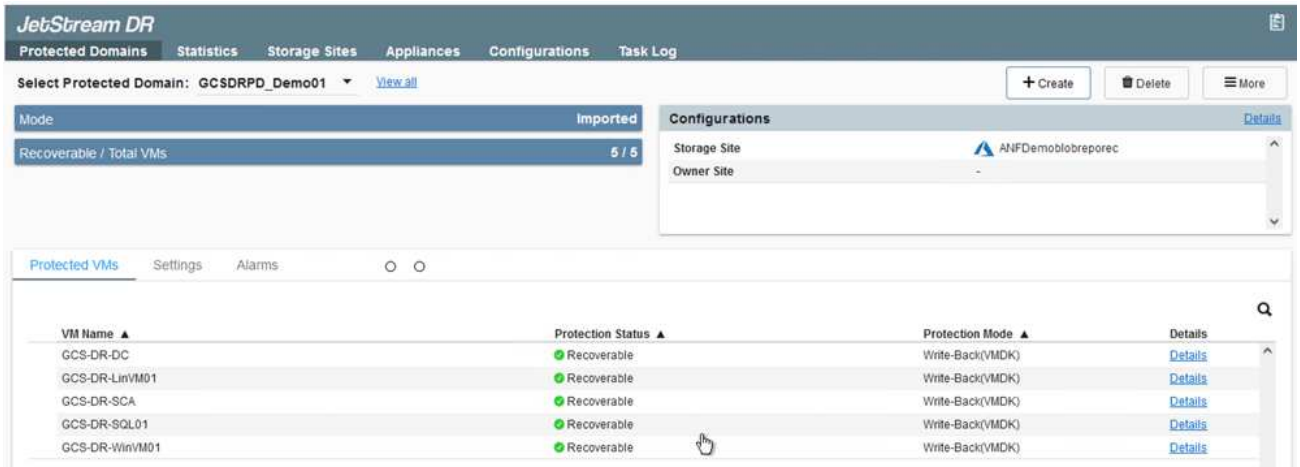
2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente di JetStream DR, andare su SDDC Datacenter > Configura > JetStream DR.



3. Dall'interfaccia JetStream DR, completare le seguenti attività:
   a. Aggiungere l'account di Azure Blob Storage utilizzato per proteggere il cluster locale come sito di archiviazione, quindi eseguire l'opzione Scansiona domini.
   b. Nella finestra di dialogo pop-up che appare, seleziona il dominio protetto da importare e poi clicca sul relativo link Importa.



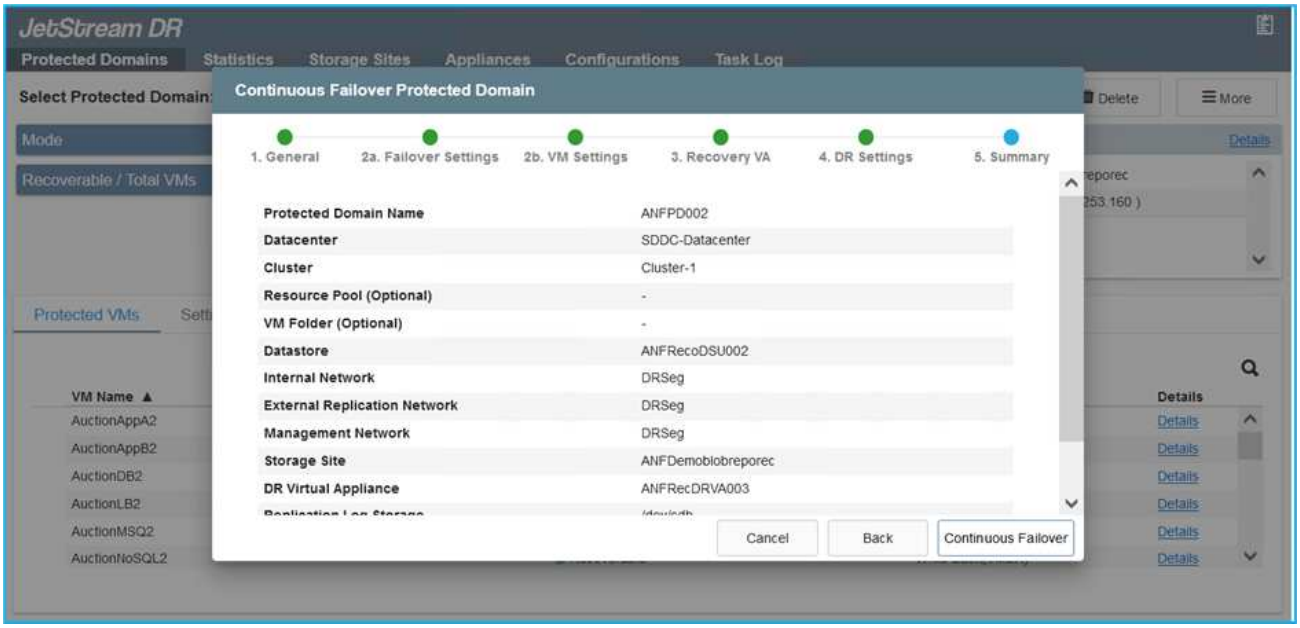
4. Il dominio viene importato per il ripristino. Vai alla scheda Domini protetti e verifica che sia stato selezionato il dominio desiderato oppure scegli quello desiderato dal menu Seleziona dominio protetto. Viene visualizzato un elenco delle VM recuperabili nel dominio protetto.



5. Dopo aver importato i domini protetti, distribuire gli appliance DRVA.

Questi passaggi possono anche essere automatizzati utilizzando i piani creati da CPT.

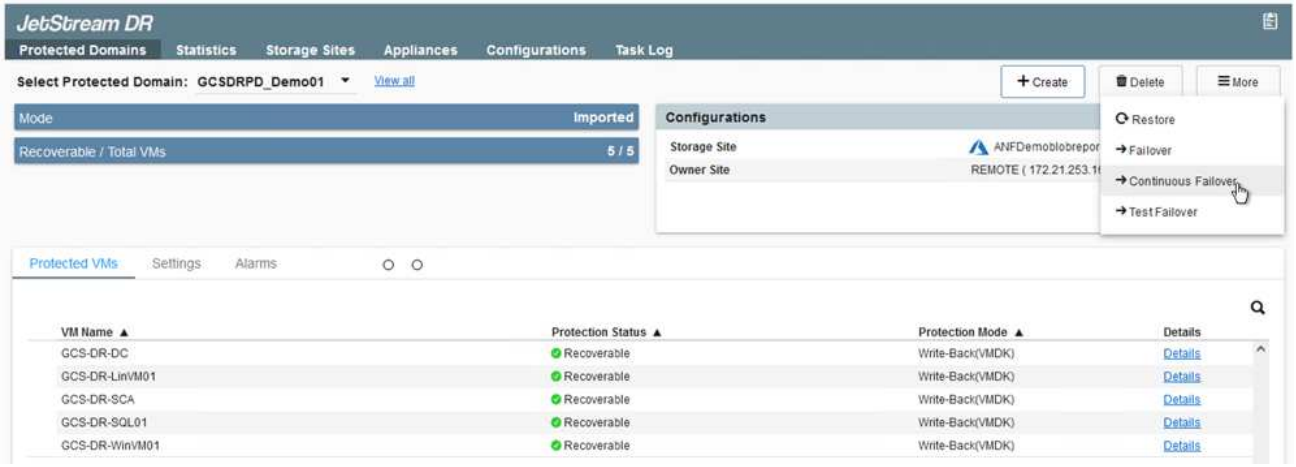
6. Creare volumi di log di replicazione utilizzando i datastore vSAN o ANF disponibili.
7. Importare i domini protetti e configurare il VA di ripristino per utilizzare un datastore ANF per i posizionamenti delle VM.



Assicurarsi che DHCP sia abilitato sul segmento selezionato e che siano disponibili sufficienti IP. Gli IP dinamici vengono utilizzati temporaneamente mentre i domini sono in fase di ripristino. Ogni VM in fase 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 continuo o failover). In questo esempio è stata selezionata la reidratazione continua (failover continuo).

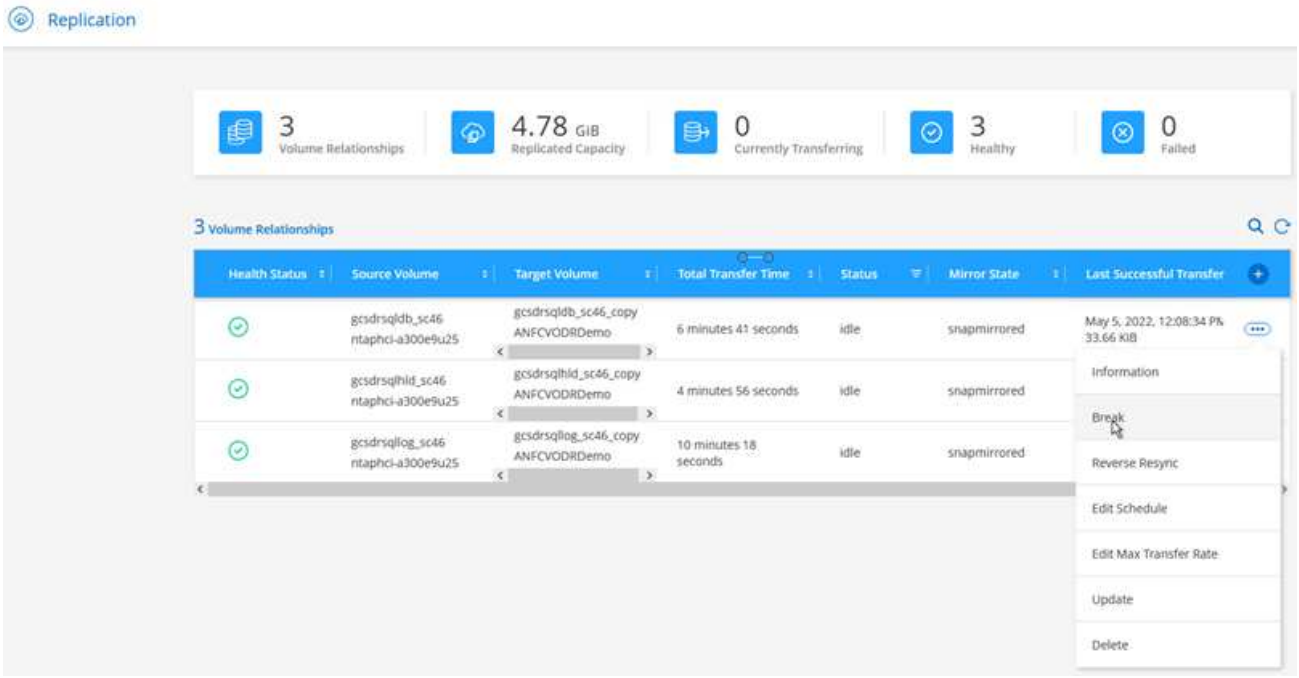
Sebbene il failover continuo e le modalità di failover differiscano nel momento in cui viene eseguita la configurazione, entrambe le modalità di failover vengono configurate utilizzando gli stessi passaggi. I passaggi di failover vengono configurati ed eseguiti insieme in risposta a un evento disastroso. Il failover continuo può essere configurato in qualsiasi momento e quindi consentito in esecuzione in background durante il normale funzionamento del sistema. Dopo che si è verificato un evento disastroso, viene completato il failover continuo per trasferire immediatamente la proprietà delle VM protette al sito di ripristino (RTO prossimo allo zero).

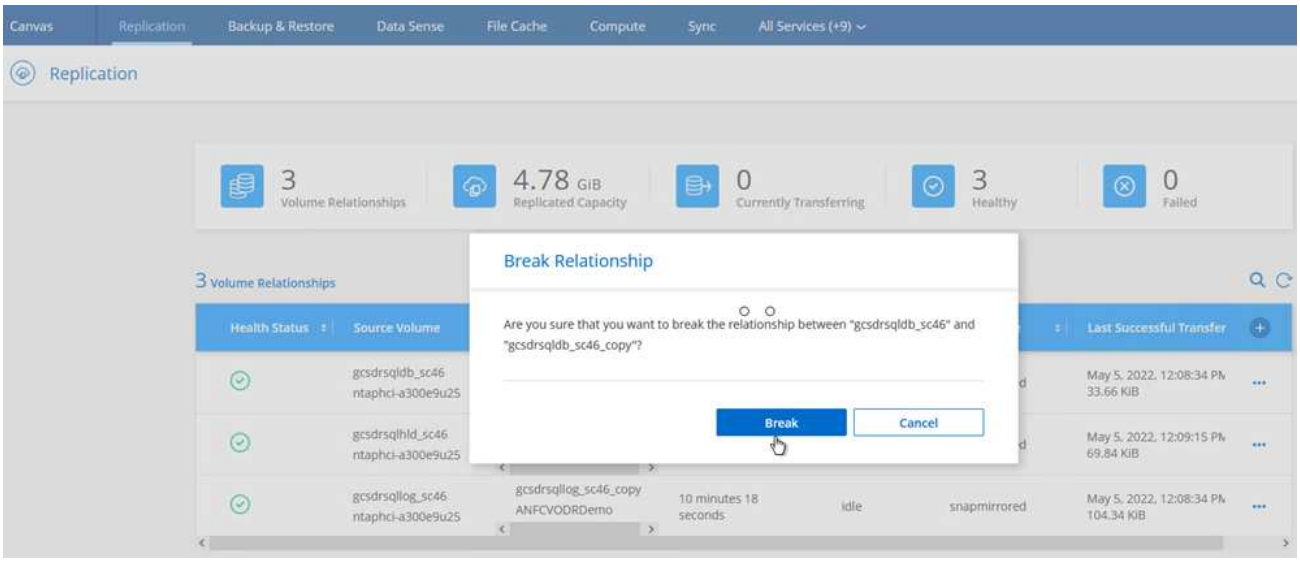


Viene avviato il processo di failover continuo, il cui avanzamento può essere monitorato dall'interfaccia utente. Facendo clic sull'icona blu nella sezione Fase corrente viene visualizzata una finestra pop-up che mostra i dettagli della fase corrente del processo di failover.

▼ **Failover e Failback**

1. Dopo che si è verificato un disastro nel cluster protetto dell'ambiente on-premise (guasto parziale o completo), è possibile attivare il failover per le VM che utilizzano Jetstream dopo aver interrotto la relazione SnapMirror per i rispettivi volumi applicativi.

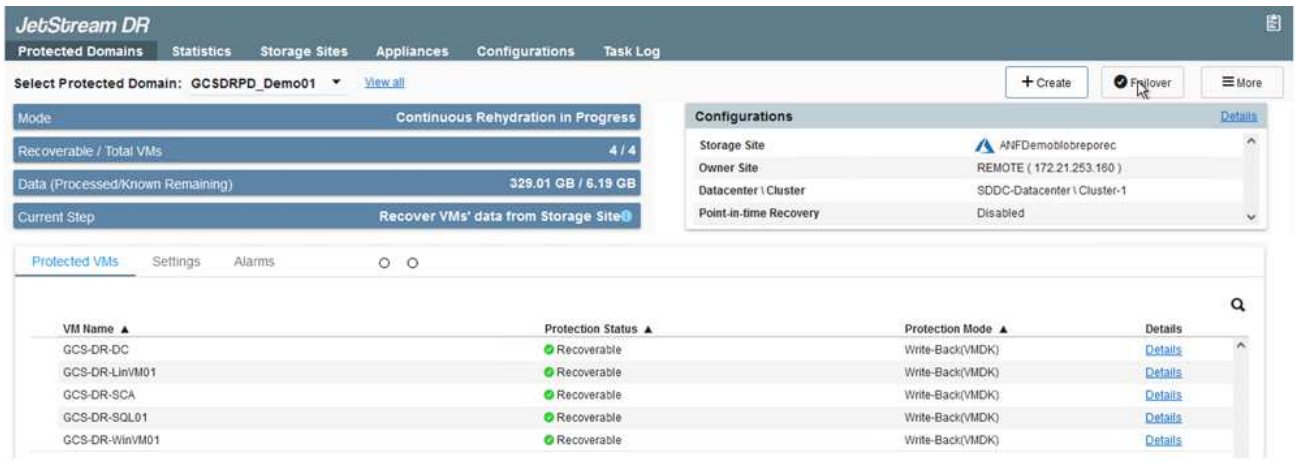


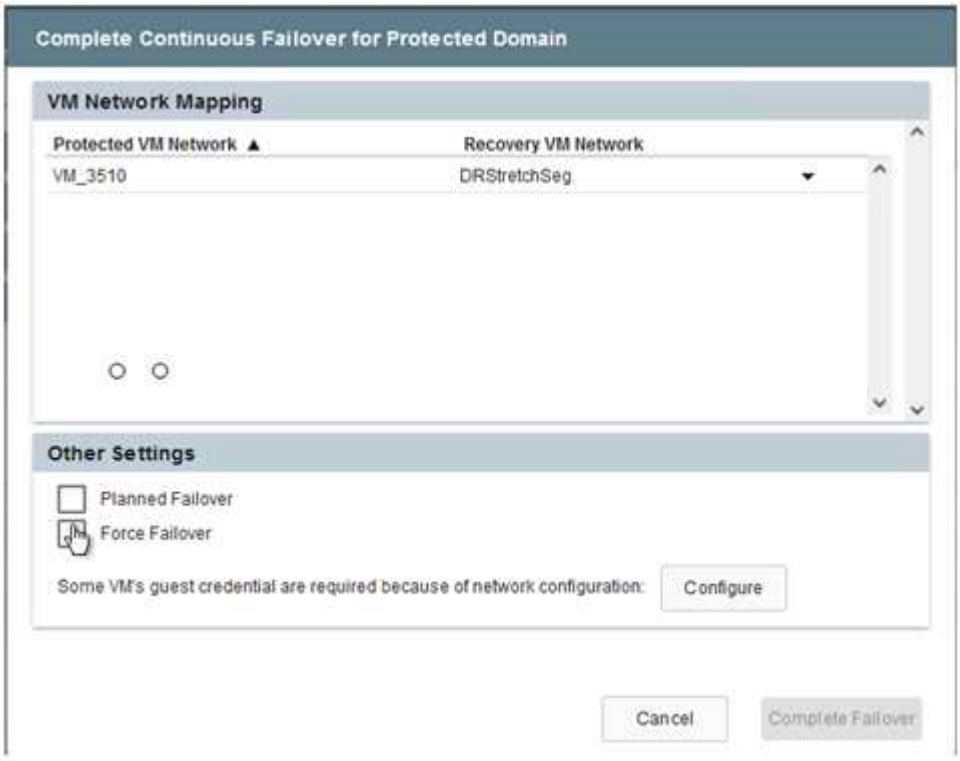


Questo passaggio può essere facilmente automatizzato per facilitare il processo di recupero.

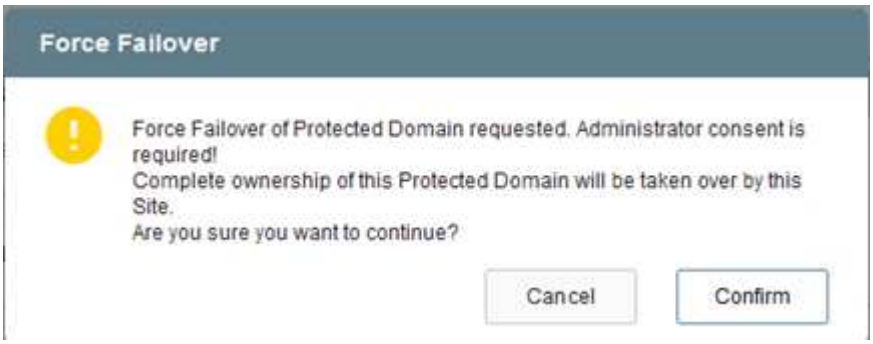
2. Accedere all'interfaccia utente di Jetstream su AVS SDDC (lato destinazione) e attivare l'opzione di failover per completare il failover. La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

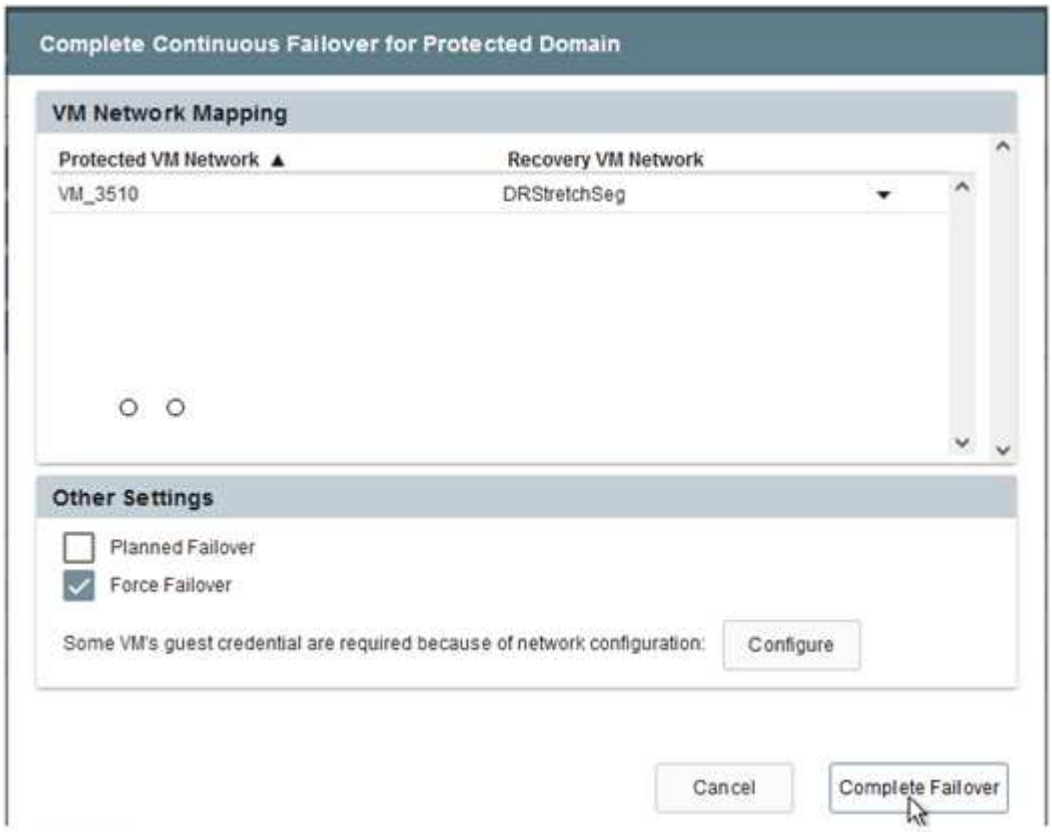
   Nella finestra di dialogo che appare al termine del failover, è possibile specificare l'attività di failover come pianificata o come forzata.





Il failover forzato presuppone che il sito primario non sia più accessibile e che la proprietà del dominio protetto debba essere assunta direttamente dal sito di ripristino.





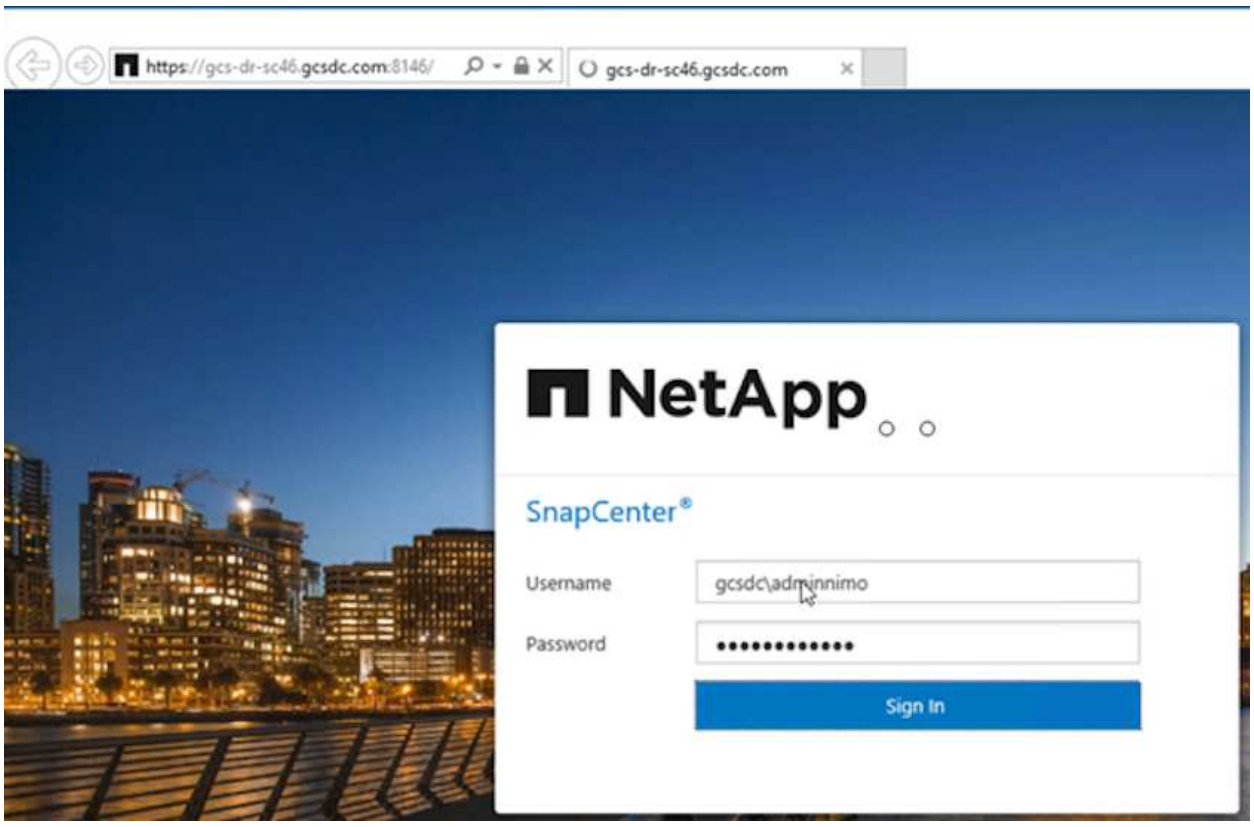
3. Una volta completato il failover continuo, viene visualizzato un messaggio che conferma il completamento dell'attività. Una volta completata l'attività, accedere alle VM ripristinate per configurare le sessioni ISCSI o NFS.

La modalità di failover cambia in In esecuzione in failover e lo stato della VM è Recuperabile. Tutte le VM del dominio protetto sono ora in esecuzione nel sito di ripristino nello stato specificato dalle impostazioni del runbook di failover.

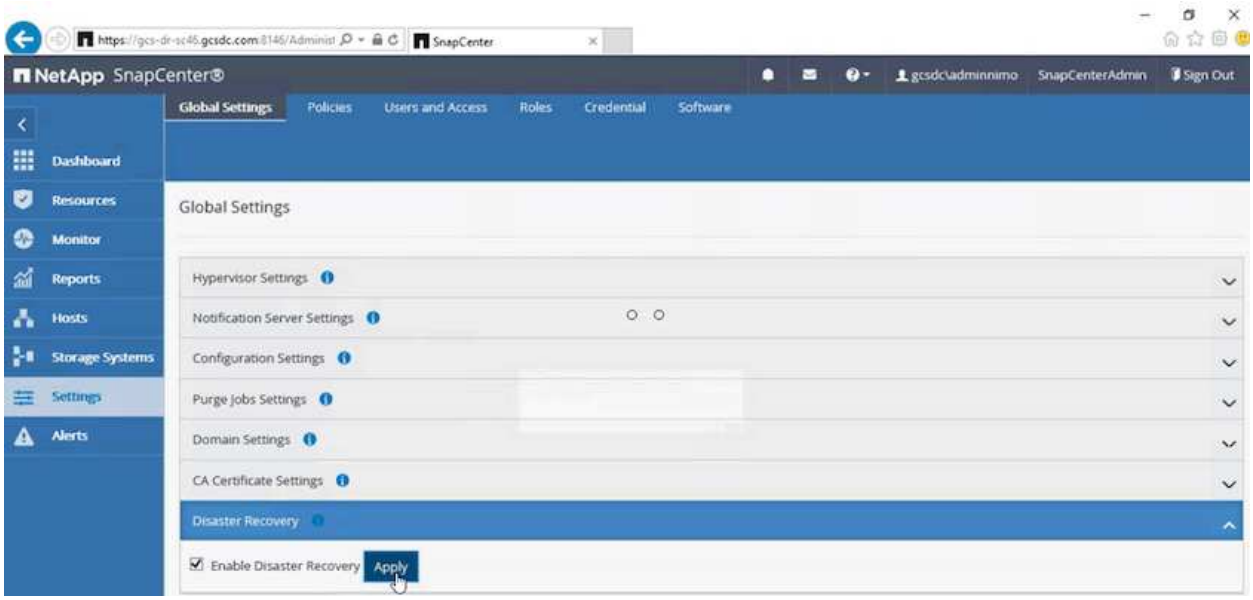
Per verificare la configurazione e l'infrastruttura del failover, JetStream DR può essere utilizzato in modalità di test (opzione Test Failover) per osservare il ripristino delle macchine virtuali e dei relativi dati dall'archivio oggetti in un ambiente di ripristino di test. Quando una procedura di failover viene eseguita in modalità test, il suo funzionamento è simile a un vero e proprio processo di failover.



4. Dopo aver ripristinato le macchine virtuali, utilizzare il ripristino di emergenza dell'archiviazione per l'archiviazione in-guest. Per dimostrare questo processo, in questo esempio viene utilizzato SQL Server.
5. Accedere alla VM SnapCenter recuperata su AVS SDDC e abilitare la modalità DR.
   a. Accedi all'interfaccia utente SnapCenter tramite il browserN.



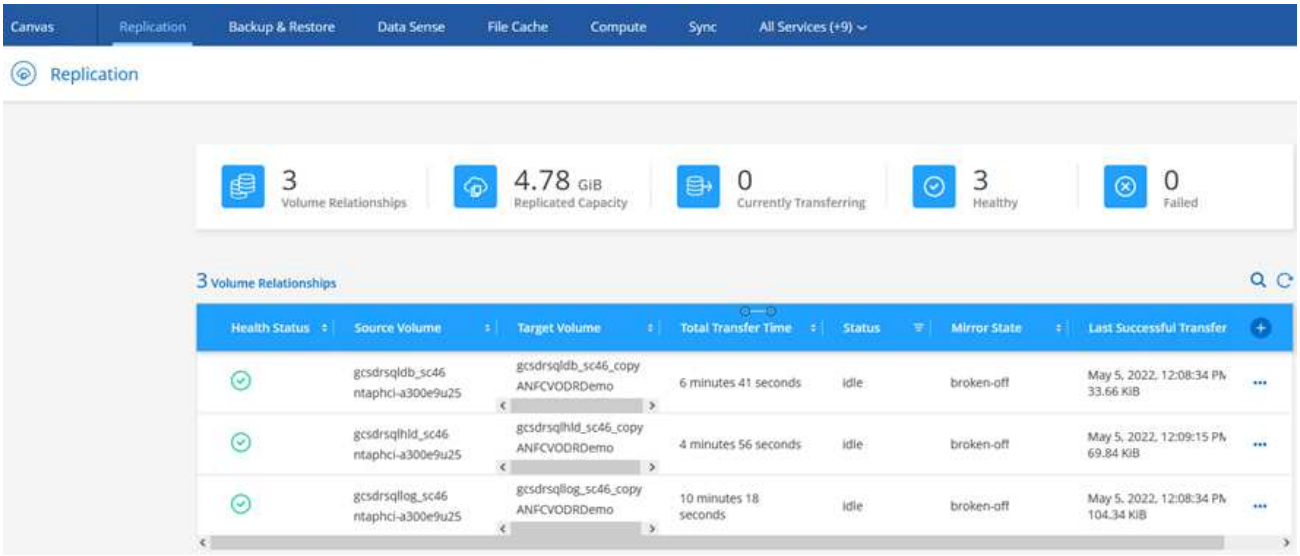
   b. Nella pagina Impostazioni, vai su Impostazioni > Impostazioni globali > Ripristino di emergenza.
   c. Selezionare Abilita ripristino di emergenza.
   d. Fare clic su Applica.



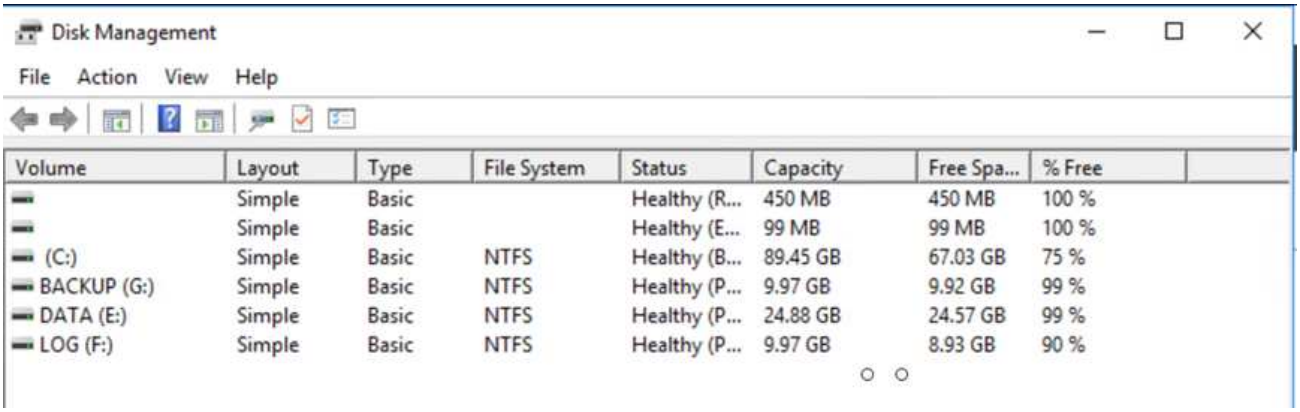
e. Verificare se il processo DR è abilitato facendo clic su Monitor > Processi.

> Per il ripristino di emergenza dello storage è consigliabile utilizzare NetApp SnapCenter 4.6 o versione successiva. Per le versioni precedenti, è necessario utilizzare snapshot coerenti con l'applicazione (replicati tramite SnapMirror) ed eseguire il ripristino manuale nel caso in cui i backup precedenti debbano essere ripristinati nel sito di ripristino di emergenza.

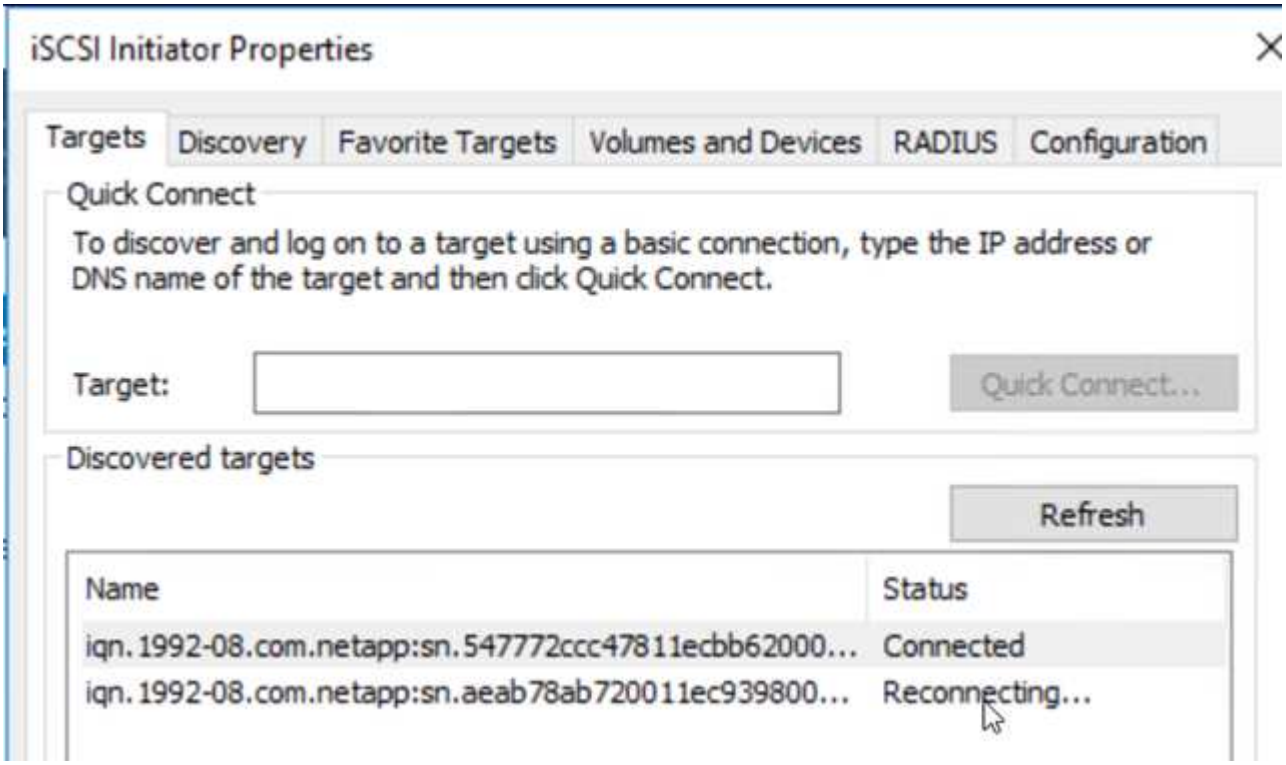
6. Assicurarsi che la relazione SnapMirror sia interrotta.



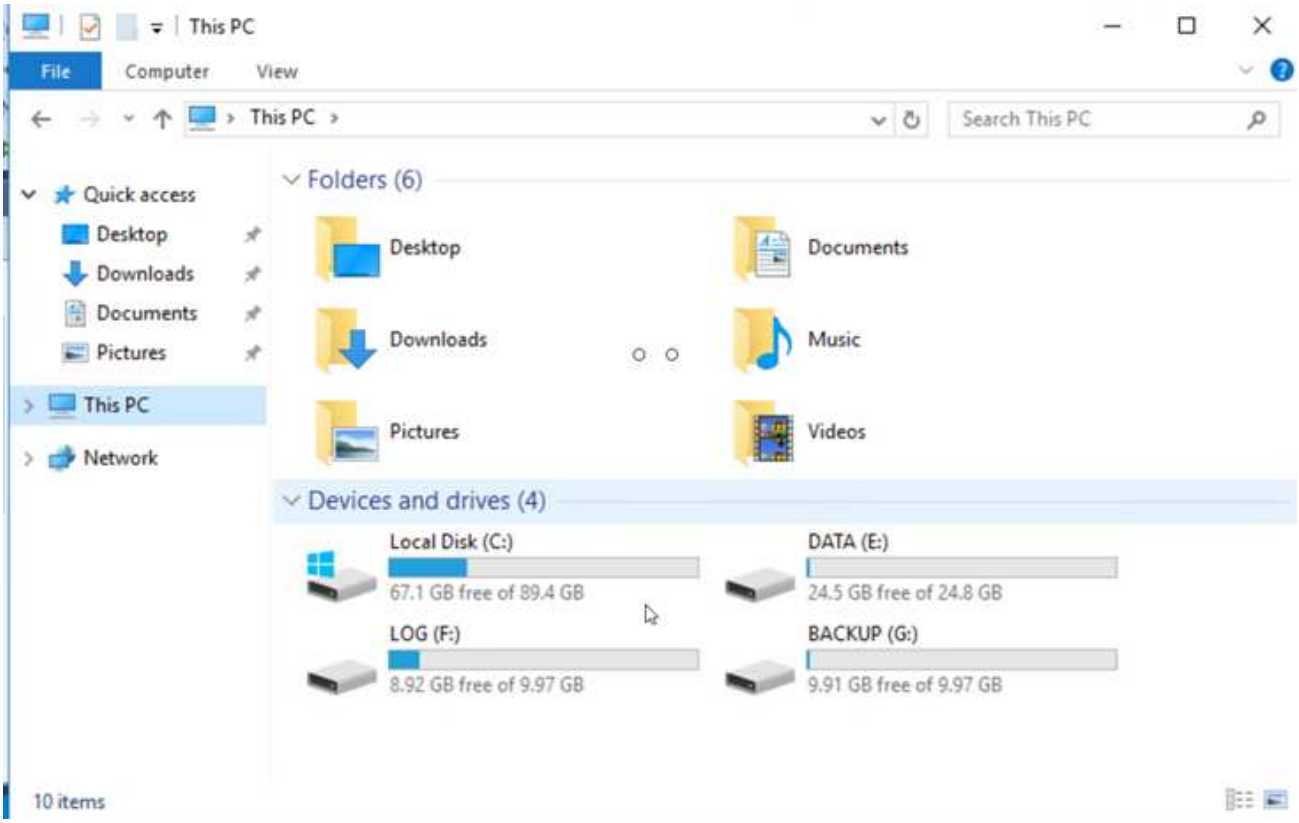
7. Collegare la LUN da Cloud Volumes ONTAP alla VM guest SQL ripristinata con le stesse lettere di unità.



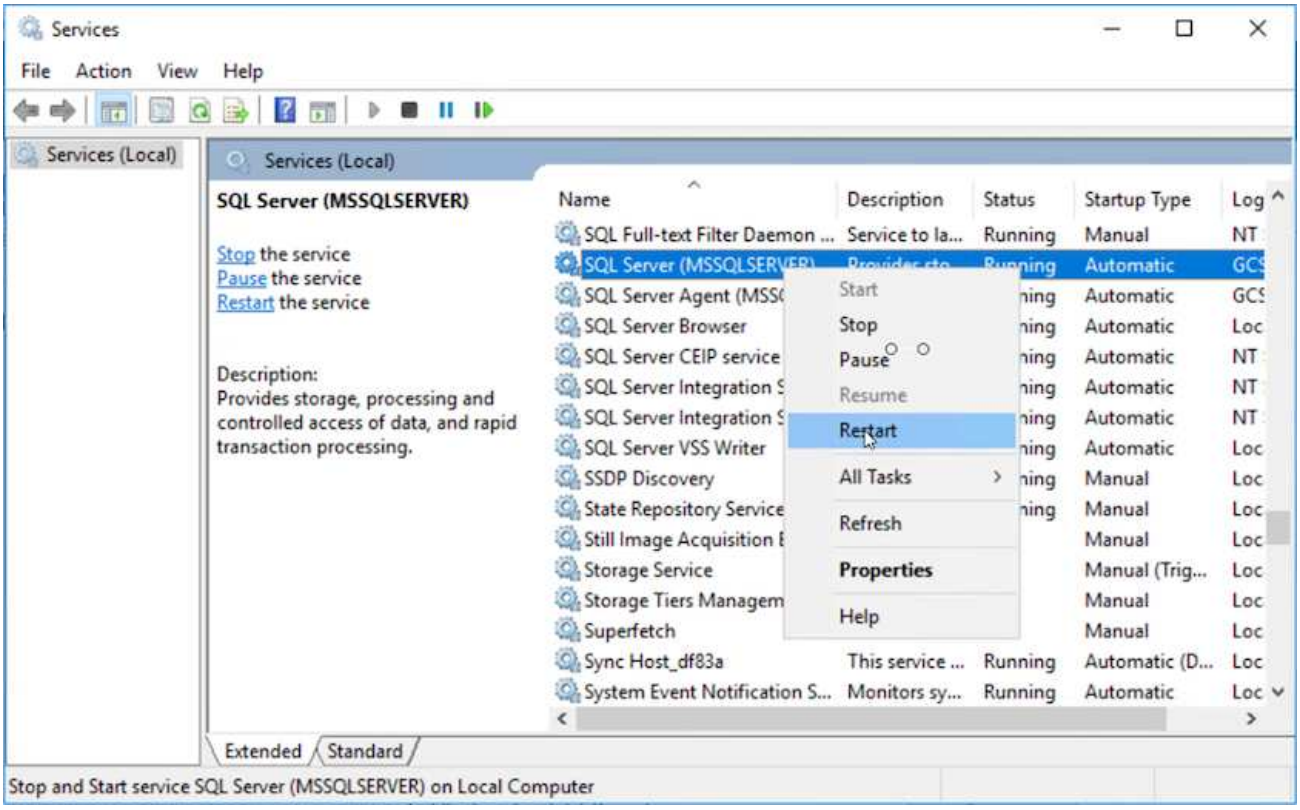
8. Aprire iSCSI Initiator, cancellare la sessione disconnessa precedente e aggiungere la nuova destinazione insieme al multipath per i volumi Cloud Volumes ONTAP replicati.



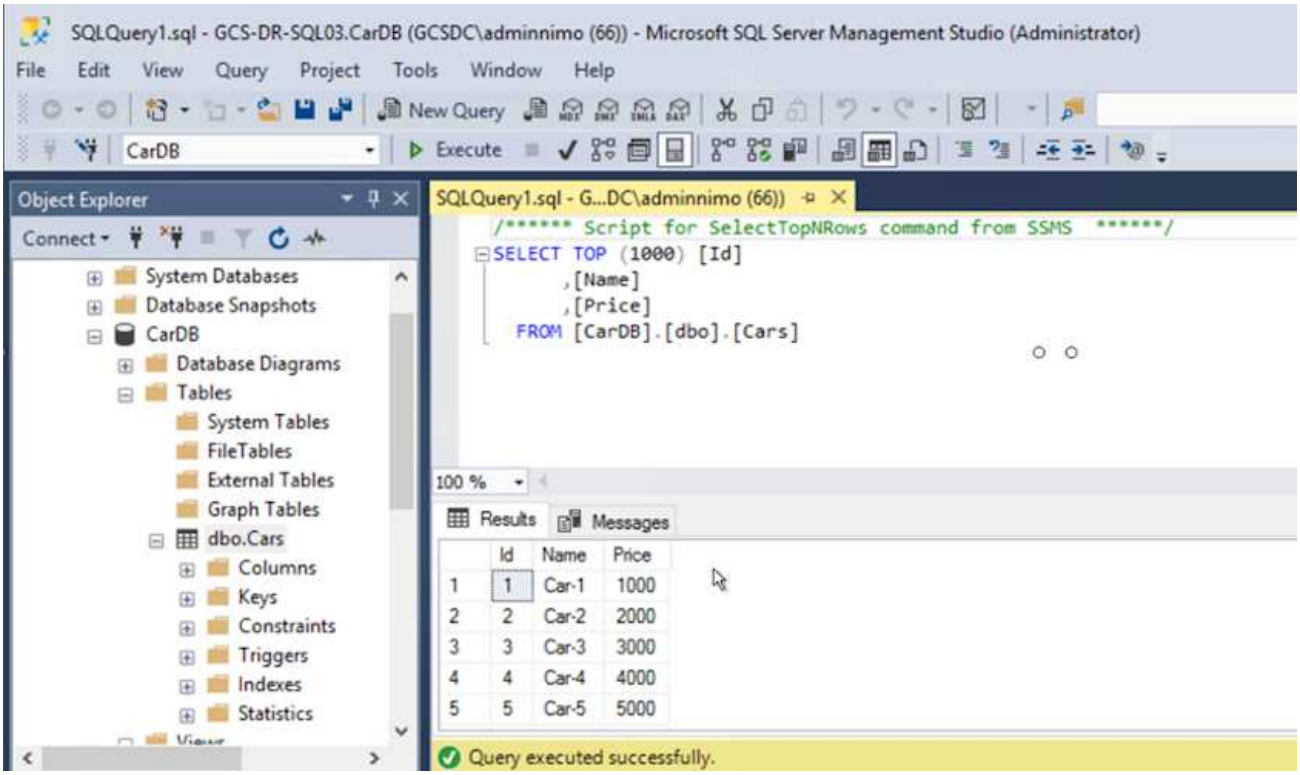
9. Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.



10. Riavviare il servizio del server MSSQL.



11. Assicurarsi che le risorse SQL siano di nuovo online.



Nel caso di NFS, collegare i volumi utilizzando il comando mount e aggiornare il `/etc/fstab` voci.

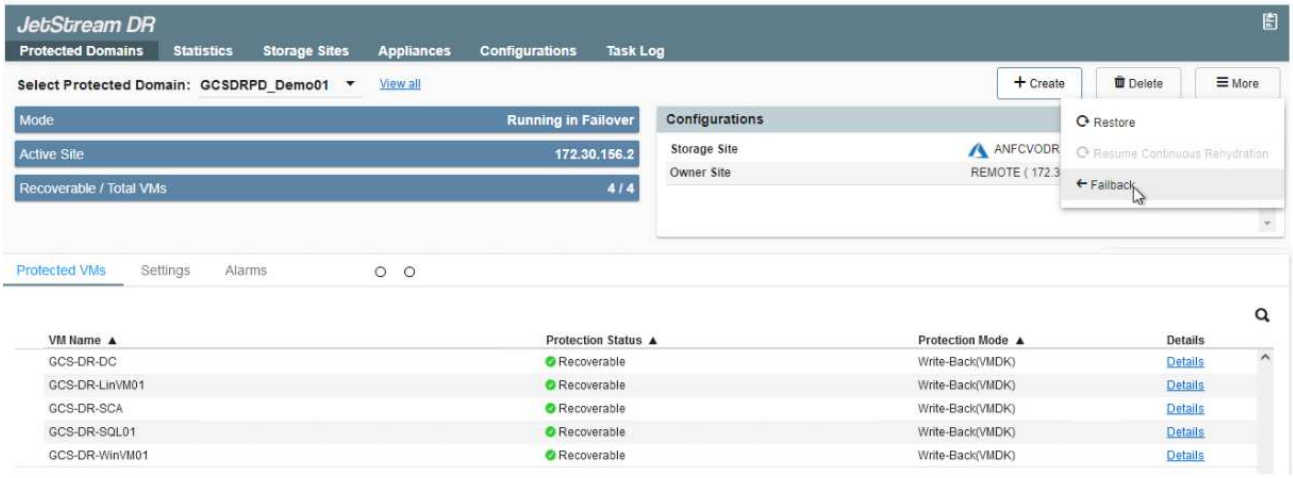
A questo punto, le operazioni possono riprendere e gli affari continuano normalmente.

Sul lato NSX-T, è possibile creare un gateway di livello 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 entrare o uscire dall'ambiente, in modo che qualsiasi attività di triage, contenimento o rafforzamento possa essere eseguita senza il rischio di contaminazione incrociata. Questa operazione esula dallo scopo del presente documento, ma può essere facilmente eseguita per simulare l'isolamento.

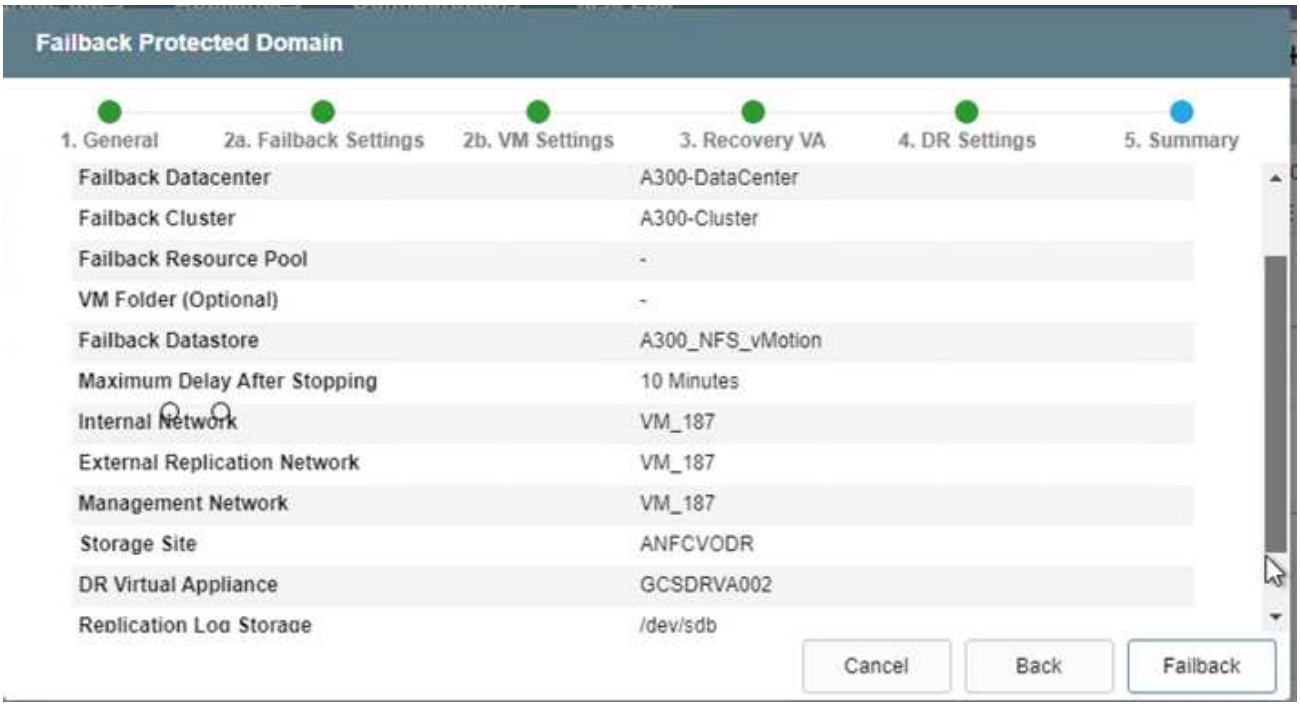
Una volta che il sito primario è di nuovo attivo e funzionante, è possibile eseguire il failback. La protezione della VM viene ripristinata da Jetstream e la relazione SnapMirror deve essere invertita.

1. Ripristinare l'ambiente locale. A seconda del tipo di incidente di emergenza, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software JetStream DR.
2. Accedere all'ambiente locale ripristinato, andare all'interfaccia utente di Jetstream DR e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione Failback nell'interfaccia utente.

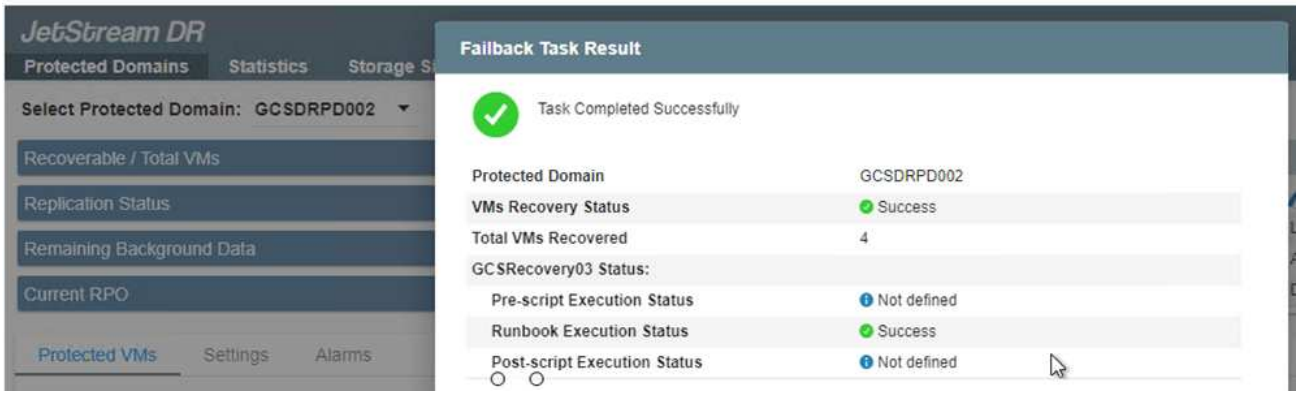
Il piano di failback generato da CPT può essere utilizzato anche per avviare il ritorno delle VM e dei relativi dati dall'archivio oggetti all'ambiente VMware originale.



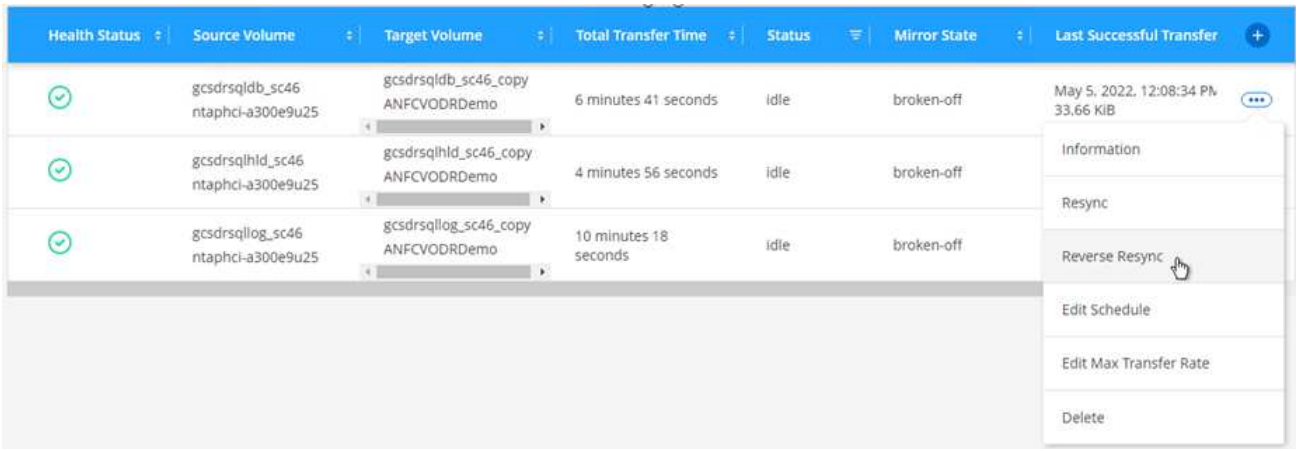
Specificare il ritardo massimo dopo la sospensione delle VM nel sito di ripristino e il loro riavvio nel sito protetto. Il tempo necessario per completare questo processo include il completamento della replica dopo l'arresto delle VM di failover, il tempo necessario per pulire il sito di ripristino e il tempo necessario per ricreare le VM nel sito protetto. NetApp consiglia 10 minuti.

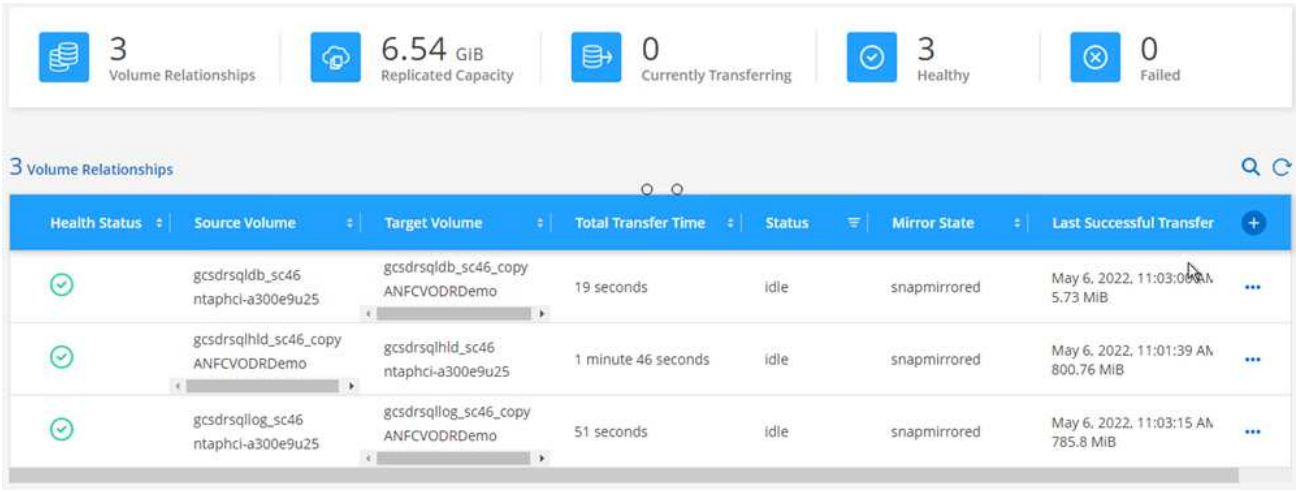


3. Completare il processo di failback e quindi confermare la ripresa della protezione della VM e la coerenza dei dati.

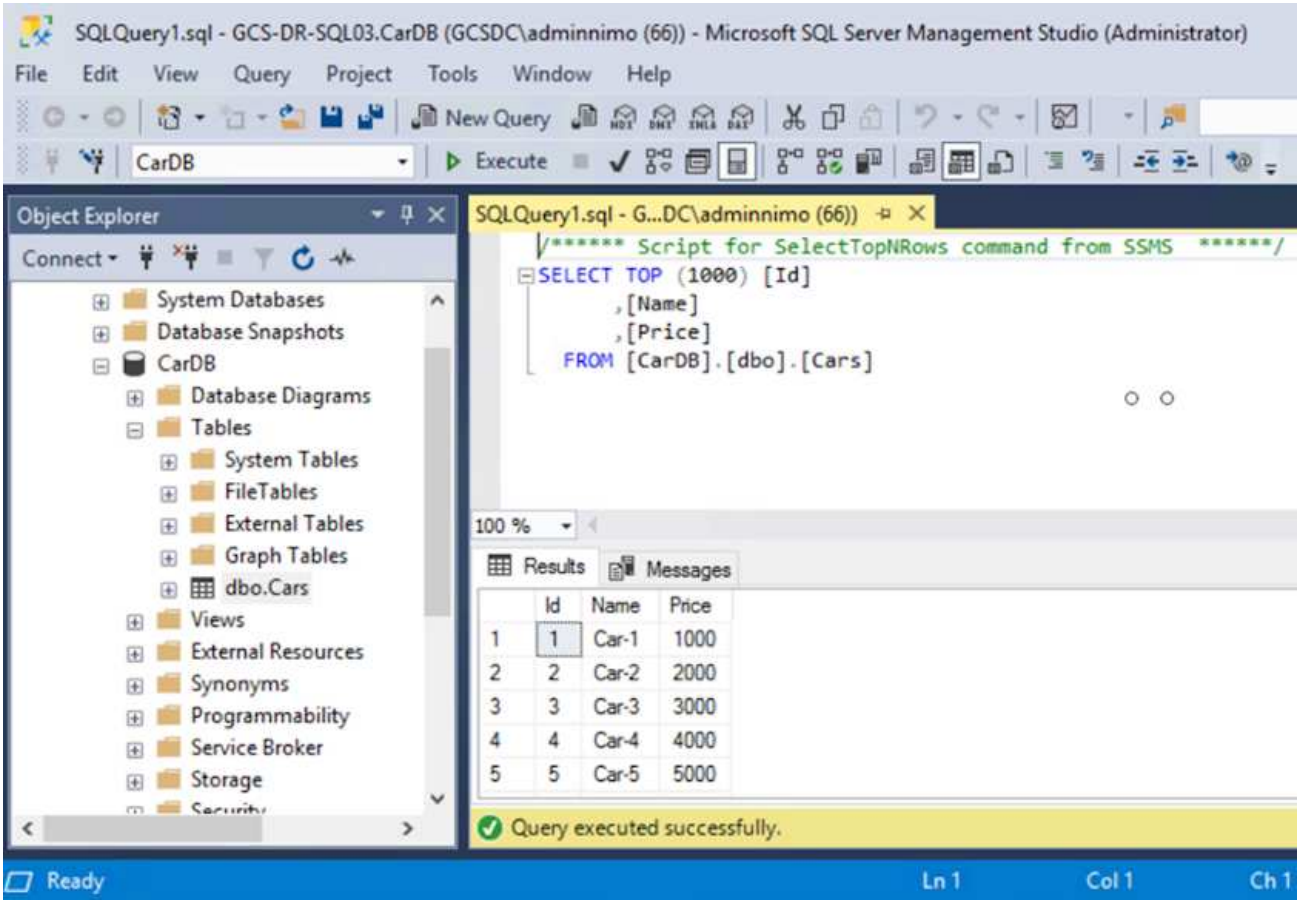


4. Dopo aver ripristinato le VM, scollegare lo storage secondario dall'host e connettersi allo storage primario.





5. Riavviare il servizio del server MSSQL.
6. Verificare che le risorse SQL siano di nuovo online.



Per eseguire il failback sullo 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 di 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, database simili e qualsiasi altra applicazione che utilizzi l'archiviazione connessa agli ospiti.

Come sempre, testare i passaggi necessari per il ripristino dei carichi di lavoro critici prima di trasferirli in produzione.

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Ripristina qualsiasi punto disponibile nel tempo con la conservazione degli snapshot ONTAP .
- È disponibile l'automazione completa per tutti i passaggi necessari al ripristino di centinaia o migliaia di VM, a partire dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- SnapCenter utilizza meccanismi di clonazione che non modificano il volume replicato.
  - In questo modo si evita il rischio di danneggiamento dei dati per volumi e snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.

- Sfrutta i dati DR per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.

- L'ottimizzazione di CPU e RAM può contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

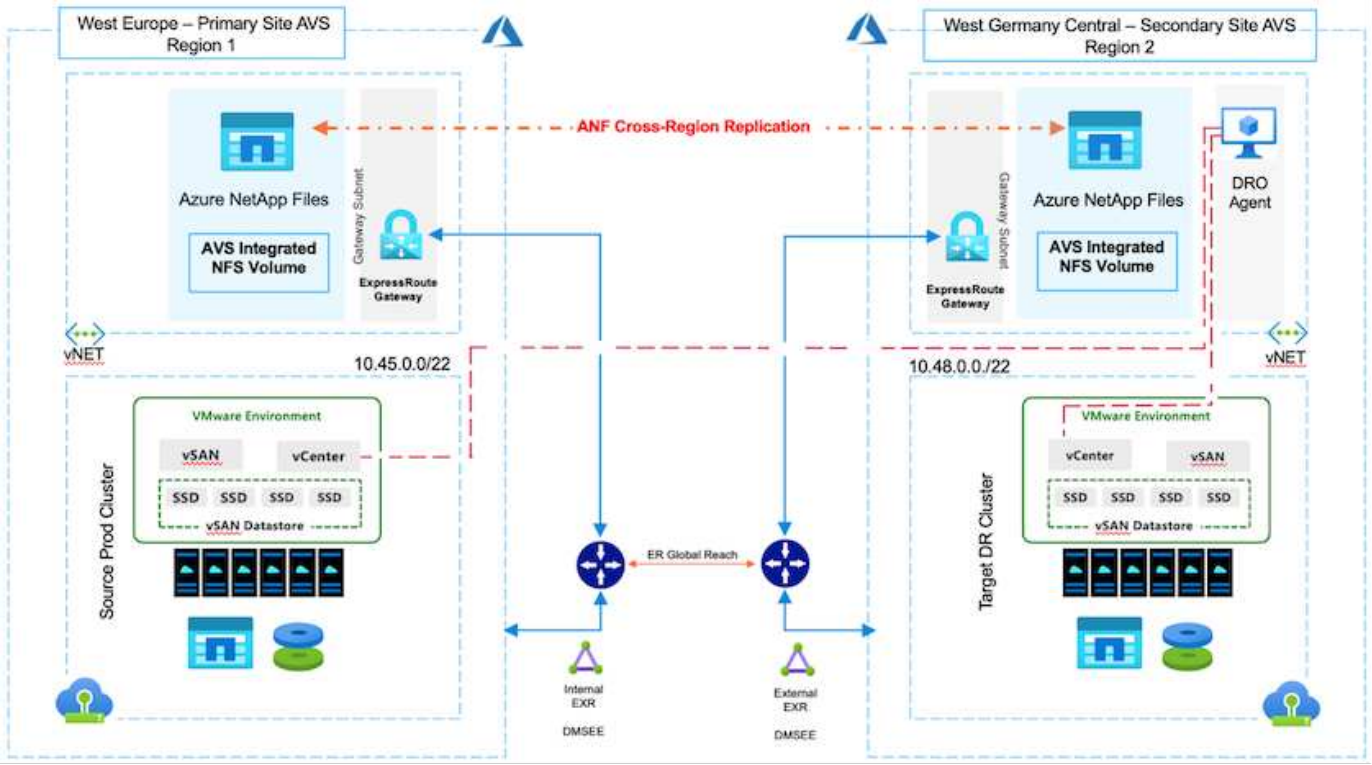
TR-4955: Disaster Recovery con Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

Il disaster recovery mediante replica a livello di blocco tra regioni all'interno del cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati (ad esempio, ransomware).

Panoramica

Grazie alla replica dei volumi tra regioni di Azure NetApp Files (ANF), i carichi di lavoro VMware in esecuzione su un sito SDDC di Azure VMware Solution (AVS) che utilizza volumi di Azure NetApp Files come datastore NFS sul sito AVS primario possono essere replicati su un sito AVS secondario designato nella regione di ripristino di destinazione.

Disaster Recovery Orchestrator (DRO) (una soluzione con script e interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da un AVS SDDC a un altro. DRO automatizza il ripristino interrompendo il peering di replicazione e quindi montando il volume di destinazione come datastore, tramite la registrazione della VM su AVS, sui mapping di rete direttamente su NSX-T (incluso in tutti i cloud privati AVS).



Prerequisiti e raccomandazioni generali

- Verificare di aver abilitato la replica tra regioni creando un peering di replica. Vedere "Crea la replica del volume per Azure NetApp Files" .

- È necessario configurare ExpressRoute Global Reach tra i cloud privati di origine e di destinazione della soluzione Azure VMware.

- È necessario disporre di un'entità di servizio in grado di accedere alle risorse.
- È supportata la seguente topologia: dal sito AVS primario al sito AVS secondario.
- Configurare il "replicazione" pianificare per ogni volume in modo appropriato in base alle esigenze aziendali e alla velocità di modifica dei dati.

> Le topologie a cascata e fan-in e fan-out non sono supportate.

Iniziare

Distribuisci la soluzione Azure VMware

IL "Soluzione Azure VMware" (AVS) è un servizio cloud ibrido che fornisce VMware SDDC completamente funzionali all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione proprietaria 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 l'archiviazione iperconvergente e NSX per la rete e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture dei data center leader del settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure nativi. La combinazione di Azure VMware Solution SDDC e Azure NetApp Files garantisce le migliori prestazioni con una latenza di rete minima.

Per configurare un cloud privato AVS su Azure, seguire i passaggi descritti in questo"collegamento" per la documentazione NetApp e in questo "collegamento" per la documentazione Microsoft. Per scopi DR è possibile utilizzare un ambiente con luce pilota allestito con una configurazione minima. Questa configurazione contiene solo componenti essenziali per supportare le applicazioni critiche e può essere scalata e generare più host per gestire la maggior parte del carico in caso di failover.

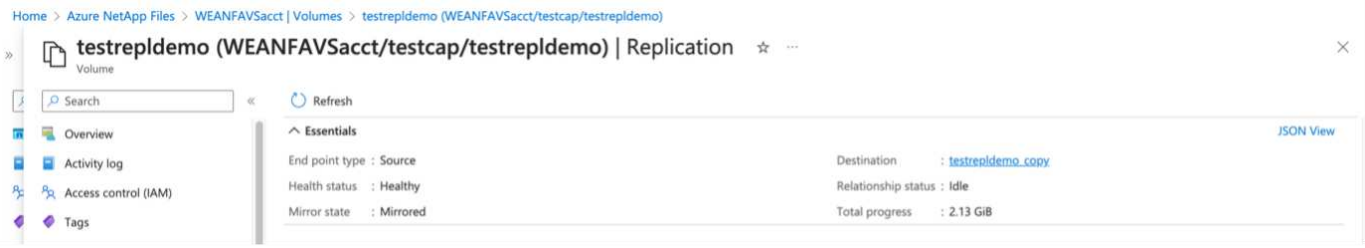
> Nella versione iniziale, DRO supporta un cluster AVS SDDC esistente. La creazione di SDDC su richiesta sarà disponibile in una prossima versione.

Provisioning e configurazione Azure NetApp Files

"Azure NetApp Files"è un servizio di archiviazione file misurato, di classe enterprise e ad alte prestazioni. Segui i passaggi in questo "collegamento" per effettuare il provisioning e configurare Azure NetApp Files come datastore NFS per ottimizzare le distribuzioni cloud private AVS.

Crea la replica del volume per i volumi di datastore basati su Azure NetApp Files

Il primo passo è impostare la replica tra regioni per i volumi di datastore desiderati dal sito primario AVS al sito secondario AVS con le frequenze e le ritenzioni appropriate.



Segui i passaggi in questo "collegamento" per impostare la replicazione tra regioni creando un peering di replicazione. 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 d'uso specifico, è possibile selezionare il livello di servizio standard e quindi "modificare il livello di servizio" in caso di un vero disastro o di simulazioni DR.

Una relazione di replicazione tra regioni è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a usare DRO, utilizzare il sistema operativo Ubuntu sulla macchina virtuale Azure designata e assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti:

- Entità del servizio che può accedere alle risorse.
- Assicurarsi che esista una connettività appropriata per le istanze SDDC di origine e di destinazione e Azure NetApp Files .
- Se si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.

Requisiti del sistema operativo:

- Ubuntu Focal 20.04 (LTS)Il seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
- Docker
- Docker-componi
- 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:

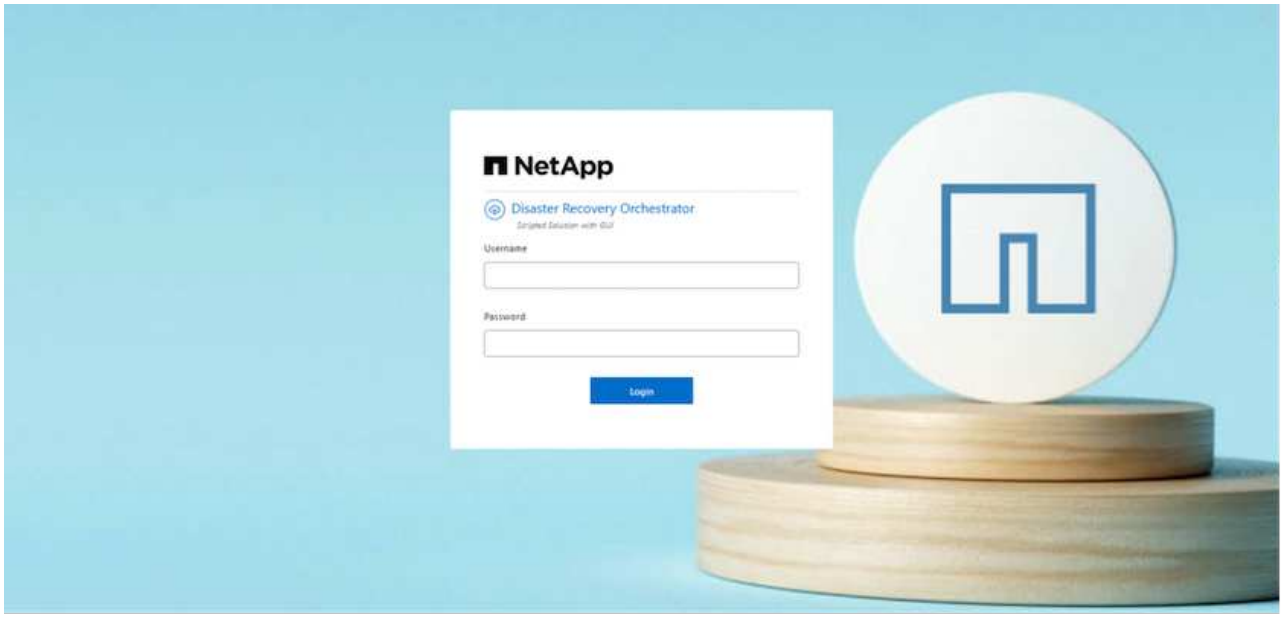
```
git clone https://github.com/NetApp/DRO-Azure.git
```

L'agente deve essere installato nella regione del sito AVS secondario o nella regione del sito AVS primario in una AZ separata rispetto all'SDDC.

2. Decomprimi il pacchetto, esegui lo script di distribuzione e inserisci 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. Accedi 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 carichi di lavoro dal sito AVS primario al sito AVS secondario. NetApp consiglia di distribuire l'agente DRO nel sito AVS secondario e di configurare la connessione gateway ExpressRoute in modo che l'agente DRO possa comunicare tramite la rete con i componenti AVS e Azure NetApp Files appropriati.

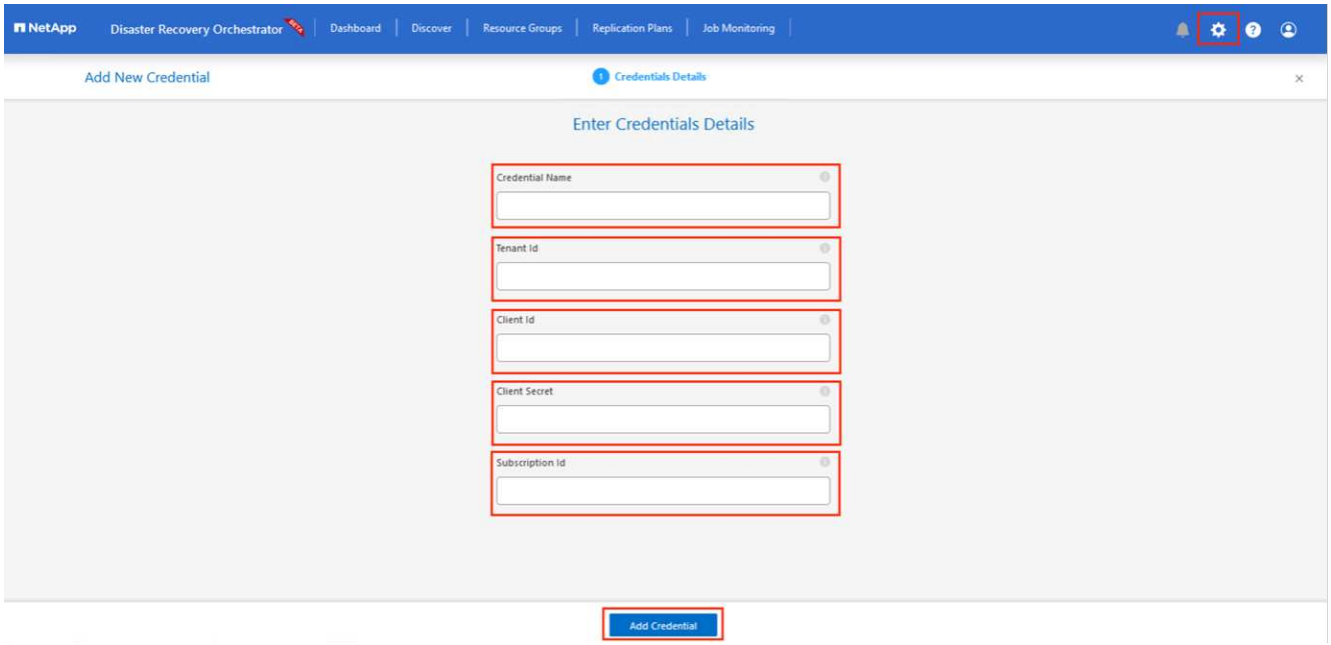
Il primo passo è aggiungere le credenziali. DRO richiede l'autorizzazione per individuare Azure NetApp Files e la soluzione Azure VMware. È possibile concedere le autorizzazioni necessarie a un account Azure creando e configurando un'applicazione Azure Active Directory (AD) e ottenendo le credenziali Azure necessarie a DRO. È necessario associare l'entità servizio alla sottoscrizione di Azure e assegnarle un ruolo personalizzato che disponga delle autorizzazioni richieste. Quando si aggiungono ambienti di origine e di destinazione, viene richiesto di selezionare le credenziali associate al servizio principale. È necessario aggiungere queste credenziali a DRO prima di poter fare clic su Aggiungi nuovo sito.

Per eseguire questa operazione, completare i seguenti passaggi:

1. Apri DRO in un browser supportato e usa il nome utente e la password predefiniti/`admin`/`admin`). La password può essere reimpostata dopo il primo accesso utilizzando l'opzione Cambia password.
2. Nell'angolo in alto a destra della console DRO, fare clic sull'icona **Impostazioni** e selezionare **Credenziali**.
3. Fare clic su Aggiungi nuove credenziali e seguire i passaggi della procedura guidata.
4. Per definire le credenziali, immettere le informazioni sull'entità servizio di Azure Active Directory che concede le autorizzazioni richieste:
    - Nome della credenziale
    - ID inquilino
    - ID cliente
    - Segreto del cliente
    - ID abbonamento

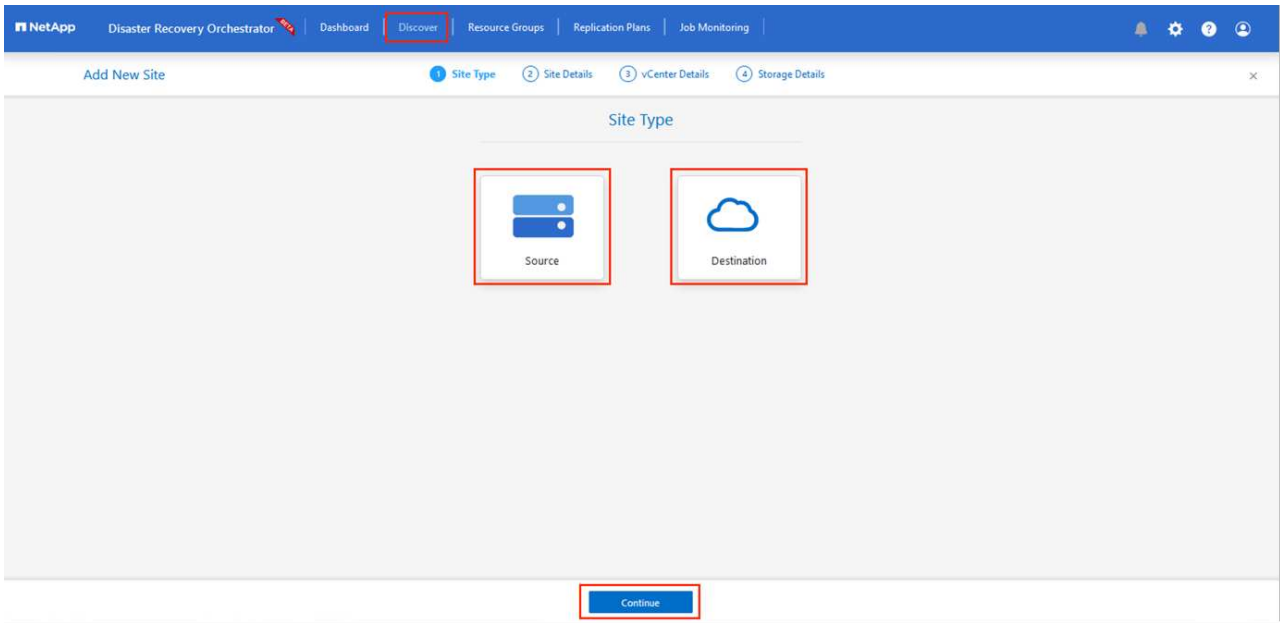
    Avresti dovuto acquisire queste informazioni quando hai creato l'applicazione AD.

5. Conferma i dettagli sulle nuove credenziali e fai clic su 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 di archiviazione dei file di Azure NetApp) a DRO. Per aggiungere il sito di origine e quello di destinazione, completare i seguenti passaggi:

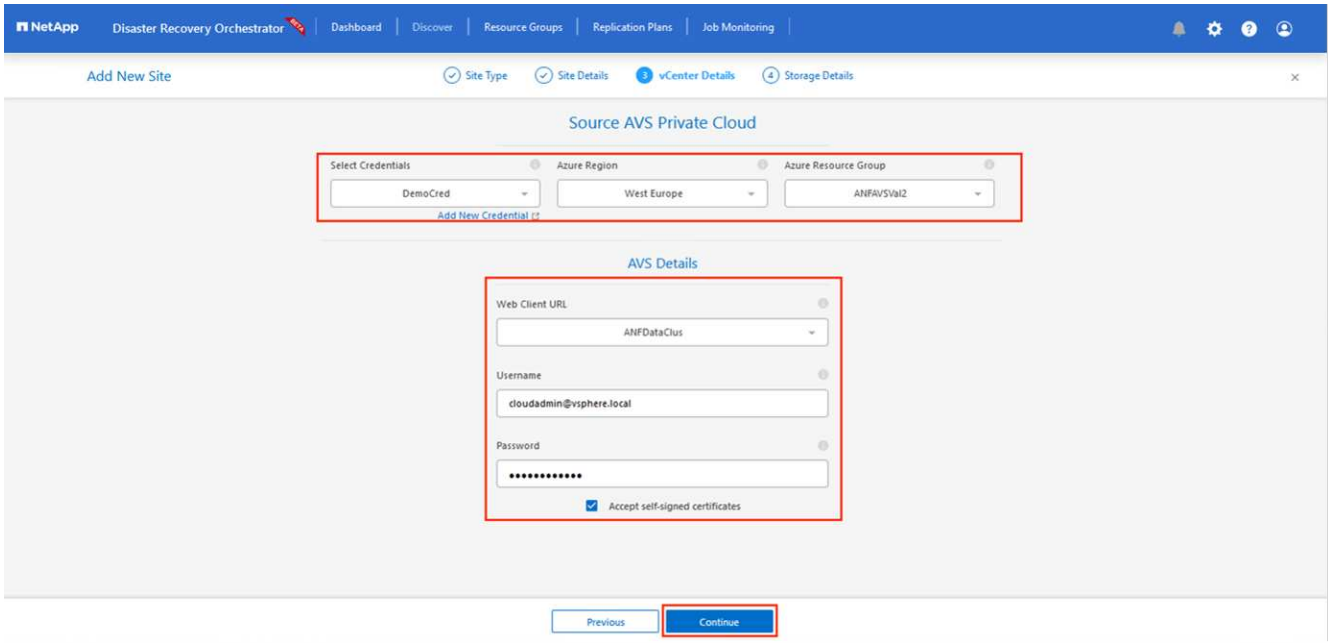
6. Vai alla scheda **Scopri**.
7. Fare clic su **Aggiungi nuovo sito**.
8. Aggiungere il seguente sito AVS primario (designato come **Origine** nella console).
   - SDDC vCenter
   - Account di archiviazione Azure NetApp Files
9. Aggiungere il seguente sito AVS secondario (designato come **Destinazione** nella console).
   - SDDC vCenter
   - Account di archiviazione Azure NetApp Files



10. Aggiungi i dettagli del sito cliccando su **Origine**, immettendo un nome descrittivo per il sito e selezionando il connettore. Quindi fare clic su **Continua**.

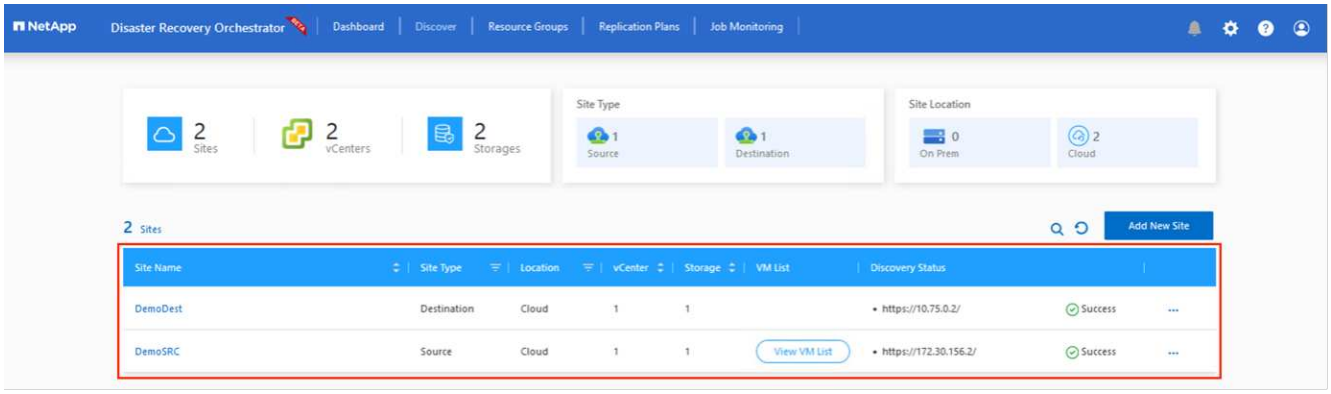
> A scopo dimostrativo, in questo documento viene trattata l'aggiunta di un sito sorgente.

11. Aggiornare i dettagli di vCenter. Per fare ciò, seleziona le credenziali, la regione di Azure e il gruppo di risorse dal menu a discesa per l'SDDC AVS primario.
12. DRO elenca tutti gli SDDC disponibili nella regione. Selezionare l'URL del cloud privato designato dal menu a discesa.
13. Entra nel `cloudadmin@vsphere.local` credenziali utente. È possibile accedervi dal portale di Azure. Seguire i passaggi indicati in questo "collegamento" . Una volta fatto, clicca su **Continua**.

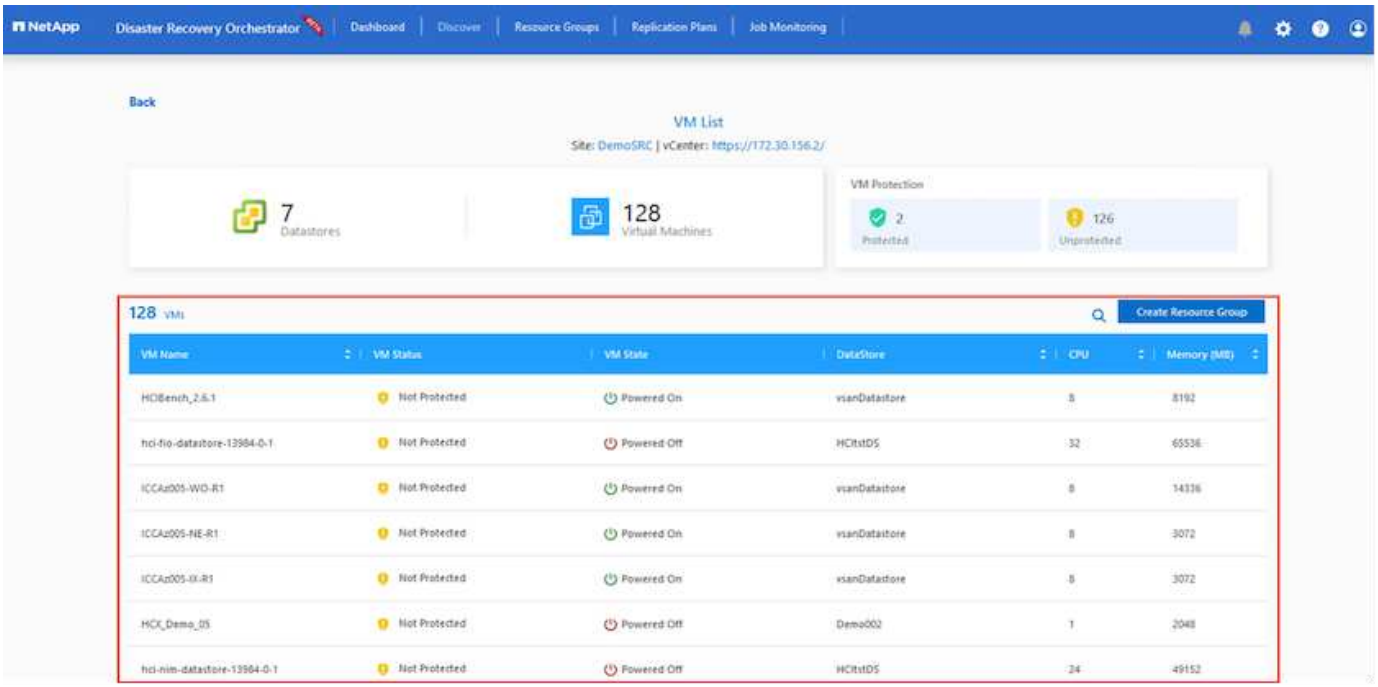


14. Selezionare i dettagli dell'archivio di origine (ANF) selezionando il gruppo di risorse di Azure e l'account NetApp .

15. Fare clic su **Crea sito**.



Una volta aggiunto, DRO esegue la rilevazione automatica e visualizza le VM che dispongono di repliche interregionali corrispondenti dal sito di origine al sito di destinazione. DRO rileva automaticamente le reti e i segmenti utilizzati dalle VM e li popola.



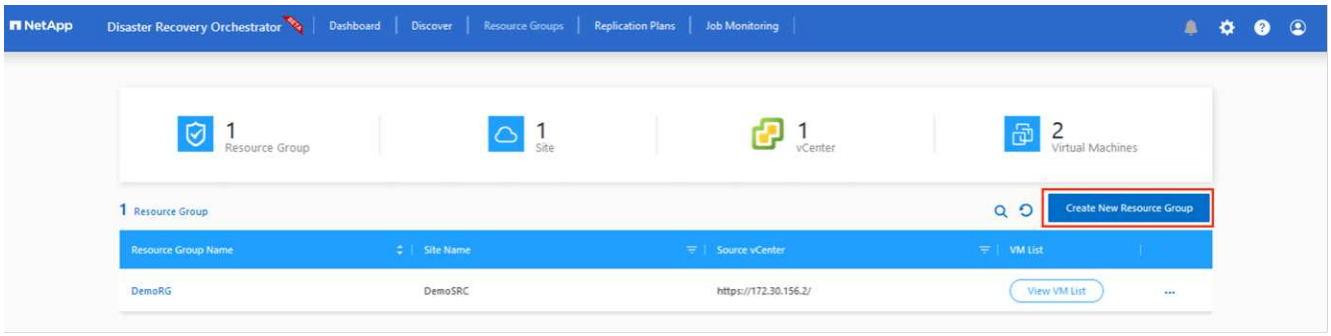
Il passaggio successivo consiste nel raggruppare le VM richieste nei rispettivi gruppi funzionali come gruppi di risorse.

Raggruppamenti di risorse

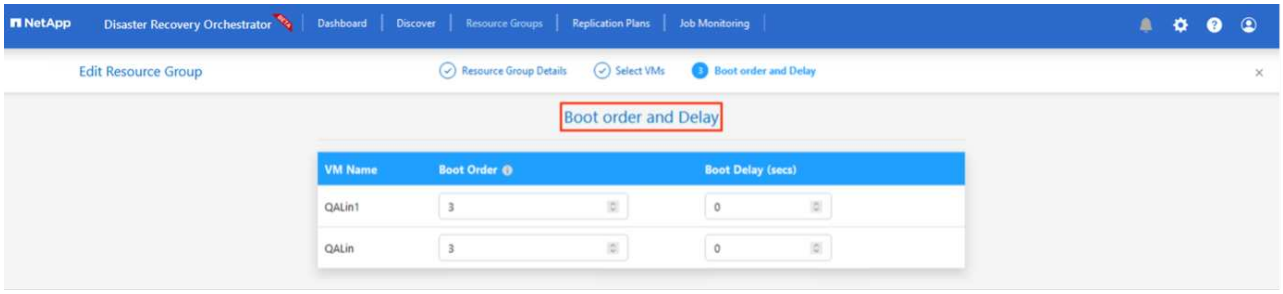
Dopo aver aggiunto le piattaforme, raggruppa le VM che desideri ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e convalide facoltative delle applicazioni che possono essere eseguite al momento del ripristino.

Per iniziare a creare gruppi di risorse, fare clic sulla voce di menu **Crea nuovo gruppo di risorse**.

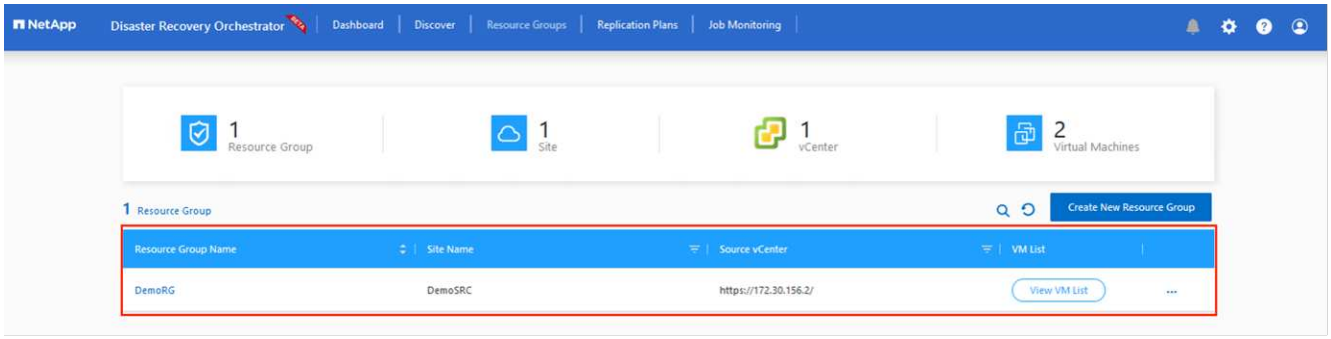
1. Accedi a **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.



2. In Nuovo gruppo di risorse, seleziona il sito di origine dal menu a discesa e fai clic su **Crea**.
3. Fornisci i dettagli del gruppo di risorse e fai clic su **Continua**.
4. Selezionare le VM appropriate utilizzando l'opzione di ricerca.
5. Selezionare **Ordine di avvio** e **Ritardo di avvio** (sec) per tutte le VM selezionate. Imposta l'ordine della sequenza di accensione selezionando ogni macchina virtuale e impostandone la priorità. Il valore predefinito per tutte le macchine virtuali è 3. Le opzioni sono le seguenti:
   - La prima macchina virtuale ad accendersi
   - Predefinito
   - L'ultima macchina virtuale ad accendersi



6. Fare clic su **Crea gruppo di risorse**.

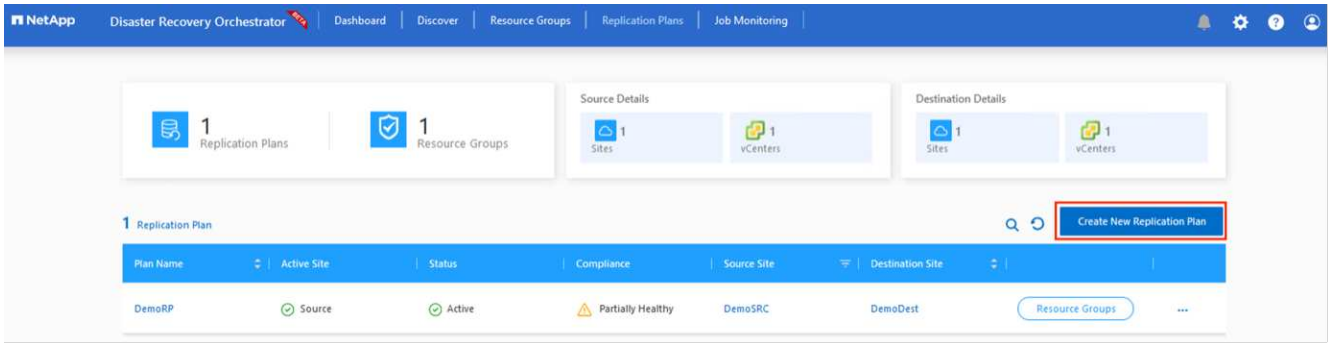


Piani di replicazione

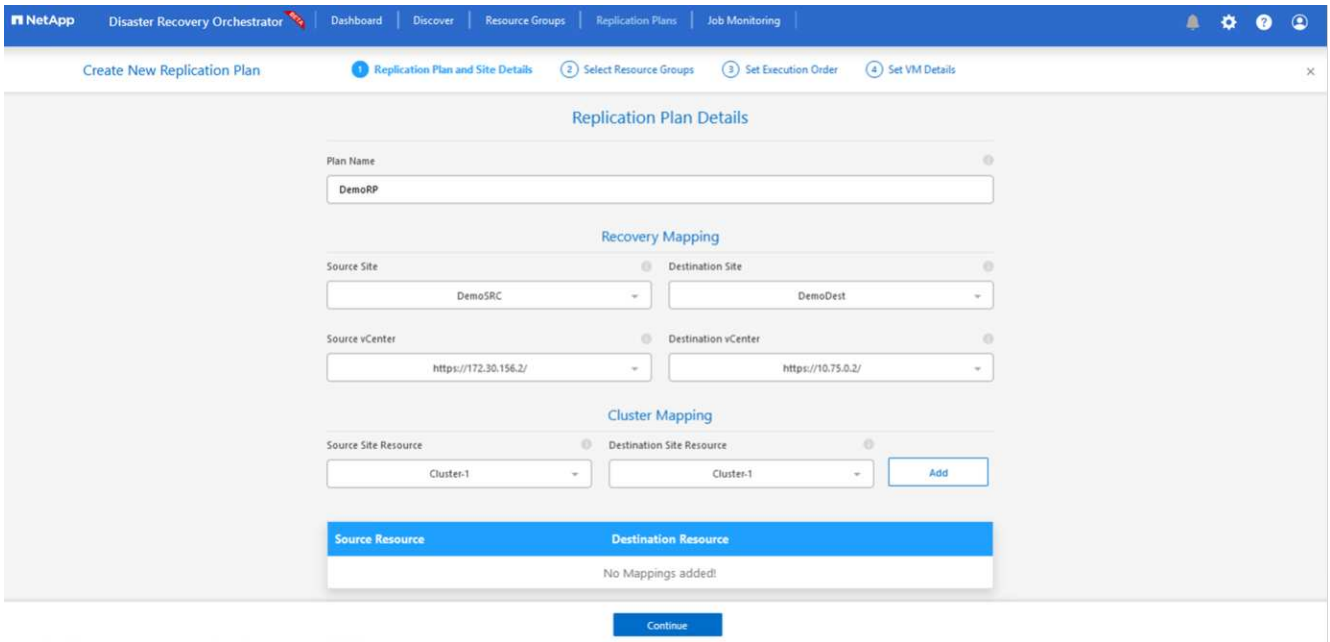
È necessario disporre di un piano per ripristinare le applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dal menu a discesa, scegliere i gruppi di risorse da includere in questo piano e includere anche il raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, livello 1, livello 2 e così via). I piani vengono spesso chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda Piano di replica e fare clic su **Nuovo piano di replica**.

Per iniziare a creare un piano di replicazione, completare i seguenti passaggi:

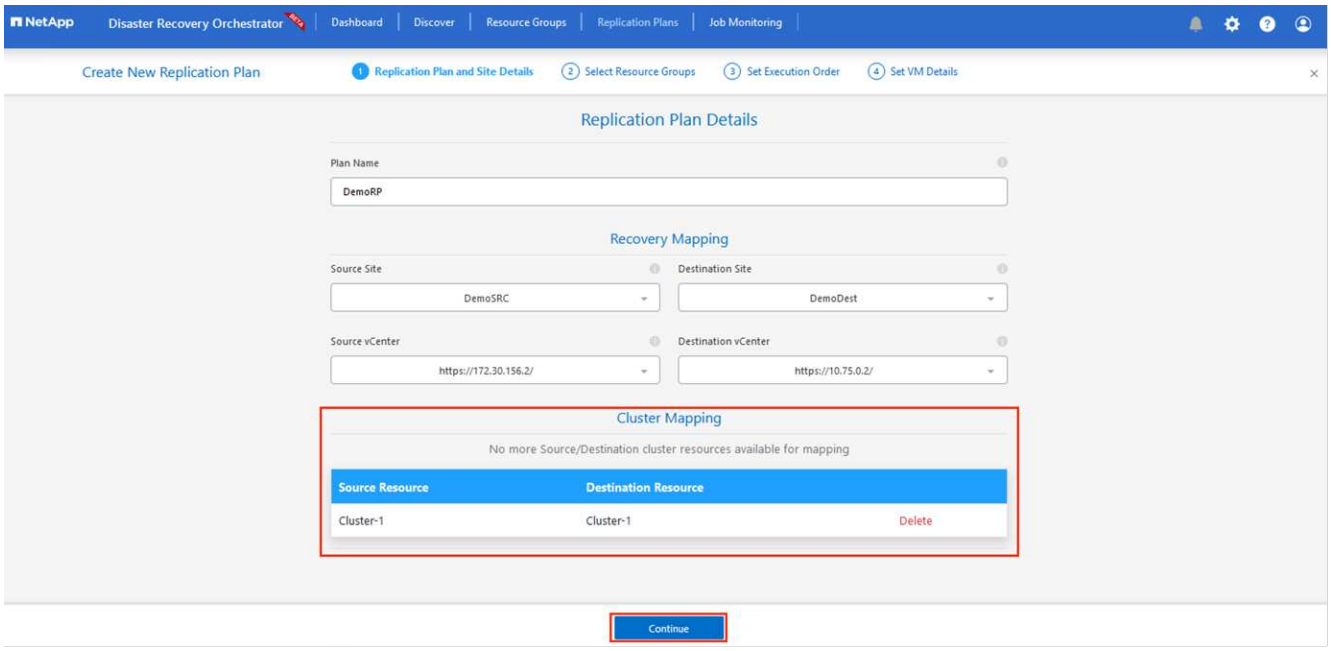
1. Passare a **Piani di replicazione** e fare clic su **Crea nuovo piano di replicazione**.



2. Nel **Nuovo piano di replica**, fornire 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.

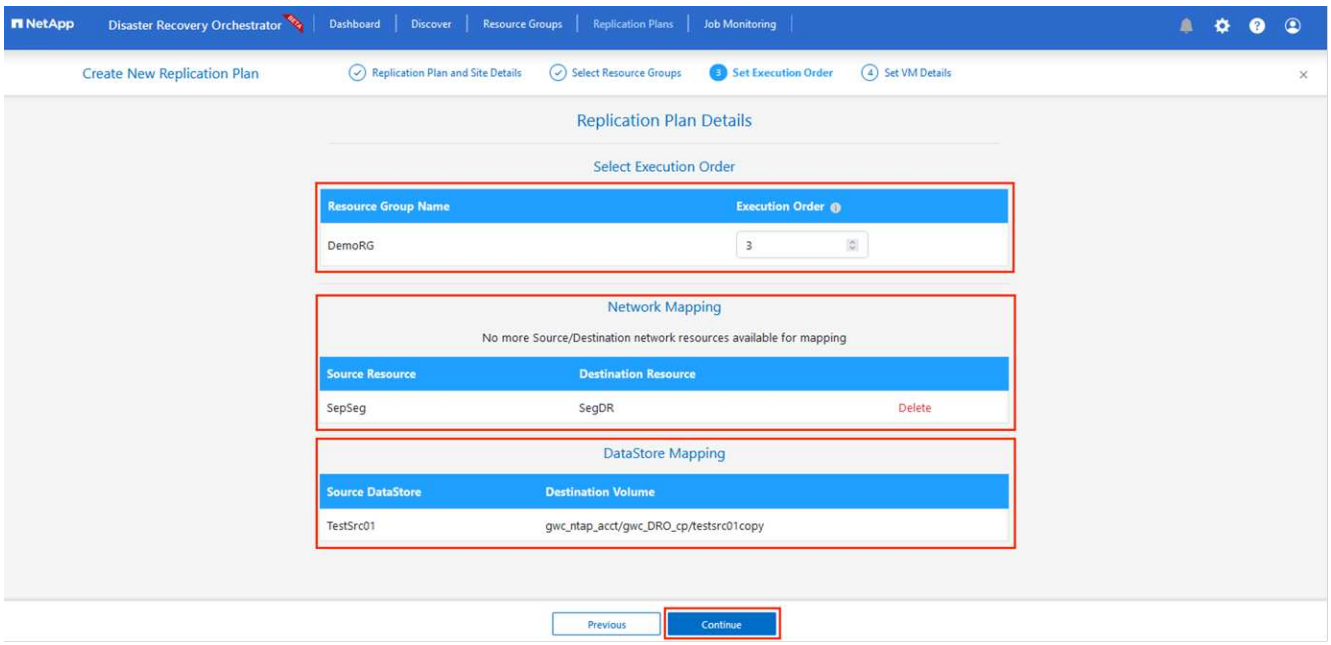


3. Una volta completata la mappatura del ripristino, selezionare **Cluster Mapping**.



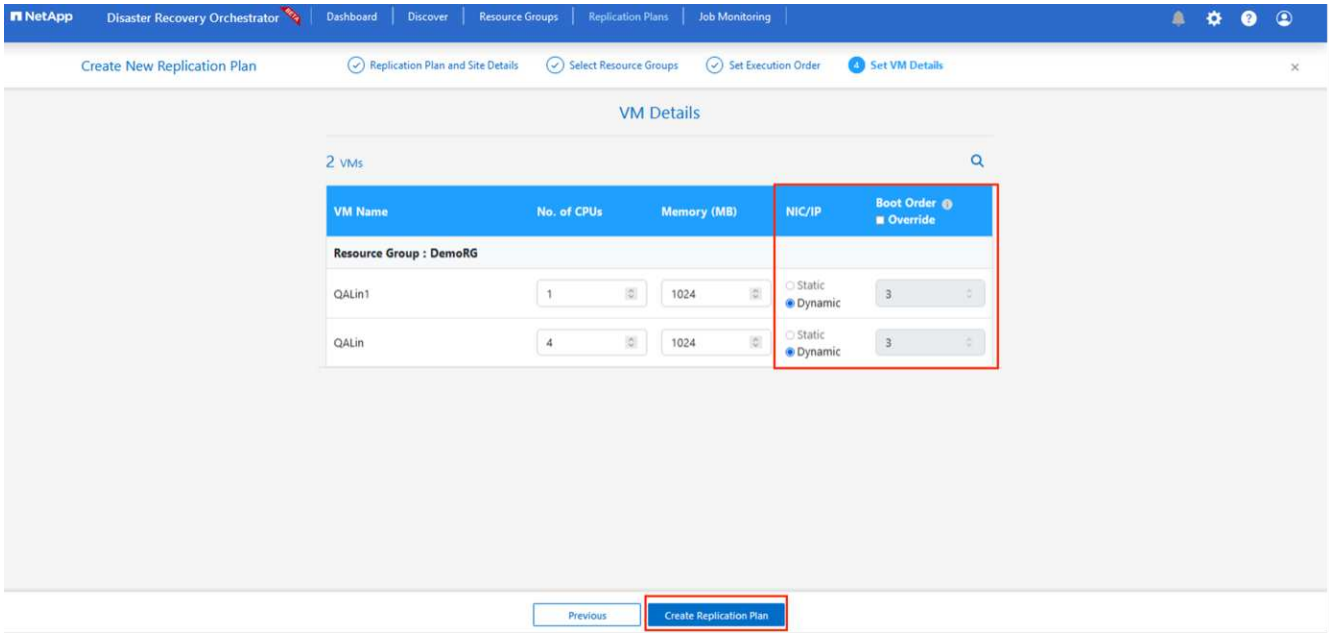
4. Selezionare **Dettagli gruppo di risorse** e fare clic su **Continua**.
5. Imposta l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza delle operazioni quando sono presenti più gruppi di risorse.
6. Una volta fatto, imposta la mappatura di rete sul segmento appropriato. I segmenti dovrebbero essere già forniti sul cluster AVS secondario e, per mappare le VM su di essi, selezionare il segmento appropriato.
7. Le mappature dei datastore vengono selezionate automaticamente in base alla selezione delle VM.

> La replicazione interregionale (CRR) avviene a livello di volume. Pertanto, tutte le VM residenti sul rispettivo volume vengono replicate nella destinazione CRR. Assicurarsi di selezionare tutte le VM che fanno parte del datastore, perché vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.

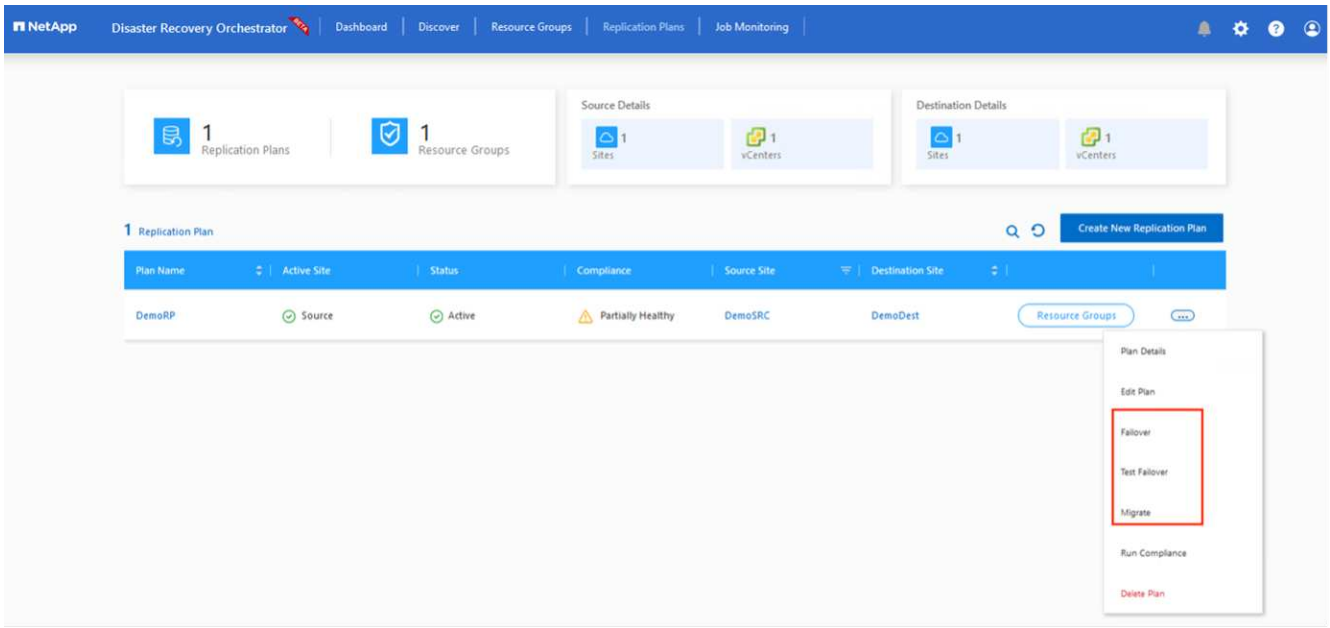


8. In Dettagli VM, è possibile ridimensionare facoltativamente i parametri CPU e RAM delle VM. Ciò può

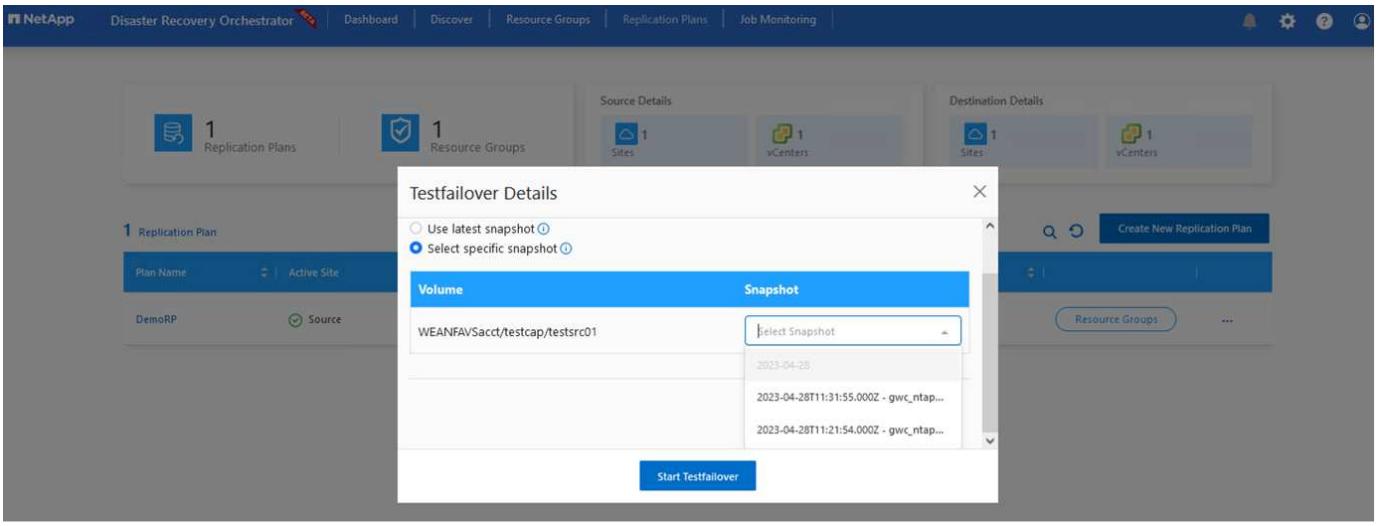
essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o quando si eseguono test di ripristino di emergenza senza dover predisporre un'infrastruttura VMware fisica uno a uno. Modificare inoltre l'ordine di avvio e il ritardo di avvio (in secondi) per tutte le VM selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche rispetto a quanto 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 è possibile apportare modifiche in questa fase.



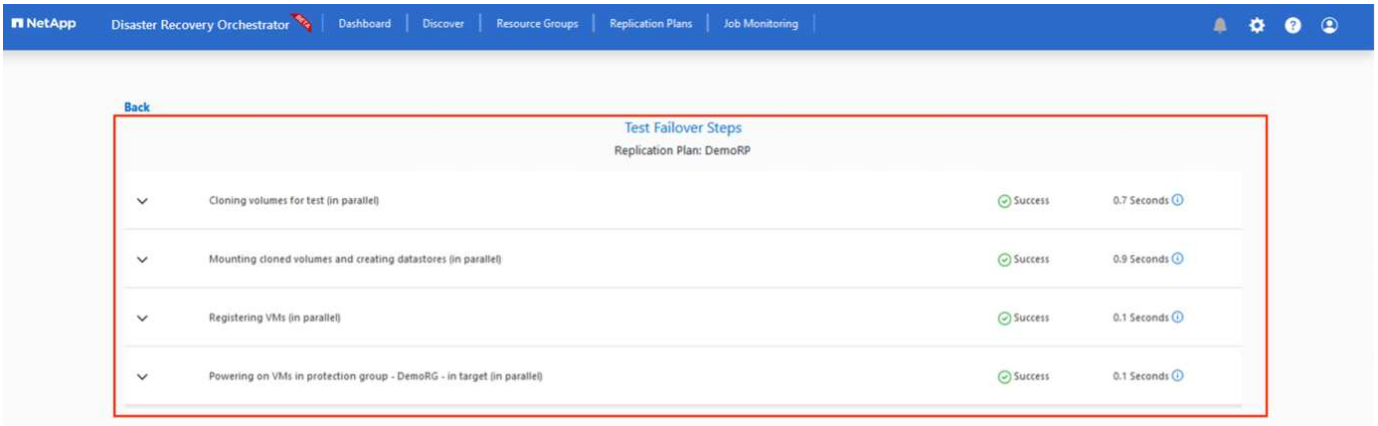
9. Fare clic su **Crea piano di replicazione**. Dopo aver creato il piano di replicazione, è possibile utilizzare le opzioni di failover, failover di prova o migrazione, a seconda delle proprie esigenze.



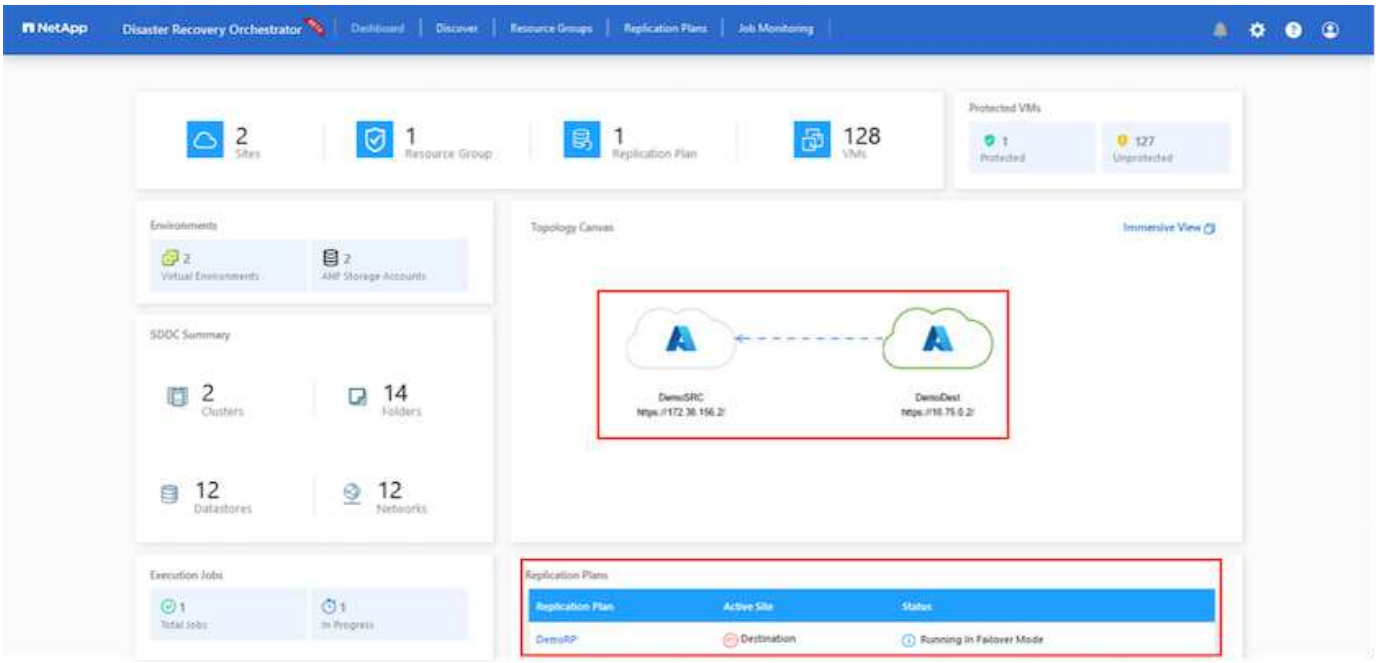
Durante le opzioni di failover e di test failover, viene utilizzato lo snapshot più recente oppure è possibile selezionare uno snapshot specifico da uno snapshot point-in-time. L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come un ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i punti temporali disponibili.



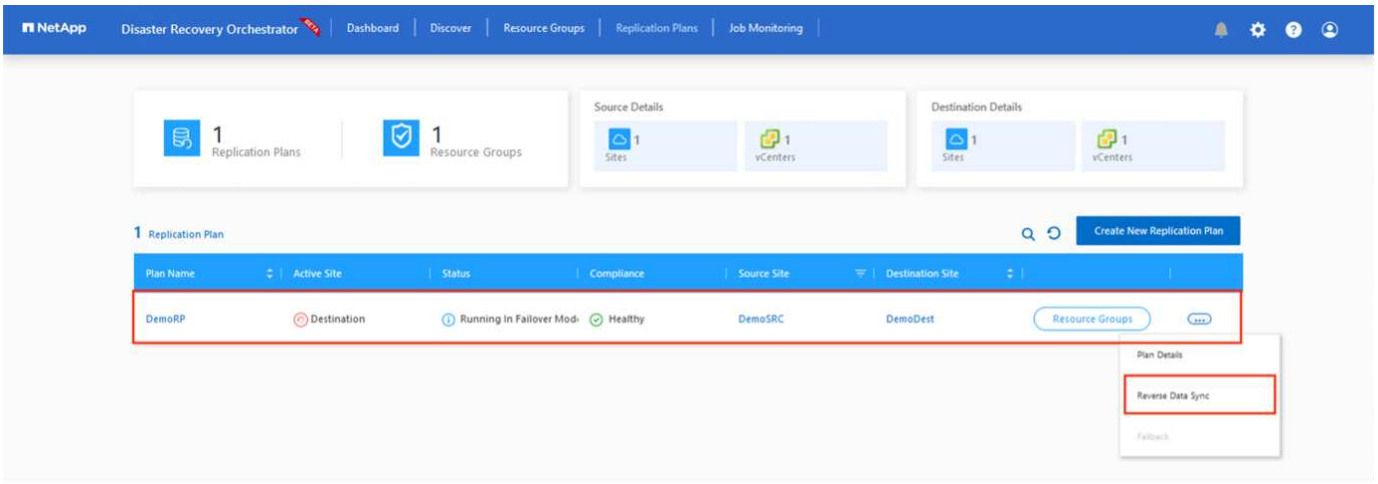
Per attivare il failover o il failover di prova con la configurazione specificata nel piano di replica, è possibile fare clic su **Failover** o **Failover di prova**. È possibile monitorare il piano di replicazione nel menu delle attività.



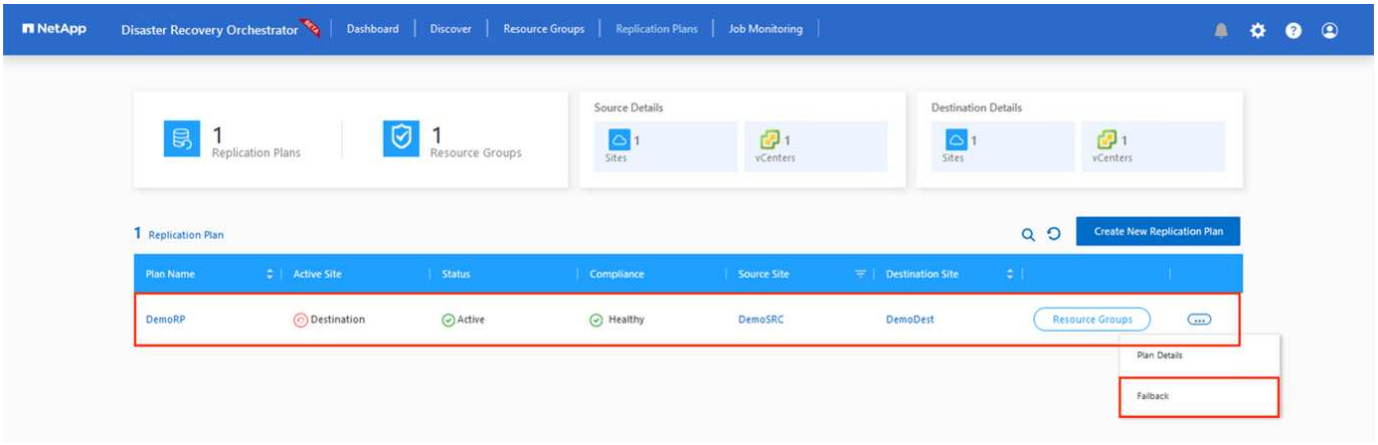
Dopo l'attivazione del failover, gli elementi recuperati possono essere visualizzati nel sito secondario AVS SDDC vCenter (VM, reti e datastore). Per impostazione predefinita, le VM vengono ripristinate nella cartella Workload.

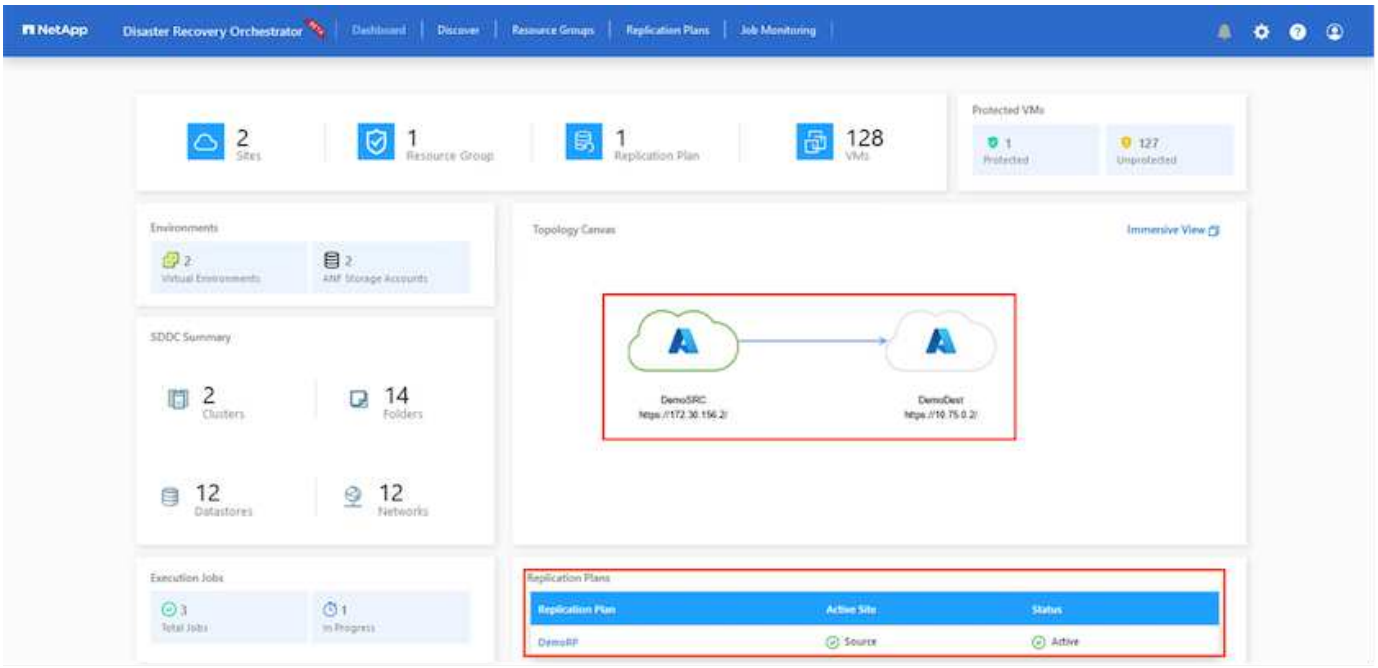


Il failback può essere attivato a livello del piano di replica. In caso di failover del test, è possibile utilizzare l'opzione tear down per annullare le modifiche e rimuovere il volume appena creato. I failback correlati al failover sono un processo in due fasi. Selezionare il piano di replicazione e selezionare **Sincronizzazione dati inversa**.



Una volta completato questo passaggio, attivare il failback per tornare al sito AVS primario.





Dal portale di Azure possiamo vedere che lo stato di integrità della replica è stato interrotto per i volumi appropriati che erano stati mappati sul sito secondario AVS SDDC come volumi di lettura/scrittura. Durante il failover di prova, DRO non mappa il volume di destinazione o di replica. Crea invece un nuovo volume dello snapshot di replica tra regioni richiesto ed espone il volume come un 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 replicazione possono continuare durante i test 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 recupero di dati danneggiati.

Recupero da ransomware

Recuperare i dati da un ransomware può essere un compito arduo. Nello specifico, può essere difficile per le organizzazioni IT individuare con precisione qual è il punto di ritorno sicuro e, una volta determinato, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi ricorrenti (ad esempio, da malware inattivi o tramite applicazioni vulnerabili).

DRO affronta queste problematiche consentendo alle organizzazioni di recuperare da qualsiasi momento disponibile. I carichi di lavoro vengono quindi ripristinati su reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro senza essere esposte al traffico nord-sud. Questo processo offre ai team di sicurezza un luogo sicuro in cui condurre analisi forensi e identificare eventuali

malware nascosti o inattivi.

Conclusione

La soluzione di disaster recovery Azure NetApp Files e Azure VMware offre i seguenti vantaggi:

- Sfrutta la replica efficiente e resiliente tra più regioni Azure NetApp Files .
- Ripristina qualsiasi punto temporale disponibile con la conservazione degli snapshot.
- Automatizza completamente tutti i passaggi necessari per ripristinare centinaia o migliaia di VM dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- Il ripristino del carico di lavoro sfrutta il processo "Crea nuovi volumi dagli snapshot più recenti", che non manipola il volume replicato.
- Evita qualsiasi rischio di danneggiamento dei dati sui volumi o sugli snapshot.
- Evitare interruzioni della replica durante i flussi di lavoro dei test DR.
- Sfrutta i dati DR e le risorse di elaborazione cloud per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.
- L'ottimizzazione di CPU e RAM può contribuire a ridurre i costi del cloud consentendo il ripristino su cluster di elaborazione più piccoli.

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, consultare i seguenti documenti e/o siti web:

- Crea la replica del volume per Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replica tra regioni di volumi di Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Soluzione Azure VMware"

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

- Distribuire e configurare l'ambiente di virtualizzazione su Azure

  "Configurazione di AVS su Azure"

- Distribuisci e configura la soluzione Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Utilizzo di Veeam Replication e del datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware

Gli archivi dati di Azure NetApp Files (ANF) separano l'archiviazione dall'elaborazione e offrono la flessibilità necessaria a qualsiasi organizzazione per trasferire i propri carichi di lavoro sul cloud. Fornisce ai clienti un'infrastruttura di storage flessibile e ad alte

prestazioni, scalabile indipendentemente dalle risorse di elaborazione. L'archivio dati Azure NetApp Files semplifica e ottimizza la distribuzione insieme ad Azure VMware Solution (AVS) come sito di disaster recovery per ambienti VMWare locali.

Panoramica

Gli archivi dati NFS basati su volumi Azure NetApp Files (ANF) possono essere utilizzati per replicare i dati da ambienti locali tramite qualsiasi soluzione di terze parti convalidata che fornisca funzionalità di replica delle VM. Aggiungendo gli archivi dati di Azure NetApp Files , sarà possibile ottimizzare i costi di distribuzione rispetto alla creazione di un SDDC di Azure VMware Solution con un'enorme quantità di host ESXi per ospitare l'archiviazione. Questo approccio è chiamato "Pilot Light Cluster". Un cluster di luci pilota è una configurazione host AVS minima (3 nodi AVS) insieme alla capacità di Azure NetApp Files Datastore.

L'obiettivo è mantenere un'infrastruttura a basso costo con tutti i componenti principali per gestire un failover. Un cluster di luci pilota può essere ampliato e predisporre più host AVS in caso di failover. Una volta completato il failover e ripristinate le normali operazioni, il gruppo di spie luminose può tornare a funzionare in modalità a basso costo.

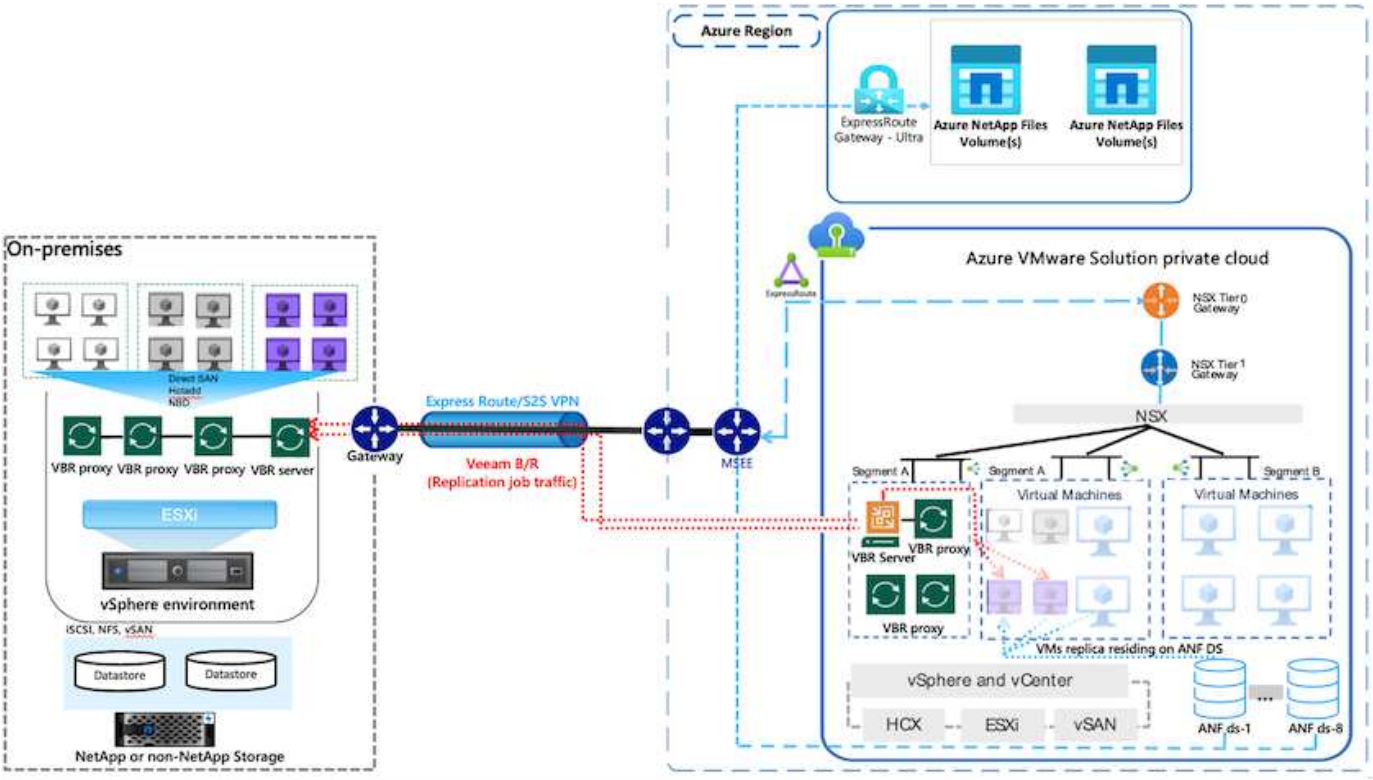
Scopi del presente documento

In questo articolo viene descritto come utilizzare il datastore di Azure NetApp Files con Veeam Backup and Replication per configurare il disaster recovery per le VM VMware locali (AVS) utilizzando la funzionalità del software di replica delle VM Veeam.

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 creerà una copia esatta delle VM nel formato nativo VMware vSphere sul cluster AVS SDDC di destinazione. Veeam Backup & Replication manterrà la copia sincronizzata con la VM originale. La replica fornisce il miglior obiettivo di tempo di ripristino (RTO) poiché è presente una copia montata di una VM nel sito DR in uno stato pronto per l'avvio.

Questo meccanismo di replicazione garantisce che i carichi di lavoro possano essere avviati rapidamente in un AVS SDDC in caso di evento disastroso. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e connessioni lente. Inoltre, filtra anche i blocchi di dati duplicati, i blocchi di dati zero, i file di swap e i "file del sistema operativo guest della VM esclusi". Il software comprimerà anche il traffico di replica. Per evitare che i processi di replicazione 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 guidato dai processi, ovvero la replica viene eseguita configurando i processi di replica. In caso di disastro, è possibile attivare il failover per ripristinare le VM eseguendo il failover sulla relativa copia replica. Quando viene eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito sullo stato più recente di una replica o su uno qualsiasi dei suoi punti di ripristino noti. Ciò consente il ripristino da ransomware o test isolati, a seconda delle necessità. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.



Distribuzione della soluzione

Gradini di alto livello

1. Il software Veeam Backup and Replication è in esecuzione in un ambiente locale con connettività di rete adeguata.
2. "Distribuisci la soluzione Azure VMware (AVS)"cloud privato e"collegare gli archivi dati Azure NetApp Files" agli host della soluzione Azure VMware.

   Per scopi DR è possibile utilizzare un ambiente con luce pilota allestito con una configurazione minima. In caso di incidente, le VM effettueranno il failover su questo cluster e potranno essere aggiunti nodi aggiuntivi.

3. Impostare il processo di replica per creare repliche di VM utilizzando Veeam Backup and Replication.
4. Creare un piano di failover ed eseguire il failover.
5. Una volta completato l'evento disastroso e quando il sito primario è attivo, tornare alle VM di produzione.

Prerequisiti per la replica delle VM Veeam sui datastore AVS e ANF

1. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa sia ai cluster AVS SDDC di origine che a quelli di destinazione.
2. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai vCenter di origine e di destinazione.
3. L'archivio dati di Azure NetApp Files di destinazione deve disporre di spazio libero sufficiente per archiviare i VMDK delle VM replicate.

Per ulteriori informazioni, fare riferimento alla sezione "Considerazioni e limitazioni" trattata"Qui" .

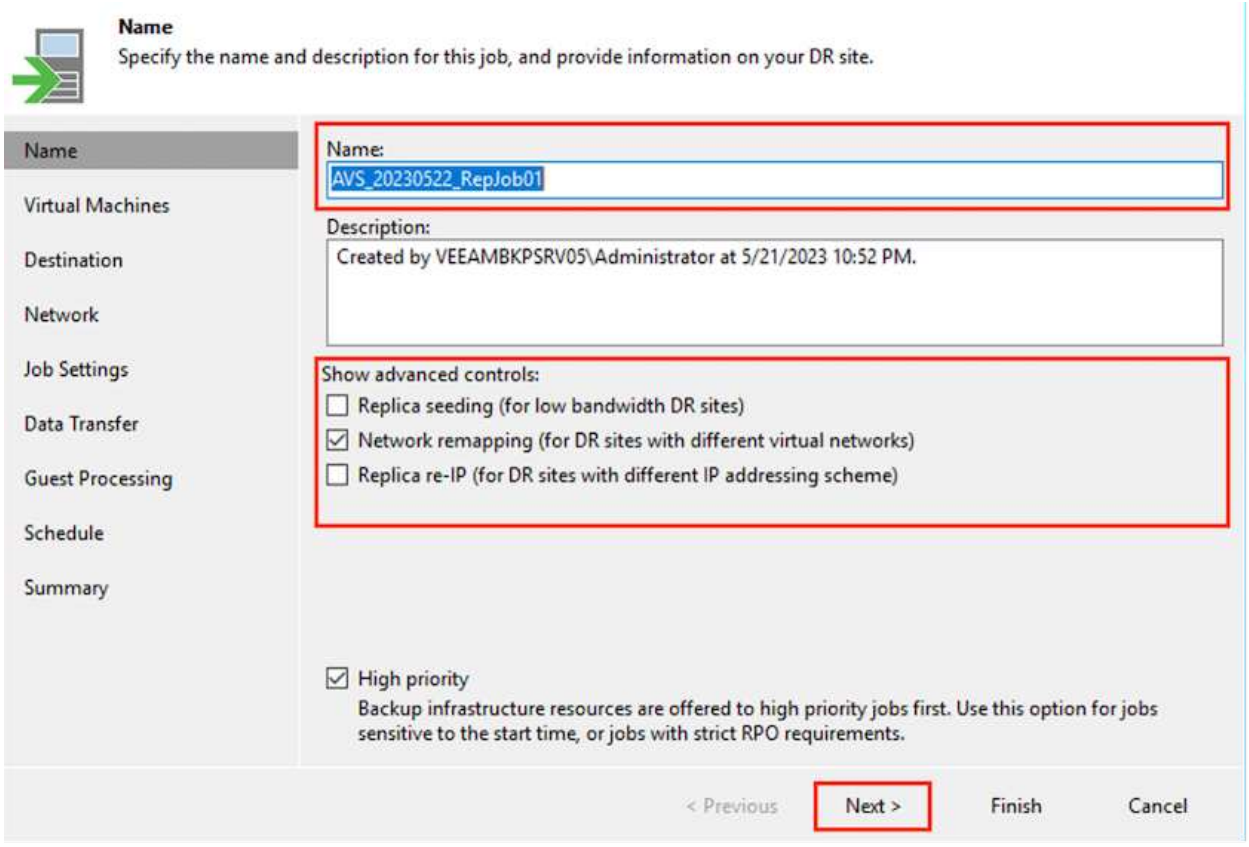
Dettagli di distribuzione

▼ **Passaggio 1: replicare le VM**

Veeam Backup & Replication sfrutta le funzionalità di snapshot di VMware vSphere. Durante la replica, Veeam Backup & Replication richiede a VMware vSphere di creare uno snapshot della VM. Lo snapshot della VM è la copia di una VM in un dato momento che include dischi virtuali, stato del sistema, configurazione e metadati. Veeam Backup & Replication utilizza lo snapshot come origine dei dati per la replica.

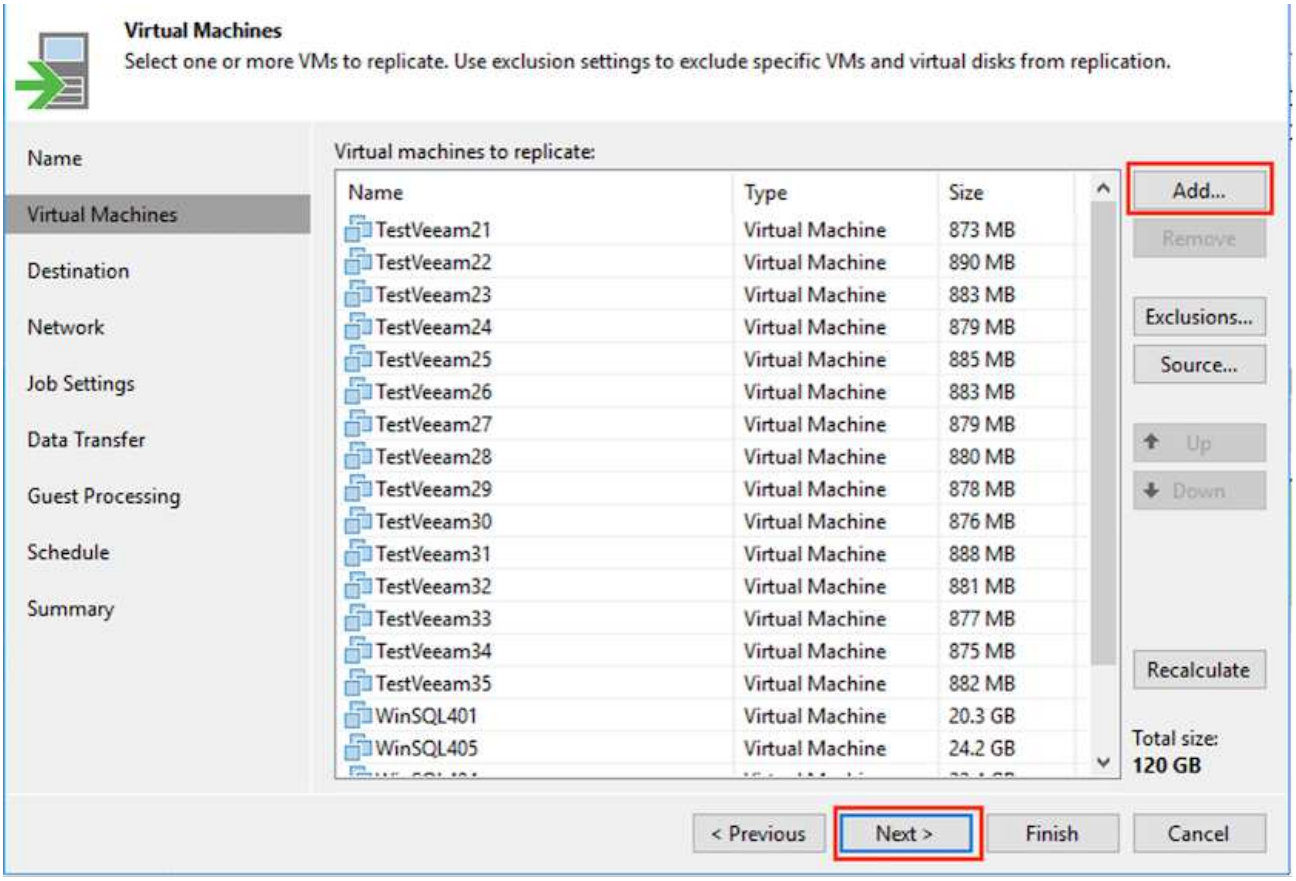
Per replicare le VM, seguire i passaggi seguenti:

1. Aprire la console Veeam Backup & Replication.
2. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo dei processi e selezionare Processo di replica > Macchina virtuale.
3. Specificare un nome per il lavoro e selezionare la casella di controllo avanzata appropriata. Fare clic su Avanti.
   - Selezionare la casella di controllo Replica seeding se la connettività tra locale e Azure ha una larghezza di banda limitata. *Selezionare la casella di controllo Rimappatura di rete (per siti AVS SDDC con reti diverse) se i segmenti su Azure VMware Solution SDDC non corrispondono a quelli delle reti dei siti locali.
   - Se lo schema di indirizzamento IP nel sito di produzione locale è diverso dallo schema nel sito AVS di destinazione, selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso).

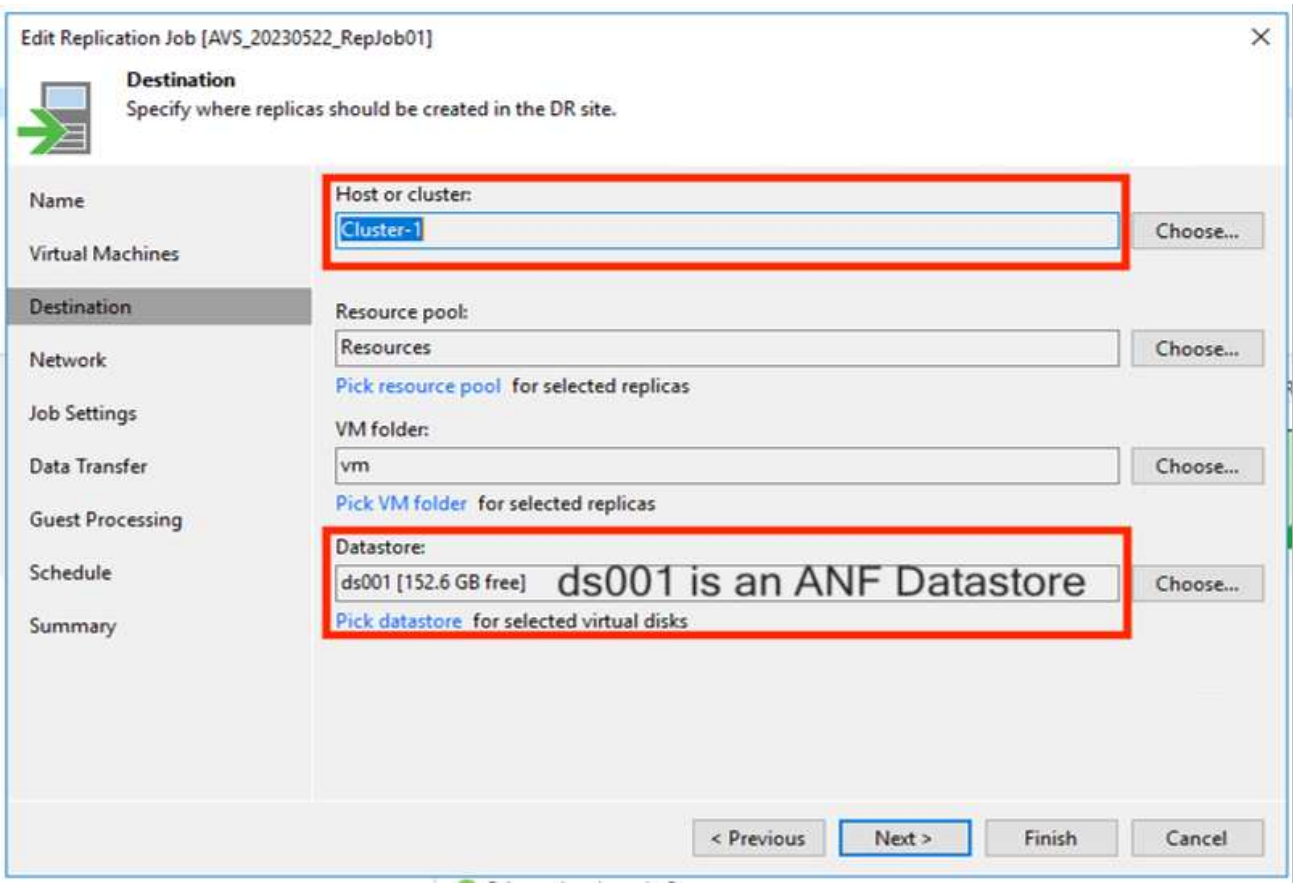


4. Selezionare le VM da replicare nel datastore di Azure NetApp Files collegato a un SDDC di Azure VMware Solution nel passaggio Macchine **virtuali**. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità disponibile del datastore vSAN. In un cluster di luci pilota, la capacità

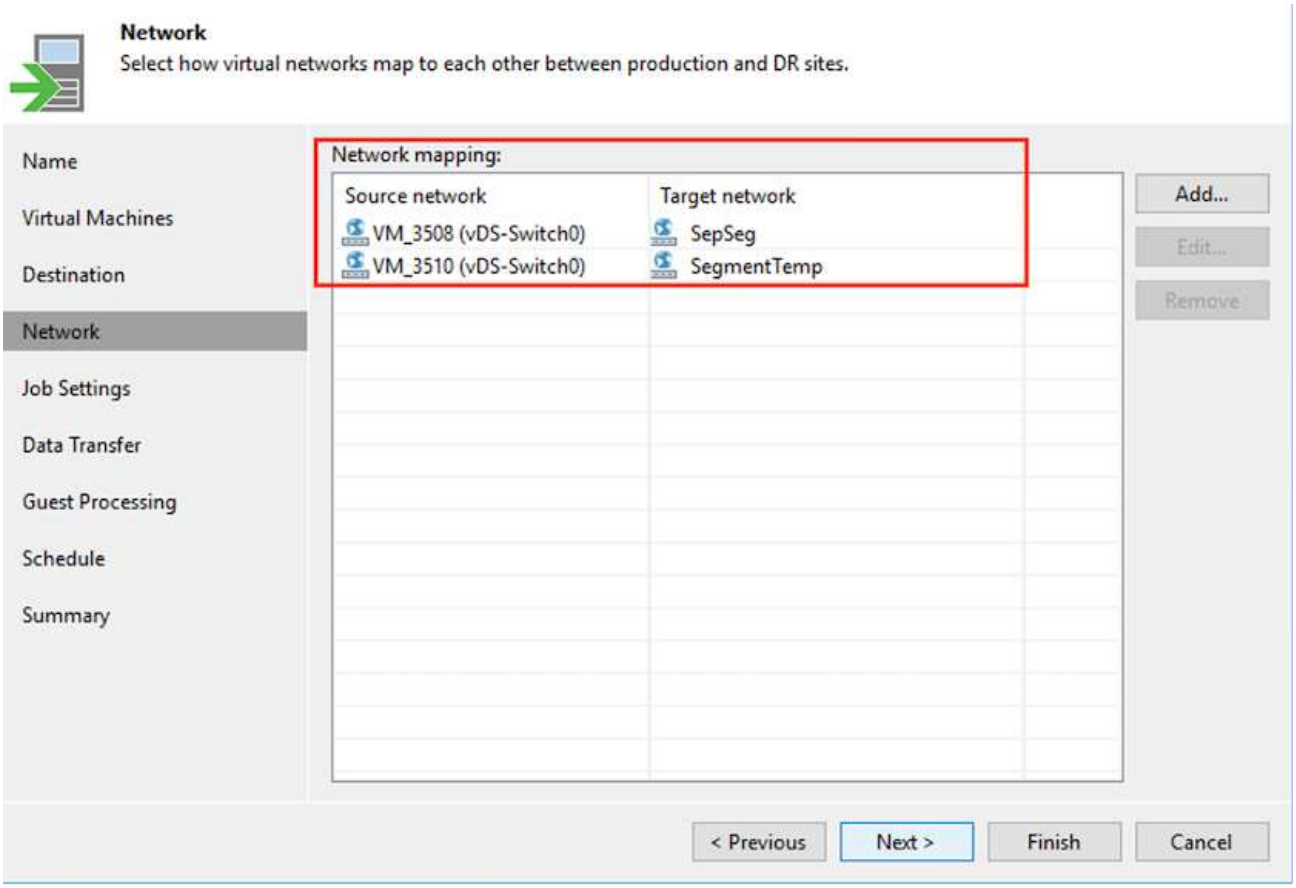
utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere facilmente inserito negli archivi dati di Azure NetApp Files, in modo che le macchine virtuali possano essere ripristinate e il cluster possa essere espanso per soddisfare i requisiti di CPU/memoria. Fare clic su **Aggiungi**, quindi nella finestra **Aggiungi oggetto** selezionare le VM o i contenitori VM necessari e fare clic su **Aggiungi**. Fare clic su **Avanti**.



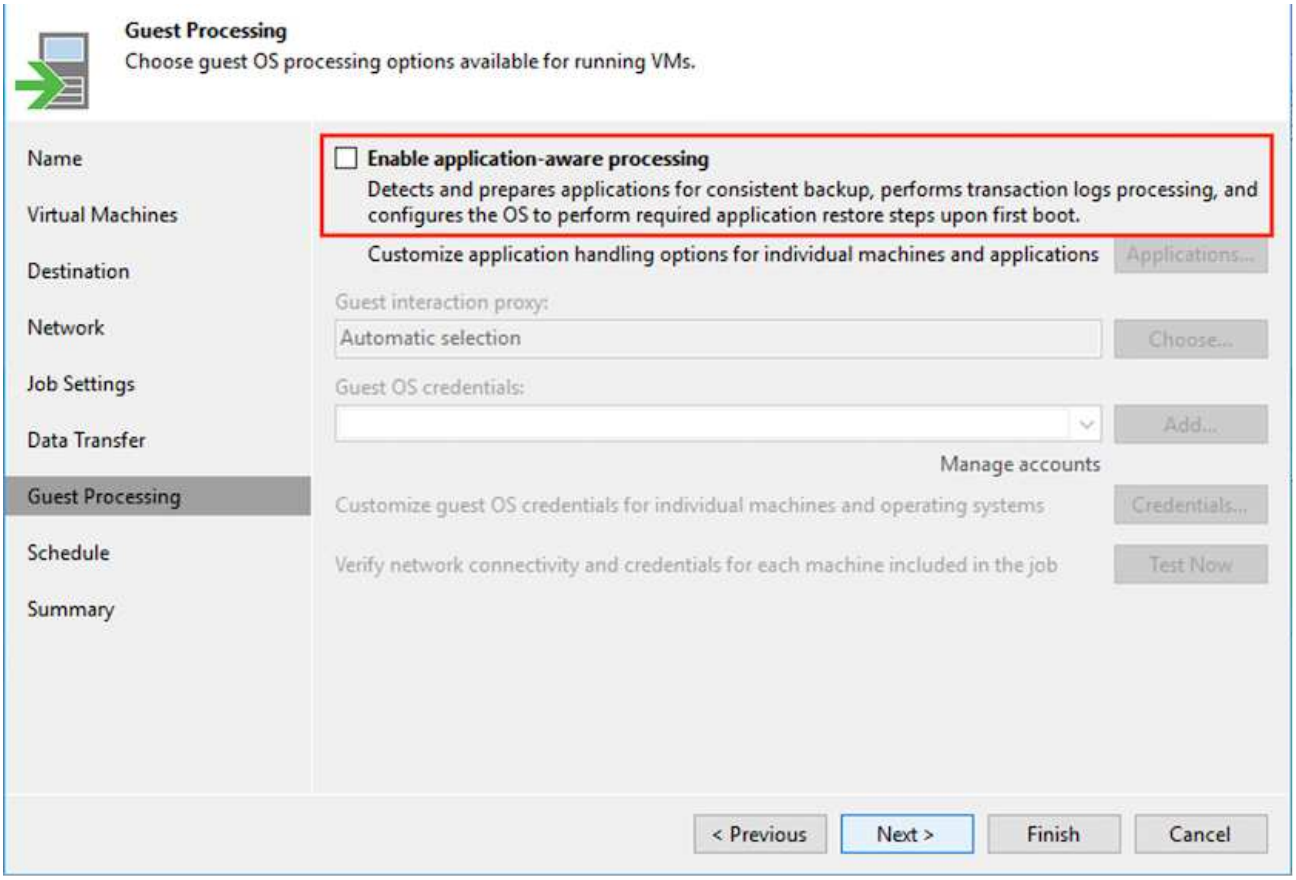
5. Successivamente, selezionare la destinazione come cluster/host SDDC di Azure VMware Solution e il pool di risorse appropriato, la cartella VM e il datastore FSx ONTAP per le repliche VM. Quindi fare clic su **Avanti**.



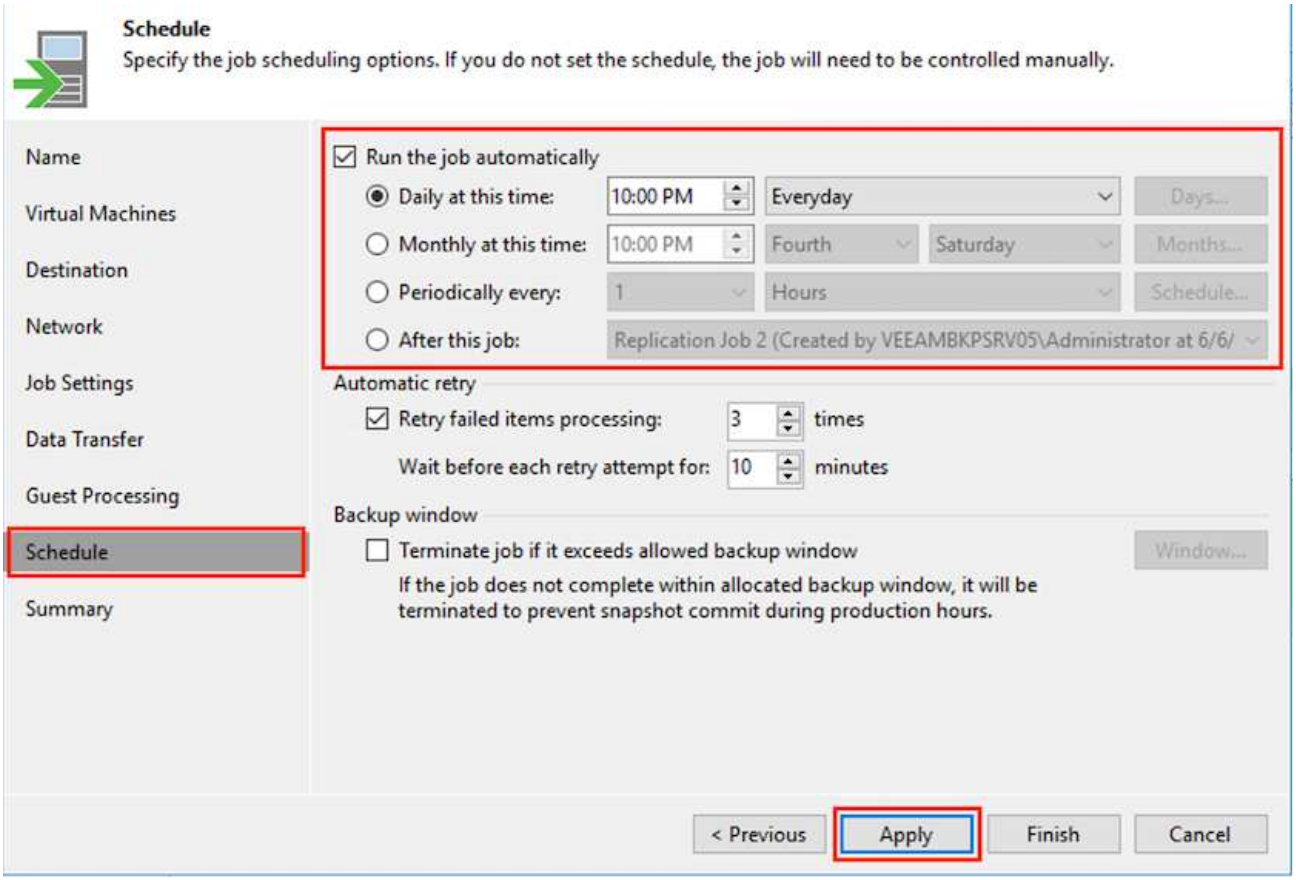
6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e quella di destinazione in base alle esigenze.



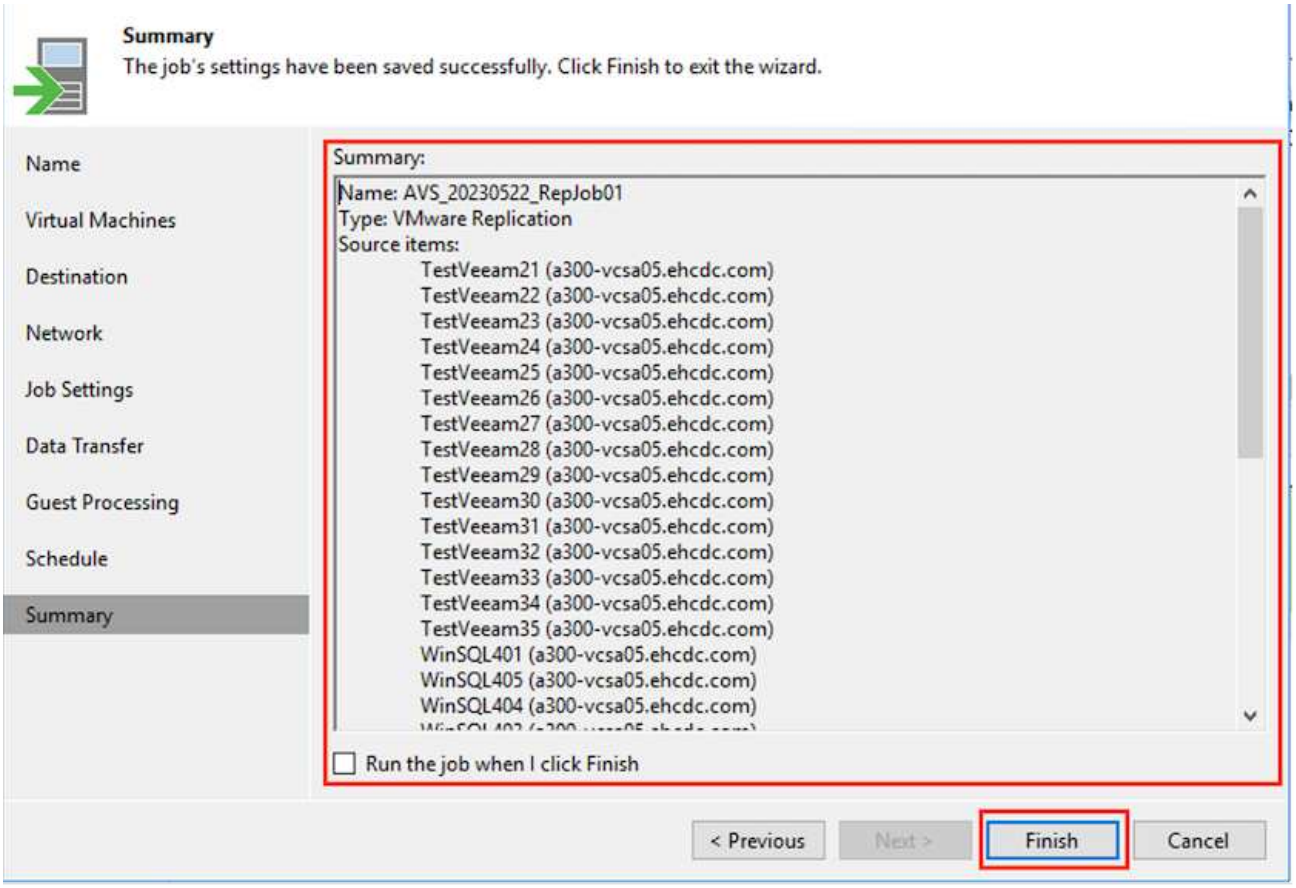
7. Nel passaggio **Impostazioni processo**, specificare il repository di backup in cui verranno archiviati i metadati per le repliche delle VM, i criteri di conservazione e così via.
8. Aggiorna i server proxy **Origine** e **Destinazione** nel passaggio **Trasferimento dati** e lascia la selezione **Automatica** (predefinita), mantieni selezionata l'opzione **Diretta** e fai clic su **Avanti**.
9. Nella fase **Elaborazione guest**, selezionare l'opzione **Abilita elaborazione basata sull'applicazione** in base alle esigenze. Fare clic su **Avanti**.



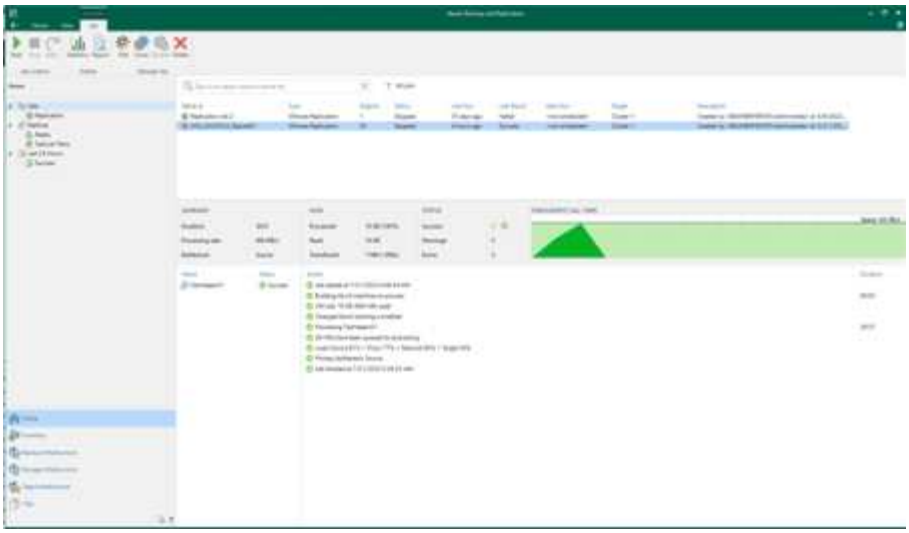
10. Selezionare la pianificazione della replica per eseguire il processo di replica regolarmente.



11. Nella fase **Riepilogo** della procedura guidata, rivedere i dettagli del processo di replica. Per avviare il processo subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il processo quando faccio clic su Fine**, altrimenti lasciare la casella di controllo deselezionata. Quindi fare clic su **Fine** per chiudere la procedura guidata.



Una volta avviato il processo di replica, le VM con il suffisso specificato verranno popolate sul cluster/host AVS SDDC di destinazione.



Per ulteriori informazioni sulla replica Veeam, fare riferimento"Come funziona la replicazione"

▼ **Passaggio 2: creare un piano di failover**

Una volta completata la replicazione o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire il failover per le VM dipendenti una alla volta o come gruppo automaticamente. Il piano di failover è il modello per l'ordine in cui vengono elaborate le VM, inclusi i ritardi di avvio. Il piano di failover aiuta anche a garantire che le VM dipendenti critiche siano già in esecuzione.

Per creare il piano, vai alla nuova sottosezione denominata **Repliche** e seleziona **Piano di failover**. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo momento e li utilizzerà per avviare le repliche delle VM.

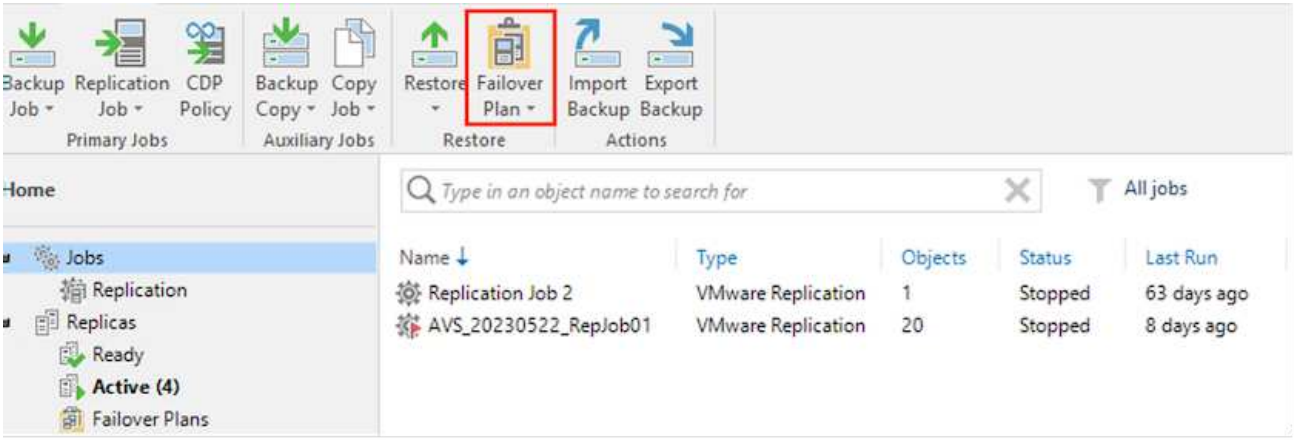
Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e quando le repliche delle VM sono nello stato Pronto.

Il numero massimo di VM che possono essere avviate simultaneamente durante l'esecuzione di un piano di failover è 10

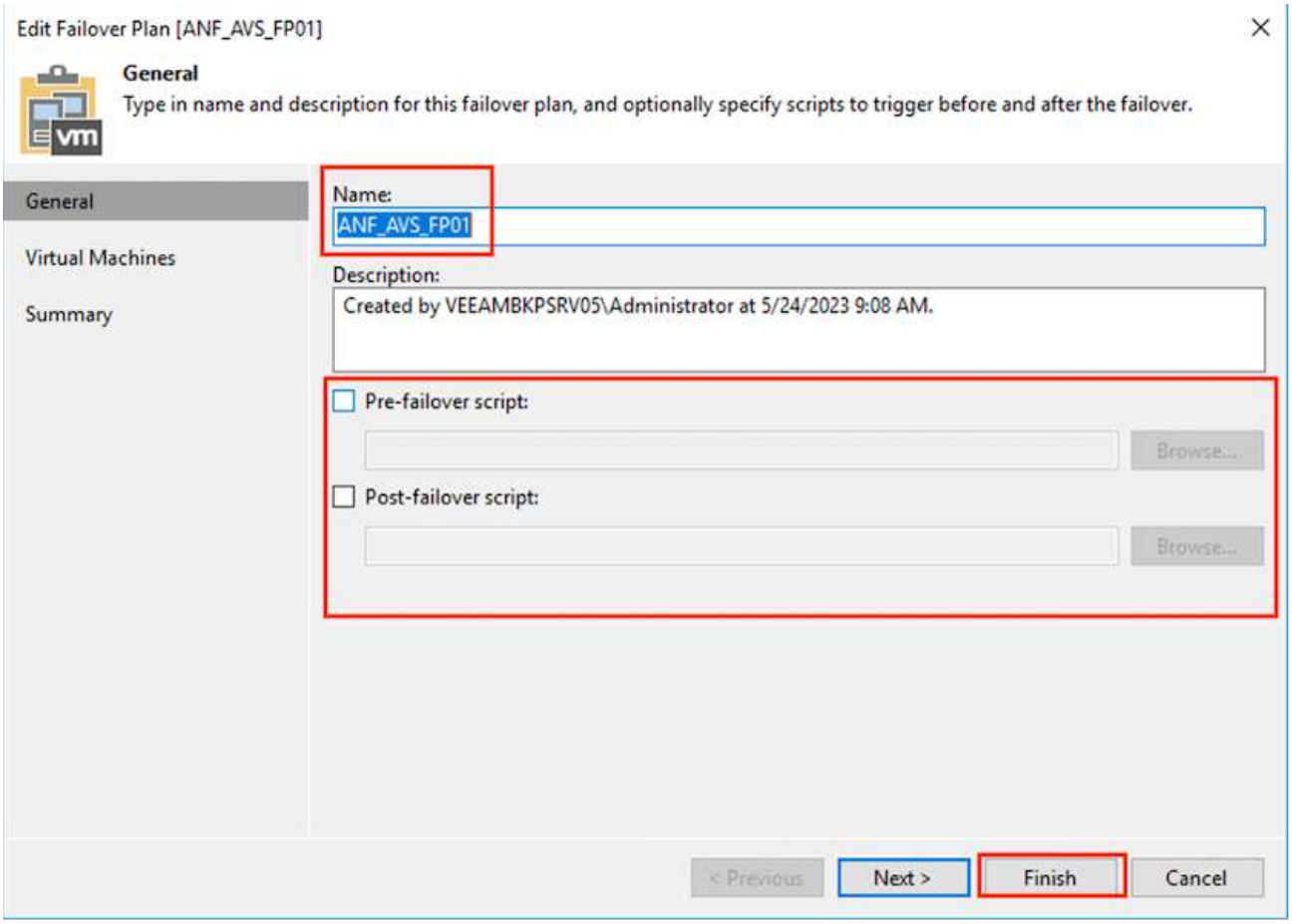
Durante il processo di failover, le VM di origine non verranno spente

Per creare il **Piano di failover**, procedere come segue:

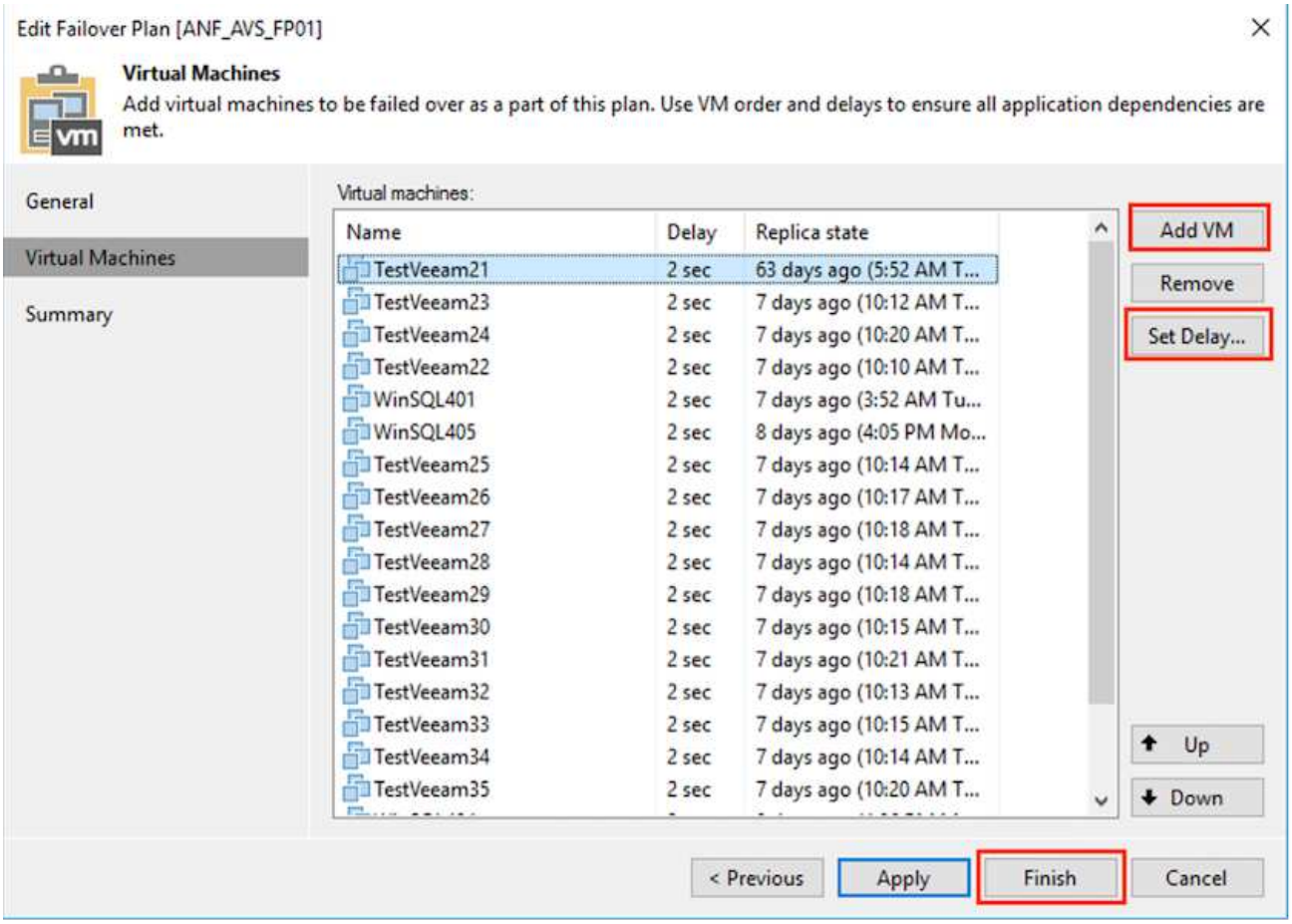
1. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo Repliche e selezionare Piani di failover > Piano di failover > VMware vSphere.



2. Successivamente, fornisci un nome e una descrizione al piano. È possibile aggiungere script pre e post-failover in base alle esigenze. Ad esempio, eseguire uno script per arrestare le VM prima di avviare le VM replicate.



3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze dell'applicazione.



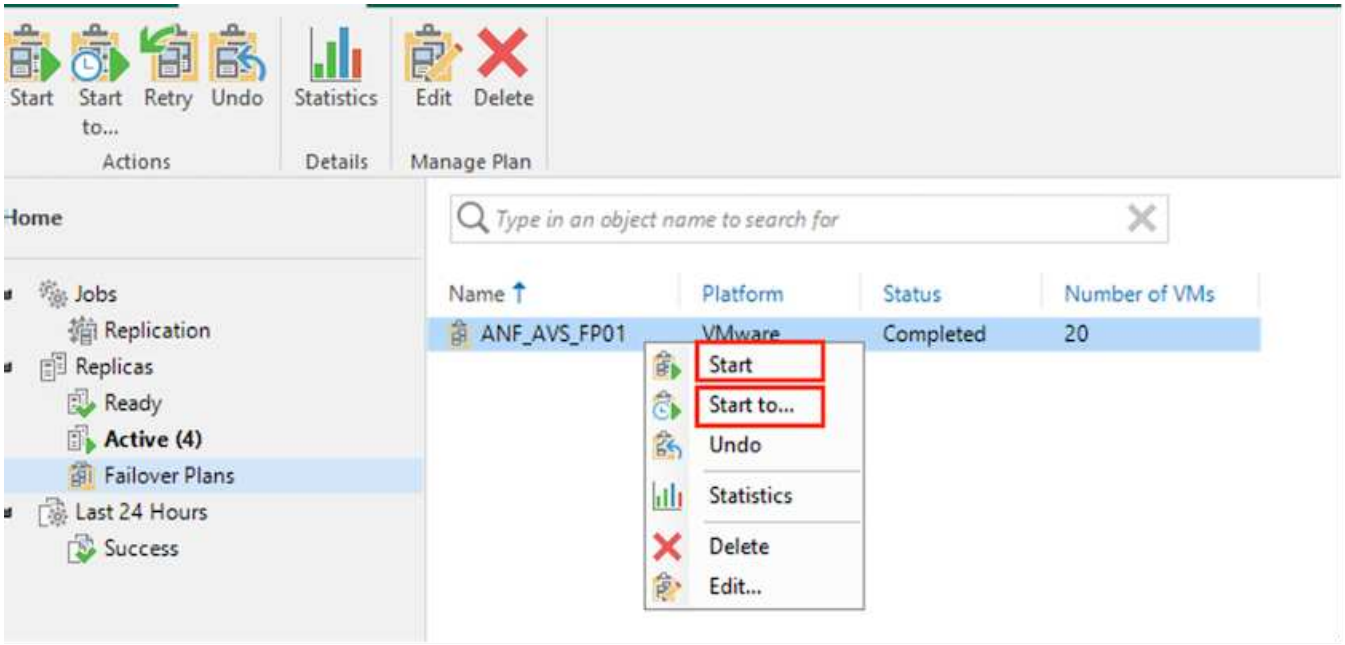
Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento"Creazione di processi di replicazione" .

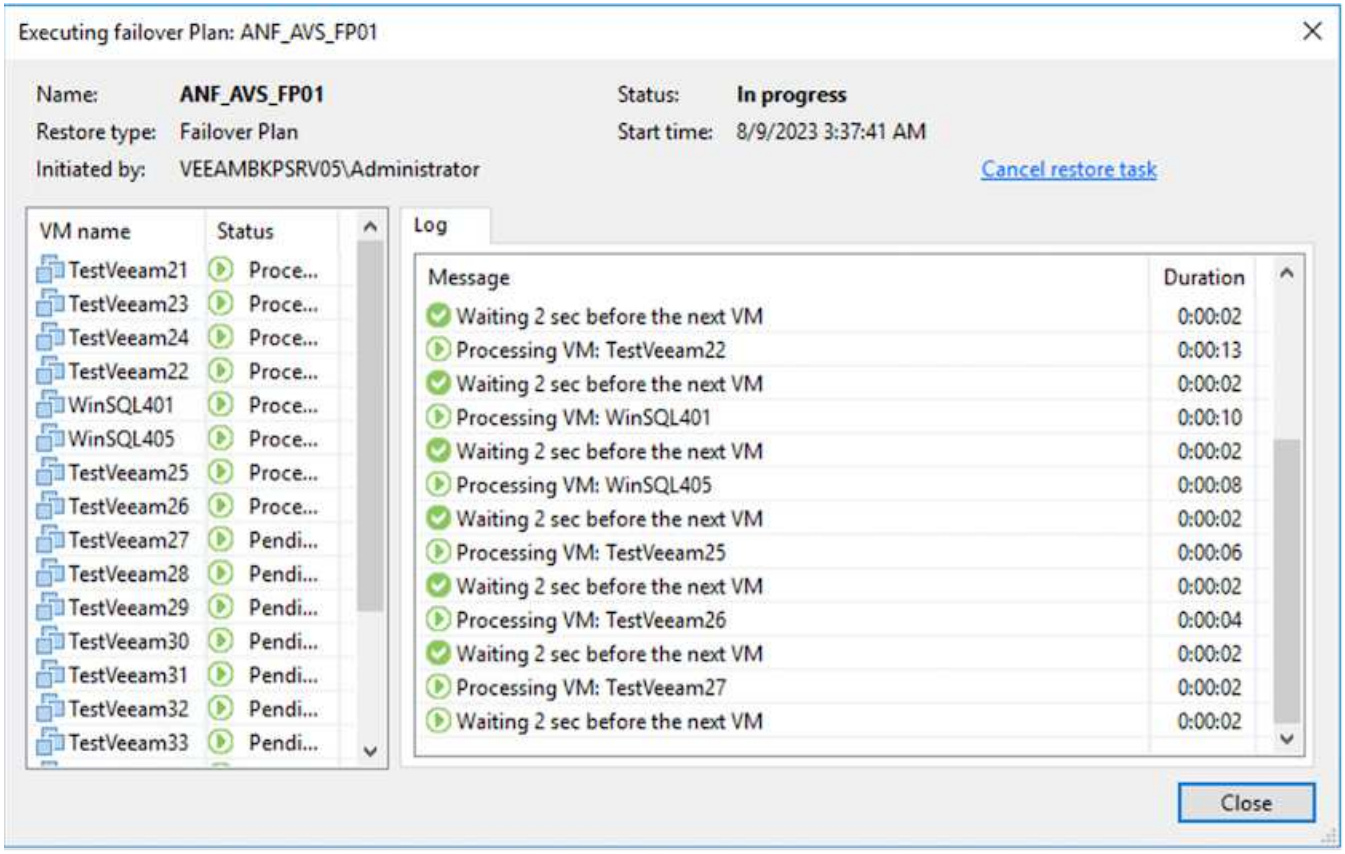
▼ **Passaggio 3: eseguire il piano di failover**

Durante il failover, la VM di origine nel sito di produzione viene commutata sulla sua 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 sua replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni 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 alle normali operazioni.

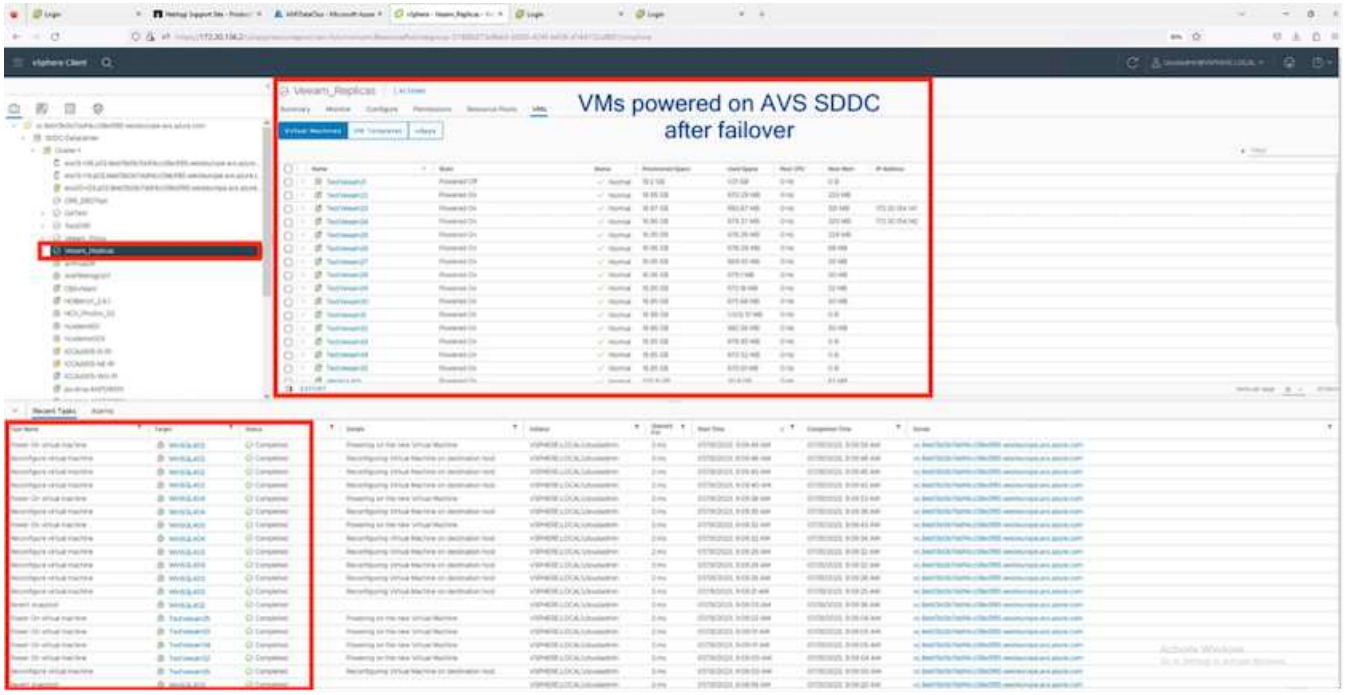
ⓘ Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante il failover.

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**. Verrà eseguito il failover utilizzando i punti di ripristino più recenti delle repliche delle VM. Per eseguire il failover su punti di ripristino specifici delle repliche delle VM, selezionare **Avvia su**.

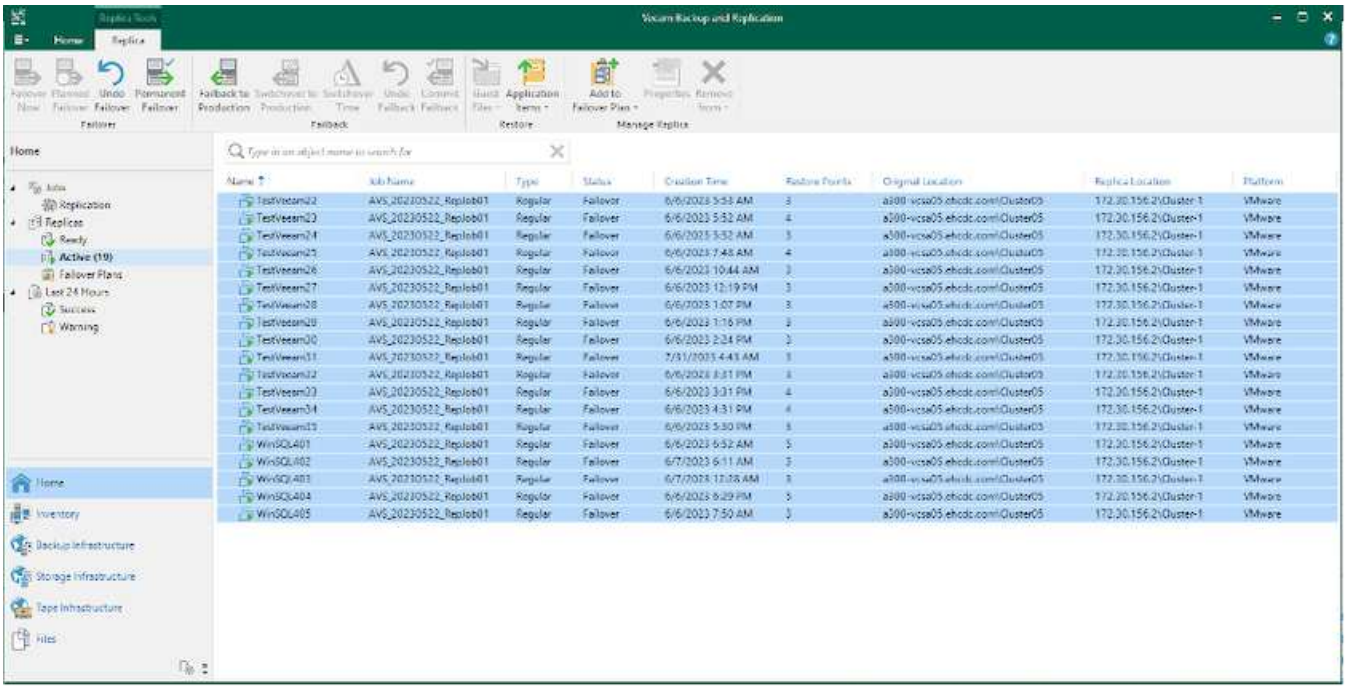




Lo stato della replica della VM cambia da Pronto a Failover e le VM verranno avviate sul cluster/host SDDC di Azure VMware Solution (AVS) di destinazione.



Una volta completato il failover, lo stato delle VM cambierà in "Failover".



Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine finché la sua replica non torna allo stato Pronto.

Per informazioni dettagliate sui piani di failover, fare riferimento"Piani di failover" .

▼ **Fase 4: failback al sito di produzione**

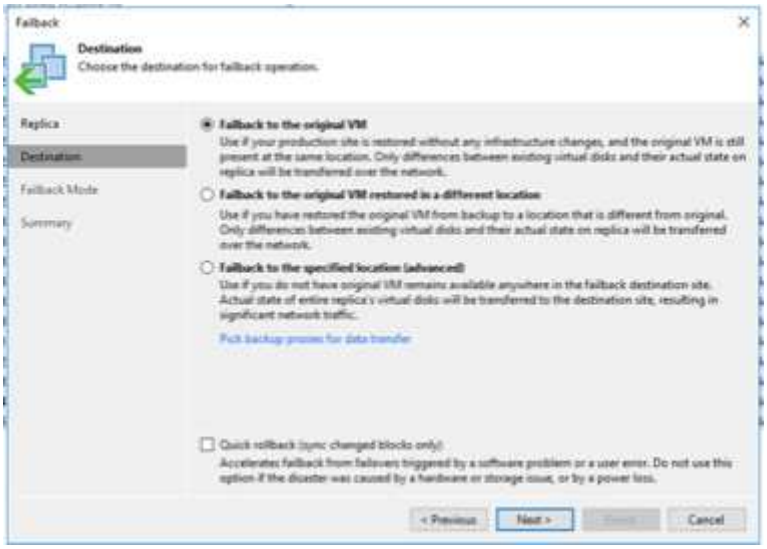
Quando il piano di failover è in esecuzione, viene considerato un passaggio intermedio e deve essere finalizzato in base ai requisiti. Le opzioni includono quanto segue:

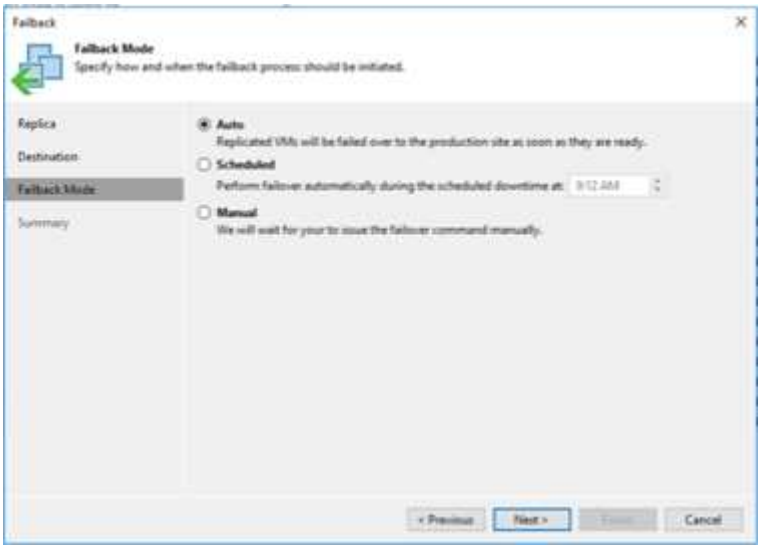
- **Failback in produzione**: torna alla VM originale e trasferisci tutte le modifiche apportate mentre la replica della VM era in esecuzione alla VM originale.

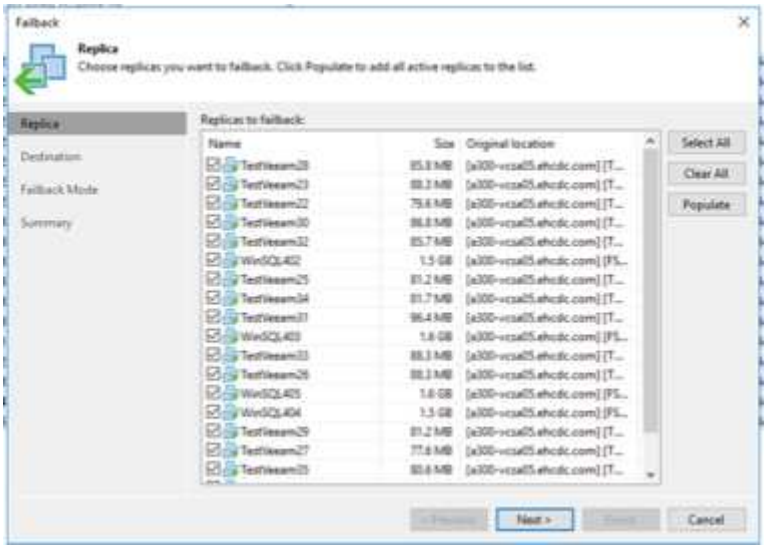
> Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Selezionare **Commit failback** (una volta confermato che la VM originale funziona come previsto) oppure Annulla failback per tornare alla replica della VM se la VM originale non funziona come previsto.

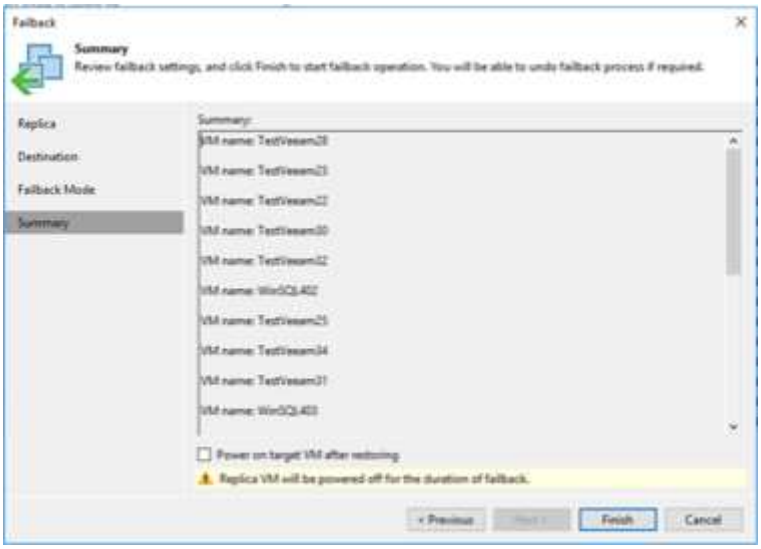
- **Annulla failover**: torna alla VM originale e ignora tutte le modifiche apportate alla replica della VM mentre era in esecuzione.
- **Failover permanente**: passa in modo permanente dalla VM originale a una replica della VM e utilizza questa replica come VM originale.

In questa demo è stato scelto il failback in produzione. Durante il passaggio Destinazione della procedura guidata è stato selezionato il failback sulla macchina virtuale originale ed è stata abilitata la casella di controllo "Accendi macchina virtuale dopo il ripristino".



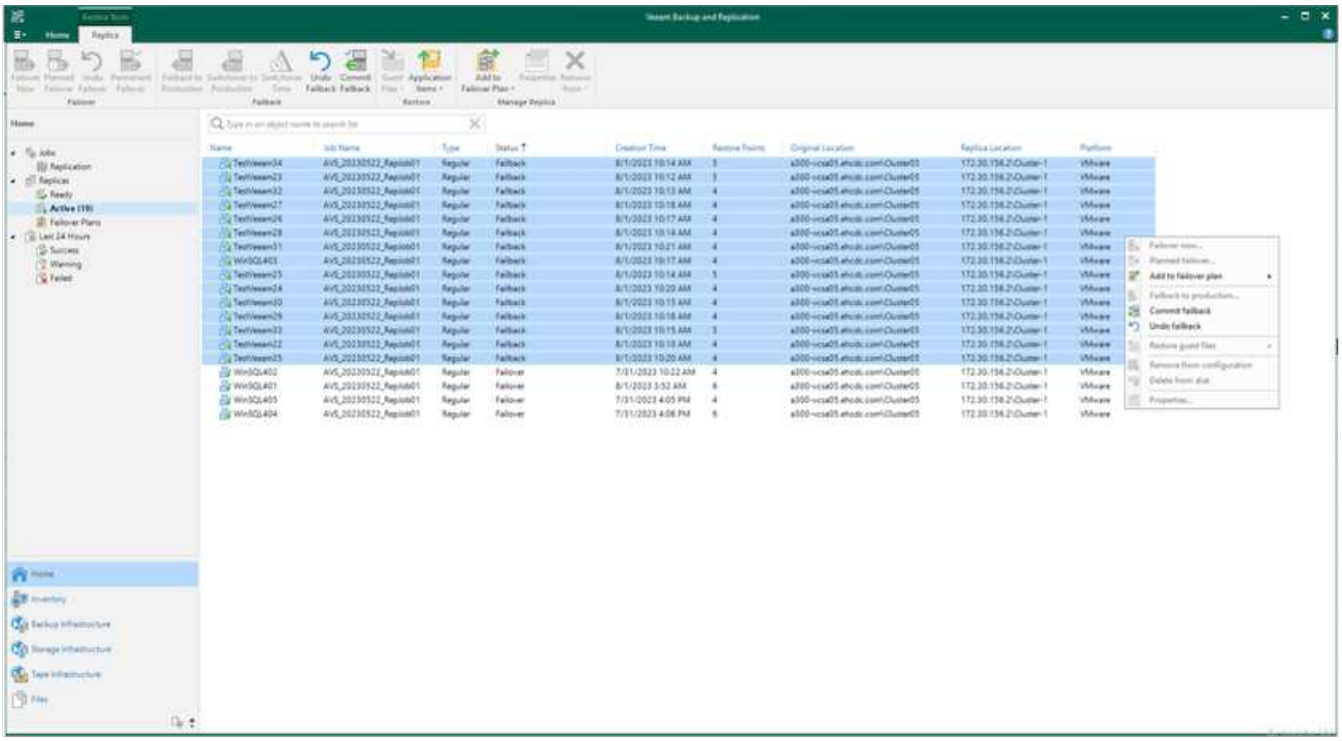




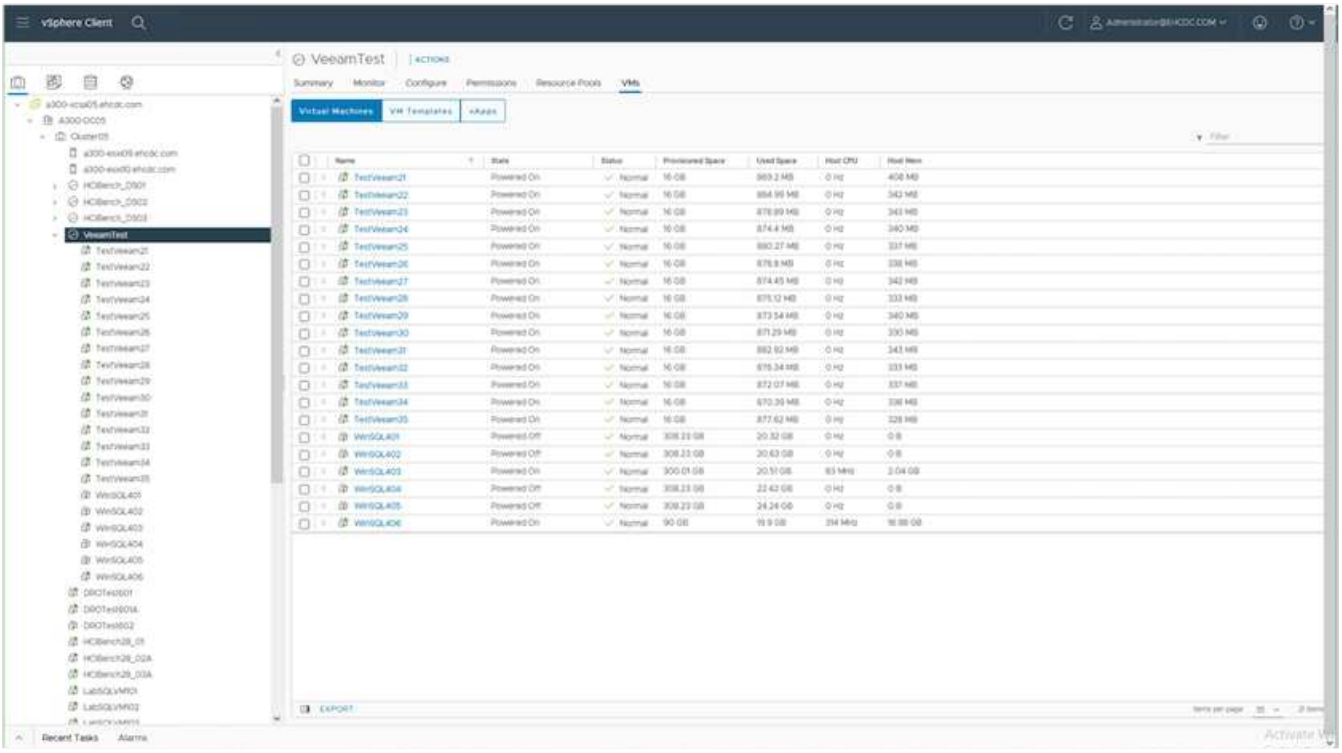


Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene eseguito, conferma che le modifiche inviate alla VM sottoposta a failback (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività 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 completato il failback in produzione, tutte le VM vengono ripristinate nel sito di produzione originale.



Conclusione

La funzionalità di datastore Azure NetApp Files consente a Veeam o a qualsiasi strumento di terze parti convalidato di fornire una soluzione DR a basso costo sfruttando i cluster Pilot Light anziché creare un cluster di grandi dimensioni solo per ospitare repliche di VM. Ciò fornisce un modo efficace per gestire un piano di disaster recovery personalizzato e su misura e per riutilizzare i prodotti di backup esistenti internamente per il

disaster recovery, consentendo il disaster recovery basato su cloud tramite l'uscita dai data center DR locali. In caso di emergenza è possibile effettuare il failover cliccando su un pulsante oppure effettuare il failover automaticamente se si verifica un'emergenza.

Per saperne di più su questo processo, non esitate a seguire il video tutorial 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 di Azure NetApp Files tramite VMware HCX - Guida introduttiva

Uno dei casi d'uso più comuni per la soluzione Azure VMware e il datastore Azure NetApp Files è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e fornisce vari meccanismi di migrazione per spostare macchine virtuali (VM) locali e i relativi dati negli archivi dati di Azure NetApp Files .

Panoramica: migrazione di macchine virtuali con VMware HCX, datastore Azure NetApp Files e soluzione Azure VMware

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento del carico di lavoro e persino la continuità aziendale tra i cloud. È incluso come parte di Azure VMware Solution Private Cloud e offre numerose modalità per migrare i carichi di lavoro e può essere utilizzato per operazioni di disaster recovery (DR).

Questo documento fornisce una guida dettagliata per il provisioning dell'archivio dati di Azure NetApp Files , seguito dal download, dalla distribuzione e dalla configurazione di VMware HCX, inclusi tutti i suoi componenti principali in locale e sul lato Azure VMware Solution, tra cui Interconnect, Network Extension e ottimizzazione WAN per abilitare vari meccanismi di migrazione delle VM.

> ⓘ VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione avviene a livello di VM. Pertanto, il presente documento è applicabile ai clienti NetApp esistenti e non NetApp che intendono distribuire Azure NetApp Files con Azure VMware Solution per una distribuzione cloud VMware conveniente.

▼ gradini di alto livello

Questo elenco fornisce i passaggi generali necessari per installare e configurare HCX Cloud Manager sul lato cloud di Azure e installare HCX Connector in locale:

1. Installare HCX tramite il portale di Azure.
2. Scarica e distribuisci il programma di installazione di HCX Connector Open Virtualization Appliance (OVA) nel VMware vCenter Server locale.
3. Attiva HCX con la chiave di licenza.
4. Associare VMware HCX Connector on-premise ad Azure VMware Solution HCX Cloud Manager.
5. Configurare il profilo di rete, il profilo di elaborazione e il service mesh.
6. (Facoltativo) Eseguire l'estensione di rete per evitare il re-IP durante le migrazioni.
7. Convalidare lo stato dell'appliance e assicurarsi che la migrazione sia possibile.
8. Migrare i carichi di lavoro delle VM.

▼ Prerequisiti

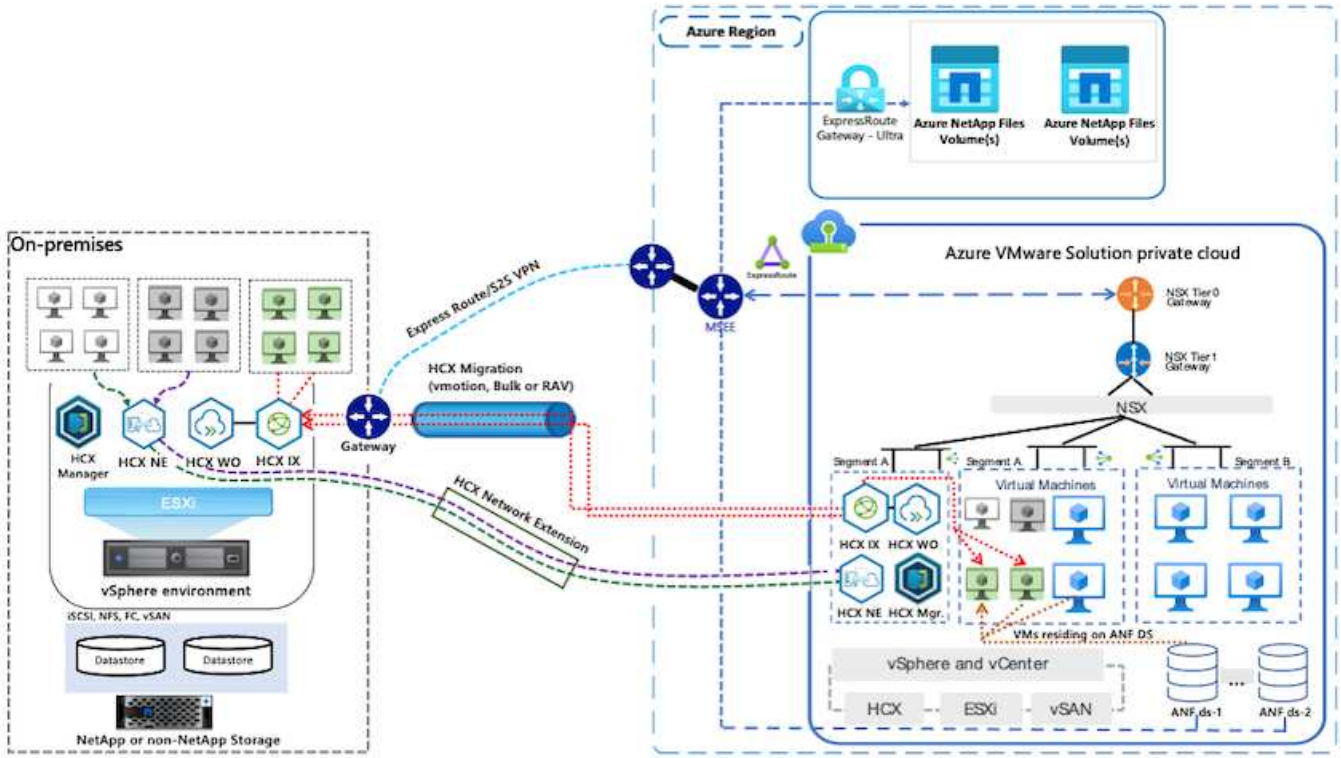
Prima di iniziare, assicurati che siano soddisfatti i seguenti prerequisiti. Per maggiori informazioni, vedere questo "collegamento" . Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando la chiave di licenza dal portale Azure VMware Solution. Dopo aver scaricato il programma di installazione OVA, procedere con il processo di installazione come descritto di seguito.

HCX Advanced è l'opzione predefinita, mentre VMware HCX Enterprise Edition è disponibile anche tramite ticket di supporto e supportata senza costi aggiuntivi.

- Utilizzare un data center software-defined (SDDC) di una soluzione VMware Azure esistente o creare un cloud privato utilizzando questo"Collegamento NetApp" o questo "Collegamento Microsoft" .
- La migrazione delle VM e dei dati associati dal data center locale abilitato per VMware vSphere richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, "impostare una connessione VPN da sito a sito o Express Route con portata globale" tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server locale al cloud privato Azure VMware Solution deve supportare la migrazione delle VM tramite vMotion.
- Assicurati che il necessario "regole e porte del firewall" sono consentiti per il traffico vMotion tra il vCenter Server locale e SDDC vCenter. Nel cloud privato, il routing sulla rete vMotion è configurato per impostazione predefinita.
- Il volume NFS Azure NetApp Files deve essere montato come archivio dati nella soluzione Azure VMware. Seguire i passaggi dettagliati in questo "collegamento" per collegare gli archivi dati di Azure NetApp Files agli host di Azure VMware Solutions.

▼ Architettura di alto livello

A scopo di test, l'ambiente di laboratorio locale utilizzato per questa convalida è stato connesso tramite una VPN da sito a sito, che consente la connettività locale ad Azure VMware Solution.



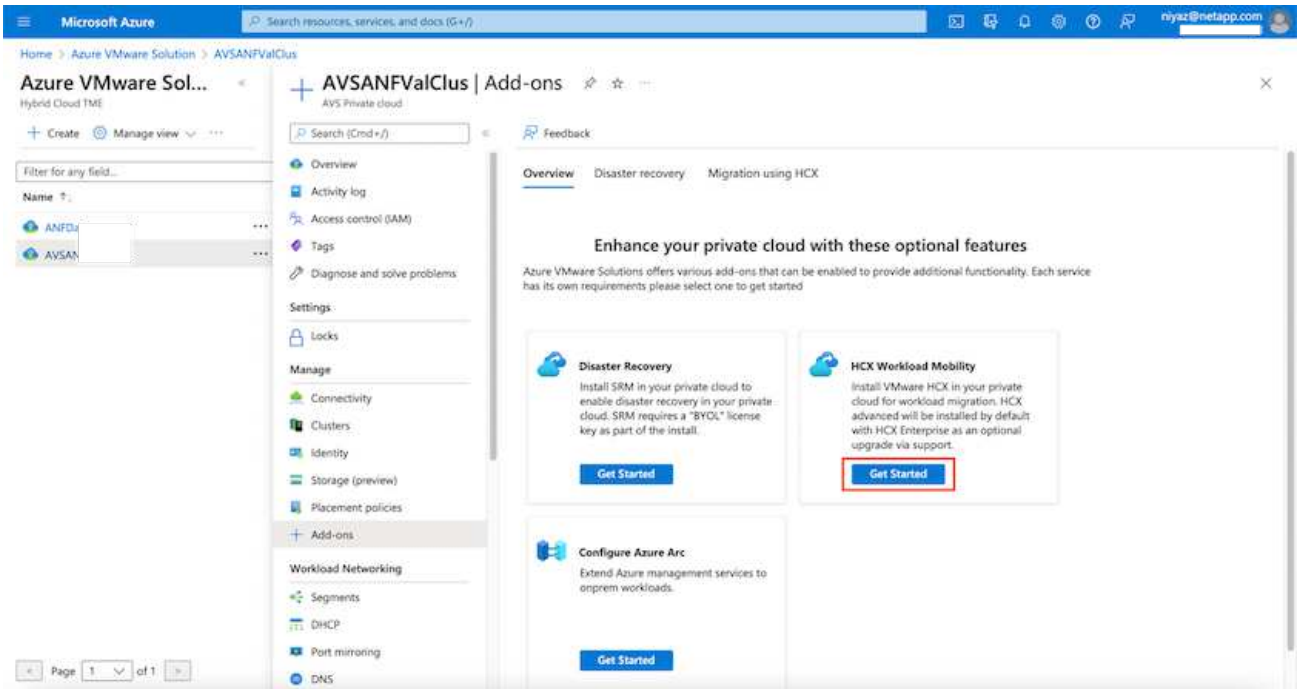
Distribuzione della soluzione

Per completare l'implementazione di questa soluzione, seguire la serie di passaggi:

▼ **Passaggio 1: installare HCX tramite il portale di Azure utilizzando l'opzione Componenti aggiuntivi**

Per eseguire l'installazione, completare i seguenti passaggi:

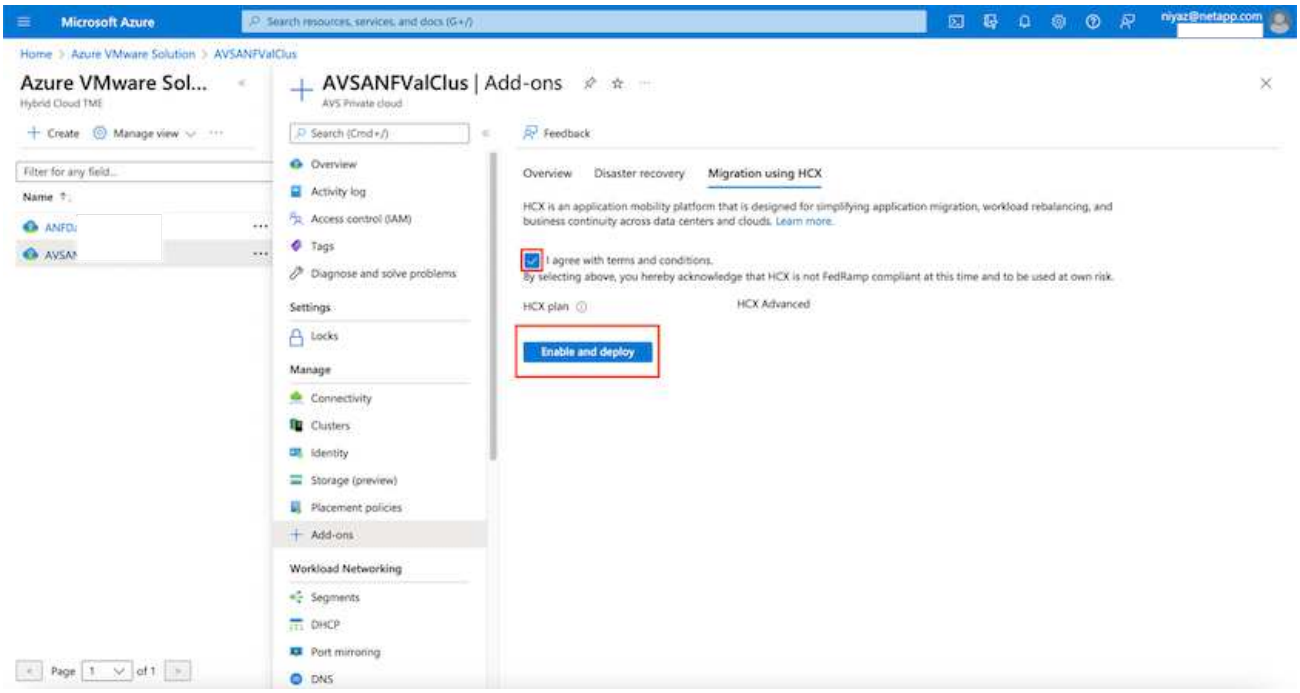
1. Accedi al portale di Azure e accedi al cloud privato della soluzione Azure VMware.
2. Seleziona il cloud privato appropriato e accedi ai componenti aggiuntivi. Per farlo, andare su **Gestisci > Componenti aggiuntivi**.
3. Nella sezione HCX Workload Mobility, fare clic su **Inizia**.



4. Seleziona l'opzione **Accetto i termini e le condizioni** e fai clic su **Abilita e distribuisci**.

> La distribuzione predefinita è HCX Advanced. Apri una richiesta di supporto per abilitare l'edizione Enterprise.

> L'implementazione richiede circa 25-30 minuti.



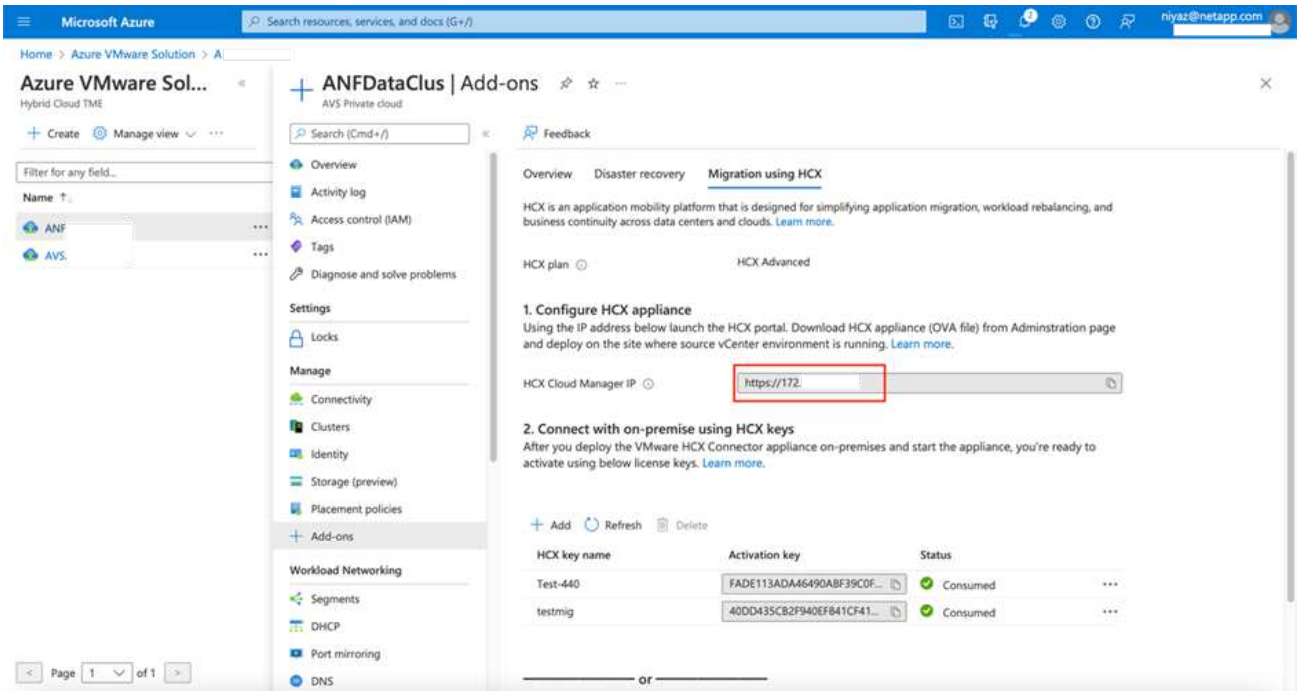
▼ **Passaggio 2: distribuire l'OVA del programma di installazione nel vCenter Server locale**

Per consentire al connettore locale di connettersi a HCX Manager in Azure VMware Solution, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente locale.

Per scaricare e installare HCX Connector nel vCenter Server locale, completare i seguenti passaggi:

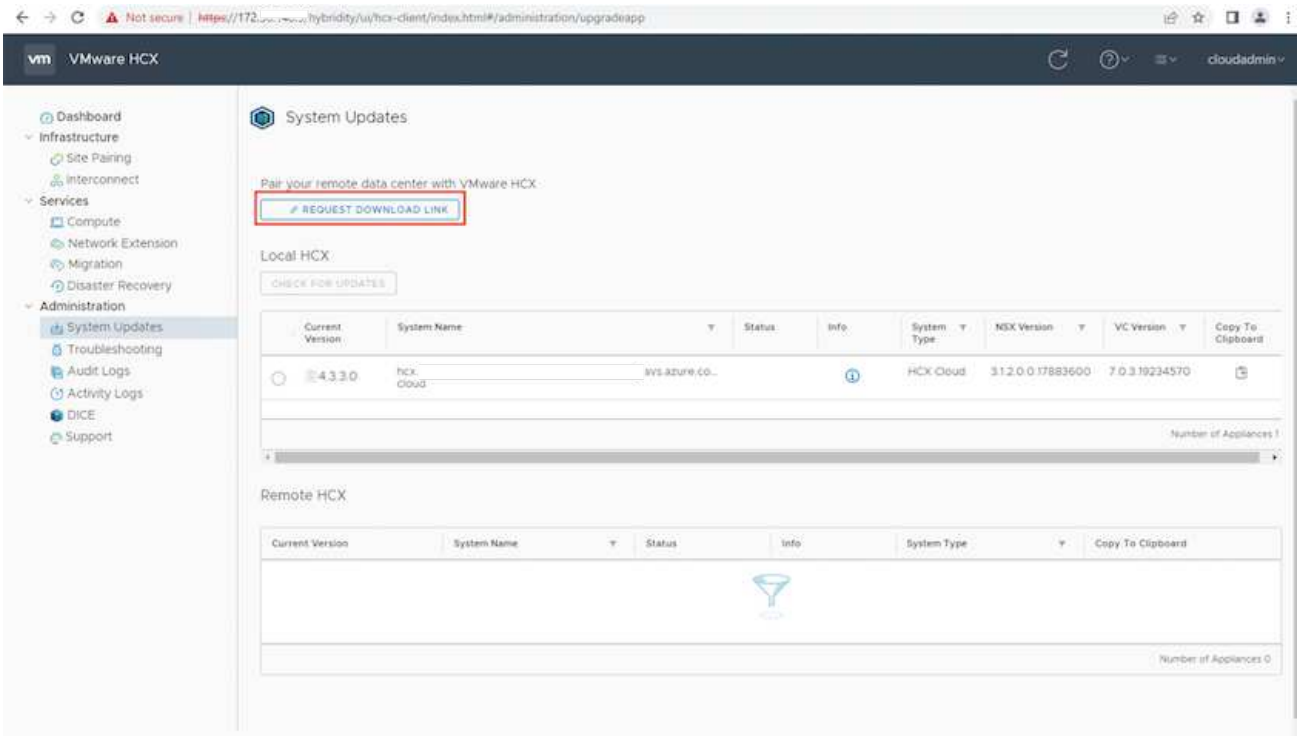
1. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato, quindi seleziona **Gestisci > Componenti aggiuntivi > Migrazione** utilizzando HCX e copia il portale HCX Cloud Manager per scaricare il file OVA.

   Utilizzare le credenziali utente CloudAdmin predefinite per accedere al portale HCX.

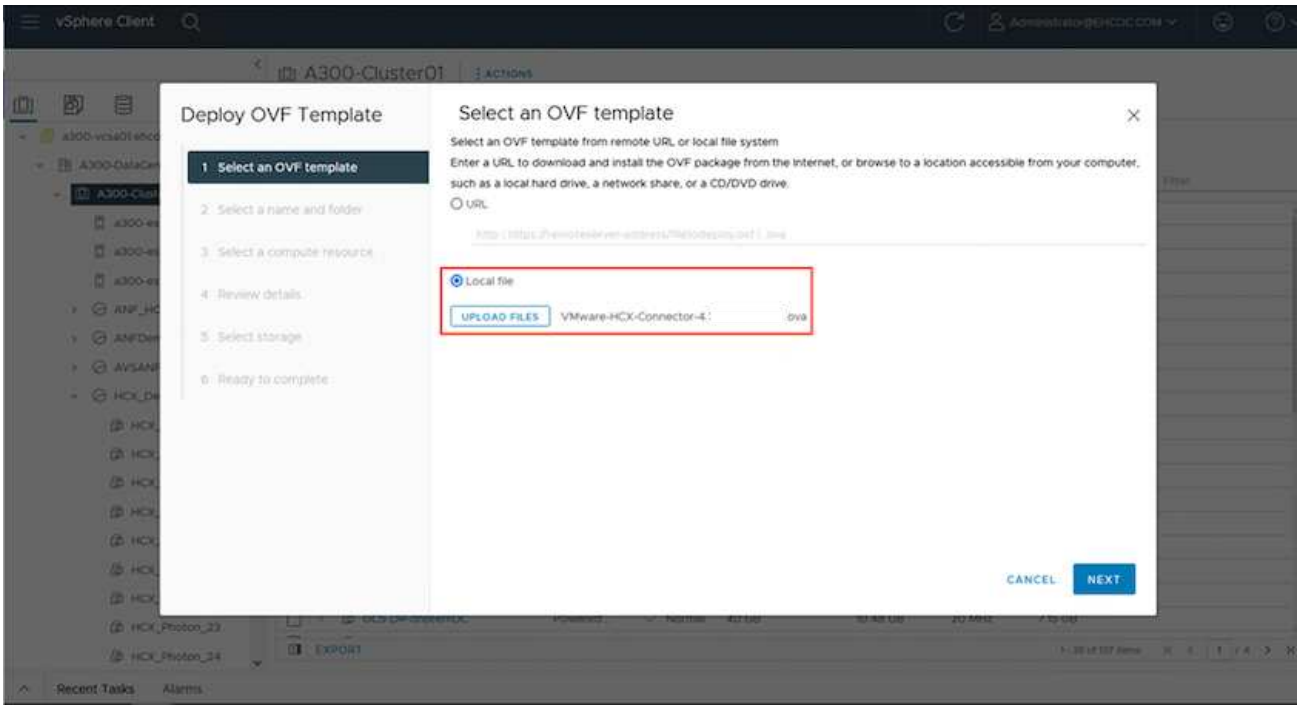


2. Dopo aver effettuato l'accesso al portale HCX con cloudadmin@vsphere.local utilizzando jumphost, vai su **Amministrazione > Aggiornamenti di sistema** e fai clic su **Richiedi collegamento per il download**.

> Scarica o copia il collegamento all'OVA e incollalo in un browser per avviare il processo di download del file OVA di VMware HCX Connector da distribuire sul vCenter Server locale.



3. Dopo aver scaricato l'OVA, distribuiscilo nell'ambiente VMware vSphere locale utilizzando l'opzione **Distribuisci modello OVF**.



4. Immettere tutte le informazioni richieste per la distribuzione OVA, fare clic su **Avanti**, quindi su **Fine** per distribuire il connettore VMware HCX OVA.

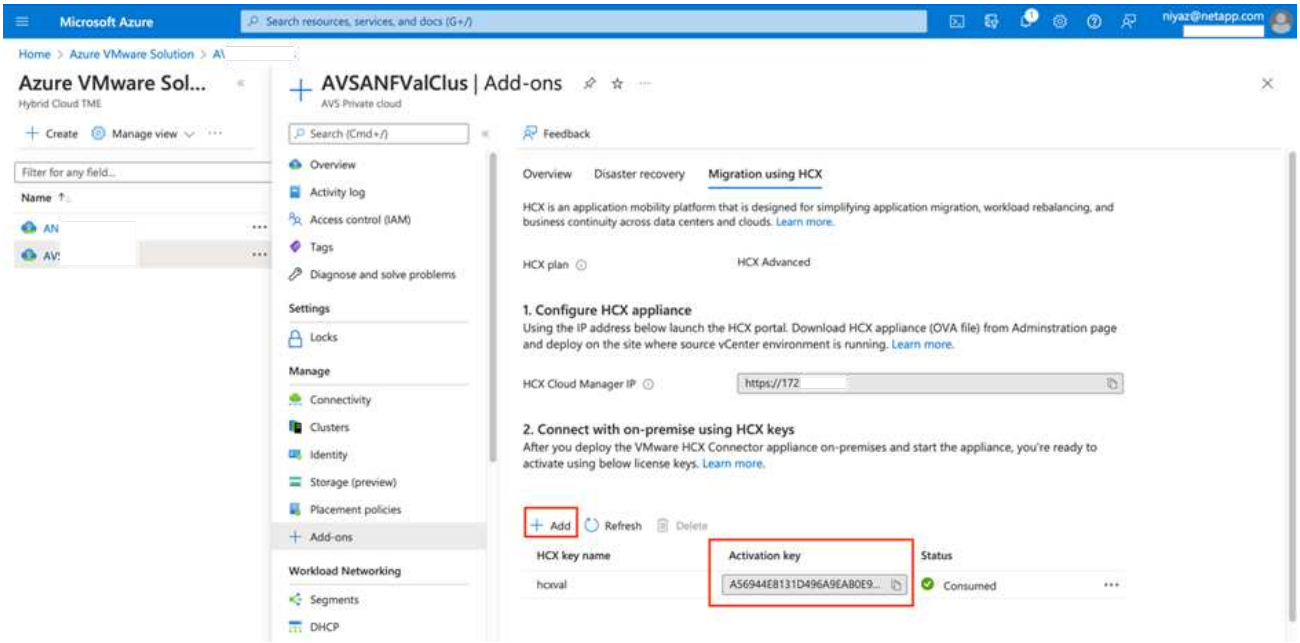
   Accendere manualmente l'appliance virtuale.

Per istruzioni dettagliate, vedere il "Guida utente VMware HCX" .

▼ **Passaggio 3: Attiva HCX Connector con la chiave di licenza**

Dopo aver distribuito VMware HCX Connector OVA in locale e avviato l'appliance, completare i seguenti passaggi per attivare HCX Connector. Generare la chiave di licenza dal portale Azure VMware Solution e attivarla in VMware HCX Manager.

1. Dal portale di Azure, vai alla soluzione Azure VMware, seleziona il cloud privato e seleziona **Gestisci > Componenti aggiuntivi > Migrazione tramite HCX**.
2. In **Connetti con locale tramite chiavi HCX**, fai clic su **Aggiungi** e copia la chiave di attivazione.



   Per ogni HCX Connector on-premise distribuito è richiesta una chiave separata.

3. Accedi a VMware HCX Manager on-premise all'indirizzo `"https://hcxmanagerIP:9443"` utilizzando le credenziali di amministratore.

   Utilizzare la password definita durante la distribuzione OVA.

4. Nella licenza, inserisci la chiave copiata dal passaggio 3 e clicca su **Attiva**.

   L'HCX Connector locale deve avere accesso a Internet.

5. In **Posizione del data center**, indicare la posizione più vicina per l'installazione di VMware HCX Manager in locale. Fare clic su **Continua**.
6. In **Nome sistema**, aggiorna il nome e fai clic su **Continua**.
7. Fare clic su **Sì, continua**.

8. In **Connetti il tuo vCenter**, fornisci il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fai clic su **Continua**.

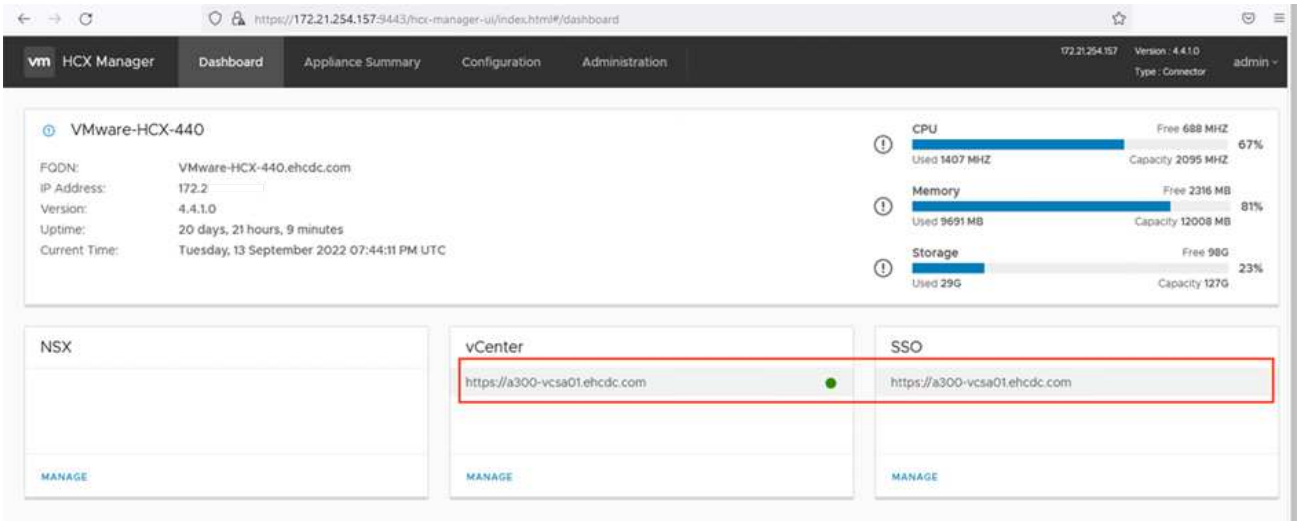
   Utilizzare l'FQDN per evitare problemi di connettività in seguito.

9. In **Configura SSO/PSC**, fornire l'FQDN o l'indirizzo IP del Platform Services Controller e fare clic su **Continua**.

   Immettere l'FQDN o l'indirizzo IP di VMware vCenter Server.

10. Verificare che le informazioni immesse siano corrette e fare clic su **Riavvia**.
11. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata. Sia vCenter Server che SSO devono disporre dei parametri di configurazione appropriati, che dovrebbero essere gli stessi della pagina precedente.

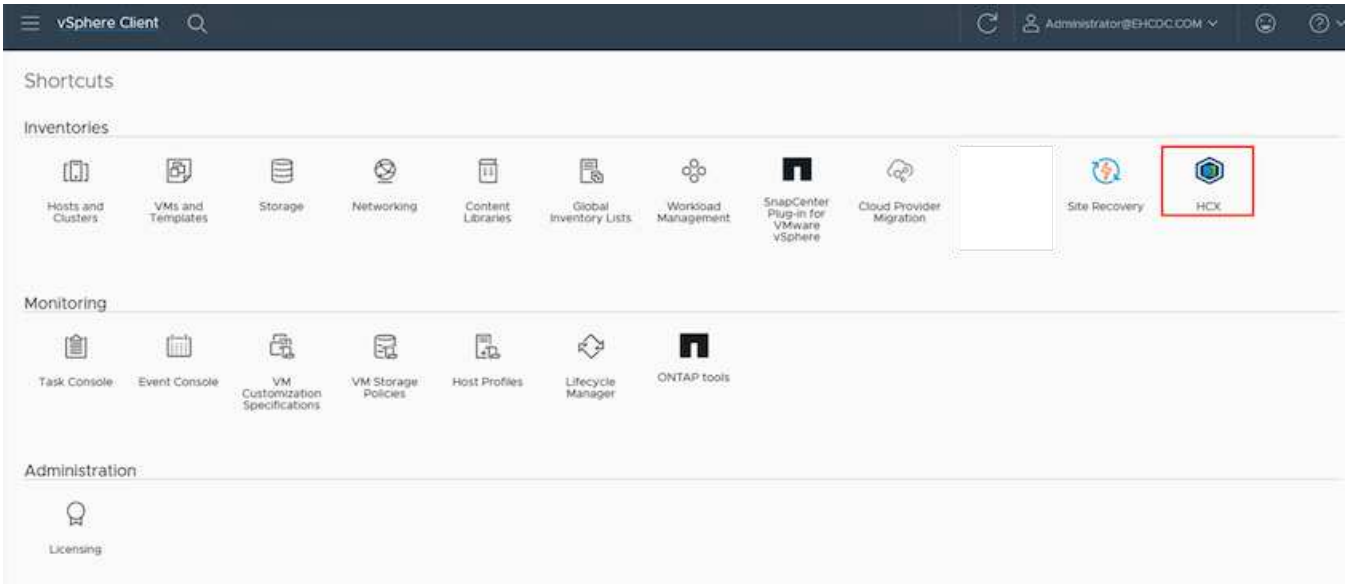
    Questo processo dovrebbe richiedere circa 10-20 minuti affinché il plug-in venga aggiunto al vCenter Server.



▼ **Passaggio 4: associare VMware HCX Connector locale ad Azure VMware Solution HCX Cloud Manager**

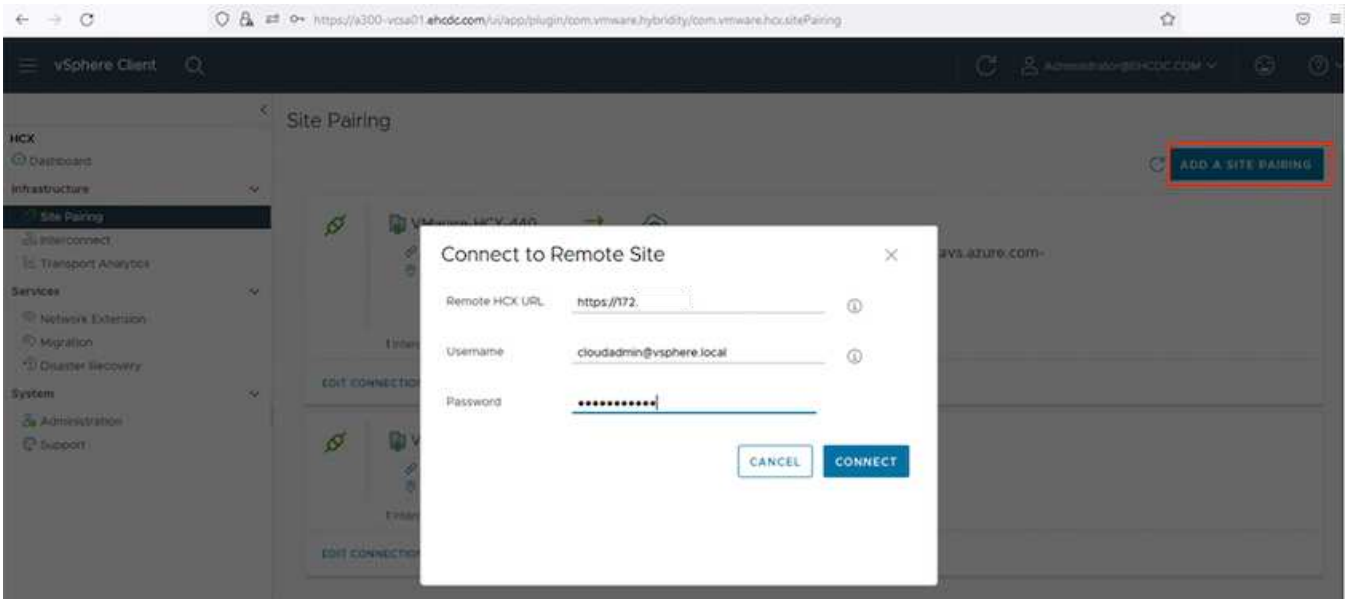
Dopo aver installato HCX Connector sia in locale che in Azure VMware Solution, configurare VMware HCX Connector locale per il cloud privato Azure VMware Solution aggiungendo l'associazione. Per configurare l'associazione dei siti, completare i seguenti passaggi:

1. Per creare una coppia di siti tra l'ambiente vCenter locale e Azure VMware Solution SDDC, accedere al vCenter Server locale e utilizzare il nuovo plug-in HCX vSphere Web Client.



1. In Infrastruttura, fare clic su **Aggiungi un'associazione di siti**.

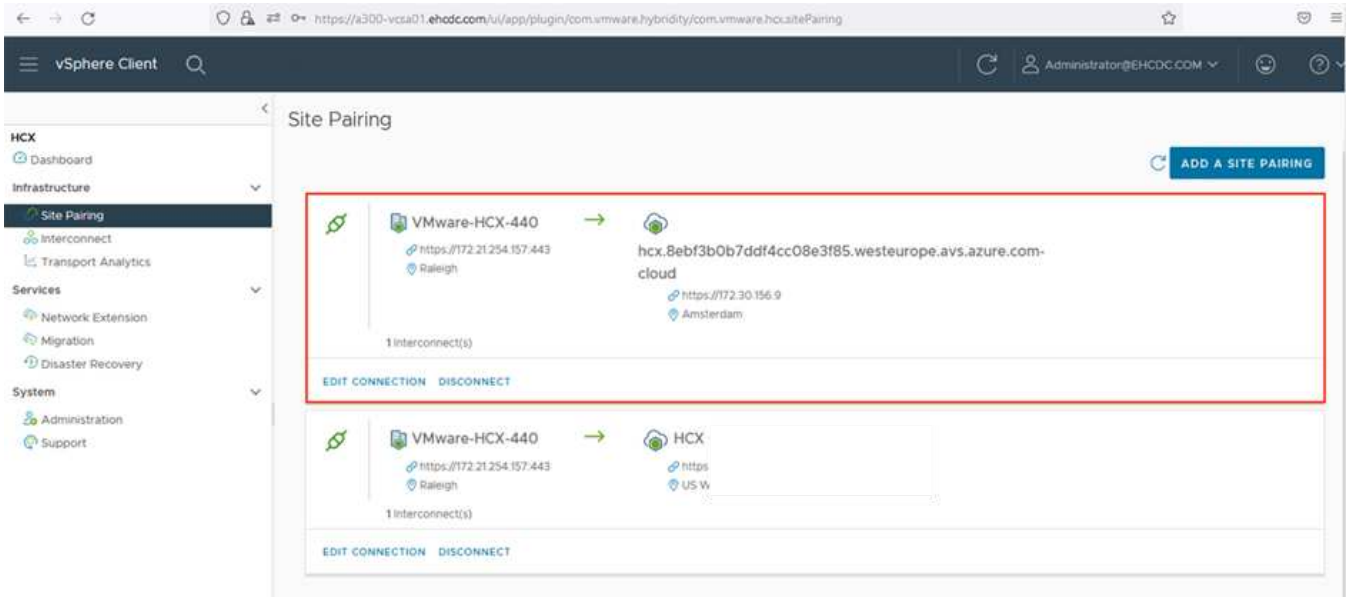
Immettere l'URL o l'indirizzo IP di Azure VMware Solution HCX Cloud Manager e le credenziali per il ruolo CloudAdmin per accedere al cloud privato.



1. Fare clic su **Connetti**.

VMware HCX Connector deve essere in grado di indirizzare all'IP di HCX Cloud Manager tramite la porta 443.

1. Dopo aver creato l'associazione, l'associazione del sito appena configurata è disponibile sulla dashboard HCX.

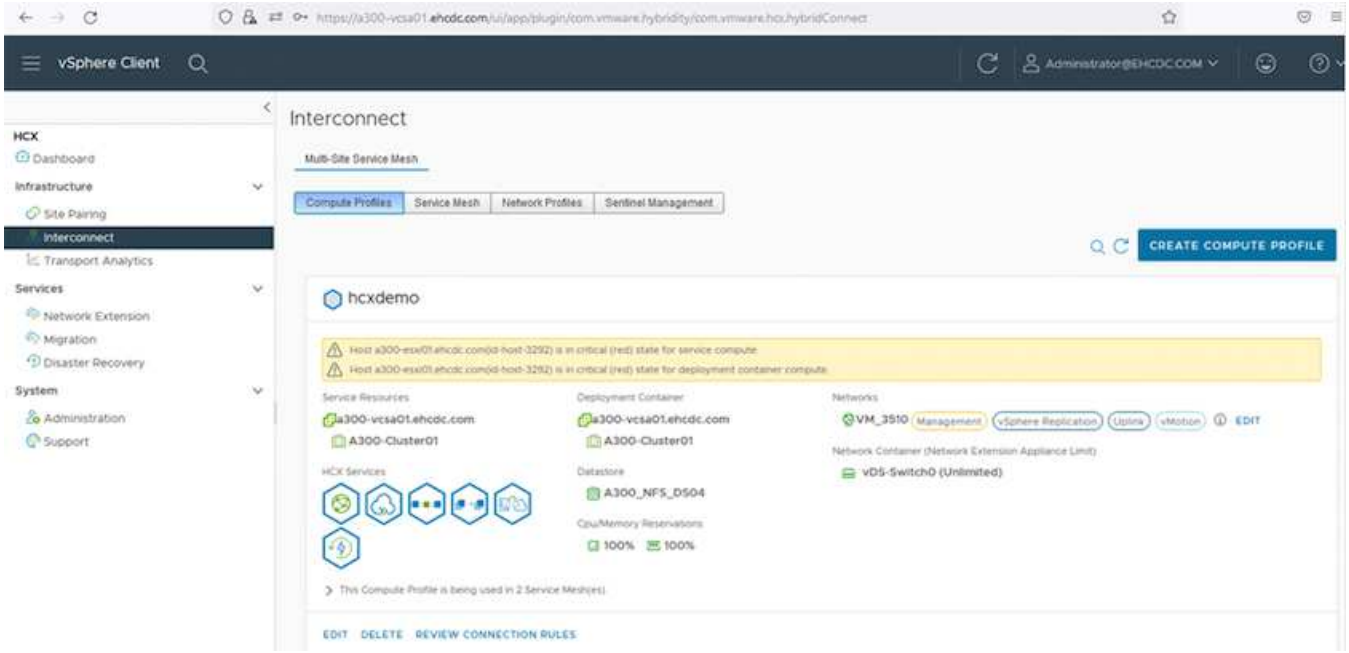


▼ **Passaggio 5: configurare il profilo di rete, il profilo di elaborazione e il service mesh**

L'appliance di servizi VMware HCX Interconnect fornisce funzionalità di replicazione e migrazione basate su vMotion tramite Internet e connessioni private al sito di destinazione. L'interconnessione fornisce crittografia, ingegneria del traffico e mobilità delle VM. Per creare un'appliance di servizi Interconnect, completare i seguenti passaggi:

1. In Infrastruttura, seleziona **Interconnessione > Multi-Site Service Mesh > Profili di calcolo > Crea profilo di calcolo**.

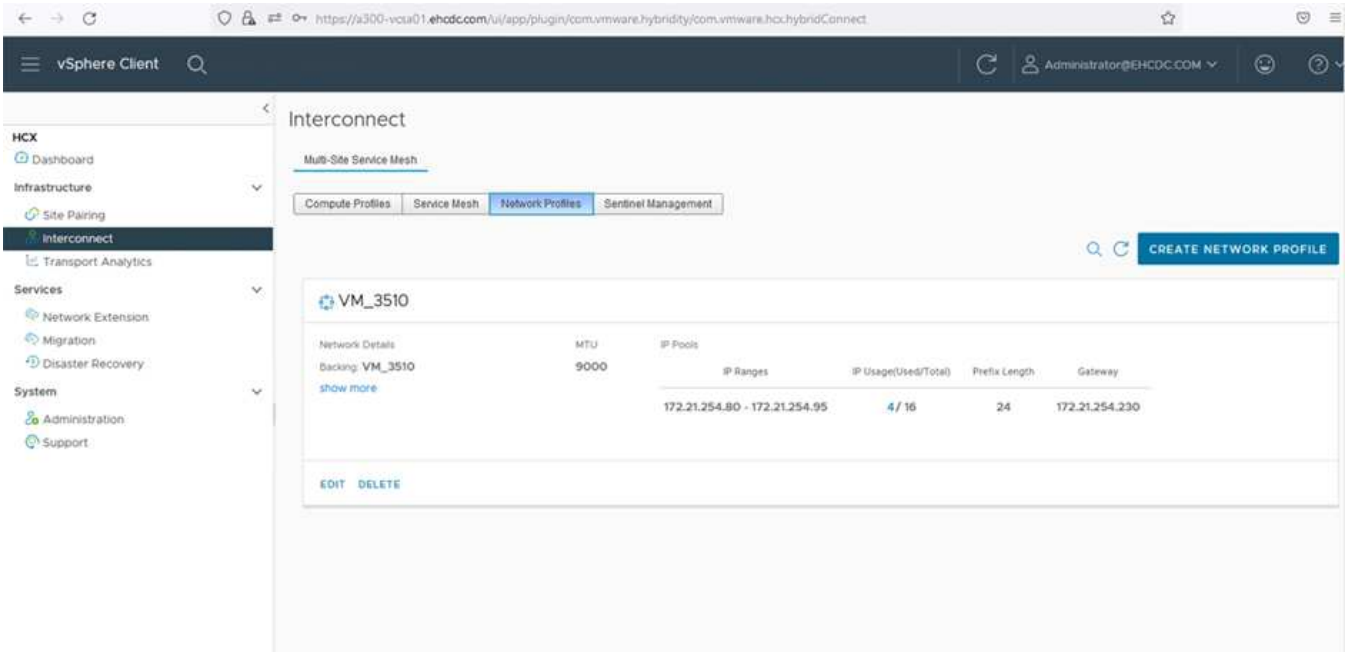
I profili di calcolo definiscono i parametri di distribuzione, tra cui gli apparecchi distribuiti e la parte del data center VMware accessibile al servizio HCX.



1. Dopo aver creato il profilo di calcolo, creare i profili di rete selezionando **Multi-Site Service Mesh > Profili di rete > Crea profilo di rete**.

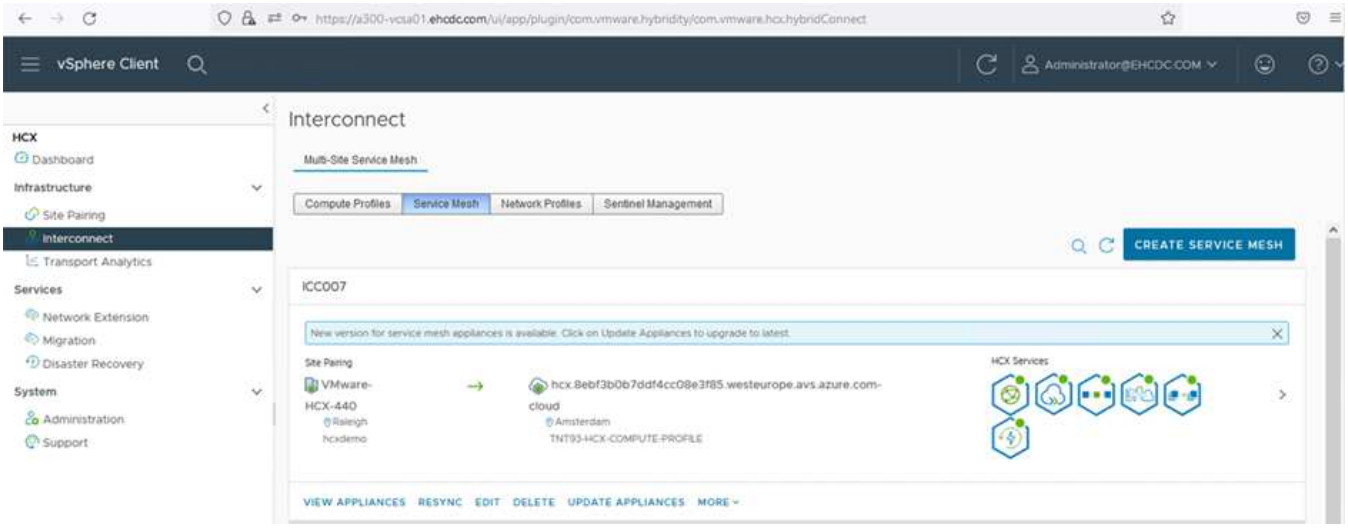
Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati da HCX per i suoi dispositivi virtuali.

Per questo passaggio sono necessari due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione agli Interconnect Appliance.



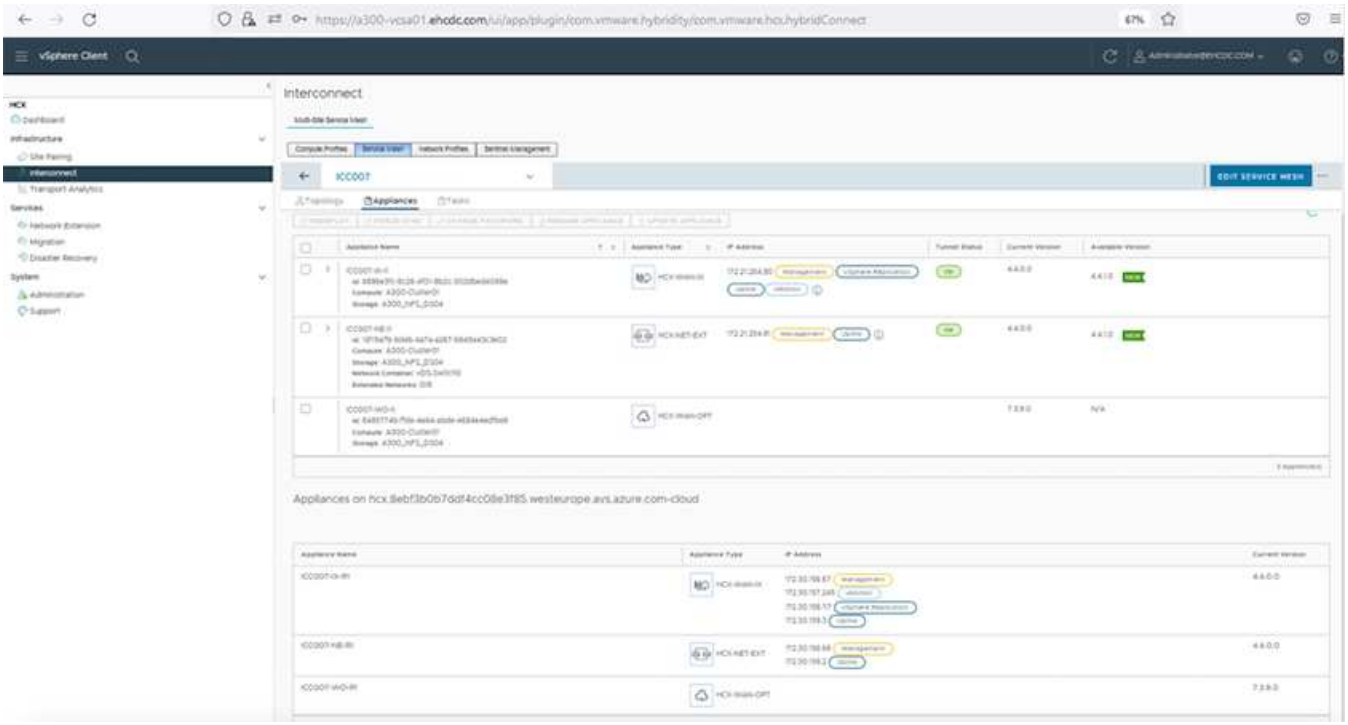
1. Al momento, i profili di calcolo e di rete sono stati creati correttamente.
2. Creare Service Mesh selezionando la scheda **Service Mesh** nell'opzione **Interconnessione** e selezionare i siti locali e Azure SDDC.
3. Service Mesh specifica una coppia di profili di rete e di elaborazione locali e remoti.

Come parte di questo processo, gli appliance HCX vengono distribuiti e configurati automaticamente sia sul sito di origine che su quello di destinazione per creare un fabric di trasporto sicuro.



1. Questo è il passaggio finale della configurazione. Il completamento dell'implementazione dovrebbe richiedere circa 30 minuti. Dopo aver configurato il service mesh, l'ambiente è pronto con i tunnel IPsec

creati correttamente per migrare le VM del carico di lavoro.



▼ **Fase 6: Migrazione dei carichi di lavoro**

I carichi di lavoro possono essere migrati in modo bidirezionale tra ambienti SDDC locali e Azure utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso entità attivate da VMware HCX utilizzando più tecnologie di migrazione, quali migrazione in blocco HCX, HCX vMotion, migrazione a freddo HCX, HCX Replication Assisted vMotion (disponibile con l'edizione HCX Enterprise) e migrazione assistita del sistema operativo HCX (disponibile con l'edizione HCX Enterprise).

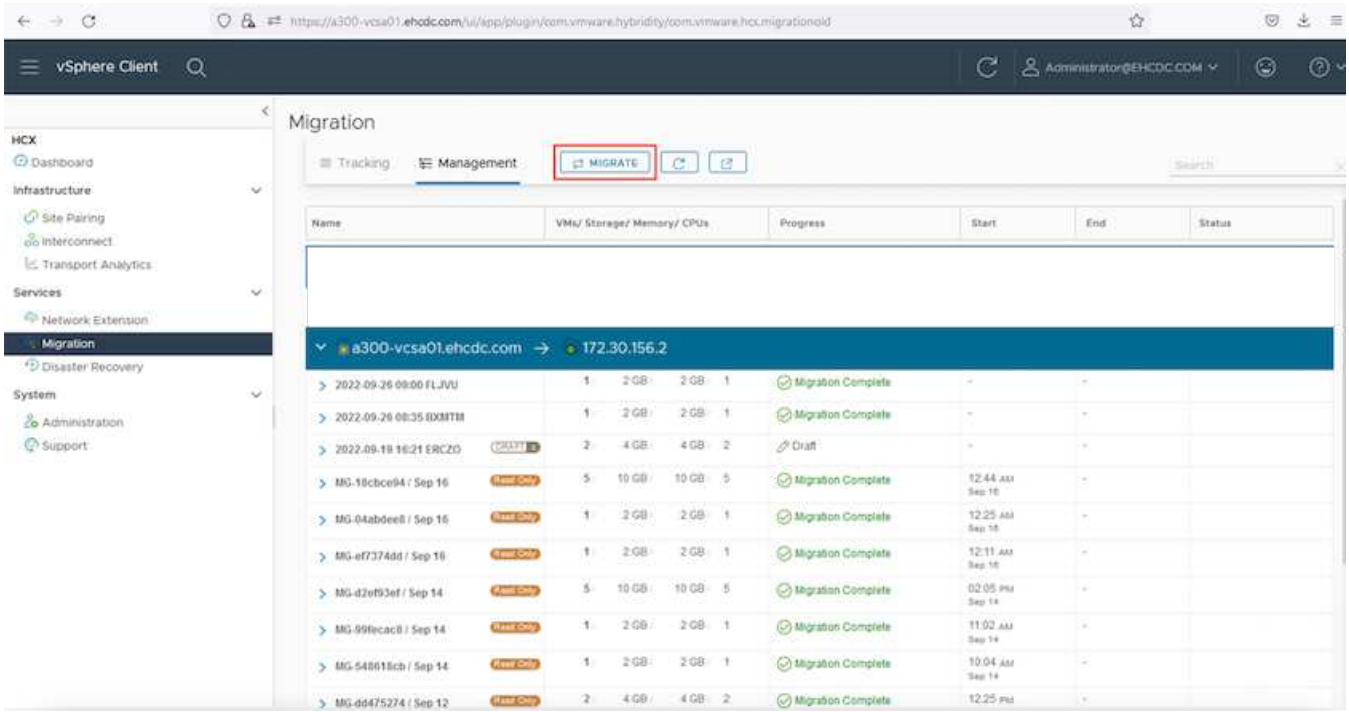
Per saperne di più sui vari meccanismi di migrazione HCX, vedere "Tipi di migrazione VMware HCX" .

Migrazione in blocco

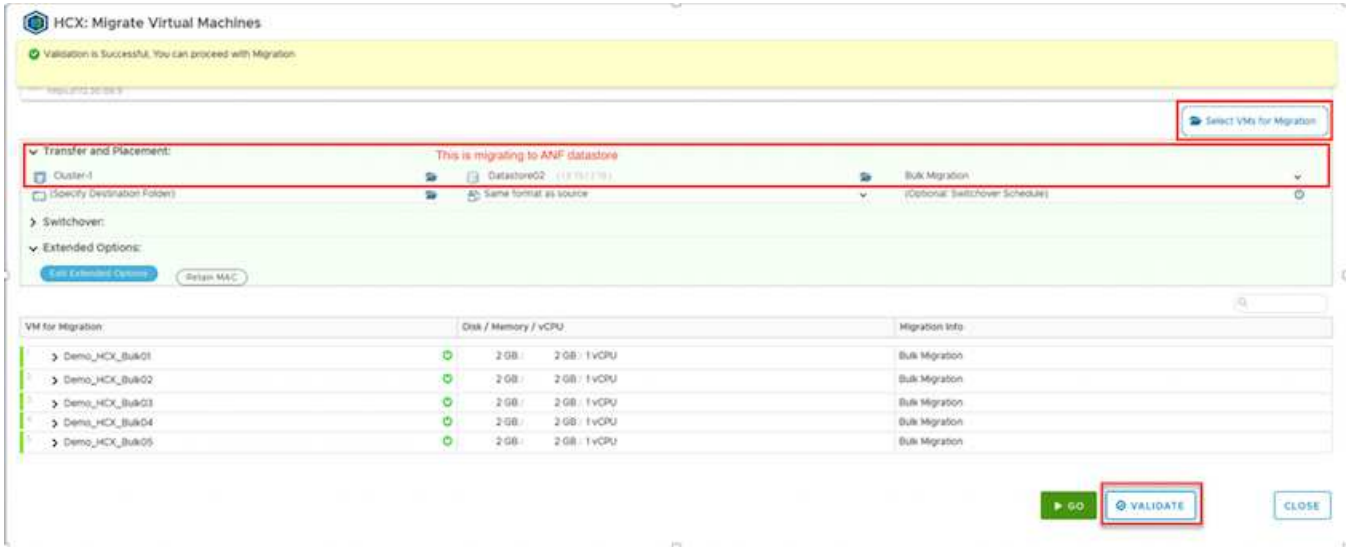
Questa sezione descrive in dettaglio il meccanismo di migrazione in blocco. Durante una migrazione in blocco, la funzionalità di migrazione in blocco di HCX utilizza vSphere Replication per migrare i file del disco ricreando al contempo la VM sull'istanza vSphere HCX di destinazione.

Per avviare migrazioni di VM in blocco, completare i seguenti passaggi:

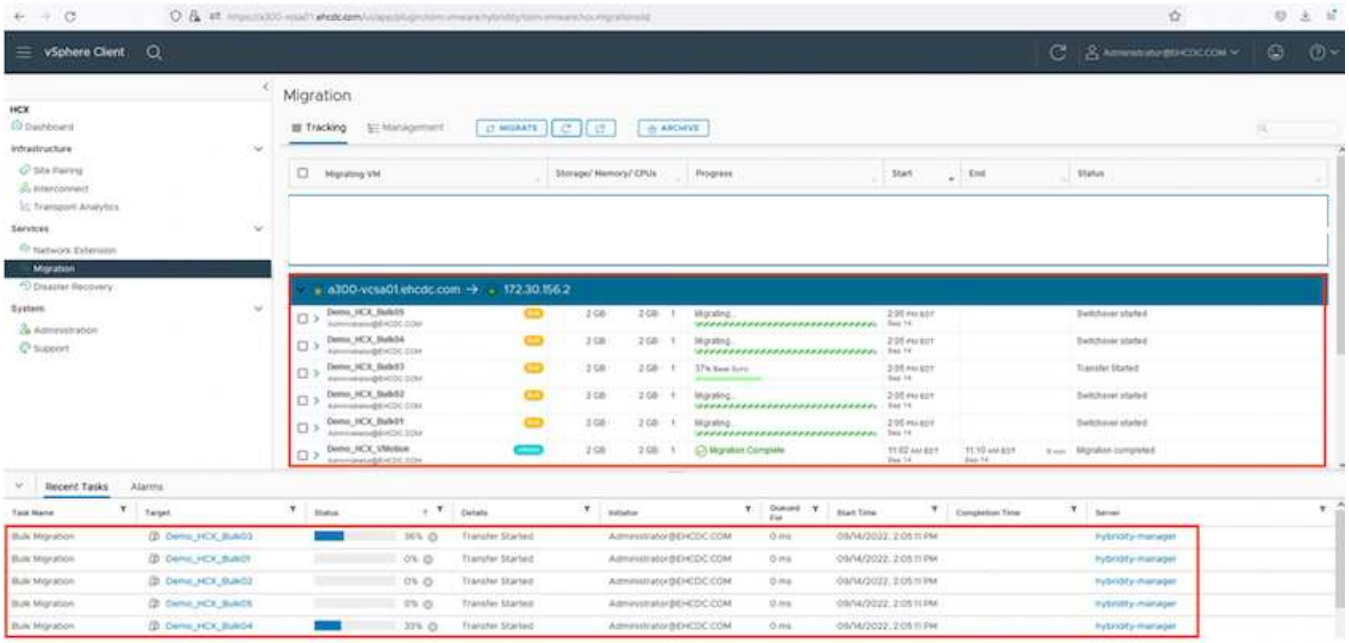
1. Accedi alla scheda **Migra** in **Servizi > Migrazione**.



1. In **Connessione al sito remoto**, seleziona la connessione al sito remoto e seleziona l'origine e la destinazione. In questo esempio, la destinazione è l'endpoint SDDC HCX della soluzione Azure VMware.
2. Fare clic su **Seleziona VM per la migrazione**. Fornisce un elenco di tutte le VM locali. Selezionare le VM in base all'espressione match:value e fare clic su **Aggiungi**.
3. Nella sezione **Trasferimento e posizionamento**, aggiorna i campi obbligatori (**Cluster**, **Archiviazione**, **Destinazione** e **Rete**), incluso il profilo di migrazione, e fai clic su **Convalida**.

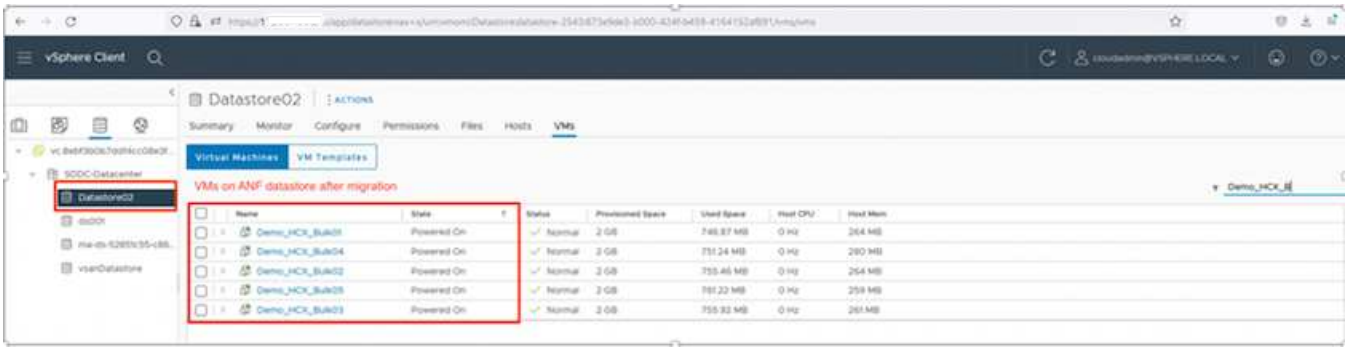


1. Una volta completati i controlli di convalida, fare clic su **Vai** per avviare la migrazione.



Durante questa migrazione, viene creato un disco segnaposto sul datastore di Azure NetApp Files specificato all'interno del vCenter di destinazione per consentire la replica dei dati del disco della macchina virtuale di origine sui dischi segnaposto. HBR viene attivato per una sincronizzazione completa con la destinazione e, una volta completata la baseline, viene eseguita una sincronizzazione incrementale in base al ciclo RPO (Recovery Point Objective). Una volta completata la sincronizzazione completa/incrementale, il passaggio viene attivato automaticamente, a meno che non venga impostata una pianificazione specifica.

1. Una volta completata la migrazione, convalidarla accedendo al vCenter SDDC di destinazione.

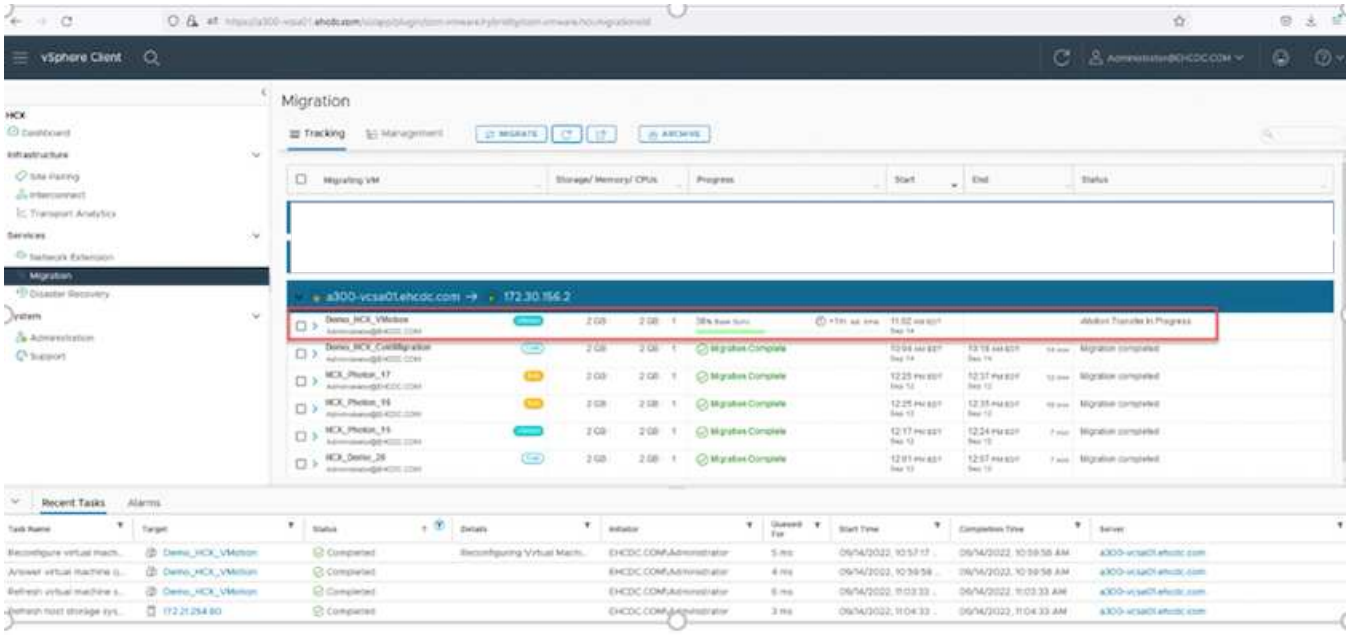


Per informazioni aggiuntive e dettagliate sulle varie opzioni di migrazione e su come migrare i carichi di lavoro da locale ad Azure VMware Solution utilizzando HCX, vedere "Considerazioni sulla migrazione VMware HCX" .

Per saperne di più su questo processo, guarda il seguente video:

Migrazione del carico di lavoro tramite HCX

Ecco uno screenshot dell'opzione HCX vMotion.



Per saperne di più 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

Che si punti a un cloud all-cloud o ibrido e che i dati risiedano su qualsiasi tipo/fornitore di storage in locale, Azure NetApp Files e HCX offrono ottime opzioni per distribuire e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO, rendendo i requisiti dei dati uniformi al livello dell'applicazione. Qualunque sia il caso d'uso, scegli Azure VMware Solution insieme ad Azure NetApp Files per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti in locale e su più cloud, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per connettere lo storage e migrare le VM tramite VMware vSphere Replication, VMware vMotion o persino Network File Copy (NFC).

Da asporto

I punti chiave di questo documento includono:

- Ora è possibile utilizzare Azure NetApp Files come archivio dati su Azure VMware Solution SDDC.
- È possibile migrare facilmente i dati da un ambiente locale al datastore di Azure NetApp Files .
- È possibile espandere e ridurre facilmente il datastore di Azure NetApp Files per soddisfare i requisiti di capacità e prestazioni durante l'attività di migrazione.

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, fare riferimento ai seguenti link del sito web:

- Documentazione della soluzione Azure VMware

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

- Documentazione Azure NetApp Files

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

- Considerazioni sulla migrazione di VMware HCX

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp per GCP/GCVE

Funzionalità NetApp per Google Cloud Platform GCVE

Scopri di più sulle funzionalità che NetApp offre a Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE): da NetApp come dispositivo di archiviazione guest connesso o datastore NFS supplementare alla migrazione di flussi di lavoro, estensione/bursting nel cloud, backup/ripristino e disaster recovery.

Passa alla sezione del contenuto desiderato selezionando tra le seguenti opzioni:

- "Configurazione di GCVE in GCP"
- "Opzioni di archiviazione NetApp per GCVE"
- "Soluzioni cloud NetApp /VMware"

Configurazione di GCVE in GCP

Come per l'ambiente on-premise, la pianificazione di un ambiente di virtualizzazione basato su cloud è fondamentale per un ambiente di produzione di successo per la creazione di VM e la migrazione.

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



L'archiviazione in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Google Cloud NetApp Volumes a GCVE.

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

- Distribuisci e configura GCVE
- Abilita l'accesso privato a GCVE

Visualizza il dettaglio"passaggi di configurazione per GCVE" .

Opzioni di archiviazione NetApp per GCVE

Lo storage NetApp può essere utilizzato in diversi modi, sia come Guess Connected che come datastore NFS supplementare, all'interno di GCP GCVE.

Per favore visita"Opzioni di archiviazione NetApp supportate" per maggiori informazioni.

Google Cloud supporta l'archiviazione NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come storage connesso agli ospiti
- Google Cloud NetApp Volumes (NetApp Volumes) come datastore NFS supplementare

Visualizza il dettaglio"opzioni di archiviazione per la connessione degli ospiti per GCVE" . Visualizza il dettaglio"opzioni di datastore NFS supplementari per GCVE" .

Per saperne di più"Supporto del datastore Google Cloud NetApp Volumes per Google Cloud VMware Engine (blog NetApp)" O"Come utilizzare Google Cloud NetApp Volumes come datastore per Google Cloud VMware Engine (blog di Google)"

Casi d'uso della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi d'uso sono semplici da implementare in Azure AVS. Questi casi sono definiti per ciascuna delle aree cloud definite da VMware:

- Protezione (include sia Disaster Recovery che Backup/Ripristino)
- Estendere
- Migrare

"Esplora le soluzioni NetApp per Google Cloud GCVE"

Proteggi i carichi di lavoro su GCP/GCVE

Ripristino di emergenza coerente con le applicazioni con NetApp SnapCenter e Veeam Replication

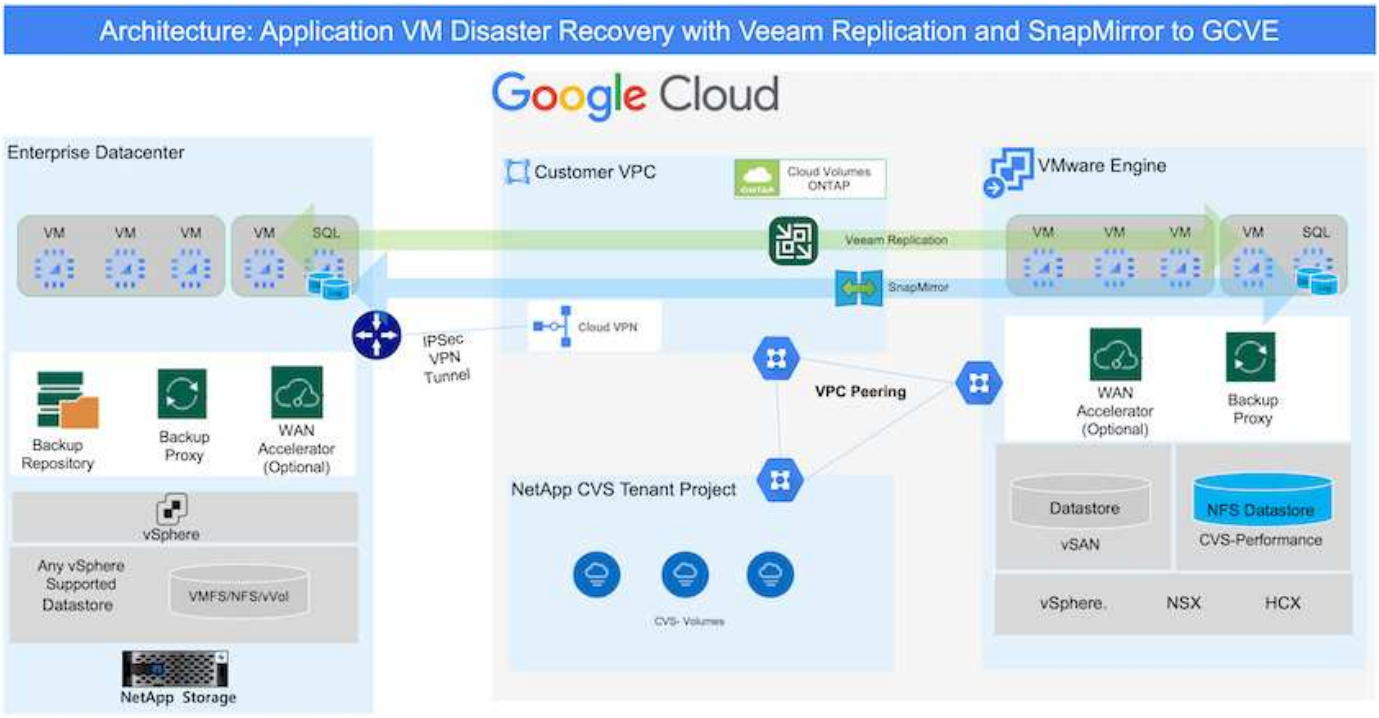
Il disaster recovery sul cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati come il ransomware. Con NetApp SnapMirror, i carichi di lavoro VMware on-premise che utilizzano storage connesso agli ospiti possono essere replicati su NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud.

Panoramica

Molti clienti sono alla ricerca di una soluzione efficace per il disaster recovery delle loro macchine virtuali applicative ospitate su VMware vSphere. Molti di loro utilizzano la soluzione di backup esistente per eseguire il ripristino in caso di emergenza. Spesso questa soluzione aumenta l'RTO e non soddisfa le aspettative. Per ridurre RPO e RTO, la replica delle VM Veeam può essere utilizzata anche da on-prem a GCVE, purché siano disponibili connettività di rete e un ambiente con autorizzazioni appropriate. NOTA: Veeam VM Replication non protegge i dispositivi di storage connessi alla VM guest, come i mount iSCSI o NFS all'interno della VM guest. Bisogna proteggerli separatamente.

Per una replica coerente delle applicazioni per SQL VM e per ridurre l'RTO, abbiamo utilizzato SnapCenter per orchestrare le operazioni snapmirror del database SQL e dei volumi di registro.

Questo documento fornisce un approccio passo passo per configurare ed eseguire il disaster recovery utilizzando NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Ipotesi

Questo documento si concentra sull'archiviazione in-guest per i dati delle applicazioni (nota anche come guest connected) e presuppone che l'ambiente locale utilizzi SnapCenter per backup coerenti con le applicazioni.

> Il presente documento si applica 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 aziendali.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizzare opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN locale.

> Esistono diverse opzioni per connettere i data center locali a Google Cloud, il che ci impedisce di descrivere un flusso di lavoro specifico in questo documento. Per il metodo di connettività on-premise-a-Google più appropriato, fare riferimento alla documentazione di Google Cloud.

Distribuzione della soluzione DR

Panoramica sulla distribuzione della soluzione

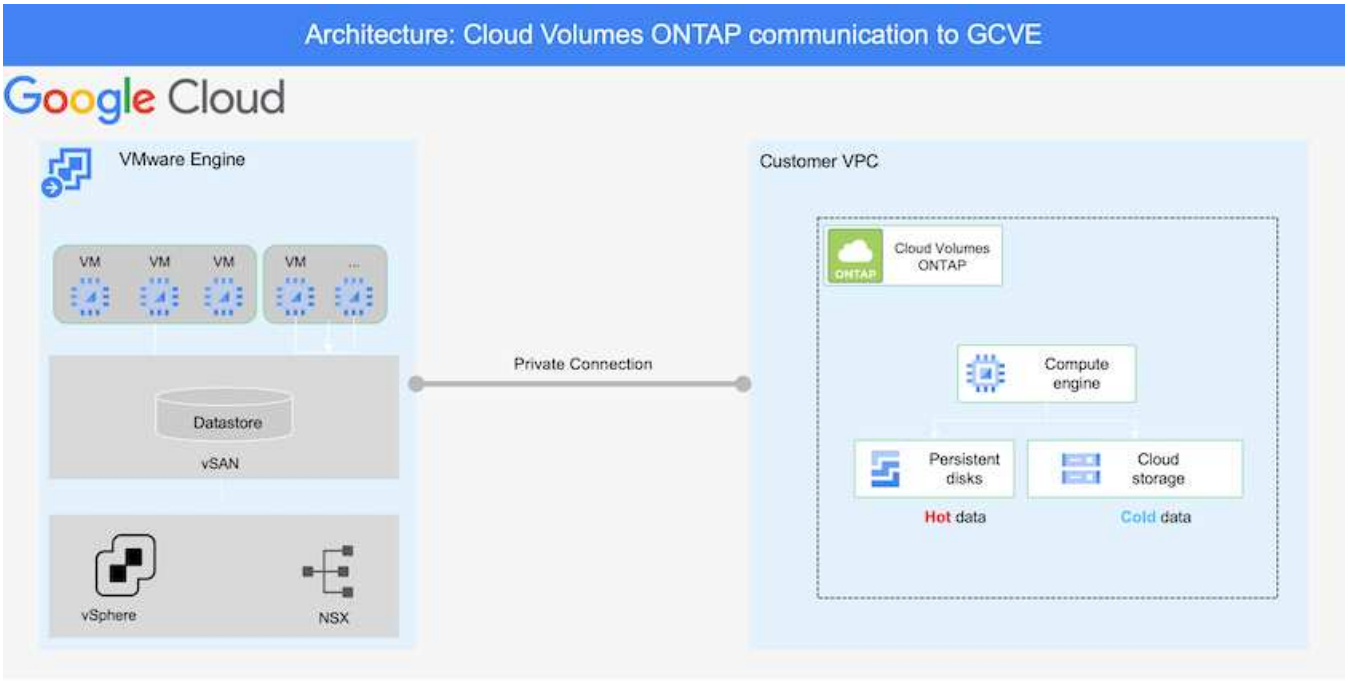
1. Assicurarsi che i dati dell'applicazione vengano sottoposti a backup tramite SnapCenter con i requisiti RPO necessari.
2. Effettua il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta tramite NetApp Console all'interno dell'abbonamento e della rete virtuale appropriati.
   a. Configurare SnapMirror per i volumi applicativi pertinenti.
   b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti SnapMirror dopo i processi pianificati.
3. Installa il software Veeam e inizia a replicare le macchine virtuali sull'istanza Google Cloud VMware Engine.

4. Durante un evento di disastro, interrompi la relazione di SnapMirror utilizzando NetApp Console e attiva il failover delle macchine virtuali con Veeam.
   a. Ricollegare i LUN ISCSI e i mount NFS per le VM dell'applicazione.
   b. Pubblica le applicazioni online.
5. Richiamare il failback sul sito protetto tramite la risincronizzazione inversa SnapMirror dopo il ripristino del sito primario.

Dettagli di distribuzione

▼ **Configura CVO su Google Cloud e replica i volumi su CVO**

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") e replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze e le conservazioni degli snapshot desiderate.



Per istruzioni dettagliate di esempio sulla configurazione SnapCenter e sulla replica dei dati, fare riferimento a"Configurazione della replica con SnapCenter"

Revisione della protezione delle VM SQL con SnapCenter

▼ **Configurare gli host GCVE e l'accesso ai dati CVO**

Due fattori importanti da considerare quando si implementa l'SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e per quanto tempo mantenere in servizio l'SDDC. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. L'SDDC può essere composto da un minimo di tre host, fino a diventare un cluster multi-host in una distribuzione su larga scala.

Google Cloud NetApp Volumes per NFS Datastore e Cloud Volumes ONTAP per database e log SQL possono essere distribuiti su qualsiasi VPC e GCVE deve disporre di una connessione privata a tale VPC per montare il datastore NFS e far sì che la VM si connetta alle LUN iSCSI.

Per configurare GCVE SDDC, vedere"Distribuisci e configura l'ambiente di virtualizzazione su Google Cloud Platform (GCP)" . Come prerequisito, verificare che le VM guest residenti 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 (VM con VMDK applicativi e VM con storage in-guest) utilizzando la funzionalità Veeam Replication e sfruttando SnapMirror per le copie dei volumi applicativi su Cloud Volumes ONTAP.

▼ **Installa i componenti Veeam**

In base allo scenario di distribuzione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere distribuiti. Per questo caso d'uso, non è necessario distribuire l'archivio oggetti per Veeam e nemmeno il repository Scale-out è necessario. "Fare riferimento alla documentazione Veeam per la procedura di installazione" Per ulteriori informazioni, fare riferimento"Migrazione con Veeam Replication"

▼ **Configurare la replica della VM con Veeam**

Sia vCenter on-premise che vCenter GCVE devono essere registrati con Veeam. "Configurazione del processo di replica della VM vSphere" Nella fase di elaborazione guest della procedura guidata, selezionare Disabilita elaborazione applicazione poiché utilizzeremo SnapCenter per il backup e il ripristino basati sull'applicazione.

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

▼ **Failover della VM di Microsoft SQL Server**

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.
- Ripristina qualsiasi punto disponibile nel tempo con la conservazione degli snapshot ONTAP .
- È disponibile l'automazione completa per tutti i passaggi necessari al ripristino di centinaia o migliaia di VM, a partire dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- SnapCenter utilizza meccanismi di clonazione che non modificano il volume replicato.
  - In questo modo si evita il rischio di danneggiamento dei dati per volumi e snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.
  - Sfrutta i dati DR per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.
- Veeam Replication consente di modificare gli indirizzi IP delle VM sul sito DR.

Disaster recovery delle applicazioni con SnapCenter, Cloud Volumes ONTAP e Veeam Replication

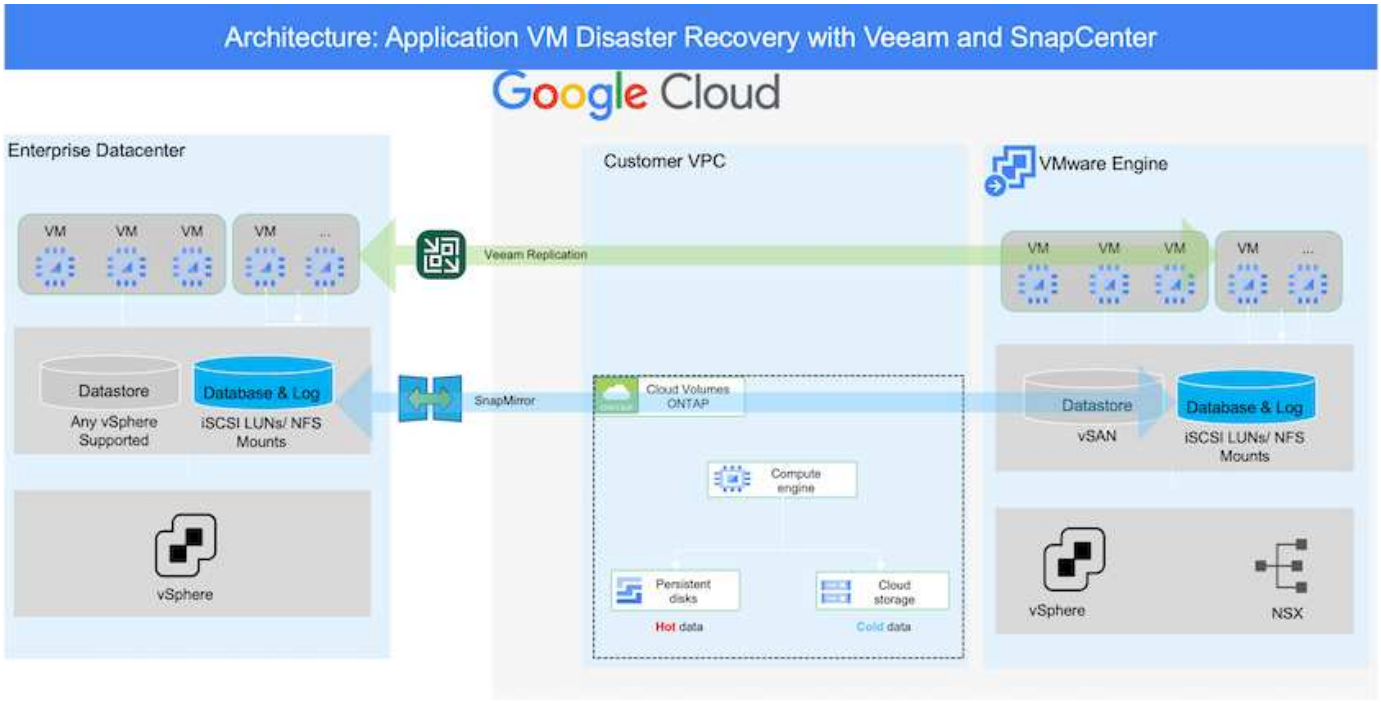
Il disaster recovery sul cloud è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati come il ransomware. Con NetApp SnapMirror, i carichi di lavoro VMware on-premise che utilizzano storage connesso agli ospiti possono essere replicati su NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud.

Panoramica

Questo riguarda i dati delle applicazioni; ma che dire delle VM stesse? Il ripristino di emergenza dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. Per raggiungere questo obiettivo, SnapMirror insieme a Veeam può essere utilizzato per ripristinare senza

problemi i carichi di lavoro replicati da locale a Cloud Volumes ONTAP utilizzando l'archiviazione vSAN per i VMDK delle VM.

Questo documento fornisce un approccio passo passo per configurare ed eseguire il disaster recovery utilizzando NetApp SnapMirror, Veeam e Google Cloud VMware Engine (GCVE).



Ipotesi

Questo documento si concentra sull'archiviazione in-guest per i dati delle applicazioni (nota anche come guest connected) e presuppone che l'ambiente locale utilizzi SnapCenter per backup coerenti con le applicazioni.

> Il presente documento si applica 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 aziendali.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizzare opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN locale.

> Esistono diverse opzioni per connettere i data center locali a Google Cloud, il che ci impedisce di descrivere un flusso di lavoro specifico in questo documento. Per il metodo di connettività on-premise-a-Google più appropriato, fare riferimento alla documentazione di Google Cloud.

Distribuzione della soluzione DR

Panoramica sulla distribuzione della soluzione

1. Assicurarsi che i dati dell'applicazione vengano sottoposti a backup tramite SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning Cloud Volumes ONTAP con la dimensione corretta dell'istanza utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.

a. Configurare SnapMirror per i volumi applicativi pertinenti.

b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti SnapMirror dopo i processi pianificati.

3. Installa il software Veeam e inizia a replicare le macchine virtuali sull'istanza Google Cloud VMware Engine.
4. In caso di disastro, interrompi la relazione SnapMirror utilizzando Cloud Manager e attiva il failover delle macchine virtuali con Veeam.

   a. Ricollegare i LUN ISCSI e i mount NFS per le VM dell'applicazione.

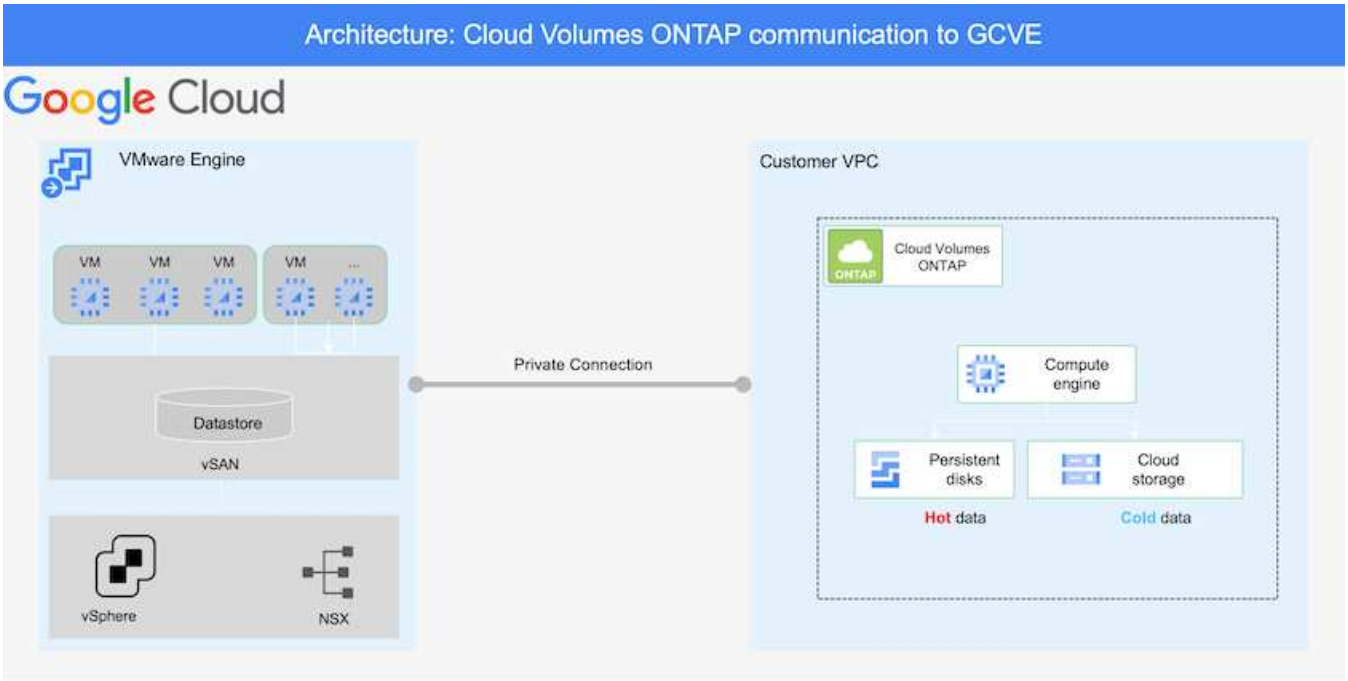
   b. Pubblica le applicazioni online.

5. Richiamare il failback sul sito protetto tramite la risincronizzazione inversa SnapMirror dopo il ripristino del sito primario.

Dettagli di distribuzione

▼ **Configura CVO su Google Cloud e replica i volumi su CVO**

Il primo passo è configurare Cloud Volumes ONTAP su Google Cloud ("cvo") e replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze e le conservazioni degli snapshot desiderate.



Per istruzioni dettagliate di esempio sulla configurazione SnapCenter e sulla 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 considerare quando si implementa l'SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e per quanto tempo mantenere in servizio l'SDDC. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. L'SDDC può essere composto da un minimo di tre host, fino a diventare un cluster multi-host in una distribuzione su larga scala.

Cloud Volumes ONTAP può essere distribuito su qualsiasi VPC e GCVE deve disporre di una connessione privata a tale VPC affinché la VM si connetta alle LUN iSCSI.

Per configurare GCVE SDDC, vedere"Distribuisci e configura l'ambiente di virtualizzazione su Google Cloud Platform (GCP)" . Come prerequisito, verificare che le VM guest residenti 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 (VM con VMDK applicativi e VM con storage in-guest) utilizzando la funzionalità Veeam Replication e sfruttando SnapMirror per le copie dei volumi applicativi su Cloud Volumes ONTAP.

▼ **Installa i componenti Veeam**

In base allo scenario di distribuzione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere distribuiti. Per questo caso d'uso, non è necessario distribuire l'archivio oggetti per Veeam e nemmeno il repository Scale-out è necessario.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Fare riferimento alla documentazione Veeam per la procedura di installazione"]

▼ **Configurare la replica della VM con Veeam**

Sia vCenter on-premise che vCenter GCVE devono essere registrati con Veeam. "Configurazione del processo di replica della VM vSphere" Nella fase di elaborazione guest della procedura guidata, selezionare Disabilita elaborazione applicazione poiché utilizzeremo SnapCenter per il backup e il ripristino basati sull'applicazione.

Configurazione del processo di replica della VM vSphere

▼ **Failover della VM di Microsoft SQL Server**

Failover della VM di Microsoft SQL Server

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Ripristina qualsiasi punto disponibile nel tempo con la conservazione degli snapshot ONTAP .
- È disponibile l'automazione completa per tutti i passaggi necessari al ripristino di centinaia o migliaia di VM, a partire dalle fasi di archiviazione, elaborazione, rete e convalida delle applicazioni.
- SnapCenter utilizza meccanismi di clonazione che non modificano il volume replicato.
  - In questo modo si evita il rischio di danneggiamento dei dati per volumi e snapshot.
  - Evita interruzioni della replicazione durante i flussi di lavoro dei test DR.
  - Sfrutta i dati DR per flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e aggiornamenti e test di correzione.
- Veeam Replication consente di modificare gli indirizzi IP delle VM sul sito DR.

Utilizzo di Veeam Replication e del datastore Google Cloud NetApp Volumes per il disaster recovery su Google Cloud VMware Engine

Un piano completo di disaster recovery è fondamentale per le aziende in tempi di crisi. Molte organizzazioni sfruttano il cloud computing per le operazioni quotidiane e il disaster recovery. Questo approccio proattivo può ridurre o eliminare costose interruzioni aziendali.

Questo articolo descrive come utilizzare Veeam Backup & Replication per configurare il disaster recovery per le VM VMware on-premise su Google Cloud VMware Engine (GCVE) con Google Cloud NetApp Volumes (NetApp Volumes).

Panoramica

Google Cloud NetApp Volumes è un servizio di archiviazione di Google e NetApp disponibile per Google Cloud. Il servizio NetApp Volumes fornisce storage NFS/SMB ad alte prestazioni. Lo storage NFS NetApp Volumes certificato VMware può essere utilizzato come datastore esterno per gli host ESXi in GCVE. Gli utenti devono creare una connessione peering tra il loro cloud privato GCVE e il progetto NetApp Volumes. Non ci sono costi di rete derivanti dall'accesso allo storage all'interno di una regione. Gli utenti possono creare volumi NetApp Volumes nella console Google Cloud e abilitare la protezione dall'eliminazione prima di montare i volumi come datastore sui loro host ESXi.

Gli archivi dati NFS basati su NetApp Volumes possono essere utilizzati per replicare i dati da ambienti locali utilizzando qualsiasi soluzione di terze parti convalidata che fornisca funzionalità di replica delle VM. Aggiungendo datastore NetApp Volumes, è possibile ottimizzare i costi di distribuzione anziché creare un SDDC basato su Google Cloud VMware Engine (GCVE) con un gran numero di host ESXi per ospitare lo storage. Questo approccio è chiamato "Pilot Light Cluster". Un cluster di luci pilota è una configurazione host GCVE minima (3 host GCVE ESXi) insieme alla capacità dei datastore NetApp Volumes per consentire un ridimensionamento indipendente per soddisfare i requisiti di capacità.

L'obiettivo è quello di sostenere un'infrastruttura conveniente, dotata solo dei componenti essenziali per gestire un failover. Un cluster di spie pilota può espandersi e aggiungere altri host GCVE in caso di failover. Una volta risolto il failover e riprese le normali operazioni, il gruppo di spie luminose può ridurre le sue dimensioni, tornando a una modalità operativa a basso costo.

Scopi del presente documento

Questo articolo descrive come utilizzare un datastore Google Cloud NetApp Volumes con Veeam Backup & Replication per configurare il disaster recovery per le VM VMware on-premise su GCVE utilizzando la funzionalità del software di replica delle VM Veeam.

Veeam Backup & Replication è un'applicazione di backup e replica per ambienti virtuali. Quando le macchine virtuali vengono replicate, Veeam Backup & Replication creerà una copia esatta delle VM nel formato nativo VMware vSphere sul cluster GCVE SDDC di destinazione. Veeam Backup & Replication manterrà la copia sincronizzata con la VM originale. La replica fornisce il miglior obiettivo di tempo di ripristino (RTO) poiché è presente una copia montata di una VM nel sito DR in uno stato pronto per l'avvio.

Questo meccanismo di replicazione garantisce che i carichi di lavoro possano essere avviati rapidamente in GCVE in caso di un evento disastroso. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e connessioni lente. Inoltre, filtra anche i blocchi di dati duplicati, i blocchi di dati zero, i file di swap e i "file del sistema operativo guest della VM esclusi". Il software comprimerà anche il traffico di replica. Per evitare che i processi di replicazione 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 guidato dai processi, ovvero la replica viene eseguita configurando i processi di replica. In caso di disastro, è possibile attivare il failover per ripristinare le VM eseguendo il failover sulla relativa copia replica. Quando viene eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito sullo stato più recente di una replica o su uno qualsiasi dei suoi punti di ripristino validi noti. Ciò consente il ripristino del ransomware o test isolati, a seconda delle necessità. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.

Panoramica della soluzione

Questa soluzione comprende i seguenti passaggi di alto livello:

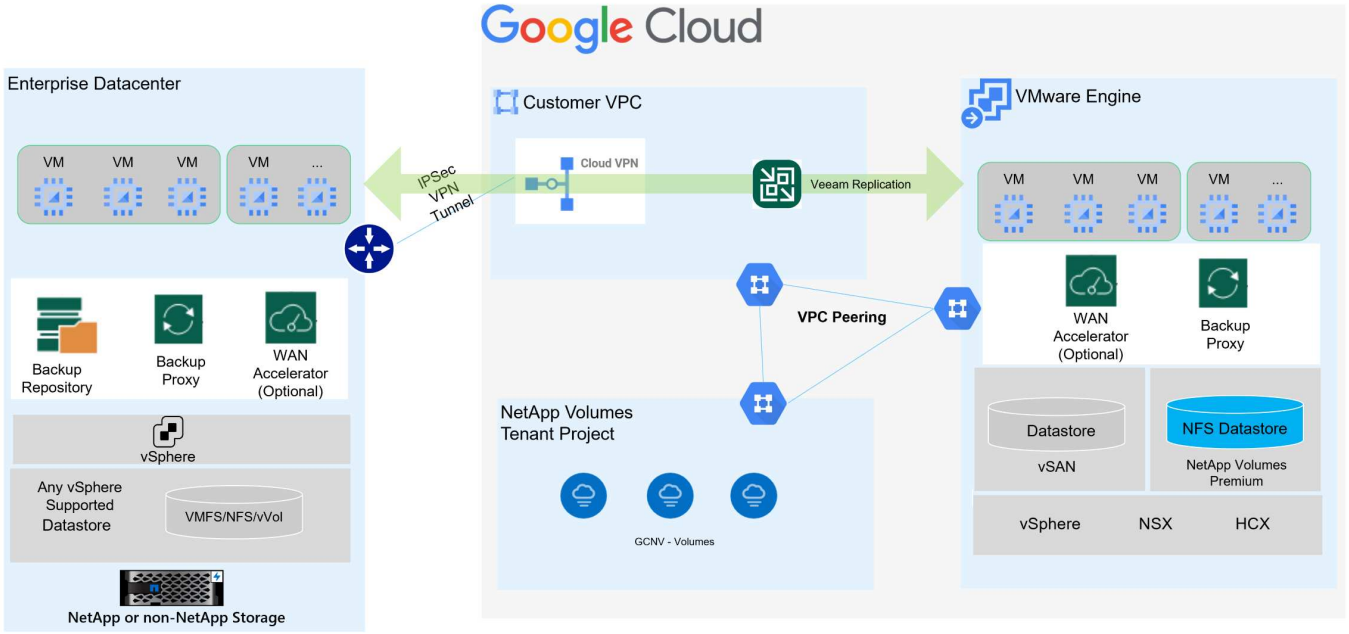
1. Crea un volume NFS utilizzando Google Cloud NetApp Volumes
2. Seguire la procedura GCP per creare un datastore GCVE dal volume NFS NetApp Volumes.
3. Imposta un processo di replica per creare repliche di VM utilizzando Veeam Backup & Replication.
4. Creare un piano di failover ed eseguire il failover.
5. Una volta completato l'evento disastroso e quando il sito primario è attivo, tornare alle VM di produzione.

> Quando si crea un volume in NetApp Volumes, da utilizzare come datastore GCVE, è supportato solo NFS v3.

Per ulteriori informazioni sull'utilizzo dei volumi NFS NetApp Volumes come datastore per GCVE, consultare "Utilizzo del volume NFS come datastore vSphere ospitato da Google Cloud NetApp Volumes" .

Architettura

Il diagramma seguente mostra l'architettura della soluzione presentata in questa documentazione. Una best practice consigliata è quella di disporre di un server Veeam Backup & Replication sia nella sede locale che nell'SDDC GCVE. Il backup e il ripristino vengono eseguiti e gestiti dal server Veeam in locale, mentre la replica è gestita dal server Veeam nel GCVE SDDC. Questa architettura garantisce la massima disponibilità in caso di guasto nel data center primario.



Prerequisiti per Veeam Replication su datastore GCVE e NetApp Volumes

Questa soluzione richiede i seguenti componenti e configurazioni:

1. NetApp Volumes dispone di uno Storage Pool con capacità libera sufficiente per ospitare il volume NFS da creare.
2. Il software Veeam Backup and Replication è in esecuzione in un ambiente locale con connettività di rete adeguata.

3. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa sia ai cluster GCVE SDDC di origine che a quelli di destinazione.
4. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa alle VM del server Veeam Proxy sia nei cluster GCVE di origine che di destinazione.
5. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai vCenter di origine e di destinazione.

Gli utenti devono creare una connessione peering tra il loro cloud privato GCVE e il progetto NetApp Volumes utilizzando le pagine Peering di rete VPC o Connessioni private nell'interfaccia utente della console VMware Engine Cloud.

> Veeam richiede un account utente della soluzione GCVE con privilegi elevati quando aggiungi il server GCVE vCenter all'inventario di Veeam Backup and Replication. Per ulteriori informazioni, fai riferimento alla documentazione di Google Cloud Platform (GCP), "Elevazione dei privilegi di VMware Engine".

Per ulteriori informazioni fare riferimento a "Considerazioni e limitazioni" nella documentazione di Veeam Backup & Replication.

Fasi di distribuzione

Le sezioni seguenti descrivono i passaggi di distribuzione per creare e montare un datastore NFS utilizzando Google Cloud NetApp Volumes e utilizzare Veeam Backup and Replication per implementare una soluzione completa di disaster recovery tra un data center locale e Google Cloud VMware Engine.

Crea volume NFS e datastore NetApp Volumes per GCVE

Fare riferimento a "Utilizzo del volume NFS come datastore vSphere ospitato da Google Cloud NetApp Volumes" per una panoramica su come utilizzare Google Cloud NetApp Volumes come datastore per GCVE.

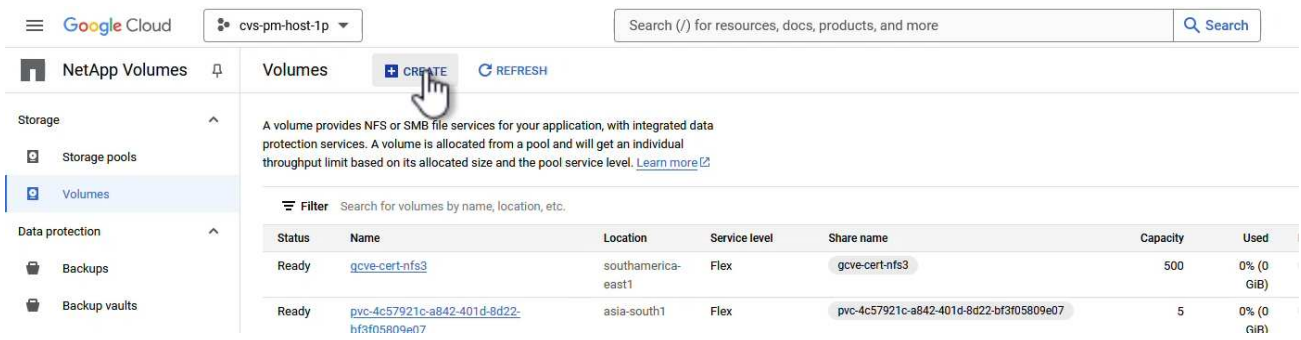
Completare i seguenti passaggi per creare e utilizzare un datastore NFS per GCVE utilizzando NetApp Volumes:

▼ **Crea volume NFS NetApp Volumes**

È possibile accedere a Google Cloud NetApp Volumes dalla console di Google Cloud Platform (GCP).

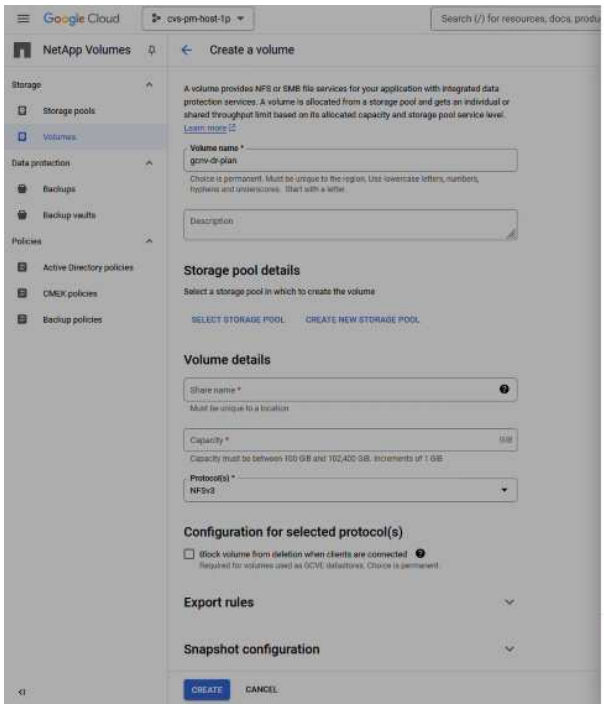
Fare riferimento a "Crea un volume" nella documentazione di Google Cloud NetApp Volumes per informazioni dettagliate su questo passaggio.

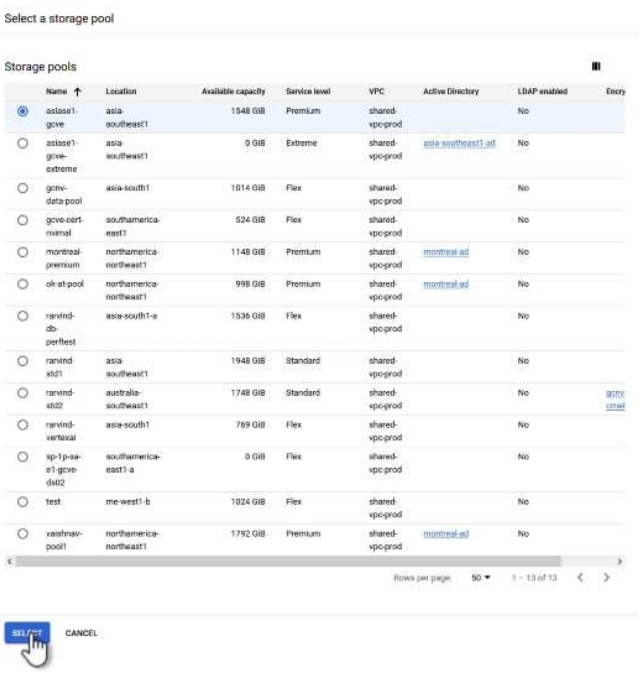
1. In un browser web, vai a https://console.cloud.google.com/ e accedi alla tua console GCP. Per iniziare, cerca * NetApp Volumes*.
2. Nell'interfaccia di gestione * NetApp Volumes*, fare clic su **Crea** per iniziare a creare un volume NFS.

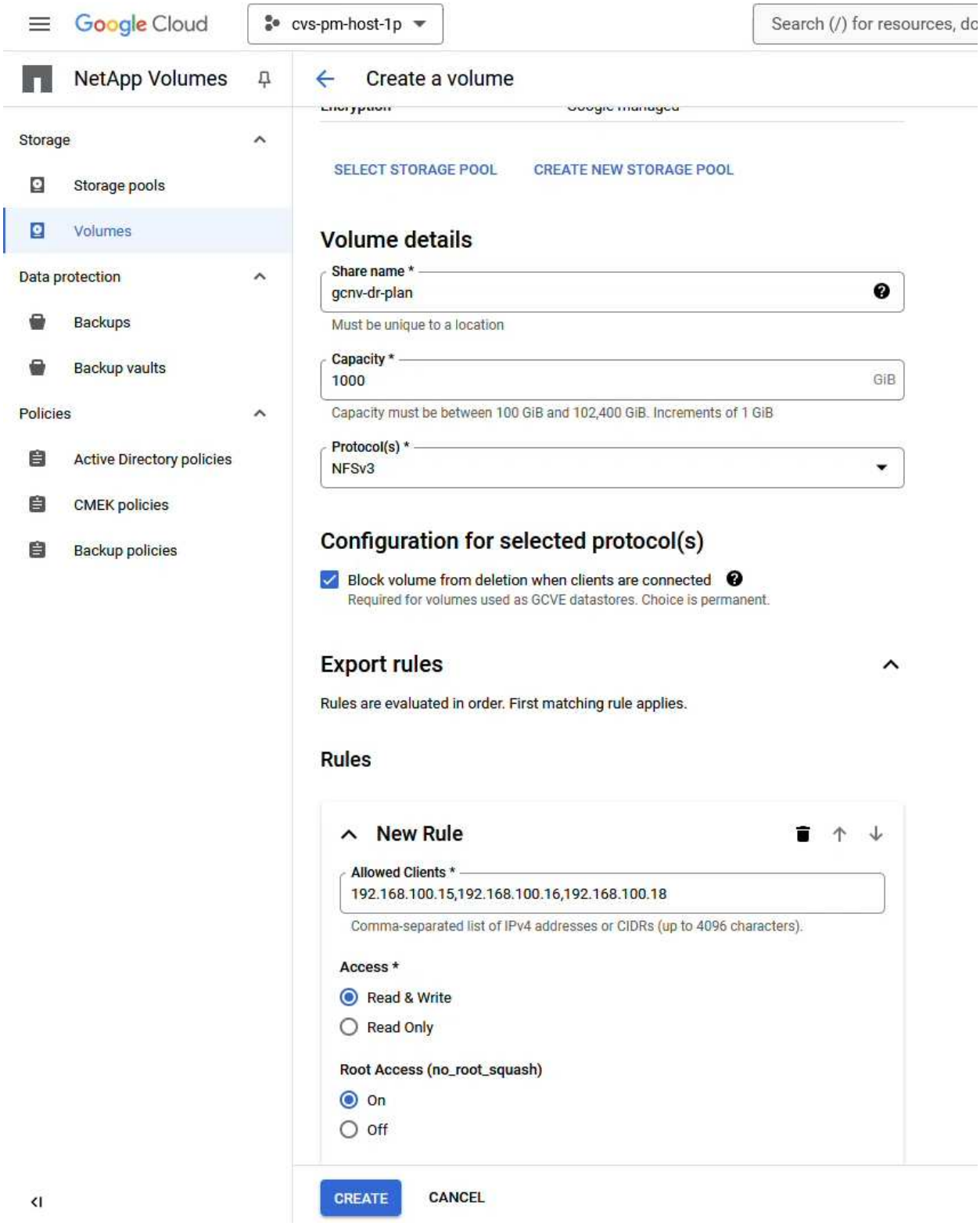


3. Nella procedura guidata **Crea un volume**, compila tutte le informazioni richieste:
   - Un nome per il volume.
   - Pool di archiviazione su cui creare il volume.
   - Nome di condivisione utilizzato durante il montaggio del volume NFS.
   - La capacità del volume in GiB.
   - Il protocollo di archiviazione da utilizzare.
   - Selezionare la casella per **Bloccare il volume dall'eliminazione quando i client sono connessi** (richiesto da GCVE durante il montaggio come datastore).
   - Le regole di esportazione per l'accesso al volume. Si tratta degli indirizzi IP degli adattatori ESXi sulla rete NFS.
   - Una pianificazione di snapshot utilizzata per proteggere il volume mediante snapshot locali.
   - Facoltativamente, scegliere di eseguire il backup del volume e/o creare etichette per il volume.

> Quando si crea un volume in NetApp Volumes, da utilizzare come datastore GCVE, è supportato solo NFS v3.

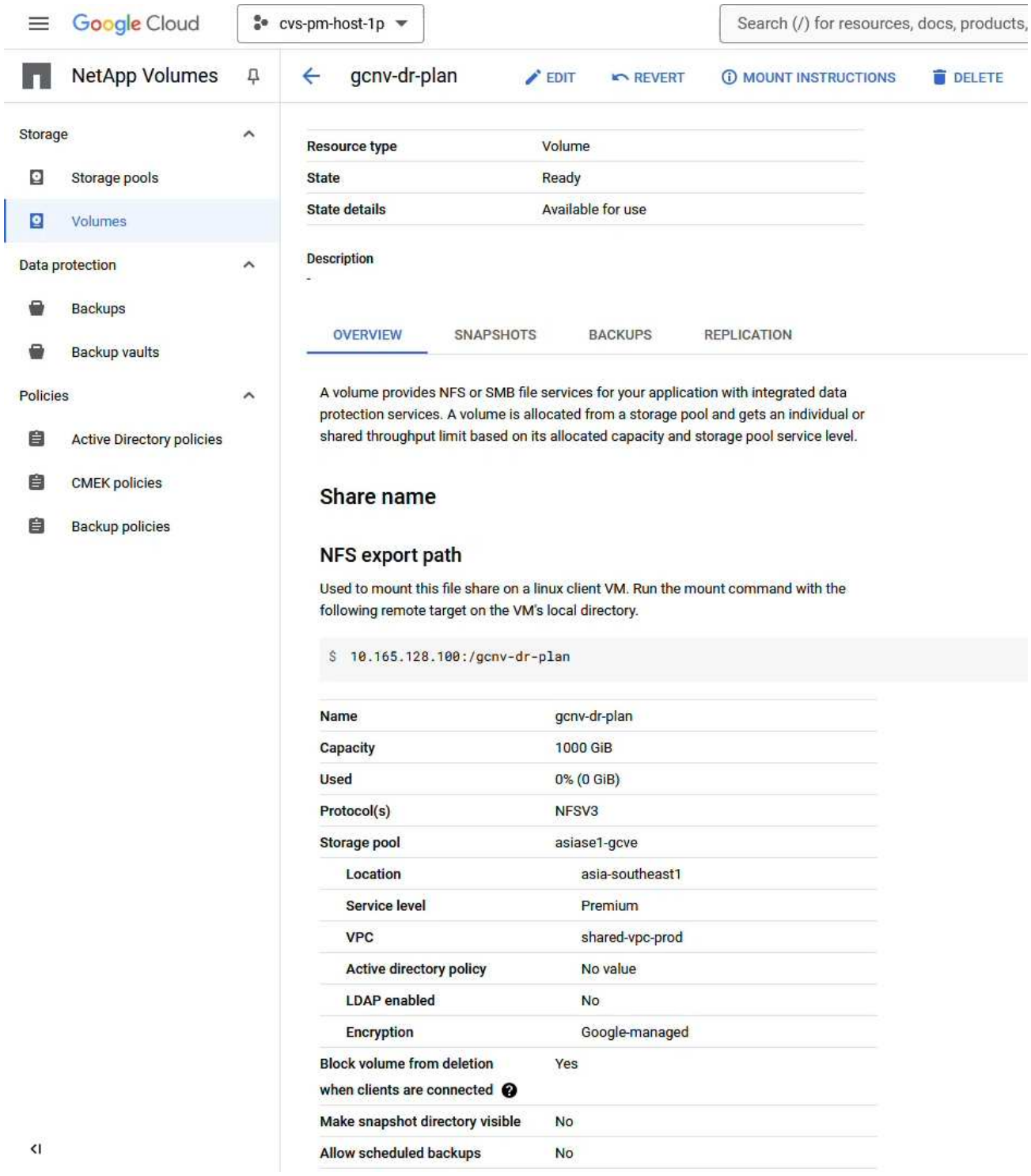






Fare clic su **Crea** per terminare la creazione del volume.

4. Una volta creato il volume, è possibile visualizzare il percorso di esportazione NFS necessario per montare il volume nella pagina delle proprietà del volume.



▼ **Montare il datastore NFS in GCVE**

Al momento della stesura di questo documento, il processo per montare un datastore in GCVE richiede l'apertura di un ticket di supporto GCP per montare il volume come datastore NFS.

Fare riferimento a "Utilizzo del volume NFS come datastore vSphere ospitato da Google Cloud NetApp Volumes" per maggiori informazioni.

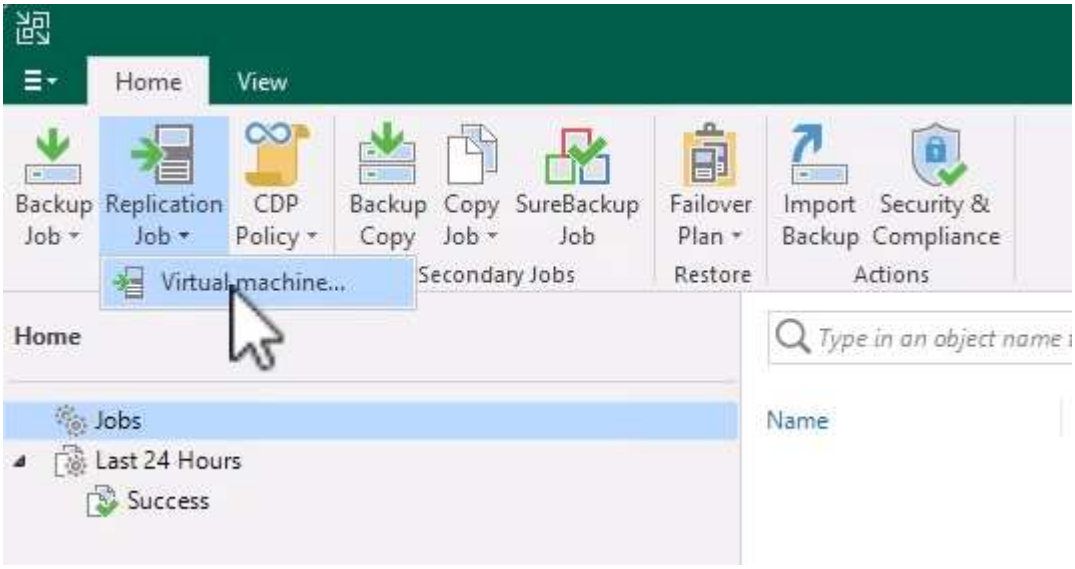
Replicare le VM su GCVE ed eseguire il piano di failover e il failback

▼ **Replicare le VM nel datastore NFS in GCVE**

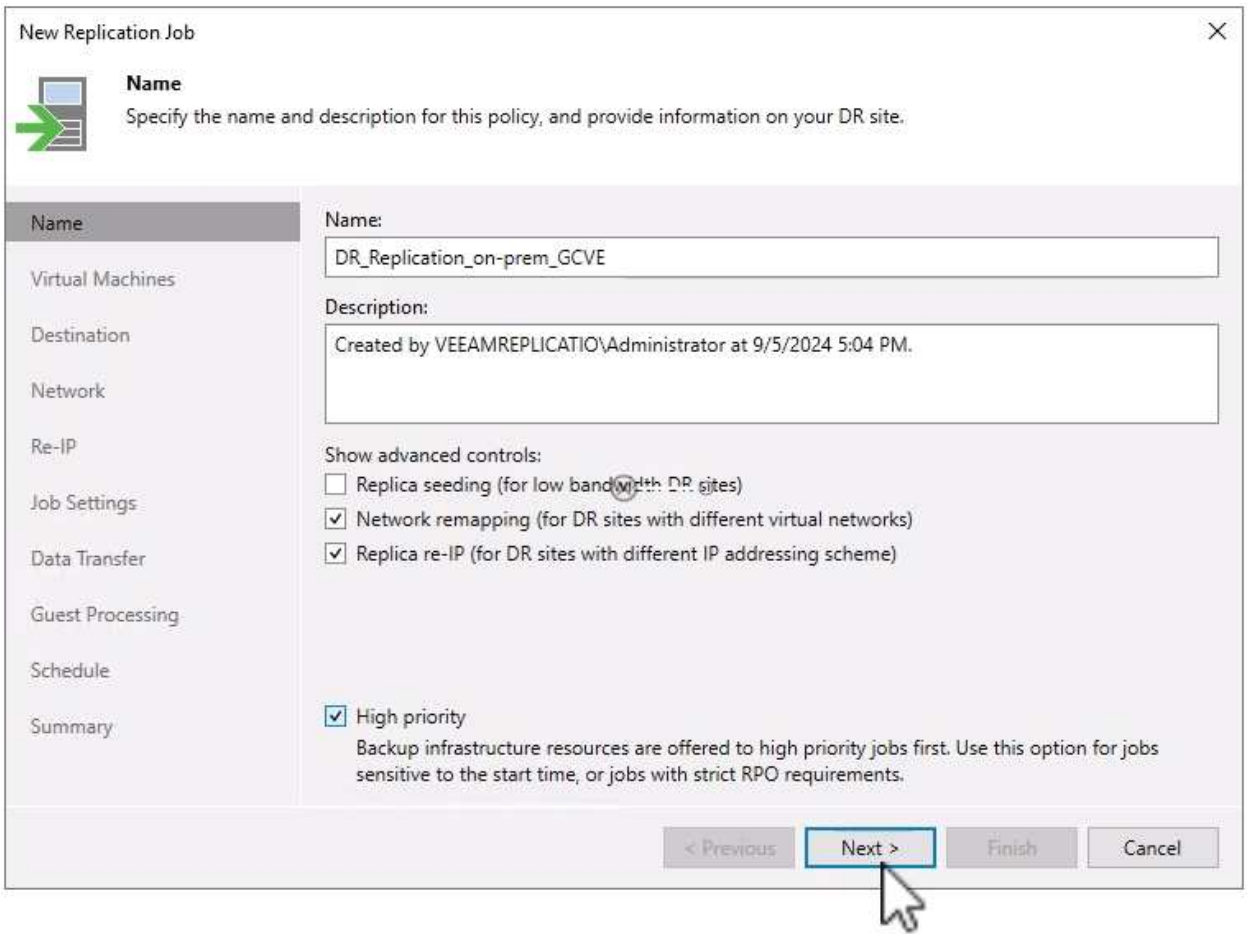
Veeam Backup & Replication sfrutta le funzionalità di snapshot di VMware vSphere durante la replica; Veeam Backup & Replication richiede a VMware vSphere di creare uno snapshot della VM. Lo snapshot della VM è la copia di una VM in un dato momento che include dischi virtuali, stato del sistema, configurazione e metadati. Veeam Backup & Replication utilizza lo snapshot come origine dei dati per la replica.

Per replicare le VM, completare i seguenti passaggi:

1. Aprire la console Veeam Backup & Replication.
2. Nella scheda **Home**, fare clic su **Replication Job > Macchina virtuale…**

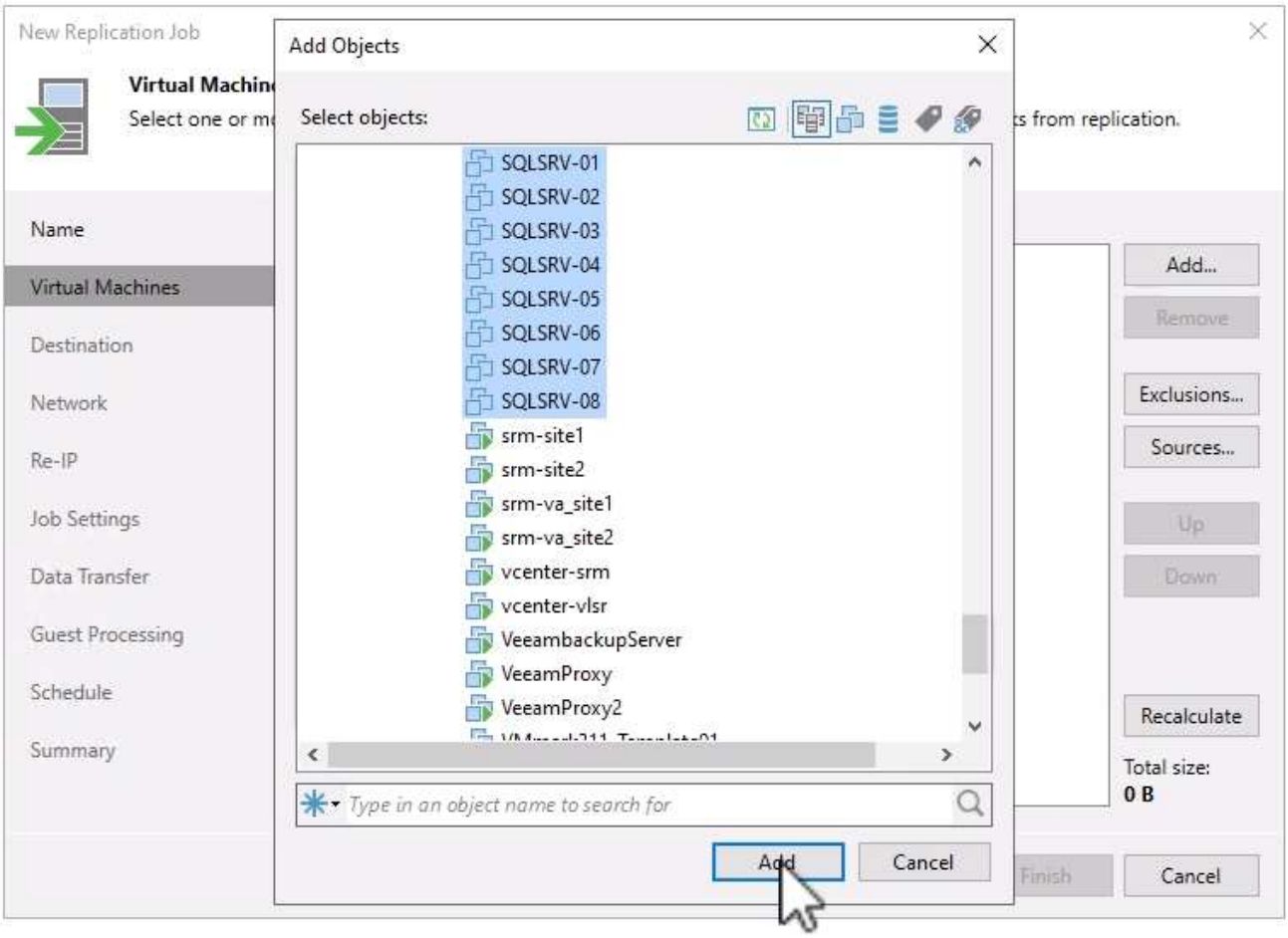


3. Nella pagina **Nome** della procedura guidata **Nuovo processo di replica**, specificare un nome per il processo e selezionare le caselle di controllo avanzate appropriate.
   - Selezionare la casella di controllo Replica seeding se la connettività tra locale e GCP ha una larghezza di banda limitata.
   - Selezionare la casella di controllo Rimappatura di rete (per siti GCVE SDDC con reti diverse) se i segmenti sul GCVE SDDC non corrispondono a quelli delle reti del sito locale.
   - Selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso) se lo schema di indirizzamento IP nel sito di produzione locale è diverso dallo schema nel sito GCVE di destinazione.

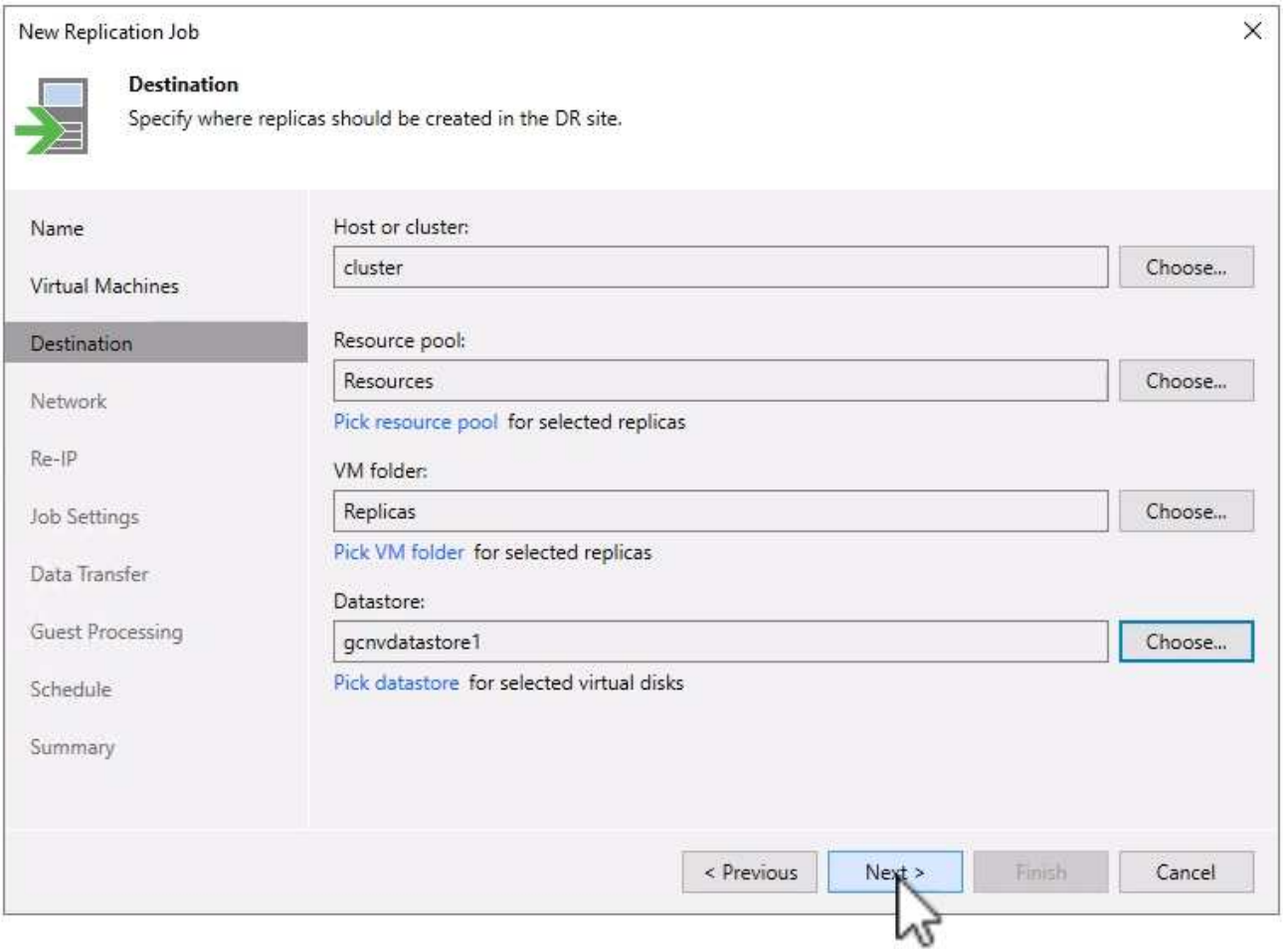


4. Nella pagina **Macchine virtuali**, seleziona le VM da replicare nel datastore NetApp Volumes collegato a un GCVE SDDC. Fare clic su **Aggiungi**, quindi nella finestra **Aggiungi oggetto** selezionare le VM o i contenitori VM necessari e fare clic su **Aggiungi**. Fare clic su **Avanti**.

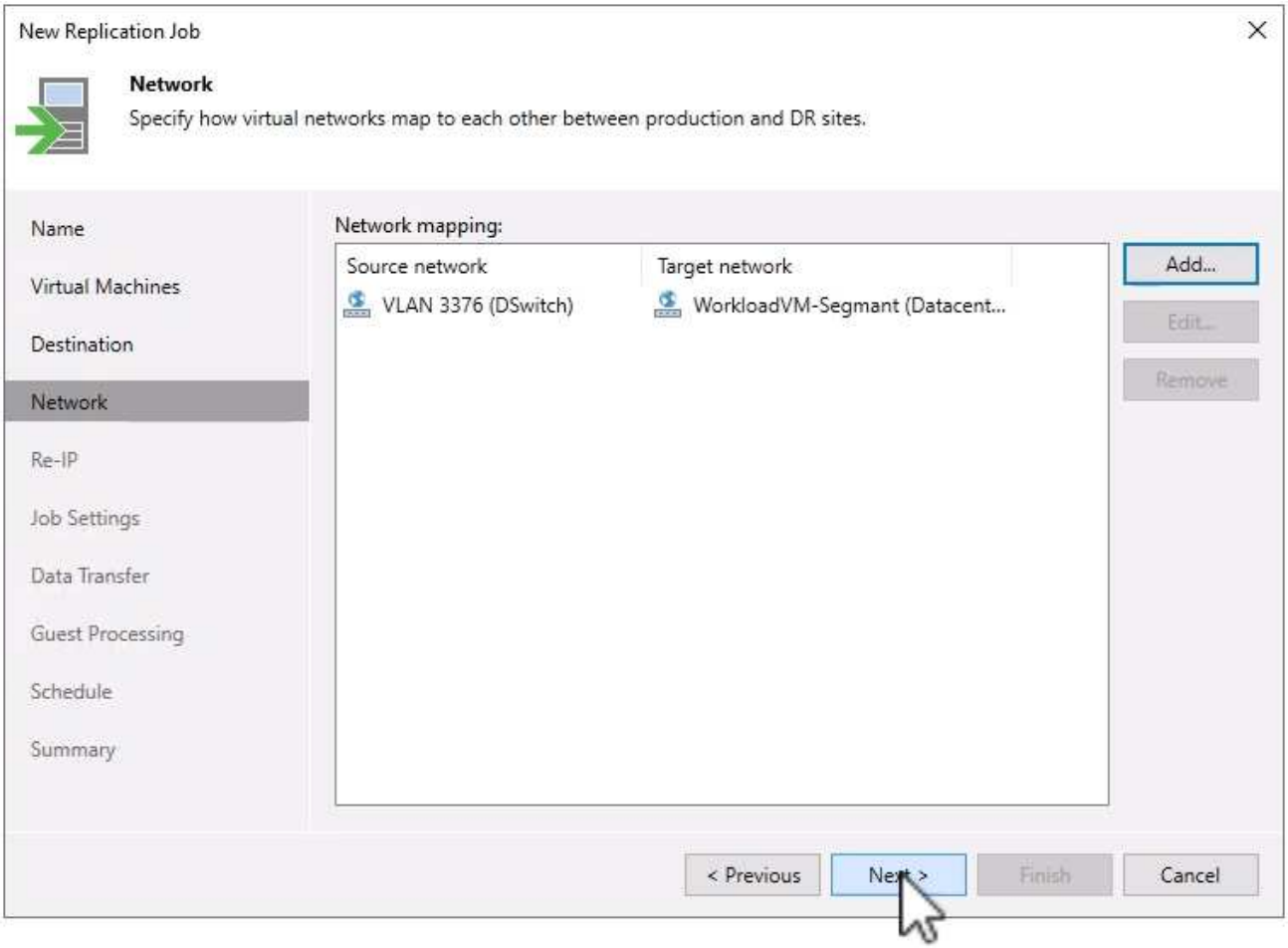
> ⓘ Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità disponibile del datastore vSAN. In un cluster di luci pilota, la capacità utilizzabile di un cluster vSAN a 3 nodi sarà limitata. Il resto dei dati può essere facilmente inserito negli archivi dati di Google Cloud NetApp Volumes, in modo che le VM possano essere recuperate e il cluster possa essere successivamente espanso per soddisfare i requisiti di CPU/memoria.



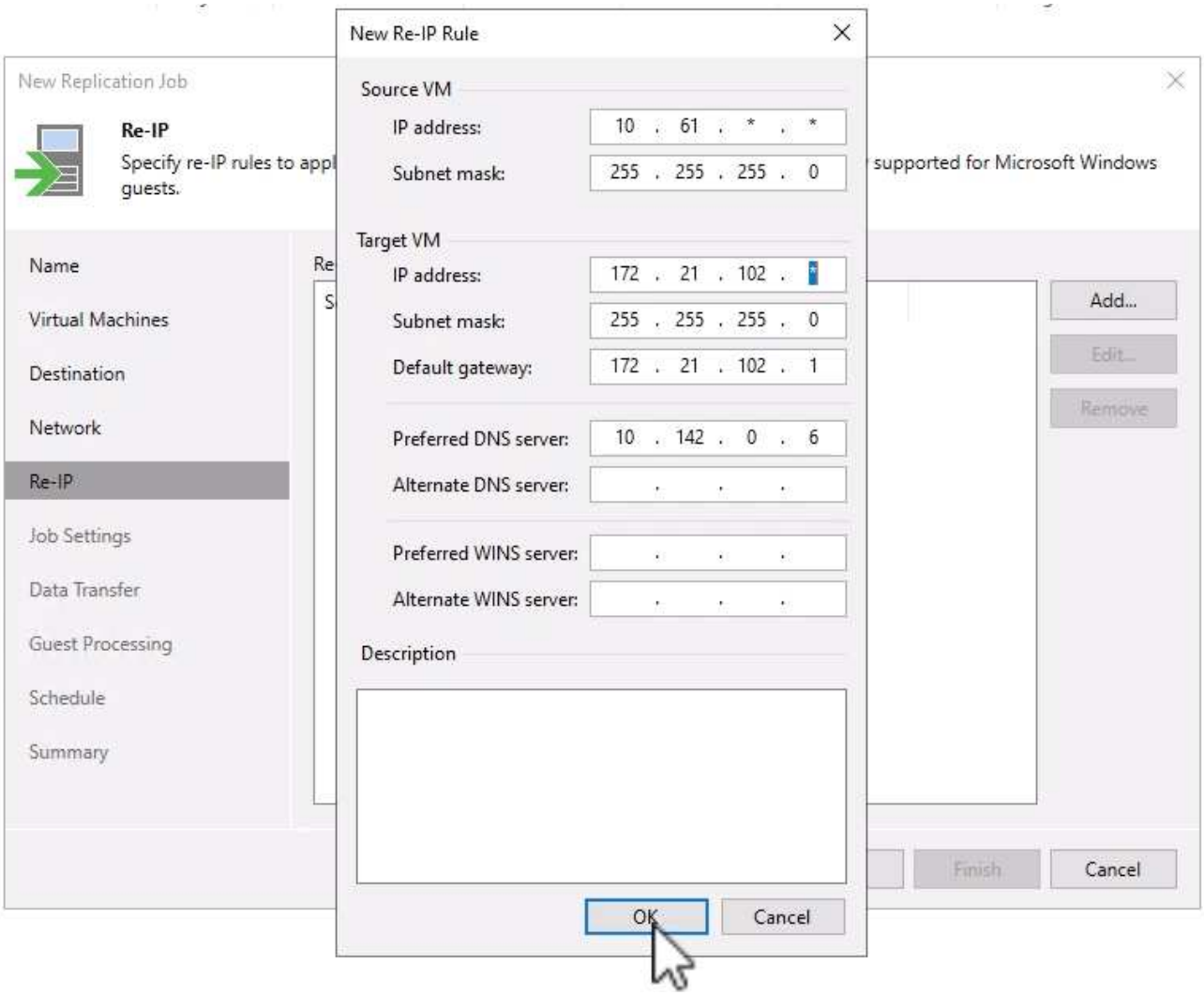
5. Nella pagina **Destinazione**, selezionare la destinazione come cluster/host GCVE SDDC e il pool di risorse appropriato, la cartella VM e il datastore NetApp Volumes per le repliche VM. Fare clic su **Avanti** per continuare.



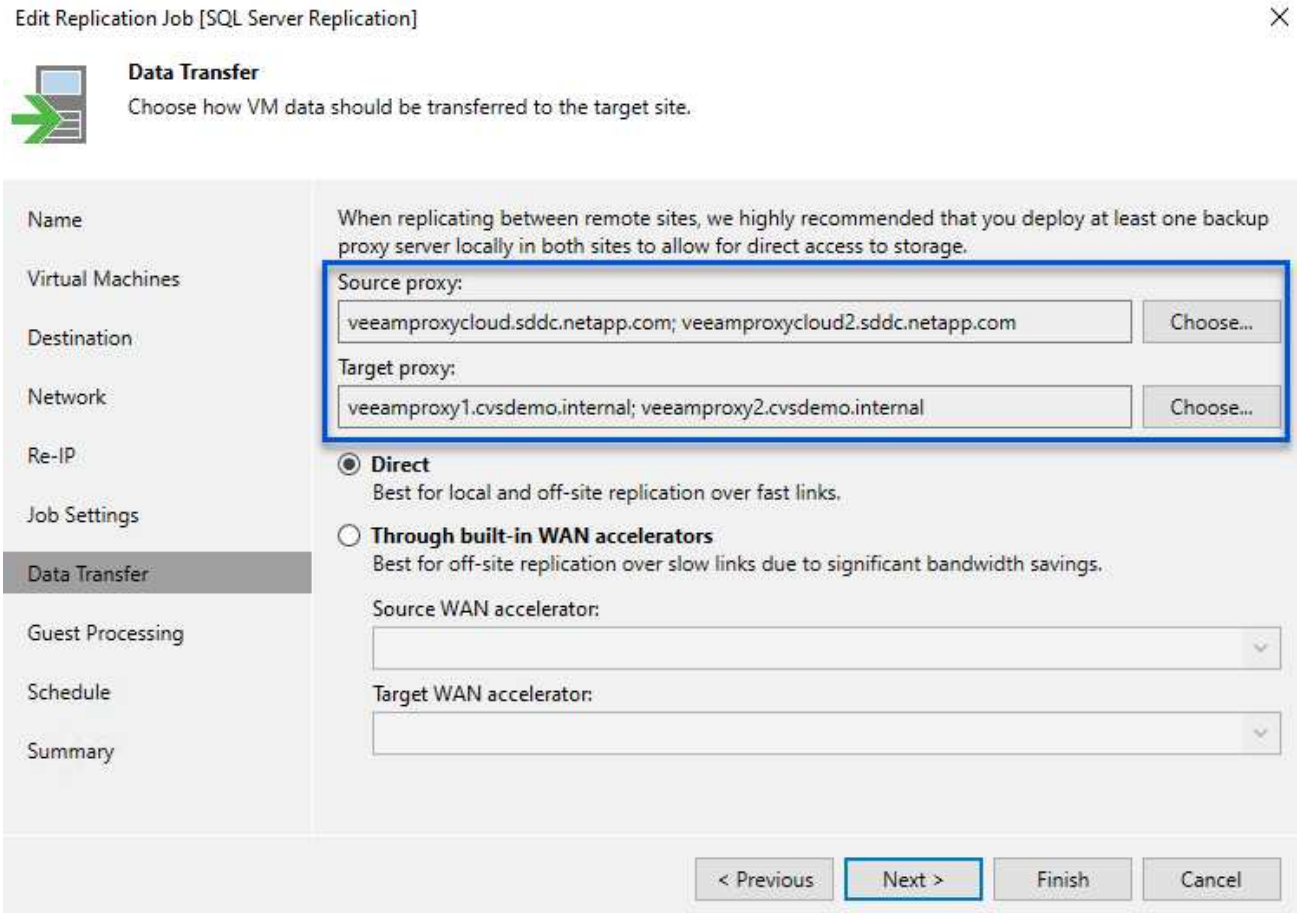
6. Nella pagina **Rete**, creare la mappatura tra le reti virtuali di origine e di destinazione in base alle esigenze. Fare clic su **Avanti** per continuare.



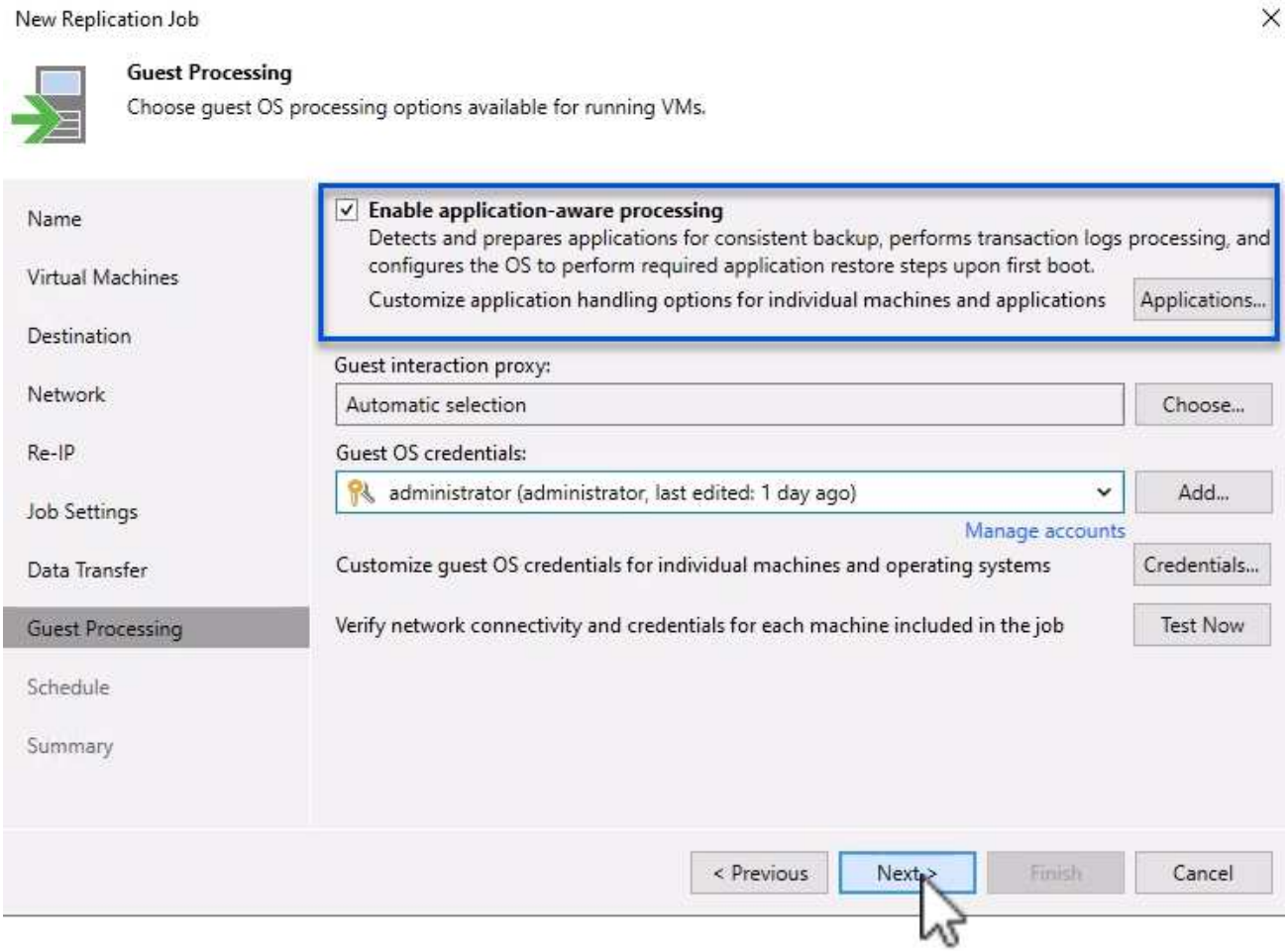
7. Nella pagina **Re-IP**, fare clic sul pulsante **Aggiungi…** per aggiungere una nuova regola re-IP. Compila gli intervalli IP delle VM di origine e di destinazione per specificare la rete che verrà applicata alle VM di origine in caso di failover. Utilizzare gli asterischi per specificare un intervallo di indirizzi indicato per quell'ottetto. Fare clic su **Avanti** per continuare.



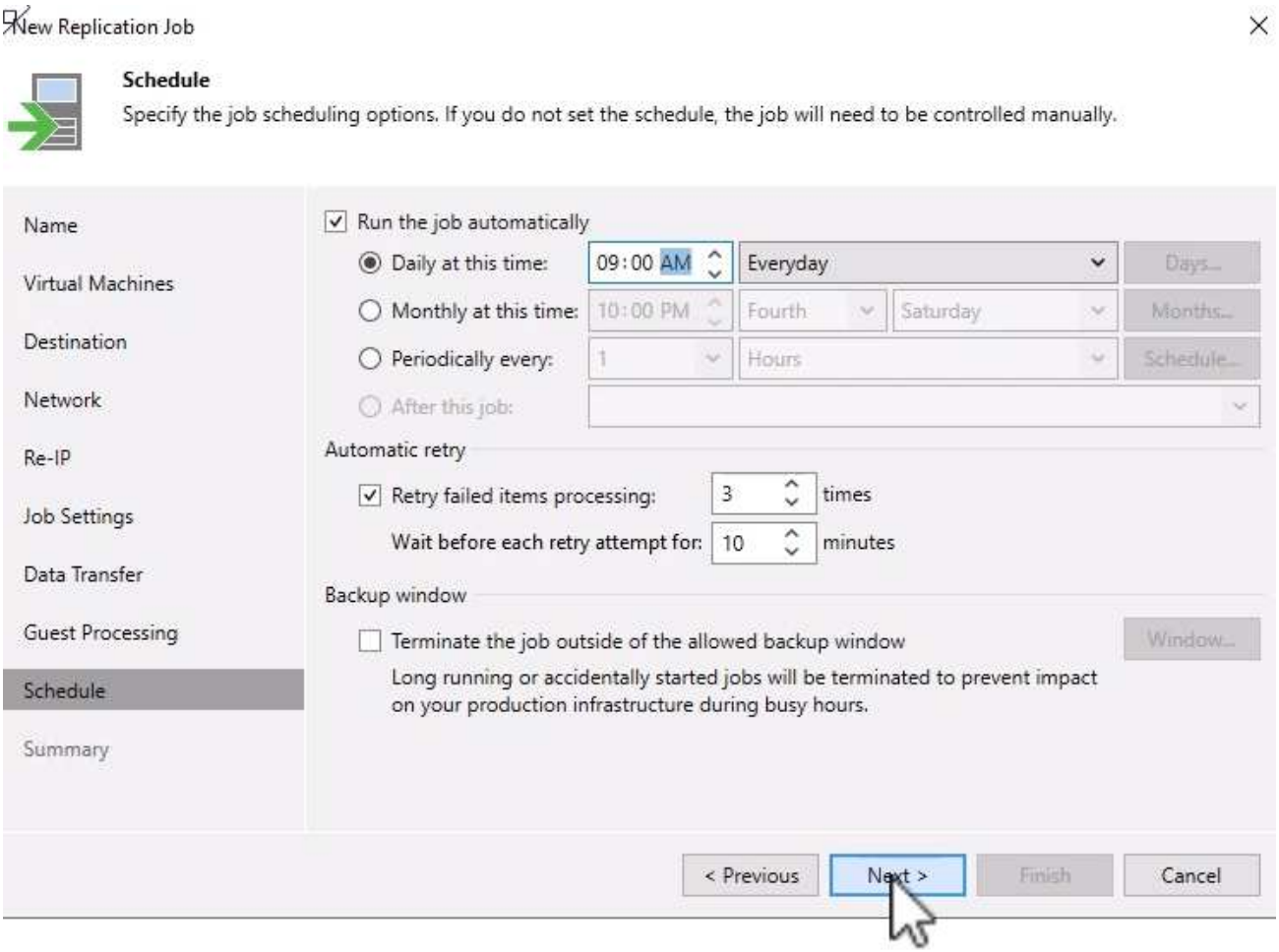
8. Nella pagina **Impostazioni processo**, specificare il repository di backup in cui verranno archiviati i metadati per le repliche delle VM, i criteri di conservazione e selezionare il pulsante in basso per **Avanzate…** per ulteriori impostazioni del processo. Fare clic su **Avanti** per continuare.
9. In **Trasferimento dati**, seleziona i server proxy che risiedono nei siti di origine e di destinazione e mantieni selezionata l'opzione Diretto. Qui è possibile selezionare anche gli acceleratori WAN, se configurati. Fare clic su **Avanti** per continuare.



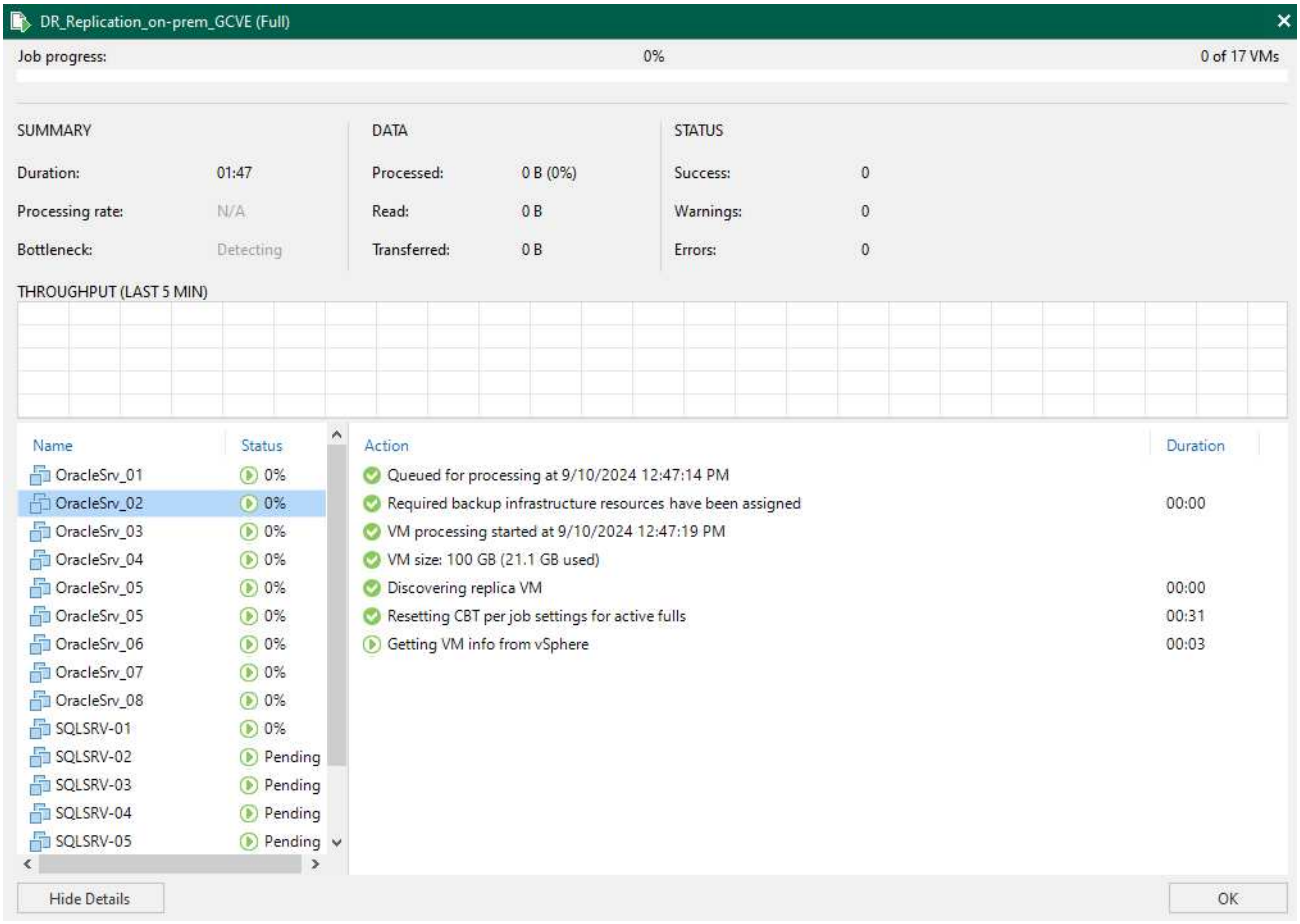
10. Nella pagina **Elaborazione guest**, seleziona la casella **Abilita elaborazione basata sull'applicazione** se necessario e seleziona le **Credenziali del sistema operativo guest**. Fare clic su **Avanti** per continuare.



11. Nella pagina **Pianificazione**, definire gli orari e la frequenza con cui verrà eseguito il processo di replica. Fare clic su **Avanti** per continuare.



12. Infine, rivedi l'impostazione del lavoro nella pagina **Riepilogo**. Selezionare la casella **Esegui il processo quando clicco su Fine** e fare clic su **Fine** per completare la creazione del processo di replica.
13. Una volta eseguito, il processo di replicazione può essere visualizzato nella finestra di stato del processo.



Per ulteriori informazioni sulla replica Veeam, fare riferimento a"Come funziona la replicazione"

▼ **Creare un piano di failover**

Una volta completata la replicazione o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire il failover per le VM dipendenti una alla volta o come gruppo automaticamente. Il piano di failover è il modello per l'ordine in cui vengono elaborate le VM, inclusi i ritardi di avvio. Il piano di failover aiuta anche a garantire che le VM dipendenti critiche siano già in esecuzione.

Dopo aver completato la replicazione o il seeding iniziale, creare un piano di failover. Questo piano funge da modello strategico per orchestrare il failover delle VM dipendenti, singolarmente o come gruppo. Definisce l'ordine di elaborazione delle VM, incorpora i ritardi di avvio necessari e garantisce che le VM dipendenti critiche siano operative prima delle altre. Implementando un piano di failover ben strutturato, le organizzazioni possono semplificare il processo di disaster recovery, riducendo al minimo i tempi di inattività e mantenendo l'integrità dei sistemi interdipendenti durante un evento di failover.

Durante la creazione del piano, Veeam Backup & Replication identifica e utilizza automaticamente i punti di ripristino più recenti per avviare le repliche delle VM.

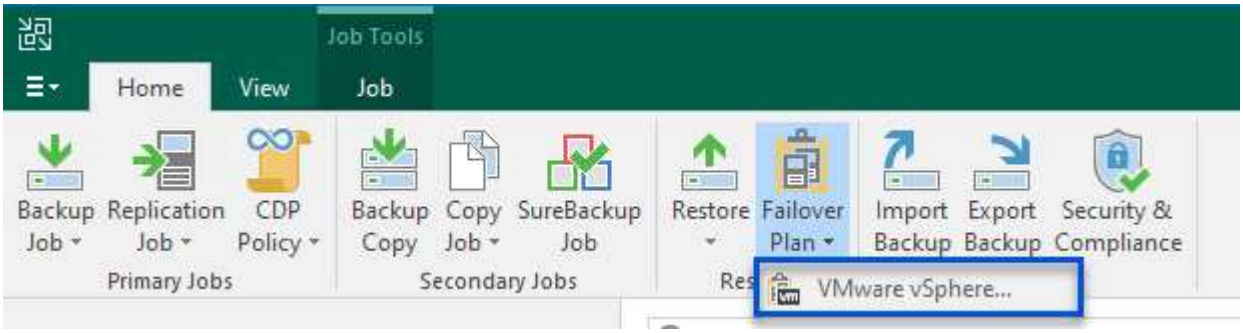
ⓘ Il piano di failover può essere creato solo una volta completata la replica iniziale e quando le repliche delle VM sono nello stato Pronto.

ⓘ Il numero massimo di VM che possono essere avviate simultaneamente durante l'esecuzione di un piano di failover è 10.

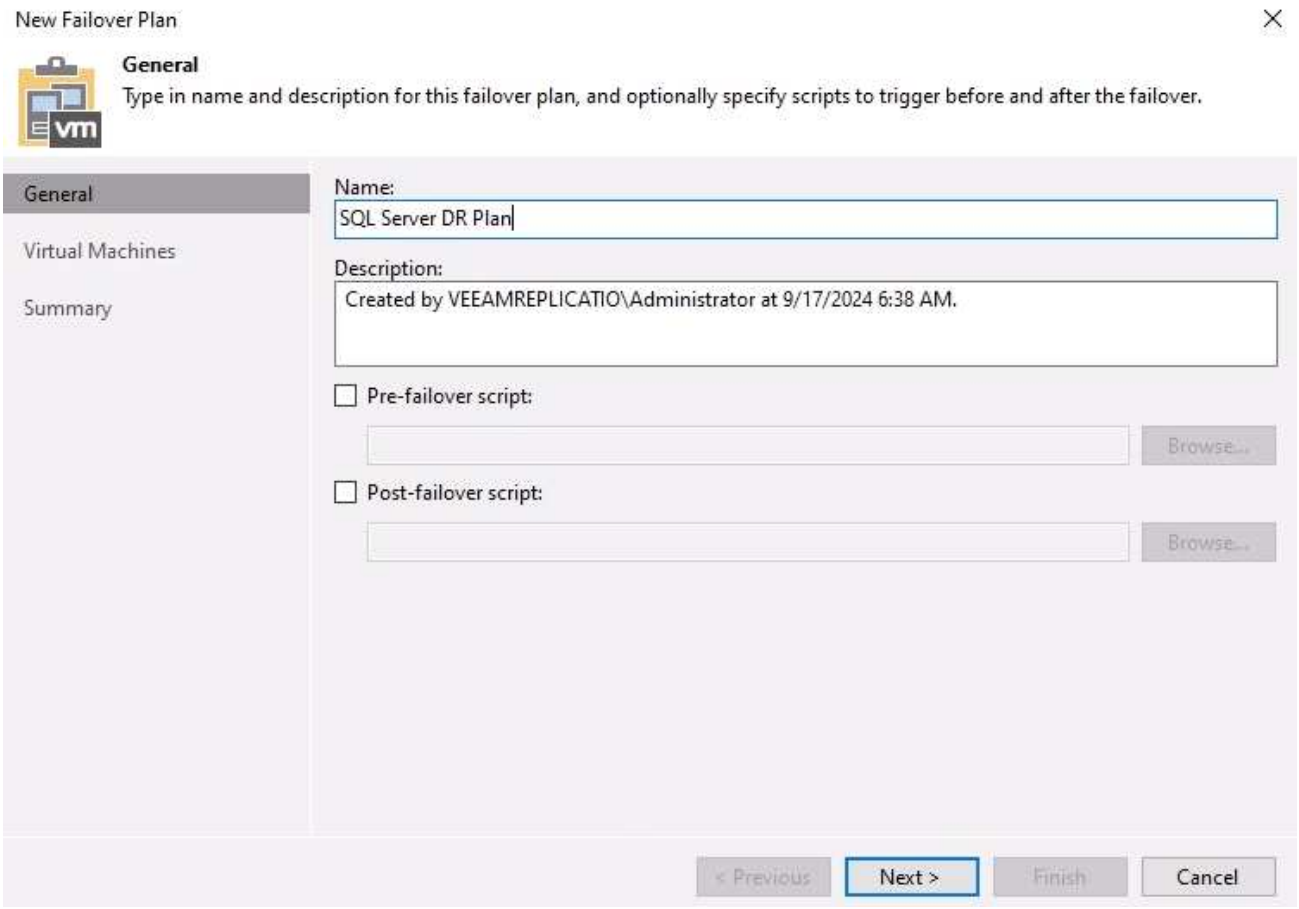
ⓘ Durante il processo di failover, le VM di origine non verranno spente.

Per creare il **Piano di failover**, completare i seguenti passaggi:

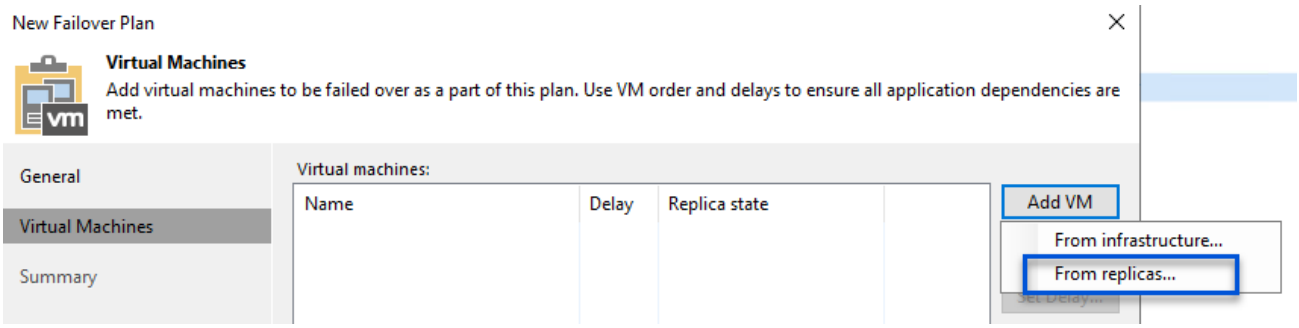
1. Nella vista **Home**, fare clic sul pulsante **Piano di failover** nella sezione **Ripristina**. Nel menu a discesa, seleziona **VMware vSphere…**

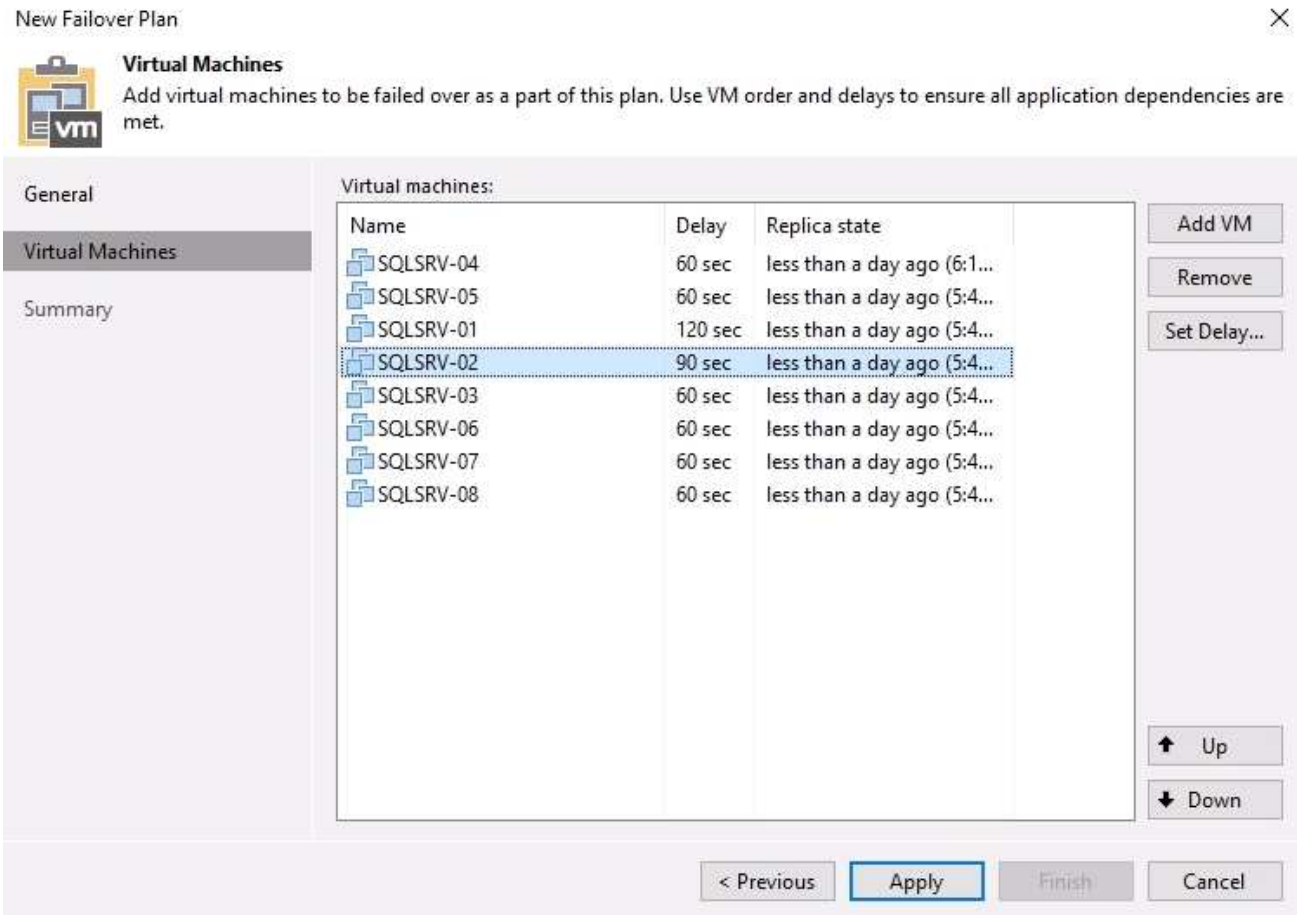


2. Nella pagina **Generale** della procedura guidata **Nuovo piano di failover**, immettere un nome e una descrizione per il piano. È possibile aggiungere script pre e post-failover in base alle esigenze. Ad esempio, eseguire uno script per arrestare le VM prima di avviare le VM replicate.



3. Nella pagina **Macchine virtuali**, fare clic sul pulsante **Aggiungi VM** e selezionare **Da repliche…**. Selezionare le VM che faranno parte del piano di failover, quindi modificare l'ordine di avvio delle VM e gli eventuali ritardi di avvio richiesti per soddisfare le dipendenze dell'applicazione.





Fare clic su **Applica** per continuare.

4. Infine, rivedere tutte le impostazioni del piano di failover e fare clic su **Fine** per creare il piano di failover.

Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento a"Creazione di processi di replicazione" .

▼ **Eseguire il piano di failover**

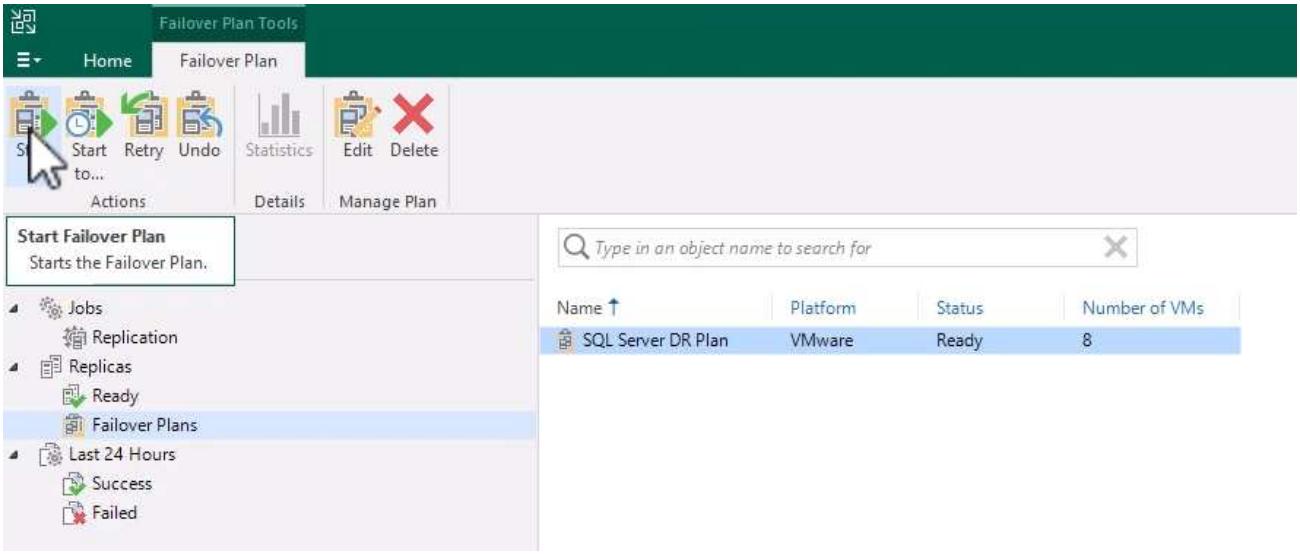
Durante il failover, la VM di origine nel sito di produzione passa alla sua replica nel sito di disaster recovery. Come parte del processo, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e trasferisce tutte le attività di I/O dalla VM di origine alla sua replica. Le repliche servono non solo per i disastri reali, ma anche per simulare le esercitazioni DR. Nella simulazione di failover, la VM di origine continua a funzionare. Una volta completati i test necessari, il failover può essere annullato, riportando le

operazioni alla normalità.

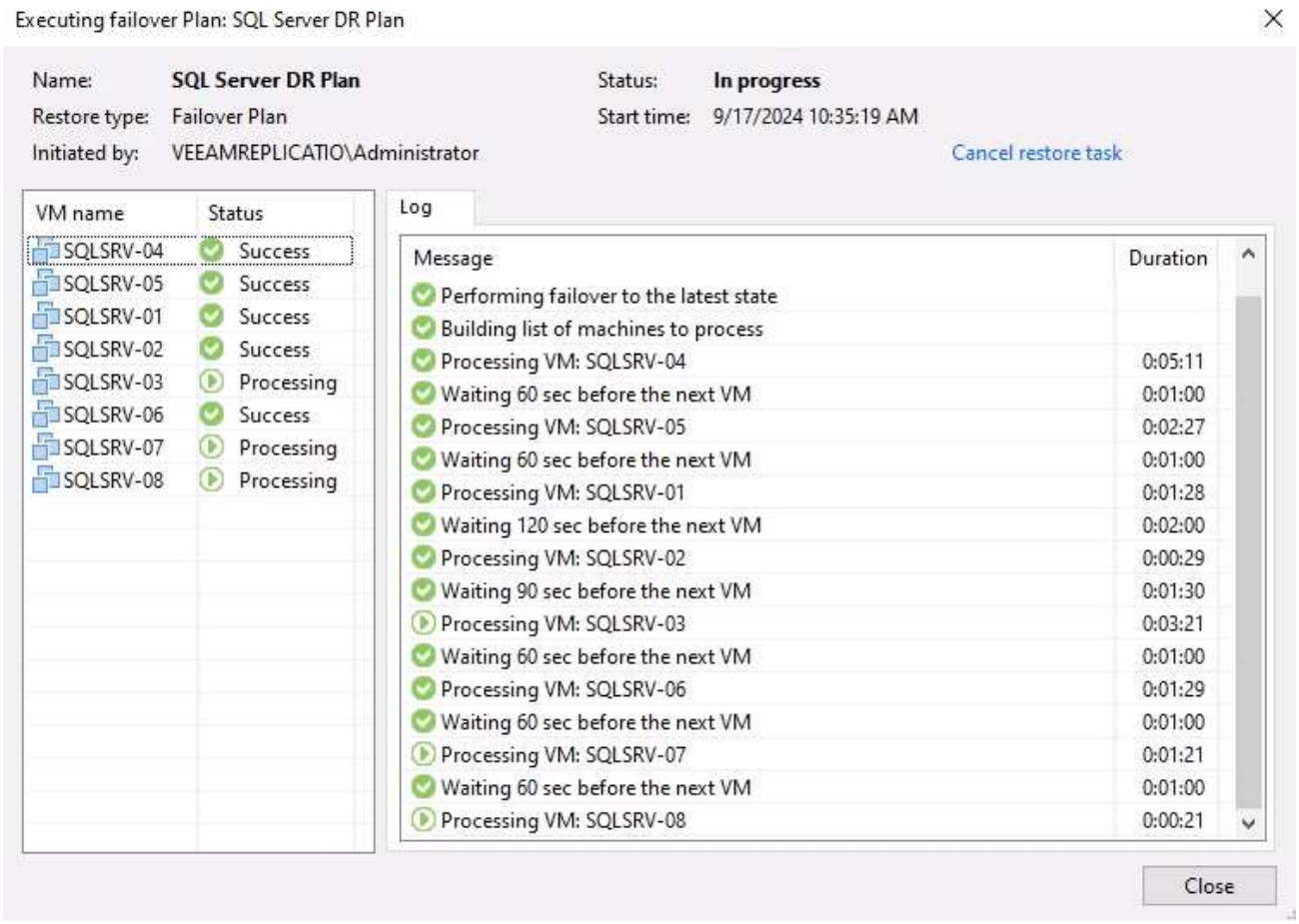
Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante il failover.

Completare i seguenti passaggi per avviare il piano di failover:

1. Per iniziare, nella vista **Home**, fare clic su **Repliche > Piani di failover** nel menu a sinistra e quindi sul pulsante **Avvia**. In alternativa, è possibile utilizzare il pulsante **Avvia su…** per eseguire il failover su un punto di ripristino precedente.



2. Monitorare l'avanzamento del failover nella finestra **Esecuzione del piano di failover**.



Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine finché la sua replica non torna allo stato Pronto.

Per informazioni dettagliate sui piani di failover, fare riferimento"Piani di failover" .

▼ **Failback al sito di produzione**

L'esecuzione di un failover è considerata una fase intermedia e deve essere finalizzata in base ai requisiti. Le opzioni includono quanto segue:

- **Failback in produzione**: ripristina la VM originale e sincronizza tutte le modifiche apportate durante il periodo di attività della replica con la VM di origine.

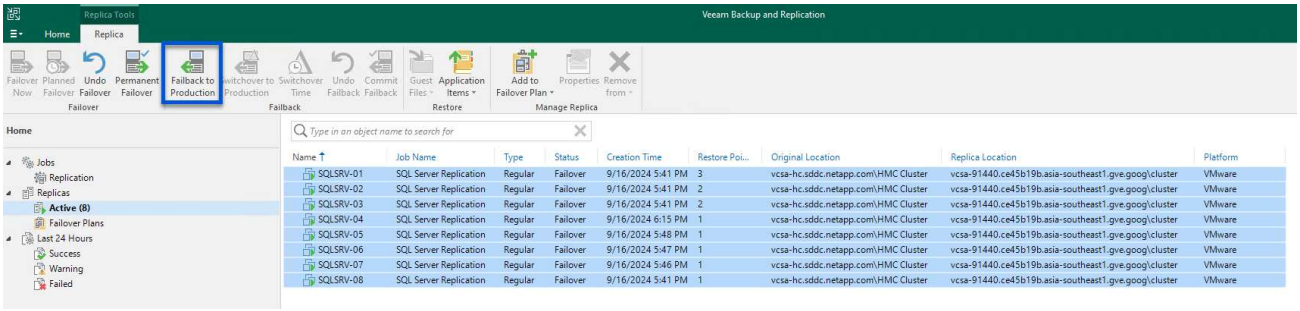
Durante il failback, le modifiche vengono trasferite ma non applicate immediatamente. Selezionare **Commit failback** una volta verificata la funzionalità della VM originale. In alternativa, selezionare **Annulla failback** per ripristinare la replica della VM se la VM originale presenta un comportamento imprevisto.

- **Annulla failover**: ripristina la VM originale, ignorando tutte le modifiche apportate alla replica della VM durante il suo periodo operativo.
- **Failover permanente**: passaggio permanente dalla VM originale alla sua replica, stabilendo la replica come nuova VM primaria per le operazioni in corso.

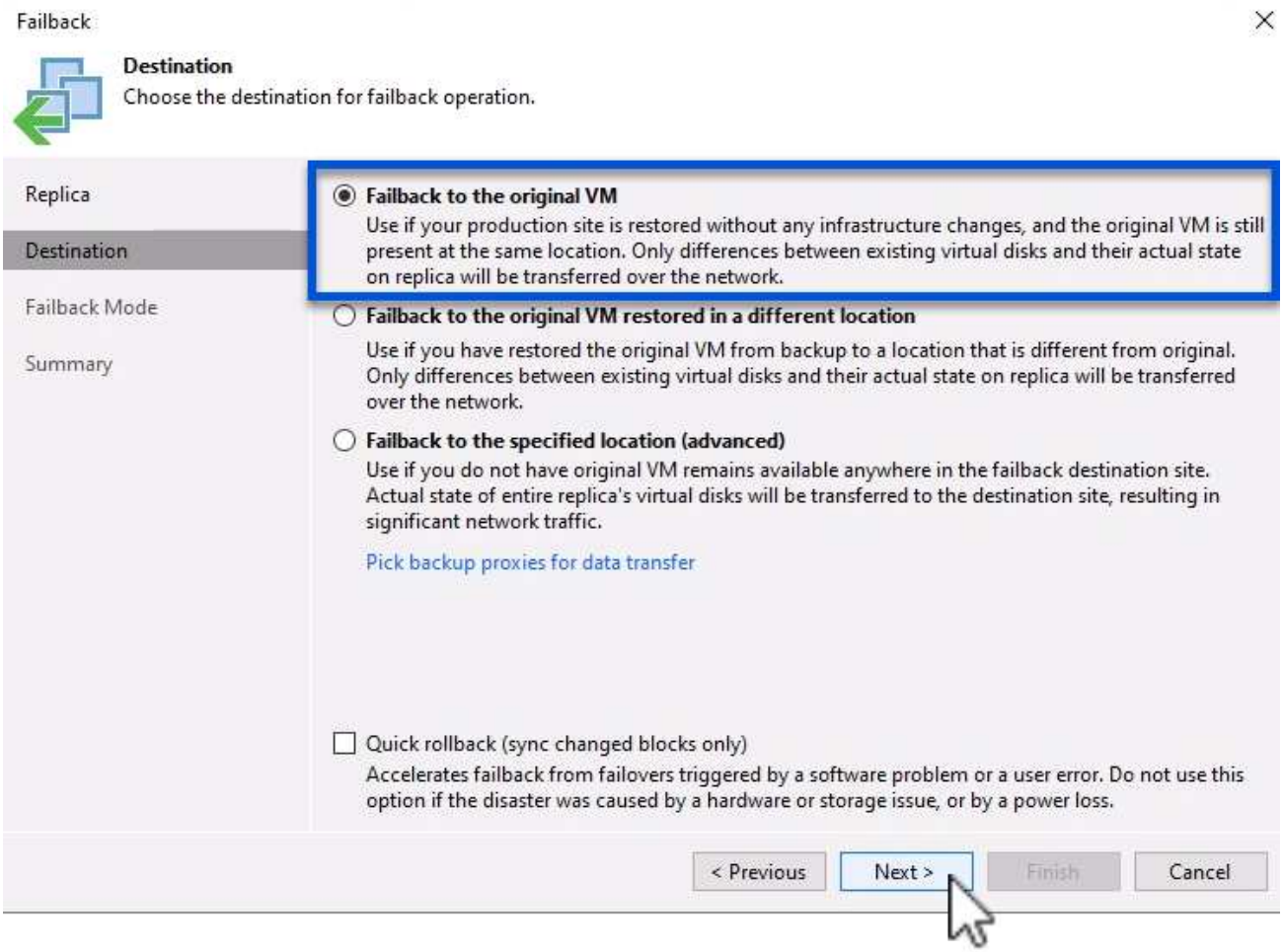
In questo scenario è stata selezionata l'opzione "Failback in produzione".

Completare i seguenti passaggi per eseguire un failback sul sito di produzione:

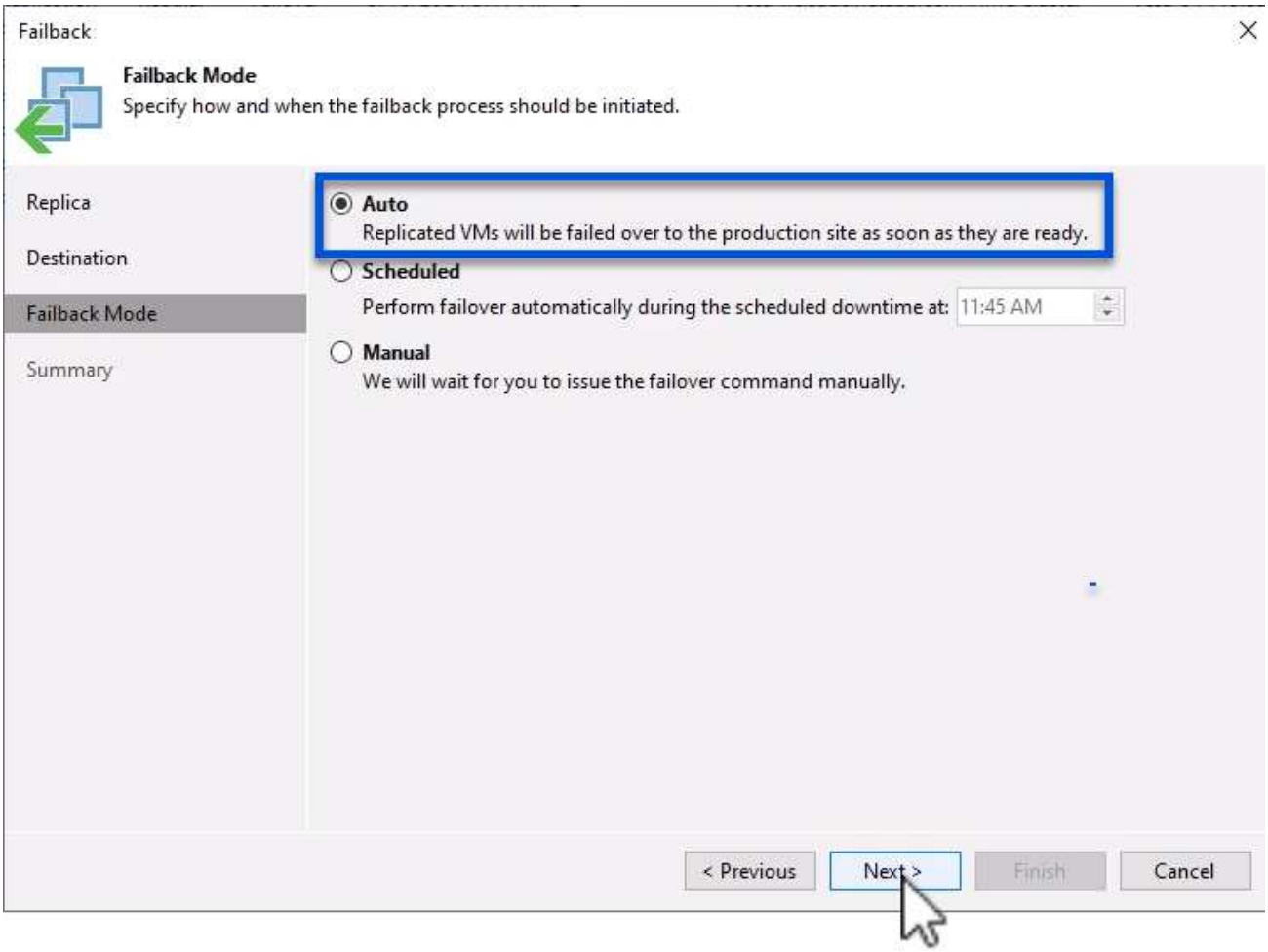
1. Dalla vista **Home**, fare clic su **Repliche > Attive** nel menu a sinistra. Selezionare le VM da includere e fare clic sul pulsante **Failback in produzione** nel menu in alto.



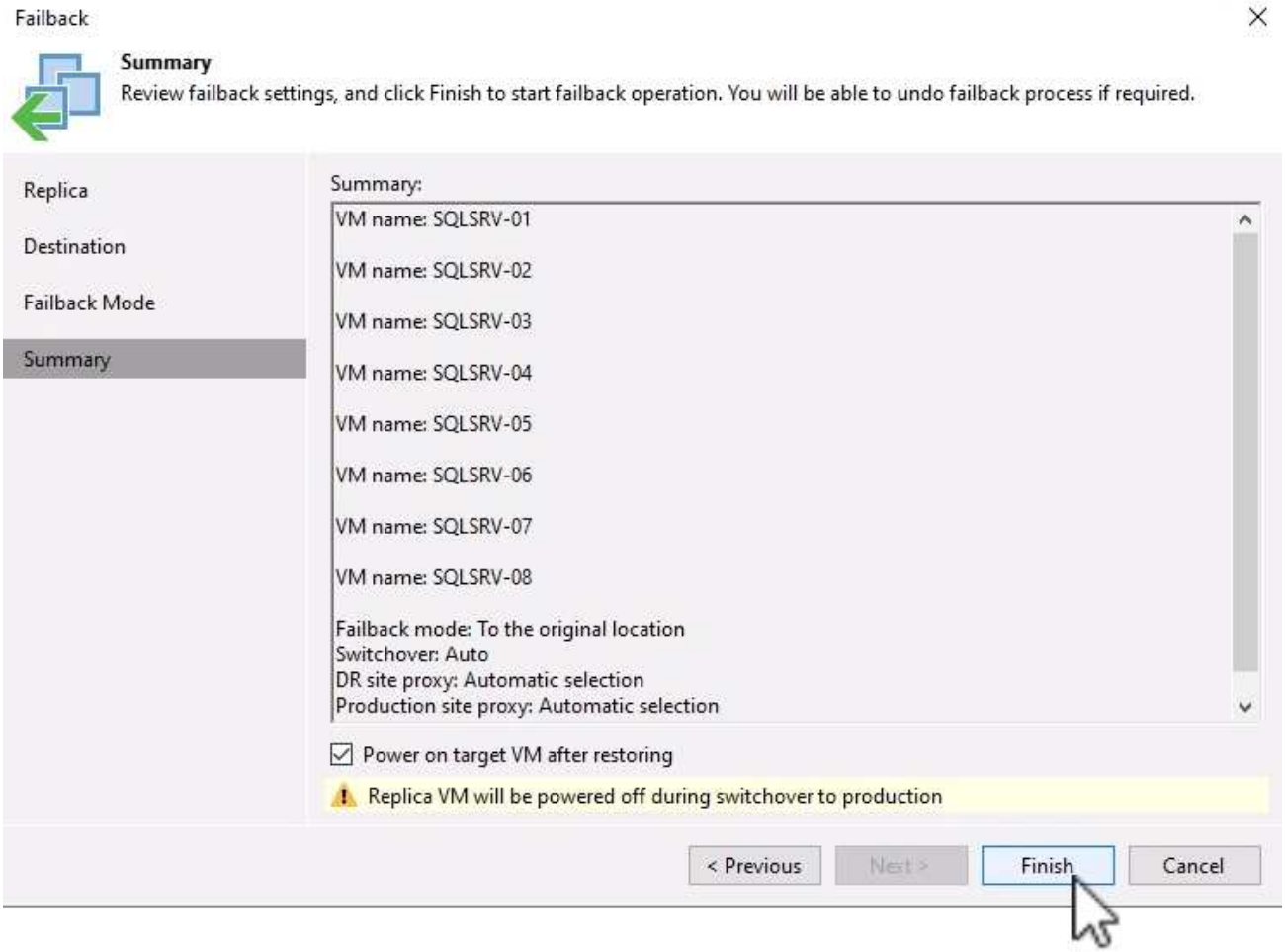
2. Nella pagina **Replica** della procedura guidata **Failback**, selezionare le repliche da includere nel processo di failback.
3. Nella pagina **Destinazione**, seleziona **Failback sulla VM originale** e fai clic su **Avanti** per continuare.



4. Nella pagina **Modalità failback**, seleziona **Auto** per avviare il failback il prima possibile.

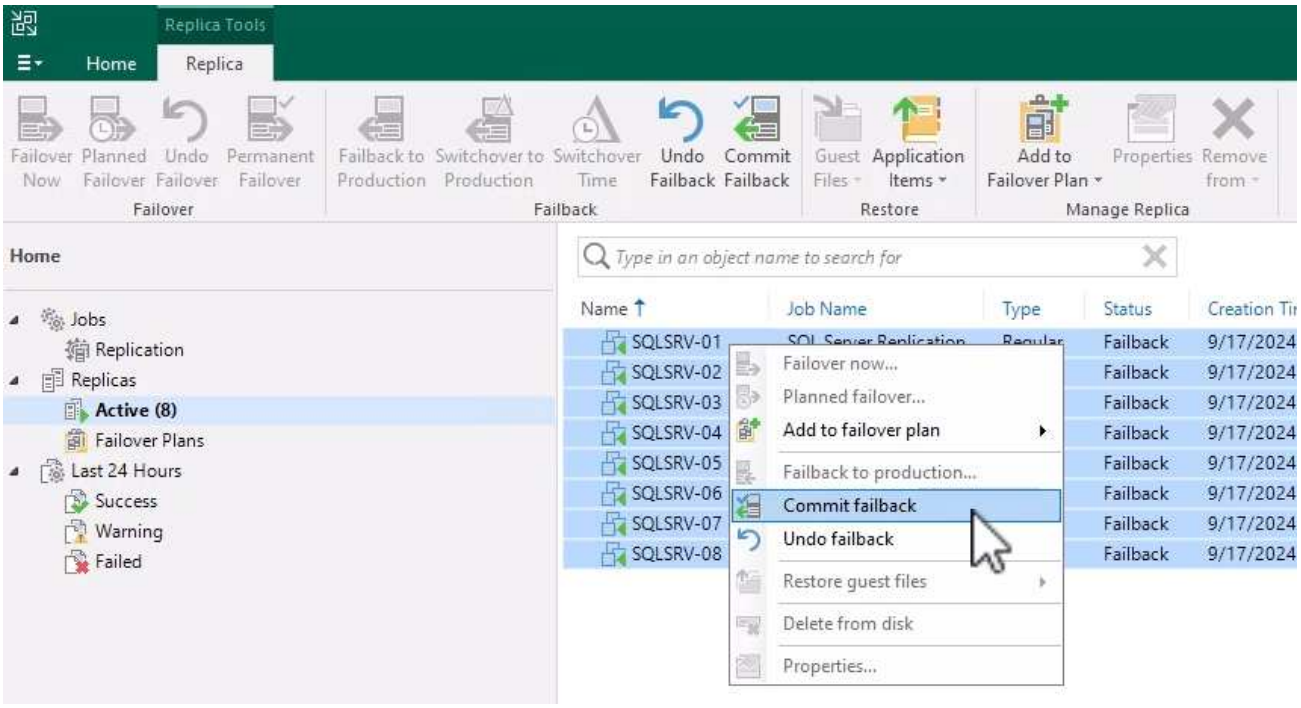


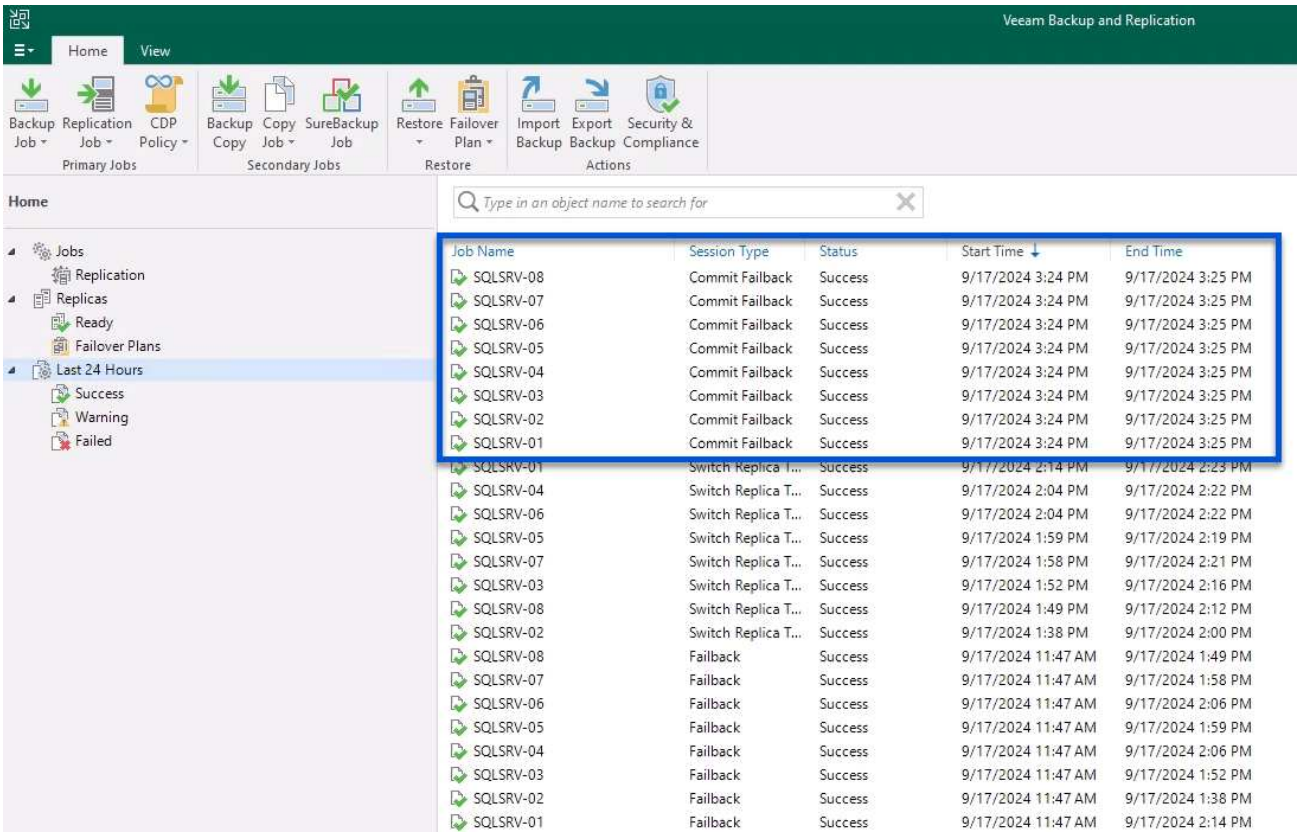
5. Nella pagina **Riepilogo**, scegli se **Accendere la macchina virtuale di destinazione dopo il ripristino** e quindi fai clic su Fine per avviare il processo di failback.



Il commit di failback finalizza l'operazione di failback, confermando la corretta integrazione delle modifiche nella VM di produzione. Dopo il commit, Veeam Backup & Replication riprende le normali attività di replica per la VM di produzione ripristinata. Ciò modifica lo stato della replica ripristinata da *Failback* a *Ready*.

1. Per eseguire il failback, vai su **Repliche > Attive**, seleziona le VM da eseguire, fai clic con il pulsante destro del mouse e seleziona **Esegui failback**.





Una volta completato il failback in produzione, tutte le VM vengono ripristinate nel sito di produzione originale.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per"Failover e failback per la replica" .

Conclusione

La funzionalità del datastore di Google Cloud NetApp Volumes consente a Veeam e ad altri strumenti di terze parti convalidati di fornire soluzioni di disaster recovery (DR) convenienti. Utilizzando cluster di luci pilota anziché grandi cluster dedicati per le repliche delle VM, le organizzazioni possono ridurre significativamente le spese. Questo approccio consente strategie di disaster recovery personalizzate che sfruttano le soluzioni di backup interne esistenti per il disaster recovery basato su cloud, eliminando la necessità di data center locali aggiuntivi. In caso di disastro, il failover può essere avviato con un solo clic o configurato per avvenire automaticamente, garantendo la continuità aziendale con tempi di inattività minimi.

Per saperne di più su questo processo, non esitate a seguire il video tutorial dettagliato.

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

Migrazione dei carichi di lavoro su GCP/GCVE

Migrazione dei carichi di lavoro al datastore Google Cloud NetApp Volumes su Google Cloud VMware Engine utilizzando VMware HCX - Guida introduttiva

Uno dei casi d'uso 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 fornisce vari meccanismi di migrazione per spostare le macchine virtuali (VM) locali e i relativi dati nei datastore NFS di Cloud Volume Service.

Panoramica: migrazione di macchine virtuali con VMware HCX, datastore Google Cloud NetApp Volumes e Google Cloud VMware Engine (GCVE)

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento del carico di lavoro e persino la continuità aziendale tra i cloud. È incluso come parte di Google Cloud VMware Engine Private Cloud e offre numerose modalità per migrare i carichi di lavoro e può essere utilizzato per operazioni di disaster recovery (DR).

Questo documento fornisce una guida dettagliata per il provisioning del datastore di Cloud Volume Service, seguito dal download, dalla distribuzione e dalla configurazione di VMware HCX, inclusi tutti i suoi componenti principali in locale e sul lato Google Cloud VMware Engine, tra cui Interconnect, Network Extension e ottimizzazione WAN per abilitare vari meccanismi di migrazione delle VM.

> VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione avviene a livello di VM. Pertanto, il presente documento è applicabile ai clienti NetApp esistenti e NetApp che intendono implementare Cloud Volume Service con Google Cloud VMware Engine per un'implementazione cloud VMware conveniente.

▼ **gradini di alto livello**

Questo elenco fornisce i passaggi di alto livello necessari per associare e migrare le VM a HCX Cloud Manager sul lato Google Cloud VMware Engine da HCX Connector in locale:

1. Preparare HCX tramite il portale Google VMware Engine.
2. Scarica e distribuisci il programma di installazione di HCX Connector Open Virtualization Appliance (OVA) nel VMware vCenter Server locale.
3. Attiva HCX con la chiave di licenza.
4. Associa VMware HCX Connector on-premise a Google Cloud VMware Engine HCX Cloud Manager.

5. Configurare il profilo di rete, il profilo di elaborazione e il service mesh.
6. (Facoltativo) Eseguire l'estensione di rete per evitare il re-IP durante le migrazioni.
7. Convalidare lo stato dell'appliance e assicurarsi che la migrazione sia possibile.
8. Migrare i carichi di lavoro delle VM.

▼ Prerequisiti

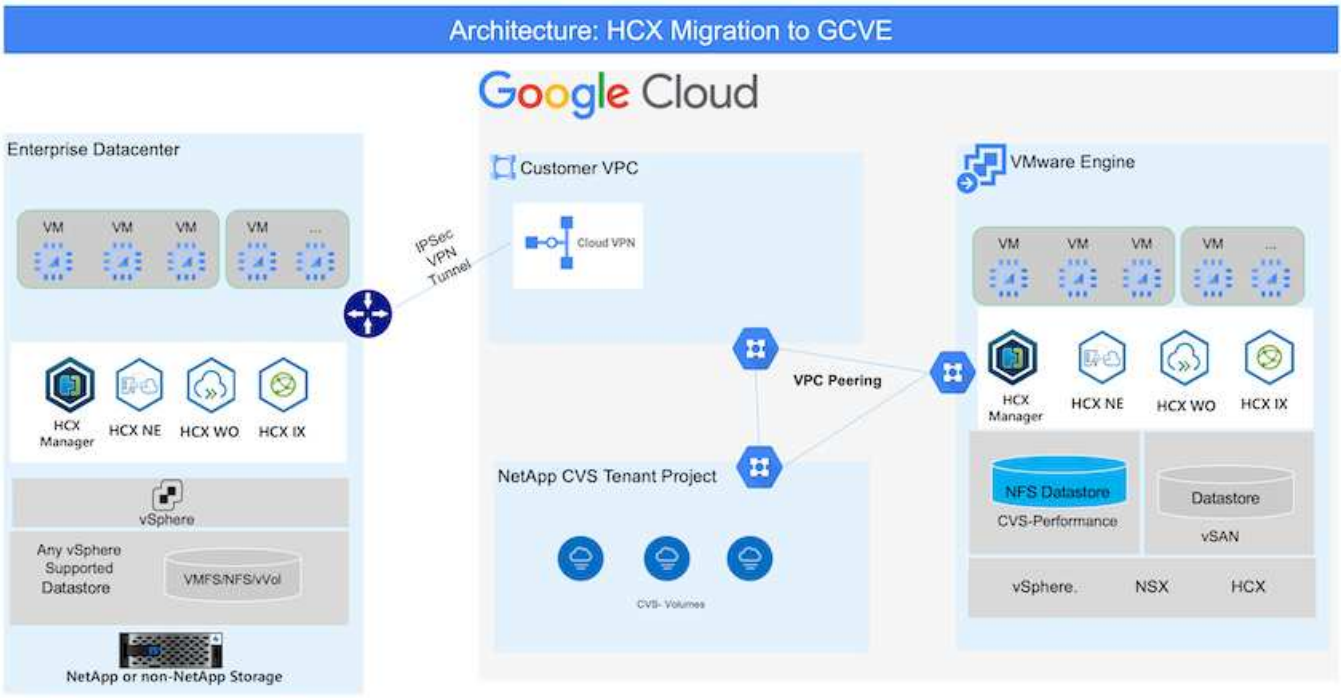
Prima di iniziare, assicurati che siano soddisfatti i seguenti prerequisiti. Per maggiori informazioni, vedere questo "collegamento" . Una volta soddisfatti i prerequisiti, inclusa la connettività, scarica la chiave di licenza HCX dal portale Google Cloud VMware Engine. Dopo aver scaricato il programma di installazione OVA, procedere con il processo di installazione come descritto di seguito.

> ⓘ HCX Advanced è l'opzione predefinita, mentre VMware HCX Enterprise Edition è disponibile anche tramite ticket di supporto e supportata senza costi aggiuntivi. Fare riferimento "questo collegamento"

- Utilizzare un data center software-defined (SDDC) Google Cloud VMware Engine esistente o creare un cloud privato utilizzando questo"Collegamento NetApp" o questo "Collegamento Google" .
- La migrazione delle VM e dei dati associati dal data center locale abilitato per VMware vSphere richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, "impostare 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 Google Cloud VMware Engine deve supportare la migrazione delle VM tramite vMotion.
- Assicurati che il necessario "regole e porte del firewall" sono consentiti per il traffico vMotion tra il vCenter Server locale e SDDC vCenter.
- Il volume NFS di Cloud Volume Service deve essere montato come datastore in Google Cloud VMware Engine. Seguire i passaggi dettagliati in questo "collegamento" per collegare i datastore di Cloud Volume Service agli host Google Cloud VMware Engines.

▼ Architettura di alto livello

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



Per maggiori dettagli sull'utilizzo di VMware HCX con Google, fare riferimento a "Collegamento VMware"

Distribuzione della soluzione

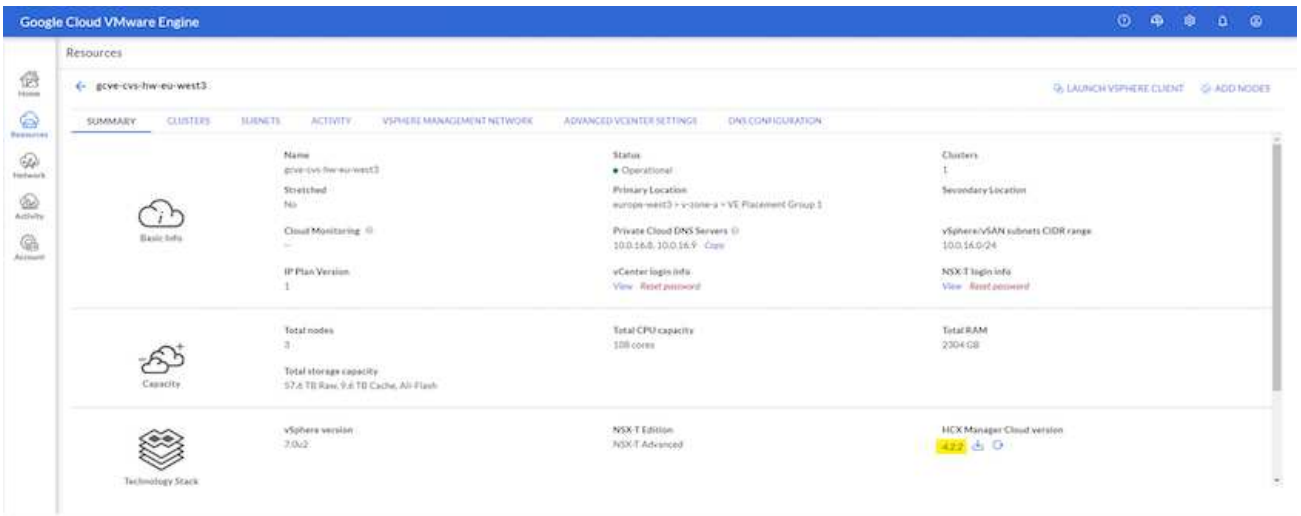
Per completare l'implementazione di questa soluzione, seguire la serie di passaggi:

▼ **Passaggio 1: preparare HCX tramite il portale Google VMware Engine**

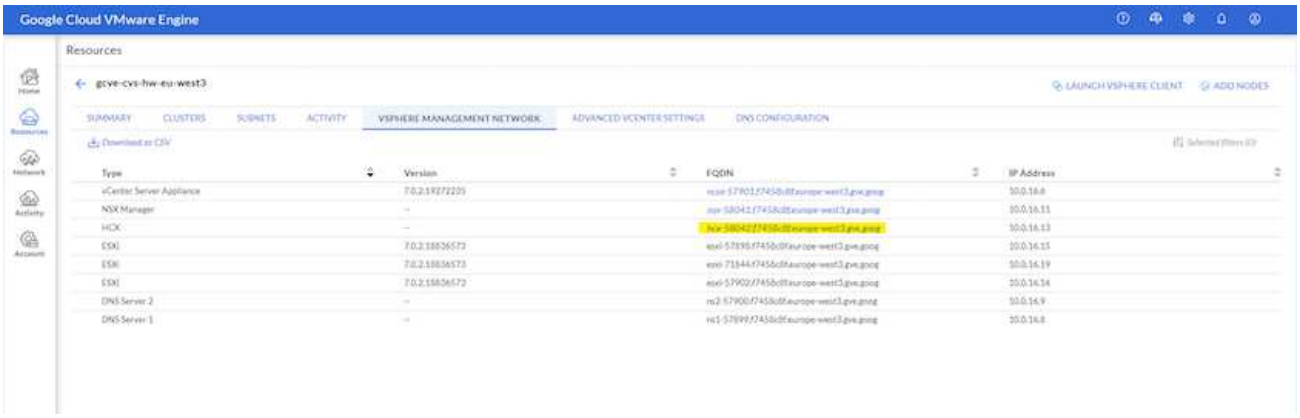
Il componente HCX Cloud Manager viene installato automaticamente quando si esegue il provisioning del cloud privato con VMware Engine. Per preparare l'associazione del sito, completare i seguenti passaggi:

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

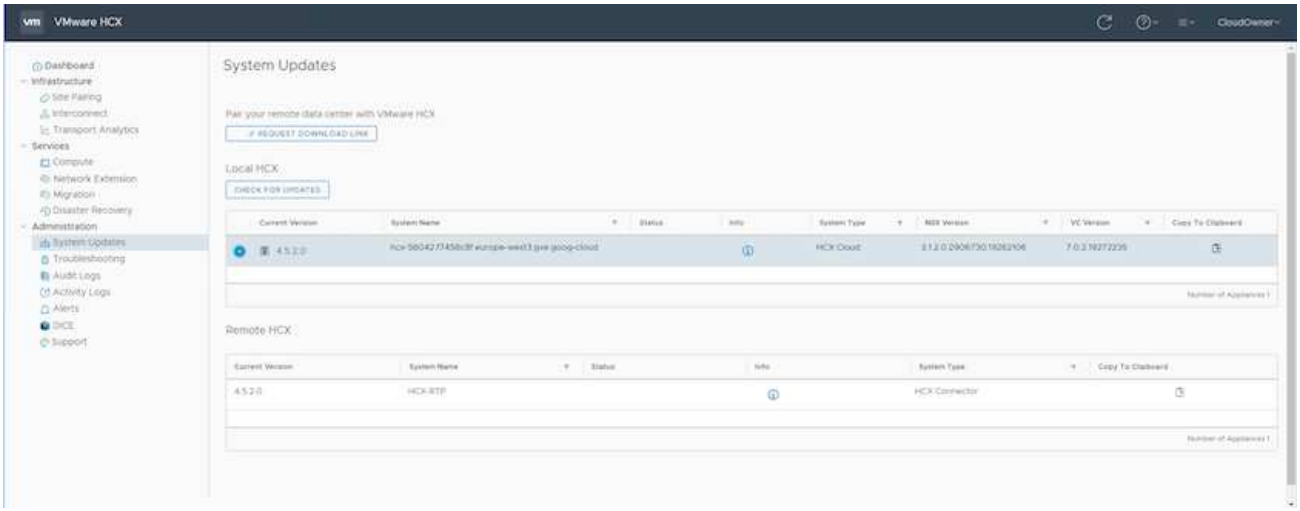
   Puoi accedere alla console HCX cliccando sul link della versione HCX



   oppure facendo clic su HCX FQDN nella scheda vSphere Management Network.



2. In HCX Cloud Manager, vai su **Amministrazione > Aggiornamenti di sistema**.
3. Fare clic su **Richiedi collegamento per il download** e scaricare il file OVA.



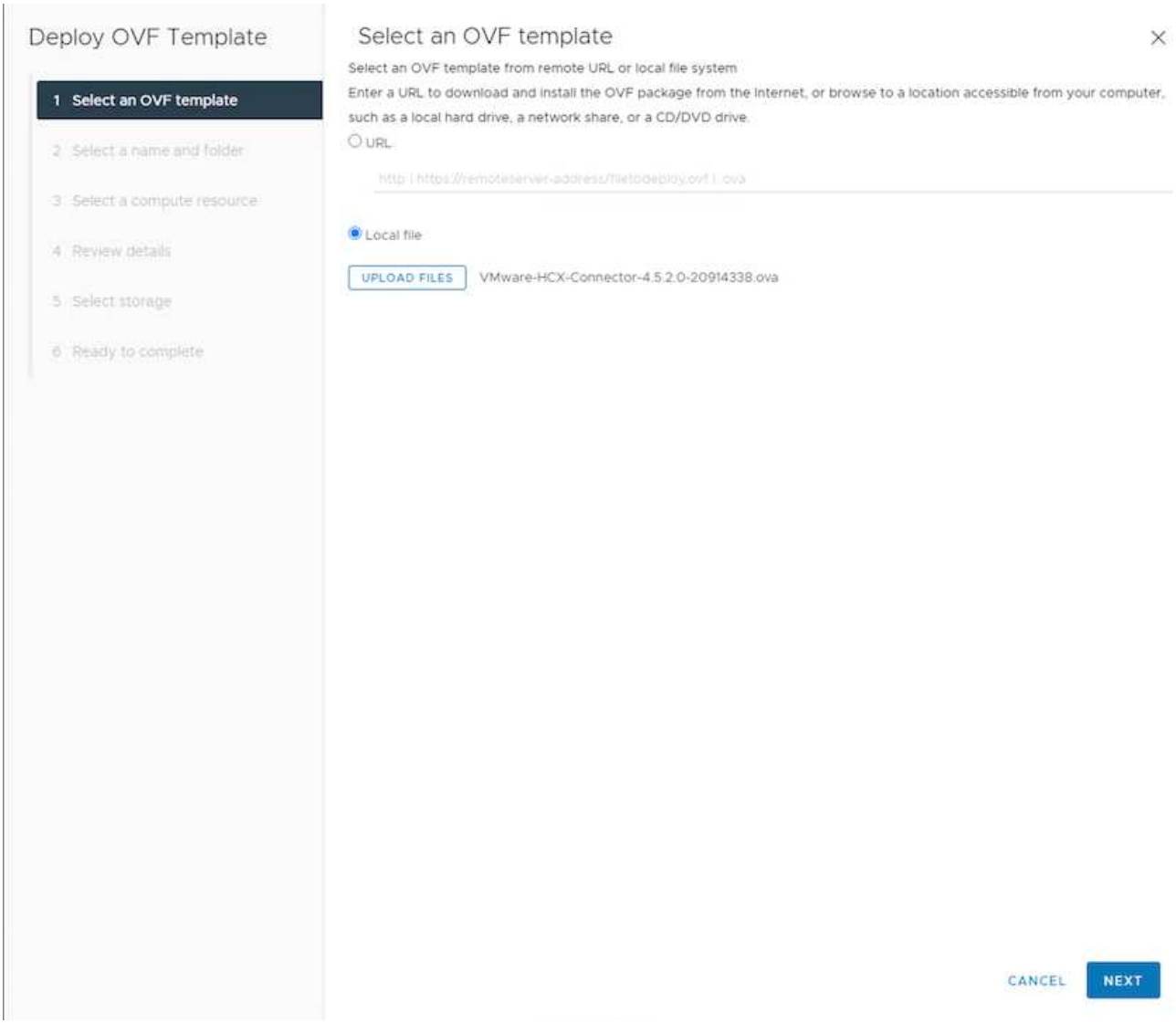
4. Aggiornare HCX Cloud Manager all'ultima versione disponibile dall'interfaccia utente di HCX Cloud Manager.

▼ **Passaggio 2: distribuire l'OVA del programma di installazione nel vCenter Server locale**

Per consentire al connettore on-premise di connettersi 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 vCenter Server locale, completare i seguenti passaggi:

1. Scaricare l'ova dalla console HCX su Google Cloud VMware Engine come indicato nel passaggio precedente.
2. Dopo aver scaricato l'OVA, distribuiscilo nell'ambiente VMware vSphere locale utilizzando l'opzione **Distribuisci modello OVF**.



3. Immettere tutte le informazioni richieste per la distribuzione OVA, fare clic su **Avanti**, quindi su **Fine** per distribuire il connettore VMware HCX OVA.

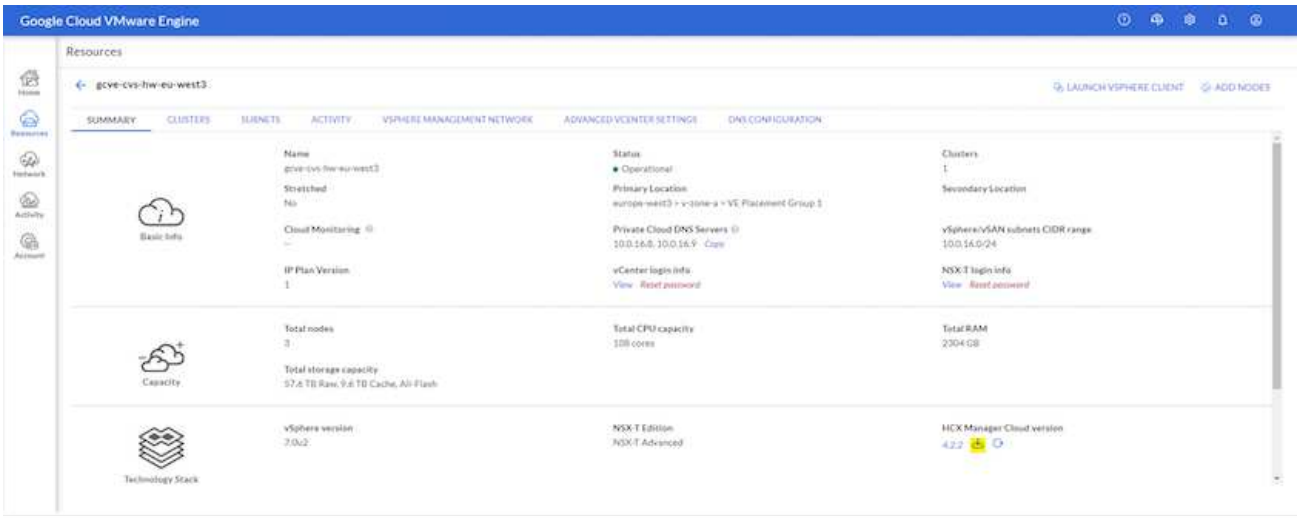
   Accendere manualmente l'appliance virtuale.

Per istruzioni dettagliate, vedere il "Documentazione di Google HCX" .

▼ **Passaggio 3: Attiva HCX Connector con la chiave di licenza**

Dopo aver distribuito VMware HCX Connector OVA in locale e avviato l'appliance, completare i seguenti passaggi per attivare HCX Connector. Genera la chiave di licenza dal portale Google Cloud VMware Engine e attivala in VMware HCX Manager.

1. Dal portale VMware Engine, fare clic su Risorse, selezionare il cloud privato e **fare clic sull'icona di download in HCX Manager Cloud Version**.



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

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

   Utilizzare l'hcxmanagerIP e la password definiti durante la distribuzione OVA.

3. Nella licenza, inserisci la chiave copiata dal passaggio 3 e clicca su **Attiva**.

   L'HCX Connector locale deve avere accesso a Internet.

4. In **Posizione del data center**, indicare la posizione più vicina per l'installazione di VMware HCX Manager in locale. Fare clic su **Continua**.
5. In **Nome sistema**, aggiorna il nome e fai clic su **Continua**.
6. Fare clic su **Sì, continua**.
7. In **Connetti il tuo vCenter**, fornisci il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fai clic su **Continua**.

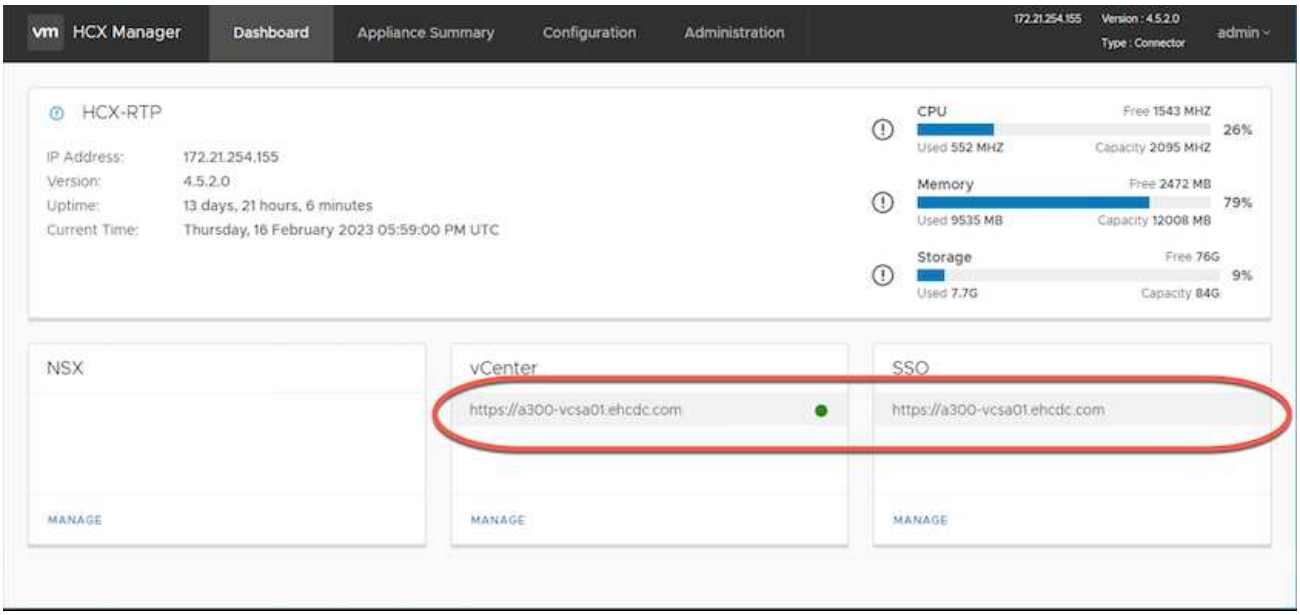
   Utilizzare l'FQDN per evitare problemi di connettività in seguito.

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

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

9. Verificare che le informazioni immesse siano corrette e fare clic su **Riavvia**.
10. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata. Sia vCenter Server che SSO devono disporre dei parametri di configurazione appropriati, che dovrebbero essere gli stessi della pagina precedente.

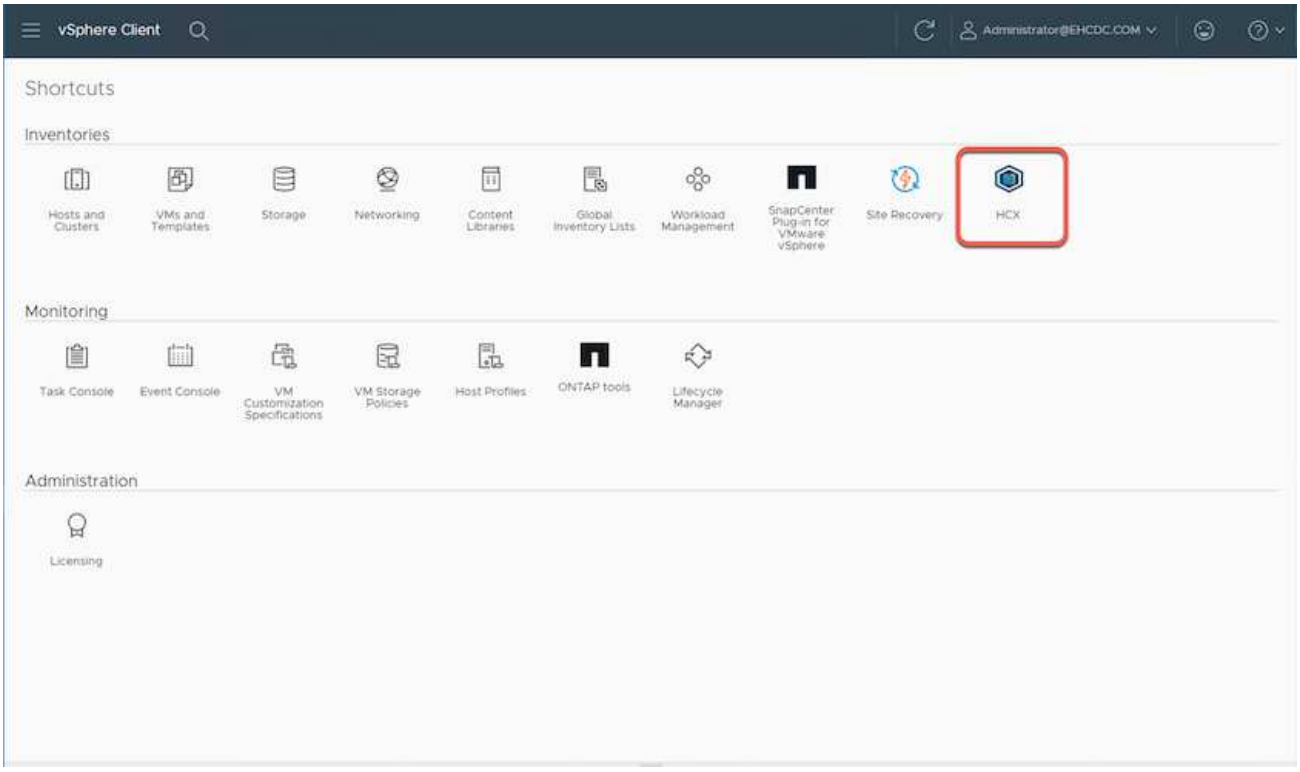
    Questo processo dovrebbe richiedere circa 10-20 minuti affinché il plug-in venga aggiunto al vCenter Server.



▼ Passaggio 4: associare VMware HCX Connector on-premise a Google Cloud VMware Engine HCX Cloud Manager

Dopo aver distribuito e configurato HCX Connector su vCenter locale, stabilire la connessione a Cloud Manager aggiungendo l'associazione. Per configurare l'associazione dei siti, completare i seguenti passaggi:

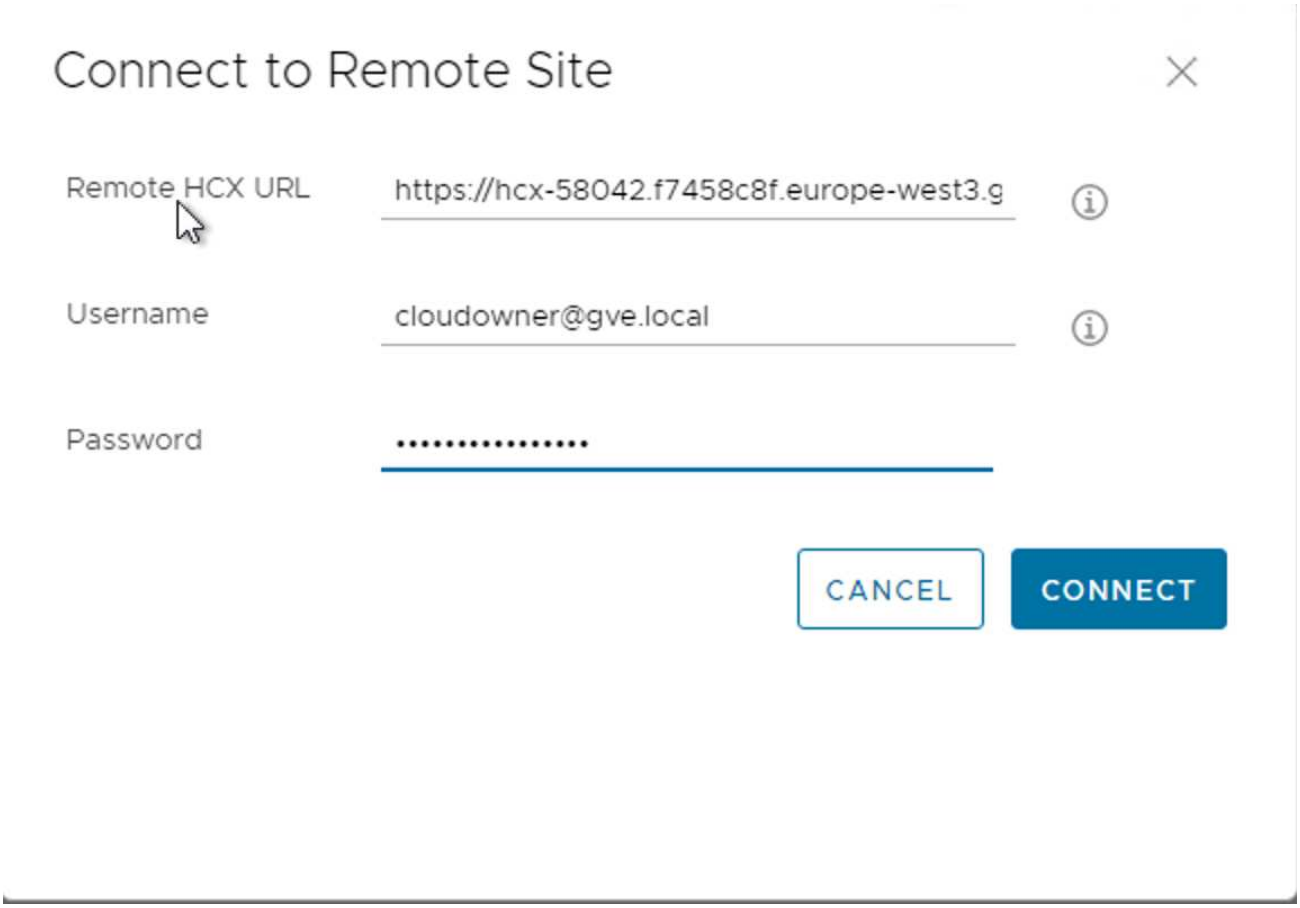
1. Per creare una coppia di siti tra l'ambiente vCenter on-premise e Google Cloud VMware Engine SDDC, accedi al vCenter Server on-premise e apri il nuovo plug-in HCX vSphere Web Client.



2. In Infrastruttura, fare clic su **Aggiungi un'associazione di siti**.

Immettere l'URL o l'indirizzo IP di Google Cloud VMware Engine HCX Cloud Manager e

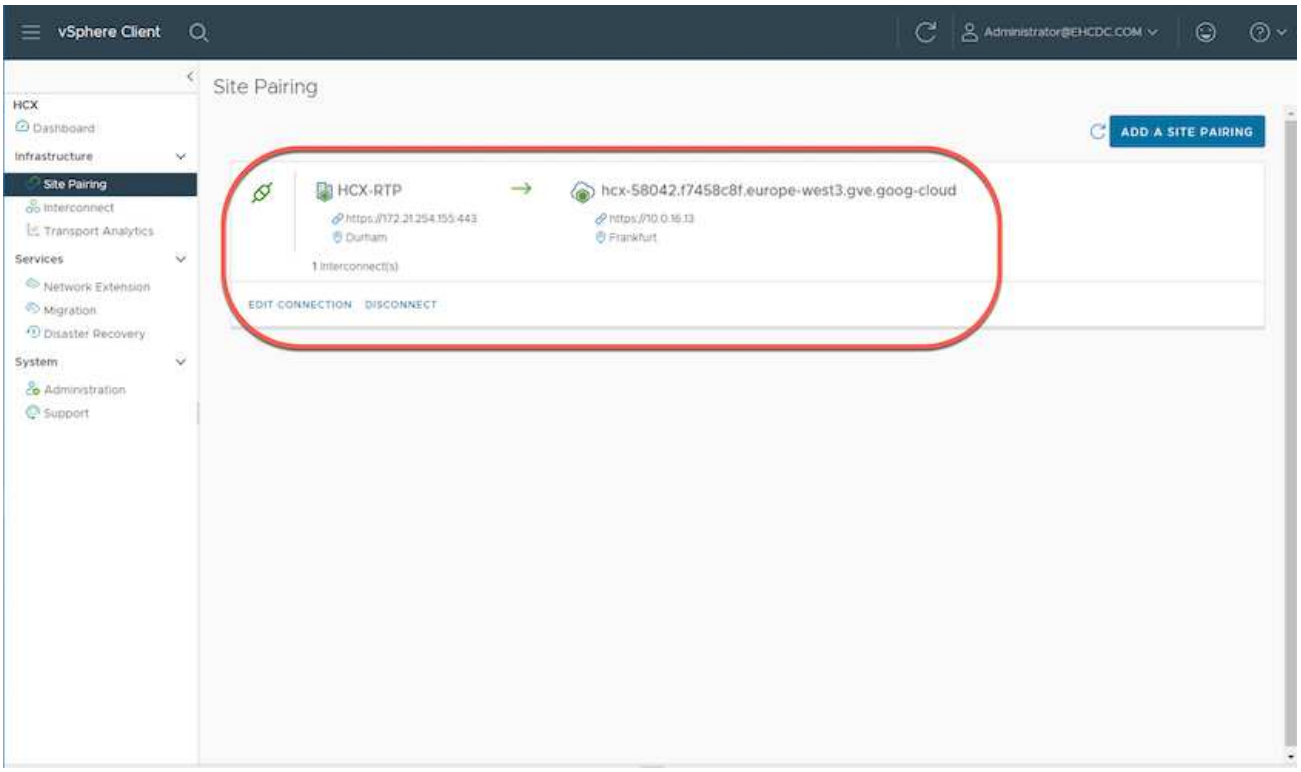
le credenziali dell'utente con privilegi Cloud-Owner-Role per accedere al cloud privato.



3. Fare clic su **Connetti**.

VMware HCX Connector deve essere in grado di indirizzare all'IP di HCX Cloud Manager tramite la porta 443.

4. Dopo aver creato l'associazione, l'associazione del sito appena configurata è disponibile sulla dashboard HCX.

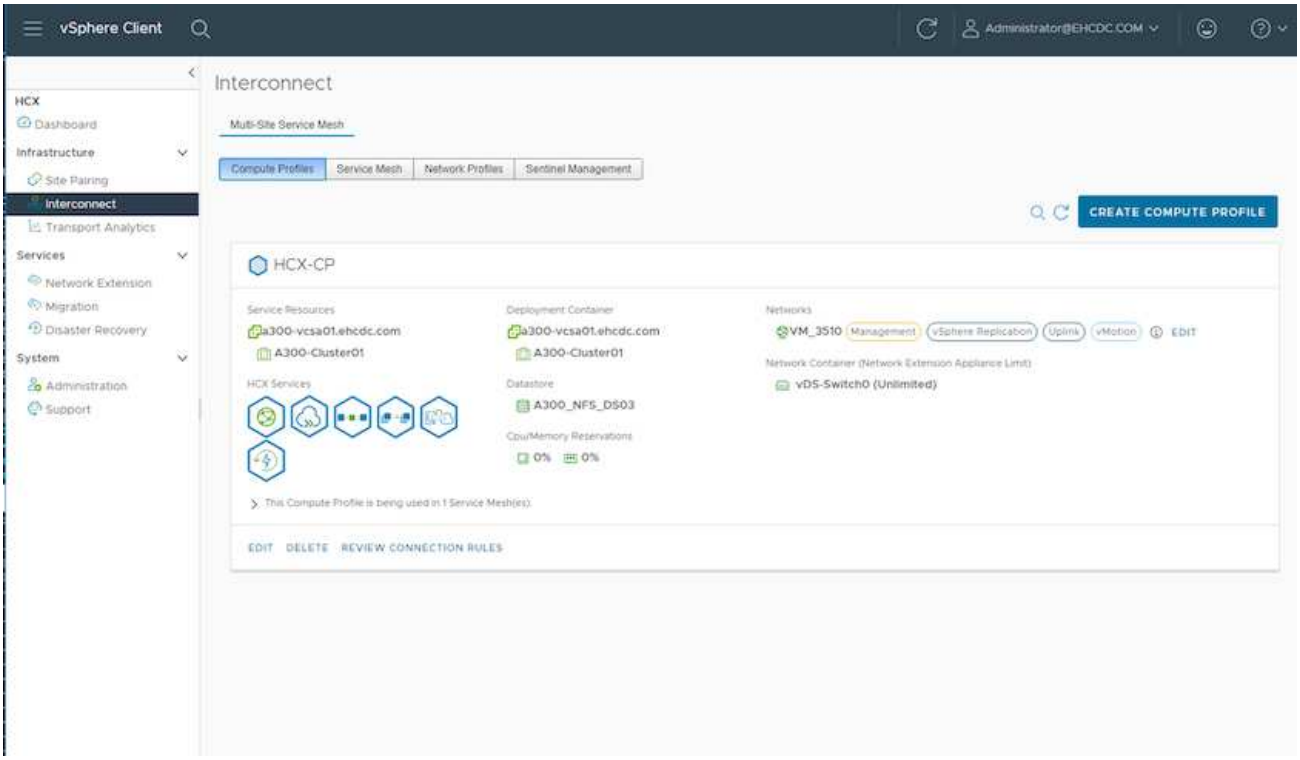


▼ **Passaggio 5: configurare il profilo di rete, il profilo di elaborazione e il service mesh**

L'appliance di servizi VMware HCX Interconnect fornisce funzionalità di replicazione e migrazione basate su vMotion tramite Internet e connessioni private al sito di destinazione. L'interconnessione fornisce crittografia, ingegneria del traffico e mobilità delle VM. Per creare un'appliance di servizi Interconnect, completare i seguenti passaggi:

1. In Infrastruttura, seleziona **Interconnessione > Multi-Site Service Mesh > Profili di calcolo > Crea profilo di calcolo**.

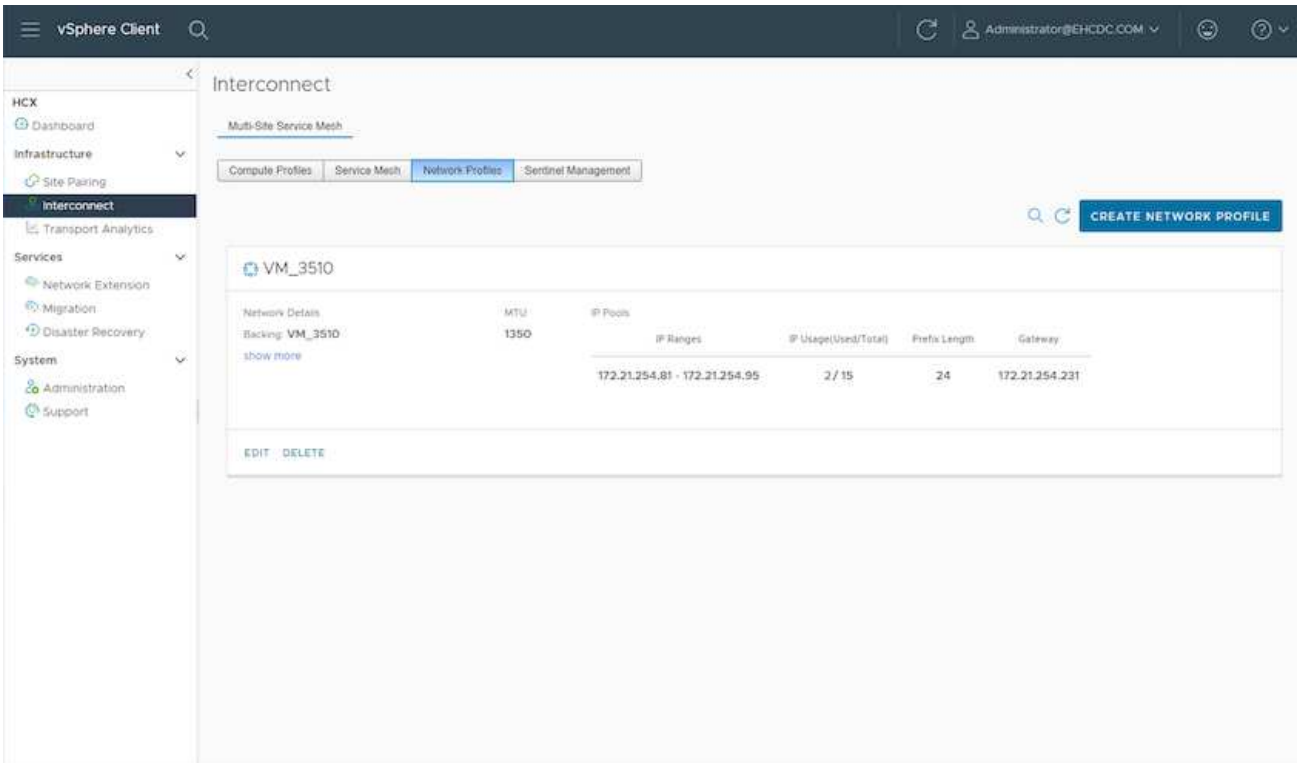
> I profili di calcolo definiscono i parametri di distribuzione, tra cui gli apparecchi distribuiti e la parte del data center VMware accessibile al servizio HCX.



2. Dopo aver creato il profilo di calcolo, creare i profili di rete selezionando **Multi-Site Service Mesh > Profili di rete > Crea profilo di rete**.

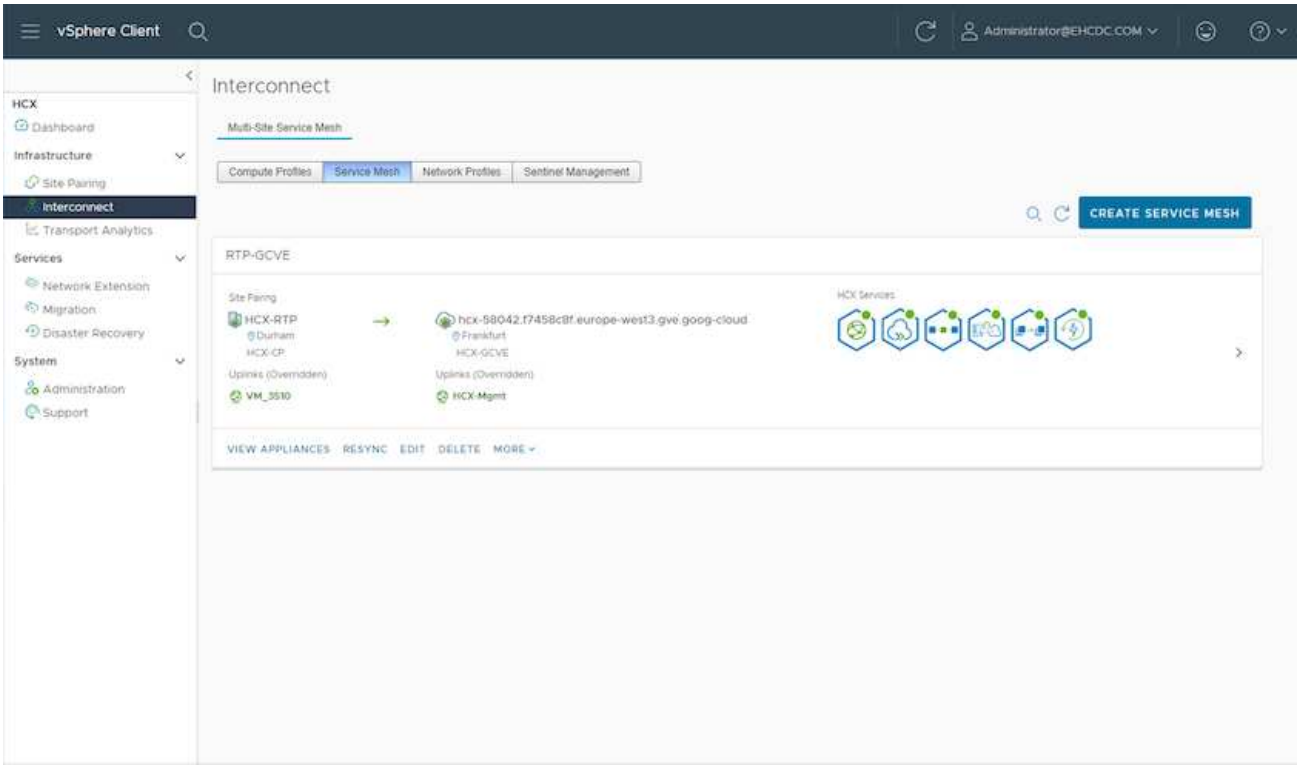
   Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati da HCX per i suoi dispositivi virtuali.

   > Per questo passaggio sono necessari due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione agli Interconnect Appliance.

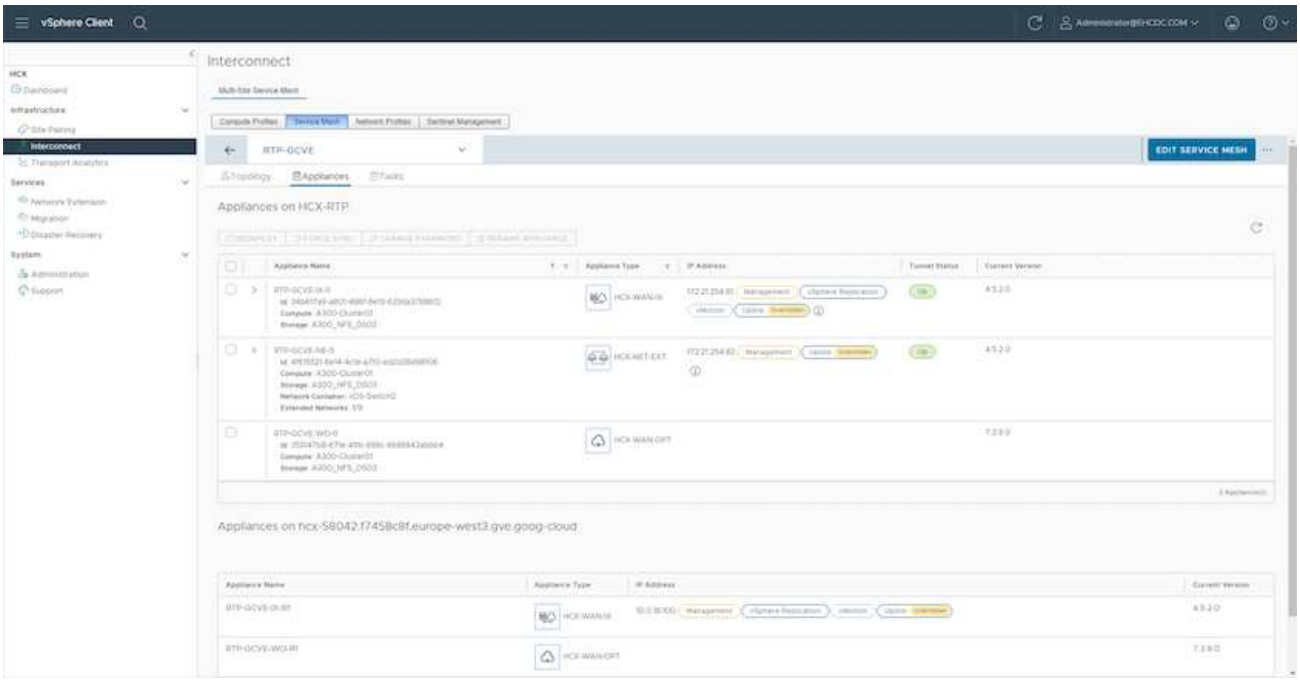


3. Al momento, i profili di calcolo e di rete sono stati creati correttamente.
4. Creare il Service Mesh selezionando la scheda **Service Mesh** nell'opzione **Interconnessione** e selezionare i siti SDDC locali e GCVE.
5. Service Mesh specifica una coppia di profili di rete e di elaborazione locali e remoti.

> Come parte di questo processo, gli appliance HCX vengono distribuiti e configurati automaticamente sia sul sito di origine che su quello di destinazione per creare un fabric di trasporto sicuro.



6. Questo è il passaggio finale della configurazione. Il completamento dell'implementazione dovrebbe richiedere circa 30 minuti. Dopo aver configurato il service mesh, l'ambiente è pronto con i tunnel IPsec creati correttamente per migrare le VM del carico di lavoro.



▼ Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati in modo bidirezionale tra SDDC locali e GCVE utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso entità attivate da VMware HCX utilizzando più tecnologie di migrazione, quali migrazione in blocco HCX, HCX vMotion, migrazione a freddo HCX, HCX Replication Assisted vMotion (disponibile con l'edizione HCX Enterprise) e migrazione assistita del sistema operativo HCX (disponibile con l'edizione HCX Enterprise).

Per saperne di più sui vari meccanismi di migrazione HCX, vedere "Documentazione sulla migrazione di VM VMware tramite VMware HCX" .

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

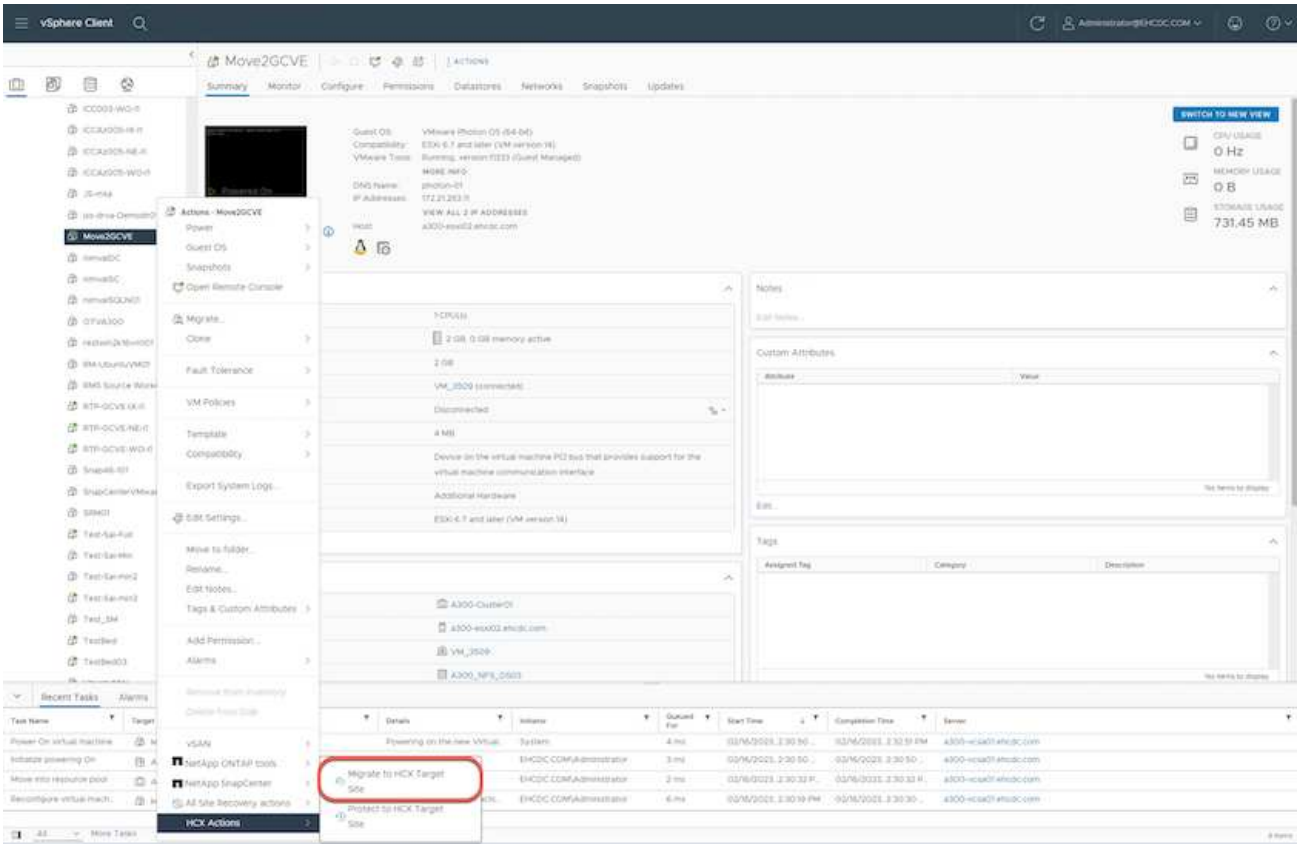
> ⓘ L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host nel vCenter Server. Le risorse di processore, memoria, storage e rete visualizzate su questo oggetto non rappresentano il consumo effettivo sull'hypervisor fisico che ospita l'appliance IX.

HCX vMotion

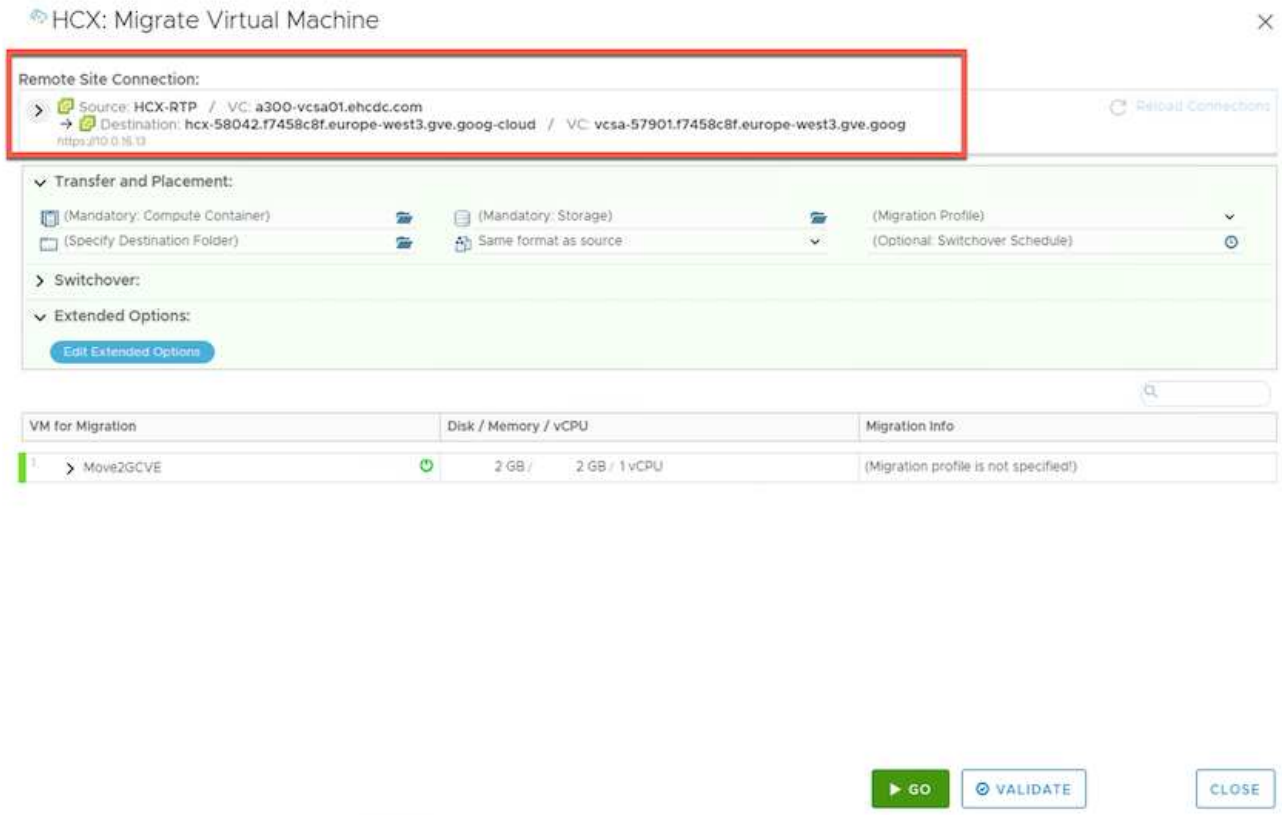
Questa sezione descrive il meccanismo HCX vMotion. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una VM a GCVE. L'opzione di migrazione vMotion viene utilizzata per migrare lo stato di una singola VM alla volta. Durante questo metodo di migrazione non si verifica alcuna interruzione del servizio.

> ⓘ È necessario che sia presente un'estensione di rete (per il gruppo di porte a cui è collegata la VM) per poter migrare la VM senza dover modificare l'indirizzo IP.

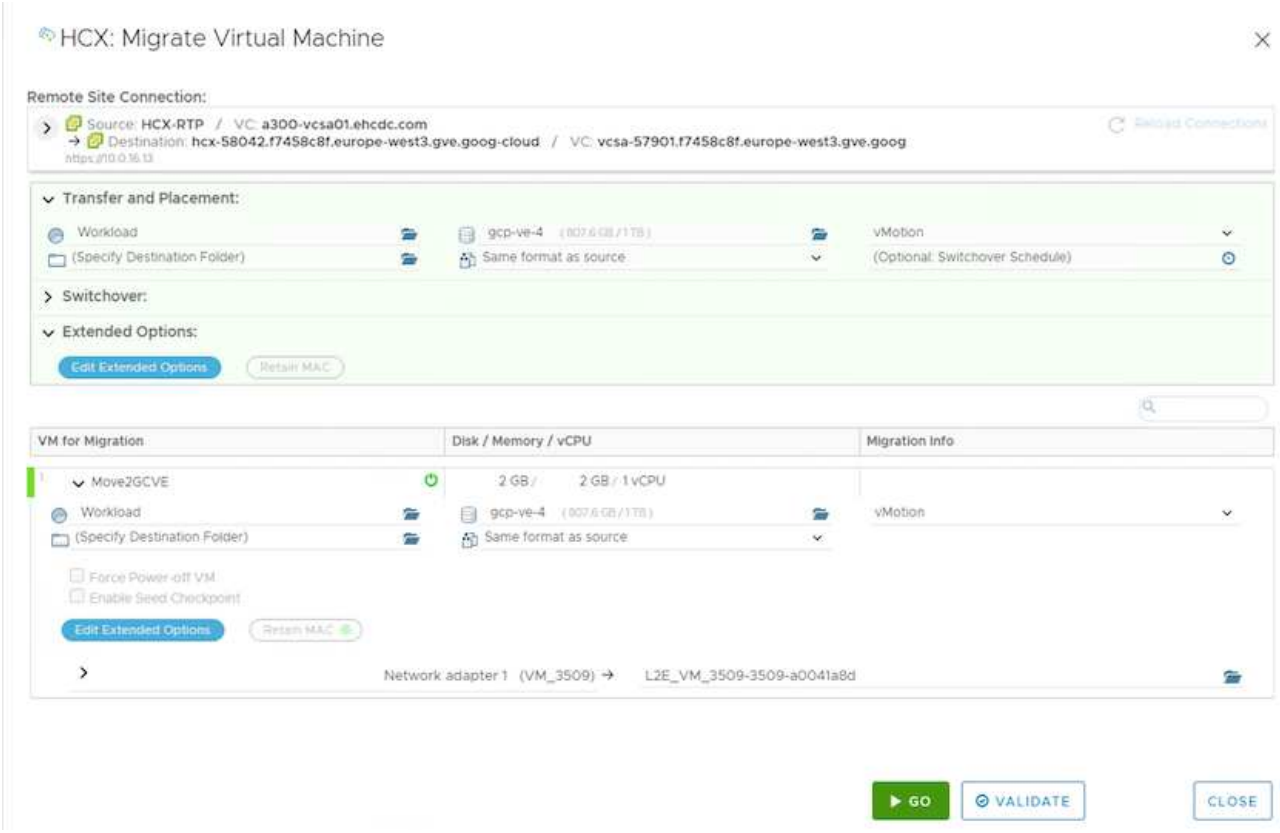
1. Dal client vSphere on-premise, vai su Inventario, fai clic con il pulsante destro del mouse sulla VM da migrare e seleziona Azioni HCX > Migra al sito di destinazione HCX.



2. Nella procedura guidata Migra macchina virtuale, selezionare la connessione al sito remoto (GCVE di destinazione).



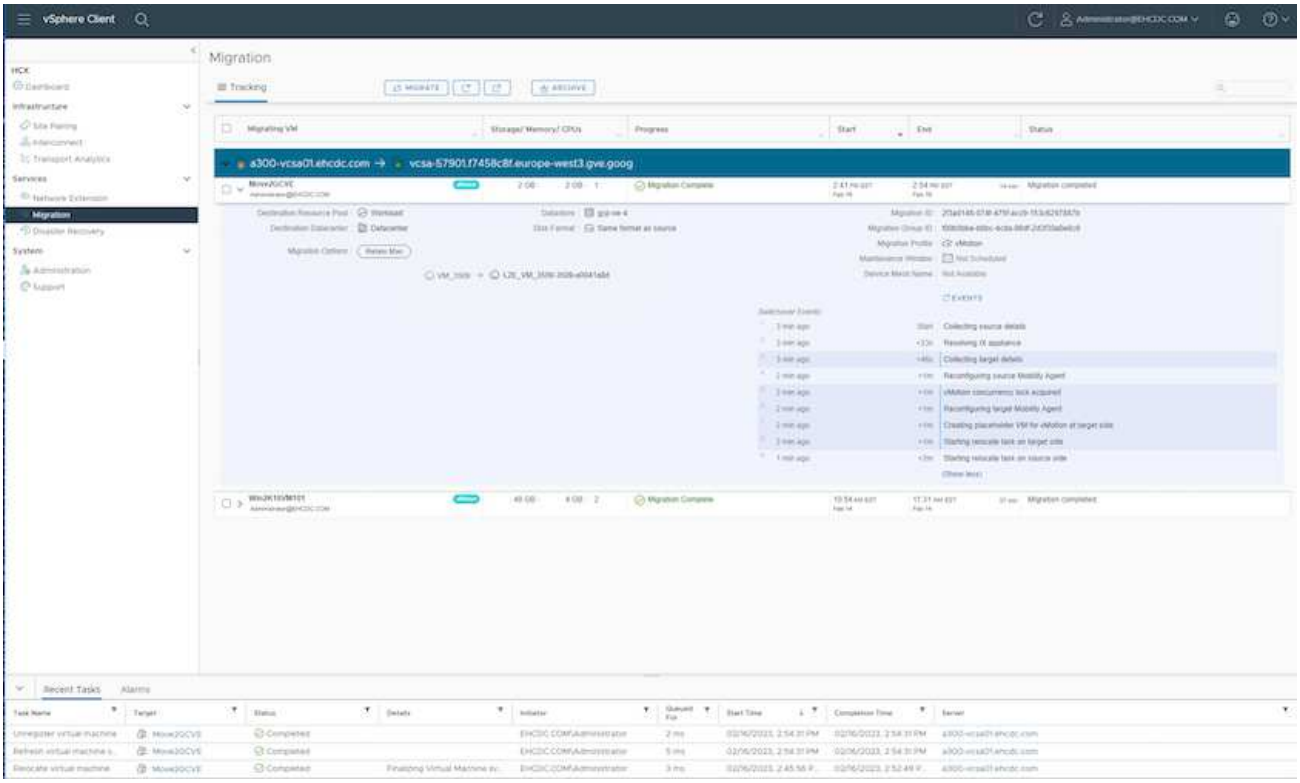
3. Aggiornare i campi obbligatori (Cluster, Storage e Rete di destinazione), quindi fare clic su Convalida.



4. Una volta completati i controlli di convalida, fare clic su Vai per avviare la migrazione.

> Il trasferimento vMotion cattura la memoria attiva della VM, il suo stato di esecuzione, il suo indirizzo IP e il suo indirizzo MAC. Per ulteriori informazioni sui requisiti e le limitazioni di HCX vMotion, vedere "Informazioni su VMware HCX vMotion e sulla migrazione a freddo" .

5. È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migrazione.



Il datastore NFS di destinazione Google Cloud NetApp Volumes (NetApp Volumes) deve disporre di spazio sufficiente per gestire la migrazione.

Conclusione

Che si punti a un cloud all-cloud o ibrido e che i dati risiedano su qualsiasi tipo/fornitore di storage in locale, Cloud Volume Service e HCX offrono ottime opzioni per distribuire e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO, rendendo i requisiti dei dati trasparenti per il livello applicativo. Qualunque sia il caso d'uso, scegli Google Cloud VMware Engine insieme a Cloud Volume Service per ottenere rapidamente i vantaggi del cloud, un'infrastruttura e operazioni coerenti su cloud locali e multipli, portabilità bidirezionale dei carichi di lavoro e capacità e prestazioni di livello aziendale. Si tratta dello stesso processo e delle stesse procedure note utilizzate per connettere lo storage e migrare le VM tramite VMware vSphere Replication, VMware vMotion o persino Network File Copy (NFC).

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'ambiente locale al datastore Cloud Volume Service.
- È possibile espandere e ridurre facilmente il datastore di Cloud Volume Service per soddisfare i requisiti di capacità e prestazioni durante l'attività di migrazione.

Video di Google e VMware come riferimento

▼ **Da Google**

- "Distribuisci HCX Connector con GCVE"
- "Configurare HCX ServiceMesh con GCVE"

- "Migrazione della VM con HCX a GCVE"

▼ **Da VMware**

- "Distribuzione del connettore HCX per GCVE"
- "Configurazione HCX ServiceMesh per GCVE"
- "Migrazione del carico di lavoro HCX a GCVE"

Dove trovare ulteriori informazioni

Per saperne di più sulle informazioni descritte nel presente documento, fare riferimento ai seguenti link del sito web:

- Documentazione di Google Cloud VMware Engine

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

- Documentazione del servizio Cloud Volume

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Guida utente VMware HCX

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

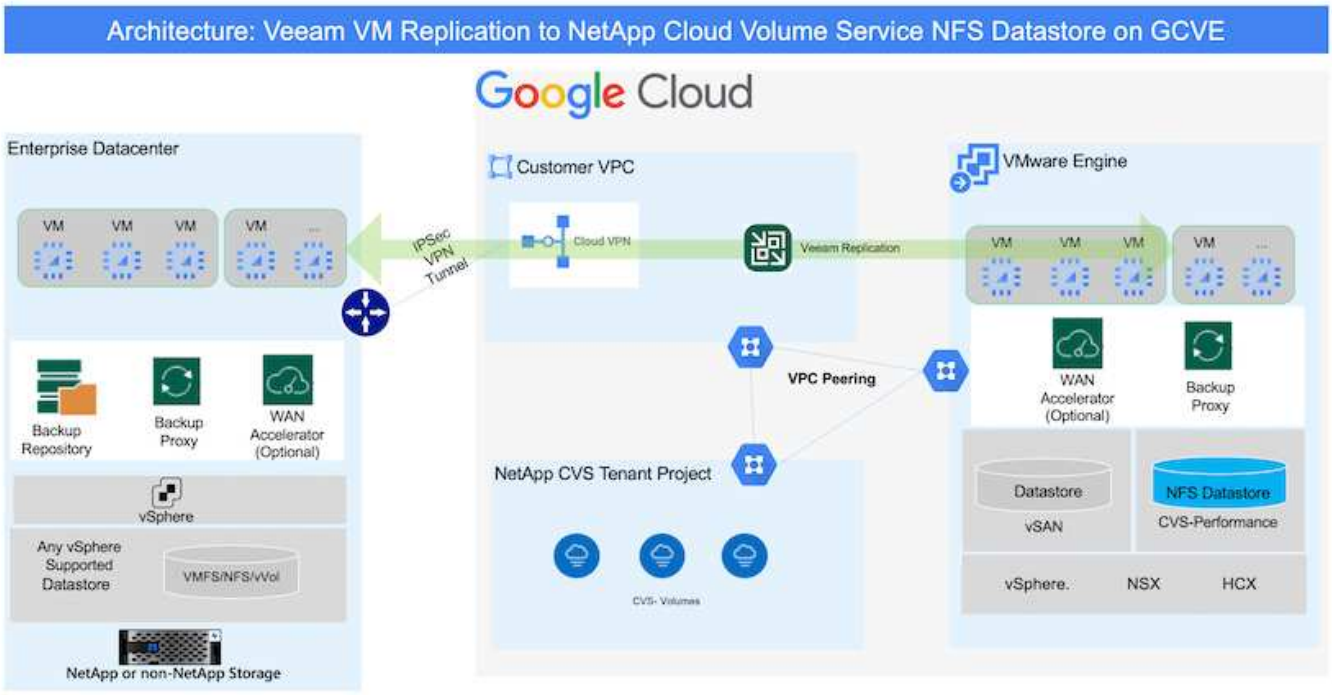
Migrazione della VM su Google Cloud NetApp Volumes NFS Datastore su Google Cloud VMware Engine utilizzando la funzionalità Veeam Replication

I clienti che attualmente utilizzano Veeam per le proprie esigenze di protezione dei dati continueranno a utilizzare questa soluzione per migrare i carichi di lavoro su GCVE e sfruttare i vantaggi dei datastore NFS Google Cloud NetApp Volumes .

Panoramica

I carichi di lavoro delle VM in esecuzione su VMware vSphere possono essere migrati su Google Cloud VMware Engine (GCVE) utilizzando la funzionalità Veeam Replication.

Questo documento fornisce un approccio passo passo per configurare ed eseguire la migrazione di VM che utilizza Google Cloud NetApp Volumes, Veeam e Google Cloud VMware Engine (GCVE).



Ipotesi

Questo documento presuppone che tu abbia a disposizione Google Cloud VPN, Cloud Interconnect o altre opzioni 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 locali a Google Cloud, il che ci impedisce di descrivere un flusso di lavoro specifico in questo documento. Fare riferimento al"Documentazione di Google Cloud" per il metodo di connettività on-premise-a-Google appropriato.

Distribuzione della soluzione di migrazione

Panoramica sulla distribuzione della soluzione

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

Dettagli di distribuzione

Assicurati che il datastore NFS di Google Cloud NetApp Volumes sia montato su GCVE vCenter

Accedi a GCVE vCenter e assicurati che sia disponibile un datastore NFS con spazio sufficiente. In caso contrario, fare riferimento"Montare i volumi NetApp come datastore NFS su GCVE"

Assicurarsi che Veeam Backup Recovery sia distribuito sull'ambiente VMware vSphere esistente

Si prega di fare riferimento"Componenti di replicazione Veeam" documentazione per installare i componenti richiesti.

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

Sia vCenter on-premise che vCenter GCVE devono essere registrati con Veeam. "Configurazione del processo di replica della VM vSphere" Ecco un video che spiega come"Configurare il processo di replica" .

> La VM replica può avere un IP diverso dalla VM di origine e può anche essere connessa a un gruppo di porte diverso. Per maggiori dettagli, guarda il video qui sopra.

Eseguire il failover del processo di replica di Veeam

Per migrare le VM, eseguire"Eseguire il failover"

Eseguire il failover permanente su Veeam.

Per trattare GCVE come il nuovo ambiente sorgente, eseguire"Failover permanente"

Vantaggi di questa soluzione

- Per la migrazione è possibile utilizzare l'infrastruttura di backup Veeam esistente.
- Veeam Replication consente di modificare gli indirizzi IP delle VM sul sito di destinazione.
- Ha la capacità di rimappare i dati esistenti replicati al di fuori di Veeam (come i dati replicati dal sistema NetApp)
- Ha la possibilità di specificare diversi gruppi di porte di rete sul sito di destinazione.
- È possibile specificare l'ordine di accensione delle VM.
- Utilizza VMware Change Block Tracking per ridurre al minimo la quantità di dati da inviare sulla WAN.
- Capacità di eseguire script pre e post per la replica.
- Capacità di eseguire script pre e post per gli snapshot.

Proteggi i dati con Google Cloud NetApp Volumes in Google Cloud

TR-4918: Panoramica sulla sicurezza - Google Cloud NetApp Volumes in Google Cloud

Oliver Krause, Justin Parisi, NetApp

La sicurezza, soprattutto nel cloud dove l'infrastruttura è al di fuori del controllo degli amministratori dello storage, è fondamentale per affidare i propri dati ai servizi offerti dai provider di cloud. Questo documento fornisce una panoramica delle offerte di sicurezza che "Google Cloud NetApp Volumes fornisce in Google Cloud".

Pubblico di destinazione

Il pubblico a cui è destinato il presente documento include, a titolo esemplificativo ma non esaustivo, i seguenti ruoli:

- Fornitori di cloud
- Amministratori di storage
- Architetti di stoccaggio
- Risorse sul campo
- decisori aziendali

Se avete domande sul contenuto di questo rapporto tecnico, consultate la sezione"Contattaci."

Abbreviazione	Definizione
NetApp Volumes-SW	Google Cloud NetApp Volumes, tipo di servizio NetApp Volumes
NetApp Volumes-Prestazioni	Cloud Volume Service, tipo di servizio NetApp Volumes-Performance
Annuncio di pubblica utilità	

Come Google Cloud NetApp Volumes in Google Cloud protegge i tuoi dati

Google Cloud NetApp Volumes in Google Cloud offre molteplici modi per proteggere i tuoi dati in modo nativo.

Architettura sicura e modello di locazione

Google Cloud NetApp Volumes fornisce un'architettura sicura in Google Cloud segmentando la gestione dei servizi (piano di controllo) e l'accesso ai dati (piano dati) su endpoint diversi in modo che nessuno dei due possa avere un impatto sull'altro (vedere la sezione"Architettura Google Cloud NetApp Volumes"). Utilizza Google "accesso ai servizi privati" (PSA) quadro per fornire il servizio. Questo framework distingue tra il produttore del servizio, fornito e gestito da NetApp, e il consumatore del servizio, che è un Virtual Private Cloud (VPC) in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni file di Google Cloud NetApp Volumes .

In questa architettura, gli inquilini (vedere la sezione"Modello di locazione") sono definiti come progetti Google Cloud completamente isolati l'uno dall'altro, a meno che non siano esplicitamente connessi dall'utente. I tenant consentono l'isolamento completo dei volumi di dati, dei servizi di denominazione esterni e di altri elementi essenziali della soluzione dagli altri tenant utilizzando la piattaforma di volumi Google Cloud NetApp Volumes . Poiché la piattaforma Google Cloud NetApp Volumes è connessa tramite peering VPC, anche a essa si applica tale isolamento. È possibile abilitare la condivisione dei volumi Google Cloud NetApp Volumes tra più progetti utilizzando una VPC condivisa (vedere la sezione"VPC condivise"). È possibile applicare controlli di accesso alle condivisioni SMB e alle esportazioni NFS per limitare chi o cosa può visualizzare o modificare i set di dati.

Gestione solida dell'identità per il piano di controllo

Nel piano di controllo in cui avviene la configurazione di Google Cloud NetApp Volumes , la gestione delle identità viene gestita utilizzando "Gestione dell'accesso all'identità (IAM)" . IAM è un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (permessi) per le istanze dei progetti Google Cloud. Tutta la configurazione viene eseguita con le API Google Cloud NetApp Volumes tramite un trasporto HTTPS sicuro utilizzando la crittografia TLS 1.2, mentre l'autenticazione viene eseguita tramite token JWT per una maggiore sicurezza. L'interfaccia utente della console Google per Google Cloud NetApp Volumes traduce l'input dell'utente in chiamate API Google Cloud NetApp Volumes .

Rafforzamento della sicurezza - Limitazione delle superfici di attacco

Una parte efficace della sicurezza consiste nel limitare il numero di superfici di attacco disponibili in un servizio. Le superfici di attacco possono includere vari elementi, tra cui dati inattivi, trasferimenti in corso, accessi e gli stessi set di dati.

Un servizio gestito rimuove alcune delle superfici di attacco intrinsecamente previste dalla sua progettazione. Gestione delle infrastrutture, 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 essere umano interviene effettivamente sulle configurazioni, il che contribuisce a ridurre il numero di errori intenzionali e non intenzionali. La rete è isolata in modo che solo i servizi necessari possano accedere l'uno all'altro. La crittografia è integrata nell'archiviazione dei dati e solo il piano dati necessita dell'attenzione degli amministratori Google Cloud NetApp Volumes in termini di sicurezza. Nascondendo la maggior parte della gestione dietro un'interfaccia API, la sicurezza viene raggiunta limitando le superfici di attacco.

Modello Zero Trust

Storicamente, la filosofia della sicurezza informatica è stata quella di fidarsi ma verificare, e si è manifestata affidandosi esclusivamente a meccanismi esterni (come firewall e sistemi di rilevamento delle intrusioni) per mitigare le minacce. Tuttavia, attacchi e violazioni si sono evoluti per aggirare la verifica negli ambienti attraverso phishing, ingegneria sociale, minacce interne e altri metodi che forniscono la verifica per entrare nelle reti e creare scompiglio.

Zero Trust è diventato una nuova metodologia di sicurezza, il cui mantra attuale è "non fidarsi di nulla e verificare comunque tutto". Pertanto, per impostazione predefinita, non è consentito alcun accesso. Questo mantra viene applicato in vari modi, tra cui firewall standard e sistemi di rilevamento delle intrusioni (IDS), nonché con i seguenti metodi:

- Metodi di autenticazione avanzati (come i token Kerberos crittografati AES o JWT)
- Singole fonti solide di identità (ad esempio Windows Active Directory, Lightweight Directory Access Protocol (LDAP) e Google IAM)
- Segmentazione della rete e multitenancy sicura (solo gli inquilini hanno accesso per impostazione predefinita)
- Controlli di accesso granulari con criteri di accesso con privilegi minimi
- Piccoli elenchi esclusivi di amministratori dedicati e fidati con audit digitale e tracciabilità cartacea

Google Cloud NetApp Volumes in esecuzione su Google Cloud aderisce al modello Zero Trust implementando il principio "non fidarti di nulla, verifica tutto".

Crittografia

Crittografare i dati a riposo (vedere la sezione"Crittografia dei dati a riposo") utilizzando cifrari XTS-AES-256 con NetApp Volume Encryption (NVE) e in volo con"Crittografia SMB" o supporto NFS Kerberos 5p. Puoi stare tranquillo sapendo che i trasferimenti di replica tra regioni sono protetti dalla crittografia TLS 1.2 (vedi la sezione "Replica tra regioni"). Inoltre, la rete Google fornisce anche comunicazioni crittografate (vedere la sezione"Crittografia dei dati in transito") per un ulteriore livello di protezione contro gli 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. Riguarda anche il modo in cui ci riprendiamo dagli attacchi, se e quando si verificano. Questa strategia include la protezione dei dati e i backup. Google Cloud NetApp Volumes fornisce metodi per replicare in altre regioni in caso di interruzioni (vedere la sezione"Replicazione interregionale") o se un set di dati è stato colpito da un attacco ransomware. Può anche

eseguire backup asincroni dei dati in posizioni esterne all'istanza di Google Cloud NetApp Volumes utilizzando"Backup Google Cloud NetApp Volumes" . Con backup regolari, la mitigazione degli eventi di sicurezza può richiedere meno tempo, facendo risparmiare denaro e stress agli amministratori.

Mitigazione rapida del ransomware con copie Snapshot leader del settore

Oltre alla protezione dei dati e ai backup, Google Cloud NetApp Volumes fornisce 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 il minimo disagio. I tempi e gli effetti del ripristino dipendono dalla pianificazione degli snapshot, ma è possibile creare copie snapshot che forniscono un delta di appena un'ora negli attacchi ransomware. Le copie snapshot hanno un effetto trascurabile sulle prestazioni e sull'utilizzo della capacità e rappresentano un approccio a basso rischio e ad alto rendimento per proteggere i set di dati.

Considerazioni sulla sicurezza e superfici di attacco

Il primo passo per capire come proteggere i propri dati è identificare i rischi e le potenziali superfici di attacco.

Tra questi rientrano (ma non sono limitati a) quanto segue:

- Amministrazione e accessi
- Dati a riposo
- Dati in volo
- Rete e firewall
- Ransomware, malware e virus

Comprendere le superfici di attacco può aiutarti a proteggere meglio i tuoi ambienti. Google Cloud NetApp Volumes in Google Cloud prende già in considerazione molti di questi argomenti e implementa la 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 dei malintenzionati violano le tue credenziali amministrative, hanno le chiavi del castello e possono fare tutto ciò che vogliono: modificare le configurazioni, eliminare volumi e backup, creare backdoor o disattivare le pianificazioni degli snapshot.

Google Cloud NetApp Volumes per Google Cloud offre protezione contro gli accessi amministrativi non autorizzati tramite l'offuscamento dello storage come servizio (StaaS). Google Cloud NetApp Volumes è completamente gestito dal provider cloud, senza possibilità di accesso esterno. Tutte le operazioni di installazione e configurazione sono completamente automatizzate, quindi un amministratore umano non deve mai interagire con i sistemi, se non in circostanze molto rare.

Se è richiesto l'accesso, Google Cloud NetApp Volumes in Google Cloud protegge gli accessi mantenendo un elenco molto breve di amministratori attendibili che hanno accesso ai sistemi. Questo controllo aiuta a ridurre il numero di potenziali malintenzionati che hanno accesso. Inoltre, la rete di Google Cloud nasconde i sistemi dietro livelli di sicurezza di rete ed espone al mondo esterno solo ciò che è necessario. Per informazioni sull'architettura di Google Cloud, Google Cloud NetApp Volumes , vedere la sezione"Architettura Google Cloud NetApp Volumes ."

Amministrazione e aggiornamenti del cluster

Due aree con potenziali rischi per la sicurezza includono l'amministrazione del cluster (cosa succede se un malintenzionato ha accesso amministrativo) e gli aggiornamenti (cosa succede se un'immagine software viene compromessa).

Protezione dell'amministrazione dello storage

L'archiviazione fornita come servizio elimina il rischio aggiuntivo di esposizione per gli amministratori, impedendo l'accesso agli utenti finali al di fuori del data center cloud. Invece, l'unica configurazione effettuata è quella relativa al piano di accesso ai dati da parte dei clienti. Ogni tenant gestisce i propri volumi e nessun tenant può raggiungere altre istanze Google Cloud NetApp Volumes . Il servizio è gestito dall'automazione, con un elenco molto ristretto di amministratori fidati a cui è concesso l'accesso ai sistemi attraverso i processi trattati nella sezione"Funzionamento del servizio."

Il tipo di servizio NetApp Volumes-Performance offre la replica tra regioni come opzione per fornire protezione dei dati a una regione diversa in caso di guasto di una regione. In questi casi, è possibile eseguire il failover Google Cloud NetApp Volumes nella regione non interessata per mantenere l'accesso ai dati.

Aggiornamenti del servizio

Gli aggiornamenti aiutano a proteggere i sistemi vulnerabili. Ogni aggiornamento apporta 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 di poter essere autorizzati, per verificare che vengano utilizzate immagini ufficiali e che gli aggiornamenti non siano compromessi da malintenzionati.

Con Google Cloud NetApp Volumes, gli aggiornamenti vengono gestiti dai team del provider cloud, il che elimina l'esposizione al rischio per i team di amministrazione, fornendo esperti esperti in configurazione e aggiornamenti che hanno automatizzato e completamente testato il processo. Gli aggiornamenti non interrompono le attività e Google Cloud NetApp Volumes mantiene gli aggiornamenti più recenti per garantire i migliori risultati complessivi.

Per informazioni sul team di amministratori che esegue questi aggiornamenti del servizio, vedere la sezione"Funzionamento del servizio."

Protezione dei dati a riposo

La crittografia dei dati a riposo è importante per proteggere i dati sensibili in caso di furto, restituzione o riutilizzo del disco. I dati in Google Cloud NetApp Volumes sono protetti quando sono inattivi mediante crittografia basata su software.

- Per NetApp Volumes-SW vengono utilizzate le chiavi generate da Google.
- Per NetApp Volumes-Performance, le chiavi per volume vengono archiviate in un gestore di chiavi integrato in Google Cloud NetApp Volumes, che utilizza NetApp ONTAP CryptoMod per generare chiavi di crittografia AES-256. CryptoMod è presente nell'elenco dei moduli convalidati CMVP FIPS 140-2. Vedere "Certificato FIPS 140-2 n. 4144" .

A partire da novembre 2021, la funzionalità di anteprima CMEK (Customer-managed Encryption) è stata resa disponibile per NetApp Volumes-Performance. Questa funzionalità consente di crittografare le chiavi per volume con chiavi master per progetto e per regione ospitate in Google Key Management Service (KMS). KMS consente di collegare gestori di chiavi esterni.

Per informazioni dettagliate su come configurare KMS per NetApp Volumes-Performance, "consultare la documentazione Google Cloud NetApp Volumes".

Per maggiori informazioni sull'architettura, vedere la sezione"Architettura Google Cloud NetApp Volumes ."

Protezione dei dati durante il trasporto

Oltre a proteggere i dati a riposo, è necessario essere in grado di proteggere i dati anche quando sono in transito tra l'istanza di Google Cloud NetApp Volumes e un client o una destinazione di replica. Google Cloud NetApp Volumes fornisce la crittografia per i dati in transito tramite protocolli NAS utilizzando metodi di crittografia quali la crittografia SMB tramite Kerberos, la firma/sigillatura dei pacchetti e NFS Kerberos 5p per la crittografia end-to-end dei trasferimenti di dati.

La replica dei volumi Google Cloud NetApp Volumes utilizza TLS 1.2, che sfrutta i metodi di crittografia AES-GCM.

La maggior parte dei protocolli di comunicazione in volo non sicuri, come telnet, NDMP e così via, sono disabilitati per impostazione predefinita. Tuttavia, il DNS non è crittografato da Google Cloud NetApp Volumes (nessun supporto DNS Sec) e, quando possibile, dovrebbe essere crittografato utilizzando la crittografia di rete esterna. Vedi la sezione"Crittografia dei dati in transito" per maggiori informazioni sulla protezione dei dati durante il trasporto.

Per informazioni sulla crittografia del protocollo NAS, vedere la sezione"Protocolli NAS."

Utenti e gruppi per i permessi NAS

Una parte della protezione dei dati nel cloud riguarda la corretta autenticazione 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 archiviazione.

Google Cloud NetApp Volumes utilizza l'autenticazione standard di utenti e gruppi Windows basata su Active Directory per le condivisioni SMB e le autorizzazioni in stile Windows. Il servizio può anche sfruttare provider di identità UNIX come LDAP per utenti e gruppi UNIX per esportazioni NFS, convalida ID NFSv4, autenticazione Kerberos e ACL NFSv4.

> Attualmente solo Active Directory LDAP è supportato con Google Cloud NetApp Volumes per la funzionalità LDAP.

Rilevamento, prevenzione e mitigazione di ransomware, malware e virus

Ransomware, malware e virus rappresentano una minaccia costante per gli amministratori e il rilevamento, la prevenzione e la mitigazione di tali minacce sono sempre priorità assolute per le aziende. Un singolo attacco ransomware su un set di dati critico può potenzialmente costare milioni di dollari, quindi è utile fare tutto il possibile per ridurre al minimo il rischio.

Sebbene Google Cloud NetApp Volumes attualmente non includa misure native di rilevamento o prevenzione, come la protezione antivirus o "rilevamento automatico del ransomware", esistono modi per ripristinare rapidamente i dati da un evento ransomware abilitando pianificazioni regolari di Snapshot. Le copie Snapshot sono puntatori immutabili e di sola lettura ai blocchi modificati nel file system, sono pressoché istantanee, hanno un impatto minimo sulle prestazioni e occupano spazio solo quando i dati vengono modificati o eliminati. Puoi impostare pianificazioni per le copie Snapshot in modo che corrispondano all'obiettivo di punto di ripristino (RPO)/obiettivo di tempo di ripristino (RTO) accettabile desiderato e puoi conservare fino a 1.024 copie Snapshot per volume.

Il supporto Snapshot è incluso senza costi aggiuntivi (oltre ai costi di archiviazione dei dati per i blocchi modificati/dati conservati dalle copie Snapshot) con Google Cloud NetApp Volumes e, in caso di attacco

ransomware, può essere utilizzato per ripristinare una copia Snapshot precedente all'attacco. Il ripristino degli snapshot richiede solo pochi secondi, dopodiché è possibile tornare a gestire i dati normalmente. Per ulteriori informazioni, vedere "La soluzione NetApp contro il ransomware" .

Per impedire che il ransomware colpisca la tua azienda è necessario un approccio multistrato che includa uno o più dei seguenti elementi:

- Protezione degli endpoint
- Protezione contro le minacce esterne tramite firewall di rete
- Rilevamento di anomalie nei dati
- Backup multipli (in loco e fuori sede) di set di dati critici
- Test di ripristino regolari dei backup
- Copie di snapshot NetApp immutabili e di sola lettura
- Autenticazione multifattoriale per infrastrutture critiche
- Audit di sicurezza degli accessi al sistema

Questo elenco è tutt'altro che esaustivo, ma rappresenta un buon modello da seguire quando si ha a che fare con i potenziali attacchi ransomware. Google Cloud NetApp Volumes in Google Cloud offre diversi modi per proteggersi dagli eventi ransomware e ridurne gli effetti.

Copie Snapshot immutabili

Google Cloud NetApp Volumes fornisce in modo nativo copie Snapshot immutabili di sola lettura, che vengono eseguite secondo una pianificazione personalizzabile per un rapido ripristino puntuale in caso di eliminazione dei dati o se un intero volume è stato vittima di un attacco ransomware. I ripristini snapshot di copie Snapshot valide 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 sulle prestazioni della tecnologia Snapshot è trascurabile.

Poiché le copie Snapshot in Google Cloud NetApp Volumes sono di sola lettura, non possono essere infettate da ransomware, a meno che il ransomware non si sia diffuso nel set di dati senza essere notato e non siano state create copie Snapshot dei dati infettati dal ransomware. Ecco perché è necessario prendere in considerazione anche il rilevamento del ransomware basato sulle anomalie dei dati. Google Cloud NetApp Volumes al momento non fornisce il rilevamento in modo nativo, ma è possibile utilizzare un software di monitoraggio esterno.

Backup e ripristini

Google Cloud NetApp Volumes offre funzionalità di backup client NAS standard (ad esempio backup su NFS o SMB).

- NetApp Volumes-Performance offre la replica dei volumi tra regioni diverse verso altri volumi NetApp Volumes-Performance. Per ulteriori informazioni, vedi "replicazione del volume" nella documentazione di Google Cloud NetApp Volumes.
- NetApp Volumes-SW offre funzionalità native del servizio per il backup/ripristino dei volumi. Per ulteriori informazioni, consulta "backup su cloud" la documentazione di Google Cloud NetApp Volumes.

La replica del volume fornisce una copia esatta del volume di origine per un failover rapido in caso di disastro, compresi gli eventi ransomware.

Replicazione interregionale

NetApp Volumes-Performance consente di replicare in modo sicuro i volumi nelle regioni di Google Cloud per casi d'uso di protezione dei dati e archiviazione utilizzando la crittografia TLS1.2 AES 256 GCM su una rete di servizi backend controllata da NetApp tramite interfacce specifiche utilizzate per la replica in esecuzione sulla rete di Google. Un volume primario (di origine) contiene i dati di produzione attivi e viene replicato su un volume secondario (di destinazione) per fornire una replica esatta del set di dati 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 residente su un volume primario viene replicato sul volume secondario, nella replica iniziale verrà trasferito 1 TB di spazio. Se il database contiene alcune centinaia di righe (ipoteticamente, alcuni MB) che cambiano tra l'inizializzazione e il successivo aggiornamento, solo i blocchi con le righe modificate vengono replicati sul database secondario (alcuni MB). Ciò contribuisce a garantire che i tempi di trasferimento rimangano bassi e che i costi di replicazione restino bassi.

Tutte le autorizzazioni su file e cartelle vengono replicate sul volume secondario, ma le autorizzazioni di accesso alla condivisione (ad esempio 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 dovrebbe sfruttare gli stessi servizi di nomi e le connessioni di dominio Active Directory per garantire 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, convertendo così il volume secondario in lettura-scrittura.

Le repliche del volume sono di sola lettura, il 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 un ransomware ha crittografato il set di dati primario. I dati di sola lettura non verranno crittografati, ma se il volume primario viene interessato e si verifica una replica, anche i blocchi infetti verranno replicati. È possibile utilizzare copie Snapshot più vecchie e non interessate per il ripristino, ma gli SLA potrebbero non rientrare nell'intervallo RTO/RPO promesso, a seconda della rapidità con cui viene rilevato un attacco.

Inoltre, con la gestione della replica tra regioni (CRR) in Google Cloud, puoi prevenire azioni amministrative dannose, come l'eliminazione di volumi, l'eliminazione di Snapshot o le modifiche al calendario di Snapshot. Questo 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 possono eliminare i volumi di destinazione, dagli amministratori CRR, che non possono eseguire alcuna operazione sui volumi. Consulta "Considerazioni sulla sicurezza" nella documentazione di Google Cloud NetApp Volumes le autorizzazioni consentite per ciascun gruppo di amministratori.

Backup Google Cloud NetApp Volumes

Sebbene Google Cloud NetApp Volumes garantisca un'elevata durabilità dei dati, eventi esterni possono causare la perdita di dati. In caso di un evento dannoso per la sicurezza, come un virus o un ransomware, i backup e i ripristini diventano fondamentali per ripristinare tempestivamente l'accesso ai dati. Un amministratore potrebbe eliminare accidentalmente un volume Google Cloud NetApp Volumes . Oppure gli utenti vogliono semplicemente conservare versioni di backup dei propri dati per molti mesi e mantenere lo spazio di copia Snapshot aggiuntivo all'interno del volume diventa un problema di costi. Sebbene le copie snapshot dovrebbero essere il metodo preferito per conservare le versioni di backup delle ultime settimane per ripristinare i dati persi, esse si trovano all'interno del volume e vanno perse se il volume viene rimosso.

Per tutti questi motivi, Google Cloud NetApp Volumes offre servizi di backup tramite "Backup Google Cloud NetApp Volumes".

Il backup Google Cloud NetApp Volumes genera una copia del volume su Google Cloud Storage (GCS). Esegue il backup solo dei dati effettivamente archiviati nel volume, non dello spazio libero. Funziona in modo

incrementale per sempre, ovvero trasferisce il contenuto del volume una volta e da quel momento in poi 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 spazio di archiviazione per i backup, riducendo i costi. Poiché il prezzo mensile dello spazio di backup è inferiore rispetto a quello di un volume, è il luogo ideale in cui conservare le versioni di backup più a lungo.

Gli utenti possono utilizzare un backup di Google Cloud NetApp Volumes per ripristinare qualsiasi versione del backup sullo stesso volume o su un volume diverso all'interno della stessa regione. Se il volume di origine viene eliminato, i dati di backup vengono conservati e devono essere gestiti (ad esempio, eliminati) in modo indipendente.

Il backup di Google Cloud NetApp Volumes è integrato in Google Cloud NetApp Volumes come opzione. Puoi decidere quali volumi proteggere attivando il backup di Google Cloud NetApp Volumes per ciascun volume. Consulta la "Documentazione sul backup Google Cloud NetApp Volumes" per informazioni sui backup, la "numero massimo di versioni di backup supportate", la pianificazione e "prezzi".

Tutti i dati di backup di un progetto vengono archiviati in 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 Google Cloud NetApp Volumes , ma sono in fase di valutazione altre opzioni. Per informazioni aggiornate, consultare la documentazione.

Il trasporto dei dati da un bucket Google Cloud NetApp Volumes 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 di Google Cloud NetApp Volumes (creazione, eliminazione e ripristino dei backup), un utente deve disporre del ruolo "roles/netapp.admin".

Panoramica

Per fidarsi di una soluzione cloud è fondamentale comprenderne l'architettura e il modo in cui è protetta. Questa sezione illustra diversi aspetti dell'architettura di Google Cloud NetApp Volumes in Google per contribuire ad alleviare potenziali preoccupazioni sulla protezione dei dati, nonché per evidenziare le aree in cui potrebbero essere necessari ulteriori passaggi di configurazione per ottenere la distribuzione più sicura.

L'architettura generale di Google Cloud NetApp Volumes può essere suddivisa in due componenti principali: il piano di controllo e il piano dati.

Piano di controllo

Il piano di controllo in Google Cloud NetApp Volumes è l'infrastruttura backend gestita dagli amministratori Google Cloud NetApp Volumes e dal software di automazione nativo NetApp . Questo piano è completamente trasparente per gli utenti finali e include networking, hardware di storage, aggiornamenti software e così via per contribuire a fornire valore a una soluzione residente nel cloud come Google Cloud NetApp Volumes.

Piano dati

Il piano dati in Google Cloud NetApp Volumes include i volumi di dati effettivi e la configurazione complessiva Google Cloud NetApp Volumes (ad esempio controllo degli accessi, autenticazione Kerberos e così via). Il piano dati è interamente sotto il controllo degli utenti finali e dei consumatori della piattaforma Google Cloud NetApp Volumes .

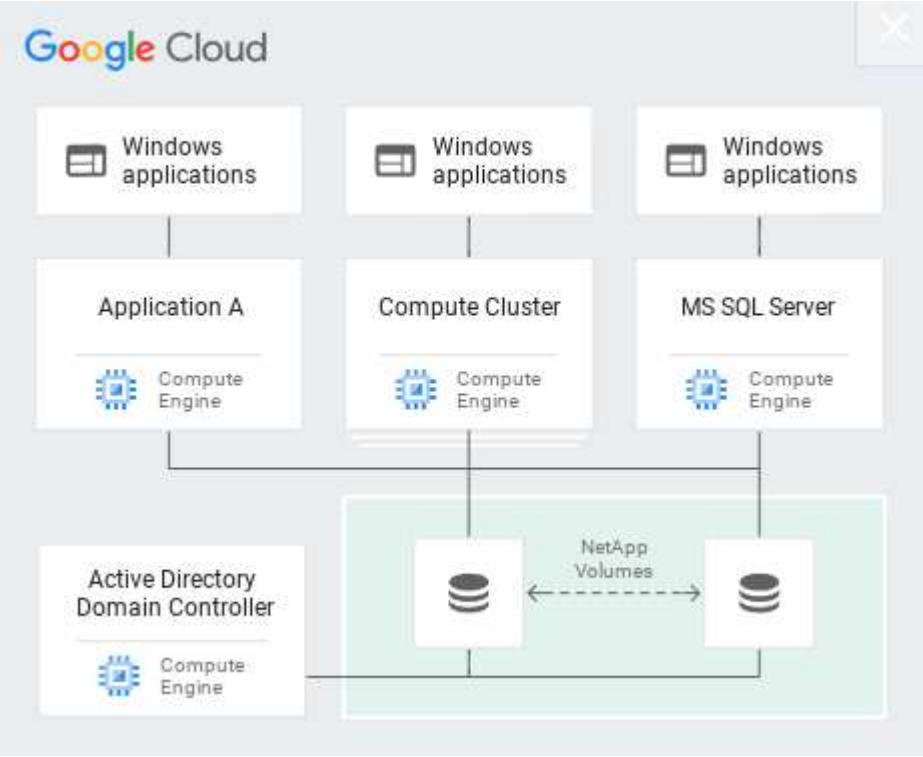
Esistono differenze sostanziali nel modo in cui ogni aereo viene messo in sicurezza e gestito. Le sezioni seguenti illustrano queste differenze, a partire da una panoramica dell'architettura Google Cloud NetApp

Volumes .

Architettura Google Cloud NetApp Volumes

In modo simile ad altri servizi nativi di Google Cloud come CloudSQL, Google Cloud VMware Engine (GCVE) e FileStore, Google Cloud NetApp Volumes utilizza "Annuncio di servizio pubblico di Google" per fornire il servizio. In PSA, i servizi vengono creati all'interno di un progetto di produttore di servizi, che utilizza "Peering di rete VPC" per connettersi al consumatore del servizio. Il produttore del servizio è fornito e gestito da NetApp, mentre il consumatore del servizio è una VPC in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni file di Google Cloud NetApp Volumes .

La figura seguente, a cui si fa riferimento da "Documentazione di Google Cloud NetApp Volumes", esamina una vista high-level.



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. Il riquadro blu a sinistra raffigura l'utente VPC (consumatore del servizio), il riquadro blu a destra è il produttore del servizio fornito da NetApp. Entrambi sono connessi tramite peering VPC.

Modello di locazione

In Google Cloud NetApp Volumes, i singoli progetti sono considerati tenant univoci. Ciò significa che la manipolazione dei volumi, delle copie Snapshot e così via vengono eseguite per ogni singolo 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 in essi contenuti per impostazione predefinita. Questa è considerata la vista del piano di controllo del servizio.

VPC condivise

Nella vista del piano dati, Google Cloud NetApp Volumes può connettersi a una VPC condivisa. È possibile creare volumi nel progetto di hosting o in uno dei progetti di servizio connessi alla VPC condivisa. Tutti i progetti (host o servizi) connessi a quella VPC condivisa sono in grado di raggiungere i volumi a livello di rete (TCP/IP). Poiché tutti i client con connettività di rete sulla VPC condivisa possono potenzialmente accedere ai dati tramite protocolli NAS, è necessario utilizzare il controllo degli accessi sul singolo volume (ad esempio elenchi di controllo degli accessi (ACL) utente/gruppo e nomi host/indirizzi IP per le esportazioni NFS) per controllare chi può accedere ai dati.

È possibile connettere Google Cloud NetApp Volumes a un massimo di cinque VPC per progetto del cliente. Sul piano di controllo, il progetto consente di gestire tutti i volumi creati, indipendentemente dalla VPC a cui sono connessi. Sul piano dati, le VPC sono isolate l'una dall'altra e ogni volume può essere connesso a una sola 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 alla VPC condivisa sono in grado di vedere il volume, mentre, a livello di gestione, il piano di controllo consente solo al progetto proprietario di vedere il volume.

Controlli del servizio VPC

I controlli del servizio VPC stabiliscono un perimetro di controllo degli accessi attorno ai servizi Google Cloud collegati a Internet e accessibili in tutto il mondo. Questi servizi forniscono il controllo degli accessi tramite le identità degli utenti, ma non possono limitare la provenienza delle richieste di posizione di rete. I controlli del servizio VPC colmano questa lacuna introducendo funzionalità per limitare l'accesso a reti definite.

Il piano dati di Google Cloud NetApp Volumes non è connesso a Internet esterno, bensì a VPC private con confini di rete (perimetri) ben definiti. All'interno di tale rete, ogni volume utilizza un controllo di accesso specifico del protocollo. Qualsiasi connettività di rete esterna viene creata esplicitamente dagli amministratori del progetto Google Cloud. Il piano di controllo, tuttavia, non fornisce le stesse protezioni del piano dati e può essere accessibile da chiunque da qualsiasi luogo con credenziali valide ("Token JWT").

In breve, il piano dati di Google Cloud NetApp Volumes offre la possibilità di controllare l'accesso alla rete, senza il requisito di supportare i controlli del servizio VPC e senza utilizzarli esplicitamente.

Considerazioni sullo sniffing/tracciamento dei pacchetti

Le acquisizioni di pacchetti possono essere utili per risolvere problemi di rete o altri problemi (ad esempio autorizzazioni NAS, connettività LDAP e così via), ma possono anche essere utilizzate in modo dannoso per ottenere informazioni sugli indirizzi IP di rete, sugli indirizzi MAC, sui nomi di utenti e gruppi e sul livello di sicurezza utilizzato sugli endpoint. A causa del modo in cui sono configurate le regole di rete, VPC e firewall di Google Cloud, l'accesso indesiderato ai pacchetti di rete dovrebbe essere difficile da ottenere senza credenziali di accesso utente o"Token JWT" nelle istanze cloud. Le acquisizioni di pacchetti sono possibili solo sugli endpoint (ad esempio sulle macchine virtuali (VM)) e solo sugli endpoint interni alla VPC, a meno che non venga utilizzata una VPC condivisa e/o un tunnel di rete esterno/inoltro IP per consentire esplicitamente il traffico esterno agli endpoint. Non c'è modo di intercettare il traffico esterno ai client.

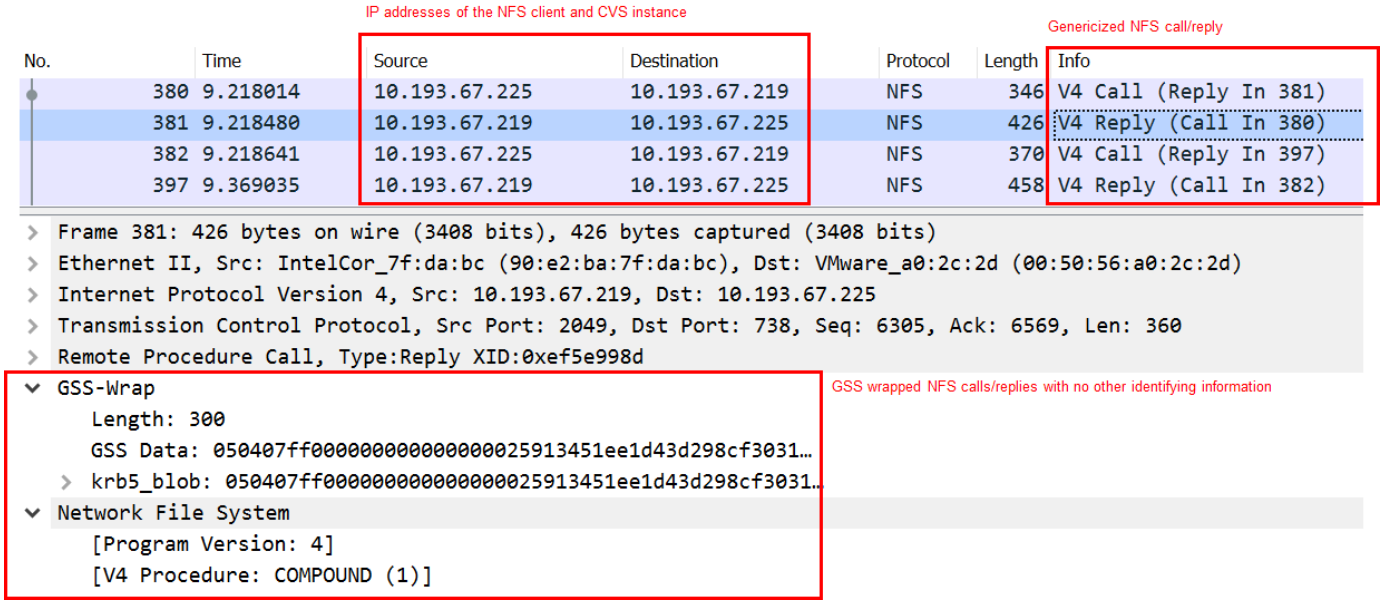
Quando vengono utilizzate VPC condivise, la crittografia in-flight con NFS Kerberos e/o"Crittografia SMB" può mascherare gran parte delle informazioni ricavate dalle tracce. Tuttavia, una parte del traffico viene ancora inviata in testo normale, come ad esempio"DNS" E"Query LDAP" . La figura seguente mostra l'acquisizione di un pacchetto da una query LDAP in testo normale proveniente da Google Cloud NetApp Volumes e le potenziali informazioni identificative esposte. Le query LDAP in Google Cloud NetApp Volumes attualmente non supportano la crittografia o LDAP su SSL. NetApp Volumes-Performance supporta la firma LDAP, se

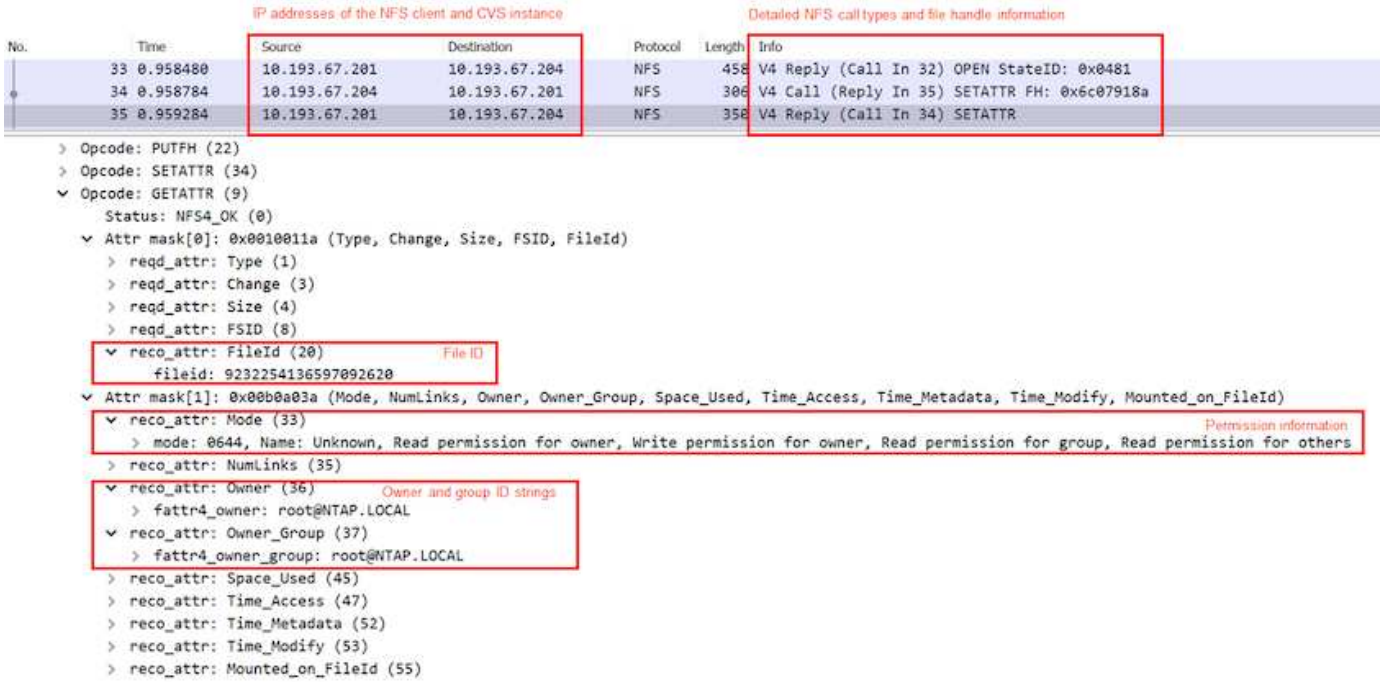
richiesta da Active Directory. NetApp Volumes-SW non supporta la firma LDAP.



unixUserPassword viene interrogato da LDAP e non viene inviato in testo normale, bensì in un hash salato. Per impostazione predefinita, Windows LDAP non popola i campi unixUserPassword. Questo campo è obbligatorio solo se è necessario sfruttare Windows LDAP per gli accessi interattivi tramite LDAP ai client. Google Cloud NetApp Volumes non supporta gli accessi LDAP interattivi alle istanze.

La figura seguente mostra l'acquisizione di un pacchetto da una conversazione NFS Kerberos accanto all'acquisizione di NFS su AUTH_SYS. Si noti come le informazioni disponibili in una traccia differiscano tra i due e come l'abilitazione della crittografia in-flight offra una maggiore sicurezza complessiva per il traffico NAS.





Interfacce di rete VM

Un trucco che gli aggressori potrebbero tentare è quello di aggiungere una nuova scheda di interfaccia di rete (NIC) a una VM in "modalità promiscua" (port mirroring) oppure abilitare la modalità promiscua su una NIC esistente per intercettare tutto il traffico. In Google Cloud, l'aggiunta di una nuova NIC richiede l'arresto completo di una VM, il che genera avvisi, in modo che gli aggressori non possano farlo senza essere notati.

Inoltre, le NIC non possono essere impostate in modalità promiscua e attiveranno avvisi in Google Cloud.

Architettura del piano di controllo

Tutte le azioni di gestione su Google Cloud NetApp Volumes vengono eseguite tramite API. La gestione di Google Cloud NetApp Volumes integrata in GCP Cloud Console utilizza anche l'API Google Cloud NetApp Volumes .

Gestione dell'identità e degli accessi

Gestione dell'identità e degli accessi("SONO") è un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (permessi) per le istanze del progetto Google Cloud. Google IAM fornisce un registro di controllo completo delle autorizzazioni, delle autorizzazioni e delle rimozioni. Attualmente Google Cloud NetApp Volumes non fornisce l'audit del piano di controllo.

Panoramica delle autorizzazioni/permessi

IAM offre autorizzazioni granulari integrate per Google Cloud NetApp Volumes. Puoi trovare un "elenco completo dei permessi granulari qui".

IAM offre anche due ruoli predefiniti denominati `netappcloudvolumes.admin` E `netappcloudvolumes.viewer` . Questi ruoli possono essere assegnati a utenti specifici o account di servizio.

Assegnare ruoli e autorizzazioni appropriati per consentire agli utenti IAM di gestire Google Cloud NetApp Volumes.

Ecco alcuni esempi di utilizzo di autorizzazioni granulari:

- Crea un ruolo personalizzato con solo autorizzazioni di ottenimento/elenco/creazione/aggiornamento in modo che gli utenti non possano eliminare volumi.
- Utilizzare un ruolo personalizzato con solo `snapshot.*` autorizzazioni per creare un account di servizio utilizzato per creare un'integrazione Snapshot coerente con l'applicazione.
- Crea un ruolo personalizzato da delegare `volumereplication.*` a utenti specifici.

Account di servizio

Per effettuare chiamate API Google Cloud NetApp Volumes tramite script o "Terraformare" , 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 Google Cloud NetApp Volumes in due modi diversi:

- Genera una chiave JSON e utilizza le API di Google per ricavarne un token JWT. Questo è l'approccio più semplice, ma prevede la gestione manuale dei segreti (la chiave JSON).
- Utilizzo "Impersonificazione dell'account di servizio" con `roles/iam.serviceAccountTokenCreator` . Il codice (script, Terraform e così via) viene eseguito con "Credenziali predefinite dell'applicazione" e impersona l'account di servizio per ottenerne le autorizzazioni. Questo approccio rispecchia le migliori pratiche di sicurezza di Google.

Vedi "Creazione dell'account di servizio e della chiave privata" la documentazione di Google Cloud per ulteriori informazioni.

API Google Cloud NetApp Volumes

L'API di Google Cloud NetApp Volumes utilizza un'API basata su REST che usa HTTPS (TLSv1.2) come trasporto di rete sottostante. Puoi trovare la definizione più recente dell'API e informazioni su come utilizzarla all'indirizzo "API di Cloud Volumes nella documentazione di Google Cloud".

L'endpoint API è gestito e protetto da NetApp tramite la funzionalità HTTPS standard (TLSv1.2).

Token JWT

L'autenticazione all'API viene eseguita con token JWT bearer("RFC-7519"). I token JWT validi devono essere ottenuti tramite l'autenticazione Google Cloud IAM. Ciò deve essere fatto recuperando un token da IAM fornendo una chiave JSON dell'account di servizio.

Registrazione di controllo

Attualmente non sono disponibili registri di controllo accessibili all'utente.

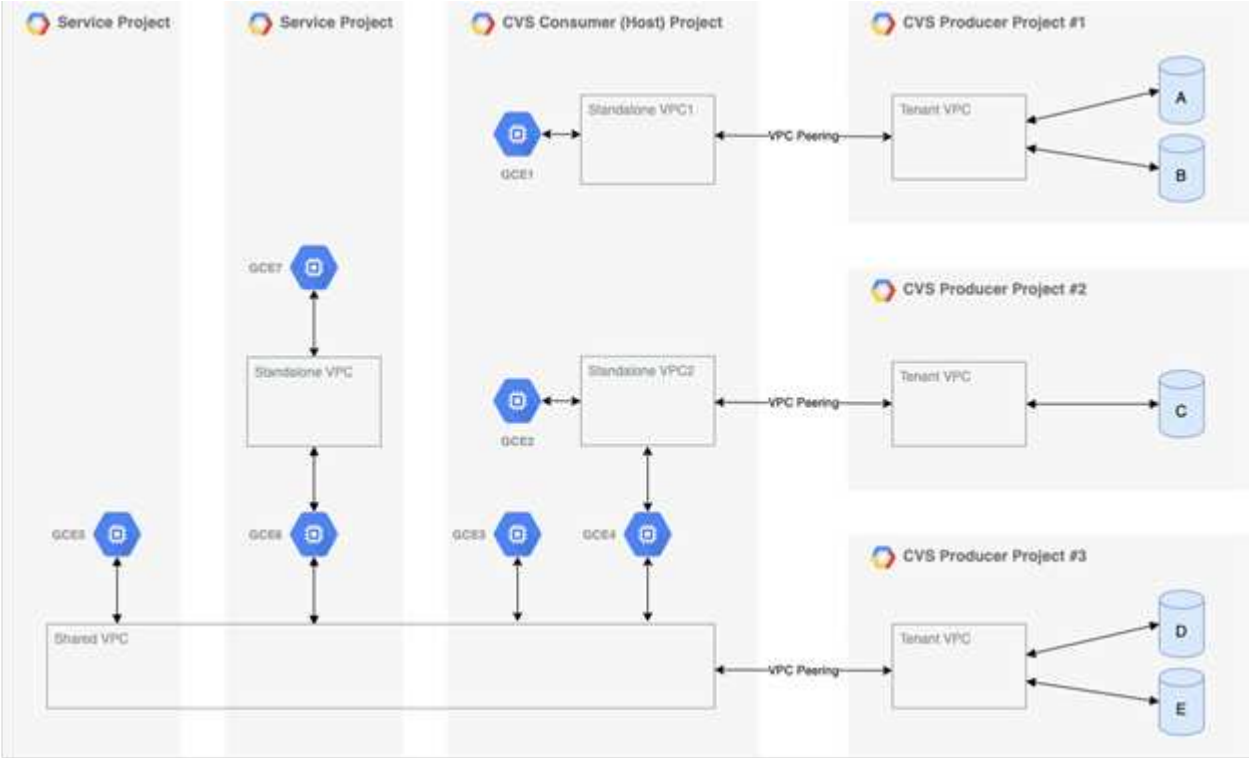
Architettura del piano dati

Google Cloud NetApp Volumes per Google Cloud sfrutta Google Cloud "accesso ai servizi privati" struttura. In questo framework, gli utenti possono connettersi a Google Cloud NetApp Volumes. Questo framework utilizza strutture di Service Networking e peering VPC come altri servizi Google Cloud, garantendo un isolamento completo tra i tenant.

Per una panoramica dell'architettura di Google Cloud NetApp Volumes per Google Cloud, vedi "Architettura

per Google Cloud NetApp Volumes".

Le VPC utente (autonome o condivise) sono collegate alle VPC all'interno dei progetti tenant gestiti da Google Cloud NetApp Volumes , che ospitano i volumi.



La figura precedente mostra un progetto (il progetto consumer NetApp Volumes al centro) con tre reti VPC connesse a Google Cloud NetApp Volumes e più VM Compute Engine (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 una VPC condivisa, condivisa 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 i volumi del tipo di servizio NetApp Volumes-Performance.

GCE7 non può accedere ad alcun volume.

I dati possono essere crittografati sia in transito (utilizzando la crittografia Kerberos e/o SMB) sia a riposo in Google Cloud NetApp Volumes.

Crittografia dei dati in transito

I dati in transito possono essere crittografati a livello di protocollo NAS e la rete Google Cloud stessa è 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 accennato nella sezione "Architettura Google Cloud NetApp Volumes ", Google Cloud NetApp Volumes viene distribuito tramite un progetto produttore PSA controllato da NetApp.

Nel caso di NetApp Volumes-SW, il tenant produttore esegue le VM di Google per fornire il servizio. Il traffico tra le VM degli utenti e le VM Google Cloud NetApp Volumes viene crittografato automaticamente da Google.

Sebbene il percorso dati per NetApp Volumes-Performance non sia completamente crittografato a livello di rete, NetApp e Google utilizzano una combinazione "della crittografia IEEE 802.1AE (MACSec)" , "incapsulamento" (crittografia dei dati) e reti fisicamente limitate per proteggere i dati in transito tra il tipo di servizio Google Cloud NetApp Volumes NetApp Volumes e Google Cloud.

Protocolli NAS

I protocolli NAS NFS e SMB forniscono la crittografia di trasporto opzionale a livello di protocollo.

Crittografia SMB

"Crittografia SMB"fornisce la crittografia end-to-end dei dati SMB e protegge i dati da intercettazioni su reti non affidabili. È possibile abilitare la crittografia sia per la connessione dati client/server (disponibile solo per i client compatibili con SMB3.x) sia per l'autenticazione del server/controller di dominio.

Quando la crittografia SMB è abilitata, i client che non supportano la crittografia non possono accedere alla condivisione.

Google Cloud NetApp Volumes supporta i cifrari di sicurezza RC4-HMAC, AES-128-CTS-HMAC-SHA1 e AES-256-CTS-HMAC-SHA1 per la crittografia SMB. SMB negozia il tipo di crittografia più elevato supportato dal server.

NFSv4.1 Kerberos

Per NFSv4.1, NetApp Volumes-Performance offre l'autenticazione Kerberos come descritto in "RFC7530" È possibile abilitare Kerberos in base al volume.

Il tipo di crittografia più potente attualmente disponibile per Kerberos è AES-256-CTS-HMAC-SHA1. Google Cloud NetApp Volumes 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 fornisce tre diversi livelli di sicurezza per i mount NFS, che consentono di scegliere il livello di sicurezza Kerberos.

Secondo 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.
```

Come regola generale, più il livello di sicurezza di Kerberos deve intervenire, peggiori saranno le prestazioni, poiché il client e il server impiegano tempo a crittografare e decrittografare le operazioni NFS per ogni pacchetto inviato. Molti client e server NFS forniscono supporto per l'offload AES-NI sulle CPU per una migliore esperienza complessiva, ma l'impatto sulle prestazioni di Kerberos 5p (crittografia end-to-end

completa) è significativamente maggiore rispetto all'impatto di Kerberos 5 (autenticazione utente).

La tabella seguente mostra le differenze tra i diversi livelli in termini di sicurezza e prestazioni.

Livello di sicurezza	Sicurezza	Prestazione
NFSv3—sys	• Meno sicuro; testo normale con ID utente/ID gruppo numerici • In grado di visualizzare UID, GID, indirizzi IP client, percorsi di esportazione, nomi file, autorizzazioni nelle acquisizioni di pacchetti	• Ideale per la maggior parte dei casi
NFSv4.x—sys	• Più sicuro di NFSv3 (ID client, corrispondenza stringa nome/stringa dominio) ma comunque testo normale • In grado di visualizzare UID, GID, indirizzi IP client, stringhe di nomi, ID di dominio, percorsi di esportazione, nomi di file, autorizzazioni nelle acquisizioni di pacchetti	• Adatto per carichi di lavoro sequenziali (come macchine virtuali, database, file di grandi dimensioni) • Scarso con elevato numero di file/elevato numero di metadati (peggio del 30-50%)
NFS—krb5	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: racchiude UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al mount necessita di un ticket Kerberos valido (tramite nome utente/password o scambio manuale di chiavi); il ticket scade dopo un periodo di tempo specificato e l'utente deve autenticarsi nuovamente per accedere • Nessuna crittografia per le operazioni NFS o protocolli ausiliari come mount/portmapper/nlm (può vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime nelle acquisizioni di pacchetti)	• Il migliore nella maggior parte dei casi per Kerberos; peggiore di AUTH_SYS

Livello di sicurezza	Sicurezza	Prestazione
NFS—krb5i	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: racchiude UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al mount necessita di un ticket Kerberos valido (tramite nome utente/password o scambio manuale di chiavi); il ticket scade dopo un periodo di tempo specificato e l'utente deve autenticarsi nuovamente per accedere • Nessuna crittografia per le operazioni NFS o protocolli ausiliari come mount/portmapper/nlm (può vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime nelle acquisizioni di pacchetti) • A ogni pacchetto viene aggiunto un checksum Kerberos GSS per garantire che nulla intercetti i pacchetti. Se i checksum corrispondono, la conversazione è consentita.	• Meglio di krb5p perché il payload NFS non è crittografato; l'unico sovraccarico aggiuntivo rispetto a krb5 è il checksum di integrità. Le prestazioni di krb5i non saranno molto peggiori di quelle di krb5, ma subiranno un certo degrado.

Livello di sicurezza	Sicurezza	Prestazione
NFS – krb5p	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: racchiude UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al mount necessita di un ticket Kerberos valido (tramite nome utente/password o scambio manuale di keytab); il ticket scade dopo un periodo di tempo specificato e l'utente deve autenticarsi nuovamente per accedere • Tutti i payload dei pacchetti NFS sono crittografati con il wrapper GSS (non è possibile visualizzare handle di file, autorizzazioni, nomi di file, atime/mtime nelle acquisizioni dei pacchetti). • Include controllo di 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)	• Peggiori prestazioni tra i livelli di sicurezza; krb5p deve crittografare/decrittografare di più. • Prestazioni migliori rispetto a krb5p con NFSv4.x per carichi di lavoro con un numero elevato di file.

In Google Cloud NetApp Volumes, 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 Google Cloud NetApp Volumes. Per informazioni su come NFS Kerberos viene visualizzato nelle acquisizioni dei pacchetti, vedere la sezione "Considerazioni sullo sniffing/tracciamento dei pacchetti."

Crittografia dei dati a riposo

Tutti i volumi in Google Cloud NetApp Volumes sono crittografati a riposo mediante crittografia AES-256, il che significa che tutti i dati utente scritti sui supporti vengono crittografati e possono essere decrittografati solo con una chiave per volume.

- Per NetApp Volumes-SW vengono utilizzate le chiavi generate da Google.
- Per NetApp Volumes-Performance, le chiavi per volume vengono archiviate in un gestore chiavi integrato in Google Cloud NetApp Volumes.

A partire da novembre 2021, è stata resa disponibile l'anteprima della funzionalità delle chiavi di crittografia gestite dal cliente (CMEK). Ciò consente di crittografare le chiavi per volume con una chiave master per

progetto e per regione ospitata in "Servizio di gestione delle chiavi di Google (KMS)." KMS consente di collegare gestori di chiavi esterni.

Per informazioni sulla configurazione di KMS per NetApp Volumes-Performance, consulta "Impostazione delle chiavi di crittografia gestite dal cliente".

Firewall

Google Cloud NetApp Volumes espone più porte TCP per gestire condivisioni NFS e SMB:

- "Porte richieste per l'accesso NFS"
- "Porte richieste per l'accesso SMB"

Inoltre, SMB, NFS con LDAP, incluso Kerberos, e le configurazioni a doppio protocollo richiedono l'accesso a un dominio Windows Active Directory. Le connessioni ad Active Directory devono essere "configurato" configurate a livello di regione. I controller di dominio (DC) di Active Directory vengono identificati utilizzando "Rilevamento DC basato su DNS" i server DNS specificati. Vengono utilizzati tutti i DC restituiti. L'elenco dei DC idonei può essere limitato specificando un sito di Active Directory.

Google Cloud NetApp Volumes si connette utilizzando indirizzi IP dell'intervallo CIDR assegnato con il comando `gcloud compute address` mentre "onboarding di Google Cloud NetApp Volumes". Puoi usare questo CIDR come indirizzi di origine per configurare i firewall in entrata per i controller di dominio di Active Directory.

I controller di dominio di Active Directory devono "esporre le porte ai CIDR di Google Cloud NetApp Volumes come menzionato qui".

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 NetApp Volumes consente l'accesso condiviso ai dati su più client NAS. Inoltre, Google Cloud NetApp Volumes può fornire accesso simultaneo ai client NFS e SMB/CIFS (doppio protocollo), rispettando tutte le impostazioni di identità e autorizzazione sui file e sulle cartelle nelle condivisioni NAS. Per mantenere la massima sicurezza possibile nel trasferimento dei dati, Google Cloud NetApp Volumes supporta la crittografia del protocollo in transito tramite crittografia SMB e NFS Kerberos 5p.

Il doppio protocollo è disponibile solo con NetApp Volumes-Performance.

Nozioni di base sui protocolli NAS

I protocolli NAS sono metodi che consentono a più client su una rete di accedere agli stessi dati su un sistema di archiviazione, come Google Cloud NetApp Volumes su GCP. NFS e SMB sono i protocolli NAS definiti e operano su base client/server, dove Google Cloud NetApp Volumes funge da server. I client inviano richieste di accesso, lettura e scrittura al server, il quale 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, si segue la seguente procedura generale.

1. Il client chiede al server informazioni sulla directory (autorizzazioni, proprietario, gruppo, ID file, spazio disponibile e così via); il server risponde con le informazioni se il client e l'utente richiedenti dispongono delle autorizzazioni necessarie sulla cartella padre.
2. Se le autorizzazioni sulla directory consentono l'accesso, il client chiede al server se il nome del file che si sta creando esiste già nel file system. Se il nome del file è già in uso, la creazione fallisce. 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 della directory e il nome del file e imposta gli orari di accesso e di modifica. Il server assegna un ID file univoco al file per garantire che non vengano creati altri file con lo stesso ID file.
4. Il client invia una chiamata per verificare gli attributi del file prima dell'operazione WRITE. Se i permessi lo consentono, il client scrive il nuovo file. Se il protocollo/applicazione utilizza il blocco, il client chiede al server un blocco per impedire ad altri client di accedere al file mentre è bloccato, in modo da prevenire il danneggiamento dei dati.

NFS

NFS è un protocollo di file system distribuito che rappresenta uno standard IETF aperto definito nella Request for Comments (RFC) e che consente a chiunque di implementare il protocollo.

I volumi in Google Cloud NetApp Volumes vengono condivisi tra i client NFS esportando un percorso accessibile a un client o a un set di client. Le autorizzazioni per montare queste esportazioni sono definite da criteri e regole di esportazione, configurabili dagli amministratori di Google Cloud NetApp Volumes .

L'implementazione NetApp NFS è considerata uno standard di riferimento per il protocollo e viene utilizzata in innumerevoli ambienti NAS aziendali. Le sezioni seguenti riguardano NFS e le funzionalità di sicurezza specifiche disponibili in Google Cloud NetApp Volumes e come vengono implementate.

Utenti e gruppi UNIX locali predefiniti

Google Cloud NetApp Volumes contiene diversi utenti e gruppi UNIX predefiniti per varie funzionalità di base. Al momento, questi utenti e gruppi non possono essere modificati o eliminati. Al momento non è possibile aggiungere nuovi utenti e gruppi locali a Google Cloud NetApp Volumes. Gli utenti e i gruppi UNIX al di fuori di quelli predefiniti devono essere forniti da un servizio di denominazione LDAP esterno.

Nella tabella seguente sono riportati 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
• radice:0 • utentepc:65534 • nessuno:65535	• radice:0 • demone:1 • utentepc:65534 • nessuno:65535

Quando si utilizza NFSv4.1, l'utente root potrebbe essere visualizzato come nobody quando si eseguono comandi di elenco directory sui client NFS. Ciò è dovuto alla configurazione del mapping del dominio ID del client. Vedi la sezione chiamataNFSv4.1 e l'utente/gruppo nobody

per maggiori dettagli 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. Data la potenza di questo account, le migliori pratiche di sicurezza spesso richiedono che l'utente root sia disabilitato o limitato in qualche modo. Nelle esportazioni NFS, il potere che un utente root ha sui file e sulle cartelle può essere controllato in Google Cloud NetApp Volumes tramite criteri e regole di esportazione e un concetto noto come root squash.

Lo squashing della root garantisce che l'utente root che accede a un mount NFS venga compresso nell'utente numerico anonimo 65534 (vedere la sezione "L'utente anonimo ") ed è attualmente disponibile solo quando si utilizza NetApp Volumes-Performance selezionando Off per l'accesso root durante la creazione della regola della policy di esportazione. Se l'utente root viene compresso nell'utente anonimo, non ha più accesso per eseguire chown o "comandi setuid/setgid (il bit sticky)" su file o cartelle nel mount 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 ai file eliminati per i quali non ha autorizzazioni esplicite. Se si desidera limitare l'accesso ai permessi di file e cartelle di un utente root, valutare l'utilizzo di 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 che viene mappato alle richieste client che arrivano senza credenziali NFS valide. Ciò può includere l'utente root quando si utilizza il root squashing. L'utente anonimo in Google Cloud NetApp Volumes è 65534.

Questo UID è normalmente associato al nome utente `nobody` O `nfsnobody` in ambienti Linux. Google Cloud NetApp Volumes 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 corrispondente valido in LDAP.

A causa delle differenze nei nomi utente tra Linux e Google Cloud NetApp Volumes per UID 65534, la stringa del nome per gli utenti mappati su 65534 potrebbe non corrispondere quando si utilizza NFSv4.1. Di conseguenza, potresti vedere `nobody` come utente su alcuni file e cartelle. Vedi la sezione "NFSv4.1 e l'utente/gruppo nobody " per informazioni su questo problema e su come risolverlo.

Controllo degli accessi/esportazioni

L'accesso iniziale all'esportazione/condivisione per i mount NFS è controllato tramite regole di policy di esportazione basate sull'host contenute in una policy di esportazione. Un IP host, un nome host, una subnet, un netgroup o un dominio vengono definiti per consentire l'accesso al montaggio della condivisione NFS e il livello di accesso consentito all'host. Le opzioni di configurazione delle regole dei criteri di esportazione dipendono dal livello di Google Cloud NetApp Volumes .

Per NetApp Volumes-SW, sono disponibili le seguenti opzioni per la configurazione dei criteri di esportazione:

- **Corrispondenza cliente.** Elenco di indirizzi IP separati da virgole, elenco di nomi host, subnet, netgroup, nomi di dominio separati da virgole.
- **Regole di accesso RO/RW.** Selezionare lettura/scrittura o sola lettura per controllare il livello di accesso all'esportazione. NetApp Volumes-Performance offre le seguenti opzioni:
- **Corrispondenza cliente.** Elenco di indirizzi IP separati da virgole, elenco di nomi host, subnet, netgroup, nomi di dominio separati da virgole.

- **Regole di accesso RO/RW.** Selezionare lettura/scrittura o sola lettura per controllare il livello di accesso all'esportazione.
- **Accesso root (attivato/disattivato).** Configura la radice squash (vedere la sezione "L'utente root " per i dettagli).
- **Tipo di protocollo.** Ciò limita l'accesso al mount NFS a una versione specifica del protocollo. Quando si specificano sia NFSv3 che NFSv4.1 per il volume, lasciare entrambi i campi vuoti oppure selezionare entrambe le caselle.
- **Livello di sicurezza Kerberos (quando è selezionato Abilita Kerberos).** Fornisce le opzioni krb5, krb5i e/o krb5p per l'accesso in sola lettura o in lettura-scrittura.

Cambia proprietà (chown) e cambia gruppo (chgrp)

NFS su Google Cloud NetApp Volumes consente solo all'utente root di eseguire chown/chgrp su file e cartelle. Altri utenti vedono un `Operation not permitted` errore, anche sui file di loro proprietà. Se si utilizza la zucca radice (come descritto nella sezione "L'utente root "), la root viene ridotta a un utente non root e non gli è consentito l'accesso a chown e chgrp. Al momento non esistono soluzioni alternative in Google Cloud NetApp Volumes per consentire chown e chgrp agli utenti non root. Se sono necessarie modifiche alla proprietà, valutare l'utilizzo di volumi a doppio protocollo e impostare lo stile di sicurezza su NTFS per controllare le autorizzazioni dal lato Windows.

Gestione dei permessi

Google Cloud NetApp Volumes supporta sia i bit di modalità (ad esempio 644, 777 e così via per rwx) sia gli ACL NFSv4.1 per controllare le autorizzazioni sui client NFS per i volumi che utilizzano lo stile di sicurezza UNIX. Per questi viene utilizzata la gestione standard dei permessi (ad esempio chmod, chown o nfs4_setfacl) e funzionano 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 Google Cloud NetApp Volumes sugli utenti Windows, che vengono poi utilizzati per risolvere le autorizzazioni NTFS. Ciò richiede una connessione LDAP a Google Cloud NetApp Volumes per fornire traduzioni da ID numerico a nome utente, poiché Google Cloud NetApp Volumes richiede un nome utente UNIX valido per essere mappato correttamente a un nome utente Windows.

Fornitura di ACL granulari per NFSv3

I permessi dei bit di modalità riguardano solo il proprietario, il gruppo e tutti gli altri nella semantica, il che significa che non sono presenti controlli granulari di accesso utente per NFSv3 di base. Google Cloud NetApp Volumes non supporta ACL POSIX né attributi estesi (come chattr), pertanto gli ACL granulari sono possibili solo nei seguenti scenari con NFSv3:

- Volumi di sicurezza NTFS (è richiesto un server CIFS) con mapping utente UNIX-Windows validi.
- ACL NFSv4.1 applicati tramite un client di amministrazione che monta NFSv4.1 per applicare gli ACL.

Entrambi i metodi richiedono una connessione LDAP per la gestione dell'identità UNIX e informazioni valide su utenti e gruppi UNIX (vedere la sezione"LDAP") e sono disponibili solo con istanze NetApp Volumes-Performance. Per utilizzare 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 stabilite connessioni SMB. Per utilizzare gli ACL NFSv4.1 con i mount NFSv3, è necessario selezionare `Both (NFSv3/NFSv4.1)` come tipo di protocollo.

I bit della modalità UNIX standard non forniscono lo stesso livello di granularità nelle autorizzazioni fornito dagli ACL NTFS o NFSv4.x. Nella tabella seguente viene confrontata la granularità delle autorizzazioni tra i bit della modalità NFSv3 e gli ACL NFSv4.1. Per informazioni sugli ACL NFSv4.1, vedere "nfs4_acl - Elenchi di

controllo di accesso NFSv4" .

Bit della modalità NFSv3	ACL NFSv4.1
• Imposta l'ID utente durante l'esecuzione • Imposta l'ID del gruppo durante l'esecuzione • Salva il testo scambiato (non definito in POSIX) • Autorizzazione di lettura per il proprietario • Autorizzazione di scrittura per il proprietario • Eseguire l'autorizzazione per il proprietario su un file; oppure cercare (cercare) l'autorizzazione per il proprietario nella directory • Permesso di lettura per il gruppo • Permesso di scrittura per il gruppo • Eseguire l'autorizzazione per il gruppo su un file; oppure cercare (cercare) l'autorizzazione per il gruppo nella directory • Permesso di lettura per gli altri • Autorizzazione di scrittura per gli altri • Eseguire l'autorizzazione per altri su un file; oppure cercare (cercare) l'autorizzazione per altri nella directory	Tipi di voci di controllo di accesso (ACE) (Consenti/Nega/Audit) * Flag di ereditarietà * directory-inherit * file-inherit * no-propagate-inherit * inherit-only Permessi * lettura dati (file) / elenco directory (directory) * scrittura dati (file) / creazione file (directory) * aggiunta dati (file) / creazione sottodirectory (directory) * esecuzione (file) / modifica directory (directory) * eliminazione * eliminazione figlio * lettura attributi * scrittura attributi * lettura attributi denominati * scrittura attributi denominati * lettura ACL * scrittura ACL * scrittura proprietario * Sincronizzazione

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 rimuovono la limitazione tramite ACL granulari per utenti e gruppi (fino a 1024 voci per ACE).

Inoltre, Google Cloud NetApp Volumes offre un supporto esteso per i gruppi, consentendoti di aumentare il numero massimo di gruppi supportati fino a 32. Ciò richiede una connessione LDAP a un LDAP server che contiene identità UNIX valide di utenti e gruppi. Per ulteriori informazioni su come configurarlo, vedi "Creazione e gestione di volumi NFS" nella documentazione di Google.

ID utente e gruppo NFSv3

Gli ID utente e gruppo NFSv3 vengono trasmessi in rete come ID numerici anziché come nomi. Google Cloud NetApp Volumes non esegue alcuna risoluzione del nome utente per questi ID numerici con NFSv3, mentre i volumi in stile sicurezza UNIX utilizzano solo bit di modalità. Quando sono presenti ACL NFSv4.1, è necessaria una ricerca di ID numerico e/o di stringa di nome per risolvere correttamente l'ACL, anche quando si utilizza NFSv3. Con i volumi di sicurezza NTFS, Google Cloud NetApp Volumes deve risolvere un ID numerico in un utente UNIX valido e quindi mapparlo in un utente Windows valido per negoziare i diritti di accesso.

Limitazioni di sicurezza degli ID utente e 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 considerato implicitamente attendibile. Ciò espone il file system a potenziali violazioni semplicemente falsificando un ID numerico. Per prevenire falle di sicurezza come questa, sono disponibili alcune opzioni per Google Cloud NetApp Volumes.

- 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 che consenta l’accesso a un mount. Kerberos è disponibile con le istanze NetApp Volumes-Performance e solo con NFSv4.1.
- Limitando l’elenco degli host nelle regole dei criteri di esportazione si limitano i client NFSv3 che hanno accesso al volume Google Cloud NetApp Volumes .
- Utilizzando volumi a doppio protocollo e applicando ACL NTFS al volume, i client NFSv3 sono costretti a risolvere gli ID numerici in nomi utente UNIX validi per autenticarsi correttamente e accedere ai mount. Per farlo è necessario abilitare LDAP e configurare le identità degli utenti e dei gruppi UNIX.
- Eliminando l’utente root si limitano i danni che un utente root può causare a un mount NFS, ma non si eliminano completamente i rischi. Per maggiori informazioni, consultare la sezione "L’utente root ."

In definitiva, la sicurezza NFS è limitata a ciò che offre la versione del protocollo che si sta utilizzando. NFSv3, pur essendo generalmente più performante di NFSv4.1, non garantisce lo stesso livello di sicurezza.

NFSv4.1

NFSv4.1 offre maggiore sicurezza e affidabilità rispetto a NFSv3, per i seguenti motivi:

- Blocco integrato tramite un meccanismo basato sul leasing
- Sessioni con stato
- Tutte le funzionalità NFS su una singola porta (2049)
- Solo TCP
- Mappatura del dominio ID
- Integrazione Kerberos (NFSv3 può utilizzare Kerberos, ma solo per NFS, non per protocolli ausiliari come NLM)

Dipendenze NFSv4.1

Grazie alle funzionalità di sicurezza aggiuntive di NFSv4.1, sono coinvolte alcune dipendenze esterne che non erano necessarie per utilizzare NFSv3 (similmente a come SMB richiede dipendenze come Active Directory).

ACL NFSv4.1

Google Cloud NetApp Volumes offre supporto per ACL NFSv4.x, che offrono vantaggi distintivi rispetto alle normali autorizzazioni in stile POSIX, come i seguenti:

- Controllo granulare dell’accesso degli utenti a file e directory
- Migliore sicurezza NFS
- Migliorata interoperabilità con CIFS/SMB
- Rimozione della limitazione NFS di 16 gruppi per utente con sicurezza AUTH_SYS
- Gli ACL aggirano la necessità di risoluzione dell’ID gruppo (GID), rimuovendo di fatto il limite GID. Gli ACL NFSv4.1 sono controllati dai client NFS, non da Google Cloud NetApp Volumes. Per utilizzare gli ACL NFSv4.1, assicurati che la versione software del tuo 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 hanno funzionalità simili. Tuttavia, negli 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

A titolo di riferimento, vengono definiti i seguenti termini:

- **Elenco di controllo degli accessi (ACL).** Un elenco di voci di autorizzazione.
- **Controllo accessi (ACE).** Una voce di autorizzazione nell'elenco.

Quando un client imposta un ACL NFSv4.1 su un file durante un'operazione SETATTR, Google Cloud NetApp Volumes imposta tale ACL sull'oggetto, sostituendo qualsiasi ACL esistente. Se non è presente alcun ACL su un file, le autorizzazioni della modalità sul file vengono calcolate in base a OWNER@, GROUP@ e EVERYONE@. Se nel file sono presenti bit SUID/SGID/STICKY, questi non vengono interessati.

Quando un client ottiene un ACL NFSv4.1 su un file durante un'operazione GETATTR, Google Cloud NetApp Volumes legge l'ACL NFSv4.1 associato all'oggetto, crea 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 a partire dai bit di modalità e restituito al client.

L'accesso viene negato se nell'ACL è presente un DENY ACE; l'accesso viene concesso se è presente un ALLOW ACE. Tuttavia, l'accesso viene negato anche se nessuno dei due 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 composto dagli ACE ALLOW e DENY.

Se una base `chmod` se eseguito su un file o una cartella con ACL NFSv4.1 impostati, gli ACL utente e gruppo esistenti vengono conservati, ma gli ACL predefiniti OWNER@, GROUP@, EVERYONE@ vengono modificati.

Un client che utilizza ACL NFSv4.1 può impostare e visualizzare ACL per file e directory sul sistema. Quando un nuovo file o una nuova sottodirectory viene creato in una directory che ha un ACL, quell'oggetto eredita tutti gli ACE nell'ACL che sono stati contrassegnati con l'appropriato "flag di eredità" .

Se un file o una directory ha un ACL NFSv4.1, tale ACL viene utilizzato per controllare l'accesso indipendentemente dal protocollo utilizzato per accedere al file o alla directory.

I file e le directory ereditano gli ACE dagli ACL NFSv4 sulle directory padre (eventualmente con le opportune modifiche), a condizione che gli ACE siano stati contrassegnati con i flag di ereditarietà corretti.

Quando un file o una directory viene creato come risultato di una richiesta NFSv4, l'ACL sul file o sulla directory risultante varia a seconda che la richiesta di creazione del file includa un ACL o solo le autorizzazioni di accesso ai file UNIX standard. L'ACL dipende anche dal fatto che la directory padre disponga di un ACL.

- 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 padre non ha un ACL, viene utilizzata la modalità file client per impostare le autorizzazioni di accesso ai file UNIX standard.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard e la directory padre ha un ACL non ereditabile, sul nuovo oggetto viene impostato un ACL predefinito basato sui bit di modalità passati nella richiesta.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory padre ha un ACL, gli ACE nell'ACL della directory padre vengono ereditati dal nuovo file o directory, a condizione che gli ACE siano stati contrassegnati con i flag 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 di queste lettere, vedere "COME: utilizzare NFSv4 ACL" .

Comportamento ACL NFSv4.1 con umask ed ereditarietà ACL

"Gli ACL NFSv4 offrono la possibilità di offrire l'ereditarietà ACL" . L'ereditarietà ACL significa che i file o le cartelle creati sotto gli oggetti con ACL NFSv4.1 impostati possono ereditare gli ACL in base alla configurazione del "Flag di ereditarietà ACL" .

"Umask"viene utilizzato per controllare il livello di autorizzazione con cui file e cartelle vengono creati in una directory senza l'interazione dell'amministratore. Per impostazione predefinita, Google Cloud NetApp Volumes consente a umask di sovrascrivere gli ACL ereditati, che è il comportamento previsto secondo "RFC 5661" .

Formattazione ACL

Gli ACL NFSv4.1 hanno una formattazione specifica. L'esempio seguente è un ACE impostato 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 "permettere". In questo caso i flag di ereditarietà non sono impostati, perché il principale non è un gruppo e non include l'ereditarietà. Inoltre, poiché ACE non è una voce AUDIT, non è necessario impostare i flag 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 nome non può essere risolta dal client e dal server), l'ACL potrebbe non comportarsi come previsto oppure la modifica dell'ACL potrebbe non essere applicata e generare un errore.

Esempi di errori includono:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

NEGAZIONE esplicita

Le autorizzazioni NFSv4.1 possono includere attributi DENY espliciti per OWNER, GROUP e EVERYONE. Ciò avviene perché gli ACL NFSv4.1 sono di tipo default-deny, ovvero se un ACL non viene concesso esplicitamente da un ACE, viene negato. Gli attributi DENY espliciti sovrascrivono qualsiasi ACCESS ACE, esplicito o meno.

Gli ACE DENY sono impostati con un tag di attributo di `D` .

Nell’esempio seguente, a GROUP@ sono concessi tutti i permessi di lettura ed esecuzione, ma gli è negato tutto l’accesso 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 DENY dovrebbero essere evitati ove possibile perché possono essere fonte di confusione e complicazioni; gli ACL ALLOW che non sono definiti esplicitamente vengono implicitamente negati. Quando vengono impostati gli ACE DENY, agli utenti potrebbe essere negato l’accesso quando si aspettano che venga concesso.

Il set precedente di ACE equivale a 755 bit di modalità, il che significa:

- Il proprietario ha pieni diritti.
- I gruppi hanno accesso di sola lettura.
- Altri hanno solo la modalità di lettura.

Tuttavia, anche se i permessi vengono modificati in base all’equivalente di 775, l’accesso può essere negato a causa dell’impostazione DENY esplicita 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 mount NFSv4.1 sia effettivamente chi dichiara di essere. In questi casi, il nome utente e il nome del gruppo provenienti dal client NFSv4.1 aggiungono una stringa di nome e la inviano all’istanza di Google Cloud NetApp Volumes . Se la combinazione di nome utente/gruppo e stringa ID non corrisponde, l’utente e/o il gruppo viene compresso nell’utente predefinito nobody specificato in `/etc/idmapd.conf` file sul client.

Questa stringa ID è un requisito per il corretto rispetto delle autorizzazioni, in particolare quando sono in uso ACL NFSv4.1 e/o Kerberos. Di conseguenza, le dipendenze del server del servizio nomi, come i server LDAP, sono necessarie per garantire la coerenza tra i client e Google Cloud NetApp Volumes per una corretta risoluzione dell’identità dei nomi di utenti e gruppi.

Google Cloud NetApp Volumes utilizza un valore di nome di dominio ID predefinito statico di `defaultv4iddomain.com` . I client NFS utilizzano per impostazione predefinita 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 abilitato in Google Cloud NetApp Volumes, Google Cloud NetApp Volumes automatizza la modifica del dominio ID NFS in base a quanto 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 Google Cloud NetApp Volumes riesce a 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 compressi in

nobody. Se Google Cloud NetApp Volumes non riesce a trovare un nome utente o un nome di gruppo nei file locali o in LDAP, viene utilizzato il valore ID numerico e il client NFS risolve correttamente il nome (simile al comportamento di NFSv3).

Senza modificare il dominio ID NFSv4.1 del client in modo che corrisponda a quello utilizzato dal volume Google Cloud NetApp Volumes , si verifica il seguente comportamento:

- Gli utenti e i gruppi UNIX con voci locali in Google Cloud NetApp Volumes (ad esempio root, come definito in utenti e gruppi UNIX locali) vengono compressi nel valore nobody.
- Gli utenti e i gruppi UNIX con voci in LDAP (se Google Cloud NetApp Volumes è configurato per utilizzare LDAP) vengono compressi in nobody se i domini DNS sono diversi tra i client NFS e Google Cloud NetApp Volumes.
- Gli utenti e i gruppi UNIX senza voci locali o voci LDAP utilizzano il valore ID numerico e vengono risolti nel nome specificato sul client NFS. Se sul client non esiste alcun nome, 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, ecco come appare 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 maggiori informazioni su questo problema e su come risolverlo, consultare la sezione "NFSv4.1 e l'utente/gruppo nobody ."

Dipendenze Kerberos

Se si prevede di utilizzare Kerberos con NFS, è necessario disporre di quanto segue con Google Cloud NetApp Volumes:

- Dominio Active Directory per i servizi del Kerberos Distribution Center (KDC)
- Dominio Active Directory con attributi utente e gruppo popolati con informazioni UNIX per la funzionalità LDAP (NFS Kerberos in Google Cloud NetApp Volumes richiede un mapping tra SPN utente e utente UNIX per un corretto funzionamento).

- LDAP abilitato sull'istanza Google Cloud NetApp Volumes
- Dominio Active Directory per i servizi DNS

NFSv4.1 e l'utente/gruppo nobody

Uno dei problemi più comuni riscontrati con una configurazione NFSv4.1 è quando un file o una cartella viene visualizzato in un elenco utilizzando `ls` come di proprietà del `user:group` combinazione di `nobody:nobody` .

Per 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 il gruppo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Chi è nessuno?

IL `nobody` l'utente in NFSv4.1 è diverso dall' `nfsnobody` utente. È possibile visualizzare come un client NFS vede ciascun utente eseguendo il comando `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, il `nobody` utente è l'utente predefinito definito da `idmapd.conf` file e può essere definito come qualsiasi utente che si desidera utilizzare.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Perché succede questo?

Poiché la sicurezza tramite la mappatura delle stringhe dei nomi è un principio fondamentale delle operazioni NFSv4.1, il comportamento predefinito quando una stringa dei nomi non corrisponde correttamente è quello di comprimere l'utente in uno che normalmente non avrà accesso ai file e alle cartelle di proprietà di utenti e gruppi.

Quando vedi `nobody` per l'utente e/o il gruppo negli elenchi dei file, questo in genere significa che qualcosa in NFSv4.1 non è configurato correttamente. Qui può entrare in gioco la distinzione tra maiuscole e minuscole.

Ad esempio, se user1@CVSDEMO.LOCAL (uid 1234, gid 1234) accede a un'esportazione, Google Cloud NetApp Volumes deve essere in grado di trovare user1@CVSDEMO.LOCAL (uid 1234, gid 1234). Se l'utente in Google Cloud NetApp Volumes è USER1@CVSDEMO.LOCAL, non ci sarà corrispondenza (USER1 maiuscolo anziché 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'
```

Sia il client che il server devono concordare sul fatto che un utente sia effettivamente chi dichiara di essere, pertanto è necessario verificare quanto segue per assicurarsi che l'utente visualizzato dal client abbia le stesse informazioni dell'utente visualizzato da Google Cloud NetApp Volumes .

- **Dominio ID NFSv4.x.** Cliente: `idmapd.conf` file; Google Cloud NetApp Volumes utilizza `defaultv4iddomain.com` e non può essere modificato manualmente. Se si utilizza LDAP con NFSv4.1, Google Cloud NetApp Volumes modifica il dominio ID in quello utilizzato dal dominio di ricerca DNS, che è lo stesso del dominio AD.
- **Nome utente e ID numerici.** Ciò determina dove il client sta cercando i nomi utente e sfrutta la configurazione del cambio del servizio nomi: client: `nsswitch.conf` e/o file passwd e group locali; Google Cloud NetApp Volumes non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è abilitato.
- **Nome del gruppo e ID numerici.** Ciò determina dove il client sta cercando i nomi dei gruppi e sfrutta la configurazione dello switch del servizio nomi: client: `nsswitch.conf` e/o file passwd e group locali; Google Cloud NetApp Volumes non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è abilitato.

Nella quasi totalità dei casi, se vedi `nobody` negli elenchi di utenti e gruppi dei client, il problema è la traduzione dell'ID di dominio del nome utente o gruppo tra Google Cloud NetApp Volumes e il client NFS. Per evitare questo scenario, utilizzare LDAP per risolvere le informazioni sugli utenti e sui gruppi tra i client e Google Cloud NetApp Volumes.

Visualizzazione delle stringhe ID nome per NFSv4.1 sui client

Se si utilizza NFSv4.1, durante le operazioni NFS viene eseguita una mappatura nome-stringa, come descritto in precedenza.

Oltre all'utilizzo `/var/log/messages` per trovare un problema con gli ID NFSv4, puoi usare "nfsidmap -l" comando sul client NFS per visualizzare quali nomi utente sono stati correttamente mappati sul dominio NFSv4.

Ad esempio, questo è l'output del comando dopo che un utente che può essere trovato dal client e Google

Cloud NetApp Volumes 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 viene mappato correttamente nel dominio ID NFSv4.1 (in questo caso, `netapp-user`) tenta di accedere allo stesso mount e tocca un file, gli viene assegnato `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 all'utente `pcuser` nel display ma non `netapp-user` ; questo è l'utente anonimo nella nostra regola di politica 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 di file a più client SMB su una rete Ethernet. File e cartelle sono presentati ai client tramite

condivisioni, che possono essere configurate con diverse proprietà e offrono il controllo degli accessi tramite autorizzazioni a livello di condivisione. SMB può essere presentato a qualsiasi client che supporti il protocollo, inclusi client Windows, Apple e Linux.

Google Cloud NetApp Volumes fornisce supporto per 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 Google Cloud NetApp Volumes , Google Cloud NetApp Volumes cerca un nome utente UNIX utilizzando i metodi configurati dagli amministratori di Google Cloud NetApp Volumes .
- Se è configurato un provider di identità UNIX esterno (LDAP) e i nomi utente Windows/UNIX sono identici, i nomi utente Windows verranno mappati 1:1 ai nomi utente UNIX senza bisogno di alcuna configurazione aggiuntiva. Quando LDAP è abilitato, Active Directory viene utilizzato per ospitare gli attributi UNIX per gli oggetti utente e gruppo.
- Se i nomi Windows e i nomi UNIX non corrispondono in modo identico, è necessario configurare LDAP per consentire a Google Cloud NetApp Volumes 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 vengono mappati su un utente UNIX locale predefinito denominato `pcuser` in Google Cloud NetApp Volumes. Ciò significa che i file scritti in Windows dagli utenti che corrispondono a `pcuser` mostra la proprietà UNIX come `pcuser` in ambienti NAS multiprotocollo. `pcuser` ecco effettivamente il `nobody` utente in ambienti Linux (UID 65534).

Nelle distribuzioni con solo SMB, il `pcuser` la mappatura avviene comunque, ma non avrà importanza, perché la proprietà dell'utente e del gruppo 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 volumi NFS o a doppio protocollo dopo la loro creazione.

Windows sfrutta Kerberos per l'autenticazione del nome utente con i controller di dominio Active Directory, il che richiede uno scambio di nome utente/password con i controller di dominio Active Directory, esterno all'istanza di Google Cloud NetApp Volumes . L'autenticazione Kerberos viene utilizzata quando `\\SERVERNAME` Il percorso UNC viene utilizzato dai client SMB e vale quanto segue:

- Esiste una voce DNS A/AAAA per SERVERNAME
- Esiste un SPN valido per l'accesso SMB/CIFS per SERVERNAME

Quando viene creato un volume SMB Google Cloud NetApp Volumes , il nome dell'account macchina viene creato come definito nella sezione"Come Google Cloud NetApp Volumes viene visualizzato in Active Directory." Il nome dell'account macchina diventa anche il percorso di accesso alla condivisione SMB perché Google Cloud NetApp Volumes sfrutta il DNS dinamico (DDNS) per creare le voci A/AAAA e PTR necessarie nel DNS e le voci SPN necessarie sul principale dell'account macchina.

> Per creare voci PTR, la zona di ricerca inversa per l'indirizzo IP dell'istanza di Google Cloud NetApp Volumes deve esistere sul server DNS.

Ad esempio, questo volume Google Cloud NetApp Volumes utilizza il seguente percorso di condivisione UNC: `\\cvs-east- 433d.cvsdemo.local` .

In Active Directory, queste sono le voci SPN generate da Google Cloud NetApp 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
```

Ecco il risultato della ricerca DNS diretta/inversa:

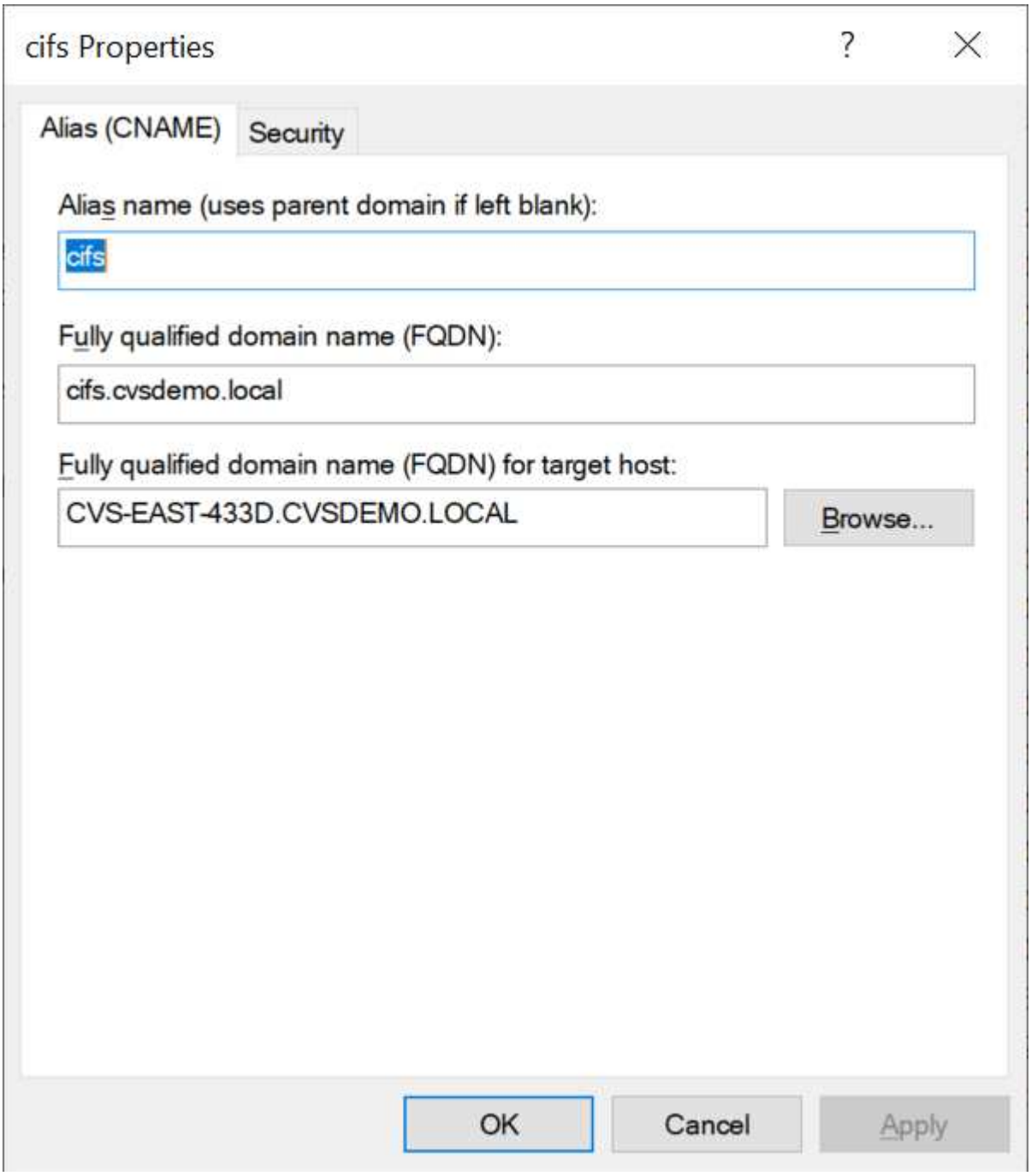
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Facoltativamente, è possibile applicare un maggiore controllo degli accessi abilitando/richiedendo la crittografia SMB per le condivisioni SMB in Google Cloud NetApp Volumes. Se la crittografia SMB non è supportata da uno degli endpoint, l'accesso non è consentito.

Utilizzo di alias di nomi SMB

In alcuni casi, potrebbe essere un problema di sicurezza per gli utenti finali conoscere il nome dell'account macchina utilizzato per Google Cloud NetApp Volumes. In altri casi, potresti semplicemente voler fornire un percorso di accesso più semplice ai tuoi utenti finali. In questi casi è possibile creare alias SMB.

Se si desidera creare alias per il percorso di condivisione SMB, è possibile sfruttare quello che è noto come record CNAME nel DNS. Ad esempio, se si desidera utilizzare il nome `\\CIFS` per accedere alle azioni invece di `\\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 SPN aggiuntivo aggiunto all'account macchina esistente forniscono l'accesso Kerberos.



Ecco 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:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Questa è la query SPN risultante dopo l'aggiunta di nuovi SPN:

```
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 una cattura di pacchetti, possiamo vedere la richiesta di configurazione della sessione utilizzando l'SPN collegato 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

Google Cloud NetApp Volumes 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 che puoi utilizzare. Con la crittografia AES e SMB abilitata, il livello di sicurezza aumenta ulteriormente.

Google Cloud NetApp Volumes supporta anche la compatibilità con le versioni precedenti per l'autenticazione LM e NTLM. Quando Kerberos non è configurato correttamente (ad esempio durante la creazione di alias SMB), l'accesso condiviso ricorre a metodi di autenticazione più deboli (ad esempio NTLMv2). Poiché questi meccanismi sono meno sicuri, in alcuni ambienti Active Directory sono disabilitati. Se i metodi di autenticazione più deboli sono disabilitati e Kerberos non è configurato correttamente, l'accesso alla condivisione fallisce perché non esiste un metodo di autenticazione valido a cui ricorrere.

Per informazioni sulla configurazione/visualizzazione dei livelli di autenticazione supportati in Active Directory, vedere "Sicurezza di rete: livello di autenticazione di LAN Manager" .

Modelli di autorizzazione

Autorizzazioni NTFS/File

Le autorizzazioni NTFS sono le autorizzazioni applicate ai file e alle cartelle nei file system che aderiscono alla logica NTFS. È possibile applicare le autorizzazioni NTFS in `Basic` O `Advanced` e può essere impostato su `Allow` O `Deny` per il controllo degli accessi.

Le autorizzazioni di base includono quanto segue:

- Controllo completo
- Modificare
- Leggi ed esegui
- Leggere
- Scrivere

Quando si impostano le autorizzazioni per un utente o un gruppo, definite ACE, queste risiedono in un ACL. Le autorizzazioni NTFS utilizzano le stesse basi di lettura/scrittura/esecuzione dei bit della modalità UNIX, ma possono anche estendersi a controlli di accesso più granulari ed estesi (noti anche come autorizzazioni speciali), come Assumi proprietà, Crea cartelle/Aggiungi dati, Scrivi attributi e altro ancora.

I bit della 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 forniscono le stesse funzionalità degli ACL NTFS.

Le autorizzazioni NTFS sono più specifiche delle autorizzazioni di condivisione e possono essere utilizzate insieme a queste ultime. Con le strutture di autorizzazione NTFS si applica la più restrittiva. Pertanto, i dinieghi espliciti a un utente o a un gruppo annullano anche il Controllo completo quando si definiscono i diritti di accesso.

Le autorizzazioni NTFS sono controllate dai client SMB di Windows.

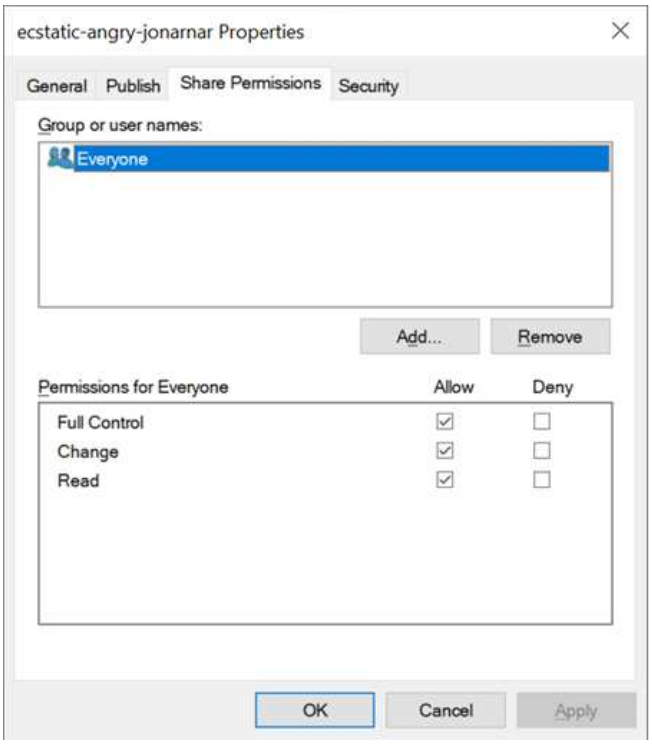
Condividi i permessi

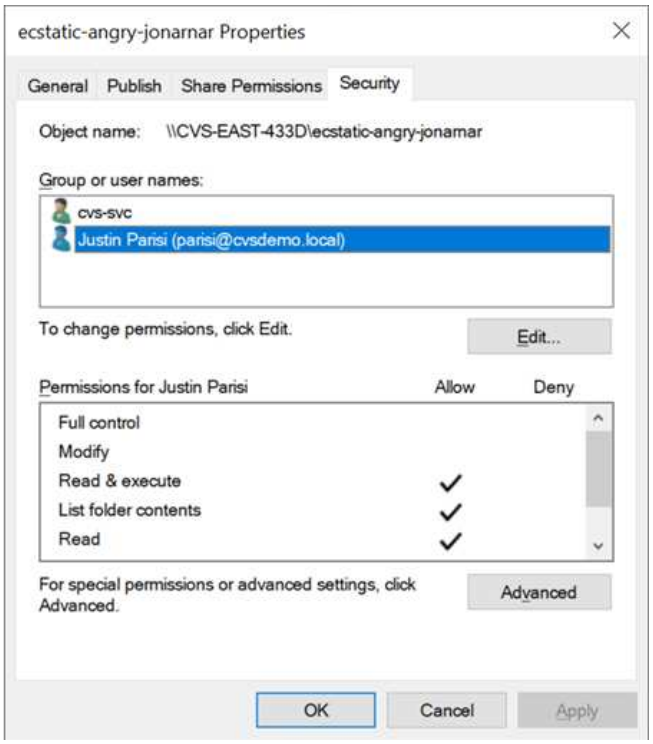
Le autorizzazioni di condivisione sono più generali delle autorizzazioni NTFS (solo Lettura/Modifica/Controllo completo) e controllano l'accesso iniziale a una condivisione SMB, in modo simile al funzionamento delle regole dei criteri di esportazione NFS.

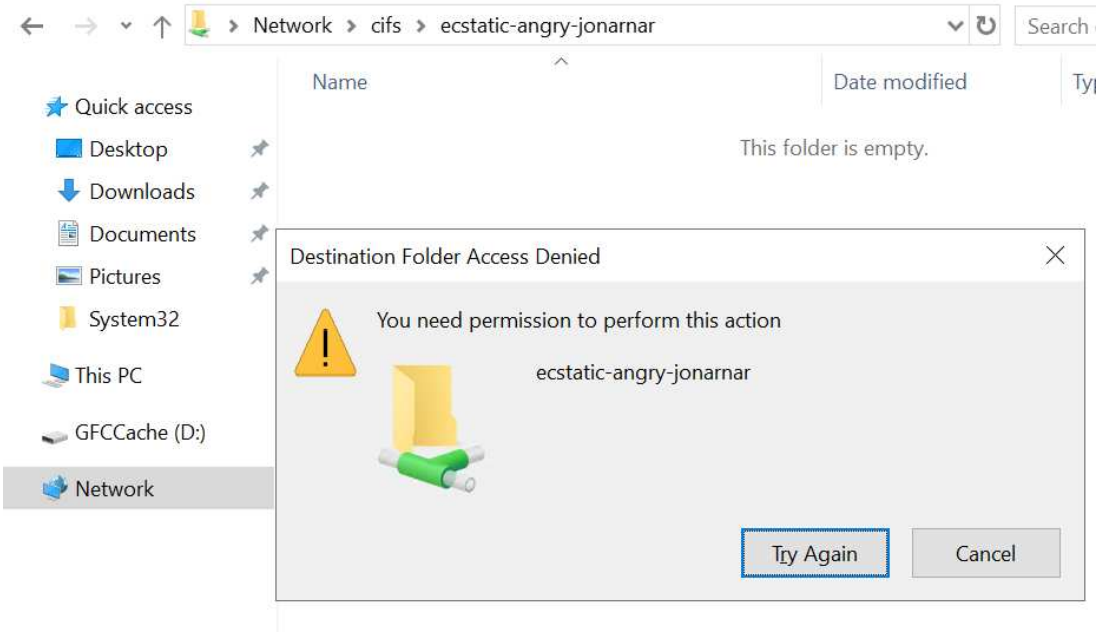
Sebbene le regole dei criteri di esportazione NFS controllino l'accesso tramite informazioni basate sull'host, quali indirizzi IP o nomi host, le autorizzazioni di condivisione SMB possono controllare l'accesso utilizzando ACE utente e gruppo in un ACL di condivisione. È possibile impostare gli ACL di condivisione dal client Windows o dall'interfaccia utente di gestione Google Cloud NetApp Volumes .

Per impostazione predefinita, gli ACL di condivisione e gli ACL del volume iniziale includono Tutti con controllo completo. Gli ACL dei file dovrebbero essere modificati, ma le autorizzazioni di condivisione vengono annullate 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 del volume Google Cloud NetApp Volumes , gli viene negato l'accesso per creare file e cartelle anche se l'ACL di condivisione è impostato su Tutti con controllo completo, come mostrato nella figura seguente.







Per ottenere i migliori risultati in termini di sicurezza, procedere come segue:

- Rimuovere tutti dagli ACL di condivisione e file e impostare invece l'accesso alla condivisione per utenti o gruppi.
- Utilizzare gruppi per il controllo degli accessi anziché singoli utenti per semplificare la gestione e accelerare la rimozione/aggiunta di utenti per condividere gli ACL tramite la gestione dei gruppi.
- Consentire un accesso di condivisione meno restrittivo e più generale agli ACE sulle autorizzazioni di condivisione e bloccare l'accesso agli utenti e ai gruppi con autorizzazioni di file per un controllo di accesso più granulare.
- Evitare l'uso generale di ACL di negazione esplicite, perché sostituiscono gli ACL di autorizzazione. Limitare l'uso di ACL di negazione esplicita per utenti o gruppi a cui è necessario impedire rapidamente

l'accesso a un file system.

- Assicurati di prestare attenzione al "Eredità 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 implica che a ogni file al di sotto di tale directory o volume vengano aggiunte autorizzazioni ereditate, il che può creare comportamenti indesiderati quali accessi/negazioni involontarie e lunghi cicli di modifica delle autorizzazioni man mano che ogni file viene modificato.

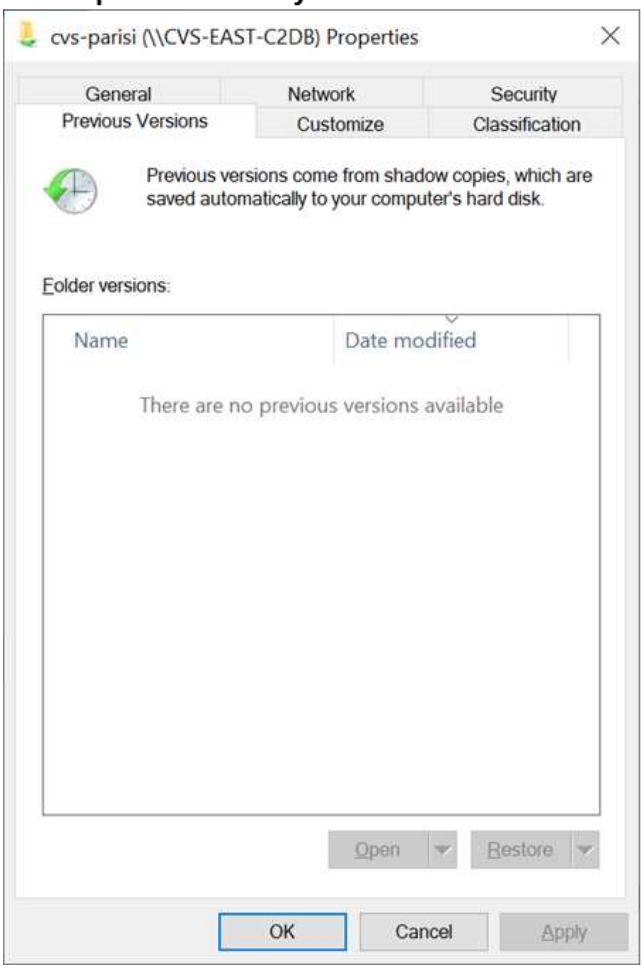
Le funzionalità di sicurezza della condivisione SMB

Quando si crea per la prima volta un volume con accesso SMB in Google Cloud NetApp Volumes, vengono presentate una serie di opzioni per proteggere tale volume.

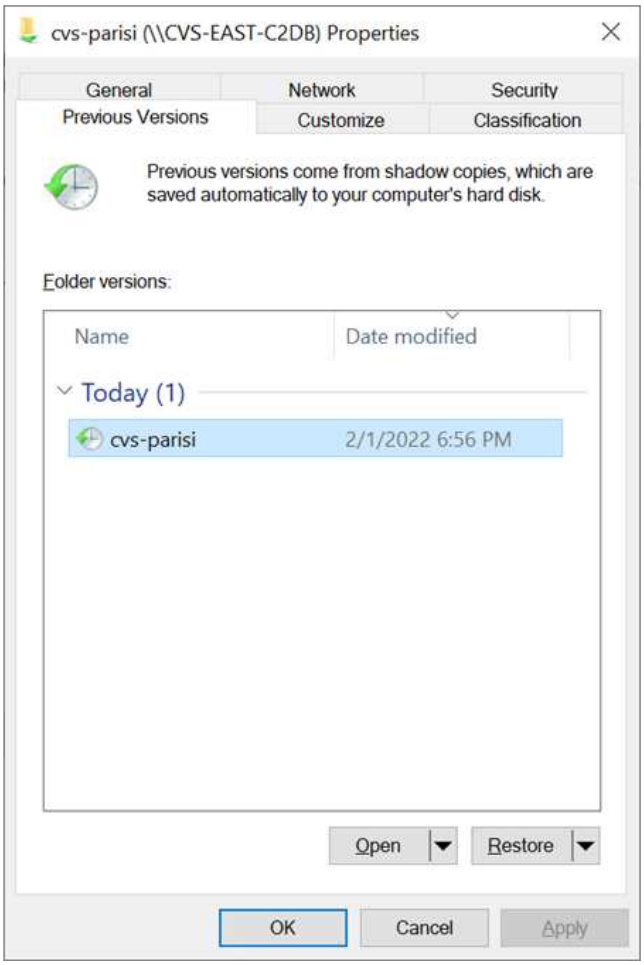
Alcune di queste scelte dipendono dal livello di Google Cloud NetApp Volumes (Prestazioni o Software) e includono:

- **Rendi visibile la directory degli snapshot (disponibile sia per NetApp Volumes-Performance che per NetApp Volumes-SW).** Questa opzione controlla se i client SMB possono accedere o meno alla directory Snapshot in una condivisione SMB(`\\server\share\~snapshot` e/o scheda Versioni precedenti). L'impostazione predefinita è Non selezionato, il che significa che il volume per impostazione predefinita nasconde e non consente l'accesso al `~snapshot` directory e non vengono visualizzate copie Snapshot nella scheda Versioni precedenti per il volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Potrebbe essere opportuno nascondere le copie Snapshot agli utenti finali per motivi di sicurezza, prestazioni (nascondere queste cartelle dalle scansioni AV) o preferenze. Gli snapshot di Google Cloud NetApp Volumes

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 sui file o sulle cartelle al momento in cui è stata creata la 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. Gli utenti e i 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 fuori dalla directory Snapshot.

- **Abilita la crittografia SMB (disponibile sia per NetApp Volumes-Performance che per NetApp Volumes-SW).** Per impostazione predefinita, la crittografia SMB è disabilitata sulla condivisione SMB (non selezionata). Selezionando la casella si abilita la crittografia SMB, il che significa che il traffico tra il client e il server SMB viene crittografato durante il transito, negoziando i livelli di crittografia più elevati supportati. Google Cloud NetApp Volumes supporta la crittografia fino a AES-256 per SMB. L'abilitazione della crittografia SMB comporta una riduzione delle prestazioni che potrebbe essere percepita o meno dai client SMB, nell'ordine del 10-20%. NetApp consiglia vivamente di effettuare dei test per verificare se tale riduzione delle prestazioni è accettabile.
- **Nascondi condivisione SMB (disponibile sia per NetApp Volumes-Performance che per NetApp Volumes-SW).** Impostando questa opzione si nasconde il percorso di condivisione SMB dalla normale navigazione. Ciò significa che i client che non conoscono il percorso di condivisione non possono vedere le condivisioni quando accedono al percorso UNC predefinito (ad esempio `\\NetApp Volumes-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).
- **Abilita l'enumerazione basata sull'accesso (ABE) (solo NetApp Volumes-SW).** Questa operazione è simile a quella per nascondere la condivisione SMB, con la differenza che le condivisioni o i file vengono nascosti solo agli utenti o ai gruppi che non dispongono delle autorizzazioni per accedere agli oggetti. Ad esempio, se l'utente Windows `joe` non è consentito almeno l'accesso in lettura tramite i permessi, quindi l'utente Windows `joe` non riesco a vedere la condivisione SMB o i file. Questa opzione è disabilitata per impostazione predefinita, ma è possibile abilitarla selezionando la casella di controllo. Per ulteriori informazioni su ABE, consultare l'articolo della Knowledge Base NetApp "Come funziona l'enumerazione basata sull'accesso (ABE)?"
- **Abilita il supporto della condivisione Continuously Available (CA) (solo NetApp Volumes-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 backend Google Cloud NetApp Volumes . Non si tratta di una funzione di sicurezza, ma offre una migliore resilienza complessiva. Attualmente, solo le applicazioni SQL Server e FSLogix sono supportate per questa funzionalità.

Condivisioni nascoste predefinite

Quando un server SMB viene creato in Google Cloud NetApp Volumes, ci sono "condivisioni amministrative nascoste" (utilizzando la convenzione di denominazione $) che vengono creati in aggiunta alla condivisione SMB del volume dati. Tra questi rientrano C$ (accesso allo spazio dei nomi) e IPC$ (condivisione di named pipe per la comunicazione tra programmi, 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: viene utilizzata esclusivamente per chiamate RPC e "Per impostazione predefinita, Windows non consente l'accesso anonimo a queste condivisioni" .

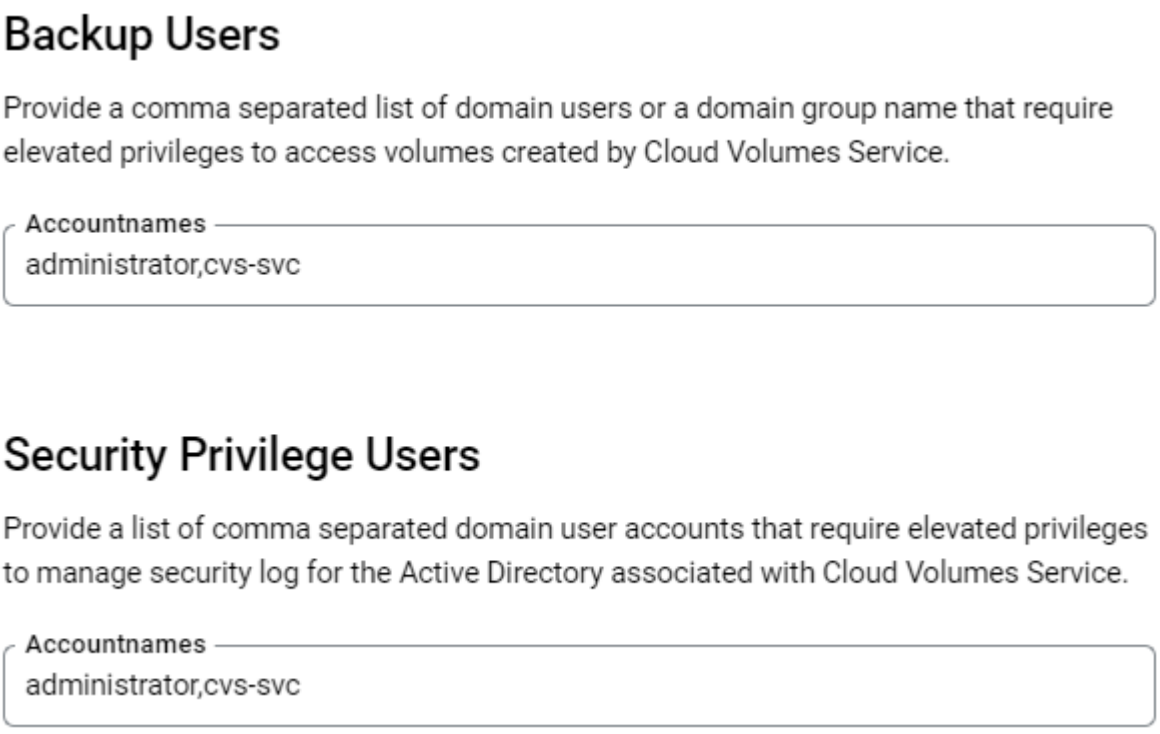
La condivisione C$ consente l'accesso BUILTIN/Administrators per impostazione predefinita, ma l'automazione Google Cloud NetApp Volumes rimuove l'ACL della condivisione e non consente l'accesso a nessuno perché l'accesso alla condivisione C$ consente la visibilità di tutti i volumi montati nei file system di Google Cloud NetApp Volumes . Di conseguenza, i tentativi di navigare verso `\\SERVER\C$` fallire.

Account con diritti di amministratore/backup locali/INTEGRATI

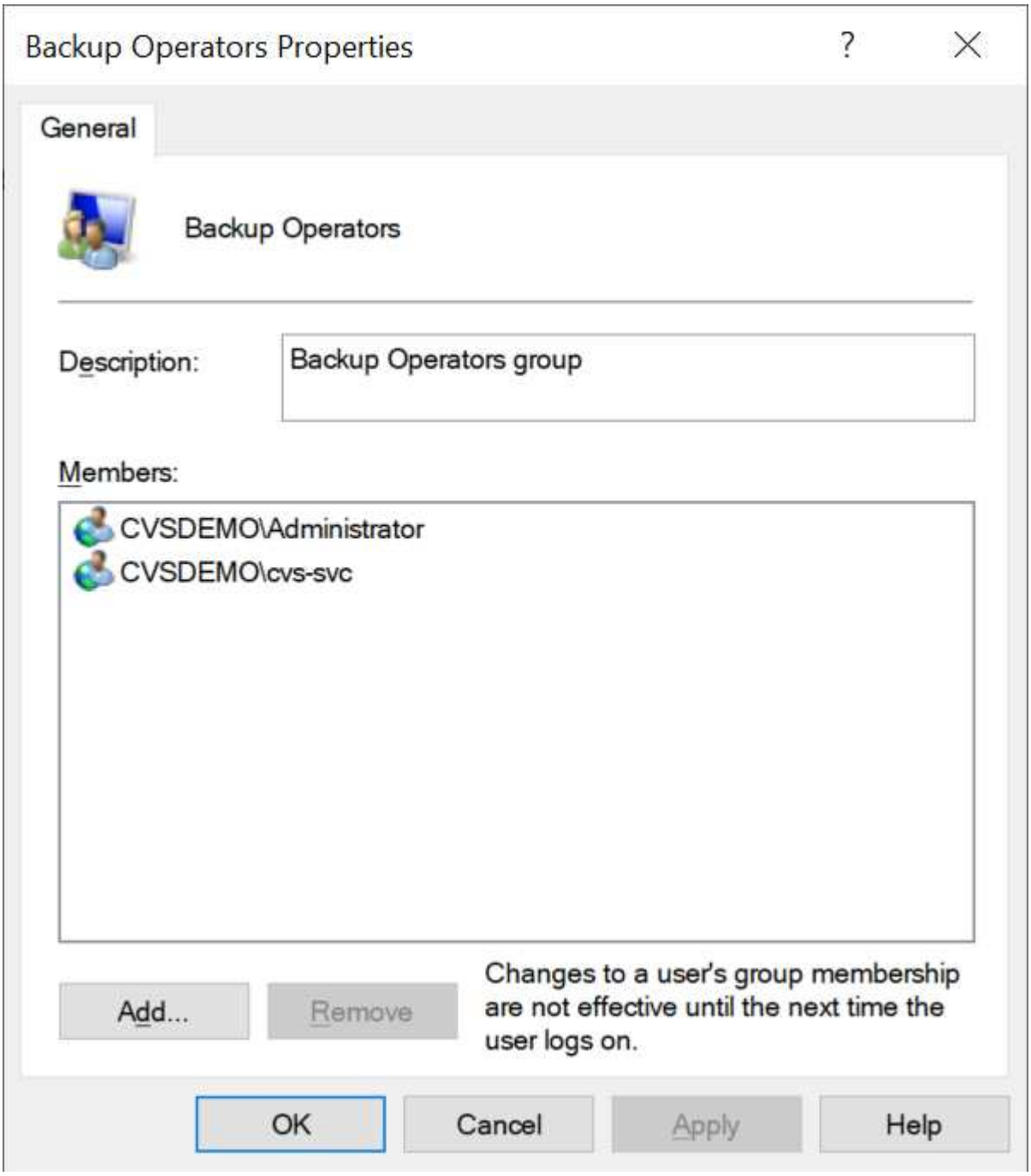
I server SMB Google Cloud NetApp Volumes mantengono funzionalità simili ai normali server SMB Windows, in quanto sono presenti gruppi locali (ad esempio BUILTIN\Administrators) che applicano diritti di accesso a utenti e gruppi di dominio selezionati.

Quando si specifica un utente da aggiungere agli utenti di backup, l'utente viene aggiunto al gruppo BUILTIN\Backup Operators nell'istanza di Google Cloud NetApp Volumes che utilizza quella connessione Active Directory, che quindi ottiene "SeBackupPrivilege e SeRestorePrivilege" .

Quando si aggiunge un utente agli utenti con privilegi di sicurezza, all'utente viene assegnato il privilegio di sicurezza, che è utile in alcuni casi di utilizzo dell'applicazione, come "SQL Server su condivisioni SMB" .



È possibile visualizzare le appartenenze ai gruppi locali Google Cloud NetApp Volumes tramite MMC con i privilegi appropriati. La figura seguente mostra gli utenti aggiunti tramite la console Google Cloud NetApp Volumes .

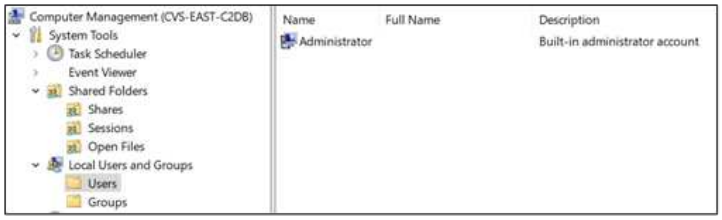


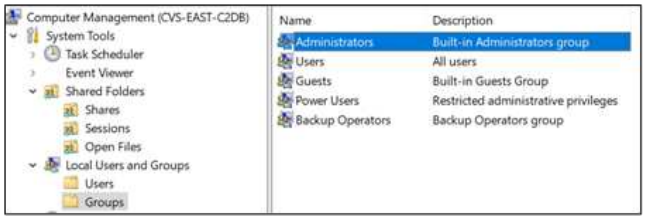
La tabella seguente mostra l'elenco dei gruppi BUILTIN predefiniti e quali utenti/gruppi vengono aggiunti per impostazione predefinita.

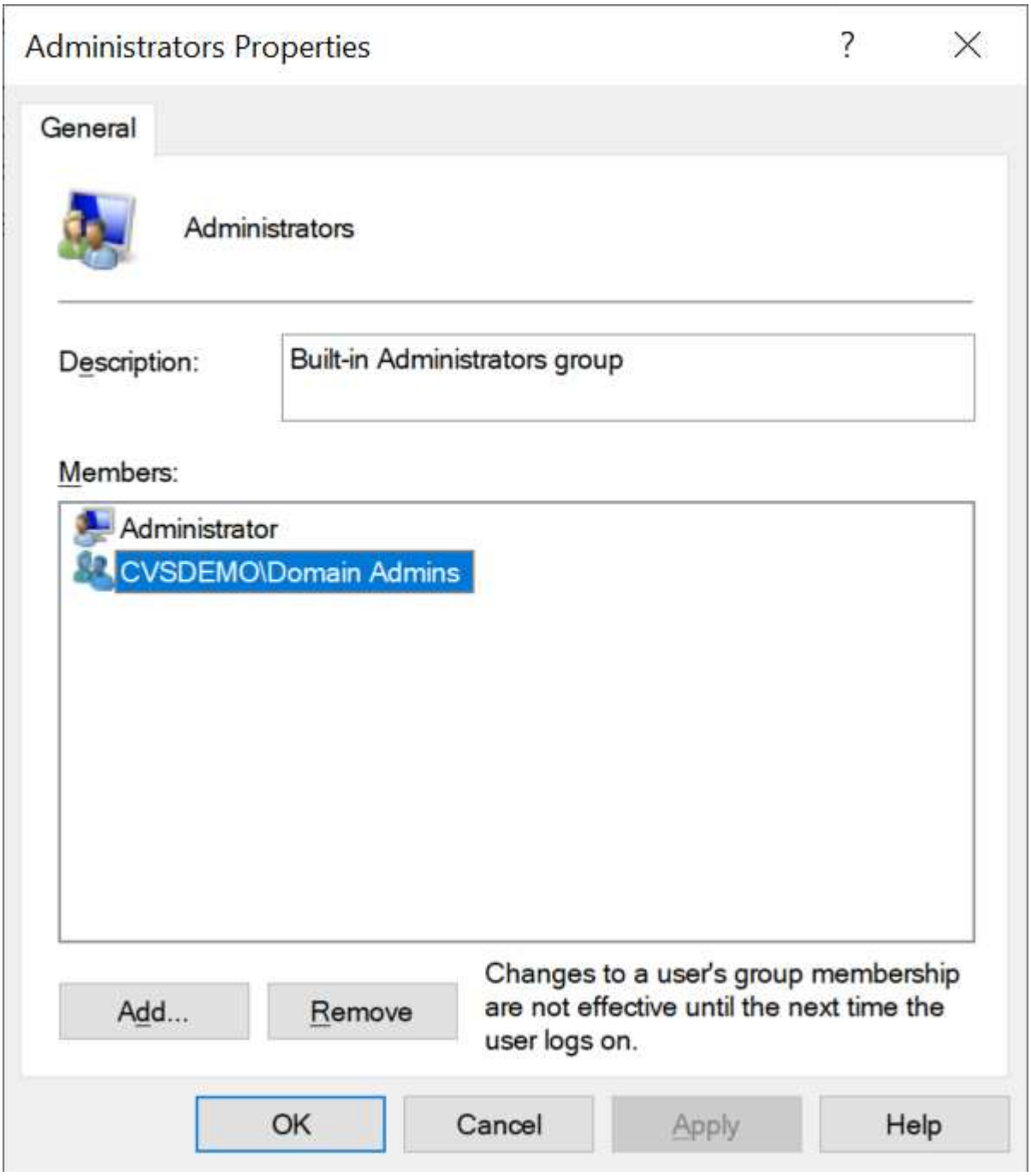
Gruppo locale/INTEGRATO	Membri predefiniti
BUILTIN\Amministratori*	DOMINIO\Amministratori di dominio
BUILTIN\Operatori di backup*	Nessuno
BUILTIN\Ospiti	DOMINIO\Ospiti del dominio
BUILTIN\Utenti esperti	Nessuno
BUILTIN\Utenti di dominio	DOMINIO\Utenti del dominio

*L’appartenenza al gruppo è controllata nella configurazione della connessione Google Cloud NetApp Volumes Active Directory.

È possibile visualizzare utenti e gruppi locali (e 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 Administrator vengono aggiunti al gruppo BUILTIN\Administrators in Google Cloud NetApp Volumes. Al momento non è possibile modificarlo.







Accesso MMC/Gestione computer

L'accesso SMB in Google Cloud NetApp Volumes fornisce connettività al Computer Management MMC, che consente di visualizzare le condivisioni, gestire gli ACL delle condivisioni e visualizzare/gestire le sessioni SMB e aprire i file.

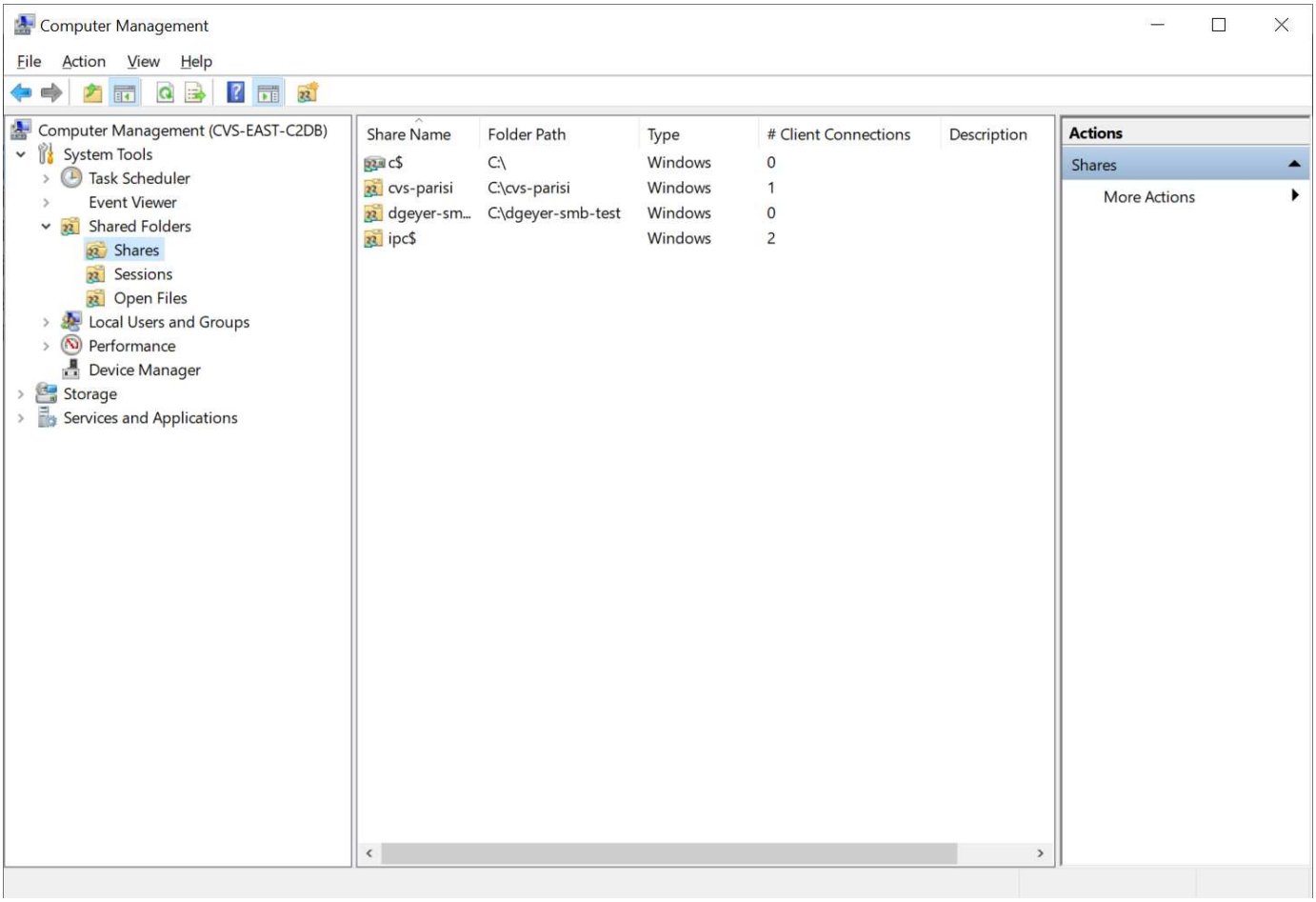
Per utilizzare MMC per visualizzare le condivisioni e le sessioni SMB in Google Cloud NetApp Volumes, l'utente attualmente connesso deve essere un amministratore di dominio. Ad altri utenti è consentito l'accesso per visualizzare o gestire il server SMB da MMC e viene visualizzata la finestra di dialogo Non hai autorizzazioni quando si tenta di visualizzare condivisioni o sessioni sull'istanza SMB di Google Cloud NetApp Volumes .

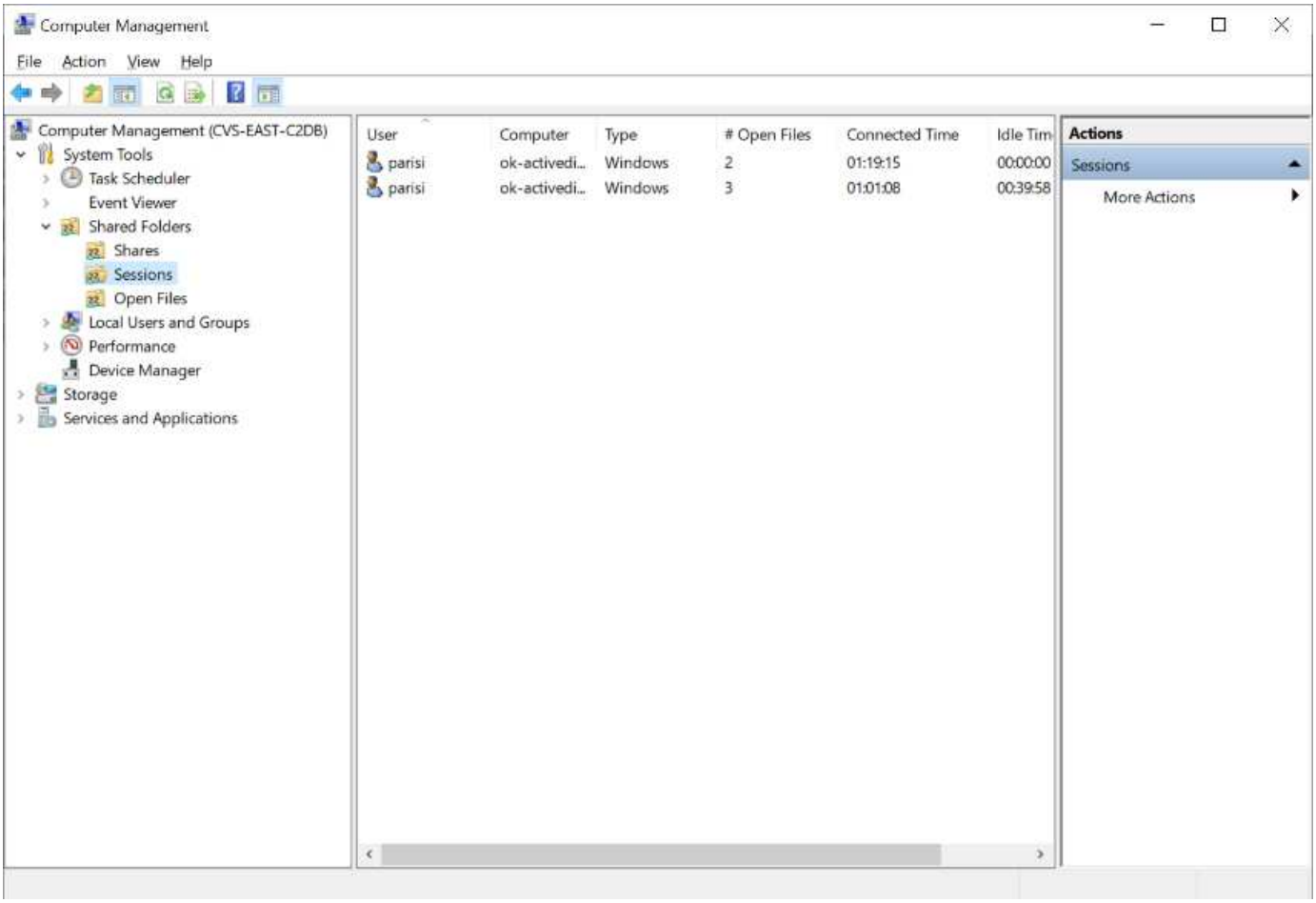
Per connettersi al server SMB, aprire Gestione computer, fare clic con il pulsante destro del mouse su Gestione computer e quindi selezionare Connetti a un altro computer. Si apre la finestra di dialogo Seleziona

computer, in cui è possibile immettere il nome del server SMB (disponibile nelle informazioni sul volume Google Cloud NetApp Volumes).

Quando visualizzi le condivisioni SMB con le autorizzazioni appropriate, vedi tutte le condivisioni disponibili nell'istanza di Google Cloud NetApp Volumes che condividono la connessione ad Active Directory. Per controllare questo comportamento, imposta l'opzione Nascondi condivisioni SMB sull'istanza del volume Google Cloud NetApp Volumes .

Ricorda che è consentita una sola connessione Active Directory per regione.





Nella tabella seguente è riportato un elenco delle funzionalità supportate/non supportate per MMC.

Funzioni supportate	Funzioni non supportate
• Visualizza le azioni • Visualizza le sessioni SMB attive • Visualizza i file aperti • Visualizza utenti e gruppi locali • Visualizza le appartenenze ai gruppi locali • Enumera l'elenco delle sessioni, dei file e delle connessioni ad albero nel sistema • Chiudere i file aperti nel sistema • Chiudere le sessioni aperte • Crea/gestisci condivisioni	• Creazione di nuovi utenti/gruppi locali • Gestione/visualizzazione di utenti/gruppi locali esistenti • Visualizza eventi o registri delle prestazioni • Gestione dello storage • Gestione di servizi e applicazioni

Informazioni sulla sicurezza del server SMB

Il server SMB in Google Cloud NetApp Volumes utilizza una serie di opzioni che definiscono i criteri di sicurezza per le connessioni SMB, tra cui aspetti quali lo sfasamento dell'orologio Kerberos, l'età dei ticket, la crittografia e altro ancora.

La tabella seguente contiene un elenco di tali opzioni, la loro funzione, le configurazioni predefinite e se

possono essere modificate con Google Cloud NetApp Volumes. Alcune opzioni non si applicano a Google Cloud NetApp Volumes.

Opzione di sicurezza	Cosa fa	Valore predefinito	Può cambiare?
Massima differenza tra l'orologio Kerberos e quello di rete (minuti)	Distorsione temporale massima tra Google Cloud NetApp Volumes e i controller di dominio. Se la differenza oraria supera i 5 minuti, l'autenticazione Kerberos fallisce. Questo è impostato sul valore predefinito di Active Directory.	5	NO
Durata del ticket Kerberos (ore)	Tempo massimo di validità di un ticket Kerberos prima di richiedere un rinnovo. Se non si verifica alcun rinnovo prima delle 10 ore, è necessario ottenere un nuovo biglietto. Google Cloud NetApp Volumes esegue questi rinnovi automaticamente. Il valore predefinito di Active Directory è 10 ore.	10	NO
Rinnovo massimo dei ticket Kerberos (giorni)	Numero massimo di giorni per cui è possibile rinnovare un ticket Kerberos prima che sia necessaria una nuova richiesta di autorizzazione. Google Cloud NetApp Volumes rinnova automaticamente i ticket per le connessioni SMB. Il valore predefinito di Active Directory è sette giorni.	7	NO
Timeout di connessione Kerberos KDC (sec)	Numero di secondi prima che scada il tempo di una connessione KDC.	3	NO
Richiedi la firma per il traffico SMB in entrata	Impostazione per richiedere la firma per il traffico SMB. Se impostato su true, i client che non supportano la firma non riescono a connettersi.	Falso	

Opzione di sicurezza	Cosa fa	Valore predefinito	Può cambiare?
Richiedi complessità password per account utente locali	Utilizzato per le password degli utenti SMB locali. Google Cloud NetApp Volumes non supporta la creazione di utenti locali, pertanto questa opzione non si applica a Google Cloud NetApp Volumes.	VERO	NO
Utilizzare start_tls per le connessioni LDAP di Active Directory	Utilizzato per abilitare l'avvio delle connessioni TLS per Active Directory LDAP. Google Cloud NetApp Volumes al momento non supporta questa abilitazione.	Falso	NO
La crittografia AES-128 e AES-256 per Kerberos è abilitata?	Questa opzione controlla se la crittografia AES viene utilizzata per le connessioni Active Directory ed è controllata tramite l'opzione Abilita crittografia AES per l'autenticazione Active Directory durante la creazione/modifica della connessione Active Directory.	Falso	SÌ
Livello di compatibilità LM	Livello di dialetti di autenticazione supportati per le connessioni Active Directory. Vedi la sezione "Dialetti di autenticazione SMB " per maggiori informazioni.	ntlmv2-krb	NO
Richiedi crittografia SMB per il traffico CIFS in entrata	Richiede la crittografia SMB per tutte le condivisioni. Questa opzione non è utilizzata da Google Cloud NetApp Volumes; impostare invece la crittografia in base al volume (vedere la sezione "Le funzionalità di sicurezza della condivisione SMB ").	Falso	NO

Opzione di sicurezza	Cosa fa	Valore predefinito	Può cambiare?
Sicurezza della sessione client	Imposta la firma e/o la sigillatura per la comunicazione LDAP. Questa impostazione non è attualmente disponibile in Google Cloud NetApp Volumes, ma potrebbe essere necessaria nelle versioni future per risolvere il problema. La correzione dei problemi di autenticazione LDAP dovuti alla patch di Windows è trattata nella sezione"Associazione del canale LDAP." .	Nessuno	NO
Abilitazione SMB2 per connessioni DC	Utilizza SMB2 per le connessioni CC. Abilitato per impostazione predefinita.	Predefinito di sistema	NO
Ricerca di referral LDAP	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando una voce non viene trovata nel primo server. Al momento questa funzionalità non è supportata da Google Cloud NetApp Volumes.	Falso	NO
Utilizzare LDAPS per connessioni Active Directory sicure	Abilita l'uso di LDAP su SSL. Attualmente non supportato da Google Cloud NetApp Volumes.	Falso	NO
La crittografia è richiesta per la connessione DC	Richiede la crittografia per le connessioni DC riuscite. Disabilitato per impostazione predefinita in Google Cloud NetApp Volumes.	Falso	NO

Doppio protocollo/multiprotocollo

Google Cloud NetApp Volumes offre la possibilità di condividere gli stessi set di dati sia con client SMB che NFS, mantenendo al contempo le autorizzazioni di accesso appropriate ("doppio protocollo"). Ciò avviene coordinando la mappatura delle identità tra i protocolli e utilizzando un LDAP server back-end centralizzato per fornire le identità UNIX a Google Cloud NetApp Volumes. Puoi utilizzare Windows Active Directory per

fornire utenti Windows e UNIX e semplificarne l'utilizzo.

Controllo degli accessi

- **Condividi i controlli di accesso.** Determina 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 del client alle esportazioni. Le esportazioni NFS vengono gestite dall'istanza di Google Cloud NetApp Volumes . SMB utilizza condivisioni CIFS/SMB e ACL di condivisione per fornire un controllo più granulare a livello di utente e di gruppo. È possibile configurare gli ACL a livello di condivisione solo dai client SMB utilizzando https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Computer Management^] con un account che dispone di diritti di amministratore sull'istanza Google Cloud NetApp Volumes (vedere la sezione "Account con diritti di amministratore/backup locali/INTEGRATI").
- **Controlli di accesso ai file.** Controlla le autorizzazioni a livello di file o cartella e sono sempre gestite dal client NAS. I client NFS possono utilizzare bit in modalità tradizionale (rwx) o ACL NFSv4. I client SMB sfruttano le autorizzazioni NTFS.

Il controllo di accesso per i volumi che forniscono dati sia a NFS che a SMB dipende dal protocollo in uso. Per informazioni sui permessi con doppio protocollo, vedere la sezione "Modello di autorizzazione ."

Mappatura degli utenti

Quando un client accede a un volume, Google Cloud NetApp Volumes tenta di mappare l'utente in arrivo a un utente valido nella direzione opposta. Ciò è necessario affinché venga determinato un accesso corretto attraverso i protocolli e per garantire che l'utente che richiede l'accesso sia effettivamente chi dichiara di essere.

Ad esempio, se un utente Windows denominato `joe` tenta di accedere a un volume con autorizzazioni UNIX tramite SMB, quindi Google Cloud NetApp Volumes esegue una ricerca per trovare un utente UNIX corrispondente denominato `joe` . Se ne esiste uno, i file vengono scritti su una condivisione SMB come utente Windows `joe` appare come utente UNIX `joe` dai client NFS.

In alternativa, se un utente UNIX denominato `joe` tenta di accedere a un volume Google Cloud NetApp Volumes con autorizzazioni Windows, l'utente UNIX deve essere in grado di mapparsi a un utente Windows valido. In caso contrario, l'accesso al volume verrà 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 autorizzazione

Quando si utilizzano configurazioni a doppio protocollo, Google Cloud NetApp Volumes 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 oppure, nel caso di un protocollo doppio, in base a una scelta effettuata al momento della creazione del volume Google Cloud NetApp Volumes .

- Se si utilizza solo NFS, i volumi Google Cloud NetApp Volumes utilizzano autorizzazioni UNIX.
- Se si utilizza solo SMB, i volumi Google Cloud NetApp Volumes utilizzano autorizzazioni NTFS.

Se si sta creando un volume a doppio protocollo, è possibile scegliere lo stile ACL durante la creazione del volume. Questa decisione dovrebbe essere presa in base alla gestione dei permessi desiderata. Se gli utenti gestiscono le autorizzazioni dai client Windows/SMB, selezionare NTFS. Se i tuoi utenti preferiscono utilizzare client NFS e chmod/chown, utilizza gli stili di sicurezza UNIX.

Considerazioni sulla creazione di connessioni Active Directory

Google Cloud NetApp Volumes offre la possibilità di connettere la tua istanza di Google Cloud NetApp Volumes a un server Active Directory esterno per la gestione delle identità sia per gli utenti SMB che UNIX. Per utilizzare SMB in Google Cloud NetApp Volumes è necessario creare una connessione Active Directory.

La configurazione prevede diverse opzioni che richiedono una certa considerazione per motivi di sicurezza. Il server Active Directory esterno può essere un'istanza locale o nativa del cloud. Se si utilizza un server Active Directory locale, non esporre il dominio alla rete esterna (ad esempio con una DMZ o un indirizzo IP esterno). Utilizzare invece tunnel privati sicuri o VPN, trust forestali unidirezionali o connessioni di rete dedicate alle reti locali con "Accesso privato a Google" . Per ulteriori informazioni su "best practice per l'utilizzo di Active Directory in Google Cloud" .

> NetApp Volumes-SW richiede che i server Active Directory si trovino nella stessa regione. Se si tenta una connessione DC in NetApp Volumes-SW a un'altra regione, il tentativo fallisce. Quando si utilizza NetApp Volumes-SW, assicurarsi di creare siti Active Directory che includano i DC di Active Directory e quindi specificare i siti in Google Cloud NetApp Volumes per evitare tentativi di connessione DC tra regioni.

Credenziali di Active Directory

Quando SMB o LDAP per NFS sono abilitati, Google Cloud NetApp Volumes interagisce con i controller di Active Directory per creare un oggetto account macchina da utilizzare per l'autenticazione. Non c'è differenza rispetto al 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 sicurezza non consentono l'uso di un account amministratore Windows su server esterni come Google Cloud NetApp Volumes. In alcuni casi, come buona pratica di sicurezza, l'utente amministratore di Windows viene completamente disabilitato.

Autorizzazioni necessarie per creare account macchina SMB

Per aggiungere oggetti macchina Google Cloud NetApp Volumes a un Active Directory, è necessario un account che abbia diritti amministrativi sul dominio o che abbia "autorizzazioni delegate per creare e modificare oggetti account macchina" è richiesto a una OU specificata. È possibile farlo con la procedura guidata Delega del controllo in Active Directory creando un'attività personalizzata che fornisca all'utente l'accesso alla creazione/eliminazione di oggetti computer con le seguenti autorizzazioni di accesso:

- Lettura/scrittura
- Crea/Elimina tutti gli oggetti figlio
- Leggi/scrivi tutte le proprietà
- Cambia/Reimposta password

In questo modo si aggiunge automaticamente un ACL di sicurezza per l'utente definito all'OU in Active Directory e si riduce al minimo l'accesso all'ambiente Active Directory. Dopo che un utente è stato delegato, è possibile fornire il nome utente e la password come credenziali di Active Directory in questa finestra.

> Il nome utente e la password trasmessi al dominio Active Directory sfruttano la crittografia Kerberos durante la query e la creazione dell'oggetto account macchina per una maggiore sicurezza.

Dettagli della connessione Active Directory

The "Dettagli di connessione ad Active Directory" forniscono indicazioni agli amministratori per fornire informazioni specifiche sullo schema di Active Directory per il posizionamento degli account macchina, come ad esempio:

- **Tipo di connessione Active Directory.** Utilizzato per specificare se la connessione Active Directory in una regione viene utilizzata per i volumi del tipo di servizio Google Cloud NetApp Volumes o NetApp Volumes-Performance. Se questa impostazione non è corretta su una connessione esistente, potrebbe non funzionare correttamente se utilizzata o modificata.
- **Dominio.** Il nome di dominio di Active Directory.
- **Sito.** Limita i server Active Directory a un sito specifico per motivi di sicurezza e prestazioni "considerazioni". Questo è necessario quando più server Active Directory si estendono su più regioni, perché Google Cloud NetApp Volumes attualmente non supporta le richieste di autenticazione Active Directory verso server Active Directory in una regione diversa da quella dell'istanza Google Cloud NetApp Volumes. (Ad esempio, il domain controller Active Directory si trova in una regione supportata solo da NetApp Volumes-Performance, ma si desidera una condivisione SMB in un'istanza NetApp Volumes-SW.)
- **Server DNS.** Server DNS da utilizzare nelle ricerche dei nomi.
- **Nome NetBIOS (facoltativo).** Se lo si desidera, il nome NetBIOS del server. Questo è ciò che viene utilizzato quando vengono creati nuovi account macchina utilizzando la connessione Active Directory. Ad esempio, se il nome NetBIOS è impostato su NetApp Volumes-EAST, i nomi degli account macchina saranno NetApp Volumes-EAST-{1234}. Vedi la sezione"Come Google Cloud NetApp Volumes viene visualizzato in Active Directory" per maggiori informazioni.
- **Unità organizzativa (UO).** L'unità organizzativa specifica per creare l'account del computer. Questa funzionalità è utile se si delega il controllo a un utente per gli account macchina di una specifica OU.
- **Crittografia AES.** È anche possibile selezionare o deselezionare la casella di controllo Abilita crittografia AES per autenticazione AD. L'abilitazione della crittografia AES per l'autenticazione di Active Directory garantisce una maggiore sicurezza per la comunicazione tra Google Cloud NetApp Volumes e Active Directory durante le ricerche di utenti e gruppi. Prima di abilitare questa opzione, verifica con l'amministratore del tuo dominio che i controller di dominio Active Directory supportino l'autenticazione AES.

> Per impostazione predefinita, la maggior parte dei server Windows non disabilita i cifrari più deboli (come DES o RC4-HMAC), ma se si sceglie di disabilitarli, verificare che la connessione di Google Cloud NetApp Volumes Active Directory sia stata configurata per abilitare AES. In caso contrario, si verificheranno errori di autenticazione. L'abilitazione della crittografia AES non disabilita i cifrari più deboli, ma aggiunge il supporto per i cifrari AES all'account macchina SMB Google Cloud NetApp Volumes .

Dettagli del dominio Kerberos

Questa opzione non si applica ai server SMB. Viene invece utilizzato durante la configurazione di NFS Kerberos per il sistema Google Cloud NetApp Volumes . Una volta inseriti questi dettagli, il dominio NFS Kerberos viene configurato (simile a un file krb5.conf su Linux) e viene utilizzato quando NFS Kerberos viene specificato durante la creazione del volume Google Cloud NetApp Volumes , poiché la connessione Active Directory funge da NFS Kerberos Distribution Center (KDC).

> Al momento, i KDC non Windows non sono supportati per l'utilizzo con Google Cloud NetApp Volumes.

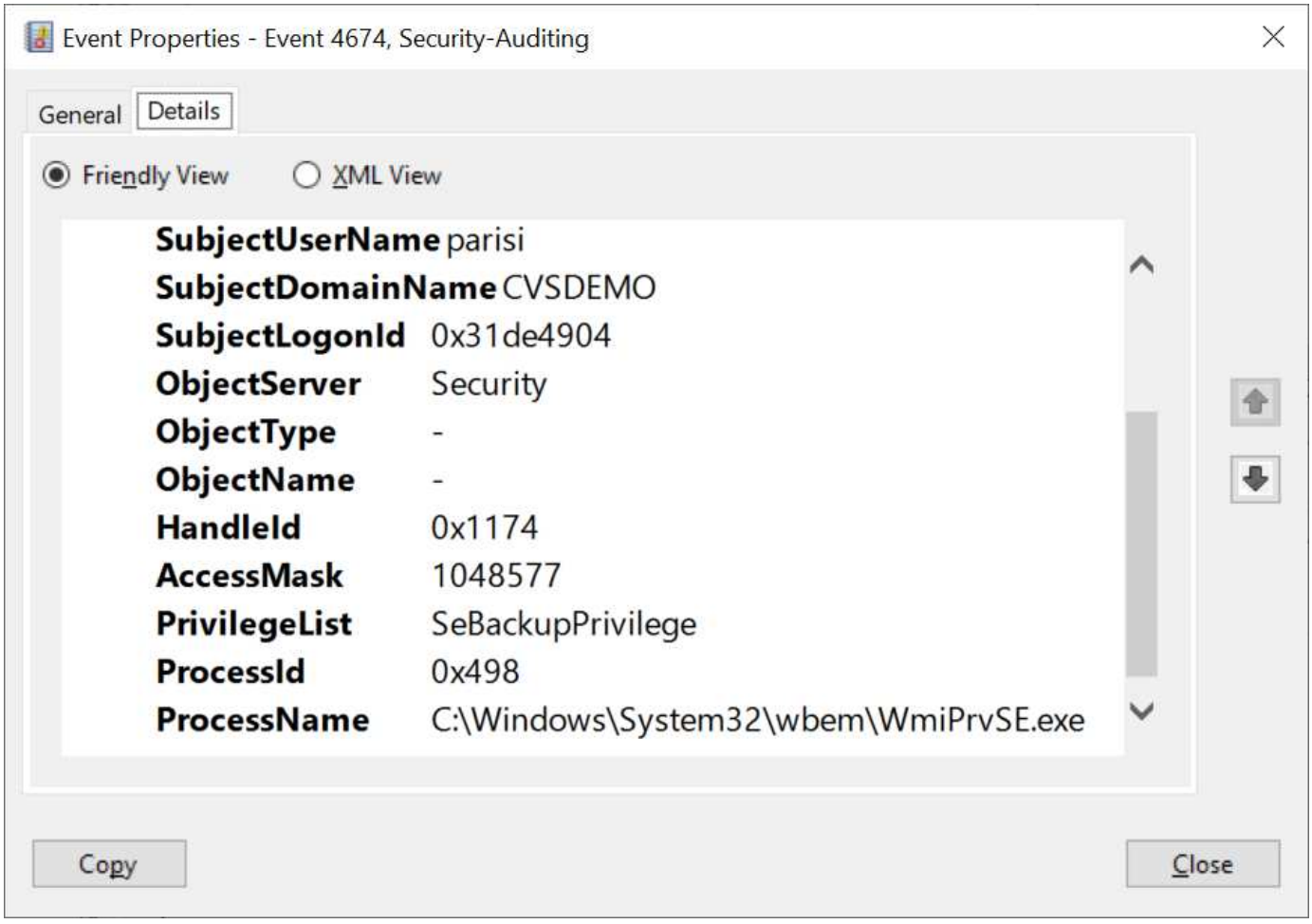
Regione

Una regione consente di specificare la posizione in cui risiede la connessione Active Directory. Questa regione deve essere la stessa regione del volume Google Cloud NetApp Volumes .

- **Utenti NFS locali con LDAP.** In questa sezione è presente anche un'opzione per consentire agli utenti NFS locali con LDAP. Questa opzione deve essere lasciata deselezionata se si desidera estendere il supporto di appartenenza al gruppo utenti UNIX oltre il limite 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 questa opzione deselezionata. 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 Google Cloud NetApp Volumes . I privilegi di backup (SeBackupPrivilege) sono necessari per alcune applicazioni per eseguire correttamente il backup e il ripristino dei dati nei volumi NAS. Questo utente ha un livello elevato di accesso ai dati nel volume, quindi dovresti considerare "abilitando la verifica dell'accesso di quell'utente" . Dopo l'abilitazione, gli eventi di controllo vengono visualizzati in Visualizzatore eventi > Registri di Windows > Sicurezza.



Utenti con privilegi di sicurezza

Questa opzione consente di specificare gli utenti Windows che dispongono delle autorizzazioni di modifica della sicurezza per il volume Google Cloud NetApp Volumes . I privilegi di sicurezza (SeSecurityPrivilege) sono necessari per alcune applicazioni("come SQL Server") per impostare correttamente i permessi durante

l'installazione. Questo privilegio è necessario per gestire il registro di sicurezza. Sebbene questo privilegio non sia potente quanto 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 Google Cloud NetApp Volumes viene visualizzato in Active Directory

Google Cloud NetApp Volumes viene visualizzato in Active Directory come un normale oggetto account macchina. Le convenzioni di denominazione sono le seguenti.

- CIFS/SMB e NFS Kerberos creano oggetti account macchina separati.
- NFS con LDAP abilitato crea un account macchina in Active Directory per i binding LDAP Kerberos.
- I volumi a doppio protocollo con LDAP condividono l'account macchina CIFS/SMB per LDAP e SMB.
- Gli account macchina CIFS/SMB utilizzano una convenzione di denominazione NAME-1234 (ID casuale di quattro cifre con un trattino aggiunto a un nome di <10 caratteri) per l'account macchina. È possibile definire NAME tramite l'impostazione del nome NetBIOS sulla connessione Active Directory (vedere la sezione "Dettagli della connessione Active Directory ").
- NFS Kerberos utilizza NFS-NAME-1234 come convenzione di denominazione (fino a 15 caratteri). Se vengono utilizzati più di 15 caratteri, il nome è NFS-TRUNCATED-NAME-1234.
- Le istanze NetApp Volumes-Performance solo NFS con LDAP abilitato creano un account macchina SMB per l'associazione al server LDAP con la stessa convenzione di denominazione delle istanze CIFS/SMB.
- Quando viene creato un account macchina SMB, le condivisioni amministrative nascoste predefinite (vedere la sezione"Condivisioni nascoste predefinite") vengono create anche (c$, admin$, ipc$), ma a tali condivisioni non sono assegnati ACL e sono inaccessibili.
- Per impostazione predefinita, gli oggetti account macchina vengono posizionati in CN=Computer, ma è possibile specificare un'unità organizzativa diversa quando necessario. Vedi la sezione "Autorizzazioni necessarie per creare account macchina SMB " per informazioni sui diritti di accesso necessari per aggiungere/rimuovere oggetti account macchina per Google Cloud NetApp Volumes.

Quando Google Cloud NetApp Volumes aggiunge l'account macchina SMB ad Active Directory, vengono compilati i seguenti campi:

- cn (con il nome del server SMB specificato)
- dNSHostName (con SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (consente DES_CBC_MD5, RC4_HMAC_MD5 se la crittografia AES non è abilitata; se la crittografia AES è abilitata, DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 sono consentiti per lo scambio di ticket Kerberos con l'account macchina per 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 disabilitare i tipi di crittografia Kerberos più deboli (enctype) sull'account macchina, è possibile modificare il valore msDS-SupportedEncryptionTypes sull'account macchina impostando uno dei valori nella tabella seguente per consentire solo AES.

valore msDS-SupportedEncryptionTypes	Enctype abilitato
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 abilitare la crittografia AES per gli account macchina SMB, fare clic su Abilita crittografia AES per autenticazione AD durante la creazione della connessione Active Directory.

Per abilitare la crittografia AES per NFS Kerberos, "consultare la documentazione Google Cloud NetApp Volumes".

Altre dipendenze del servizio infrastruttura NAS (KDC, LDAP e DNS)

Quando si utilizza Google Cloud NetApp Volumes per le condivisioni NAS, potrebbero essere necessarie dipendenze esterne per un corretto funzionamento. Queste dipendenze si verificano in circostanze specifiche. La tabella seguente mostra le varie opzioni di configurazione e quali dipendenze sono necessarie, se presenti.

Configurazione	Dipendenze richieste
Solo NFSv3	Nessuno
Solo Kerberos NFSv3	Directory attiva di Windows: * KDC * DNS * LDAP
Solo NFSv4.1	Configurazione della mappatura dell'ID client (/etc/idmap.conf)
Solo Kerberos NFSv4.1	• Configurazione della mappatura dell'ID client (/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
Solo PMI	Directory attiva: * KDC * DNS
NAS multiprotocollo (NFS e SMB)	• Configurazione del mapping dell'ID client (solo NFSv4.1; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

Rotazione delle chiavi Kerberos/reimpostazione delle password per gli oggetti account macchina

Con gli account macchina SMB, Google Cloud NetApp Volumes pianifica reimpostazioni periodiche della password per l'account macchina SMB. Questi ripristini delle password avvengono tramite crittografia Kerberos e sono programmati ogni quarta domenica a un orario casuale tra le 23:00 e l'1:00. Queste reimpostazioni delle password modificano le versioni delle chiavi Kerberos, ruotano le keytab archiviate nel sistema Google Cloud NetApp Volumes e aiutano a mantenere un livello di sicurezza più elevato per i server SMB in esecuzione in Google Cloud NetApp Volumes. Le password degli account macchina sono casuali e

non sono note agli amministratori.

Per gli account macchina Kerberos NFS, la reimpostazione della password avviene solo quando viene creata/scambiata una nuova keytab con il KDC. Al momento, questa operazione non è possibile in Google Cloud NetApp Volumes.

Porte di rete per l'utilizzo con LDAP e Kerberos

Quando utilizzi LDAP e Kerberos, dovresti determinare le porte di rete usate da questi servizi. Puoi trovare un elenco completo delle porte usate da Google Cloud NetApp Volumes nel "Documentazione Google Cloud NetApp Volumes sulle considerazioni sulla sicurezza".

LDAP

Google Cloud NetApp Volumes funge da client LDAP e utilizza query di ricerca LDAP standard per ricerche di utenti e gruppi per identità UNIX. LDAP è necessario se si intende utilizzare utenti e gruppi al di fuori degli utenti predefiniti standard forniti da Google Cloud NetApp Volumes. LDAP è necessario anche se si prevede di utilizzare NFS Kerberos con entità utente (ad esempio user1@domain.com). Attualmente è supportato solo LDAP che utilizza Microsoft Active Directory.

Per utilizzare Active Directory come server LDAP UNIX, è necessario popolare gli attributi UNIX necessari sugli utenti e sui gruppi che si intende utilizzare per le identità UNIX. Google Cloud NetApp Volumes utilizza un modello di schema LDAP predefinito che interroga gli attributi in base a "RFC-2307-bis" . Di conseguenza, la tabella seguente mostra gli attributi minimi necessari di Active Directory da popolare per utenti e gruppi e a cosa serve ciascun attributo.

Per ulteriori informazioni sull'impostazione degli attributi LDAP in Active Directory, vedi "Gestione dell'accesso a doppio protocollo."

Attributo	Cosa fa
uid*	Specifica il nome utente UNIX
Numero uid*	Specifica l'ID numerico dell'utente UNIX
NumeroGid*	Specifica l'ID numerico del gruppo primario dell'utente UNIX
objectClass*	Specifica il tipo di oggetto utilizzato; Google Cloud NetApp Volumes richiede che "user" sia incluso nell'elenco delle classi di oggetti (è incluso nella maggior parte delle distribuzioni di Active Directory per impostazione predefinita).
nome	Informazioni generali sull'account (nome reale, numero di telefono e così via, noti anche come gecos)
unixUserPassword	Non è necessario impostarlo; non viene utilizzato nelle ricerche di identità UNIX per l'autenticazione NAS. Impostando questa opzione, il valore unixUserPassword configurato viene visualizzato in testo normale.

Attributo	Cosa fa
unixHomeDirectory	Definisce il percorso verso le directory home UNIX quando un utente esegue l'autenticazione tramite LDAP da un client Linux. Impostare questa opzione se si desidera utilizzare LDAP per la funzionalità della directory home UNIX.
loginShell	Definisce il percorso verso la shell bash/profile per i client Linux quando un utente si autentica tramite LDAP.

*Indica che l'attributo è obbligatorio per il corretto funzionamento con Google Cloud NetApp Volumes. Gli attributi rimanenti sono riservati esclusivamente all'uso lato client.

Attributo	Cosa fa
cn*	Specifica il nome del gruppo UNIX. Quando si utilizza Active Directory per LDAP, questa impostazione viene effettuata al momento della creazione dell'oggetto, ma può essere modificata in seguito. Questo nome non può essere uguale a quello di 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 Google Cloud NetApp Volumes utilizza l'attributo uid per i nomi utente UNIX.
NumeroGid*	Specifica l'ID numerico del gruppo UNIX.
objectClass*	Specifica il tipo di oggetto utilizzato; Google Cloud NetApp Volumes richiede che il gruppo sia incluso nell'elenco delle classi di oggetti (questo attributo è incluso nella maggior parte delle distribuzioni di Active Directory per impostazione predefinita).
memberUid	Specifica quali utenti UNIX sono membri del gruppo UNIX. Con Active Directory LDAP in Google Cloud NetApp Volumes, questo campo non è necessario. Lo schema LDAP Google Cloud NetApp Volumes utilizza il campo Membro per le appartenenze ai gruppi.
Membro*	Obbligatorio per appartenenze a gruppi/gruppi UNIX secondari. Questo campo viene popolato aggiungendo utenti Windows ai gruppi Windows. Tuttavia, se i gruppi Windows non hanno attributi UNIX popolati, non vengono inclusi negli elenchi di appartenenza al gruppo dell'utente UNIX. Tutti i gruppi che devono essere disponibili in NFS devono popolare gli attributi di gruppo UNIX richiesti elencati in questa tabella.

*Indica che l'attributo è obbligatorio per il corretto funzionamento con Google Cloud NetApp Volumes. Gli attributi rimanenti sono riservati esclusivamente all'uso lato client.

Informazioni di binding LDAP

Per interrogare gli utenti in LDAP, Google Cloud NetApp Volumes deve effettuare il binding (accesso) al servizio LDAP. Questo accesso ha autorizzazioni di sola lettura e viene utilizzato per interrogare gli attributi LDAP UNIX per le ricerche nelle directory. Attualmente, i binding LDAP sono possibili solo utilizzando un account macchina SMB.

È possibile abilitare LDAP solo per `NetApp Volumes-Performance` istanze e utilizzarlo per volumi NFSv3, NFSv4.1 o a doppio protocollo. Per una corretta distribuzione del volume abilitato LDAP, è necessario stabilire una connessione Active Directory nella stessa regione del volume Google Cloud NetApp Volumes .

Quando LDAP è abilitato, in scenari specifici si verifica quanto segue.

- Se per il progetto Google Cloud NetApp Volumes viene utilizzato solo NFSv3 o NFSv4.1, viene creato un nuovo account macchina nel controller di dominio Active Directory e il client LDAP in Google Cloud NetApp Volumes si collega ad Active Directory utilizzando le credenziali dell'account macchina. 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 Google Cloud NetApp Volumes vengono utilizzati volumi a doppio protocollo, per associare il client LDAP in Google Cloud NetApp Volumes ad Active Directory viene utilizzato solo l'account macchina creato per l'accesso SMB. Non vengono creati account macchina aggiuntivi.
- Se i volumi SMB dedicati vengono creati separatamente (prima o dopo l'abilitazione dei volumi NFS con LDAP), l'account macchina per i binding LDAP viene condiviso con l'account macchina SMB.
- Se è abilitato anche NFS Kerberos, vengono creati due account macchina: uno per le condivisioni SMB e/o i binding LDAP e uno per l'autenticazione NFS Kerberos.

Query LDAP

Sebbene i binding LDAP siano crittografati, le query LDAP vengono trasmesse in rete in testo normale utilizzando la porta LDAP comune 389. Questa porta nota non può essere attualmente modificata in Google Cloud NetApp Volumes. Di conseguenza, chiunque abbia accesso allo sniffing dei pacchetti nella rete può vedere i nomi degli utenti e dei gruppi, gli ID numerici e le appartenenze ai gruppi.

Tuttavia, le VM di Google Cloud non possono intercettare il traffico unicast di altre VM. Solo le VM che partecipano attivamente al traffico LDAP (ovvero che sono in grado di effettuare il binding) possono visualizzare il traffico proveniente dal server LDAP. Per ulteriori informazioni sullo sniffing dei pacchetti in Google Cloud NetApp Volumes, vedere la sezione"Considerazioni sullo sniffing/tracciamento dei pacchetti."

Impostazioni predefinite della configurazione del client LDAP

Quando LDAP è abilitato in un'istanza Google Cloud NetApp Volumes , per impostazione predefinita viene creata una configurazione client LDAP con dettagli di configurazione specifici. In alcuni casi, le opzioni non si applicano a Google Cloud NetApp Volumes (non supportate) oppure non sono configurabili.

Opzione client LDAP	Cosa fa	Valore predefinito	Può cambiare?
Elenco dei server LDAP	Imposta i nomi dei server LDAP o gli indirizzi IP da utilizzare per le query. Questa opzione non viene utilizzata per Google Cloud NetApp Volumes. Al contrario, per definire i server LDAP viene utilizzato il dominio Active Directory.	Non impostato	NO
Dominio di Active Directory	Imposta il dominio Active Directory da utilizzare per le query LDAP. Google Cloud NetApp Volumes sfrutta i record SRV per LDAP in DNS per trovare i server LDAP nel dominio.	Impostato 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 Google Cloud NetApp Volumes. Utilizzare invece i siti di Active Directory per controllare la selezione del server LDAP.	Non impostato.	NO
Associa utilizzando le credenziali del server SMB	Si collega a LDAP utilizzando l'account macchina SMB. Attualmente, l'unico metodo di associazione LDAP supportato in Google Cloud NetApp Volumes.	VERO	NO
Modello di schema	Modello di schema utilizzato per le query LDAP.	MS-AD-BIS	NO
Porta del server LDAP	Numero di porta utilizzato per le query LDAP. Google Cloud NetApp Volumes utilizza attualmente solo la porta LDAP standard 389. LDAPS/porta 636 non è attualmente supportato.	389	NO

Opzione client LDAP	Cosa fa	Valore predefinito	Può cambiare?
LDAPS è abilitato?	Controlla se per le query e le associazioni viene utilizzato LDAP su Secure Sockets Layer (SSL). Attualmente non supportato da Google Cloud NetApp Volumes.	Falso	NO
Timeout della query (sec)	Timeout per le query. Se le query richiedono più tempo del valore specificato, le query falliscono.	3	NO
Livello minimo di autenticazione Bind	Il livello di associazione minimo supportato. Poiché Google Cloud NetApp Volumes utilizza account macchina per i binding LDAP e Active Directory non supporta i binding anonimi per impostazione predefinita, questa opzione non è rilevante per la sicurezza.	Anonimo	NO
Associa DN	Nome utente/distinto (DN) utilizzato per i binding quando si utilizza il binding semplice. Google Cloud NetApp Volumes utilizza account macchina per i binding LDAP e attualmente non supporta l'autenticazione del binding semplice.	Non impostato	NO
Base DN	Il DN di base utilizzato per le ricerche LDAP.	Dominio Windows utilizzato per la connessione ad Active Directory, in formato DN (ovvero DC=dominio, DC=locale).	NO
Ambito di ricerca di base	Ambito di ricerca per le ricerche DN di base. I valori possono includere base, livello singolo o sottoalbero. Google Cloud NetApp Volumes supporta solo ricerche nei sottoalberi.	Sottoalbero	NO

Opzione client LDAP	Cosa fa	Valore predefinito	Può cambiare?
DN utente	Definisce il DN da cui iniziano le ricerche degli utenti per le query LDAP. Attualmente non supportato per Google Cloud NetApp Volumes, quindi tutte le ricerche degli utenti iniziano dal DN di base.	Non impostato	NO
Ambito di ricerca dell'utente	Ambito di ricerca per le ricerche DN utente. I valori possono includere base, livello singolo o sottoalbero. Google Cloud NetApp Volumes non supporta l'impostazione dell'ambito di ricerca dell'utente.	Sottoalbero	NO
Gruppo DN	Definisce il DN da cui iniziano le ricerche di gruppo per le query LDAP. Attualmente non supportato per Google Cloud NetApp Volumes, quindi tutte le ricerche di gruppo iniziano dal DN di base.	Non impostato	NO
Ambito di ricerca del gruppo	Ambito di ricerca per le ricerche DN di gruppo. I valori possono includere base, livello singolo o sottoalbero. Google Cloud NetApp Volumes non supporta l'impostazione dell'ambito di ricerca del gruppo.	Sottoalbero	NO
Netgroup DN	Definisce il DN da cui iniziano le ricerche netgroup per le query LDAP. Attualmente non supportato per Google Cloud NetApp Volumes, quindi tutte le ricerche netgroup iniziano dal DN di base.	Non impostato	NO

Opzione client LDAP	Cosa fa	Valore predefinito	Può cambiare?
Ambito di ricerca di Netgroup	Ambito di ricerca per le ricerche DN dei netgroup. I valori possono includere base, livello singolo o sottoalbero. Google Cloud NetApp Volumes non supporta l'impostazione dell'ambito di ricerca netgroup.	Sottoalbero	NO
Utilizzare start_tls su LDAP	Sfrutta Start TLS per connessioni LDAP basate su certificati sulla porta 389. Attualmente non supportato da Google Cloud NetApp Volumes.	Falso	NO
Abilita la ricerca netgroup-by-host	Consente la ricerca di netgroup in base al nome host anziché espandere i netgroup per elencare tutti i membri. Attualmente non supportato da Google Cloud NetApp Volumes.	Falso	NO
DN di Netgroup per host	Definisce il DN da cui iniziano le ricerche netgroup-by-host per le query LDAP. Netgroup-by-host non è attualmente supportato per Google Cloud NetApp Volumes.	Non impostato	NO
Ambito di ricerca Netgroup-by-host	Ambito di ricerca per le ricerche DN netgroup-by-host. I valori possono includere base, livello singolo o sottoalbero. Netgroup-by-host non è attualmente supportato per Google Cloud NetApp Volumes.	Sottoalbero	NO

Opzione client LDAP	Cosa fa	Valore predefinito	Può cambiare?
Sicurezza della sessione client	Definisce il livello di sicurezza della sessione utilizzato da LDAP (firma, sigillo o nessuno). La firma LDAP è supportata da NetApp Volumes-Performance, se richiesta da Active Directory. NetApp Volumes-SW non supporta la firma LDAP. Per entrambi i tipi di servizio, la sigillatura non è attualmente supportata.	Nessuno	NO
Ricerca di referral LDAP	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando una voce non viene trovata nel primo server. Al momento questa funzionalità non è supportata da Google Cloud NetApp Volumes.	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 Google Cloud NetApp Volumes.	Non impostato	NO

Utilizzo di LDAP per la mappatura asimmetrica dei nomi

Per impostazione predefinita, Google Cloud NetApp Volumes mappa gli utenti Windows e gli utenti UNIX con nomi utente identici in modo bidirezionale, senza alcuna configurazione speciale. Finché Google Cloud NetApp Volumes riesce a trovare un utente UNIX valido (con LDAP), si verifica la mappatura dei nomi 1:1. Ad esempio, se l'utente Windows `johnsmith` viene utilizzato, quindi, se Google Cloud NetApp Volumes 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` mostra la corretta proprietà dell'utente e tutti gli ACL che interessano `johnsmith` vengono rispettati indipendentemente dal protocollo NAS in uso. Questo è noto come mappatura simmetrica dei nomi.

La mappatura asimmetrica dei nomi si verifica quando l'identità dell'utente Windows e quella dell'utente UNIX non corrispondono. Ad esempio, se l'utente Windows `johnsmith` ha un'identità UNIX di `jsmith` Google Cloud NetApp Volumes ha bisogno di un modo per essere informato della variazione. Poiché Google Cloud NetApp Volumes attualmente non supporta la creazione di regole di mappatura dei nomi statici, è necessario utilizzare LDAP per cercare l'identità degli utenti sia per le identità Windows che UNIX, per garantire la corretta proprietà di file e cartelle e le autorizzazioni previste.

Per impostazione predefinita, Google Cloud NetApp Volumes include `LDAP` nell'ns-switch dell'istanza per il database di mappatura dei nomi, in modo che per fornire funzionalità di mappatura dei nomi utilizzando LDAP per nomi asimmetrici, sia sufficiente modificare solo alcuni degli attributi utente/gruppo per riflettere ciò che Google Cloud NetApp Volumes cerca.

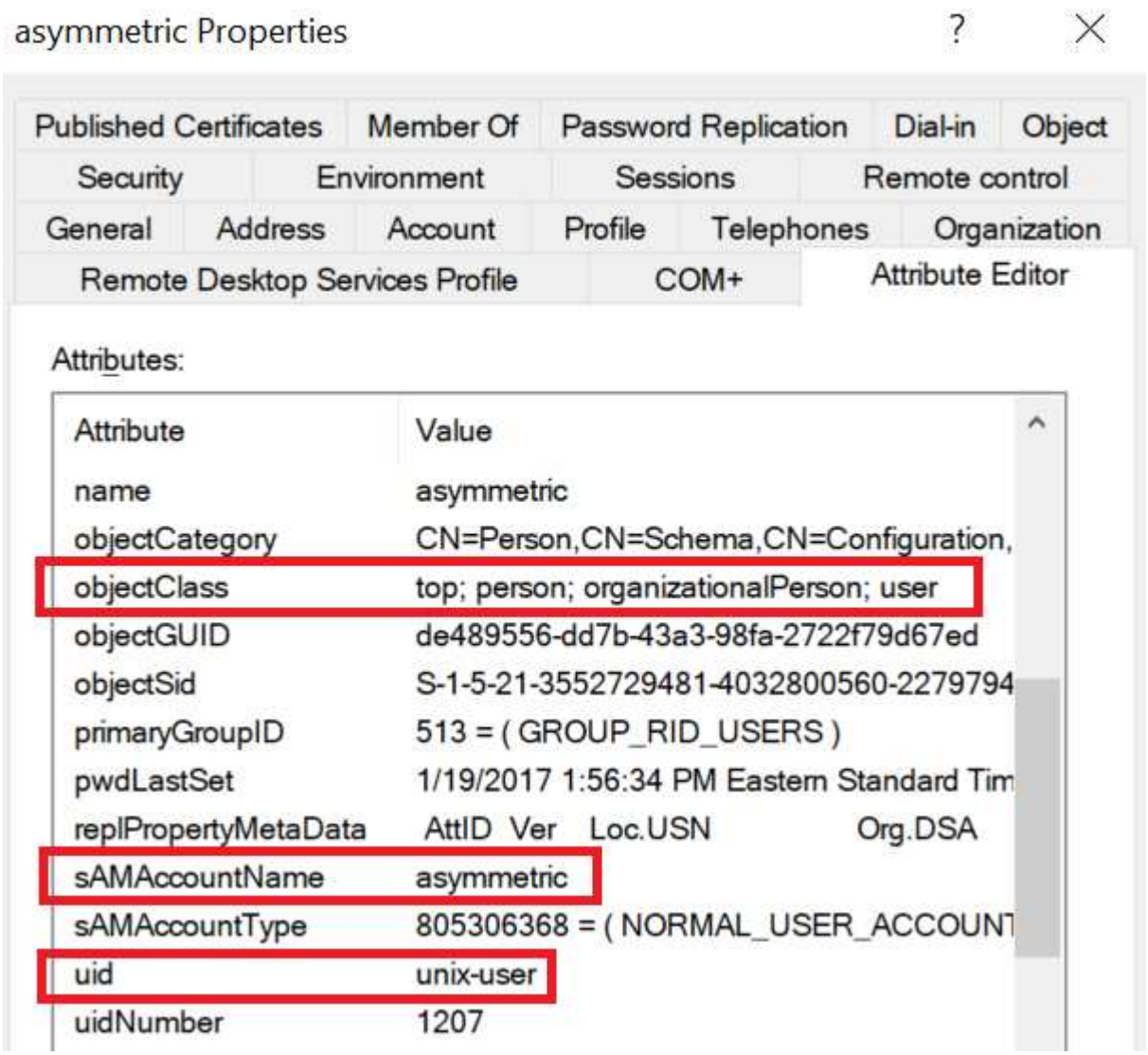
La tabella seguente mostra quali attributi devono essere popolati in LDAP per la funzionalità di mappatura dei nomi asimmetrica. Nella maggior parte dei casi, Active Directory è già configurato per farlo.

Attributo Google Cloud NetApp Volumes	**Cosa fa**	**Valore utilizzato da Google Cloud NetApp Volumes 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 altri valori, se desiderato).
Attributo da Windows a UNIX	che definisce il nome utente di Windows al momento della creazione. Google Cloud NetApp Volumes lo utilizza per le ricerche da Windows a UNIX.	Qui non è necessaria alcuna modifica; sAMAccountName è lo stesso nome di accesso di Windows.
UID	Definisce il nome utente UNIX.	Nome utente UNIX desiderato.

Google Cloud NetApp Volumes attualmente non utilizza prefissi di dominio nelle ricerche LDAP, pertanto gli ambienti LDAP con più domini non funzionano correttamente con le ricerche nella mappa dei nomi LDAP.

L'esempio seguente mostra un utente con il nome Windows `asymmetric` , il nome UNIX `unix-user` e il comportamento che segue quando scrive file sia da SMB che da NFS.

La figura seguente mostra l'aspetto degli attributi LDAP dal server Windows.



Da un client NFS, è possibile interrogare il nome UNIX ma non il nome 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, puoi vedere che il proprietario del file è impostato sull'utente Windows corretto:

```
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 mostrano il proprietario UNIX corretto, 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
```

Associazione del canale LDAP

A causa di una vulnerabilità nei controller di dominio di Windows Active Directory, "Avviso di sicurezza Microsoft ADV190023" modifica il modo in cui i DC consentono i binding LDAP.

L'impatto per Google Cloud NetApp Volumes è lo stesso di qualsiasi client LDAP. Google Cloud NetApp Volumes al momento non supporta il binding dei canali. Poiché Google Cloud NetApp Volumes supporta la firma LDAP per impostazione predefinita tramite negoziazione, l'associazione del canale LDAP non dovrebbe rappresentare un problema. Se si verificano problemi di binding a LDAP con il binding di canale abilitato, seguire i passaggi di risoluzione descritti in ADV190023 per consentire il corretto binding LDAP da Google Cloud NetApp Volumes .

DNS

Active Directory e Kerberos dipendono entrambi dal DNS per la risoluzione dei nomi host in IP/IP in nomi host. Il DNS richiede che la porta 53 sia aperta. Google Cloud NetApp Volumes non apporta alcuna modifica ai record DNS, né attualmente supporta l'uso 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" .

Tieni presente che le risorse all'interno di un progetto Google utilizzano per impostazione predefinita Google Cloud DNS, che non è connesso ad Active Directory DNS. I client che utilizzano Cloud DNS non possono risolvere i percorsi UNC restituiti da Google Cloud NetApp Volumes. I client Windows aggiunti 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, devi configurare il suo DNS in modo che usi il DNS di Active Directory. Facoltativamente, puoi configurare Cloud DNS per inoltrare le richieste al DNS di Active Directory. Vedi "Perché il mio client non riesce a risolvere il nome NetBIOS SMB?"per ulteriori informazioni.

Google Cloud NetApp Volumes al momento non supporta DNSSEC e le query DNS vengono eseguite in testo normale.

Controllo dell'accesso ai file

Attualmente non supportato per Google Cloud NetApp Volumes.

Protezione antivirus

È necessario eseguire la scansione antivirus in Google Cloud NetApp Volumes sul client in una condivisione NAS. Attualmente non esiste alcuna integrazione antivirus nativa con Google Cloud NetApp Volumes.

Funzionamento del servizio

Il team Google Cloud NetApp Volumes gestisce i servizi backend in Google Cloud e utilizza diverse strategie per proteggere la piattaforma e impedire accessi indesiderati.

Ogni cliente ottiene la propria subnet univoca, il cui accesso è separato per impostazione predefinita dagli altri clienti, e ogni tenant in Google Cloud NetApp Volumes ottiene il proprio namespace e VLAN per un isolamento totale dei dati. Dopo che un utente è stato autenticato, il Service Delivery Engine (SDE) può leggere solo i dati di configurazione specifici di quel tenant.

Sicurezza fisica

Con la dovuta pre-approvazione, solo i tecnici in loco e i Field Support Engineer (FSE) con badge NetApp hanno accesso alla gabbia e ai rack per il lavoro fisico. Non è consentita la gestione dell'archiviazione e della rete. Solo queste risorse in loco sono in grado di eseguire attività di manutenzione hardware.

Per i tecnici in loco, viene creato un ticket per la dichiarazione di lavoro (SOW) che include l'ID del rack e la posizione del dispositivo (RU); nel ticket sono inclusi anche tutti gli altri dettagli. Per gli FSE NetApp , è necessario inviare un ticket di visita al sito al COLO; il ticket deve includere i dettagli del visitatore, la data e l'ora per scopi di audit. Il SOW per l'FSE viene comunicato internamente a NetApp.

squadra operativa

Il team operativo per Google Cloud NetApp Volumes è composto da ingegneri di produzione e da un Site Reliability Engineer (SRE) per Google Cloud NetApp Volumes , nonché da tecnici e partner del supporto sul campo NetApp per l'hardware. Tutti i membri del team operativo sono accreditati per lavorare su Google Cloud e per ogni ticket inviato vengono conservati registri dettagliati del lavoro svolto. Inoltre, è in atto un rigoroso processo di controllo e approvazione delle modifiche per garantire che ogni decisione venga esaminata attentamente.

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 backend in Google Cloud NetApp Volumes. Il team SRE gestisce anche le risorse di sistema, come i volumi massimi e gli inode. Agli SRE non è consentito interagire o avere accesso ai dati dei clienti. Gli SRE forniscono anche il coordinamento con le autorizzazioni al reso del materiale (RMA), come le richieste di sostituzione di nuovi dischi o memorie per l'hardware back-end.

Responsabilità del cliente

I clienti di Google Cloud NetApp Volumes gestiscono la gestione di Active Directory e dei ruoli utente della propria organizzazione, nonché le operazioni sui volumi e sui dati. I clienti possono avere ruoli amministrativi e delegare autorizzazioni ad altri utenti finali all'interno dello stesso progetto Google Cloud utilizzando i due ruoli predefiniti forniti NetApp e Google Cloud (Amministratore e Visualizzatore).

L'amministratore può collegare in peering qualsiasi VPC all'interno del progetto del cliente a Google Cloud NetApp Volumes che il cliente ritiene appropriato. È responsabilità del cliente gestire l'accesso al proprio abbonamento al marketplace di Google Cloud e gestire le VPC che hanno accesso al piano dati.

Protezione SRE dannosa

Una possibile preoccupazione è: in che modo Google Cloud NetApp Volumes protegge da scenari in cui è presente un SRE dannoso o quando le credenziali SRE sono state compromesse?

L'accesso all'ambiente di produzione è consentito solo a un numero limitato di persone SRE. I privilegi amministrativi sono ulteriormente limitati a una manciata di amministratori esperti. Tutte le azioni eseguite da chiunque nell'ambiente di produzione Google Cloud NetApp Volumes vengono registrate e qualsiasi anomalia rispetto alla baseline o attività sospette viene rilevata dalla nostra piattaforma di intelligence sulle minacce per la gestione degli eventi e delle informazioni di sicurezza (SIEM). Di conseguenza, è possibile monitorare e mitigare le azioni dannose prima che vengano arrecati troppi danni al backend di Google Cloud NetApp Volumes .

Ciclo di vita del volume

Google Cloud NetApp Volumes 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 quando sono inattivi e l'accesso è limitato ai tenant dell'istanza di Google Cloud NetApp Volumes .

Il ciclo di vita del volume per Google Cloud NetApp Volumes è creazione-aggiornamento-eliminazione. I volumi conservano copie snapshot dei volumi finché non vengono eliminati e solo gli amministratori Google Cloud NetApp Volumes convalidati possono eliminare i volumi in Google Cloud NetApp Volumes. Quando un amministratore richiede l'eliminazione di un volume, è necessario un ulteriore passaggio di immissione del nome del volume per verificare l'eliminazione. Una volta eliminato, un volume non è più disponibile e non può essere recuperato.

Nei casi in cui un contratto Google Cloud NetApp Volumes viene rescisso, NetApp contrassegna i volumi per l'eliminazione dopo un periodo di tempo specifico. Prima della scadenza di tale periodo di tempo, è possibile recuperare i volumi su richiesta del cliente.

Certificazioni

Google Cloud NetApp Volumes per Google Cloud è attualmente certificato secondo gli standard ISO/IEC 27001:2013 e ISO/IEC 27018:2019. Il servizio ha ricevuto di recente anche il rapporto di attestazione SOC2 Tipo I. Per informazioni sull'impegno di NetApp per la sicurezza e la privacy dei dati, vedere "Conformità: 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 la nostra "Addendum Data Processing dei clienti", che include le "Clausole contrattuali standard" fornite dalla Commissione europea. Assumiamo inoltre questi impegni nella nostra Informativa sulla privacy, supportati dai valori fondamentali definiti nel nostro Codice di condotta aziendale.

Ulteriori informazioni e contatti

Per saperne di più sulle informazioni descritte nel presente documento, consultare i seguenti documenti e/o siti web:

- Documentazione di Google Cloud per Google Cloud NetApp Volumes

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Accesso al servizio privato di Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentazione del prodotto 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 contro il 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

Fateci sapere come possiamo migliorare questo rapporto tecnico.

Contattaci all'indirizzo doccomments@netapp.com. Includi RELAZIONE TECNICA 4918 nell'oggetto.

NetApp Disaster Recovery

Protezione dei dati 3-2-1 per VMware con SnapCenter Plug-in e NetApp Backup and Recovery per proteggere i carichi di lavoro VMware

La strategia di backup 3-2-1 è un metodo di protezione dei dati accettato dal settore, che fornisce un approccio completo alla salvaguardia dei dati preziosi. Questa strategia è affidabile e garantisce che, anche se si verificasse un disastro imprevisto, ci sarà comunque una copia dei dati disponibile.

Panoramica

La strategia si compone di tre regole fondamentali:

1. Conserva almeno tre copie dei tuoi dati. In questo modo si garantisce che, anche se una copia viene persa o danneggiata, saranno comunque disponibili almeno due copie su cui fare affidamento.
2. Conservare due copie di backup su supporti o dispositivi di archiviazione diversi. Diversificare i supporti di memorizzazione aiuta a proteggere da guasti specifici del dispositivo o del supporto. Se un dispositivo

viene danneggiato o un tipo di supporto si guasta, l'altra copia di backup non subisce alcun danno.

3. Infine, assicurati che almeno una copia di backup sia fuori sede. L'archiviazione fuori sede funge da misura di sicurezza contro disastri localizzati, come incendi o inondazioni, che potrebbero rendere inutilizzabili le copie in loco.

Questo documento illustra una soluzione di backup 3-2-1 che utilizza SnapCenter Plug-in for VMware vSphere (SCV) per creare backup primari e secondari delle macchine virtuali on-premise e NetApp Backup and Recovery for virtual machines per eseguire il backup di una copia dei dati su cloud storage o StorageGRID.

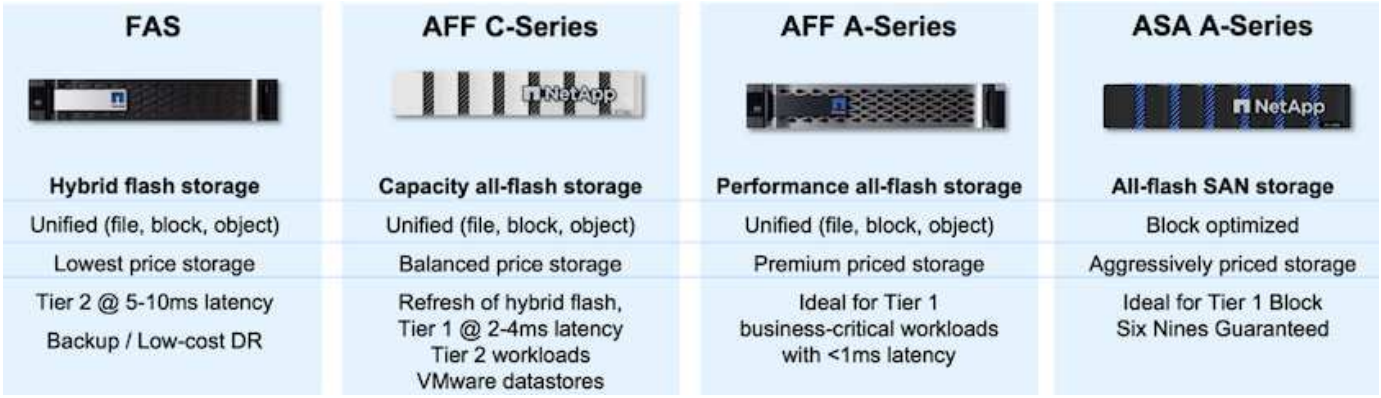
Casi d'uso

Questa soluzione affronta i seguenti casi d'uso:

- Backup e ripristino di macchine virtuali e datastore on-premise mediante il SnapCenter Plug-in for VMware vSphere.
- Backup e ripristino di macchine virtuali e datastore on-premises, ospitati su cluster ONTAP e sottoposti a backup su storage a oggetti utilizzando NetApp Backup and Recovery for virtual machines.

Archiviazione dati NetApp ONTAP

ONTAP è la soluzione di storage leader del settore di NetApp che offre storage unificato indipendentemente dall'accesso tramite protocolli SAN o NAS. La strategia di backup 3-2-1 garantisce la protezione dei dati in sede su più tipi di supporto e NetApp offre piattaforme che spaziano da flash ad alta velocità a supporti più economici.



Per maggiori informazioni su tutte le piattaforme hardware di NetApp, consulta "Archiviazione dati NetApp" .

SnapCenter Plug-in for 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 del backup e del ripristino 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 archiviazione ONTAP secondario. Grazie a questa architettura, le operazioni di ripristino delle macchine virtuali possono essere avviate facilmente dalle posizioni di backup primarie o secondarie.

SCV viene distribuito come appliance virtuale Linux utilizzando un file OVA. Il plug-in ora utilizza un'architettura di plug-in remoto. Il plug-in remoto viene eseguito all'esterno del server vCenter ed è ospitato sull'appliance virtuale SCV.

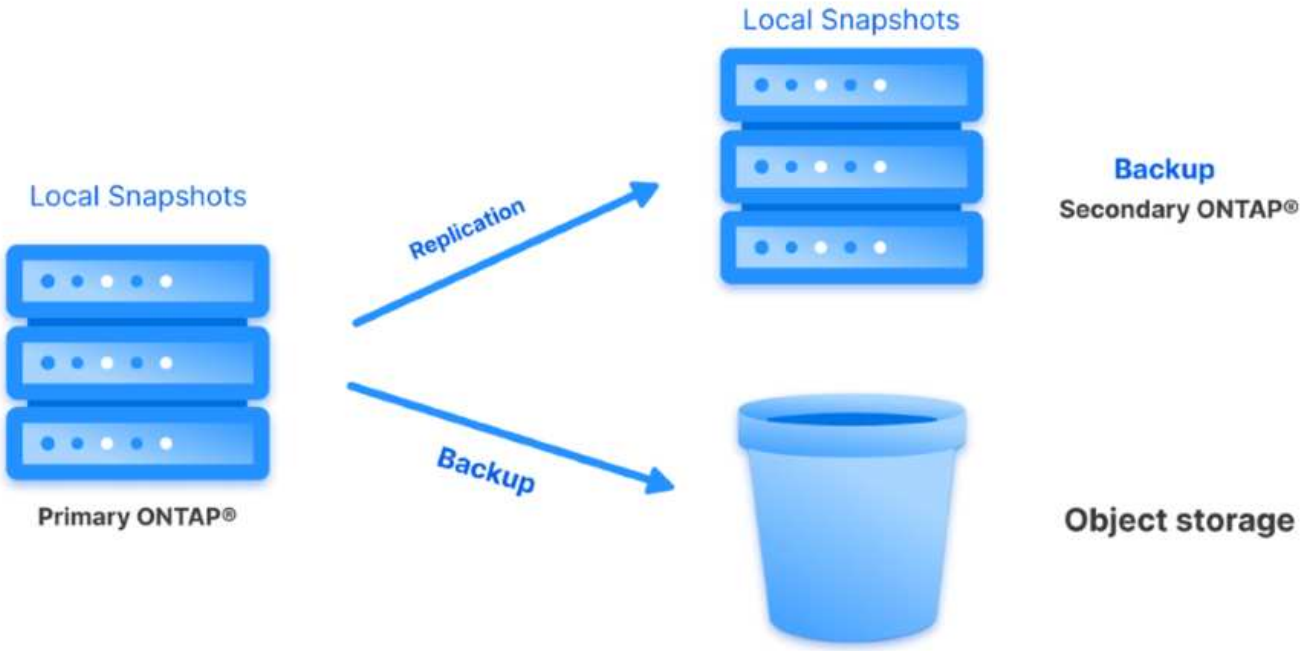
Per informazioni dettagliate su SCV fare riferimento a "Documentazione SnapCenter Plug-in for VMware vSphere" .

NetApp Backup and Recovery per proteggere i workload VMware

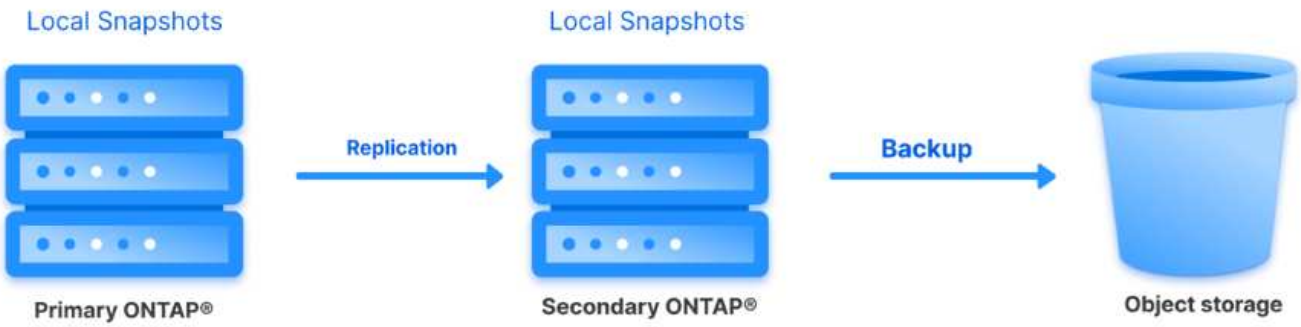
NetApp Backup and Recovery è uno strumento basato sul cloud per la gestione dei dati che fornisce un unico control plane per un'ampia gamma di operazioni di backup e recovery sia negli ambienti on-premises sia in quelli cloud. Parte della suite NetApp Backup and Recovery for VM è una funzionalità che si integra con SnapCenter Plugin for VMware vSphere (on-premises) per estendere una copia dei dati allo storage a oggetti nel cloud. In questo modo viene creata una terza copia offsite dei dati, ricavata dai backup sullo storage primario o secondario. NetApp Backup and Recovery for VMs ti semplifica la configurazione di policy di storage che trasferiscono copie dei tuoi dati da una di queste due posizioni on-premises.

La scelta tra i backup primari e secondari come origine in NetApp Backup and Recovery comporterà l'implementazione di una delle due topologie seguenti:

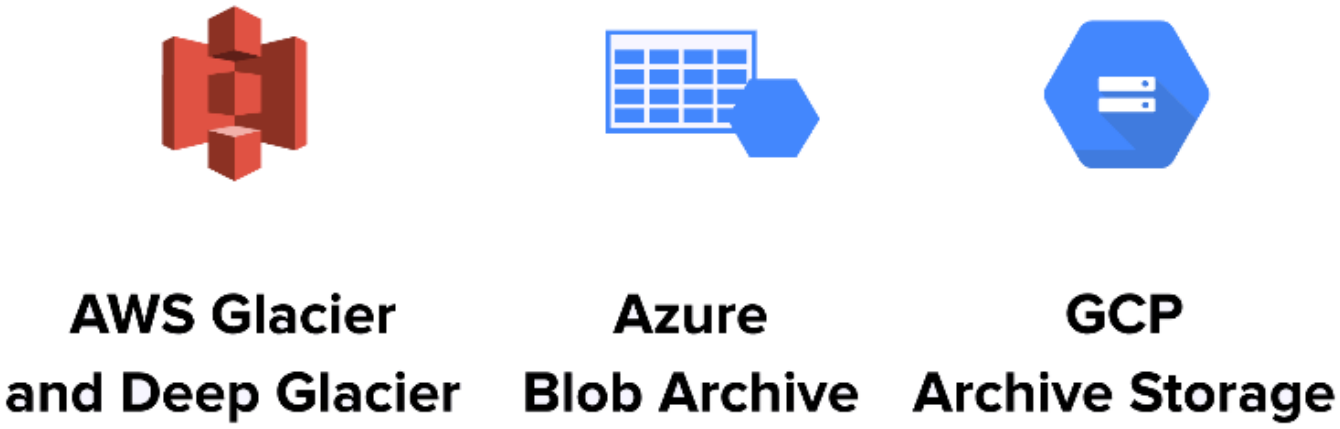
Topologia fan-out – Quando un backup viene avviato dal Plug-in SnapCenter per VMware vSphere, viene immediatamente acquisita una Snapshot locale. SCV avvia quindi un'operazione di SnapMirror che replica la Snapshot più recente nel cluster ONTAP secondario. In NetApp Backup and Recovery, una policy specifica il cluster ONTAP primario come origine per una copia Snapshot dei dati da trasferire nello storage a oggetti del cloud provider che preferisci.



Topologia a cascata – La creazione delle copie di dati primarie e secondarie tramite SCV è identica alla topologia fan-out menzionata sopra. Tuttavia, questa volta in NetApp Backup and Recovery viene creata una policy che specifica che il backup su storage a oggetti avrà origine dal cluster ONTAP secondario.



NetApp Backup and Recovery può creare copie di backup delle Snapshot di ONTAP on-premises in AWS Glacier, Azure Blob e GCP Archive storage.



Inoltre, è possibile utilizzare NetApp StorageGRID come destinazione di backup dell'archiviazione degli oggetti. Per maggiori informazioni su StorageGRID fare riferimento a "Pagina di destinazione StorageGRID" .

▼ **Panoramica sulla distribuzione della soluzione**

Questo elenco fornisce i passaggi high-level necessari per configurare questa soluzione ed eseguire operazioni di backup e ripristino da SCV e NetApp Console:

1. Configurare la relazione SnapMirror tra i cluster ONTAP da utilizzare per le copie dei dati primari e secondari.
2. Configurare il plug-in SnapCenter per VMware vSphere.
   a. Aggiungi sistemi di archiviazione
   b. Creare policy di backup
   c. Creare gruppi di risorse
   d. Eseguire il backup prima dei processi di backup
3. Configura NetApp Backup and Recovery per le macchine virtuali
   a. Aggiungi ambiente di lavoro
   b. Scopri gli apparecchi SCV e vCenter
   c. Creare policy di backup
   d. Attiva i backup

4. Ripristinare le macchine virtuali dallo storage primario e secondario utilizzando SCV.
5. Ripristina le macchine virtuali dallo storage a oggetti usando NetApp Console.

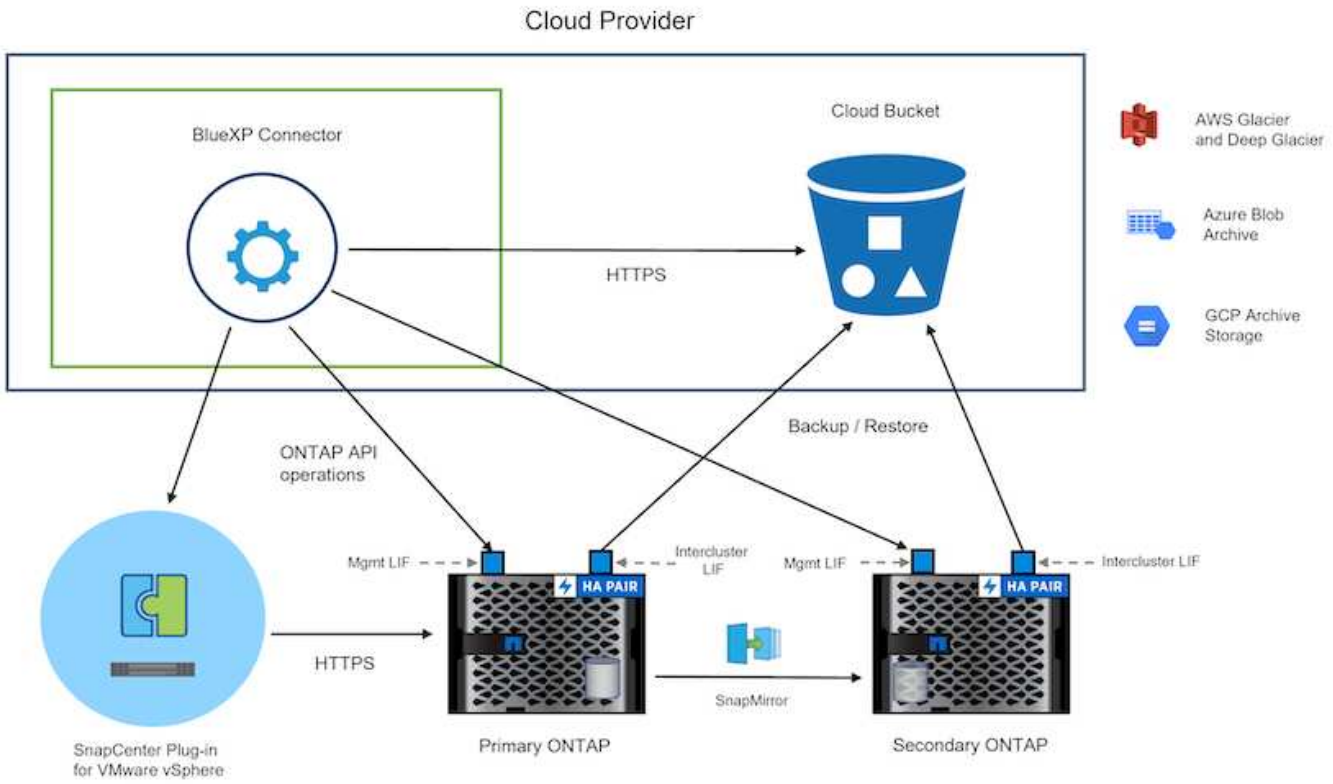
▼ **Prerequisiti**

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

1. Cluster di archiviazione ONTAP con datastore NFS o VMFS connessi a VMware vSphere. Sono supportati sia i datastore NFS che VMFS. Per questa soluzione sono stati utilizzati datastore NFS.
2. Cluster di archiviazione ONTAP secondario con relazioni SnapMirror stabilite per i volumi utilizzati per gli archivi dati NFS.
3. Agente della console installato per il cloud provider usato per i backup dello storage a oggetti.
4. Le macchine virtuali da sottoporre a backup si trovano su datastore NFS residenti nel cluster di storage ONTAP primario.
5. Connettività di rete tra l'agente di Console e le interfacce di gestione del cluster di storage ONTAP on-premises.
6. Connettività di rete tra l'agente Console e la VM dell'appliance SCV on-premises e tra l'agente Console e vCenter.
7. Connettività di rete tra i LIF intercluster ONTAP locali e il servizio di archiviazione degli oggetti.
8. DNS configurato per la gestione SVM sui cluster di storage ONTAP primari e secondari. Per maggiori informazioni fare riferimento a "Configurare il DNS per la risoluzione dei nomi host" .

Architettura di alto livello

Il test/la convalida di questa soluzione sono stati eseguiti in un laboratorio che potrebbe corrispondere o meno all'ambiente di distribuzione finale.



Distribuzione della soluzione

In questa soluzione, forniamo istruzioni dettagliate per distribuire e convalidare una soluzione che utilizza SnapCenter Plug-in for VMware vSphere, insieme a Backup and Recovery, per eseguire il backup e il ripristino di macchine virtuali Windows e Linux all'interno di un cluster VMware vSphere situato in un data center on-premises. Le macchine virtuali in questa configurazione sono archiviate su datastore NFS ospitati da un cluster storage ONTAP A300. Inoltre, un cluster 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.

Esamineremo la creazione di relazioni SnapMirror per le copie secondarie dei nostri backup gestiti da SCV e la configurazione dei processi di backup sia in SCV che in NetApp Console.

Per informazioni dettagliate sul SnapCenter Plug-in for VMware vSphere, fare riferimento a "Documentazione SnapCenter Plug-in for VMware vSphere" .

Per informazioni dettagliate su Backup and Recovery, consulta l' "Documentazione di backup e ripristino".

Stabilire relazioni SnapMirror tra cluster ONTAP

Il SnapCenter Plug-in for VMware vSphere utilizza la tecnologia ONTAP SnapMirror per gestire il trasporto di copie secondarie SnapMirror e/o SnapVault su un cluster ONTAP secondario.

I criteri di backup SCV hanno la possibilità di utilizzare relazioni SnapMirror o SnapVault . La differenza principale è che quando si utilizza l'opzione SnapMirror , la pianificazione di conservazione configurata per i backup nel criterio sarà la stessa nelle posizioni primaria e secondaria. SnapVault è progettato per l'archiviazione e quando si utilizza questa opzione è possibile stabilire una pianificazione di conservazione separata con la relazione SnapMirror per le copie snapshot sul cluster di archiviazione ONTAP secondario.

La configurazione delle relazioni di SnapMirror può essere eseguita in NetApp Console, dove molti dei

passaggi sono automatizzati, oppure utilizzando System Manager e ONTAP CLI. Tutti questi metodi sono descritti di seguito.

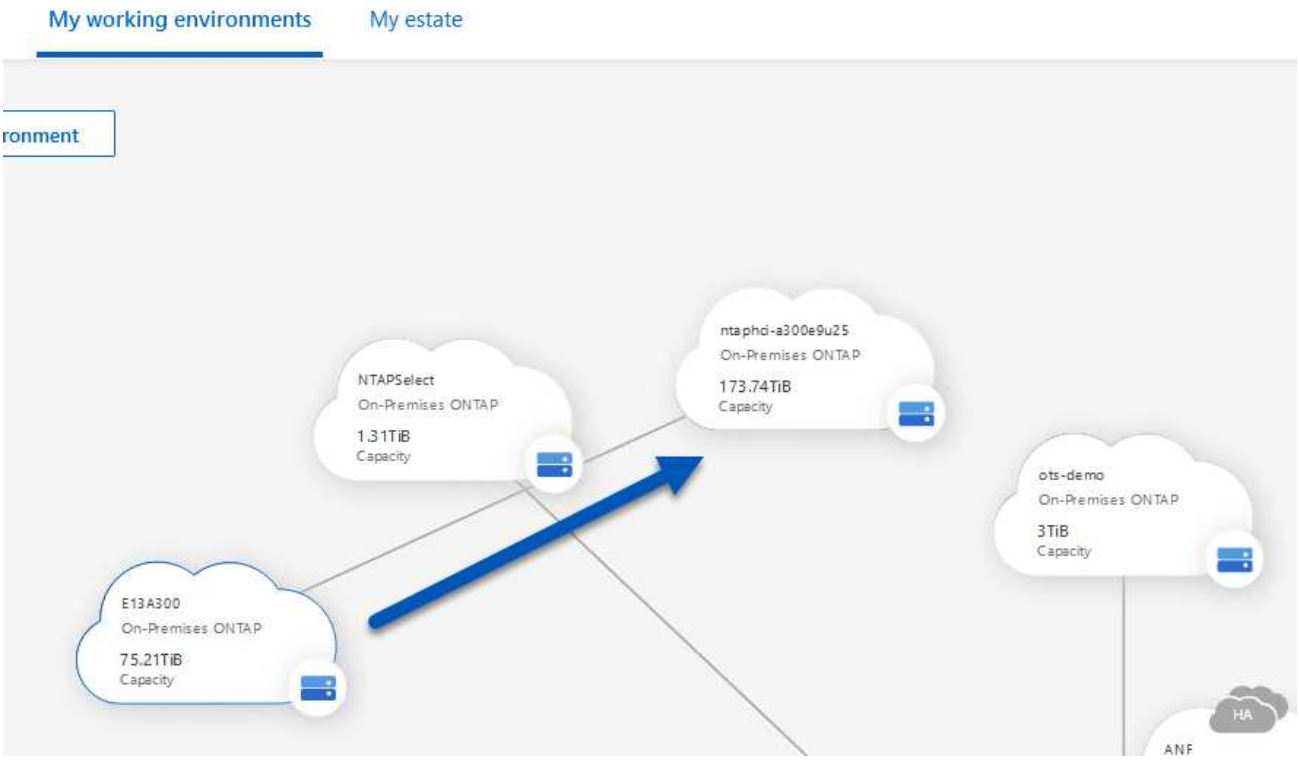
Stabilisci relazioni di SnapMirror con NetApp Console

Dalla NetApp Console devi completare i seguenti passaggi:

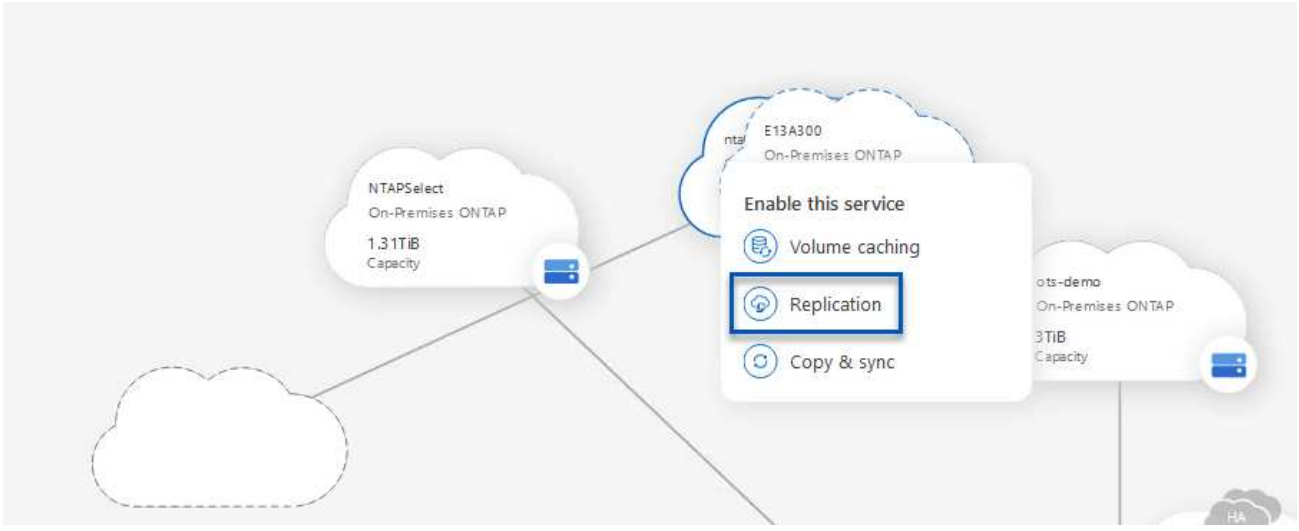
▼ **Configurazione della replica per sistemi di archiviazione ONTAP primari e secondari**

Inizia accedendo alla NetApp Console e vai a Sistemi.

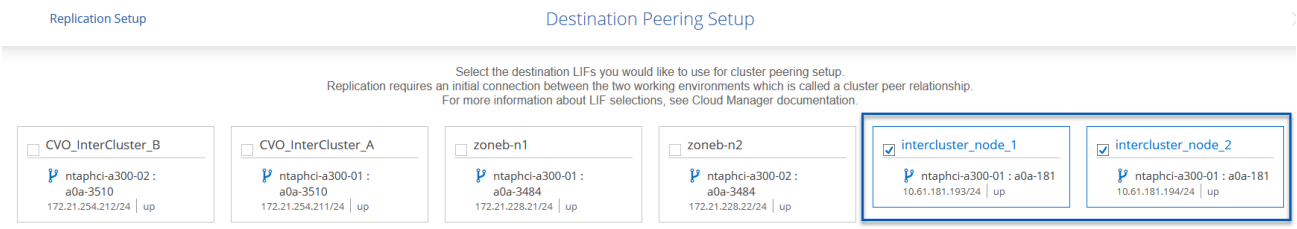
1. Trascinare e rilasciare il sistema di archiviazione ONTAP di origine (primario) sul sistema di archiviazione ONTAP di destinazione (secondario).



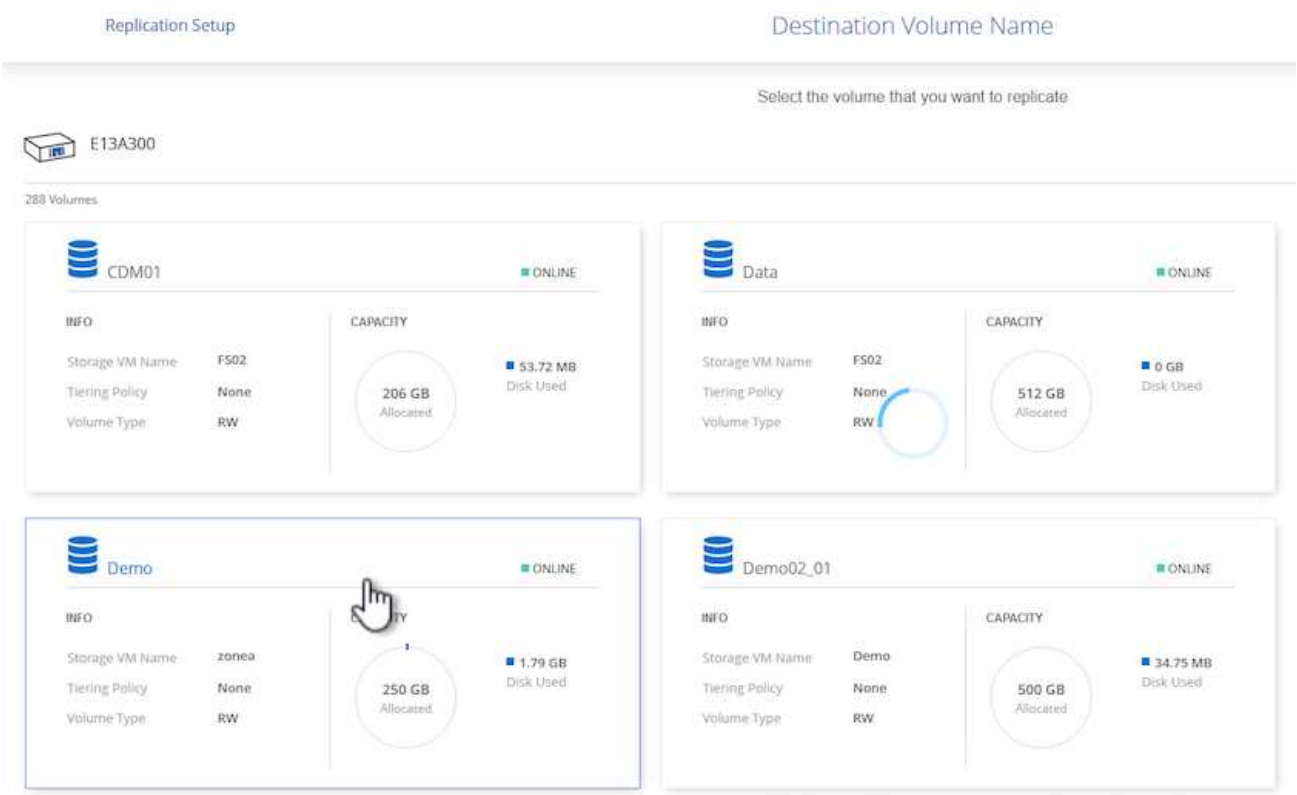
2. Dal menu che appare seleziona **Replicazione**.



3. Nella pagina **Configurazione peering di destinazione** selezionare i LIF intercluster di destinazione da utilizzare per la connessione tra i sistemi di storage.

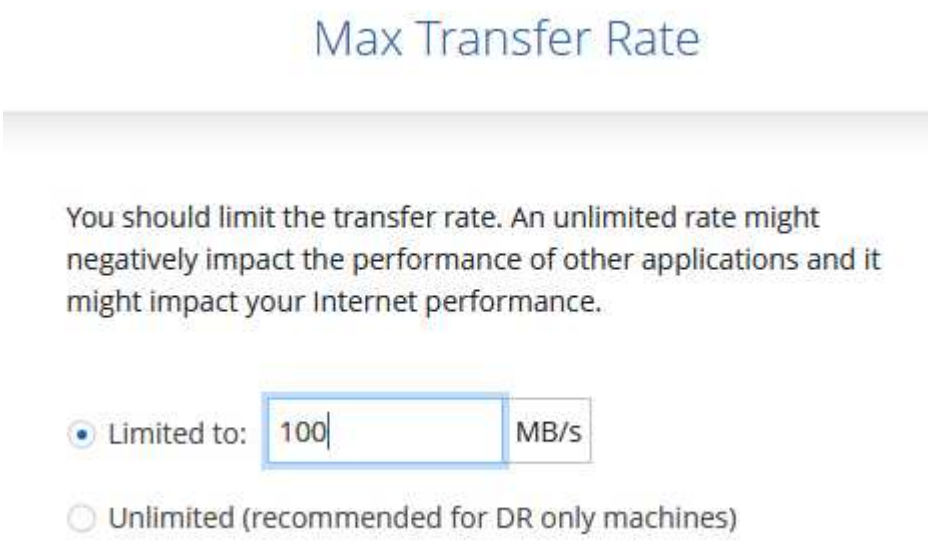


4. Nella pagina **Nome volume di destinazione**, seleziona prima il volume di origine, quindi compila il nome del volume di destinazione e seleziona l'SVM di destinazione e l'aggregato. Fare clic su **Avanti** per continuare.

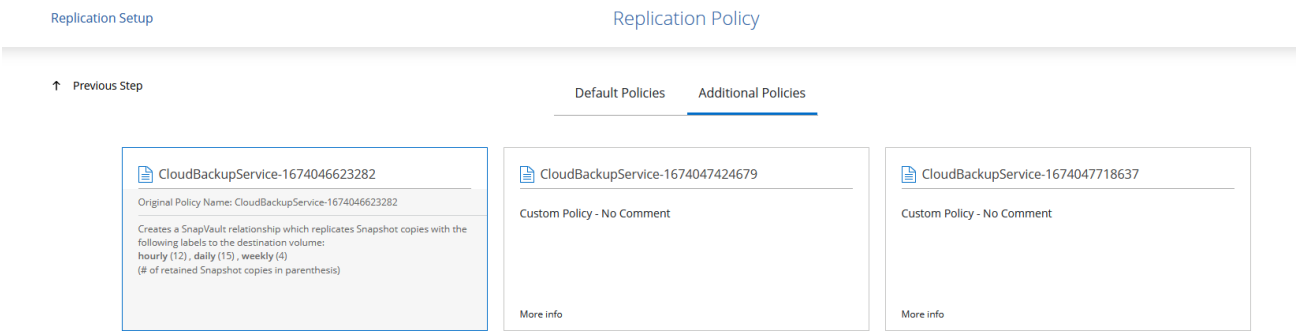




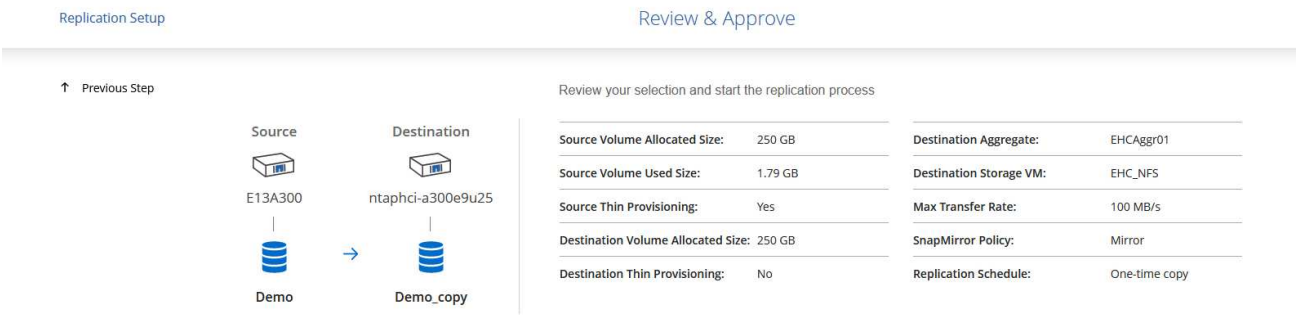
5. Selezionare la velocità di trasferimento massima a cui deve avvenire la replica.



6. Selezionare il criterio che determinerà la pianificazione della conservazione per i backup secondari. Questa policy può essere creata in anticipo (vedere la procedura manuale riportata di seguito nel passaggio **Creare una policy di conservazione degli snapshot**) oppure può essere modificata in un secondo momento, se lo si desidera.



7. Infine, rivedere tutte le informazioni e fare clic sul pulsante **Vai** per avviare il processo di configurazione della replica.



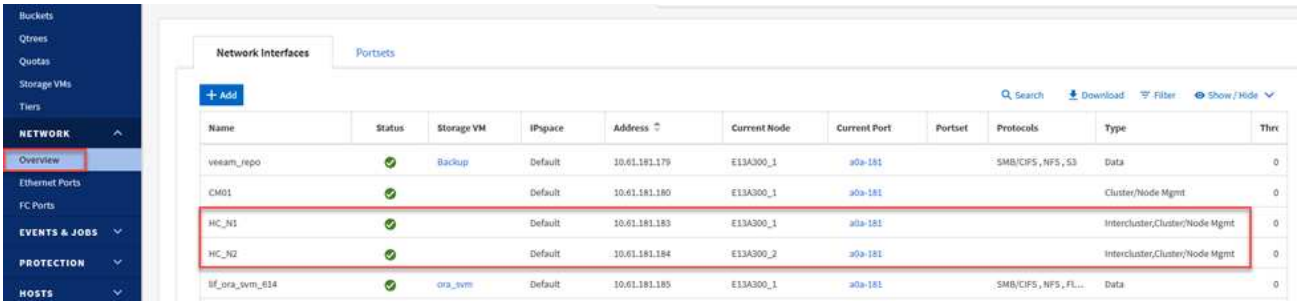
Stabilire relazioni SnapMirror con System Manager e ONTAP CLI

Tutti i passaggi necessari per stabilire relazioni SnapMirror possono essere eseguiti con System Manager o ONTAP CLI. La sezione seguente fornisce informazioni dettagliate per entrambi i metodi:

▼ Registra le interfacce logiche Intercluster di origine e destinazione

Per i cluster ONTAP di origine e di destinazione, è possibile recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

1. In ONTAP System Manager, vai alla pagina Panoramica di rete e recupera gli indirizzi IP di tipo: Intercluster configurati per comunicare con l'AWS VPC in cui è installato FSx.



2. Per recuperare gli indirizzi IP Intercluster tramite la CLI, eseguire il seguente comando:

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

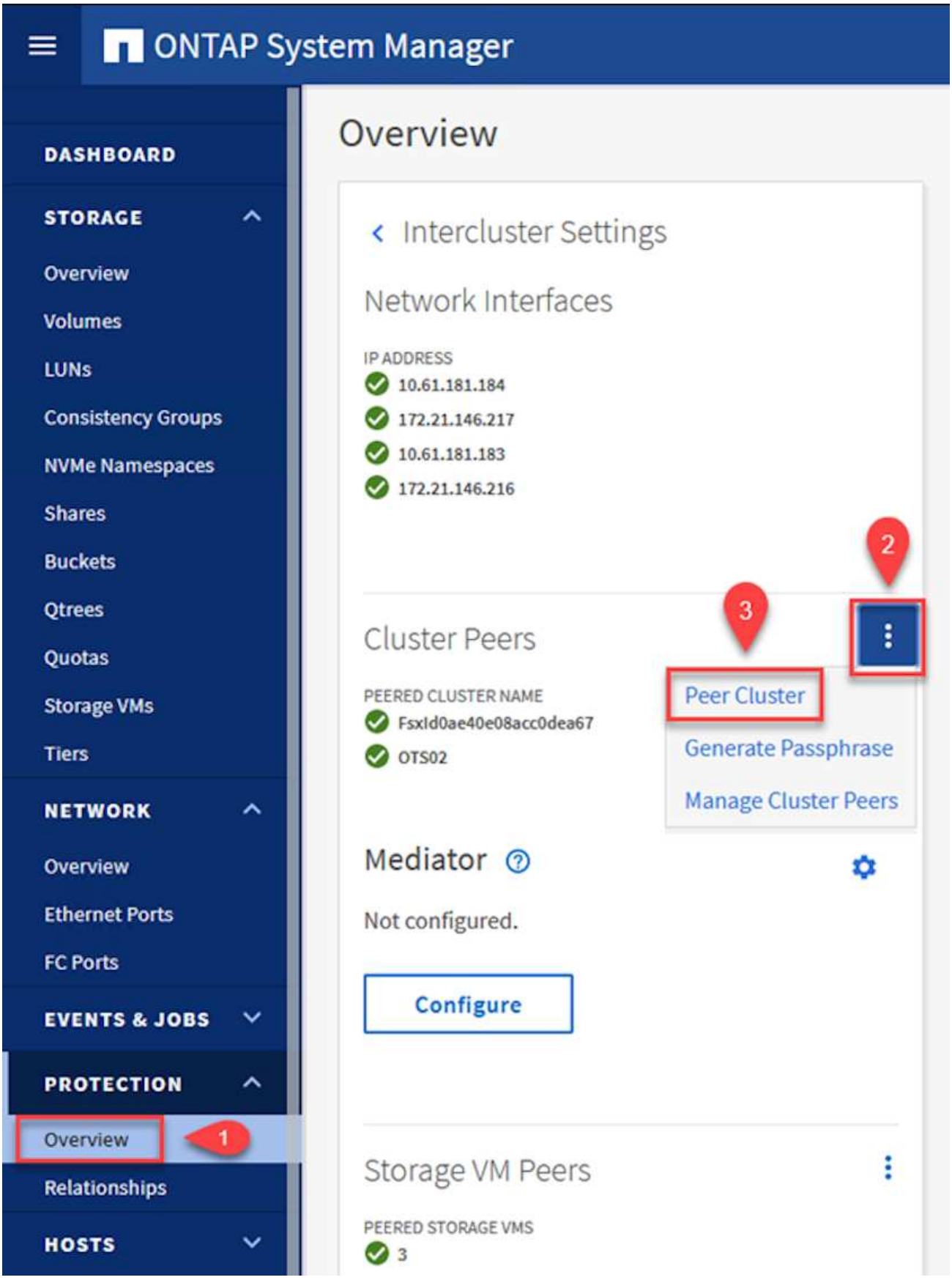
▼ Stabilire il peering dei cluster tra i cluster ONTAP

Per stabilire il peering tra cluster ONTAP , è necessario che una passphrase univoca immessa nel cluster ONTAP di avvio venga confermata nell'altro cluster peer.

1. Impostare il peering sul cluster ONTAP di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca che verrà utilizzata in seguito sul cluster di origine per finalizzare 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 ONTAP System Manager o la CLI. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Cluster.



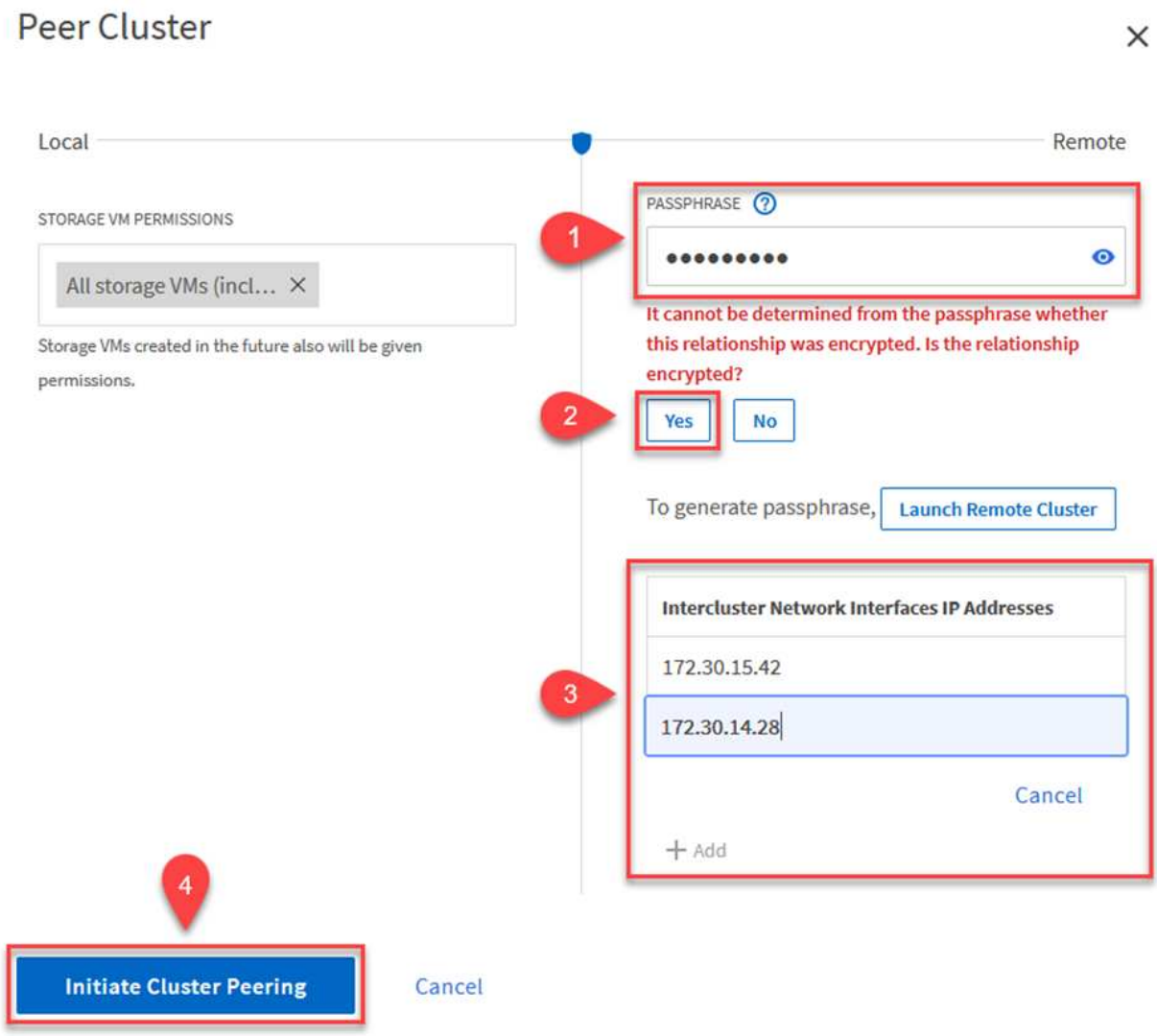
3. Nella finestra di dialogo Peer Cluster, compilare le informazioni richieste:
   a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer sul cluster ONTAP di

destinazione.

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

c. Immettere l'indirizzo/gli indirizzi IP LIF intercluster del cluster ONTAP di destinazione.

d. Fare clic su Avvia peering cluster per finalizzare il processo.



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

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

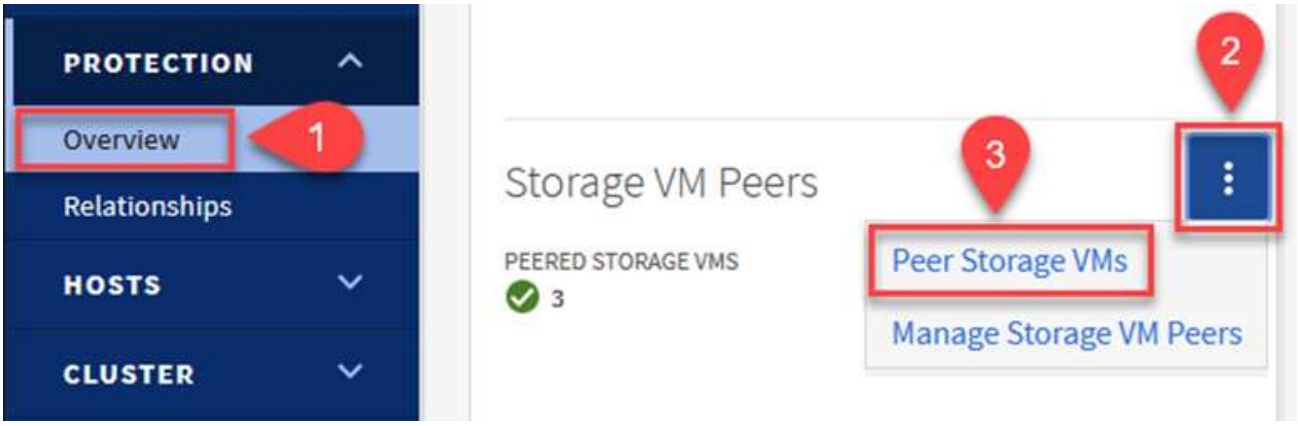
▼ **Stabilire una relazione di peering SVM**

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

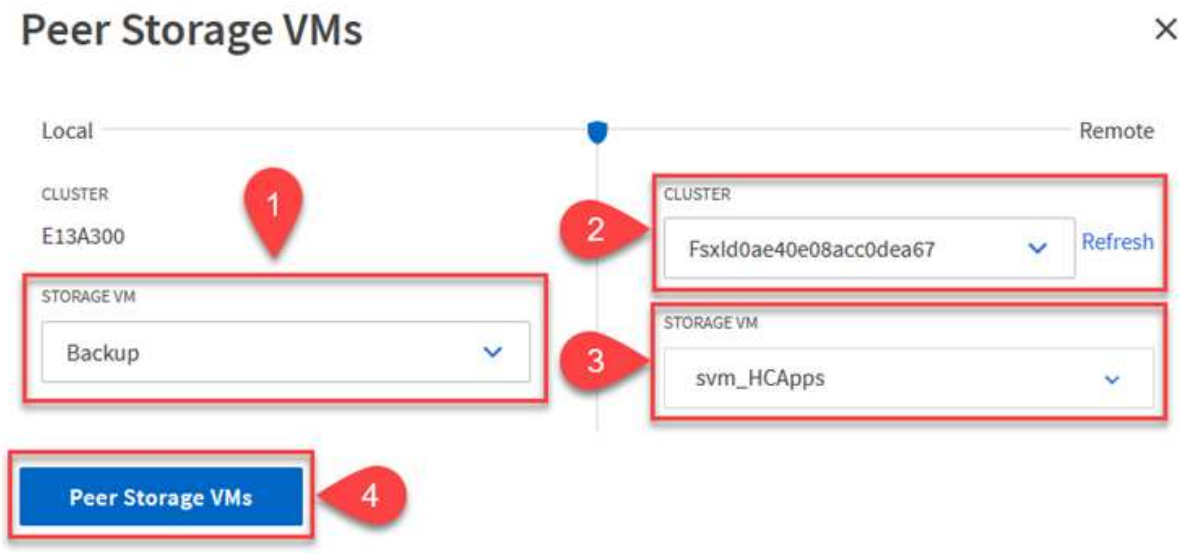
1. Dal cluster ONTAP di destinazione, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

```
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 ONTAP System Manager o con la CLI.
3. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Storage VM in Storage VM Peer.



4. Nella finestra di dialogo della VM di archiviazione peer, compilare i campi obbligatori:
   - La VM di archiviazione di origine
   - Il cluster di destinazione
   - La VM di archiviazione di destinazione



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

▼ **Creare un criterio di conservazione degli snapshot**

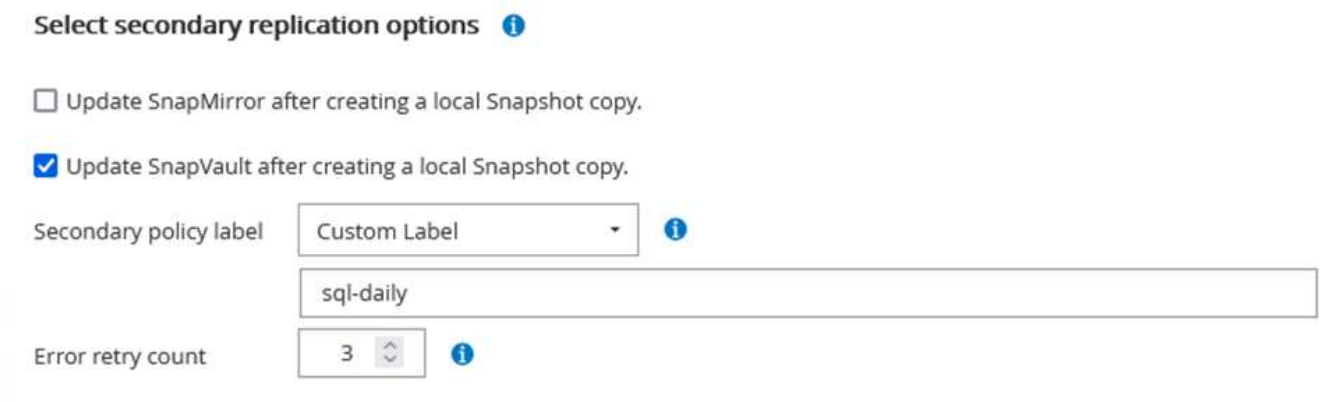
SnapCenter gestisce le pianificazioni di conservazione per i backup presenti come copie snapshot sul sistema di archiviazione primario. Ciò viene stabilito durante la creazione di una policy in SnapCenter. SnapCenter non gestisce i criteri di conservazione per i backup conservati su sistemi di archiviazione

secondari. Queste policy vengono gestite separatamente tramite una policy SnapMirror creata sul cluster FSx secondario e associata 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 .

> Nell'archiviazione secondaria, queste etichette vengono abbinate alle regole dei criteri associati al volume di destinazione allo scopo di imporre la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutti gli snapshot generati come parte di un criterio utilizzato per i backup giornalieri del database SQL Server e dei volumi di registro.



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

Per prima cosa devi creare un criterio SnapMirror con regole che stabiliscano il numero di copie snapshot da conservare.

1. Creare la policy SnapMirror sul cluster FSx.

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

2. Aggiungere regole alla policy con etichette SnapMirror che corrispondono alle etichette della policy secondaria specificate nelle policy SnapCenter .

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

   Lo script seguente fornisce un esempio di regola che potrebbe essere aggiunta a una policy:

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

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

▼ **Crea volumi di destinazione**

Per creare un volume di destinazione su ONTAP che sarà il destinatario delle copie snapshot dai nostri volumi di origine, eseguire 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 SnapMirror tra i volumi di origine e di destinazione**

Per creare una relazione SnapMirror tra un volume di origine e uno di destinazione, eseguire il seguente comando sul cluster ONTAP di destinazione:

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

▼ **Inizializza le relazioni SnapMirror**

Inizializza 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, eseguire il seguente comando sul cluster ONTAP di destinazione:

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

Configurare il SnapCenter Plug-in for VMware vSphere

Una volta installato, è possibile accedere al SnapCenter Plug-in for VMware vSphere dall'interfaccia di gestione di vCenter Server Appliance. SCV gestirà i backup per i datastore NFS montati sugli host ESXi e che contengono le VM Windows e Linux.

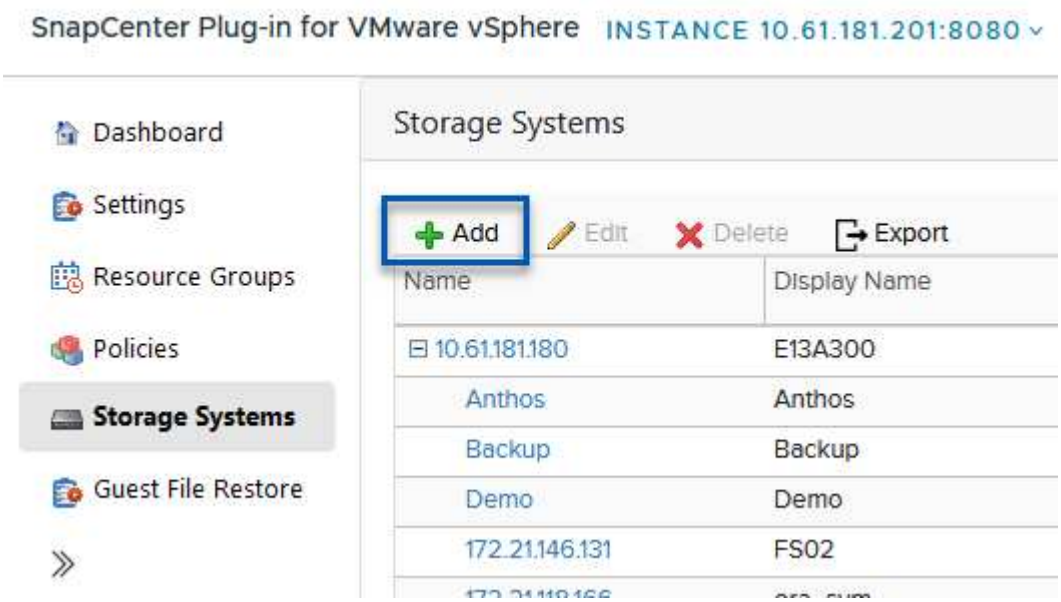
Rivedere il "Flusso di lavoro sulla protezione dei dati" sezione della documentazione SCV per maggiori informazioni sui passaggi necessari per configurare i backup.

Per configurare i backup delle macchine virtuali e degli archivi dati, è necessario completare i seguenti passaggi dall'interfaccia del plug-in.

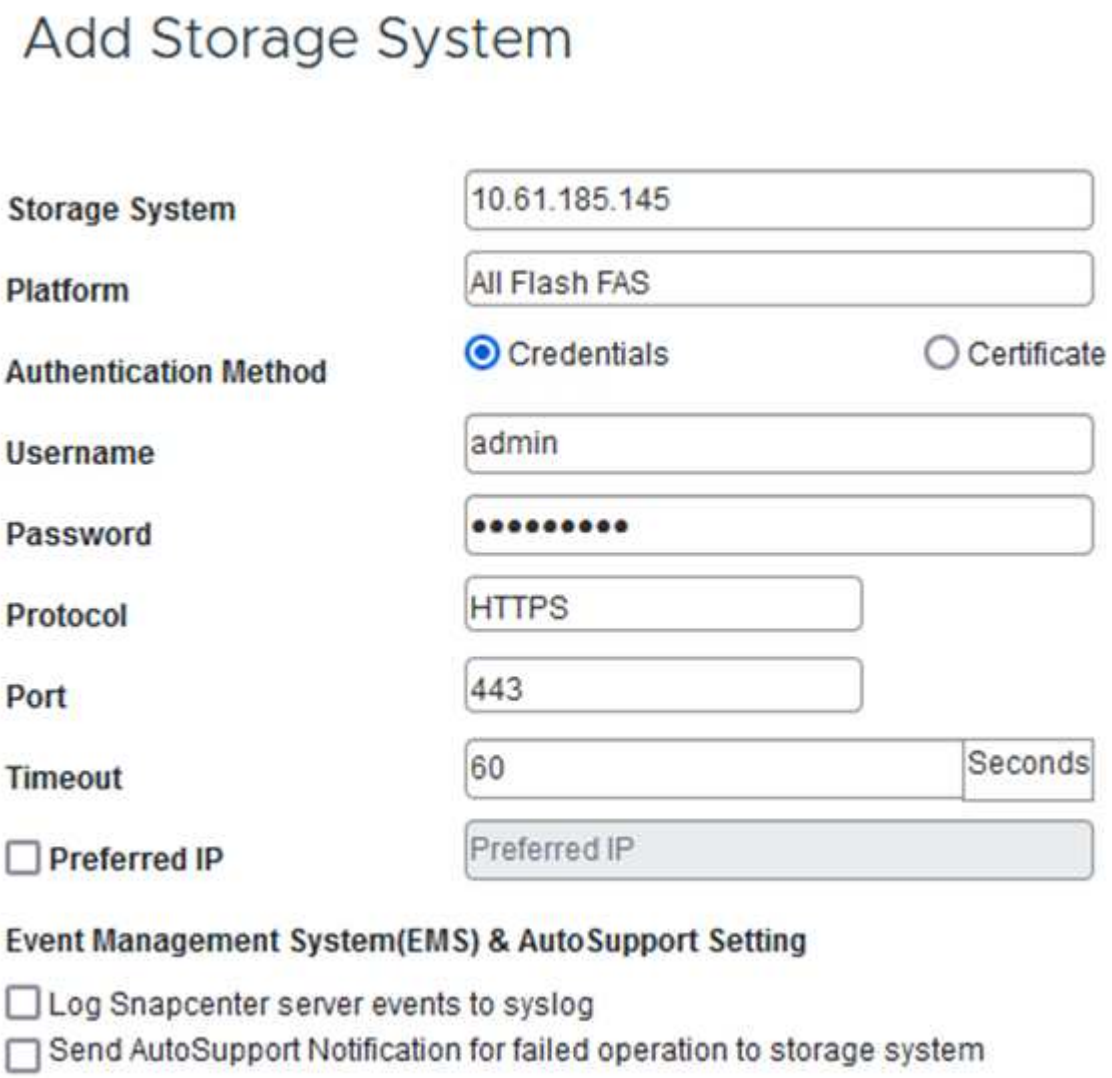
▼ **Sistemi di archiviazione Discovery ONTAP**

Scopri i cluster di archiviazione ONTAP da utilizzare per i backup primari e secondari.

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Sistemi di storage** nel menu a sinistra e clicca sul pulsante **Aggiungi**.



2. Compila le credenziali e il tipo di piattaforma per il sistema di archiviazione ONTAP primario e fai clic su **Aggiungi**.



3. Ripetere questa procedura per il sistema di archiviazione ONTAP secondario.

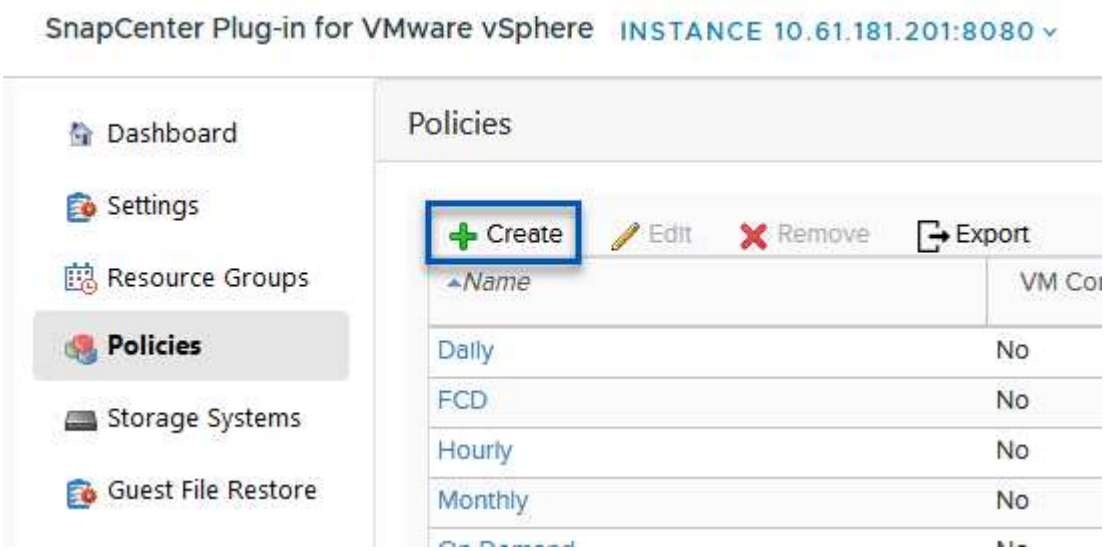
▼ **Creare policy di backup SCV**

Le policy specificano il periodo di conservazione, la frequenza e le opzioni di replica per i backup gestiti da SCV.

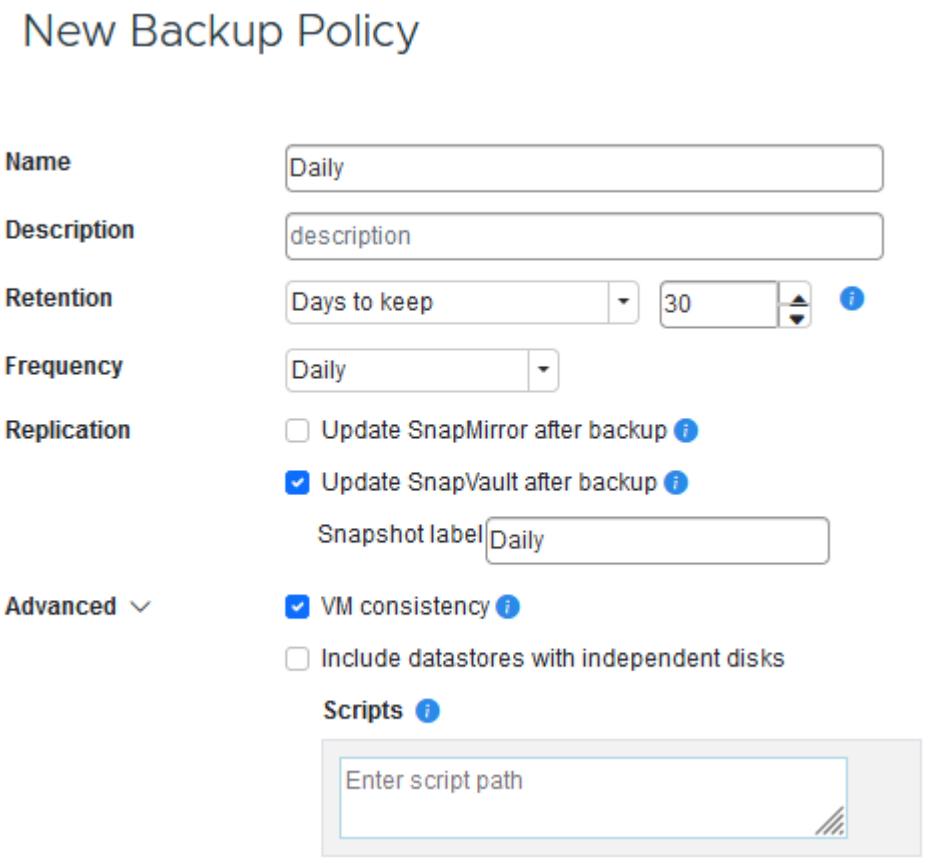
Rivedere il "Creare policy di backup per VM e datastore" sezione della documentazione per maggiori informazioni.

Per creare criteri di backup, completare i seguenti passaggi:

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Criteri** nel menu a sinistra e clicca sul pulsante **Crea**.



2. Specificare un nome per la policy, il periodo di conservazione, le opzioni di frequenza e replica e l'etichetta dello snapshot.



Quando si crea un criterio nel plug-in SnapCenter , verranno visualizzate le opzioni per SnapMirror e SnapVault. Se si sceglie SnapMirror, la pianificazione di conservazione specificata nel criterio sarà la stessa sia per gli snapshot primari che per quelli secondari. Se si sceglie SnapVault, la pianificazione della conservazione per lo snapshot secondario sarà basata su una pianificazione separata implementata con la relazione SnapMirror . Questa funzionalità è utile quando si desiderano periodi di conservazione più lunghi per i backup secondari.

Le etichette Snapshot sono utili perché possono essere usate per applicare policy con uno specifico periodo di conservazione per le copie SnapVault replicate nel cluster ONTAP secondario. Quando SCV viene usato con NetApp Data Services, il campo dell'etichetta Snapshot deve essere vuoto oppure corrispondere all'etichetta specificata nella policy di backup.

3. Ripetere la procedura per ogni polizza richiesta. Ad esempio, criteri separati per backup giornalieri, settimanali e mensili.

▼ **Creare gruppi di risorse**

I gruppi di risorse contengono i datastore e le macchine virtuali da includere in un processo di backup, insieme ai criteri associati e alla pianificazione del backup.

Rivedere il "Creare gruppi di risorse" sezione della documentazione per maggiori informazioni.

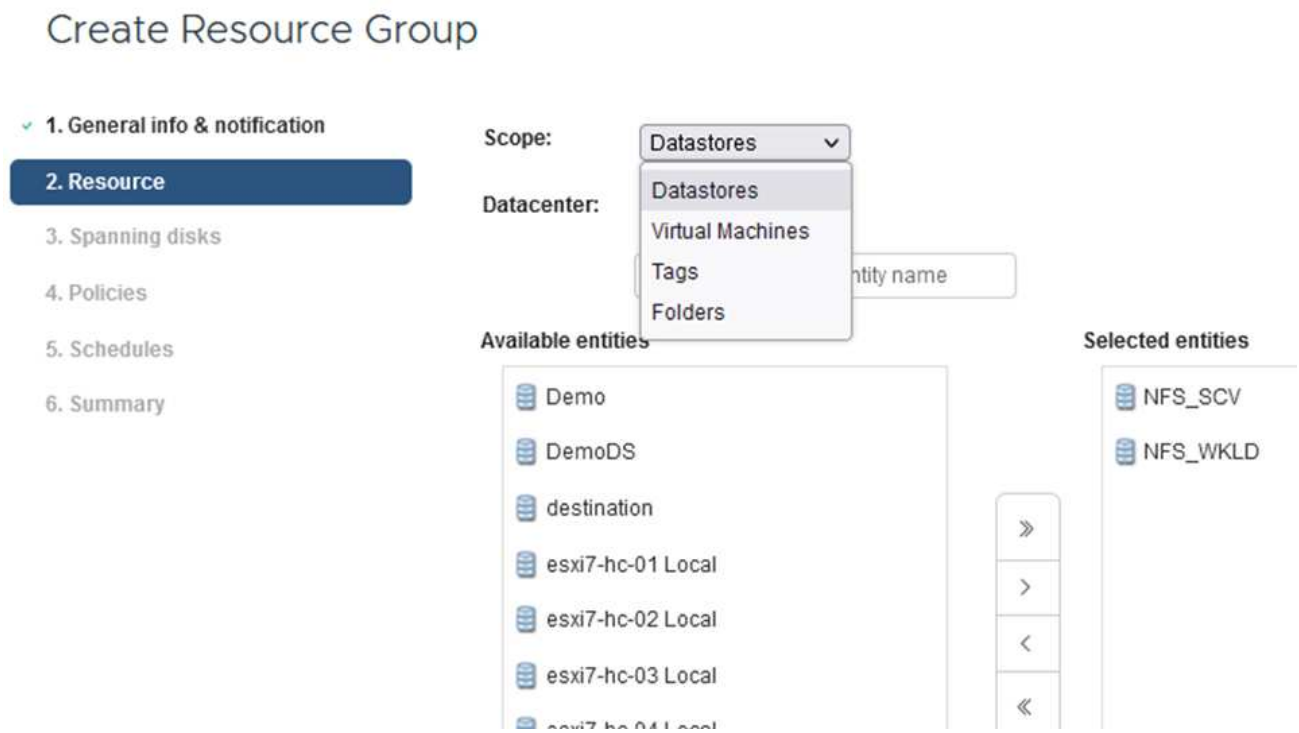
Per creare gruppi di risorse, completare i seguenti passaggi.

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Gruppi di risorse** nel menu a sinistra e clicca sul

pulsante **Crea**.

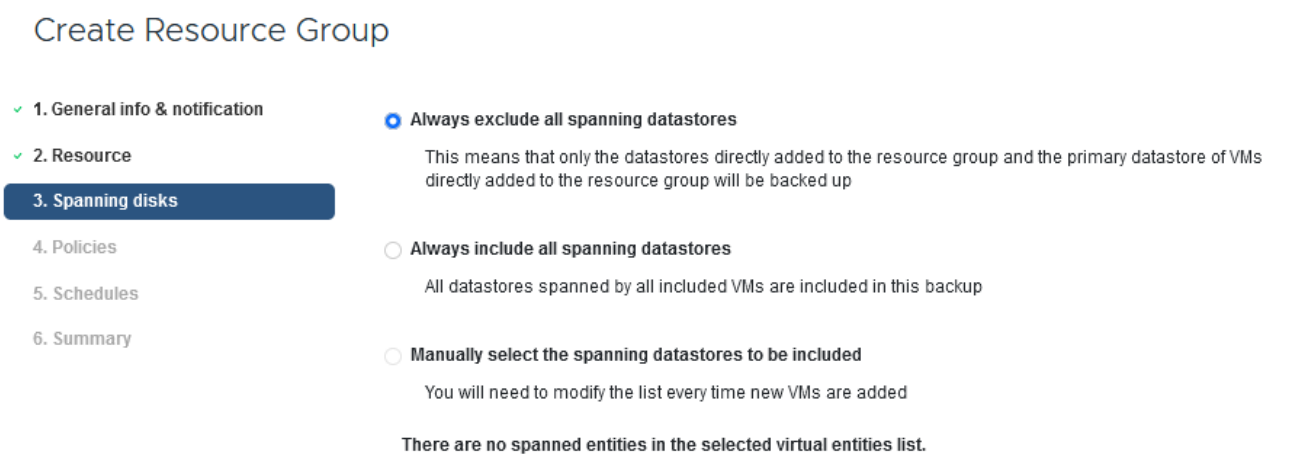


2. Nella procedura guidata Crea gruppo di risorse, immettere un nome e una descrizione per il gruppo, nonché le informazioni necessarie per ricevere le notifiche. Clicca su **Avanti**
3. Nella pagina successiva selezionare i datastore e le macchine virtuali che si desidera includere nel processo di backup, quindi fare clic su **Avanti**.



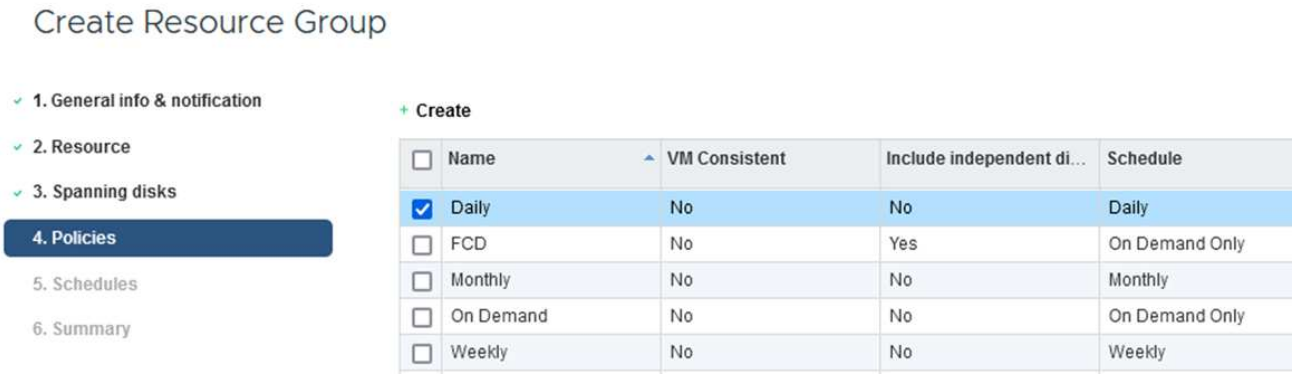
È possibile selezionare VM specifiche o interi datastore. Indipendentemente dalla scelta effettuata, viene eseguito il backup dell'intero volume (e del datastore), poiché il backup è il risultato dell'acquisizione di uno snapshot del volume sottostante. Nella maggior parte dei casi è più semplice scegliere 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. Selezionare le opzioni per l'estensione degli archivi dati per le VM con VMDK che risiedono su più archivi dati, quindi fare clic su **Avanti**.



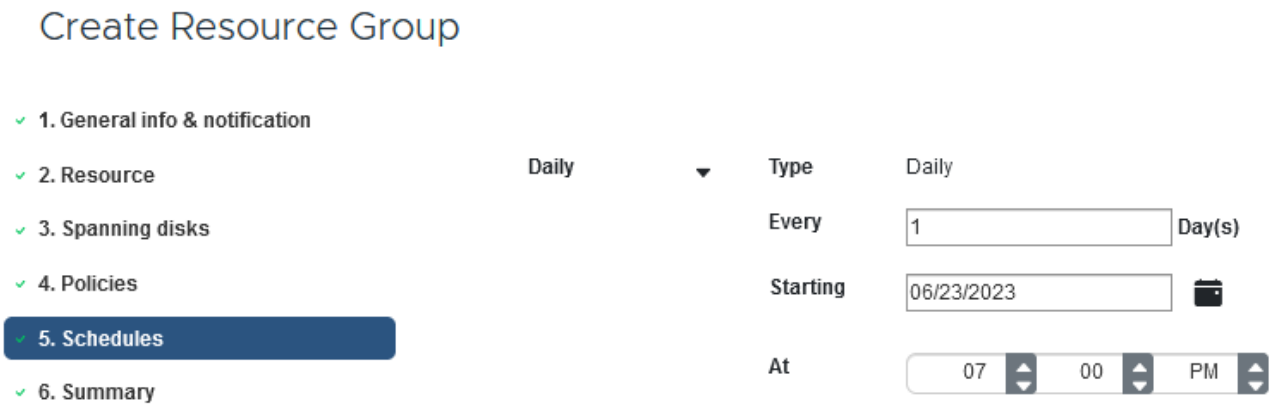
La funzionalità di backup e ripristino per la protezione dei carichi di lavoro VMware attualmente non supporta il backup di macchine virtuali con file VMDK che si estendono su più datastore.

5. Nella pagina successiva seleziona i criteri che saranno associati al gruppo di risorse e fai clic su **Avanti**.



Quando esegui il backup di Snapshot gestite da SCV nello storage a oggetti usando Backup and Recovery, a ciascun gruppo di risorse può essere associata una sola policy.

6. Selezionare una pianificazione che determinerà gli orari in cui verranno eseguiti i backup. Fare clic su **Avanti**.

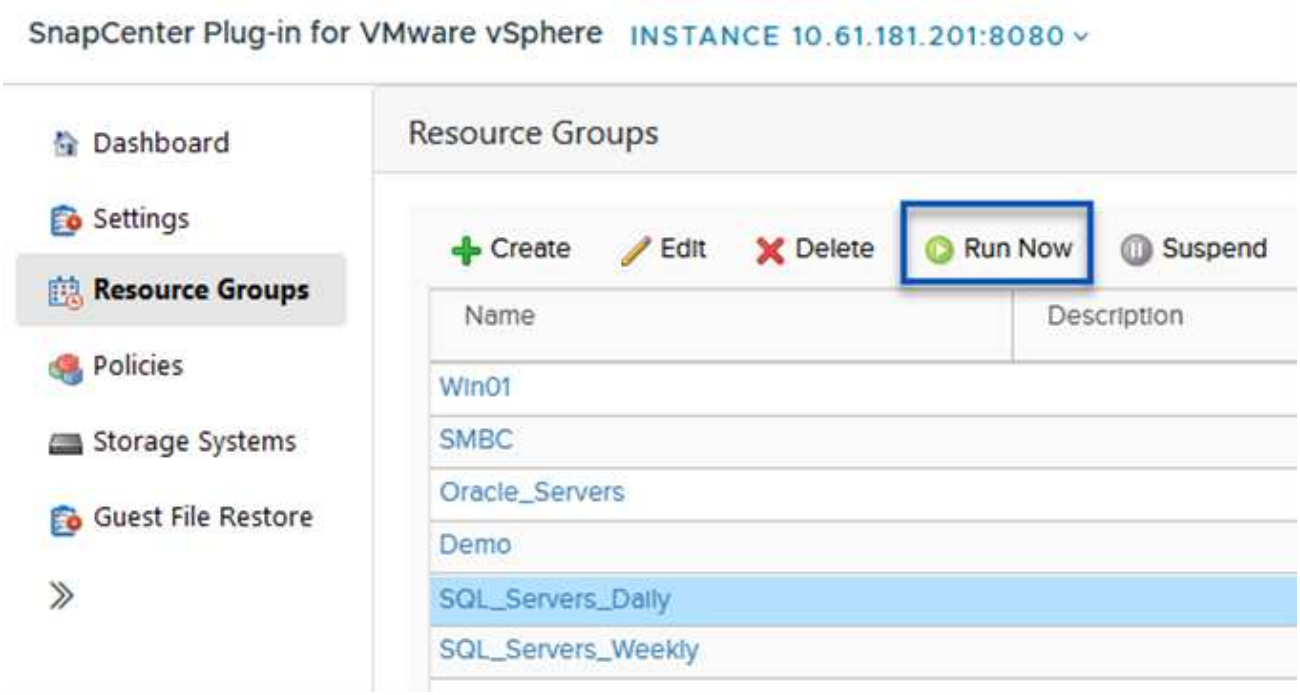


7. Infine, rivedere la pagina di riepilogo e quindi fare clic su **Fine** per completare la creazione del gruppo di risorse.

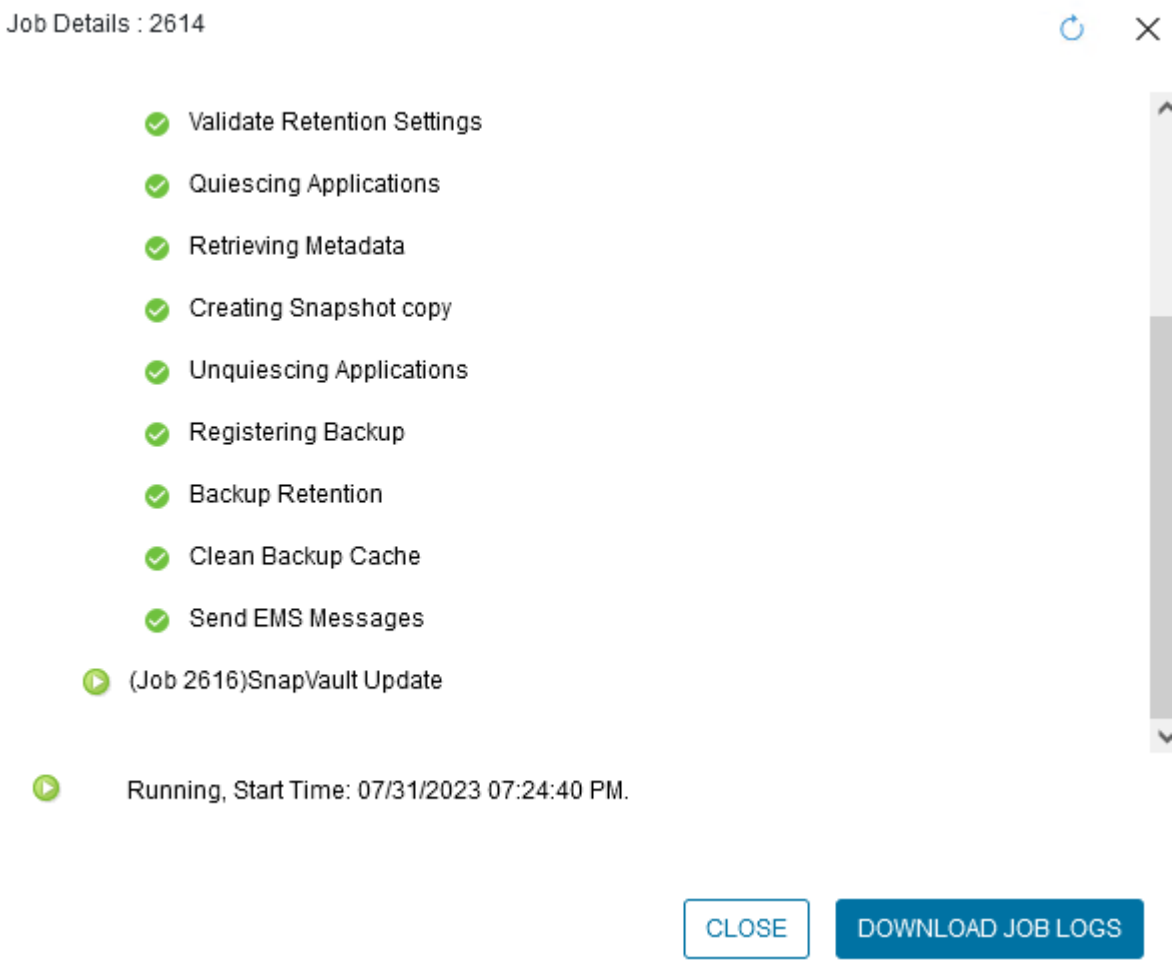
▼ **Eseguire un processo di backup**

In quest'ultimo passaggio, esegui un job di backup e monitorane l'avanzamento. Almeno un job di backup deve essere completato correttamente in SCV prima che le risorse possano essere rilevate da NetApp Console.

1. Nel SnapCenter Plug-in for 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, vai su **Dashboard** nel menu a sinistra. In **Attività recenti del lavoro** fare clic sul numero ID del lavoro per monitorare l'avanzamento del lavoro.



Configura i backup nello storage a oggetti in NetApp Console

Affinché NetApp Console possa gestire efficacemente l'infrastruttura dati, è necessaria la preventiva installazione di un agente Console. L'agente Console esegue le azioni necessarie per individuare le risorse e gestire le operazioni sui dati.

Per ulteriori informazioni sull'agente Console, consulta "Scopri di più sugli agenti di Console" nella documentazione di NetApp Console.

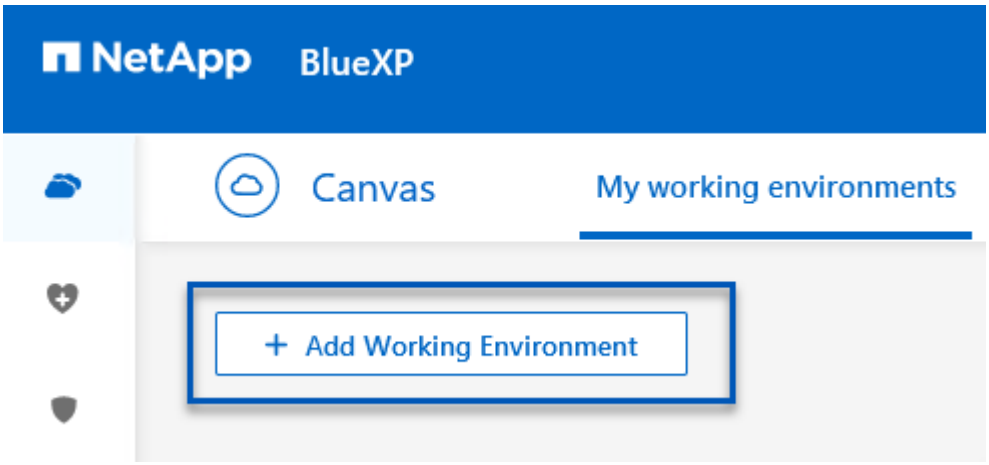
Una volta installato l'agente per il cloud provider utilizzato, dai sistemi sarà possibile visualizzare una rappresentazione grafica dello storage a oggetti.

Per configurare Backup and Recovery per eseguire il backup dei dati gestiti da SCV on-premises, completa i seguenti passaggi:

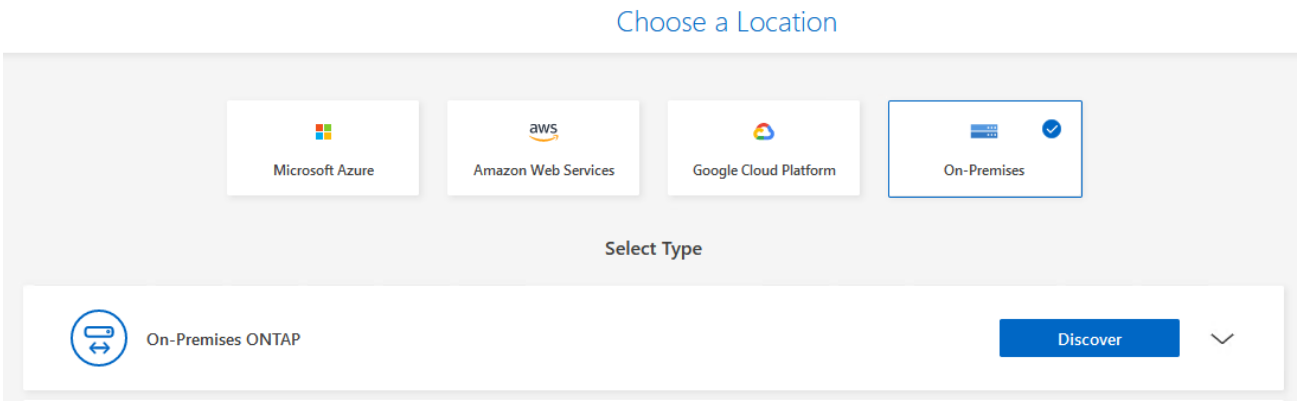
▼ **Aggiungi il sistema storage ONTAP a Systems**

Il primo passo consiste nell'aggiungere i sistemi storage ONTAP on-premises a NetApp Console.

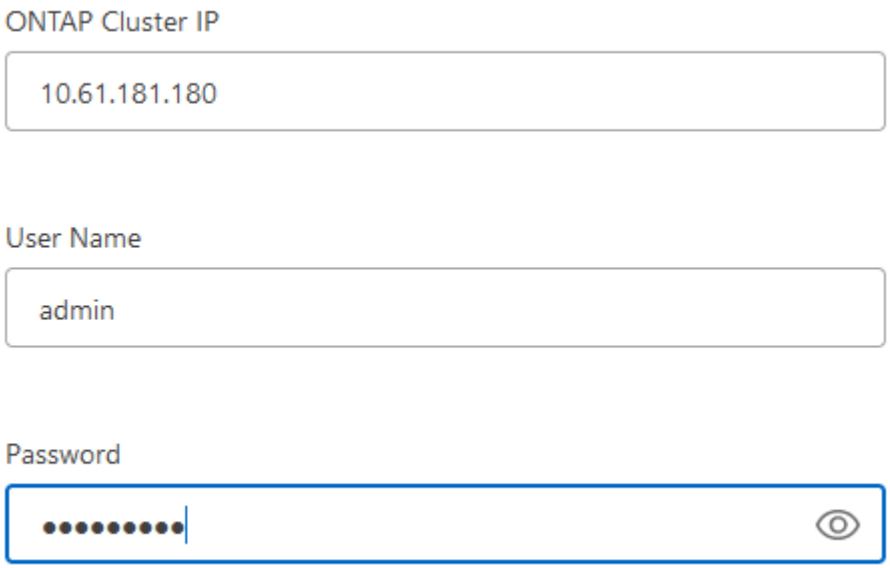
1. Dalla sezione Sistemi, fai clic su **+ Aggiungi** per iniziare.



2. Seleziona **In sede** tra le posizioni disponibili e poi clicca sul pulsante **Scopri**.



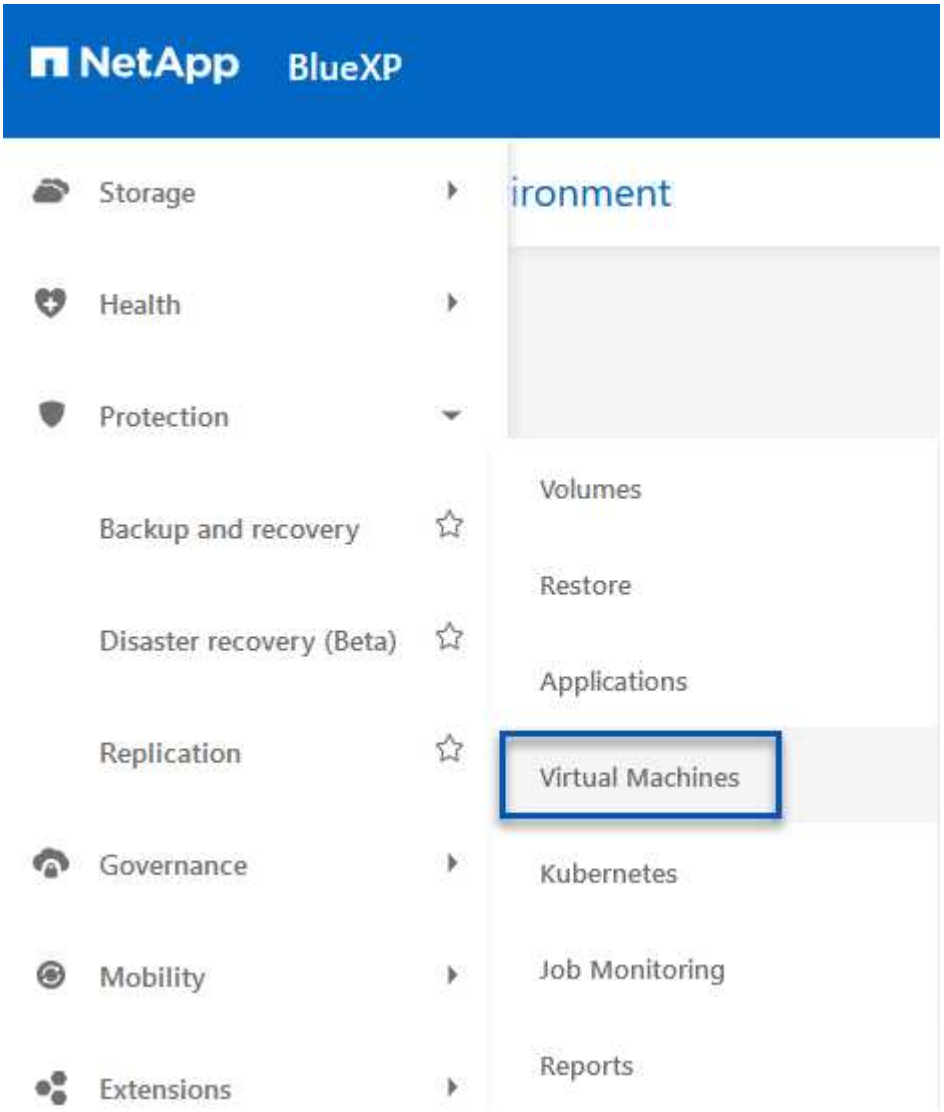
3. Compila le credenziali per il sistema di archiviazione ONTAP e clicca sul pulsante **Scopri** per aggiungere l'ambiente di lavoro.



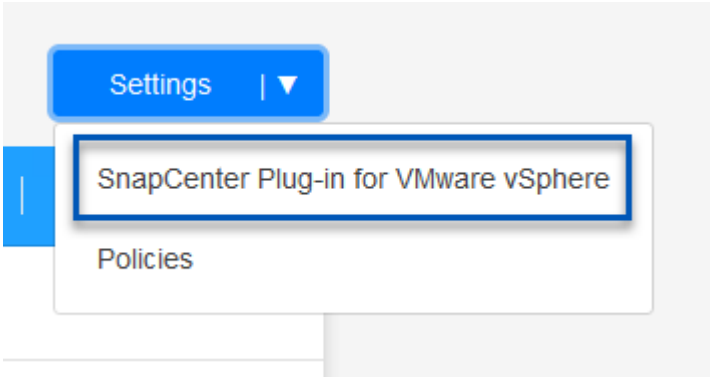
▼ Scopri l'appliance SCV on-premise e vCenter

Per scoprire le risorse del datastore locale e della macchina virtuale, aggiungere le informazioni per il broker dati SCV e le credenziali per l'appliance di gestione vCenter.

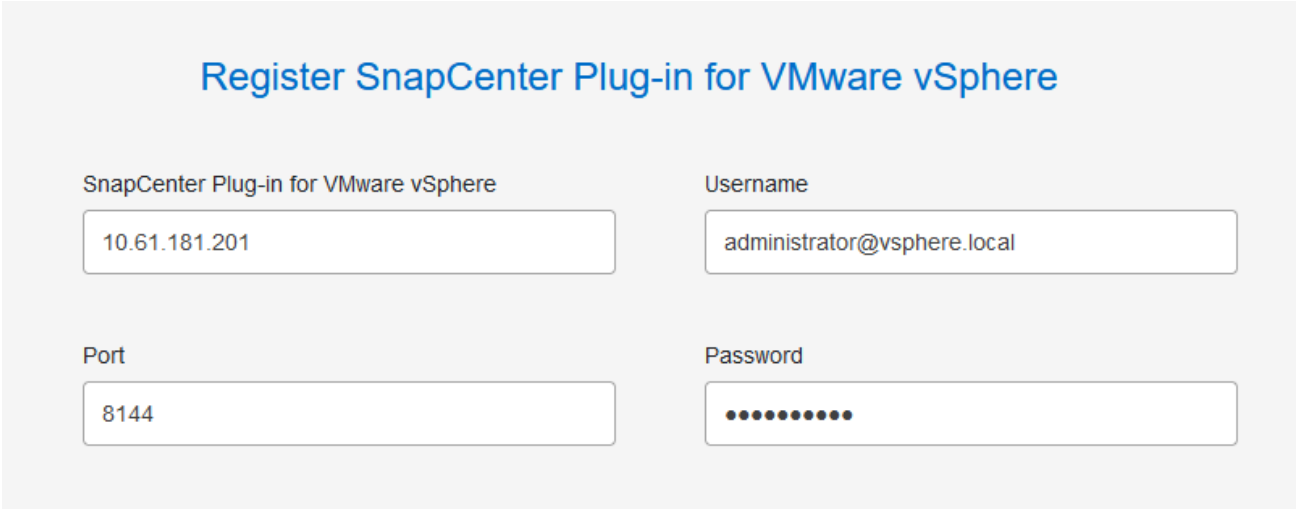
1. Nel menu a sinistra di NetApp Console, seleziona **Protection > Backup and recovery > Workloads >VMware**



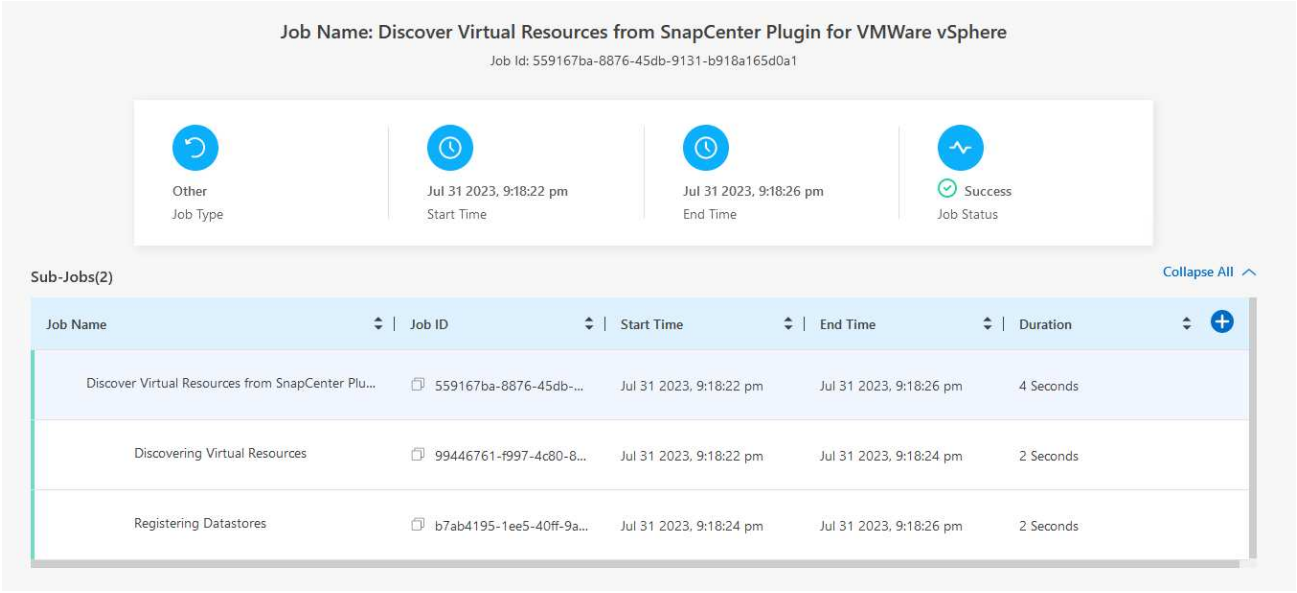
2. Dalla schermata principale Macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare * SnapCenter Plug-in for VMware vSphere*.



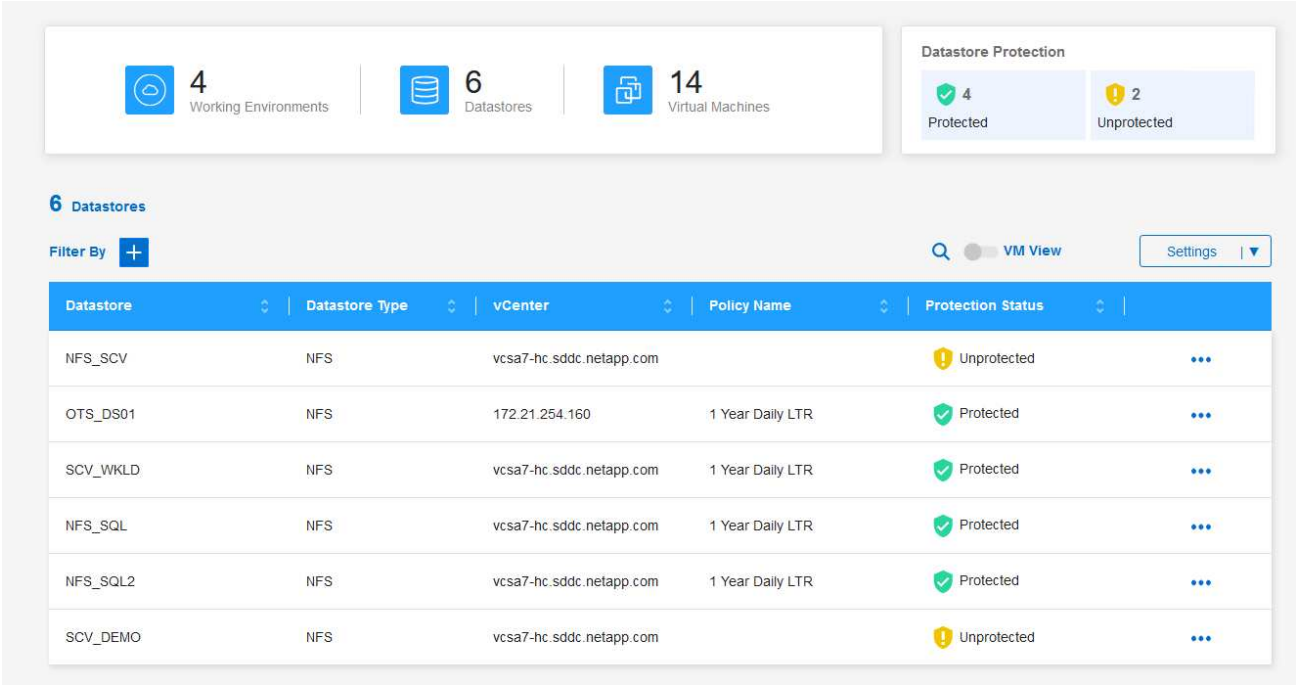
3. Fare clic sul pulsante **Registra**, quindi immettere l'indirizzo IP e il numero di porta per l'appliance SnapCenter Plug-in e il nome utente e la password per l'appliance di gestione vCenter. Fare clic sul pulsante **Registrati** per iniziare il processo di scoperta.



4. È possibile monitorare l'avanzamento dei lavori dalla scheda Monitoraggio lavori.



5. Una volta completata l'individuazione, sarà possibile visualizzare i datastore e le macchine virtuali in tutti gli appliance SCV individuati.

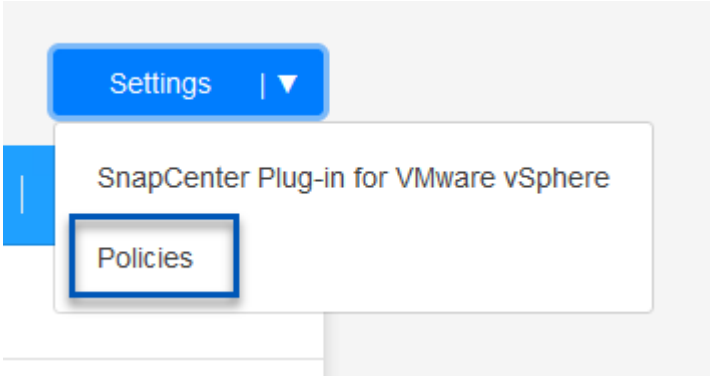


▼ Creare policy di backup

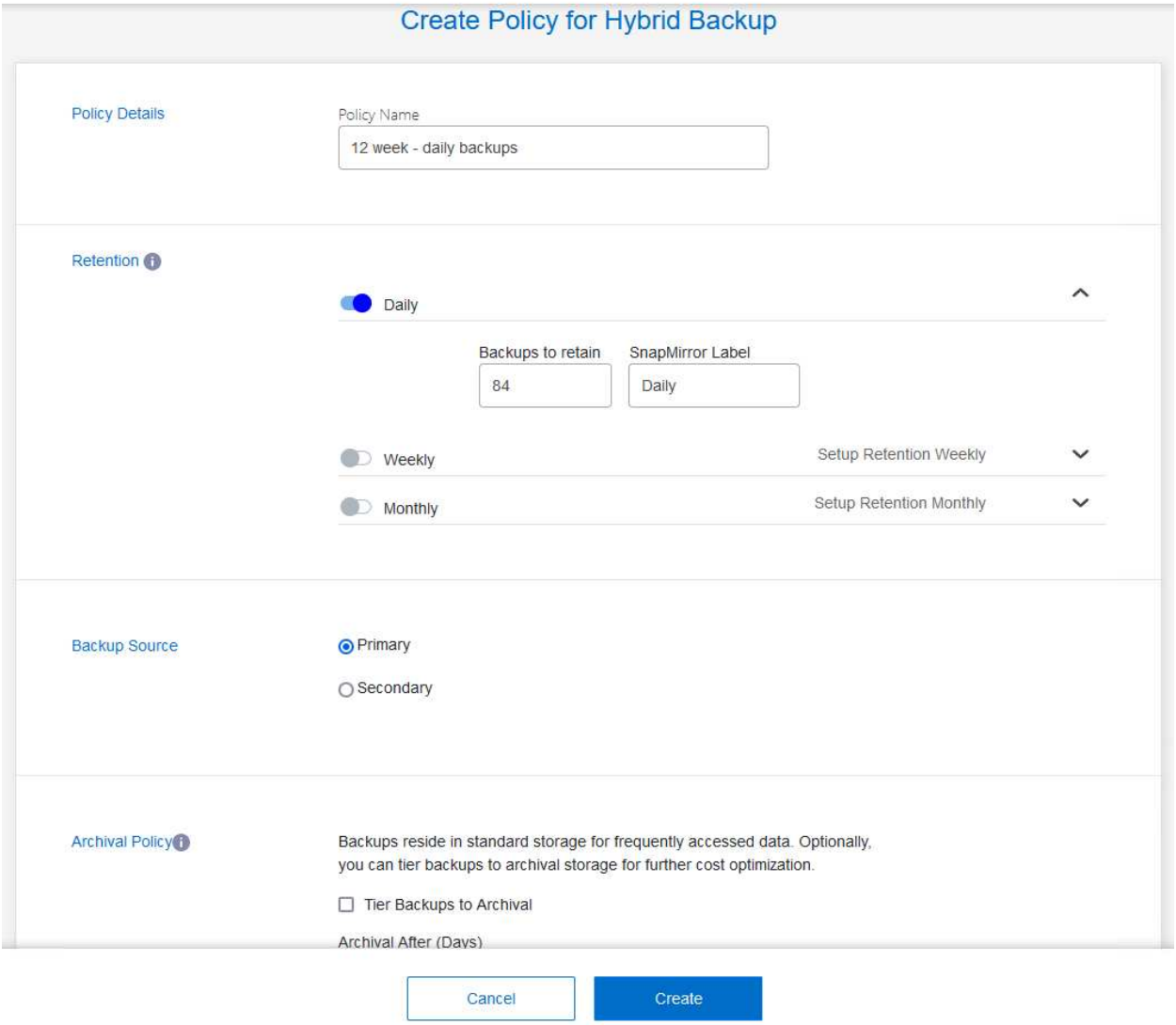
In NetApp Backup and Recovery for Virtual Machines, crea policy per specificare il periodo di conservazione, l'origine del backup e la policy di archiviazione.

Per ulteriori informazioni sulla creazione di gruppi di protezione, consulta "Crea un gruppo di protezione".

1. Dalla pagina principale di NetApp Backup and Recovery for Virtual Machines, accedi al menu a discesa **Settings** e seleziona **Policies**.



2. Fare clic su **Crea criterio** per accedere alla finestra **Crea criterio per backup ibrido**.
   a. Aggiungi un nome per la policy
   b. Seleziona il periodo di conservazione desiderato
   c. Selezionare se i backup verranno originati dal sistema di archiviazione ONTAP locale primario o secondario
   d. Facoltativamente, specificare dopo quale periodo di tempo i backup verranno archiviati in livelli diversi per un ulteriore risparmio sui costi.



L'etichetta SnapMirror immessa qui viene utilizzata per identificare a quali backup applicare la policy. Il nome dell'etichetta deve corrispondere al nome dell'etichetta nel criterio SCV locale corrispondente.

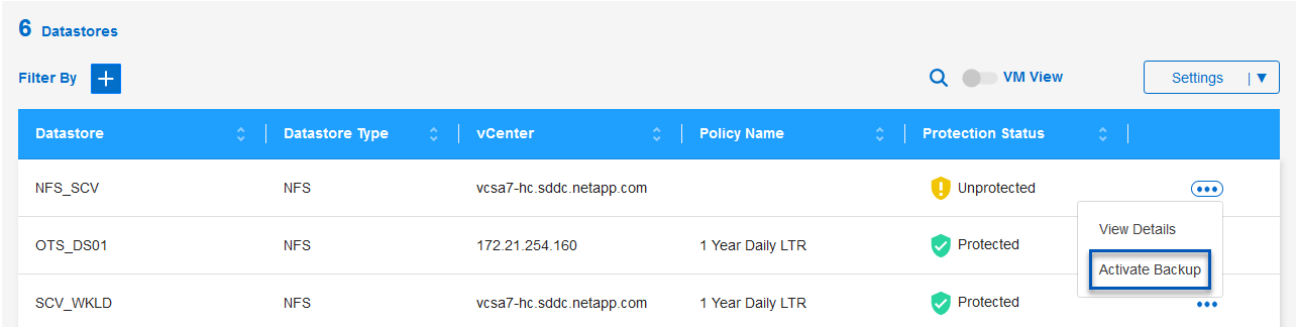
3. Fare clic su **Crea** per completare la creazione della policy.

▼ **Backup degli archivi dati su Amazon Web Services**

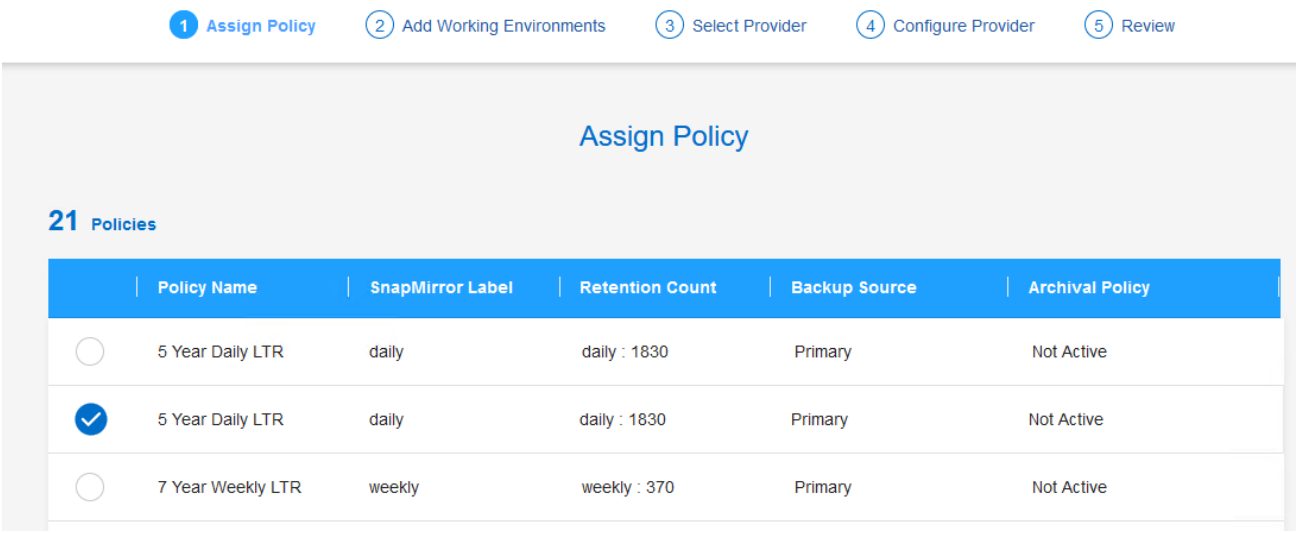
Il passaggio finale consiste nell'attivare la protezione dei dati per i singoli datastore e le macchine virtuali. I passaggi seguenti descrivono come attivare i backup su AWS.

Per ulteriori informazioni, consulta "Esegui il backup dei carichi di lavoro VMware".

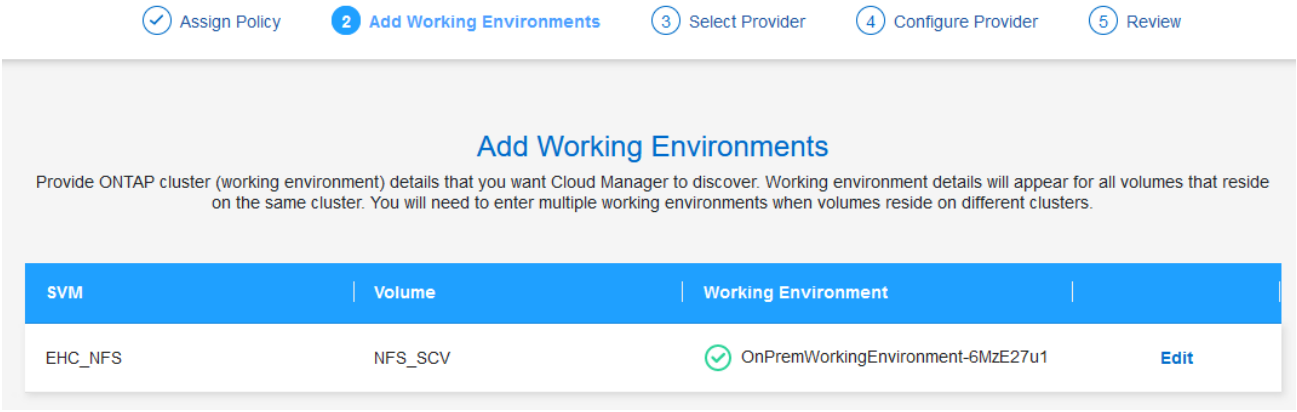
1. Dalla pagina principale di NetApp Backup and Recovery for Virtual Machines, accedi al menu a discesa delle impostazioni per il datastore di cui vuoi eseguire il backup e seleziona **Activate Backup**.



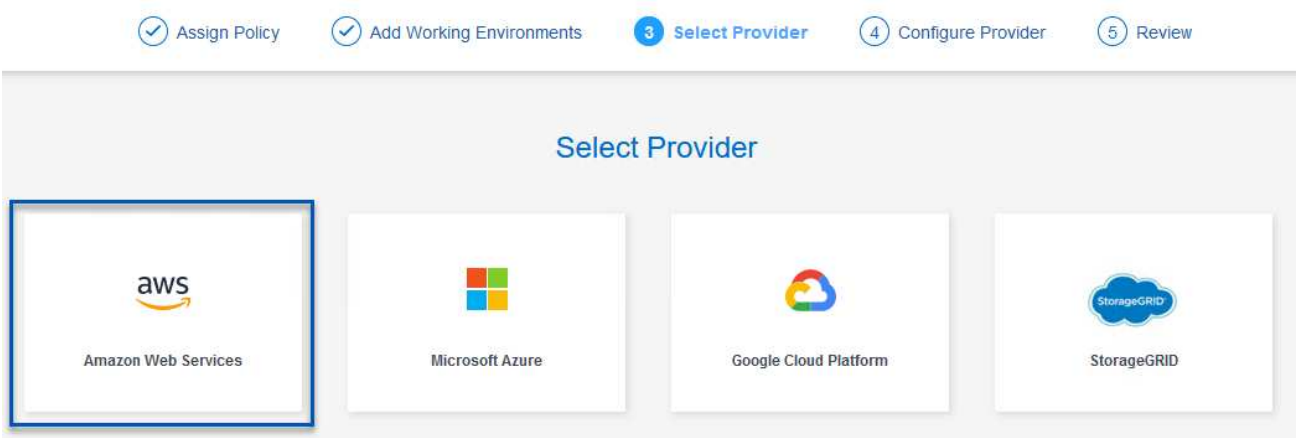
2. Assegnare la policy da utilizzare per l'operazione di protezione dei dati e fare clic su **Avanti**.



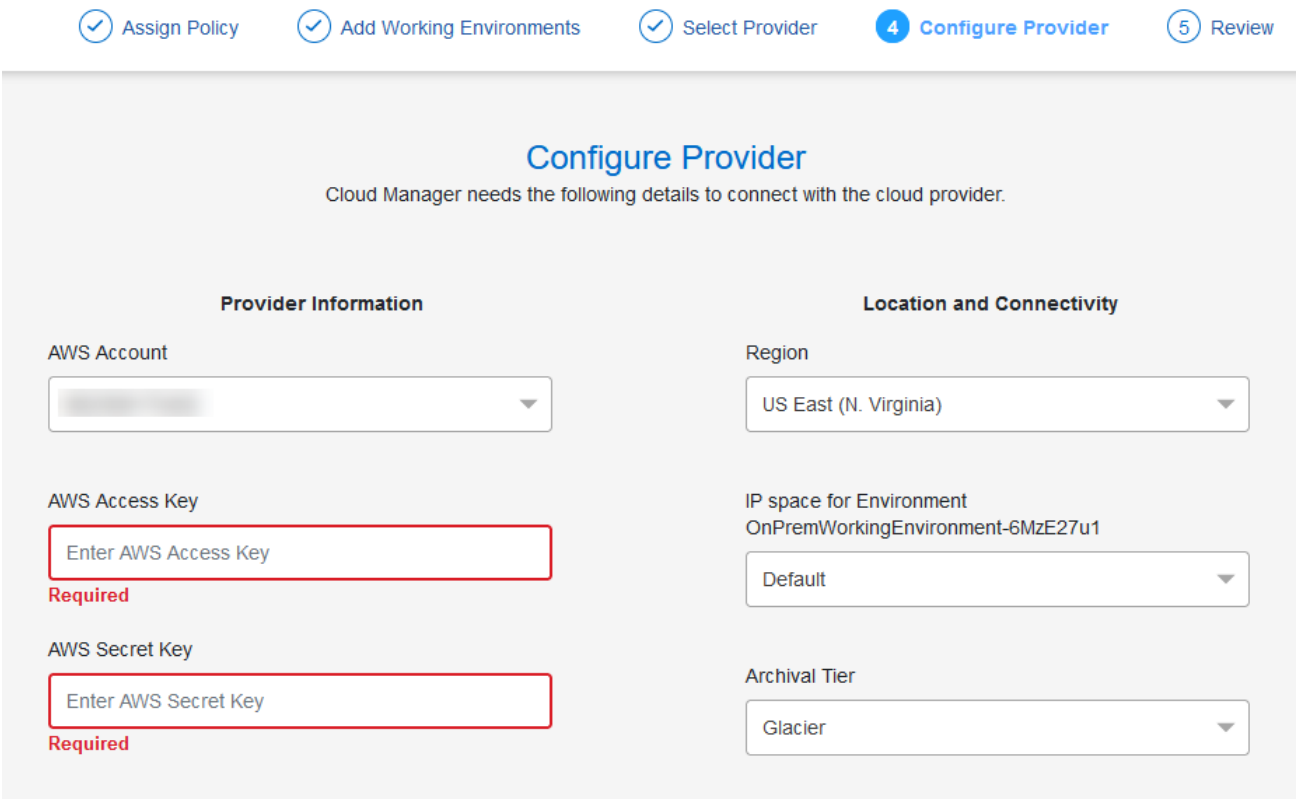
3. Nella pagina **Aggiungi ambienti di lavoro**, l'archivio dati e l'ambiente di lavoro con un segno di spunta dovrebbero apparire se l'ambiente di lavoro è stato precedentemente rilevato. Se l'ambiente di lavoro non è stato ancora scoperto, puoi aggiungerlo qui. Fare clic su **Avanti** per continuare.



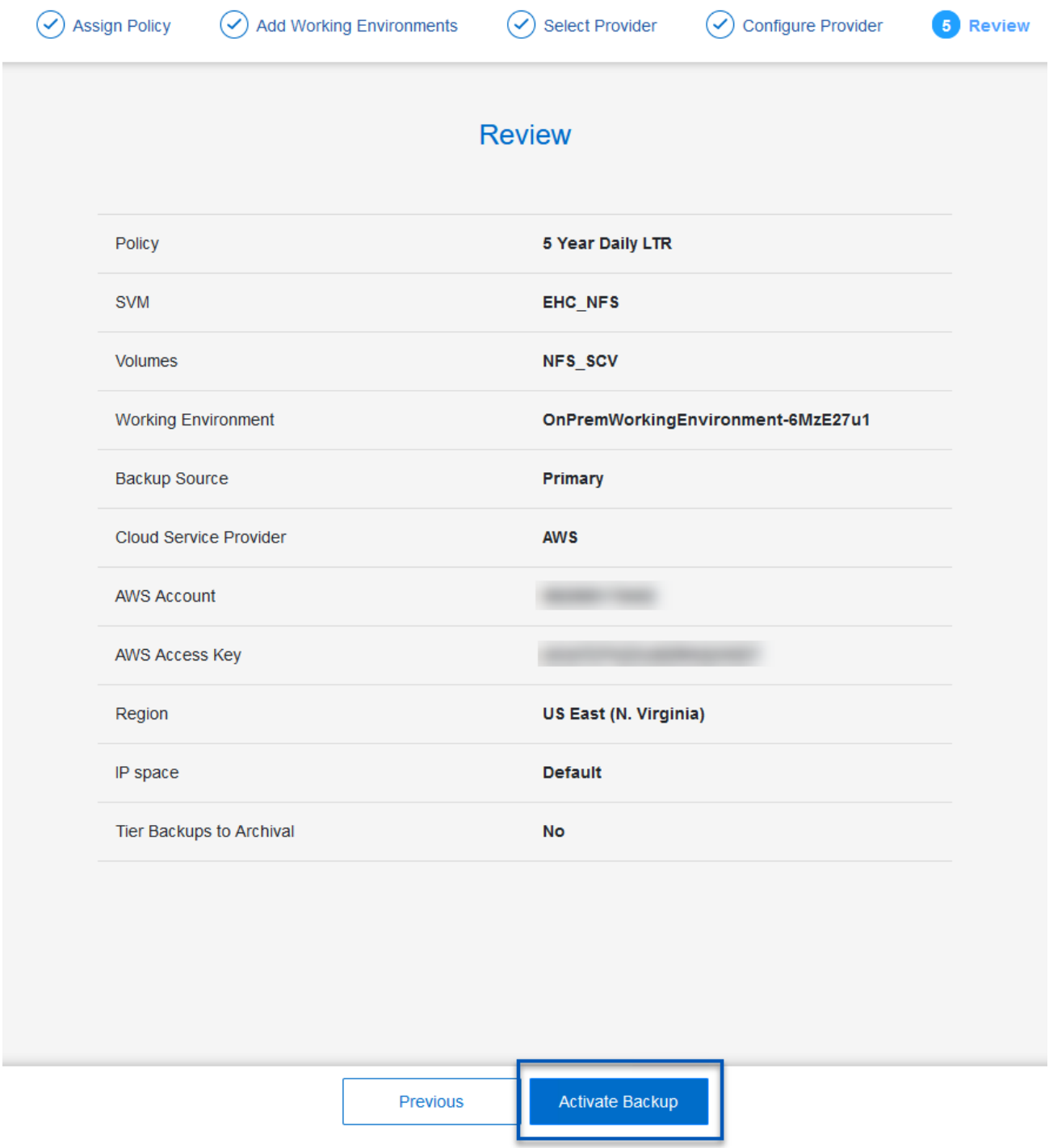
4. Nella pagina **Seleziona provider** clicca su AWS e poi clicca sul pulsante **Avanti** per continuare.



5. Compila le informazioni sulle credenziali specifiche del provider per AWS, tra cui la chiave di accesso e la chiave segreta AWS, la regione e il livello di archiviazione da utilizzare. Selezionare inoltre lo spazio IP ONTAP per il sistema di archiviazione ONTAP locale. Fare clic su **Avanti**.



6. Infine, rivedere 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. NetApp Backup and Recovery esegue ogni ora una scansione alla ricerca di eventuali Snapshot in sospeso e li trasferisce quindi allo storage a oggetti.

Ripristino di macchine virtuali in caso di perdita di dati

Garantire la salvaguardia dei tuoi dati è solo uno degli aspetti di una protezione completa dei dati. Altrettanto cruciale è la capacità di ripristinare tempestivamente i dati da qualsiasi posizione in caso di perdita di dati o di attacco ransomware. Questa capacità è fondamentale per mantenere operazioni aziendali senza interruzioni e raggiungere gli obiettivi del punto di ripristino.

NetApp offre una strategia 3-2-1 altamente adattabile, che fornisce un controllo personalizzato sui programmi di conservazione nelle posizioni di archiviazione primaria, secondaria e degli oggetti. Questa strategia offre la flessibilità necessaria per adattare gli approcci alla protezione dei dati alle esigenze specifiche.

Questa sezione fornisce una panoramica del processo di ripristino dei dati sia da SnapCenter Plug-in for VMware vSphere sia da NetApp Backup and Recovery per macchine virtuali.

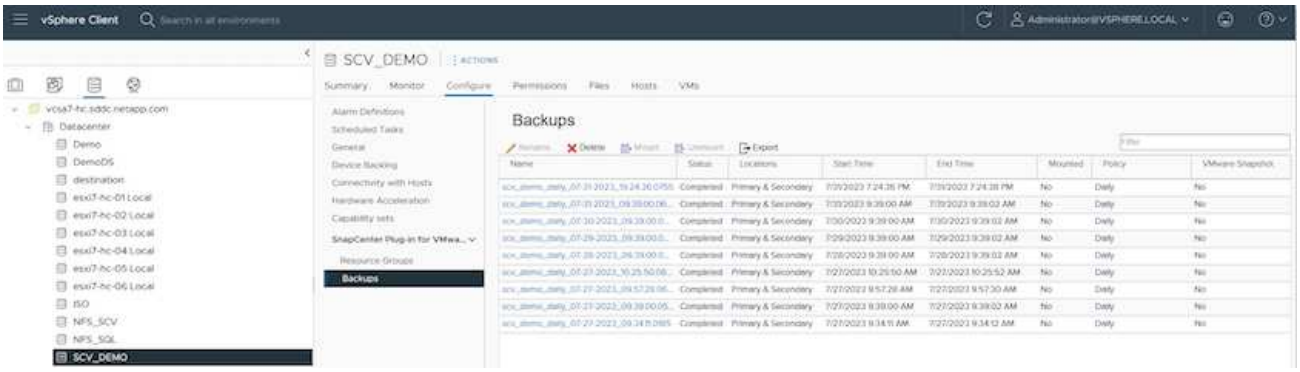
Ripristino di macchine virtuali dal SnapCenter Plug-in for VMware vSphere

Per questa soluzione le macchine virtuali sono state ripristinate nelle posizioni originali e alternative. Questa soluzione non copre tutti gli aspetti delle funzionalità di ripristino dei dati di SCV. Per informazioni approfondite su tutto ciò che SCV ha da offrire, fare riferimento al "Ripristinare le VM dai backup" nella documentazione del prodotto.

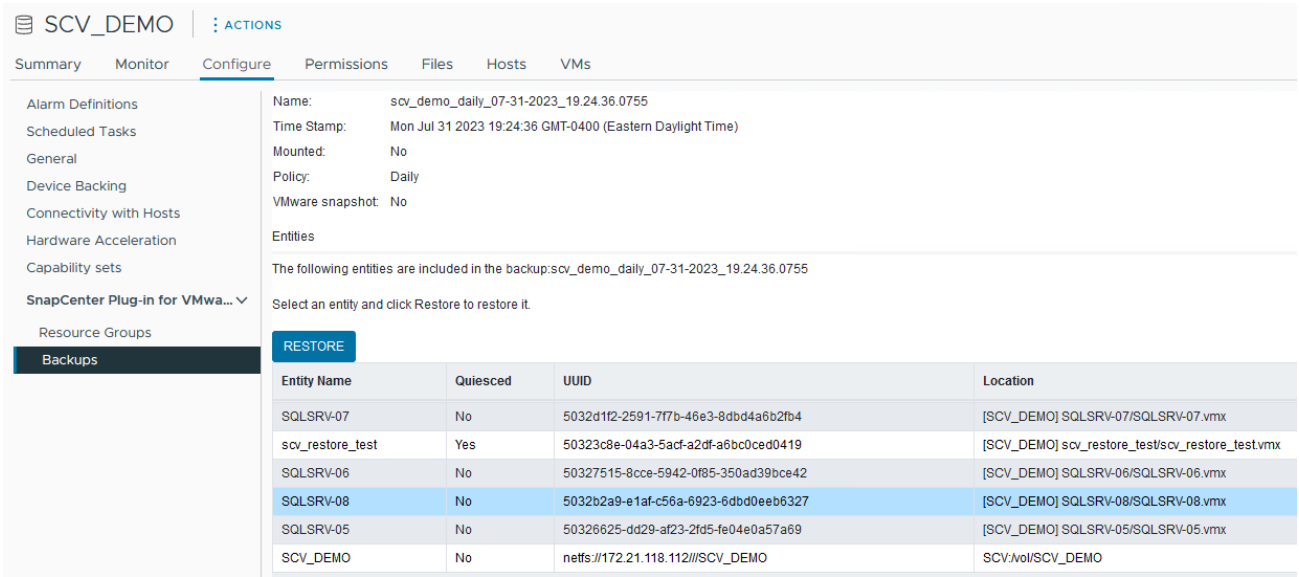
▼ **Ripristinare le macchine virtuali da SCV**

Completare i seguenti passaggi per ripristinare una macchina virtuale da un archivio primario o secondario.

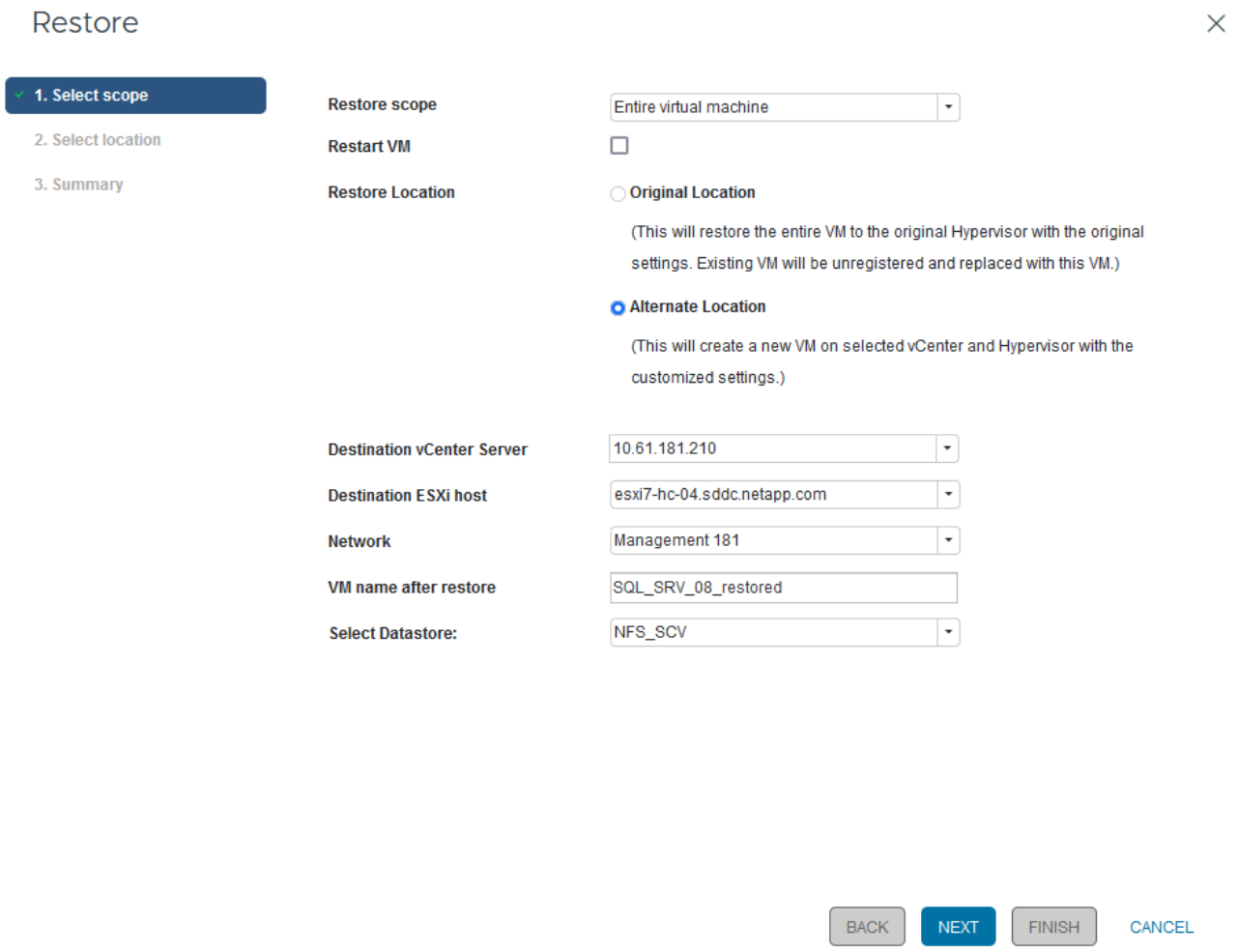
1. Dal client vCenter, vai su **Inventario > Archiviazione** e fai clic sul datastore che contiene le macchine virtuali che desideri ripristinare.
2. Dalla scheda **Configura** fare clic su **Backup** per accedere all'elenco dei backup disponibili.



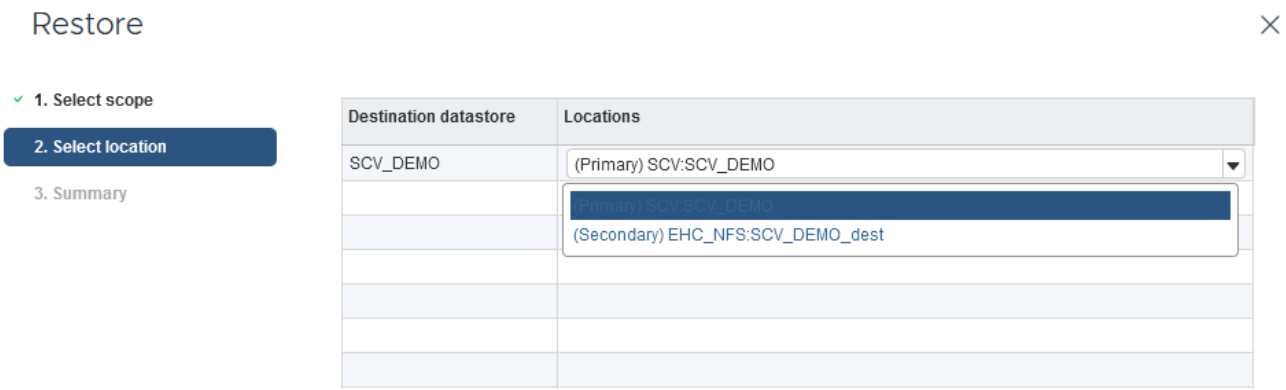
3. Fare clic su un backup per accedere all'elenco delle VM, quindi selezionare una VM da ripristinare. Fare clic su **Ripristina**.



4. Dalla procedura guidata di ripristino, seleziona se ripristinare l'intera macchina virtuale o un VMDK specifico. Selezionare se installare nella posizione originale o in una posizione alternativa, fornire il nome della VM dopo il ripristino e il datastore di destinazione. Fare clic su **Avanti**.



5. Scegliere se eseguire il backup dalla posizione di archiviazione primaria o secondaria.



6. Infine, rivedere un riepilogo del processo di backup e fare clic su Fine per avviare il processo di ripristino.

Ripristino delle macchine virtuali da NetApp Backup and Recovery for Virtual Machines

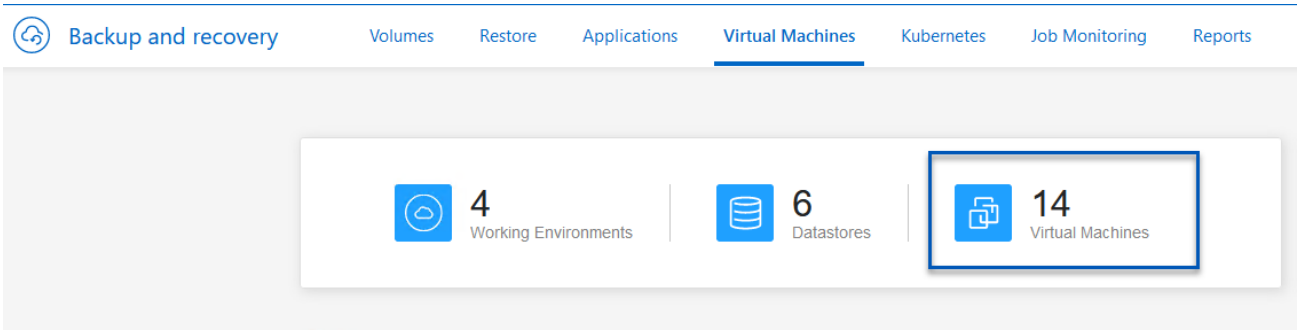
NetApp Backup and Recovery for Virtual Machines consente di ripristinare le macchine virtuali nella loro posizione originale. Puoi accedere alle funzioni di ripristino tramite la console web di NetApp Backup and Recovery.

Per ulteriori informazioni consulta "Ripristina i dati delle macchine virtuali dal cloud".

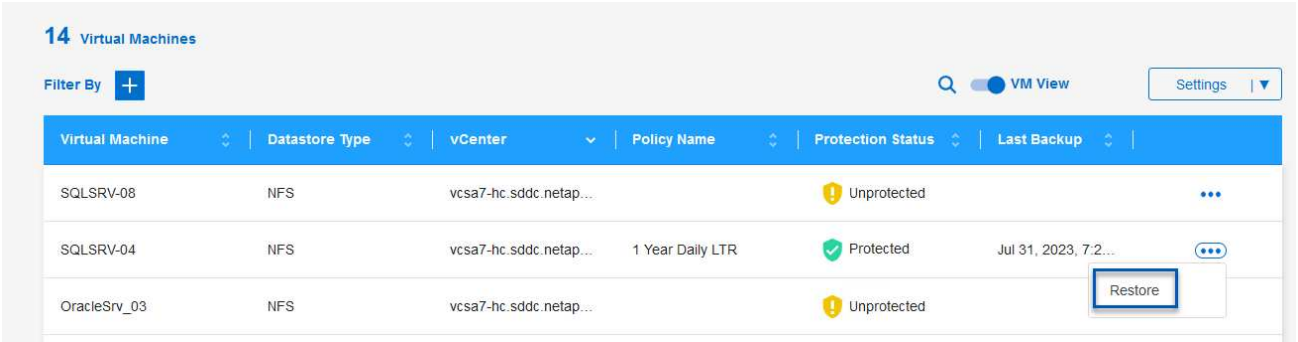
▼ **Ripristinare le macchine virtuali da NetApp Backup and Recovery**

Per ripristinare una macchina virtuale da NetApp Backup and Recovery, segui i passaggi seguenti.

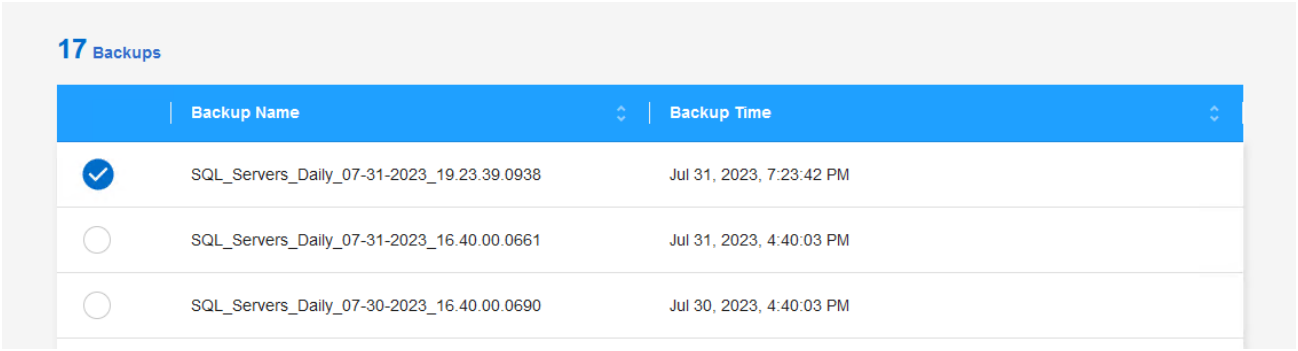
1. Passare a **Protezione > Backup e ripristino > Macchine virtuali** e fare clic su Macchine virtuali per visualizzare l'elenco delle macchine virtuali disponibili per il ripristino.



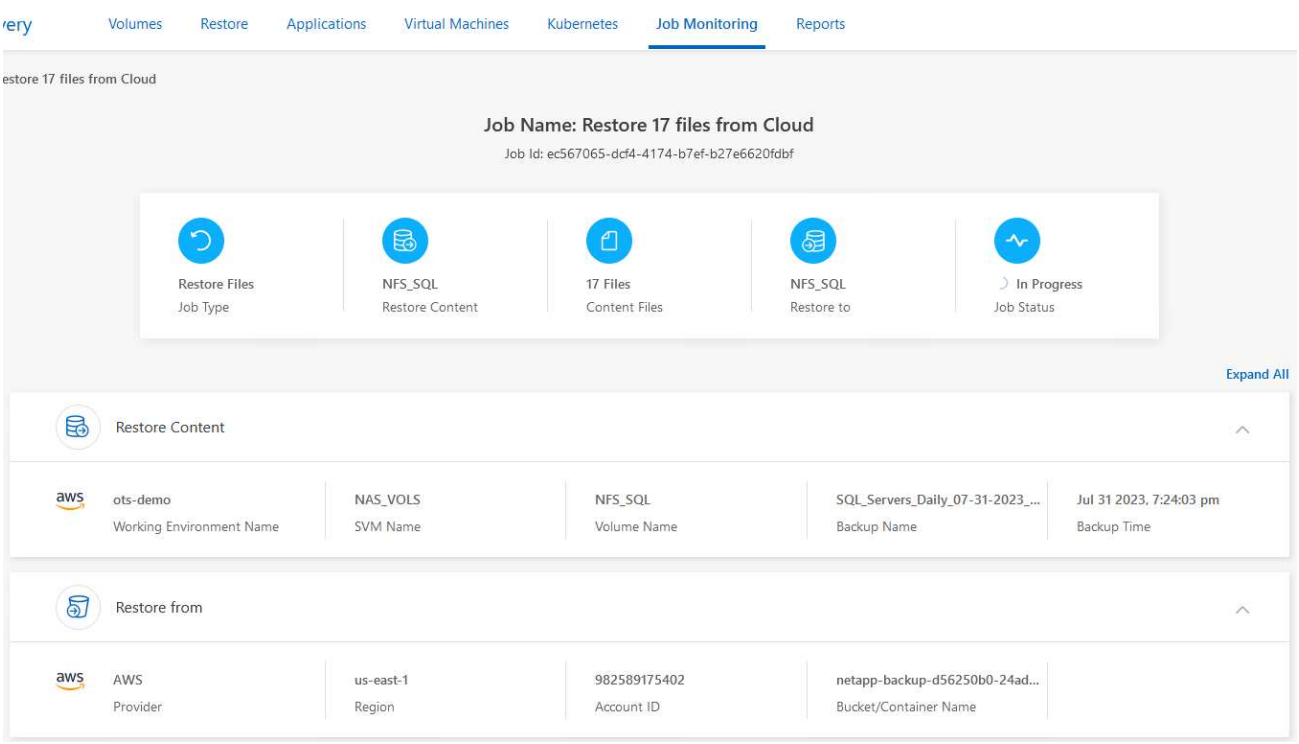
2. Accedi al menu a discesa delle impostazioni per la VM da ripristinare e seleziona



3. Selezionare il backup da cui effettuare 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, quando viene implementata con SnapCenter Plug-in for VMware vSphere e NetApp Backup and Recovery per le macchine virtuali, offre una soluzione robusta, affidabile e conveniente per la protezione dei dati. Questa strategia non solo garantisce la ridondanza e l'accessibilità dei dati, ma offre anche la flessibilità di ripristinare i dati da qualsiasi posizione e sia da sistemi storage ONTAP on-premises che da storage a oggetti basato su cloud.

Il caso d'uso presentato in questa documentazione si concentra su tecnologie di protezione dei dati collaudate che evidenziano l'integrazione tra NetApp, VMware e i principali cloud provider. 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 una pianificazione semplice, il monitoraggio e operazioni di ripristino flessibili all'interno dell'ecosistema VMware. NetApp Backup and Recovery per le macchine virtuali fornisce l'uno (1) nel 3-2-1 offrendo backup sicuri e air-gapped dei dati delle macchine virtuali su storage a oggetti basato su cloud. L'interfaccia intuitiva e il flusso di lavoro logico forniscono una piattaforma sicura per l'archiviazione a lungo termine dei dati critici.

Informazioni aggiuntive

Per saperne di più sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Documentazione SnapCenter Plug-in for VMware vSphere"
- "Documentazione di NetApp Console"

NetApp Disaster Recovery

Panoramica

Il Disaster Recovery è una priorità assoluta per ogni amministratore VMware. Poiché

VMware incapsula interi server in una serie di file che costituiscono la macchina virtuale, gli amministratori sfruttano tecniche basate su storage a blocchi, come cloni, snapshot e repliche, per proteggere queste VM. Gli array ONTAP offrono la replica integrata per trasferire i dati dei volumi, e quindi le macchine virtuali residenti sui LUN del datastore designati, da un sito all'altro. NetApp Disaster Recovery si integra con vSphere e automatizza l'intero flusso di lavoro per un failover e un failback senza interruzioni in caso di disastro. Combinando la replica dello storage con l'automazione intelligente, gli amministratori dispongono ora di un modo gestibile non solo per configurare, automatizzare e testare i piani di disaster recovery, ma anche dei mezzi per eseguirli facilmente in caso di disastro.

La parte più dispendiosa in termini di tempo di un failover DR in un ambiente VMware vSphere è l'esecuzione dei passaggi necessari per inventariare, registrare, riconfigurare e accendere le VM nel sito DR. Una soluzione ideale ha sia un basso RPO (misurato in minuti) sia un basso RTO (misurato in minuti o ore). Un fattore che spesso viene trascurato in una soluzione DR è la capacità di testare la soluzione DR in modo efficiente a intervalli periodici.

Per progettare una soluzione DR, è necessario tenere a mente i seguenti fattori:

- L'obiettivo del tempo di recupero (RTO). L'RTO indica la rapidità con cui un'azienda può riprendersi da un disastro o, più specificamente, il tempo necessario per eseguire il processo di ripristino e rendere nuovamente disponibili i servizi aziendali.
- L'obiettivo del punto di ripristino (RPO). L'RPO indica l'età dei dati recuperati dopo essere stati resi disponibili, in relazione al momento in cui si è verificato il disastro.
- Scalabilità e adattabilità. Questo fattore include la possibilità di aumentare gradualmente le risorse di archiviazione man mano che aumenta la domanda.

Per maggiori informazioni tecniche sulle soluzioni disponibili, consultare:

- "NetApp Disaster Recovery per datastore NFS"
- "NetApp Disaster Recovery per datastore VMFS"

NetApp Disaster Recovery per datastore NFS

NetApp Disaster Recovery per datastore NFS

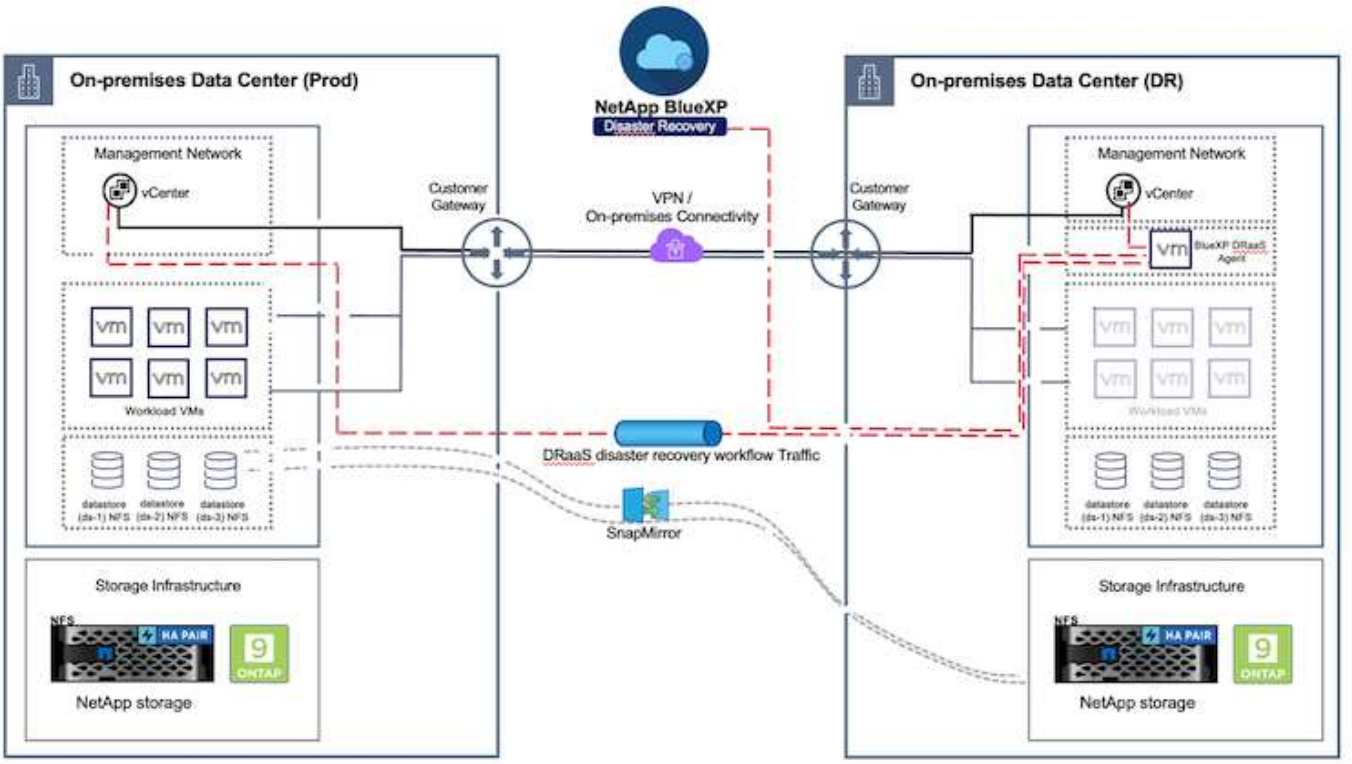
L'implementazione del disaster recovery tramite replica a livello di blocco dal sito di produzione al sito di disaster recovery è un metodo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Utilizzando la replica NetApp SnapMirror , i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali con datastore NFS possono essere replicati su un altro sistema di storage ONTAP situato in un data center di ripristino designato in cui è distribuito anche VMware.

Questa sezione del documento descrive la configurazione di NetApp Disaster Recovery per configurare il disaster recovery per le VM VMware on-premise verso un altro sito designato. Questa configurazione include l'agente Console, l'onboarding degli array ONTAP, la definizione dei siti e l'associazione di VMware vCenter. Inoltre, questo documento descrive in dettaglio come configurare la replica tra i siti e come configurare e testare un piano di recovery. L'ultima sezione contiene istruzioni per eseguire un failover completo del sito e

come eseguire il failback quando il sito primario viene ripristinato e riportato online.

Utilizzando Disaster Recovery, parte di NetApp Data Services, le aziende possono facilmente individuare i propri vCenters VMware on-premise e lo storage ONTAP. Le organizzazioni possono quindi creare gruppi di risorse, creare un piano di recovery, associarlo ai gruppi di risorse e testare o eseguire failover e failback. SnapMirror fornisce la replica a blocchi a livello di storage per mantenere aggiornati i due siti con modifiche incrementali, con un Recovery Point Objective (RPO) fino a 5 minuti. Inoltre, è possibile simulare le procedure di disaster recovery senza influire sulla produzione o sostenere costi aggiuntivi per lo storage.

Disaster Recovery sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore NFS a partire dall'ultima Snapshot replicata nel sito di disaster recovery. Dopo aver completato il test di disaster recovery, puoi eliminare facilmente l'ambiente di test senza influire sulle risorse di produzione replicate effettive. In caso di failover effettivo, Disaster Recovery orchestra tutti i passaggi necessari per avviare automaticamente le macchine virtuali protette nel sito di disaster recovery designato con pochi clic. Il servizio invertirà anche la relazione di SnapMirror verso il sito primario e replicherà eventuali modifiche dal secondario al primario per un'operazione di failback, quando necessario. Tutte queste funzionalità sono disponibili a una frazione del costo rispetto ad altre alternative ben note.

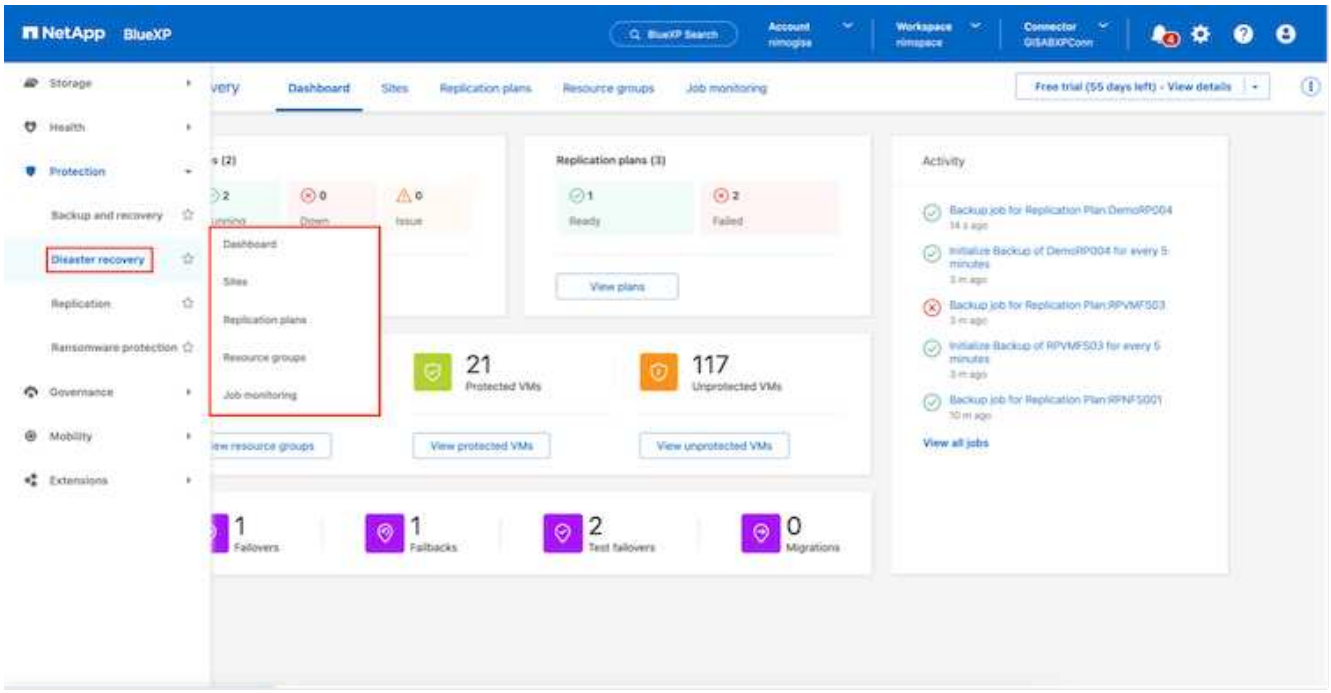


Per informazioni aggiornate e sulle versioni supportate di vCenter Server, ESXi e ONTAP per il Disaster Recovery, consulta "Configurazioni supportate per il disaster recovery".

Iniziare

Per iniziare con NetApp Disaster Recovery, usa NetApp Console e poi accedi al servizio.

1. Accedi a Console.
2. Dal menu di navigazione a sinistra di Console, seleziona Protection > Disaster Recovery.
3. Compare la Disaster Recovery Dashboard.

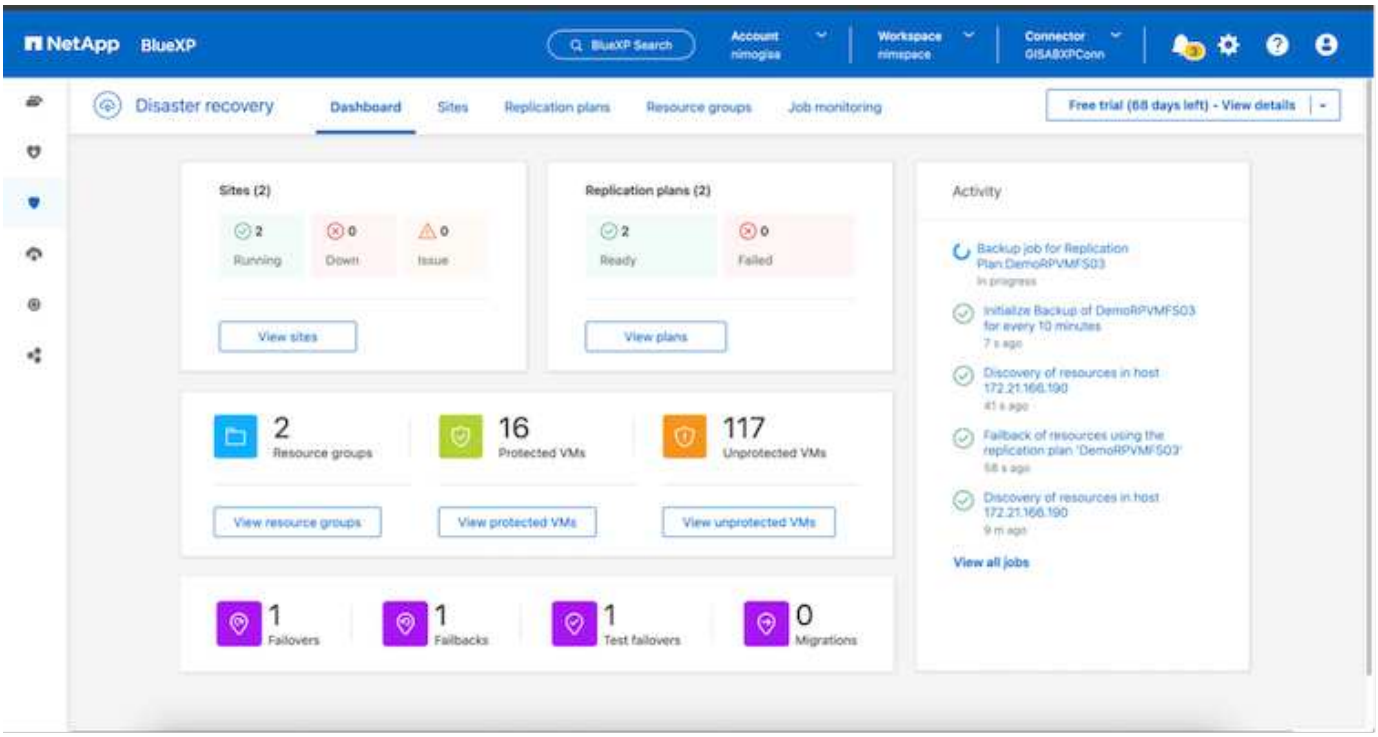


Prima di configurare il piano di Disaster Recovery, assicurati che siano soddisfatti i seguenti prerequisiti:

- L'agente della console è stato distribuito.
- L'agente dispone di connettività ai sistemi vCenter di origine e di destinazione e ai sistemi storage.
- È disponibile un cluster ONTAP con SVM abilitata per il servizio NFS.
- In Console vengono aggiunti i sistemi di storage NetApp on-premises che ospitano datastore NFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su NFS designati.
- Assicurarsi che l'ambiente disponga di versioni supportate dei server vCenter Server ed ESXi.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere un paio di clic e circa 3-5 minuti.

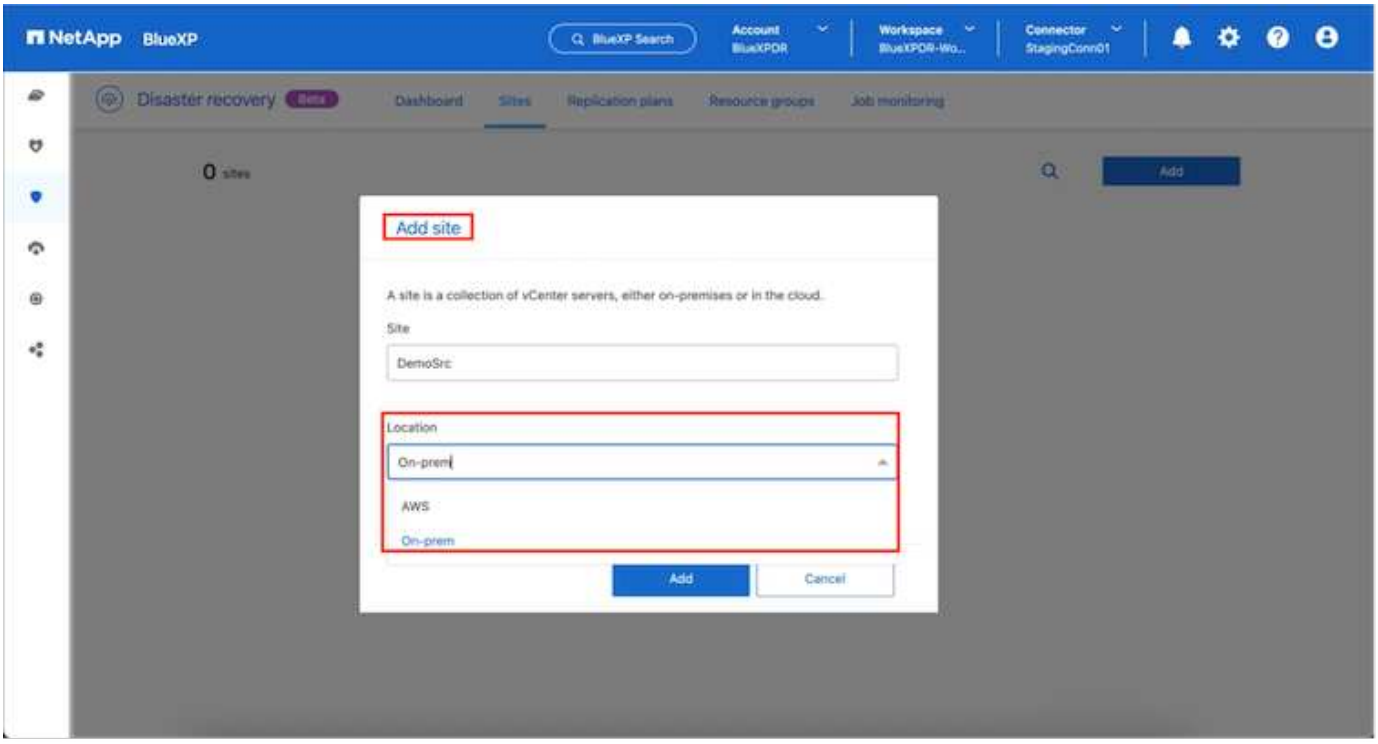
NetApp consiglia di distribuire l'agente Console nel sito di destinazione o in un terzo sito, in modo che l'agente Console possa comunicare attraverso la rete con le risorse di origine e di destinazione.



NetApp Disaster Recovery: configurazione

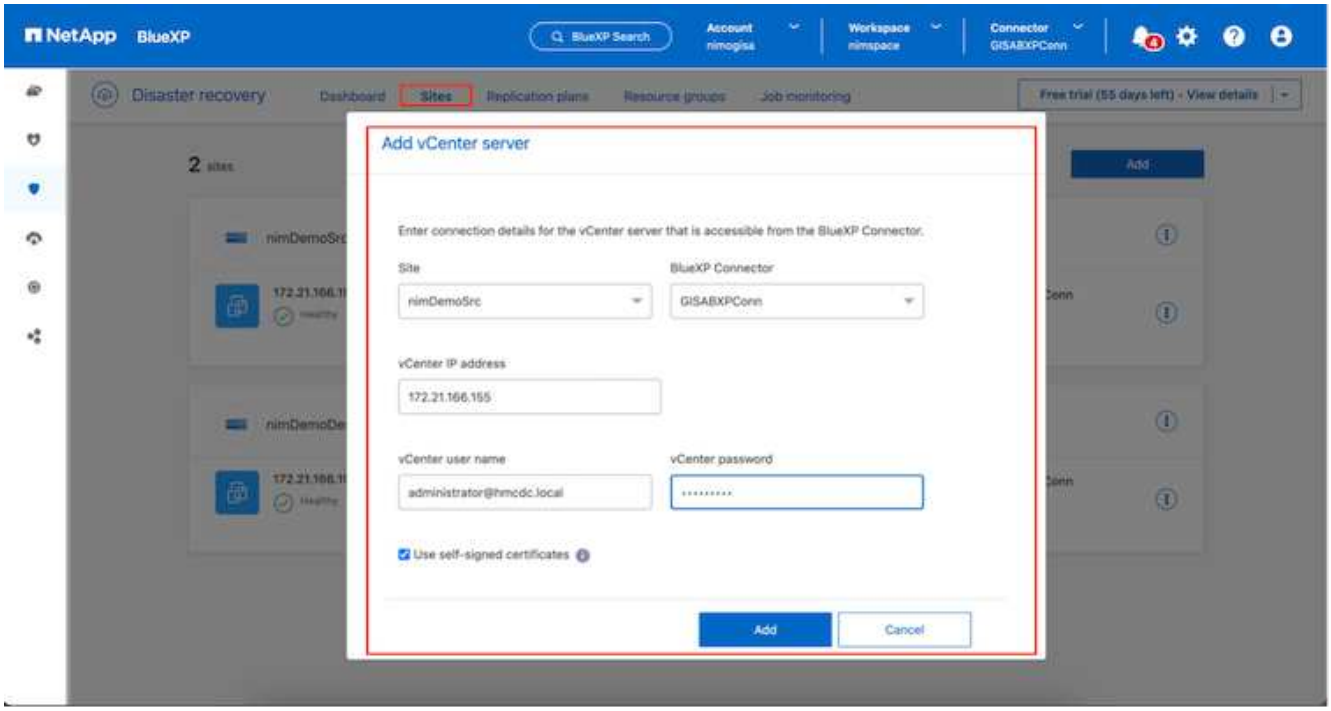
Il primo passo nella preparazione al ripristino di emergenza consiste nell'individuare e aggiungere vCenter e le risorse di storage a NetApp Disaster Recovery.

Apri Console e seleziona **Protezione > Disaster Recovery** dalla navigazione a sinistra. Fai clic su **Siti**, inserisci un nome e seleziona il tipo di posizione. Quindi, fai clic sul pulsante **Aggiungi vCenter**.

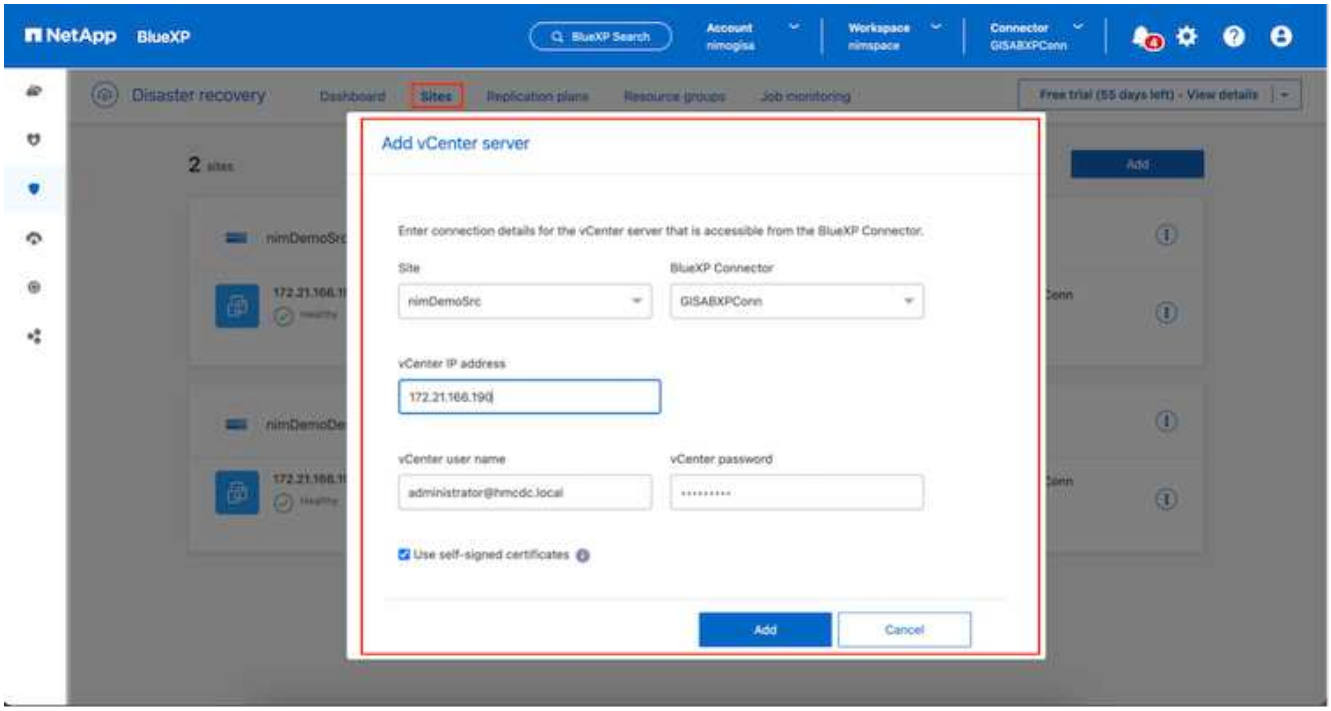


Aggiungere le seguenti piattaforme:

- **Fonte**. vCenter locale.



- **Destinazione**. VMC SDDC vCenter.



Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra l'array del sito di origine e l'array del sito di destinazione

SnapMirror fornisce la replica dei dati in un ambiente NetApp. Basata sulla tecnologia Snapshot di NetApp, la replica di SnapMirror è estremamente efficiente perché replica solo i blocchi modificati o aggiunti

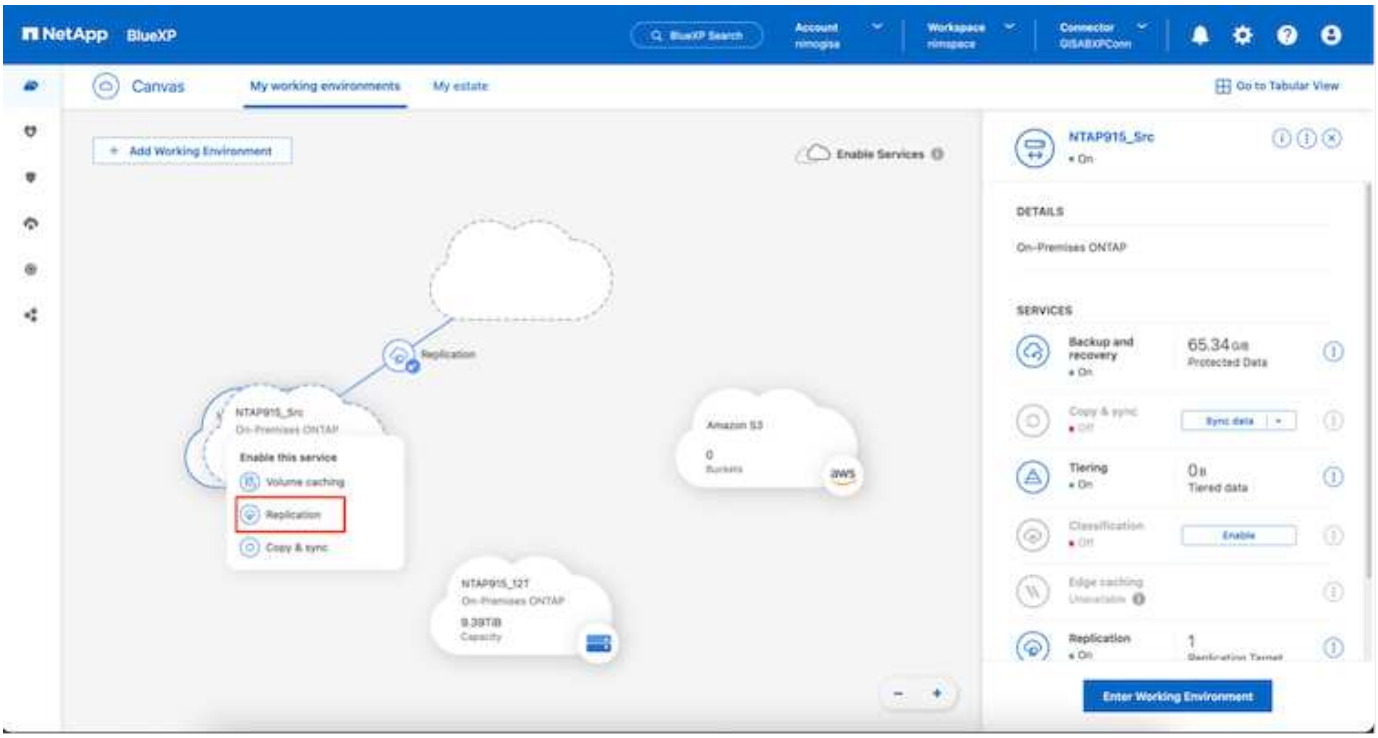
dall'aggiornamento precedente. SnapMirror si configura facilmente utilizzando NetApp OnCommand System Manager o la CLI di ONTAP. NetApp Data Services crea anche la relazione di SnapMirror, a condizione che il cluster e il peering SVM siano configurati in anticipo.

Nei casi in cui lo storage primario non sia completamente perso, SnapMirror fornisce un mezzo efficiente per risincronizzare i siti primario e di DR. SnapMirror può risincronizzare i due siti, trasferendo dal sito di DR al sito primario solo i dati modificati o nuovi, semplicemente invertendo le relazioni di SnapMirror. Ciò significa che i piani di replica dei dati nel Disaster Recovery possono essere risincronizzati in entrambe le direzioni dopo un failover senza ricopiare l'intero volume. Se una relazione viene risincronizzata nella direzione inversa, solo i nuovi dati scritti dall'ultima sincronizzazione riuscita della copia Snapshot vengono inviati di nuovo alla destinazione.

Se la relazione di SnapMirror è già configurata per il volume tramite CLI o System Manager, NetApp Data Services rileva la relazione e prosegue con il resto delle operazioni del flusso di lavoro.

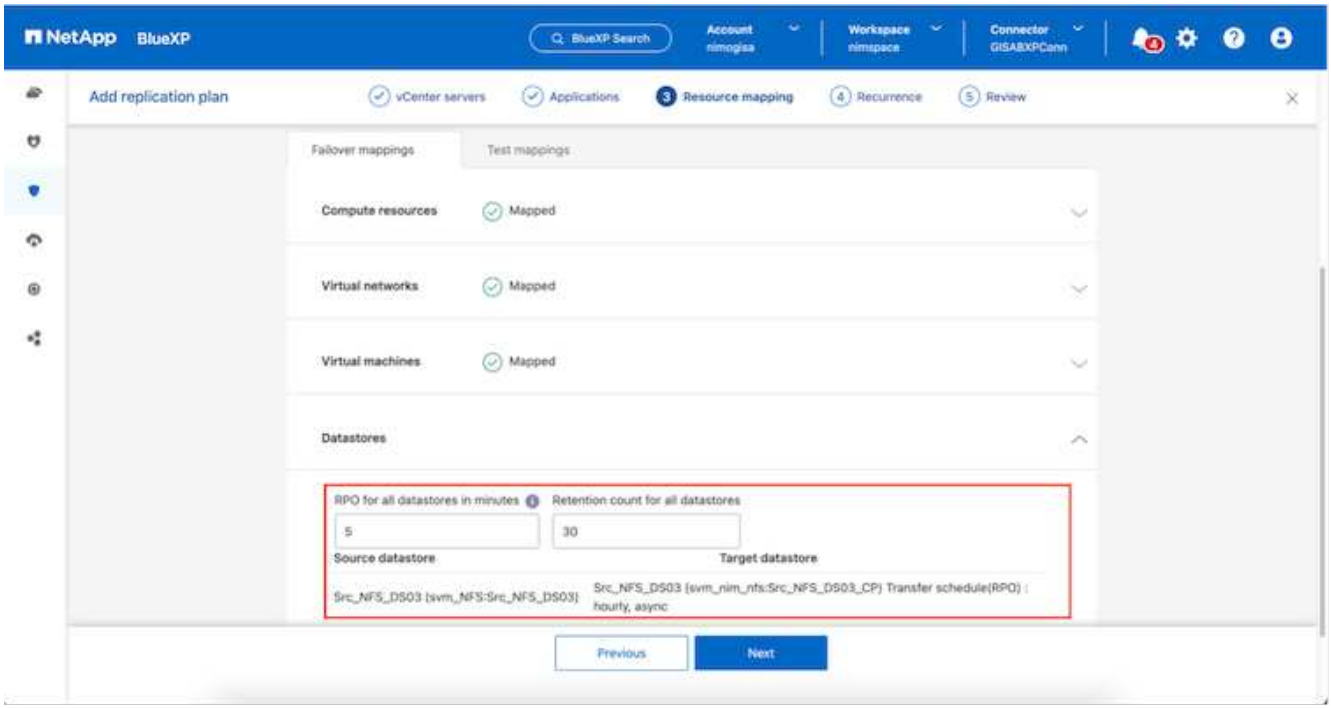
Come configurarlo per VMware Disaster Recovery

La procedura per creare la replica di SnapMirror rimane la stessa per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è utilizzare NetApp Console per configurare la replica di SnapMirror tramite un semplice drag & drop del sistema ONTAP di origine nell'ambiente verso la destinazione, in modo da attivare la procedura guidata che ti accompagna nel resto del processo.



Disaster Recovery può anche automatizzare la stessa operazione a condizione che siano soddisfatti i due criteri seguenti:

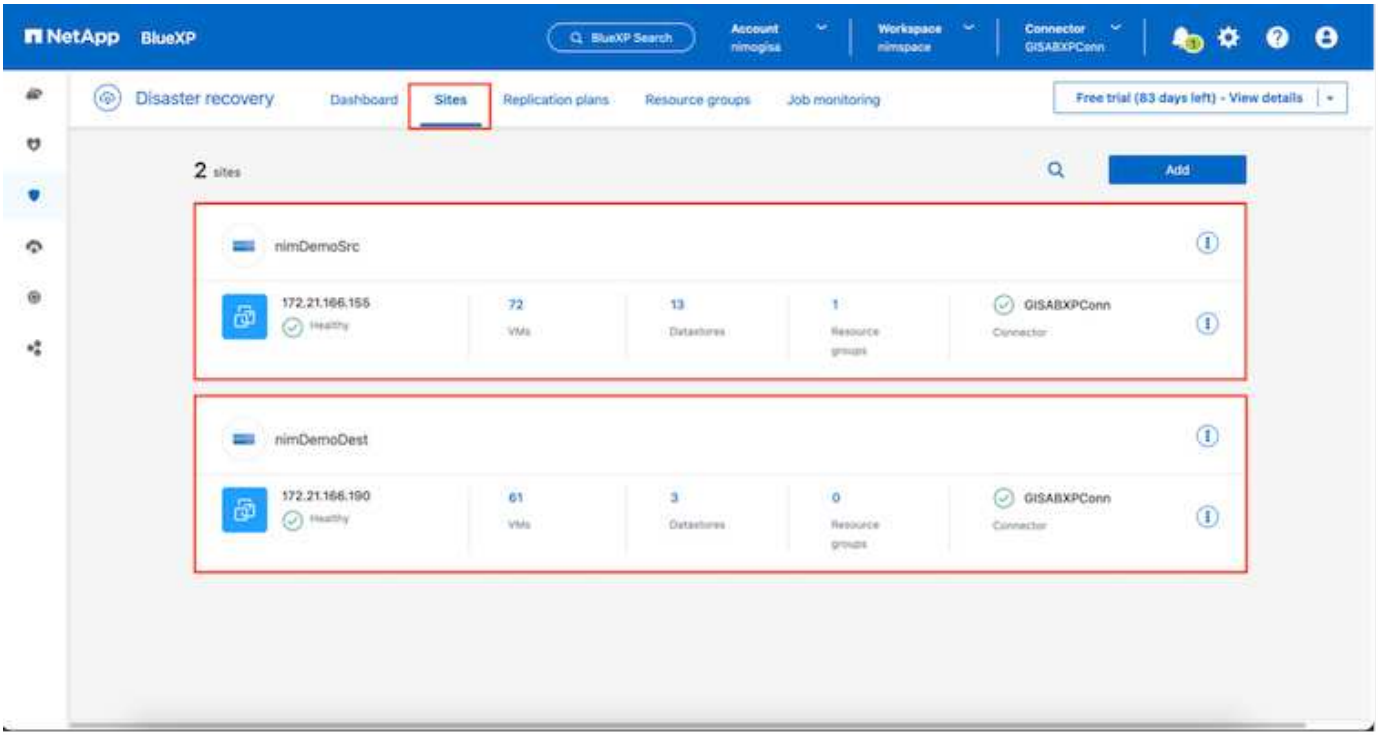
- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.



Se la relazione di SnapMirror è già configurata per il volume tramite CLI, Disaster Recovery la rileva e prosegue con il resto delle operazioni del flusso di lavoro.

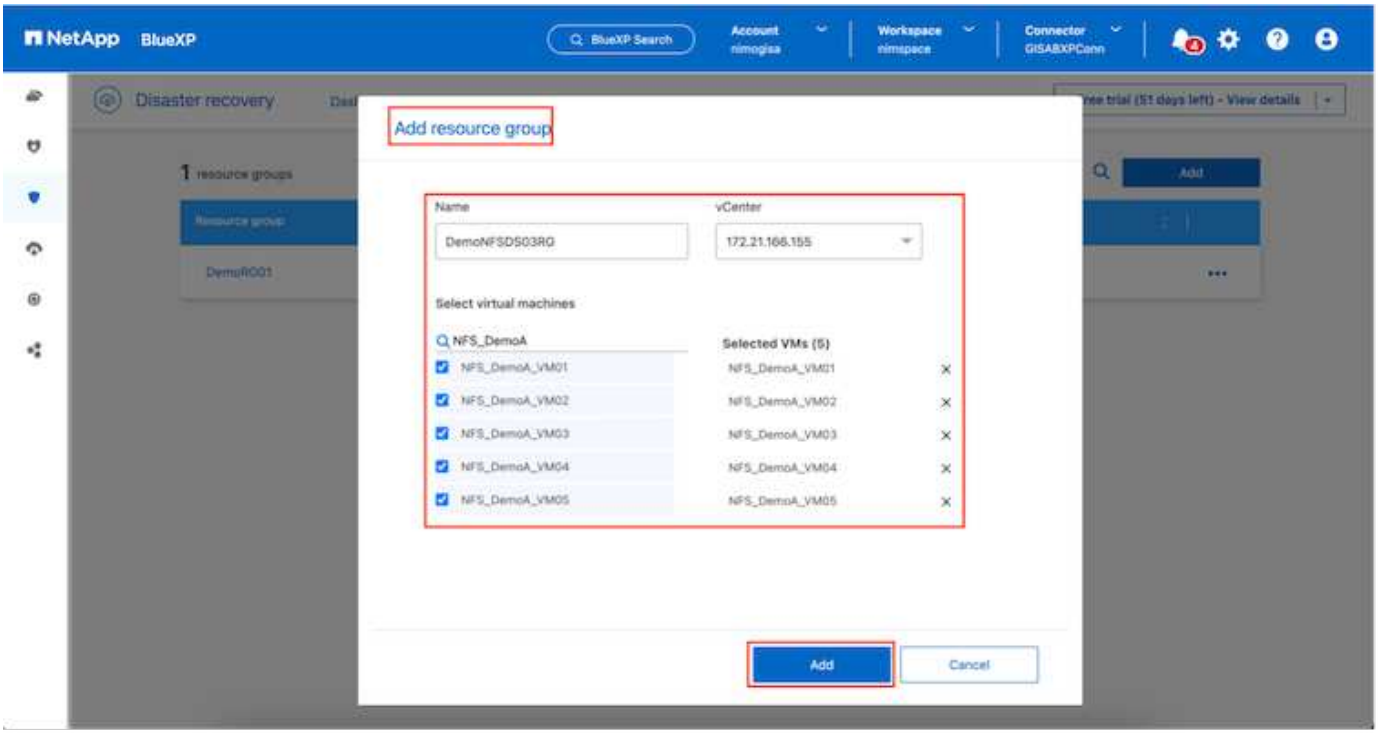
Cosa può fare il Disaster Recovery per te?

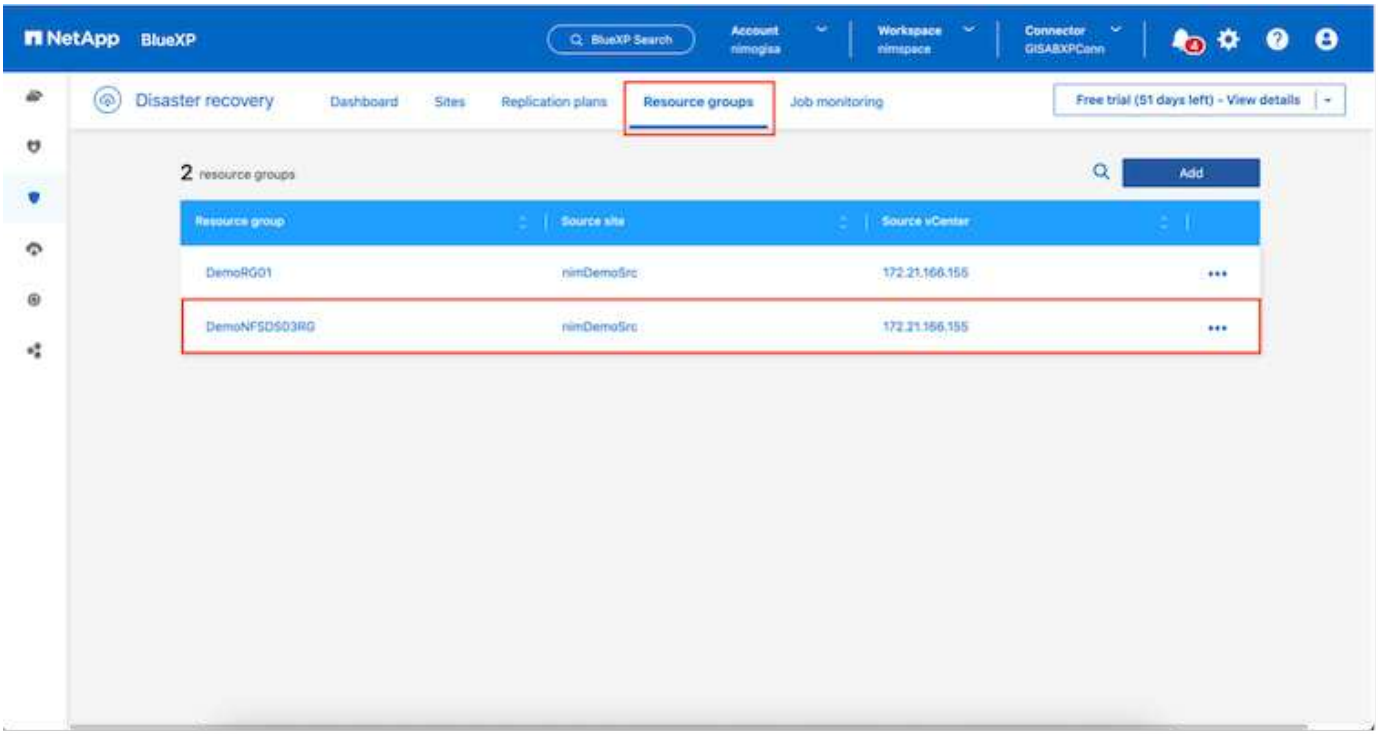
Dopo aver aggiunto i siti di origine e di destinazione, Disaster Recovery esegue automaticamente un rilevamento approfondito e visualizza le macchine virtuali insieme ai metadati associati. Disaster Recovery rileva inoltre automaticamente le reti e i gruppi di porte utilizzati dalle macchine virtuali e li compila.



Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse di Disaster

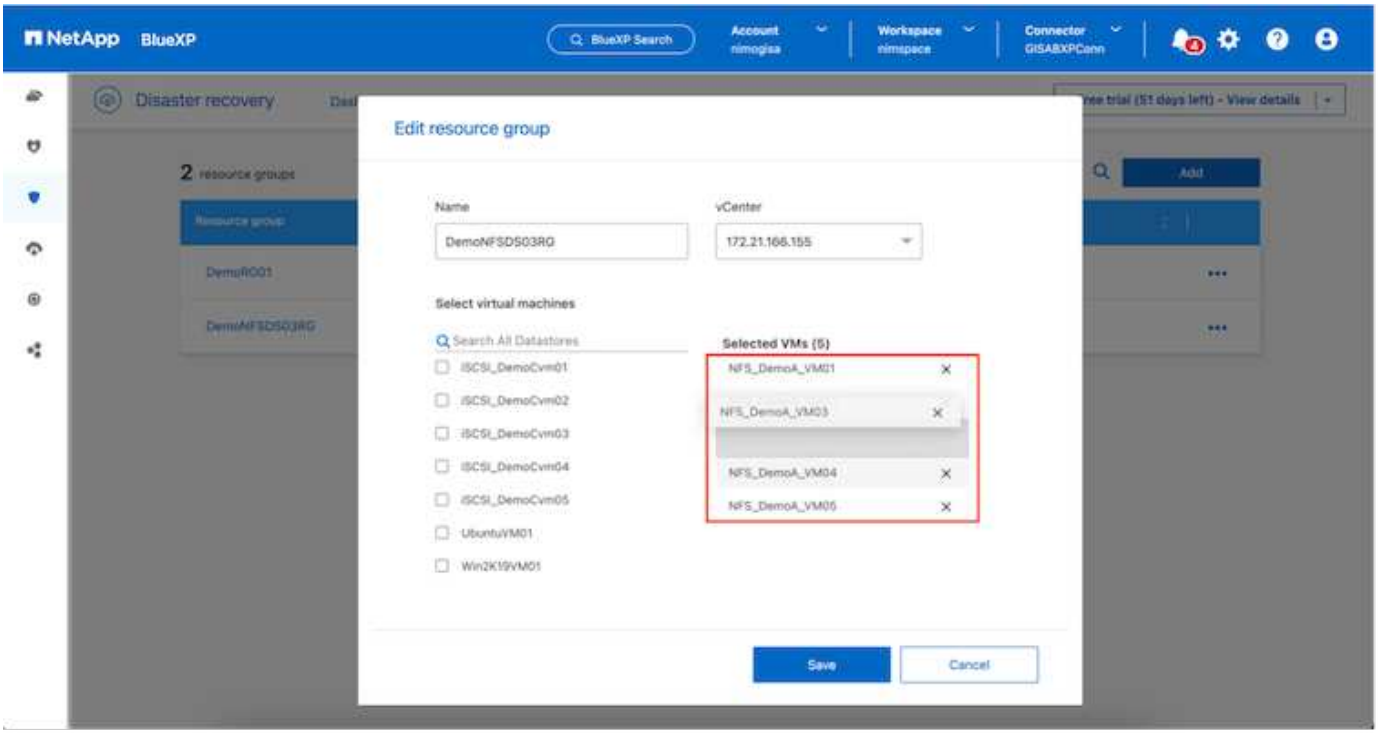
Recovery ti consentono di raggruppare un insieme di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti durante il ripristino. Per iniziare a creare gruppi di risorse, vai a **Resource Groups** e fai clic su **Create New Resource Group**.



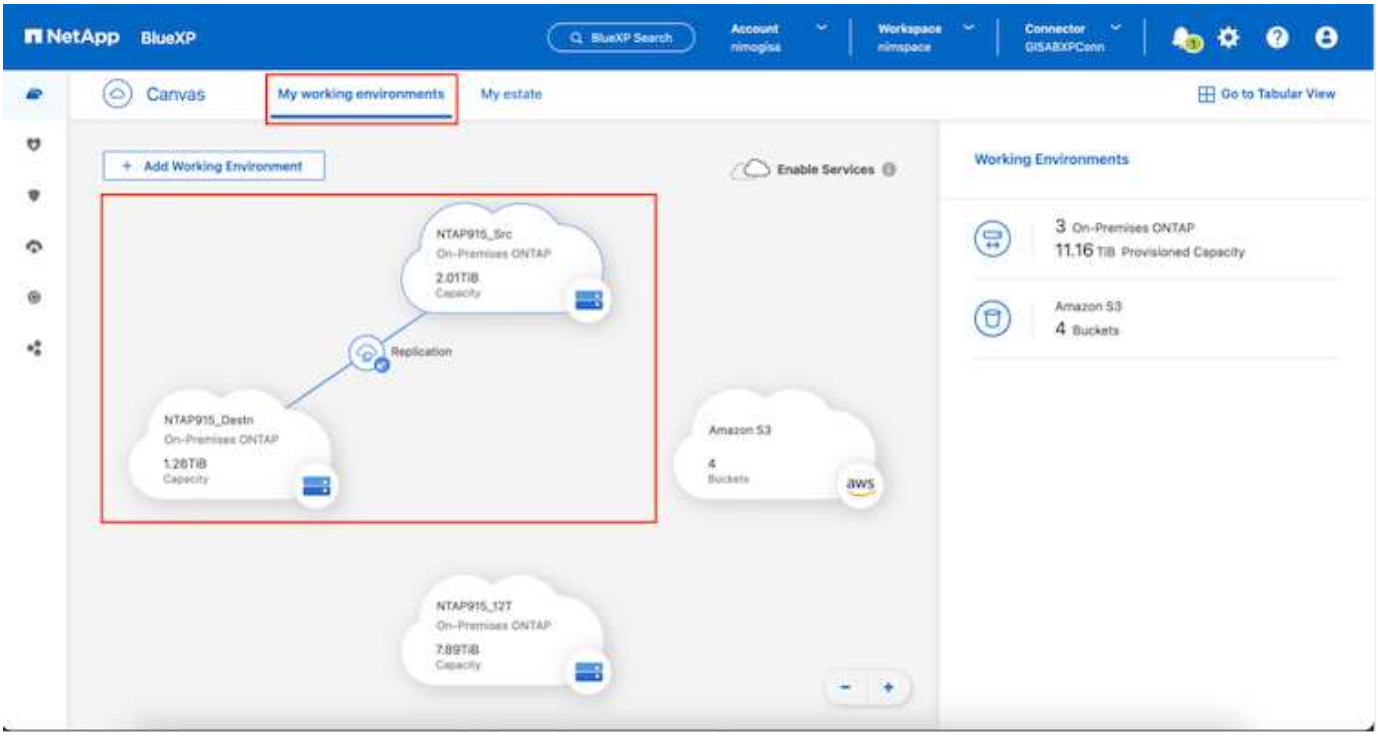


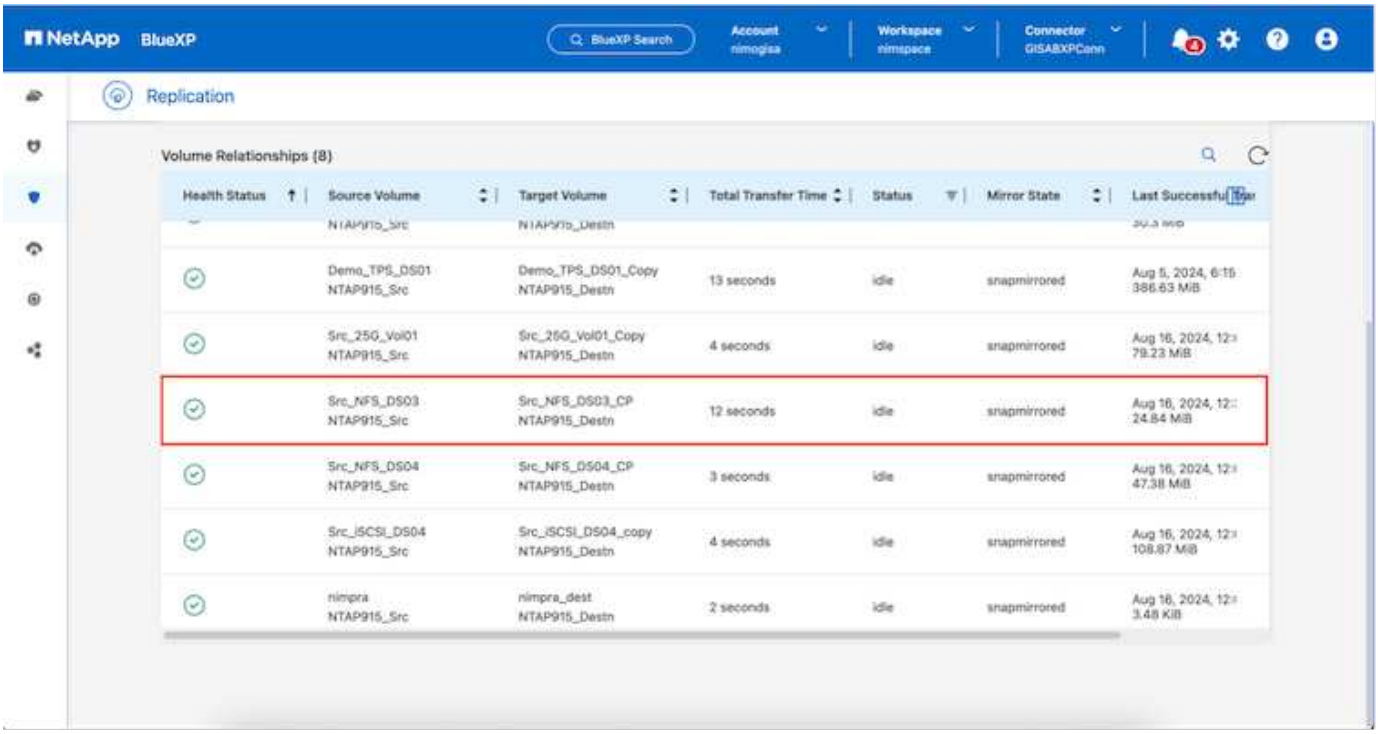
Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento della selezione.



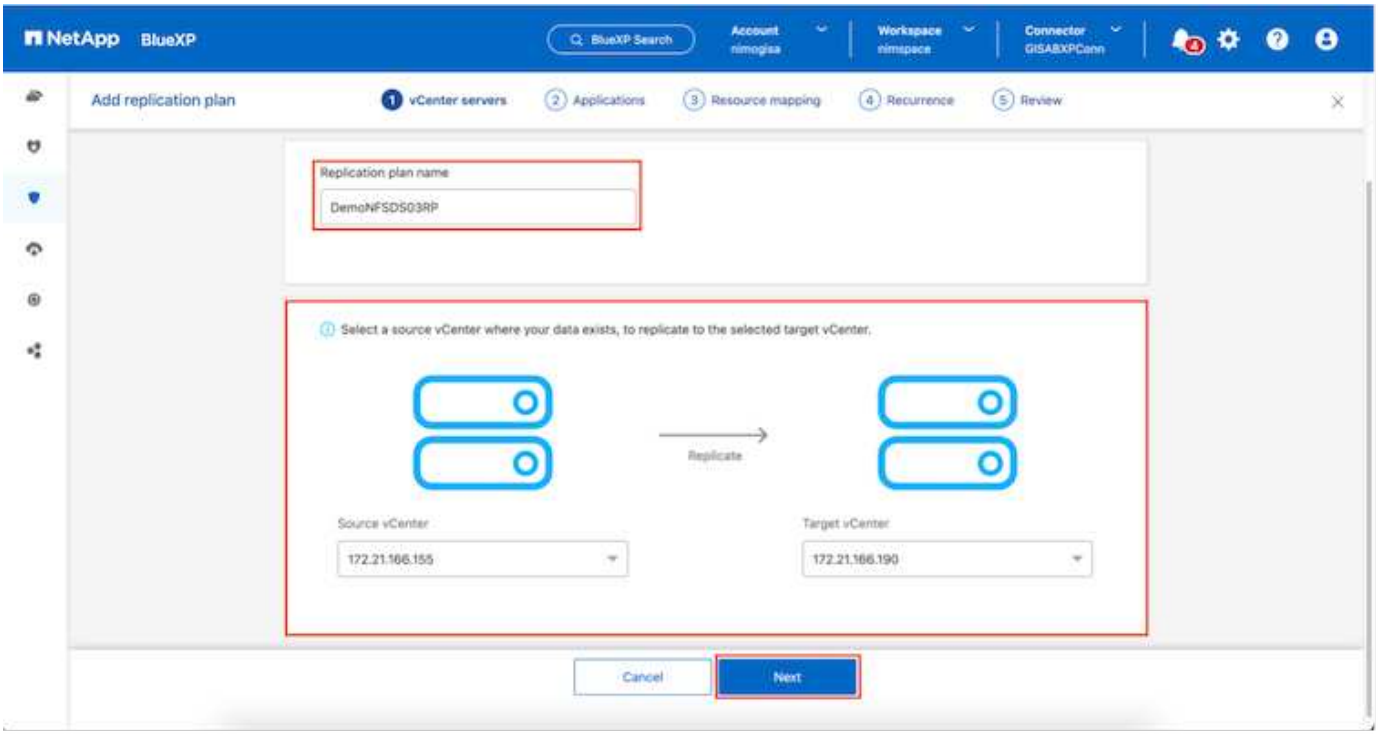
Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.





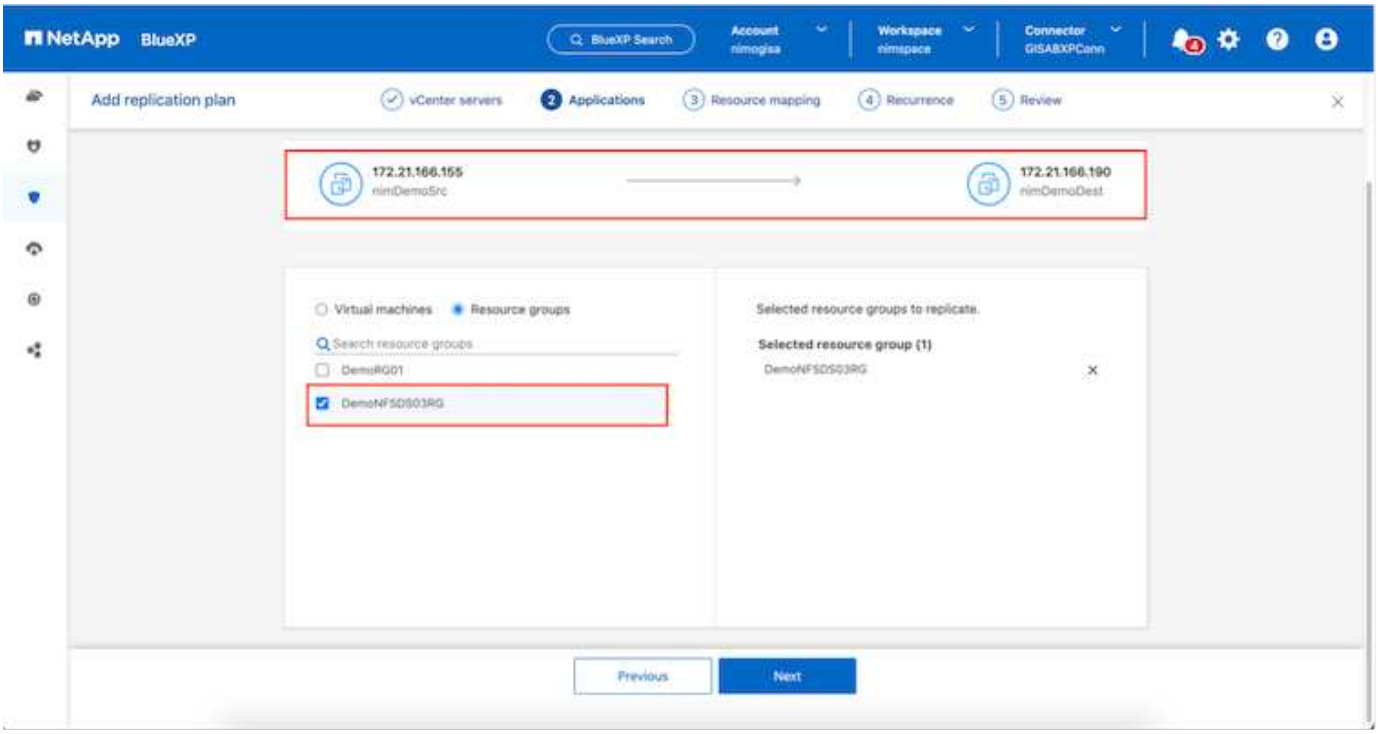
Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Aggiungi piano**.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono

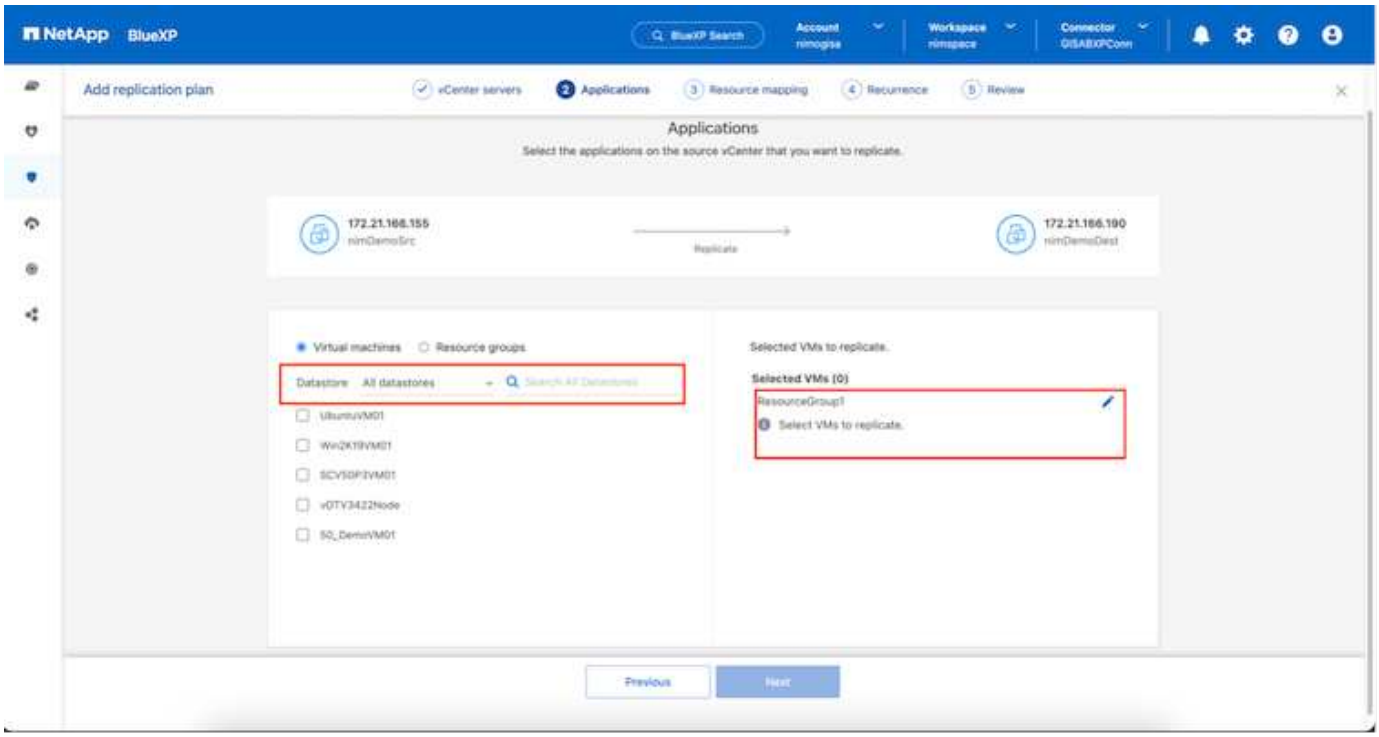
essere ripristinate le macchine virtuali delle applicazioni.



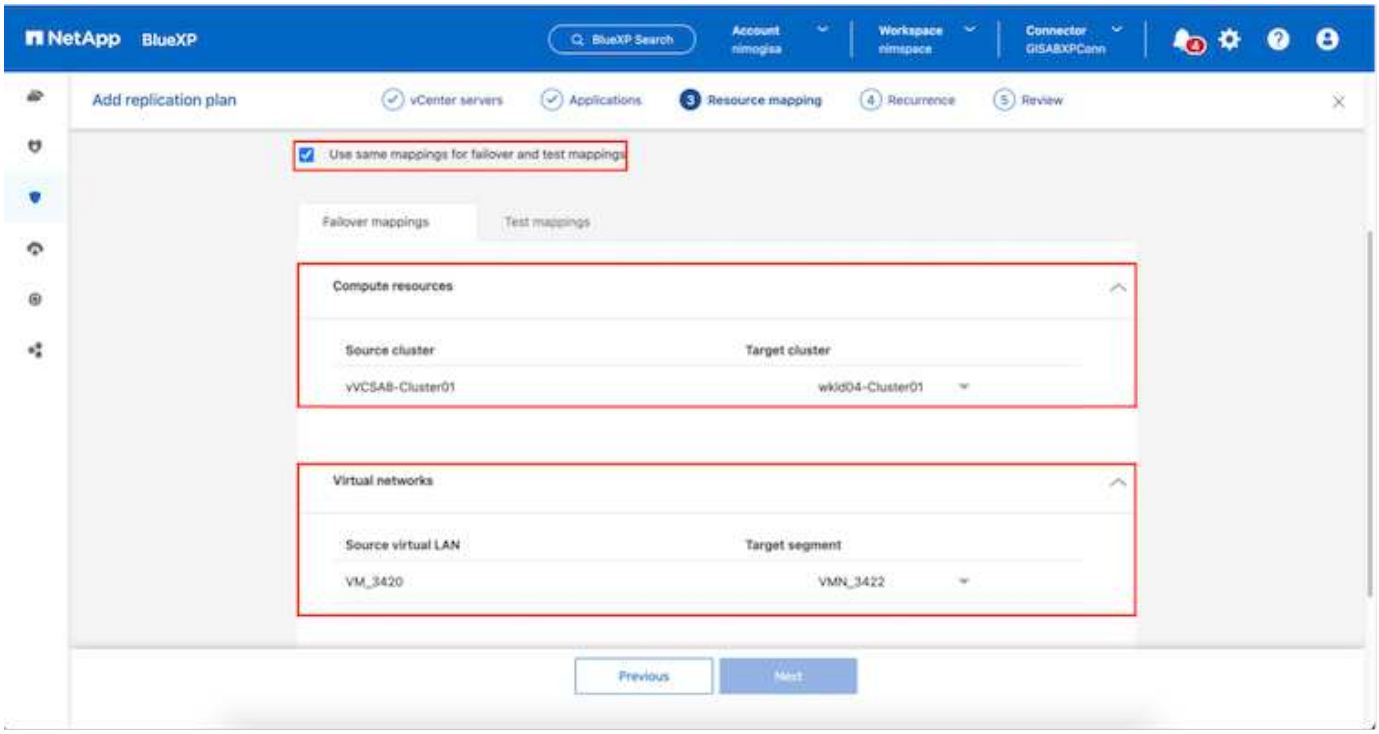
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Vengono avviati in parallelo due gruppi di risorse.

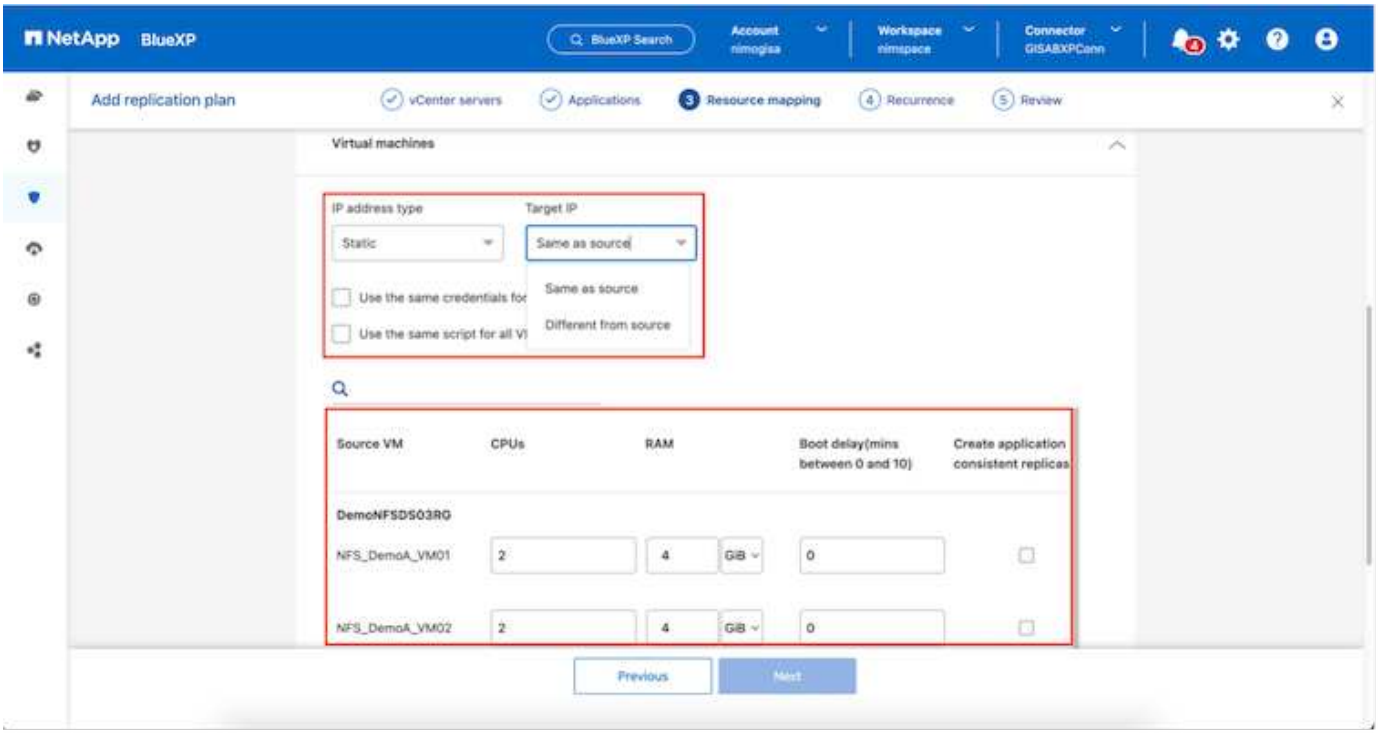
La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



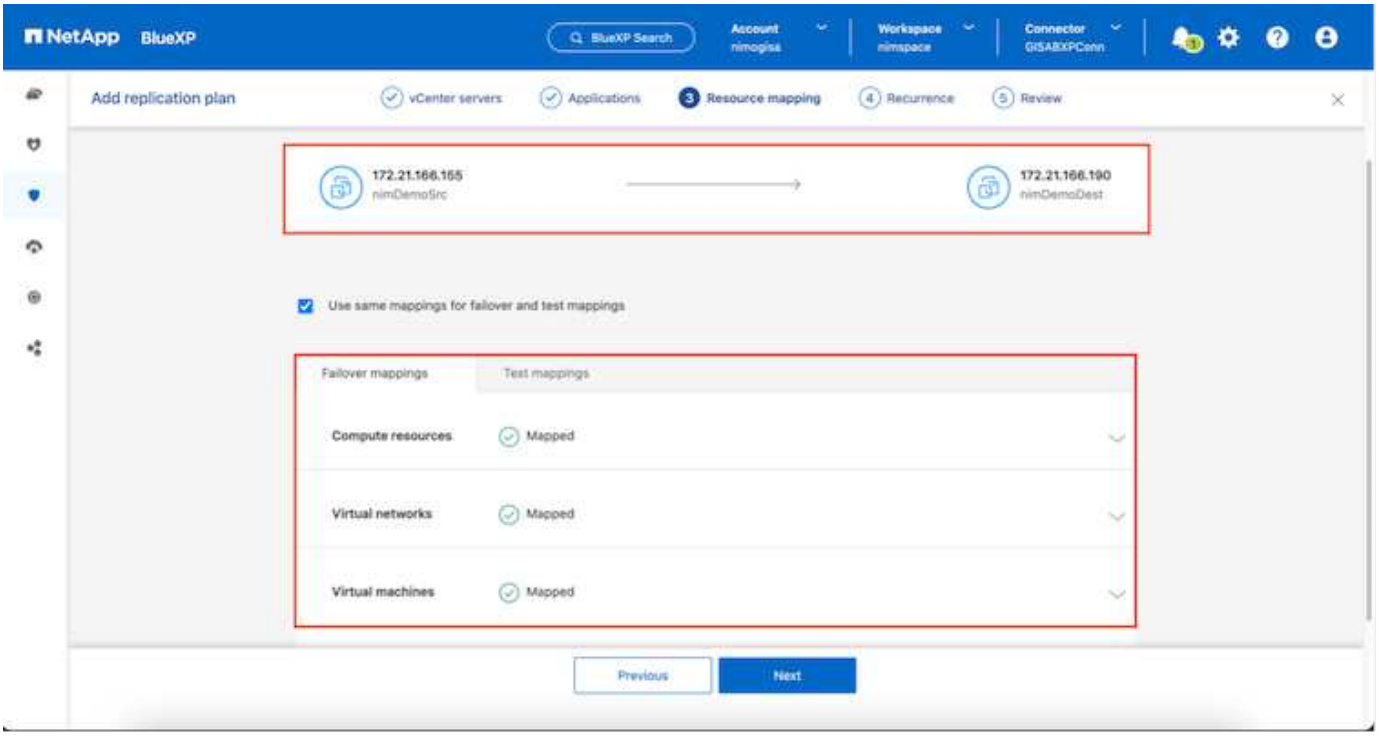
Una volta selezionati i gruppi di risorse, crea le mappature di failover. In questa fase, specifica come le risorse dell'ambiente di origine vengono mappate nella destinazione. Ciò include risorse di calcolo e reti virtuali. La personalizzazione IP, gli script pre e post, i ritardi di avvio, la coerenza delle applicazioni e così via. Per informazioni dettagliate, consulta "Creare un piano di replicazione".



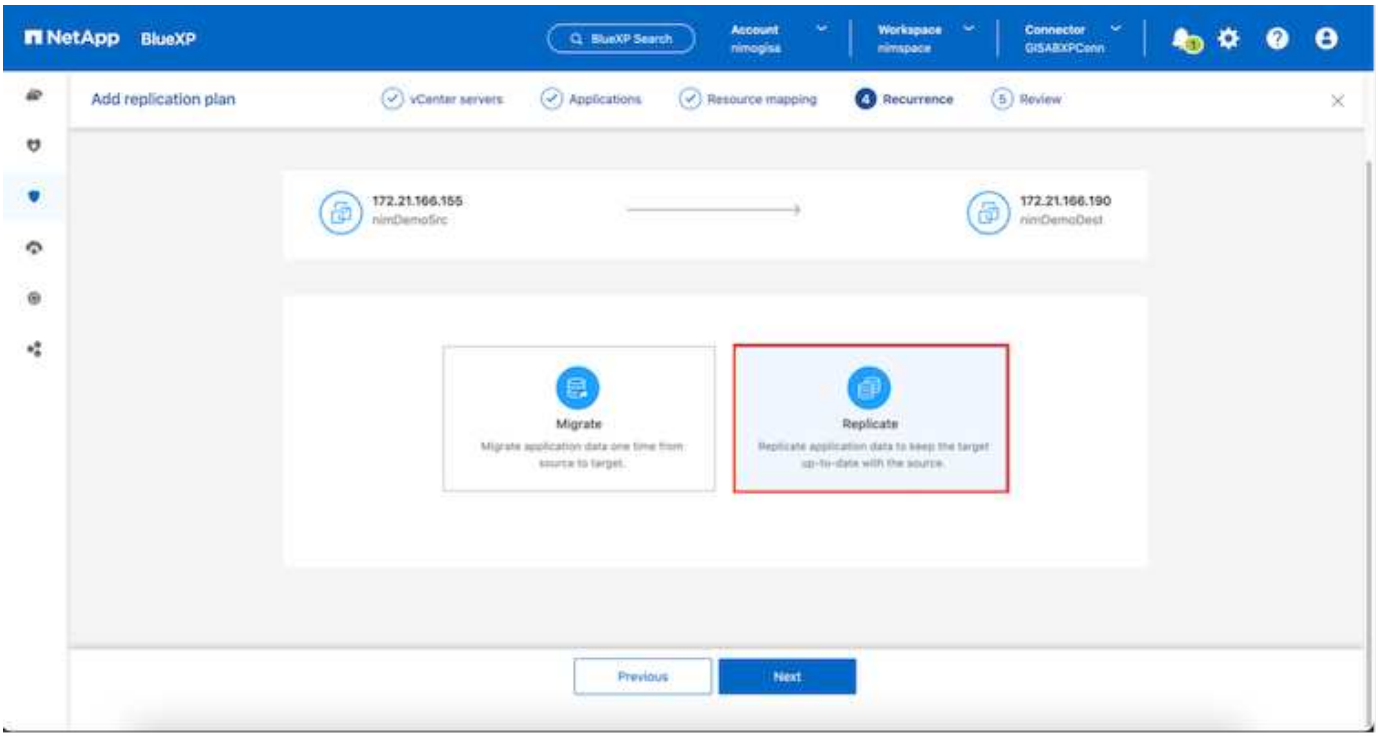
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per impostare diverse mappature per l'ambiente di test, selezionare l'opzione Mappatura test dopo aver deselezionato la casella di controllo come mostrato di seguito:



Una volta completata la mappatura delle risorse, fare clic su Avanti.

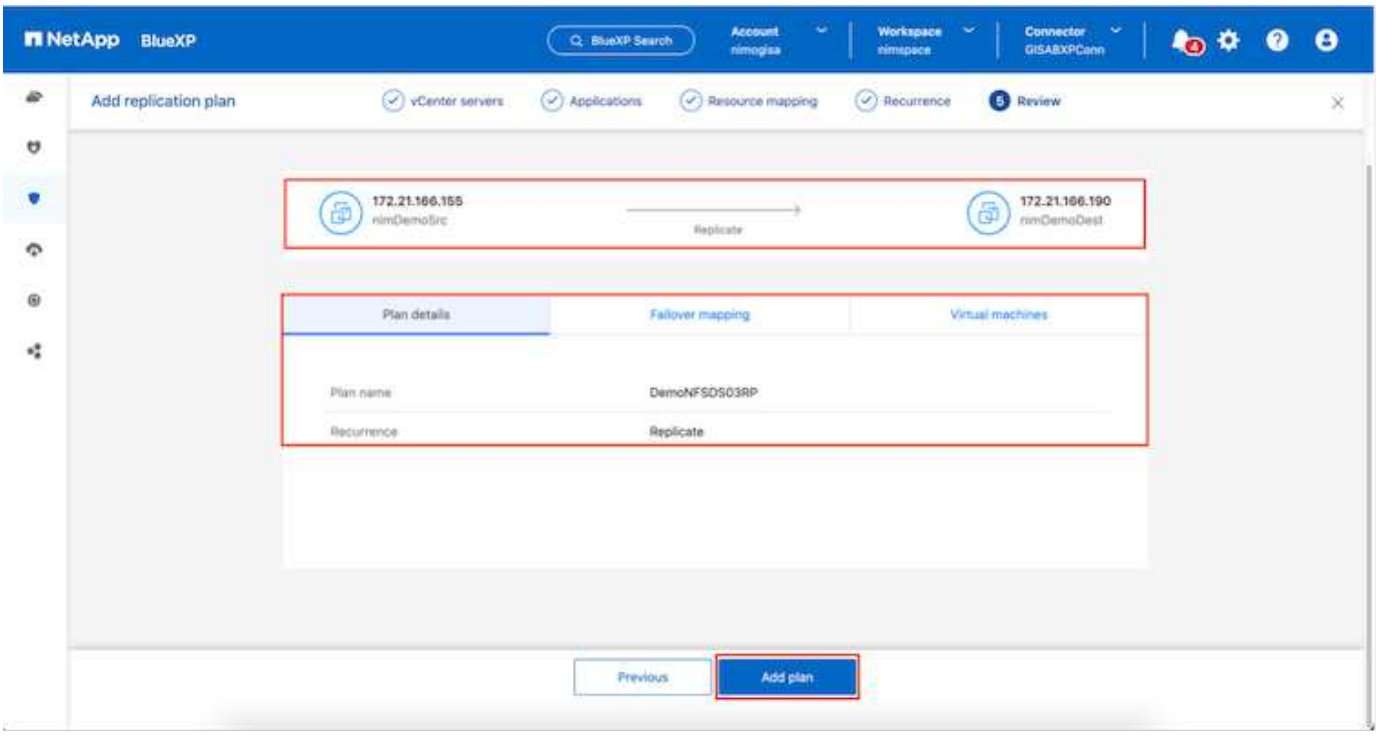


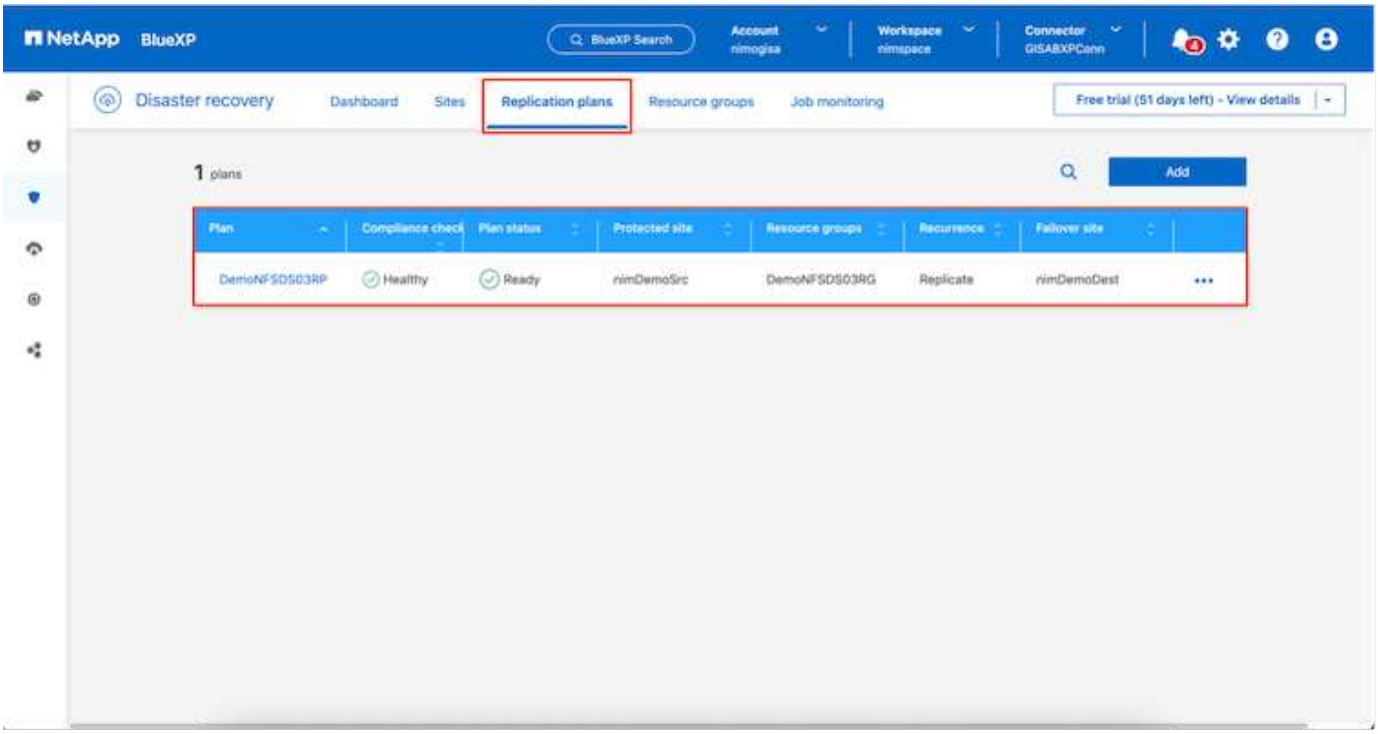
Selezionare il tipo di ricorrenza. In parole semplici, seleziona l'opzione Migra (migrazione una tantum tramite failover) o replica continua ricorrente. In questa procedura dettagliata è selezionata l'opzione Replica.



Una volta fatto, rivedi le mappature create e poi clicca su **Aggiungi piano**.

Le macchine virtuali (VM) provenienti da volumi e SVM diversi possono essere incluse in un piano di replica. A seconda del posizionamento delle VM (che si trovino sullo stesso volume o su volumi separati all'interno dello stesso SVM, oppure su volumi separati in SVM diversi), Disaster Recovery crea uno Snapshot del gruppo di coerenza.



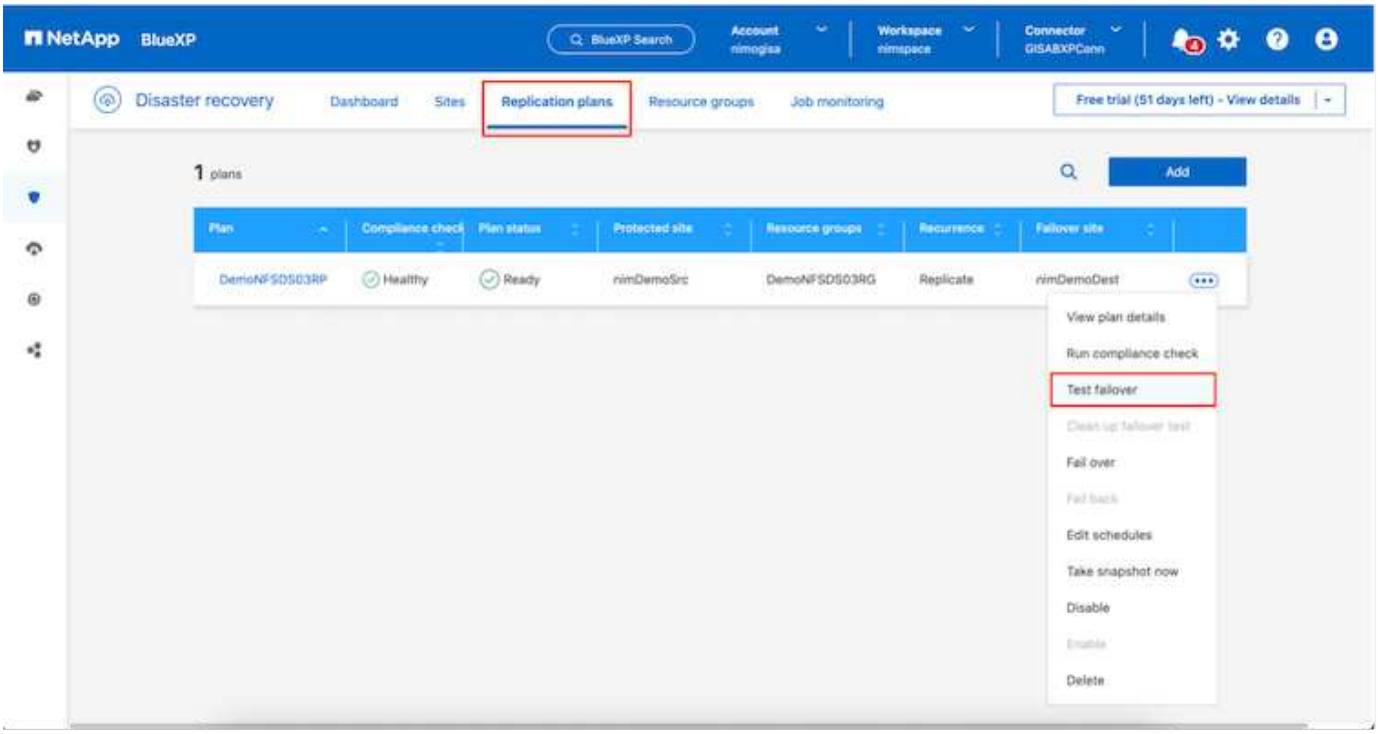


Il disaster recovery comprende i seguenti flussi di lavoro:

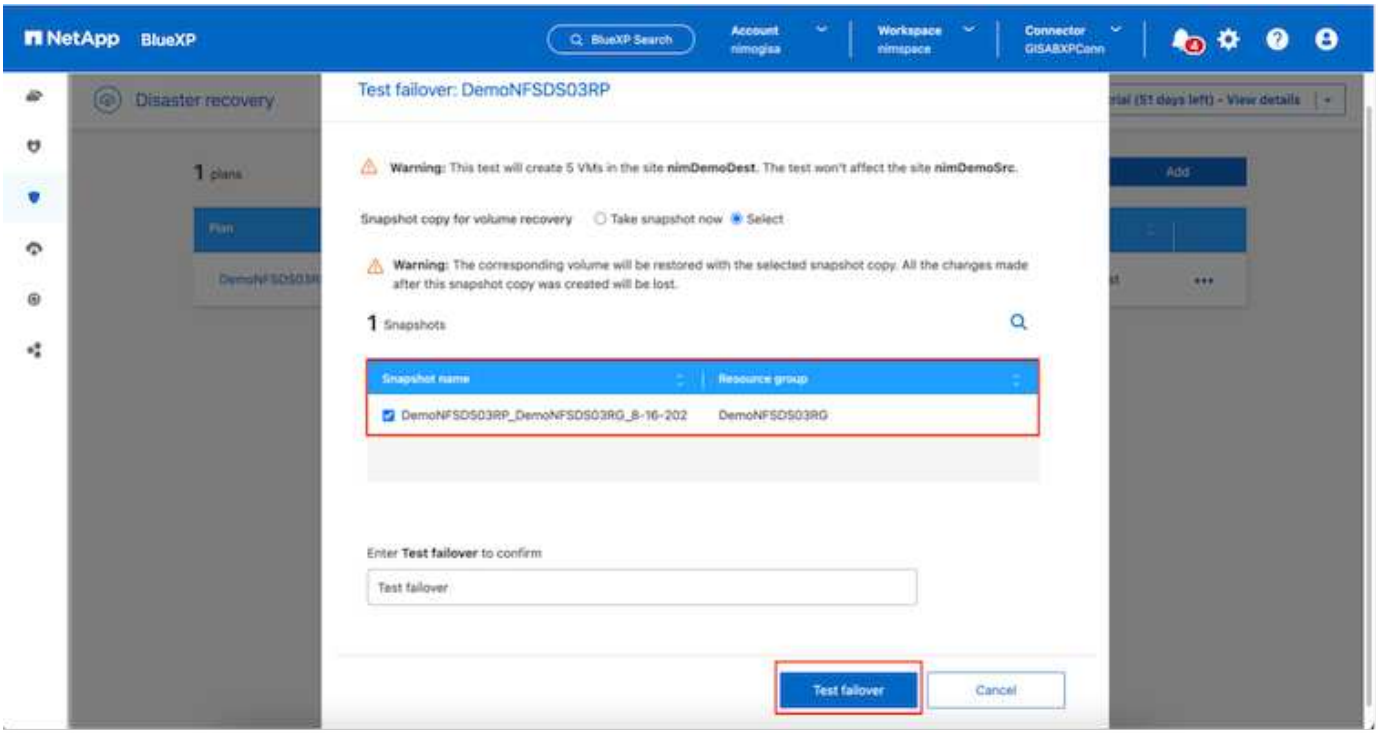
- Failover di test (incluse simulazioni automatiche periodiche)
- Test di failover di pulizia
- Failover
- Rifasamento

Failover di prova

Il test di failover in Disaster Recovery è una procedura operativa che consente agli amministratori VMware di convalidare completamente i loro piani di recovery senza interrompere gli ambienti di produzione. Durante un test di failover, Disaster Recovery crea copie NetApp FlexClone efficienti in termini di spazio dei volumi datastore NFS replicati sul sistema storage di DR. Questi volumi FlexClone vengono quindi montati sugli host ESXi nel sito di DR e le VM vengono avviate in una rete di test isolata. Questo processo consente agli amministratori di verificare che i loro piani di disaster recovery funzioneranno come previsto in caso di un disastro reale.



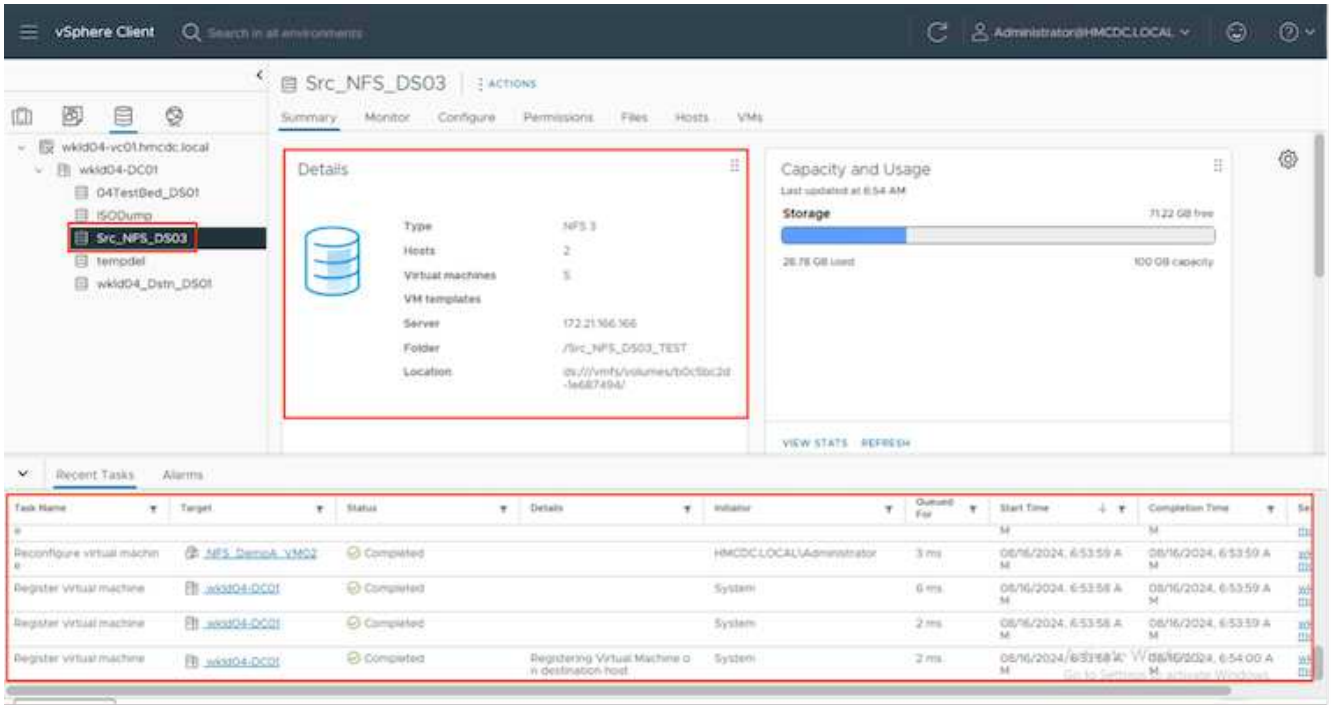
La funzionalità di Disaster Recovery include la possibilità di selezionare lo Snapshot come opzione facoltativa nell'operazione di failover di test. Questa funzionalità consente all'amministratore VMware di verificare che tutte le modifiche apportate di recente nell'ambiente siano replicate al sito di destinazione e siano quindi presenti durante il test. Tali modifiche includono le patch al sistema operativo guest della VM



Quando l'amministratore VMware esegue un'operazione di failover di prova, Disaster Recovery automatizza le seguenti attività:

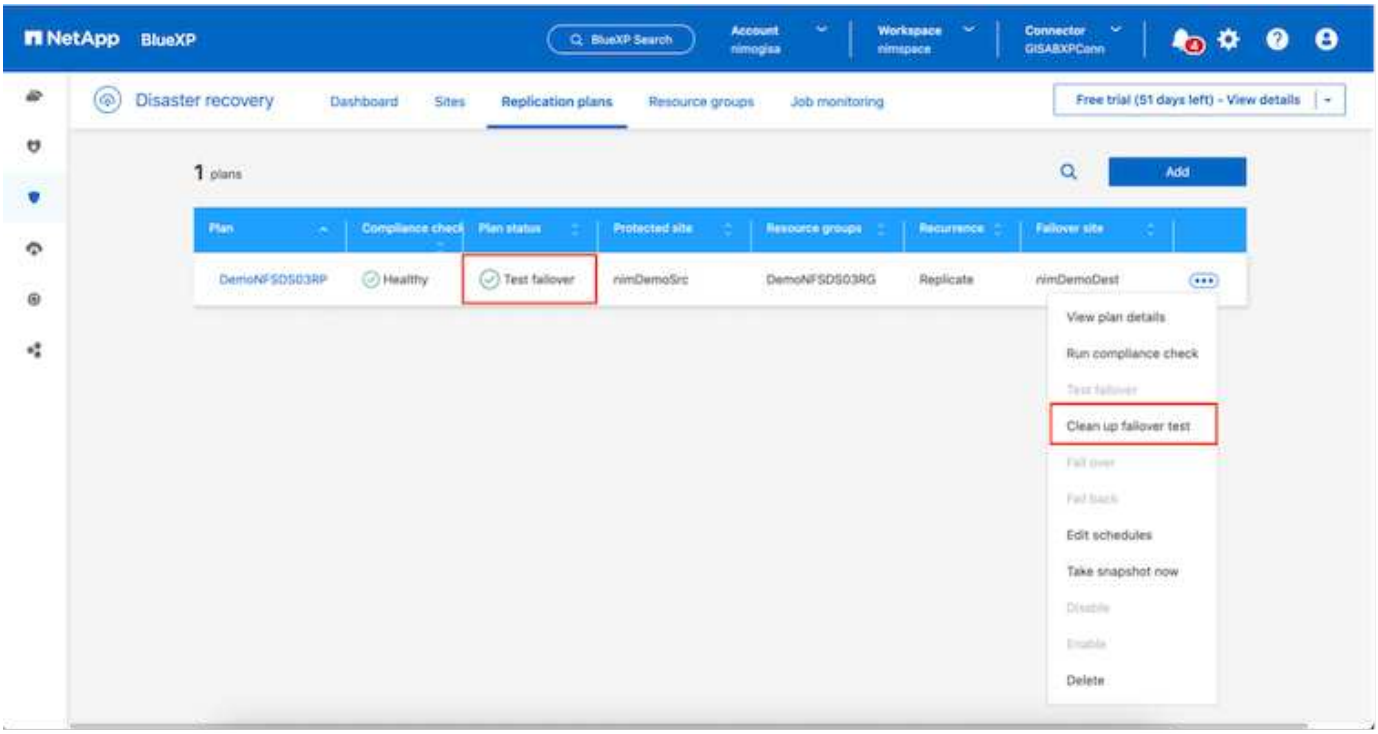
- Attivazione delle relazioni SnapMirror per aggiornare l'archiviazione nel sito di destinazione con tutte le modifiche recenti apportate nel sito di produzione.

- Creazione di volumi NetApp FlexClone dei volumi FlexVol sull'array di archiviazione DR.
- Collegamento dei datastore NFS nei volumi FlexClone agli host ESXi nel sito DR.
- Collegamento degli adattatori di rete della VM alla rete di prova specificata durante la mappatura.
- Riconfigurazione delle impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito DR.
- Esecuzione di tutti i comandi personalizzati memorizzati nel piano di replicazione.
- Accensione delle VM nell'ordine definito nel piano di replica.



Operazione di test di failover di pulizia

L'operazione di test di failover di pulizia avviene dopo il completamento del test del piano di replica e quando l'amministratore VMware risponde al prompt di pulizia.



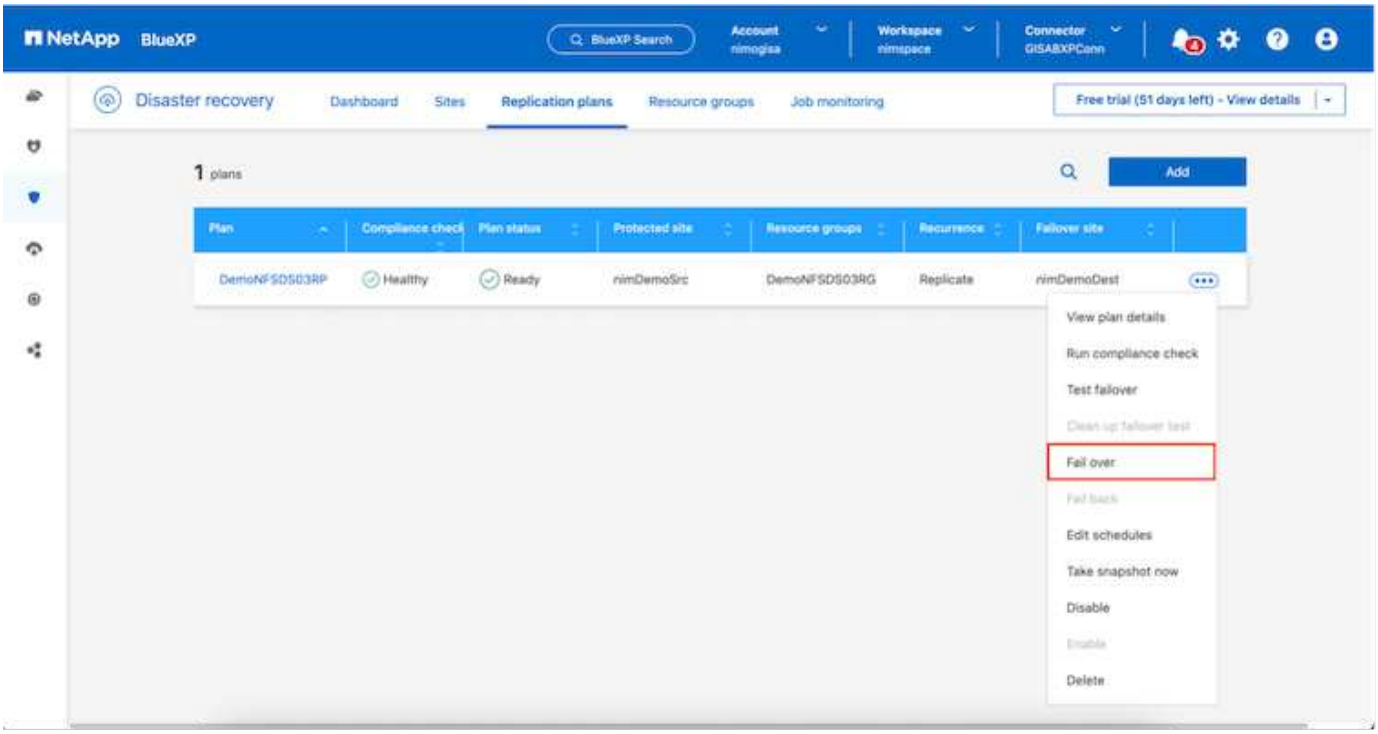
Questa azione reimposterà le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto.

Quando l'amministratore VMware esegue un'operazione di ripristino, Disaster Recovery completa il seguente processo:

1. Spegne ogni VM recuperata nella copia FlexClone utilizzata per il test.
2. Elimina il volume FlexClone utilizzato per presentare le VM recuperate durante il test.

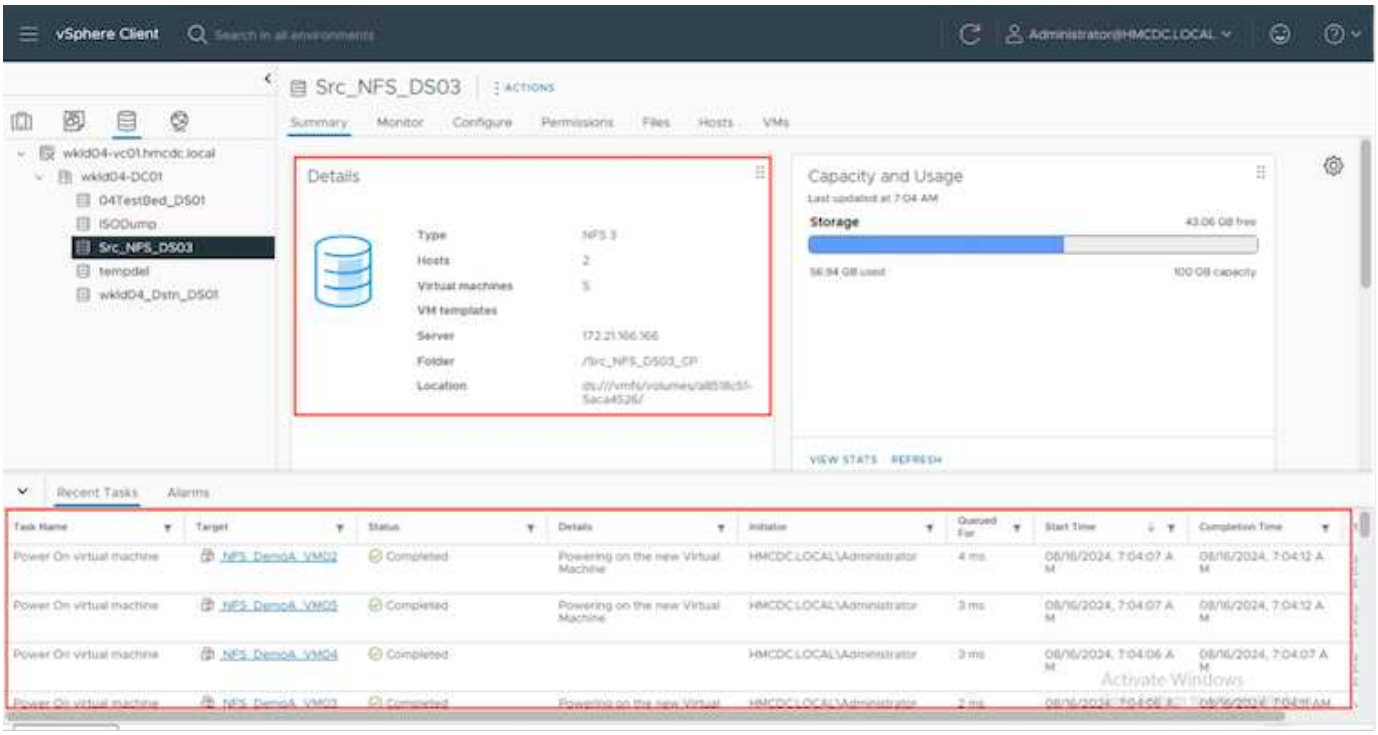
Migrazione pianificata e failover

Il Disaster Recovery prevede due metodi per eseguire un failover effettivo: la migrazione pianificata e il failover. Il primo metodo, la migrazione pianificata, include l'arresto delle VM e la sincronizzazione della replica dello storage nel processo per ripristinare o spostare efficacemente le VM nel sito di destinazione. La migrazione pianificata richiede l'accesso al sito di origine. Il secondo metodo, il failover, è un failover pianificato/non pianificato in cui le VM vengono ripristinate nel sito di destinazione dall'ultimo intervallo di replica dello storage che è stato completato con successo. A seconda del RPO definito nella soluzione, è prevedibile una certa perdita di dati nello scenario di Disaster Recovery.



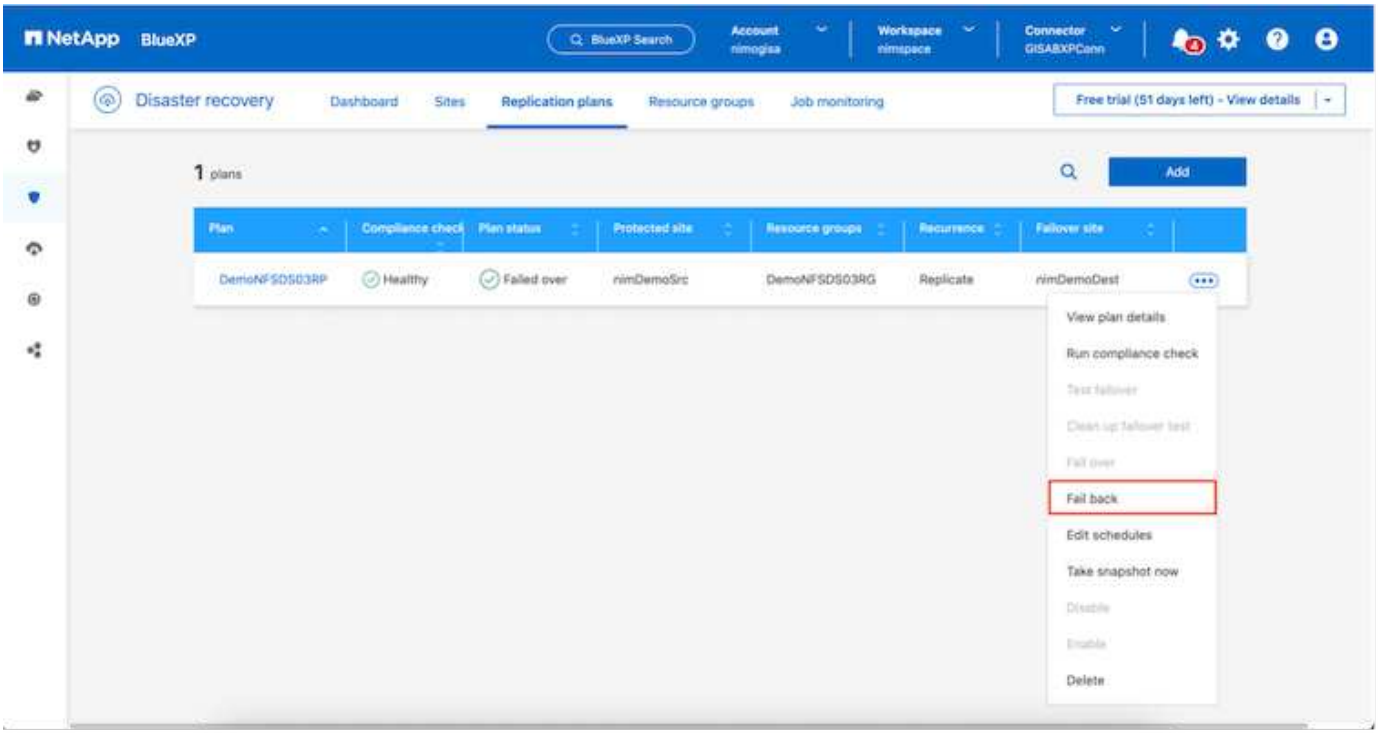
Quando l'amministratore VMware esegue un'operazione di failover, Disaster Recovery automatizza le seguenti attività:

- Interrompere ed eseguire il failover delle relazioni NetApp SnapMirror .
- Collegare i datastore NFS replicati agli host ESXi nel sito DR.
- Collegare gli adattatori di rete della VM alla rete del sito di destinazione appropriata.
- Riconfigurare le impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito di destinazione.
- Eseguire eventuali comandi personalizzati memorizzati nel piano di replicazione.
- Accendere le VM nell'ordine definito nel piano di replica.



Rifasamento

Un failback è una procedura facoltativa che ripristina la configurazione originale dei siti di origine e di destinazione dopo un ripristino.



Gli amministratori VMware possono configurare ed eseguire una procedura di failback quando sono pronti a ripristinare i servizi sul sito di origine.

NOTA: Disaster Recovery replica (risincronizza) tutte le modifiche sulla macchina virtuale di origine originale prima di invertire la direzione della replica. Questo processo inizia da una relazione che ha completato il

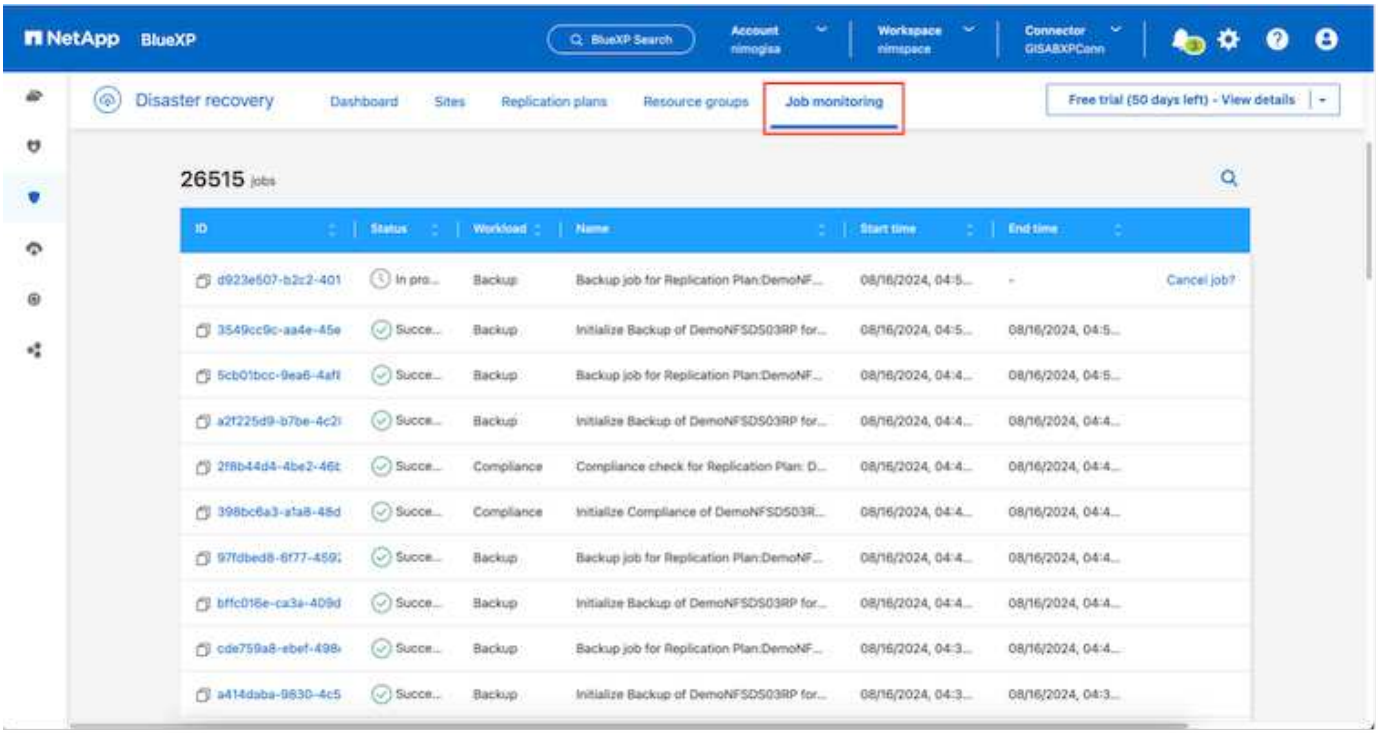
failover verso una destinazione e prevede i seguenti passaggi:

- Spegnere e annullare la registrazione delle macchine virtuali e dei volumi sul sito di destinazione.
- Interrompere la relazione SnapMirror sulla sorgente originale per renderla di lettura/scrittura.
- Risincronizzare la relazione SnapMirror per invertire la replica.
- Montare il volume sulla sorgente, accendere e registrare le macchine virtuali di origine.

Per ulteriori dettagli su come accedere e configurare Disaster Recovery, consulta la documentazione "Scopri NetApp Disaster Recovery for VMware".

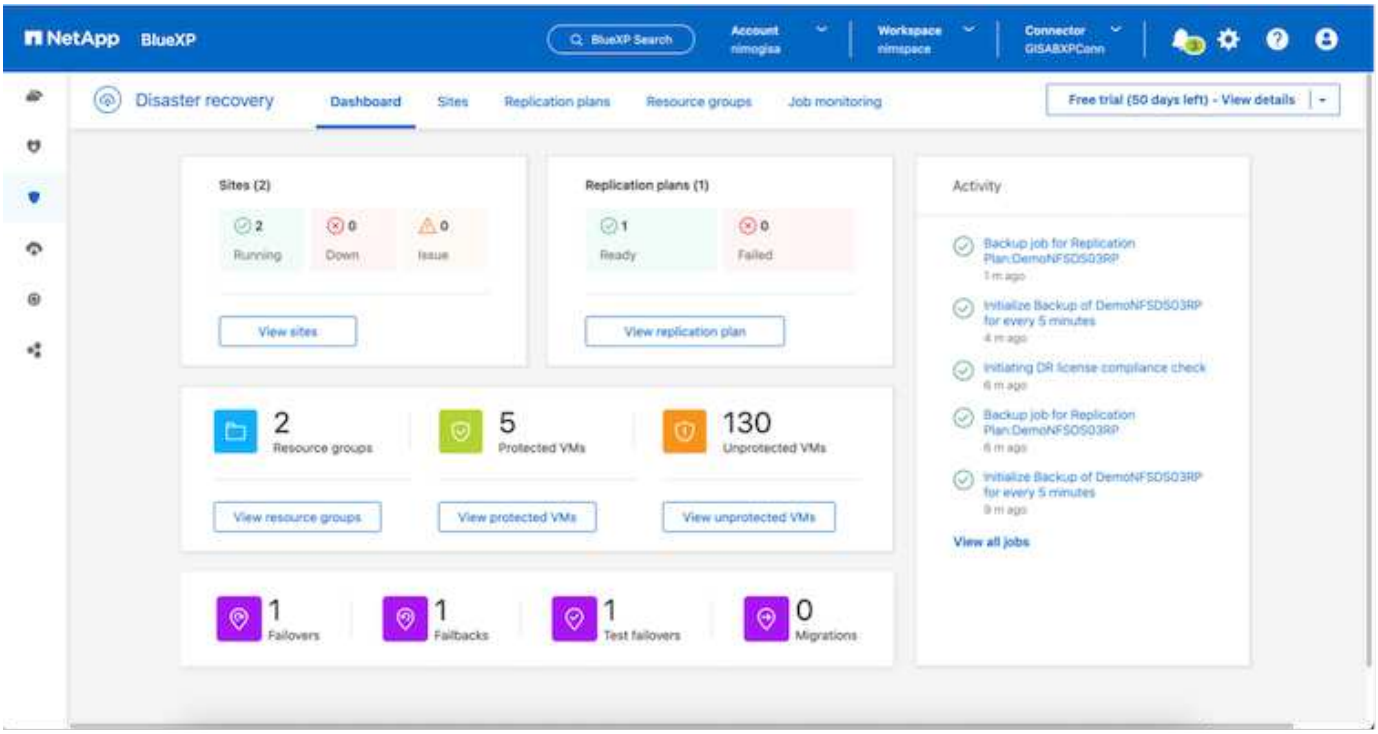
Monitoraggio e dashboard

Da Console o da ONTAP CLI, puoi monitorare lo stato di integrità della replica per i volumi datastore appropriati e tenere traccia dello stato di un failover o di un failover di test tramite Job Monitoring.



Se un lavoro è in corso o in coda e si desidera interromperlo, è disponibile un'opzione per annullarlo.

Con la dashboard di disaster recovery, puoi valutare con sicurezza lo stato dei siti di disaster recovery e dei piani di replica. Questo ti consente di identificare rapidamente siti e piani integri, disconnessi o degradati.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il"simulatore di soluzioni" .

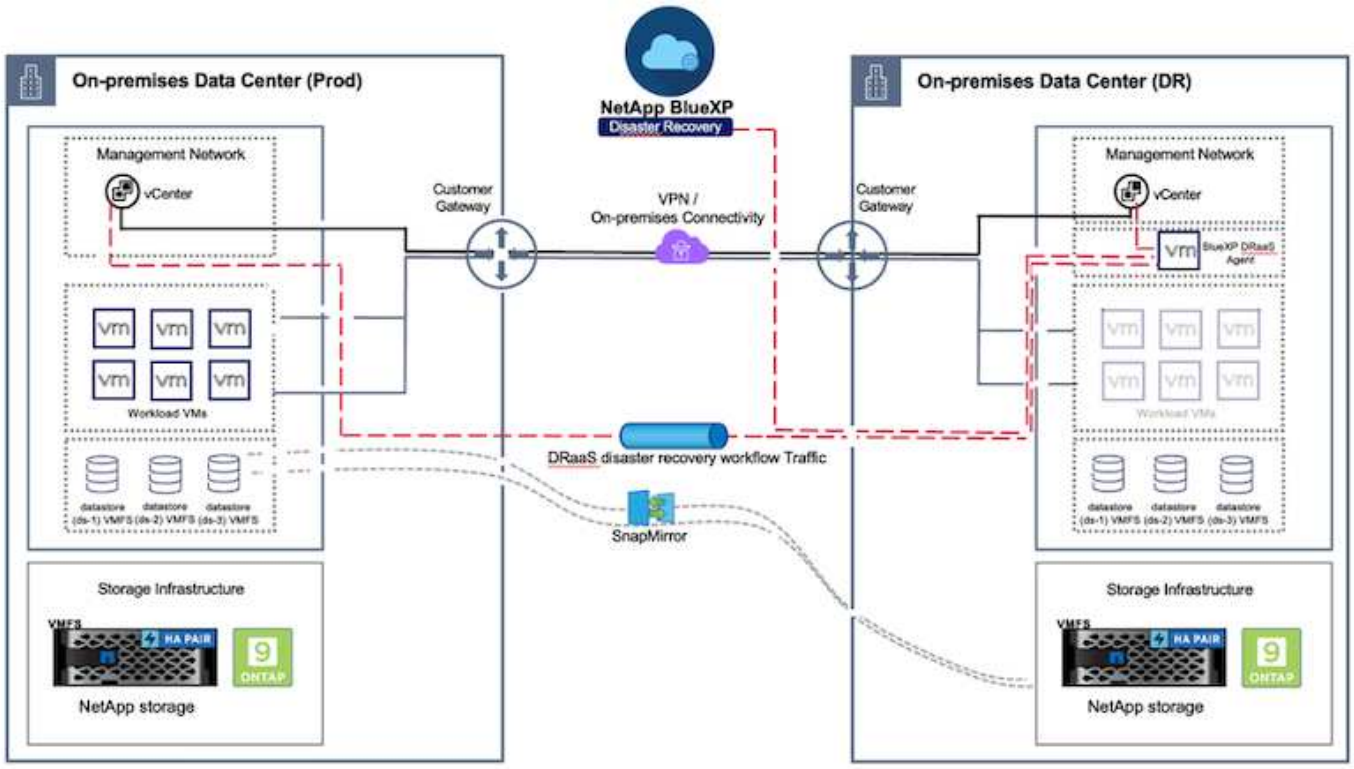
NetApp Disaster Recovery per datastore VMFS

Il disaster recovery mediante replica a livello di blocco dal sito di produzione al sito di disaster recovery è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Con la replica NetApp SnapMirror , i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali che utilizzano datastore VMFS possono essere replicati su un altro sistema di storage ONTAP in un data center di ripristino designato in cui risiede VMware

Questa sezione del documento descrive la configurazione di NetApp Diaster Recovery per impostare il disaster recovery delle VM VMware on-premises su un altro sito designato. Come parte di questa configurazione, Console agent, onboarding degli array ONTAP, definizione dei siti e associazione di VMware vCenter. Inoltre, questo documento descrive in dettaglio come configurare la replica tra i siti e come impostare e testare un piano di recovery. L'ultima sezione contiene istruzioni per eseguire un failover completo del sito e come eseguire il failback quando il sito primario viene ripristinato e riportato online.

Utilizzando Disaster Recovery, parte di NetApp Data Services, puoi individuare i tuoi vCenters VMware on-premises insieme allo storage ONTAP, creare gruppi di risorse, creare un piano di recovery, associarlo ai gruppi di risorse e testare o eseguire il failover e il failback. SnapMirror fornisce la replica a blocchi a livello di storage per mantenere aggiornati i due siti con modifiche incrementali, con un RPO fino a 5 minuti. È inoltre possibile simulare le procedure di DR come esercitazione regolare senza influire sui datastore di produzione e replicati né sostenere costi di storage aggiuntivi. NetApp Data Services sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore VMFS a partire dall'ultimo Snapshot replicato nel sito di DR. Una volta completato il test di DR, puoi semplicemente eliminare l'ambiente di test,

sempre senza alcun impatto sulle effettive risorse di produzione replicate. Quando è necessario un failover effettivo (pianificato o non pianificato), con pochi clic Disaster Recovery orchestrerà tutti i passaggi necessari per avviare automaticamente le macchine virtuali protette nel sito di disaster recovery designato. Il servizio invertirà anche la relazione di SnapMirror verso il sito primario e replicherà eventuali modifiche dal secondario al primario per un'operazione di failback, quando necessario. Tutto questo può essere ottenuto con una frazione del costo rispetto ad altre alternative ben note.

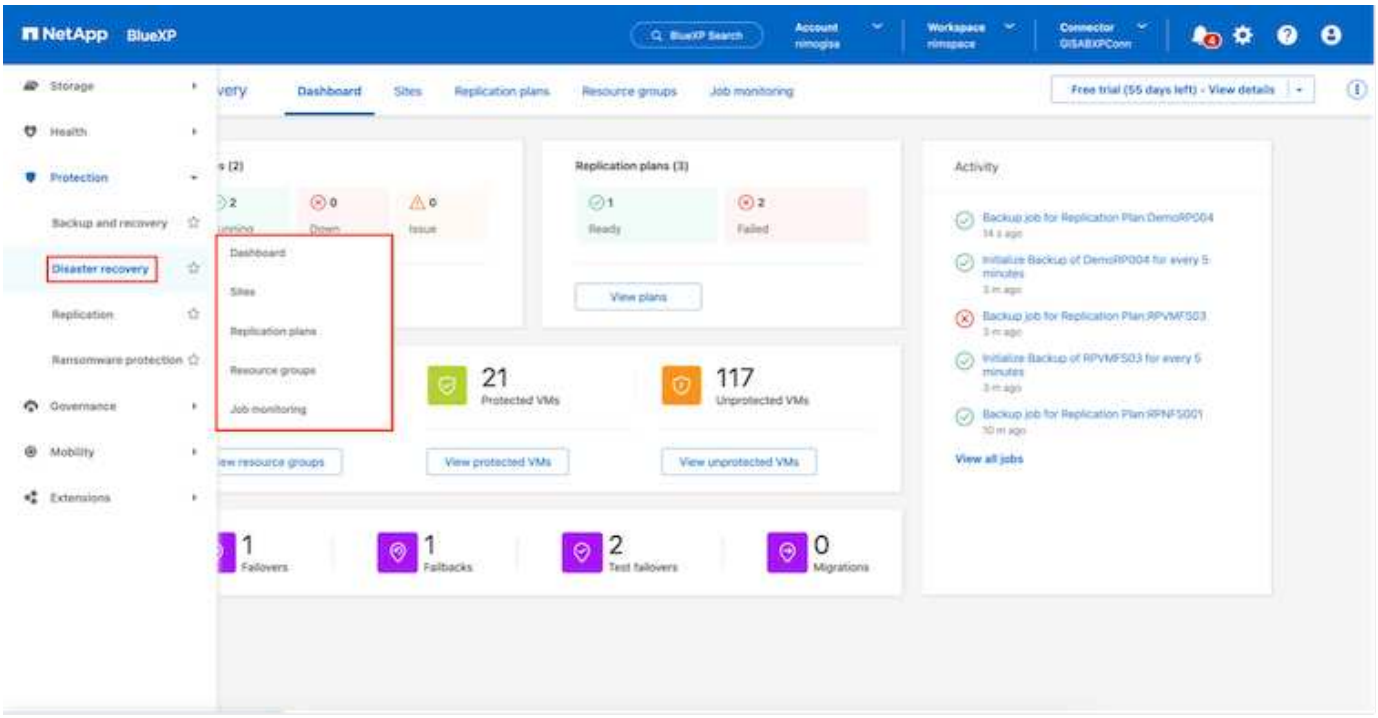


Per informazioni aggiornate e sulle versioni supportate di vCenter Server, ESXi e ONTAP per il Disaster Recovery, consulta "Configurazioni supportate per il disaster recovery".

Iniziare

Per iniziare a utilizzare Disaster Recovery, usa NetApp Console e poi accedi al servizio.

1. Accedi a Console.
2. Dal menu di navigazione a sinistra della Console, seleziona Protezione > Ripristino di emergenza.
3. Compare la Disaster Recovery Dashboard.

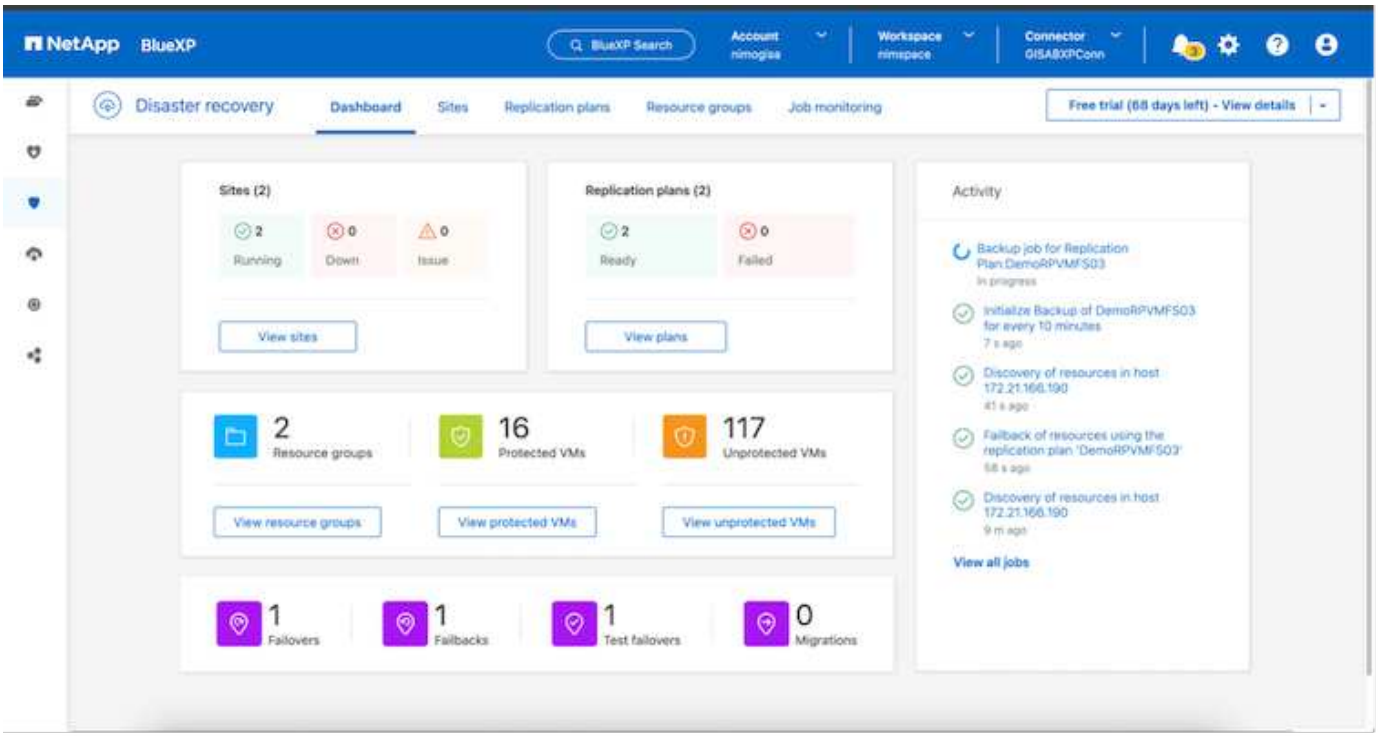


Prima di configurare il piano di disaster recovery, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Console agent è distribuito in AWS VPC.
- Le istanze dell'agente della console dispongono di connettività ai sistemi vCenter di origine e di destinazione e ai sistemi storage.
- In Console, aggiungi i sistemi di storage on-premises NetApp che ospitano datastore VMFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su VMFS designati.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere dai 3 ai 5 minuti.

NetApp consiglia di distribuire l'agente Console nel sito di disaster recovery o in un sito terzo, in modo che l'agente Console possa comunicare attraverso la rete con le risorse di origine e di destinazione durante interruzioni reali o calamità naturali.

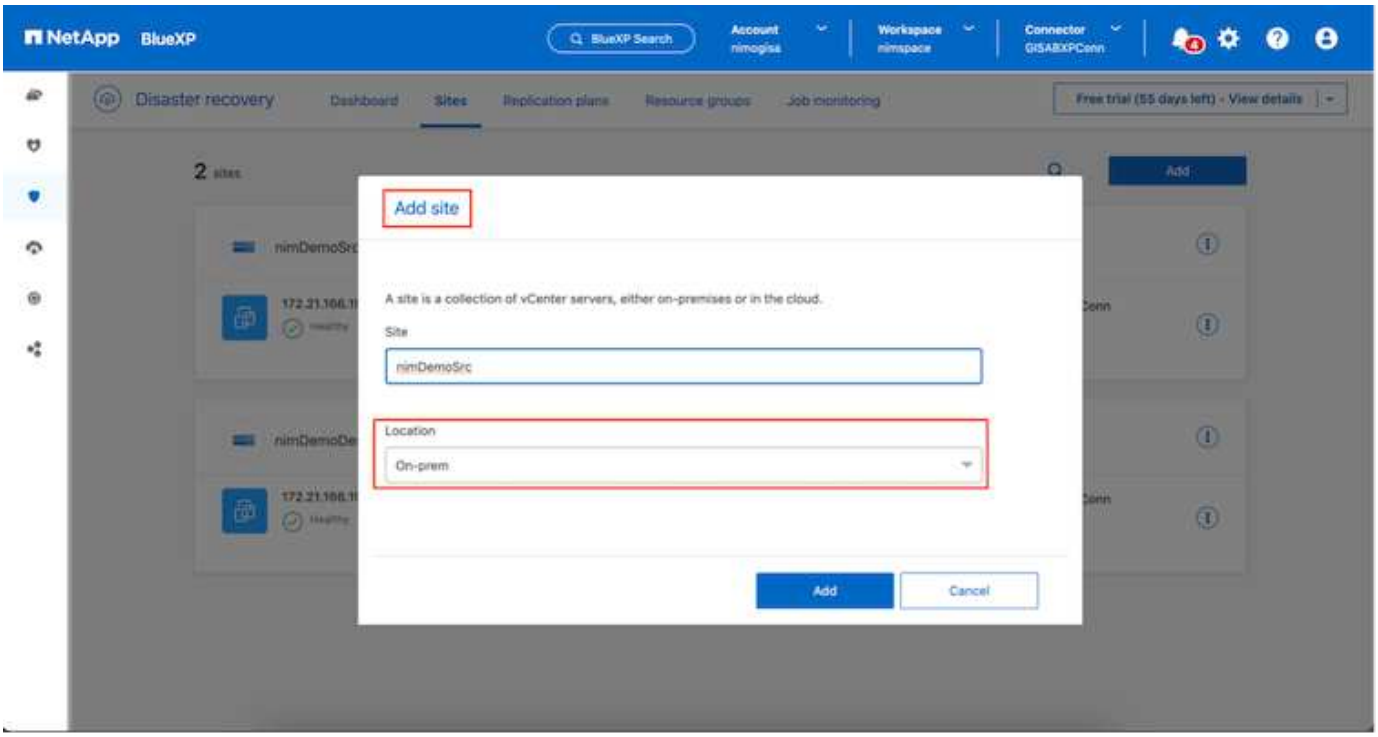


Al momento della stesura di questo documento, il supporto per i datastore VMFS da locale a locale è in fase di anteprima tecnologica. Questa funzionalità è supportata sia con i datastore VMFS basati sul protocollo FC che ISCSI.

Configurazione del disaster recovery

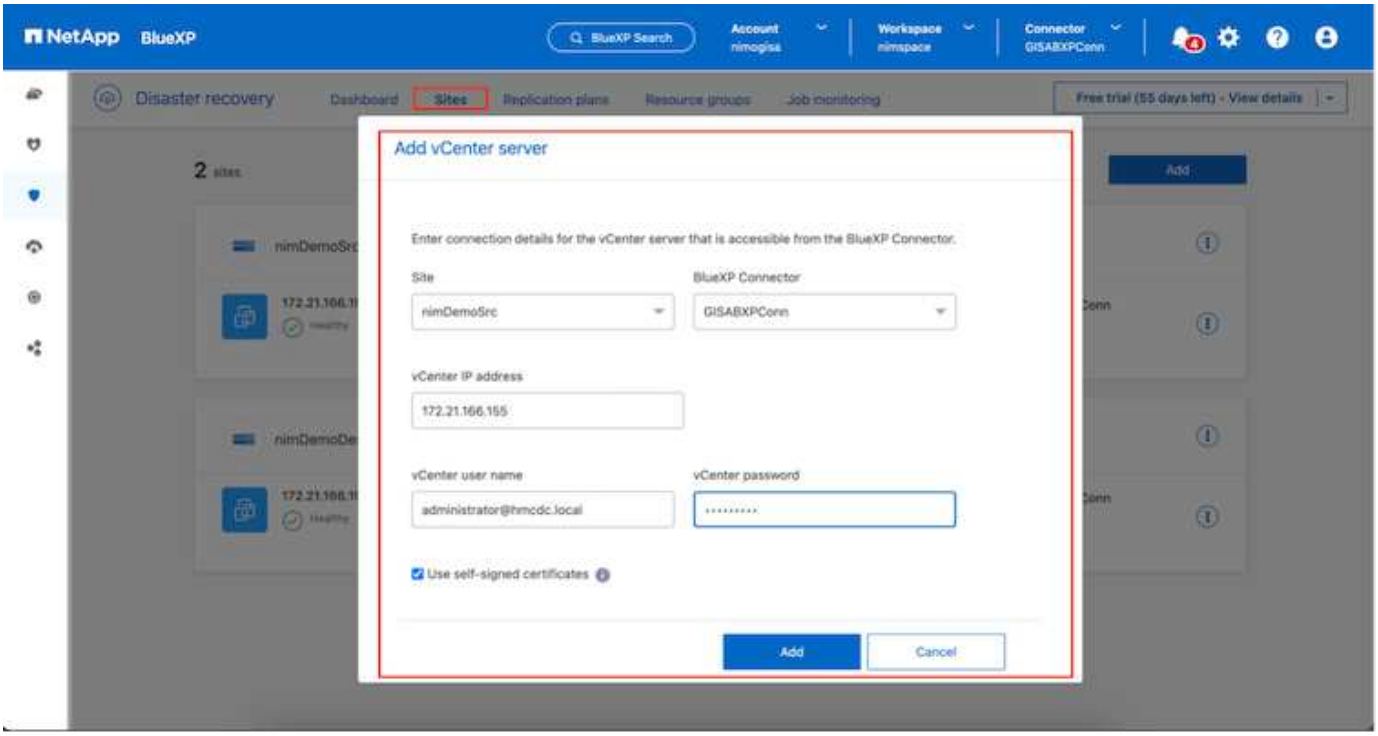
Il primo passo per prepararti al disaster recovery è individuare e aggiungere vCenter e le risorse di storage on-premises a Disaster Recovery.

Assicurati che i sistemi storage ONTAP siano aggiunti all'ambiente di lavoro nel canvas. Apri Console e seleziona **Protection > Disaster Recovery** nella navigazione a sinistra. Seleziona **Rileva server vCenter** oppure usa il menu in alto e seleziona **Sites > Add > Add vCenter**.

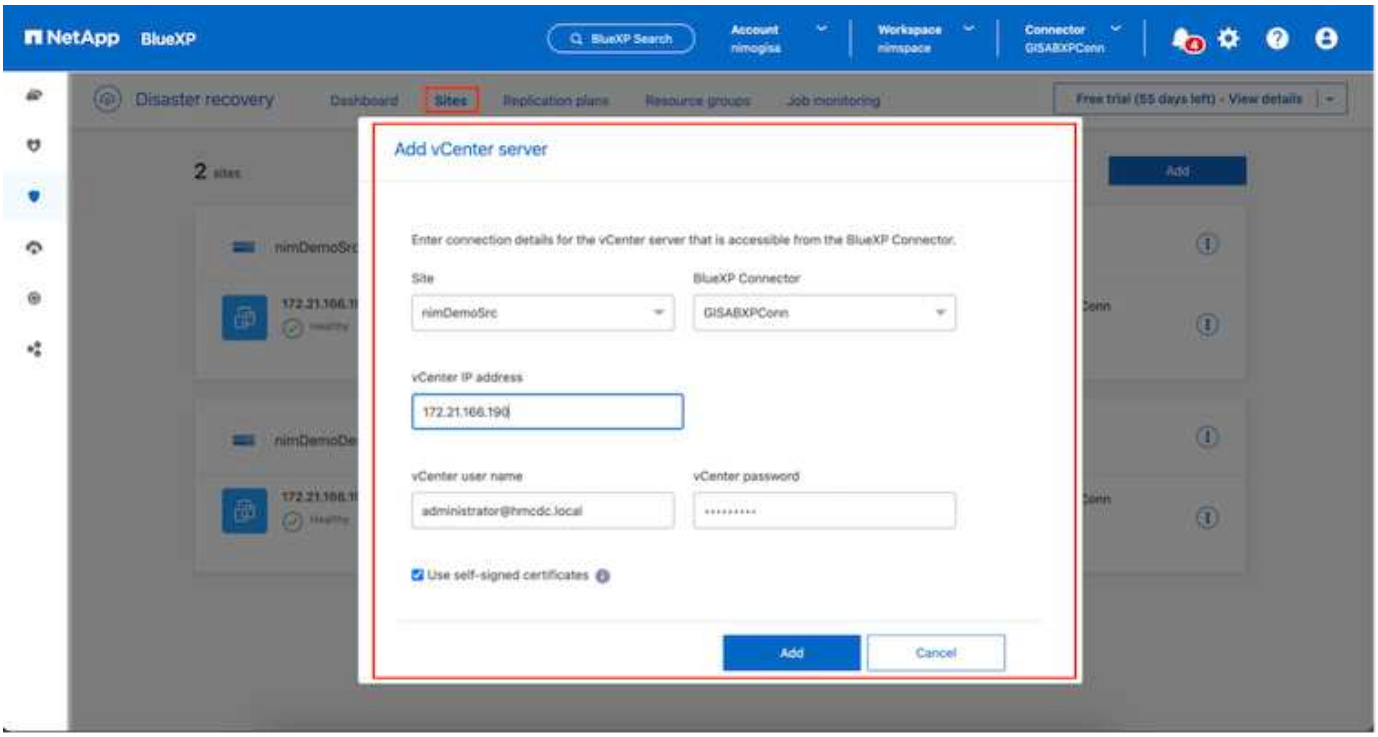


Aggiungere le seguenti piattaforme:

- **Fonte**. vCenter locale.



- **Destinazione**. VMC SDDC vCenter.



Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra il sito di origine e quello di destinazione

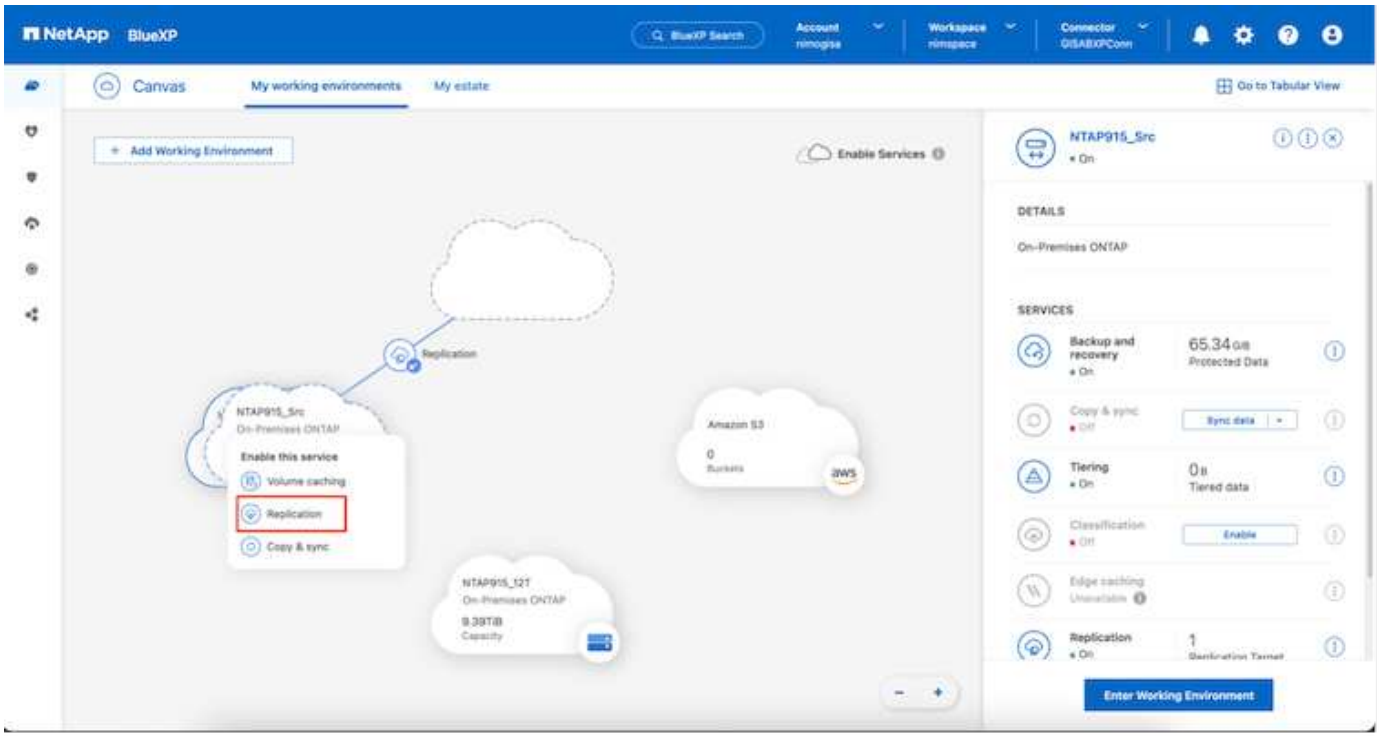
SnapMirror utilizza gli snapshot ONTAP per gestire il trasferimento dei dati da una posizione all'altra. Inizialmente, una copia completa basata su uno snapshot del volume di origine viene copiata sulla destinazione per eseguire una sincronizzazione di base. Quando si verificano modifiche ai dati all'origine, viene creato un nuovo snapshot e confrontato con lo snapshot di base. I blocchi che risultano modificati vengono quindi replicati nella destinazione, con lo snapshot più recente che diventa la baseline corrente o lo snapshot comune più recente. Ciò consente di ripetere il processo e di inviare aggiornamenti incrementali alla destinazione.

Una volta stabilita una relazione SnapMirror , il volume di destinazione è in uno stato di sola lettura online e quindi è ancora accessibile. SnapMirror funziona con blocchi fisici di archiviazione, anziché a livello di file o altro livello logico. Ciò significa che il volume di destinazione è una replica identica del volume di origine, inclusi snapshot, impostazioni del volume, ecc. Se il volume di origine utilizza funzionalità di efficienza dello spazio ONTAP , come la compressione dei dati e la deduplicazione dei dati, il volume replicato manterrà queste ottimizzazioni.

L'interruzione della relazione SnapMirror rende il volume di destinazione scrivibile e in genere viene utilizzato per eseguire un failover quando SnapMirror viene utilizzato per sincronizzare i dati in un ambiente DR. SnapMirror è sufficientemente sofisticato da consentire la risincronizzazione efficiente dei dati modificati nel sito di failover con il sistema primario, qualora questo dovesse tornare online in seguito, e quindi consentire il ripristino della relazione SnapMirror originale.

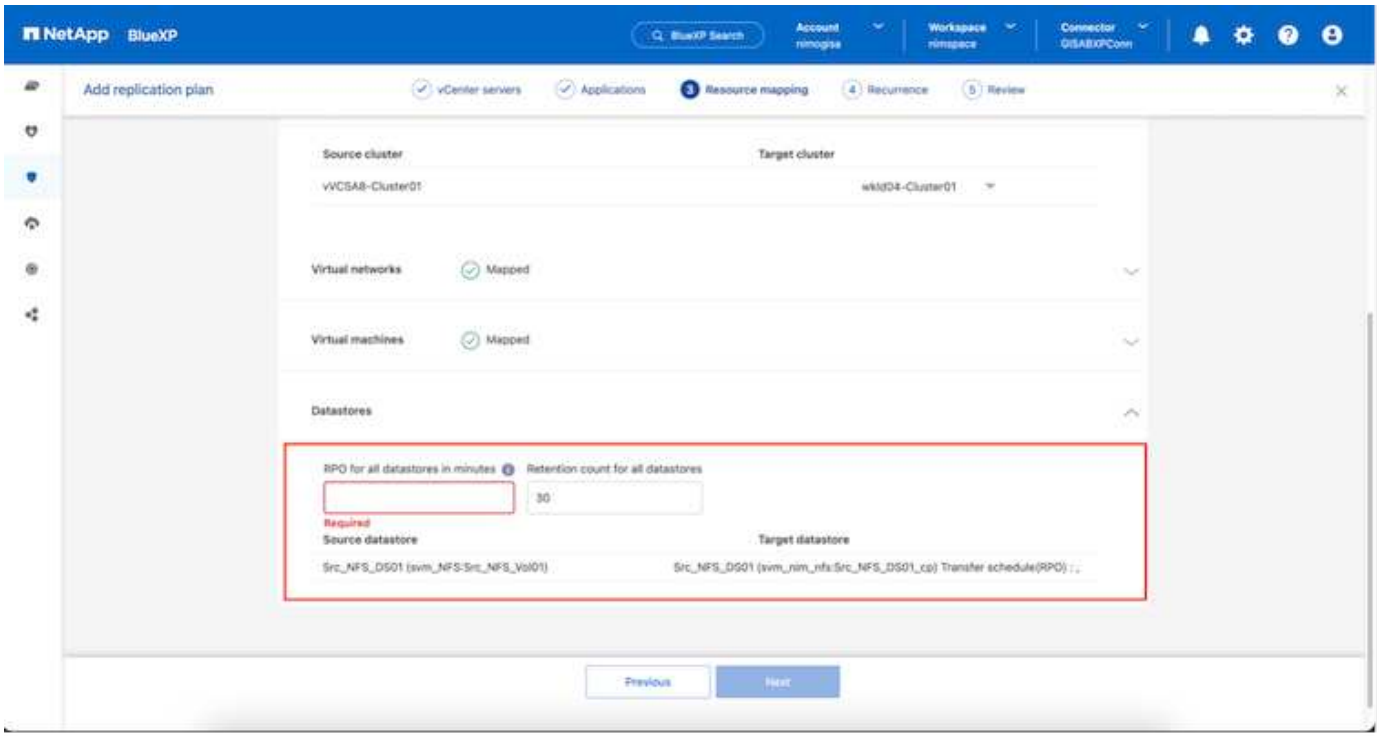
Come configurarlo per VMware Disaster Recovery

La procedura per creare la replica di SnapMirror rimane la stessa per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è utilizzare Console per configurare la replica di SnapMirror tramite un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione, attivando così la procedura guidata che ti accompagna nel resto del processo.



NetApp Data Services possono anche automatizzare lo stesso processo, a condizione che siano soddisfatti i due criteri seguenti:

- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.

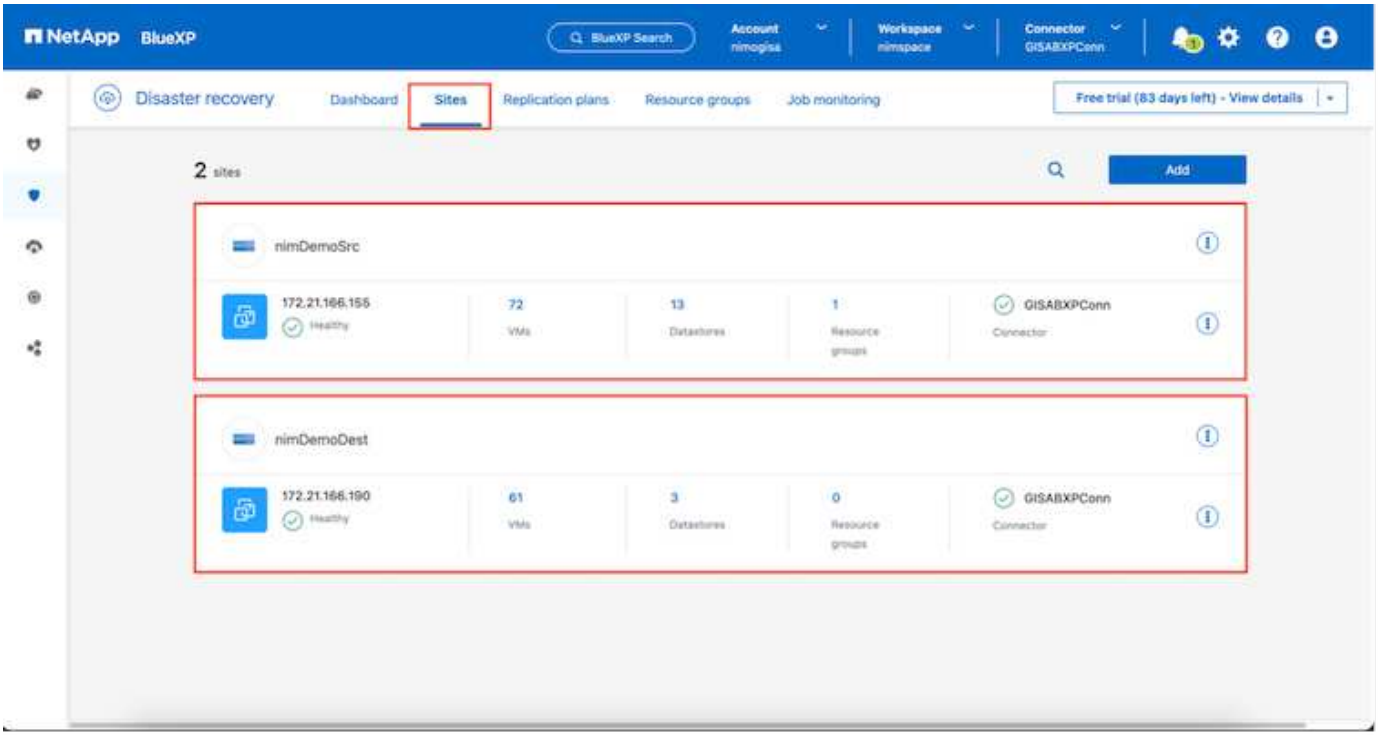


Se la relazione di SnapMirror è già configurata per il volume tramite CLI, Console la rileva e prosegue con le restanti operazioni del flusso di lavoro.

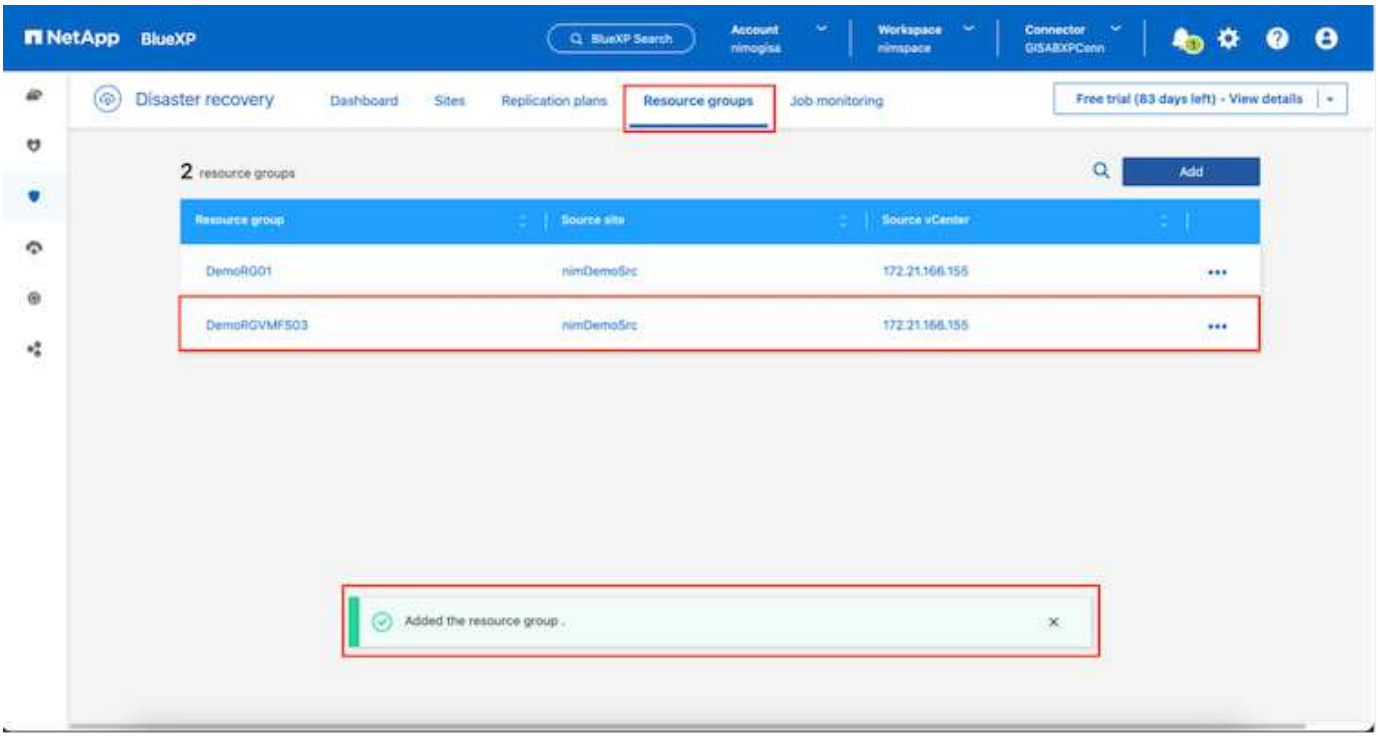
Oltre agli approcci sopra descritti, la replica di SnapMirror può essere creata anche tramite ONTAP CLI o System Manager. Indipendentemente dal metodo utilizzato per sincronizzare i dati utilizzando SnapMirror, Disaster Recovery orchestra il flusso di lavoro per operazioni di disaster recovery fluide ed efficienti.

Cosa può fare il Disaster Recovery per te?

Dopo aver aggiunto i siti di origine e di destinazione, Disaster Recovery esegue automaticamente un rilevamento approfondito e visualizza le macchine virtuali insieme ai metadati associati. Disaster Recovery rileva inoltre automaticamente le reti e i gruppi di porte utilizzati dalle macchine virtuali e li compila.

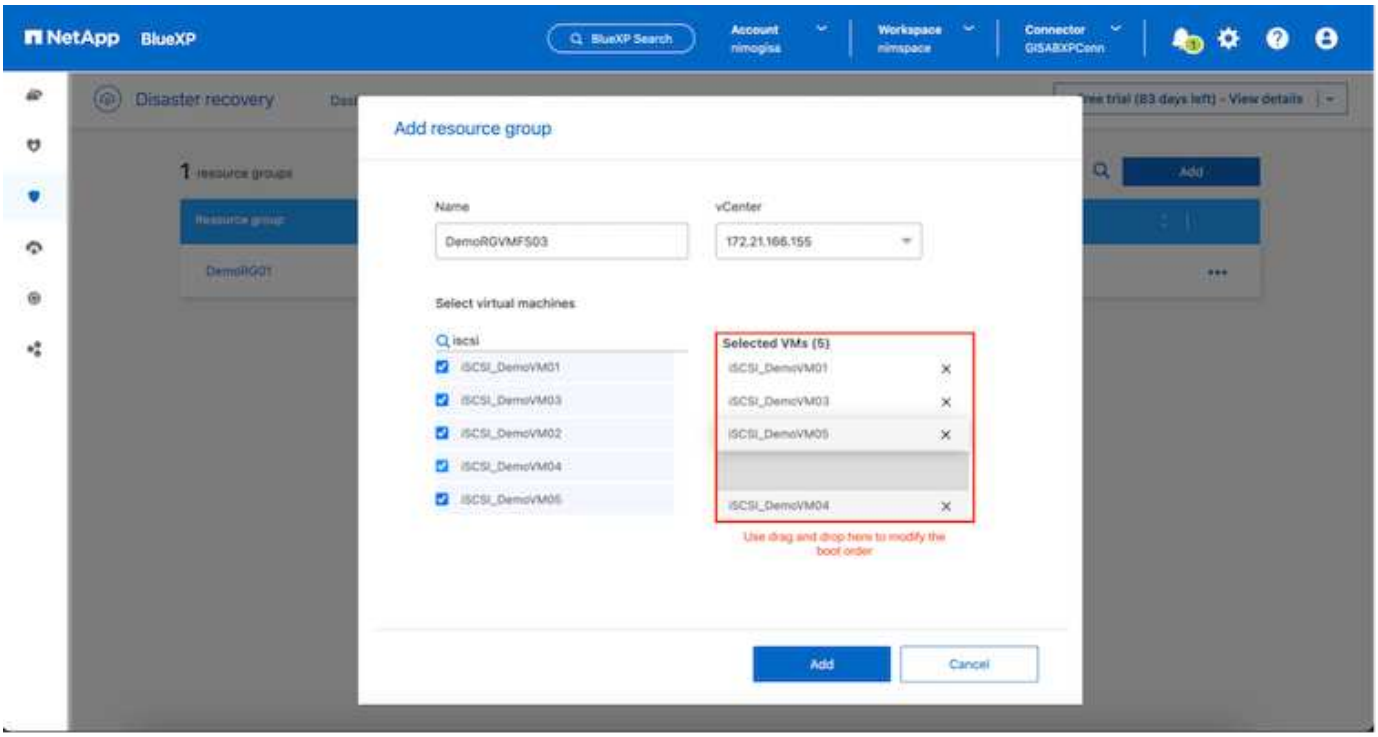


Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse di Disaster Recovery ti consentono di raggruppare un insieme di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti durante il ripristino. Per iniziare a creare gruppi di risorse, vai a **Resource Groups** e fai clic su **Create New Resource Group**.

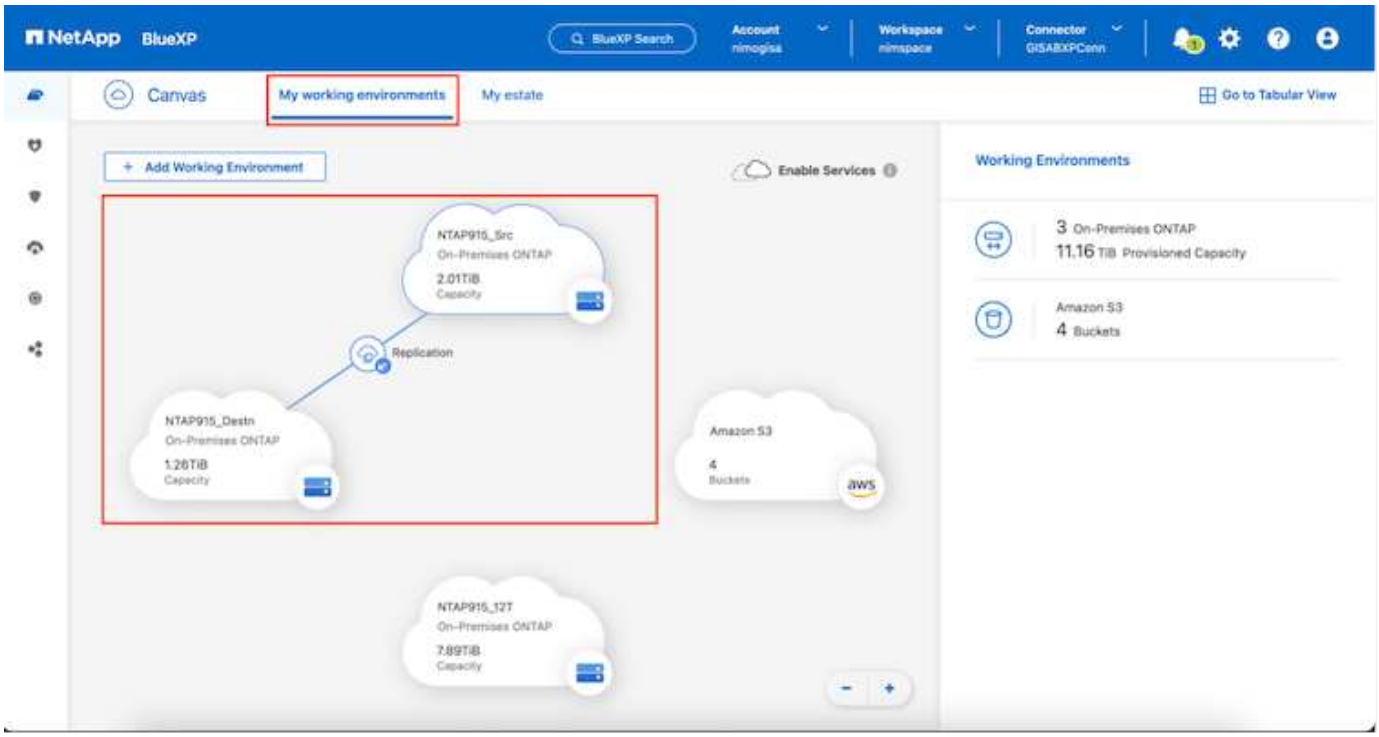


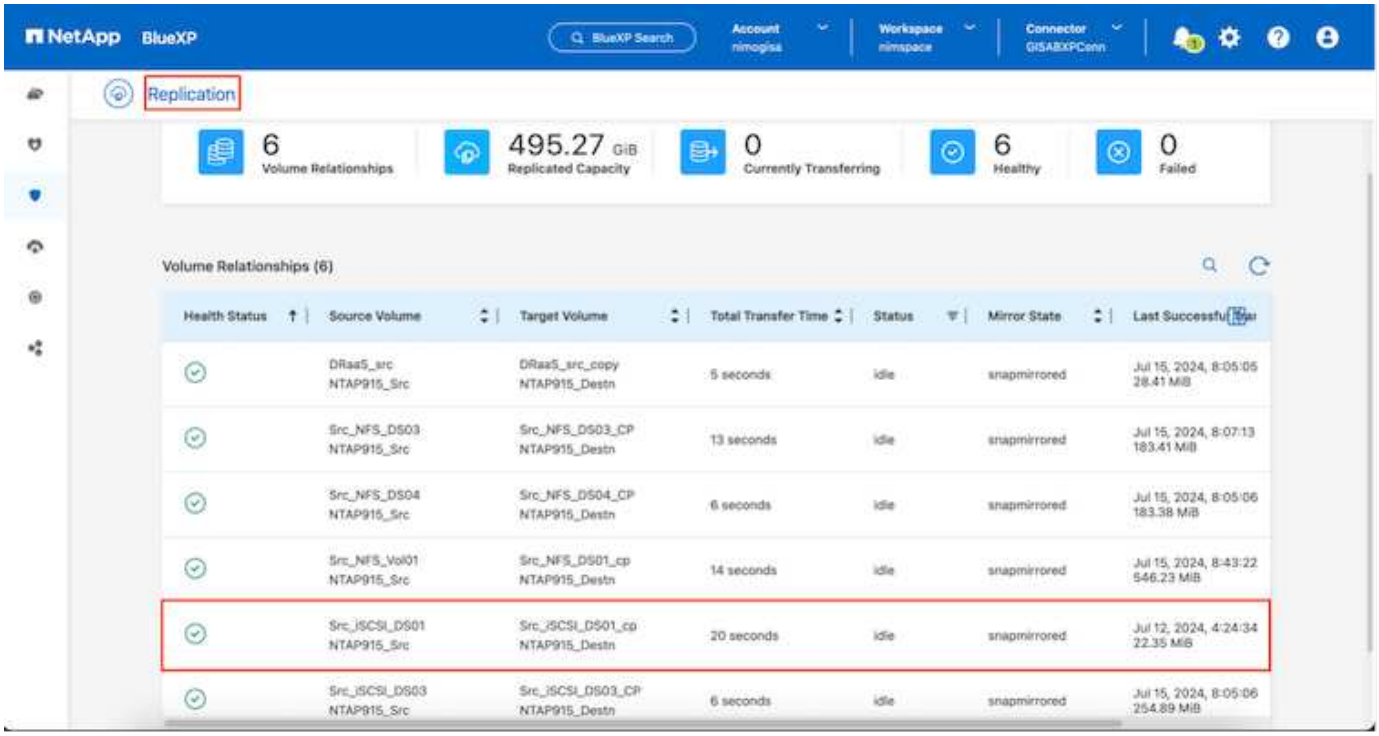
Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento della selezione.



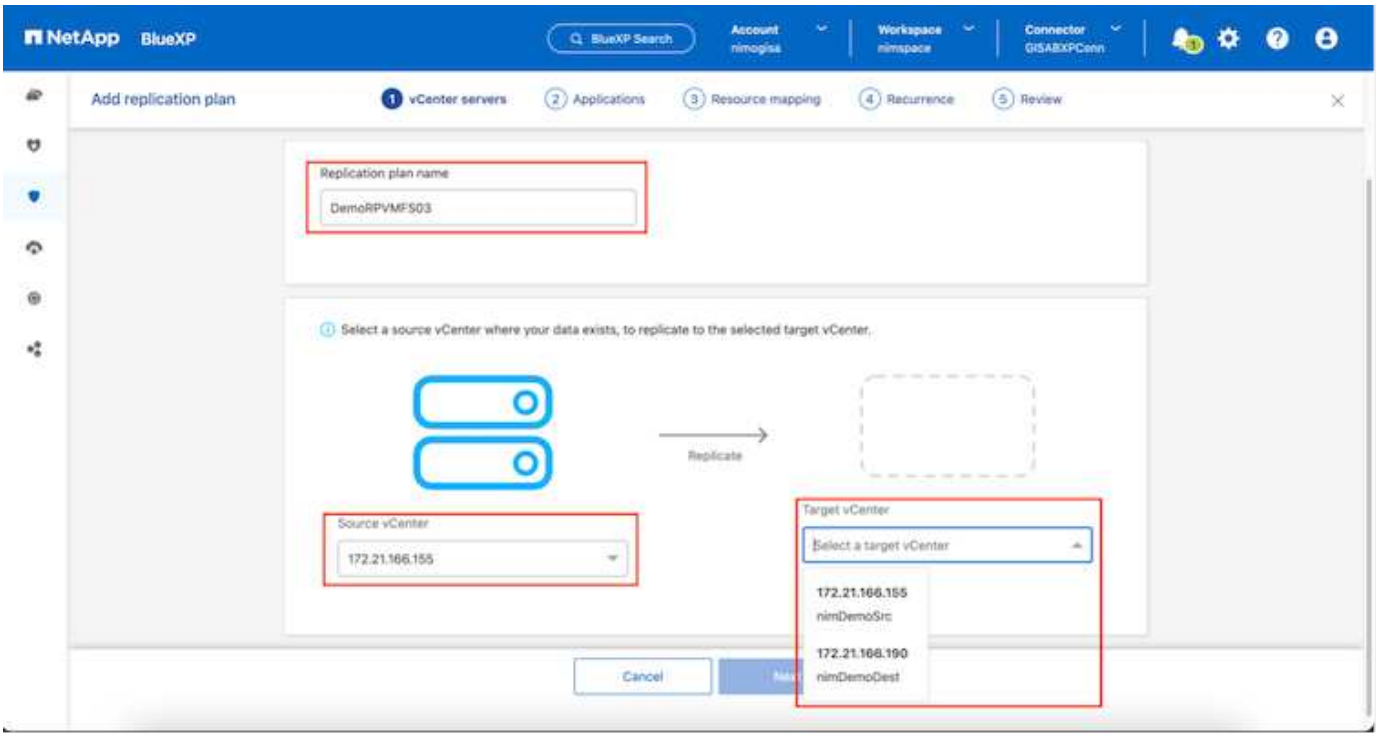
Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.



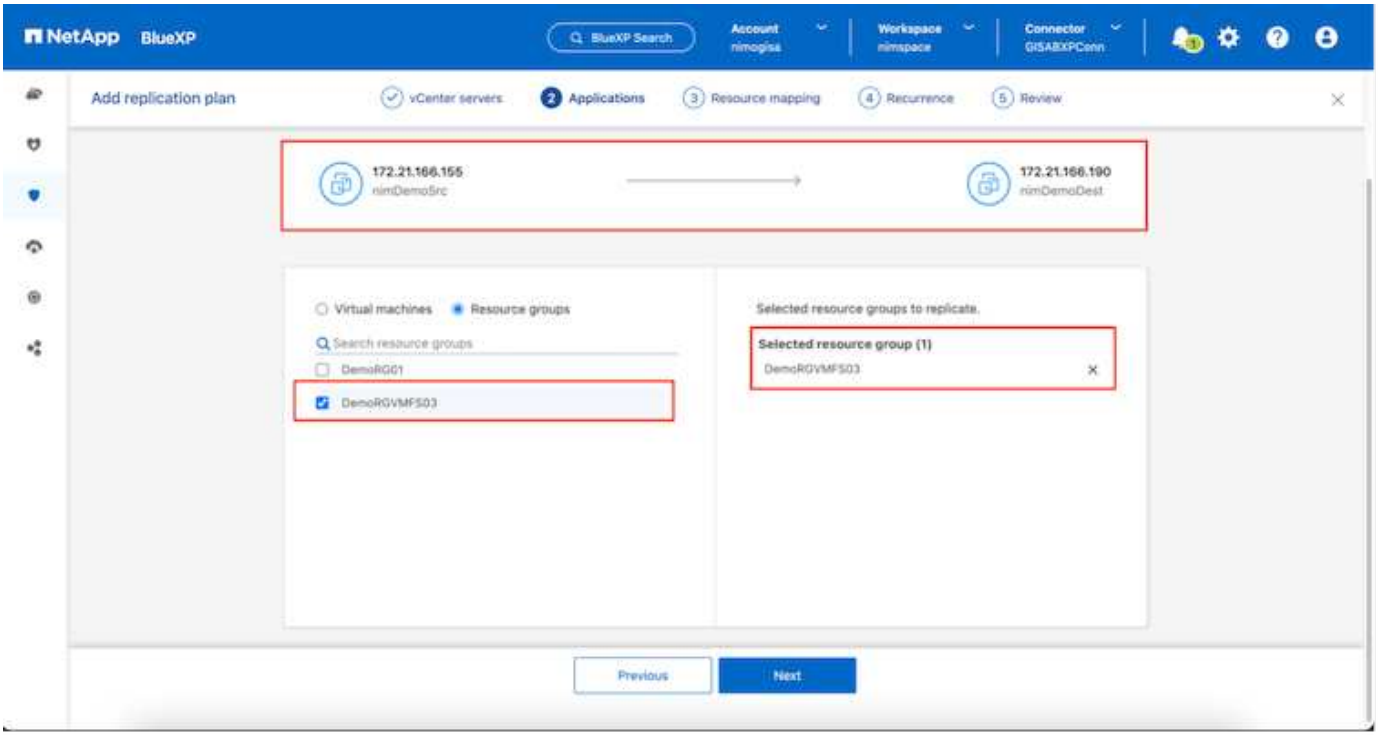


Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Aggiungi piano**.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



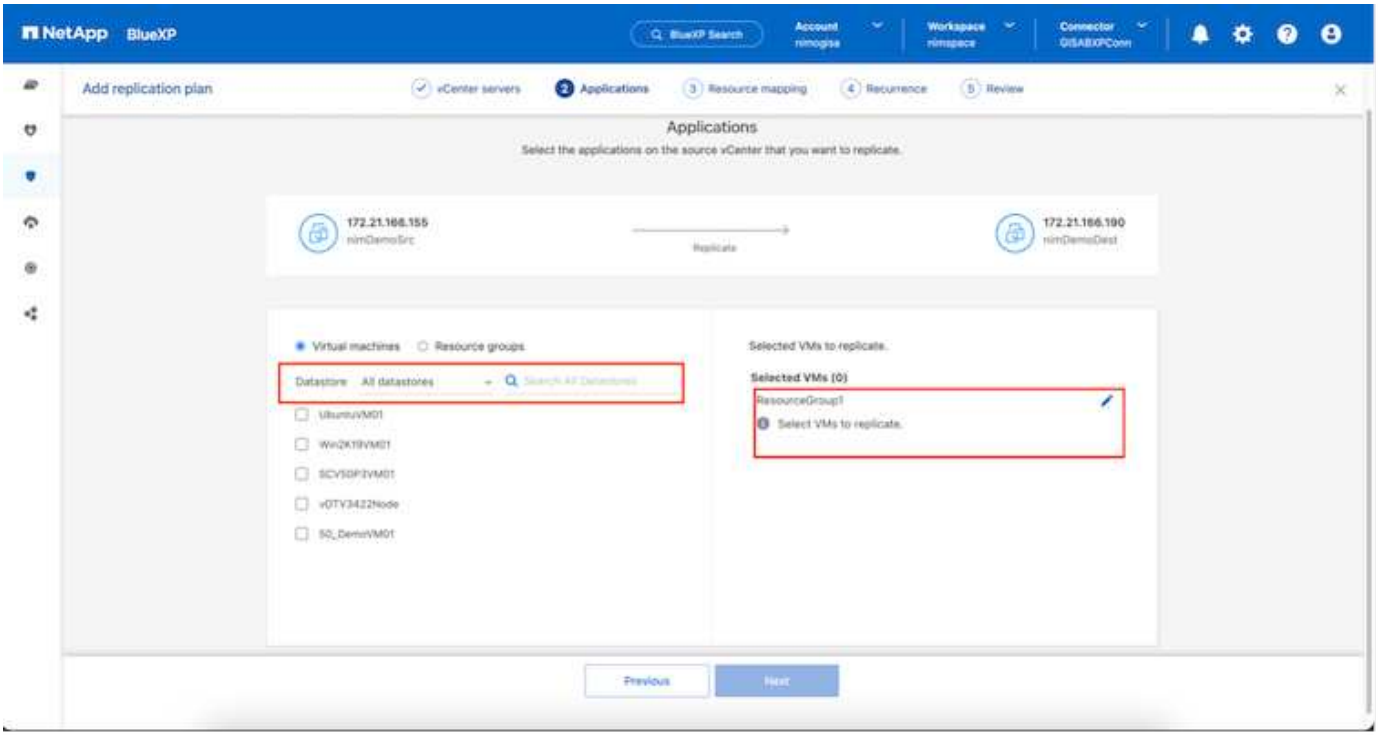
Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono essere ripristinate le macchine virtuali delle applicazioni.



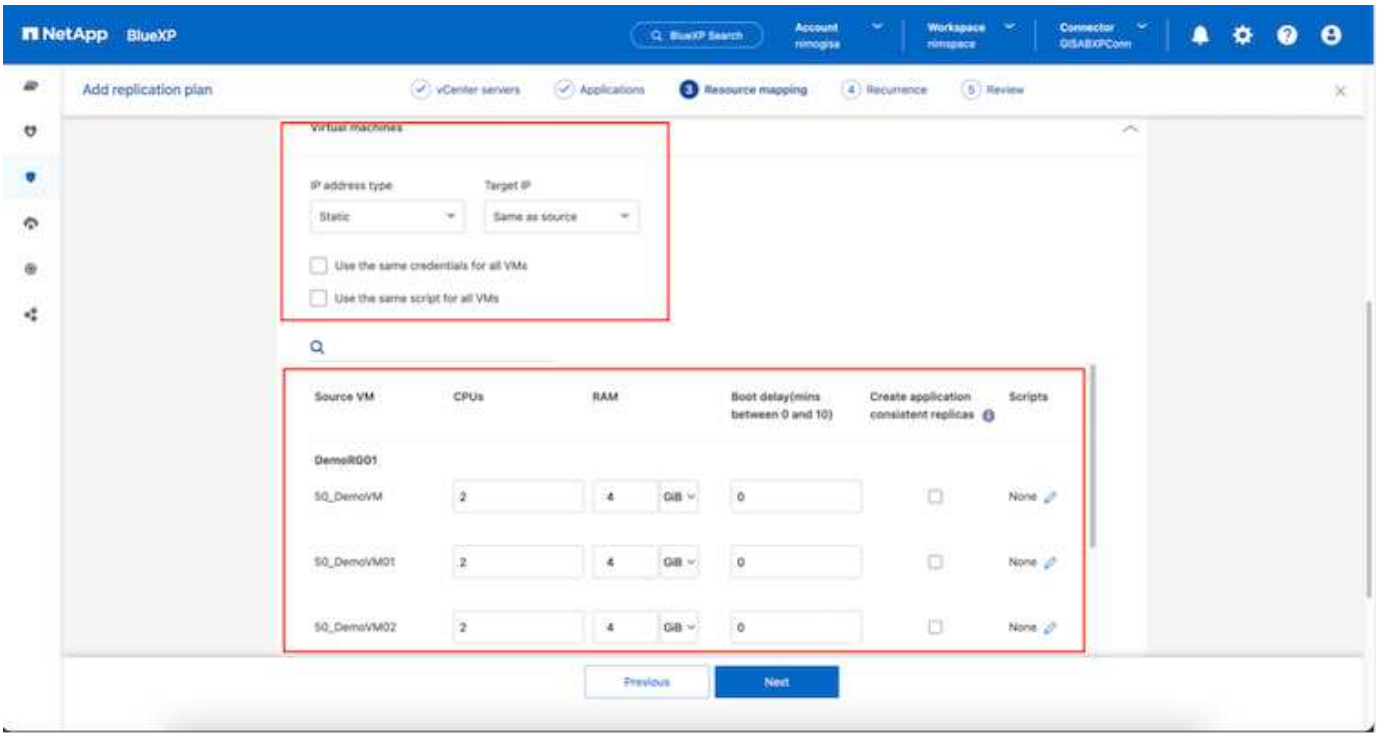
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Vengono avviati in parallelo due gruppi di risorse.

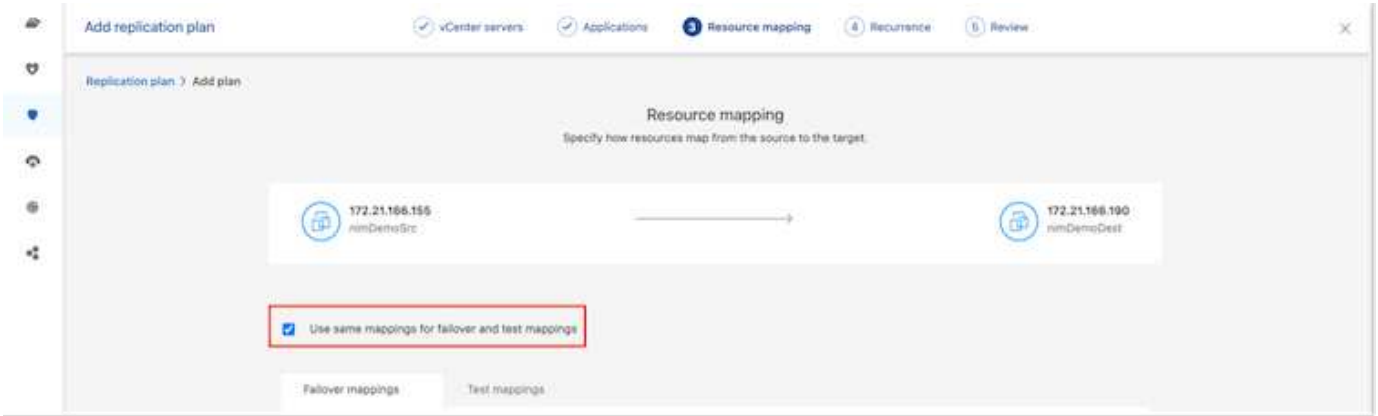
La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



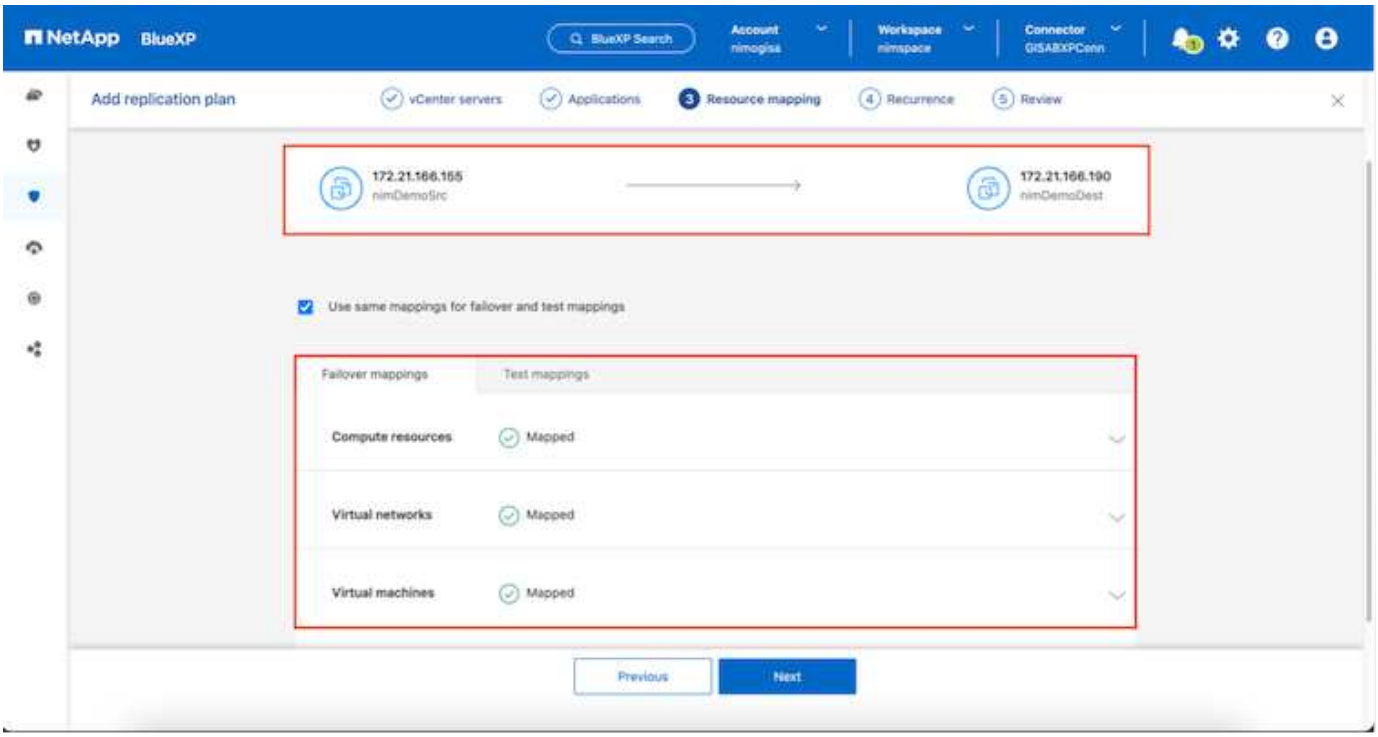
Una volta selezionati i gruppi di risorse, crea le mappature di failover. In questa fase, specifica come le risorse dell'ambiente di origine vengono mappate all'ambiente di destinazione. Ciò include risorse di calcolo e reti virtuali. Personalizzazione IP, script pre e post, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, consulta "Creare un piano di replicazione".



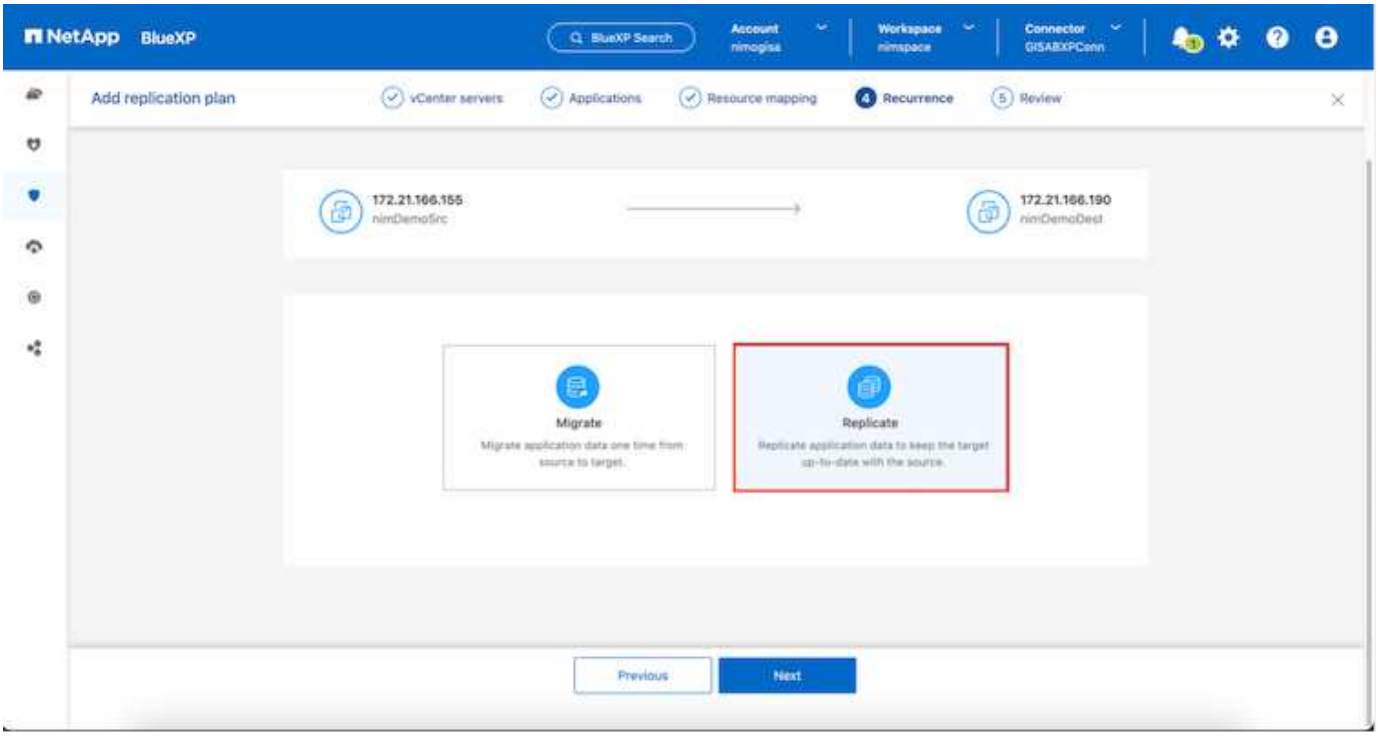
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per applicare mappature diverse per l'ambiente di test, selezionare l'opzione Mappatura test dopo aver deselezionato la casella di controllo come mostrato di seguito:



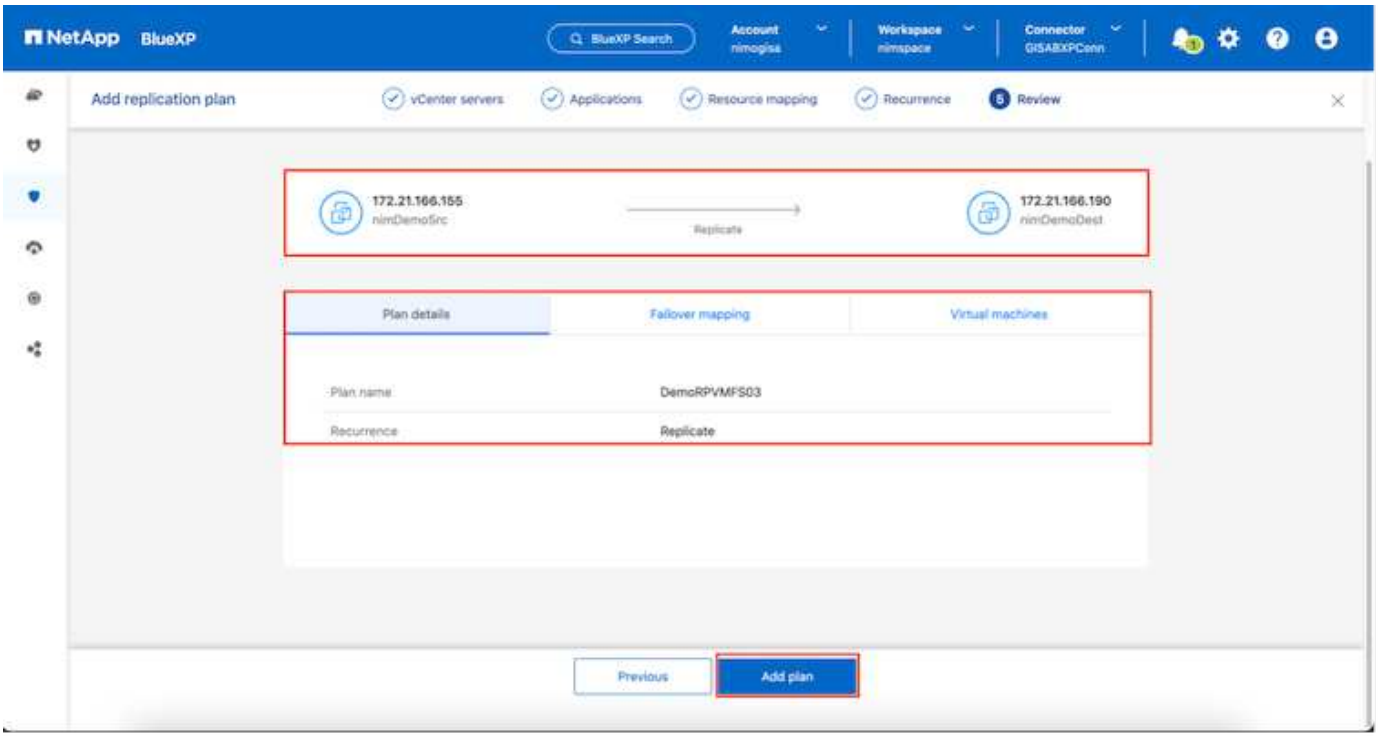
Una volta completata la mappatura delle risorse, fare clic su Avanti.

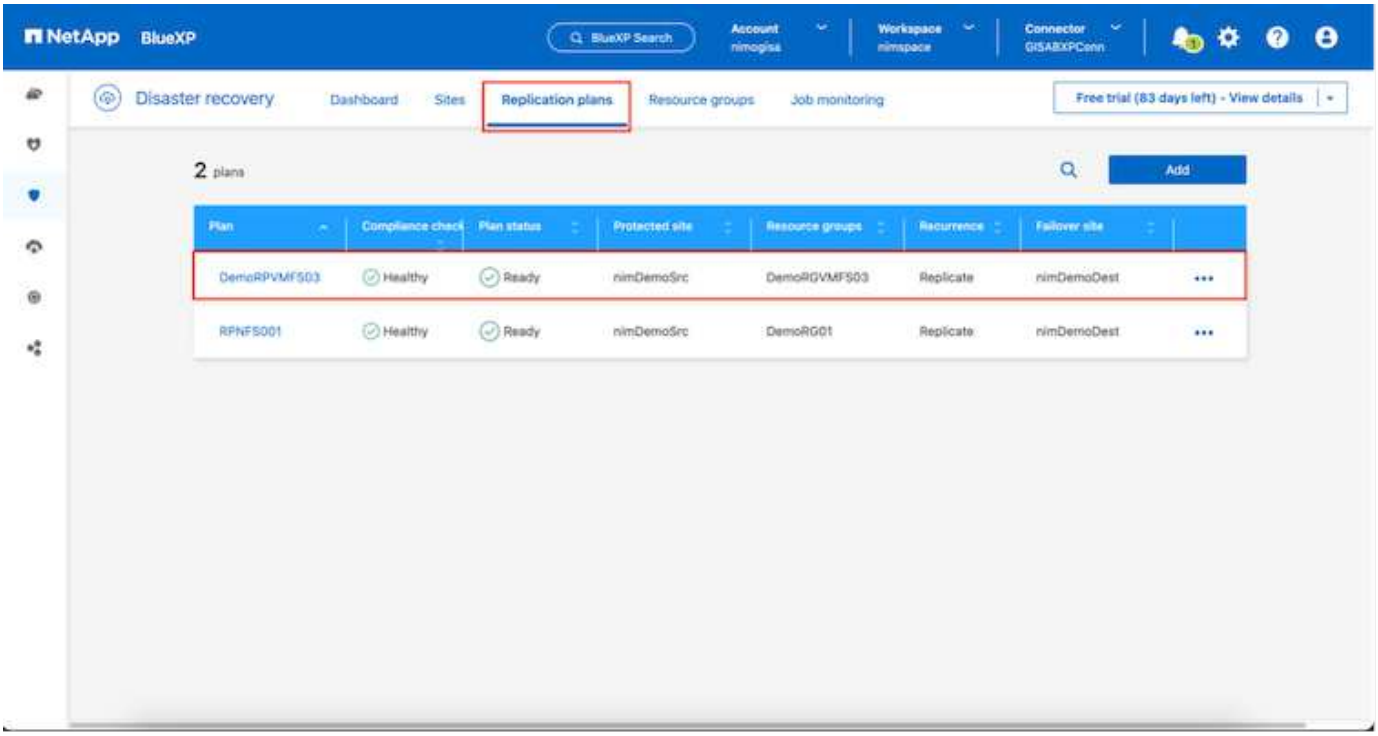


Selezionare il tipo di ricorrenza. In parole semplici, seleziona l'opzione Migra (migrazione una tantum tramite failover) o replica continua ricorrente. In questa procedura dettagliata è selezionata l'opzione Replica.

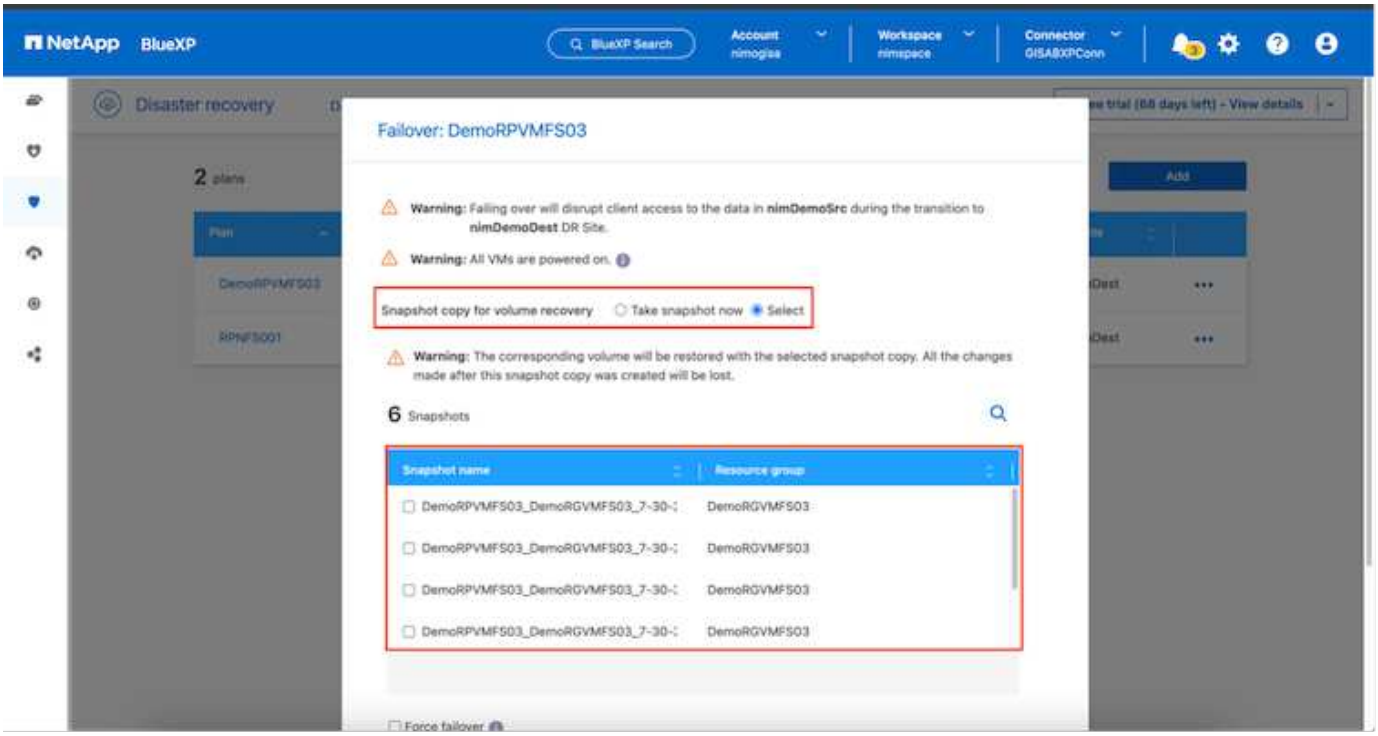


Una volta fatto, rivedi le mappature create e poi fai clic su Aggiungi piano.

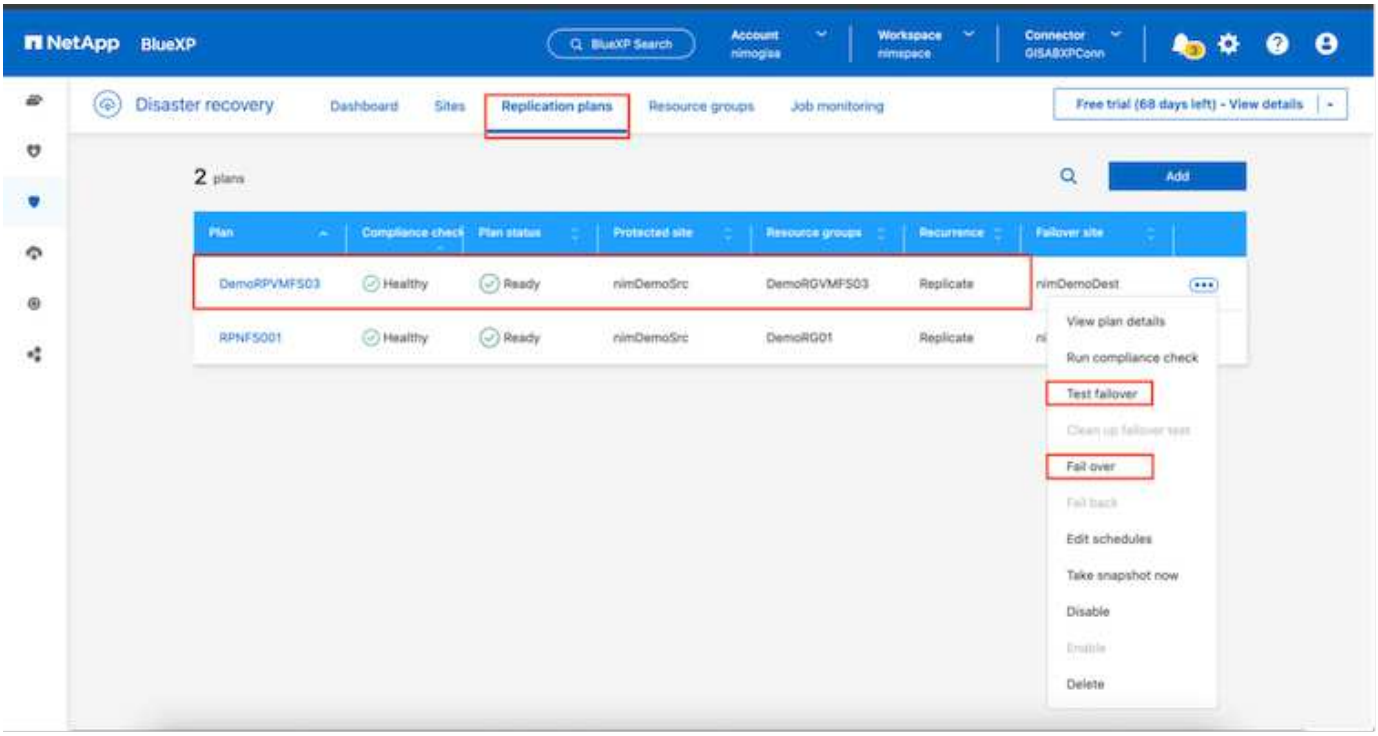




Una volta creato il piano di replica, puoi eseguire il failover in base ai requisiti selezionando l'opzione di failover, l'opzione di test-failover o l'opzione di migrazione. Disaster Recovery garantisce che il processo di replica venga eseguito secondo il piano ogni 30 minuti. Durante le opzioni di failover e test-failover, puoi utilizzare la copia Snapshot di SnapMirror più recente oppure selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (in base al criterio di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile in caso di un evento di corruzione come il ransomware, in cui le repliche più recenti sono già compromesse o crittografate. Disaster Recovery mostra tutti i punti di recovery disponibili.



Per attivare il failover o il failover di prova con la configurazione specificata nel piano di replica, fare clic su **Failover** o **Failover di prova**.

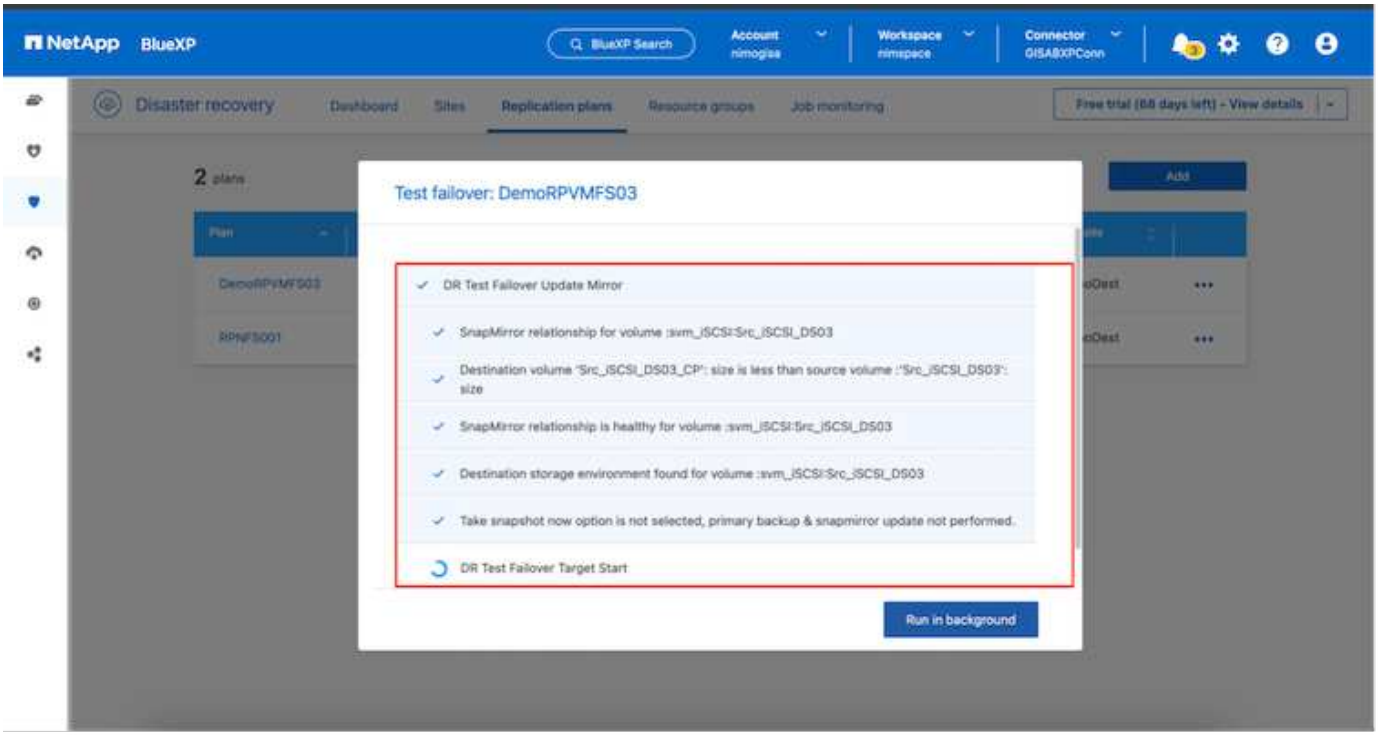


Cosa succede durante un'operazione di failover o di test failover?

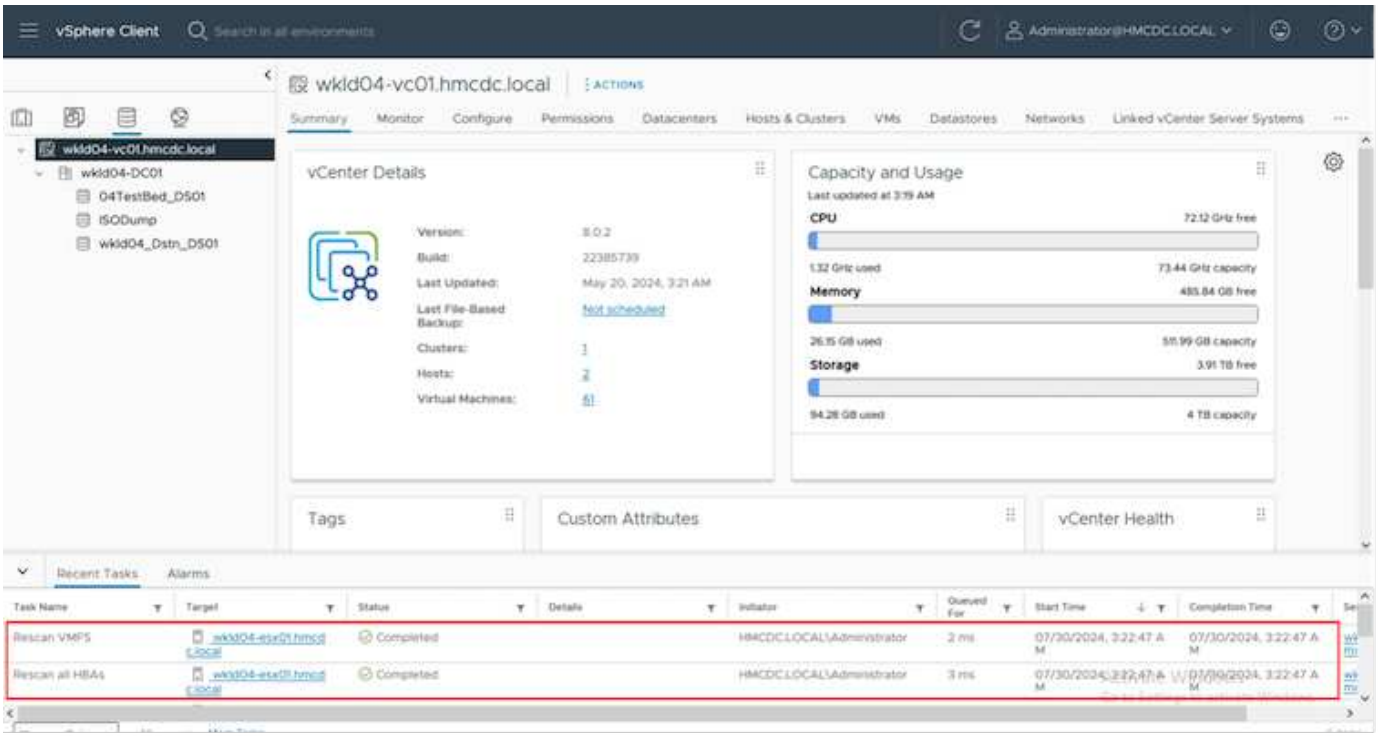
Durante un'operazione di failover di prova, Disaster Recovery crea un volume FlexClone sul sistema storage ONTAP di destinazione utilizzando la copia Snapshot più recente o uno snapshot selezionato del volume di destinazione.

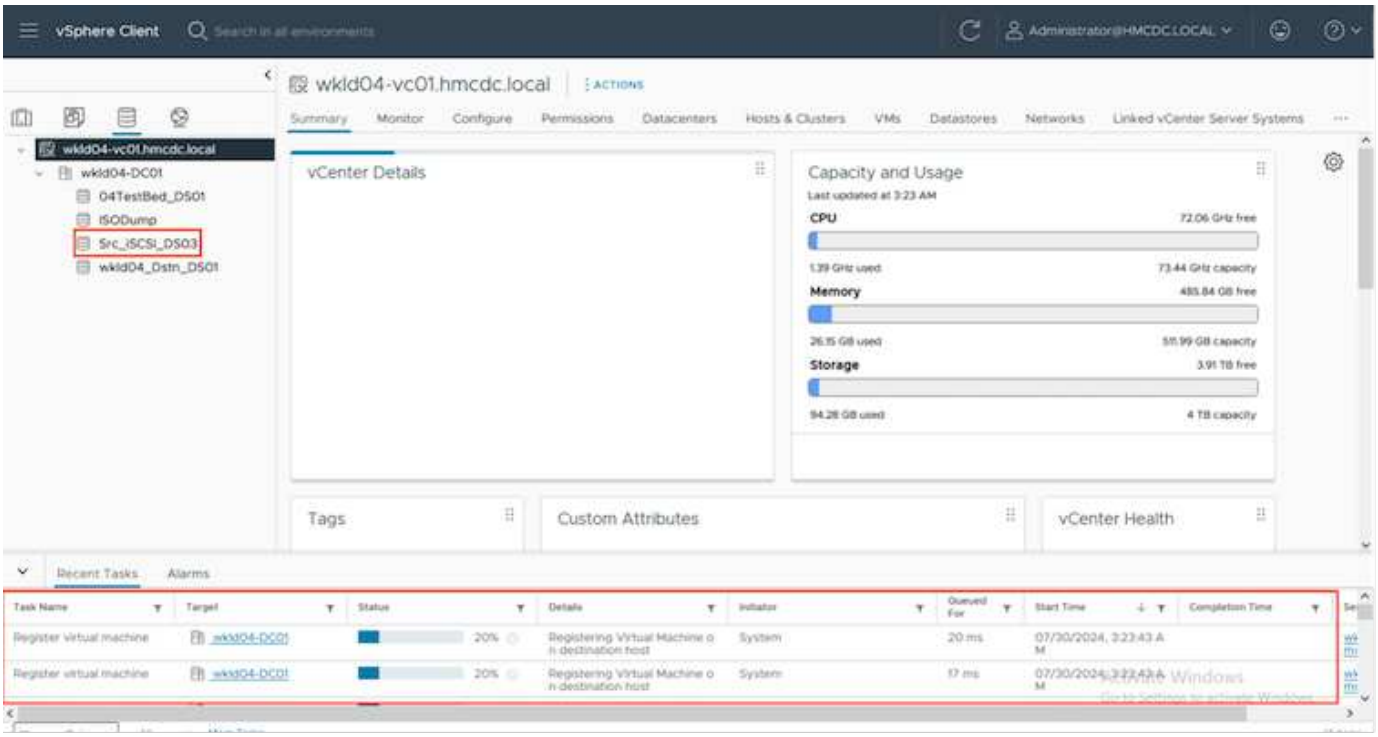
Un'operazione di failover di prova crea un volume clonato sul sistema di archiviazione ONTAP di destinazione.

L'esecuzione di un'operazione di ripristino di prova non influisce sulla replica SnapMirror .



Durante il processo, Disaster Recovery non mappa il volume di destinazione originale. Al contrario, crea un nuovo volume FlexClone dallo Snapshot selezionato e mappa agli host ESXi un datastore temporaneo che supporta il volume FlexClone.

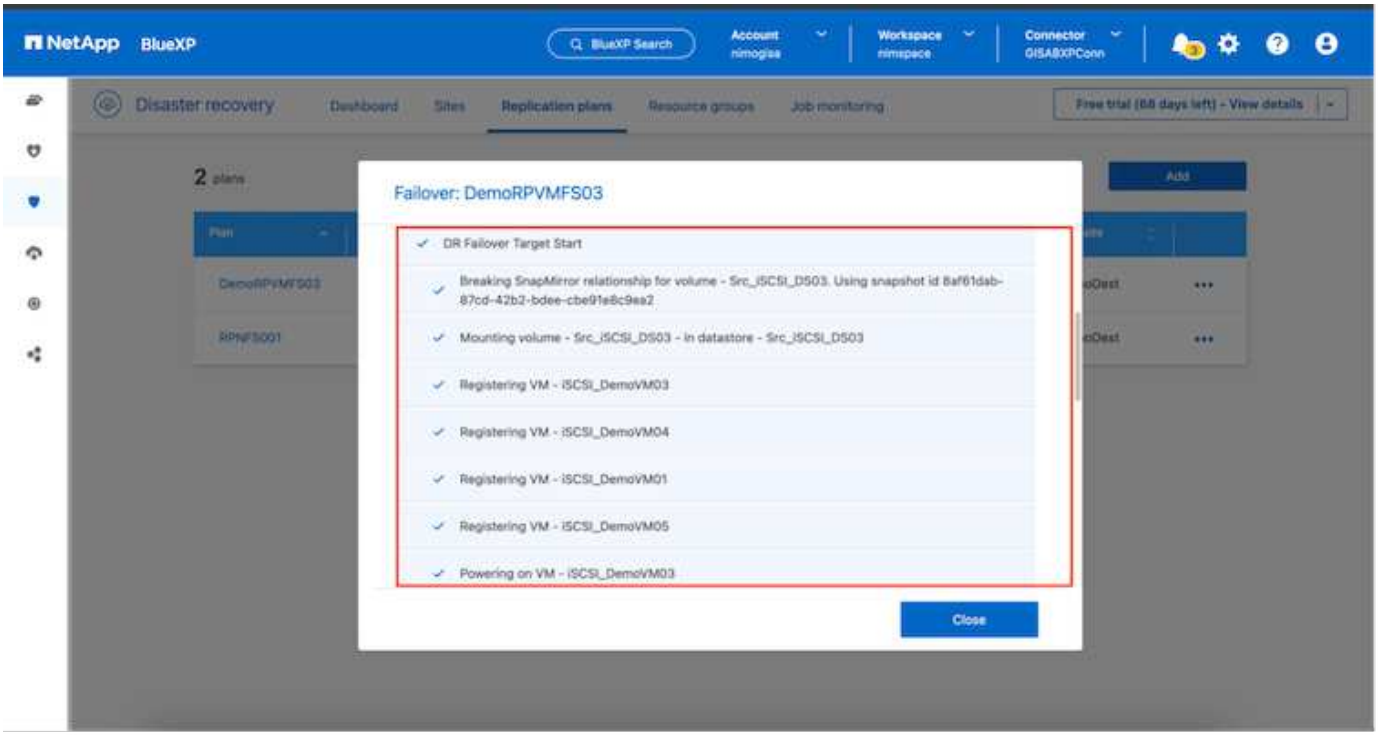




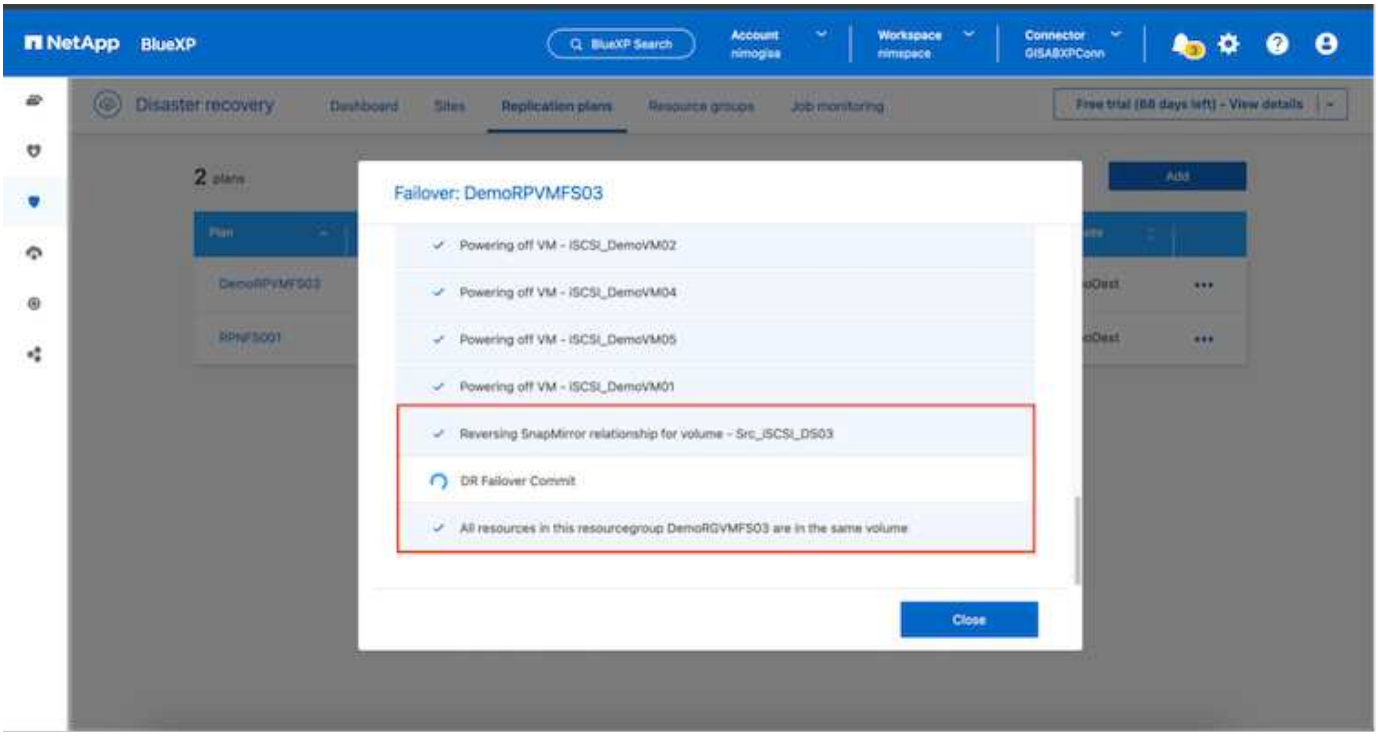
Quando l'operazione di failover di test è completata, puoi avviare l'operazione di pulizia usando **"Pulizia test failover"**. Durante questa operazione, Disaster Recovery elimina il volume FlexClone utilizzato nell'operazione.

In caso di un evento catastrofico reale, Disaster Recovery esegue le seguenti operazioni:

1. Interrompe la relazione SnapMirror tra i siti.
2. Monta il volume del datastore VMFS dopo la nuova firma per un utilizzo immediato.
3. Registrare le VM
4. Accendere le VM

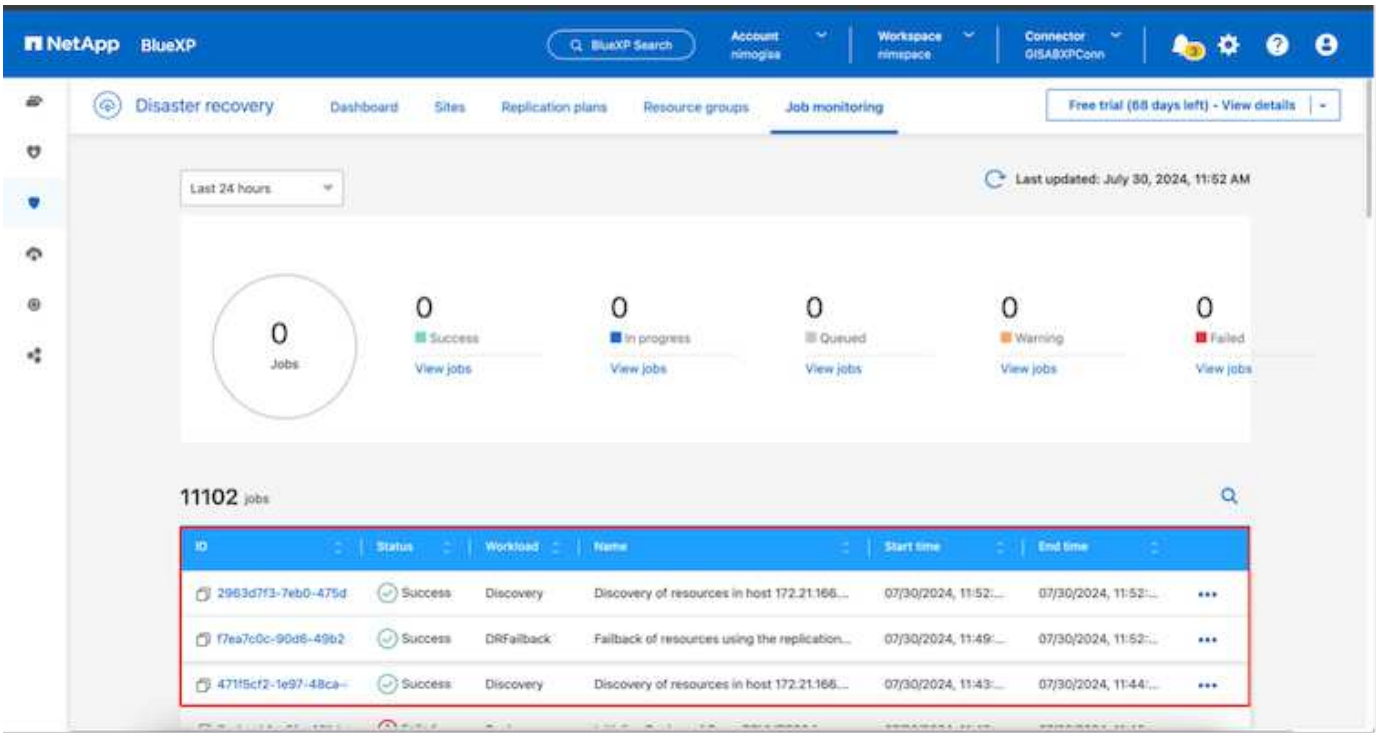


Una volta che il sito primario è attivo e funzionante, Disaster Recovery abilita la risincronizzazione inversa per SnapMirror e il failback, operazioni che possono essere nuovamente eseguite con un semplice clic.



Se si sceglie l'opzione di migrazione, questa viene considerata un evento di failover pianificato. In questo caso, viene attivato un ulteriore passaggio che consiste nello spegnimento delle macchine virtuali nel sito di origine. Il resto dei passaggi rimane lo stesso dell'evento di failover.

Da Console o da ONTAP CLI, puoi monitorare lo stato di integrità della replica per i volumi datastore appropriati e tenere traccia dello stato di un failover o di un failover di test tramite Job Monitoring.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il"simulatore di soluzioni" .

Multicloud ibrido NetApp con carichi di lavoro containerizzati Red Hat OpenShift

Iniziare

Soluzioni NetApp Hybrid Multicloud per carichi di lavoro Red Hat OpenShift Container

NetApp sta riscontrando un aumento significativo di clienti che modernizzano le proprie applicazioni aziendali legacy e creano 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.

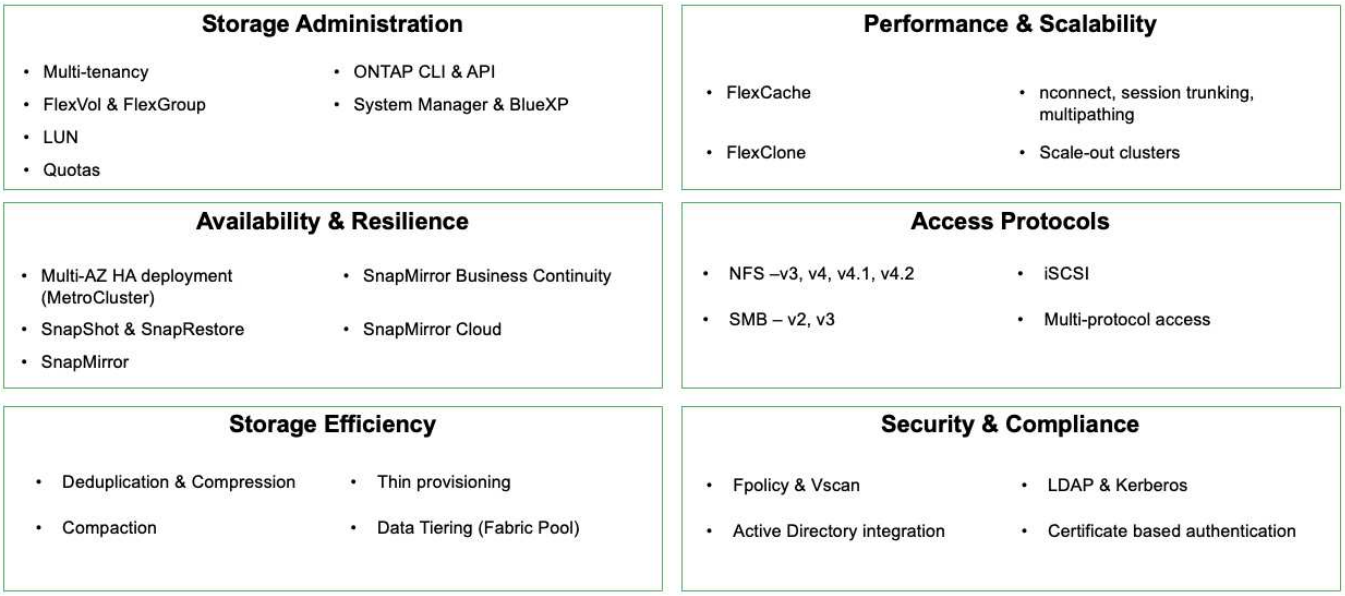
Panoramica

Poiché sempre più clienti iniziano ad adottare container nelle proprie aziende, NetApp è nella posizione ideale per soddisfare le esigenze di storage persistente delle loro applicazioni stateful e le esigenze classiche di gestione dei dati, 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 container e distribuzioni Kubernetes.

- Archiviazione autogestita in sede:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Archiviazione gestita dal provider in locale:
  - NetApp Keystone fornisce Storage as a Service (STaaS)
- Archiviazione autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP(CVO) fornisce storage autogestito negli hyperscaler
- Archiviazione gestita dal provider nel cloud:
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files e Google Cloud NetApp Volumes forniscono storage basato su file nel cloud.

ONTAP feature highlights

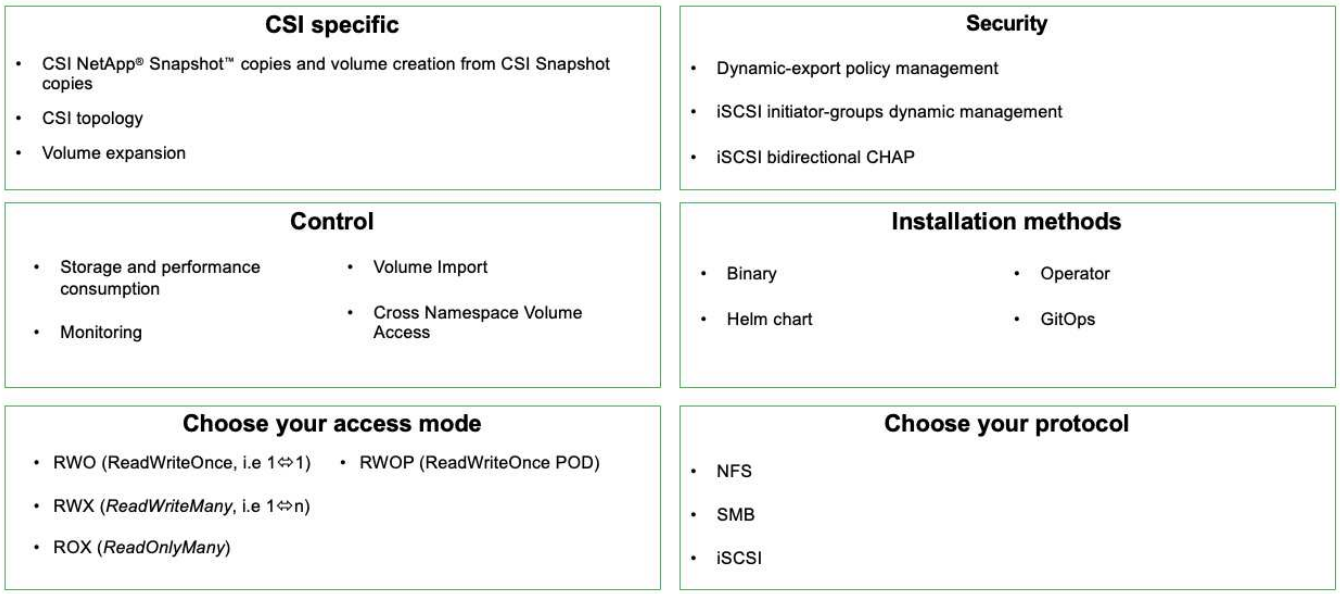


NetApp Console ti consente di gestire tutte le tue risorse di storage e dati da un unico piano di controllo/interfaccia.

Puoi utilizzare NetApp Console per creare e amministrare cloud storage (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi di storage on-prem e edge.

- NetApp Trident** è uno Storage Orchestrator conforme a CSI che consente un utilizzo rapido e semplice di storage persistente supportato da una varietà di opzioni di storage NetApp sopra menzionate. Si tratta di un software open source gestito e supportato da NetApp.

Astra Trident CSI feature highlights



I carichi di lavoro dei container critici per l'azienda necessitano di più di semplici volumi persistenti. I requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti Kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti Kubernetes oltre ai dati utente: alcuni esempi sono i seguenti: - oggetti Kubernetes come specifiche di pod, PVC, distribuzioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie snapshot, backup, cloni - risorse personalizzate come CR e CRD

NetApp Trident Protect, disponibile come componente aggiuntivo gratuito di NetApp Trident, offre funzionalità avanzate di gestione dei dati applicativi che migliorano la funzionalità e la disponibilità delle applicazioni Kubernetes stateful supportate da sistemi di storage NetApp ONTAP. Trident Protect semplifica la gestione, la protezione e lo spostamento dei carichi di lavoro containerizzati sia su cloud pubblici che in ambienti on-premises. Offre inoltre solide funzionalità di automazione tramite la sua API e CLI.

Questa documentazione di riferimento fornisce la convalida della protezione dei dati delle applicazioni basate su container, distribuite sulla piattaforma RedHat OpenShift utilizzando Trident Protect. Inoltre, la soluzione fornisce dettagli di alto livello per la distribuzione 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 utilizzando il provisioner Trident CSI.

Proposte di valore delle soluzioni NetApp Hybrid Multicloud per i carichi di lavoro dei container Red Hat OpenShift

La maggior parte dei clienti non inizia a creare ambienti basati su Kubernetes senza alcuna infrastruttura esistente. Forse si tratta di un'officina informatica tradizionale che esegue la maggior parte delle proprie applicazioni aziendali su macchine virtuali (ad esempio in grandi ambienti VMware). Quindi iniziano a creare piccoli ambienti basati su container per soddisfare le esigenze dei loro moderni team di sviluppo di applicazioni. Queste iniziative solitamente iniziano in piccolo e diventano più diffuse man mano che i team apprendono queste nuove tecnologie e competenze e cominciano a riconoscere i numerosi vantaggi che derivano dalla loro adozione. La buona notizia per i clienti è che NetApp è in grado di soddisfare le esigenze di entrambi gli ambienti. Questa serie di soluzioni per il multicloud ibrido con Red Hat OpenShift consentirà ai clienti NetApp di adottare tecnologie e servizi cloud moderni senza dover rinnovare l'intera infrastruttura e organizzazione. NetApp è in grado di garantire gestione, protezione, sicurezza e portabilità dei dati coerenti, indipendentemente dal fatto che le applicazioni e i dati dei clienti siano ospitati in sede, nel cloud, eseguiti su macchine virtuali o su container. Grazie a queste nuove soluzioni, lo stesso valore che NetApp ha offerto negli ambienti dei data center on-premise per decenni sarà disponibile nell'intero orizzonte dati aziendale, senza richiedere investimenti significativi per riorganizzare, acquisire nuove competenze o creare nuovi team. NetApp è ben posizionata per aiutare i clienti a risolvere queste sfide aziendali, indipendentemente dalla fase in cui si trovano nel loro percorso verso il cloud.

NetApp Hybrid Multi-Cloud con Red Hat Openshift:

- Offre ai clienti progetti e pratiche convalidati che illustrano i modi migliori per gestire, proteggere, mettere in sicurezza e migrare i propri dati e applicazioni quando si utilizza Red Hat OpenShift con soluzioni di storage basate su NetApp .

- Presenta le best practice per i clienti che utilizzano Red Hat OpenShift con storage NetApp in ambienti VMware, infrastrutture bare metal o una combinazione di entrambi.
- Dimostrare strategie e opzioni per ambienti sia on-premise che cloud, nonché per ambienti ibridi in cui vengono utilizzati entrambi.

Soluzioni supportate di NetApp Hybrid Multicloud per carichi di lavoro di Red Hat OpenShift Container

La soluzione testa e convalida Migration & Centralized Data Protection con OpenShift Container Platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp Console e NetApp Trident Protect.

Per questa soluzione, i seguenti scenari sono testati e convalidati da NetApp. La soluzione è suddivisa in più scenari in base alle seguenti caratteristiche:

- in sede
- nuvola
  - cluster OpenShift autogestiti e storage NetApp autogestito
  - cluster OpenShift gestiti dal provider e storage NetApp gestito dal provider

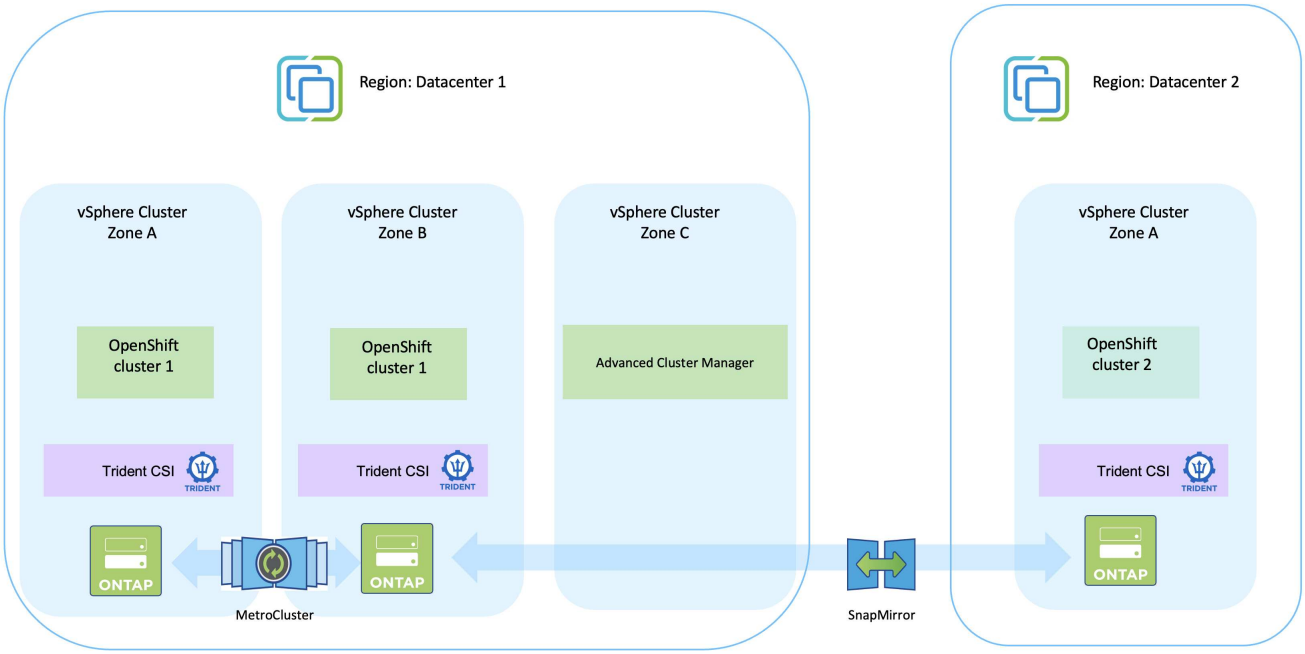
In futuro svilupperemo ulteriori soluzioni e casi d'uso.

Scenario 1: Protezione e migrazione dei dati nell'ambiente on-premise tramite Trident Protect

In sede: cluster OpenShift autogestiti e storage NetApp autogestito

- Utilizza Trident Protect per proteggere le applicazioni e supportare la migrazione tra i cluster on-premises.

Scenario 1

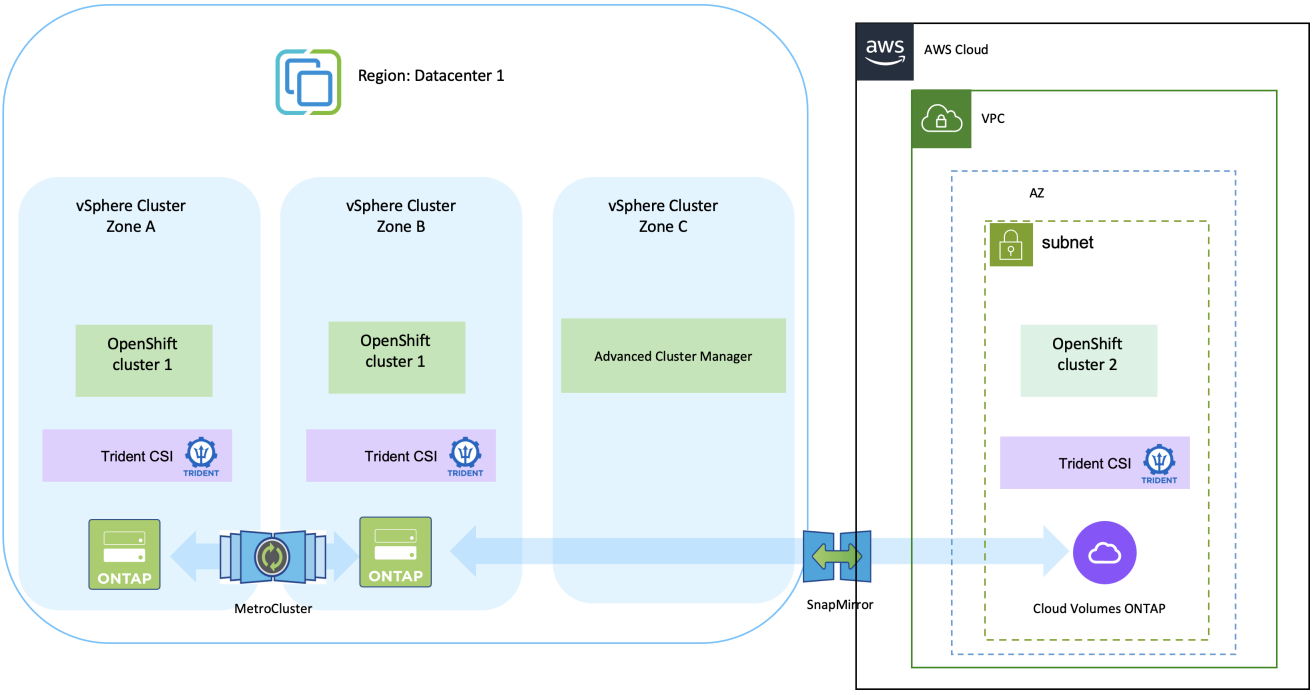


Scenario 2: Protezione dei dati e migrazione dall'ambiente locale all'ambiente AWS utilizzando Trident Protect

In sede: cluster OpenShift autogestito e storage autogestito AWS Cloud: cluster OpenShift autogestito e storage autogestito

- Utilizza Trident Protect per proteggere le applicazioni e supportare la migrazione tra i cluster locali e i cluster OpenShift autogestiti in AWS.

Scenario 2

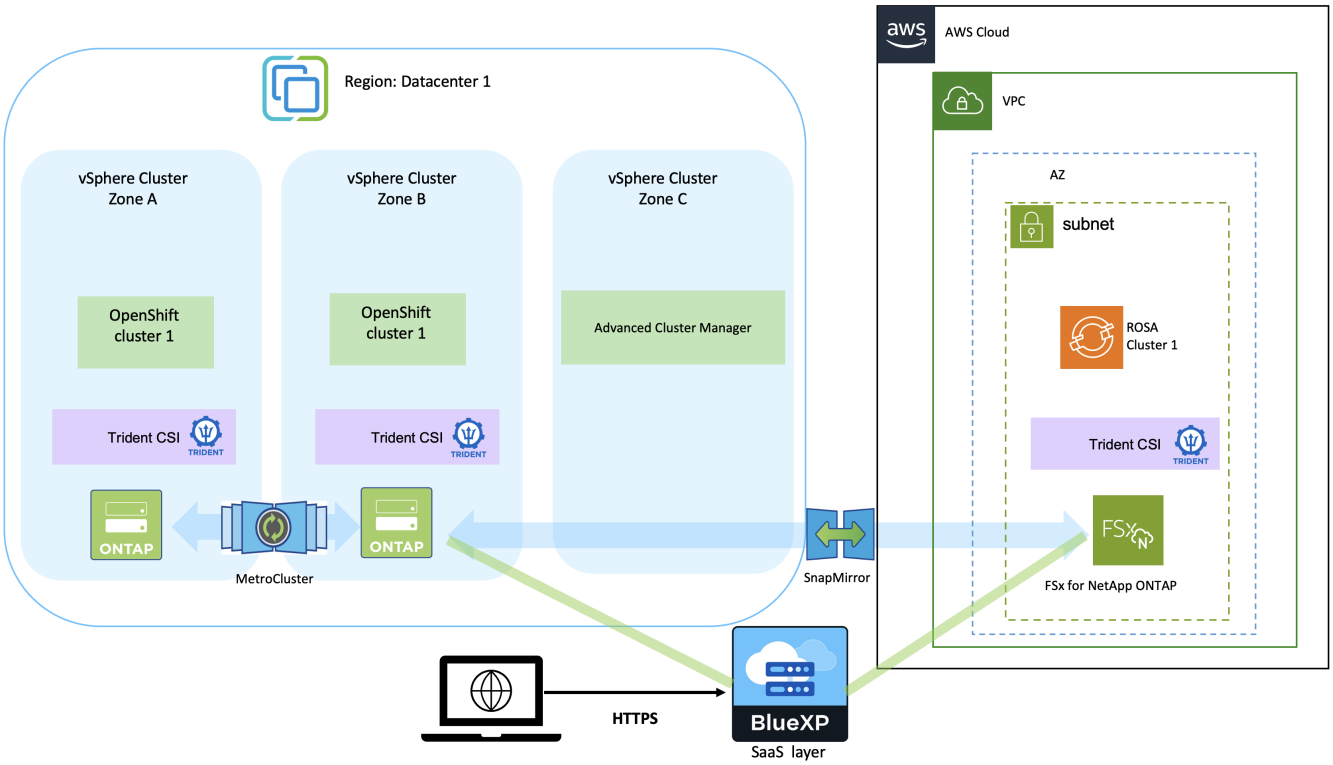


Scenario 3: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente AWS

In sede: cluster OpenShift autogestito e storage autogestito AWS Cloud: cluster OpenShift gestito dal provider (ROSA) e storage gestito dal provider (FSx ONTAP)

- Con NetApp Console, esegui la replica dei volumi persistenti (FSx ONTAP).
- Utilizzando OpenShift GitOps, ricrea i metadati dell'applicazione.

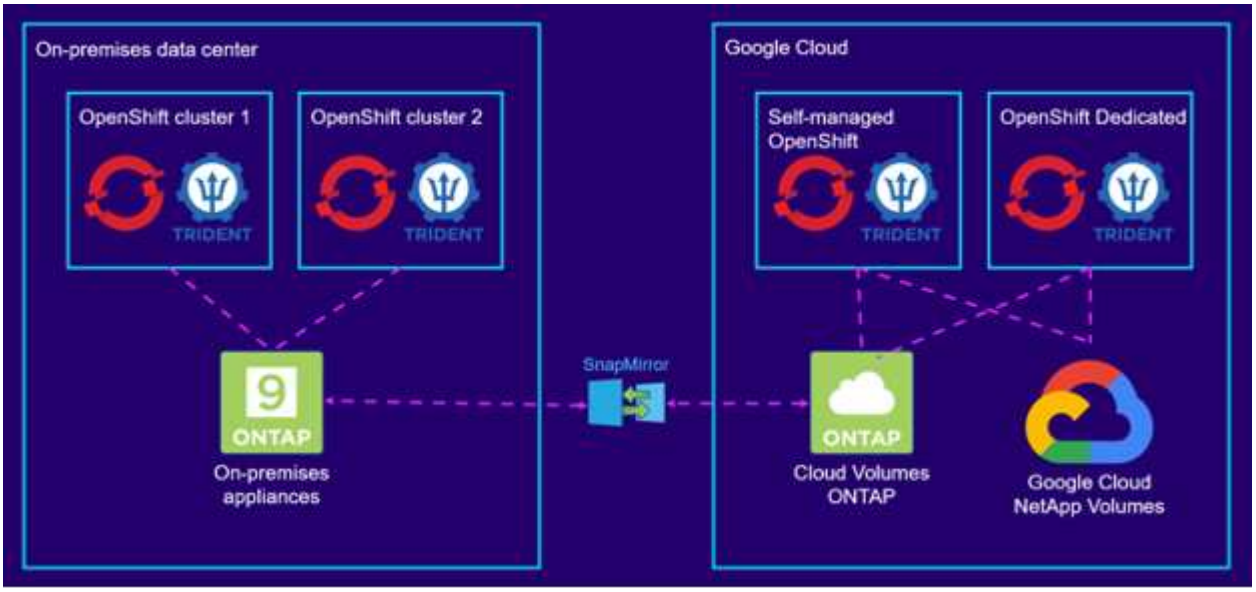
Scenario 3



Scenario 4: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente GCP tramite Trident Protect

In sede: cluster OpenShift autogestito e storage autogestito Google Cloud: cluster OpenShift autogestito e storage autogestito

- Utilizza Trident Protect per proteggere le applicazioni e supportare la migrazione tra i cluster on-premises e Google Cloud OpenShift.

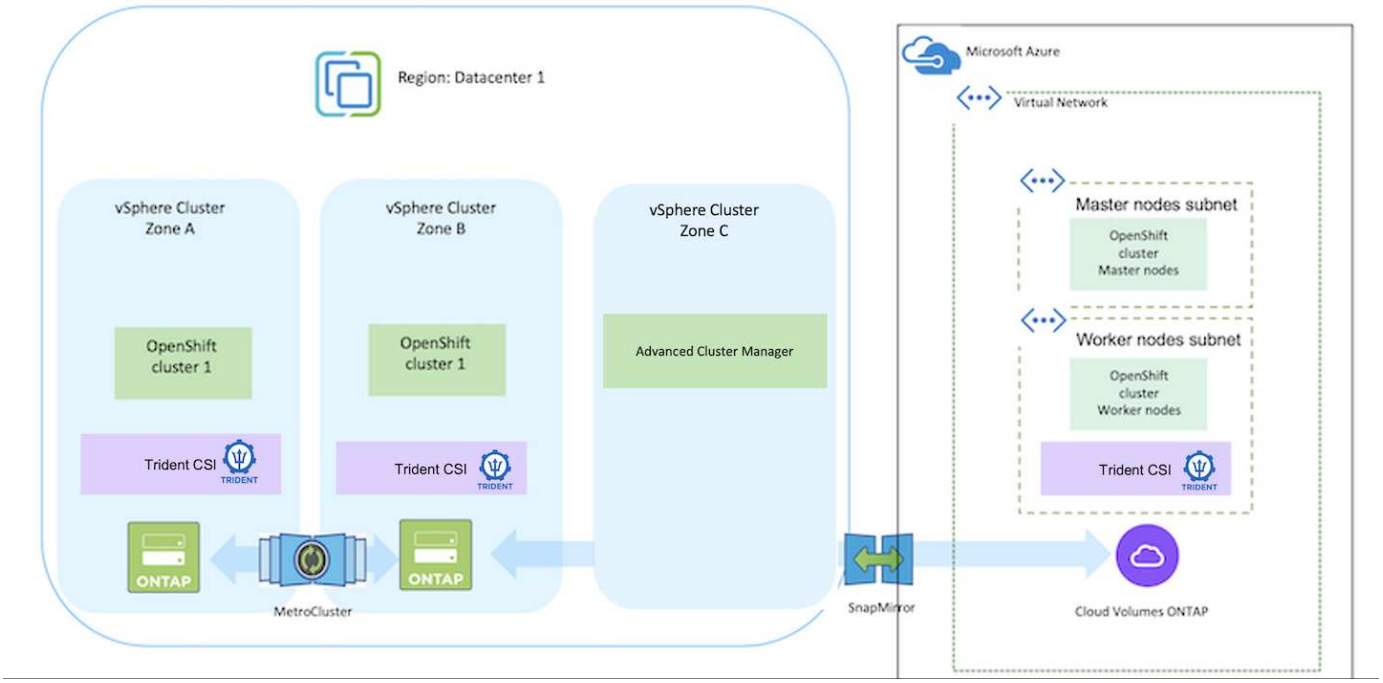


Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster , fare riferimento"Qui" .

Scenario 5: Protezione dei dati e migrazione dall'ambiente locale all'ambiente Azure tramite Trident Protect

In locale: cluster OpenShift autogestito e storage autogestito Azure Cloud: cluster OpenShift autogestito e storage autogestito

- Utilizza Trident Protect per proteggere le applicazioni e supportare la migrazione tra l'ambiente locale e i cluster OpenShift in Azure.



Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster , fare riferimento"Qui" .

Versioni di 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, OpenShift Advanced Cluster Manager, NetApp ONTAP e NetApp Trident Protect.

Gli scenari 1, 2 e 3 della soluzione sono stati convalidati utilizzando le versioni come mostrato nella tabella seguente:

Componente	Versione
VMware	vSphere Client versione 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cruiser Hub	OpenShift 4.11.34
Cluster di origine e destinazione	OpenShift 4.12.9 in locale e in AWS
* NetApp Trident*	Server e client Trident 23.04.0
* NetApp Trident Protect*	Trident Protect 22.11.0-82
* NetApp ONTAP*	ONTAP 9.12.1

AWS FSx ONTAP	Singolo AZ

Lo scenario 4 della soluzione è stato convalidato utilizzando le versioni come mostrato nella tabella seguente:

Componente	Versione
VMware	vSphere Client versione 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Cruiser Hub	OpenShift 4.13.13
Cluster di origine e destinazione	OpenShift 4.13.12 in locale e in Google Cloud
* NetApp Trident*	Trident Server e Client 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Singola AZ, Singolo nodo, 9.14.0

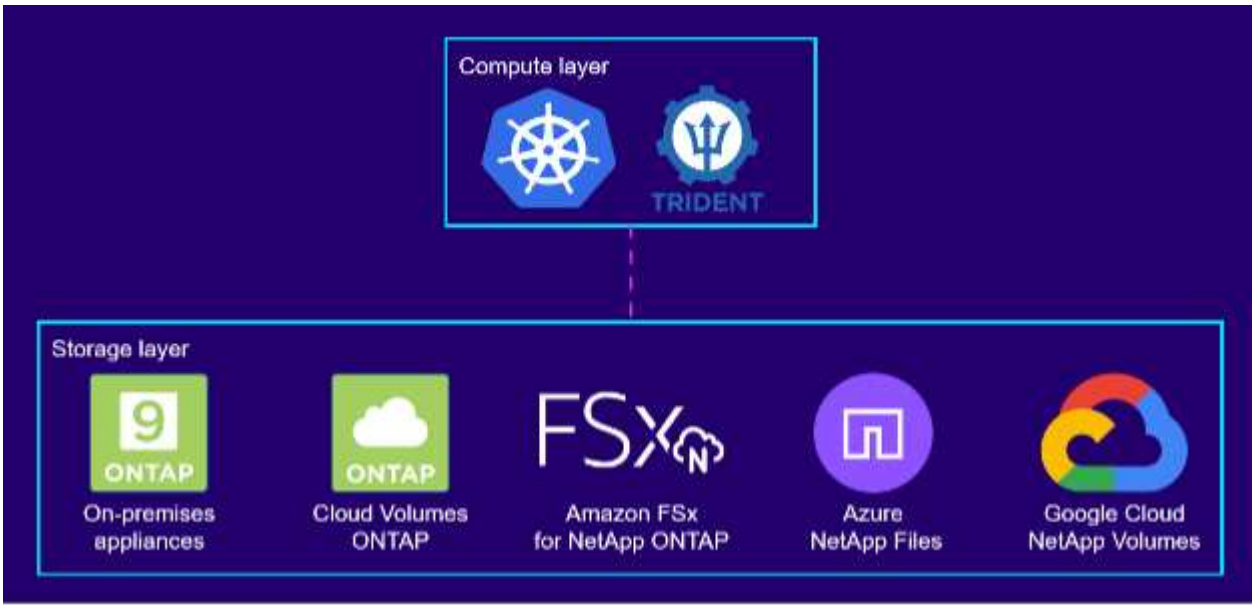
Lo scenario 5 della soluzione è stato convalidato utilizzando le versioni come mostrato nella tabella seguente:

Componente	Versione
VMware	vSphere Client versione 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Cluster di origine e destinazione	OpenShift 4.13.25 in locale e in Azure
* NetApp Trident*	Trident Server e Client 23.10.0
* NetApp Trident Protect*	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Singola AZ, Singolo nodo, 9.14.0

Integrazioni di NetApp Storage supportate con Red Hat OpenShift Containers

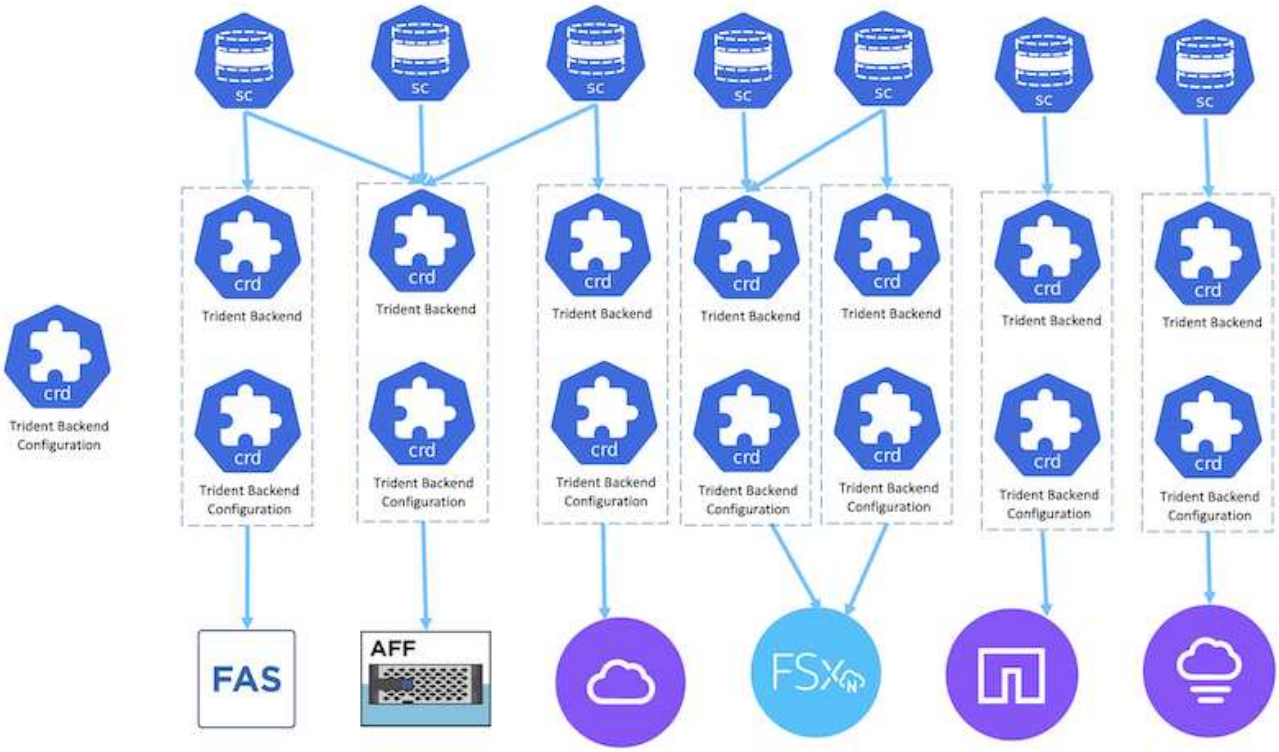
Indipendentemente dal fatto che i container Red Hat OpenShift siano in esecuzione su VMware o negli hyperscaler, NetApp Trident può essere utilizzato come provisioner CSI per i vari tipi di storage back-end NetApp supportati.

Il diagramma seguente illustra i vari storage backend NetApp che possono essere integrati con i cluster OpenShift utilizzando NetApp Trident.



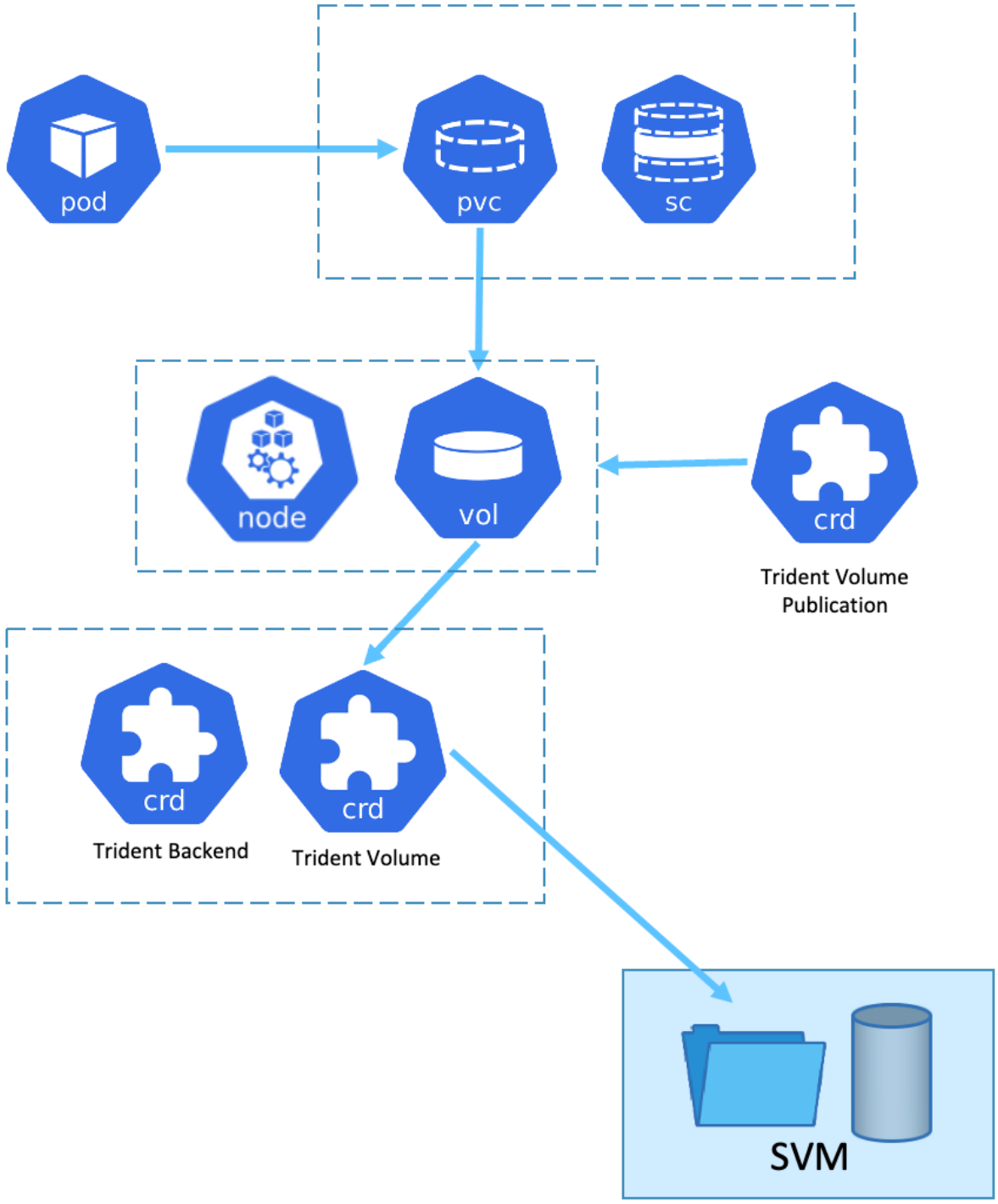
ONTAP Storage Virtual Machine (SVM) garantisce una multi-tenancy sicura. Un singolo cluster OpenShift può connettersi a una singola SVM o a più SVM o persino a più cluster ONTAP . La classe di archiviazione filtra l'archiviazione back-end in base ai parametri o alle etichette. Gli amministratori di storage definiscono i parametri per connettersi al sistema di storage utilizzando la configurazione backend Trident. Una volta stabilita la connessione, viene creato il backend Trident e vengono popolate le informazioni che la classe di archiviazione può filtrare.

Di seguito è illustrata la relazione tra storageclass e backend.



Il proprietario dell'applicazione richiede un volume persistente utilizzando la classe di archiviazione. La classe di archiviazione filtra l'archiviazione backend.

Di seguito è illustrata la relazione tra il pod e lo storage backend.



Opzioni dell'interfaccia di archiviazione dei container (CSI)

Negli ambienti vSphere, i clienti possono scegliere il driver VMware CSI e/o Trident CSI per l'integrazione con ONTAP. Con VMware CSI, i volumi persistenti vengono utilizzati come dischi SCSI locali, mentre con Trident vengono utilizzati tramite 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 distribuzioni basate su FC, si preferisce VMware CSI e

SnapMirror Business Continuity (SMBC) fornisce elevata disponibilità a livello di zona.

VMware CSI supporta

- Datastore basati su Core Block (FC, FCoE, iSCSI, NVMeoF)
- Archivi dati basati su file core (NFS v3, v4)
- Datastore vVol (blocco e file)

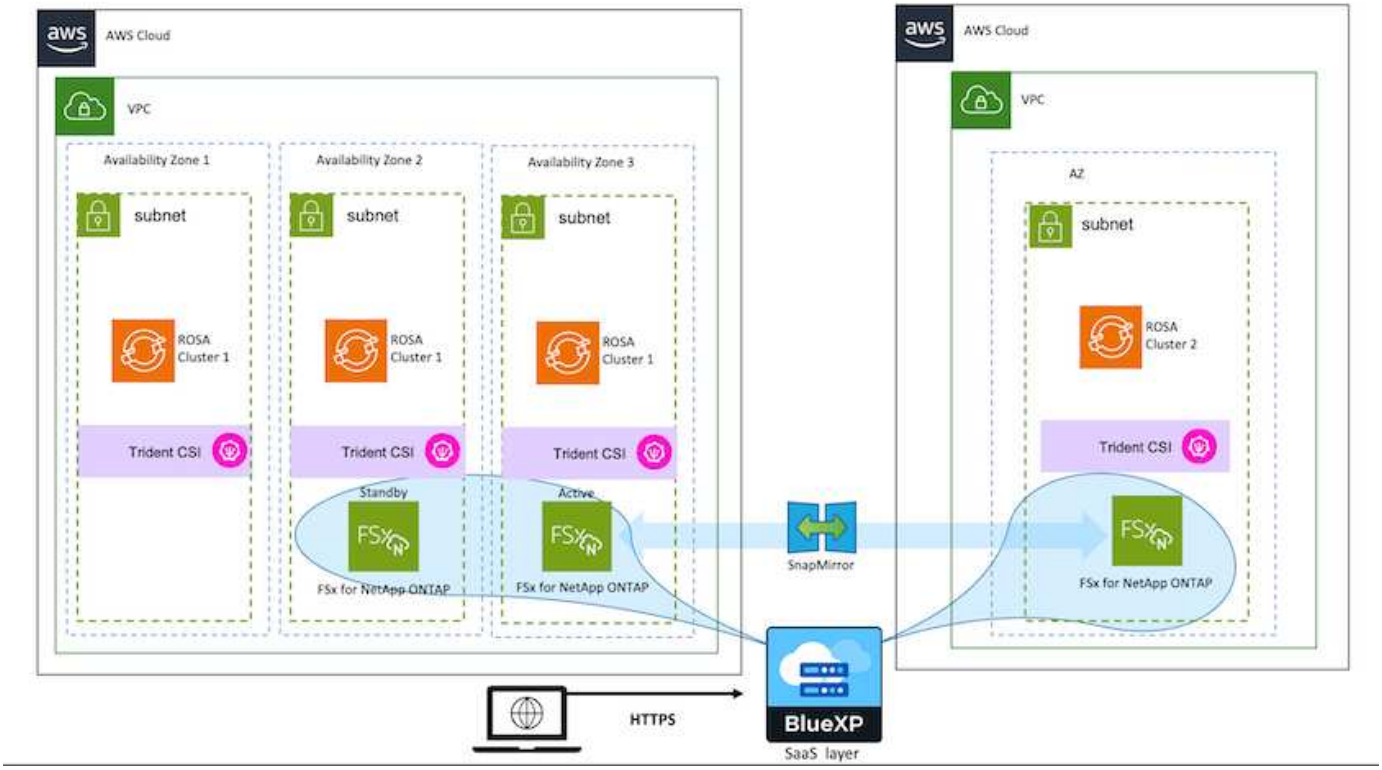
Trident ha i seguenti driver per supportare ONTAP

- 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)

Sia per VMware CSI che per Trident CSI, ONTAP supporta nconnect, session trunking, kerberos, ecc. per NFS e multipathing, autenticazione chap, ecc. per protocolli a blocchi.

In AWS, Amazon FSx for NetApp ONTAP (FSx ONTAP) può essere distribuito in una singola zona di disponibilità (AZ) o in più AZ. Per i carichi di lavoro di produzione che richiedono elevata disponibilità, la multi-AZ offre tolleranza agli errori a livello di zona e una cache di lettura NVMe migliore rispetto alla singola AZ. Per maggiori informazioni, controlla"Linee guida sulle prestazioni AWS" .

Per risparmiare sui costi del sito di disaster recovery, è possibile utilizzare un singolo AZ FSx ONTAP
.



Per il numero di SVM supportati da FSx ONTAP, fare riferimento"gestione della macchina virtuale di archiviazione FSx ONTAP"

Documentazione aggiuntiva

Ecco altra documentazione di riferimento:

1. "VMware vSphere"
2. "Documentazione del prodotto della piattaforma OpenShift Container"
3. "Installazione di cluster della piattaforma container OpenShift"
4. "Documentazione avanzata del prodotto di gestione dei cluster"
5. "Creazione di un cluster utilizzando ACM"
6. "Distribuzione di Red Hat Quay su OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda (Open source) offre una raccolta di hook di esecuzione di riferimento per le più diffuse applicazioni cloud native ad alta intensità di dati
10. "NetApp servizi dati"
11. "architettura classica di Red Hat OpenShift Service on AWS"
12. "Amazon FSx ONTAP"
13. "Installazione di OpenShift Clusters su GCP"
14. "Installazione di OpenShift Clusters su Azure"

Openshift per ambienti on-premise

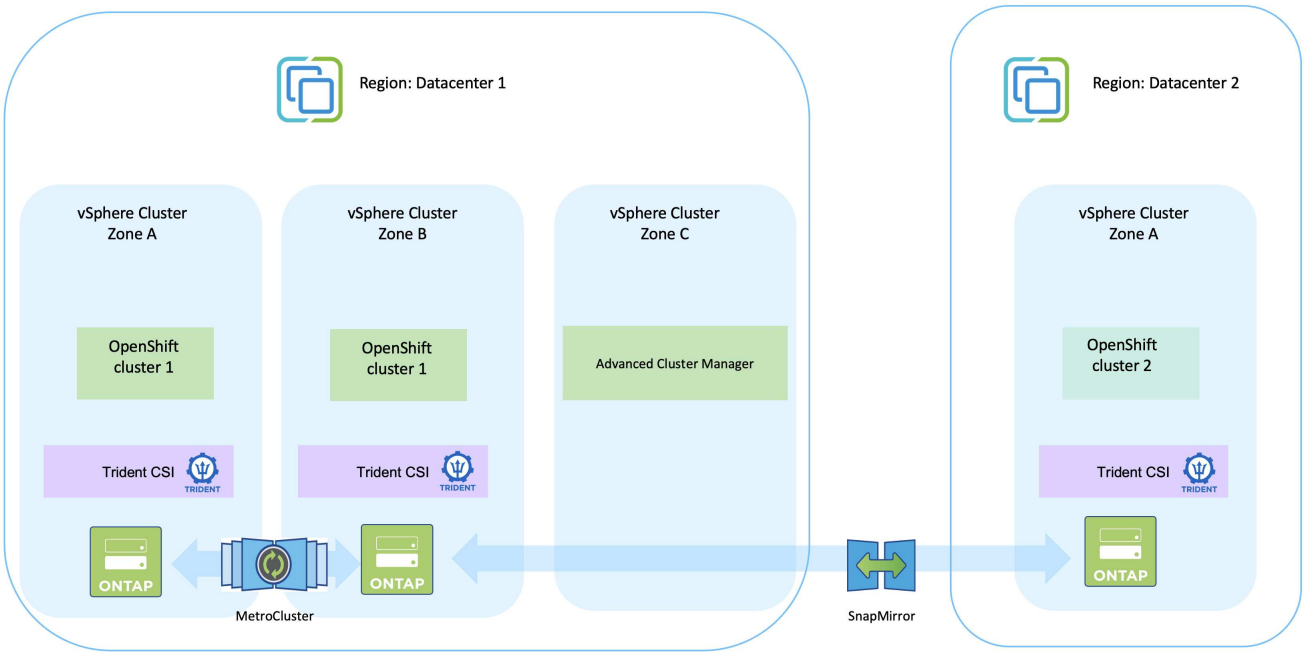
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware

Se i clienti hanno la necessità di eseguire le loro moderne applicazioni containerizzate sull'infrastruttura dei loro data center privati, possono farlo. Dovrebbero pianificare e distribuire la piattaforma container Red Hat OpenShift (OCP) per un ambiente di produzione di successo per la distribuzione dei carichi di lavoro dei container. I loro cluster OCP possono essere distribuiti su VMware o bare metal.

Lo storage NetApp ONTAP garantisce protezione dei dati, affidabilità e flessibilità per le distribuzioni di container. Trident funge da fornitore di storage dinamico per utilizzare lo storage ONTAP persistente per le applicazioni stateful dei clienti. NetApp Trident Protect può essere utilizzato per i numerosi requisiti di gestione dei dati delle applicazioni con stato, quali protezione dei dati, migrazione e continuità aziendale.

Con VMware vSphere, gli strumenti NetApp ONTAP forniscono un plug-in vCenter che può essere utilizzato per il provisioning degli archivi dati. Applica i tag e utilizzali con OpenShift per memorizzare la configurazione e i dati del nodo. L'archiviazione basata su NVMe garantisce una latenza inferiore e prestazioni elevate.

Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container utilizzando Trident Protect

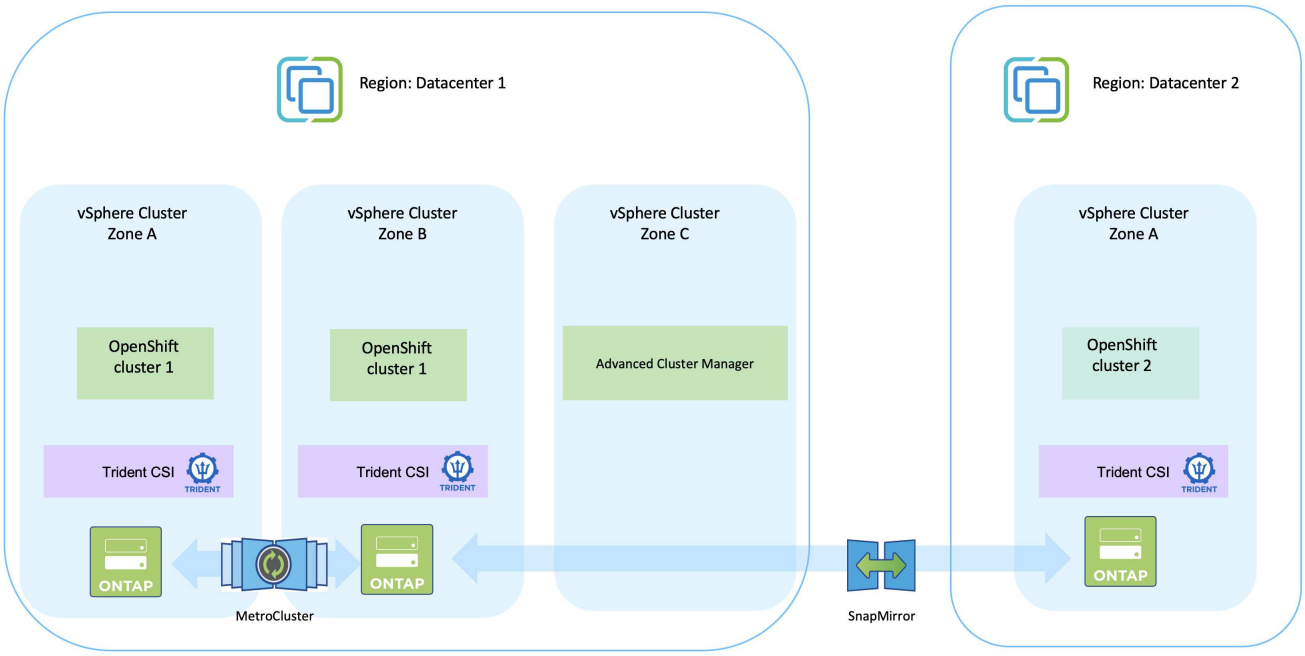


Distribuisci e configura la piattaforma Red Hat OpenShift Container su VMware

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift e le applicazioni con stato su di essi. Mostra l'utilizzo di array di storage NetApp ONTAP con l'ausilio di Trident per fornire volumi persistenti.

> Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Ecco un diagramma che illustra i cluster distribuiti su VMware in un data center.



Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Distribuisci e configura una VM CentOS**

- Viene distribuito nell'ambiente VMware vSphere.
- Questa VM viene utilizzata per distribuire alcuni componenti della soluzione, come NetApp Trident e NetApp Trident Protect.
- Durante l'installazione, su questa VM viene configurato un utente root.

▼ **Distribuisci e configura un cluster OpenShift Container Platform su VMware vSphere (Hub Cluster)**

Consulta le istruzioni per il metodo "Distribuzione assistita" per implementare un cluster OCP.

Ricordare quanto segue: - Creare una chiave pubblica e privata ssh da fornire al programma di installazione. Queste chiavi verranno utilizzate per accedere ai nodi master e worker, se necessario. - Scaricare il programma di installazione dall'installatore assistito. Questo programma viene utilizzato per avviare le VM create nell'ambiente VMware vSphere per i nodi master e worker. - Le VM devono avere i requisiti minimi di CPU, memoria e disco rigido. (Fare riferimento ai comandi vm create su"Questo" pagina per il master e i nodi worker che forniscono queste informazioni) - Il diskUUID deve essere abilitato su tutte le VM. - Creare almeno 3 nodi per il master e 3 nodi per il worker. - Una volta rilevati dal programma di installazione, attivare il pulsante di integrazione VMware vSphere.

▼ **Installa Advanced Cluster Management sul cluster Hub**

L'installazione avviene tramite l'Advanced Cluster Management Operator sul cluster Hub. Fare riferimento alle istruzioni"Qui" .

▼ **Installa due cluster OCP aggiuntivi (origine e destinazione)**

- I cluster aggiuntivi possono essere distribuiti utilizzando ACM sul cluster Hub.
- Fai riferimento alle istruzioni "Qui".

▼ **Configurare l'archiviazione NetApp ONTAP**

- Installare un cluster ONTAP con connettività alle VM OCP nell'ambiente VMWare.
- Creare una SVM.
- Configurare i dati NAS lif per accedere allo storage in SVM.

▼ **Installa NetApp Trident sui cluster OCP**

- Installa NetApp Trident su tutti e tre i cluster: hub, origine e destinazione
- Fai riferimento alle istruzioni "Qui".
- Creare un backend di archiviazione per ontap-nas.
- Creare una classe di archiviazione per ontap-nas.
- Fare riferimento alle istruzioni"Qui" .

▼ **Distribuire un'applicazione sul cluster di origine**

Utilizzare OpenShift GitOps per distribuire un'applicazione. (ad esempio Postgres, Ghost)

Il passaggio successivo consiste nell'utilizzare Trident Protect per la protezione dei dati e la migrazione dei dati dal cluster di origine a quello di destinazione. Fare riferimento"Qui" per istruzioni.

Protezione dei dati tramite Trident Protect

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su Red Hat OpenShift Container in esecuzione su VMware vSphere utilizzando Trident Protect.

Mentre gli utenti intraprendono il loro percorso di modernizzazione delle applicazioni con Red Hat OpenShift, dovrebbe essere prevista una strategia di protezione dei dati per proteggerli da cancellazioni accidentali o altri errori umani. Spesso una strategia di protezione è richiesta anche per motivi normativi o di conformità per proteggere i loro dati da un disastro.

I requisiti di protezione dei dati variano dal ripristino di una copia in un dato momento al failover automatico su 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 numerose funzionalità, come multitenancy, multiprotocollo, elevate prestazioni e capacità, replicazione e memorizzazione nella cache per sedi multi-sito, sicurezza e flessibilità.

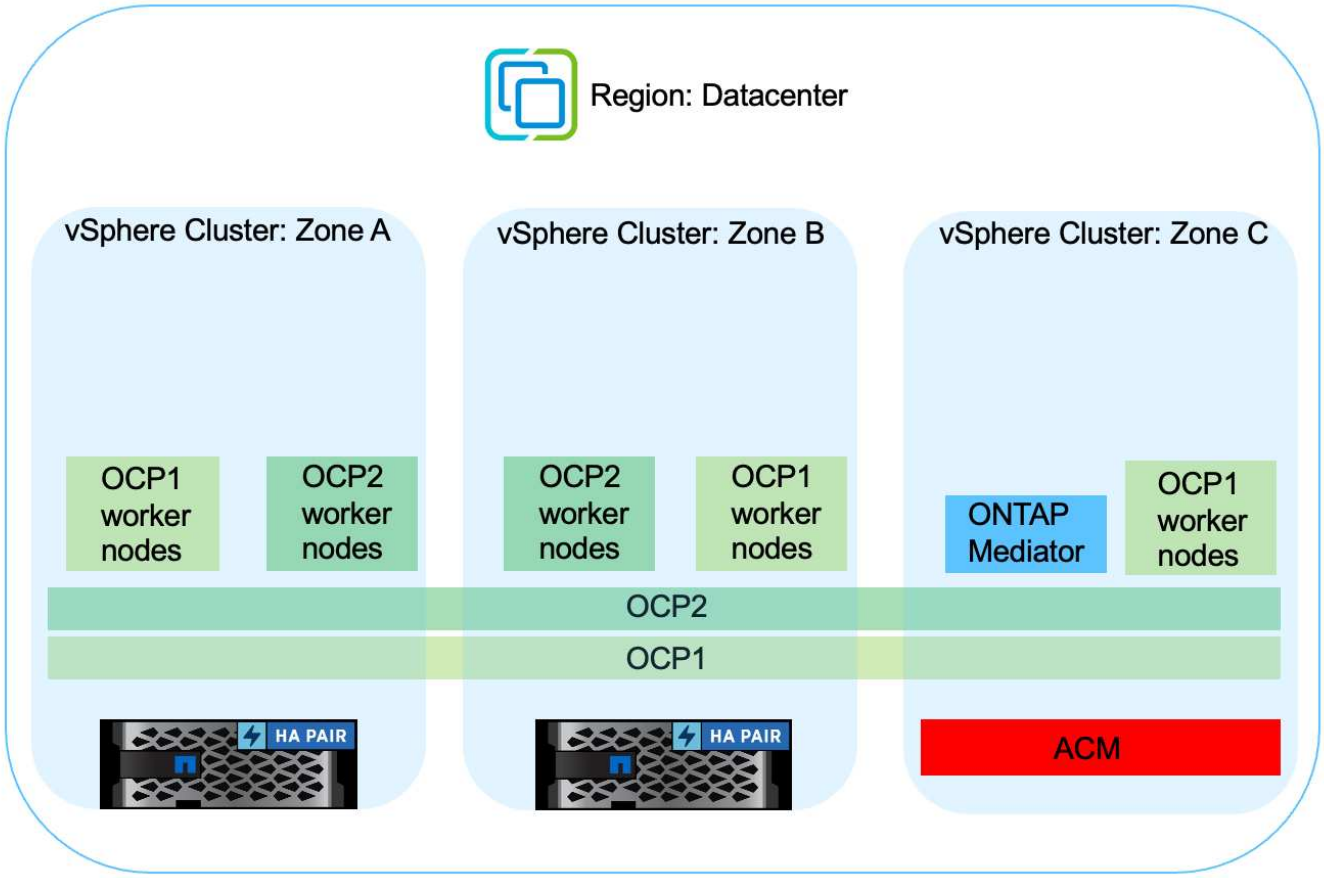
Per dettagli sulla protezione e la migrazione dei carichi di lavoro dei container utilizzando Trident Protect, consultare la seguente sezione: - "Proteggi e migra le app Container utilizzando Trident Protect"

Continuità aziendale con MetroCluster

La maggior parte della nostra piattaforma hardware per ONTAP è dotata di funzionalità di elevata disponibilità per proteggere i dispositivi dai guasti, evitando la necessità di eseguire il ripristino di emergenza. Tuttavia, per proteggersi da incendi o altri disastri e continuare l'attività con RPO pari a zero e RTO basso, spesso si ricorre alla soluzione MetroCluster .

I clienti che attualmente dispongono di un sistema ONTAP possono estenderlo a MetroCluster aggiungendo sistemi ONTAP supportati entro i limiti di distanza per fornire il ripristino di emergenza a livello di zona. Trident, CSI (Container Storage Interface), supporta NetApp ONTAP, inclusa la configurazione MetroCluster , nonché altre opzioni come Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, ecc. Trident fornisce cinque opzioni di driver di archiviazione per ONTAP e sono tutte supportate per la configurazione MetroCluster . Fare riferimento"Qui" per ulteriori dettagli sui driver di archiviazione ONTAP supportati da Trident.

La soluzione MetroCluster richiede un'estensione di rete di livello 2 o la capacità di accedere allo stesso indirizzo di rete da entrambi i domini di errore. Una volta configurata MetroCluster , la soluzione è trasparente per i proprietari delle applicazioni, poiché tutti i volumi nella svm MetroCluster sono protetti e beneficiano dei vantaggi di SyncMirror (RPO zero).



Per la configurazione Trident Backend (TBC), non specificare dataLIF e SVM quando si utilizza la configurazione MetroCluster . Specificare l'IP di gestione SVM per managementLIF e utilizzare le credenziali del ruolo vsadmin.

Sono disponibili dettagli sulle funzionalità di protezione dei dati di Trident Protect "Qui".

Cloud ibrido con componenti autogestiti

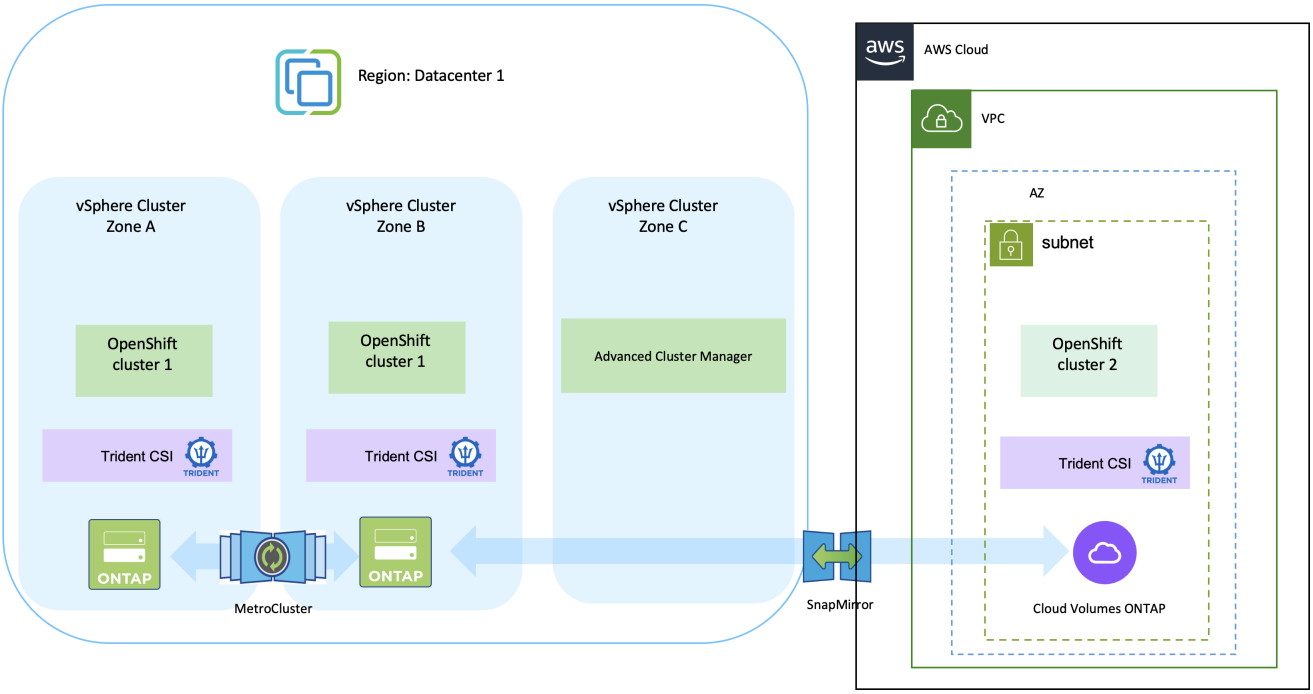
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido

I clienti potrebbero trovarsi a un punto del loro percorso di modernizzazione in cui sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i carichi di lavoro dai loro data center al cloud. Possono scegliere di utilizzare container OpenShift autogestiti e storage NetApp autogestito nel cloud per vari motivi. Dovrebbero pianificare e distribuire la piattaforma container Red Hat OpenShift (OCP) nel cloud per creare un ambiente di produzione di successo per la migrazione dei carichi di lavoro dei container dai loro data center. I loro cluster OCP possono essere distribuiti su VMware o Bare Metal nei loro data center e su AWS, Azure o Google Cloud nell'ambiente cloud.

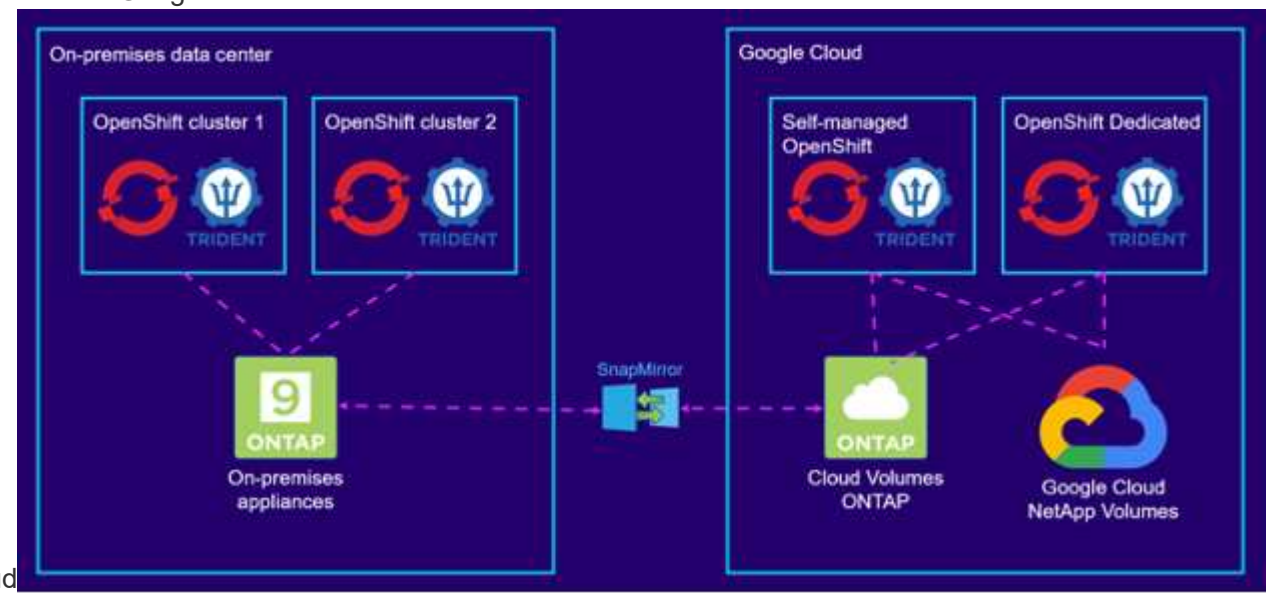
NetApp Cloud Volumes ONTAP storage offre protezione dei dati, affidabilità e flessibilità per le distribuzioni di container in AWS, Azure e Google Cloud. Trident funge da dynamic storage provisioner per consumare lo storage persistente Cloud Volumes ONTAP per le applicazioni stateful dei clienti. Trident Protect può essere utilizzato per i requisiti di gestione dei dati delle applicazioni stateful, come protezione dei dati, migrazione e continuità aziendale.

Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container in un cloud ibrido utilizzando Trident Protect

In locale e
AWS

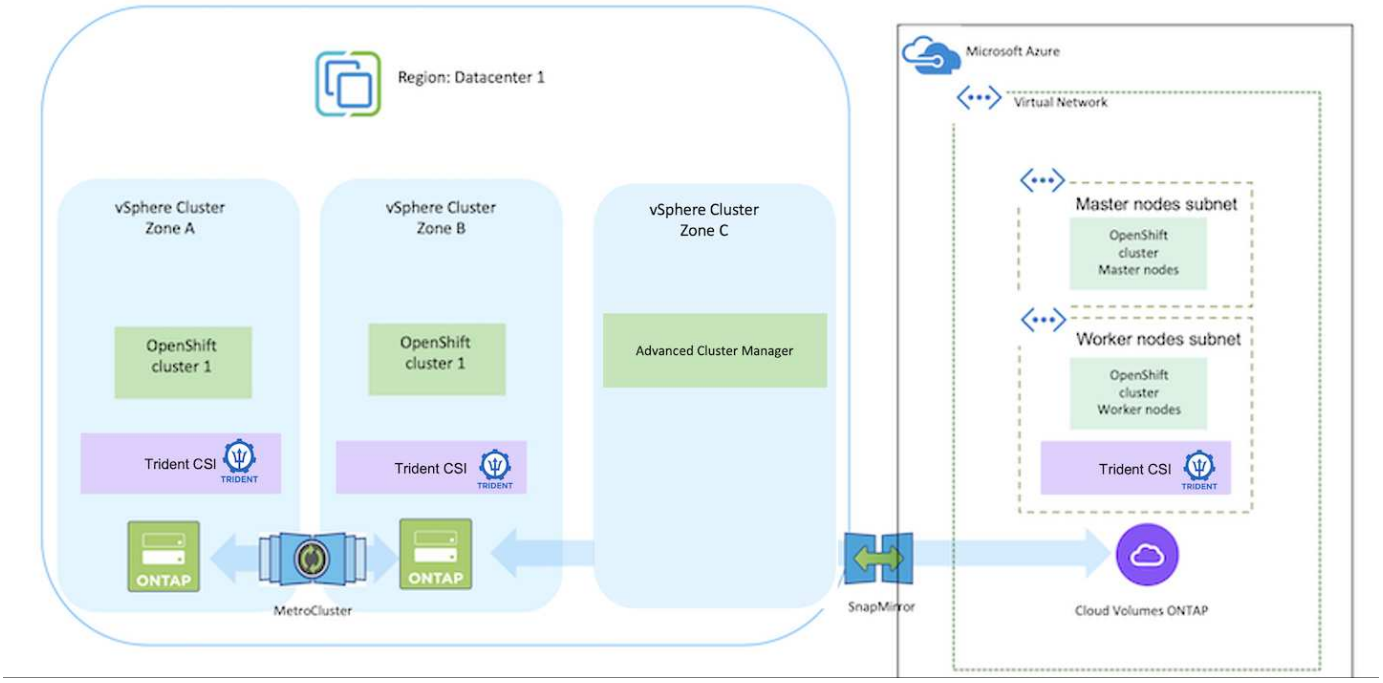


In locale e su Google



Cloud

In locale e nel cloud di

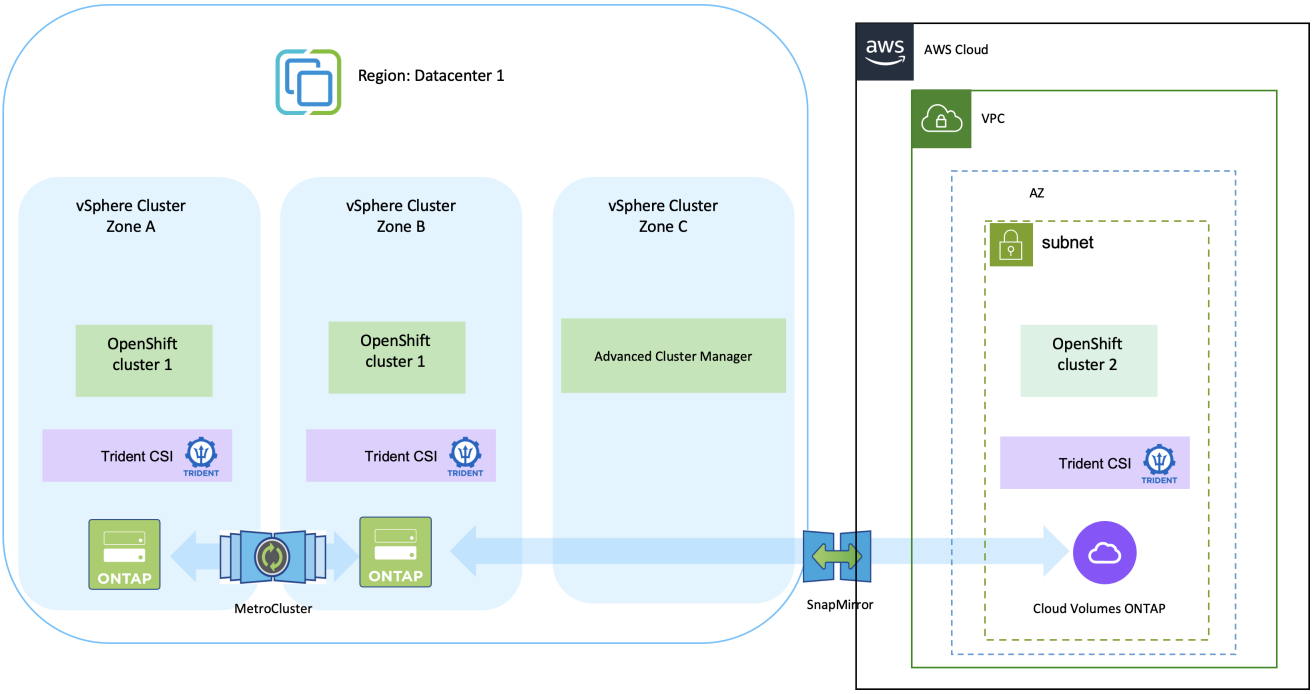


Distribuisci e configura la piattaforma Red Hat OpenShift Container su AWS

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in AWS e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Trident Protect per eseguire attività di protezione e migrazione dei dati per le applicazioni con stato.

Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container su AWS. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Ecco un diagramma che illustra i cluster distribuiti su AWS e connessi al data center tramite una VPN.



Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Installa un cluster OCP su AWS da Advanced Cluster Management.**

- Crea una VPC con una connessione VPN da sito a sito (utilizzando pfsense) per connetterti alla rete locale.
- La rete locale è dotata di connettività Internet.
- Crea 3 subnet private in 3 diverse zone di disponibilità.
- Creare una zona ospitata privata Route 53 e un resolver DNS per la VPC.

Crea un cluster OpenShift su AWS dalla procedura guidata di Advanced Cluster Management (ACM). Consulta le istruzioni "Qui".

Puoi anche creare il cluster in AWS dalla console Hybrid Cloud di OpenShift. Consulta "Qui" per le istruzioni.

Quando si crea il cluster tramite ACM, è possibile personalizzare l'installazione modificando il file yaml dopo aver compilato i dettagli nella visualizzazione del modulo. Dopo aver creato il cluster, è possibile effettuare l'accesso tramite SSH ai nodi del cluster per la risoluzione dei problemi o per ulteriori configurazioni manuali. Utilizza la chiave ssh fornita durante l'installazione e il nome utente core per effettuare l'accesso.

▼ **Distribuisci Cloud Volumes ONTAP in AWS tramite NetApp Console.**

- Installare il connettore nell'ambiente VMware locale. Fare riferimento alle istruzioni"Qui" .
- Distribuisci un'istanza CVO in AWS utilizzando il connettore. Fare riferimento alle istruzioni"Qui" .

Il connettore può essere installato anche nell'ambiente cloud. Fare riferimento"Qui" per ulteriori informazioni.

▼ **Installa Trident nel cluster OCP**

- Distribuisci Trident Operator tramite Helm. Consulta le istruzioni "Qui"
- Creare un backend e una classe di archiviazione. Fare riferimento alle istruzioni"Qui" .

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

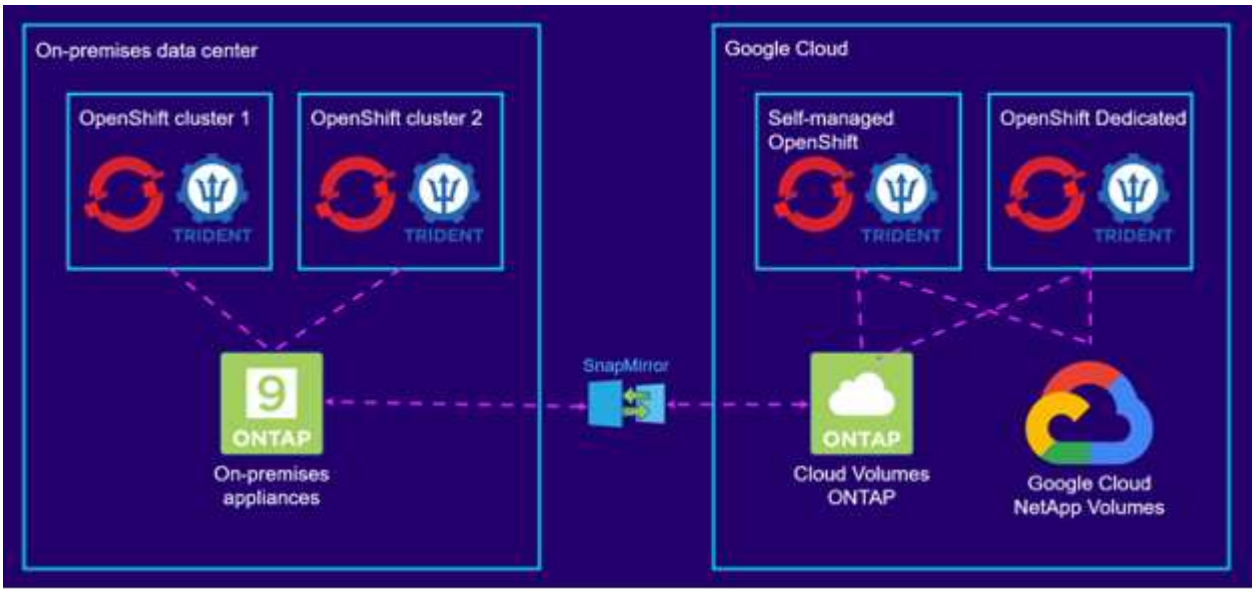
Oggi i provider cloud consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi di cluster basati su zone. I nodi possono essere ubicati in diverse zone di disponibilità all'interno di una regione o tra regioni diverse. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multizona, Trident utilizza la topologia CSI. Utilizzando la funzionalità CSI Topology, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle regioni e alle zone di disponibilità. Fare riferimento"Qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Distribuisci e configura la piattaforma container Red Hat OpenShift su Google Cloud

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in GCP e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage Google Cloud NetApp Volumes e NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti.

Ecco un diagramma che mostra i cluster distribuiti su GCP e connessi al data center tramite una VPN.



Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container in GCP. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

Installa un cluster OCP su GCP dalla CLI

- Assicurati di aver soddisfatto tutti i prerequisiti indicati "Qui".
- Per la connettività VPN tra locale e GCP, è stata creata e configurata una VM pfsense. Per le 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 di rete remoti per la Fase 2 possono essere configurati solo dopo l'esecuzione del programma di installazione del cluster OpenShift e la creazione dei componenti infrastrutturali per il cluster.
  - La VPN in Google Cloud può essere configurata solo dopo che i componenti dell'infrastruttura per il cluster sono stati creati dal programma di installazione.
- Ora installa il cluster OpenShift su GCP.
  - Ottieni il programma di installazione e il pull secret e distribuisci il cluster seguendo i passaggi indicati nella documentazione "Qui".
  - L'installazione crea una rete VPC in Google Cloud Platform. Crea anche una zona privata in Cloud DNS e aggiunge record A.
    - 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 record A nel DNS dell'ambiente locale utilizzando l'indirizzo IP nei record A del DNS di Google Cloud.
  - L'installazione del cluster è completata e verranno forniti un file kubeconfig, nonché nome utente e password per accedere alla console del cluster.

Distribuisci Google Cloud NetApp Volumes

- Google Cloud NetApp Volumes può essere aggiunto ai tuoi progetti come descritto"Qui" .

Distribuisci Cloud Volumes ONTAP in GCP utilizzando NetApp Console

- Installa un agente Console in Google Cloud. Consulta le istruzioni "Qui".
- Distribuisci un'istanza CVO in Google Cloud utilizzando l'agente. Consulta le istruzioni "Qui".

Installa Trident nel cluster OCP in GCP

- Esistono molti metodi per implementare Trident, come mostrato "Qui".
- Per questo progetto, hai installato Trident distribuendo manualmente Trident Operator seguendo le istruzioni "Qui".
- Creare classi di backend e di archiviazione. Fare riferimento alle istruzioni"Qui" .

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

Oggi i provider cloud consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi di cluster basati su zone. I nodi possono essere ubicati in diverse zone di disponibilità all'interno di una regione o tra regioni diverse. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multizona,

Trident utilizza la topologia CSI. Utilizzando la funzionalità CSI Topology, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle regioni e alle zone di disponibilità. Fare riferimento"Qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Video dimostrativo

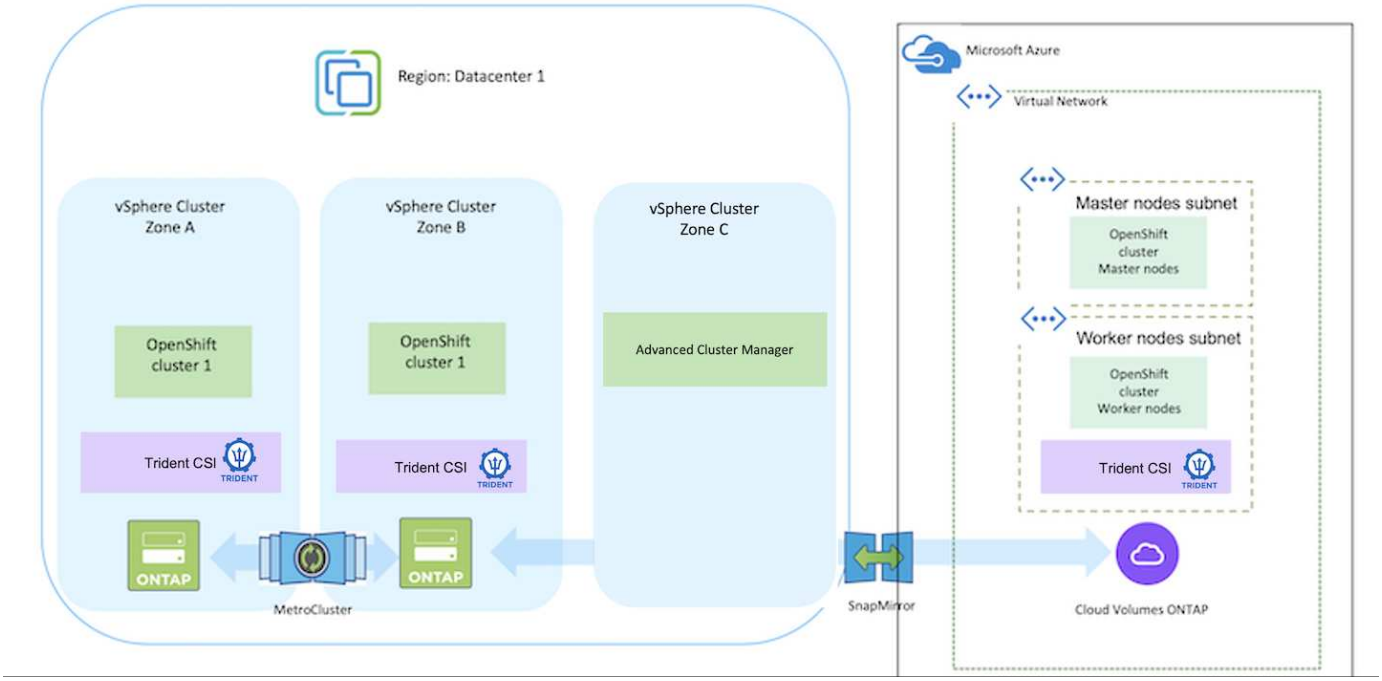
Installazione di OpenShift Cluster su Google Cloud Platform

Importazione di cluster OpenShift in Trident Protect

Distribuisci e configura la piattaforma Red Hat OpenShift Container su Azure

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in Azure e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Trident Protect per eseguire attività di protezione e migrazione dei dati per le applicazioni con stato.

Ecco un diagramma che mostra i cluster distribuiti su Azure e connessi al data center tramite una VPN.



Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container in Azure. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Installare un cluster OCP su Azure dalla CLI.**

- Assicurati di aver soddisfatto tutti i prerequisiti indicati "Qui".
- Creare una VPN, subnet e gruppi di sicurezza di rete e una zona DNS privata. Crea un gateway VPN e una connessione VPN da sito a sito.
- Per la connettività VPN tra locale e Azure, è stata creata e configurata una VM pfsense. Per le istruzioni, vedere"Qui" .
- Ottieni il programma di installazione e il pull secret e distribuisci il cluster seguendo i passaggi indicati nella documentazione "Qui".
- L'installazione del cluster è completata e verranno forniti un file kubeconfig, nonché nome utente e 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:
```

▼ **Distribuisci Cloud Volumes ONTAP in Azure utilizzando NetApp Console.**

- Installa un agente NetApp Console in Azure. Fai riferimento alle istruzioni "Qui".
- Distribuisci un'istanza CVO in Azure utilizzando l'agente. Consulta le istruzioni "Qui".

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

Oggi i provider cloud consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi di cluster basati su zone. I nodi possono essere ubicati in diverse zone di disponibilità all'interno di una regione o tra regioni diverse. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multizona, Trident utilizza la topologia CSI. Utilizzando la funzionalità CSI Topology, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle regioni e alle zone di disponibilità. Fare riferimento"Qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Protezione dei dati tramite Trident Protect

Per dettagli sulla protezione e la migrazione dei carichi di lavoro dei container utilizzando Trident Protect, consultare la seguente sezione: - "Proteggi e migra le app Container utilizzando Trident Protect"

Cloud ibrido con componenti gestiti dal provider

Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift gestiti

I clienti potrebbero essere "nati nel cloud" oppure trovarsi in una fase del loro percorso di modernizzazione in cui sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i

carichi di lavoro dai loro data center al cloud. Possono scegliere di utilizzare container OpenShift gestiti dal provider e storage NetApp gestito dal provider nel cloud per eseguire i propri carichi di lavoro. Dovrebbero pianificare e distribuire i cluster di container Managed Red Hat OpenShift nel cloud per creare un ambiente di produzione di successo per i loro carichi di lavoro di container. NetApp fornisce soluzioni di storage completamente gestite per le soluzioni Managed Red Hat in tutti e tre i principali cloud pubblici.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP garantisce protezione dei dati, affidabilità e flessibilità per le distribuzioni di container in AWS. Trident funge da fornitore di storage dinamico per utilizzare lo storage FSx ONTAP persistente per le applicazioni con stato dei clienti.

Poiché ROSA può essere distribuito in modalità HA con nodi del piano di controllo distribuiti su più zone di disponibilità, FSx ONTAP può anche essere fornito con l'opzione Multi-AZ che fornisce elevata disponibilità e protezione contro i guasti AZ.

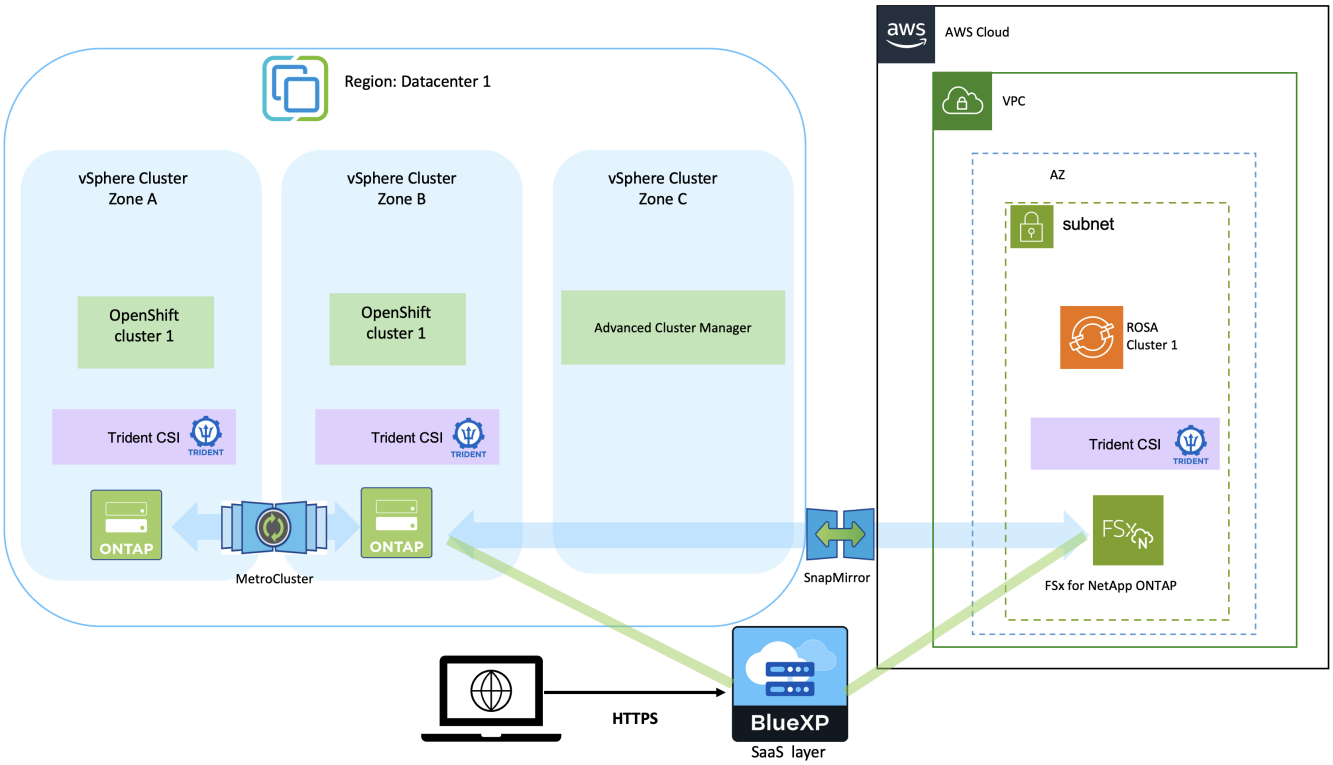
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated è una piattaforma applicativa completamente gestita che consente di creare, distribuire e scalare rapidamente le applicazioni nel cloud ibrido. Google Cloud NetApp Volumes fornisce volumi persistenti, portando la suite completa delle funzionalità di gestione dei dati aziendali di ONTAP alle distribuzioni OpenShift in Google Cloud.

Distribuisci e configura la piattaforma Managed Red Hat OpenShift Container su AWS

Questa sezione descrive un flusso di lavoro high-level per la configurazione dei cluster Managed Red Hat OpenShift su AWS (ROSA). Illustra l'utilizzo di Amazon FSx for NetApp ONTAP (FSx ONTAP) gestito come backend di storage da Trident per fornire volumi persistenti. Vengono forniti dettagli sul deployment di FSx ONTAP su AWS utilizzando NetApp Console. Inoltre, vengono forniti dettagli sull'utilizzo di NetApp Console e OpenShift GitOps (Argo CD) per eseguire attività di protezione e migrazione dei dati per le applicazioni stateful sui cluster ROSA.

Ecco un diagramma che illustra i cluster ROSA distribuiti su AWS e che utilizzano FSx ONTAP 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 FSx ONTAP utilizzando Trident. Esistono diversi modi per distribuire cluster ROSA e FSx ONTAP in AWS. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

Installare i cluster ROSA

- Crea due VPC e configura la connettività peering VPC tra le VPC.
- Consulta "Qui" per le istruzioni per installare i cluster ROSA.

Installa FSx ONTAP

- Installa FSx ONTAP sulle VPC da NetApp Console. Fai riferimento a "Qui" per la creazione dell'account NetApp Console e per iniziare. Fai riferimento a "Qui" per installare FSx ONTAP. Fai riferimento a "Qui" per creare un connettore in AWS per gestire FSx ONTAP.
- Distribuisci FSx ONTAP utilizzando AWS. Fare riferimento"Qui" per la distribuzione tramite la console AWS.

Installa Trident sui cluster ROSA (utilizzando il grafico Helm)

- Utilizza un Helm chart per installare Trident sui cluster ROSA. Consulta il link alla documentazione: qui.

Integrazione di FSx ONTAP con Trident per cluster ROSA

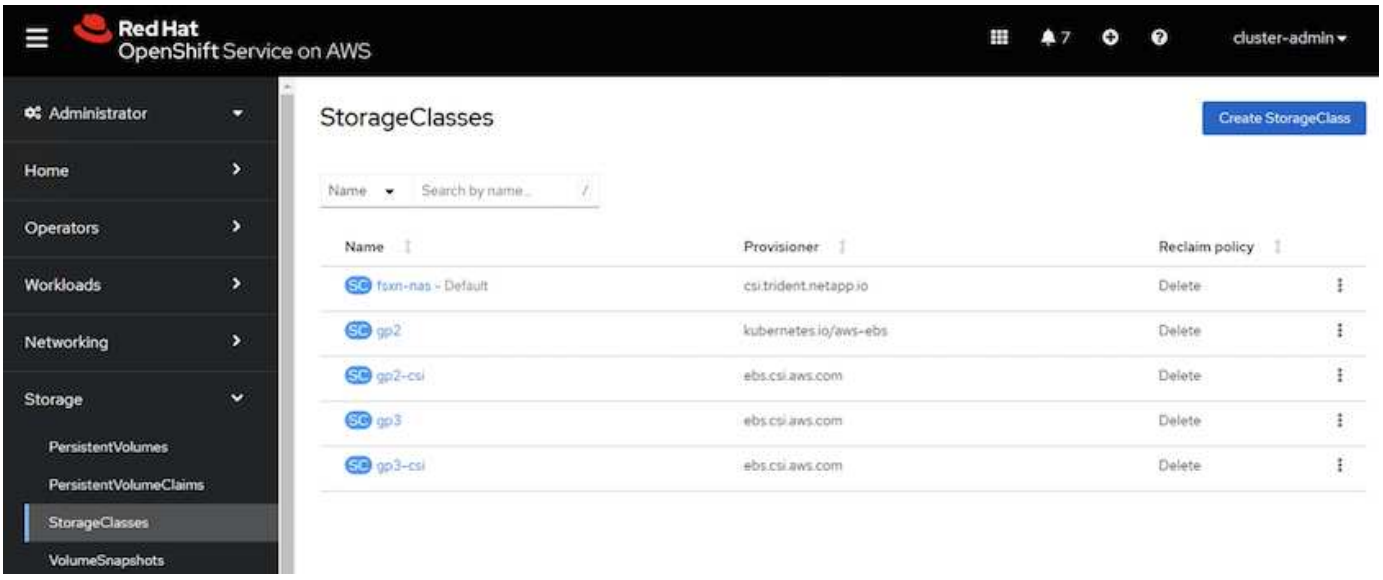
OpenShift GitOps può essere utilizzato per distribuire Trident CSI su tutti i cluster gestiti non appena vengono registrati su ArgoCD tramite ApplicationSet.

```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 backend e storage utilizzando Trident (per FSx ONTAP)

- Fare riferimento"Qui" per i dettagli sulla creazione di classi di backend e storage.
- Imposta come predefinita la classe di archiviazione creata per FsxN con Trident CSI dalla console OpenShift. Vedi screenshot qui sotto:



Distribuisci un'applicazione utilizzando OpenShift GitOps (Argo CD)

- Installa l'operatore OpenShift GitOps sul cluster. Consulta le istruzioni "Qui".
- SetUp una nuova istanza di Argo CD per il cluster. Consulta le istruzioni "Qui".

Apri la console di Argo CD e distribuisci un'app. Ad esempio, puoi distribuire un'app Jenkins utilizzando Argo CD con un Helm Chart. Quando crei l'applicazione, fornisci i seguenti dettagli: Project: default cluster:

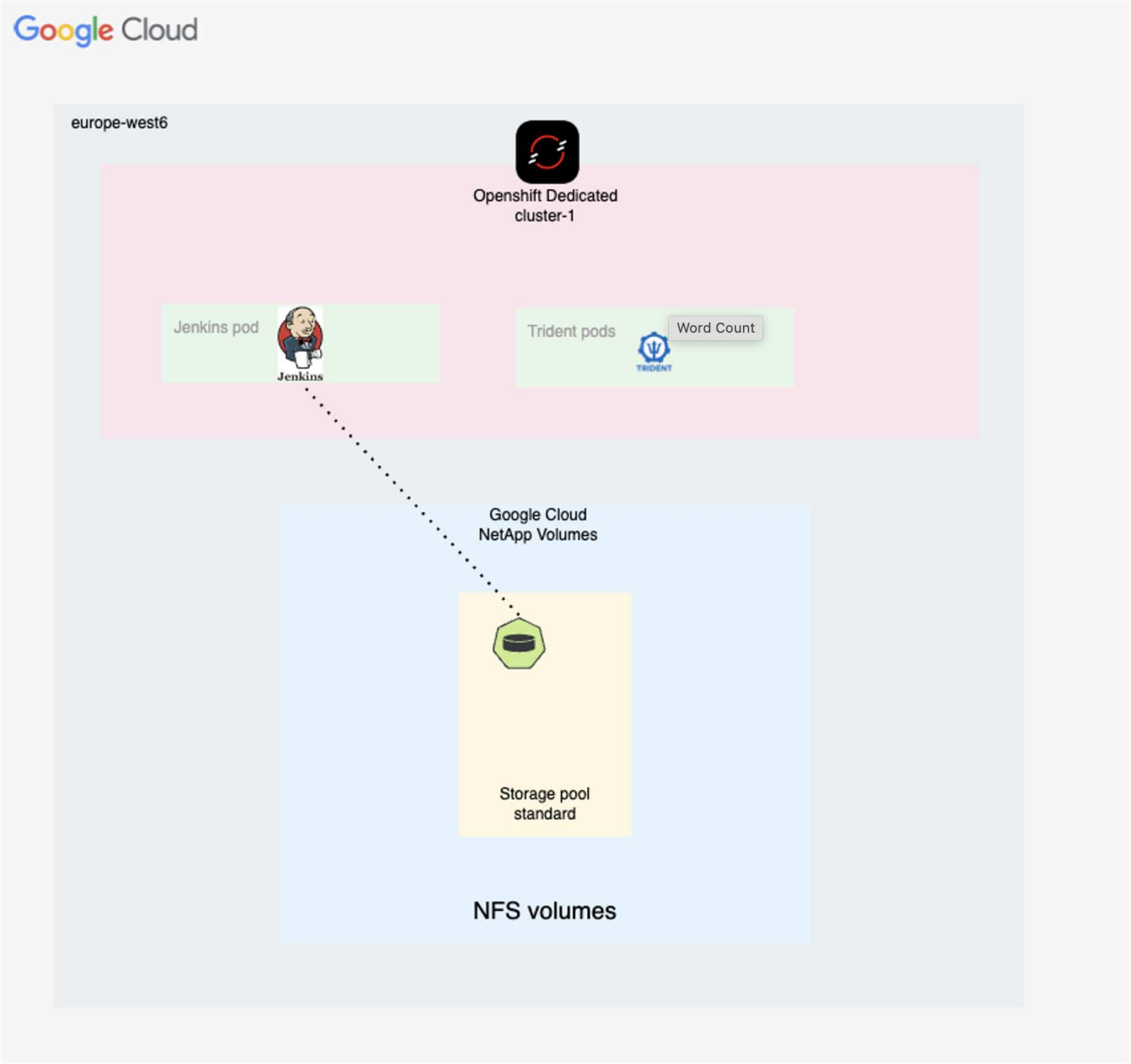
'https://kubernetes.default.svc'[] (senza virgolette) Namespace: Jenkins L'url per l'Helm Chart: 'https://charts.bitnami.com/bitnami'[] (senza virgolette)

Parametri Helm: global.storageClass: fsxn-nas

Distribuisci e configura OpenShift Dedicated su Google Cloud con Google Cloud NetApp Volumes

Questa sezione descrive un flusso di lavoro di alto livello per la configurazione di cluster OpenShift Dedicated (OSD) sulla piattaforma Google Cloud. Mostra NetApp Trident che utilizza Google Cloud NetApp Volumes come backend di archiviazione per fornire volumi persistenti per applicazioni con stato eseguite con Kubernetes.

Ecco un diagramma che illustra un cluster OSD distribuito su Google Cloud e che utilizza NetApp Volumes come storage back-end.



Il processo di configurazione può essere suddiviso nei seguenti passaggi:

Installa i cluster OSD in Google Cloud

- Se si desidera utilizzare una VPC esistente per il cluster, è necessario creare la VPC, due subnet, un router cloud e due NAT cloud GCP per il cluster OSD. Fare riferimento"Qui" per istruzioni.
- Consulta "Qui" per istruzioni su come installare i cluster OSD su GCP utilizzando il modello di fatturazione Customer Cloud Subscription (CCS). OSD è incluso anche in Google Cloud Marketplace. Un video che mostra come installare OSD utilizzando la soluzione Google Cloud Marketplace si trova "Qui".

Abilita Google Cloud NetApp Volumes

- Fare riferimento"Qui" per informazioni sulla configurazione dell'accesso a Google Cloud NetApp Volumes. Segui tutti i passaggi fino a e incluso
- Creare un pool di archiviazione. Fare riferimento"Qui" per informazioni su come configurare un pool di archiviazione su Google Cloud NetApp Volumes. I volumi per le applicazioni Kubernetes con stato in esecuzione su OSD verranno creati all'interno del pool di archiviazione.

Installa Trident sui cluster OSD (utilizzando la tabella Helm)

- Utilizza un Helm chart per installare Trident sui cluster OSD. Consulta "Qui" per le istruzioni su come installare l'Helm chart.

Integrazione di NetApp Volumes con NetApp Trident per cluster OSD

Crea classi di backend e storage utilizzando Trident (per Google Cloud NetApp Volumes)

- Per i dettagli sulla creazione del backend, fare riferimento qui.
- Se una qualsiasi delle classi di archiviazione correnti in Kubernetes è contrassegnata come predefinita, rimuovere l'annotazione modificando la classe di archiviazione.
- Creare almeno una classe di archiviazione per i volumi NetApp con il provisioner Trident CSI. Rendi predefinita solo una delle classi di archiviazione utilizzando un'annotazione. Ciò consentirà a un PVC di utilizzare questa classe di archiviazione quando non è esplicitamente indicata nel manifesto del PVC. Di seguito è riportato un esempio con l'annotazione.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

Distribuisci un'applicazione utilizzando OpenShift GitOps (Argo CD)

- Installa l'operatore OpenShift GitOps sul cluster. Fai riferimento alle istruzioni "Qui".
- SetUp una nuova istanza di Argo CD per il cluster. Consulta le istruzioni "Qui".

Apri la console di Argo CD e distribuisci un'app. Ad esempio, puoi distribuire un'app Jenkins utilizzando Argo

CD con un Helm Chart. Quando crei l'applicazione, fornisci i seguenti dettagli: Project: default cluster: 'https://kubernetes.default.svc'[] (senza virgolette) Namespace: Jenkins L'url per l'Helm Chart: 'https://charts.bitnami.com/bitnami'[] (senza virgolette)

Protezione dei dati

Per dettagli sulla protezione e la migrazione dei carichi di lavoro dei container utilizzando Trident Protect, consultare la seguente sezione: - "Proteggi e migra le app Container utilizzando Trident Protect"

Ulteriori soluzioni NetApp Hybrid Multicloud per carichi di lavoro Red Hat OpenShift

Vedi le seguenti soluzioni aggiuntive:

- "Soluzione container Red Hat OpenShift on-premises"
- "Soluzione container Red Hat OpenShift Service on AWS"
- "Soluzione di virtualizzazione Red Hat OpenShift on-premises"
- "Soluzione di virtualizzazione Red Hat OpenShift Service on AWS"

Proteggi i dati utilizzando Trident Protect

Protezione dei dati per le app container in OpenShift Container Platform utilizzando Trident Protect

Questa sezione del documento di riferimento fornisce dettagli sulla creazione di snapshot e backup di Container Apps utilizzando Trident Protect. NetApp Trident Protect offre avanzate capacità di gestione dei dati delle applicazioni che migliorano la funzionalità e la disponibilità delle applicazioni Kubernetes stateful supportate dai sistemi di storage NetApp ONTAP e dal NetApp Trident CSI storage provisioner. Trident Protect crea snapshot e backup delle applicazioni. Ciò significa che snapshot e backup vengono creati non solo per i dati delle applicazioni nei volumi persistenti, ma anche per i metadati delle applicazioni. Gli snapshot e i backup creati da Trident Protect possono essere archiviati in uno qualsiasi dei seguenti storage a oggetti e ripristinati da essi in un secondo momento.

- AWS S3
- Archiviazione BLOB di Azure
- Google Cloud Storage
- ONTAP S3
- StorageGrid
- Qualsiasi altro storage compatibile con S3

Trident Protect utilizza il modello Kubernetes di controllo degli accessi in base al ruolo (RBAC). Per impostazione predefinita, Trident Protect fornisce un singolo namespace di sistema chiamato trident-protect e il relativo account di servizio predefinito. Se hai un'organizzazione con molti utenti o esigenze di sicurezza

specifiche, puoi utilizzare le funzionalità RBAC di Trident Protect per ottenere un controllo più granulare sull'accesso a risorse e namespace.

Ulteriori informazioni su RBAC in Trident Protect possono essere trovate nel "Documentazione Trident Protect"

> L'amministratore del cluster ha accesso alle risorse nello spazio dei nomi trident-protect predefinito e può anche accedere alle risorse in tutti gli altri spazi dei nomi. Gli utenti non possono creare risorse personalizzate (CR) per la gestione dei dati delle applicazioni, come CR Snapshot e Backup, nello spazio dei nomi trident-protect. Come buona pratica, gli utenti dovranno creare tali CR nello spazio dei nomi dell'applicazione.

Trident Protect può essere installato seguendo le istruzioni fornite nella documentazione "Qui". Questa sezione mostrerà il flusso di lavoro per la protezione dei dati delle applicazioni container e il ripristino delle applicazioni utilizzando Trident Protect. 1. Creazione di Snapshot (su richiesta o pianificata) 2. Ripristino da Snapshot (ripristino nello stesso namespace o in uno diverso) 3. Creazione di backup 4. Ripristino da backup

▼ **Prerequisito**

Prima di creare le snapshot e i backup per un'applicazione, lo storage a oggetti deve essere configurato in Trident Protect per archiviare le snapshot e i backup. Questo viene fatto utilizzando il bucket CR. Solo gli amministratori possono creare un bucket CR e configurarlo. Il bucket CR è noto come AppVault in Trident Protect. Gli oggetti AppVault sono la rappresentazione dichiarativa del workflow Kubernetes di un bucket di storage. Un CR AppVault contiene le configurazioni necessarie affinché un bucket possa essere utilizzato nelle operazioni di protezione, come backup, snapshot, operazioni di ripristino e replica SnapMirror.

In questo esempio, mostreremo l'utilizzo di ONTAP S3 come storage a oggetti. Ecco il flusso di lavoro per la creazione di AppVault CR per ONTAP S3: 1. Creare un server di archivio di oggetti S3 nella SVM nel cluster ONTAP. 2. Creare un bucket nel server di archivio di oggetti. 3. Creare un utente S3 nella SVM. Conservare la access key e la secret key in un luogo sicuro. 4. In OpenShift, creare un secret per archiviare le credenziali ONTAP S3. 5. Creare un oggetto AppVault per ONTAP S3

Configura Trident Protect AppVault per ONTAP S3

Esempio di file YAML per la configurazione di Trident Protect con ONTAP S3 come AppVault

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
```

```
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

Esempio di file yaml per l'installazione dell'app PostgreSQL

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
```

```
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ **Crea snapshot**

Creazione di uno snapshot on-demand

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+----------------+--------------+-----------+-----+-------+
|      NAME      |   APP REF    |   STATE   | AGE | ERROR |
+----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                        READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49   1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                  Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                  SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS          SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

Creazione di una pianificazione Utilizzando il seguente comando, gli snapshot verranno creati ogni giorno alle 15:33 e verranno conservati due snapshot e due backup.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily --hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+-------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+-------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

Creazione di una pianificazione tramite yaml

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+-------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+-------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

È possibile visualizzare gli snapshot creati in base a questa pianificazione.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

Vengono creati anche snapshot del volume.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ Elimina l'applicazione per simulare la perdita dell'applicazione

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ Ripristina da Snapshot allo stesso namespace

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

L'applicazione e il suo PVC vengono ripristinati nello stesso namespace.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ Ripristina da Snapshot a uno spazio dei nomi diverso

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |      APPVAULT      |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

Puoi vedere che l'applicazione è stata ripristinata in un nuovo namespace.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                  Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ Crea backup

Creazione di un backup su richiesta

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Creazione di una pianificazione per il backup

I backup giornalieri e orari nell'elenco sopra vengono creati in base alla pianificazione impostata in precedenza.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ **Ripristina dal backup**

Eliminare l'applicazione e i PVC per simulare una perdita di dati.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Ripristina nello stesso namespace #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" creato.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

L’applicazione e i PVC vengono ripristinati nello stesso namespace.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w   1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                 Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

Ripristina in uno spazio dei nomi diverso Crea un nuovo spazio dei nomi. Ripristina da un backup al nuovo namespace.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p   1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                 Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ **Migrazione delle applicazioni**

Per clonare o migrare un’applicazione su un cluster diverso (eseguire un clone tra cluster), crea un backup sul cluster di origine e poi ripristina il backup su un cluster di destinazione. Assicurarsi che Trident Protect sia installato sul cluster di destinazione.

Sul cluster di origine, eseguire i passaggi mostrati nell’immagine seguente:

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

Dal cluster di origine, cambia contesto al cluster di destinazione. Quindi, assicurati che AppVault sia accessibile dal contesto del cluster di destinazione e ottieni i contenuti di AppVault dal cluster di destinazione.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+---------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
|    CLUSTER    |     APP     |  TYPE  |            NAME             |        TIMESTAMP        |
                    PATH                                                                    |
+---------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1                 | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                                                  |
| ocp-cluster11 | postgres-app | backup | backup1                     | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                                                               |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd                                            |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d                                            |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc                                           |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031                                           |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1    | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3                                              |
```

Utilizzare il percorso di backup dall'elenco e creare un oggetto CR backuprestore come mostrato nel comando seguente.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|          NAME            |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

Ora puoi vedere che i pod dell'applicazione e i pvc sono stati creati nel cluster di destinazione.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                   READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                         STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Proteggi le VM in Red Hat OpenShift Virtualization utilizzando Trident Protect

Proteggi le VM in OpenShift Virtualization utilizzando snapshot e backup. Questa procedura include la creazione di un AppVault utilizzando ONTAP S3 storage a oggetti, la configurazione di Trident Protect per acquisire i dati delle VM, inclusi oggetti di risorse Kubernetes, volumi persistenti e immagini interne, e il ripristino dei dati quando necessario.

Le macchine virtuali nell'ambiente di virtualizzazione OpenShift sono applicazioni containerizzate che vengono eseguite nei nodi worker della piattaforma OpenShift Container. È importante proteggere i metadati delle VM e i dischi persistenti delle VM, in modo che sia possibile recuperarli quando vengono persi o danneggiati.

I dischi persistenti delle VM di OpenShift Virtualization possono essere supportati dallo storage ONTAP integrato nel OpenShift Cluster utilizzando "Trident CSI". In questa sezione utilizziamo "Trident Protect" per creare snapshot e backup delle VM, inclusi i loro volumi di dati, su ONTAP object storage.

Quando necessario, eseguiamo il ripristino da uno snapshot o da un backup.

Trident Protect consente snapshot, backup, ripristini e disaster recovery di applicazioni e VM su un OpenShift cluster. Per le VM di OpenShift Virtualization, i dati che possono essere protetti con Trident Protect includono oggetti di risorse Kubernetes associati alle VM, volumi persistenti e immagini interne.

Di seguito sono riportate le versioni dei vari componenti utilizzati per gli esempi in questa sezione

- "Cluster OpenShift 4.17"
- "OpenShift Virtualization installato tramite OpenShift Virtualization Operator fornito da Red Hat"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

Crea AppVault per storage a oggetti

▼ **Crea AppVault**

Prima di creare le snapshot e i backup per un'applicazione o una VM, lo storage a oggetti deve essere configurato in Trident Protect per archiviare le snapshot e i backup. Questo viene fatto utilizzando il bucket CR. Solo gli amministratori possono creare un bucket CR e configurarlo. Il bucket CR è noto come AppVault in Trident Protect. Gli oggetti AppVault sono la rappresentazione dichiarativa del workflow Kubernetes di un bucket di storage. Un CR AppVault contiene le configurazioni necessarie affinché un bucket possa essere utilizzato nelle operazioni di protezione, come backup, snapshot, operazioni di ripristino e replica SnapMirror.

In questo esempio, mostreremo l'utilizzo di ONTAP S3 come storage a oggetti. Ecco il flusso di lavoro per la creazione di AppVault CR per ONTAP S3: 1. Creare un server di archivio di oggetti S3 nella SVM nel cluster ONTAP. 2. Creare un bucket nel server di archivio di oggetti. 3. Creare un utente S3 nella SVM. Conservare la access key e la secret key in un luogo sicuro. 4. In OpenShift, creare una secret per archiviare le credenziali ONTAP S3. 5. Creare un oggetto AppVault per ONTAP S3

Configura Trident Protect AppVault per ONTAP S3

```
# alias tp='tridentctl-protect'
```

```
# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3
```

```
# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

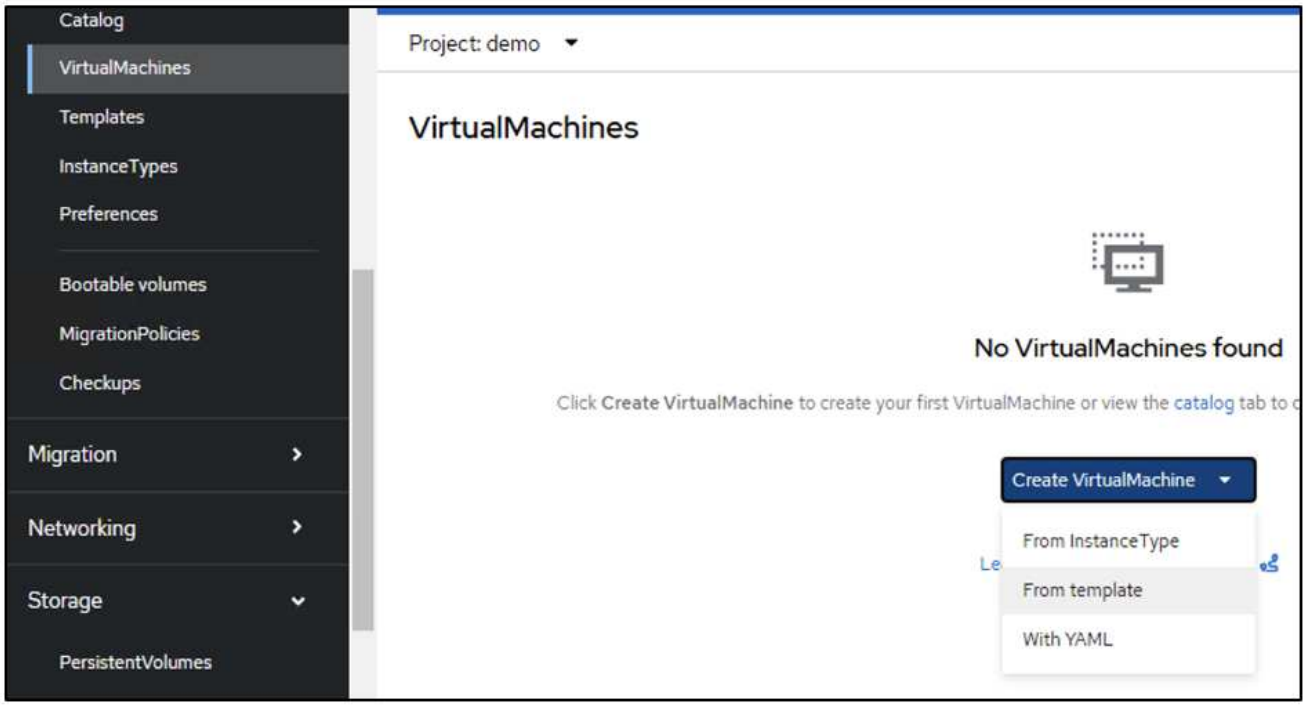
Creare una VM in OpenShift Virtualization

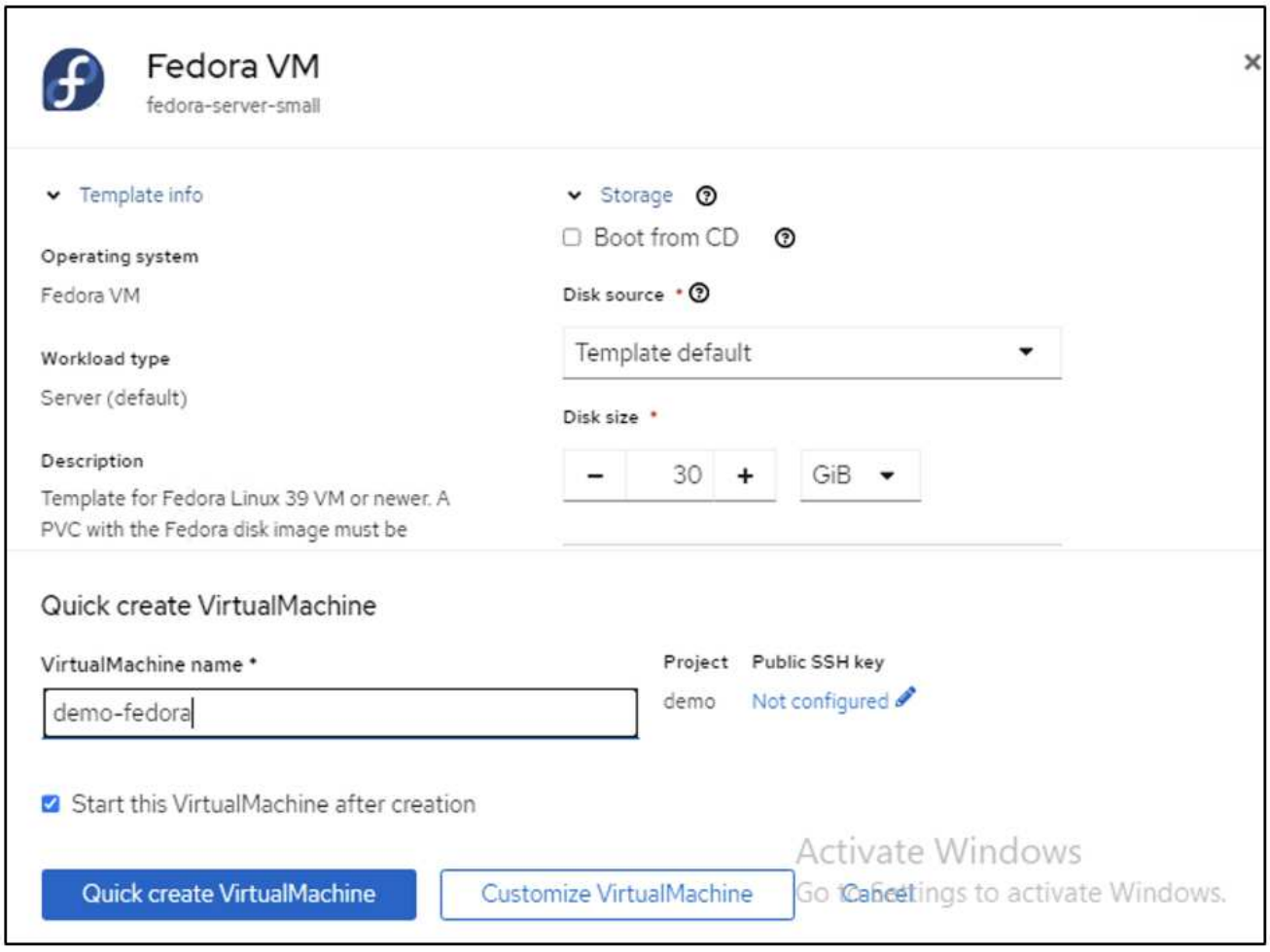
▼ **Creare una VM in OpenShift Virtualization**

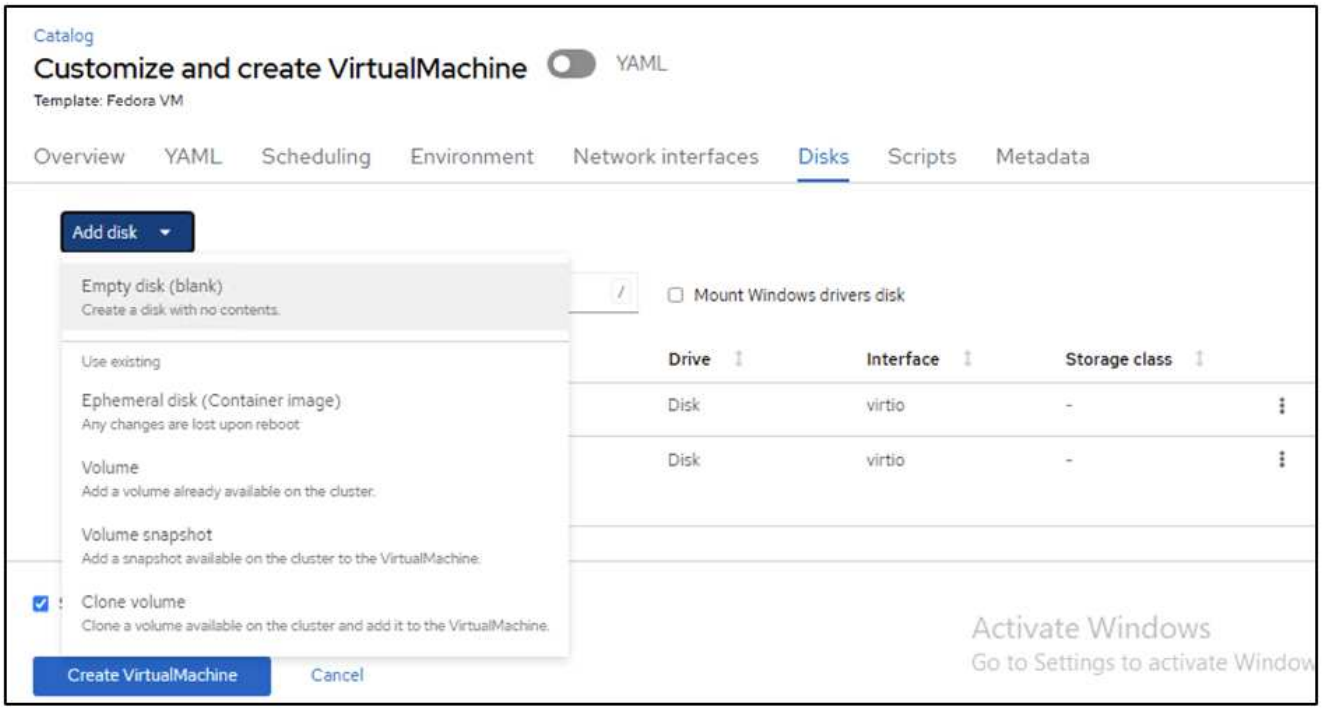
Gli screenshot seguenti mostrano la creazione della VM (demo-fedora nello spazio dei nomi demo) dalla console utilizzando il modello. Il disco radice sceglie automaticamente la classe di archiviazione predefinita, quindi verificare che la classe di archiviazione predefinita sia impostata correttamente. In questa configurazione, la classe di archiviazione predefinita è **sc-zonea-san**. Quando si crea il disco aggiuntivo, assicurarsi di scegliere la classe di archiviazione sc-zonea-san e di selezionare la casella di controllo "**Applica impostazioni di archiviazione ottimizzate**". In questo modo le modalità di accesso verranno impostate su RWX e la modalità volume su Blocco.

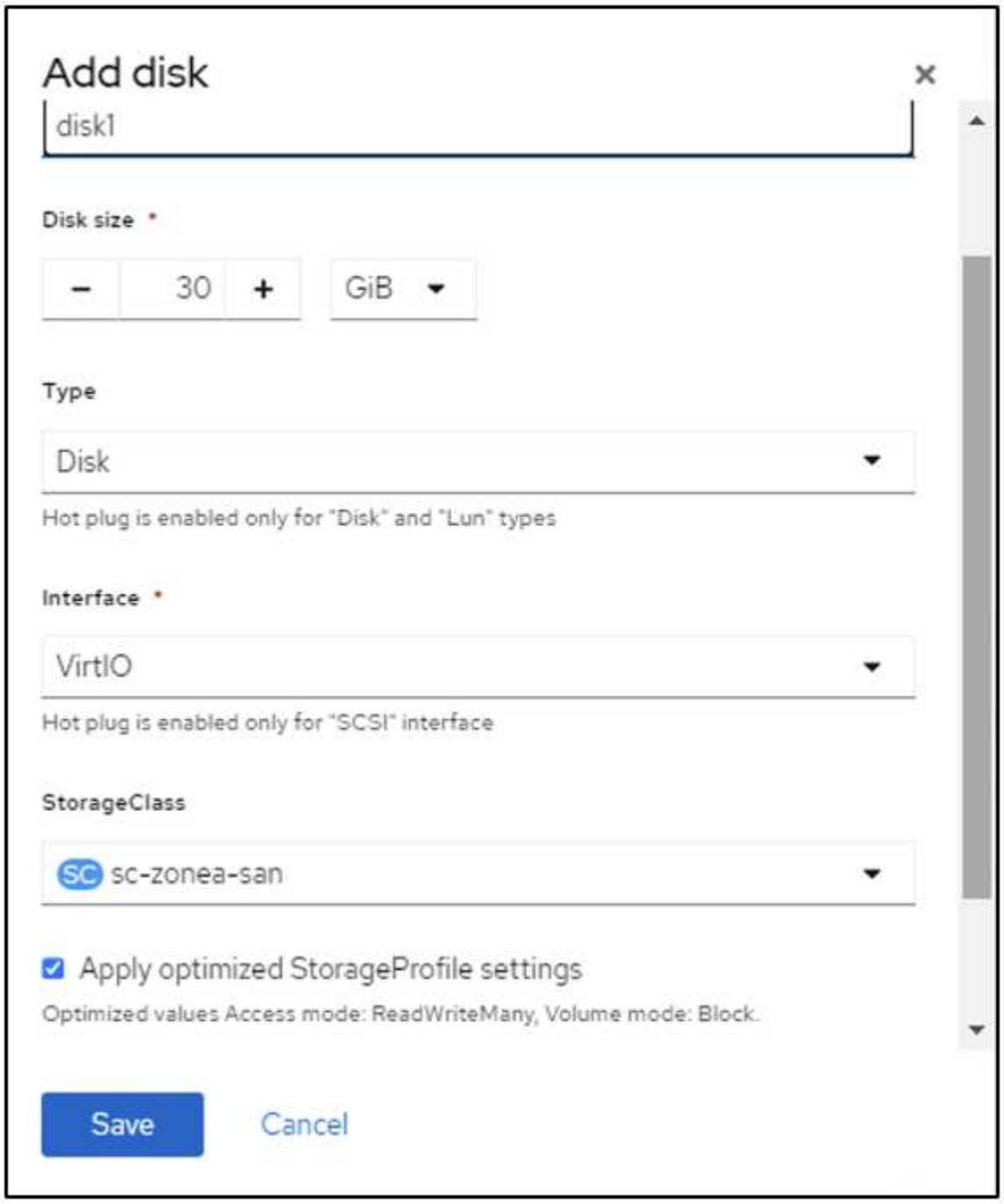
Trident supporta la modalità di accesso RWX in modalità Block Volume per SAN (iSCSI, NVMe/TCP e FC). (È la modalità di accesso predefinita per NAS). La modalità di accesso RWX è necessaria se in un secondo momento è necessario eseguire la migrazione live delle VM.

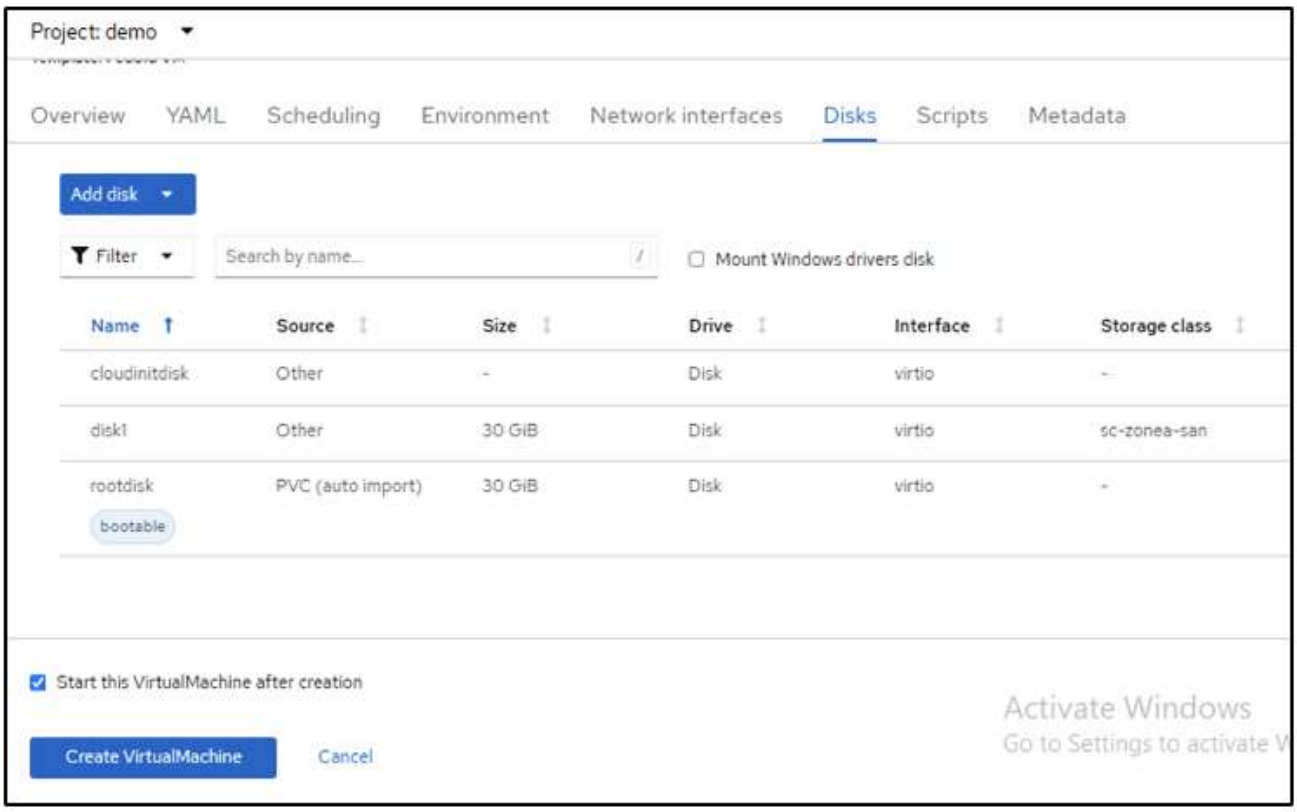



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Crea un’app

▼ **Crea app**

Crea un’app Trident Protect per la VM

Nell’esempio, lo spazio dei nomi demo ha una VM e tutte le risorse dello spazio dei nomi sono incluse quando si crea l’app.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

Proteggi l'app creando un backup

▼ **Crea backup**

Crea un backup su richiesta

Creare un backup per l'app (demo-vm) creata in precedenza che includa tutte le risorse nello spazio dei nomi demo. Fornire il nome dell'appvault in cui verranno archiviati i backup.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Crea backup pianificati

Creare una pianificazione per i backup specificando la granularità e il numero di backup da conservare.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Ripristina dal backup

▼ **Ripristina dai backup**

Ripristina la VM nello stesso namespace

Nell'esempio, il backup demo-vm-backup-on-demand contiene il backup con demo-app per la VM Fedora.

Per prima cosa, elimina la VM e assicurati che i PVC, il pod e gli oggetti VM vengano eliminati dallo spazio dei nomi "demo"

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

Ora, crea un oggetto di ripristino tramite backup sul posto.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verificare che la VM, i pod e i PVC siano ripristinati

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Ripristina la VM in uno spazio dei nomi diverso

Per prima cosa crea un nuovo namespace in cui vuoi ripristinare l'app, in questo esempio demo2. Quindi creare un oggetto di backup e ripristino

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

Verificare che la VM, i pod e i pvc siano creati nel nuovo namespace demo2.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Proteggi l'app utilizzando gli snapshot

▼ Crea snapshot

Crea uno snapshot on-demand Crea uno snapshot per l'app e specifica l'appvault in cui deve essere archiviato.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Crea una pianificazione per gli snapshot Crea una pianificazione per gli snapshot. Specificare la granularità e il numero di snapshot da conservare.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-
s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n
demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-----------------------------------------+---------+----------------+-----------+-------+--------+
|                  NAME                   |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand               | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000             | demo-vm | Delete         | Completed |       | 1m29s  |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Ripristina da snapshot

▼ Ripristina da snapshot

Ripristinare la VM dallo snapshot nello stesso namespace Eliminare la VM demo-fedora dal namespace demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

Creare un oggetto snapshot-in-place-restore dallo snapshot della VM.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
```

```
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+-----------------------------------+-------------------+-----------+-------+--------+
|               NAME                |     APPVAULT      |   STATE   | ERROR |  AGE   |
+-----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+-----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verificare che la VM e i suoi PVC siano creati nello spazio dei nomi demo.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

Ripristina la VM dallo snapshot in uno spazio dei nomi diverso

Eliminare la VM nello spazio dei nomi demo2 precedentemente ripristinata dal backup.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

Creare l'oggetto di ripristino dello snapshot dallo snapshot e fornire la mappatura dello spazio dei nomi.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+------------------+-----------+-------+--------+
|               NAME                |     APPVAULT     |   STATE   | ERROR |  AGE   |
+-----------------------------------+------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+------------------+-----------+-------+--------+
```

Verificare che la VM e i suoi PVC siano ripristinati nel nuovo namespace demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                          STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                             Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san     <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san     <unset>                 29h
[root@localhost RedHat]#
```

Ripristina una VM specifica

▼ Selezione di VM specifiche in uno spazio dei nomi per creare snapshot/backup e ripristinare

Nell'esempio precedente, avevamo una singola VM all'interno di uno spazio dei nomi. Includendo l'intero namespace nel backup, sono state acquisite tutte le risorse associate a quella VM. Nell'esempio seguente, aggiungiamo un'altra VM allo stesso namespace e creiamo un'app solo per questa nuova VM utilizzando un selettore di etichette.

Crea una nuova VM (demo-centos vm) nello spazio dei nomi demo

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora   81m     Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g  1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh  1/1     Running   0          81m

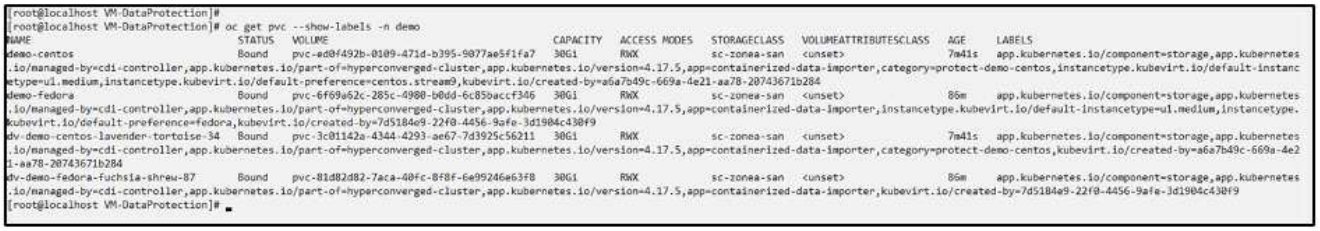
NAME                                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                             Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                             Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Etichettare la VM demo-centos e le risorse associate

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

Verificare che la VM demo-centos e i pvc abbiano le etichette

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```



Crea un'app solo per una VM specifica (demo-centos) utilizzando il selettore di etichette

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

Il metodo per creare backup e snapshot su richiesta e in base a una pianificazione è lo stesso mostrato in precedenza. Poiché l'app trident-protect utilizzata per creare snapshot o backup contiene solo la VM specifica dello spazio dei nomi, il ripristino da essi ripristina solo una VM specifica. Di seguito è riportato un esempio di operazione di backup/ripristino.

Crea un backup di una VM specifica in uno spazio dei nomi utilizzando la relativa app

Nei passaggi precedenti è stata creata un'app utilizzando selettori di etichette per includere solo la macchina virtuale CentOS nello spazio dei nomi demo. Crea un backup (backup su richiesta, in questo esempio) per questa app.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+-------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME              |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand  | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand      | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500   | demo-vm         | Retain         | Completed |       | 56m17s |
+-------------------------------+-----------------+----------------+-----------+-------+--------+
```

Ripristina una VM specifica nello stesso namespace Il backup di una VM specifica (centos) è stato creato utilizzando l'app corrispondente. Se da questo viene creato un backup-in-place-restore o un backup-restore, verrà ripristinata solo questa specifica VM. Eliminare la VM Centos.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora    4m27s   Running   True

NAME                                                                 STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                    Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                                    Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34            Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87                Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    5m17s   Running   True

NAME                                                                 STATUS   VOLUME
persistentvolumeclaim/demo-fedora                                    Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87                Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

Creare un ripristino sul posto del backup da demo-centos-backup-on-demand e verificare che la VM centos sia stata ricreata.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore  | ontap-s3-appvault  | Completed |       | 57m9s |
| demo-fedora-restore  | ontap-s3-appvault  | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                     AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                                STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                   Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34           Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87               Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

Ripristinare una VM specifica in uno spazio dei nomi diverso Creare un ripristino di backup in uno spazio dei nomi diverso (demo3) da demo-centos-backup-on-demand e verificare che la VM centos sia stata ricreata.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-
demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault  | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                     AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                                STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                                   Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34           Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

Dimostrazione video

Il seguente video mostra una dimostrazione della protezione di una VM tramite snapshot

Protezione di una VM

Proteggere le app contenitore utilizzando strumenti di terze parti

Protezione dei dati per le app container nella piattaforma container OpenShift tramite OpenShift API for Data Protection (OADP)

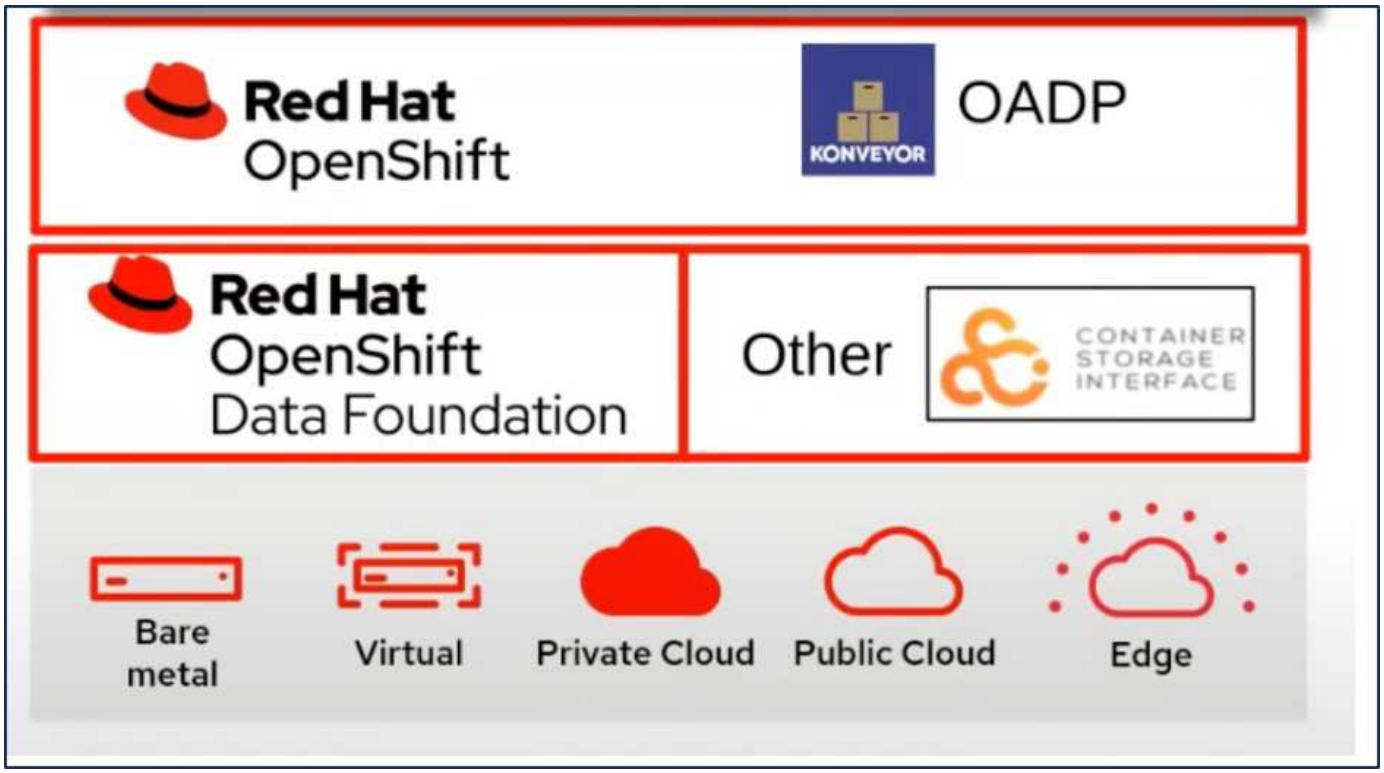
Questa sezione del documento di riferimento fornisce dettagli sulla creazione di backup di Container Apps utilizzando OpenShift API for Data Protection (OADP) con Velero su NetApp ONTAP S3 o NetApp StorageGRID S3. I backup delle risorse con ambito namespace, inclusi i volumi persistenti (PV) dell'app, vengono creati utilizzando gli snapshot CSI Trident .

Lo storage persistente per le app container può essere supportato dallo storage ONTAP integrato nel cluster OpenShift utilizzando "Trident CSI". In questa sezione utilizziamo "API OpenShift per la protezione dei dati (OADP)" per eseguire il backup delle app, inclusi i relativi volumi di dati, su

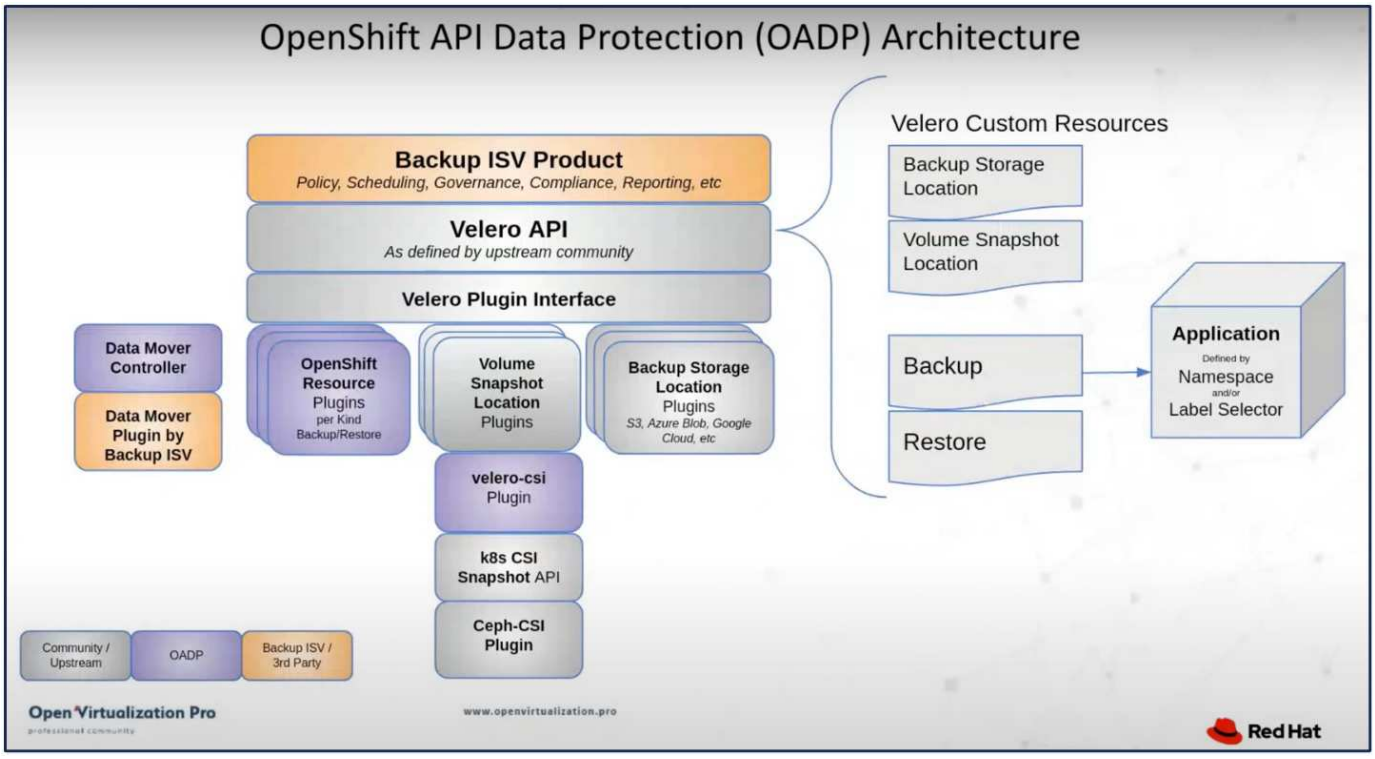
- Archiviazione di oggetti ONTAP
- StorageGrid

Quando necessario, eseguiamo il ripristino dal backup. Si prega di notare che l'app può essere ripristinata solo nel cluster da cui è stato creato il backup.

OADP consente il backup, il ripristino e il disaster recovery delle applicazioni su un cluster OpenShift. I dati che possono essere protetti con OADP includono oggetti di risorse Kubernetes, volumi persistenti e immagini interne.



Red Hat OpenShift ha sfruttato le soluzioni sviluppate dalle comunità OpenSource per la protezione dei dati. "Velero" è uno strumento open source per eseguire backup e ripristini in modo sicuro, eseguire il disaster recovery e migrare le risorse del cluster Kubernetes e i volumi persistenti. Per utilizzare Velero in modo semplice, OpenShift ha sviluppato l'operatore OADP e il plugin Velero per integrarli con i driver di archiviazione CSI. Il nucleo delle API OADP esposte si basa sulle API Velero. Dopo aver installato e configurato l'operatore OADP, le operazioni di backup/ripristino che possono essere eseguite si basano sulle operazioni esposte dall'API Velero.



OADP 1.3 è disponibile nell'hub operatore del cluster OpenShift 4.12 e versioni successive. Dispone di un Data Mover integrato in grado di spostare gli snapshot del volume CSI in un archivio oggetti remoto. Ciò garantisce portabilità e durata spostando gli snapshot in una posizione di archiviazione degli oggetti durante il backup. Gli snapshot sono quindi disponibili per il ripristino dopo i disastri.

Di seguito sono riportate le versioni dei vari componenti utilizzati per gli esempi in questa sezione

- Cluster OpenShift 4.14
- Operatore OADP 1.13 fornito da Red Hat
- Velero CLI 1.13 per Linux
- Trident 24.02
- ONTAP 9.12
- postgresql installato tramite helm.

"Trident CSI" "API OpenShift per la protezione dei dati (OADP)" "Velero"

Installazione dell'operatore OpenShift API for Data Protection (OADP)

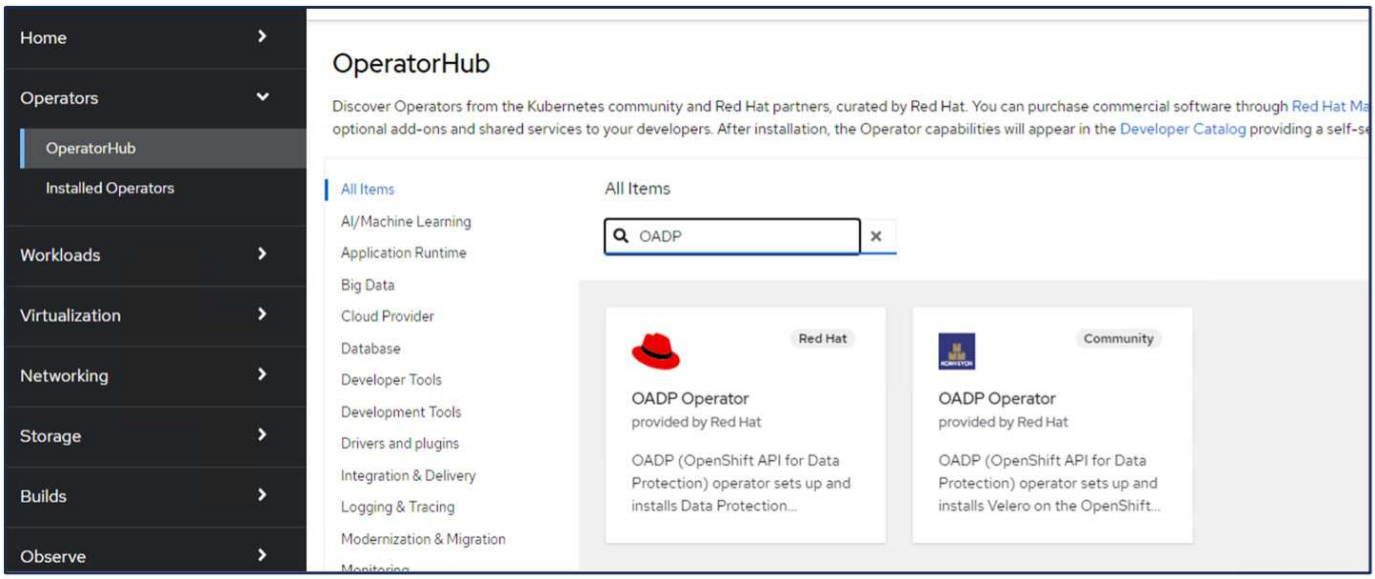
Questa sezione descrive l'installazione dell'operatore OpenShift API for Data Protection (OADP).

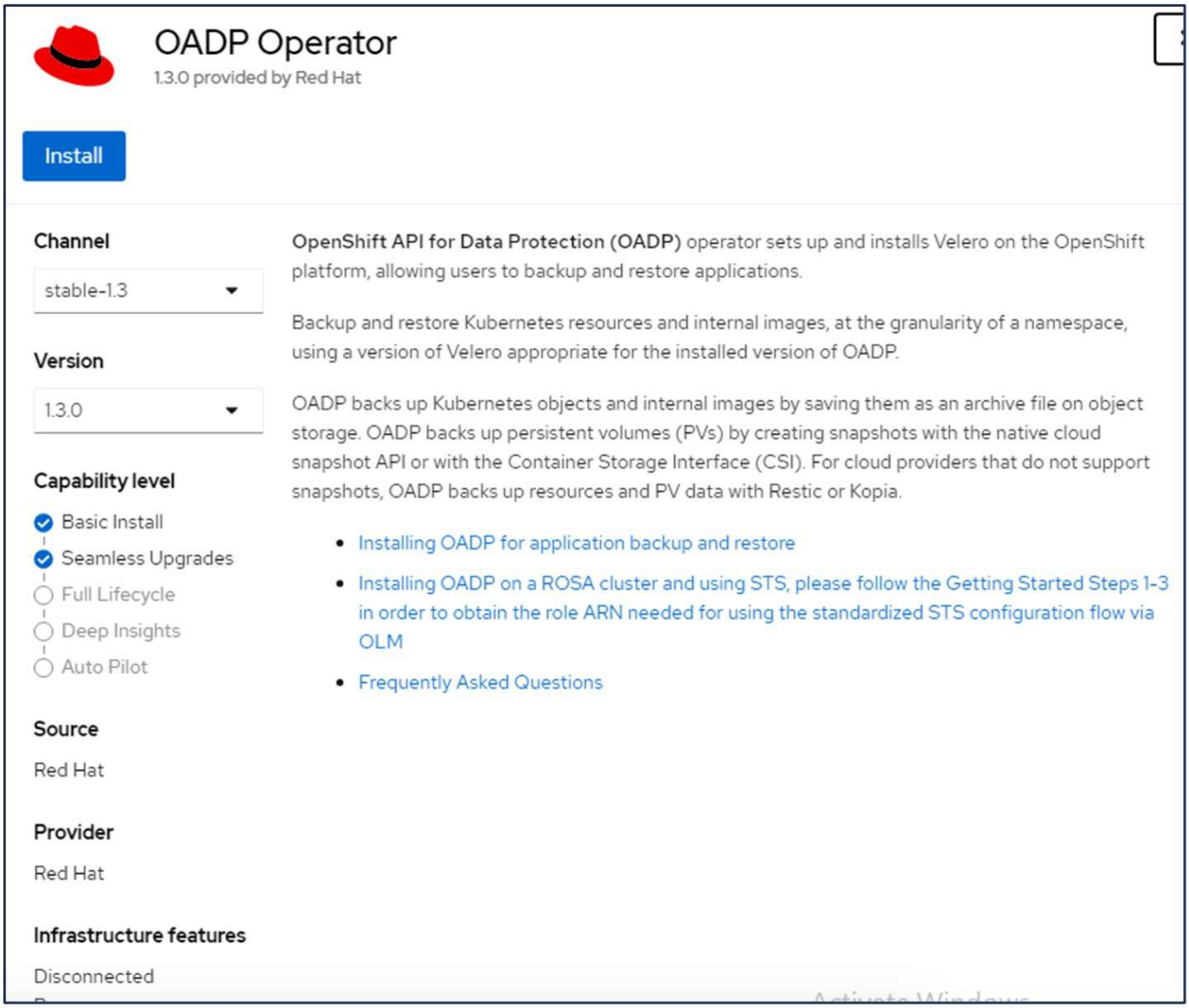
Prerequisiti

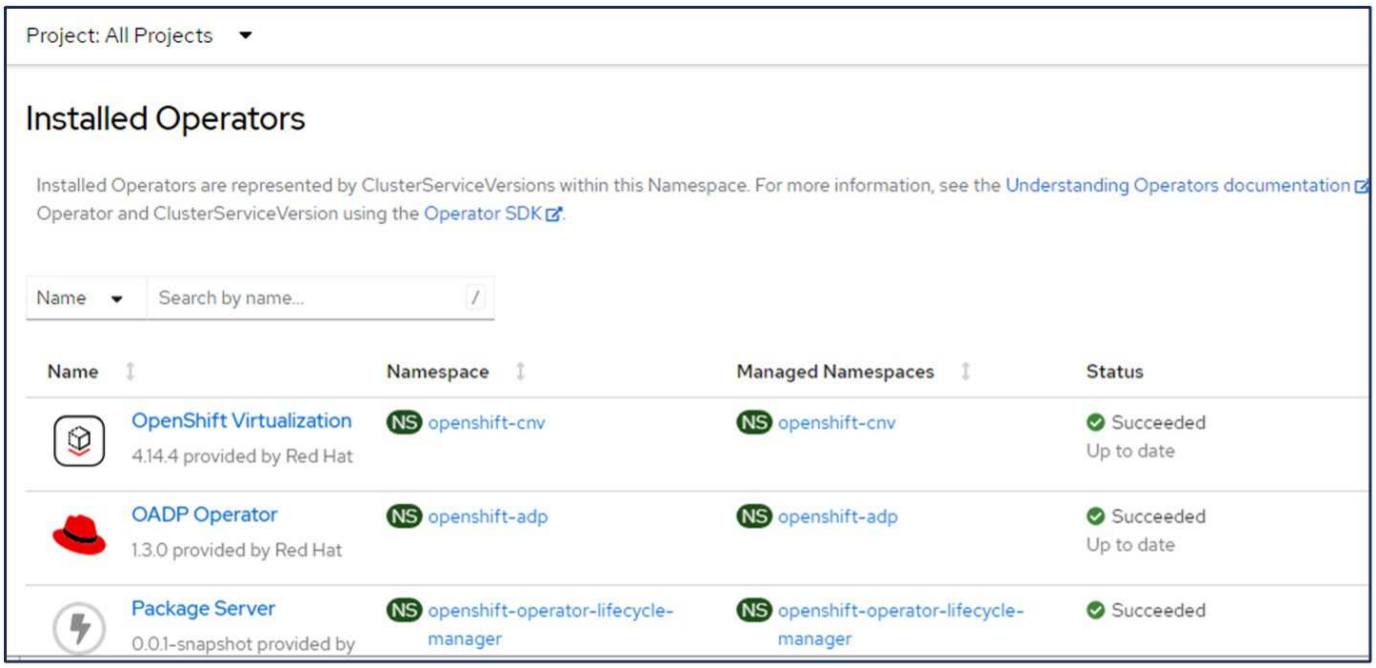
- Un cluster Red Hat OpenShift (successivo alla versione 4.12) installato su un'infrastruttura bare-metal con nodi worker RHCOS
- Un cluster NetApp ONTAP integrato con il cluster tramite Trident
- Un backend Trident configurato con un SVM su cluster ONTAP
- Una StorageClass configurata sul cluster OpenShift con Trident come provisioner
- Classe Trident Snapshot creata sul cluster
- Accesso di amministrazione del cluster al cluster Red Hat OpenShift
- Accesso amministratore al cluster NetApp ONTAP
- Un'applicazione, ad esempio postgresql, distribuita sul cluster
- Una postazione di lavoro di amministrazione con gli strumenti tridentctl e oc installati e aggiunti a $PATH

Passaggi per installare l'operatore OADP

1. Accedere all'Operator Hub del cluster e selezionare l'operatore Red Hat OADP. Nella pagina Installa, utilizza tutte le selezioni predefinite e fai clic su Installa. Nella pagina successiva, utilizzare nuovamente tutte le impostazioni predefinite e fare clic su Installa. L'operatore OADP verrà installato nello spazio dei nomi openshift-adp.


Home
Operators
OperatorHub
Installed Operators
Workloads
Virtualization
Networking
Storage
Builds
Observe
OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Ma
optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-se
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
Drivers and plugins
Integration & Delivery
Logging & Tracing
Modernization & Migration
All Items
OADP
Red Hat
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...
Community
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Velero on the OpenShift...


OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions



Prerequisiti per la configurazione Velero con dettagli Ontap S3

Dopo aver completato l'installazione dell'operatore, configurare l'istanza di Velero. Velero può essere configurato per utilizzare Object Storage compatibile con S3. Configurare ONTAP S3 utilizzando le procedure mostrate nel"Sezione Gestione dell'archiviazione degli oggetti della documentazione ONTAP" . Per l'integrazione con Velero, avrai bisogno delle seguenti informazioni dalla configurazione ONTAP S3.

- Un'interfaccia logica (LIF) che può essere utilizzata per accedere a S3
- Credenziali utente per accedere a S3 che includono la chiave di accesso e la chiave di accesso segreta
- Un nome di bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'Object Storage, è necessario installare il certificato TLS sul server Object Storage.

Prerequisiti per la configurazione di Velero con StorageGrid S3

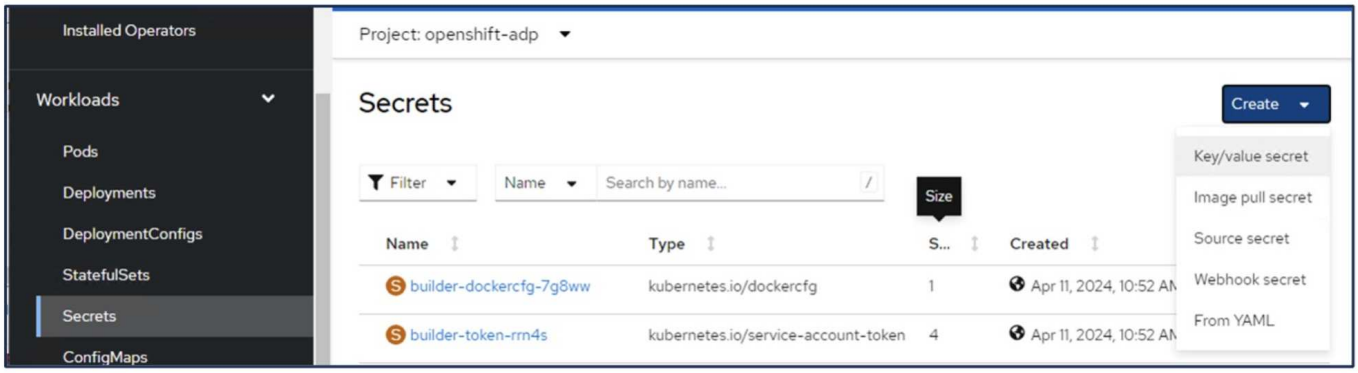
Velero può essere configurato per utilizzare Object Storage compatibile con S3. È possibile configurare StorageGrid S3 utilizzando le procedure illustrate in"Documentazione StorageGrid" . Per l'integrazione con Velero, saranno necessarie le seguenti informazioni dalla configurazione di StorageGrid S3.

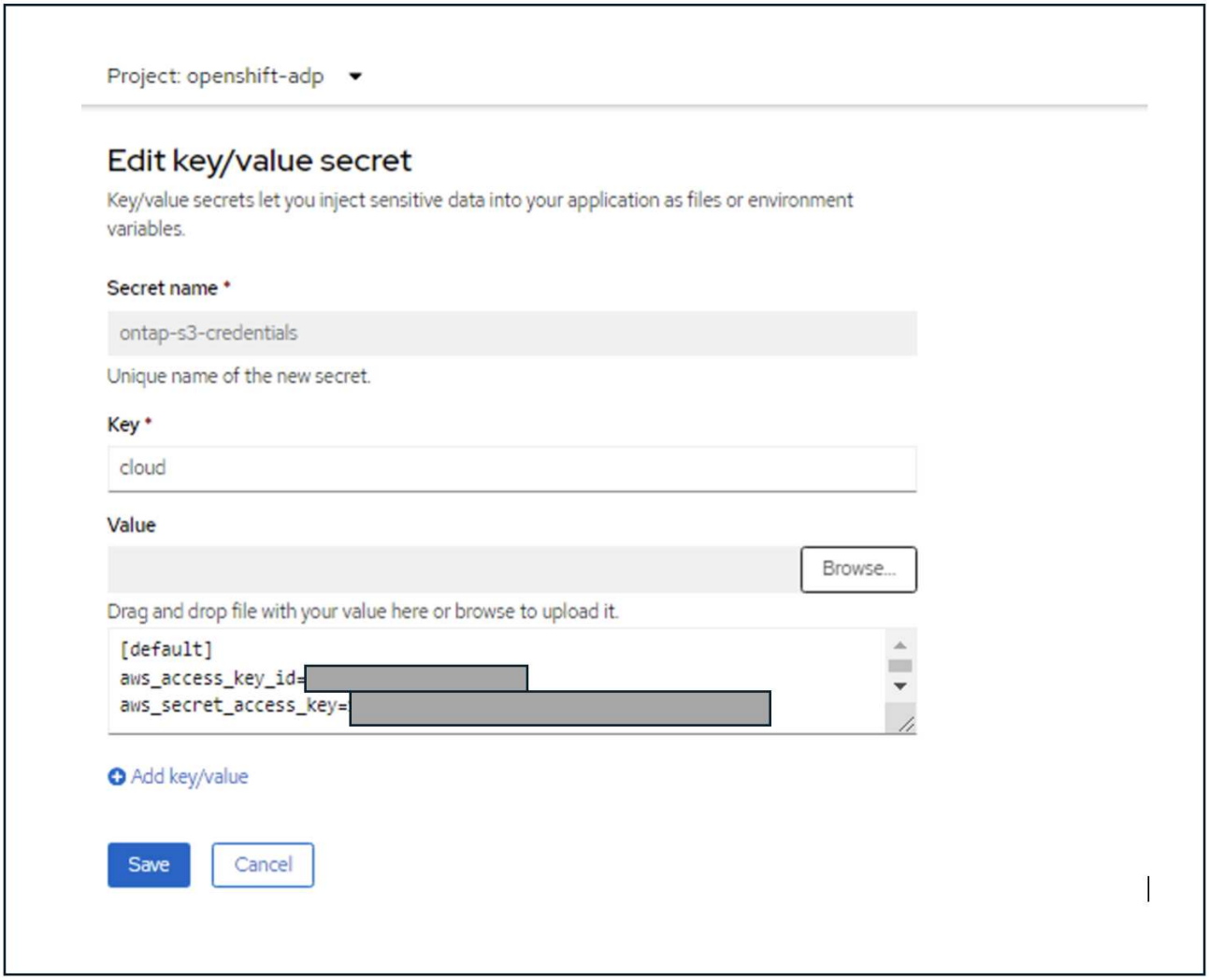
- L'endpoint che può essere utilizzato per accedere a S3
- Credenziali utente per accedere a S3 che includono la chiave di accesso e la chiave di accesso segreta
- Un nome di bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'Object Storage, è necessario installare il certificato TLS sul server Object Storage.

Passaggi per configurare Velero

- Per prima cosa, crea un segreto per le credenziali utente ONTAP S3 o per le credenziali utente StorageGrid Tenant. Questo verrà utilizzato per configurare Velero in seguito. È possibile creare un segreto dalla CLI o dalla console Web. Per creare un segreto dalla console Web, seleziona Segreti, quindi fai clic su Segreto chiave/valore. Fornire i valori per il nome della credenziale, la chiave e il valore come mostrato. Assicurati di utilizzare l'ID della chiave di accesso e la chiave di accesso segreta del tuo utente S3. Dai un

nome appropriato al segreto. Nell'esempio seguente viene creato un segreto con credenziali utente ONTAP S3 denominato ontap-s3-credentials.





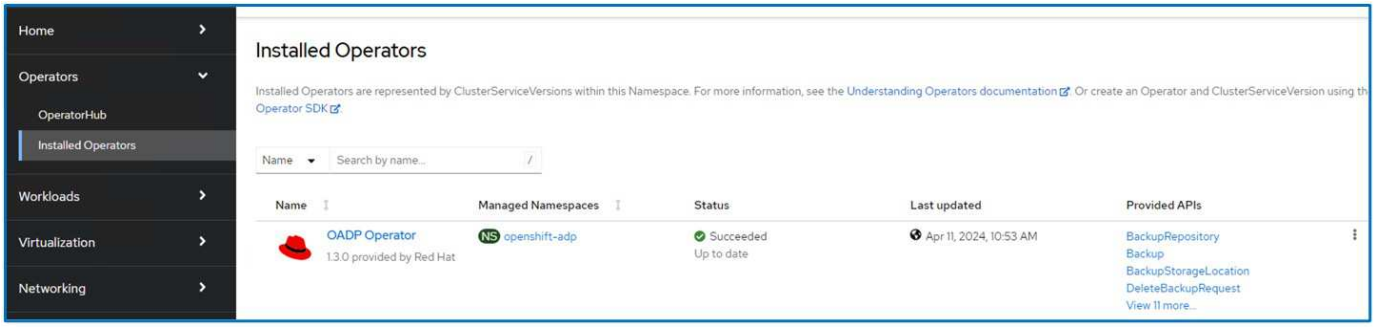
Per creare un segreto denominato sg-s3-credentials dalla CLI è possibile utilizzare il seguente comando.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

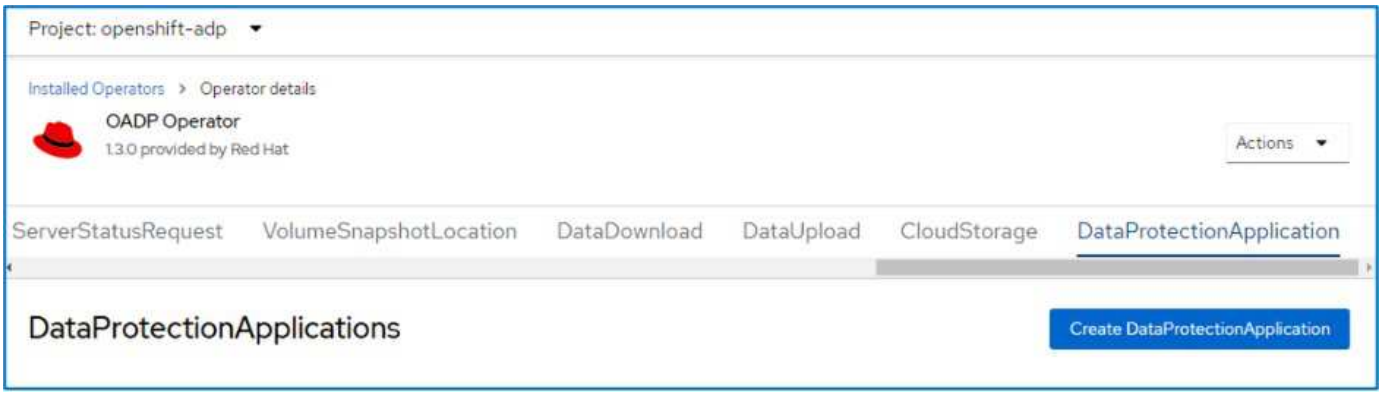
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- Successivamente, per configurare Velero, seleziona Operatori installati dalla voce di menu in Operatori, fai clic sull'operatore OADP e seleziona la scheda **DataProtectionApplication**.



Fare clic su Crea applicazione di protezione dati. Nella visualizzazione del modulo, specificare un nome per l'applicazione DataProtection oppure utilizzare il nome predefinito.



Ora vai alla vista YAML e sostituisci le informazioni specifiche come mostrato negli esempi di file yaml riportati di seguito.

Esempio di file yaml per la configurazione di Velero con ONTAP S3 come backupLocation

```
spec:
  backupLocations:
    - velero:
        config:
```

```
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Esempio di file yaml per la configurazione di Velero con StorageGrid S3 come backupLocation

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
```

```
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

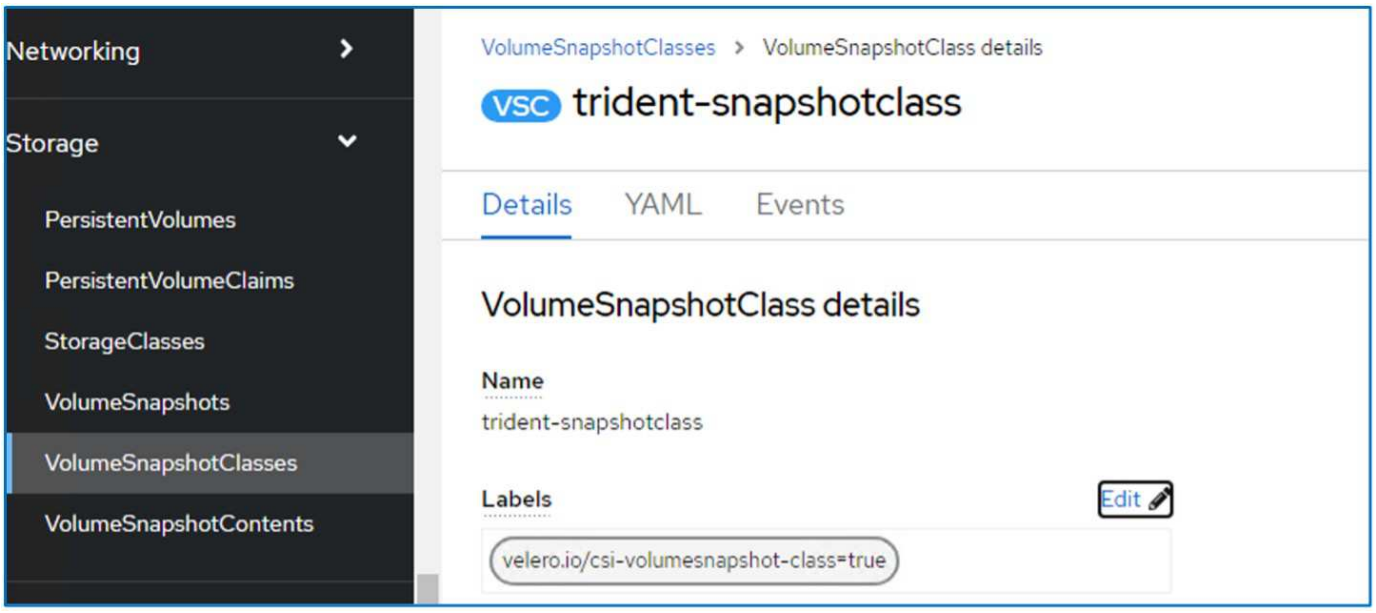
La sezione spec nel file yaml dovrebbe essere configurata in modo appropriato per i seguenti parametri simili all'esempio sopra

backupLocations ONTAP S3 o StorageGrid S3 (con le relative credenziali e altre informazioni come mostrato nel file yaml) è configurato come BackupLocation predefinito per velero.

snapshotLocations Se si utilizzano snapshot Container Storage Interface (CSI), non è necessario specificare una posizione per lo snapshot perché verrà creato un CR VolumeSnapshotClass per registrare il driver CSI. Nel nostro esempio, utilizzi Trident CSI e in precedenza hai creato VolumeSnapShotClass CR utilizzando il driver Trident CSI.

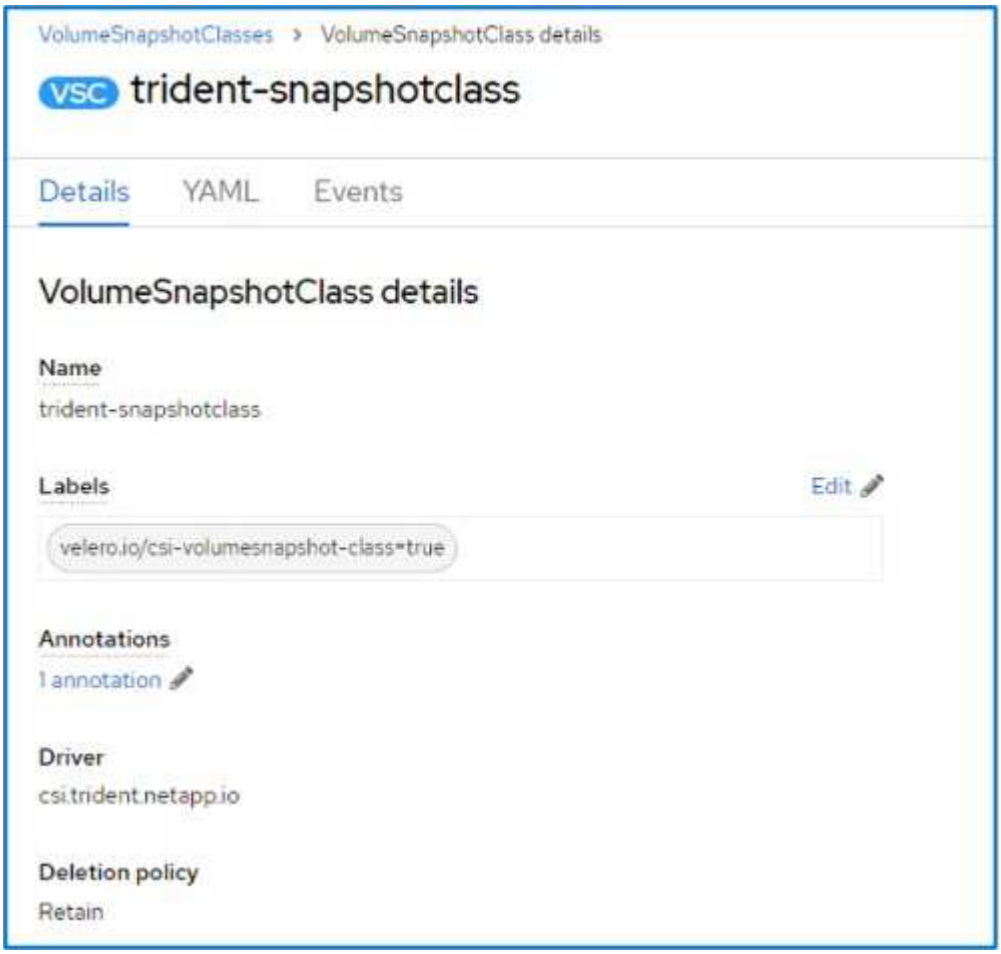
Abilita il plugin CSI Aggiungi csi ai plugin predefiniti per Velero per eseguire il backup di volumi persistenti con snapshot CSI. I plugin Velero CSI, per eseguire il backup dei PVC supportati da CSI, sceglieranno VolumeSnapshotClass nel cluster su cui è impostata l'etichetta **velero.io/csi-volumesnapshot-class**. Per questo

- È necessario aver creato il tridente VolumeSnapshotClass.
- Modifica l'etichetta della classe trident-snapshot e impostala su **velero.io/csi-volumesnapshot-class=true** come mostrato di seguito.

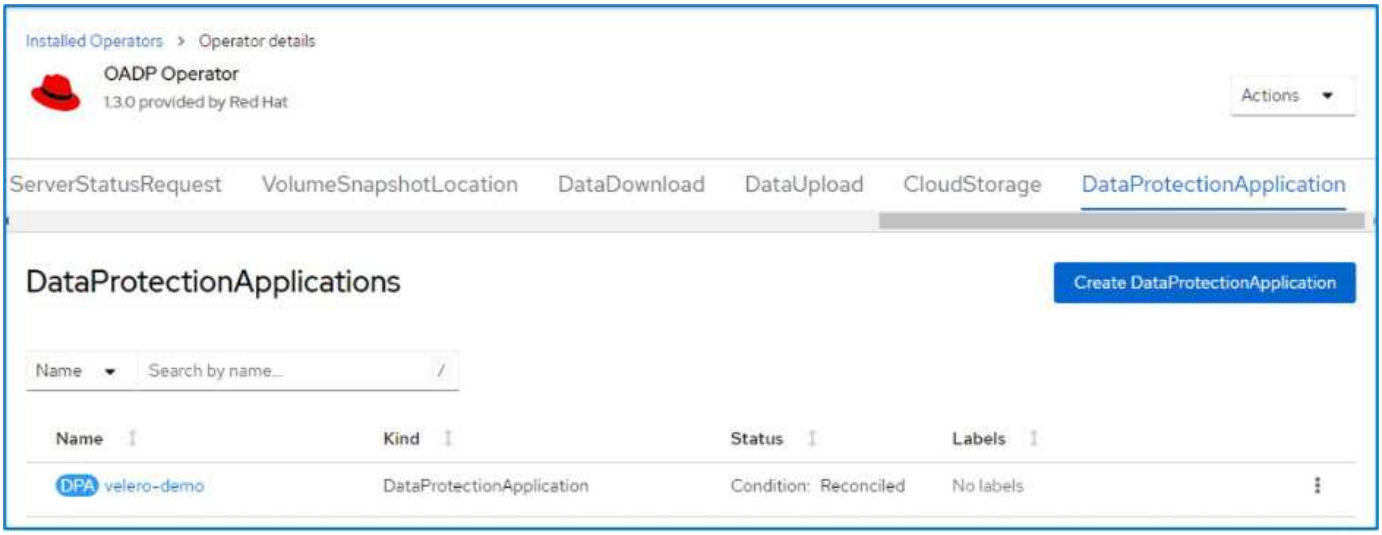


Assicurarsi che gli snapshot possano essere mantenuti anche se gli oggetti VolumeSnapshot vengono eliminati. Ciò può essere fatto impostando **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi comporterà la perdita completa di tutti i PVC in esso contenuti.

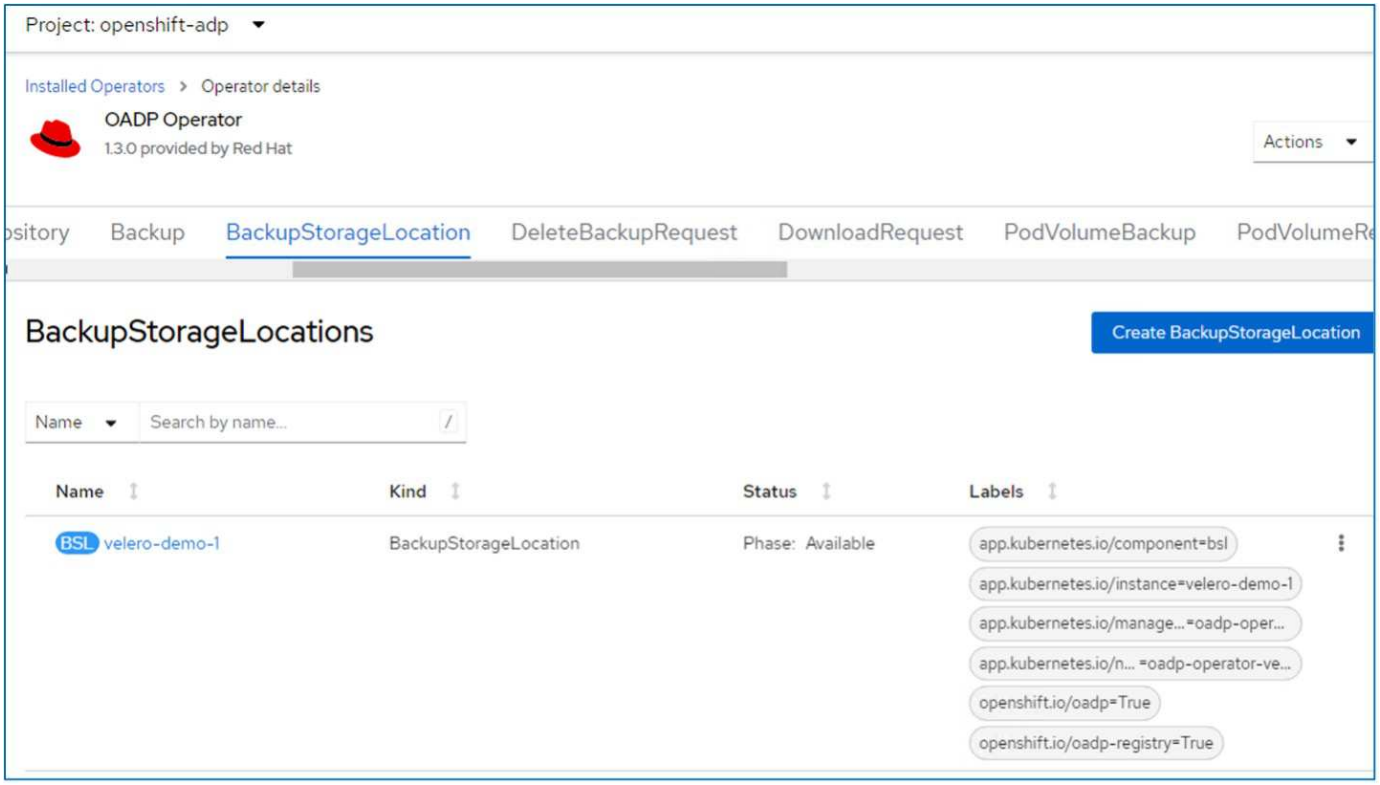
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Assicurarsi che DataProtectionApplication sia stato creato e che sia in condizione: Riconciliato.



L'operatore OADP creerà un BackupStorageLocation corrispondente. Questo verrà utilizzato durante la creazione di un backup.



Creazione di backup su richiesta per le app in OpenShift Container Platform

Questa sezione descrive come creare un backup su richiesta per le VM in OpenShift Virtualization.

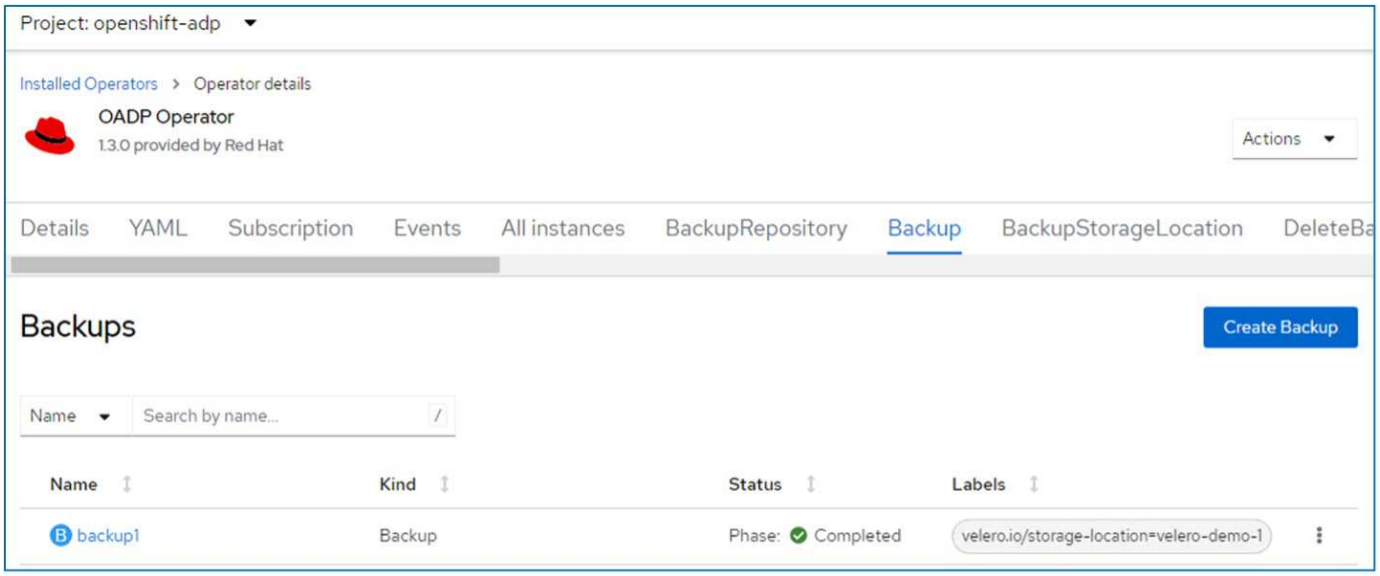
Passaggi per creare un backup di un'app

Per creare un backup su richiesta di un'app (metadati dell'app e volumi persistenti dell'app), fai clic sulla scheda **Backup** per creare una Backup Custom Resource (CR). Viene fornito un file yaml di esempio per creare la Backup CR. Utilizzando questo yaml, verrà eseguito il backup dell'app e del suo storage persistente nel namespace specificato. Puoi impostare parametri aggiuntivi come mostrato nell'"documentazione".

Il CSI creerà uno snapshot dei volumi persistenti e delle risorse dell'app nello spazio dei nomi specificato. Questo snapshot verrà archiviato nella posizione di backup specificata nel file yaml. Il backup rimarrà nel sistema per 30 giorni, come specificato nel ttl.

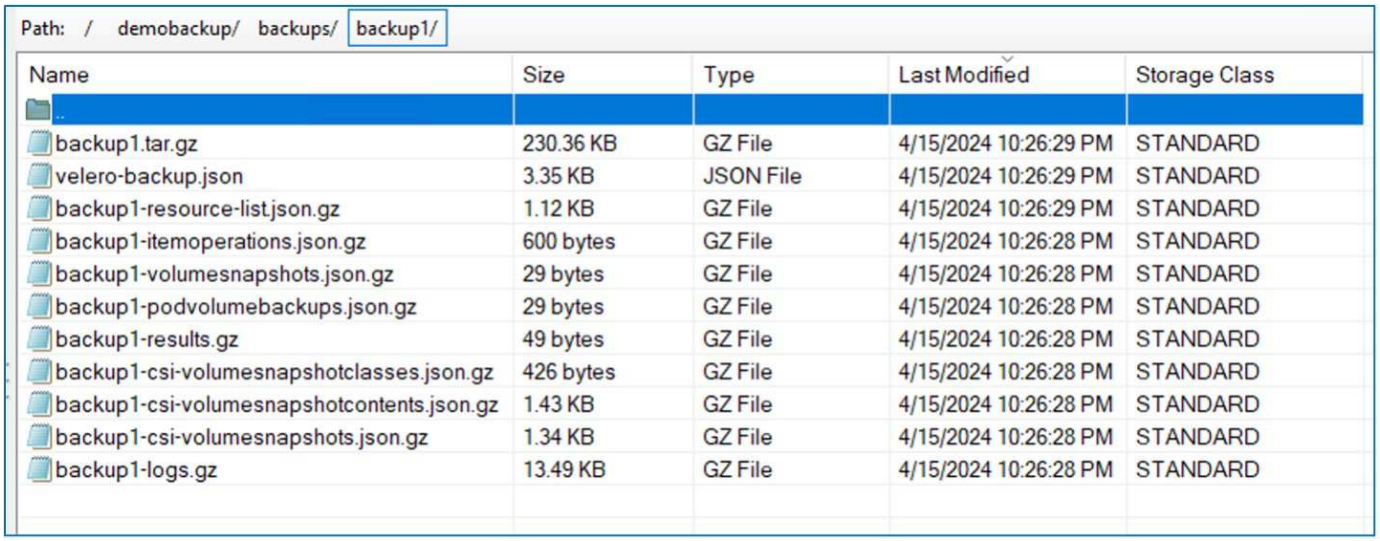
```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
  ttl: 720h0m0s
```

Una volta completato il backup, la relativa fase verrà visualizzata come completata.



È possibile ispezionare il backup nell'archivio oggetti con l'ausilio di un'applicazione browser S3. Il percorso del backup viene visualizzato nel bucket configurato con il nome del prefisso (velero/container-demo-backup). È possibile visualizzare il contenuto del backup, inclusi gli snapshot del volume, i registri e altri metadati dell'applicazione.

In StorageGrid è anche possibile utilizzare la console S3 disponibile in Tenant Manager per visualizzare gli oggetti di backup.



Creazione di backup pianificati per le app

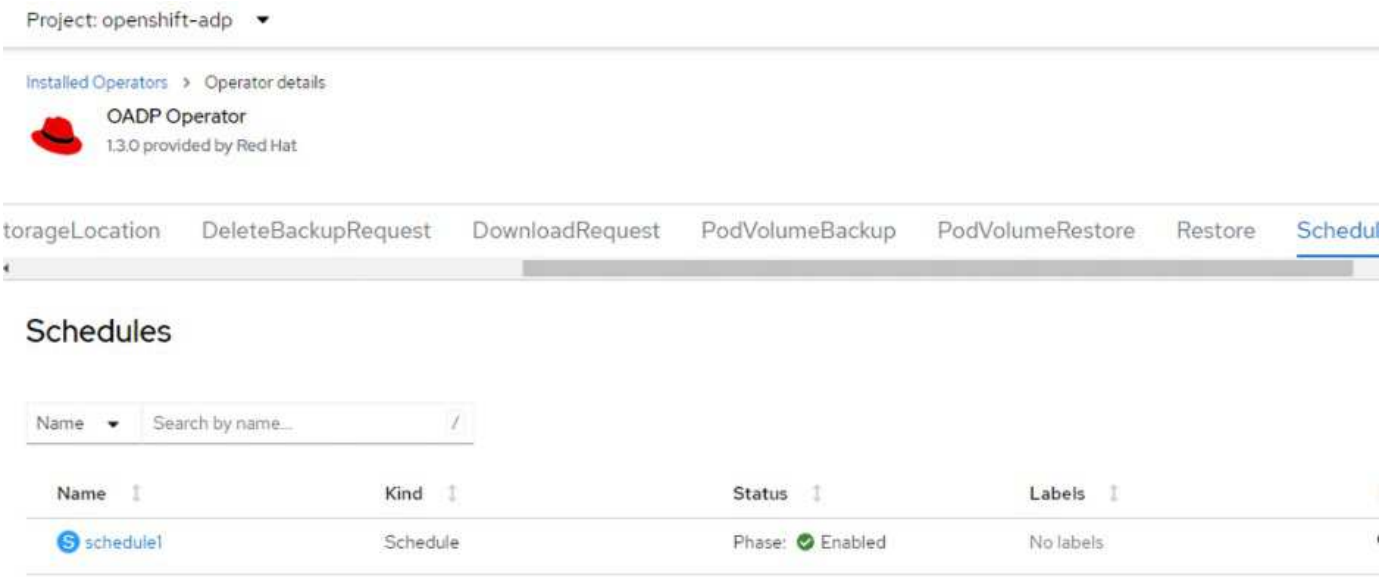
Per creare backup pianificati, è necessario creare un CR pianificato. La pianificazione è semplicemente un'espressione Cron che consente di specificare l'ora in cui si desidera creare il backup. Di seguito è riportato un esempio di file yaml per creare una Schedule CR.

```
apiVersion: velero.io/v1
kind: Schedule
```

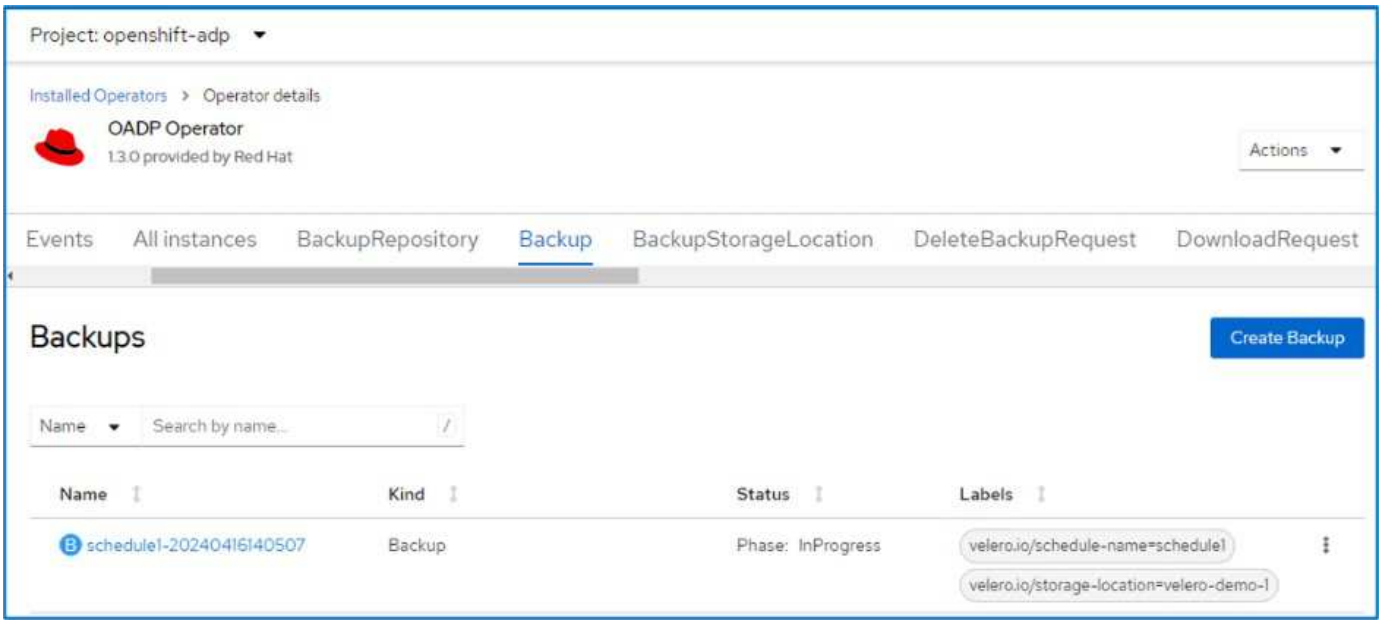
```
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

L'espressione Cron 0 7 * * * significa che ogni giorno verrà creato un backup alle 7:00. Vengono inoltre specificati gli spazi dei nomi da includere nel backup e la posizione di archiviazione per il backup. Quindi, invece di un Backup CR, viene utilizzato il metodo Schedule CR per creare un backup all'ora e con la frequenza specificate.

Una volta creata, la pianificazione sarà abilitata.



I backup verranno creati in base a questa pianificazione e potranno essere visualizzati nella scheda Backup.



Migrare un'app da un cluster a un altro

Le funzionalità di backup e ripristino di Velero lo rendono uno strumento prezioso per la migrazione dei dati tra cluster. Questa sezione descrive come migrare le app da un cluster a un altro creando un backup dell'app nell'archivio oggetti da un cluster e quindi ripristinando l'app dallo stesso archivio oggetti a un altro cluster. .

▼ **Backup dal primo cluster**

Prerequisiti per il Cluster 1

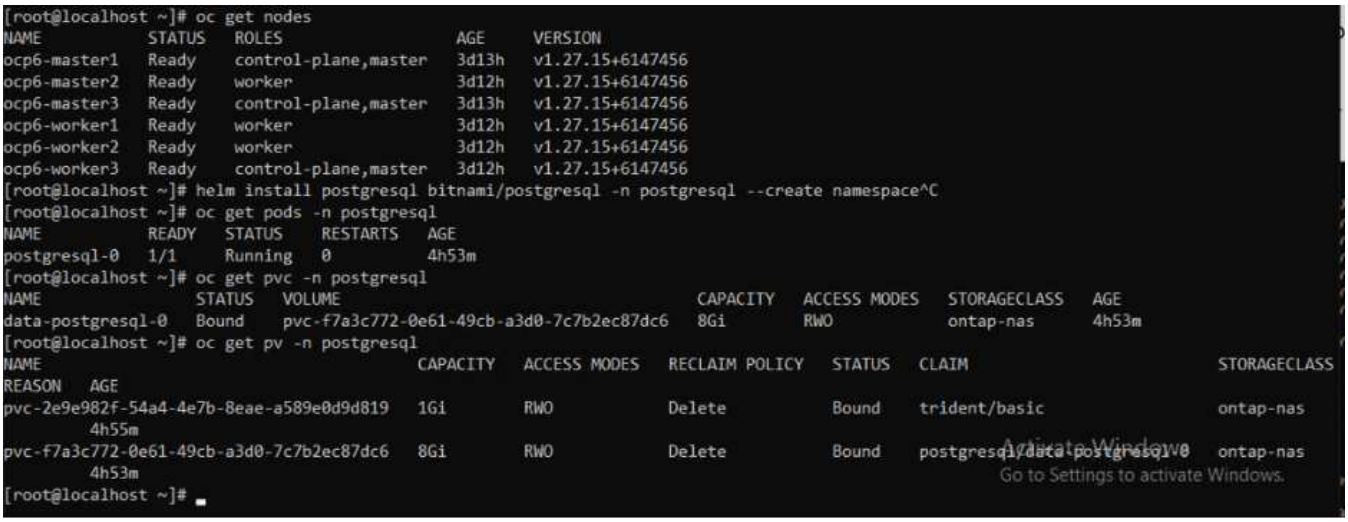
- Trident deve essere installato sul cluster.
- È necessario creare un backend Trident e una classe Storage.
- L'operatore OADP deve essere installato sul cluster.
- DataProtectionApplication deve essere configurato.

Utilizzare la seguente specifica per configurare l'oggetto DataProtectionApplication.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
```

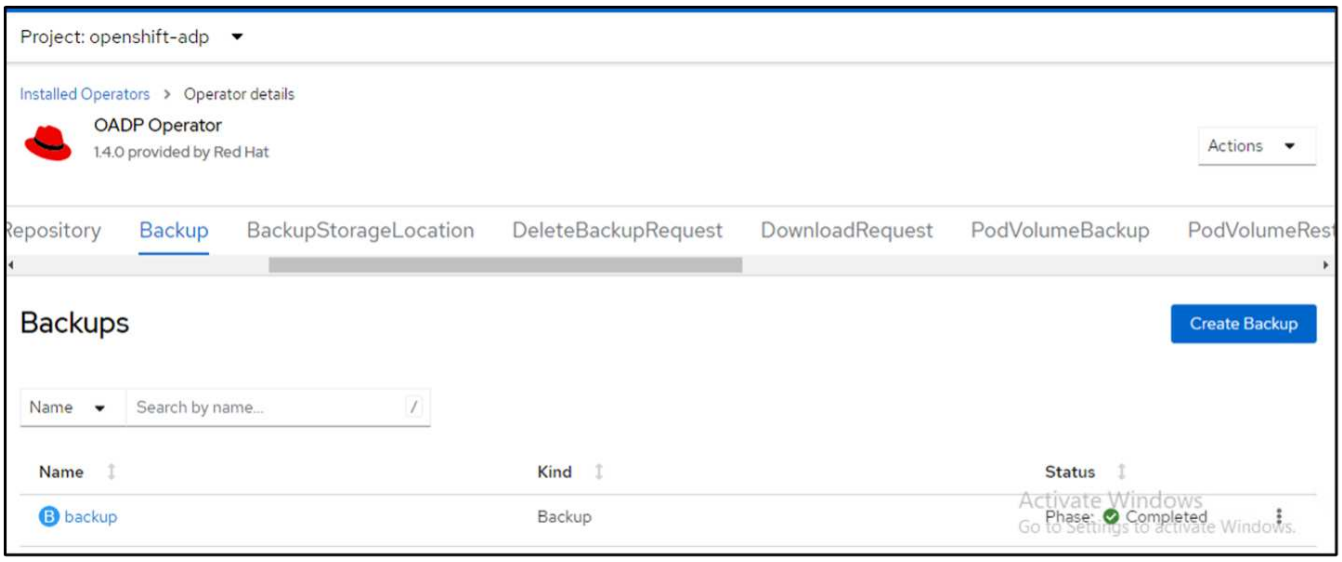
```
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Creare un'applicazione sul cluster ed eseguirne un backup. Ad esempio, installa un'applicazione Postgres.



- Utilizzare la seguente specifica per il CR di backup:

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



È possibile fare clic sulla scheda **Tutte le istanze** per visualizzare i diversi oggetti creati e in movimento attraverso le diverse fasi, fino ad arrivare infine alla fase di backup **completato**.

Un backup delle risorse nello spazio dei nomi postgresql verrà archiviato nella posizione Object Storage (ONTAP S3) specificata in backupLocation nella specifica OADP.

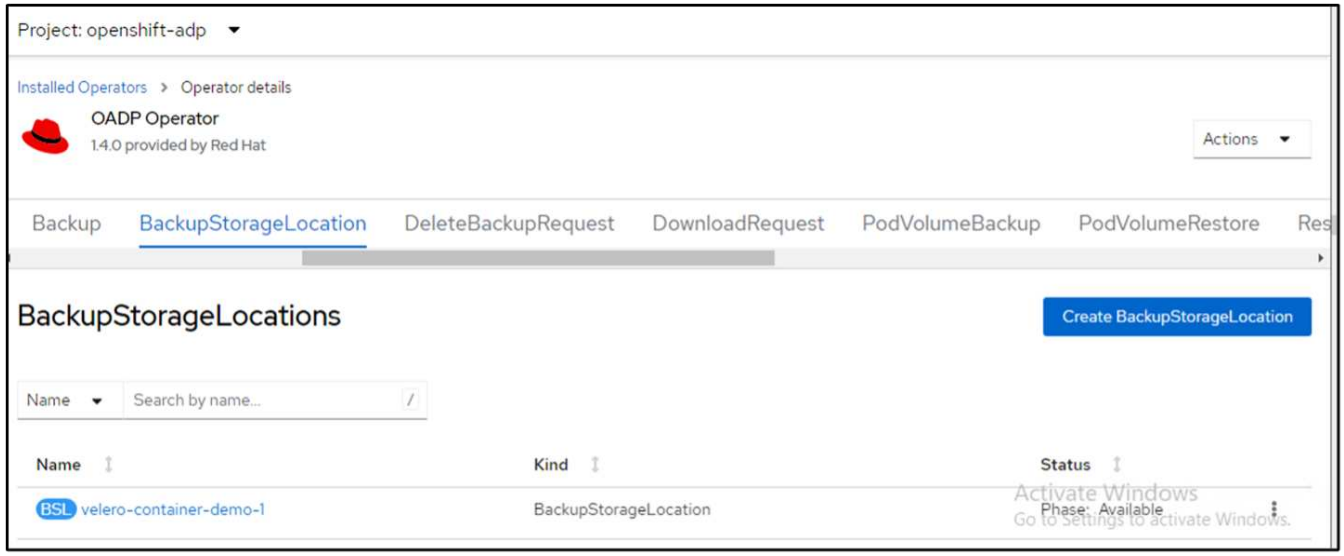
▼ **Ripristinare un secondo cluster**

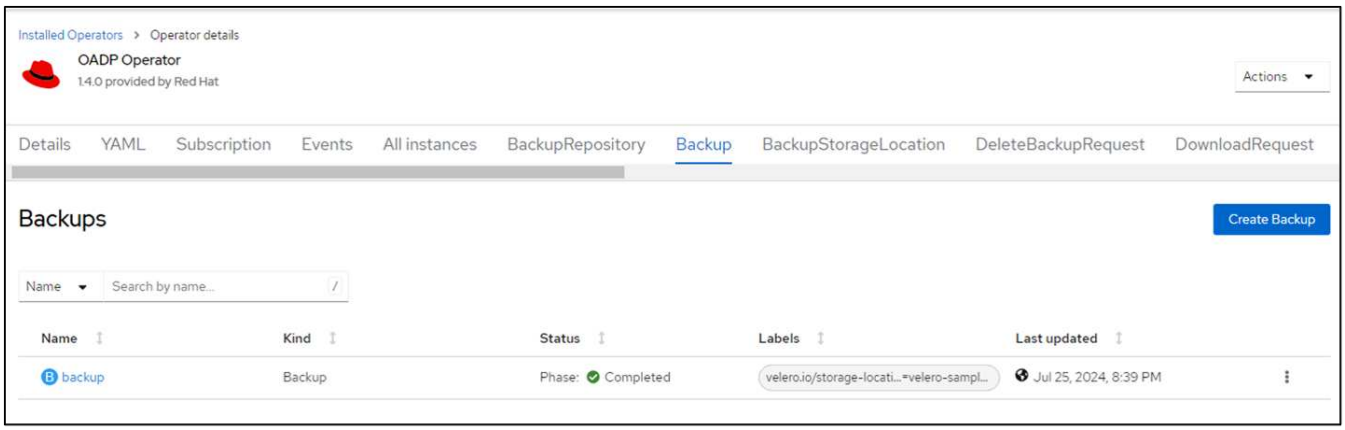
Prerequisiti per il Cluster 2

- Trident deve essere installato sul cluster 2.
- L'app PostgreSQL NON deve essere già installata nello spazio dei nomi PostgreSQL.
- L'operatore OADP deve essere installato sul cluster 2 e BackupStorage Location deve puntare alla stessa posizione di archiviazione degli oggetti in cui è stato archiviato il backup dal primo cluster.
- Il CR di backup deve essere visibile dal secondo cluster.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic        ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc     vsphere-sc              2d7
h
[root@localhost ~]#
```



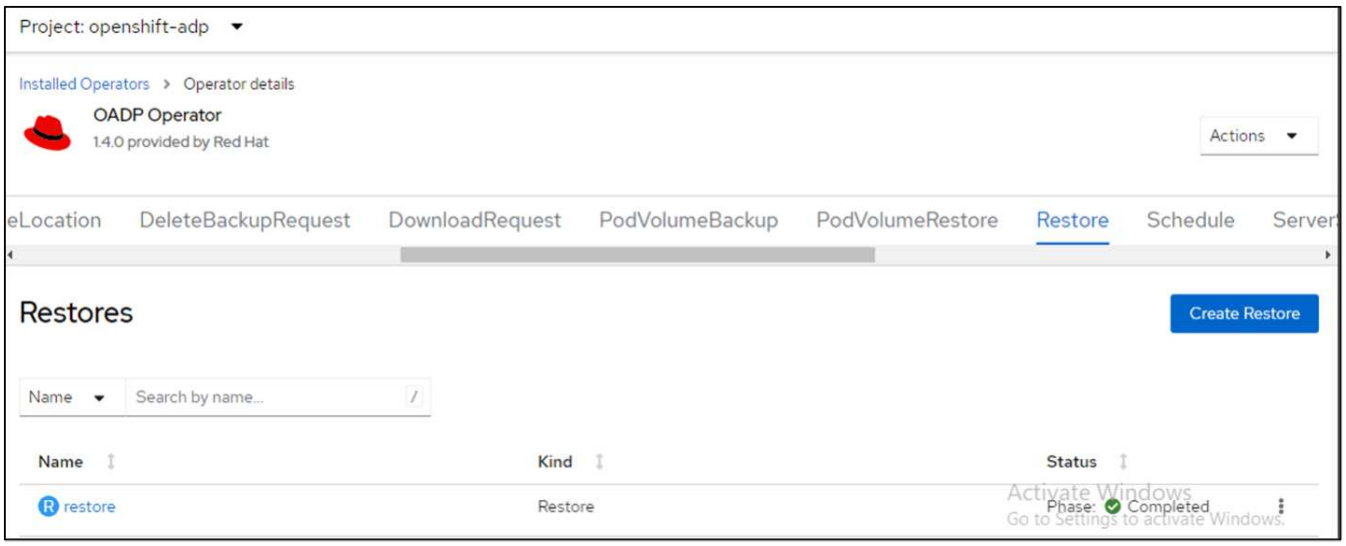


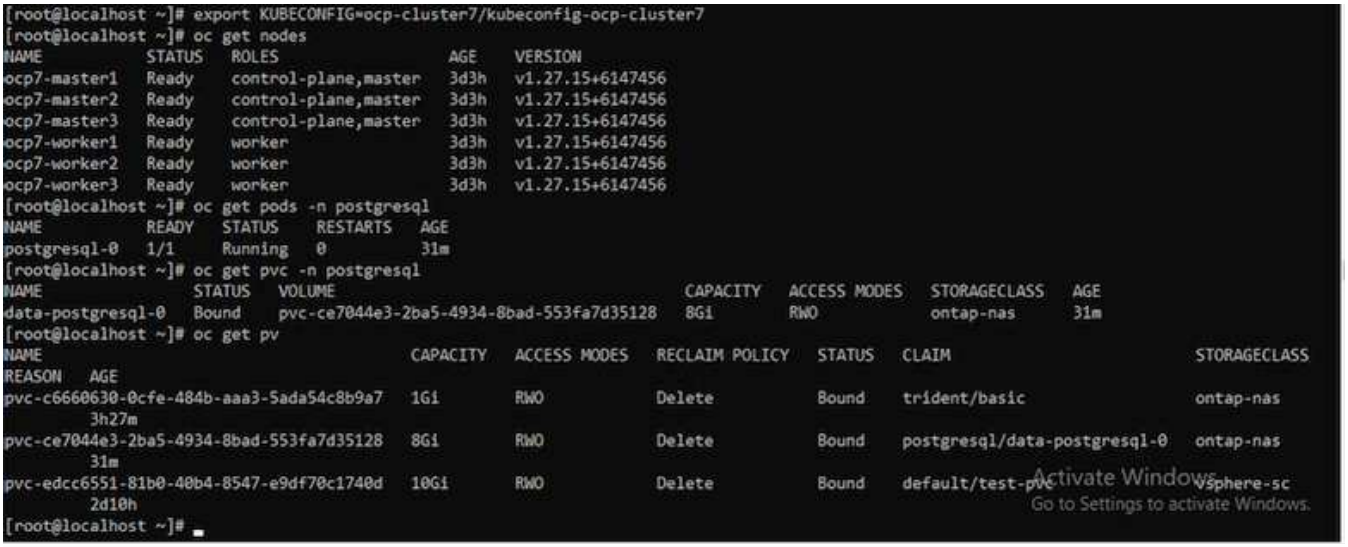
Ripristina l'app su questo cluster dal backup. Utilizzare il seguente yaml per creare il ripristino CR.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
```

```
  backupName: backup
  restorePVs: true
```

Una volta completato il ripristino, vedrai che l'app PostgreSQL è in esecuzione su questo cluster ed è associata al PVC e a un PV corrispondente. Lo stato dell'app è lo stesso di quando è stato effettuato il backup.





Ripristinare un'app da un backup

Questa sezione descrive come ripristinare le app da un backup.

Prerequisiti

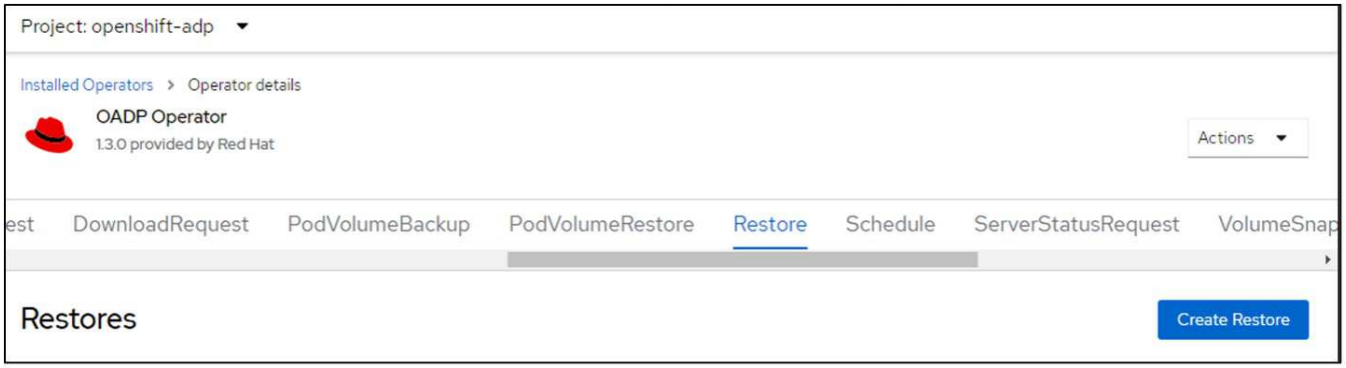
Per ripristinare da un backup, supponiamo che lo spazio dei nomi in cui era presente l'app sia stato eliminato accidentalmente.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

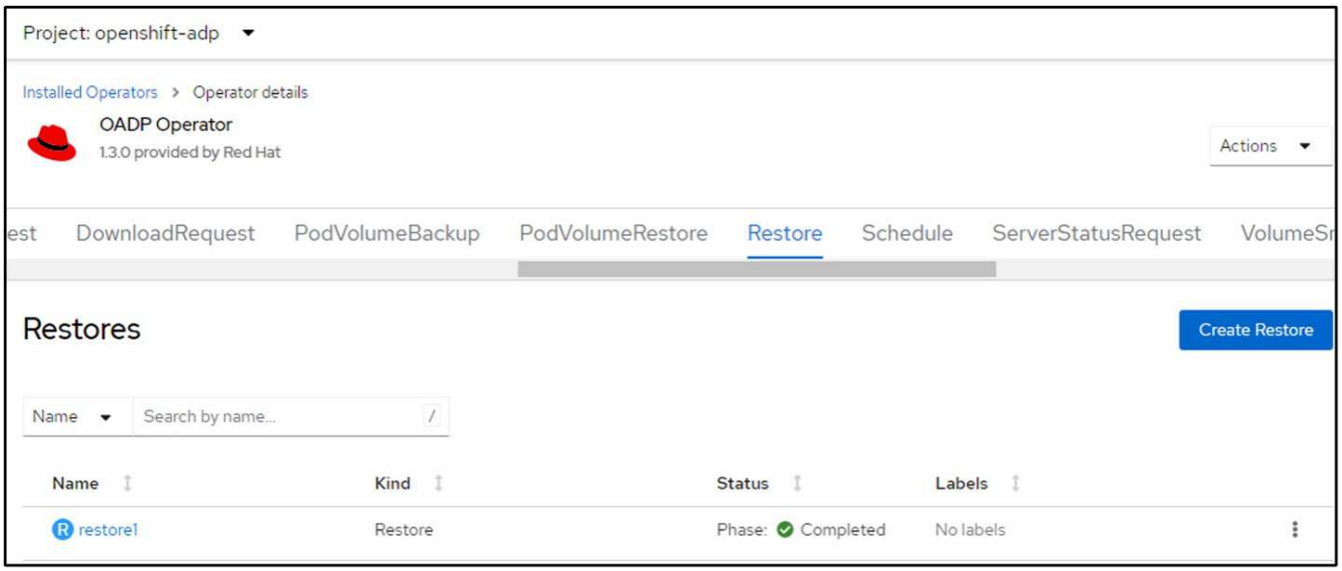
▼ **Ripristina nello stesso namespace**

Per ripristinare dal backup che hai appena creato, devi creare una risorsa di ripristino personalizzata (CR). Devi assegnarle un nome, specificare il nome del backup da cui vuoi eseguire il ripristino e impostare restorePVs su true. Puoi impostare parametri aggiuntivi come mostrato nella "documentazione". Fai clic sul pulsante Create.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Quando la fase risulta completata, puoi vedere che l'app è stata ripristinata allo stato in cui era stata scattata l'istantanea. L'app viene ripristinata nello stesso namespace.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ **Ripristina in uno spazio dei nomi diverso**

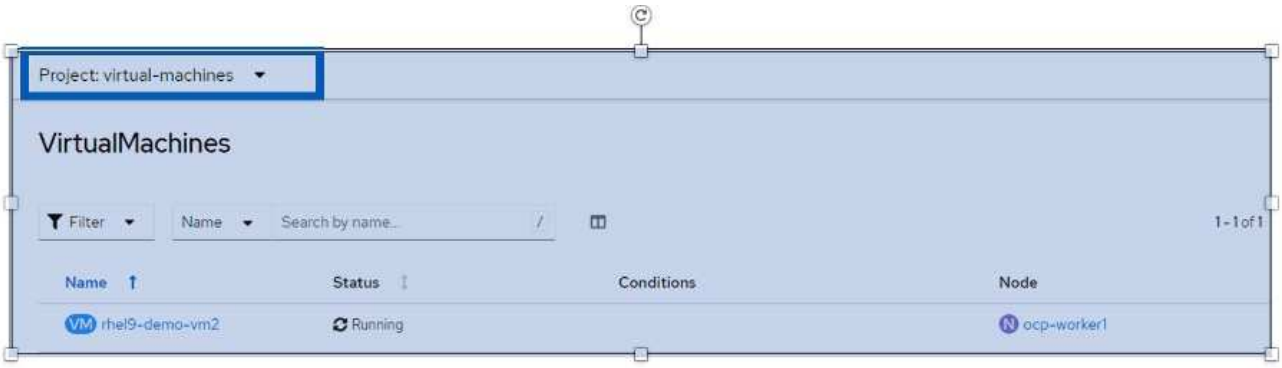
Per ripristinare l'app in uno spazio dei nomi diverso, puoi fornire un namespaceMapping nella definizione yaml del Restore CR.

Il seguente file yaml di esempio crea un ripristino CR per ripristinare un'app e il suo archivio persistente dallo spazio dei nomi postgresql al nuovo spazio dei nomi postgresql-restored.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
```

```
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

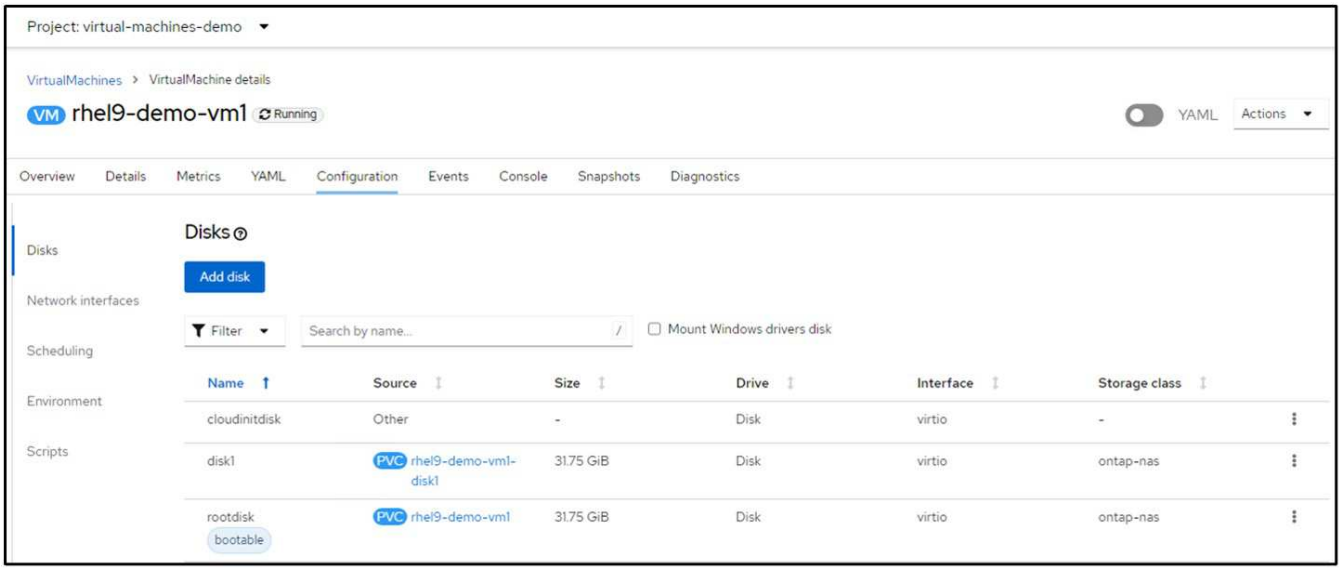
Quando la fase risulta completata, puoi vedere che l'app è stata ripristinata allo stato in cui era stata scattata l'istantanea. L'app viene ripristinata in uno spazio dei nomi diverso, come specificato nello yaml.

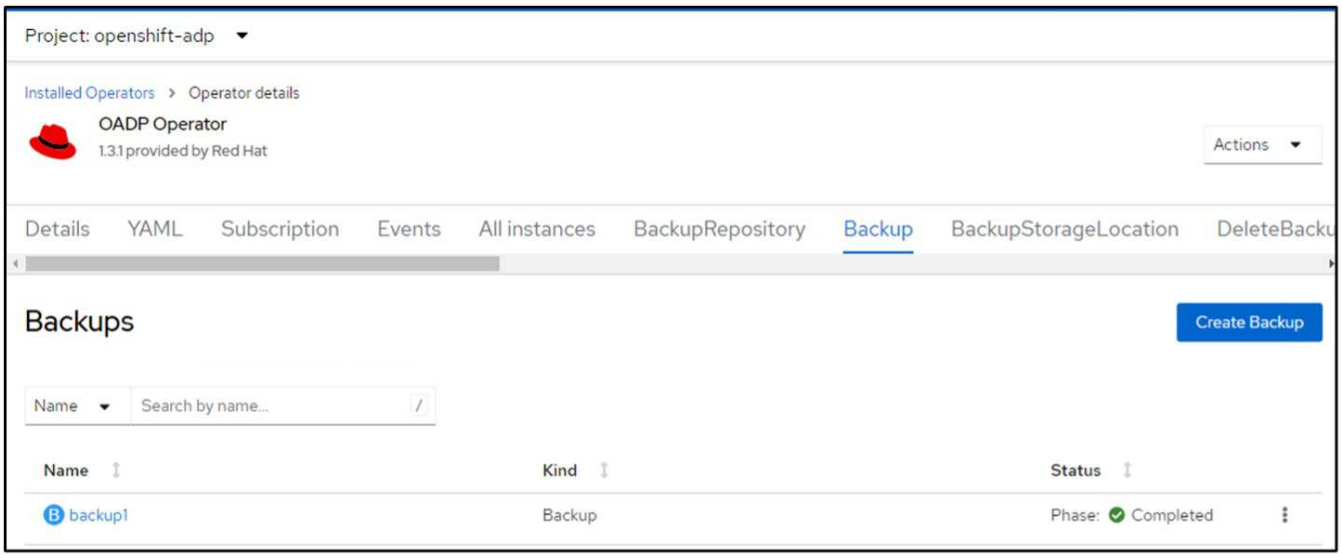


▼ **Ripristina in una classe di archiviazione diversa**

Velero offre la possibilità generica di modificare le risorse durante il ripristino specificando patch JSON. Le patch json vengono applicate alle risorse prima che vengano ripristinate. Le patch json sono specificate in una configmap e la configmap è referenziata nel comando restore. Questa funzionalità consente di eseguire il ripristino utilizzando classi di archiviazione diverse.

Nell'esempio seguente, l'app, durante la distribuzione, utilizza ontap-nas come classe di archiviazione per i suoi volumi persistenti. Viene creato un backup dell'app denominato backup-postgresql-ontaps3.





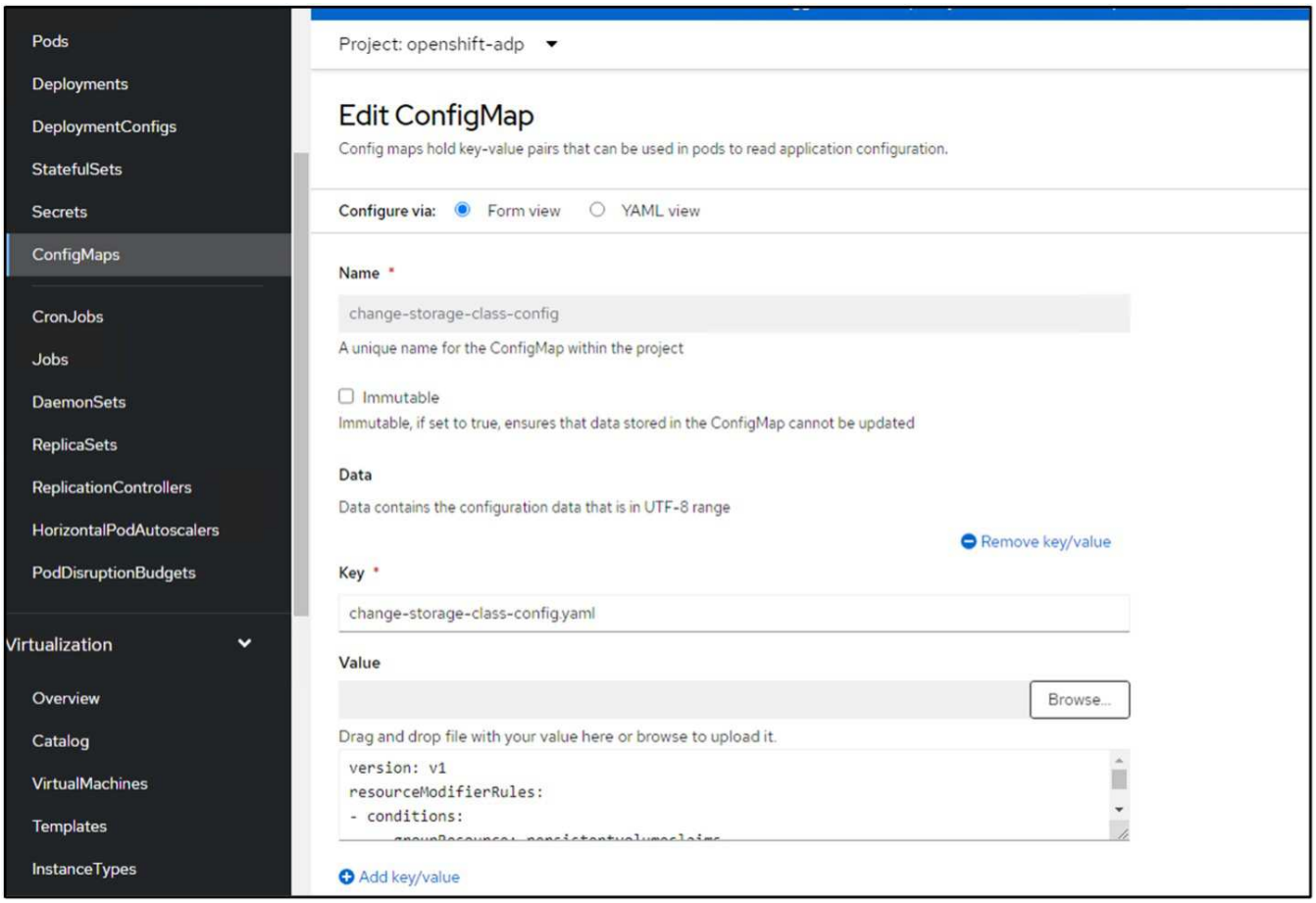
Simula la perdita dell'app disinstallandola.

Per ripristinare la VM utilizzando una classe di archiviazione diversa, ad esempio la classe di archiviazione ontap-nas-eco, è necessario eseguire i due passaggi seguenti:

Passaggio 1

Crea una mappa di configurazione (console) nello spazio dei nomi openshift-adp come segue: Compila i dettagli come mostrato nello screenshot: Seleziona lo spazio dei nomi: openshift-adp Nome: change-ontap-sc (può essere qualsiasi nome) Chiave: change-ontap-sc-config.yaml: Valore:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



L’oggetto mappa di configurazione risultante dovrebbe apparire così (CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"


BinaryData
====

Events:  <none>
```

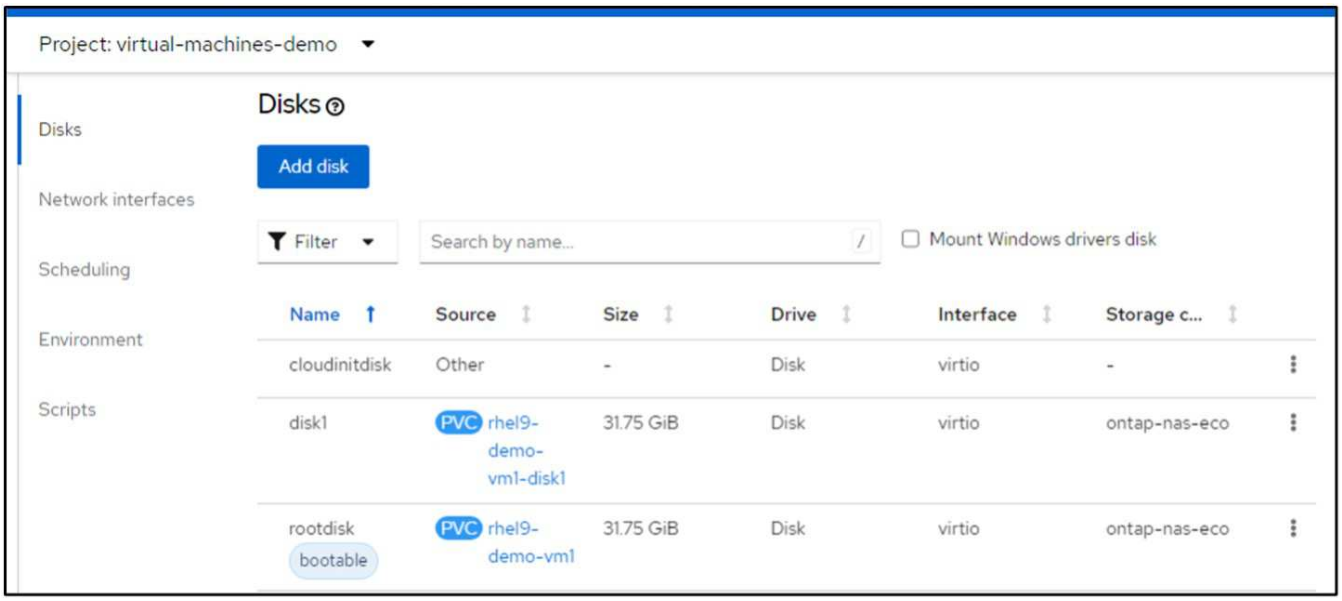
Questa mappa di configurazione applicherà la regola del modificatore di risorse quando viene creato il ripristino. Verrà applicata una patch per sostituire il nome della classe di archiviazione in ontap-nas-eco per tutte le richieste di volume persistenti che iniziano con rhel.

Passaggio 2

Per ripristinare la VM utilizzare il seguente comando dalla CLI di Velero:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

L'app viene ripristinata nello stesso namespace con le richieste di volume persistenti create utilizzando la classe di archiviazione ontap-nas-eco.



Eliminazione di backup e ripristini utilizzando Velero

Questa sezione descrive come eliminare backup e ripristini di app nella piattaforma container OpenShift utilizzando Velero.

Elenca tutti i backup

È possibile elencare tutti i CR di backup utilizzando lo strumento OC CLI o lo strumento Velero CLI. Scarica Velero CLI come indicato nelle istruzioni nel"Documentazione Velero" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminazione di un backup

È possibile eliminare un Backup CR senza eliminare i dati di Object Storage utilizzando lo strumento OC CLI. Il backup verrà rimosso dall'output CLI/Console. Tuttavia, poiché il backup corrispondente non viene rimosso dall'archivio oggetti, riapparirà nell'output della CLI/console.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

Se si desidera eliminare il CR di backup e i dati di archiviazione degli oggetti associati, è possibile farlo utilizzando lo strumento Velero CLI.

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Eliminazione del ripristino

È possibile eliminare l'oggetto Restore CR utilizzando OC CLI o Velero CLI

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

Guarda video e demo sulle soluzioni multicloud ibride con NetApp

Guarda i video sulle soluzioni multicloud ibride per Amazon Web Services con NetApp

Esplora la libreria video completa di NetApp con soluzioni multicloud ibride per AWS con NetApp. Guarda i video sullo storage connesso agli ospiti, sui risparmi sul costo totale di proprietà, sugli archivi dati supplementari e sui flussi di lavoro di migrazione per VMware Cloud on AWS e Amazon FSx for ONTAP, inclusi gli scenari Windows e Linux.

Archiviazione connessa agli ospiti

Archiviazione connessa guest Windows con FSx ONTAP tramite iSCSI

Archiviazione connessa guest Linux con FSx ONTAP tramite NFS

TCO e datastore supplementari

Risparmio sul TCO di VMware Cloud su AWS con Amazon FSx ONTAP

Datastore supplementare VMware Cloud su AWS con Amazon FSx ONTAP

Flussi di lavoro di migrazione (HCX)

Configurazione e distribuzione di VMware HCX per VMC

Dimostrazione di migrazione vMotion con VMware HCX per VMC e FSx ONTAP

Dimostrazione di migrazione a freddo con VMware HCX per VMC e FSx ONTAP

Guarda i video sulle soluzioni multicloud ibride per il cloud Azure VMware con NetApp

Esplora la libreria video completa di NetApp con soluzioni multicloud ibride per Azure VMware Solution (AVS) con NetApp. Questa raccolta include video su datastore supplementari, disaster recovery e flussi di lavoro di migrazione.

Datastore supplementari

Panoramica del datastore supplementare della soluzione Azure VMware con Azure NetApp Files

Ripristino dopo un disastro

Soluzione Azure VMware DR con Cloud Volumes ONTAP, SnapCenter e JetStream

Flussi di lavoro di migrazione (HCX)

Dimostrazione di migrazione a freddo con VMware HCX per AVS e ANF

Dimostrazione vMotion con VMware HCX per AVS e ANF

Dimostrazione di migrazione in blocco con VMware HCX per AVS e ANF

Guarda i video sulle soluzioni multicloud ibride per Red Hat OpenShift con NetApp

Esplora la completa libreria video di NetApp con soluzioni multicloud ibride per Red Hat OpenShift con NetApp. Questa raccolta include demo su snapshot e ripristino per OpenShift su AWS (ROSA) con FSx ONTAP, integrazione con Trident, failover e fail-back per app e distribuzione automatizzata di Oracle RAC su FlexPod con Ansible.

Istantanee e ripristino

Snapshot/ripristino per applicazioni su cluster Red Hat OpenShift Service on AWS (ROSA) con storage Amazon FSx ONTAP

Integrazione dello storage

Integrazione di FSx ONTAP con Trident

Failover e fail-back

Failover e fail-back delle app su ROSA con FSx ONTAP

Automazione delle soluzioni



Distribuzione automatizzata di Oracle 19c RAC su FlexPod con Ansible

Leggi i blog sulle soluzioni cloud degli esperti NetApp

Leggi i blog che offrono indicazioni pratiche e best practice per integrare lo storage ONTAP con le soluzioni cloud NetApp .

Integrazione VMware con AWS e Amazon FSx per ONTAP

- "Migrare le VM VMware su AWS utilizzando Amazon EC2 e il protocollo iSCSI Amazon FSx ONTAP"
- "Amazon EVS ora si integra con FSx per ONTAP"
- "Amazon EVS annuncia il supporto per FSx per ONTAP"
- "Configurare Hybrid Cloud con FSx ONTAP e VMware Cloud su AWS SDDC utilizzando VMware HCX"

Soluzione Azure VMware

- "Ottimizza lo storage e i carichi di lavoro VMware ad alta intensità di dati in qualsiasi cloud"
- "Carichi di lavoro VMware su Azure VMware Solution? Leggi prima questo."

Motore VMware di Google Cloud

- "Supporto del datastore Google Cloud NetApp Volumes per Google Cloud VMware Engine (NetApp)"
- "Come utilizzare NetApp Volumes come datastore per Google Cloud VMware Engine (Google)"
- "Blog NetApp : un modo migliore per migrare le tue app ad alto contenuto di storage su Google Cloud"

Protezione e gestione dei dati

- "Protezione dei dati 3-2-1 per VMware con SnapCenter Plug-in e NetApp Backup and Recovery per le VM"
- "Osservabilità per il data center moderno con NetApp Cloud Insights"

NetApp per carichi di lavoro dei container OpenShift

- "NetApp ONTAP funge anche da storage per i log nella piattaforma container Red Hat OpenShift"

VMware Sovereign Cloud

- "Presentazione della nuova iniziativa Sovereign Cloud"

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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