Virtualizzazione VMware

NetApp Solutions

NetApp
September 26, 2024

Sommario

Soluzioni NetApp per la virtualizzazione con VMware di Broadcom

VMware vSphere con ONTAP

ONTAP è da quasi vent'anni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione e ridurre i costi. Questo documento presenta la soluzione ONTAP per vSphere, incluse le informazioni più recenti sui prodotti e le Best practice, per ottimizzare l'implementazione, ridurre i rischi e semplificare la gestione.

Per ulteriori informazioni, visitare il sito "VMware vSphere con ONTAP"

VMware vSphere Foundation (Fondazione VMware vSphere)

NFS Reference Guide for vSphere 8

NFS v3 - Guida di riferimento per vSphere 8

VMware vSphere Foundation (VVF) è una piattaforma Enterprise in grado di fornire vari workload virtualizzati. Il nucleo di vSphere è VMware vCenter, l'hypervisor ESXi, i componenti di networking e i vari servizi delle risorse. In combinazione con ONTAP, le infrastrutture virtualizzate basate su VMware offrono notevoli vantaggi in termini di flessibilità, scalabilità e funzionalità.

Utilizzo di NFS v3 con vSphere 8 e dei sistemi storage ONTAP

Il presente documento fornisce informazioni sulle opzioni di storage disponibili per VMware Cloud vSphere Foundation utilizzando gli array all-flash di NetApp. Le opzioni di storage supportate sono coperte con istruzioni specifiche per l'implementazione di datastore NFS. Inoltre, viene dimostrato VMware Live Site Recovery per il disaster recovery dei datastore NFS. Infine, viene esaminata la protezione autonoma da ransomware di NetApp per lo storage NFS.

Casi di utilizzo

Casi d'utilizzo illustrati nella presente documentazione:

- Opzioni di storage per i clienti che cercano ambienti uniformi su cloud pubblici e privati.
- Implementazione di un'infrastruttura virtuale per i carichi di lavoro.
- Soluzione storage scalabile realizzata su misura per soddisfare esigenze in evoluzione, anche se non allineata direttamente ai requisiti delle risorse di calcolo.
- Proteggi macchine virtuali e datastore utilizzando il plug-in SnapCenter per VMware vSphere.
- Utilizzo di VMware Live Site Recovery per il disaster recovery dei datastore NFS.
- Strategia di rilevamento del ransomware, con diversi livelli di protezione a livello di host ESXi e VM guest.

Pubblico

Questa soluzione è destinata alle seguenti persone:

- Architetti delle soluzioni alla ricerca di opzioni di storage più flessibili per ambienti VMware che siano progettati per massimizzare il TCO.
- Solution Architect in cerca di opzioni storage VVF che offrono opzioni di protezione dei dati e disaster recovery con i principali cloud provider.
- Amministratori dello storage che desiderano istruzioni specifiche su come configurare il VVF con lo storage NFS.
- Amministratori dello storage che desiderano istruzioni specifiche su come proteggere macchine virtuali e datastore che risiedono sullo storage ONTAP.

Panoramica sulla tecnologia

La guida di riferimento VVF di NFS v3 per vSphere 8 è costituita dai seguenti componenti principali:

VMware vSphere Foundation (Fondazione VMware vSphere)

Componente centrale di vSphere Foundation, VMware vCenter è una piattaforma di gestione centralizzata per la configurazione, il controllo e l'amministrazione degli ambienti vSphere. VCenter funge da base per la gestione delle infrastrutture virtualizzate, consentendo agli amministratori di implementare, monitorare e gestire macchine virtuali, container e host ESXi all'interno dell'ambiente virtuale.

La soluzione VVF supporta sia i workload Kubernetes nativi che quelli basati su macchine virtuali. I componenti chiave includono:

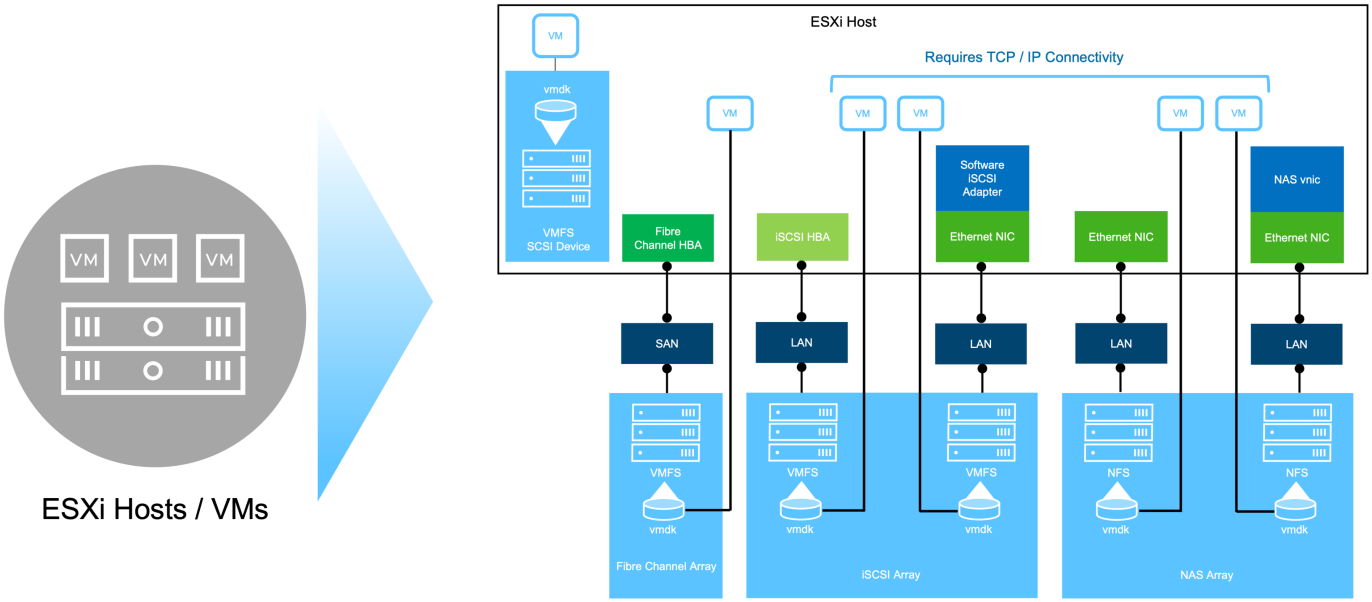
- VMware vSphere
- VMware vSAN
- Aria standard
- VMware Tanzu Kubernetes Grid Service per vSphere
- Switch distribuito vSphere

Per ulteriori informazioni sui componenti inclusi nel VVF, fare riferimento all'architettura e alla pianificazione, fare riferimento a "Confronto live dei prodotti VMware vSphere".

Opzioni di archiviazione VVF

Lo storage è un elemento centrale di un ambiente virtuale potente e di successo. Lo storage tramite datastore VMware o casi di utilizzo connessi agli ospiti libera le capacità dei tuoi carichi di lavoro poiché puoi scegliere il miglior prezzo per GB che offra il massimo valore riducendo al contempo il sottoutilizzo. ONTAP è da quasi vent'anni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione e ridurre i costi.

Di norma, le opzioni storage VMware sono organizzate come offerte storage tradizionali e software-defined storage. I modelli di storage tradizionali comprendono storage locale e di rete, mentre i modelli di storage software-defined comprendono vSAN e volumi virtuali VMware (vVol).



Per "Introduzione allo storage nell'ambiente vSphere" ulteriori informazioni sui tipi di storage supportati per VMware vSphere Foundation, fare riferimento a .

NetApp ONTAP

Esistono numerosi motivi interessanti per cui decine di migliaia di clienti hanno scelto ONTAP come soluzione di storage primario per vSphere. Questi includono quanto segue:

1. **Sistema di storage unificato:** ONTAP offre un sistema di storage unificato che supporta protocolli SAN e NAS. Questa versatilità consente un'integrazione perfetta di varie tecnologie di storage all'interno di un'unica soluzione.
2. **Solida protezione dei dati:** ONTAP offre solide funzionalità di protezione dei dati tramite istantanee efficienti in termini di spazio. Queste istantanee consentono processi di backup e ripristino efficienti, garantendo la sicurezza e l'integrità dei dati delle applicazioni.
3. **Strumenti di gestione completi:** ONTAP offre una vasta gamma di strumenti progettati per aiutare a gestire efficacemente i dati delle applicazioni. Questi tool semplificano le attività di gestione dello storage, migliorando l'efficienza operativa e semplificando l'amministrazione.
4. **Efficienza dello storage:** ONTAP include diverse funzioni di efficienza dello storage, abilitate per impostazione predefinita, progettate per ottimizzare l'utilizzo dello storage, ridurre i costi e migliorare le prestazioni complessive del sistema.

L'utilizzo di ONTAP con VMware offre una grande flessibilità quando si tratta di specifiche esigenze applicative. Sono supportati i seguenti protocolli come datastore VMware con utilizzo di ONTAP: * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4,1

L'utilizzo di un sistema storage separato dall'hypervisor consente di trasferire molte funzioni e massimizzare l'investimento nei sistemi host vSphere. Questo approccio non solo garantisce che le risorse host siano incentrate sui carichi di lavoro delle applicazioni, ma evita anche effetti casuali sulle performance delle applicazioni derivanti dalle operazioni di storage.

L'utilizzo di ONTAP insieme a vSphere è un'ottima combinazione che consente di ridurre le spese relative all'hardware host e al software VMware. Puoi anche proteggere i tuoi dati a un costo inferiore con performance elevate e costanti. Poiché i carichi di lavoro virtualizzati sono mobili, è possibile esplorare diversi approcci

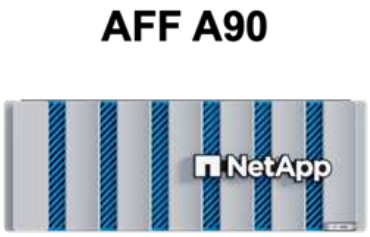
utilizzando Storage vMotion per spostare le macchine virtuali tra datastore VMFS, NFS o vVol, tutti sullo stesso sistema storage.

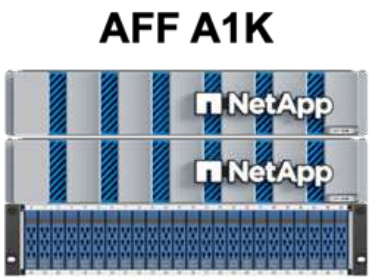
Array All-Flash NetApp

NetApp AFF (All Flash FAS) è una linea di prodotti di array di storage all-flash. È progettato per fornire soluzioni storage dalle performance elevate e a bassa latenza per i carichi di lavoro Enterprise. La serie AFF combina i vantaggi della tecnologia flash con le funzioni di gestione dei dati di NetApp, offrendo alle organizzazioni una piattaforma storage potente ed efficiente.

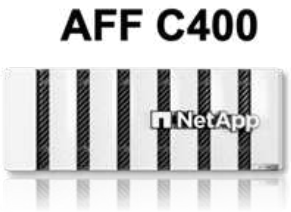
La linea AFF comprende sia i modelli A-Series che C-Series.

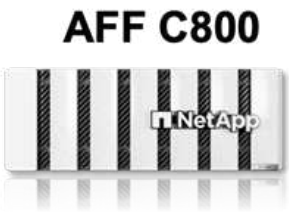
Gli array flash NetApp A-Series all-NVMe sono progettati per carichi di lavoro dalle performance elevate, offrendo latenza estremamente bassa ed elevata resilienza, rendendoli adatti ad applicazioni mission-critical.





I Flash Array C-Series QLC mirano a casi di utilizzo di capacità più elevata, fornendo la velocità della tecnologia flash insieme al risparmio della tecnologia flash ibrida.





Supporto dei protocolli di storage

AFF supporta tutti i protocolli standard utilizzati per la virtualizzazione, sia i datastore che lo storage connesso come guest, inclusi NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), NVME over Fabrics e S3. I clienti possono scegliere la soluzione migliore per i propri carichi di lavoro e applicazioni.

NFS - NetApp AFF fornisce il supporto per NFS, consentendo l'accesso basato su file ai datastore VMware. Datastore connesso a NFS da numerosi host ESXi, superano di gran lunga i limiti imposti ai file system VMFS. L'utilizzo di NFS con vSphere offre alcuni benefici di facilità di utilizzo e di visibilità dell'efficienza dello storage. ONTAP include funzionalità di accesso ai file disponibili per il protocollo NFS. È possibile attivare un server NFS ed esportare volumi o qtree.

Per informazioni sulla progettazione delle configurazioni NFS, fare riferimento alla "Documentazione di gestione dello storage NAS" .

ISCSI - NetApp AFF fornisce un solido supporto per iSCSI, consentendo l'accesso a livello di blocco ai

dispositivi di storage su reti IP. Offre un'integrazione perfetta con gli initiator iSCSI, consentendo un provisioning e una gestione efficienti delle LUN iSCSI. Funzionalità avanzate di ONTAP, come multipathing, autenticazione CHAP e supporto ALUA.

Per istruzioni sulla progettazione delle configurazioni iSCSI, fare riferimento alla "Documentazione di riferimento per la configurazione SAN".

Fibre Channel - NetApp AFF offre un supporto completo per Fibre Channel (FC), una tecnologia di rete ad alta velocità comunemente utilizzata nelle reti SAN. ONTAP si integra perfettamente con l'infrastruttura FC, fornendo un accesso a livello di blocco affidabile ed efficiente ai dispositivi storage. Offre funzioni come zoning, multi-path e fabric login (FLOGI) per ottimizzare le prestazioni, migliorare la sicurezza e garantire una connettività perfetta negli ambienti FC.

Per informazioni sulla progettazione delle configurazioni Fibre Channel, fare riferimento alla "Documentazione di riferimento per la configurazione SAN" .

NVMe over Fabrics - NetApp ONTAP supporta NVMe over Fabrics. NVMe/FC consente l'utilizzo di dispositivi storage NVMe su un'infrastruttura Fibre Channel e NVMe/TCP su reti IP di storage.

Per informazioni sulla progettazione su NVMe, fare riferimento a. "Configurazione, supporto e limitazioni NVMe".

Tecnologia Active-Active

Gli array all-flash NetApp offrono percorsi Active-Active attraverso i due controller, eliminando la necessità per il sistema operativo host di attendere il guasto di un percorso attivo, prima di attivare il percorso alternativo. Ciò significa che l'host può utilizzare tutti i percorsi disponibili su tutti i controller, garantendo che i percorsi attivi siano sempre presenti, indipendentemente dal fatto che il sistema si trovi in uno stato regolare o stia eseguendo un'operazione di failover del controller.

Per ulteriori informazioni, consultare "Data Protection e disaster recovery" la documentazione.

Garanzie di archiviazione

Con gli array all-flash di NetApp, NetApp offre un set esclusivo di garanzie storage. I vantaggi esclusivi includono:

Garanzia di efficienza dello storage: con la garanzia di efficienza dello storage è possibile ottenere prestazioni elevate riducendo al minimo i costi di storage. 4:1:1 per i carichi di lavoro SAN. **Garanzia di recovery ransomware:** recovery di dati garantito in caso di attacco ransomware.

Per informazioni dettagliate, vedere "Landing page di NetApp AFF" .

Strumenti NetApp ONTAP per VMware vSphere

Un potente componente di vCenter è la possibilità di integrare plug-in o estensioni che ne migliorano ulteriormente le funzionalità e offrono funzionalità e caratteristiche aggiuntive. Questi plug-in estendono le funzionalità di gestione di vCenter e consentono agli amministratori di integrare soluzioni, tool e servizi di 3rd parti nel proprio ambiente vSphere.

NetApp ONTAP Tools per VMware è una suite completa di strumenti progettati per facilitare la gestione del ciclo di vita delle macchine virtuali negli ambienti VMware tramite l'architettura vCenter Plug-in. Questi tool si integrano perfettamente con l'ecosistema VMware, consentendo un provisioning efficiente dei datastore e offrendo protezione essenziale per le macchine virtuali. Con i tool di ONTAP per VMware vSphere, gli amministratori possono gestire senza problemi i task di gestione del ciclo di vita dello storage.

Strumenti ONTAP completi 10 risorse sono disponibili "Strumenti ONTAP per le risorse di documentazione di VMware vSphere".

Per visualizzare la soluzione di implementazione 10 degli strumenti ONTAP, visitare il sito Web all'indirizzo "Utilizza i tool ONTAP 10 per configurare datastore NFS per vSphere 8"

Plug-in NetApp NFS per VMware VAAI

Il plug-in NFS NetApp per VAAI (API vStorage per l'integrazione degli array) migliora le operazioni di storage trasferendo determinate attività nel sistema storage NetApp, migliorando performance ed efficienza. Sono incluse operazioni come la copia completa, l'azzeramento dei blocchi e il blocco assistito da hardware. Inoltre, il plug-in VAAI ottimizza l'utilizzo dello storage riducendo la quantità di dati trasferiti sulla rete durante le operazioni di provisioning delle macchine virtuali e cloning.

Il plug-in NFS di NetApp per VAAI può essere scaricato dal sito di supporto NetApp e viene caricato e installato sugli host ESXi utilizzando tool ONTAP per VMware vSphere.

Per ulteriori informazioni, fare riferimento "NetApp NFS Plug-in per la documentazione di VMware VAAI" a.

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere (SCV) è una soluzione software di NetApp che offre una protezione dei dati completa per ambienti VMware vSphere. È progettato per semplificare e ottimizzare il processo di protezione e gestione delle macchine virtuali (VM) e dei datastore. SCV utilizza le istantanee basate sullo storage e la replica sugli array secondari per soddisfare gli obiettivi di tempi di ripristino inferiori.

Il plug-in SnapCenter per VMware vSphere offre in un'interfaccia unificata le seguenti funzionalità, integrate con il client vSphere:

Istantanee basate su criteri - SnapCenter consente di definire criteri per la creazione e la gestione di istantanee coerenti con le applicazioni delle macchine virtuali (VM) in VMware vSphere.

Automazione - la creazione e la gestione automatizzate delle snapshot basate su policy definite contribuiscono a garantire una protezione dei dati coerente ed efficiente.

VM-Level Protection - la protezione granulare a livello di VM consente una gestione e un ripristino efficienti delle singole macchine virtuali.

Funzioni di efficienza dello storage - l'integrazione con le tecnologie di storage NetApp offre funzioni di efficienza dello storage come la deduplica e la compressione per le snapshot, riducendo al minimo i requisiti di storage.

Il plug-in di SnapCenter orchestra l'arresto delle macchine virtuali insieme alle istantanee basate su hardware sugli storage array di NetApp. La tecnologia SnapMirror viene utilizzata per replicare le copie di backup su sistemi storage secondari, incluso il cloud.

Per ulteriori informazioni, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere".

L'integrazione di BlueXP permette strategie di backup 3-2-1 che estendono le copie dei dati allo storage a oggetti nel cloud.

Per ulteriori informazioni sulle strategie di backup 3-2-1 con BlueXP, visita il sito "Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM".

Per istruzioni dettagliate sull'implementazione del plug-in SnapCenter, fare riferimento alla soluzione "Utilizza il

plug-in SnapCenter per VMware vSphere per proteggere le VM nei domini del carico di lavoro VCF".

Considerazioni sullo storage

Sfruttando i datastore NFS di ONTAP con VMware vSphere, avrai a disposizione un ambiente scalabile, facile da gestire e dalle performance elevate, in grado di offrire rapporti VM-datastore irraggiungibili con protocolli storage basati su blocchi. Questa architettura può comportare un aumento di dieci volte della densità dei datastore, accompagnato da una corrispondente riduzione del numero dei datastore.

NConnect for NFS: un altro vantaggio dell'utilizzo di NFS è la possibilità di sfruttare la funzione **nConnect**. NConnect consente più connessioni TCP per i volumi del datastore NFS v3, ottenendo così un throughput più elevato. In questo modo è possibile aumentare il parallelismo e per i datastore NFS. I clienti che implementano datastore con NFS versione 3 possono aumentare il numero di connessioni al server NFS, massimizzando l'utilizzo delle schede di interfaccia di rete ad alta velocità.

Per informazioni dettagliate su nConnect, fare riferimento a "Funzionalità NFS nConnect con VMware e NetApp".

Session trunking for NFS: a partire da ONTAP 9.14,1, i client che utilizzano NFSv4,1 possono sfruttare il trunking di sessione per stabilire connessioni multiple a varie LIF sul server NFS. In questo modo è possibile trasferire i dati più velocemente e migliorare la resilienza utilizzando il multipathing. Il trunking risulta particolarmente vantaggioso quando si esportano volumi FlexVol in client che supportano il trunking, come i client VMware e Linux, o quando si utilizza NFS su protocolli RDMA, TCP o pNFS.

Per ulteriori informazioni, fare riferimento "Panoramica del trunking NFS" a.

FlexVol Volumes: NetApp consiglia di utilizzare volumi **FlexVol** per la maggior parte dei datastore NFS. Mentre i datastore di dimensioni maggiori possono migliorare l'efficienza dello storage e i vantaggi operativi, è consigliabile prendere in considerazione l'utilizzo di almeno quattro datastore (FlexVol Volumes) per memorizzare le macchine virtuali su un singolo controller del ONTAP. In genere, gli amministratori implementano datastore basati su volumi FlexVol con capacità comprese tra 4TB TB e 8TB TB. Queste dimensioni offrono un buon equilibrio tra performance, facilità di gestione e protezione dei dati. Gli amministratori possono partire con poco e scalare il datastore in base alle esigenze (fino a un massimo di 100TB PB). I datastore più piccoli facilitano un recovery più rapido da backup o disastri ed è possibile spostarli rapidamente nel cluster. Questo approccio consente il massimo dell'utilizzo delle prestazioni delle risorse hardware e consente datastore con policy di recovery differenti.

FlexGroup Volumes: per gli scenari che richiedono un archivio dati di grandi dimensioni, NetApp consiglia l'utilizzo di volumi **FlexGroup**. I volumi FlexGroup non hanno virtualmente vincoli di capacità o di numero di file, consentendo agli amministratori di eseguire facilmente il provisioning di un enorme namespace singolo. L'utilizzo di FlexGroup Volumes non comporta overhead aggiuntivi di manutenzione o gestione. Non sono necessari datastore multipli per le performance con i volumi FlexGroup, in quanto scalano intrinsecamente. Utilizzando ONTAP e volumi FlexGroup con VMware vSphere, puoi stabilire datastore semplici e scalabili che sfruttano tutta la potenza dell'intero cluster ONTAP.

Protezione ransomware

Il software per la gestione dei dati NetApp ONTAP dispone di una suite completa di tecnologie integrate per aiutarti a proteggere, rilevare e ripristinare in caso di attacchi ransomware. La funzionalità NetApp SnapLock Compliance integrata in ONTAP impedisce l'eliminazione dei dati memorizzati in un volume abilitato utilizzando la tecnologia WORM (write once, Read many) con data retention avanzata. Dopo che è stato stabilito il periodo di conservazione e la copia Snapshot è bloccata, nemmeno un amministratore dello storage con un sistema Privileges completo o un membro del team di supporto NetApp può eliminare la copia Snapshot. Tuttavia, cosa più importante, un hacker con credenziali compromesse non può eliminare i dati.

NetApp garantisce che saremo in grado di recuperare le copie NetApp® Snapshot™ protette sugli array idonei e, in caso contrario, rimborseremo l'organizzazione.

Per ulteriori informazioni sulla garanzia di ripristino dal ransomware, consulta: "Garanzia di recupero Ransomeware".

Per "Panoramica della protezione ransomware autonoma" ulteriori informazioni dettagliate, fare riferimento alla .

Scoprite la soluzione completa nel centro di documentazione delle soluzioni NetApps: "Protezione autonoma dal ransomware per lo storage NFS"

Considerazioni sul disaster recovery

NetApp offre lo storage più sicuro al mondo. NetApp può contribuire a proteggere l'infrastruttura dei dati e delle applicazioni, spostare i dati tra storage on-premise e cloud, e contribuire a garantire la disponibilità dei dati tra i cloud. ONTAP dispone di potenti tecnologie di sicurezza e data Protection che aiutano a proteggere i clienti dai disastri grazie al rilevamento proattivo delle minacce e al ripristino rapido di dati e applicazioni.

VMware Live Site Recovery, precedentemente noto come VMware Site Recovery Manager, offre un'automazione ottimizzata basata su policy per la protezione delle macchine virtuali all'interno del client web vSphere. Questa soluzione sfrutta le tecnologie avanzate di gestione dei dati di NetApp attraverso l'adattatore di replica dello storage come parte degli strumenti ONTAP per VMware. Sfruttando le funzionalità di NetApp SnapMirror per la replica basata su array, gli ambienti VMware possono trarre vantaggio da una delle tecnologie ONTAP più affidabili e mature. SnapMirror garantisce trasferimenti dei dati sicuri e altamente efficienti copiando solo i blocchi del file system modificati, piuttosto che intere macchine virtuali o datastore. Inoltre, questi blocchi sfruttano tecniche di risparmio dello spazio come deduplica, compressione e compaction. Con l'introduzione di SnapMirror indipendenti dalla versione nei moderni sistemi ONTAP, puoi ottenere flessibilità nella scelta dei cluster di origine e destinazione. SnapMirror si è affermata come potente strumento per il disaster recovery e, in combinazione con Live Site Recovery, offre livelli superiori di scalabilità, prestazioni e risparmi sui costi rispetto alle alternative di storage locali.

Per ulteriori informazioni, fare riferimento alla "Panoramica di VMware Site Recovery Manager".

Scoprite la soluzione completa nel centro di documentazione delle soluzioni NetApps: "Protezione autonoma dal ransomware per lo storage NFS"

BlueXP DRaaS (Disaster Recovery as a Service) per NFS è una soluzione di disaster recovery conveniente ideata per carichi di lavoro VMware in esecuzione su sistemi ONTAP on-premise con datastore NFS. Sfrutta la replica di NetApp SnapMirror per proteggerti dai fuori servizio del sito e dagli eventi di corruzione dei dati, come gli attacchi ransomware. Integrato con la console NetApp BlueXP , questo servizio consente una facile gestione e il rilevamento automatico di vCenter VMware e storage ONTAP. Le organizzazioni possono creare e testare i piani di disaster recovery, raggiungendo un recovery point objective (RPO) di massimo 5 minuti tramite la replica a livello di blocco. BlueXP DRaaS utilizza la tecnologia FlexClone di ONTAP per test efficienti in termini di spazio senza influire sulle risorse di produzione. Il servizio orchestra i processi di failover e failback, consentendo l'attivazione delle macchine virtuali protette nel sito di disaster recovery designato con il minimo sforzo. Rispetto ad altre alternative ben note, BlueXP DRaaS offre queste funzionalità a costi nettamente inferiori, rendendo una soluzione efficiente per le organizzazioni per la configurazione, il test e l'esecuzione di operazioni di disaster recovery per i propri ambienti VMware utilizzando sistemi storage ONTAP.

Scoprite la soluzione completa nel centro di documentazione delle soluzioni NetApps: "Dr utilizzando BlueXP DRaaS per datastore NFS"

Panoramica delle soluzioni

Soluzioni descritte nella presente documentazione:

- **NFS nConnect con NetApp e VMware**. Fare clic su **"qui"** per i passaggi di distribuzione.
  - **Utilizzare gli strumenti ONTAP 10 per configurare gli archivi dati NFS per vSphere 8**. Fare clic su **"qui"** per i passaggi di distribuzione.
  - **Distribuire e utilizzare il plug-in SnapCenter per VMware vSphere per proteggere e ripristinare le VM**. Fare clic su **"qui"** per i passaggi di distribuzione.
  - **Disaster Recovery di archivi dati NFS con VMware Site Recovery Manager**. Fare clic su **"qui"** per i passaggi di distribuzione.
  - **Protezione autonoma da ransomware per lo storage NFS**. Fare clic su **"qui"** per i passaggi di distribuzione.

Funzionalità NFS nConnect con NetApp e VMware

A partire da VMware vSphere 8,0 U1 (come Tech-preview), la funzionalità nconnect consente a più connessioni TCP per i volumi del datastore NFS v3 di aumentare il throughput. I clienti che utilizzano un datastore NFS possono ora incrementare il numero di connessioni al server NFS, ottimizzando così l'utilizzo delle schede di interfaccia di rete ad alta velocità.

> La funzione è generalmente disponibile per NFS v3 con 8,0 U2, fare riferimento alla sezione di memorizzazione a "Note sulla versione di VMware vSphere 8,0 Update 2". Il supporto di NFS v4,1 viene aggiunto con vSphere 8,0 U3. Per ulteriori informazioni, consulta "Note sulla versione di vSphere 8,0 Update 3"

Casi di utilizzo

- Ospita un maggior numero di macchine virtuali per datastore NFS sullo stesso host.
- Migliora le performance del datastore NFS.
- Fornisci un'opzione per offrire servizio a un Tier più elevato per le applicazioni basate su VM e container.

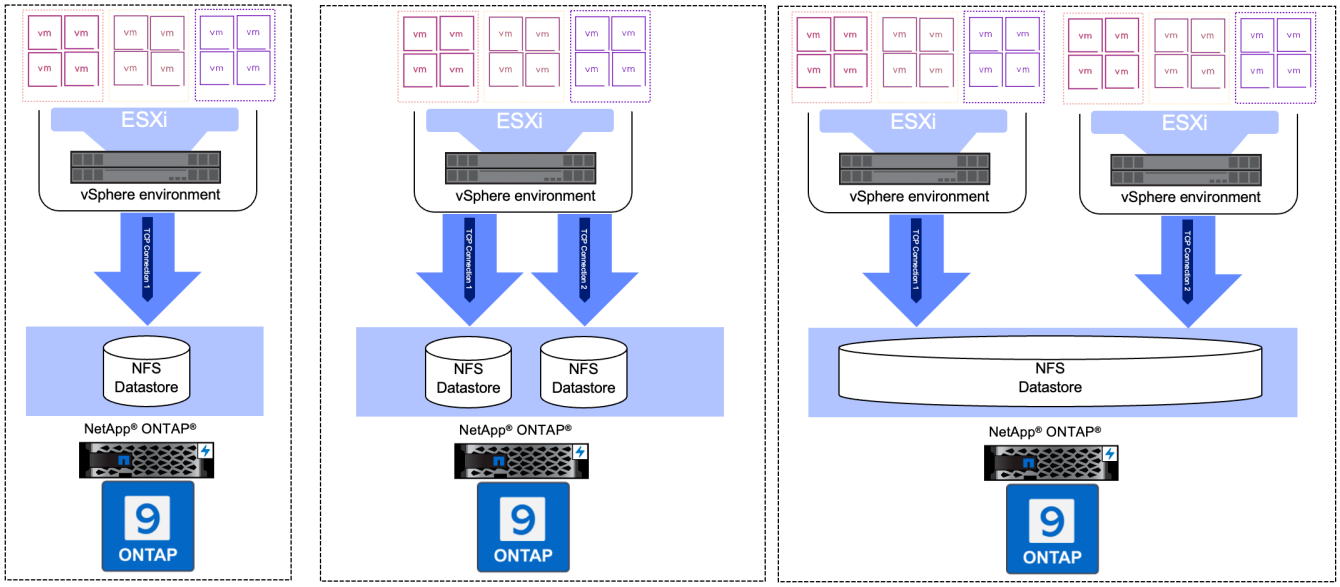
Dettagli tecnici

Lo scopo di nconnect è fornire più connessioni TCP per datastore NFS su un host vSphere. Questo aiuta ad aumentare il parallelismo e le performance per i datastore NFS. In ONTAP, quando viene stabilito un montaggio NFS, viene creato un ID connessione (CID). Tale CID fornisce fino a 128 operazioni simultanee in-flight. Quando tale numero viene superato dal client, ONTAP applica una forma di controllo di flusso fino a quando non può liberare alcune risorse disponibili al completamento di altre operazioni. In genere, queste pause non superano di qualche microsecondi, ma nel corso di milioni di operazioni si accumulano e creano problemi di performance. NConnect può prendere il limite di 128 e moltiplicarlo per il numero di sessioni nconnect sul client, che fornisce più operazioni simultanee per CID e può potenzialmente aggiungere vantaggi in termini di performance. Per ulteriori dettagli, fare riferimento a. "Guida alle Best practice e all'implementazione di NFS"

Datastore NFS predefinito

Per risolvere i limiti di performance di una singola connessione di un datastore NFS, vengono montati datastore aggiuntivi o vengono aggiunti host per aumentare la connessione.

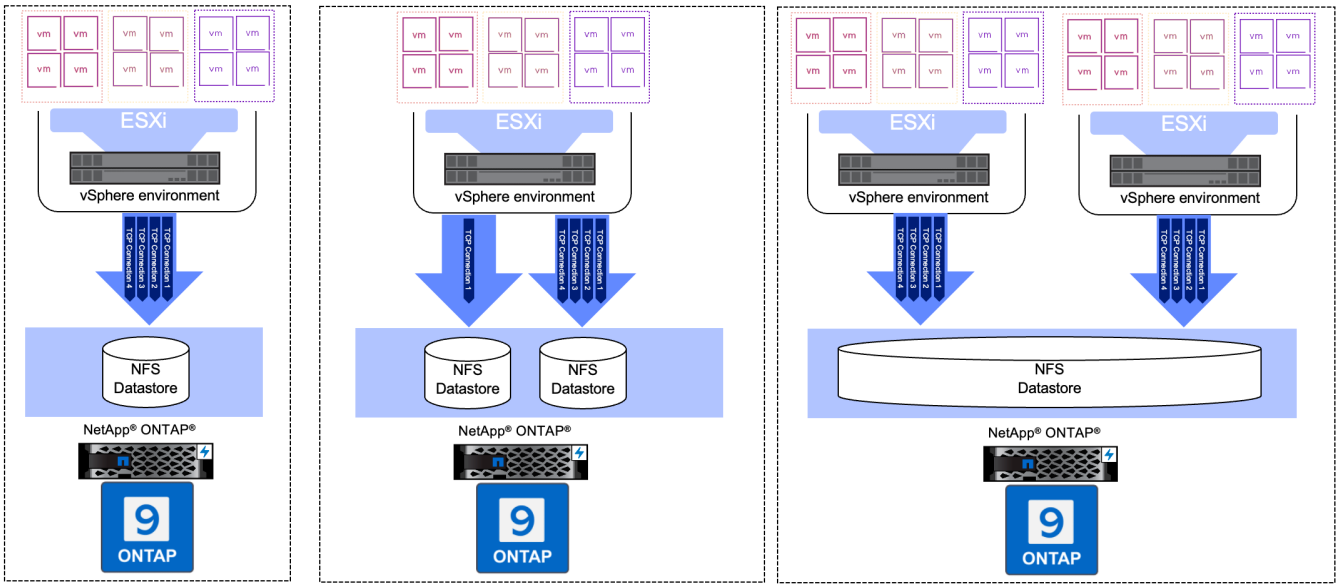
Without nConnect feature with NetApp and VMware



Con nConnect NFS Datastore

Una volta creato il datastore NFS utilizzando gli strumenti ONTAP o altre opzioni, il numero di connessione per datastore NFS può essere modificato utilizzando lo strumento vSphere CLI, PowerCLI, govc o altre opzioni API. Per evitare problemi di performance insieme a vMotion, mantenere lo stesso numero di connessioni per il datastore NFS su tutti gli host vSphere che fanno parte di vSphere Cluster.

With nConnect feature with NetApp and VMware



Prerequisito

Per utilizzare la funzione nconnect, devono essere soddisfatte le seguenti dipendenze.

Versione di ONTAP	Versione vSphere	Commenti
9,8 o superiore	8 aggiornamento 1	Anteprima tecnica con opzione per aumentare il numero di connessioni.
9,8 o superiore	8 aggiornamento 2	Generalmente disponibile con opzione per aumentare e diminuire il numero di connessioni.
9,8 o superiore	8 aggiornamento 3	NFS 4,1 e supporto multi-path.

Aggiornare il numero di connessione al datastore NFS

Una singola connessione TCP viene utilizzata quando si crea un datastore NFS con ONTAP Tools o vCenter. Per aumentare il numero di connessioni, è possibile utilizzare l'interfaccia CLI di vSphere. Il comando di riferimento è mostrato di seguito.

```
# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1
datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the number of connections for existing NFSv3
datastore.
esxcli storage nfs param set -v <datastore_name> -c
<number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v
<datastore_name> -c <number_of_connections>
```

Oppure utilizzare PowerCLI come illustrato di seguito

```
$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData
.ConfigManager.DatastoreSystem
$nfsSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfsSpec.RemoteHost = "nfs_server.ontap.local"
$nfsSpec.RemotePath = "/DS01"
$nfsSpec.LocalPath = "DS01"
$nfsSpec.AccessMode = "readWrite"
$nfsSpec.Type = "NFS"
$nfsSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfsSpec)
```

Ecco l'esempio di aumentare il numero di connessioni con lo strumento govc.

```
$env.GOVC_URL = 'vcenter.vsphere.local'
$env.GOVC_USERNAME = 'administrator@vsphere.local'
$env.GOVC_PASSWORD = 'XXXXXXXXX'
$env.GOVC_Datastore = 'DS01'
# $env.GOVC_INSECURE = 1
$env.GOVC_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list
```

Fare riferimento a. "Articolo della KB di VMware 91497" per ulteriori informazioni.

Considerazioni di progettazione

Il numero massimo di connessioni supportate da ONTAP dipende dal modello di piattaforma di storage. Cercare exec_ctx su "Guida alle Best practice e all'implementazione di NFS" per ulteriori informazioni.

Con l'aumento del numero di connessioni per datastore NFSv3, il numero di datastore NFS che è possibile

montare su quell'host vSphere diminuisce. Il numero totale di connessioni supportate per host vSphere è 256. Controllare "Articolo della KB di VMware 91481" Per i limiti del datastore per host vSphere.

> Il datastore vVol non supporta la funzione nConnect. Tuttavia, gli endpoint del protocollo contano verso il limite di connessione. Al momento della creazione del datastore vVol, viene creato un endpoint di protocollo per ogni dato lif di SVM.

Utilizza i tool ONTAP 10 per configurare datastore NFS per vSphere 8

I tool ONTAP per VMware vSphere 10 offrono un'architettura di nuova generazione che offre High Availability e scalabilità native per il provider VASA (con supporto di vVol iSCSI e NFS). In questo modo è possibile semplificare la gestione di più server VMware vCenter e cluster ONTAP.

In questo scenario dimostreremo come implementare e utilizzare gli strumenti ONTAP per VMware vSphere 10 e configurare un datastore NFS per vSphere 8.

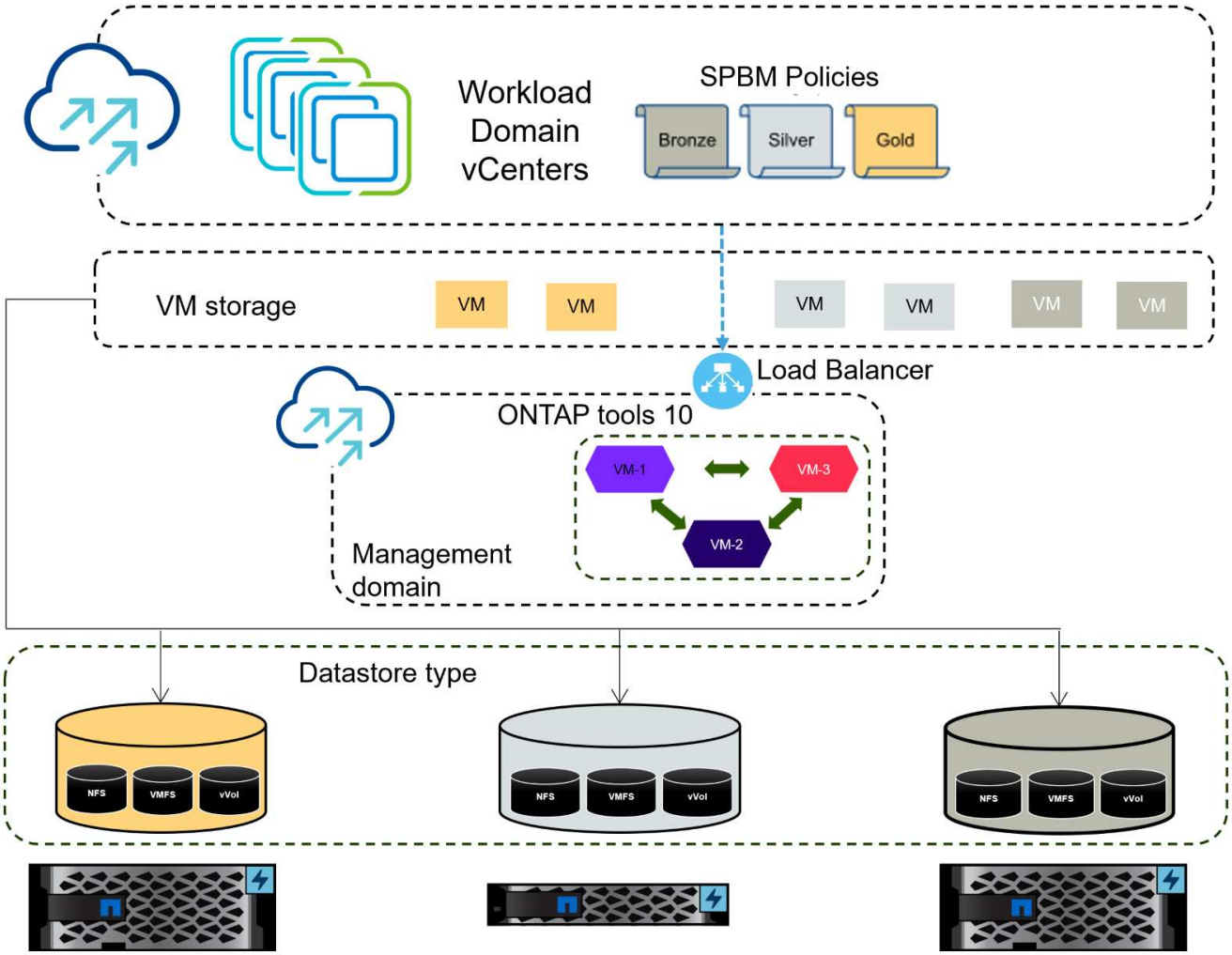
Panoramica della soluzione

Questo scenario copre i seguenti passaggi di alto livello:

- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico NFS.
- Creare un gruppo di porte distribuite per la rete NFS sul cluster vSphere 8.
- Creare un adattatore vmkernel per NFS sugli host ESXi nel cluster vSphere 8.
- Implementa i tool ONTAP 10 e registrati con il cluster vSphere 8.
- Creare un nuovo datastore NFS nel cluster vSphere 8.

Architettura

Il diagramma seguente mostra i componenti architetturali di un tool ONTAP per l'implementazione di VMware vSphere 10.



Prerequisiti

Questa soluzione richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP AFF con porte per dati fisici su switch ethernet dedicati al traffico di storage.
- L'implementazione del cluster vSphere 8 è stata completata e il client vSphere è accessibile.
- I tool ONTAP per il modello OVA di VMware vSphere 10 sono stati scaricati dal sito di supporto NetApp.

NetApp consiglia progettazioni di rete ridondanti per NFS, per fornire la tolleranza agli errori di sistemi storage, switch, adattatori di rete e sistemi host. È comune implementare NFS con una singola subnet o più subnet a seconda dei requisiti architetturali.

Fare riferimento a. "Best practice per l'esecuzione di NFS con VMware vSphere" Per informazioni dettagliate specifiche di VMware vSphere.

Per assistenza sulla rete per l'utilizzo di ONTAP con VMware vSphere, fare riferimento al "Configurazione di rete - NFS" Della documentazione relativa alle applicazioni aziendali NetApp.

Strumenti ONTAP completi 10 risorse sono disponibili "Strumenti ONTAP per le risorse di documentazione di VMware vSphere".

Fasi di implementazione

Per implementare ONTAP Tools 10 e utilizzarlo per creare un archivio dati NFS nel dominio di gestione VCF, attenersi alla seguente procedura:

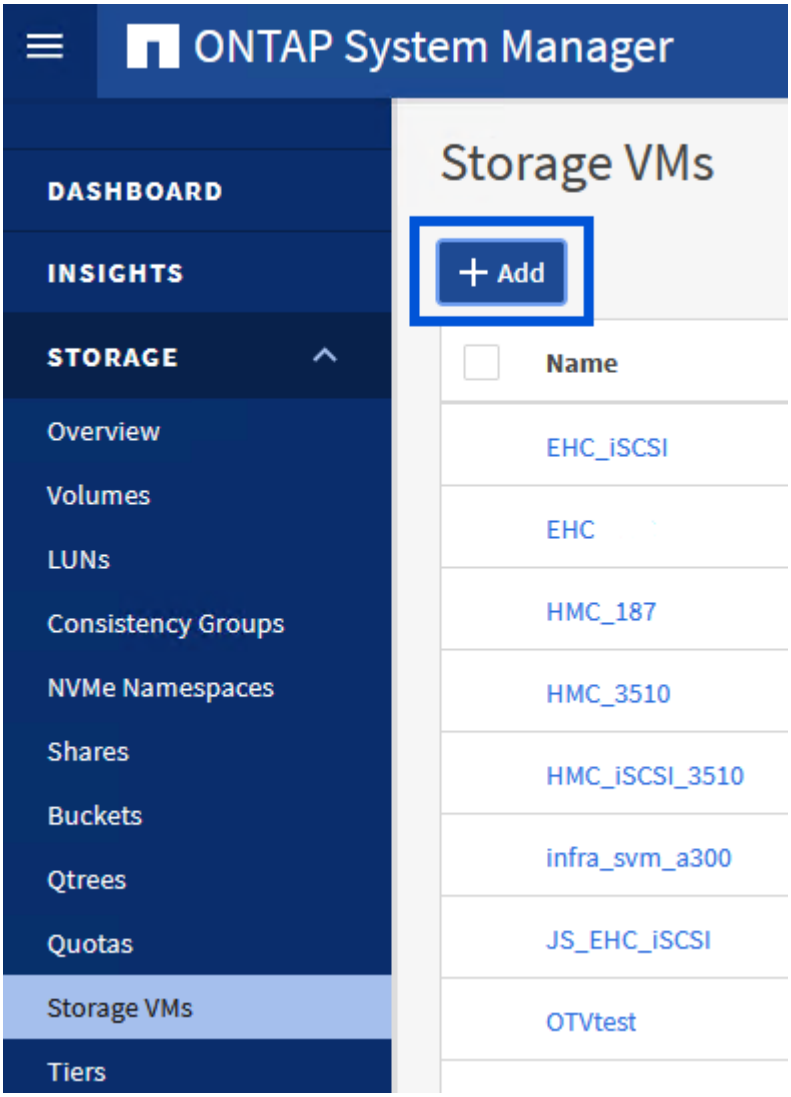
Crea SVM e LIF su un sistema storage ONTAP

Il passaggio seguente viene eseguito in Gestione di sistema di ONTAP.

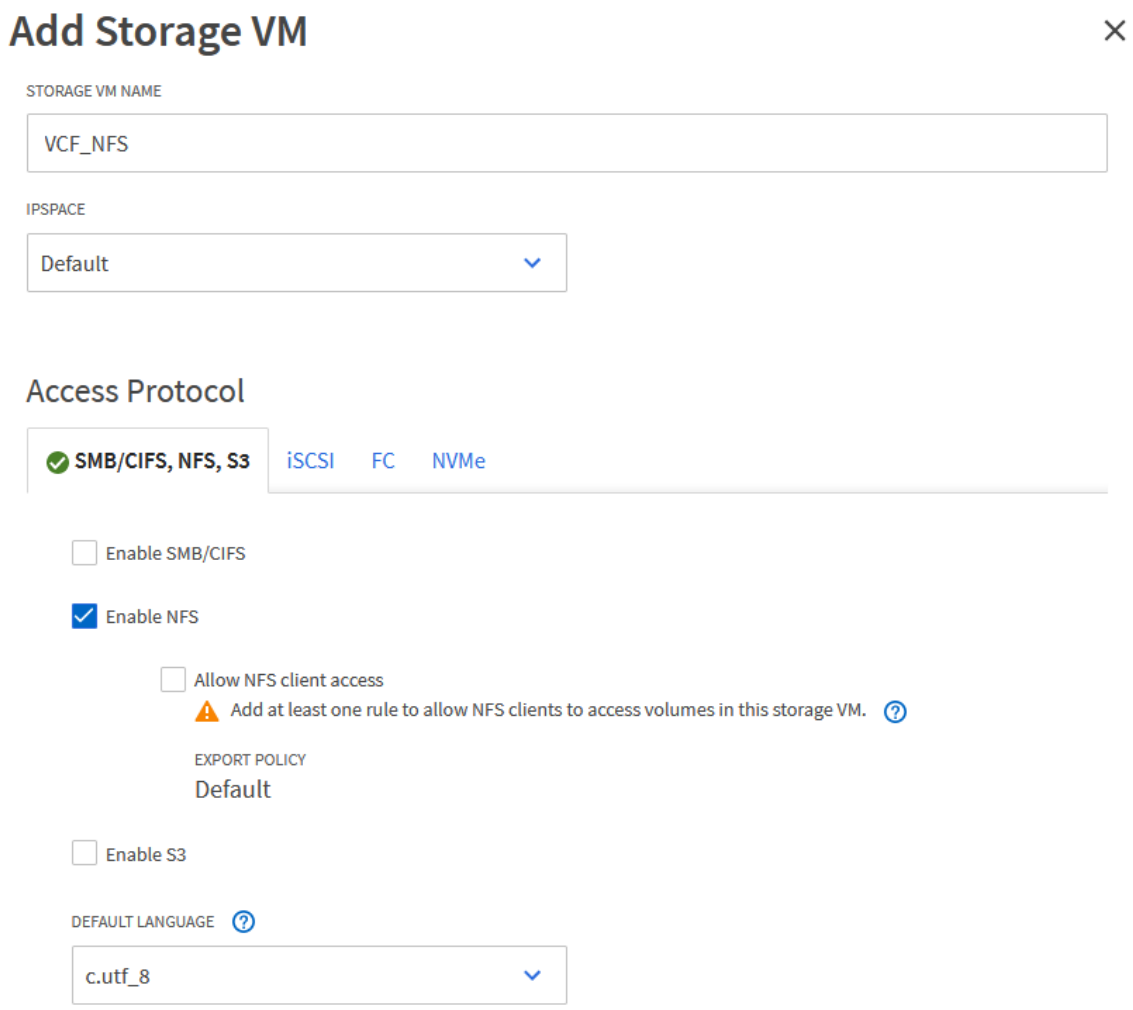
Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per il traffico NFS.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.

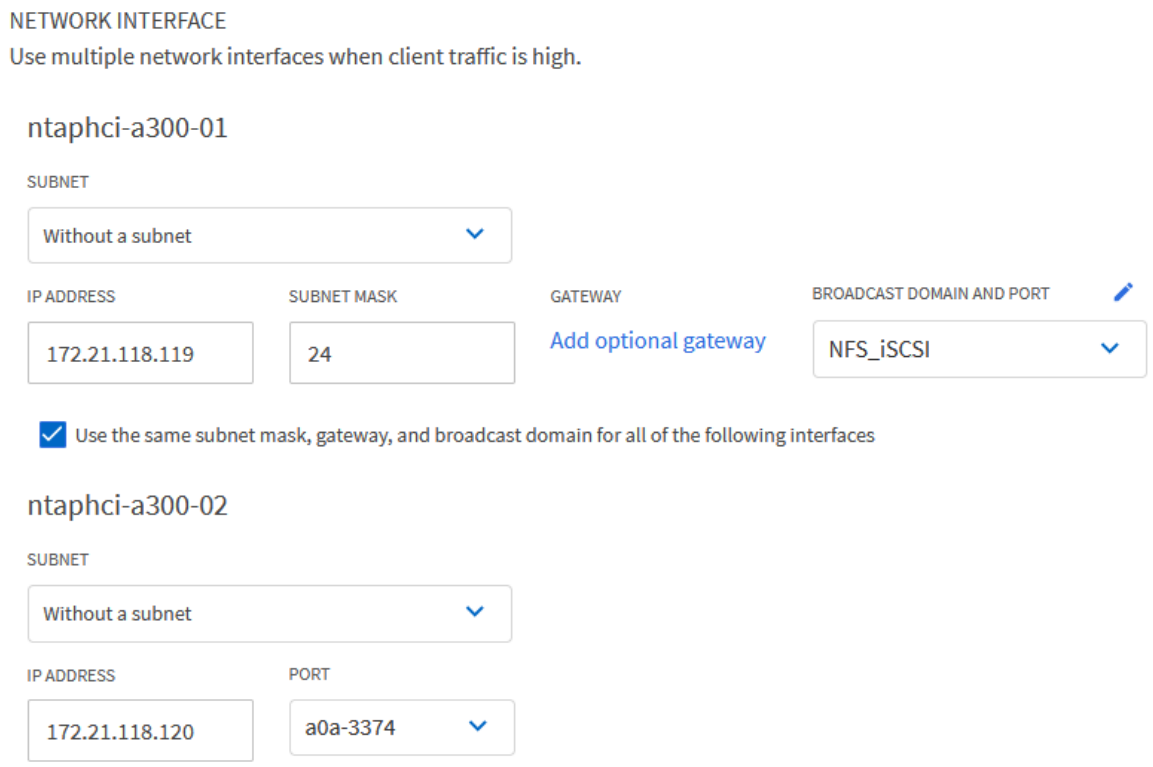


2. Nella procedura guidata **Add Storage VM** (Aggiungi VM di storage) fornire un **Name** (Nome) per la SVM, selezionare **IP Space** (spazio IP), quindi, in **Access Protocol** (protocollo di accesso), fare clic sulla scheda **SMB/CIFS, NFS, S3** e selezionare la casella **Enable NFS** (Abilita NFS*).

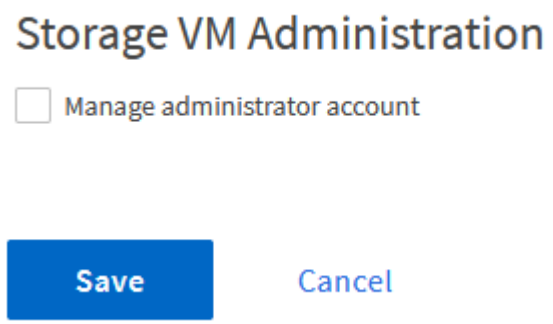


Non è necessario selezionare il pulsante **Allow NFS client access** (Consenti accesso client NFS) poiché gli strumenti ONTAP per VMware vSphere verranno utilizzati per automatizzare il processo di distribuzione del datastore. Ciò include la fornitura dell'accesso client agli host ESXi.

3. Nella sezione **interfaccia di rete** compilare i campi **indirizzo IP**, **Subnet Mask** e **Broadcast Domain and Port** per la prima LIF. Per LIF successive, la casella di controllo può essere abilitata per usare impostazioni comuni a tutte le LIF rimanenti o per usare impostazioni separate.



4. Scegliere se attivare l'account Storage VM Administration (per ambienti multi-tenancy) e fare clic su **Save** (Salva) per creare la SVM.



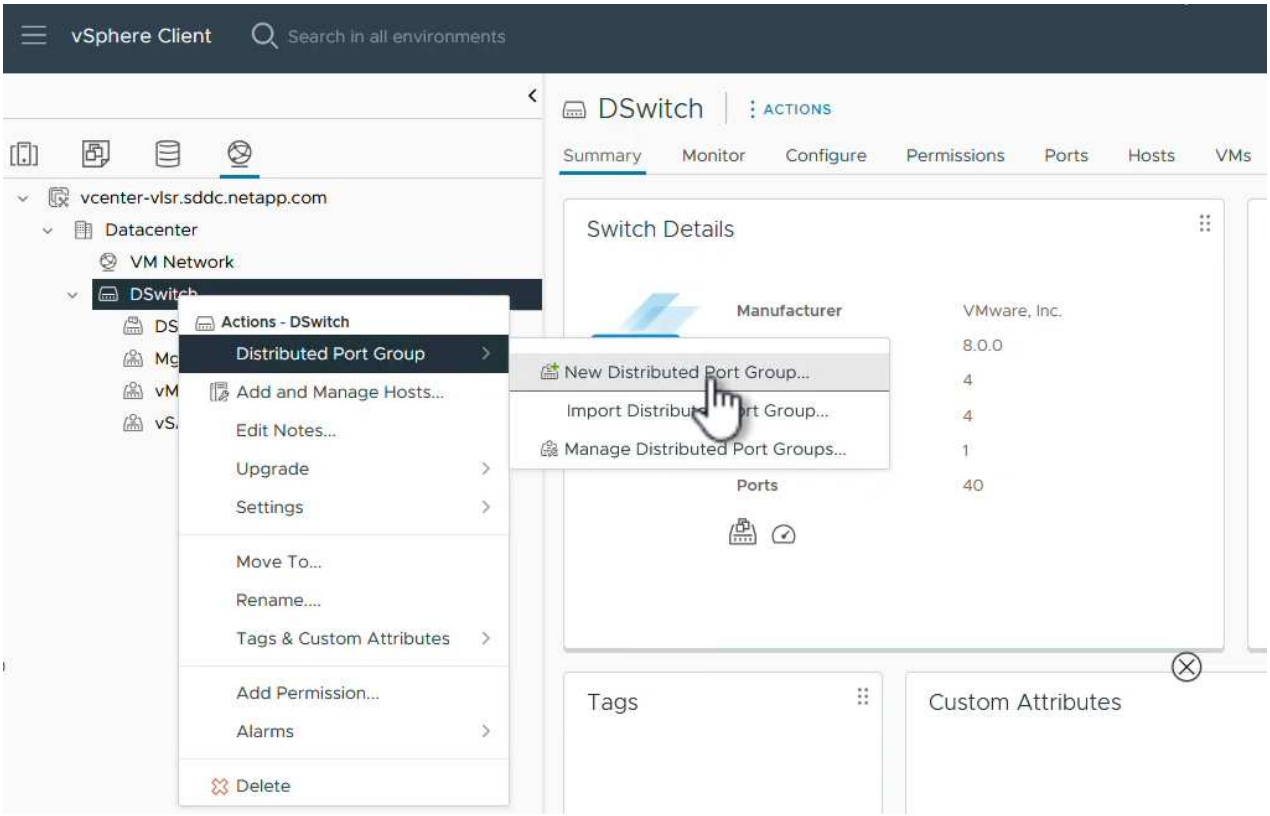
Configurare il networking per NFS sugli host ESXi

I seguenti passaggi vengono eseguiti sul cluster VI workload Domain utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-on, pertanto il client vSphere è comune nei domini di gestione e carico di lavoro.

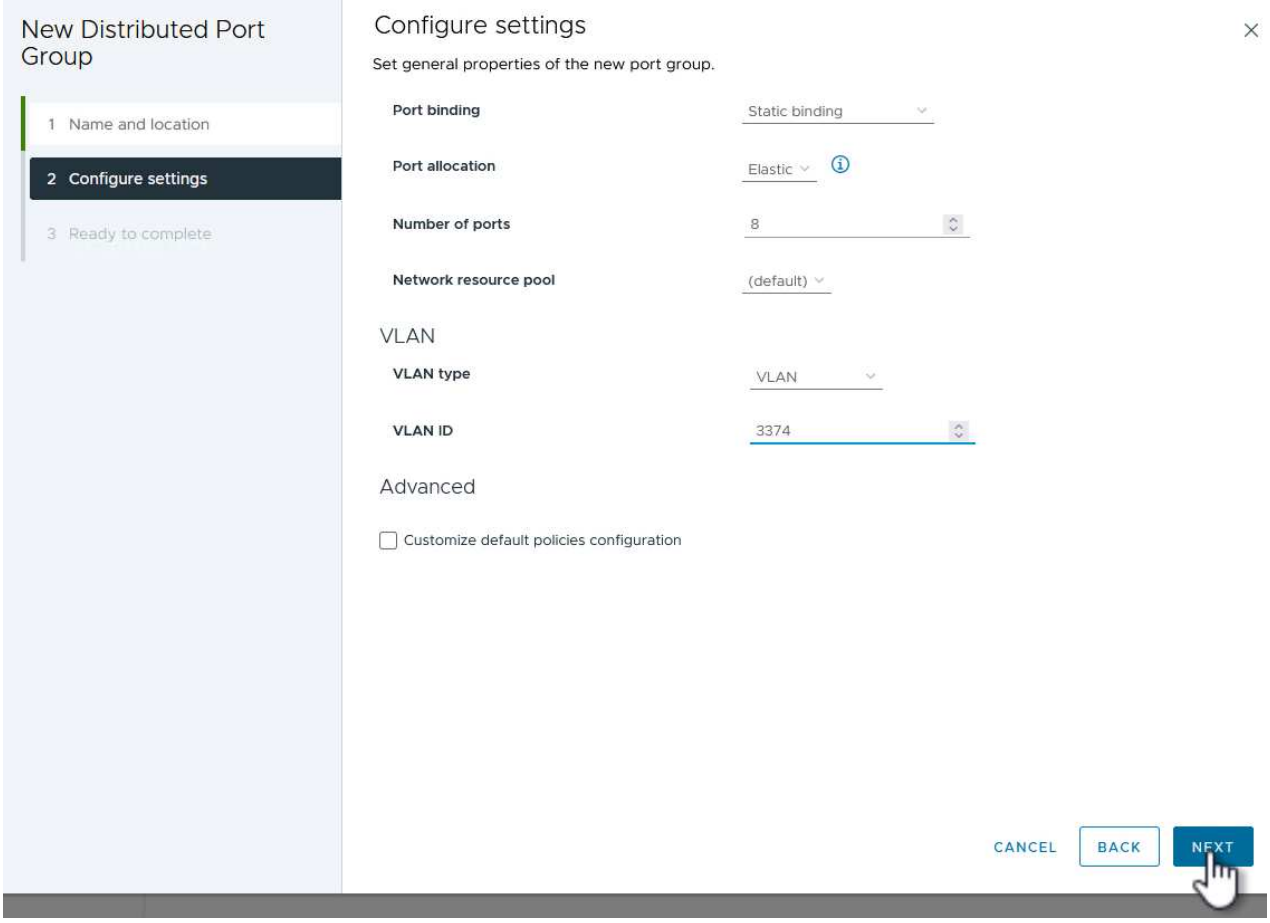
Creare un gruppo di porte distribuite per il traffico NFS

Completare quanto segue per creare un nuovo gruppo di porte distribuite per la rete per il trasporto del traffico NFS:

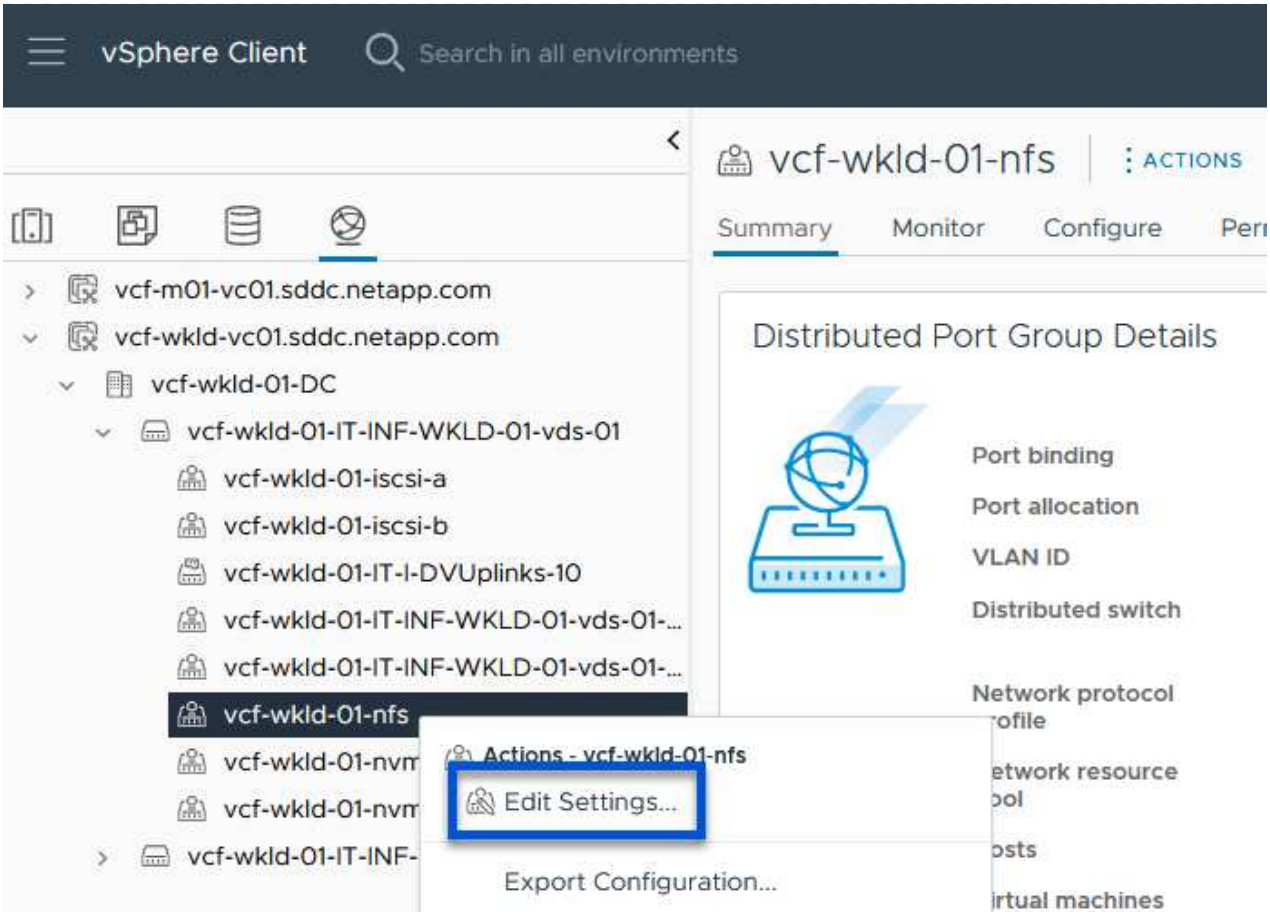
1. Dal client vSphere , accedere a **Inventory > Networking** per il dominio del carico di lavoro. Passare allo Switch distribuito esistente e scegliere l'azione da creare **nuovo Gruppo di porte distribuite…**.



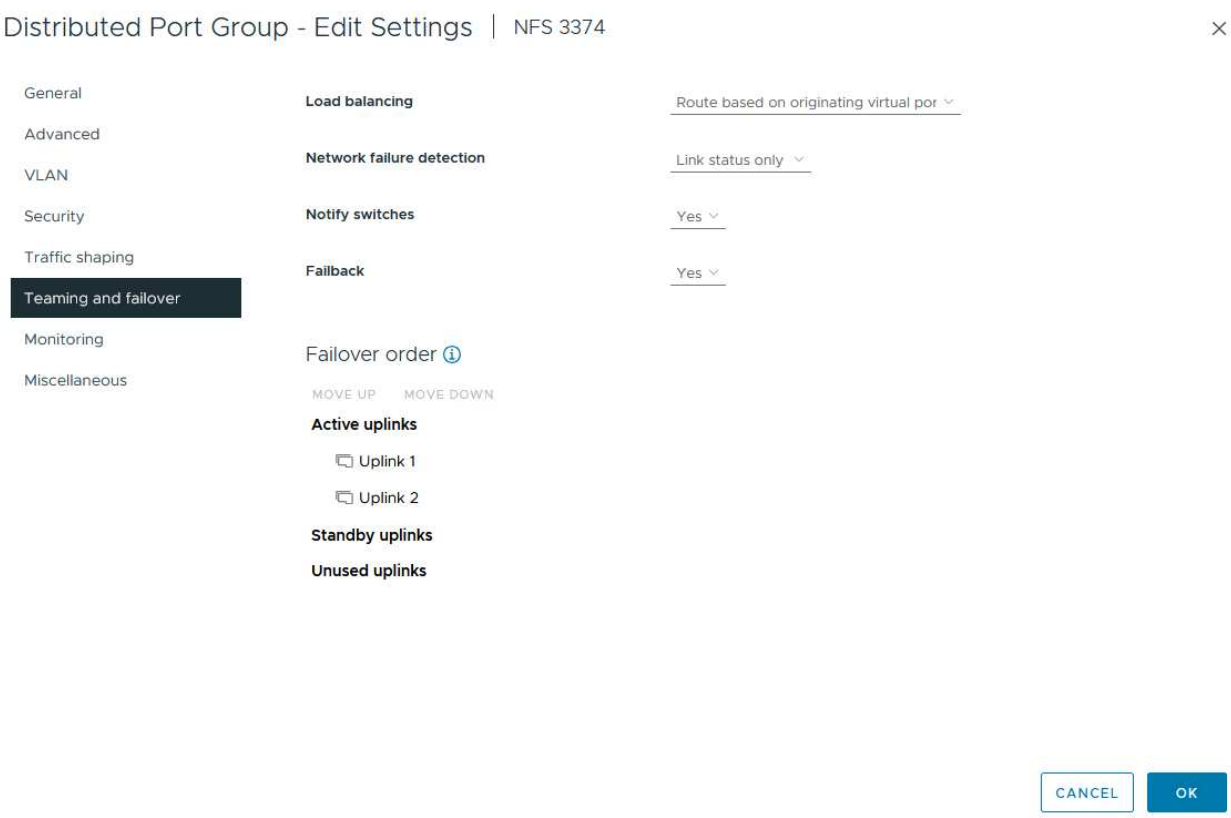
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare clic su **Avanti** per continuare.



4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **fine** per creare il nuovo gruppo di porte distribuite.
5. Una volta creato il gruppo di porte, accedere al gruppo di porte e selezionare l'azione **Modifica impostazioni…**.



6. Nella pagina **Distributed Port Group - Edit Settings**, accedere a **Teaming and failover** nel menu a sinistra. Abilitare il raggruppamento per gli uplink da utilizzare per il traffico NFS assicurandosi che siano Uniti nell'area **uplink attivi**. Spostare gli uplink non utilizzati verso il basso su **uplink non utilizzati**.

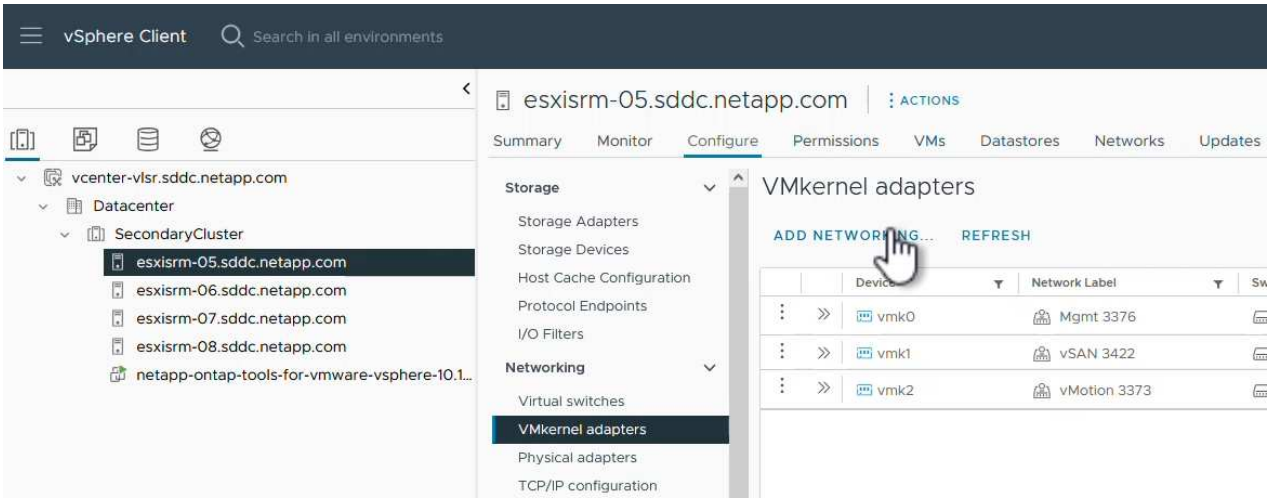


7. Ripetere questa procedura per ogni host ESXi nel cluster.

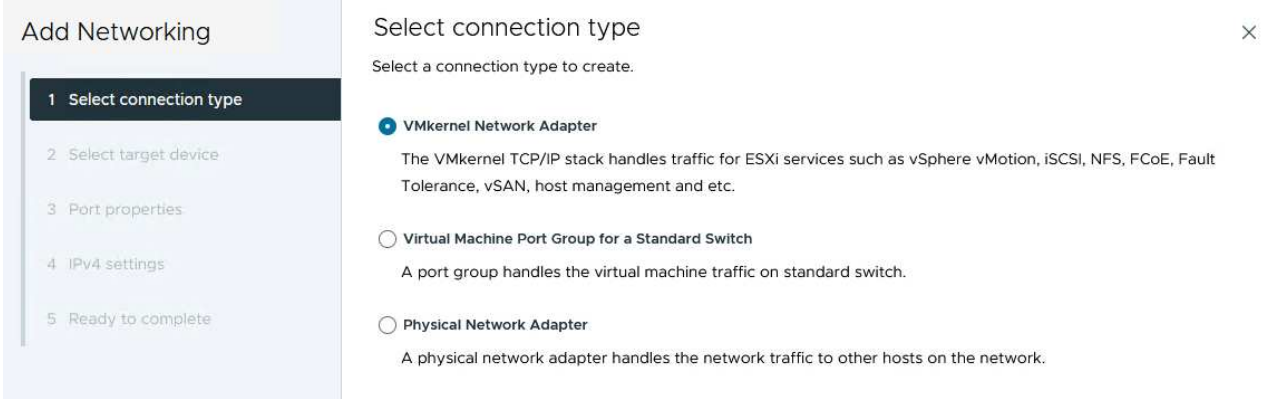
Creare un adattatore VMkernel su ciascun host ESXi

Ripetere questo processo su ogni host ESXi nel dominio del carico di lavoro.

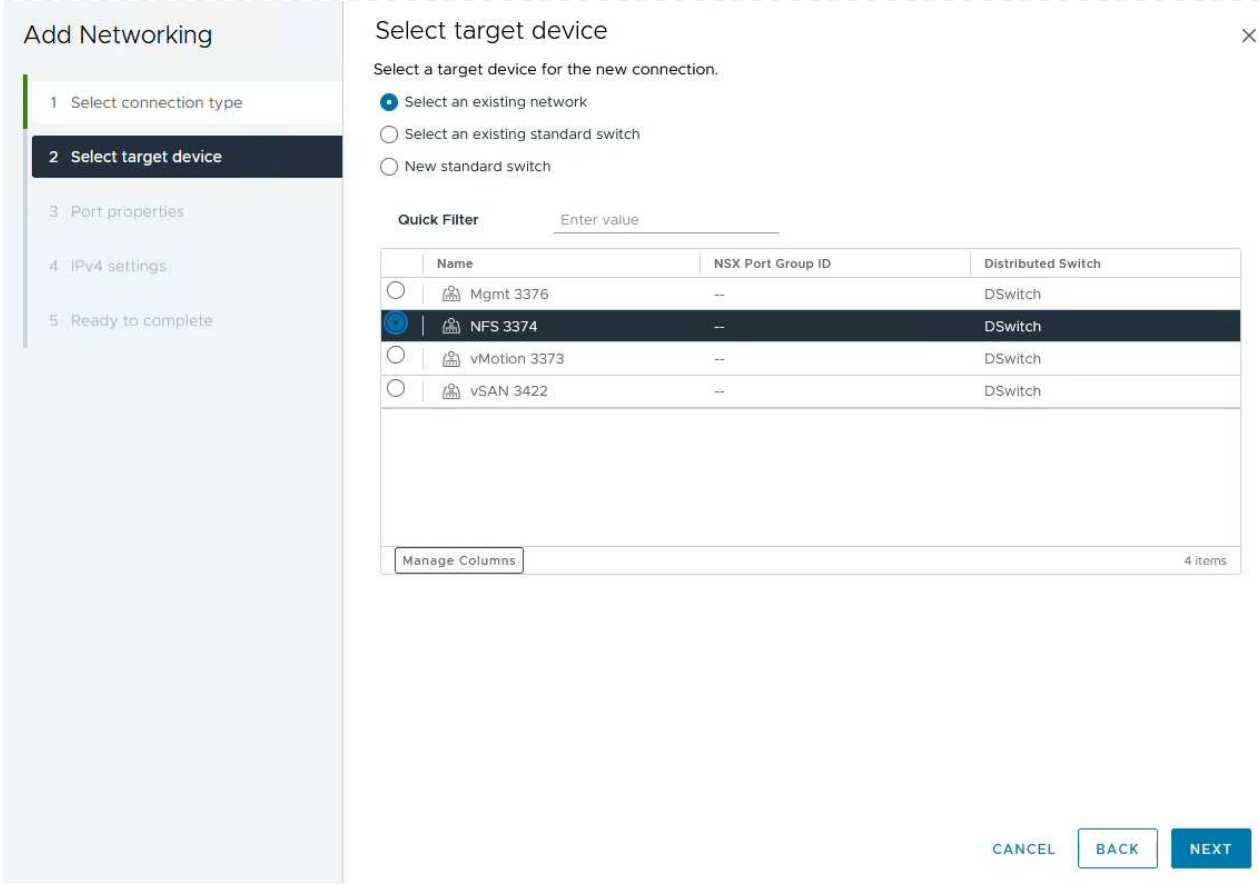
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configure** selezionare **VMkernel adapters** e fare clic su **Add Networking…** per iniziare.



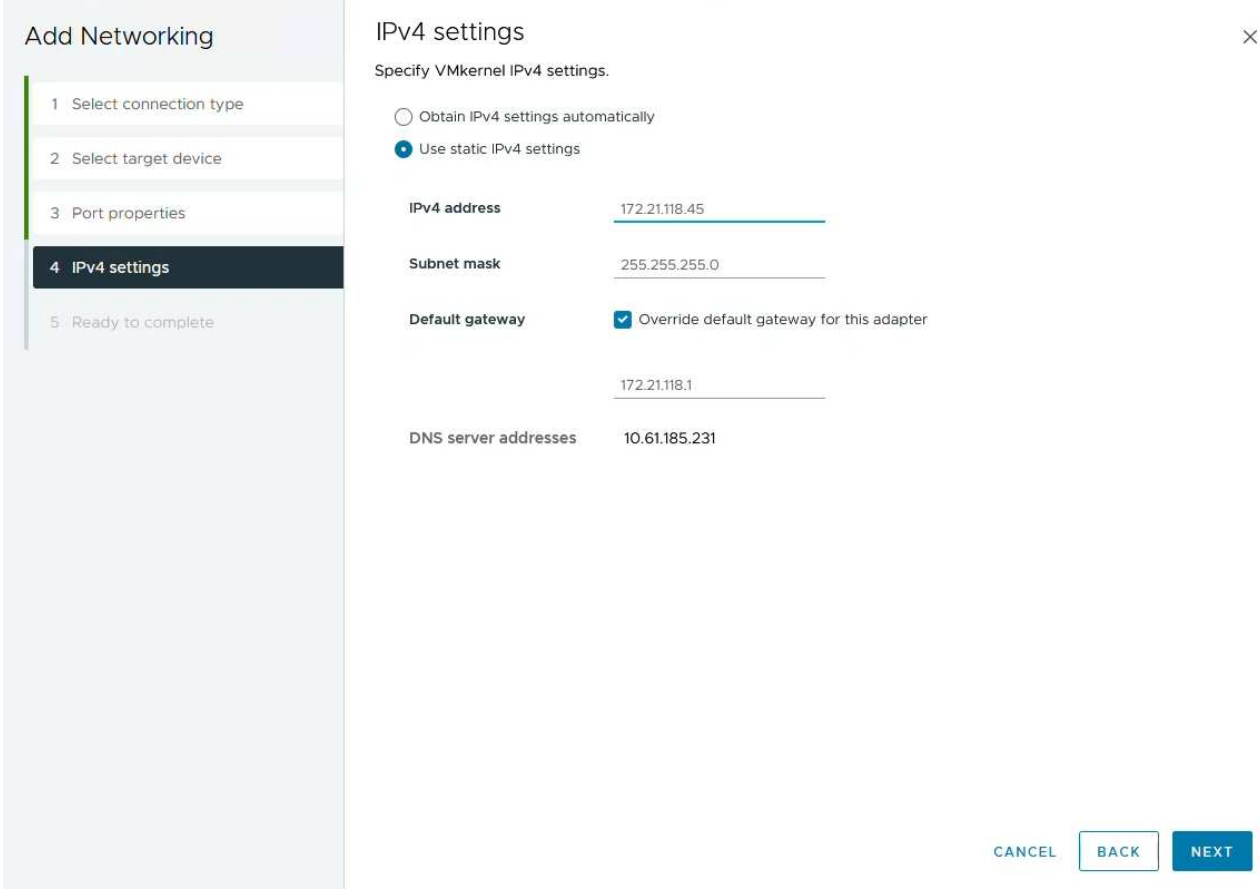
2. Nella finestra **Select Connection type** (Seleziona tipo di connessione), scegliere **VMkernel Network Adapter** (scheda di rete VMkernel) e fare clic su **Next** (Avanti) per continuare.



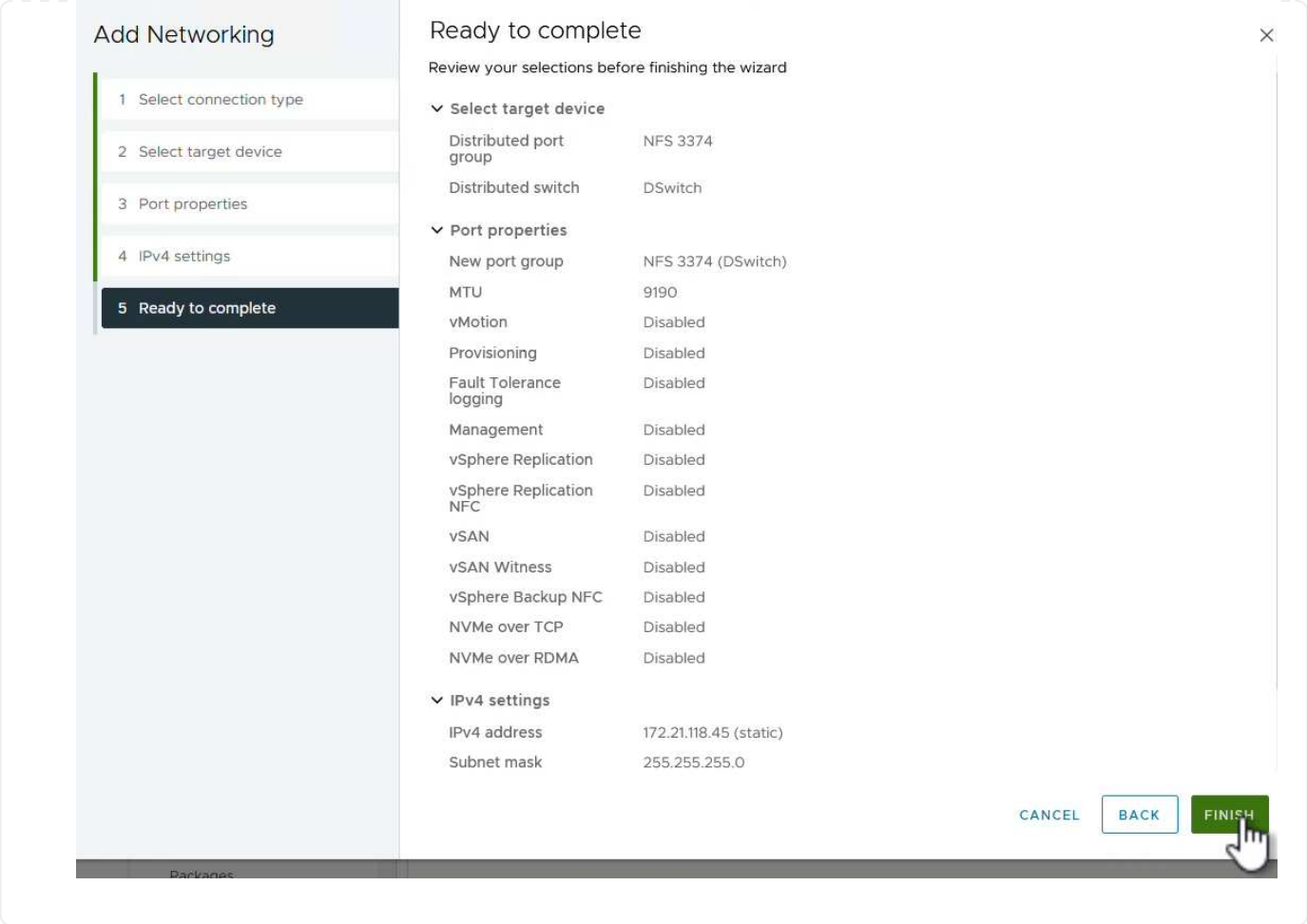
3. Nella pagina **Seleziona dispositivo di destinazione**, scegliere uno dei gruppi di porte distribuiti per NFS creati in precedenza.



4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite (nessun servizio abilitato) e fare clic su **Avanti** per continuare.
5. Nella pagina **IPv4 settings** compilare i campi **IP address**, **Subnet mask** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.



6. Rivedere le selezioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare l'adattatore VMkernel.



Implementare e utilizzare gli strumenti ONTAP 10 per configurare lo storage

I seguenti passaggi vengono eseguiti sul cluster vSphere 8 utilizzando il client vSphere e prevedono la distribuzione di OTV, la configurazione di ONTAP Tools Manager e la creazione di un datastore vVol NFS.

Per la documentazione completa sulla distribuzione e l'utilizzo degli strumenti ONTAP per VMware vSphere 10, fare riferimento a "Preparazione all'implementazione dei tool ONTAP per VMware vSphere".

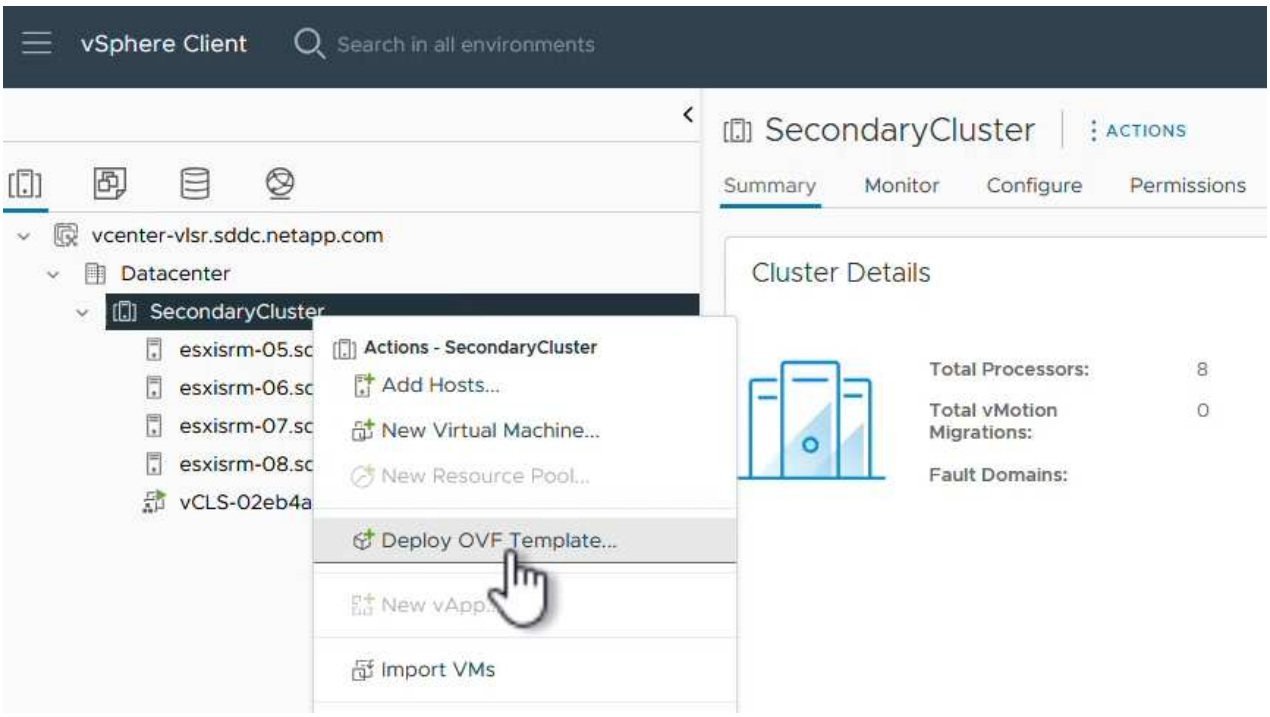
Implementa i tool ONTAP per VMware vSphere 10

I tool ONTAP per VMware vSphere 10 vengono implementati come appliance delle macchine virtuali e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP. Strumenti ONTAP 10 è dotato di un nuovo portale di gestione globale per la gestione delle connessioni a più server vCenter e backend storage ONTAP.

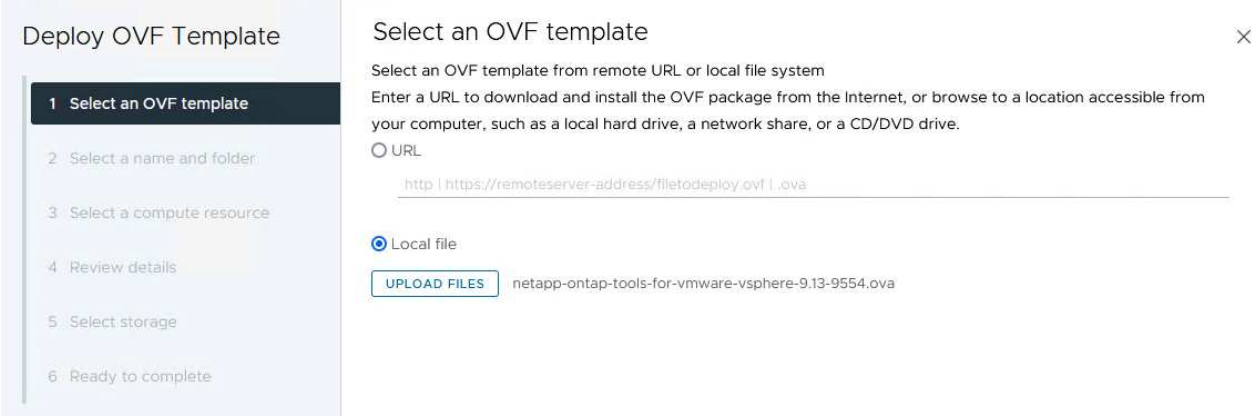
> In uno scenario di implementazione non ha, sono necessari tre indirizzi IP disponibili. Un indirizzo IP è allocato per il bilanciamento del carico, un altro per il piano di controllo Kubernetes e il restante per il nodo. In un'implementazione ha, sono necessari due indirizzi IP aggiuntivi per il secondo e il terzo nodo, oltre ai tre iniziali. Prima dell'assegnazione, i nomi host devono essere associati agli indirizzi IP nel DNS. È importante che tutti e cinque gli indirizzi IP si trovino sulla stessa VLAN, scelta per la distribuzione.

Completa quanto segue per implementare i tool ONTAP per VMware vSphere:

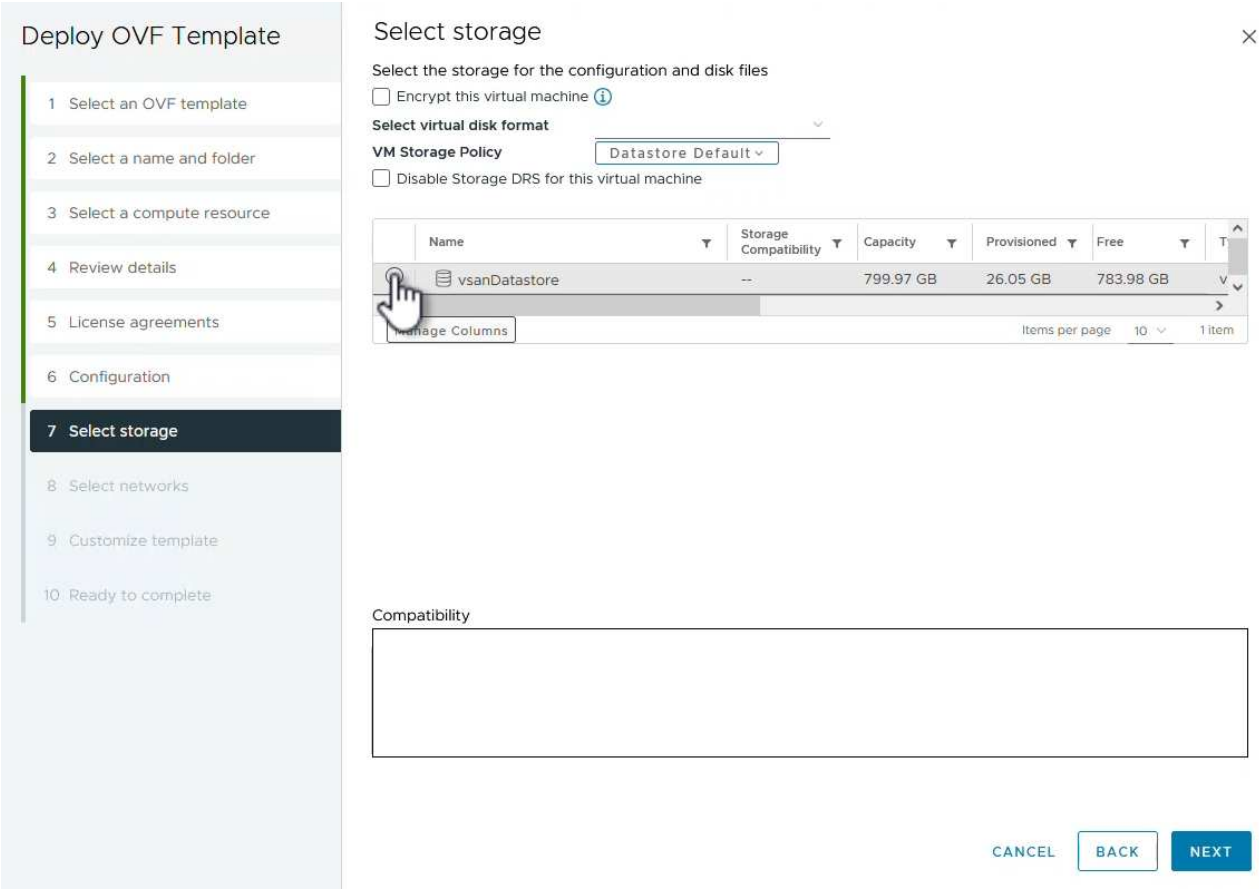
1. Ottenere l'immagine OVA degli strumenti ONTAP dal "Sito di supporto NetApp"e scaricarla in una cartella locale.
2. Effettua l'accesso all'appliance vCenter per il cluster vSphere 8.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Deploy OVF Template…**



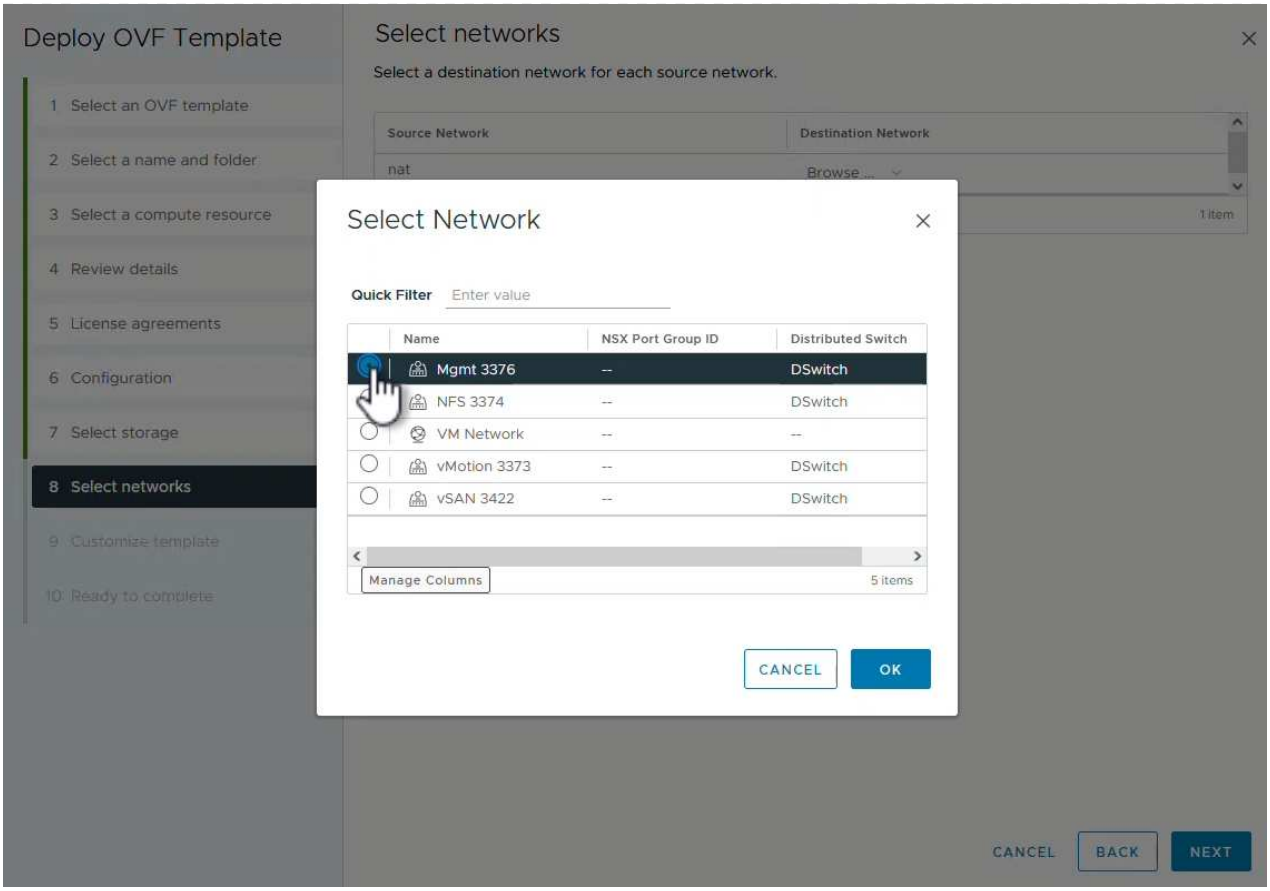
4. Nella procedura guidata **Deploy OVF Template** fare clic sul pulsante di opzione **file locale** e selezionare il file OVA di ONTAP Tools scaricato nel passaggio precedente.



5. Per i passaggi da 2 a 5 della procedura guidata, selezionare un nome e una cartella per la macchina virtuale, selezionare la risorsa di elaborazione, esaminare i dettagli e accettare il contratto di licenza.
6. Per la posizione dello storage dei file di configurazione e del disco, selezionare un datastore locale o un datastore vSAN.

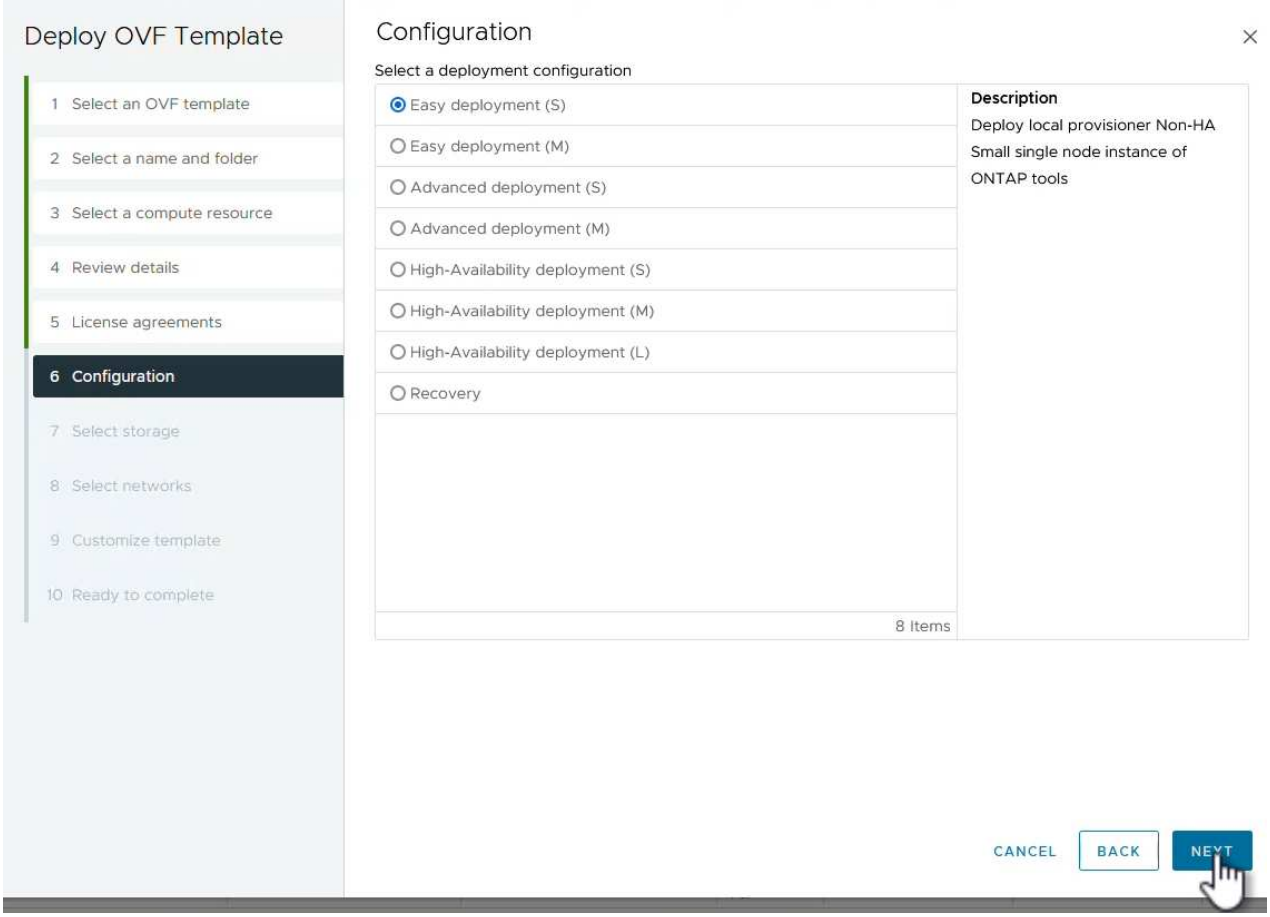


7. Nella pagina Seleziona rete, selezionare la rete utilizzata per la gestione del traffico.



8. Nella pagina di configurazione, selezionare la configurazione di distribuzione da utilizzare. In questo scenario viene utilizzato il metodo di distribuzione semplice.

> ONTAP Tool 10 offre diverse configurazioni di implementazione, incluse implementazioni ad alta disponibilità che utilizzano nodi multipli. Per la documentazione su tutte le configurazioni di distribuzione, fare riferimento alla "Preparazione all'implementazione dei tool ONTAP per VMware vSphere".



9. Nella pagina Personalizza modello compilare tutte le informazioni richieste:
   - Nome utente dell'applicazione da utilizzare per registrare il provider VASA e SRA in vCenter Server.
   - Abilita ASUP per il supporto automatizzato.
   - URL proxy ASUP, se necessario.
   - Nome utente e password dell'amministratore.
   - Server NTP.
   - Password utente di manutenzione per accedere alle funzioni di gestione dalla console.
   - IP del bilanciatore di carico.
   - IP virtuale per il piano di controllo K8s.
   - Macchina virtuale principale per selezionare la macchina virtuale corrente come principale (per configurazioni ha).
   - Nome host della macchina virtuale
   - Specificare i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

Customize the deployment properties of this software solution.

10 properties have invalid values

System Configuration	8 settings
Application username(*)	Username to assign to the Application vsphere-services
Application password(*)	Password to assign to the Application Password •••••••••• Confirm Password ••••••••••
Enable ASUP	Select this checkbox to enable ASUP ☑
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '-', '.', '!' special characters are supported
Administrator password(*)	Password to assign to the Administrator

CANCEL BACK NEXT

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Customize template

Maintenance user password(*)	Password to assign to maint user account Password •••••••••• Confirm Password ••••••••••
Deployment Configuration	**3 settings**
Load balancer IP(*)	Load balancer IP (*) 172.21.120.57
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane 172.21.120.58
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. ☑
Node Configuration	**10 settings**
HostName(*)	Specify the hostname for the VM
IP Address(*)	Specify the IP address for the appliance
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack

CANCEL BACK NEXT

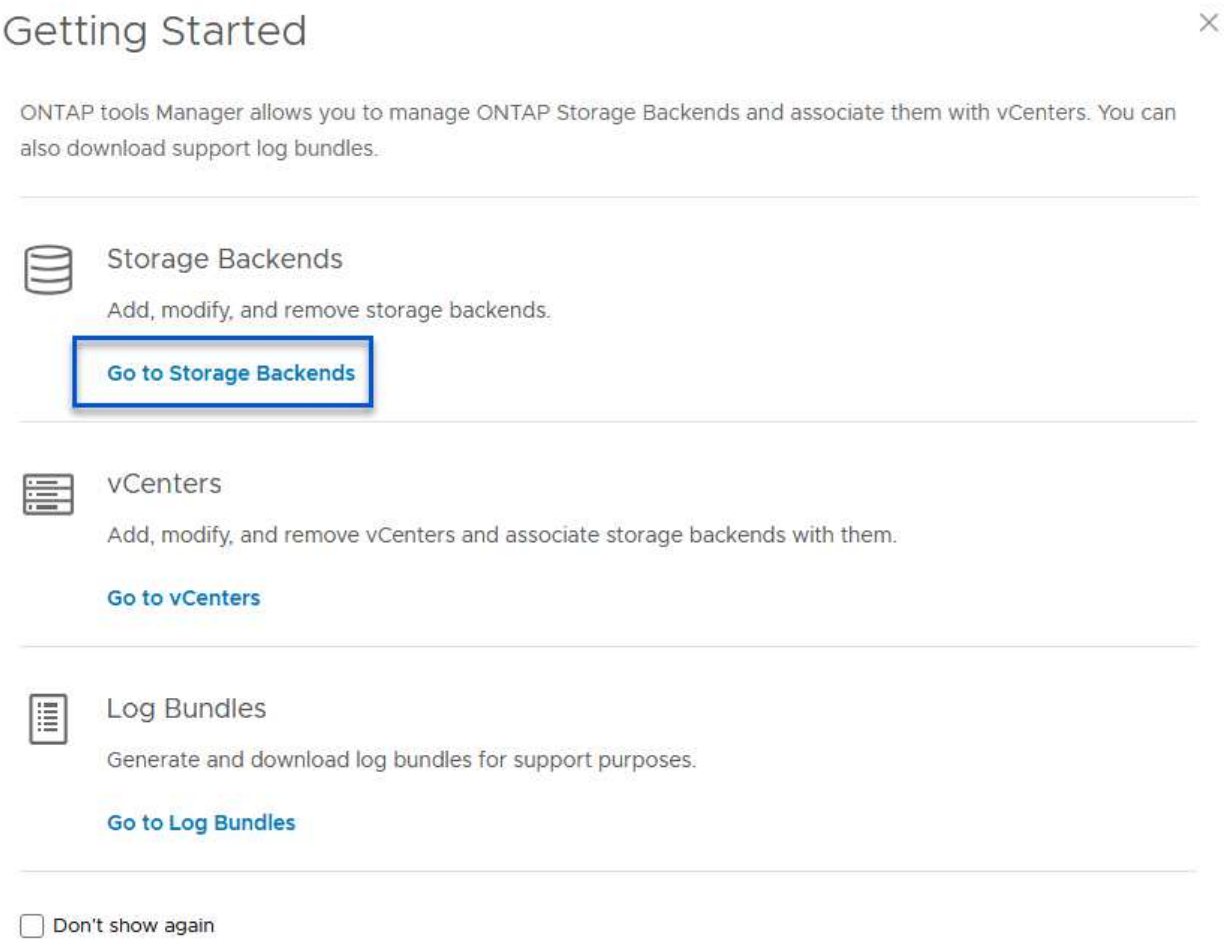
10. Esaminare tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare a distribuire l'appliance ONTAP Tools.

Connettere il backend dello storage e vCenter Server agli strumenti ONTAP 10.

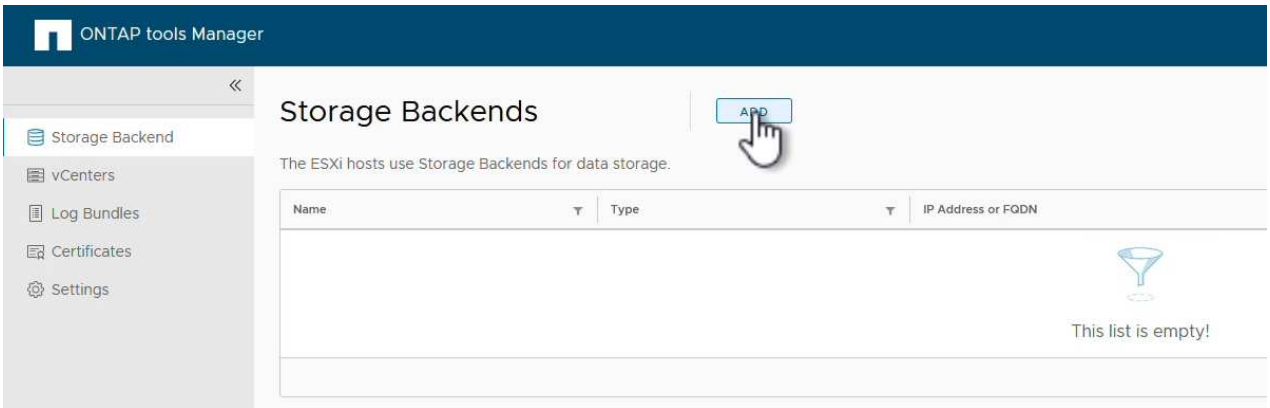
ONTAP Tools Manager viene utilizzato per configurare le impostazioni globali per ONTAP Tools 10.

1. Accedere a ONTAP Tools Manager accedendo a https://loadBalanceIP:8443/virtualization/ui/ in un browser Web e utilizzando le credenziali amministrative fornite durante la distribuzione.

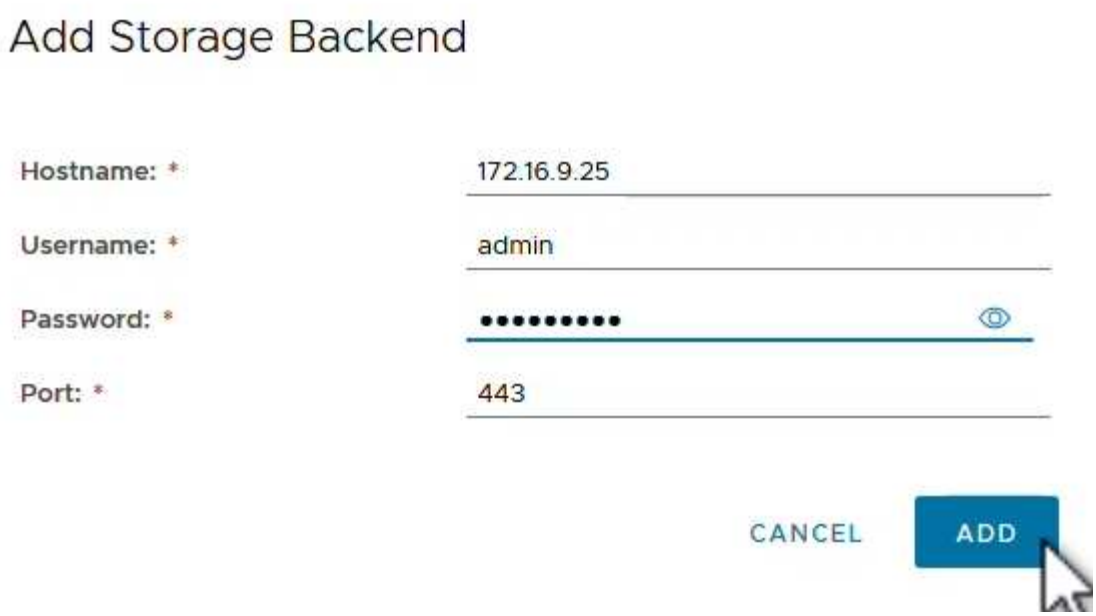
2. Nella pagina **Getting Started** (operazioni preliminari*), fare clic su **Go to Storage Backends** (Vai ai backend di archiviazione).



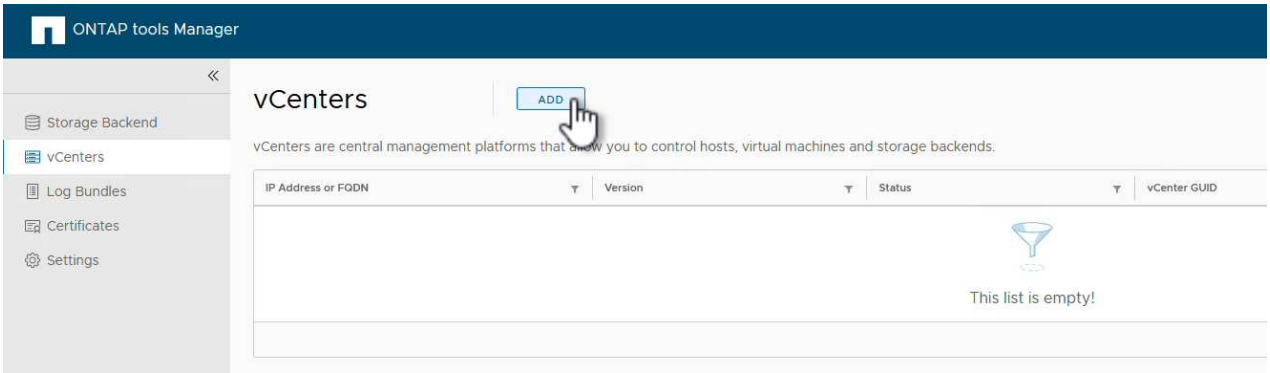
3. Nella pagina **backend di archiviazione**, fare clic su **ADD** per inserire le credenziali di un sistema di archiviazione ONTAP da registrare con gli strumenti ONTAP 10.



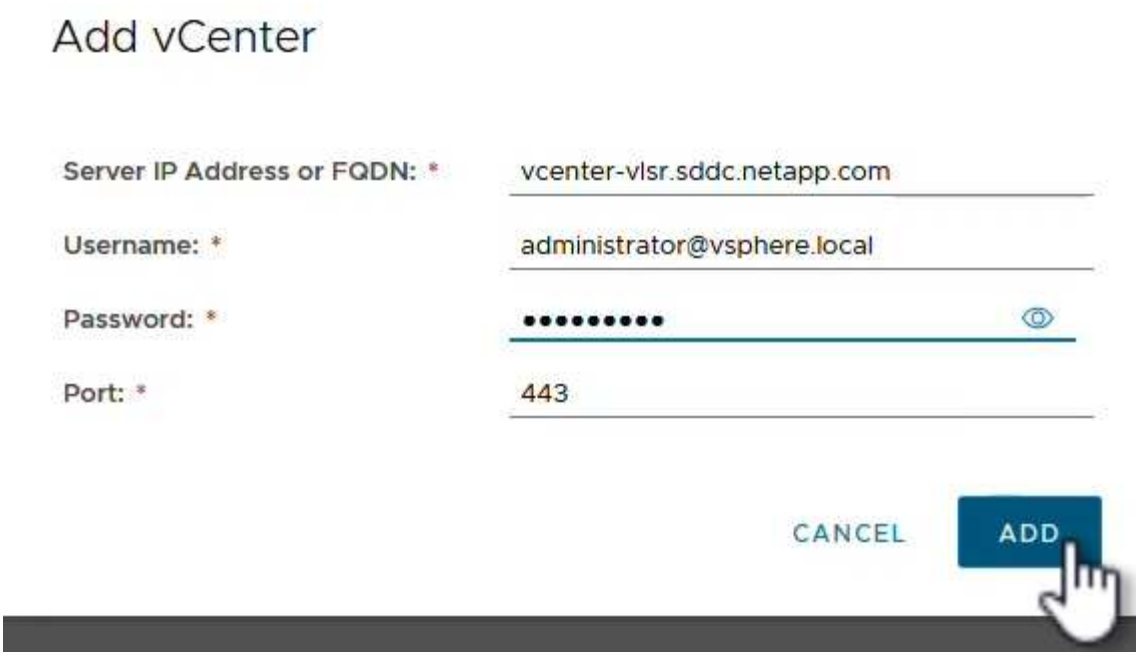
4. Nella casella **Aggiungi backend archiviazione**, immettere le credenziali per il sistema di archiviazione ONTAP.



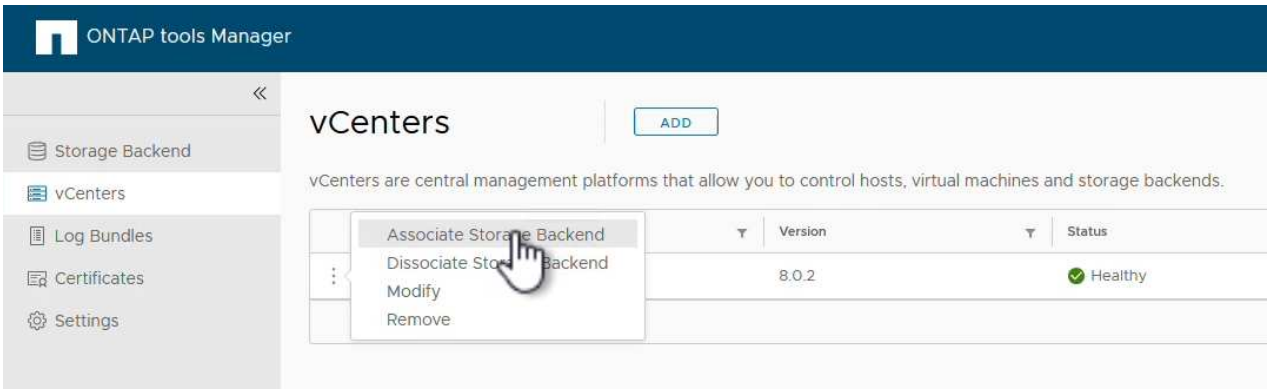
5. Nel menu a sinistra, fare clic su **vCenter**, quindi su **ADD** per inserire le credenziali di un server vCenter da registrare con gli strumenti ONTAP 10.



6. Nella casella **Aggiungi vCenter**, compila le credenziali per il sistema storage ONTAP.

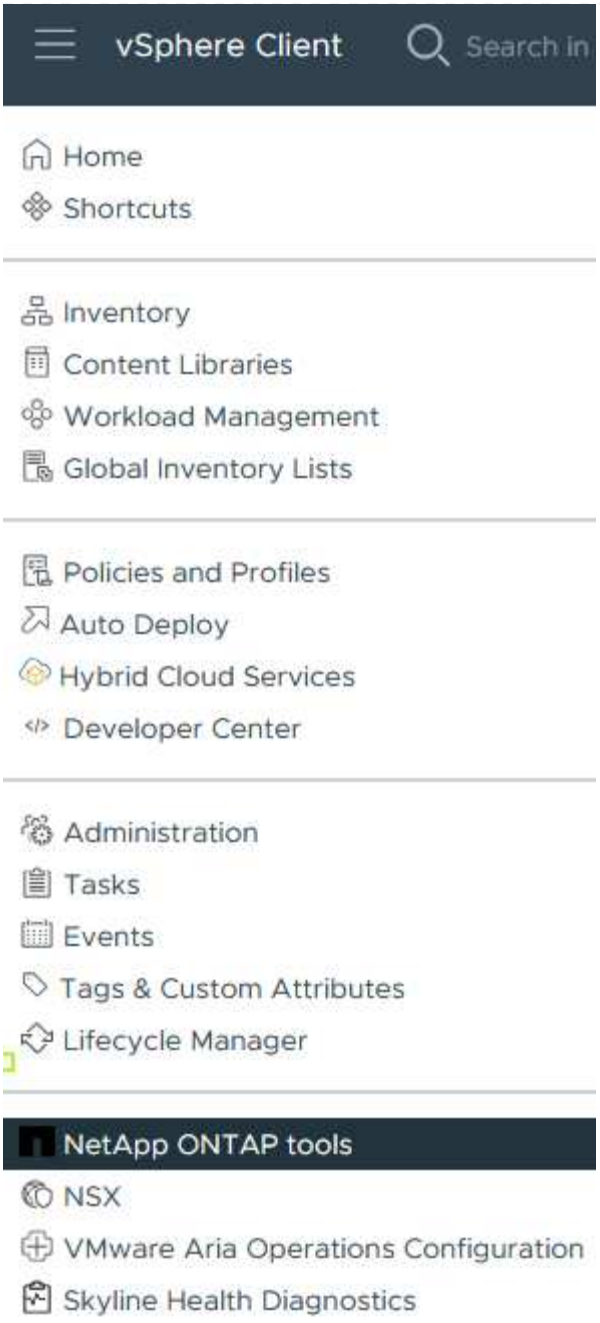


7. Dal menu verticale a tre punti per il nuovo server vCenter, selezionare **Associa backend storage**.

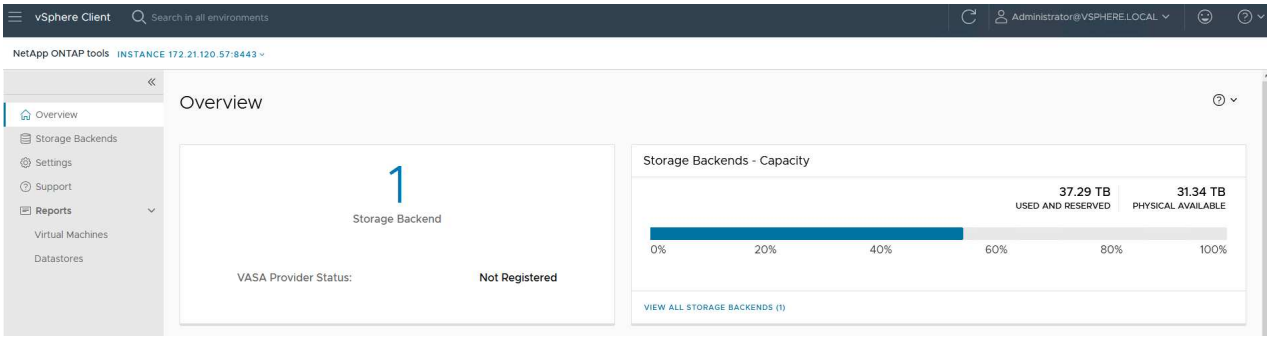


8. Nella casella **associate Storage backend**, selezionare il sistema di archiviazione ONTAP da associare al server vCenter e fare clic su **associate** per completare l'azione.

9. Per verificare l'installazione, accedere al client vSphere e selezionare **NetApp ONTAP tools** dal menu a sinistra.



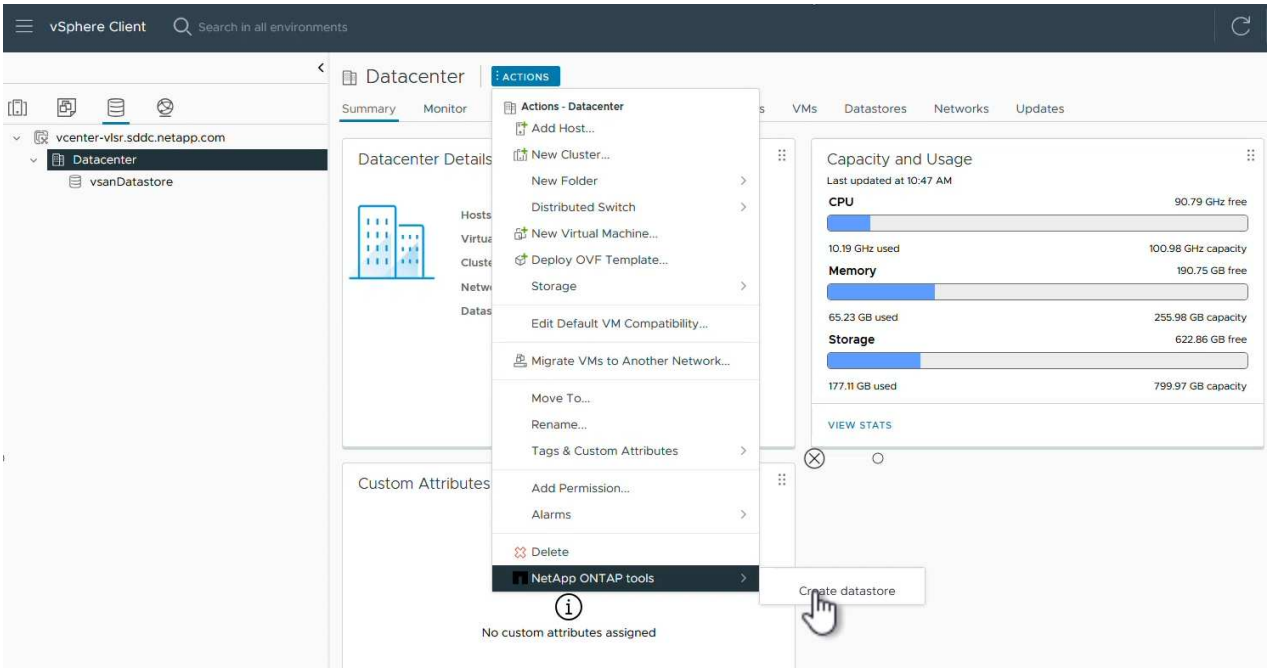
10. Dalla dashboard degli strumenti di ONTAP dovresti vedere che a vCenter Server è stato associato un backend storage.



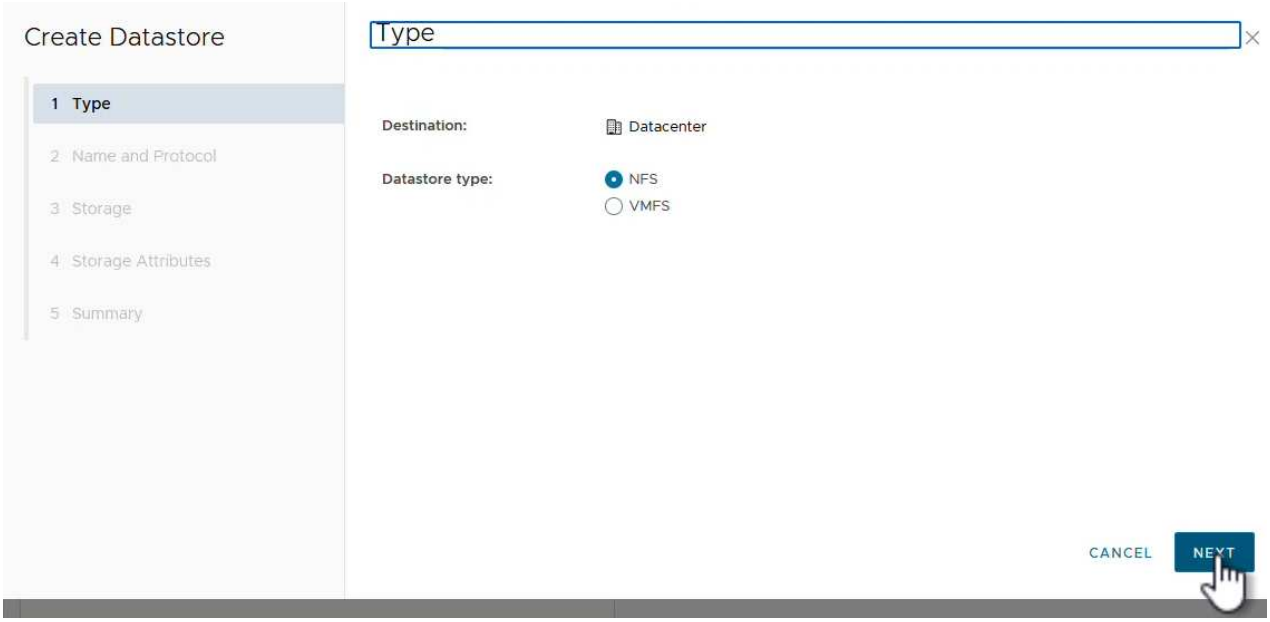
Creare un datastore NFS utilizzando gli strumenti ONTAP 10

Completa i seguenti passaggi per implementare un datastore ONTAP, in esecuzione su NFS, usando i tool ONTAP 10.

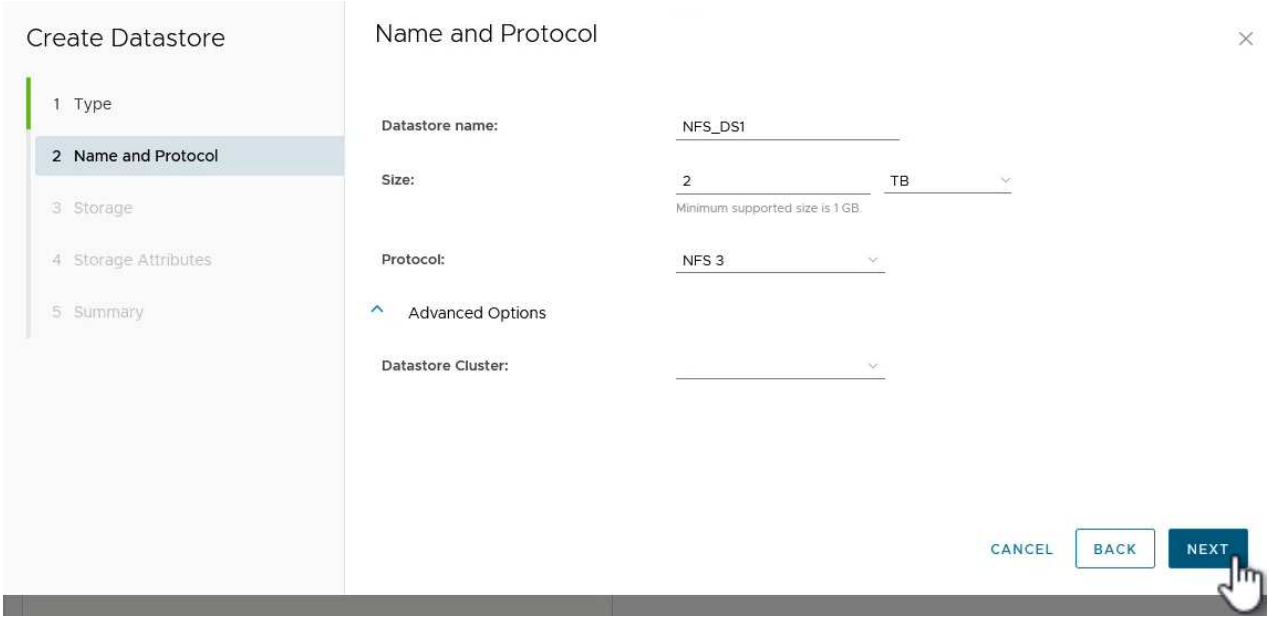
1. Nel client vSphere, accedere all'inventario dello storage. Dal menu **AZIONI**, selezionare **Strumenti NetApp ONTAP > Crea archivio dati**.



2. Nella pagina **tipo** della procedura guidata Crea datastore, fare clic sul pulsante di opzione NFS, quindi su **Avanti** per continuare.

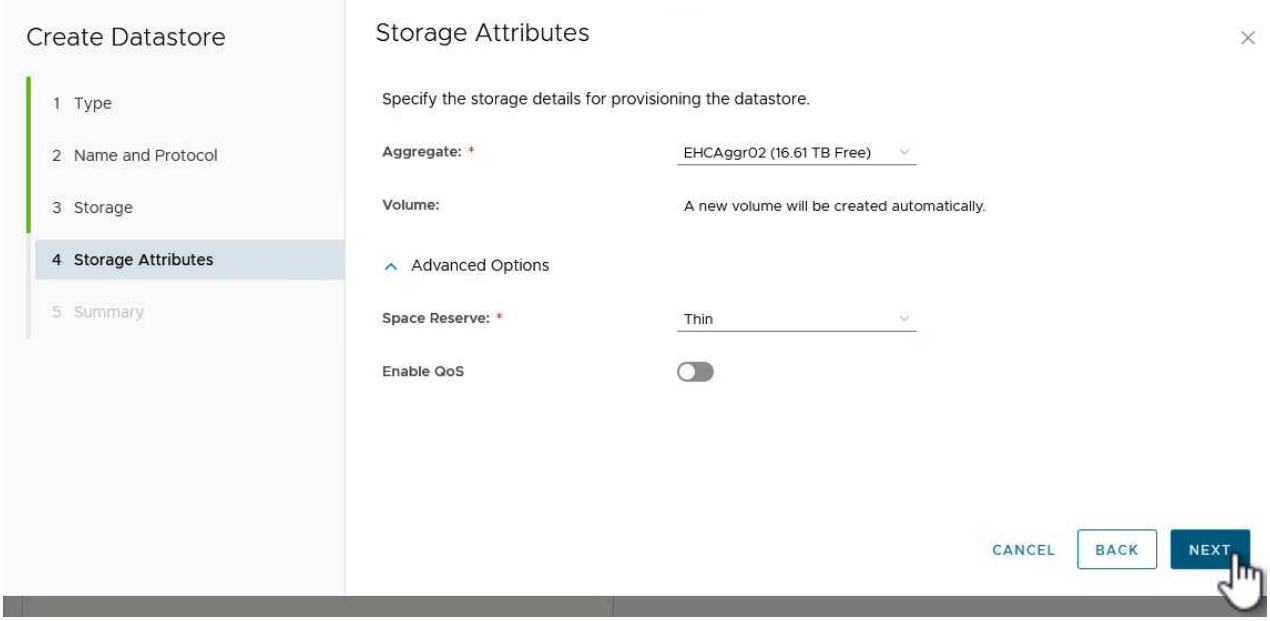


3. Nella pagina **Nome e protocollo**, compilare il nome, le dimensioni e il protocollo per il datastore. Fare clic su **Avanti** per continuare.

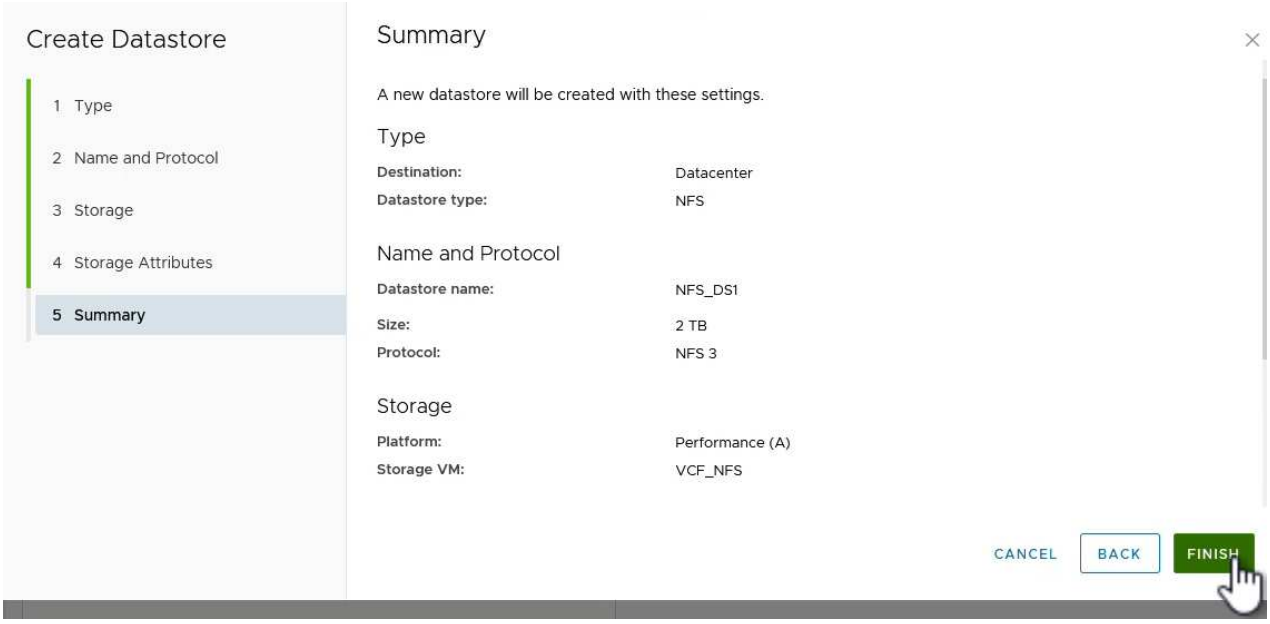


4. Nella pagina **Storage** selezionare una piattaforma (filtra il sistema di archiviazione in base al tipo) e una VM di archiviazione per il volume. In alternativa, selezionare un criterio di esportazione personalizzato. Fare clic su **Avanti** per continuare.

5. Nella pagina **attributi archiviazione** selezionare l'aggregato di archiviazione da utilizzare e, facoltativamente, opzioni avanzate quali la prenotazione dello spazio e la qualità del servizio. Fare clic su **Avanti** per continuare.



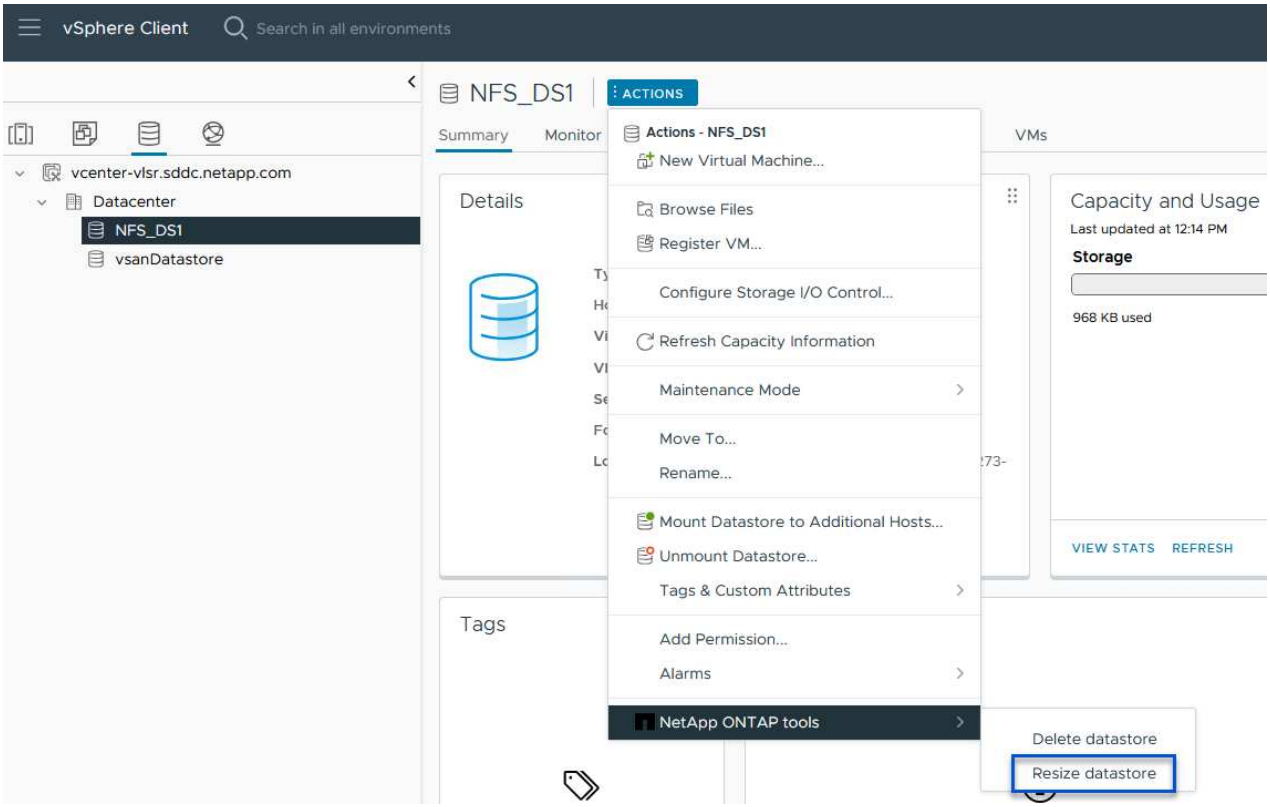
6. Infine, rivedere il **Summary** e fare clic su Finish (fine) per iniziare a creare il datastore NFS.



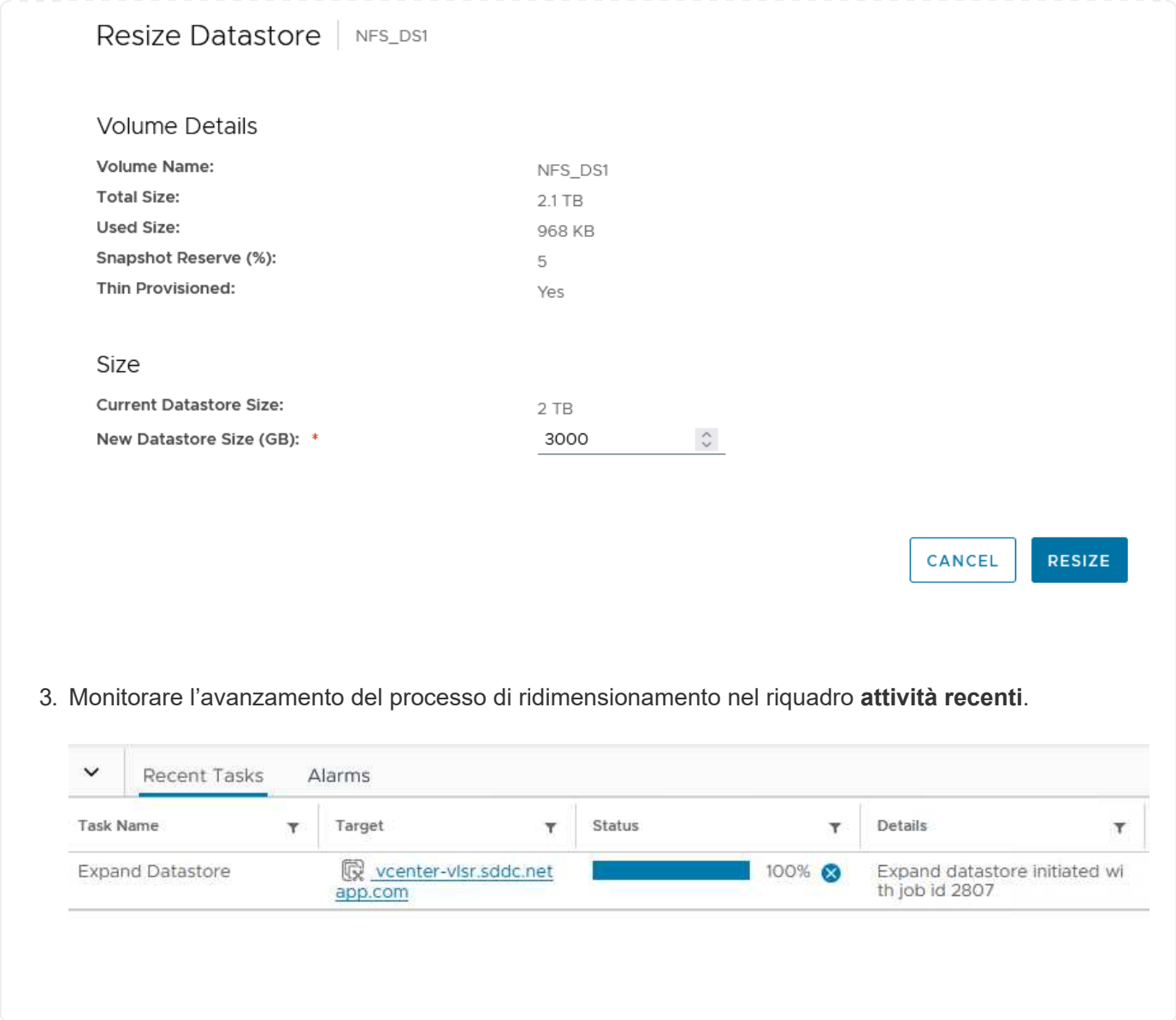
Ridimensionamento di un datastore NFS utilizzando strumenti ONTAP 10

Completa i seguenti passaggi per ridimensionare un datastore NFS esistente con i tool ONTAP 10.

1. Nel client vSphere, accedere all'inventario dello storage. Dal menu **AZIONI**, selezionare **Strumenti NetApp ONTAP > Ridimensiona archivio dati**.



2. Nella procedura guidata **Ridimensiona datastore**, immettere le nuove dimensioni del datastore in GB e fare clic su **Ridimensiona** per continuare.



3. Monitorare l'avanzamento del processo di ridimensionamento nel riquadro **attività recenti**.

Ulteriori informazioni

Per un elenco completo dei tool ONTAP per le risorse di VMware vSphere 10, consultare "Strumenti ONTAP per le risorse di documentazione di VMware vSphere" .

Per ulteriori informazioni sulla configurazione dei sistemi storage ONTAP, consultare il "Documentazione di ONTAP 10"centro dati.

Utilizza VMware Site Recovery Manager per il disaster recovery dei datastore NFS

L'utilizzo degli strumenti ONTAP per VMware vSphere 10 e Site Replication Adapter (SRA) insieme a VMware Site Recovery Manager (SRM) apporta un valore significativo alle attività di disaster recovery. I tool ONTAP 10 offrono solide funzionalità di storage, tra cui high Availability e scalabilità native per il provider VASA, con supporto per vVol iSCSI e NFS. Ciò garantisce la disponibilità dei dati e semplifica la gestione di più server VMware vCenter e cluster ONTAP. Utilizzando SRA con VMware Site Recovery Manager, le organizzazioni possono ottenere una replica e un failover perfetti delle macchine

virtuali e dei dati tra i siti, consentendo processi di disaster recovery efficienti. La combinazione di tool ONTAP e SRA permette alle aziende di proteggere i workload critici, ridurre al minimo il downtime e mantenere la business continuity in caso di eventi imprevisti o disastri.

I tool ONTAP 10 semplificano la gestione dello storage e le funzioni di efficienza, migliorano la disponibilità e riducono i costi dello storage e l'overhead operativo, sia che si utilizzi SAN o NAS. Utilizza le Best practice per il provisioning degli archivi dati e ottimizza le impostazioni degli host ESXi per gli ambienti di storage a blocchi e NFS. Per tutti questi vantaggi, NetApp consiglia questo plug-in quando si utilizza vSphere con sistemi che eseguono il software ONTAP.

SRA viene utilizzato insieme a SRM per gestire la replica dei dati delle macchine virtuali tra siti di produzione e disaster recovery per datastore VMFS e NFS tradizionali e per il test senza interruzioni delle repliche DR. Consente di automatizzare le attività di rilevamento, ripristino e protezione.

In questo scenario, dimostreremo come distribuire e utilizzare VMware Site Recovery Manager per proteggere i datastore ed eseguire un failover di test e finale su un sito secondario. Vengono inoltre discussi il ripristino e il failback.

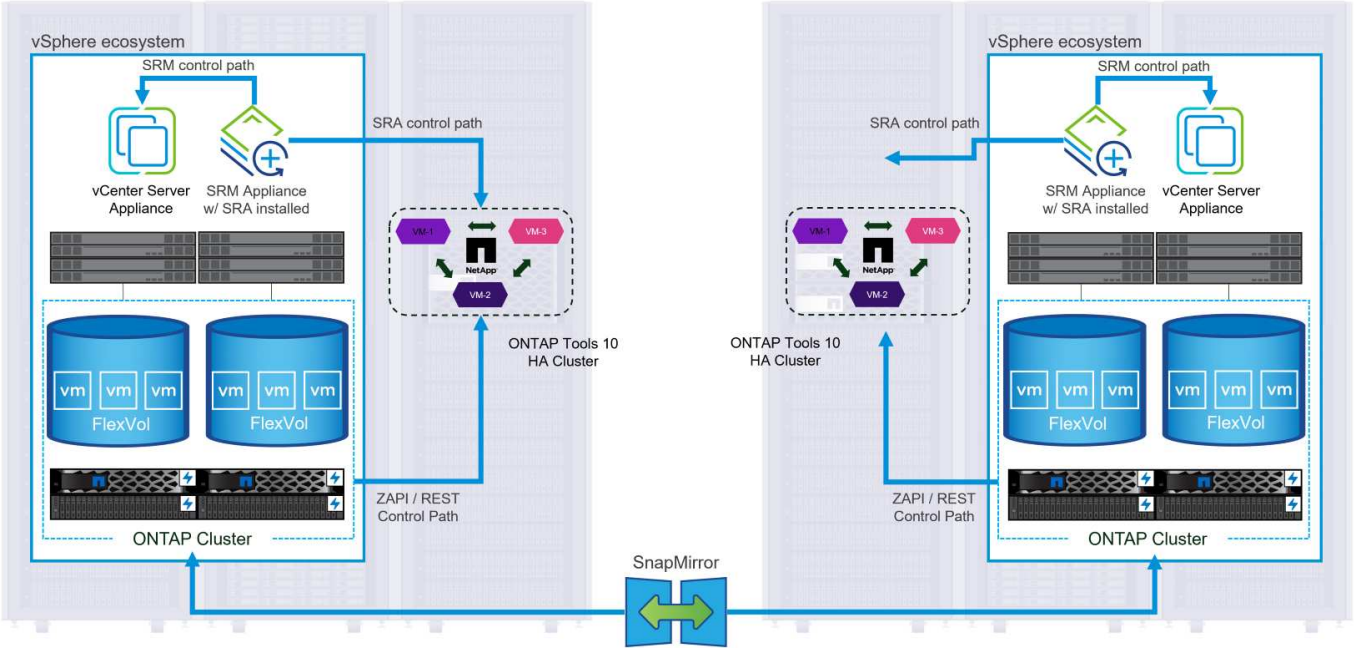
Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

- Configurare SRM con i server vCenter nei siti primario e secondario.
- Installa l'adattatore SRA per i tool ONTAP per VMware vSphere 10 e registrati con vCenter.
- Crea relazioni SnapMirror tra i sistemi storage ONTAP di origine e di destinazione
- Configurare Site Recovery per SRM.
- Esecuzione del test e failover finale.
- Discutere della protezione e del failback.

Architettura

Il diagramma seguente mostra un'architettura tipica di VMware Site Recovery con strumenti ONTAP per VMware vSphere 10 configurati in una configurazione a disponibilità elevata a 3 nodi.



Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Cluster vSphere 8 installati nelle posizioni principale e secondaria con networking adeguato per le comunicazioni tra ambienti.
- Sistemi storage ONTAP in posizioni primarie e secondarie, con porte per dati fisici su switch ethernet dedicati al traffico storage NFS.
- Gli strumenti ONTAP per VMware vSphere 10 sono installati e entrambi i server vCenter sono registrati.
- Le appliance VMware Site Replication Manager sono state installate per i siti primario e secondario.
  - Le mappature dell'inventario (rete, cartella, risorsa, criterio di archiviazione) sono state configurate per SRM.

NetApp consiglia progettazioni di rete ridondanti per NFS, per fornire la tolleranza agli errori di sistemi storage, switch, adattatori di rete e sistemi host. È comune implementare NFS con una singola subnet o più subnet a seconda dei requisiti architetturali.

Fare riferimento a. "Best practice per l'esecuzione di NFS con VMware vSphere" Per informazioni dettagliate specifiche di VMware vSphere.

Per assistenza sulla rete per l'utilizzo di ONTAP con VMware vSphere, fare riferimento al "Configurazione di rete - NFS" Della documentazione relativa alle applicazioni aziendali NetApp.

Per la documentazione NetApp sull'utilizzo dello storage ONTAP con VMware SRM, fare riferimento a. "VMware Site Recovery Manager con ONTAP"

Fasi di implementazione

Nelle sezioni seguenti vengono descritte le fasi di distribuzione per implementare e verificare una configurazione di VMware Site Recovery Manager con il sistema di archiviazione ONTAP.

Crea una relazione di SnapMirror tra i sistemi storage ONTAP

Per proteggere i volumi del datastore, è necessario stabilire una relazione di SnapMirror tra i sistemi storage ONTAP di origine e di destinazione.

Per "QUI" informazioni complete sulla creazione di relazioni di SnapMirror per ONTAP Volumes, consulta la documentazione di ONTAP.

Le istruzioni dettagliate sono descritte nel seguente documento, disponibile "QUI". Questa procedura spiega come creare relazioni di peer cluster e SVM e quindi relazioni SnapMirror per ogni volume. Queste operazioni possono essere eseguite in Gestione sistema di ONTAP o utilizzando l'interfaccia a riga di comando di ONTAP.

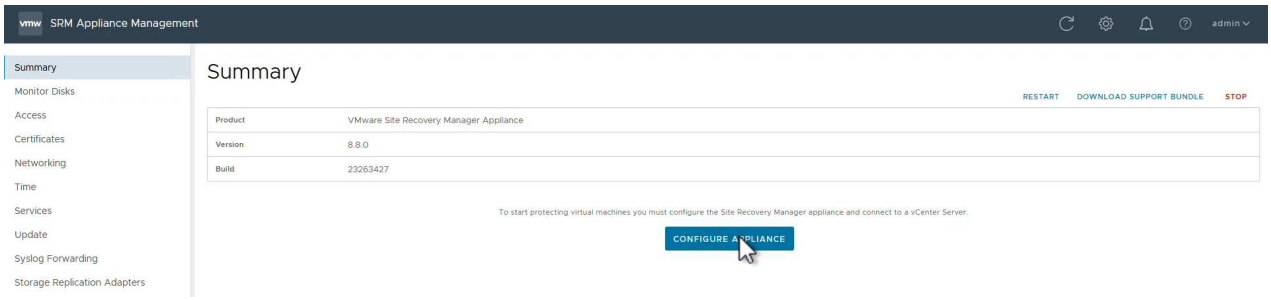
Configurare l'appliance SRM

Completare i seguenti passaggi per configurare l'appliance SRM e l'adattatore SRA.

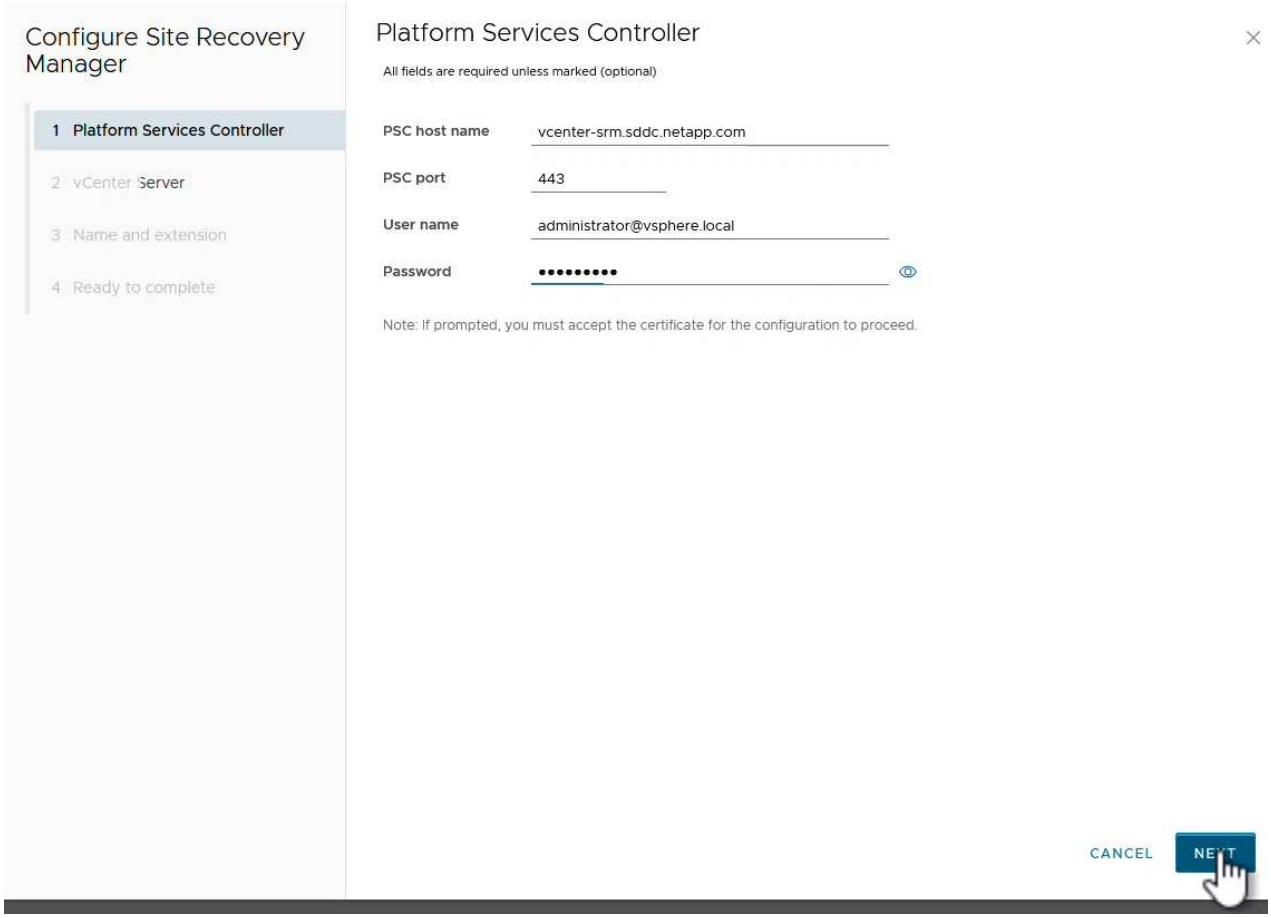
Collegare l'appliance SRM per i siti primario e secondario

I seguenti passaggi devono essere completati sia per il sito primario che per quello secondario.

1. In un browser Web, `https://<SRM_appliance_IP>:5480` accedere a e accedere. Fare clic su **Configure Appliance** per iniziare.

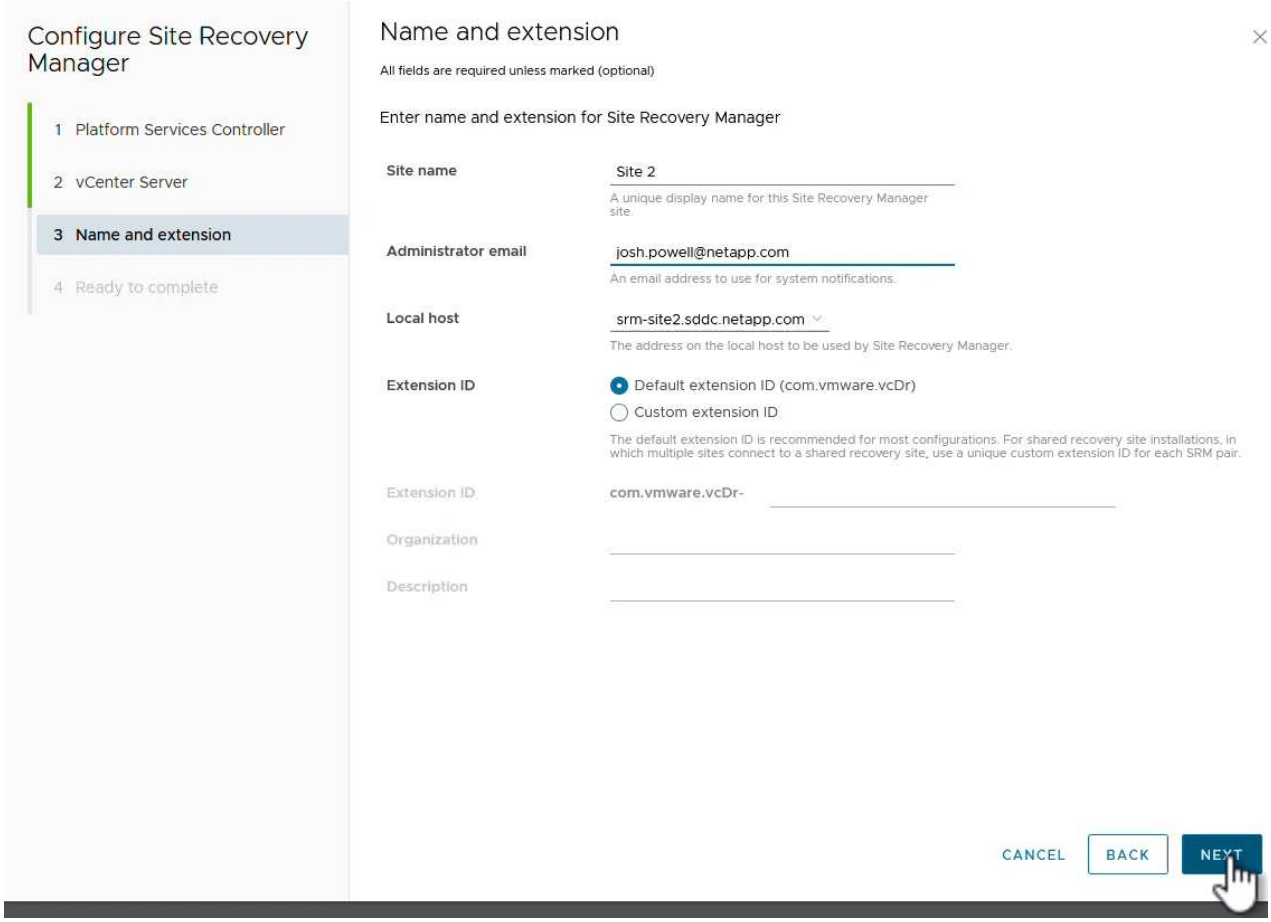


2. Nella pagina **Platform Services Controller** della procedura guidata Configura Site Recovery Manager, immettere le credenziali del server vCenter a cui verrà registrato SRM. Fare clic su **Avanti** per continuare.



3. Nella pagina **vCenter Server**, visualizzare il Vserver connesso e fare clic su **Avanti** per continuare.

4. Nella pagina **Nome ed estensione**, immettere un nome per il sito SRM, un indirizzo e-mail degli amministratori e l'host locale che verrà utilizzato da SRM. Fare clic su **Avanti** per continuare.

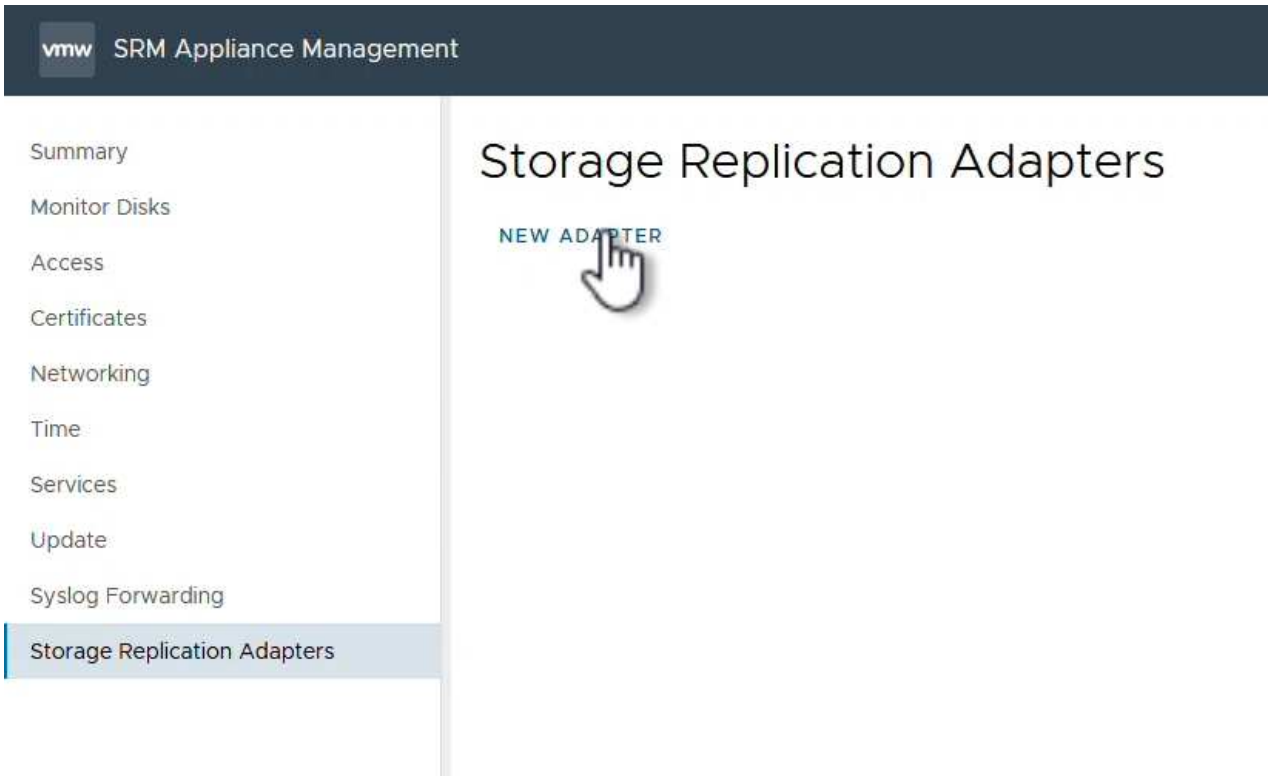


5. Nella pagina **Pronto per il completamento**, rivedere il riepilogo delle modifiche

Configurare SRA sull'appliance SRM

Completare i seguenti passaggi per configurare SRA sul dispositivo SRM:

1. Scaricare SRA for ONTAP Tools 10 dal sito Web "Sito di supporto NetApp" e salvare il file tar.gz in una cartella locale.
2. Nell'appliance di gestione SRM, fare clic su **Storage Replication Adapters** nel menu a sinistra, quindi su **New Adapter**.



3. Seguire le istruzioni riportate sul sito della documentazione di ONTAP Tools 10 all'indirizzo "Configurare SRA sull'appliance SRM". Una volta completata l'operazione, SRA può comunicare con SRA utilizzando l'indirizzo IP e le credenziali fornite dal server vCenter.

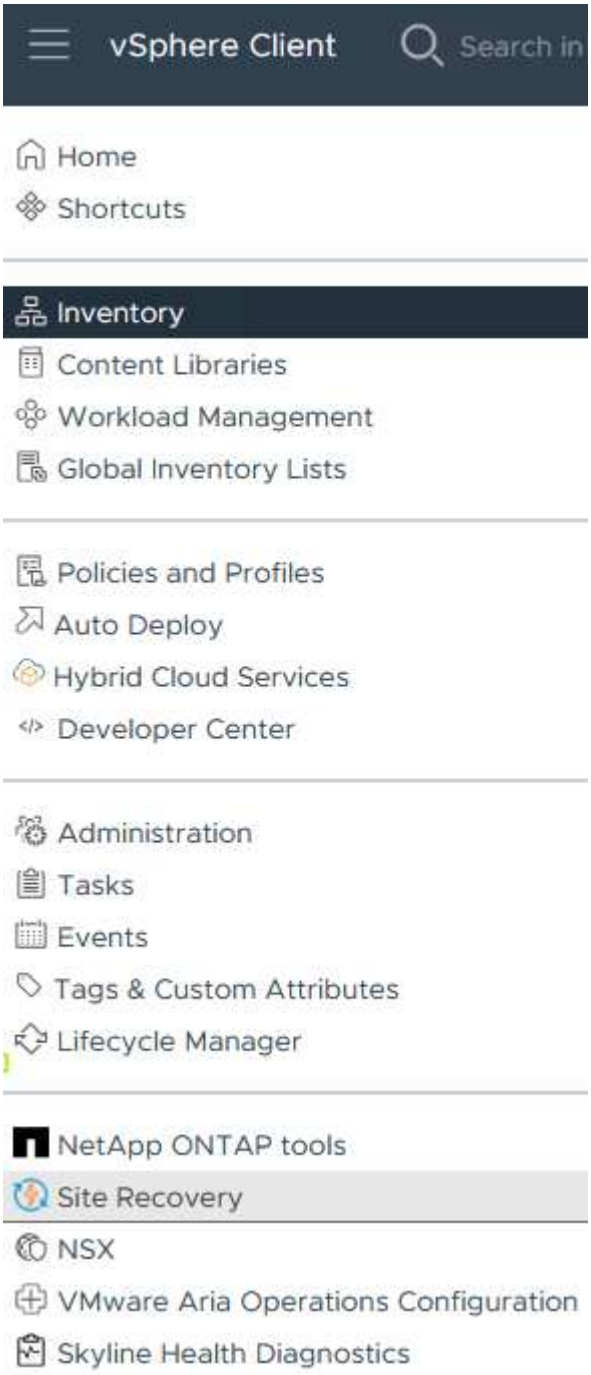
Configurare Site Recovery per SRM

Completare i seguenti passaggi per configurare l'associazione del sito, creare gruppi di protezione,

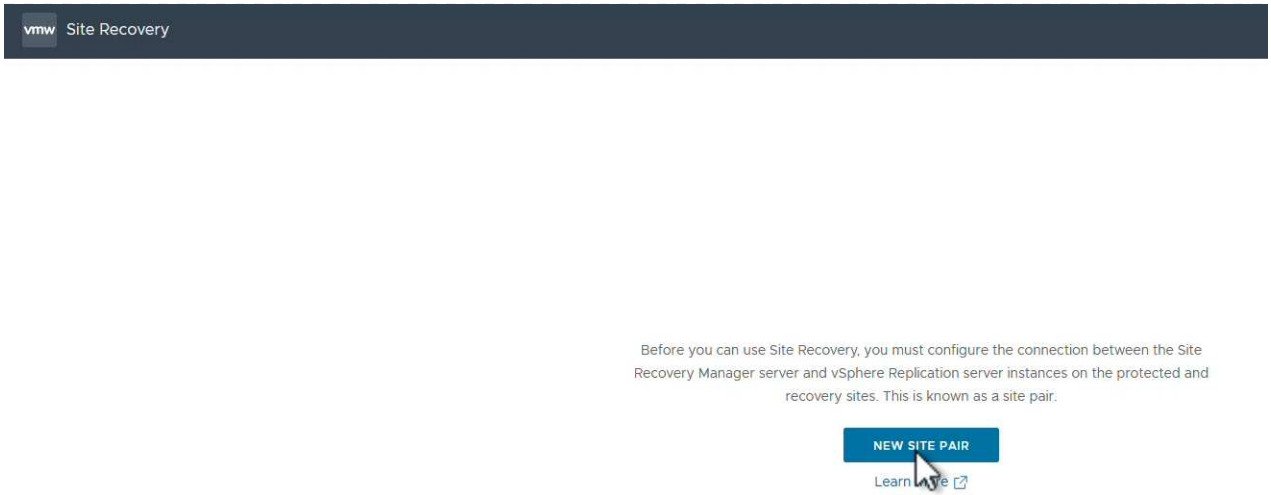
Configurare l’associazione del sito per SRM

Il passaggio seguente viene completato nel client vCenter del sito primario.

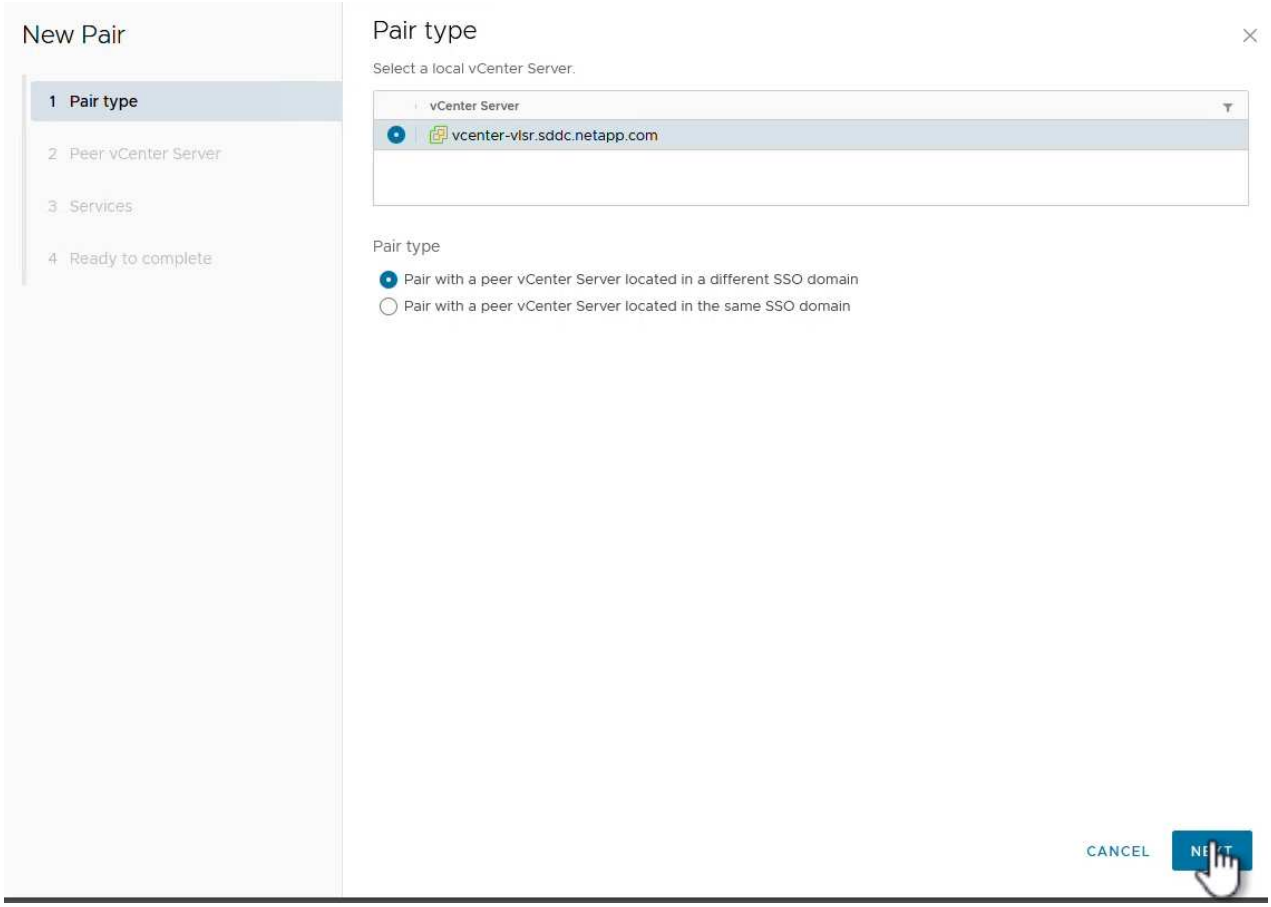
1. Nel client vSphere, fare clic su **Site Recovery** nel menu a sinistra. Viene aperta una nuova finestra del browser nell’interfaccia utente di gestione SRM del sito primario.



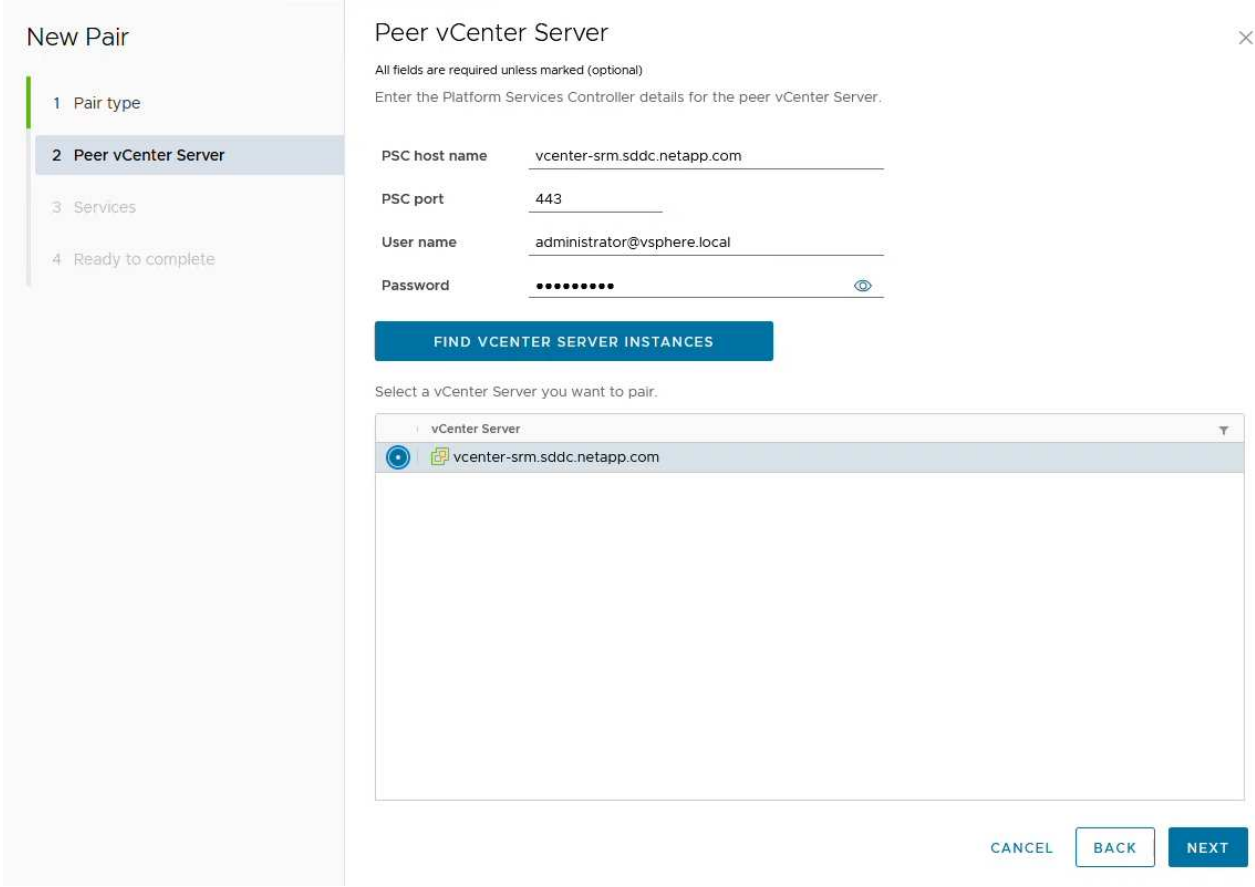
2. Nella pagina **Site Recovery**, fare clic su **NUOVA COPPIA DI SITI**.



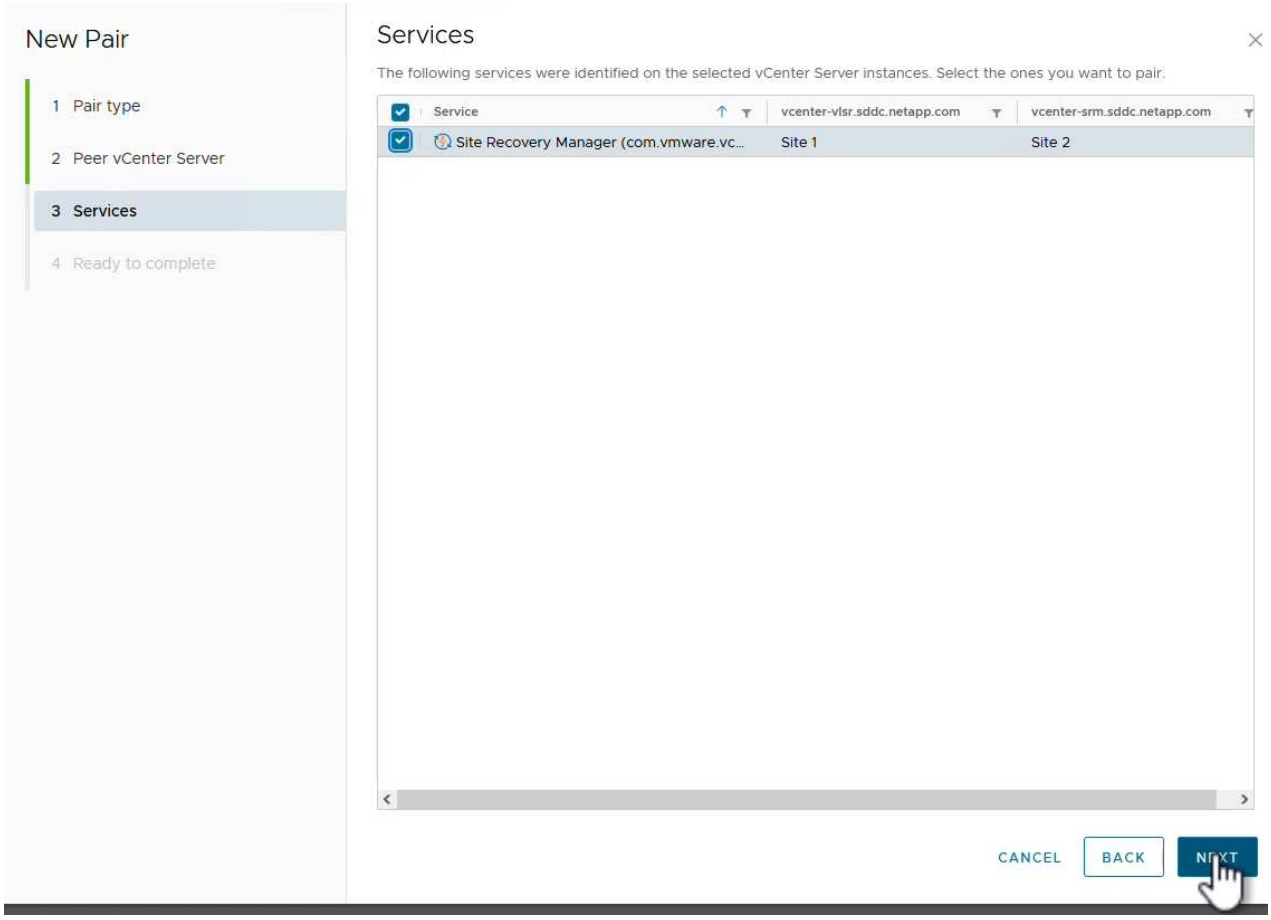
3. Nella pagina **tipo di coppia** della procedura guidata **Nuova coppia**, verificare che il server vCenter locale sia selezionato e selezionare **tipo di coppia**. Fare clic su **Avanti** per continuare.



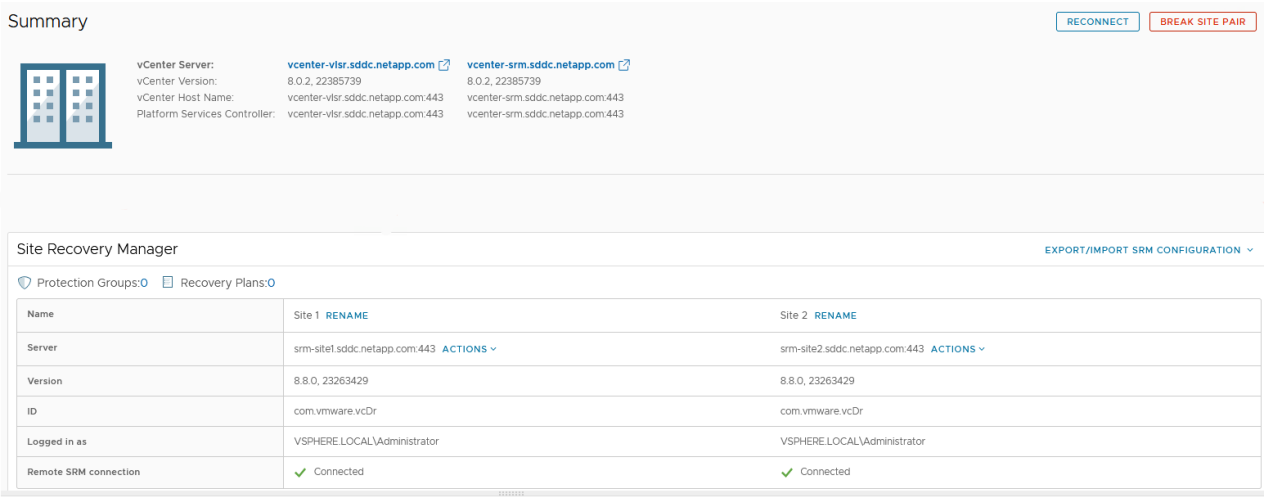
4. Nella pagina **Peer vCenter** compilare le credenziali di vCenter nel sito secondario e fare clic su **trova istanze vCenter**. Verificare che l'istanza di vCenter sia stata rilevata e fare clic su **Avanti** per continuare.



5. Nella pagina **servizi**, selezionare la casella accanto all'associazione del sito proposta. Fare clic su **Avanti** per continuare.



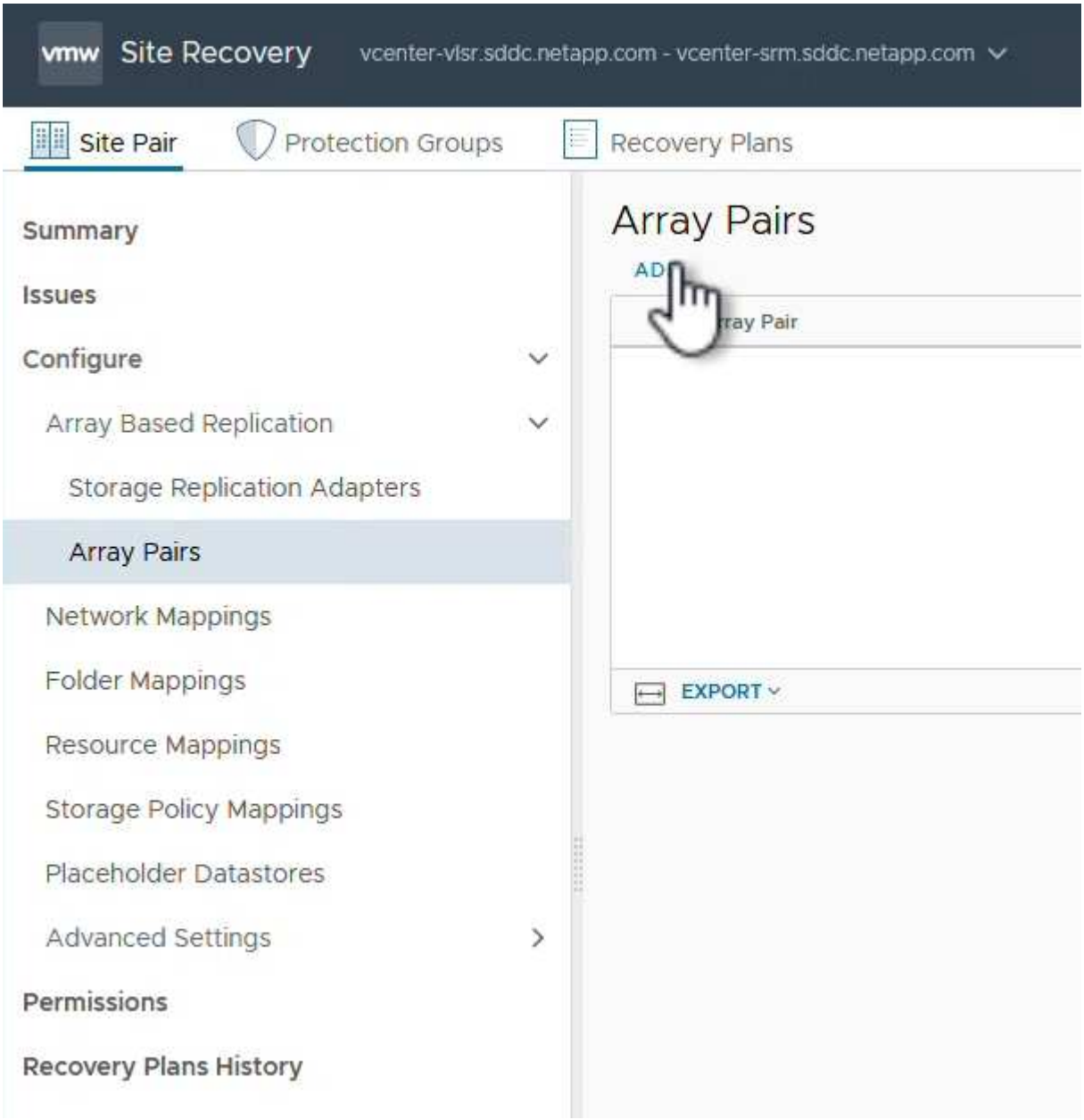
6. Nella pagina **Pronto per il completamento**, esaminare la configurazione proposta e quindi fare clic sul pulsante **fine** per creare l'associazione del sito
7. La nuova coppia di siti e il relativo riepilogo possono essere visualizzati nella pagina Riepilogo.



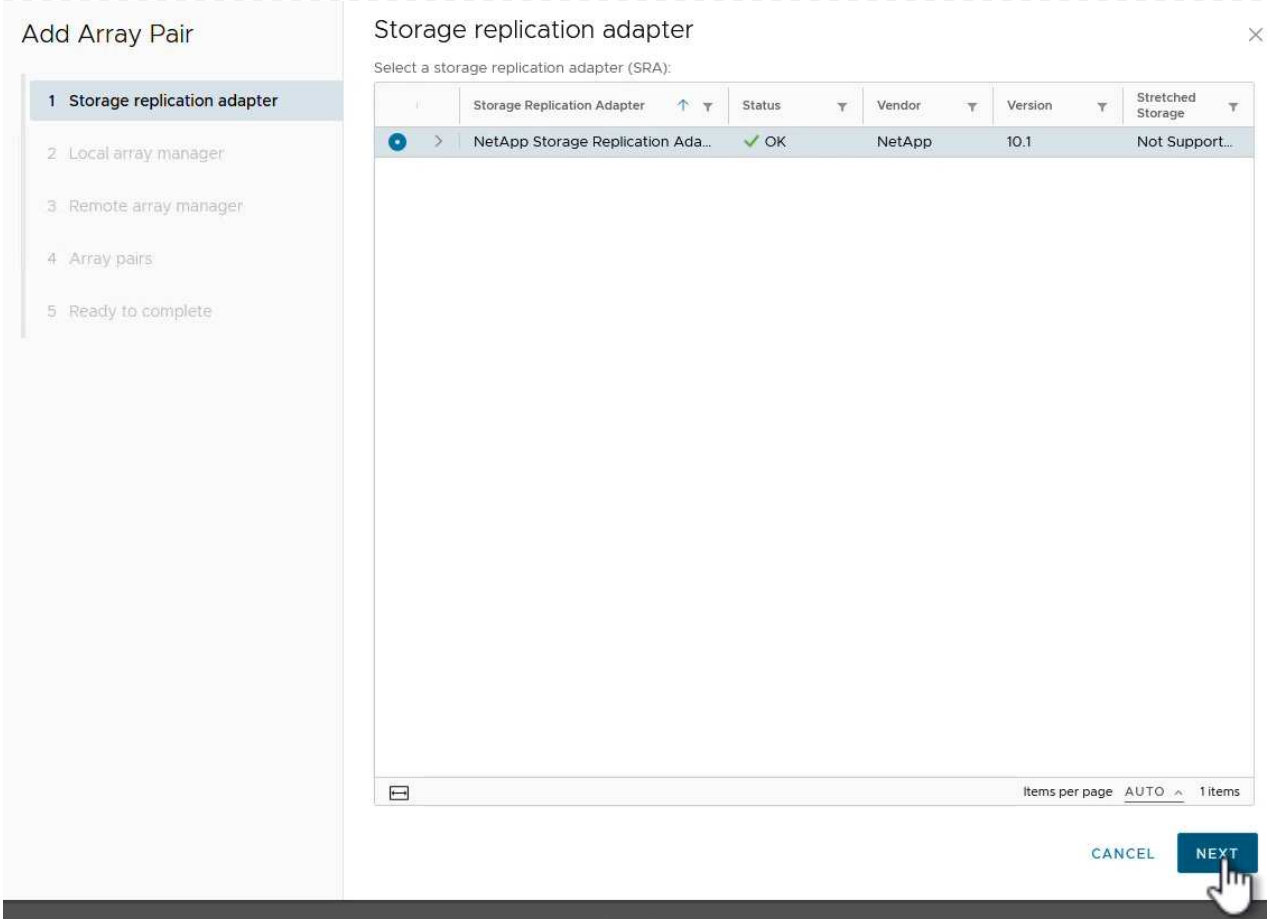
Aggiungere una coppia di array per SRM

Il passaggio seguente viene completato nell'interfaccia Site Recovery del sito primario.

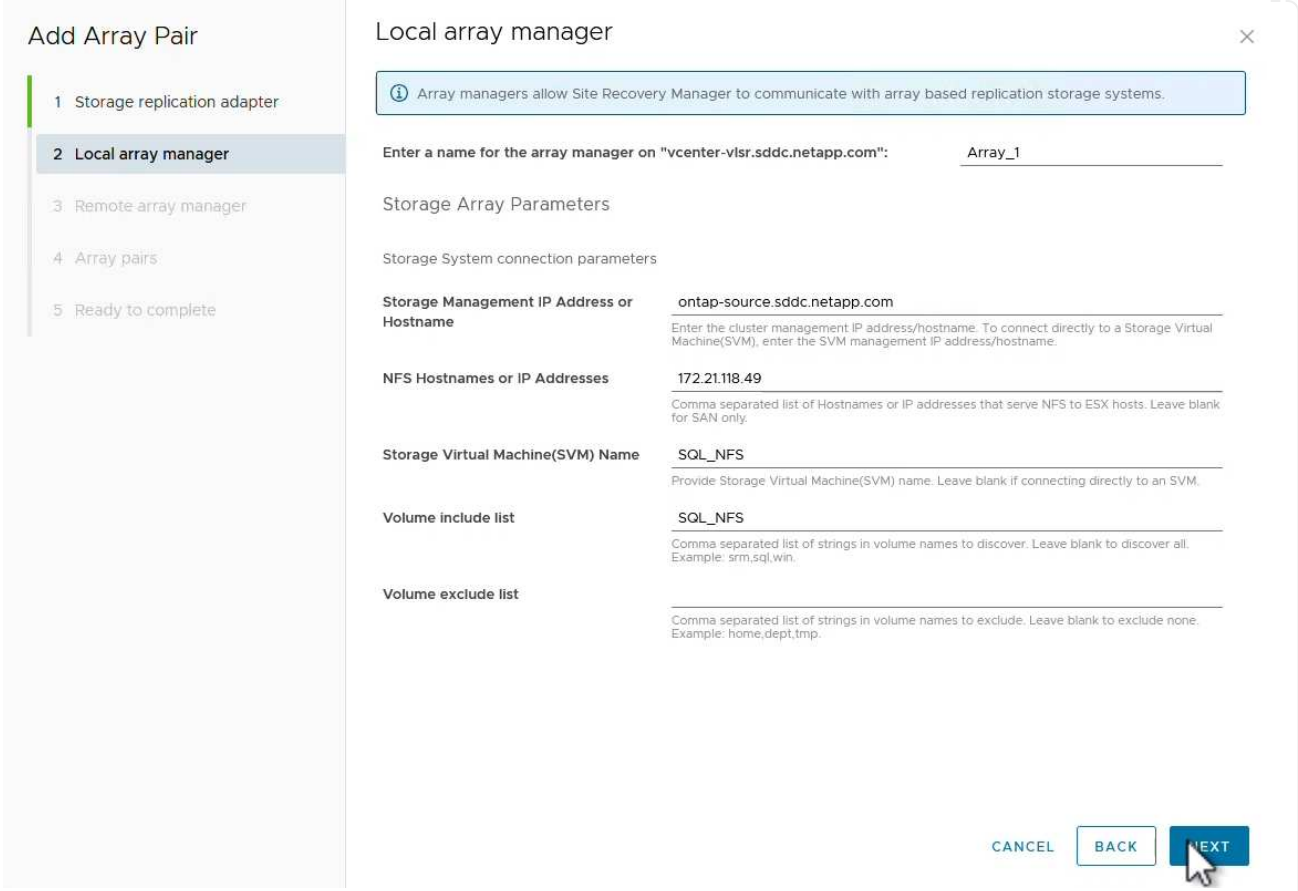
1. Nell'interfaccia Site Recovery (recupero sito), selezionare **Configure > Array Based Replication > Array Pairs** (Configura > replica basata su array > coppie di array*) nel menu a sinistra. Fare clic su **ADD** per iniziare.



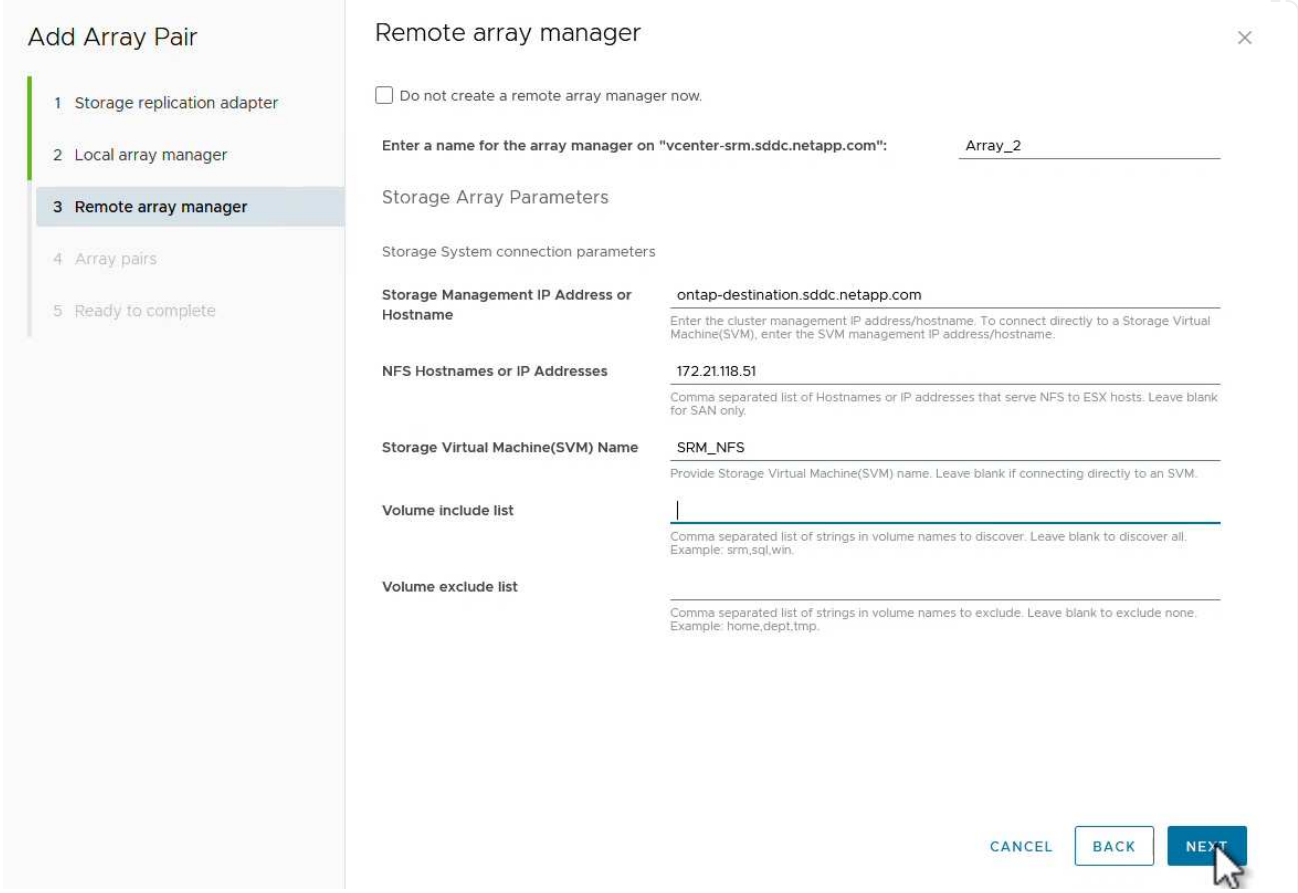
2. Nella pagina **scheda di replica archiviazione** della procedura guidata **Aggiungi coppia array**, verificare che l'adattatore SRA sia presente per il sito primario e fare clic su **Avanti** per continuare.



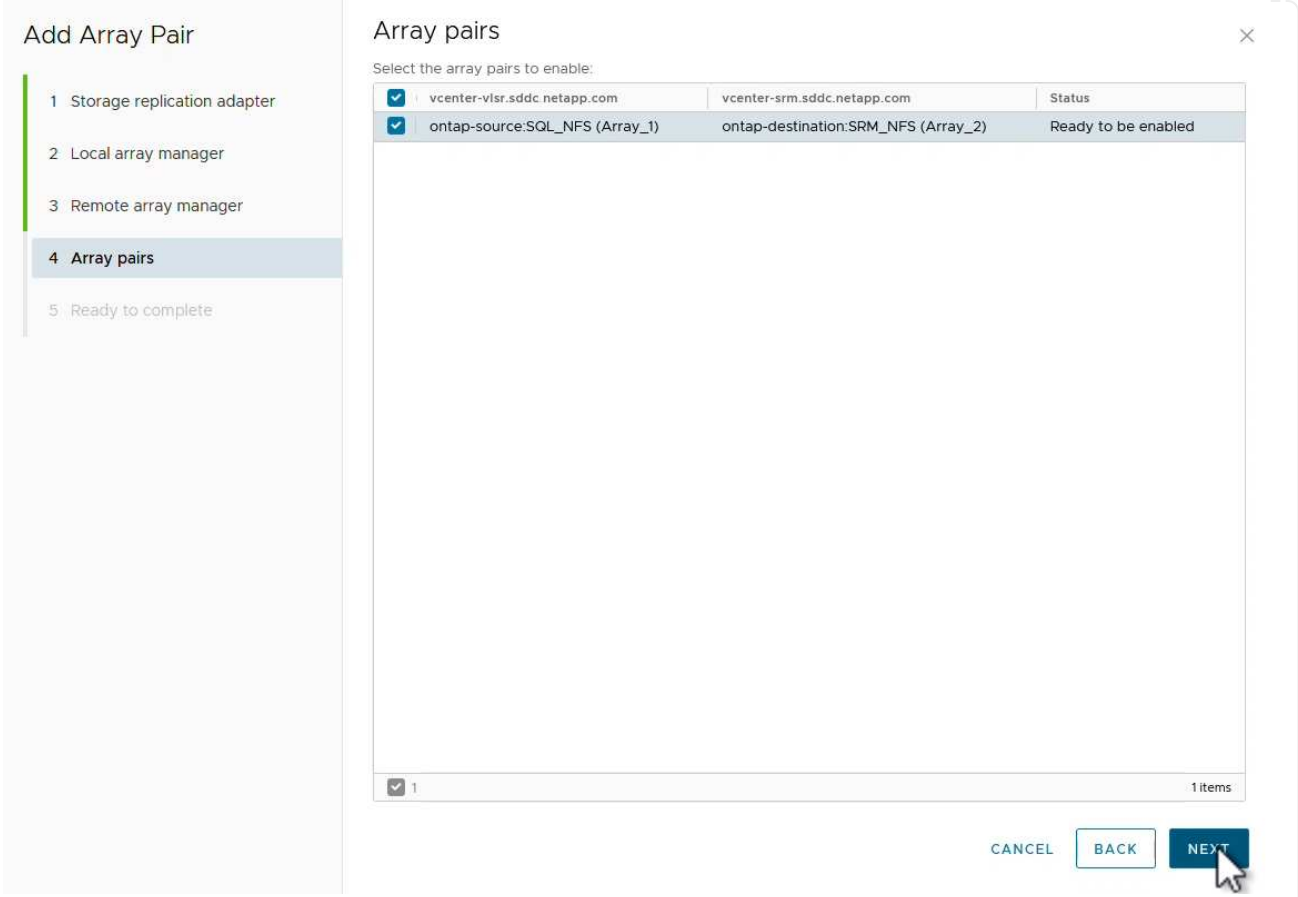
3. Nella pagina **Gestione array locale**, immettere un nome per l'array nel sito primario, l'FQDN del sistema storage, gli indirizzi IP della SVM che servono NFS e, facoltativamente, i nomi di volumi specifici da rilevare. Fare clic su **Avanti** per continuare.



4. Nell'applicazione **Gestione array remoto** inserire le stesse informazioni dell'ultimo passaggio per il sistema di archiviazione ONTAP nel sito secondario.



5. Nella pagina **Array Pairs**, selezionare le coppie di array da attivare e fare clic su **Next** per continuare.

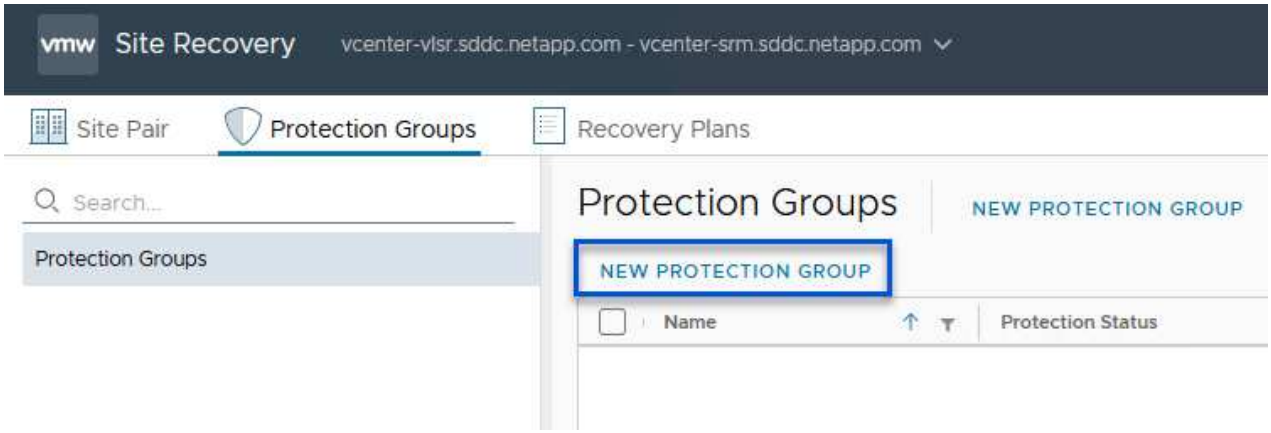


6. Rivedere le informazioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare la coppia di matrici.

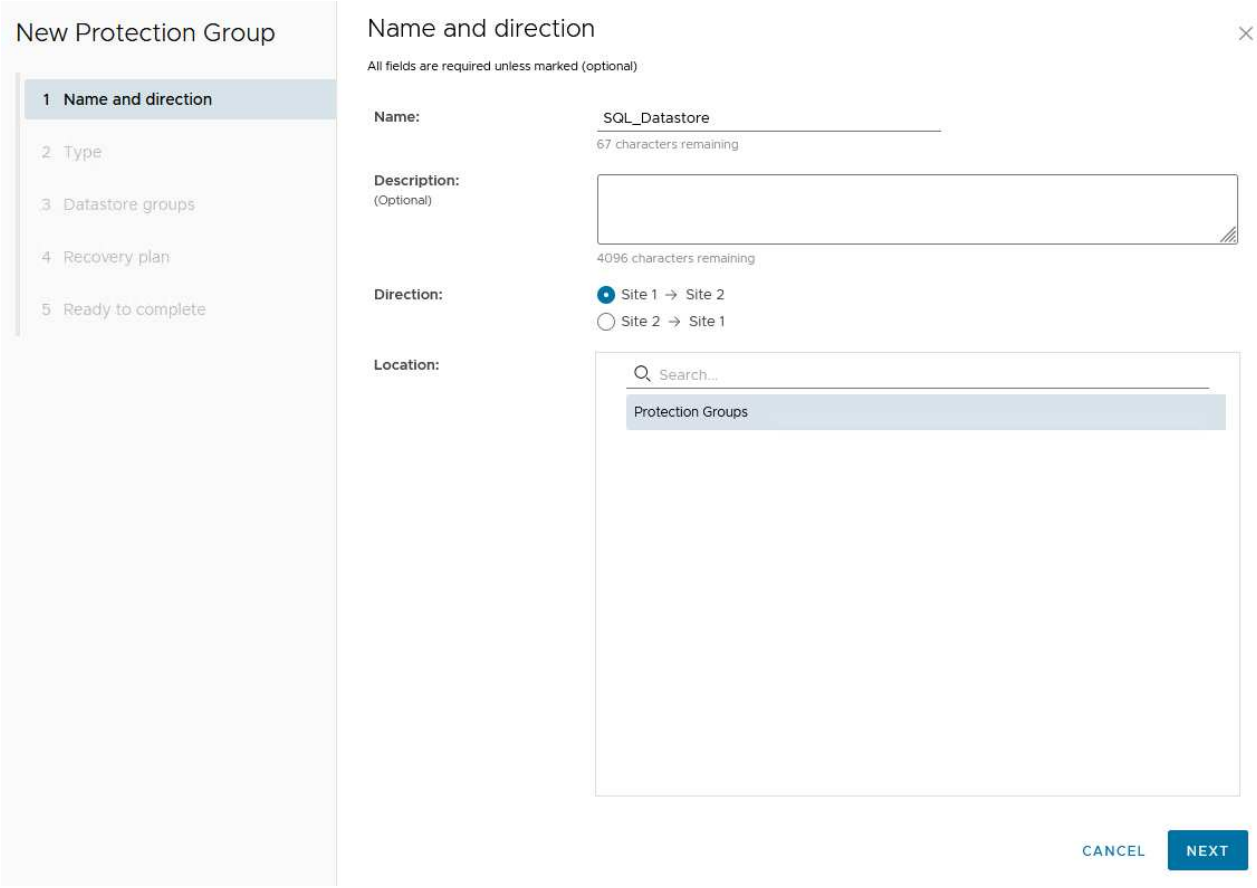
Configurare i gruppi di protezione per SRM

Il passaggio seguente viene completato nell'interfaccia Site Recovery del sito primario.

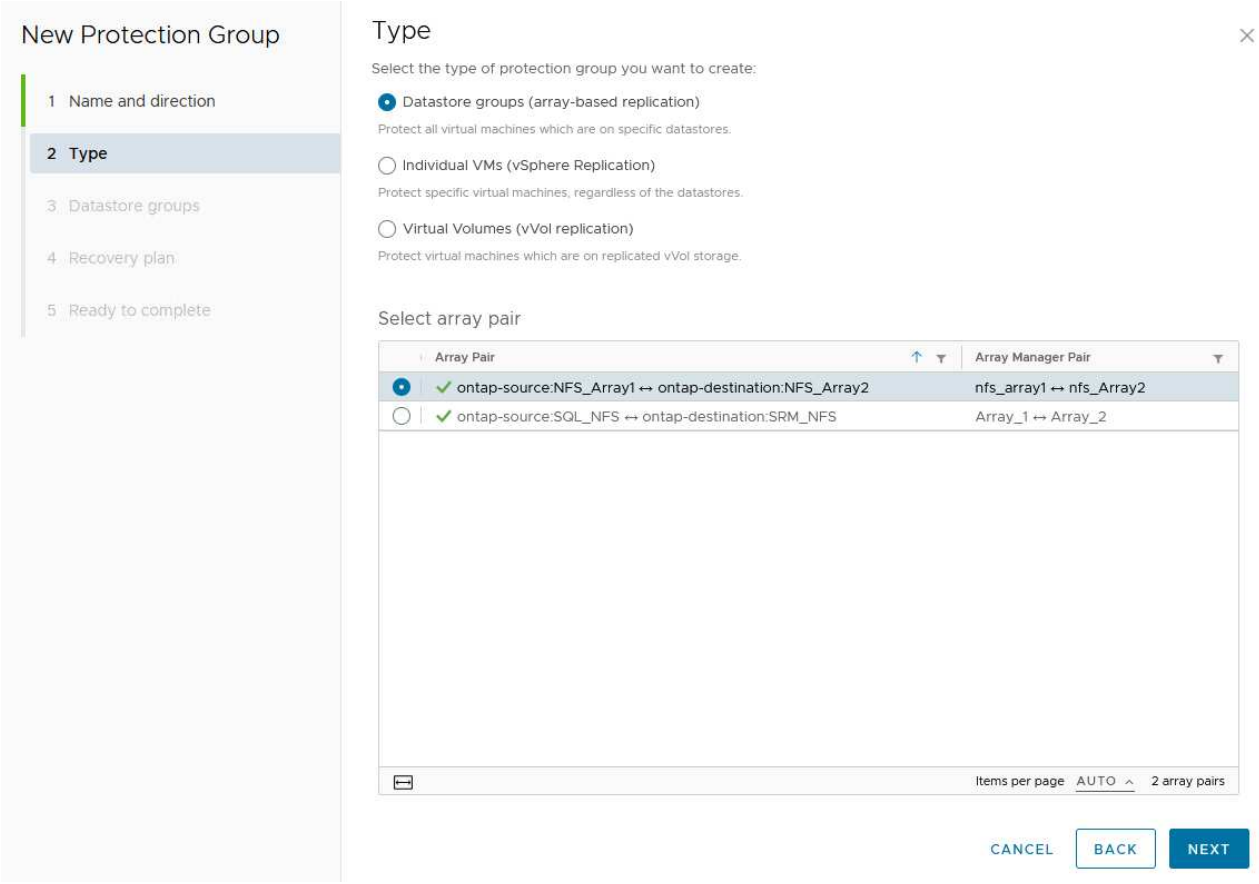
1. Nell'interfaccia Site Recovery fare clic sulla scheda **gruppi di protezione**, quindi su **nuovo gruppo di protezione** per iniziare.



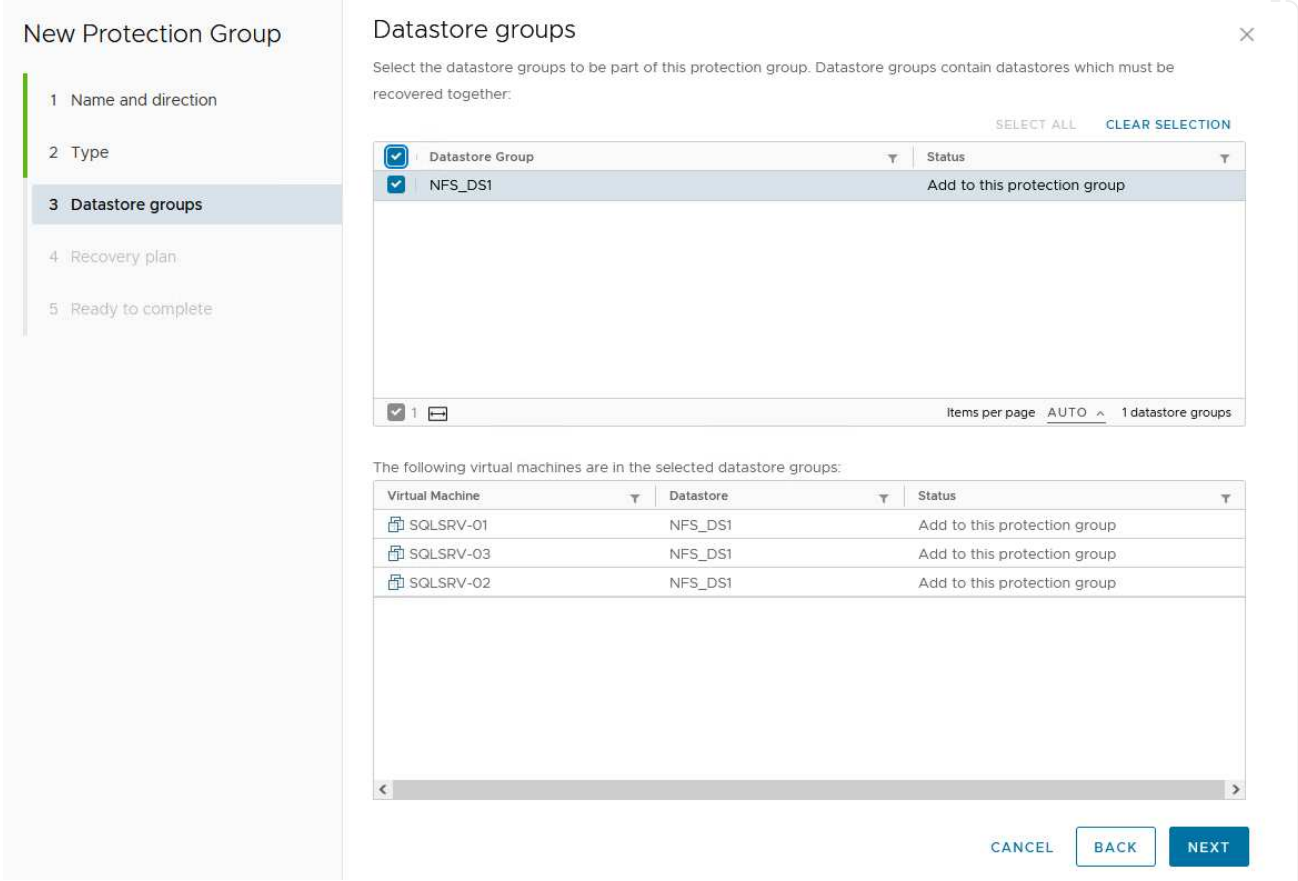
2. Nella pagina **Nome e direzione** della procedura guidata **nuovo gruppo di protezione**, fornire un nome per il gruppo e scegliere la direzione del sito per la protezione dei dati.



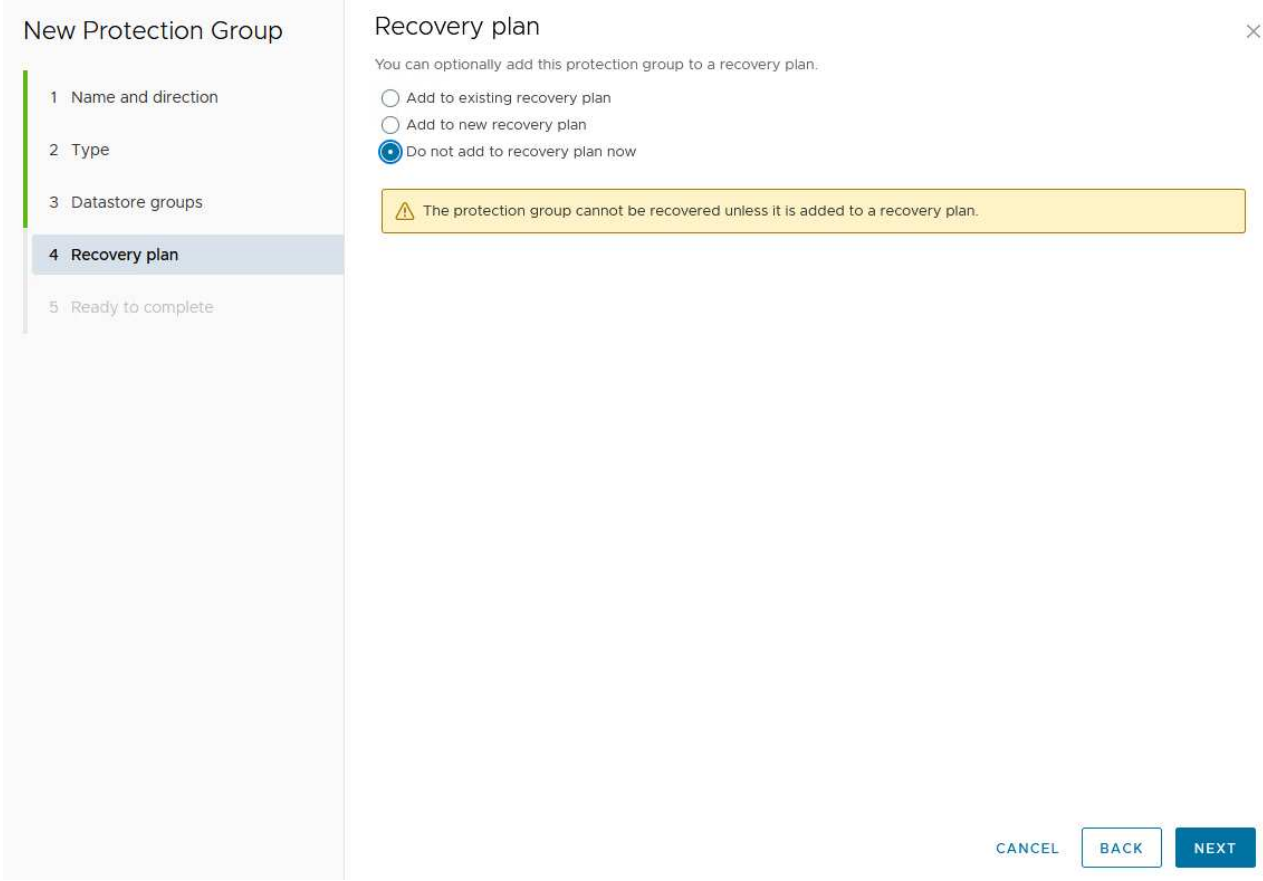
3. Nella pagina **Type** selezionare il tipo di gruppo di protezione (datastore, VM o vVol) e selezionare la coppia di array. Fare clic su **Avanti** per continuare.



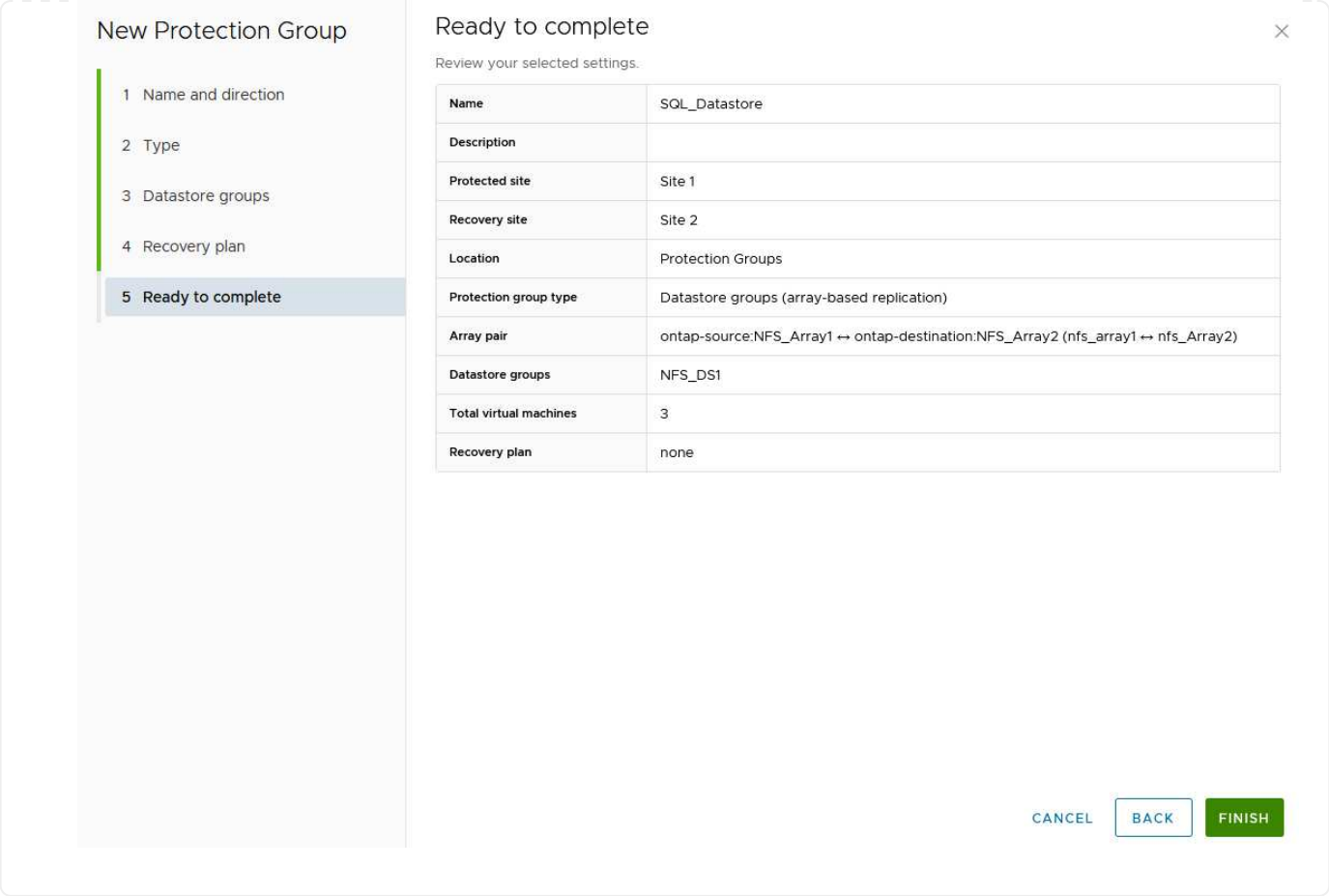
4. Nella pagina **Datastore groups**, selezionare gli archivi dati da includere nel gruppo di protezione. Le VM attualmente presenti nel datastore vengono visualizzate per ogni datastore selezionato. Fare clic su **Avanti** per continuare.



5. Nella pagina **piano di ripristino**, scegliere se aggiungere il gruppo protezione a un piano di ripristino. In questo caso, il piano di ripristino non è ancora stato creato, quindi è selezionato **non aggiungere al piano di ripristino**. Fare clic su **Avanti** per continuare.



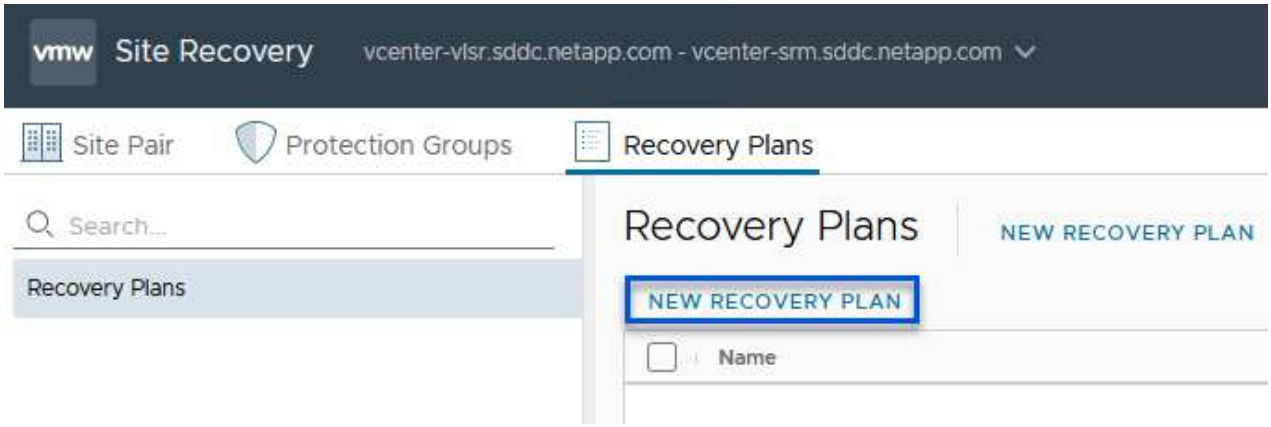
6. Nella pagina **Pronto per il completamento**, esaminare i nuovi parametri del gruppo di protezione e fare clic su **fine** per creare il gruppo.


New Protection Group
1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete
Ready to complete
Review your selected settings.
Name
SQL_Datastore
Description
Protected site
Site 1
Recovery site
Site 2
Location
Protection Groups
Protection group type
Datastore groups (array-based replication)
Array pair
ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_Array2)
Datastore groups
NFS_DS1
Total virtual machines
3
Recovery plan
none
CANCEL
BACK
FINISH

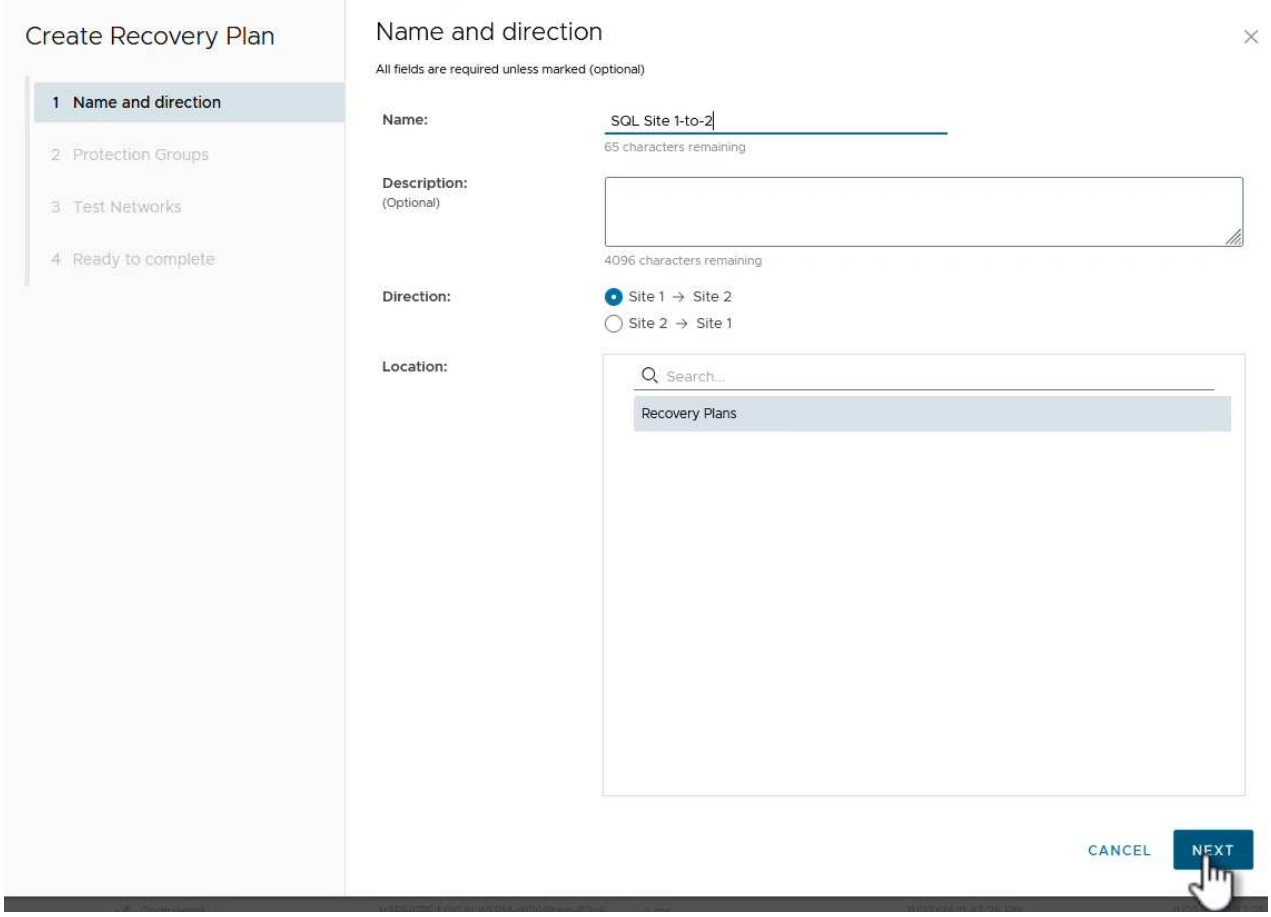
Configurare il piano di ripristino per SRM

Il passaggio seguente viene completato nell'interfaccia Site Recovery del sito primario.

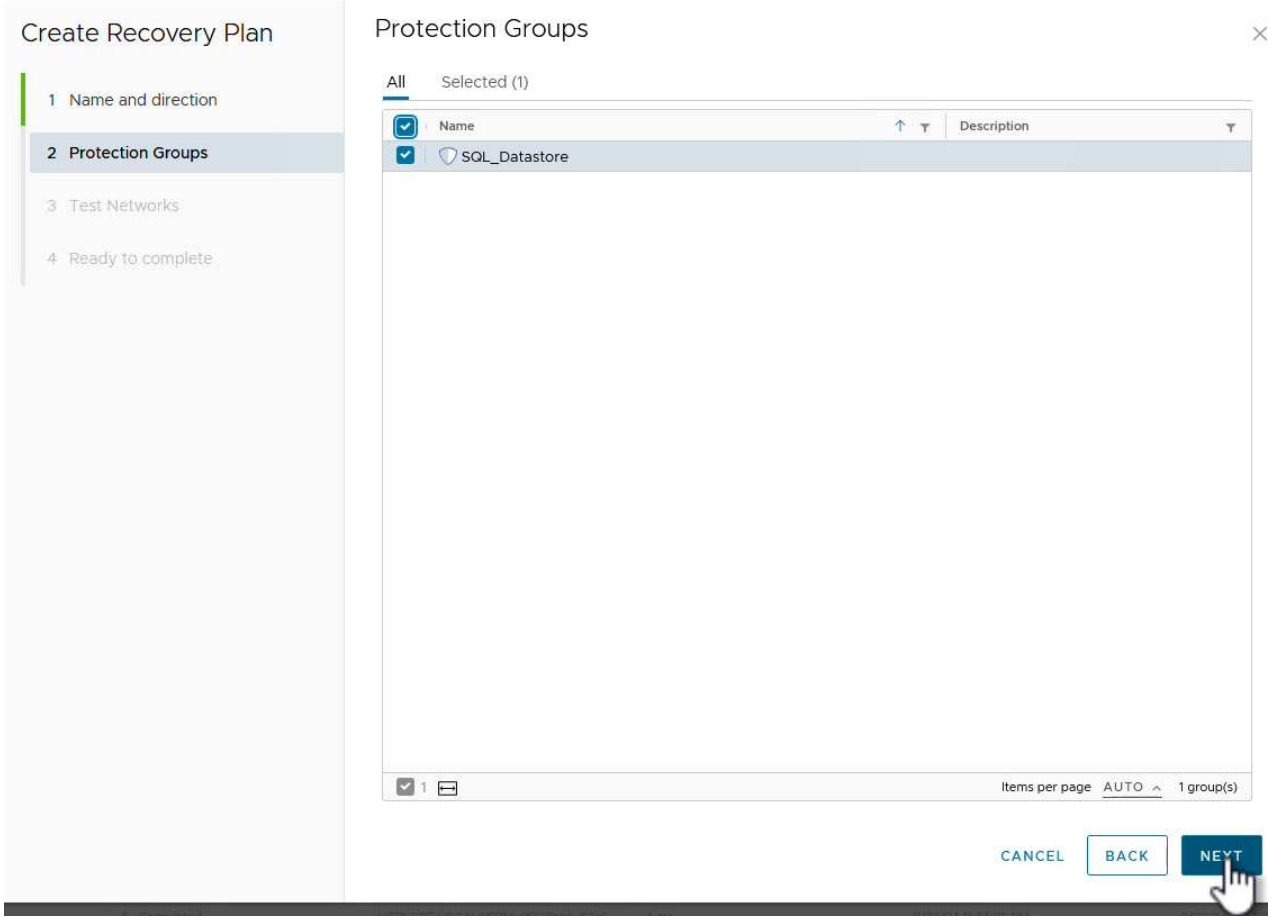
1. Nell'interfaccia Site Recovery fare clic sulla scheda **Recovery plan** (piano di ripristino), quindi su **New Recovery Plan** (nuovo piano di ripristino) per iniziare.



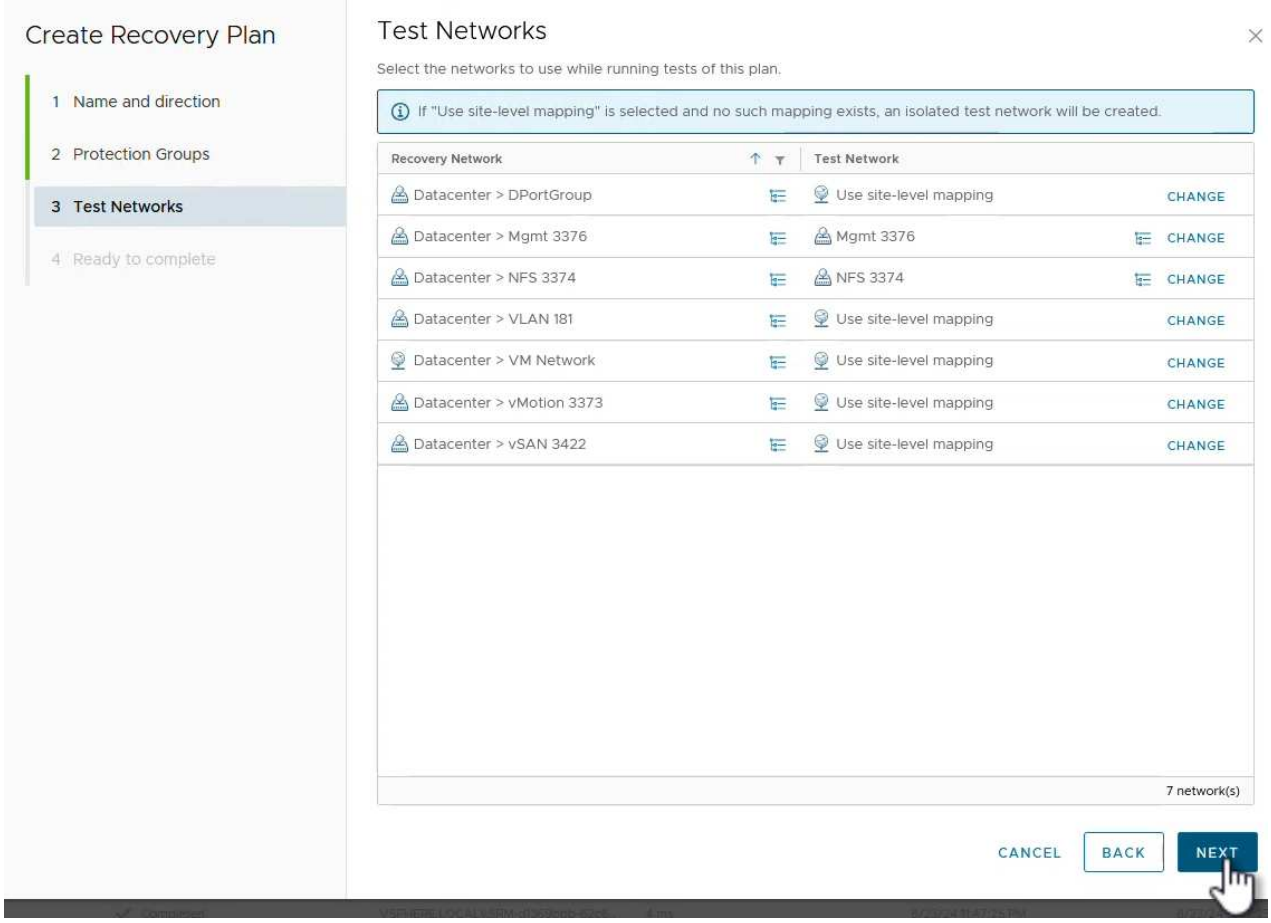
2. Nella pagina **Nome e direzione** della procedura guidata **Crea piano di ripristino**, fornire un nome per il piano di ripristino e scegliere la direzione tra i siti di origine e di destinazione. Fare clic su **Avanti** per continuare.



3. Nella pagina **gruppi di protezione**, selezionare i gruppi di protezione creati in precedenza da includere nel piano di ripristino. Fare clic su **Avanti** per continuare.



4. Su **Test Networks** configurare reti specifiche che verranno utilizzate durante il test del piano. Se non esiste alcuna mappatura o se non è selezionata alcuna rete, verrà creata una rete di prova isolata. Fare clic su **Avanti** per continuare.



5. Nella pagina **Pronto per il completamento**, esaminare i parametri scelti e fare clic su **fine** per creare il piano di ripristino.

Operazioni di disaster recovery con SRM

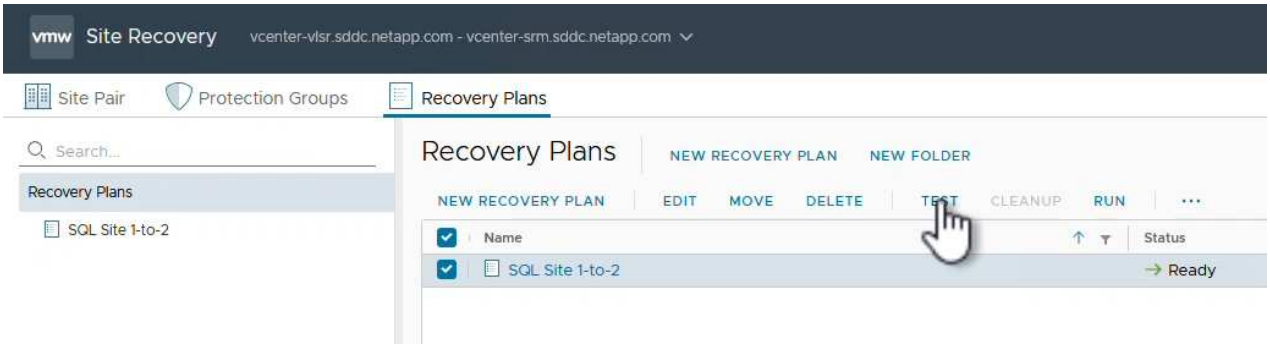
In questa sezione verranno trattate varie funzioni dell'utilizzo del disaster recovery con SRM, tra cui il test del failover, l'esecuzione del failover, la riprotezione e il failback.

Per "Best practice operative" ulteriori informazioni sull'utilizzo dello storage ONTAP con operazioni di disaster recovery SRM, fare riferimento a.

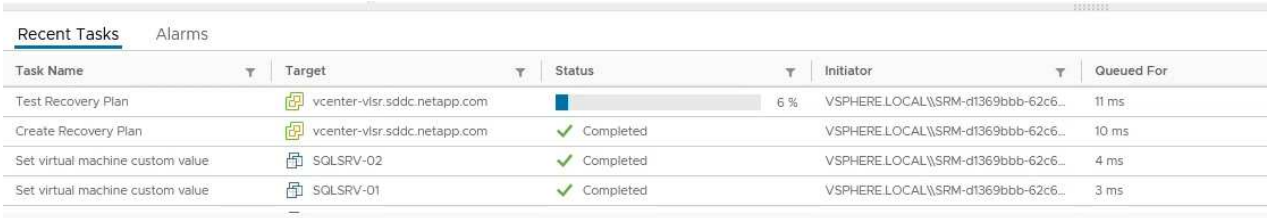
Verifica del failover con SRM

Il passaggio seguente viene completato nell'interfaccia Site Recovery.

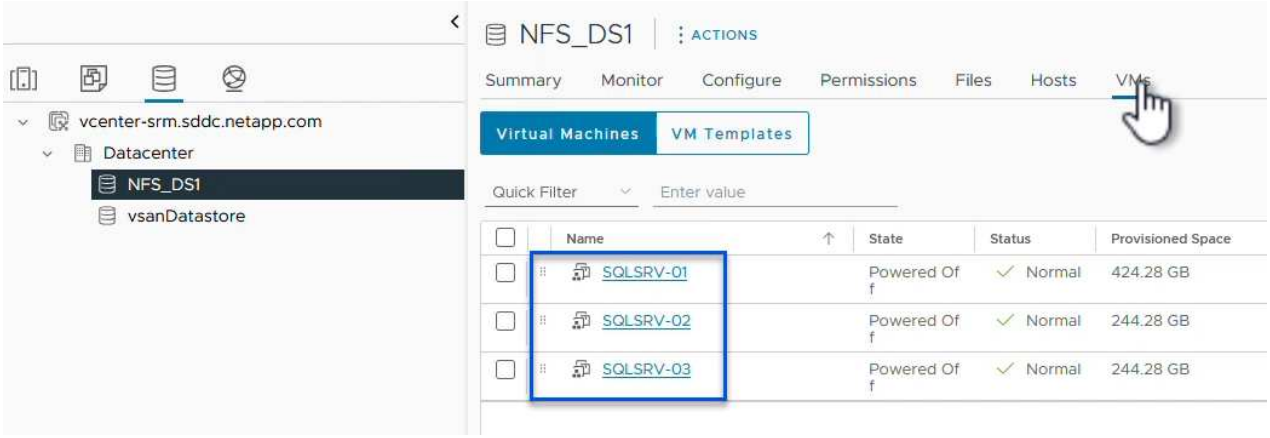
1. Nell'interfaccia Site Recovery fare clic sulla scheda **Recovery plan** (piano di ripristino), quindi selezionare un piano di ripristino. Fare clic sul pulsante **Test** per avviare il test di failover sul sito secondario.



2. È possibile visualizzare l'avanzamento del test dal riquadro attività di Site Recovery e dal riquadro attività di vCenter.

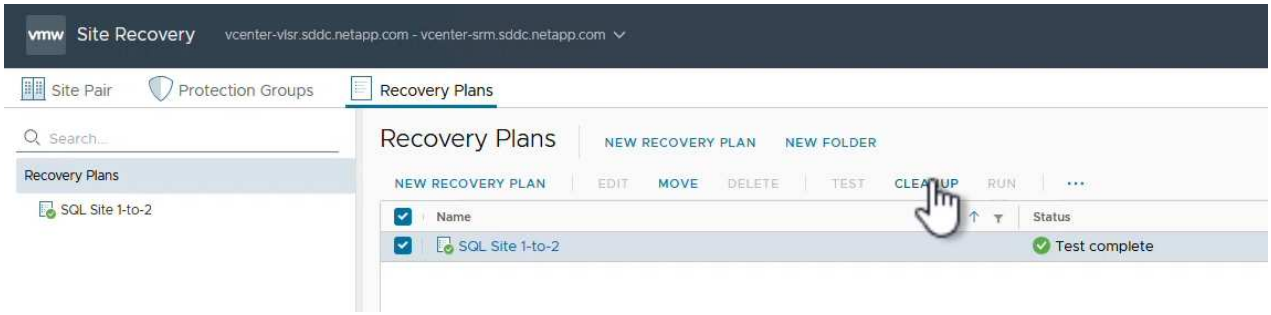


3. SRM invia comandi tramite SRA al sistema di storage ONTAP secondario. Viene creato un FlexClone dello snapshot più recente e montato nel cluster vSphere secondario. Il datastore appena montato può essere visualizzato nell'inventario dello storage.



4. Una volta completato il test, fare clic su **Cleanup** per disinstallare il datastore e tornare all'ambiente

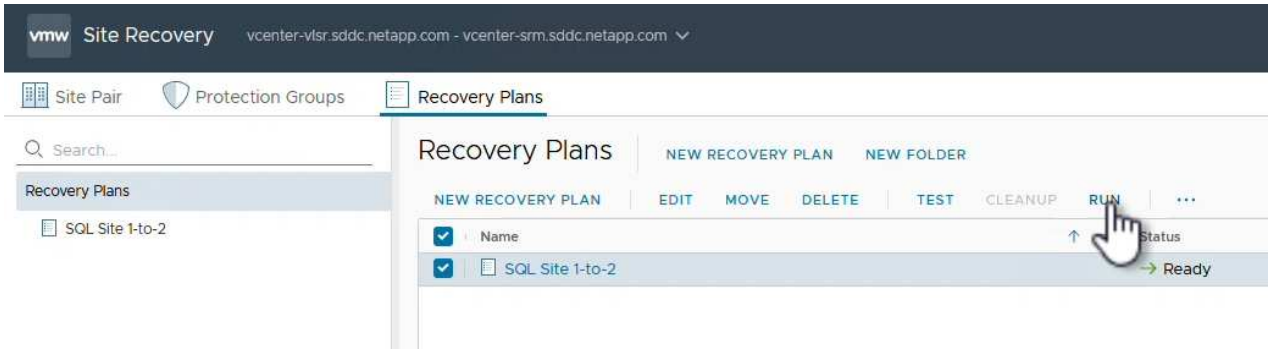
originale.



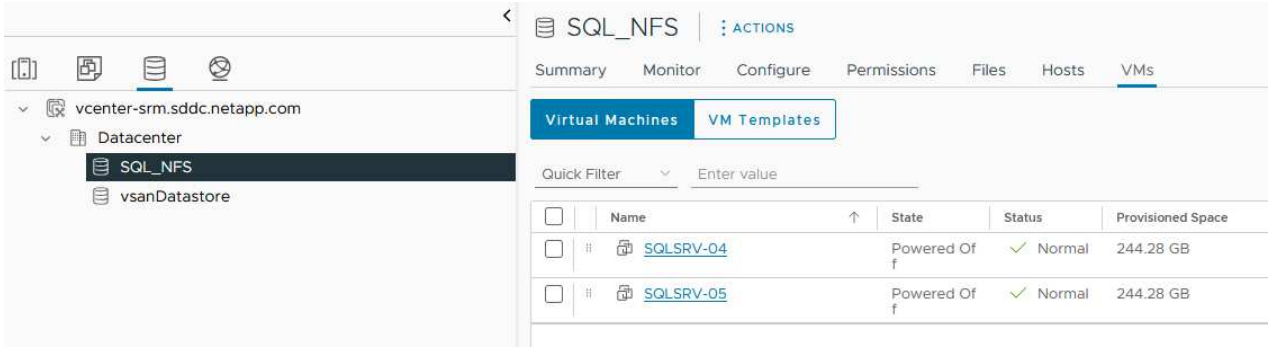
Esecuzione di un piano di ripristino con SRM

Eseguire un ripristino completo e il failover sul sito secondario.

1. Nell'interfaccia Site Recovery fare clic sulla scheda **Recovery plan** (piano di ripristino), quindi selezionare un piano di ripristino. Fare clic sul pulsante **Esegui** per avviare il failover al sito secondario.



2. Una volta completato il failover, potrai vedere il datastore montato e le macchine virtuali registrate nel sito secondario.



Una volta completato il failover, in SRM sono possibili funzioni aggiuntive.

Reprotezione: Una volta completato il processo di ripristino, il sito di ripristino precedentemente designato assume il ruolo del nuovo sito di produzione. Tuttavia, è importante notare che la replica di SnapMirror viene interrotta durante l'operazione di ripristino, lasciando il nuovo sito di produzione vulnerabile a futuri disastri. Per

garantire una protezione continua, si consiglia di stabilire una nuova protezione per il nuovo sito di produzione replicandolo in un altro sito. Nei casi in cui il sito di produzione originale rimane operativo, l'amministratore VMware può riutilizzarlo come nuovo sito di ripristino, invertendo effettivamente la direzione della protezione. È fondamentale sottolineare che la ri-protezione è possibile solo in caso di guasti non catastrofici, che richiedono l'eventuale recuperabilità dei server vCenter originali, dei server ESXi, dei server SRM e dei rispettivi database. Se questi componenti non sono disponibili, diventa necessaria la creazione di un nuovo gruppo di protezione e di un nuovo piano di ripristino.

Failback: Un'operazione di failback è un failover inverso, che restituisce le operazioni al sito originale. È fondamentale assicurarsi che il sito originale abbia riacquistato la funzionalità prima di avviare il processo di failback. Per garantire un failback regolare, si consiglia di eseguire un failover di test dopo aver completato il processo di protezione e prima di eseguire il failback finale. Questa pratica funge da fase di verifica, confermando che i sistemi del sito originale sono pienamente in grado di gestire l'operazione. Seguendo questo approccio, è possibile ridurre al minimo i rischi e garantire una transizione più affidabile all'ambiente di produzione originale.

Ulteriori informazioni

Per la documentazione NetApp sull'utilizzo dello storage ONTAP con VMware SRM, fare riferimento a. "VMware Site Recovery Manager con ONTAP"

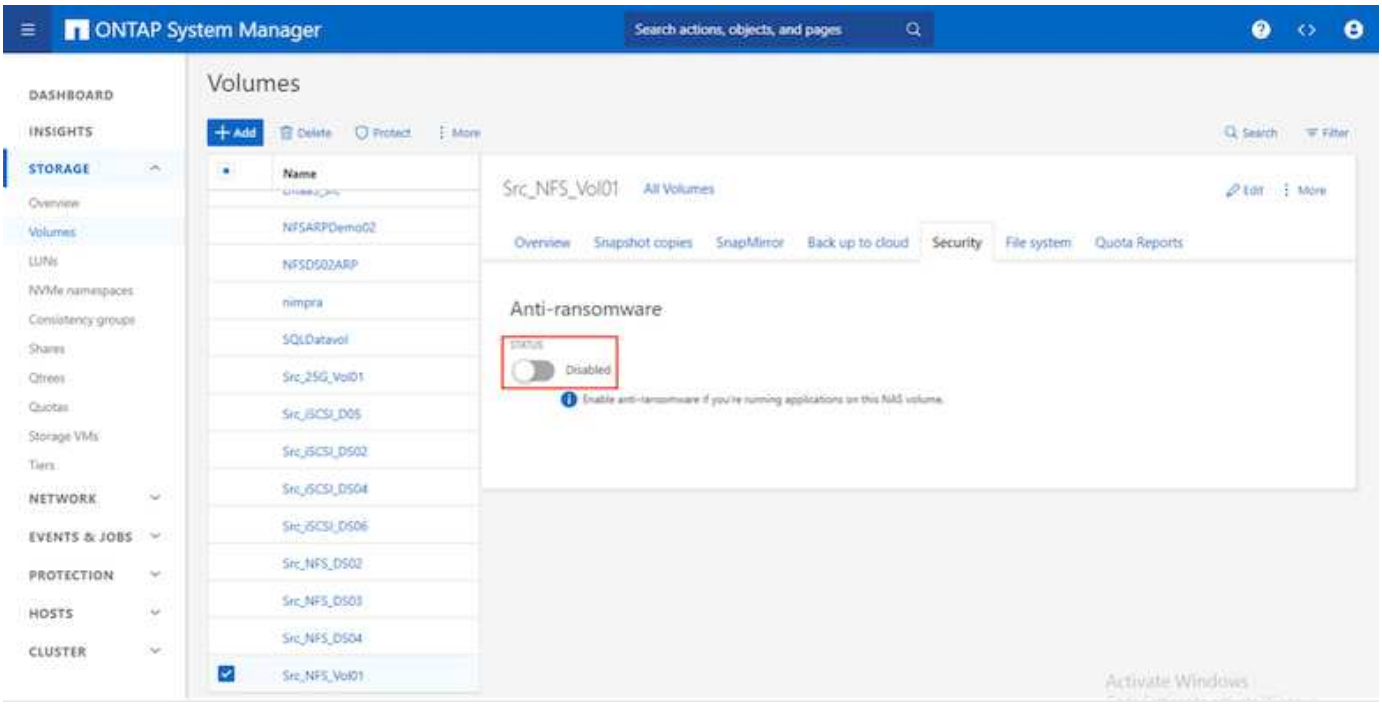
Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Protezione autonoma dal ransomware per lo storage NFS

Rilevare il ransomware il prima possibile è fondamentale per prevenirne la diffusione ed evitare costosi downtime. Un'efficace strategia di rilevamento ransomware deve incorporare vari livelli di protezione a livello di host ESXi e VM guest. Mentre sono implementate più misure di sicurezza per creare una difesa completa contro gli attacchi ransomware, ONTAP permette di aggiungere più livelli di protezione all'approccio di difesa generale. Per citare alcune funzionalità, inizia con Snapshot, protezione autonoma da ransomware, snapshot a prova di manomissione e così via.

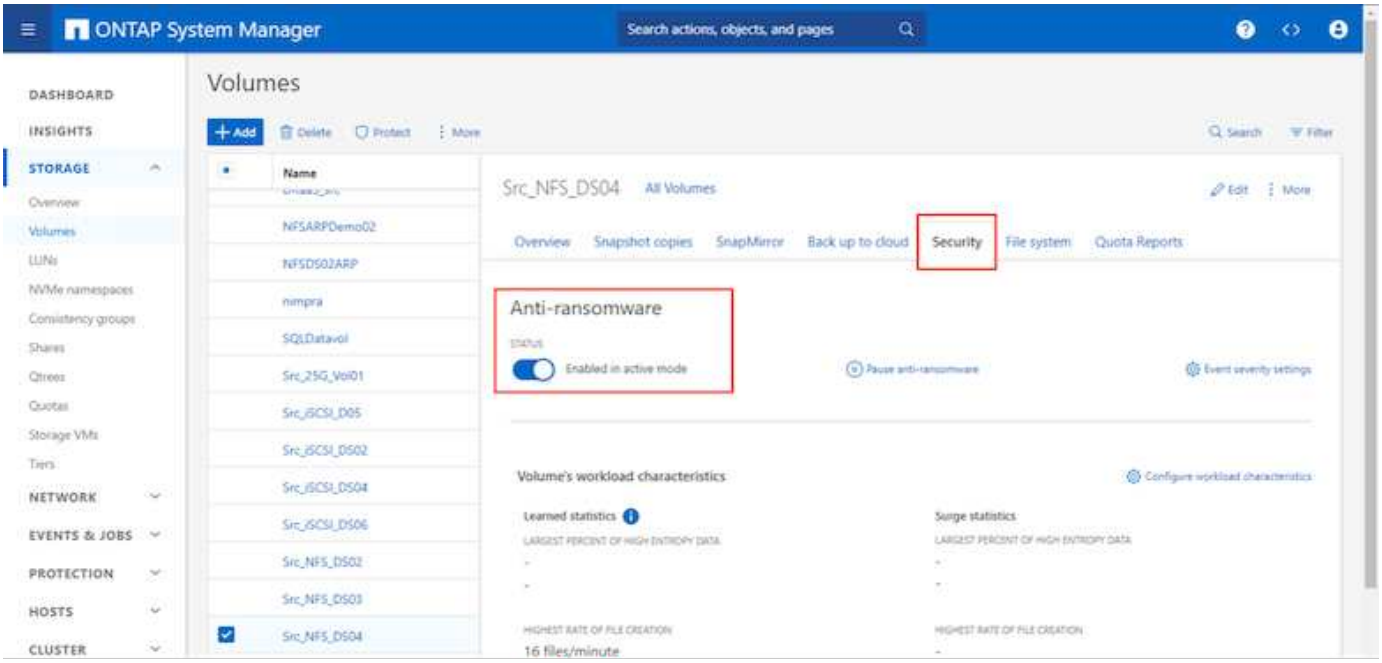
Analizziamo il modo in cui le funzionalità sopra menzionate si integrano con VMware per proteggere e ripristinare i dati contro il ransomware. Per proteggere vSphere e le macchine virtuali guest dagli attacchi, è essenziale adottare diverse misure, tra cui la segmentazione, l'utilizzo di EDR/XDR/SIEM per gli endpoint e l'installazione degli aggiornamenti per la protezione e il rispetto delle linee guida appropriate per la protezione avanzata. Ogni macchina virtuale residente in un datastore ospita anche un sistema operativo standard. Garantisci l'installazione e l'aggiornamento regolare delle suite di prodotti anti-malware dei server aziendali, un componente essenziale della strategia di protezione dal ransomware su più livelli. Insieme a questo, abilita la protezione autonoma dal ransomware (ARP) sul volume NFS che alimenta il datastore. ARP sfrutta ML onbox integrato che analizza l'attività dei carichi di lavoro dei volumi più l'entropia dei dati per rilevare automaticamente il ransomware. ARP è configurabile tramite l'interfaccia di gestione integrata di ONTAP o System Manager ed è abilitato per ogni volume.



Con il nuovo NetApp ARP/ai, che è attualmente in anteprima tecnologica, non c'è bisogno di una modalità di apprendimento. Invece, può passare direttamente alla modalità attiva con la sua funzionalità di rilevamento ransomware basata su ai.

Con ONTAP One, tutti questi set di funzioni sono completamente gratuiti. Accedi alla solida suite di prodotti NetApp per la protezione dei dati, la sicurezza e tutte le funzioni offerte da ONTAP senza doverti preoccupare delle barriere delle licenze.

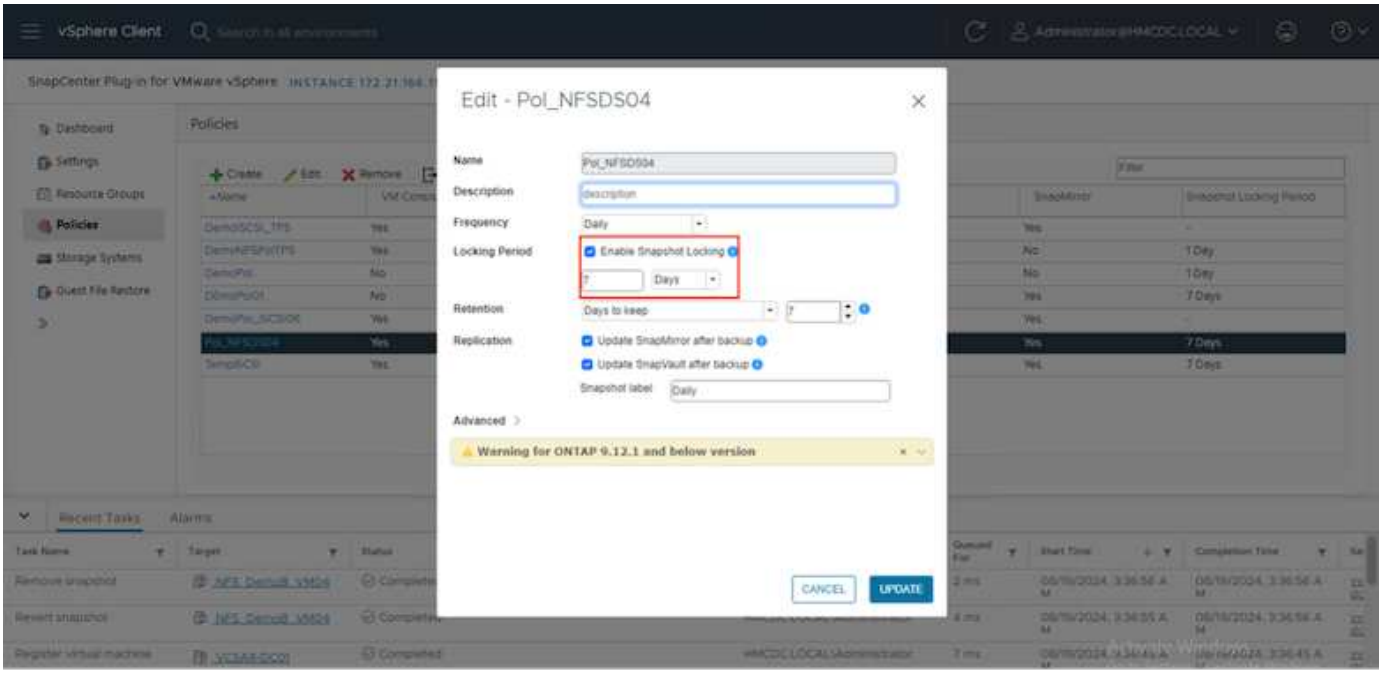
Una volta in modalità attiva, inizia a cercare l'attività anomala del volume che potrebbe essere un ransomware. Se viene rilevata un'attività anomala, viene immediatamente creata una copia Snapshot automatica che fornisce un punto di ripristino il più vicino possibile all'infezione dei file. ARP è in grado di rilevare le modifiche nelle estensioni di file specifiche della VM su un volume NFS situato all'esterno della VM quando viene aggiunta una nuova estensione al volume crittografato o quando viene modificata l'estensione di un file.



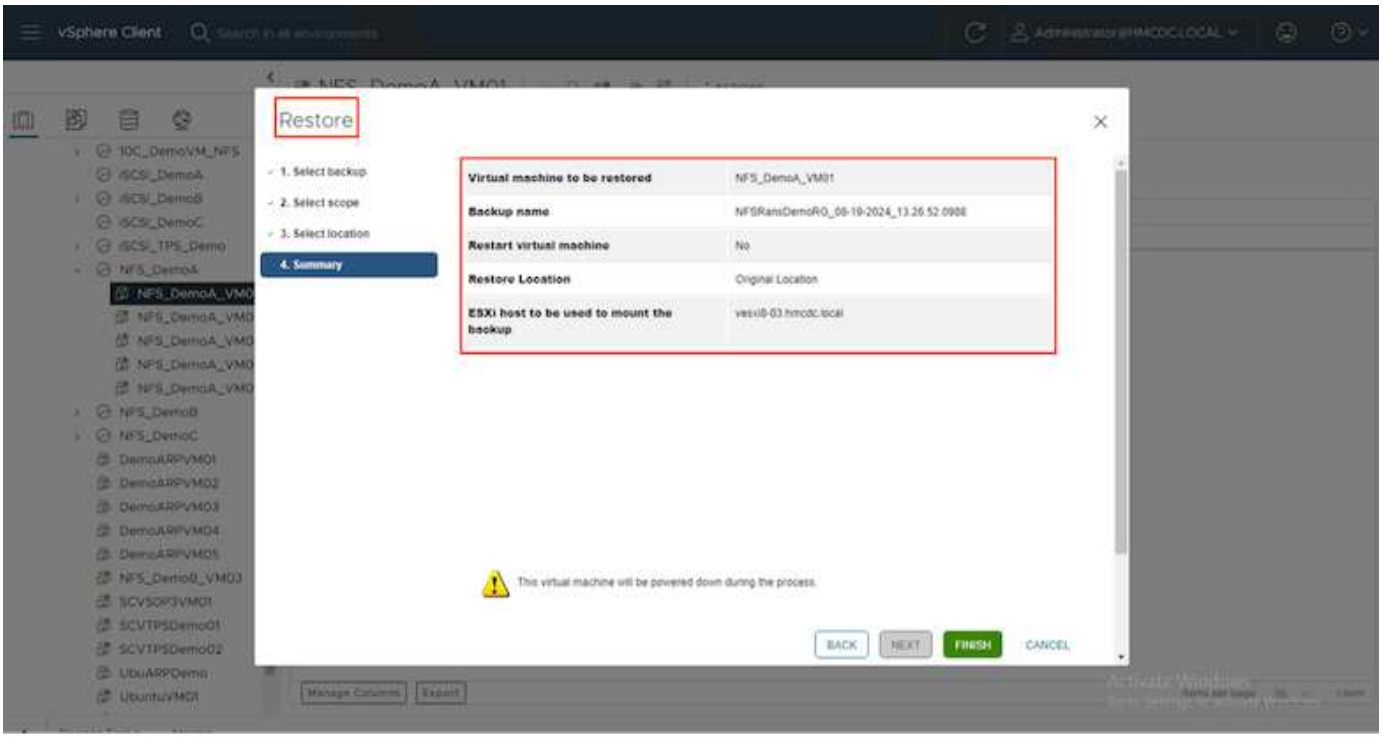
Se un attacco ransomware riguarda la macchina virtuale (VM) e altera i file all'interno della macchina virtuale senza apportare modifiche all'esterno della macchina virtuale, l'Advanced ransomware Protection (ARP) rileverà comunque la minaccia se l'entropia predefinita della macchina virtuale è bassa, ad esempio per i tipi di file .txt, .docx o .mp4. Anche se ARP crea uno snapshot di protezione in questo scenario, non genera un avviso di minaccia perché le estensioni dei file al di fuori della VM non sono state manomesse. In tali scenari, gli strati iniziali di difesa identificherebbero l'anomalia, tuttavia ARP aiuta a creare uno snapshot basato sull'entropia.

Per informazioni dettagliate, fare riferimento alla sezione "ARP e macchine virtuali" nel "ARP usecases e considerazioni".

Passando da file a dati di backup, gli attacchi ransomware puntano sempre più ai backup e ai punti di recovery delle snapshot, cercando di eliminarli prima di iniziare a crittografare i file. Tuttavia, con ONTAP, questo può essere impedito creando snapshot antimanomissione su sistemi primari o secondari con "Blocco copia NetApp Snapshot™".



Questi Snapshot non possono essere eliminati o modificati da autori di attacchi ransomware o amministratori fuori controllo, in modo che siano disponibili anche in seguito a un attacco. In caso di impatto sul datastore o su macchine virtuali specifiche, SnapCenter può ripristinare i dati delle macchine virtuali in pochi secondi, riducendo al minimo i downtime dell'organizzazione.



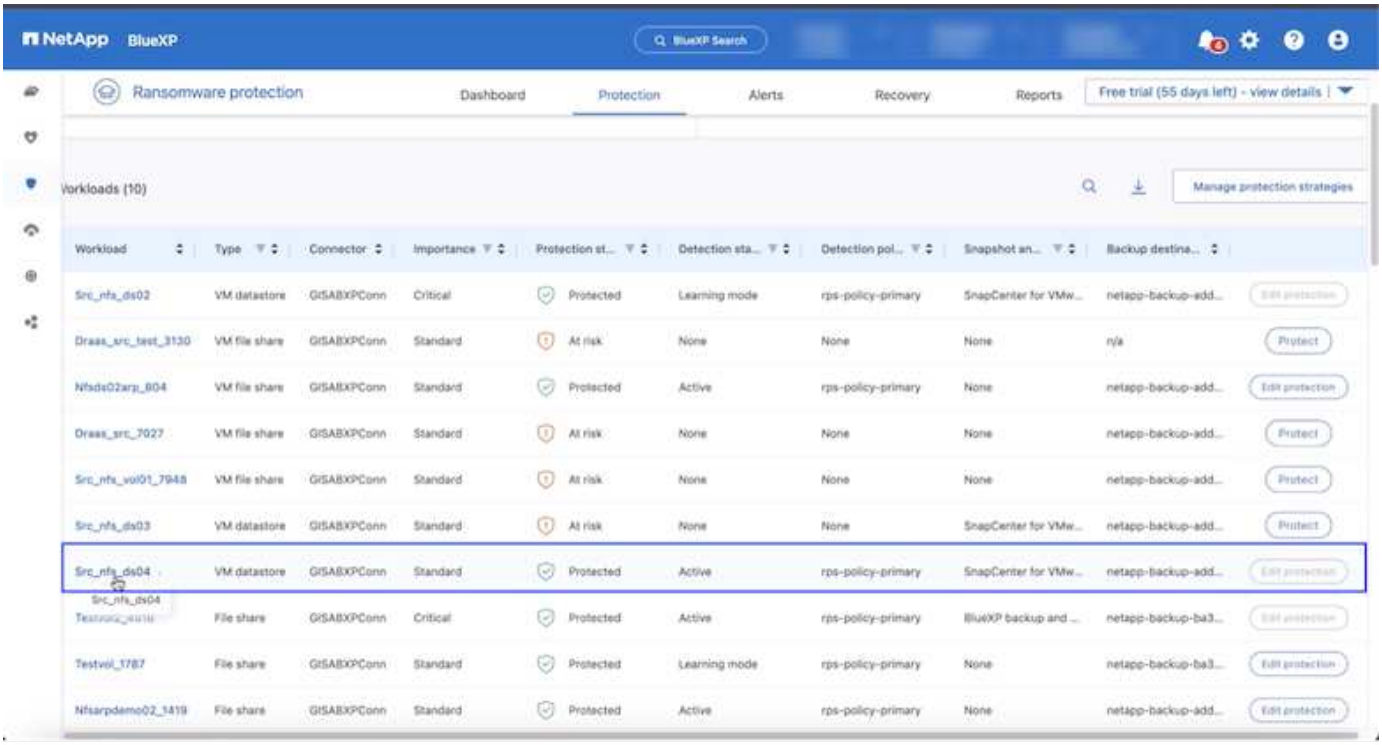
Quanto sopra dimostra in che modo lo storage ONTAP aggiunge un ulteriore livello alle tecniche esistenti, migliorando la predisposizione per il futuro dell'ambiente.

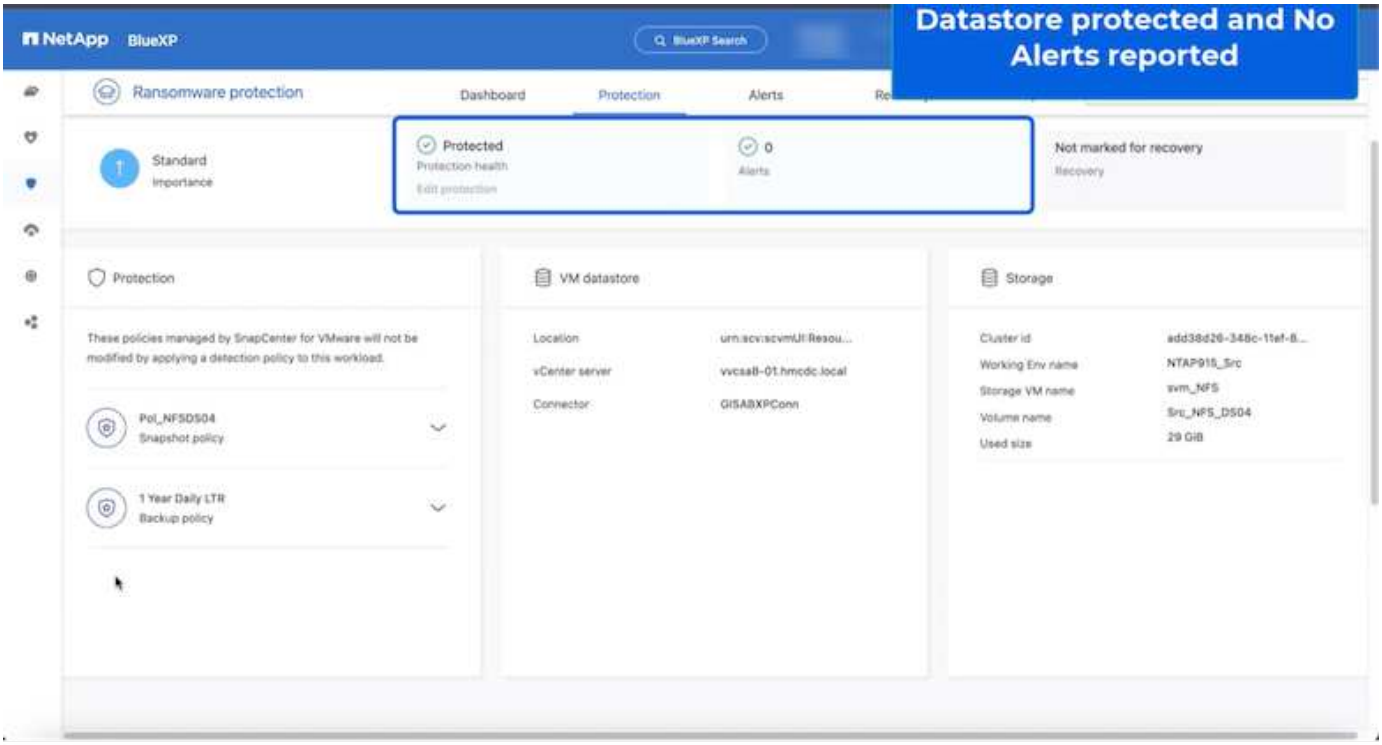
Per ulteriori informazioni, visualizzare le istruzioni per "Soluzioni NetApp per il ransomware".

Ora, se tutti questi elementi devono essere orchestrati e integrati con strumenti SIEM, è possibile utilizzare il servizio OFFTAP come la protezione ransomware BlueXP . È un servizio ideato per proteggere i dati da

ransomware. Questo servizio offre protezione per i workload basati sulle applicazioni come Oracle, MySQL, datastore VM e file share sullo storage NFS on-premise.

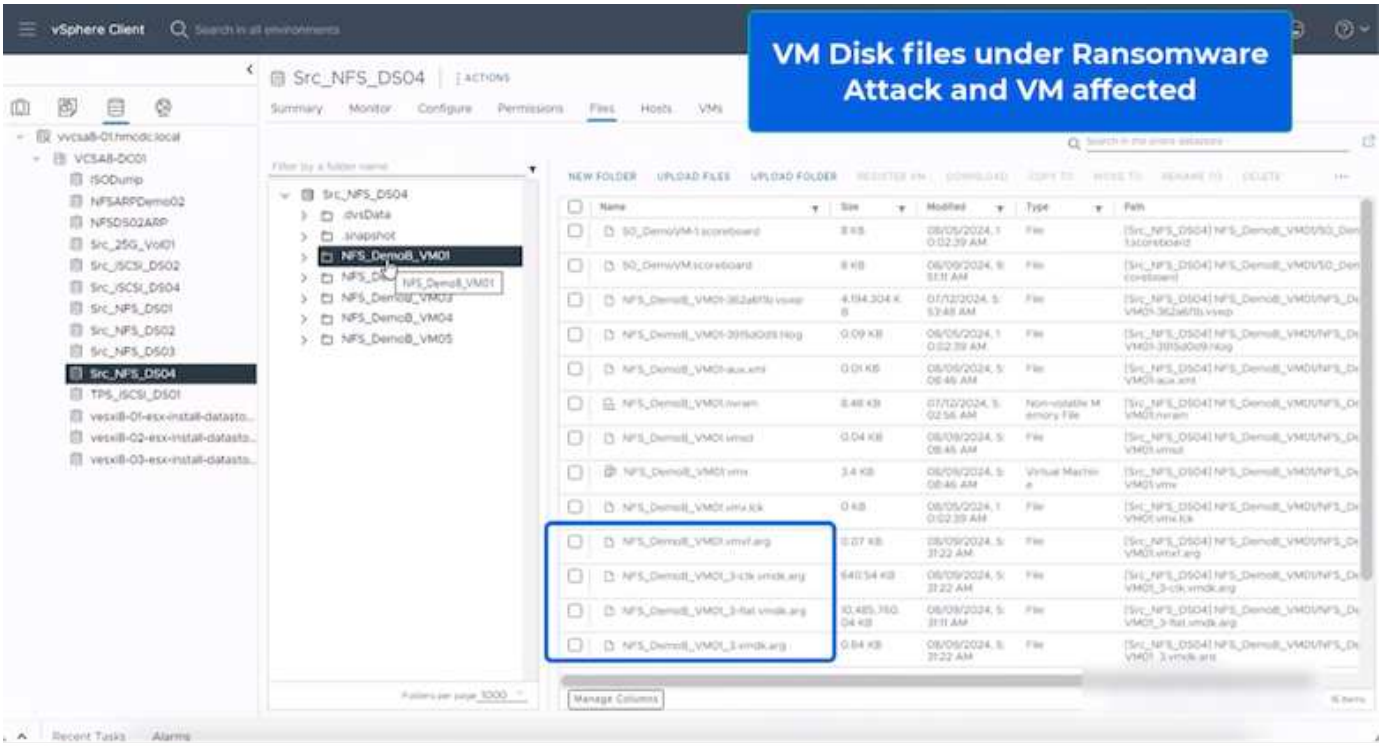
In questo esempio, il datastore NFS "Src_NFS_DS04" è protetto tramite la protezione ransomware BlueXP .



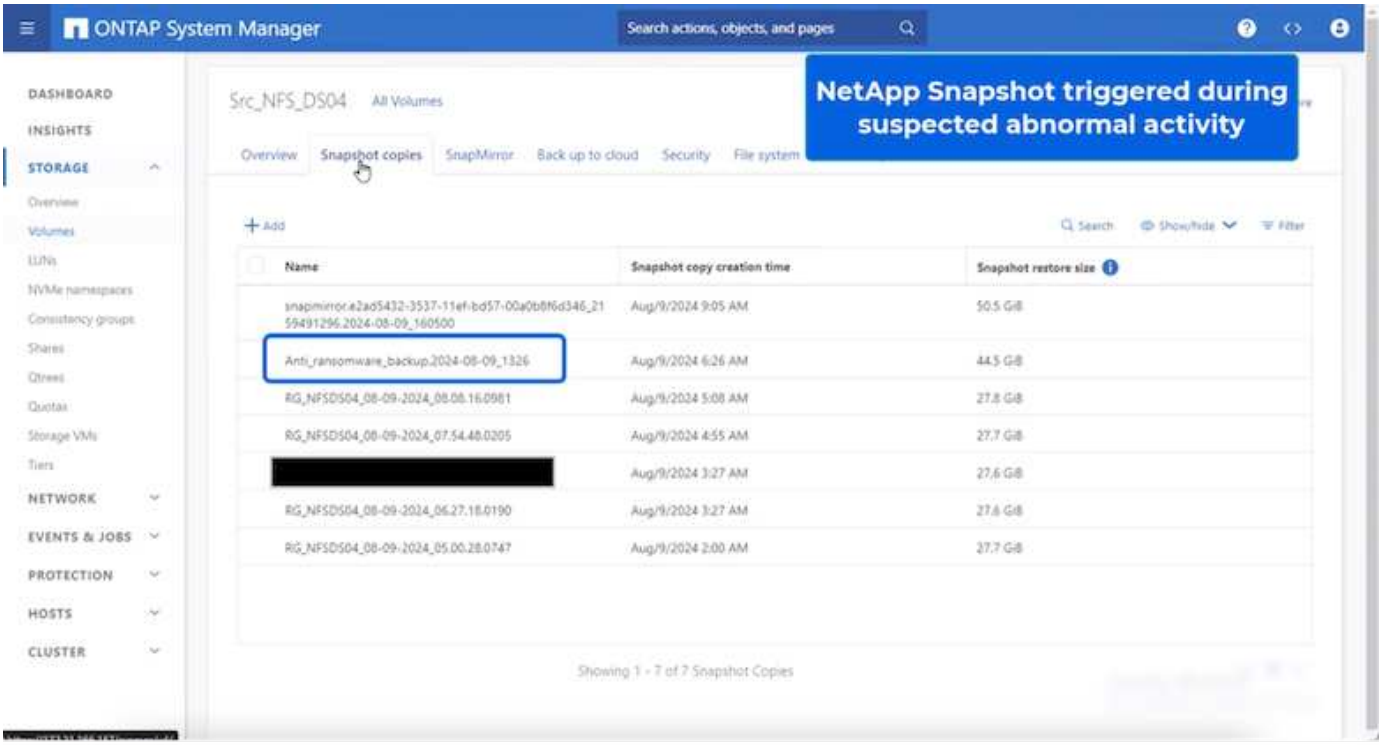


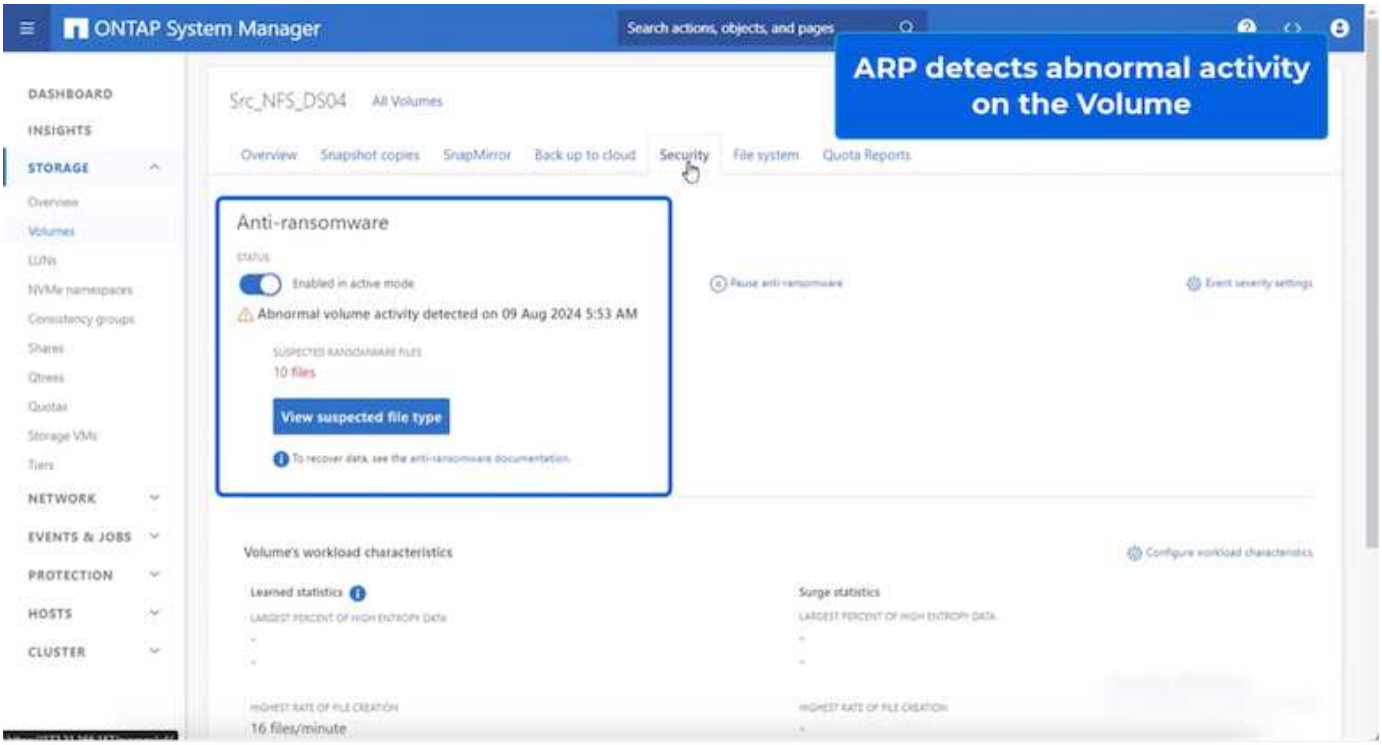
Per informazioni dettagliate sulla configurazione della protezione ransomware BlueXP , fare riferimento a "Imposta la protezione dal ransomware BlueXP " e "Configurare le impostazioni di protezione dal ransomware BlueXP".

È giunto il momento di descrivere questo concetto con un esempio. In questa procedura dettagliata, il datastore “Src_NFS_DS04” è interessato.

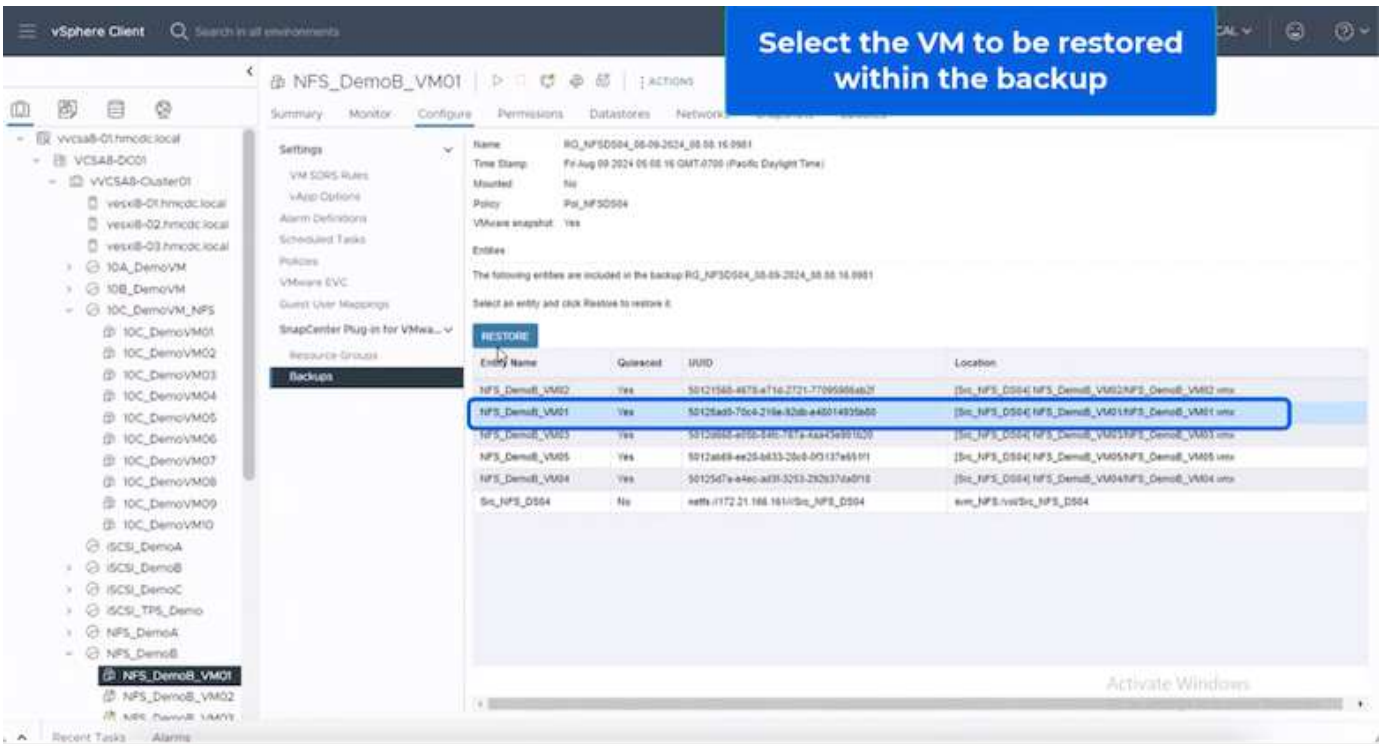


ARP ha immediatamente attivato uno snapshot sul volume al momento del rilevamento.





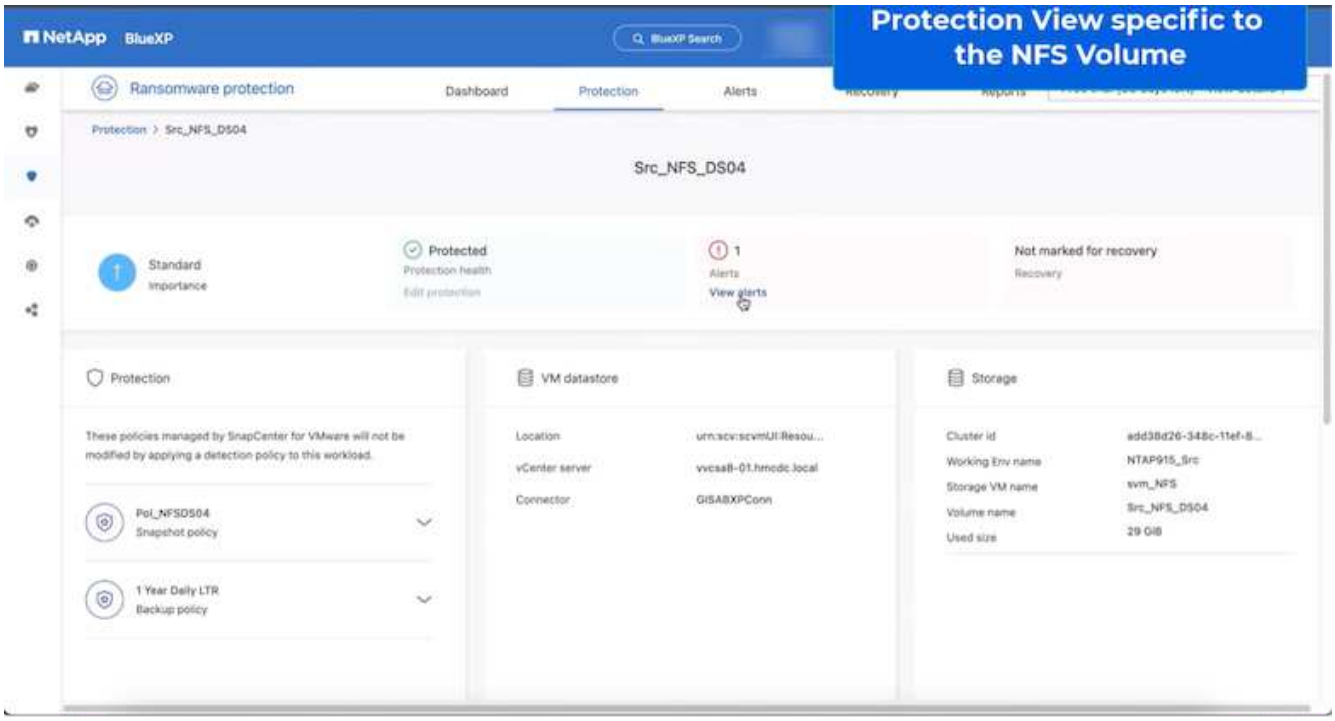
Una volta completata l'analisi forense, è possibile eseguire i ripristini in modo rapido e perfetto utilizzando la protezione dal ransomware di SnapCenter o BlueXP . Con SnapCenter, andare alle macchine virtuali interessate e selezionare lo snapshot appropriato da ripristinare.



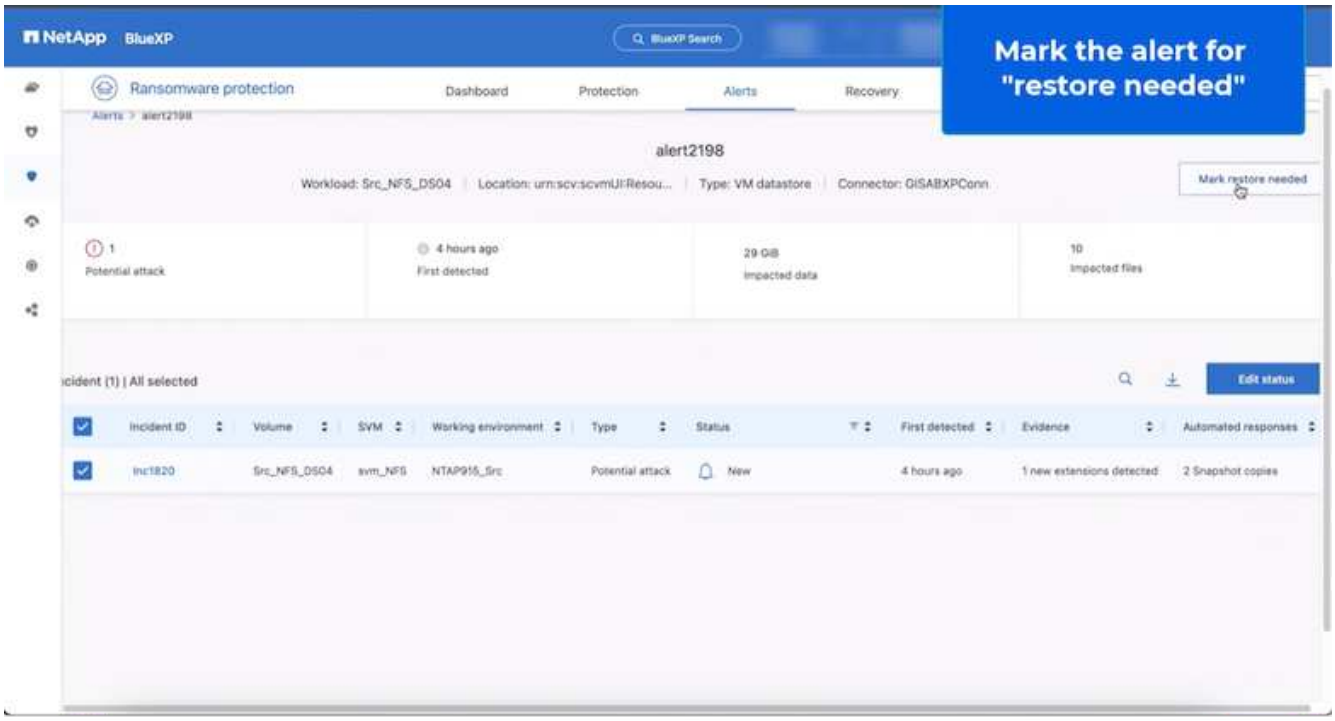
Questa sezione analizza il modo in cui la protezione ransomware BlueXP orchestra il recovery da un incidente ransomware in cui i file delle VM sono crittografati.

Se la macchina virtuale è gestita da SnapCenter, la protezione anti-ransomware BlueXP ripristina lo stato precedente della macchina virtuale utilizzando il processo coerente con la macchina virtuale.

1. Accedi alla protezione ransomware di BlueXP ed è visualizzato un avviso sulla Dashboard di protezione ransomware di BlueXP .
2. Fare clic sull'avviso per esaminare gli incidenti relativi a quel volume specifico per l'avviso generato

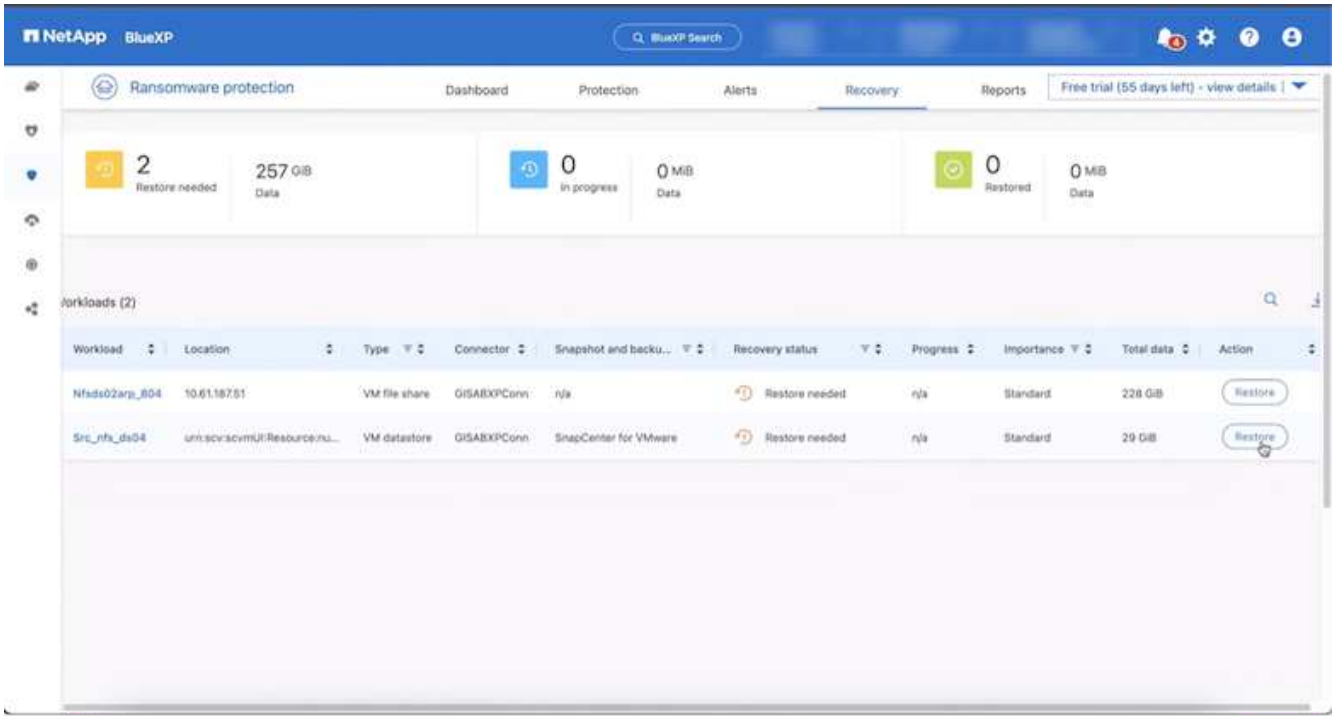


3. Contrassegna l'incidente ransomware come pronto per il recovery (dopo la neutralizzazione degli incidenti) selezionando "Mark restore needed"

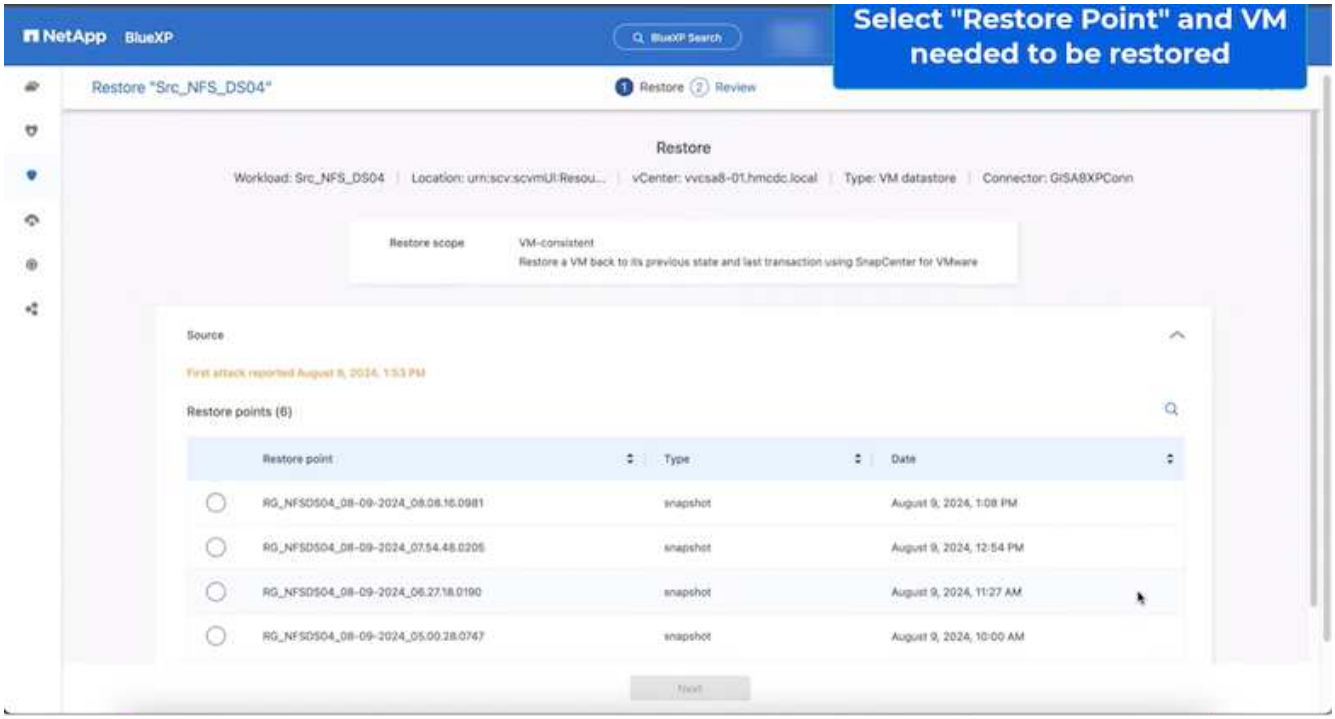


L'avviso può essere ignorato se l'incidente risulta falso positivo.

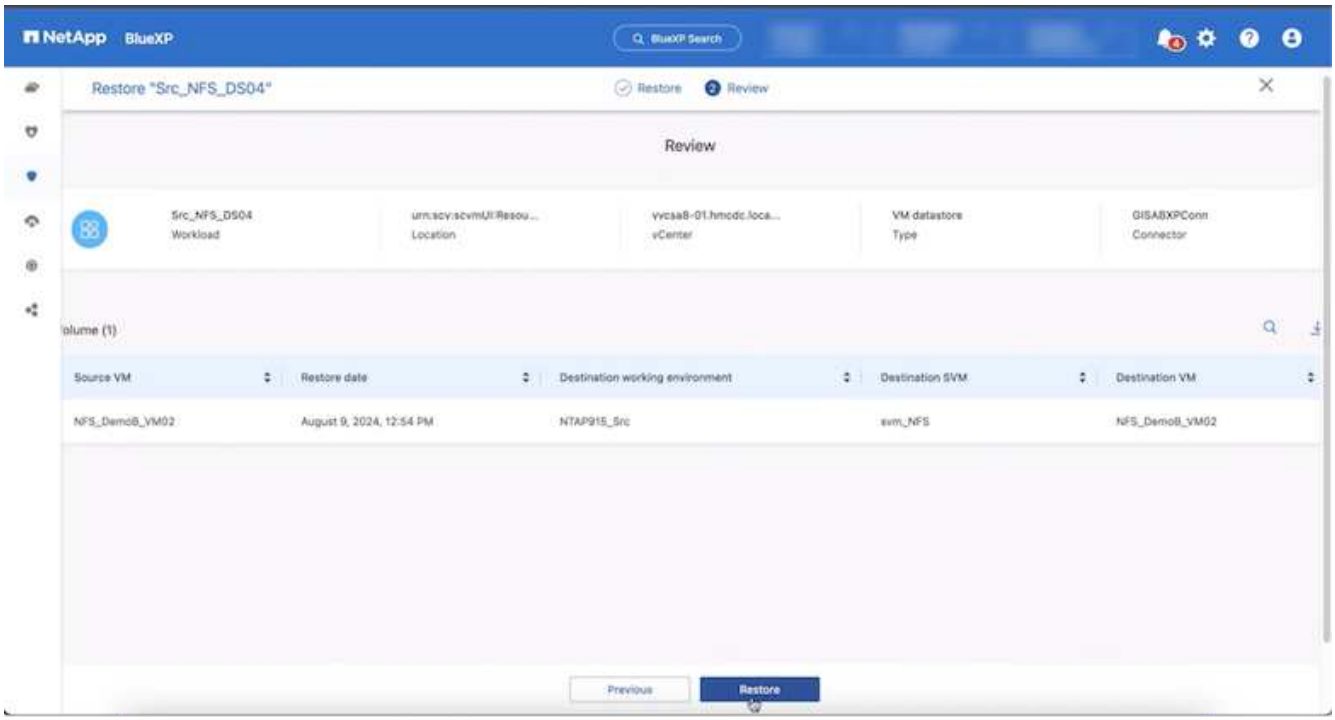
4. Accedere alla scheda Recovery (Ripristino), esaminare le informazioni sul carico di lavoro nella pagina Recovery (Ripristino), selezionare il volume del datastore che si trova nello stato "Restore needed" (Ripristino necessario) e selezionare Restore (Ripristina).



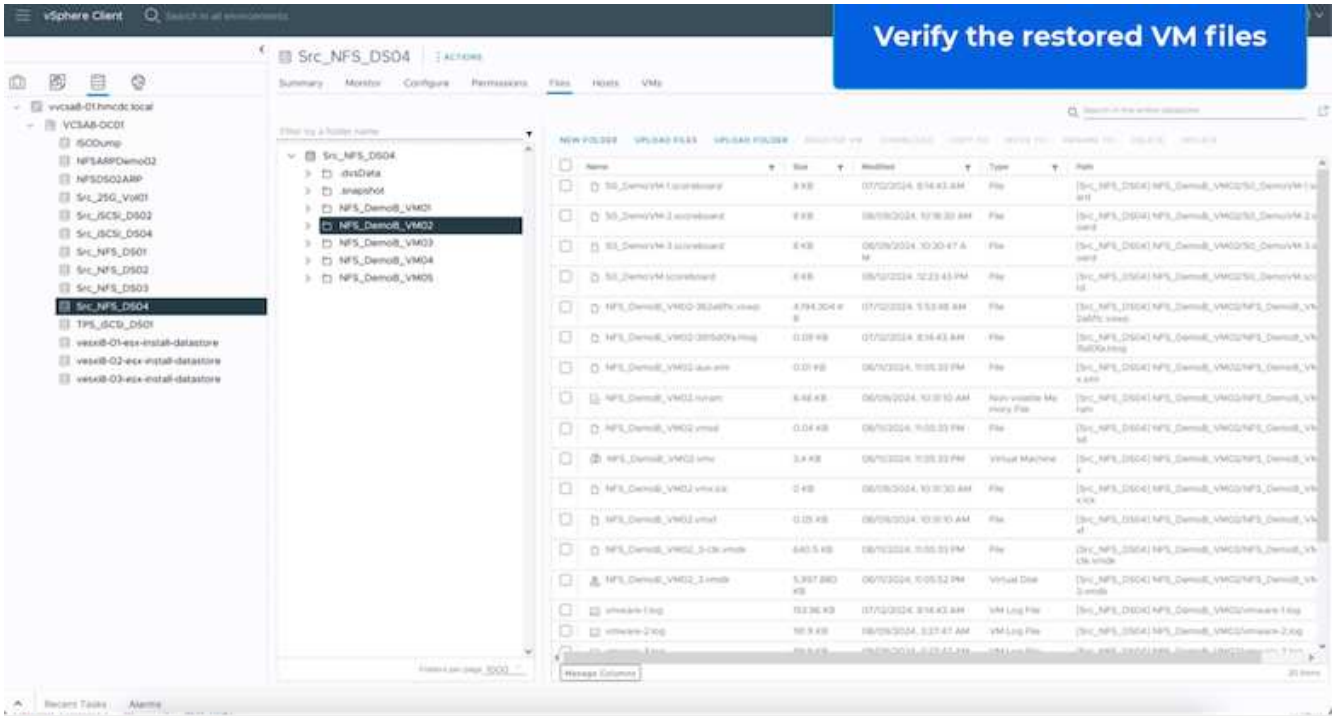
5. In questo caso, l'ambito del ripristino è "da VM" (per SnapCenter per VM, l'ambito del ripristino è "da VM")



6. Scegliere il punto di ripristino da utilizzare per ripristinare i dati, quindi selezionare destinazione e fare clic su Ripristina.



7. Dal menu superiore, selezionare Recovery (Ripristino) per esaminare il carico di lavoro nella pagina Recovery (Ripristino) in cui lo stato dell'operazione si sposta tra gli stati. Una volta completato il ripristino, i file della VM vengono ripristinati come mostrato di seguito.



> Il ripristino può essere eseguito da SnapCenter per VMware o plug-in SnapCenter, a seconda dell'applicazione.

La soluzione NetApp fornisce vari strumenti efficaci per visibilità, rilevamento e correzione, aiutandoti a rilevare tempestivamente il ransomware, prevenire questa diffusione e ripristinare rapidamente, se necessario, per evitare costosi downtime. Le soluzioni di difesa tradizionali a layer rimangono le più diffuse, così come quelle di

partner e terze parti per la visibilità e il rilevamento. Una correzione efficace rimane una parte fondamentale della risposta a qualsiasi minaccia.

Volumi virtuali VMware con ONTAP

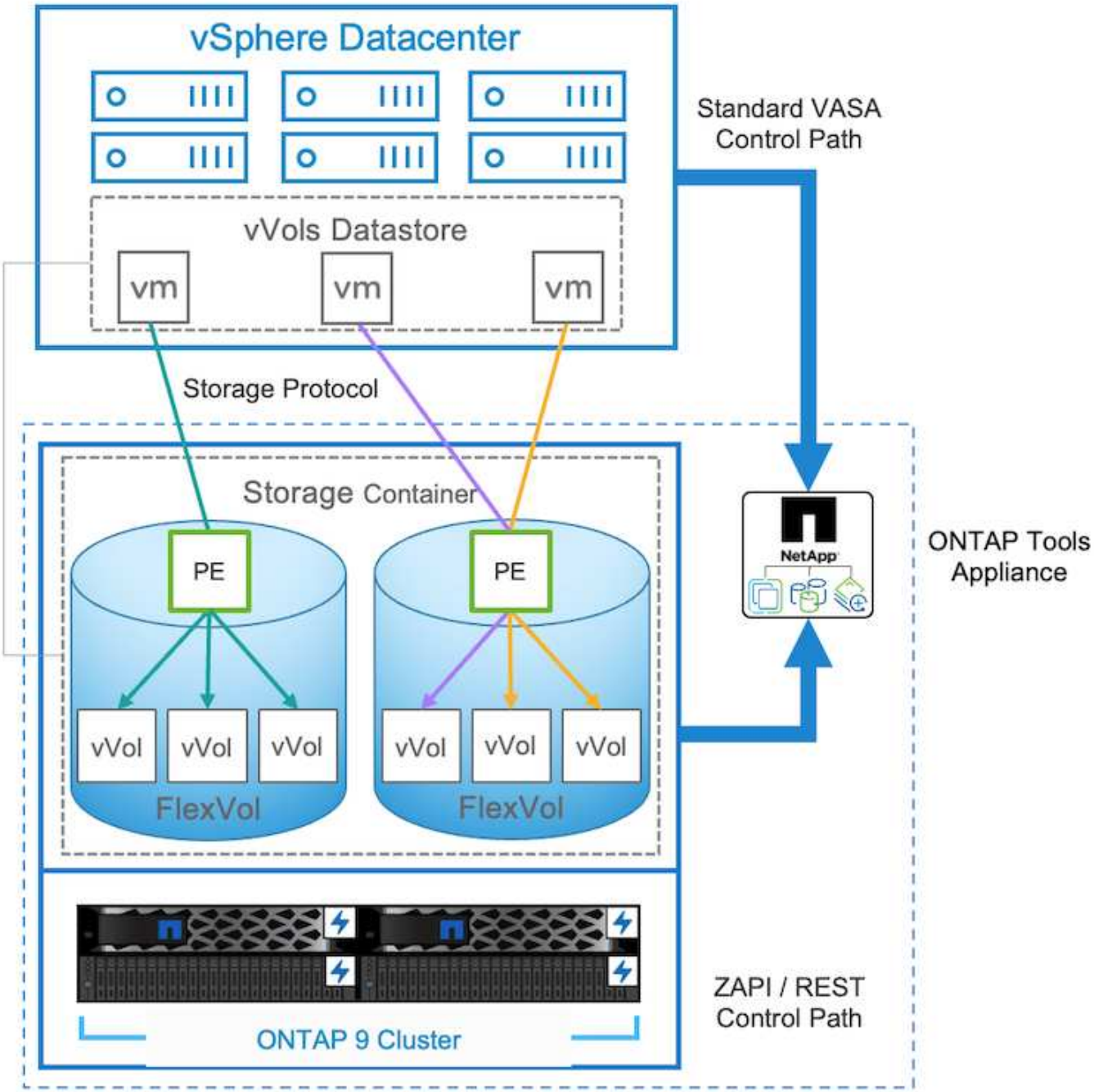
I volumi virtuali di VMware (vVol) consentono di utilizzare requisiti specifici delle applicazioni per prendere decisioni sul provisioning dello storage sfruttando l'ampio set di funzionalità degli storage array. L'API vSphere per Storage Awareness (VASA) consente a un amministratore delle macchine virtuali di utilizzare con facilità qualsiasi funzionalità storage necessarie per il provisioning delle macchine virtuali senza dover interagire con il team di storage. Prima di VASA, gli amministratori delle macchine virtuali potevano definire le policy di storage delle macchine virtuali, ma dovevano collaborare con gli amministratori dello storage per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o le convenzioni di denominazione. Con VASA, gli amministratori di vCenter con le autorizzazioni appropriate possono definire una serie di funzionalità di storage che gli utenti di vCenter possono utilizzare per eseguire il provisioning delle macchine virtuali. La mappatura tra policy di storage delle macchine virtuali e profilo di funzionalità di storage del datastore consente a vCenter di visualizzare un elenco di datastore compatibili per la selezione, nonché di abilitare altre tecnologie come aria (precedentemente nota come vRealize) Automation o Tanzu Kubernetes Grid per selezionare automaticamente lo storage da una policy assegnata. Questo approccio è noto come gestione basata su criteri di storage. Anche se i profili e le policy delle funzionalità di storage possono essere utilizzati anche con i datastore tradizionali, la nostra attenzione qui è dedicata agli archivi dati vVols. Il provider VASA per ONTAP è incluso come parte dei tool ONTAP per VMware vSphere.

I vantaggi offerti dall'offerta di provider VASA fuori dallo storage array includono:

- Una singola istanza può gestire più array di storage.
- Il ciclo di rilascio non deve dipendere dalla versione del sistema operativo di archiviazione.
- Le risorse sugli storage array sono molto costose.

Ogni datastore vVol si basa sul container storage, che rappresenta una voce logica nel provider VASA per definire la capacità dello storage. Il container di storage con strumenti ONTAP è costruito con ONTAP Volumes. È possibile espandere il container di storage aggiungendo volumi ONTAP all'interno della stessa SVM.

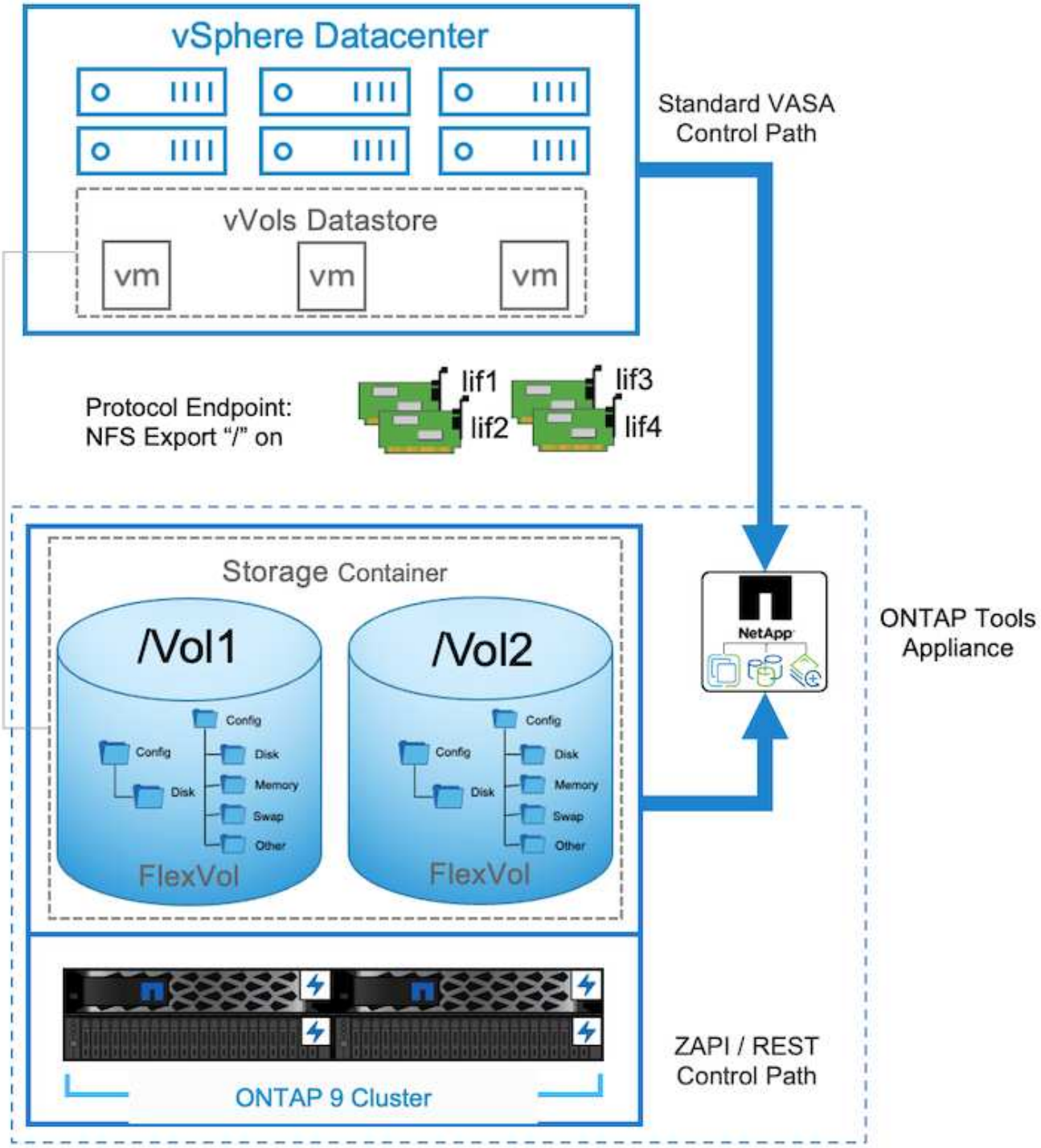
L'endpoint del protocollo (PE) è gestito principalmente dagli strumenti ONTAP. Nel caso di vVol basati su iSCSI, viene creato un PE per ogni volume ONTAP che fa parte di quel container di storage o datastore vVol. Il PE per iSCSI è un LUN di piccole dimensioni (4MiB GB per 9.x e 2GiB GB per 10.x) presentato all'host vSphere e i criteri di multipathing vengono applicati al PE.

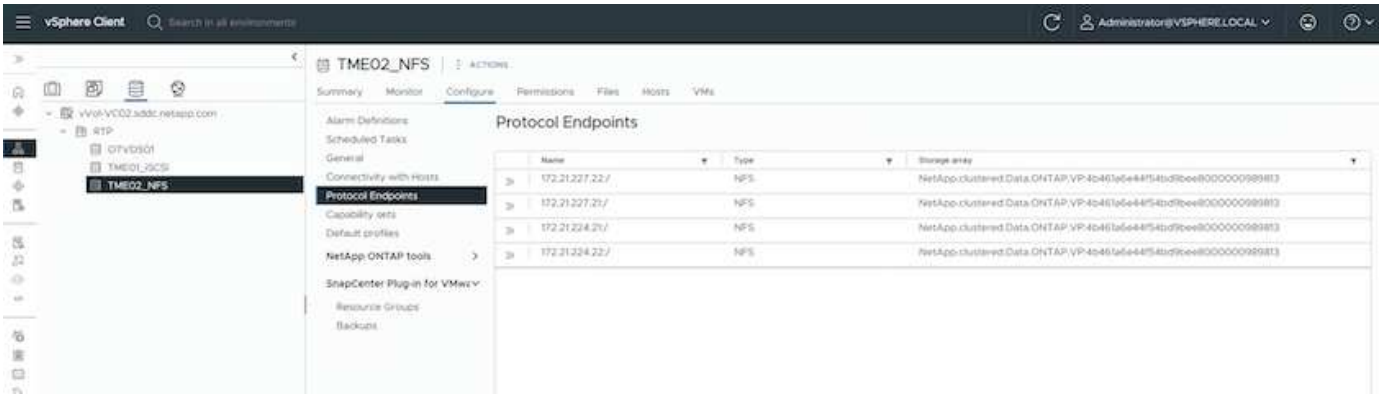



```
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint  -fields size
vserver path                                                  size
------- ------------------------------------------------- ----
zoneb   /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb   /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb   /vol/TME01_iSCSI_01/vvolPE-1723727751956          4MB
zoneb   /vol/TME01_iSCSI_02/vvolPE-1723727751970          4MB
4 entries were displayed.
```

Per NFS, viene creato un PE per l'esportazione del file system root con ogni lif dei dati NFS su SVM in cui

risiede il container di storage o il datastore vVol.





I tool ONTAP gestiscono il ciclo di vita di PE e anche la comunicazione host vSphere con l'espansione e la riduzione del cluster vSphere. ONTAP tools API è disponibile per l'integrazione con i tool di automazione esistenti.

Al momento, i tool ONTAP per VMware vSphere sono disponibili con due release.

Strumenti ONTAP 9.x

- Quando è richiesto il supporto vVol per NVMe/FC
- Requisiti normativi USA federali o UE
- Più casi di utilizzo integrati con il plug-in SnapCenter per VMware vSphere

Strumenti ONTAP 10.x

- Disponibilità elevata
- Multi-tenancy
- Scala grande
- Supporto Active Sync di SnapMirror per datastore VMFS
- La prossima integrazione per alcuni casi di utilizzo con il plug-in SnapCenter per VMware vSphere

Perché vVol?

I volumi virtuali di VMware (vVol) offrono i seguenti benefici:

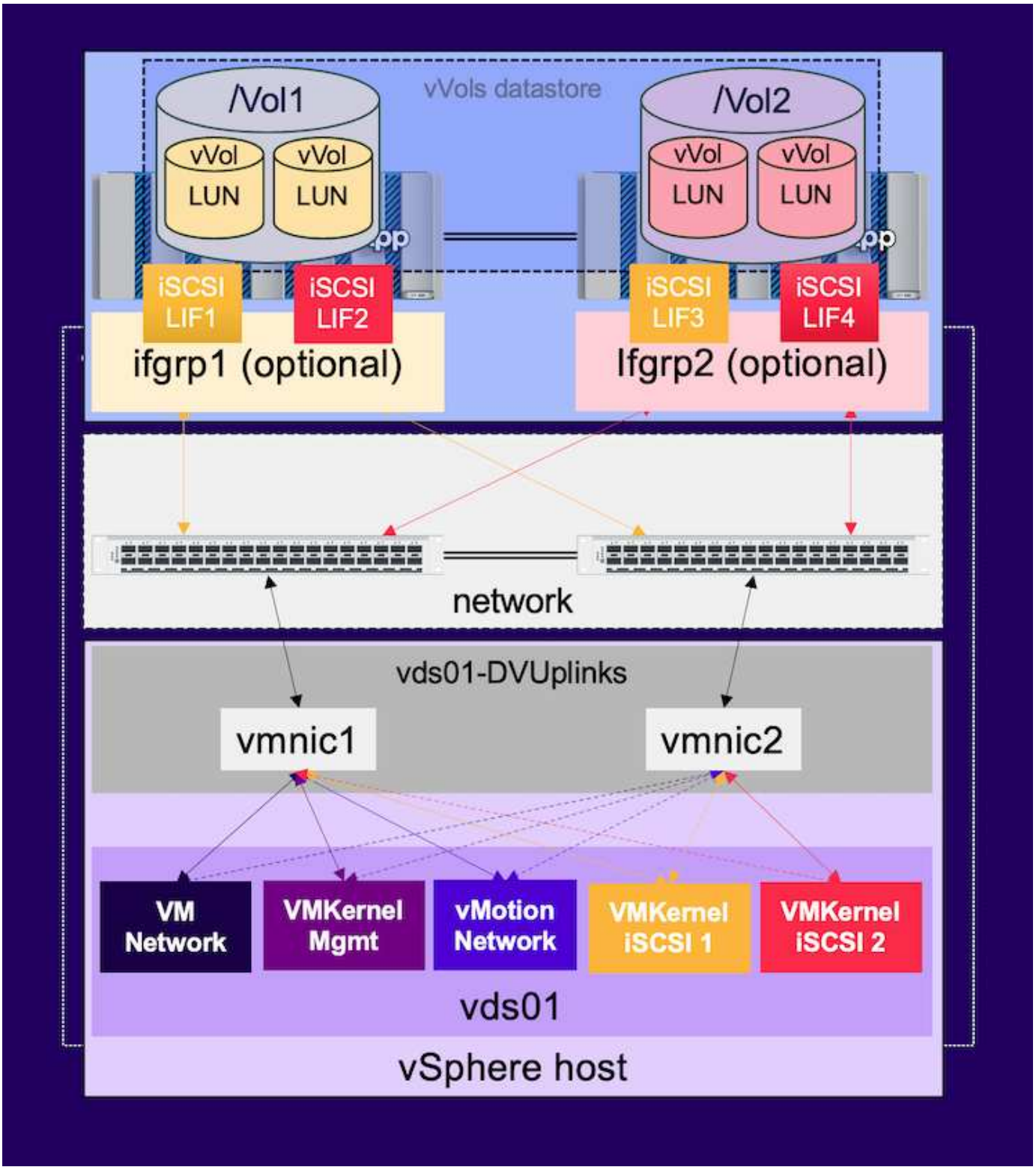
- Provisioning semplificato (non è necessario preoccuparsi dei limiti LUN massimi per ogni host vSphere o dover creare esportazioni NFS per ogni volume)
- Riduce al minimo il numero di percorsi iSCSI/FC (per vVol basato su SCSI a blocchi)
- Snapshot, cloni e altre operazioni storage vengono in genere trasferite nello storage array e funzionano molto più velocemente.
- Migrazione semplificata dei dati per le macchine virtuali (non è necessario coordinarsi con altri proprietari di macchine virtuali sulla stessa LUN)
- Policy di QoS applicate a livello di disco della macchina virtuale anziché a livello di volume.
- Semplicità operativa (i vendor di soluzioni storage offrono le proprie funzionalità differenziate nel provider VASA)
- Supporta VM su larga scala.
- Supporto della replica vVol per la migrazione tra vCenter.

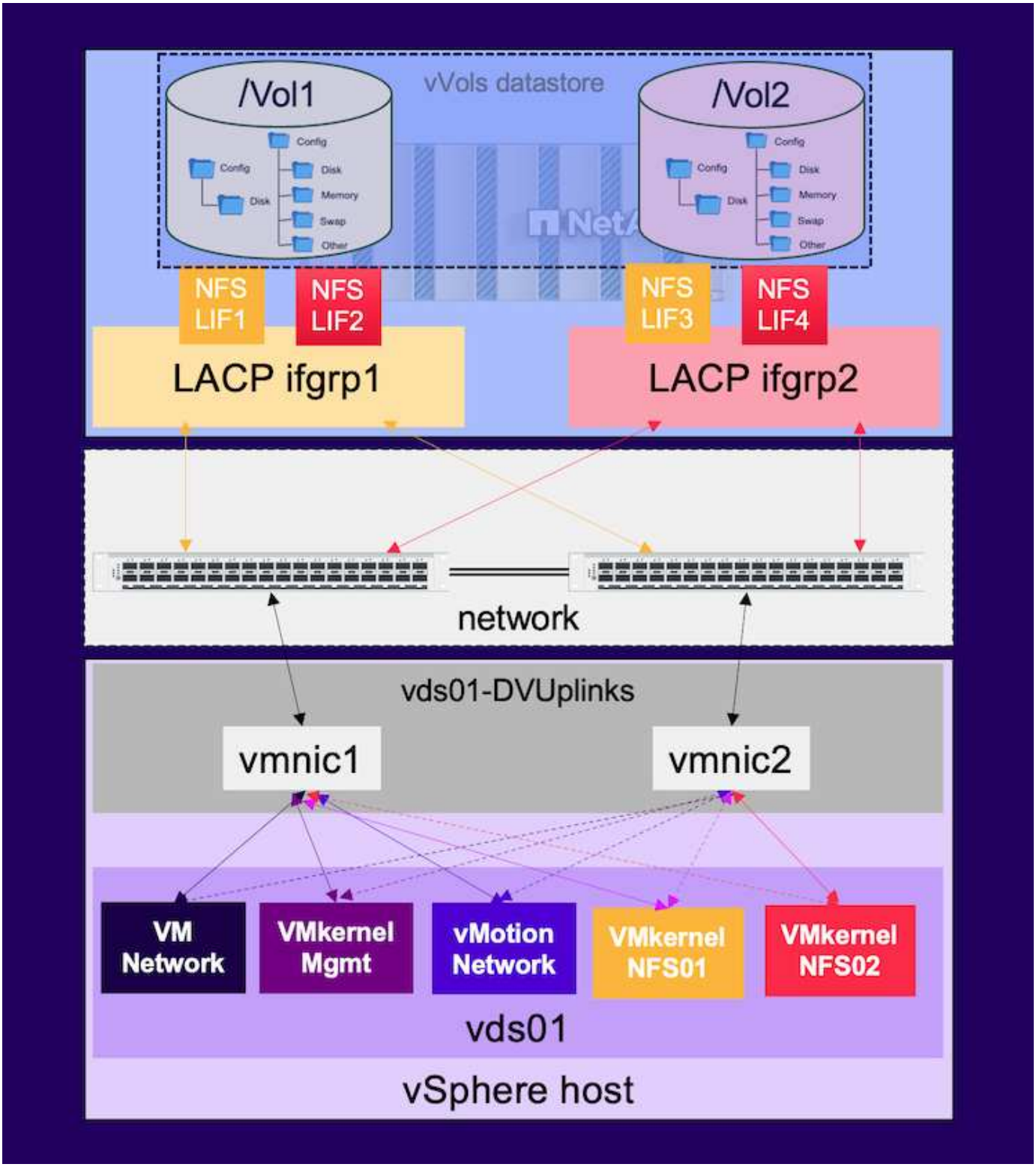
- Gli amministratori dello storage possono eseguire il monitoraggio a livello del disco delle VM.

Opzioni di connettività

L'ambiente dual fabric è generalmente consigliato per le reti di storage per gestire high Availability, performance e fault tolerance. I vVol sono supportati con iSCSI, FC, NFSv3 e NVMe/FC. NOTA: Fare riferimento alla "Tool di matrice di interoperabilità (IMT)"versione dello strumento ONTAP supportata

L'opzione di connettività rimane coerente con le opzioni del datastore VMFS o NFS. Di seguito è illustrato un esempio di rete vSphere di riferimento per iSCSI e NFS.


vVols datastore
/Vol1
vVol
LUN
vVol
LUN
/Vol2
vVol
LUN
vVol
LUN
iSCSI LIF1
iSCSI LIF2
iSCSI LIF3
iSCSI LIF4
ifgrp1 (optional)
Ifgrp2 (optional)
network
vds01-DVUplinks
vmnic1
vmnic2
VM Network
VMKernel Mgmt
vMotion Network
VMKernel iSCSI 1
VMKernel iSCSI 2
vds01
vSphere host

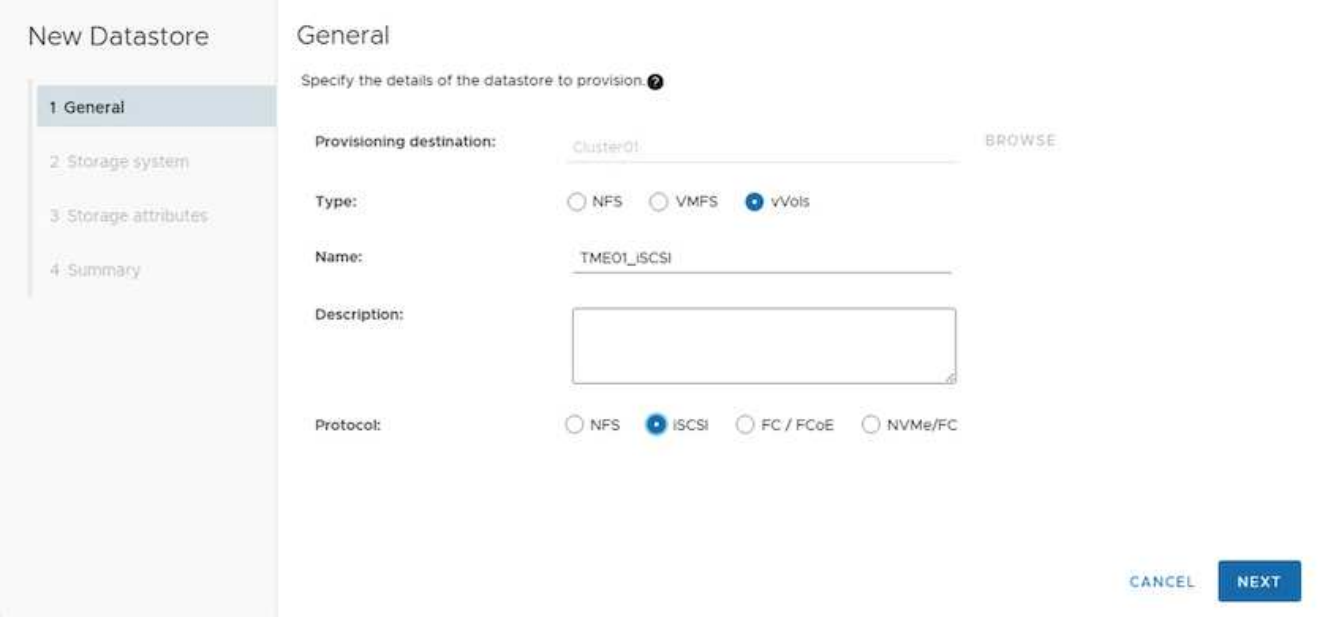


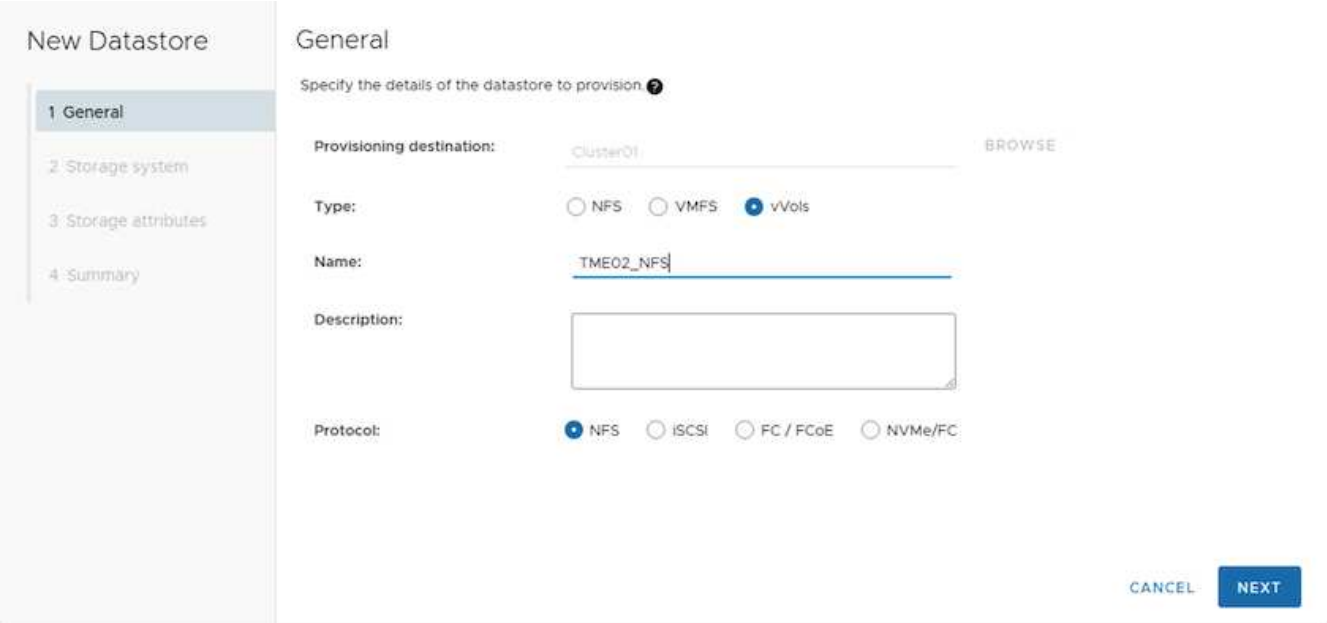
Provisioning con gli strumenti ONTAP per VMware vSphere

È possibile eseguire il provisioning del datastore vVol in modo simile a quello di VMFS o NFS utilizzando i tool ONTAP. Se il plug-in degli strumenti ONTAP non è disponibile sull'interfaccia utente del client vSphere, fare riferimento alla sezione come iniziare riportata di seguito.

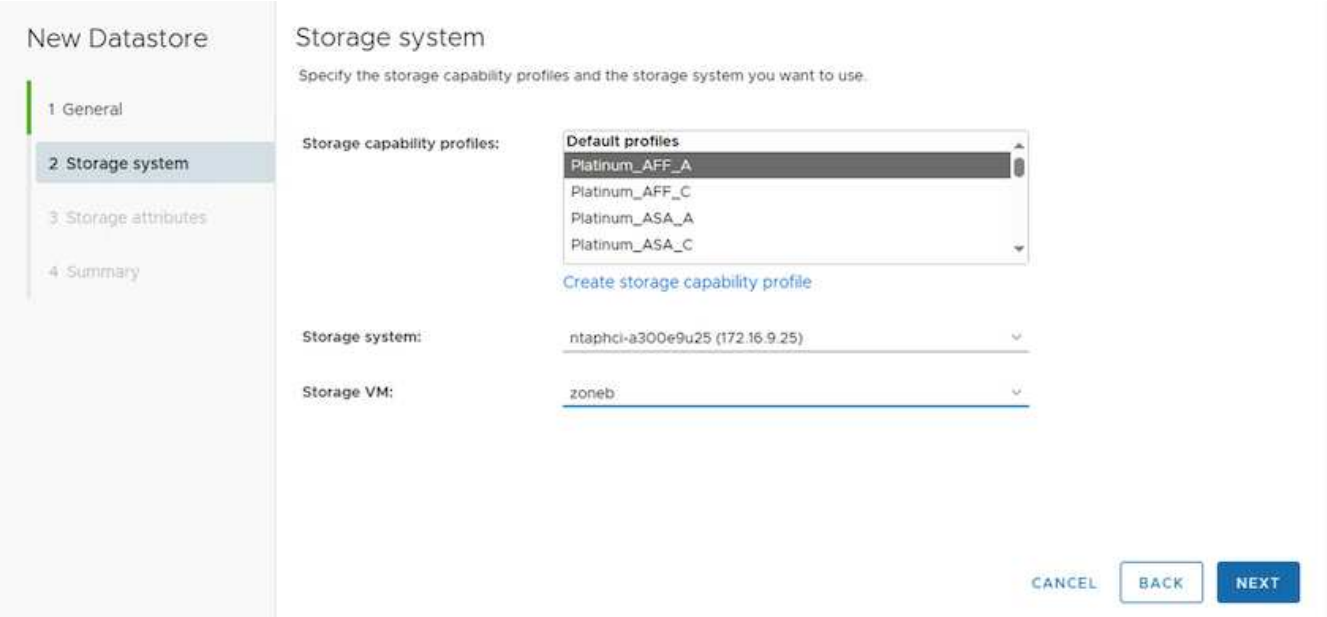
Con gli strumenti ONTAP 9,13

1. Fare clic con il pulsante destro del mouse sul cluster o sull'host vSphere e selezionare Esegui il provisioning del datastore in Strumenti NetApp ONTAP.
2. Mantenere il tipo come vVol, fornire il nome per l'archivio dati e selezionare il protocollo desiderato

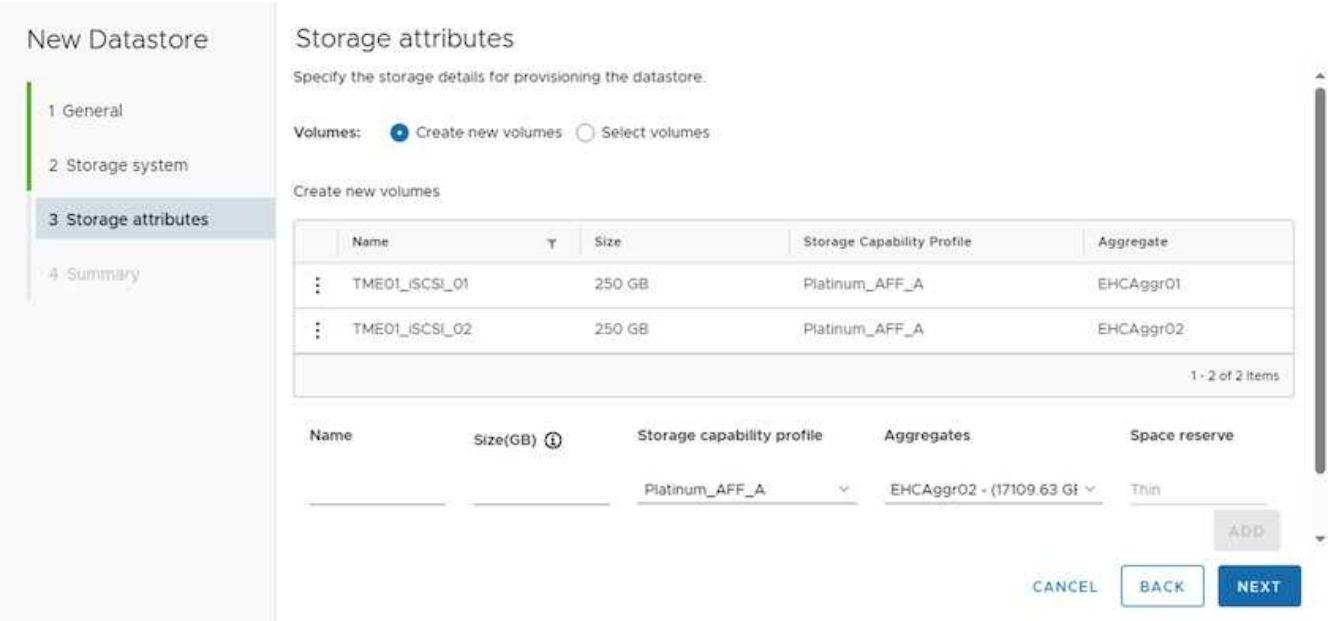




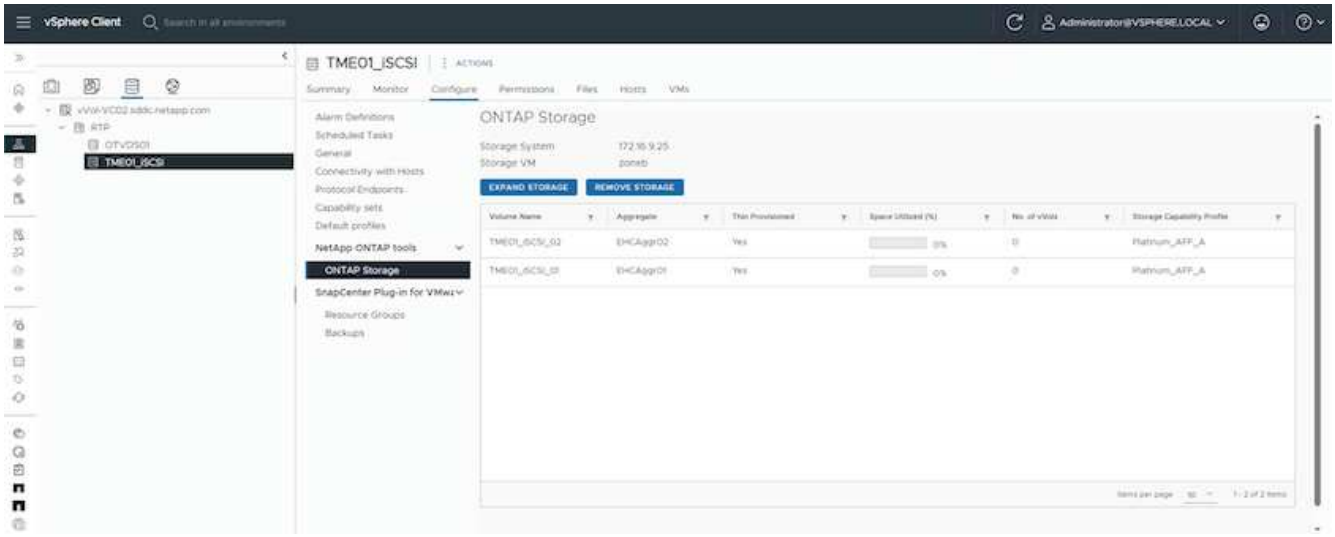
3. Seleziona il profilo di capacità dello storage desiderato, scegli il sistema storage e la SVM.



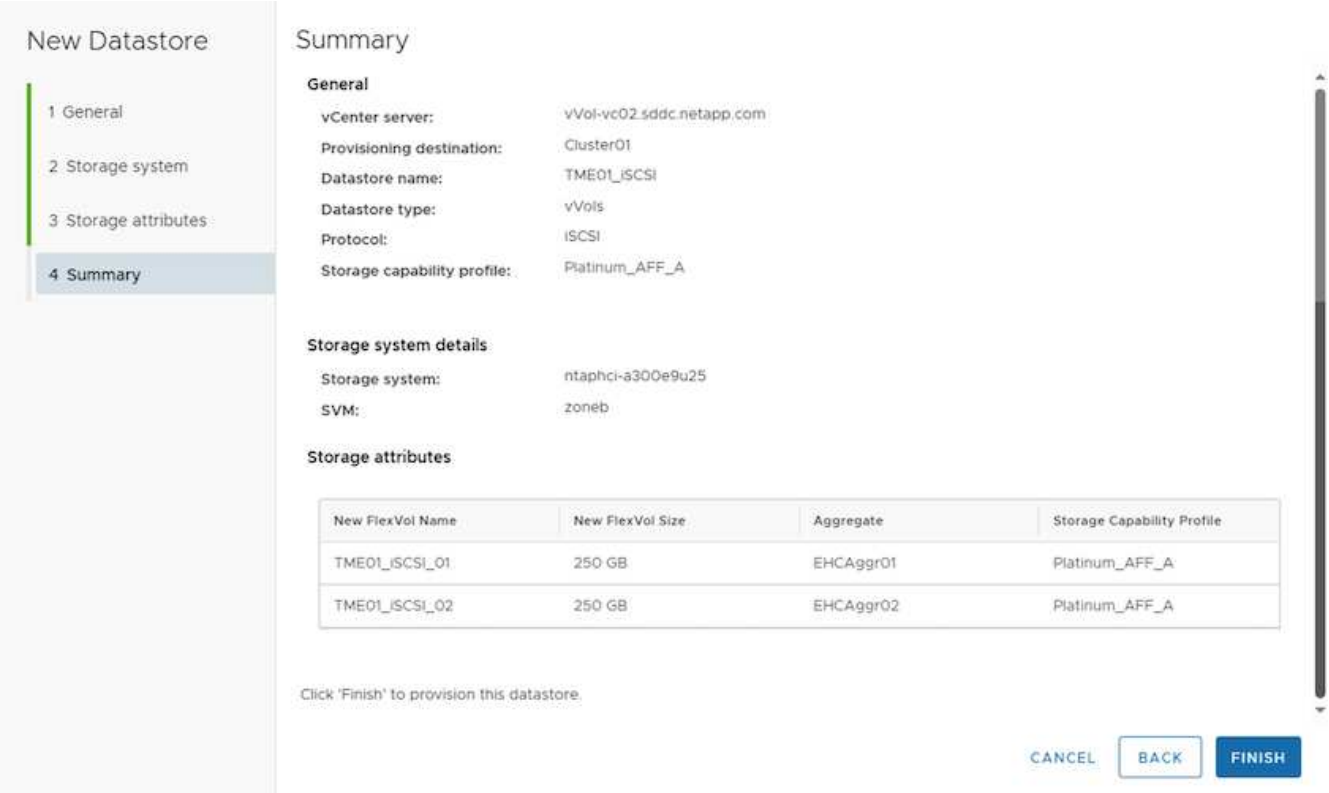
4. Crea nuovi volumi ONTAP o selezionali esistenti per il datastore vVol.



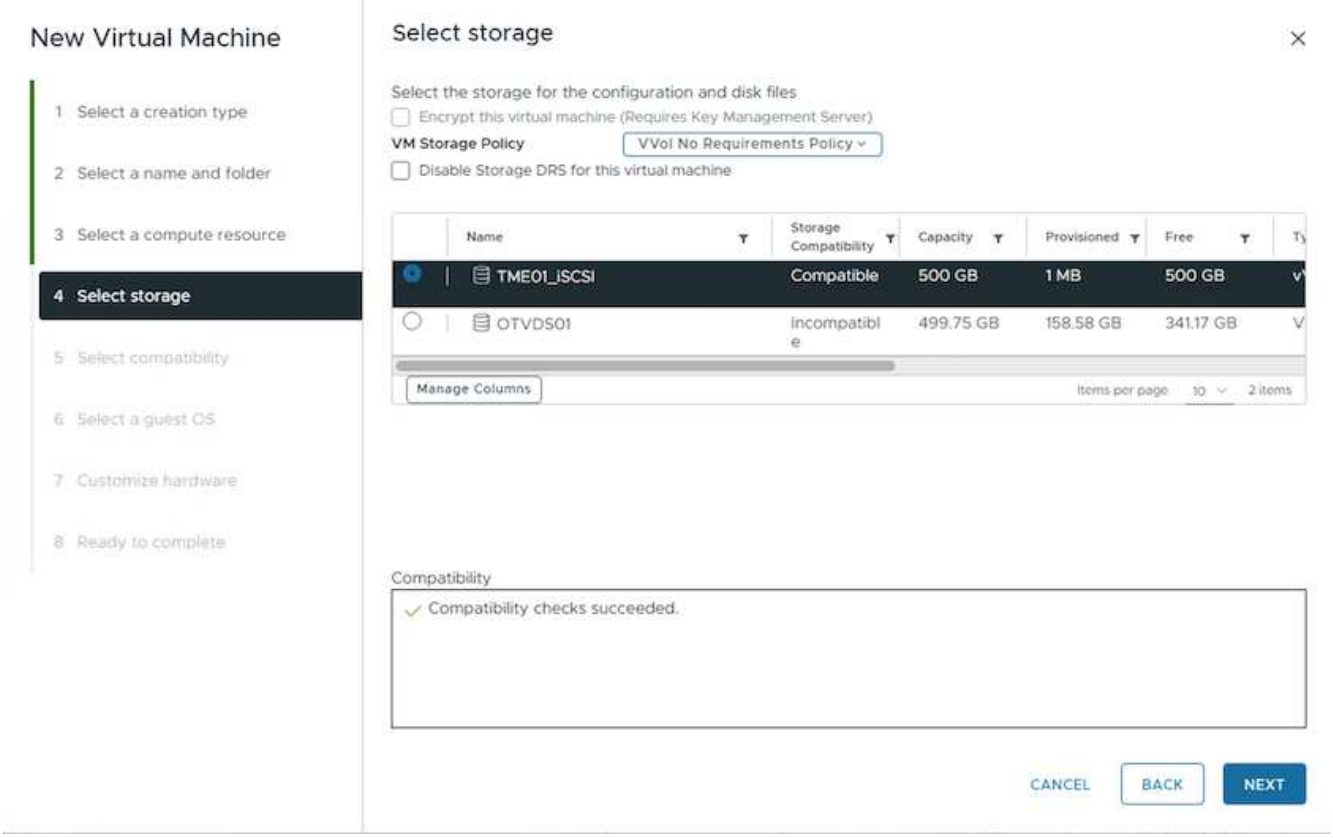
È possibile visualizzare o modificare i volumi ONTAP in un secondo momento dall'opzione relativa al datastore.



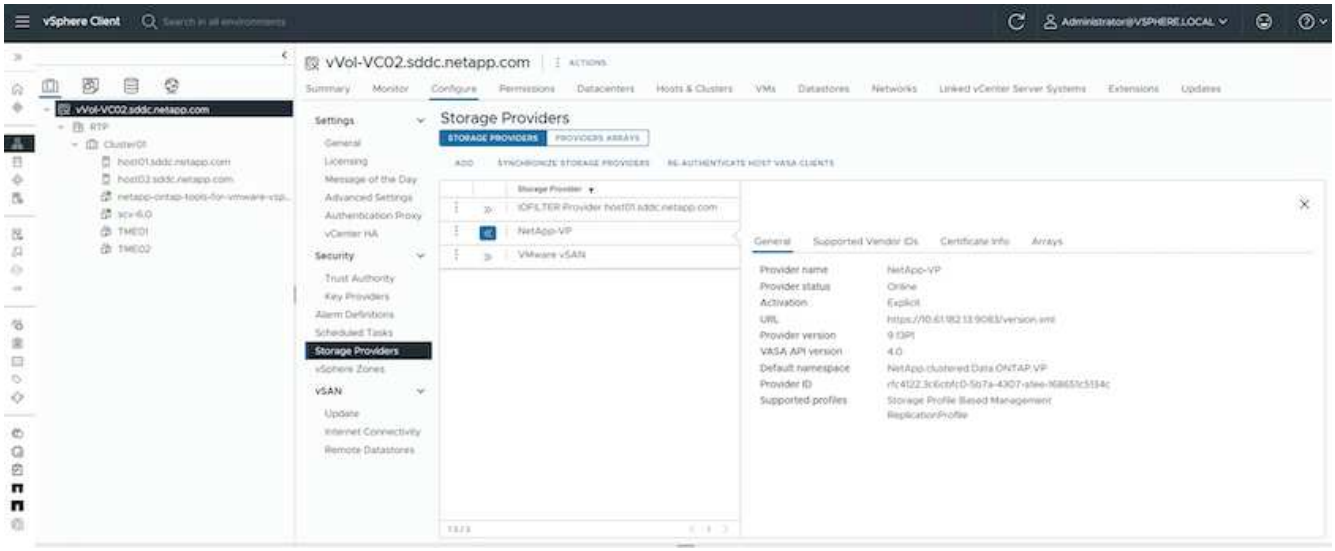
5. Rivedere il riepilogo e fare clic su fine per creare il datastore vVol.



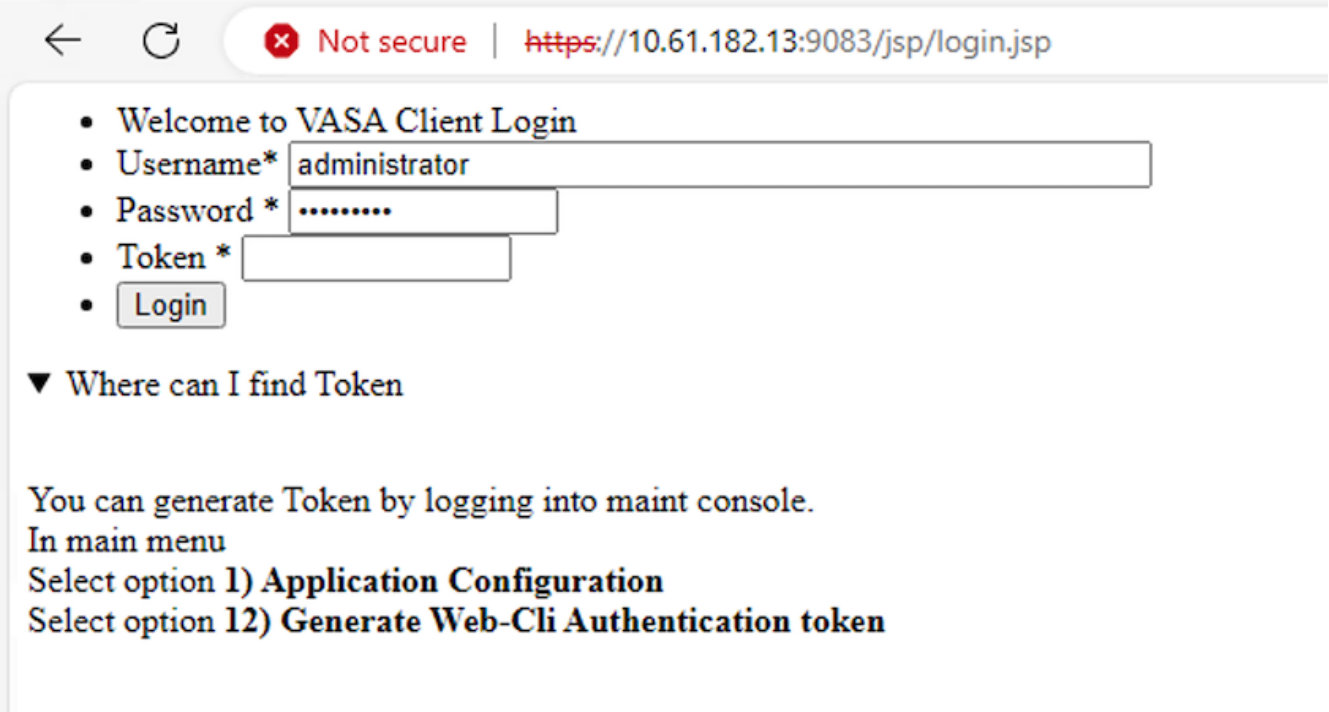
6. Una volta creato, il datastore vVol può essere utilizzato come qualsiasi altro datastore. Segue un esempio di assegnazione di un datastore basato su policy storage delle macchine virtuali a una macchina virtuale che viene creata.



7. I dettagli di vVol possono essere recuperati usando l'interfaccia CLI basata su web. L'URL del portale è lo stesso dell'URL del provider VASA senza il nome file version.xml.



La credenziale deve corrispondere alle informazioni utilizzate durante la fornitura degli strumenti ONTAP



Oppure utilizzare la password aggiornata con la console di manutenzione di ONTAP Tools.

```
Application Configuration Menu:
-------------------------------
   1 ) Display server status summary
   2 ) Start Virtual Storage Console service
   3 ) Stop  Virtual Storage Console service
   4 ) Start VASA Provider and SRA service
   5 ) Stop VASA Provider and SRA service
   6 ) Change 'administrator' user password
   7 ) Re-generate certificates
   8 ) Hard reset database
   9) Change LOG level for Virtual Storage Console service
   10) Change LOG level for VASA Provider and SRA service
   11) Display TLS configuration
   12) Generate Web-Cli Authentication token
   13) Start ONTAP tools plug-in service
   14) Stop ONTAP tools plug-in service
   15) Start Log Integrity service
   16) Stop Log Integrity service
   17) Change database password

   b ) Back
   x ) Exit

 Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

This token is for one time use only.Its valid for 20 minutes.


 Press ENTER to continue.
```

Selezionare l'interfaccia CLI basata sul Web.

NetApp ONTAP tools for VMware vSphere - Control Panel:

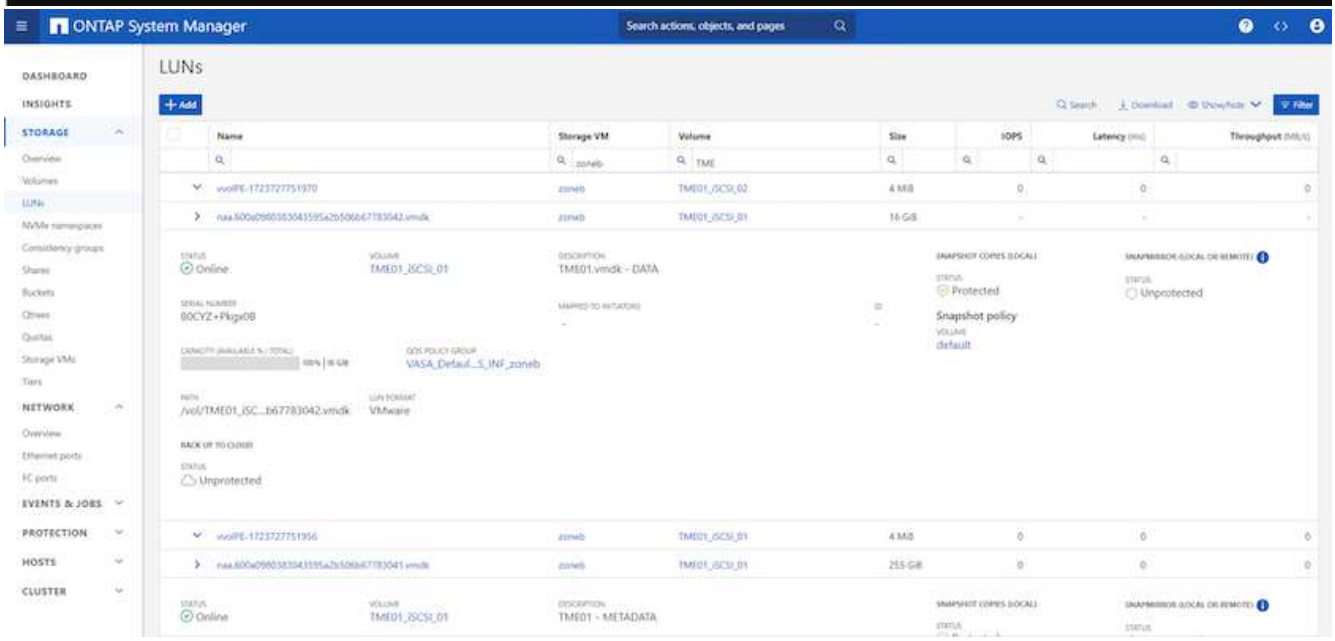
Operation	Description
Web based CLI interface	Web based access to the command line interface for administrative tasks
Inventory	Listing of all objects and information currently known in Unified Virtual Appliance database
Statistics	Listing of all counters and information regarding internal state
Right Now	See what operations are in flight right now
Logout	Logout

Build Release 9.13P1
Build Timestamp 03/08/2024 11:11:42 AM
System up since Thu Aug 15 02:23:18 UTC 2024
Current time Thu Aug 15 17:59:26 UTC 2024

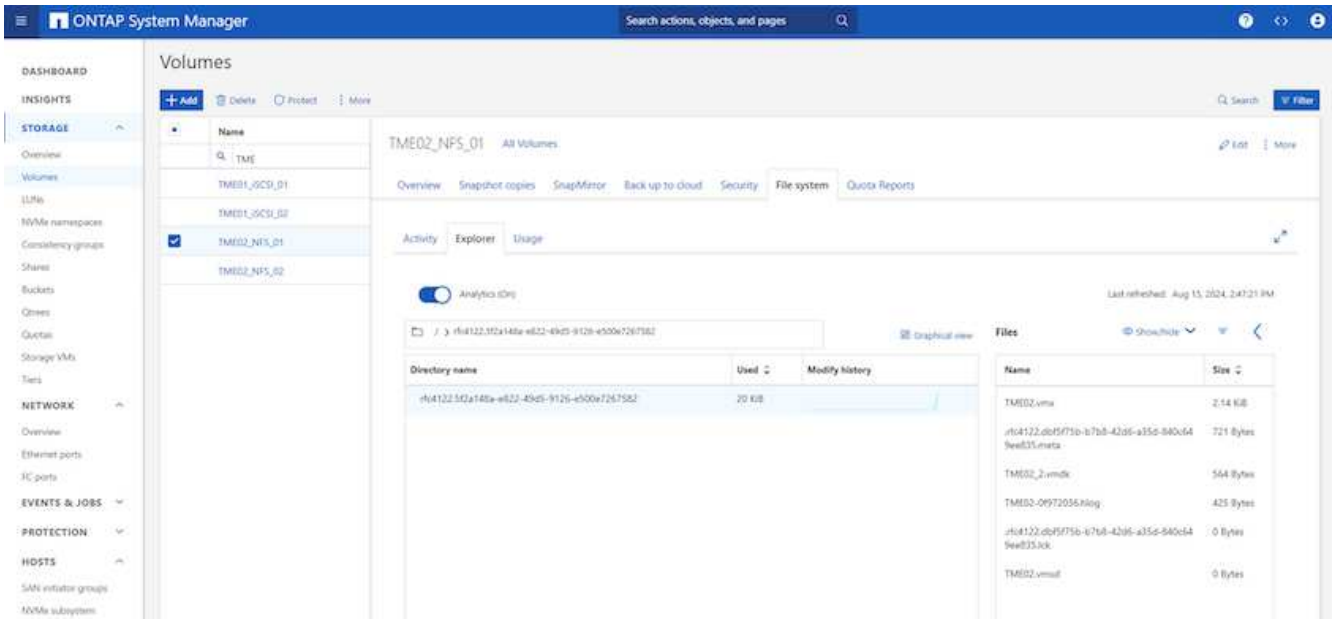
Digitare il comando desiderato dall'elenco dei comandi disponibili. Per elencare i dettagli vVol insieme alle informazioni sullo storage sottostante, provare vvol list -verbose=true

per basato su LUN, è possibile utilizzare anche la cli di ONTAP o System Manager.

```
ntaphci-a300e9u25::> lun show -vserver zoneb -class vvol  -fields comment,size
vserver path                                                      size  comment
------- ------------------------------------------------------------ ----- -------
zoneb   /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 16GB
zoneb   /vol/Demo01_fv02/naa.600a098038304359463f515057683737.vmdk 16GB
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk
                                                                  255GB TME01 - METADATA
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk
                                                                  16GB  TME01.vmdk - DATA
zoneb   /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk
                                                                  16GB  TME01.vmdk - DATA
```

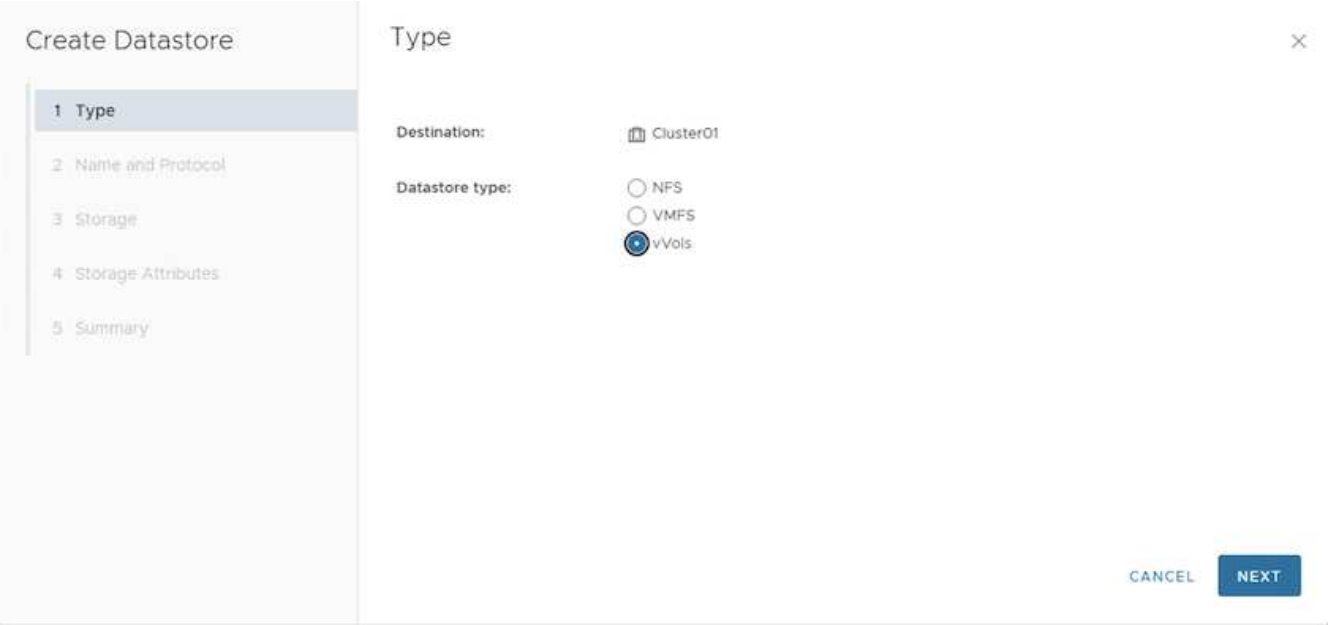


Per i sistemi basati su NFS, è possibile utilizzare System Manager per esplorare l'archivio dati.

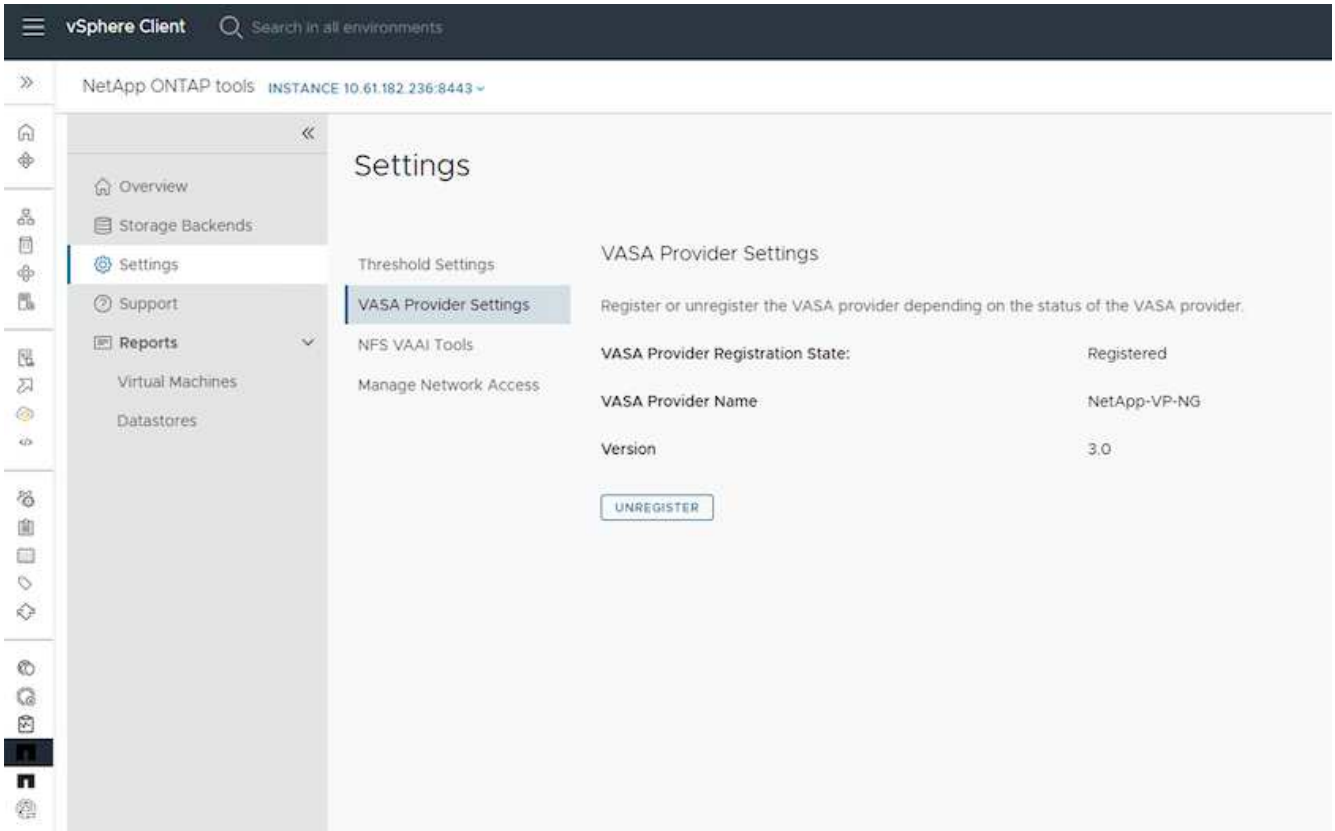


Con gli strumenti ONTAP 10,1

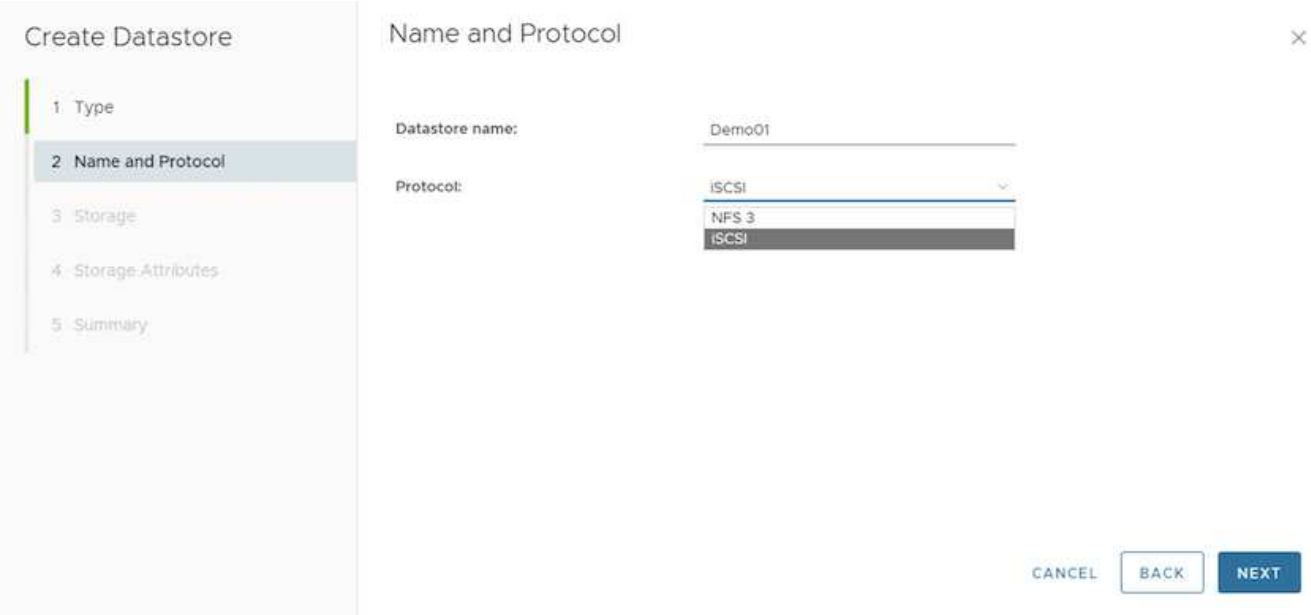
1. Fare clic con il pulsante destro del mouse sul cluster o sull'host vSphere e selezionare Crea datastore (10,1) in Strumenti NetApp ONTAP.
2. Selezionare il tipo di datastore come vVol.



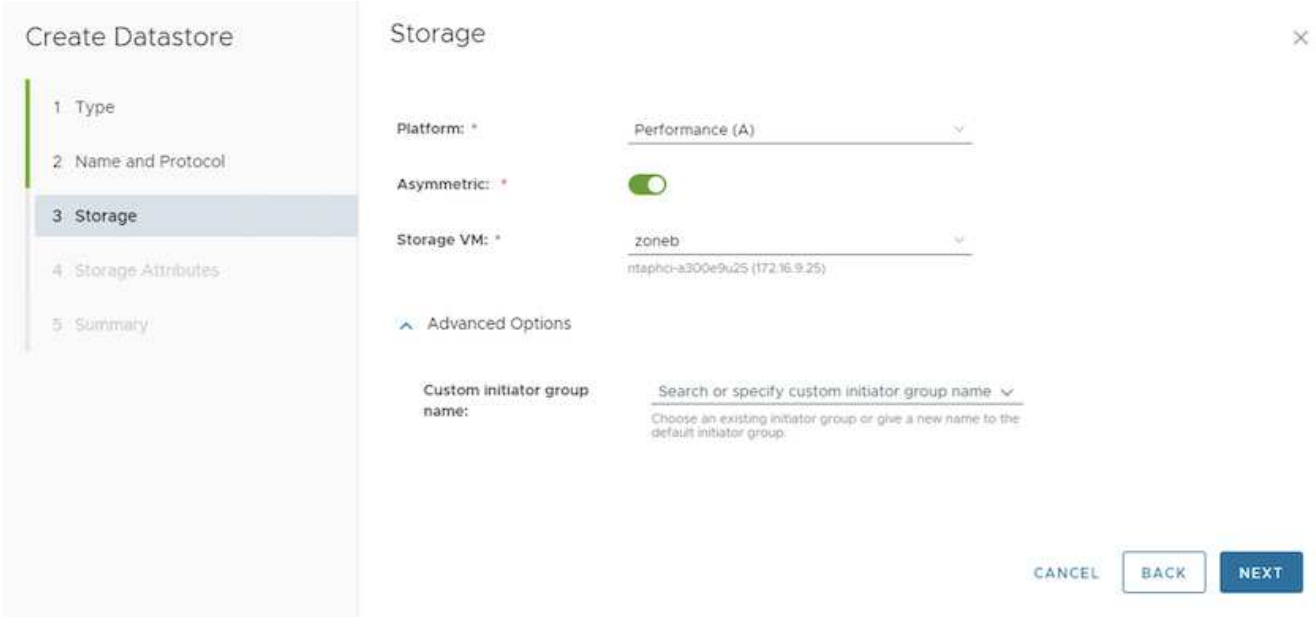
Se l'opzione vVol non è disponibile, verificare che il provider VASA sia registrato.



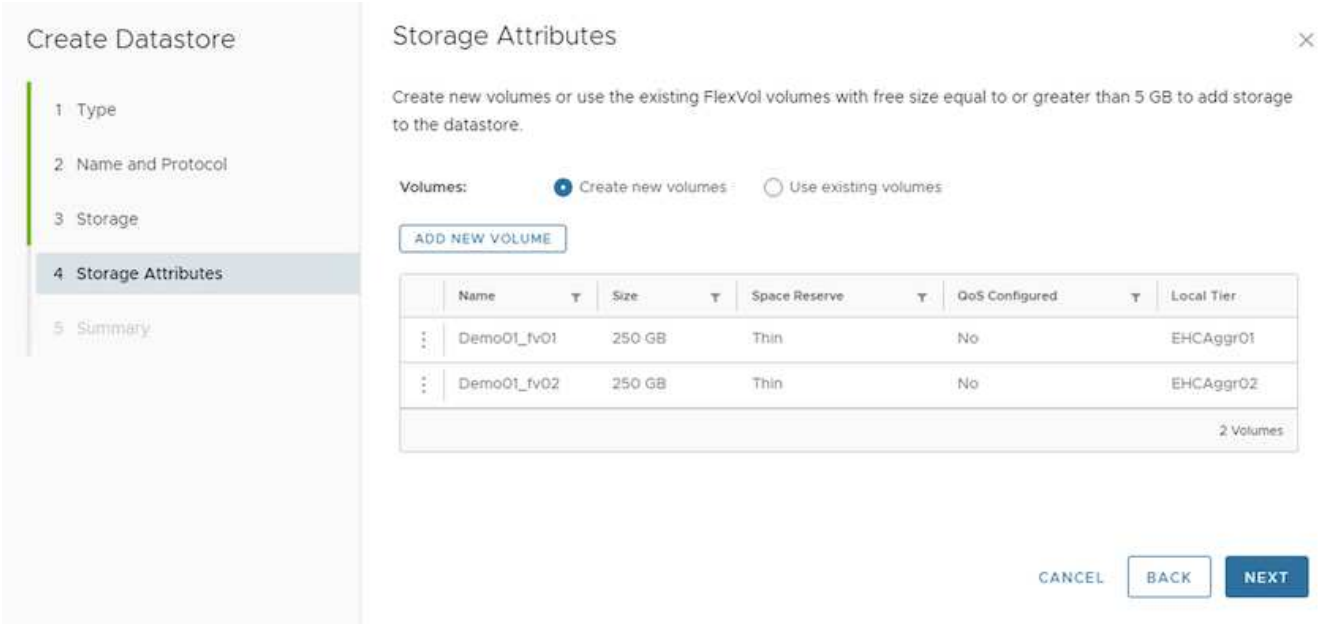
3. Fornire il nome del datastore vVol e selezionare il protocollo di trasporto.



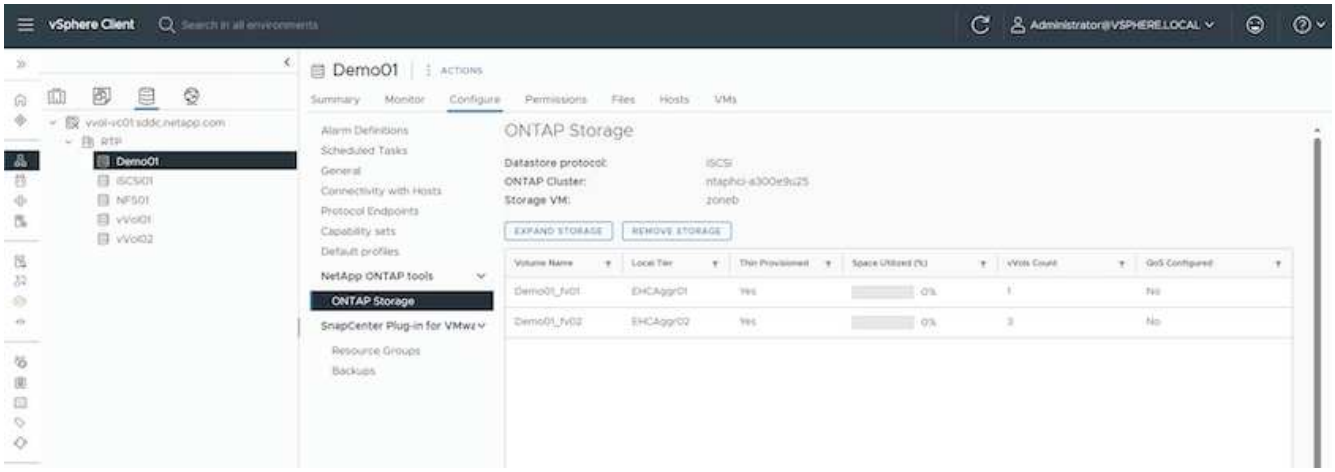
4. Selezionare Platform and Storage VM (piattaforma e VM di storage).



5. Creare o utilizzare volumi ONTAP esistenti per il datastore vVol.



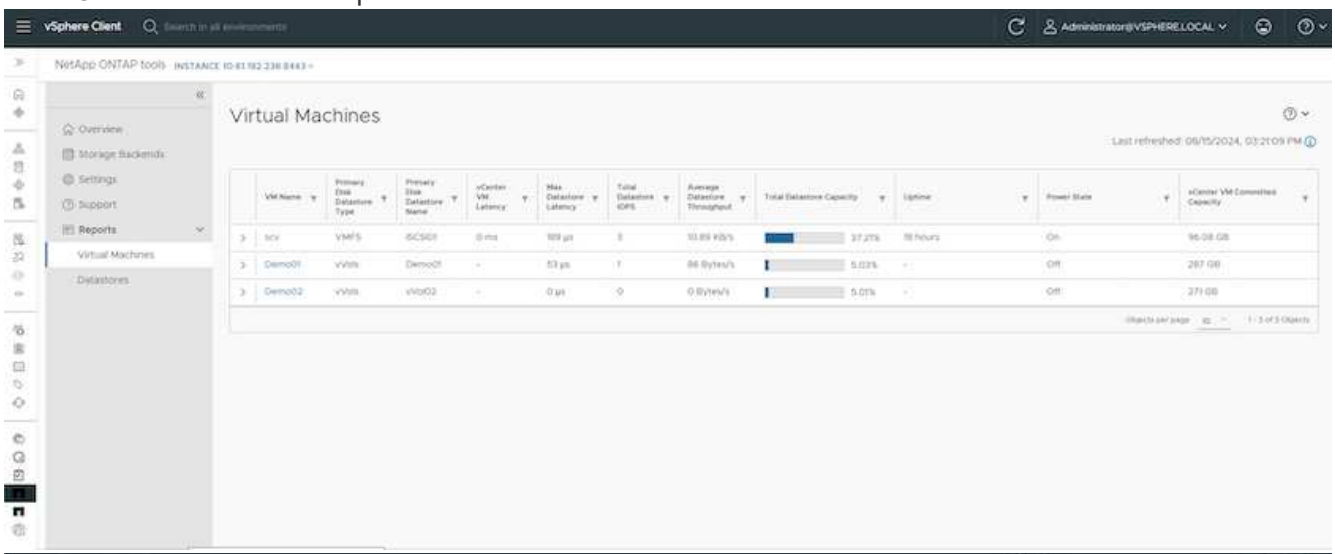
I volumi ONTAP possono essere visualizzati o aggiornati in un secondo momento dalla configurazione del datastore.

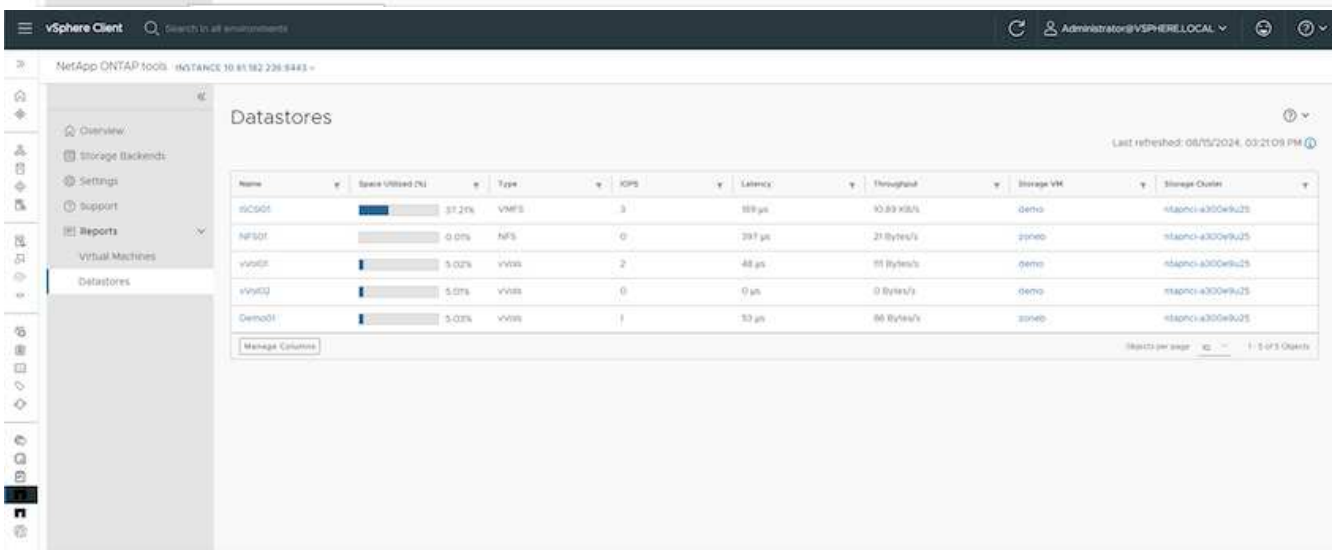


6. Una volta eseguito il provisioning del datastore vVol, questo può essere utilizzato in modo simile a

qualsiasi altro datastore.

7. I tool ONTAP forniscono il report VM e datastore.

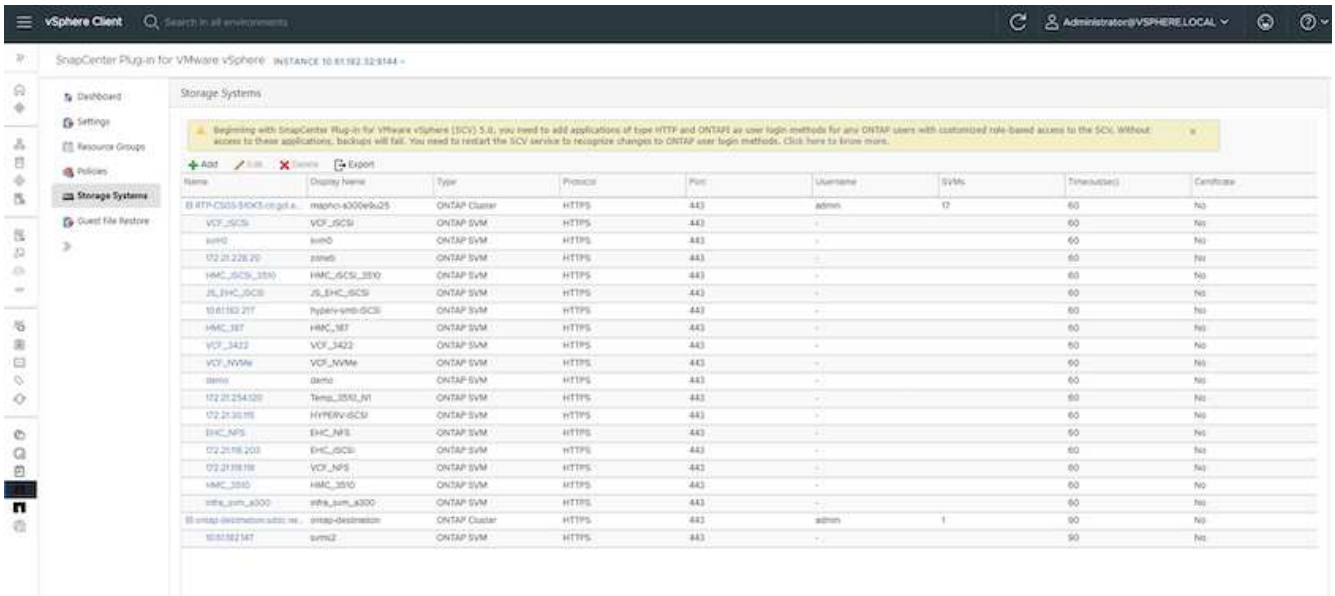




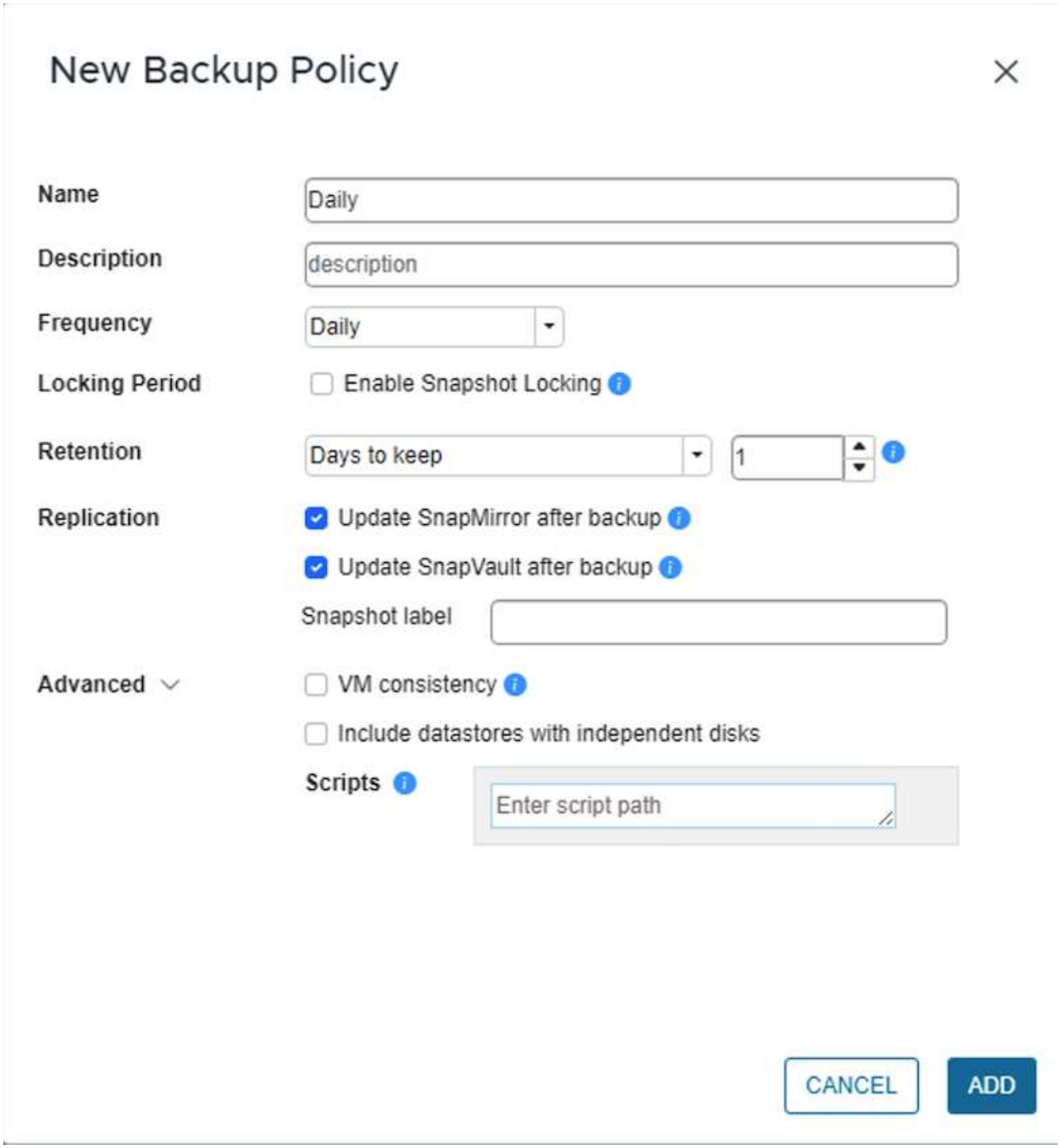
Data Protection delle VM su datastore vVol

Una panoramica sulla data Protection delle macchine virtuali nel datastore vVol è disponibile all'indirizzo "Protezione dei vVol".

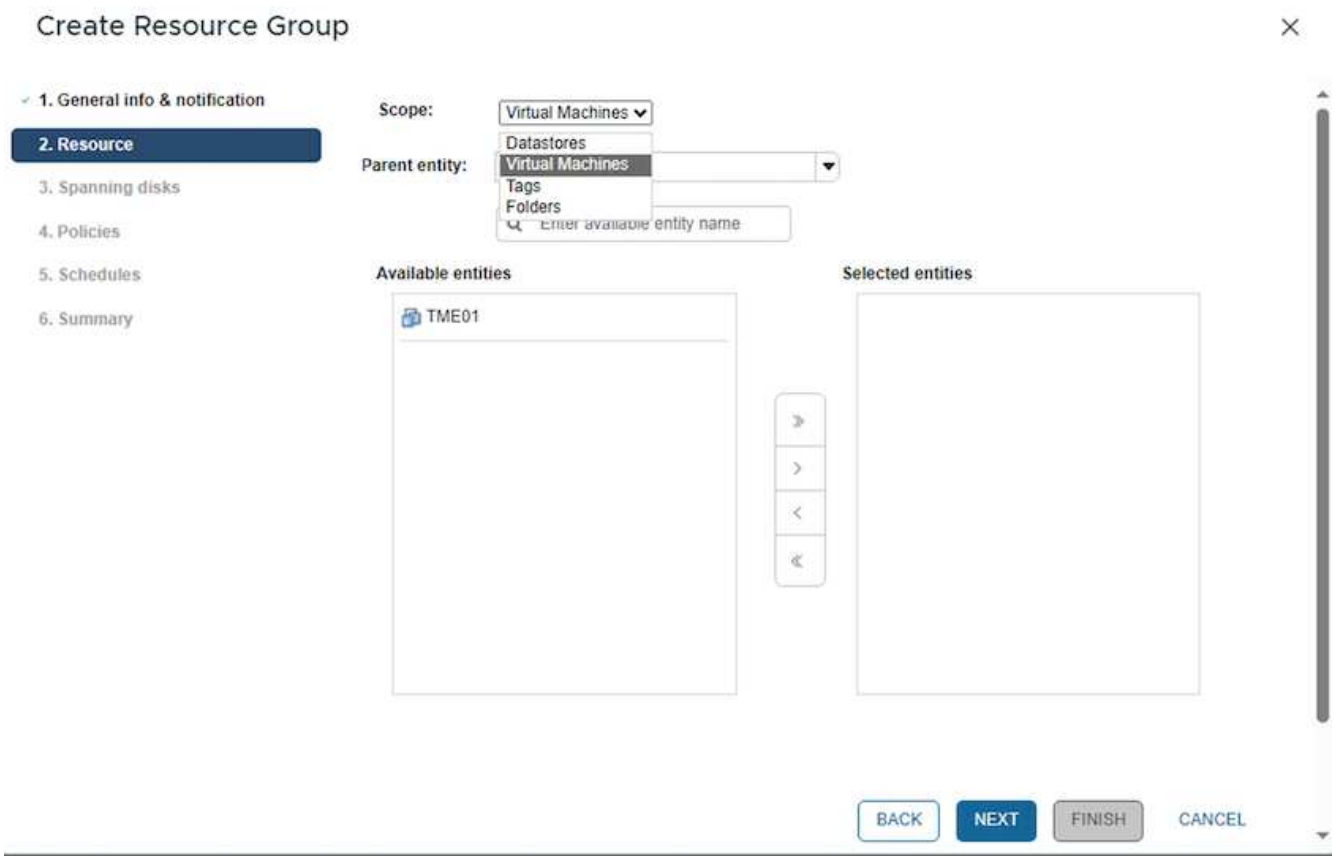
1. Registra il sistema storage che ospita il datastore vVol e qualsiasi partner di replica.



2. Creare un criterio con gli attributi richiesti.

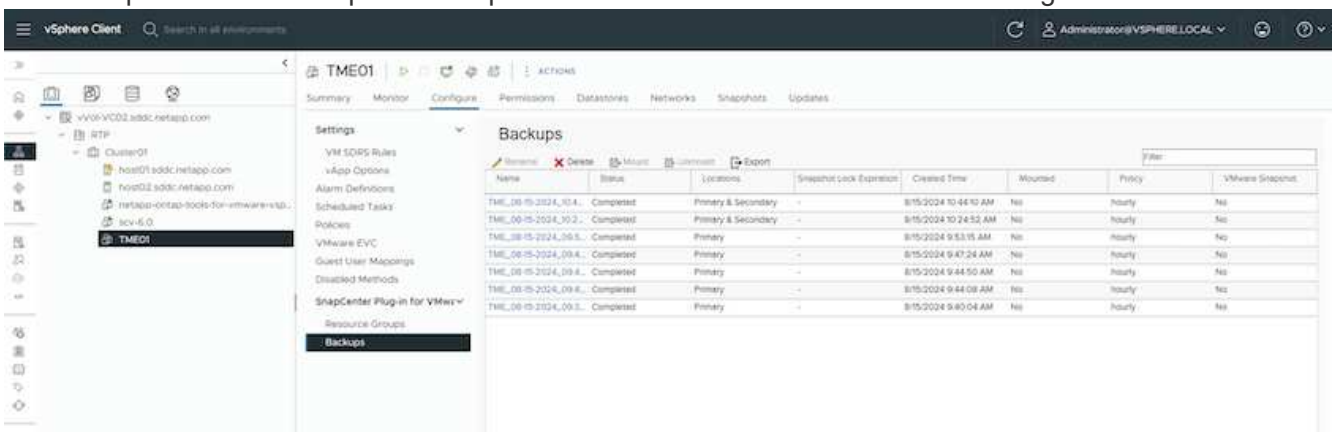


3. Creare un gruppo di risorse e associarlo ai criteri.



NOTA: Per il datastore vVol, è necessario proteggersi con VM, tag o cartella. Il datastore vVol non può essere incluso nel gruppo di risorse.

4. Lo stato specifico del backup della VM può essere visualizzato dalla scheda di configurazione.



5. La VM può essere ripristinata dalla sua posizione principale o secondaria.

Consulta i "Documentazione del plug-in SnapCenter"casi di utilizzo aggiuntivi.

Migrazione di macchine virtuali da datastore tradizionali a datastore vVol

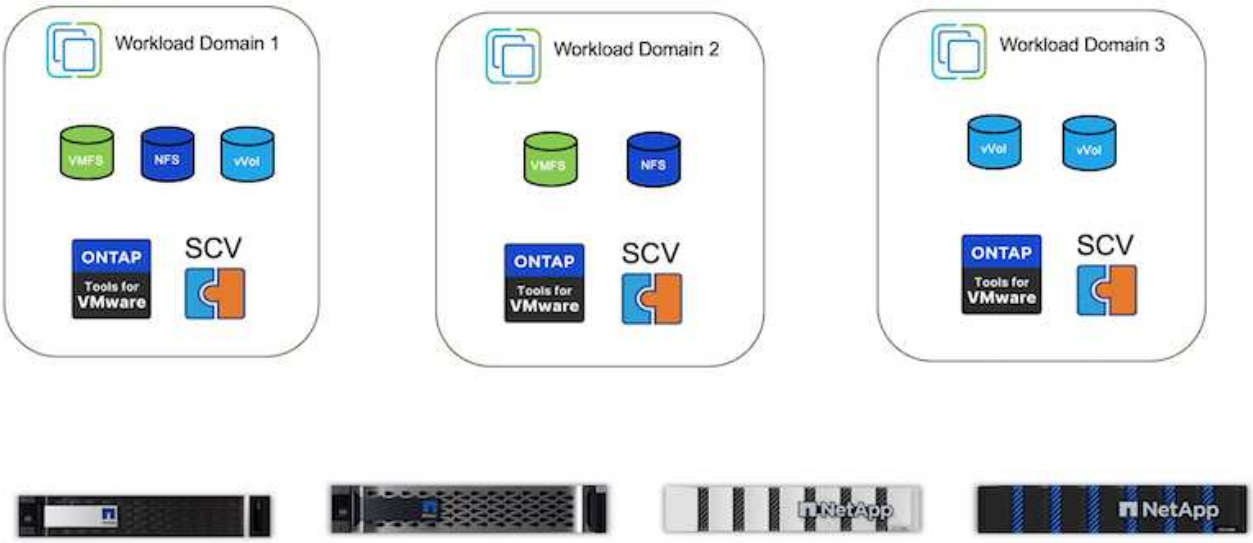
Per migrare le macchine virtuali da altri datastore in un datastore vVol, sono disponibili diverse opzioni in base allo scenario. Può variare da una semplice operazione di storage vMotion a una migrazione mediante HCX. Per "Migra le macchine virtuali nel datastore ONTAP"ulteriori dettagli, fare riferimento alla sezione.

Migrazione delle macchine virtuali tra datastore vVol

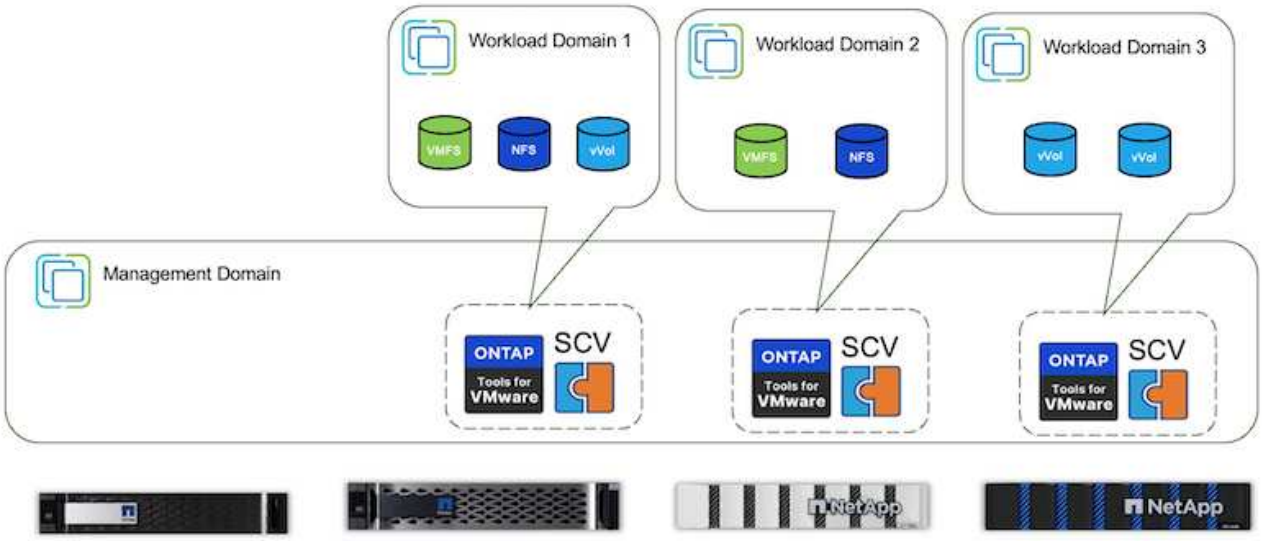
Per la migrazione di massa di macchine virtuali tra datastore vVol, controllare "Migra le macchine virtuali nel datastore ONTAP".

Esempio di architettura di riferimento

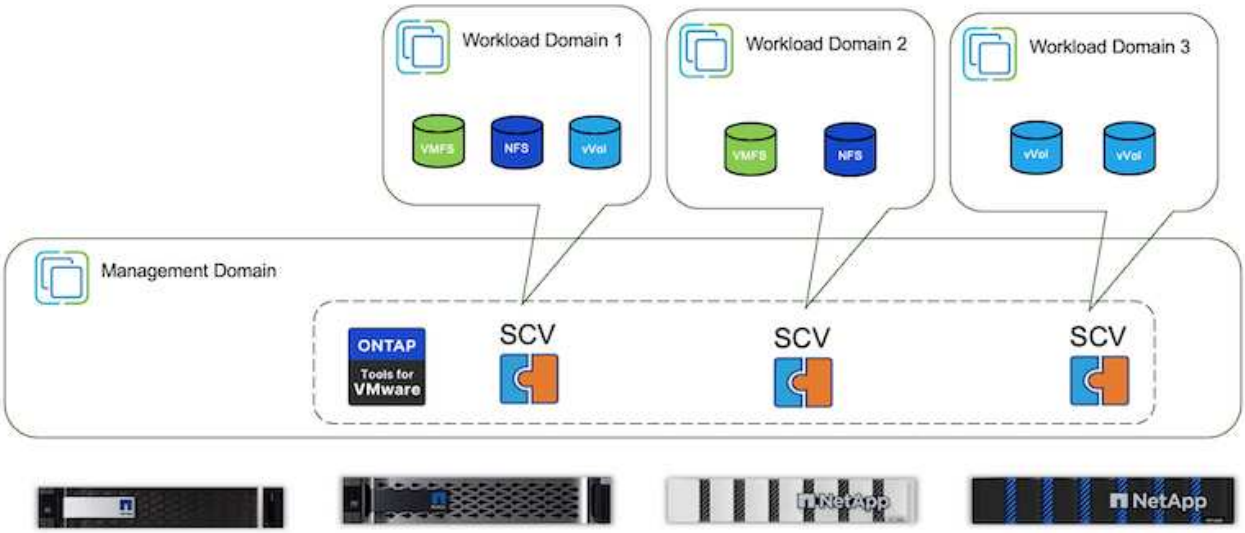
I tool ONTAP per VMware vSphere e SCV possono essere installati sullo stesso vCenter che sta gestendo o su un altro server vCenter. È meglio evitare di ospitare nel datastore vVol che sta gestendo.



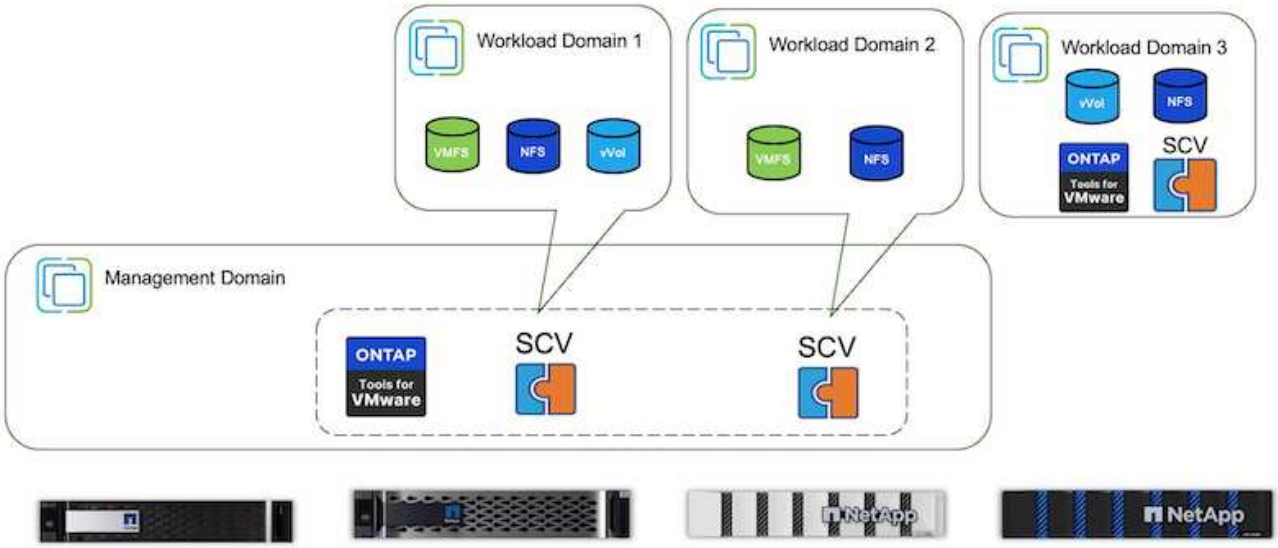
Poiché molti clienti ospitano i propri server vCenter su uno diverso invece che sulla gestione, un approccio simile viene consigliato anche per gli strumenti ONTAP e SCV.



Con i tool ONTAP 10.x, una singola istanza può gestire più ambienti vCenter. I sistemi storage sono registrati a livello globale con credenziali del cluster e le SVM sono assegnate a ogni tenant server vCenter.



È supportato anche un mix di modelli dedicati e condivisi.



Come iniziare

Se gli strumenti ONTAP non sono installati nel proprio ambiente, scaricarli da "Sito di supporto NetApp" e seguire le istruzioni disponibili all'indirizzo "Utilizzo di vVol con ONTAP".

Guida alla distribuzione per VMFS

Le soluzioni e le offerte di storage di NetApp consentono ai clienti di sfruttare appieno i vantaggi di un'infrastruttura virtualizzata. Con le soluzioni NetApp, i clienti possono implementare in modo efficiente un software di gestione dei dati completo garantendo funzionalità di automazione, efficienza, protezione dei dati e sicurezza per soddisfare efficacemente i più esigenti requisiti relativi alle performance. L'Unione del software ONTAP con VMware vSphere consente di ridurre i costi di licenza legati all'hardware host

e a VMware, garantire la protezione dei dati a costi inferiori e offrire performance costantemente elevate.

Introduzione

I carichi di lavoro virtualizzati sono mobili. Pertanto, gli amministratori utilizzano VMware Storage vMotion per spostare le macchine virtuali tra datastore VMFS (Virtual Machine file System), NFS o vVol, che risiedono tutti sullo stesso sistema storage ed esplorare così diversi approcci di storage se utilizzano un sistema all-flash o utilizzano i modelli ASA più recenti con l'innovazione SAN per una maggiore efficienza dei costi.

Il messaggio chiave in questo caso è che la migrazione a ONTAP migliora l'esperienza del cliente e le prestazioni delle applicazioni, offrendo al contempo la flessibilità per la migrazione dei dati e delle applicazioni tra FCP, iSCSI, NVMe/FC e NVMe/TCP. Per le aziende profondamente investite in VMware vSphere, l'utilizzo dello storage ONTAP è un'opzione conveniente date le attuali condizioni di mercato, che rappresenta un'opportunità unica. Le aziende di oggi si trovano di fronte a nuovi imperativi che un moderno approccio SAN può affrontare in modo semplice e rapido. Ecco alcuni dei modi in cui i clienti NetApp nuovi ed esistenti stanno aggiungendo valore con ONTAP.

- Efficienza dei costi: L'efficienza dello storage integrata consente a ONTAP di ridurre significativamente i costi dello storage. I sistemi NetApp ASA possono eseguire tutte le funzionalità di efficienza dello storage in produzione senza alcun impatto sulle performance. NetApp semplifica il piano per questi benefici di efficienza garantendo i livelli di efficienza più efficaci sul mercato.
- Protezione dei dati - il software SnapCenter che utilizza le snapshot offre protezione avanzata dei dati a livello di VM e applicazione per varie applicazioni aziendali implementate in una configurazione VM.
- Sicurezza: Utilizza le copie Snapshot per la protezione da malware e ransomware. Migliora la protezione rendendo immutabili le copie snapshot utilizzando il blocco delle istantanee e il software NetApp SnapLock®.
- Cloud - ONTAP fornisce un'ampia gamma di opzioni di cloud ibrido che consentono alle aziende di combinare cloud pubblici e privati, offrendo flessibilità e riducendo l'overhead di gestione dell'infrastruttura. Il supporto supplementare per datastore basato sulle offerte ONTAP consente di utilizzare VMware Cloud su Azure, AWS e Google per l'implementazione ottimizzata del TCO, la data Protection e la business continuity, evitando al contempo dipendenza dal vendor.
- Flessibilità - ONTAP è ben attrezzata per soddisfare le esigenze in rapida evoluzione delle aziende moderne. Con ONTAP ONE, tutte queste funzionalità sono fornite di serie con un sistema ONTAP senza costi aggiuntivi.

Dimensionare correttamente e ottimizzare

Con le imminenti modifiche alle licenze, le organizzazioni stanno affrontando in modo proattivo il potenziale aumento del TCO (Total Cost of Ownership). Stanno ottimizzando strategicamente la propria infrastruttura VMware mediante un'aggressiva gestione delle risorse e un corretto dimensionamento per ottimizzare l'utilizzo delle risorse e ottimizzare la pianificazione della capacità. Grazie all'uso efficace di strumenti specializzati, le organizzazioni possono identificare e recuperare in modo efficiente le risorse sprecate, riducendo di conseguenza il numero di core e le spese di licenza complessive. È importante sottolineare che molte organizzazioni stanno già integrando queste pratiche nelle valutazioni del cloud, dimostrando come questi processi e strumenti siano in grado di ridurre in modo efficace i problemi di costo in ambienti on-premise ed eliminare le spese di migrazione superflue in hypervisor alternativi.

Dispositivo per la valutazione del TCO

NetApp ha creato un semplice dispositivo per la valutazione del TCO che fungerebbe da pietra miliare nell'avvio di questo percorso di ottimizzazione. Lo strumento di valutazione del TCO utilizza RVtools o metodi

di input manuali per progettare facilmente il numero di host necessari per la data implementazione e calcolare i risparmi per ottimizzare l'implementazione utilizzando i sistemi storage NetApp ONTAP. Tieni presente che questa è la pietra a gradini.

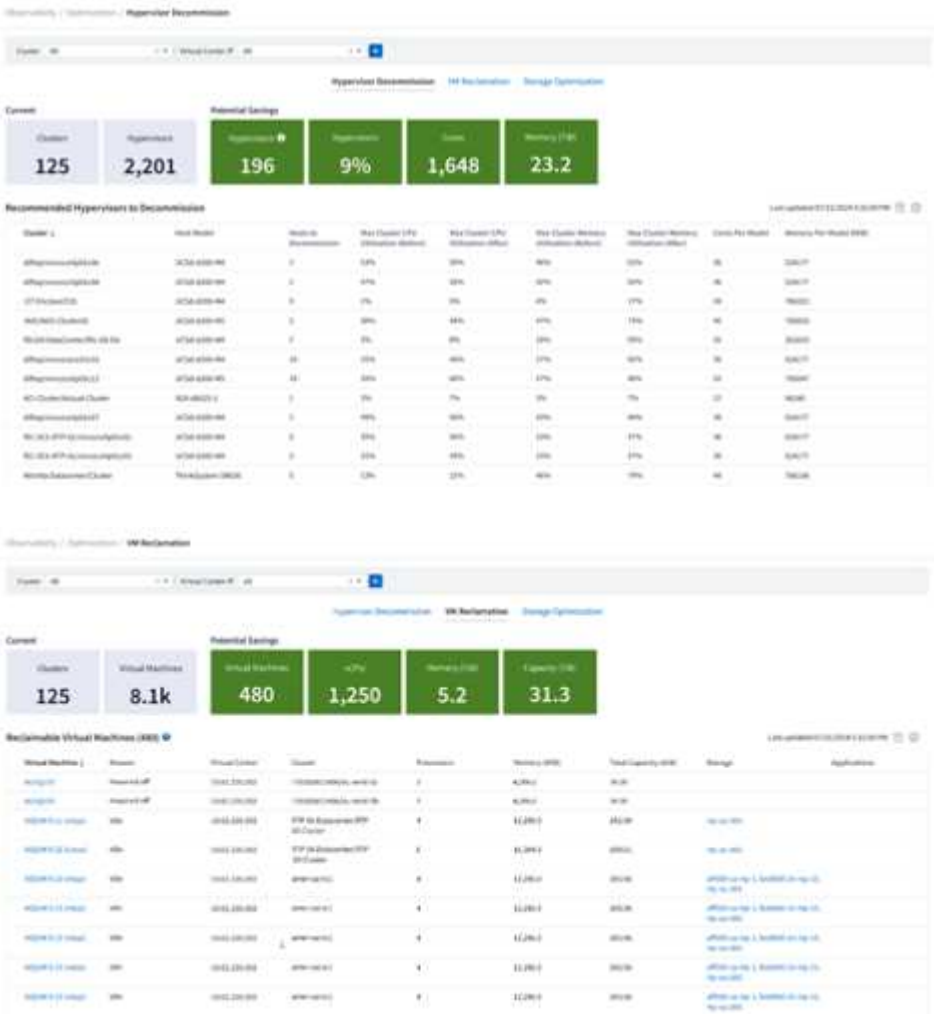
> Il tool per la valutazione del TCO è accessibile solo ai partner e ai team sul campo di NetApp. Collabora con gli account team di NetApp per valutare il tuo ambiente esistente.

Ecco uno screenshot dello strumento per la valutazione del TCO.

Cloud Insights

Una volta che lo stimatore mostra i risparmi possibili (situazione tipica di qualsiasi organizzazione), è giunto il momento di analizzare a fondo i profili io del carico di lavoro nelle macchine virtuali utilizzando metriche in tempo reale. Per questo motivo, NetApp fornisce Cloud Insights. Attraverso analisi e consigli dettagliati per il recupero delle VM, Cloud Insights può aiutare le aziende a prendere decisioni informate sull'ottimizzazione del loro ambiente VM. Consente di identificare dove recuperare le risorse o disattivare gli host con un impatto minimo sulla produzione, aiutando le aziende a gestire le modifiche apportate dall'acquisizione di VMware da parte di Broadcom in modo intelligente e strategico. In altre parole, Cloud Insight aiuta le imprese a sottrarre le emozioni alle decisioni. Invece di reagire al cambiamento con panico o frustrazione, possono utilizzare le informazioni fornite dallo strumento Cloud Insights per prendere decisioni razionali e strategiche che bilanciano l'ottimizzazione dei costi con efficienza delle operazioni e produttività.

Di seguito sono riportati gli screenshot di Cloud Insights.



Condurre valutazioni regolari per individuare le risorse sottoutilizzate, aumentare la densità delle macchine virtuali e utilizzare i cluster VMware per controllare i costi crescenti associati alle nuove licenze in abbonamento. È consigliabile ridurre il numero di core per CPU a 16 per gli acquisti di nuovi server, in modo da allinearlo alle modifiche dei modelli di licenza VMware.

Con NetApp, esegui una corretta dimensionamento dei tuoi ambienti virtualizzati e introduci performance di storage flash convenienti, assieme a soluzioni di gestione dei dati semplificate e ransomware, per garantire che le organizzazioni siano preparate per il nuovo modello di abbonamento, ottimizzando al contempo le risorse IT attualmente in uso.

Strumenti NetApp ONTAP per VMware vSphere

Per migliorare e semplificare ulteriormente l'integrazione di VMware, NetApp offre diversi tool OFFTAP che è possibile utilizzare con NetApp ONTAP e VMware vSphere per gestire in modo efficiente gli ambienti virtualizzati. In questa sezione verranno illustrati i tool ONTAP per VMware. Gli strumenti ONTAP per VMware vSphere 10 forniscono un set completo di strumenti per la gestione del ciclo di vita delle macchine virtuali, semplificando la gestione dello storage, migliorando le funzioni di efficienza, migliorando la disponibilità e riducendo i costi di storage e l'overhead operativo. Questi tool si integrano perfettamente con l'ecosistema VMware, facilitando il provisioning dei datastore e offrendo una protezione di base per le macchine virtuali. La release 10.x degli strumenti ONTAP per VMware vSphere comprende microservizi basati su eventi scalabili orizzontalmente implementati come Open Virtual Appliance (OVA), seguendo le Best practice per il provisioning dei datastore e ottimizzando le impostazioni dell'host ESXi per ambienti di storage sia NFS che a blocchi. Considerando questi vantaggi, si consiglia di utilizzare OTV come Best practice per i sistemi che

eseguono il software ONTAP.

Per iniziare

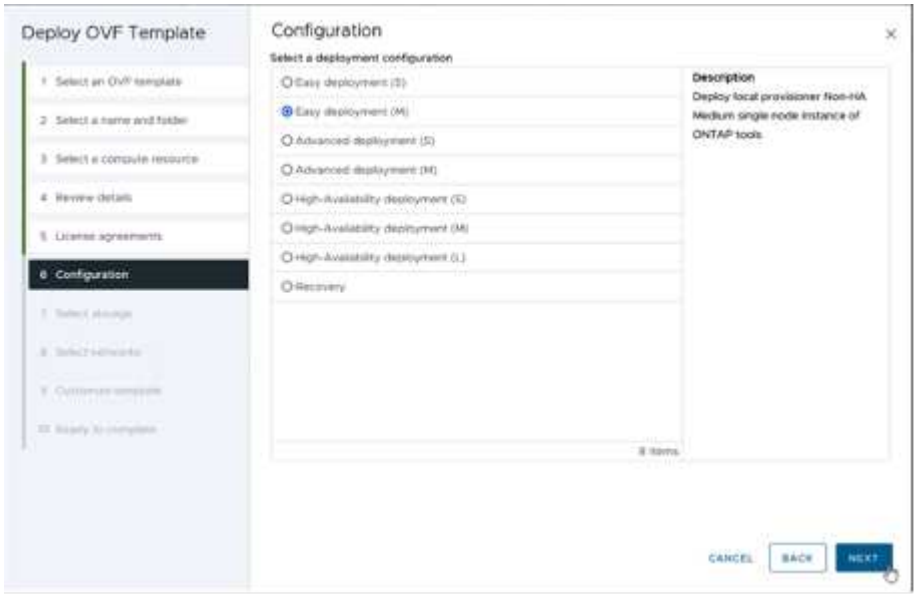
Prima di distribuire e configurare gli strumenti ONTAP per VMware, verificare che siano soddisfatti i prerequisiti. Al termine, implementa una configurazione a nodo singolo.

> Sono richiesti tre indirizzi IP per l'implementazione - un indirizzo IP per il bilanciamento del carico, un indirizzo IP per il piano di controllo di Kubernetes e uno per il nodo.

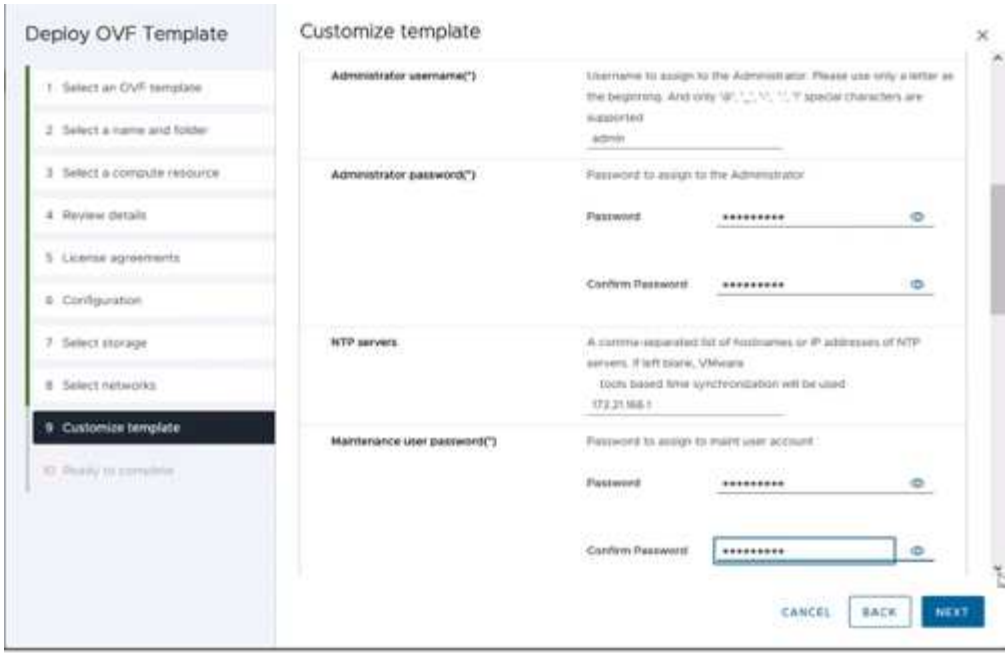
Fasi

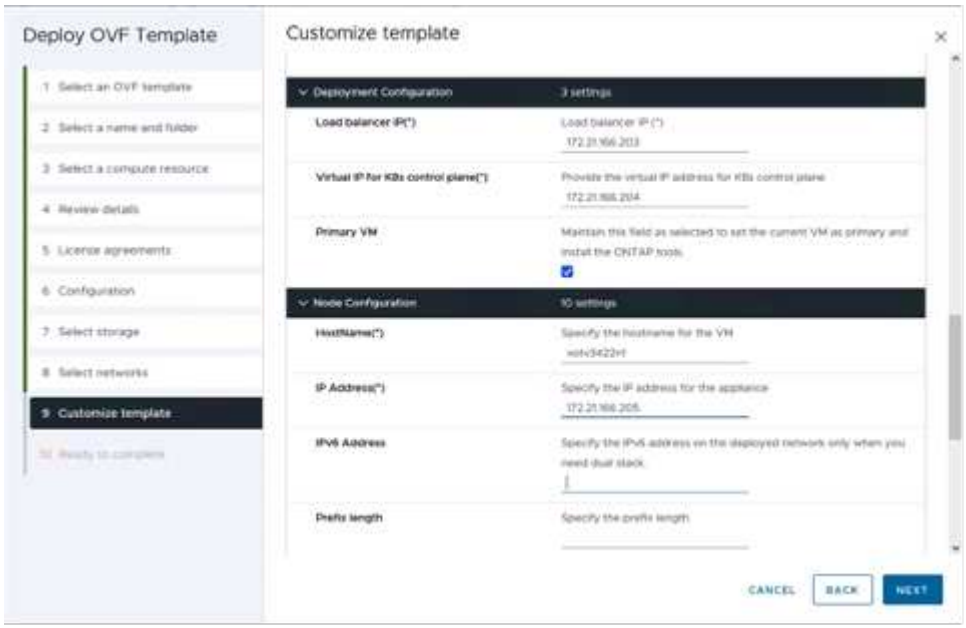
1. Accedere al server vSphere.
2. Passare al cluster o all'host in cui si desidera distribuire l'OVA.
3. Fare clic con il pulsante destro del mouse sulla posizione desiderata e selezionare Deploy OVF template (implementa modello OVF).
   a. Immettere l'URL per il file .ova o navigare alla cartella in cui è stato salvato il file .ova, quindi selezionare Avanti.
4. Selezionare un nome, una cartella, un cluster/host per la macchina virtuale e selezionare Avanti.
5. Nella finestra di configurazione, selezionare la configurazione facile deployment(S), deployment(M) o deployment(S) avanzato o deployment(M) avanzato.

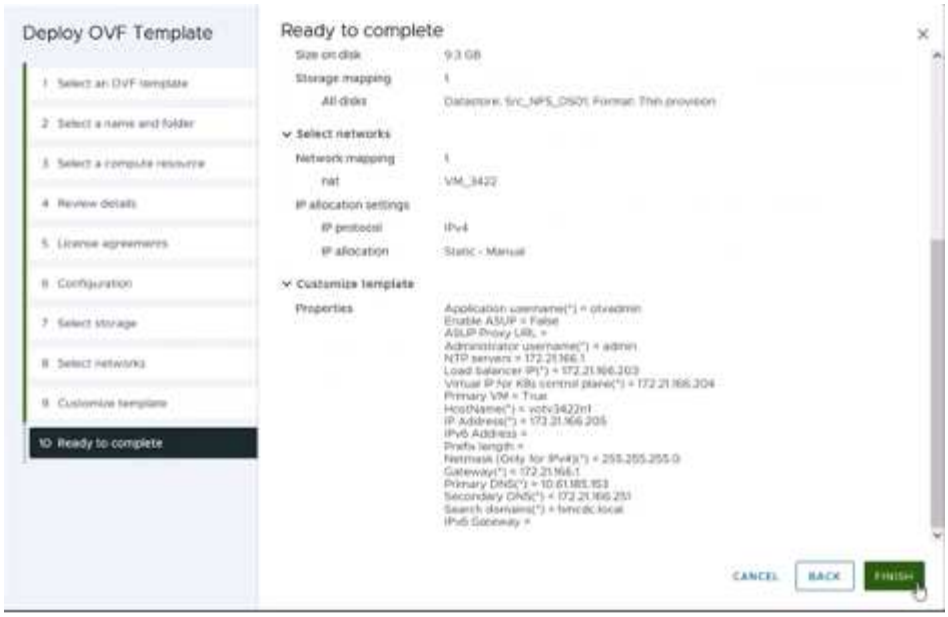
> In questa procedura dettagliata viene utilizzata l'opzione di distribuzione semplificata.



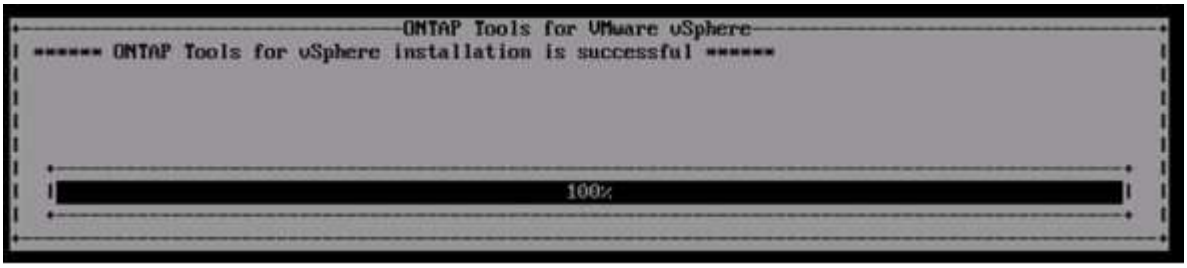
6. Scegliere il datastore per implementare l'OVA e la rete di origine e di destinazione. Al termine, selezionare Avanti.
7. È ora di personalizzare il modello > finestra di configurazione del sistema.

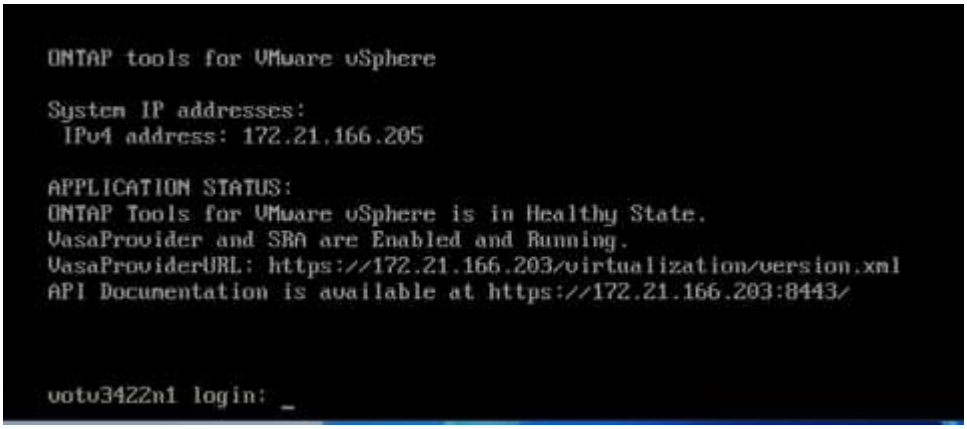

Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete
Customize template
Administrator username(*)
admin
Administrator password(*)
Password to assign to the Administrator
Password
Confirm Password
NTP servers
172.21.166.1
Maintenance user password(*)
Password to assign to maint user account
Password
Confirm Password
CANCEL
BACK
NEXT


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete
Customize template
Deployment Configuration
3 settings
Load balancer IP(*)
Load balancer IP (*)
172.21.166.203
Virtual IP for K8s control plane(*)
Provide the virtual IP address for K8s control plane
172.21.166.204
Primary VM
Maintain this field as selected to set the current VM as primary and install the ONTAP tools.
Node Configuration
10 settings
HostName(*)
Specify the hostname for the VM
IP Address(*)
Specify the IP address for the appliance
172.21.166.205
IPv6 Address
Specify the IPv6 address on the deployed network only when you need dual stack.
Prefix length
Specify the prefix length
CANCEL
BACK
NEXT



Una volta completata l'installazione, la console Web mostra lo stato degli strumenti ONTAP per VMware vSphere.

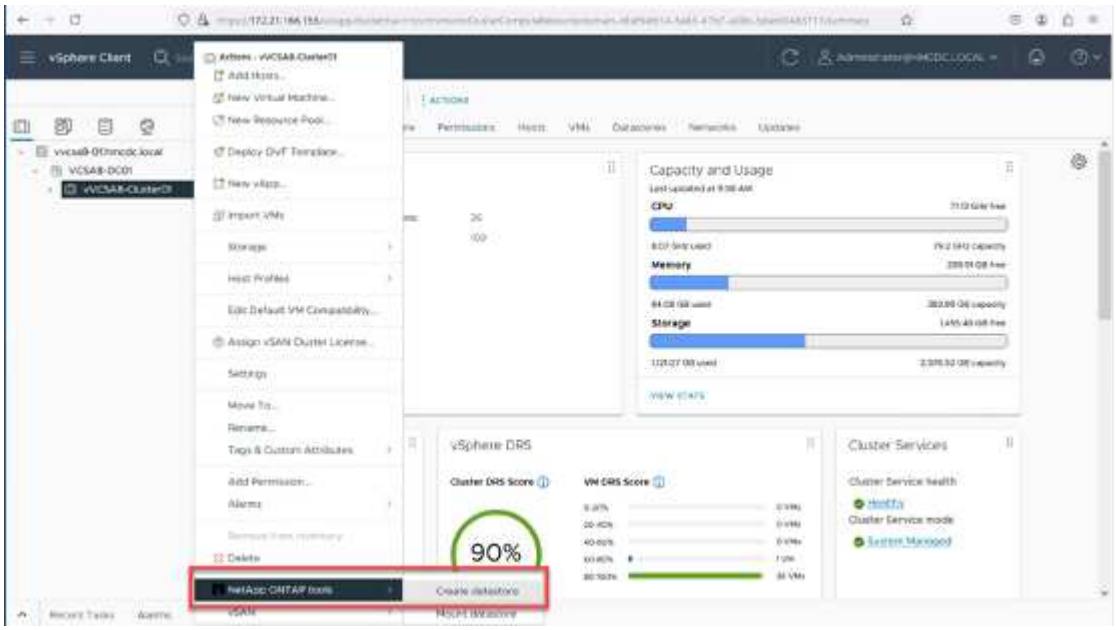




> La procedura guidata per la creazione di datastore supporta il provisioning di datastore VMFS, NFS e vVol.

Per questa procedura dettagliata, è giunto il momento di eseguire il provisioning di datastore VMFS basati su ISCSI.

1. Accedere al client vSphere utilizzando https://vcenterip/ui
2. Fare clic con il pulsante destro del mouse su un host o un cluster host o un datastore, quindi selezionare Strumenti NetApp ONTAP > Crea archivio dati.



3. Nel riquadro tipo, selezionare VMFS in tipo datastore.

4. Nel riquadro Nome e protocollo, immettere il nome del datastore, le dimensioni e le informazioni sul protocollo. Nella sezione Opzioni avanzate del riquadro, selezionare il cluster di datastore se si desidera aggiungere questo datastore.

5. Selezionare piattaforma e VM di archiviazione nel riquadro archiviazione. Specificare il nome del gruppo iniziatore personalizzato nella sezione Opzioni avanzate del riquadro (facoltativo). È possibile scegliere un igroup esistente per l'archivio dati o creare un nuovo igroup con un nome personalizzato.

6. Nel riquadro degli attributi dello storage, selezionare aggregate dal menu a discesa. Selezionare Space Reserve (riserva di spazio), Volume Options (opzione volume) e Enable QoS Options (attiva opzioni QoS) come richiesto dalla sezione Advanced Options (Opzioni avanzate).

7. Esaminare i dettagli del datastore nel riquadro Riepilogo e fare clic su fine. Il datastore VMFS viene creato e montato su tutti gli host.

Fai riferimento a questi link per il provisioning del datastore vVol, FC, NVMe/TCP.

Offload VAAI

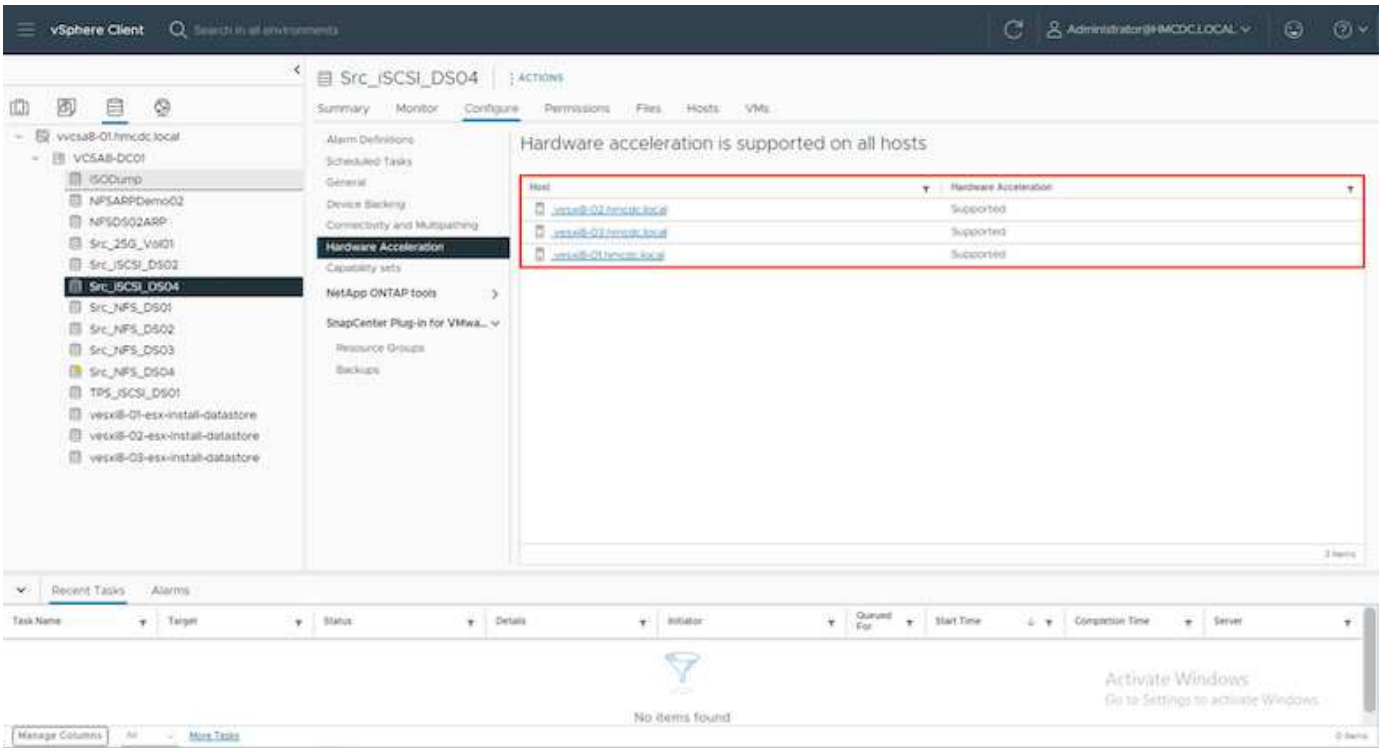
Le primitive VAAI vengono utilizzate nelle operazioni vSphere di routine, come creazione, cloning, migrazione, avvio e arresto delle macchine virtuali. Queste operazioni possono essere eseguite tramite il client vSphere per semplicità o dalla riga di comando per lo scripting o per ottenere tempi più precisi. VAAI per SAN è supportato nativamente da ESX. VAAI è sempre abilitato sui sistemi storage NetApp supportati e offre supporto nativo per le seguenti operazioni VAAI sullo storage SAN:

- Offload delle copie
- Blocco ATS (Atomic Test & Set)
- Scrivi lo stesso
- Gestione delle condizioni di spazio insufficiente
- Bonifica dello spazio

```
[root@vesxi8-02:~] esxcli storage core device vaai status get -d=naa.600a09805a506576495d576a57553455
naa.600a09805a506576495d576a57553455
   VAAI Plugin Name: VMW_VAAIP_NETAPP
   ATS Status: supported
   Clone Status: supported
   Zero Status: supported
   Delete Status: supported
```

Verificare che HardwareAcceleratedMove sia attivato tramite le opzioni di configurazione avanzate ESX.

Assicurarsi che il LUN abbia attivato la "allocazione dello spazio". Se non è attivata, attivare l'opzione ed eseguire nuovamente la scansione di tutti gli HBA.

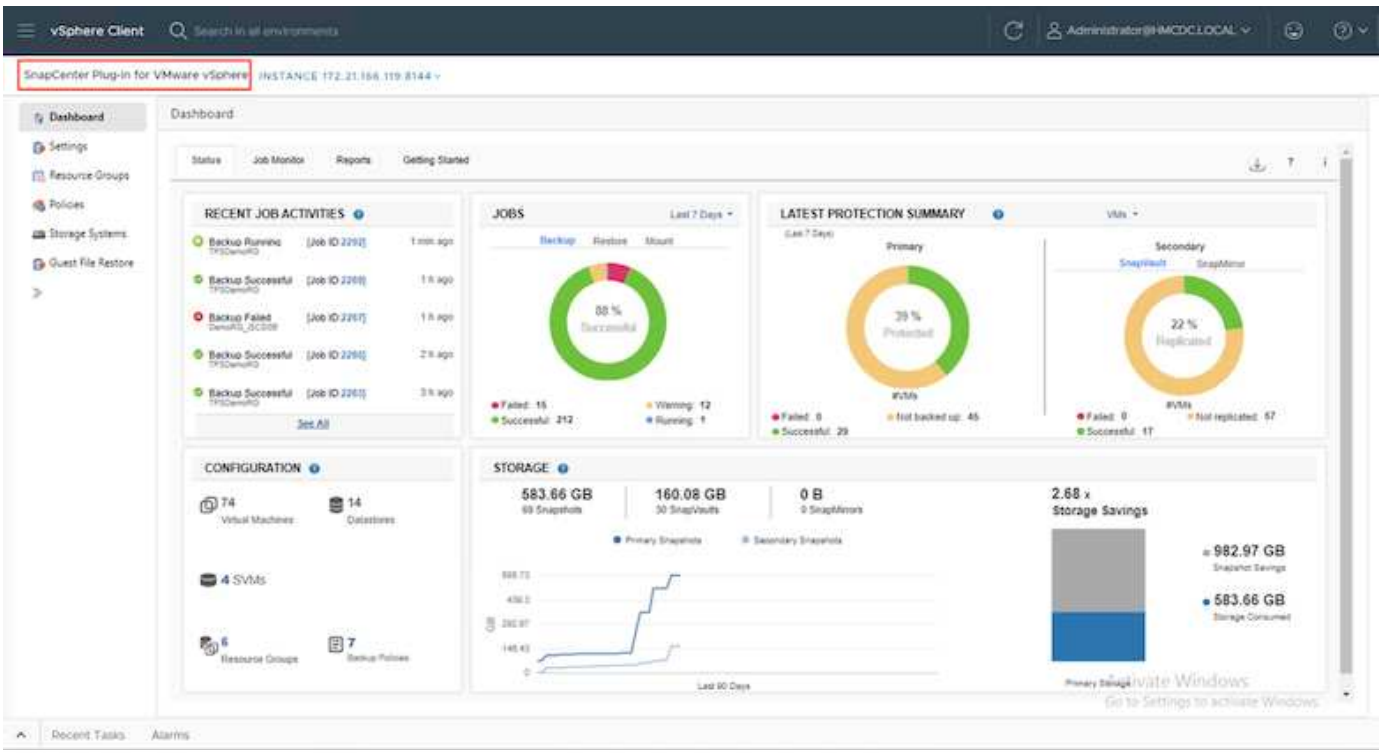


Questi valori sono facilmente impostabili utilizzando gli strumenti ONTAP per VMware vSphere. Dal dashboard Panoramica, accedere alla scheda di conformità dell'host ESXi e selezionare l'opzione Applica impostazioni consigliate. Nella finestra Apply Recommended host settings (Applica impostazioni host consigliate), selezionare gli host e fare clic su Next (Avanti) per applicare le impostazioni dell'host consigliate da NetApp.

Visualizzare le istruzioni dettagliate per "Host ESXi consigliato e altre impostazioni ONTAP".

Protezione dei dati

Un backup efficiente delle macchine virtuali sul datastore VMFS e un loro rapido recupero sono alcuni dei vantaggi chiave di ONTAP per vSphere. Grazie all'integrazione con vCenter, il software NetApp SnapCenter® offre un'ampia gamma di funzionalità di backup e ripristino per le macchine virtuali. Offre operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con i crash e coerenti con le VM per VM, datastore e VMDK. Funziona anche con SnapCenter Server per supportare operazioni di backup e ripristino basate sull'applicazione in ambienti VMware utilizzando i plug-in specifici delle applicazioni di SnapCenter. L'utilizzo delle copie Snapshot consente di eseguire copie rapide della macchina virtuale o del datastore senza alcun impatto sulle prestazioni e di utilizzare la tecnologia NetApp SnapMirror® o NetApp SnapVault® per la protezione dei dati off-site a lungo termine.



Il flusso di lavoro è semplice. Aggiungi sistemi di storage primario e SVM (e secondario se richiesto SnapMirror/SnapVault).

Passaggi di alto livello per l'implementazione e la configurazione:

1. Scarica SnapCenter per VMware Plug-in OVA
2. Accedere con le credenziali del client vSphere
3. Distribuire il modello OVF per avviare la procedura guidata di distribuzione di VMware e completare l'installazione
4. Per accedere al plug-in, selezionare Plug-in SnapCenter per VMware vSphere dal menu
5. Aggiungi archiviazione
6. Creare policy di backup
7. Creare gruppi di risorse
8. Gruppi di risorse di backup
9. Ripristinare l'intera macchina virtuale o un disco virtuale specifico

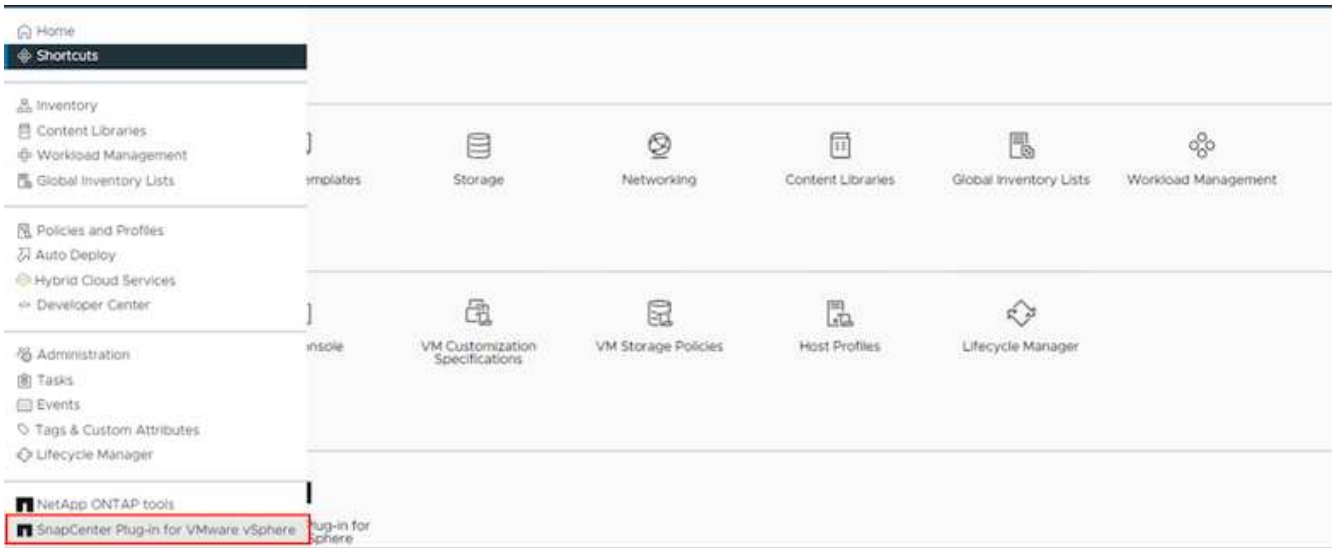
Configurazione del plug-in SnapCenter per VMware per macchine virtuali

Per proteggere le macchine virtuali e i datastore iSCSI che le ospitano, è necessario implementare il plug-in SnapCenter per VMware. Si tratta di una semplice importazione OVF.

La procedura di distribuzione è la seguente:

1. Scaricare l'appliance virtuale aperta (OVA) dal sito di supporto NetApp.
2. Accedere a vCenter.
3. In vCenter, fare clic con il pulsante destro del mouse su qualsiasi oggetto di inventario, ad esempio data center, cartella, cluster o host, e selezionare Deploy OVF Template (implementa modello OVF).
4. Seleziona le impostazioni giuste che includono storage, rete e personalizza il modello per aggiornare vCenter e le sue credenziali. Una volta esaminato, fare clic su fine.
5. Attendere il completamento delle attività di importazione e distribuzione di OVF.
6. Una volta implementato con successo il plug-in SnapCenter per VMware, questo verrà registrato in vCenter. Lo stesso può essere verificato accedendo a Administration > Client Plugin

7. Per accedere al plug-in, spostarsi sul sidecar sinistro della pagina del client web vCenter, selezionare Plug-in SnapCenter per VMware.



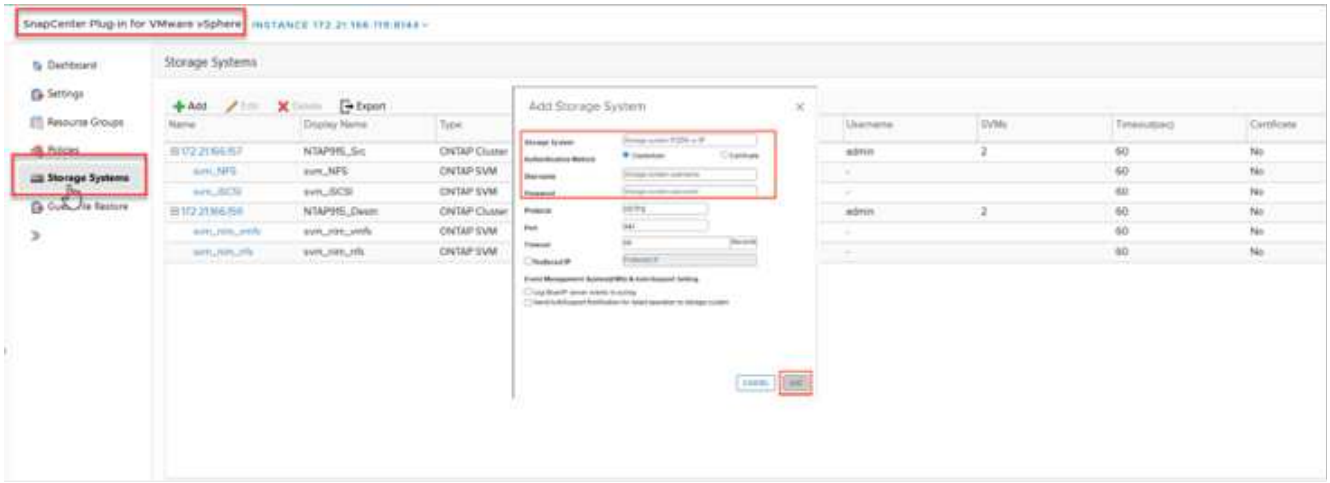
Aggiungere spazio di archiviazione, creare criteri e gruppo di risorse

Aggiunta di un sistema di storage

Il passaggio successivo consiste nell'aggiungere il sistema di archiviazione. L'endpoint di gestione del cluster o l'IP dell'endpoint di amministrazione della Storage Virtual Machine (SVM) deve essere aggiunto come sistema storage per il backup o il ripristino delle macchine virtuali. L'aggiunta di storage consente al plug-in SnapCenter per VMware di riconoscere e gestire le operazioni di backup e ripristino in vCenter.

Il processo è diretto.

1. Dal menu di navigazione a sinistra, selezionare Plug-in SnapCenter per VMware.
2. Selezionare Storage Systems (sistemi storage).
3. Selezionare Aggiungi per aggiungere le informazioni relative allo "storage".
4. Utilizzare le credenziali come metodo di autenticazione e immettere il nome utente e la relativa password, quindi fare clic su Aggiungi per salvare le impostazioni.



Creare un criterio di backup

Una strategia di backup completa include fattori come quando, cosa eseguire il backup e quanto tempo conservare i backup. Le snapshot possono essere distribuite su base oraria o giornaliera per eseguire il backup di interi datastore. Questo approccio non solo acquisisce i datastore, ma consente anche di eseguire il backup e il ripristino di macchine virtuali e VMDK all'interno di tali archivi dati.

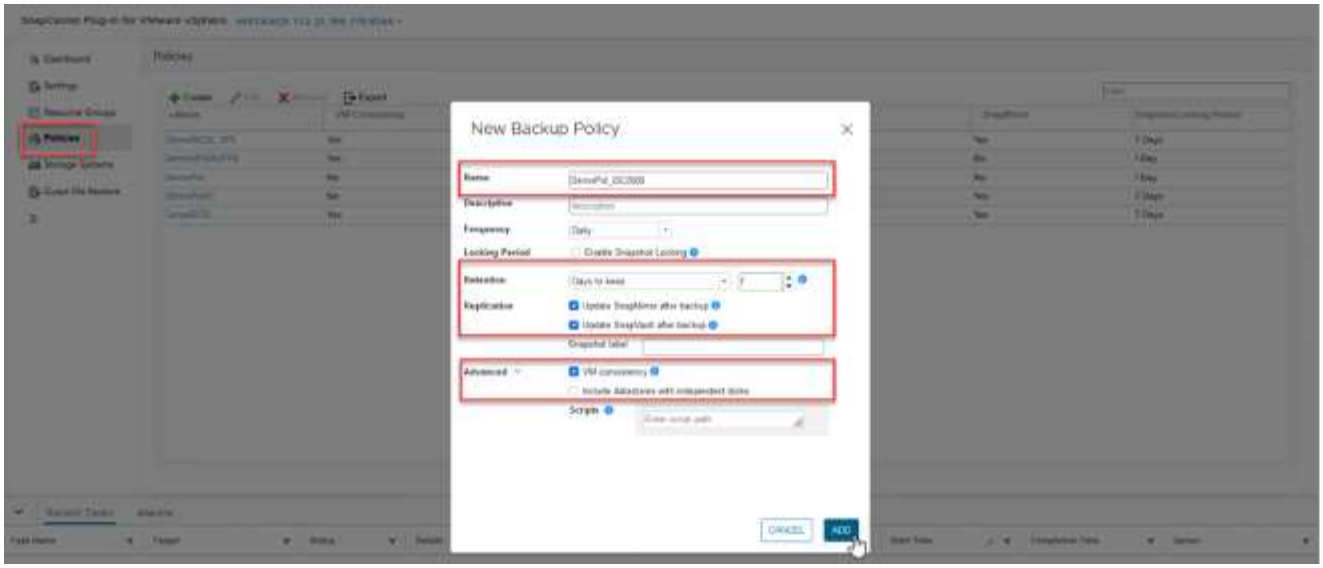
Prima di eseguire il backup delle macchine virtuali e dei datastore, è necessario creare un criterio di backup e un gruppo di risorse. I criteri di backup includono impostazioni quali i criteri di pianificazione e conservazione. Per creare un criterio di backup, procedere come segue.

1. Nel riquadro di sinistra del Navigator del plug-in SnapCenter per VMware, fare clic su Criteri.
2. Nella pagina Policy, fare clic su Create (Crea) per avviare la procedura guidata.

3. Nella pagina New Backup Policy (nuovo criterio di backup), immettere il nome del criterio.
4. Specificare la conservazione, le impostazioni di frequenza e la replica.

> Per replicare le copie Snapshot in un sistema storage secondario mirror o vault, le relazioni devono essere configurate in anticipo.

> Per consentire backup coerenti con le VM, è necessario installare ed eseguire gli strumenti VMware. Quando la casella coerenza VM è selezionata, le VM vengono prima disattivate, quindi VMware esegue uno snapshot coerente della VM (memoria esclusa), quindi il plug-in SnapCenter per VMware esegue l'operazione di backup, quindi le operazioni della VM vengono ripristinate.



Una volta creato il criterio, il passaggio successivo consiste nel creare il gruppo di risorse che definirà gli archivi dati iSCSI e le macchine virtuali di cui eseguire il backup. Una volta creato il gruppo di risorse, è il momento di attivare i backup.

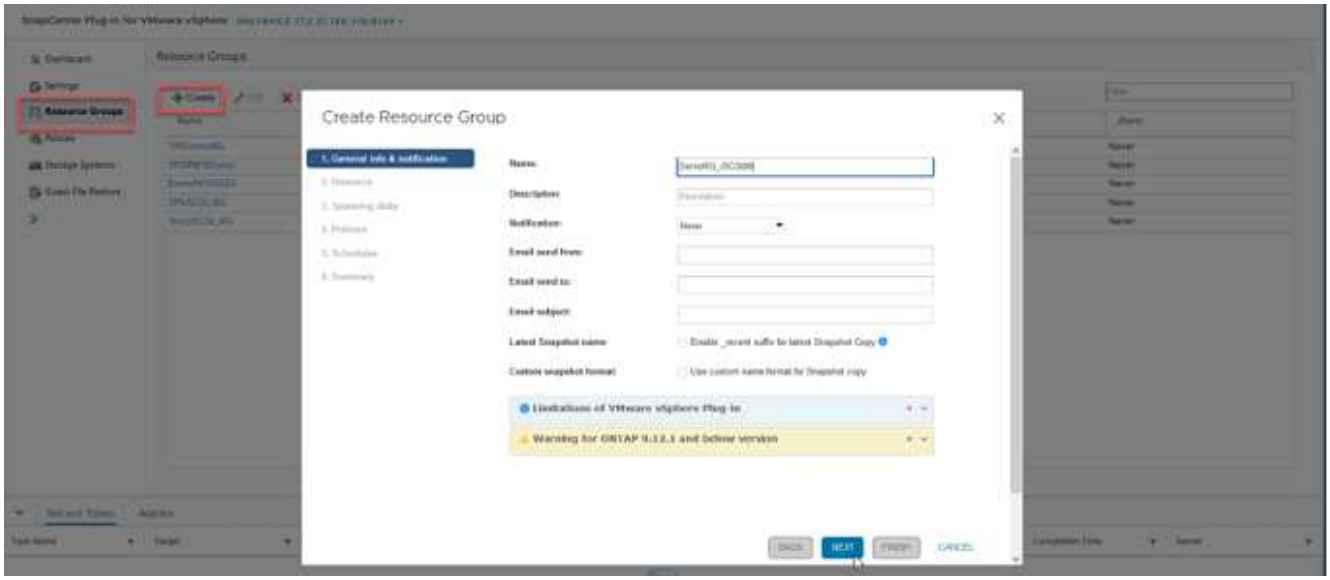
Crea gruppo di risorse

Un gruppo di risorse è il container per macchine virtuali e datastore da proteggere. Le risorse possono essere aggiunte o rimosse ai gruppi di risorse in qualsiasi momento.

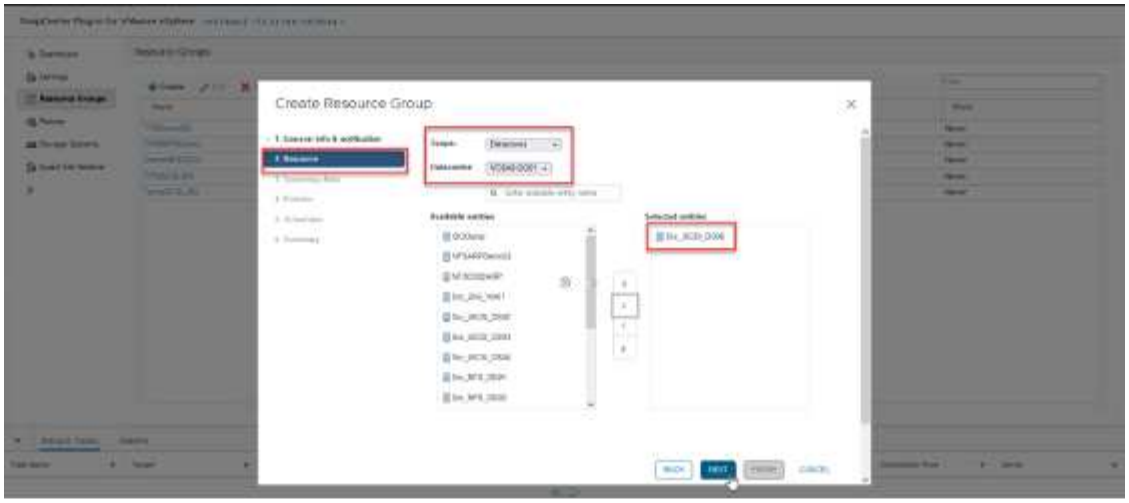
Per creare un gruppo di risorse, procedere come segue.

1. Nel riquadro di sinistra del Navigatore del plug-in SnapCenter per VMware, fare clic su gruppi di risorse.
2. Nella pagina gruppi di risorse, fare clic su Crea per avviare la procedura guidata.

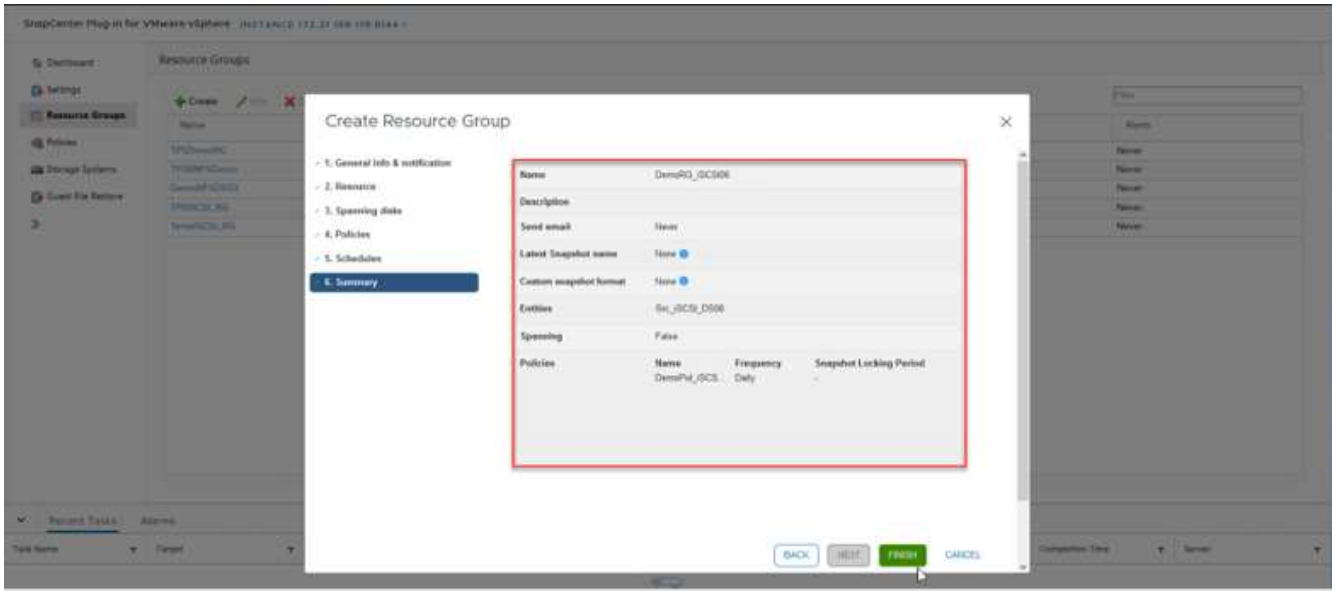
   Un'altra opzione per creare un gruppo di risorse consiste nel selezionare rispettivamente la singola macchina virtuale o il datastore e nel creare un gruppo di risorse.



3. Nella pagina risorse, selezionare l'ambito (macchine virtuali o datastore) e il data center.

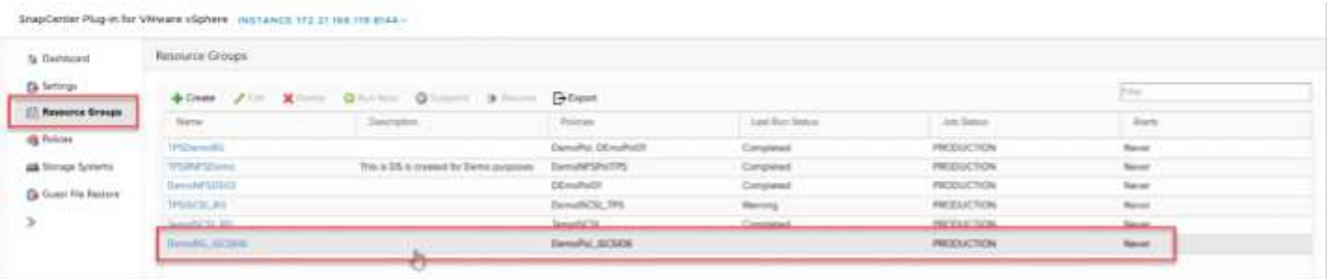


4. Nella pagina Spanning Disks (dischi di spanning), selezionare un'opzione per macchine virtuali con più VMDK in più datastore
5. Il passo successivo consiste nell'associare un criterio di backup. Selezionare un criterio esistente o creare un nuovo criterio di backup.
6. Nella pagina Pianificazioni, configurare la pianificazione di backup per ciascun criterio selezionato.



7. Una volta effettuate le selezioni appropriate, fare clic su Finish (fine).

   In questo modo si crea un nuovo gruppo di risorse e si aggiunge all'elenco dei gruppi di risorse.

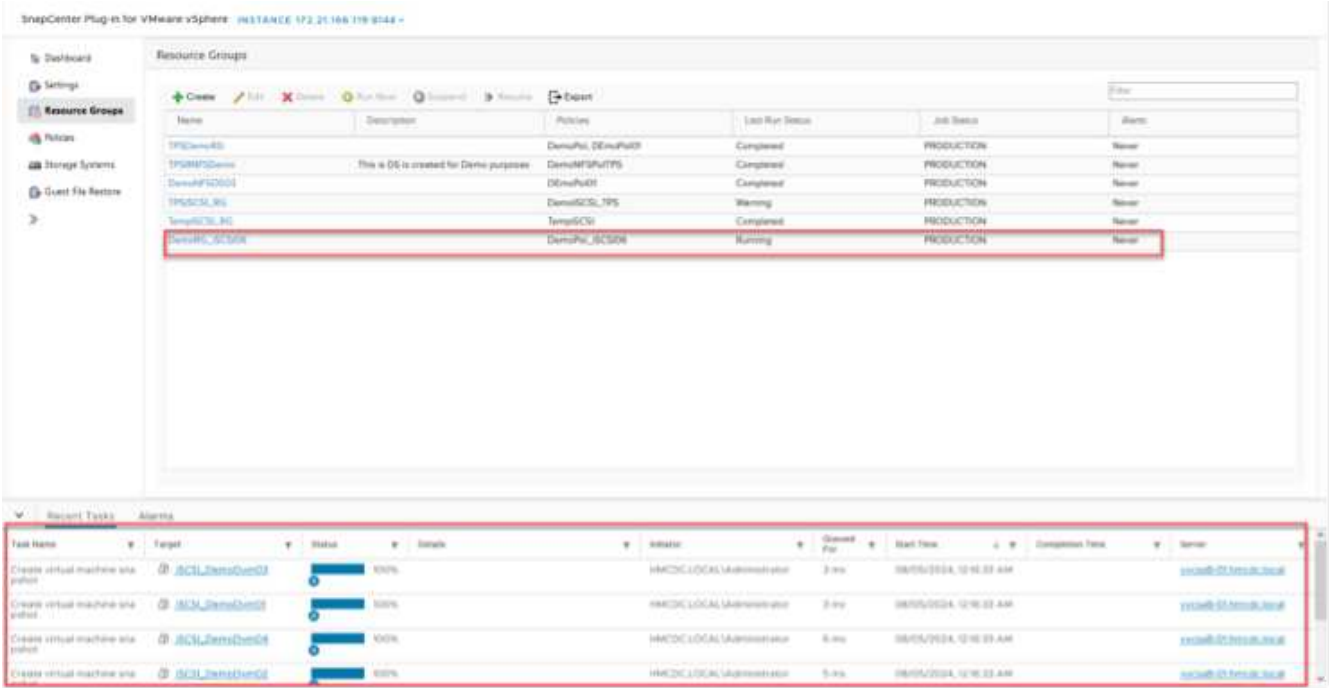


Eseguire il backup dei gruppi di risorse

Ora è il momento di attivare un backup. Le operazioni di backup vengono eseguite su tutte le risorse definite in un gruppo di risorse. Se un gruppo di risorse dispone di un criterio allegato e di una pianificazione configurata, i backup vengono eseguiti automaticamente in base alla pianificazione.

1. Nell'area di navigazione a sinistra della pagina del client Web vCenter, selezionare Plug-in SnapCenter per VMware > gruppi di risorse, quindi selezionare il gruppo di risorse designato. Selezionare Esegui ora per avviare il backup ad-hoc.

2. Se il gruppo di risorse dispone di più criteri configurati, selezionare il criterio per l'operazione di backup nella finestra di dialogo Esegui backup ora.
3. Selezionare OK per avviare il backup.

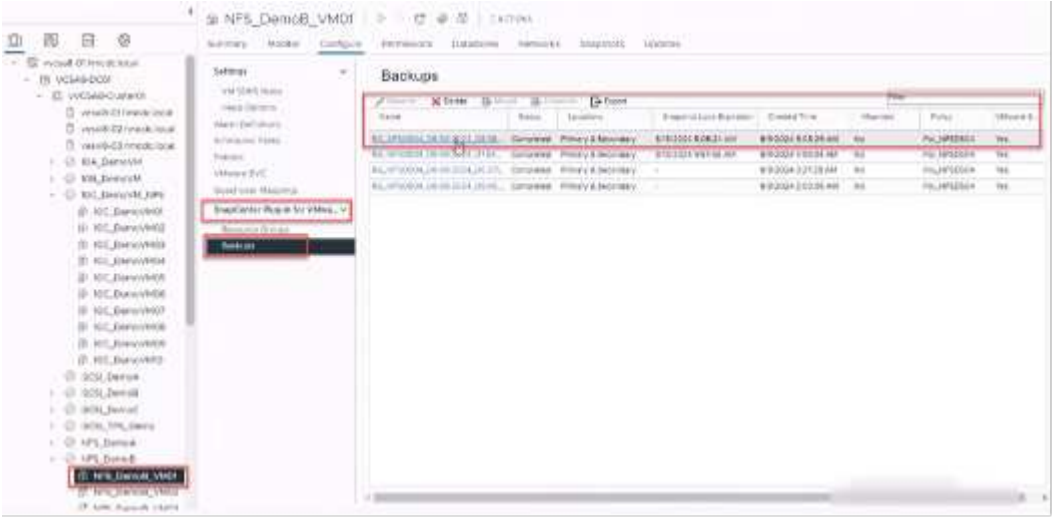


Monitorare l'avanzamento dell'operazione selezionando attività recenti nella parte inferiore della finestra o in Job Monitor del dashboard per ulteriori dettagli.

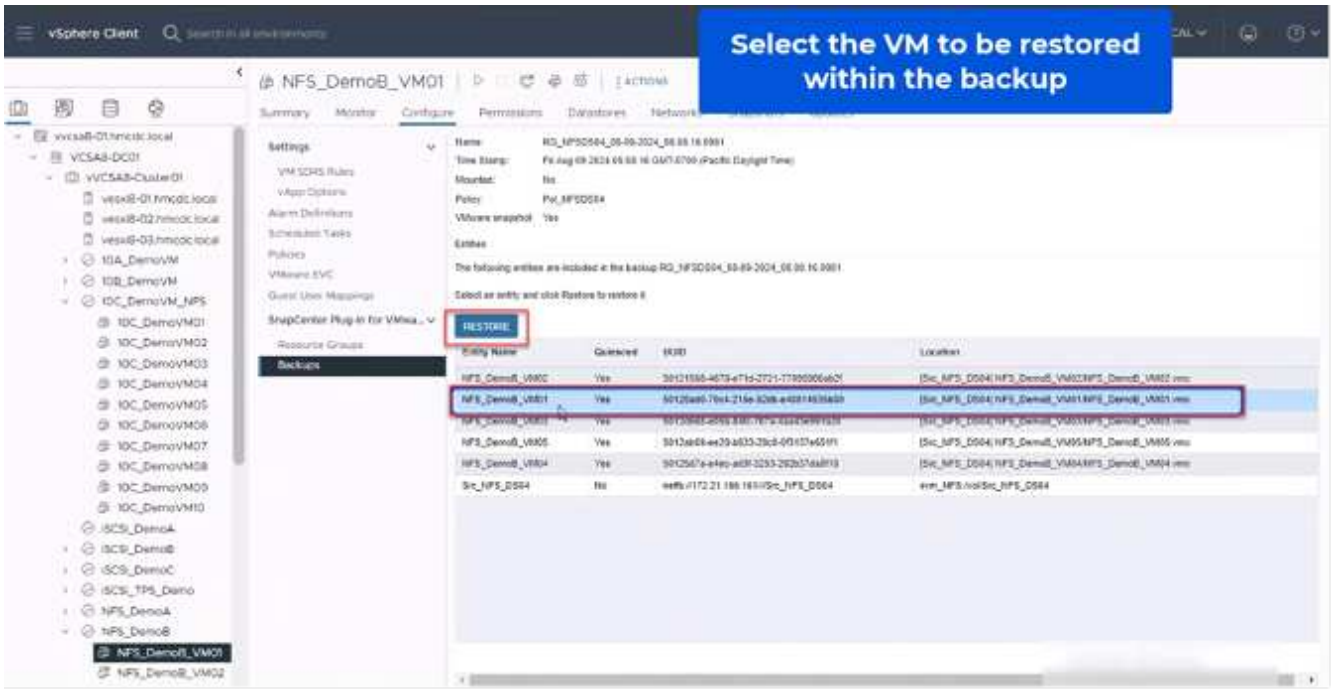
Ripristino delle VM dal backup

Il plug-in di SnapCenter per VMware consente di ripristinare le macchine virtuali (VM) in vCenter. Durante il ripristino di una macchina virtuale, è possibile ripristinarla nel datastore originale montato sull'host ESXi originale, che sovrascriverà il contenuto esistente con la copia di backup selezionata oppure una macchina virtuale eliminata/rinominata può essere ripristinata da una copia di backup (l'operazione sovrascrive i dati nei dischi virtuali originali). Per eseguire il ripristino, attenersi alla seguente procedura:

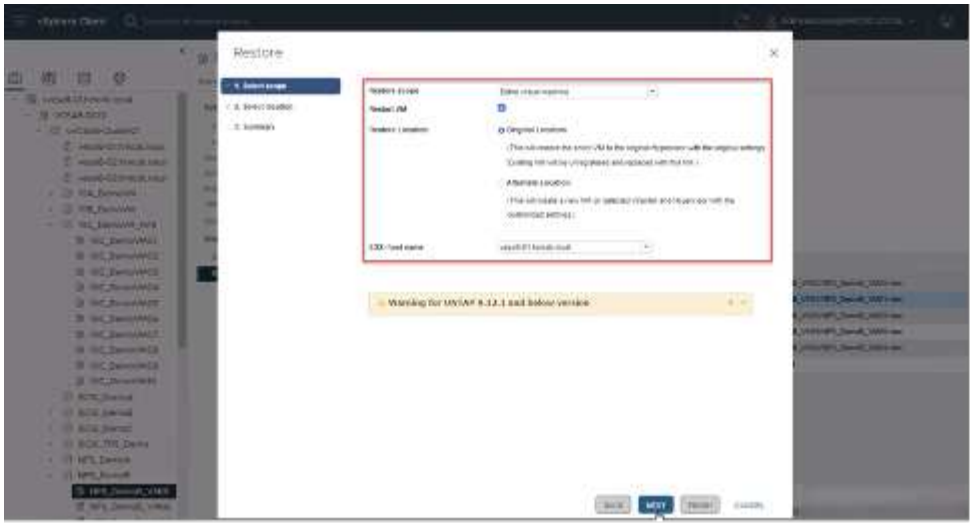
1. Nella GUI del client web VMware vSphere, selezionare Menu nella barra degli strumenti. Selezionare inventario, quindi macchine virtuali e modelli.
2. Nella barra di navigazione a sinistra, selezionare la macchina virtuale, quindi selezionare la scheda Configura, selezionare Backup in Plug-in SnapCenter per VMware. Fare clic sul processo di backup da cui deve essere ripristinata la VM.



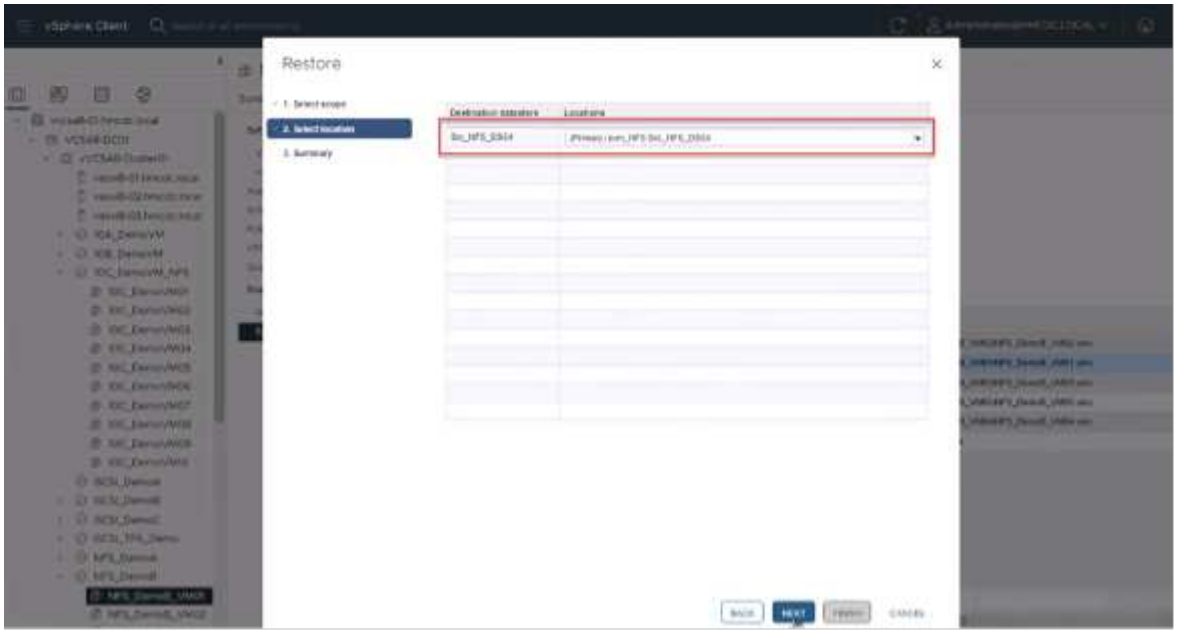
3. Selezionare la VM da ripristinare dal backup.



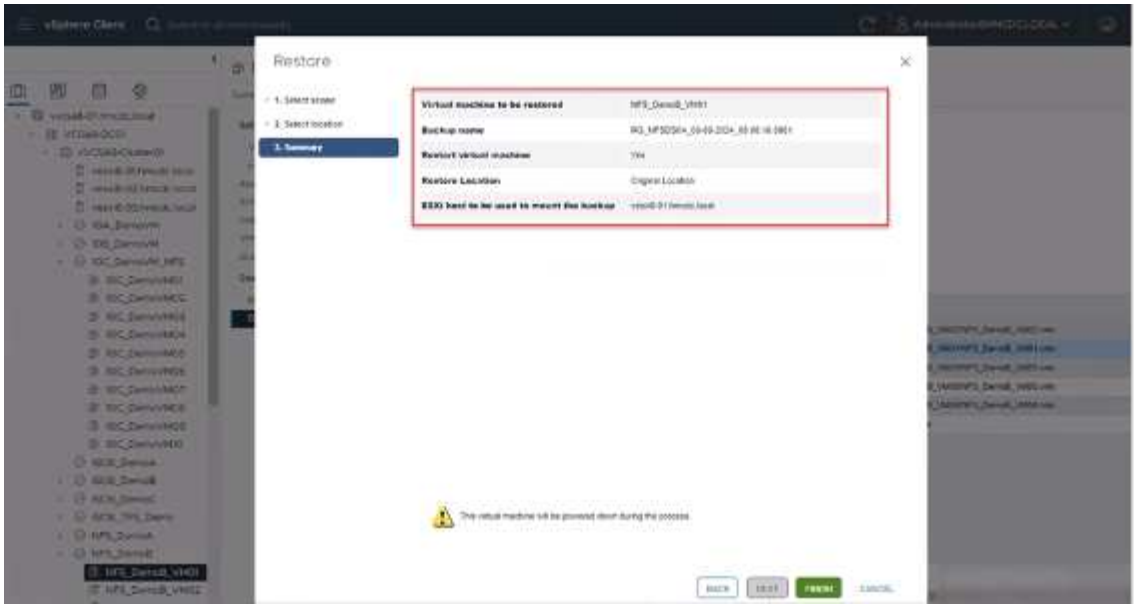
4. Nella pagina Select Scope (Seleziona ambito), selezionare Whole Virtual Machine (intera macchina virtuale) nel campo Restore Scope (Ripristina ambito), quindi selezionare Restore location (Ripristina posizione) e immettere le informazioni ESXi di destinazione in cui montare il backup. Attivare la casella di controllo Riavvia VM se la VM deve essere accesa dopo l'operazione di ripristino.



5. Nella pagina Seleziona posizione, selezionare la posizione per la posizione principale.



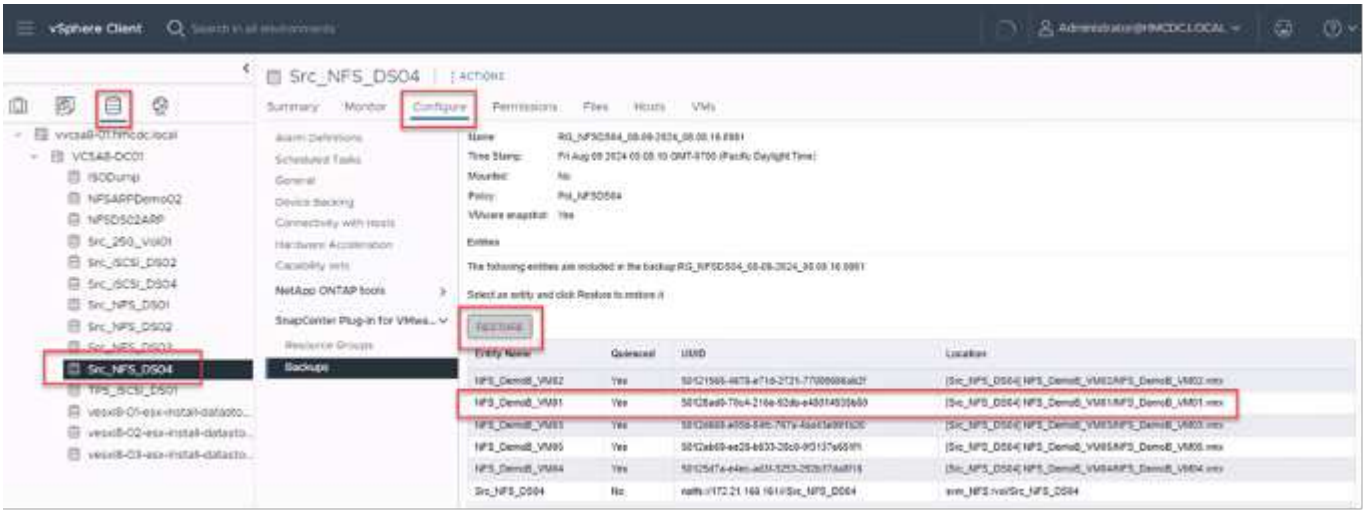
6. Esaminare la pagina Riepilogo, quindi selezionare fine.



Monitorare l'avanzamento dell'operazione selezionando attività recenti nella parte inferiore dello schermo.

> Sebbene le VM vengano ripristinate, non vengono aggiunte automaticamente ai gruppi di risorse precedenti. Pertanto, se è necessaria la protezione di tali macchine virtuali, aggiungere manualmente le macchine virtuali ripristinate ai gruppi di risorse appropriati.

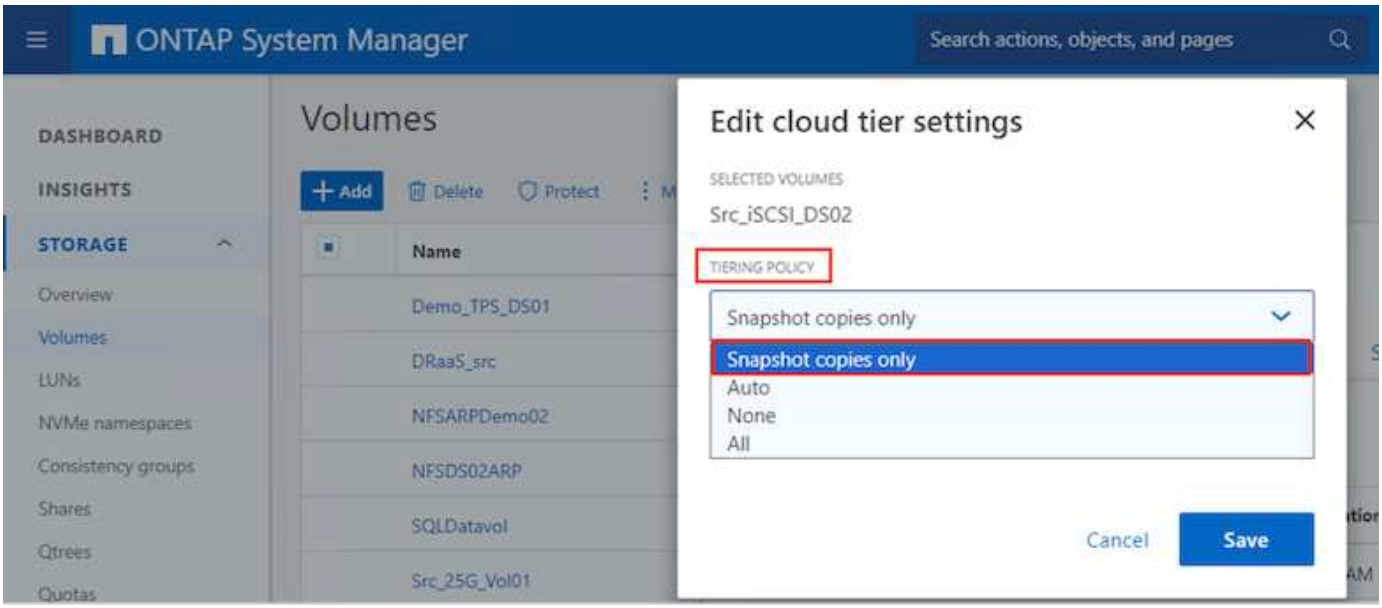
Cosa succederebbe se la VM originale venisse eliminata. Con il plug-in SnapCenter per VMware, è semplice. L'operazione di ripristino di una VM eliminata può essere eseguita a livello di datastore. Andare al datastore corrispondente > Configura > Backup e selezionare la VM eliminata, quindi selezionare Ripristina.



In sintesi, quando si utilizza lo storage ONTAP ASA per ottimizzare il TCO per un'implementazione VMware, utilizzare il plug-in SnapCenter per VMware come metodo semplice ed efficiente per il backup delle macchine virtuali. Consente di eseguire il backup e il ripristino delle VM in modo perfetto e veloce, poiché il completamento dei backup snapshot richiede letteralmente pochi secondi.

Fai riferimento "guida alle soluzioni"a queste "documentazione del prodotto"informazioni e per informazioni sulla configurazione, il backup, il ripristino dal sistema di storage primario o secondario SnapCenter o persino dai backup archiviati nello storage a oggetti per la conservazione a lungo termine.

Per ridurre i costi di storage, è possibile abilitare il tiering dei volumi FabricPool per spostare automaticamente i dati per le copie Snapshot in un Tier di storage a costi inferiori. Le copie Snapshot utilizzano in genere oltre il 10% dello storage allocato. Anche se importanti per la protezione dei dati e il disaster recovery, queste copie point-in-time sono raramente utilizzate e non costituiscono un utilizzo efficiente dello storage dalle performance elevate. Con la policy "solo Snapshot" per FabricPool, puoi facilmente liberare spazio sullo storage ad alte performance. Quando questa policy è abilitata, i blocchi di copia degli snapshot inattivi nel volume che non sono utilizzati dal file system attivo vengono spostati nel Tier di oggetti e, una volta letti, la copia Snapshot viene spostata nel Tier locale per ripristinare una macchina virtuale o un intero datastore. Questo Tier di oggetti può essere sotto forma di cloud privato (come NetApp StorageGRID) o cloud pubblico (come AWS o Azure).

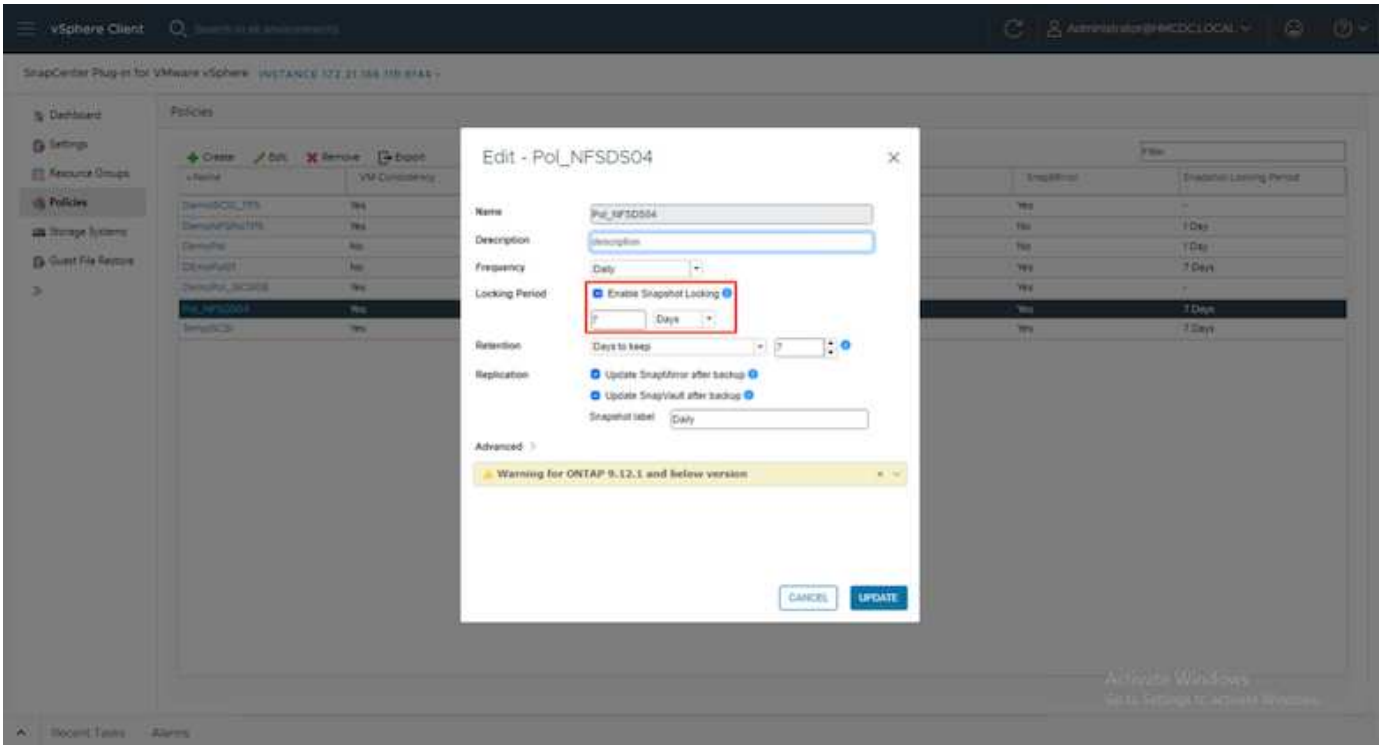


Visualizzare le istruzioni dettagliate per "VMware vSphere con ONTAP".

Protezione ransomware

Uno dei modi più efficaci per la protezione dagli attacchi ransomware è tramite l'implementazione di misure di sicurezza multi-layer. Ogni macchina virtuale residente in un datastore ospita un sistema operativo standard. Garantisci l'installazione e l'aggiornamento regolare delle suite di prodotti anti-malware dei server aziendali, un componente essenziale della strategia di protezione dal ransomware su più livelli. Inoltre, implementa la data Protection sfruttando la tecnologia Snapshot di NetApp per garantire un recovery rapido e affidabile in caso di attacco ransomware.

Gli attacchi ransomware puntano sempre più ai backup e ai recovery point snapshot, cercando di eliminarli prima di iniziare a crittografare i file. Tuttavia, con ONTAP questo può essere evitato creando snapshot antimanomissione su sistemi primari o secondari con "Blocco copia NetApp Snapshot™" in ONTAP. Questi Snapshot non possono essere eliminati o modificati da autori di attacchi ransomware o amministratori fuori controllo, in modo che siano disponibili anche in seguito a un attacco. È possibile ripristinare i dati della macchina virtuale in pochi secondi, riducendo al minimo i tempi di inattività dell'organizzazione. Inoltre, puoi scegliere la pianificazione e la durata di blocco delle snapshot più adatte alla tua organizzazione.



Come parte dell'approccio a più layer, esiste anche una soluzione ONTAP nativa integrata per la protezione della cancellazione non autorizzata delle copie Snapshot di backup. È noto come verifica multiamministratore o MAV, disponibile in ONTAP 9.11,1 e versioni successive. L'approccio ideale sarà quello di utilizzare query per operazioni specifiche MAV.

Per ulteriori informazioni su MAV e su come configurarne le funzionalità di protezione, vedere "Panoramica sulla verifica multi-admin".

Migrazione

Molte organizzazioni IT stanno adottando un approccio "cloud-first" ibrido durante la fase di trasformazione. I clienti stanno valutando la propria infrastruttura IT e spostando i carichi di lavoro nel cloud in base a tale valutazione e rilevamento. Le ragioni della migrazione al cloud variano e possono includere fattori quali elasticità e burst, uscita del data center, consolidamento dei data center, scenari di fine vita, fusioni, acquisizioni e altro ancora. Il ragionamento di migrazione di ogni organizzazione dipende dalle priorità aziendali specifiche, con l'ottimizzazione dei costi che rappresenta la priorità più alta. La scelta del giusto cloud storage è fondamentale per il passaggio al cloud ibrido, in quanto libera tutta la potenza dell'implementazione e della flessibilità del cloud.

Attraverso l'integrazione con i servizi 1P basati su NetApp su ciascun hyperscaler, le organizzazioni possono realizzare una soluzione cloud basata su vSphere senza un semplice approccio alla migrazione, senza re-platforming, modifiche IP e modifiche architetturali. Inoltre, questa ottimizzazione consente di scalare l'impatto dello storage mantenendo il numero di host alla quantità minima richiesta in vSphere, senza modificare la gerarchia dello storage, la sicurezza o i file resi disponibili.

- Visualizzare le istruzioni dettagliate per "Migra i carichi di lavoro in FSX per il datastore ONTAP".
- Visualizzare le istruzioni dettagliate per "Migra i carichi di lavoro nel datastore Azure NetApp Files".
- Visualizzare le istruzioni dettagliate per "Migra i carichi di lavoro nel datastore dei volumi di Google Cloud NetApp".

Disaster recovery

Disaster Recovery tra i siti on-premise

Per ulteriori dettagli, visitare il sito Web all'indirizzo "Dr utilizzando BlueXP DRaaS per archivi dati VMFS"

Disaster recovery tra on-premise e VMware Cloud in qualsiasi hyperscaler

Per i clienti che desiderano utilizzare VMware Cloud su qualsiasi hyperscaler come destinazione di disaster recovery, è possibile utilizzare datastore basati sullo storage ONTAP (Azure NetApp Files, FSX per ONTAP, Google Cloud NetApp Volumes) per replicare i dati da sistemi on-premise, utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle VM. Aggiungendo datastore basati su storage ONTAP, potrai eseguire un disaster recovery ottimizzato in termini di costi sulla destinazione, con un numero inferiore di host ESXi. Ciò consente anche di decommissionare un sito secondario nell'ambiente on-premise, ottenendo così notevoli risparmi sui costi.

- Visualizzare le istruzioni dettagliate per "Disaster recovery in FSX per ONTAP".
- Visualizzare le istruzioni dettagliate per "Disaster recovery nel datastore Azure NetApp Files".
- Visualizzare le istruzioni dettagliate per "Disaster recovery nel datastore Google Cloud NetApp Volumes".

Conclusione

Questa soluzione dimostra l'approccio ottimale all'utilizzo delle tecnologie SAN di ONTAP e degli strumenti OFFTAP per fornire servizi IT essenziali alle aziende, sia oggi che in futuro. Questi vantaggi sono particolarmente vantaggiosi per gli ambienti virtualizzati che eseguono VMware vSphere in una configurazione SAN. Grazie alla flessibilità e alla scalabilità dei sistemi storage NetApp, le organizzazioni possono stabilire una base per l'aggiornamento e la modifica della propria infrastruttura, in modo da soddisfare le esigenze di business in continuo cambiamento. Questo sistema è in grado di gestire i carichi di lavoro correnti e migliorare l'efficienza dell'infrastruttura, riducendo così i costi operativi e preparandosi per i carichi di lavoro futuri.

Array SAN all-flash NetApp con VMware vSphere 8

Array SAN all-flash NetApp con VMware vSphere 8

Da quasi vent'anni, il software NetApp ONTAP si è affermata come soluzione di storage leader per gli ambienti VMware vSphere, introducendo continuamente funzioni innovative che semplificano la gestione e riducono i costi. NetApp è leader affermato nello sviluppo di piattaforme di storage NAS e unificate che offrono un'ampia gamma di supporto per la connettività e i protocolli. Accanto a questo segmento di mercato, ci sono molti clienti che preferiscono la semplicità e i vantaggi economici delle piattaforme storage SAN a blocchi che si concentrano nell'esecuzione di un solo lavoro bene. L'array SAN all-flash (ASA) di NetApp mantiene questa promessa con semplicità su larga scala e con funzionalità di gestione e automazione coerenti per tutte le applicazioni e cloud provider.

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica della soluzione

Scopo del presente documento

In questo documento tratteremo il valore esclusivo dell'utilizzo dei sistemi storage NetApp ASA con VMware vSphere e forniremo una panoramica della tecnologia dell'array SAN all-flash NetApp. Inoltre, esamineremo

strumenti aggiuntivi per semplificare il provisioning dello storage, la protezione dei dati e il monitoraggio del data center VMware e ONTAP.

Le sezioni relative all'implementazione di questo documento trattano la creazione di datastore vVol con tool ONTAP per VMware vSphere e l'osservabilità per il moderno data center con NetApp Cloud Insights.

Panoramica sulla tecnologia

Questa soluzione include tecnologie innovative di VMware e NetApp.

VMware vSphere 8,0

VMware vSphere è una piattaforma di virtualizzazione che trasforma le risorse fisiche in pool di calcolo, rete e storage utilizzabili per soddisfare i requisiti applicativi e relativi al carico di lavoro dei clienti. I componenti principali di VMware vSphere sono:

- **ESXi** - hypervisor di VMware che consente l'astrazione di processori di elaborazione, memoria, rete e altre risorse e li rende disponibili per macchine virtuali e carichi di lavoro dei container.
- **VCenter** - VMware vCenter è una piattaforma di gestione centralizzata per interagire con risorse di calcolo, networking e storage come parte di un'infrastruttura virtuale. VCenter gioca un ruolo cruciale nella semplificazione dell'amministrazione dell'infrastruttura virtualizzata.

Nuovi miglioramenti in vSphere 8,0

VSphere 8,0 introduce alcuni nuovi miglioramenti, tra cui, a titolo esemplificativo:

Scalabilità - vSphere 8,0 supporta le più recenti CPU Intel e AMD e ha limiti estesi per i dispositivi vGPU, gli host ESXi, le VM per cluster e i dispositivi i/o VM DirectPath.

Distributed Services Engine - trasferimento di rete con NSX alle unità di elaborazione dati (DPU).

Efficienza migliorata dei dispositivi - vSphere 8,0 potenzia le funzionalità di gestione dei dispositivi con funzioni quali unità periferiche e Device Virtualization Extensions (DVX).

Sicurezza migliorata - l'inclusione di un timeout SSH e di una politica di provisioning TPM rafforza il framework di sicurezza.

Integrazione con i servizi di cloud ibrido - questa funzionalità facilita una transizione perfetta tra workload on-premise e cloud.

Kubernetes Runtime integrato - con l'inclusione di Tanzu, vSphere 8,0 semplifica l'orchestrazione dei container.

Per ulteriori informazioni, consultare il blog, "Novità di vSphere 8".

Volumi virtuali VMware (vVol)

I vVol sono un nuovo rivoluzionario approccio alla gestione dello storage nei cluster vSphere, che offre una gestione semplificata e un controllo più granulare delle risorse storage. Ciascun disco virtuale di un datastore di vVol è un vVol e diventa un oggetto LUN nativo nel sistema storage. L'integrazione del sistema storage e di vSphere avviene tramite il provider **VMware API per Storage Awareness (VASA)** e consente al sistema storage di essere consapevole dei dati delle VM e di gestirli di conseguenza. Le policy di storage definite nel client vCenter vengono utilizzate per allocare e gestire le risorse di storage.

I vVol sono un approccio semplificato alla gestione dello storage e sono preferiti in alcuni casi di utilizzo.

Per ulteriori informazioni sui vVol, vedere la "Guida introduttiva di vVol".

NVMe over Fabrics

Con la release di vSphere 8,0, NVMe è ora supportato end-to-end e completo supporto per vVol con NVMe-TCP e NVMe-FC.

Per informazioni dettagliate sull'utilizzo di NVMe con vSphere, fare riferimento a. "Informazioni sullo storage VMware NVMe" Nella documentazione di vSphere Storage.

NetApp ONTAP

Il software NetApp ONTAP è da quasi vent'anni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione e ridurre i costi. L'utilizzo di ONTAP insieme a vSphere è un'ottima combinazione che consente di ridurre le spese relative all'hardware host e al software VMware. Puoi anche proteggere i tuoi dati a costi inferiori con performance elevate e costanti sfruttando al contempo l'efficienza dello storage nativo.

Funzioni di base di ONTAP

Copie Snapshot NetApp: Copie Snapshot di una macchina virtuale o di un datastore, per garantire che non vi sia alcun impatto sulle performance in fase di creazione o utilizzo di una snapshot. Queste repliche possono fungere da punti di ripristino per le VM o come semplice salvaguardia dei dati. Queste Snapshot basate su array sono diverse dalle Snapshot VMware (coerenza). Il metodo più semplice per generare una copia Snapshot ONTAP è tramite il plug-in SnapCenter per VMware vSphere, eseguendo il backup di macchine virtuali e datastore.

- **Efficienza dello storage**: ONTAP offre deduplica e compressione in background e real-time, deduplica zero-block e data compaction.
- **Trasferimento di volumi e LUN**: Consente lo spostamento senza interruzioni di volumi e LUN che supportano datastore vSphere e vVol nel cluster ONTAP per bilanciare performance e capacità o supportare upgrade e manutenzione senza interruzioni.
- **La ricollocazione di volume e LUN** - ONTAP consente lo spostamento senza interruzioni di volumi e LUN che ospitano datastore vSphere e vVol all'interno del cluster ONTAP. Ciò contribuisce al bilanciamento di performance e capacità e consente di eseguire upgrade senza interruzioni.
- **Quality of Service** - QoS è una funzione che consente la gestione delle prestazioni su un singolo LUN, volume o file. Può essere utilizzato per limitare una macchina virtuale aggressiva o per garantire che una macchina virtuale critica riceva risorse di performance sufficienti.
- **Crittografia** - crittografia dei volumi NetApp e crittografia aggregata NetApp. Queste opzioni offrono un approccio semplice e basato su software per crittografare i dati a riposo, assicurandone la protezione.
- **Fabric Pool** - questa funzionalità esegue il tiering dei dati ad accesso meno frequente in un archivio di oggetti separato, liberando storage flash di valore. Operando a livello di blocchi, è in grado di identificare ed eseguire il tiering dei dati più cold in modo efficiente, ottimizzando le risorse di storage e riducendo i costi.
- **Automazione**: Semplifica i task di storage e gestione dei dati utilizzando le API REST ONTAP per l'automazione e sfruttando i moduli Ansible per una perfetta gestione della configurazione dei sistemi ONTAP. I moduli Ansible offrono una comoda soluzione per gestire in modo efficiente le configurazioni dei sistemi ONTAP. La combinazione di questi potenti strumenti consente di ottimizzare i flussi di lavoro e migliorare la gestione globale dell'infrastruttura storage.

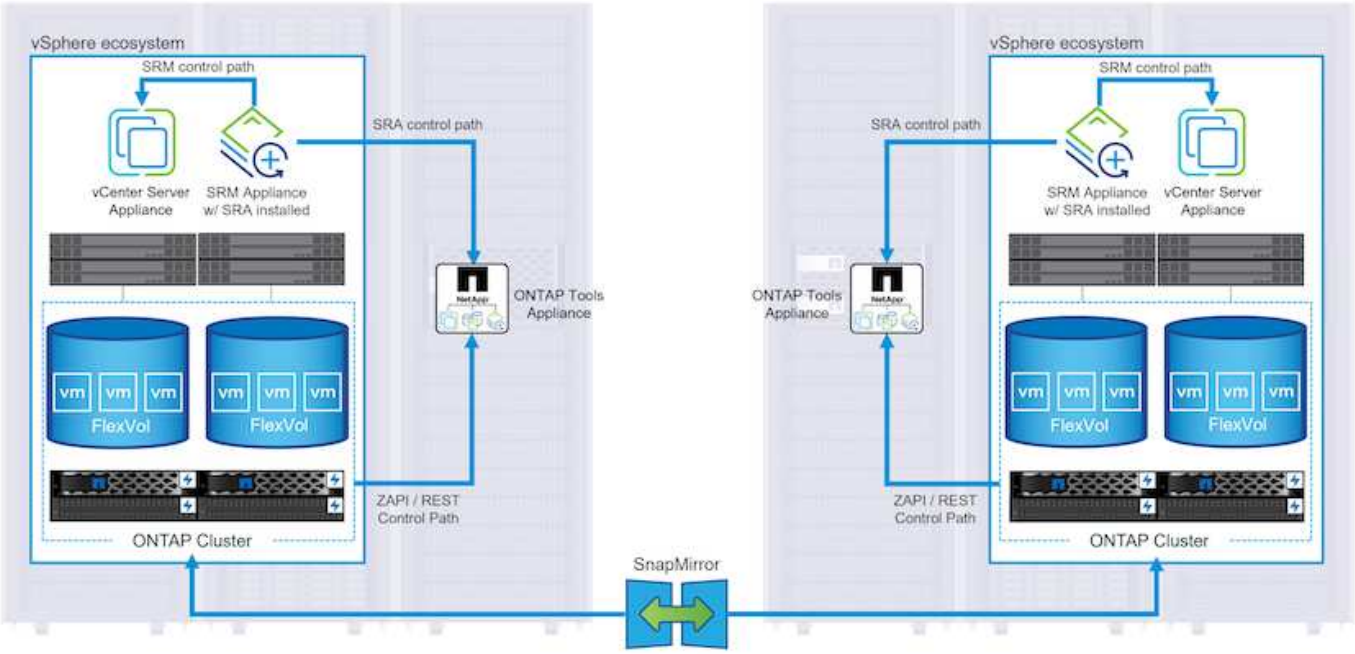
Funzionalità di disaster recovery ONTAP

NetApp ONTAP offre solide soluzioni di disaster recovery per gli ambienti VMware. Queste soluzioni sfruttano tecnologie di replica SnapMirror tra sistemi di storage primario e secondario per consentire il failover e il recovery rapido in caso di guasto.

Scheda di replica archiviazione:
L'adattatore di replica dello storage NetApp (SRA) è un componente software che fornisce integrazione tra i sistemi di storage NetApp e VMware Site Recovery Manager (SRM). Agevola la replica dei dati delle macchine virtuali su tutti gli storage array NetApp, offrendo solide funzionalità di disaster recovery e protezione dei dati. L'SRA utilizza SnapMirror e SnapVault per eseguire la replica dei dati delle macchine virtuali in diversi sistemi di storage o in diverse aree geografiche.

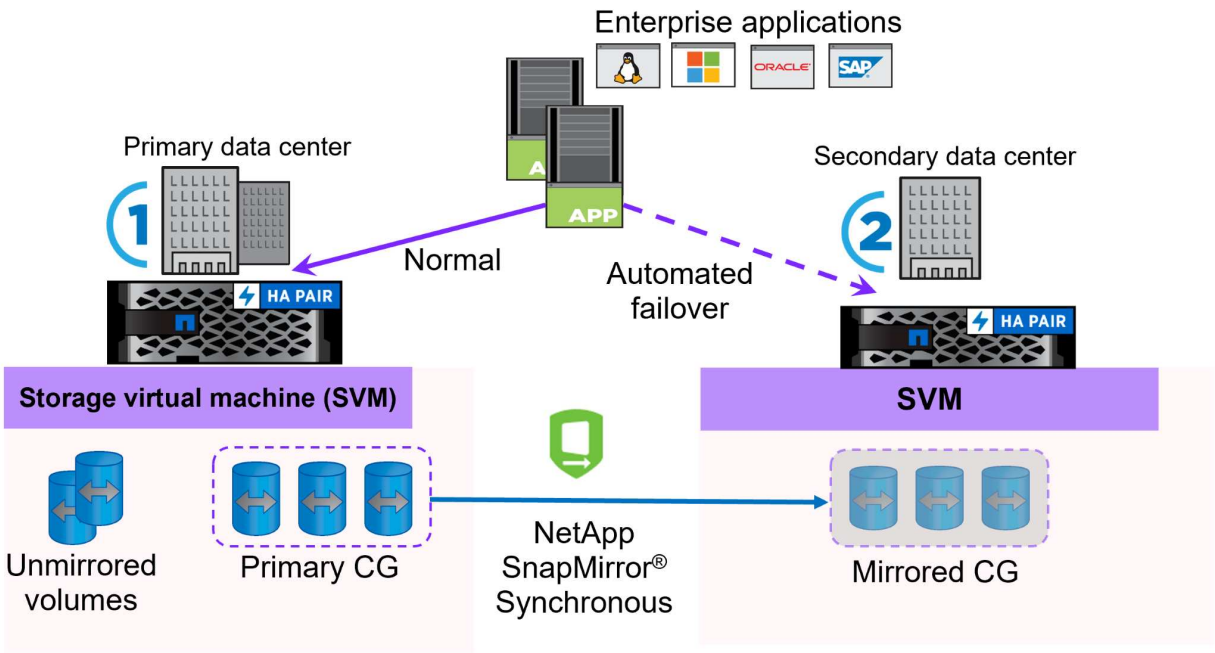
L'adattatore offre una replica asincrona a livello di Storage Virtual Machine (SVM) utilizzando la tecnologia SnapMirror ed estende il supporto per VMFS negli ambienti storage SAN (iSCSI e FC) e NFS negli ambienti storage NAS.

NetApp SRA viene installato come parte degli strumenti ONTAP per VMware vSphere.



Per informazioni sull'adattatore di replica dello storage NetApp per SRM, fare riferimento a. "VMware Site Recovery Manager con NetApp ONTAP".

Business Continuity SnapMirror:
SnapMirror è una tecnologia di replica dei dati NetApp che offre replica sincrona dei dati tra sistemi storage. Consente la creazione di copie multiple dei dati in posizioni diverse, fornendo la possibilità di ripristinare i dati in caso di disastro o perdita di dati. SnapMirror offre flessibilità in termini di frequenza di replica e consente la creazione di copie point-in-time dei dati a scopo di backup e ripristino. SM-BC replica i dati a livello di Consistency Group.

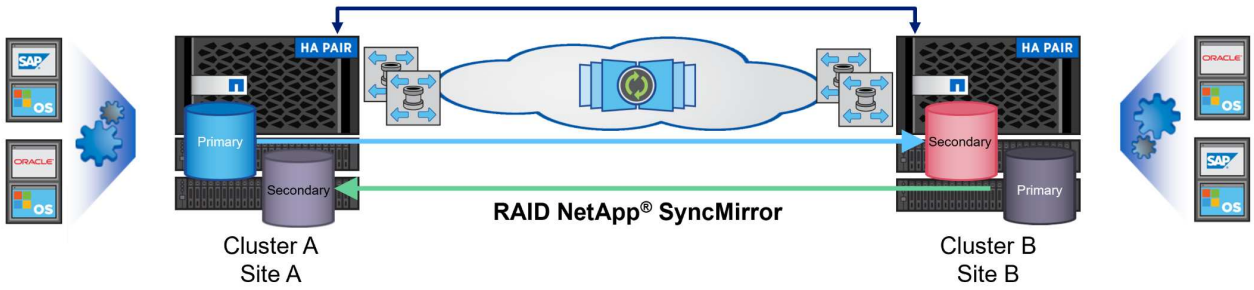


Per ulteriori informazioni, fare riferimento a SnapMirror "Panoramica sulla continuità del business".

NetApp MetroCluster:
NetApp MetroCluster è una soluzione di disaster recovery e high Availability che offre una replica dei dati sincrona tra due sistemi storage NetApp distribuiti a livello geografico. È progettato per garantire la disponibilità e la protezione continue dei dati nel caso di guasti estesi a un intero sito.

MetroCluster utilizza SyncMirror per eseguire la replica sincrona dei dati appena al di sopra del livello RAID. SyncMirror è progettato per una transizione efficiente tra modalità sincrona e asincrona. In questo modo, il cluster di storage primario continua a funzionare in stato non replicato, in situazioni in cui il sito secondario diventa temporaneamente inaccessibile. SyncMirror eseguirà anche la replica su uno stato di RPO = 0 al ripristino della connettività.

MetroCluster può operare su reti basate su IP o utilizzando fibre channel.



Per informazioni dettagliate sull'architettura e la configurazione di MetroCluster, consultare la "Sito di documentazione MetroCluster".

Modello di licenza ONTAP One

ONTAP One è un modello di licenza completo che consente di accedere a tutte le funzionalità di ONTAP senza richiedere licenze aggiuntive. Ad esempio protezione dei dati, disaster recovery, alta disponibilità, integrazione del cloud, efficienza dello storage, prestazioni e sicurezza. I clienti con sistemi storage NetApp concessi in licenza con Flash, Core Plus Data Protection o Premium hanno diritto a una licenza ONTAP One, che consente loro di massimizzare l'utilizzo dei propri sistemi storage.

La licenza ONTAP ONE include tutte le seguenti funzioni:

NVMeoF – abilita l'utilizzo di NVMe over Fabrics per front-end client io, NVMe/FC e NVMe/TCP.

FlexClone – consente la creazione rapida di una clonazione efficiente in termini di spazio dei dati basata su snapshot.

S3 – attiva il protocollo S3 per i client front-end io.

SnapRestore – consente il ripristino rapido dei dati dalle istantanee.

Protezione autonoma dal ransomware - attiva la protezione automatica delle condivisioni di file NAS quando viene rilevata un'attività anomala del file system.

Multi tenant Key Manager - consente di disporre di più gestori di chiavi per i diversi tenant del sistema.

SnapLock – consente la protezione dei dati da modifiche, eliminazioni o danneggiamenti sul sistema.

SnapMirror Cloud – consente la replica dei volumi di sistema in destinazioni di oggetti.

S3 SnapMirror – consente la replica degli oggetti ONTAP S3 in destinazioni alternative compatibili con S3.

Array SAN all-flash NetApp

L'array SAN all-flash NetApp (ASA) è una soluzione storage ad elevate performance progettata per soddisfare le esigenti necessità dei data center moderni. Combina velocità e affidabilità dello storage flash con le funzioni avanzate di gestione dei dati di NetApp, in modo da offrire performance, scalabilità e protezione dei dati eccezionali.

La linea ASA comprende sia i modelli A-Series che C-Series.

Gli array flash NetApp A-Series all-NVMe sono progettati per carichi di lavoro dalle performance elevate, offrendo latenza estremamente bassa ed elevata resilienza, rendendoli adatti ad applicazioni mission-critical.

I Flash Array C-Series QLC mirano a casi di utilizzo di capacità più elevata, fornendo la velocità della tecnologia flash insieme al risparmio della tecnologia flash ibrida.

Per informazioni dettagliate, consultare la "Landing page di NetApp ASA".

Caratteristiche di NetApp ASA

L'array SAN all-flash NetApp include le seguenti funzionalità:

Performance - l'array SAN all-flash sfrutta i dischi a stato solido (SSD), con un'architettura NVMe end-to-end, per offrire performance estremamente veloci, riducendo in modo significativo la latenza e migliorando i tempi di risposta delle applicazioni. Fornisce IOPS elevati e una bassa latenza costanti, il che la rende adatta a carichi di lavoro sensibili alla latenza come database, virtualizzazione e analytics.

Scalabilità - gli array SAN all-flash NetApp sono realizzati con un'architettura scale-out che consente alle organizzazioni di scalare perfettamente la propria infrastruttura storage in base alle esigenze crescenti. Con la possibilità di aggiungere nodi storage aggiuntivi, le organizzazioni possono espandere capacità e performance senza interruzioni, facendo in modo che il proprio storage possa restare al passo con le crescenti esigenze in termini di dati.

Gestione dati - il sistema operativo Data ONTAP di NetApp è alla base dell'array SAN all-flash, fornendo una suite completa di funzioni di gestione dati. Queste funzionalità includono thin provisioning, deduplica, compressione e data compaction, che ottimizzano l'utilizzo dello storage e riducono i costi. Le funzionalità avanzate di data Protection come snapshot, replica e crittografia garantiscono l'integrità e la sicurezza dei dati archiviati.

Integrazione e flessibilità - l'array SAN all-flash si integra con l'ecosistema più ampio di NetApp, consentendo un'integrazione perfetta con altre soluzioni storage NetApp, come le implementazioni di cloud ibrido con NetApp Cloud Volumes ONTAP. Supporta inoltre protocolli standard del settore come Fibre Channel (FC) e iSCSI, consentendo una facile integrazione nelle infrastrutture SAN esistenti.

Analytics e automazione - il software di gestione di NetApp, incluso NetApp Cloud Insights, offre funzionalità complete di monitoring, analytics e automazione. Questi tool consentono agli amministratori di ottenere informazioni utili sul proprio ambiente storage, ottimizzare le performance e automatizzare i task di routine, semplificando la gestione dello storage e migliorando l'efficienza delle operazioni.

Protezione dei dati e business continuity - l'array SAN all-flash offre funzionalità di protezione dei dati integrate, come istantanee point-in-time, replica e funzionalità di disaster recovery. Queste funzionalità garantiscono la disponibilità dei dati e agevolano un rapido recovery in caso di perdita di dati o errori di sistema.

Supporto del protocollo

Il sistema ASA supporta tutti i protocolli SAN standard tra cui iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) e NVME over Fabrics.

ISCSI - NetApp ASA fornisce un solido supporto per iSCSI, consentendo l'accesso a livello di blocco ai dispositivi di storage su reti IP. Offre un'integrazione perfetta con gli initiator iSCSI, consentendo un provisioning e una gestione efficienti delle LUN iSCSI. Funzionalità avanzate di ONTAP, come multipathing, autenticazione CHAP e supporto ALUA.

Per istruzioni sulla progettazione delle configurazioni iSCSI, fare riferimento a .

Fibre Channel - NetApp ASA offre un supporto completo per Fibre Channel (FC), una tecnologia di rete ad alta velocità comunemente utilizzata nelle reti SAN. ONTAP si integra perfettamente con l'infrastruttura FC, fornendo un accesso a livello di blocco affidabile ed efficiente ai dispositivi storage. Offre funzioni come zoning, multi-path e fabric login (FLOGI) per ottimizzare le prestazioni, migliorare la sicurezza e garantire una connettività perfetta negli ambienti FC.

Per informazioni sulla progettazione delle configurazioni Fibre Channel, fare riferimento alla "Documentazione di riferimento per la configurazione SAN".

NVMe over Fabrics - NetApp ONTAP e ASA supportano NVMe over Fabrics. NVMe/FC consente l'utilizzo di dispositivi storage NVMe su un'infrastruttura Fibre Channel e NVMe/TCP su reti IP di storage.

Per informazioni sulla progettazione su NVMe, fare riferimento a. "Configurazione, supporto e limitazioni NVMe".

Tecnologia Active-Active

Gli array SAN all-flash NetApp offrono percorsi Active-Active attraverso entrambi i controller, eliminando la necessità per il sistema operativo host di attendere un errore di percorso attivo, prima di attivare il percorso alternativo. Ciò significa che l'host può utilizzare tutti i percorsi disponibili su tutti i controller, garantendo che i percorsi attivi siano sempre presenti, indipendentemente dal fatto che il sistema si trovi in uno stato regolare o stia eseguendo un'operazione di failover del controller.

Inoltre, NetApp ASA offre una caratteristica distintiva che migliora notevolmente la velocità del failover SAN. Ogni controller replica continuamente i metadati LUN essenziali al proprio partner. Di conseguenza, ogni controller è pronto ad assumersi le responsabilità del Data Serving in caso di guasto improvviso del partner. Questa disponibilità è possibile perché il controller possiede già le informazioni necessarie per iniziare a utilizzare le unità precedentemente gestite dal controller guasto.

Con il path Active-Active, i takeover pianificati e non pianificati hanno tempi di ripresa io di 2-3 secondi.

Per ulteriori informazioni, vedere "TR-4968, array All-SAS NetApp – disponibilità e integrità dei dati con NetApp ASA".

Garanzie di archiviazione

Con gli array SAN all-flash di NetApp, NetApp offre un set esclusivo di garanzie storage. I vantaggi esclusivi includono:

Garanzia di efficienza dello storage: con la garanzia di efficienza dello storage è possibile ottenere prestazioni elevate riducendo al minimo i costi di storage. 4:1:1 per i carichi di lavoro SAN.

Garanzia di disponibilità dei dati del 99,9999% (6 nove): garantisce la correzione per i downtime non pianificati superiori a 31,56 secondi all'anno.

Garanzia di recovery ransomware: recovery di dati garantito in caso di attacco ransomware.

Vedere "Portale dei prodotti NetApp ASA" per ulteriori informazioni.

Plug-in NetApp per VMware vSphere

I servizi storage di NetApp sono strettamente integrati con VMware vSphere tramite l'utilizzo dei seguenti plug-in:

Strumenti ONTAP per VMware vSphere

I tool ONTAP per VMware consentono agli amministratori di gestire lo storage NetApp direttamente dal client vSphere. ONTAP Tools ti consente di implementare e gestire datastore, nonché di eseguire il provisioning dei datastore vVol.
I tool ONTAP consentono il mapping dei datastore ai profili di funzionalità dello storage che determinano un set di attributi del sistema storage. Ciò consente la creazione di datastore con attributi specifici, come le performance dello storage e la qualità del servizio.

Gli strumenti ONTAP includono i seguenti componenti:

Virtual Storage Console (VSC): la console VSC comprende l'interfaccia integrata con il client vSphere in cui è possibile aggiungere storage controller, eseguire il provisioning dei datastore, monitorare le performance dei datastore e visualizzare e aggiornare le impostazioni dell'host ESXi.

VASA Provider: il provider VASA (VMware vSphere APIs for Storage Awareness) per ONTAP invia informazioni sullo storage utilizzato da VMware vSphere al vCenter Server, consentendo il provisioning dei datastore vVol (VMware Virtual Volumes), la creazione e l'utilizzo di profili di capacità dello storage, la verifica della conformità e il monitoraggio delle performance.

Storage Replication Adapter (SRA): se abilitato e utilizzato con VMware Site Recovery Manager (SRM), SRA facilita il ripristino di datastore vCenter Server e macchine virtuali in caso di guasto, consentendo la configurazione di siti protetti e siti di ripristino per il disaster recovery.

Per ulteriori informazioni sugli strumenti NetApp ONTAP per VMware, vedere "Strumenti ONTAP per la documentazione VMware vSphere".

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere (SCV) è una soluzione software di NetApp che offre una protezione dei dati completa per ambienti VMware vSphere. È progettato per semplificare e ottimizzare il processo di protezione e gestione delle macchine virtuali (VM) e dei datastore.

Il plug-in SnapCenter per VMware vSphere offre in un'interfaccia unificata le seguenti funzionalità, integrate con il client vSphere:

Istantanee basate su criteri - SnapCenter consente di definire criteri per la creazione e la gestione di istantanee coerenti con le applicazioni delle macchine virtuali (VM) in VMware vSphere.

Automazione - la creazione e la gestione automatizzate delle snapshot basate su policy definite contribuiscono a garantire una protezione dei dati coerente ed efficiente.

VM-Level Protection - la protezione granulare a livello di VM consente una gestione e un ripristino efficienti delle singole macchine virtuali.

Funzioni di efficienza dello storage - l'integrazione con le tecnologie di storage NetApp offre funzioni di efficienza dello storage come la deduplica e la compressione per le snapshot, riducendo al minimo i requisiti di storage.

Il plug-in di SnapCenter orchestra l'arresto delle macchine virtuali insieme alle istantanee basate su hardware sugli storage array di NetApp. La tecnologia SnapMirror viene utilizzata per replicare le copie di backup su sistemi storage secondari, incluso il cloud.

Per ulteriori informazioni, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere".

L'integrazione di BlueXP permette strategie di backup 3-2-1 che estendono le copie dei dati allo storage a oggetti nel cloud.

Per ulteriori informazioni sulle strategie di backup 3-2-1 con BlueXP, visita il sito "Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM".

NetApp Cloud Insights

NetApp Cloud Insights semplifica l'osservazione dell'infrastruttura on-premise e cloud e offre funzionalità di analytics e troubleshooting per risolvere problemi complessi. Cloud Insights raccoglie i dati da un ambiente del data center e li invia nel cloud. Ciò avviene con il software installato localmente chiamato unità di acquisizione e con collettori specifici abilitati per le risorse nel data center.

Le risorse in Cloud Insights possono essere contrassegnate con annotazioni che forniscono un metodo per organizzare e classificare i dati. Il dashboard può essere creato utilizzando un'ampia gamma di widget per la visualizzazione dei dati e le query metriche possono essere create per viste tabulari dettagliate dei dati.

Cloud Insights dispone di numerose dashboard pronte all'uso che consentono di azzerare su tipi specifici di aree problematiche e categorie di dati.

Cloud Insights è uno strumento eterogeneo progettato per raccogliere dati da un'ampia gamma di dispositivi. Tuttavia, è disponibile una libreria di modelli, denominata ONTAP Essentials, che consente ai clienti NetApp di iniziare rapidamente.

Per informazioni dettagliate su come iniziare a utilizzare Cloud Insights, fare riferimento alla "Landing page di NetApp BlueXP e Cloud Insights".

Array SAN all-flash NetApp con VMware vSphere 8

I tool ONTAP per VMware consentono agli amministratori di gestire lo storage NetApp direttamente dal client vSphere. ONTAP Tools ti consente di implementare e gestire

datastore, nonché di eseguire il provisioning dei datastore vVol.
I tool ONTAP consentono il mapping dei datastore ai profili di funzionalità dello storage che determinano un set di attributi del sistema storage. Ciò consente la creazione di datastore con attributi specifici, come le performance dello storage e la qualità del servizio.

Autore: Josh Powell - NetApp Solutions Engineering

Gestire lo storage a blocchi con tool ONTAP per VMware vSphere

Gli strumenti ONTAP includono i seguenti componenti:

Virtual Storage Console (VSC): la console VSC comprende l'interfaccia integrata con il client vSphere in cui è possibile aggiungere storage controller, eseguire il provisioning dei datastore, monitorare le performance dei datastore e visualizzare e aggiornare le impostazioni dell'host ESXi.

VASA Provider: il provider VASA (VMware vSphere APIs for Storage Awareness) per ONTAP invia informazioni sullo storage utilizzato da VMware vSphere al vCenter Server, consentendo il provisioning dei datastore vVol (VMware Virtual Volumes), la creazione e l'utilizzo di profili di capacità dello storage, la verifica della conformità e il monitoraggio delle performance.

Storage Replication Adapter (SRA): se abilitato e utilizzato con VMware Site Recovery Manager (SRM), SRA facilita il ripristino di datastore vCenter Server e macchine virtuali in caso di guasto, consentendo la configurazione di siti protetti e siti di ripristino per il disaster recovery.

Per ulteriori informazioni sugli strumenti NetApp ONTAP per VMware, vedere "Strumenti ONTAP per la documentazione VMware vSphere".

Panoramica sull'implementazione della soluzione

Questa soluzione dimostrerà l'utilizzo dei tool ONTAP per VMware vSphere per il provisioning di datastore vVol) e la creazione di una macchina virtuale in un datastore vVol.

Ciascun disco virtuale di un datastore di vVol è un vVol e diventa un oggetto LUN nativo nel sistema storage. L'integrazione del sistema storage e di vSphere avviene tramite il provider VMware API for Storage Awareness (VASA) (installato con ONTAP Tools) e consente al sistema storage di essere consapevole dei dati delle macchine virtuali e di gestirli di conseguenza. Le policy di storage definite nel client vCenter vengono utilizzate per allocare e gestire le risorse di storage.

Per informazioni dettagliate sui vVol con ONTAP, fare riferimento a. "VVol di volumi virtuali) con ONTAP".

Questa soluzione copre i seguenti passaggi di alto livello:

1. Aggiunta di un sistema di storage nei tool ONTAP.
2. Creare un profilo di funzionalità di storage in ONTAP Tools.
3. Creare un datastore vVol in ONTAP Tools.
4. Creare una policy di storage delle macchine virtuali nel client vSphere.
5. Creare una nuova macchina virtuale nell'archivio dati vVol.

Prerequisiti

In questa soluzione sono stati utilizzati i seguenti componenti:

1. Array SAN all-flash NetApp A400 con ONTAP 9,13.
2. SVM iSCSI creata su ASA con connettività di rete agli host ESXi.
3. Tool ONTAP per VMware vSphere 9,13 (provider VASA abilitato per impostazione predefinita).
4. Cluster vSphere 8,0 (appliance vCenter e host ESXi).

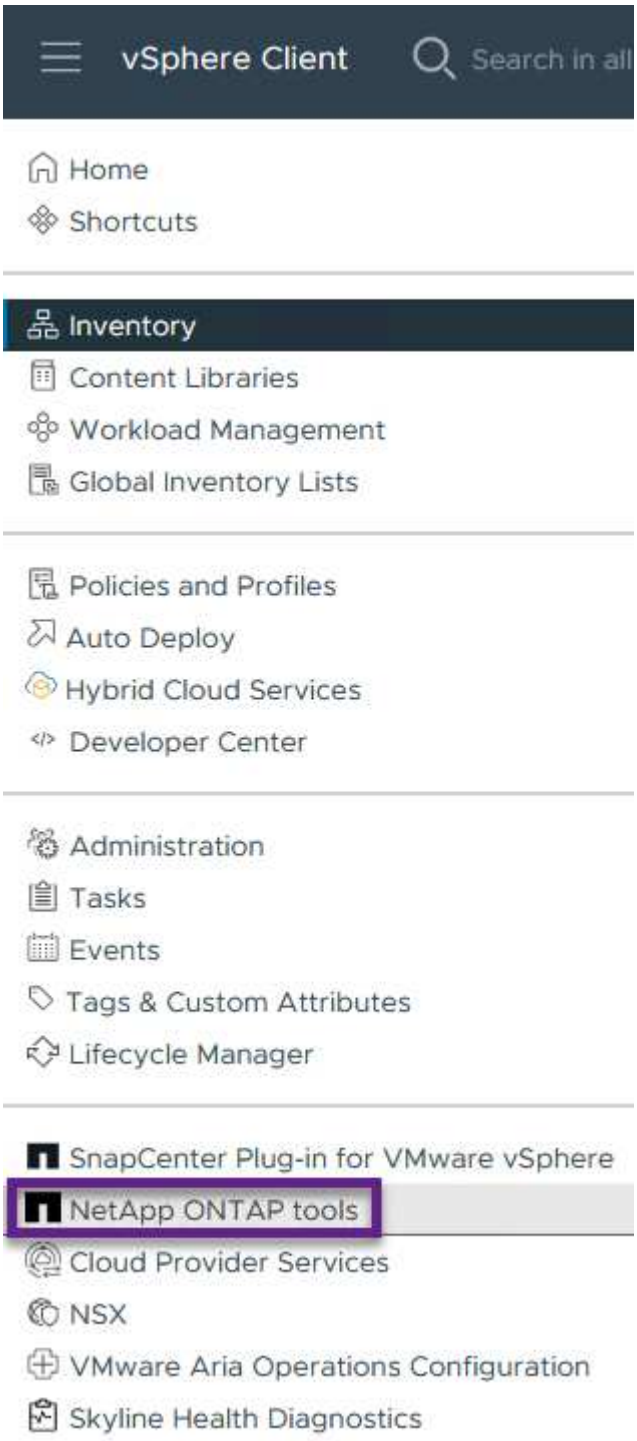
Implementazione della soluzione

Creare un datastore vVol in ONTAP Tools

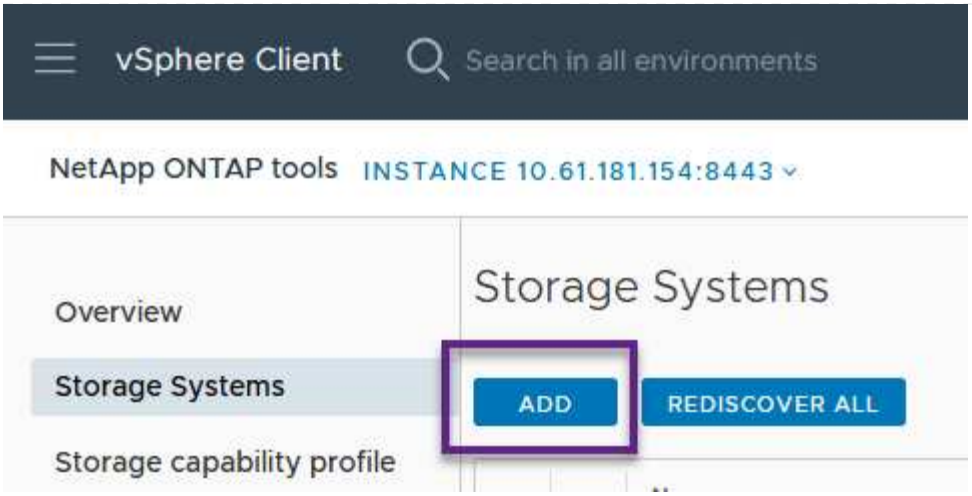
Per creare un datastore vVol in Strumenti di ONTAP, attenersi alla seguente procedura:

Aggiunta di un sistema di storage ai tool ONTAP.

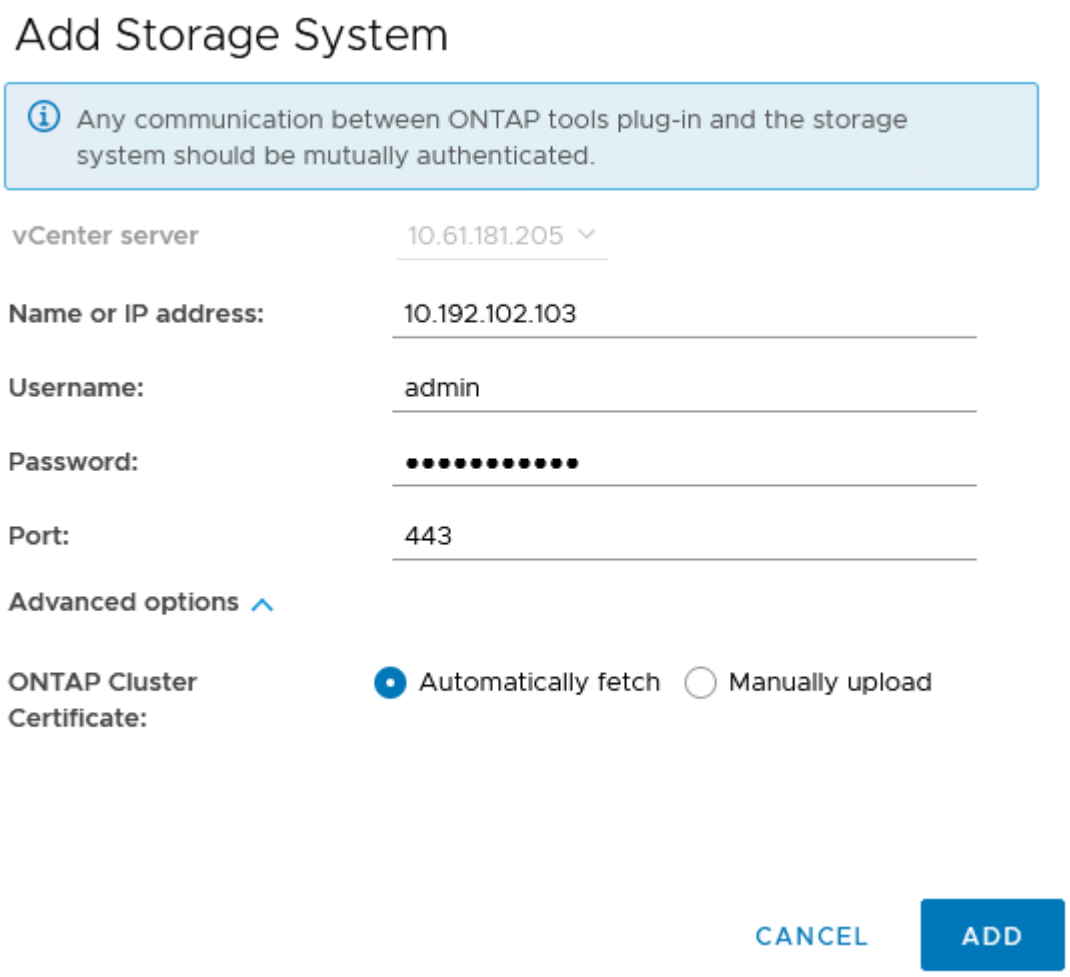
1. Accedere agli strumenti NetApp ONTAP selezionandoli dal menu principale del client vSphere.



2. In Strumenti di ONTAP, selezionare **sistemi di archiviazione** dal menu a sinistra, quindi premere **Aggiungi**.



3. Immettere l'indirizzo IP, le credenziali del sistema di archiviazione e il numero di porta. Fare clic su **Aggiungi** per avviare il processo di ricerca.

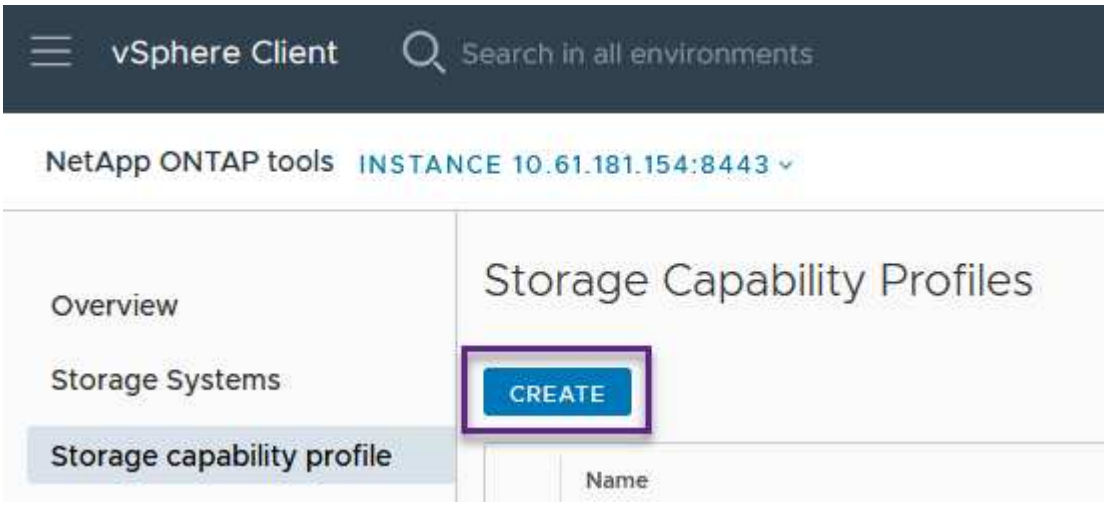


Creare un profilo di funzionalità di storage in ONTAP Tools

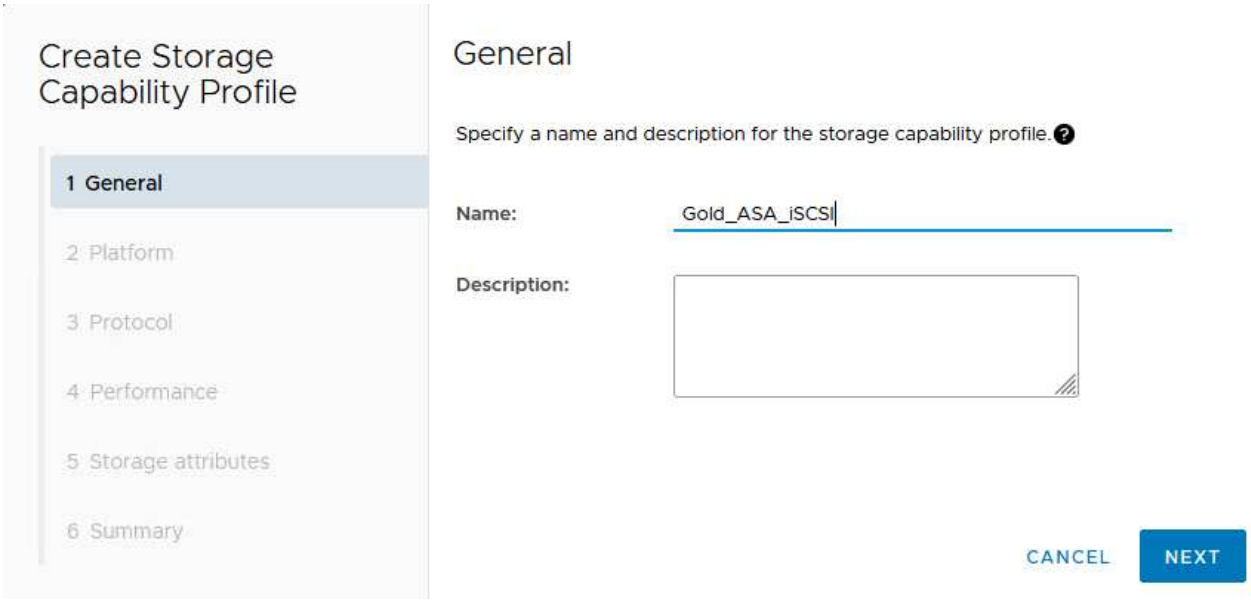
I profili di capacità dello storage descrivono le funzionalità fornite da uno storage array o da un sistema storage. Includono le definizioni della qualità del servizio e vengono utilizzate per selezionare i sistemi storage che soddisfano i parametri definiti nel profilo.

Per creare un profilo di capacità di archiviazione negli strumenti ONTAP, completare i seguenti passaggi:

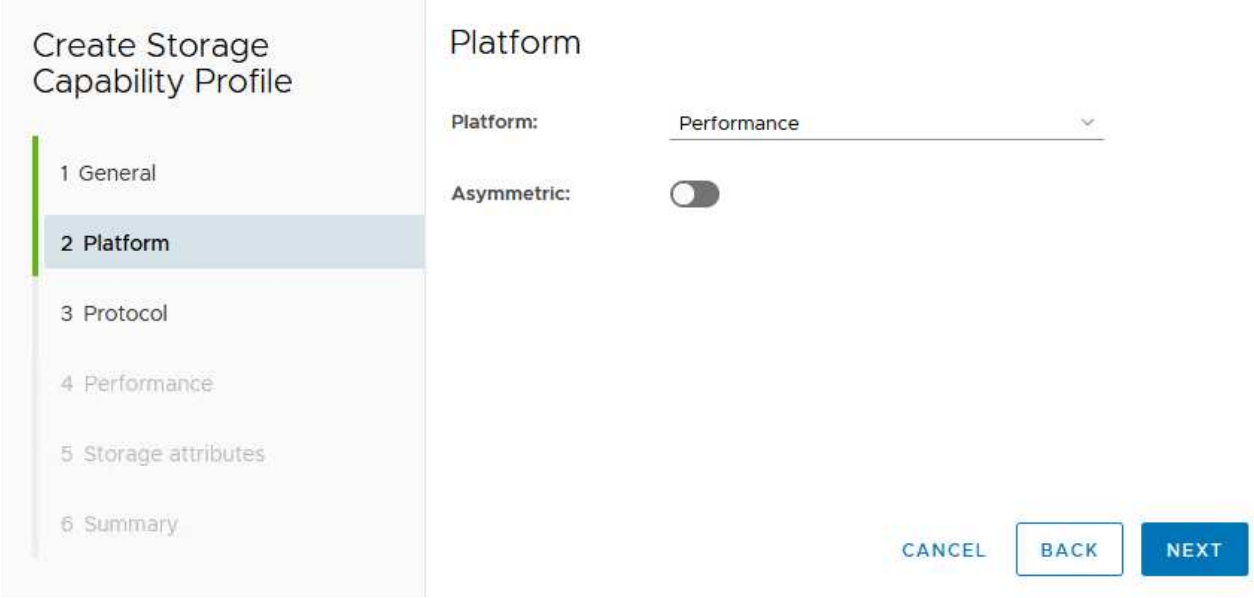
1. In Strumenti di ONTAP, selezionare **Profilo capacità di archiviazione** dal menu a sinistra, quindi premere **Crea**.



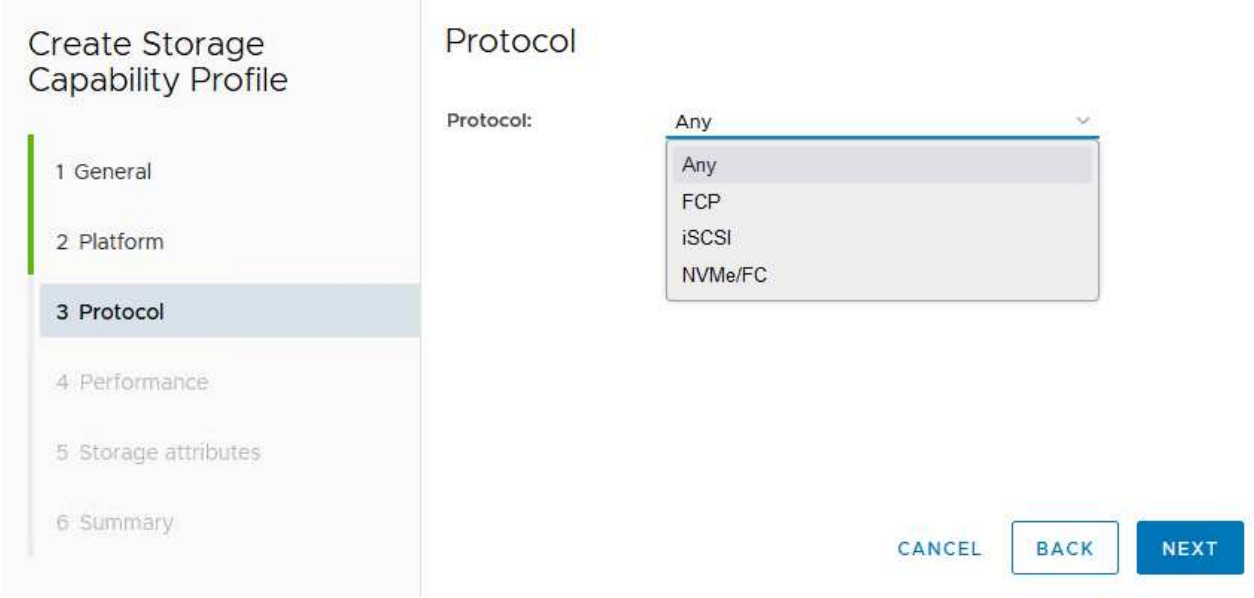
2. Nella procedura guidata **Crea profilo capacità di archiviazione** fornire un nome e una descrizione del profilo e fare clic su **Avanti**.



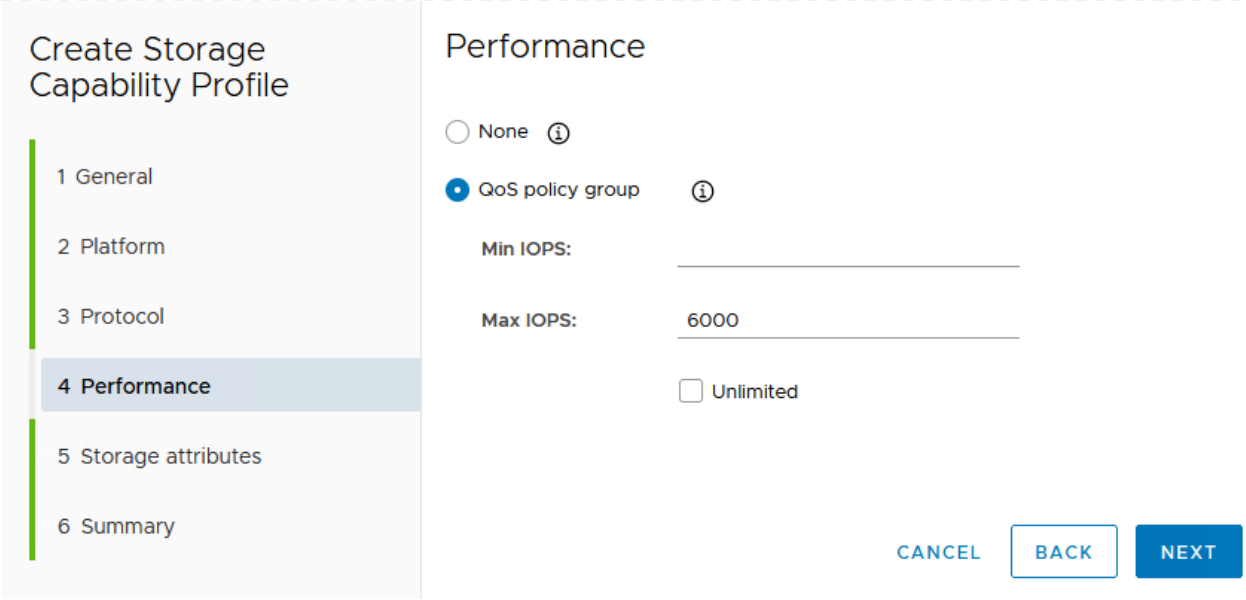
3. Seleziona il tipo di piattaforma e per specificare che il sistema storage deve essere un array SAN all-flash impostato su **asimmetrico** su falso.



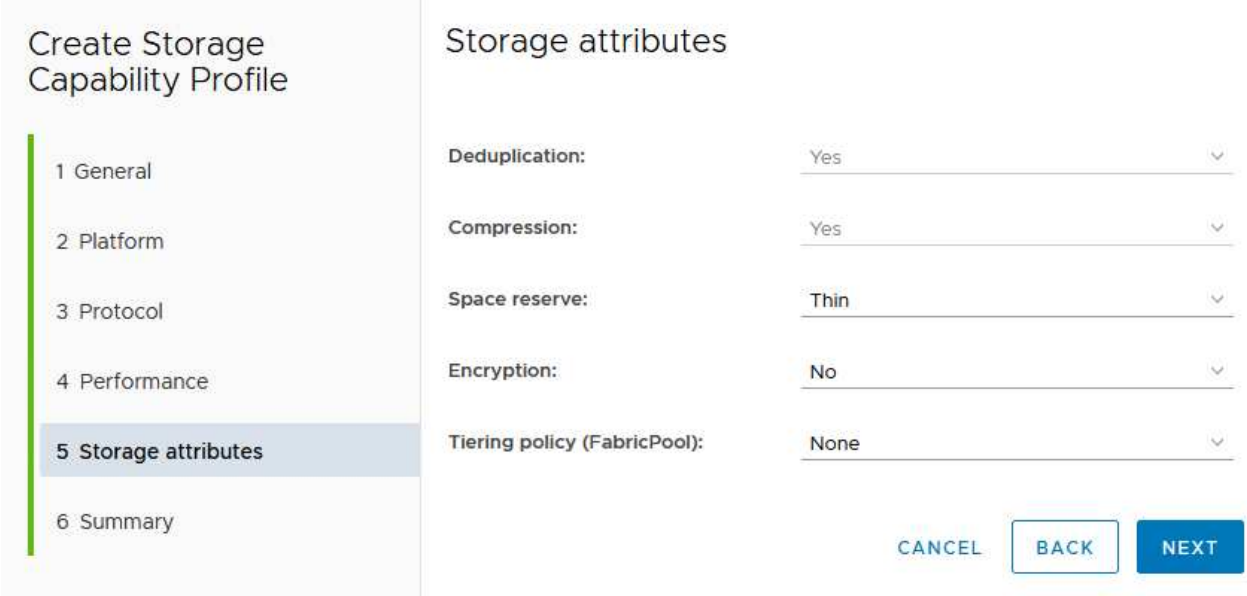
4. Quindi, selezionare Choice of Protocol (scelta del protocollo) o **Any** (qualsiasi) per consentire tutti i protocolli possibili. Fare clic su **Avanti** per continuare.



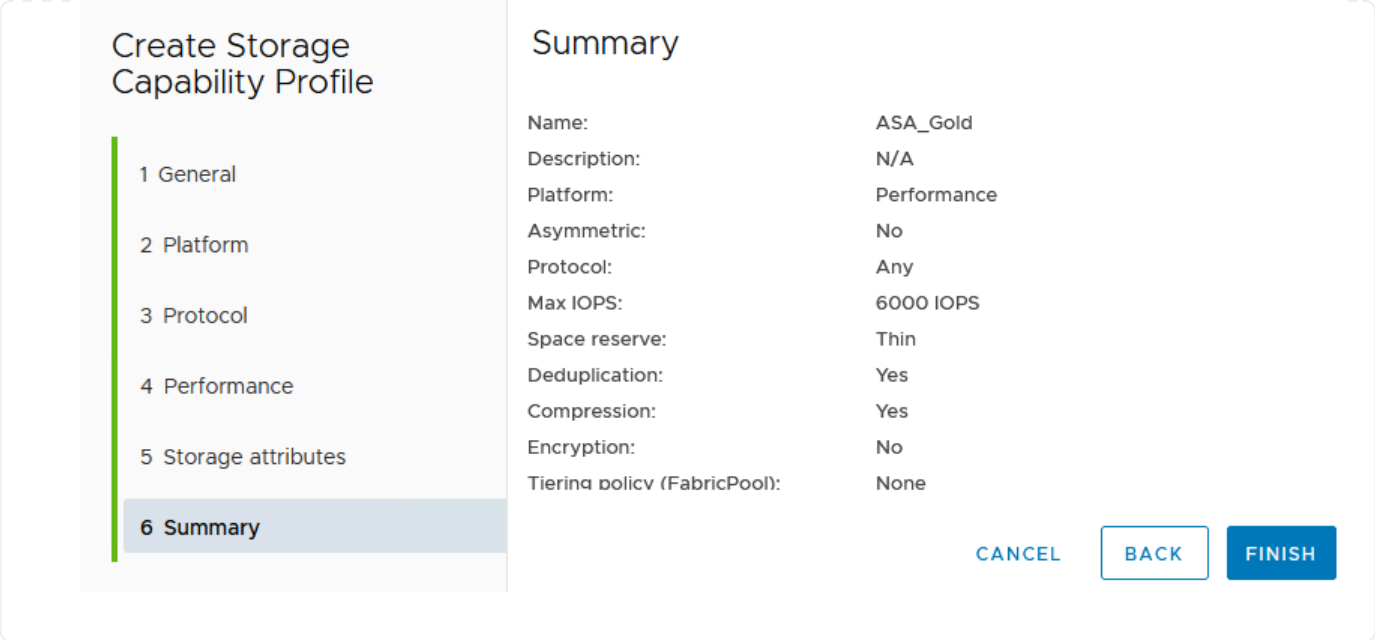
5. La pagina **performance** consente di impostare la qualità del servizio sotto forma di IOPS minimi e massimi consentiti.



6. Completare la pagina **attributi di archiviazione** selezionando l'efficienza di archiviazione, la prenotazione dello spazio, la crittografia e qualsiasi criterio di tiering in base alle esigenze.



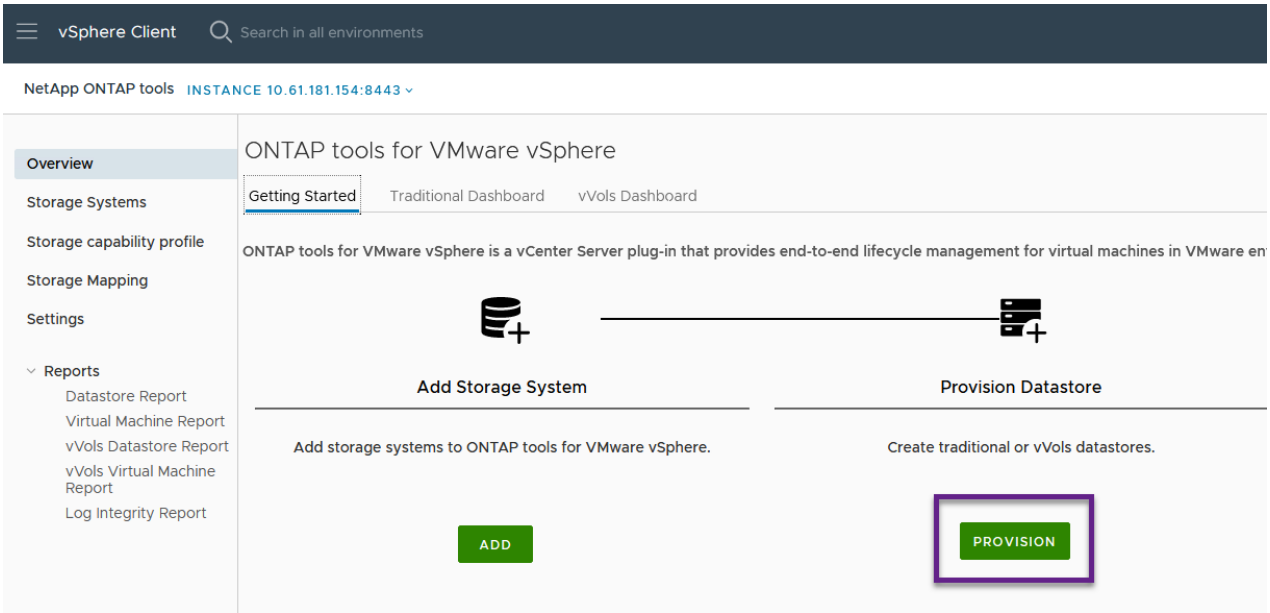
7. Infine, rivedere il riepilogo e fare clic su fine per creare il profilo.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: No
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

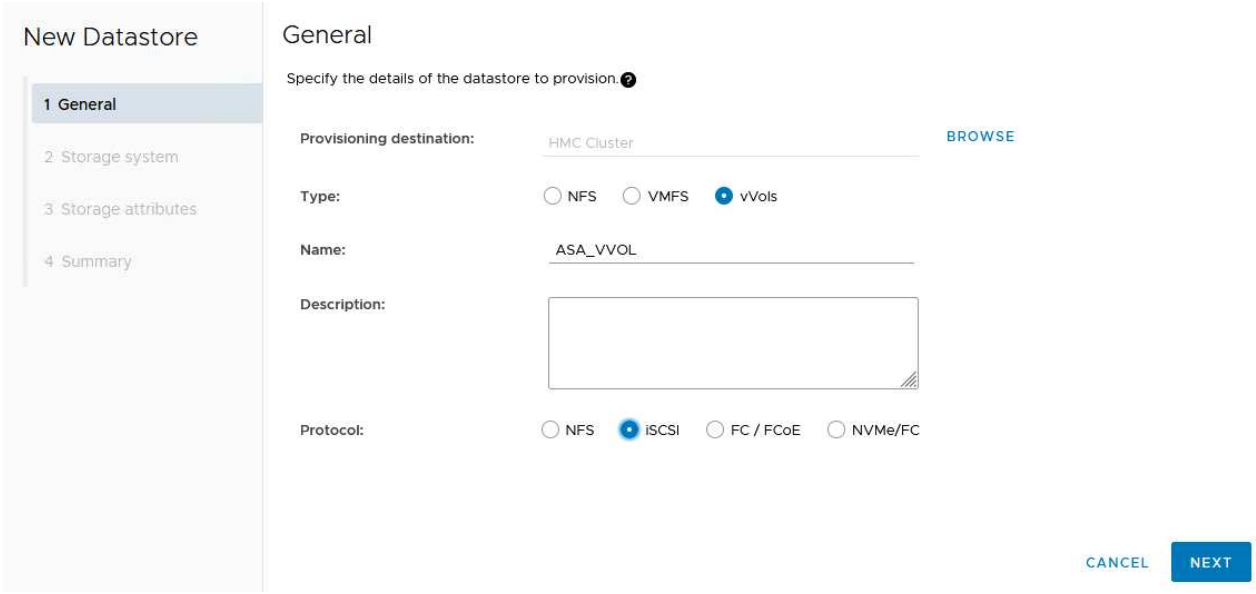
Creare un datastore vVol in ONTAP Tools

Per creare un datastore vVol in Strumenti di ONTAP, attenersi alla seguente procedura:

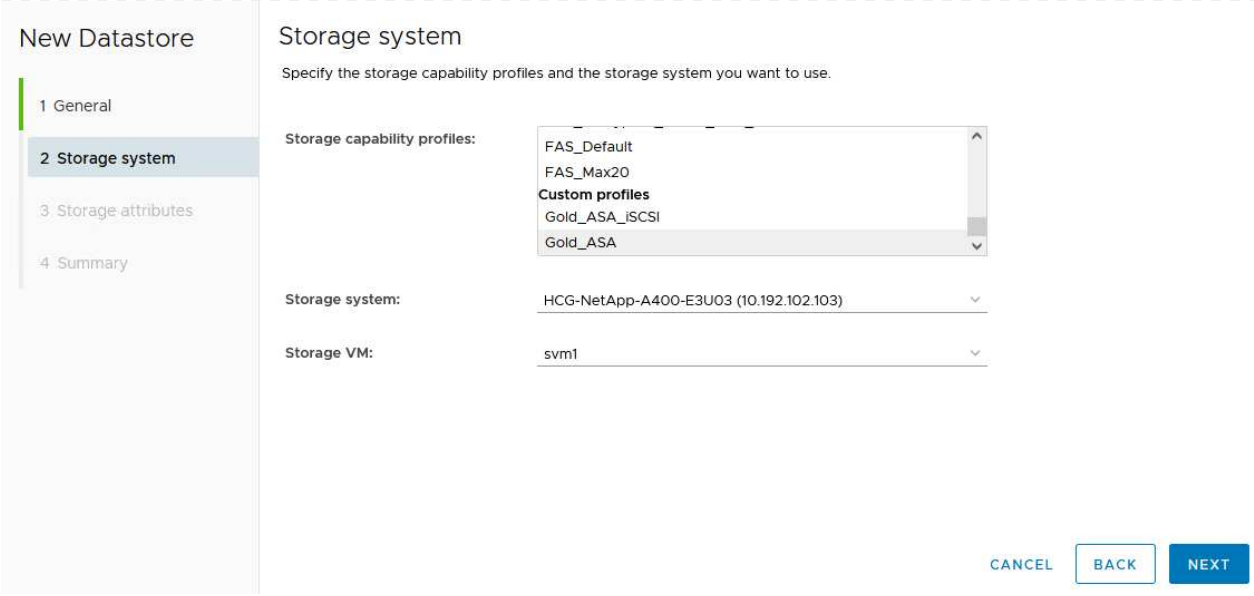
1. In Strumenti di ONTAP selezionare **Panoramica** e dalla scheda **Guida introduttiva** fare clic su **Provision** per avviare la procedura guidata.



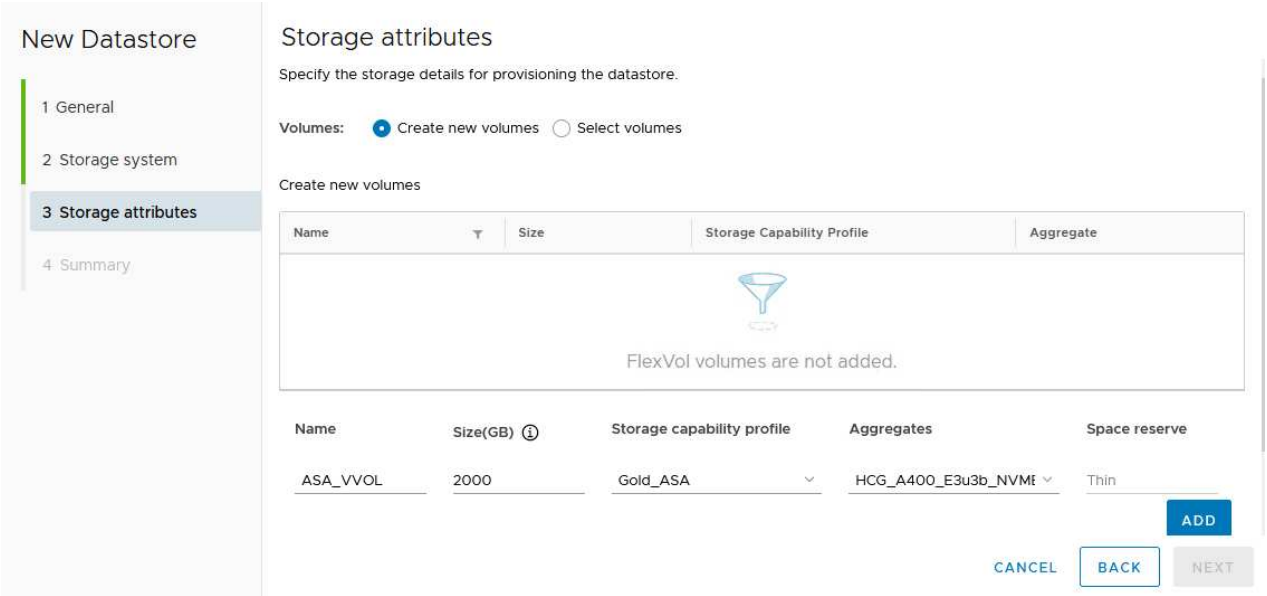
2. Nella pagina **Generale** della procedura guidata nuovo datastore selezionare il data center vSphere o la destinazione del cluster. Selezionare **vVol** come tipo di dastatore, inserire un nome per il datastore e selezionare il protocollo.



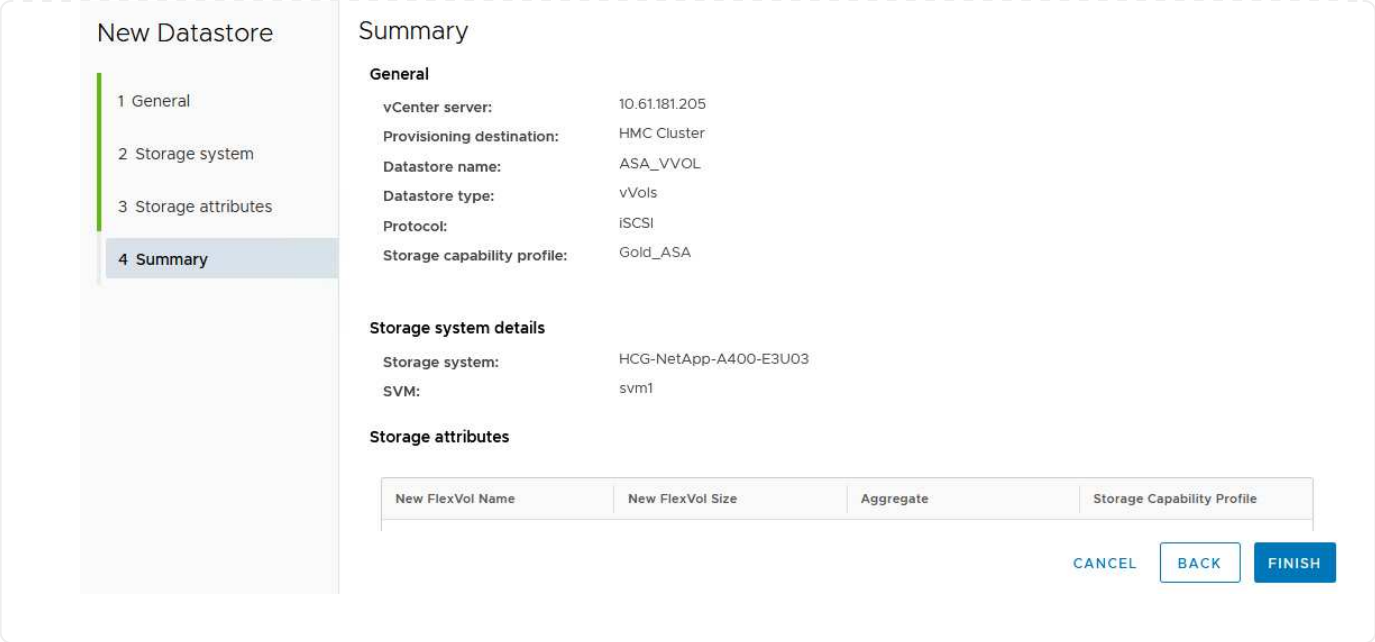
3. Nella pagina **sistema storage**, seleziona un profilo di funzionalità storage, il sistema storage e la SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **attributi archiviazione**, selezionare per creare un nuovo volume per l'archivio dati e specificare gli attributi di archiviazione del volume da creare. Fare clic su **Aggiungi** per creare il volume, quindi su **Avanti** per continuare.



5. Infine, rivedere il riepilogo e fare clic su **fine** per avviare il processo di creazione del datastore vVol.



Creare una policy di storage delle macchine virtuali nel client vSphere

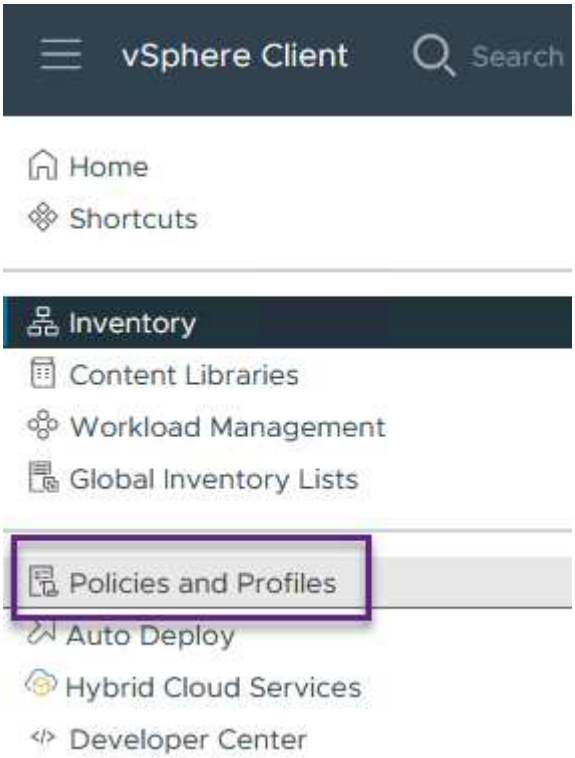
Un criterio di storage delle macchine virtuali è un insieme di regole e requisiti che definiscono le modalità di archiviazione e gestione dei dati delle macchine virtuali. Specifica le caratteristiche di storage desiderate, come performance, disponibilità e servizi dati, per una VM specifica.

In questo caso, il task implica la creazione di una policy per lo storage delle macchine virtuali per specificare che verrà generata una macchina virtuale sui datastore vVol e per stabilire un mapping uno-a-uno con il profilo di funzionalità dello storage precedentemente generato.

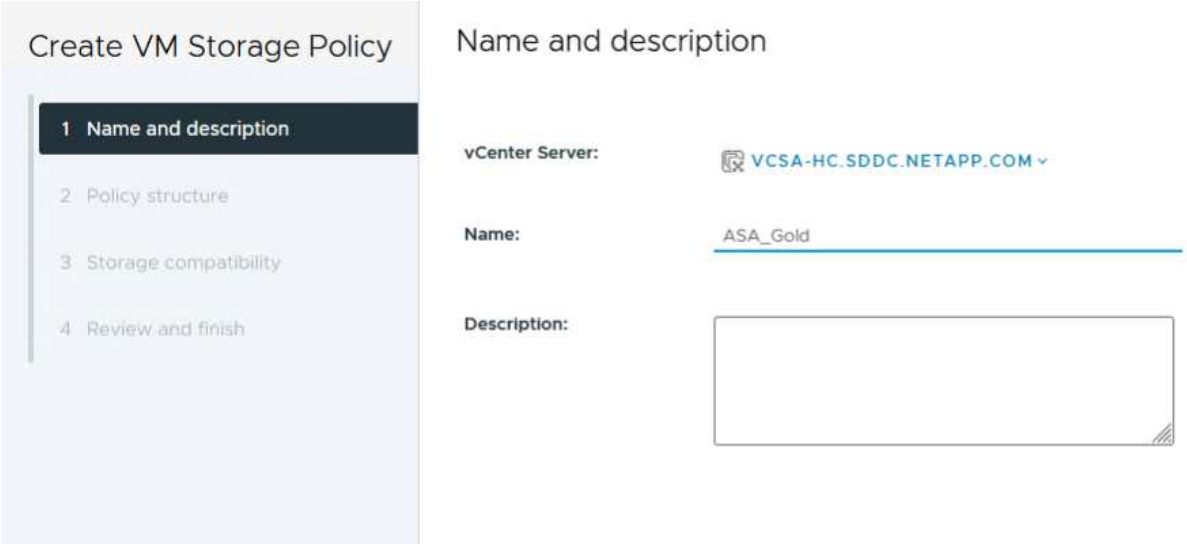
Crea una policy di storage delle macchine virtuali

Per creare un criterio di archiviazione VM, completare i seguenti passaggi:

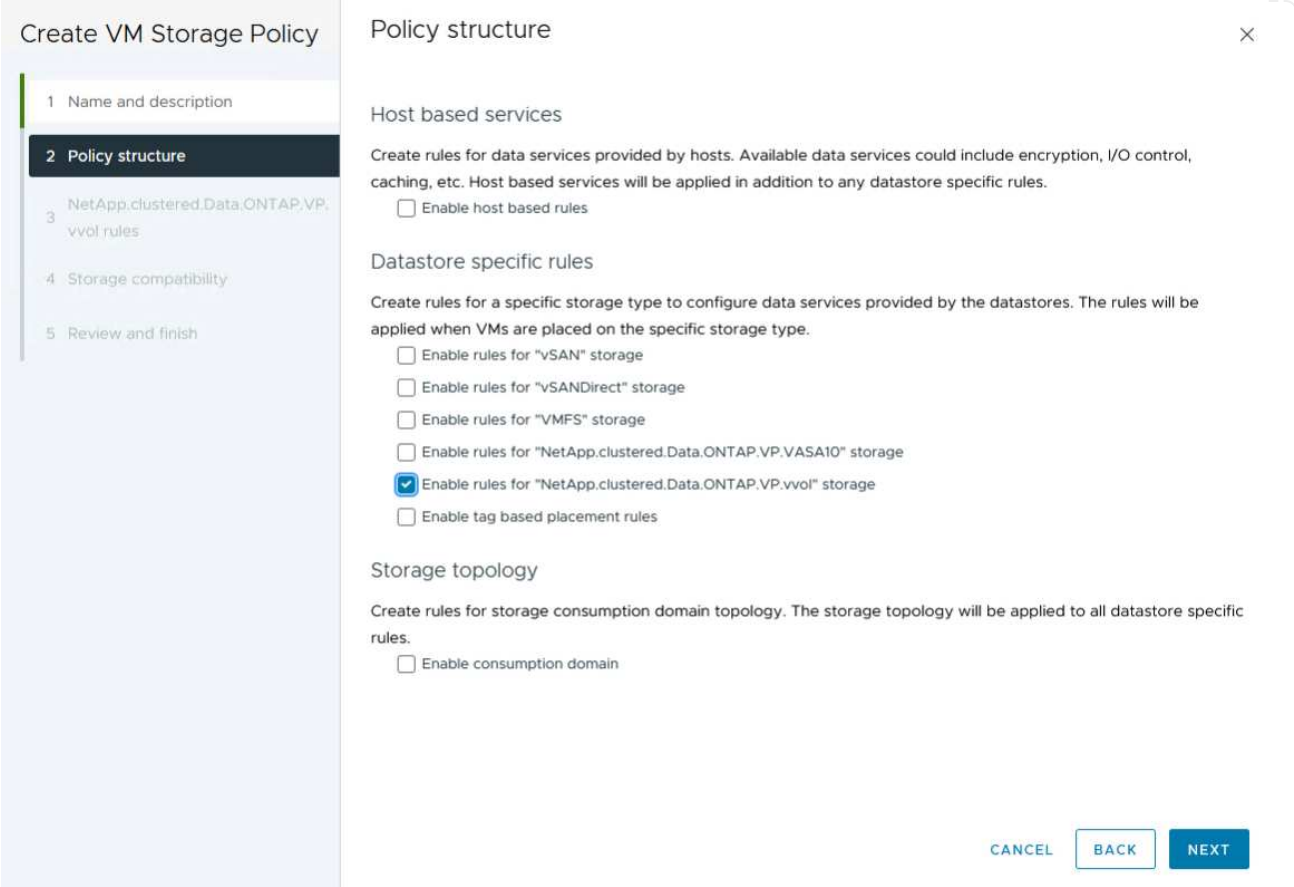
1. Dal menu principale dei client vSphere, selezionare **Criteri e profili**.



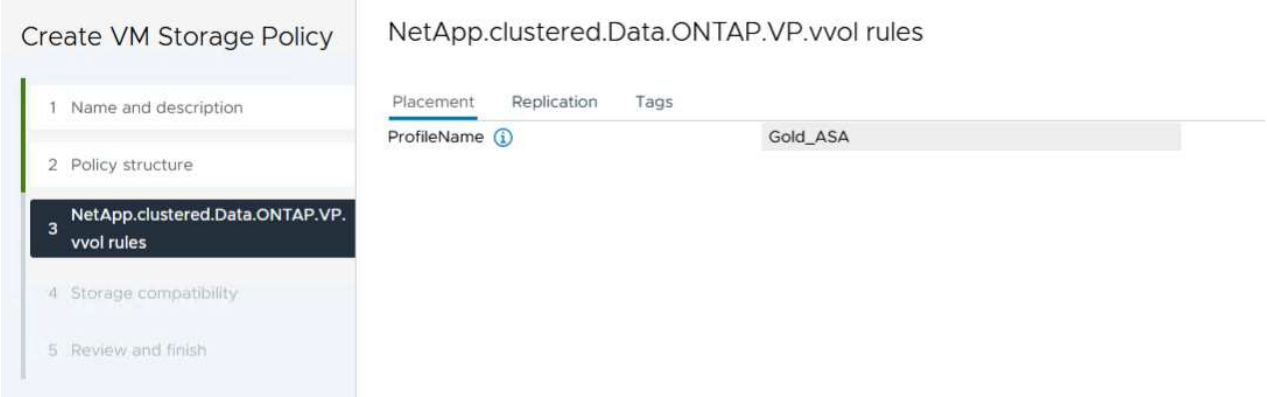
2. Nella procedura guidata **Create VM Storage Policy** (Crea criterio di archiviazione VM), compilare prima un nome e una descrizione per il criterio e fare clic su **Next** (Avanti) per continuare.



3. Nella pagina **struttura criteri**, selezionare per abilitare le regole per lo storage vVol di NetApp Clustered Data ONTAP e fare clic su **Avanti**.



4. Nella pagina successiva, specifica della struttura dei criteri scelta, selezionare il profilo delle capacità di storage che descrive i sistemi storage da utilizzare nei criteri storage delle macchine virtuali. Fare clic su **Avanti** per continuare.



5. Nella pagina **compatibilità storage**, esaminare l'elenco dei datastore vSAN che corrispondono a questo criterio e fare clic su **Avanti**.
6. Infine, rivedere il criterio da implementare e fare clic su **fine** per creare il criterio.

Creare una policy di storage delle macchine virtuali nel client vSphere

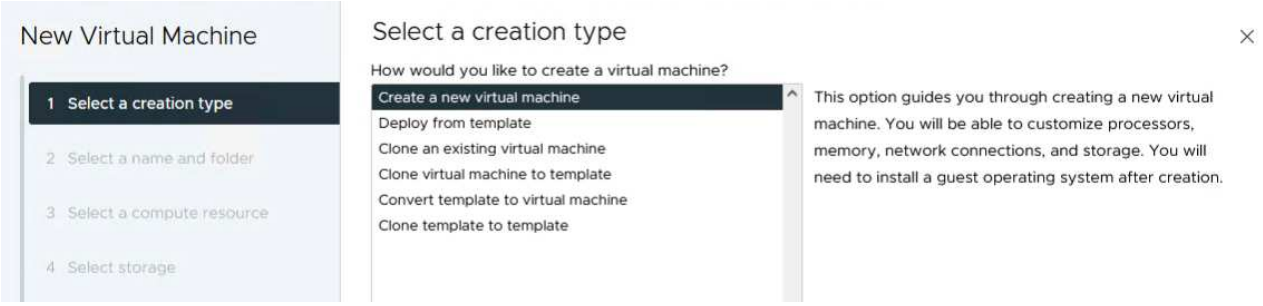
Un criterio di storage delle macchine virtuali è un insieme di regole e requisiti che definiscono le modalità di archiviazione e gestione dei dati delle macchine virtuali. Specifica le caratteristiche di storage desiderate, come performance, disponibilità e servizi dati, per una VM specifica.

In questo caso, il task implica la creazione di una policy per lo storage delle macchine virtuali per specificare che verrà generata una macchina virtuale sui datastore vVol e per stabilire un mapping uno-a-uno con il profilo di funzionalità dello storage precedentemente generato.

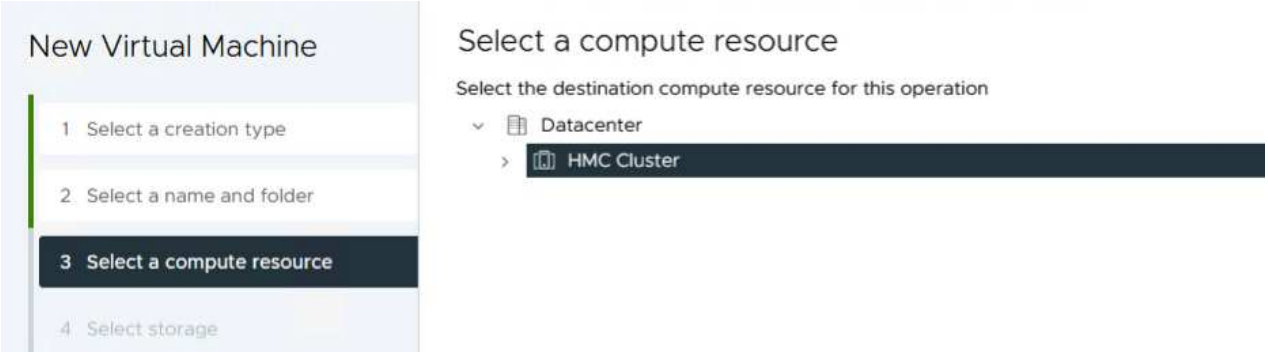
Creare una macchina virtuale su un datastore vVol

Infine, occorre creare una macchina virtuale utilizzando i criteri di storage delle macchine virtuali creati in precedenza:

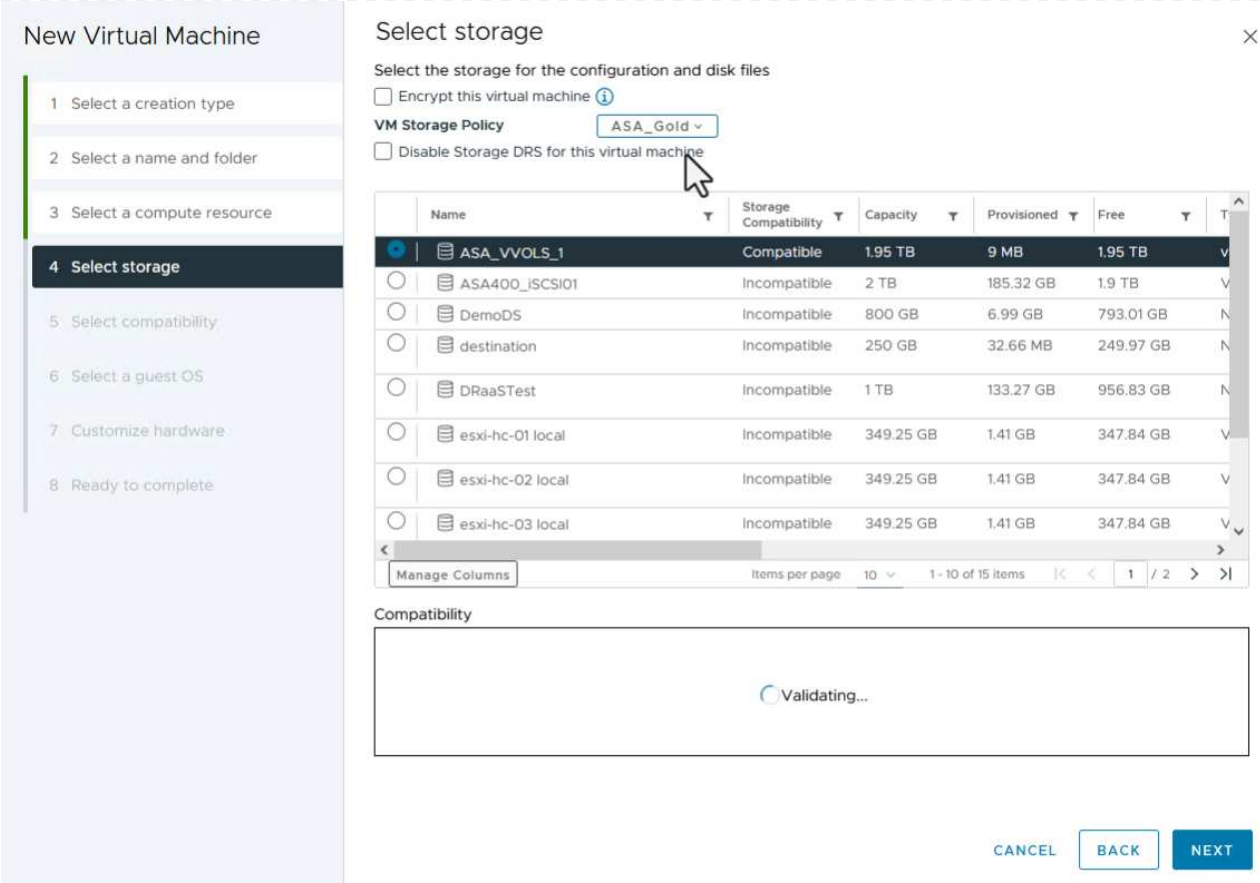
1. Dalla procedura guidata **Nuova macchina virtuale** selezionare **Crea nuova macchina virtuale** e selezionare **Avanti** per continuare.



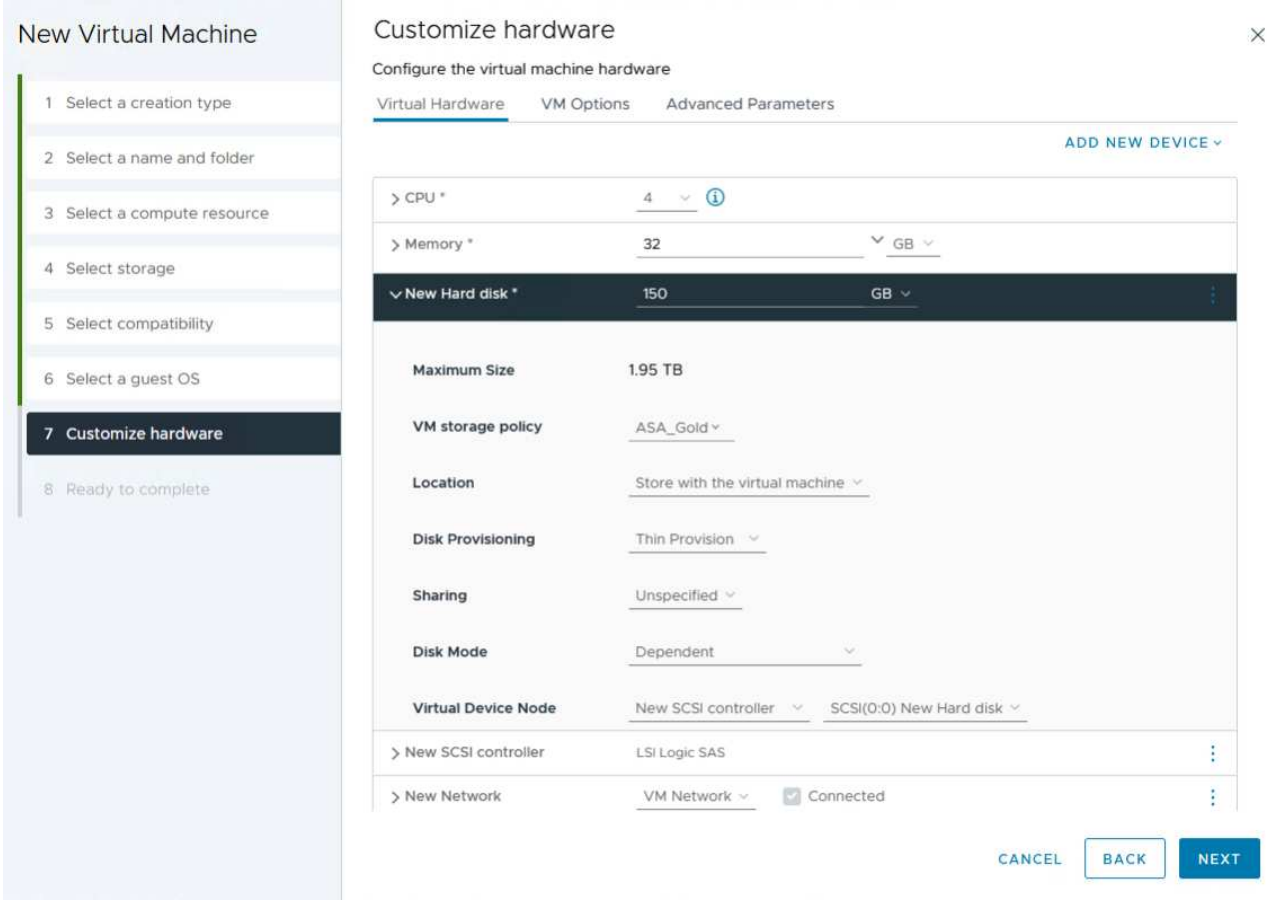
2. Immettere un nome e selezionare una posizione per la macchina virtuale e fare clic su **Avanti**.
3. Nella pagina **Select a compute resource** (Seleziona una risorsa di elaborazione), selezionare una destinazione e fare clic su **Next** (Avanti).



4. Nella pagina **Select storage** (Seleziona storage), seleziona un criterio storage per le macchine virtuali e il datastore vVol che corrisponderanno alla destinazione della macchina virtuale. Fare clic su **Avanti**.



5. Nella pagina **Select Compatibility** (Seleziona compatibilità), scegliere le versioni vSphere con cui sarà compatibile la VM.
6. Selezionare la famiglia e la versione del sistema operativo guest per la nuova macchina virtuale e fare clic su **Avanti**.
7. Compilare la pagina **Personalizza hardware**. Si noti che è possibile selezionare un criterio di archiviazione VM separato per ogni disco rigido (file VMDK).



8. Infine, rivedere la pagina di riepilogo e fare clic su **fine** per creare la VM.

In sintesi, NetApp ONTAP Tools automatizza il processo di creazione di datastore vVol sui sistemi storage ONTAP, I profili di funzionalità dello storage definiscono non solo i sistemi storage da utilizzare per la creazione di datastore, ma anche le policy di qualità del servizio che è possibile implementare in base a un singolo VMDK. VVol offre un paradigma di gestione dello storage semplificato e la stretta integrazione tra NetApp e VMware rende questa soluzione pratica per un controllo granulare, efficiente e ottimizzato sugli ambienti virtualizzati.

Array SAN all-flash NetApp con VMware vSphere 8

NetApp Cloud Insights è una piattaforma di monitoring e analytics dell'infrastruttura basata su cloud progettata per fornire visibilità e informazioni complete su performance, salute e costi delle infrastrutture IT, sia on-premise che nel cloud. Le funzioni principali di NetApp Cloud Insights includono monitoraggio in tempo reale, dashboard personalizzabili, analytics predittivi e strumenti di ottimizzazione dei costi, consentendo alle organizzazioni di gestire e ottimizzare in modo efficace i propri ambienti on-premise e cloud.

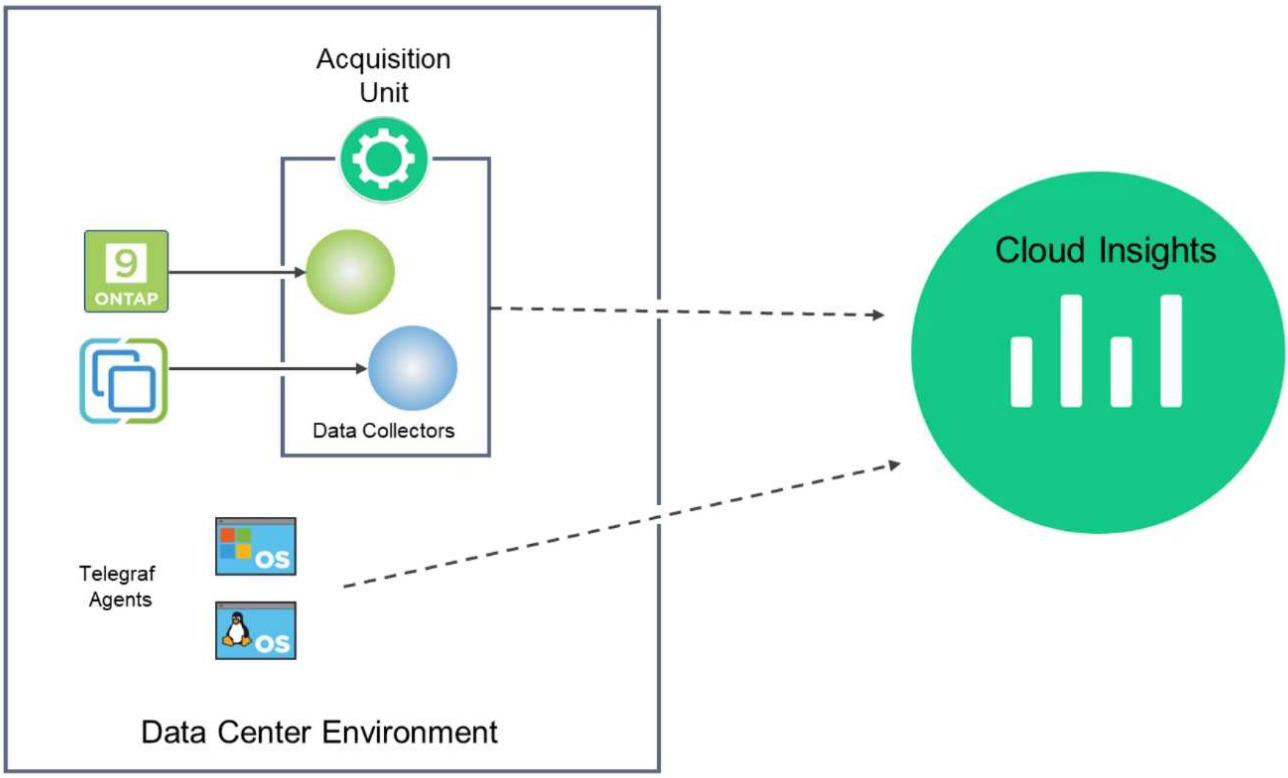
Autore: Josh Powell - NetApp Solutions Engineering

Monitoraggio dello storage on-premise con NetApp Cloud Insights

NetApp Cloud Insights opera attraverso il software dell'unità di acquisizione, che è configurato con i raccoglitori di dati per asset come VMware vSphere e i sistemi storage NetApp ONTAP. Questi raccoglitori raccolgono i

dati e li trasmettono a Cloud Insights. La piattaforma utilizza quindi una varietà di dashboard, widget e query di metrica per organizzare i dati in analisi approfondite che gli utenti possono interpretare.

Schema dell'architettura Cloud Insights:



Panoramica sull'implementazione della soluzione

Questa soluzione fornisce un'introduzione al monitoring dei sistemi storage on-premise di VMware vSphere e ONTAP utilizzando NetApp Cloud Insights.

Questo elenco fornisce i passaggi di alto livello trattati in questa soluzione:

1. Configurare Data Collector per un cluster vSphere.
2. Configurare Data Collector per un sistema di archiviazione ONTAP.
3. Utilizzare le regole di annotazione per contrassegnare le risorse.
4. Esplorare e correlare le risorse.
5. USA una dashboard superiore della latenza delle macchine virtuali per isolare i noisy neighbor.
6. Identifica le opportunità per il corretto dimensionamento delle macchine virtuali.
7. Utilizzare le query per isolare e ordinare le metriche.

Prerequisiti

Questa soluzione utilizza i seguenti componenti:

1. Array SAN all-flash NetApp A400 con ONTAP 9,13.
2. Cluster VMware vSphere 8,0.

3. Account NetApp Cloud Insights.
4. Software dell’unità di acquisizione NetApp Cloud Insights installato su una macchina virtuale locale con connettività di rete agli asset per la raccolta dei dati.

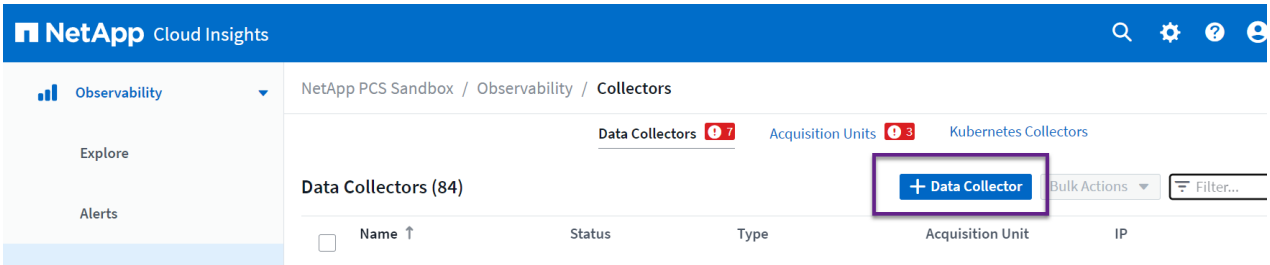
Implementazione della soluzione

Configurare Data Collector

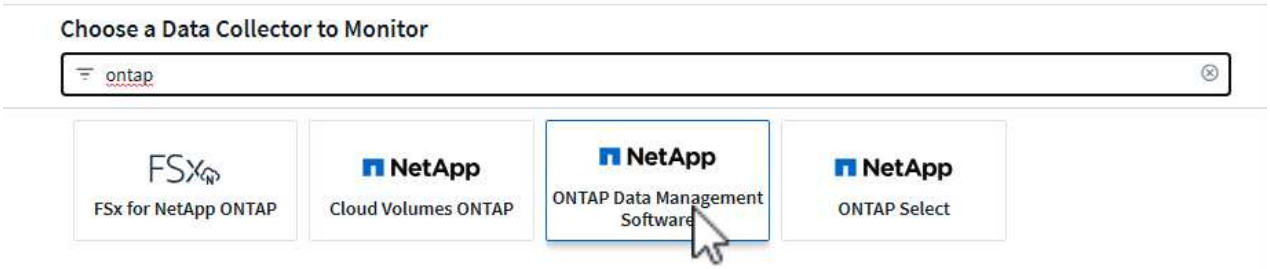
Per configurare Data Collector per i sistemi di storage VMware vSphere e ONTAP, completare i seguenti passaggi:

Aggiunta di un Data Collector per un sistema di archiviazione ONTAP

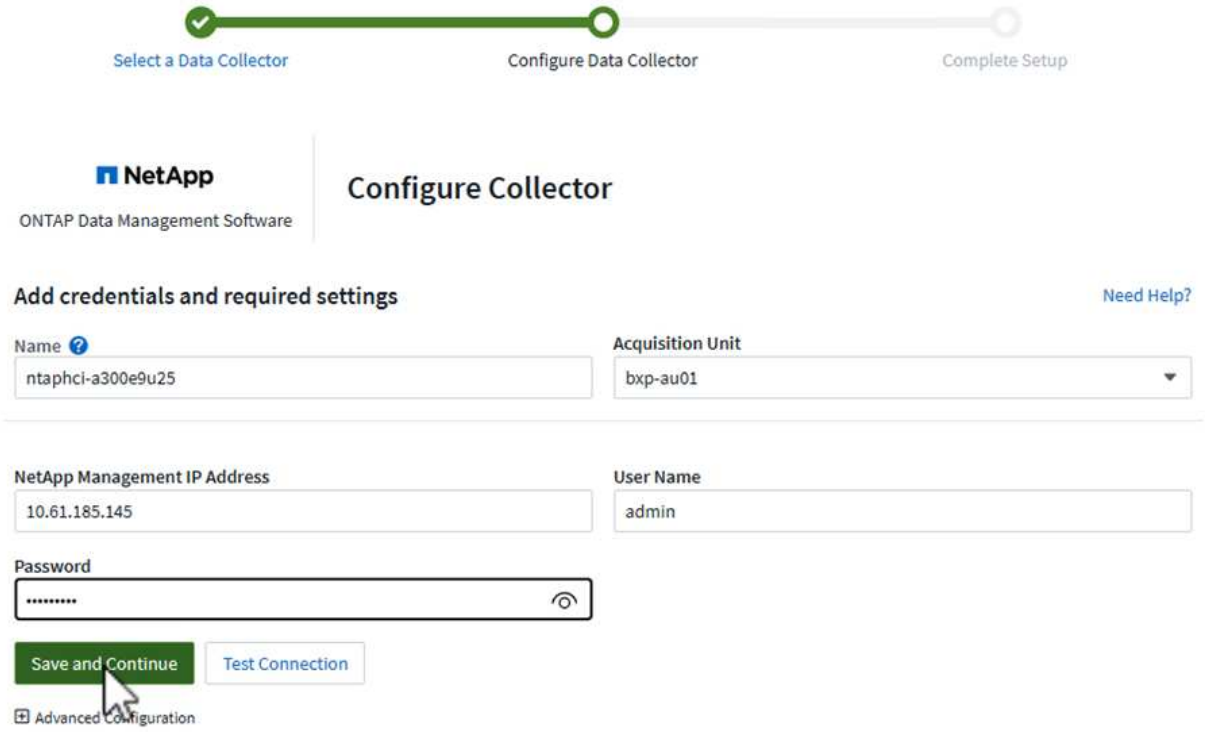
1. Una volta effettuato l'accesso a Cloud Insights, accedere a **osservabilità > Collector > Data Collector** e premere il pulsante per installare un nuovo Data Collector.



2. Da qui cercare **ONTAP** e fare clic su **Software di gestione dati ONTAP**.

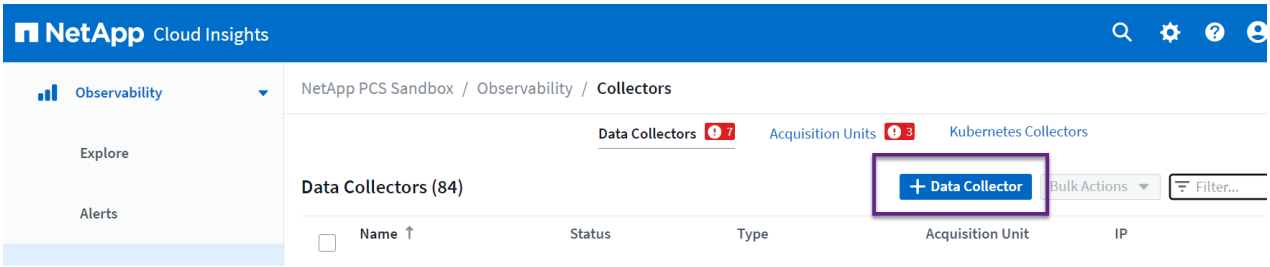


3. Nella pagina **Configure Collector** (Configura modulo di raccolta) compilare un nome per il raccoglitore, specificare l'unità di acquisizione * corretta e fornire le credenziali per il sistema di archiviazione ONTAP. Fare clic su **Salva e continua**, quindi su **completa installazione** nella parte inferiore della pagina per completare la configurazione.

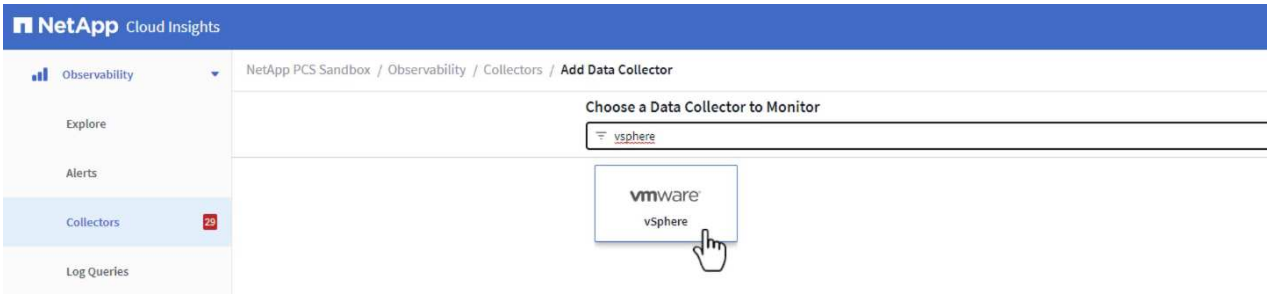


Aggiunta di un Data Collector per un cluster VMware vSphere

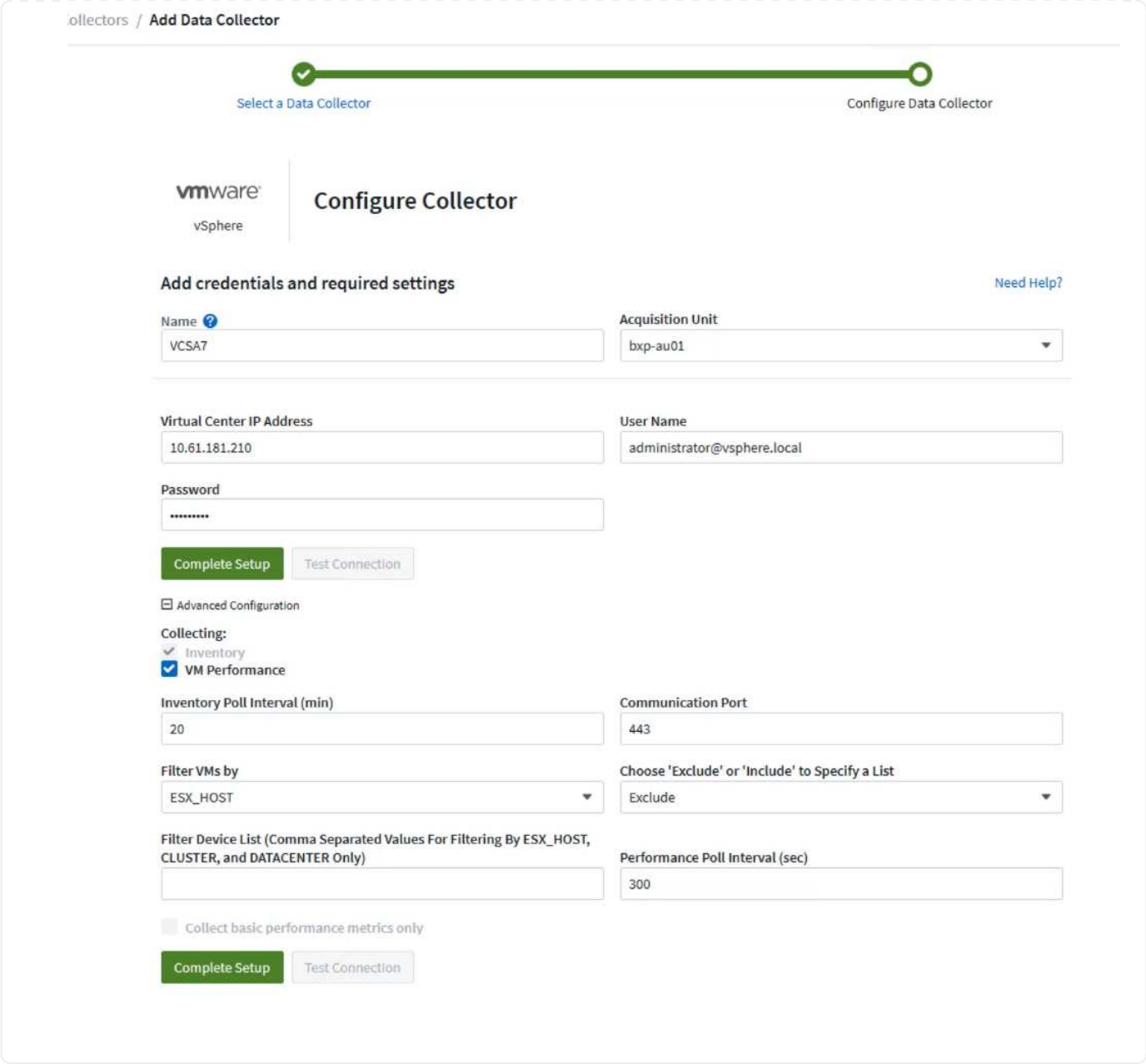
1. Ancora una volta, accedere a **osservabilità > Collector > Data Collector** e premere il pulsante per installare un nuovo Data Collector.



2. Da qui cercare **vSphere** e fare clic su **VMware vSphere**.



3. Nella pagina **Configure Collector** compilare un nome per il Collector, specificare l'unità di acquisizione * corretta e fornire le credenziali per il server vCenter. Fare clic su **Salva e continua**, quindi su **completa installazione** nella parte inferiore della pagina per completare la configurazione.



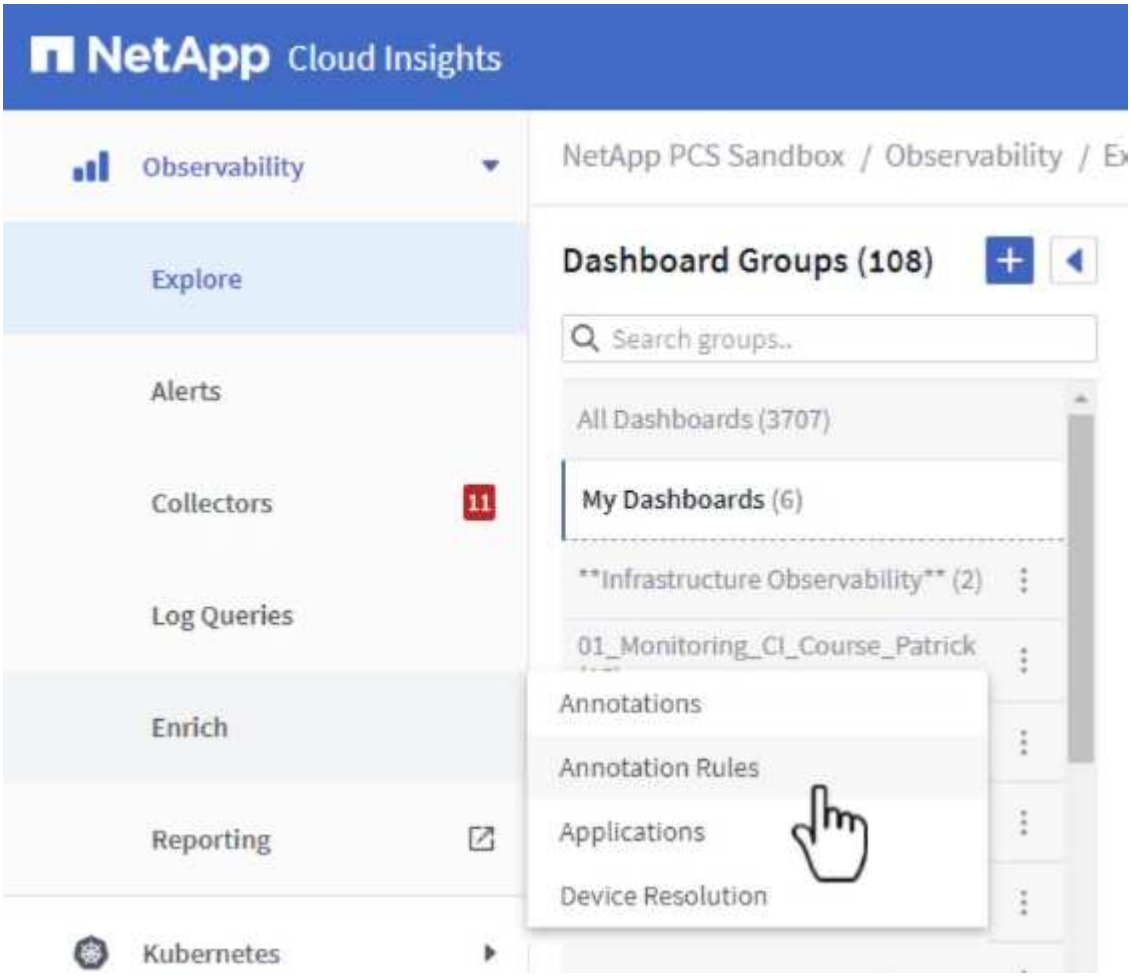
Aggiungere annotazioni alle risorse

Le annotazioni sono un metodo utile per contrassegnare le risorse in modo che possano essere filtrate e altrimenti identificate nelle varie viste e query metriche disponibili in Cloud Insights.

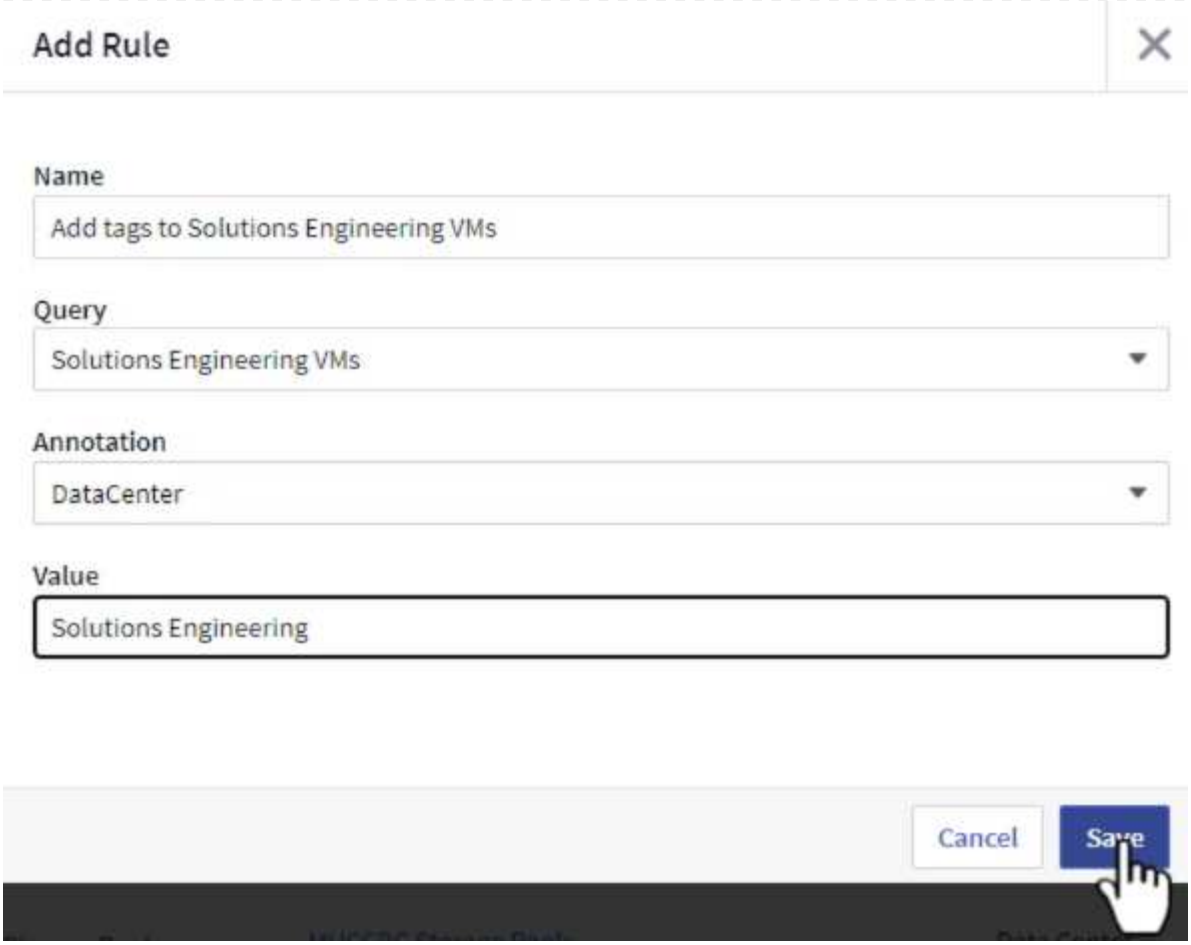
In questa sezione, le annotazioni verranno aggiunte alle risorse delle macchine virtuali per il filtraggio da parte di **Data Center**.

Utilizzare le regole di annotazione per contrassegnare le risorse

1. Nel menu a sinistra, accedere a **osservabilità > arricchimento > regole di annotazione** e fare clic sul pulsante **+ regola** in alto a destra per aggiungere una nuova regola.



2. Nella finestra di dialogo **Aggiungi regola** immettere un nome per la regola, individuare una query a cui applicare la regola, il campo di annotazione interessato e il valore da compilare.



3. Infine, nell'angolo superiore destro della pagina **regole annotazione** fare clic su **Esegui tutte le regole** per eseguire la regola e applicare l'annotazione alle risorse.

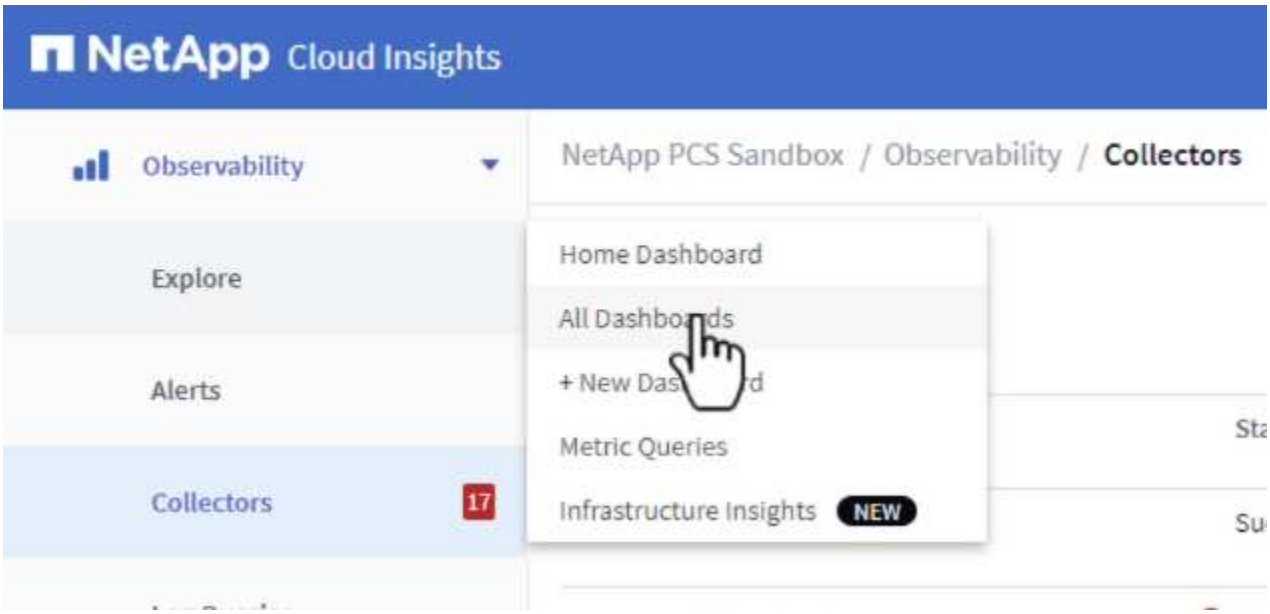
Esplorare e correlare le risorse

Cloud Insights trae conclusioni logiche circa le risorse in esecuzione sui sistemi storage e sui cluster vsphere.

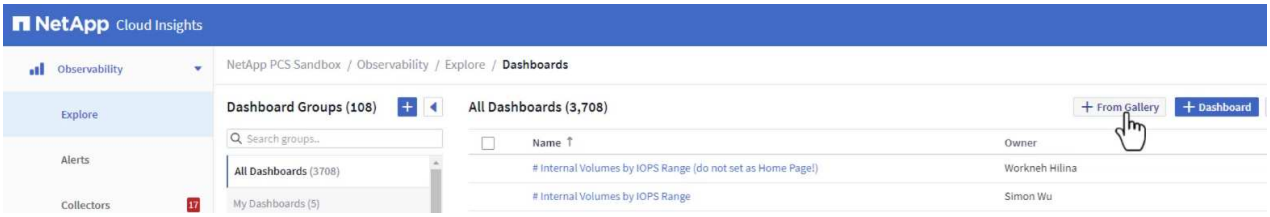
In questa sezione viene illustrato come utilizzare i dashboard per correlare le risorse.

Correlazione delle risorse da una dashboard delle performance dello storage

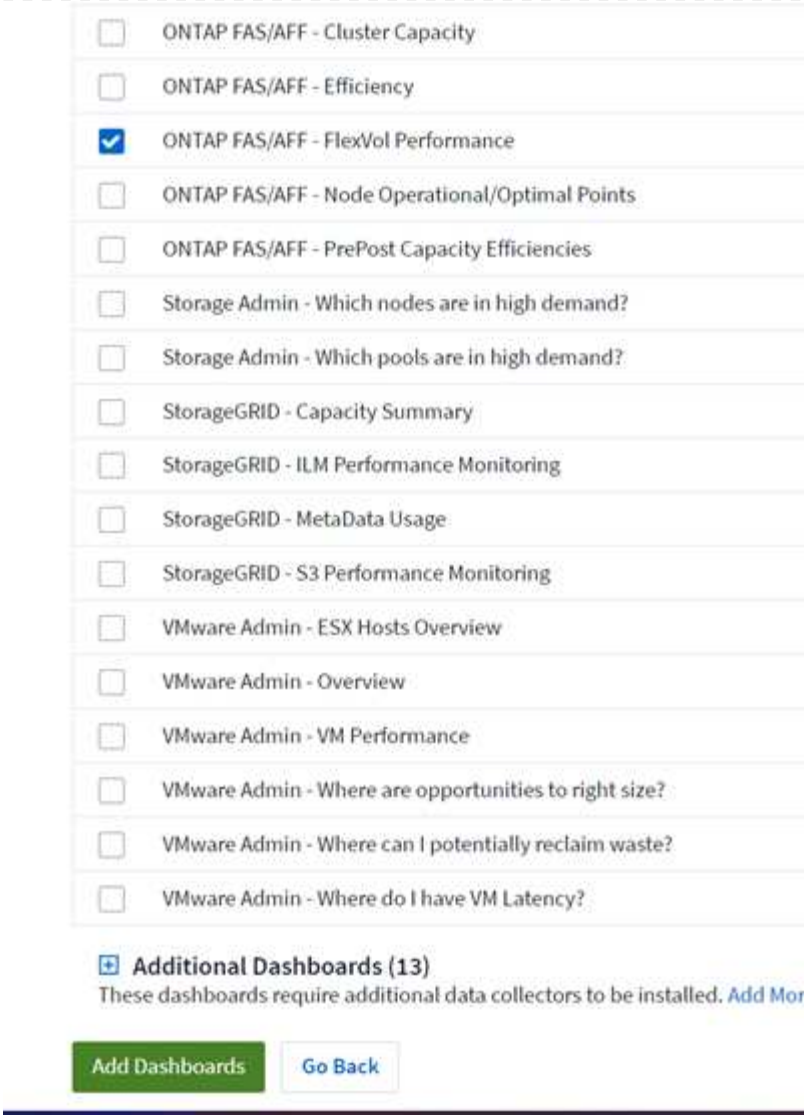
1. Nel menu a sinistra, accedere a **osservabilità > Esplora > tutti i dashboard**.



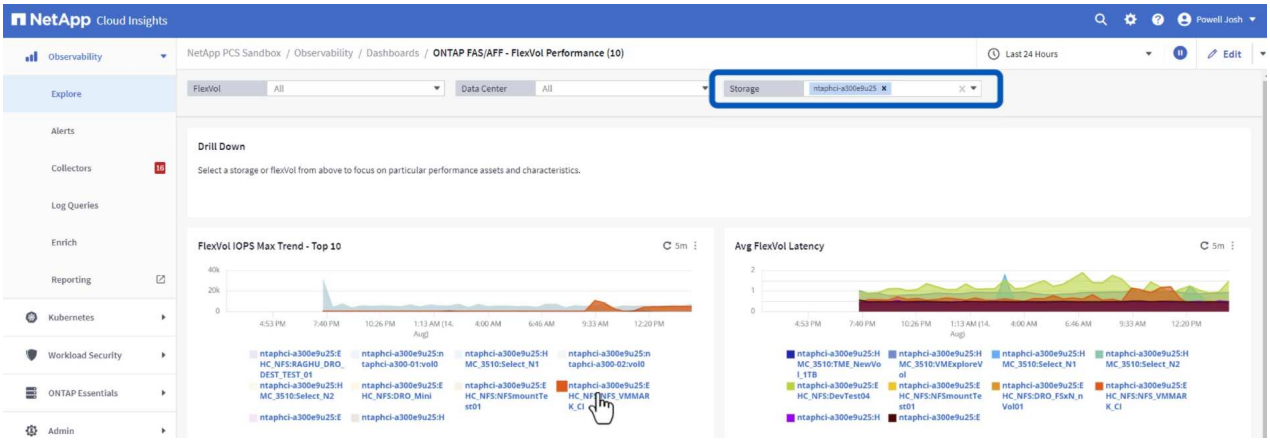
2. Fare clic sul pulsante **+ da galleria** per visualizzare un elenco di dashboard pronti per l'uso che è possibile importare.



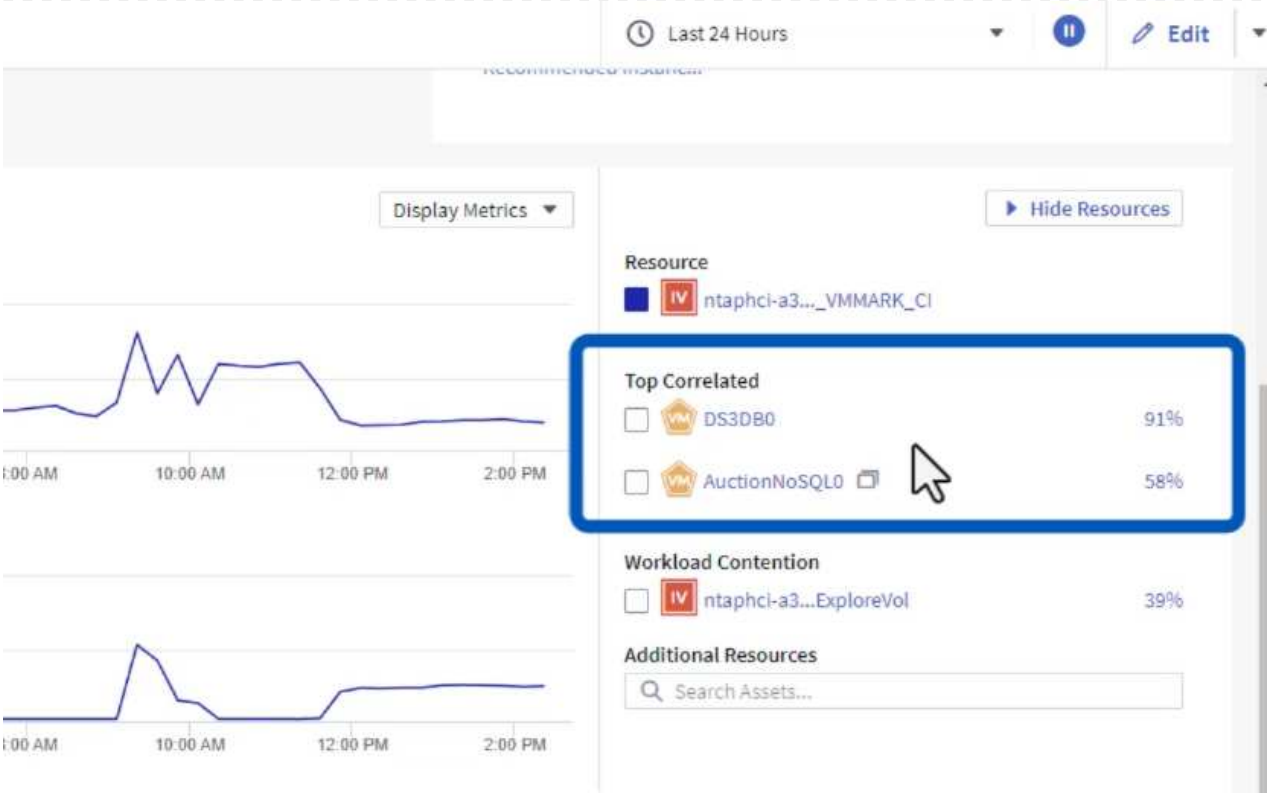
3. Scegliere un dashboard per le prestazioni FlexVol dall'elenco e fare clic sul pulsante **Aggiungi dashboard** nella parte inferiore della pagina.



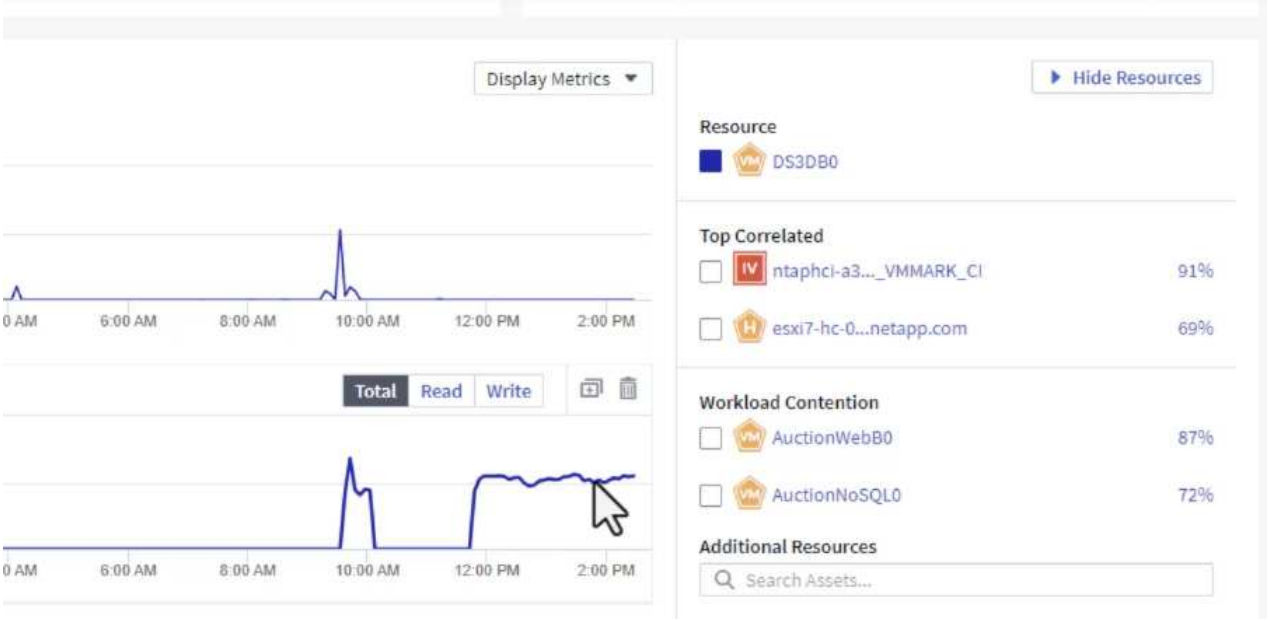
4. Una volta importata, aprire la dashboard. Da qui è possibile visualizzare vari widget con dati dettagliati sulle prestazioni. Aggiungi un filtro per visualizzare un singolo sistema di storage e seleziona un volume di storage per analizzare i dettagli.



5. Da questa vista sono visibili le varie metriche correlate a questo volume di storage e al top utilizzato e delle macchine virtuali correlate in esecuzione sul volume.



6. Facendo clic sulla macchina virtuale con i risultati di utilizzo più elevati nelle metriche per tale macchina virtuale, è possibile visualizzare eventuali problemi potenziali.



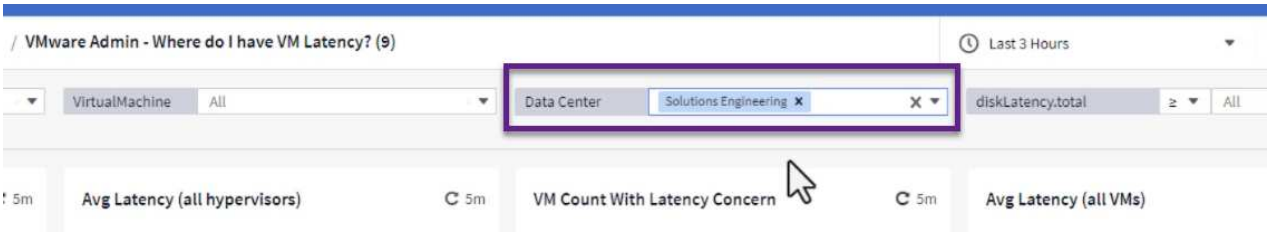
USA Cloud Insights per identificare i noisy neighbor

Cloud Insights presenta dashboard in grado di isolare facilmente peer VM che hanno un impatto negativo sulle altre VM in esecuzione sullo stesso volume storage.

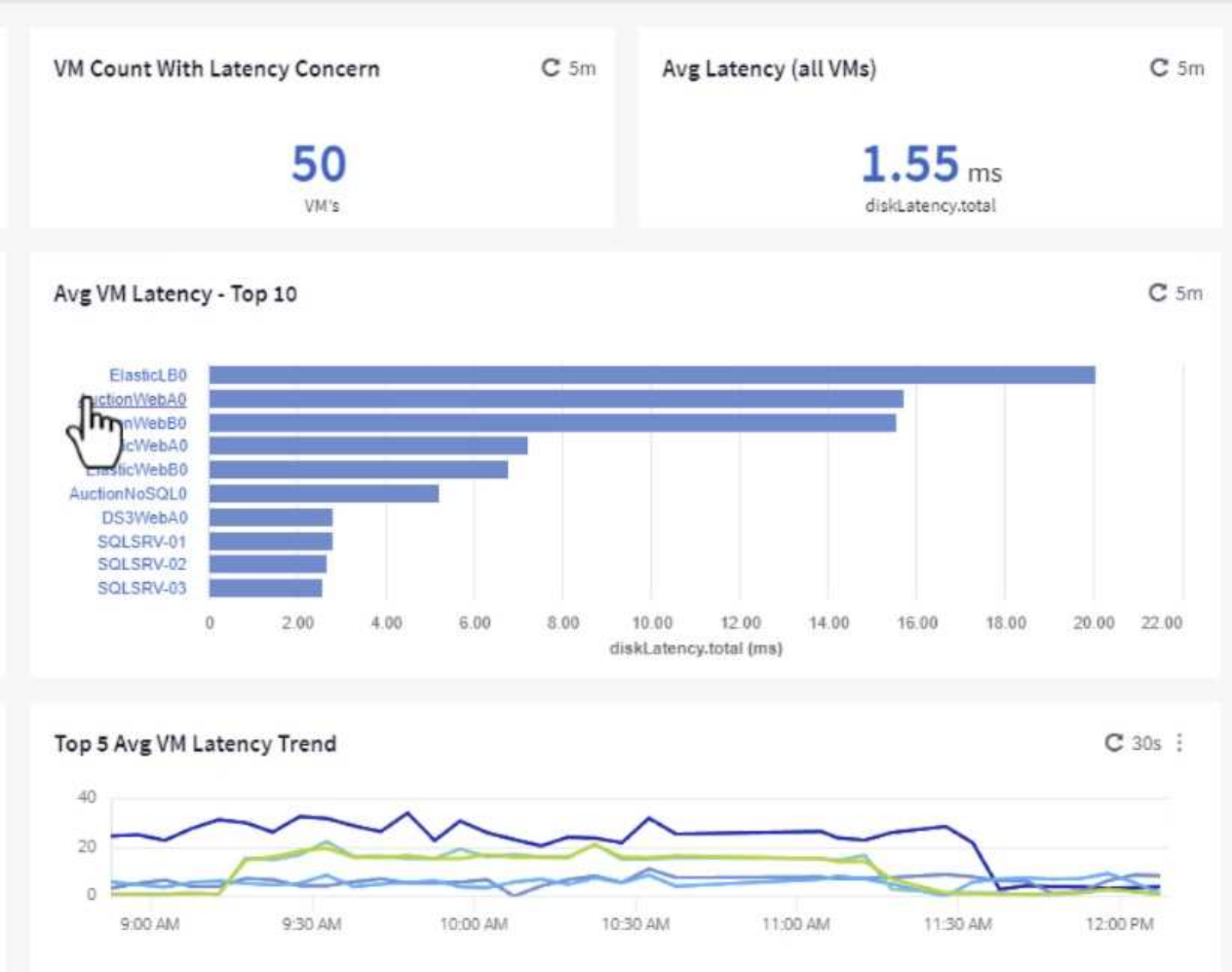
USA una dashboard superiore della latenza delle macchine virtuali per isolare i noisy neighbor

1. In questo esempio si accede a una dashboard disponibile nella **Gallery** chiamata **VMware Admin - dove si trova la latenza della VM?**

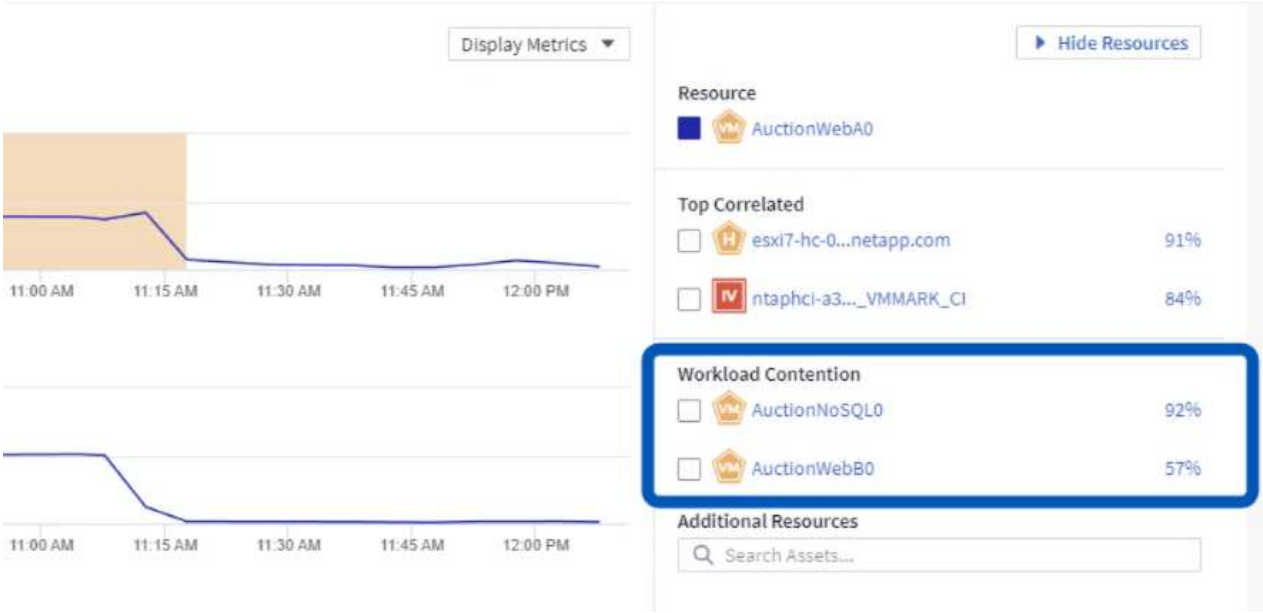
2. Successivamente, filtrare in base all'annotazione **Data Center** creata in una fase precedente per visualizzare un sottoinsieme di risorse.



3. Questa dashboard mostra un elenco delle 10 macchine virtuali principali in base alla latenza media. Da qui, fare clic sulla VM di interesse per approfondire i dettagli.



4. Le VM che potenzialmente causano un conflitto nel carico di lavoro sono elencate e disponibili. Analizza in dettaglio le metriche relative alle prestazioni di queste VM per esaminare eventuali problemi potenziali.

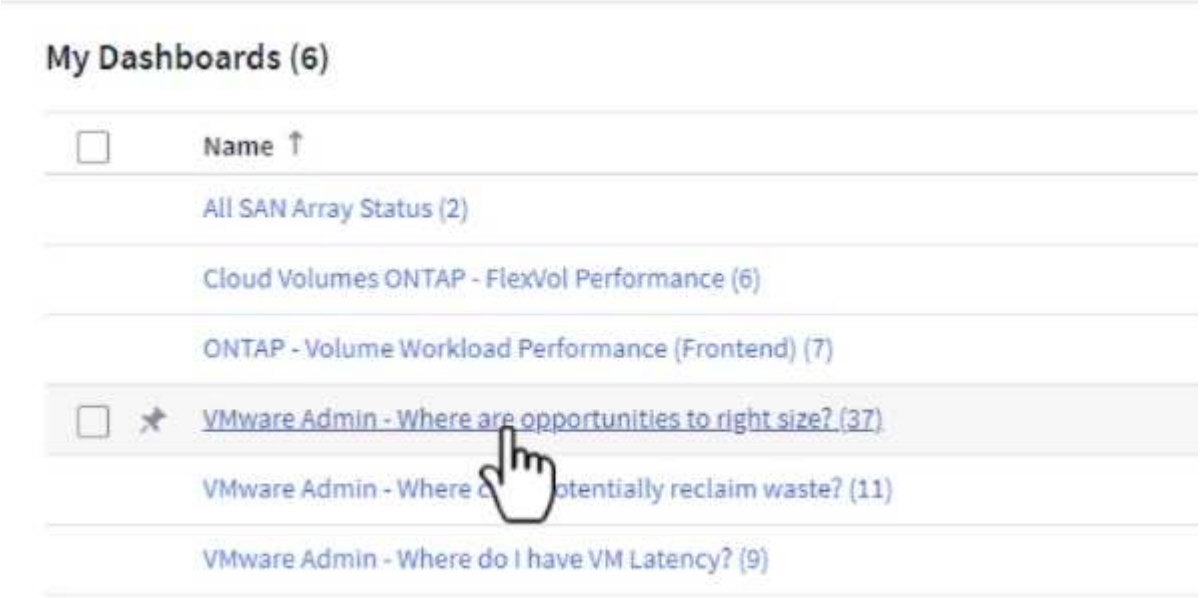


Visualizzare le risorse sottoutilizzate in Cloud Insights

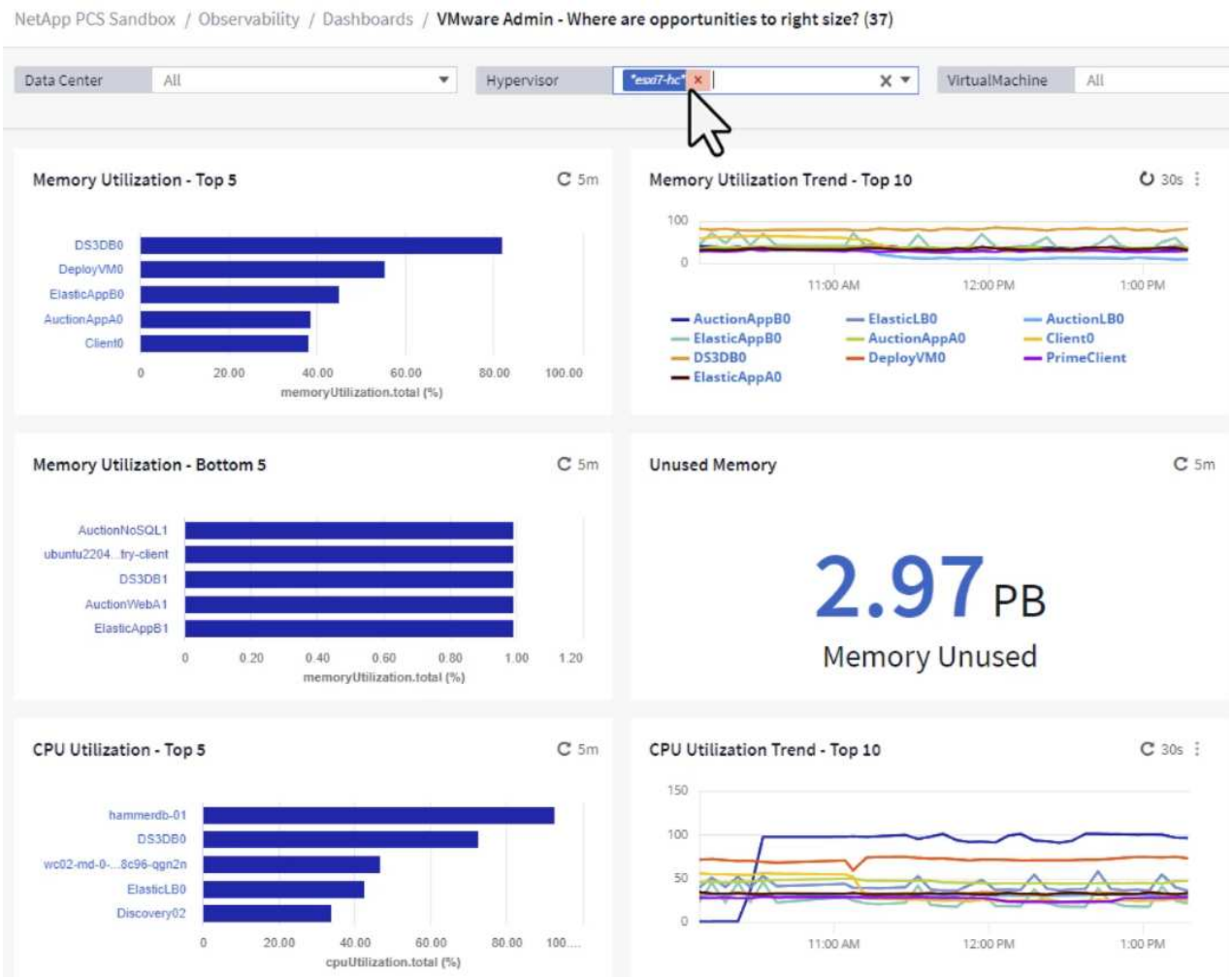
Associando le risorse delle macchine virtuali ai requisiti effettivi dei carichi di lavoro, è possibile ottimizzare l'utilizzo delle risorse con risparmi sui costi di infrastruttura e servizi cloud. I dati in Cloud Insights possono essere customizzati per visualizzare facilmente le macchine virtuali utilizzate, o quelle sottoutilizzate.

Identifica le opportunità per il corretto dimensionamento delle macchine virtuali

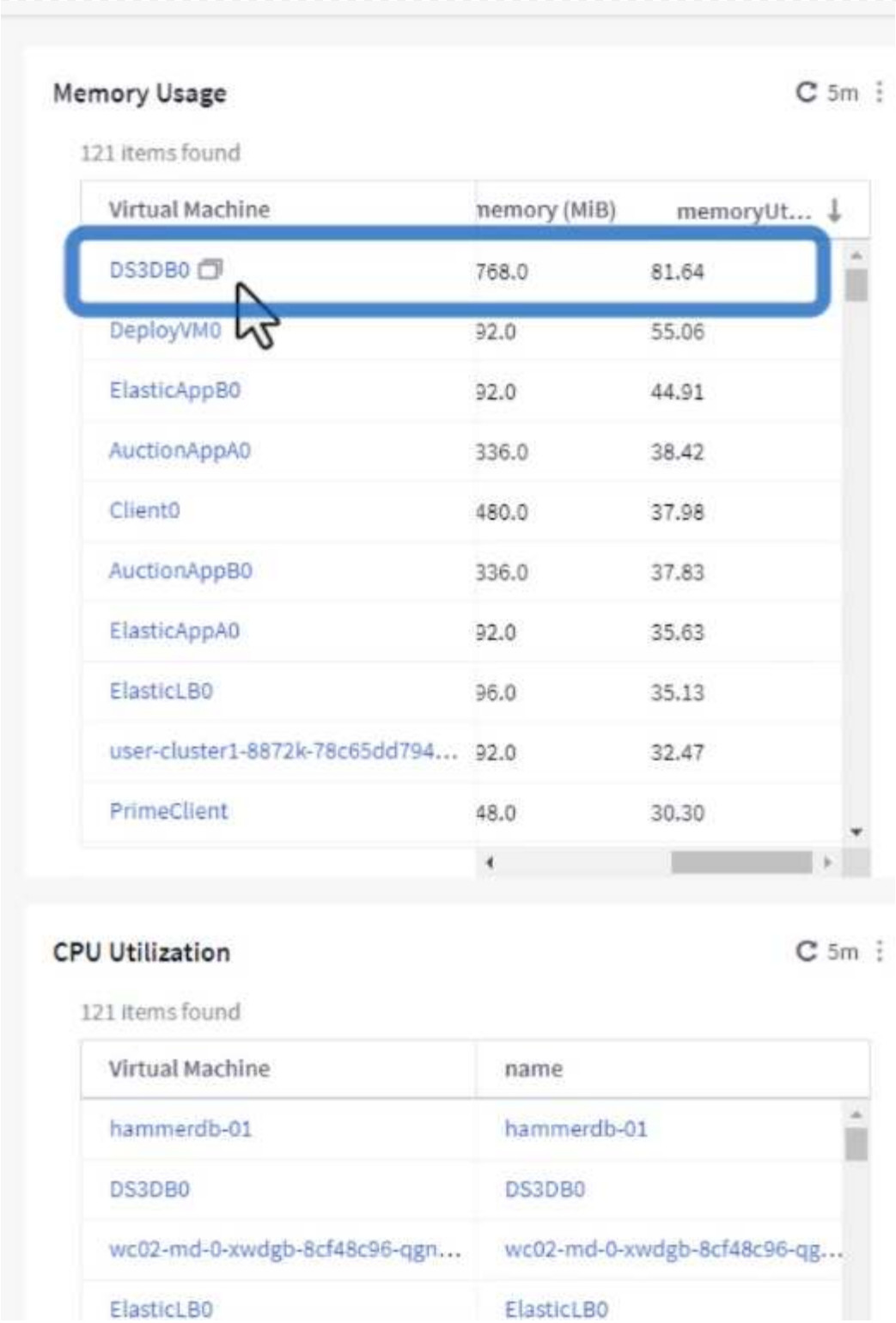
1. In questo esempio si accede a un dashboard disponibile nella **Gallery** chiamato **VMware Admin - dove sono le opportunità di dimensioni corrette?**



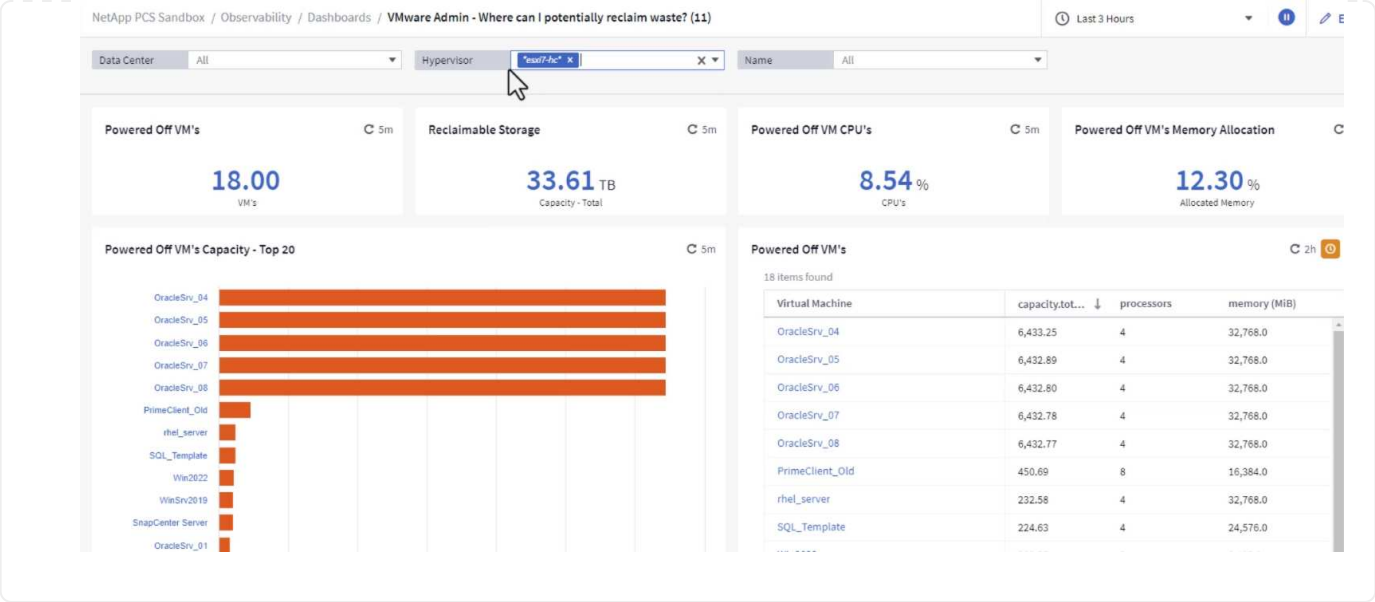
2. Primo filtro da parte di tutti gli host ESXi nel cluster. È quindi possibile visualizzare la classificazione delle macchine virtuali superiore e inferiore in base all'utilizzo della memoria e della CPU.



3. Le tabelle consentono l’ordinamento e forniscono maggiori dettagli in base alle colonne dei dati scelti.



4. Un altro dashboard chiamato **VMware Admin - dove posso potenzialmente recuperare gli sprechi?** mostra VM disattivate ordinate in base al loro utilizzo di capacità.

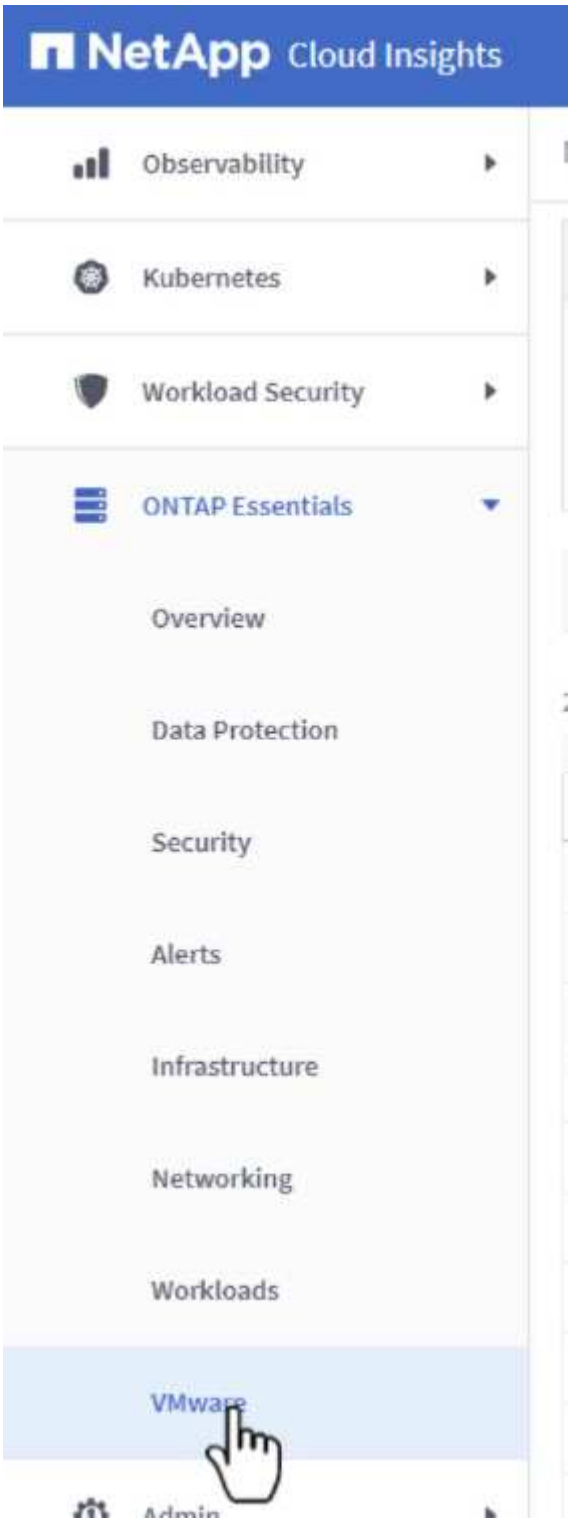


Utilizzare le query per isolare e ordinare le metriche

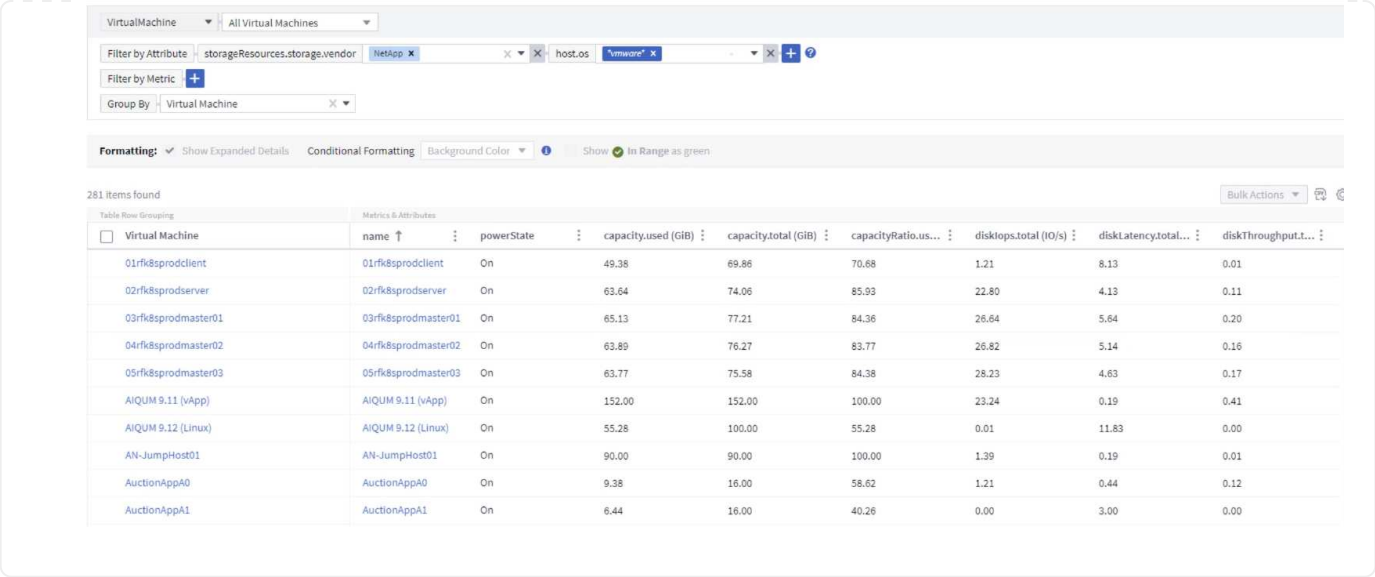
La quantità di dati catturati da Cloud Insights è abbastanza completa. Le query metriche offrono un metodo efficace per ordinare e organizzare grandi quantità di dati in modi utili.

Visualizzate una query VMware dettagliata in ONTAP Essentials

1. Accedere a **ONTAP Essentials > VMware** per accedere a una query metrica VMware completa.



2. In questa visualizzazione vengono visualizzate più opzioni per il filtraggio e il raggruppamento dei dati nella parte superiore. Tutte le colonne di dati sono personalizzabili e possono essere aggiunte facilmente colonne aggiuntive.



Conclusione

Questa soluzione è stata ideata come nozioni di base per scoprire come iniziare a utilizzare NetApp Cloud Insights e mostrare alcune delle potenti funzionalità che questa soluzione di osservabilità può fornire. Il prodotto include centinaia di dashboard e query metriche che semplificano l'utilizzo immediato. La versione completa di Cloud Insights è disponibile come versione di prova di 30 giorni e la versione di base è disponibile gratuitamente per i clienti NetApp.

Ulteriori informazioni

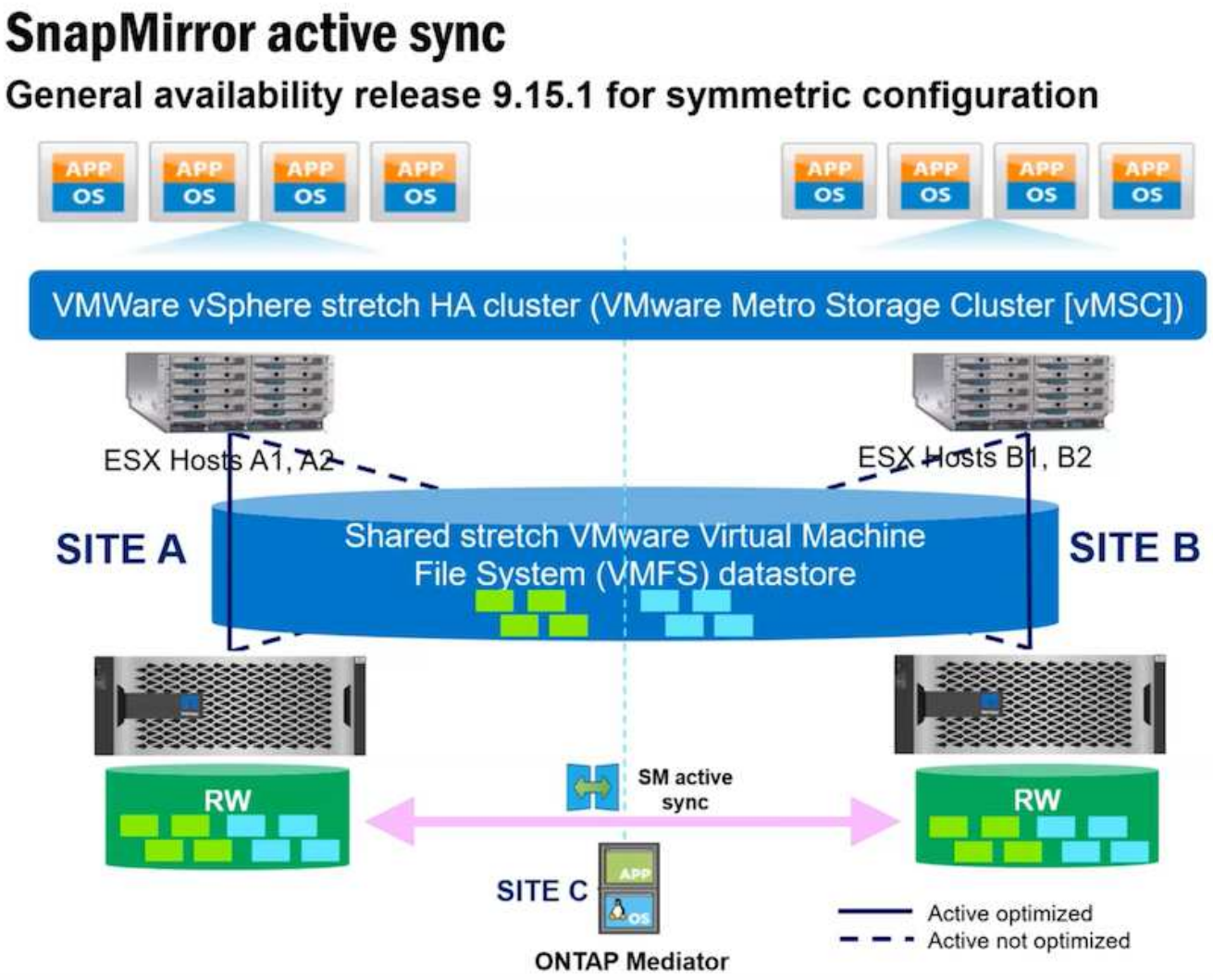
Per ulteriori informazioni sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Landing page di NetApp BlueXP e Cloud Insights"
- "Documentazione NetApp Cloud Insights"

Cluster di storage VMware vSphere Metro con sincronizzazione attiva SnapMirror

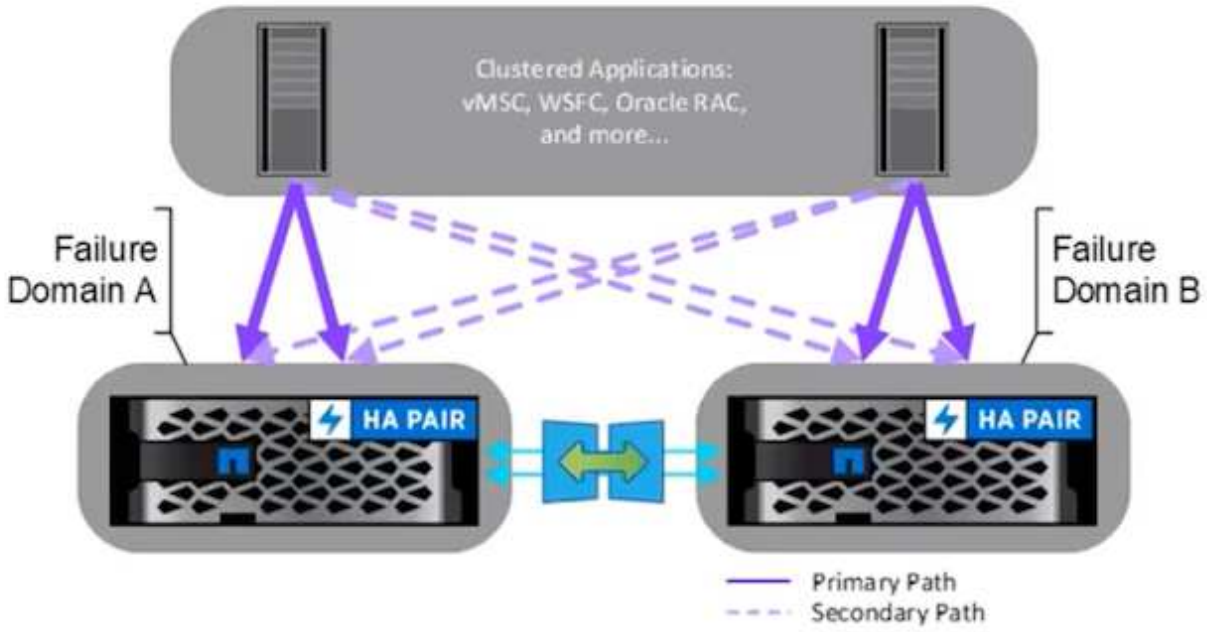
"VMware vSphere Metro Storage Cluster (vMSC)" È una soluzione cluster estesa a diversi domini di errore per fornire * mobilità del carico di lavoro tra zone o siti di disponibilità. * prevenzione del downtime * prevenzione dei disastri * recupero rapido

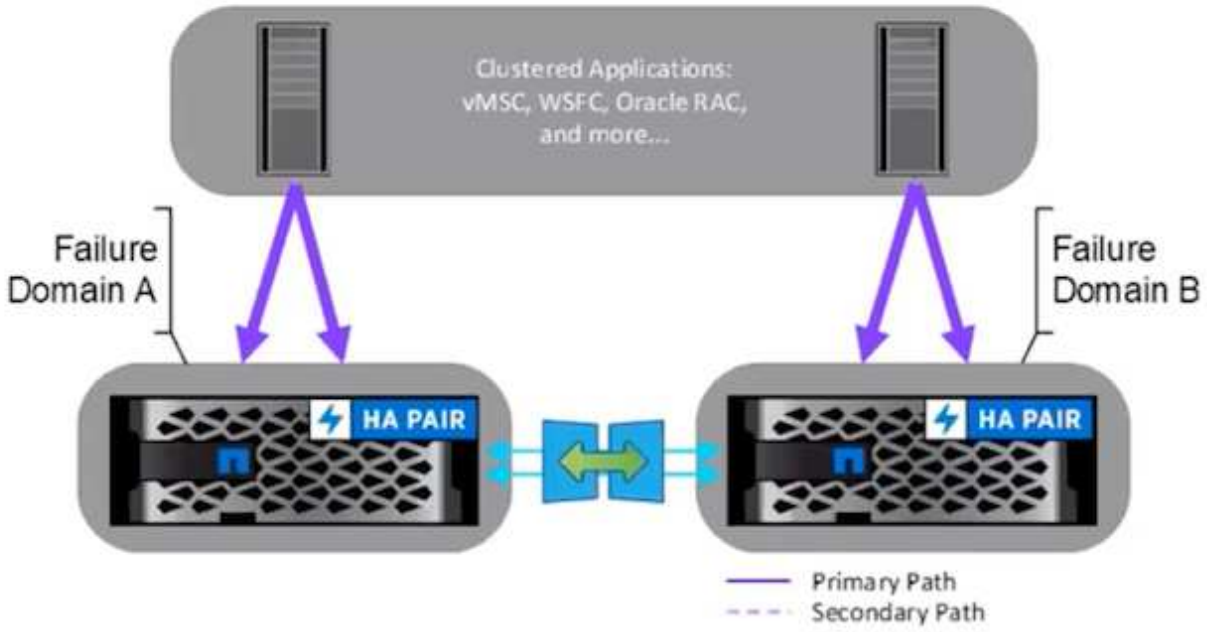
Questo documento fornisce i dettagli dell'implementazione di vMSC con l' "Sincronizzazione attiva SnapMirror (SM-AS)" utilizzo di System Manager e degli strumenti ONTAP. Mostra inoltre in che modo la VM può essere protetta replicando nel terzo sito e gestita con il plug-in SnapCenter per VMware vSphere.



SnapMirror Active Sync supporta gli storage array ASA, AFF e FAS. Si consiglia di utilizzare lo stesso tipo (modelli Performance/Capacity) su entrambi i domini di errore. Attualmente sono supportati solo protocolli di blocco quali FC e iSCSI. Per ulteriori linee guida di supporto, fare riferimento a. "Tool di matrice di interoperabilità" "Hardware Universe"

VMSC supporta due diversi modelli di distribuzione denominati accesso host uniforme e accesso host non uniforme. Con una configurazione di accesso uniforme agli host, ogni host del cluster ha accesso al LUN in entrambi i domini di errore. Viene generalmente utilizzata in diverse zone di disponibilità nello stesso data center.





Nella configurazione di accesso host non uniforme, l'host ha accesso solo al dominio di errore locale. Viene generalmente utilizzato in siti diversi in cui l'esecuzione di più cavi nei domini di errore è un'opzione restrittiva.

In modalità di accesso host non uniforme, le VM verranno riavviate in un altro dominio di errore da vSphere ha. La disponibilità delle applicazioni verrà compromessa in base al progetto. La modalità di accesso host non uniforme è supportata solo con ONTAP 9,15 in avanti.

Prerequisiti

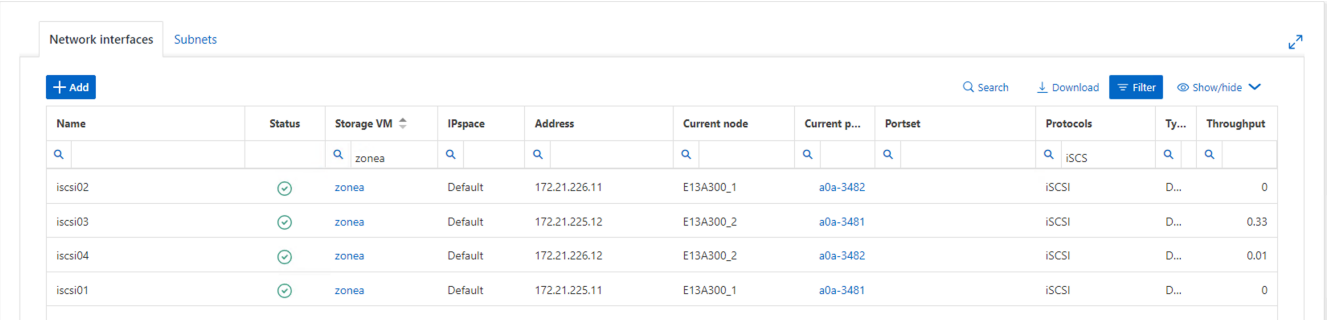
- "Gli host VMware vSphere sono stati implementati con un fabric di storage doppio (due HBA o doppia VLAN per iSCSI) per host".
- "Gli storage array vengono implementati con aggregazione dei collegamenti per le porte dati (per iSCSI)".
- "Sono disponibili Storage VM e LIF"
- "La latenza inter-cluster deve essere inferiore a 10 millisecondi".
- "ONTAP Mediator VM è distribuito su un dominio di errore diverso"
- "È stata stabilita una relazione di peer cluster"
- "È stata stabilita una relazione di peer SVM"
- "ONTAP Mediator registrato nel cluster ONTAP"

Se si utilizza un certificato autofirmato, il certificato CA può essere recuperato da <installation path>/ontap_mediator/server_config/ca.crt sulla macchina virtuale mediatore.

Accesso all'host non uniforme vMSC con l'interfaccia utente di ONTAP System Manager.

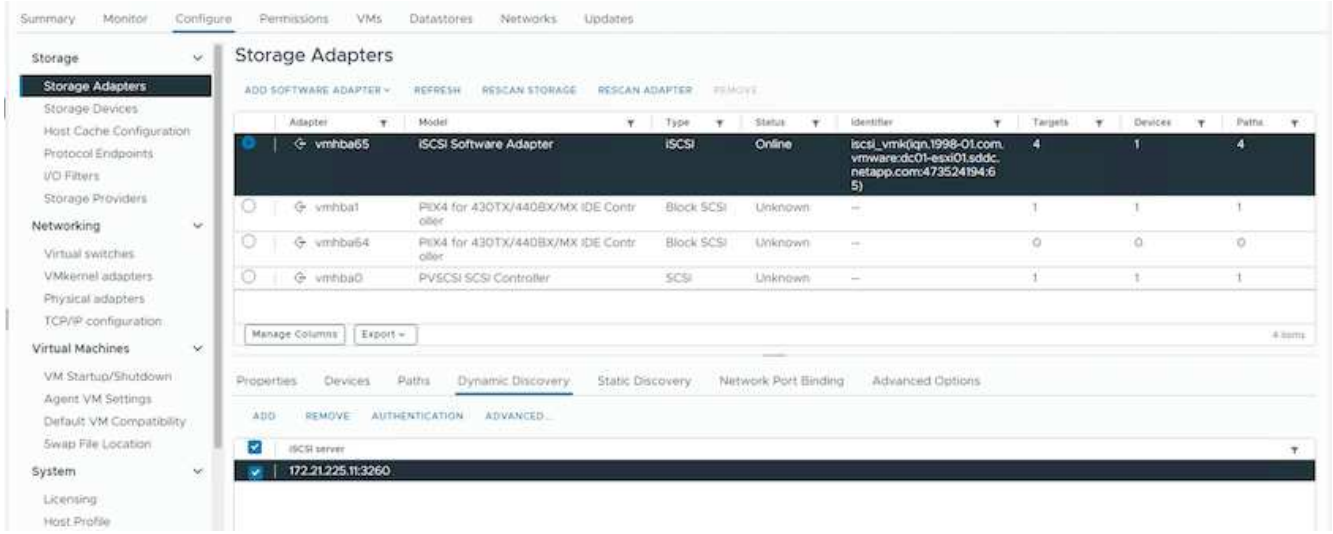
Nota: È possibile utilizzare gli strumenti ONTAP 10,2 o versioni successive per il provisioning di datastore allungato con modalità di accesso host non uniforme senza cambiare più interfacce utente. Questa sezione è solo un riferimento se non vengono utilizzati gli strumenti ONTAP.

1. Annotare uno degli indirizzi IP lif dei dati iSCSI dall'array di archiviazione del dominio di errore locale.



Name	Status	Storage VM	IPspace	Address	Current node	Current p...	Portset	Protocols	Ty...	Throughput
		zonea						iSCS		
iscsi02		zonea	Default	172.21.226.11	E13A300_1	a0a-3482		iSCSI	D...	0
iscsi03		zonea	Default	172.21.225.12	E13A300_2	a0a-3481		iSCSI	D...	0.33
iscsi04		zonea	Default	172.21.226.12	E13A300_2	a0a-3482		iSCSI	D...	0.01
iscsi01		zonea	Default	172.21.225.11	E13A300_1	a0a-3481		iSCSI	D...	0

2. Su vSphere host iSCSI Storage Adapter, aggiungere l'IP iSCSI nella scheda Dynamic Discovery (rilevamento dinamico).

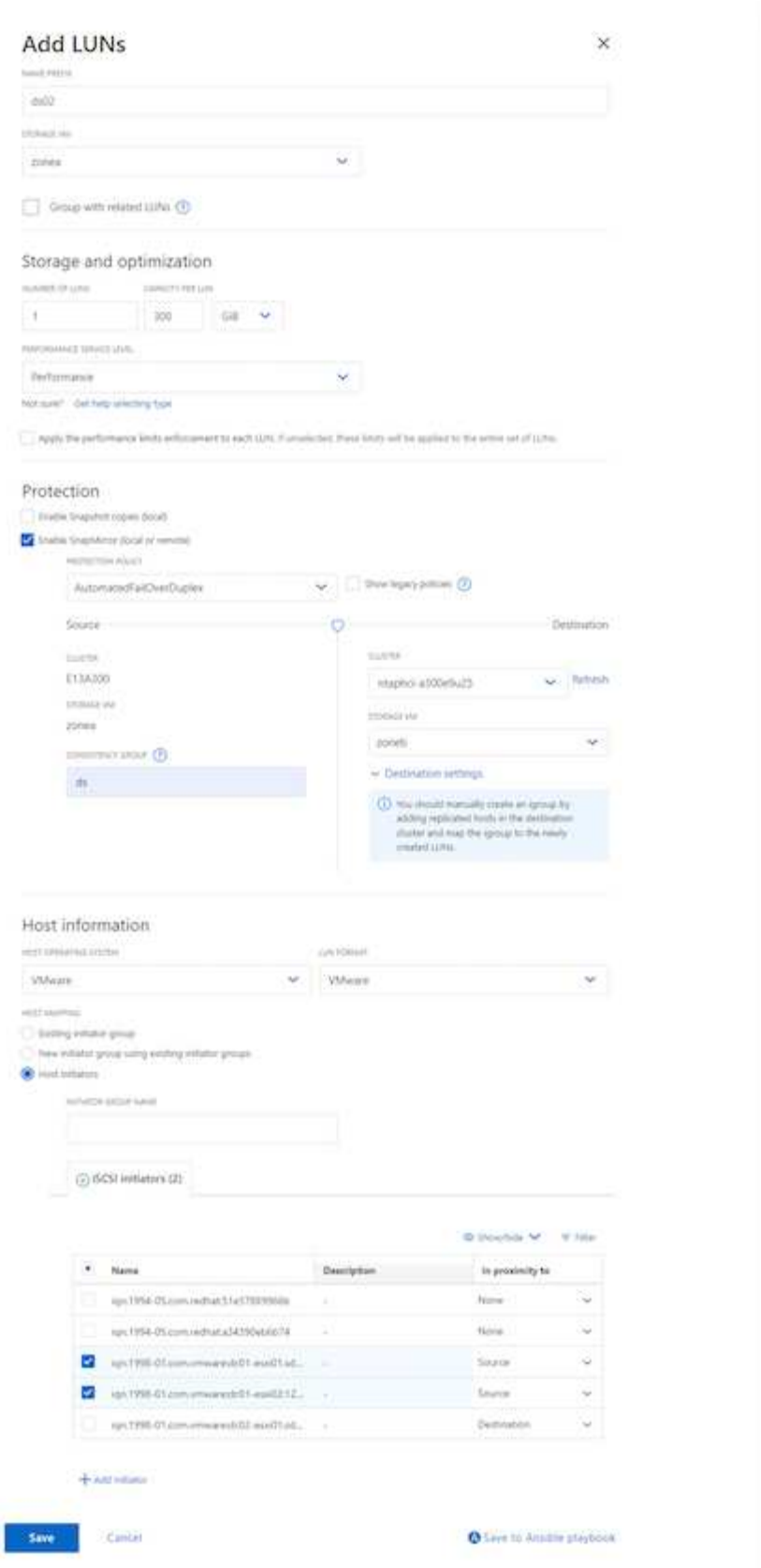


Per la modalità di accesso uniforme, è necessario fornire l'indirizzo lif dei dati iSCSI del dominio di errore di origine e di destinazione.

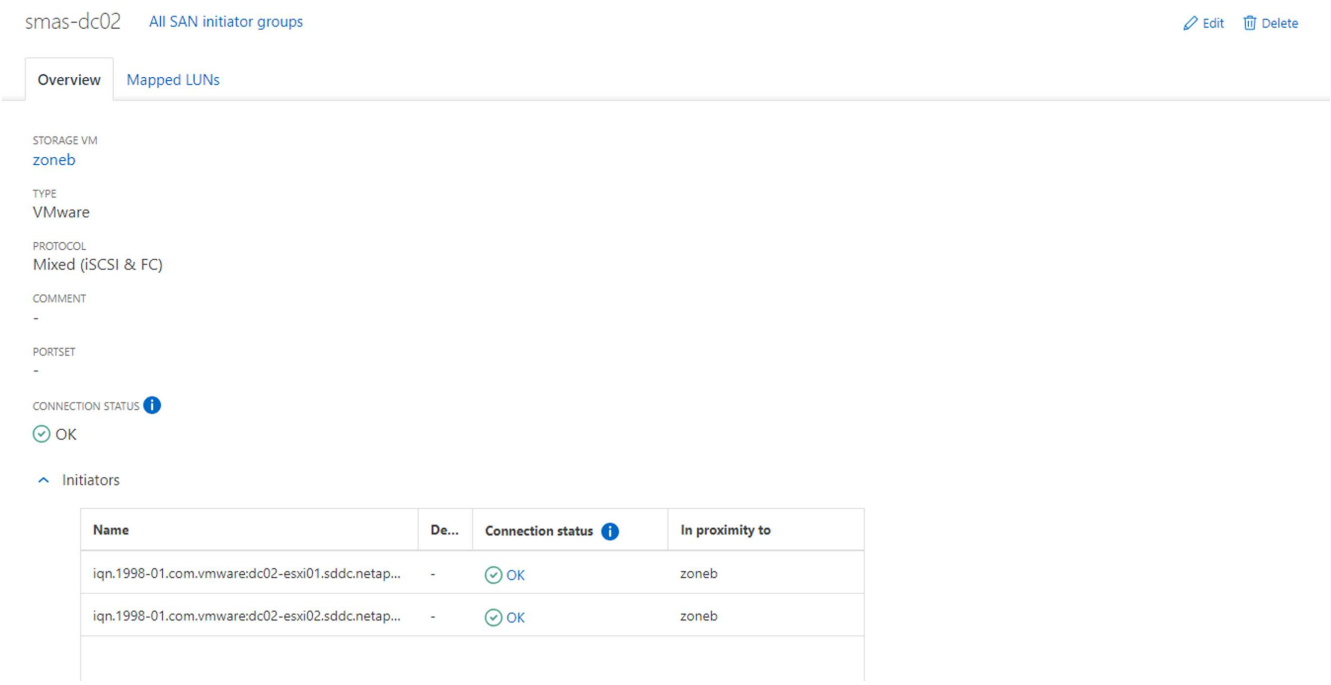
3. Ripetere il passaggio precedente sugli host vSphere per l'altro dominio di errore aggiungendo i dati iSCSI locali lif IP nella scheda Dynamic Discovery.
4. Se la connettività di rete è corretta, per ogni host vSphere deve essere presente quattro connessioni iSCSI con due nic VMkernel iSCSI e due cicli di vita dati iSCSI per storage controller.

```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
            Tpgroup             Conn  Local           Remote          TCP Recv
Vserver     Name          TSIH  ID    Address         Address         Size
----------- ------------- ----- ----- --------------- --------------- --------
zonea       iscsi01          23     0 172.21.225.11   172.21.225.71         0
zonea       iscsi03          17     0 172.21.225.12   172.21.225.71         0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.226.71
            Tpgroup             Conn  Local           Remote          TCP Recv
Vserver     Name          TSIH  ID    Address         Address         Size
----------- ------------- ----- ----- --------------- --------------- --------
zonea       iscsi02          24     0 172.21.226.11   172.21.226.71         0
zonea       iscsi04          16     0 172.21.226.12   172.21.226.71         0
2 entries were displayed.
```

5. Creare LUN mediante Gestione di sistema di ONTAP, configurare SnapMirror con il criterio di replica AutomatedFailOverDuplex, scegliere gli initiator dell'host e impostare la prossimità dell'host.

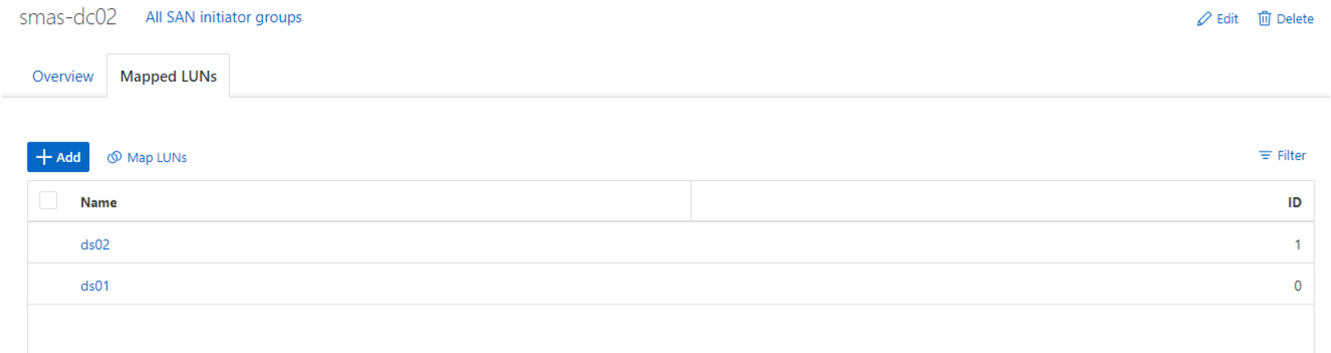


6. Su un altro array di storage del dominio di errore, creare il gruppo iniziatore SAN con i relativi iniziatori host vSphere e impostare la prossimità dell'host.

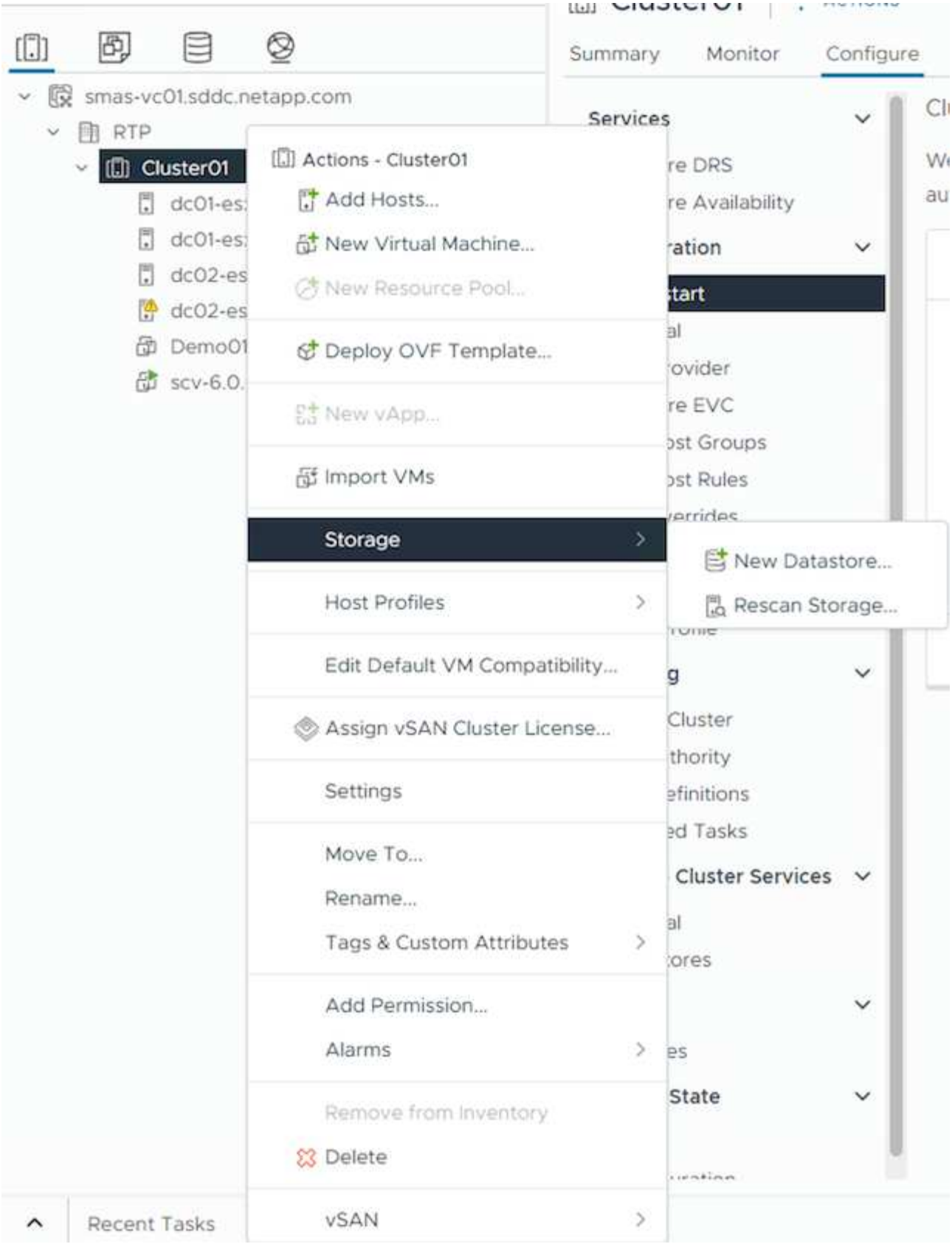


Per la modalità di accesso uniforme, l'igroup può essere replicato dal dominio di errore di origine.

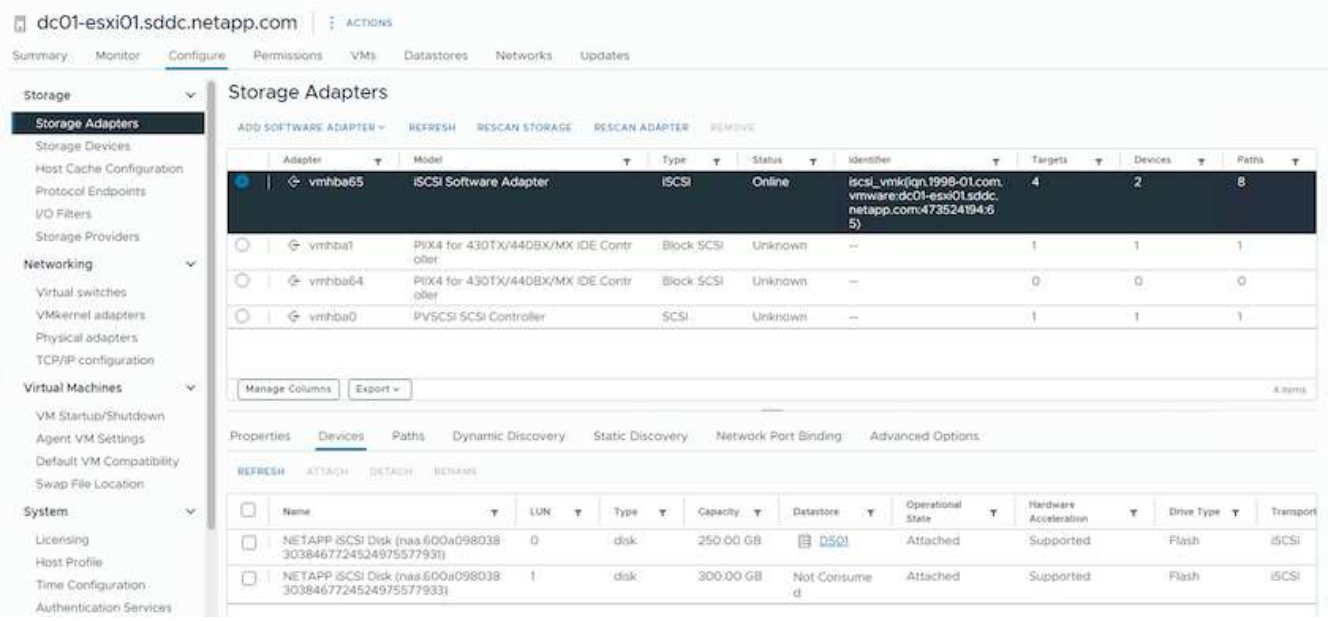
7. Mappare il LUN replicato con lo stesso ID di mappatura del dominio di errore di origine.



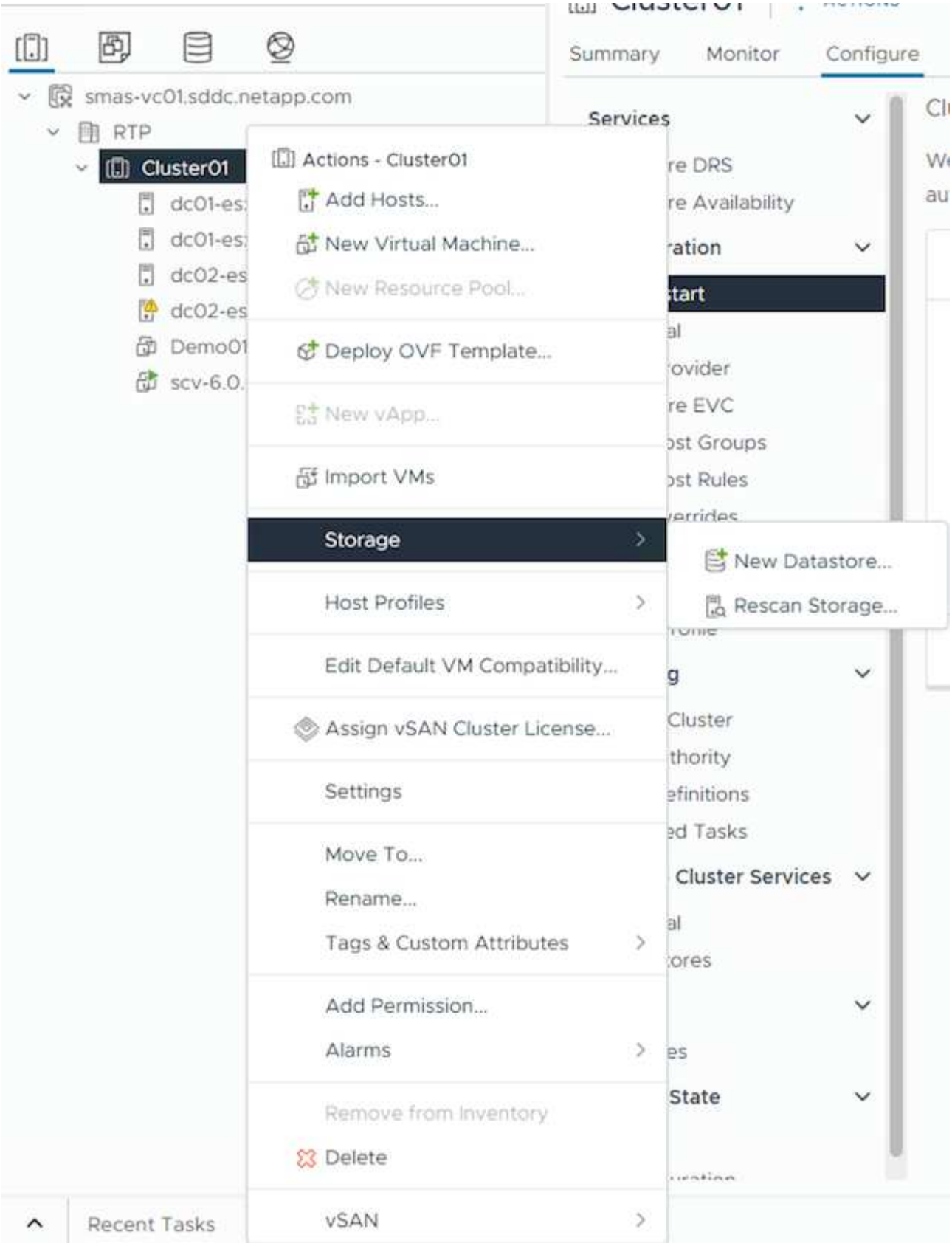
8. Su vCenter, fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Rescan Storage (archiviazione di nuova scansione).



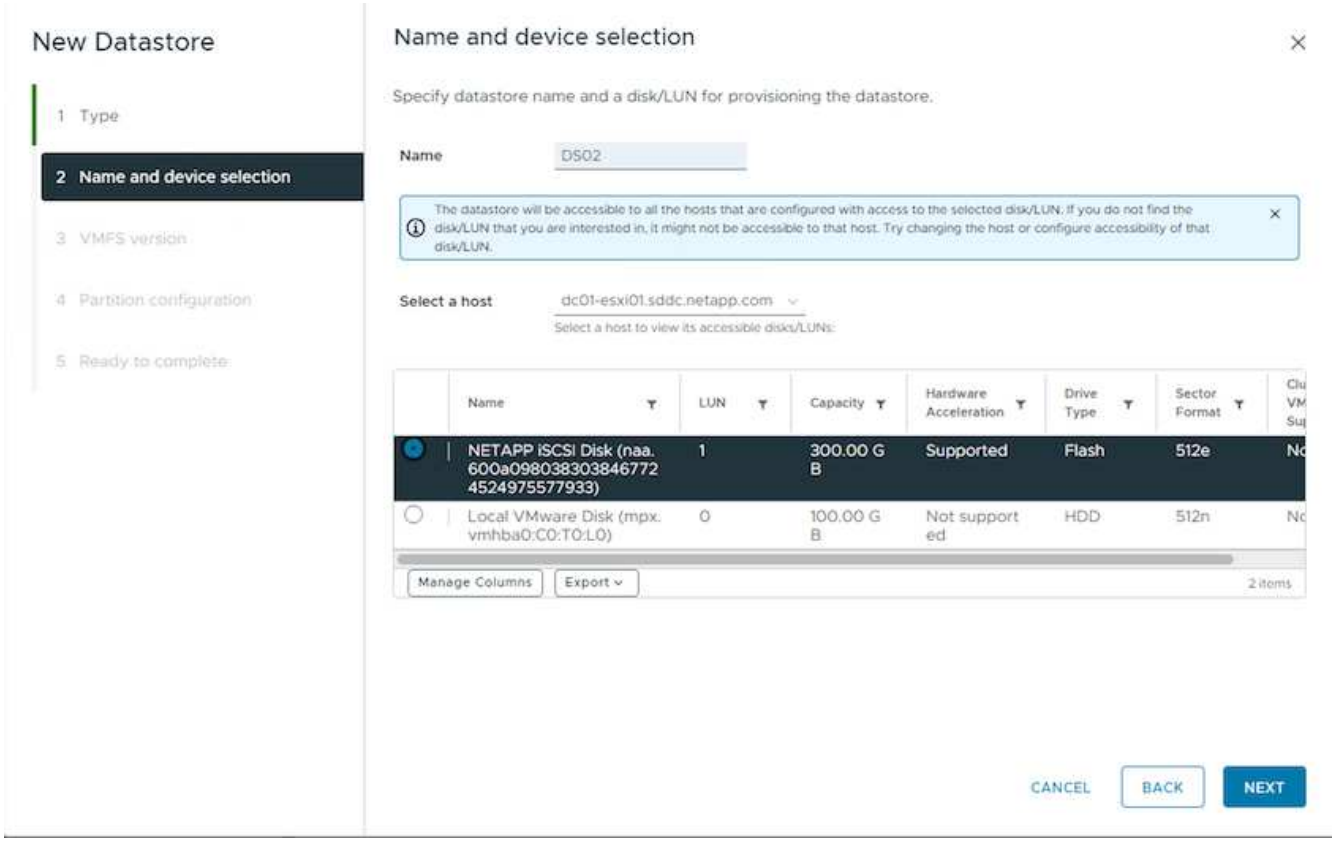
9. Su uno degli host vSphere nel cluster, verificare che il dispositivo appena creato sia visualizzato con il datastore non utilizzato.



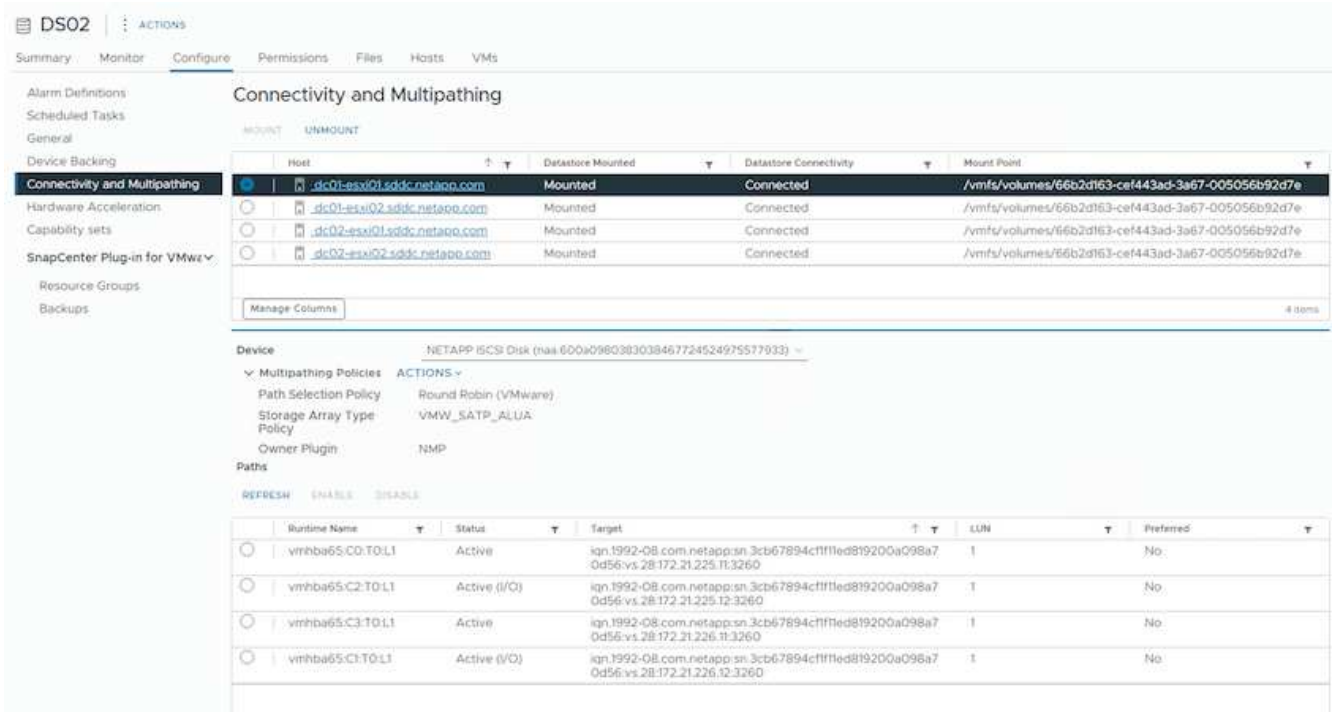
10. Su vCenter, fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione New DataStore (nuovo datastore).

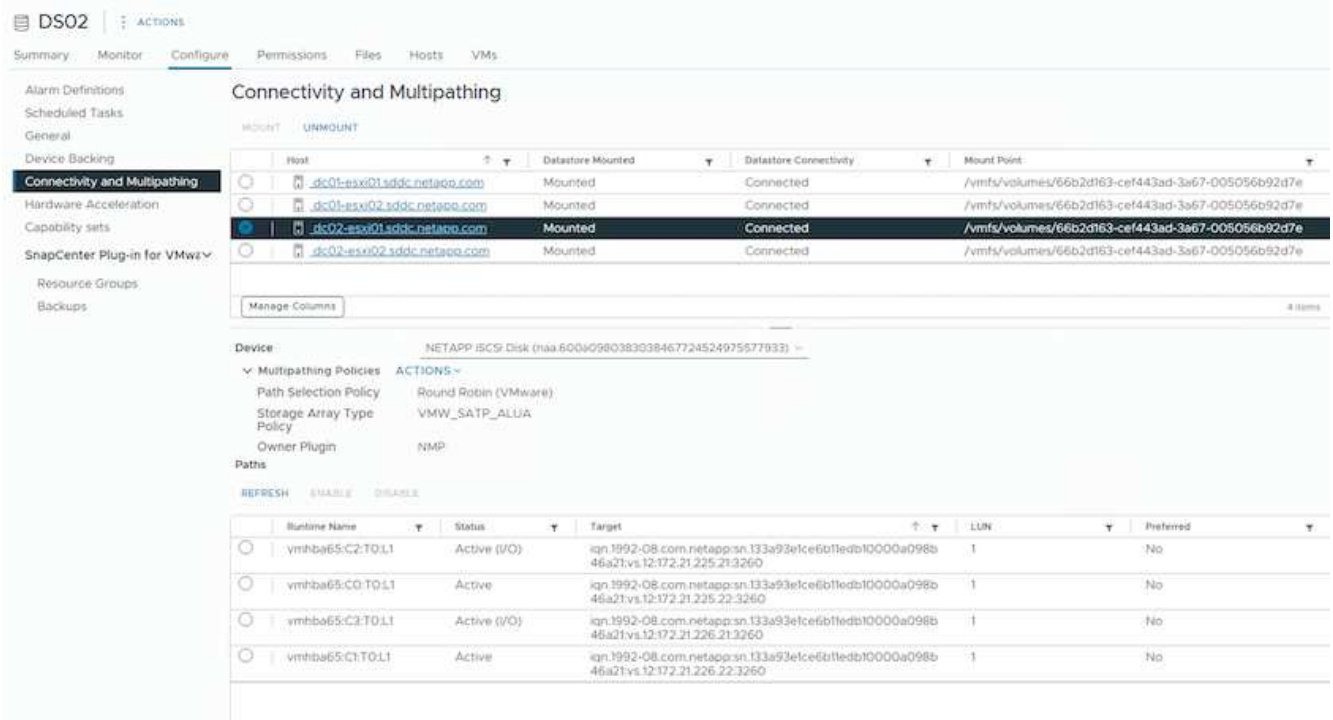


11. Durante la procedura guidata, ricordarsi di fornire il nome del datastore e selezionare il dispositivo con la capacità e l'ID del dispositivo corretti.



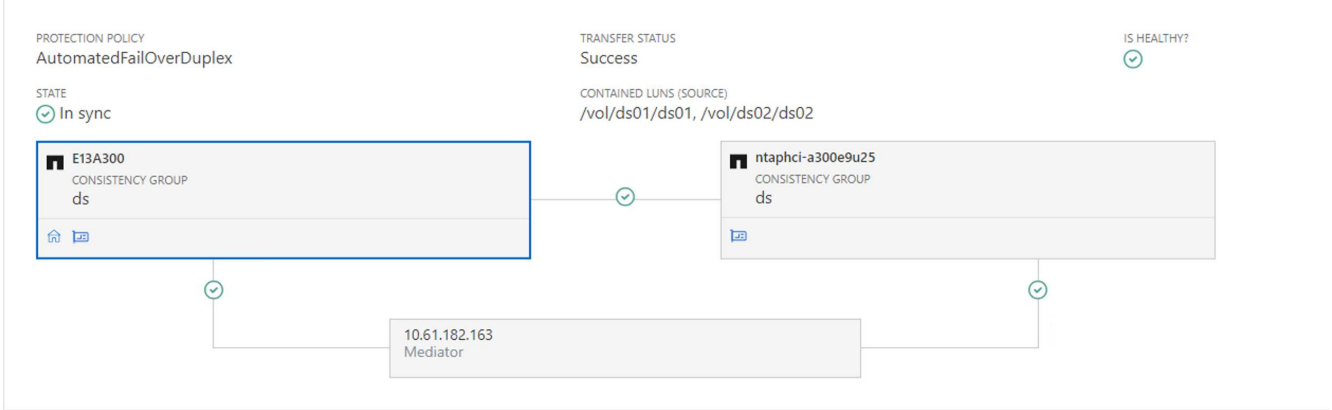
12. Verificare che il datastore sia montato su tutti gli host del cluster in entrambi i domini di errore.





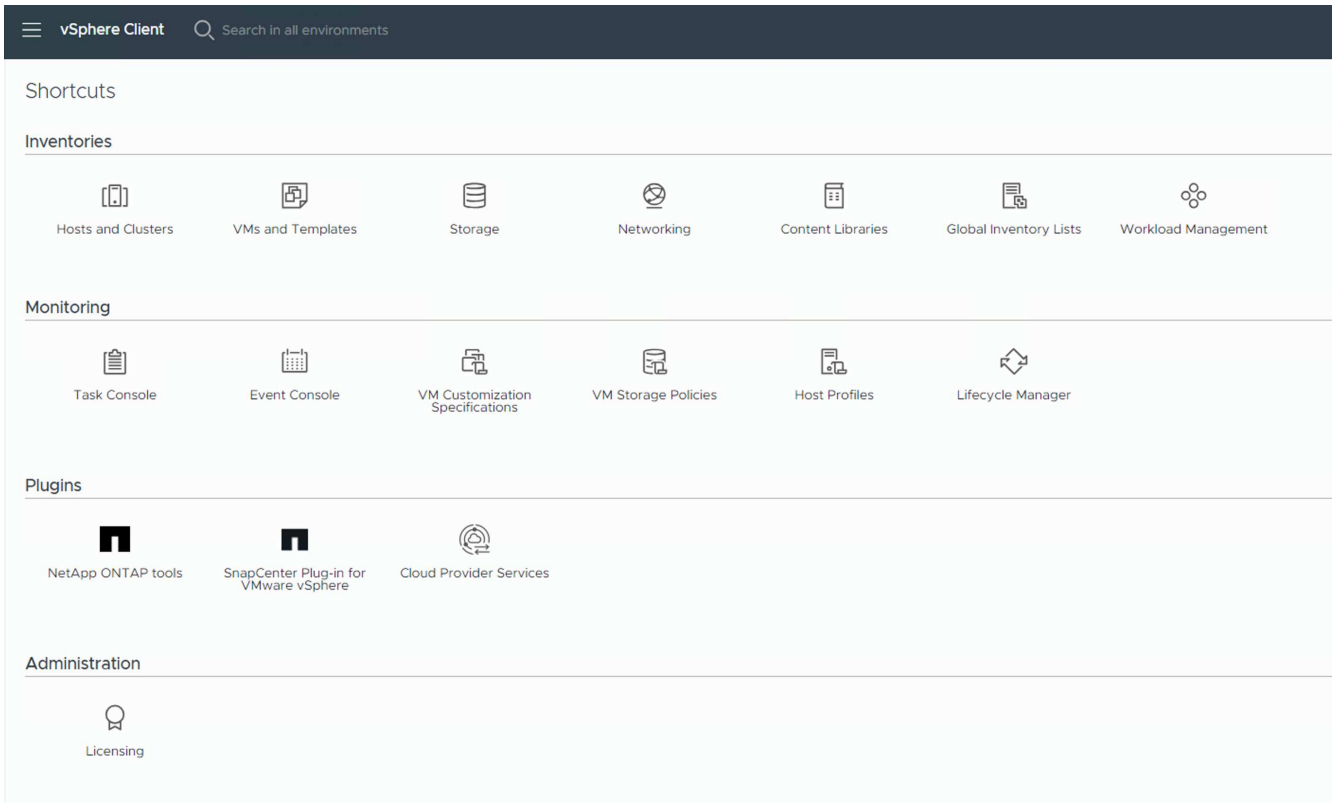
Le schermate precedenti mostrano i/o attivo su un singolo controller da quando abbiamo utilizzato AFF. Per ASA, avrà io attivo su tutti i percorsi.

13. Quando vengono aggiunti altri datastore, è necessario ricordare di espandere il gruppo di coerenza esistente per renderlo coerente all'interno del cluster vSphere.



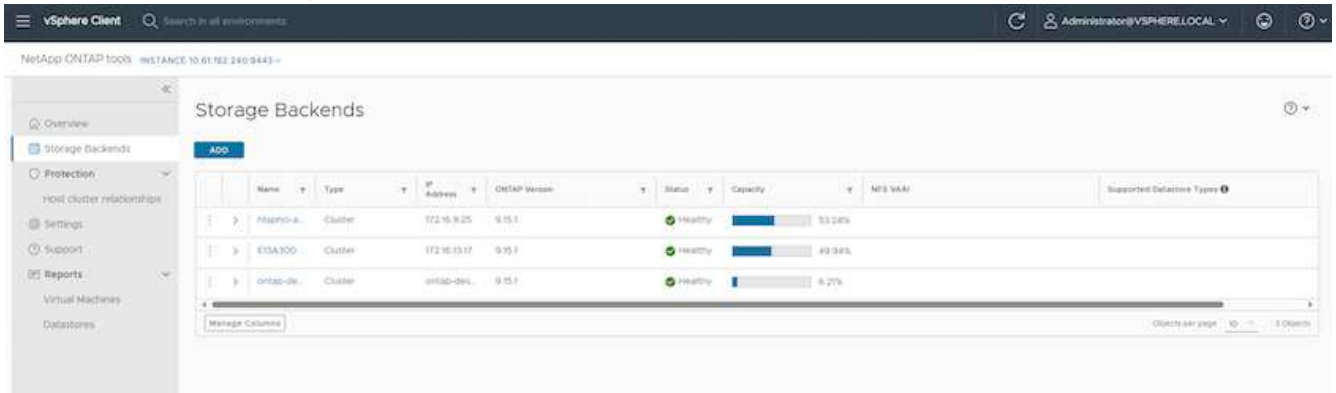
VMSC modalità di accesso host uniforme con gli strumenti ONTAP.

1. Verifica che NetApp ONTAP Tools sia distribuito e registrato in vCenter.



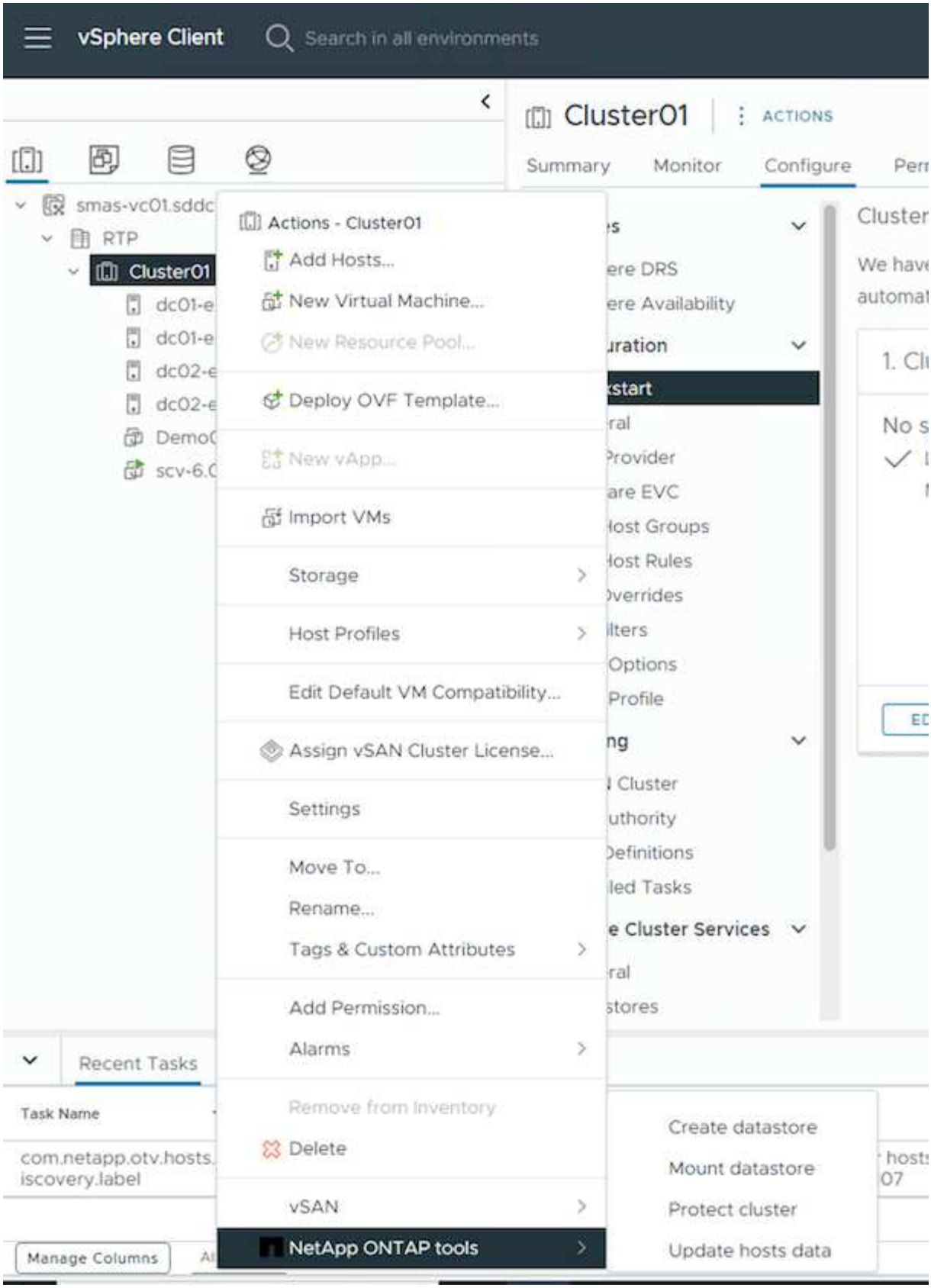
In caso contrario, seguire "Distribuzione degli strumenti ONTAP" e. "Aggiungere un'istanza del server vCenter"

2. Assicurarsi che i sistemi di archiviazione ONTAP siano registrati in Strumenti ONTAP. Questo include sia i sistemi di storage del dominio di errore che il terzo per la replica remota asincrona da utilizzare per la protezione VM con il plugin SnapCenter per VMware vSphere.

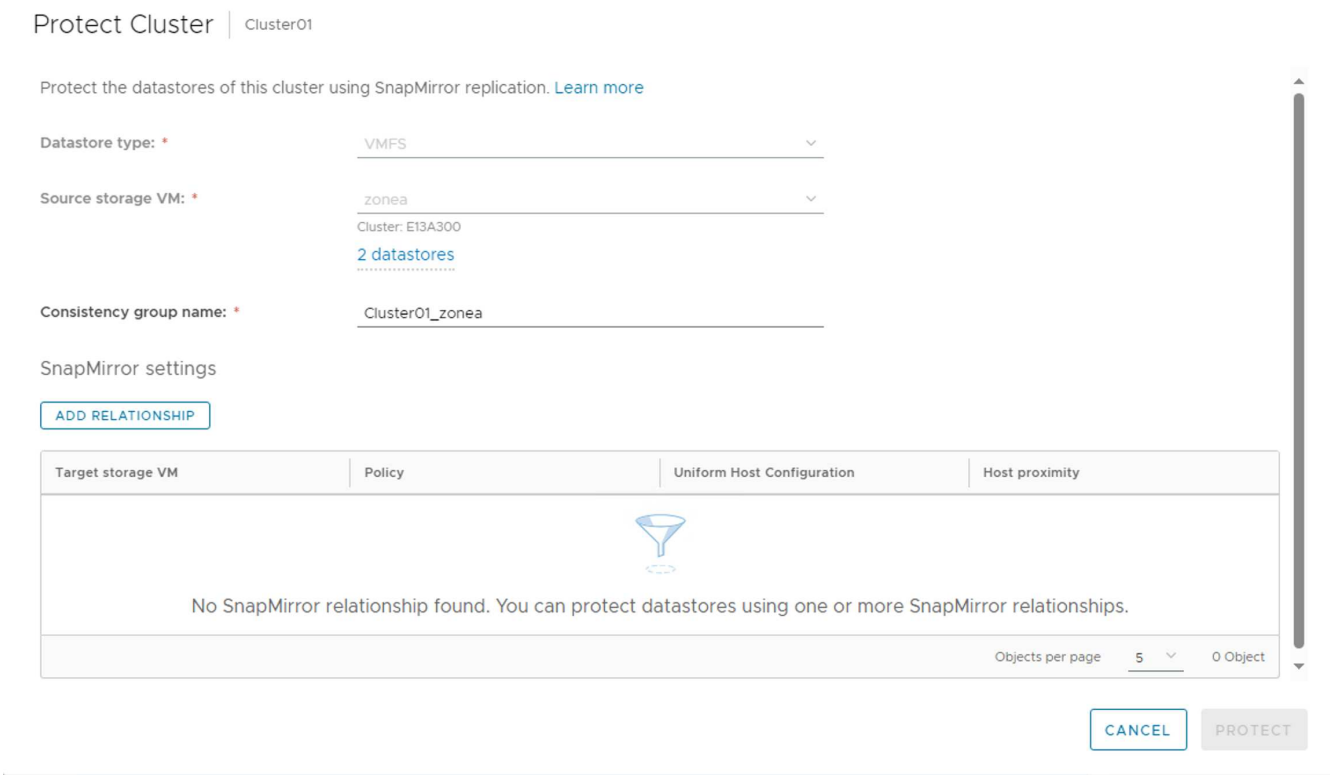


In caso contrario, procedere come indicato di seguito "Aggiungere il backend dello storage utilizzando l'interfaccia utente del client vSphere"

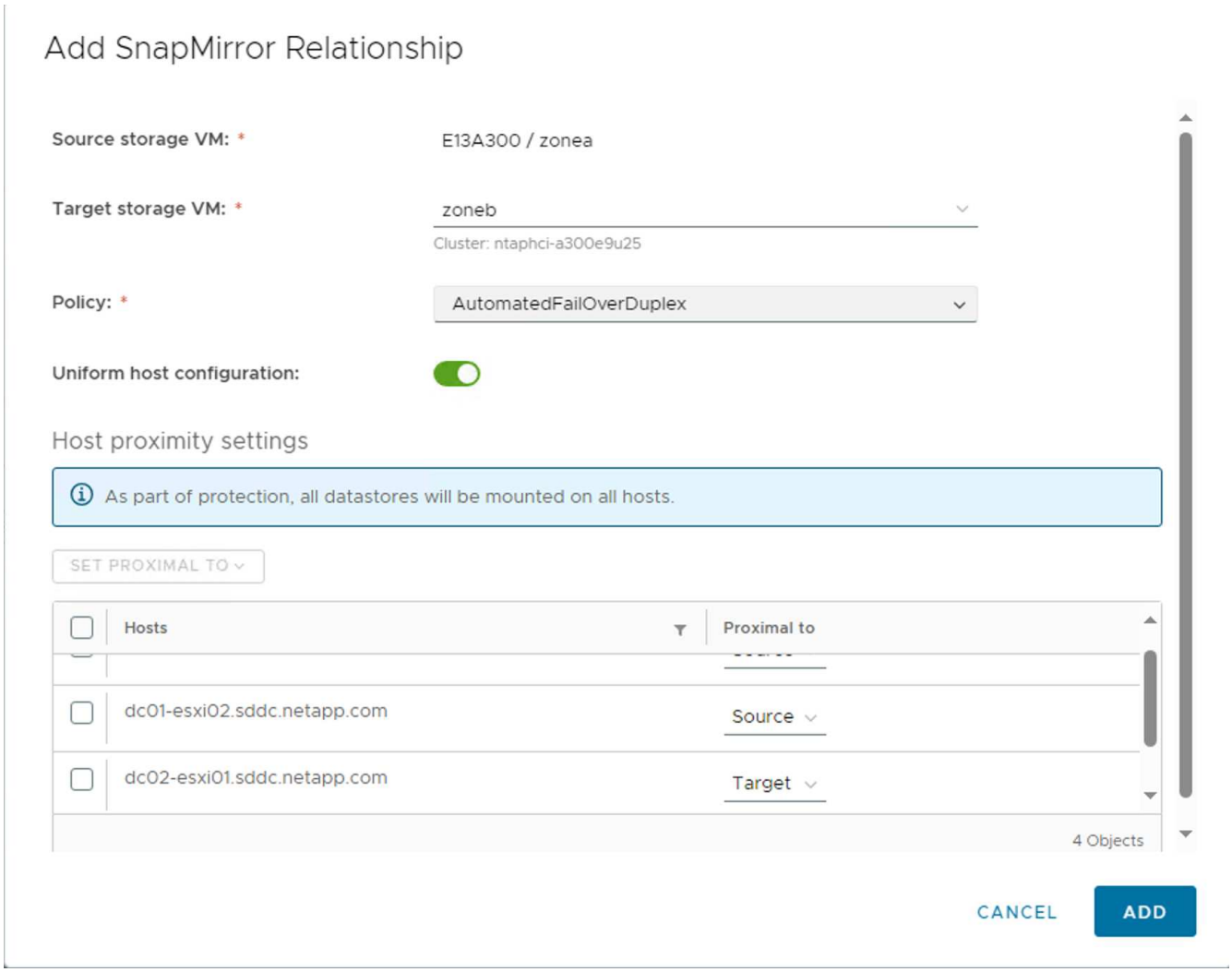
3. Aggiornare i dati degli host per la sincronizzazione con gli strumenti ONTAP e quindi "creare un datastore".



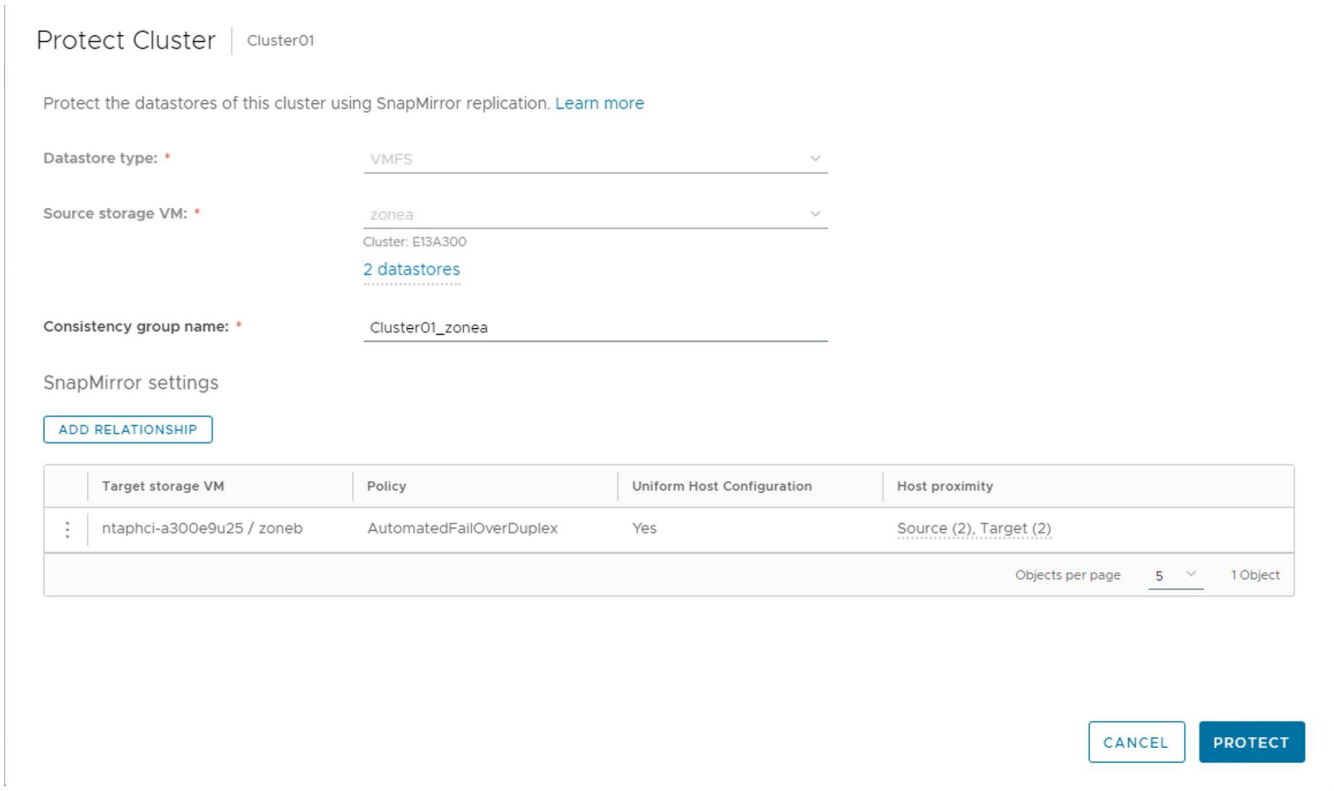
4. Per abilitare SM-as, fare clic con il pulsante destro del mouse sul cluster vSphere e scegliere Protect cluster on NetApp ONTAP Tools (fare riferimento alla schermata precedente)
5. Mostra i datastore esistenti per il cluster insieme ai dettagli delle SVM. Il nome CG predefinito è <nome cluster vSphere>_<SVM name>. Fare clic sul pulsante Aggiungi relazione.



6. Scegliere la SVM di destinazione e impostare il criterio su AutomatedFailOverDuplex per SM-AS. È presente un interruttore a levetta per la configurazione uniforme dell'host. Impostare la prossimità per ciascun host.

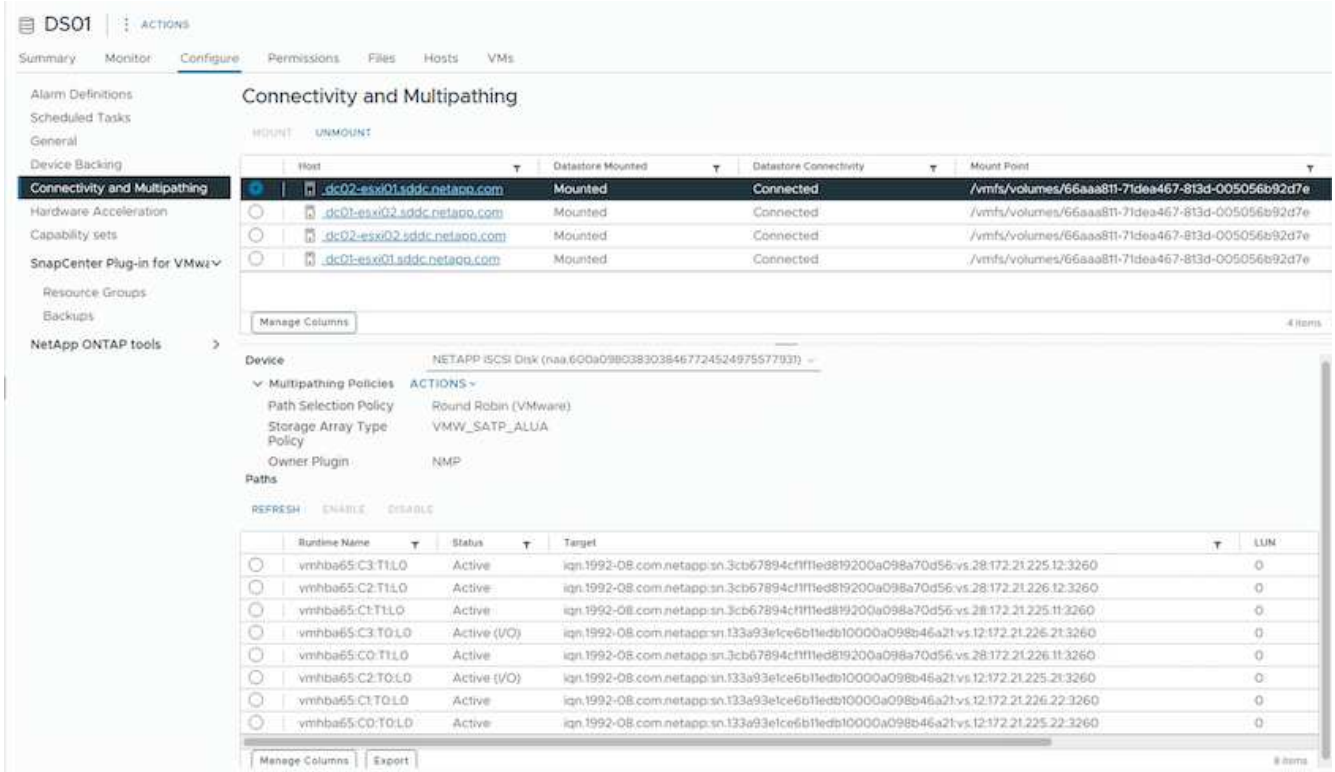


7. Verificare le informazioni sulla promozione dell'host e altri dettagli. Se necessario, aggiungere un'altra relazione al terzo sito con la policy di replica asincrona. Quindi, fare clic su Proteggi.



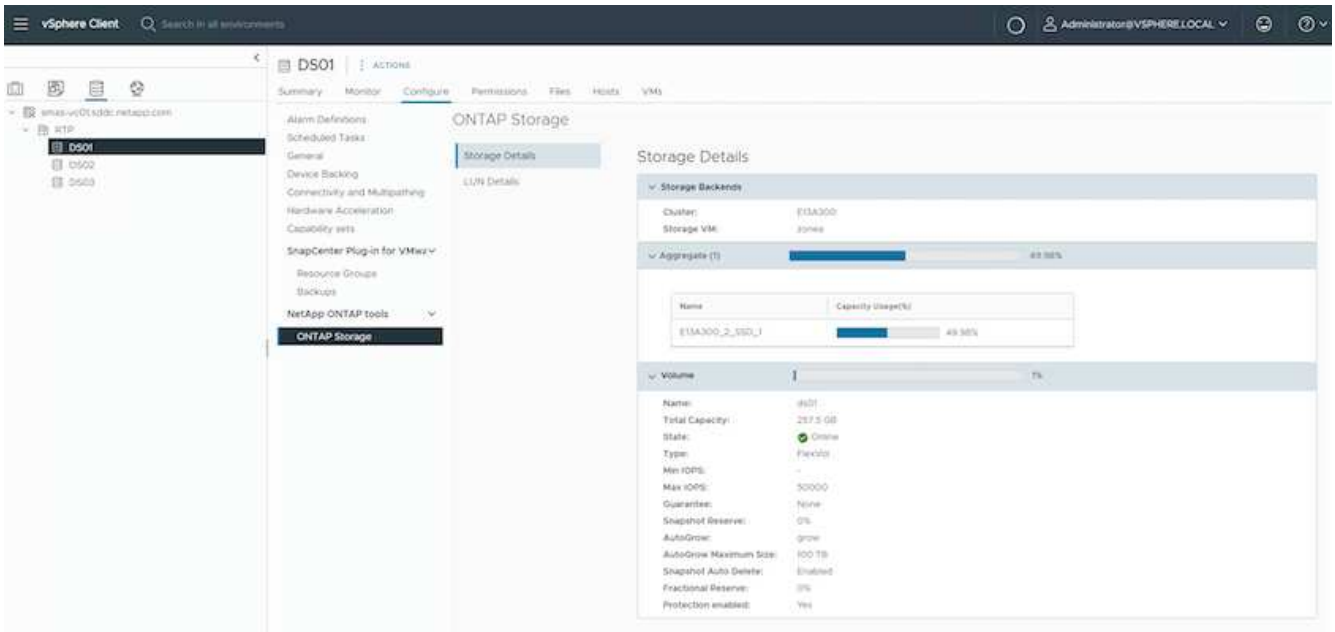
NOTA: Se si intende utilizzare il plug-in SnapCenter per VMware vSphere 6,0, è necessario configurare la replica a livello di volume anziché a livello di gruppo di coerenza.

8. Con un accesso host uniforme, l'host dispone di una connessione iSCSI a entrambi gli array di storage dei domini di errore.

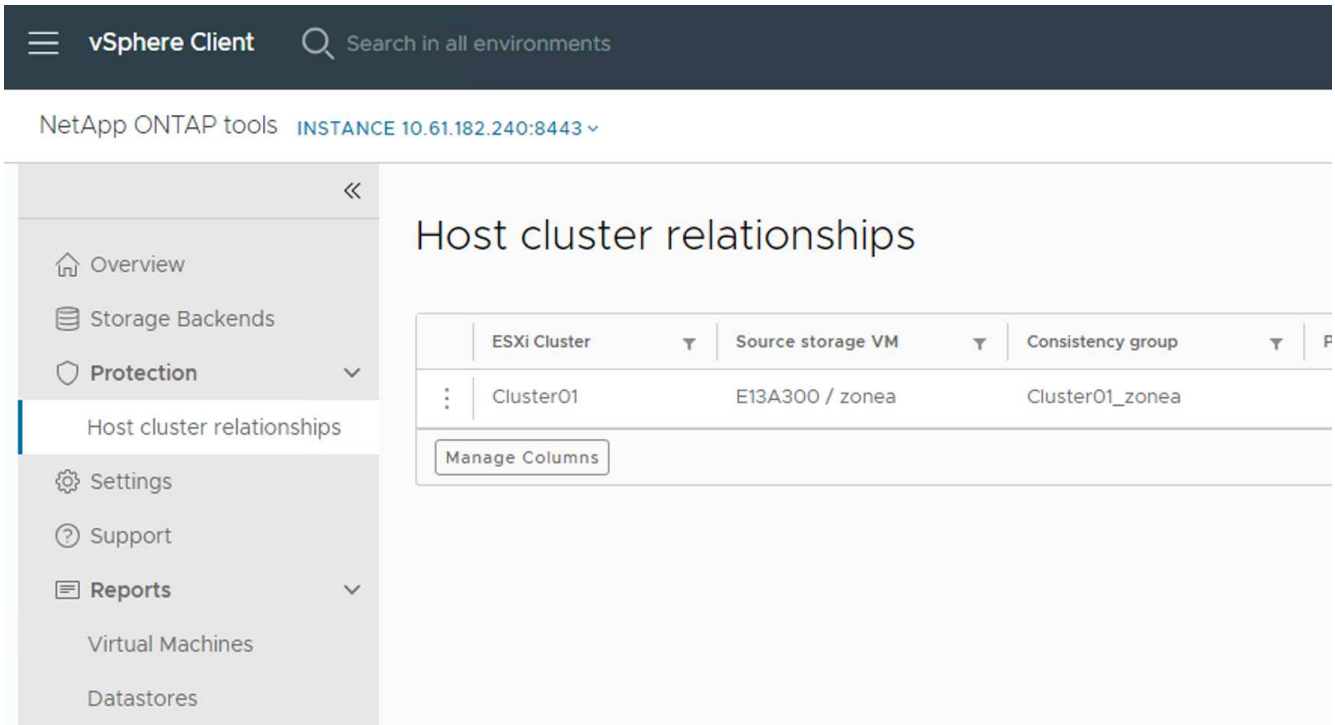


NOTA: La schermata precedente è di AFF. Se si utilizza ASA, l'i/o ATTIVO deve trovarsi in tutti i percorsi con connessioni di rete appropriate.

9. Il plugin ONTAP Tools indica anche che il volume è protetto o meno.

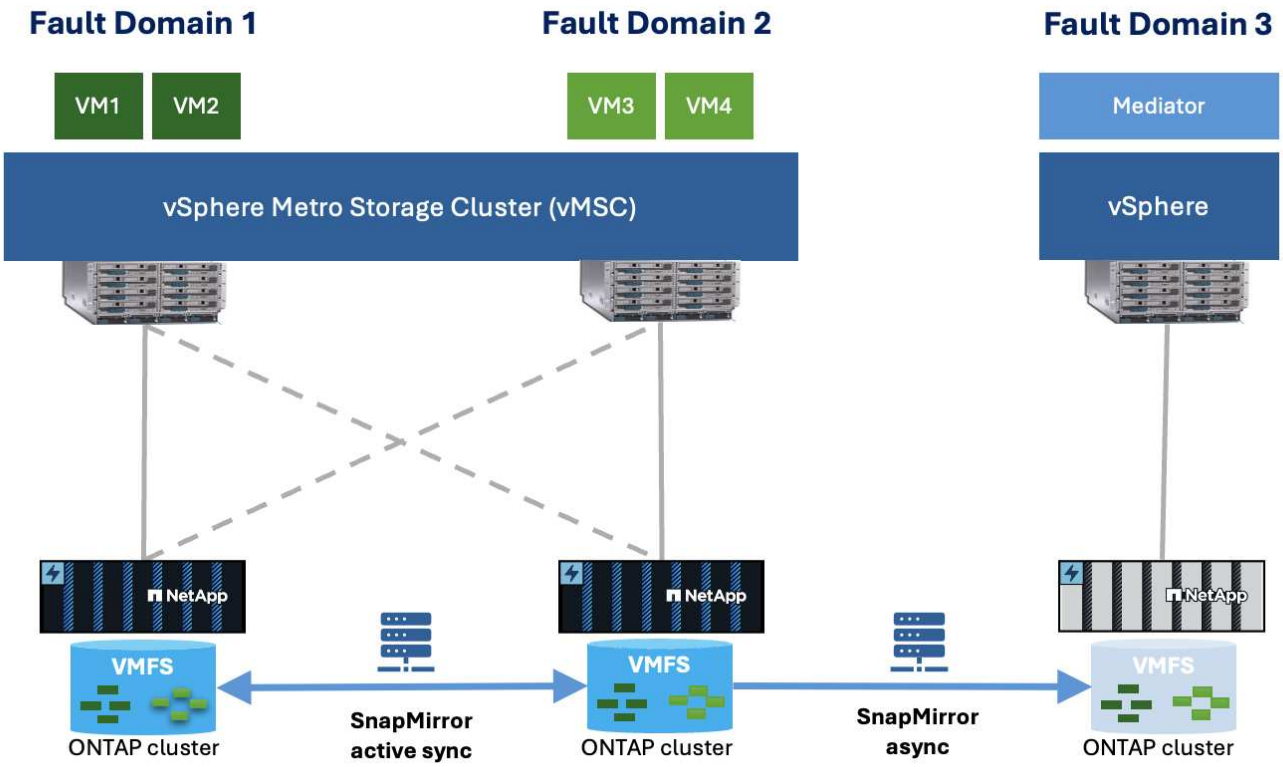


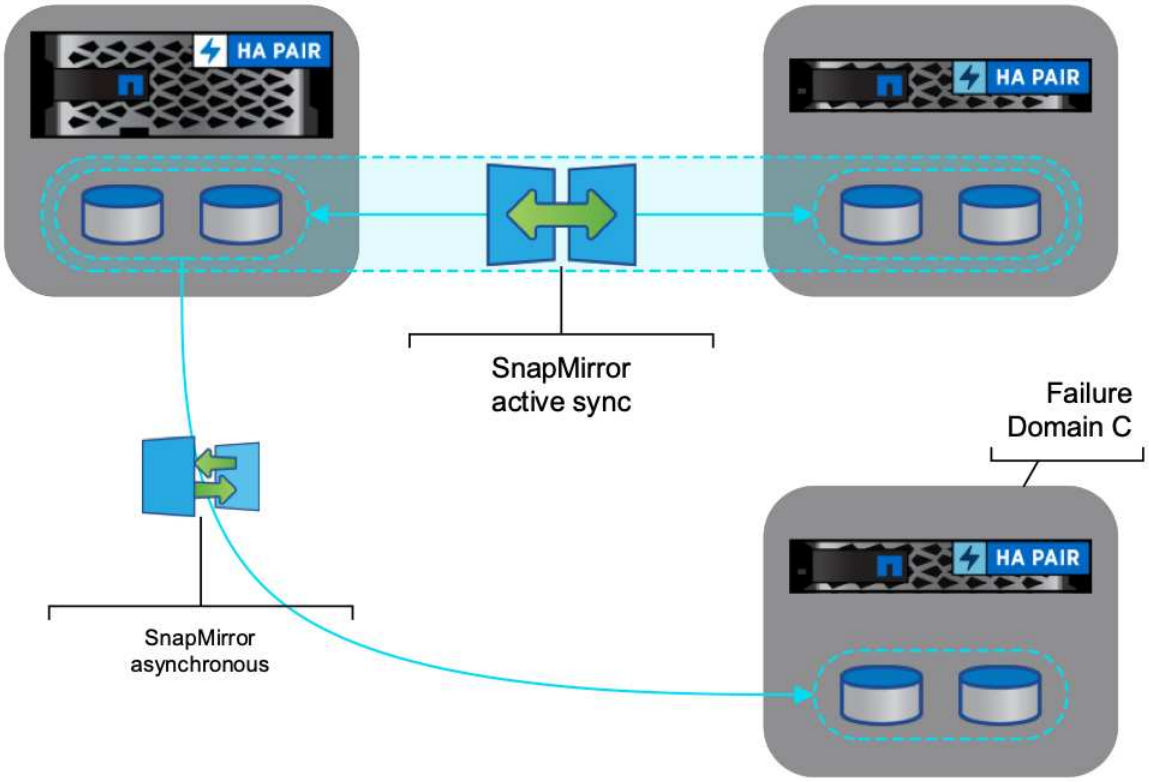
10. Per ulteriori dettagli e per aggiornare le informazioni di prossimità dell'host, è possibile utilizzare l'opzione Relazioni cluster host in ONTAP Tools.

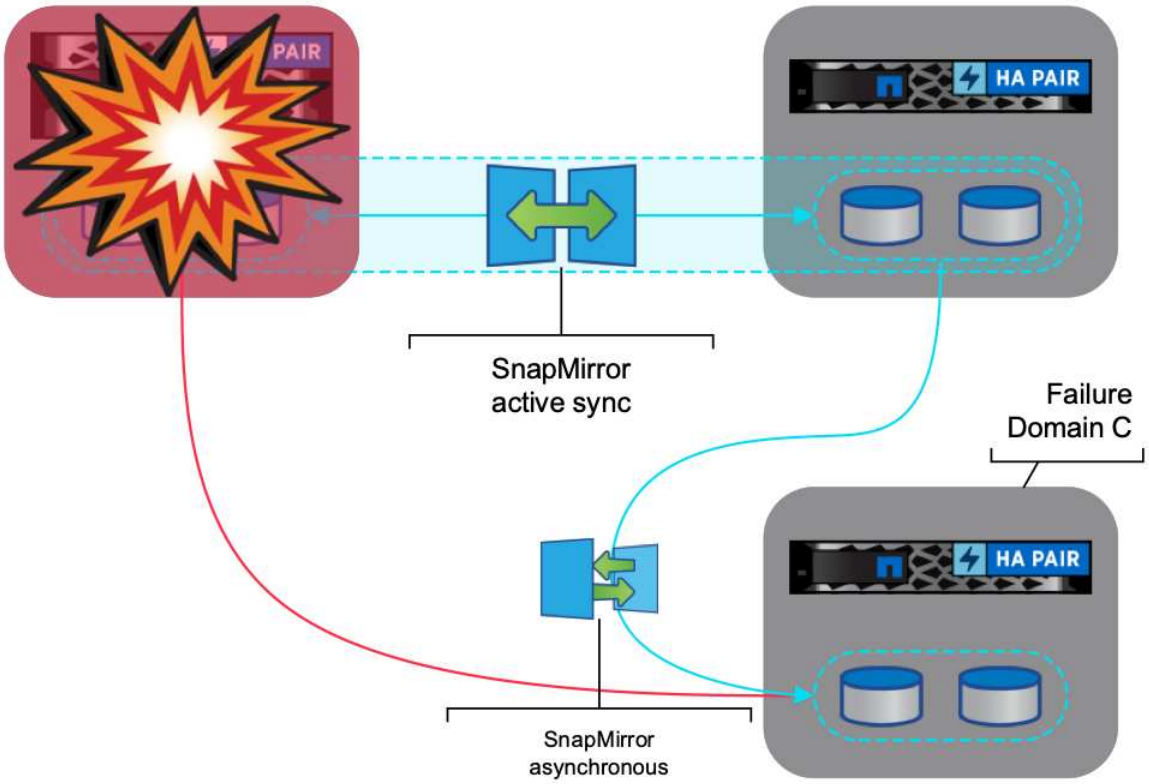


Protezione VM con plug-in SnapCenter per VMware vSphere.

Il plug-in SnapCenter per VMware vSphere (SCV) 6,0 o versione successiva supporta la sincronizzazione attiva di SnapMirror e anche in combinazione con SnapMirror Async per la replica nel terzo dominio di errore.

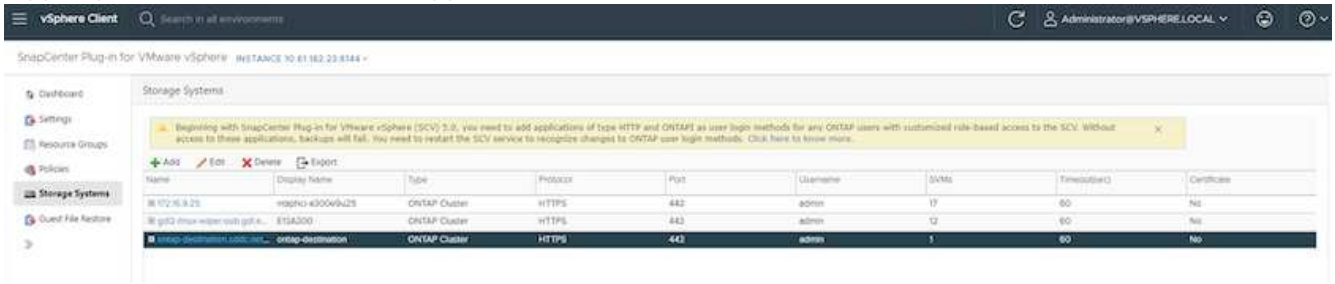

Fault Domain 1
Fault Domain 2
Fault Domain 3
VM1
VM2
VM3
VM4
Mediator
vSphere Metro Storage Cluster (vMSC)
vSphere
NetApp
NetApp
NetApp
VMFS
VMFS
VMFS
ONTAP cluster
SnapMirror
active sync
ONTAP cluster
SnapMirror
async
ONTAP cluster


HA PAIR
HA PAIR
SnapMirror
active sync
Failure
Domain C
HA PAIR
SnapMirror
asynchronous

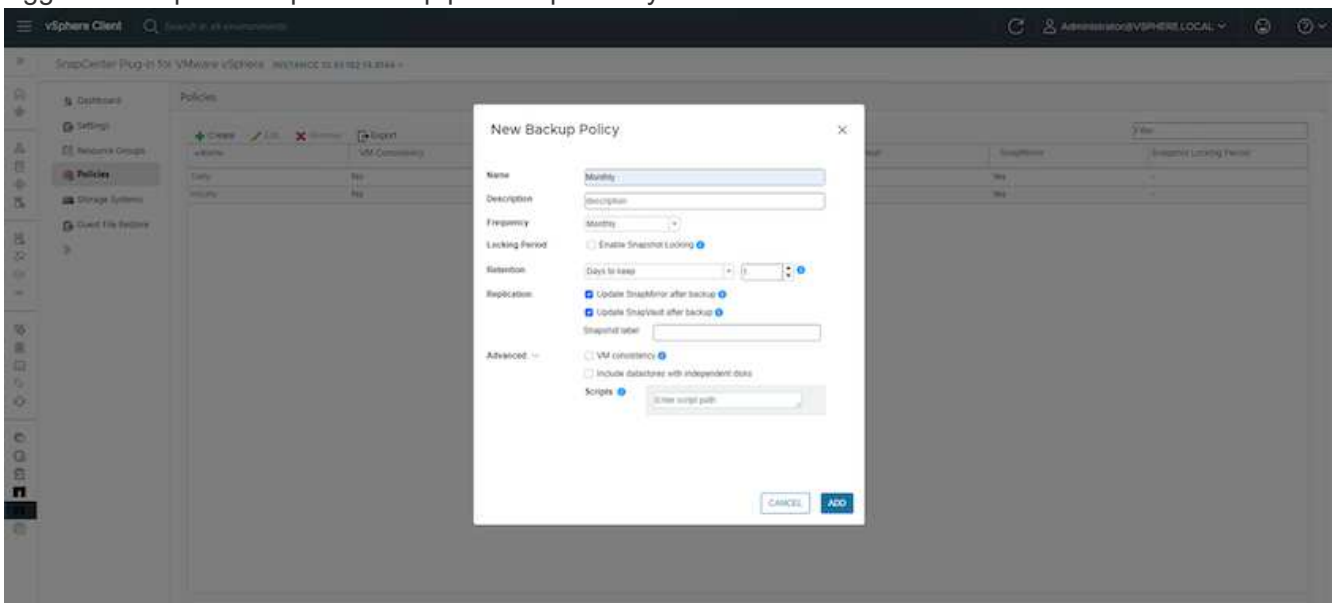

PAIR
HA PAIR
SnapMirror
active sync
Failure
Domain C
HA PAIR
SnapMirror
asynchronous

I casi di utilizzo supportati includono: * Backup e ripristino della VM o del datastore da uno dei domini di errore con sincronizzazione attiva SnapMirror. * Ripristinare le risorse dal terzo dominio di errore.

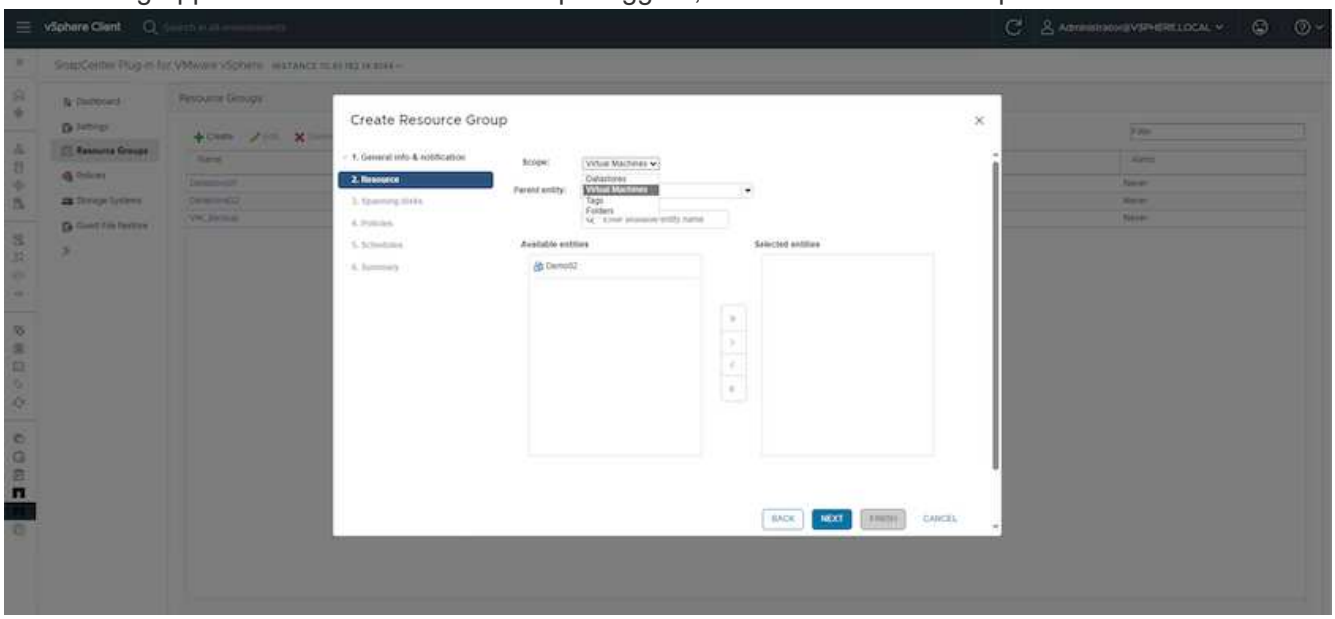
1. Aggiungere tutti i sistemi di stoccaggio ONTAP previsti per l'uso nel distributore idraulico.



2. Crea criterio. Assicurarsi che Aggiorna SnapMirror dopo il backup sia controllato per SM-AS e anche Aggiorna SnapVault dopo il backup per la replica Async al terzo dominio di errore.

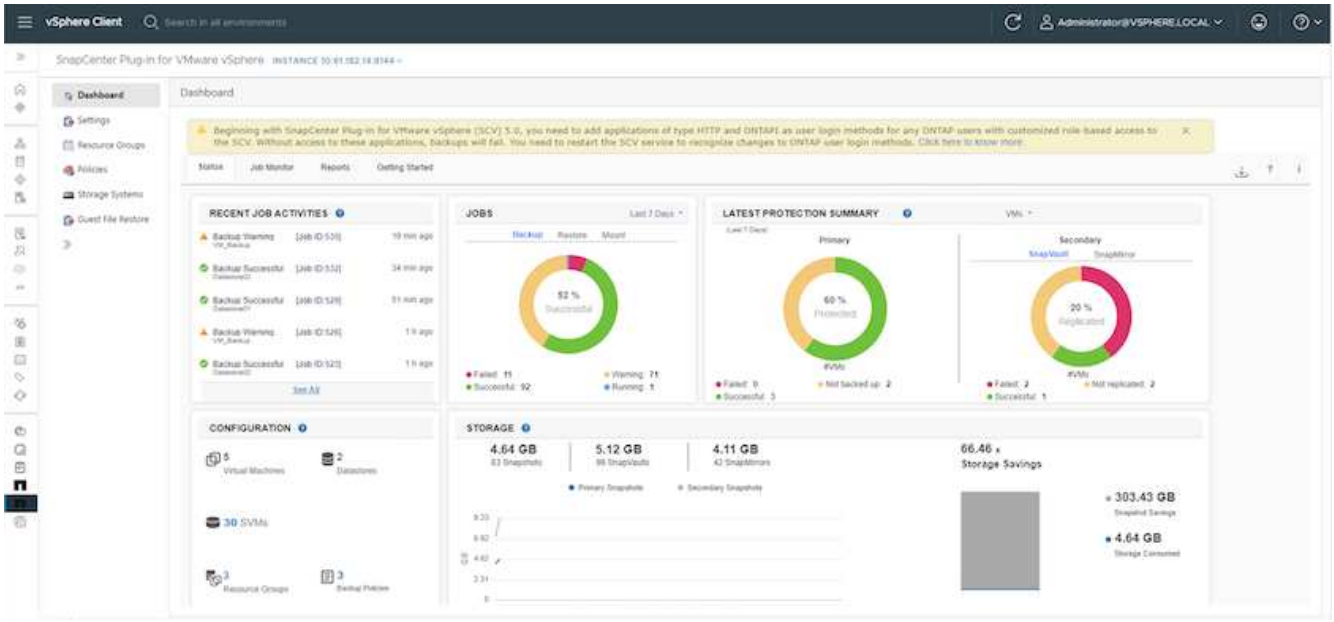


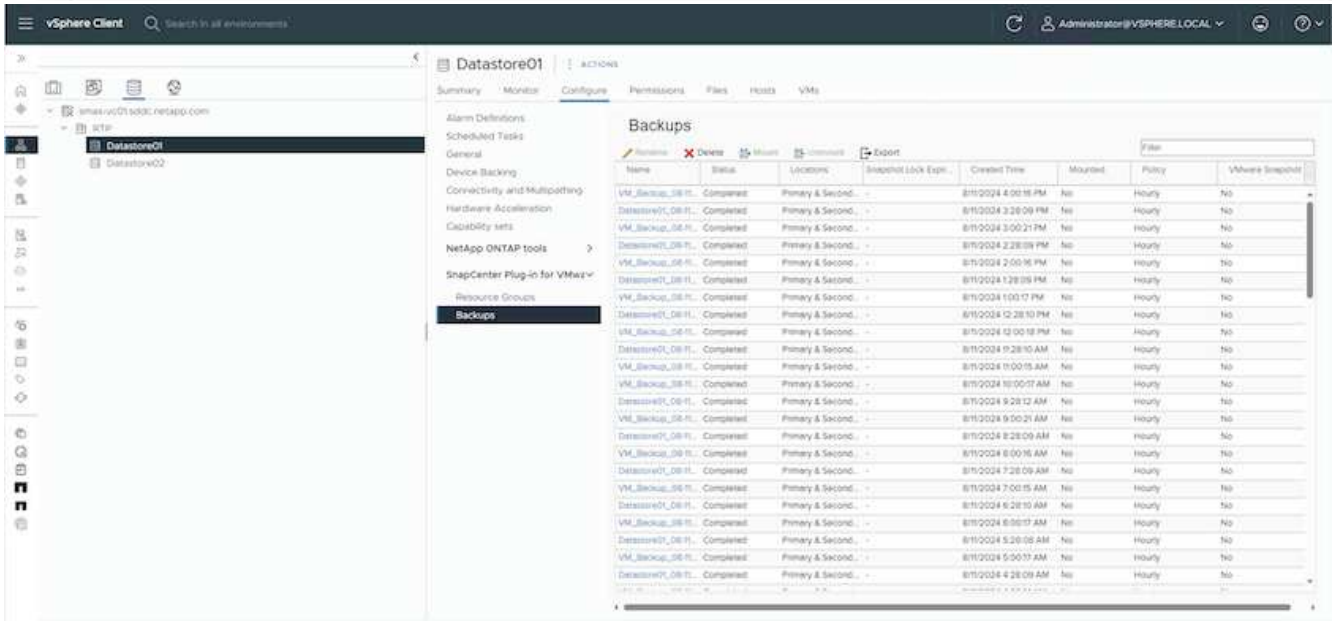
3. Creare un gruppo di risorse con elementi da proteggere, da associare a criteri e pianificazioni.

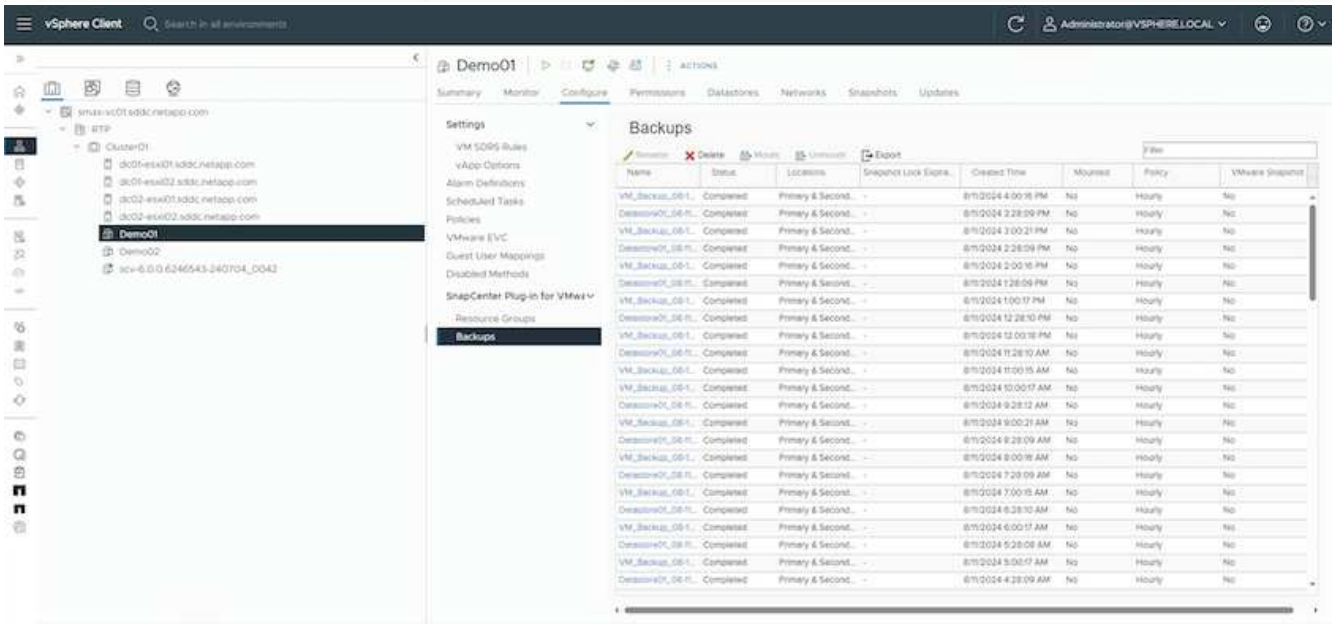


NOTA: Il nome dell'istantanea che termina con _Recent non è supportato con SM-AS.

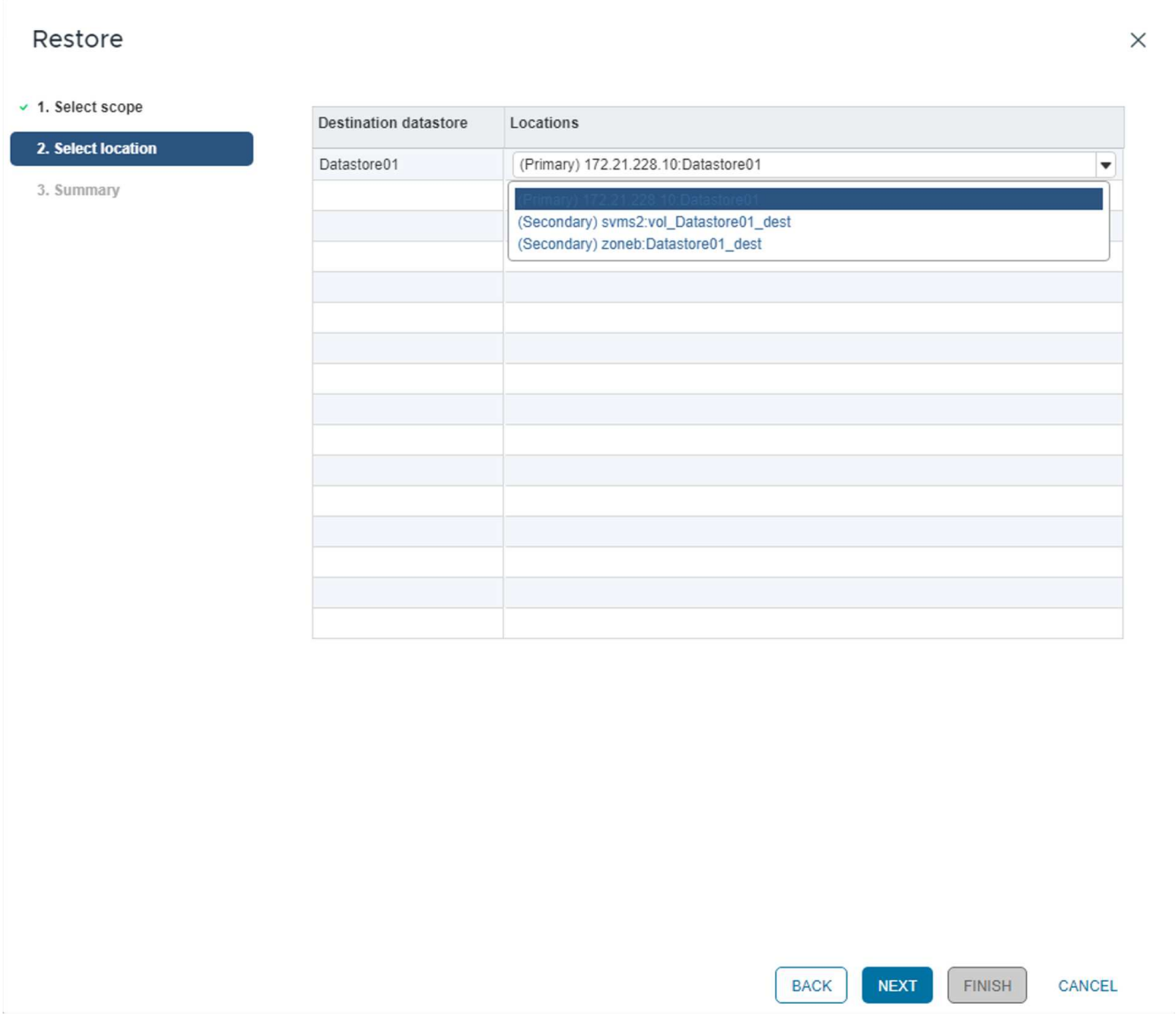
4. I backup vengono eseguiti all'ora pianificata in base ai criteri associati al gruppo di risorse. I processi possono essere monitorati dal monitor processi Dashboard o dalle informazioni di backup su tali risorse.


vSphere Client
Administrator@VSPHERE.LOCAL
SnapCenter Plug-in for VMware vSphere
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
RECENT JOB ACTIVITIES
JOBS
LATEST PROTECTION SUMMARY
Primary
Secondary
CONFIGURATION
STORAGE
4.64 GB
5.12 GB
4.11 GB
66.46 x
Storage Savings
303.43 GB
4.64 GB
30 SVMs

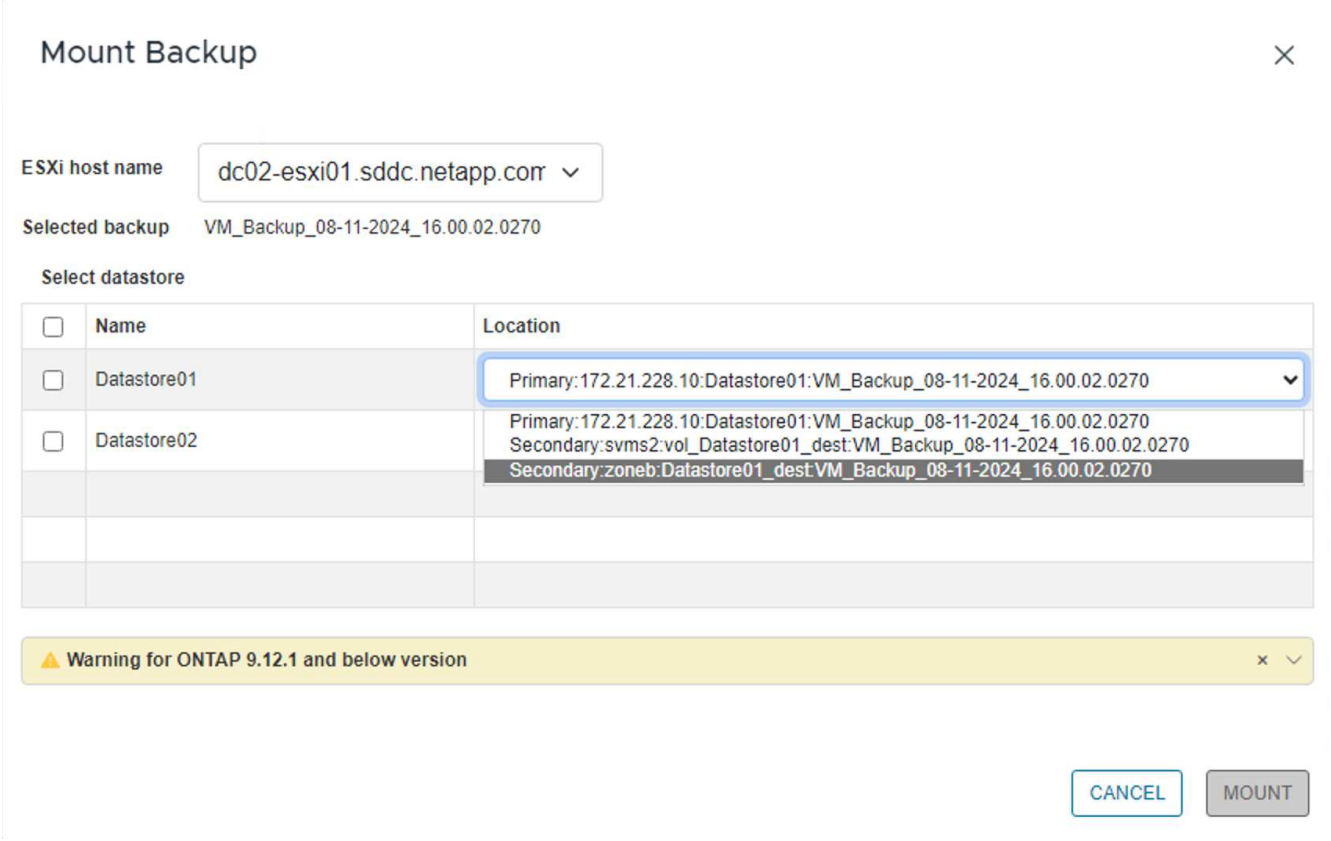

vSphere Client
Administrator@VSPHERE.LOCAL
Datastore01
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capability sets
NetApp ONTAP tools
SnapCenter Plug-in for VMware
Resource Groups
Backups
Backups
Delete
Export


vSphere Client
Administrator@VSPHERE.LOCAL
Demo01
Summary
Monitor
Configure
Permissions
Datastores
Networks
Snapshots
Updates
Settings
VM SDRS Rules
vApp Options
Alarm Definitions
Scheduled Tasks
Policies
VMware EVC
Guest User Mappings
Disabled Methods
SnapCenter Plug-in for VMware
Resource Groups
Backups
Backups
Delete
Export

5. Le macchine virtuali possono essere ripristinate sullo stesso vCenter o in un vCenter alternativo dalla SVM sul dominio di errore primario o da una delle posizioni secondarie.



6. Un’opzione simile è disponibile anche per l’operazione di montaggio del datastore.



Per assistenza nelle operazioni aggiuntive con il distributore idraulico, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere"

VMware Cloud Foundation

VMware Cloud Foundation

VMware Cloud Foundation (VCF) è un set di tecnologie che offre un percorso semplice per accedere a un'esperienza di cloud ibrido. Nella soluzione VCF, viene fornito supporto per i workload Kubernetes nativi e basati sulle macchine virtuali. I servizi essenziali come VMware vSphere, VMware vSAN, VMware NSX-T Data Center e VMware vRealize Cloud Management sono parte integrante del pacchetto VCF. Una volta combinati, questi servizi creano un'infrastruttura software-defined in grado di gestire la gestione di calcolo, storage, rete, sicurezza e cloud. Questa infrastruttura collettiva offre un'esperienza ibrida, in cui il framework VCF estende l'ambiente dal data center on-site ad Amazon Web Services (AWS), Azure e Google Cloud.

Risorse di documentazione

Per informazioni dettagliate sulle offerte NetApp per VMware Cloud Foundation, fare riferimento alle seguenti quattro (4) serie di blog in parte:

- "NetApp e VMware Cloud Foundation Made Easy parte 1: Introduzione"
- "NetApp e VMware Cloud Foundation Easy Part 2: Storage principale VCF e ONTAP"
- "NetApp e VMware Cloud Foundation hanno semplificato parte 3: VCF e storage Element Principal"

- "NetApp e VMware Cloud Foundation Made Easy - parte 4: Strumenti ONTAP per VMware e storage supplementare"

VMware Cloud Foundation con NetApp All-Flash SAN Array

- "VCF con array NetApp ASA, Introduzione e panoramica della tecnologia"
- "Utilizzare gli strumenti ONTAP per distribuire gli archivi dati iSCSI in un dominio di gestione VCF"
- "Utilizzare gli strumenti ONTAP per distribuire datastore vVol (iSCSI) in un dominio del carico di lavoro VI"
- "Configurare i datastore NVMe su TCP per l'utilizzo in un dominio di carico di lavoro VI"
- "Distribuire e utilizzare il plug-in SnapCenter per VMware vSphere per proteggere e ripristinare le macchine virtuali in un dominio del carico di lavoro VI"

VMware Cloud Foundation con NetApp All-Flash AFF Array

- "VCF con array NetApp AFF, Introduzione e panoramica della tecnologia"
- "Utilizzare ONTAP con NFS come storage principale per i domini di carico di lavoro VI"
- "USA gli strumenti ONTAP per implementare i datastore NFS in un dominio del carico di lavoro VI"

Soluzioni NetApp FlexPod per VMware Cloud Foundation

- "Espansione del cloud ibrido FlexPod con VMware Cloud Foundation"
- "FlexPod come dominio del carico di lavoro per la base cloud di VMware"
- "FlexPod as a workload Domain for VMware Cloud Foundation Design Guide (in inglese)"

VCF con array NetApp ASA

VMware Cloud Foundation con NetApp All-Flash SAN Array

VMware Cloud Foundation (VCF) è una piattaforma SDDC (Software Defined Data Center) integrata che fornisce uno stack completo di infrastrutture software-defined per eseguire applicazioni aziendali in un ambiente di cloud ibrido. Combina funzionalità di calcolo, storage, networking e gestione in una piattaforma unificata, offrendo un'esperienza operativa coerente su cloud pubblici e privati.

Autore: Josh Powell

Il presente documento fornisce informazioni sulle opzioni di storage disponibili per VMware Cloud Foundation utilizzando l'array SAN all-flash DI NetApp. Le opzioni di storage supportate sono coperte da istruzioni specifiche per la distribuzione di datastore iSCSI come storage supplementare per domini di gestione e datastore vVol (iSCSI) e NVMe/TCP come datastore supplementare per domini di workload. Inoltre, viene offerta la data Protection di macchine virtuali e datastore che utilizzano SnapCenter per VMware vSphere.

Casi di utilizzo

Casi d'utilizzo illustrati nella presente documentazione:

- Opzioni di storage per i clienti che cercano ambienti uniformi su cloud pubblici e privati.
- Soluzione automatizzata per l'implementazione dell'infrastruttura virtuale per i domini di carico di lavoro.
- Soluzione storage scalabile realizzata su misura per soddisfare esigenze in evoluzione, anche se non

allineata direttamente ai requisiti delle risorse di calcolo.

- Distribuire storage supplementare ai domini di gestione e carico di lavoro VI utilizzando ONTAP Tools per VMware vSphere.
- Proteggi macchine virtuali e datastore utilizzando il plug-in SnapCenter per VMware vSphere.

Pubblico

Questa soluzione è destinata alle seguenti persone:

- Architetti delle soluzioni alla ricerca di opzioni di storage più flessibili per ambienti VMware che siano progettati per massimizzare il TCO.
- Solution Architect in cerca di opzioni storage VCF che offrono opzioni di protezione dei dati e disaster recovery con i principali cloud provider.
- Amministratori dello storage che desiderano istruzioni specifiche su come configurare VCF con lo storage principale e supplementare.
- Amministratori dello storage che desiderano istruzioni specifiche su come proteggere macchine virtuali e datastore che risiedono sullo storage ONTAP.

Panoramica sulla tecnologia

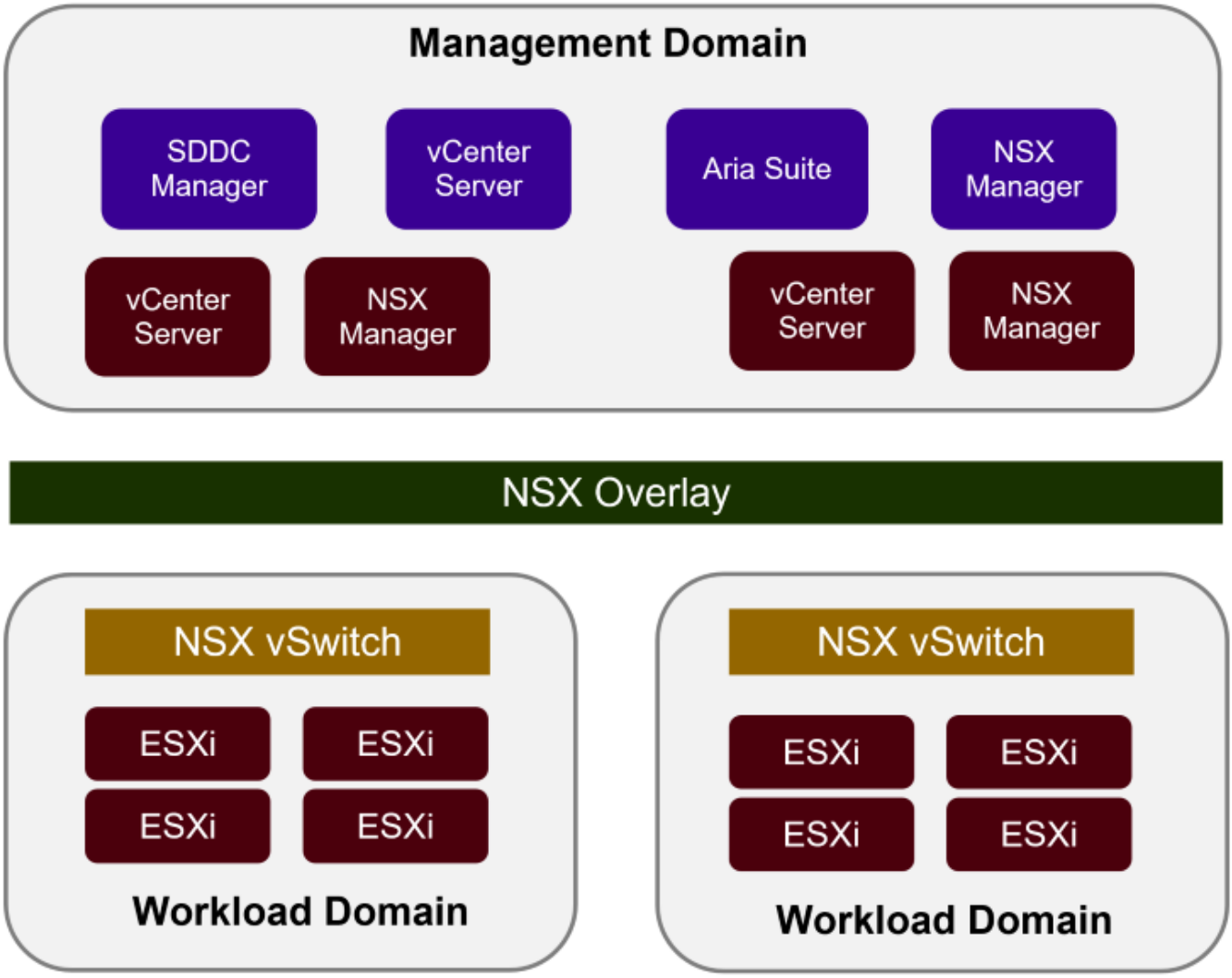
La soluzione VCF con NetApp ASA comprende i seguenti componenti principali:

VMware Cloud Foundation

VMware Cloud Foundation amplia le offerte di hypervisor VMware vSphere combinando componenti chiave come SDDC Manager, vSphere, vSAN, NSX e VMware aria Suite per creare un data center software-defined.

La soluzione VCF supporta sia i workload Kubernetes nativi che quelli basati su macchine virtuali. I servizi chiave come VMware vSphere, VMware vSAN, VMware NSX-T Data Center e VMware aria Cloud Management sono parte integrante del pacchetto VCF. Una volta combinati, questi servizi creano un'infrastruttura software-defined in grado di gestire in modo efficiente la gestione di calcolo, storage, networking, sicurezza e cloud.

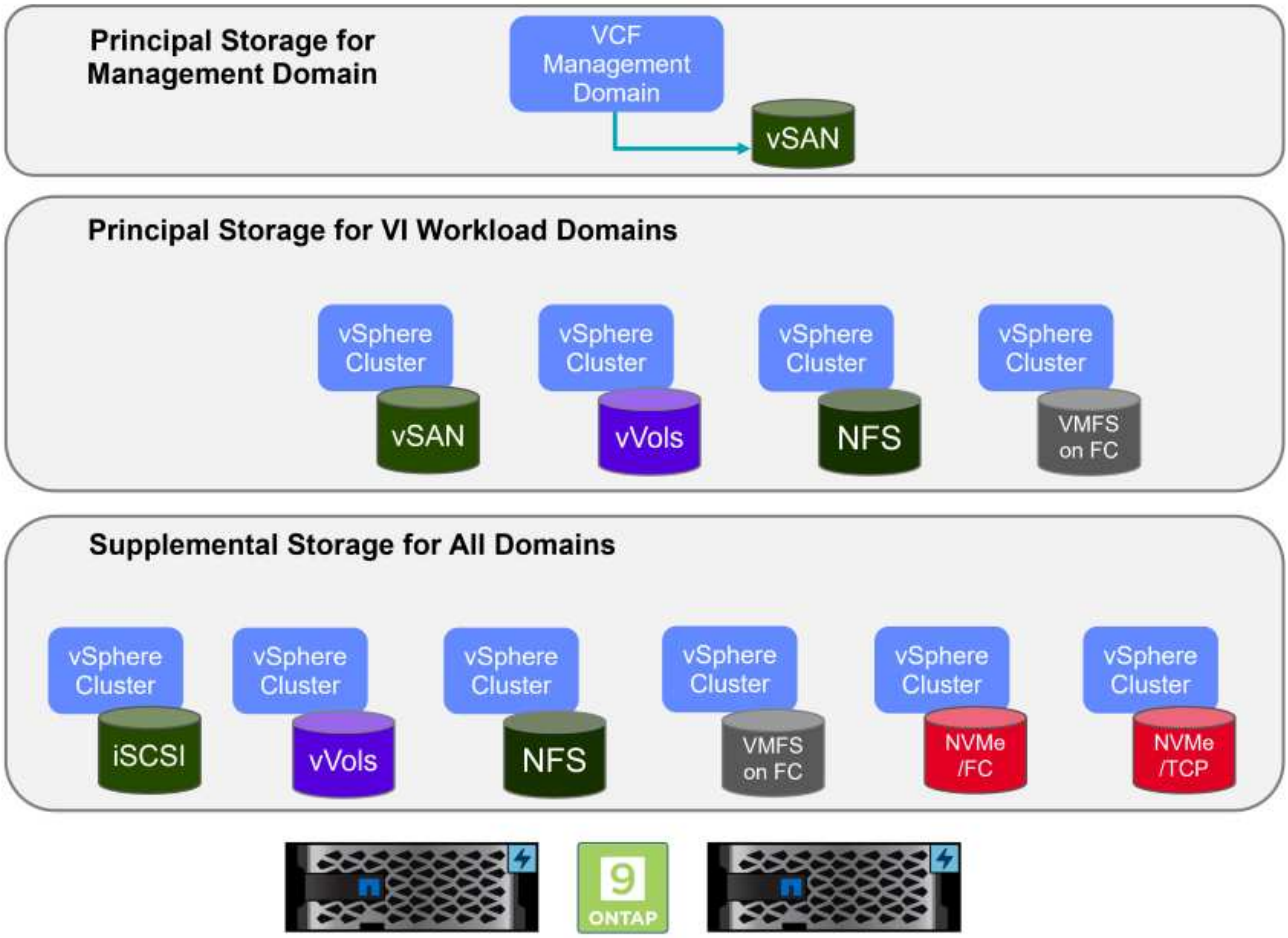
VCF è costituito da un singolo dominio di gestione e fino a 24 domini di workload VI che rappresentano ciascuno un'unità di infrastruttura predisposta per le applicazioni. Un dominio del carico di lavoro è costituito da uno o più cluster vSphere gestiti da una singola istanza vCenter.



Per ulteriori informazioni sull'architettura e la pianificazione di VCF, fare riferimento a. "Modelli di architettura e tipi di dominio del carico di lavoro in VMware Cloud Foundation".

Opzioni di archiviazione VCF

VMware divide le opzioni di storage per VCF in **Principal** e **integrative**. Il dominio di gestione VCF deve utilizzare vSAN come storage principale. Tuttavia, esistono molte opzioni di storage supplementari per il dominio di gestione e per le opzioni di storage principale e supplementare disponibili per i domini del carico di lavoro VI.



Archiviazione principale per i domini del carico di lavoro
Lo storage principale si riferisce a qualsiasi tipo di storage che può essere direttamente connesso a un dominio del carico di lavoro VI durante il processo di installazione in SDDC Manager. Lo storage principale viene implementato con il manager SDDC nell'ambito dell'orchestrazione per la creazione del cluster ed è il primo datastore configurato per un dominio del carico di lavoro. Include vSAN, vVol (VMFS), NFS e VMFS su Fibre Channel.

Archiviazione supplementare per domini di gestione e carico di lavoro
Lo storage supplementare è il tipo di storage che è possibile aggiungere ai domini di gestione o del carico di lavoro in qualsiasi momento dopo la creazione del cluster. Lo storage supplementare rappresenta la più ampia gamma di opzioni di storage supportate, tutte supportate dagli array NetApp ASA. È possibile implementare storage supplementare utilizzando i tool ONTAP per VMware vSphere per la maggior parte dei tipi di protocollo di storage.

Ulteriori risorse di documentazione per VMware Cloud Foundation:
* "Documentazione di VMware Cloud Foundation"
* "Tipi di storage supportati per VMware Cloud Foundation"
* "Gestione dello storage in VMware Cloud Foundation"

Array SAN all-flash NetApp

L'array SAN all-flash NetApp (ASA) è una soluzione storage ad elevate performance progettata per soddisfare le esigenti necessità dei data center moderni. Combina velocità e affidabilità dello storage flash con le funzioni avanzate di gestione dei dati di NetApp, in modo da offrire performance, scalabilità e protezione dei dati

eccezionali.

La linea ASA comprende sia i modelli A-Series che C-Series.

Gli array flash NetApp A-Series all-NVMe sono progettati per carichi di lavoro dalle performance elevate, offrendo latenza estremamente bassa ed elevata resilienza, rendendoli adatti ad applicazioni mission-critical.

I Flash Array C-Series QLC mirano a casi di utilizzo di capacità più elevata, fornendo la velocità della tecnologia flash insieme al risparmio della tecnologia flash ibrida.

Per informazioni dettagliate, consultare la "Landing page di NetApp ASA".

Supporto dei protocolli di storage

Il sistema ASA supporta tutti i protocolli SAN standard tra cui iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) e NVME over Fabrics.

ISCSI - NetApp ASA fornisce un solido supporto per iSCSI, consentendo l'accesso a livello di blocco ai dispositivi di storage su reti IP. Offre un'integrazione perfetta con gli initiator iSCSI, consentendo un provisioning e una gestione efficienti delle LUN iSCSI. Funzionalità avanzate di ONTAP, come multipathing, autenticazione CHAP e supporto ALUA.

Per istruzioni sulla progettazione delle configurazioni iSCSI, fare riferimento alla "Documentazione di riferimento per la configurazione SAN".

Fibre Channel - NetApp ASA offre un supporto completo per Fibre Channel (FC), una tecnologia di rete ad alta velocità comunemente utilizzata nelle reti SAN. ONTAP si integra perfettamente con l'infrastruttura FC, fornendo un accesso a livello di blocco affidabile ed efficiente ai dispositivi storage. Offre funzioni come zoning, multi-path e fabric login (FLOGI) per ottimizzare le prestazioni, migliorare la sicurezza e garantire una

connettività perfetta negli ambienti FC.

Per informazioni sulla progettazione delle configurazioni Fibre Channel, fare riferimento alla "Documentazione di riferimento per la configurazione SAN".

NVMe over Fabrics - NetApp ONTAP e ASA supportano NVMe over Fabrics. NVMe/FC consente l'utilizzo di dispositivi storage NVMe su un'infrastruttura Fibre Channel e NVMe/TCP su reti IP di storage.

Per informazioni sulla progettazione su NVMe, fare riferimento a. "Configurazione, supporto e limitazioni NVMe"

Tecnologia Active-Active

Gli array SAN all-flash NetApp offrono percorsi Active-Active attraverso entrambi i controller, eliminando la necessità per il sistema operativo host di attendere un errore di percorso attivo, prima di attivare il percorso alternativo. Ciò significa che l'host può utilizzare tutti i percorsi disponibili su tutti i controller, garantendo che i percorsi attivi siano sempre presenti, indipendentemente dal fatto che il sistema si trovi in uno stato regolare o stia eseguendo un'operazione di failover del controller.

Inoltre, NetApp ASA offre una caratteristica distintiva che migliora notevolmente la velocità del failover SAN. Ogni controller replica continuamente i metadati LUN essenziali al proprio partner. Di conseguenza, ogni controller è pronto ad assumersi le responsabilità del Data Serving in caso di guasto improvviso del partner. Questa disponibilità è possibile perché il controller possiede già le informazioni necessarie per iniziare a utilizzare le unità precedentemente gestite dal controller guasto.

Con il path Active-Active, i takeover pianificati e non pianificati hanno tempi di ripresa io di 2-3 secondi.

Per ulteriori informazioni, vedere "TR-4968, array All-SAS NetApp – disponibilità e integrità dei dati con NetApp ASA".

Garanzie di archiviazione

Con gli array SAN all-flash di NetApp, NetApp offre un set esclusivo di garanzie storage. I vantaggi esclusivi includono:

Garanzia di efficienza dello storage: con la garanzia di efficienza dello storage è possibile ottenere prestazioni elevate riducendo al minimo i costi di storage. 4:1:1 per i carichi di lavoro SAN.

Garanzia di disponibilità dei dati del 99,9999% (6 nove): garantisce la correzione per i downtime non pianificati superiori a 31,56 secondi all'anno.

Garanzia di recovery ransomware: recovery di dati garantito in caso di attacco ransomware.

Vedere "Portale dei prodotti NetApp ASA" per ulteriori informazioni.

Strumenti NetApp ONTAP per VMware vSphere

ONTAP Tools per VMware vSphere consente agli amministratori di gestire lo storage NetApp direttamente dal client vSphere. ONTAP Tools ti consente di implementare e gestire datastore, nonché di eseguire il provisioning dei datastore vVol.

I tool ONTAP consentono il mapping dei datastore ai profili di funzionalità dello storage che determinano un set

di attributi del sistema storage. Ciò consente la creazione di datastore con attributi specifici, come le performance dello storage e la qualità del servizio.

ONTAP Tools include inoltre un provider **VASA (VMware vSphere APIs for Storage Awareness)** per i sistemi storage ONTAP, che consente il provisioning dei datastore vVol (VMware Virtual Volumes), la creazione e l'utilizzo di profili di funzionalità dello storage, la verifica della conformità e il monitoraggio delle performance.

Per ulteriori informazioni sugli strumenti NetApp ONTAP, vedere "Strumenti ONTAP per la documentazione VMware vSphere" pagina.

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere (SCV) è una soluzione software di NetApp che offre una protezione dei dati completa per ambienti VMware vSphere. È progettato per semplificare e ottimizzare il processo di protezione e gestione delle macchine virtuali (VM) e dei datastore. SCV utilizza le istantanee basate sullo storage e la replica sugli array secondari per soddisfare gli obiettivi di tempi di ripristino inferiori.

Il plug-in SnapCenter per VMware vSphere offre in un'interfaccia unificata le seguenti funzionalità, integrate con il client vSphere:

Istantanee basate su criteri - SnapCenter consente di definire criteri per la creazione e la gestione di istantanee coerenti con le applicazioni delle macchine virtuali (VM) in VMware vSphere.

Automazione - la creazione e la gestione automatizzate delle snapshot basate su policy definite contribuiscono a garantire una protezione dei dati coerente ed efficiente.

VM-Level Protection - la protezione granulare a livello di VM consente una gestione e un ripristino efficienti delle singole macchine virtuali.

Funzioni di efficienza dello storage - l'integrazione con le tecnologie di storage NetApp offre funzioni di efficienza dello storage come la deduplica e la compressione per le snapshot, riducendo al minimo i requisiti di storage.

Il plug-in di SnapCenter orchestra l'arresto delle macchine virtuali insieme alle istantanee basate su hardware sugli storage array di NetApp. La tecnologia SnapMirror viene utilizzata per replicare le copie di backup su sistemi storage secondari, incluso il cloud.

Per ulteriori informazioni, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere".

L'integrazione di BlueXP permette strategie di backup 3-2-1 che estendono le copie dei dati allo storage a oggetti nel cloud.

Per ulteriori informazioni sulle strategie di backup 3-2-1 con BlueXP, visita il sito "Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM".

Panoramica della soluzione

Gli scenari presentati in questa documentazione dimostrano come utilizzare i sistemi di storage ONTAP come storage supplementare per i domini di gestione e di carico di lavoro. Inoltre, per proteggere macchine virtuali e datastore viene utilizzato il plug-in SnapCenter per VMware vSphere.

Scenari trattati nella presente documentazione:

- **Utilizzare gli strumenti ONTAP per distribuire gli archivi dati iSCSI in un dominio di gestione VCF**. Fare clic su **"qui"** per le fasi di implementazione.

- **Utilizzare gli strumenti ONTAP per distribuire gli archivi dati vVol (iSCSI) in un dominio del carico di lavoro VI**. Fare clic su "qui" per le fasi di implementazione.
- **Configurare i datastore NVMe su TCP per l'utilizzo in un dominio di carico di lavoro VI**. Fare clic su "qui" per le fasi di implementazione.
- **Distribuire e utilizzare il plug-in SnapCenter per VMware vSphere per proteggere e ripristinare le VM in un dominio del carico di lavoro VI**. Fare clic su "qui" per le fasi di implementazione.

Utilizzare gli strumenti di ONTAP per configurare l'archiviazione supplementare per i domini di gestione VCF

In questo scenario verrà illustrato come distribuire e utilizzare ONTAP Tools per VMware vSphere (OTV) per configurare un datastore iSCSI per un dominio di gestione VCF.

Autore: Josh Powell

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

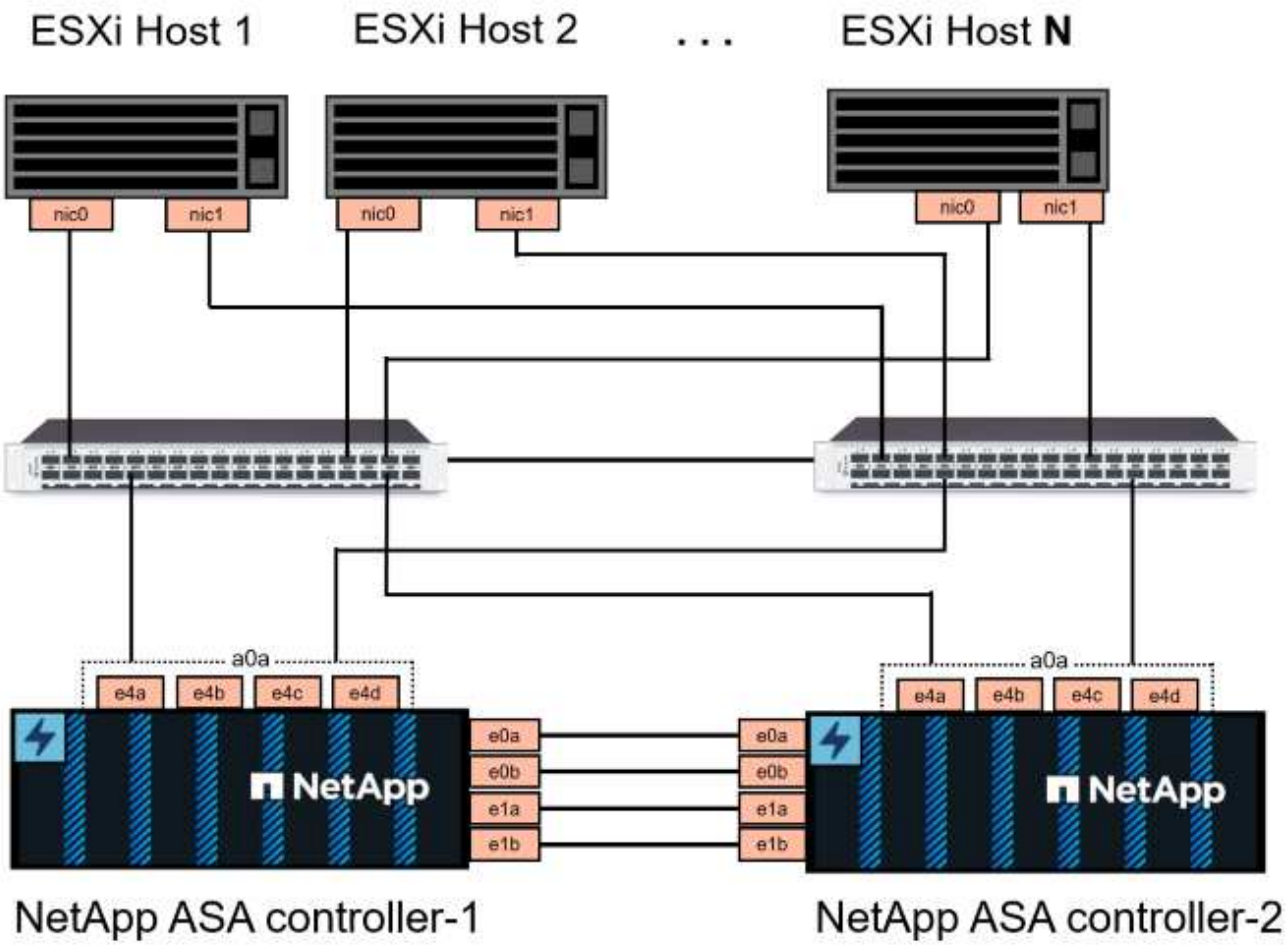
- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio di gestione VCF.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio di gestione VCF.
- Distribuire gli strumenti ONTAP nel dominio di gestione VCF.
- Creare un nuovo datastore VMFS nel dominio di gestione VCF.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con porte per dati fisici su switch ethernet dedicati al traffico di storage.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.

NetApp consiglia di progettare reti completamente ridondanti per iSCSI. Il diagramma seguente illustra un esempio di configurazione ridondante, che fornisce tolleranza agli errori per sistemi di archiviazione, switch, schede di rete e sistemi host. Consultare il NetApp "Riferimento alla configurazione SAN" per ulteriori informazioni.



Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti ethernet separate per tutte le SVM nelle configurazioni iSCSI.

Questa documentazione illustra il processo di creazione di una nuova SVM e specifica le informazioni dell'indirizzo IP per creare LIF multipli per il traffico iSCSI. Per aggiungere nuove LIF a una SVM esistente, fare riferimento a. "Creazione di una LIF (interfaccia di rete)".

Per ulteriori informazioni sull'utilizzo degli archivi dati iSCSI VMFS con VMware, fare riferimento a. "Datastore vSphere VMFS - backend storage iSCSI con ONTAP".

> Nelle situazioni in cui più adattatori VMkernel sono configurati sulla stessa rete IP, si consiglia di utilizzare il binding della porta iSCSI del software sugli host ESXi per garantire che si verifichi il bilanciamento del carico tra le schede di rete. Fare riferimento all'articolo della KB "Considerazioni sull'utilizzo del binding della porta iSCSI del software in ESX/ESXi (2038869)".

Fasi di implementazione

Per distribuire ONTAP Tools e utilizzarlo per creare un datastore VMFS nel dominio di gestione VCF, attenersi alla seguente procedura:

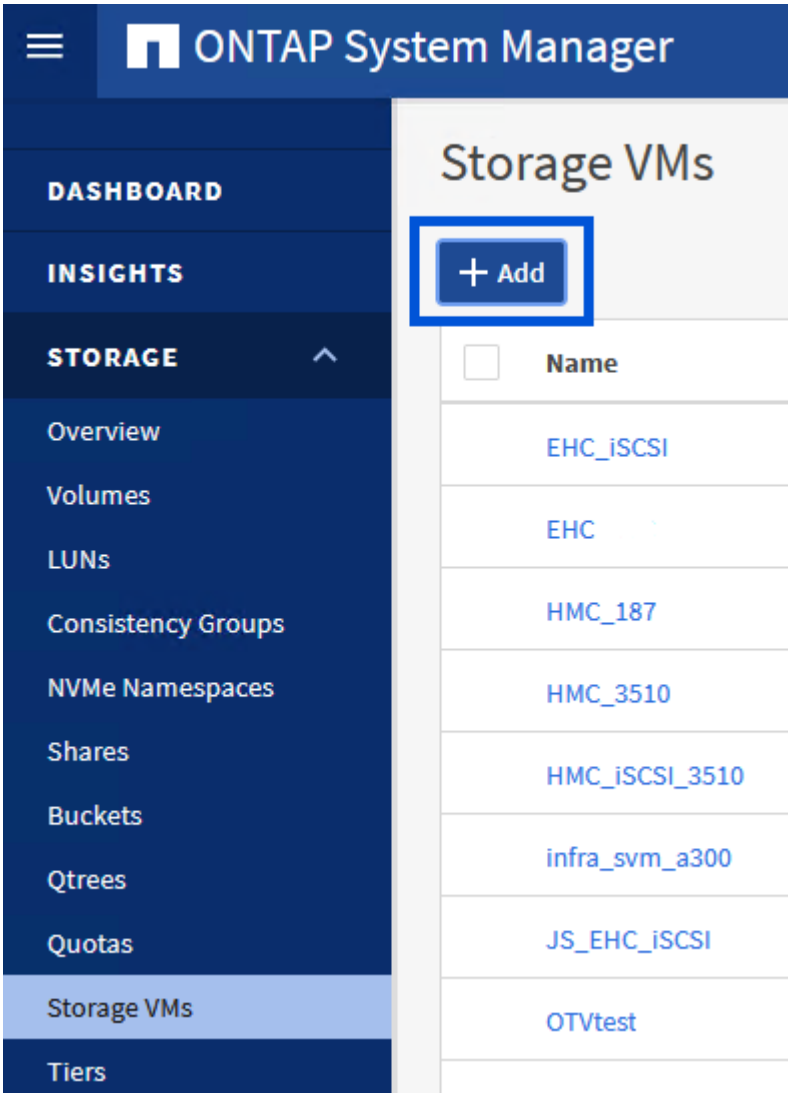
Crea SVM e LIF su un sistema storage ONTAP

Il passaggio seguente viene eseguito in Gestione di sistema di ONTAP.

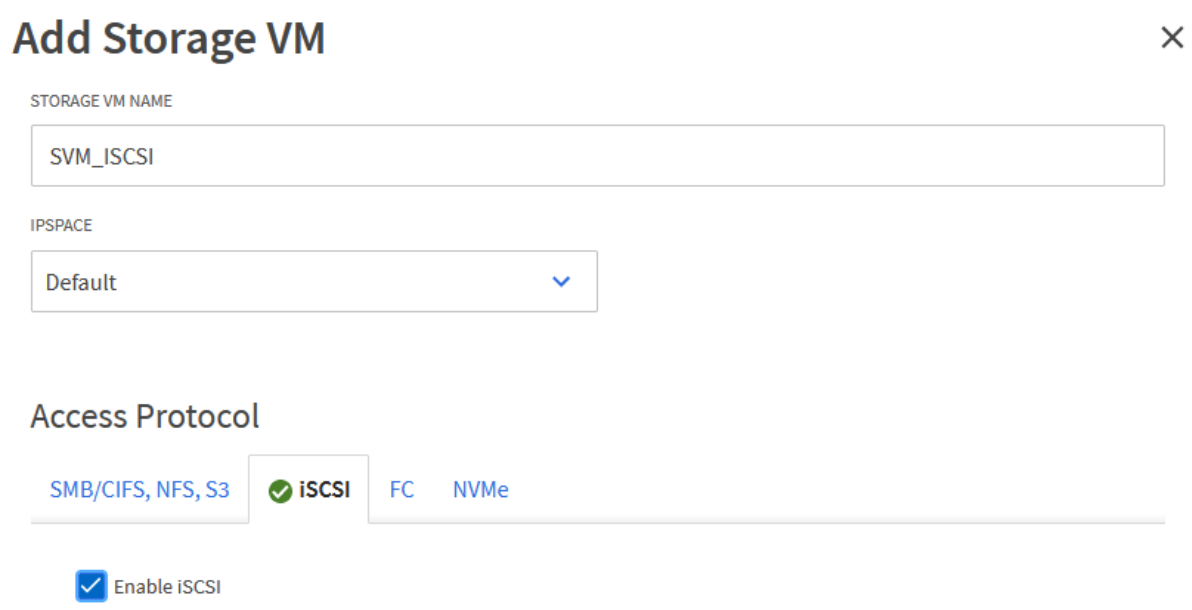
Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per il traffico iSCSI.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.

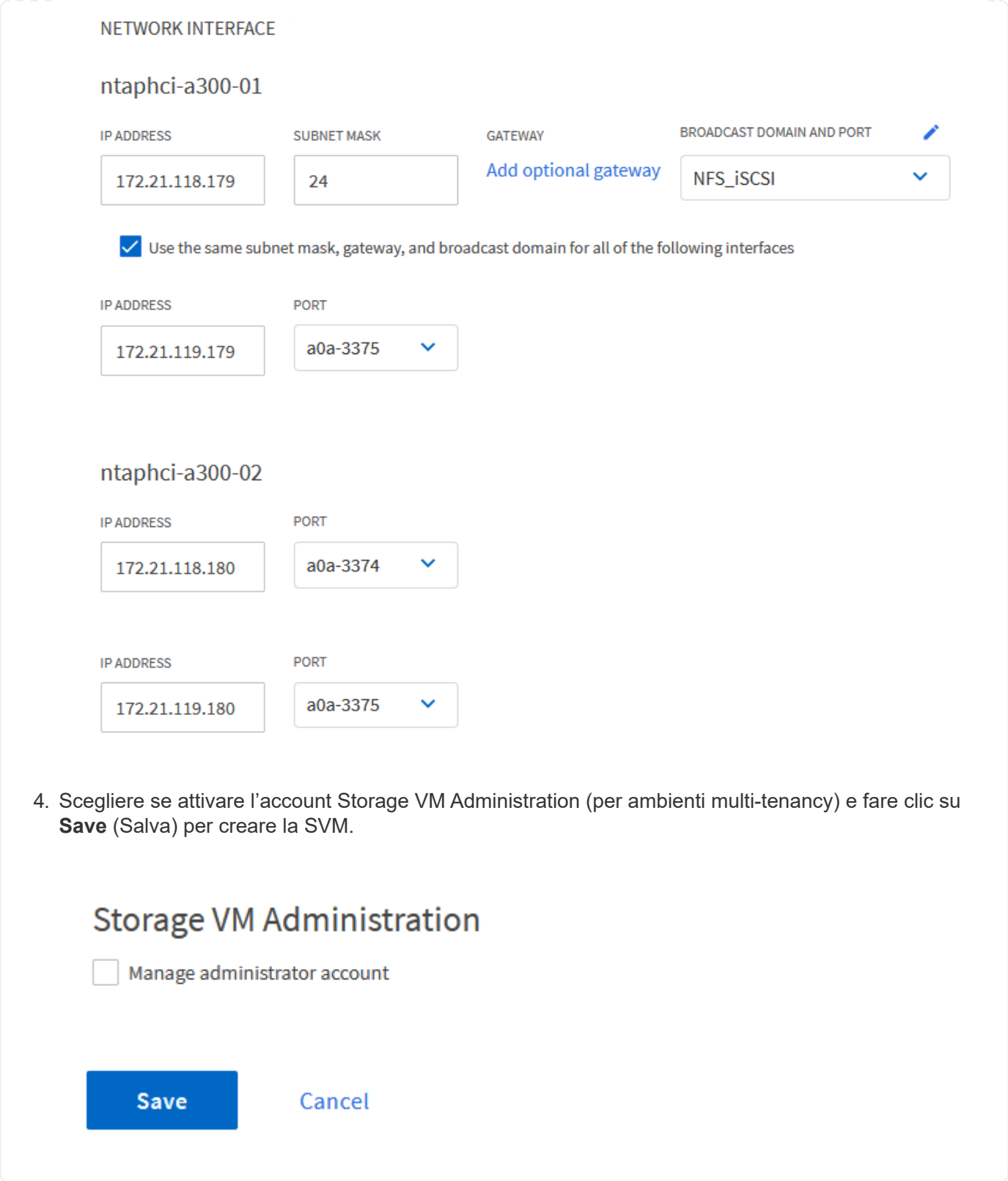


2. Nella procedura guidata **Add Storage VM** (Aggiungi VM di storage) specificare un **Name** (Nome) per la SVM, selezionare **IP Space** (spazio IP), quindi, in **Access Protocol (protocollo di accesso), fare clic sulla scheda *iSCSI** e selezionare la casella **Enable iSCSI** (Abilita iSCSI*).



3. Nella sezione **interfaccia di rete** compilare i campi **indirizzo IP**, **Subnet Mask** e **Broadcast Domain and Port** per la prima LIF. Per LIF successive, la casella di controllo può essere abilitata per usare impostazioni comuni a tutte le LIF rimanenti o per usare impostazioni separate.

> Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti Ethernet separate per tutte le SVM nelle configurazioni iSCSI.



4. Scegliere se attivare l'account Storage VM Administration (per ambienti multi-tenancy) e fare clic su **Save** (Salva) per creare la SVM.

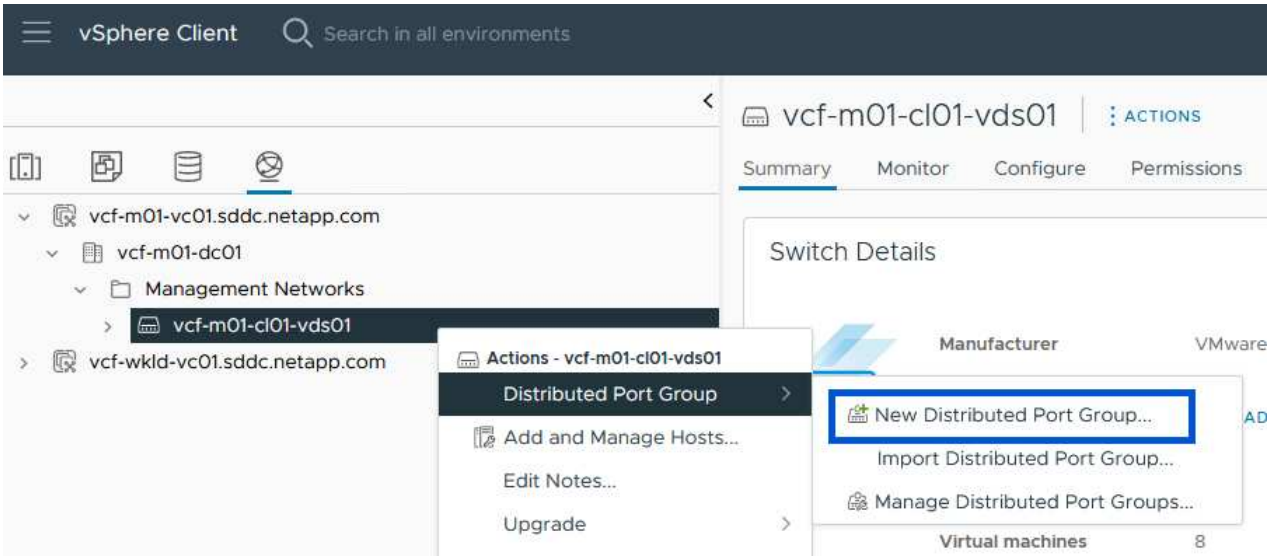
Configurare il networking per iSCSI sugli host ESXi

I seguenti passaggi vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere.

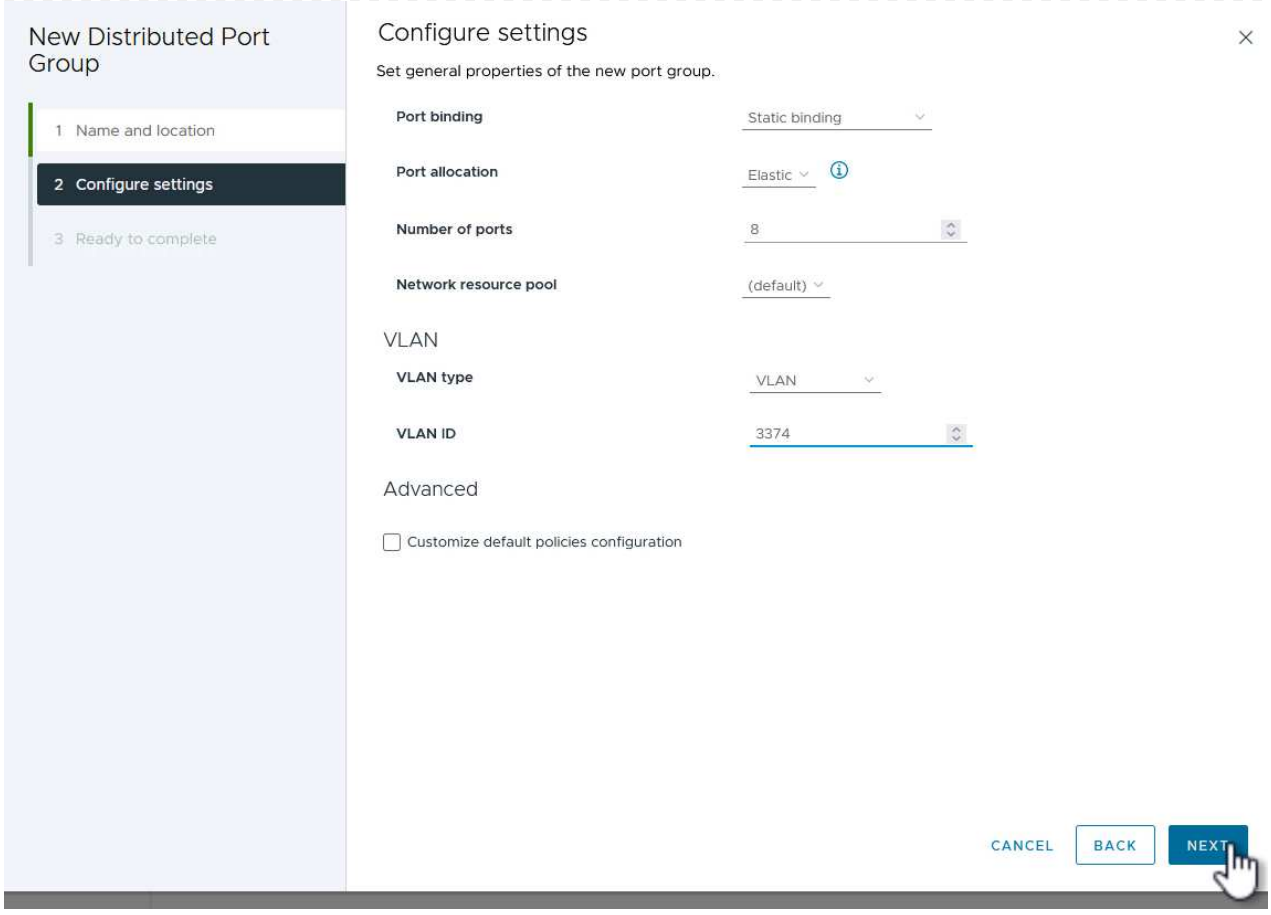
Creare gruppi di porte distribuite per il traffico iSCSI

Completare quanto segue per creare un nuovo gruppo di porte distribuite per ogni rete iSCSI:

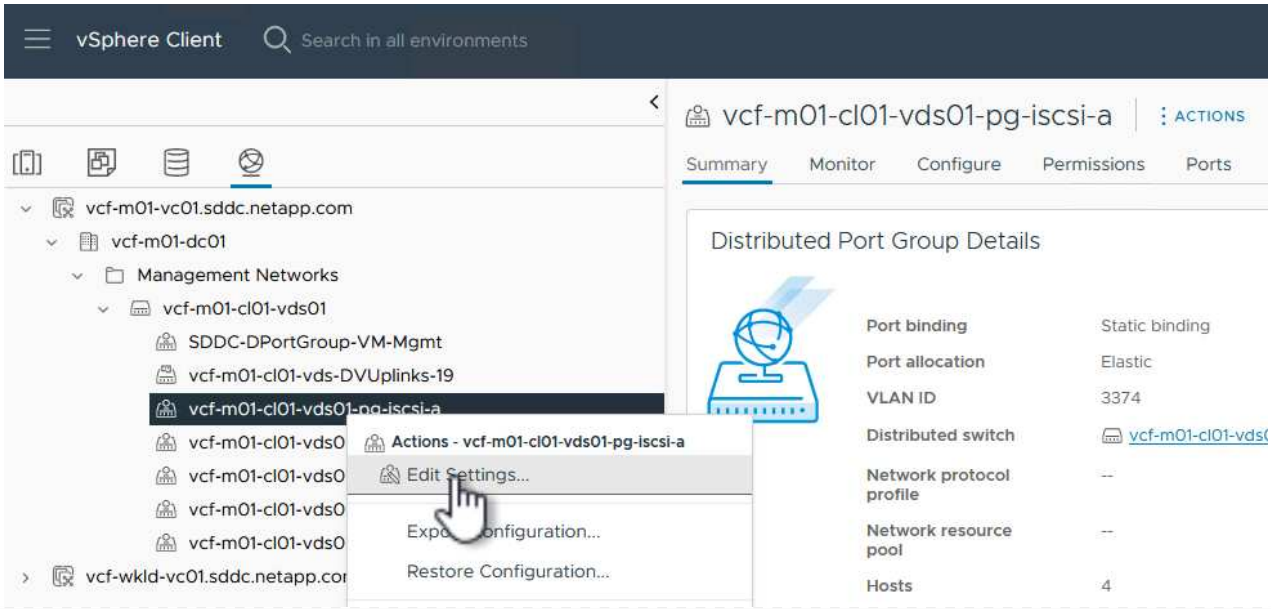
1. Dal client vSphere per il cluster del dominio di gestione, accedere a **Inventory > Networking**. Passare allo Switch distribuito esistente e scegliere l'azione da creare **nuovo Gruppo di porte distribuite…**.



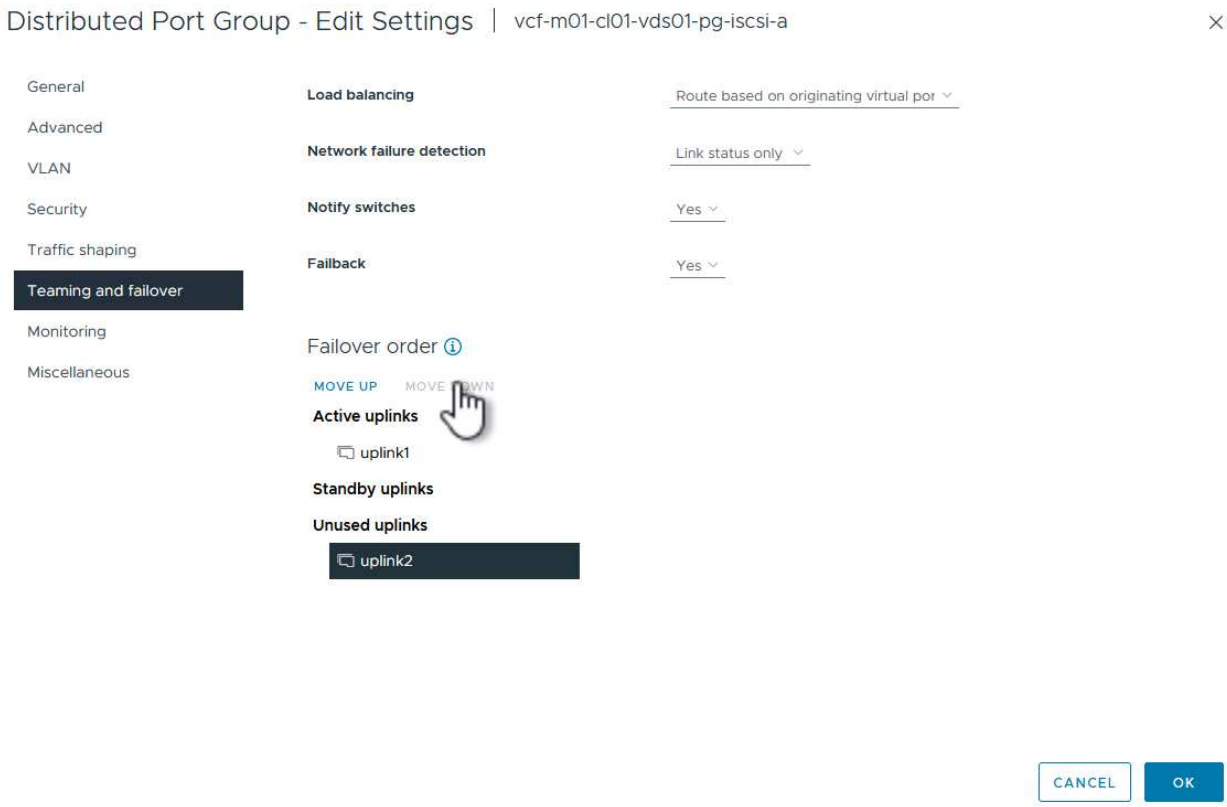
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare clic su **Avanti** per continuare.



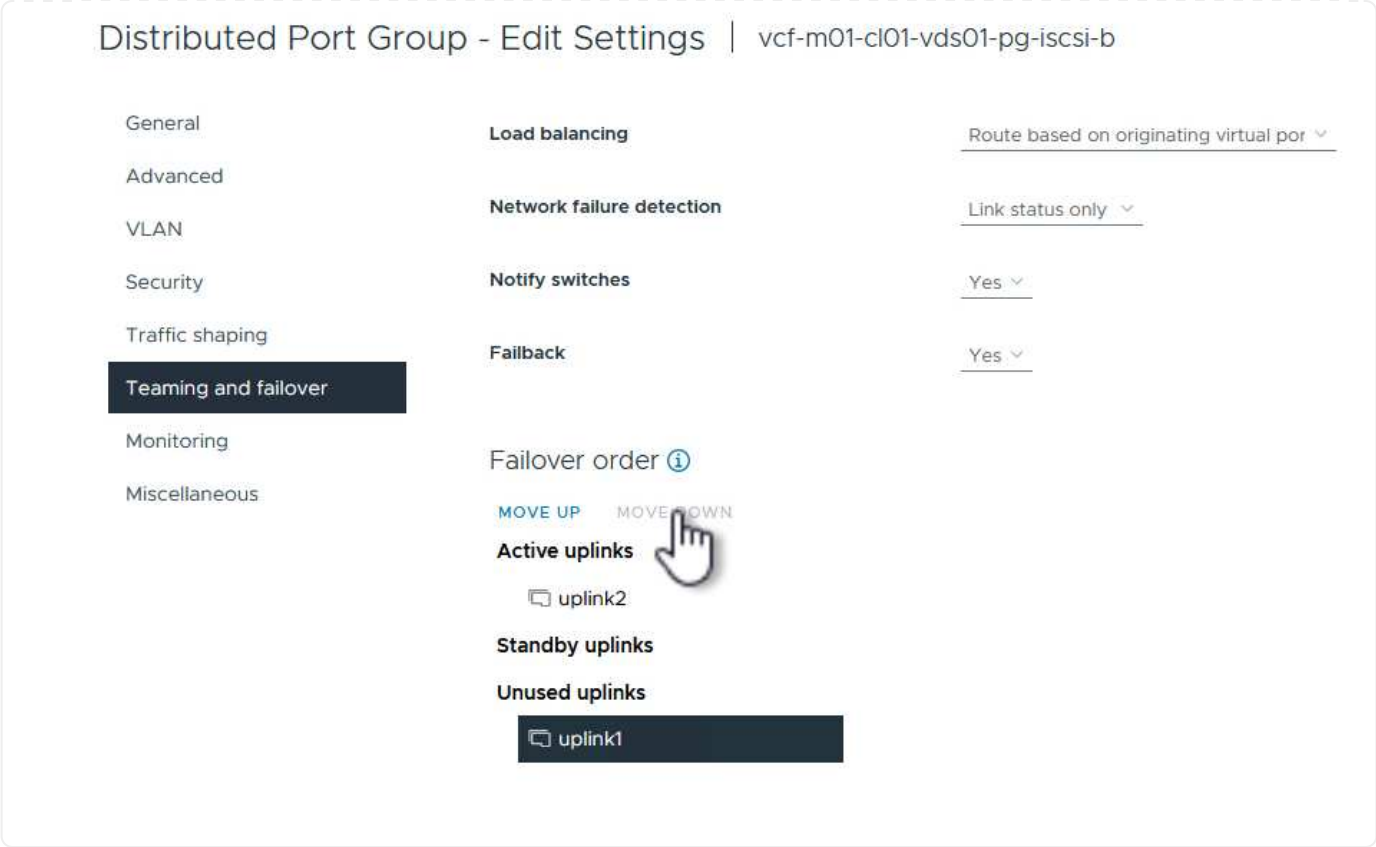
4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **fine** per creare il nuovo gruppo di porte distribuite.
5. Ripetere questa procedura per creare un gruppo di porte distribuite per la seconda rete iSCSI utilizzata e assicurarsi di aver immesso l'ID **VLAN** corretto.
6. Una volta creati entrambi i gruppi di porte, accedere al primo gruppo di porte e selezionare l'azione **Modifica impostazioni…**.



7. Nella pagina **Gruppo porte distribuite - Modifica impostazioni**, accedere a **Teaming and failover** nel menu a sinistra e fare clic su **uplink2** per spostarlo in basso in **uplink non utilizzati**.



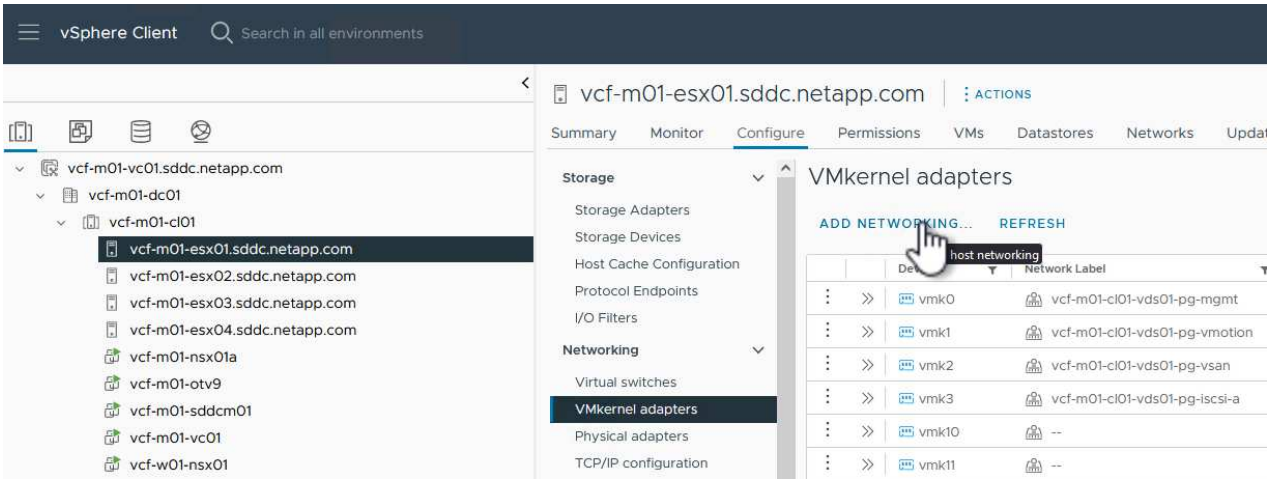
8. Ripetere questo passaggio per il secondo gruppo di porte iSCSI. Tuttavia, questa volta si sposta **uplink1** verso il basso in **uplink non utilizzati**.


Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

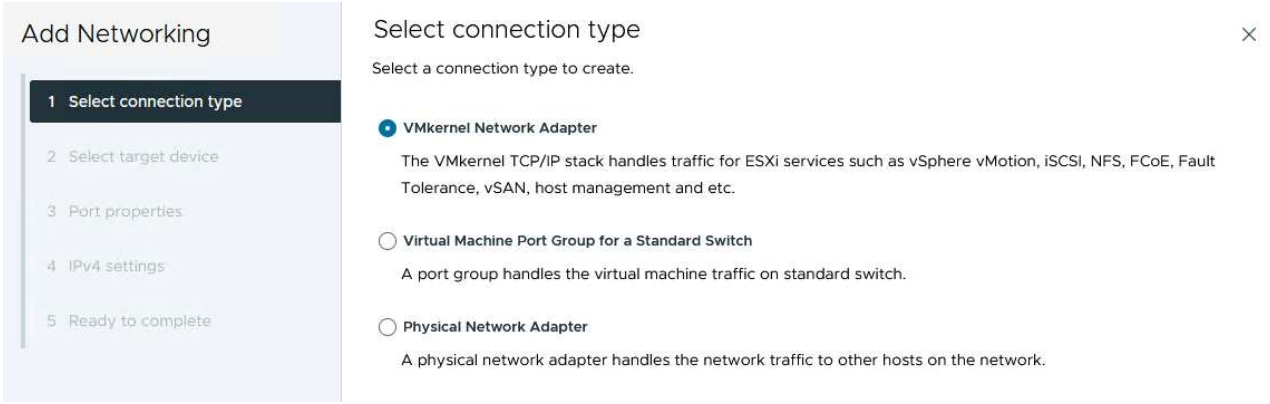
Creare adattatori VMkernel su ciascun host ESXi

Ripetere questo processo su ogni host ESXi nel dominio di gestione.

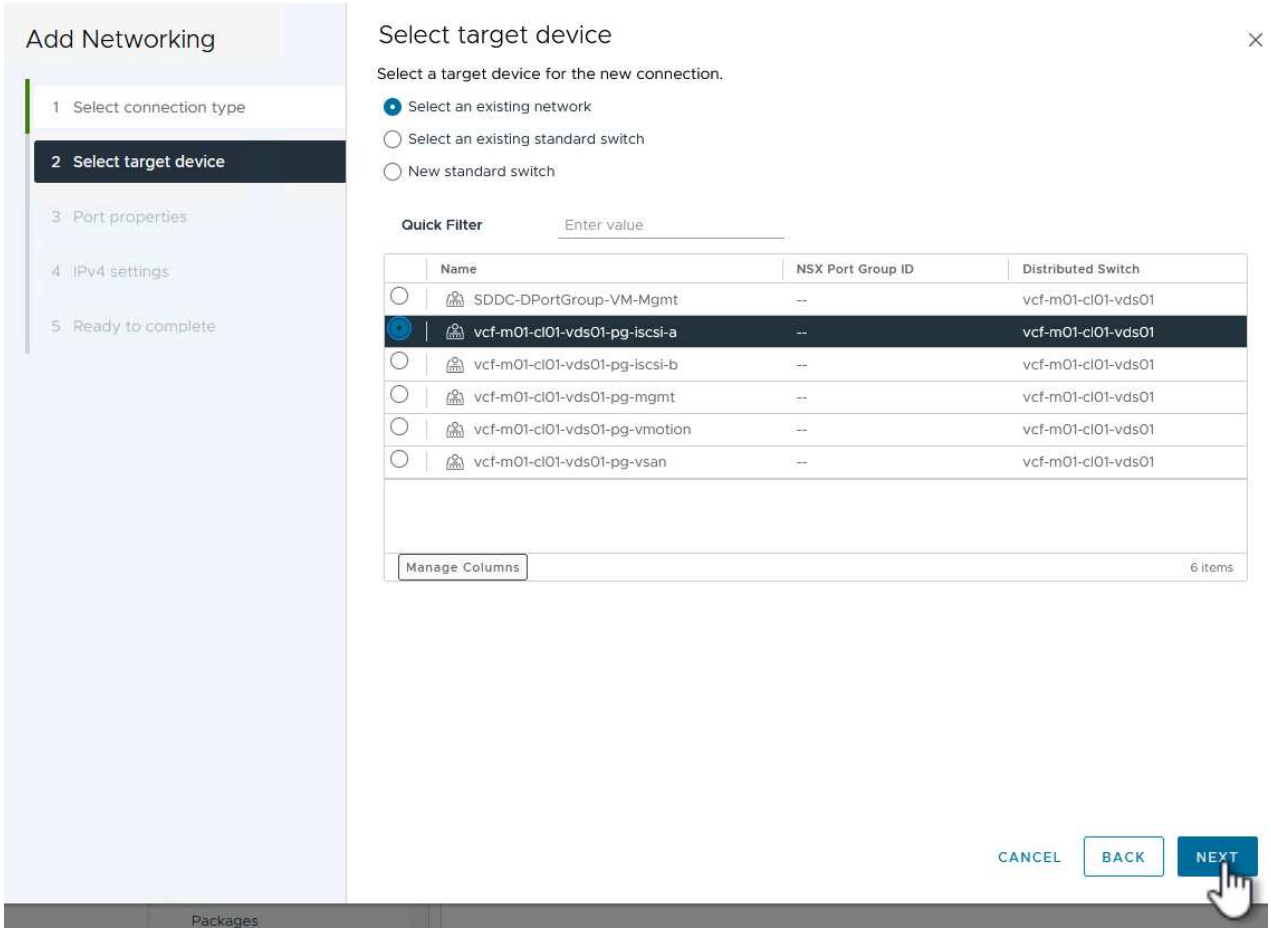
1. Dal client vSphere, accedere a uno degli host ESXi nell'inventario del dominio di gestione. Dalla scheda **Configure** selezionare **VMkernel adapters** e fare clic su **Add Networking…** per iniziare.



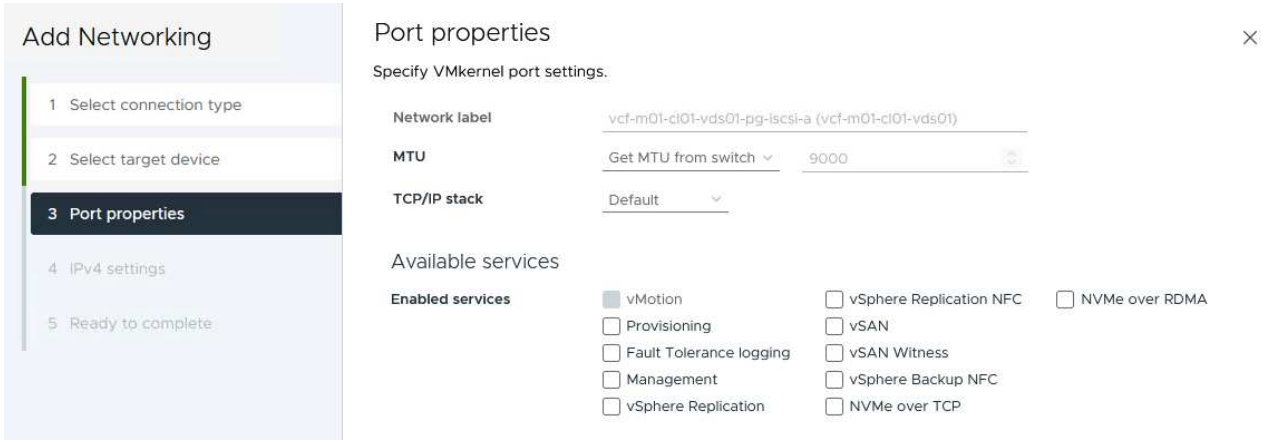
2. Nella finestra **Select Connection type** (Seleziona tipo di connessione), scegliere **VMkernel Network Adapter** (scheda di rete VMkernel) e fare clic su **Next** (Avanti) per continuare.



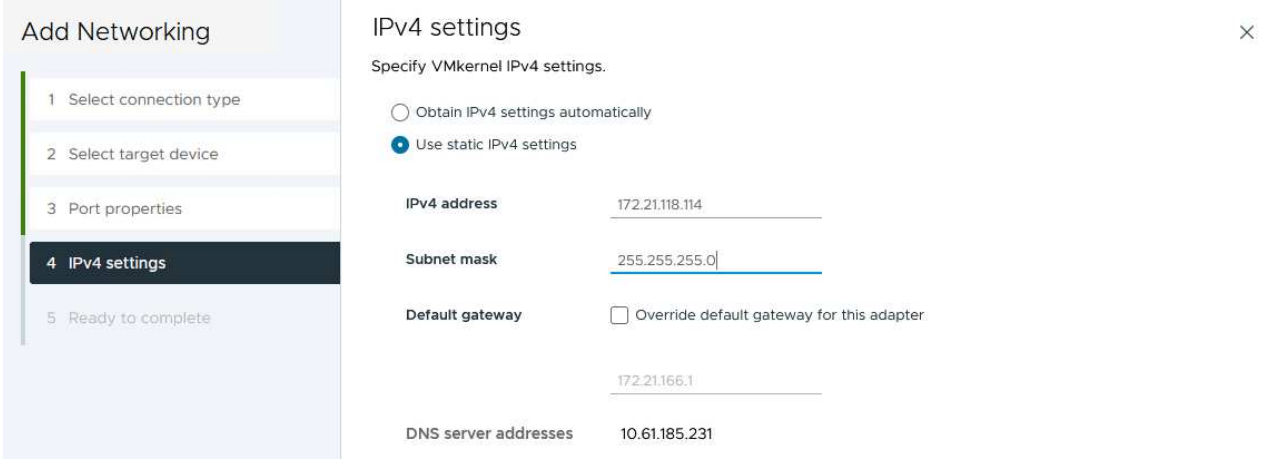
3. Nella pagina **Seleziona dispositivo di destinazione**, scegliere uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



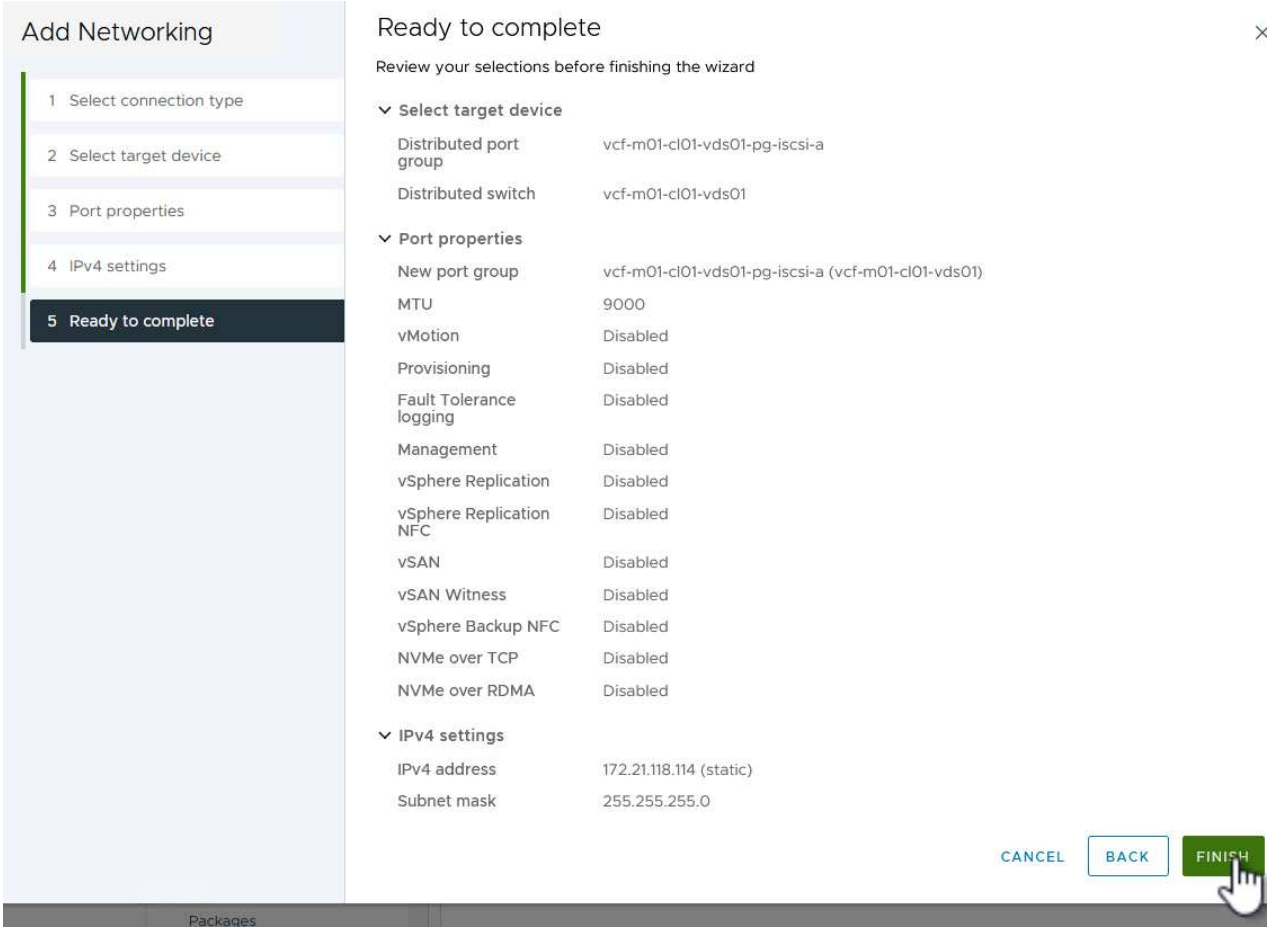
4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e fare clic su **Avanti** per continuare.



5. Nella pagina **IPv4 settings** compilare i campi **IP address**, **Subnet mask** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.



6. Rivedere le selezioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare l'adattatore VMkernel.



7. Ripetere questa procedura per creare un adattatore VMkernel per la seconda rete iSCSI.

Implementazione e utilizzo degli strumenti di ONTAP per configurare lo storage

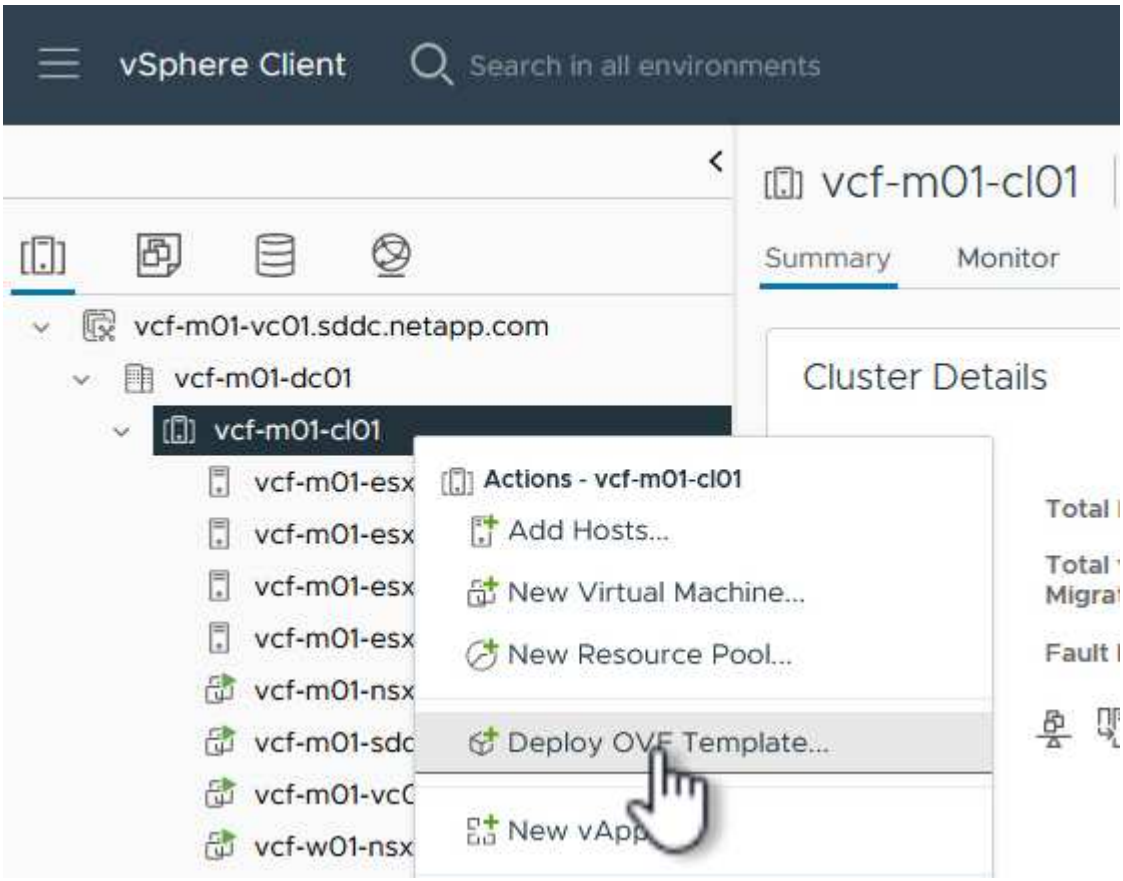
I seguenti passaggi vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere e prevedono la distribuzione di OTV, la creazione di un datastore iSCSI VMFS e la migrazione delle VM di gestione al nuovo datastore.

Implementa i tool ONTAP per VMware vSphere

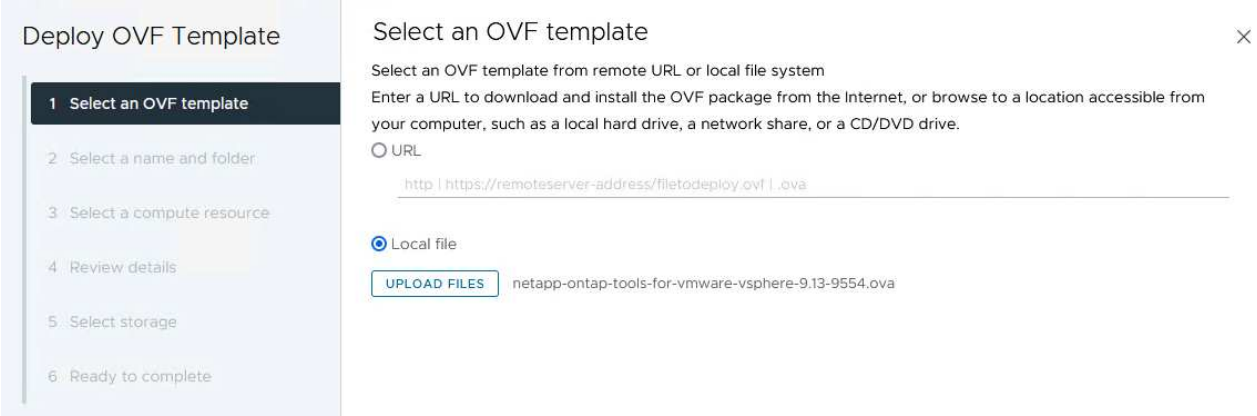
I tool ONTAP per VMware vSphere (OTV) vengono implementati come appliance delle macchine virtuali e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP.

Completa quanto segue per implementare i tool ONTAP per VMware vSphere:

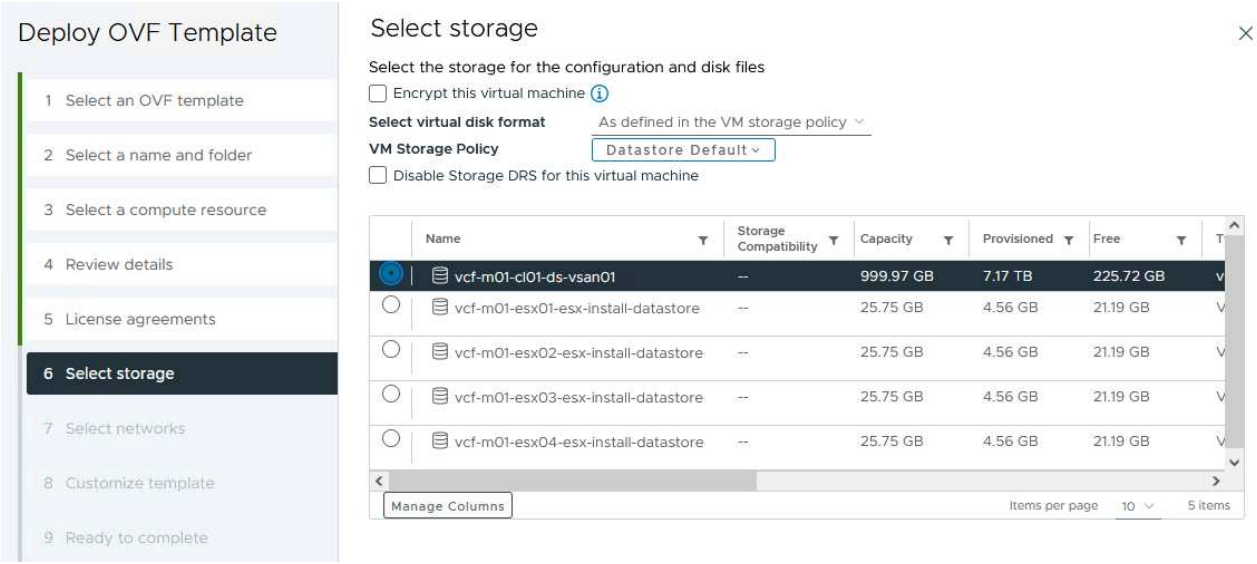
1. Ottenere l'immagine OVA degli strumenti ONTAP dal "Sito di supporto NetApp" e scaricarlo in una cartella locale.
2. Accedere all'appliance vCenter per il dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Deploy OVF Template…**



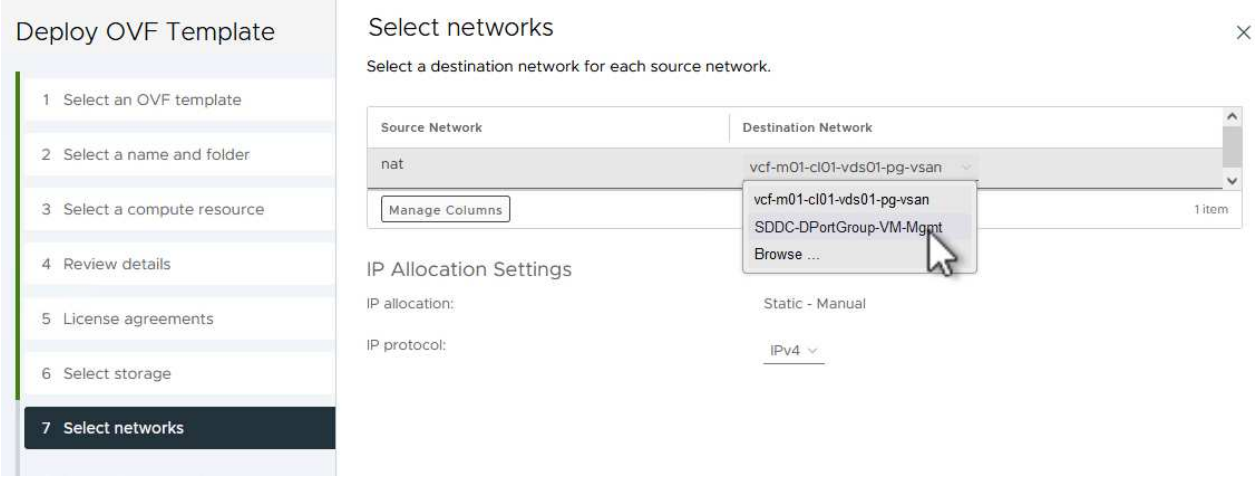
4. Nella procedura guidata **Deploy OVF Template** fare clic sul pulsante di opzione **file locale** e selezionare il file OVA di ONTAP Tools scaricato nel passaggio precedente.



5. Per i passaggi da 2 a 5 della procedura guidata, selezionare un nome e una cartella per la macchina virtuale, selezionare la risorsa di elaborazione, esaminare i dettagli e accettare il contratto di licenza.
6. Per la posizione di archiviazione dei file di configurazione e del disco, selezionare il datastore vSAN del cluster del dominio di gestione VCF.

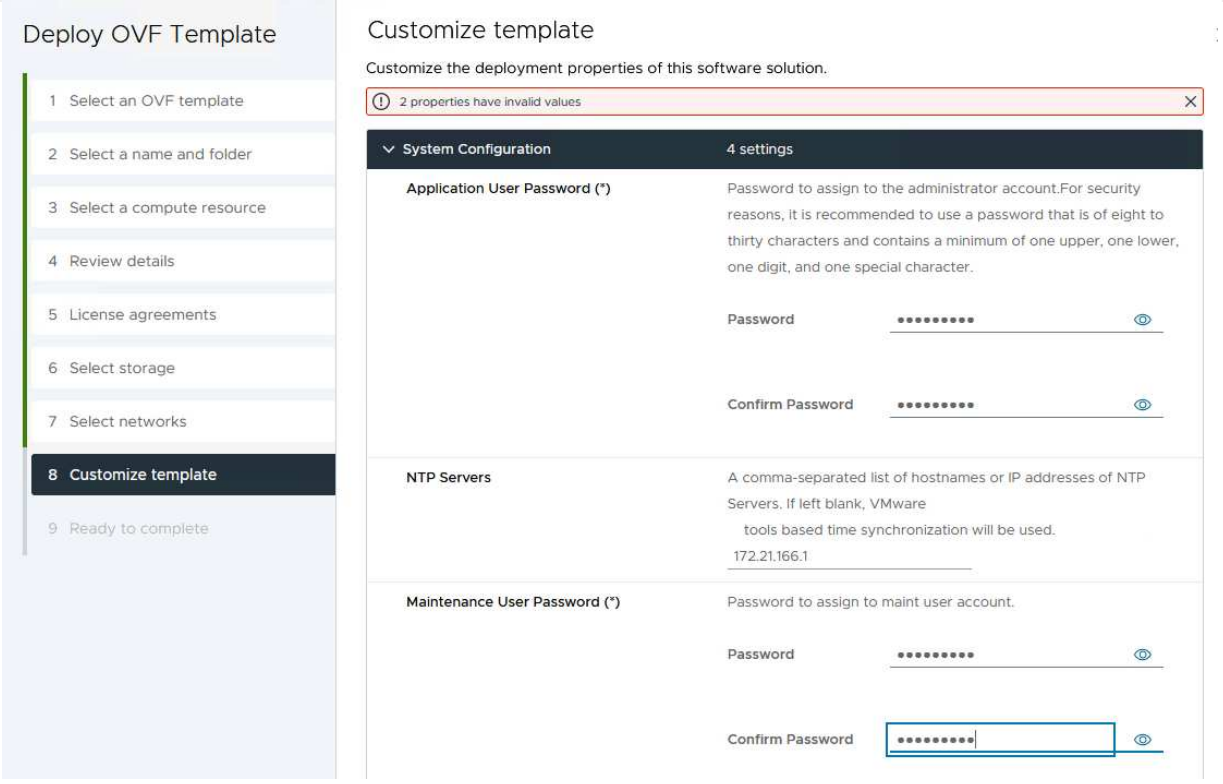


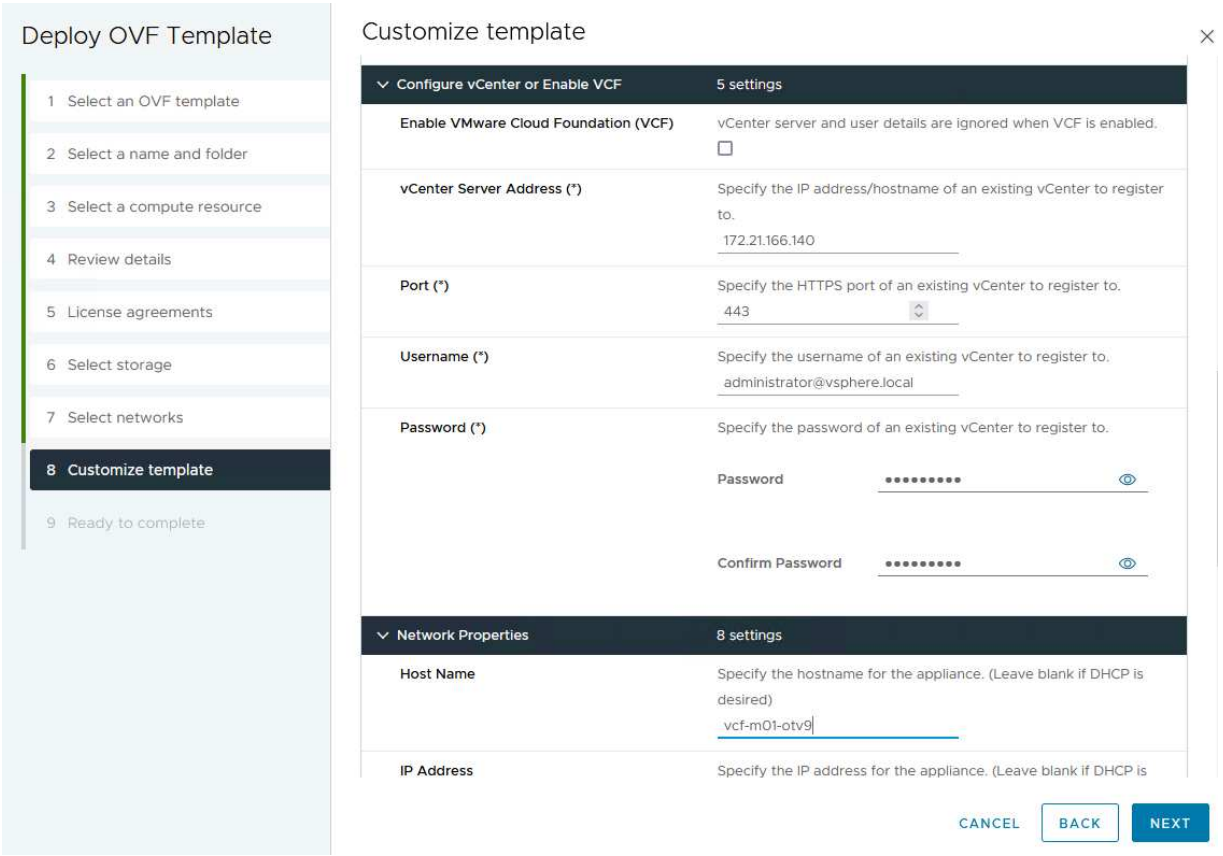
7. Nella pagina Seleziona rete, selezionare la rete utilizzata per la gestione del traffico.



8. Nella pagina Personalizza modello compilare tutte le informazioni richieste:
   - Password da utilizzare per l'accesso amministrativo a OTV.
   - Indirizzo IP del server NTP.
   - Password dell'account di manutenzione OTV.
   - Password DB Derby OTV.
   - Non selezionare la casella di controllo **Abilita VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire lo storage supplementare.
   - FQDN o indirizzo IP dell'appliance vCenter e fornire le credenziali per vCenter.
   - Specificare i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.



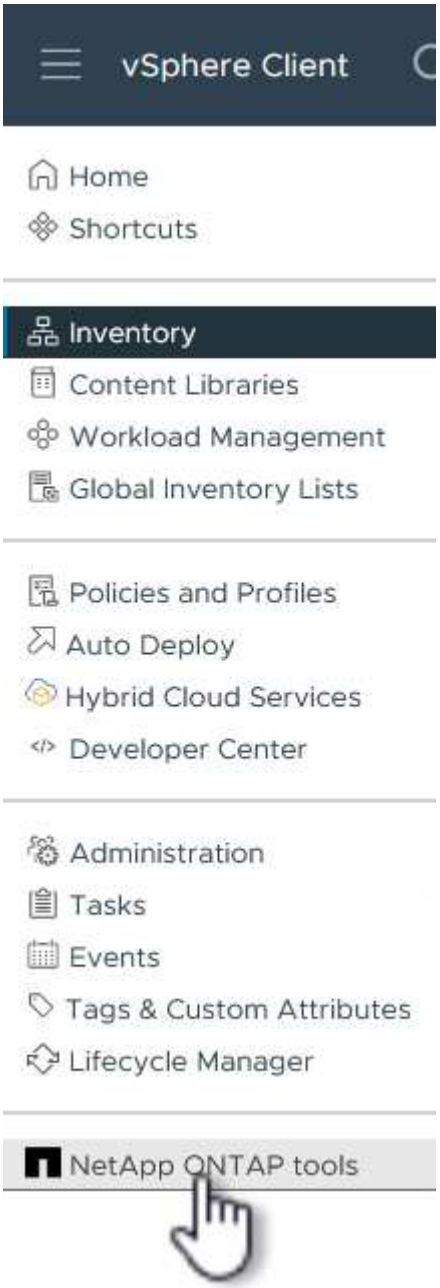


9. Leggere tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare a implementare l'apparecchio OTV.

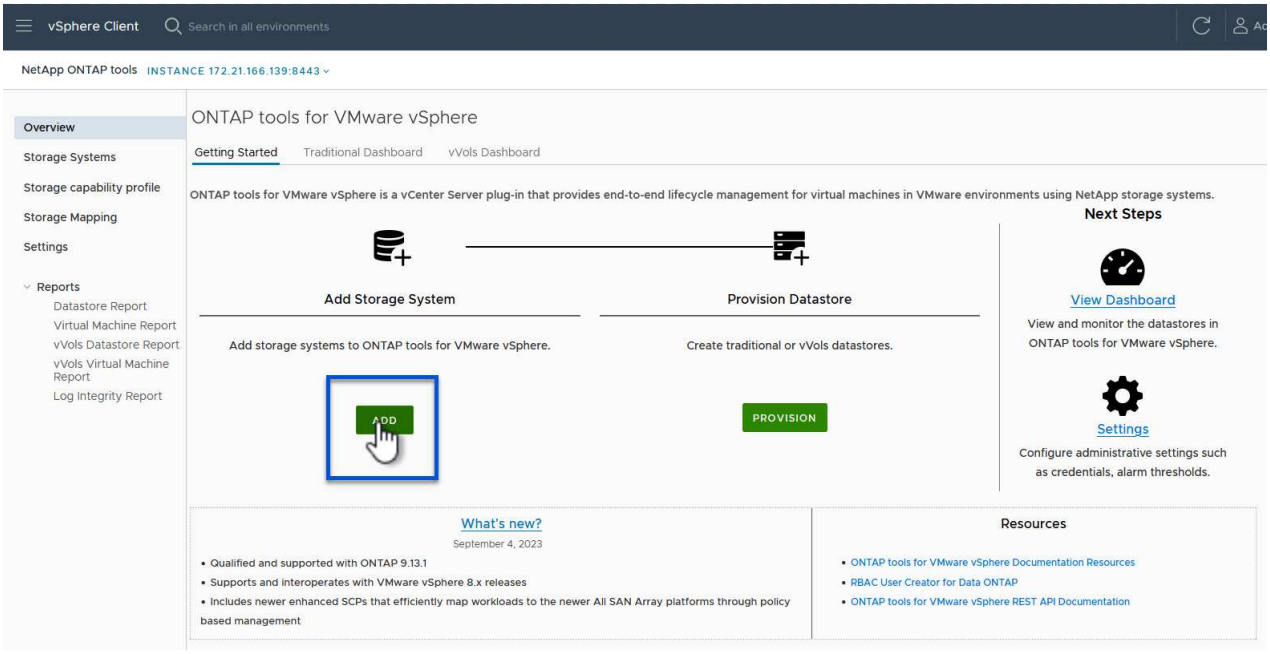
Configurare un datastore iSCSI VMFS sul dominio di gestione utilizzando OTV

Completare quanto segue per utilizzare OTV per configurare un datastore iSCSI VMFS come storage supplementare nel dominio di gestione:

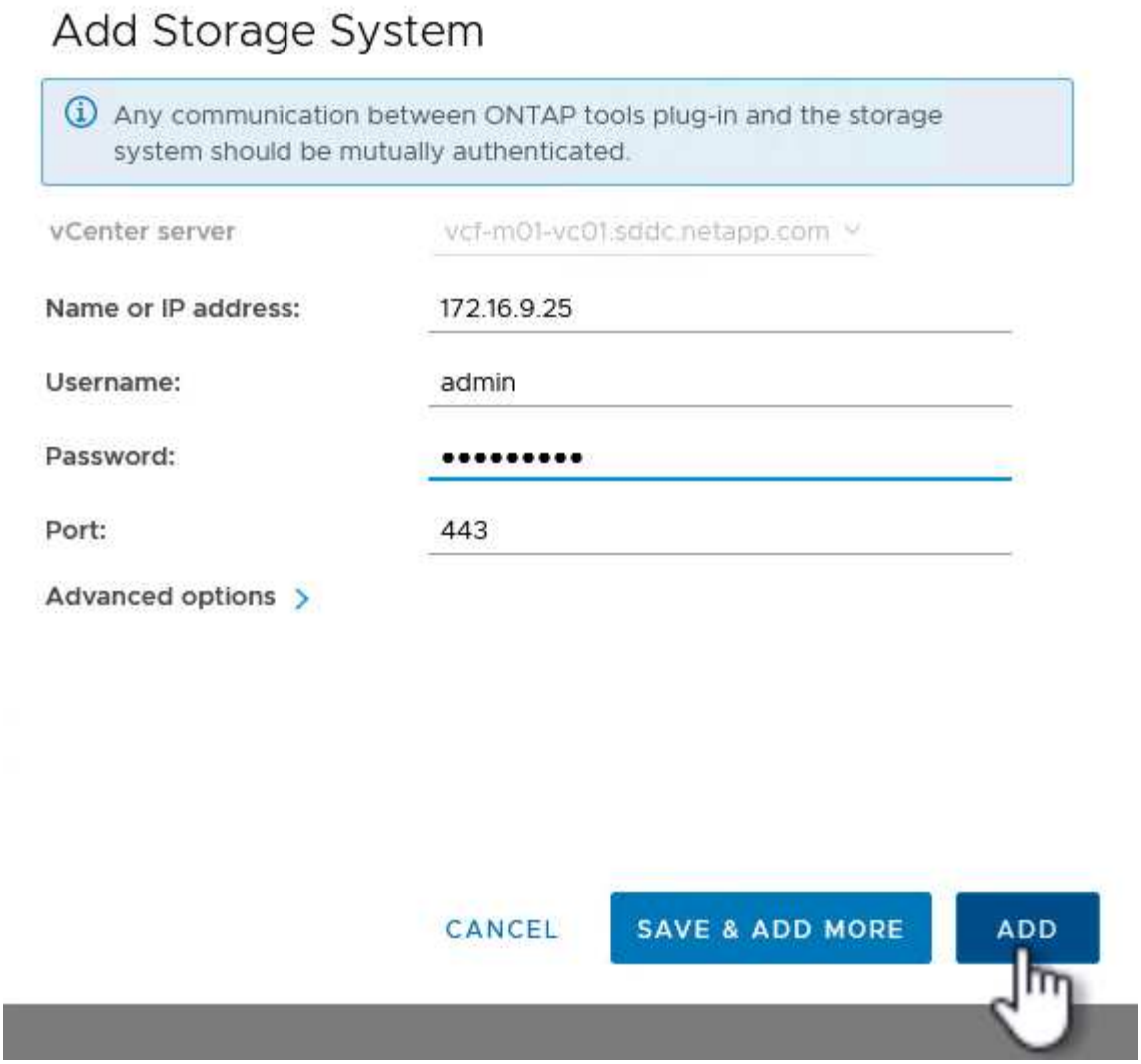
1. Nel client vSphere, accedere al menu principale e selezionare **Strumenti NetApp ONTAP**.



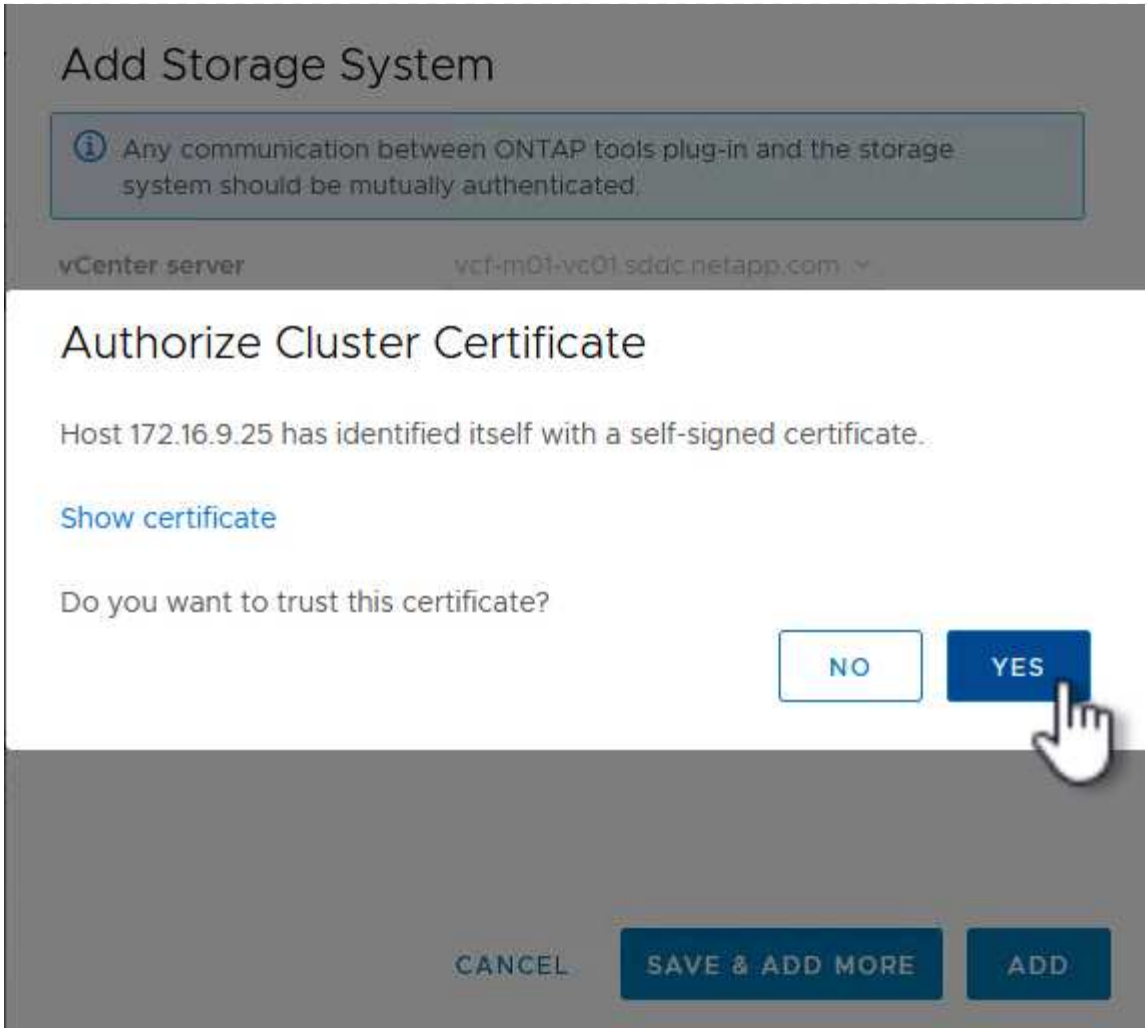
2. Una volta entrati in **Strumenti di ONTAP**, dalla pagina Guida introduttiva (o da **sistemi di archiviazione**), fare clic su **Aggiungi** per aggiungere un nuovo sistema di archiviazione.



3. Fornire l’indirizzo IP e le credenziali del sistema di archiviazione ONTAP e fare clic su **Aggiungi**.



4. Fare clic su **Sì** per autorizzare il certificato del cluster e aggiungere il sistema di archiviazione.

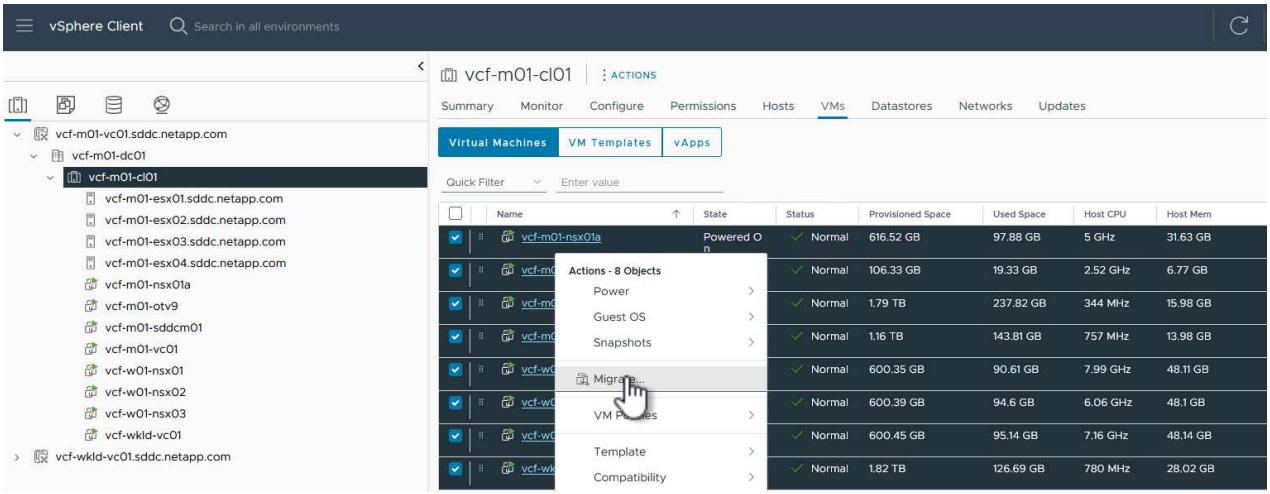

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
SAVE & ADD MORE
ADD

Migrazione di VM di gestione's al datastore iSCSI

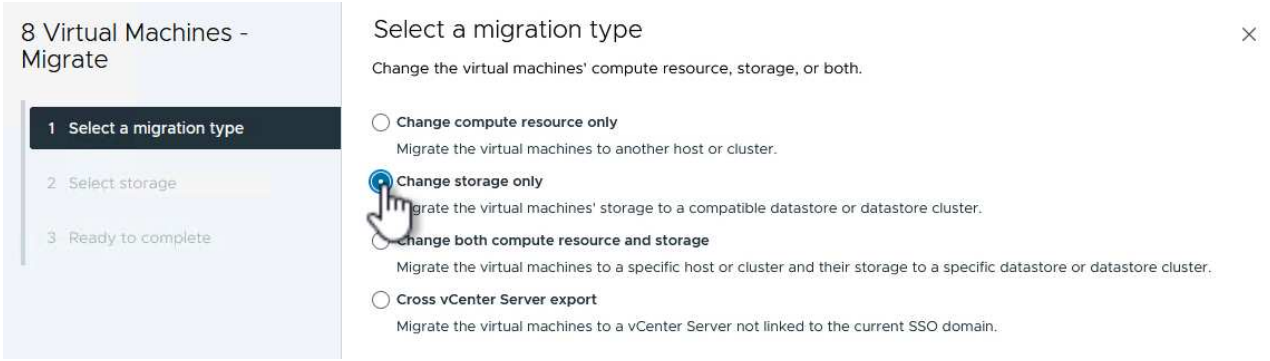
Nei casi in cui si preferisce utilizzare lo storage ONTAP per proteggere la VM di gestione VCF, vMotion può essere utilizzato per migrare la VM nel datastore iSCSI appena creato.

Completare i seguenti passaggi per migrare le VM di gestione VCF nel datastore iSCSI.

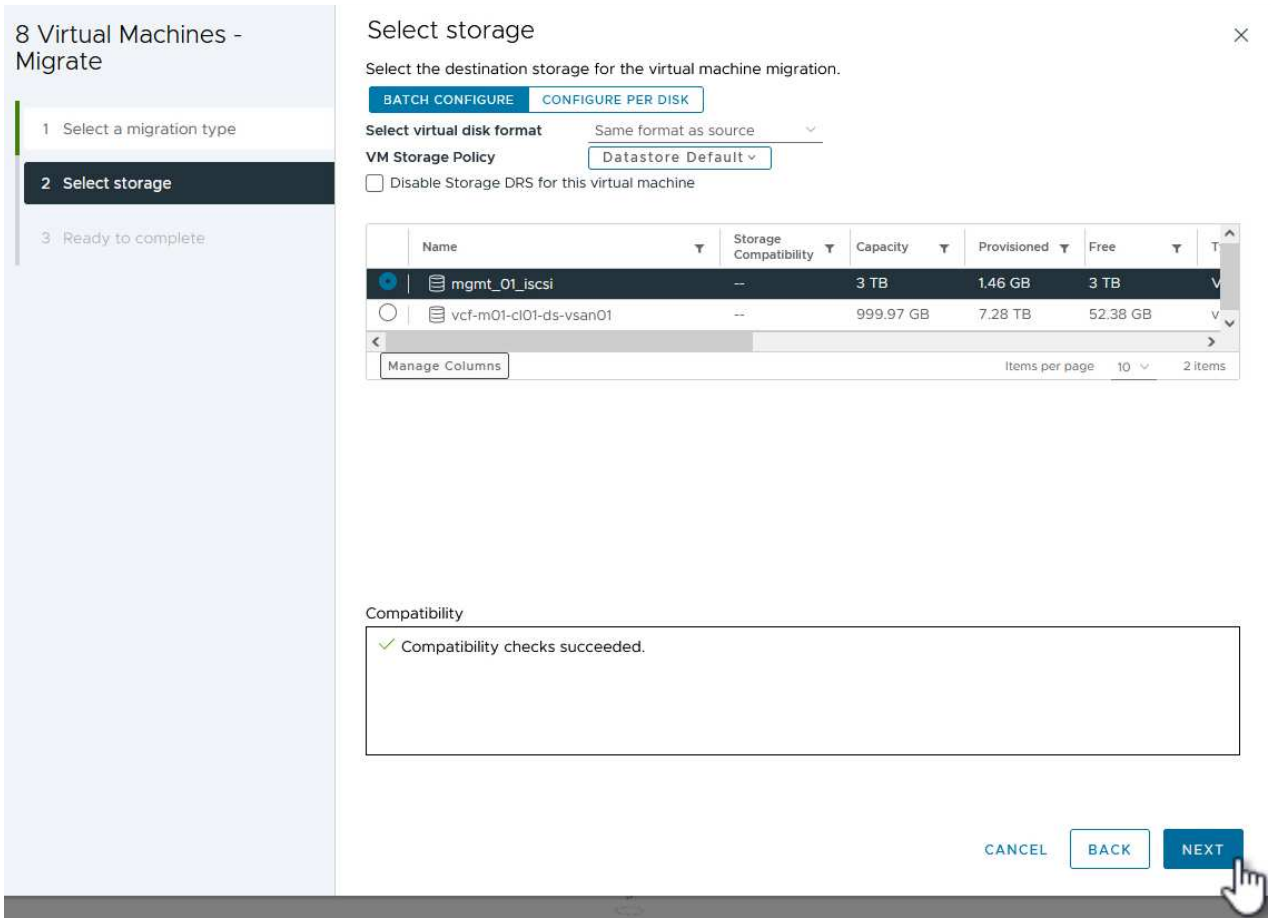
1. Dal client vSphere, passare al cluster del dominio di gestione e fare clic sulla scheda **VM**.
2. Selezionare le VM da migrare nel datastore iSCSI, fare clic con il pulsante destro del mouse e selezionare **Migrate...**.



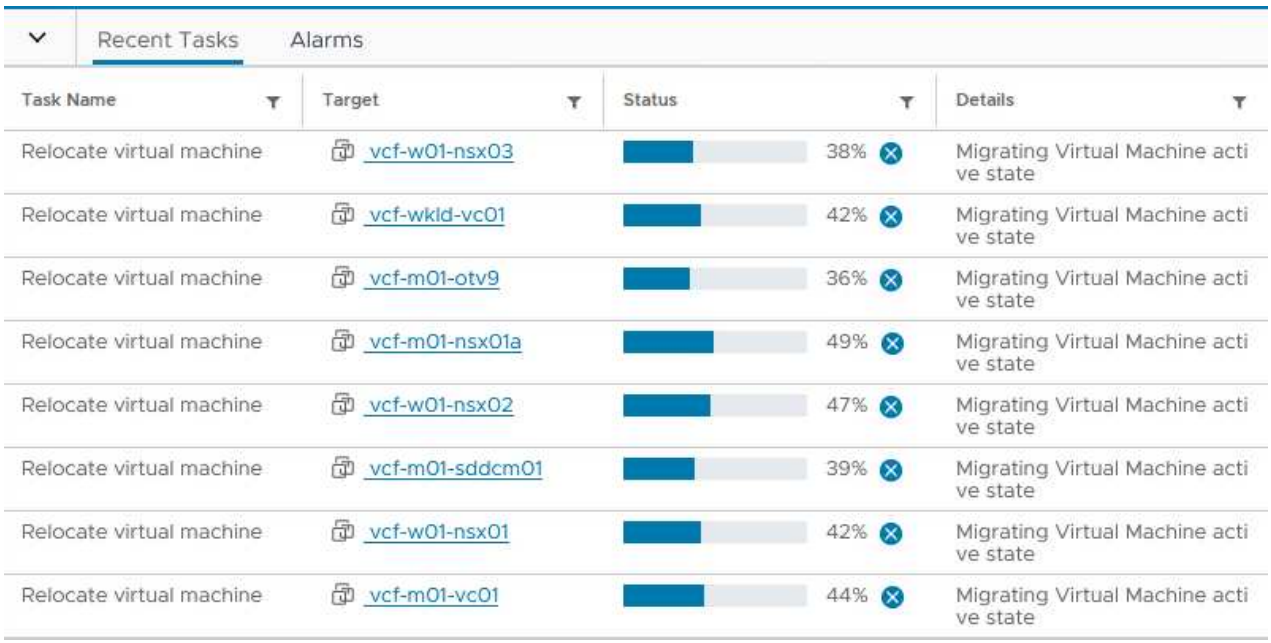
3. Nella procedura guidata **macchine virtuali - migrazione**, selezionare **Cambia solo archiviazione** come tipo di migrazione e fare clic su **Avanti** per continuare.



4. Nella pagina **Select storage** (Seleziona storage), selezionare il datastore iSCSI e selezionare **Next** (Avanti) per continuare.



5. Rivedere le selezioni e fare clic su **fine** per avviare la migrazione.
6. Lo stato di rilocazione può essere visualizzato dal riquadro **attività recenti**.



Ulteriori informazioni

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Video dimostrativo per questa soluzione

Archivi dati iSCSI come archiviazione supplementare per i domini di gestione VCF

Utilizzare gli strumenti di ONTAP per configurare l'archiviazione supplementare (vVol) per i domini del carico di lavoro VCF

In questo scenario verrà illustrato come distribuire e utilizzare ONTAP Tools per VMware vSphere per configurare un datastore **vVol** per un dominio del carico di lavoro VCF.

ISCSI viene utilizzato come protocollo storage per il datastore vVol.

Autore: Josh Powell

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

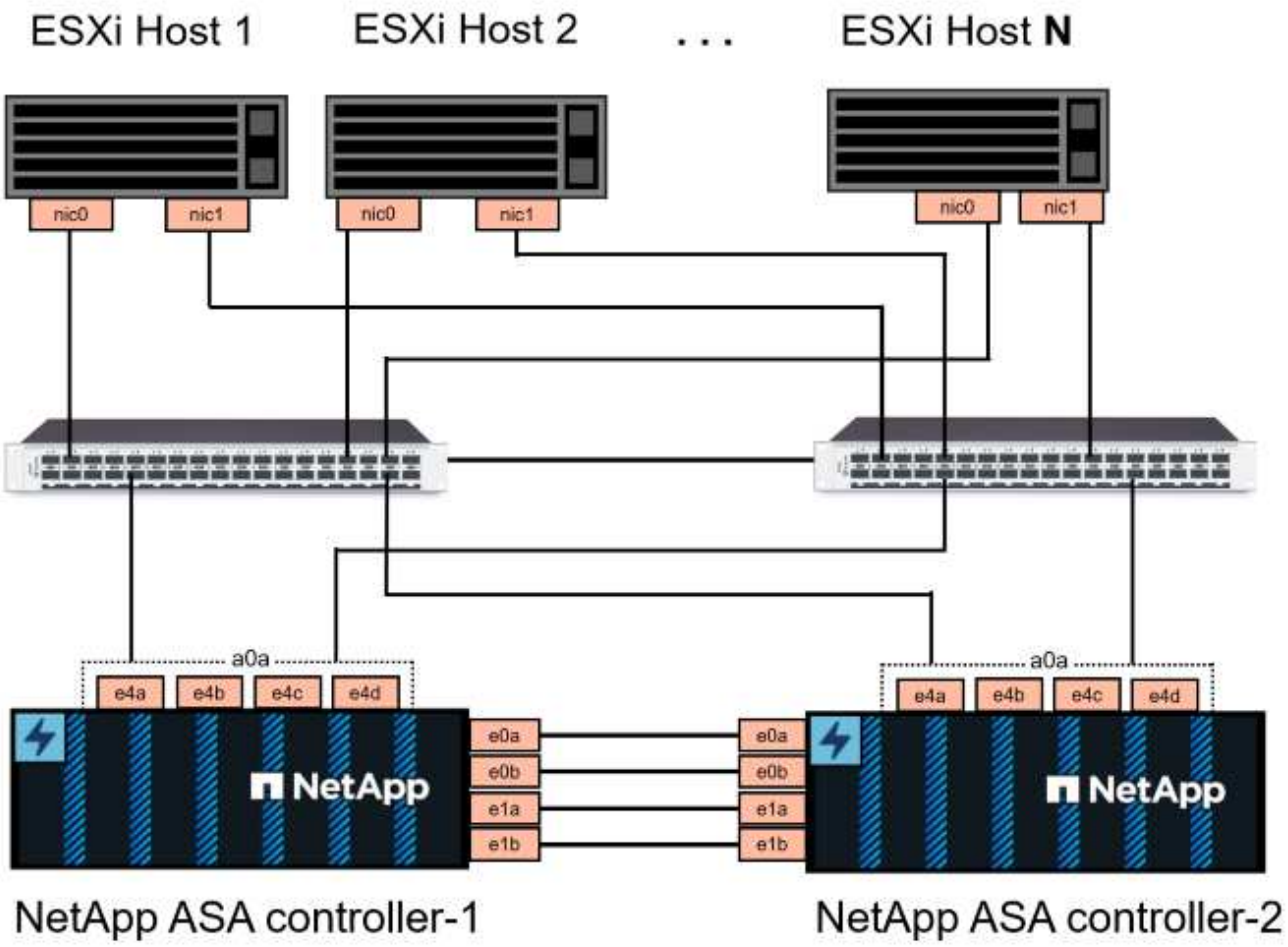
- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Distribuire gli strumenti ONTAP nel dominio del carico di lavoro VI.
- Creare un nuovo datastore vVol nel dominio del carico di lavoro VI.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con porte per dati fisici su switch ethernet dedicati al traffico di storage.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.

NetApp consiglia di progettare reti completamente ridondanti per iSCSI. Il diagramma seguente illustra un esempio di configurazione ridondante, che fornisce tolleranza agli errori per sistemi di archiviazione, switch, schede di rete e sistemi host. Consultare il NetApp "Riferimento alla configurazione SAN" per ulteriori informazioni.



Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti ethernet separate per tutte le SVM nelle configurazioni iSCSI.

Questa documentazione illustra il processo di creazione di una nuova SVM e specifica le informazioni dell'indirizzo IP per creare LIF multipli per il traffico iSCSI. Per aggiungere nuove LIF a una SVM esistente, fare riferimento a. "Creazione di una LIF (interfaccia di rete)".

> Nelle situazioni in cui più adattatori VMkernel sono configurati sulla stessa rete IP, si consiglia di utilizzare il binding della porta iSCSI del software sugli host ESXi per garantire che si verifichi il bilanciamento del carico tra le schede di rete. Fare riferimento all'articolo della KB "Considerazioni sull'utilizzo del binding della porta iSCSI del software in ESX/ESXi (2038869)".

Per ulteriori informazioni sull'utilizzo degli archivi dati iSCSI VMFS con VMware, fare riferimento a. "Datastore vSphere VMFS - backend storage iSCSI con ONTAP".

Fasi di implementazione

Per distribuire ONTAP Tools e utilizzarlo per creare un datastore vVol nel dominio di gestione VCF, completare i seguenti passaggi:

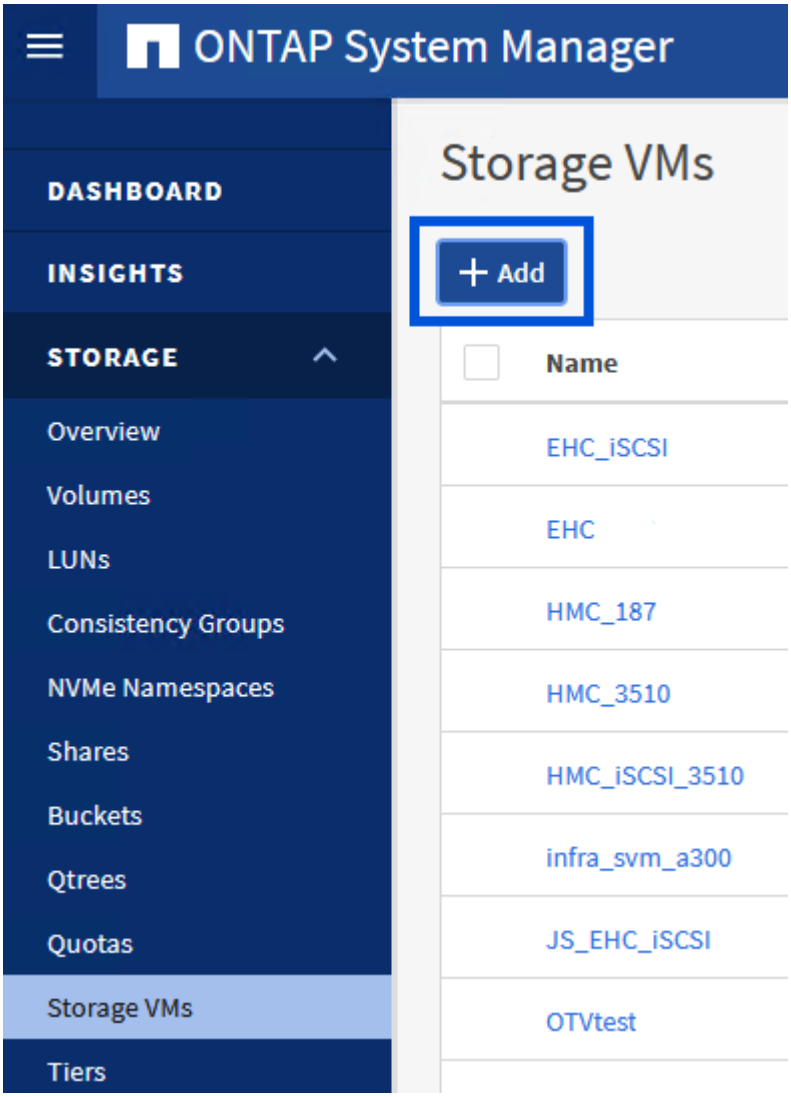
Crea SVM e LIF su un sistema storage ONTAP

Il passaggio seguente viene eseguito in Gestione di sistema di ONTAP.

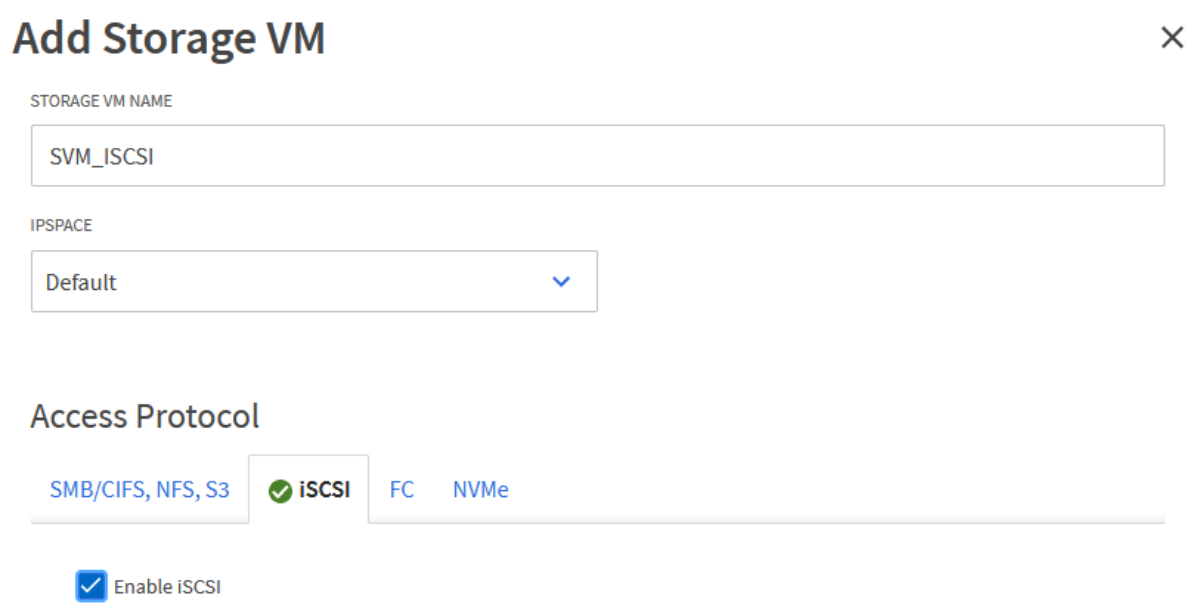
Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per il traffico iSCSI.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.

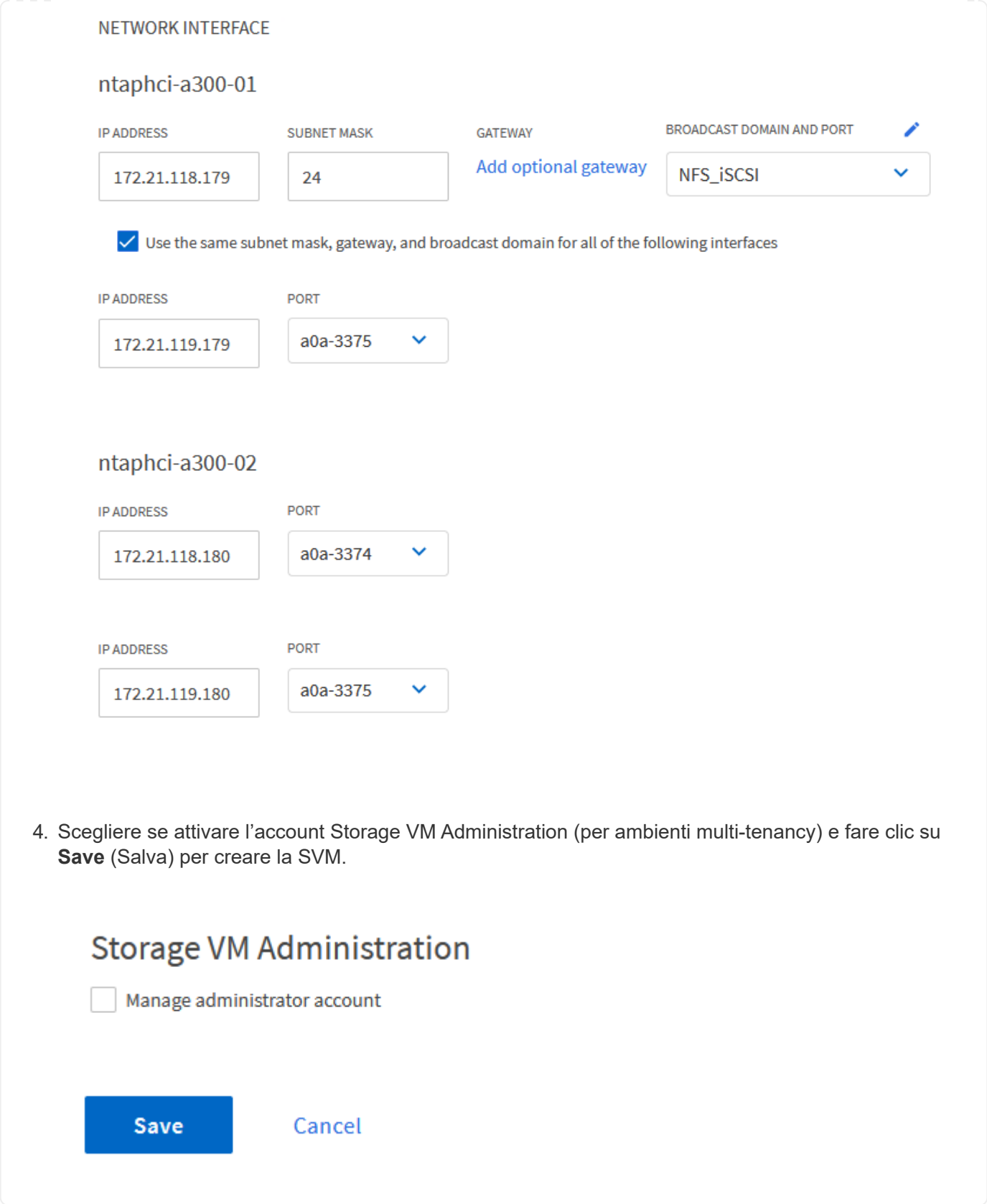


2. Nella procedura guidata **Add Storage VM** (Aggiungi VM di storage) specificare un **Name** (Nome) per la SVM, selezionare **IP Space** (spazio IP), quindi, in **Access Protocol** (protocollo di accesso), fare clic sulla scheda **iSCSI** e selezionare la casella **Enable iSCSI** (Abilita iSCSI*).



3. Nella sezione **interfaccia di rete** compilare i campi **indirizzo IP**, **Subnet Mask** e **Broadcast Domain and Port** per la prima LIF. Per LIF successive, la casella di controllo può essere abilitata per usare impostazioni comuni a tutte le LIF rimanenti o per usare impostazioni separate.

> Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti Ethernet separate per tutte le SVM nelle configurazioni iSCSI.



4. Scegliere se attivare l'account Storage VM Administration (per ambienti multi-tenancy) e fare clic su **Save** (Salva) per creare la SVM.

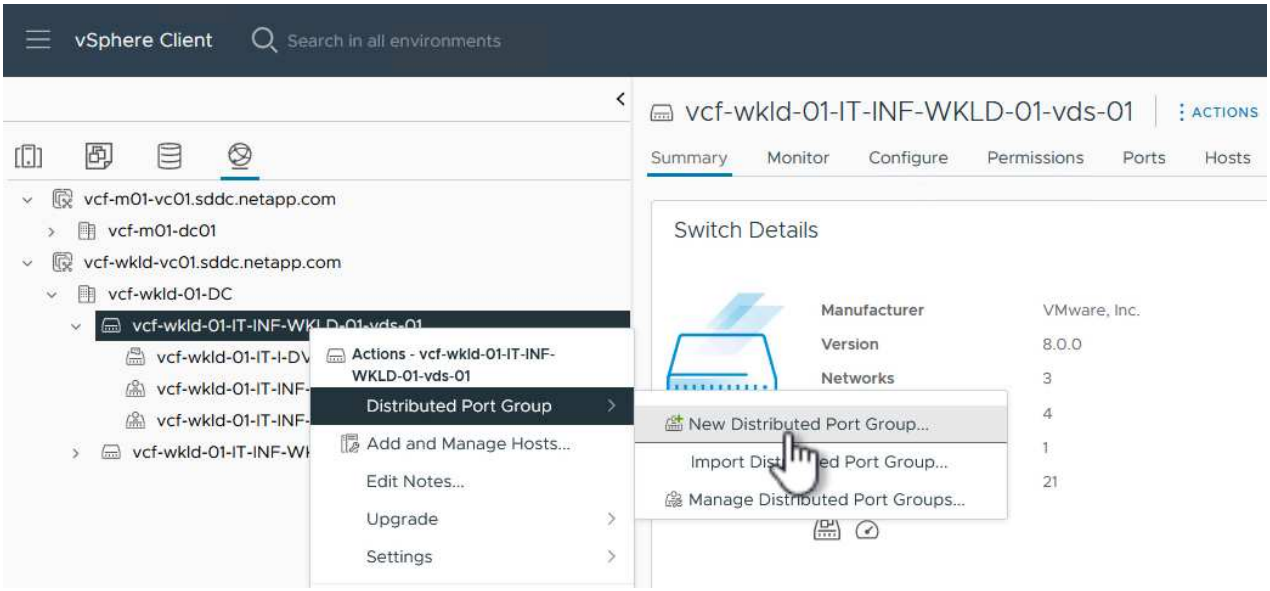
Configurare il networking per iSCSI sugli host ESXi

I seguenti passaggi vengono eseguiti sul cluster VI workload Domain utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-on, pertanto il client vSphere è comune nei domini di gestione e carico di lavoro.

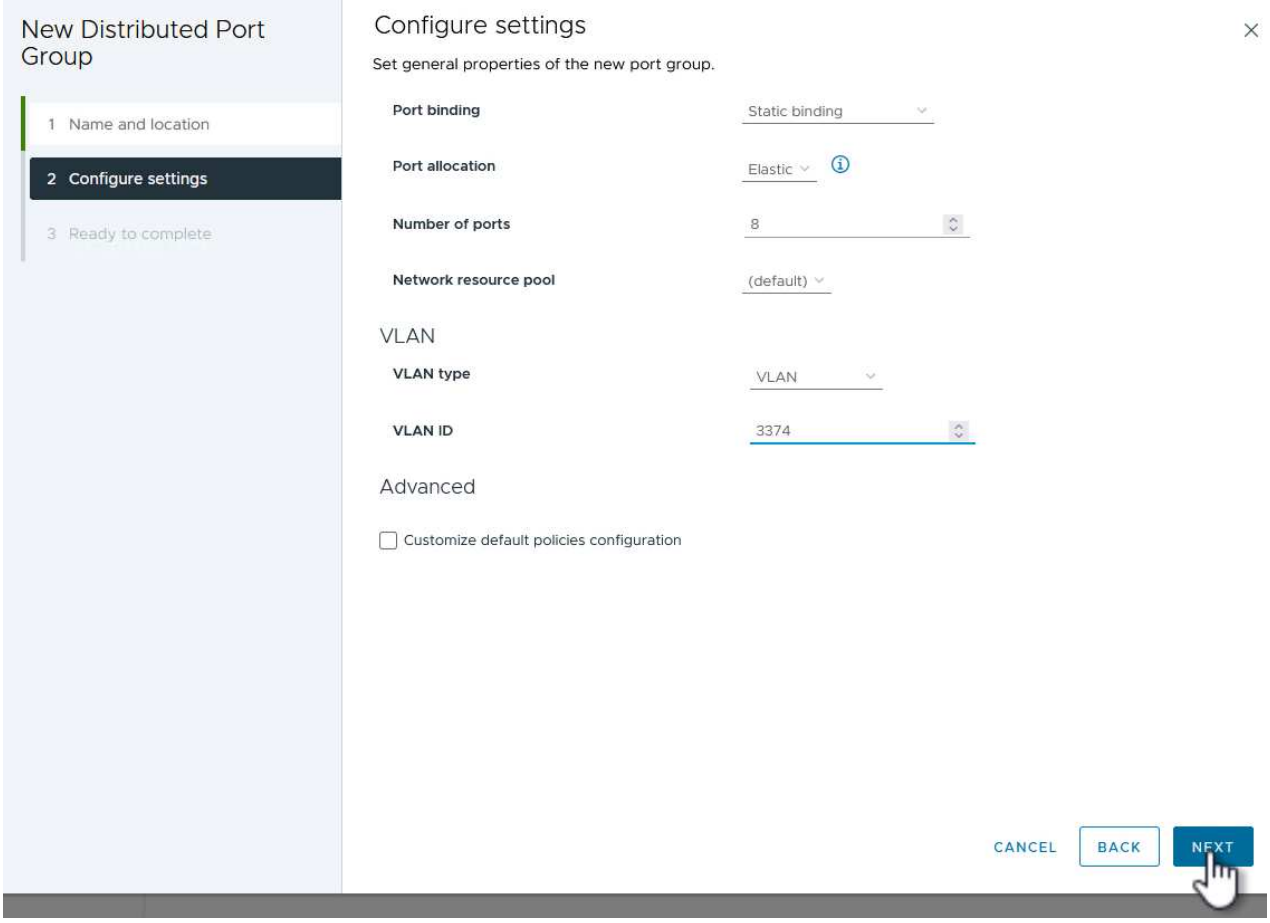
Creare gruppi di porte distribuite per il traffico iSCSI

Completare quanto segue per creare un nuovo gruppo di porte distribuite per ogni rete iSCSI:

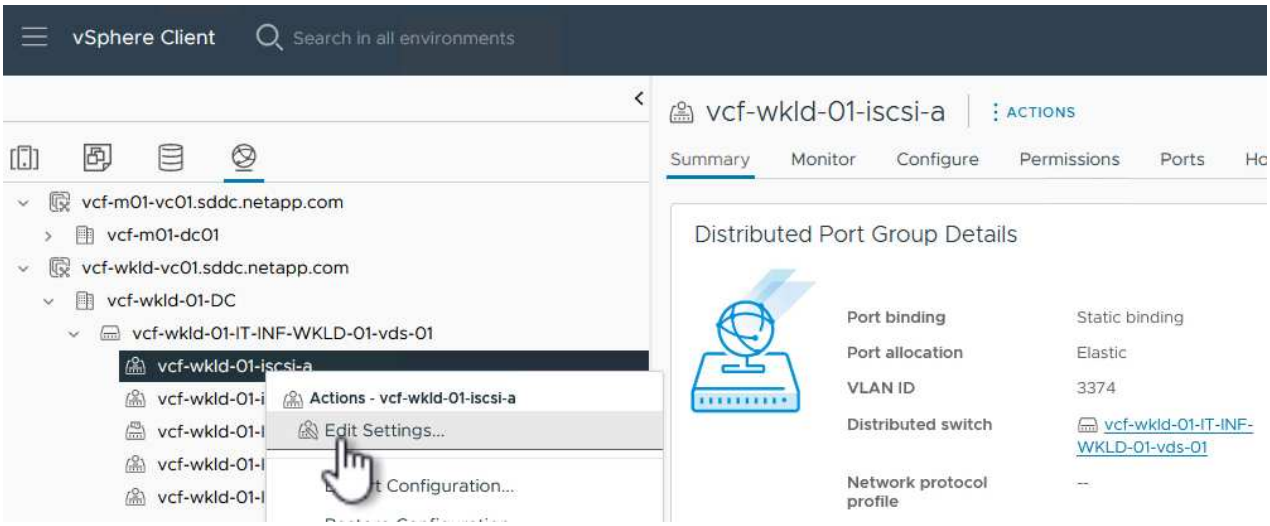
1. Dal client vSphere , accedere a **Inventory > Networking** per il dominio del carico di lavoro. Passare allo Switch distribuito esistente e scegliere l'azione da creare **nuovo Gruppo di porte distribuite…**.



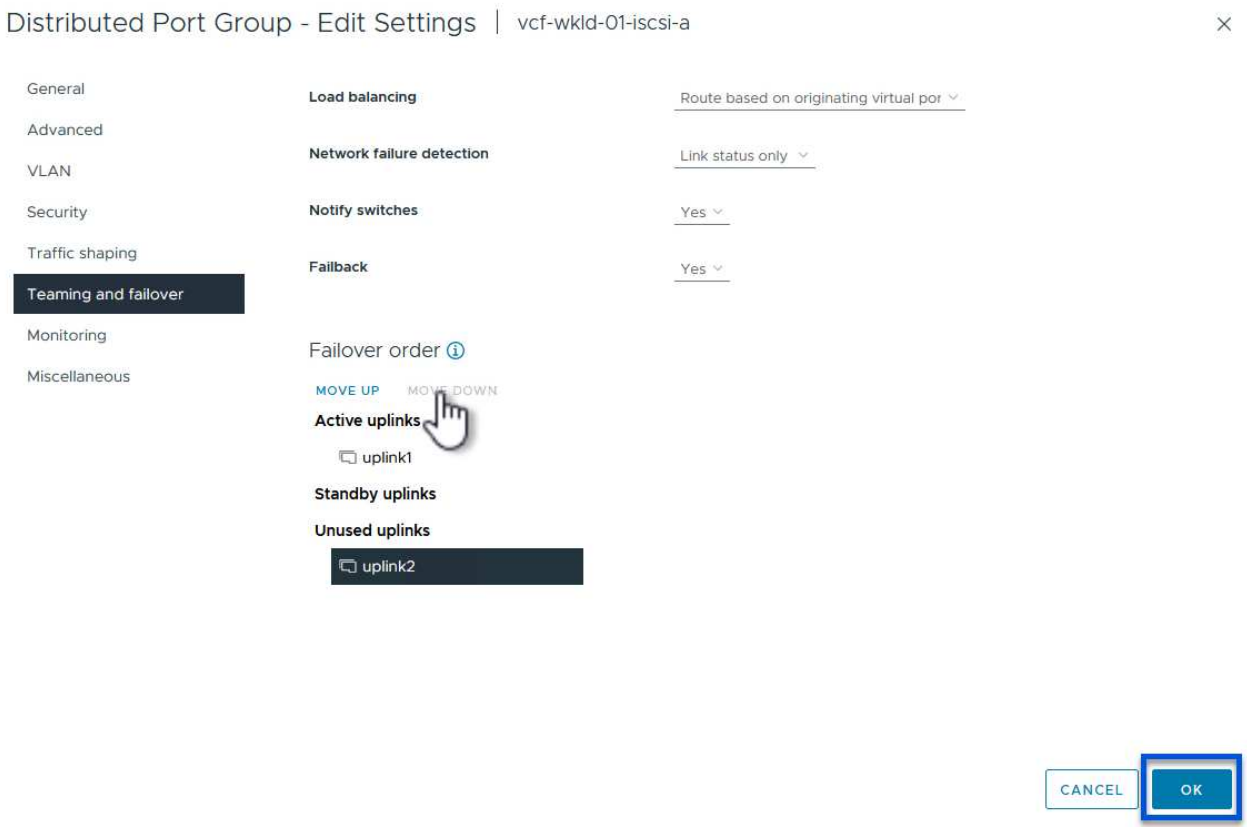
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare clic su **Avanti** per continuare.



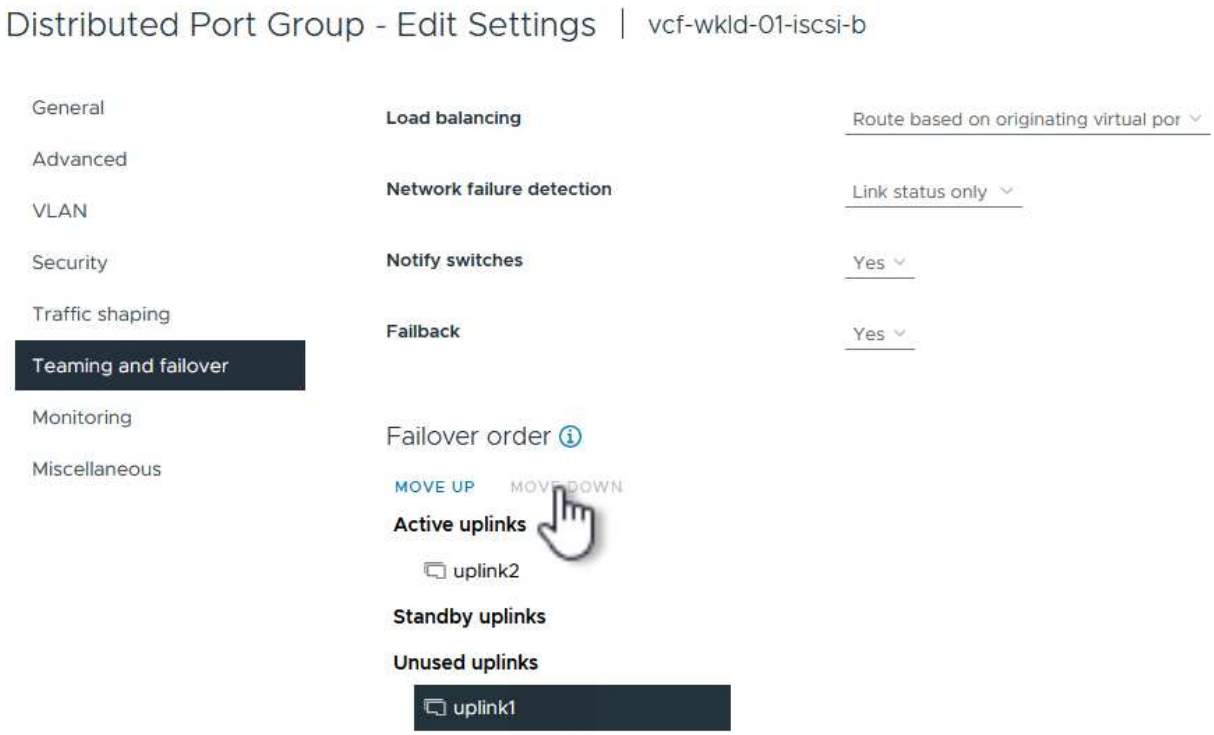
4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **fine** per creare il nuovo gruppo di porte distribuite.
5. Ripetere questa procedura per creare un gruppo di porte distribuite per la seconda rete iSCSI utilizzata e assicurarsi di aver immesso l'ID **VLAN** corretto.
6. Una volta creati entrambi i gruppi di porte, accedere al primo gruppo di porte e selezionare l'azione **Modifica impostazioni…**.



7. Nella pagina **Gruppo porte distribuite - Modifica impostazioni**, accedere a **Teaming and failover** nel menu a sinistra e fare clic su **uplink2** per spostarlo in basso in **uplink non utilizzati**.



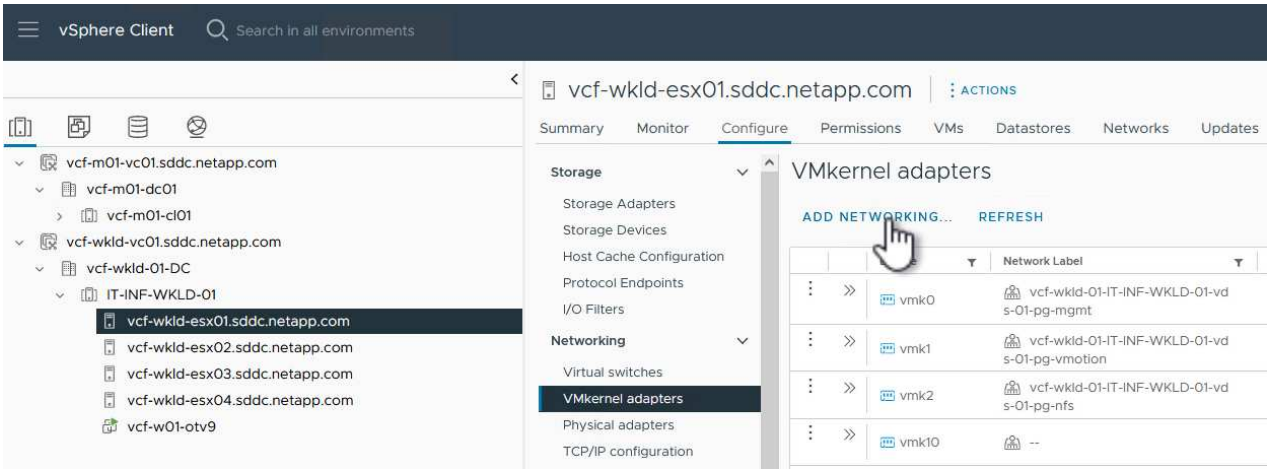
8. Ripetere questo passaggio per il secondo gruppo di porte iSCSI. Tuttavia, questa volta si sposta **uplink1** verso il basso in **uplink non utilizzati**.



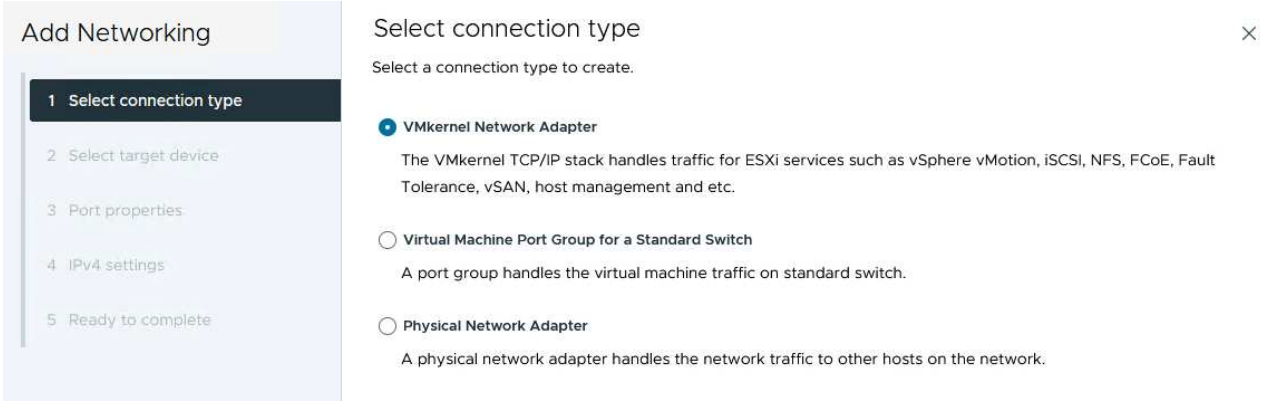
Creare adattatori VMkernel su ciascun host ESXi

Ripetere questo processo su ogni host ESXi nel dominio del carico di lavoro.

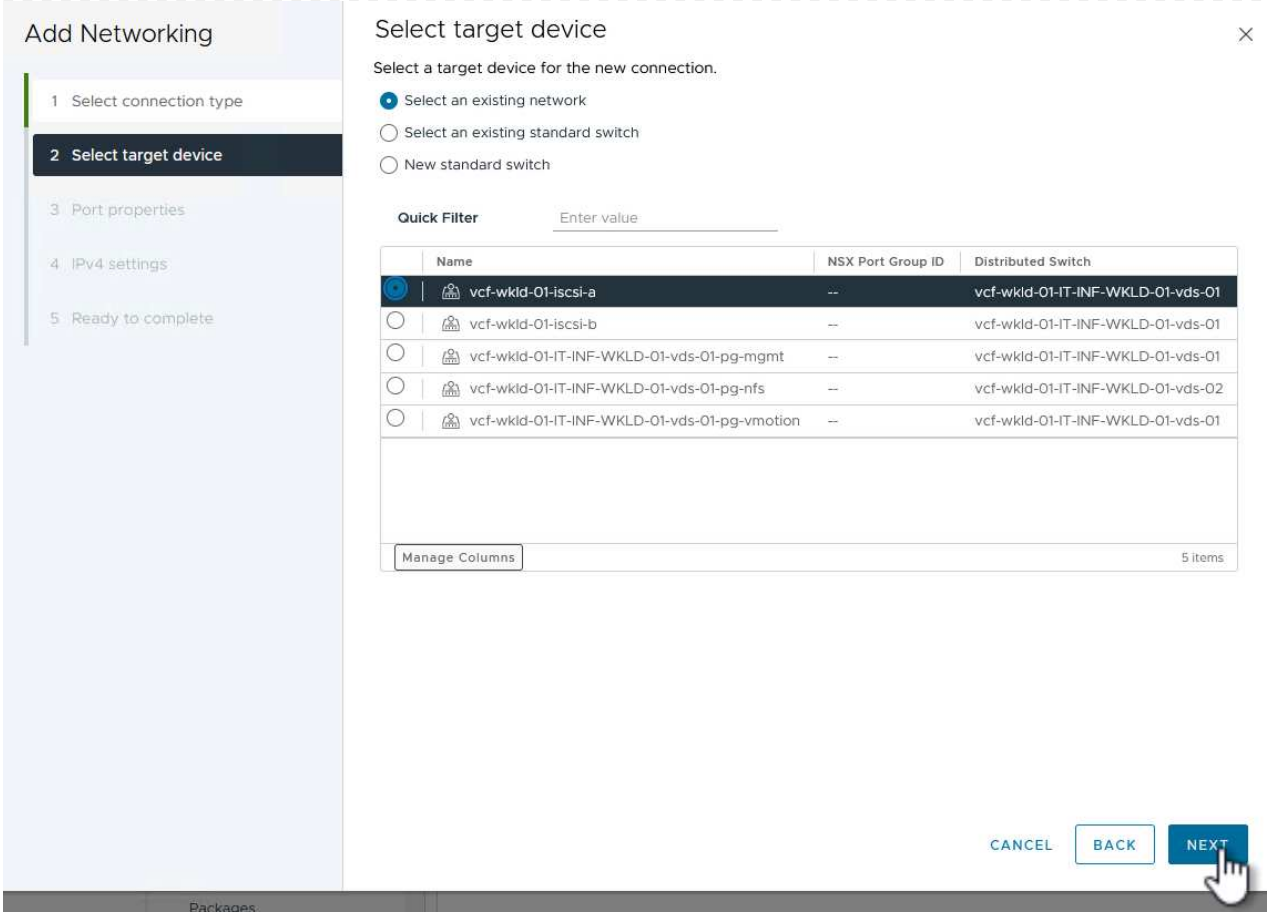
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configure** selezionare **VMkernel adapters** e fare clic su **Add Networking…** per iniziare.



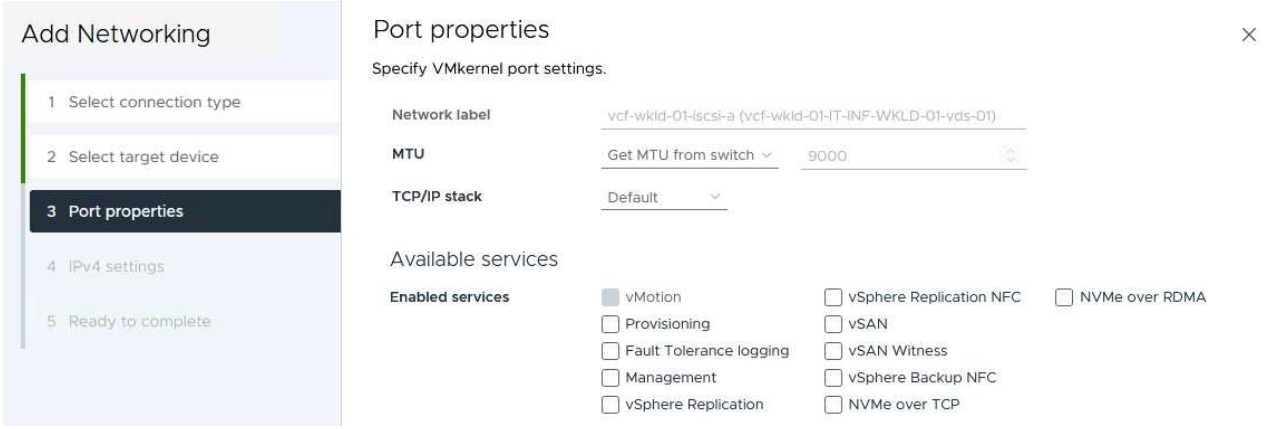
2. Nella finestra **Select Connection type** (Seleziona tipo di connessione), scegliere **VMkernel Network Adapter** (scheda di rete VMkernel) e fare clic su **Next** (Avanti) per continuare.



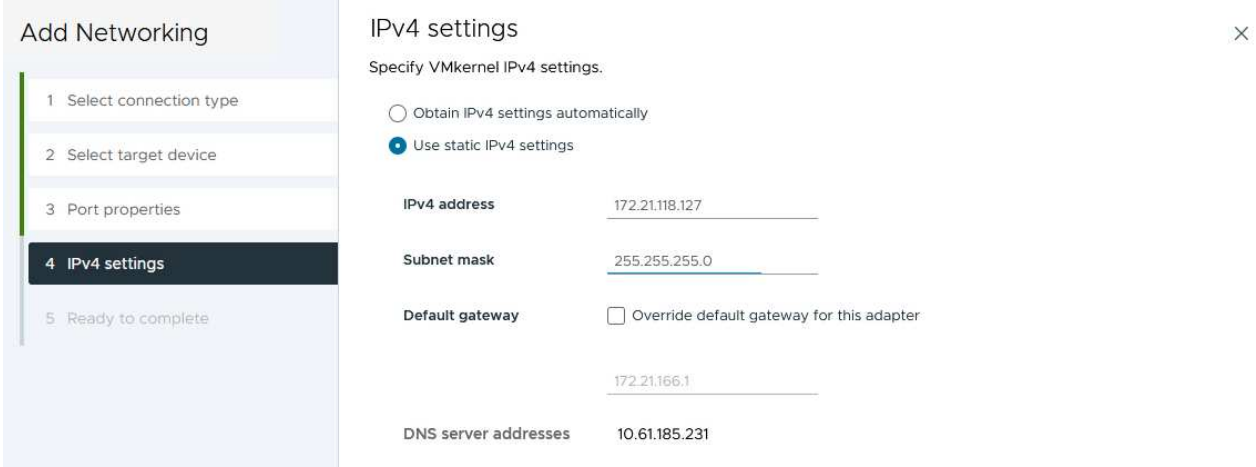
3. Nella pagina **Seleziona dispositivo di destinazione**, scegliere uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



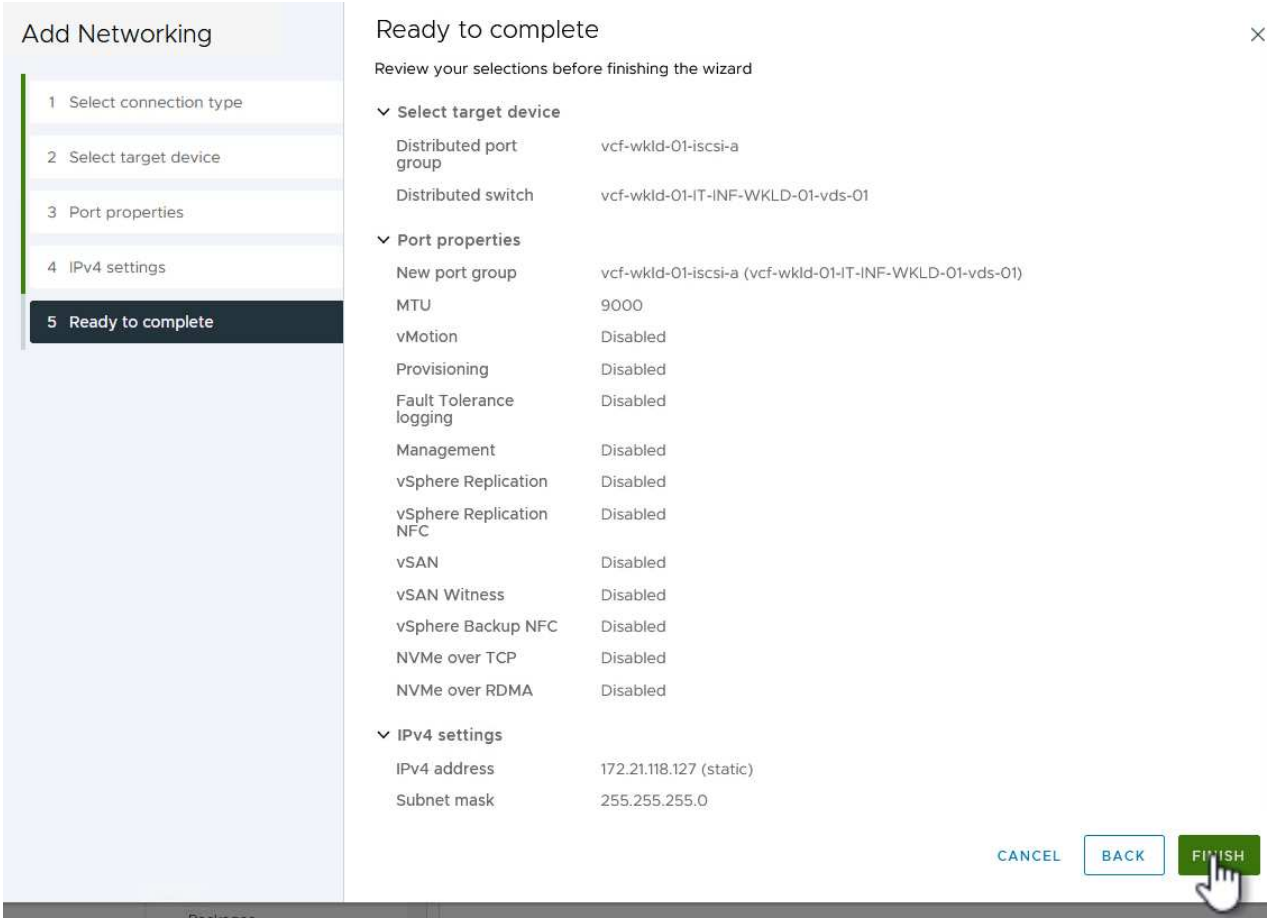
4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e fare clic su **Avanti** per continuare.



5. Nella pagina **IPv4 settings** compilare i campi **IP address**, **Subnet mask** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.



6. Rivedere le selezioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare l'adattatore VMkernel.



7. Ripetere questa procedura per creare un adattatore VMkernel per la seconda rete iSCSI.

Implementazione e utilizzo degli strumenti di ONTAP per configurare lo storage

I seguenti passaggi vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere e prevedono la distribuzione di strumenti ONTAP, la creazione di un datastore iSCSI vVol e la migrazione delle VM di gestione al nuovo datastore.

Per i domini del carico di lavoro VI, ONTAP Tools viene installato nel cluster di gestione VCF ma registrato con vCenter associato al dominio del carico di lavoro VI.

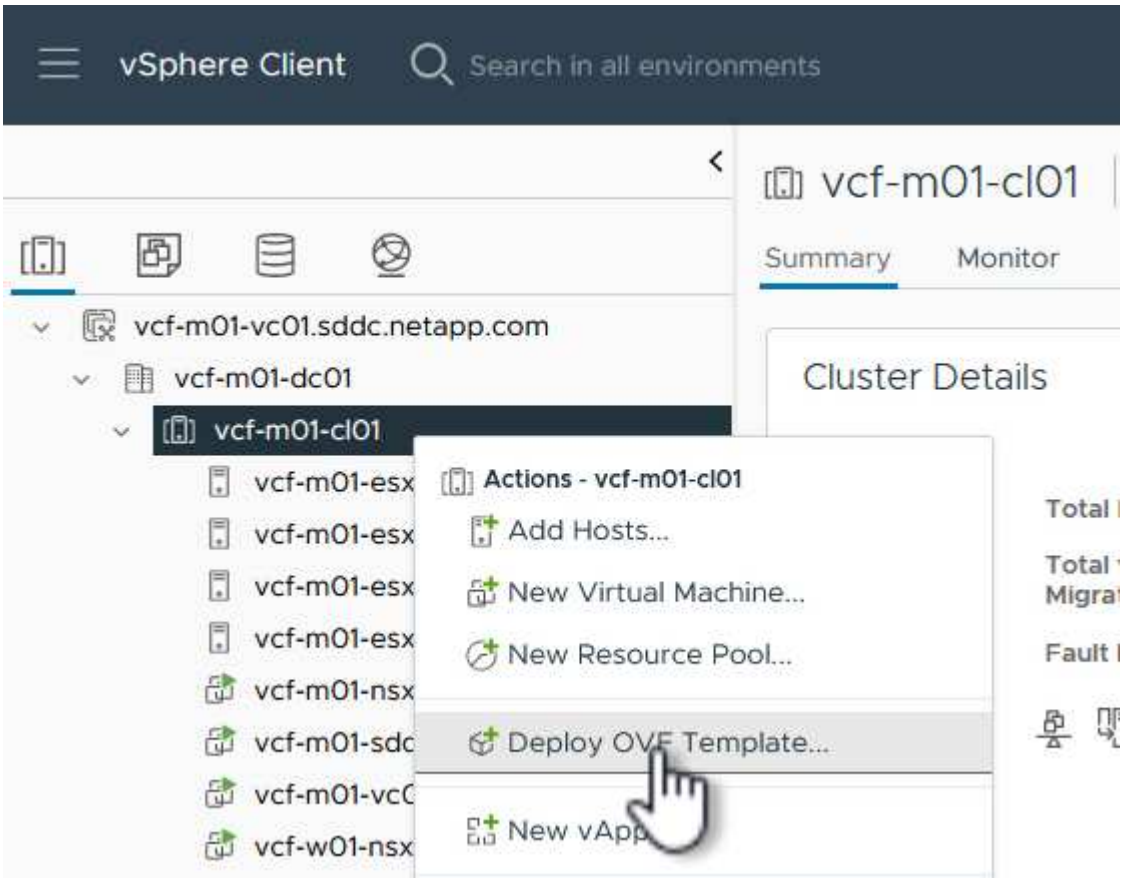
Per ulteriori informazioni sulla distribuzione e l'utilizzo degli strumenti ONTAP in un ambiente vCenter multiplo, fare riferimento a. "Requisiti per la registrazione degli strumenti ONTAP in più ambienti vCenter Server".

Implementa i tool ONTAP per VMware vSphere

I tool ONTAP per VMware vSphere vengono implementati come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP.

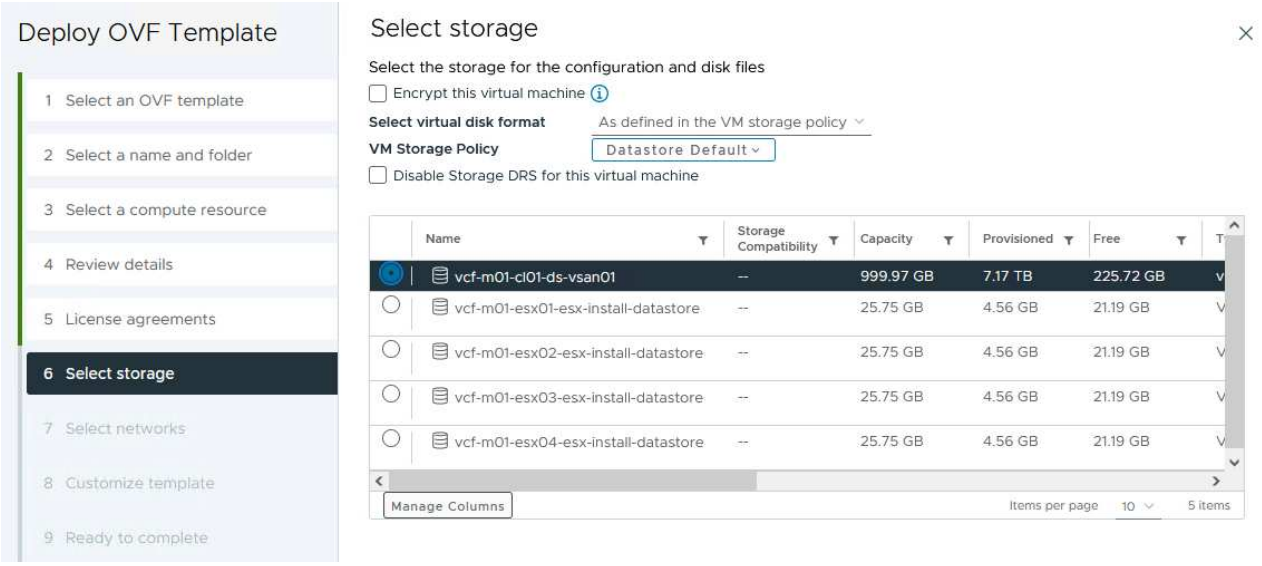
Completa quanto segue per implementare i tool ONTAP per VMware vSphere:

1. Ottenere l'immagine OVA degli strumenti ONTAP dal "Sito di supporto NetApp" e scaricarlo in una cartella locale.
2. Accedere all'appliance vCenter per il dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Deploy OVF Template…**

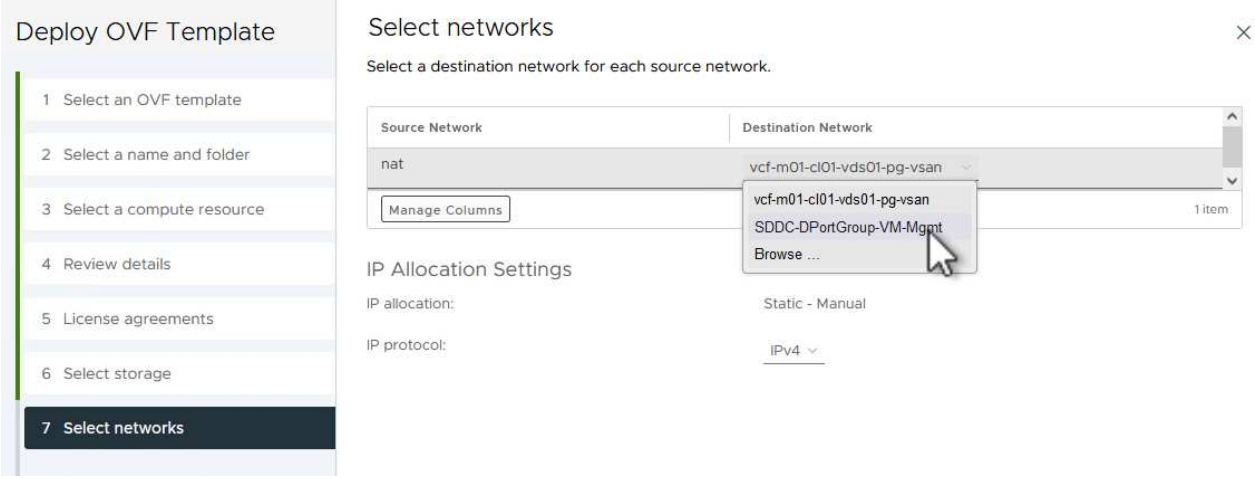


4. Nella procedura guidata **Deploy OVF Template** fare clic sul pulsante di opzione **file locale** e selezionare il file OVA di ONTAP Tools scaricato nel passaggio precedente.

5. Per i passaggi da 2 a 5 della procedura guidata, selezionare un nome e una cartella per la macchina virtuale, selezionare la risorsa di elaborazione, esaminare i dettagli e accettare il contratto di licenza.
6. Per la posizione di archiviazione dei file di configurazione e del disco, selezionare il datastore vSAN del cluster del dominio di gestione VCF.

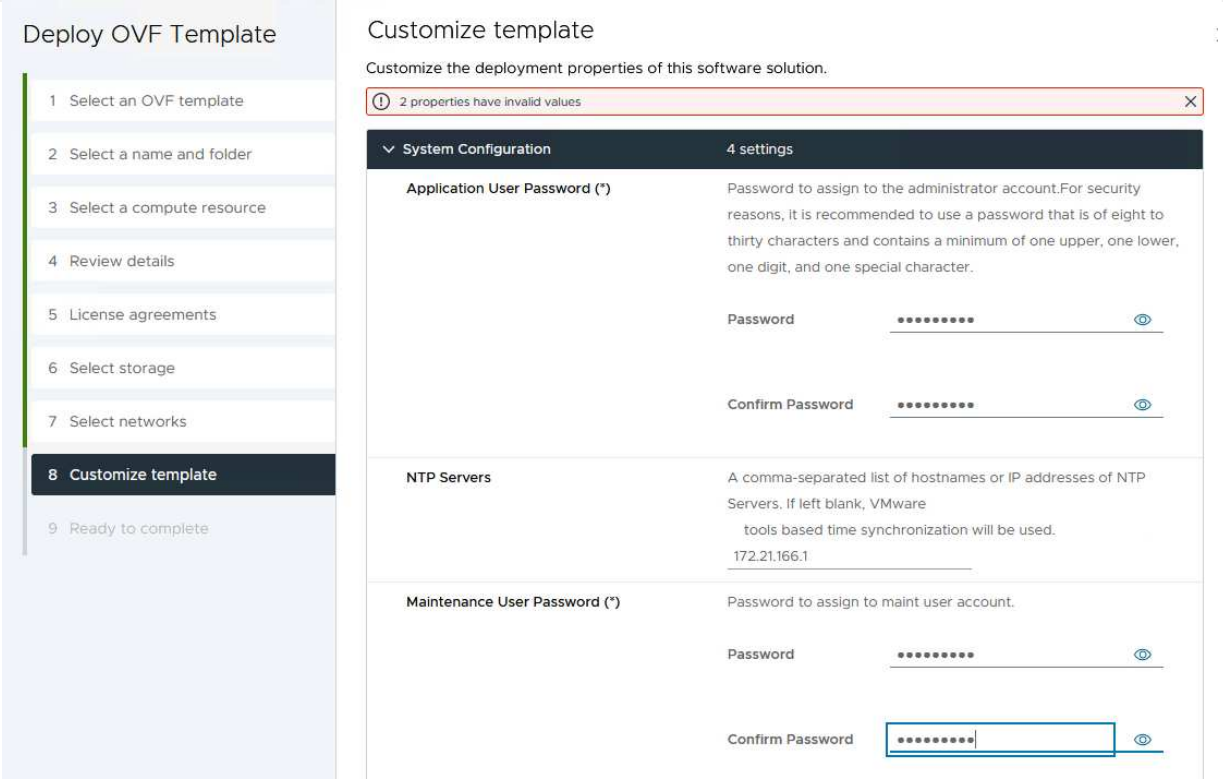


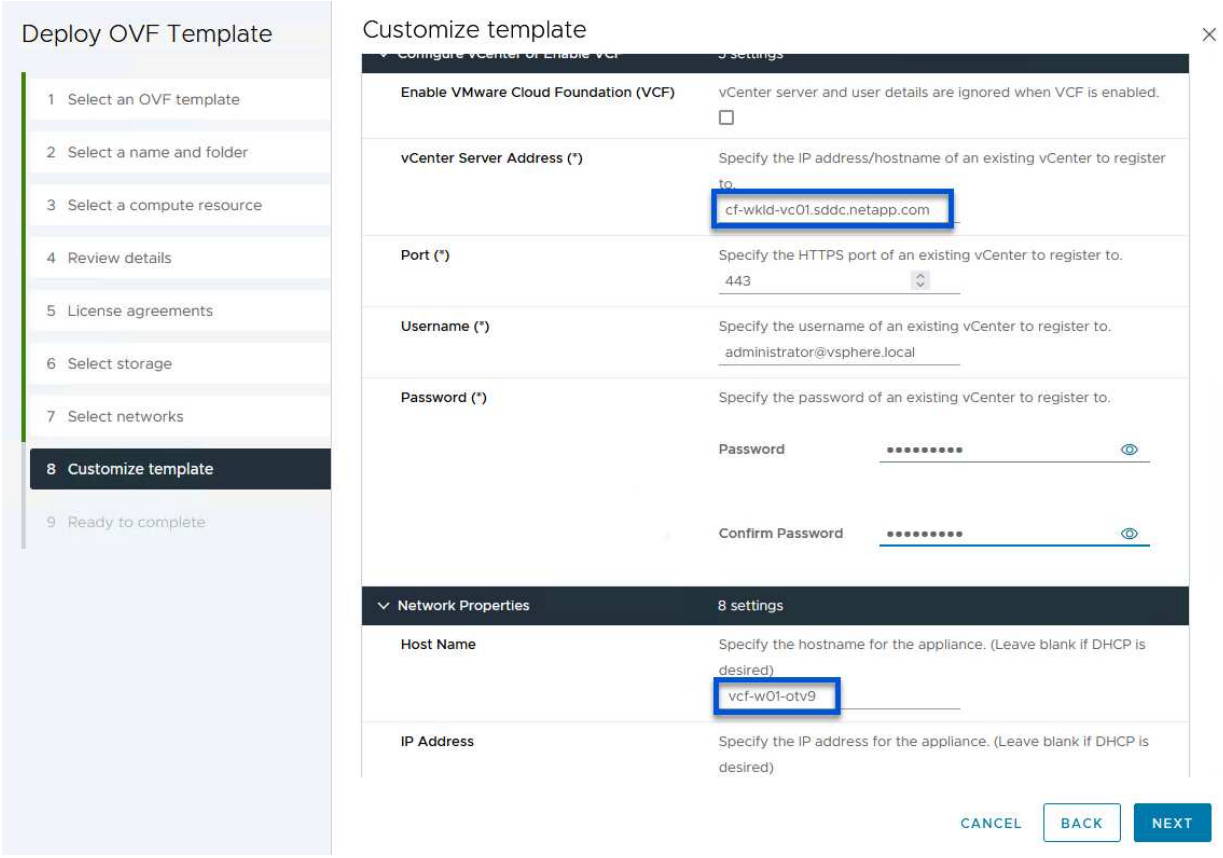
7. Nella pagina Seleziona rete, selezionare la rete utilizzata per la gestione del traffico.



8. Nella pagina Personalizza modello compilare tutte le informazioni richieste:
   - Password da utilizzare per l'accesso amministrativo agli strumenti ONTAP.
   - Indirizzo IP del server NTP.
   - Password dell'account di manutenzione degli strumenti ONTAP.
   - Password database derby strumenti ONTAP.
   - Non selezionare la casella di controllo **Abilita VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire lo storage supplementare.
   - FQDN o indirizzo IP dell'appliance vCenter per **VI workload Domain**
   - Credenziali per l'appliance vCenter del **VI workload Domain**
   - Specificare i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.

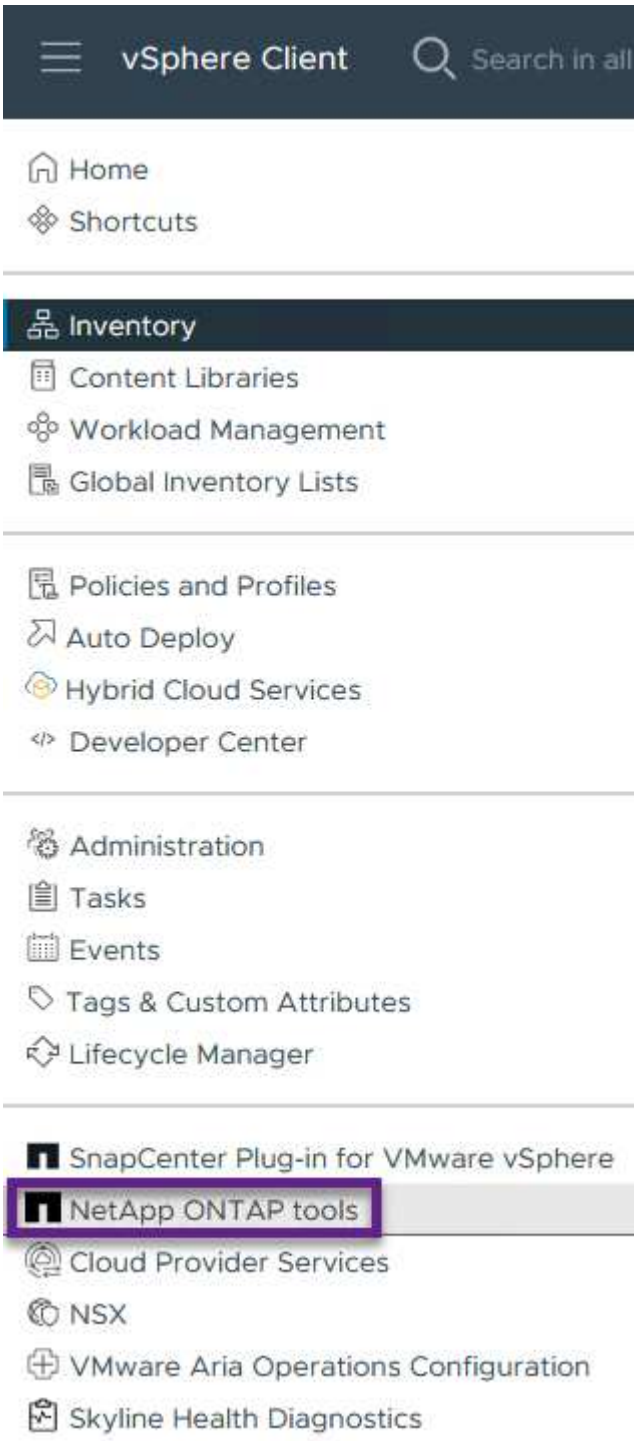




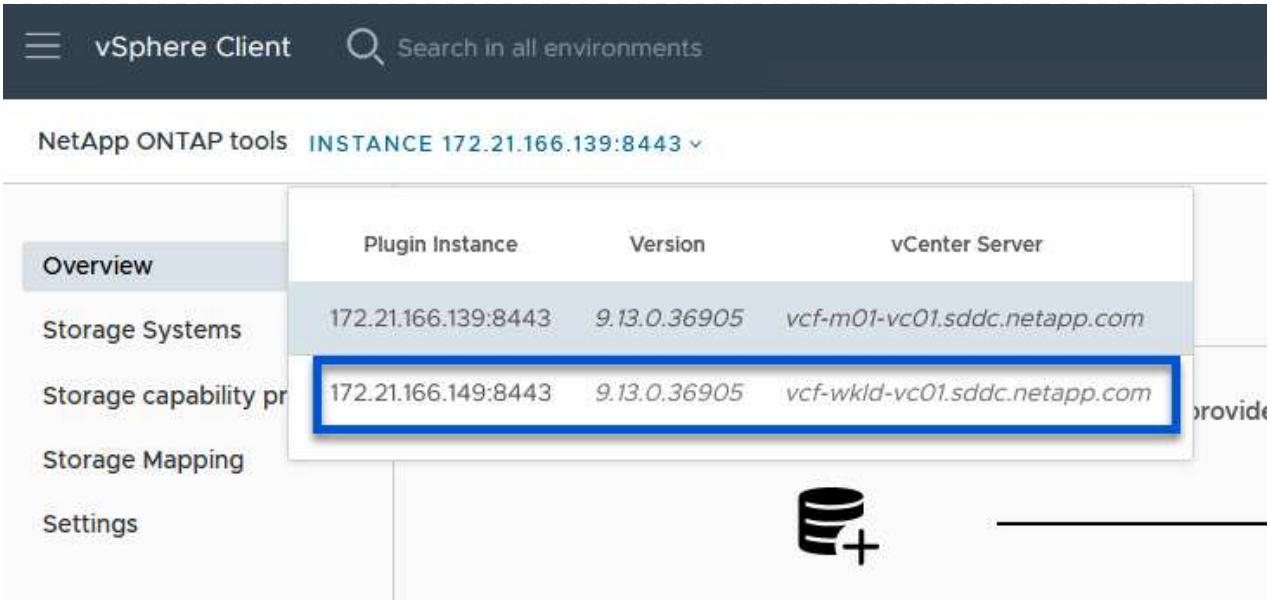
9. Leggere tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare a distribuire l'appliance ONTAP Tools.

Aggiunta di un sistema di storage ai tool ONTAP.

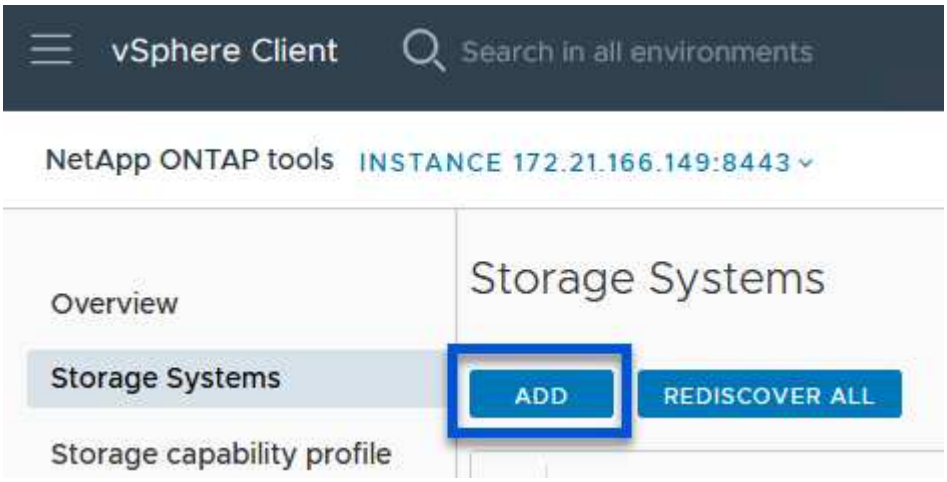
1. Accedere agli strumenti NetApp ONTAP selezionandoli dal menu principale del client vSphere.



2. Dal menu a discesa **INSTANCE** nell'interfaccia dello strumento ONTAP, selezionare l'istanza Strumenti ONTAP associata al dominio del carico di lavoro da gestire.

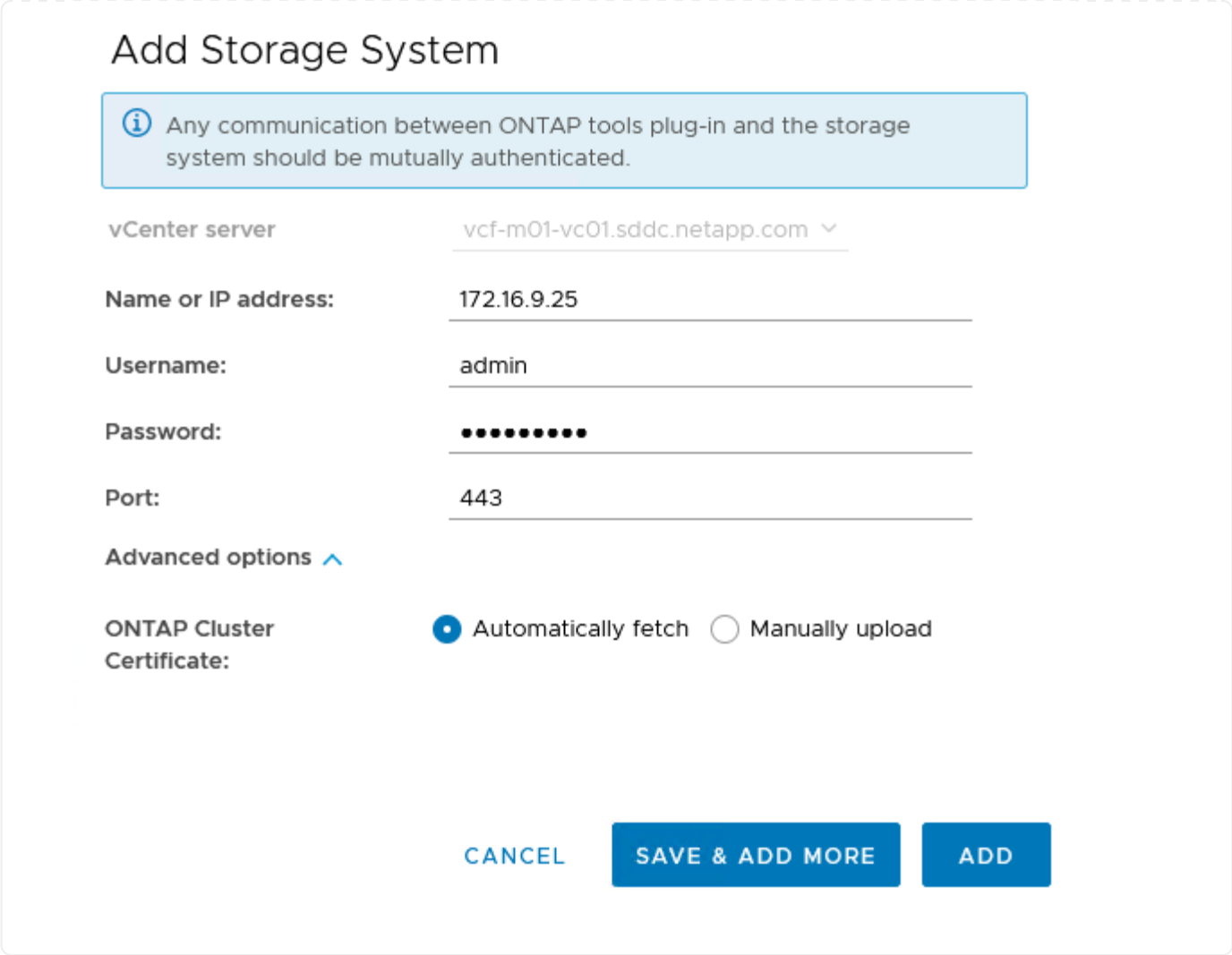


3. In Strumenti di ONTAP, selezionare **sistemi di archiviazione** dal menu a sinistra, quindi premere **Aggiungi**.



4. Immettere l'indirizzo IP, le credenziali del sistema di archiviazione e il numero di porta. Fare clic su **Aggiungi** per avviare il processo di ricerca.

> VVol richiede le credenziali del cluster ONTAP al posto delle credenziali SVM. Per ulteriori informazioni, fare riferimento a. "Aggiungere sistemi storage" Nella documentazione relativa agli strumenti ONTAP.

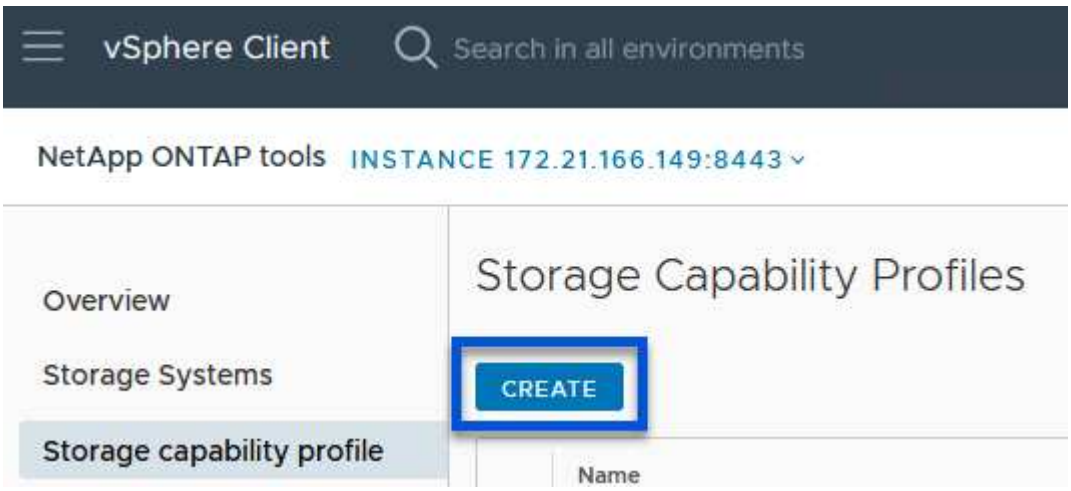

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Creare un profilo di funzionalità di storage in ONTAP Tools

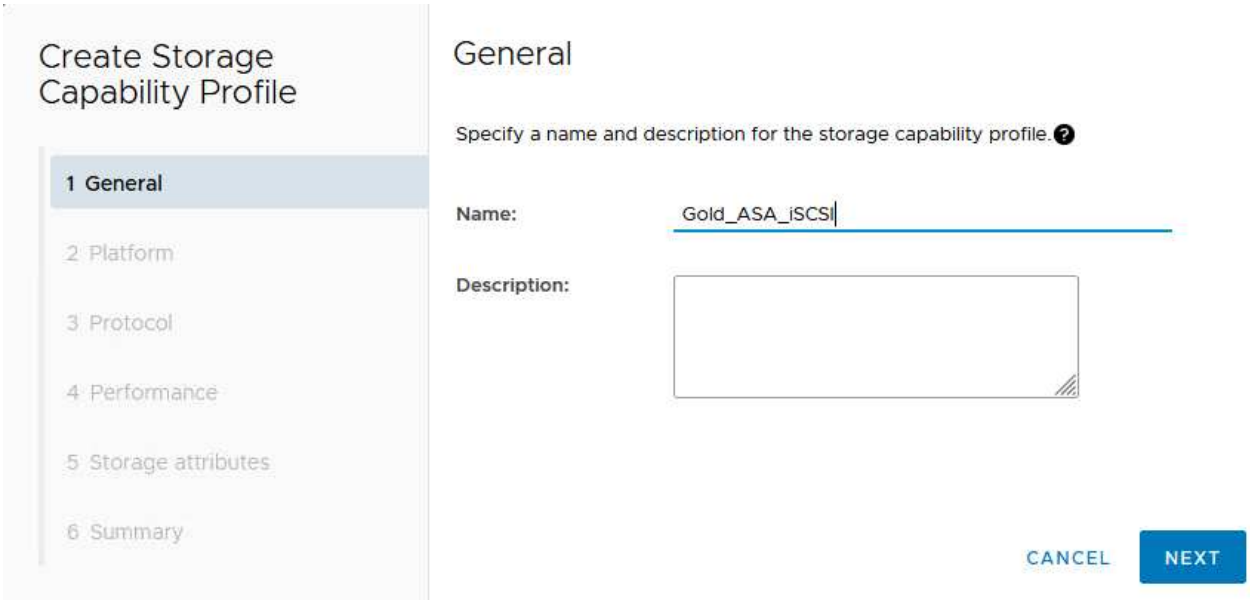
I profili di capacità dello storage descrivono le funzionalità fornite da uno storage array o da un sistema storage. Includono le definizioni della qualità del servizio e vengono utilizzate per selezionare i sistemi storage che soddisfano i parametri definiti nel profilo. È possibile utilizzare uno dei profili forniti oppure crearne uno nuovo.

Per creare un profilo di capacità di archiviazione negli strumenti ONTAP, completare i seguenti passaggi:

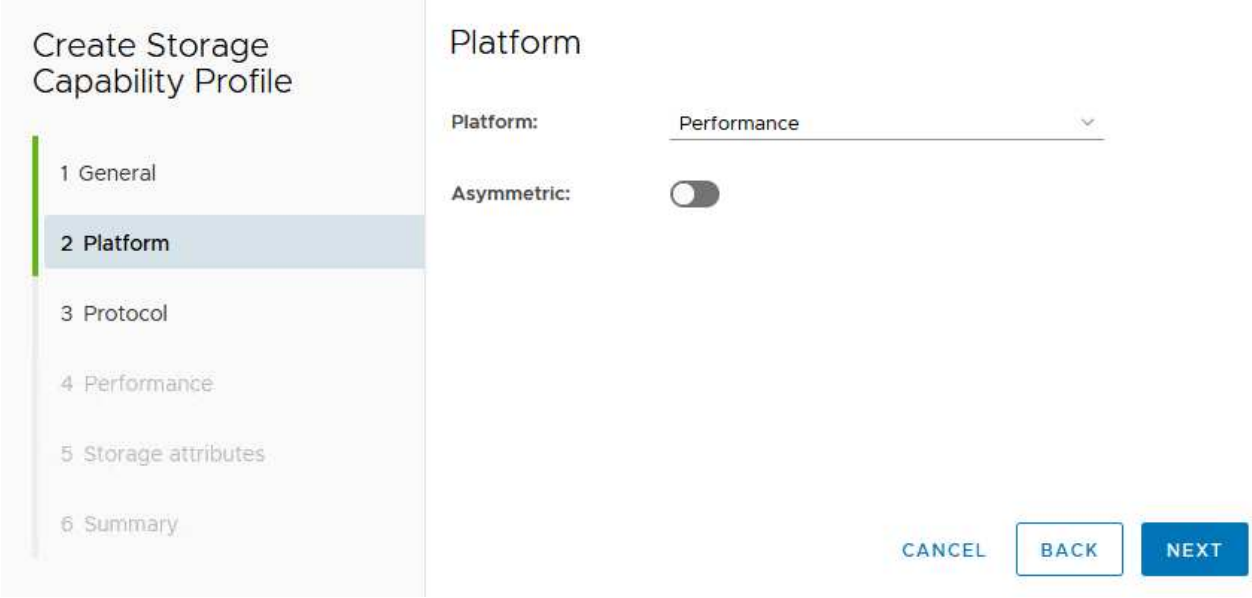
1. In Strumenti di ONTAP, selezionare **Profilo capacità di archiviazione** dal menu a sinistra, quindi premere **Crea**.



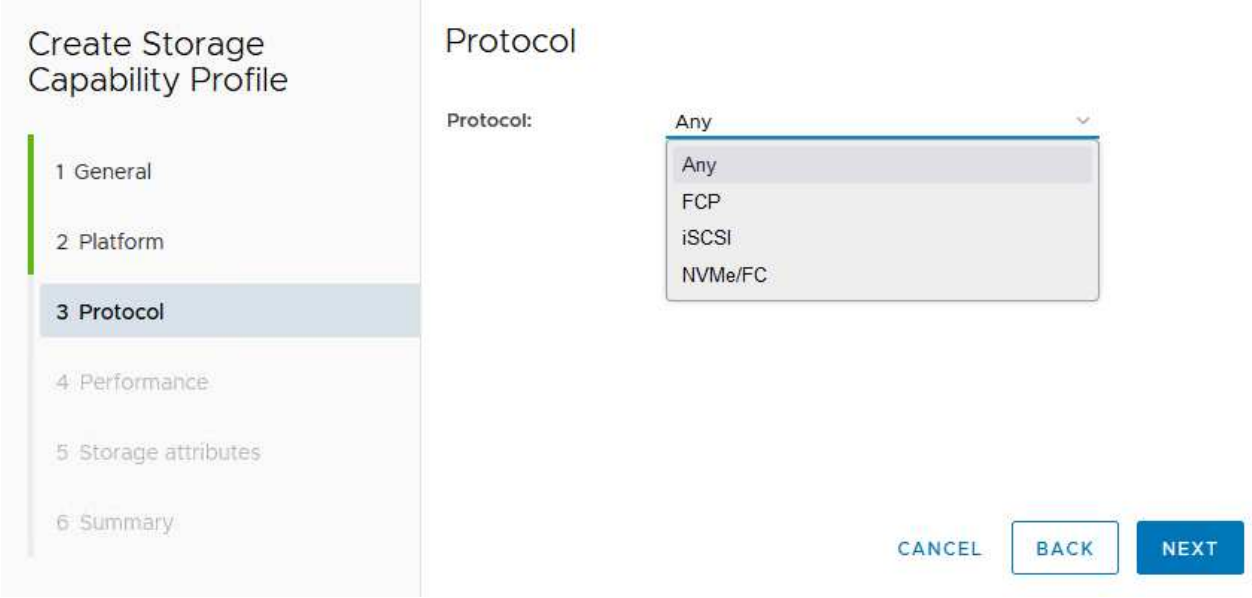
2. Nella procedura guidata **Crea profilo capacità di archiviazione** fornire un nome e una descrizione del profilo e fare clic su **Avanti**.



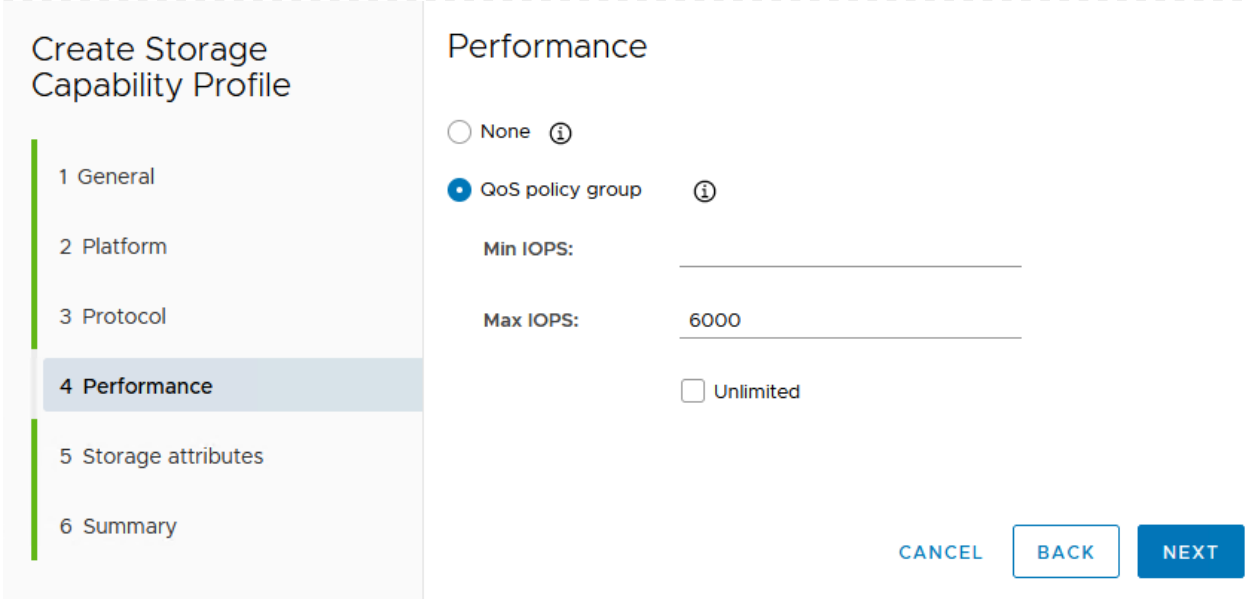
3. Seleziona il tipo di piattaforma e per specificare che il sistema storage deve essere un array SAN all-flash impostato su **asimmetrico** su falso.



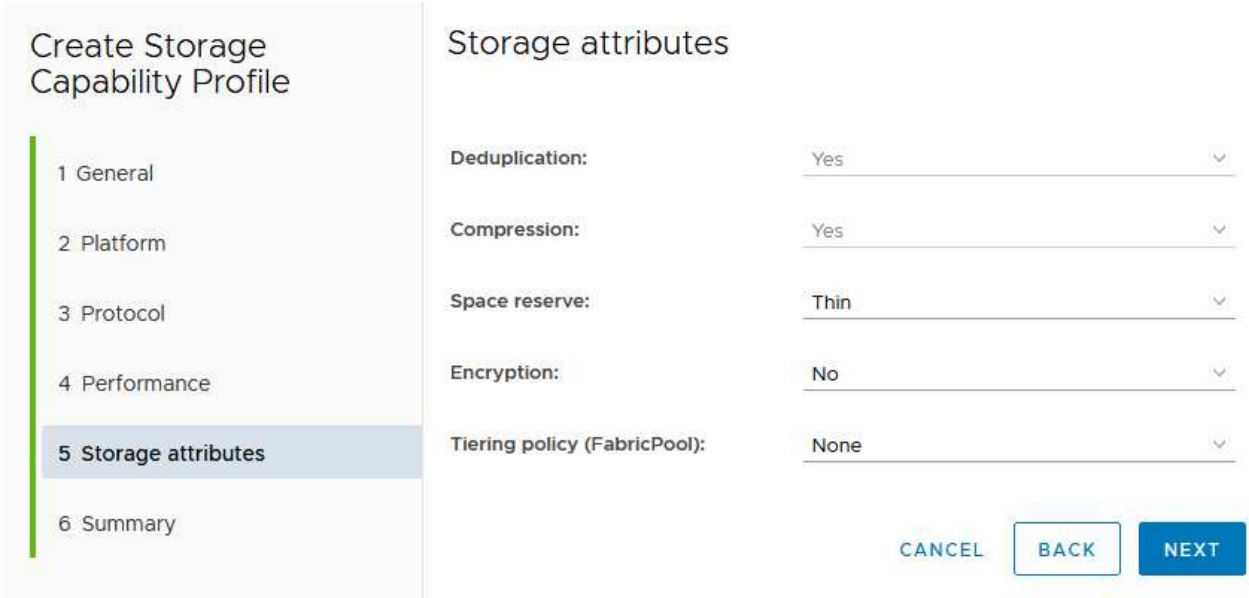
4. Quindi, selezionare Choice of Protocol (scelta del protocollo) o **Any** (qualsiasi) per consentire tutti i protocolli possibili. Fare clic su **Avanti** per continuare.



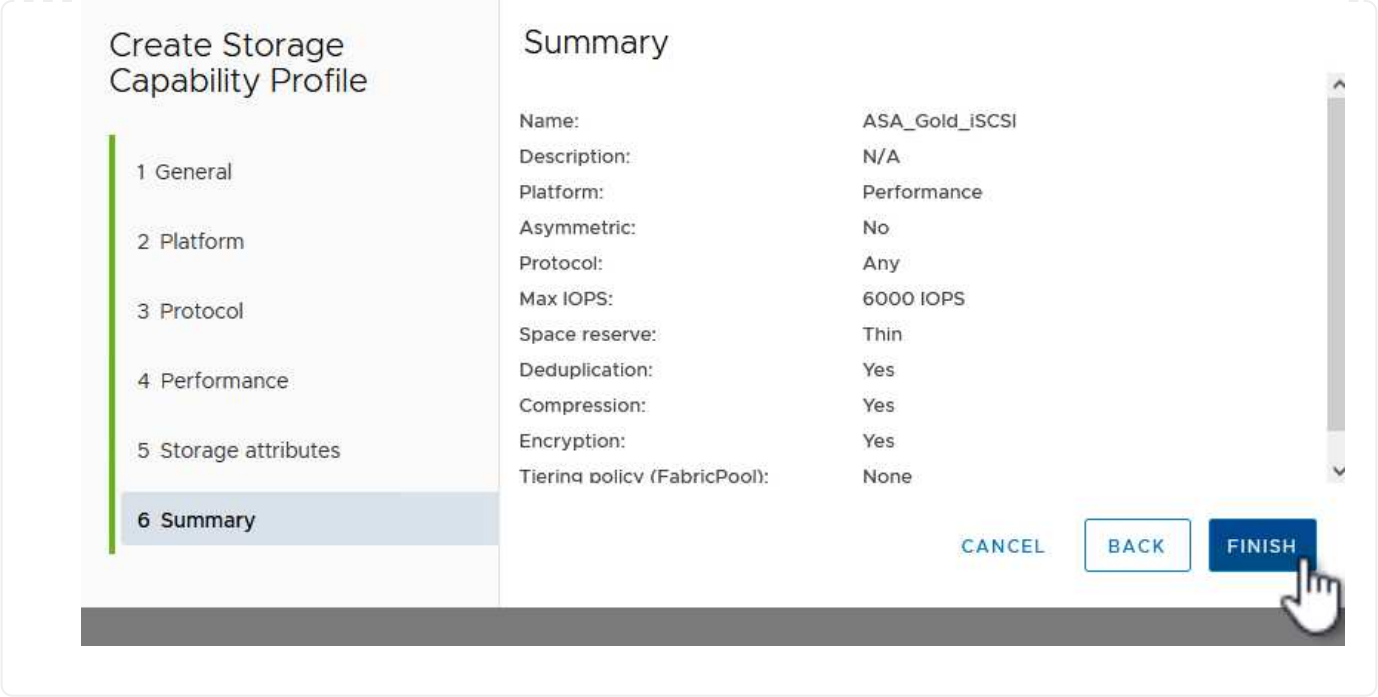
5. La pagina **performance** consente di impostare la qualità del servizio sotto forma di IOPS minimi e massimi consentiti.



6. Completare la pagina **attributi di archiviazione** selezionando l'efficienza di archiviazione, la prenotazione dello spazio, la crittografia e qualsiasi criterio di tiering in base alle esigenze.



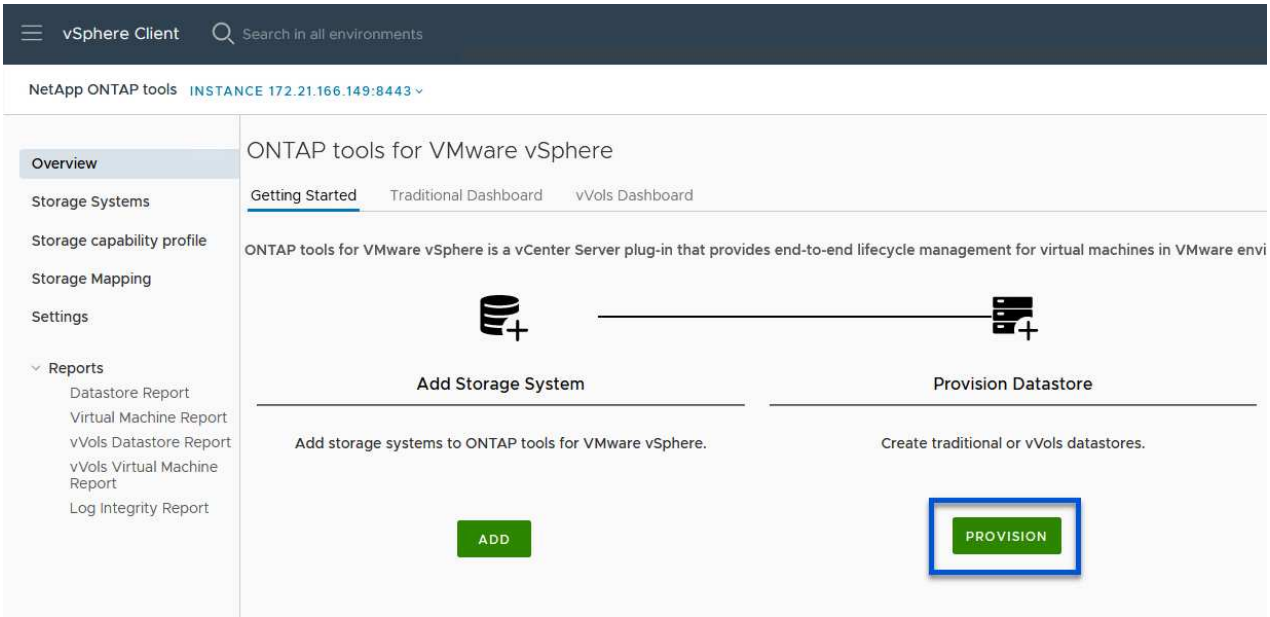
7. Infine, rivedere il riepilogo e fare clic su fine per creare il profilo.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold_iSCSI
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: Yes
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

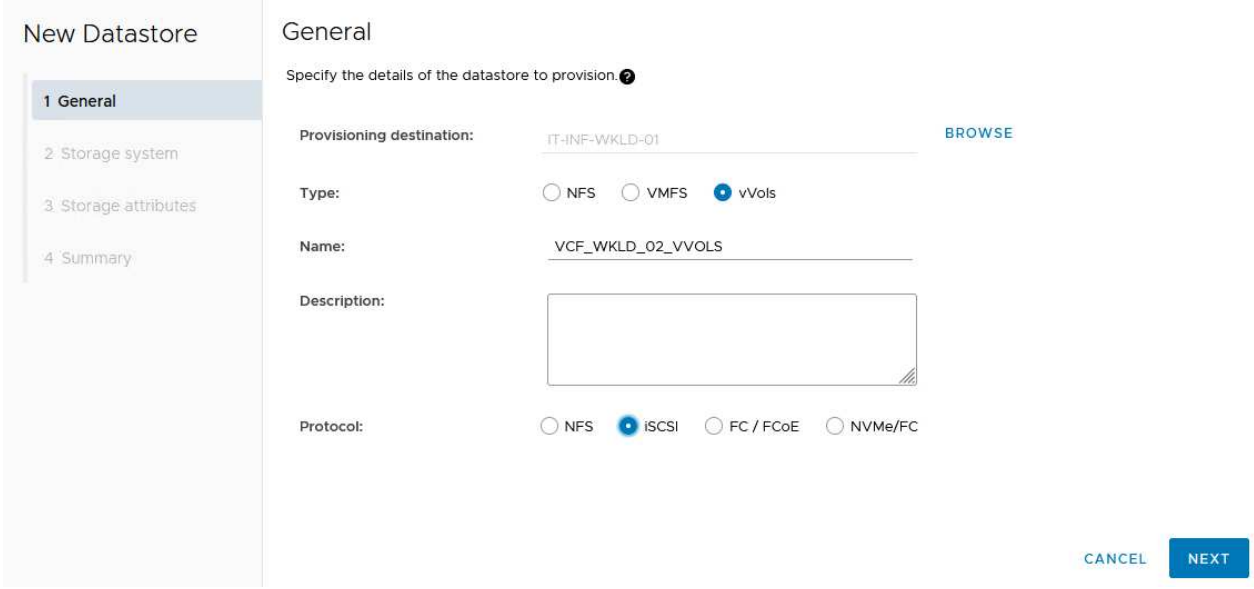
Creare un datastore vVol in ONTAP Tools

Per creare un datastore vVol in Strumenti di ONTAP, attenersi alla seguente procedura:

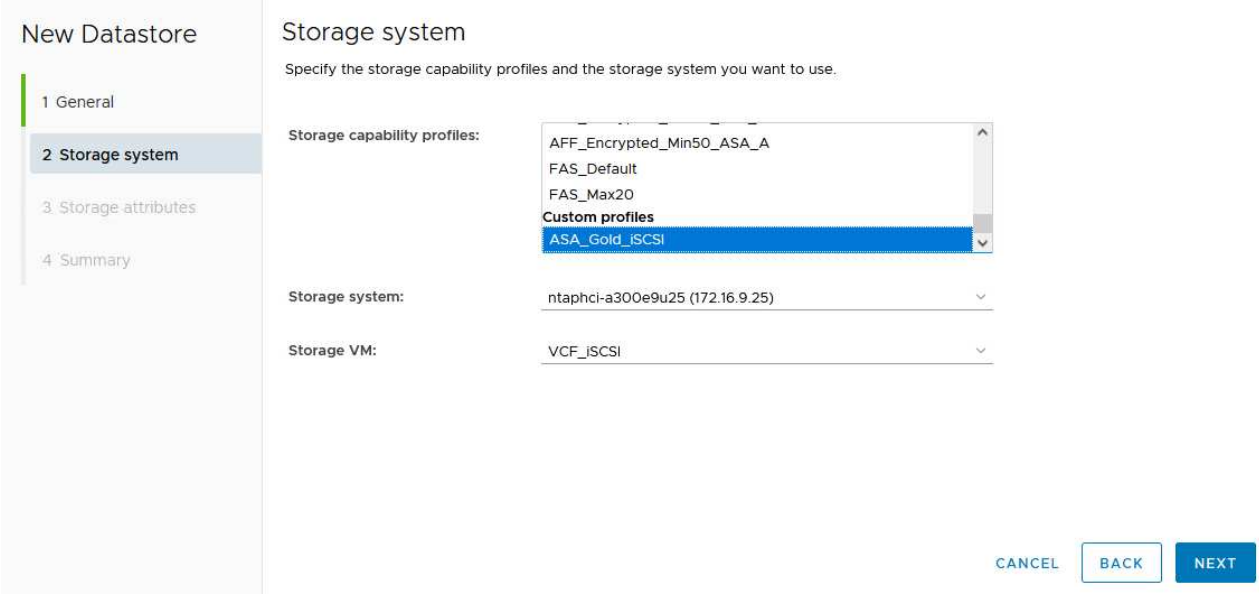
1. In Strumenti di ONTAP selezionare **Panoramica** e dalla scheda **Guida introduttiva** fare clic su **Provision** per avviare la procedura guidata.



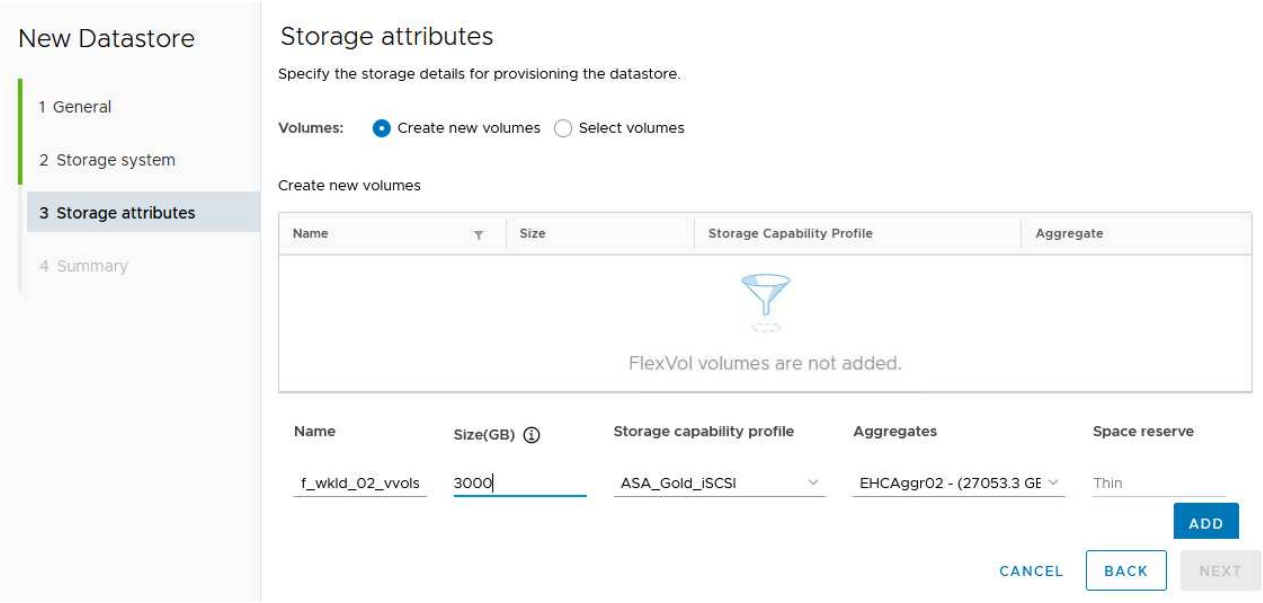
2. Nella pagina **Generale** della procedura guidata nuovo datastore selezionare il data center vSphere o la destinazione del cluster. Selezionare **vVol** come tipo di datastore, specificare un nome per il datastore e selezionare **iSCSI** come protocollo. Fare clic su **Avanti** per continuare.



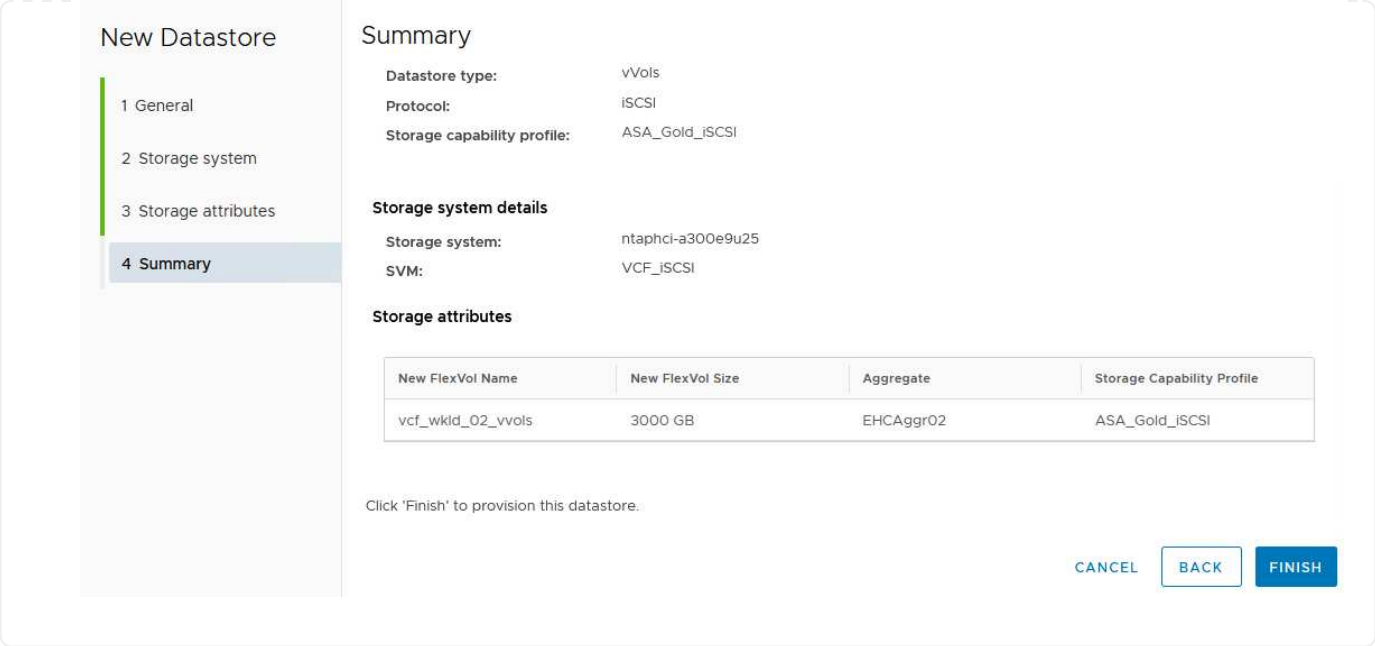
3. Nella pagina **sistema storage**, seleziona un profilo di funzionalità storage, il sistema storage e la SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **attributi archiviazione**, selezionare per creare un nuovo volume per l'archivio dati e specificare gli attributi di archiviazione del volume da creare. Fare clic su **Aggiungi** per creare il volume, quindi su **Avanti** per continuare.



5. Infine, rivedere il riepilogo e fare clic su **fine** per avviare il processo di creazione del datastore vVol.



Ulteriori informazioni

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Configurare lo storage supplementare NVMe/TCP per i domini del carico di lavoro VCF

In questo scenario, dimostreremo come configurare lo storage supplementare NVMe/TCP per un dominio di carico di lavoro VCF.

Autore: Josh Powell

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

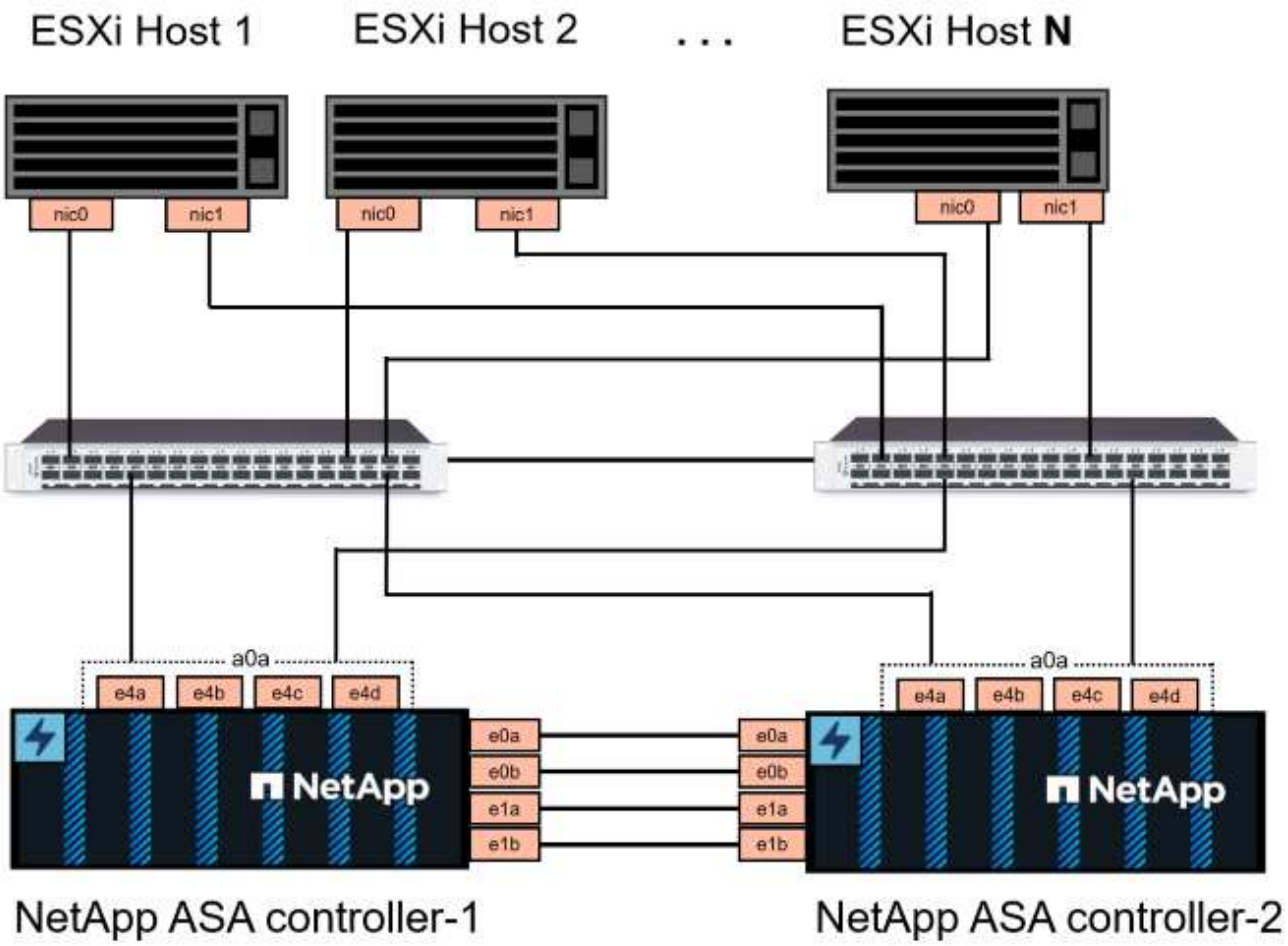
- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico NVMe/TCP.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Aggiungere adattatori NVMe/TCP sugli host ESXi.
- Implementa il datastore NVMe/TCP.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con porte per dati fisici su switch ethernet dedicati al traffico di storage.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.

NetApp consiglia design di rete completamente ridondanti per NVMe/TCP. Il diagramma seguente illustra un esempio di configurazione ridondante, che fornisce tolleranza agli errori per sistemi di archiviazione, switch, schede di rete e sistemi host. Consultare il NetApp "Riferimento alla configurazione SAN" per ulteriori informazioni.



Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti ethernet separate per tutte le SVM nelle configurazioni NVMe/TCP.

Questa documentazione illustra il processo di creazione di una nuova SVM e specifica delle informazioni dell'indirizzo IP per creare LIF multipli per il traffico NVMe/TCP. Per aggiungere nuove LIF a una SVM esistente, fare riferimento a. "Creazione di una LIF (interfaccia di rete)".

Per ulteriori informazioni sulle considerazioni sulla progettazione NVMe per i sistemi storage ONTAP, fare riferimento a. "Configurazione, supporto e limitazioni NVMe".

Fasi di implementazione

Per creare un datastore VMFS su un dominio di carico di lavoro VCF utilizzando NVMe/TCP, completa i seguenti passaggi.

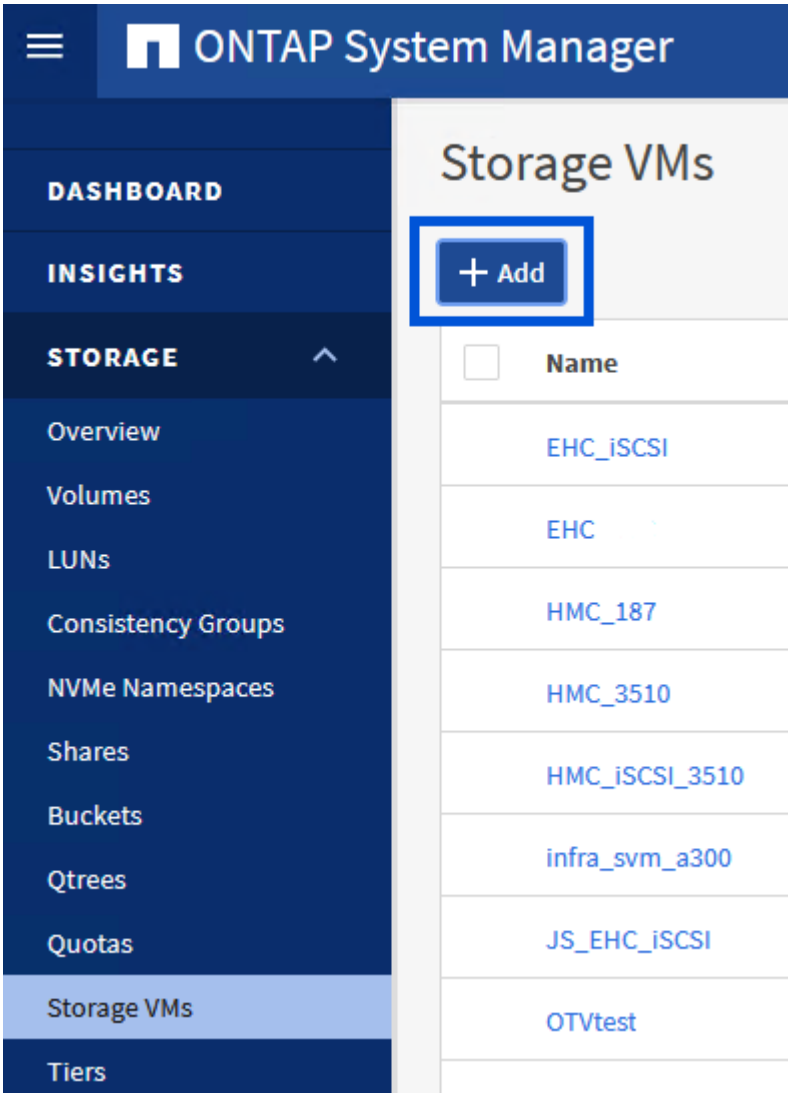
Crea SVM, LIF e namespace NVMe su un sistema storage ONTAP

Il passaggio seguente viene eseguito in Gestione di sistema di ONTAP.

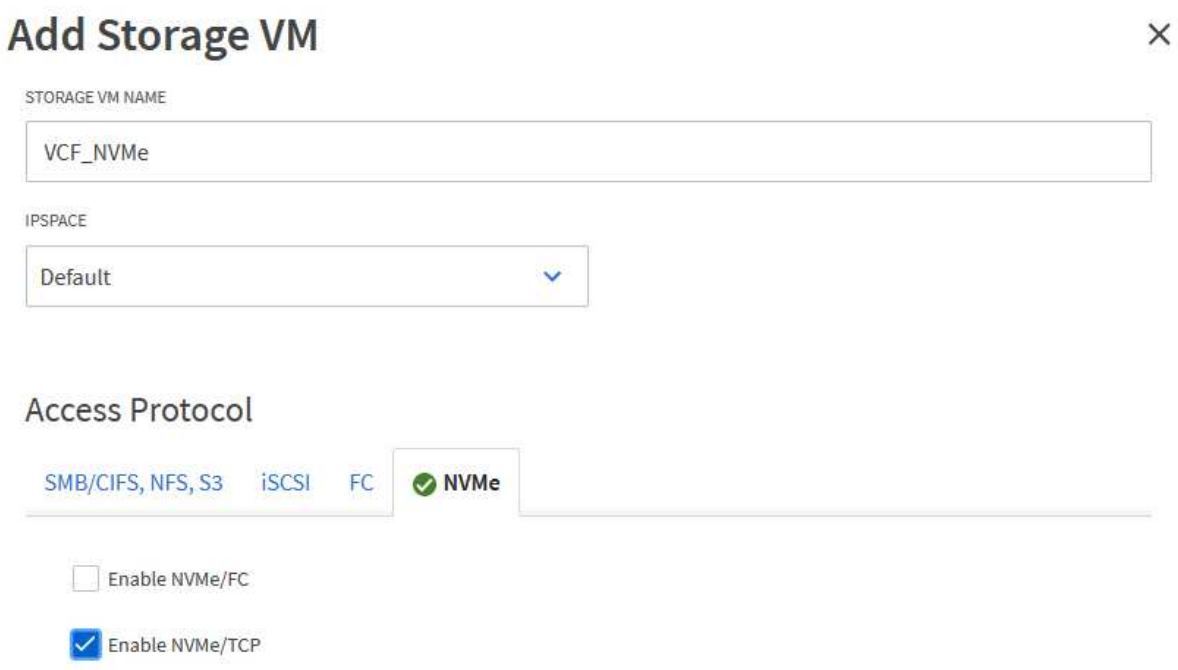
Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per traffico NVMe/TCP.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.



2. Nella procedura guidata **Add Storage VM** (Aggiungi VM di storage) fornire un **Name** (Nome) per la SVM, selezionare **IP Space** (spazio IP), quindi, in **Access Protocol** (protocollo di accesso), fare clic sulla scheda **NVMe** e selezionare la casella **Enable NVMe/TCP** (Abilita NVMe/TCP*).



3. Nella sezione **interfaccia di rete** compilare i campi **indirizzo IP**, **Subnet Mask** e **Broadcast Domain and Port** per la prima LIF. Per LIF successive, la casella di controllo può essere abilitata per usare impostazioni comuni a tutte le LIF rimanenti o per usare impostazioni separate.

> Per il multipathing e il failover su percorsi multipli, NetApp consiglia di disporre di un minimo di due LIF per nodo storage in reti Ethernet separate per tutte le SVM nelle configurazioni NVMe/TCP.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS: 172.21.118.189
SUBNET MASK: 24
GATEWAY: Add optional gateway
BROADCAST DOMAIN AND PORT: NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS: 172.21.119.189
PORT: a0a-3375

ntaphci-a300-02

IP ADDRESS: 172.21.118.190
PORT: a0a-3374

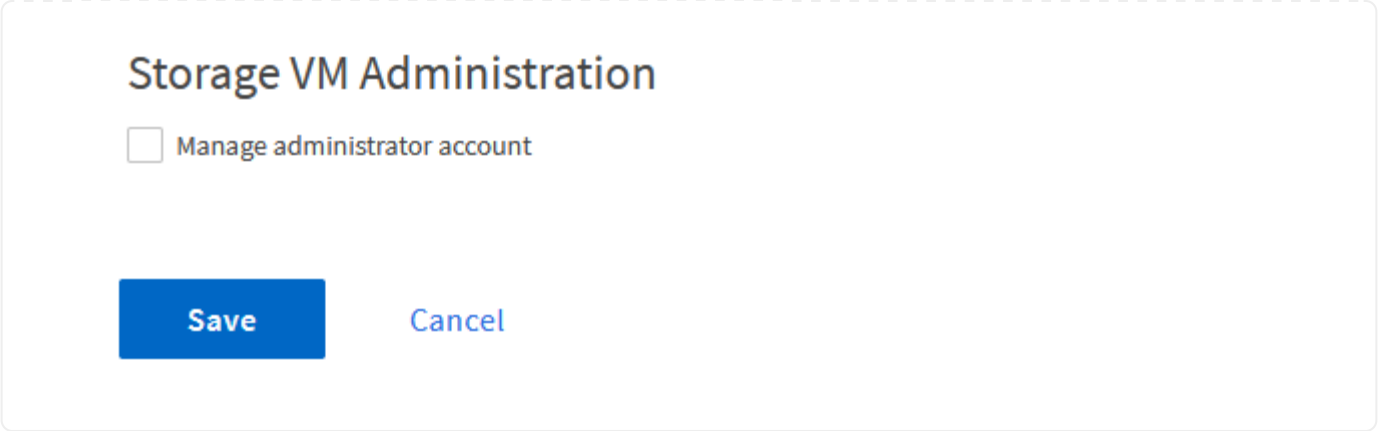
IP ADDRESS: 172.21.119.190
PORT: a0a-3375

Storage VM Administration

Manage administrator account

Save Cancel

4. Scegliere se attivare l'account Storage VM Administration (per ambienti multi-tenancy) e fare clic su **Save** (Salva) per creare la SVM.


Storage VM Administration
Manage administrator account
Save
Cancel

Creare il namespace NVMe

I namespace NVMe sono analoghi alle LUN per iSCSI o FC. È necessario creare il namespace NVMe prima di poter implementare un datastore VMFS da vSphere Client. Per creare il namespace NVMe, occorre prima ottenere il NVMe Qualified Name (NQN) da ogni host ESXi nel cluster. L'NQN viene utilizzato da ONTAP per fornire il controllo dell'accesso allo spazio dei nomi.

Completare i seguenti passaggi per creare un namespace NVMe:

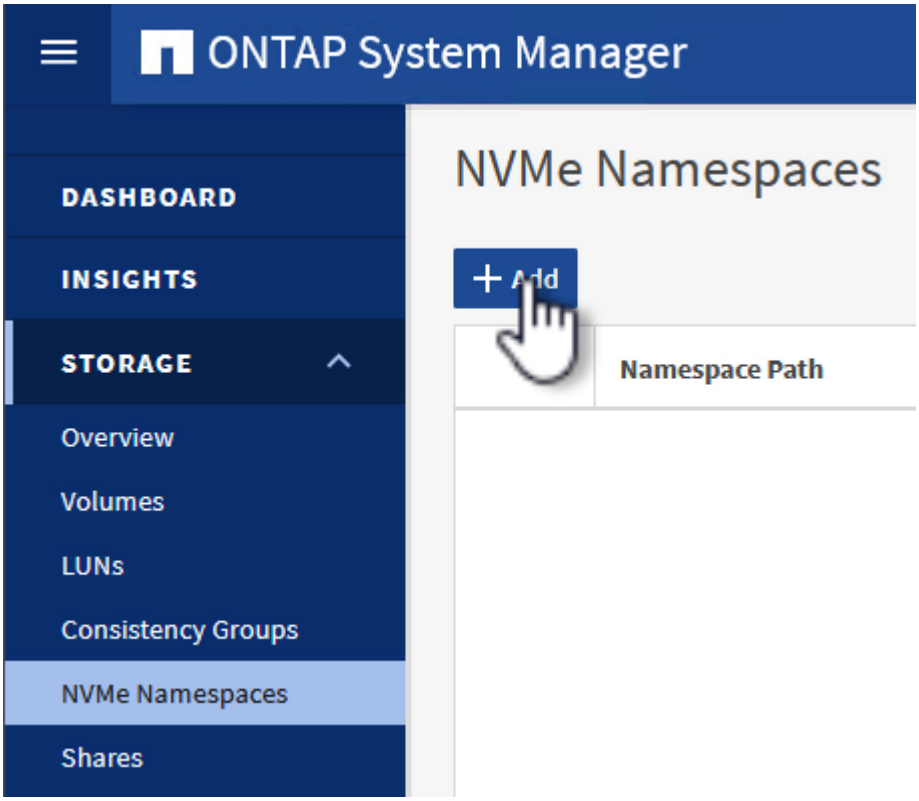
1. Aprire una sessione SSH con un host ESXi nel cluster per ottenere il proprio NQN. Utilizzare il seguente comando dall'interfaccia CLI:

   ```
   esxcli nvme info get
   ```

   Dovrebbe essere visualizzato un output simile al seguente:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

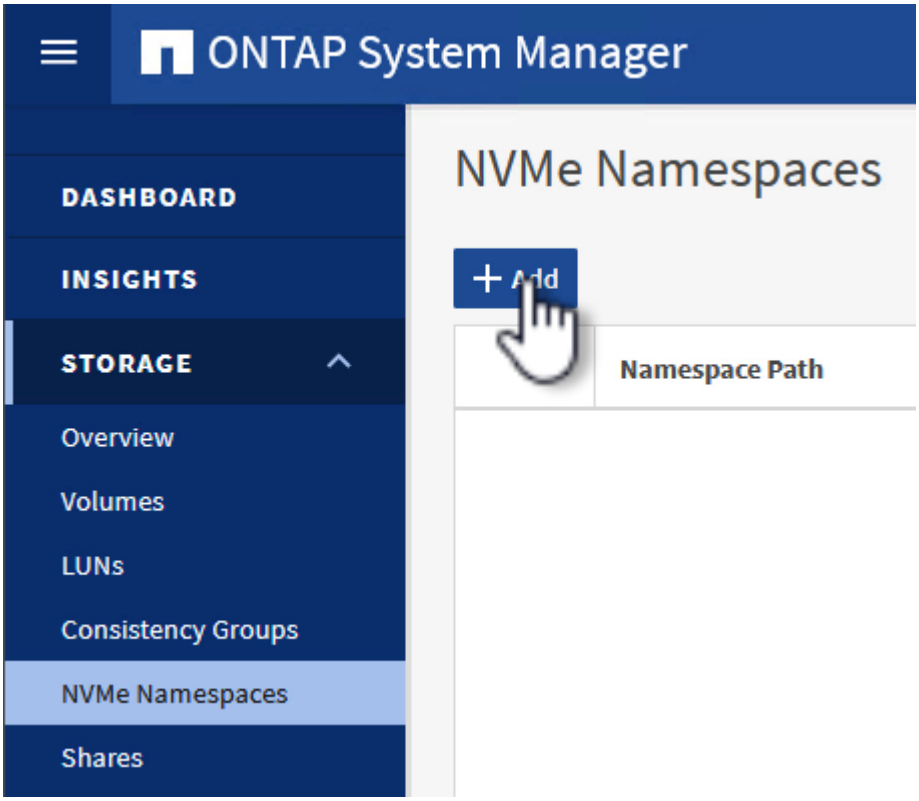
2. Registrare l'NQN per ciascun host ESXi nel cluster
3. Da Gestione di sistema di ONTAP, accedere a **NVMe Namespaces** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.



4. Nella pagina **Add NVMe Namespace**, inserire un prefisso nome, il numero di namespace da creare, le dimensioni dello spazio dei nomi e il sistema operativo host che accederà allo spazio dei nomi.

Nella sezione **host NQN** creare un elenco separato da virgole degli NQN precedentemente raccolti dagli host ESXi che accederanno agli spazi dei nomi.

Fare clic su **altre opzioni** per configurare elementi aggiuntivi come il criterio di protezione delle istantanee. Infine, fare clic su **Save** per creare lo spazio dei nomi NVMe.



+

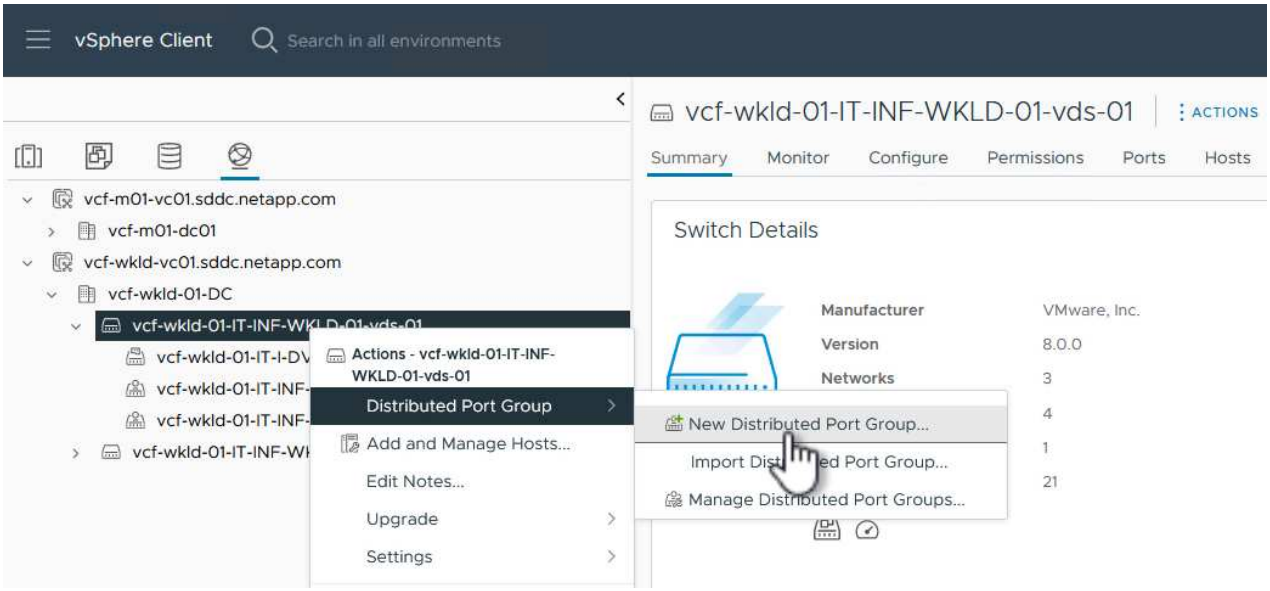
Configurare le schede di rete e il software NVMe sugli host ESXi

I seguenti passaggi vengono eseguiti sul cluster di dominio del carico di lavoro VI utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-on, pertanto il client vSphere è comune sia ai domini di gestione che ai domini di workload.

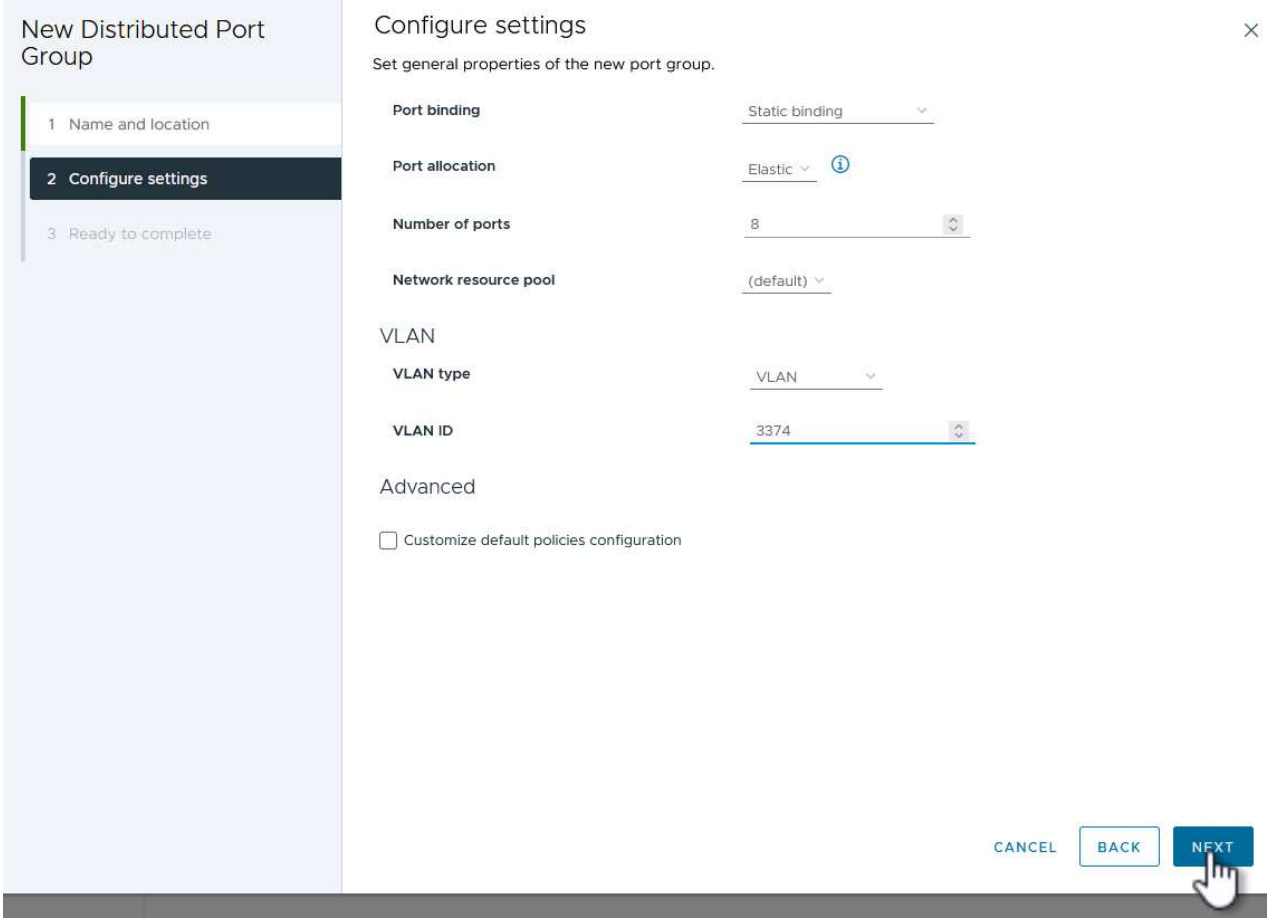
Creare gruppi di porte distribuite per il traffico NVME/TCP

Completare quanto segue per creare un nuovo gruppo di porte distribuite per ogni rete NVMe/TCP:

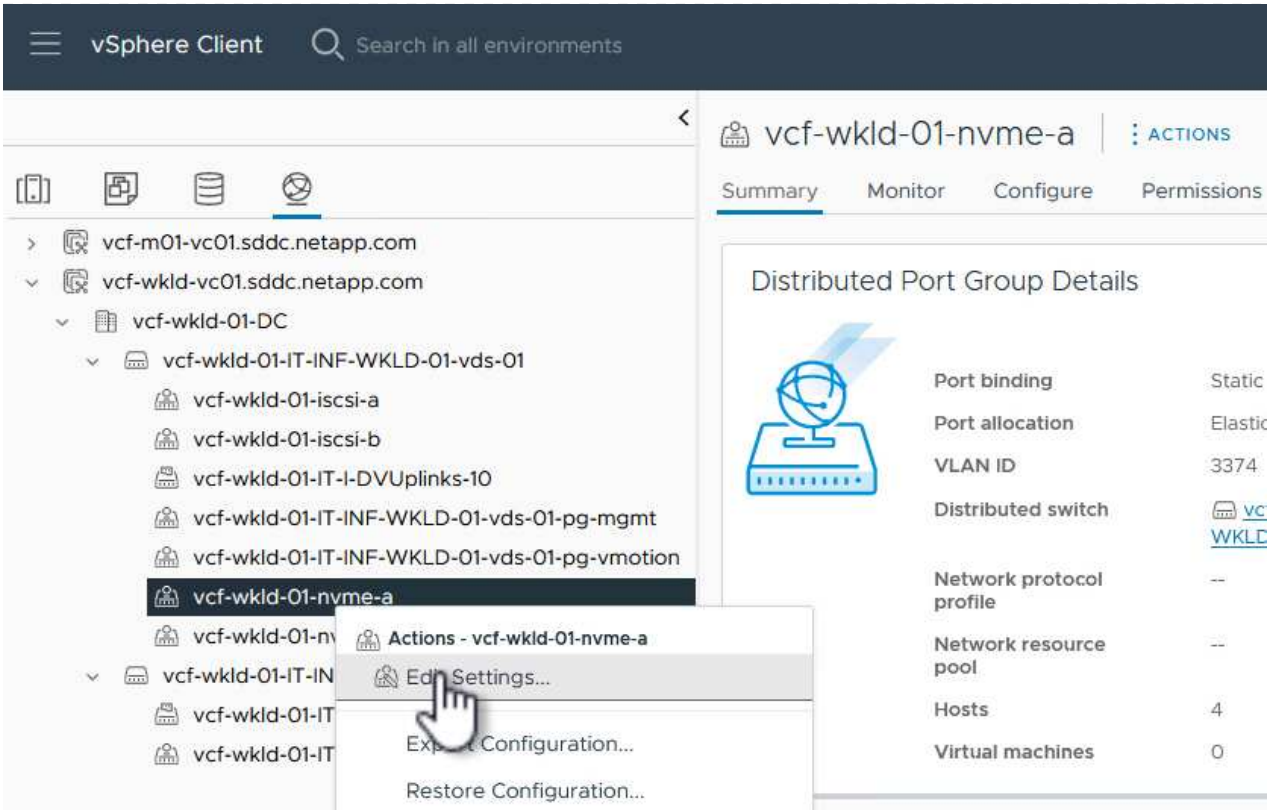
1. Dal client vSphere , accedere a **Inventory > Networking** per il dominio del carico di lavoro. Passare allo Switch distribuito esistente e scegliere l'azione da creare **nuovo Gruppo di porte distribuite…**.



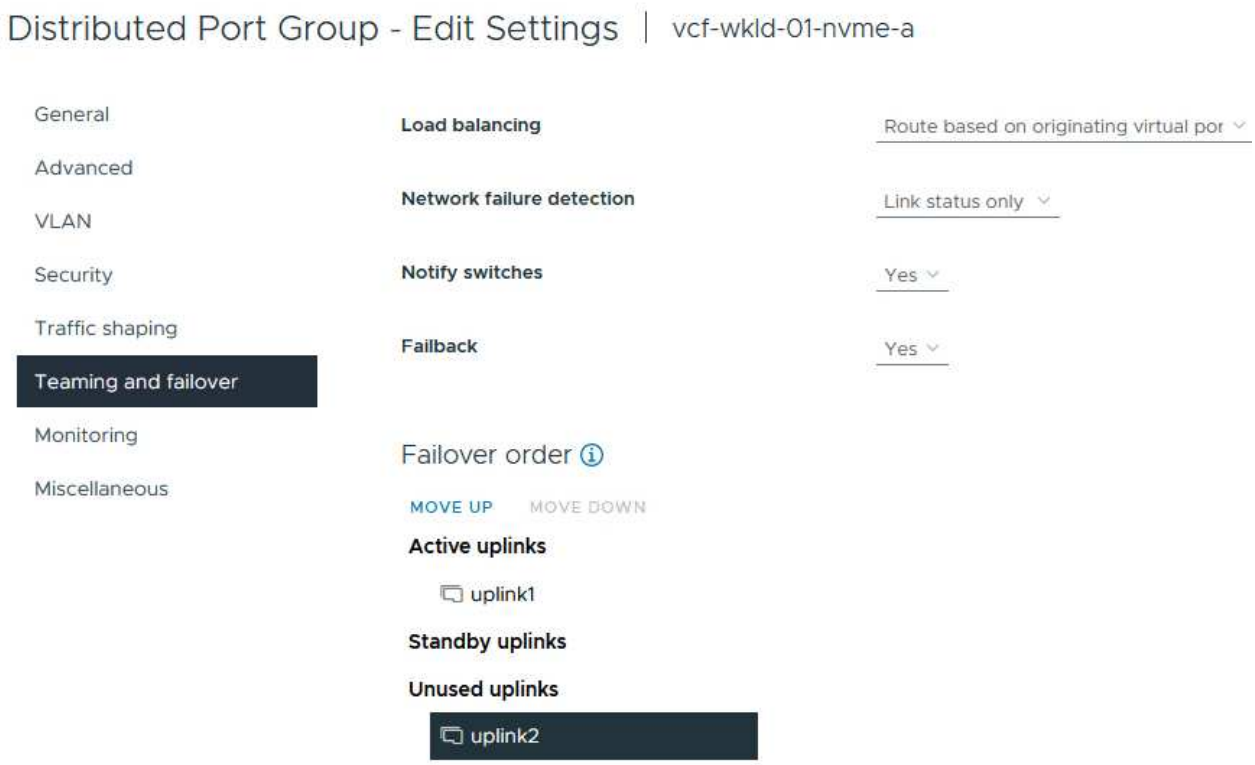
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare clic su **Avanti** per continuare.



4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **fine** per creare il nuovo gruppo di porte distribuite.
5. Ripetere questa procedura per creare un gruppo di porte distribuite per la seconda rete NVMe/TCP in uso e assicurarsi di aver immesso il corretto **VLAN ID**.
6. Una volta creati entrambi i gruppi di porte, accedere al primo gruppo di porte e selezionare l'azione **Modifica impostazioni…**.

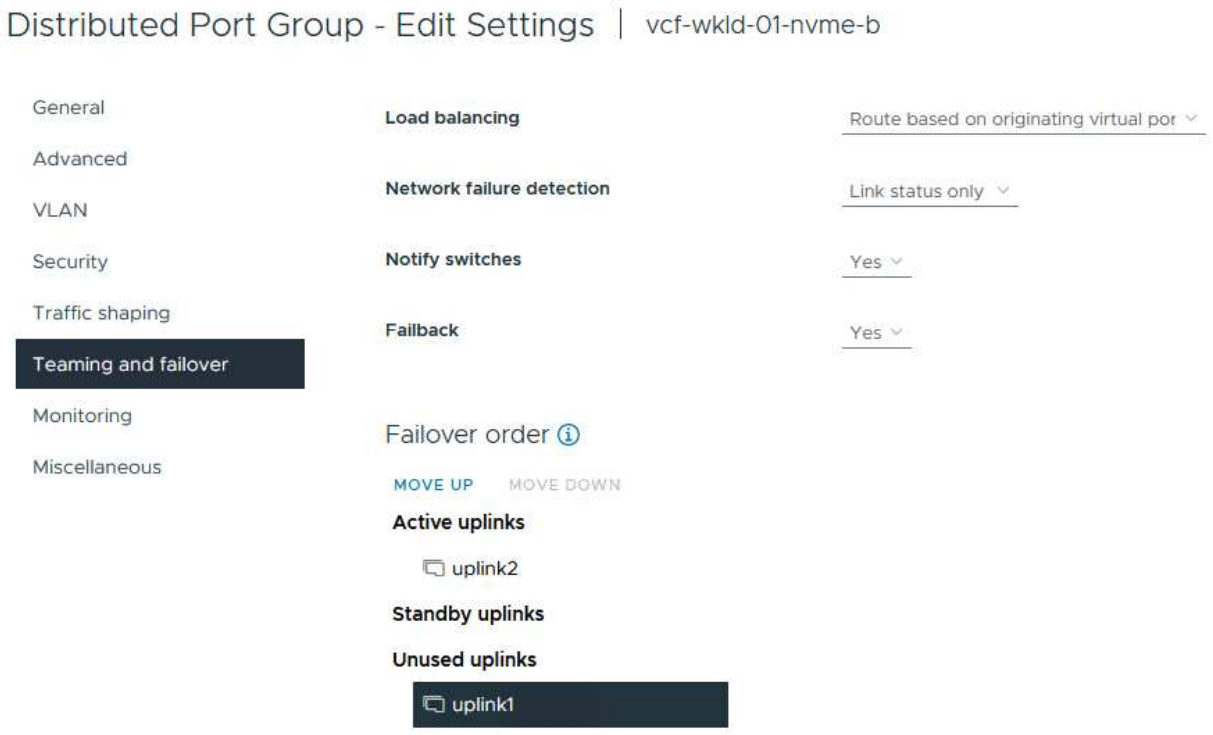


7. Nella pagina **Gruppo porte distribuite - Modifica impostazioni**, accedere a **Teaming and failover** nel menu a sinistra e fare clic su **uplink2** per spostarlo in basso in **uplink non utilizzati**.



8. Ripetere questo passo per il secondo gruppo di porte NVMe/TCP. Tuttavia, questa volta si sposta

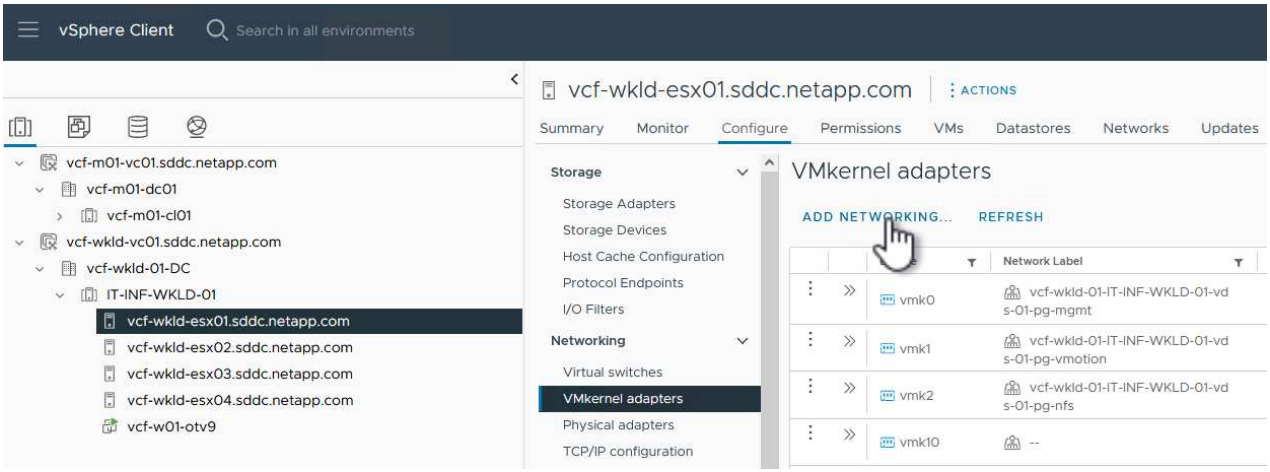
uplink1 verso il basso in **uplink non utilizzati**.



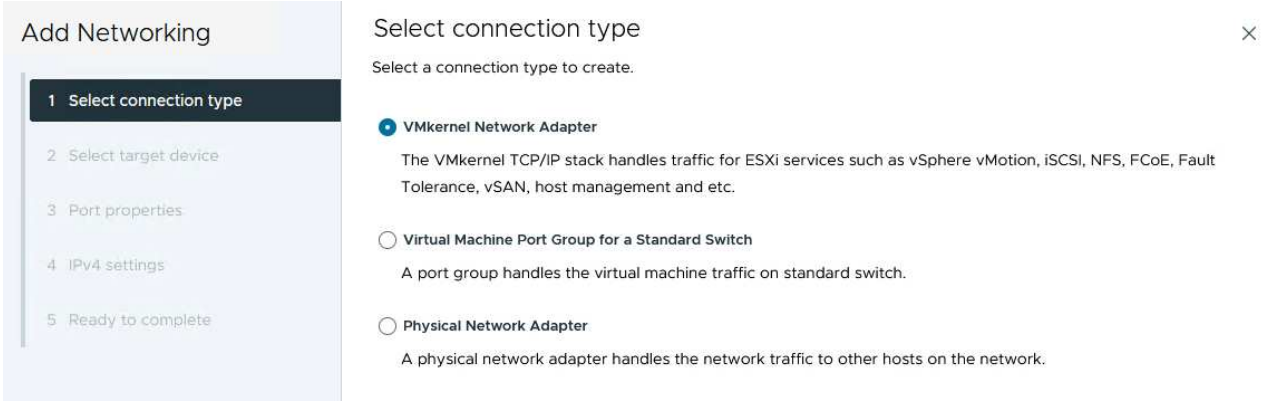
Creare adattatori VMkernel su ciascun host ESXi

Ripetere questo processo su ogni host ESXi nel dominio del carico di lavoro.

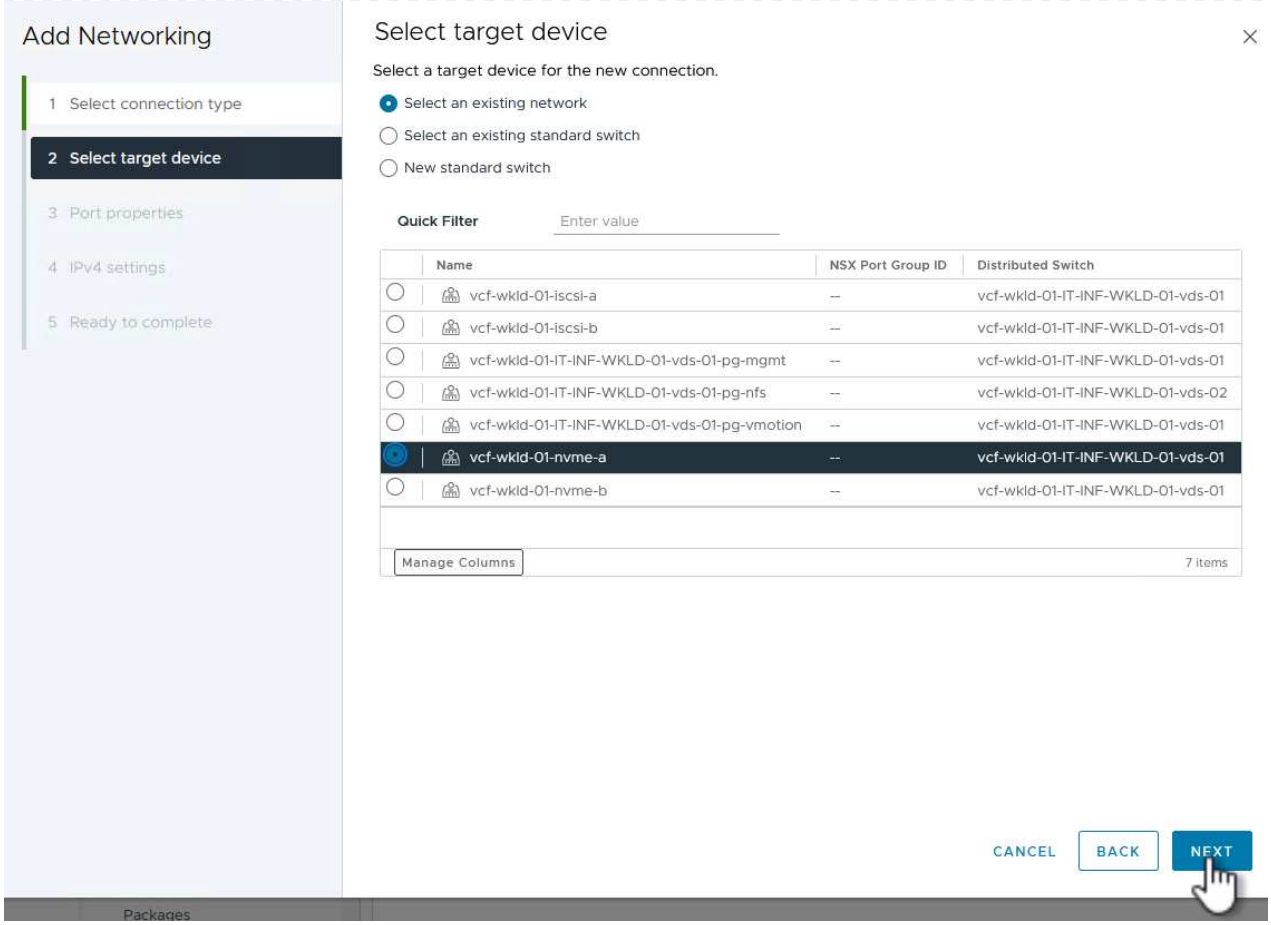
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configure** selezionare **VMkernel adapters** e fare clic su **Add Networking…** per iniziare.



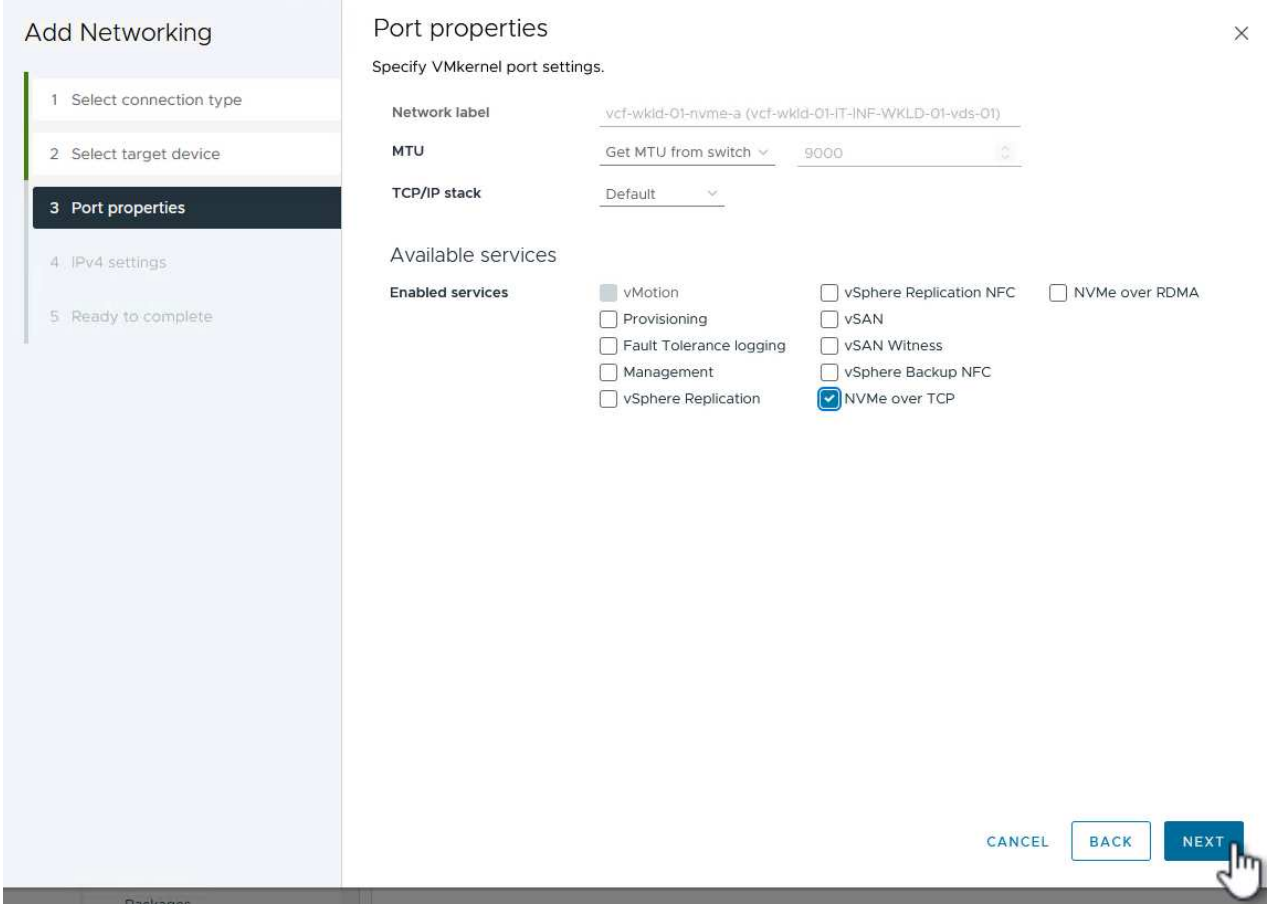
2. Nella finestra **Select Connection type** (Seleziona tipo di connessione), scegliere **VMkernel Network Adapter** (scheda di rete VMkernel) e fare clic su **Next** (Avanti) per continuare.



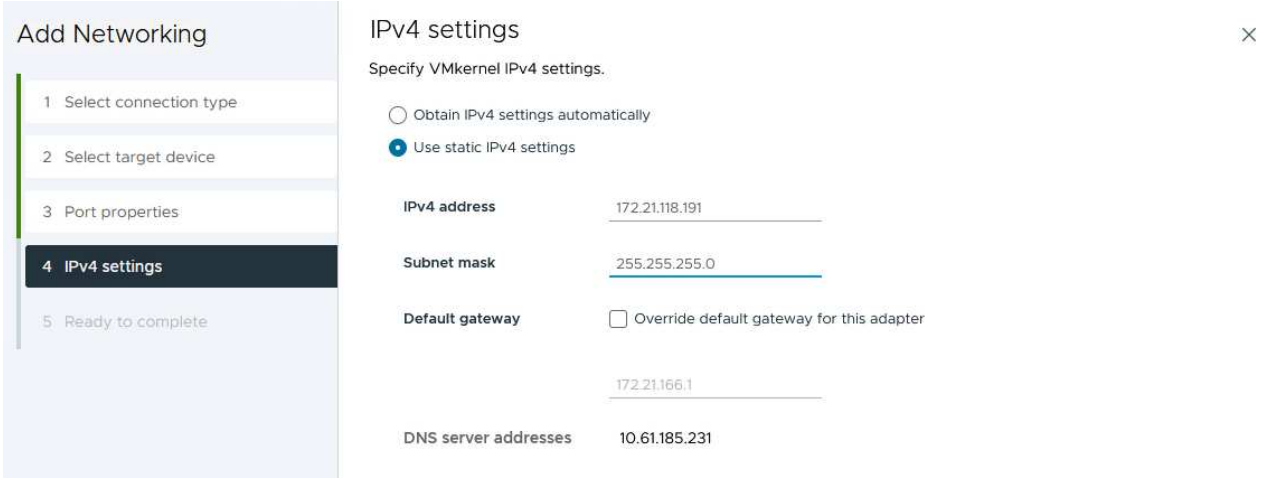
3. Nella pagina **Seleziona dispositivo di destinazione**, scegliere uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



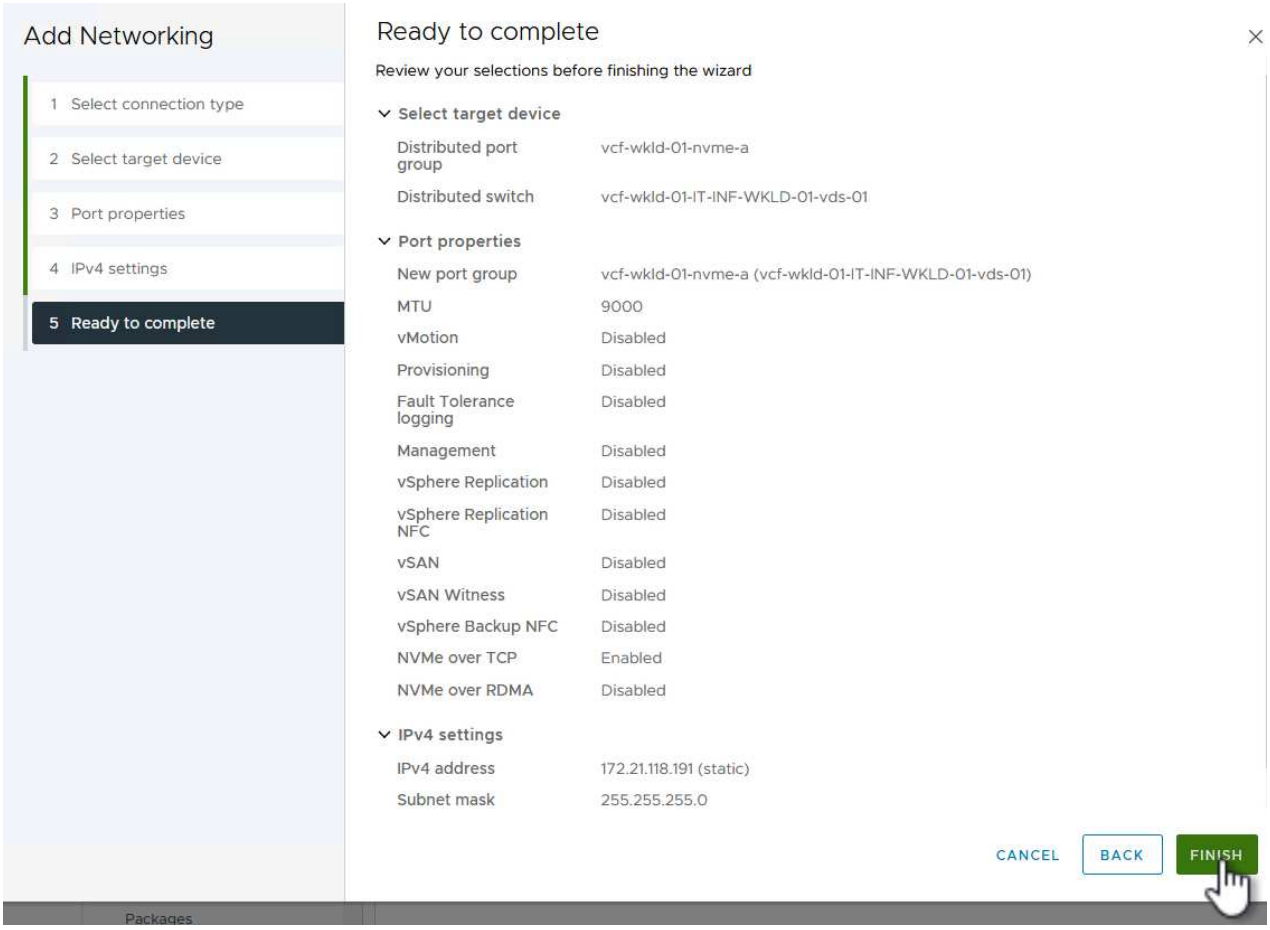
4. Nella pagina **Proprietà porta** fare clic sulla casella **NVMe su TCP** e fare clic su **Avanti** per continuare.



5. Nella pagina **IPv4 settings** compilare i campi **IP address**, **Subnet mask** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.



6. Rivedere le selezioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare l'adattatore VMkernel.



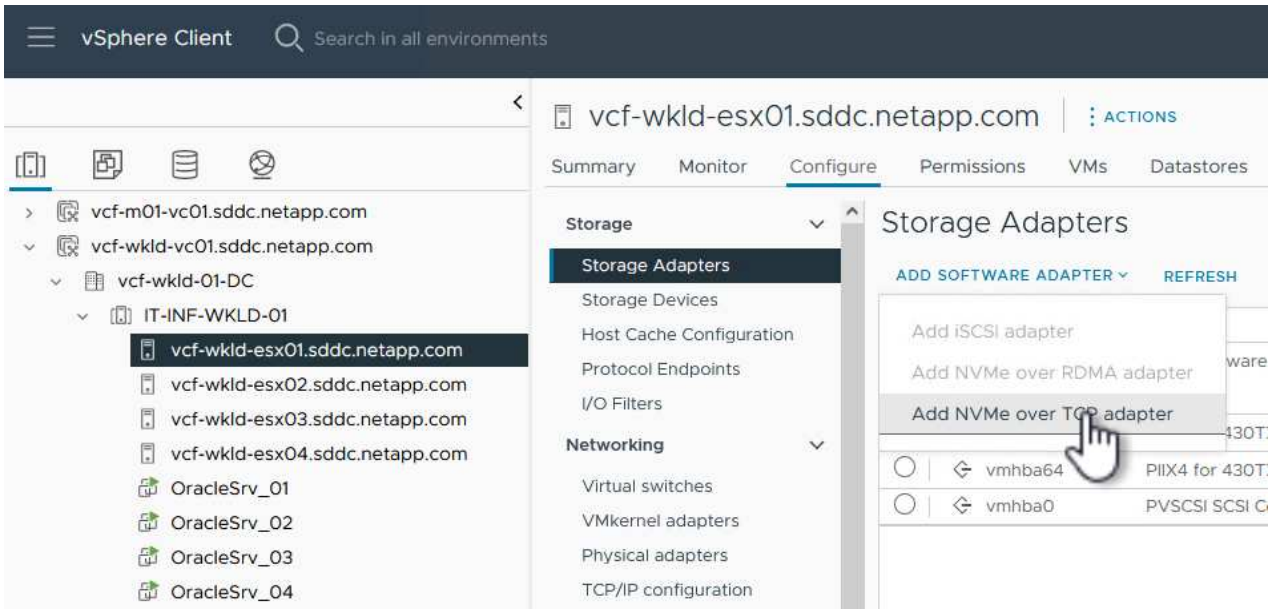
7. Ripetere questa procedura per creare un adattatore VMkernel per la seconda rete iSCSI.

Aggiungi adattatore NVMe over TCP

Ogni host ESXi nel cluster del dominio del carico di lavoro deve avere installato un adattatore software NVMe over TCP per ogni rete NVMe/TCP consolidata dedicata al traffico storage.

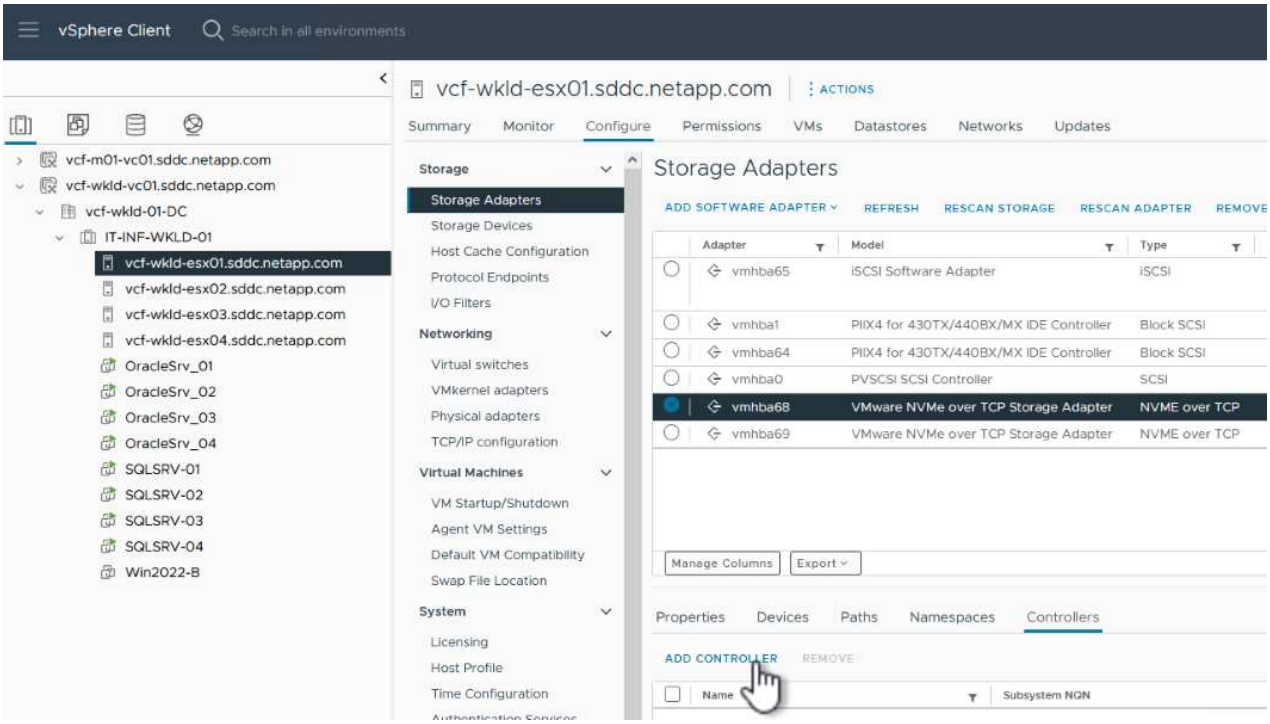
Per installare gli adattatori NVMe over TCP e rilevare i controller NVMe, attenersi alla seguente procedura:

1. Nel client vSphere, accedere a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dalla scheda **Configure** (Configura), fare clic su **Storage Adapters** (schede di memoria) nel menu a discesa **Add Software Adapter** (Aggiungi scheda software) e selezionare **Add NVMe over TCP adapter** (Aggiungi scheda NVMe su TCP).

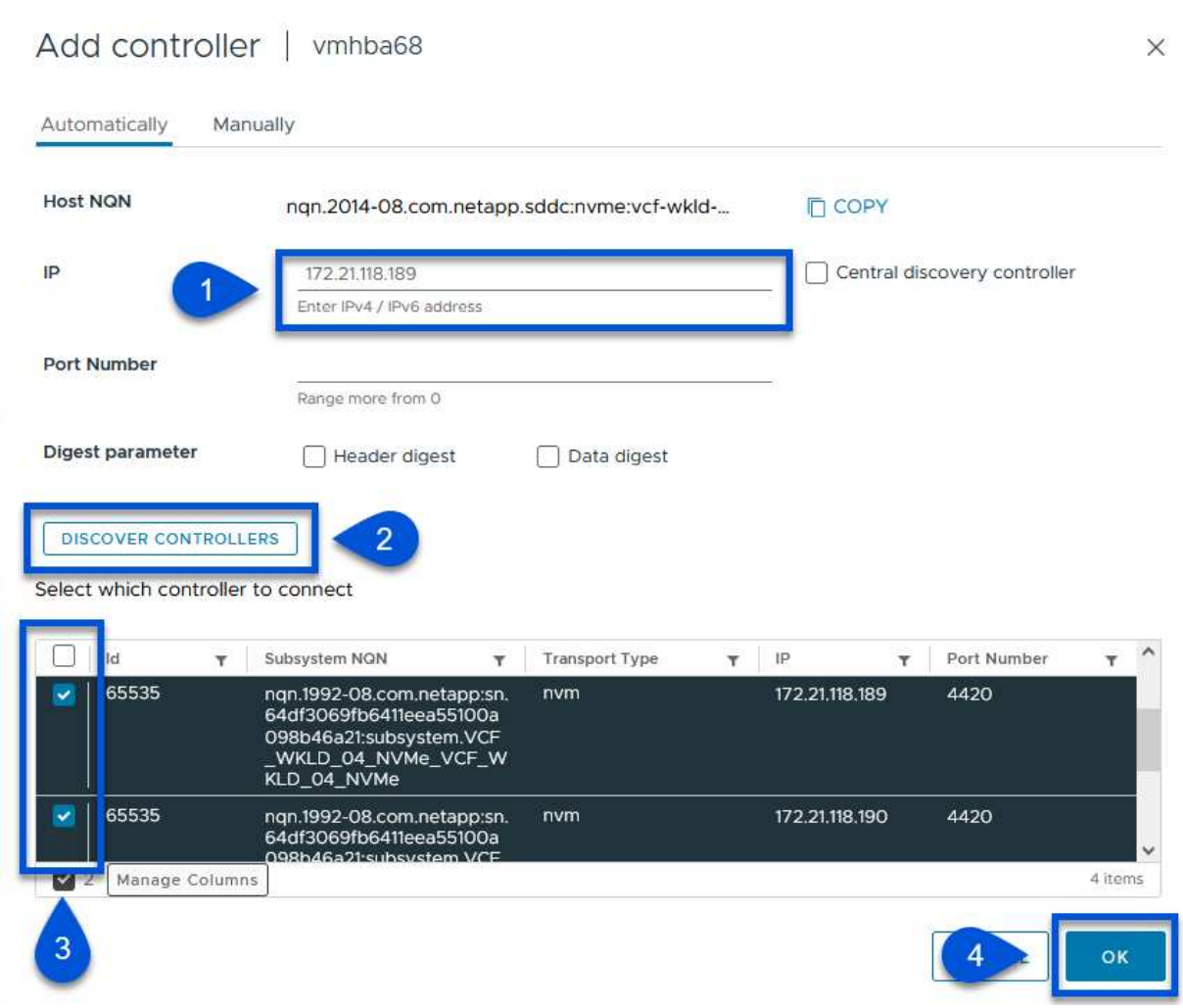


2. Nella finestra **Add Software NVMe over TCP adapter** (Aggiungi adattatore NVMe su TCP), accedere al menu a discesa **Physical Network Adapter** (scheda di rete fisica) e selezionare l'adattatore di rete fisico corretto su cui abilitare l'adattatore NVMe.

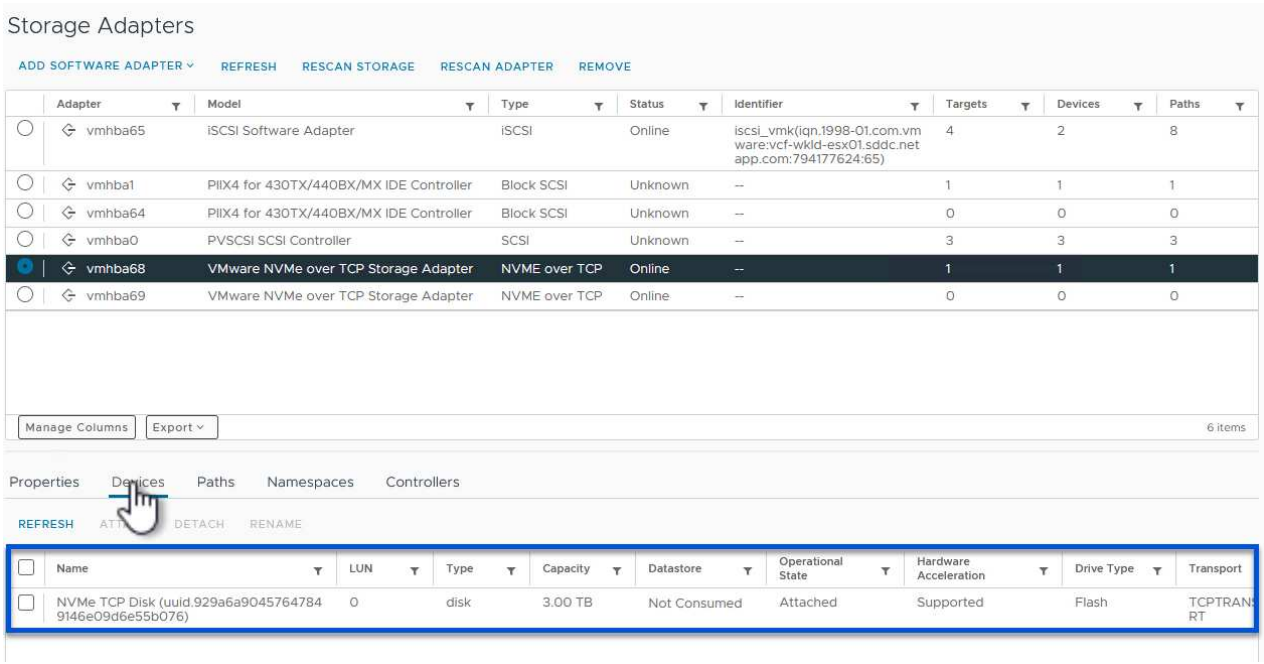
3. Ripetere questa procedura per la seconda rete assegnata al traffico NVMe su TCP, assegnando l'adattatore fisico corretto.
4. Selezionare una delle schede NVMe over TCP appena installate e, nella scheda **Controller**, selezionare **Aggiungi controller**.



5. Nella finestra **Aggiungi controller**, selezionare la scheda **automaticamente** e completare i seguenti passaggi.
   - Immettere gli indirizzi IP per una delle interfacce logiche SVM sulla stessa rete dell'adattatore fisico assegnato a questo adattatore NVMe over TCP.
   - Fare clic sul pulsante **Scopri controller**.
   - Dall'elenco dei controller rilevati, fare clic sulla casella di controllo per i due controller con indirizzi di rete allineati con questo adattatore NVMe over TCP.
   - Fare clic sul pulsante **OK** per aggiungere i controller selezionati.



6. Dopo qualche secondo dovresti vedere il namespace NVMe nella scheda Devices (dispositivi).

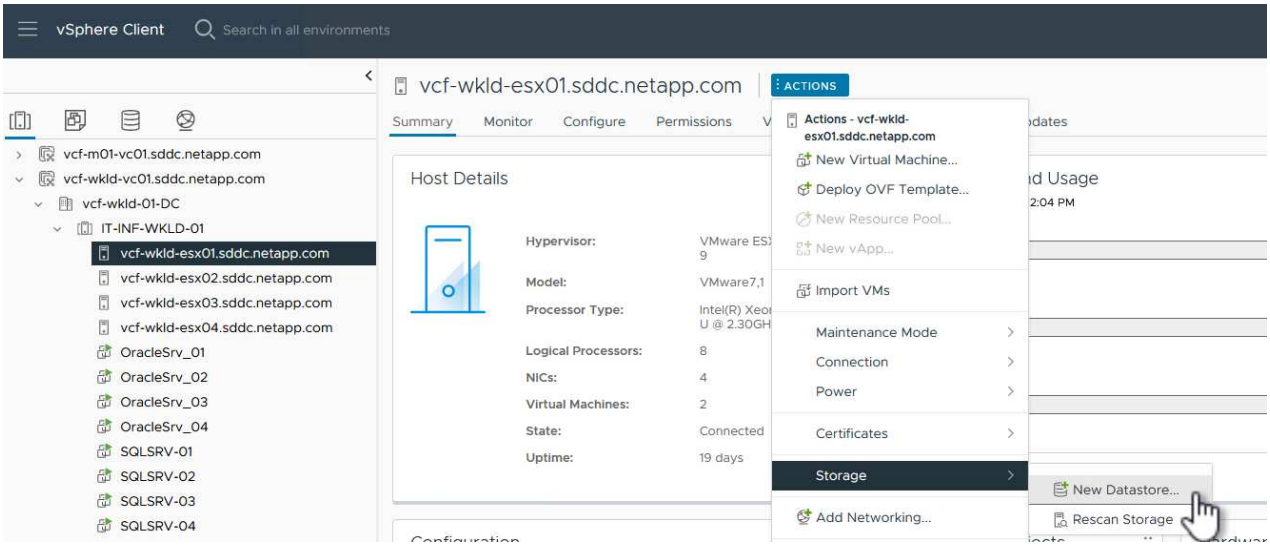


7. Ripetere questa procedura per creare un adattatore NVMe over TCP per la seconda rete stabilita per il traffico NVMe/TCP.

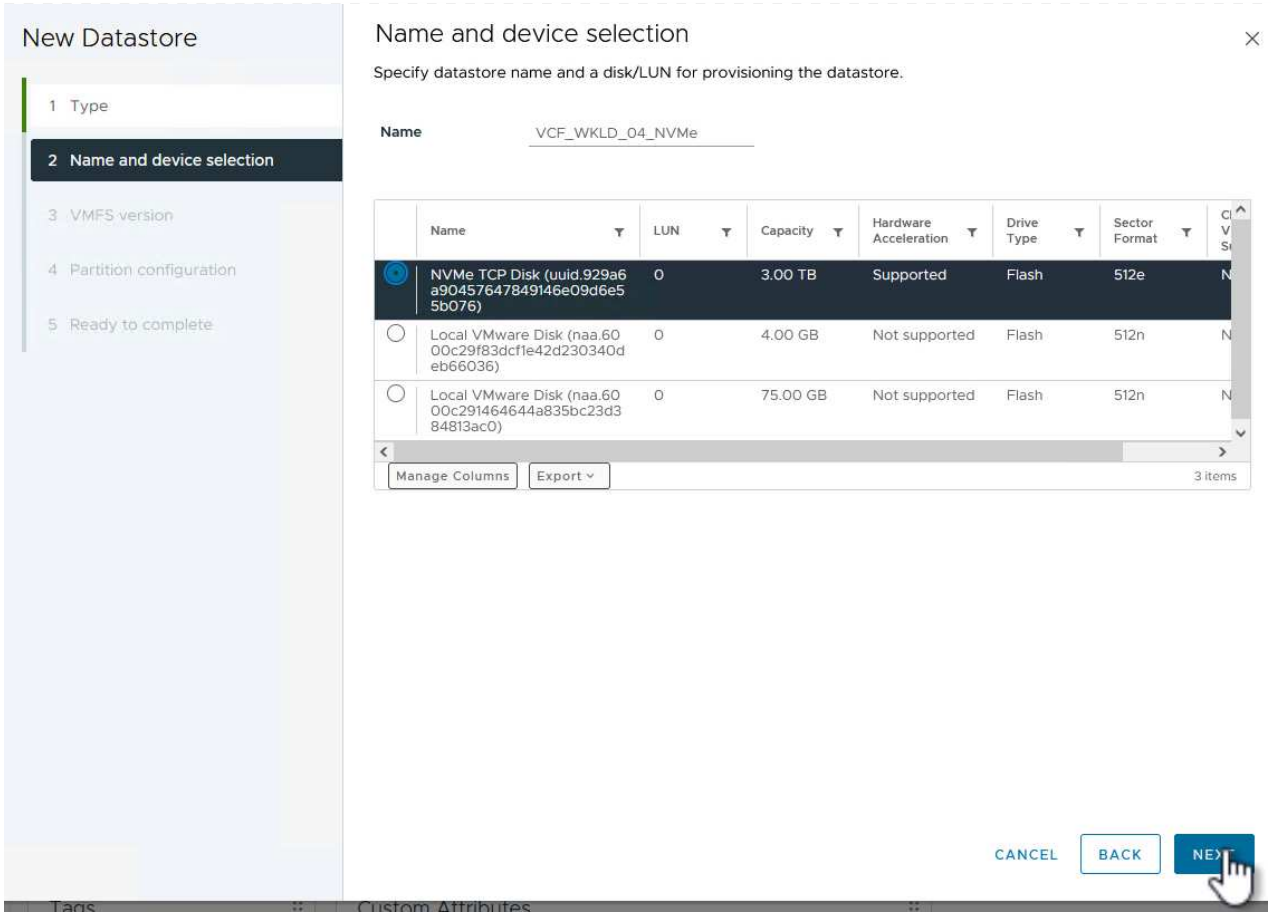
Implementa datastore NVMe su TCP

Per creare un datastore VMFS nel namespace NVMe, completa i seguenti passaggi:

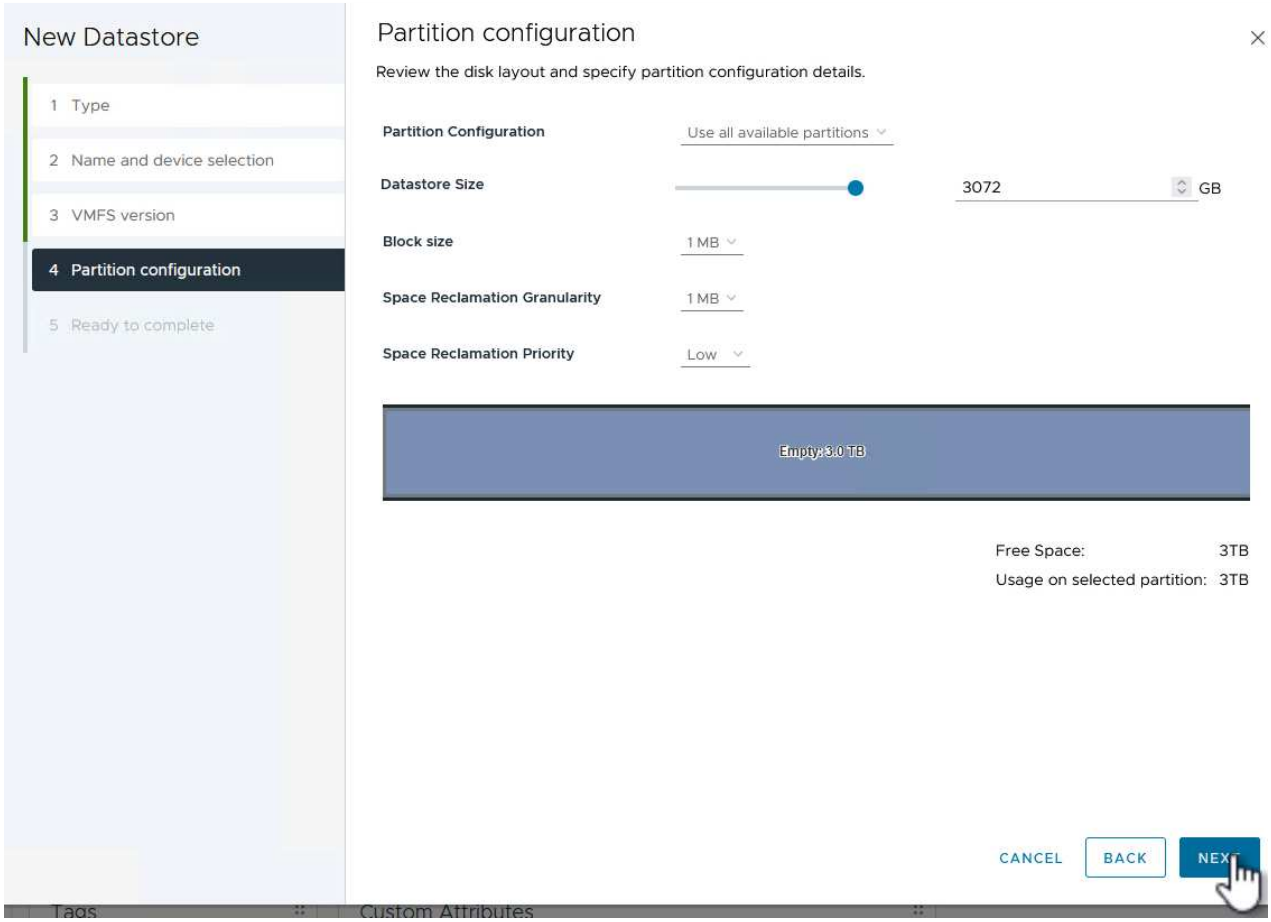
1. Nel client vSphere, accedere a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dal menu **azioni**, selezionare **archiviazione > nuovo archivio dati…**.



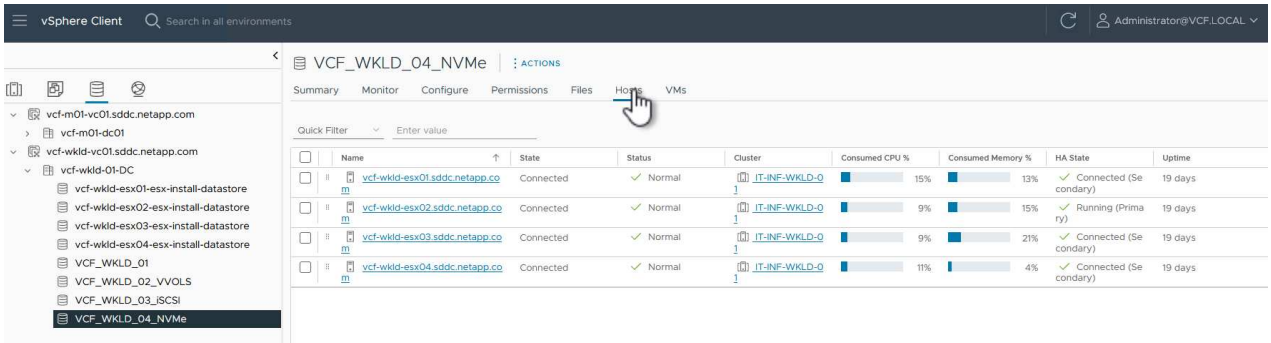
2. Nella procedura guidata **nuovo datastore**, selezionare **VMFS** come tipo. Fare clic su **Avanti** per continuare.
3. Nella pagina **selezione nome e dispositivo**, fornire un nome per l'archivio dati e selezionare lo spazio dei nomi NVMe dall'elenco dei dispositivi disponibili.



4. Nella pagina **VMFS versione** selezionare la versione di VMFS per il datastore.
5. Nella pagina **Partition Configuration**, apportare le modifiche desiderate allo schema di partizione predefinito. Fare clic su **Avanti** per continuare.



6. Nella pagina **Pronto per il completamento**, rivedere il riepilogo e fare clic su **fine** per creare il datastore.
7. Accedere al nuovo datastore nell'inventario e fare clic sulla scheda **hosts**. Se configurato correttamente, tutti gli host ESXi nel cluster devono essere elencati e avere accesso al nuovo datastore.



Ulteriori informazioni

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Utilizza il plug-in SnapCenter per VMware vSphere per proteggere le VM nei domini del carico di lavoro VCF

In questo scenario dimostreremo come implementare e utilizzare il plug-in SnapCenter per VMware vSphere (SCV) per eseguire il backup e il ripristino di VM e datastore in un dominio di carico di lavoro VCF. SCV utilizza la tecnologia Snapshot di ONTAP per eseguire copie di backup veloci ed efficienti dei volumi di storage ONTAP che ospitano i datastore vSphere. Le tecnologie SnapMirror e SnapVault vengono utilizzate per creare backup secondari su un sistema storage separato e con policy di conservazione che simulano il volume originale o possono essere indipendenti dal volume originale per la conservazione a lungo termine.

ISCSI viene utilizzato come protocollo storage per il datastore VMFS in questa soluzione.

Autore: Josh Powell

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

- Distribuire il plug-in SnapCenter per VMware vSphere (SCV) nel dominio del carico di lavoro VI.
- Aggiungere i sistemi di stoccaggio al distributore idraulico.
- Creare criteri di backup in SCV.
- Creare gruppi di risorse in SCV.
- Utilizzare SCV per eseguire il backup di datastore o macchine virtuali specifiche.
- Utilizzare SCV per ripristinare le macchine virtuali in una posizione alternativa nel quadro strumenti.
- Utilizzare SCV per ripristinare i file in un file system Windows.

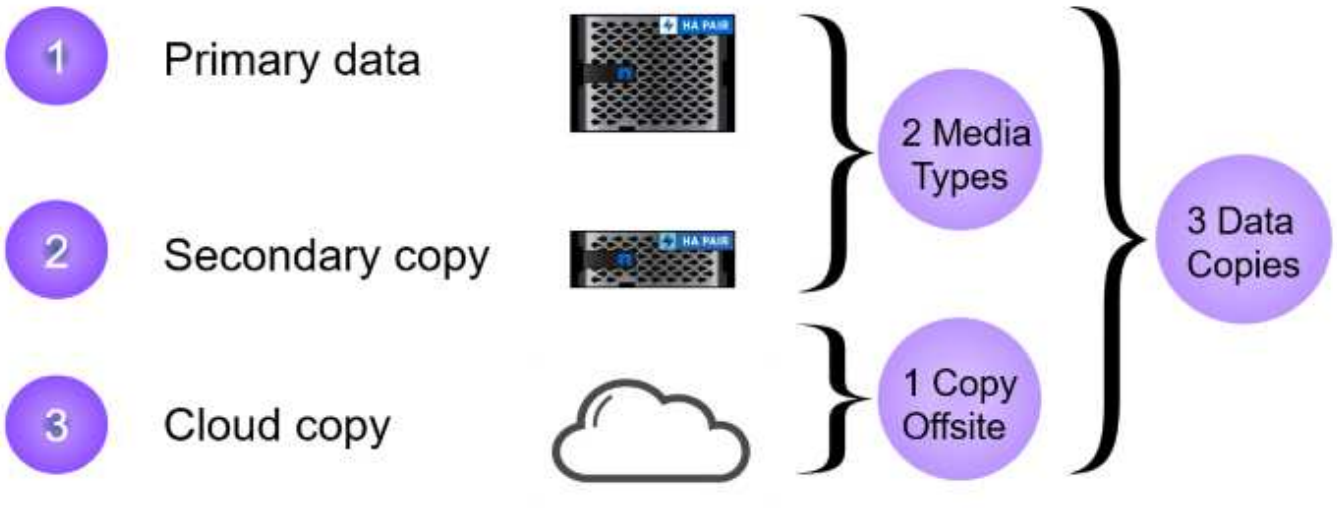
Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con archivi dati VMFS iSCSI allocati al cluster di dominio del carico di lavoro.
- Un sistema di storage ONTAP secondario configurato per ricevere backup secondari utilizzando SnapMirror.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.
- Le macchine virtuali sono presenti sul gruppo SCV è designato come protezione.

Per informazioni sulla configurazione degli archivi dati VMFS iSCSI come storage supplementare, fare riferimento a. **"ISCSI come archiviazione supplementare per i domini di gestione"** ivi descritti. Il processo per utilizzare OTV per implementare i datastore è identico per i domini di gestione e carico di lavoro.

Oltre alla replica dei backup eseguiti con SCV nello storage secondario, è possibile realizzare copie offsite dei dati nello storage a oggetti su uno dei tre (3) cloud provider leader, utilizzando il backup e recovery di NetApp BlueXP per le VM. Per ulteriori informazioni, consultare la soluzione "Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM".



Fasi di implementazione

Per implementare il plug-in SnapCenter e utilizzarlo per creare backup e ripristinare macchine virtuali e datastore, attenersi alla seguente procedura:

Distribuire e utilizzare SCV per proteggere i dati in un dominio del carico di lavoro VI

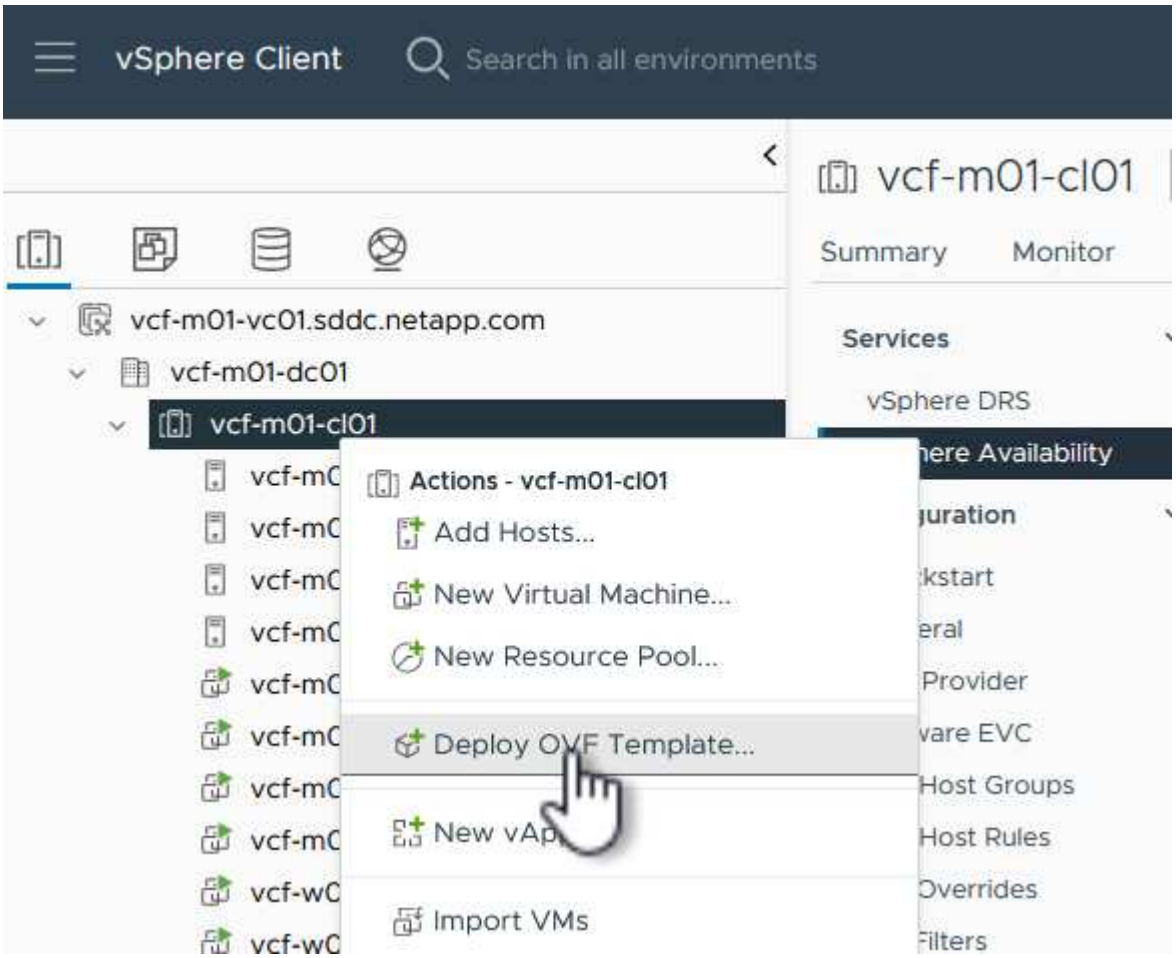
Completare i seguenti passaggi per distribuire, configurare e utilizzare SCV per proteggere i dati in un dominio del carico di lavoro VI:

Implementa il plug-in SnapCenter per VMware vSphere

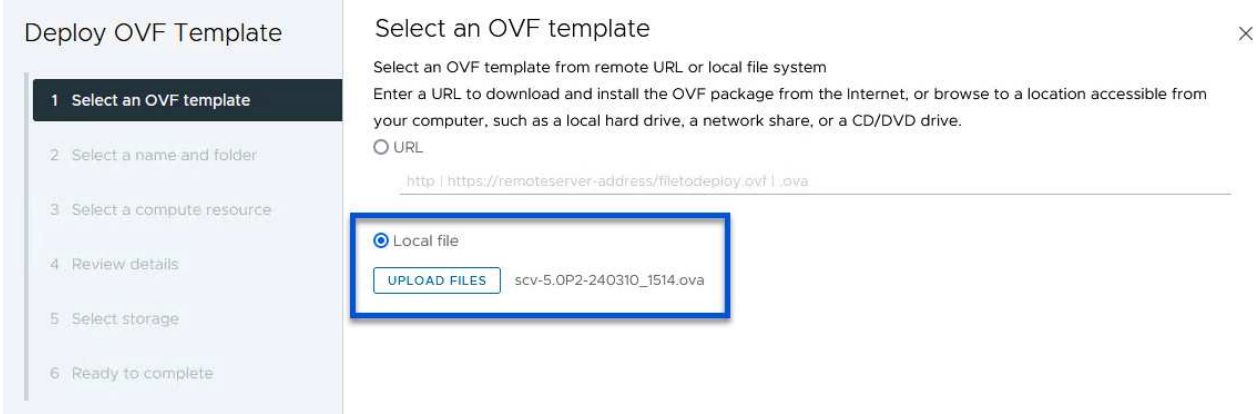
Il plug-in SnapCenter è ospitato nel dominio di gestione VCF ma registrato in vCenter per il dominio del carico di lavoro VI. È necessaria un'istanza SCV per ciascuna istanza di vCenter e, tenere presente che un dominio del carico di lavoro può includere cluster multipli gestiti da una singola istanza di vCenter.

Completare i seguenti passaggi dal client vCenter per distribuire SCV al dominio del carico di lavoro VI:

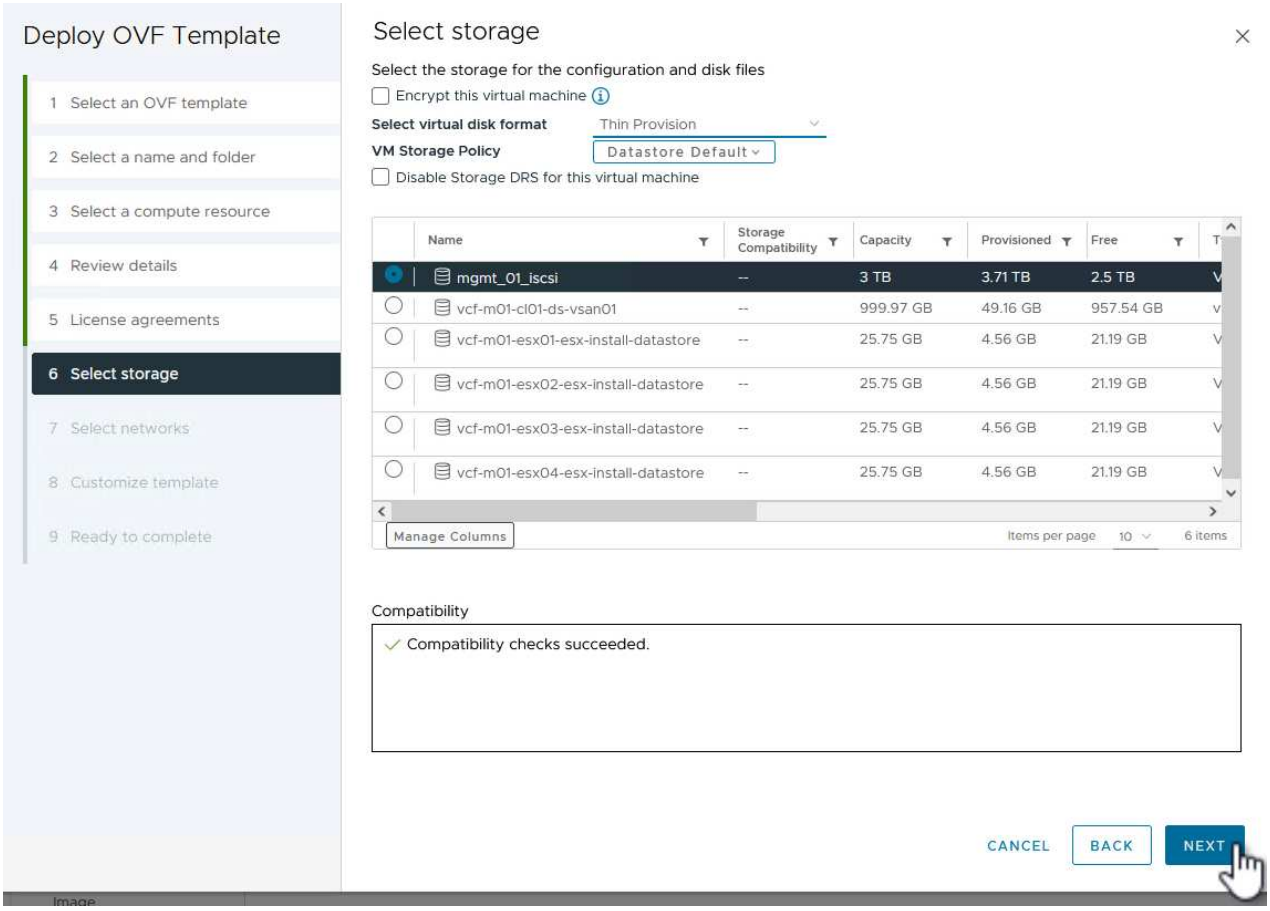
1. Scaricare il file OVA per l'implementazione dei distributori idraulici dall'area di download del sito di assistenza NetApp "**QUI**".
2. Dal client vCenter del dominio di gestione, selezionare **Deploy OVF Template…**.



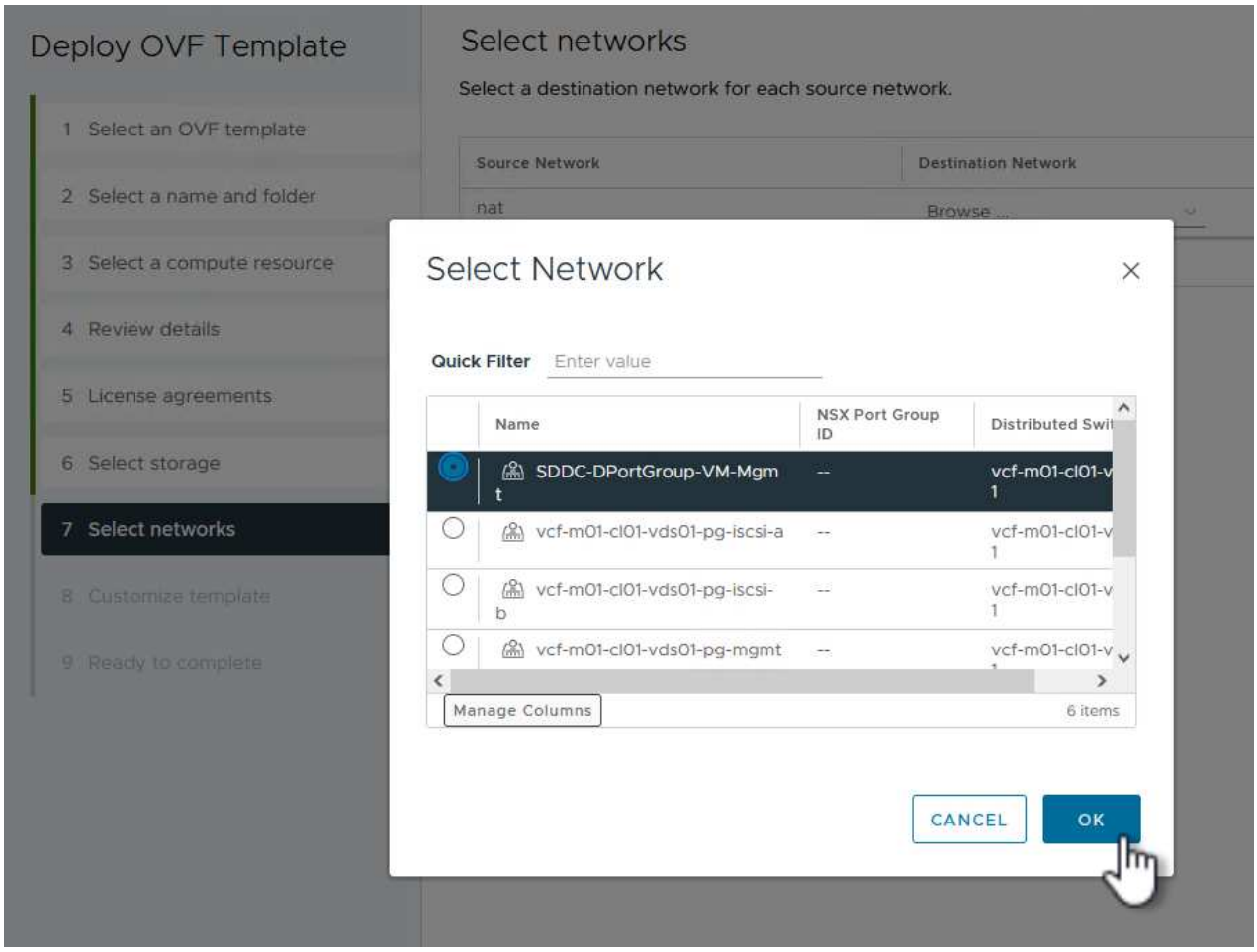
3. Nella procedura guidata **Deploy OVF Template**, fare clic sul pulsante di opzione **Local file**, quindi selezionare per caricare il modello OVF scaricato in precedenza. Fare clic su **Avanti** per continuare.



4. Nella pagina **Select name and folder** (Seleziona nome e cartella*), fornire un nome per la VM del broker di dati SCV e una cartella nel dominio di gestione. Fare clic su **Avanti** per continuare.
5. Nella pagina **selezionare una risorsa di calcolo**, selezionare il cluster del dominio di gestione o l'host ESXi specifico all'interno del cluster in cui installare la VM.
6. Esaminare le informazioni relative al modello OVF nella pagina **Dettagli revisione** e accettare i termini di licenza nella pagina **contratti di licenza**.
7. Nella pagina **Select storage** (Seleziona storage), scegliere il datastore in cui verrà installata la macchina virtuale e selezionare **virtual disk format** (formato disco virtuale) e **VM Storage Policy** (criterio archiviazione VM). In questa soluzione, la macchina virtuale verrà installata in un datastore VMFS iSCSI situato in un sistema storage ONTAP, come precedentemente implementato in una sezione separata di questa documentazione. Fare clic su **Avanti** per continuare.

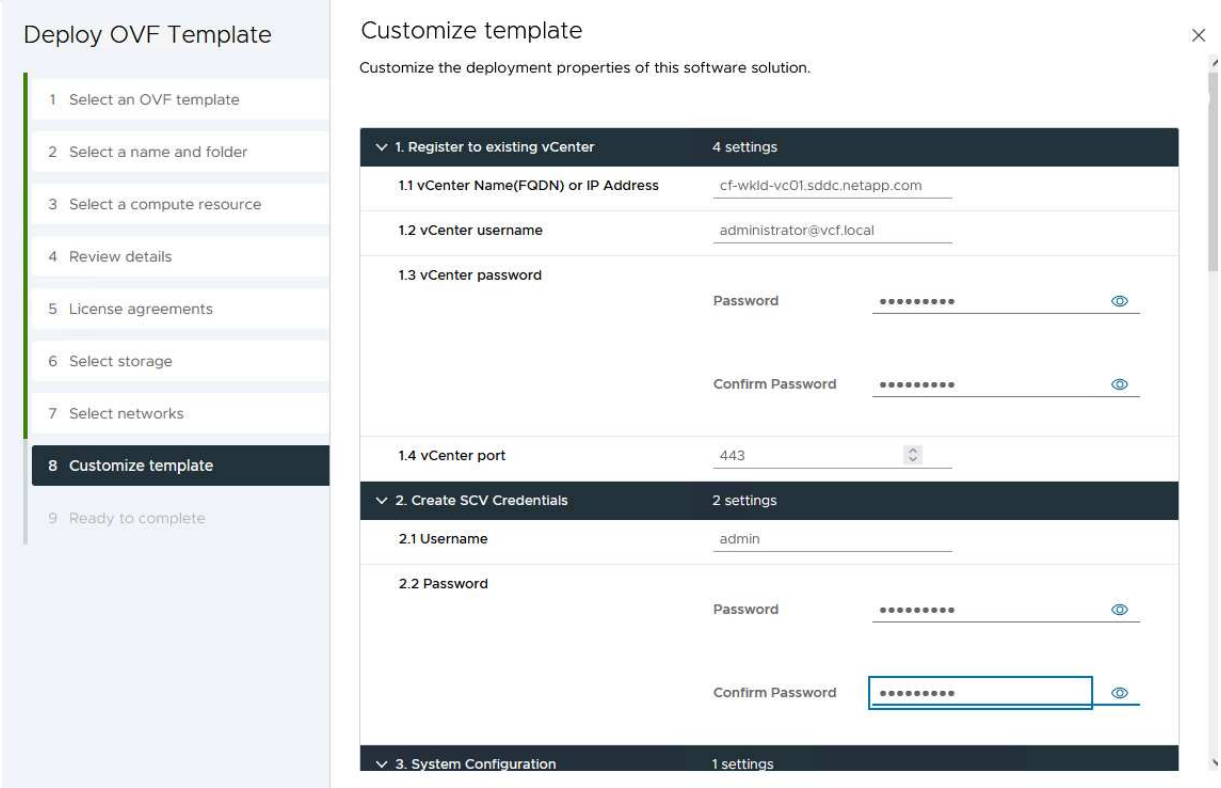


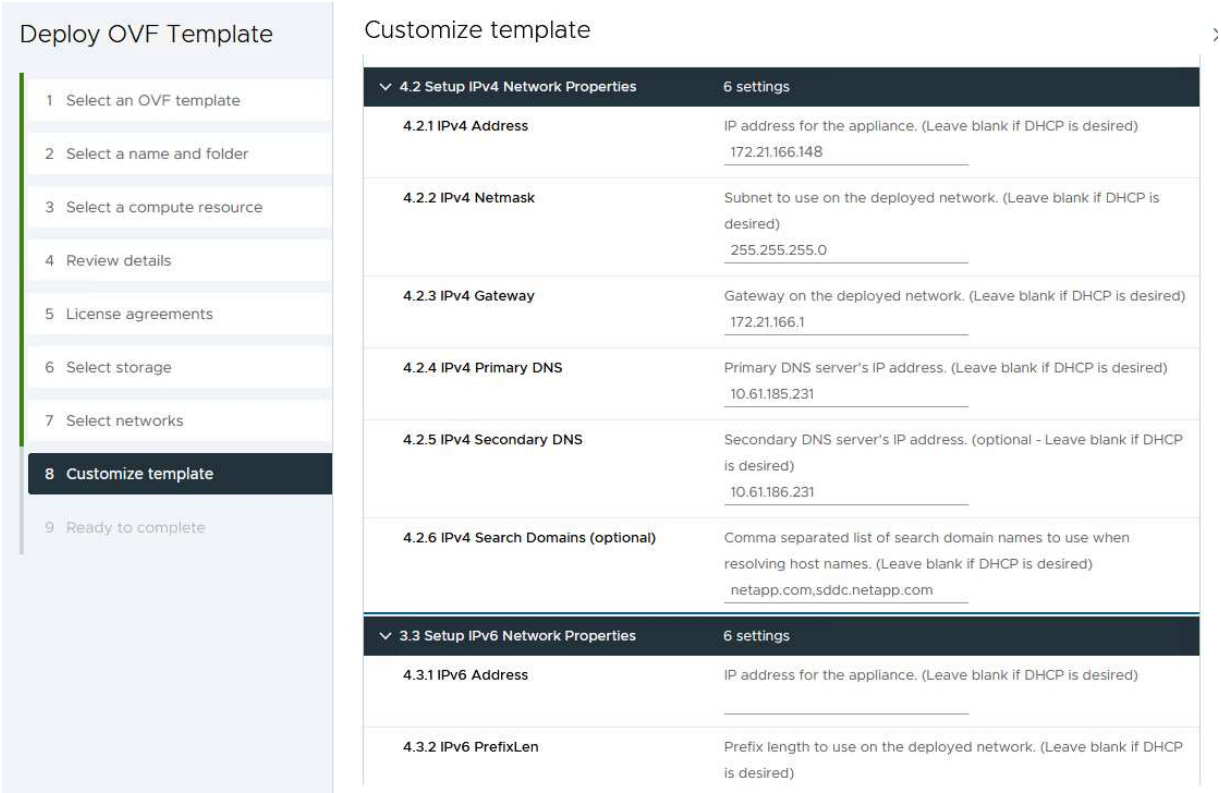
8. Nella pagina **Seleziona rete**, seleziona la rete di gestione in grado di comunicare con l'appliance vCenter del dominio del carico di lavoro e con i sistemi storage ONTAP primari e secondari.

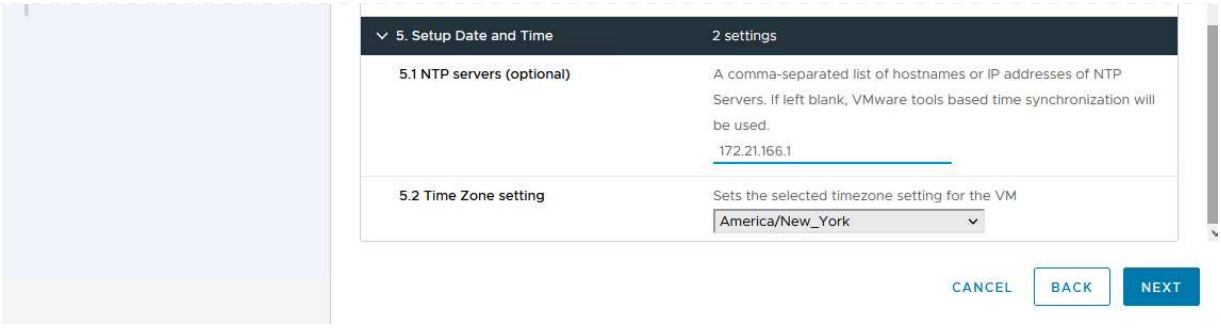


9. Nella pagina **Personalizza modello** compilare tutte le informazioni necessarie per la distribuzione:
   - FQDN o IP e credenziali per l'appliance vCenter del dominio del carico di lavoro.
   - Credenziali per l'account amministrativo SCV.
   - Credenziali per l'account di manutenzione SCV.
   - IPv4 informazioni dettagliate sulle proprietà di rete (è possibile utilizzare anche IPv6).
   - Impostazioni di data e ora.

   Fare clic su **Avanti** per continuare.


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
1. Register to existing vCenter
4 settings
1.1 vCenter Name(FQDN) or IP Address
cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username
administrator@vcf.local
1.3 vCenter password
Password
Confirm Password
1.4 vCenter port
443
2. Create SCV Credentials
2 settings
2.1 Username
admin
2.2 Password
Password
Confirm Password
3. System Configuration
1 settings


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
4.2 Setup IPv4 Network Properties
6 settings
4.2.1 IPv4 Address
IP address for the appliance. (Leave blank if DHCP is desired)
172.21.166.148
4.2.2 IPv4 Netmask
Subnet to use on the deployed network. (Leave blank if DHCP is desired)
255.255.255.0
4.2.3 IPv4 Gateway
Gateway on the deployed network. (Leave blank if DHCP is desired)
172.21.166.1
4.2.4 IPv4 Primary DNS
Primary DNS server's IP address. (Leave blank if DHCP is desired)
10.61.185.231
4.2.5 IPv4 Secondary DNS
Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired)
10.61.186.231
4.2.6 IPv4 Search Domains (optional)
Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired)
netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties
6 settings
4.3.1 IPv6 Address
IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen
Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

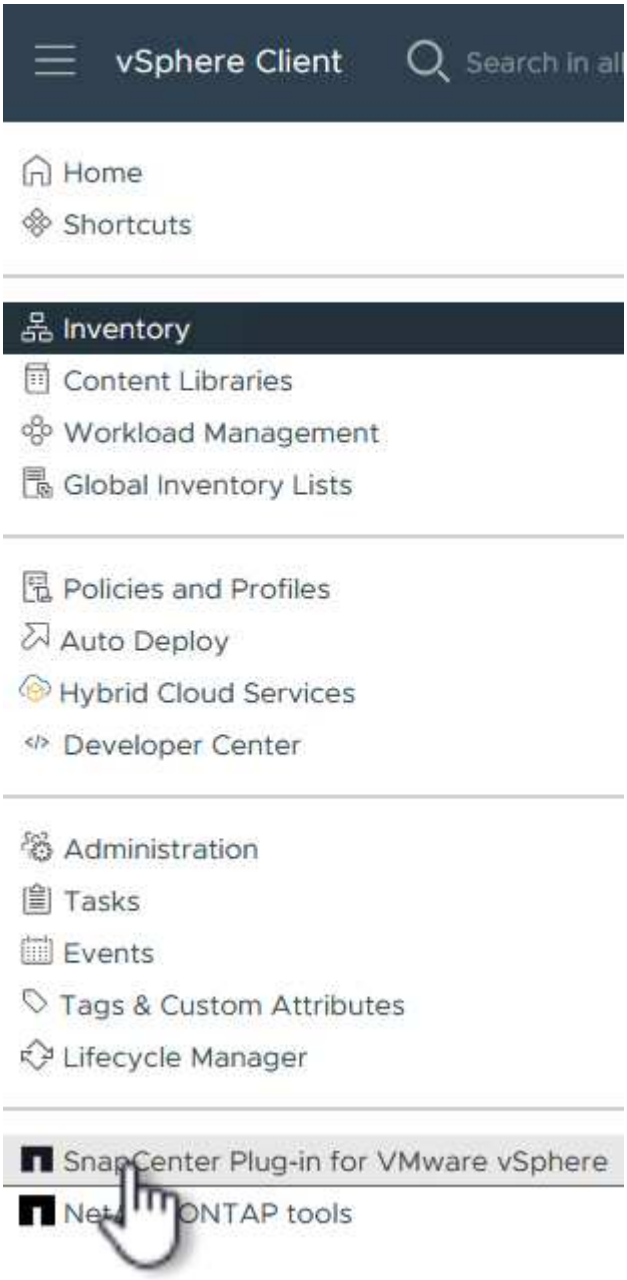


10. Infine, nella pagina **Pronto per il completamento**, esaminare tutte le impostazioni e fare clic su fine per avviare la distribuzione.

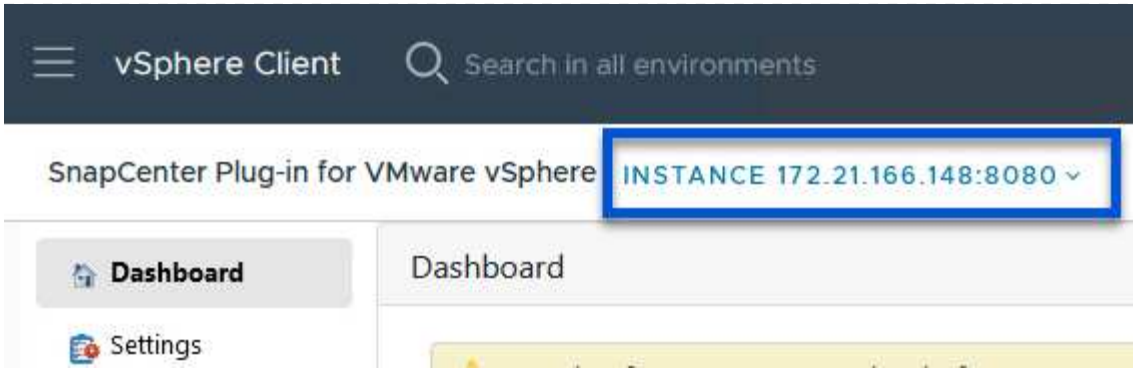
Aggiungere i sistemi di stoccaggio al distributore idraulico

Una volta installato il plug-in SnapCenter, completare i seguenti passaggi per aggiungere i sistemi di stoccaggio al distributore idraulico:

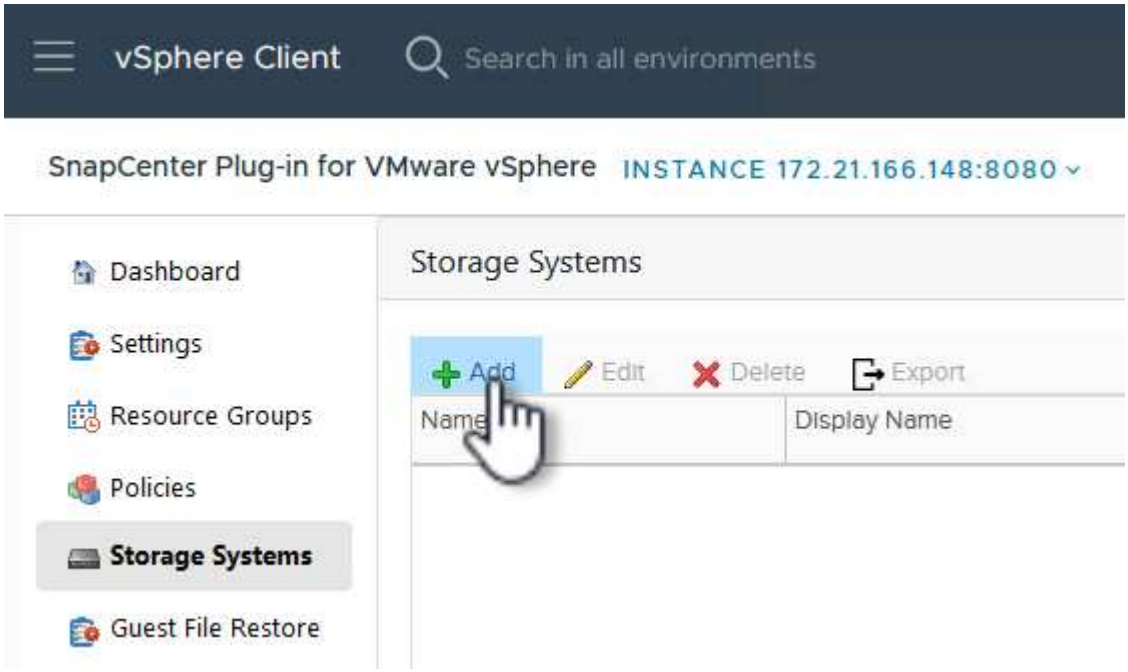
1. SCV è accessibile dal menu principale di vSphere Client.



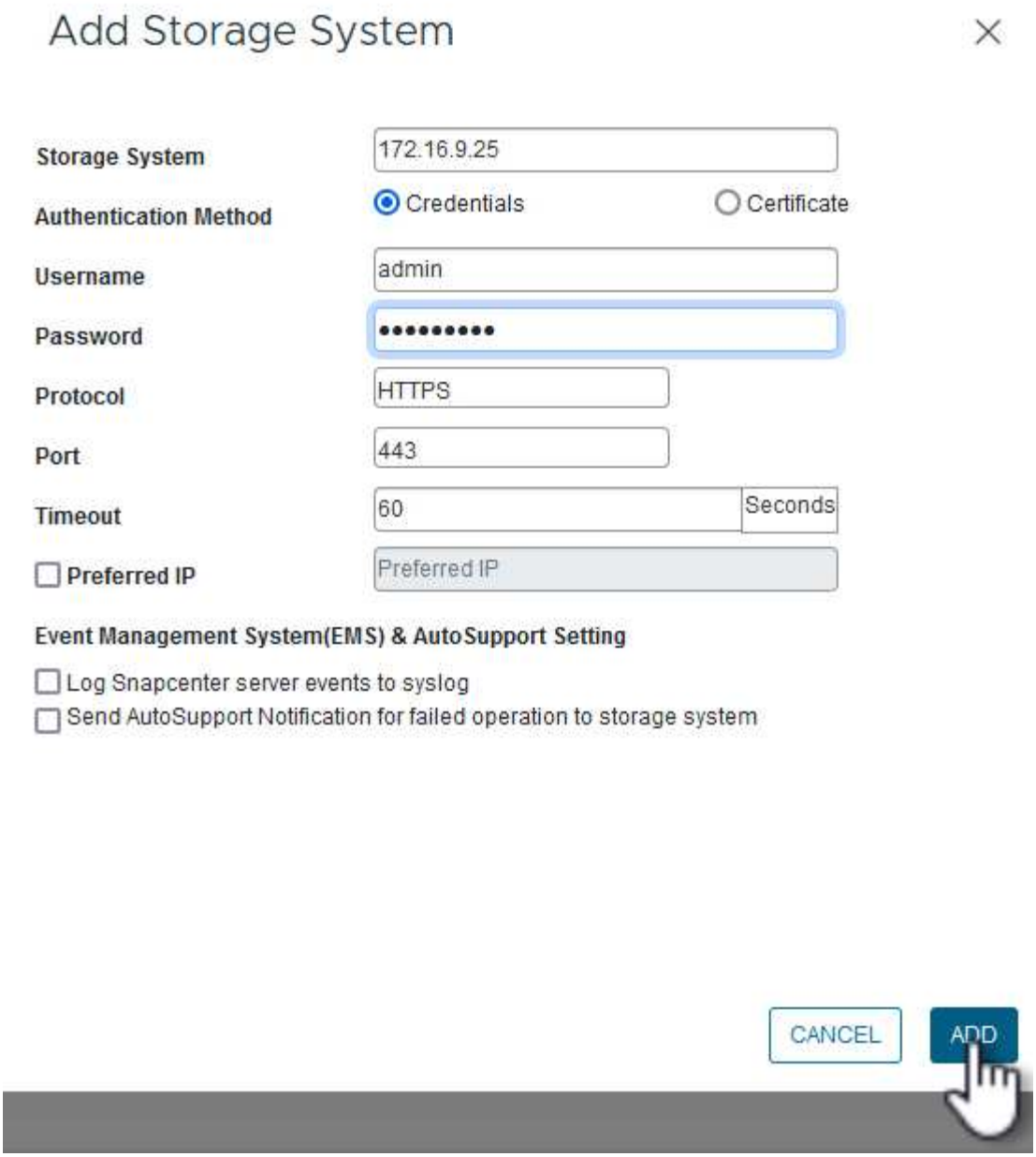
2. Nella parte superiore dell'interfaccia utente SCV, selezionare l'istanza SCV corretta che corrisponde al cluster vSphere da proteggere.



3. Accedere a **Storage Systems** nel menu a sinistra e fare clic su **Add** per iniziare.



4. Nel modulo **Aggiungi sistema di archiviazione**, immettere l'indirizzo IP e le credenziali del sistema di archiviazione ONTAP da aggiungere, quindi fare clic su **Aggiungi** per completare l'azione.



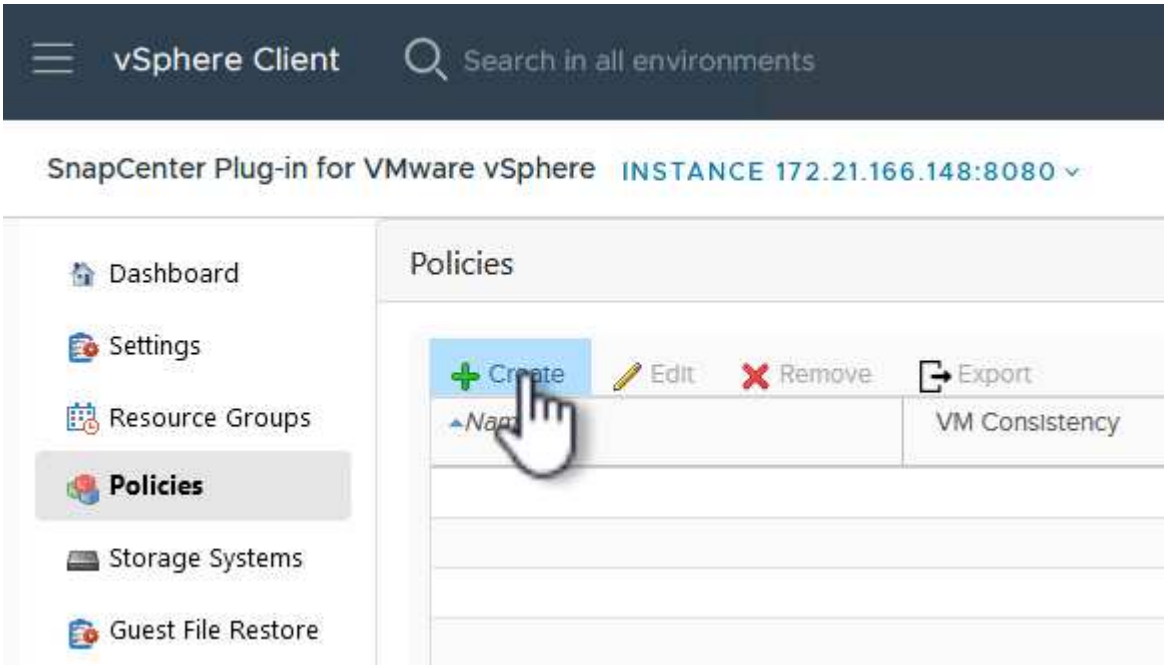
5. Ripetere questa procedura per tutti i sistemi di storage aggiuntivi da gestire, inclusi tutti i sistemi da utilizzare come destinazioni di backup secondarie.

Configurare i criteri di backup in SCV

Per ulteriori informazioni sulla creazione delle politiche di backup dei distributori idraulici, fare riferimento a. "Creare policy di backup per macchine virtuali e datastore".

Completare i seguenti passaggi per creare un nuovo criterio di backup:

1. Dal menu a sinistra, selezionare **Policies** e fare clic su **Create** per iniziare.



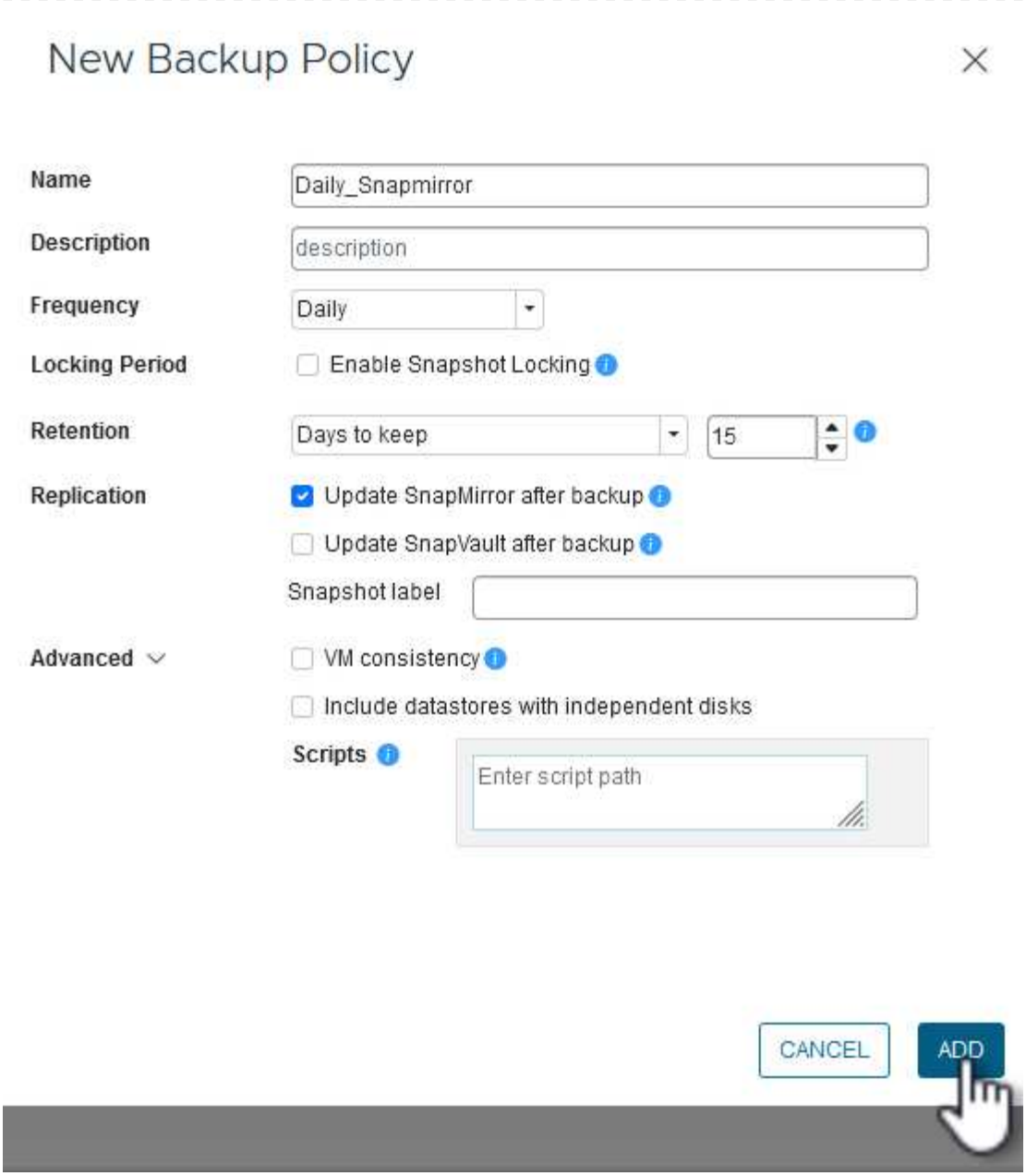
2. Nel modulo **Nuova policy di backup**, fornire un **Nome** e **Descrizione** per il criterio, la **frequenza** in cui verranno eseguiti i backup e il periodo **conservazione** che specifica la durata di conservazione del backup.

   Periodo di blocco abilita la funzione ONTAP SnapLock per creare istantanee antimanomissione e consente la configurazione del periodo di blocco.

   Per **Replica** selezionare per aggiornare le relazioni SnapMirror o SnapVault sottostanti per il volume di storage ONTAP.

   > Le repliche di SnapMirror e SnapVault sono simili in quanto utilizzano la tecnologia ONTAP SnapMirror per replicare in modo asincrono i volumi storage in un sistema storage secondario, per una maggiore protezione e sicurezza. Per le relazioni di SnapMirror, il programma di conservazione specificato nella politica di backup dei distributori idraulici regolerà la conservazione per il volume primario e secondario. Con le relazioni di SnapVault, è possibile stabilire un piano di conservazione separato sul sistema di storage secondario per pianificazioni di conservazione a lungo termine o diverse. In questo caso, l'etichetta dell'istantanea viene specificata nella politica di backup dei distributori idraulici e nella politica associata al volume secondario, per identificare i volumi a cui applicare la pianificazione di conservazione indipendente.

   Scegliere eventuali opzioni avanzate aggiuntive e fare clic su **Aggiungi** per creare il criterio.

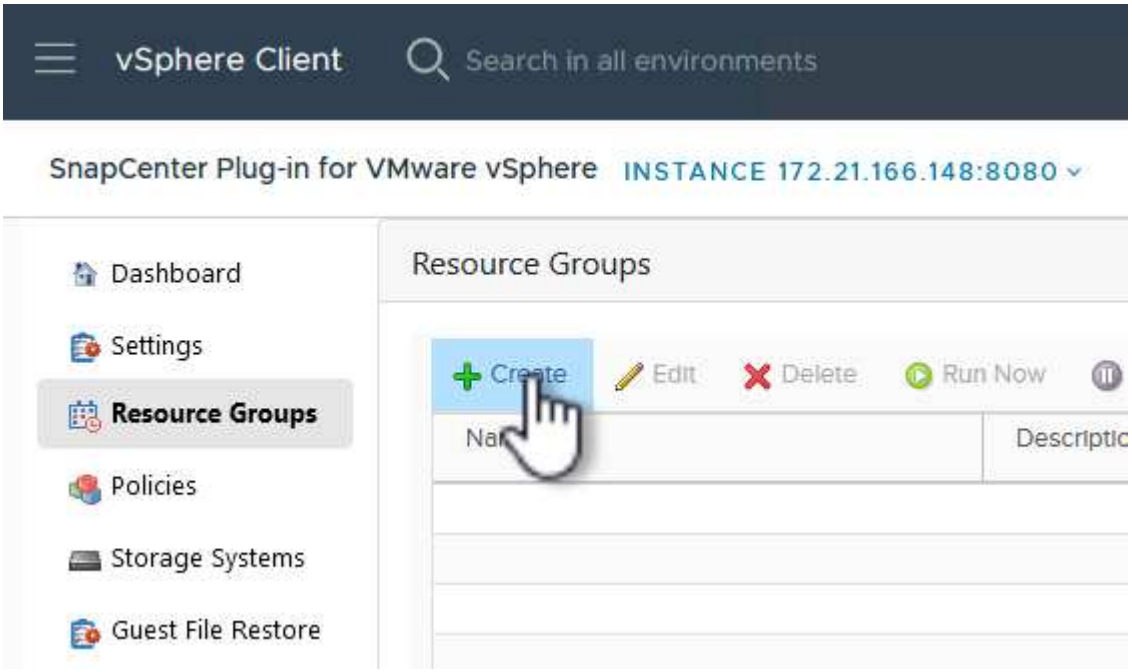

New Backup Policy
Name
Daily_Snapmirror
Description
description
Frequency
Daily
Locking Period
Enable Snapshot Locking
Retention
Days to keep
15
Replication
Update SnapMirror after backup
Update SnapVault after backup
Snapshot label
Advanced
VM consistency
Include datastores with independent disks
Scripts
Enter script path
CANCEL
ADD

Creare gruppi di risorse in SCV

Per ulteriori informazioni sulla creazione di gruppi di risorse SCV, fare riferimento a. "Creare gruppi di risorse".

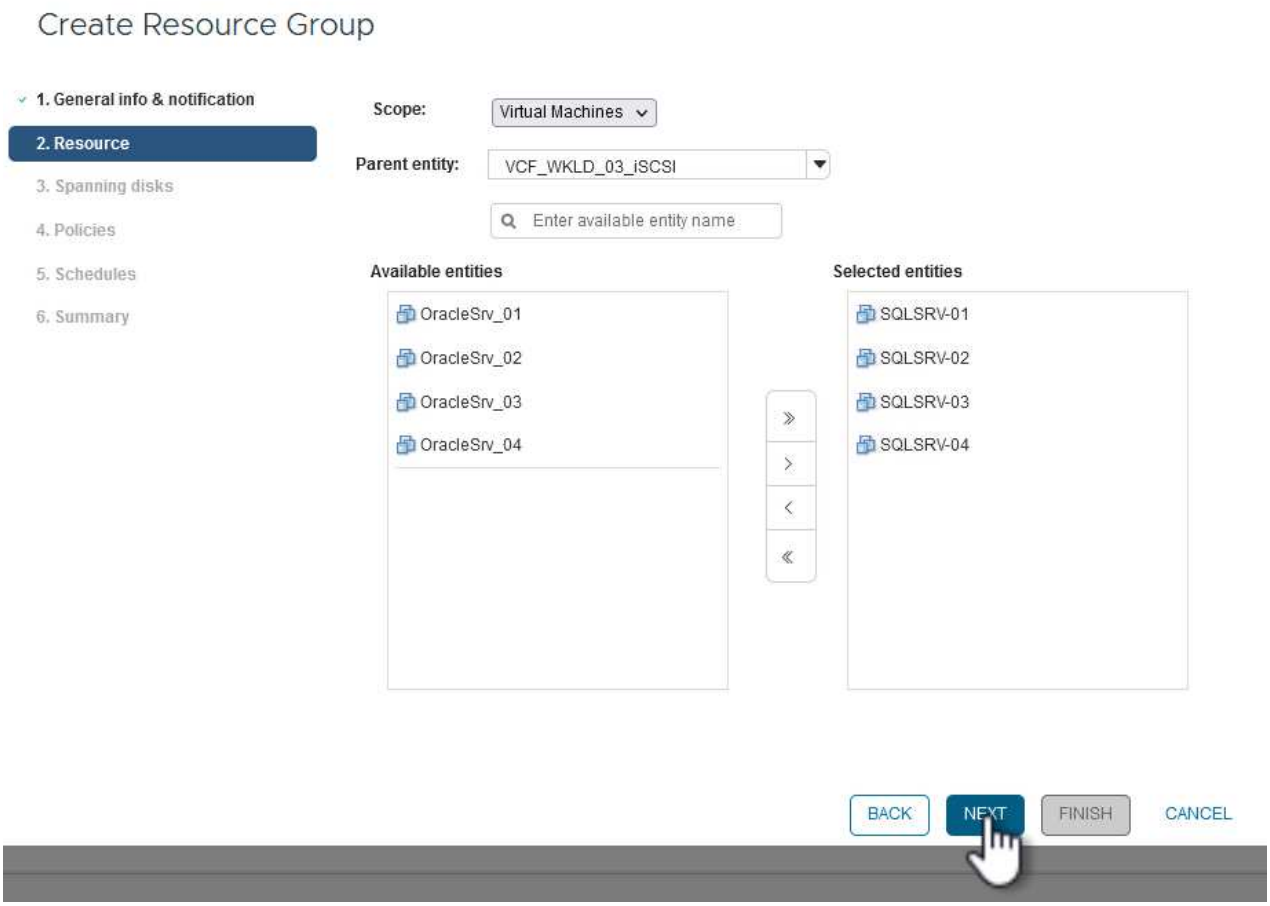
Completare i seguenti passaggi per creare un nuovo gruppo di risorse:

1. Dal menu a sinistra, selezionare **gruppi di risorse** e fare clic su **Crea** per iniziare.

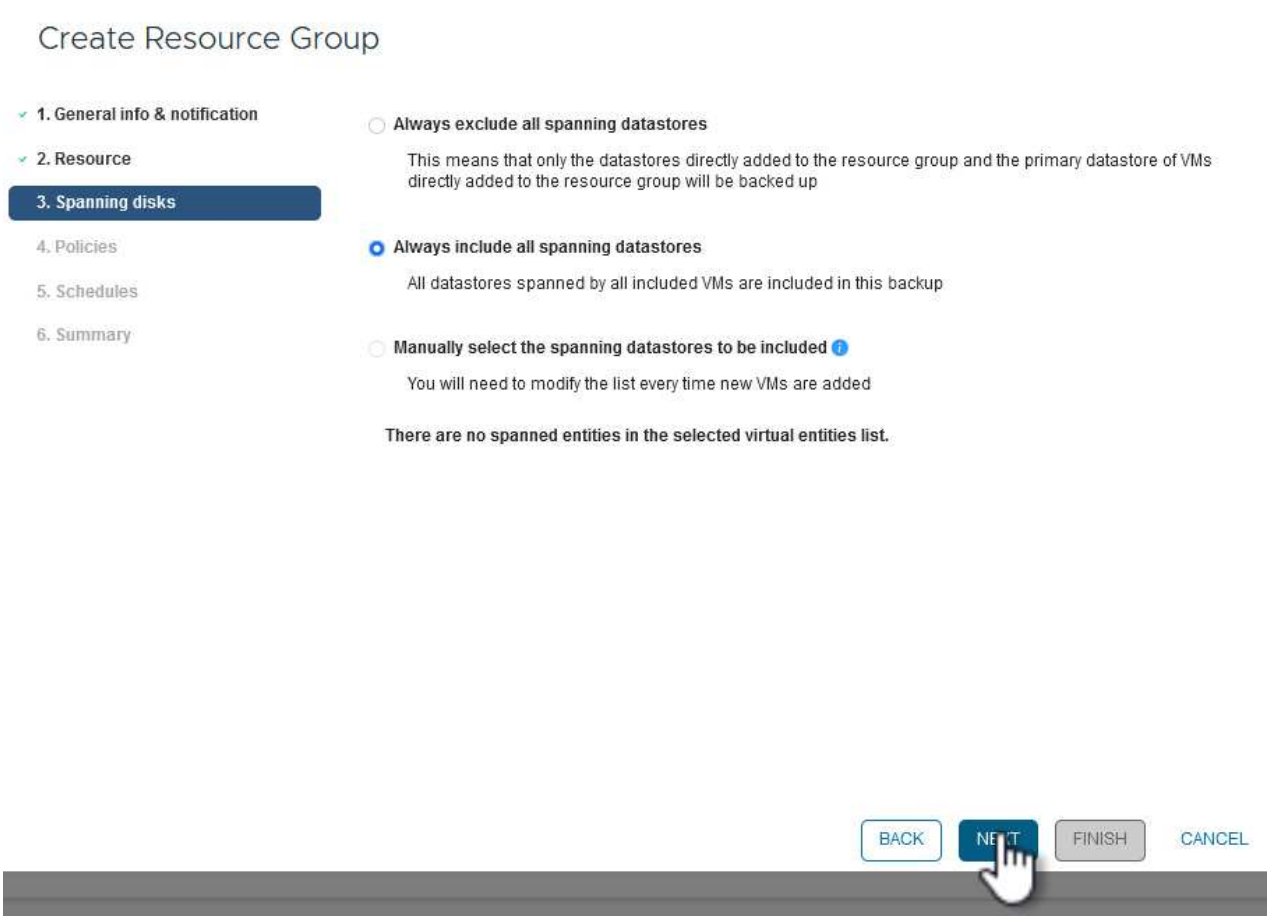


2. Nella pagina **informazioni generali e notifica**, fornire un nome per il gruppo di risorse, le impostazioni di notifica e le eventuali opzioni aggiuntive per la denominazione delle istantanee.
3. Nella pagina **risorsa** selezionare gli archivi dati e le VM da proteggere nel gruppo di risorse. Fare clic su **Avanti** per continuare.

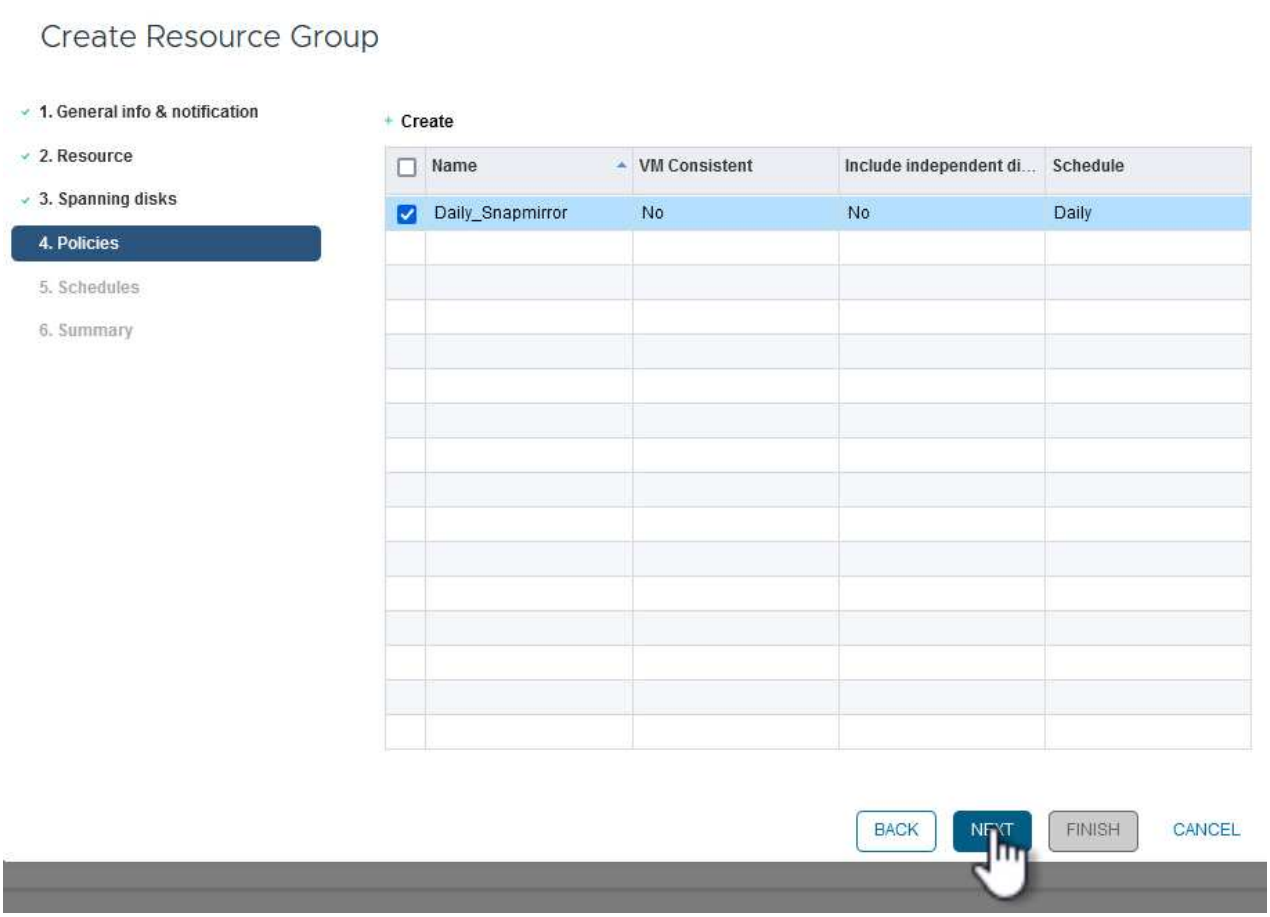
> Anche quando sono selezionate solo macchine virtuali specifiche, viene sempre eseguito il backup dell'intero datastore. Ciò è dovuto al fatto che ONTAP crea snapshot del volume che ospita il datastore. Tuttavia, la selezione solo di macchine virtuali specifiche per il backup limita la possibilità di ripristino solo a queste macchine virtuali.



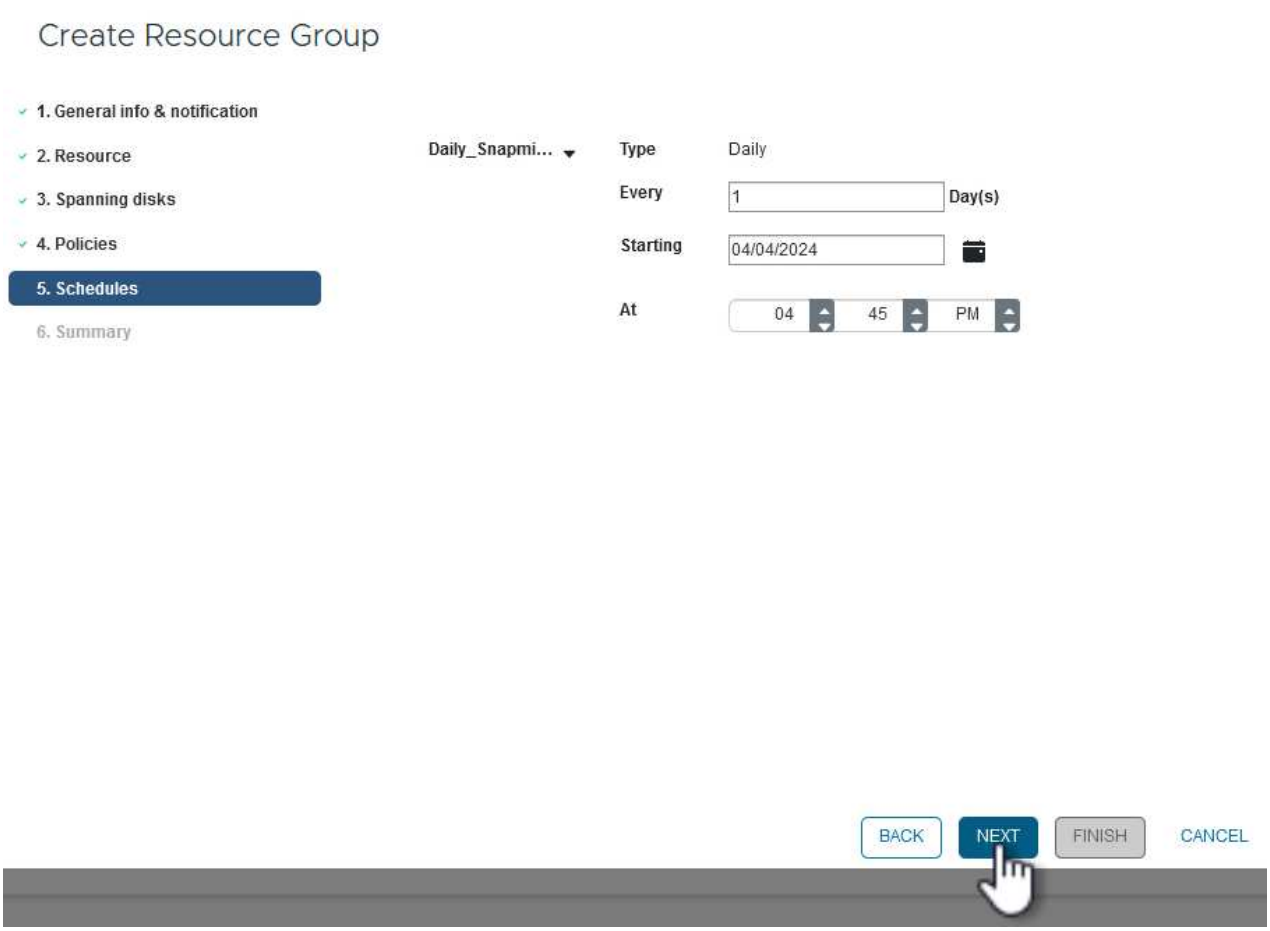
4. Nella pagina **dischi di spanning** selezionare l'opzione per la gestione delle macchine virtuali con VMDK che coprono più archivi dati. Fare clic su **Avanti** per continuare.



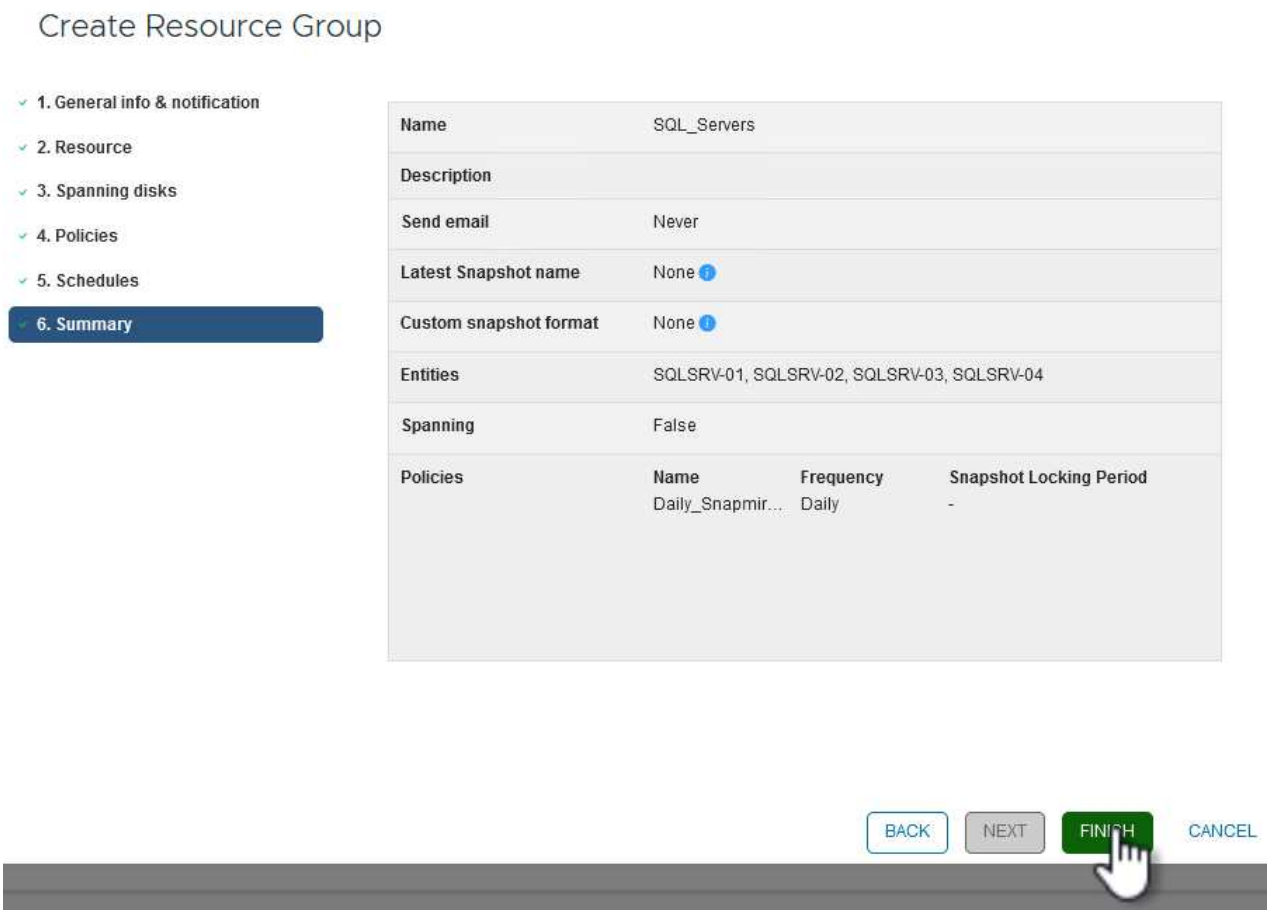
5. Nella pagina **Criteri**, selezionare uno o più criteri creati in precedenza da utilizzare con questo gruppo di risorse. Fare clic su **Avanti** per continuare.



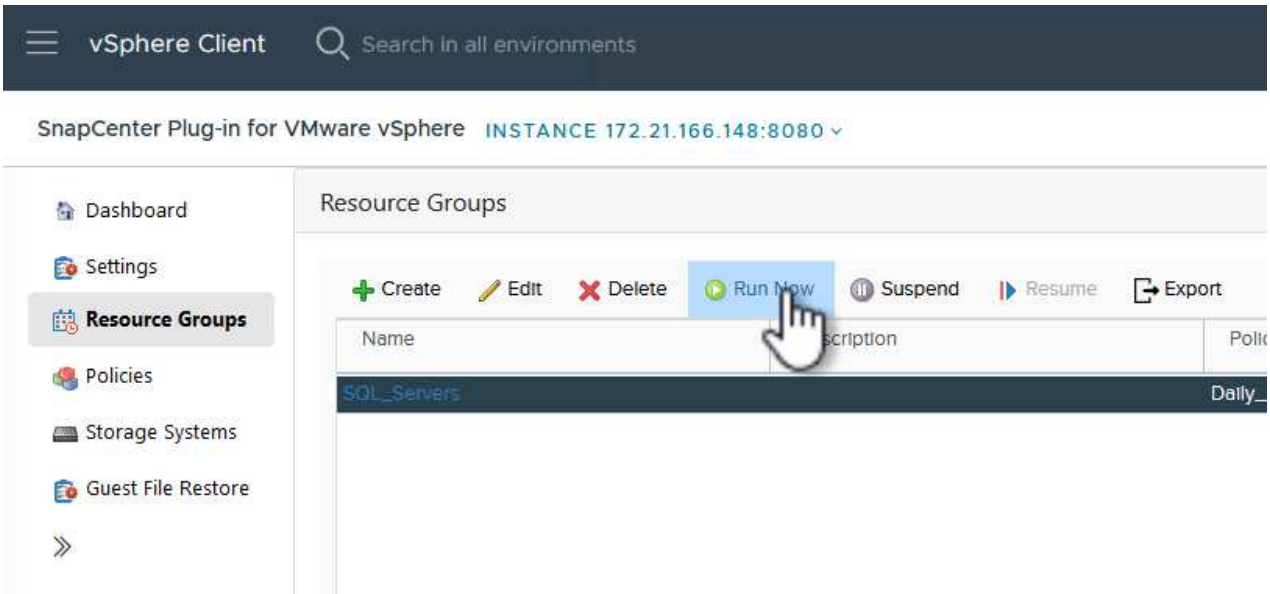
6. Nella pagina **piani di lavoro** stabilire quando verrà eseguito il backup configurando la ricorrenza e l'ora del giorno. Fare clic su **Avanti** per continuare.



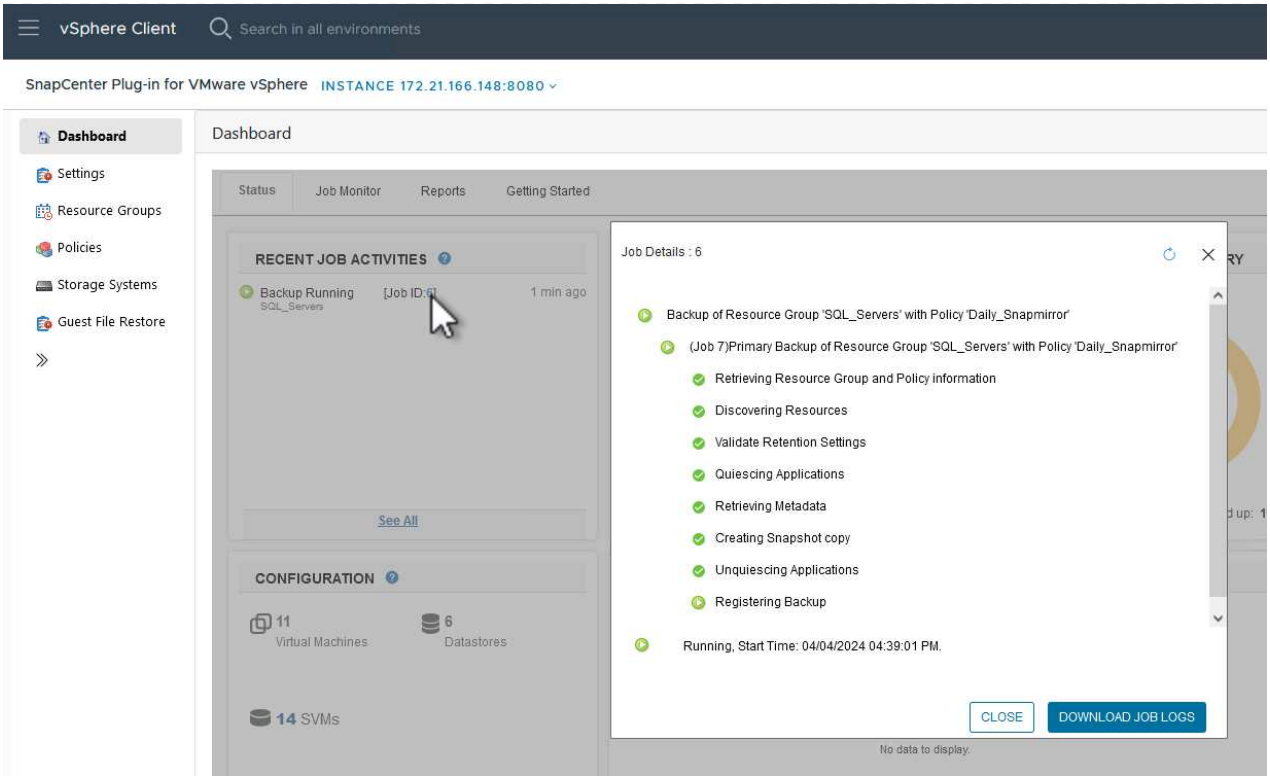
7. Infine, esaminare il **Riepilogo** e fare clic su **fine** per creare il gruppo di risorse.



8. Dopo aver creato il gruppo di risorse, fare clic sul pulsante **Esegui ora** per eseguire il primo backup.



9. Accedere al **Dashboard** e, in **Recent Job Activities**, fare clic sul numero accanto a **Job ID** per aprire il monitoraggio del processo e visualizzare l'avanzamento del processo in esecuzione.



Utilizzare SCV per ripristinare VM, VMDK e file

Il plug-in SnapCenter consente il ripristino di macchine virtuali, VMDK, file e cartelle da backup primari o secondari.

Le macchine virtuali possono essere ripristinate sull'host originale, su un host alternativo nello stesso vCenter Server o su un host ESXi alternativo gestito dallo stesso vCenter o da qualsiasi vCenter in modalità collegata.

Le macchine virtuali vVol possono essere ripristinate sull'host originale.

I VMDK delle macchine virtuali tradizionali possono essere ripristinati nel datastore originale o in un datastore alternativo.

I VMDK delle macchine virtuali vVol possono essere ripristinati nel datastore originale.

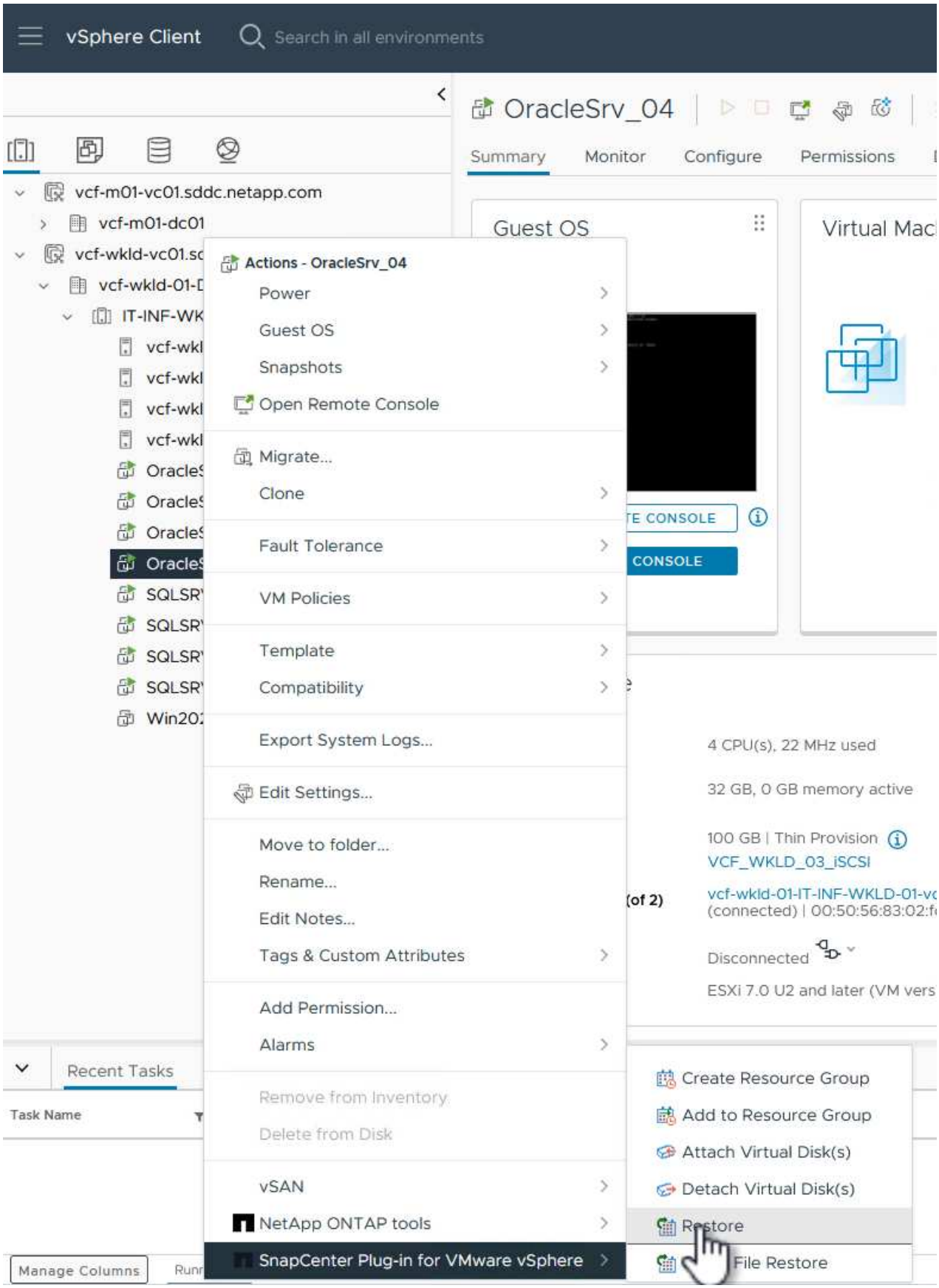
È possibile ripristinare singoli file e cartelle in una sessione di ripristino dei file guest, allegando una copia di backup di un disco virtuale e ripristinando i file o le cartelle selezionati.

Completare i seguenti passaggi per ripristinare VM, VMDK o singole cartelle.

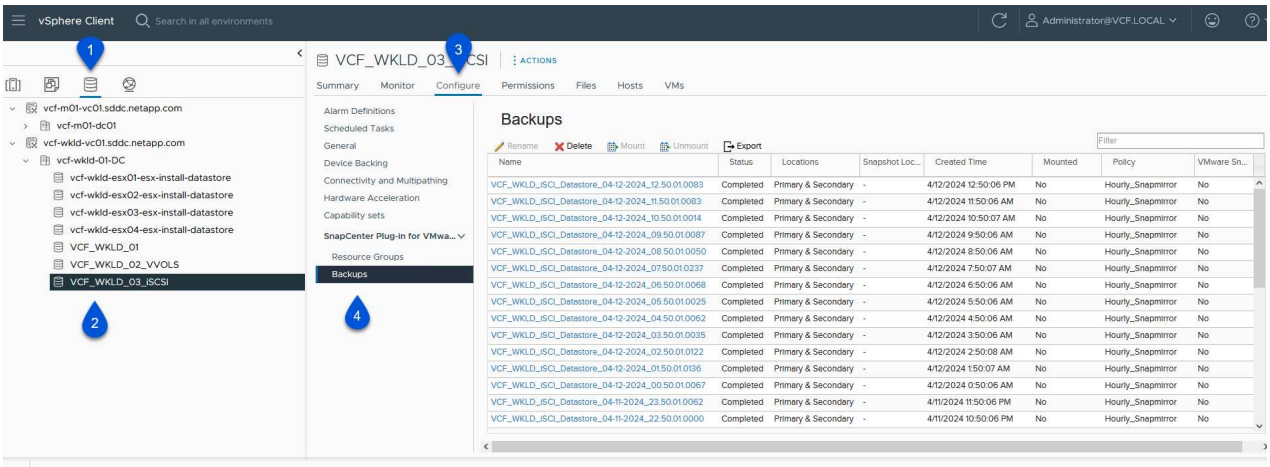
Ripristino delle VM con il plug-in SnapCenter

Completare i seguenti passaggi per ripristinare una VM con SCV:

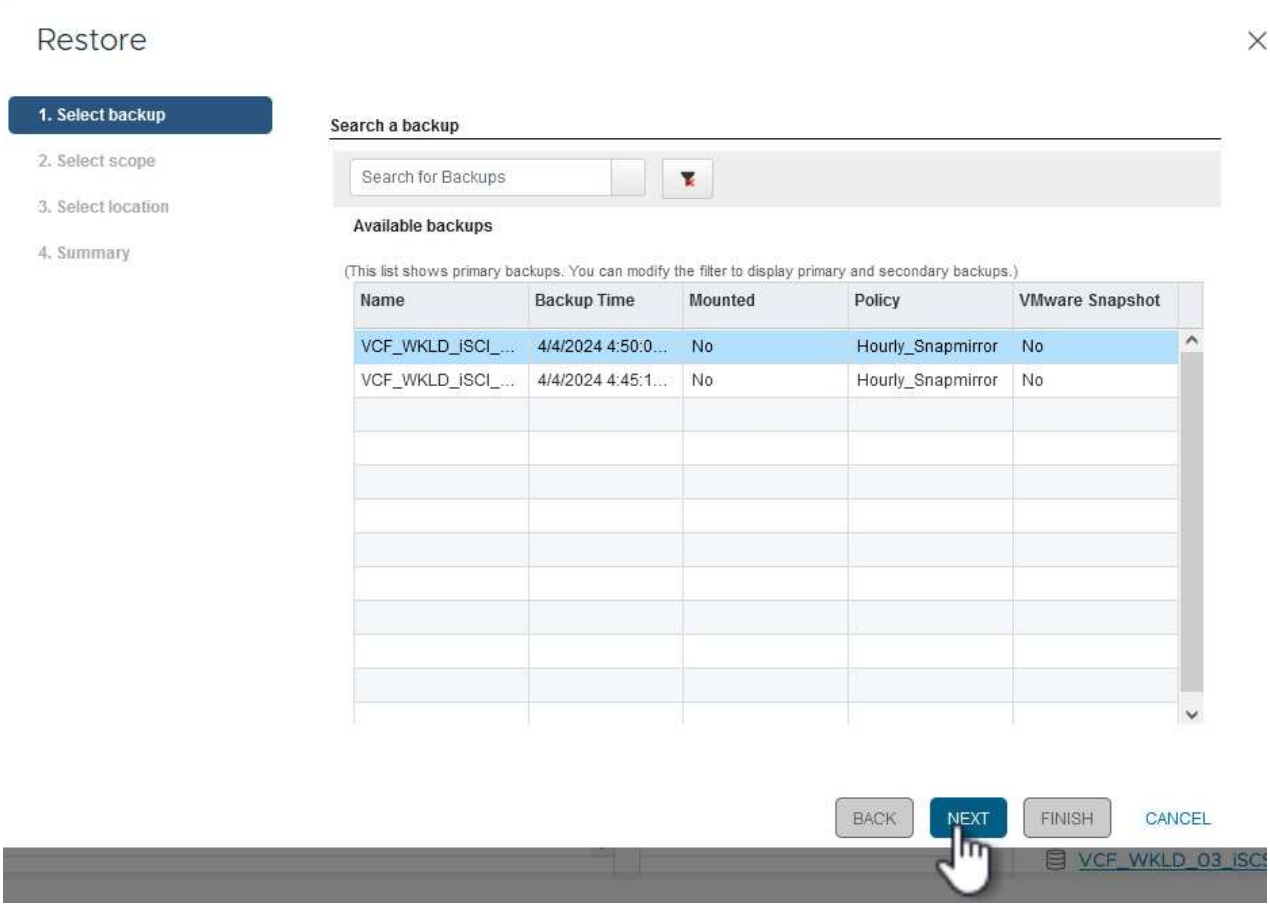
1. Accedere alla VM da ripristinare nel client vSphere, fare clic con il pulsante destro del mouse e selezionare **SnapCenter Plug-in for VMware vSphere**. Selezionare **Ripristina** dal sottomenu.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
Oracle
Oracle
Oracle
Oracle
SQLSR
SQLSR
SQLSR
SQLSR
Win20
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore

Un'alternativa è accedere al datastore nell'inventario, quindi nella scheda **Configura** andare a **plug-in SnapCenter per VMware vSphere > Backup**. Dal backup scelto, selezionare le VM da ripristinare.

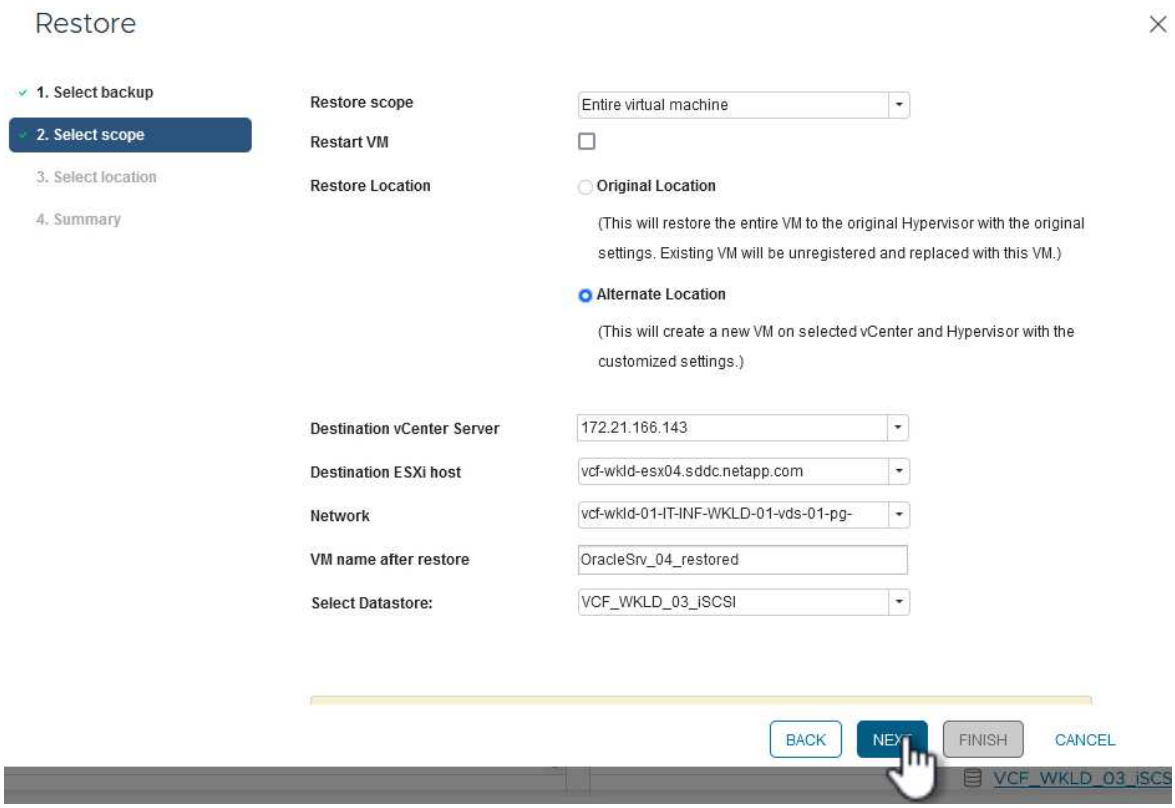


2. Nella procedura guidata **Restore** selezionare il backup da utilizzare. Fare clic su **Avanti** per continuare.



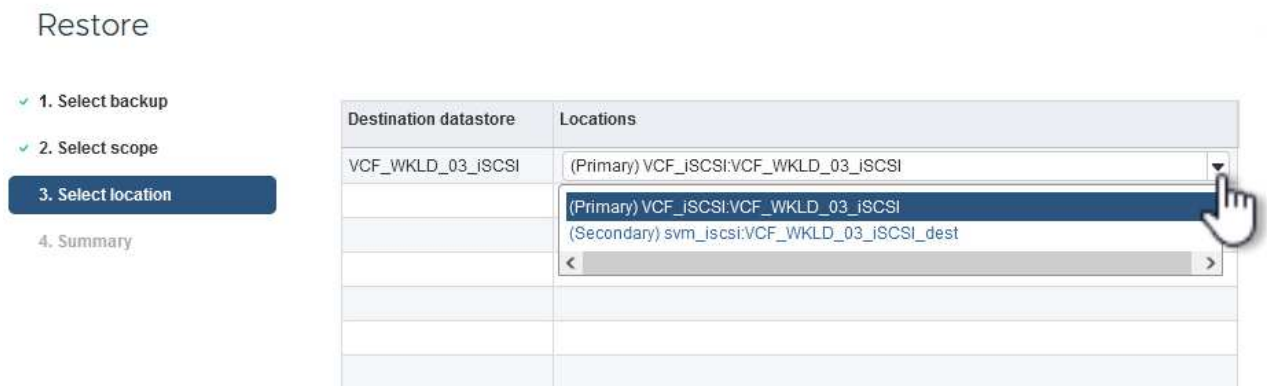
3. Nella pagina **Seleziona ambito** compilare tutti i campi obbligatori:

- **Ripristina ambito** - selezionare per ripristinare l'intera macchina virtuale.
- **Riavvia VM** - consente di scegliere se avviare la VM dopo il ripristino.
- **Ripristina posizione** - scegliere di ripristinare la posizione originale o in una posizione alternativa. Quando si sceglie una posizione alternativa, selezionare le opzioni da ciascuno dei campi:
  - **Destinazione vCenter Server** - vCenter locale o vCenter alternativo in modalità collegata
  - **Host ESXi di destinazione**
  - **Rete**
  - **Nome VM dopo il ripristino**
  - **Seleziona archivio dati:**

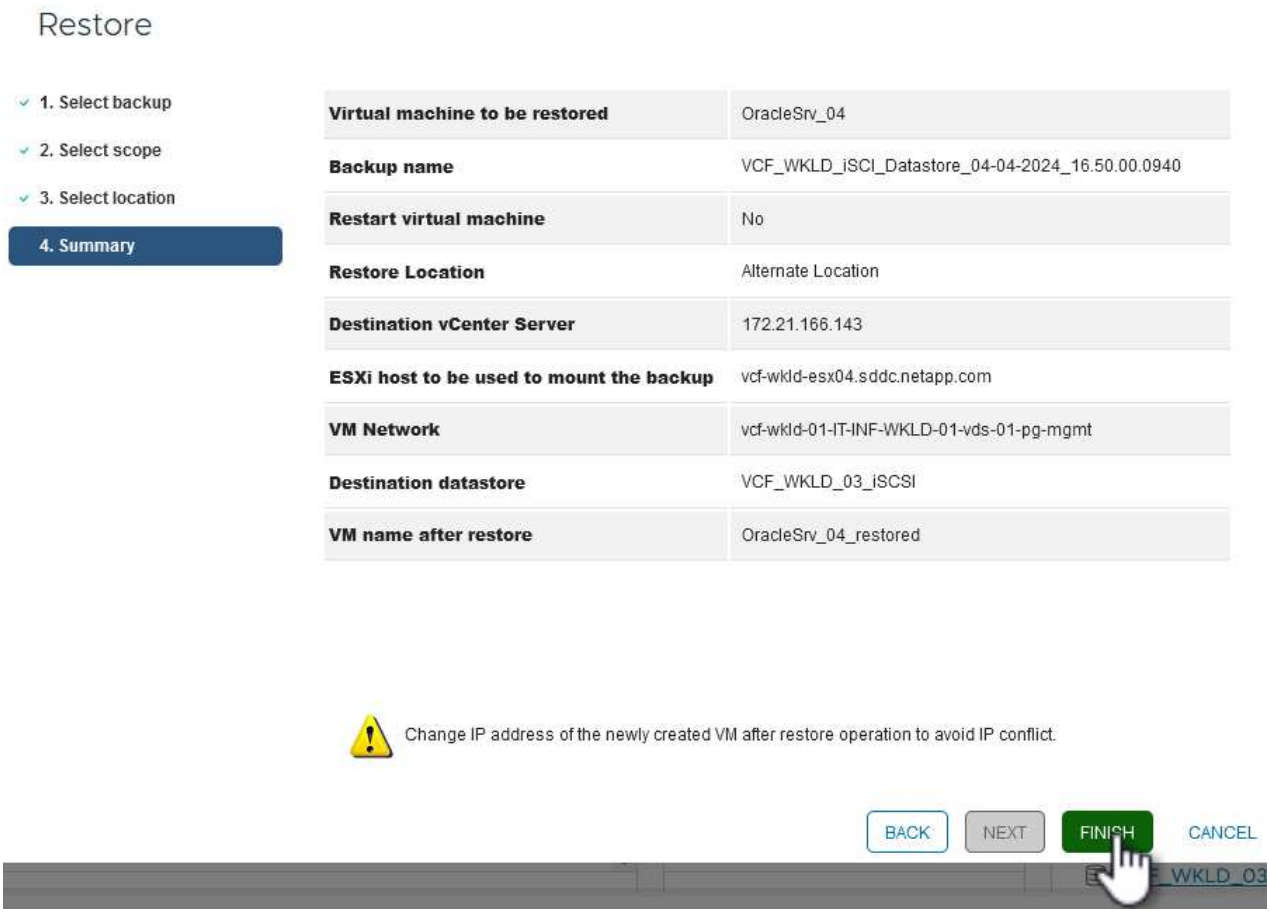


Fare clic su **Avanti** per continuare.

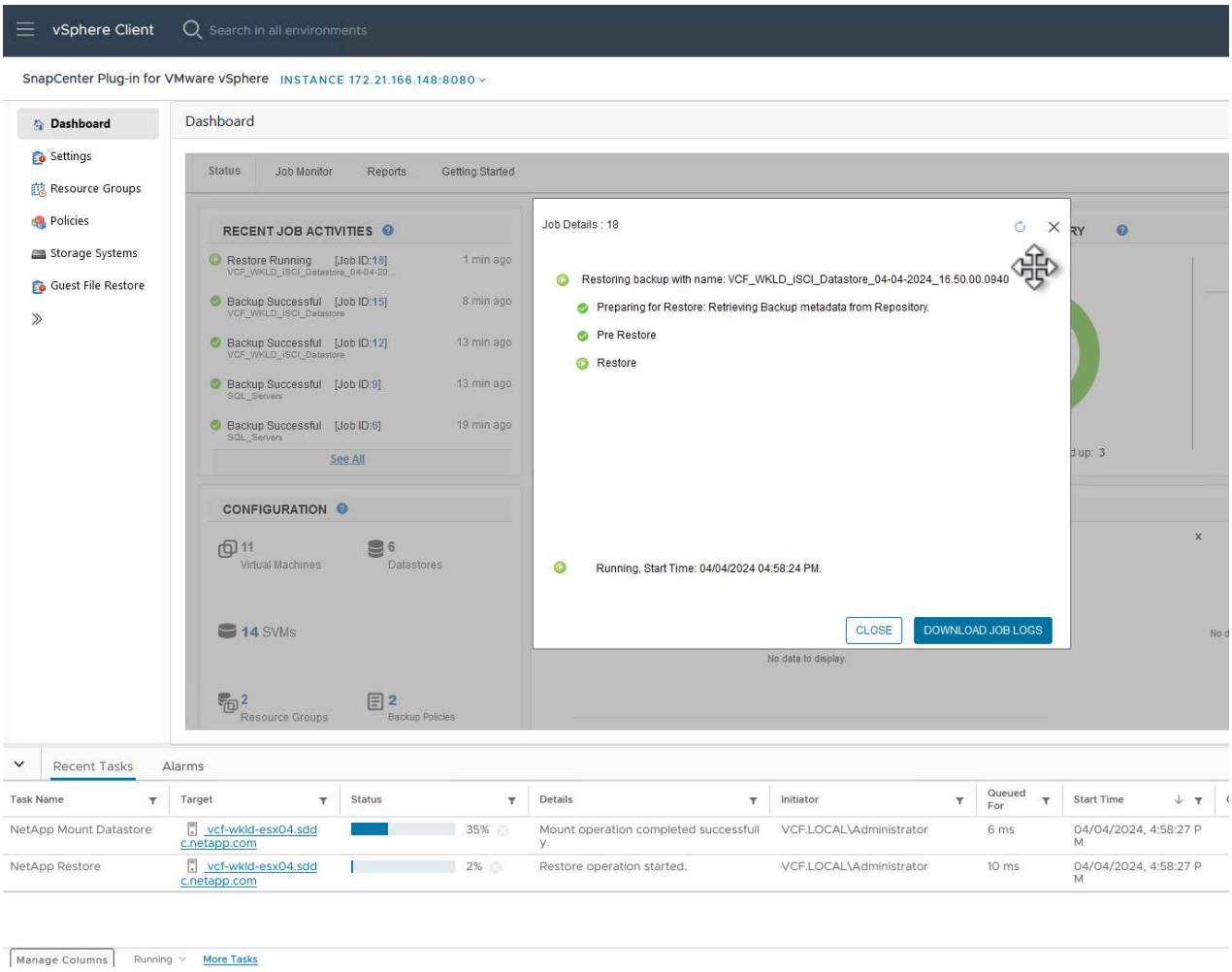
4. Nella pagina **Seleziona posizione**, scegliere di ripristinare la macchina virtuale dal sistema di storage ONTAP primario o secondario. Fare clic su **Avanti** per continuare.



5. Infine, esaminare il **Riepilogo** e fare clic su **fine** per avviare il processo di ripristino.



6. L'avanzamento del processo di ripristino può essere monitorato dal riquadro **Recent Tasks** (attività recenti) nel client vSphere e dal monitoraggio dei processi in SCV.

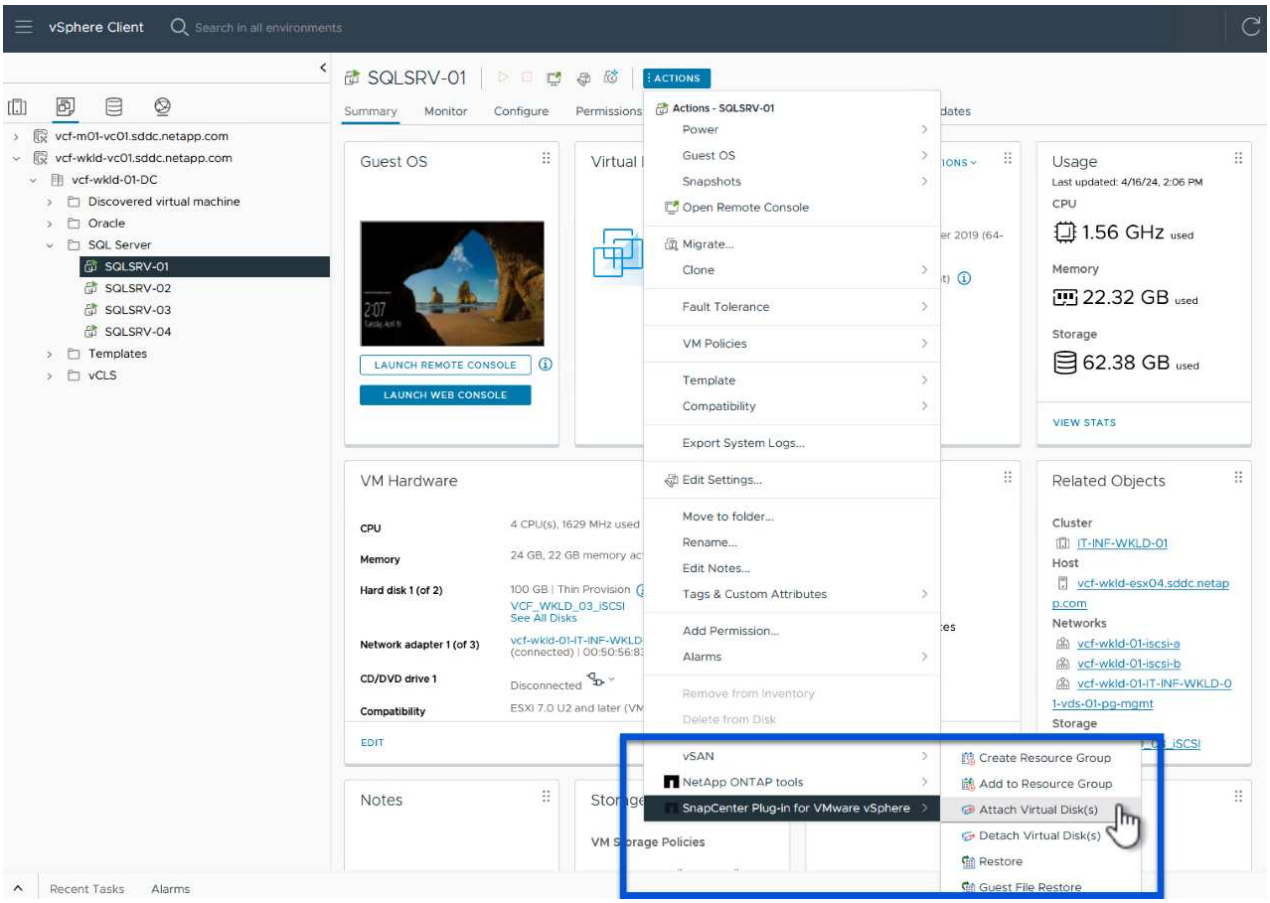

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

Ripristinare VMDK utilizzando il plug-in SnapCenter

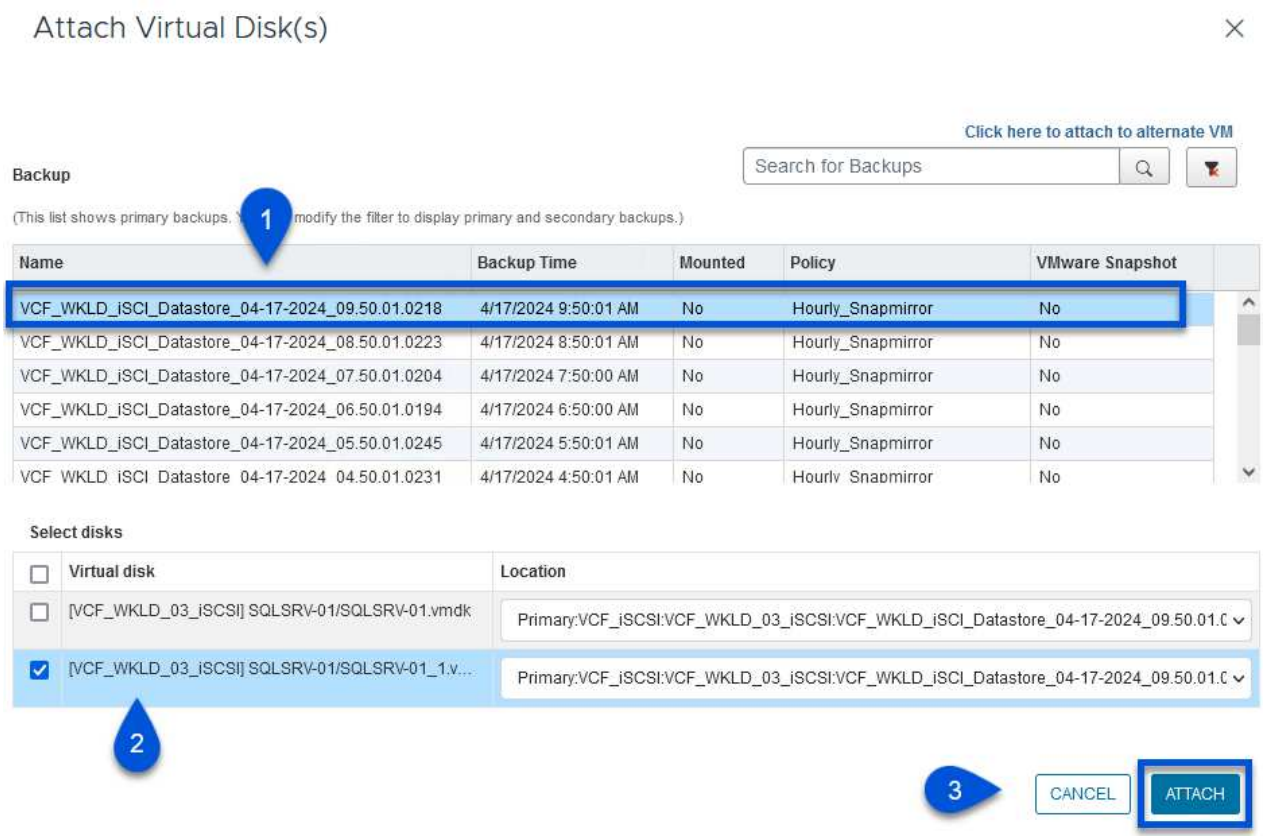
ONTAP Tools consente il ripristino completo dei file VMDK nella posizione originale o la possibilità di collegare un file VMDK come nuovo disco a un sistema host. In questo scenario, un VMDK verrà collegato a un host Windows per accedere al file system.

Per collegare un VMDK da un backup, attenersi alla seguente procedura:

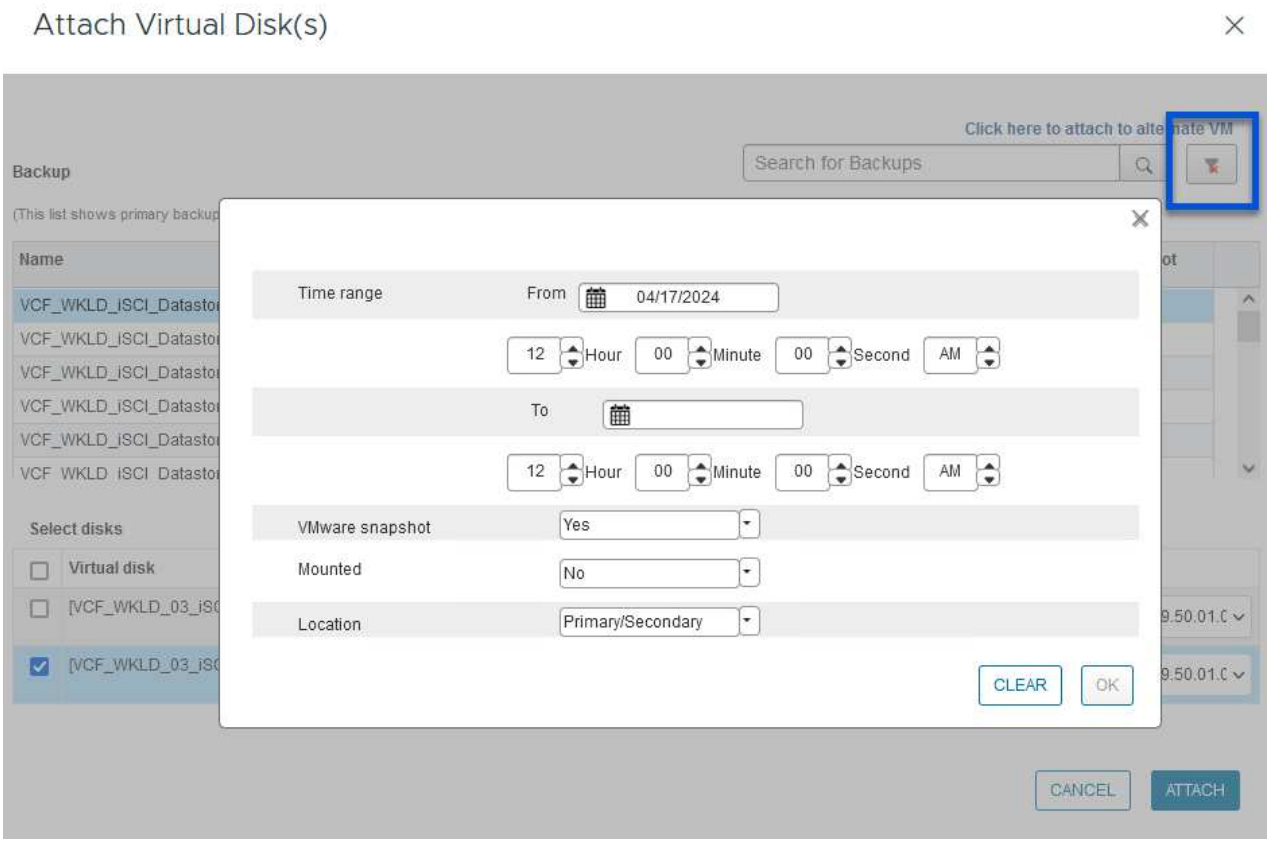
1. Nel client vSphere, passare a una VM e, dal menu **azioni**, selezionare **Plug-in SnapCenter per VMware vSphere > Allega dischi virtuali**.



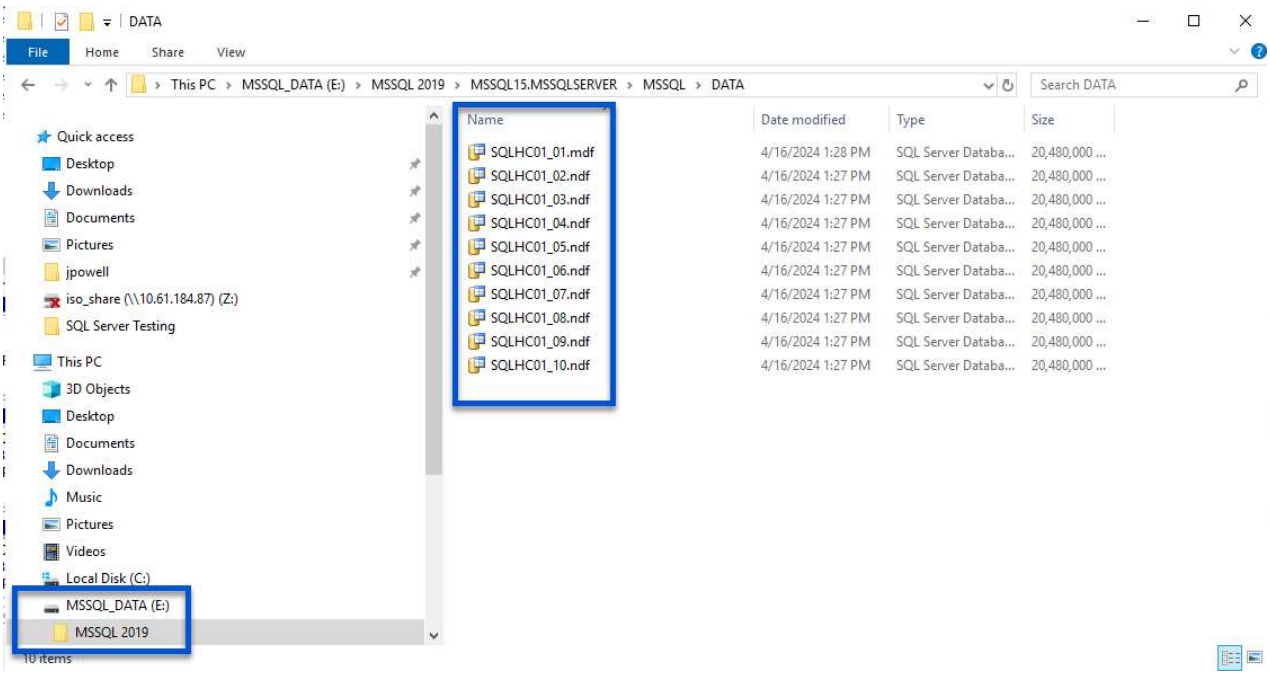
2. Nella procedura guidata **Allega dischi virtuali**, selezionare l'istanza di backup da utilizzare e il VMDK specifico da collegare.



Le opzioni dei filtri consentono di individuare i backup e visualizzare i backup dei sistemi di storage primario e secondario.



3. Dopo aver selezionato tutte le opzioni, fare clic sul pulsante **Allega** per avviare il processo di ripristino e collegare il VMDK all'host.
4. Una volta completata la procedura di collegamento, è possibile accedere al disco dal sistema operativo del sistema host. In questo caso SCV ha collegato il disco con il file system NTFS all'unità e: Di Windows SQL Server e i file di database SQL sul file system sono accessibili tramite Esplora file.



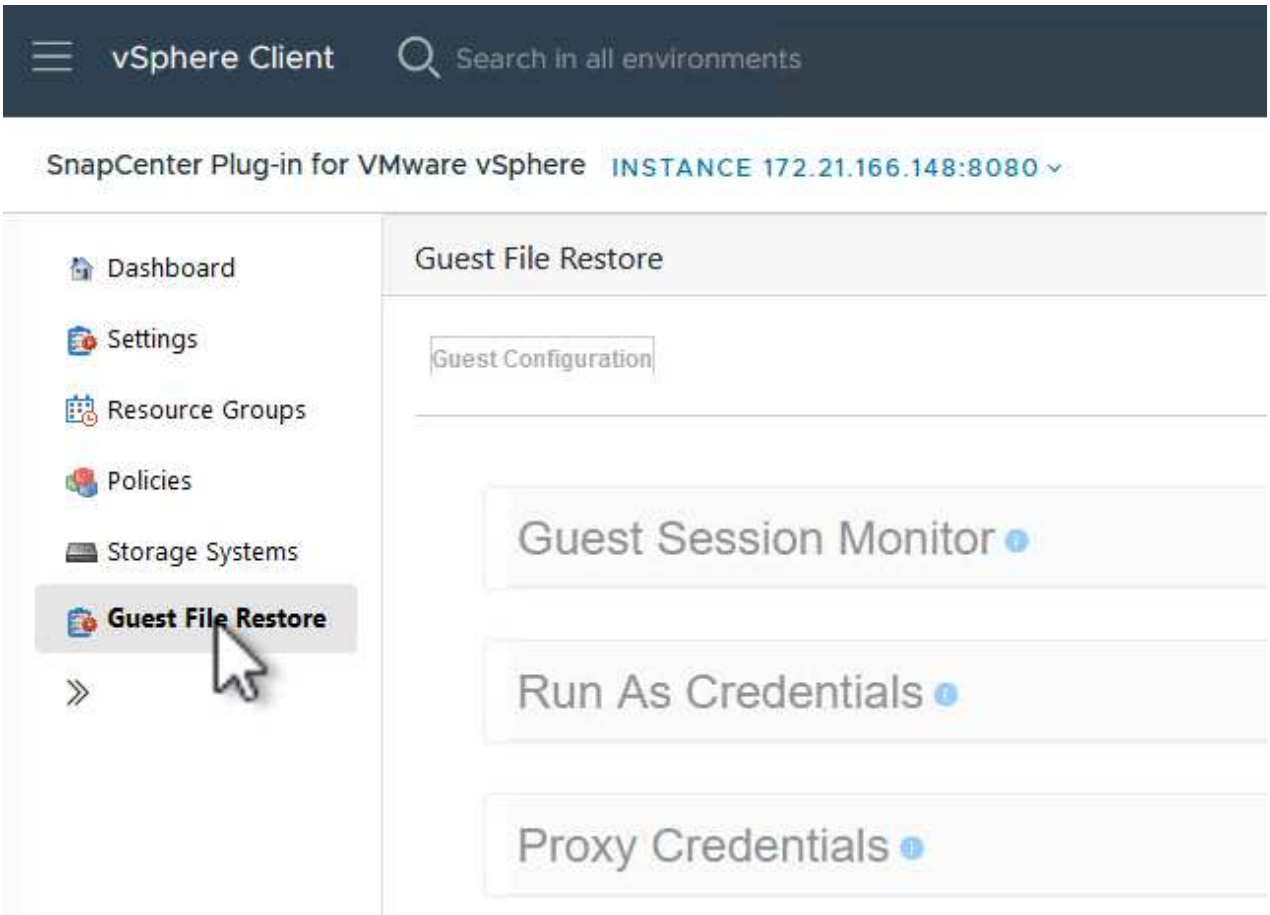
Ripristino del file system guest mediante il plug-in SnapCenter

ONTAP Tools consente di eseguire il ripristino del file system guest da un VMDK sui sistemi operativi Windows Server. Questo è preformato centralmente dall'interfaccia del plug-in SnapCenter.

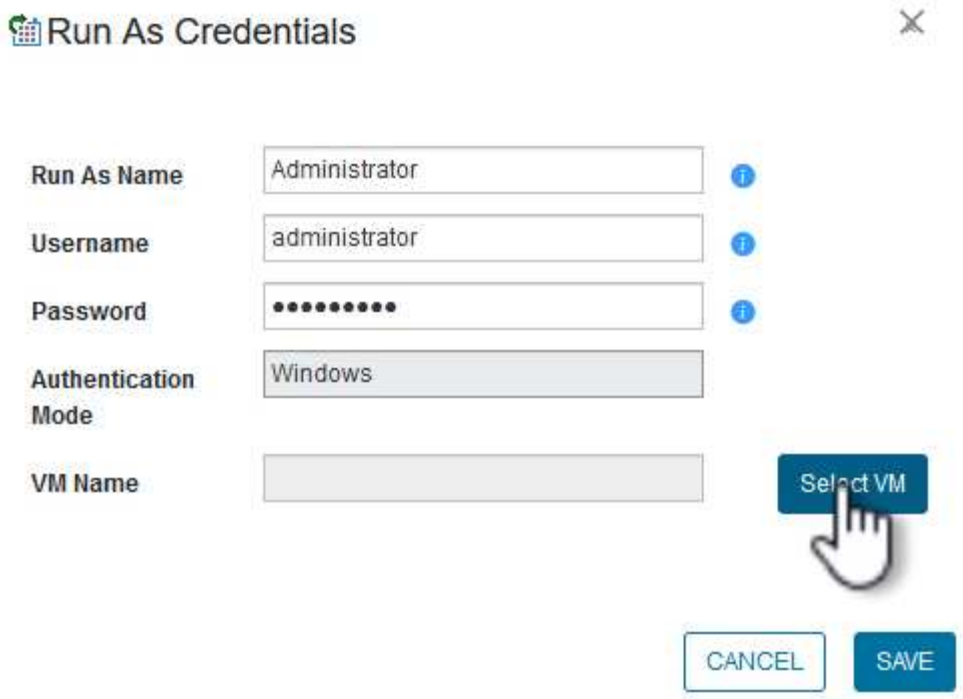
Per informazioni dettagliate, fare riferimento a. "Ripristinare file e cartelle guest" Sul sito della documentazione del distributore idraulico.

Per eseguire un ripristino del file system guest per un sistema Windows, attenersi alla seguente procedura:

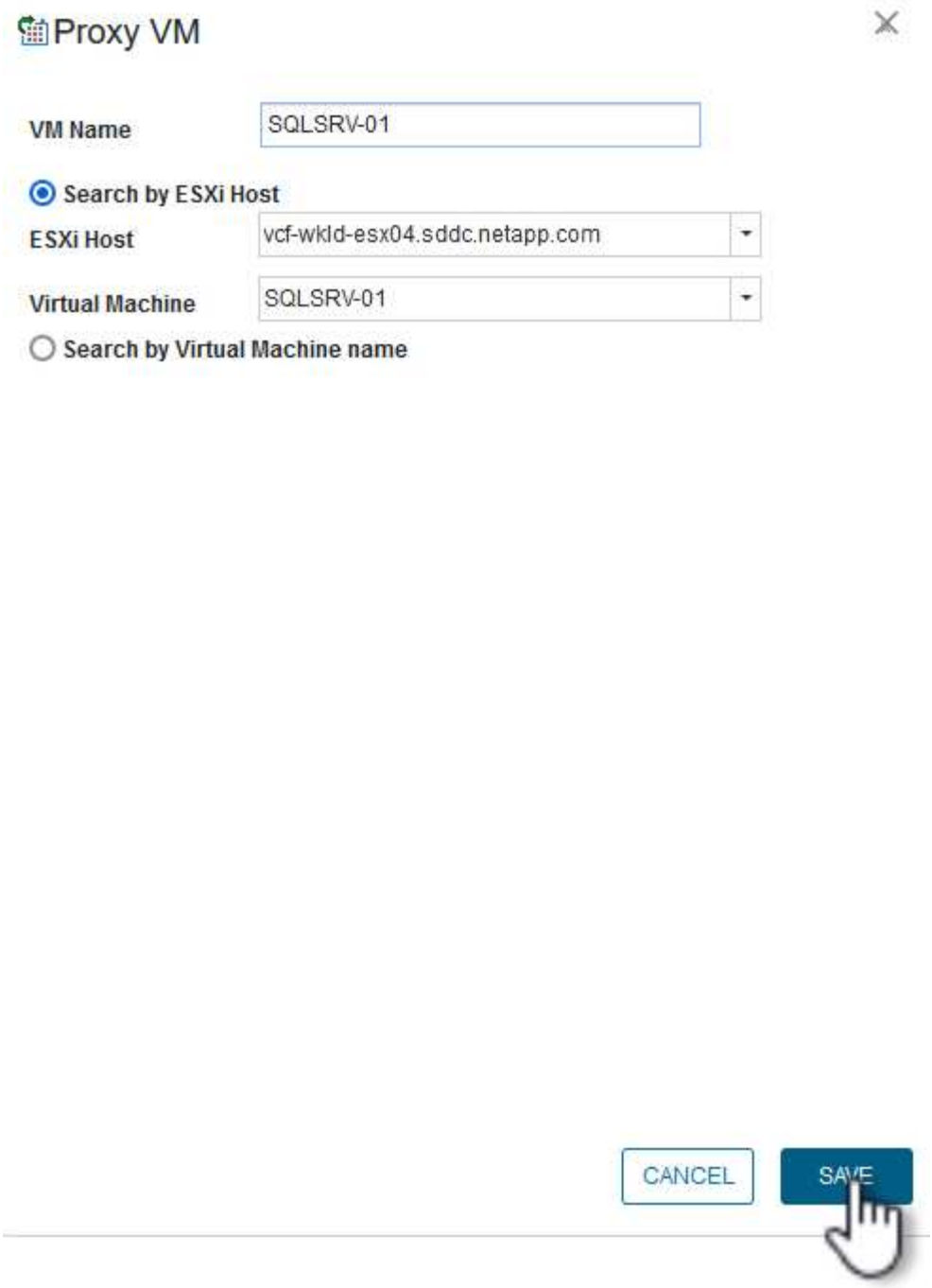
1. Il primo passaggio consiste nel creare credenziali Esegui come per fornire l'accesso al sistema host Windows. Nel client vSphere, accedere all'interfaccia del plug-in CSV e fare clic su **Guest file Restore** nel menu principale.



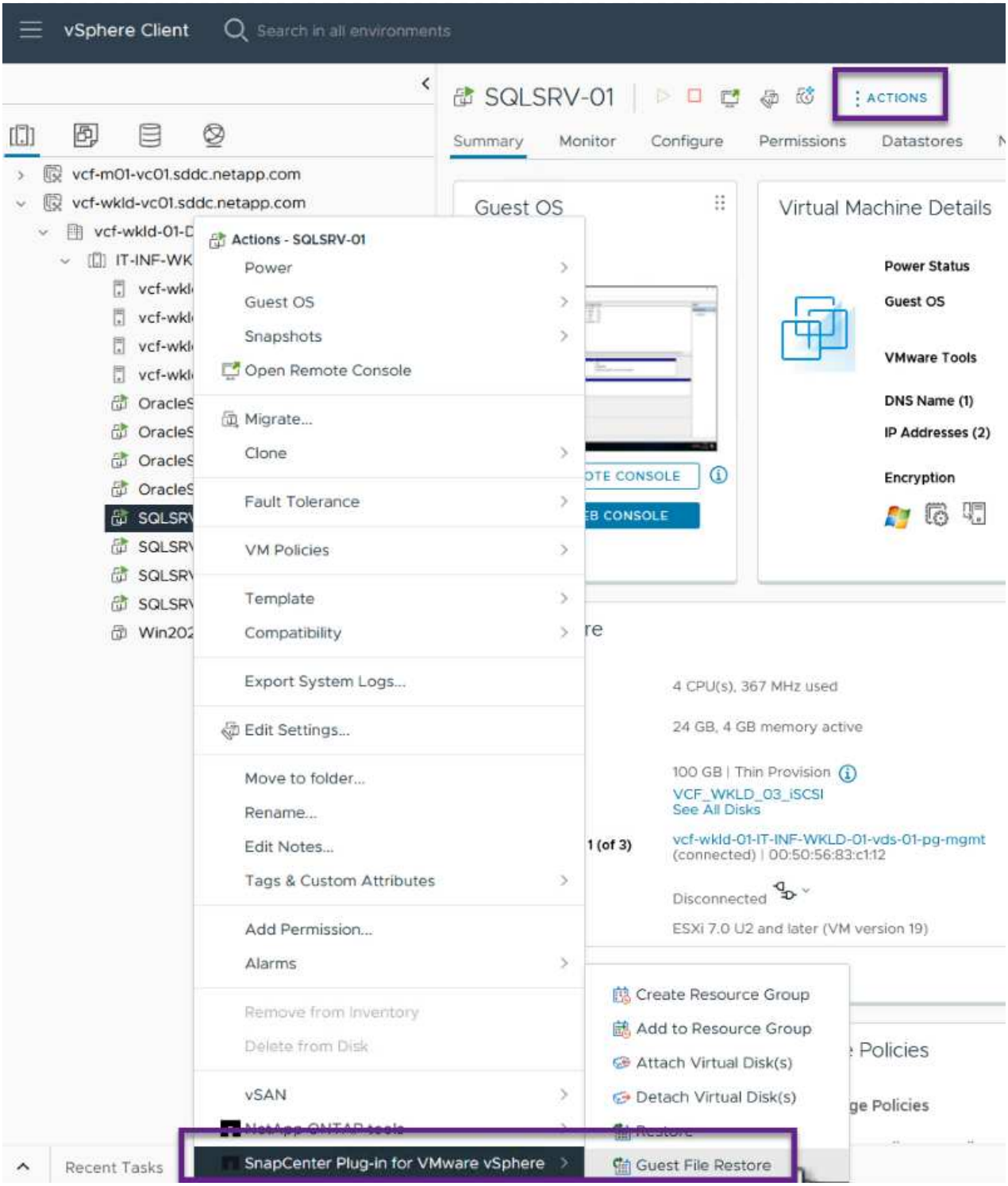
2. In **Esegui come credenziali** fare clic sull'icona **+** per aprire la finestra **Esegui come credenziali**.
3. Immettere un nome per il record delle credenziali, un nome utente e una password dell'amministratore per il sistema Windows, quindi fare clic sul pulsante **Select VM** (Seleziona VM) per selezionare una VM proxy opzionale da utilizzare per il ripristino.



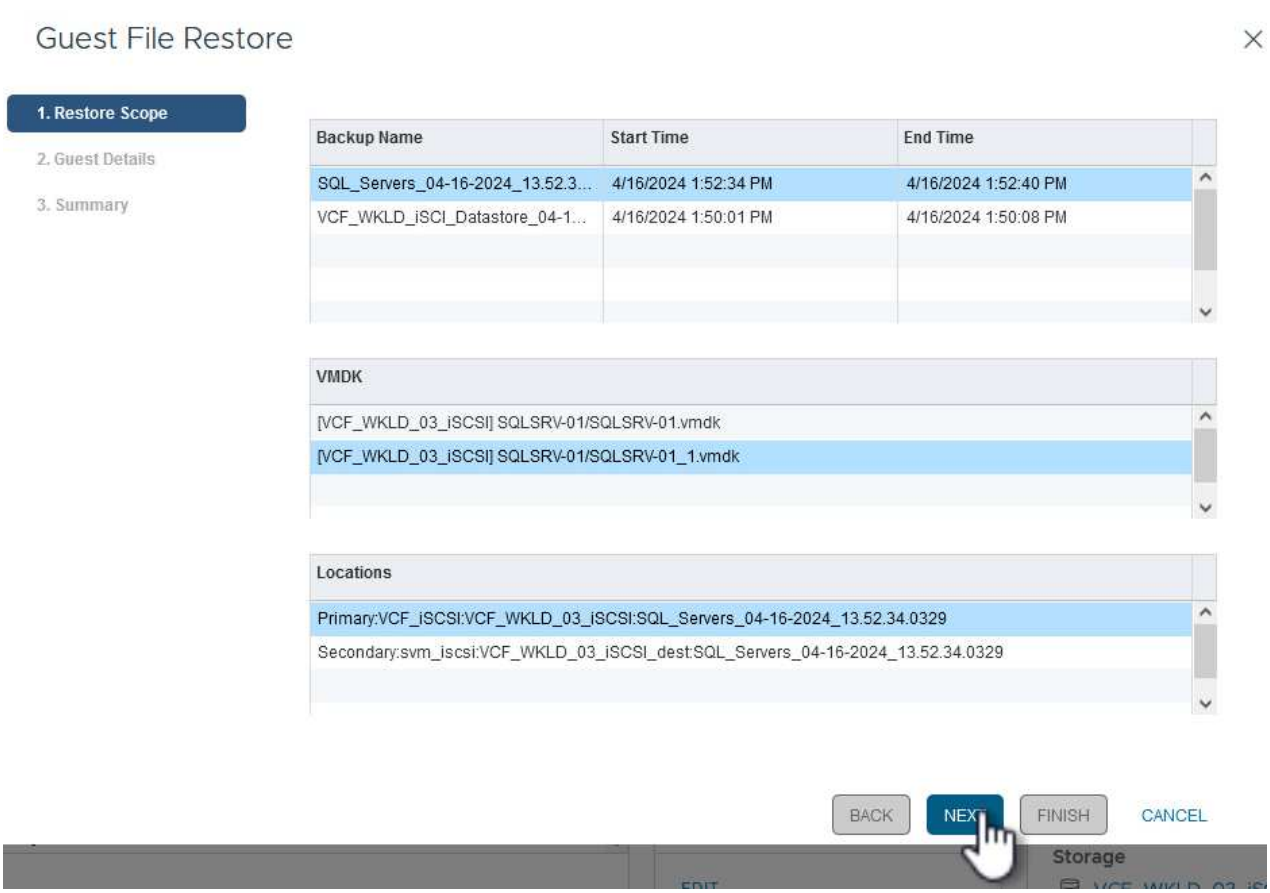
4. Nella pagina Proxy VM, fornire un nome per la VM e individuarla ricercando per host ESXi o per nome. Una volta selezionata, fare clic su **Salva**.



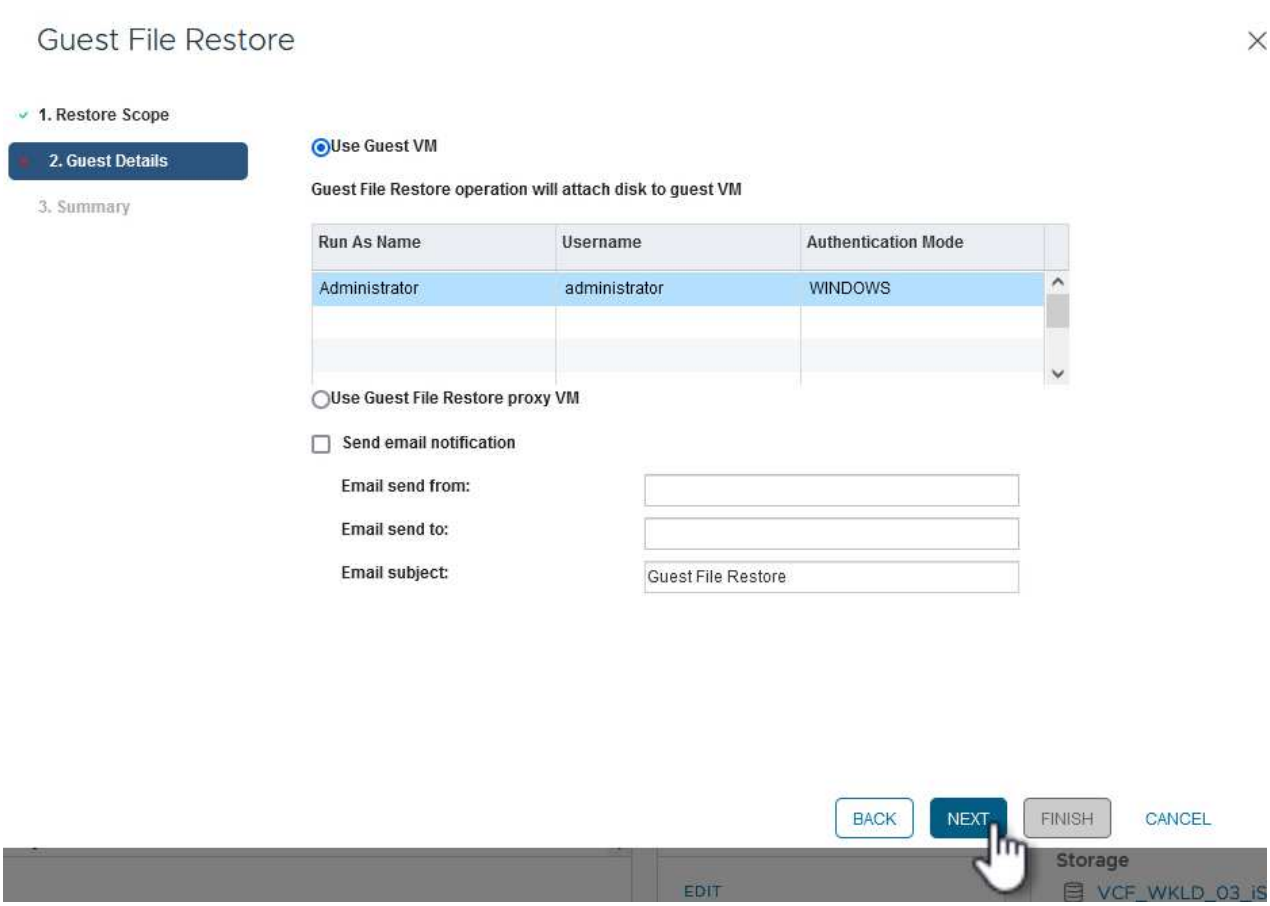
5. Fare nuovamente clic su **Salva** nella finestra **Esegui come credenziali** per completare il salvataggio del record.
6. Quindi, passare a una VM nell'inventario. Dal menu **azioni**, oppure facendo clic con il pulsante destro del mouse sulla macchina virtuale, selezionare **Plug-in SnapCenter per VMware vSphere > Ripristino file guest**.



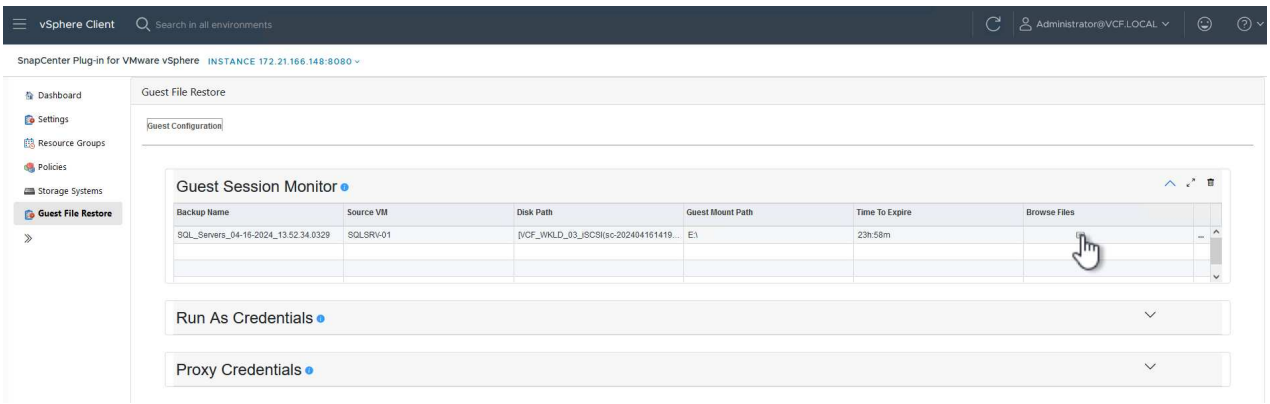
7. Nella pagina **Restore Scope** della procedura guidata **Guest file Restore**, selezionare il backup da cui eseguire il ripristino, il VMDK specifico e la posizione (primaria o secondaria) da cui ripristinare il VMDK. Fare clic su **Avanti** per continuare.



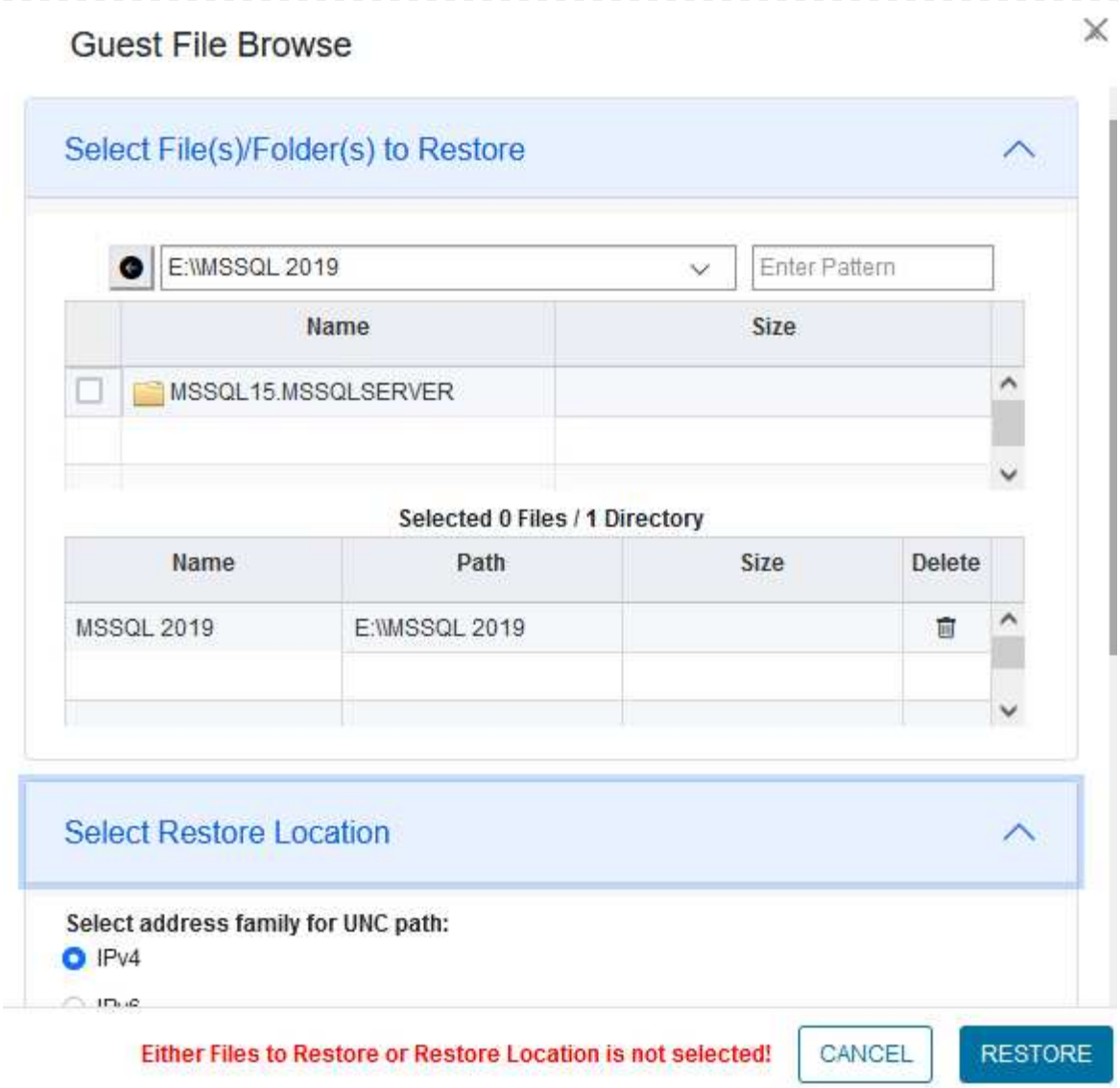
8. Nella pagina **Dettagli ospite**, selezionare per utilizzare **Guest VM** o **Use gues file Restore proxy VM** per il ripristino. Inoltre, se lo si desidera, compilare qui le impostazioni per le notifiche e-mail. Fare clic su **Avanti** per continuare.

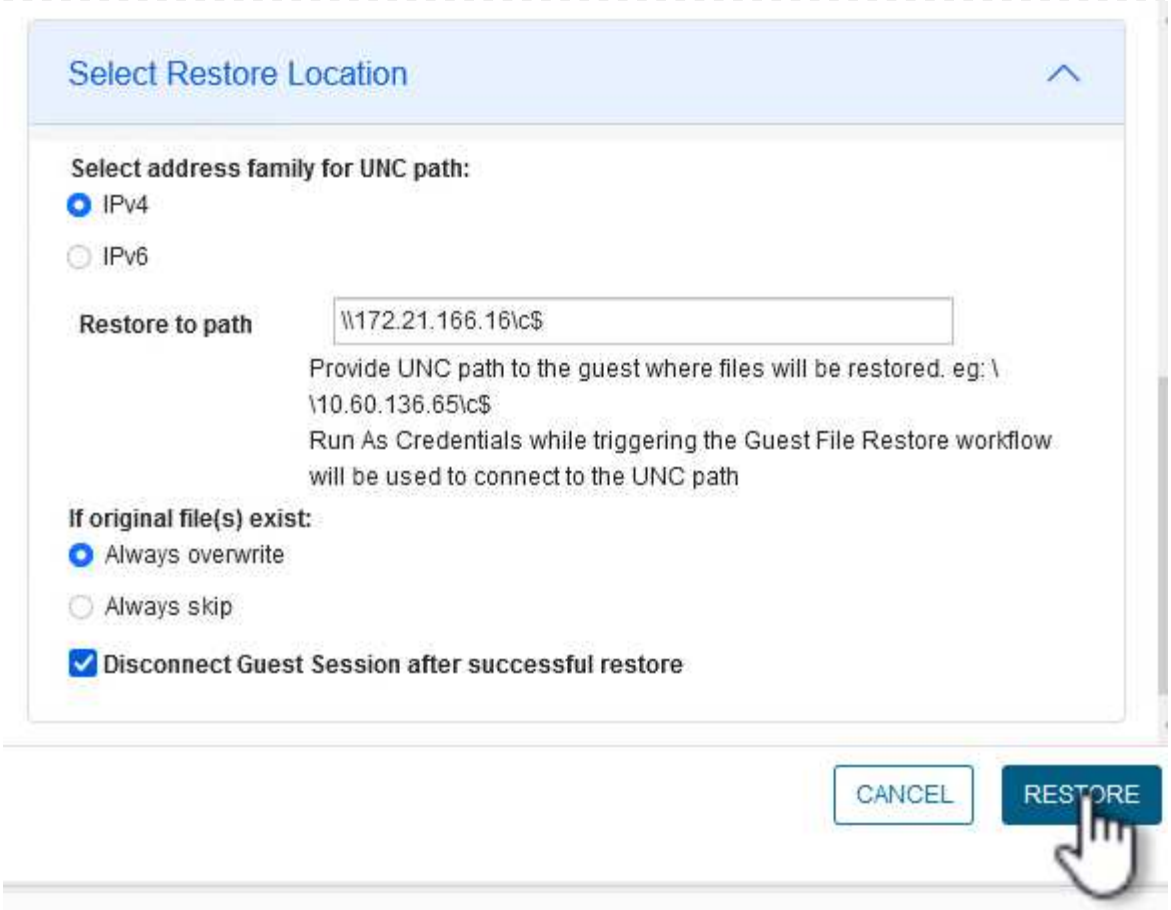


9. Infine, esaminare la pagina **Riepilogo** e fare clic su **fine** per avviare la sessione Ripristino configurazione di sistema file guest.
10. Nell'interfaccia del plug-in SnapCenter, accedere nuovamente a **Ripristino file guest** e visualizzare la sessione in esecuzione in **monitoraggio sessione guest**. Fare clic sull'icona sotto **Sfoglia file** per continuare.



11. Nella procedura guidata **Guest file Browse** selezionare la cartella o i file da ripristinare e la posizione del file system in cui ripristinarli. Infine, fare clic su **Restore** per avviare il processo **Restore**.


Guest File Browse
Select File(s)/Folder(s) to Restore
E:\MSSQL 2019
Enter Pattern
Name
Size
MSSQL15.MSSQLSERVER
Selected 0 Files / 1 Directory
Name
Path
Size
Delete
MSSQL 2019
E:\MSSQL 2019
Select Restore Location
Select address family for UNC path:
IPv4
Either Files to Restore or Restore Location is not selected!
CANCEL
RESTORE



12. Il processo di ripristino può essere monitorato dal riquadro attività del client vSphere.

Ulteriori informazioni

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sull'utilizzo del plug-in SnapCenter per VMware vSphere, consultare la "Plug-in SnapCenter per la documentazione di VMware vSphere".

VCF con array NetApp AFF

VMware Cloud Foundation con array NetApp AFF

VMware Cloud Foundation (VCF) è una piattaforma SDDC (Software Defined Data Center) integrata che fornisce uno stack completo di infrastrutture software-defined per eseguire applicazioni aziendali in un ambiente di cloud ibrido. Combina funzionalità di calcolo, storage, networking e gestione in una piattaforma unificata, offrendo un'esperienza operativa coerente su cloud pubblici e privati.

Autore: Josh Powell, Ravi BCB

Il presente documento fornisce informazioni sulle opzioni di storage disponibili per VMware Cloud Foundation utilizzando il sistema storage AFF all-flash di NetApp. Le opzioni di storage supportate sono coperte da istruzioni specifiche per la creazione di domini di workload con datastore NFS e vVol come storage principale, oltre a una gamma di opzioni di storage supplementari.

Casi di utilizzo

Casi d'utilizzo illustrati nella presente documentazione:

- Opzioni di storage per i clienti che cercano ambienti uniformi su cloud pubblici e privati.
- Soluzione automatizzata per l'implementazione dell'infrastruttura virtuale per i domini di carico di lavoro.
- Soluzione storage scalabile realizzata su misura per soddisfare esigenze in evoluzione, anche se non allineata direttamente ai requisiti delle risorse di calcolo.
- Distribuire i domini del carico di lavoro VCF VI utilizzando ONTAP come storage principale.
- Distribuire lo storage supplementare ai domini del carico di lavoro VI utilizzando gli strumenti ONTAP per VMware vSphere.

Pubblico

Questa soluzione è destinata alle seguenti persone:

- Architetti delle soluzioni alla ricerca di opzioni di storage più flessibili per ambienti VMware che siano progettati per massimizzare il TCO.
- Solution Architect in cerca di opzioni storage VCF che offrono opzioni di protezione dei dati e disaster recovery con i principali cloud provider.
- Amministratori dello storage che desiderano comprendere come configurare VCF con lo storage principale e supplementare.

Panoramica sulla tecnologia

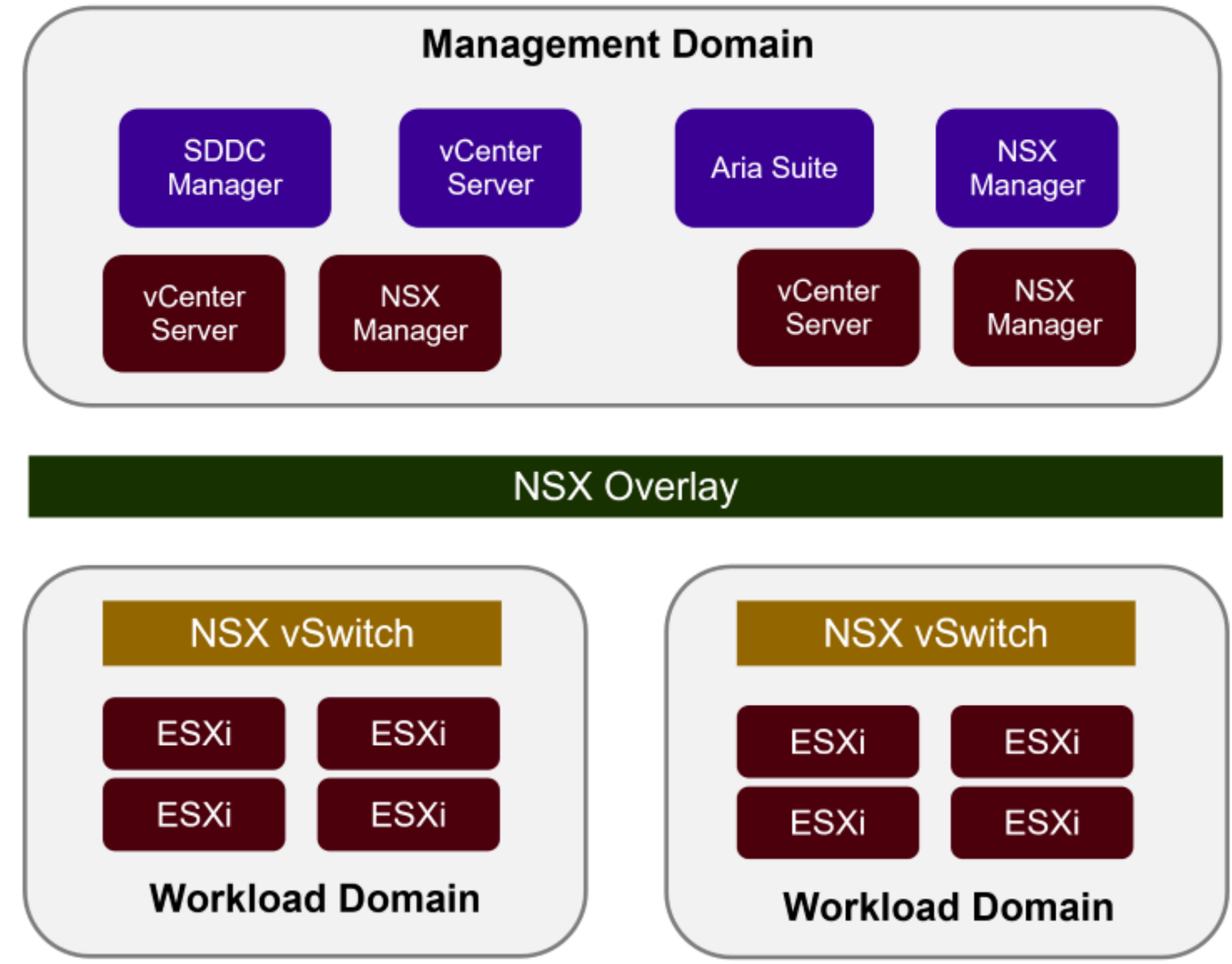
La soluzione VCF con NetApp AFF comprende i seguenti componenti principali:

VMware Cloud Foundation

VMware Cloud Foundation amplia le offerte di hypervisor VMware vSphere combinando componenti chiave come SDDC Manager, vSphere, vSAN, NSX e VMware aria Suite per creare un data center virtualizzato.

La soluzione VCF supporta sia i workload Kubernetes nativi che quelli basati su macchine virtuali. I servizi chiave come VMware vSphere, VMware vSAN, VMware NSX-T Data Center e VMware vRealize Cloud Management sono componenti integrali del pacchetto VCF. Una volta combinati, questi servizi creano un'infrastruttura software-defined in grado di gestire in modo efficiente la gestione di calcolo, storage, networking, sicurezza e cloud.

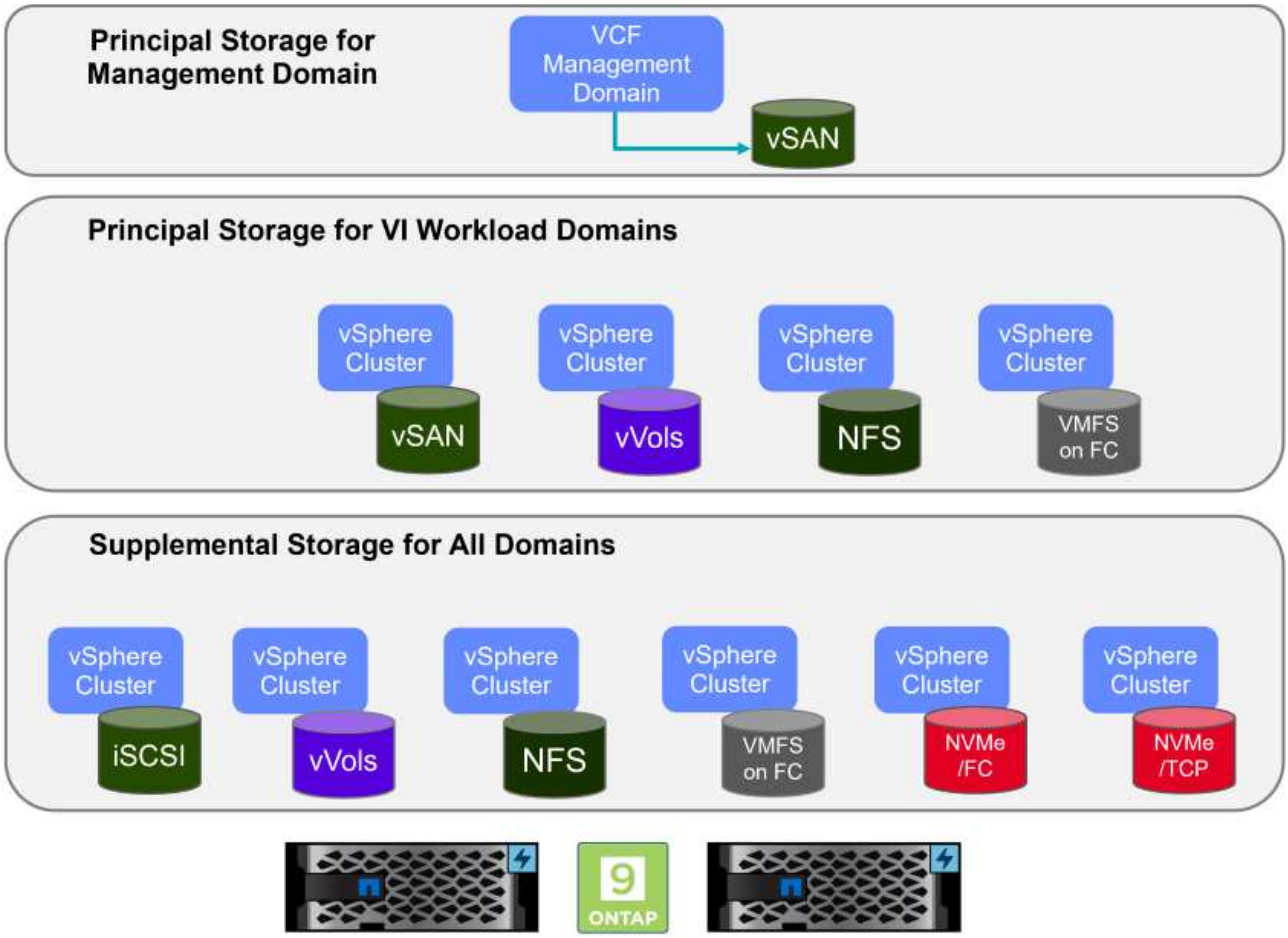
VCF è costituito da un singolo dominio di gestione e fino a 24 domini del carico di lavoro VI che rappresentano ciascuna un'unità di infrastruttura predisposta per le applicazioni. Un dominio del carico di lavoro è costituito da uno o più cluster vSphere gestiti da una singola istanza vCenter.



Per ulteriori informazioni sull'architettura e la pianificazione di VCF, fare riferimento a. "Modelli di architettura e tipi di dominio del carico di lavoro in VMware Cloud Foundation".

Opzioni di archiviazione VCF

VMware divide le opzioni di storage per VCF in **Principal** e **integrative**. Il dominio di gestione VCF deve utilizzare vSAN come storage principale. Tuttavia, esistono molte opzioni di archiviazione supplementari per il dominio di gestione e opzioni di archiviazione principale e supplementare disponibili per i domini del carico di lavoro VI.



Archiviazione principale per i domini del carico di lavoro
L'archiviazione principale si riferisce a qualsiasi tipo di archiviazione che può essere collegata direttamente a un dominio del carico di lavoro VI durante il processo di installazione in SDDC Manager. Lo storage principale è il primo datastore configurato per un dominio del carico di lavoro e include vSAN, vVol (VMFS), NFS e VMFS su Fibre Channel.

Archiviazione supplementare per domini di gestione e carico di lavoro
Lo storage supplementare è il tipo di storage che è possibile aggiungere ai domini di gestione o del carico di lavoro in qualsiasi momento dopo la creazione del cluster. Lo storage supplementare rappresenta la più ampia gamma di opzioni di storage supportate, tutte supportate dagli array NetApp AFF.

Ulteriori risorse di documentazione per VMware Cloud Foundation:
* "Documentazione di VMware Cloud Foundation"
* "Tipi di storage supportati per VMware Cloud Foundation"
* "Gestione dello storage in VMware Cloud Foundation"

Array storage all-flash NetApp

Gli array NetApp AFF (All Flash FAS) sono soluzioni storage ad alte performance progettate per sfruttare la velocità e l'efficienza della tecnologia flash. Gli array AFF incorporano funzionalità di gestione integrata dei dati quali backup basati su snapshot, replica, thin provisioning e funzionalità di protezione dei dati.

Gli array NetApp AFF utilizzano il sistema operativo per lo storage ONTAP, offrendo un supporto completo del

protocollo di storage per tutte le opzioni di storage compatibili con VCF, il tutto all'interno di un'architettura unificata.

Gli storage array NetApp AFF sono disponibili nella serie A dalle performance più elevate e in una serie C QLC basata su flash. Entrambe le serie utilizzano dischi flash NVMe.

Per ulteriori informazioni sugli storage array NetApp AFF A-Series, consultare la "NetApp AFF A-Series" landing page.

Per ulteriori informazioni sugli storage array NetApp C-Series, consultare la "NetApp AFF C-Series" landing page.

Strumenti NetApp ONTAP per VMware vSphere

ONTAP Tools per VMware vSphere (OTV) consente agli amministratori di gestire lo storage NetApp direttamente dal client vSphere. ONTAP Tools ti consente di implementare e gestire datastore, nonché di eseguire il provisioning dei datastore vVol.

I tool ONTAP consentono il mapping dei datastore ai profili di funzionalità dello storage che determinano un set di attributi del sistema storage. Ciò consente la creazione di datastore con attributi specifici, come le performance dello storage e la qualità del servizio.

ONTAP Tools include inoltre un provider **VASA (VMware vSphere APIs for Storage Awareness)** per i sistemi di storage ONTAP che consente il provisioning dei datastore vVol (VMware Virtual Volumes), la creazione e l'utilizzo di profili di funzionalità di storage, la verifica della conformità e il monitoraggio delle performance.

Per ulteriori informazioni sugli strumenti NetApp ONTAP, vedere "Strumenti ONTAP per la documentazione VMware vSphere" pagina.

Panoramica della soluzione

Negli scenari presentati in questa documentazione, verrà illustrato come utilizzare i sistemi di storage ONTAP come storage principale per le implementazioni del dominio di carico di lavoro VCF VI. Inoltre, installeremo e utilizzeremo gli strumenti ONTAP per VMware vSphere per configurare datastore supplementari per i domini del carico di lavoro VI.

Scenari trattati nella presente documentazione:

- **Configurare e utilizzare un datastore NFS come storage principale durante la distribuzione del dominio del carico di lavoro VI.** fare clic **"qui"** per le fasi di implementazione.
- **Installare e dimostrare l'uso degli strumenti ONTAP per configurare e montare gli archivi dati NFS come archiviazione supplementare nei domini del carico di lavoro VI.** fare clic su **"qui"** per le fasi di implementazione.

NFS come storage principale per i domini del carico di lavoro VI

In questo scenario verrà illustrato come configurare un datastore NFS come storage principale per la distribuzione di un dominio del carico di lavoro VI in VCF. Se necessario, faremo riferimento alla documentazione esterna per le operazioni che devono essere eseguite in SDDC Manager di VCF e descriveremo le operazioni specifiche per la parte relativa alla configurazione dello storage.

Autore: Josh Powell, Ravi BCB

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

- Verifica dell'networking per la Storage Virtual Machine (SVM) di ONTAP e della presenza di un'interfaccia logica (LIF) per il traffico NFS.
- Creare una policy di esportazione per consentire agli host ESXi di accedere al volume NFS.
- Crea un volume NFS sul sistema storage ONTAP.
- Creare un pool di rete per il traffico NFS e vMotion in SDDC Manager.
- Commissione di host in VCF per l'utilizzo in un dominio del carico di lavoro VI.
- Implementare un dominio del carico di lavoro VI in VCF utilizzando un datastore NFS come storage principale.
- Installare il plug-in NetApp NFS per VMware VAAI

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Sistema storage NetApp AFF con una Storage Virtual Machine (SVM) configurata per consentire il traffico NFS.
- L'interfaccia logica (LIF) è stata creata nella rete IP per il trasporto del traffico NFS e associata alla SVM.
- La distribuzione del dominio di gestione VCF è completa e l'interfaccia di SDDC Manager è accessibile.
- 4 host ESXi configurati per la comunicazione sulla rete di gestione VCF.
- Indirizzi IP riservati per il traffico di storage vMotion e NFS sulla VLAN o sul segmento di rete stabilito a tale scopo.

> Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

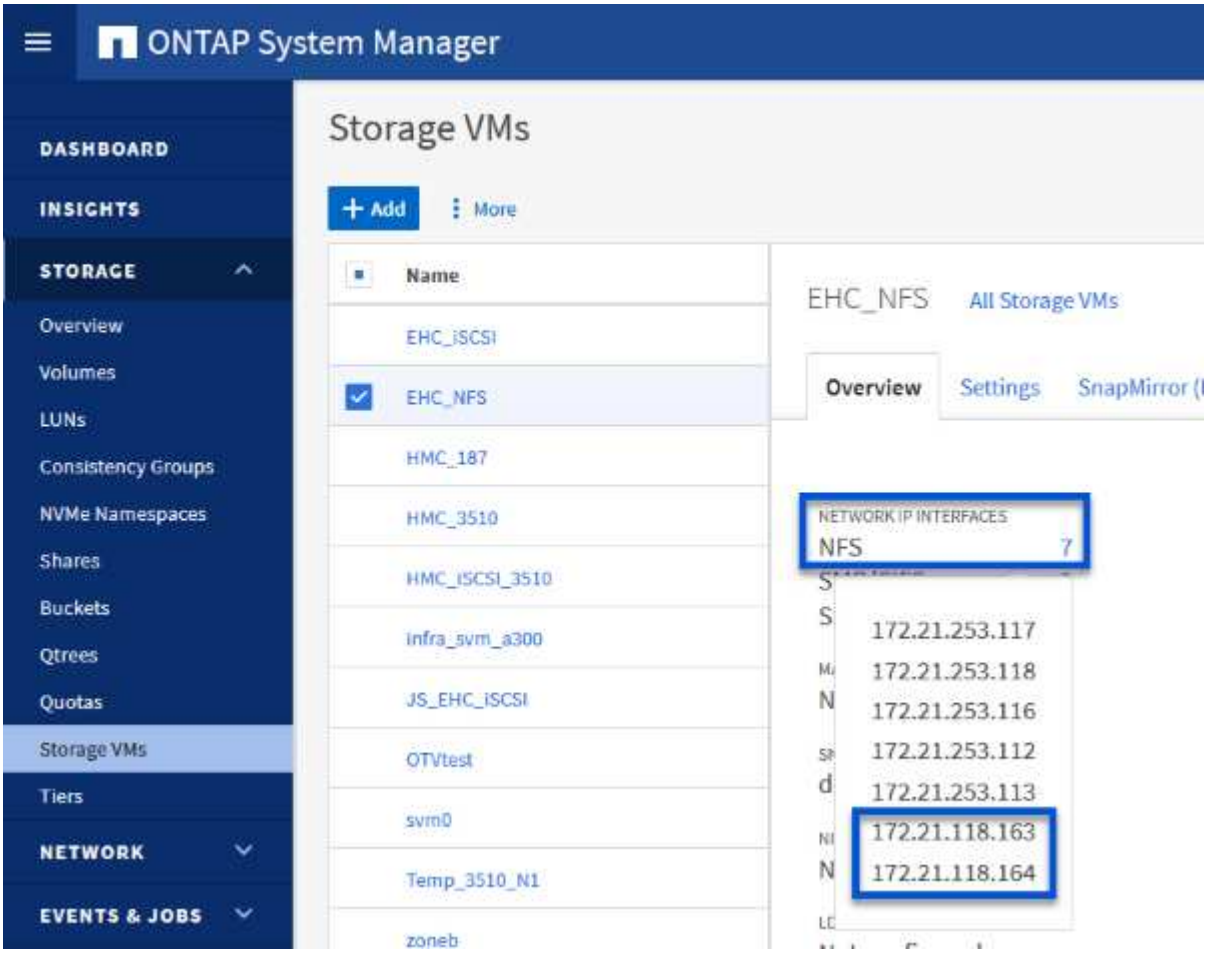
Fasi di implementazione

Per implementare un dominio del carico di lavoro VI con un datastore NFS come storage principale, completare i seguenti passaggi:

Verifica della rete per ONTAP SVM

Verificare che siano state stabilite le interfacce logiche richieste per la rete che trasporta il traffico NFS tra il cluster di storage ONTAP e il dominio del carico di lavoro VI.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic sulla SVM da utilizzare per il traffico NFS. Nella scheda **Panoramica**, sotto **NETWORK IP INTERFACES**, clicca sul valore numerico a destra di **NFS**. Nell'elenco, verifica che siano elencati gli indirizzi IP LIF richiesti.



In alternativa, verifica le LIF associate a una SVM dalla CLI di ONTAP utilizzando il seguente comando:

```
network interface show -vserver <SVM_NAME>
```

1. Verificare che gli host ESXi siano in grado di comunicare con il server NFS ONTAP. Accedere all'host ESXi tramite SSH e eseguire il ping della LIF SVM:

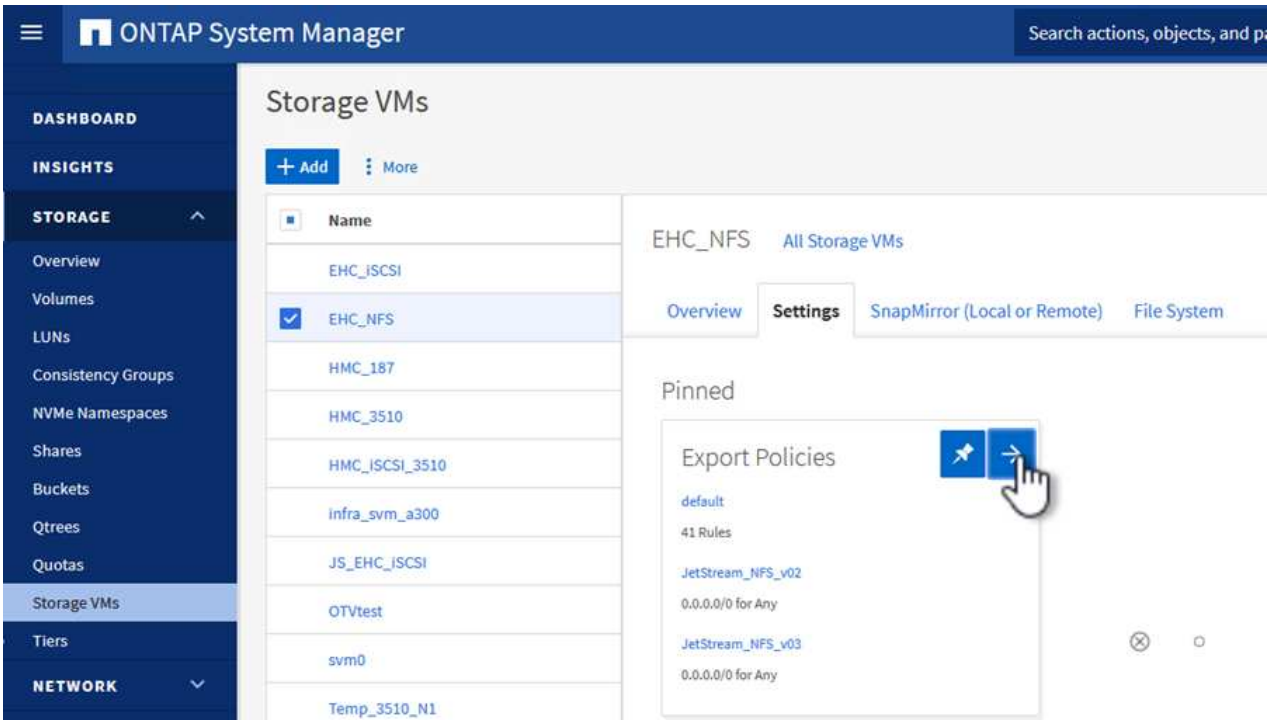
```
vmkping <IP Address>
```

Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

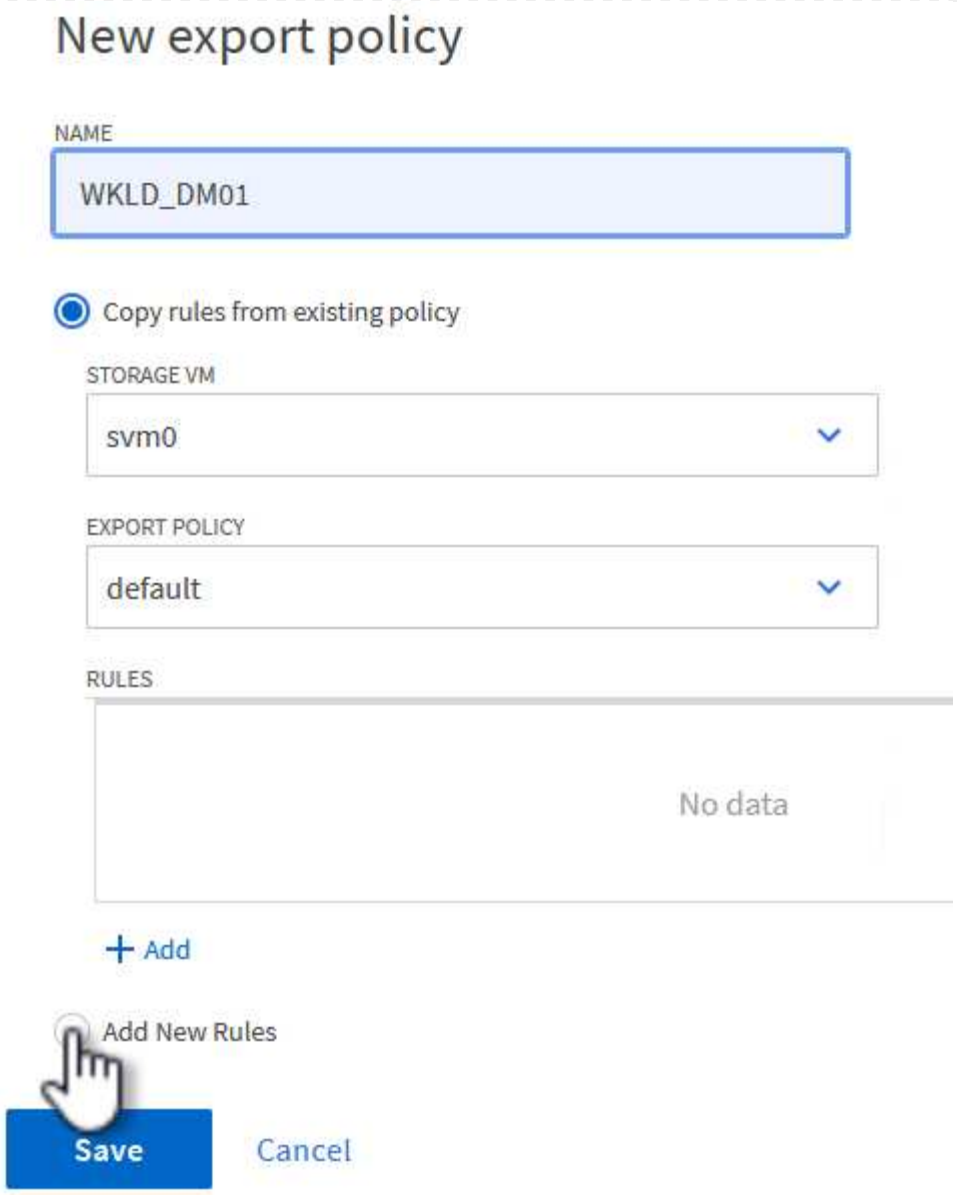
Crea una policy di esportazione per la condivisione del volume NFS

Creare una policy di esportazione in ONTAP System Manager per definire il controllo dell'accesso per i volumi NFS.

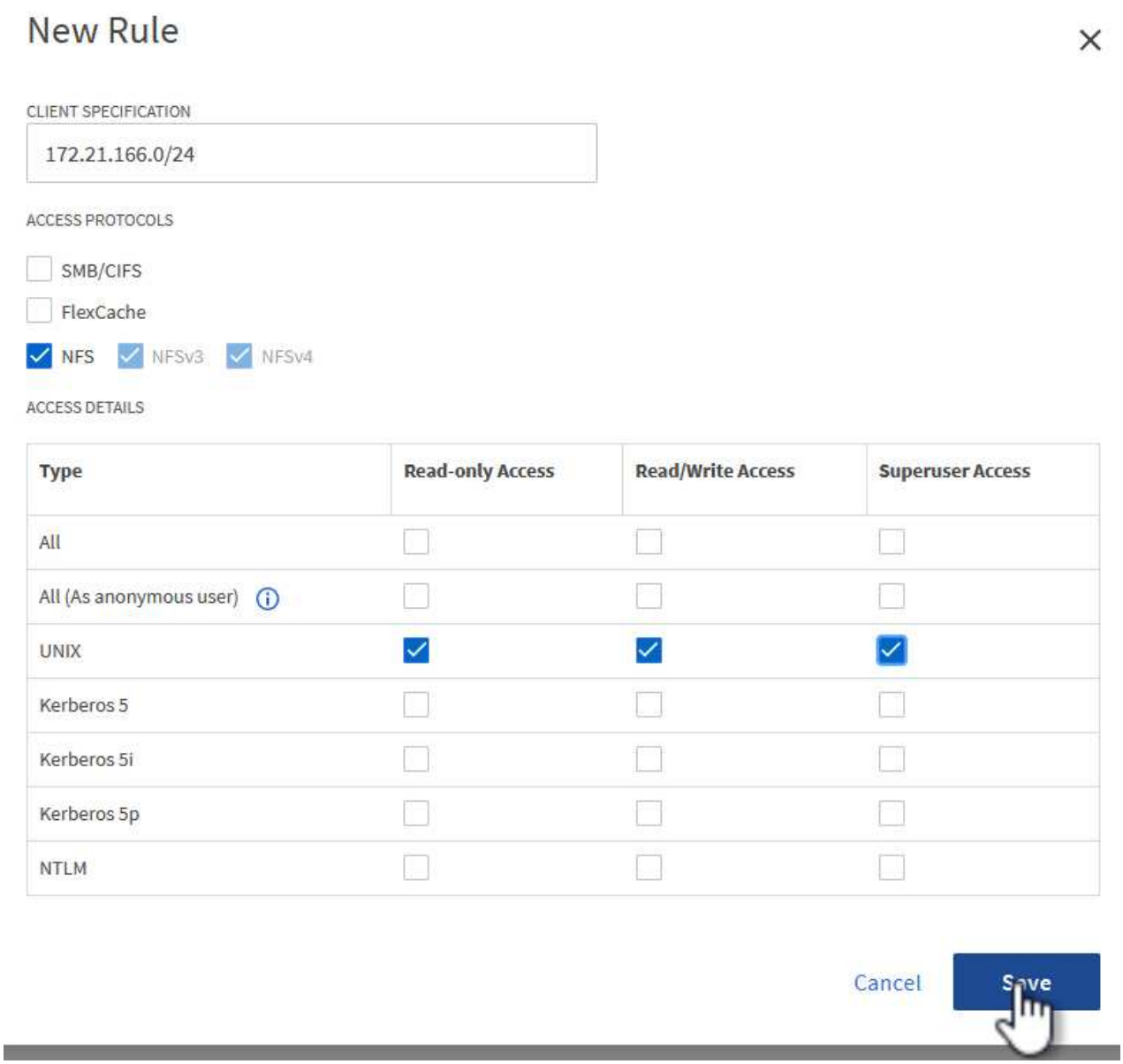
1. In Gestione sistema di ONTAP, fare clic su **Storage VM** nel menu a sinistra e selezionare una SVM dall'elenco.
2. Nella scheda **Impostazioni** individuare **Esporta criteri** e fare clic sulla freccia per accedere.



3. Nella finestra **Nuova policy di esportazione** aggiungere un nome per la policy, fare clic sul pulsante **Aggiungi nuove regole**, quindi sul pulsante **+Aggiungi** per iniziare ad aggiungere una nuova regola.



4. Immettere gli indirizzi IP, l'intervallo degli indirizzi IP o la rete che si desidera includere nella regola. Deselezionare le caselle **SMB/CIFS** e **FlexCache** e selezionare i dettagli di accesso riportati di seguito. La selezione delle caselle UNIX è sufficiente per l'accesso all'host ESXi.



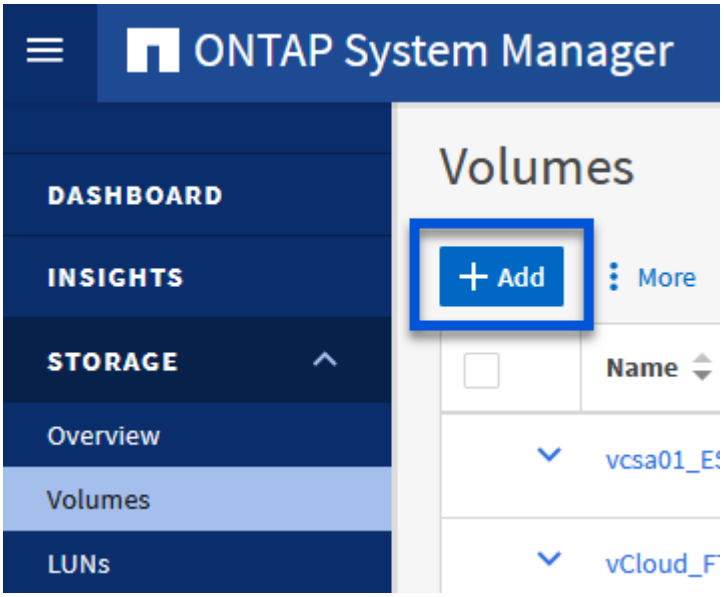
> Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario garantire che il criterio di esportazione includa la rete di gestione VCF per consentire la convalida.

5. Una volta immesse tutte le regole, fare clic sul pulsante **Salva** per salvare la nuova politica di esportazione.
6. In alternativa, è possibile creare criteri e regole di esportazione nella CLI di ONTAP. Fare riferimento alla procedura per la creazione di un criterio di esportazione e l'aggiunta di regole nella documentazione di ONTAP.
   - Utilizzare l'interfaccia CLI di ONTAP per "Creare una policy di esportazione".
   - Utilizzare l'interfaccia CLI di ONTAP per "Aggiungere una regola a un criterio di esportazione".

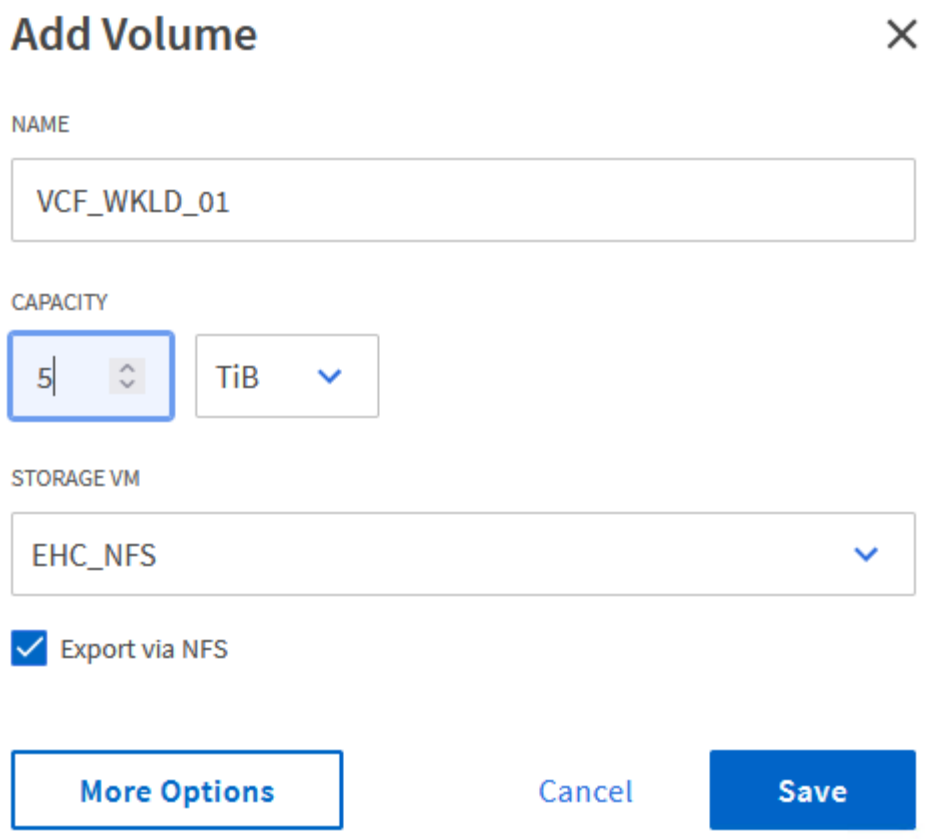
Creazione di un volume NFS

Creare un volume NFS sul sistema storage ONTAP da utilizzare come datastore nell'implementazione del dominio dei carichi di lavoro.

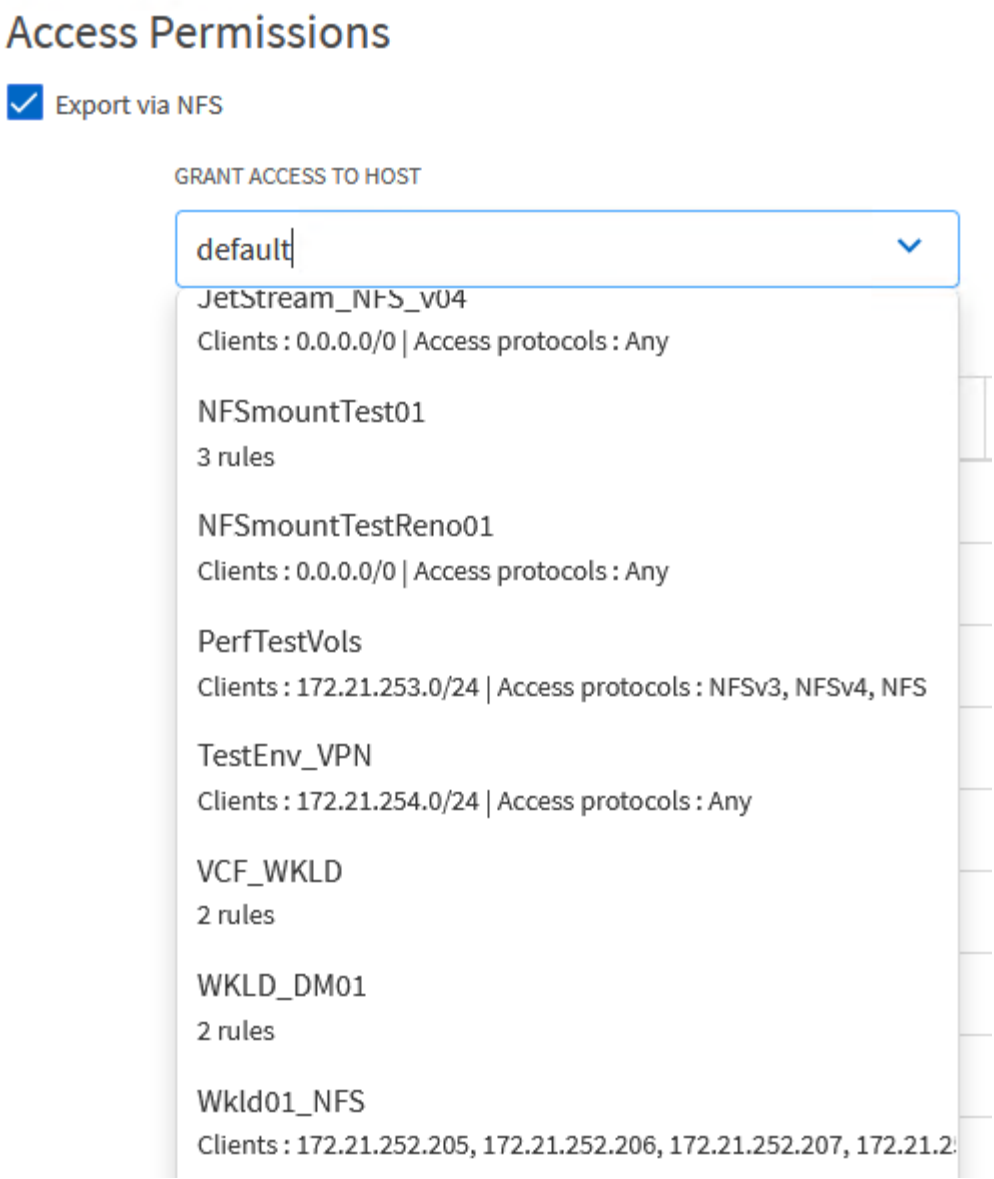
1. Da Gestione di sistema di ONTAP, accedere a **archiviazione > volumi** nel menu a sinistra e fare clic su **+Aggiungi** per creare un nuovo volume.



2. Aggiungi un nome per il volume, compila la capacità desiderata e seleziona la VM di archiviazione che ospiterà il volume. Fare clic su **altre opzioni** per continuare.



3. In autorizzazioni di accesso, selezionare il criterio di esportazione che include la rete di gestione VCF o l'indirizzo IP e gli indirizzi IP di rete NFS che verranno utilizzati per la convalida del traffico NFS Server e NFS.



+

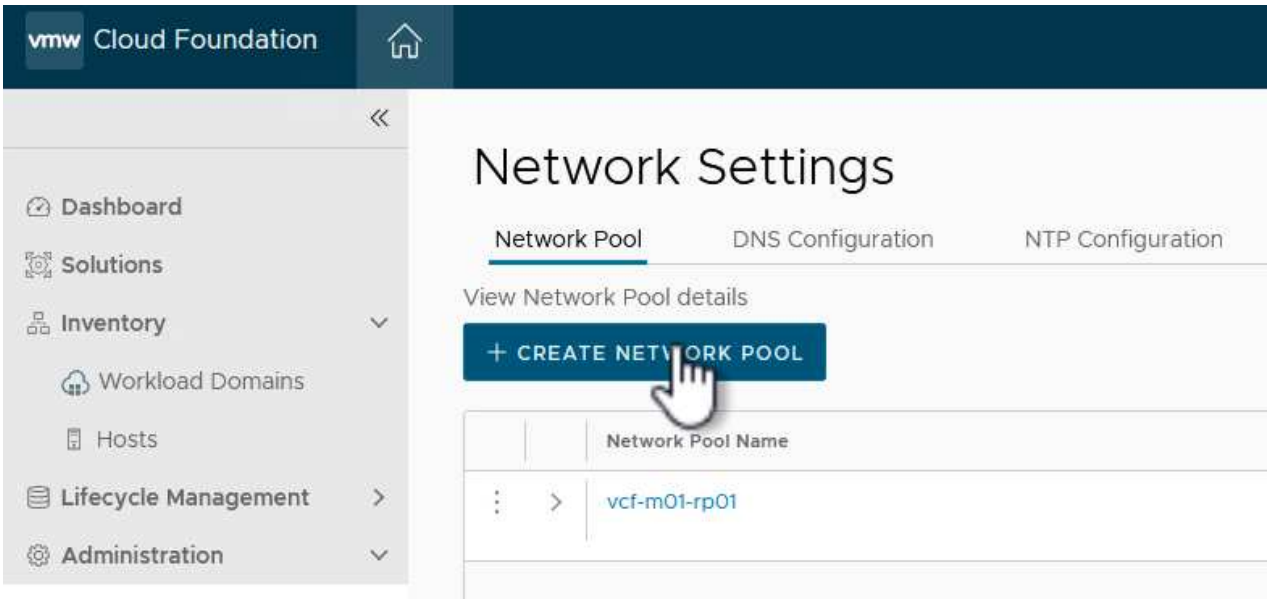
> Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

1. In alternativa, è possibile creare volumi ONTAP nella CLI di ONTAP. Per ulteriori informazioni, fare riferimento a. "lun create (crea lun)" Nella documentazione dei comandi ONTAP.

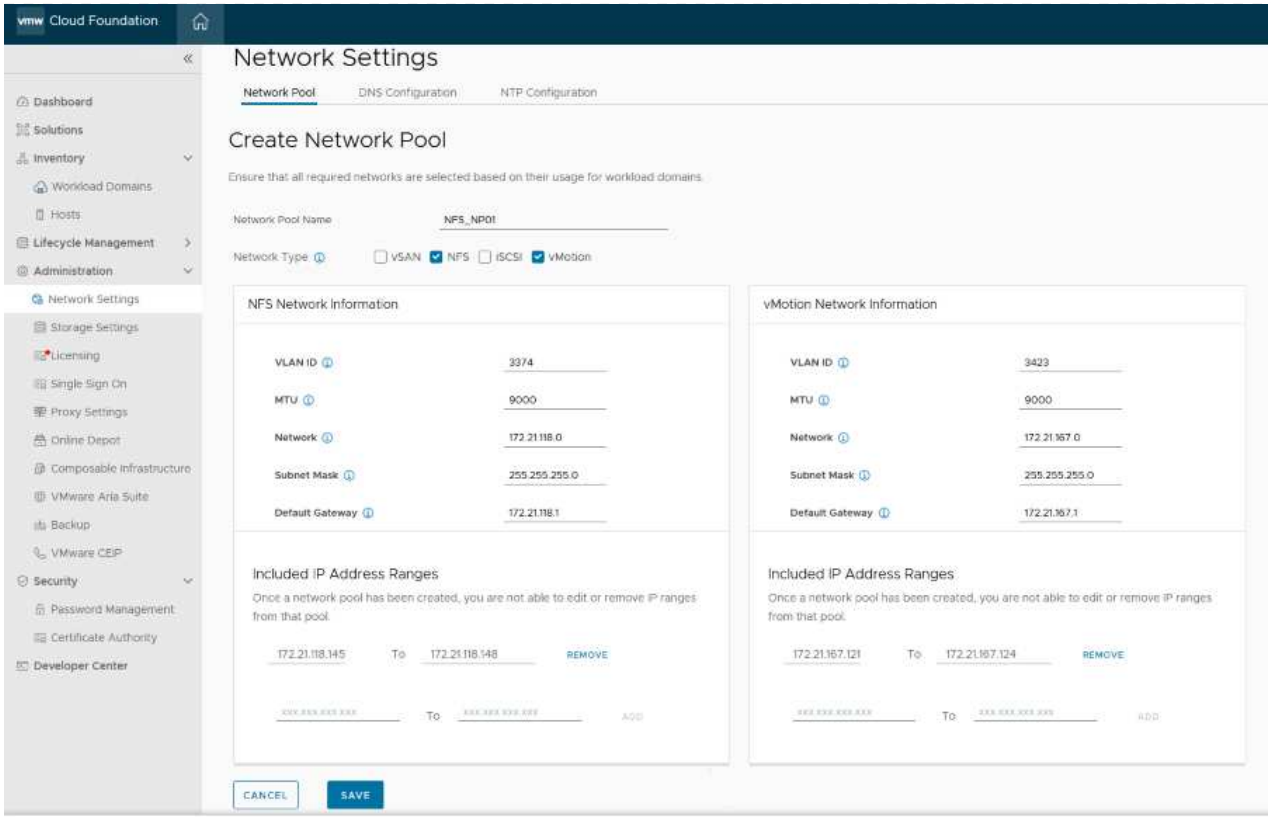
Creare un pool di rete in SDDC Manager

Il pool di rete deve essere creato in SDDC Manager prima di mettere in funzione gli host ESXi, come preparazione per la loro distribuzione in un dominio del carico di lavoro VI. Il pool di rete deve includere le informazioni di rete e gli intervalli di indirizzi IP affinché gli adattatori VMkernel possano essere utilizzati per la comunicazione con il server NFS.

1. Dall'interfaccia Web di SDDC Manager, accedere a **Impostazioni di rete** nel menu a sinistra e fare clic sul pulsante **+ Crea pool di rete**.



2. Immettere un nome per il pool di rete, selezionare la casella di controllo NFS e compilare tutti i dettagli di rete. Ripetere questa operazione per le informazioni sulla rete vMotion.



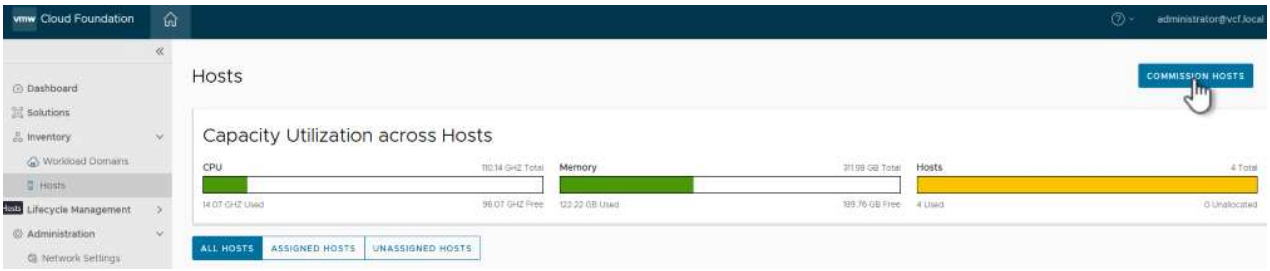
3. Fare clic sul pulsante **Salva** per completare la creazione del pool di rete.

La commissione ospita

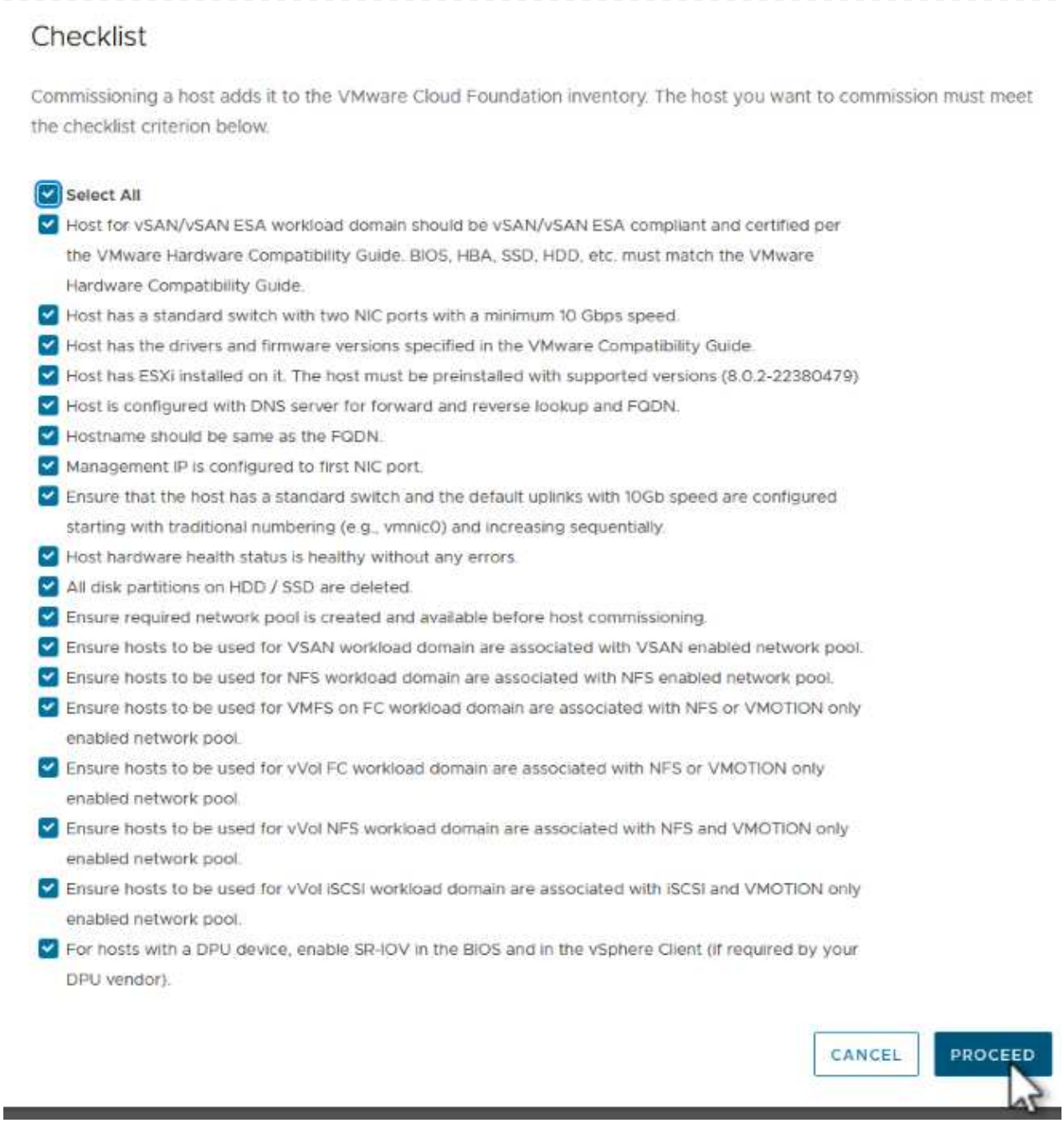
Prima di poter distribuire gli host ESXi come dominio del carico di lavoro, è necessario aggiungerli all'inventario di SDDC Manager. Ciò comporta la fornitura delle informazioni richieste, il superamento della convalida e l'avvio del processo di messa in funzione.

Per ulteriori informazioni, vedere "La commissione ospita" Nella Guida all'amministrazione di VCF.

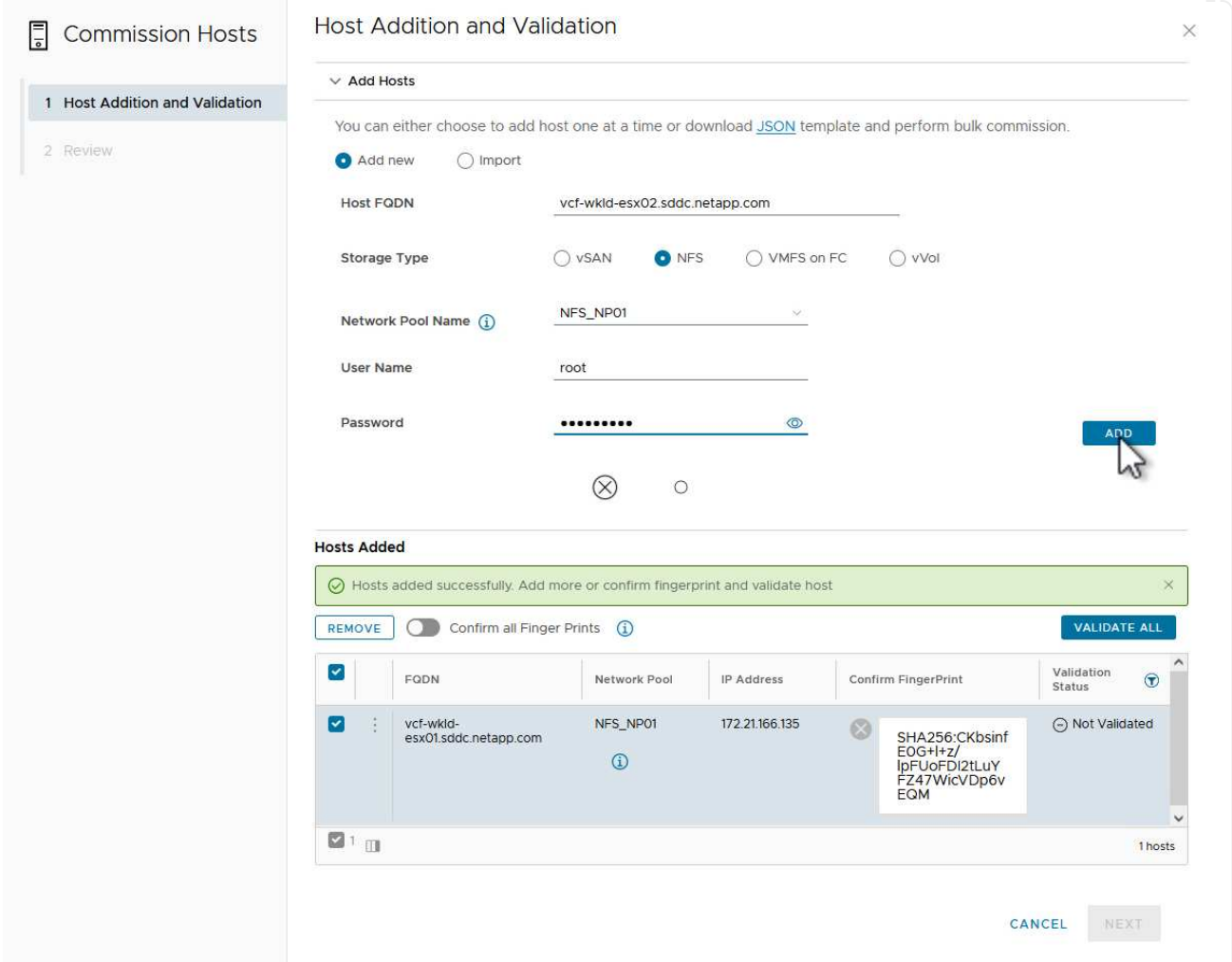
1. Dall'interfaccia di SDDC Manager, accedere a **hosts** nel menu a sinistra e fare clic sul pulsante **Commission hosts**.



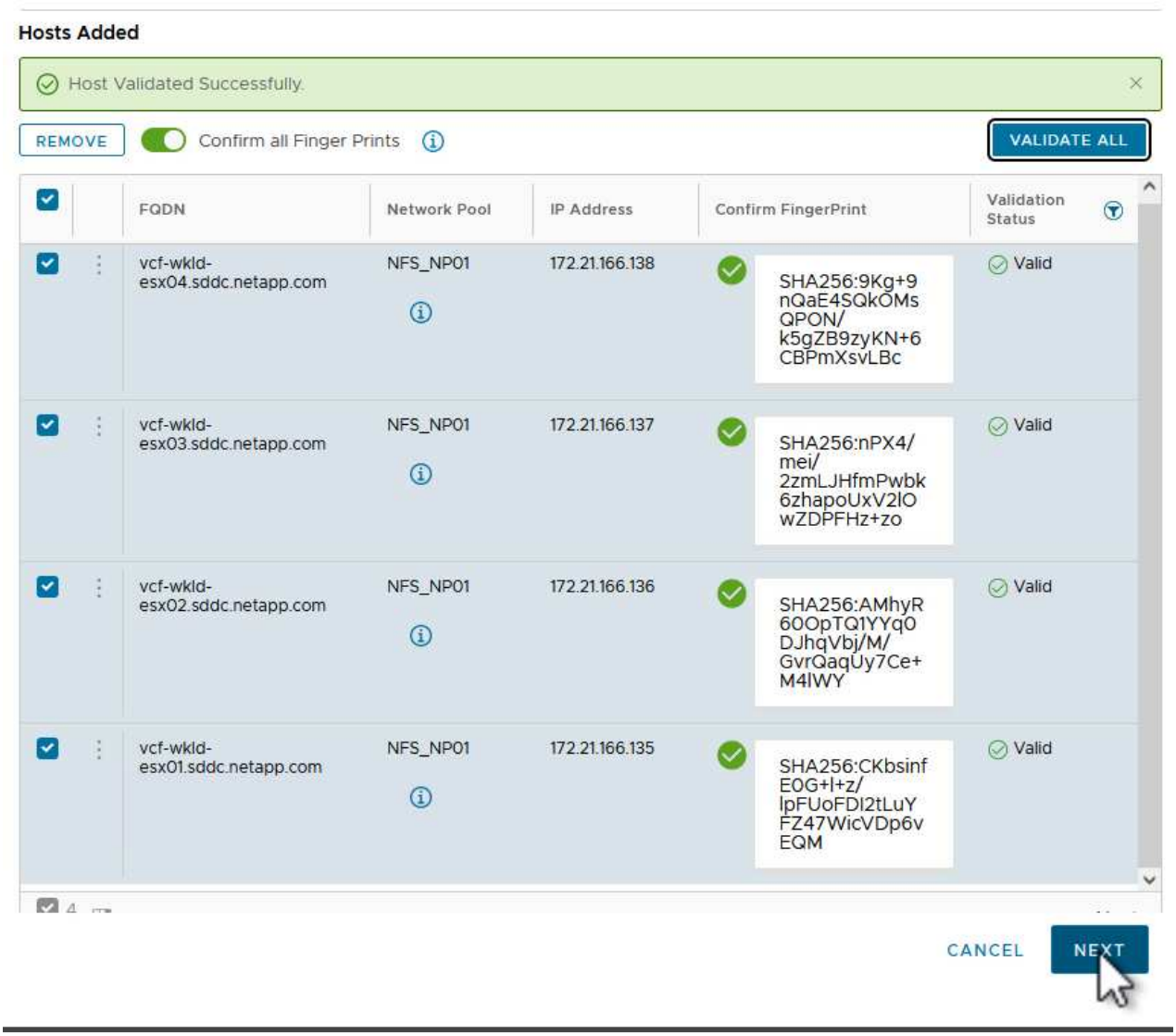
2. La prima pagina è una lista di controllo dei prerequisiti. Selezionare due volte tutti i prerequisiti e selezionare tutte le caselle di controllo per procedere.



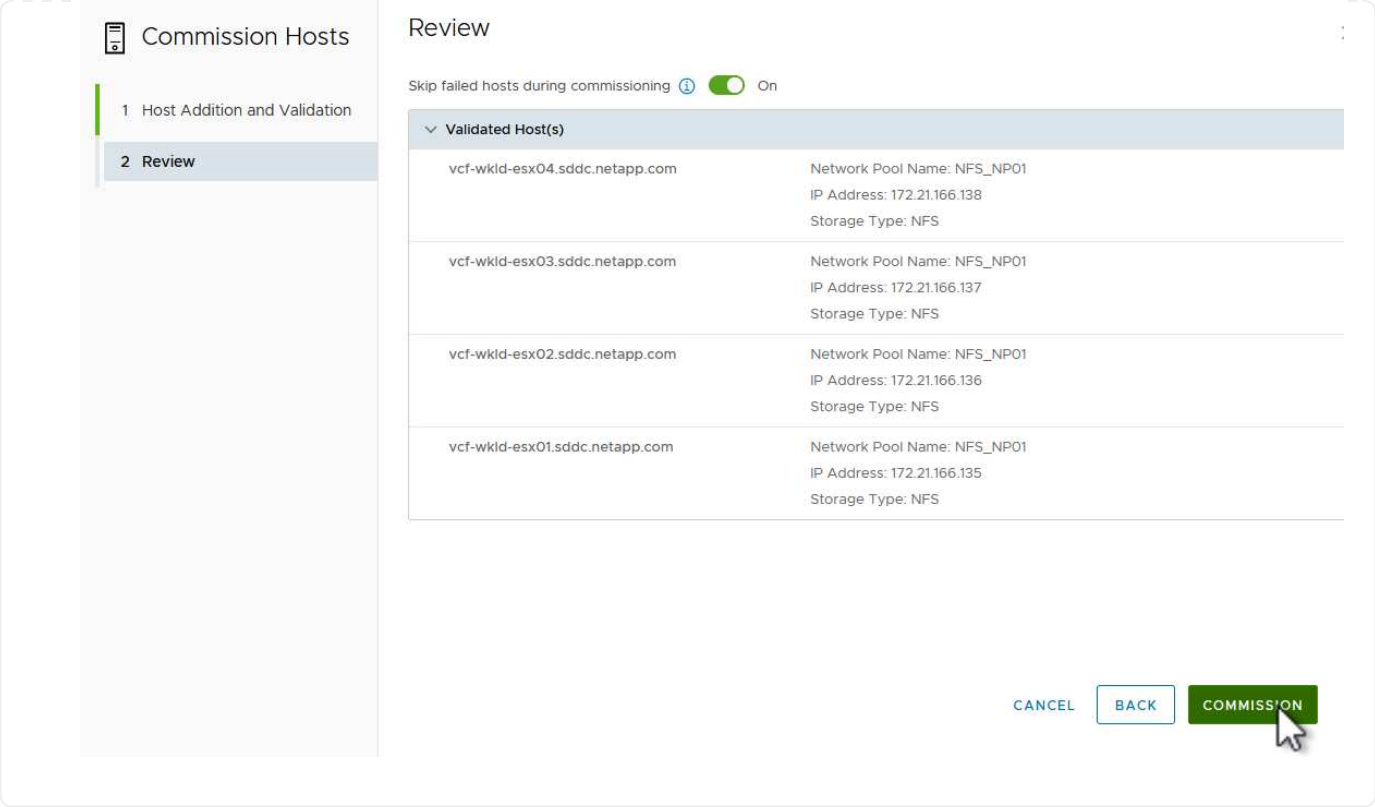
3. Nella finestra **aggiunta host e convalida** compilare il nome **FQDN host**, **tipo di archiviazione**, il nome **pool di rete** che include gli indirizzi IP di archiviazione vMotion e NFS da utilizzare per il dominio del carico di lavoro e le credenziali per accedere all'host ESXi. Fare clic su **Aggiungi** per aggiungere l'host al gruppo di host da convalidare.



4. Una volta aggiunti tutti gli host da convalidare, fare clic sul pulsante **convalida tutto** per continuare.
5. Presupponendo che tutti gli host siano convalidati, fare clic su **Avanti** per continuare.



6. Rivedere l'elenco degli host da mettere in servizio e fare clic sul pulsante **Commissione** per avviare il processo. Monitorare il processo di messa in funzione dal Task pane in SDDC Manager.

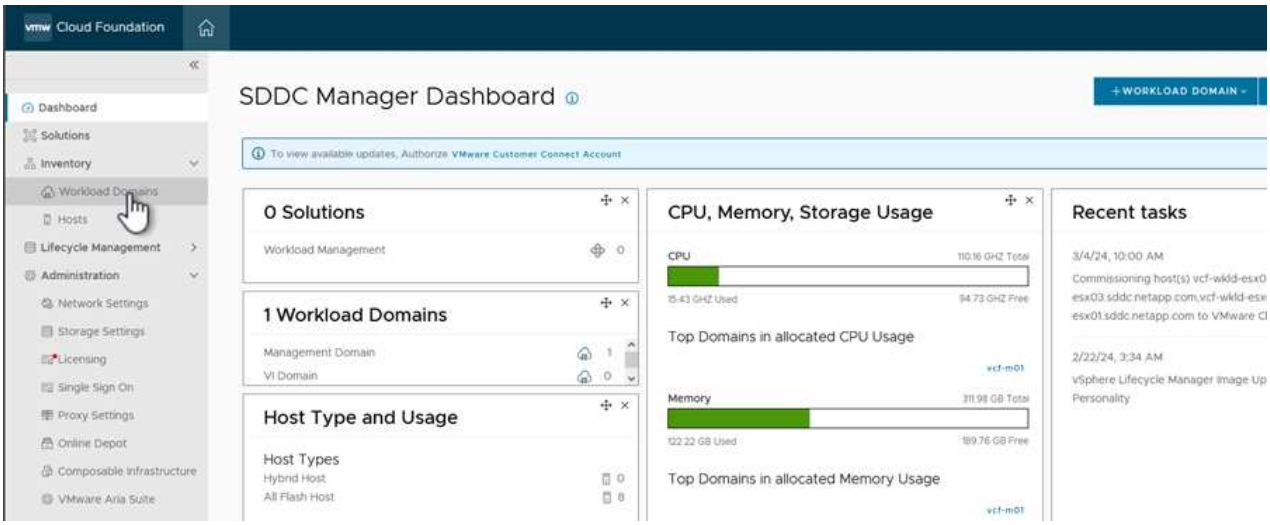

Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

Distribuire il dominio del carico di lavoro VI

La distribuzione dei domini del carico di lavoro VI viene eseguita utilizzando l'interfaccia di VCF Cloud Manager. Qui verranno presentate solo le fasi relative alla configurazione dello storage.

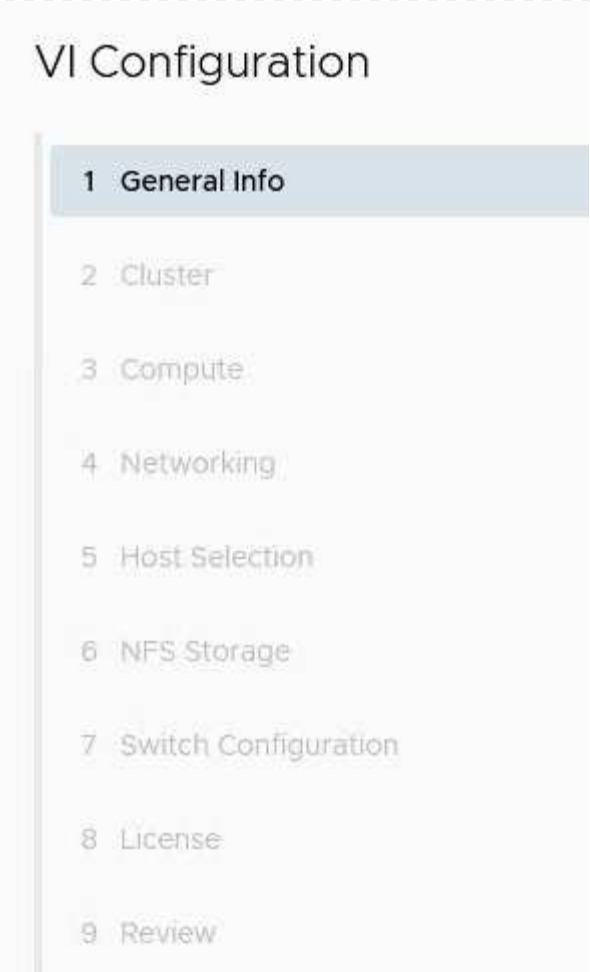
Per istruzioni dettagliate sull'implementazione di un dominio del carico di lavoro VI, fare riferimento a. "Distribuire un dominio del carico di lavoro VI utilizzando l'interfaccia utente di SDDC Manager".

1. Dalla dashboard di SDDC Manager, fare clic su **+ workload Domain** nell'angolo in alto a destra per creare un nuovo dominio del carico di lavoro.



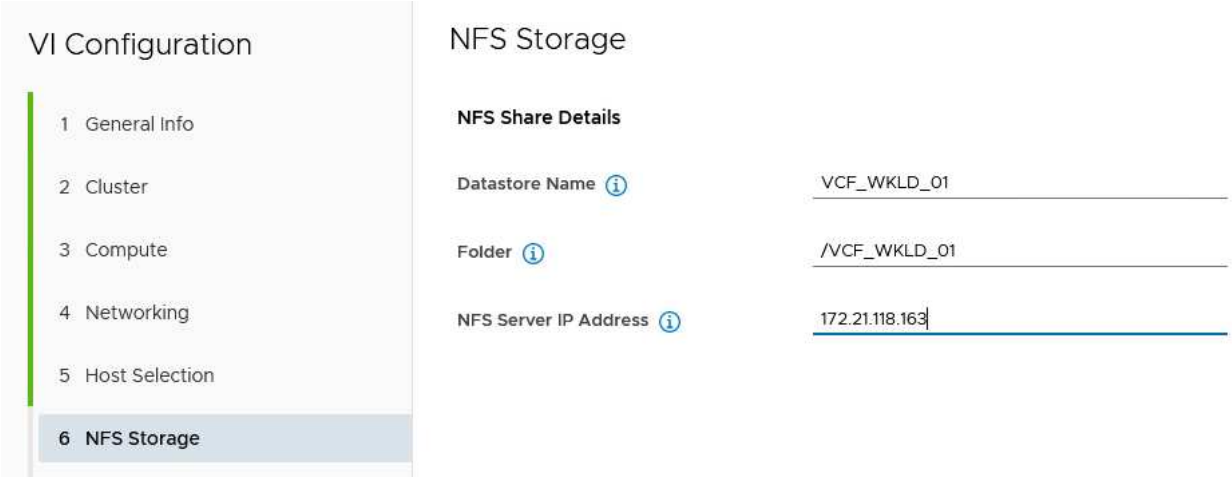
2. Nella procedura guidata di configurazione vi compilare le sezioni **informazioni generali, cluster, elaborazione, rete** e **selezione host** secondo necessità.

Per informazioni sulla compilazione delle informazioni richieste nella procedura guidata di configurazione VI, fare riferimento a. "Distribuire un dominio del carico di lavoro VI utilizzando l'interfaccia utente di SDDC Manager".

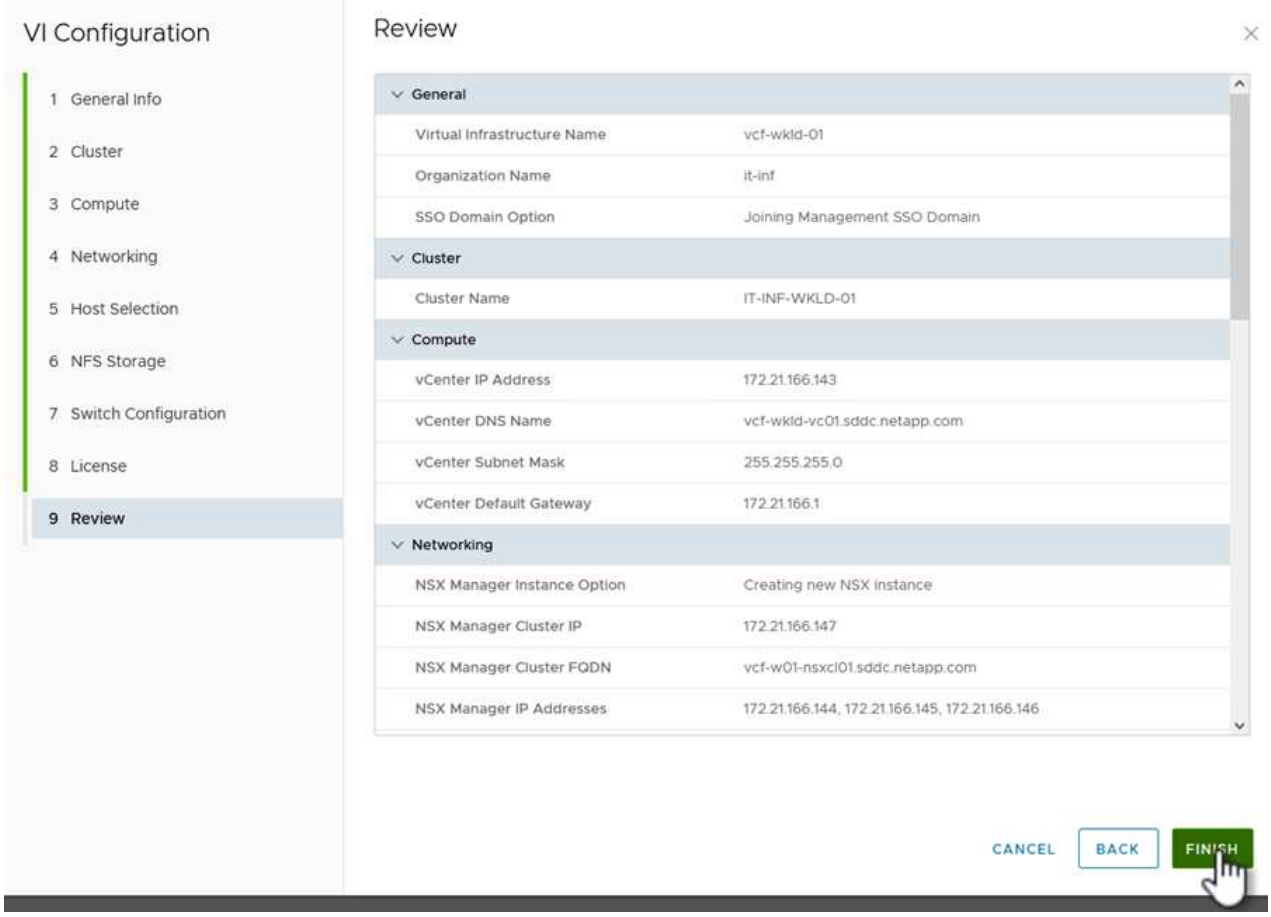


+

1. Nella sezione Storage NFS compilare il Nome datastore, il punto di montaggio della cartella del volume NFS e l'indirizzo IP della LIF delle macchine virtuali di storage NFS di ONTAP.



2. Nella procedura guidata di configurazione VI completare la procedura di configurazione e licenza dello switch, quindi fare clic su **fine** per avviare il processo di creazione del dominio del carico di lavoro.



3. Monitorare il processo e risolvere eventuali problemi di convalida che si verificano durante il processo.

Installare il plug-in NetApp NFS per VMware VAAI

Il plug-in NFS di NetApp per VMware VAAI integra le librerie di dischi virtuali VMware installate sull'host ESXi e offre operazioni di cloning con performance più elevate e completate più rapidamente. Questa è una procedura consigliata quando si utilizzano i sistemi storage ONTAP con VMware vSphere.

Per istruzioni dettagliate sull'implementazione del plug-in NFS NetApp per VMware VAAI, seguire le istruzioni sul sito "Installare il plug-in NetApp NFS per VMware VAAI".

Video dimostrativo per questa soluzione

Archivi dati NFS come archiviazione principale per i domini del carico di lavoro VCF

Utilizzare gli strumenti di ONTAP per configurare lo storage supplementare (NFS e vVol) per i domini del carico di lavoro VCF

In questo scenario dimostreremo come implementare e utilizzare ONTAP Tools per VMware vSphere per configurare sia un archivio dati **NFS** che un archivio dati **vVol** per un dominio del carico di lavoro VCF.

NFS viene utilizzato come protocollo storage per il datastore vVol.

Autore: Josh Powell, Ravi BCB

Panoramica dello scenario

Questo scenario copre i seguenti passaggi di alto livello:

- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico NFS.
- Creare un gruppo di porte distribuite per la rete NFS nel dominio del carico di lavoro VI.
- Creare un adattatore vmkernel per NFS sugli host ESXi per il dominio del carico di lavoro VI.
- Distribuire gli strumenti ONTAP nel dominio del carico di lavoro VI.
- Creare un nuovo datastore NFS nel dominio del carico di lavoro VI.
- Creare un nuovo datastore vVol nel dominio del carico di lavoro VI.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP AFF con porte per dati fisici su switch ethernet dedicati al traffico di storage.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.

NetApp consiglia progettazioni di rete ridondanti per NFS, per fornire la tolleranza agli errori di sistemi storage, switch, adattatori di rete e sistemi host. È comune implementare NFS con una singola subnet o più subnet a seconda dei requisiti architetturali.

Fare riferimento a. "Best practice per l'esecuzione di NFS con VMware vSphere" Per informazioni dettagliate specifiche di VMware vSphere.

Per assistenza sulla rete per l'utilizzo di ONTAP con VMware vSphere, fare riferimento al "Configurazione di rete - NFS" Della documentazione relativa alle applicazioni aziendali NetApp.

Questa documentazione illustra il processo di creazione di una nuova SVM e specifica le informazioni relative all'indirizzo IP per creare LIF multipli per il traffico NFS. Per aggiungere nuove LIF a una SVM esistente, fare riferimento a. "Creazione di una LIF (interfaccia di rete)".

Fasi di implementazione

Per implementare ONTAP Tools e utilizzarlo per creare un datastore vVol e NFS nel dominio di gestione VCF, completare i seguenti passaggi:

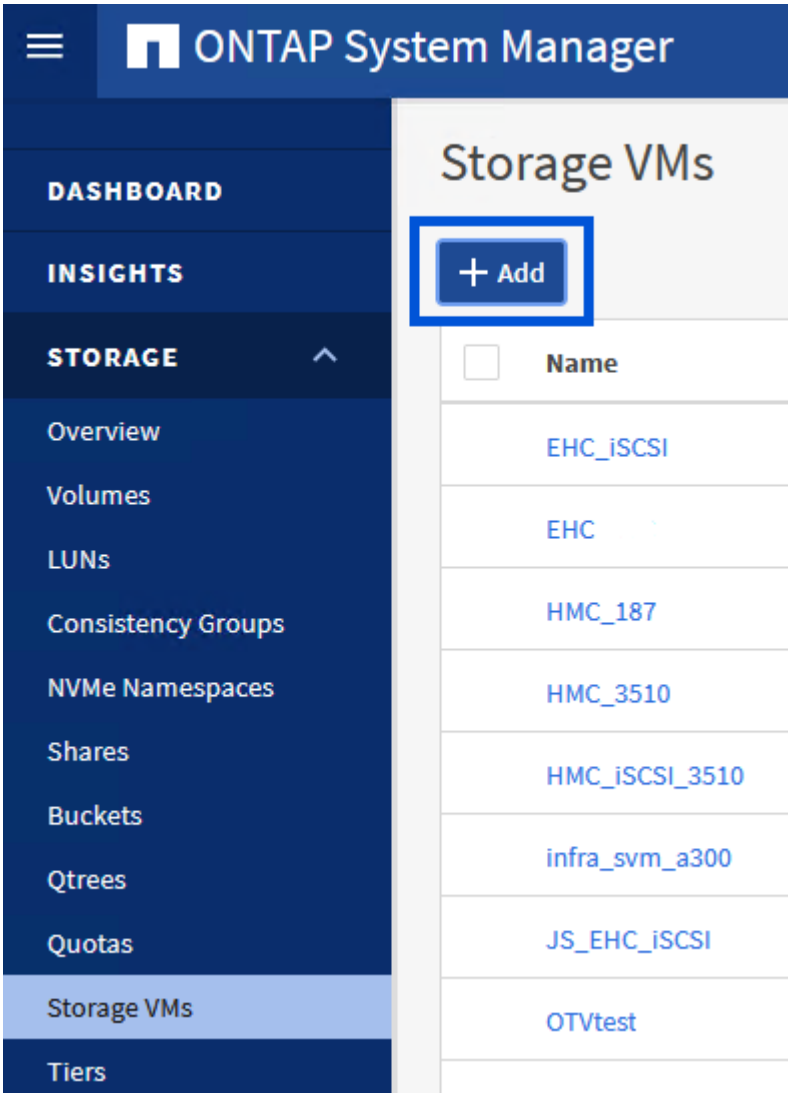
Crea SVM e LIF su un sistema storage ONTAP

Il passaggio seguente viene eseguito in Gestione di sistema di ONTAP.

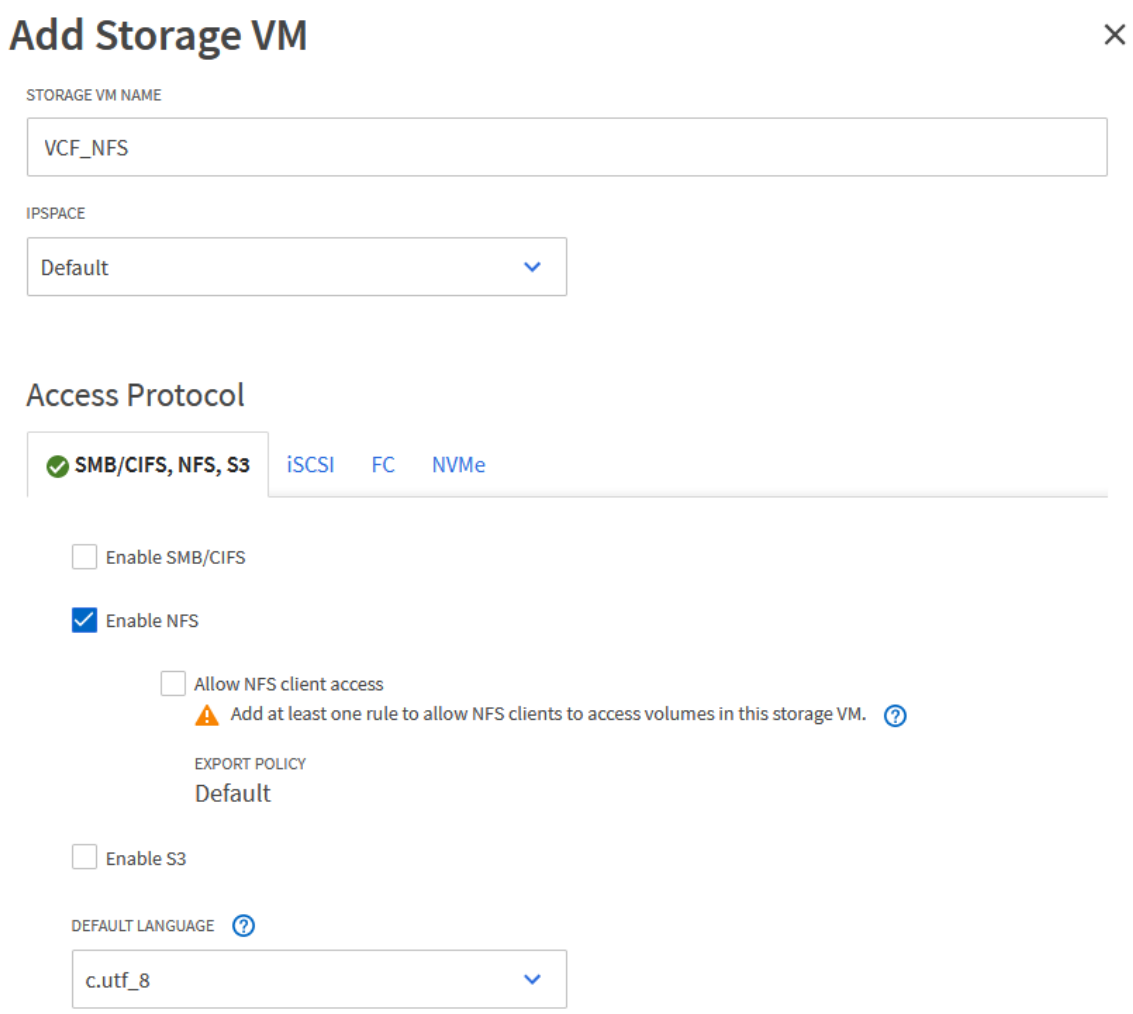
Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per il traffico NFS.

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.

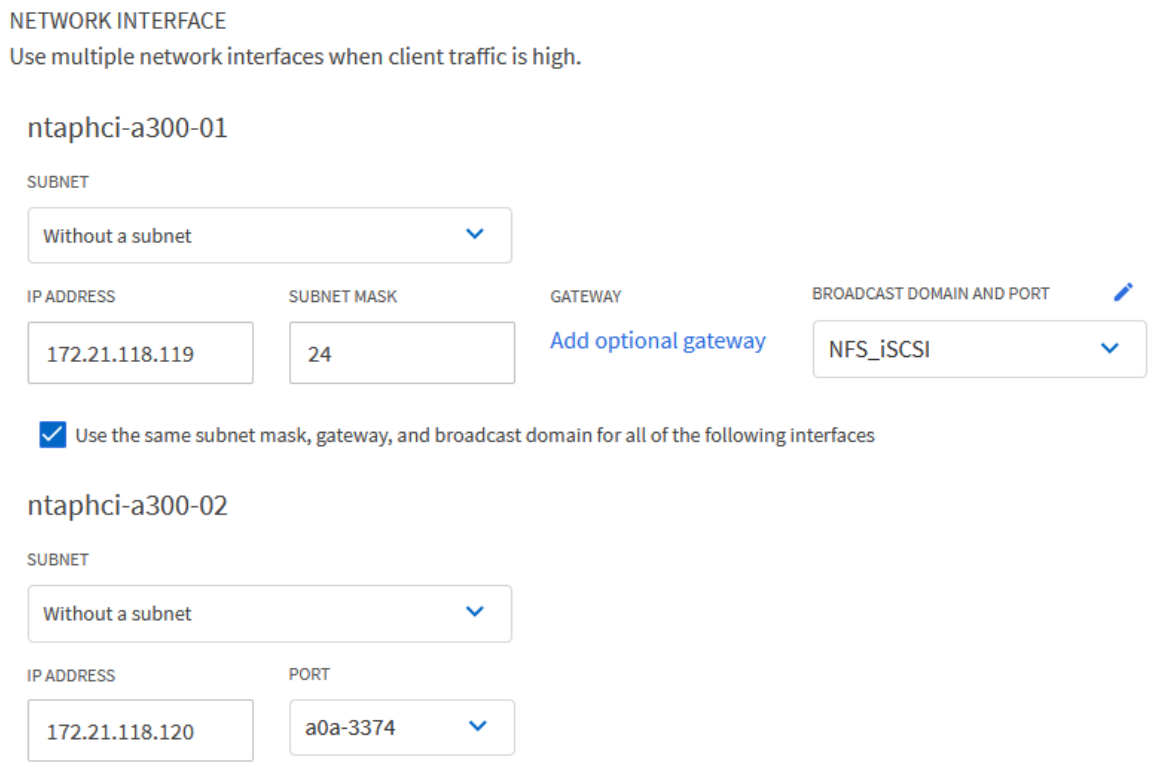


2. Nella procedura guidata **Add Storage VM** (Aggiungi VM di storage) fornire un **Name** (Nome) per la SVM, selezionare **IP Space** (spazio IP), quindi, in **Access Protocol** (protocollo di accesso), fare clic sulla scheda **SMB/CIFS, NFS, S3** e selezionare la casella **Enable NFS** (Abilita NFS*).

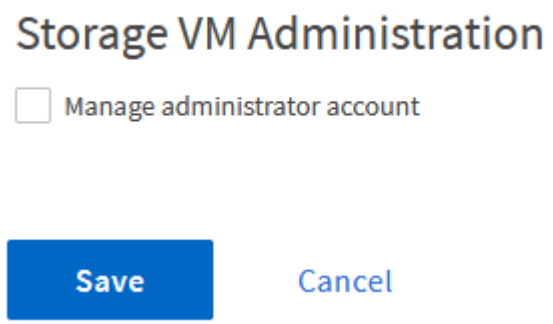


Non è necessario selezionare il pulsante **Allow NFS client access** (Consenti accesso client NFS) poiché ONTAP Tools per VMware vSphere verrà utilizzato per automatizzare il processo di distribuzione del datastore. Ciò include la fornitura dell'accesso client agli host ESXi.

3. Nella sezione **interfaccia di rete** compilare i campi **indirizzo IP**, **Subnet Mask** e **Broadcast Domain and Port** per la prima LIF. Per LIF successive, la casella di controllo può essere abilitata per usare impostazioni comuni a tutte le LIF rimanenti o per usare impostazioni separate.



4. Scegliere se attivare l'account Storage VM Administration (per ambienti multi-tenancy) e fare clic su **Save** (Salva) per creare la SVM.



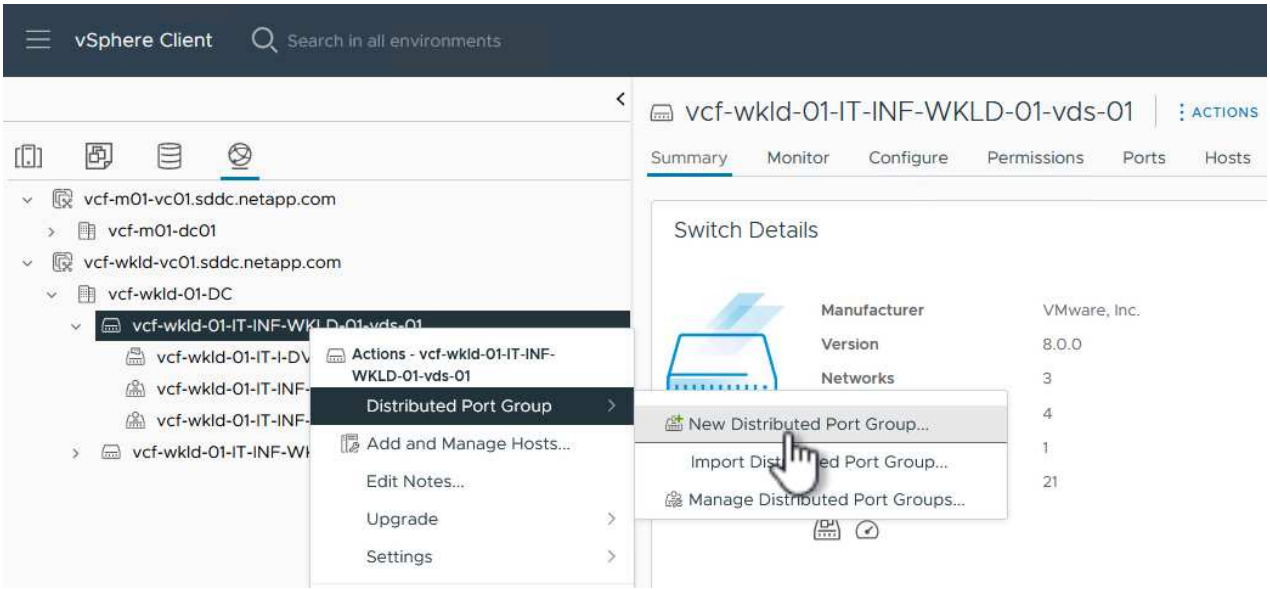
Configurare il networking per NFS sugli host ESXi

I seguenti passaggi vengono eseguiti sul cluster VI workload Domain utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-on, pertanto il client vSphere è comune nei domini di gestione e carico di lavoro.

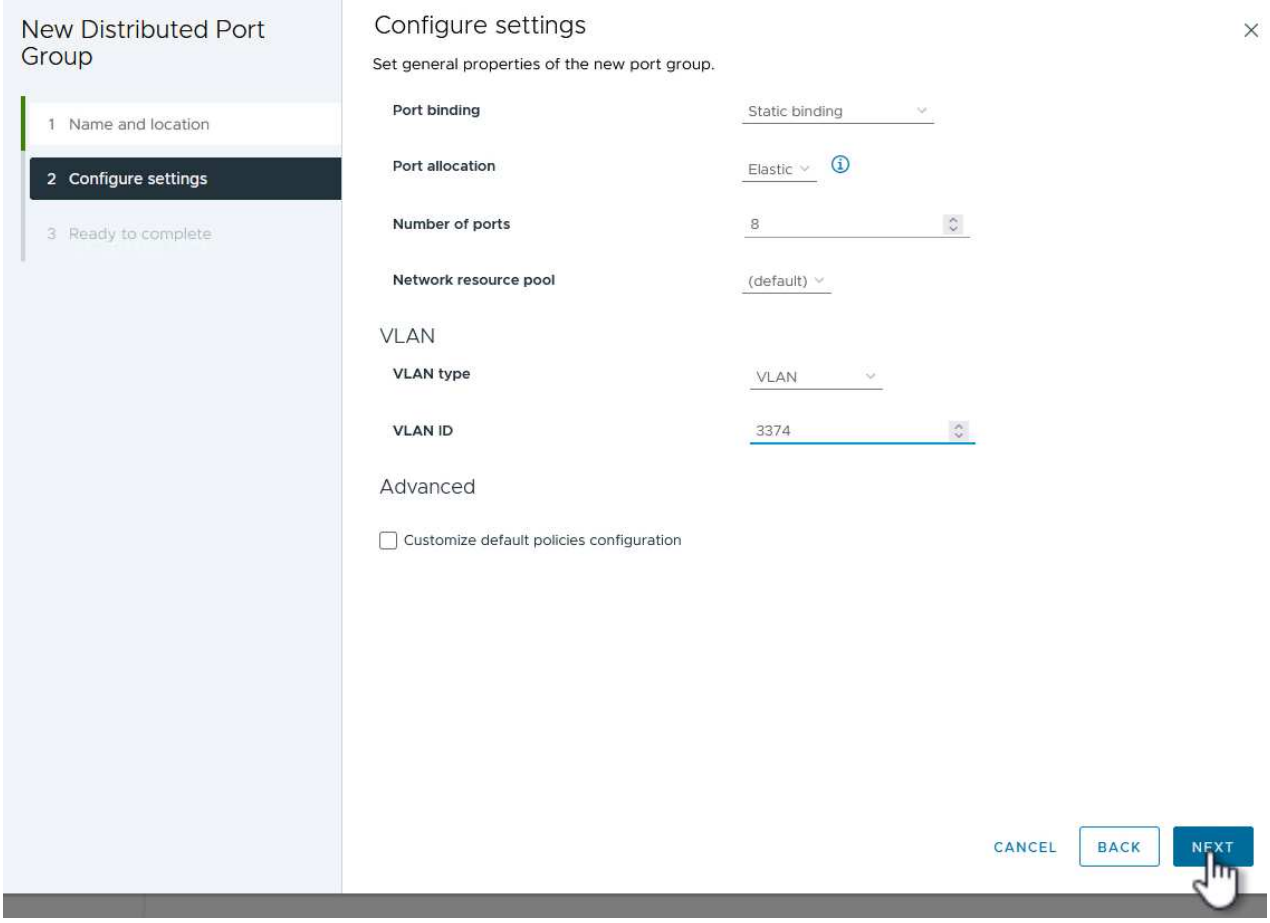
Creare un gruppo di porte distribuite per il traffico NFS

Completare quanto segue per creare un nuovo gruppo di porte distribuite per la rete per il trasporto del traffico NFS:

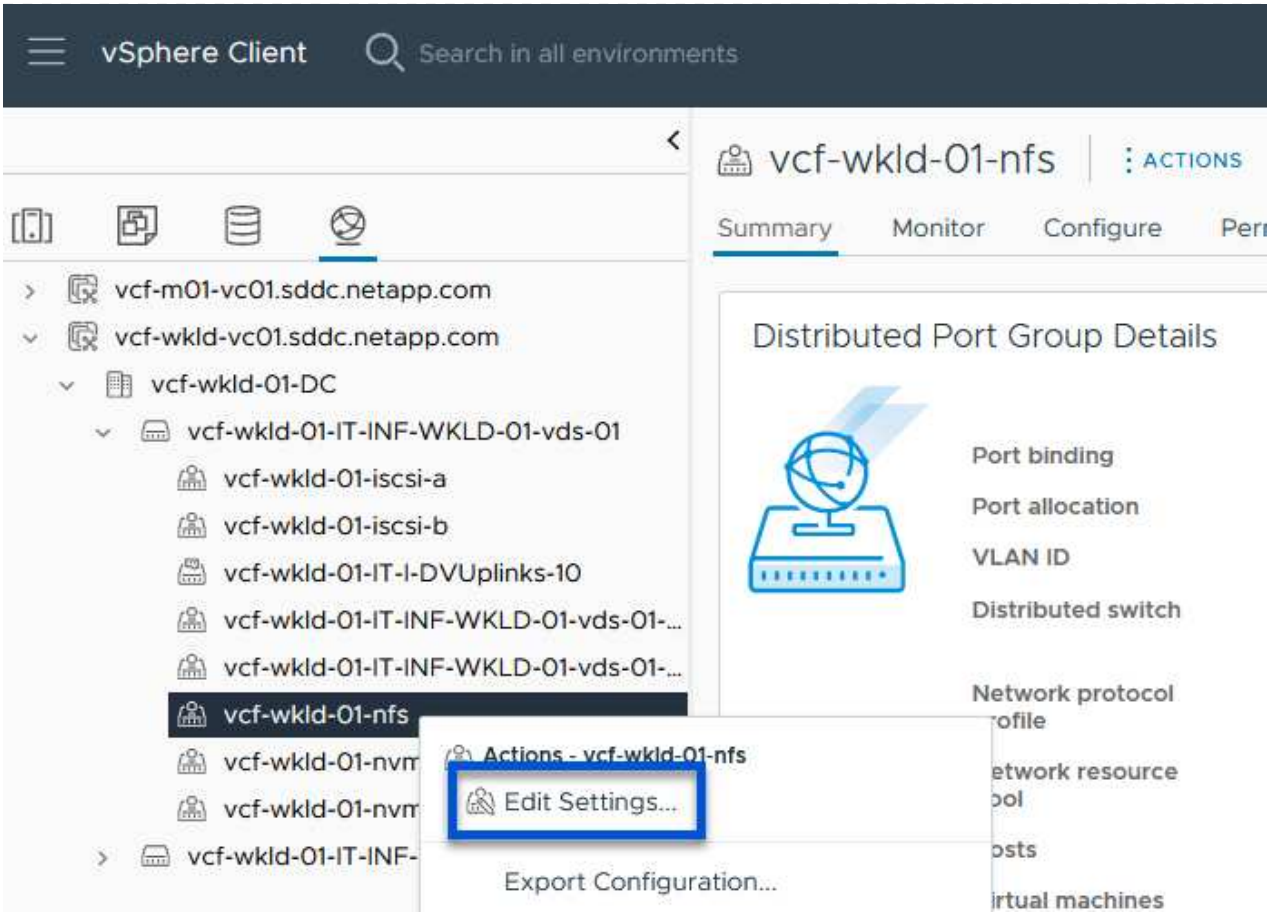
1. Dal client vSphere , accedere a **Inventory > Networking** per il dominio del carico di lavoro. Passare allo Switch distribuito esistente e scegliere l'azione da creare **nuovo Gruppo di porte distribuite…**.



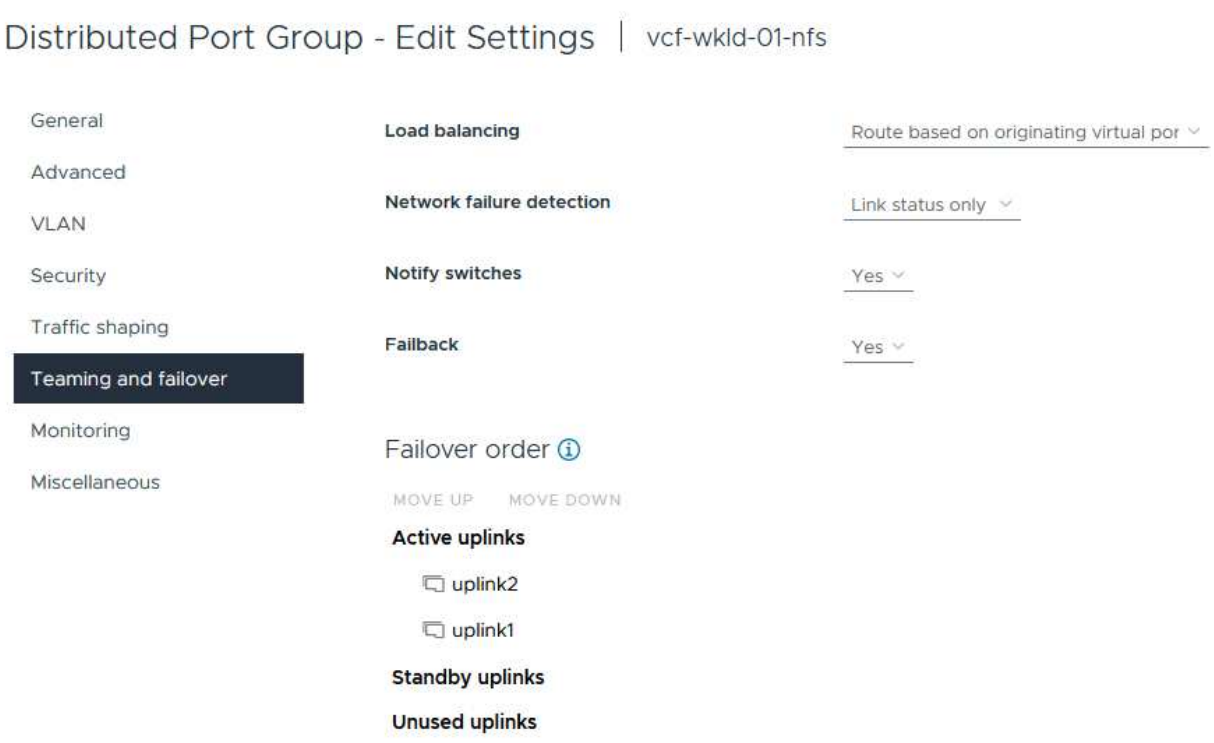
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare clic su **Avanti** per continuare.



4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **fine** per creare il nuovo gruppo di porte distribuite.
5. Una volta creato il gruppo di porte, accedere al gruppo di porte e selezionare l'azione **Modifica impostazioni…**.



6. Nella pagina **Gruppo porte distribuite - Modifica impostazioni**, accedere a **raggruppamento e failover** nel menu a sinistra. Abilitare il raggruppamento per gli uplink da utilizzare per il traffico NFS assicurandosi che siano Uniti nell'area **uplink attivi**. Spostare gli uplink non utilizzati verso il basso su **uplink non utilizzati**.

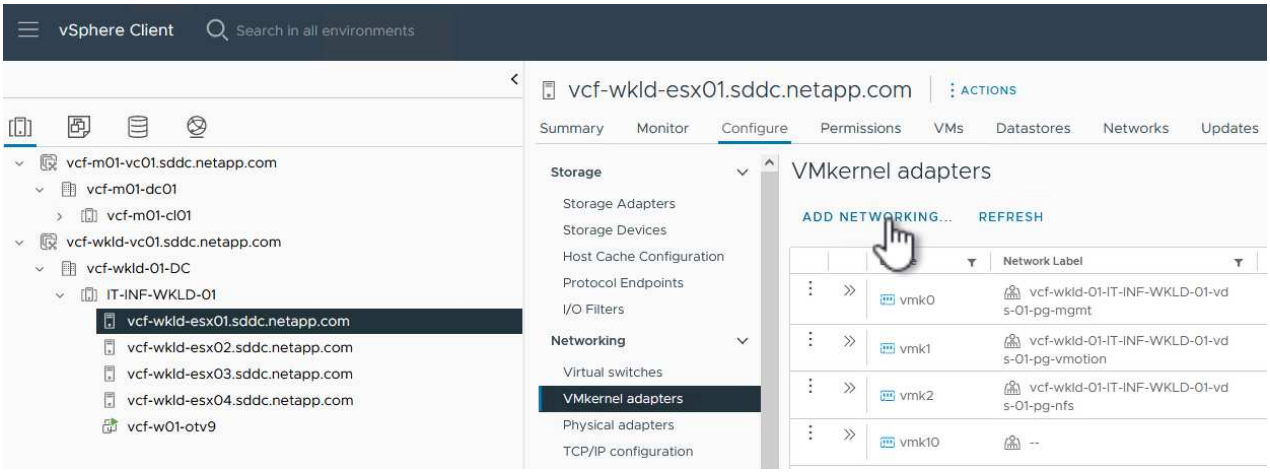


7. Ripetere questa procedura per ogni host ESXi nel cluster.

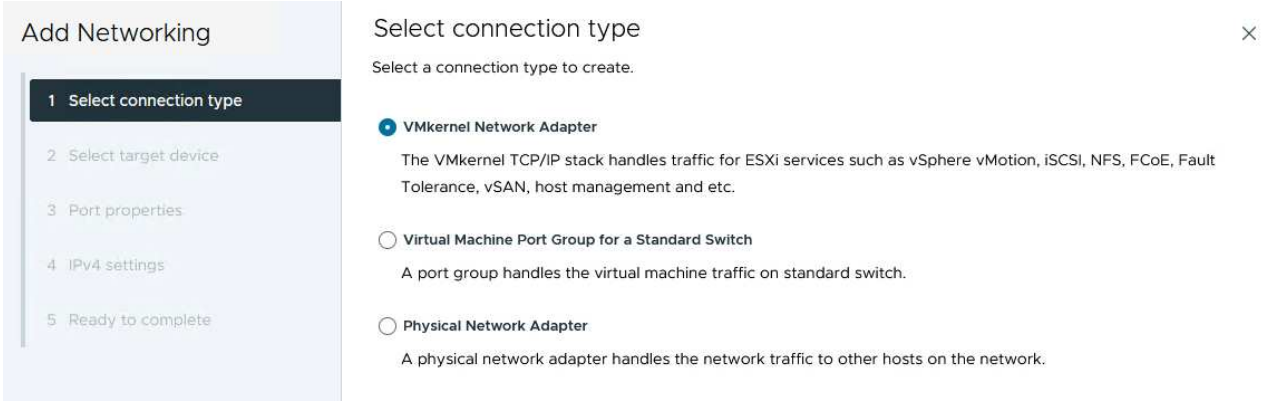
Creare un adattatore VMkernel su ciascun host ESXi

Ripetere questo processo su ogni host ESXi nel dominio del carico di lavoro.

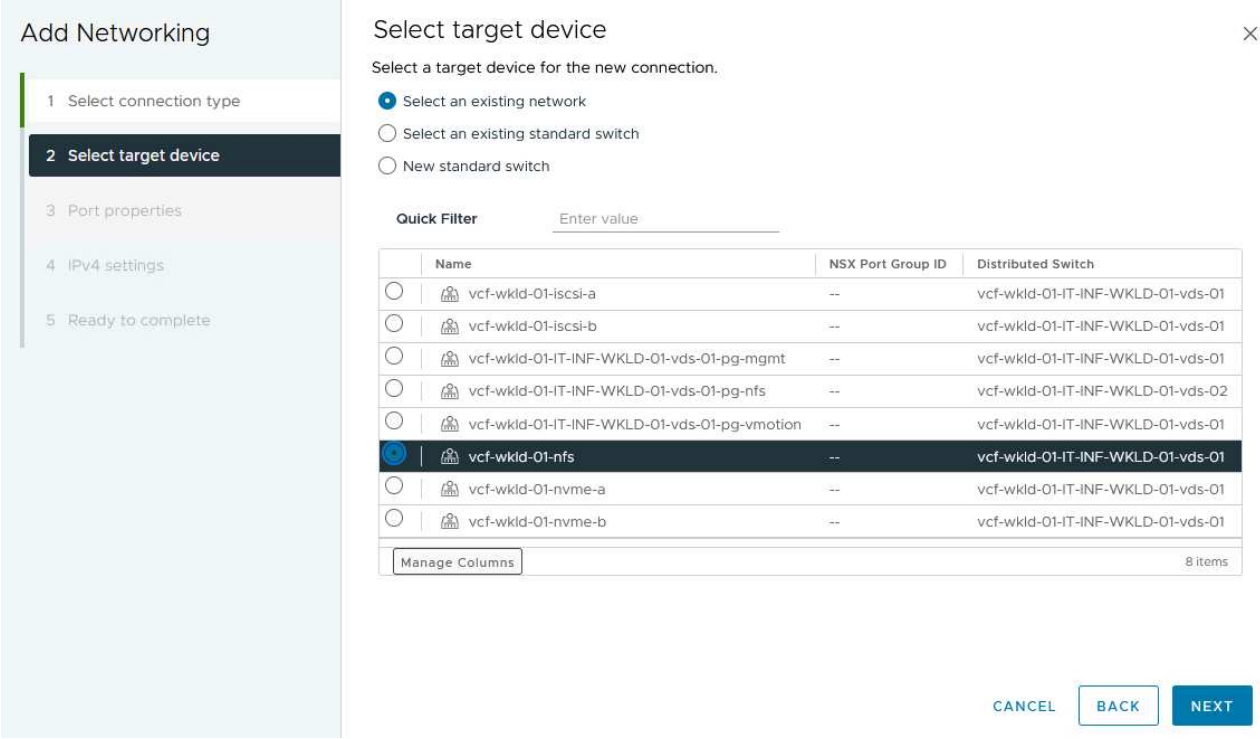
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configure** selezionare **VMkernel adapters** e fare clic su **Add Networking…** per iniziare.



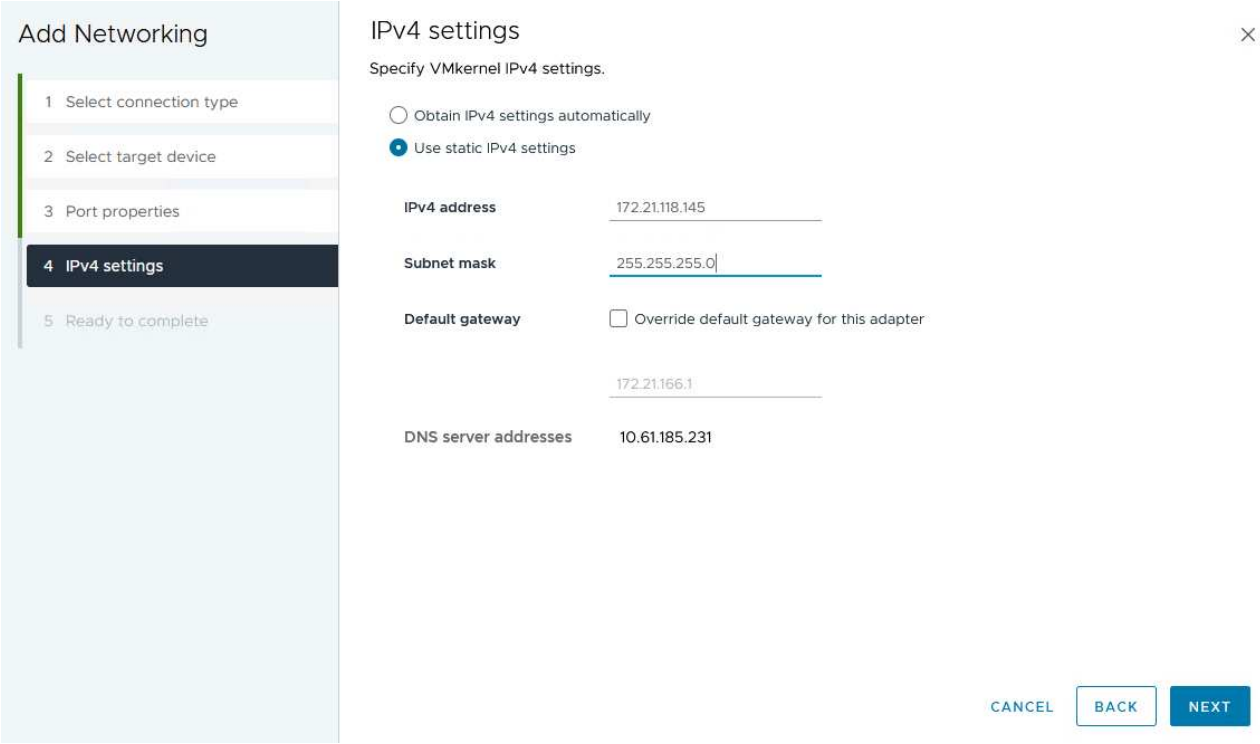
2. Nella finestra **Select Connection type** (Seleziona tipo di connessione), scegliere **VMkernel Network Adapter** (scheda di rete VMkernel) e fare clic su **Next** (Avanti) per continuare.



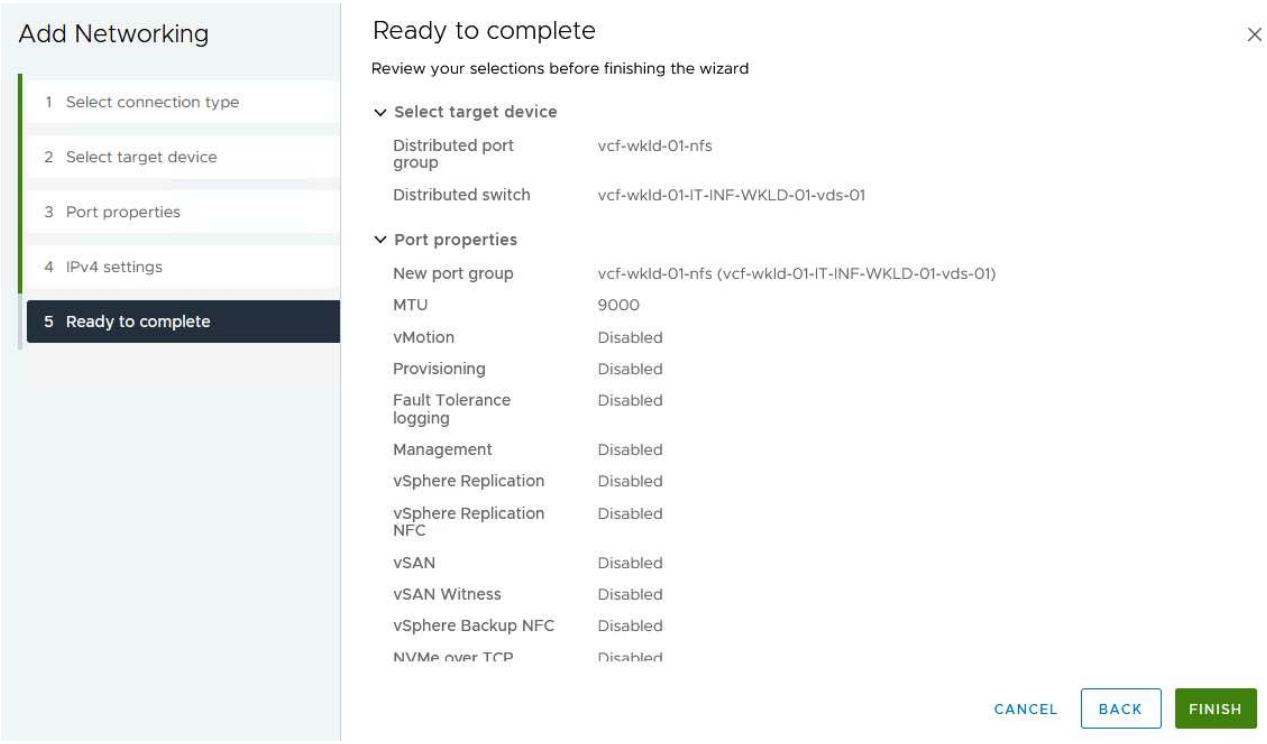
3. Nella pagina **Seleziona dispositivo di destinazione**, scegliere uno dei gruppi di porte distribuiti per NFS creati in precedenza.



4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite (nessun servizio abilitato) e fare clic su **Avanti** per continuare.
5. Nella pagina **IPv4 settings** compilare i campi **IP address**, **Subnet mask** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.



6. Rivedere le selezioni nella pagina **Pronto per il completamento** e fare clic su **fine** per creare l'adattatore VMkernel.



Implementazione e utilizzo degli strumenti di ONTAP per configurare lo storage

I seguenti passaggi vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere e prevedono la distribuzione di OTV, la creazione di un datastore vVol NFS e la migrazione delle VM di gestione al nuovo datastore.

Per i domini di carico di lavoro VI, OTV viene installato nel cluster di gestione VCF ma registrato con vCenter associato al dominio del carico di lavoro VI.

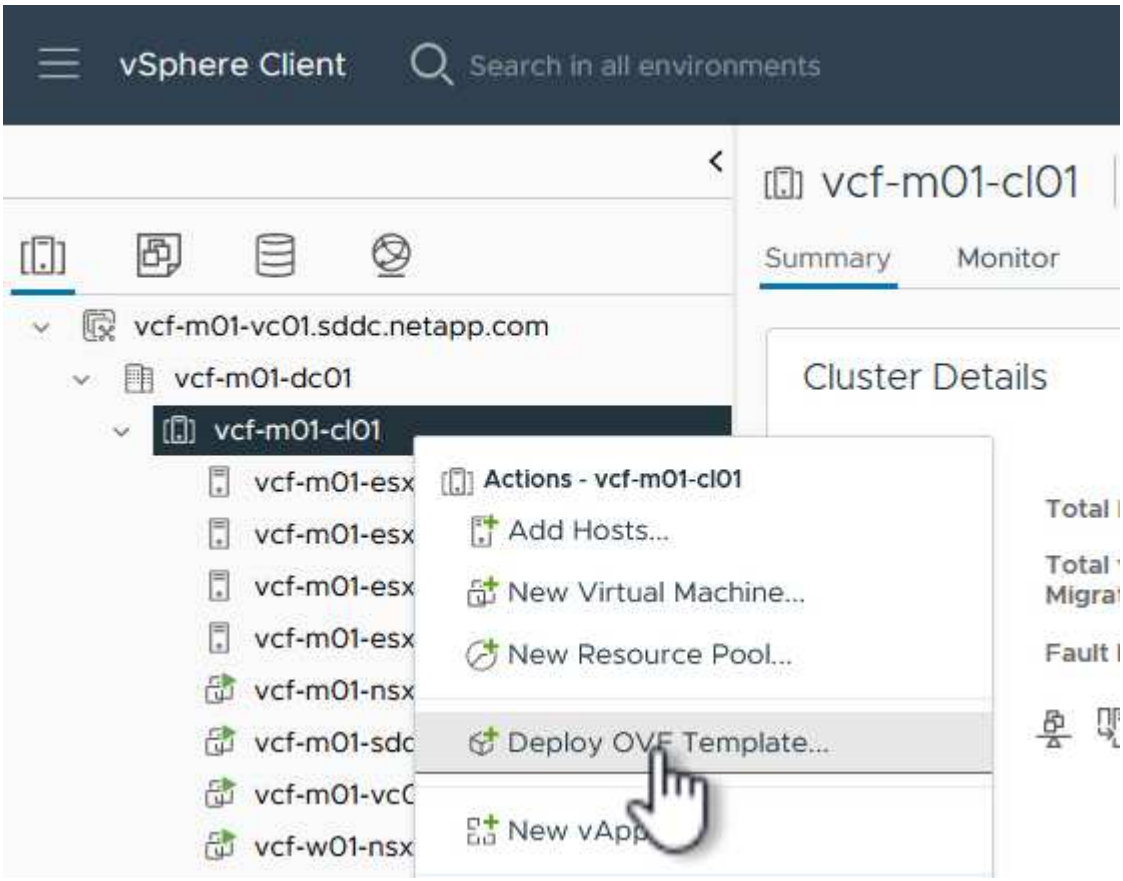
Per ulteriori informazioni sulla distribuzione e l'utilizzo degli strumenti ONTAP in un ambiente vCenter multiplo, fare riferimento a. "Requisiti per la registrazione degli strumenti ONTAP in più ambienti vCenter Server".

Implementa i tool ONTAP per VMware vSphere

I tool ONTAP per VMware vSphere (OTV) vengono implementati come appliance delle macchine virtuali e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP.

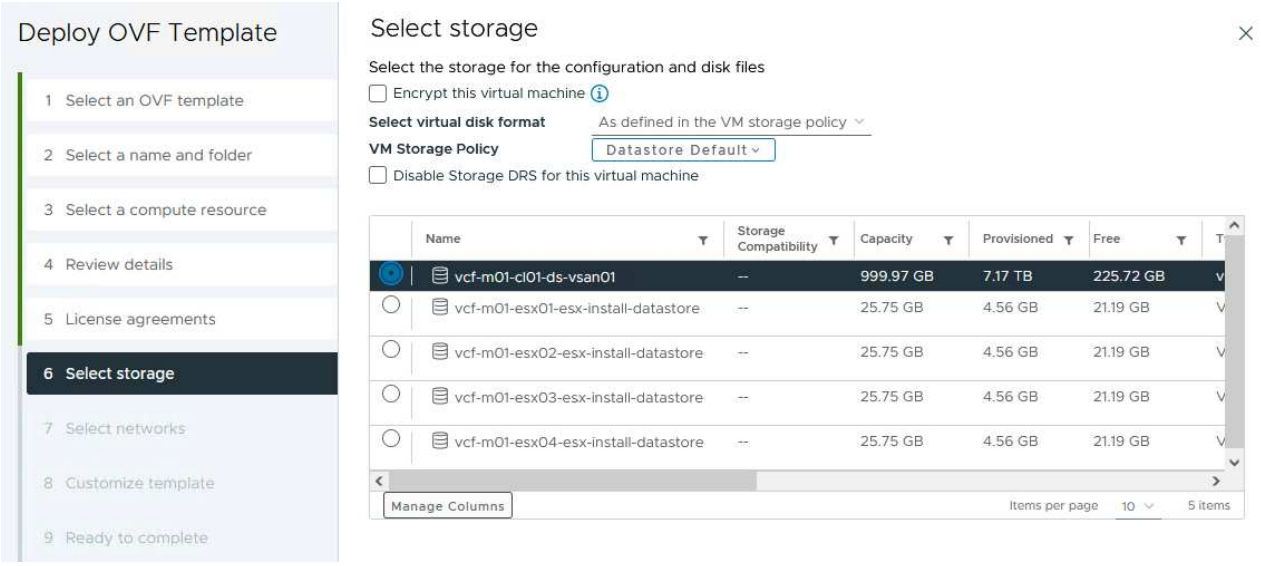
Completa quanto segue per implementare i tool ONTAP per VMware vSphere:

1. Ottenere l'immagine OVA degli strumenti ONTAP dal "Sito di supporto NetApp" e scaricarlo in una cartella locale.
2. Accedere all'appliance vCenter per il dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Deploy OVF Template…**

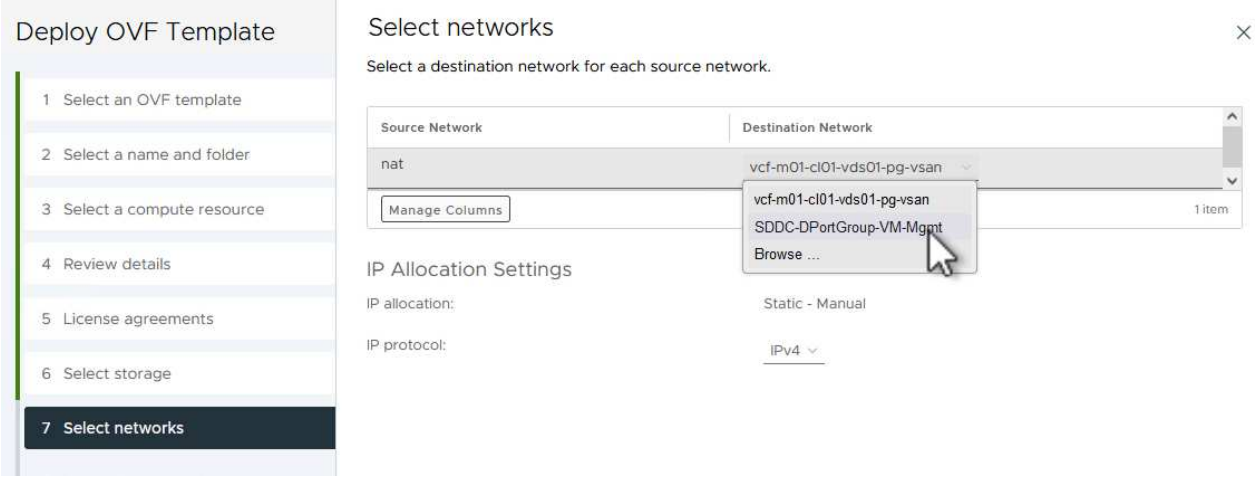


4. Nella procedura guidata **Deploy OVF Template** fare clic sul pulsante di opzione **file locale** e selezionare il file OVA di ONTAP Tools scaricato nel passaggio precedente.

5. Per i passaggi da 2 a 5 della procedura guidata, selezionare un nome e una cartella per la macchina virtuale, selezionare la risorsa di elaborazione, esaminare i dettagli e accettare il contratto di licenza.
6. Per la posizione di archiviazione dei file di configurazione e del disco, selezionare il datastore vSAN del cluster del dominio di gestione VCF.

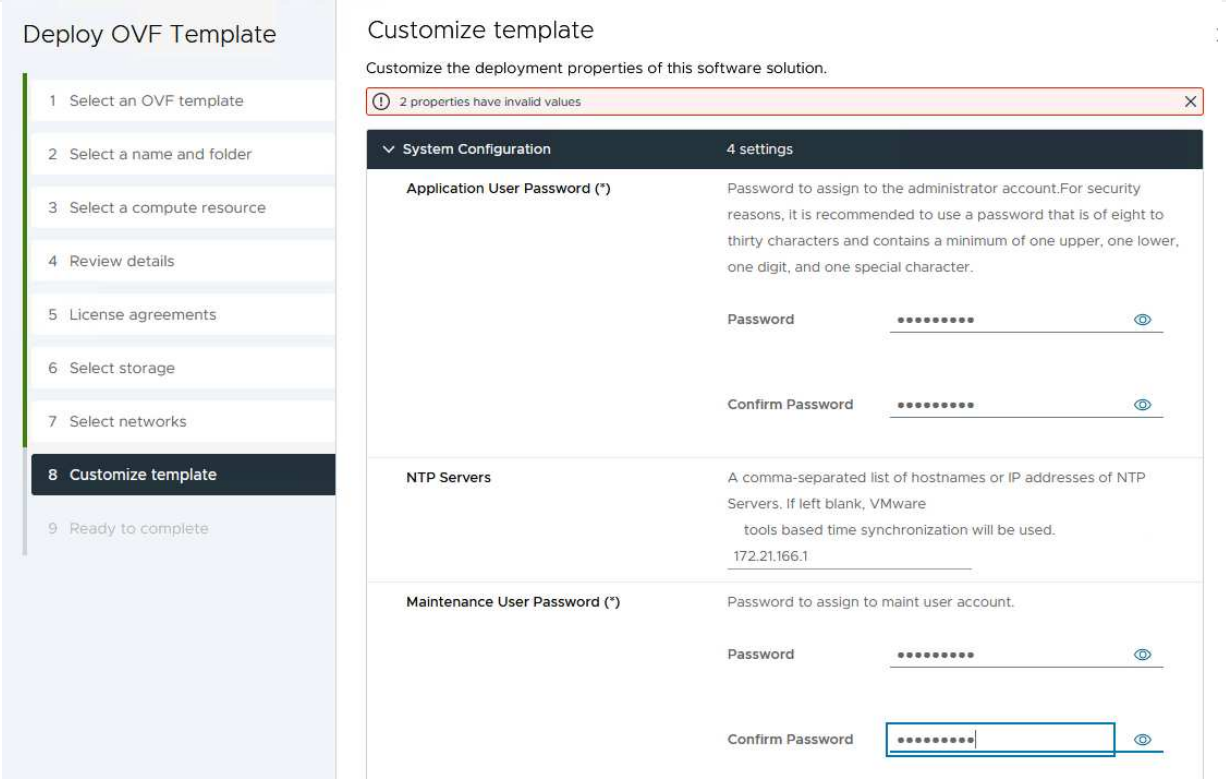


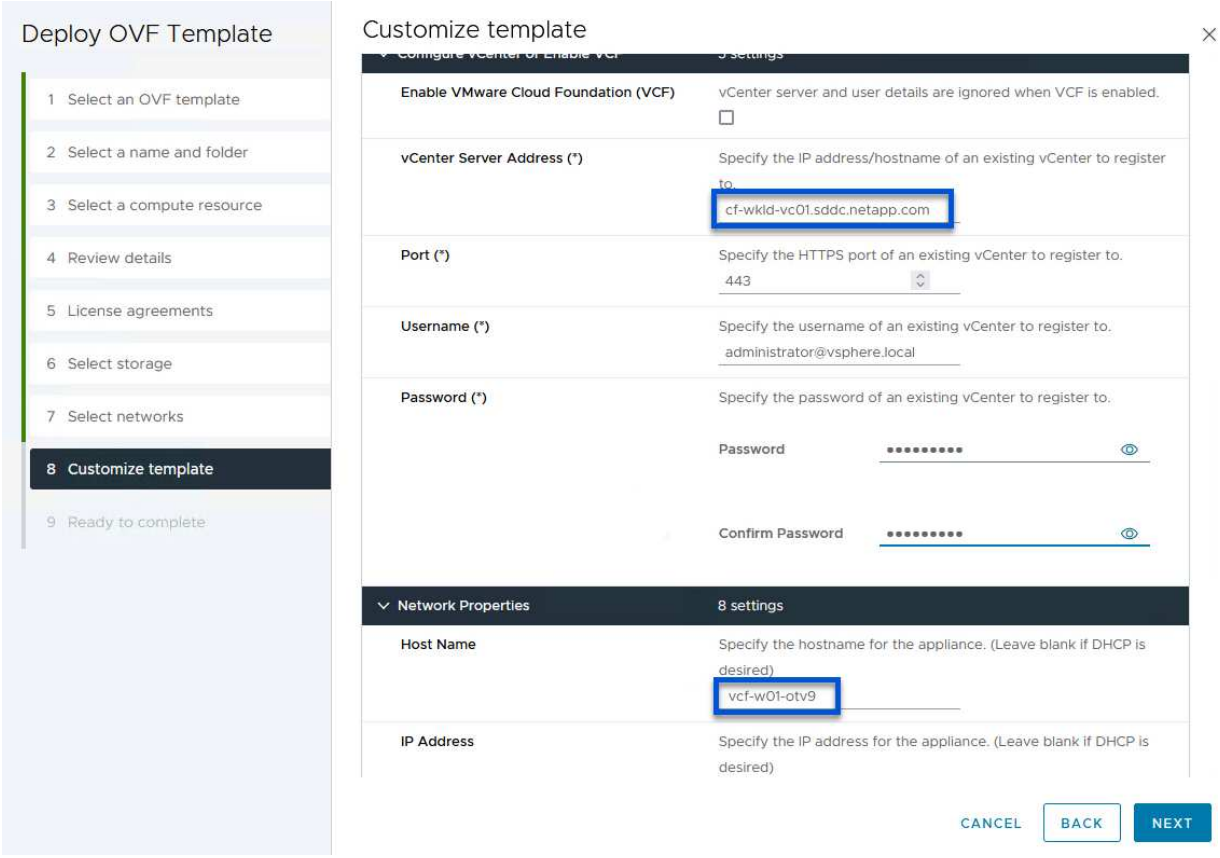
7. Nella pagina Seleziona rete, selezionare la rete utilizzata per la gestione del traffico.



8. Nella pagina Personalizza modello compilare tutte le informazioni richieste:
   - Password da utilizzare per l'accesso amministrativo a OTV.
   - Indirizzo IP del server NTP.
   - Password dell'account di manutenzione OTV.
   - Password DB Derby OTV.
   - Non selezionare la casella di controllo **Abilita VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire lo storage supplementare.
   - FQDN o indirizzo IP dell'appliance vCenter per **VI workload Domain**
   - Credenziali per l'appliance vCenter del **VI workload Domain**
   - Specificare i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.

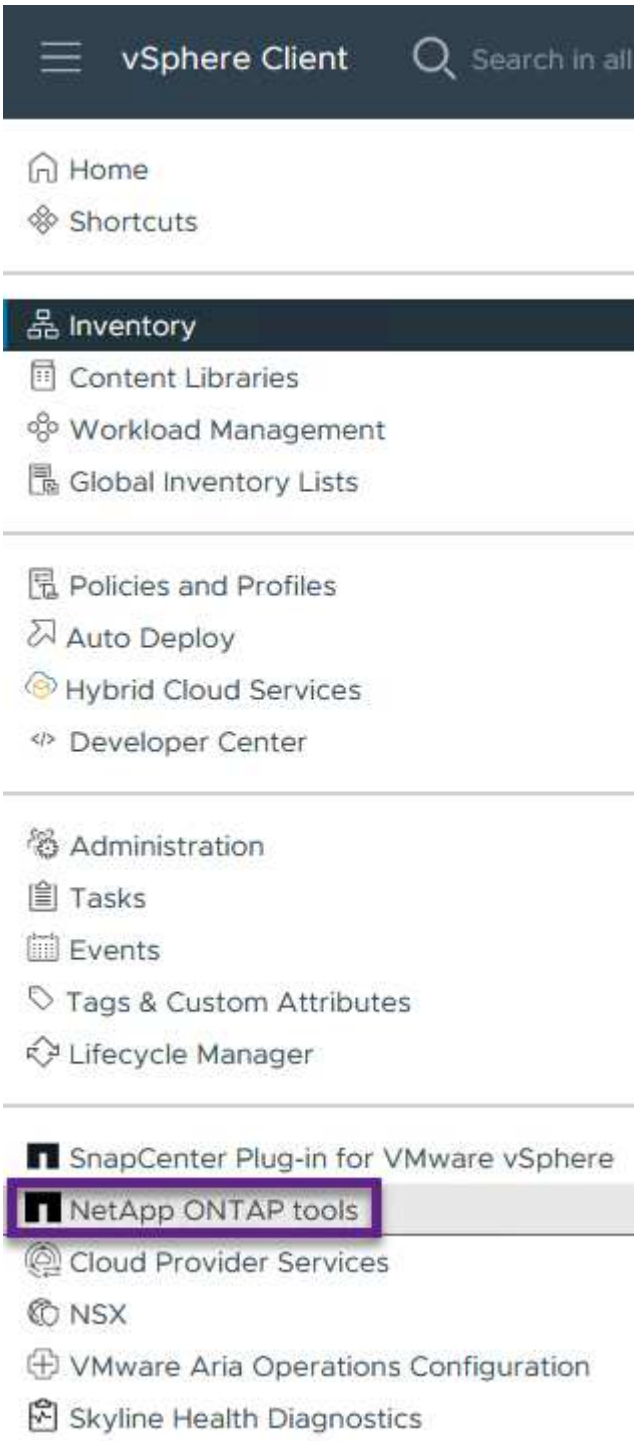




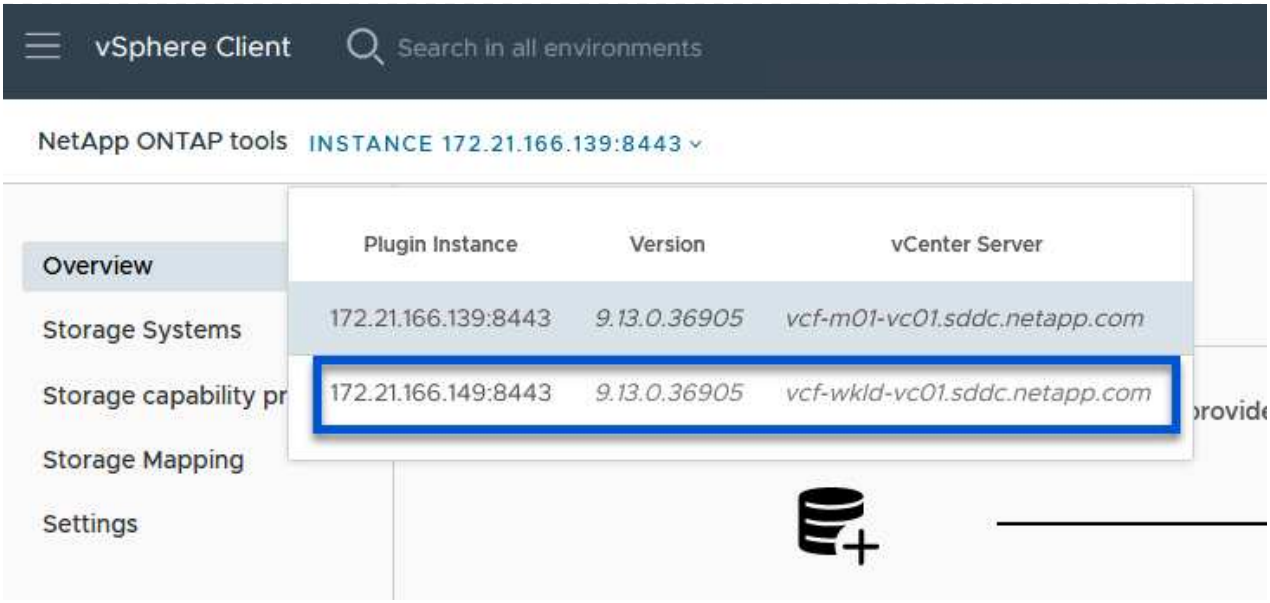
9. Leggere tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare a implementare l'apparecchio OTV.

Aggiunta di un sistema di storage ai tool ONTAP.

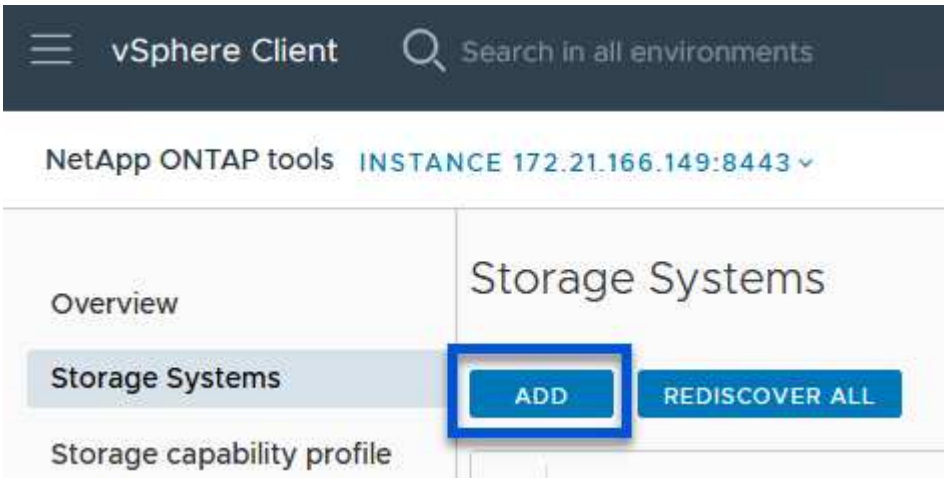
1. Accedere agli strumenti NetApp ONTAP selezionandoli dal menu principale del client vSphere.



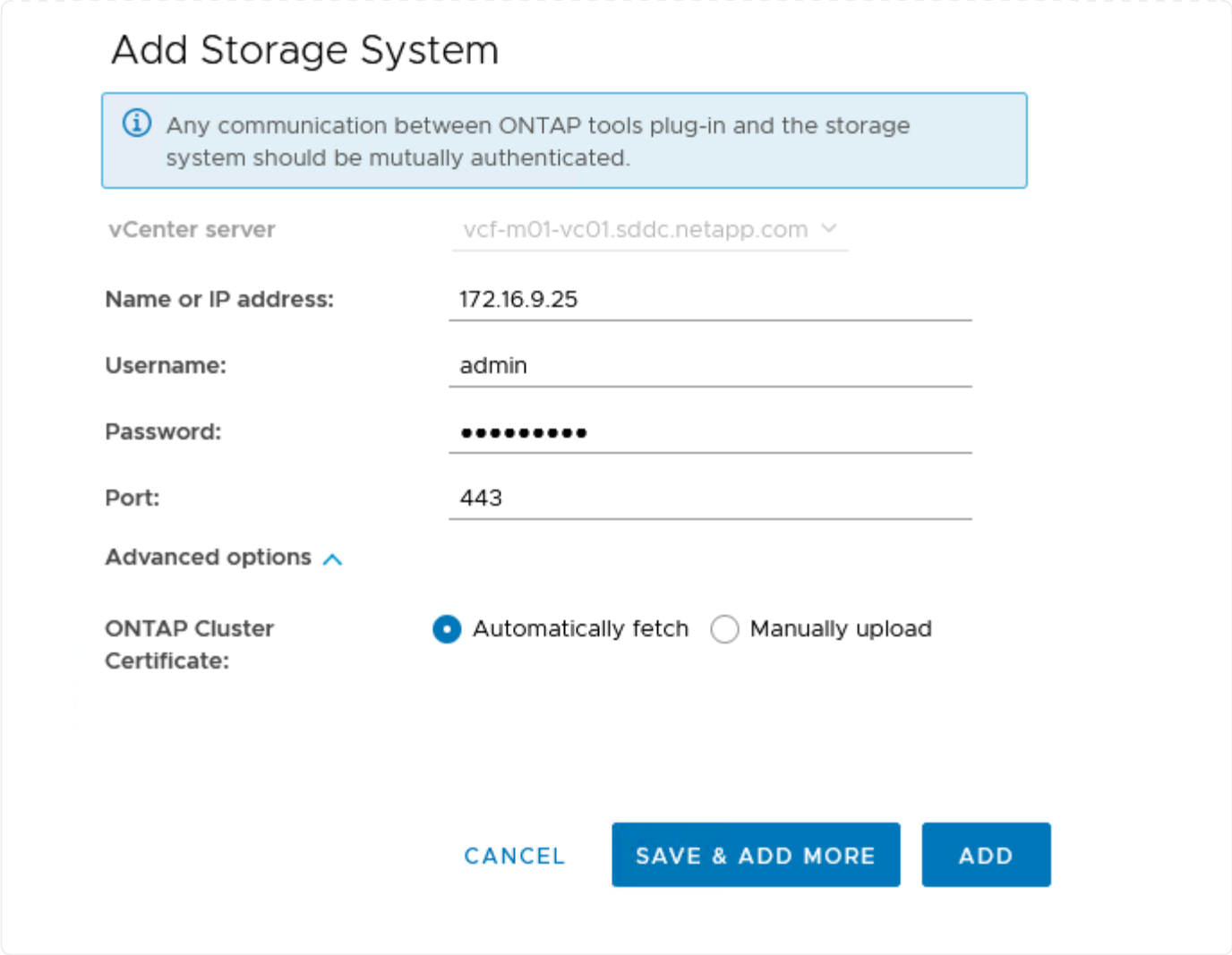
2. Dal menu a discesa **INSTANCE** nell'interfaccia dello strumento ONTAP, selezionare l'istanza OTV associata al dominio del carico di lavoro da gestire.



3. In Strumenti di ONTAP, selezionare **sistemi di archiviazione** dal menu a sinistra, quindi premere **Aggiungi**.



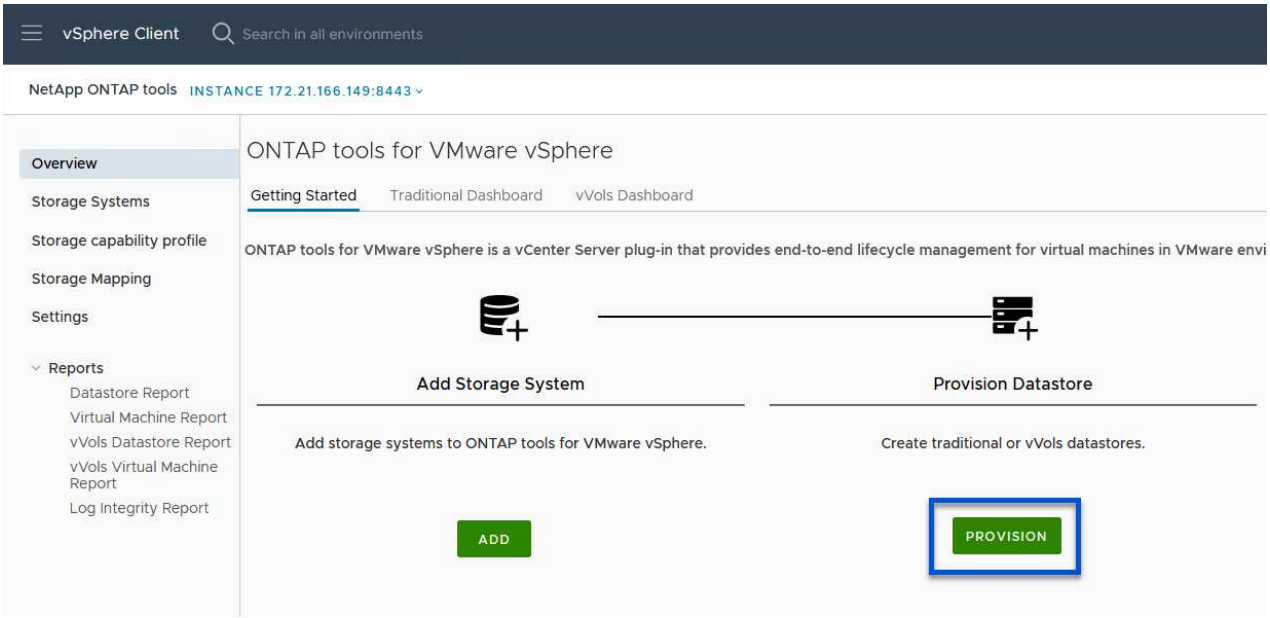
4. Immettere l'indirizzo IP, le credenziali del sistema di archiviazione e il numero di porta. Fare clic su **Aggiungi** per avviare il processo di ricerca.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Creare un datastore NFS in ONTAP Tools

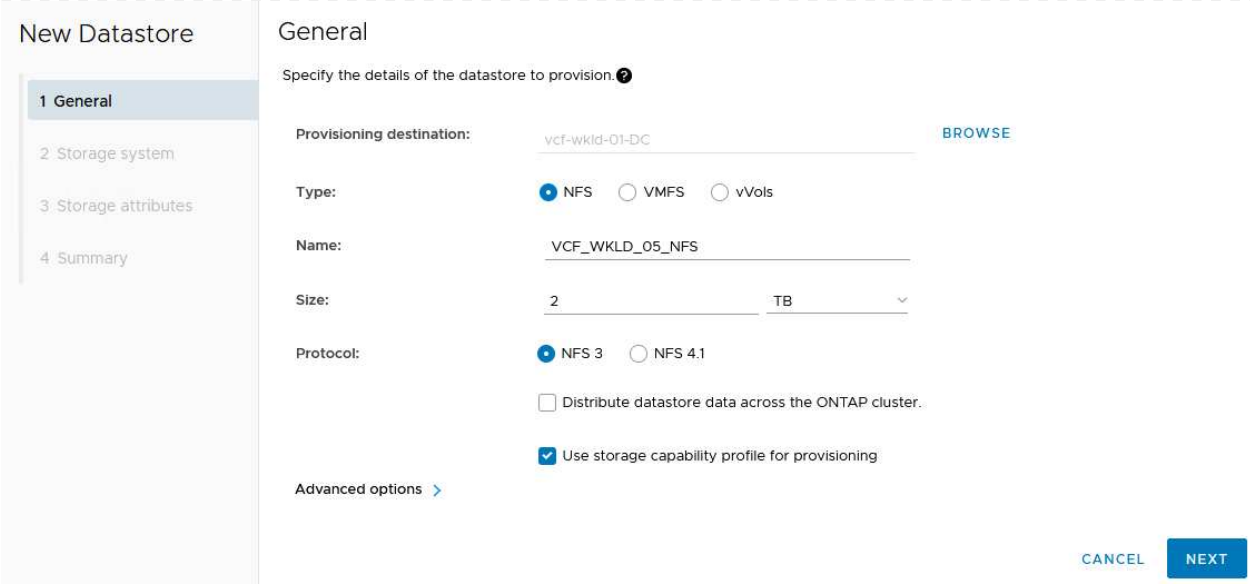
Completa i seguenti passaggi per implementare un datastore ONTAP in esecuzione su NFS usando i tool di ONTAP.

1. In Strumenti di ONTAP selezionare **Panoramica** e dalla scheda **Guida introduttiva** fare clic su **Provision** per avviare la procedura guidata.

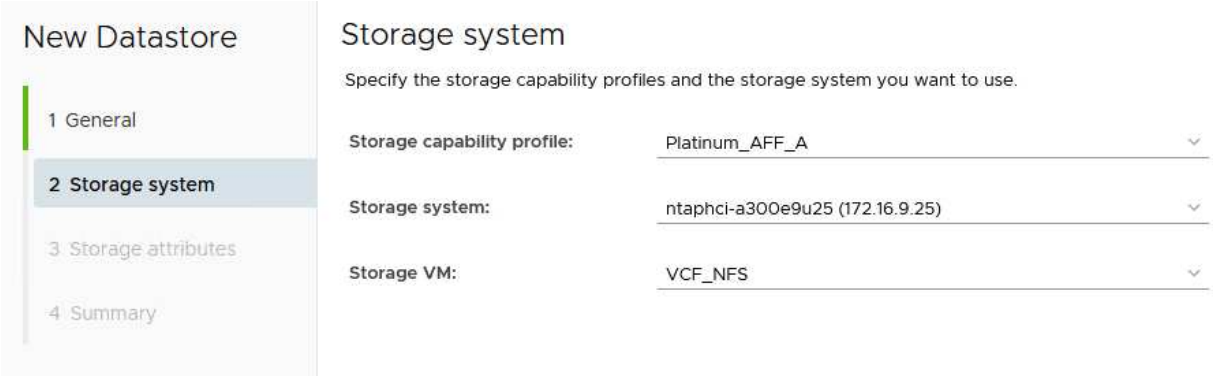


2. Nella pagina **Generale** della procedura guidata nuovo datastore selezionare il data center vSphere o la destinazione del cluster. Selezionare **NFS** come tipo di datastore, specificare un nome per il datastore e selezionare il protocollo. Scegliere se utilizzare i volumi FlexGroup e se utilizzare un file con funzionalità di storage per il provisioning. Fare clic su **Avanti** per continuare.

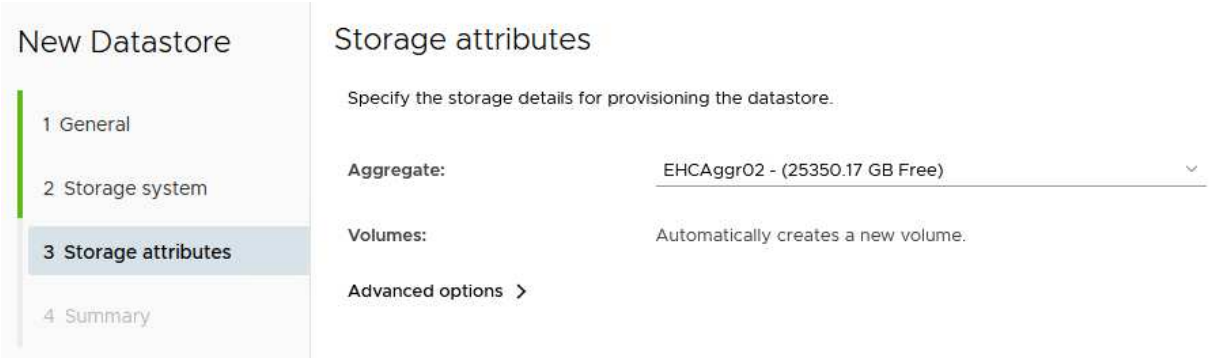
   Nota: Selezionando **distribuire i dati del datastore nel cluster** si crea il volume sottostante come volume FlexGroup che preclude l'utilizzo dei profili di funzionalità dello storage. Fare riferimento a. "Configurazioni supportate e non supportate per i volumi FlexGroup" Per ulteriori informazioni sull'utilizzo di FlexGroup Volumes.



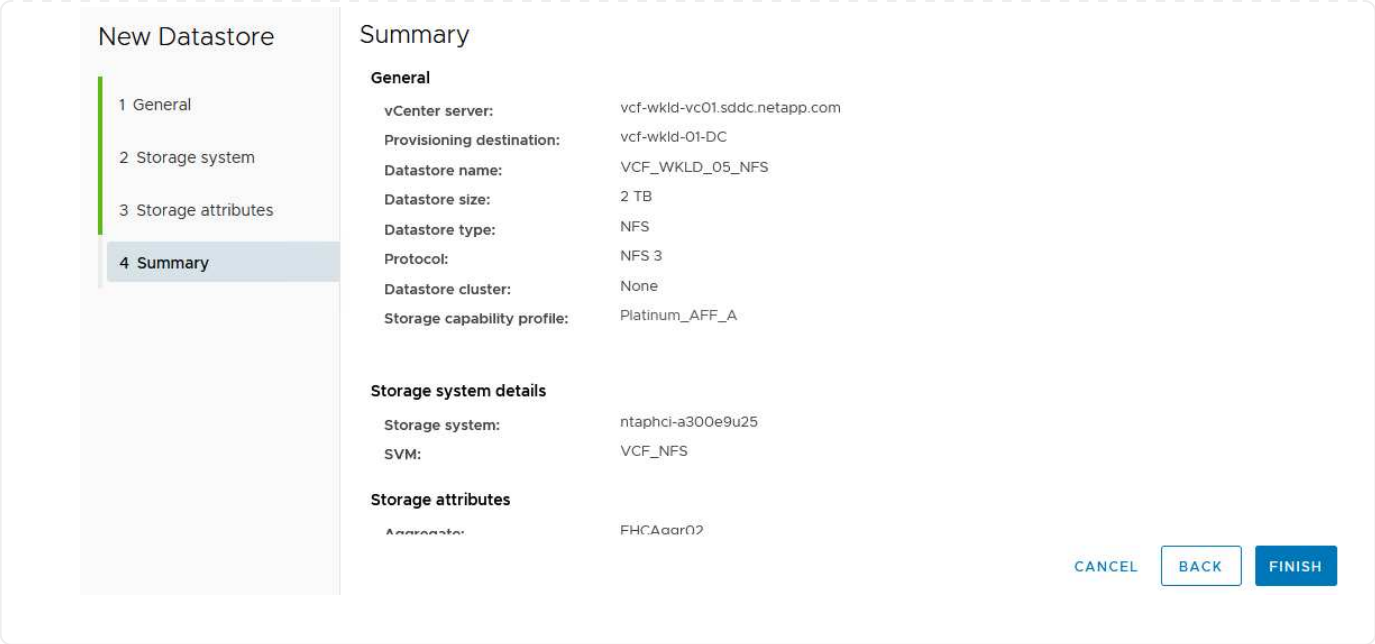
3. Nella pagina **sistema storage**, seleziona un profilo di funzionalità storage, il sistema storage e la SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **attributi archiviazione**, selezionare l'aggregato da utilizzare, quindi fare clic su **Avanti** per continuare.



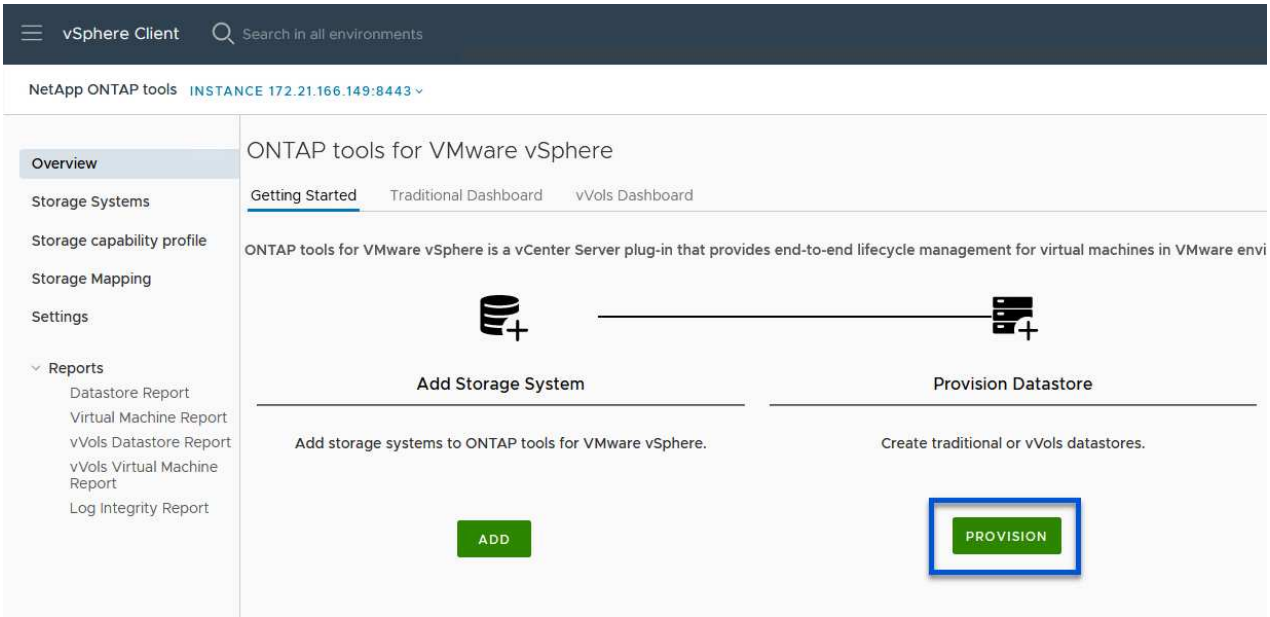
5. Infine, rivedere il **Summary** e fare clic su Finish (fine) per iniziare a creare il datastore NFS.


New Datastore
1 General
2 Storage system
3 Storage attributes
4 Summary
Summary
General
vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_05_NFS
Datastore size: 2 TB
Datastore type: NFS
Protocol: NFS 3
Datastore cluster: None
Storage capability profile: Platinum_AFF_A
Storage system details
Storage system: ntaphci-a300e9u25
SVM: VCF_NFS
Storage attributes
CANCEL
BACK
FINISH

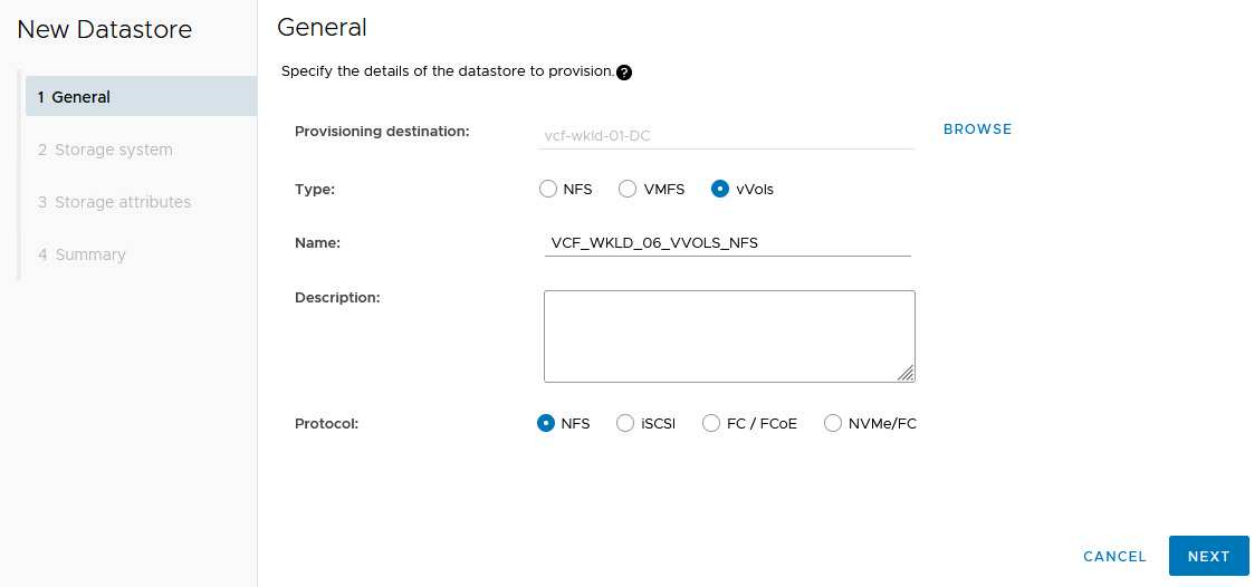
Creare un datastore vVol in ONTAP Tools

Per creare un datastore vVol in Strumenti di ONTAP, attenersi alla seguente procedura:

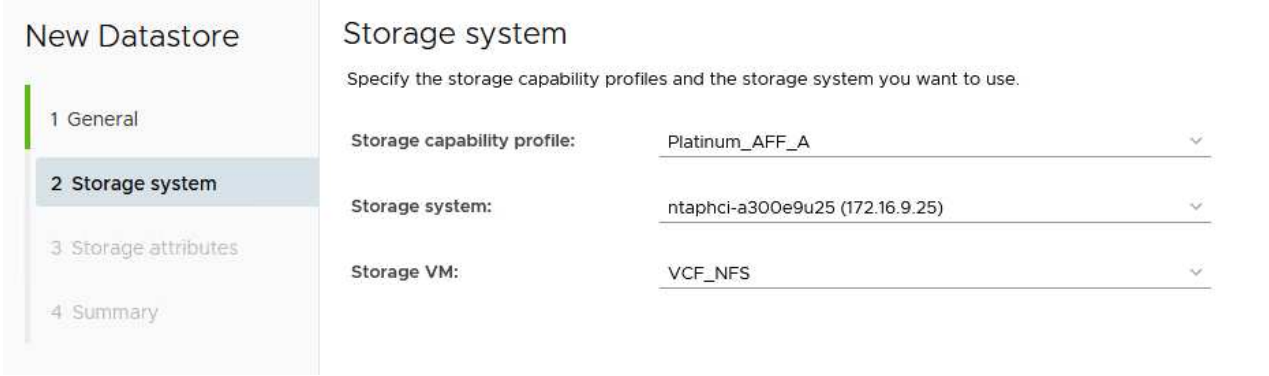
1. In Strumenti di ONTAP selezionare **Panoramica** e dalla scheda **Guida introduttiva** fare clic su **Provision** per avviare la procedura guidata.



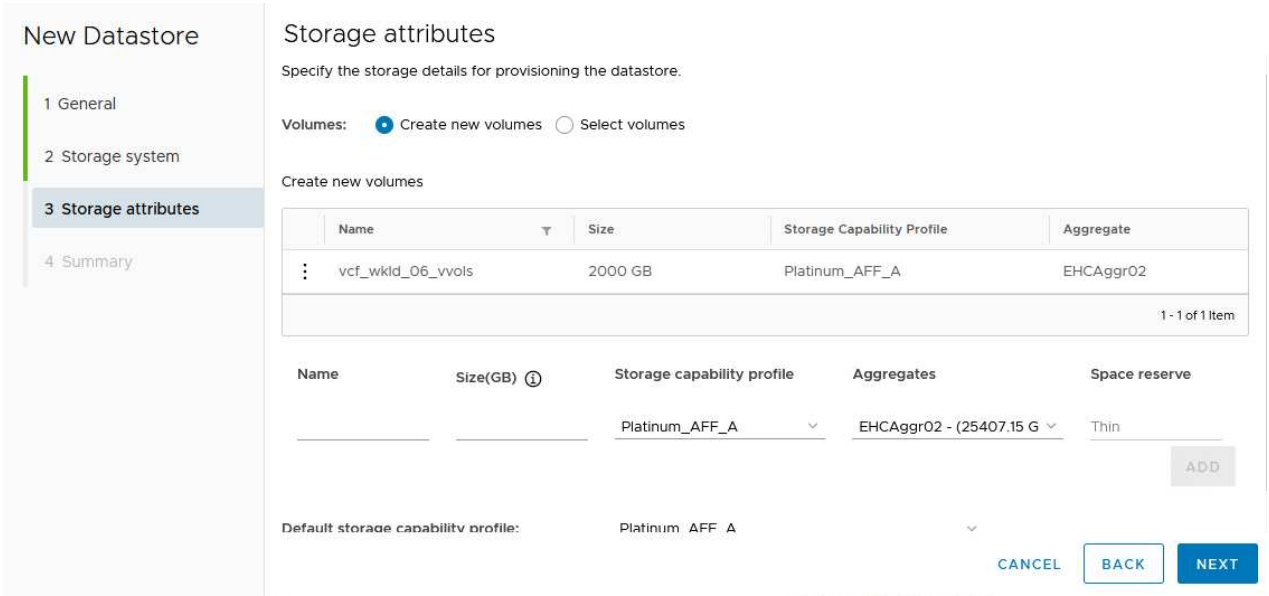
2. Nella pagina **Generale** della procedura guidata nuovo datastore selezionare il data center vSphere o la destinazione del cluster. Selezionare **vVol** come tipo di archivio dati, inserire un nome per il datastore e selezionare **NFS** come protocollo. Fare clic su **Avanti** per continuare.



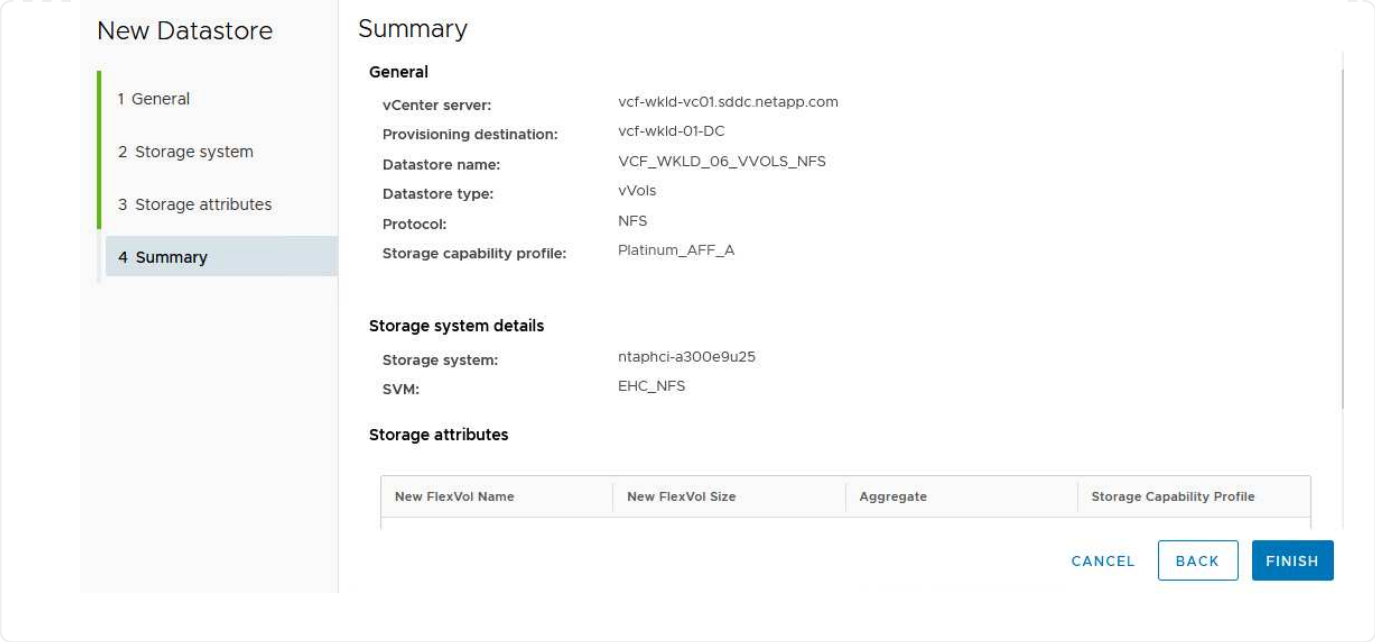
3. Nella pagina **sistema storage**, seleziona un profilo di funzionalità storage, il sistema storage e la SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **attributi archiviazione**, selezionare per creare un nuovo volume per l'archivio dati e specificare gli attributi di archiviazione del volume da creare. Fare clic su **Aggiungi** per creare il volume, quindi su **Avanti** per continuare.



5. Infine, esaminare il **Riepilogo** e fare clic su **fine** per avviare il processo di creazione del datastore vVol.



Ulteriori informazioni

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la "Documentazione di ONTAP 9" centro.

Per informazioni sulla configurazione di VCF, fare riferimento a. "Documentazione di VMware Cloud Foundation".

Migrazione delle VM

Migrazione delle macchine virtuali nei datastore ONTAP

Autore: Suresh Thoppay

VMware vSphere di Broadcom supporta datastore VMFS, NFS e vVol per l'hosting di macchine virtuali. I clienti possono creare questi datastore con infrastrutture iperconvergenti o sistemi storage centralizzati e condivisi. Spesso i clienti vedono il valore dell'hosting sui sistemi storage basati su ONTAP per fornire snapshot efficienti in termini di spazio e cloni delle macchine virtuali, flessibilità nella scelta di vari modelli di implementazione nei data center e nei cloud, efficienza delle operazioni con strumenti di monitoraggio e avviso, sicurezza, governance e strumenti di conformità opzionali per ispezionare i dati delle macchine virtuali, ecc,.

Le macchine virtuali ospitate nei datastore ONTAP possono essere protette utilizzando il plug-in SnapCenter per VMware vSphere (SCV). SCV crea istantanee basate sullo storage e replica nel sistema di storage ONTAP remoto. È possibile eseguire il ripristino da sistemi storage primari o secondari.

I clienti hanno la flessibilità di scegliere Cloud Insights o aria Operations o una combinazione di entrambi o altri strumenti di terze parti che utilizzano l'api ONTAP per la risoluzione dei problemi, il monitoraggio delle prestazioni, la creazione di report e le funzioni di notifica degli avvisi.

I clienti possono effettuare facilmente il provisioning del datastore utilizzando il plug-in vCenter di ONTAP Tools

o la sua API; inoltre, le macchine virtuali possono essere migrate nei datastore ONTAP anche mentre sono attive.

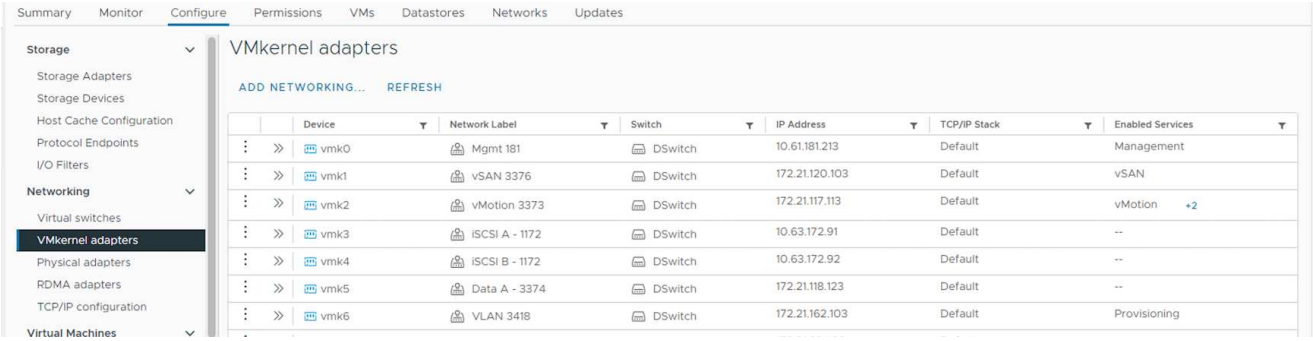
> Alcune macchine virtuali implementate con un tool di gestione esterno come aria Automation, Tanzu (o altri modelli Kubernetes) dipendono di solito dalla policy di storage delle macchine virtuali. Se la migrazione tra datastore all'interno della stessa policy storage delle macchine virtuali, dovrebbe avere un impatto minore per le applicazioni. Chiedere ai proprietari delle applicazioni di eseguire la migrazione corretta di tali macchine virtuali nel nuovo datastore. Introduzione di vSphere 8 "Notifica VMotion" Per preparare l'applicazione per vMotion.

Requisiti di rete

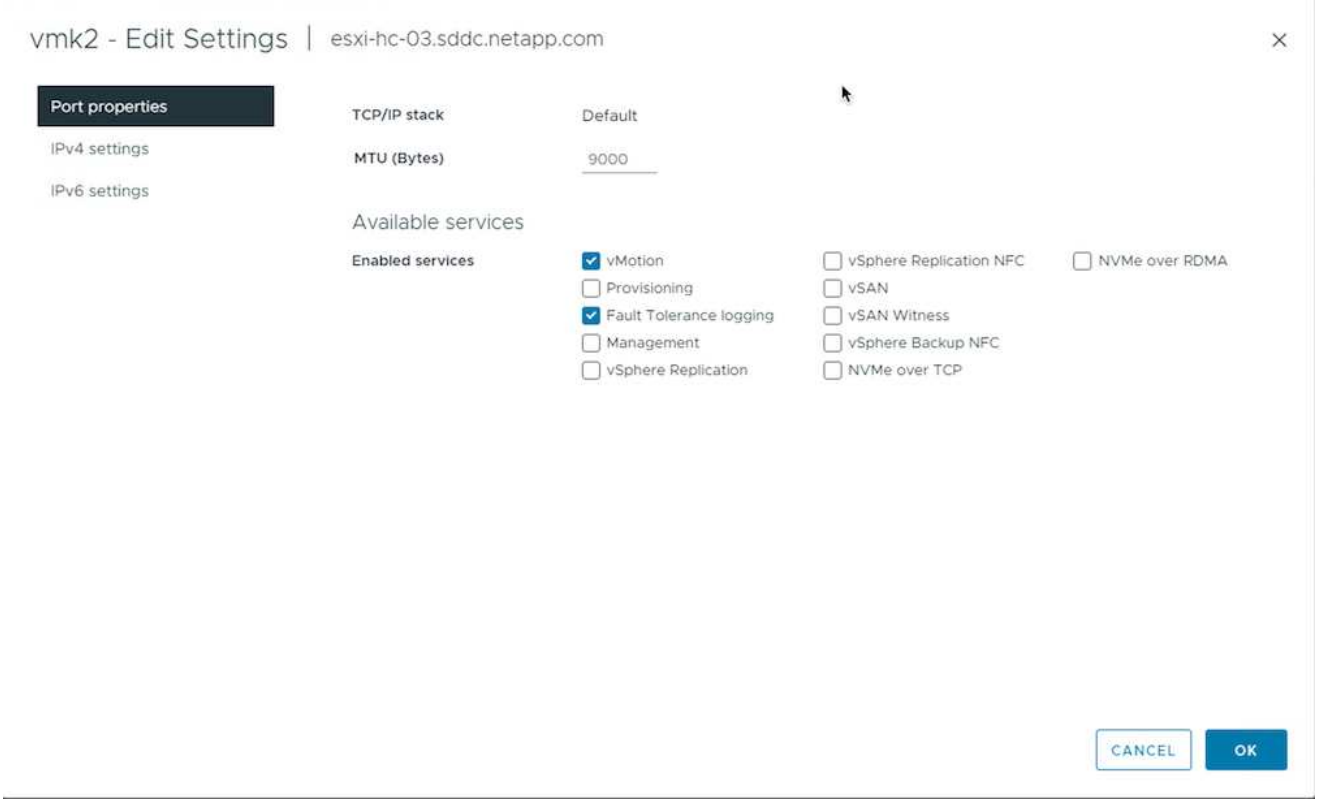
Migrazione delle macchine virtuali con vMotion

Si presuppone che nel datastore ONTAP sia già in uso una rete di storage doppia per garantire connettività, tolleranza agli errori e incremento delle performance.

La migrazione delle VM negli host vSphere viene gestita anche dall'interfaccia VMkernel dell'host vSphere. Per la migrazione a caldo (con VM attivate), viene utilizzata l'interfaccia VMkernel con il servizio abilitato vMotion e per la migrazione a freddo (con VM disattivate), l'interfaccia VMkernel con il servizio di provisioning attivato viene utilizzata per spostare i dati. Se non è stata trovata un'interfaccia valida, verrà utilizzata l'interfaccia di gestione per spostare i dati, cosa che potrebbe non essere desiderabile per alcuni casi di utilizzo.



Quando si modifica l'interfaccia VMkernel, di seguito è riportata l'opzione che consente di abilitare i servizi richiesti.



Assicurarsi che siano disponibili almeno due schede nic uplink attive ad alta velocità per il gruppo di porte utilizzato dalle interfacce vMotion e Provisioning VMkernel.

Scenari di migrazione delle VM

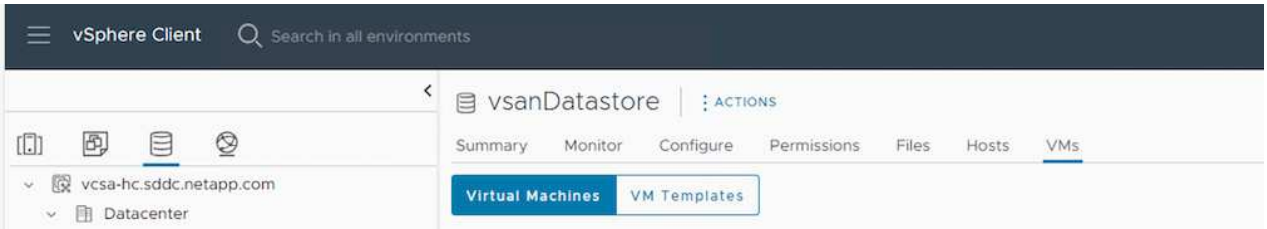
VMotion viene spesso utilizzato per eseguire la migrazione delle macchine virtuali indipendentemente dallo stato di alimentazione. Di seguito sono riportate ulteriori considerazioni e procedure di migrazione per scenari specifici.

> Capire "Condizioni VM e limitazione di vSphere vMotion" Prima di procedere con le opzioni di migrazione delle macchine virtuali.

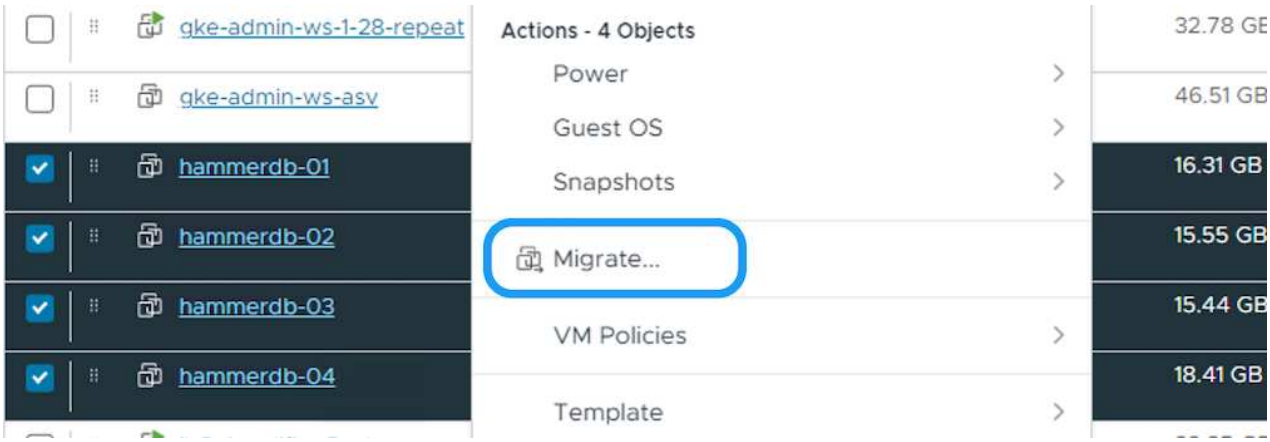
Migrazione di VM da datastore vSphere specifico

Seguire la procedura riportata di seguito per eseguire la migrazione delle macchine virtuali al nuovo datastore utilizzando l'interfaccia utente.

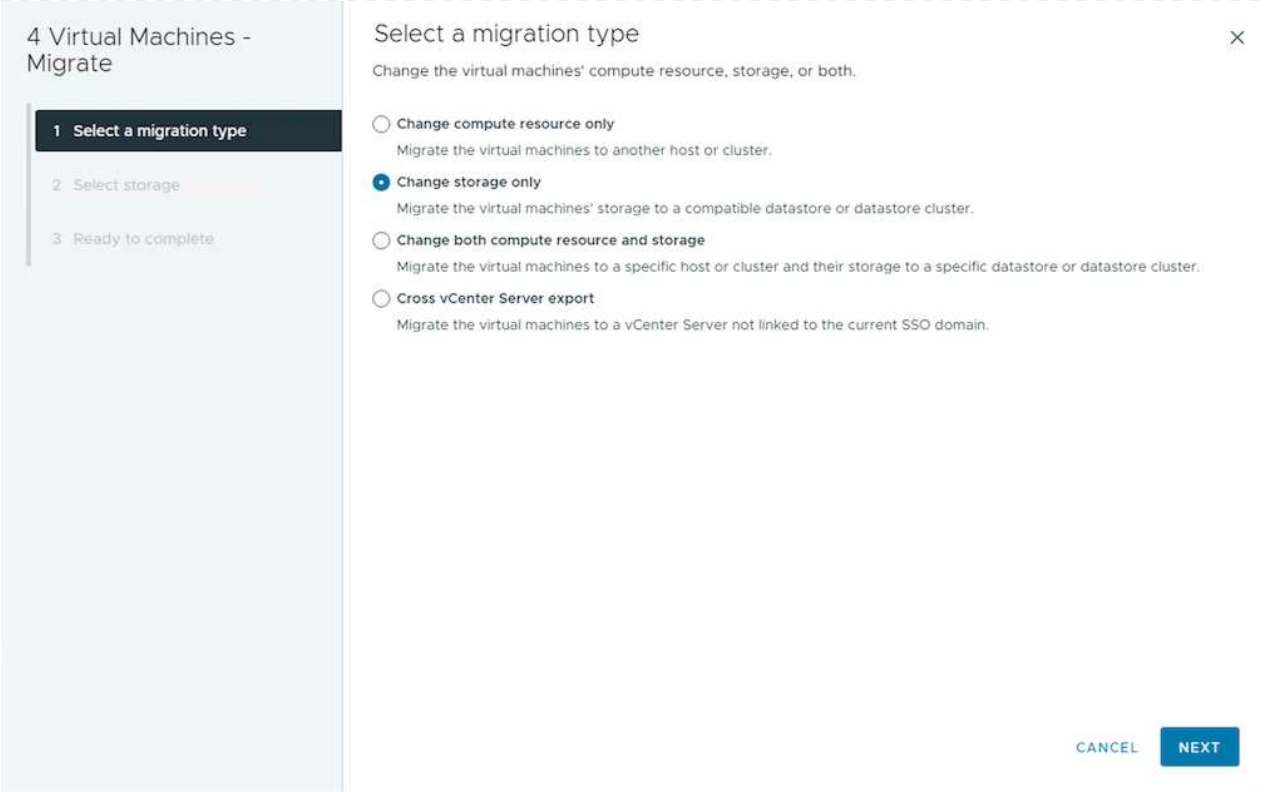
1. Con vSphere Web Client, selezionare il datastore dall'inventario dello storage e fare clic sulla scheda VM.



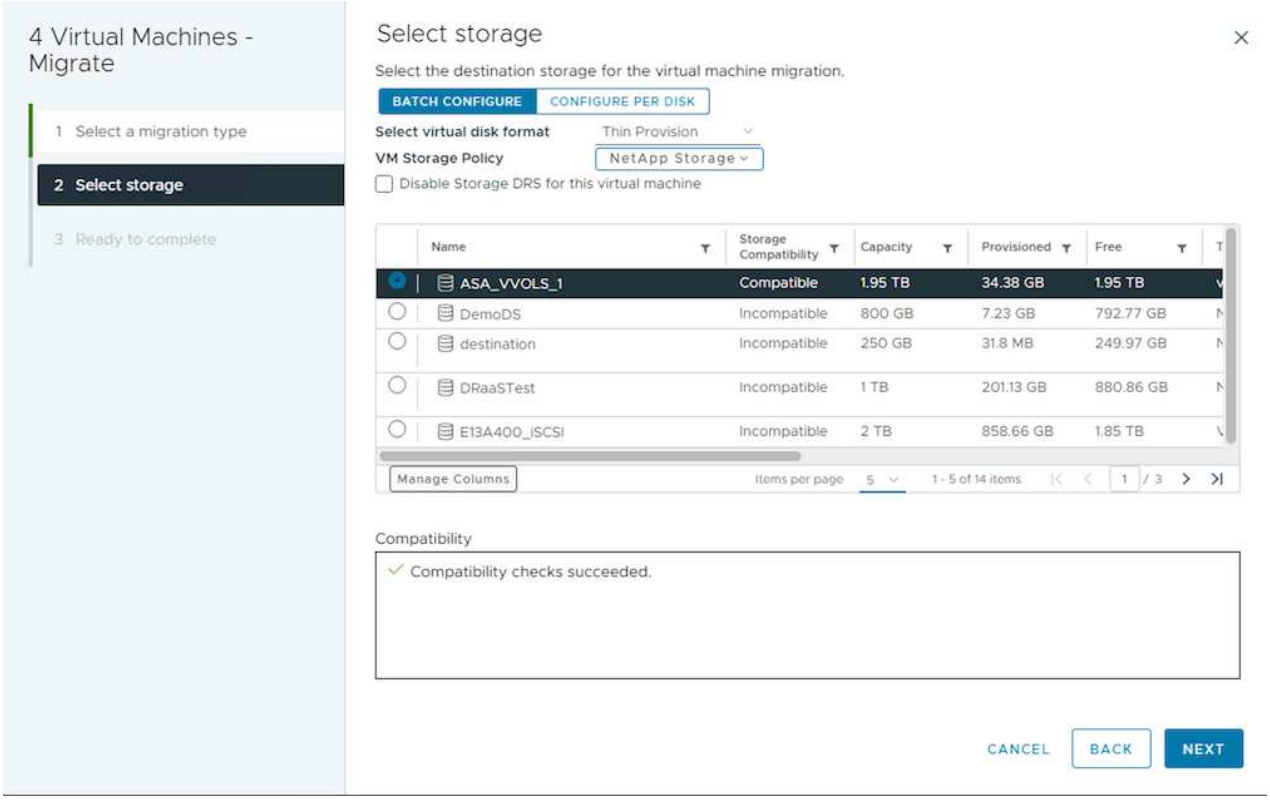
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



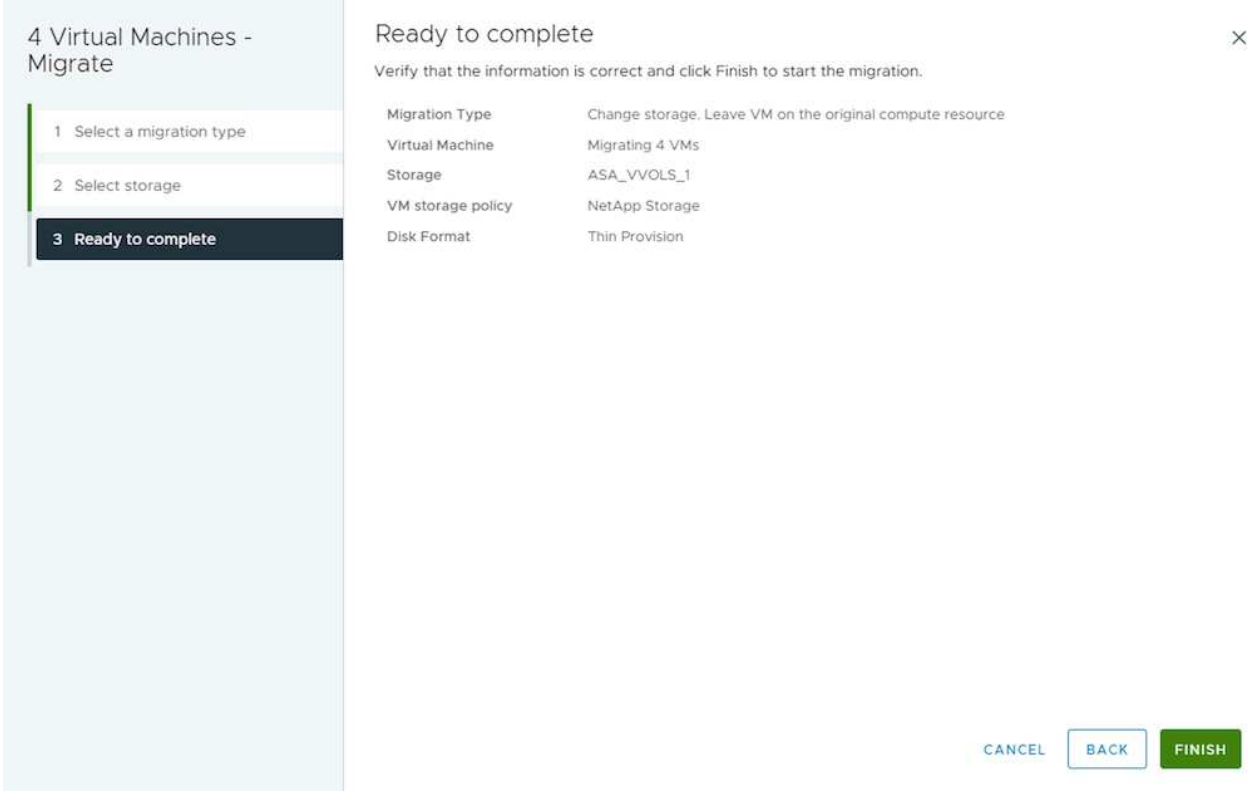
3. Scegliere l'opzione per modificare solo l'archiviazione, quindi fare clic su Avanti



4. Seleziona la policy storage della macchina virtuale desiderata e scegli l'archivio dati compatibile. Fare clic su Avanti.



5. Rivedere e fare clic su fine.



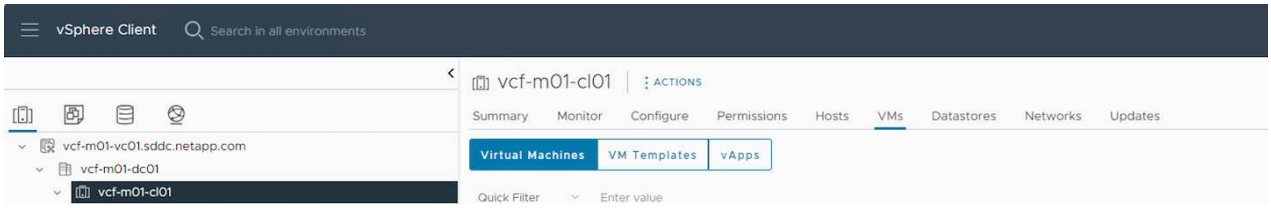
Per migrare le macchine virtuali utilizzando PowerCLI, ecco lo script di esempio.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

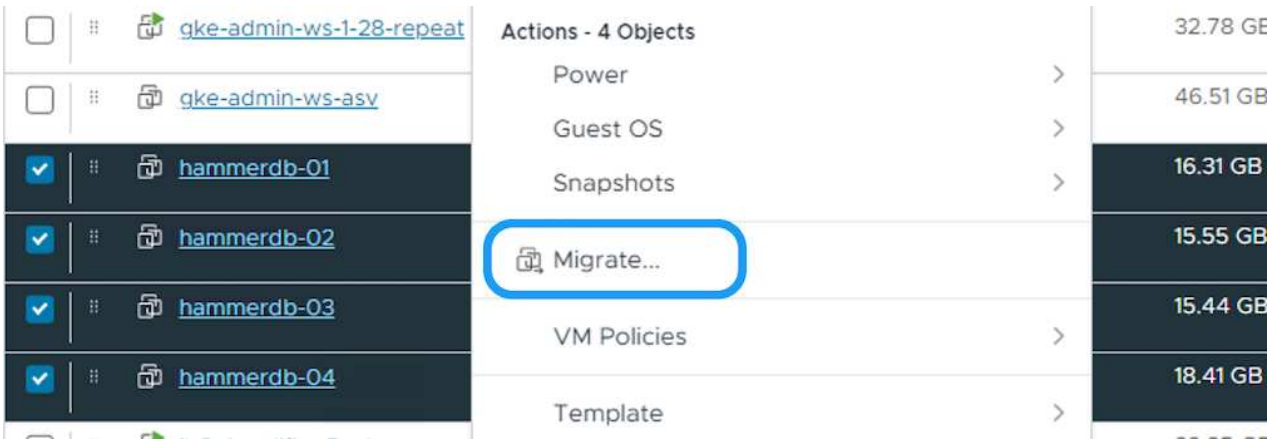
Migrazione di macchine virtuali nello stesso cluster vSphere

Seguire la procedura riportata di seguito per eseguire la migrazione delle macchine virtuali al nuovo datastore utilizzando l'interfaccia utente.

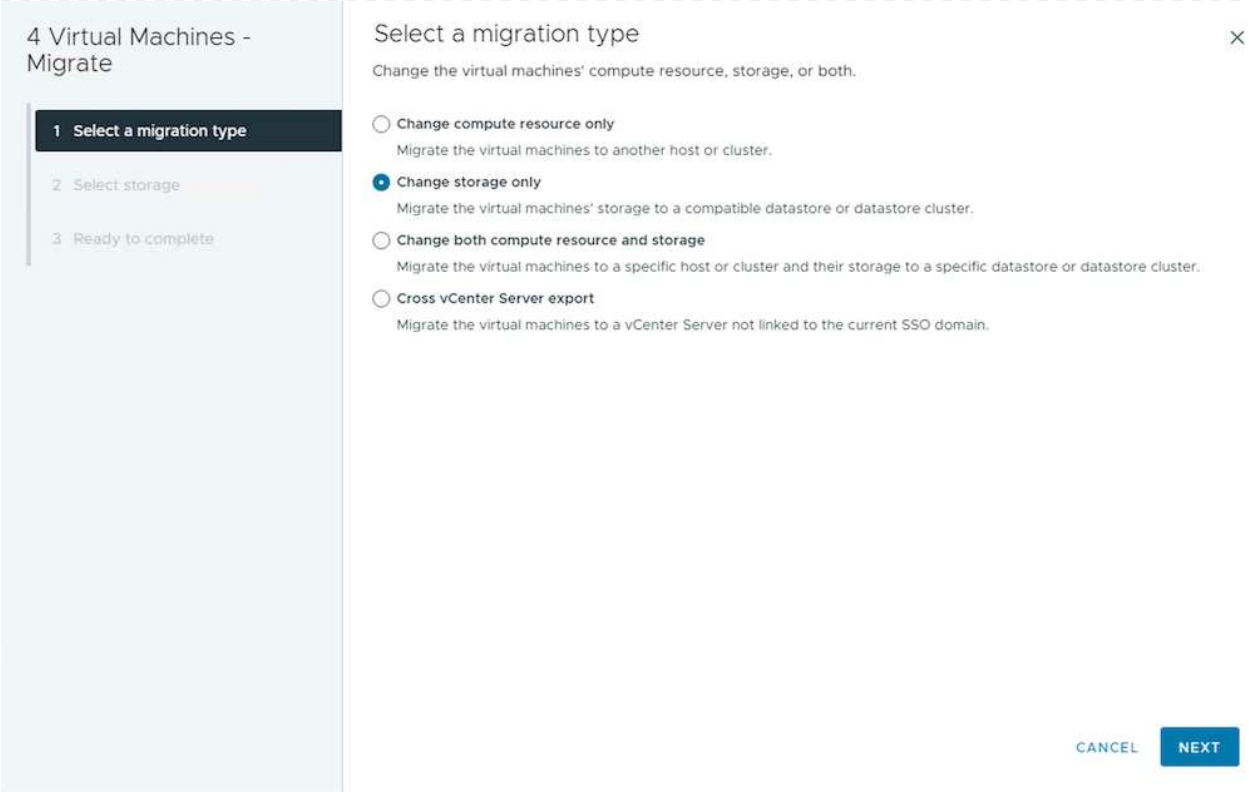
1. Con vSphere Web Client, selezionare il cluster dall'inventario host e cluster e fare clic sulla scheda VM.



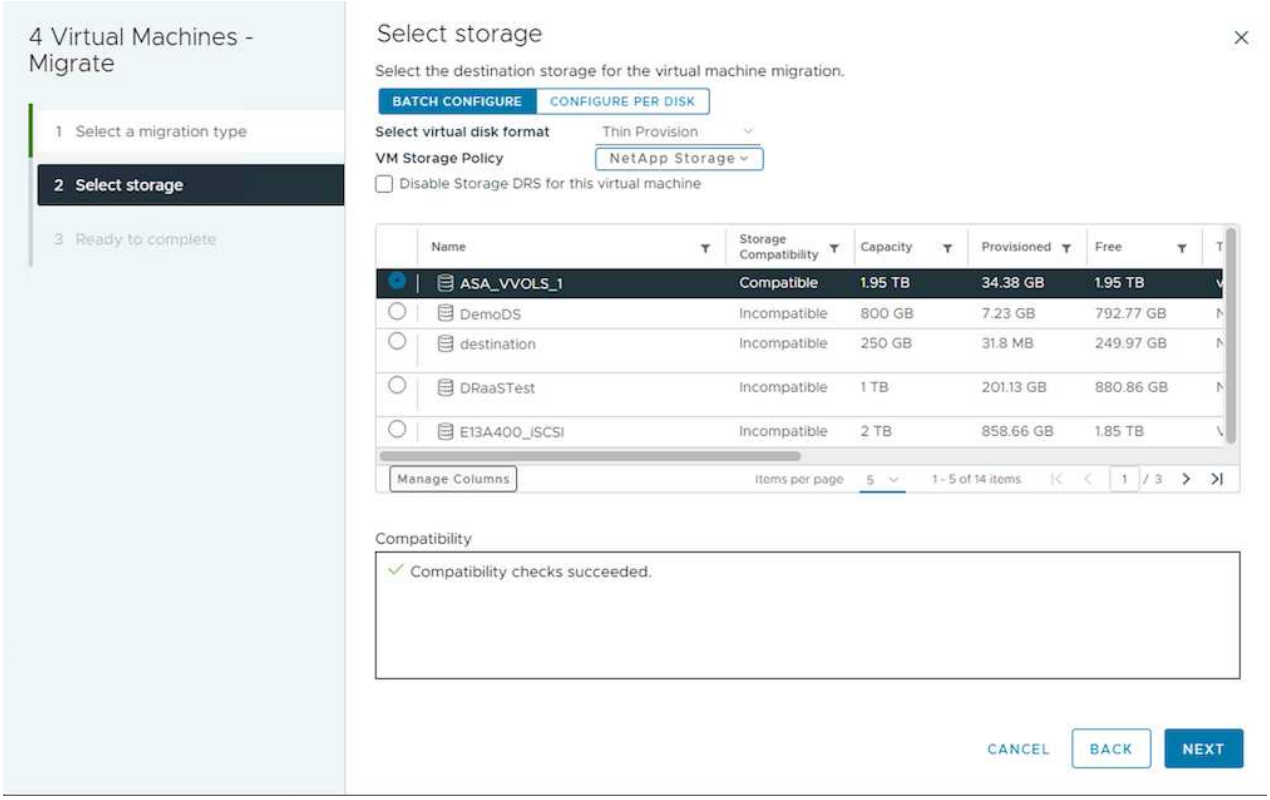
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



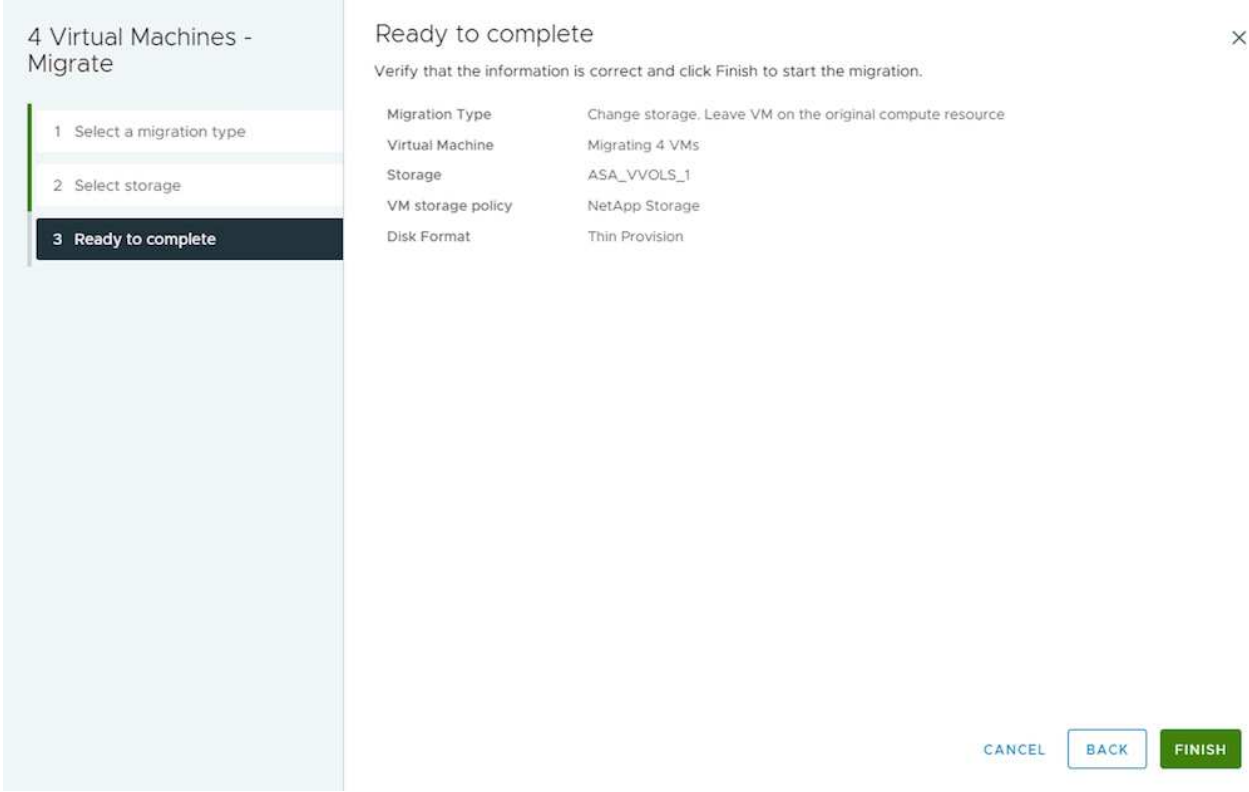
3. Scegliere l'opzione per modificare solo l'archiviazione, quindi fare clic su Avanti



4. Seleziona la policy storage della macchina virtuale desiderata e scegli l'archivio dati compatibile. Fare clic su Avanti.



5. Rivedere e fare clic su fine.



Per migrare le macchine virtuali utilizzando PowerCLI, ecco lo script di esempio.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

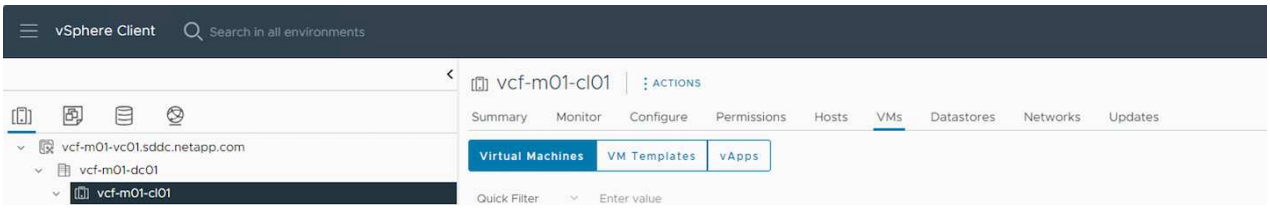
Quando viene utilizzato DataStore Cluster con DRS (Dynamic Resource Scheduling) di storage completamente automatizzato ed entrambi i datastore (origine e destinazione) sono dello stesso tipo (VMFS/NFS/vVol), mantenere entrambi i datastore nello stesso cluster storage e migrare le macchine virtuali dal datastore di origine, abilitando la modalità di manutenzione sull'origine. L'esperienza sarà simile a come gli host di calcolo sono gestiti per la manutenzione.

Migrazione di VM in più cluster vSphere

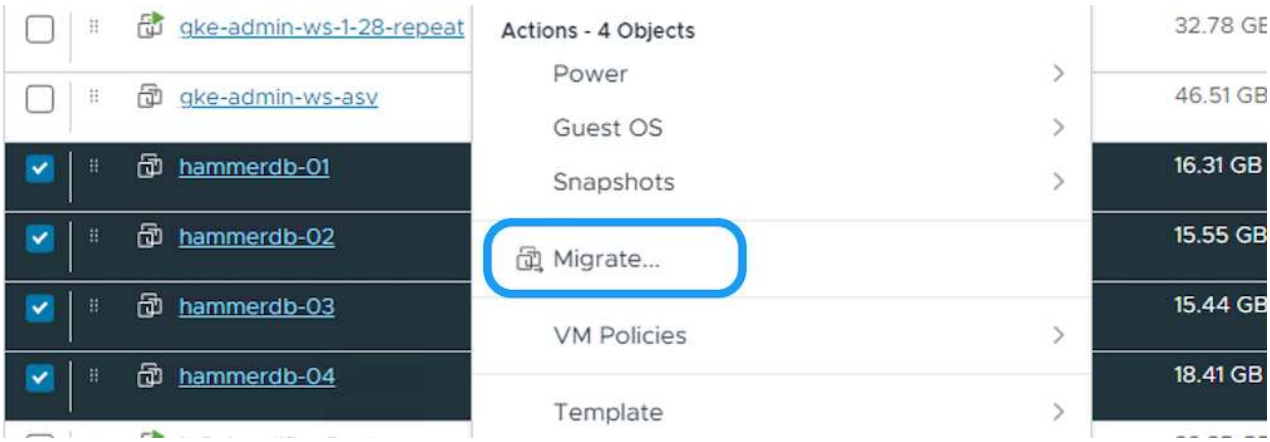
> Fare riferimento a. "Compatibilità CPU e compatibilità vSphere Enhanced vMotion" Quando gli host di origine e di destinazione sono di famiglia o modello CPU diversi.

Seguire la procedura riportata di seguito per eseguire la migrazione delle macchine virtuali al nuovo datastore utilizzando l'interfaccia utente.

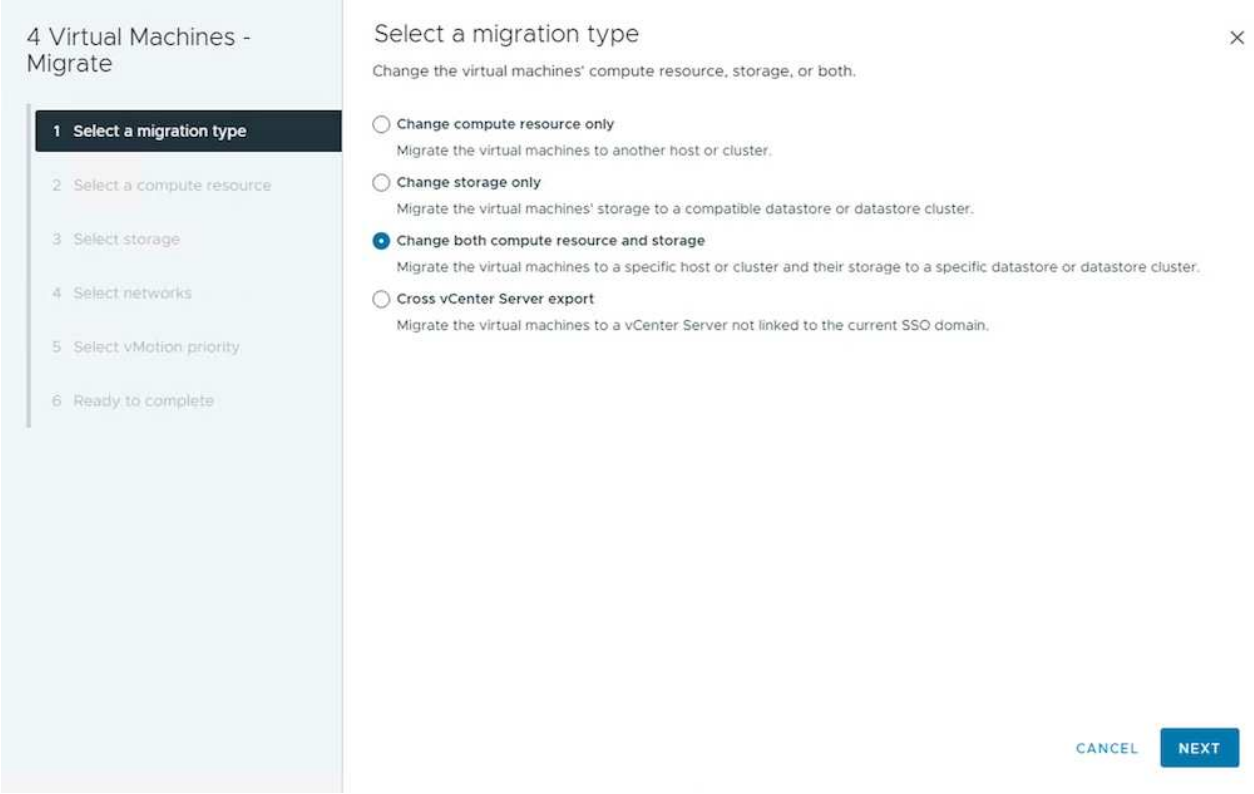
1. Con vSphere Web Client, selezionare il cluster dall'inventario host e cluster e fare clic sulla scheda VM.



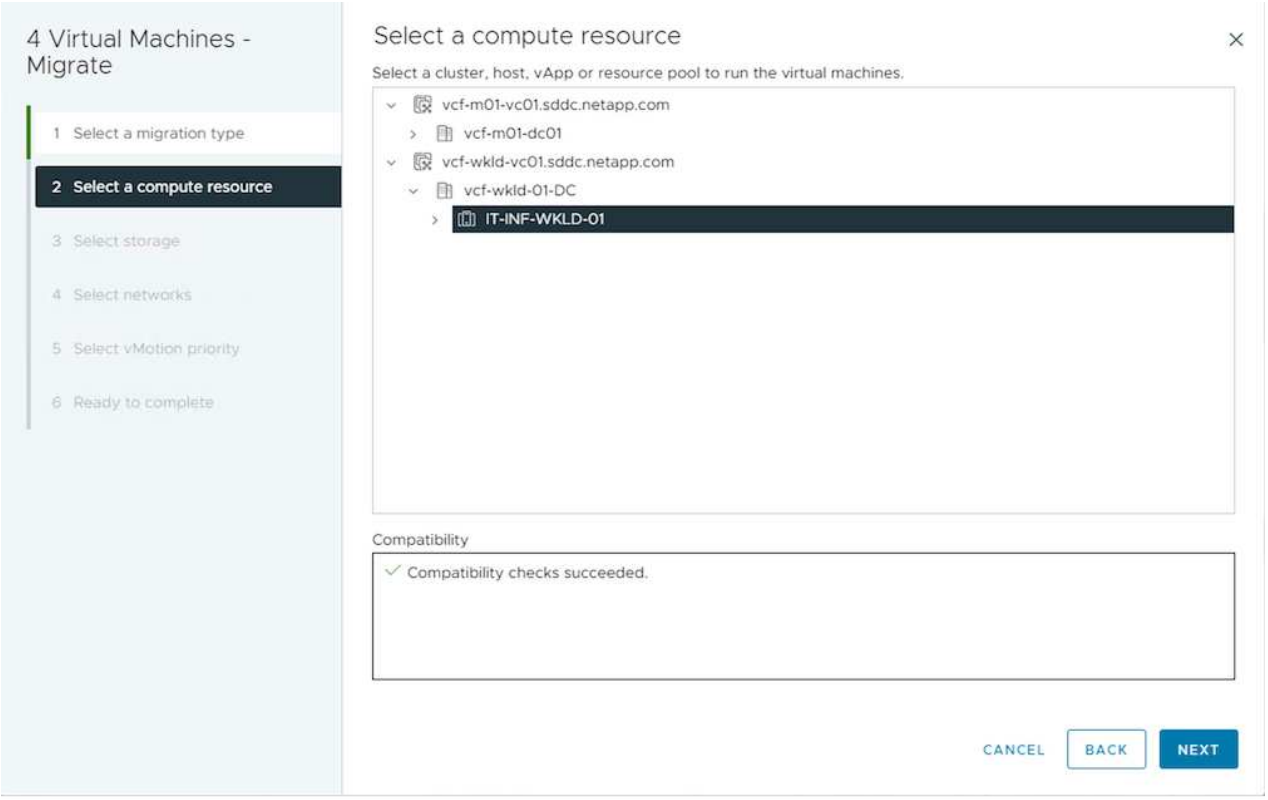
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



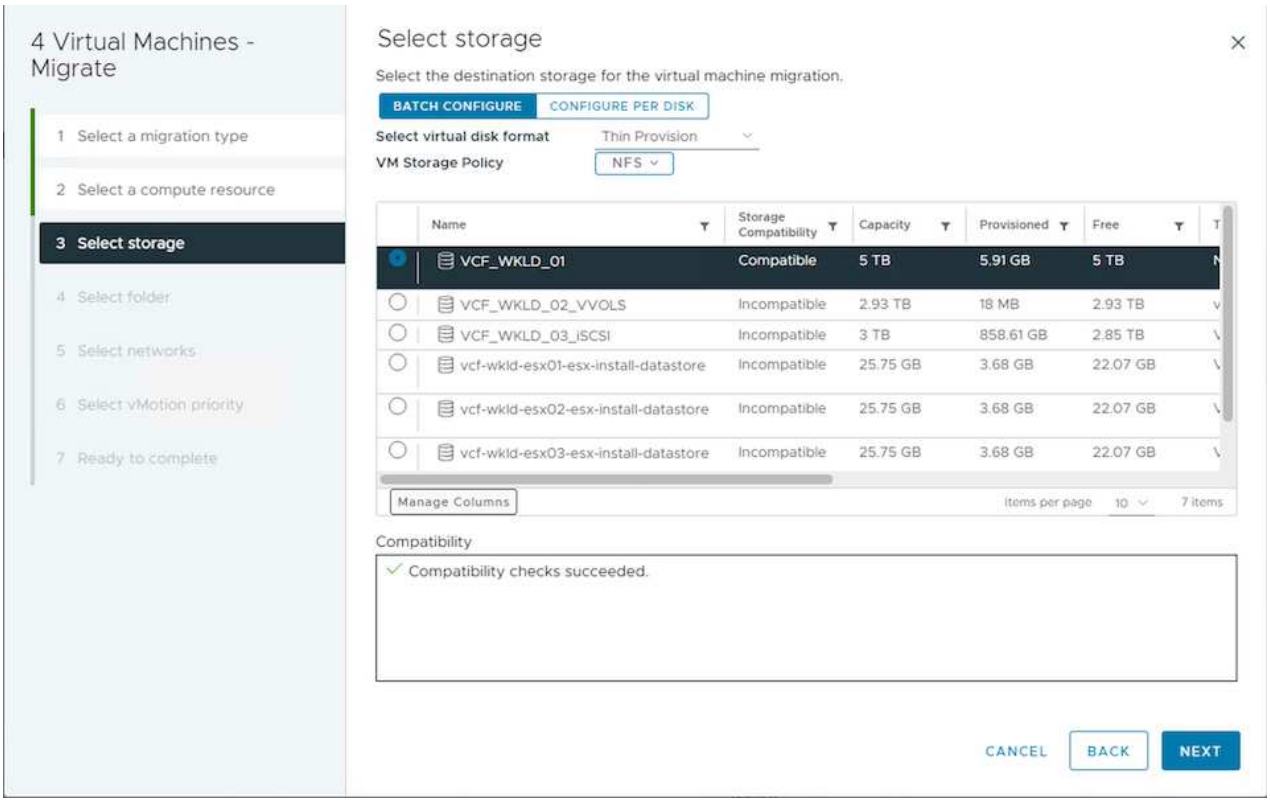
3. Scegliere l'opzione per modificare la risorsa di calcolo e l'archiviazione, quindi fare clic su Avanti



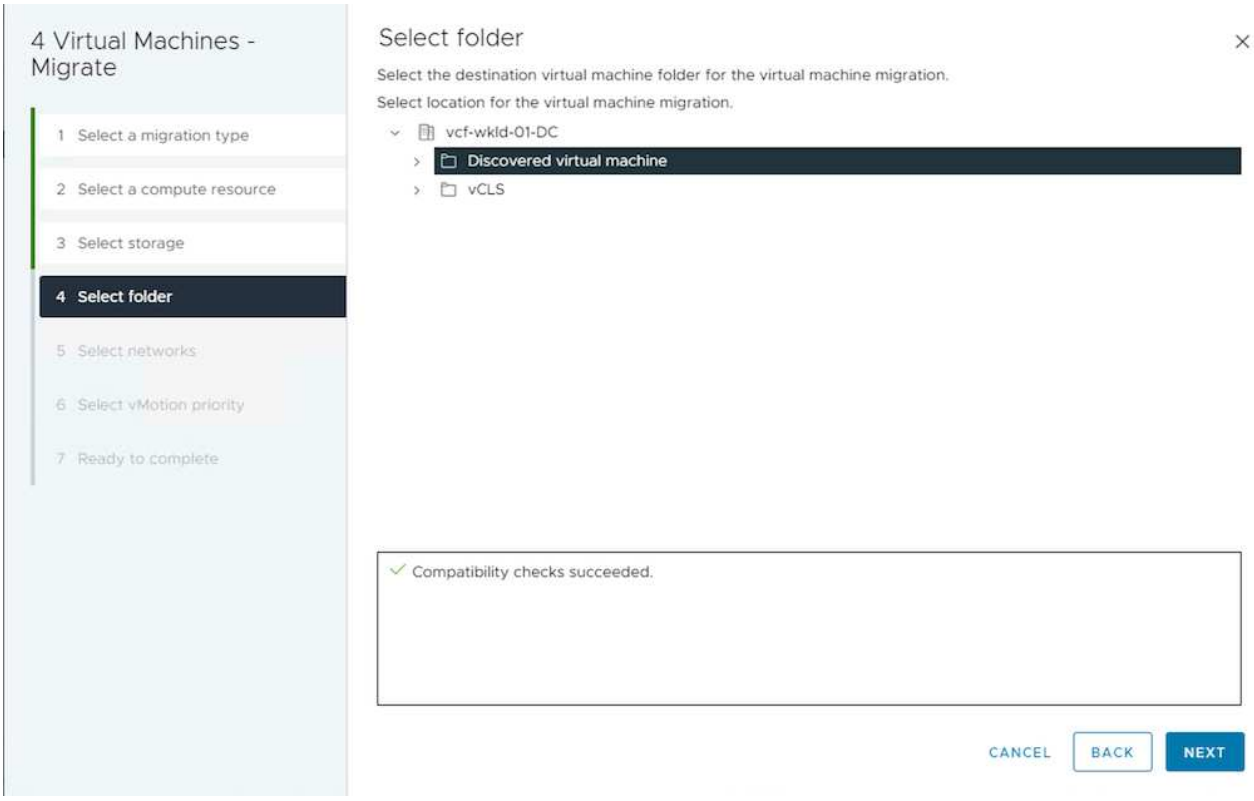
4. Naviga e scegli il cluster giusto per migrare.



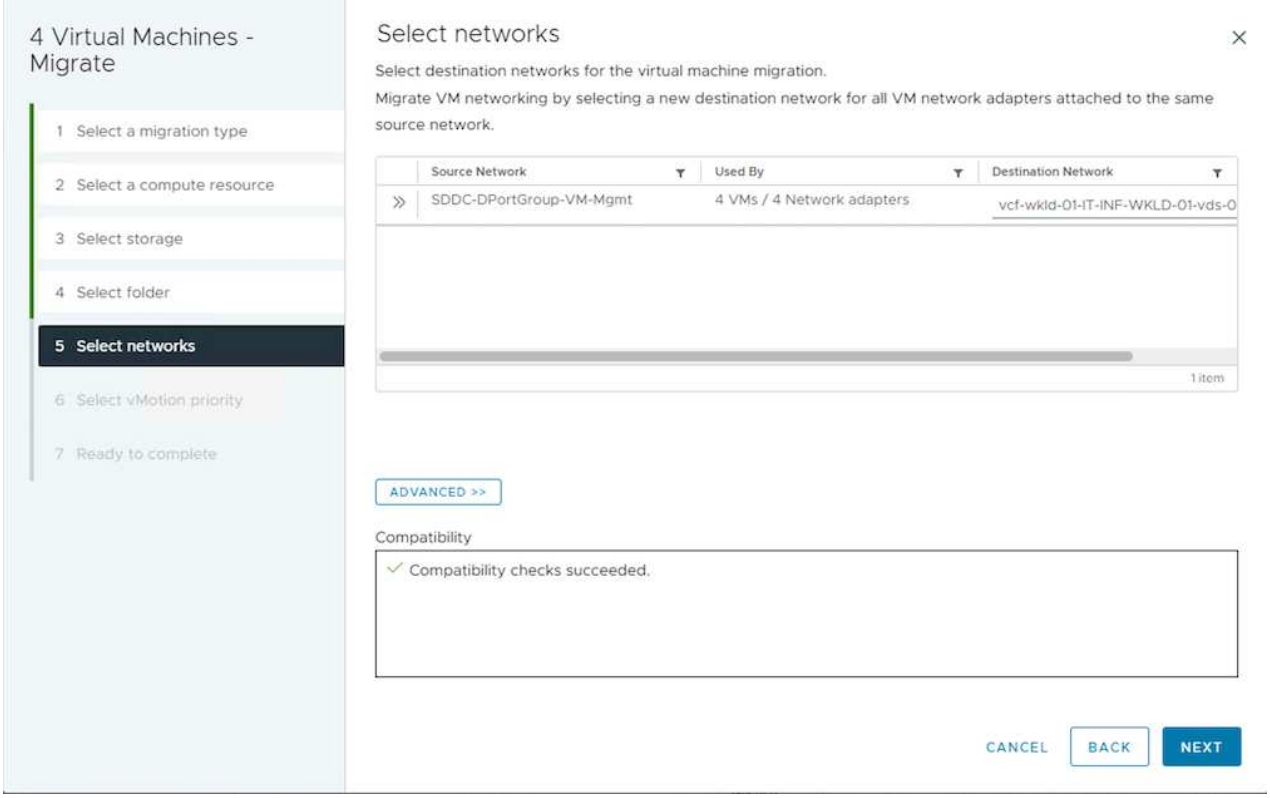
5. Seleziona la policy storage della macchina virtuale desiderata e scegli l’archivio dati compatibile. Fare clic su Avanti.



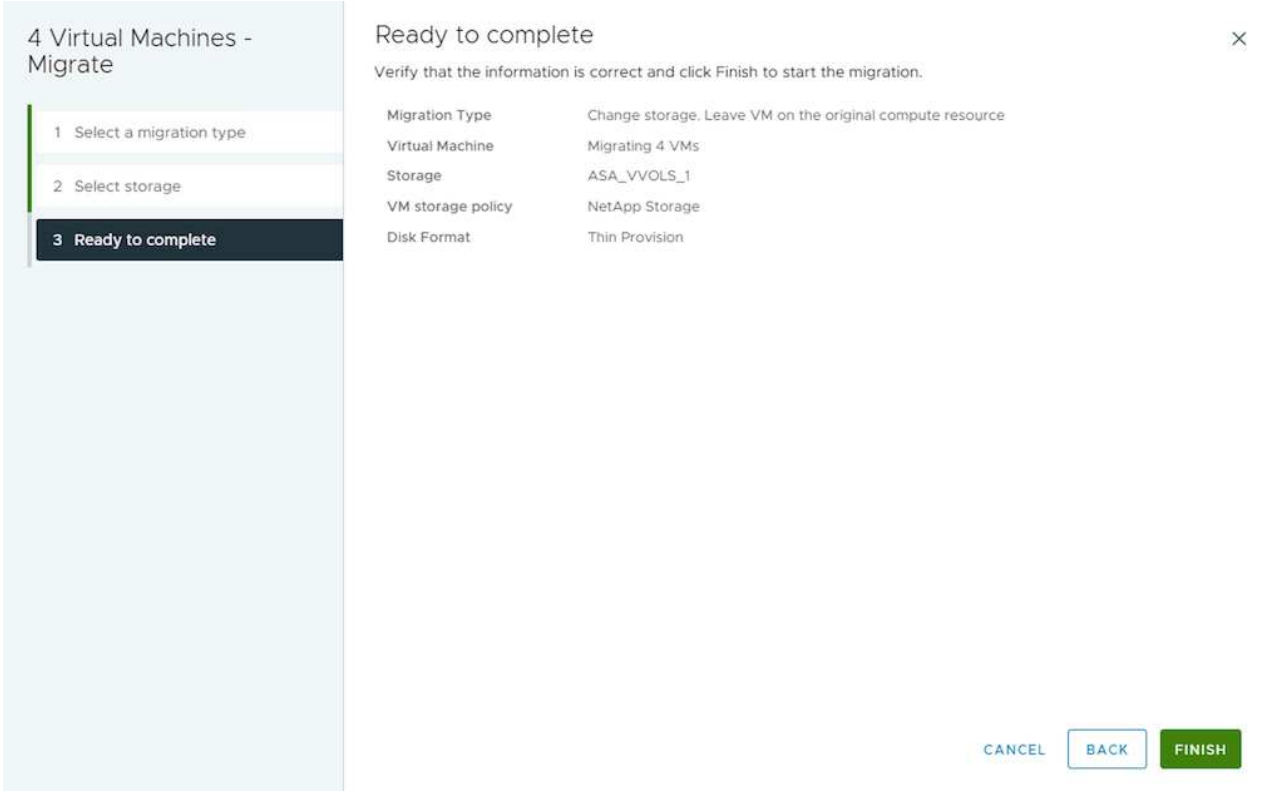
6. Scegliere la cartella VM per posizionare le VM di destinazione.



7. Selezionare il gruppo di porte di destinazione.



8. Rivedere e fare clic su fine.



Per migrare le macchine virtuali utilizzando PowerCLI, ecco lo script di esempio.

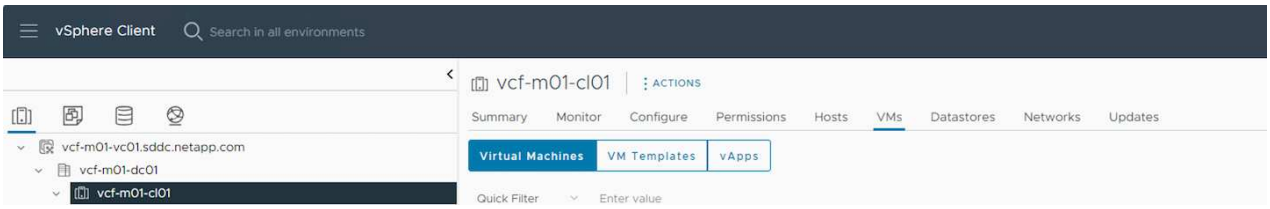
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migrazione di VM tra server vCenter nello stesso dominio SSO

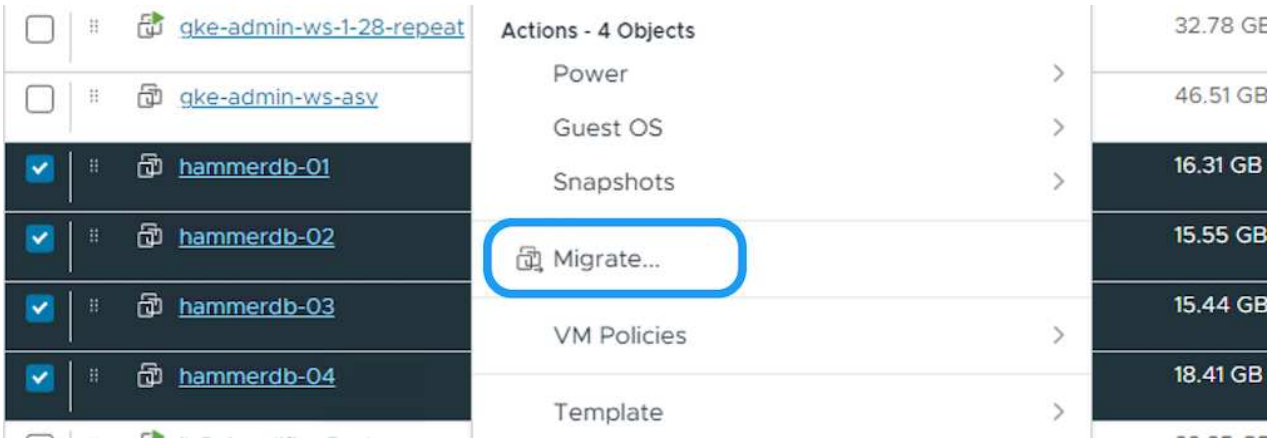
Seguire la procedura riportata di seguito per migrare le macchine virtuali al nuovo server vCenter elencato nella stessa interfaccia utente del client vSphere.

> Per ulteriori requisiti come le versioni vCenter di origine e destinazione, ecc., controllare "Documentazione vSphere sui requisiti di vMotion tra le istanze del server vCenter"

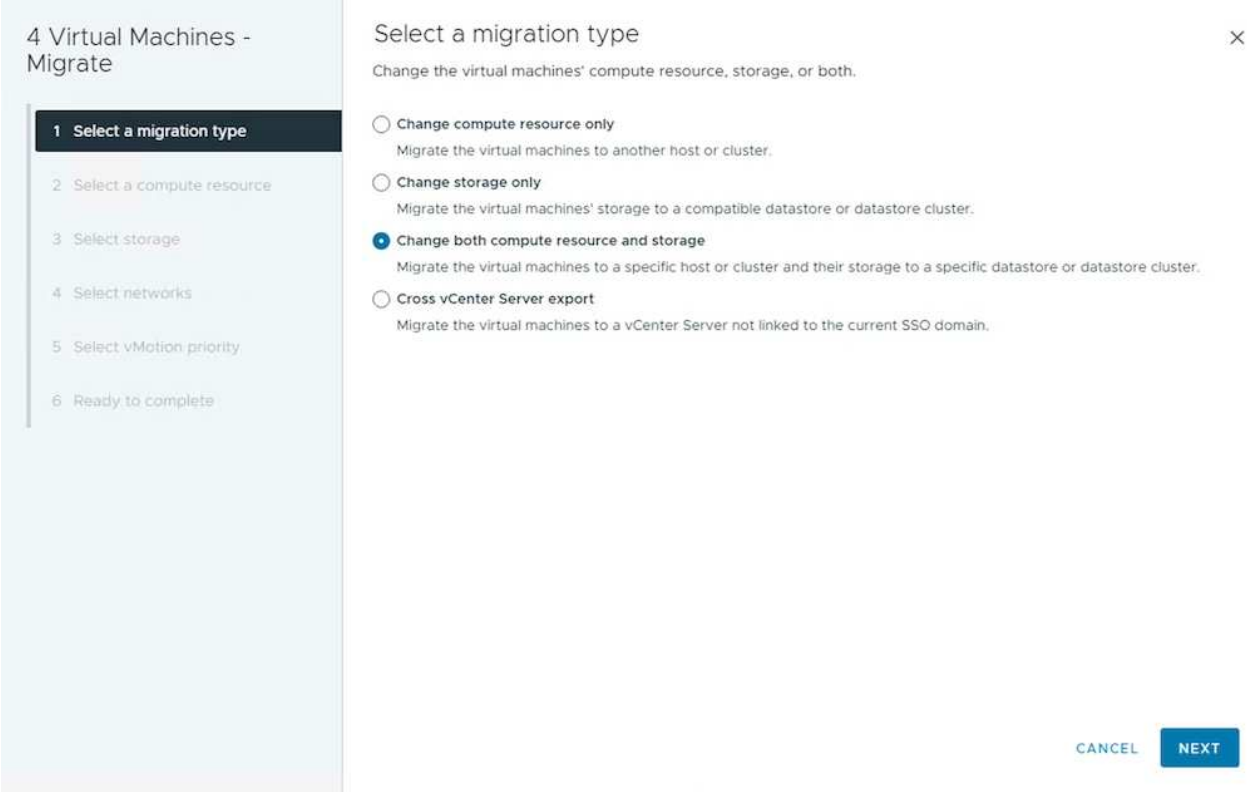
1. Con vSphere Web Client, selezionare il cluster dall'inventario host e cluster e fare clic sulla scheda VM.



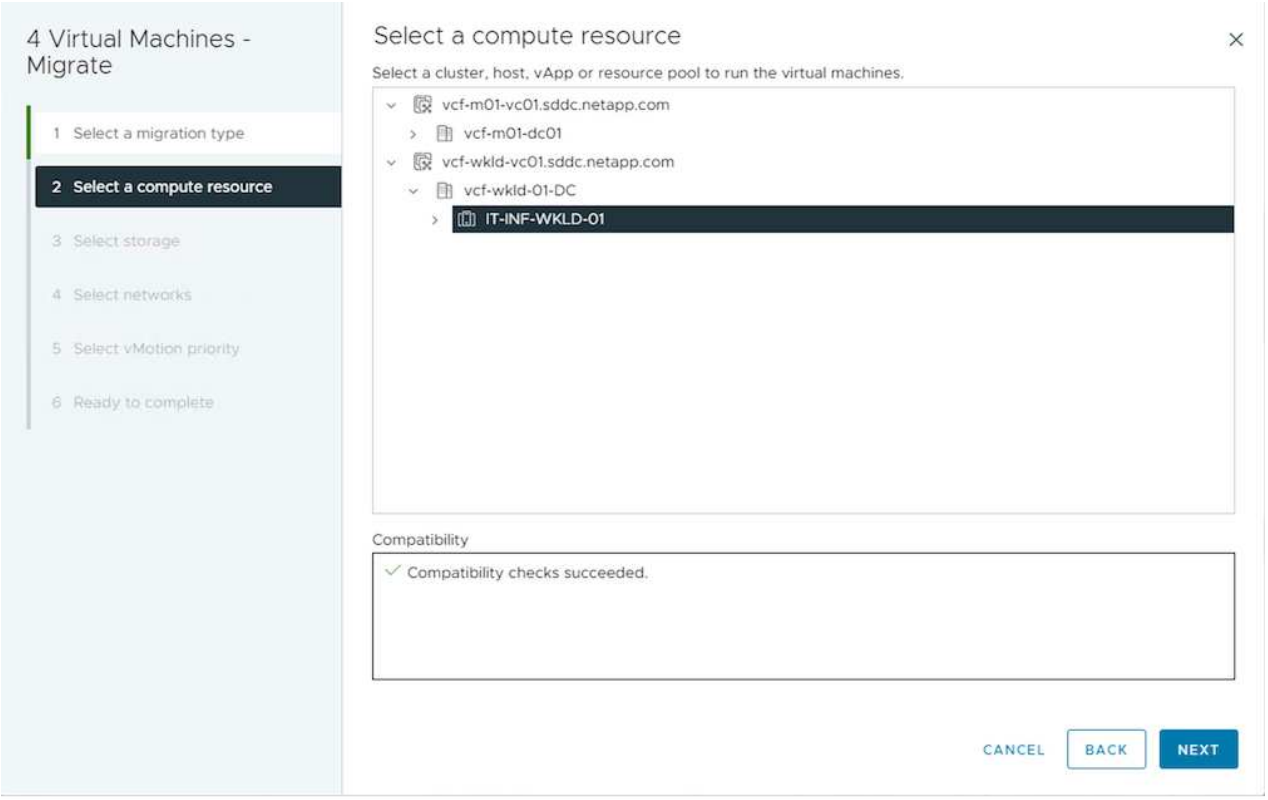
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



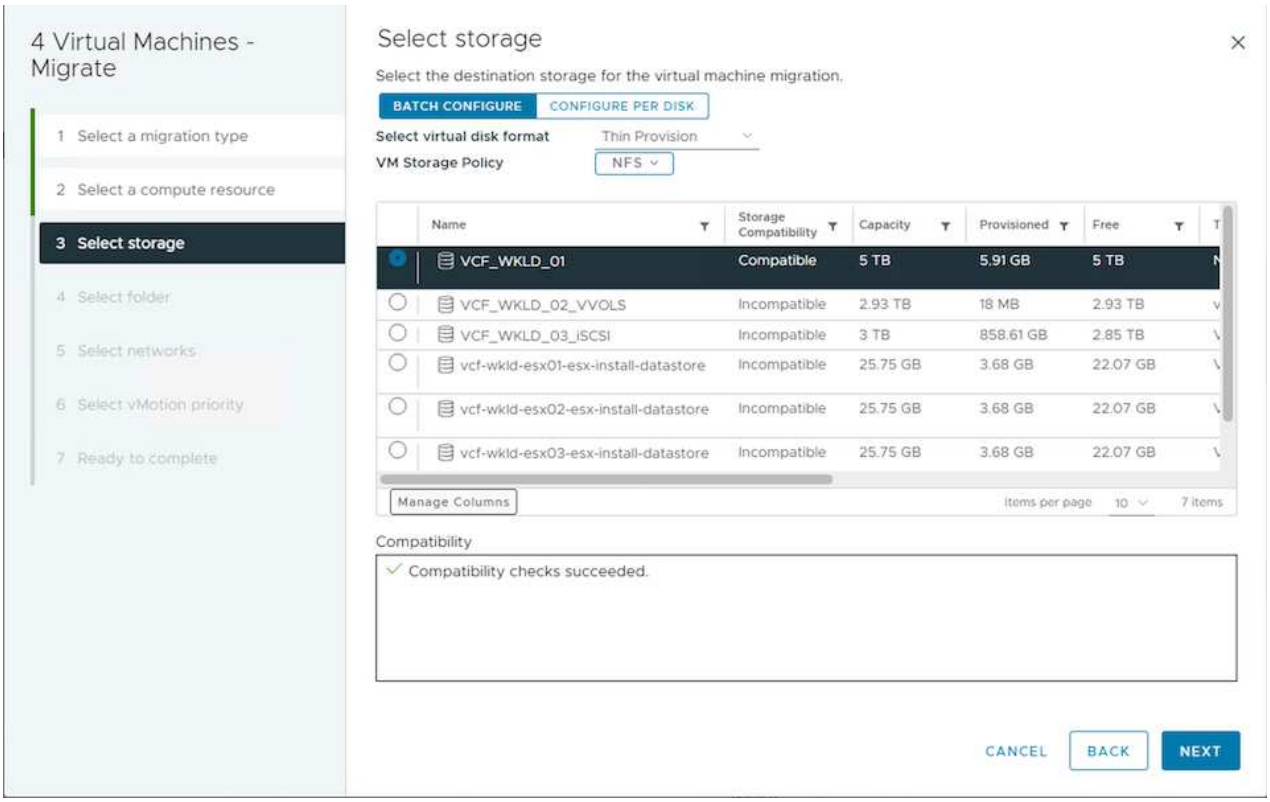
3. Scegliere l'opzione per modificare la risorsa di calcolo e l'archiviazione, quindi fare clic su Avanti



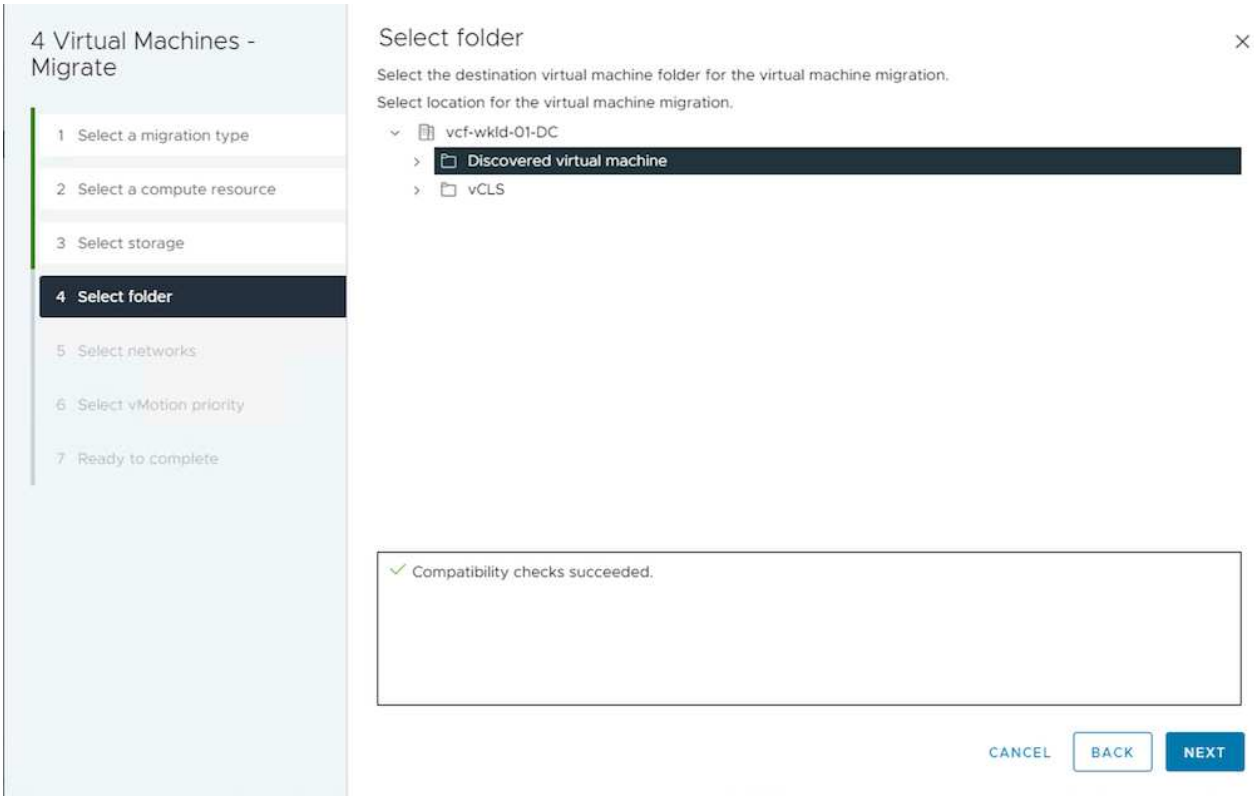
4. Selezionare il cluster di destinazione nel server vCenter di destinazione.



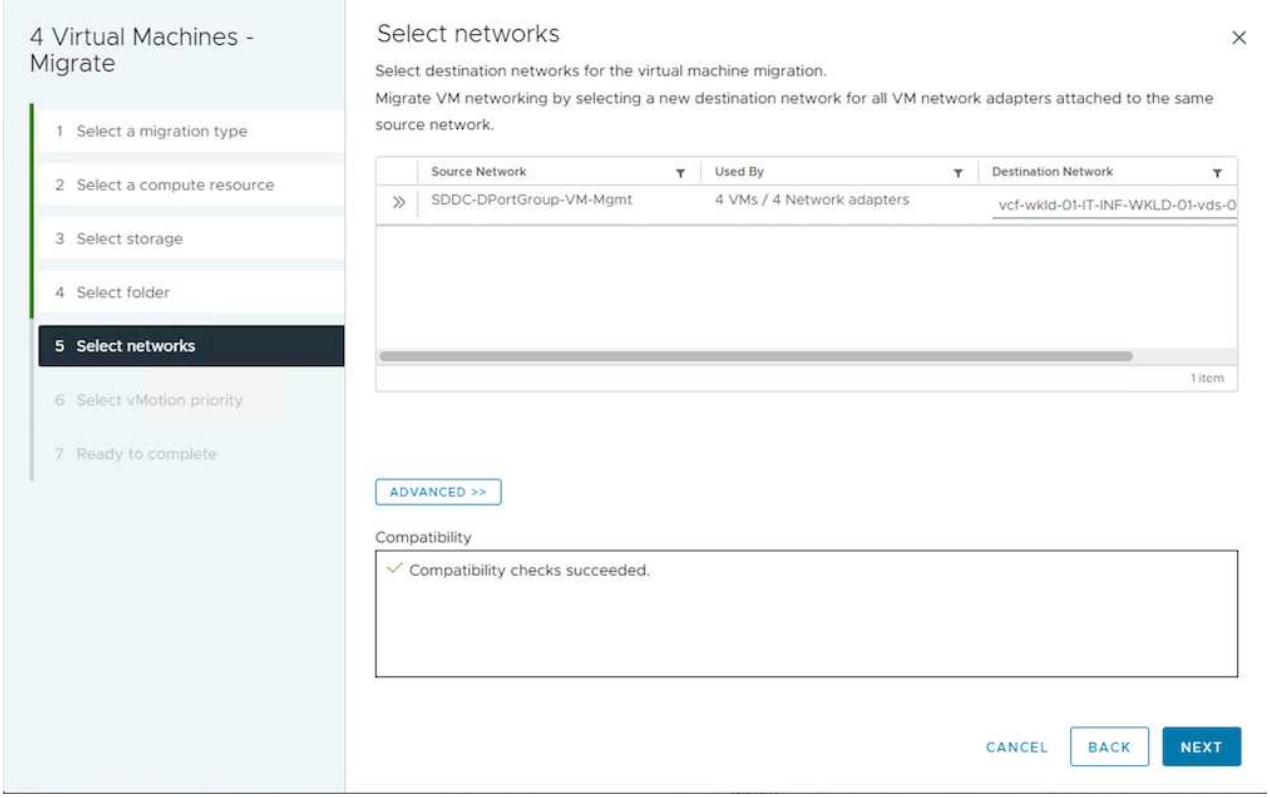
5. Seleziona la policy storage della macchina virtuale desiderata e scegli l’archivio dati compatibile. Fare clic su Avanti.



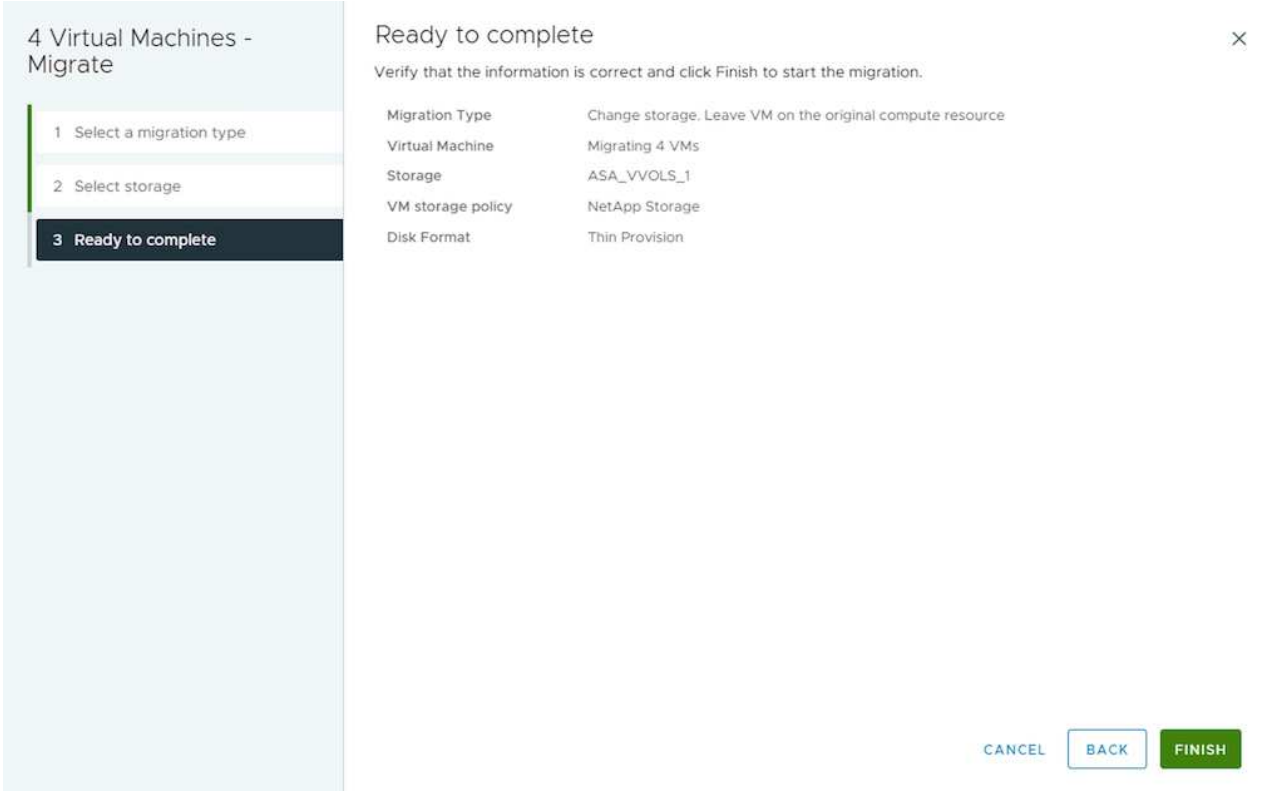
6. Scegliere la cartella VM per posizionare le VM di destinazione.



7. Selezionare il gruppo di porte di destinazione.



8. Esaminare le opzioni di migrazione e fare clic su fine.



Per migrare le macchine virtuali utilizzando PowerCLI, ecco lo script di esempio.

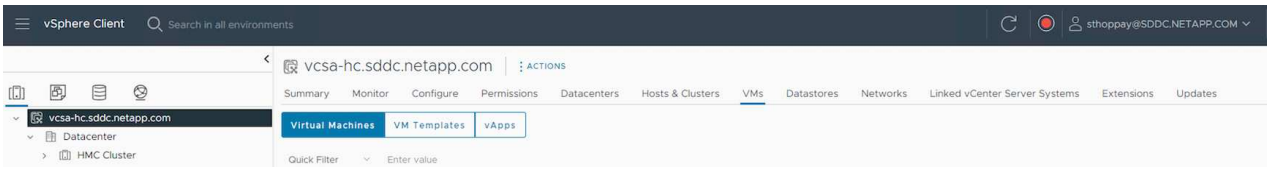
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migrazione di macchine virtuali tra server vCenter in un dominio SSO diverso

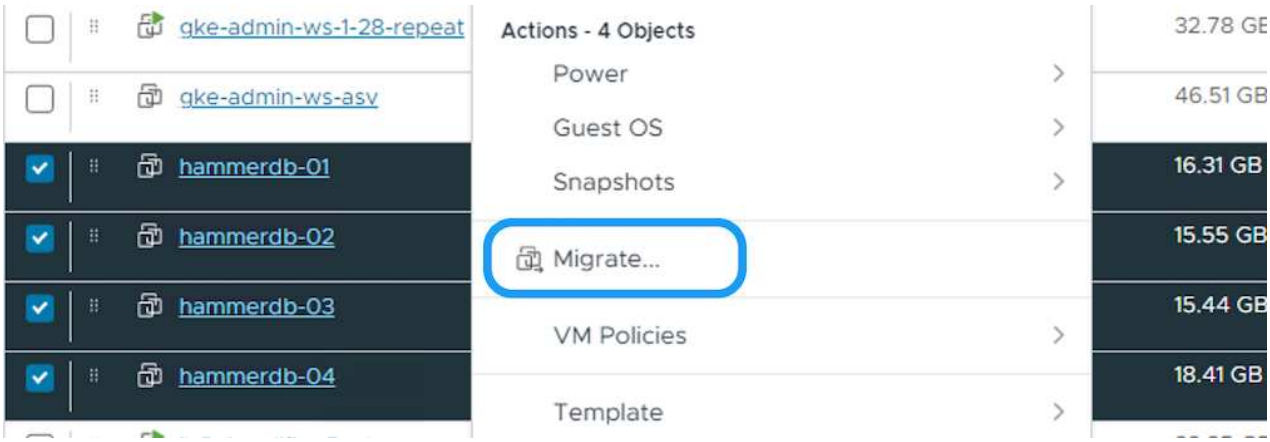
> Questo scenario presuppone che la comunicazione esista tra i server vCenter. In caso contrario, controllare lo scenario di ubicazione del data center riportato di seguito. Per i prerequisiti, controllare "Documentazione vSphere su Advanced Cross vCenter vMotion"

Seguire la procedura riportata di seguito per migrare le macchine virtuali a un server vCenter diverso utilizzando l'interfaccia utente.

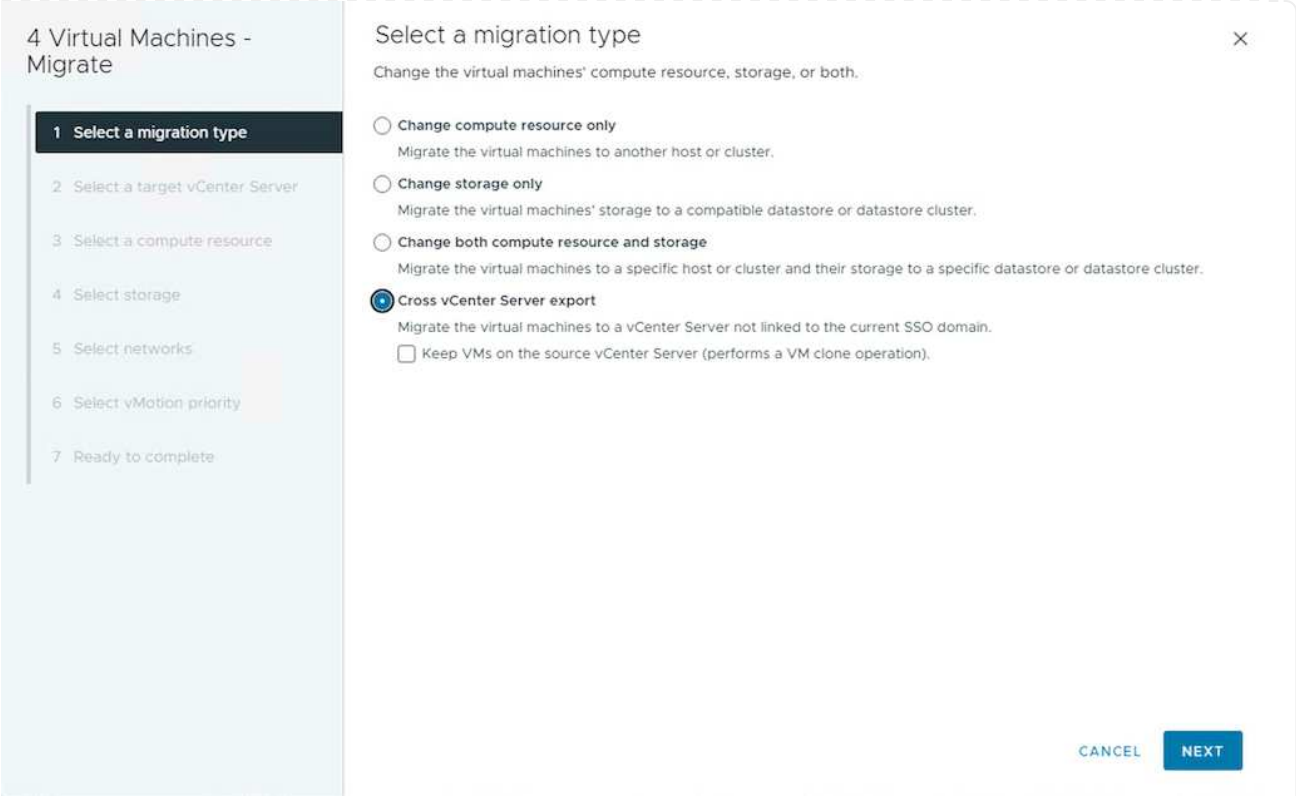
1. Con vSphere Web Client, selezionare il server vCenter di origine e fare clic sulla scheda VM.



2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

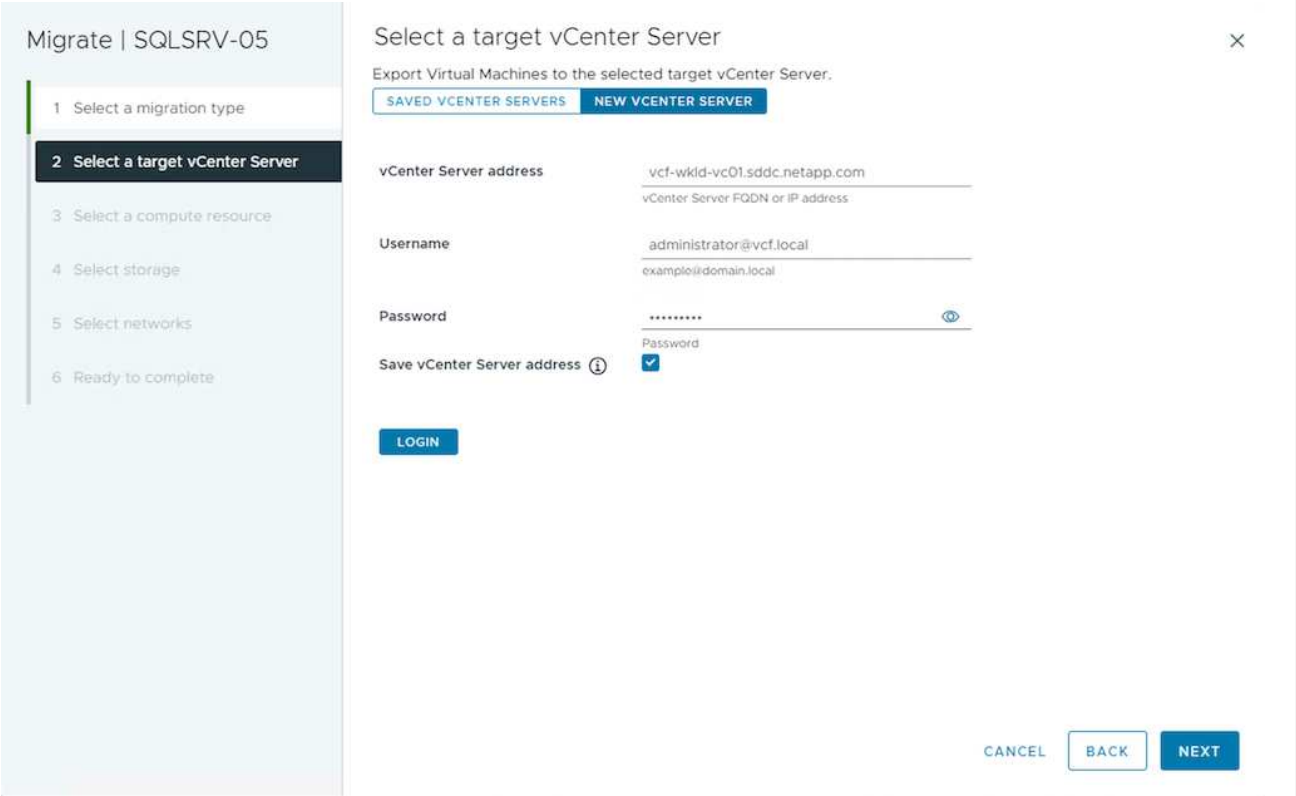


3. Scegliere l'opzione Cross vCenter Server Export, quindi fare clic su Next

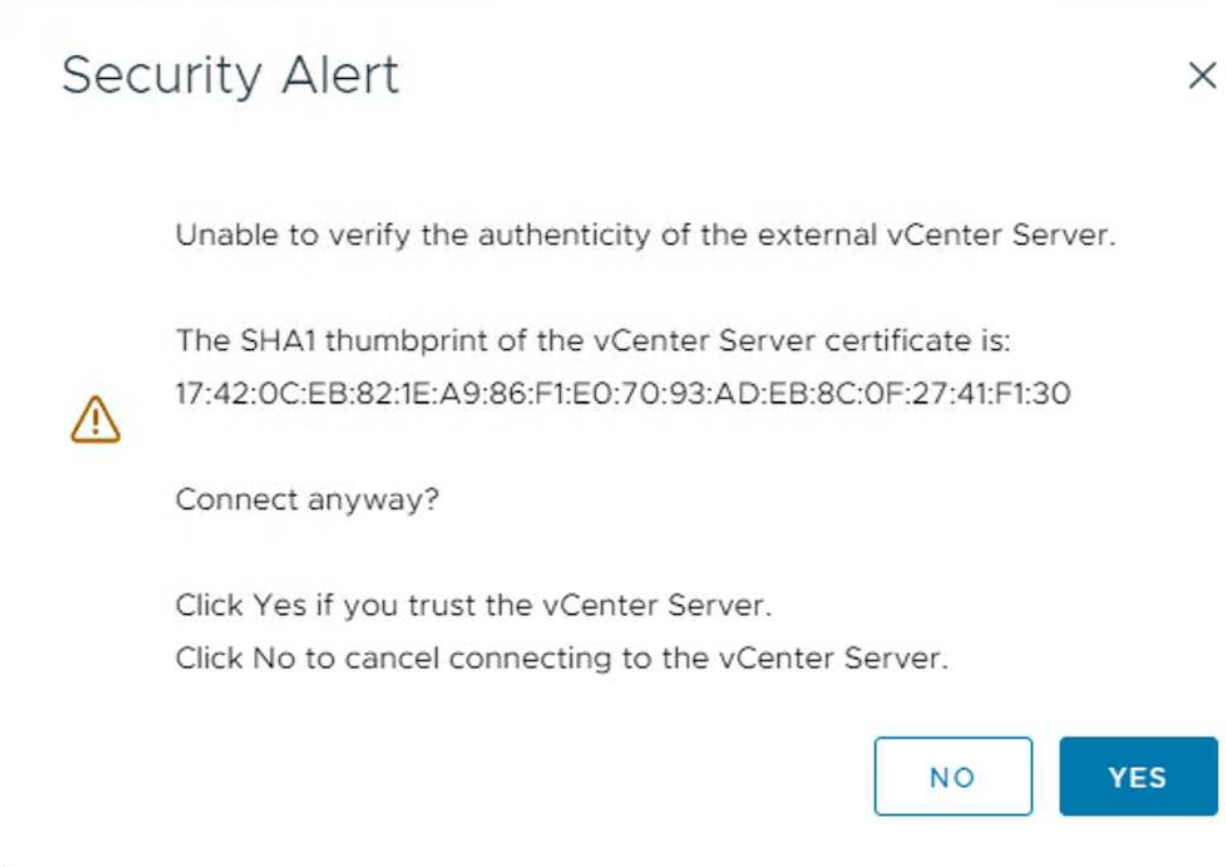


È anche possibile importare una VM dal server vCenter di destinazione. Per questa procedura, controllare "Importazione o clonazione di una macchina virtuale con Advanced Cross vCenter vMotion"

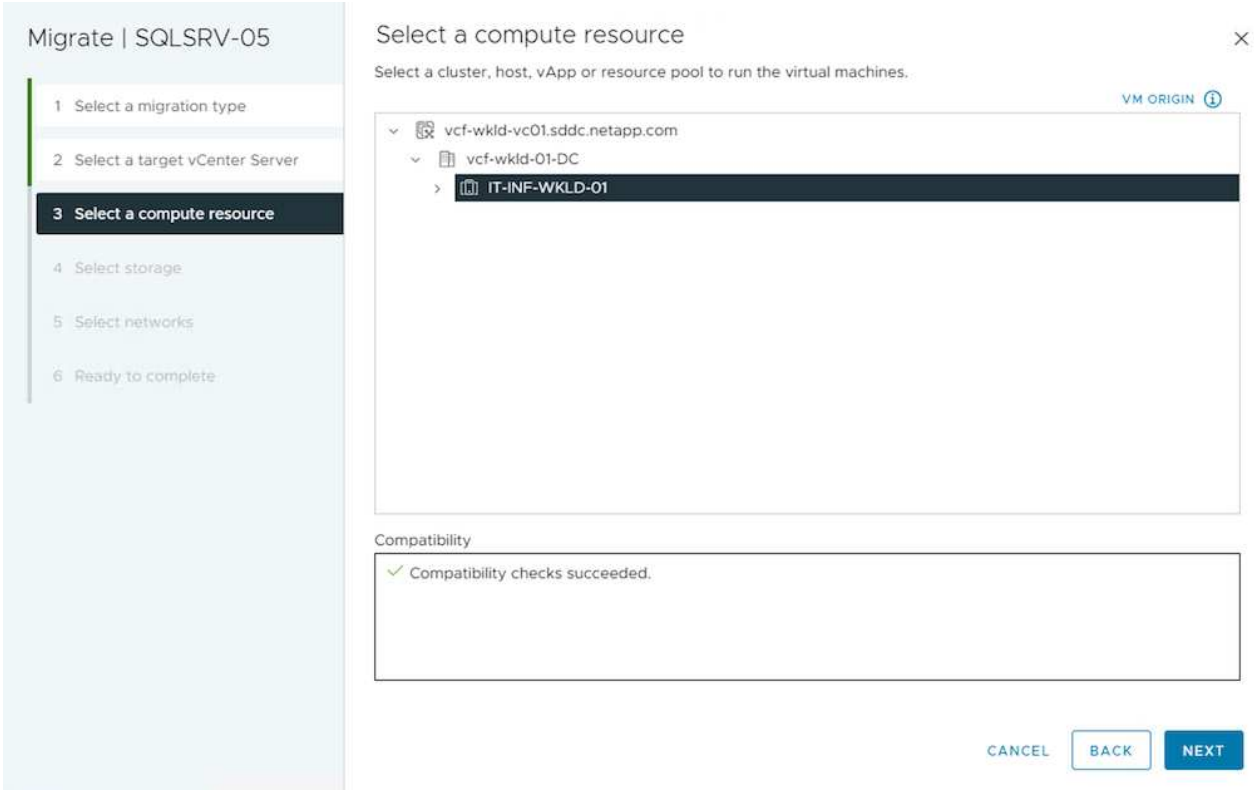
4. Fornire i dettagli delle credenziali vCenter e fare clic su Login (accesso).



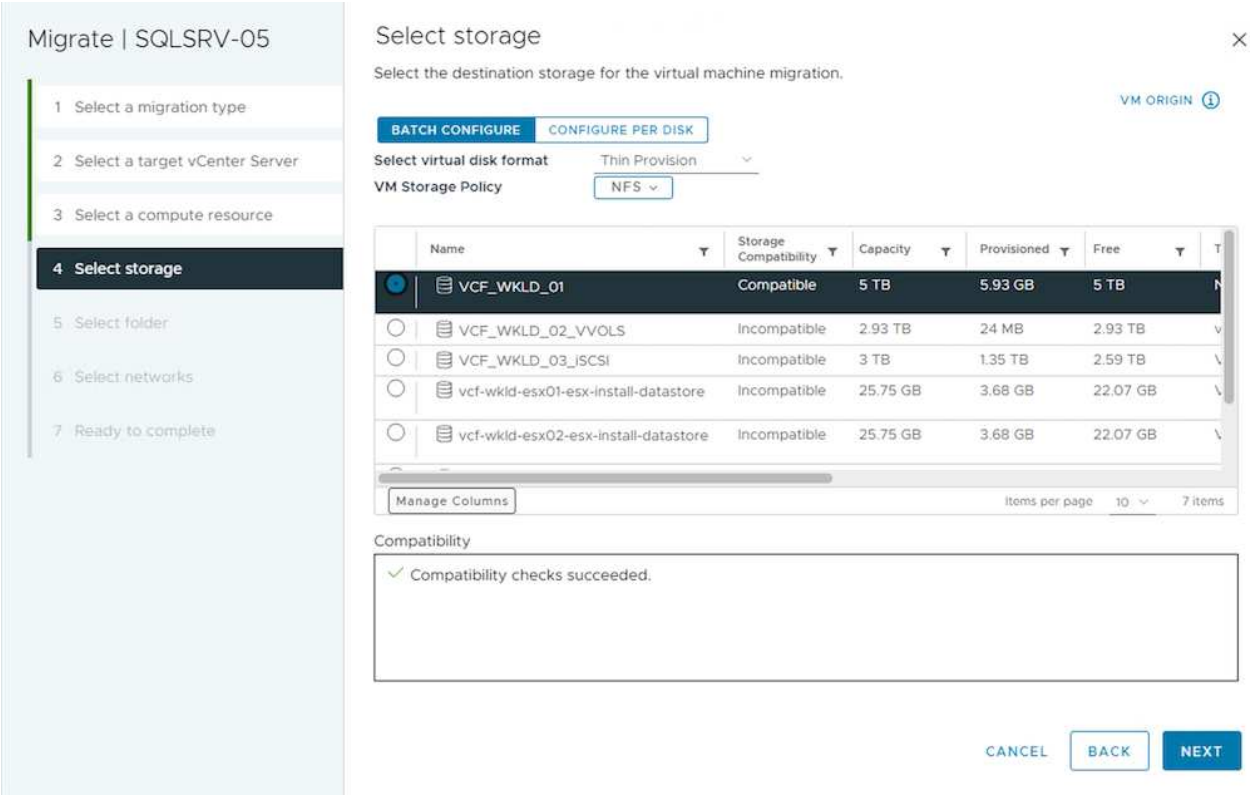
5. Confermare e accettare l'identificazione del certificato SSL del server vCenter



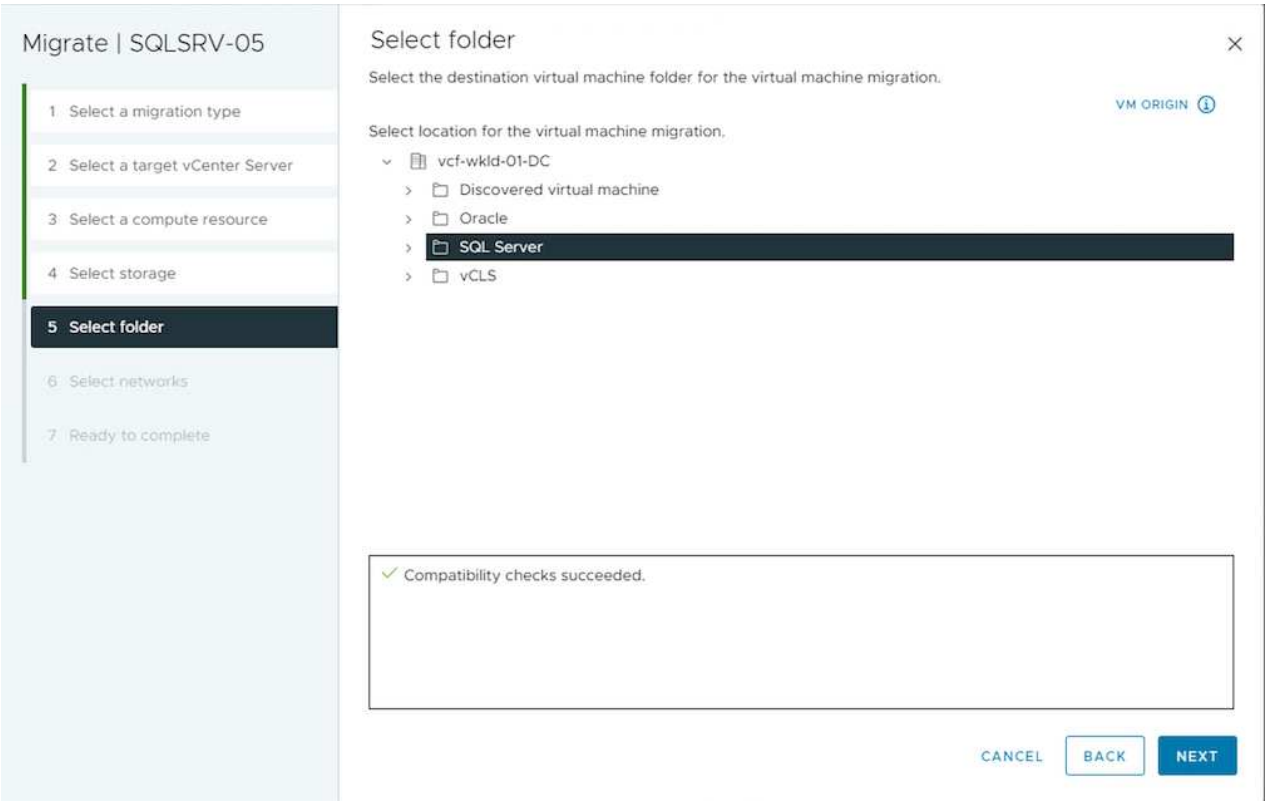
6. Espandi vCenter di destinazione e seleziona il cluster di calcolo di destinazione.



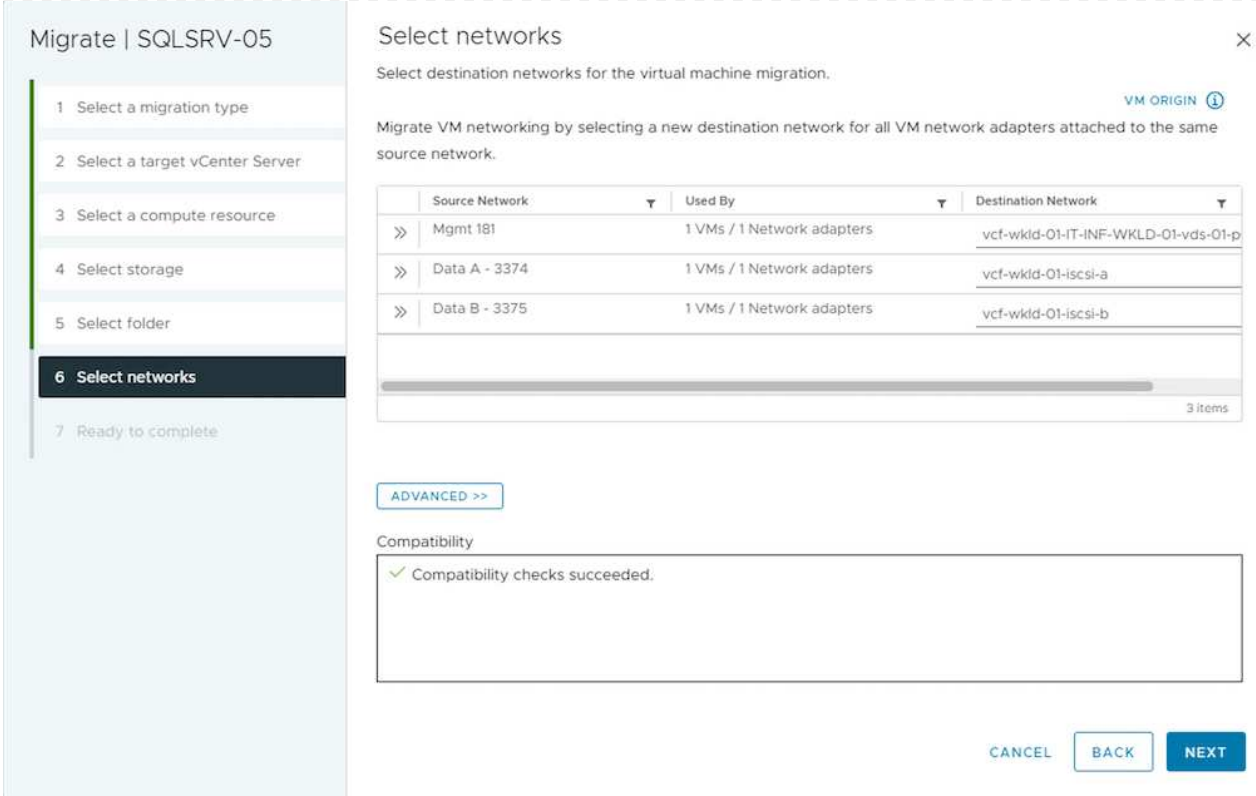
7. Seleziona il datastore di destinazione in base alla policy storage della macchina virtuale.



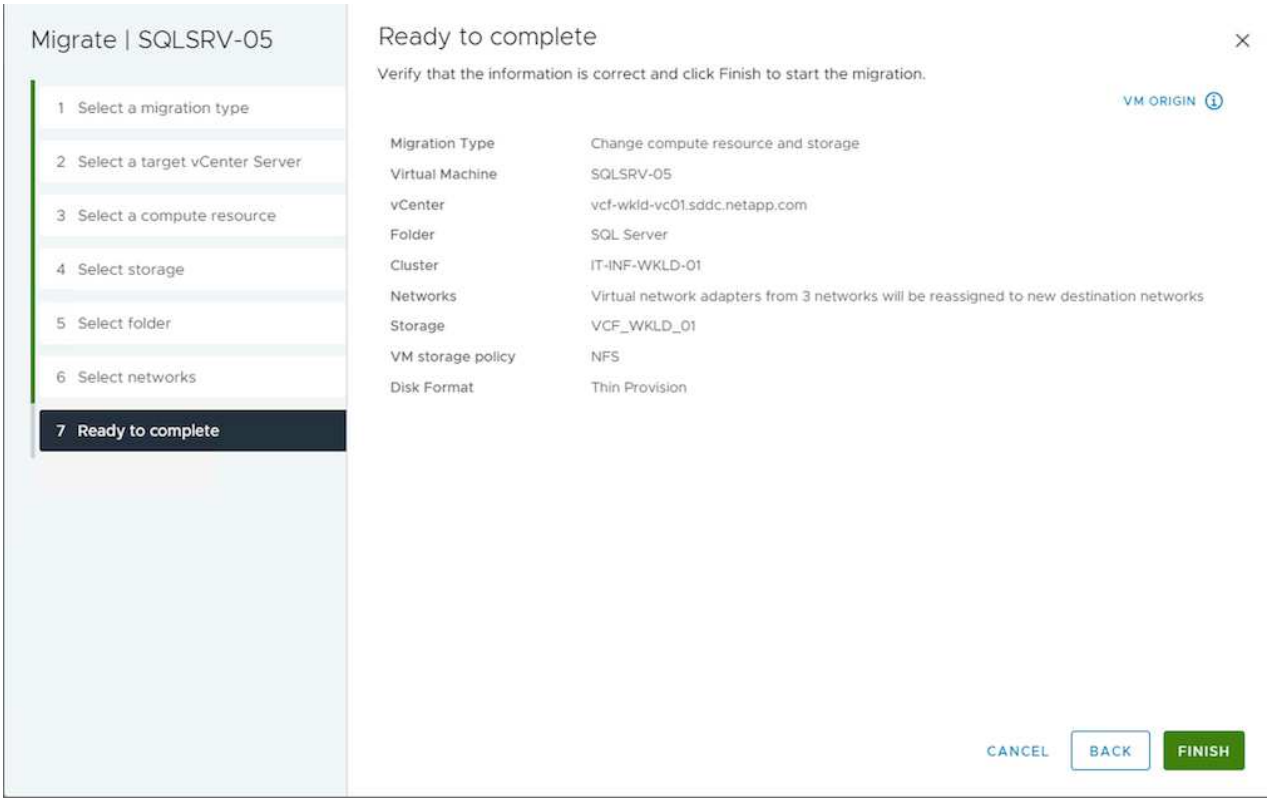
8. Selezionare la cartella VM di destinazione.



9. Scegliere il gruppo di porte VM per ciascuna mappatura della scheda di interfaccia di rete.



10. Esaminare e fare clic su fine per avviare vMotion sui server vCenter.



Per migrare le macchine virtuali utilizzando PowerCLI, ecco lo script di esempio.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migrazione di VM nelle ubicazioni dei data center

- Quando il traffico di livello 2 viene esteso tra i data center utilizzando NSX Federation o altre opzioni, seguire la procedura per la migrazione delle VM tra i server vCenter.
- HCX fornisce vari "tipi di migrazione" Include vMotion assistito dalla replica nei data center per spostare la VM senza downtime.
- "Site Recovery Manager (SRM)" È generalmente destinato a scopi di ripristino di emergenza e spesso viene utilizzato per la migrazione pianificata mediante la replica basata su array di storage.
- Utilizzo dei prodotti per la protezione continua dei dati (CDP) "VSphere API per io (VAIO)" Per intercettare i dati e inviare una copia nella posizione remota per una soluzione RPO prossima allo zero.
- Possono essere utilizzati anche i prodotti di backup e ripristino. Ma spesso porta a un RTO più lungo.
- "Disaster Recovery as a Service (DRaaS) di BlueXP" Utilizza la replica basata su storage array e automatizza alcune attività per il ripristino delle macchine virtuali nel sito di destinazione.

Migrazione delle VM in un ambiente di cloud ibrido

- "Configurare la modalità di collegamento ibrida" e seguire la procedura di "Migrazione di VM tra server vCenter nello stesso dominio SSO"
- HCX fornisce vari "tipi di migrazione" Incluso il vMotion assistito dalla replica nei data center per spostare la VM mentre è accesa.
  - Link:../ehc/aws-migrate-vmware-hcx.html [TR 4942: Migrazione dei carichi di lavoro nel datastore FSX ONTAP con VMware HCX]
  - Link:../ehc/azure-migrate-vmware-hcx.html [TR-4940: Migrazione dei carichi di lavoro nel datastore Azure NetApp Files utilizzando VMware HCX - Guida rapida]
  - Link:../ehc/gcp-migrate-vmware-hcx.html [migrazione dei carichi di lavoro nel datastore di NetApp Cloud Volume Service su Google Cloud VMware Engine utilizzando VMware HCX - Guida rapida]
- "Disaster Recovery as a Service (DRaaS) di BlueXP" Utilizza la replica basata su storage array e automatizza alcune attività per il ripristino delle macchine virtuali nel sito di destinazione.
- Con i prodotti CDP (Continuous Data Protection) supportati che utilizzano "VSphere API per io (VAIO)" Per intercettare i dati e inviare una copia nella posizione remota per una soluzione RPO prossima allo zero.

> Quando la macchina virtuale di origine risiede su un datastore vVol a blocchi, può essere replicata con SnapMirror in Amazon FSX per NetApp ONTAP o Cloud Volumes ONTAP (CVO) presso altri cloud provider supportati e consumare come volume iSCSI con macchine virtuali native del cloud.

Scenari di migrazione dei modelli VM

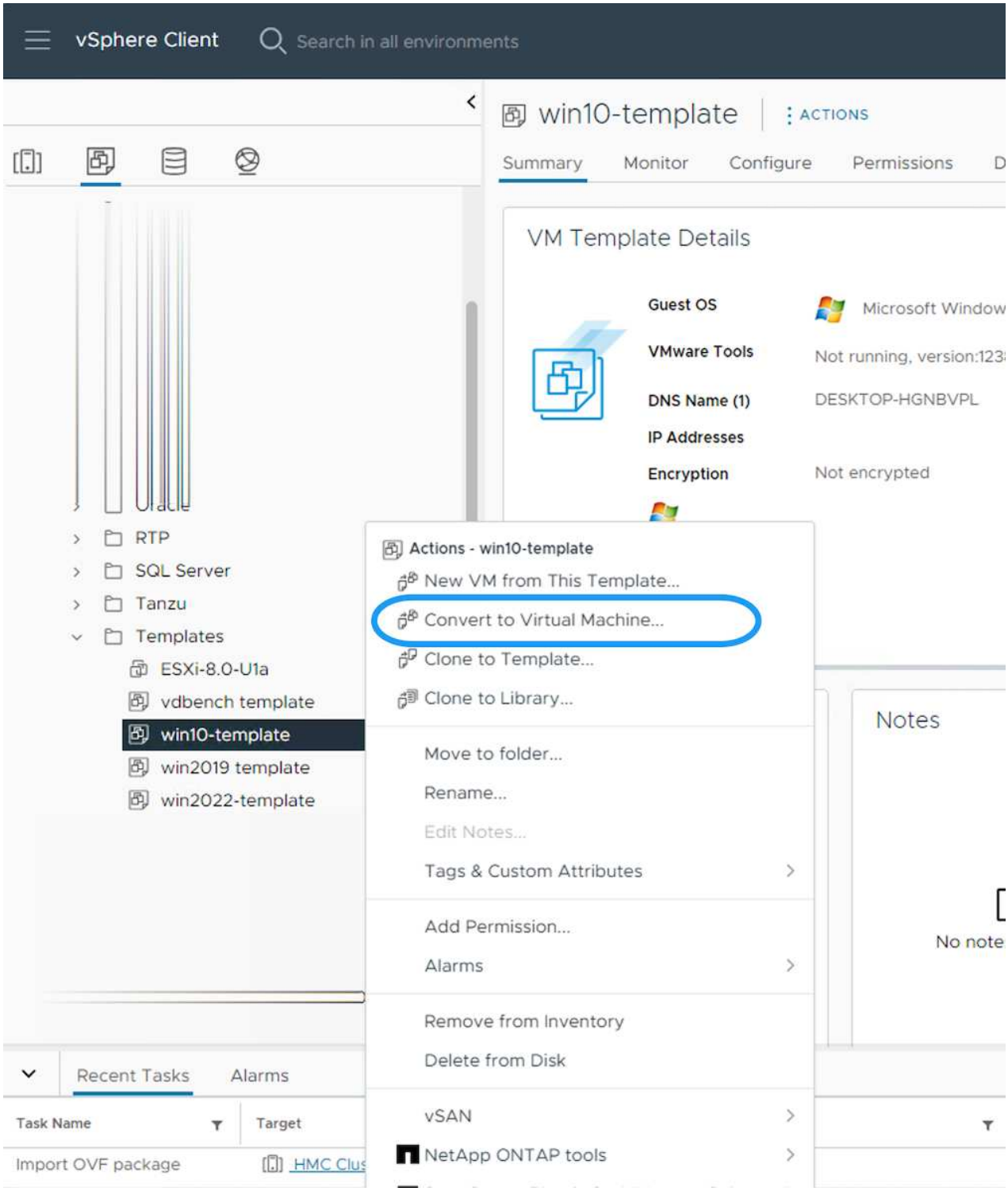
I modelli VM possono essere gestiti da vCenter Server o da una libreria di contenuti. Distribuzione di modelli VM, modelli OVF e OVA, altri tipi di file sono gestiti pubblicandoli nella libreria di contenuti locali e le librerie di contenuti remoti possono abbonarsi ad essa.

- I modelli VM memorizzati nell'inventario vCenter possono essere convertiti in VM e utilizzano le opzioni di migrazione delle VM.

- Modelli OVF e OVA, altri tipi di file memorizzati nella libreria di contenuti possono essere clonati in altre librerie di contenuti.
- I modelli VM della libreria di contenuti possono essere ospitati in qualsiasi datastore e devono essere aggiunti alla nuova libreria di contenuti.

Migrazione di modelli VM ospitati nel datastore

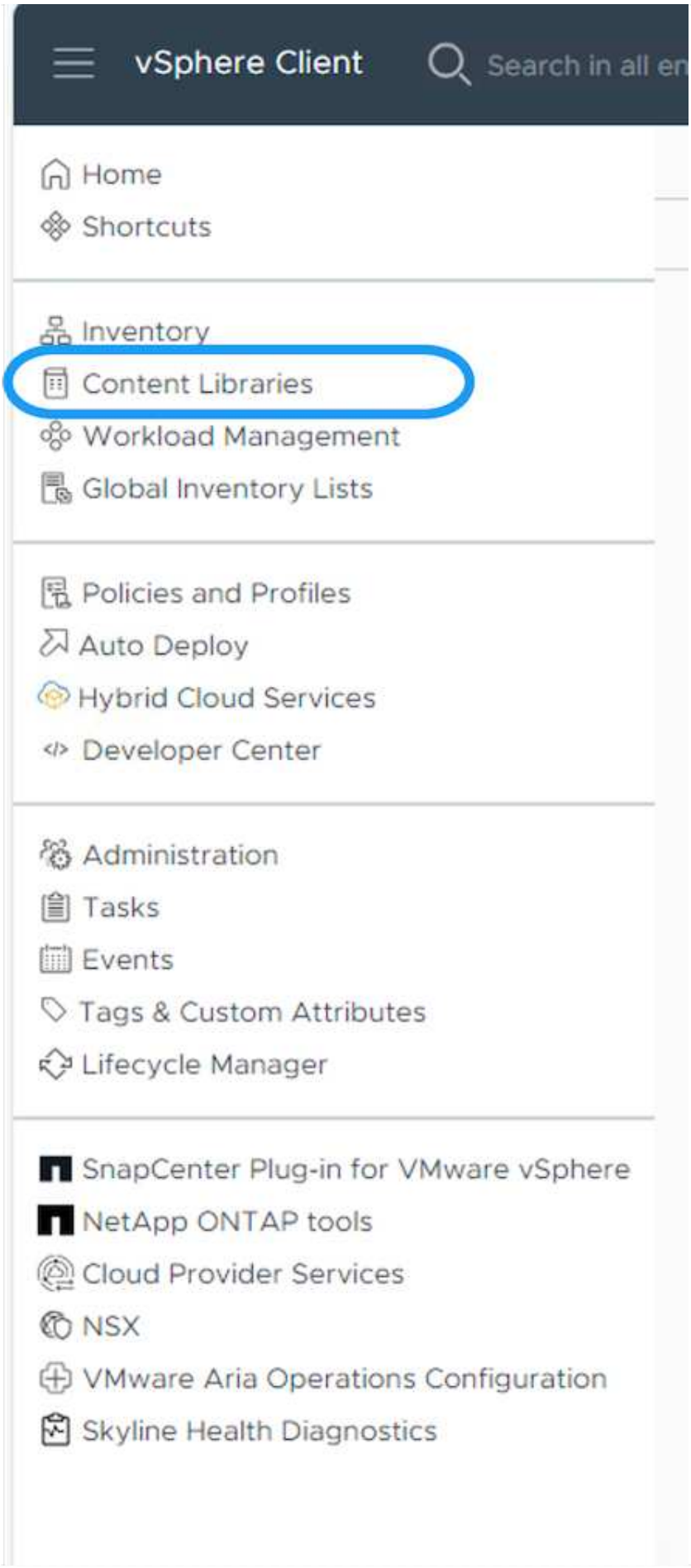
1. In vSphere Web Client, fare clic con il pulsante destro del mouse sul modello VM nella vista della cartella VM e modelli e selezionare l'opzione per la conversione in VM.



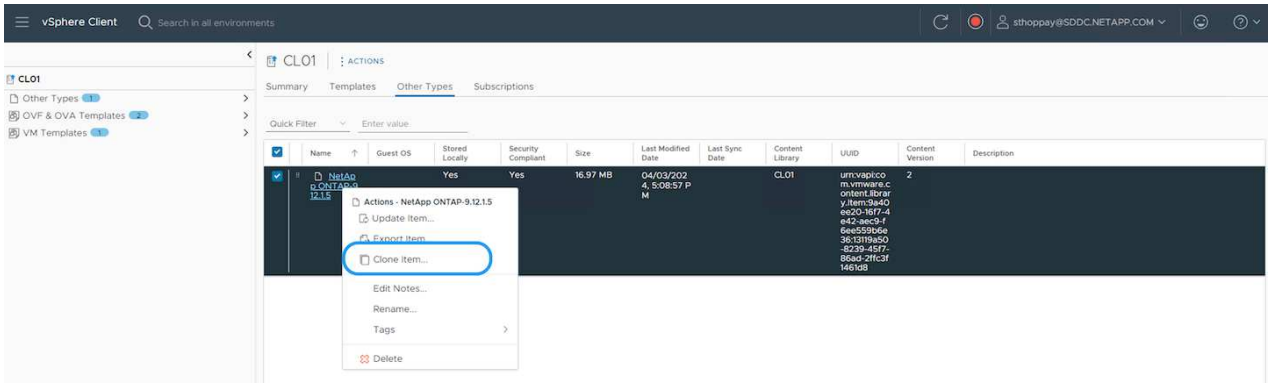
2. Una volta convertito come VM, segui le opzioni di migrazione delle VM.

Clone degli elementi della libreria dei contenuti

1. In vSphere Web Client, selezionare Librerie di contenuti

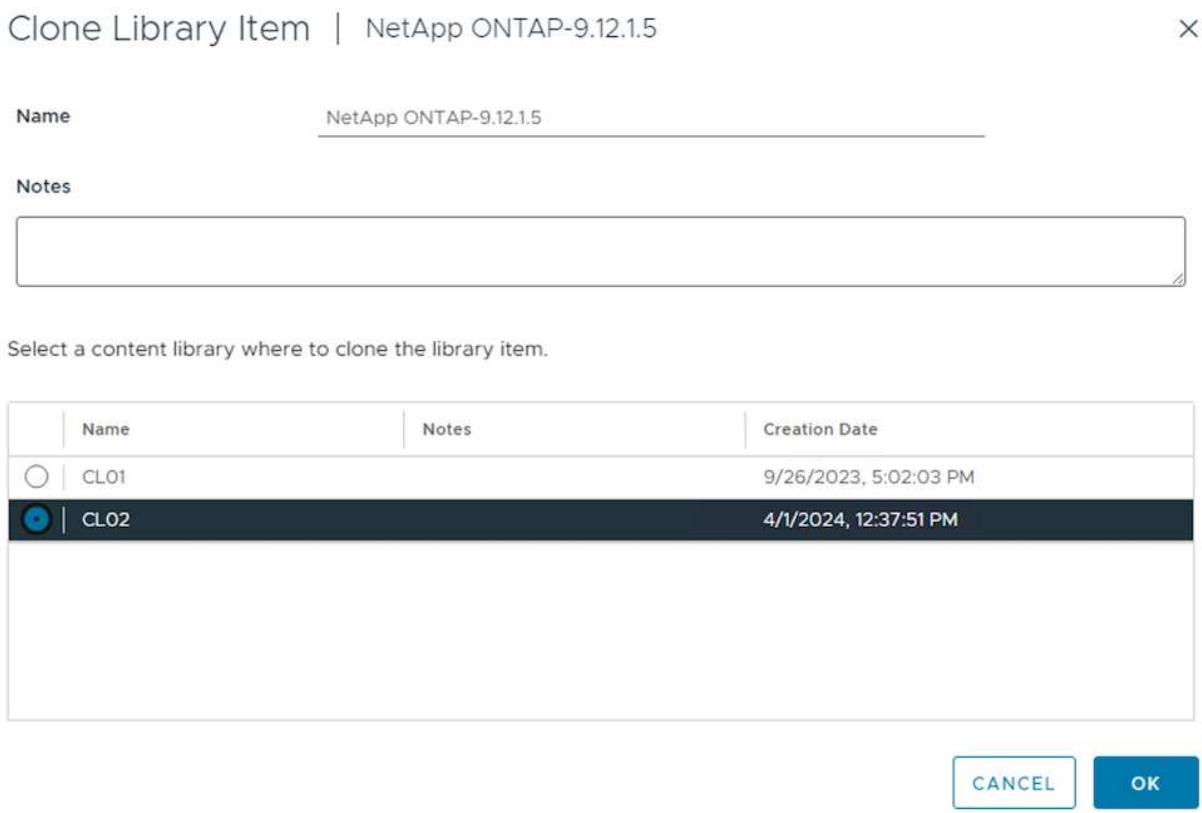

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. Selezionare la libreria di contenuti in cui si desidera clonare l'elemento
3. Fare clic con il pulsante destro del mouse sull'elemento e fare clic su Clona elemento ..

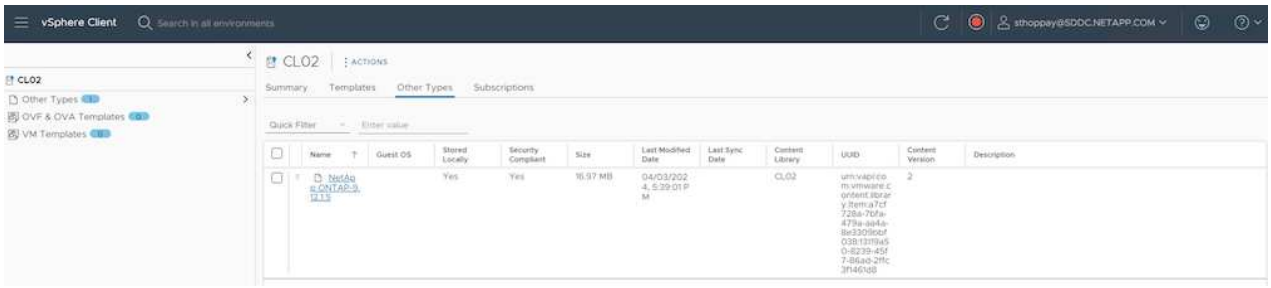


> Se si utilizza il menu azione, assicurarsi che sia elencato l'oggetto di destinazione corretto per eseguire l'azione.

4. Selezionare la libreria di contenuti di destinazione e fare clic su OK.



5. Verificare che l'elemento sia disponibile nella libreria di contenuti di destinazione.

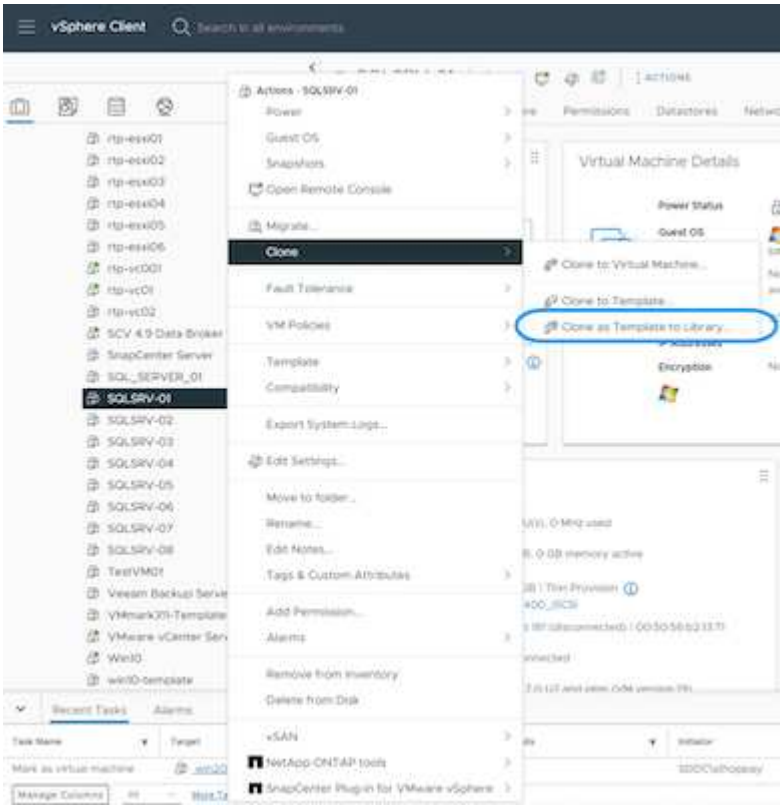


Di seguito è riportato lo script PowerCLI di esempio per copiare gli elementi della libreria dei contenuti da CL01 a CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

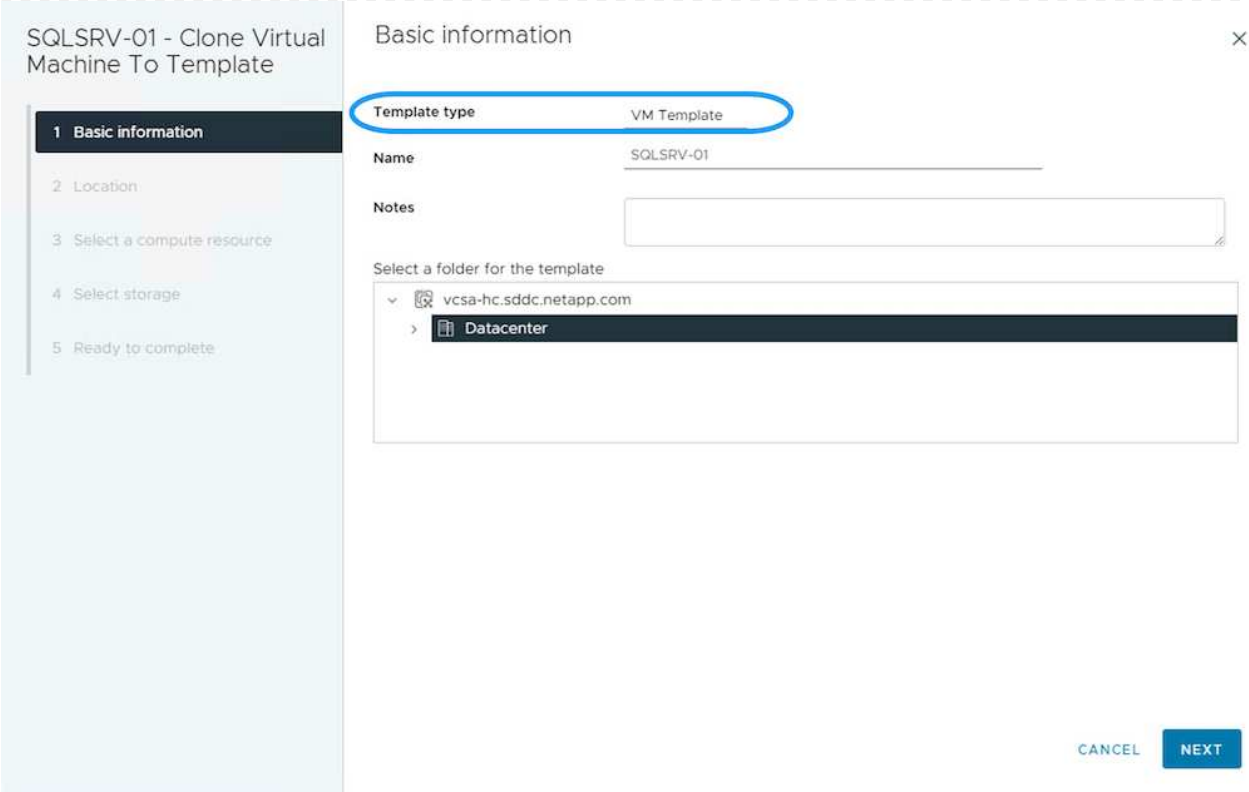
Aggiunta di VM come modelli nella Libreria dei contenuti

1. In vSphere Web Client, selezionare la VM e fare clic con il pulsante destro del mouse per scegliere Clone as Template (Clona come modello) in Library (Libreria)



Quando il modello VM è selezionato per clonare in libary, può essere memorizzato solo come modello OVF e OVA e non come modello VM.

2. Confermare che il tipo di modello sia selezionato come modello VM e seguire la procedura guidata per completare l'operazione.



Per ulteriori dettagli sui modelli VM nella libreria di contenuti, consulta "Guida all'amministrazione di vSphere VM"

Casi di utilizzo

Migrazione dai sistemi storage di terze parti (incluso vSAN) ai datastore ONTAP.

- In base alla posizione di provisioning del datastore ONTAP, scegli le opzioni di migrazione delle macchine virtuali da sopra.

Migrazione dalla versione precedente alla versione più recente di vSphere.

- Se non è possibile eseguire l'aggiornamento sul posto, è possibile creare un nuovo ambiente e utilizzare le opzioni di migrazione riportate sopra.

Nell'opzione di migrazione Cross vCenter, importare da destinazione se l'opzione di esportazione non è disponibile sull'origine. Per questa procedura, controllare "Importazione o clonazione di una macchina virtuale con Advanced Cross vCenter vMotion"

Migrazione al dominio del carico di lavoro VCF.

- Migra le macchine virtuali da ciascun cluster vSphere al dominio del carico di lavoro di destinazione.

> Per consentire la comunicazione di rete con le VM esistenti su altri cluster su vCenter di origine, estendere il segmento NSX aggiungendo gli host vcenter vSphere di origine alla zona di trasporto o utilizzare L2 bridge su edge per consentire la comunicazione L2 in VLAN. Controllare la documentazione NSX di "Configurare una macchina virtuale Edge per il bridging"

Risorse aggiuntive

- "Migrazione delle macchine virtuali vSphere"
- "Novità di vSphere 8 per vMotion"
- "Risorse vSphere vMotion"
- "Configurazioni di gateway di livello 0 in NSX Federation"
- "Manuale dell'utente di HCX 4,8"
- "Documentazione di VMware Site Recovery Manager"
- "Disaster recovery di BlueXP per VMware"

Migra le macchine virtuali su Amazon EC2 con FSxN

Migrazione delle macchine virtuali ad Amazon EC2 con FSxN: Panoramica

Le organizzazioni stanno accelerando le migrazioni verso soluzioni di cloud computing su AWS, sfruttando servizi come le istanze di Amazon Elastic Compute Cloud (Amazon EC2) e Amazon FSX per NetApp ONTAP (FSX per ONTAP) per modernizzare la propria infrastruttura IT, ottenere risparmi sui costi e migliorare l'efficienza delle operazioni. Queste offerte AWS consentono migrazioni che ottimizzano il total cost of ownership (TCO) attraverso modelli di prezzo basati sul consumo e funzionalità per lo storage Enterprise, fornendo la flessibilità e la scalabilità necessarie per soddisfare le esigenze di business globali in evoluzione.

Panoramica

Per le aziende profondamente investite in VMware vSphere, la migrazione ad AWS è un'opzione conveniente, date le attuali condizioni di mercato, che rappresenta un'opportunità unica.

Mentre queste organizzazioni passano ad AWS, cercano di capitalizzare sull'agilità e i benefici economici del cloud, preservando al tempo stesso set di funzionalità familiari, in particolare per quanto riguarda lo storage. Mantenere una perfetta operatività con protocolli di storage familiari, in particolare iSCSI, processi, strumenti e competenze è fondamentale per la migrazione dei carichi di lavoro o la configurazione di soluzioni di disaster recovery.

Utilizzando il servizio di storage gestito AWS FSX per ONTAP per preservare le funzionalità dello storage Enterprise, che troppo venendo da qualsiasi storage di vendor di terze parti on-premise, le aziende possono sbloccare la potenza di AWS, riducendo al minimo l'interruzione e massimizzando i loro investimenti futuri.

Questo report tecnico spiega come migrare le macchine virtuali VMware vSphere on-premise in un'istanza di Amazon EC2 con dischi dati posizionati in FSX per le LUN iSCSI ONTAP utilizzando la funzionalità "data-mobility-as-code" di Cirrus Migrate Cloud (CMC) di MigrateOps.

Requisiti della soluzione

I clienti VMware stanno cercando di risolvere una serie di sfide. Queste organizzazioni vogliono:

1. Sfruttare le funzionalità dello storage Enterprise, come thin provisioning, tecnologie per l'efficienza dello storage, cloni a impatto zero, backup integrati, replica a livello di blocco, e tiering. Questo aiuta a ottimizzare le attività di migrazione e l'implementazione a prova di futuro su AWS a partire dal giorno 1.
2. Ottimizza le implementazioni dello storage su AWS che utilizzano le istanze di Amazon EC2 integrando FSX per ONTAP e le funzionalità di ottimizzazione dei costi che offre.
3. Ridurre il total cost of ownership (TCO) legato all'utilizzo di istanze Amazon EC2 con soluzioni di storage a blocchi dimensionando in modo corretto le istanze di Amazon EC2 per soddisfare i parametri di IOPS e throughput richiesti. Con lo storage a blocchi, le operazioni su disco Amazon EC2 limitano la larghezza di banda e i tassi di i/O. Il file storage con FSX per ONTAP sfrutta la larghezza di banda della rete. In altre parole, FSX per ONTAP non ha limiti di i/o a livello di VM.

Panoramica dei componenti tecnici

Concetti di FSX per ONTAP

Amazon FSX per NetApp ONTAP è un servizio di storage AWS completamente gestito che fornisce i file system NetApp® ONTAP® con tutte le note funzioni di gestione dei dati ONTAP, le prestazioni e le API su AWS. Il suo storage dalle performance elevate supporta diversi protocolli (NFS, SMB, iSCSI), offrendo un singolo servizio per i carichi di lavoro che utilizzano le istanze Windows, Linux e macOS EC2.

Poiché FSX for ONTAP è un file system ONTAP, offre una serie di funzionalità e servizi NetApp familiari, tra cui la tecnologia di replica dei dati SnapMirror®, i thin clone e le copie NetApp Snapshot™. Sfruttando un Tier di capacità a basso costo tramite tiering dei dati, FSX per ONTAP è flessibile e può raggiungere una scalabilità virtualmente illimitata. Inoltre, grazie alla tecnologia per l'efficienza dello storage NetApp, permette di ridurre ulteriormente i costi relativi allo storage su AWS. Per ulteriori informazioni, vedere "Introduzione ad Amazon FSX per ONTAP".

File System

La risorsa centrale di FSX per ONTAP è il suo file system basato sullo storage su dischi a stato solido (SSD). Durante il provisioning di un file system FSX per ONTAP, l'utente inserisce una velocità di throughput e una capacità di storage desiderate e seleziona un VPC Amazon in cui si troverà il file system.

Gli utenti possono anche scegliere tra due modelli di distribuzione integrati ad alta disponibilità per il file system: Implementazione di Multi-Availability zone (AZ) o di una singola AZ. Ciascuna di queste opzioni offre il proprio livello di durata e disponibilità, che i clienti possono scegliere in base ai requisiti di business continuity del caso d'utilizzo. Le implementazioni multi-AZ sono costituite da nodi doppi che si replicano senza problemi tra due AZS. L'opzione di distribuzione single-AZ più conveniente struttura il file system in due nodi divisi tra due domini di errore separati che risiedono entrambi all'interno di una singola AZ.
Macchine virtuali di storage
Ai dati nel file system FSX per ONTAP si accede tramite una partizione storage logica chiamata Storage Virtual Machine (SVM). Una SVM è in realtà un suo file server dotato di propri data e access point amministrativi. Quando si accede alle LUN iSCSI su un file system FSX per ONTAP, l'istanza di Amazon EC2 si interfaccia direttamente con la SVM utilizzando l'indirizzo IP dell'endpoint iSCSI della SVM.

Anche se è possibile mantenere una singola SVM in un cluster, è possibile eseguire diverse SVM in un cluster

solo in svariati utilizzi e benefici. I clienti sono in grado di determinare il numero ottimale di SVM da configurare tenendo in considerazione le esigenze aziendali, compresi i requisiti per l'isolamento del workload.

Volumi

I dati all'interno di una SVM di FSX per ONTAP vengono memorizzati e organizzati in strutture note come volumi, che agiscono come container virtuali. Un singolo volume può essere configurato con uno o più LUN. I dati memorizzati in ciascun volume consumano la capacità di archiviazione nel file system. Tuttavia, poiché FSX per ONTAP esegue il thin provisioning del volume, il volume occupa solo la capacità di storage per la quantità di dati che vengono memorizzati.

Il concetto di Cirrus Migrate Cloud MigrateOps

CMC è un'offerta Software-as-a-Service (SaaS) traducibile di Cirrus Data Solutions, Inc. Disponibile tramite AWS Marketplace. MigrateOps è una funzionalità di automazione Data-Mobility-as-Code di CMC che consente di gestire in modo dichiarativo le operazioni di mobilità dei dati su larga scala utilizzando semplici configurazioni delle operazioni in YAML. Una configurazione MigrateOps determina il modo in cui eseguire le attività di mobilità dei dati. Per ulteriori informazioni su MigrateOps, consulta "Informazioni su MigrateOps".

MigrateOps adotta un approccio incentrato sull'automazione, costruito ad hoc per ottimizzare l'intero processo, garantendo la mobilità dei dati Enterprise cloud-scale senza interruzioni operative. Oltre alle funzionalità già ricche di funzionalità offerte da CMC per l'automazione, MigrateOps aggiunge altre automazioni spesso gestite esternamente, come:

- Correzione del sistema operativo
- Cutover delle applicazioni e pianificazione dell'approvazione
- Migrazione del cluster senza downtime
- Integrazione della piattaforma cloud pubblico/privato
- Integrazione della piattaforma di virtualizzazione
- Integrazione della gestione dello storage aziendale
- Configurazione SAN (iSCSI)

Con le attività sopra elencate completamente automatizzate, tutti i noiosi passaggi necessari per la preparazione della macchina virtuale on-premise di origine (ad esempio l'aggiunta di agenti e strumenti AWS), la creazione di LUN FSX di destinazione, la configurazione di iSCSI e multipath/MPIO nell'istanza di destinazione AWS, inoltre, tutte le attività di arresto/avvio dei servizi dell'applicazione vengono eliminate specificando semplicemente i parametri in un file YAML.

FSX per ONTAP viene utilizzato per fornire le LUN di dati e dimensionare correttamente il tipo di istanza di Amazon EC2, fornendo tutte le funzionalità che le organizzazioni avevano in precedenza nei propri ambienti on-premise. La funzionalità MigrateOps di CMC verrà utilizzata per automatizzare tutti i passaggi coinvolti, incluso il provisioning di LUN iSCSI mappati, trasformando questo processo in un'operazione dichiarativa e prevedibile.

Nota: CMC richiede l'installazione di un agente molto sottile sulle istanze della macchina virtuale di origine e di destinazione per garantire il trasferimento sicuro dei dati dall'archiviazione di origine in FSX per ONTAP.

Vantaggi dell'utilizzo di Amazon FSX per NetApp ONTAP con EC2 istanze

Lo storage FSX per ONTAP per le istanze di Amazon EC2 offre diversi vantaggi:

- Throughput elevato e storage a bassa latenza che offrono performance costantemente elevate per i carichi

di lavoro più esigenti

- Il caching intelligente NVMe migliora le performance
- Capacità, throughput e IOPS regolabili possono essere modificati in tempo reale e si adattano rapidamente alle esigenze di storage in continua evoluzione
- Replica dei dati a blocchi dallo storage ONTAP on-premise ad AWS
- Accessibilità multiprotocollo come ad esempio iSCSI, ampiamente utilizzata nelle implementazioni VMware on-premise
- La tecnologia NetApp Snapshot™ e il DR orchestrati da SnapMirror impediscono la perdita di dati e accelerano il ripristino
- Funzionalità di efficienza dello storage per ridurre l'impatto e i costi dello storage, compresi thin provisioning, deduplica dei dati, compressione e compaction
- La replica efficiente riduce il tempo necessario per creare i backup da ore a pochi minuti, ottimizzando l'RTO
- Opzioni granulari per il backup e il ripristino dei file con NetApp SnapCenter®

L'implementazione delle istanze di Amazon EC2 con FSX ONTAP come layer di storage basato su iSCSI offre performance elevate, funzionalità di gestione dei dati mission-critical e funzionalità di efficienza dello storage per la riduzione dei costi che possono trasformare la tua implementazione su AWS.

Usando Flash cache, diverse sessioni iSCSI e sfruttando una dimensione del set di lavoro del 5%, FSX per ONTAP offre IOPS pari a circa 350K, fornendo livelli di performance per soddisfare anche i workload più esigenti.

Poiché in FSX per ONTAP vengono applicati solo i limiti della larghezza di banda dello storage a blocchi, gli utenti possono sfruttare piccoli tipi di istanze di Amazon EC2 e ottenere gli stessi tassi di performance di tipi di istanze più grandi. L'utilizzo di tali piccoli tipi di istanze mantiene bassi i costi di calcolo, ottimizzando il TCO.

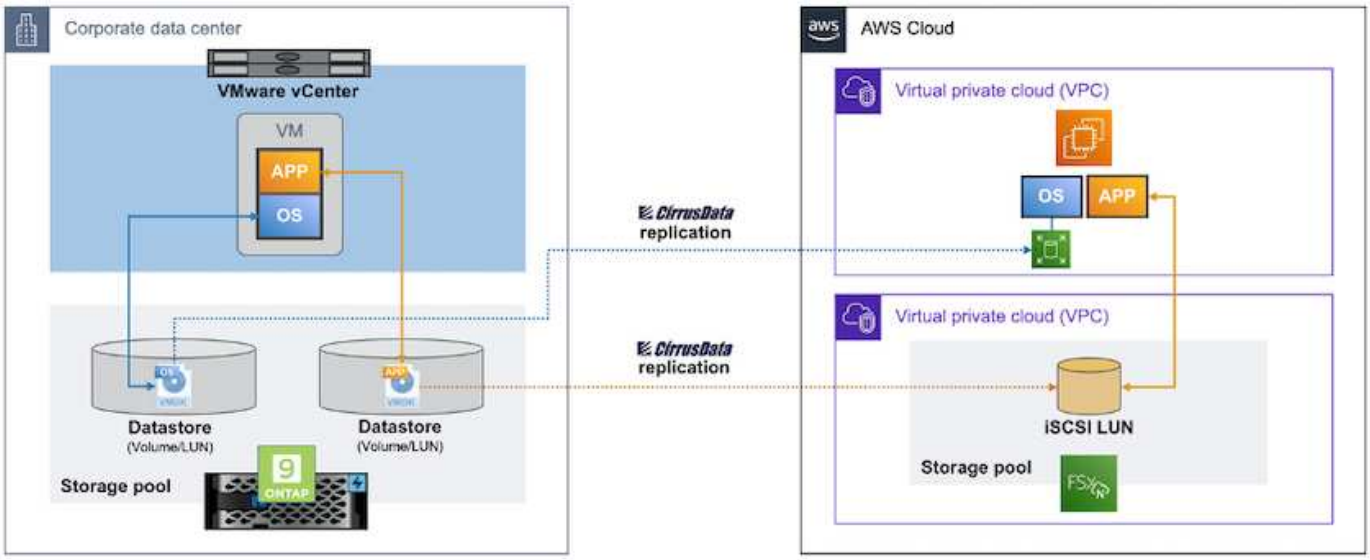
La possibilità di FSX per ONTAP di distribuire più protocolli è un altro vantaggio che consente di standardizzare un singolo servizio storage AWS per un'ampia gamma di requisiti esistenti di dati e file service. Per le aziende profondamente investite in VMware vSphere, la migrazione ad AWS è un'opzione conveniente, date le attuali condizioni di mercato, che rappresenta un'opportunità unica.

Eseguire la migrazione delle macchine virtuali ad Amazon EC2 utilizzando FSxN: Architettura e prerequisiti

Questo articolo illustra l'architettura di alto livello e i prerequisiti per la distribuzione per il completamento della migrazione.

Architettura di alto livello

Il diagramma seguente illustra l'architettura di alto livello della migrazione dei dati VMDK (Virtual Machine Disk) su VMware ad AWS mediante CMC MigrateOps:



Come migrare le macchine virtuali VMware in AWS con Amazon EC2 e FSX per ONTAP iSCSI

Prerequisiti

Prima di iniziare la procedura dettagliata, verificare che siano soddisfatti i seguenti prerequisiti:

Su AWS

- Un account AWS. Sono incluse le autorizzazioni per le subnet, l'installazione di VPC, le tabelle di routing, la migrazione delle regole di protezione, i gruppi di protezione, e altri requisiti per il networking, ad esempio il bilanciamento del carico. Come per qualsiasi migrazione, la maggior parte dello sforzo e della considerazione dovrebbe andare in rete.
- Ruoli IAM appropriati che consentono di eseguire il provisioning di istanze di FSX per ONTAP e Amazon EC2.
- Le tabelle di instradamento e i gruppi di sicurezza possono comunicare con FSX per ONTAP.
- Aggiungi una regola in entrata al gruppo di sicurezza appropriato (vedi sotto per ulteriori dettagli) per consentire un trasferimento sicuro dei dati dal data center on-premise ad AWS.
- Un DNS valido in grado di risolvere i nomi di dominio Internet pubblici.
- Verificare che la risoluzione DNS funzioni e consenta di risolvere i nomi host.
- Per performance ottimali e il dimensionamento corretto, utilizza i dati relativi alle performance dell'ambiente di origine per dimensionare correttamente lo storage FSX per ONTAP.
- Ogni sessione MigrateOps utilizza un EIP, pertanto la quota per EIP dovrebbe essere aumentata per ottenere più parallelismo. Tenere presente che la quota EIP predefinita è 5.
- (In caso di migrazione di carichi di lavoro basati su Active Directory) Un dominio Active Directory di Windows su Amazon EC2.

Per Cirrus Migrate Cloud

- Un account Cirrus Data Cloud all'indirizzo "cloud.cirrusdata.com" Deve essere creato prima di utilizzare CMC. È necessario consentire la comunicazione in uscita con CDN, endpoint Cirrus Data e archivio software tramite HTTPS.
- Consente la comunicazione (in uscita) con i servizi Cirrus Data Cloud tramite il protocollo HTTPS (porta 443).

- Affinché un host possa essere gestito dal progetto CMC, il software CMC distribuito deve avviare una connessione TCP in uscita unidirezionale a Cirrus Data Cloud.
- Consente l'accesso al protocollo TCP, porta 443, a portal-gateway.cloud.cirrusdata.com, che è attualmente a 208.67.222.222.
- Consente richieste HTTP POST (tramite connessione HTTPS) con payload di dati binari (application/octet-stream). Questo è simile a un caricamento di file.
- Assicurarsi che portal-gateway.cloud.cirrusdata.com sia risolvibile dal DNS (o tramite il file host del sistema operativo).
- Se si dispone di rigide regole per proibire alle istanze del prodotto di effettuare connessioni in uscita, è possibile utilizzare la funzione "Management Relay" di CMC, dove la connessione 443 in uscita proviene da un singolo host non in produzione protetto.

Nota: Nessun dato di archiviazione viene mai inviato all'endpoint Cirrus Data Cloud. Vengono inviati solo i metadati di gestione, con possibilità di masking dei dati in modo che non siano inclusi nome host, nome volume e IP di rete reali.

Per migrare i dati dai repository di storage on-premise ad AWS, MigrateOps automatizza la gestione di una connessione H2H (host-to-host). Si tratta di connessioni di rete ottimizzate, unidirezionali e basate su TCP, utilizzate da CMC per facilitare la migrazione remota. Questo processo offre compressione e crittografia always-on che possono ridurre la quantità di traffico fino a otto volte, a seconda della natura dei dati.

Nota: CMC è progettato in modo che nessun dato di produzione/i/o lasci la rete di produzione durante l'intera fase di migrazione. Di conseguenza, è necessaria una connettività diretta tra l'host di origine e di destinazione.

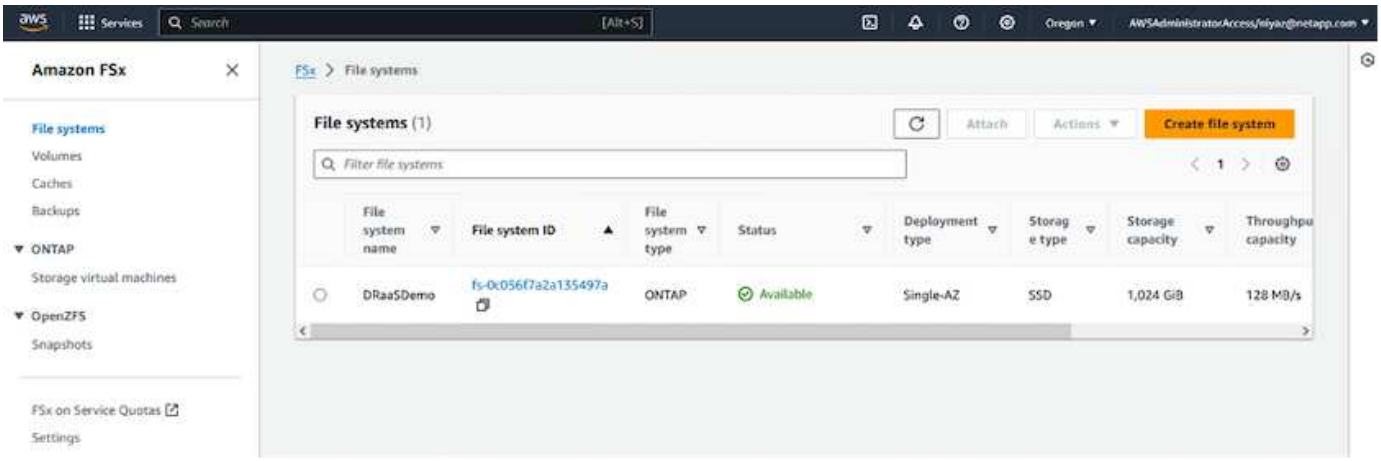
Migra le macchine virtuali su Amazon EC2 con FSxN: Deployment Guide

In questo articolo viene descritta la procedura di distribuzione di queste soluzioni di migrazione.

Configurare FSX per ONTAP e dati Cirrus per le operazioni di migrazione

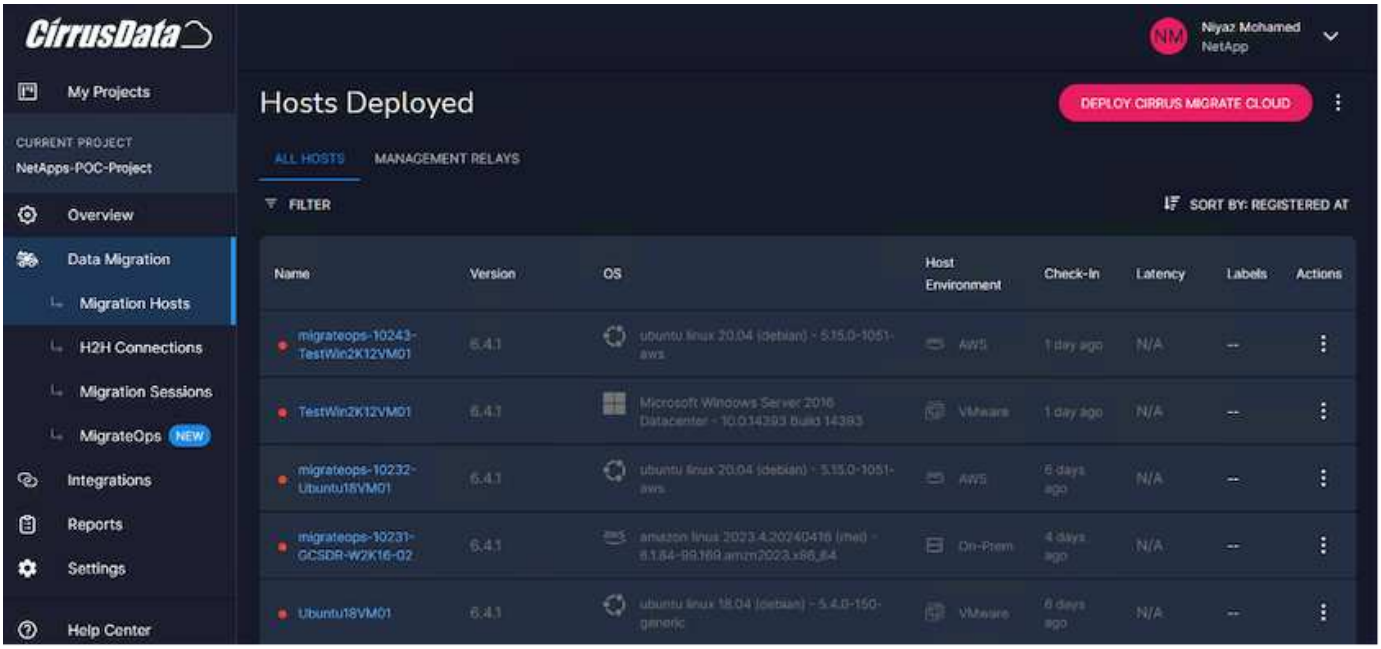
Questo "guida dettagliata all'implementazione" Mostra come aggiungere un volume FSX per ONTAP a un VPC. Poiché questi passaggi sono di natura sequenziale, assicurarsi che siano trattati in ordine.

Ai fini di questa dimostrazione, "DRaaSDemo" è il nome del file system creato.



Una volta configurato il VPC AWS e eseguito il provisioning di FSX per ONTAP in base ai tuoi requisiti di performance, effettua l'accesso a. "cloud.cirrusdata.com" e. "creare un nuovo progetto" o accedere a un

progetto esistente.



Prima di creare la ricetta per MigrazionOps, è necessario aggiungere AWS Cloud come integrazione. CMC offre integrazione integrata con FSX per ONTAP e AWS. L'integrazione di FSX per ONTAP offre le seguenti funzionalità automatizzate:

Prepara il file system FSX for ONTAP:

- Creare nuovi volumi e LUN che corrispondano ai volumi di origine

Nota: Un disco di destinazione nel modello FSX per ONTAP FS è un "LUN" creato su un "volume" che ha capacità sufficiente per contenere il LUN più una quantità ragionevole di overhead per facilitare snapshot e metadati. L'automazione CMC si occupa di tutti questi dettagli per creare il volume appropriato e il LUN con parametri opzionali definiti dall'utente.

- Creare un'entità host (denominata iGroup in FSX) con IQN iniziatore host
- Mappare i volumi appena creati alle entità host appropriate utilizzando le mappature
- Creare tutte le altre configurazioni necessarie

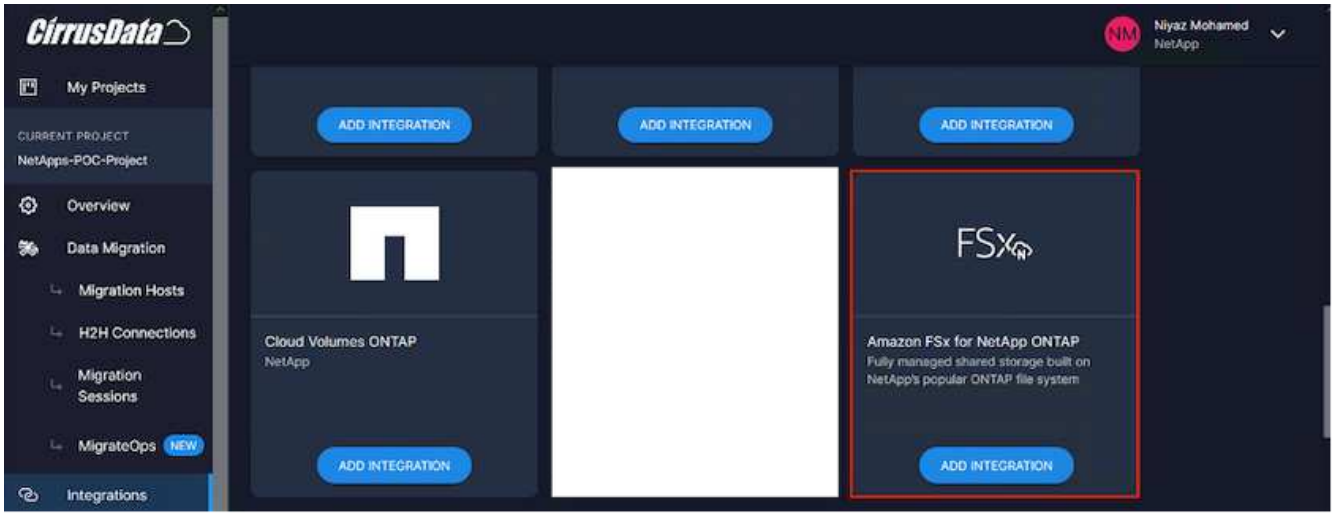
Preparare l'host di produzione per la connessione iSCSI:

- Se necessario, installare e configurare la funzione iSCSI e impostare l'iniziatore.
- Se necessario, installare e configurare Multipath (MPIO per Windows) con gli identificatori del fornitore appropriati.
- Se necessario, modificare le impostazioni di sistema in base alle Best practice del fornitore, ad esempio con le impostazioni udev su Linux.
- Creare e gestire connessioni iSCSI come le destinazioni iSCSI permanenti/preferite in Windows.

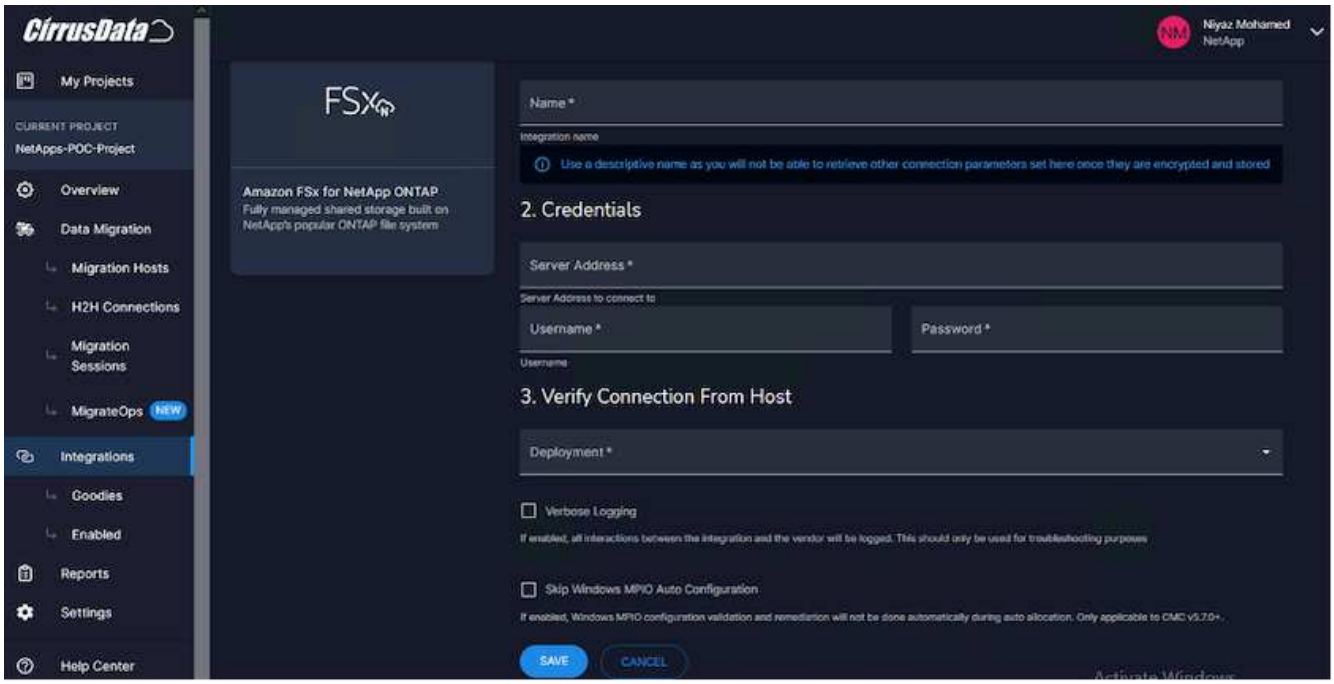
Per configurare l'integrazione CMC per FSX per ONTAP e AWS, attenersi alla seguente procedura:

1. Accedere al portale Cirrus Data Cloud.
2. Passare al progetto per il quale si desidera abilitare l'integrazione.

3. Vai a integrazioni → Goodies.
4. Scorri fino a trovare FSX per NetApp ONTAP e fai clic su AGGIUNGI INTEGRAZIONE.



5. Fornire un nome descrittivo (esclusivamente a scopo di visualizzazione) e aggiungere le credenziali appropriate.



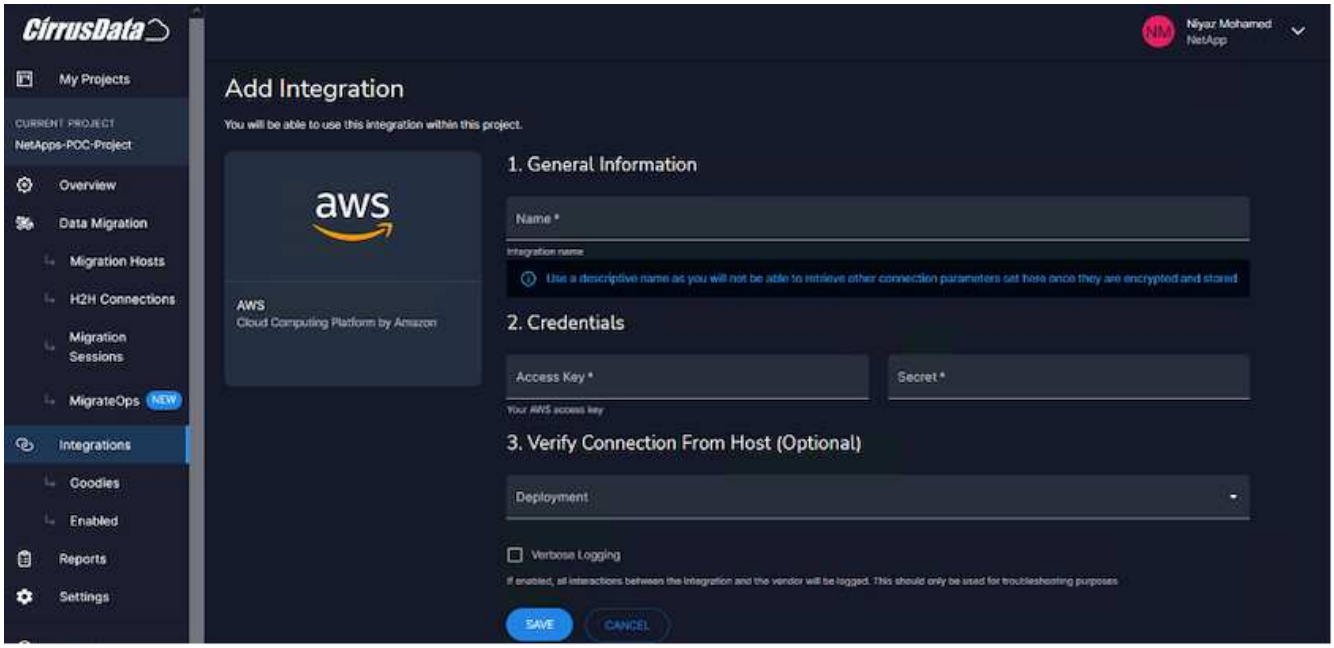
6. Una volta creata l'integrazione, durante la creazione di una nuova sessione di migrazione, selezionare Auto allocate Destination Volumes (allocazione automatica volumi di destinazione) per allocare automaticamente nuovi volumi in FSX for ONTAP.

   Nota: I nuovi LUN verranno creati con le stesse dimensioni del volume di origine, a meno che non sia attivata l'opzione "migrazione a volumi più piccoli" per la migrazione.

   Nota: Se un'entità host (iGroup) non esiste già, ne verrà creata una nuova. Tutti gli IQN iniziatori iSCSI host verranno aggiunti alla nuova entità host.

   Nota: Se esiste già un'entità host esistente con uno degli iniziatori iSCSI, verrà riutilizzata.

7. Al termine, aggiungere l'integrazione per AWS, seguendo le istruzioni visualizzate sullo schermo.



Nota: Questa integrazione viene utilizzata durante la migrazione delle macchine virtuali dallo storage on-premise ad AWS insieme all'integrazione di FSX per ONTAP.

Nota: Utilizzare i relè di gestione per comunicare con Cirrus Data Cloud se non è presente una connessione diretta in uscita per le istanze di produzione da migrare.

Con l'aggiunta delle integrazioni, è il momento di registrare gli host con il progetto. Affrontiamo questo con uno scenario di esempio.

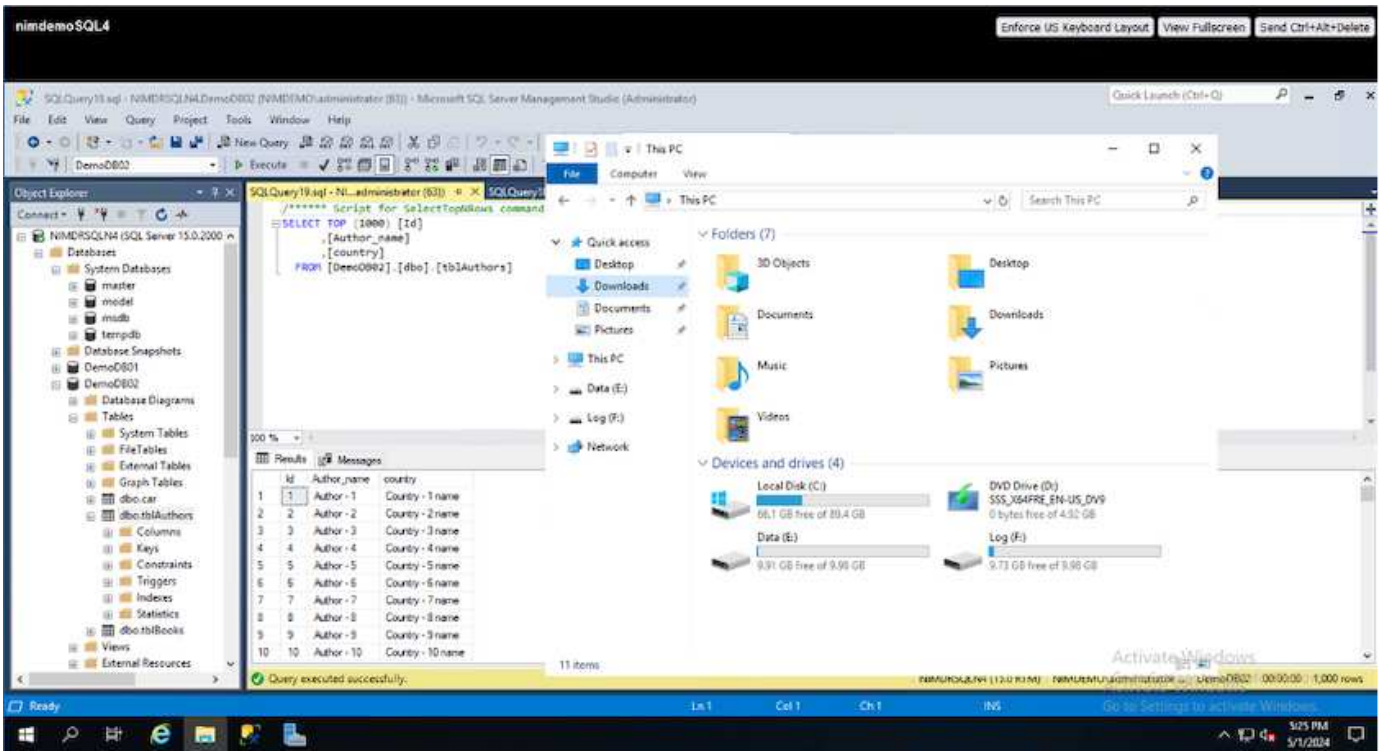
Scenario di registrazione host

VM VMware guest che risiedono in vCenter nel data center on-premise:

- Windows 2016 in esecuzione con SQL Server con tre VMDK, inclusi il sistema operativo e i dischi dati. Sta eseguendo un database attivo. Il database si trova in un volume di dati supportato da due VMDK.

Nota: Poiché l'origine è un ambiente VMware e vengono utilizzati VMDK, il software iSCSI Initiator di Windows non è attualmente configurato su questa VM guest. Per connettersi allo storage di destinazione tramite iSCSI, è necessario installare e configurare sia iSCSI che MPIO. L'integrazione di Cirrus Data Cloud eseguirà questa installazione automaticamente durante il processo.

Nota: L'integrazione configurata nella sezione precedente automatizza la configurazione del nuovo storage di destinazione nella creazione dei nuovi dischi, nella configurazione delle entità host e dei relativi IQN e perfino nella correzione della VM dell'applicazione (host) per le configurazioni iSCSI e multipath.



Questa dimostrazione migrerà i VMDK delle applicazioni da ciascuna macchina virtuale a un volume iSCSI con provisioning e mappatura automatici da FSX per ONTAP. In questo caso, il VMDK del sistema operativo verrà migrato su un volume Amazon EBS, dal momento che le istanze di Amazon EC2 supportano questo Amazon EBS solo come disco di avvio.

Nota: Il fattore di scala con questo approccio di migrazione è la larghezza di banda della rete e il tubo che collega on-premise ad AWS VPC. Poiché ciascuna VM ha configurato 1:1 sessione host, le prestazioni complessive della migrazione dipendono da due fattori:

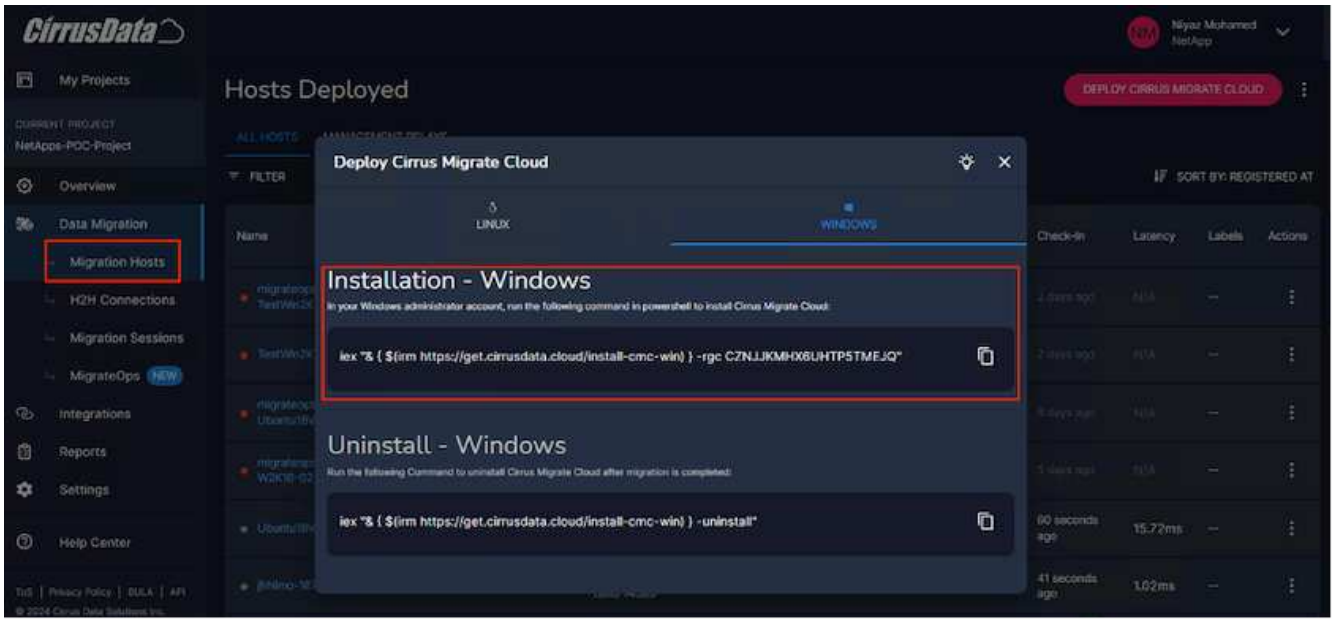
- Larghezza di banda della rete
- Tipo di istanza di destinazione e larghezza di banda ENI

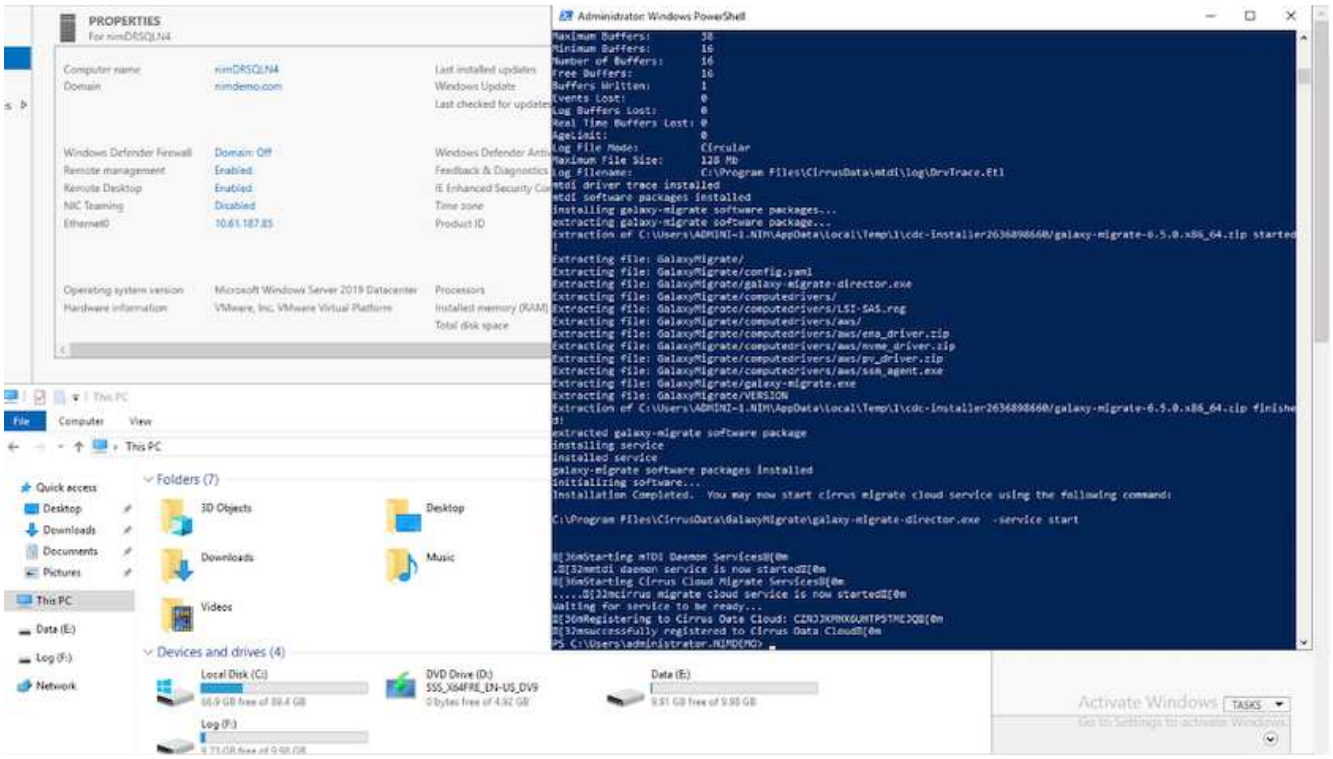
Le fasi di migrazione sono le seguenti:

1. Installare l'agente CMC su ogni host (Windows e Linux) designato per la fase di migrazione. Questa operazione può essere eseguita eseguendo un comando di installazione a una riga.

   A tale scopo, accedere a migrazione dei dati > host di migrazione > fare clic su "Deploy Cirrus Migrate Cloud" e selezionare "Windows".

   Quindi, copiare `iex` All'host ed eseguirlo usando PowerShell. Una volta completata la distribuzione dell'agente, l'host viene aggiunto al progetto in "host di migrazione".





2. Preparare il codice YAML per ogni macchina virtuale.

   Nota: È fondamentale disporre di un YAML per ogni VM che specifichi la ricetta o il piano necessari per l'attività di migrazione.

   YAML fornisce il nome dell'operazione, le note (descrizione) insieme al nome della ricetta come `MIGRATEOPS_AWS_COMPUTE`, il nome host (`system_name`) e il nome dell'integrazione (`integration_name`) e la configurazione di origine e destinazione. È possibile specificare script personalizzati come azione prima e dopo il cutover.

```
operations:
    -   name: Win2016 SQL server to AWS
```

```
        notes: Migrate OS to AWS with EBS and Data to FSx for ONTAP
        recipe: MIGRATEOPS_AWS_COMPUTE
        config:
            system_name: Win2016-123
            integration_name: NimAWShybrid
            migrateops_aws_compute:
                region: us-west-2
                compute:
                    instance_type: t3.medium
                    availability_zone: us-west-2b
                network:
                    vpc_id: vpc-05596abe79cb653b7
                    subnet_id: subnet-070aeb9d6b1b804dd
                    security_group_names:
                        - default
                destination:
                    default_volume_params:
                        volume_type: GP2
                    iscsi_data_storage:
                        integration_name: DemoDRaaS
                        default_volume_params:
                            netapp:
                                qos_policy_name: ""
                migration:
                    session_description: Migrate OS to AWS with EBS and
Data to FSx for ONTAP
                    qos_level: MODERATE
                cutover:
                    stop_applications:
                        - os_shell:
                              script:
                                  - stop-service -name 'MSSQLSERVER'
-Force
                                  - Start-Sleep -Seconds 5
                                  - Set-Service -Name 'MSSQLSERVER'
-StartupType Disabled
                                  - write-output "SQL service stopped
and disabled"

                        - storage_unmount:
                              mountpoint: e
                        - storage_unmount:
                              mountpoint: f
                    after_cutover:
                        - os_shell:
                              script:
```

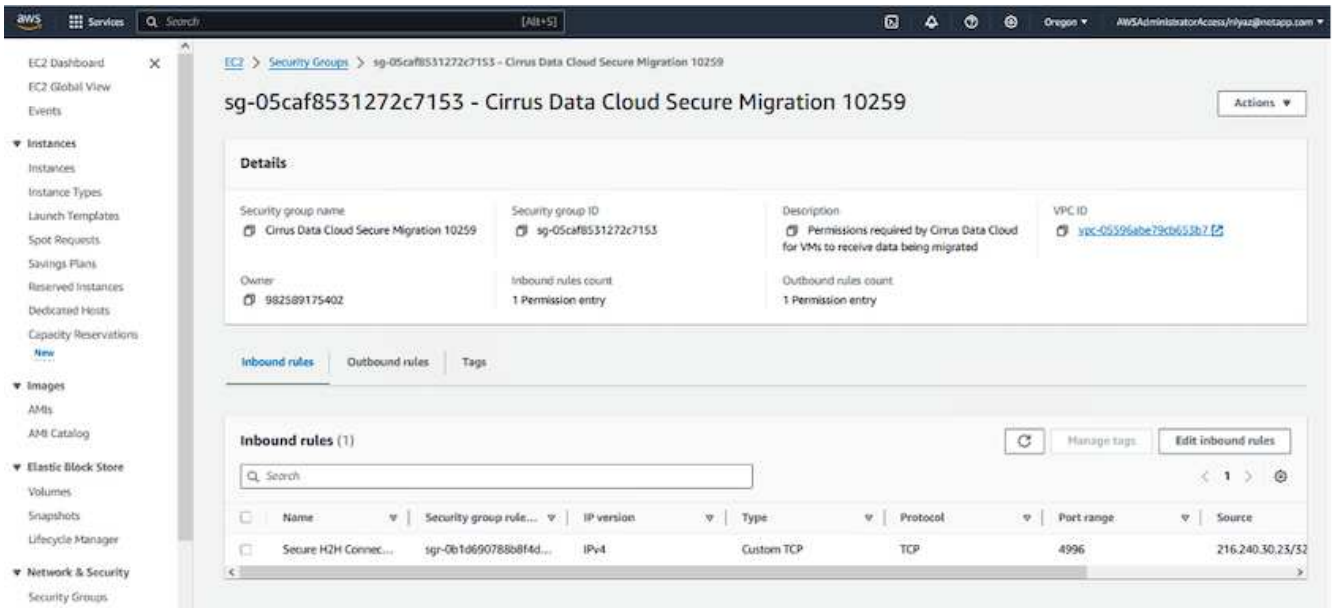
```
                                    - stop-service -name 'MSSQLSERVER'
-Force
                                    - write-output "Waiting 90 seconds to
mount disks..." > log.txt
                                    - Start-Sleep -Seconds 90
                                    - write-output "Now re-mounting disks
E and F for SQL..." >>log.txt
                        - storage_unmount:
                              mountpoint: e
                        - storage_unmount:
                              mountpoint: f
                        - storage_mount_all: {}
                        - os_shell:
                              script:
                                    - write-output "Waiting 60 seconds to
restart SQL Services..." >>log.txt
                                    - Start-Sleep -Seconds 60
                                    - stop-service -name 'MSSQLSERVER'
-Force
                                    - Start-Sleep -Seconds 3
                                    - write-output "Start SQL Services..."
>>log.txt
                                    - Set-Service -Name 'MSSQLSERVER'
-StartupType Automatic
                                    - start-service -name 'MSSQLSERVER'
                                    - write-output "SQL started" >>log.txt
```

3. Una volta implementati gli YAML, creare la configurazione MigrateOps. Per farlo, vai a migrazione dei dati > MigrateOps, fai clic su "Avvia nuova operazione" e inserisci la configurazione in un formato YAML valido.
4. Fare clic su "Create Operation" (Crea operazione).

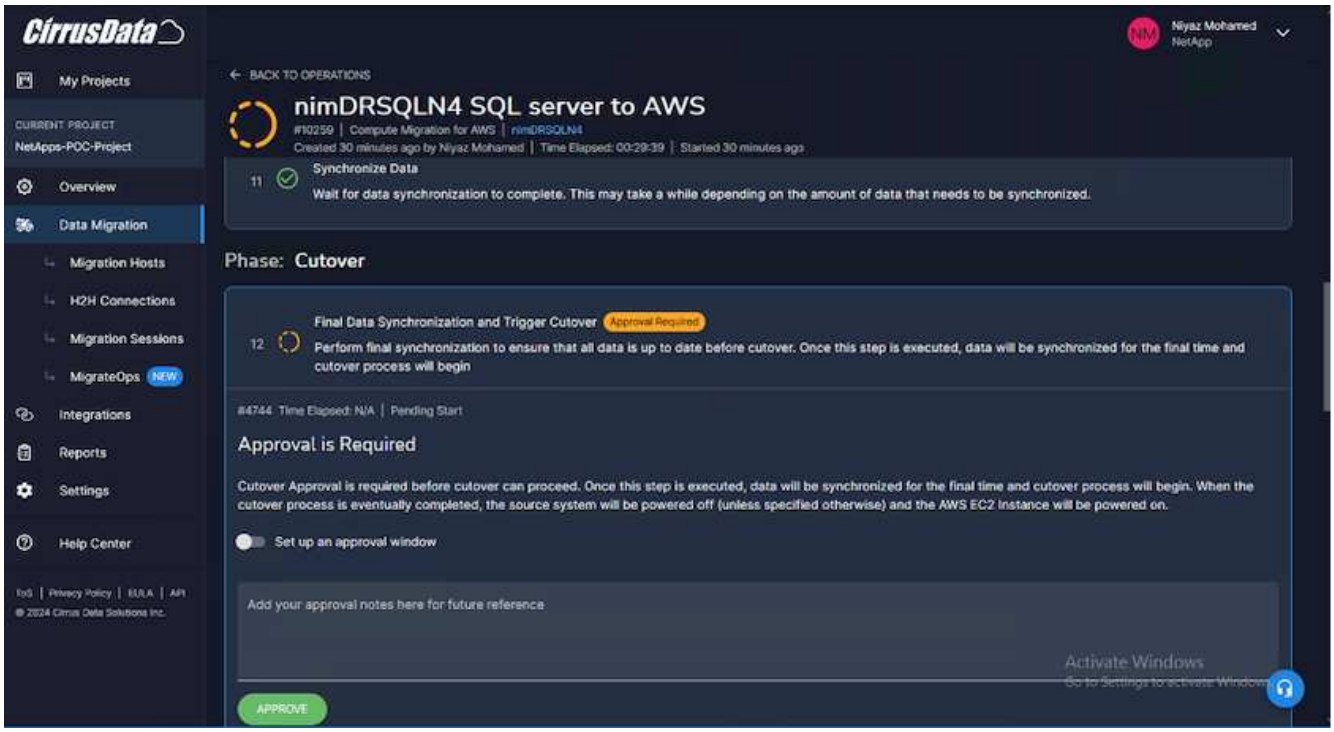
   Nota: Per ottenere il parallelismo, ogni host deve avere un file YAML specificato e configurato.

5. A meno che il `scheduled_start_time` il campo è specificato nella configurazione, l'operazione verrà avviata immediatamente.
6. L'operazione verrà eseguita e proseguirà. Dall'interfaccia utente di Cirrus Data Cloud, è possibile monitorare l'avanzamento con messaggi dettagliati. Questi passaggi includono automaticamente le attività che vengono normalmente eseguite manualmente, come l'esecuzione dell'allocazione automatica e la creazione di sessioni di migrazione.

Nota: Durante la migrazione da host a host, verrà creato un gruppo di protezione aggiuntivo con una regola che consente la porta 4996 in entrata, che consentirà la porta richiesta per la comunicazione e verrà automaticamente eliminata una volta completata la sincronizzazione.



7. Durante la sincronizzazione di questa sessione di migrazione, è prevista una fase futura della fase 3 (cutover) con l'etichetta "Approval Required" (approvazione obbligatoria). In una ricetta MigrateOps, per poter essere eseguite, le attività critiche (come i tagli alla migrazione) richiedono l'approvazione dell'utente. Gli operatori di progetto o gli amministratori possono approvare queste attività dall'interfaccia utente. È inoltre possibile creare una finestra di approvazione futura.



8. Una volta approvata, l’operazione MigrateOps continua con il cutover.
9. Dopo un breve istante, l’operazione sarà completata.

Nota: Con l’aiuto della tecnologia Cirrus Data cMotion™, la memorizzazione della destinazione è stata mantenuta aggiornata con tutte le ultime modifiche. Pertanto, dopo l’approvazione data, l’intero processo di cutover finale richiederà un tempo molto breve, in meno di un minuto.

Verifica post-migrazione

Analizziamo l’istanza di Amazon EC2 migrata che esegue il sistema operativo Windows Server e completiamo i seguenti passaggi:

1. Windows SQL Services è stato avviato.

2. Il database è di nuovo online e utilizza lo storage del dispositivo multipath iSCSI.
3. Tutti i nuovi record di database aggiunti durante la migrazione possono essere trovati nel database appena migrato.
4. Il vecchio storage è ora offline.

Nota: Con un solo clic per inviare l'operazione di mobilità dei dati come codice e un clic per approvare il cutover, la VM è stata migrata correttamente da VMware on-premise a un'istanza di Amazon EC2 utilizzando FSX per ONTAP e le sue funzionalità iSCSI.

Nota: A causa della limitazione delle API AWS, le macchine virtuali convertite vengono visualizzate come "Ubuntu". Questo è strettamente un problema di visualizzazione e non influisce sulla funzionalità dell'istanza migrata. Una prossima release risolverà questo problema.

Nota: È possibile accedere alle istanze di Amazon EC2 migrate utilizzando le credenziali utilizzate sul lato on-premise.

Migra le macchine virtuali su Amazon EC2 con FSxN: Altre possibilità e conclusioni

In questo articolo vengono illustrate altre possibilità per questa soluzione di migrazione e viene concluso l'argomento.

Altre possibilità

Lo stesso approccio può essere esteso per la migrazione di macchine virtuali che utilizzano lo storage in-guest su macchine virtuali on-premise. È possibile migrare il sistema operativo VMDK utilizzando CMC, mentre le LUN iSCSI in-guest possono essere replicate mediante SnapMirror. Il processo richiede la rottura del mirror e l'associazione della LUN all'istanza di Amazon EC2 appena migrata, come illustrato nel diagramma sottostante.

Conclusione

Questo documento ha fornito una procedura dettagliata per l'utilizzo della funzionalità MigrateOps di CMC per la migrazione in AWS dei dati archiviati in repository VMware on-premise utilizzando le istanze di Amazon EC2 ed FSX per ONTAP.

Il video seguente mostra il processo di migrazione dall'inizio alla fine:

Migrazione delle macchine virtuali VMware su Amazon EC2

Per controllare la GUI e la migrazione locale di base di Amazon EBS in FSX per ONTAP, guarda questo video dimostrativo di cinque minuti:

Migrazione a qualsiasi storage in scala con Cirrus Migrate Cloud

Multicloud ibrido NetApp con soluzioni VMware

Casi d'utilizzo di multicloud ibrido di VMware

Casi di utilizzo per NetApp Hybrid Multibloud con VMware

Panoramica dei casi di utilizzo importanti per l'organizzazione IT durante la pianificazione di implementazioni cloud ibrido o cloud-first.

Casi di utilizzo più comuni

I casi di utilizzo includono:

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

- Modernizzazione delle applicazioni sfruttando le tecnologie supplementari del cloud.

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

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

Dentro il percorso DELL'IT

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

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

Comprendere l'importanza delle opzioni di storage NFS supplementari

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

Consideriamo questo scenario:

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

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

Automazione VMware vSphere

Introduzione all'automazione per ONTAP e vSphere

Questa pagina descrive i vantaggi dell'automazione delle funzionalità ONTAP di base in un ambiente VMware vSphere.

Automazione VMware

L'automazione è parte integrante della gestione degli ambienti VMware fin dai primi giorni di VMware ESX. La capacità di implementare l'infrastruttura come codice ed estendere le pratiche alle operazioni del cloud privato aiuta ad alleviare i problemi legati a scalabilità, flessibilità, self-provisioning ed efficienza.

L'automazione può essere organizzata nelle seguenti categorie:

- **Implementazione dell'infrastruttura virtuale**
- **Operazioni della macchina guest**
- **Operazioni cloud**

Gli amministratori hanno a disposizione numerose opzioni per l'automazione dell'infrastruttura. Sia attraverso l'utilizzo di funzionalità vSphere native come profili host o specifiche di personalizzazione per le macchine virtuali alle API disponibili sui componenti software VMware, sui sistemi operativi e sui sistemi storage NetApp, sono disponibili documentazione e indicazioni significative.

Data ONTAP 8.0.1 e versioni successive supportano alcune API VMware vSphere per l'integrazione degli array (VAAI) quando l'host ESX esegue ESX 4.1 o versioni successive. VAAI è un insieme di API che consentono la comunicazione tra host VMware vSphere ESXi e dispositivi di storage. Queste funzionalità consentono di trasferire le operazioni dall'host ESX al sistema storage e aumentare il throughput di rete. L'host ESX attiva automaticamente le funzioni nell'ambiente corretto. È possibile determinare la misura in cui il sistema utilizza le funzioni VAAI controllando le statistiche contenute nei contatori VAAI.

Il punto di partenza più comune per l'automazione dell'implementazione di un ambiente VMware è il provisioning di datastore a blocchi o basati su file. È importante definire i requisiti delle attività effettive prima di sviluppare l'automazione corrispondente.

Per ulteriori informazioni sull'automazione degli ambienti VMware, consultare le seguenti risorse:

- "Il NetApp Pub". Automazione e gestione della configurazione NetApp.
- "La community Ansible Galaxy per VMware". Una raccolta di risorse Ansible per VMware.
- "Risorse VMware {code}". Risorse necessarie per progettare soluzioni per il data center software-defined, inclusi forum, standard di progettazione, codice di esempio e tool per sviluppatori.

Provisioning tradizionale dello storage a blocchi

Provisioning tradizionale dello storage a blocchi vSphere con ONTAP

VMware vSphere supporta le seguenti opzioni di datastore VMFS con il supporto del protocollo SAN ONTAP indicato.

Opzioni datastore VMFS	Supporto del protocollo SAN ONTAP
"Fibre Channel (FC)"	sì
"Fibre Channel over Ethernet (FCoE)"	sì
"ISCSI"	sì

Opzioni datastore VMFS	Supporto del protocollo SAN ONTAP
Estensioni iSCSI per RDMA (iSER)	no
"NVMe su fabric con FC (NVMe/FC)"	sì
NVMe su fabric con RDMA su Ethernet convergente (NVMe/RoCE)	no

Se è richiesto iSER o NVMe/RoCE VMFS, controllare i sistemi storage basati su SANtricity.

Datastore vSphere VMFS - backend dello storage Fibre Channel con ONTAP

In questa sezione viene illustrata la creazione di un datastore VMFS con lo storage Fibre Channel (FC) ONTAP.

Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con {ontap_version}
- Credenziali ONTAP (nome SVM, ID utente e password)
- WWPN ONTAP di host, destinazione e informazioni su SVM e LUN
- "Il foglio di lavoro di configurazione FC completo"
- Credenziali vCenter Server
- Informazioni sugli host vSphere
  - {vsphere_version}
- Switch fabric
  - Con porte dati ONTAP FC e host vSphere collegati
  - Con la funzione NPIV (N_Port ID Virtualization) attivata
  - Creare una singola zona di destinazione dell'iniziatore.
    - Creare una zona per ciascun iniziatore (singola zona iniziatore).
    - Per ciascuna zona, includere una destinazione che sia l'interfaccia logica FC ONTAP (WWPN) per le SVM. Devono essere presenti almeno due interfacce logiche per nodo per SVM. Non utilizzare la WWPN delle porte fisiche.
- Un tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso.

Provisioning di un datastore VMFS

Per eseguire il provisioning di un datastore VMFS, attenersi alla seguente procedura:

1. Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)"
2. Verificare che il "Configurazione FCP supportata".

Attività di ONTAP

1. "Verificare di disporre di una licenza ONTAP per FCP."

a. Utilizzare `system license show` Per verificare che FCP sia presente nell'elenco.

b. Utilizzare `licen se add -license-code <license code>` per aggiungere la licenza.

2. Assicurarsi che il protocollo FCP sia attivato su SVM.

   a. "Verificare l'FCP su una SVM esistente."

   b. "Configurare l'FCP su una SVM esistente."

   c. "Crea la nuova SVM con FCP."

3. Assicurarsi che le interfacce logiche FCP siano disponibili su una SVM.

   a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.

   b. Quando viene creata una SVM con la GUI, le interfacce logiche fanno parte di tale processo.

   c. Per rinominare le interfacce di rete, utilizzare `Network Interface modify`.

4. "Creare e mappare un LUN." Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere.

Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili in "Informazioni sull'adattatore di storage".
2. "Eseguire il provisioning di un datastore VMFS con gli strumenti ONTAP".

Datastore vSphere VMFS - protocollo storage Fibre Channel over Ethernet con ONTAP

In questa sezione viene illustrata la creazione di un datastore VMFS con il protocollo di trasporto Fibre Channel over Ethernet (FCoE) allo storage ONTAP.

Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select) con {ontap_version}
- Credenziali ONTAP (nome SVM, ID utente e password)
- "Una combinazione FCoE supportata"
- "Un foglio di lavoro di configurazione completo"
- Credenziali vCenter Server
- Informazioni sugli host vSphere
  - {vsphere_version}
- Switch fabric
  - Con porte dati ONTAP FC o host vSphere collegati
  - Con la funzione NPIV (N_Port ID Virtualization) attivata
  - Creare una singola zona di destinazione dell'iniziatore.
  - "Zoning FC/FCoE configurato"
- Switch di rete
  - Supporto FCoE
  - Supporto DCB

    - "Frame jumbo per FCoE"
- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

Eseguire il provisioning di un datastore VMFS

- Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)".
- "Verificare che la configurazione FCoE sia supportata".

Attività di ONTAP

1. "Verificare la licenza ONTAP per FCP."
    a. Utilizzare `system license show` Per verificare che l'FCP sia presente nell'elenco.
    b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. Verificare che il protocollo FCP sia attivato su SVM.
    a. "Verificare l'FCP su una SVM esistente."
    b. "Configurare l'FCP su una SVM esistente."
    c. "Creare una nuova SVM con FCP."
3. Verificare che le interfacce logiche FCP siano disponibili su SVM.
    a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.
    b. Quando la SVM viene creata con la GUI, le interfacce logiche fanno parte di tale processo.
    c. Per rinominare l'interfaccia di rete, utilizzare `Network Interface modify`.
4. "Creare e mappare un LUN"; Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere.

Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili in "informazioni sull'adattatore di storage".
2. "Eseguire il provisioning di un datastore VMFS con gli strumenti ONTAP".

Datastore vSphere VMFS - backend storage iSCSI con ONTAP

In questa sezione viene descritta la creazione di un datastore VMFS con lo storage iSCSI ONTAP.

Per il provisioning automatico, utilizzare il seguente script: [Ansible].

Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con {ontap_version}
- Credenziali ONTAP (nome SVM, ID utente e password)
- Informazioni su porta di rete ONTAP, SVM e LUN per iSCSI
- "Un foglio di lavoro di configurazione iSCSI completo"
- Credenziali vCenter Server

- Informazioni sugli host vSphere
  - {vsphere_version}
- Informazioni IP adattatore VMkernel iSCSI
- Switch di rete
  - Con porte dati di rete del sistema ONTAP e host vSphere collegati
  - VLAN configurate per iSCSI
  - (Opzionale) link aggregation configurato per le porte dati di rete ONTAP
- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

Fasi

1. Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)".
2. "Verificare che la configurazione iSCSI sia supportata."
3. Completare le seguenti attività di ONTAP e vSphere.

Attività di ONTAP

1. "Verificare la licenza ONTAP per iSCSI".
   a. Utilizzare `system license show` Comando per verificare se iSCSI è presente nell'elenco.
   b. Utilizzare `license add -license-code <license code>` per aggiungere la licenza.
2. "Verificare che il protocollo iSCSI sia attivato su SVM."
3. Verificare che le interfacce logiche di rete iSCSI siano disponibili su SVM.

   Quando si crea una SVM utilizzando la GUI, vengono create anche le interfacce di rete iSCSI.

4. Utilizzare `Network interface` per visualizzare o apportare modifiche all'interfaccia di rete.

   Si consigliano due interfacce di rete iSCSI per nodo.

5. "Creare un'interfaccia di rete iSCSI." È possibile utilizzare la policy di servizio default-data-block.
6. "Verificare che il servizio dati-iscsi sia incluso nella politica di servizio." È possibile utilizzare `network interface service-policy show` per verificare.
7. "Verificare che i frame jumbo siano attivati."
8. "Creare e mappare il LUN." Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere. Ripetere questo passaggio per ogni LUN.

Attività di VMware vSphere

1. Verificare che almeno una NIC sia disponibile per la VLAN iSCSI. Due schede di rete sono preferite per migliorare le performance e la tolleranza agli errori.
2. "Identificare il numero di NIC fisiche disponibili sull'host vSphere."
3. "Configurare iSCSI Initiator." Un caso d'utilizzo tipico è un iniziatore iSCSI software.
4. "Verificare che lo stack TCPIP per iSCSI sia disponibile".

5. "Verificare che i portgroup iSCSI siano disponibili".
    - In genere utilizziamo un singolo switch virtuale con più porte di uplink.
    - Utilizzare la mappatura dell'adattatore 1:1.
6. Verificare che gli adattatori VMkernel iSCSI siano abilitati per corrispondere al numero di NIC e che gli IP siano assegnati.
7. "Collegare l'adattatore software iSCSI agli adattatori VMkernel iSCSI."
8. "Eseguire il provisioning del datastore VMFS con gli strumenti ONTAP". Ripetere questo passaggio per tutti gli archivi dati.
9. "Verificare il supporto dell'accelerazione hardware."

Quali sono le prossime novità?

Una volta completate queste attività, il datastore VMFS è pronto per il provisioning delle macchine virtuali.

Ansible Playbook

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
       password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
    - name: Generate a Session ID for ONTAP tools with vCenter
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
        validate_certs: false
        method: POST
        return_content: yes
        body_format: json
        body:
          vcenterUserName: "{{ vcenter_username }}"
```

```
          vcenterPassword: "{{ vcenter_password }}"
      register: login

    # Get existing registered ONTAP Cluster info with ONTAP tools
    - name: Get ONTAP Cluster info from ONTAP tools
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
        validate_certs: false
        method: Get
        return_content: yes
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      register: clusterinfo

    - name: Get ONTAP Cluster ID
      set_fact:
        ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
      vars:
        clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

    - name: Get ONTAP SVM ID
      set_fact:
        ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
      vars:
        svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

    - name: Get Aggregate detail
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
        validate_certs: false
        method: GET
        return_content: yes
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
          cluster-id: "{{ ontap_svm_id }}"
      when: ontap_svm_id != ''
      register: aggrinfo

    - name: Select Aggregate with max free capacity
      set_fact:
        aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
```

```
      vars:
        aggrquery: "max_by(records, &freeCapacity).name"

    - name: Convert datastore size in MB
      set_fact:
        datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

    - name: Get vSphere Cluster Info
      uri:
        url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
        validate_certs: false
        method: GET
        return_content: yes
        body_format: json
        headers:
          vmware-api-session-id: "{{ vclogin.json.value }}"
      when: vsphere_cluster != ''
      register: vcenterclusterid

    - name: Create iSCSI VMFS-6 Datastore with ONTAP tools
      uri:
        url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
        validate_certs: false
        method: POST
        return_content: yes
        status_code: [200]
        body_format: json
        body:
          traditionalDatastoreRequest:
            name: "{{ iscsi_datastore_name }}"
            datastoreType: VMFS
            protocol: ISCSI
            spaceReserve: Thin
            clusterID:  "{{ ontap_cluster_id }}"
            svmID: "{{ ontap_svm_id }}"
            targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
            datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
            vmfsFileSystem: VMFS6
            aggrName: "{{ aggr_name }}"
            existingFlexVolName: ""
            volumeStyle: FLEXVOL
            datastoreClusterMoref: ""
```

```
        headers:
          vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
      register: result
      changed_when: result.status == 200
```

Archivio dati vSphere VMFS - NVMe/FC con ONTAP

In questa sezione viene descritta la creazione di un datastore VMFS con storage ONTAP utilizzando NVMe/FC.

Di cosa hai bisogno

- Competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- "Comprensione di base di NVMe/FC".
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con {ontap_version}
- Credenziali ONTAP (nome SVM, ID utente e password)
- WWPN ONTAP per informazioni su host, destinazione, SVM e LUN
- "Un foglio di lavoro di configurazione FC completo"
- Server vCenter
- Informazioni sugli host vSphere ({vsphere_version})
- Switch fabric
  - Con porte dati ONTAP FC e host vSphere collegati.
  - Con la funzione NPIV (N_Port ID Virtualization) attivata.
  - Creare una singola zona di destinazione dell'iniziatore.
  - Creare una zona per ciascun iniziatore (singola zona iniziatore).
  - Per ciascuna zona, includere una destinazione che sia l'interfaccia logica FC ONTAP (WWPN) per le SVM. Devono essere presenti almeno due interfacce logiche per nodo per SVM. Non utilizzare la WWPN delle porte fisiche.

Provisioning del datastore VMFS

1. Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)".
2. "Verificare che la configurazione NVMe/FC sia supportata."

Attività di ONTAP

1. "Verificare la licenza ONTAP per FCP."Utilizzare `system license show` E verificare se NVMe_of è elencato. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. Verificare che il protocollo NVMe sia attivato sulla SVM.
   a. "Configurare le SVM per NVMe."
3. Verificare che le interfacce logiche NVMe/FC siano disponibili sulle SVM.
   a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.

b. Quando si crea una SVM con la GUI, le interfacce logiche fanno parte di tale processo.

c. Per rinominare l'interfaccia di rete, utilizzare il comando `Network Interface modify`.

4. "Creare lo spazio dei nomi e il sottosistema NVMe"

Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili all'indirizzo "Informazioni sull'adattatore di storage"
2. "Eseguire l'installazione del driver vSphere host NVMe e le attività di convalida"
3. "Crea datastore VMFS"

Provisioning di file storage tradizionale

Provisioning tradizionale dello storage di file vSphere con ONTAP

VMware vSphere supporta i seguenti protocolli NFS, entrambi compatibili con ONTAP.

- "NFS versione 3"
- "NFS versione 4.1"

Se hai bisogno di aiuto per selezionare la versione NFS corretta per vSphere, controlla "Questo confronto tra le versioni dei client NFS".

Riferimento

"Caratteristiche del datastore e del protocollo vSphere: NFS"

Datastore vSphere NFS - versione 3 con ONTAP

Creazione di datastore NFS versione 3 con storage NAS ONTAP.

Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) che esegue {ONTAP_version}
- Credenziali ONTAP (nome SVM, ID utente, password)
- Informazioni su porta di rete ONTAP, SVM e LUN per NFS
  - "Un foglio di lavoro di configurazione NFS completo"
- Credenziali vCenter Server
- Informazioni sugli host vSphere per {vSphere_version}
- NFS VMkernel adapter IP information
- Switch di rete
  - Con porte dati di rete del sistema ONTAP e host vSphere collegati
  - VLAN configurate per NFS
  - (Opzionale) link aggregation configurato per le porte dati di rete ONTAP

- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

Fasi

- Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)"
  - "Verificare che la configurazione NFS sia supportata."
- Completare le seguenti attività di ONTAP e vSphere.

Attività di ONTAP

1. "Verificare la licenza ONTAP per NFS."
   a. Utilizzare `system license show` Controllare che NFS sia presente nell'elenco.
   b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. "Seguire il workflow di configurazione di NFS."

Attività di VMware vSphere

"Seguire il flusso di lavoro per la configurazione del client NFS per vSphere."

Riferimento

"Caratteristiche del datastore e del protocollo vSphere: NFS"

Quali sono le prossime novità?

Una volta completate queste attività, il datastore NFS è pronto per il provisioning delle macchine virtuali.

Archivio dati vSphere NFS - versione 4.1 con ONTAP

Questa sezione descrive la creazione di un datastore NFS versione 4.1 con storage NAS ONTAP.

Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Sistema storage ONTAP (file FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp) con {ontap_version}
- Credenziali ONTAP (nome SVM, ID utente, password)
- Informazioni su porta di rete ONTAP, SVM e LUN per NFS
- "Un foglio di lavoro di configurazione NFS completo"
- Credenziali vCenter Server
- Informazioni sugli host vSphere {vsphere_version}
- NFS VMkernel adapter IP information
- Switch di rete
  - Con porte dati di rete del sistema ONTAP, host vSphere e connessi
  - VLAN configurate per NFS

    - (Opzionale) link aggregation configurato per le porte dati di rete ONTAP
- Tool ONTAP per VMware vSphere implementati, configurati e pronti all'uso

Fasi

- Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)."
    - "Verificare che la configurazione NFS sia supportata."
- Completare le attività ONTAP e vSphere fornite di seguito.

Attività di ONTAP

1. "Verificare la licenza ONTAP per NFS"
    a. Usareil `system license show` Comando per verificare se NFS è elencato.
    b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. "Seguire il workflow di configurazione di NFS"

Attività di VMware vSphere

"Seguire il flusso di lavoro Configurazione client NFS per vSphere."

Quali sono le prossime novità?

Una volta completate queste attività, il datastore NFS è pronto per il provisioning delle macchine virtuali.

Desktop virtuali

Virtual Desktop Services (VDS)

Cloud ibrido VDI con NetApp Virtual Desktop Service

TR-4861: Cloud ibrido VDI con Virtual Desktop Service

Suresh Thoppay, NetApp

NetApp Virtual Desktop Service (VDS) consente di orchestrare Remote Desktop Services (RDS) nei principali cloud pubblici e nei cloud privati. VDS supporta Windows Virtual Desktop (WVD) su Microsoft Azure. VDS automatizza molte attività che devono essere eseguite dopo l'implementazione di WVD o RDS, tra cui la configurazione delle condivisioni di file SMB (per profili utente, dati condivisi e disco principale utente), l'abilitazione delle funzionalità Windows, l'installazione di applicazioni e agenti, firewall e policy e così via.

Gli utenti utilizzano VDS per desktop dedicati, desktop condivisi e applicazioni remote. VDS fornisce eventi con script per l'automazione della gestione delle applicazioni per i desktop e riduce il numero di immagini da gestire.

VDS offre un singolo portale di gestione per la gestione delle implementazioni in ambienti cloud pubblici e privati.

Valore per il cliente

L'esplosione della forza lavoro remota del 2020 ha cambiato i requisiti di business continuity. I reparti IT devono affrontare nuove sfide per il provisioning rapido di desktop virtuali e quindi richiedere agilità di provisioning, gestione remota e i vantaggi TCO di un cloud ibrido che semplifica il provisioning on-premise e delle risorse cloud. Hanno bisogno di una soluzione di cloud ibrido che:

- Affronta la realtà dello spazio di lavoro post-COVID per consentire modelli di lavoro flessibili con dinamiche globali
- Consente di eseguire turni di lavoro semplificando e accelerando l'implementazione degli ambienti di lavoro per tutti i dipendenti, dai task worker agli utenti più esigenti
- Mobilizza la forza lavoro fornendo risorse VDI ricche e sicure indipendentemente dalla posizione fisica
- Semplifica l'implementazione del cloud ibrido
- Automatizza e semplifica la gestione della riduzione dei rischi

Casi di utilizzo

L'infrastruttura VDI ibrida con NetApp VDS consente ai service provider e agli amministratori dei desktop virtuali aziendali di espandere facilmente le risorse in altri ambienti cloud senza influire sugli utenti. La disponibilità di risorse on-premise offre un migliore controllo delle risorse e un'ampia scelta di opzioni (calcolo, GPU, storage e rete) per soddisfare la domanda.

Questa soluzione si applica ai seguenti casi di utilizzo:

- Nel cloud per i picchi della domanda di desktop e applicazioni remoti
- Riduzione del TCO per applicazioni e desktop remoti a esecuzione prolungata ospitandoli on-premise con storage flash e risorse GPU
- Facilità di gestione di desktop e applicazioni remoti negli ambienti cloud
- Sperimenta desktop e applicazioni remoti utilizzando un modello software-as-a-service con risorse on-premise

Pubblico di destinazione

Il pubblico di riferimento per la soluzione comprende i seguenti gruppi:

- EUC/VDI Architect che vogliono comprendere i requisiti per un VDS ibrido
- Partner NetApp che desiderano assistere i clienti nelle loro esigenze di desktop remoto e applicazioni
- Clienti NetApp HCI esistenti che desiderano soddisfare le esigenze di desktop remoto e applicazioni

Panoramica del servizio Virtual Desktop di NetApp

NetApp offre numerosi servizi cloud, tra cui il provisioning rapido di desktop virtuale con applicazioni WVD o remote e la rapida integrazione con Azure NetApp Files.

Tradizionalmente, il provisioning e l'erogazione di servizi desktop remoti ai clienti richiedono settimane. Oltre al provisioning, può essere difficile gestire applicazioni, profili utente, dati condivisi e oggetti di policy di gruppo per applicare le policy. Le regole del firewall possono aumentare la complessità e richiedere un set di competenze e strumenti separati.

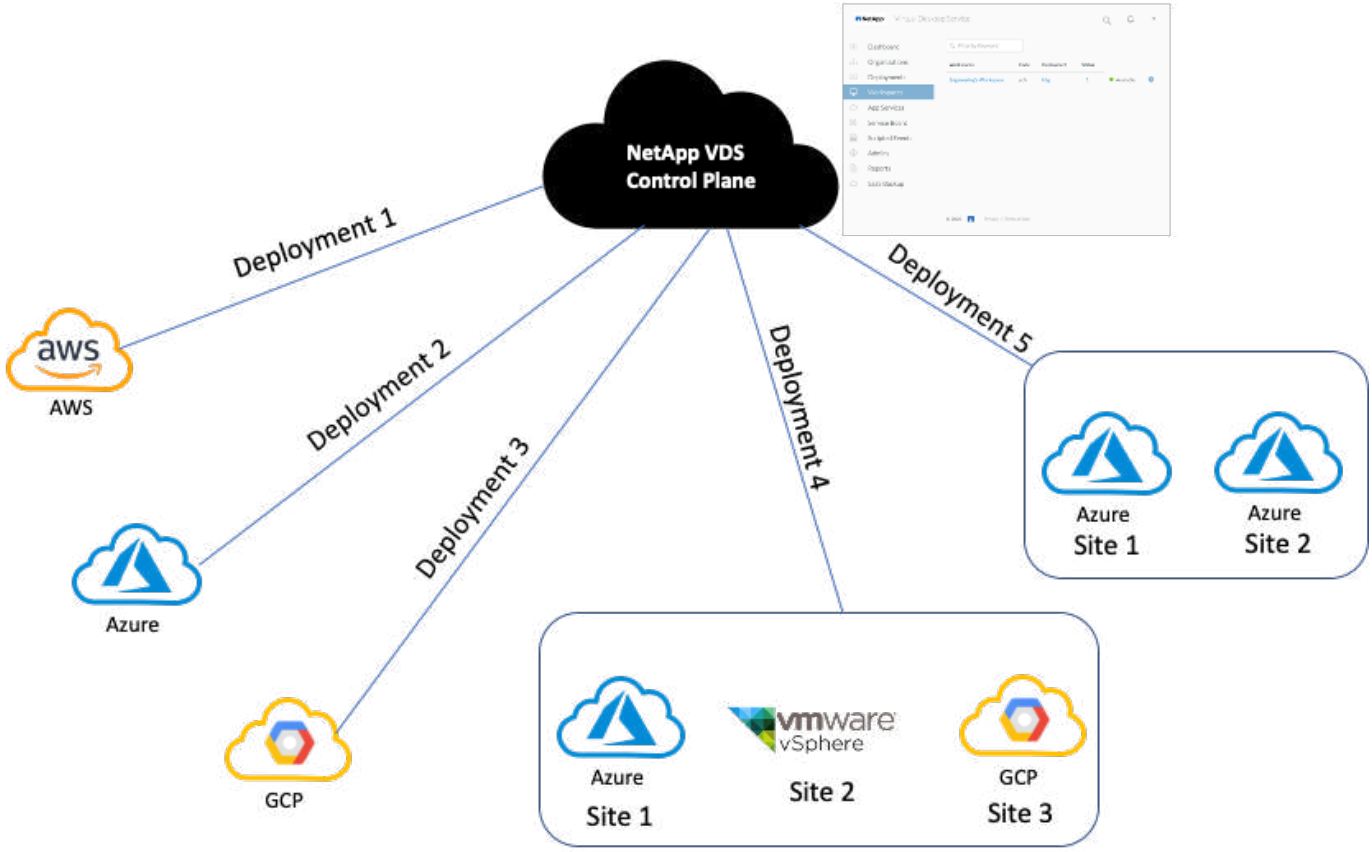
Con il servizio Microsoft Azure Windows Virtual Desktop, Microsoft si occupa della manutenzione dei componenti di Remote Desktop Services, consentendo ai clienti di concentrarsi sul provisioning delle aree di lavoro nel cloud. I clienti devono eseguire il provisioning e gestire lo stack completo, che richiede competenze speciali per gestire gli ambienti VDI.

Con NetApp VDS, i clienti possono implementare rapidamente desktop virtuali senza doversi preoccupare di dove installare i componenti dell'architettura come broker, gateway, agenti e così via. I clienti che richiedono il controllo completo del proprio ambiente possono collaborare con un team di servizi professionali per raggiungere i propri obiettivi. I clienti utilizzano i VDS come servizio e possono quindi concentrarsi sulle principali sfide aziendali.

NetApp VDS è un'offerta software-as-a-service per la gestione centralizzata di implementazioni multiple in ambienti AWS, Azure, GCP o cloud privato. Microsoft Windows Virtual Desktop è disponibile solo su Microsoft Azure. NetApp VDS consente di orchestrare i servizi di desktop remoto Microsoft in altri ambienti.

Microsoft offre sessioni multiple su Windows 10 esclusivamente per ambienti Windows Virtual Desktop su Azure. L'autenticazione e l'identità sono gestite dalla tecnologia dei desktop virtuali; WVD richiede Azure Active Directory sincronizzato (con ad Connect) con Active Directory e le VM di sessione collegate ad Active Directory. RDS richiede Active Directory per l'identità e l'autenticazione dell'utente e l'Unione e la gestione del dominio delle macchine virtuali.

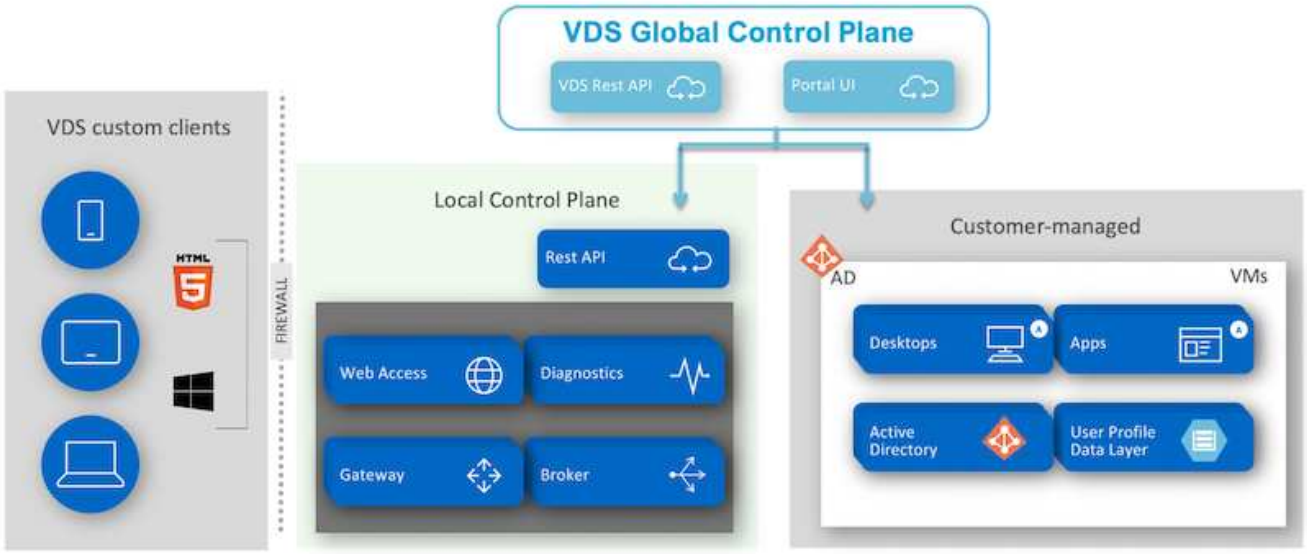
Nella figura seguente viene illustrata una topologia di implementazione di esempio.



Ogni implementazione è associata a un dominio Active Directory e fornisce ai client un punto di accesso per aree di lavoro e applicazioni. Un provider di servizi o un'azienda che dispone di più domini Active Directory ha in genere più implementazioni. Un singolo dominio Active Directory che si estende in più regioni ha in genere una singola implementazione con più siti.

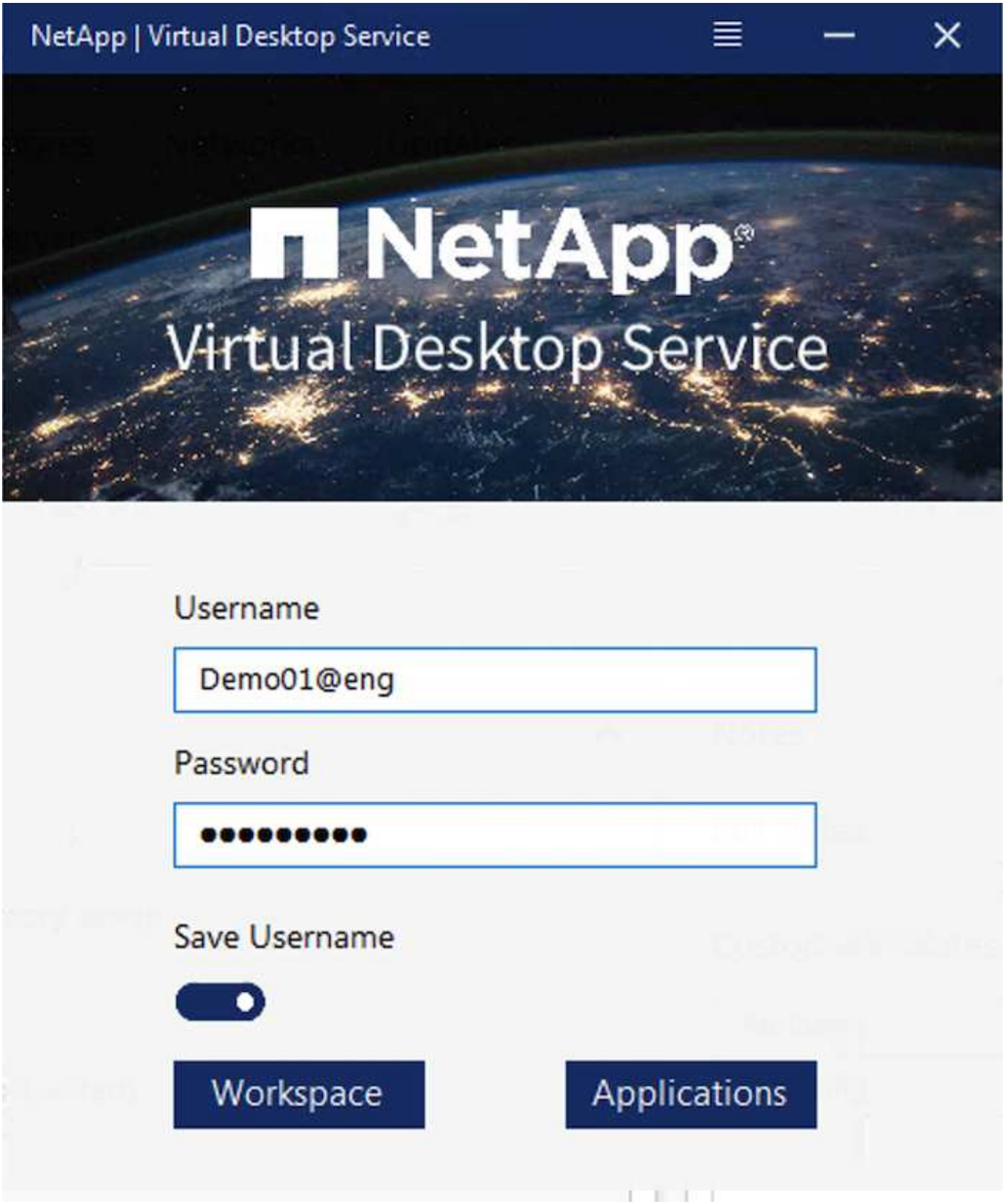
Per WVD in Azure, Microsoft fornisce un servizio Platform-as-a-Service utilizzato da NetApp VDS. Per altri ambienti, NetApp VDS orchestrerà l'implementazione e la configurazione dei servizi di desktop remoto Microsoft. NetApp VDS supporta sia WVD Classic che WVD ARM e può essere utilizzato anche per aggiornare le versioni esistenti.

Ogni implementazione dispone di servizi per la propria piattaforma, che comprendono Cloud Workspace Manager (endpoint REST API), un gateway HTML 5 (connessione alle macchine virtuali da un portale di gestione VDS), RDS Gateway (Access Point per i client) e un controller di dominio. La figura seguente mostra l'architettura del piano di controllo VDS per l'implementazione RDS.



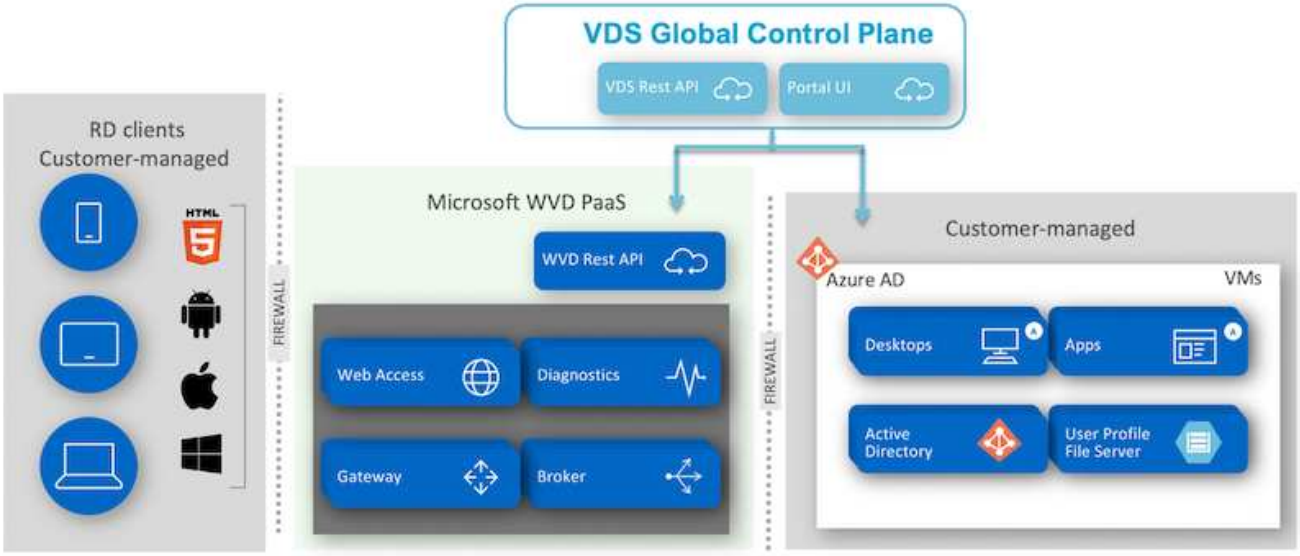
Per le implementazioni RDS, NetApp VDS può essere facilmente accessibile da Windows e dai browser utilizzando software client che può essere personalizzato per includere logo e immagini del cliente. In base alle credenziali dell'utente, fornisce all'utente l'accesso a aree di lavoro e applicazioni approvate. Non è necessario configurare i dettagli del gateway.

La figura seguente mostra il client NetApp VDS.



Nell'implementazione di Azure WVD, Microsoft gestisce l'access point per i client e può essere utilizzato da un client Microsoft WVD disponibile in modalità nativa per diversi sistemi operativi. È inoltre possibile accedervi da un portale basato su web. La configurazione del software client deve essere gestita dall'oggetto Criteri di gruppo (GPO) o in altri modi preferiti dai clienti.

La seguente figura illustra l'architettura del piano di controllo VDS per le implementazioni di Azure WVD.



Oltre all'implementazione e alla configurazione dei componenti richiesti, NetApp VDS gestisce anche la gestione degli utenti, la gestione delle applicazioni, la scalabilità delle risorse e l'ottimizzazione.

NetApp VDS può creare utenti o concedere agli account utente esistenti l'accesso allo spazio di lavoro cloud o ai servizi applicativi. Il portale può essere utilizzato anche per la reimpostazione delle password e la delega dell'amministrazione di un sottoinsieme di componenti. Gli amministratori dell'helpdesk o i tecnici di livello 3 possono affiancare le sessioni degli utenti per la risoluzione dei problemi o connettersi ai server dall'interno del portale.

NetApp VDS può utilizzare i modelli di immagine creati dall'utente oppure quelli esistenti sul mercato per il provisioning basato sul cloud. Per ridurre il numero di immagini da gestire, è possibile utilizzare un'immagine di base e il provisioning di eventuali applicazioni aggiuntive necessarie utilizzando il framework fornito per includere qualsiasi tool della riga di comando come chocolatey, MSIX app attach, PowerShell e così via. Anche gli script personalizzati possono essere utilizzati come parte degli eventi del ciclo di vita delle macchine.

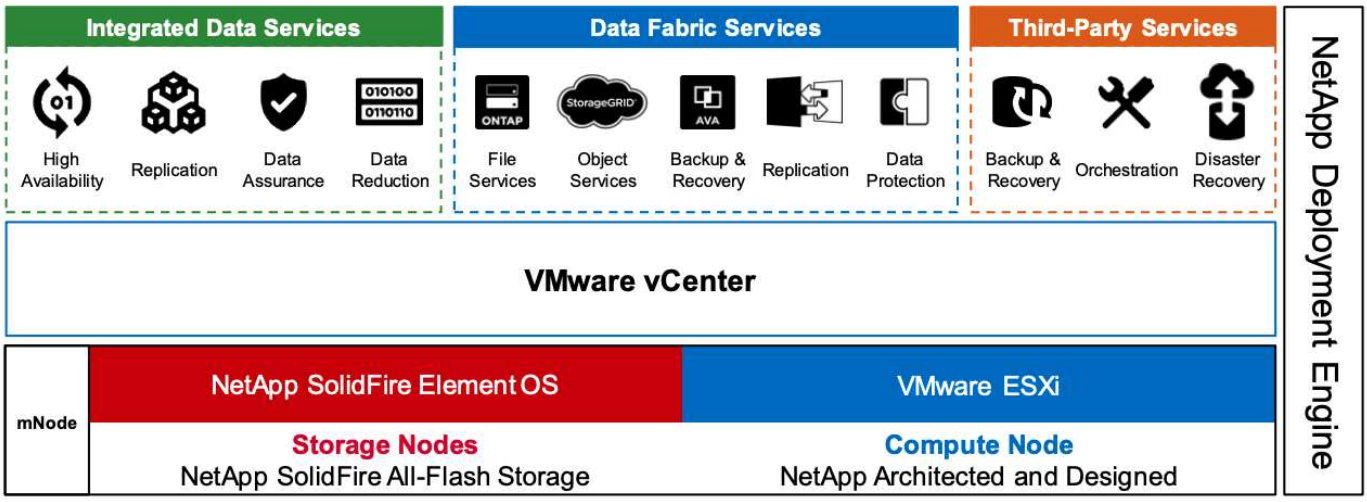
Panoramica di NetApp HCI

NetApp HCI è un'infrastruttura di cloud ibrido costituita da una combinazione di nodi di storage e nodi di calcolo. È disponibile come unità a due rack o come unità a rack singolo, a seconda del modello. L'installazione e la configurazione necessarie per implementare le macchine virtuali sono automatizzate con NetApp Deployment Engine (NDE). I cluster di calcolo vengono gestiti con VMware vCenter e i cluster di storage vengono gestiti con il plug-in vCenter implementato con NDE. Una VM di gestione chiamata mNode viene implementata come parte di NDE.

NetApp HCI gestisce le seguenti funzioni:

- Aggiornamenti della versione
- Invio di eventi a vCenter
- Gestione del plug-in vCenter
- Tunnel VPN per il supporto
- Il raccoglitore di NetApp Active IQ Digital Advisor (noto anche come Digital Advisor)

- L'estensione dei NetApp Cloud Services on-premise, consentendo un'infrastruttura di cloud ibrido. La figura seguente mostra i componenti HCI.



Nodi di storage

I nodi di storage sono disponibili come unità rack a mezza larghezza o a larghezza intera. Inizialmente sono necessari almeno quattro nodi di storage e un cluster può espandersi fino a 40 nodi. Un cluster di storage può essere condiviso tra più cluster di calcolo. Tutti i nodi di storage contengono un controller della cache per migliorare le performance di scrittura. Un singolo nodo fornisce 50.000 o 100.000 IOPS con una dimensione del blocco 4K.

I nodi di storage NetApp HCI eseguono il software NetApp Element, che fornisce limiti di QoS minimi, massimi e burst. Il cluster di storage supporta una combinazione di nodi di storage, anche se un nodo di storage non può superare un terzo della capacità totale.

Nodi di calcolo

> NetApp supporta lo storage connesso a qualsiasi server di calcolo elencato nella "Guida alla compatibilità VMware".

I nodi di calcolo sono disponibili in metà larghezza, larghezza completa e due dimensioni di unità rack. I modelli NetApp HCI H410C e H610C sono basati su processori scalabili Intel Skylake. H615C è basato su processori scalabili Intel Cascade Lake di seconda generazione. Esistono due modelli di calcolo che contengono GPU: Il modello H610C contiene due schede NVIDIA M10 e il modello H615C contiene tre schede NVIDIA T4.

NVIDIA T4 dispone di 40 core RT che forniscono la potenza di calcolo necessaria per fornire il ray tracing in tempo reale. Lo stesso modello di server utilizzato da progettisti e ingegneri può ora essere utilizzato anche dagli artisti per creare immagini fotorealistiche con luce che rimbalza dalle superfici proprio come nella vita reale. Questa GPU compatibile con RTX produce prestazioni di ray tracing in tempo reale fino a cinque Giga raggi al secondo. NVIDIA T4, se combinata con il software quadro Virtual Data Center Workstation (quadro VDWS), consente agli artisti di creare design fotorealistici con ombre, riflessi e rifrazioni precise su qualsiasi dispositivo da qualsiasi posizione.

I core Tensor ti consentono di eseguire carichi di lavoro di deduzione per l'apprendimento approfondito. Durante l'esecuzione di questi carichi di lavoro, NVIDIA T4 con quadro VDWS offre prestazioni fino a 25 volte più veloci rispetto a una macchina virtuale gestita da un server solo CPU. NetApp H615C con tre schede NVIDIA T4 in un'unità rack è la soluzione ideale per la grafica e i carichi di lavoro a elaborazione intensiva.

La figura seguente elenca le schede NVIDIA GPU e ne confronta le caratteristiche.

NVIDIA GPUs Recommended for Virtualization

	V100S	RTX 8000	RTX 6000	T4 (Available on NetApp HCI H615C)	M10 (Available on NetApp HCI H610C)	P6
GPU	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
CUDA Cores	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
Tensor Cores	640	576	576	320	—	—
RT Cores	—	72	72	40	—	—
Guaranteed QoS (GPU Scheduler)	✓	✓	✓	✓	—	✓
Live Migration	✓	✓	✓	✓	✓	✓
Multi-vGPU	✓	✓	✓	✓	✓	✓
Memory Size	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
vGPU Profiles	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
Form Factor	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
Power	250 W /300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
Thermal	passive	passive	passive	passive	passive	bare board
vGPU Software Support	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
Use Case	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to highend 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multimonitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

La GPU M10 rimane la migliore soluzione TCO per i casi di utilizzo dei knowledge worker. Tuttavia, il T4 rappresenta un'ottima alternativa quando si desidera standardizzare su una GPU che può essere utilizzata in diversi casi di utilizzo, come workstation virtuali, performance grafiche, rendering interattivo in tempo reale e deduzione. Con il T4, L'IT può sfruttare le stesse risorse GPU per eseguire carichi di lavoro misti—ad esempio, eseguendo VDI durante il giorno e riutilizzando le risorse per eseguire i carichi di lavoro di calcolo di notte.

Il nodo di calcolo H610C è costituito da due unità rack; il modello H615C è un'unità rack di dimensioni pari a una e consuma meno energia. Il modello H615C supporta la codifica e la decodifica H.264 e H.265 (High Efficiency Video Coding [HEVC]) 4:4:4. Supporta anche il decoder VP9 sempre più diffuso; anche il pacchetto container WebM fornito da YouTube utilizza il codec VP9 per il video.

Il numero di nodi in un cluster di calcolo è determinato da VMware; attualmente è 96 con VMware vSphere 7.0 Update 1. La combinazione di diversi modelli di nodi di calcolo in un cluster è supportata quando è attivata la compatibilità vMotion avanzata (EVC).

Licenze NVIDIA

Quando si utilizza un H610C o H615C, la licenza per la GPU deve essere acquistata dai partner NVIDIA autorizzati a rivendere le licenze. È possibile trovare i partner NVIDIA con "ricerca partner". Cerca competenze come GPU virtuale (vGPU) o Tesla.

Il software NVIDIA vGPU è disponibile in quattro edizioni:

- NVIDIA GRID Virtual PC (GRID VPC)

- Applicazioni virtuali NVIDIA GRID (GRID vApps)
- Workstation NVIDIA quadro Virtual Data Center (quadro VDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

PC virtuale GRID

Questo prodotto è ideale per gli utenti che desiderano un desktop virtuale che offra un'esperienza utente ottimale per applicazioni Microsoft Windows, browser, video ad alta definizione e supporto multi-monitor. NVIDIA GRID Virtual PC offre un'esperienza nativa in un ambiente virtuale, consentendo di eseguire tutte le applicazioni del PC a piene performance.

APPLICAZIONI Grid Virtual

LE APPLICAZIONI GRID vApps sono destinate alle organizzazioni che implementano un Remote Desktop Session host (RDSH) o altre soluzioni basate su sessioni o streaming di applicazioni. Progettati per offrire applicazioni Microsoft Windows alle massime performance, i desktop RDSH ospitati da Windows Server sono supportati anche DA GRID vApps.

Quadro Virtual Data Center Workstation

Questa edizione è ideale per i designer mainstream e high-end che utilizzano potenti applicazioni per la creazione di contenuti 3D come Dassault CATIA, SOLIDWORKS, 3Dexcite, Siemens NX, PTC Creo, Schlumberger Petrel, o Autodesk Maya. NVIDIA quadro VDWS consente agli utenti di accedere alle proprie applicazioni grafiche professionali con funzionalità e prestazioni complete, ovunque si trovino su qualsiasi dispositivo.

NVIDIA Virtual ComputeServer

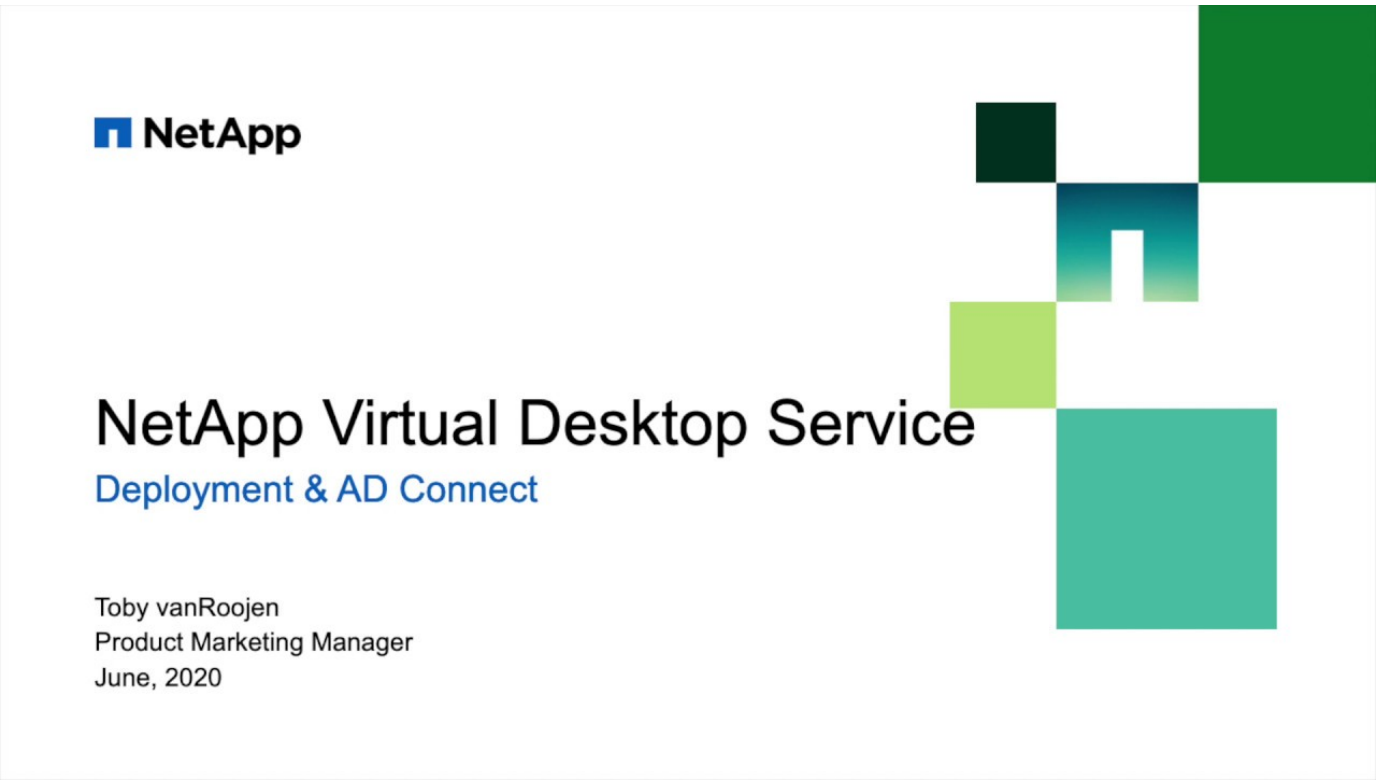
Molte organizzazioni eseguono carichi di lavoro server a elaborazione intensiva come intelligenza artificiale (ai), deep learning (DL) e data science. In questi casi di utilizzo, il software NVIDIA vComputeServer virtualizza la GPU NVIDIA, che accelera i carichi di lavoro dei server a elaborazione intensiva con funzionalità come codice di correzione degli errori, eliminazione delle pagine, peer-to-peer su NVLink e multi-vGPU.

> Una licenza quadro VDWS consente di utilizzare GRID VPC e NVIDIA vComputeServer.

Implementazione

NetApp VDS può essere implementato su Microsoft Azure utilizzando un'applicazione di configurazione disponibile in base alla base di codice richiesta. La versione corrente è disponibile "qui" e la release di anteprima del prodotto in arrivo è disponibile "qui".

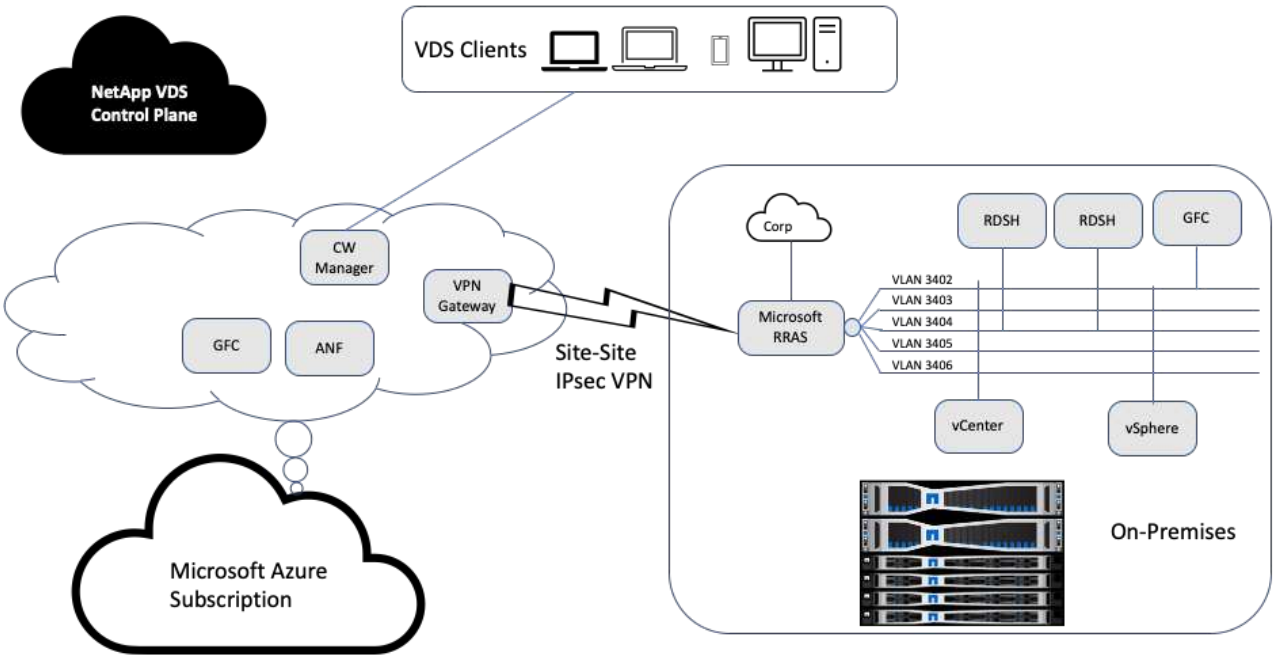
Vedere "questo video" per le istruzioni di implementazione.



Ambiente di cloud ibrido

NetApp Virtual Desktop Service può essere esteso a on-premise quando esiste una connettività tra risorse on-premise e risorse cloud. Le aziende possono stabilire il collegamento a Microsoft Azure utilizzando Express Route o una connessione VPN IPSec site-to-site. È inoltre possibile creare collegamenti ad altri cloud in modo simile utilizzando un collegamento dedicato o un tunnel VPN IPSec.

Per la convalida della soluzione, abbiamo utilizzato l’ambiente illustrato nella figura seguente.



On-premise, avevamo più VLAN per la gestione, host di sessione desktop remoto e così via. Si trovavano nella subnet 172.21.146-150.0/24 e venivano instradati alla rete aziendale utilizzando il servizio di accesso di routing remoto Microsoft. Abbiamo anche eseguito le seguenti attività:

1. Abbiamo preso nota dell'IP pubblico di Microsoft Routing and Remote Access Server (RRAS), identificato con IPchicken.com.
2. Abbiamo creato una risorsa Virtual Network Gateway (VPN basata su routing) con Azure Subscription.
3. È stata creata la connessione che fornisce l'indirizzo del gateway di rete locale per l'IP pubblico del server Microsoft RRAS.
4. Abbiamo completato la configurazione VPN su RRAS per creare un'interfaccia virtuale utilizzando l'autenticazione pre-condivisa fornita durante la creazione del gateway VPN. Se configurata correttamente, la VPN deve trovarsi nello stato connesso. Invece di Microsoft RRAS, è possibile utilizzare pfSense o altri strumenti pertinenti per creare il tunnel VPN IPSec sito-sito. Poiché è basato su route, il tunnel reindirizza il traffico in base alle subnet specifiche configurate.

Microsoft Azure Active Directory fornisce l'autenticazione dell'identità basata su oAuth. Le autenticazioni dei client aziendali richiedono in genere l'autenticazione basata su NTLM o Kerberos. I servizi di dominio Active Directory di Microsoft Azure eseguono la sincronizzazione dell'hash delle password tra Azure Active Directory e i controller di dominio on-premise utilizzando ADConnect.

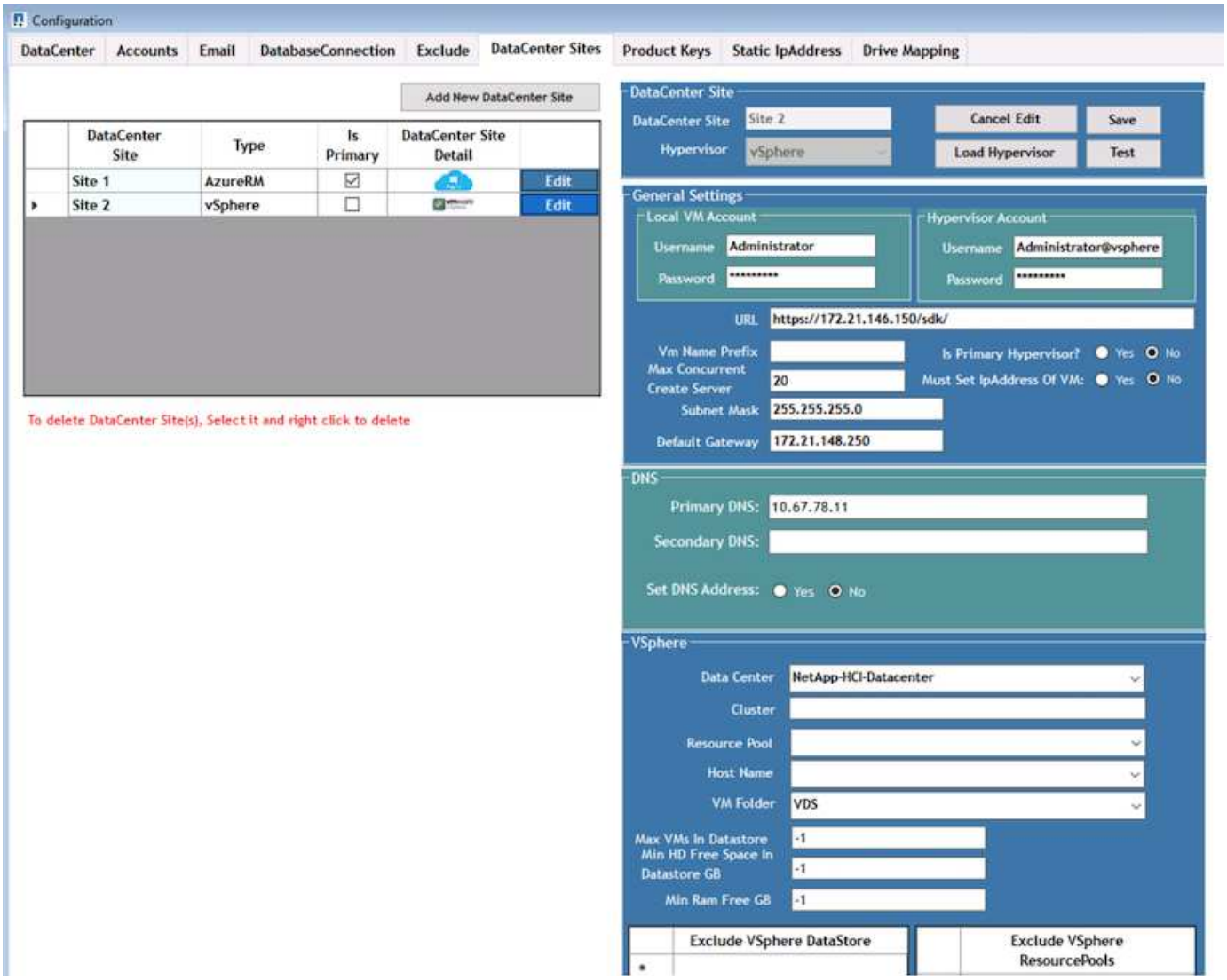
Per la convalida di questa soluzione VDS ibrida, abbiamo inizialmente implementato Microsoft Azure e aggiunto un sito aggiuntivo con vSphere. Il vantaggio di questo approccio è che i servizi della piattaforma sono stati implementati in Microsoft Azure e quindi sono stati prontamente sottoposti a backup utilizzando il portale. È quindi possibile accedere facilmente ai servizi da qualsiasi luogo, anche se il collegamento VPN del sito non è attivo.

Per aggiungere un altro sito, abbiamo utilizzato uno strumento chiamato DCConfig. Il collegamento a tale applicazione è disponibile sul desktop della macchina virtuale CWMgr (Cloud Workspace Manager). Una volta avviata l'applicazione, accedere alla scheda DataCenter Sites (Siti DataCenter), aggiungere il nuovo sito del

data center e inserire le informazioni richieste come mostrato di seguito. L'URL punta all'IP vCenter. Assicurarsi che la macchina virtuale CWMgr possa comunicare con vCenter prima di aggiungere la configurazione.

> Assicurarsi che vSphere PowerCLI 5.1 su CloudWorkspace Manager sia installato per consentire la comunicazione con l'ambiente VMware vSphere.

La seguente figura illustra la configurazione del sito del data center on-premise.



Tenere presente che sono disponibili opzioni di filtraggio per le risorse di calcolo in base al cluster specifico, al nome host o allo spazio libero della RAM. Le opzioni di filtraggio per le risorse di storage includono lo spazio libero minimo sugli archivi dati o il numero massimo di macchine virtuali per archivio dati. Gli archivi di dati possono essere esclusi utilizzando espressioni regolari. Fare clic sul pulsante Save (Salva) per salvare la configurazione.

Per convalidare la configurazione, fare clic sul pulsante Test o fare clic su Load Hypervisor (carica hypervisor) e selezionare un menu a discesa nella sezione vSphere. Deve essere compilato con i valori appropriati. È consigliabile mantenere l'hypervisor primario impostato su yes per il sito di provisioning predefinito.

I modelli di macchine virtuali creati su VMware vSphere vengono utilizzati come raccolte di provisioning su VDS. Le raccolte di provisioning sono disponibili in due forme: Condivisa e VDI. Il tipo di raccolta di

provisioning condiviso viene utilizzato per i servizi di desktop remoto per i quali viene applicata una singola policy di risorse a tutti i server. Il tipo di VDI viene utilizzato per le istanze di WVD per le quali il criterio di risorsa viene assegnato singolarmente. Ai server di una raccolta di provisioning può essere assegnato uno dei tre ruoli seguenti:

- **TSDATA.** combinazione di servizi terminal e ruolo del server dati.
- **TS.** servizi terminal (host di sessione).
- **DATA.** file server o database server. Quando si definisce il ruolo del server, è necessario scegliere il modello di macchina virtuale e lo storage (datastore). Il datastore scelto può essere limitato a un datastore specifico oppure è possibile utilizzare l'opzione meno utilizzata in cui il datastore viene scelto in base all'utilizzo dei dati.

Ogni implementazione dispone di risorse VM predefinite per l'allocazione delle risorse cloud in base a utenti attivi, fissi, carico del server o numero di utenti.

Test di carico di un singolo server con Login VSI

Il NetApp Virtual Desktop Service utilizza il protocollo Microsoft Remote Desktop per accedere alle sessioni e alle applicazioni del desktop virtuale, mentre il tool Login VSI determina il numero massimo di utenti che possono essere ospitati su un modello di server specifico. Login VSI simula l'accesso dell'utente a intervalli specifici ed esegue operazioni dell'utente come l'apertura di documenti, la lettura e la composizione di e-mail, l'utilizzo di Excel e PowerPoint, la stampa di documenti, la compressione dei file e l'esecuzione di interruzioni casuali. Quindi, misura i tempi di risposta. I tempi di risposta dell'utente sono bassi quando l'utilizzo del server è basso e aumentano quando vengono aggiunte più sessioni dell'utente. Login VSI determina la linea di base in base alle sessioni di accesso utente iniziali e riporta la sessione utente massima quando la risposta dell'utente supera i 2 secondi dalla linea di base.

NetApp Virtual Desktop Service utilizza Microsoft Remote Desktop Protocol per accedere alle applicazioni e alle sessioni di Virtual Desktop. Per determinare il numero massimo di utenti che possono essere ospitati su un modello di server specifico, è stato utilizzato il tool Login VSI. Login VSI simula l'accesso dell'utente a intervalli specifici ed esegue operazioni dell'utente come l'apertura di documenti, la lettura e la composizione di e-mail, l'utilizzo di Excel e PowerPoint, la stampa di documenti, la compressione di file, l'esecuzione di interruzioni casuali e così via. Inoltre, misura i tempi di risposta. I tempi di risposta dell'utente sono bassi quando l'utilizzo del server è basso e aumentano quando vengono aggiunte più sessioni dell'utente. Login VSI determina la linea di base in base alle sessioni di accesso utente iniziali e riporta il numero massimo di sessioni utente quando la risposta dell'utente supera i 2 secondi dalla linea di base.

La seguente tabella contiene l'hardware utilizzato per questa convalida.

Modello	Conta	Descrizione
NetApp HCI H610C	4	Tre in un cluster per i lanciatori, ad, DHCP e così via. Un server per il test del carico.
NetApp HCI H615C	1	2 x 24 C Intel Xeon Gold 6282 @2,1 GHz. 1,5 TB DI RAM.

La seguente tabella contiene il software utilizzato per la convalida.

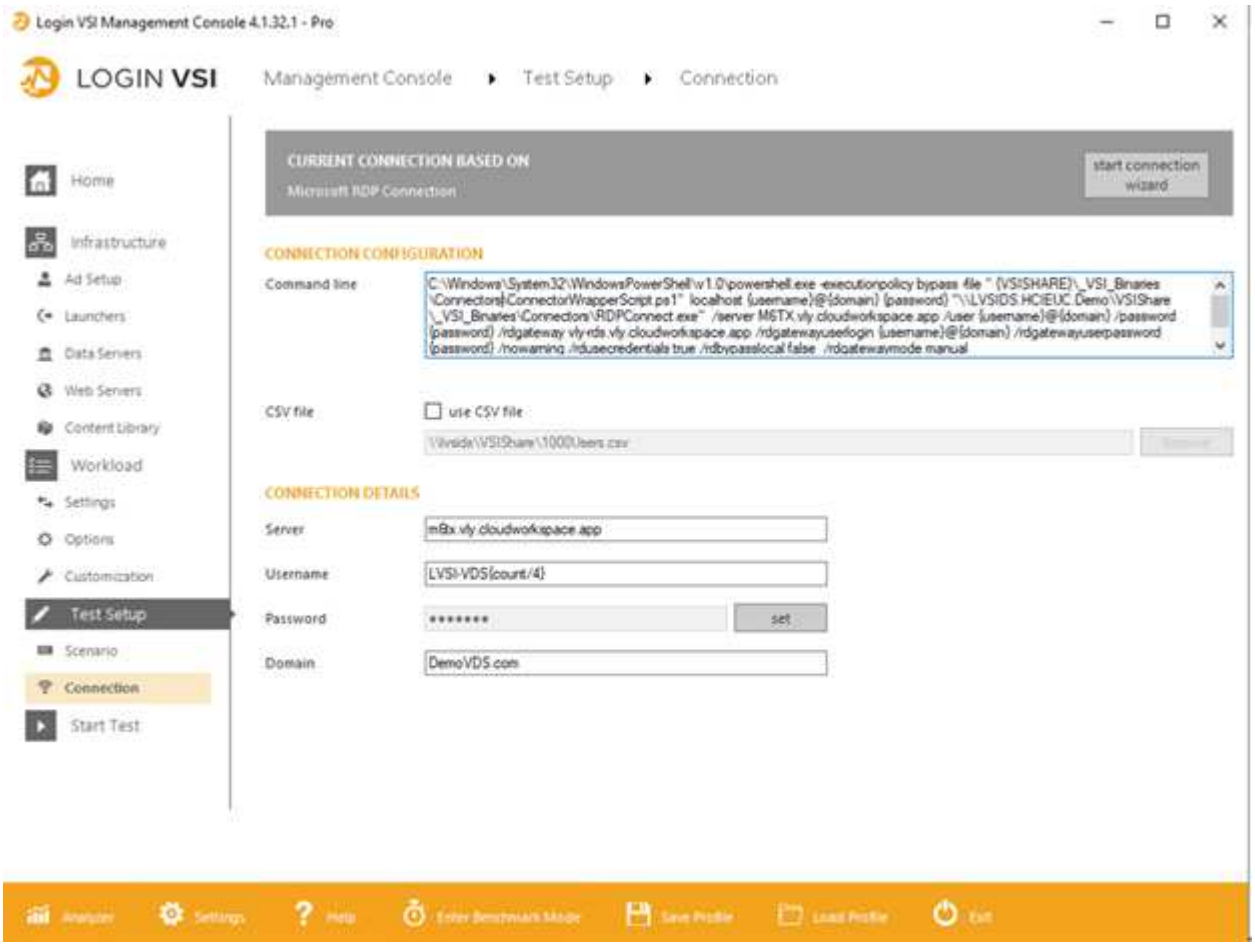
Prodotto	Descrizione
NetApp VDS 5.4	Orchestrazione
Modelli di macchine virtuali Windows 2019 1809	Sistema operativo server per RDSH
Accedere a VSI	4.1.32.1
VMware vSphere 6.7 Update 3	Hypervisor
VMware vCenter 6.7 Update 3f	Tool di gestione VMware

I risultati del test Login VSI sono i seguenti:

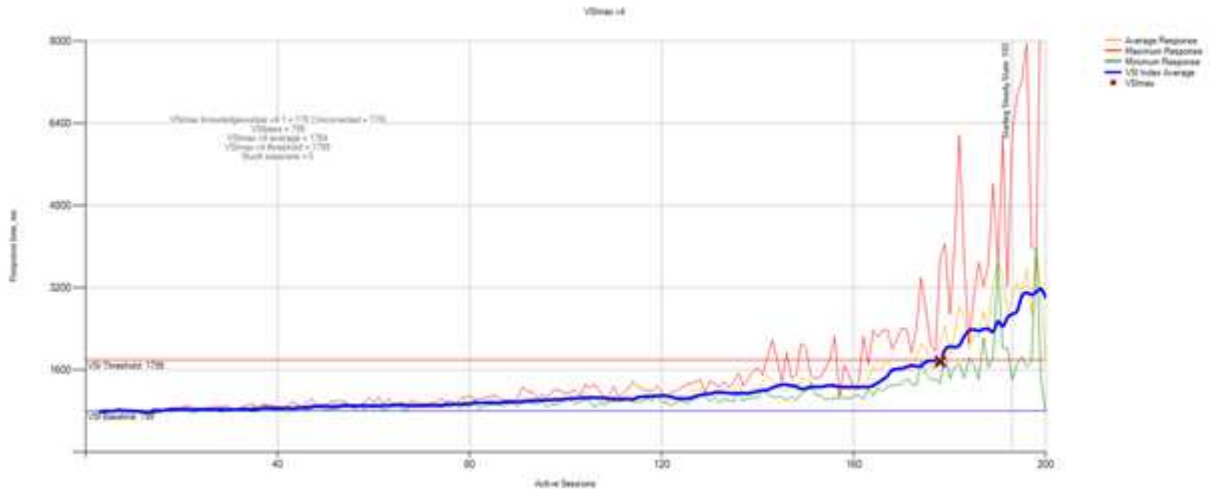
Modello	Configurazione delle macchine virtuali	Accesso VSI baseline	Accesso VSI Max
H610C	8 vCPU, 48 GB di RAM, disco da 75 GB, profilo 8Q vGPU	799	178
H615C	12 vCPU, 128 GB di RAM, disco da 75 GB	763	272

Considerando i limiti inferiori a NUMA e l'hyperthreading, le otto macchine virtuali scelte per il test e la configurazione delle macchine virtuali dipendono dai core disponibili sull'host.

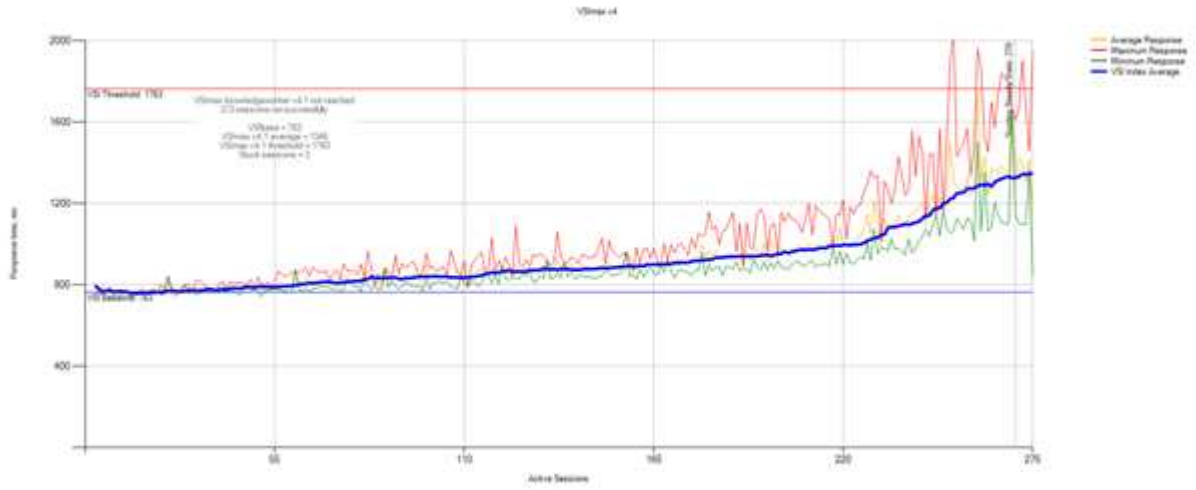
Abbiamo utilizzato 10 macchine virtuali di avvio sull'H610C, che utilizzavano il protocollo RDP per connettersi alla sessione utente. La figura seguente mostra le informazioni di connessione Login VSI.



La figura seguente mostra il tempo di risposta di Login VSI rispetto alle sessioni attive per H610C.



La figura seguente mostra il tempo di risposta di Login VSI rispetto alle sessioni attive per H615C.



Le metriche delle performance di Cloud Insights durante il test VSI di accesso H615C per host vSphere e macchine virtuali sono illustrate nella figura seguente.

Portale di gestione

È disponibile il portale NetApp VDS Cloud Workspace Management Suite "qui" e la prossima versione è disponibile "qui".

Il portale consente la gestione centralizzata di varie implementazioni VDS, tra cui una con siti definiti per utenti on-premise, amministrativi, catalogo di applicazioni ed eventi con script. Il portale viene utilizzato anche dagli utenti amministrativi per il provisioning manuale delle applicazioni, se necessario, e per la connessione a qualsiasi computer per la risoluzione dei problemi.

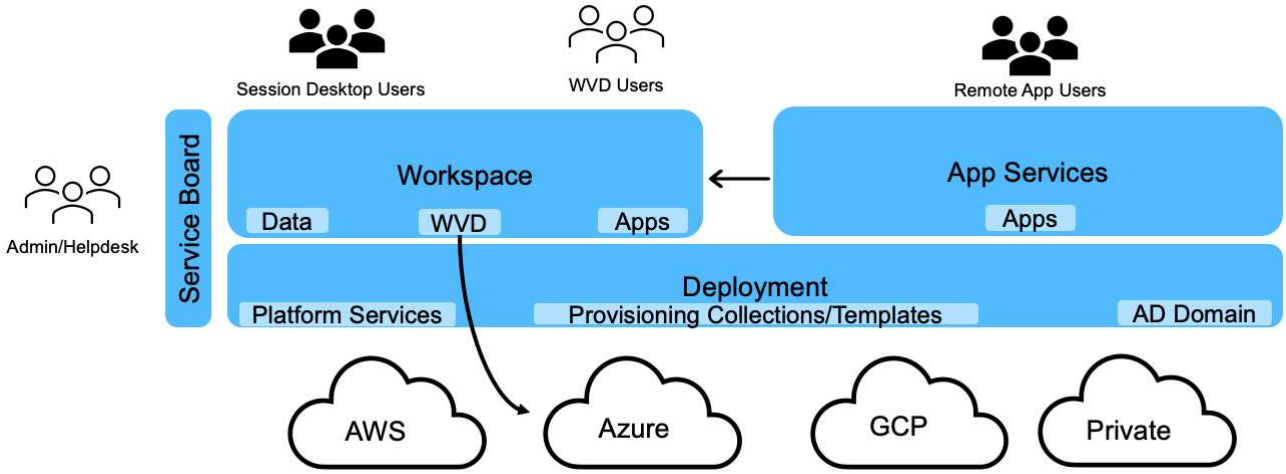
I service provider possono utilizzare questo portale per aggiungere i propri partner di canale e consentire loro di gestire i propri client.

Gestione utenti

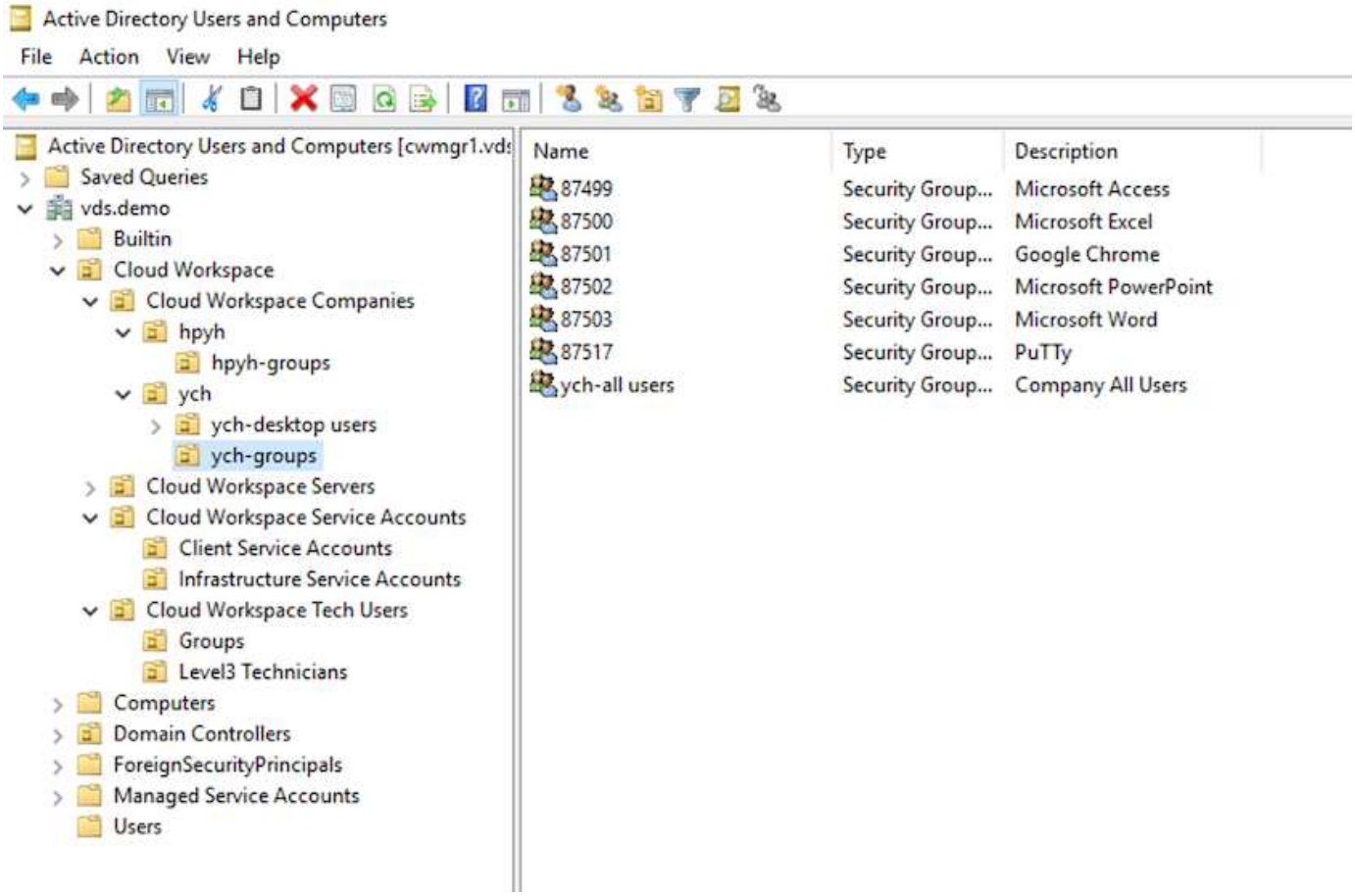
NetApp VDS utilizza Azure Active Directory per l'autenticazione dell'identità e Azure Active Directory Domain Services per l'autenticazione NTLM/Kerberos. Lo strumento ADConnect può essere utilizzato per sincronizzare un dominio Active Directory on-premise con Azure Active Directory.

È possibile aggiungere nuovi utenti dal portale oppure attivare lo spazio di lavoro cloud per gli utenti esistenti. Le autorizzazioni per le aree di lavoro e i servizi applicativi possono essere controllate da singoli utenti o da gruppi. Dal portale di gestione, è possibile definire gli utenti amministrativi per controllare le autorizzazioni per il portale, le aree di lavoro e così via.

La seguente figura illustra la gestione degli utenti in NetApp VDS.



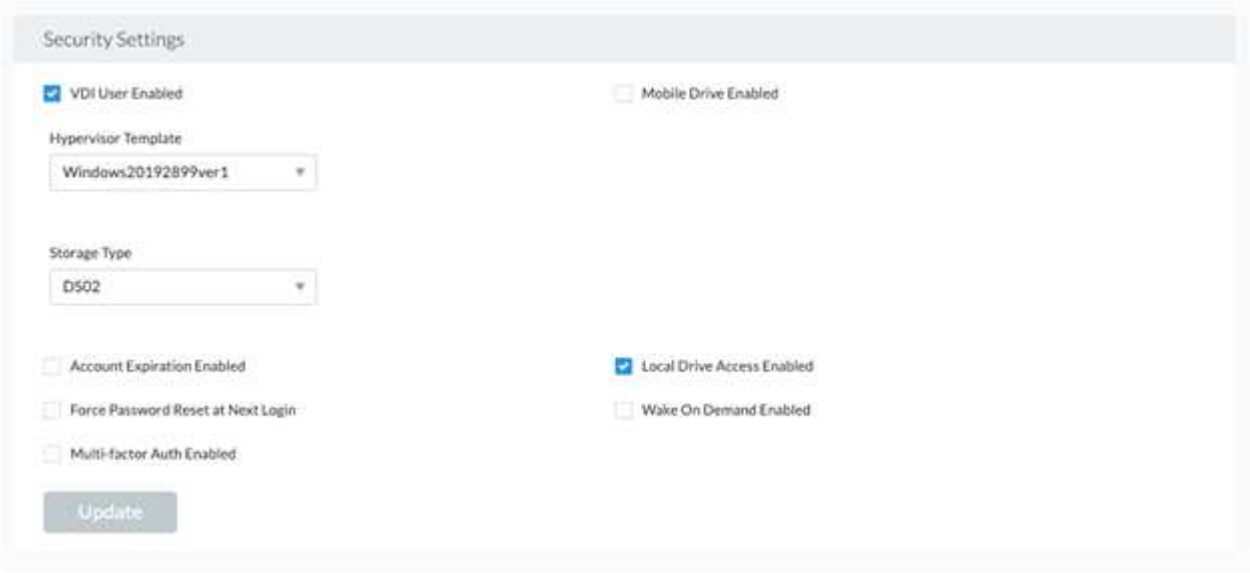
Ogni area di lavoro risiede nella propria unità organizzativa (OU) di Active Directory sotto l'unità organizzativa Cloud Workspace, come illustrato nella figura seguente.



Per ulteriori informazioni, vedere "questo video" Sulle autorizzazioni degli utenti e sulla gestione degli utenti in NetApp VDS.

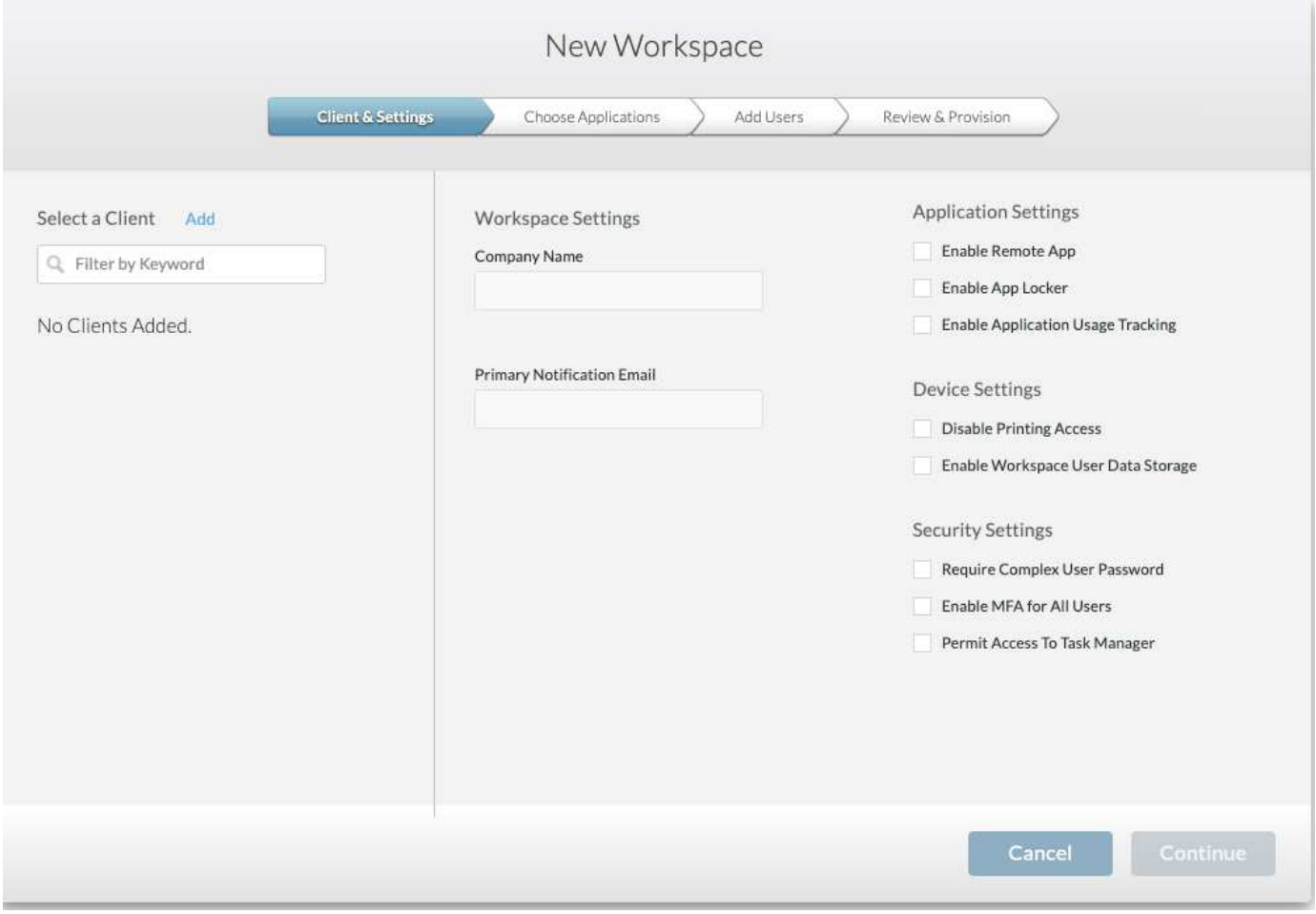
Quando un gruppo Active Directory viene definito come CRAUserGroup utilizzando una chiamata API per il data center, tutti gli utenti di tale gruppo vengono importati in CloudWorkspace per la gestione mediante l'interfaccia utente. Quando l'area di lavoro cloud è attivata per l'utente, VDS crea le cartelle principali dell'utente, i permessi delle impostazioni, gli aggiornamenti delle proprietà dell'utente e così via.

Se l’opzione VDI User Enabled (utente VDI abilitato) è selezionata, VDS crea una macchina RDS a sessione singola dedicata a tale utente. Richiede il provisioning del modello e del datastore.



Gestione dell’area di lavoro

Un’area di lavoro è costituita da un ambiente desktop, che può essere condiviso in sessioni di desktop remoto ospitate on-premise o in qualsiasi ambiente cloud supportato. Con Microsoft Azure, l’ambiente desktop può essere persistente con i desktop virtuali Windows. Ogni area di lavoro è associata a un’organizzazione o a un client specifico. Le opzioni disponibili durante la creazione di una nuova area di lavoro sono illustrate nella figura seguente.



Ogni area di lavoro è associata a un'implementazione specifica.

Le aree di lavoro contengono applicazioni e servizi app associati, cartelle di dati condivise, server e un'istanza WVD. Ogni area di lavoro può controllare le opzioni di sicurezza come l'applicazione della complessità delle password, l'autenticazione a più fattori, i controlli dei file e così via.

Le aree di lavoro possono controllare la pianificazione del carico di lavoro per accendere server aggiuntivi, limitare il numero di utenti per server o impostare la pianificazione delle risorse disponibili per un determinato periodo (sempre acceso/spento). Le risorse possono anche essere configurate per l'attivazione on-demand.

Se necessario, lo spazio di lavoro può sostituire le impostazioni predefinite delle risorse delle macchine virtuali di implementazione. Per WVD, i pool di host WVD (che contengono host di sessione e gruppi di applicazioni) e le aree di lavoro WVD possono essere gestiti anche dal portale della suite di gestione dell'area di lavoro cloud. Per ulteriori informazioni sul pool di host WVD, consultare questa sezione "video".

Gestione delle applicazioni

I task worker possono avviare rapidamente un'applicazione dall'elenco di applicazioni disponibili. I servizi app pubblicano le applicazioni dagli host della sessione di servizi Desktop remoto. Con WVD, i gruppi di applicazioni offrono funzionalità simili dai pool di host di Windows 10 a più sessioni.

Per consentire agli impiegati di potenziare gli utenti, è possibile eseguire il provisioning manuale delle applicazioni necessarie utilizzando una scheda di servizio oppure eseguire il provisioning automatico utilizzando la funzionalità di script degli eventi di NetApp VDS.

Per ulteriori informazioni, consultare "Pagina NetApp Application Entitlement".

Funzionalità di ONTAP per il servizio di desktop virtuale

Le seguenti funzionalità di ONTAP lo rendono una scelta interessante da utilizzare con un servizio di desktop virtuale.

- **Filesystem scale-out.** i volumi ONTAP FlexGroup possono crescere fino a oltre 20 PB e possono contenere più di 400 miliardi di file all'interno di un singolo namespace. Il cluster può contenere fino a 24 nodi di storage, ciascuno con un numero flessibile di schede di interfaccia di rete a seconda del modello utilizzato.

  I desktop virtuali, le cartelle home, i container dei profili utente, i dati condivisi e così via possono crescere in base alla domanda senza alcuna preoccupazione per le limitazioni del file system.

- **Analisi del file system.** puoi utilizzare il tool XCP per ottenere informazioni sui dati condivisi. Con ONTAP 9.8+ e ActiveIQ Unified Manager, è possibile eseguire query e recuperare facilmente le informazioni sui metadati dei file e identificare i dati cold.
- **Cloud Tiering.** puoi migrare i dati cold in un archivio di oggetti nel cloud o in qualsiasi storage compatibile con S3 nel tuo data center.
- **Versioni dei file.** gli utenti possono ripristinare i file protetti dalle copie Snapshot di NetApp ONTAP. Le copie Snapshot di ONTAP sono molto efficienti in termini di spazio perché registrano solo i blocchi modificati.
- **Namespace globale.** la tecnologia ONTAP FlexCache consente il caching remoto dello storage dei file, semplificando la gestione dei dati condivisi tra ubicazioni contenenti sistemi di storage ONTAP.
- **Supporto multi-tenancy sicuro.** Un singolo cluster di storage fisico può essere presentato come più array di storage virtuali ciascuno con i propri volumi, protocolli di storage, interfacce di rete logiche, dominio di identità e autenticazione, utenti di gestione e così via. Pertanto, è possibile condividere l'array di storage tra più business unit o ambienti, come test, sviluppo e produzione.

  Per garantire le performance, è possibile utilizzare la QoS adattiva per impostare i livelli di performance in base allo spazio utilizzato o allocato e controllare la capacità dello storage utilizzando le quote.

- **Integrazione VMware.** i tool ONTAP per VMware vSphere forniscono un plug-in vCenter per il provisioning dei datastore, l'implementazione delle Best practice per gli host vSphere e il monitoraggio delle risorse ONTAP.

  ONTAP supporta le API vStorage per l'integrazione degli array (VAAI) per l'offload delle operazioni SCSI/file nell'array di storage. ONTAP supporta inoltre le API vStorage per la consapevolezza dello storage (VASA) e il supporto dei volumi virtuali per protocolli a blocchi e file.

  Il plug-in SnapCenter per VMware vSphere offre un metodo semplice per eseguire il backup e il ripristino delle macchine virtuali utilizzando la funzione Snapshot su un array di storage.

  ActiveIQ Unified Manager offre visibilità della rete storage end-to-end in un ambiente vSphere. Gli amministratori possono identificare facilmente qualsiasi problema di latenza che potrebbe verificarsi negli ambienti di desktop virtuali ospitati su ONTAP.

- **Conformità alla sicurezza.** con ActiveIQ Unified Manager, è possibile monitorare più sistemi ONTAP con avvisi per eventuali violazioni delle policy.
- **Supporto multiprotocollo.** ONTAP supporta blocchi (iSCSI, FC, FCoE e NVMe/FC), file (NFSv3, NFSv4.1, SMB2.x e SMB3.x) e protocolli di storage a oggetti (S3).

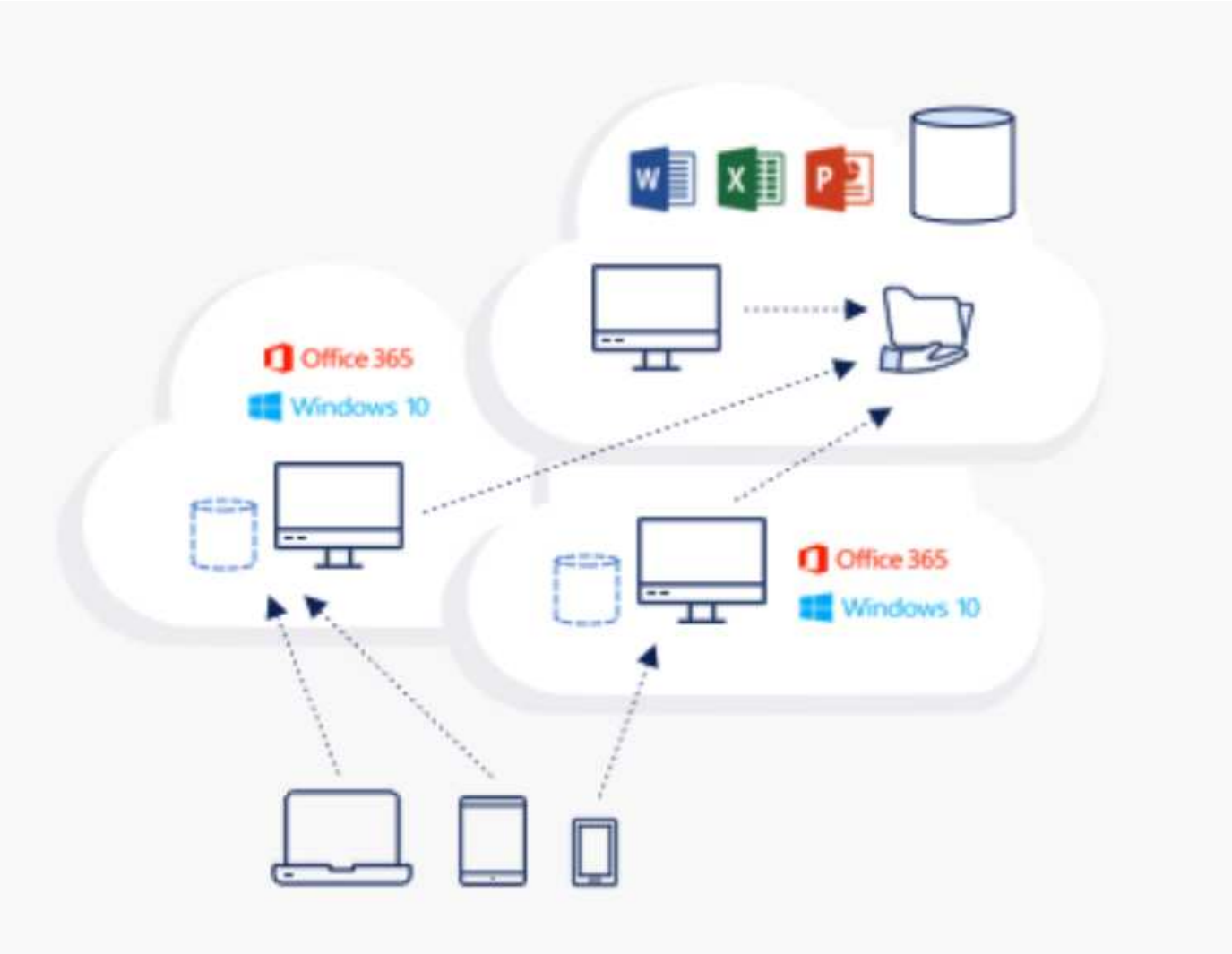
- **Supporto per l'automazione.** ONTAP fornisce moduli REST API, Ansible e PowerShell per automatizzare le attività con il portale di gestione VDS.

Gestione dei dati

Come parte dell'implementazione, è possibile scegliere il metodo di file-service per ospitare il profilo utente, i dati condivisi e la cartella del disco principale. Le opzioni disponibili sono file server, Azure Files o Azure NetApp Files. Tuttavia, dopo l'implementazione, è possibile modificare questa scelta con il tool Command Center per puntare a qualsiasi condivisione SMB. "L'hosting con NetApp ONTAP offre diversi vantaggi". Per informazioni su come modificare la condivisione SMB, consulta "Modifica livello dati".

Global file cache

Quando gli utenti sono distribuiti in più siti all'interno di uno spazio dei nomi globale, Global file cache può contribuire a ridurre la latenza per i dati ad accesso frequente. L'implementazione di Global file cache può essere automatizzata utilizzando una raccolta di provisioning ed eventi con script. Global file cache gestisce le cache di lettura e scrittura a livello locale e mantiene i blocchi dei file in diverse posizioni. Global file cache può funzionare con qualsiasi file server SMB, incluso Azure NetApp Files.



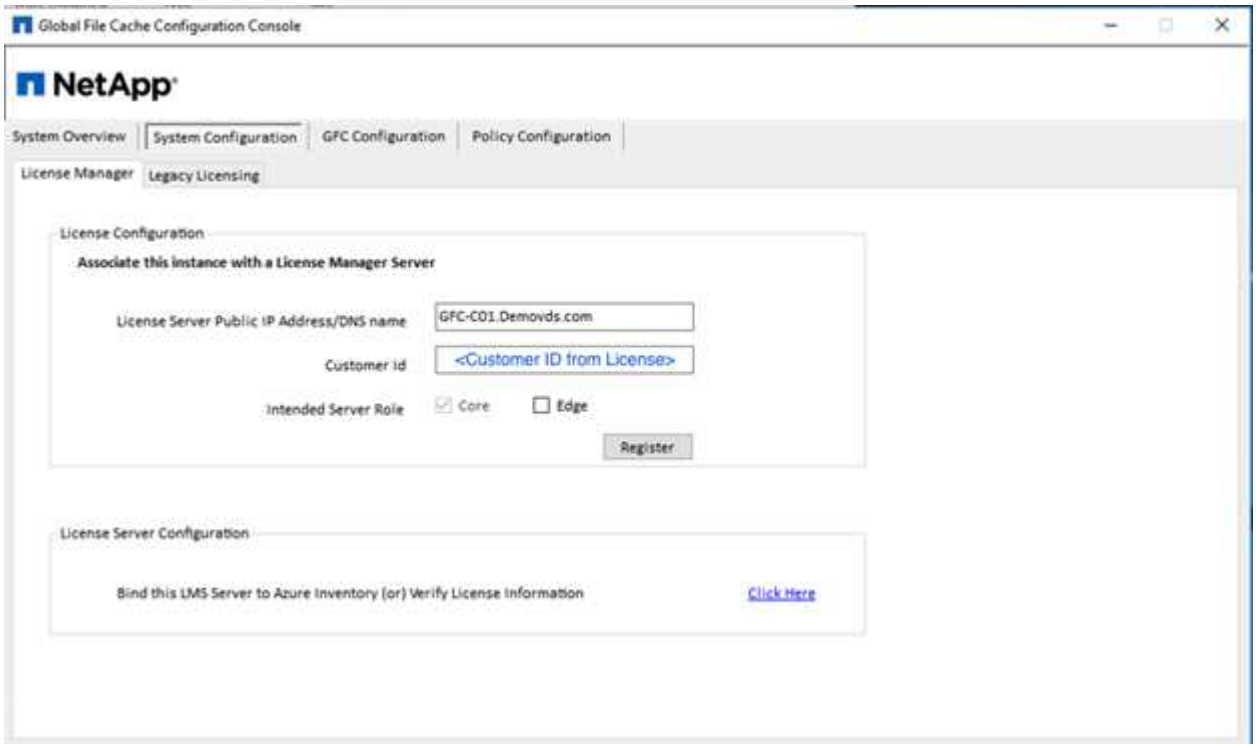
Global file cache richiede quanto segue:

- Server di gestione (server di gestione delle licenze)
- Core
- Edge con capacità disco sufficiente per memorizzare i dati nella cache

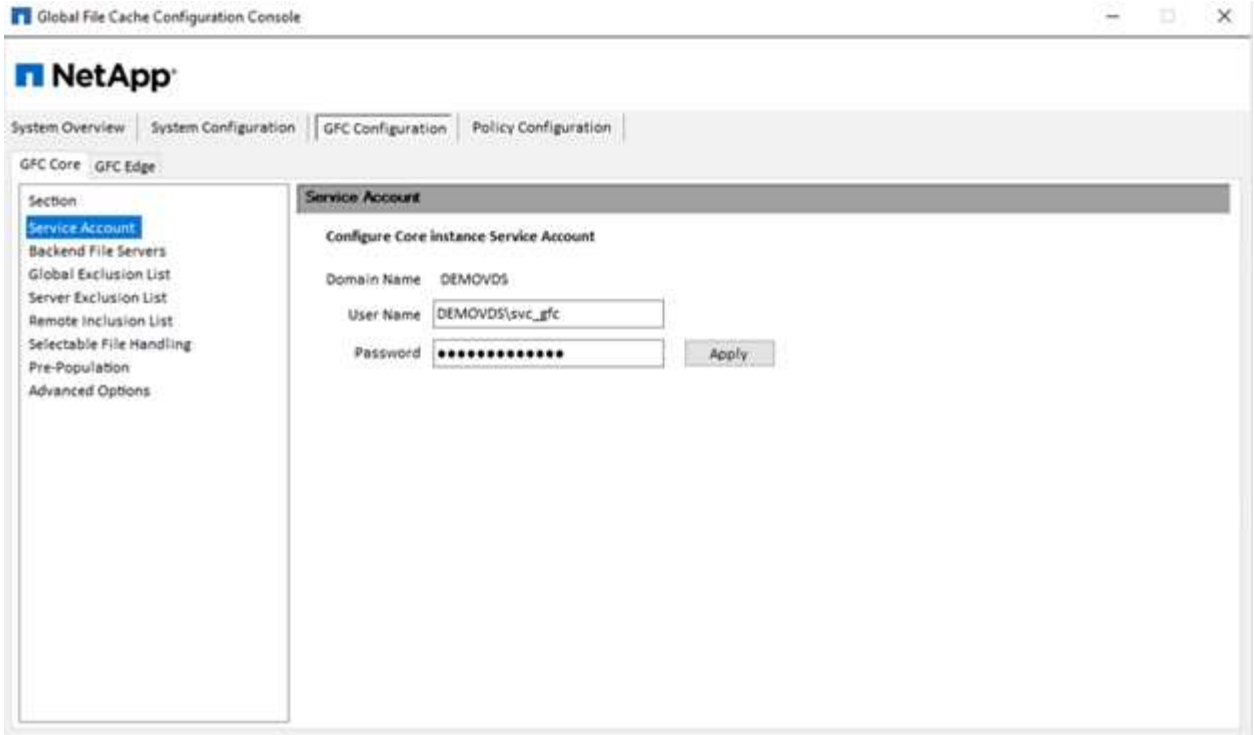
Per scaricare il software e calcolare la capacità della cache del disco per Edge, consultare "Documentazione GFC".

Per la nostra convalida, abbiamo implementato le risorse di base e di gestione sulla stessa macchina virtuale in Azure e le risorse edge in NetApp HCI. Si noti che il core è il luogo in cui è richiesto l'accesso ai dati per volumi elevati e l'edge è un sottoinsieme del core. Una volta installato il software, è necessario attivare la licenza attivata prima dell'uso. A tale scopo, attenersi alla seguente procedura:

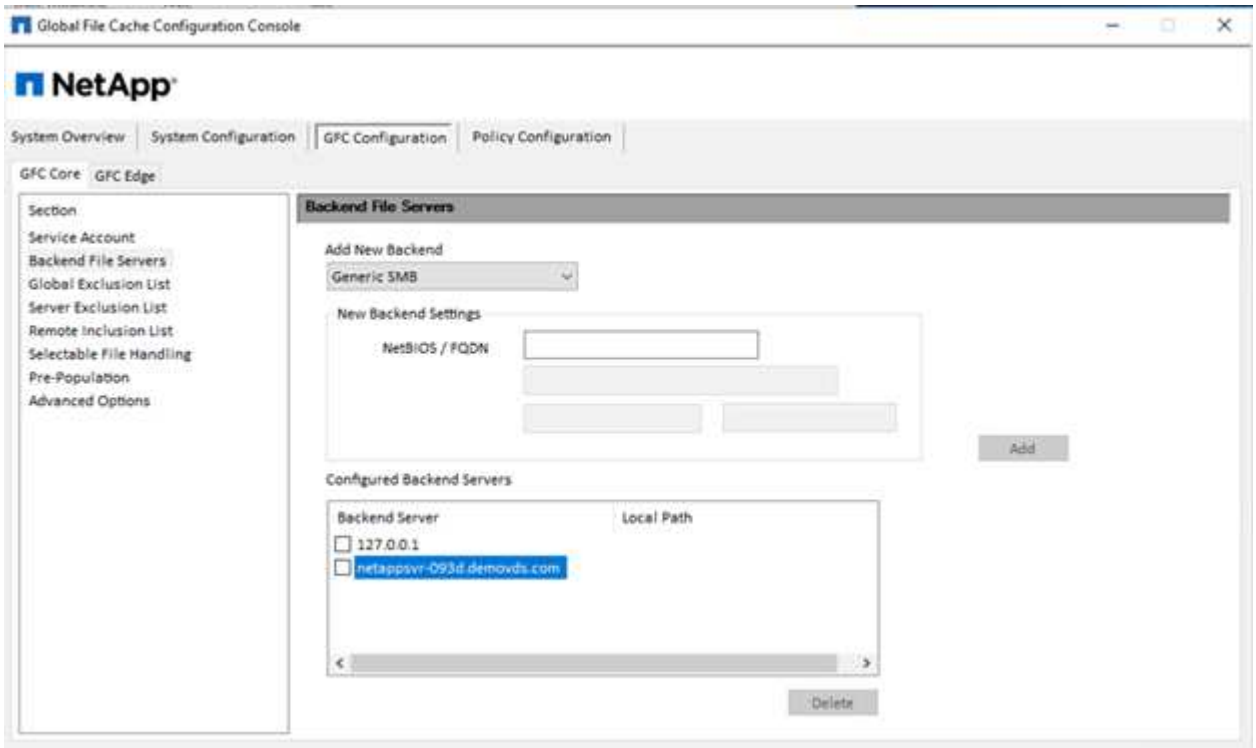
1. Nella sezione License Configuration (Configurazione licenza), utilizzare il collegamento fare clic qui per completare l'attivazione della licenza. Quindi registrare il core.



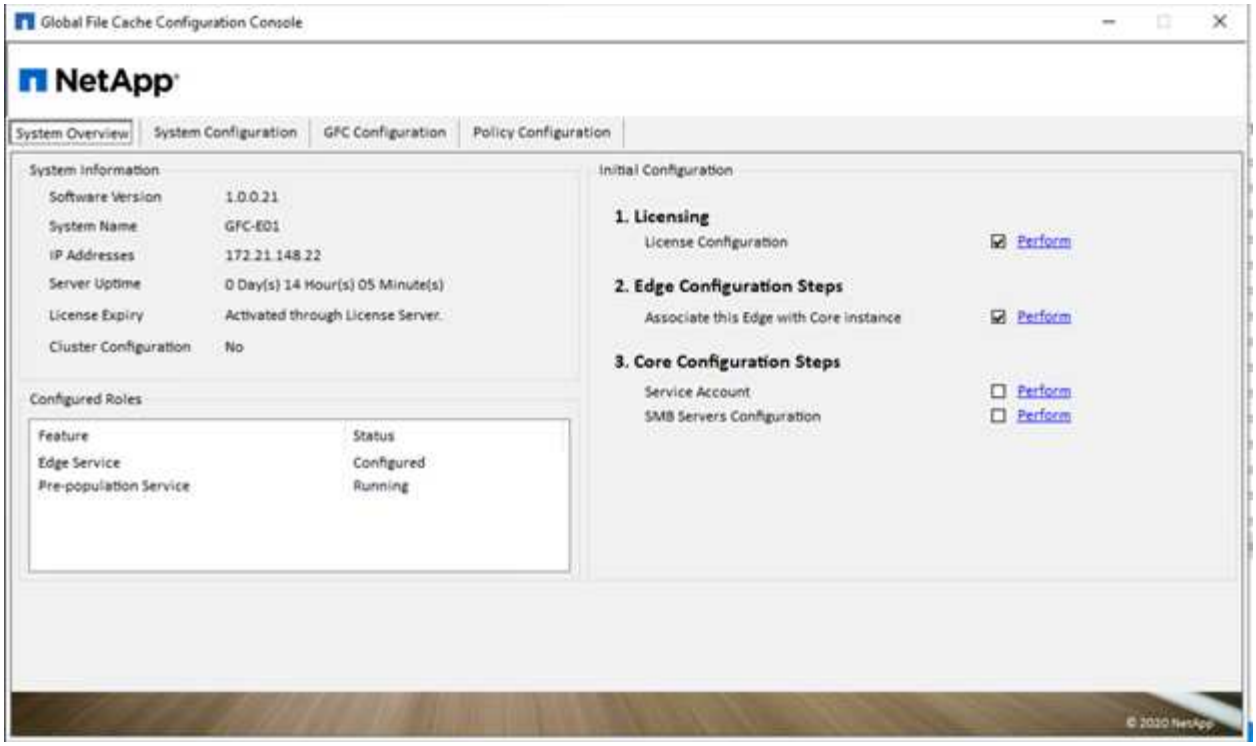
2. Fornire l'account di servizio da utilizzare per Global file cache. Per le autorizzazioni richieste per questo account, consultare "Documentazione GFC".



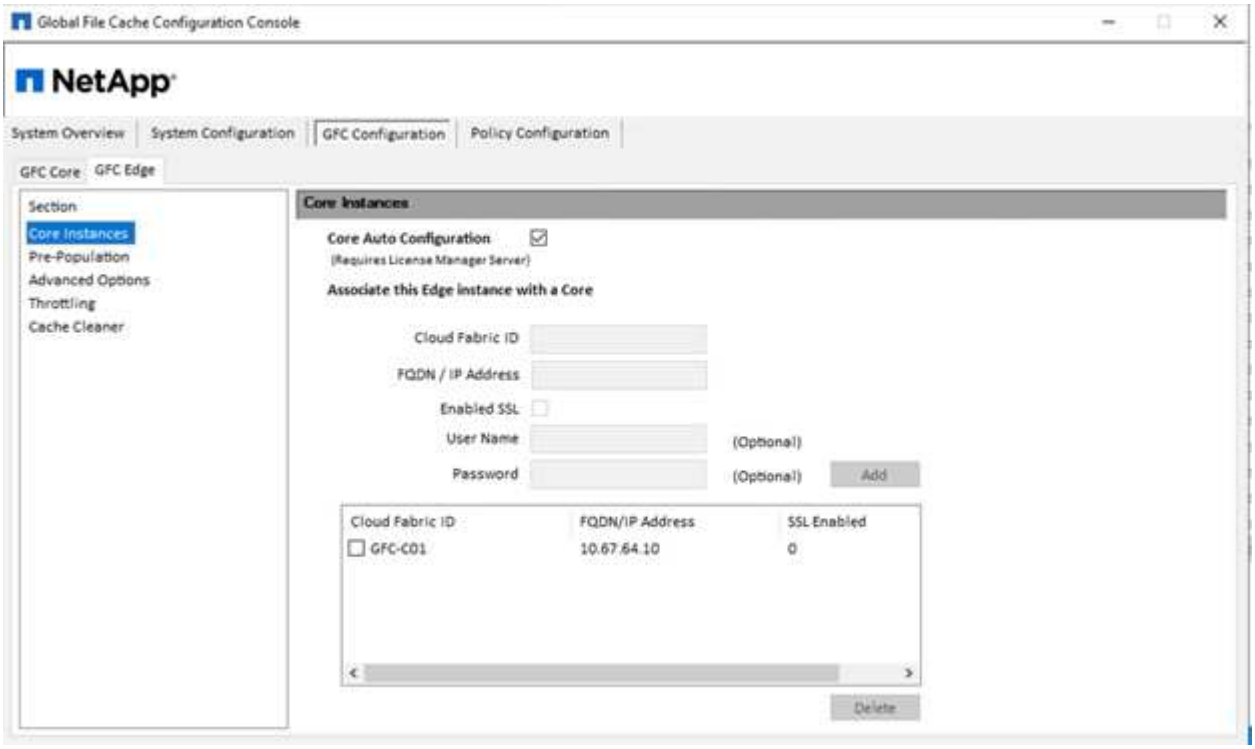
3. Aggiungere un nuovo file server back-end e fornire il nome del file server o l'IP.



4. Sul bordo, l'unità cache deve avere la lettera D. In caso contrario, utilizzare diskpart.exe per selezionare il volume e modificare la lettera dell'unità. Effettuare la registrazione con il server di licenza come edge.

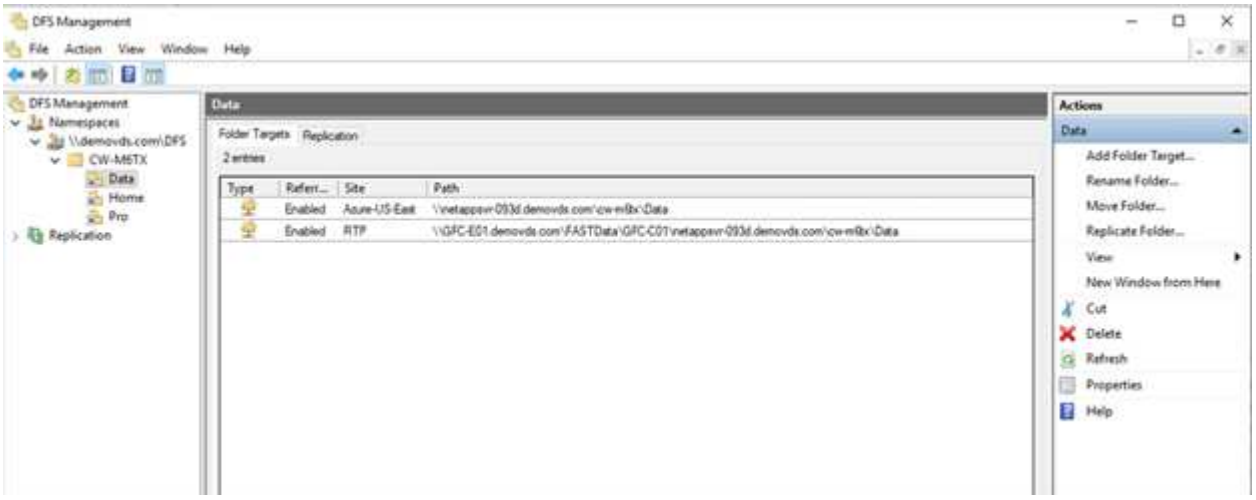


Se la configurazione automatica principale è attivata, le informazioni principali vengono recuperate automaticamente dal server di gestione delle licenze.

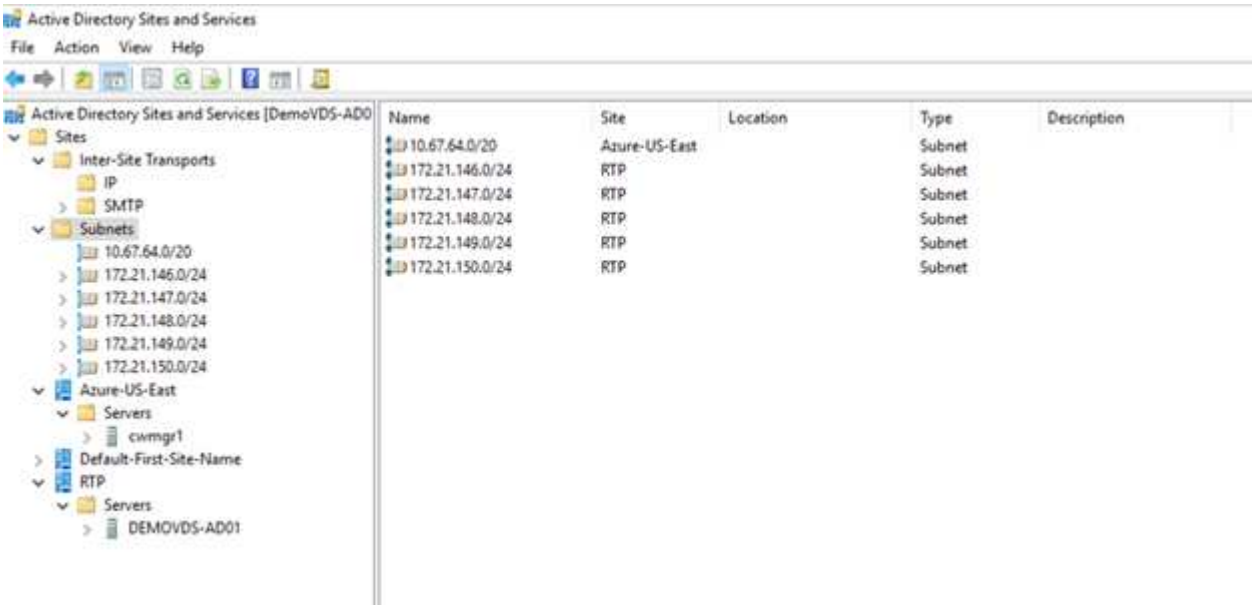


Da qualsiasi computer client, gli amministratori che hanno utilizzato per accedere alla condivisione sul file server possono accedervi con GFC edge utilizzando UNC Path `\\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>`. Gli amministratori possono includere questo percorso nello script di accesso utente o nell'oggetto Criteri di gruppo per la mappatura dei dischi degli utenti nella posizione edge.

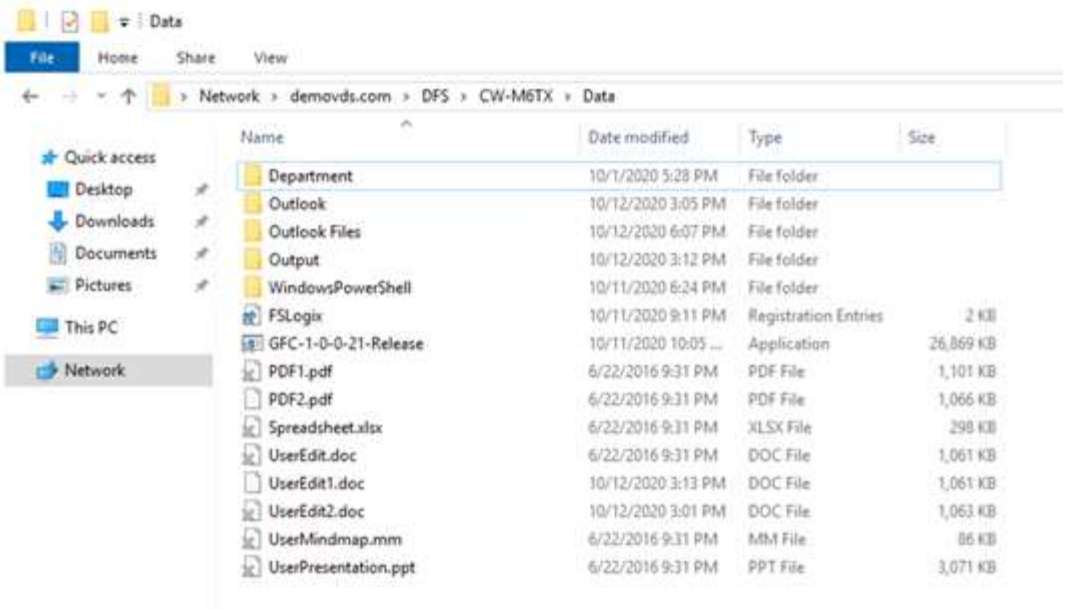
Per fornire un accesso trasparente agli utenti di tutto il mondo, un amministratore può configurare il Microsoft Distributed Filesystem (DFS) con collegamenti che puntano alle condivisioni del file server e alle ubicazioni edge.



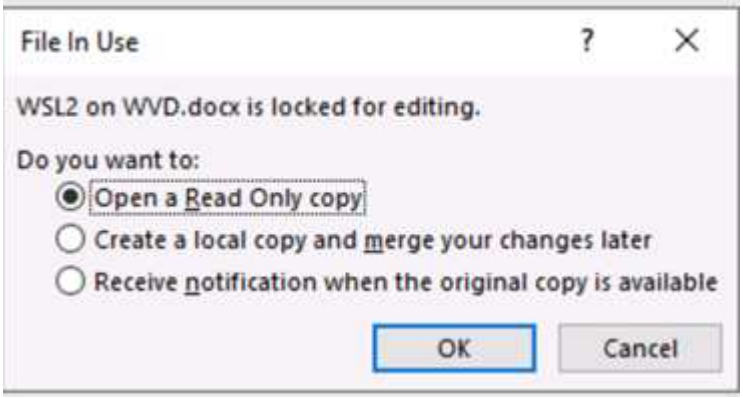
Quando gli utenti accedono con credenziali Active Directory in base alle subnet associate al sito, il client DFS utilizza il collegamento appropriato per accedere ai dati.



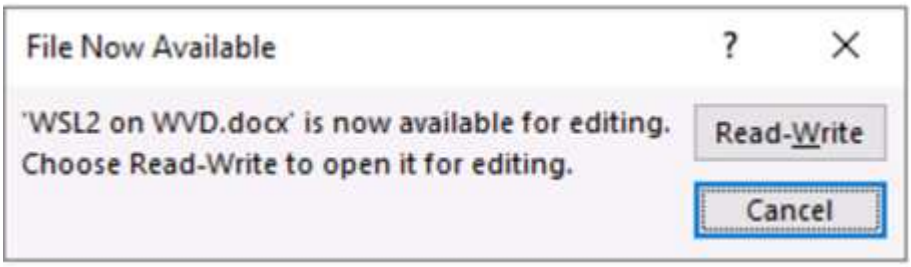
Le icone dei file cambiano a seconda che un file venga memorizzato nella cache; i file non memorizzati nella cache hanno una X grigia nell'angolo inferiore sinistro dell'icona. Dopo che un utente in una posizione edge accede a un file, tale file viene memorizzato nella cache e l'icona cambia.



Quando un file è aperto e un altro utente sta tentando di aprire lo stesso file da una posizione edge, all'utente viene richiesto di selezionare la seguente opzione:



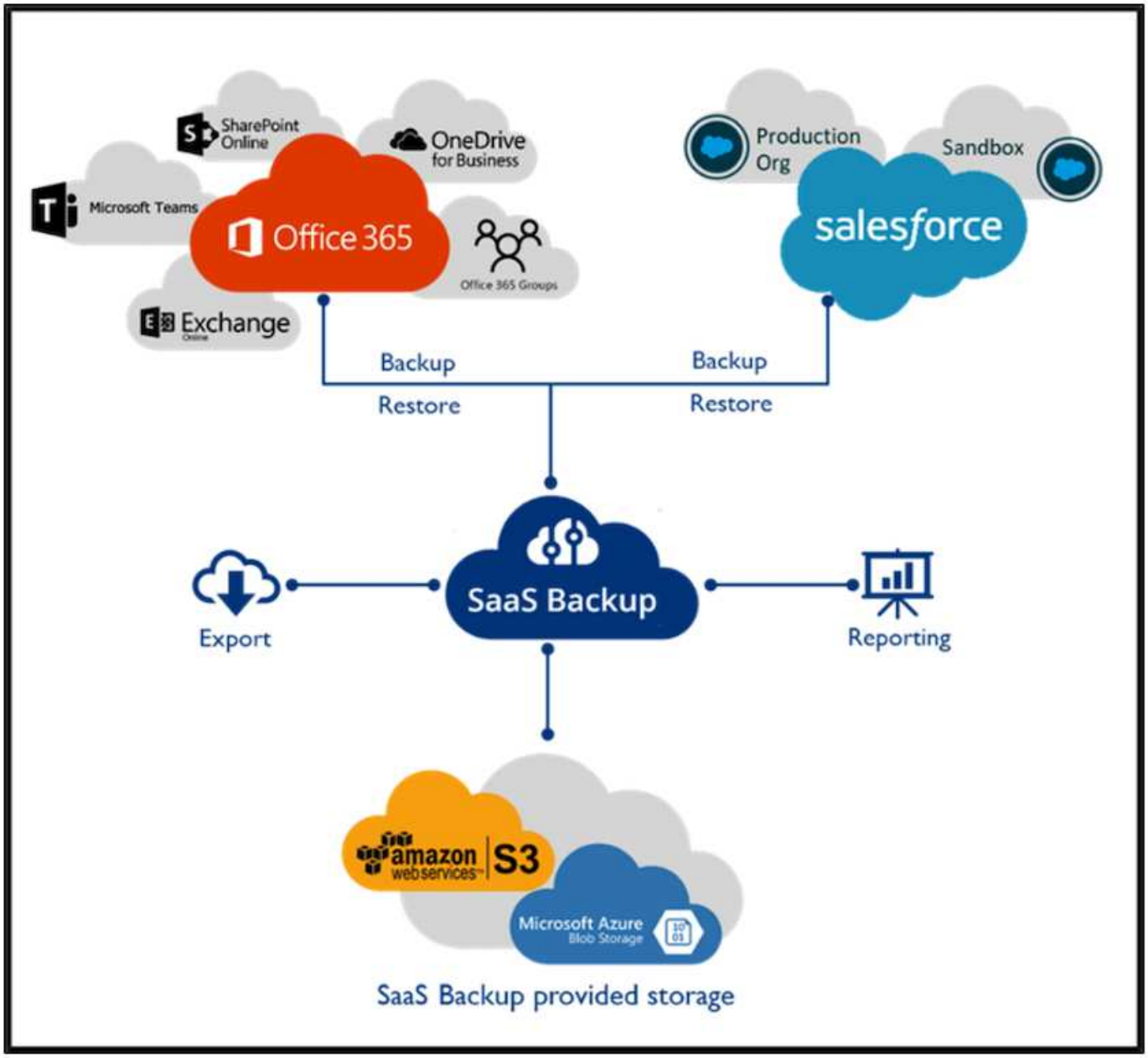
Se l'utente seleziona l'opzione per ricevere una notifica quando la copia originale è disponibile, l'utente riceve una notifica come segue:



Per ulteriori informazioni, consulta questa sezione "Video sull'implementazione di Talon e Azure NetApp Files".

Backup SaaS

NetApp VDS offre protezione dei dati per Salesforce e Microsoft Office 365, inclusi Exchange, SharePoint e Microsoft OneDrive. La figura seguente mostra come NetApp VDS fornisce SaaS Backup per questi servizi dati.



Per una dimostrazione della protezione dei dati di Microsoft Office 365, vedere "questo video".

Per una dimostrazione della protezione dei dati di Salesforce, consulta "questo video".

Gestione delle operazioni

Con NetApp VDS, gli amministratori possono delegare le attività ad altri. Possono connettersi ai server implementati per risolvere i problemi, visualizzare i log ed eseguire i report di audit. Mentre assistono i clienti, l'helpdesk o i tecnici di livello 3 possono affiancare le sessioni degli utenti, visualizzare gli elenchi dei processi e, se necessario, eliminare i processi.

Per informazioni sui file di log VDS, consultare "Risoluzione dei problemi della pagina azioni VDA non riuscite".

Per ulteriori informazioni sulle autorizzazioni minime richieste, vedere "Pagina componenti e autorizzazioni VDA".

Se si desidera clonare manualmente un server, vedere "Pagina cloning Virtual Machines".

Per aumentare automaticamente le dimensioni del disco della macchina virtuale, consultare "Pagina delle funzionalità di aumento automatico dello spazio su disco".

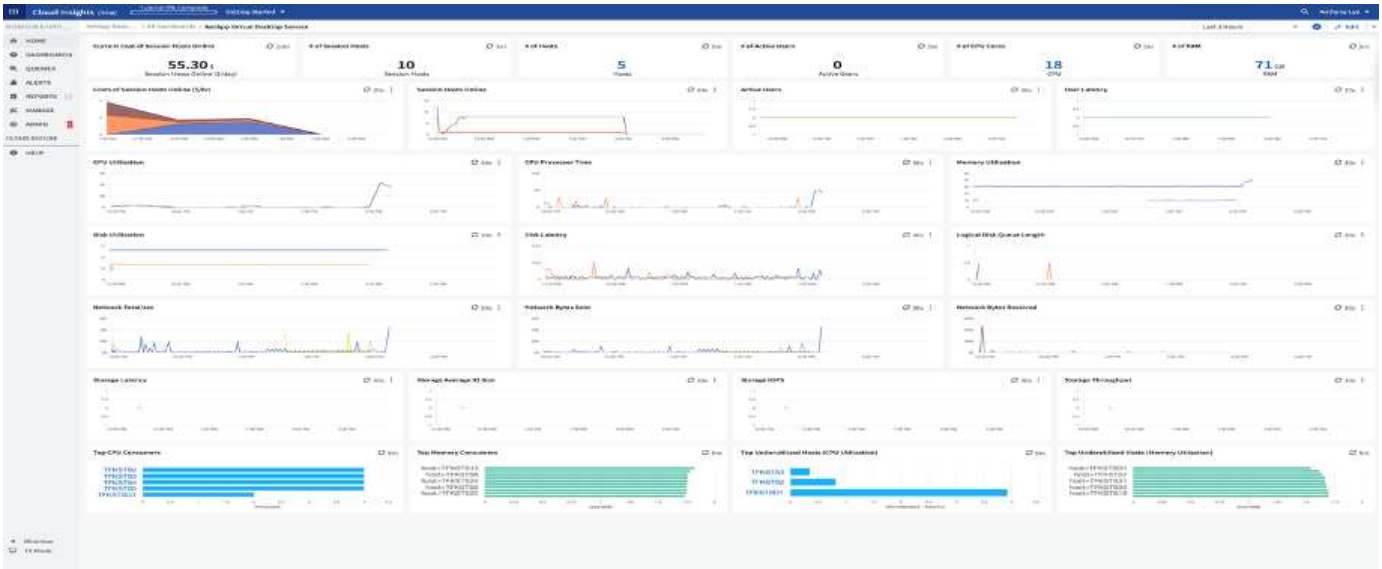
Per identificare l'indirizzo del gateway per la configurazione manuale del client, consultare "Pagina dei requisiti per l'utente finale".

Cloud Insights

NetApp Cloud Insights è uno strumento di monitoraggio basato su web che offre una visibilità completa dell'infrastruttura e delle applicazioni eseguite su NetApp e su altri componenti dell'infrastruttura di terze parti. Cloud Insights supporta cloud privati e pubblici per il monitoraggio, la risoluzione dei problemi e l'ottimizzazione delle risorse.

Solo la macchina virtuale dell'unità di acquisizione (può essere Windows o Linux) deve essere installata su un cloud privato per raccogliere le metriche dai data colleer senza la necessità di agenti. I data raccoglitori basati su agenti consentono di ottenere metriche personalizzate da Windows Performance Monitor o da qualsiasi agente di input supportato da Telegraf.

La figura seguente mostra la dashboard di Cloud Insights VDS.



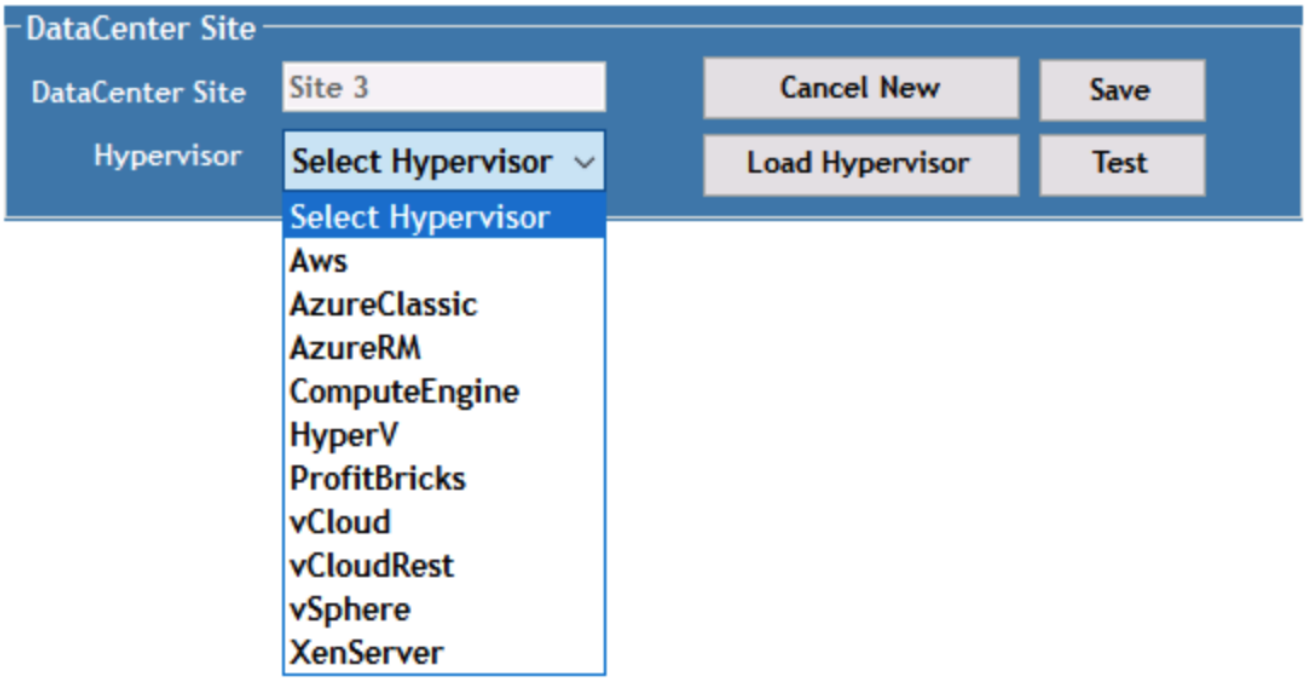
Per ulteriori informazioni su NetApp Cloud Insights, vedere "questo video".

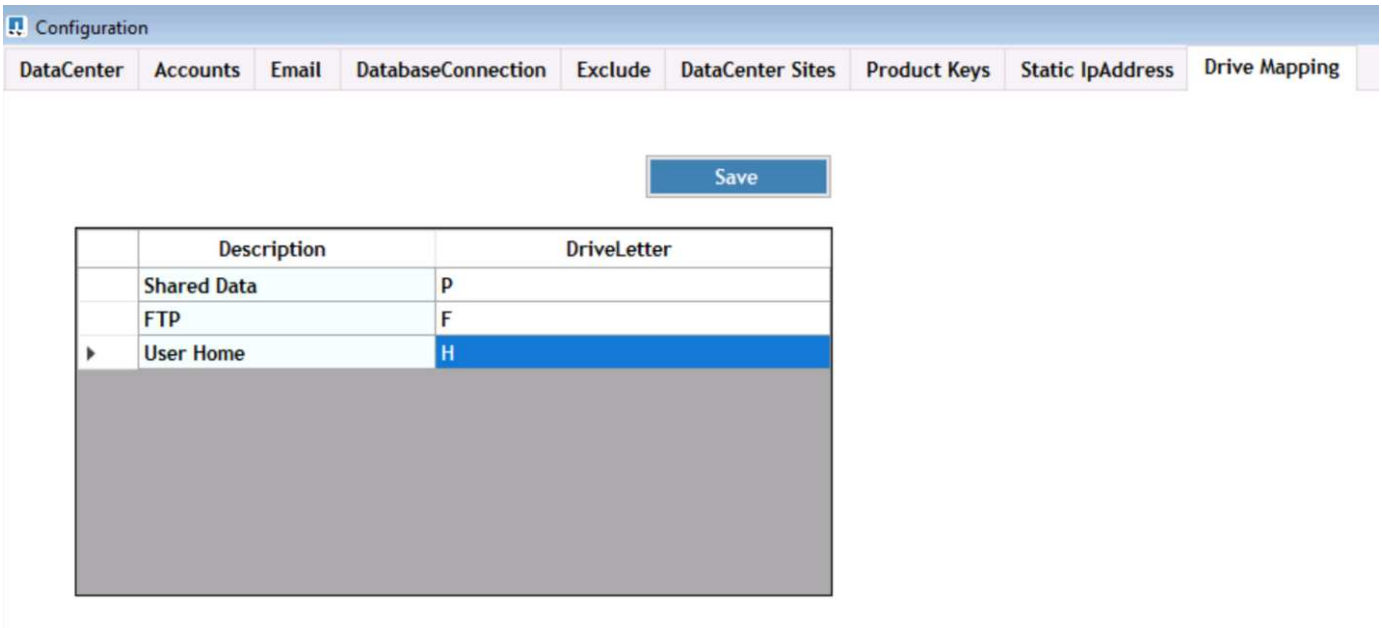
Strumenti e registri

In questa pagina vengono descritti lo strumento DCConfig, gli strumenti TestVdc e i file di log.

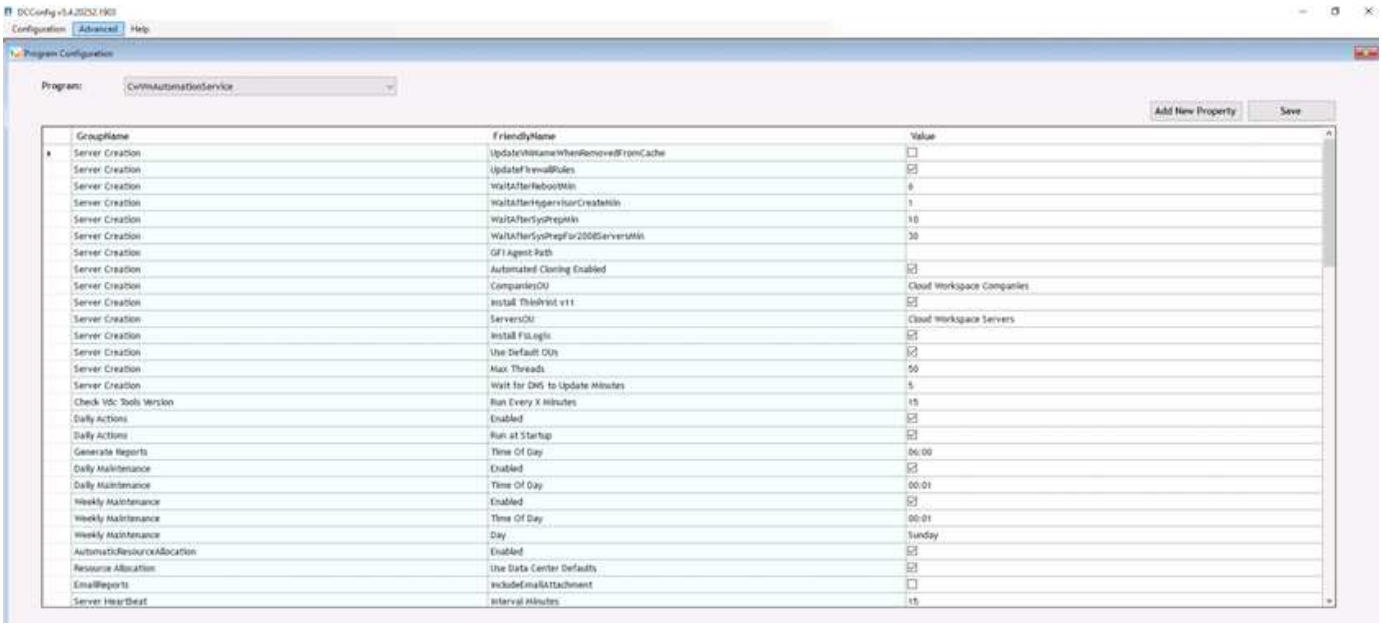
Tool DCConfig

Lo strumento DCCconfig supporta le seguenti opzioni di hypervisor per l'aggiunta di un sito:





È possibile gestire la mappatura delle lettere di unità specifiche dell'area di lavoro per i dati condivisi utilizzando l'oggetto Criteri di gruppo. Professional Services o il team di supporto possono utilizzare la scheda Advanced per personalizzare impostazioni come i nomi delle unità organizzative di Active Directory, l'opzione per attivare o disattivare la distribuzione di FSLogix, vari valori di timeout e così via.

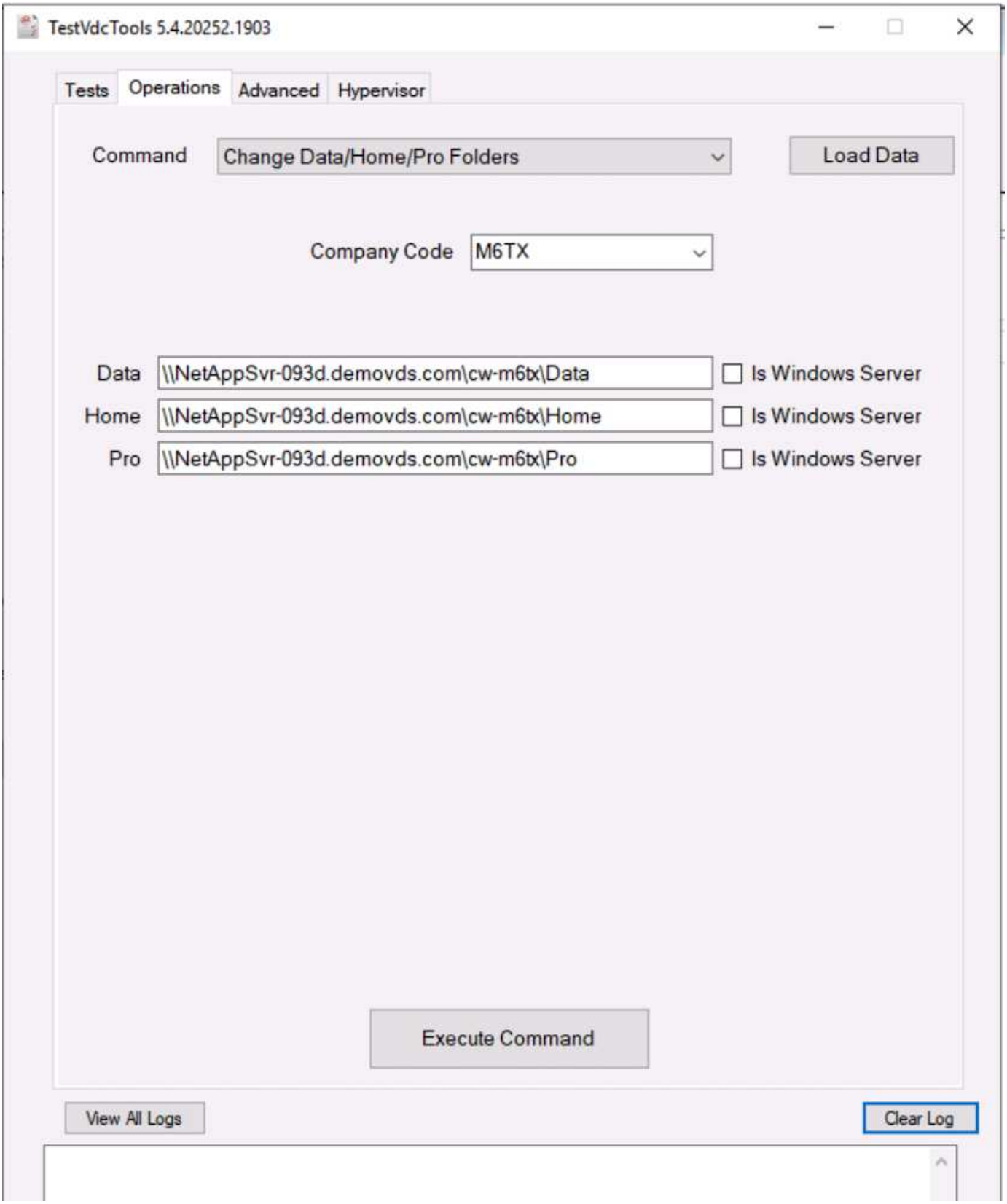


Command Center (precedentemente noto come TestVdc Tools)

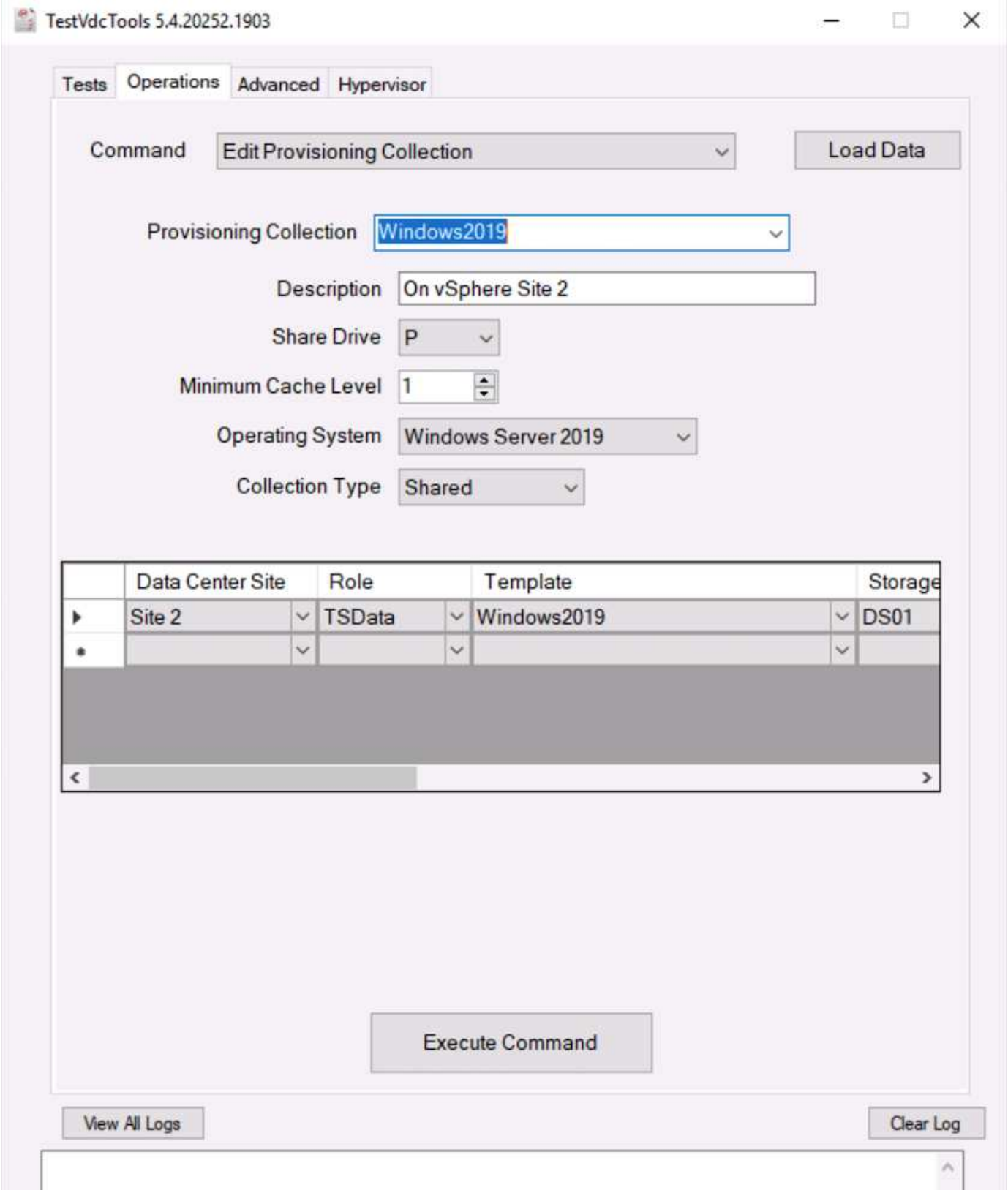
Per avviare Command Center e il ruolo richiesto, vedere "Panoramica del Command Center".

È possibile eseguire le seguenti operazioni:

- Modificare il percorso SMB per un’area di lavoro.



- Modificare il sito per la raccolta di provisioning.


TestVdcTools 5.4.20252.1903
Tests
Operations
Advanced
Hypervisor
Command
Edit Provisioning Collection
Load Data
Provisioning Collection
Windows2019
Description
On vSphere Site 2
Share Drive
P
Minimum Cache Level
1
Operating System
Windows Server 2019
Collection Type
Shared
Data Center Site
Role
Template
Storage
Site 2
TSData
Windows2019
DS01
Execute Command
View All Logs
Clear Log

File di log

Name	Date modified	Type	Size
CwAgent	9/19/2020 12:35 PM	File folder	
CWAutomationService	9/19/2020 12:34 PM	File folder	
CWManagerX	9/19/2020 12:53 PM	File folder	
CwVmAutomationService	9/19/2020 12:34 PM	File folder	
TestVdcTools	9/22/2020 8:20 PM	File folder	
report	9/19/2020 12:18 PM	Executable Jar File	705 KB

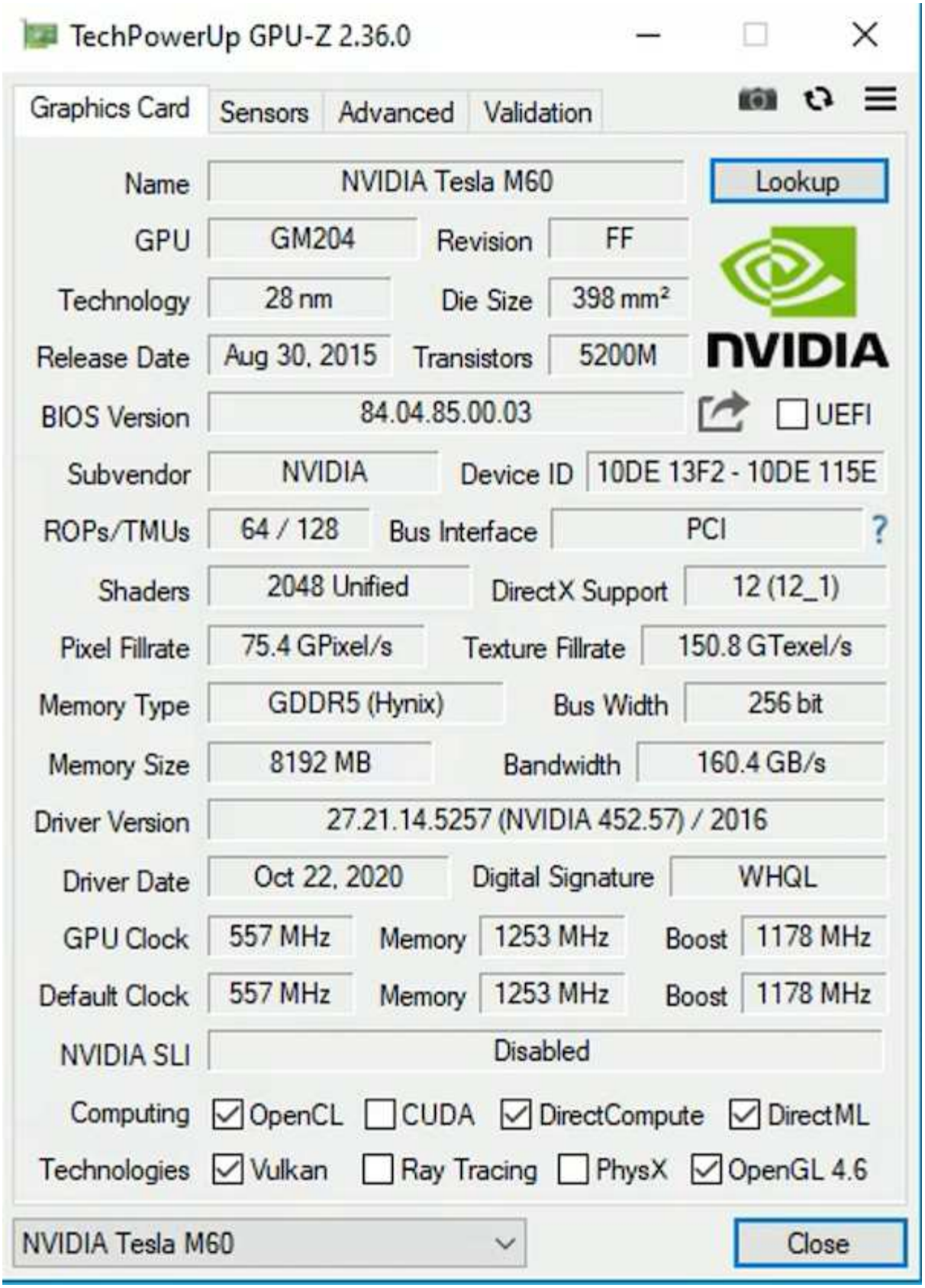
Controllare "log di automazione" per ulteriori informazioni.

Considerazioni sulla GPU

Le GPU vengono generalmente utilizzate per la visualizzazione grafica (rendering) eseguendo calcoli aritmetici ripetitivi. Questa funzionalità di calcolo ripetitivo viene spesso utilizzata per i casi di utilizzo di ai e deep learning.

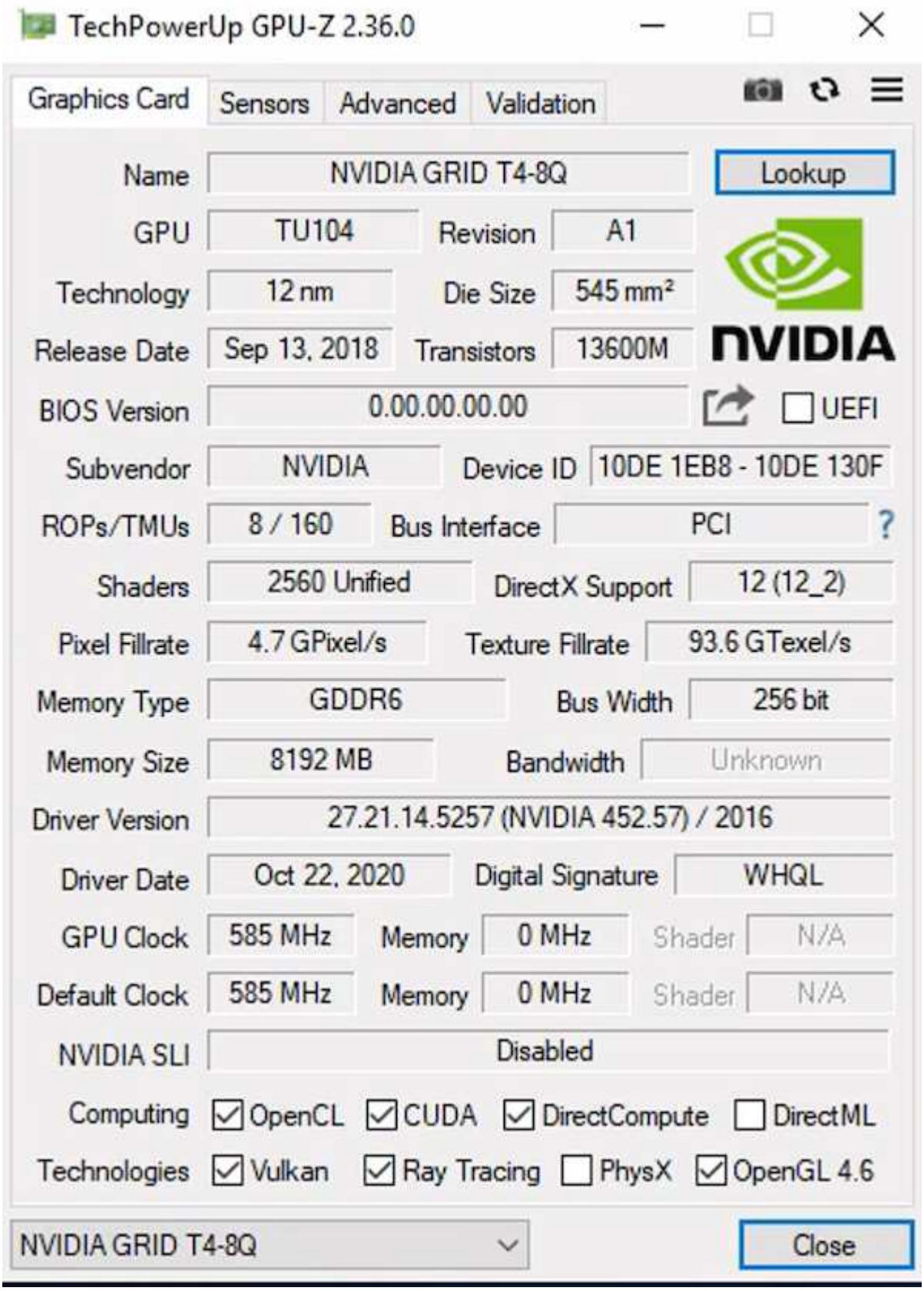
Per le applicazioni ad uso intensivo di grafica, Microsoft Azure offre la serie NV basata sulla scheda NVIDIA Tesla M60 con una o quattro GPU per macchina virtuale. Ogni scheda NVIDIA Tesla M60 include due GPU basate su Maxwell, ciascuna con 8 GB di memoria GDDR5 per un totale di 16 GB.

> La serie NV include una licenza NVIDIA.



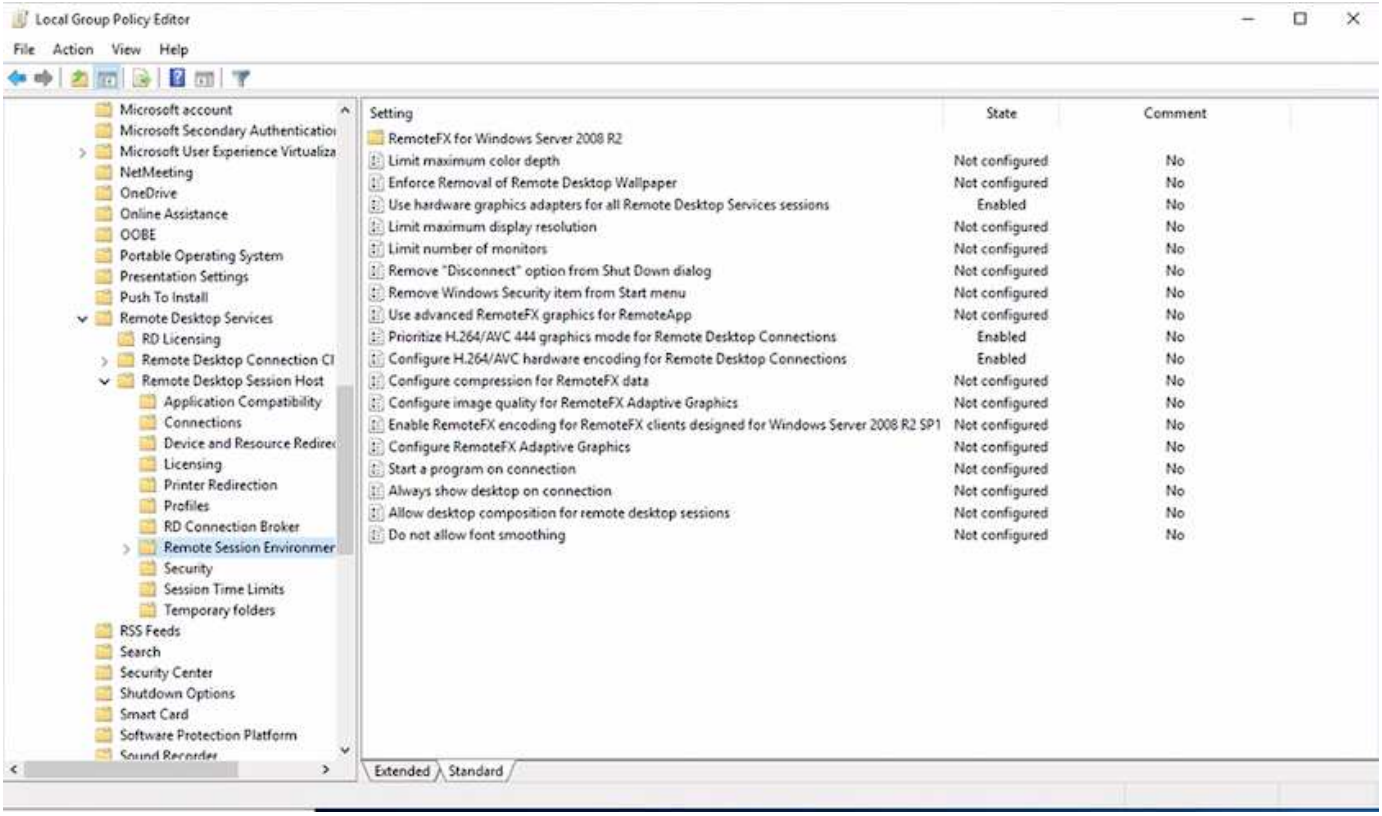
Con NetApp HCI, la GPU H615C contiene tre schede NVIDIA Tesla T4. Ogni scheda NVIDIA Tesla T4 dispone di una GPU basata su Touring con 16 GB di memoria GDDR6. Se utilizzate in un ambiente VMware vSphere, le macchine virtuali sono in grado di condividere la GPU, con ogni macchina virtuale dotata di una memoria frame buffer dedicata. Il ray tracing è disponibile con le GPU sul NetApp HCI H615C per produrre immagini realistiche, inclusi i riflessi della luce. Tenere presente che è necessario disporre di un server di licenza NVIDIA

con una licenza per le funzioni GPU.

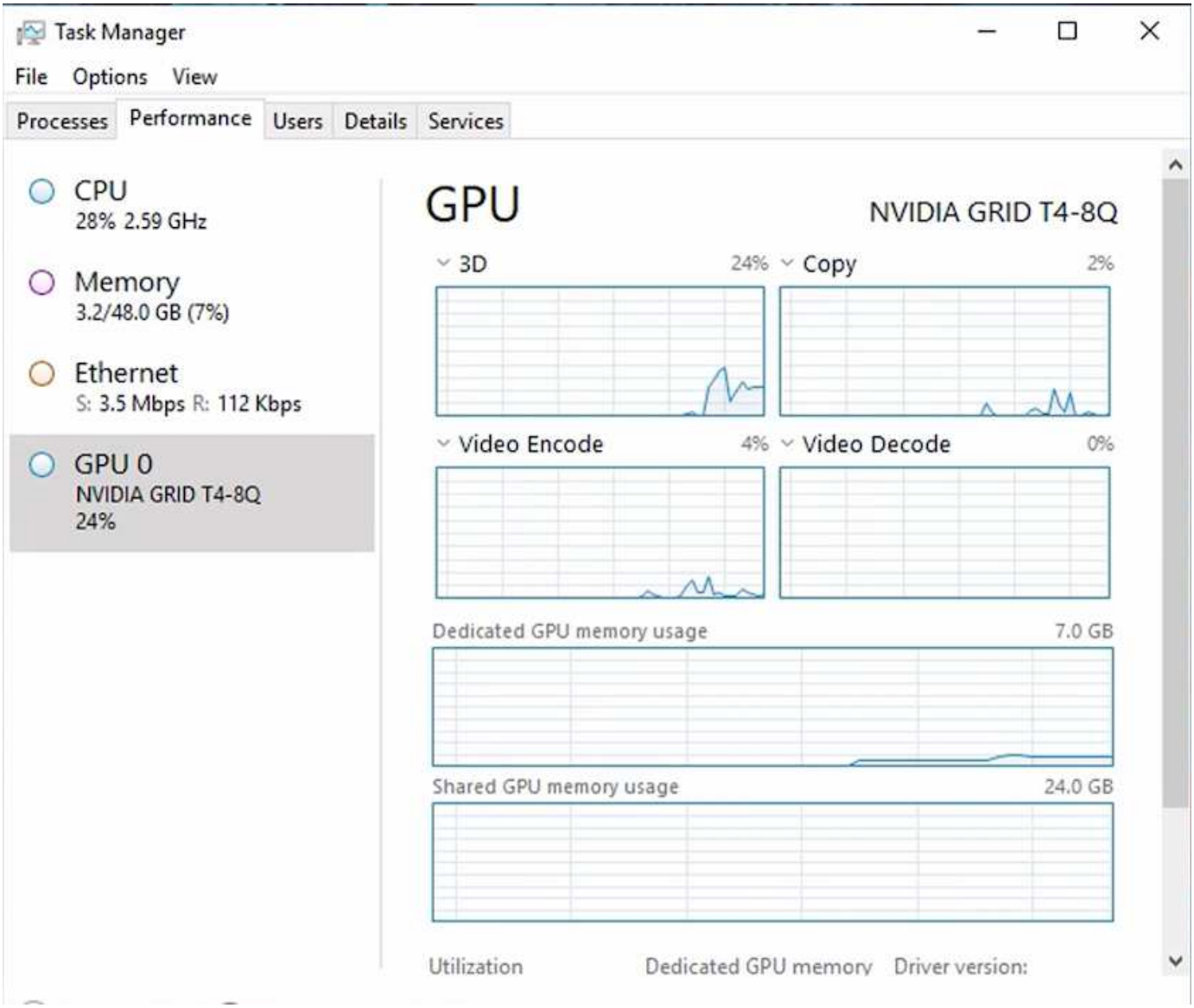


Per utilizzare la GPU, è necessario installare il driver appropriato, che può essere scaricato dal portale di licenza NVIDIA. In un ambiente Azure, il driver NVIDIA è disponibile come estensione del driver GPU. Quindi, i criteri di gruppo nella seguente schermata devono essere aggiornati per utilizzare l'hardware GPU per le

sessioni di servizio di desktop remoto. È necessario assegnare la priorità alla modalità grafica H.264 e attivare la funzionalità del codificatore.



Convalidare il monitoraggio delle performance della GPU con Task Manager o utilizzando nvidia-smi CLI quando si eseguono esempi WebGL. Assicurarsi che le risorse della GPU, della memoria e dell'encoder siano in uso.



Per assicurarsi che la macchina virtuale venga implementata in NetApp HCI H615C con servizio di desktop virtuale, definire un sito con la risorsa di cluster vCenter che dispone di host H615C. Il modello di macchina virtuale deve avere il profilo vGPU richiesto allegato.

Per gli ambienti multi-sessione condivisi, considerare l'allocazione di più profili vGPU omogenei. Tuttavia, per le applicazioni grafiche professionali di fascia alta, è meglio avere ogni macchina virtuale dedicata a un utente per mantenere le macchine virtuali isolate.

Il processore GPU può essere controllato da una policy QoS e ciascun profilo vGPU può avere frame buffer dedicati. Tuttavia, l'encoder e il decoder sono condivisi per ogni scheda. Il posizionamento di un profilo vGPU su una scheda GPU è controllato dalla policy di assegnazione della GPU host di vSphere, che può enfatizzare le performance (macchine virtuali distribuite) o il consolidamento (macchine virtuali di gruppo).

Soluzioni per il settore

Le workstation grafiche sono generalmente utilizzate in settori come produzione, sanità, energia, media e intrattenimento, istruzione, e così via. La mobilità è spesso limitata per le applicazioni a uso intensivo di grafica.

Per risolvere il problema della mobilità, i servizi di desktop virtuale offrono un ambiente desktop per tutti i tipi di lavoratori, dai task worker agli utenti esperti, utilizzando risorse hardware nel cloud o con NetApp HCI, incluse le opzioni per configurazioni flessibili della GPU. VDS consente agli utenti di accedere al proprio ambiente di lavoro da qualsiasi luogo con laptop, tablet e altri dispositivi mobili.

Per eseguire carichi di lavoro di produzione con software come ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX e così via, Le GPU disponibili su diversi cloud (a gennaio 2021) sono elencate nella seguente tabella.

Modello GPU	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	On-premise (NetApp HCI)
NVIDIA M60	Sì	Sì	Sì	No
NVIDIA T4	No	Sì	Sì	Sì
NVIDIA P100	No	Sì	No	No
NVIDIA P4	No	Sì	No	No

Sono inoltre disponibili sessioni desktop condivise con altri utenti e desktop personali dedicati. I desktop virtuali possono avere da una a quattro GPU o utilizzare GPU parziali con NetApp HCI. NVIDIA T4 è una scheda GPU versatile in grado di soddisfare le esigenze di un'ampia gamma di carichi di lavoro degli utenti. Ogni scheda GPU su NetApp HCI H615C dispone di 16 GB di memoria frame buffer e tre schede per server. Il numero di utenti che possono essere ospitati su un singolo server H615C dipende dal carico di lavoro dell'utente.

Utenti/Server	Leggero (4 GB)	Media (8 GB)	Pesante (16 GB)
H615C	12	6	3

Per determinare il tipo di utente, eseguire il profiler GPU mentre gli utenti lavorano con le applicazioni che eseguono attività tipiche. Il profiler GPU acquisisce le richieste di memoria, il numero di display e la risoluzione richiesta dagli utenti. È quindi possibile scegliere il profilo vGPU che soddisfa i requisiti.

I desktop virtuali con GPU possono supportare una risoluzione dello schermo fino a 8K, mentre l'utility nView può suddividere un singolo monitor in regioni per lavorare con diversi set di dati.

Con lo storage di file ONTAP, puoi ottenere i seguenti vantaggi:

- Un singolo namespace in grado di crescere fino a 20 PB di storage con 400 miliardi di file, senza molti input amministrativi
- Uno spazio dei nomi che può estendersi a livello globale con una Global file cache
- Multi-tenancy sicura con lo storage NetApp gestito
- Migrazione dei dati cold in archivi di oggetti utilizzando NetApp FabricPool
- Statistiche rapide sui file con analisi del file system
- Scalabilità di un cluster di storage fino a 24 nodi per aumentare capacità e performance
- Possibilità di controllare lo spazio di storage utilizzando quote e performance garantite con limiti di QoS
- Protezione dei dati con crittografia
- Soddisfare i più ampi requisiti di protezione e conformità dei dati
- Offrire opzioni flessibili di business continuity

Conclusione

NetApp Virtual Desktop Service offre un ambiente di applicazioni e desktop virtuali di facile utilizzo, con un'attenzione particolare alle sfide aziendali. Estendendo i VDS con l'ambiente ONTAP on-premise, è possibile utilizzare le potenti funzionalità NetApp in un ambiente VDS, tra cui cloni rapidi, deduplica in-line, compaction, thin provisioning, e compressione. Queste funzionalità consentono di risparmiare sui costi di storage e migliorare le performance con lo storage all-flash. Con l'hypervisor VMware vSphere, che riduce al minimo i tempi di provisioning dei server utilizzando Virtual Volumes e vSphere API per l'integrazione degli array. Utilizzando il cloud ibrido, i clienti possono scegliere l'ambiente giusto per i carichi di lavoro esigenti e risparmiare denaro. La sessione desktop in esecuzione on-premise può accedere alle risorse cloud in base alle policy.

Dove trovare ulteriori informazioni

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

- "Cloud di NetApp"
- "Documentazione sui prodotti NetApp VDS"
- "Connetti la tua rete on-premise ad Azure con VPN Gateway"
- "Portale Azure"
- "Desktop virtuale Microsoft Windows"
- "Registrazione Azure NetApp Files"

VMware Horizon

NVA-1132-DESIGN: VMware end-user computing con NetApp HCI

Suresh Thoppay, NetApp

VMware End-User Computing con NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive la progettazione architetturale e le Best practice per l'implementazione della soluzione su scala di produzione in modo affidabile e privo di rischi.

"NVA-1132-DESIGN: VMware end-user computing con NetApp HCI"

NVA-1129-DESIGN: Calcolo per l'utente finale VMware con GPU NetApp HCI e NVIDIA

Suresh Thoppay, NetApp

VMware End-User Computing con NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive la progettazione architetturale e le Best practice per l'implementazione della soluzione su scala di produzione in modo affidabile e privo di

rischi.

"NVA-1129-DESIGN: Calcolo per l'utente finale VMware con GPU NetApp HCI e NVIDIA"

NVA-1129-DEPLOY: VMware end-user computing con GPU NetApp HCI e NVIDIA

Suresh Thoppay, NetApp

VMware End-User Computing with NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive come implementare la soluzione su scala di produzione in modo affidabile e privo di rischi

"NVA-1129-DEPLOY: VMware end-user computing con GPU NetApp HCI e NVIDIA"

NetApp HCI per l'infrastruttura di desktop virtuale con VMware Horizon 7: Potenzia i tuoi utenti più esperti con la grafica 3D

Suresh Thoppay, NetApp

TR-4792 fornisce indicazioni sull'utilizzo del nodo di calcolo NetApp H615C per carichi di lavoro di grafica 3D in un ambiente VMware Horizon con unità di elaborazione grafica NVIDIA (GPU) e software di virtualizzazione. Fornisce inoltre i risultati dei test preliminari di SPECviewperf 13 per H615C.

"NetApp HCI per l'infrastruttura di desktop virtuale con VMware Horizon 7: Potenzia i tuoi utenti più esperti con la grafica 3D"

Soluzioni di virtualizzazione desktop FlexPod

Per ulteriori informazioni sulle soluzioni di virtualizzazione FlexPod, consulta la "Guide alla progettazione di FlexPod"

Demo ed esercitazioni

Video e demo sulla virtualizzazione

Guarda i seguenti video e demo che illustrano le funzionalità specifiche delle soluzioni di cloud ibrido, virtualizzazione e container.

Strumenti NetApp ONTAP per VMware vSphere

Strumenti ONTAP per VMware - Panoramica

Provisioning di archivi dati VMware iSCSI con ONTAP

Provisioning di archivi dati VMware NFS con ONTAP

Plug-in SnapCenter per VMware vSphere

Il software NetApp SnapCenter è una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system.

Il plug-in SnapCenter per VMware vSphere consente di eseguire operazioni di backup, ripristino e collegamento per macchine virtuali e operazioni di backup e montaggio per datastore registrati con SnapCenter direttamente in VMware vCenter.

Per ulteriori informazioni sul plug-in NetApp SnapCenter per VMware vSphere, consultare la "Panoramica del plug-in NetApp SnapCenter per VMware vSphere".

Plug-in SnapCenter per VMware vSphere - prerequisiti della soluzione

Plug-in SnapCenter per VMware vSphere - implementazione

Plug-in SnapCenter per VMware vSphere - flusso di lavoro di backup

Plug-in SnapCenter per VMware vSphere - flusso di lavoro di ripristino

SnapCenter - flusso di lavoro di ripristino SQL

Soluzioni per la protezione dei dati 3-2-1

Le soluzioni per la protezione dei dati 3-2-1 combinano backup primari e secondari on-premise, utilizzando la tecnologia SnapMirror, con copie replicate sullo storage a oggetti utilizzando il backup e recovery di BlueXP.

Protezione dei dati 3-2-1 per datastore VMFS con plug-in SnapCenter per backup e recovery di VMware vSphere e BlueXP per macchine virtuali

VMware Cloud su AWS con AWS FSX per NetApp ONTAP

Storage connesso guest Windows con FSX ONTAP utilizzando iSCSI

Storage connesso guest Linux con FSX ONTAP con NFS

Risparmi sul TCO di VMware Cloud su AWS con Amazon FSX per NetApp ONTAP

Archivio dati supplementare VMware Cloud su AWS con Amazon FSX per NetApp ONTAP

Installazione della configurazione e dell'implementazione di VMware HCX per VMC

Dimostrazione della migrazione a VMotion con VMware HCX per VMC e FSxN

Dimostrazione della migrazione a freddo con VMware HCX per VMC e FSxN

Azure servizi VMware su Azure con Azure NetApp Files (ANF)

Panoramica del datastore supplementare della soluzione VMware Azure con Azure NetApp Files

Soluzione VMware Azure DR con Cloud Volumes ONTAP, SnapCenter e JetStream

Dimostrazione della migrazione a freddo con VMware HCX per AVS e ANF

Dimostrazione di VMotion con VMware HCX per AVS e ANF

Dimostrazione della migrazione in blocco con VMware HCX per AVS e ANF

VMware Cloud Foundation con NetApp ONTAP

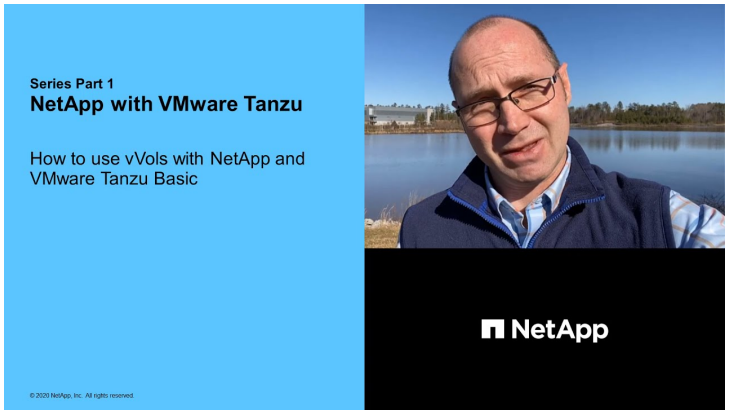
Archivi dati NFS come archiviazione principale per i domini del carico di lavoro VCF

Archivi dati iSCSI come archiviazione supplementare per i domini di gestione VCF

NetApp con VMware Tanzu

VMware Tanzu consente ai clienti di implementare, amministrare e gestire il proprio ambiente Kubernetes tramite vSphere o VMware Cloud Foundation. Questo portfolio di prodotti VMware consente ai clienti di gestire tutti i cluster Kubernetes pertinenti da un singolo piano di controllo scegliendo l'edizione VMware Tanzu più adatta alle loro esigenze.

Per ulteriori informazioni su VMware Tanzu, consultare "Panoramica di VMware Tanzu". Questa recensione illustra i casi d'utilizzo, le aggiunte disponibili e molto altro ancora su VMware Tanzu.



Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 1

Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 2

Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 3

NetApp Cloud Insights

NetApp Cloud Insights è una piattaforma completa di monitoring e analytics progettata per fornire visibilità e controllo sulla tua infrastruttura cloud e on-premise.

NetApp Cloud Insights - osservabilità per il moderno data center