VMware vSphere Foundation su NetApp

NetApp virtualization solutions

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-virtualization/vmware/vmw-vvf-overview.html on August 25, 2025. Always check docs.netapp.com for the latest.

Sommario

VMware vSphere Foundation su NetApp . . . 1
Iniziare . . . 1
Scopri come utilizzare i datastore NFS v3 sui sistemi di storage ONTAP con VMware vSphere 8 . . . 1
Scopri di più sul supporto NetApp per VMware vSphere 8 . . . 8
Scopri come utilizzare VMware vSphere 8 con storage ONTAP . . . 9
Novità di VMware vSphere 8 . . . 9
Guida alla distribuzione per VMFS . . . 10
Introduzione . . . 10
Ridimensiona e ottimizza . . . 11
Strumenti NetApp ONTAP per VMware vSphere . . . 13
Scarico VAAI . . . 18
Protezione dei dati . . . 20
Configurazione del plug-in SnapCenter per VMware per VM . . . 21
Aggiungi spazio di archiviazione, crea criteri e gruppi di risorse . . . 21
Eseguire il backup dei gruppi di risorse . . . 25
Ripristinare le VM dal backup . . . 26
Protezione ransomware . . . 30
Migrazione . . . 30
Ripristino dopo un disastro . . . 31
Conclusione . . . 31
Utilizzare nConnect sui datastore NFS v3 per migliorare le prestazioni del datastore . . . 31
Casi d’uso . . . 32
Dettagli tecnici . . . 32
Prerequisito . . . 33
Aggiorna il numero di connessione al datastore NFS . . . 34
Considerazioni di progettazione . . . 35
Configurare i datastore NFS per vSphere 8 utilizzando gli ONTAP tools for VMware vSphere . . . 36
Panoramica della soluzione . . . 36
Architettura . . . 36
Prerequisiti . . . 37
Fasi di distribuzione . . . 38
Informazioni aggiuntive . . . 67
Configurare il disaster recovery per i datastore NFS utilizzando VMware Site Recovery Manager . . . 67
Panoramica dello scenario . . . 68
Architettura . . . 68
Prerequisiti . . . 69
Fasi di distribuzione . . . 69
Operazioni di disaster recovery con SRM . . . 90
Informazioni aggiuntive . . . 93
Cluster di storage VMware vSphere Metro con sincronizzazione attiva SnapMirror . . . 93
Prerequisiti . . . 96
Accesso host non uniforme vMSC con interfaccia utente di ONTAP System Manager. . . . 96
Modalità di accesso host uniforme vMSC con strumenti ONTAP . . . 104

Protezione delle VM con il plug-in SnapCenter per VMware vSphere. . . . 110
Convertire SM ActiveSync da asimmetrico a simmetrico attivo/attivo con VMware vSphere Metro Storage Cluster . . . 117
Panoramica . . . 117
Prerequisiti . . . 118
Passaggi per convertire la sincronizzazione attiva SM asimmetrica in simmetrica . . . 118
Scopri come utilizzare VMware Virtual Volumes (vVols) con l'archiviazione ONTAP . . . 120
Panoramica . . . 120
Strumenti ONTAP 9.x . . . 123
Strumenti ONTAP 10.x . . . 123
Perché vVols? . . . 123
Opzioni di connettività . . . 124
Provisioning tramite ONTAP tools for VMware vSphere . . . 126
Protezione dei dati delle VM sul datastore vVol . . . 137
Migrazione delle VM dai datastore tradizionali al datastore vVol . . . 140
Migrazione di VM tra datastore vVol . . . 141
Esempio di architettura di riferimento . . . 141
Come iniziare . . . 142
Raccogli dati con Virtual Machine Data Collector . . . 142
Scopri come valutare la tua infrastruttura VMware utilizzando Virtual Machine Data Collector . . . 142
Raccoglitore dati macchina virtuale (VMDC) . . . 144

VMware vSphere Foundation su NetApp

Iniziare

Scopri come utilizzare i datastore NFS v3 sui sistemi di storage ONTAP con VMware vSphere 8

NetApp ONTAP e VMware vSphere 8 collaborano per offrire soluzioni di storage basate su NFS v3 scalabili e sicure per ambienti cloud ibridi che utilizzano gli array All-Flash NetApp . Scopri le opzioni di storage supportate per VMware vSphere Foundation e i principali casi d'uso, tra cui VMware Live Site Recovery per il disaster recovery e Autonomous Ransomware Protection (ARP) di NetApp per lo storage NFS.

Utilizzo di NFS v3 con vSphere 8 e sistemi di archiviazione ONTAP

Questo documento fornisce informazioni sulle opzioni di archiviazione disponibili per VMware Cloud vSphere Foundation utilizzando gli array All-Flash NetApp . Le opzioni di archiviazione supportate sono illustrate con istruzioni specifiche per la distribuzione di datastore NFS. Inoltre, viene illustrato VMware Live Site Recovery per il disaster recovery di datastore NFS. Infine, viene esaminata la protezione autonoma dai ransomware di NetApp per l'archiviazione NFS.

Casi d'uso

Casi d'uso trattati in questa documentazione:

- Opzioni di archiviazione per i clienti che cercano ambienti uniformi sia nei cloud privati che in quelli pubblici.
- Distribuzione di infrastrutture virtuali per carichi di lavoro.
- Soluzione di storage scalabile, studiata su misura per soddisfare esigenze in continua evoluzione, anche quando non è direttamente allineata con i requisiti delle risorse di elaborazione.
- Proteggi le VM e gli archivi dati utilizzando il SnapCenter Plug-in for VMware vSphere.
- Utilizzo di VMware Live Site Recovery per il ripristino di emergenza di datastore NFS.
- Strategia di rilevamento del ransomware, che include più livelli di protezione a livello di host ESXi e VM guest.

Pubblico

Questa soluzione è destinata alle seguenti persone:

- Architetti di soluzioni alla ricerca di opzioni di archiviazione più flessibili per ambienti VMware, progettate per massimizzare il TCO.
- Architetti di soluzioni alla ricerca di opzioni di archiviazione VVF che offrano protezione dei dati e opzioni di disaster recovery con i principali provider cloud.
- Amministratori di storage che desiderano istruzioni specifiche su come configurare VVF con storage NFS.
- Amministratori di storage che desiderano istruzioni specifiche su come proteggere le VM e gli archivi dati residenti nello storage ONTAP .

Panoramica della tecnologia

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

Fondazione VMware vSphere

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

La soluzione VVF supporta sia i carichi di lavoro nativi Kubernetes sia quelli basati su macchine virtuali. I componenti chiave includono:

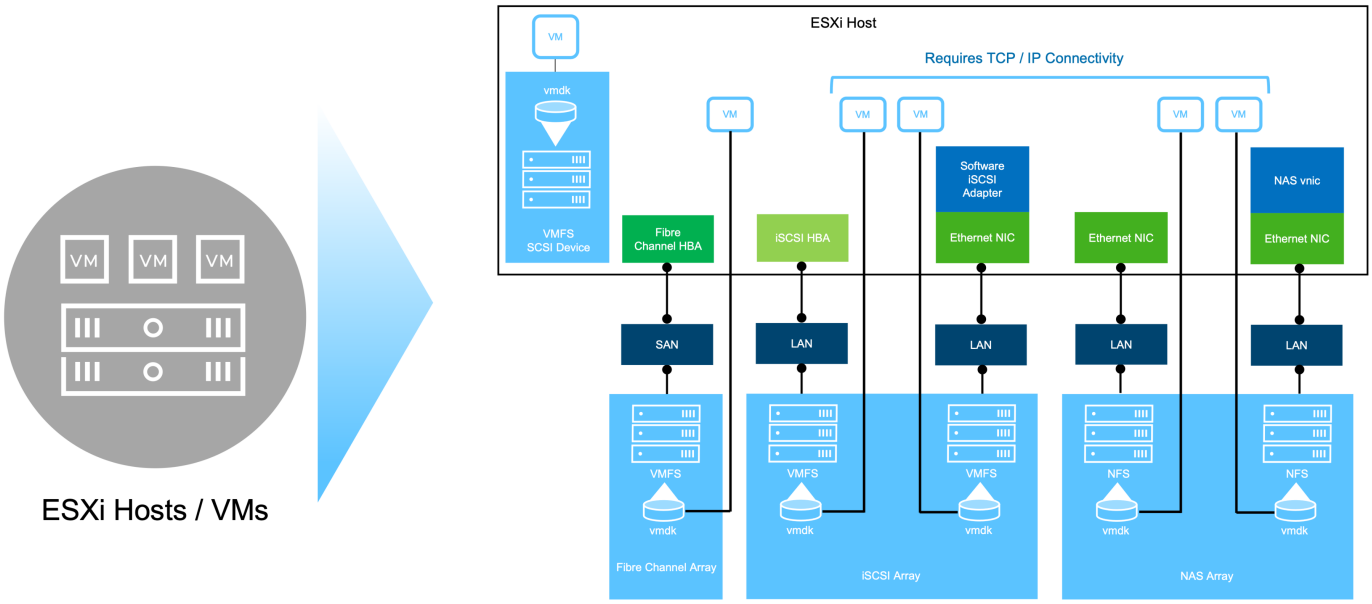
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service per vSphere
- Switch distribuito vSphere

Per ulteriori informazioni sui componenti inclusi in VVF, fare riferimento ad architettura e pianificazione, fare riferimento a "Confronto in tempo reale dei prodotti VMware vSphere" .

Opzioni di archiviazione VVF

Per un ambiente virtuale efficace e performante è fondamentale lo storage. L'archiviazione, sia tramite datastore VMware che tramite casi d'uso connessi agli ospiti, sblocca le capacità dei tuoi carichi di lavoro, consentendoti di scegliere il miglior prezzo per GB che offre il massimo valore, riducendo al contempo il sottoutilizzo. ONTAP è da quasi due decenni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo al contempo i costi.

Le opzioni di storage VMware sono in genere organizzate come offerte di storage tradizionale e di storage definito dal software. I modelli di storage tradizionali includono storage locale e di rete, mentre i modelli di storage definiti dal software includono vSAN e VMware Virtual Volumes (vVols).



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

NetApp ONTAP

Sono numerose e convincenti le ragioni per cui decine di migliaia di clienti hanno scelto ONTAP come soluzione di storage primaria per vSphere. Tra questi rientrano i seguenti:

1. **Sistema di archiviazione unificato:** ONTAP offre un sistema di archiviazione unificato che supporta sia i protocolli SAN che NAS. Questa versatilità consente l'integrazione perfetta di diverse tecnologie di storage in un'unica soluzione.
2. **Protezione dati affidabile:** ONTAP offre funzionalità di protezione dati affidabili tramite snapshot efficienti in termini di spazio. Questi snapshot 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 in modo efficace i dati delle applicazioni. Questi strumenti semplificano le attività di gestione dell'archiviazione, migliorando l'efficienza operativa e semplificando l'amministrazione.
4. **Efficienza di archiviazione:** ONTAP include diverse funzionalità di efficienza di archiviazione, abilitate di default, progettate per ottimizzare l'utilizzo dell'archiviazione, ridurre i costi e migliorare le prestazioni complessive del sistema.

L'utilizzo di ONTAP con VMware offre una grande flessibilità in base alle esigenze applicative specifiche. I seguenti protocolli sono supportati come datastore VMware utilizzando ONTAP: * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4.1

Utilizzando un sistema di storage separato dall'hypervisor è possibile delegare numerose funzioni e massimizzare l'investimento nei sistemi host vSphere. Questo approccio non solo garantisce che le risorse host siano concentrate sui carichi di lavoro delle applicazioni, ma evita anche effetti casuali sulle prestazioni delle applicazioni derivanti dalle operazioni di archiviazione.

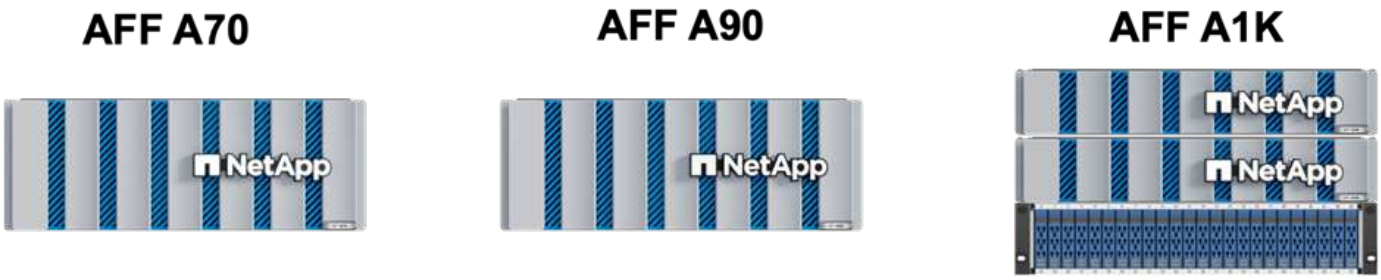
L'utilizzo di ONTAP insieme a vSphere è un'ottima combinazione che consente di ridurre le spese per l'hardware host e il software VMware. Puoi anche proteggere i tuoi dati a costi inferiori mantenendo prestazioni elevate e costanti. Poiché i carichi di lavoro virtualizzati sono mobili, è possibile esplorare diversi approcci utilizzando Storage vMotion per spostare le VM tra datastore VMFS, NFS o vVols , tutti sullo stesso sistema di storage.

Array All-Flash NetApp

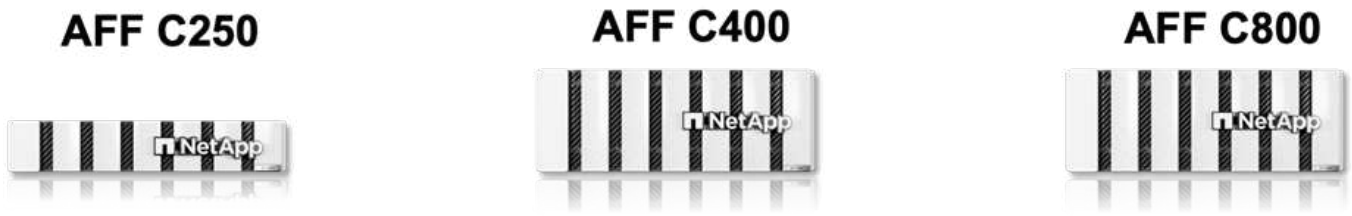
NetApp AFF (All Flash FAS) è una linea di prodotti di array di storage all-flash. È progettato per offrire soluzioni di archiviazione ad alte prestazioni e bassa latenza per carichi di lavoro aziendali. La serie AFF unisce i vantaggi della tecnologia flash alle capacità di gestione dei dati di NetApp, offrendo alle aziende una piattaforma di storage potente ed efficiente.

La gamma AFF è composta dai modelli della serie A e della serie C.

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



Gli array flash QLC della serie C sono pensati per casi d'uso ad alta capacità, offrendo la velocità del flash con i costi contenuti del flash ibrido.



Supporto del protocollo di archiviazione

L' AFF supporta tutti i protocolli standard utilizzati per la virtualizzazione, sia per gli archivi dati che per gli storage connessi agli ospiti, tra cui NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), NVME over fabric e S3. I clienti sono liberi di scegliere la soluzione più adatta ai loro carichi di lavoro e alle loro applicazioni.

NFS - NetApp AFF fornisce supporto per NFS, consentendo l'accesso basato su file ai datastore VMware. Gli archivi dati connessi tramite NFS provenienti da molti host ESXi superano di gran lunga i limiti imposti ai file system VMFS. L'utilizzo di NFS con vSphere offre alcuni vantaggi in termini di semplicità d'uso e visibilità dell'efficienza di archiviazione. ONTAP include funzionalità di accesso ai file disponibili per il protocollo NFS. È possibile abilitare un server NFS ed esportare volumi o qtree.

Per indicazioni di progettazione sulle configurazioni NFS, fare riferimento a "Documentazione sulla gestione dell'archiviazione NAS" .

iSCSI - NetApp AFF fornisce un solido supporto per iSCSI, consentendo l'accesso a livello di blocco ai dispositivi di archiviazione tramite reti IP. Offre un'integrazione perfetta con gli iniziatori iSCSI, consentendo un provisioning e una gestione efficienti delle LUN iSCSI. Funzionalità avanzate di ONTAP, come il multi-pathing, l'autenticazione CHAP e il supporto ALUA.

Per indicazioni di progettazione sulle configurazioni iSCSI fare riferimento a "Documentazione di riferimento sulla 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 di archiviazione (SAN). ONTAP si integra perfettamente con l'infrastruttura FC, garantendo un accesso affidabile ed efficiente a livello di blocco ai dispositivi di archiviazione. Offre funzionalità quali zoning, multi-pathing e fabric login (FLOGI) per ottimizzare le prestazioni, migliorare la sicurezza e garantire una connettività senza interruzioni negli ambienti FC.

Per indicazioni di progettazione sulle configurazioni Fibre Channel fare riferimento a "Documentazione di riferimento sulla configurazione SAN" .

NVMe su Fabric - NetApp ONTAP supporta NVMe su fabric. NVMe/FC consente l'utilizzo di dispositivi di archiviazione NVMe su infrastrutture Fibre Channel e NVMe/TCP su reti di archiviazione IP.

Per indicazioni di progettazione su NVMe fare riferimento a "Configurazione, supporto e limitazioni NVMe" .

Tecnologia attiva-attiva

Gli array All-Flash NetApp consentono percorsi attivi-attivi attraverso entrambi i controller, eliminando la necessità per il sistema operativo host di attendere il fallimento 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 sia in uno stato stabile o che stia subendo un'operazione di failover del controller.

Per maggiori informazioni, vedere "Protezione dei dati e ripristino di emergenza" documentazione.

Garanzie di stoccaggio

NetApp offre un set esclusivo di garanzie di storage con gli array NetApp All-flash. I vantaggi esclusivi includono:

Garanzia di efficienza di archiviazione: Ottieni prestazioni elevate riducendo al minimo i costi di archiviazione con la Garanzia di efficienza di archiviazione. 4:1 per carichi di lavoro SAN. **Garanzia di recupero da ransomware:** Recupero dati garantito in caso di attacco ransomware.

Per informazioni dettagliate vedere il "Pagina di destinazione di NetApp AFF" .

Strumenti NetApp ONTAP per VMware vSphere

Una componente potente di vCenter è la possibilità di integrare plug-in o estensioni che ne migliorano ulteriormente le funzionalità e forniscono caratteristiche e capacità aggiuntive. Questi plug-in estendono le capacità di gestione di vCenter e consentono agli amministratori di integrare soluzioni, strumenti e servizi di terze 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 la sua architettura vCenter Plug-in. Questi strumenti si integrano perfettamente con l'ecosistema VMware, consentendo un provisioning efficiente degli archivi dati e garantendo una protezione essenziale per le macchine virtuali. Con ONTAP Tools per VMware vSphere, gli amministratori possono gestire senza problemi le attività di gestione del ciclo di vita dello storage.

Strumenti ONTAP completi 10 risorse possono essere trovate "ONTAP tools for VMware vSphere Risorse di documentazione" .

Visualizza la soluzione di distribuzione degli strumenti ONTAP 10 su"Utilizzare gli strumenti ONTAP 10 per configurare i datastore NFS per vSphere 8"

Plug-in NetApp NFS per VMware VAAI

Il plug-in NetApp NFS per VAAI (vStorage APIs for Array Integration) migliora le operazioni di archiviazione delegando determinate attività al sistema di archiviazione NetApp , con conseguente miglioramento delle prestazioni e dell'efficienza. Ciò include operazioni quali la copia completa, l'azzeramento dei blocchi e il blocco assistito dall'hardware. Inoltre, il plugin VAAI ottimizza l'utilizzo dello storage riducendo la quantità di dati trasferiti sulla rete durante le operazioni di provisioning e clonazione delle macchine virtuali.

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

Fare riferimento a "Documentazione del plug-in NetApp NFS per VMware VAAI" per maggiori informazioni.

SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere (SCV) è una soluzione software di NetApp che offre una protezione completa dei dati per gli ambienti VMware vSphere. È progettato per semplificare e snellire il processo di protezione e gestione delle macchine virtuali (VM) e degli archivi dati. SCV utilizza snapshot basati sull'archiviazione e replica su array secondari per soddisfare obiettivi di tempi di ripristino più bassi.

Il SnapCenter Plug-in for VMware vSphere offre le seguenti funzionalità in un'interfaccia unificata, integrata con il client vSphere:

Snapshot basati su policy: SnapCenter consente di definire policy per la creazione e la gestione di snapshot coerenti con le applicazioni delle macchine virtuali (VM) in VMware vSphere.

Automazione - La creazione e la gestione automatizzate degli snapshot basate su criteri definiti contribuiscono a garantire una protezione dei dati coerente ed efficiente.

Protezione a livello di VM: la protezione granulare a livello di VM consente una gestione e un ripristino efficienti delle singole macchine virtuali.

Funzionalità di efficienza di archiviazione - L'integrazione con le tecnologie di archiviazione NetApp fornisce funzionalità di efficienza di archiviazione come la deduplicazione e la compressione per gli snapshot, riducendo al minimo i requisiti di archiviazione.

Il plug-in SnapCenter orchestra la disattivazione delle macchine virtuali insieme agli snapshot basati su hardware sugli array di storage NetApp . La tecnologia SnapMirror viene utilizzata per replicare copie di backup su sistemi di archiviazione secondari, anche nel cloud.

Per maggiori informazioni fare riferimento al "Documentazione SnapCenter Plug-in for VMware vSphere" .

L'integrazione BlueXP consente strategie di backup 3-2-1 che estendono le copie dei dati all'archiviazione degli oggetti nel cloud.

Per maggiori informazioni sulle strategie di backup 3-2-1 con BlueXP visita"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM" .

Per istruzioni dettagliate sulla distribuzione del plug-in SnapCenter , fare riferimento alla soluzione"Utilizzare il SnapCenter Plug-in for VMware vSphere per proteggere le VM sui domini di carico di lavoro VCF" .

Considerazioni sullo stoccaggio

Sfruttando i datastore ONTAP NFS con VMware vSphere si ottiene un ambiente ad alte prestazioni, facile da gestire e scalabile, che fornisce rapporti tra VM e datastore irraggiungibili con protocolli di storage basati su blocchi. Questa architettura può determinare un aumento di dieci volte della densità degli archivi dati, accompagnato da una corrispondente riduzione del numero di archivi dati.

nConnect per NFS: un altro vantaggio dell'utilizzo di NFS è la possibilità di sfruttare la funzionalità **nConnect**. nConnect consente più connessioni TCP per i volumi di datastore NFS v3, ottenendo così una maggiore produttività. Ciò contribuisce ad aumentare il parallelismo e per gli archivi dati NFS. I clienti che distribuiscono 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" .

Trunking di sessione per NFS: a partire da ONTAP 9.14.1, i client che utilizzano NFSv4.1 possono sfruttare il trunking di sessione per stabilire più connessioni a vari LIF sul server NFS. Ciò consente un trasferimento dati più rapido e aumenta la resilienza utilizzando il multipathing. Il trunking si rivela particolarmente utile quando si esportano volumi FlexVol verso client che supportano il trunking, come i client VMware e Linux, o quando si utilizza NFS su protocolli RDMA, TCP o pNFS.

Fare riferimento a "Panoramica del trunking NFS" per maggiori informazioni.

- Volumi FlexVol :* NetApp consiglia di utilizzare volumi * FlexVol* per la maggior parte dei datastore NFS. Sebbene datastore più grandi possano migliorare l'efficienza di archiviazione e i vantaggi operativi, è consigliabile prendere in considerazione l'utilizzo di almeno quattro datastore (volumi FlexVol) per archiviare le VM su un singolo controller ONTAP . In genere, gli amministratori distribuiscono datastore supportati da volumi FlexVol con capacità che vanno da 4 TB a 8 TB. Questa dimensione garantisce un buon equilibrio tra prestazioni, facilità di gestione e protezione dei dati. Gli amministratori possono iniziare in piccolo e poi ridimensionare il datastore in base alle esigenze (fino a un massimo di 100 TB). Gli archivi dati più piccoli facilitano un ripristino più rapido da backup o disastri e possono essere spostati rapidamente all'interno del cluster. Questo approccio consente di sfruttare al massimo le prestazioni delle risorse hardware e consente di utilizzare datastore con diverse policy di ripristino.
- Volumi FlexGroup :* per gli scenari che richiedono un datastore di grandi dimensioni, NetApp consiglia l'uso di volumi * FlexGroup*. I volumi FlexGroup non hanno praticamente vincoli di capacità o di numero di file, consentendo agli amministratori di predisporre facilmente un singolo namespace di grandi dimensioni. L'utilizzo dei volumi FlexGroup non comporta costi aggiuntivi di manutenzione o gestione. Per le prestazioni con i volumi FlexGroup non sono necessari più datastore, poiché sono intrinsecamente scalabili. Utilizzando i volumi ONTAP e FlexGroup con VMware vSphere, è possibile creare datastore semplici e scalabili che sfruttano tutta la potenza dell'intero cluster ONTAP .

Protezione dal ransomware

Il software di gestione dati NetApp ONTAP è dotato di una suite completa di tecnologie integrate per aiutarti a proteggere, rilevare e ripristinare gli attacchi ransomware. La funzionalità NetApp SnapLock Compliance integrata in ONTAP impedisce l'eliminazione dei dati archiviati in un volume abilitato utilizzando la tecnologia WORM (write once, read many) con conservazione avanzata dei dati. Dopo aver stabilito il periodo di conservazione e bloccato la copia Snapshot, nemmeno un amministratore di storage con privilegi di sistema completi o un membro del team di supporto NetApp può eliminare la copia Snapshot. Ma, cosa ancora più importante, un hacker con credenziali compromesse non può cancellare i dati.

NetApp garantisce che saremo in grado di recuperare le copie protette NetApp Snapshot sugli array idonei e, se non ci riusciremo, risarciremo la tua organizzazione.

Per maggiori informazioni sulla Ransomware Recovery Guarantee, vedere: "Garanzia di recupero da ransomware" .

Fare riferimento al "Panoramica sulla protezione autonoma dal ransomware" per informazioni più approfondite.

Consulta la soluzione completa nel centro documentazione NetApps Solutions:"Protezione autonoma contro i ransomware per l'archiviazione NFS"

Considerazioni sul ripristino in caso di disastro

NetApp fornisce lo storage più sicuro al mondo. NetApp può aiutare a proteggere i dati e l'infrastruttura delle applicazioni, a spostare i dati tra storage locali e cloud e a garantire la disponibilità dei dati tra i cloud. ONTAP è dotato di potenti tecnologie di protezione e sicurezza dei dati che aiutano a proteggere i clienti dai disastri rilevando in modo proattivo le minacce e ripristinando rapidamente dati e applicazioni.

VMware Live Site Recovery, precedentemente noto come VMware Site Recovery Manager, offre

un’automazione semplificata e 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 tramite Storage Replication Adapter come parte di ONTAP Tools per VMware. Sfruttando le capacità di NetApp SnapMirror per la replica basata su array, gli ambienti VMware possono trarre vantaggio da una delle tecnologie più affidabili e mature di ONTAP. SnapMirror garantisce trasferimenti di dati sicuri e altamente efficienti copiando solo i blocchi del file system modificati, anziché intere VM o datastore. Inoltre, questi blocchi sfruttano tecniche di risparmio di spazio come la deduplicazione, la compressione e la compattazione. Con l’introduzione di SnapMirror indipendente dalla versione nei moderni sistemi ONTAP , si ottiene maggiore flessibilità nella selezione dei cluster di origine e di destinazione. SnapMirror si è rivelato un vero e proprio strumento potente per il disaster recovery e, se abbinato a Live Site Recovery, offre maggiore scalabilità, prestazioni e risparmi sui costi rispetto alle alternative di archiviazione locale.

Per maggiori informazioni fare riferimento al "Panoramica di VMware Site Recovery Manager" .

Consulta la soluzione completa nel centro documentazione NetApps Solutions:"Protezione autonoma contro i ransomware per l’archiviazione NFS"

- BlueXP DRaaS* (Disaster Recovery as a Service) per NFS è una soluzione di disaster recovery conveniente, progettata per carichi di lavoro VMware in esecuzione su sistemi ONTAP locali con datastore NFS. Sfrutta la replicazione NetApp SnapMirror per proteggere da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Integrato con la console NetApp BlueXP , questo servizio consente una gestione semplice e la scoperta automatizzata di VMware vCenter e storage ONTAP . Le organizzazioni possono creare e testare piani di disaster recovery, raggiungendo un Recovery Point Objective (RPO) fino a 5 minuti tramite replica a livello di blocco. BlueXP DRaaS utilizza la tecnologia FlexClone di ONTAP per test efficienti in termini di spazio senza impatto sulle risorse di produzione. Il servizio orchestra i processi di failover e failback, consentendo di riportare le macchine virtuali protette sul sito di disaster recovery designato con il minimo sforzo. Rispetto ad altre alternative note, BlueXP DRaaS offre queste funzionalità a una frazione del costo, il che lo rende una soluzione efficiente per le organizzazioni che desiderano configurare, testare ed eseguire operazioni di disaster recovery per i propri ambienti VMware utilizzando sistemi di storage ONTAP .

Consulta la soluzione completa nel centro documentazione NetApps Solutions:"DR tramite BlueXP DRaaS per datastore NFS"

Panoramica delle soluzioni

Soluzioni trattate in questa documentazione:

- **Funzionalità NFS nConnect con NetApp e VMware**. Clic**"Qui"** per le fasi di distribuzione.
  - **Utilizzare gli strumenti ONTAP 10 per configurare i datastore NFS per vSphere 8**. Clic**"Qui"** per le fasi di distribuzione.
  - **Distribuisci e utilizza il SnapCenter Plug-in for VMware vSphere per proteggere e ripristinare le VM**. Clic**"Qui"** per le fasi di distribuzione.
  - **Ripristino di emergenza di datastore NFS con VMware Site Recovery Manager**. Clic**"Qui"** per le fasi di distribuzione.
  - **Protezione autonoma contro i ransomware per l’archiviazione NFS**. Clic**"Qui"** per le fasi di distribuzione.

Scopri di più sul supporto NetApp per VMware vSphere 8

La partnership tra NetApp e VMware è l’unica in cui un singolo sistema di storage soddisfa tutti i principali casi d’uso definiti da VMware.

All-Flash moderno e connesso al cloud per vSphere 8

Le implementazioni ONTAP vengono eseguite su una varietà di piattaforme, tra cui appliance progettate da NetApp, hardware di base e nel cloud pubblico. ONTAP offre storage unificato, indipendentemente dal fatto che l'accesso avvenga tramite protocolli SAN o NAS e in configurazioni che spaziano da flash ad alta velocità a supporti a basso costo fino allo storage basato su cloud. NetApp offre anche piattaforme flash appositamente progettate per semplificare e segmentare le esigenze di storage senza creare silos. Inoltre, NetApp offre un software che consente di spostare facilmente i dati tra ambienti locali e cloud. Infine, NetApp BlueXP fornisce un'unica dashboard per la gestione di tutte queste relazioni e dello spazio di archiviazione.

- "Piattaforme NetApp"

Scopri come utilizzare VMware vSphere 8 con storage ONTAP

ONTAP è da quasi due decenni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo al contempo i costi. Questo documento presenta la soluzione ONTAP per vSphere, comprese le informazioni più recenti sul prodotto e le best practice, per semplificare la distribuzione, ridurre i rischi e semplificare la gestione.

Per maggiori informazioni, visita"VMware vSphere con ONTAP"

Novità di VMware vSphere 8

Scopri le novità di VMware vSphere 8 e ONTAP 9.12. Esaminare la compatibilità delle funzionalità e del supporto ONTAP con l'infrastruttura e il software VMware.

L'integrazione delle tecnologie NetApp e VMware ha una tradizione lunga 20 anni e migliaia di ore di progettazione. Con l'avvento di vSphere 8 e ONTAP 9.12, entrambe le aziende offrono prodotti in grado di soddisfare i carichi di lavoro più esigenti dei clienti. Quando questi prodotti vengono abbinati in soluzioni, si risolvono le vere sfide dei clienti, sia in sede che nei cloud pubblici. Quando questi prodotti vengono abbinati in soluzioni, si risolvono le reali sfide dei clienti, sia in sede che nei cloud pubblici.

Per aiutarti a determinare la capacità di supporto di prodotti, protocolli, sistemi operativi, ecc., consulta le risorse seguenti:

- IL "Strumento matrice di interoperabilità NetApp" (IMT). L' IMT definisce i componenti qualificati e le versioni che è possibile utilizzare per creare configurazioni FC/FCoE, iSCSI, NFS e CIFS, nonché integrazioni con plug-in aggiuntivi e offerte software.
- IL "Guida alla compatibilità VMware" . La Guida alla compatibilità VMware elenca la compatibilità di sistema, I/O, storage/SAN, backup e molto altro con VMware Infrastructure e i prodotti software.
- "Strumenti NetApp ONTAP per VMware" . Gli ONTAP tools for VMware vSphere sono un singolo plug-in di vCenter Server che include le estensioni Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA). Completamente supportato da VMware vSphere 8, OTV 9.12 offre quotidianamente un valore reale ai clienti.

Versioni supportate da NetApp ONTAP e VMware

Si prega di attendere che la/le pagina/e si sviluppino quando si seleziona un collegamento nelle tabelle sottostanti.

Versione VMware vSphere	SAN	Non è vero	OTV	* SnapCenter*
vSphere 8	"Collegamento"	"Collegamento"	"Collegamento"	"Collegamento"
vSphere 8u1	"Collegamento"	"Collegamento"	"Collegamento"	"Collegamento"

Versione VMware vSphere	Sistema di archiviazione / protocolli	OTV - SRA	OTV – Fornitore VASA	* SnapCenter Plug-in for VMware vSphere*
vSphere 8	"Collegamento"	"Collegamento"	"Collegamento"	"Collegamento"
vSphere 8u1	"Collegamento"	"Collegamento"	"Collegamento"	"Collegamento"

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. Grazie alle soluzioni NetApp , i clienti possono implementare in modo efficiente un software completo di gestione dei dati, garantendo automazione, efficienza, protezione dei dati e funzionalità di sicurezza per soddisfare in modo efficace i più esigenti requisiti prestazionali. L'abbinamento del software ONTAP con VMware vSphere consente di ridurre le spese per l'hardware host e le licenze VMware, di garantire la protezione dei dati a costi inferiori e di fornire prestazioni elevate e costanti.

Introduzione

I carichi di lavoro virtualizzati sono mobili. Pertanto, gli amministratori utilizzano VMware Storage vMotion per spostare le VM tra i datastore VMware Virtual Machine File System (VMFS), NFS o vVols , tutti residenti sullo stesso sistema di storage, esplorando così diversi approcci di storage se si utilizza un sistema All-Flash o se si utilizzano i più recenti modelli ASA con innovazione SAN per una maggiore efficienza dei costi.

Il messaggio chiave è che la migrazione a ONTAP migliora l'esperienza del cliente e le prestazioni delle applicazioni, offrendo al contempo la flessibilità di migrare dati e applicazioni tra FCP, iSCSI, NVMe/FC e NVMe/TCP. Per le aziende che hanno investito molto in VMware vSphere, l'utilizzo dello storage ONTAP rappresenta un'opzione conveniente, date le attuali condizioni di mercato, che rappresenta un'opportunità unica. Oggi le aziende si trovano ad affrontare nuove esigenze che un moderno approccio SAN può risolvere 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 di archiviazione integrata consente a ONTAP di ridurre significativamente i costi di archiviazione. I sistemi NetApp ASA possono eseguire tutte le funzionalità di efficienza di storage in produzione senza alcun impatto sulle prestazioni. NetApp semplifica la pianificazione di questi vantaggi in termini di efficienza con la garanzia più efficace disponibile.
- Protezione dei dati: il SnapCenter software, tramite snapshot, fornisce una protezione avanzata dei dati a livello di VM e applicazione per varie applicazioni aziendali distribuite in una configurazione VM.
- Sicurezza: utilizza copie Snapshot per proteggerti da malware e ransomware. Migliora la protezione rendendo immutabili le copie Snapshot tramite il blocco Snapshot e il software NetApp SnapLock .
- Cloud - ONTAP offre un'ampia gamma di opzioni di cloud ibrido che consentono alle aziende di combinare cloud pubblici e privati, offrendo flessibilità e riducendo i costi generali di gestione dell'infrastruttura. Il

supporto supplementare per l'archivio dati basato sulle offerte ONTAP consente l'utilizzo di VMware Cloud su Azure, AWS e Google per una distribuzione ottimizzata in termini di costo totale di proprietà, protezione dei dati e continuità aziendale, evitando al contempo il lock-in del fornitore.

- Flessibilità: ONTAP è ben attrezzata per soddisfare le esigenze in rapida evoluzione delle organizzazioni moderne. Con ONTAP One, tutte queste funzionalità sono di serie nel sistema ONTAP , senza costi aggiuntivi.

Ridimensiona e ottimizza

Con le imminenti modifiche alle licenze, le organizzazioni stanno affrontando in modo proattivo il potenziale aumento del costo totale di proprietà (TCO). Stanno ottimizzando strategicamente la loro infrastruttura VMware attraverso una gestione aggressiva delle risorse e un dimensionamento corretto per migliorare l'utilizzo delle risorse e semplificare 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 complessive di licenza. È importante sottolineare che molte organizzazioni stanno già integrando queste pratiche nelle loro valutazioni cloud, dimostrando come questi processi e strumenti riducano efficacemente i problemi di costi negli ambienti on-premise ed eliminino inutili spese di migrazione verso hypervisor alternativi.

Stimatore TCO

NetApp ha creato un semplice strumento di stima del TCO che fungerà da trampolino di lancio per iniziare questo percorso di ottimizzazione. Lo strumento di stima del TCO utilizza RVtools o metodi di input manuale per prevedere facilmente quanti host sono necessari per una determinata distribuzione e calcolare i risparmi per ottimizzare la distribuzione utilizzando i sistemi di storage NetApp ONTAP . Tenete presente che questo è il trampolino di lancio.

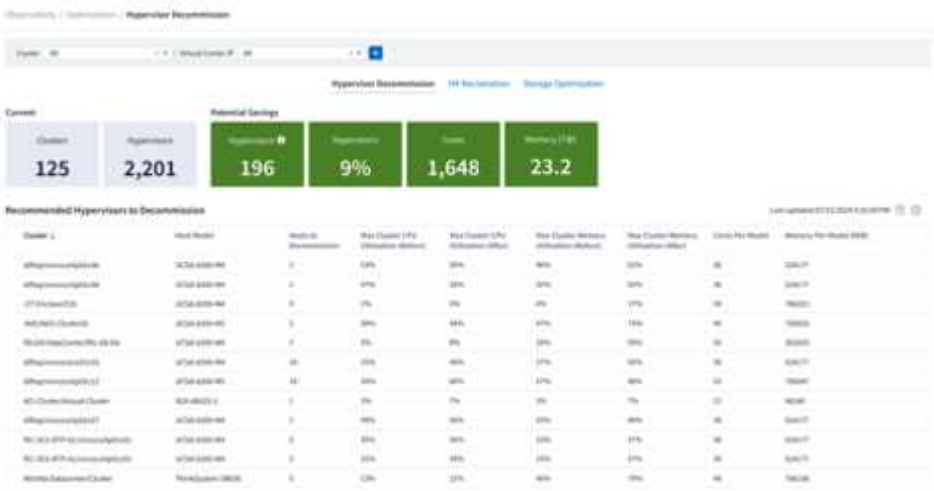
> Lo strumento di stima del TCO è accessibile solo ai team sul campo e ai partner NetApp . Collabora con i team degli account NetApp per valutare il tuo ambiente esistente.

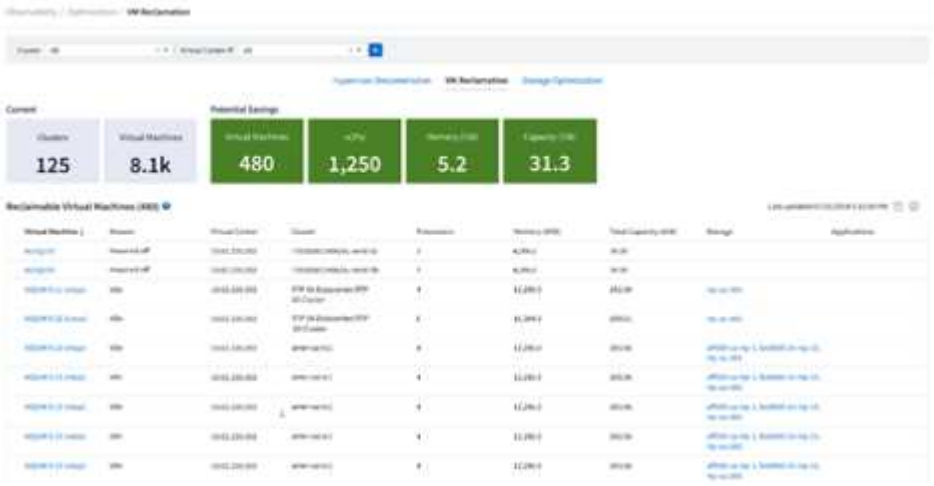
Ecco uno screenshot dello stimatore del TCO.

Cloud Insights

Una volta che lo stimatore mostra i risparmi possibili (che saranno il caso di qualsiasi organizzazione), è il momento di analizzare in modo approfondito i profili IO del carico di lavoro sulle macchine virtuali utilizzando metriche in tempo reale. Per questo, NetApp fornisce Cloud Insights. Grazie all'analisi dettagliata e ai consigli per il recupero delle VM, Cloud Insights può aiutare le aziende a prendere decisioni informate sull'ottimizzazione del loro ambiente VM. È in grado di identificare dove è possibile recuperare risorse o dismettere host con un impatto minimo sulla produzione, aiutando le aziende a gestire i cambiamenti apportati dall'acquisizione di VMware da parte di Broadcom in modo ponderato e strategico. In altre parole, Cloud Insight aiuta le aziende a eliminare l'aspetto emotivo dalle decisioni. Invece di reagire ai cambiamenti 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 l'efficienza operativa e la produttività.

Di seguito sono riportati gli screenshot di Cloud Insights.





> Eseguire valutazioni regolari per individuare le risorse sottoutilizzate, aumentare la densità delle macchine virtuali e l'utilizzo all'interno dei cluster VMware per controllare i costi crescenti associati alle nuove licenze di abbonamento. Si consiglia di ridurre il numero di core per CPU a 16 per i nuovi acquisti di server, per allinearli alle modifiche nei modelli di licenza VMware.

Con NetApp, ridimensiona correttamente i tuoi ambienti virtualizzati e introduci prestazioni di storage flash convenienti, insieme a soluzioni semplificate per la gestione dei dati e il ransomware, per garantire che le organizzazioni siano pronte per il nuovo modello di abbonamento, ottimizzando al contempo le risorse IT

attualmente disponibili.

Strumenti NetApp ONTAP per VMware vSphere

Per migliorare e semplificare ulteriormente l'integrazione con VMware, NetApp offre diversi strumenti offtap che possono essere utilizzati con NetApp ONTAP e VMware vSphere per gestire in modo efficiente gli ambienti virtualizzati. Questa sezione si concentrerà sugli strumenti ONTAP per VMware. Gli ONTAP tools for VMware vSphere 10 forniscono un set completo di strumenti per la gestione del ciclo di vita delle macchine virtuali, semplificando la gestione dello storage, potenziando le funzionalità di efficienza, migliorando la disponibilità e riducendo i costi di storage e le spese generali operative. Questi strumenti si integrano perfettamente con l'ecosistema VMware, facilitando il provisioning dei datastore e offrendo una protezione di base per le macchine virtuali. La versione 10.x degli ONTAP tools for VMware vSphere comprende microservizi scalabili orizzontalmente e basati su eventi, distribuiti come Open Virtual Appliance (OVA), seguendo le best practice per il provisioning di datastore e l'ottimizzazione delle impostazioni host ESXi per ambienti di storage a blocchi e NFS. Considerati questi vantaggi, si consiglia l'utilizzo di OTV come best practice nei sistemi che utilizzano il software ONTAP .

Iniziare

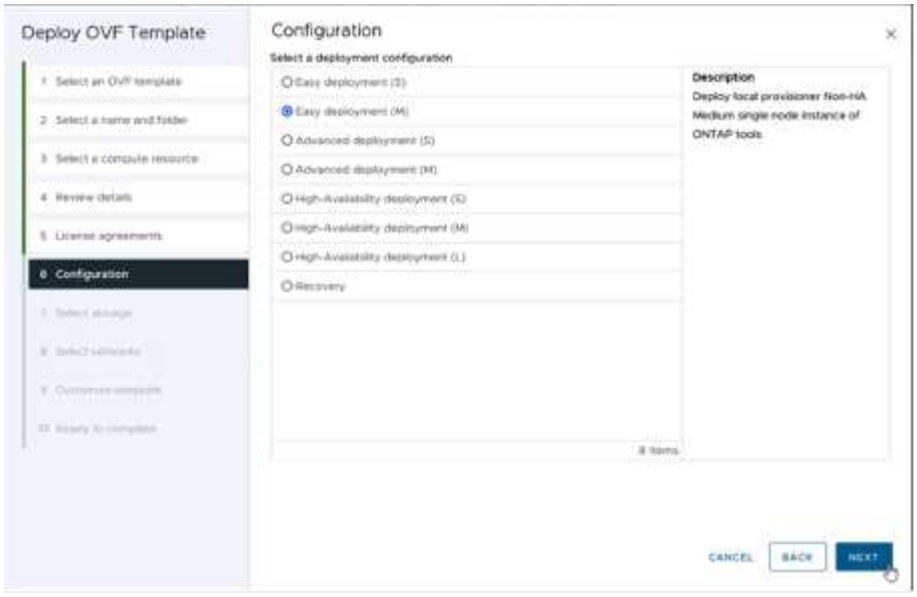
Prima di distribuire e configurare gli strumenti ONTAP per VMware, assicurarsi che siano soddisfatti i prerequisiti. Una volta fatto, distribuisci una configurazione a nodo singolo.

> Per la distribuzione sono necessari tre indirizzi IP: un indirizzo IP per il bilanciatore del carico, un indirizzo IP per il piano di controllo Kubernetes e uno per il nodo.

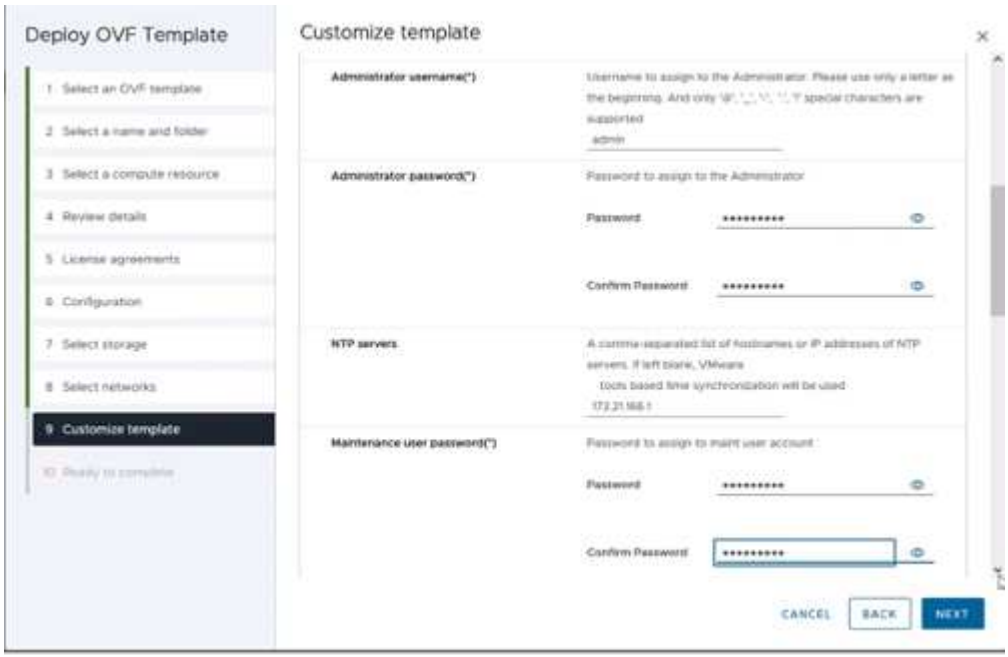
Passi

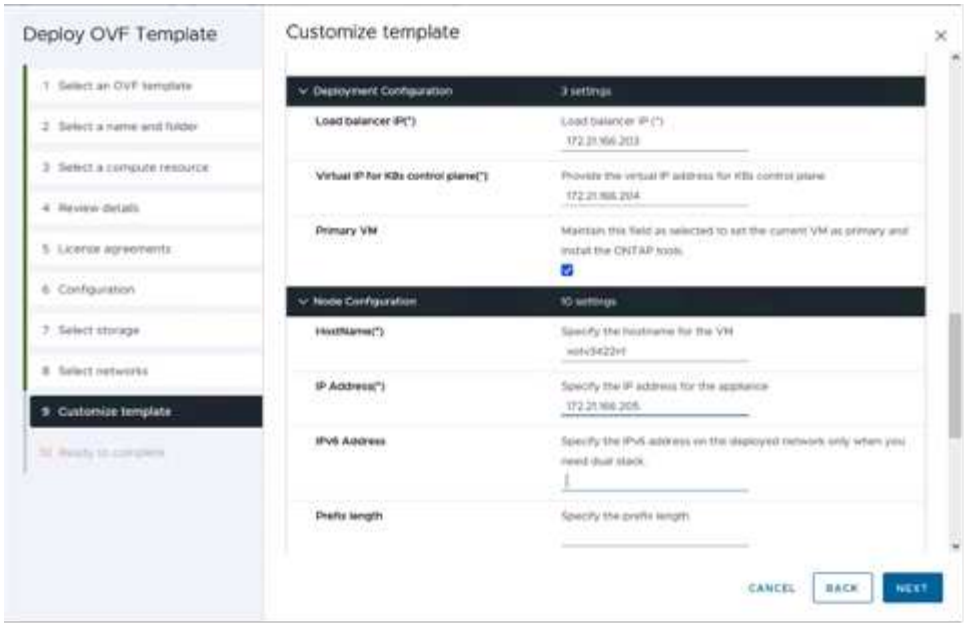
1. Accedi al server vSphere.
2. Passare al cluster o all'host in cui si desidera distribuire l'OVA.
3. Fare clic con il pulsante destro del mouse sulla posizione richiesta e selezionare Distribuisci modello OVF.
   a. Inserisci l'URL del file .ova oppure vai alla cartella in cui è salvato il file .ova, quindi seleziona Avanti.
4. Selezionare un nome, una cartella, un cluster/host per la macchina virtuale e selezionare Avanti.
5. Nella finestra Configurazione, selezionare la configurazione Distribuzione semplice (S), Distribuzione semplice (M) o Distribuzione avanzata (S) o Distribuzione avanzata (M).

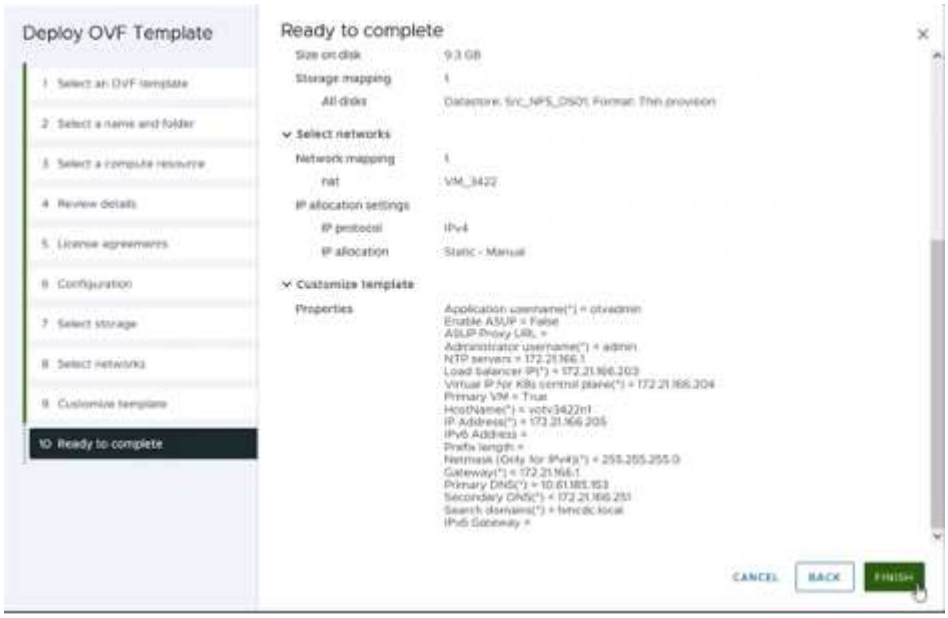
   > In questa procedura dettagliata viene utilizzata l'opzione di distribuzione semplice.



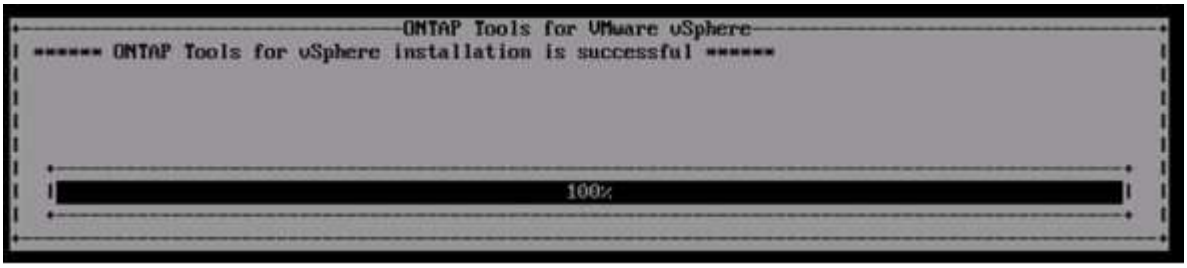
6. Selezionare il datastore in cui distribuire l'OVA e la rete di origine e di destinazione. Una volta fatto, seleziona Avanti.
7. È il momento di personalizzare il modello > finestra di configurazione del sistema.







Dopo l’installazione corretta, la console Web mostra lo stato degli ONTAP tools for VMware vSphere.

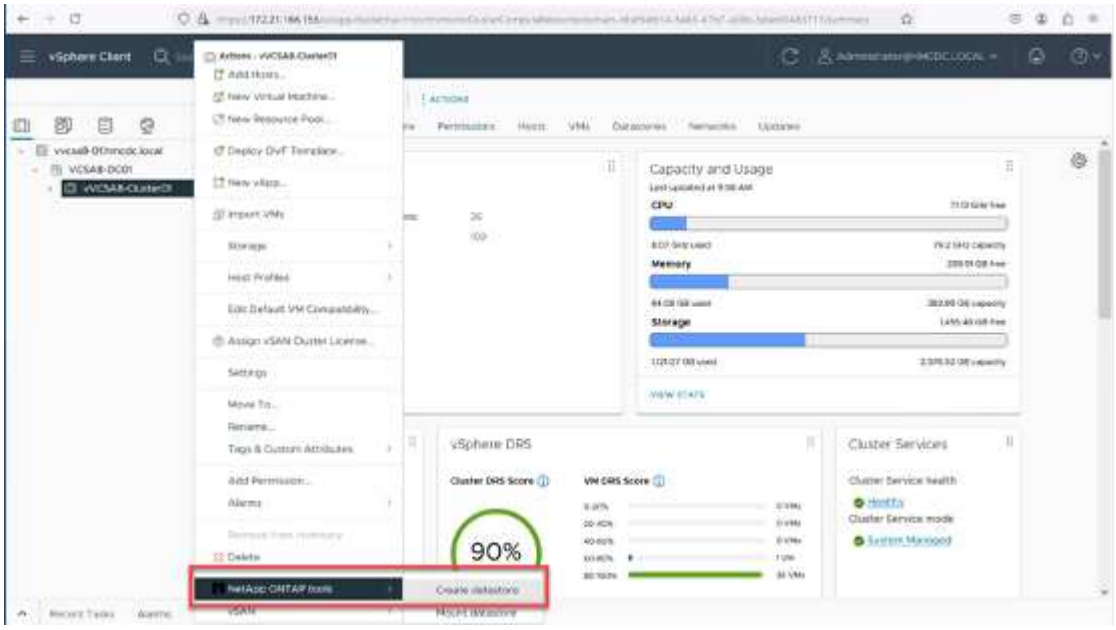


```
ONTAP tools for VMware vSphere

System IP addresses:
 IPv4 address: 172.21.166.205

APPLICATION STATUS:
ONTAP Tools for VMware vSphere is in Healthy State.
VasaProvider and SRA are Enabled and Running.
VasaProviderURL: https://172.21.166.203/virtualization/version.xml
API Documentation is available at https://172.21.166.203:8443/


votv3422n1 login: _
```

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

Per questa procedura dettagliata è il momento di predisporre datastore VMFS basati su ISCSI.

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



3. Nel riquadro Tipo, selezionare VMFS in Tipo di 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, seleziona il cluster Datastore a cui vuoi aggiungere questo datastore.

5. Selezionare Piattaforma e VM di archiviazione nel riquadro Archiviazione. Specificare il nome del gruppo di iniziatori personalizzati nella sezione Opzioni avanzate del riquadro (facoltativo). È possibile scegliere un igroup esistente per il datastore oppure crearne uno nuovo con un nome personalizzato.

6. Nel riquadro degli attributi di archiviazione, selezionare Aggrega dal menu a discesa. Selezionare Spazio riservato, opzione volume e Abilita opzioni QoS come richiesto dalla sezione 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.

Fare riferimento a questi link per il provisioning dei datastore vVol, FC, NVMe/TCP.

Scarico VAAI

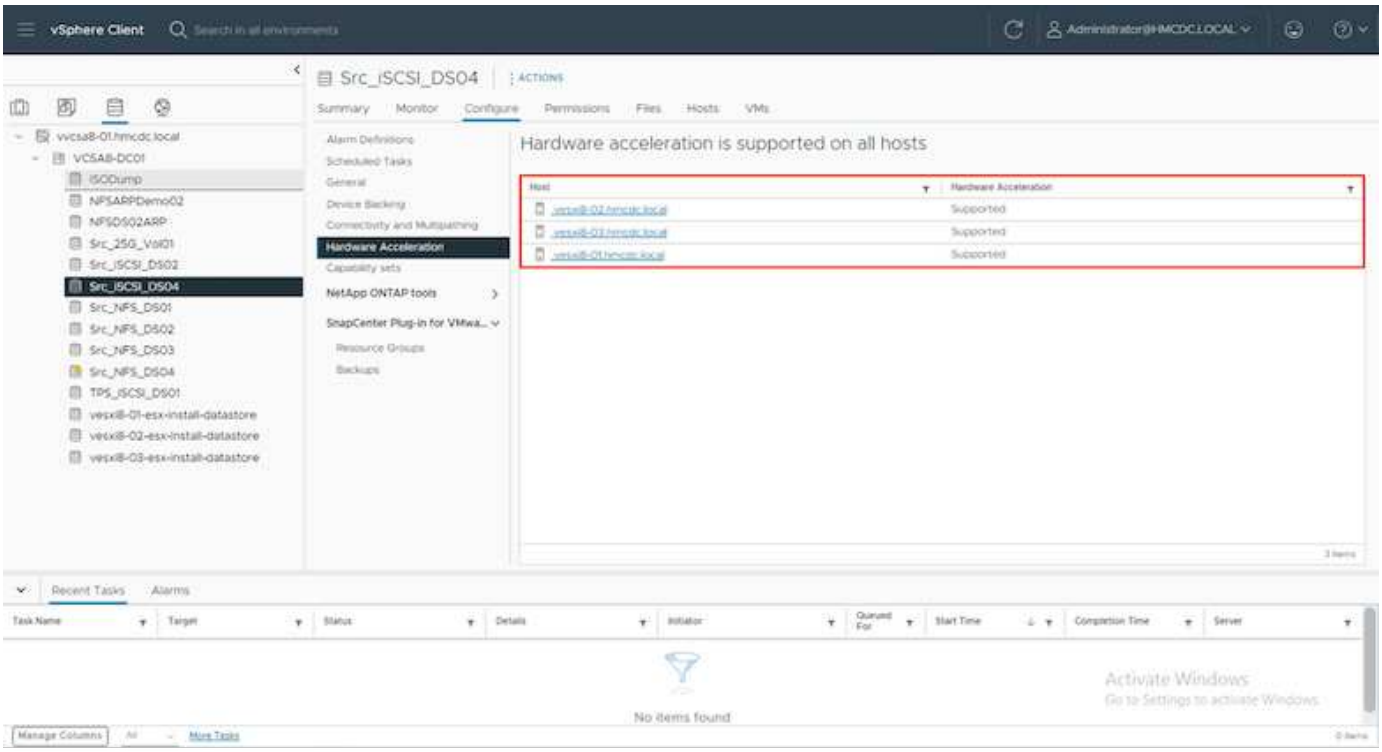
Le primitive VAAI vengono utilizzate nelle operazioni vSphere di routine, come la creazione, la clonazione, la migrazione, l'avvio e l'arresto delle VM. Per semplicità, queste operazioni possono essere eseguite tramite il client vSphere oppure dalla riga di comando per la creazione di script o per ottenere tempi più precisi. VAAI per SAN è supportato nativamente da ESX. VAAI è sempre abilitato sui sistemi di storage NetApp supportati e fornisce supporto nativo per le seguenti operazioni VAAI su storage SAN:

- Copia scarica
- Blocco Atomic Test & Set (ATS)
- Scrivi lo stesso
- Gestione delle condizioni fuori dallo spazio
- Recupero 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
```

Assicurarsi che HardwareAcceleratedMove sia abilitato tramite le opzioni di configurazione avanzate di ESX.

Assicurarsi che la LUN abbia l'opzione "allocazione spazio" abilitata. Se non è abilitata, abilitare l'opzione e ripetere la scansione di tutti gli HBA.

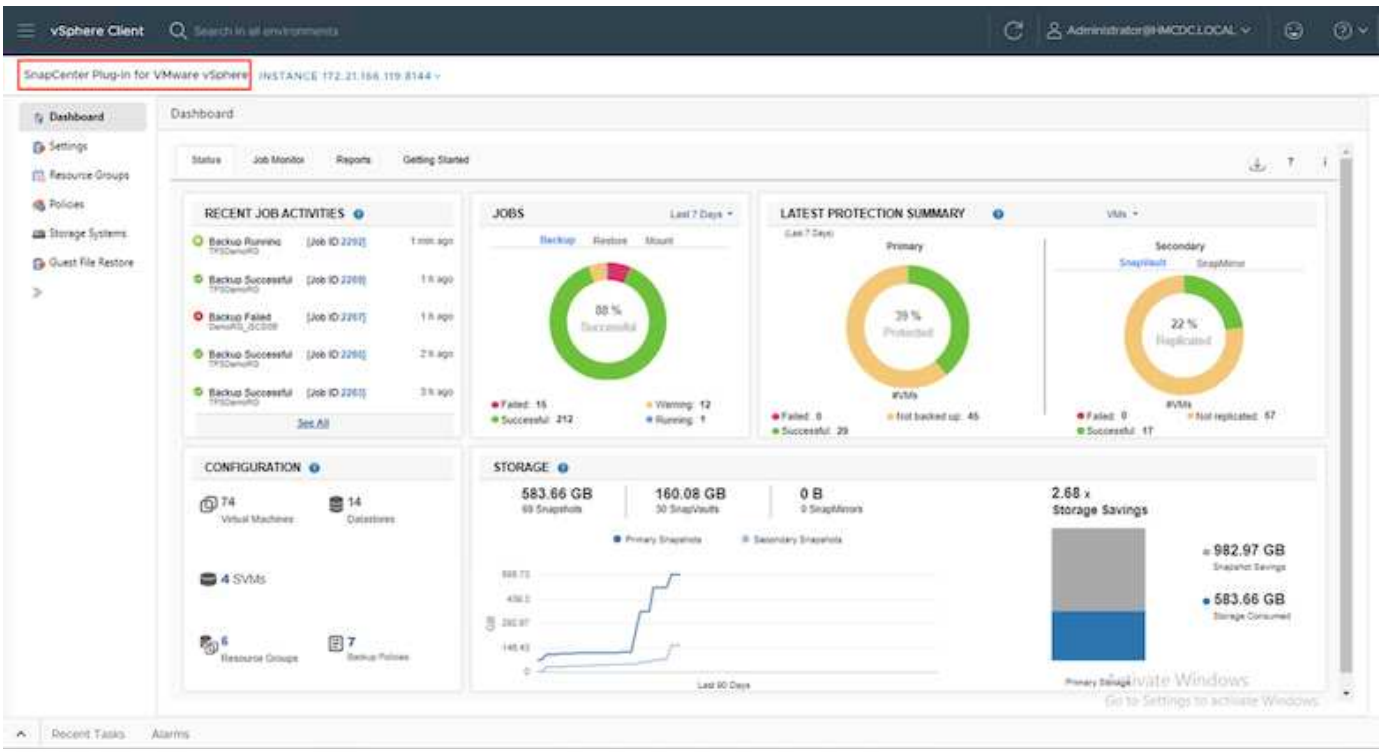


Questi valori possono essere impostati facilmente utilizzando gli ONTAP tools for VMware vSphere. Dalla dashboard Panoramica, vai alla scheda Conformità host ESXi e seleziona l'opzione Applica impostazioni consigliate. Nella finestra Applica impostazioni host consigliate, seleziona gli host e fai clic su Avanti per applicare le impostazioni host consigliate NetApp .

Visualizza la guida dettagliata per"Host ESXi consigliato e altre impostazioni ONTAP" .

Protezione dei dati

Tra i principali vantaggi di ONTAP per vSphere rientrano il backup efficiente delle VM sul datastore VMFS e il loro rapido ripristino. Grazie all'integrazione con vCenter, il software NetApp SnapCenter software offre un'ampia gamma di funzionalità di backup e ripristino per le VM. Fornisce operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con le VM per VM, datastore e VMDK. Funziona anche con SnapCenter Server per supportare operazioni di backup e ripristino basate su applicazioni in ambienti VMware utilizzando plug-in specifici per le applicazioni SnapCenter . Sfruttando le copie Snapshot è possibile effettuare copie rapide della VM o del datastore senza alcun impatto sulle prestazioni e utilizzare la tecnologia NetApp SnapMirror o NetApp SnapVault per una protezione dei dati off-site a lungo termine.



Il flusso di lavoro è semplice. Aggiungere sistemi di archiviazione primari e SVM (e secondari se è necessario SnapMirror/ SnapVault).

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

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

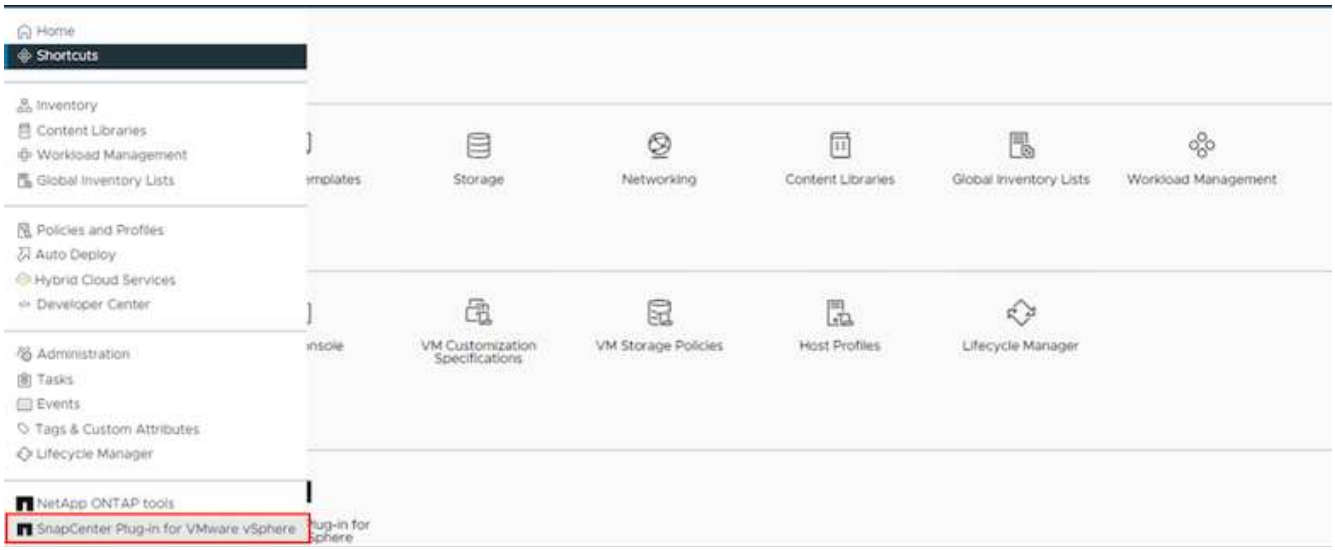
Configurazione del plug-in SnapCenter per VMware per VM

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

I passaggi per la distribuzione sono i seguenti:

1. Scarica l'Open Virtual Appliance (OVA) dal sito di supporto NetApp .
2. Accedi a vCenter.
3. In vCenter, fare clic con il pulsante destro del mouse su un oggetto dell'inventario, ad esempio un data center, una cartella, un cluster o un host, e selezionare Distribuisci modello OVF.
4. Selezionare le impostazioni corrette, tra cui storage e rete, e personalizzare il modello per aggiornare vCenter e le relative credenziali. Dopo aver effettuato la revisione, fare clic su Fine.
5. Attendere il completamento delle attività di importazione e distribuzione OVF.
6. Una volta distribuito correttamente, il plug-in SnapCenter per VMware verrà registrato in vCenter. Lo stesso può essere verificato accedendo ad Amministrazione > Plugin client

7. Per accedere al plug-in, vai sul lato sinistro della pagina del client Web vCenter e seleziona SnapCenter Plug-in per VMware.



Aggiungi spazio di archiviazione, crea criteri e gruppi di risorse

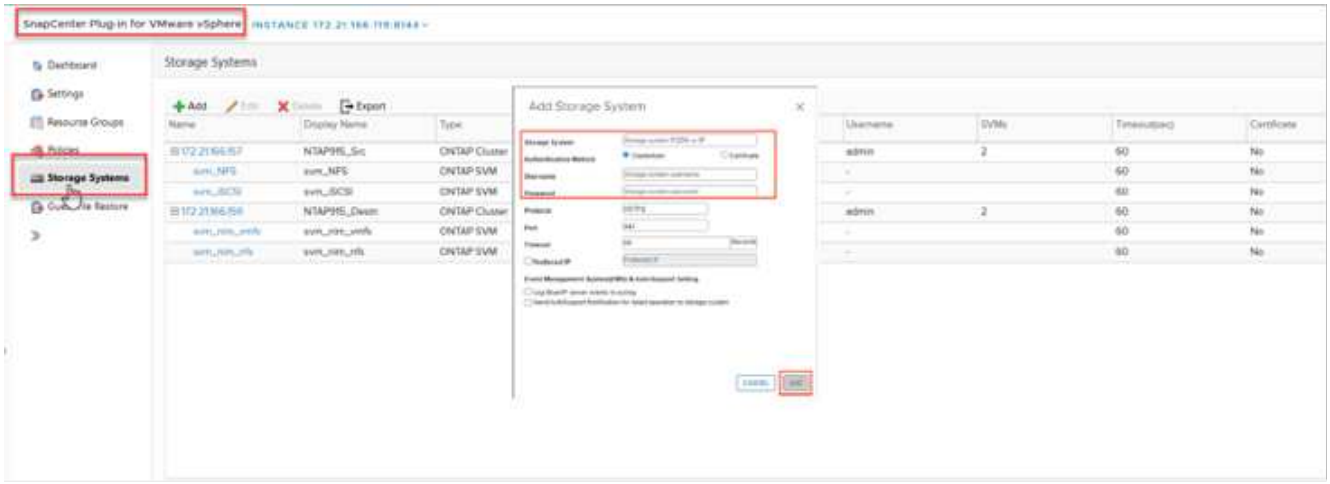
Aggiunta del sistema di archiviazione

Il passo successivo è aggiungere il sistema di archiviazione. L'IP dell'endpoint di gestione del cluster o dell'endpoint di amministrazione della macchina virtuale di archiviazione (SVM) deve essere aggiunto come sistema di archiviazione per eseguire il backup o il ripristino delle VM. L'aggiunta di storage consente al plug-in

SnapCenter per VMware di riconoscere e gestire le operazioni di backup e ripristino in vCenter.

Il procedimento è semplice.

1. Dalla barra di navigazione a sinistra, seleziona SnapCenter Plug-in per VMware.
2. Selezionare Sistemi di archiviazione.
3. Selezionare Aggiungi per aggiungere i dettagli di "archiviazione".
4. Utilizza Credenziali come metodo di autenticazione e inserisci il nome utente e la relativa password, quindi fai clic su Aggiungi per salvare le impostazioni.



Crea una policy di backup

Una strategia di backup completa include fattori quali quando, cosa sottoporre a backup e per quanto tempo conservare i backup. Gli snapshot possono essere attivati ogni ora o ogni giorno per eseguire il backup di interi datastore. Questo approccio non solo cattura i datastore, ma consente anche di eseguire il backup e il ripristino delle VM e dei VMDK all'interno di tali datastore.

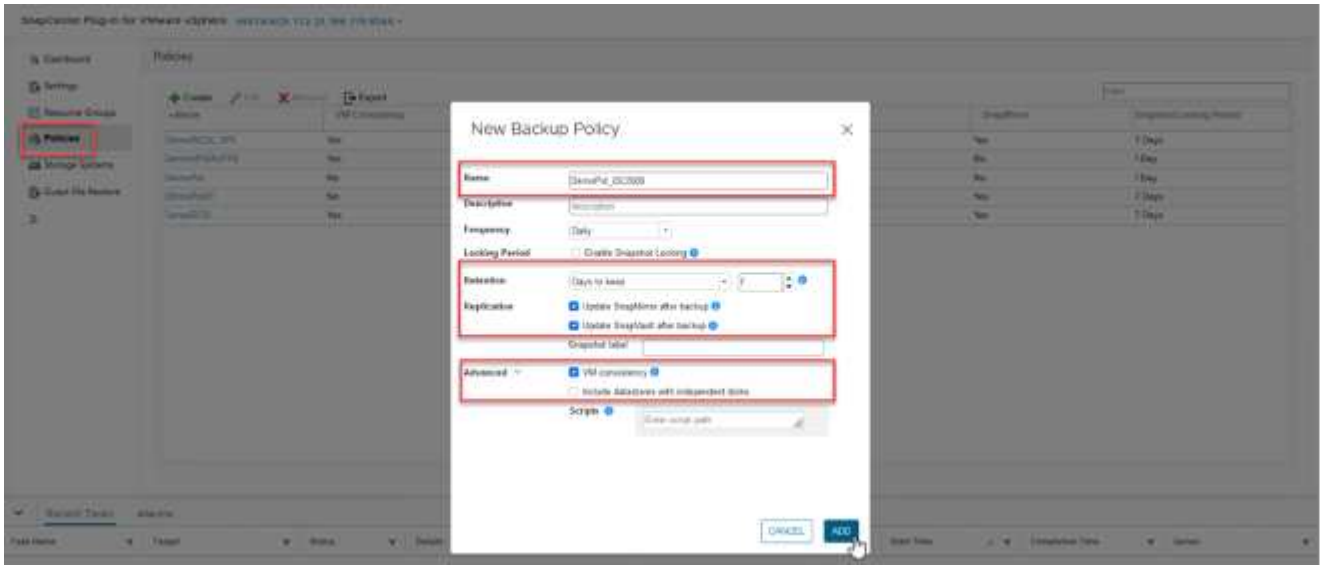
Prima di eseguire il backup delle VM e dei datastore, è necessario creare un criterio di backup e un gruppo di risorse. Una policy di backup include impostazioni quali la pianificazione e la policy di conservazione. Per creare una policy di backup, seguire i passaggi indicati di seguito.

1. Nel riquadro di navigazione sinistro del plug-in SnapCenter per VMware, fare clic su Criteri.
2. Nella pagina Criteri, fare clic su Crea per avviare la procedura guidata.

3. Nella pagina Nuova policy di backup, immettere il nome della policy.
4. Specificare le impostazioni di conservazione, frequenza e replica.

> Per replicare le copie Snapshot su un sistema di archiviazione secondario mirror o vault, è necessario configurare in anticipo le relazioni.

> Per abilitare backup coerenti con la VM, è necessario che gli strumenti VMware siano installati e in esecuzione. Quando la casella Coerenza VM è selezionata, le VM vengono prima messe in stato di quiescenza, quindi VMware esegue uno snapshot coerente con la VM (esclusa la memoria), quindi SnapCenter Plug-in per VMware esegue l'operazione di backup e infine le operazioni della VM vengono riprese.



Una volta creata la policy, il passaggio successivo consiste nel creare il gruppo di risorse che definirà gli archivi dati iSCSI e le VM appropriati di cui eseguire il backup. Dopo aver creato il gruppo di risorse, è il momento di attivare i backup.

Crea gruppo di risorse

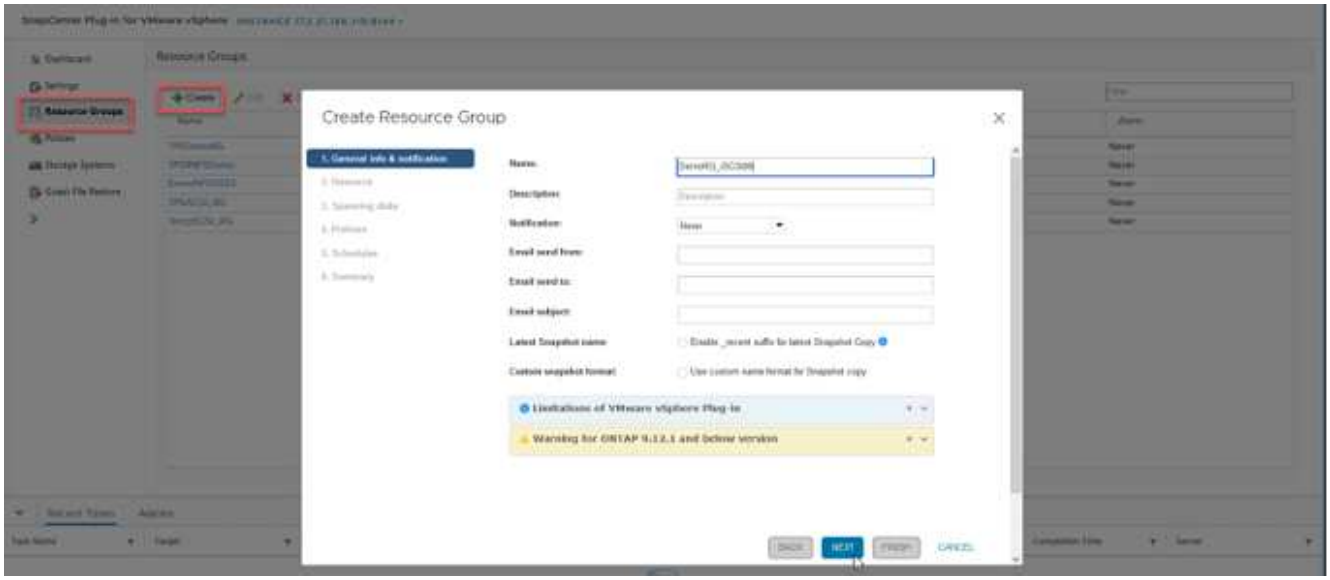
Un gruppo di risorse è il contenitore per le VM e gli archivi dati che devono essere protetti. Le risorse possono essere aggiunte o rimosse dai gruppi di risorse in qualsiasi momento.

Per creare un gruppo di risorse, seguire i passaggi indicati di seguito.

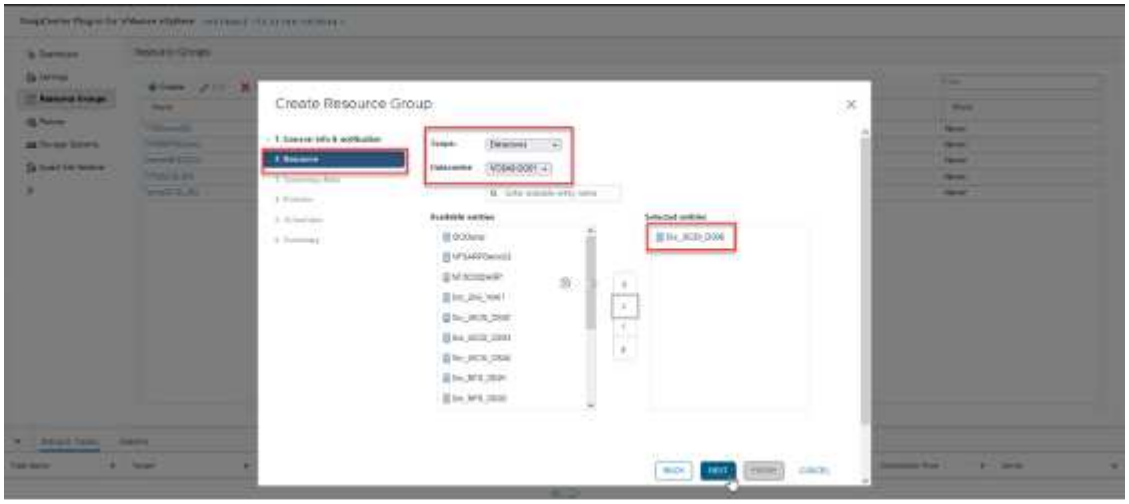
1. Nel riquadro di navigazione sinistro del plug-in SnapCenter per VMware, fare clic su Gruppi di risorse.
2. Nella pagina Gruppi di risorse, fare clic su Crea per avviare la procedura guidata.

   Un'altra opzione per creare un gruppo di risorse è selezionare la singola VM o il singolo datastore e creare

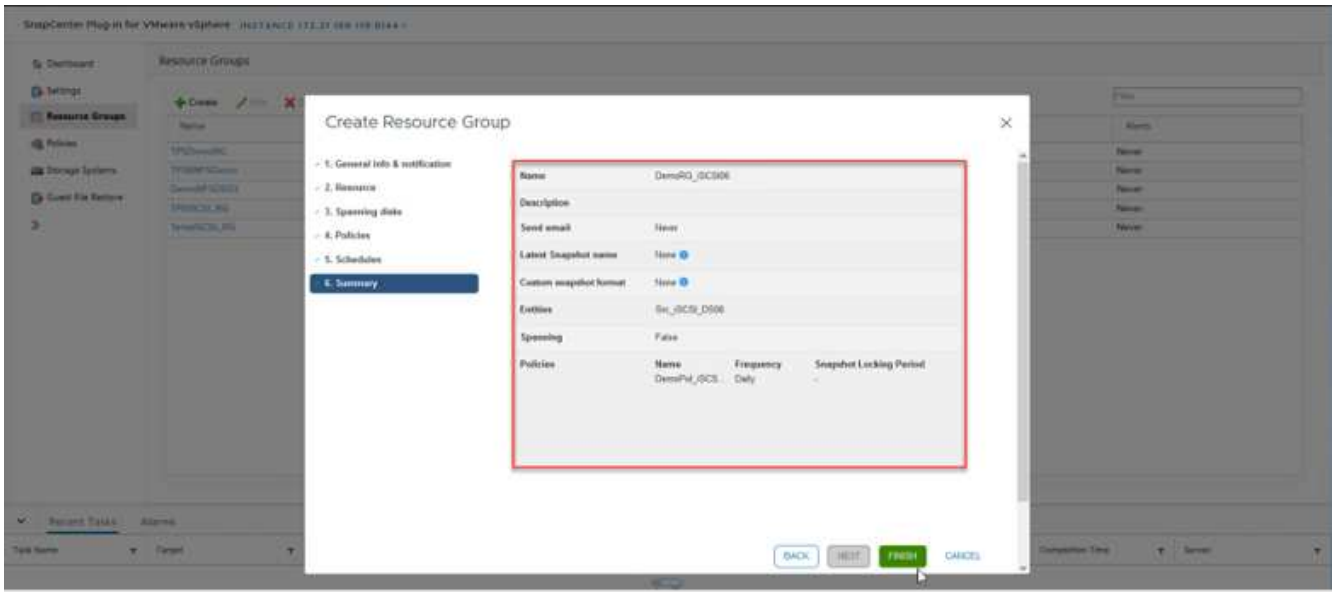
rispettivamente un gruppo di risorse.



3. Nella pagina Risorse, seleziona l'ambito (macchine virtuali o datastore) e il datacenter.

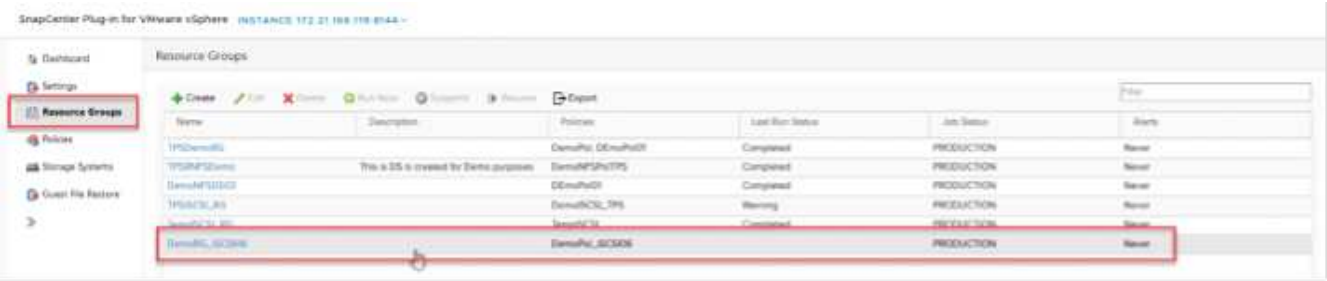


4. Nella pagina Spanning dei dischi, seleziona un'opzione per Macchine virtuali con più VMDK su più datastore
5. Il passo successivo è associare una policy di backup. Seleziona una policy esistente o crea una nuova policy di backup.
6. Nella pagina Pianificazioni, configura la pianificazione del backup per ogni criterio selezionato.



7. Una volta effettuate le selezioni appropriate, fare clic su Fine.

   Verrà creato un nuovo gruppo di risorse e aggiunto all'elenco dei gruppi di risorse.

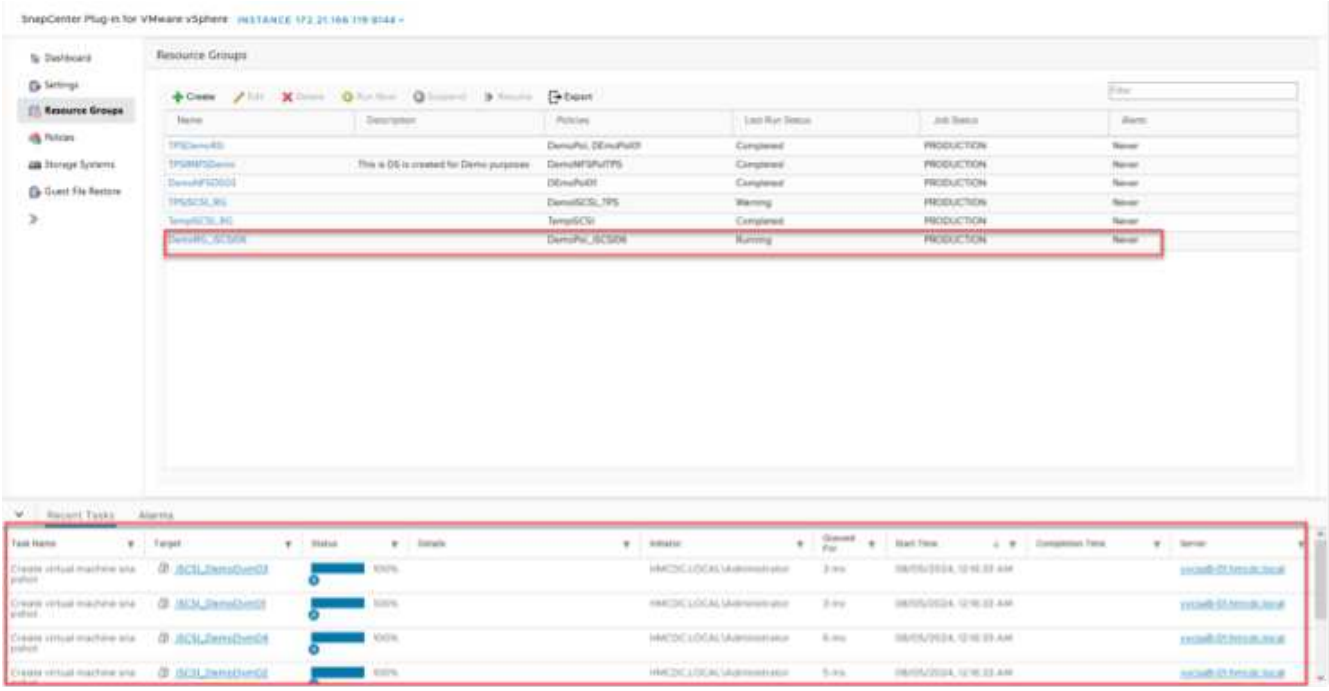


Eseguire il backup dei gruppi di risorse

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

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

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

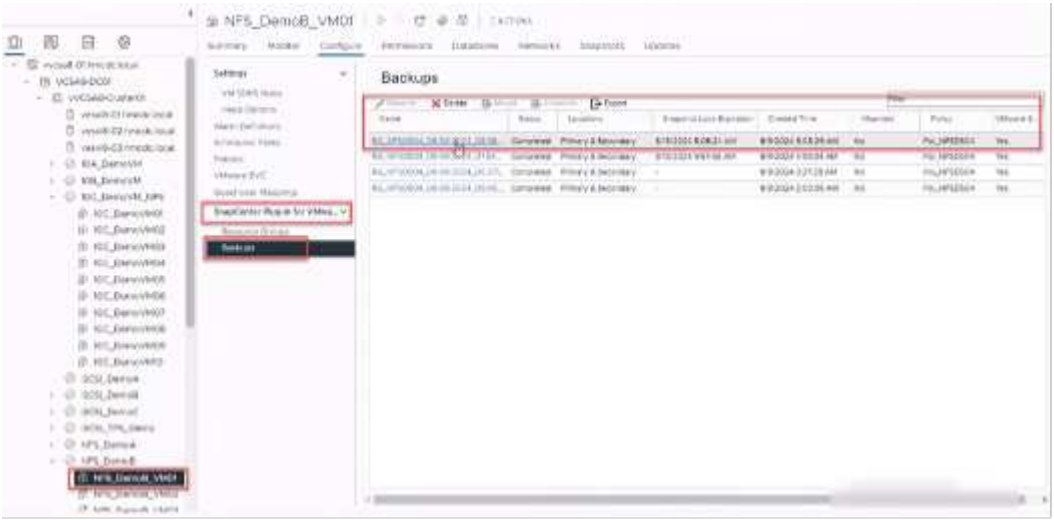


Per maggiori dettagli, monitora l'avanzamento dell'operazione selezionando Attività recenti nella parte inferiore della finestra o nel pannello Monitoraggio attività.

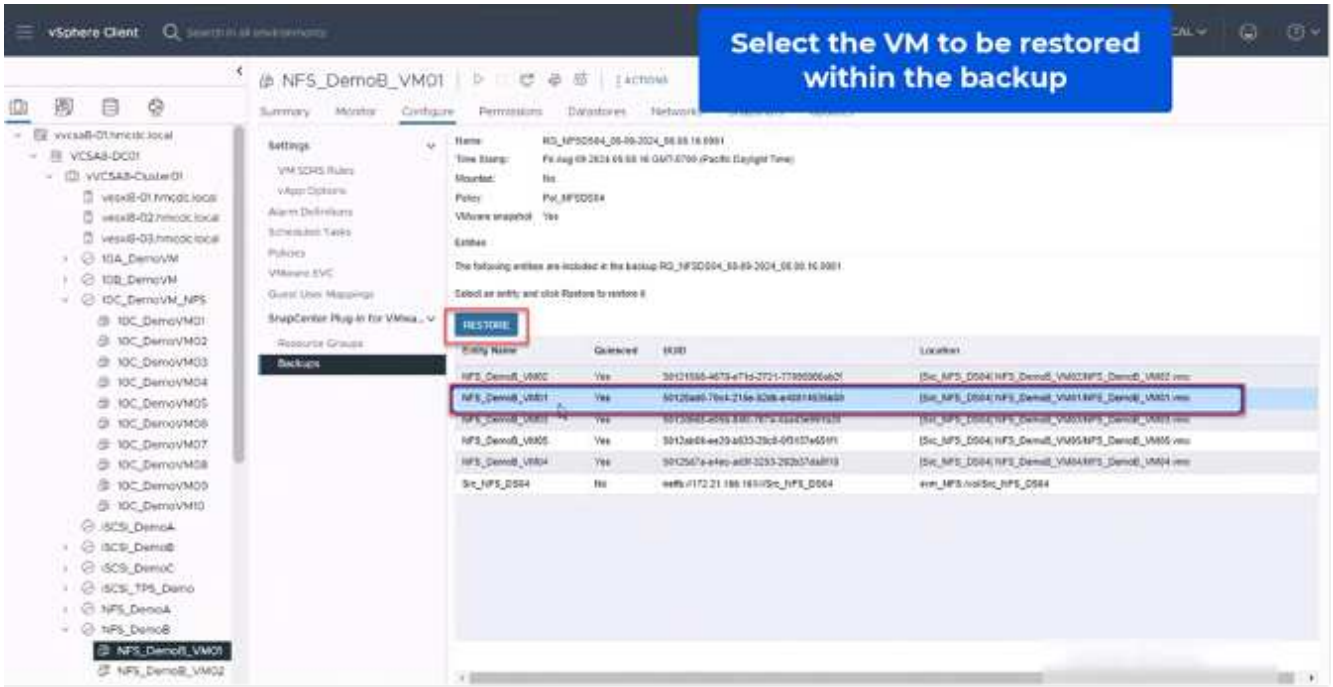
Ripristinare le VM dal backup

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

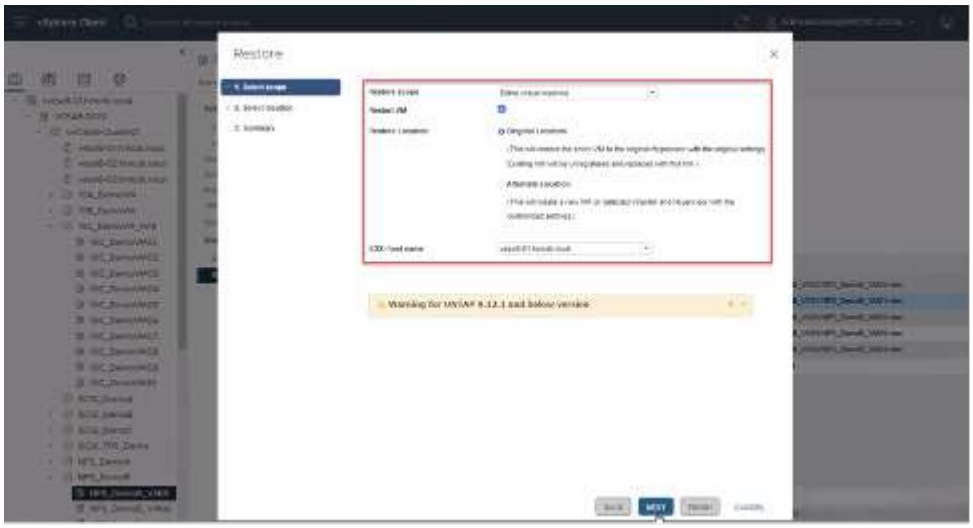
1. Nell'interfaccia utente grafica del client Web VMware vSphere, selezionare Menu nella barra degli strumenti. Selezionare Inventario e quindi Macchine virtuali e modelli.
2. Nella barra di navigazione a sinistra, seleziona la macchina virtuale, quindi seleziona la scheda Configura, seleziona Backup in SnapCenter Plug-in per VMware. Fare clic sul processo di backup da cui si desidera ripristinare la macchina virtuale.



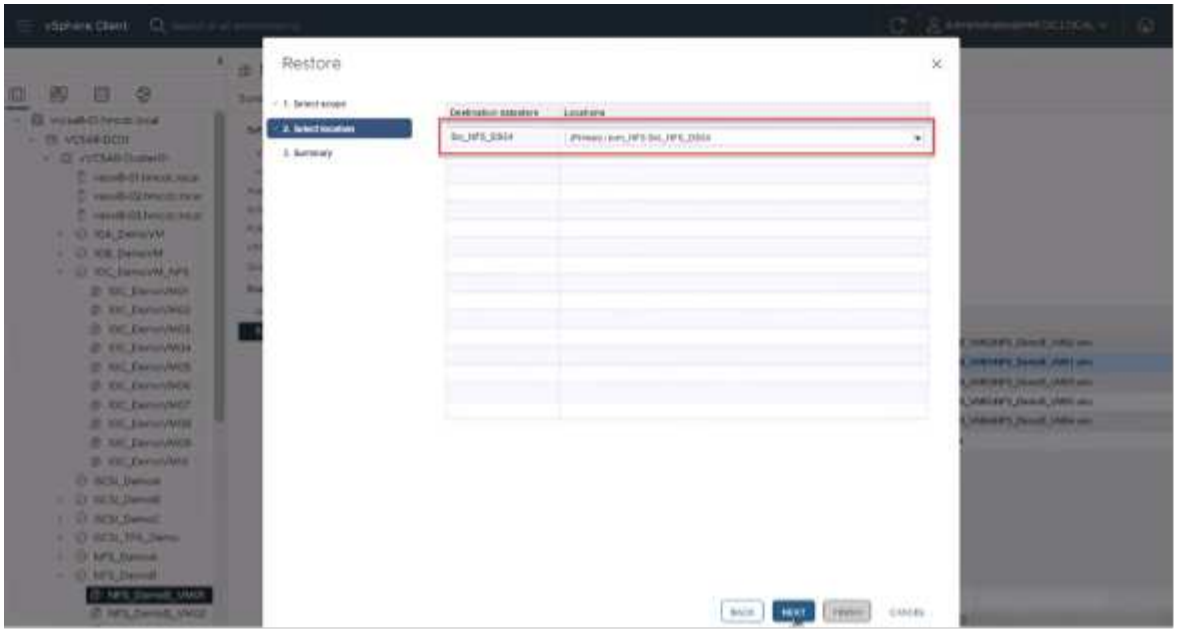
3. Selezionare la VM che deve essere ripristinata dal backup.



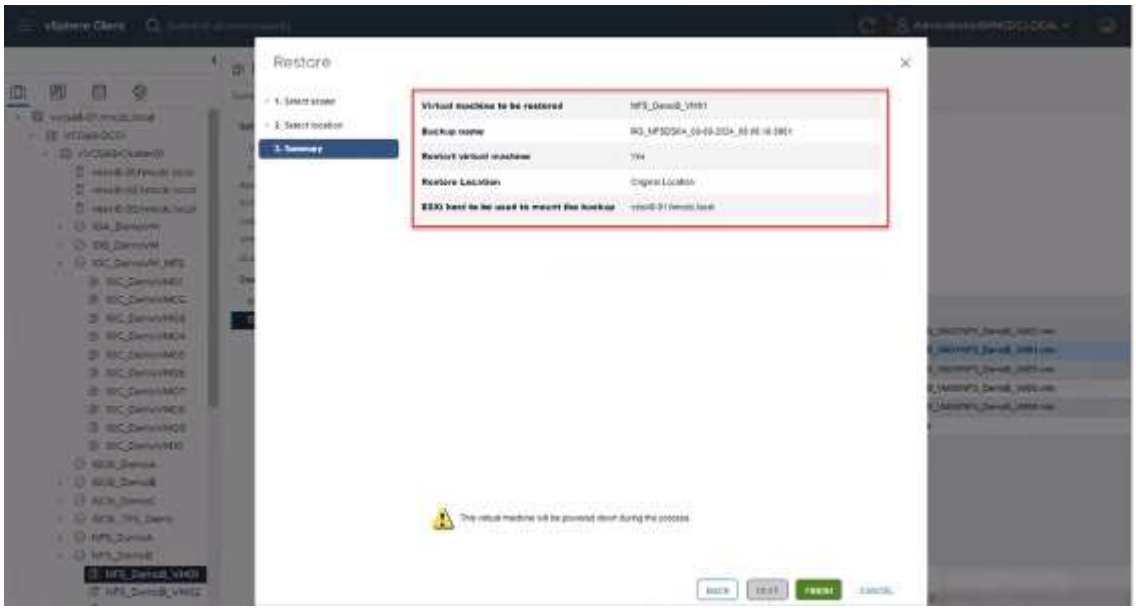
4. Nella pagina Seleziona ambito, seleziona Intera macchina virtuale nel campo Ambito di ripristino, quindi seleziona Posizione di ripristino e infine immetti le informazioni ESXi di destinazione in cui deve essere montato il backup. Abilitare la casella di controllo Riavvia VM se la VM deve essere accesa dopo l'operazione di ripristino.



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



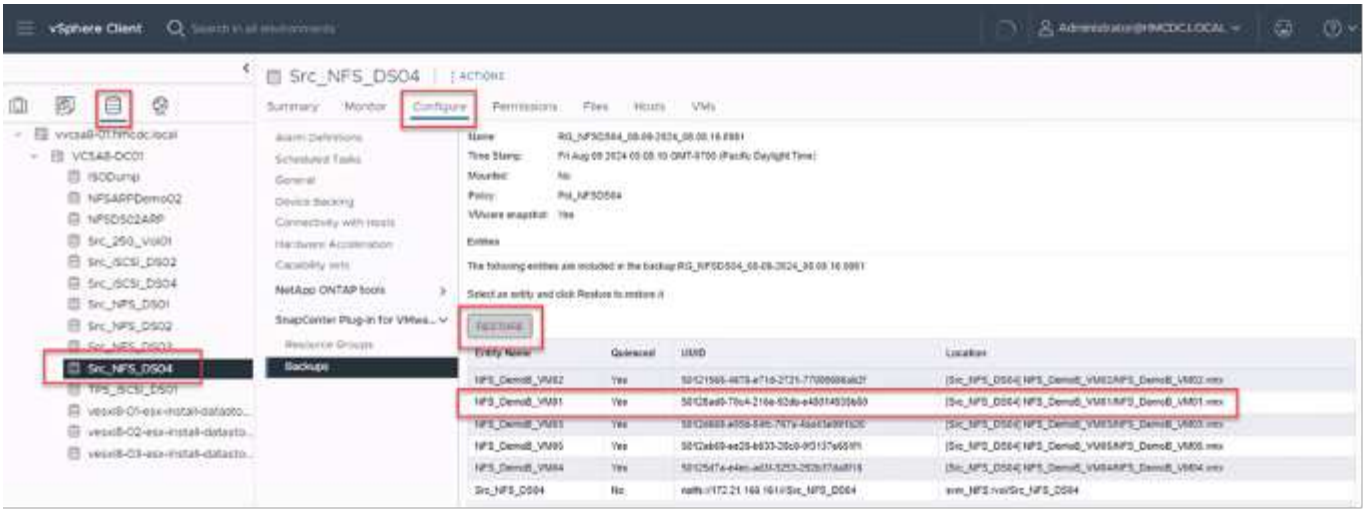
6. Rivedi la pagina Riepilogo e poi seleziona Fine.



Monitora l'avanzamento dell'operazione selezionando Attività recenti nella parte inferiore dello schermo.

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

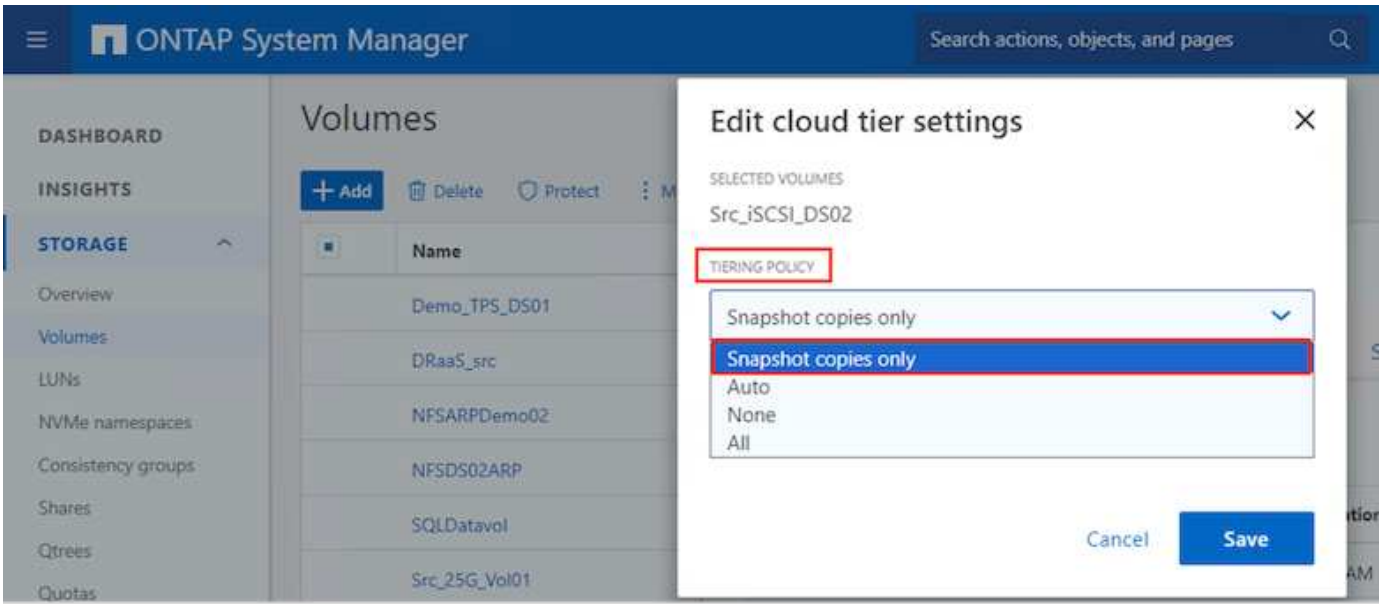
E se la VM originale fosse stata eliminata? È un'operazione semplice con il plug-in SnapCenter per VMware. L'operazione di ripristino di una VM eliminata può essere eseguita a livello di datastore. Vai al rispettivo Datastore > Configura > Backup e seleziona la VM eliminata, quindi seleziona Ripristina.



Riassumendo, quando si utilizza l'archiviazione ONTAP ASA per ottimizzare il TCO per una distribuzione VMware, utilizzare il plug-in SnapCenter per VMware come metodo semplice ed efficiente per il backup delle VM. Consente di eseguire il backup e il ripristino delle VM in modo rapido e senza interruzioni, poiché i backup snapshot richiedono letteralmente pochi secondi per essere completati.

Fare riferimento a questo"guida alla soluzione" E"documentazione del prodotto" per saperne di più sulla configurazione di Snapcenter, sul backup e sul ripristino dal sistema di archiviazione primario o secondario o anche dai backup archiviati su storage di oggetti per la conservazione a lungo termine.

Per ridurre i costi di archiviazione, è possibile abilitare la suddivisione in livelli del volume FabricPool per spostare automaticamente i dati per le copie snapshot su un livello di archiviazione più economico. Le copie snapshot in genere utilizzano oltre il 10% dello spazio di archiviazione allocato. Sebbene importanti per la protezione dei dati e il ripristino in caso di emergenza, queste copie puntuali vengono raramente utilizzate e non rappresentano un utilizzo efficiente dello storage ad alte prestazioni. Con la policy "Snapshot-Only" per FabricPool, puoi liberare facilmente spazio su storage ad alte prestazioni. Quando questa policy è abilitata, i blocchi di copia snapshot inattivi nel volume che non vengono utilizzati dal file system attivo vengono spostati nel livello oggetto e, una volta letti, la copia snapshot viene spostata nel livello locale per ripristinare una VM o un intero datastore. Questo livello di oggetti può essere sotto forma di cloud privato (ad esempio NetApp StorageGRID) o di cloud pubblico (ad esempio AWS o Azure).

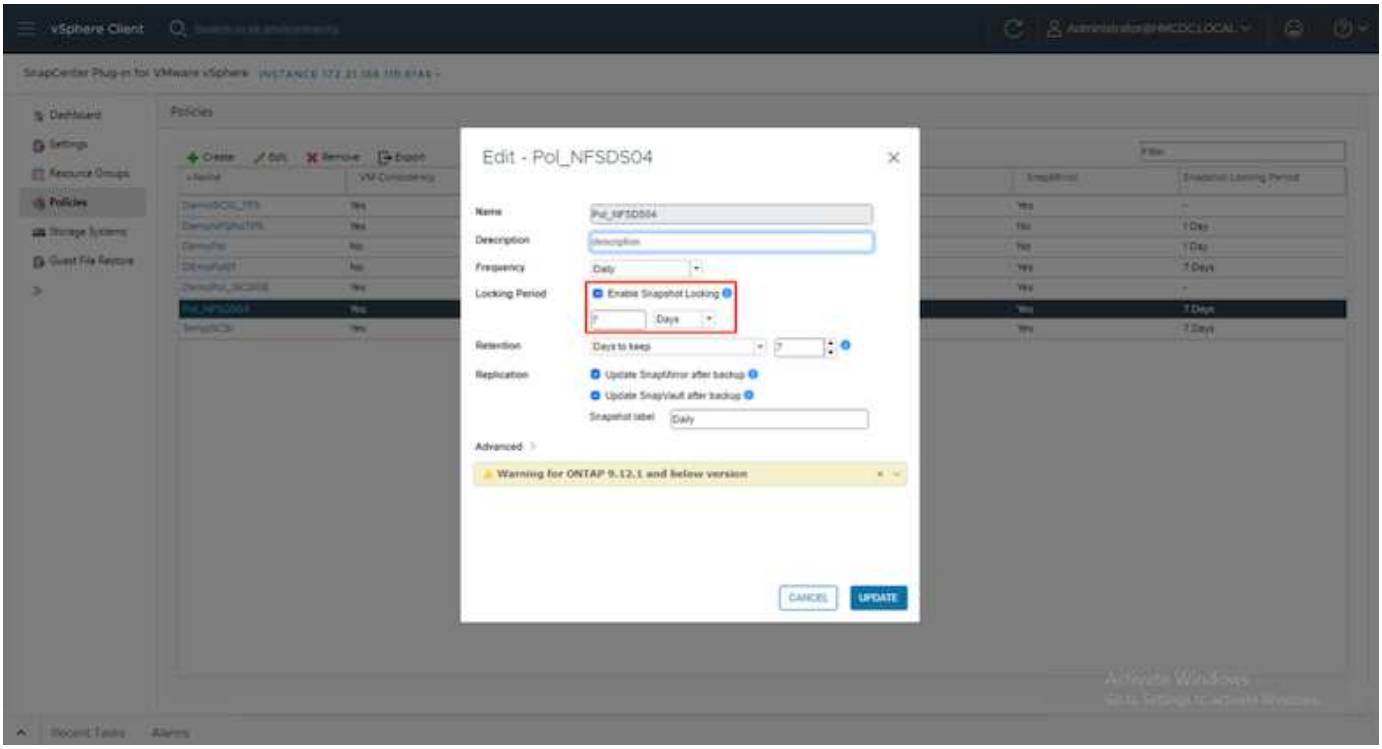


Visualizza la guida dettagliata per"VMware vSphere con ONTAP" .

Protezione ransomware

Uno dei metodi più efficaci per proteggersi dagli attacchi ransomware è l'implementazione di misure di sicurezza multilivello. Ogni macchina virtuale residente su un datastore ospita un sistema operativo standard. Assicurarsi che le suite di prodotti antimalware sui server aziendali siano installate e aggiornate regolarmente, il che rappresenta un componente essenziale della strategia di protezione anti-ransomware multilivello. Oltre a ciò, implementa la protezione dei dati sfruttando la tecnologia snapshot NetApp per garantire un ripristino rapido e affidabile da un attacco ransomware.

Gli attacchi ransomware prendono sempre più di mira i backup e i punti di ripristino degli snapshot, tentando di eliminarli prima di iniziare a crittografare i file. Tuttavia, con ONTAP questo può essere impedito creando snapshot a prova di manomissione sui sistemi primari o secondari con"Blocco della copia snapshot NetApp" ONTAP. Queste copie Snapshot non possono essere eliminate o modificate da aggressori ransomware o amministratori non autorizzati, quindi sono disponibili anche dopo un attacco. È possibile recuperare i dati delle macchine virtuali in pochi secondi, riducendo al minimo i tempi di inattività dell'organizzazione. Inoltre, hai la flessibilità di scegliere la pianificazione degli snapshot e la durata del blocco più adatte alla tua organizzazione.



Come parte dell'approccio a più livelli, è presente anche una soluzione ONTAP nativa integrata per proteggere dall'eliminazione non autorizzata delle copie di backup Snapshot. È nota come verifica multiadmin o MAV ed è disponibile in ONTAP 9.11.1 e versioni successive. L'approccio ideale sarà quello di utilizzare query per operazioni specifiche MAV.

Per saperne di più su MAV e su come configurare le sue capacità di protezione, vedere"Panoramica della verifica multi-amministratore" .

Migrazione

Molte organizzazioni IT stanno adottando un approccio cloud-first ibrido mentre attraversano una fase di trasformazione. Sulla base di questa valutazione e scoperta, i clienti stanno valutando la loro attuale infrastruttura IT e spostando i carichi di lavoro sul cloud. Le ragioni per migrare verso il cloud variano e

possono includere fattori quali elasticità e burst, uscita dal data center, consolidamento del data center, scenari di fine vita, fusioni, acquisizioni e altro ancora. Le motivazioni che spingono ogni organizzazione a procedere con la migrazione dipendono dalle sue specifiche priorità aziendali, con l'ottimizzazione dei costi come priorità assoluta. Quando si passa al cloud ibrido, è fondamentale scegliere il giusto storage cloud, poiché consente di sfruttare al meglio la potenza e l'elasticità dell'implementazione cloud.

Grazie all'integrazione con i servizi 1P forniti da NetApp su ogni iperscalare, le organizzazioni possono realizzare una soluzione cloud basata su vSphere con un semplice approccio di migrazione, senza dover riorganizzare la piattaforma, modificare l'IP o apportare modifiche all'architettura. Inoltre, questa ottimizzazione consente di ridimensionare l'ingombro dello storage mantenendo il numero di host al minimo richiesto in vSphere, senza apportare alcuna modifica alla gerarchia di storage, alla sicurezza o ai file resi disponibili.

- Visualizza la guida dettagliata per"Migrazione dei carichi di lavoro al datastore FSx ONTAP" .
- Visualizza la guida dettagliata per"Migrare i carichi di lavoro al datastore di Azure NetApp Files" .
- Visualizza la guida dettagliata per"Migrazione dei carichi di lavoro al datastore Google Cloud NetApp Volumes" .

Ripristino dopo un disastro

Disaster Recovery tra siti on-premise

Per maggiori dettagli, visitare"DR tramite BlueXP DRaaS per datastore VMFS"

Disaster Recovery tra locale e VMware Cloud in qualsiasi ambiente iperscalare

Per i clienti che desiderano utilizzare VMware Cloud su qualsiasi sistema iperscalare come destinazione di disaster recovery, è possibile utilizzare gli archivi dati basati su storage ONTAP (Azure NetApp Files, FSx ONTAP, volumi Google Cloud NetApp) per replicare i dati da locale tramite qualsiasi soluzione di terze parti convalidata che fornisca funzionalità di replica delle VM. Aggiungendo datastore basati su storage ONTAP , sarà possibile ottimizzare i costi del disaster recovery sulla destinazione con un numero inferiore di host ESXi. Ciò consente anche di dismettere il sito secondario nell'ambiente locale, consentendo così notevoli risparmi sui costi.

- Visualizza la guida dettagliata per"Ripristino di emergenza su datastore FSx ONTAP" .
- Visualizza la guida dettagliata per"Ripristino di emergenza nell'archivio dati Azure NetApp Files" .
- Visualizza la guida dettagliata per"Ripristino di emergenza nel datastore Google Cloud NetApp Volumes" .

Conclusione

Questa soluzione dimostra l'approccio ottimale all'utilizzo delle tecnologie ONTAP SAN e degli strumenti Offtap per fornire servizi IT essenziali alle aziende, sia ora che in futuro. Questi vantaggi sono particolarmente utili per gli ambienti virtualizzati che eseguono VMware vSphere in una configurazione SAN. Grazie alla flessibilità e alla scalabilità dei sistemi di storage NetApp , le organizzazioni possono gettare le basi per aggiornare e adattare la propria infrastruttura, in modo da soddisfare le mutevoli esigenze aziendali nel tempo. Questo sistema è in grado di gestire i carichi di lavoro attuali e migliorare l'efficienza dell'infrastruttura, riducendo così i costi operativi e preparando per i carichi di lavoro futuri.

Utilizzare nConnect sui datastore NFS v3 per migliorare le prestazioni del datastore

Utilizzare la funzionalità NFS nConnect per migliorare le prestazioni del datastore negli

ambienti VMware vSphere 8. Questa procedura include l'hosting di VM per datastore NFS, l'aumento delle prestazioni del datastore NFS e la configurazione di un livello superiore per le applicazioni basate su VM e container.

A partire da VMware vSphere 8.0 U1 (come anteprima tecnica), la funzionalità nconnect consente più connessioni TCP per i volumi di datastore NFS v3 per ottenere una maggiore produttività. I clienti che utilizzano l'archivio dati NFS possono ora aumentare il numero di connessioni al server NFS, massimizzando così l'utilizzo delle schede di interfaccia di rete ad alta velocità.

> La funzionalità è generalmente disponibile per NFS v3 con 8.0 U2, fare riferimento alla sezione di archiviazione su"Note di rilascio di VMware vSphere 8.0 Update 2" . Il supporto NFS v4.1 è stato aggiunto con vSphere 8.0 U3. Per maggiori informazioni, consultare"Note sulla versione di vSphere 8.0 Update 3"

Casi d'uso

- Ospita più macchine virtuali per datastore NFS sullo stesso host.
- Migliora le prestazioni del datastore NFS.
- Fornire un'opzione per offrire un servizio a un livello superiore per le applicazioni basate su VM e container.

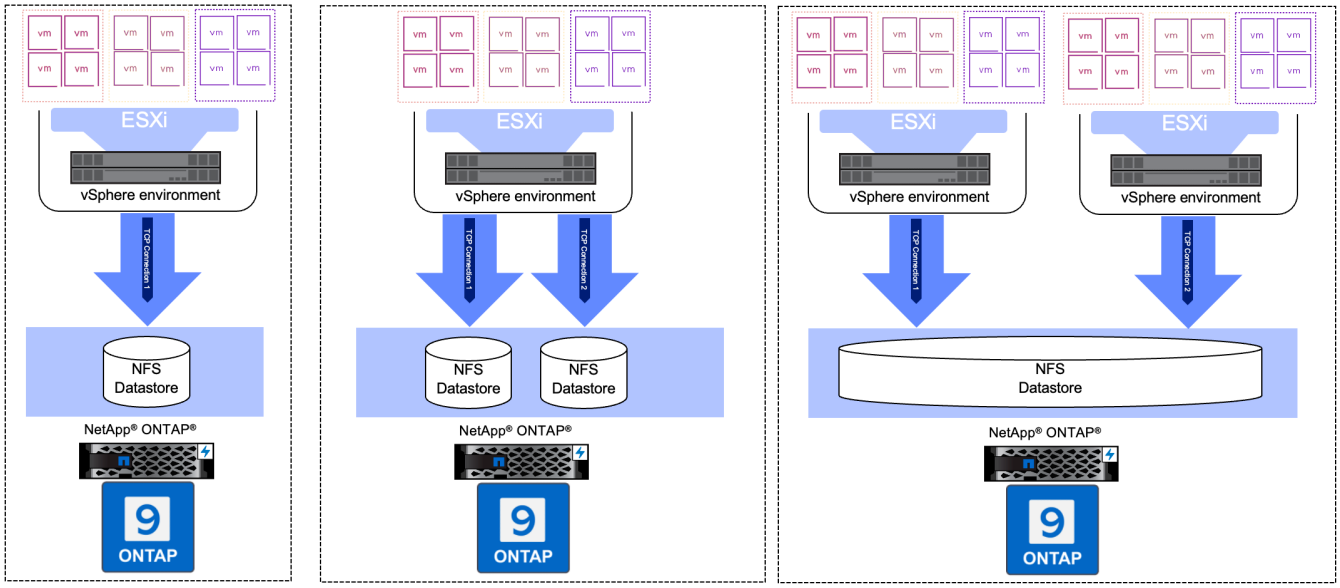
Dettagli tecnici

Lo scopo di nconnect è fornire più connessioni TCP per ogni datastore NFS su un host vSphere. Ciò contribuisce ad aumentare il parallelismo e le prestazioni dei datastore NFS. In ONTAP, quando viene stabilito un montaggio NFS, viene creato un ID di connessione (CID). Tale CID consente fino a 128 operazioni di volo simultanee. Quando il client supera tale numero, ONTAP attua una forma di controllo del flusso finché non riesce a liberare alcune risorse disponibili mentre vengono completate altre operazioni. Queste pause durano solitamente solo pochi microsecondi, ma nel corso di milioni di operazioni possono sommarsi e creare problemi di prestazioni. Nconnect può prendere il limite di 128 e moltiplicarlo per il numero di sessioni nconnect sul client, il che fornisce più operazioni simultanee per CID e può potenzialmente aggiungere vantaggi in termini di prestazioni. Per ulteriori dettagli, fare riferimento"Guida alle migliori pratiche e all'implementazione di NFS"

Archivio dati NFS predefinito

Per risolvere i limiti di prestazioni della singola connessione del datastore NFS, vengono montati datastore aggiuntivi o aggiunti host aggiuntivi per aumentare la connessione.

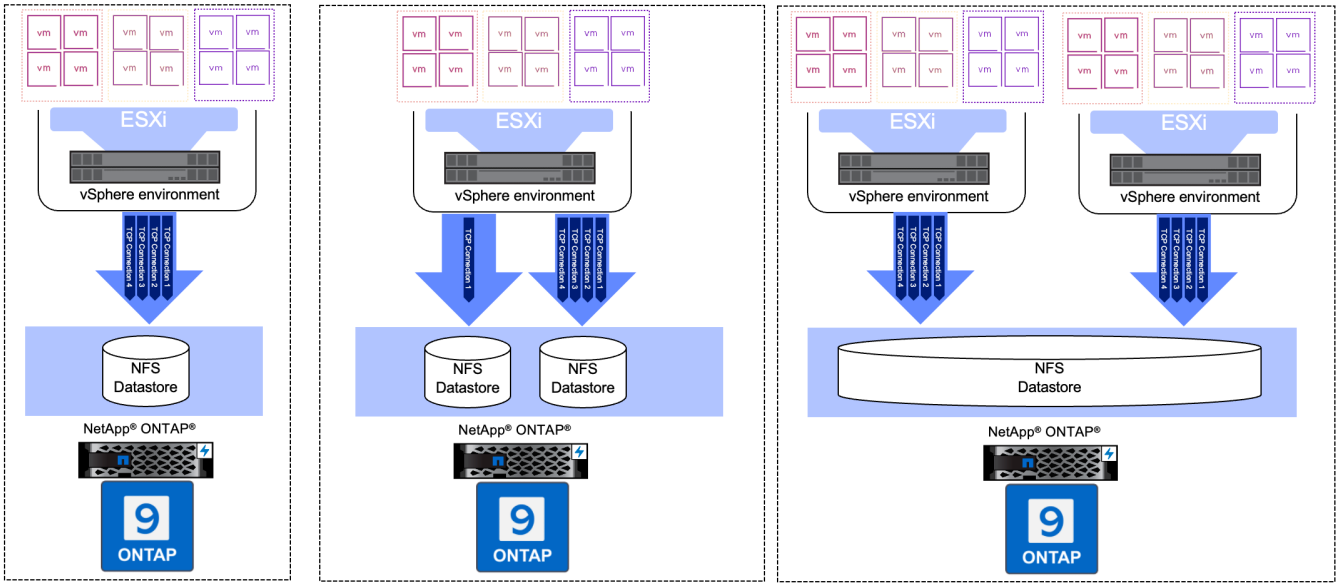
Without nConnect feature with NetApp and VMware



Con nConnect NFS Datastore

Una volta creato il datastore NFS tramite ONTAP Tools o altre opzioni, il numero di connessioni per datastore NFS può essere modificato tramite vSphere CLI, PowerCLI, govc tool o altre opzioni API. Per evitare problemi di prestazioni con vMotion, mantenere lo stesso numero di connessioni per il datastore NFS su tutti gli host vSphere che fanno parte del cluster vSphere.

With nConnect feature with NetApp and VMware



Prerequisito

Per utilizzare la funzionalità nconnect, è necessario soddisfare le seguenti dipendenze.

Versione ONTAP	Versione vSphere	Commenti
9.8 o superiore	8 Aggiornamento 1	Anteprima tecnica con possibilità di aumentare il numero di connessioni. È necessario smontare il datastore per ridurre il numero di connessioni.
9.8 o superiore	8 Aggiornamento 2	Generalmente disponibile con l'opzione di aumentare e diminuire il numero di connessioni.
9.8 o superiore	8 Aggiornamento 3	Supporto NFS 4.1 e multi-path.

Aggiorna il numero di connessione al datastore NFS

Quando si crea un datastore NFS con ONTAP Tools o con vCenter, viene utilizzata una singola connessione TCP. Per aumentare il numero di connessioni, è possibile utilizzare vSphere CLI. Di seguito è riportato il comando di riferimento.

```
# 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 simile a quello mostrato 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 un esempio di come 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"Articolo 91497 della Knowledge Base di VMware" per maggiori informazioni.

Considerazioni di progettazione

Il numero massimo di connessioni supportate su ONTAP dipende dal modello della piattaforma di archiviazione. Cerca exec_ctx su"Guida alle migliori pratiche e all'implementazione di NFS" per maggiori informazioni.

Con l'aumento del numero di connessioni per datastore NFSv3, diminuisce il numero di datastore NFS che possono essere montati su quell'host vSphere. Il numero totale di connessioni supportate per host vSphere è 256. Controllo"Articolo 91481 della Knowledge Base di VMware" per i limiti del datastore per host vSphere.

> Il datastore vVol non supporta la funzionalità nConnect. Tuttavia, gli endpoint del protocollo vengono conteggiati nel limite di connessione. Quando viene creato il datastore vVol, viene creato un endpoint del protocollo per ogni data life di SVM.

Configurare i datastore NFS per vSphere 8 utilizzando gli ONTAP tools for VMware vSphere

Distribuisci gli ONTAP tools for VMware vSphere 10 per configurare i datastore NFS in un ambiente vSphere 8. Questa procedura include la creazione di SVM e LIF per il traffico NFS, la configurazione della rete host ESXi e la registrazione degli strumenti ONTAP con il cluster vSphere.

Gli ONTAP tools for VMware vSphere 10 sono dotati di un'architettura di nuova generazione che consente elevata disponibilità e scalabilità native per il provider VASA (supportando iSCSI e NFS vVols). Ciò semplifica la gestione di più server VMware vCenter e cluster ONTAP .

In questo scenario mostreremo come distribuire e utilizzare gli ONTAP tools for VMware vSphere 10 e configurare un datastore NFS per vSphere 8.

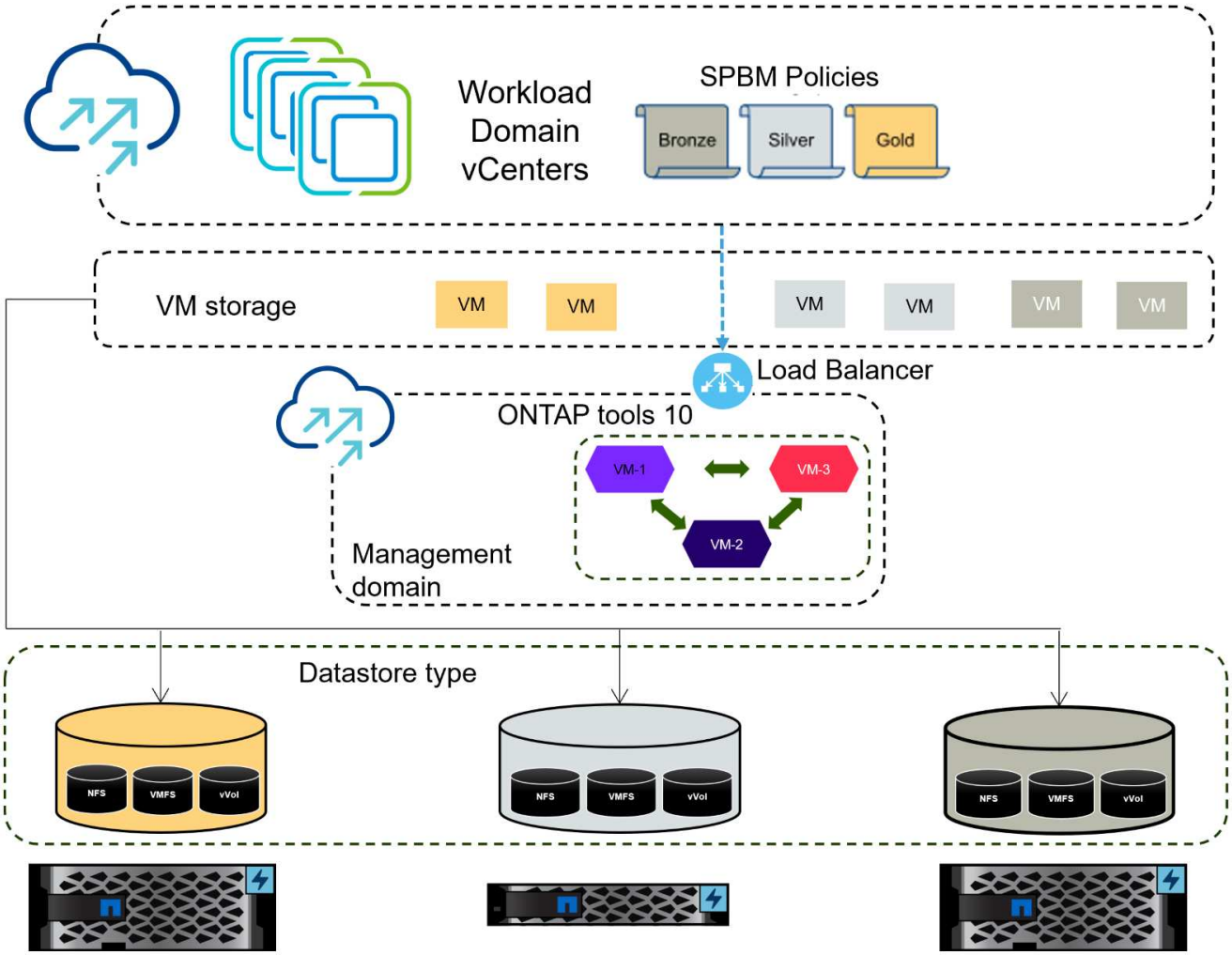
Panoramica della soluzione

Questo scenario comprende i seguenti passaggi di alto livello:

- Creare una macchina virtuale di archiviazione (SVM) con interfacce logiche (LIF) per il traffico NFS.
- Creare un gruppo di porte distribuito per la rete NFS sul cluster vSphere 8.
- Creare un adattatore vmkernel per NFS sugli host ESXi nel cluster vSphere 8.
- Distribuire gli strumenti ONTAP 10 e registrarsi nel cluster vSphere 8.
- Creare un nuovo datastore NFS sul cluster vSphere 8.

Architettura

Il diagramma seguente mostra i componenti architettonici di un'implementazione ONTAP tools for VMware vSphere 10.



Prerequisiti

Questa soluzione richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF con porte dati fisiche su switch Ethernet dedicate al traffico di archiviazione.
- La distribuzione del cluster vSphere 8 è completa e il client vSphere è accessibile.
- Il modello OVA ONTAP tools for VMware vSphere 10 è stato scaricato dal sito di supporto NetApp .

NetApp consiglia una progettazione di rete ridondante per NFS, che garantisca tolleranza agli errori per sistemi di storage, switch, adattatori di rete e sistemi host. È comune distribuire NFS con una singola subnet o più subnet a seconda dei requisiti architettonici.

Fare riferimento a "Procedure consigliate per l'esecuzione di NFS con VMware vSphere" per informazioni dettagliate specifiche su VMware vSphere.

Per indicazioni di rete sull'utilizzo di ONTAP con VMware vSphere, fare riferimento a "Configurazione di rete - NFS" sezione della documentazione delle applicazioni aziendali NetApp .

Strumenti ONTAP completi 10 risorse possono essere trovate "ONTAP tools for VMware vSphere Risorse di documentazione" .

Fasi di distribuzione

Per distribuire gli strumenti ONTAP 10 e utilizzarli per creare un datastore NFS sul dominio di gestione VCF, completare i seguenti passaggi:

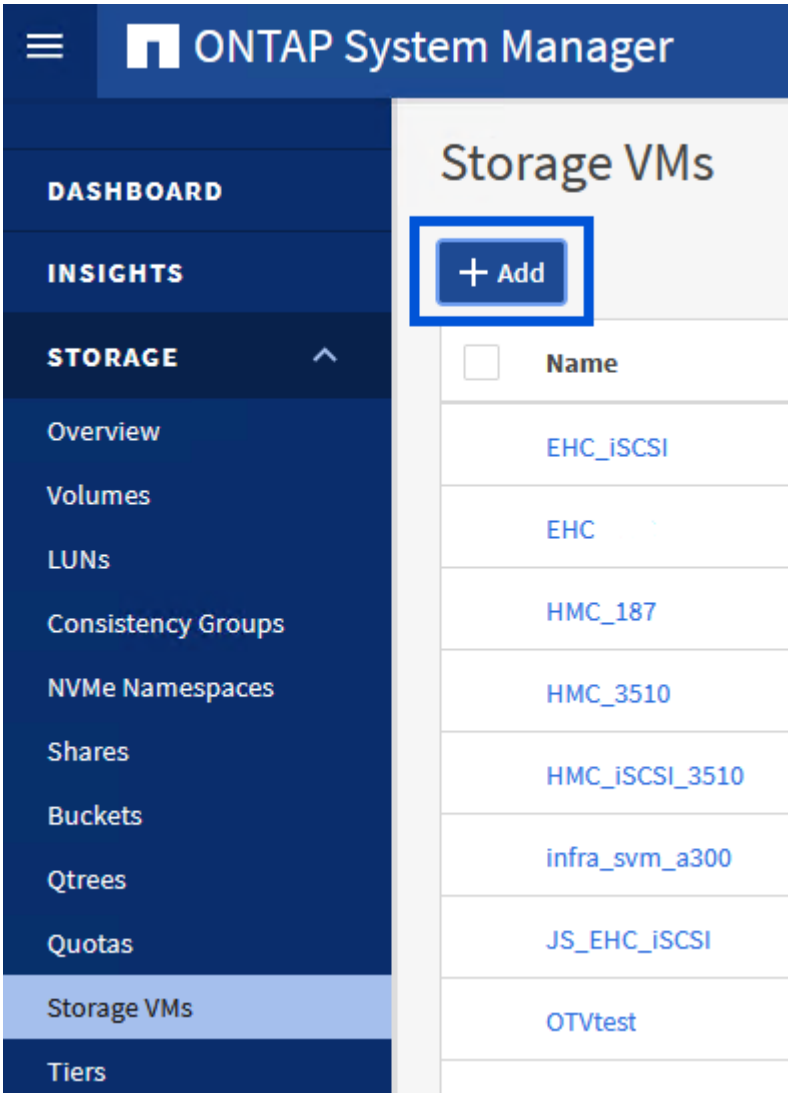
Creare SVM e LIF sul sistema di archiviazione ONTAP

Il passaggio seguente viene eseguito in ONTAP System Manager.

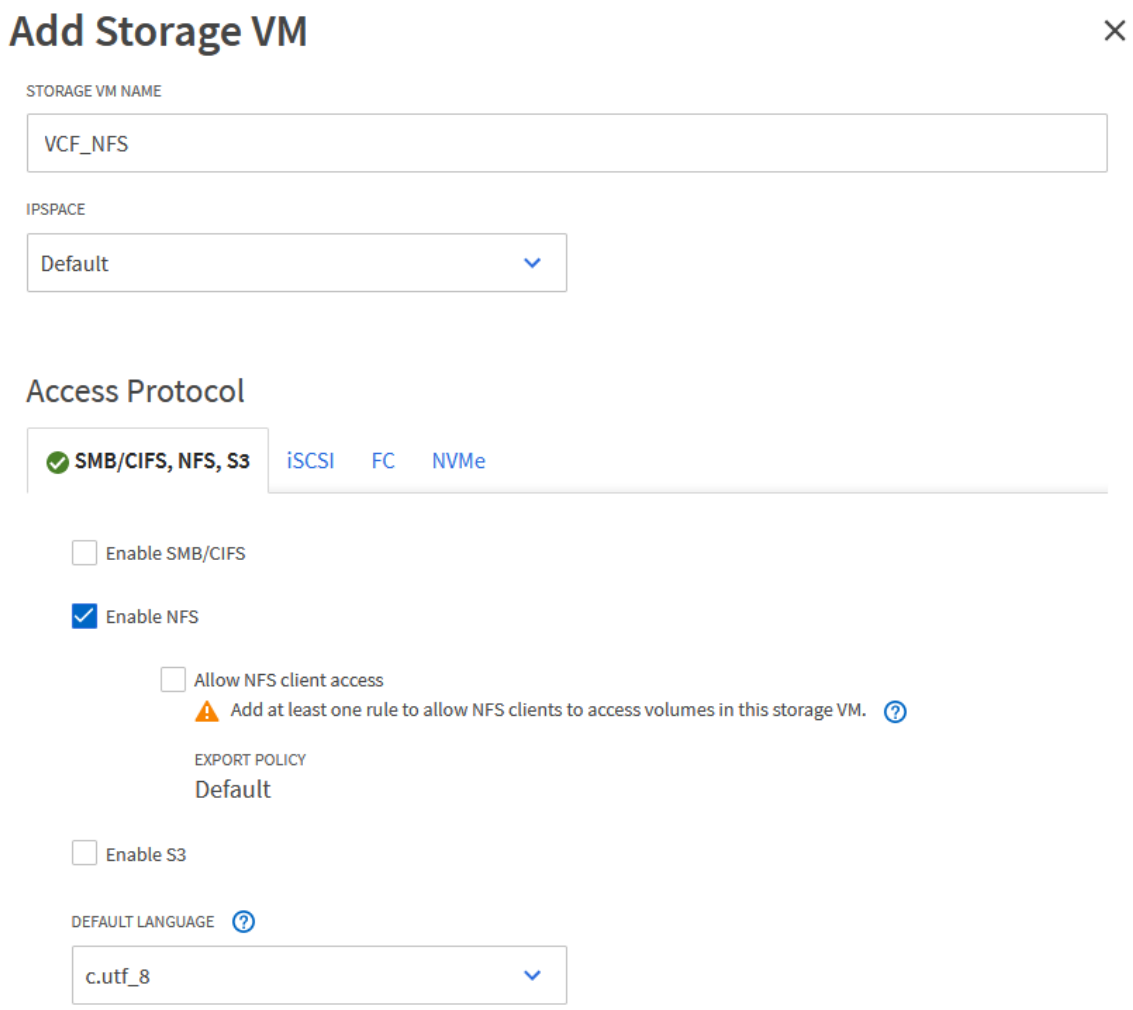
Creare la VM di archiviazione e i LIF

Completare i seguenti passaggi per creare una SVM insieme a più LIF per il traffico NFS.

1. Da ONTAP System Manager, vai su **VM di archiviazione** nel menu a sinistra e clicca su **+ Aggiungi** per iniziare.

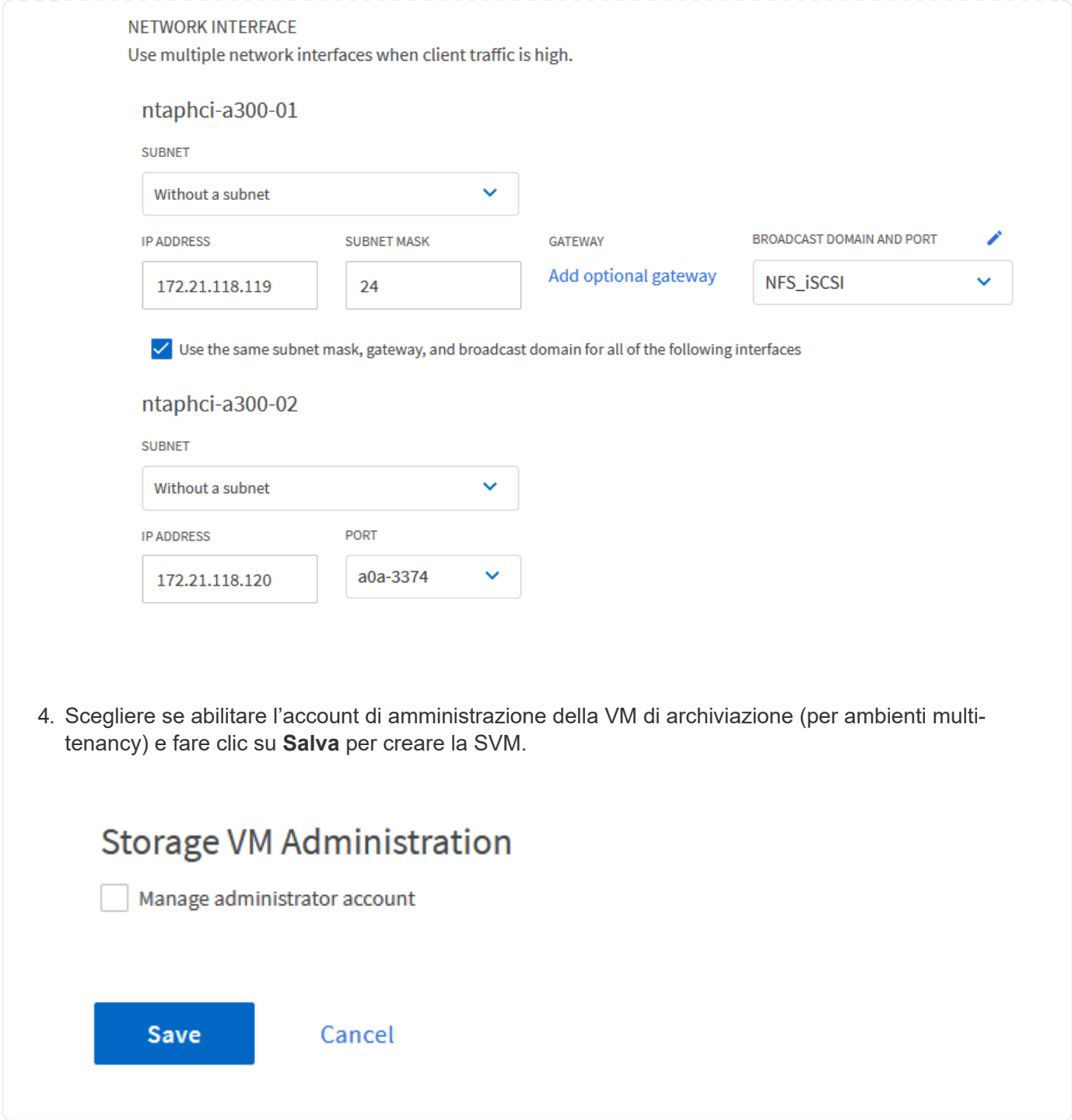


2. Nella procedura guidata **Aggiungi VM di archiviazione**, fornire un **Nome** per la SVM, selezionare lo **Spazio IP** e quindi, in **Protocollo di accesso**, fare clic sulla scheda **SMB/CIFS, NFS, S3** e selezionare la casella per **Abilitare NFS**.



Non è necessario selezionare il pulsante **Consenti accesso client NFS** in quanto verranno utilizzati gli strumenti Ontap per VMware vSphere per automatizzare il processo di distribuzione del datastore. Ciò include la fornitura di accesso client per gli host ESXi.

3. Nella sezione **Interfaccia di rete** compilare **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, la casella di controllo può essere abilitata per utilizzare impostazioni comuni a tutti i LIF rimanenti oppure per utilizzare impostazioni separate.



4. Scegliere se abilitare l'account di amministrazione della VM di archiviazione (per ambienti multi-tenancy) e fare clic su **Salva** per creare la SVM.

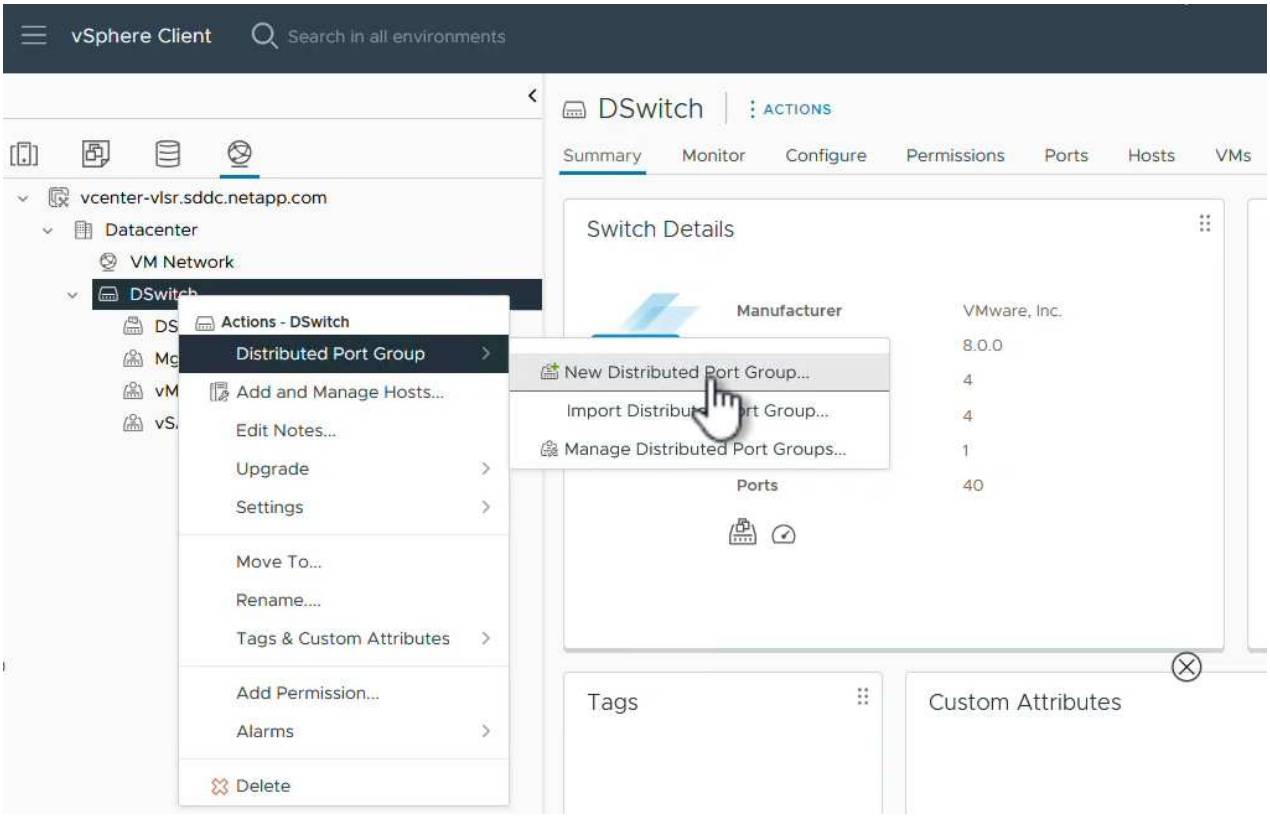
Configurare la rete per NFS sugli host ESXi

I passaggi seguenti vengono eseguiti sul cluster VI Workload Domain utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-On in modo che il client vSphere sia comune tra i domini di gestione e di carico di lavoro.

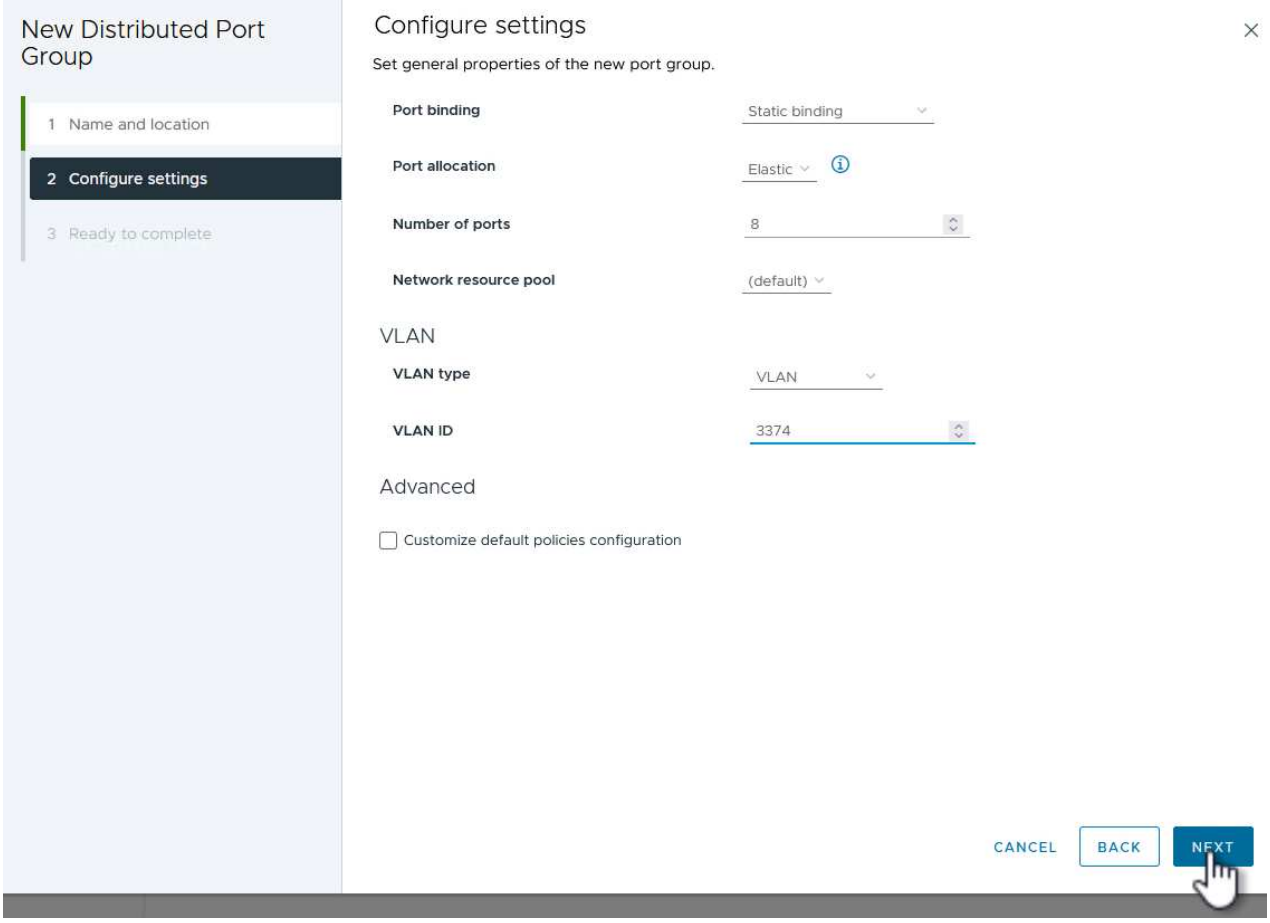
Creare un gruppo di porte distribuito per il traffico NFS

Completare quanto segue per creare un nuovo gruppo di porte distribuito affinché la rete trasporti il traffico NFS:

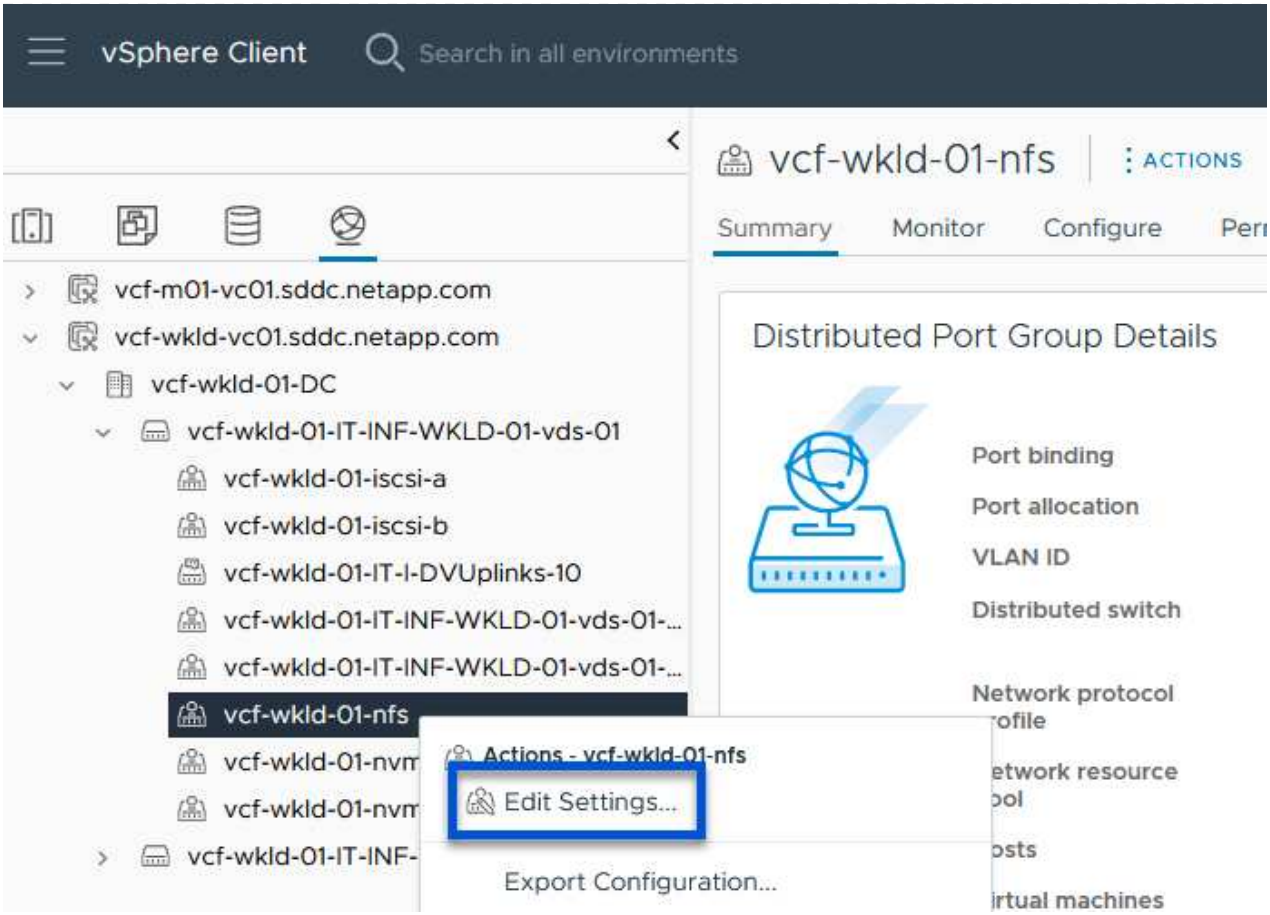
1. Dal client vSphere, accedere a **Inventario > Rete** per il dominio del carico di lavoro. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite…**.



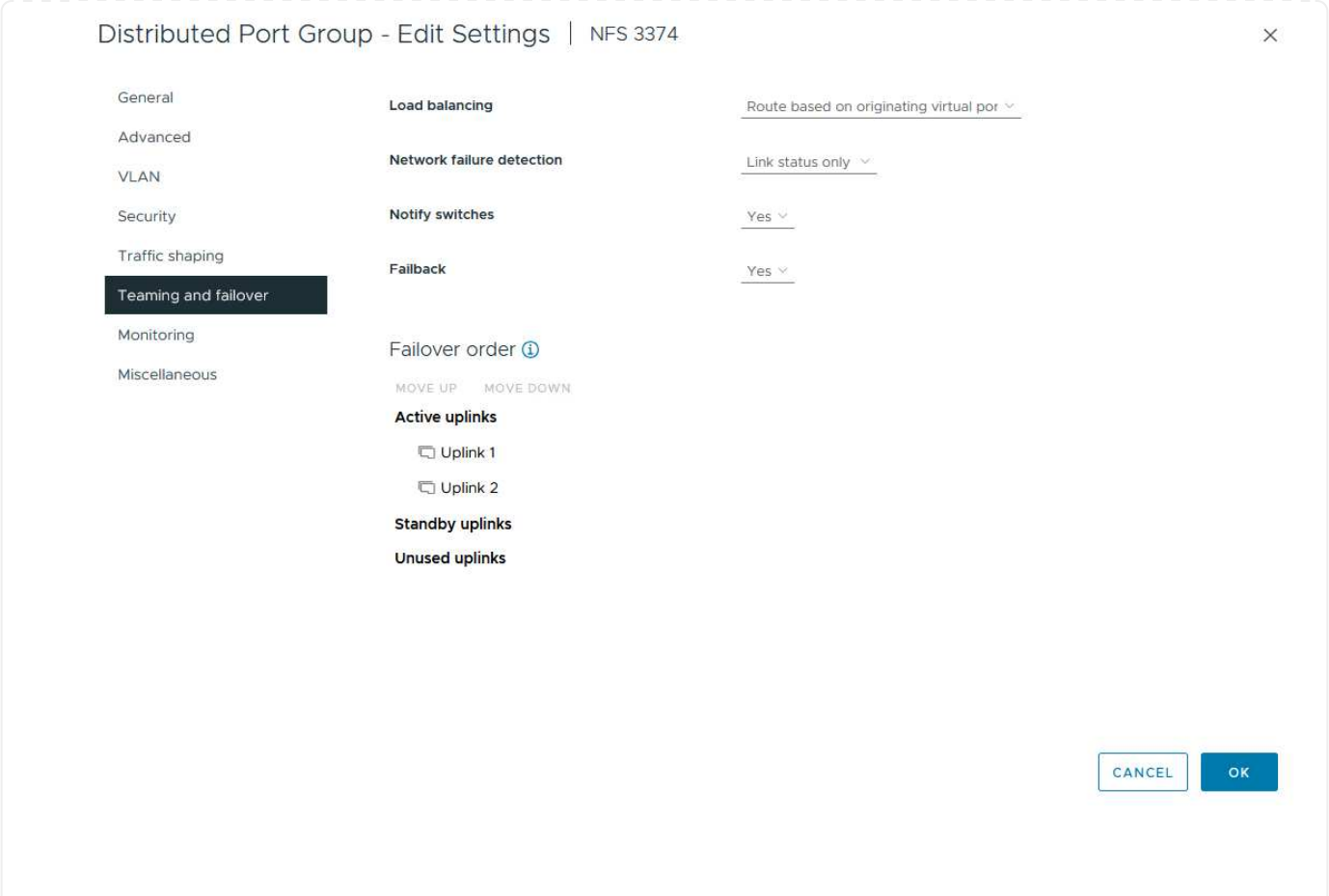
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, immettere un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare 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, accedi al gruppo di porte e seleziona l'azione **Modifica impostazioni…**.



6. Nella pagina **Gruppo di porte distribuite - Modifica impostazioni**, vai a **Teaming e failover** nel menu a sinistra. Abilitare il teaming per gli Uplink da utilizzare per il traffico NFS assicurandosi che siano tutti insieme nell'area **Uplink attivi**. Spostare tutti gli uplink non utilizzati in **Uplink non utilizzati**.

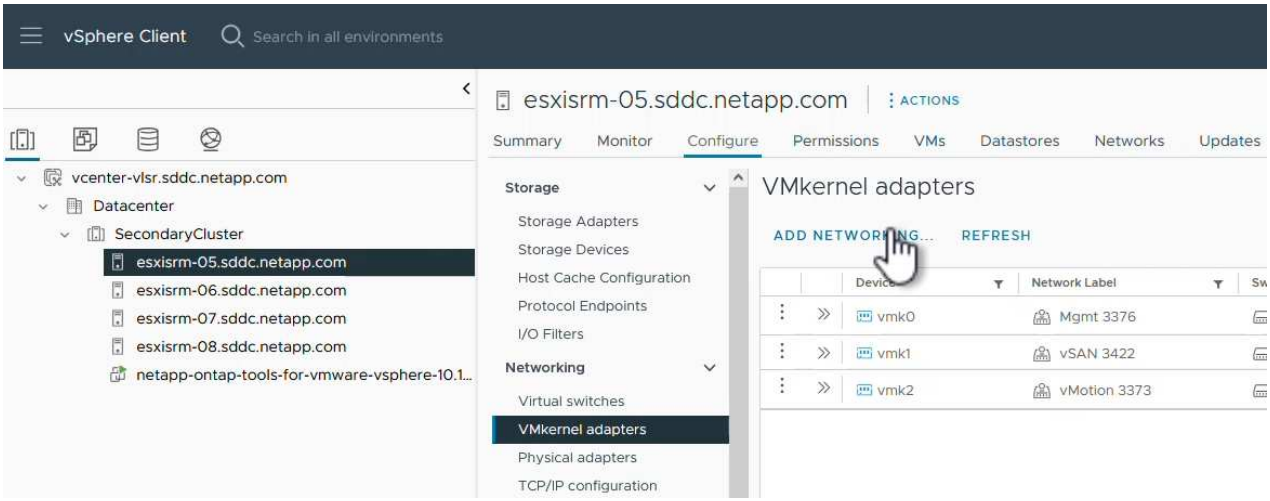


7. Ripetere questo processo per ogni host ESXi nel cluster.

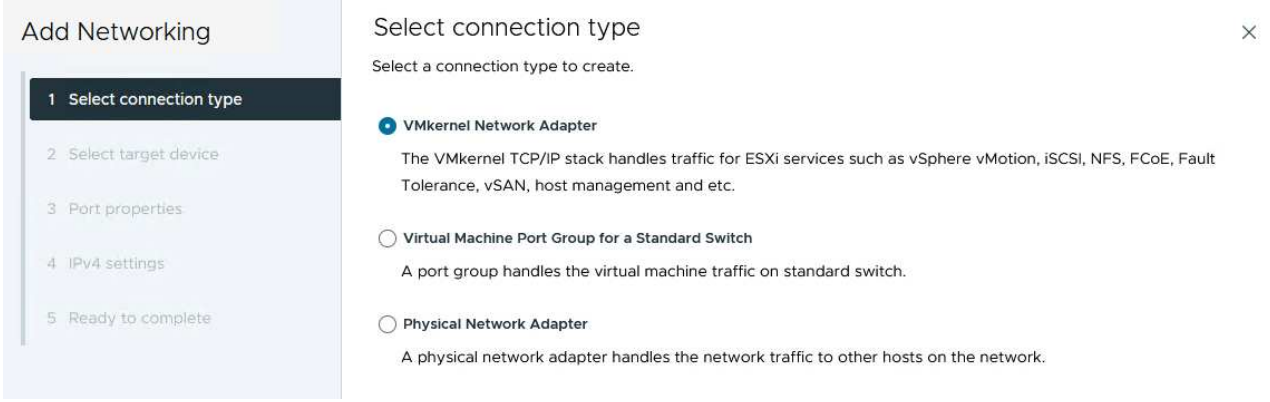
Creare un adattatore VMkernel su ciascun host ESXi

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

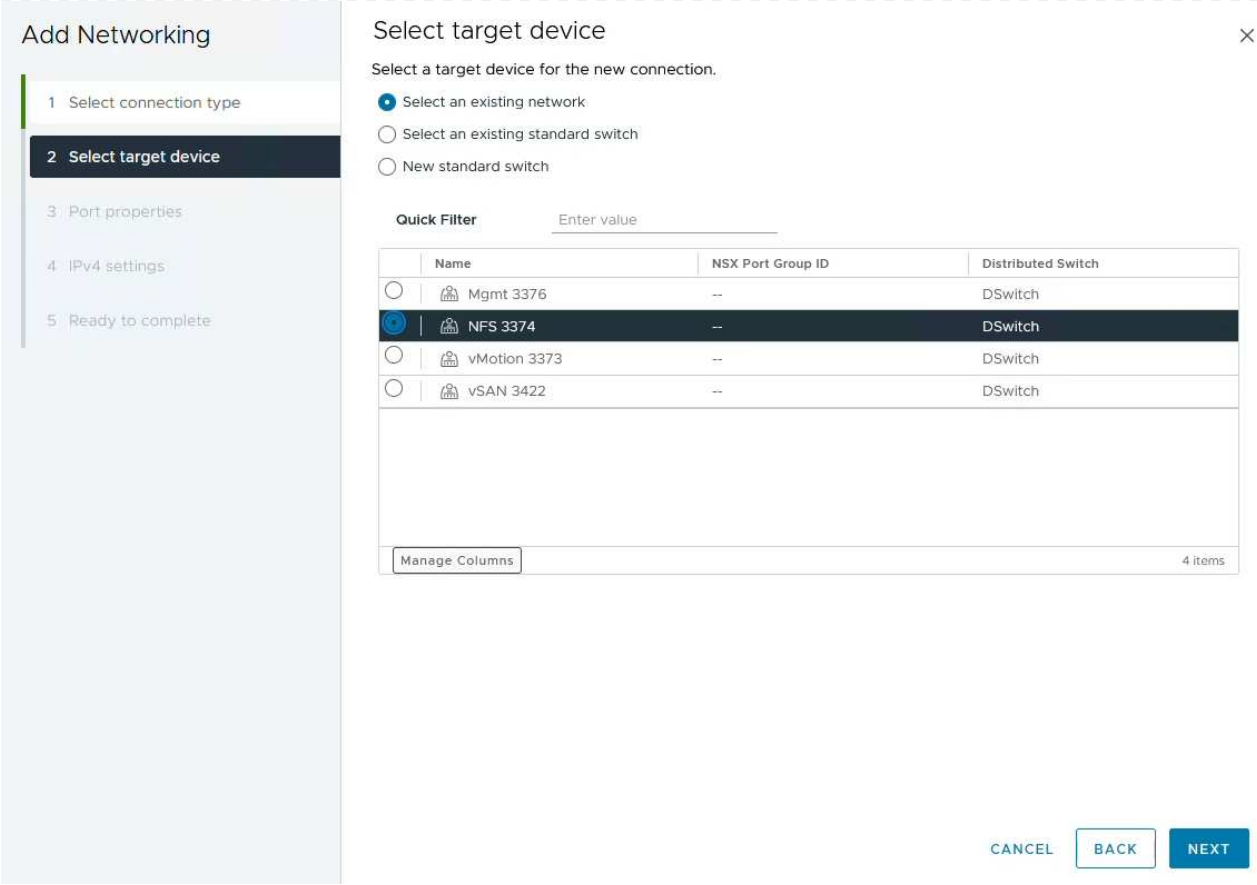
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configura** seleziona **Schede VMkernel** e clicca su **Aggiungi rete…** per iniziare.



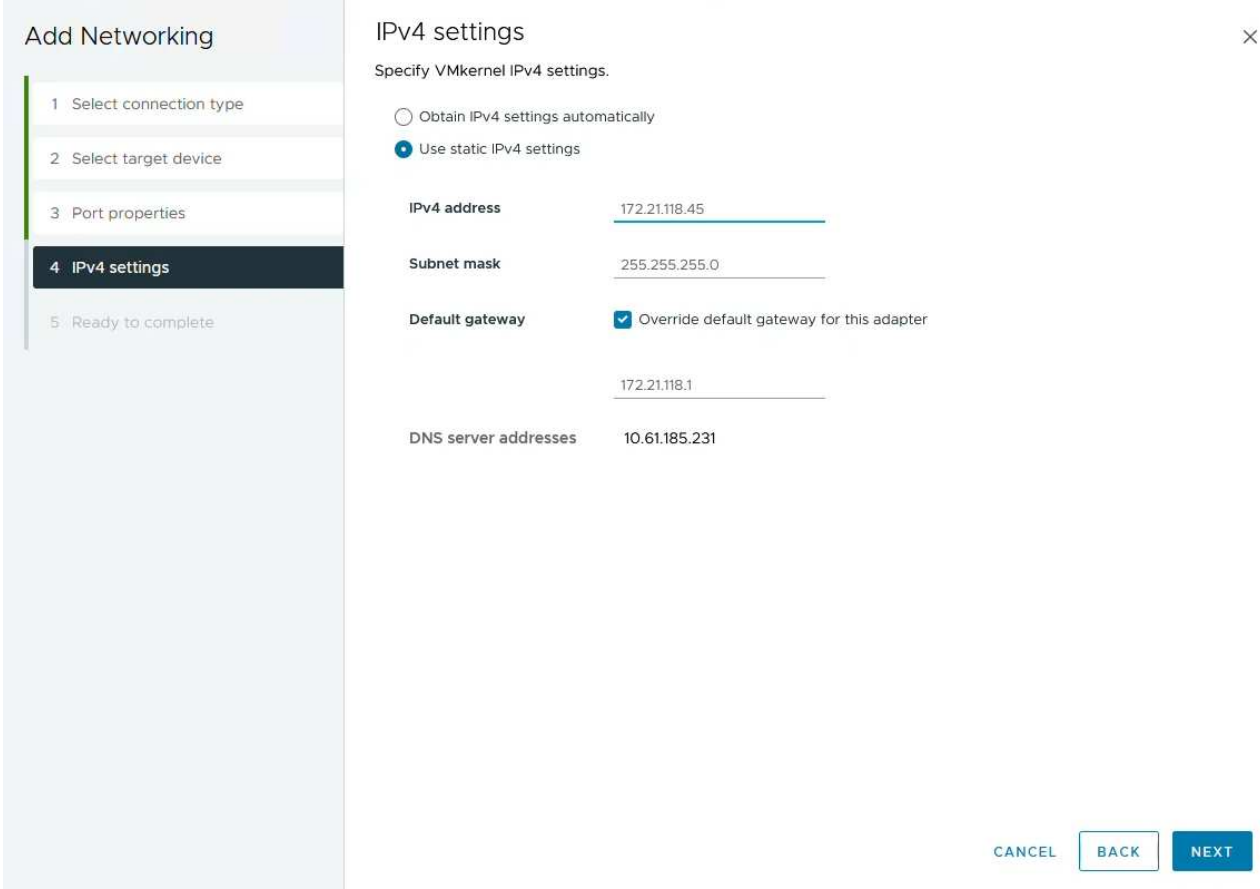
2. Nella finestra **Seleziona tipo di connessione** seleziona **Scheda di rete VMkernel** e fai clic su **Avanti** per continuare.



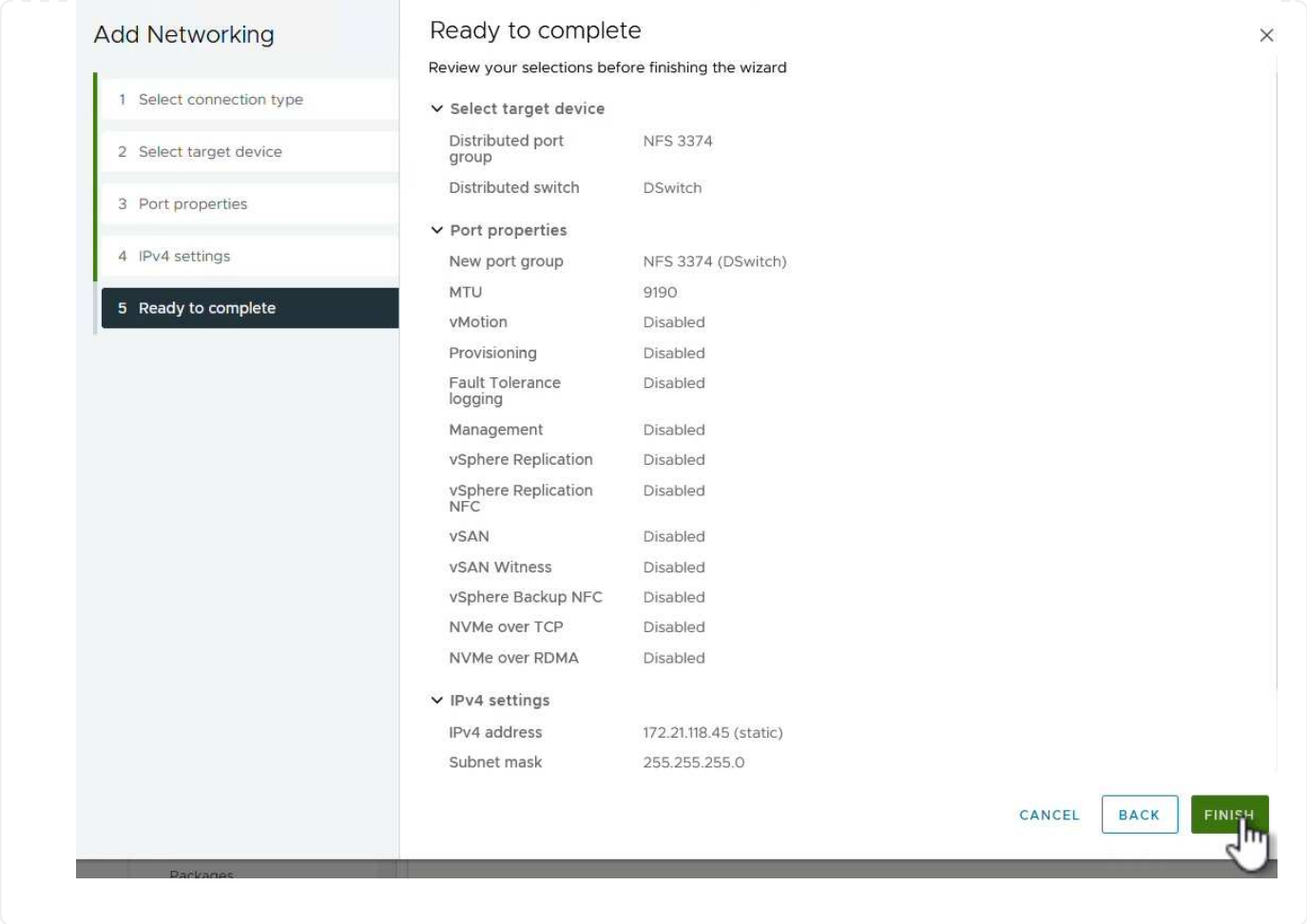
3. Nella pagina **Seleziona dispositivo di destinazione**, seleziona uno dei gruppi di porte distribuiti per NFS creati in precedenza.



4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite (nessun servizio abilitato) e fare clic su **Avanti** per continuare.
5. Nella pagina **Impostazioni IPv4** compilare **Indirizzo IP**, **Maschera di sottorete** e fornire un nuovo indirizzo IP del gateway (solo se richiesto). Fare clic su **Avanti** per continuare.



6. Rivedi le tue selezioni nella pagina **Pronto per il completamento** e fai clic su **Fine** per creare l'adattatore VMkernel.



Distribuire e utilizzare gli strumenti ONTAP 10 per configurare l'archiviazione

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

Per la documentazione completa sulla distribuzione e l'utilizzo ONTAP tools for VMware vSphere 10, fare riferimento a "Distribuisci gli ONTAP tools for VMware vSphere" .

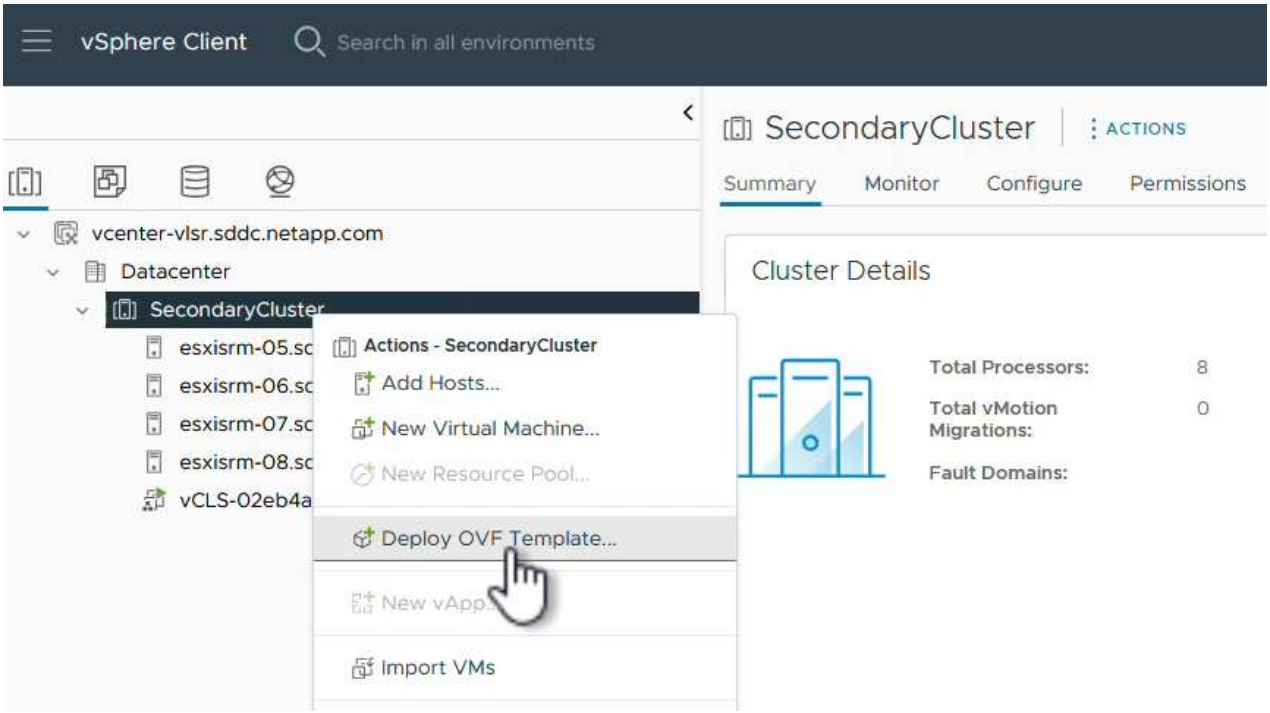
Distribuisci gli ONTAP tools for VMware vSphere 10

Gli ONTAP tools for VMware vSphere 10 vengono distribuiti come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP . ONTAP Tools 10 è dotato di un nuovo portale di gestione globale per la gestione delle connessioni a più server vCenter e backend di archiviazione ONTAP .

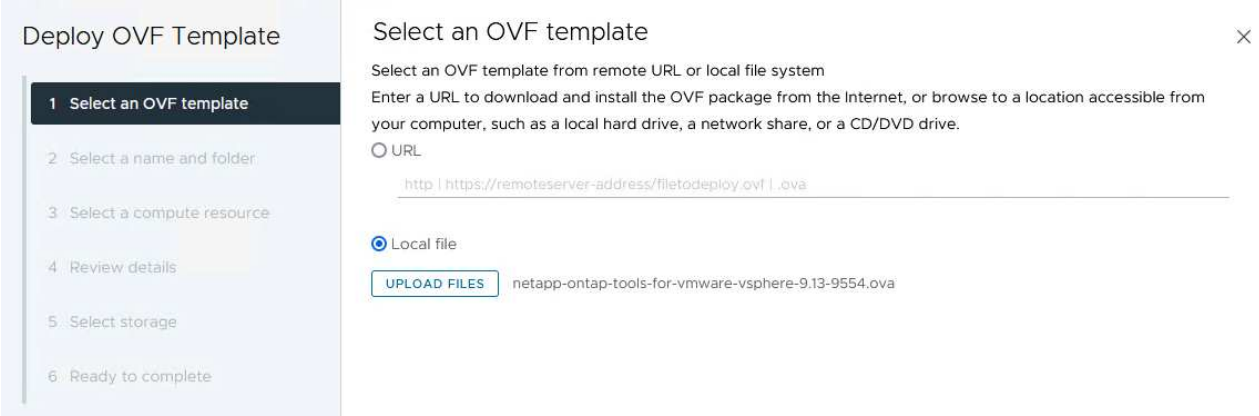
> In uno scenario di distribuzione non HA, sono richiesti tre indirizzi IP disponibili. Un indirizzo IP viene assegnato al bilanciatore del carico, un altro al piano di controllo Kubernetes e l'ultimo al nodo. In una distribuzione HA, sono necessari due indirizzi IP aggiuntivi per il secondo e il terzo 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 siano sulla stessa VLAN scelta per la distribuzione.

Completare quanto segue per distribuire gli ONTAP tools for VMware vSphere:

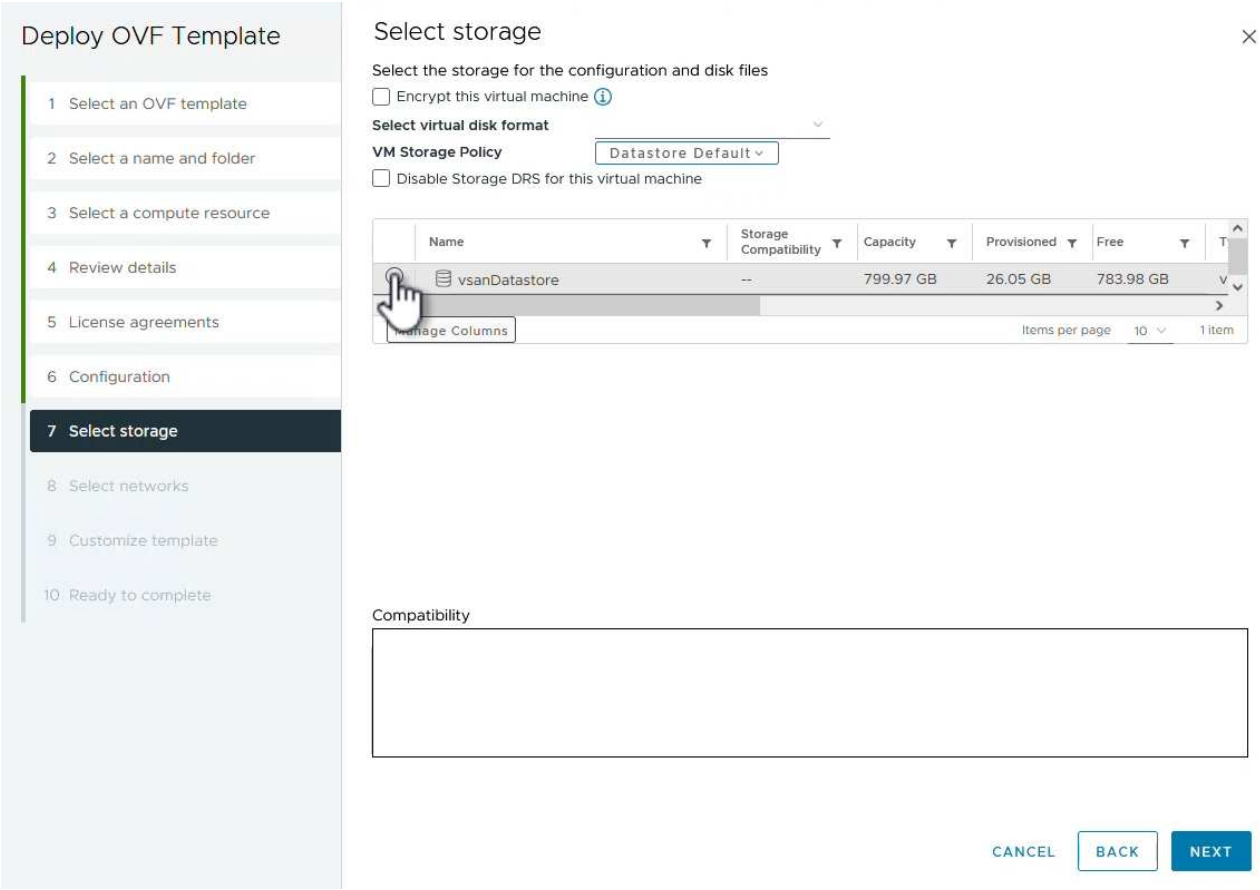
1. Ottieni l'immagine OVA degli strumenti ONTAP da"Sito di supporto NetApp" e scaricarlo in una cartella locale.
2. Accedere all'appliance vCenter per il cluster vSphere 8.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Distribuisci modello OVF…**



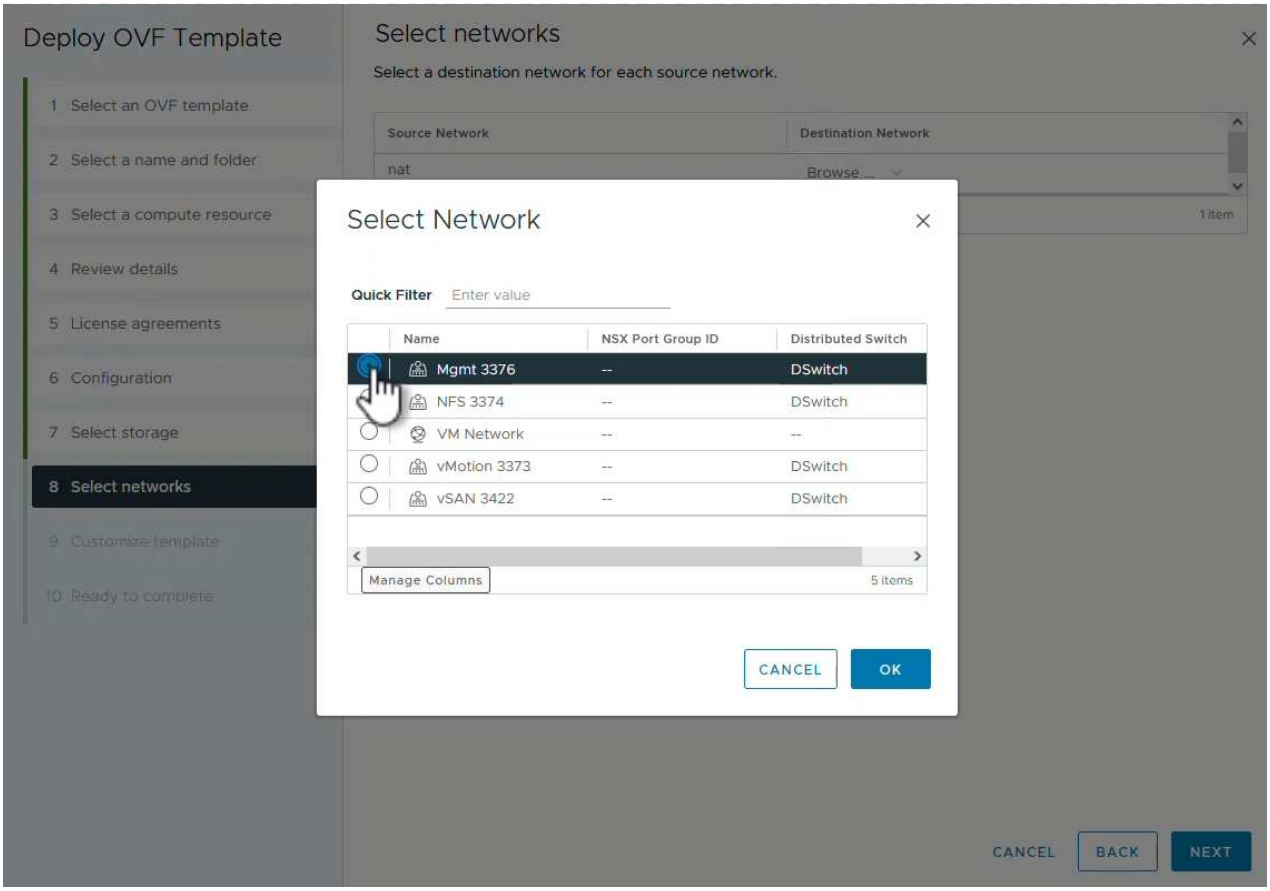
4. Nella procedura guidata **Distribuisci modello OVF**, fare clic sul pulsante di opzione **File locale** e selezionare il file OVA degli strumenti ONTAP scaricato nel passaggio precedente.



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

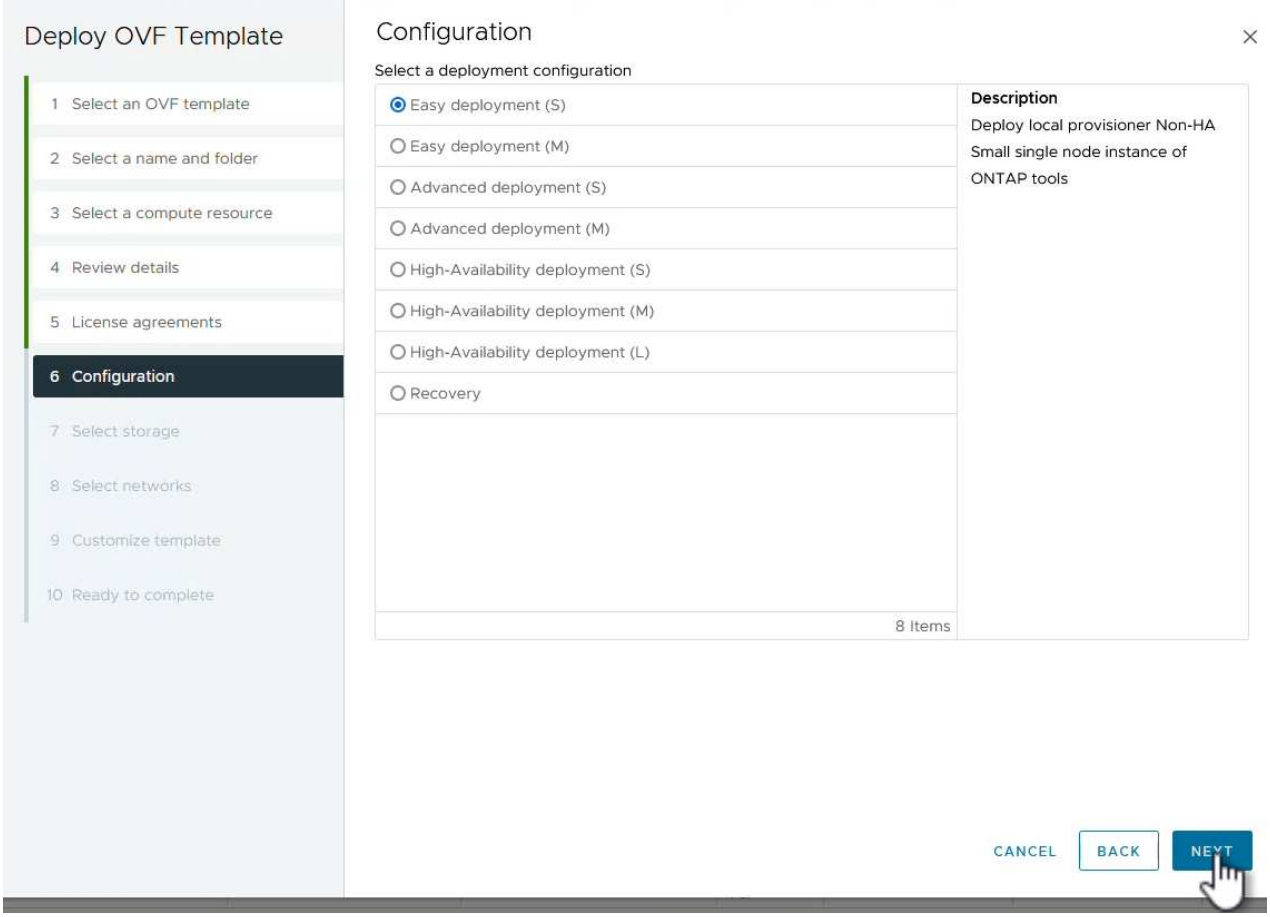


7. Nella pagina Seleziona rete seleziona la rete utilizzata per la gestione del traffico.



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

> ONTAP Tools 10 offre molteplici configurazioni di distribuzione, tra cui distribuzioni ad alta disponibilità che utilizzano più nodi. Per la documentazione su tutte le configurazioni di distribuzione e i prerequisiti, fare riferimento a "Prerequisiti per la distribuzione ONTAP tools for VMware vSphere" .



9. Nella pagina Personalizza modello compila tutte le informazioni richieste:
   - Nome utente dell'applicazione da utilizzare per registrare il provider VASA e SRA nel 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 del carico.
   - IP virtuale per il piano di controllo K8s.
   - VM primaria per selezionare la VM corrente come primaria (per configurazioni HA).
   - Nome host per la VM
   - Fornire 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

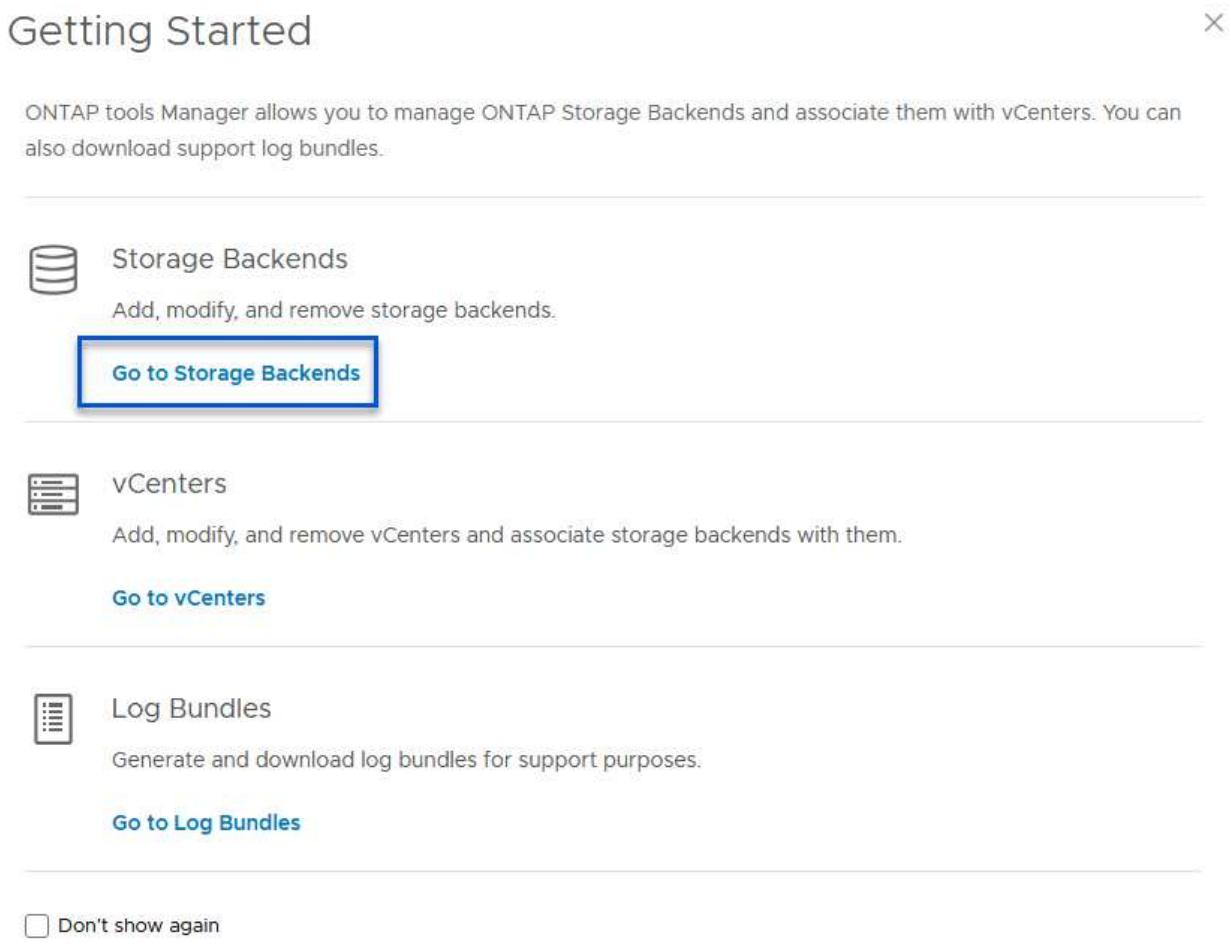
10. Rivedere tutte le informazioni nella pagina Pronto per il completamento e fare clic su Fine per iniziare a distribuire l’appliance degli strumenti ONTAP .

Collegare Storage Backend e vCenter Server agli strumenti ONTAP 10.

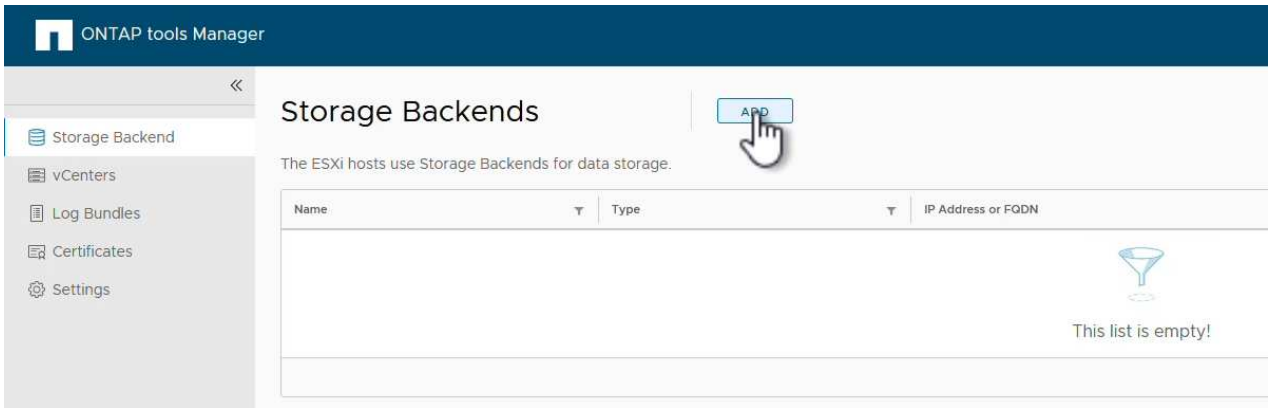
Il gestore degli strumenti ONTAP viene utilizzato per configurare le impostazioni globali per ONTAP Tools 10.

1. Accedi a ONTAP Tools Manager navigando su `https://<loadBalanceIP>:8443/virtualization/ui/` in un browser web ed effettuando l'accesso con le credenziali amministrative fornite durante la distribuzione.

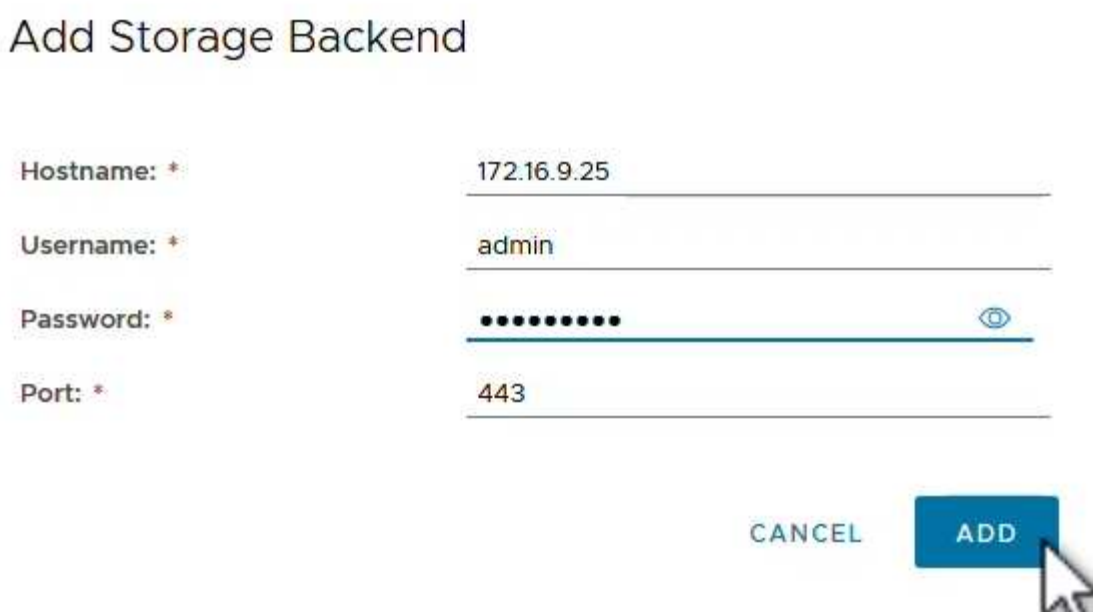
2. Nella pagina **Introduzione** fare clic su **Vai a Backend di archiviazione**.



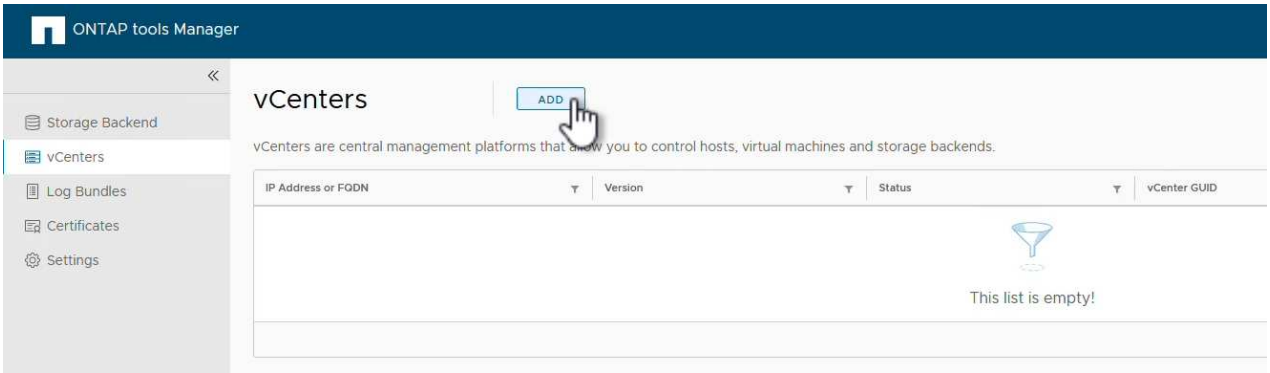
3. Nella pagina **Backend di archiviazione**, fare clic su **AGGIUNGI** per inserire le credenziali di un sistema di archiviazione ONTAP da registrare con gli strumenti ONTAP 10.



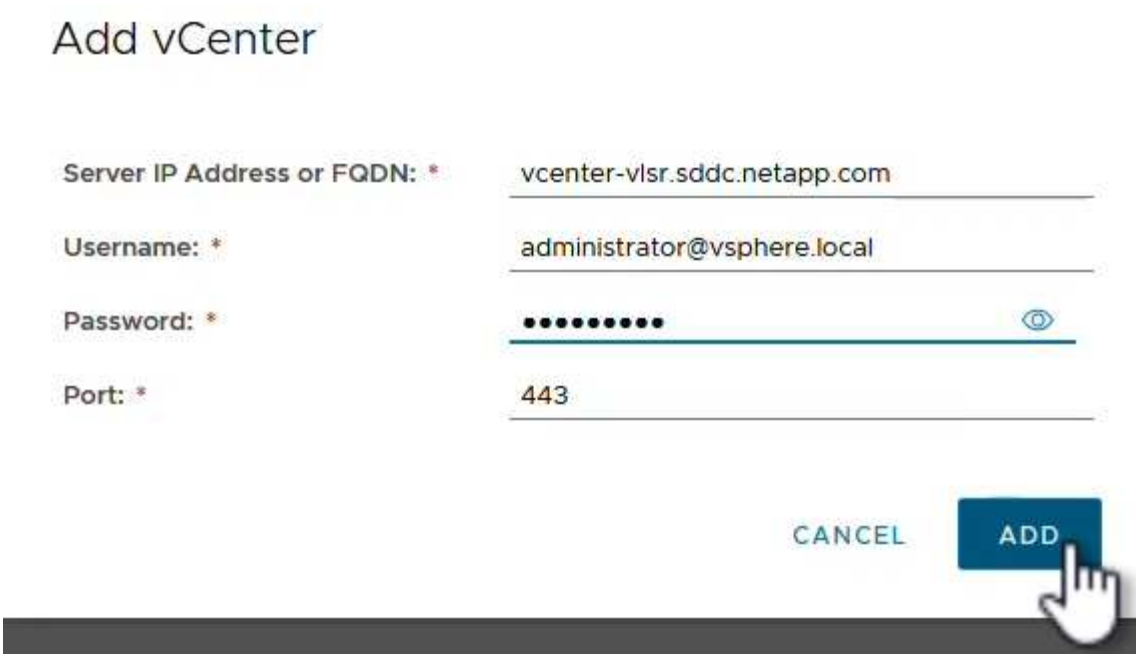
4. Nella casella **Aggiungi backend di archiviazione**, compilare le credenziali per il sistema di archiviazione ONTAP .



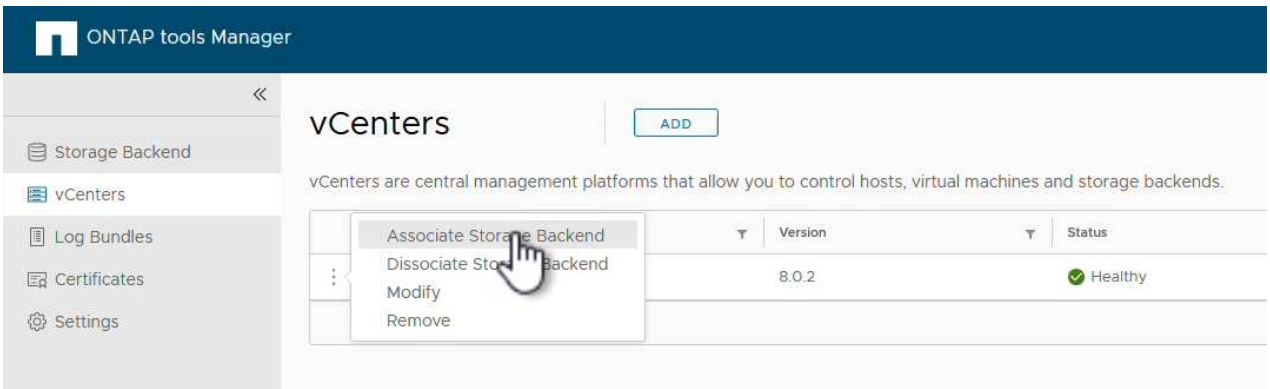
5. Nel menu a sinistra fare clic su **vCenter**, quindi su **AGGIUNGI** per inserire le credenziali di un server vCenter da registrare con gli strumenti ONTAP 10.



6. Nella casella **Aggiungi vCenter**, compilare le credenziali per il sistema di archiviazione ONTAP .

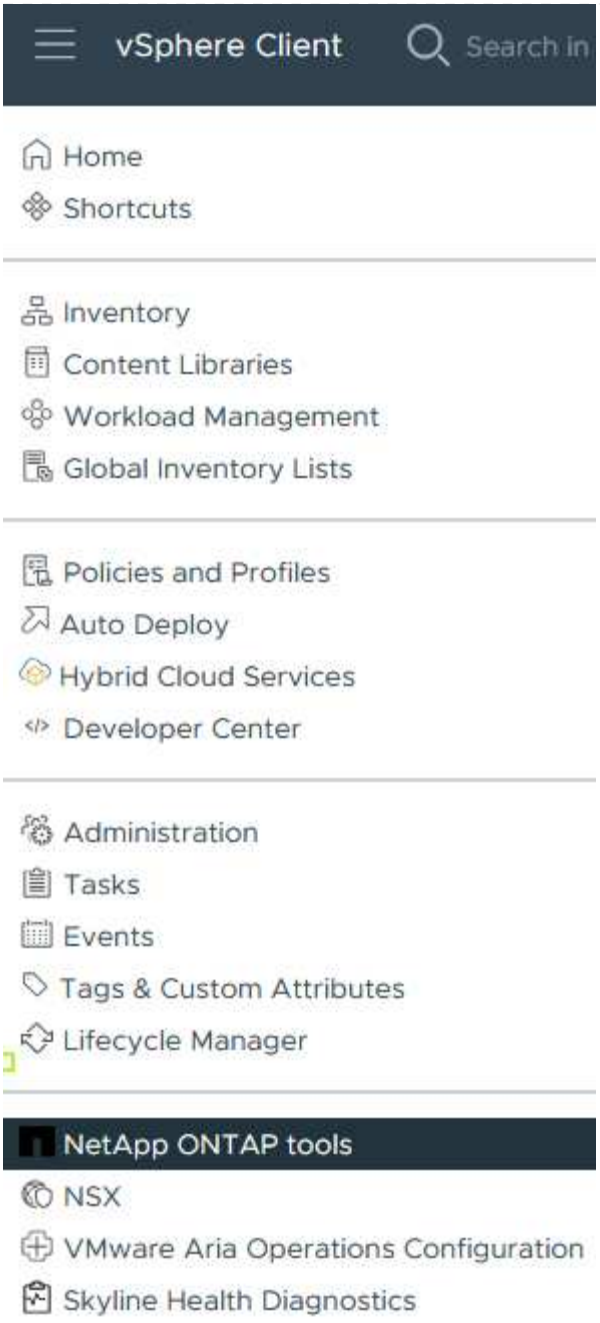


7. Dal menu verticale a tre punti per il server vCenter appena rilevato, selezionare **Associa backend di archiviazione**.

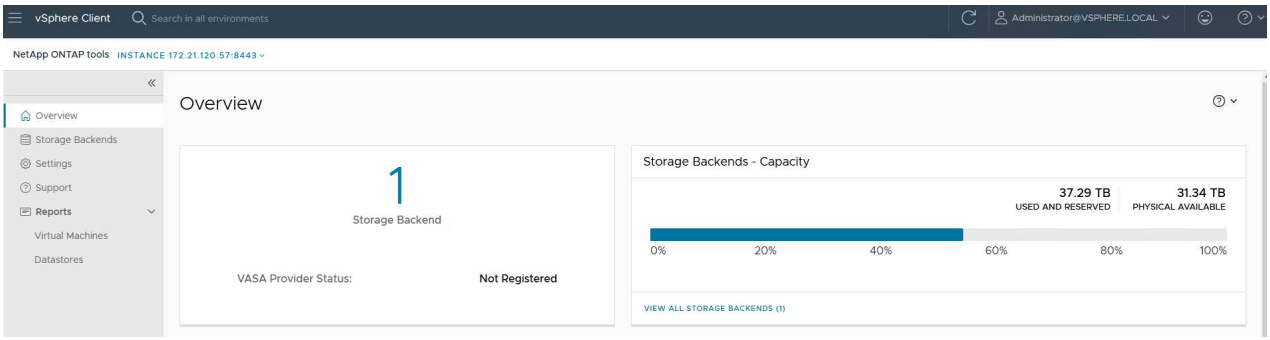


8. Nella casella **Associa backend di archiviazione**, selezionare il sistema di archiviazione ONTAP da associare al server vCenter e fare clic su **Associa** per completare l'azione.

9. Per verificare l'installazione, accedi al client vSphere e seleziona *Strumenti NetApp ONTAP * dal menu a sinistra.



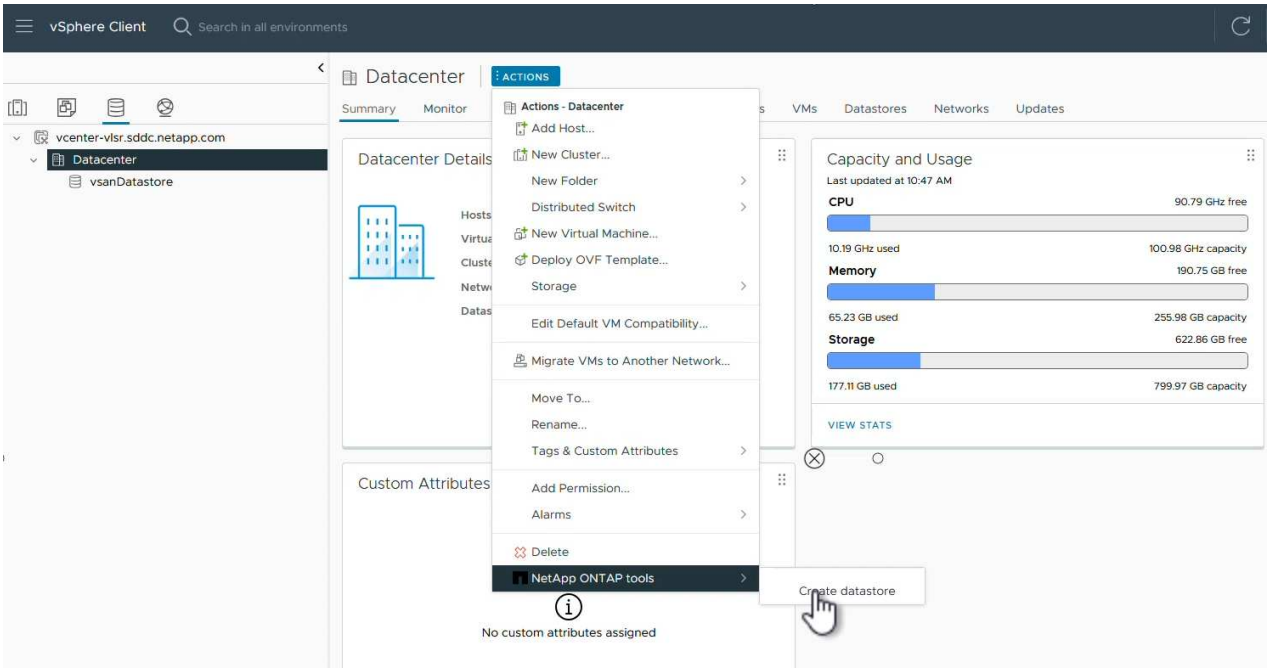
10. Dalla dashboard degli strumenti ONTAP dovresti vedere che uno Storage Backend è stato associato al vCenter Server.



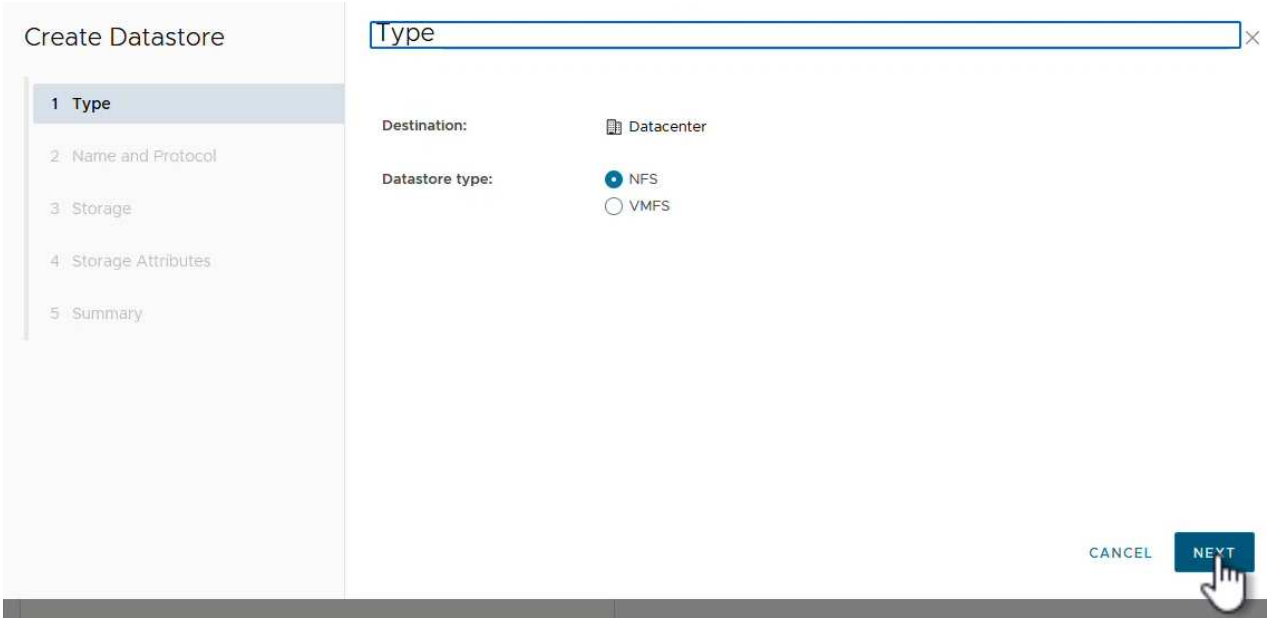
Creare un datastore NFS utilizzando gli strumenti ONTAP 10

Completare i seguenti passaggi per distribuire un datastore ONTAP , in esecuzione su NFS, utilizzando gli strumenti ONTAP 10.

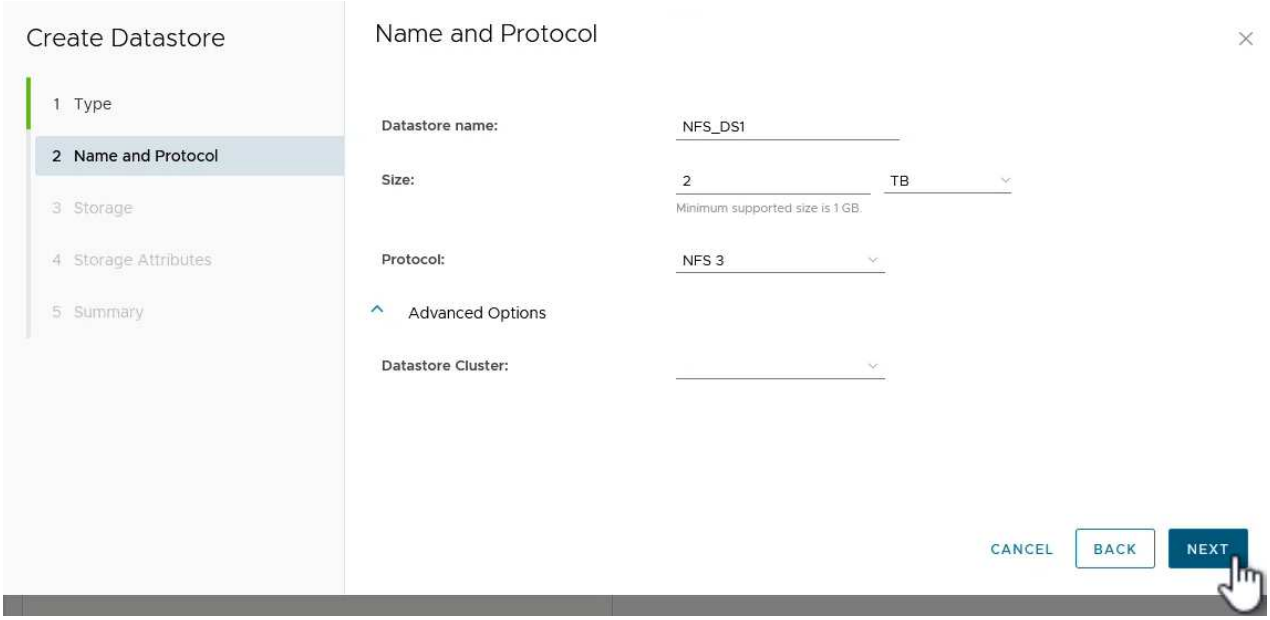
1. Nel client vSphere, accedere all'inventario di archiviazione. Dal menu **AZIONI**, selezionare **Strumenti NetApp ONTAP > Crea datastore**.



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

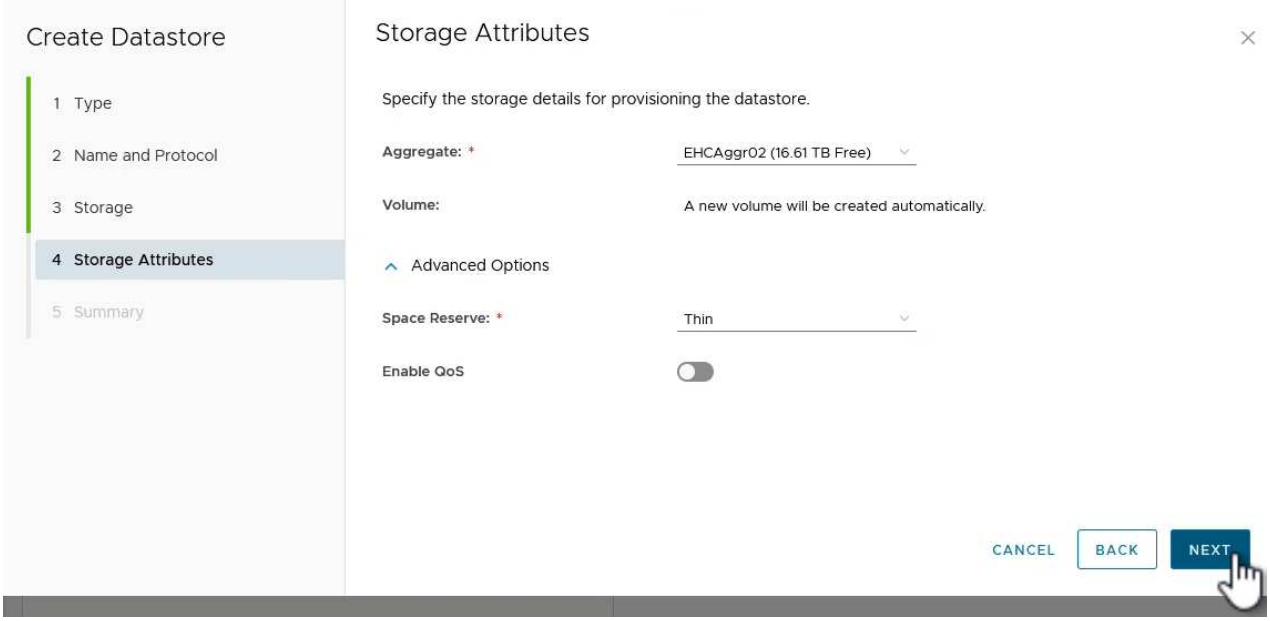


3. Nella pagina **Nome e protocollo**, compilare il nome, la dimensione e il protocollo per il datastore. Fare clic su **Avanti** per continuare.

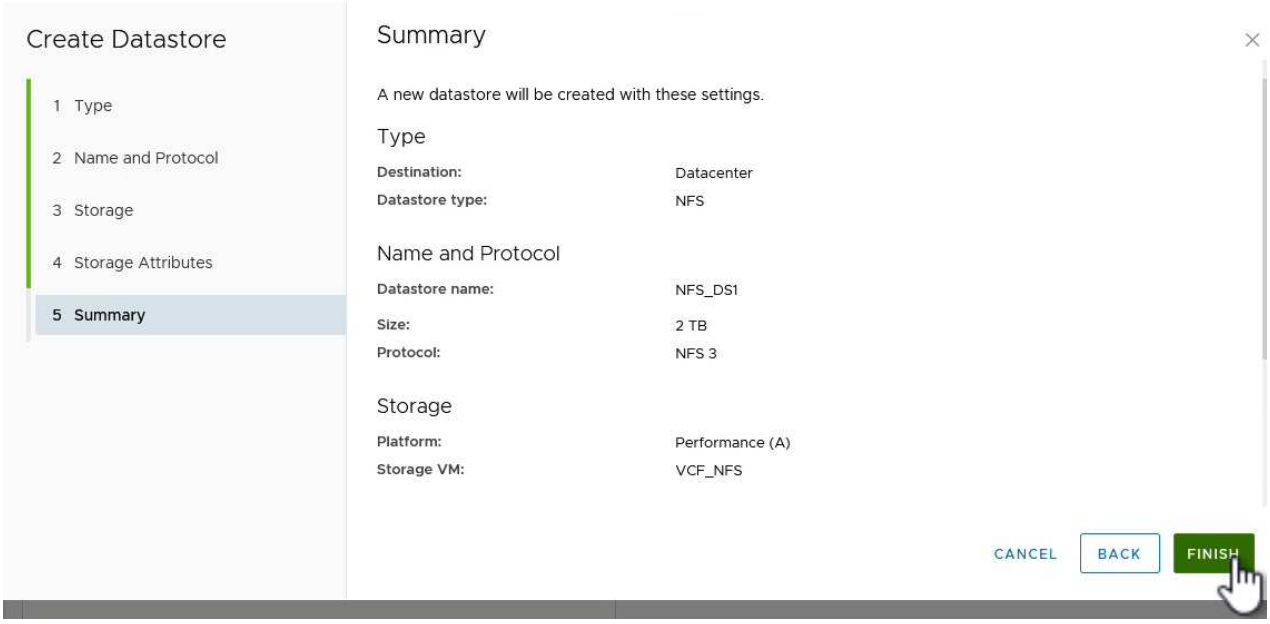


4. Nella pagina **Archiviazione** seleziona una piattaforma (filtra il sistema di archiviazione in base al tipo) e una VM di archiviazione per il volume. Facoltativamente, seleziona una policy di esportazione personalizzata. Fare clic su **Avanti** per continuare.

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



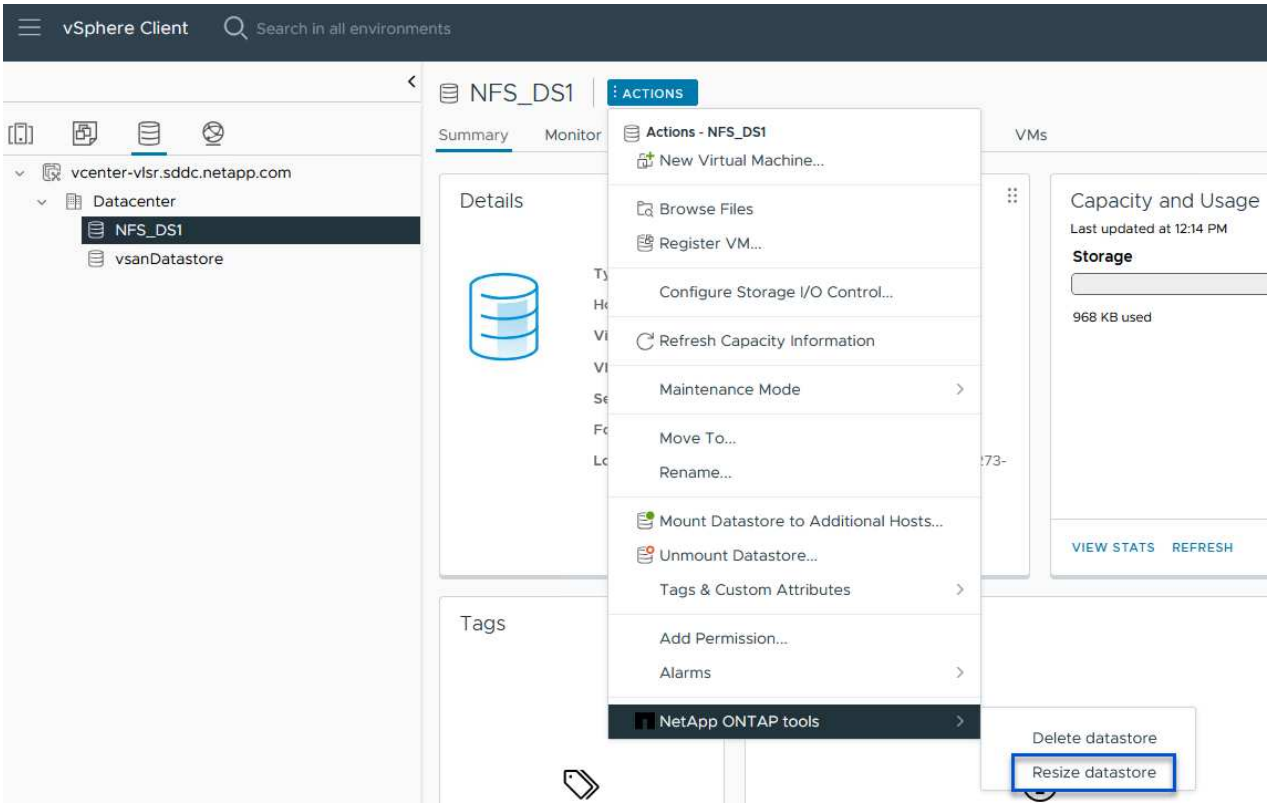
6. Infine, rivedere il **Riepilogo** e fare clic su Fine per iniziare a creare il datastore NFS.



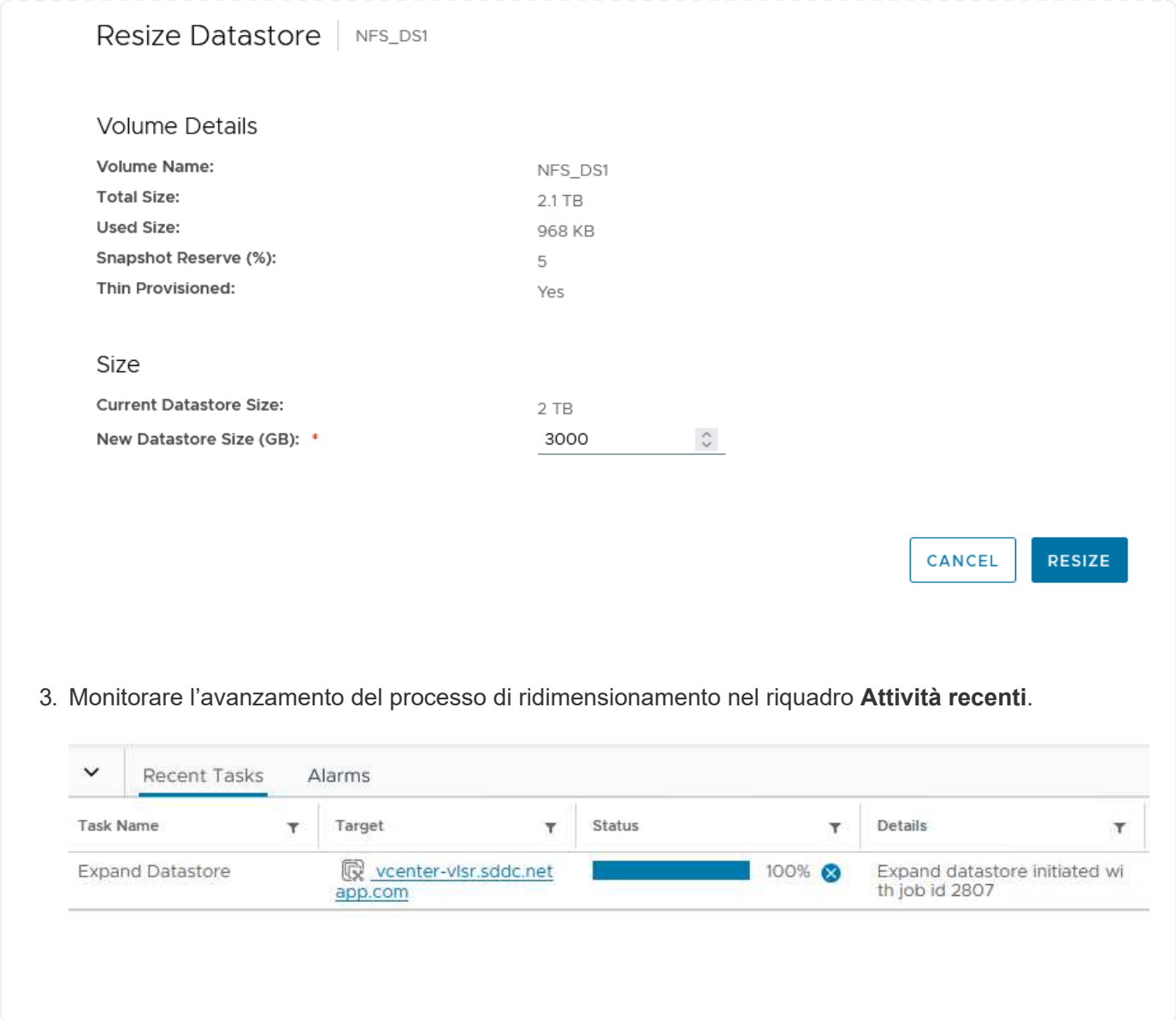
Ridimensionare un datastore NFS utilizzando gli strumenti ONTAP 10

Completare i seguenti passaggi per ridimensionare un datastore NFS esistente utilizzando gli strumenti ONTAP 10.

1. Nel client vSphere, accedere all'inventario di archiviazione. Dal menu **AZIONI**, selezionare **Strumenti NetApp ONTAP > Ridimensiona datastore**.



2. Nella procedura guidata **Ridimensiona datastore**, inserisci la nuova dimensione del datastore in GB e fai clic su **Ridimensiona** per continuare.



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

Informazioni aggiuntive

Per un elenco completo degli ONTAP tools for VMware vSphere 10, fare riferimento a "ONTAP tools for VMware vSphere Risorse di documentazione" .

Per ulteriori informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a"Documentazione ONTAP 10" centro.

Configurare il disaster recovery per i datastore NFS utilizzando VMware Site Recovery Manager

Implementare il disaster recovery per datastore NFS utilizzando VMware Site Recovery Manager (SRM) e gli ONTAP tools for VMware vSphere 10. Questa procedura include la configurazione di SRM con server vCenter nei siti primari e secondari, l'installazione di ONTAP Storage Replication Adapter (SRA), la definizione di relazioni SnapMirror tra sistemi di storage ONTAP e la configurazione del ripristino del sito per SRM.

L’utilizzo degli ONTAP tools for VMware vSphere 10 e Site Replication Adapter (SRA) in combinazione con VMware Site Recovery Manager (SRM) apporta un valore significativo agli sforzi di disaster recovery. Gli strumenti ONTAP 10 forniscono solide capacità di archiviazione, tra cui elevata disponibilità nativa e scalabilità per il provider VASA, supportando iSCSI e NFS vVols. 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 senza interruzioni delle macchine virtuali e dei dati tra i siti, consentendo processi efficienti di disaster recovery. La combinazione degli strumenti ONTAP e SRA consente alle aziende di proteggere i carichi di lavoro critici, ridurre al minimo i tempi di inattività e mantenere la continuità aziendale in caso di eventi imprevisti o disastri.

Gli strumenti ONTAP 10 semplificano la gestione dell’archiviazione e le funzionalità di efficienza, migliorano la disponibilità e riducono i costi di archiviazione e le spese generali operative, indipendentemente dal fatto che si utilizzi SAN o NAS. Utilizza le best practice per il provisioning degli archivi dati e ottimizza le impostazioni host ESXi per ambienti NFS e di archiviazione a blocchi. Per tutti questi vantaggi, NetApp consiglia questo plug-in quando si utilizza vSphere con sistemi che eseguono il software ONTAP .

L’SRA viene utilizzato insieme all’SRM per gestire la replica dei dati delle VM tra siti di produzione e di disaster recovery per i tradizionali datastore VMFS e NFS e anche per i test non disruptivi delle repliche DR. Aiuta ad automatizzare le attività di individuazione, ripristino e riprotezione.

In questo scenario mostreremo come distribuire e utilizzare VMWare Site Recovery Manager per proteggere i datastore ed eseguire sia un test che un failover finale su un sito secondario. Vengono inoltre discussi i temi della riprotezione e del failback.

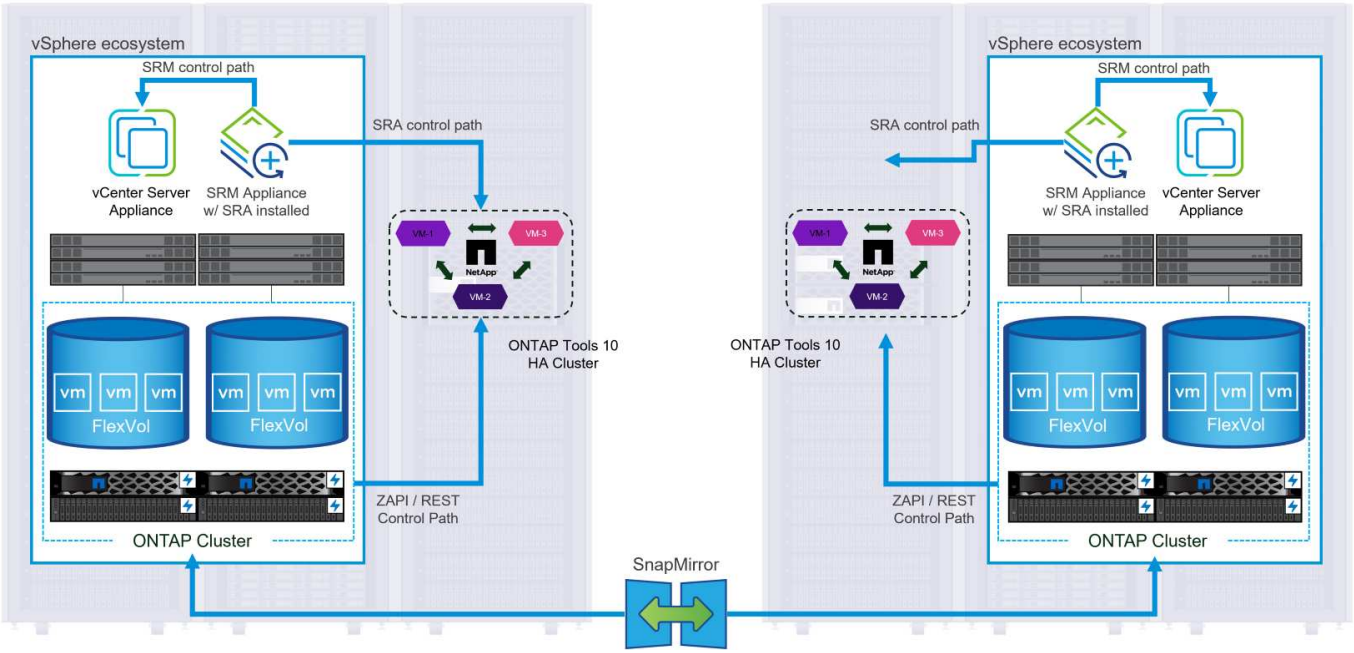
Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Configurare SRM con server vCenter nei siti primari e secondari.
- Installare l’adattatore SRA per gli ONTAP tools for VMware vSphere 10 ed effettuare la registrazione con vCenters.
- Creare relazioni SnapMirror tra i sistemi di archiviazione ONTAP di origine e di destinazione
- Configurare Site Recovery per SRM.
- Eseguire il test e il failover finale.
- Discutere di riprotezione e failback.

Architettura

Il diagramma seguente mostra una tipica architettura VMware Site Recovery con ONTAP tools for VMware vSphere 10 configurati in una configurazione ad alta disponibilità a 3 nodi.



Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Cluster vSphere 8 installati sia nella sede primaria che in quella secondaria con una rete adatta per le comunicazioni tra gli ambienti.
- Sistemi di archiviazione ONTAP sia nella sede primaria che in quella secondaria, con porte dati fisiche sugli switch Ethernet dedicate al traffico di archiviazione NFS.
- Gli ONTAP tools for VMware vSphere 10 sono installati e entrambi i server vCenter sono registrati.
- Sono stati installati i dispositivi VMware Site Replication Manager per i siti primario e secondario.
    - Sono state configurate le mappature dell'inventario (rete, cartella, risorsa, criterio di archiviazione) per SRM.

NetApp consiglia una progettazione di rete ridondante per NFS, che garantisca tolleranza agli errori per sistemi di storage, switch, adattatori di rete e sistemi host. È comune distribuire NFS con una singola subnet o più subnet a seconda dei requisiti architettonici.

Fare riferimento a "Procedure consigliate per l'esecuzione di NFS con VMware vSphere" per informazioni dettagliate specifiche su VMware vSphere.

Per indicazioni di rete sull'utilizzo di ONTAP con VMware vSphere, fare riferimento a "Configurazione di rete - NFS" sezione della documentazione delle 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 distribuzione

Nelle sezioni seguenti vengono descritti i passaggi di distribuzione per implementare e testare una configurazione di VMware Site Recovery Manager con sistema di archiviazione ONTAP .

Crea una relazione SnapMirror tra i sistemi di archiviazione ONTAP

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

Fare riferimento alla documentazione ONTAP a partire da "QUI" per informazioni complete sulla creazione di relazioni SnapMirror per volumi ONTAP .

Le istruzioni dettagliate sono descritte nel seguente documento, disponibile"QUI" . Questi passaggi descrivono come creare relazioni peer tra cluster e peer tra SVM e quindi relazioni SnapMirror per ciascun volume. Questi passaggi possono essere eseguiti in ONTAP System Manager o utilizzando ONTAP CLI.

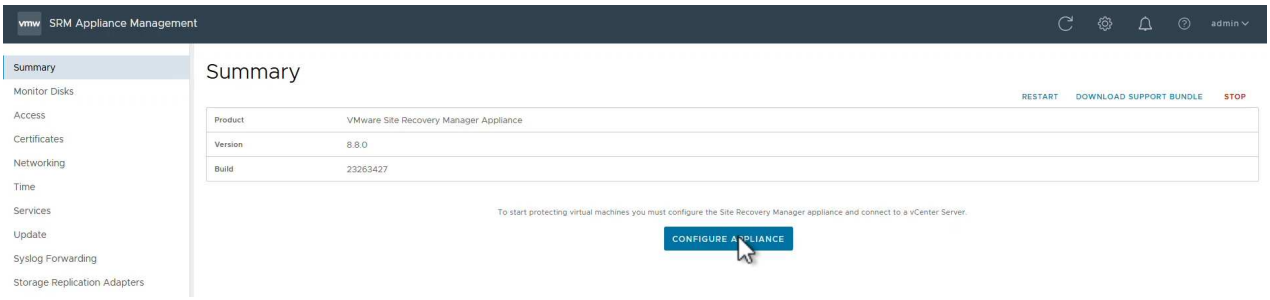
Configurare l’appliance SRM

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

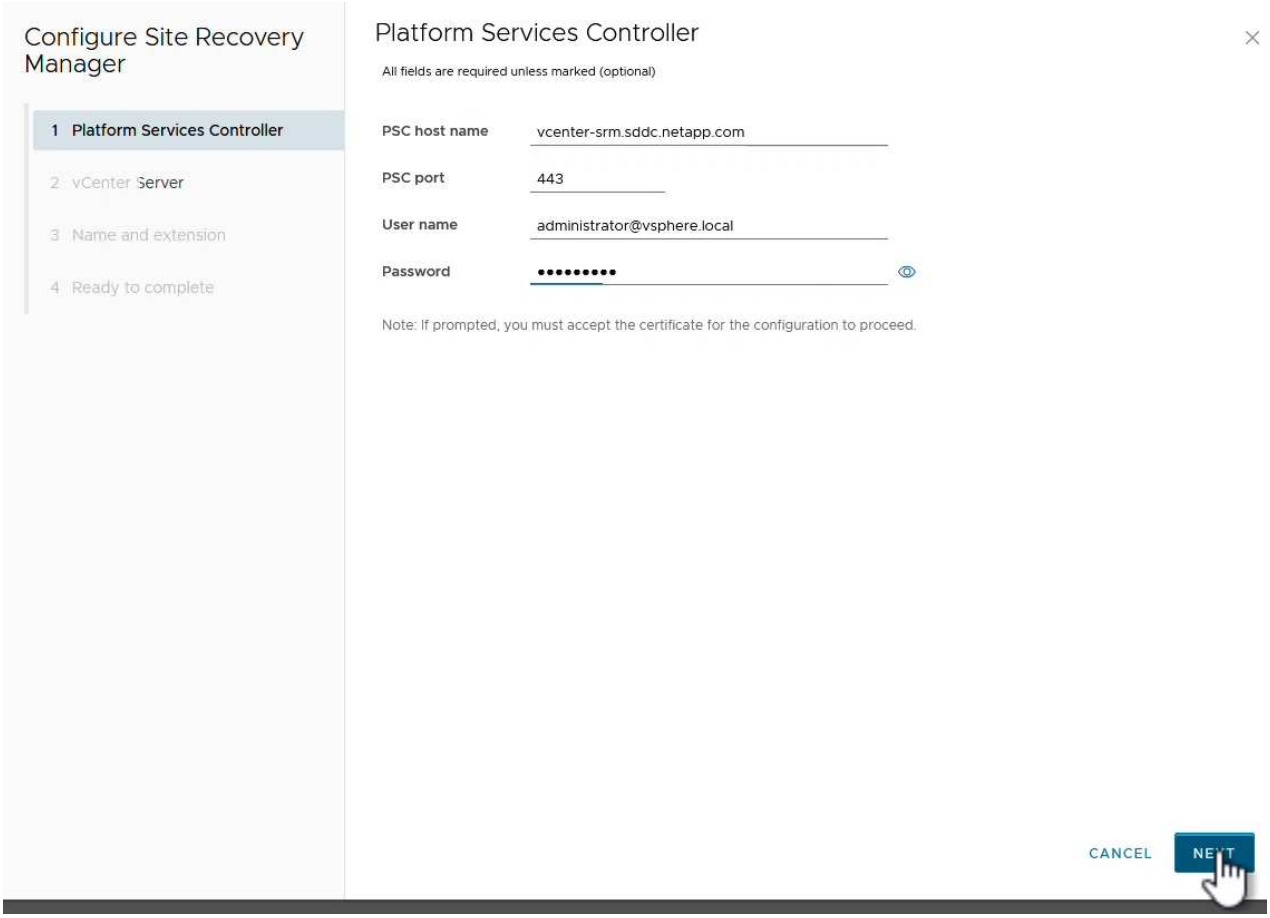
Collegare l'appliance SRM per i siti primari e secondari

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

1. In un browser web, vai a `https://<SRM_appliance_IP>:5480` ed effettua l'accesso. Fai clic su **Configura appliance** per iniziare.

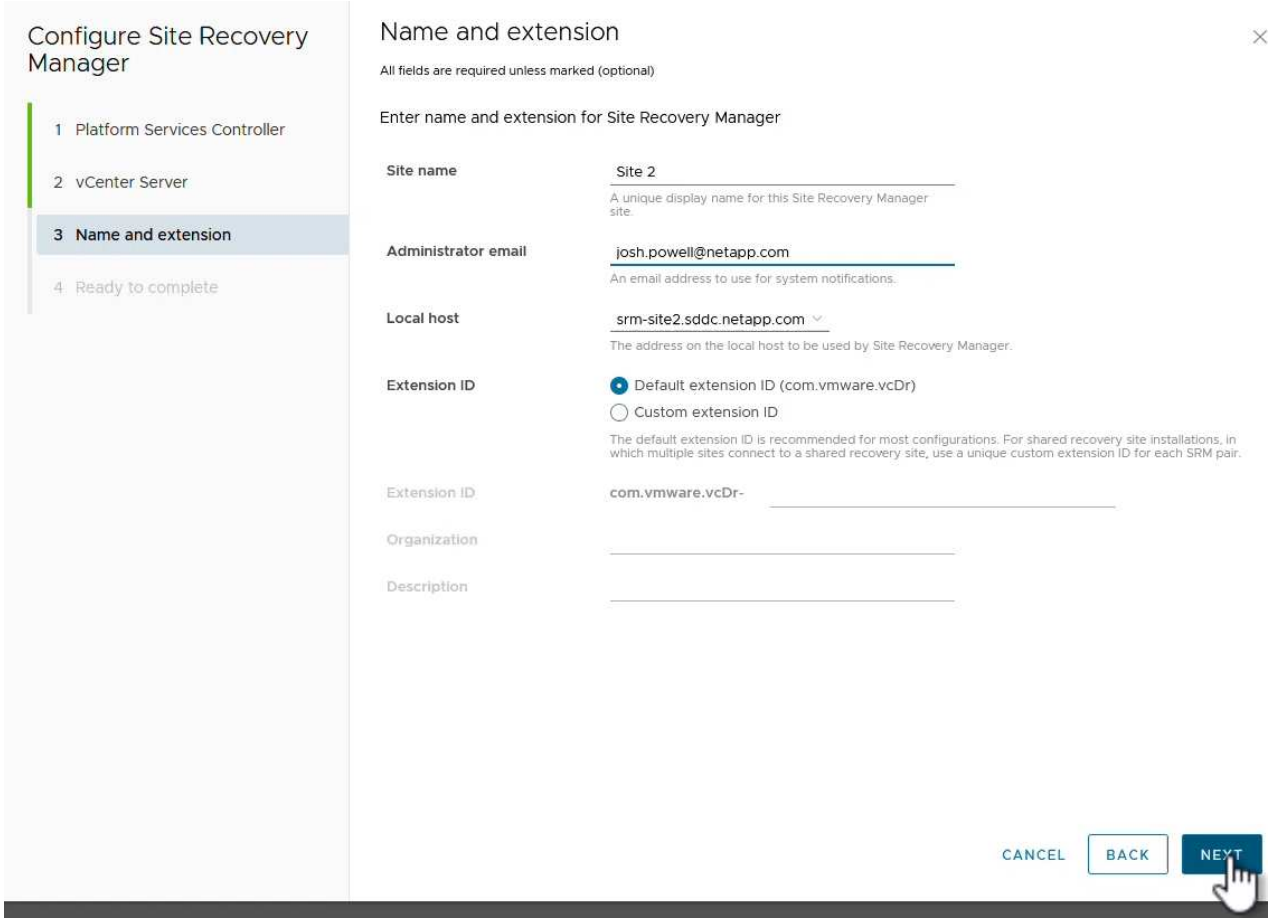


2. Nella pagina **Platform Services Controller** della procedura guidata Configura Site Recovery Manager, immettere le credenziali del server vCenter su cui verrà registrato SRM. Fare clic su **Avanti** per continuare.



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

4. Nella pagina **Nome ed estensione**, inserisci un nome per il sito SRM, un indirizzo email dell'amministratore e l'host locale che SRM dovrà utilizzare. Fare clic su **Avanti** per continuare.

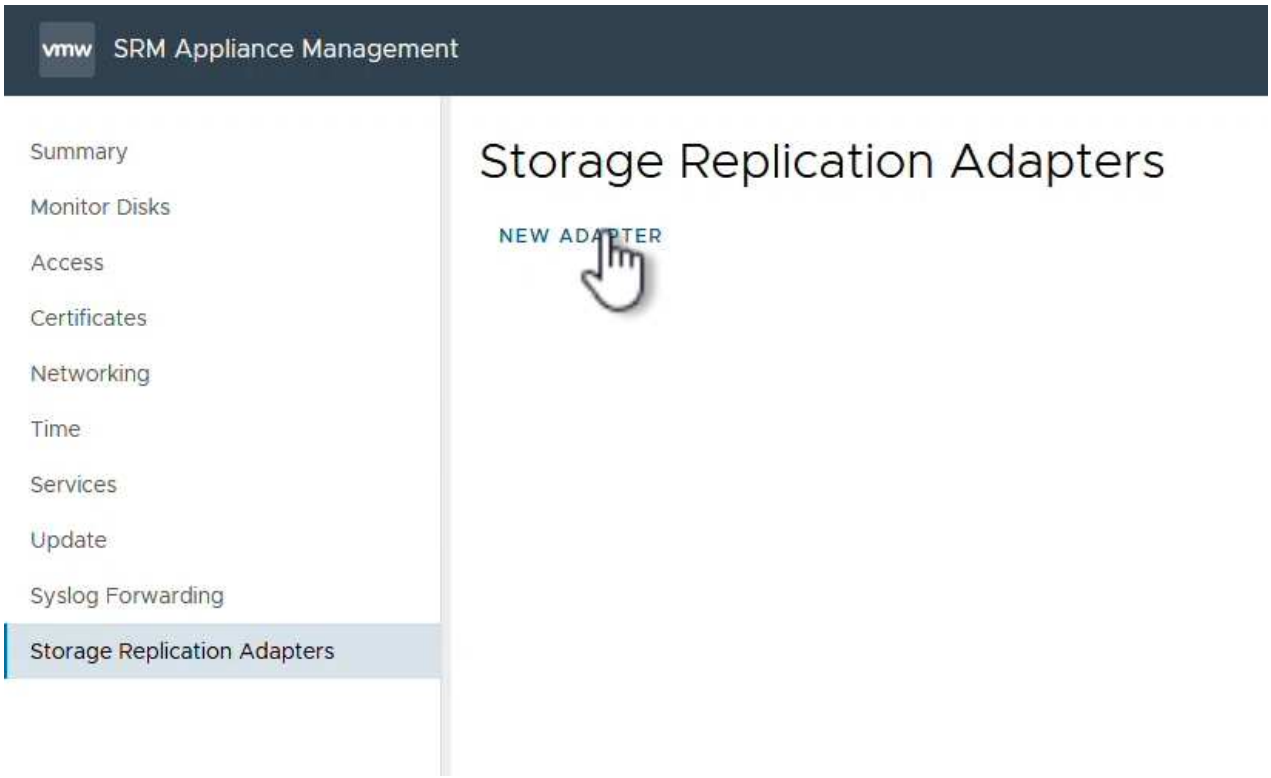


5. Nella pagina **Pronto per il completamento** rivedi il riepilogo delle modifiche

Configurare SRA sull'appliance SRM

Completare i seguenti passaggi per configurare l'SRA sull'appliance SRM:

1. Scarica l'SRA per gli strumenti ONTAP 10 su "Sito di supporto NetApp" e salvare il file tar.gz in una cartella locale.
2. Dall'appliance di gestione SRM fare clic su **Storage Replication Adapters** nel menu a sinistra e quindi su **Nuovo adattatore**.



3. Seguire i passaggi descritti nel sito di documentazione degli strumenti ONTAP 10 all'indirizzo "Configurare SRA sull'appliance SRM" . Una volta completata l'operazione, l'SRA può comunicare con l'SRA utilizzando l'indirizzo IP e le credenziali del server vCenter forniti.

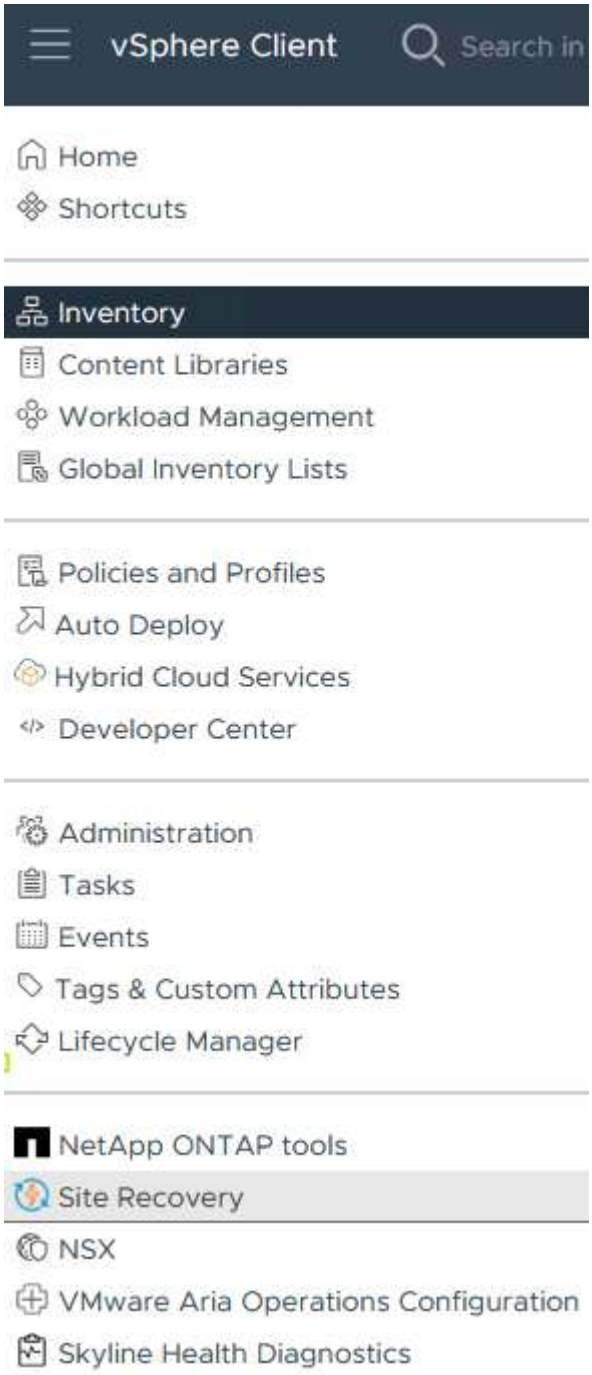
Configurare Site Recovery per SRM

Completare i seguenti passaggi per configurare l'associazione dei siti, creare gruppi di protezione,

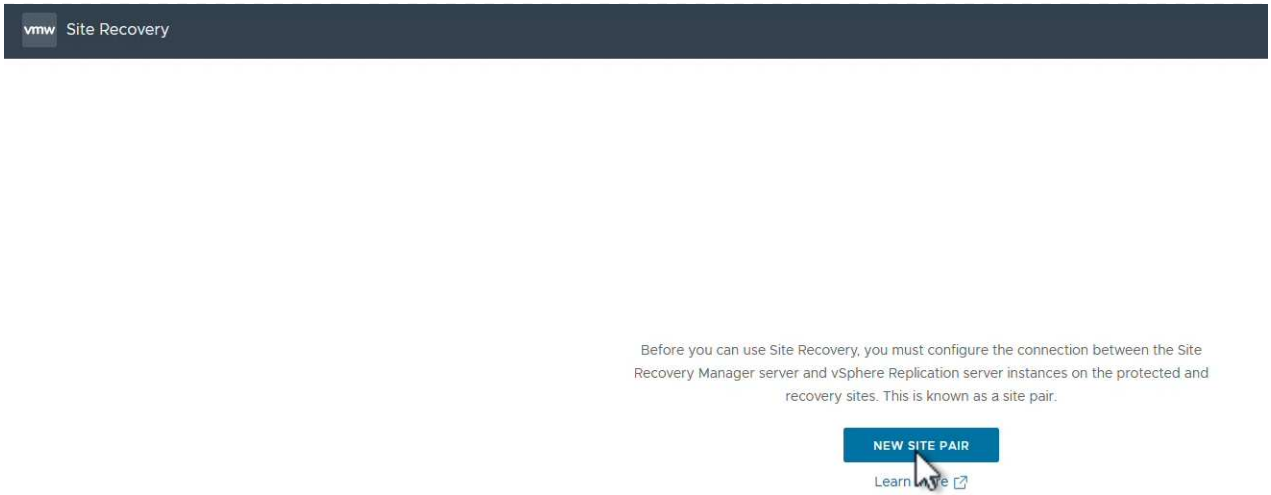
Configurare l'associazione dei siti per SRM

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

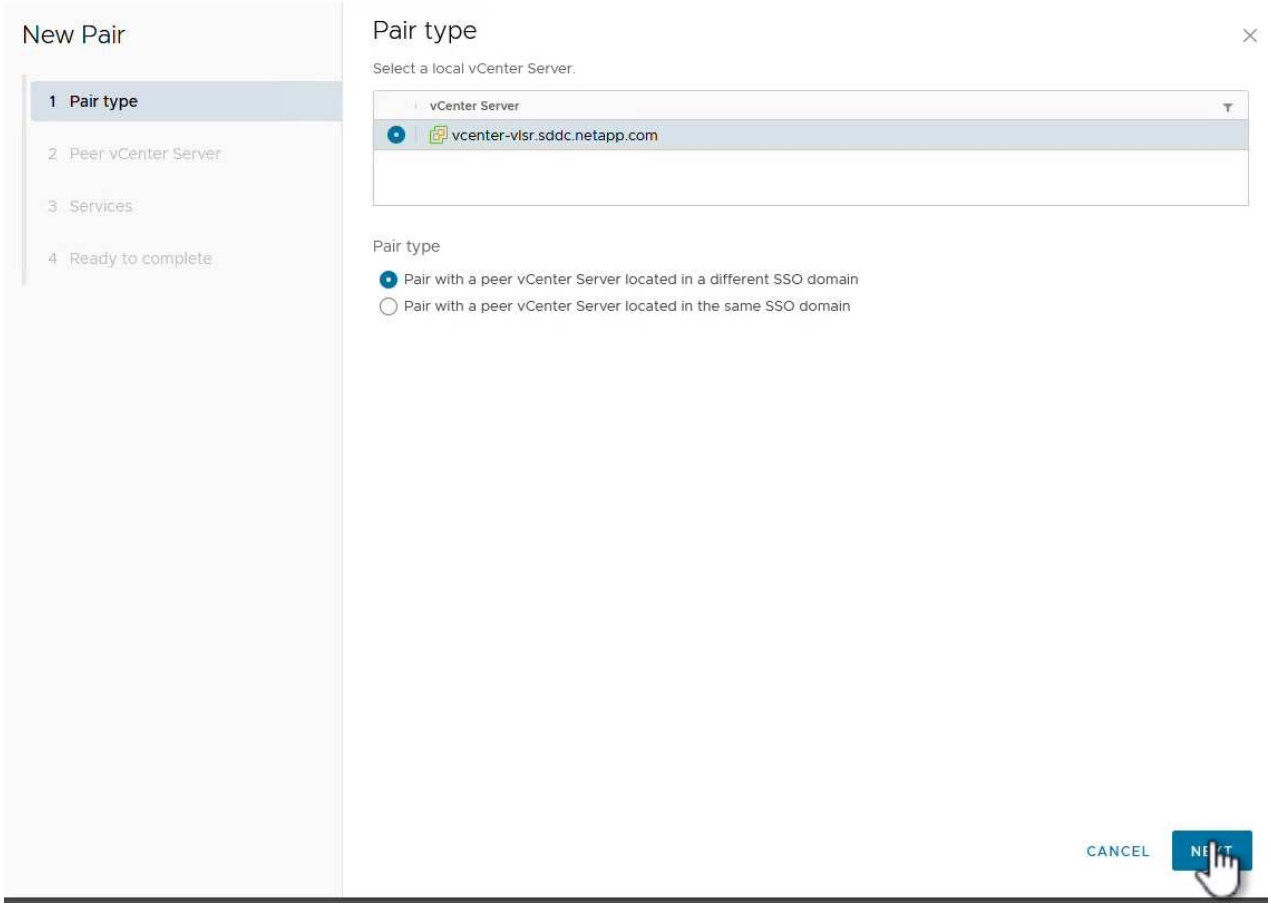
1. Nel client vSphere fare clic su **Site Recovery** nel menu a sinistra. Si apre una nuova finestra del browser con l'interfaccia utente di gestione SRM sul sito principale.



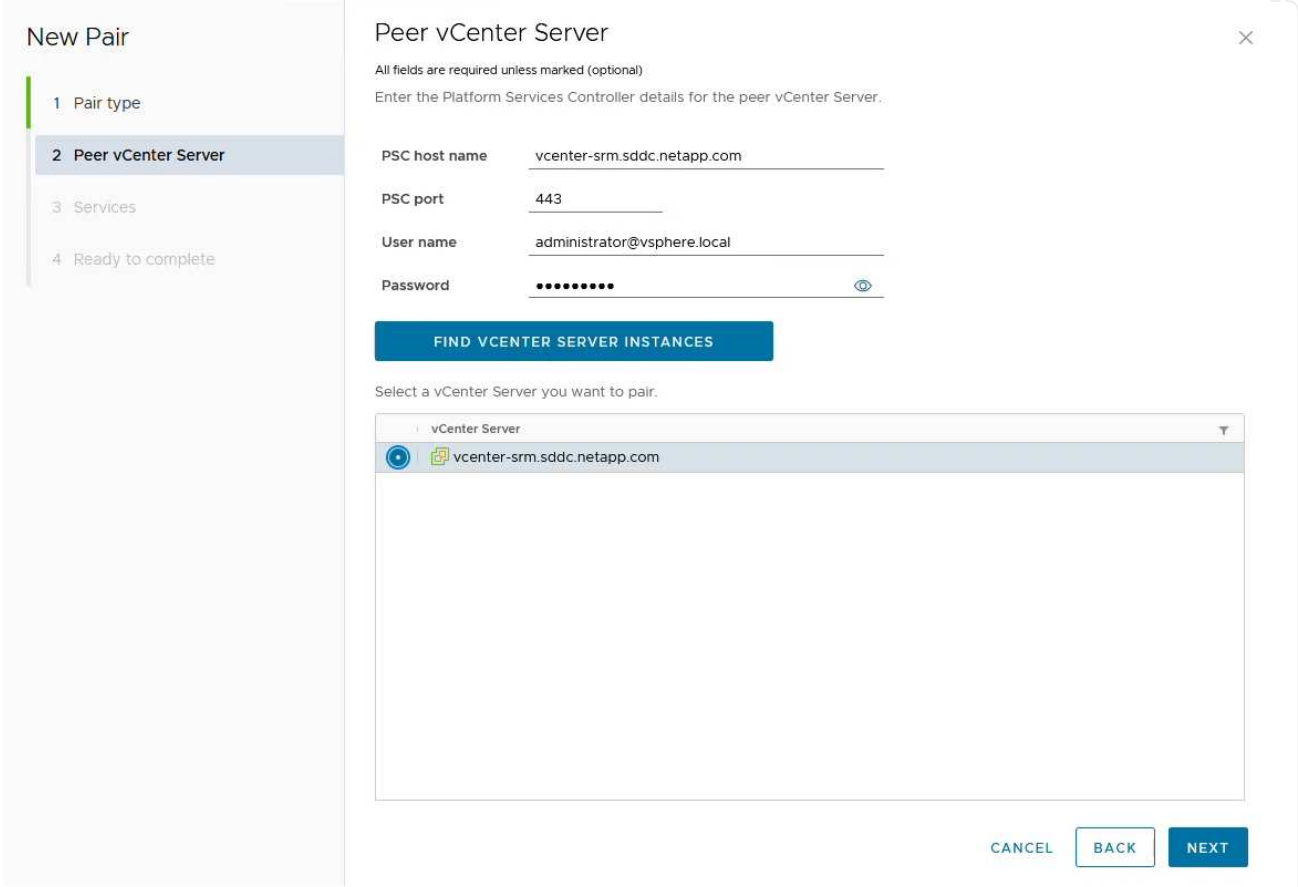
2. Nella pagina **Ripristino sito**, fare clic su **NUOVA COPPIA SITI**.



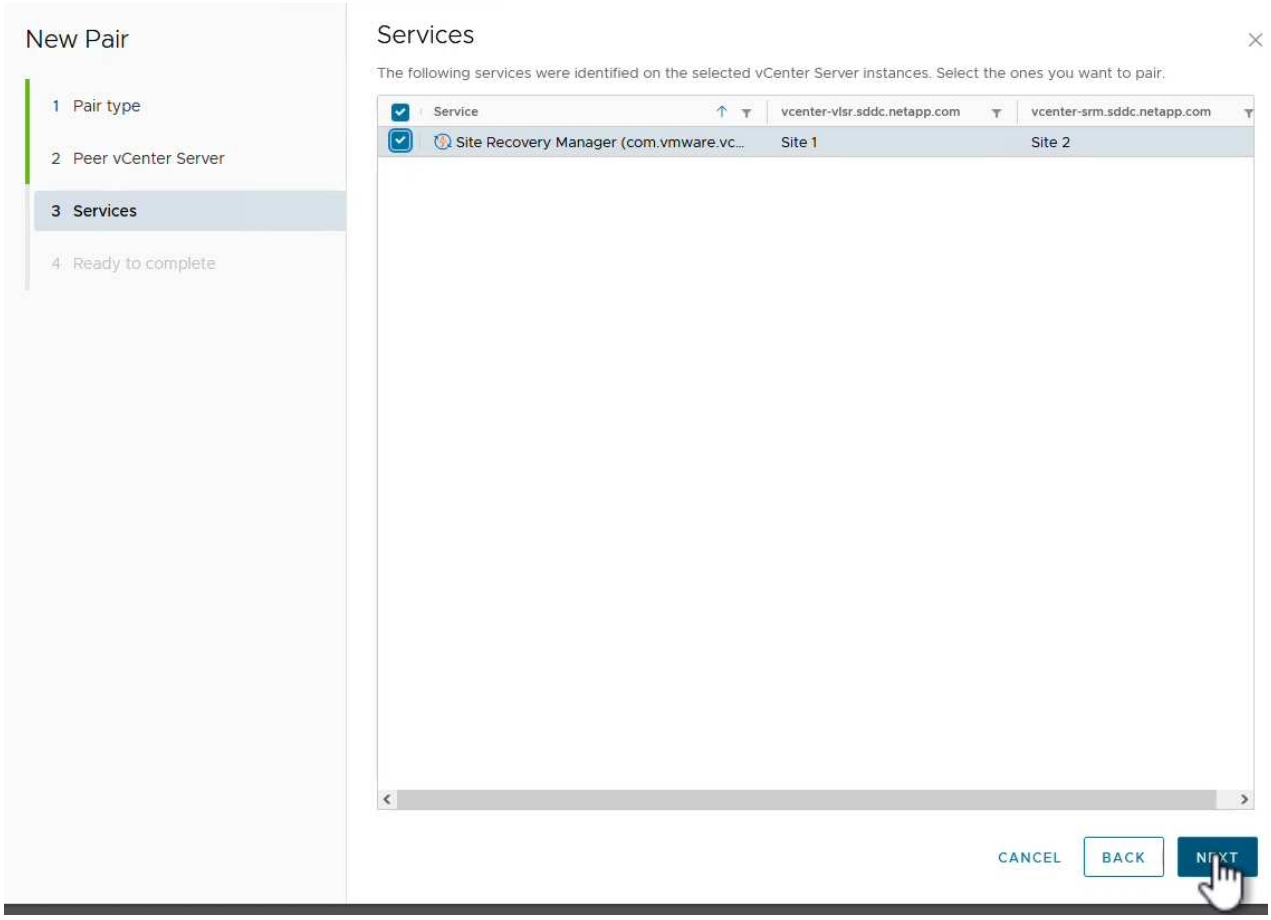
3. Nella pagina **Tipo di coppia** della **Procedura guidata Nuova coppia**, verificare che sia selezionato il server vCenter locale e selezionare il **Tipo di coppia**. Fare clic su **Avanti** per continuare.



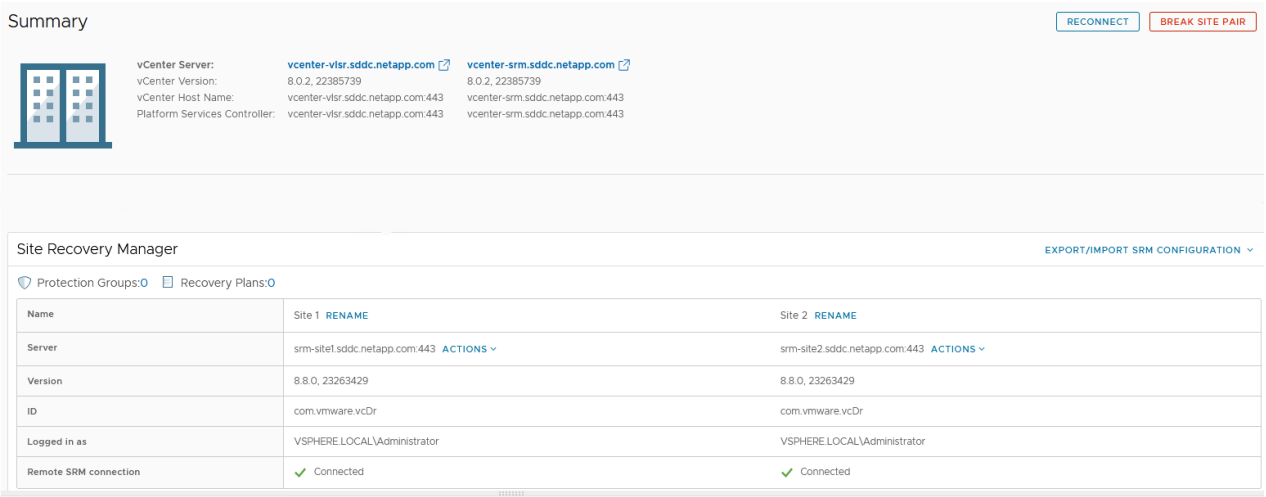
4. Nella pagina **Peer vCenter**, compilare le credenziali del vCenter nel sito secondario e fare clic su **Trova istanze vCenter**. Verificare che l'istanza vCenter sia stata rilevata e fare clic su **Avanti** per continuare.



5. Nella pagina **Servizi**, seleziona la casella accanto all'abbinamento di siti proposto. Fare clic su **Avanti** per continuare.



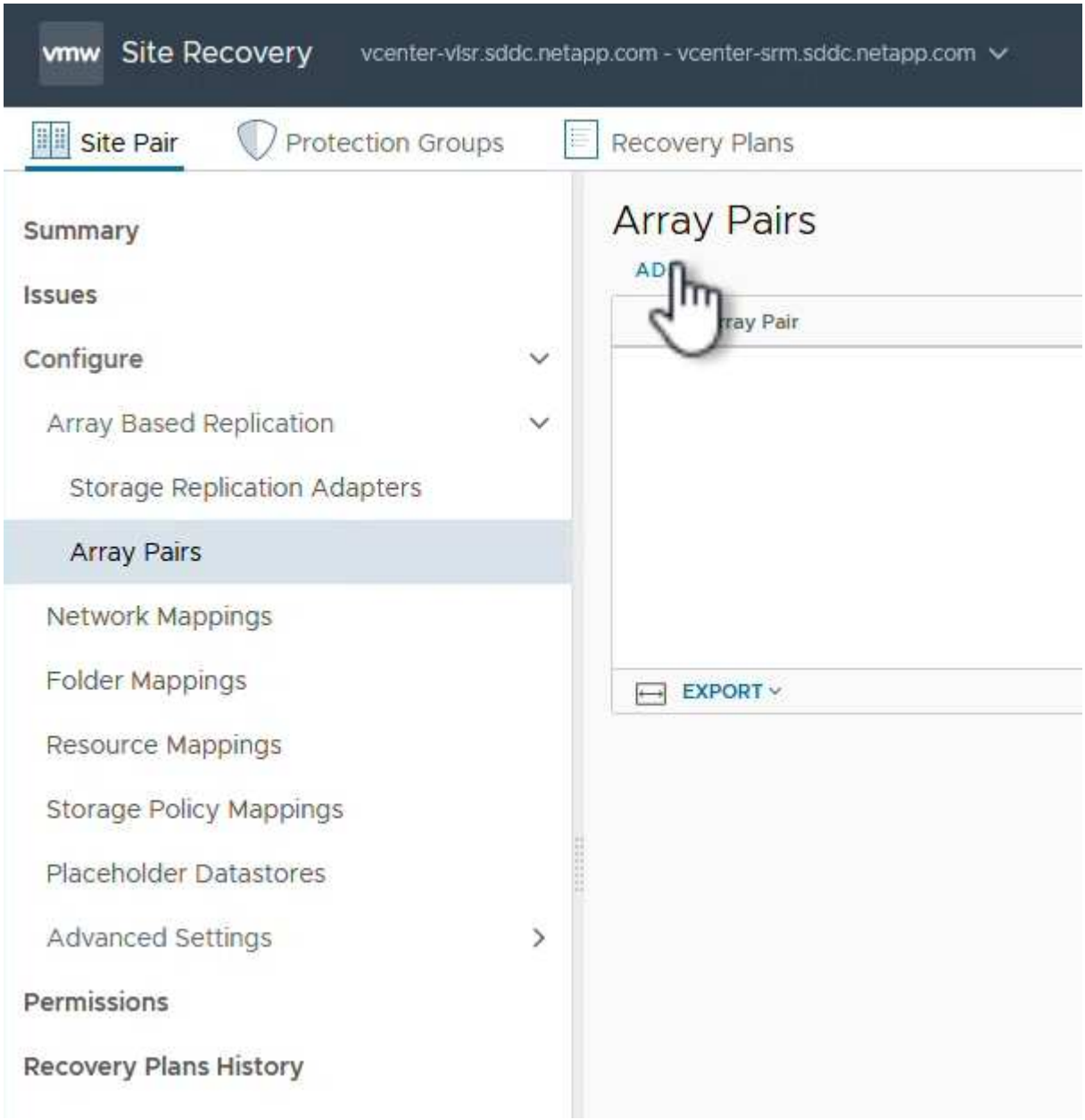
6. Nella pagina **Pronto per il completamento**, rivedere la configurazione proposta e quindi fare clic sul pulsante **Fine** per creare l'associazione del sito
7. La nuova coppia di siti e il relativo riepilogo possono essere visualizzati nella pagina Riepilogo.



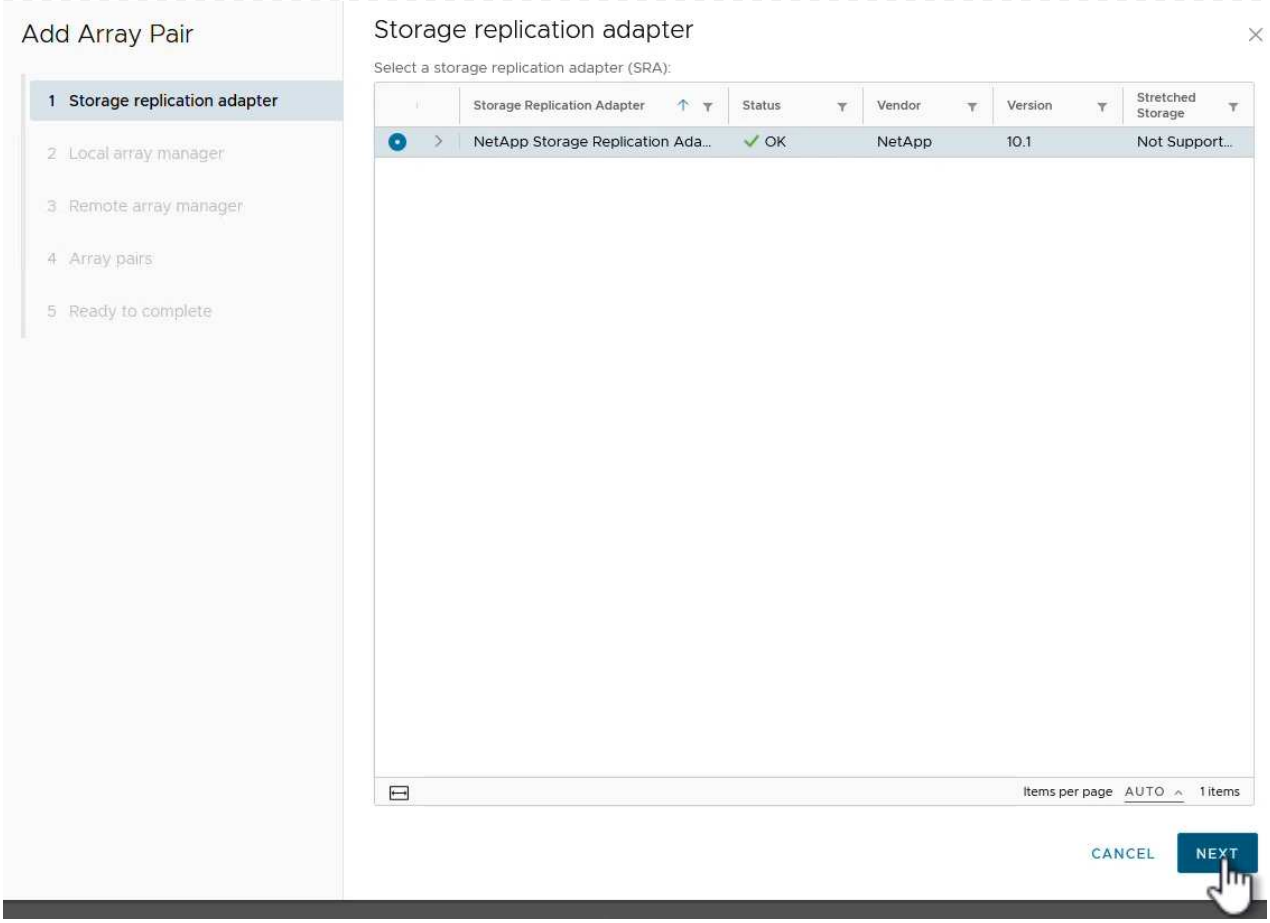
Aggiungi una coppia di array per SRM

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

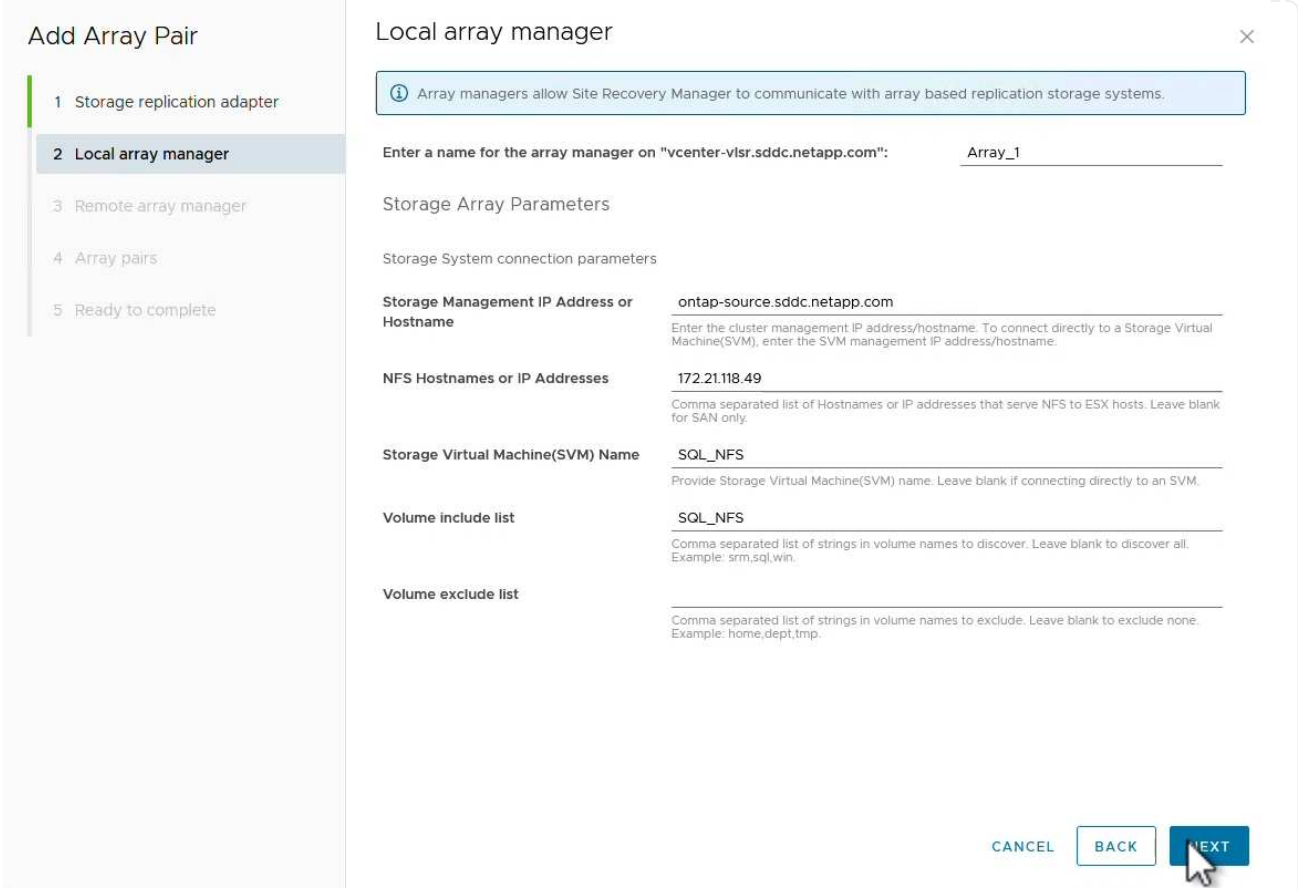
1. Nell'interfaccia di Site Recovery, accedere a **Configura > Replica basata su array > Coppie di array** nel menu a sinistra. Clicca su **AGGIUNGI** per iniziare.



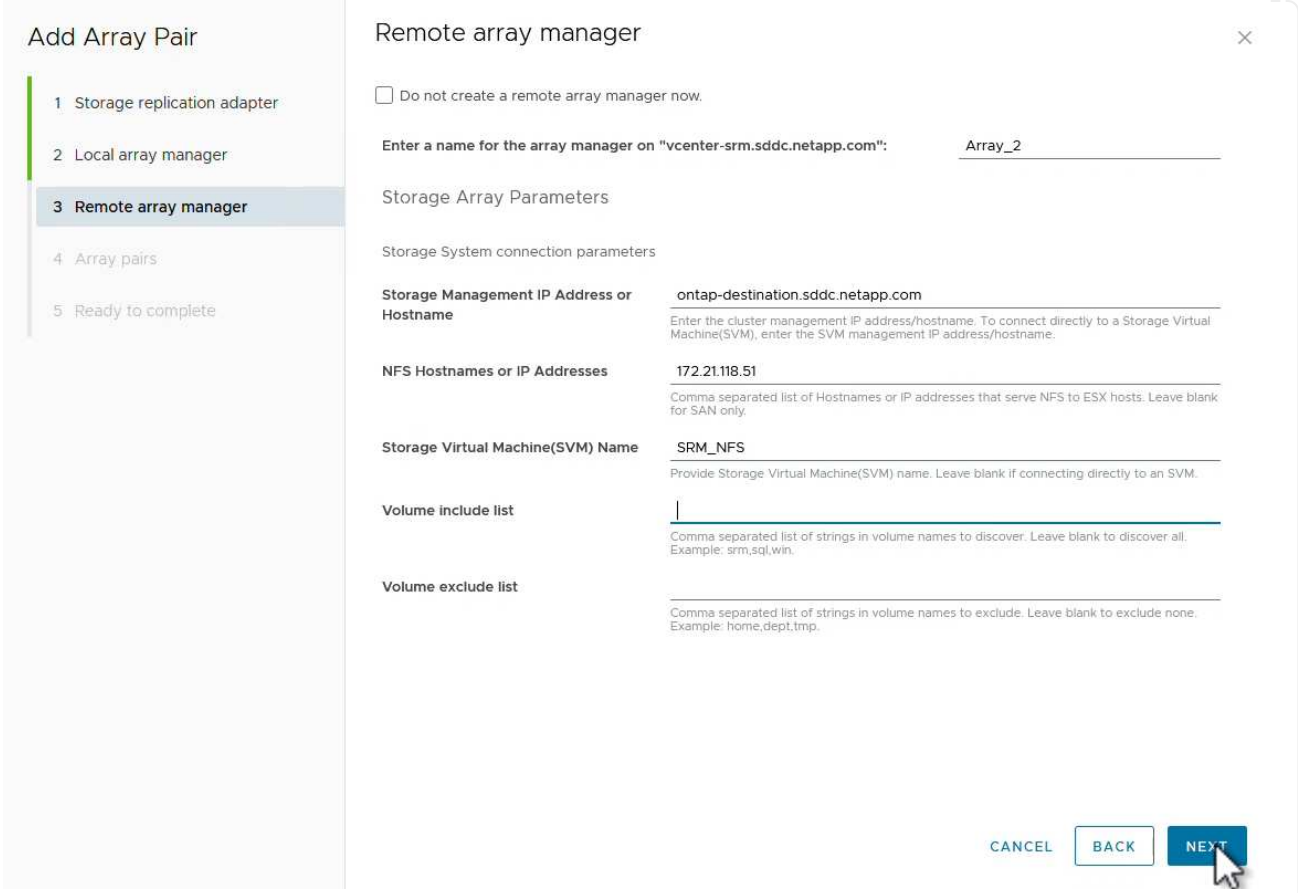
2. Nella pagina **Storage replication adapter** della procedura guidata **Aggiungi coppia di array**, verificare che l'adattatore SRA sia presente per il sito primario e fare clic su **Avanti** per continuare.



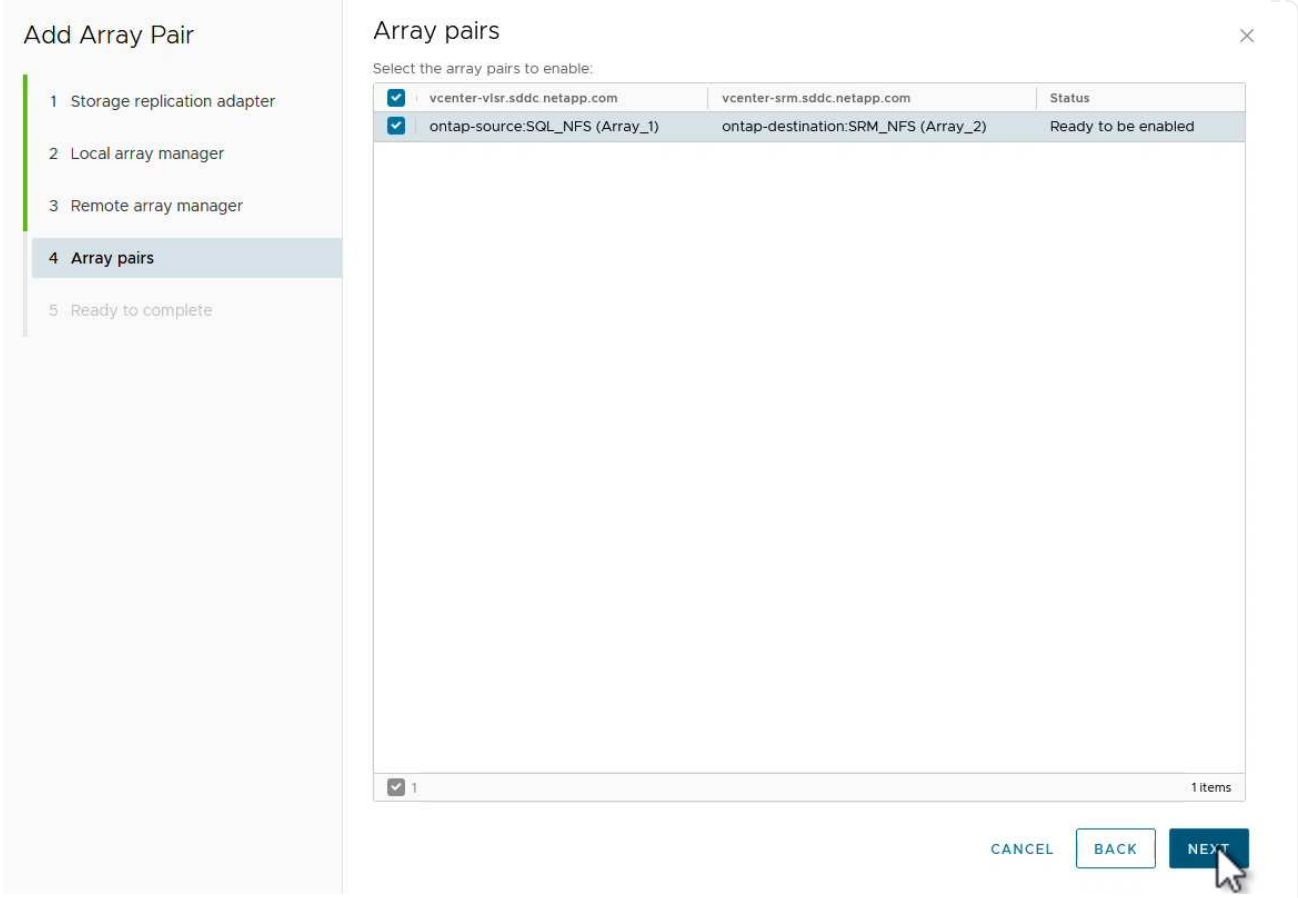
3. Nella pagina **Gestore array locale**, immettere un nome per l'array nel sito primario, il nome di dominio completo (FQDN) del sistema di archiviazione, gli indirizzi IP SVM che servono NFS e, facoltativamente, i nomi dei volumi specifici da rilevare. Fare clic su **Avanti** per continuare.



4. Nel **Remote array manager** compilare le stesse informazioni dell'ultimo passaggio per il sistema di archiviazione ONTAP nel sito secondario.



5. Nella pagina **Coppie di array**, seleziona le coppie di array da abilitare e fai clic su **Avanti** per continuare.

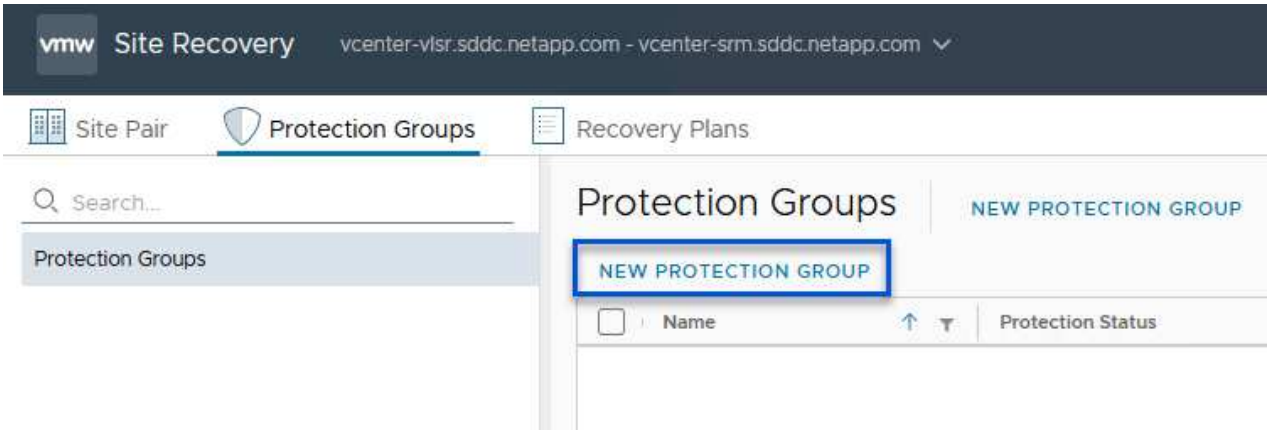


6. Rivedi le informazioni nella pagina **Pronto per il completamento** e clicca su **Fine** per creare la coppia di array.

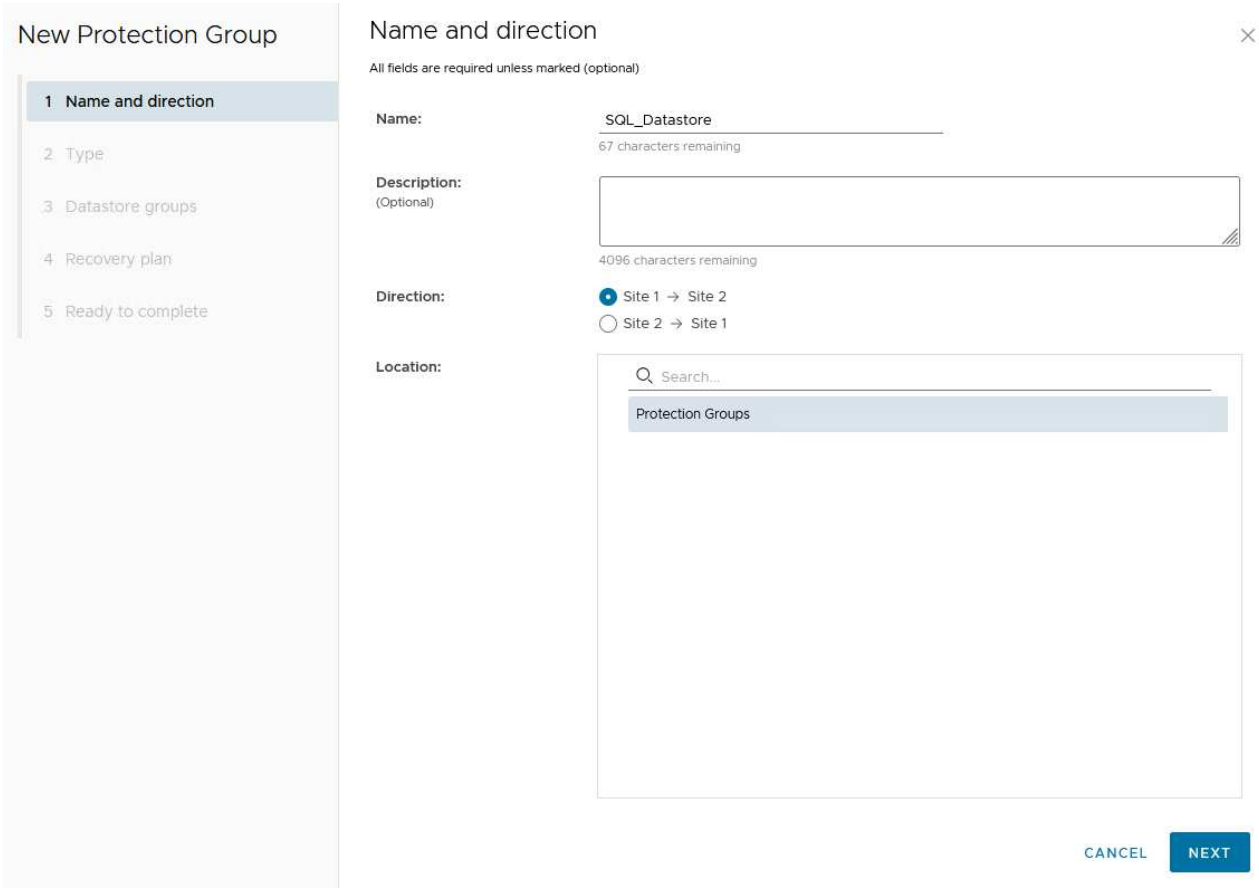
Configurare i gruppi di protezione per SRM

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

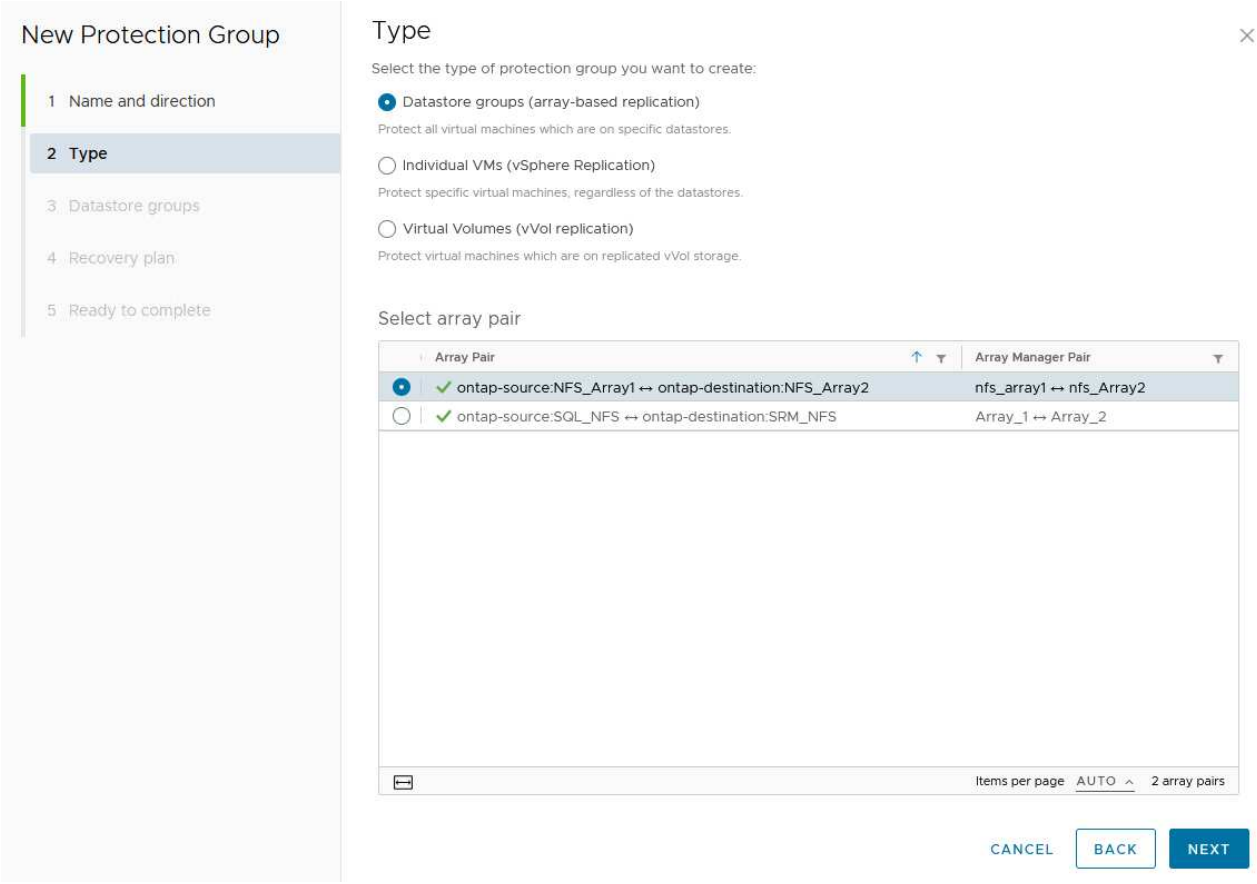
1. Nell'interfaccia di Site Recovery, fare clic sulla scheda **Gruppi di protezione** e quindi su **Nuovo gruppo di protezione** per iniziare.



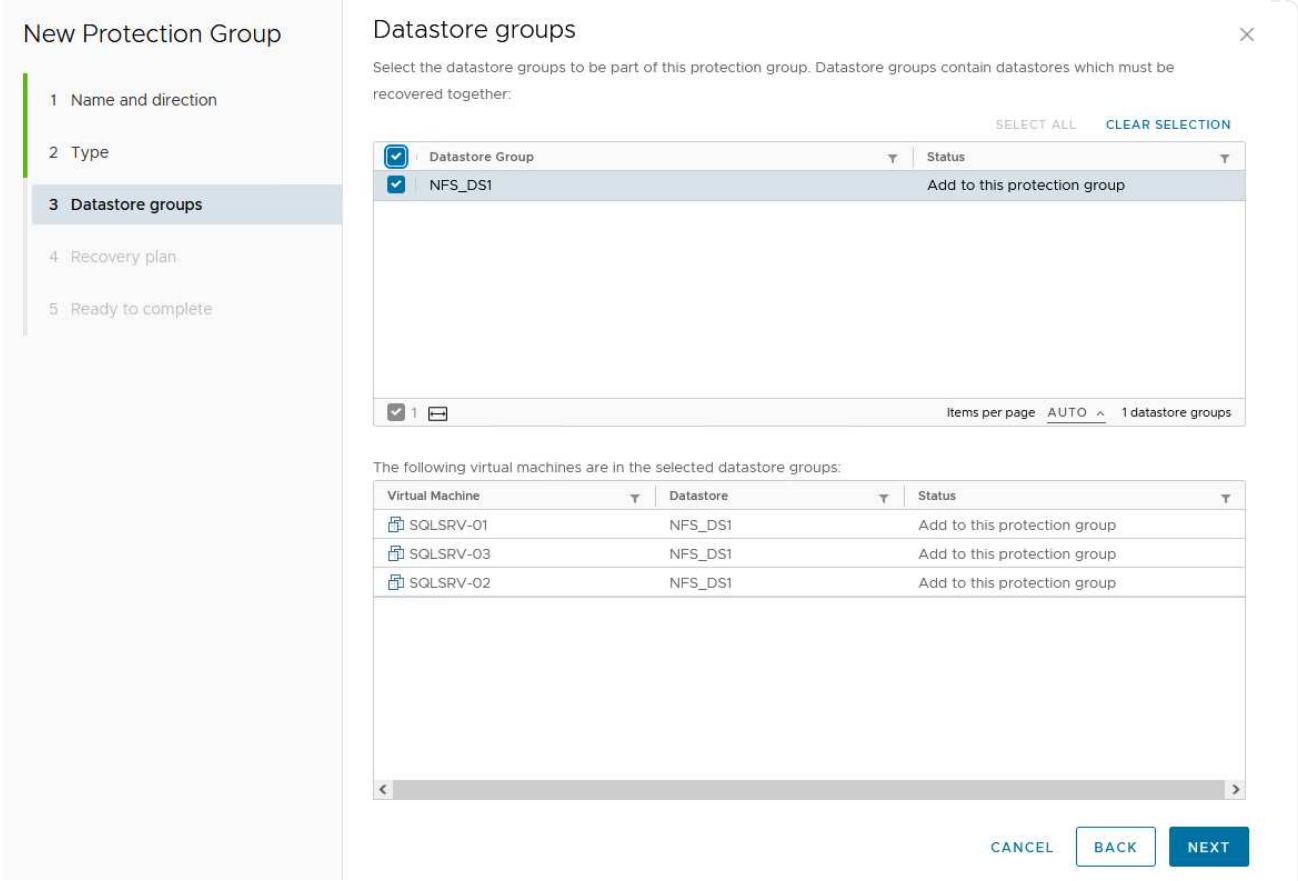
2. Nella pagina **Nome e direzione** della procedura guidata **Nuovo gruppo di protezione**, immettere un nome per il gruppo e scegliere la direzione del sito per la protezione dei dati.



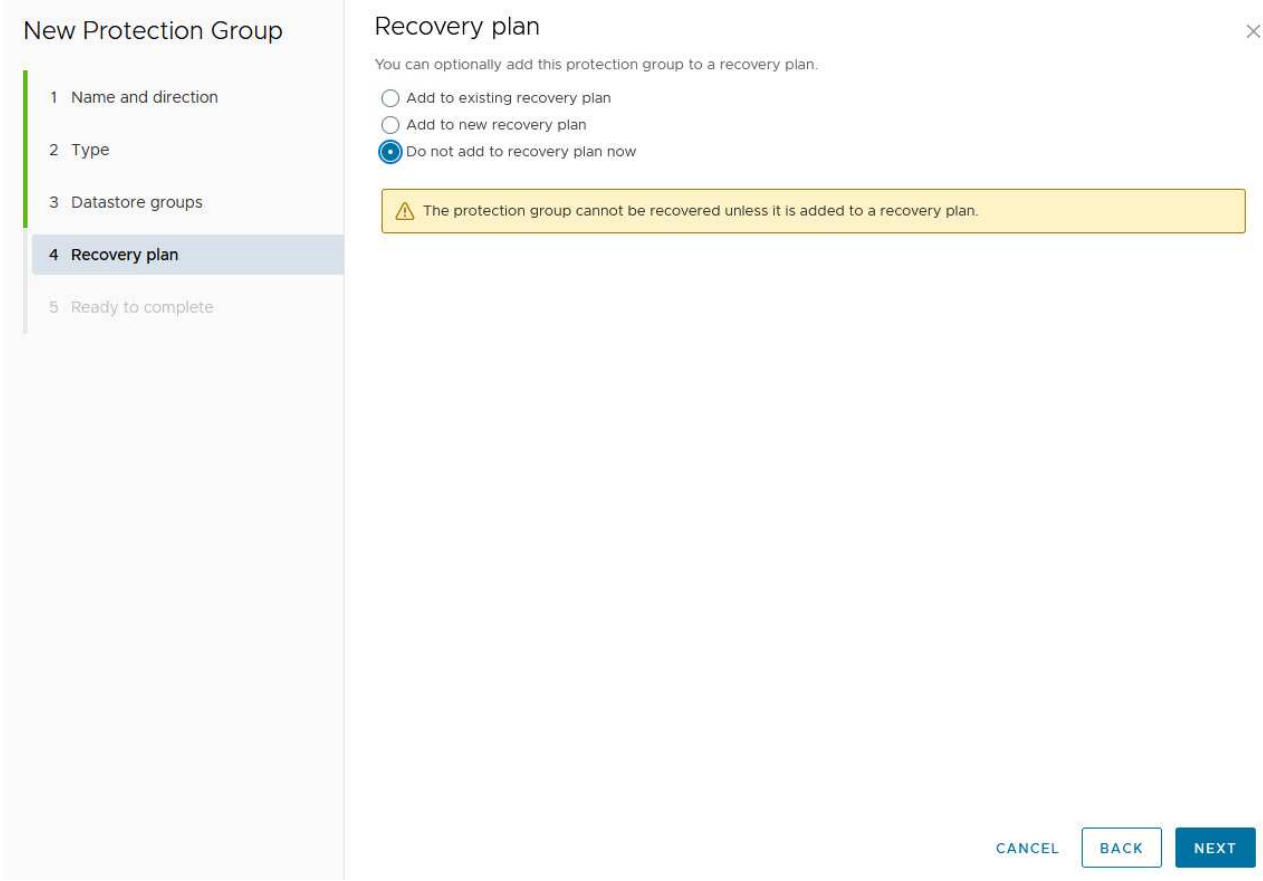
3. Nella pagina **Tipo** selezionare il tipo di gruppo di protezione (datastore, VM o vVol) e selezionare la coppia di array. Fare clic su **Avanti** per continuare.



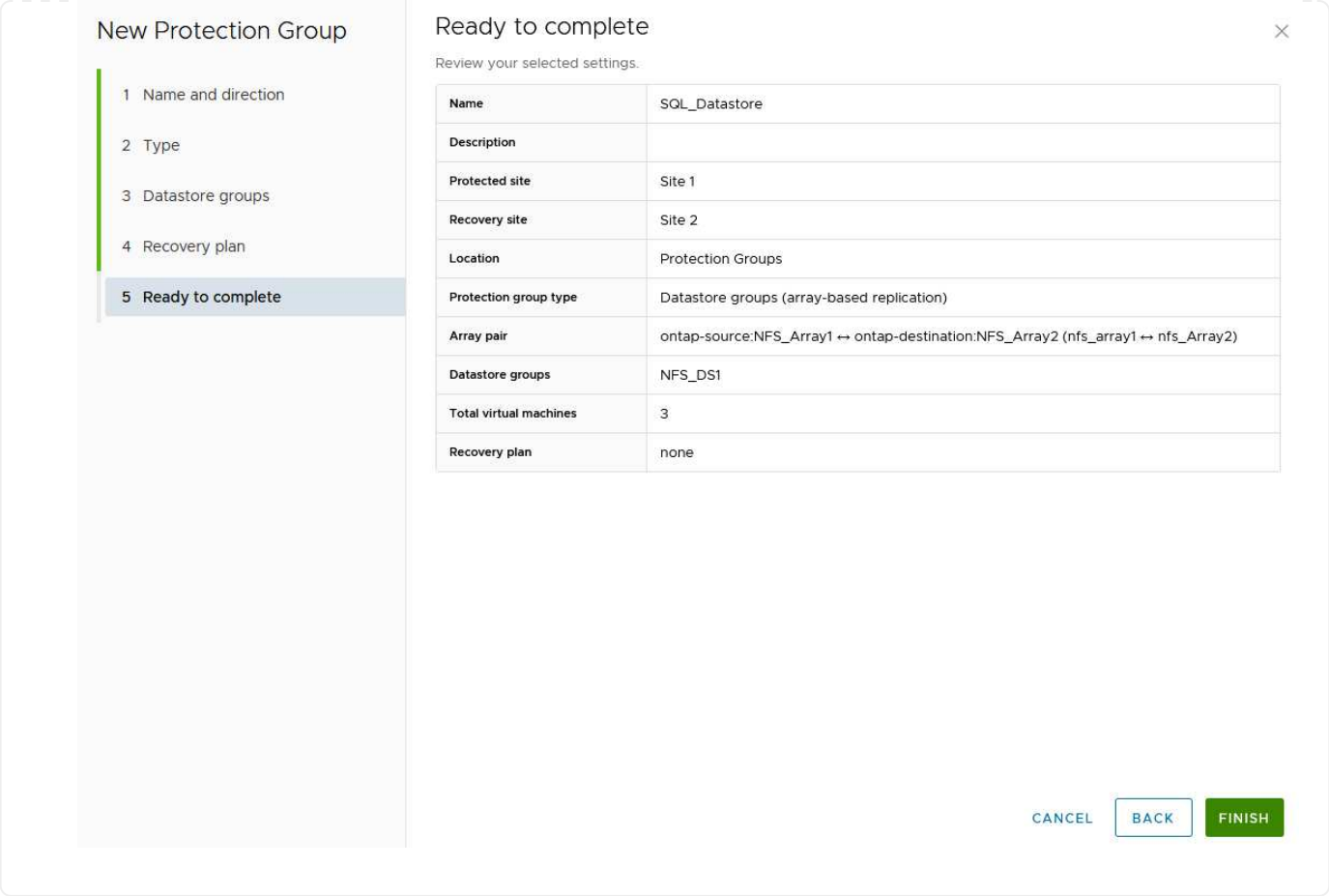
4. Nella pagina **Gruppi di datastore**, seleziona i datastore da includere nel gruppo di protezione. Per ogni datastore selezionato vengono visualizzate le VM attualmente residenti nel datastore. Fare clic su **Avanti** per continuare.



5. Nella pagina **Piano di ripristino**, è possibile scegliere facoltativamente di aggiungere il gruppo di protezione a un piano di ripristino. In questo caso, il piano di ripristino non è ancora stato creato, quindi è selezionata l'opzione **Non aggiungere al piano di ripristino**. Fare clic su **Avanti** per continuare.



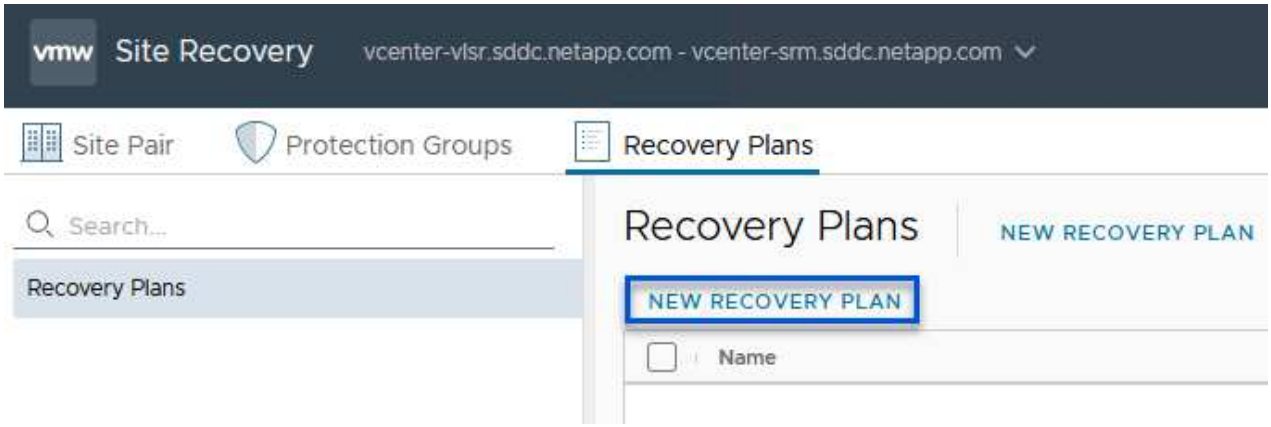
6. Nella pagina **Pronto per il completamento**, rivedere i parametri del nuovo gruppo di protezione e fare clic su **Fine** per creare il gruppo.


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

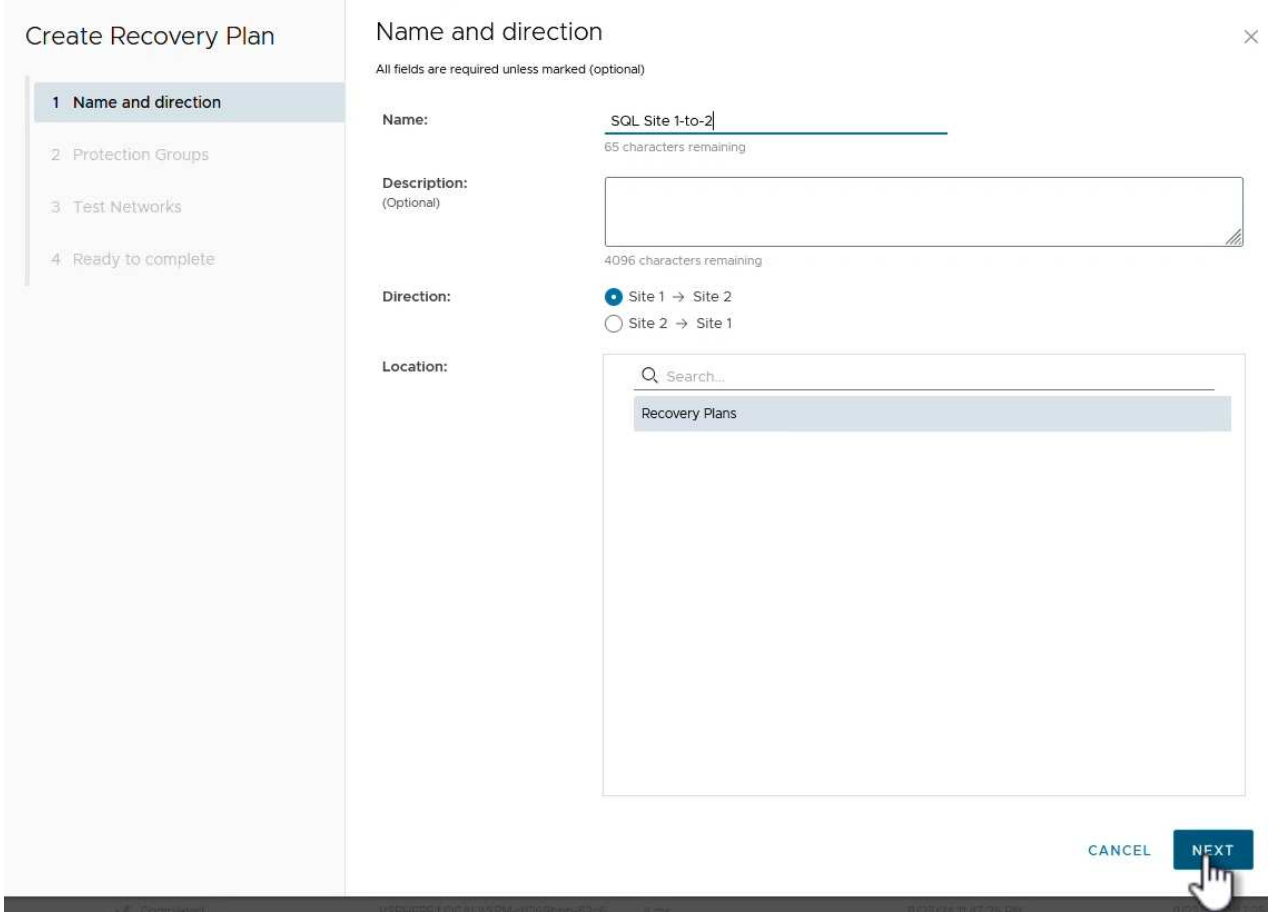
Configurare il piano di ripristino per SRM

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

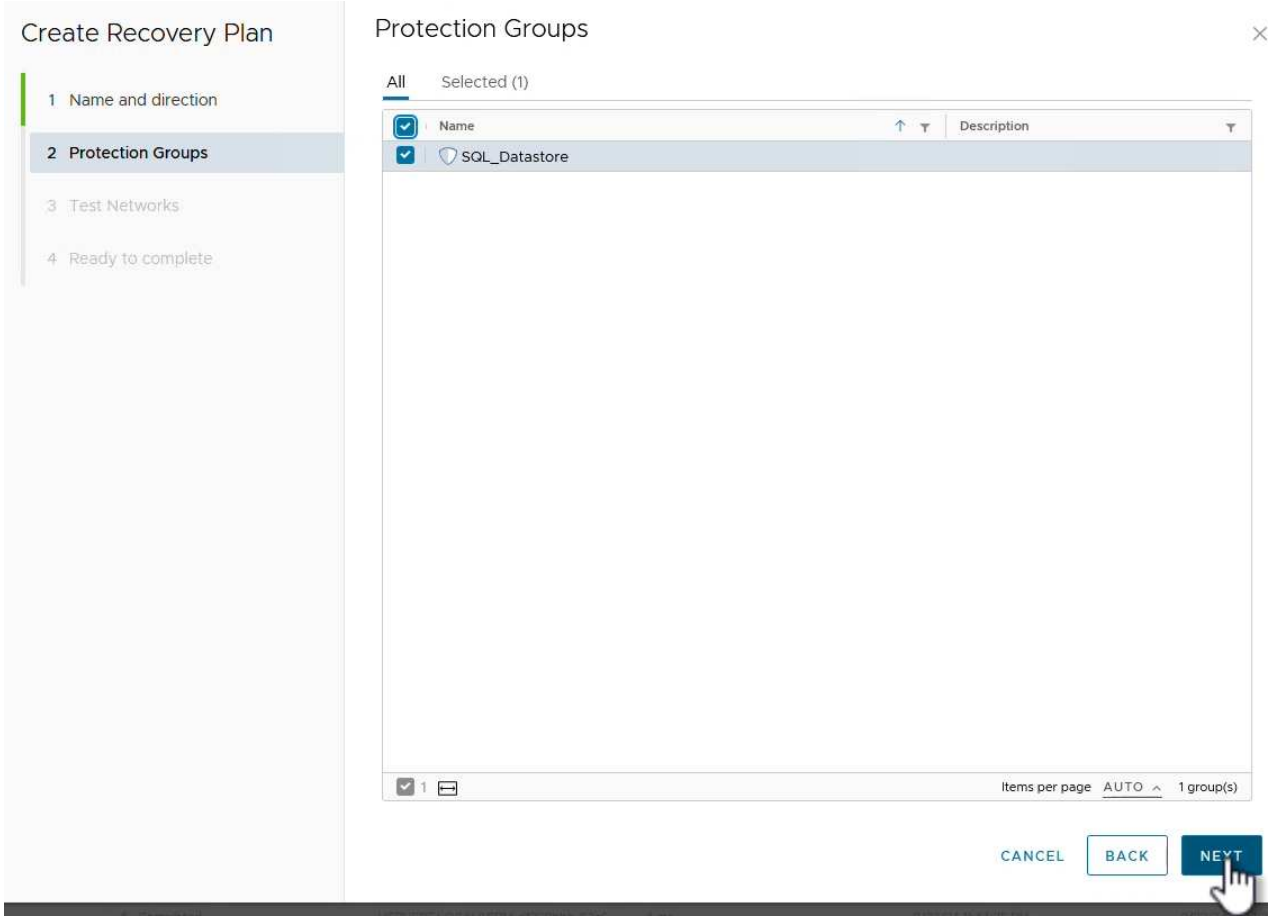
1. Nell'interfaccia di Site Recovery, fare clic sulla scheda **Piano di ripristino** e quindi su **Nuovo piano di ripristino** per iniziare.



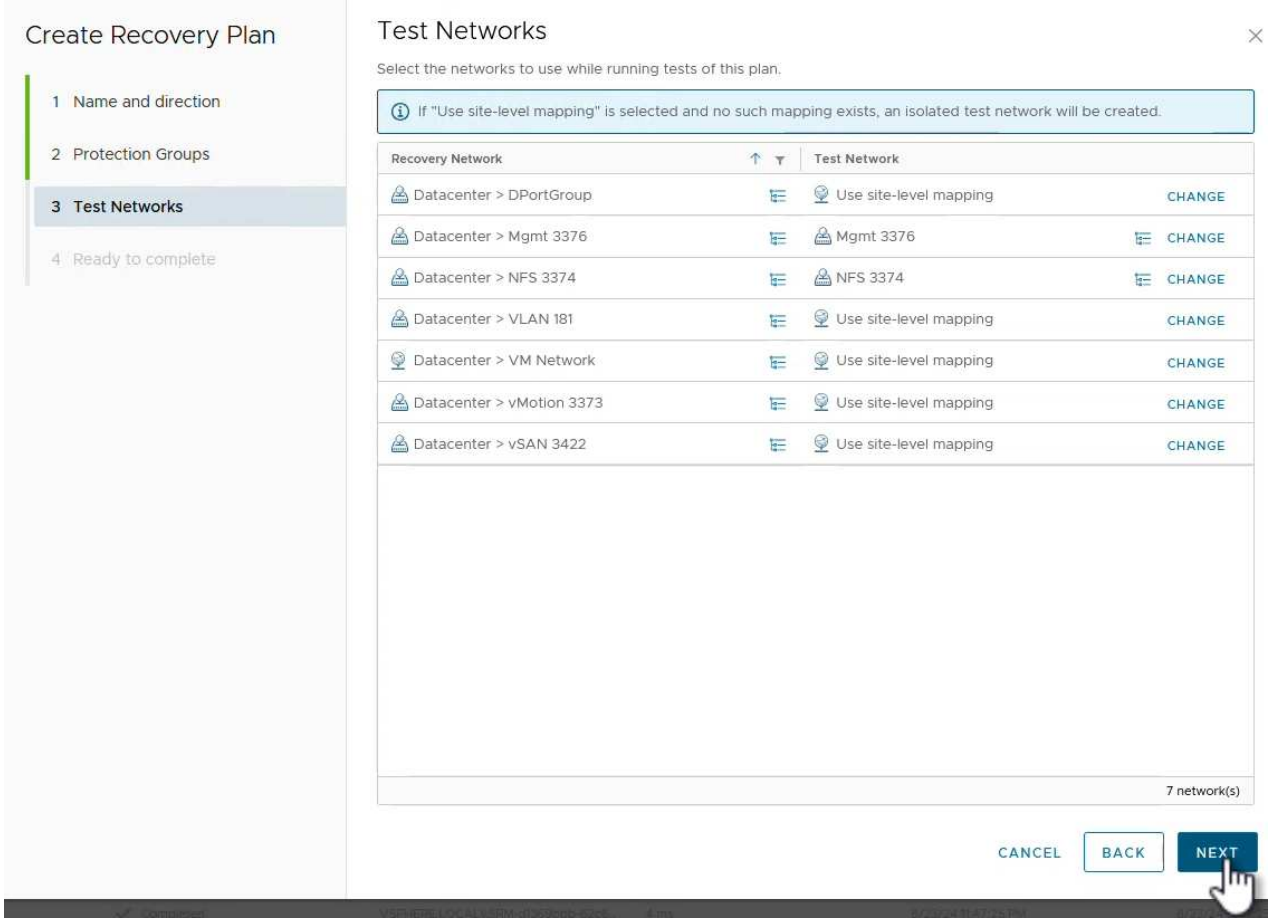
2. Nella pagina **Nome e direzione** della procedura guidata **Crea piano di ripristino**, specificare un nome per il piano di ripristino e scegliere la direzione tra i siti di origine e di destinazione. Fare clic su **Avanti** per continuare.



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. In **Reti di prova** configurare le reti specifiche che verranno utilizzate durante il test del piano. Se non esiste alcuna mappatura o se non viene selezionata alcuna rete, verrà creata una rete di prova isolata. Fare clic su **Avanti** per continuare.



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

Operazioni di disaster recovery con SRM

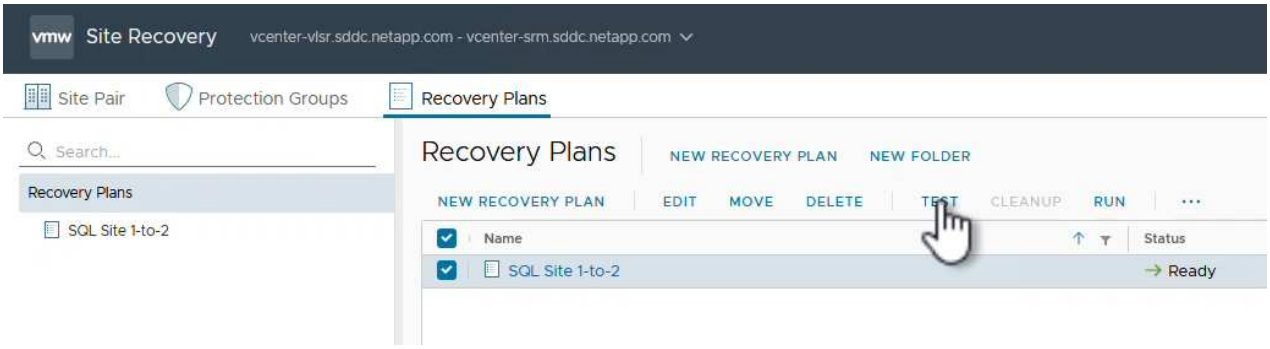
In questa sezione verranno trattate varie funzioni dell'utilizzo del disaster recovery con SRM, tra cui il test del failover, l'esecuzione del failover, l'esecuzione della riprotezione e del failback.

Fare riferimento a "Migliori pratiche operative" per ulteriori informazioni sull'utilizzo dell'archiviazione ONTAP con operazioni di disaster recovery SRM.

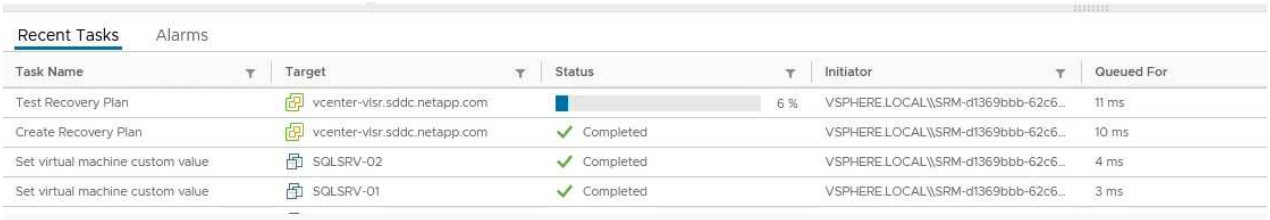
Test del failover con SRM

Il passaggio successivo viene completato nell'interfaccia di Site Recovery.

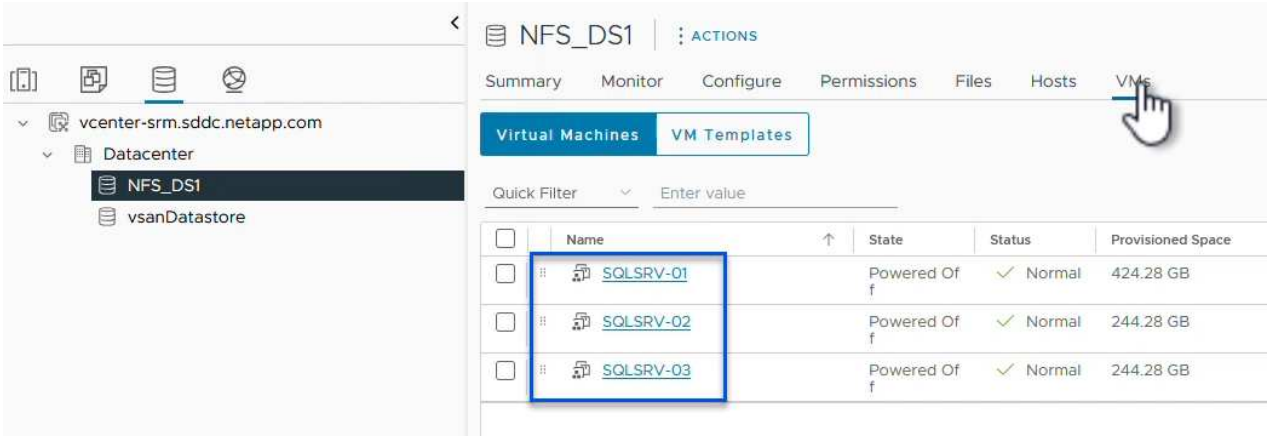
1. Nell'interfaccia di Site Recovery, fare clic sulla scheda **Piano di ripristino** e quindi selezionare un piano di ripristino. Fare clic sul pulsante **Test** per avviare il test del failover sul sito secondario.



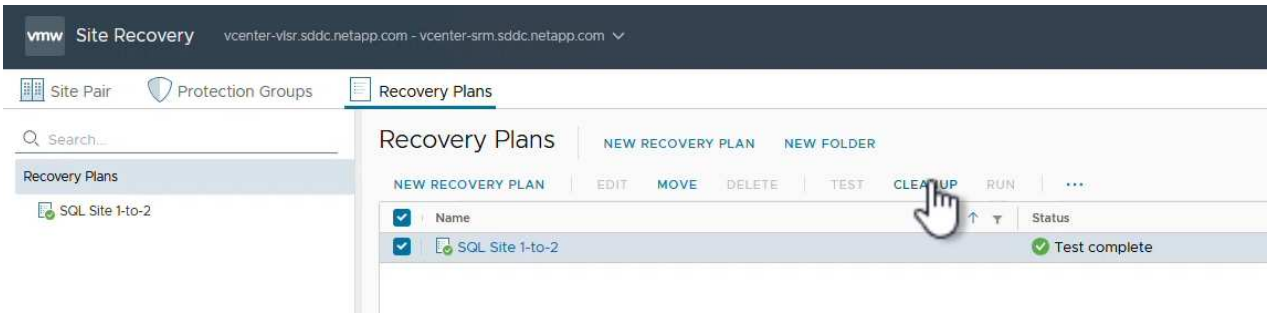
2. È possibile visualizzare l'avanzamento del test sia dal riquadro attività di Site Recovery che dal riquadro attività di vCenter.



3. SRM invia comandi tramite SRA al sistema di archiviazione ONTAP secondario. Un FlexClone dello snapshot più recente viene creato e montato sul cluster vSphere secondario. Il datastore appena montato può essere visualizzato nell'inventario di archiviazione.



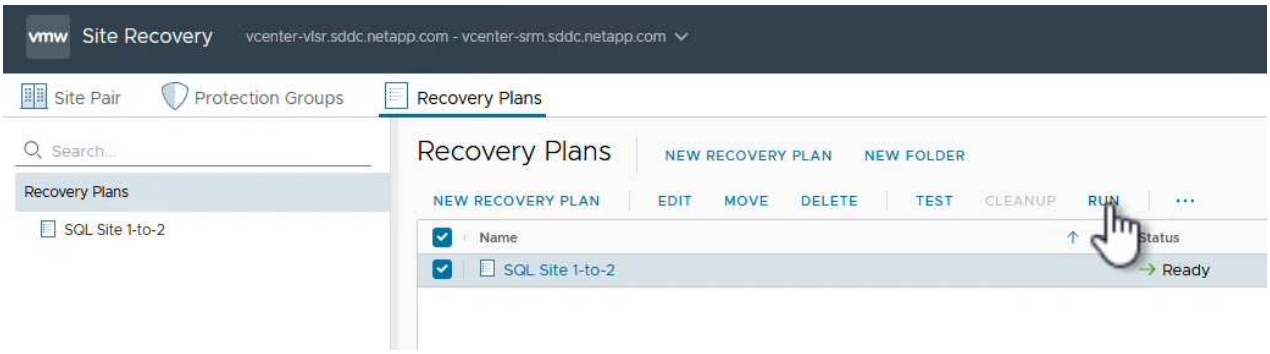
4. Una volta completato il test, fare clic su **Pulizia** per smontare il datastore e tornare all'ambiente originale.



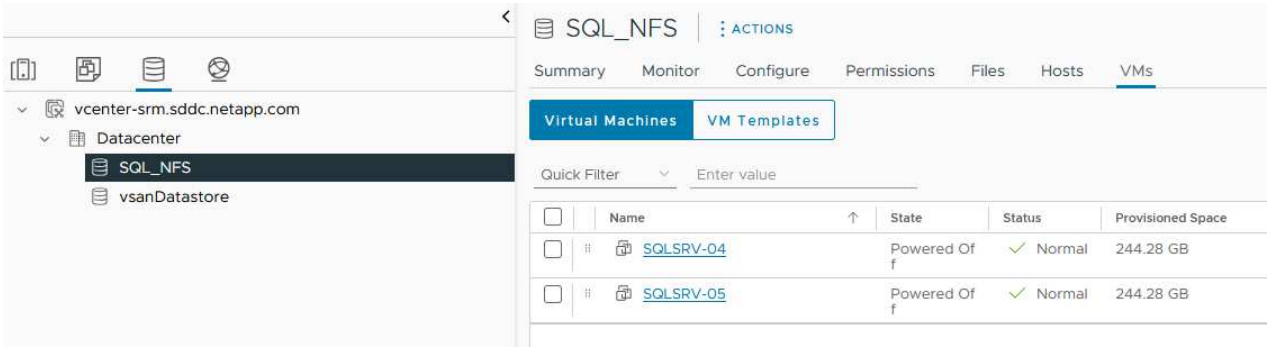
Eseguire il piano di ripristino con SRM

Eseguire un ripristino completo e un failover sul sito secondario.

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



2. Una volta completato il failover, è possibile vedere il datastore montato e le VM registrate nel sito secondario.



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

Riprotezione: 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 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 replicandola in un altro sito. Nei casi in cui il sito di produzione originale rimane funzionante, l'amministratore

VMware può riutilizzarlo come nuovo sito di ripristino, invertendo di fatto la direzione della protezione. È fondamentale sottolineare che la riprotezione è possibile solo in caso di guasti non catastrofici, che richiedono l'eventuale ripristino 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 riporta le operazioni al sito originale. È fondamentale assicurarsi che il sito originale abbia ripreso a funzionare prima di avviare il processo di failback. Per garantire un failback senza intoppi, si consiglia di eseguire un failover di prova dopo aver completato il processo di riprotezione e prima di eseguire il failback finale. Questa pratica serve come 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.

Informazioni aggiuntive

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

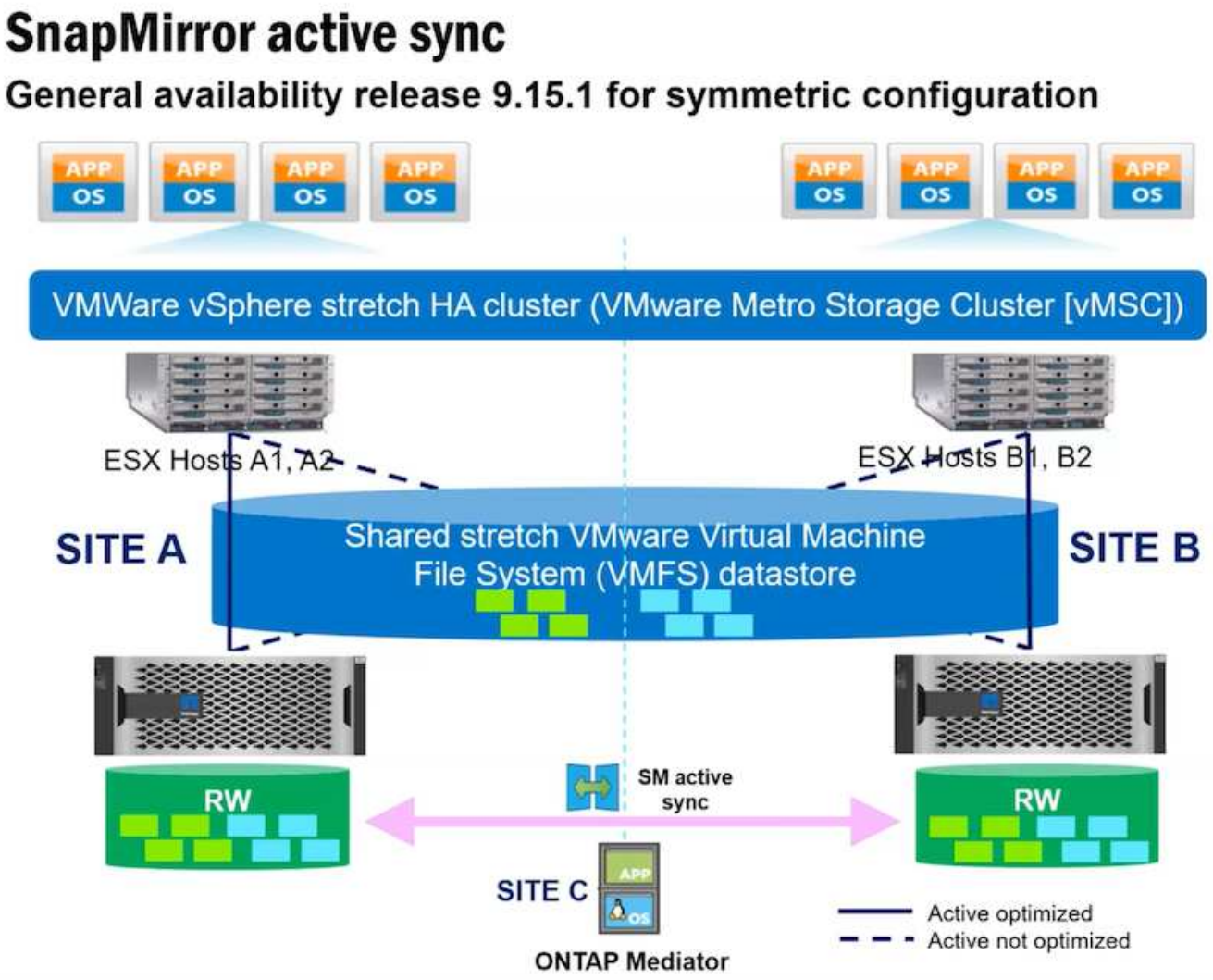
Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a"Documentazione ONTAP 9" centro.

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

Cluster di storage VMware vSphere Metro con sincronizzazione attiva SnapMirror

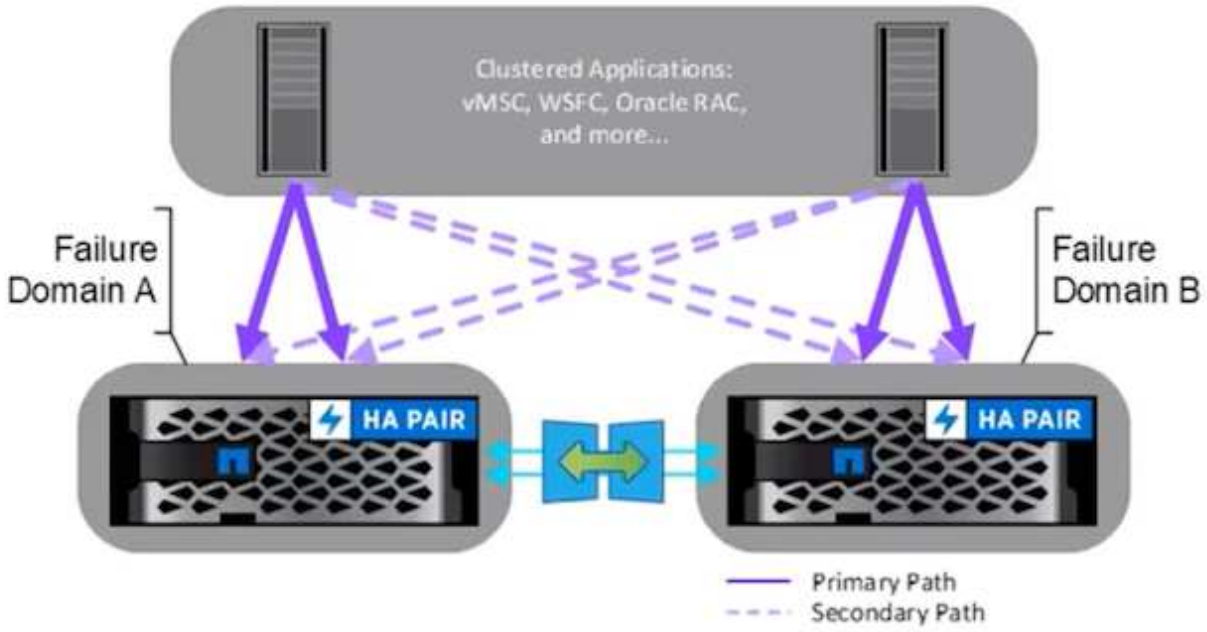
"Cluster di archiviazione metro VMware vSphere (vMSC)"è una soluzione cluster estesa su diversi domini di errore per fornire * mobilità del carico di lavoro tra zone di disponibilità o siti. * prevenzione dei tempi di inattività * prevenzione dei disastri * ripristino rapido

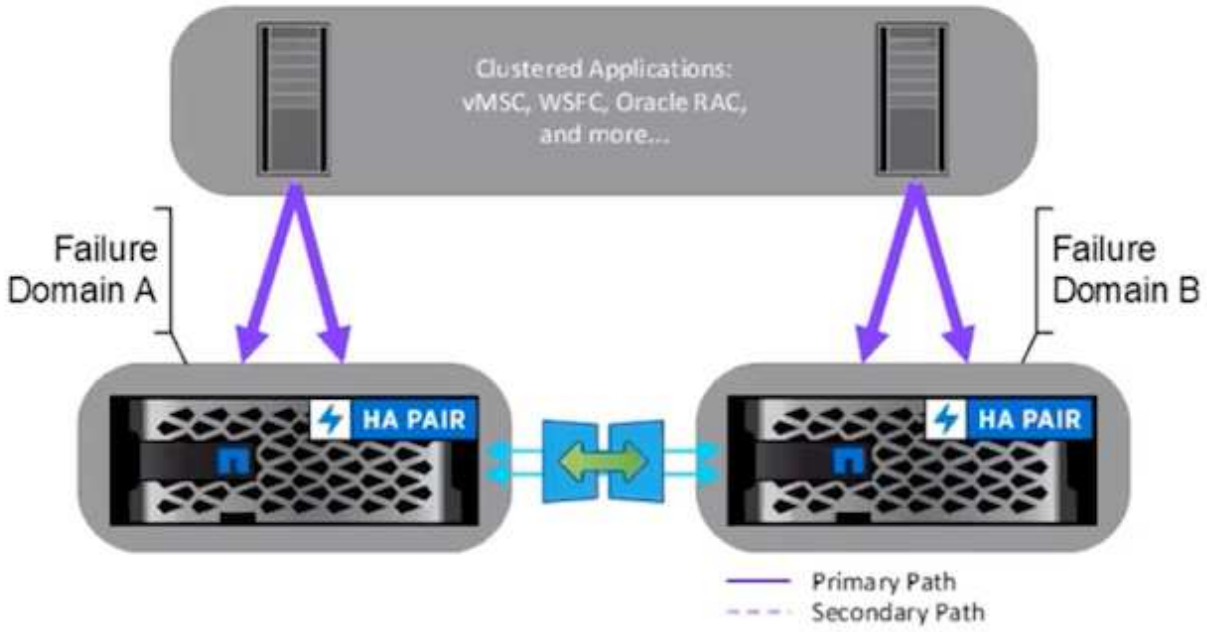
Questo documento fornisce i dettagli di implementazione vMSC con"Sincronizzazione attiva SnapMirror (SM-as)" utilizzando System Manager e ONTAP Tools. Inoltre, mostra come la VM può essere protetta replicandola su un sito terzo e gestita con il plug-in SnapCenter per VMware vSphere.



SnapMirror ActiveSync supporta array di archiviazione ASA, AFF e FAS . Si consiglia di utilizzare lo stesso tipo (modelli di prestazioni/capacità) su entrambi i domini di errore. Attualmente sono supportati solo protocolli a blocchi come FC e iSCSI. Per ulteriori linee guida di supporto, fare riferimento"Strumento di matrice di interoperabilità" E"Hardware Universe"

vMSC supporta due diversi modelli di distribuzione denominati Accesso host uniforme e Accesso host non uniforme. Nella configurazione di accesso host uniforme, ogni host del cluster ha accesso alla LUN su entrambi i domini di errore. Viene solitamente utilizzato 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 solitamente utilizzato in siti diversi in cui il passaggio di più cavi attraverso i domini di guasto rappresenta un'opzione restrittiva.

Nella modalità di accesso host non uniforme, le VM verranno riavviate in un altro dominio di errore da vSphere HA. La disponibilità dell'applicazione sarà influenzata dalla sua progettazione. La modalità di accesso host non uniforme è supportata solo da ONTAP 9.15 in poi.

Prerequisiti

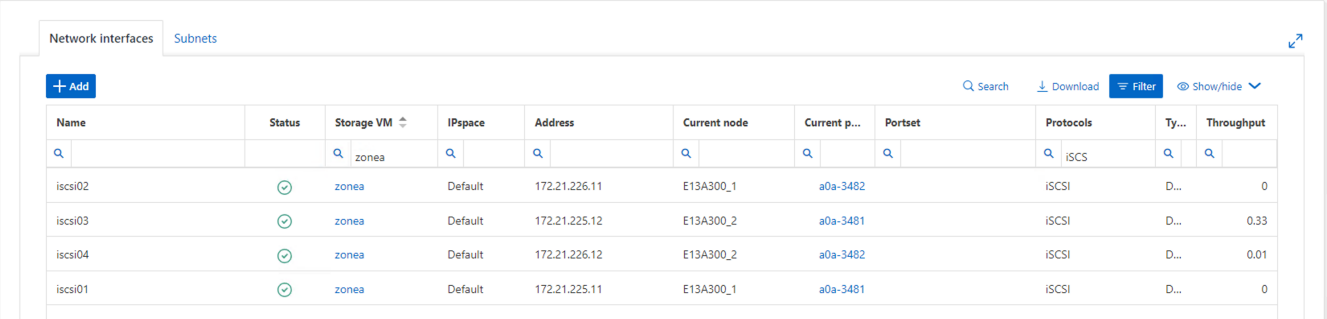
- "Host VMware vSphere distribuiti con doppio storage fabric (due HBA o doppia VLAN per iSCSI) per host" .
- "Gli array di archiviazione vengono distribuiti con aggregazione di link per le porte dati (per iSCSI)" .
- "Sono disponibili VM di archiviazione e LIF"
- "Il tempo di andata e ritorno della latenza inter-cluster deve essere inferiore a 10 millisecondi" .
- "La VM del mediatore ONTAP è distribuita su diversi domini di errore"
- "La relazione Cluster Peer è stabilita"
- "La relazione peer SVM è stabilita"
- "Mediatore ONTAP registrato nel cluster ONTAP"

Se si utilizza un certificato autofirmato, il certificato CA può essere recuperato da <percorso di installazione>/ontap_mediator/server_config/ca.crt sulla VM del mediatore.

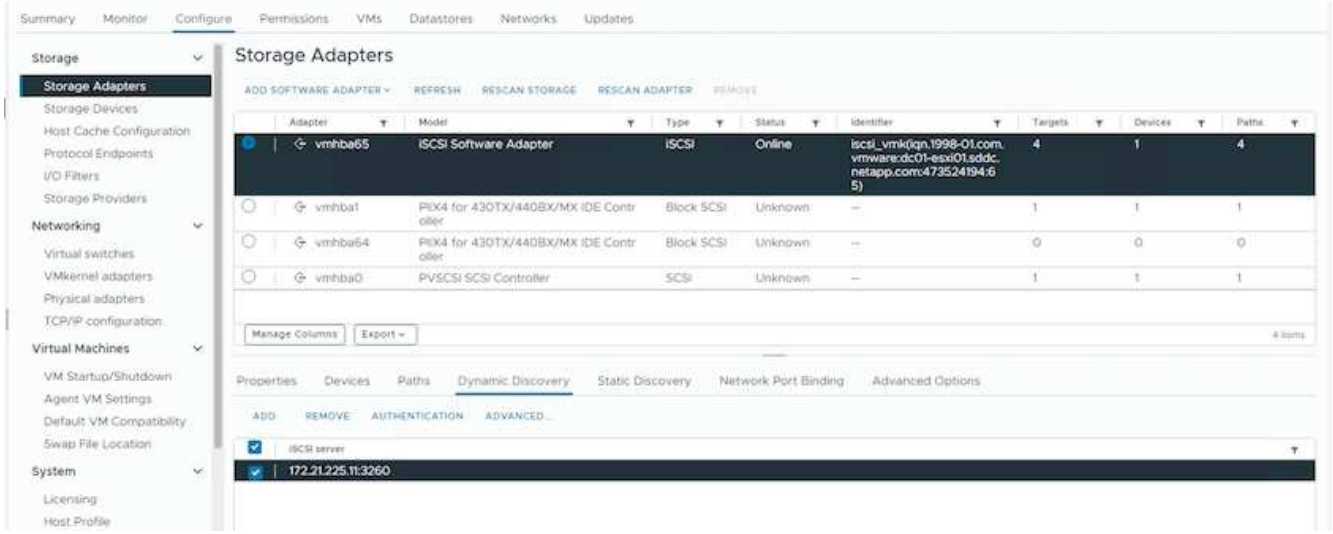
Accesso host non uniforme vMSC con interfaccia utente di ONTAP System Manager.

Nota: è possibile utilizzare ONTAP Tools 10.2 o versioni successive per predisporre un datastore esteso con modalità di accesso host non uniforme senza dover cambiare più interfacce utente. Questa sezione è solo di riferimento se non si utilizza ONTAP Tools.

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



2. Sull'adattatore di archiviazione iSCSI dell'host vSphere, aggiungere l'IP iSCSI nella scheda Rilevamento dinamico.

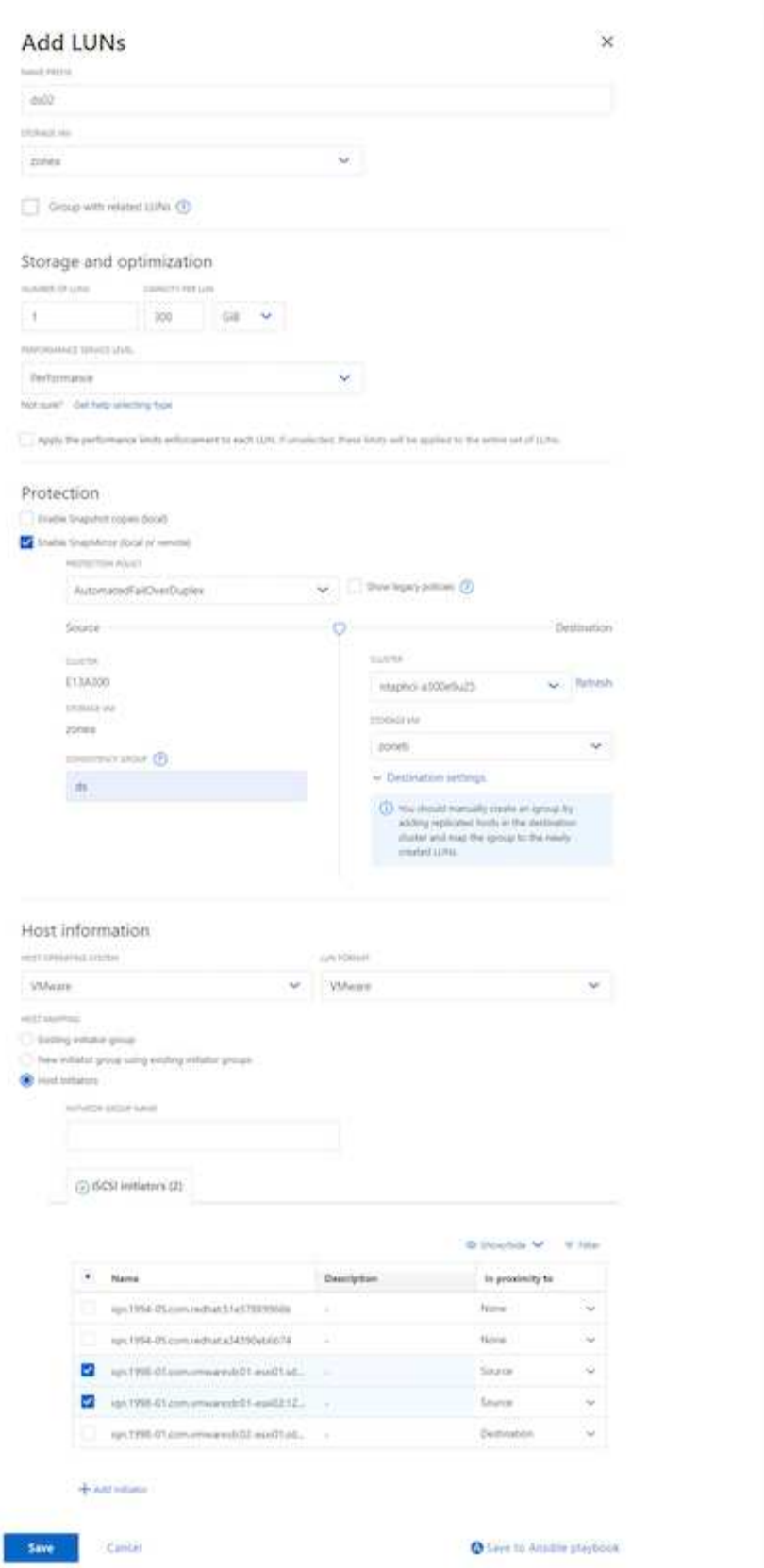


Per la modalità di accesso uniforme, è necessario fornire l'indirizzo lif dei dati iSCSI del dominio di errore di origine e di destinazione.

3. Ripetere il passaggio precedente sugli host vSphere per l'altro dominio di errore aggiungendo il suo IP di vita dei dati iSCSI locale nella scheda Dynamic Discovery.
4. Con una connettività di rete adeguata, dovrebbero esistere quattro connessioni iSCSI per ogni host vSphere dotato di due schede di rete iSCSI VMKernel e due porte dati iSCSI per ogni controller di storage.

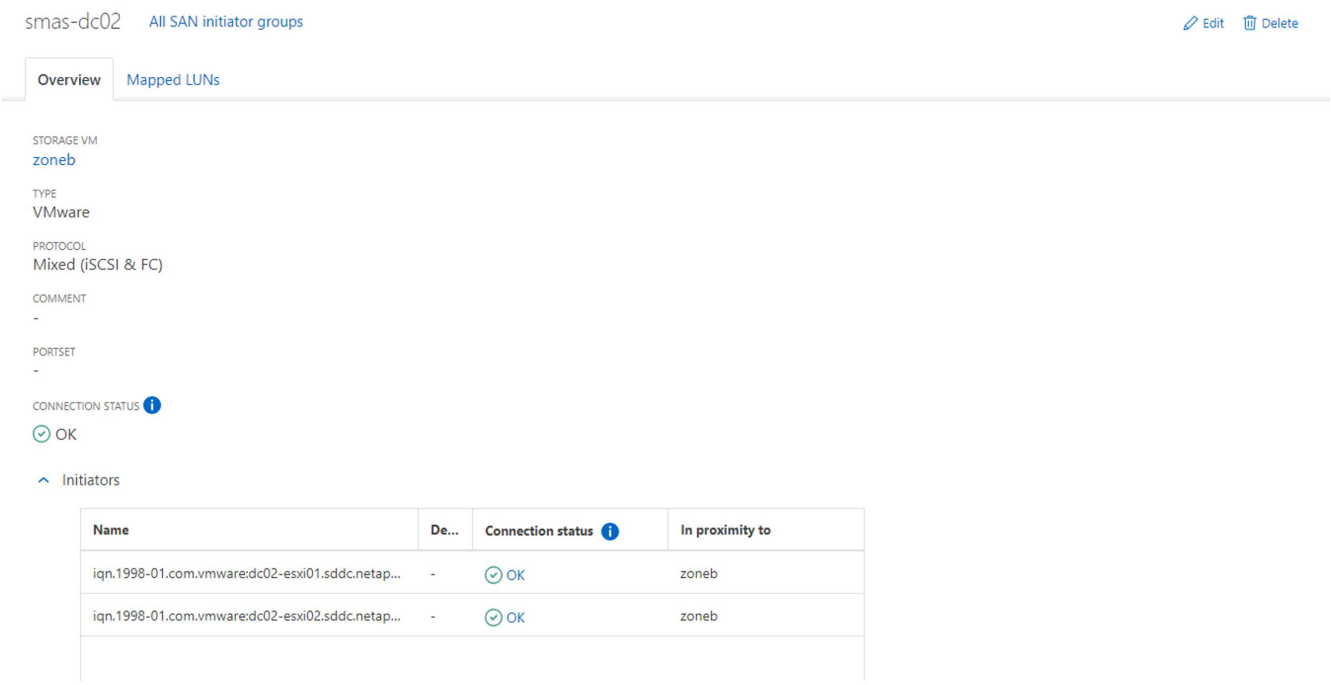
```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
            Tpgroup             Conn  Local           Remote          TCP Recv
Vserver     Name          TSIH  ID    Address         Address         Size
----------- ------------- ----- ----- --------------- --------------- --------
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 utilizzando ONTAP System Manager, configurare SnapMirror con la policy di replica AutomatedFailOverDuplex, selezionare gli iniziatori host e impostare la prossimità



dell'host.

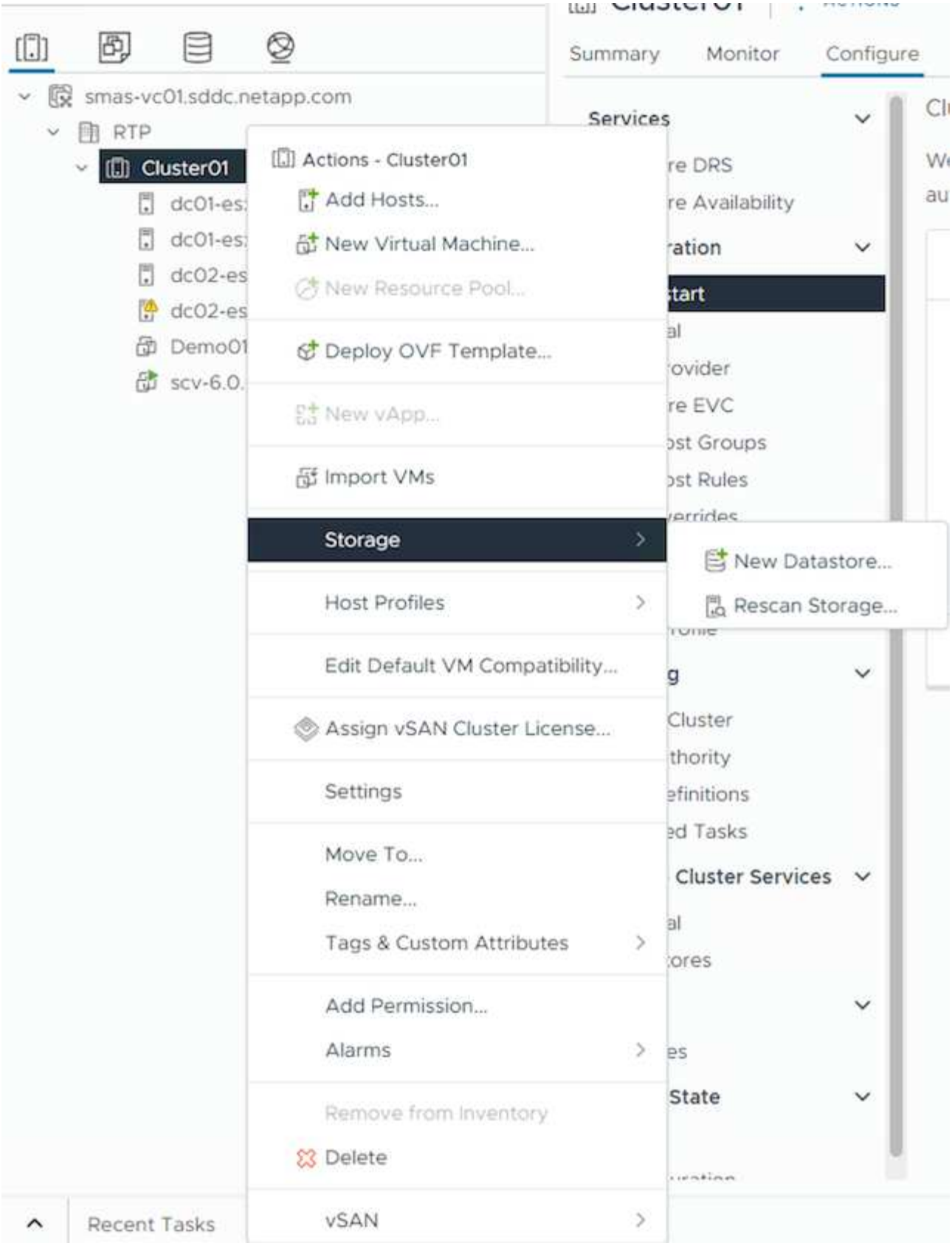
6. Su un altro array di storage del dominio di errore, creare il gruppo di iniziatori SAN con i suoi iniziatori host vSphere e impostare la prossimità
dell'host.



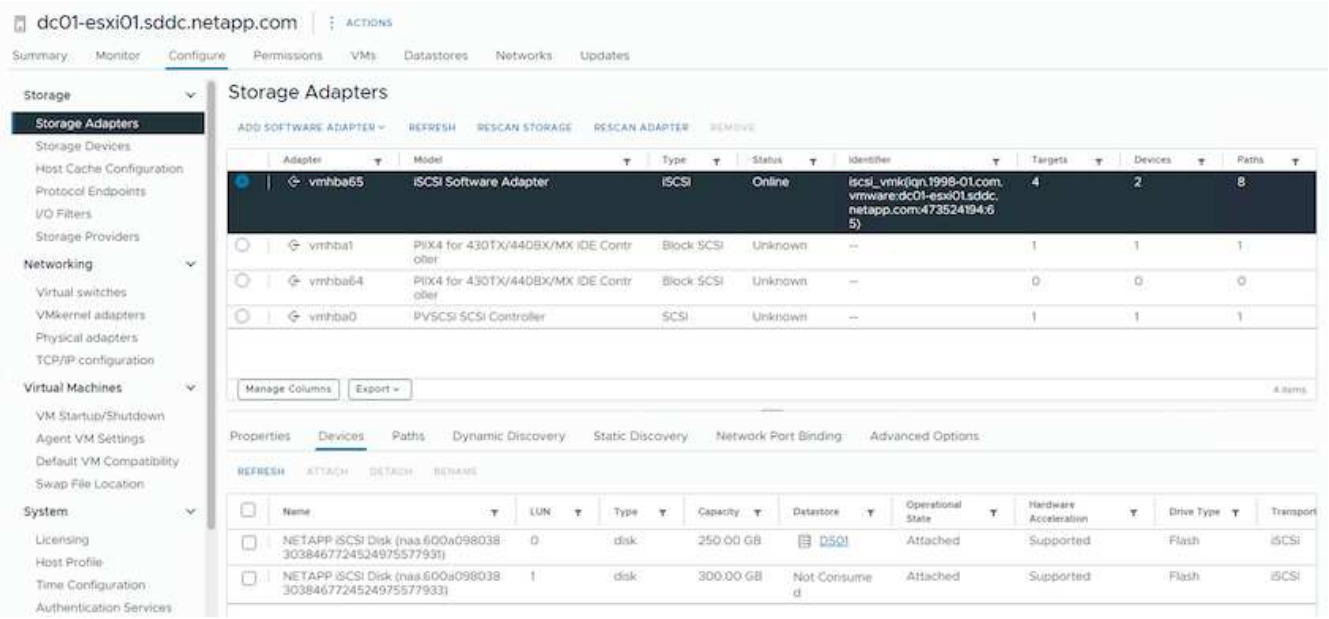
Per la modalità di accesso uniforme, l'igroup può essere replicato dal dominio di errore di origine.

7. Mappare la LUN replicata con lo stesso ID di mappatura del dominio di errore di origine.

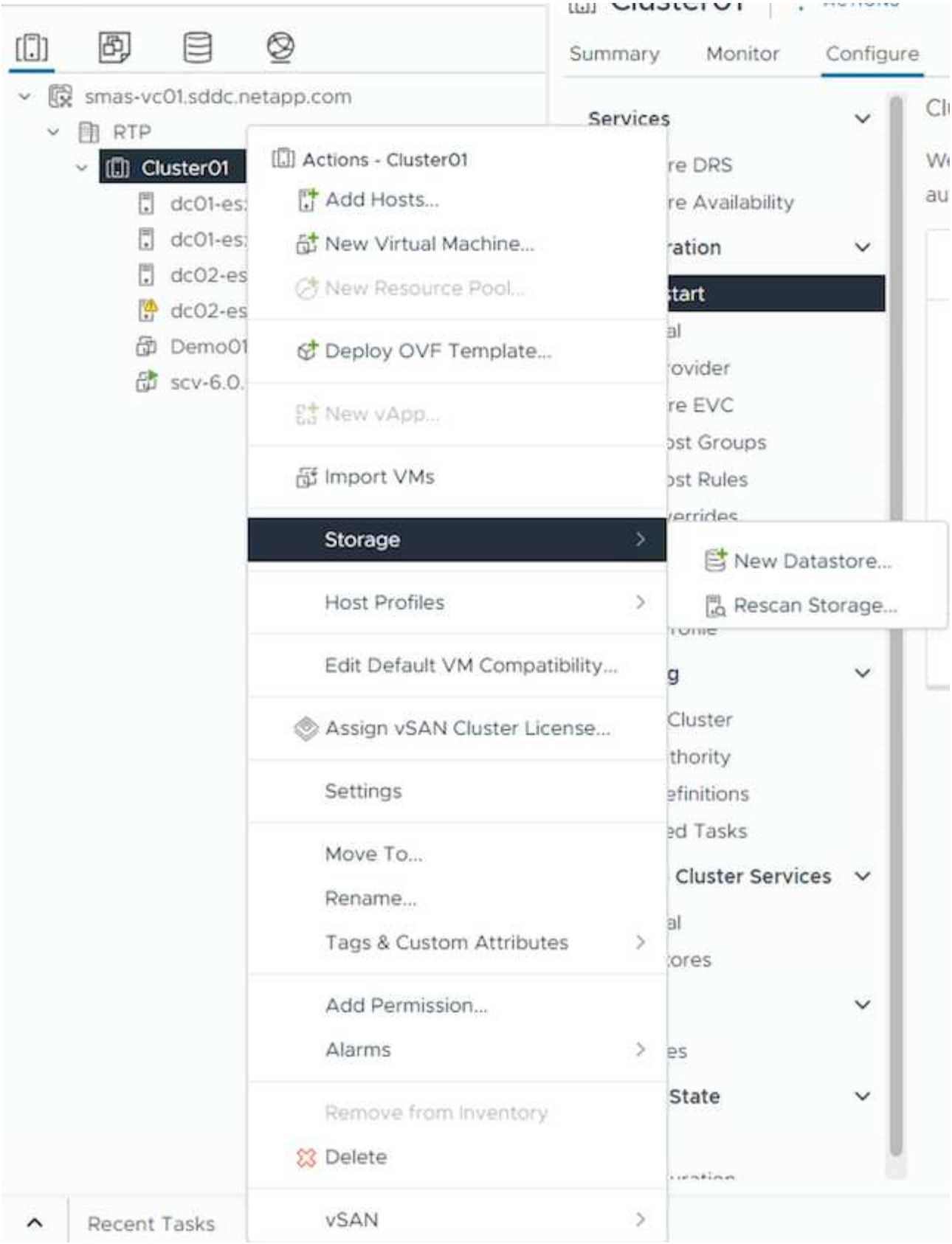
8. Su vCenter, fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Ripeti scansione
storage.



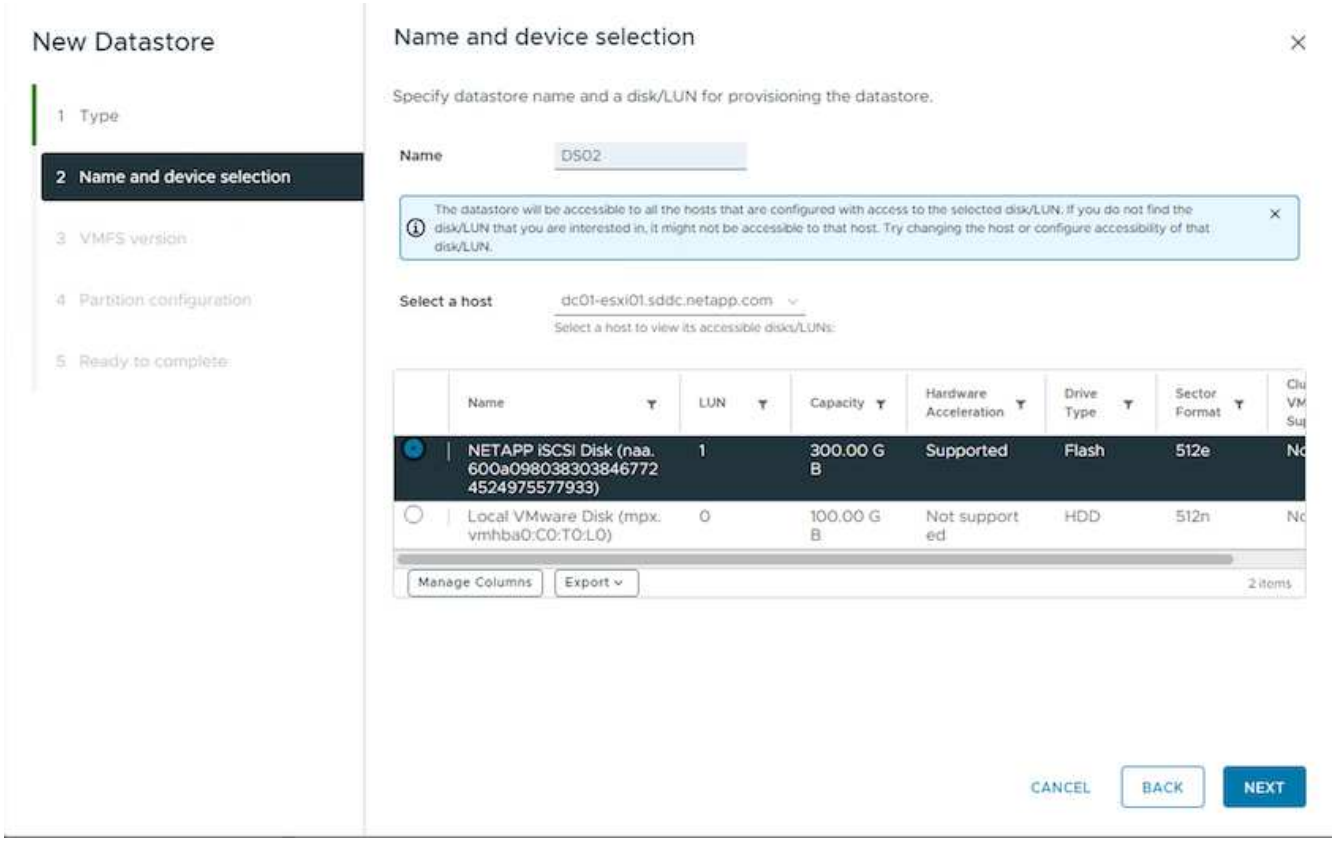
9. Su uno degli host vSphere nel cluster, verificare che il dispositivo appena creato venga visualizzato con il datastore che indica Non
consumato.



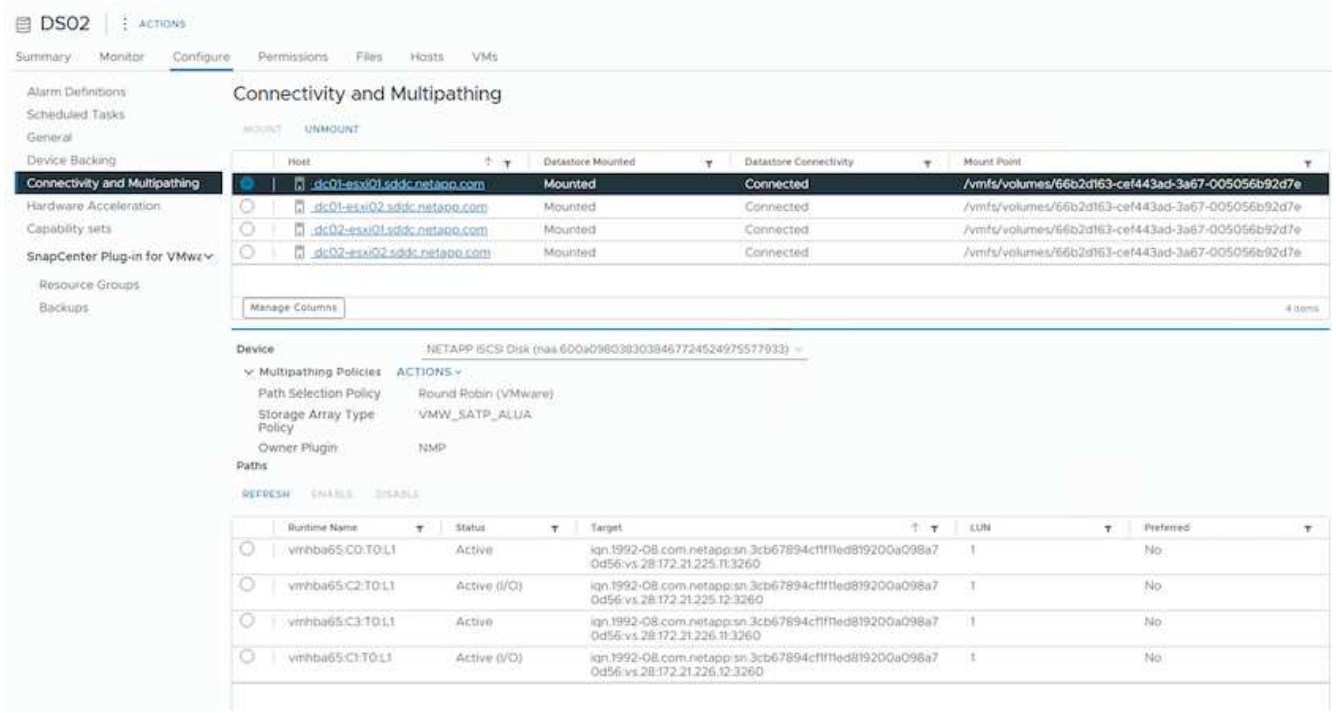
10. Su vCenter, fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Nuovo datastore.

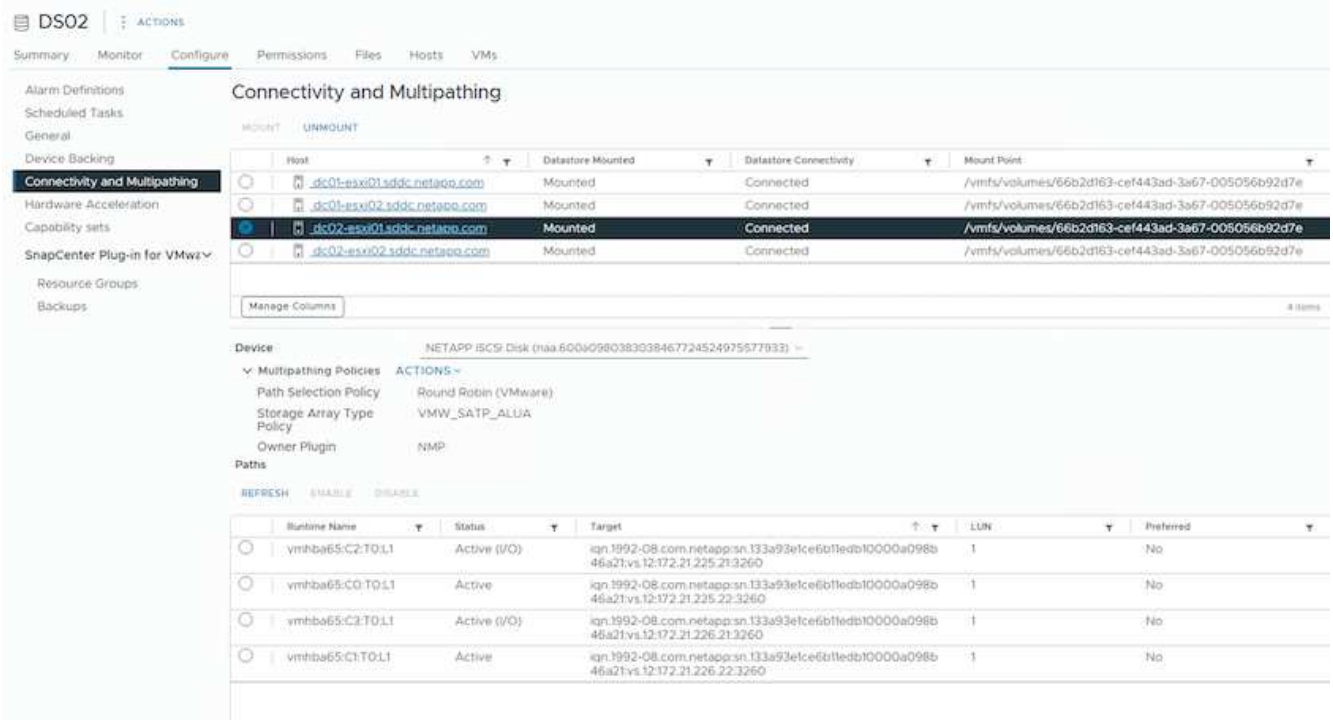


11. Nella procedura guidata, ricordarsi di fornire il nome del datastore e di selezionare il dispositivo con la capacità e l'ID dispositivo
corretti.



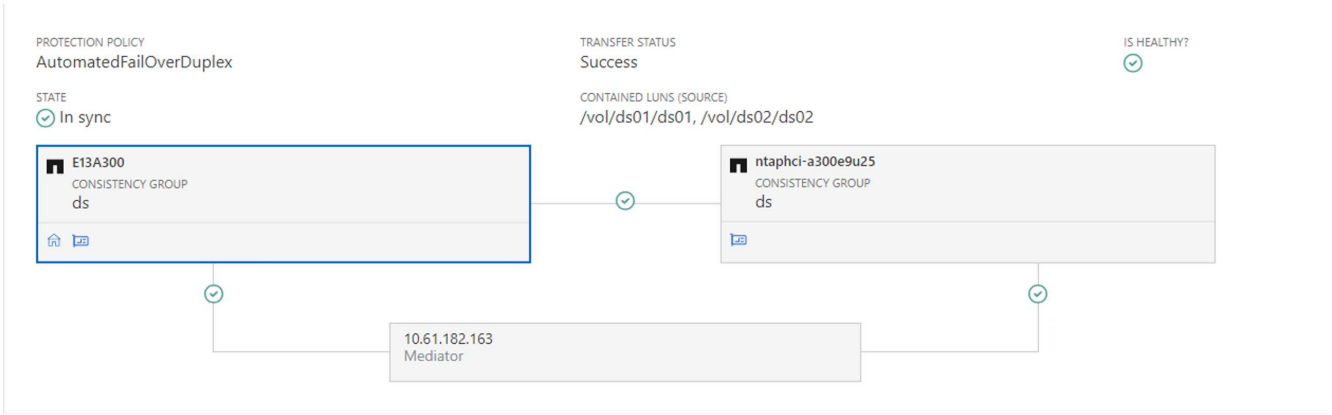
12. Verificare che il datastore sia montato su tutti gli host del cluster in entrambi i domini di errore.





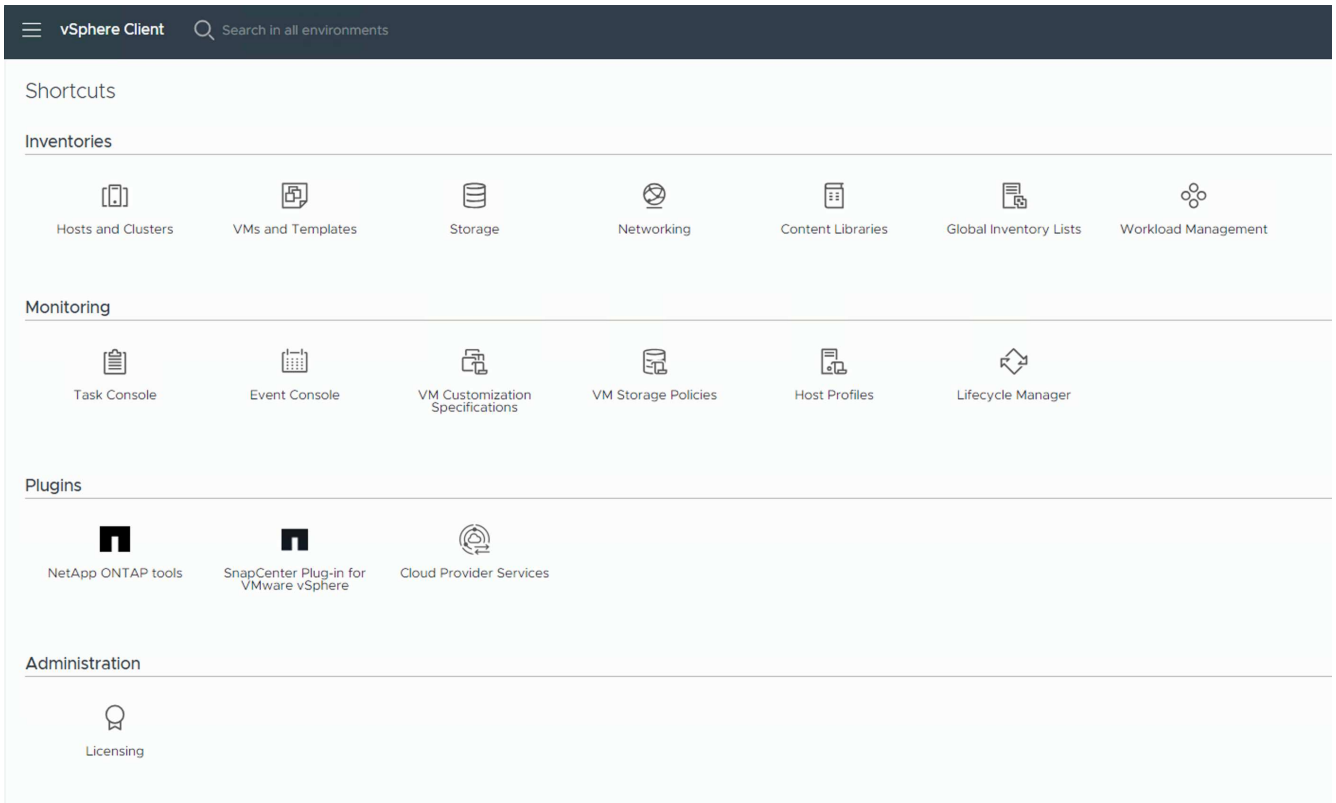
Gli screenshot sopra mostrano l'I/O attivo su un singolo controller poiché abbiamo utilizzato AFF. Per ASA, avrà Active IO su tutti i percorsi.

13. Quando si aggiungono altri datastore, è necessario ricordarsi di espandere il Consistency Group esistente per renderlo coerente in tutto il cluster vSphere.



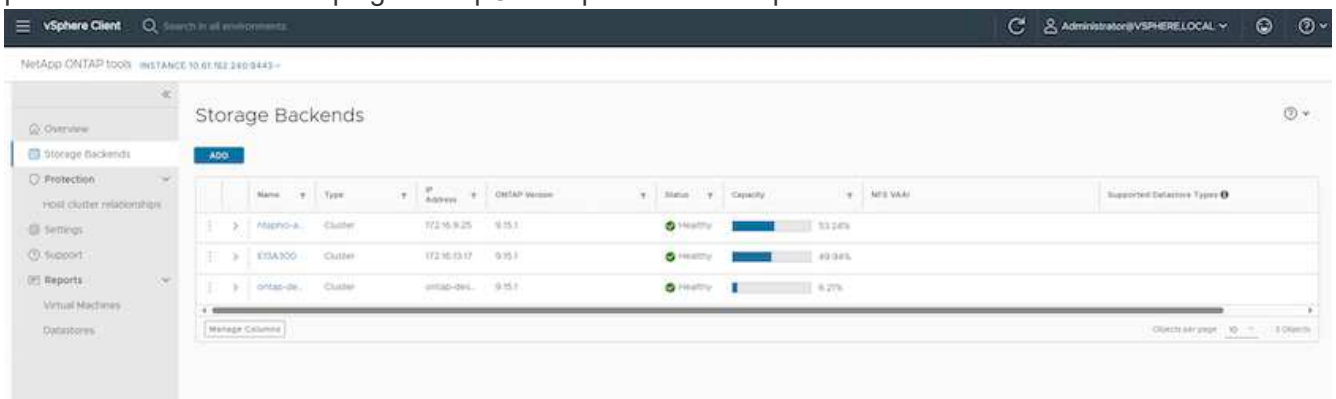
Modalità di accesso host uniforme vMSC con strumenti ONTAP .

1. Assicurarsi che NetApp ONTAP Tools sia distribuito e registrato su vCenter.



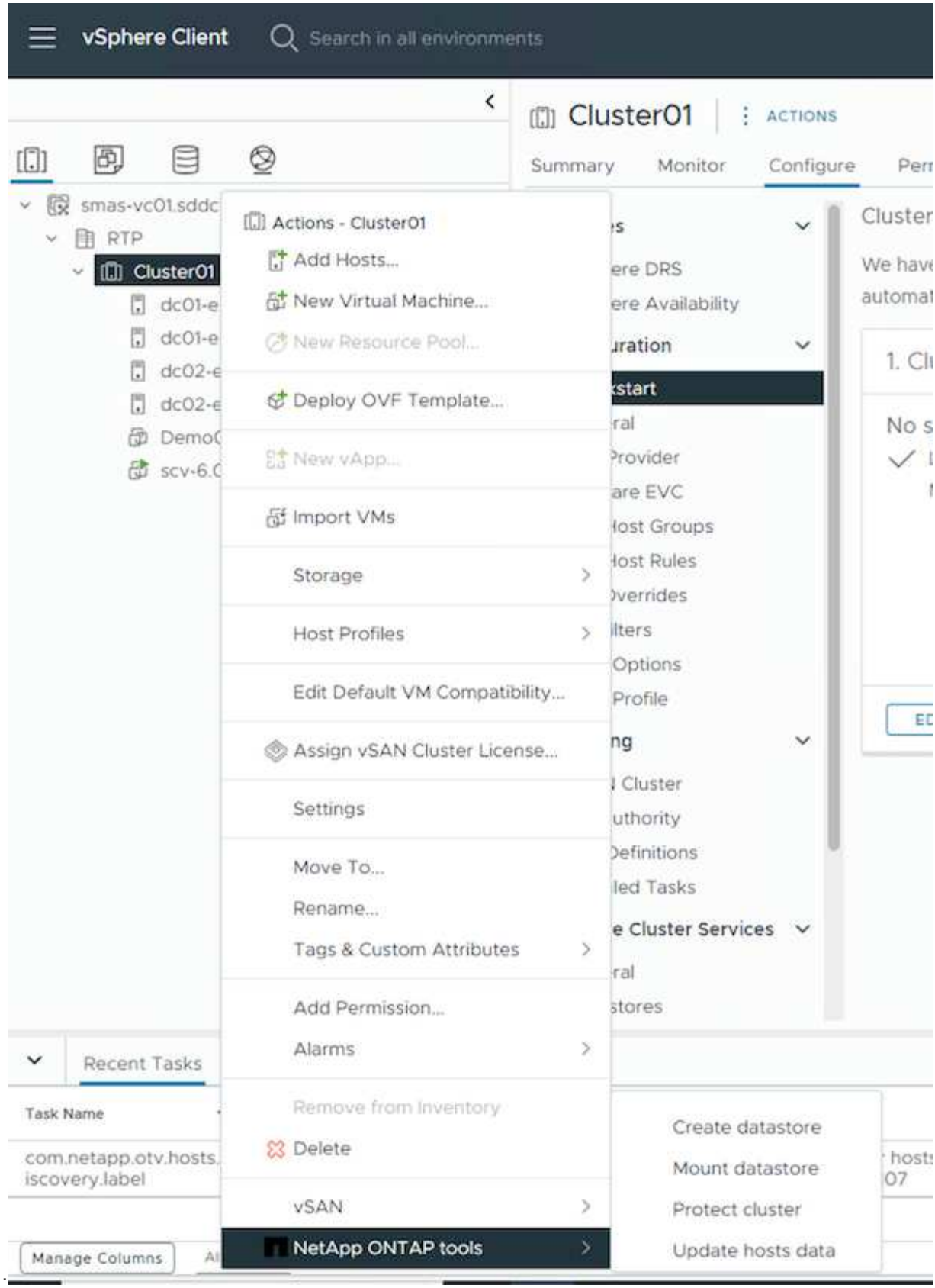
In caso contrario, seguire"Distribuzione degli strumenti ONTAP" E"Aggiungi un'istanza del server vCenter"

2. Assicurarsi che i sistemi di archiviazione ONTAP siano registrati su ONTAP Tools. Ciò include sia i sistemi di archiviazione del dominio di errore sia un terzo per la replica remota asincrona da utilizzare per la protezione delle VM con il plug-in SnapCenter per VMware vSphere.

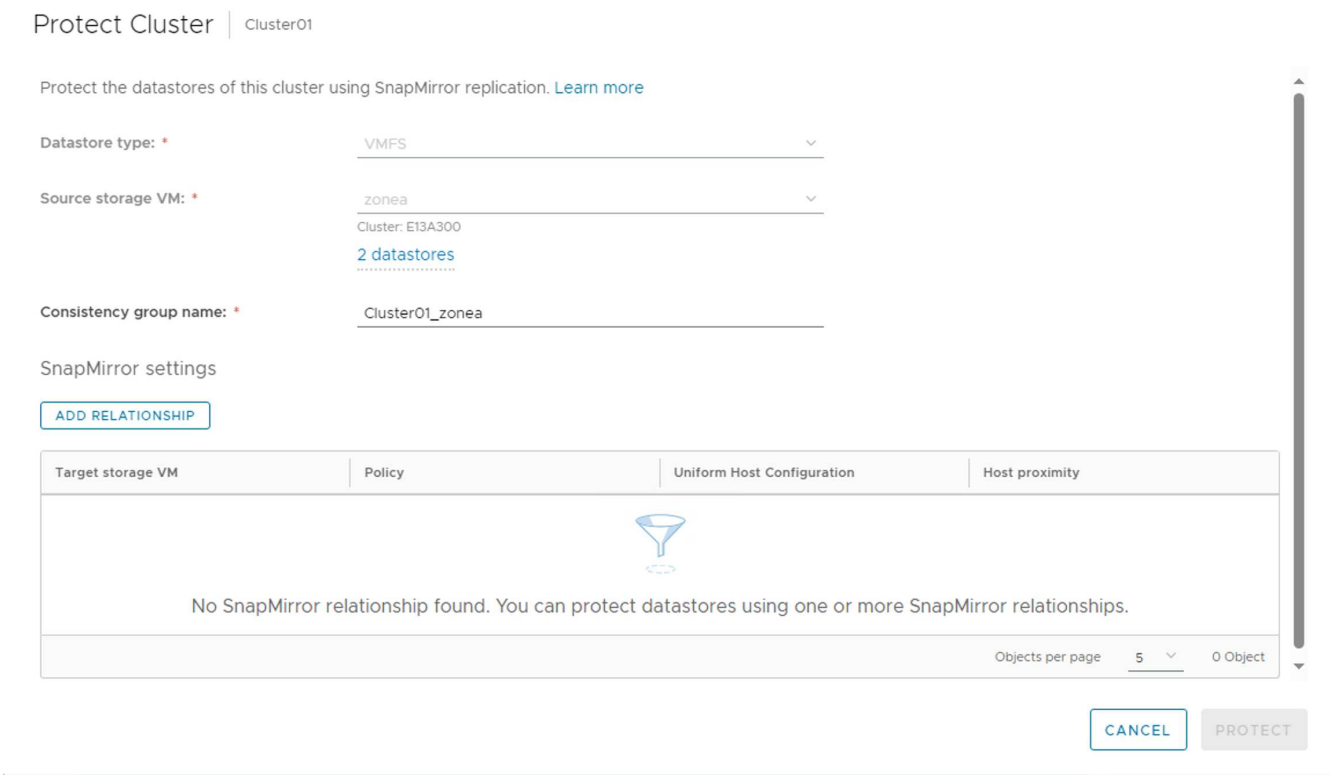


In caso contrario, seguire"Aggiungere backend di archiviazione utilizzando l'interfaccia utente del client vSphere"

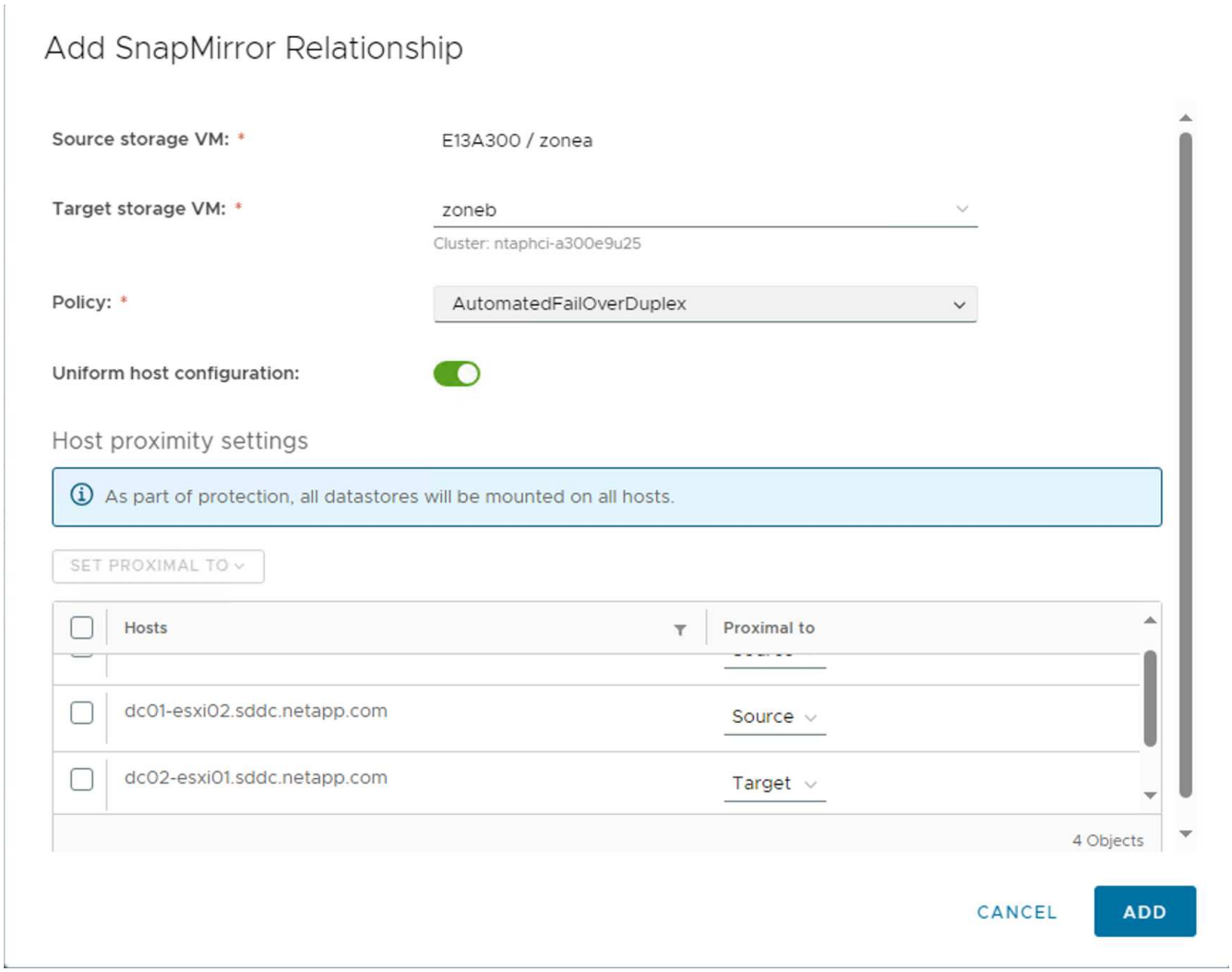
3. Aggiorna i dati degli host per sincronizzarli con ONTAP Tools e poi,"creare un archivio dati"



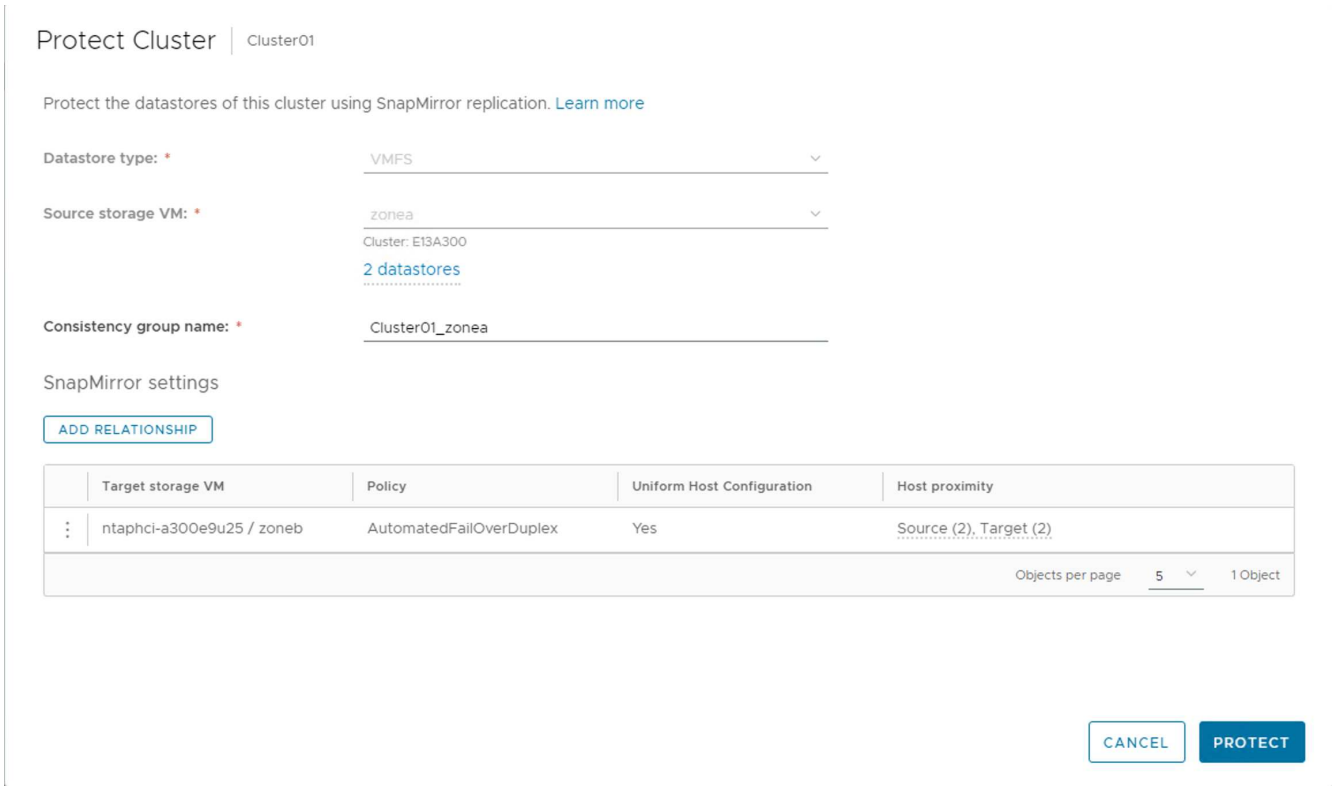
4. Per abilitare SM-as, fare clic con il pulsante destro del mouse sul cluster vSphere e selezionare Proteggi cluster su NetApp ONTAP Tools (fare riferimento allo screenshot sopra)
5. Verranno visualizzati gli archivi dati esistenti per quel cluster insieme ai dettagli SVM. Il nome CG predefinito è <nome cluster vSphere>_<nome SVM>. Fare clic sul pulsante Aggiungi relazione.



6. Selezionare l'SVM di destinazione e impostare il criterio su AutomatedFailOverDuplex per SM-as. È presente un interruttore a levetta per la configurazione host uniforme. Imposta la prossimità per ciascun host.

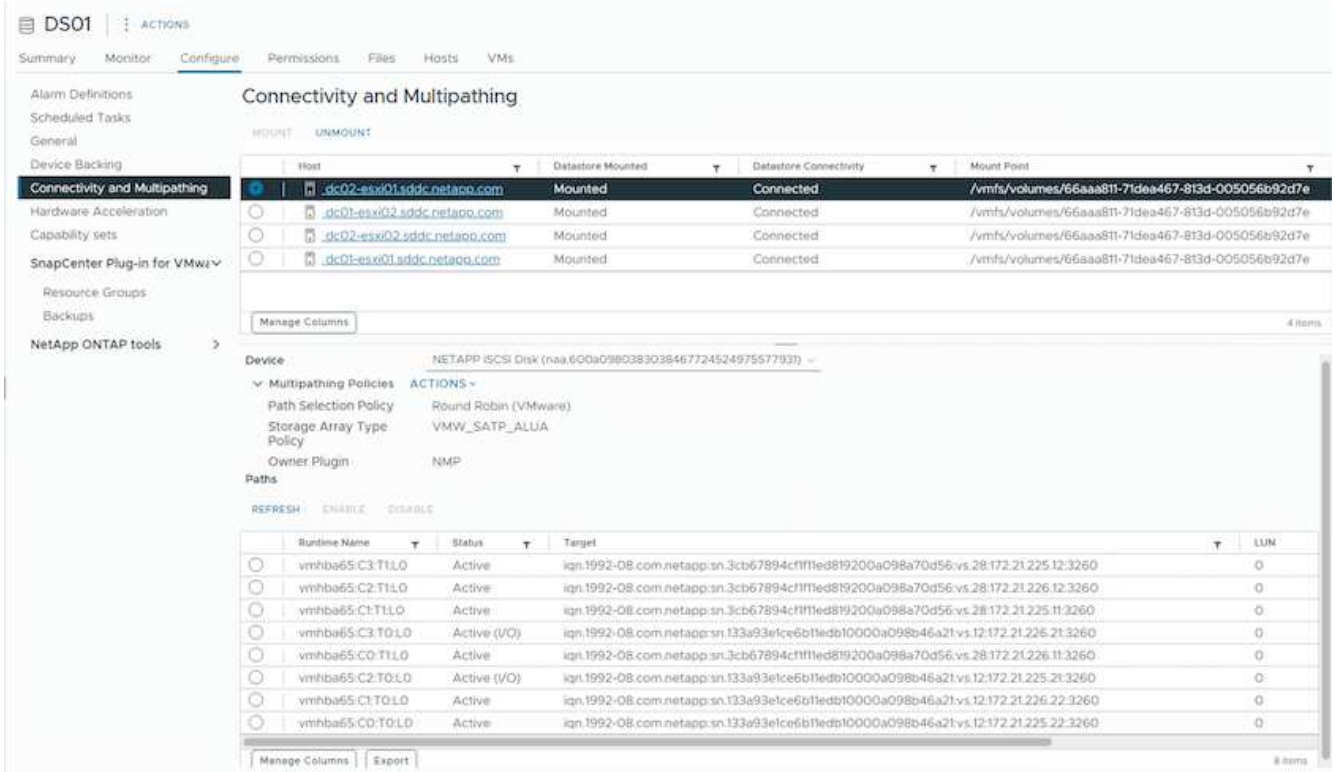


7. Verificare le informazioni sulla protezione dell'host e altri dettagli. Se necessario, aggiungere un'altra relazione al terzo sito con criterio di replicazione asincrono. Quindi, fare clic su Proteggi.



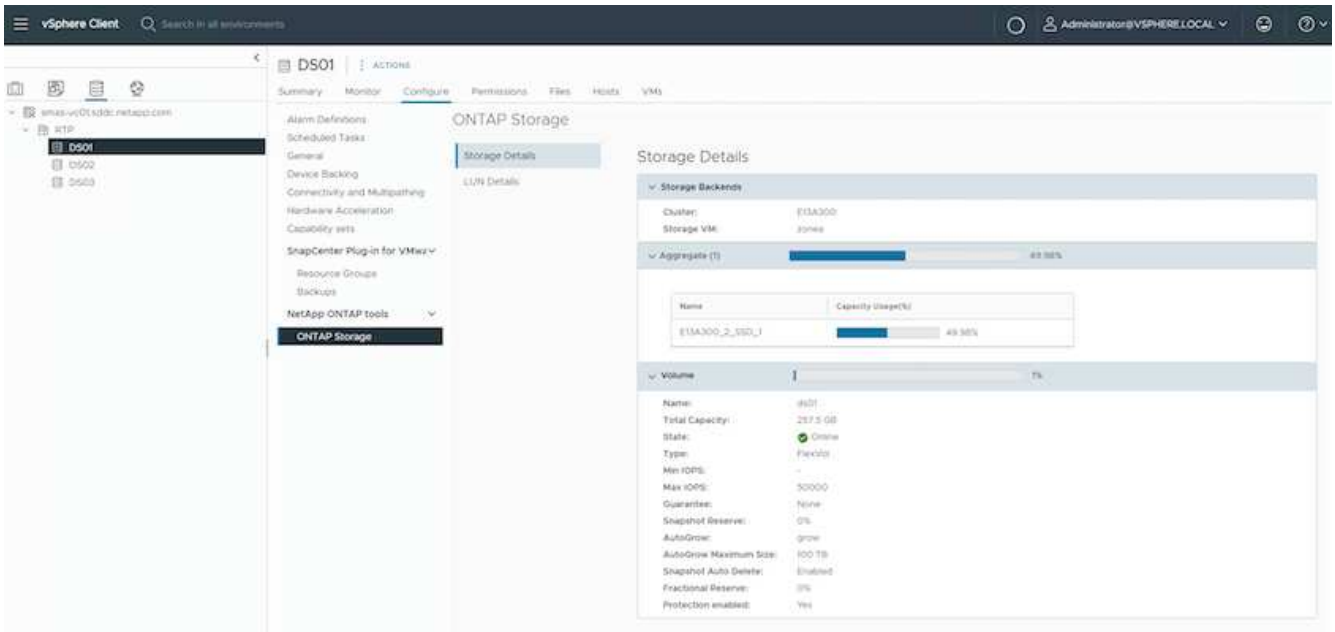
NOTA: se si prevede di utilizzare il SnapCenter Plug-in for VMware vSphere 6.0, la replica deve essere configurata a livello di volume anziché a livello di gruppo di coerenza.

8. Con l'accesso host uniforme, l'host dispone di una connessione iSCSI a entrambi gli array di archiviazione del dominio di errore.

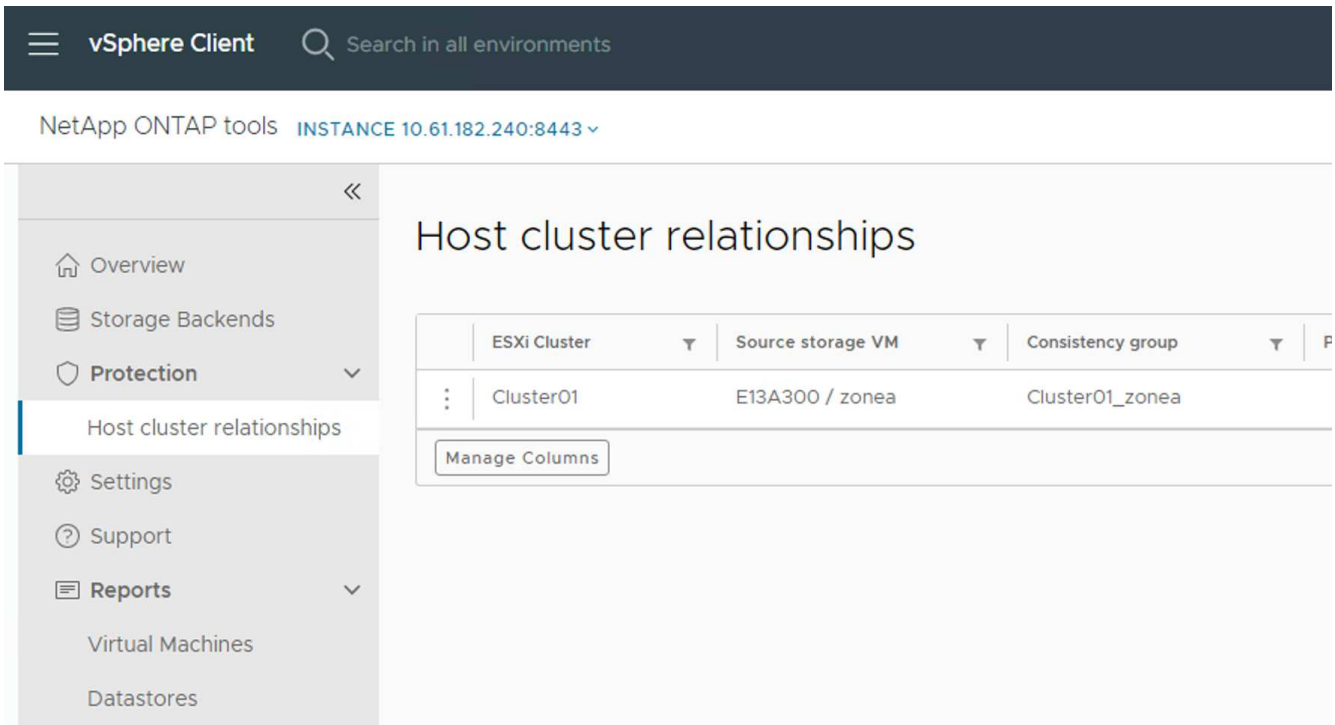


NOTA: lo screenshot qui sopra è di AFF. Se ASA, l'I/O ATTIVO dovrebbe essere presente in tutti i percorsi con connessioni di rete appropriate.

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

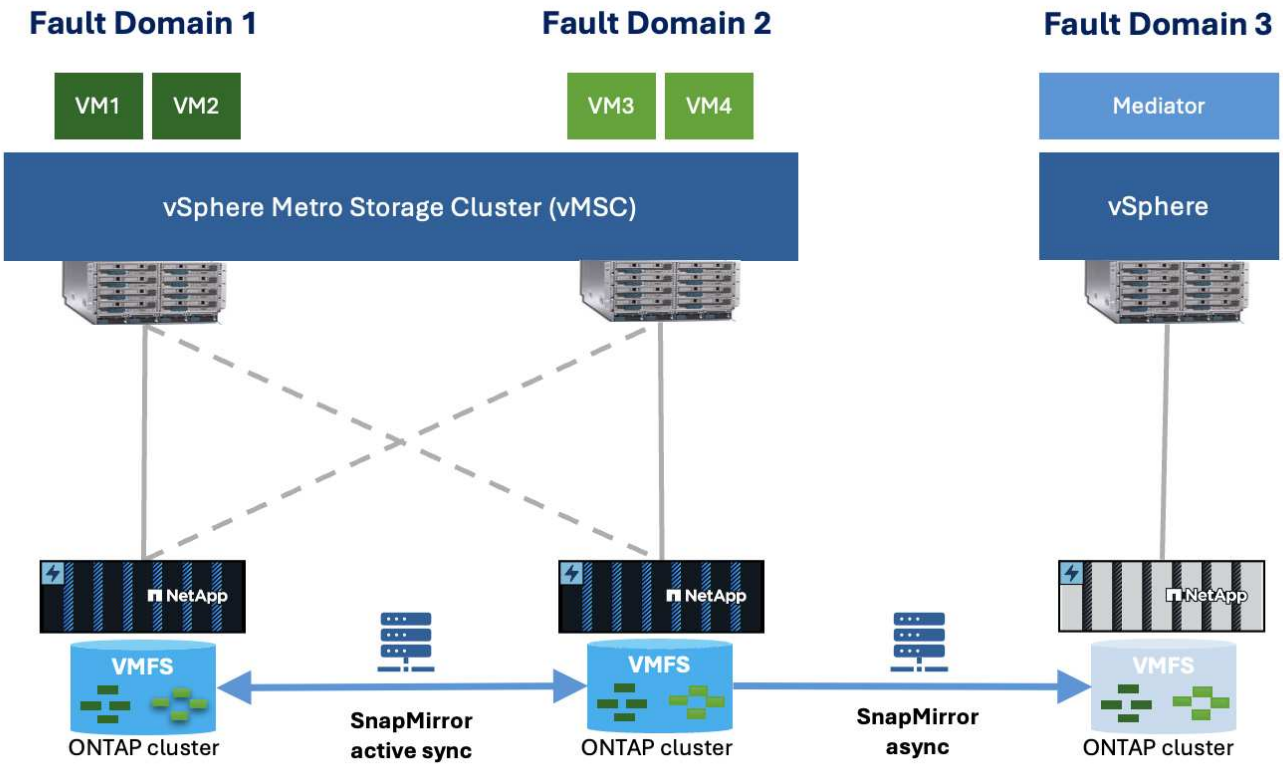


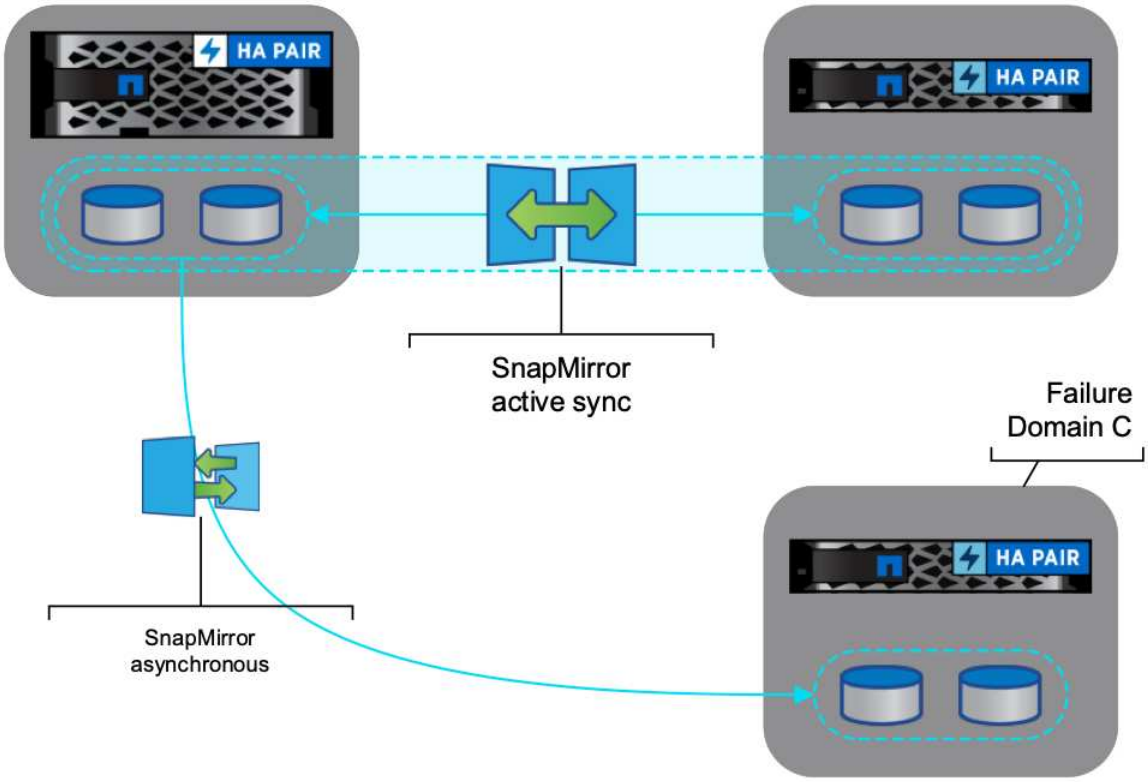
10. Per maggiori dettagli e per aggiornare le informazioni sulla prossimità dell'host, è possibile utilizzare l'opzione Relazioni cluster host negli Strumenti ONTAP
.

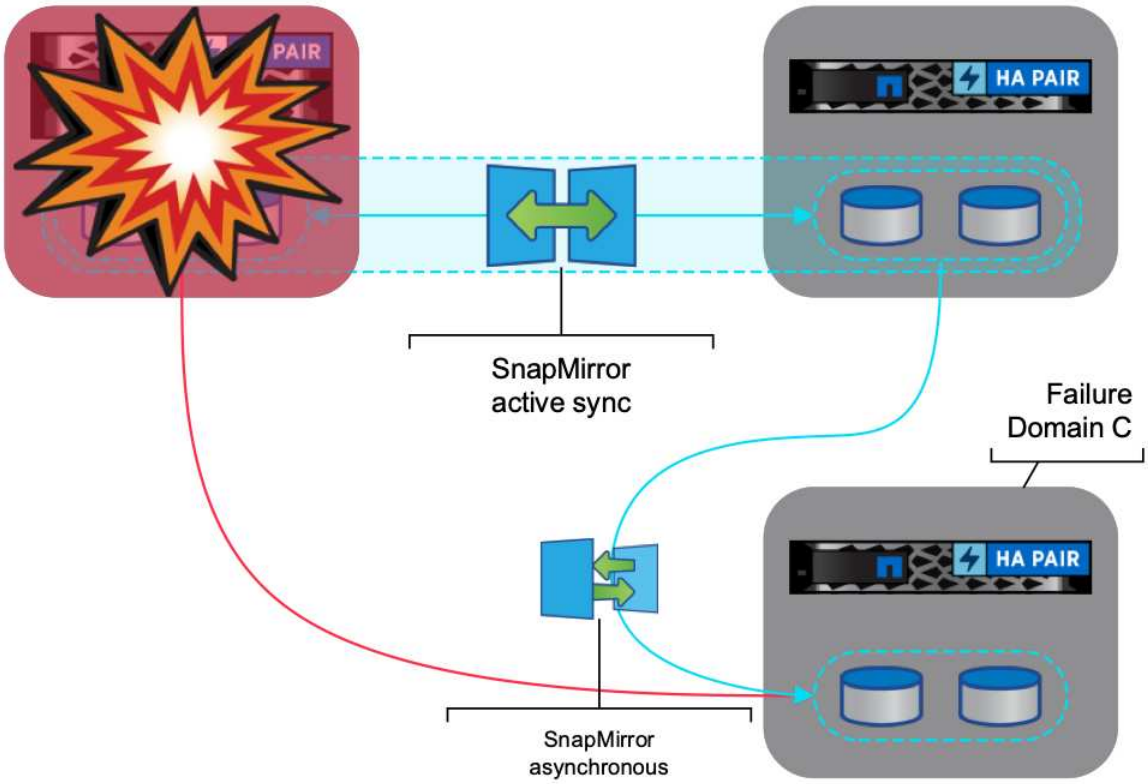


Protezione delle VM con il plug-in SnapCenter per VMware vSphere.

Il SnapCenter Plug-in for VMware vSphere (SCV) 6.0 o versioni successive supporta SnapMirror ActiveSync e, in combinazione con SnapMirror Async, consente la replica su un terzo dominio di errore.

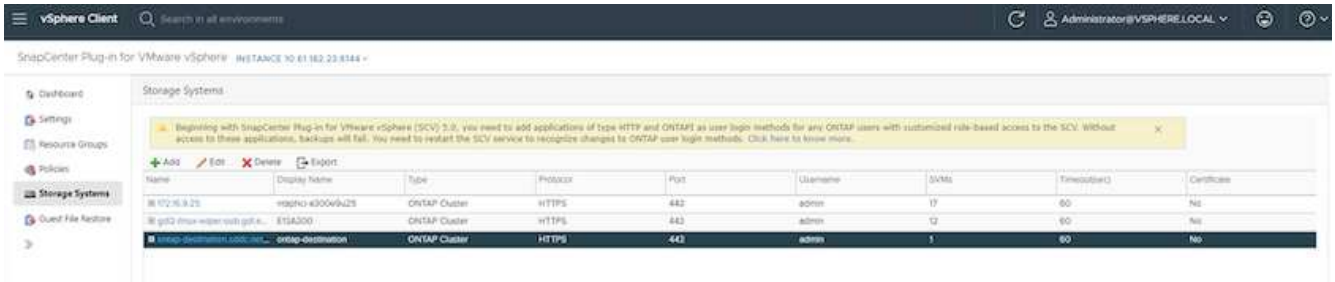

Fault Domain 1
Fault Domain 2
Fault Domain 3
VM1
VM2
VM3
VM4
Mediator
vSphere Metro Storage Cluster (vMSC)
vSphere
NetApp
NetApp
NetApp
VMFS
VMFS
VMFS
ONTAP cluster
SnapMirror
active sync
ONTAP cluster
SnapMirror
async
ONTAP cluster


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

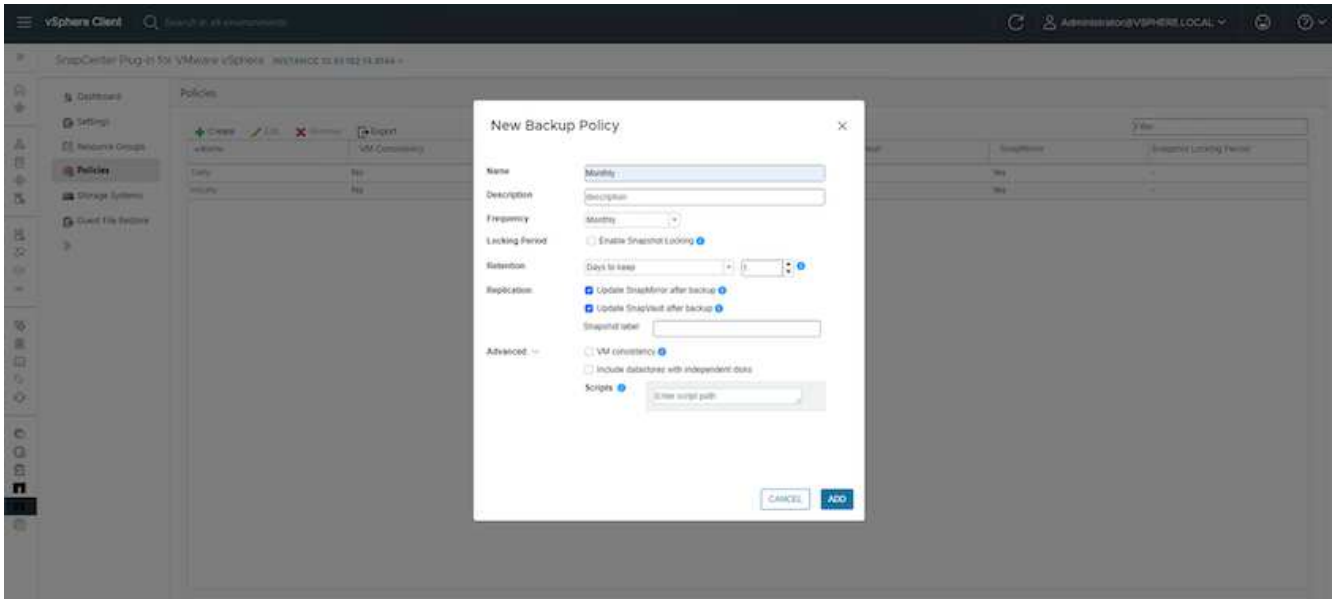

PAIR
HA PAIR
SnapMirror
active sync
Failure
Domain C
HA PAIR
SnapMirror
asynchronous

I casi d'uso supportati includono: * Backup e ripristino della VM o del Datastore da uno qualsiasi dei domini di errore con SnapMirror ActiveSync. * Ripristinare le risorse dal terzo dominio di errore.

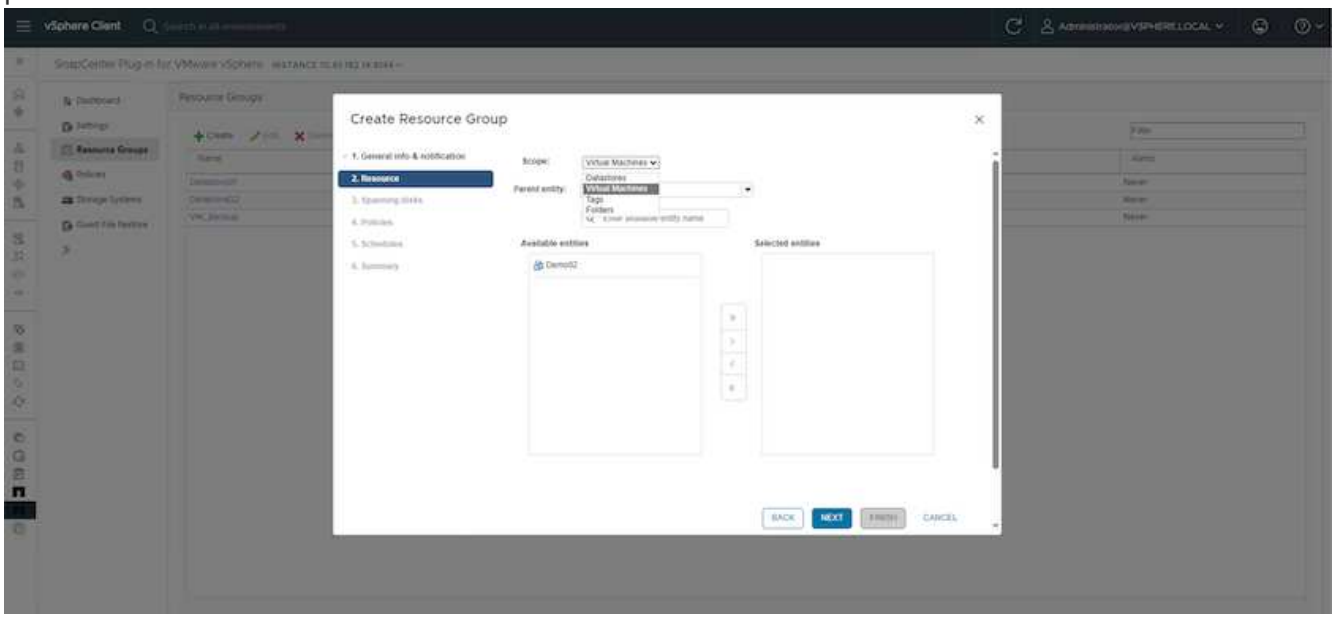
1. Aggiungere tutti i sistemi di archiviazione ONTAP che si prevede di utilizzare in SCV.



2. Crea politica. Assicurarsi che Aggiorna SnapMirror dopo il backup sia selezionato per SM-as e anche Aggiorna SnapVault dopo il backup per la replica asincrona sul terzo dominio di errore.

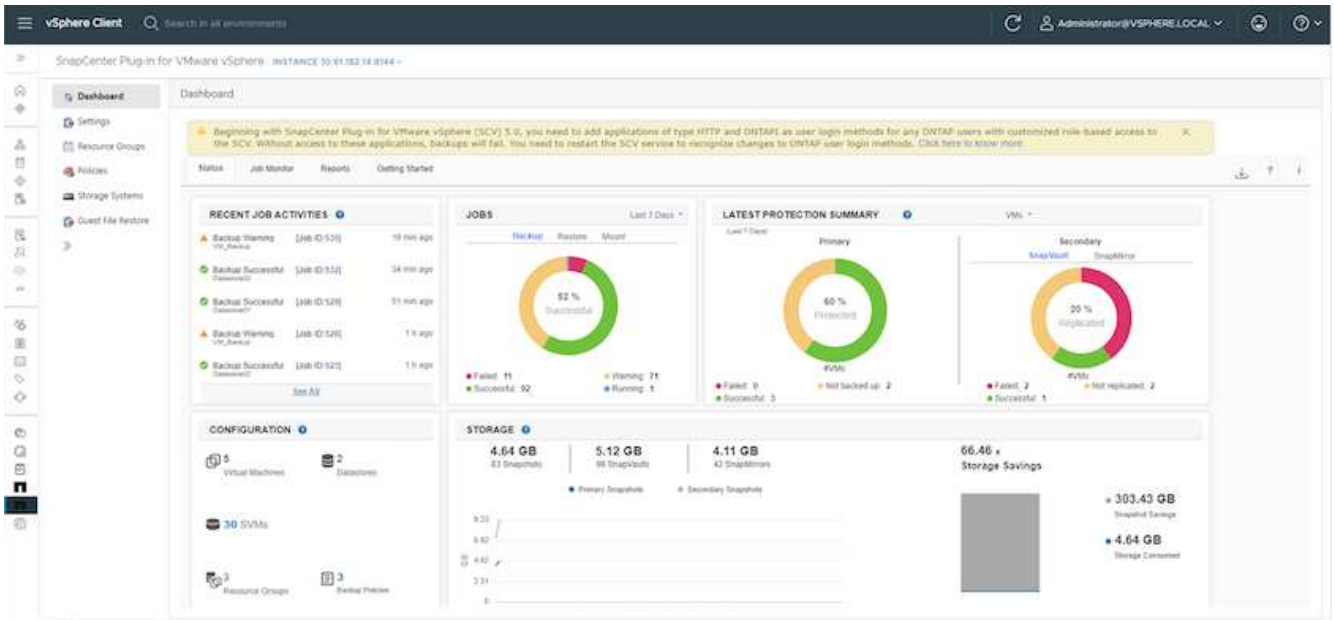


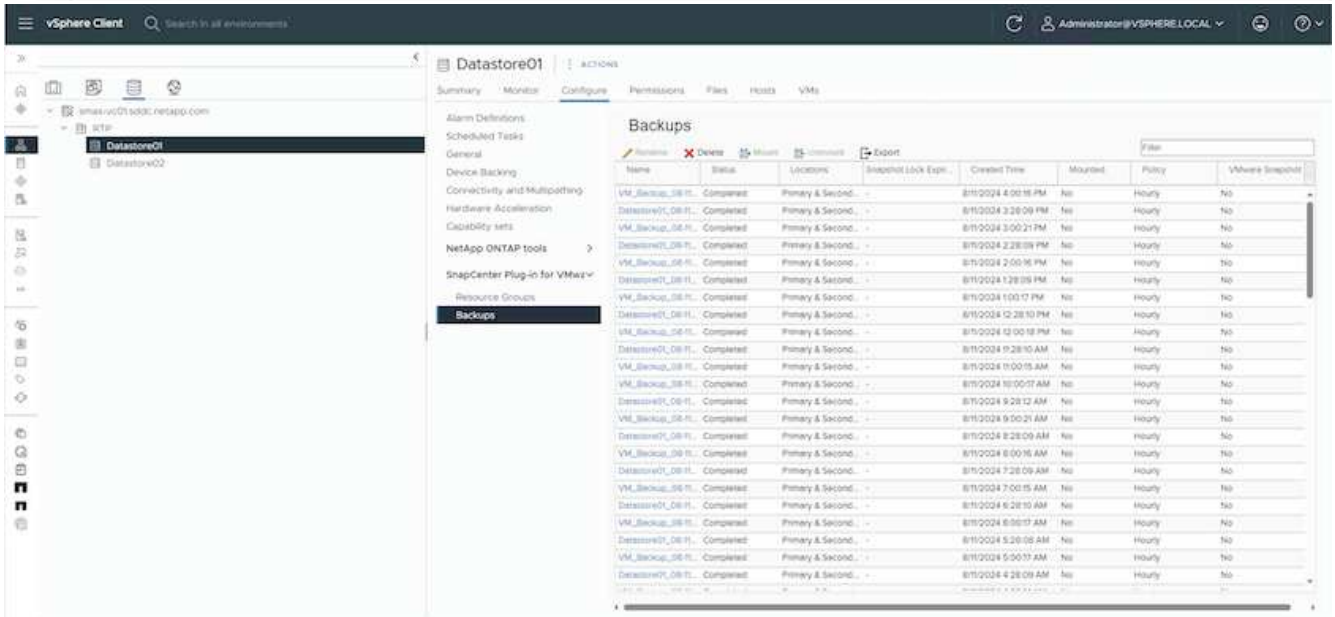
3. Creare un gruppo di risorse con gli elementi desiderati che devono essere protetti, associarli a criteri e pianificazioni.

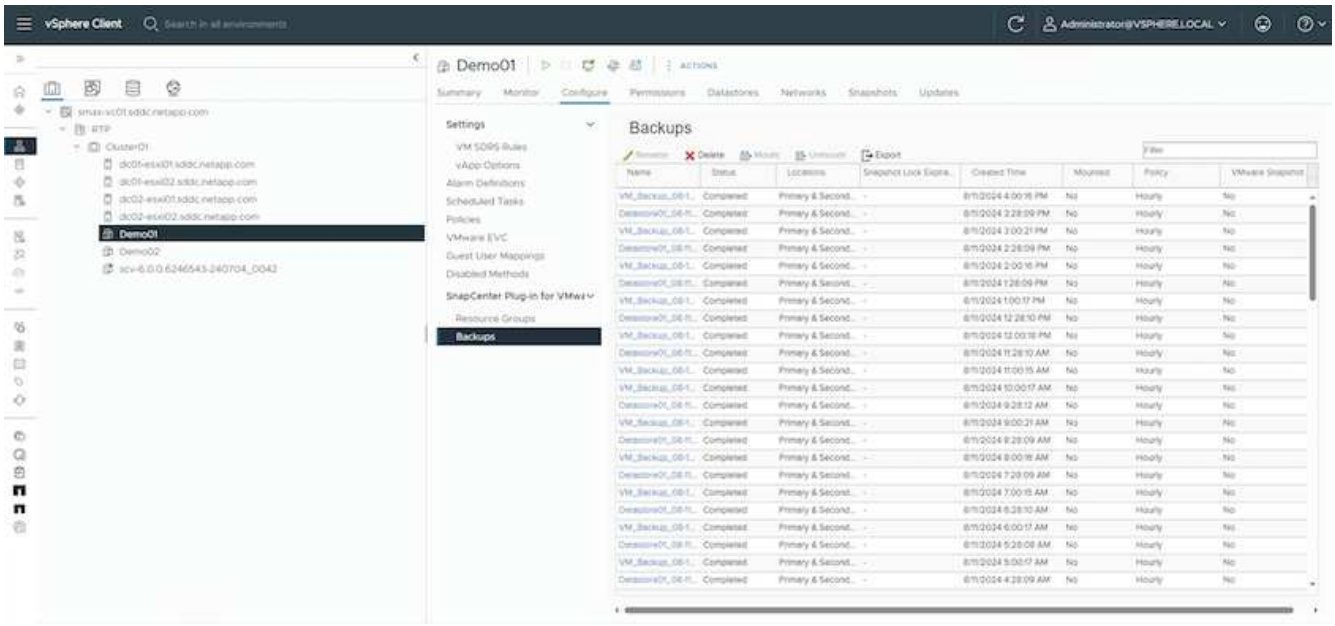


NOTA: i nomi degli snapshot che terminano con _recent non sono supportati con SM-as.

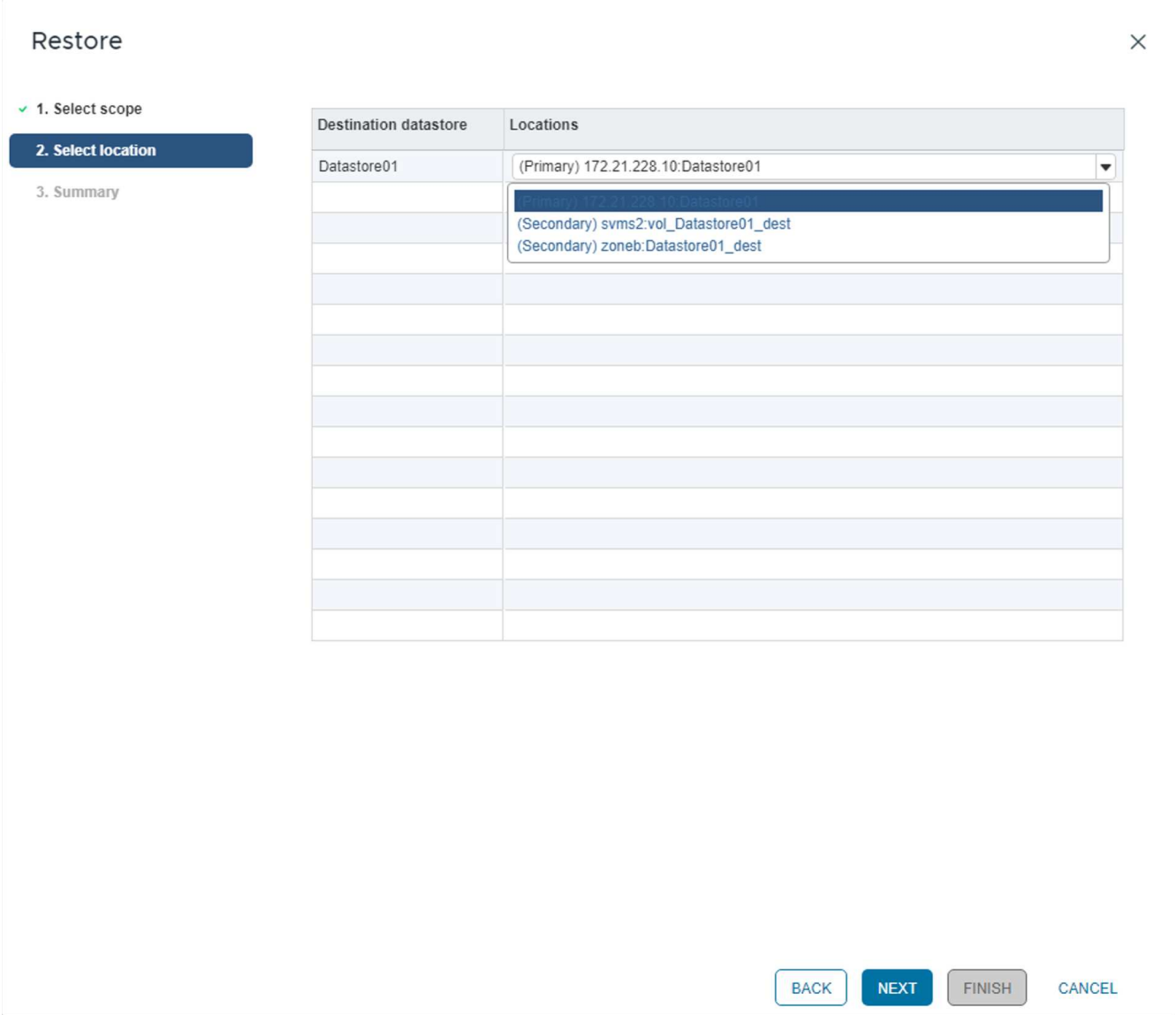
4. I backup vengono eseguiti all'orario pianificato in base ai criteri associati al gruppo di risorse. I lavori possono essere monitorati dal monitor lavori della Dashboard o dalle informazioni di backup su tali risorse.



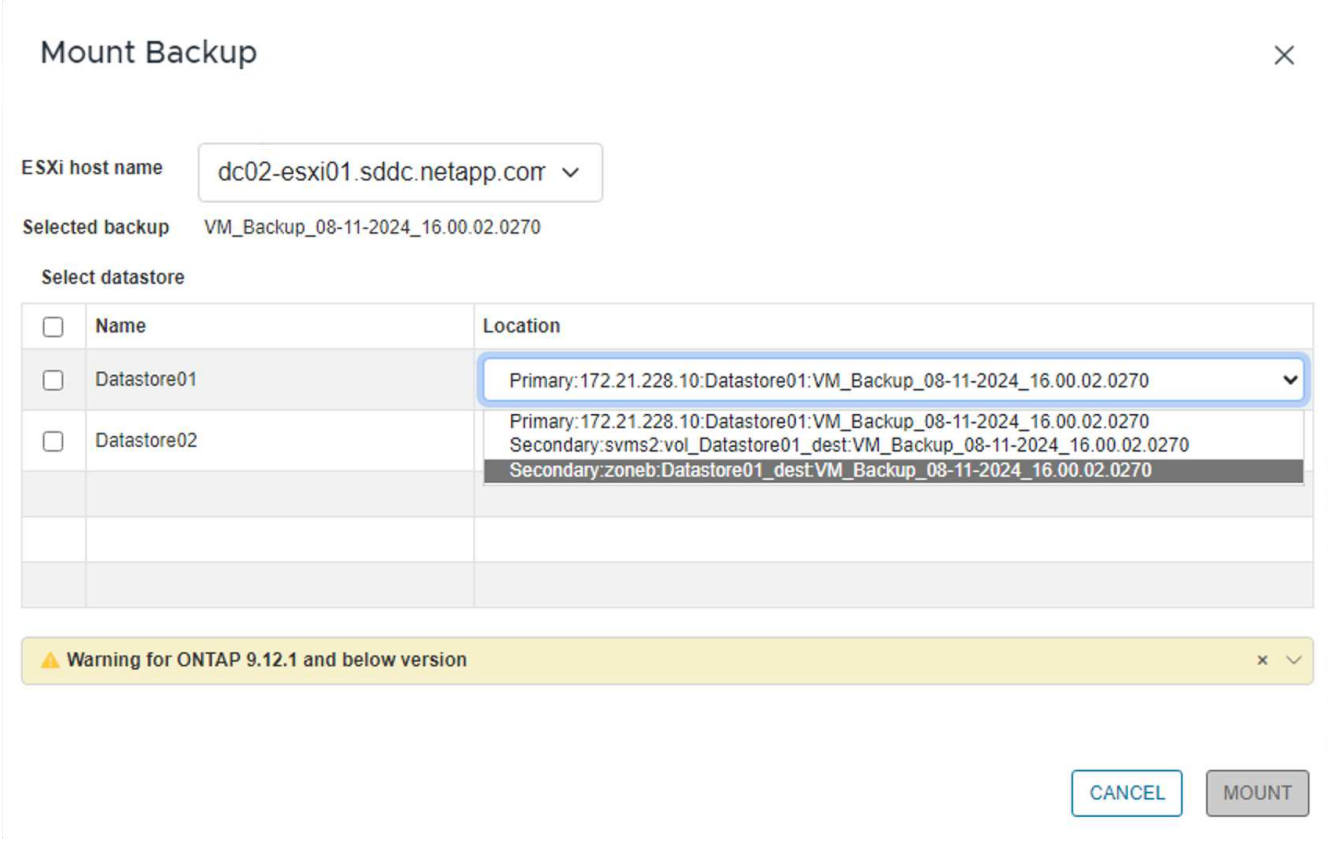




5. Le VM possono essere ripristinate sullo stesso vCenter o su un vCenter alternativo dall'SVM sul dominio di errore primario o da una delle posizioni secondarie.



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



Per assistenza con operazioni aggiuntive con SCV, fare riferimento"Documentazione SnapCenter Plug-in for VMware vSphere"

Convertire SM ActiveSync da asimmetrico a simmetrico attivo/attivo con VMware vSphere Metro Storage Cluster

Questo articolo spiega come convertire SnapMirror ActiveSync da asimmetrico a simmetrico attivo/attivo con VMware vSphere Metro Storage Cluster (VMSC).

Panoramica

"Sincronizzazione attiva NetApp Snapmirror (SM Active Sync)"è una soluzione solida per raggiungere un Recovery Time Objective (RTO) e un Recovery Point Objective (RPO) pari a zero in un ambiente virtualizzato.

"Cluster di archiviazione metro VMware vSphere (vMSC)"è una soluzione cluster estesa su diversi domini di errore e consente di distribuire macchine virtuali (VM) su due siti geograficamente separati, garantendo una disponibilità continua anche in caso di guasto di un sito.

La combinazione di vMSC con SM ActiveSync garantisce la coerenza dei dati e capacità di failover immediato tra due siti. Questa configurazione è particolarmente importante per le applicazioni mission-critical in cui qualsiasi perdita di dati o tempi di inattività sono inaccettabili.

SM Active Sync, precedentemente noto come SnapMirror Business Continuity (SMBC), consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. A partire da ONTAP 9.15.1, SM ActiveSync supporta una capacità attiva/attiva simmetrica. La modalità attiva/attiva simmetrica consente operazioni di I/O in lettura e scrittura da entrambe le copie di una LUN protetta con replica sincrona bidirezionale, in modo che

entrambe le copie della LUN possano eseguire operazioni di I/O localmente.

Questo documento illustra i passaggi per convertire SM ActiveSync da attivo/attivo asimmetrico a SM ActiveSync simmetrico in un ambiente cluster VMware Stretch, in altre parole converte SM ActiveSync da una policy di failover automatizzata a una policy di failover-duplex automatizzata. Per i dettagli su come configurare vMSC con SnapMirror ActiveSync (SM-as) utilizzando System Manager e ONTAP Tools, consultare"Cluster di storage VMware vSphere Metro con sincronizzazione attiva SnapMirror" .

Prerequisiti

- Sistemi di storage NetApp : assicurati di disporre di due cluster di storage NetApp (origine e destinazione) con licenze Snapmirror.
- Connettività di rete: verifica la connettività di rete a bassa latenza tra i sistemi di origine e di destinazione.
- Peering di cluster e SVM: configura il peering di cluster e il peering di Storage Virtual Machine (SVM) tra i cluster di origine e di destinazione.
- Versione ONTAP : assicurarsi che entrambi i cluster eseguano una versione di ONTAP che supporti la replica sincrona. Per SM ActiveSync è richiesto ONTAP 9.15.1 e versioni successive.
- Infrastruttura VMware vMSC: un cluster esteso consente ai sottosistemi di estendersi su più aree geografiche, presentando un set di risorse infrastrutturali di base unico e comune al cluster vSphere in entrambi i siti. Estende la rete e lo storage tra i siti.
- Utilizzare gli strumenti ONTAP 10.2 e versioni successive per semplificare l'uso di NetApp SnapMirror, maggiori dettagli sono disponibili"ONTAP tools for VMware vSphere 10."
- Tra il cluster primario e quello secondario deve esistere una relazione sincrona Snapmirror con RPO zero.
- È necessario annullare la mappatura di tutti i LUN sul volume di destinazione prima di poter creare la relazione Snapmirror RTO zero.
- Snapmirror ActiveSync supporta solo i protocolli SAN (non NFS/CIFS). Assicurarsi che nessun componente del gruppo di coerenza sia montato per l'accesso NAS.

Passaggi per convertire la sincronizzazione attiva SM asimmetrica in simmetrica

Nell'esempio seguente, selectrz1 è il sito primario e selectrz2 è il sito secondario.

1. Dal sito secondario, eseguire un aggiornamento SnapMirror sulla relazione esistente.

```
selectrz2::> snapmirror update -destination-path site2:/cg/CGsite1_dest
```

2. Verificare che l'aggiornamento SnapMirror sia stato completato correttamente.

```
selectrz2::> snapmirror show
```

3. Mettere in pausa ciascuna delle relazioni sincrone RPO zero.

```
 selectrz2::> snapmirror quiesce -destination-path
site2:/cg/CGsite1_dest
```

4. Eliminare ciascuna delle relazioni sincrone RPO zero.

```
selectrz2::> snapmirror delete -destination-path site2:/cg/CGsite1_dest
```

5. Rilascia la relazione SnapMirror di origine ma conserva gli snapshot comuni.

```
selectrz1::> snapmirror release -relationship-info-only  true
-destination-path svm0.1:/cg/CGsite1_dest
".
```

6. Creare una relazione sincrona SnapMirror con RTO zero con la policy AutomatedFailoverDuplex.

```
selectrz2::> snapmirror create -source-path svm0.1:/cg/CGsite1
-destination-path site2:/cg/CGsite1_dest -cg-item-mappings
site1lun1:@site1lun1_dest -policy AutomatedFailOverDuplex
```

7. Se gli host esistenti sono locali rispetto al cluster primario, aggiungere l'host al cluster secondario e stabilire la connettività con il rispettivo accesso a ciascun cluster.
8. Nel sito secondario, eliminare le mappe LUN sugli igroup associati agli host remoti.

```
selectrz2::> lun mapping delete -vserver svm0 -igroup wlkd01 -path
/vol/wkld01/wkld01
```

9. Nel sito primario, modificare la configurazione dell'iniziatore per gli host esistenti per impostare il percorso prossimale per gli iniziatori sul cluster locale.

```
selectrz1::> set -privilege advanced
selectrz1::*> igroup initiator add-proximal-vserver -vserver site1
-initiator iqn.1998-01.com.vmware:vcf-wkld-
esx01.sddc.netapp.com:575556728:67 -proximal-vserver site1
```

10. Aggiungere un nuovo igroup e un nuovo iniziatore per i nuovi host e impostare la prossimità dell'host per l'affinità dell'host con il suo sito locale. Abilitare la replica igroup per replicare la configurazione e invertire la località host sul cluster remoto.

```
selectrz1::*> igroup modify -vserver site1  -igroup smbc2smas
-replication-peer svm0.1
selectrz1::*> igroup initiator add-proximal-vserver -vserver site1
-initiator iqn.1998-01.com.vmware:vcf-wkld-
esx01.sddc.netapp.com:575556728:67 -proximal-vserver svm0.1
```

11. Scopri i percorsi sugli host e verifica che gli host abbiano un percorso attivo/ottimizzato verso la LUN di archiviazione dal cluster preferito.
12. Distribuisci l'applicazione e distribuisci i carichi di lavoro delle VM tra i cluster.
13. Risincronizzare il gruppo di coerenza.

```
selectrz2::> snapmirror resync -destination-path site2:/cg/CGsite1_dest
```

14. Eseguire nuovamente la scansione dei percorsi I/O LUN host per ripristinare tutti i percorsi alle LUN.

Scopri come utilizzare VMware Virtual Volumes (vVols) con l'archiviazione ONTAP

Scopri i vantaggi di VMware Virtual Volumes (vVols), il provisioning degli ONTAP tools for VMware vSphere, le strategie di protezione dei dati e le linee guida per la migrazione delle VM.

Panoramica

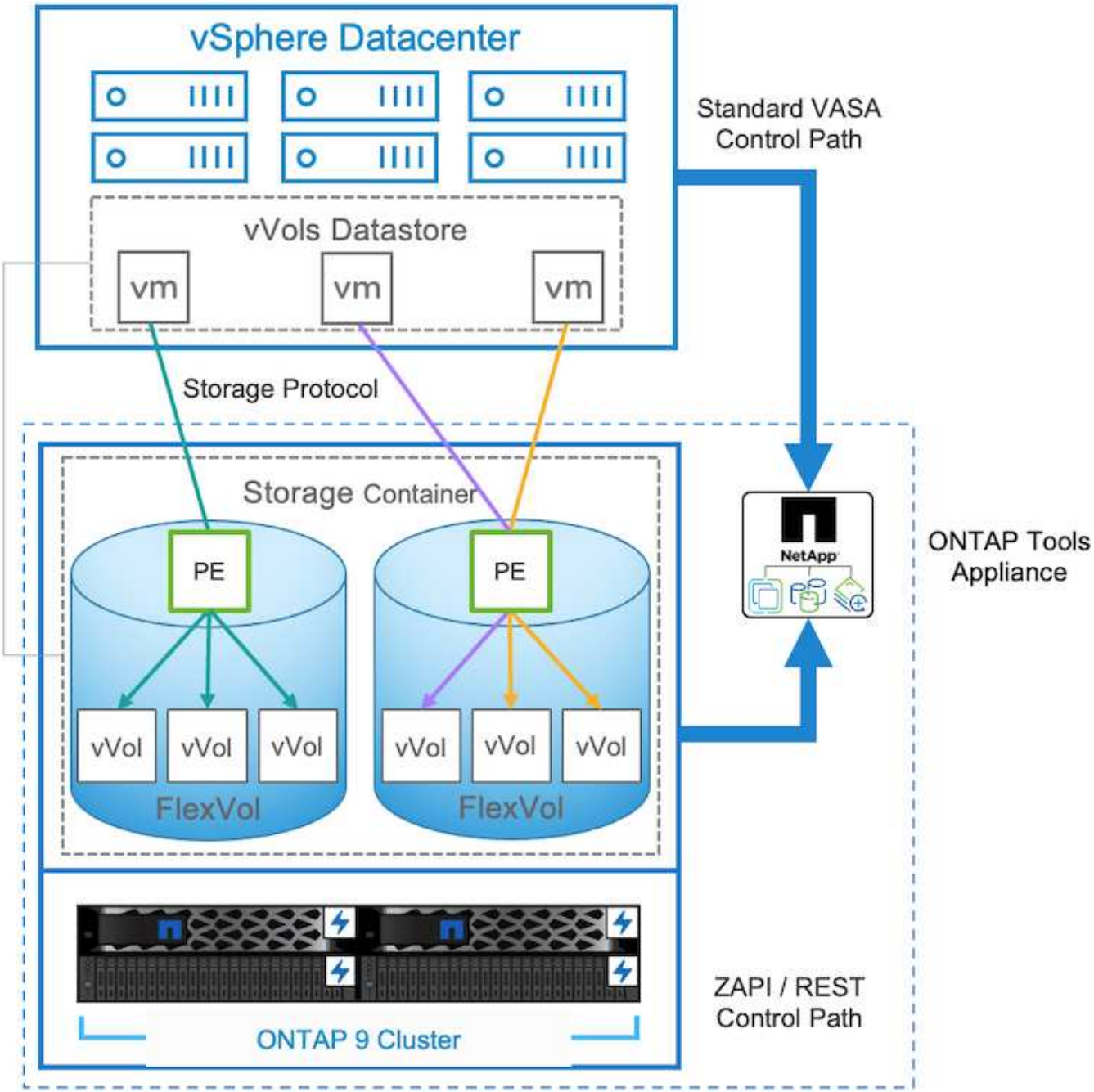
Grazie alla vSphere API for Storage Awareness (VASA), l'amministratore di VM può utilizzare facilmente tutte le funzionalità di storage necessarie per il provisioning delle VM, senza dover interagire con il proprio team di storage. Prima di VASA, gli amministratori delle VM potevano definire le policy di archiviazione delle VM, ma dovevano collaborare con i propri amministratori di archiviazione per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o convenzioni di denominazione. Con VASA, gli amministratori di vCenter dotati delle autorizzazioni appropriate possono definire una gamma di funzionalità di archiviazione che gli utenti di vCenter possono poi utilizzare per il provisioning delle VM. La mappatura tra la policy di archiviazione della VM e il profilo di capacità di archiviazione del datastore consente a vCenter di visualizzare un elenco di datastore compatibili per la selezione, oltre a consentire ad altre tecnologie come Aria (precedentemente nota come vRealize) Automation o Tanzu Kubernetes Grid di selezionare automaticamente l'archiviazione da una policy assegnata. Questo approccio è noto come gestione basata su criteri di archiviazione. Sebbene i profili e le policy di capacità di archiviazione possano essere utilizzati anche con i datastore tradizionali, in questo caso ci concentreremo sui datastore vVols . Il provider VASA per ONTAP è incluso come parte degli ONTAP tools for VMware vSphere.

I vantaggi di avere VASA Provider fuori da Storage Array includono:

- Una singola istanza può gestire più array di archiviazione.
- Il ciclo di rilascio non deve necessariamente dipendere dal rilascio del sistema operativo Storage.
- Le risorse su Storage Array sono molto costose.

Ogni datastore vVol è supportato da Storage Container, che è una voce logica nel provider VASA per definire la capacità di archiviazione. Il contenitore di archiviazione con strumenti ONTAP è costruito con volumi ONTAP . È possibile espandere il contenitore di archiviazione aggiungendo volumi ONTAP all'interno dello stesso SVM.

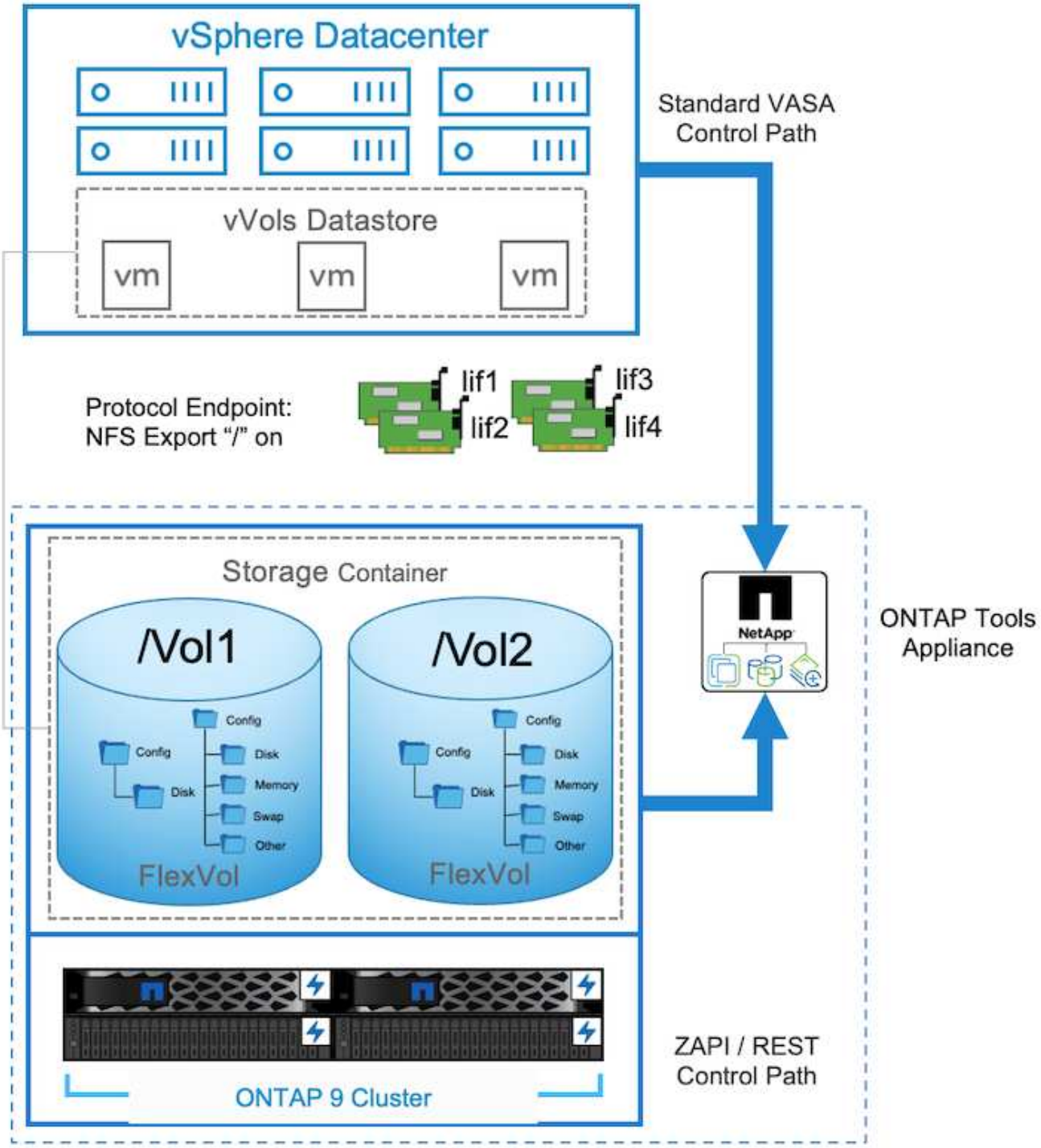
Il Protocol Endpoint (PE) è gestito principalmente dagli strumenti ONTAP . Nel caso di vVols basati su iSCSI, viene creato un PE per ogni volume ONTAP che fa parte di quel contenitore di archiviazione o datastore vVol. Il PE per iSCSI è una LUN di piccole dimensioni (4 MiB per 9.x e 2 GiB per 10.x) che viene presentata all'host vSphere e a cui vengono applicate policy di multipathing.

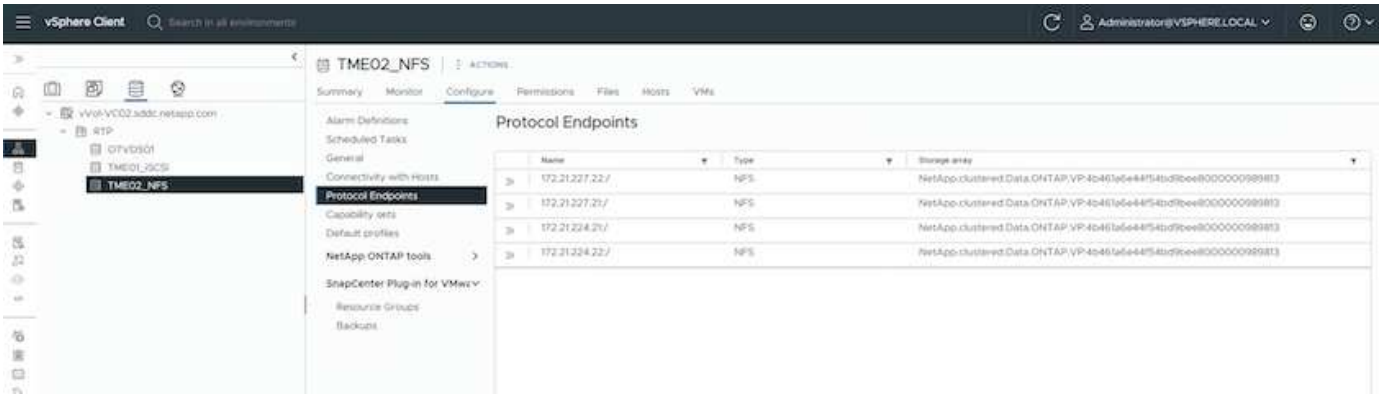



```
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint  -fields size
vserver path                                                  size
------- ------------------------------------------------- ----
zoneb   /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb   /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 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 dato NFS lif su SVM su cui risiede

il contenitore di archiviazione o il datastore vVol.





Gli strumenti ONTAP gestiscono il ciclo di vita di PE e anche la comunicazione dell'host vSphere con l'espansione e la riduzione del cluster vSphere. L'API degli strumenti ONTAP è disponibile per l'integrazione con gli strumenti di automazione esistenti.

Attualmente, gli ONTAP tools for VMware vSphere sono disponibili in due versioni.

Strumenti ONTAP 9.x

- Quando è richiesto il supporto vVol per NVMe/FC
- Requisiti normativi federali degli Stati Uniti o dell'UE
- Altri casi d'uso integrati con il SnapCenter Plug-in for VMware vSphere

Strumenti ONTAP 10.x

- Alta disponibilità
- Multi-tenancy
- Grande scala
- Supporto di sincronizzazione attiva SnapMirror per datastore VMFS
- Prossima integrazione per determinati casi d'uso con il SnapCenter Plug-in for VMware vSphere

Perché vVols?

VMware Virtual Volumes (vVols) offre i seguenti vantaggi:

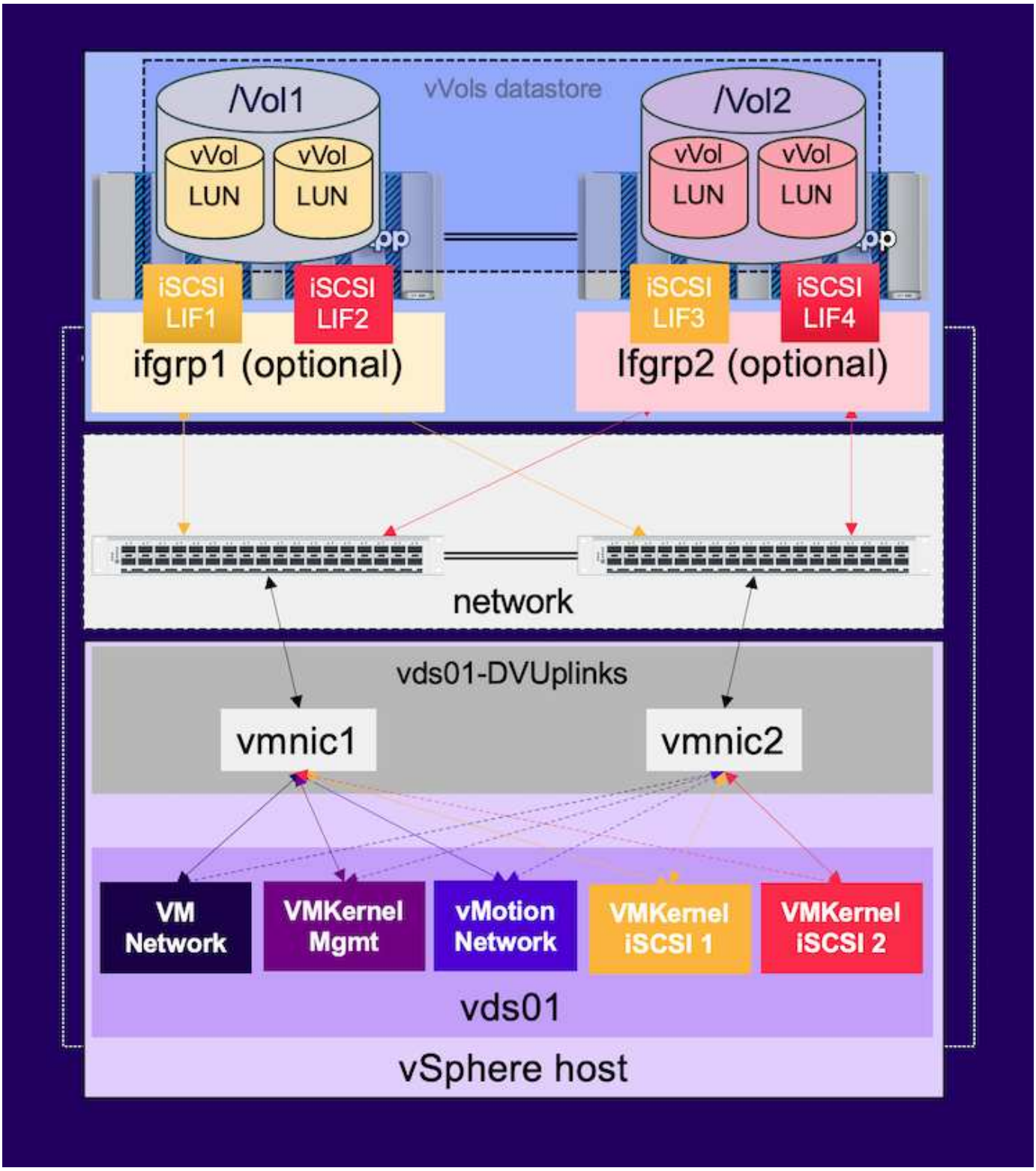
- Provisioning semplificato (non c'è bisogno di preoccuparsi dei limiti massimi di LUN per host vSphere o di dover creare le esportazioni NFS per ogni volume)
- Riduce al minimo il numero di percorsi iSCSI/FC (per vVol basati su SCSI a blocchi)
- Snapshot, cloni e altre operazioni di archiviazione vengono in genere scaricati sull'array di archiviazione e funzionano molto più velocemente.
- Migrazioni di dati semplificate per le VM (non è necessario coordinarsi con altri proprietari di VM nella stessa LUN)
- Criteri QoS applicati a livello di disco della macchina virtuale anziché a livello di volume.
- Semplicità operativa (i fornitori di storage forniscono le loro funzionalità differenziate nel provider VASA)
- Supporta VM su larga scala.
- Supporto della replica vVol per la migrazione tra vCenter.

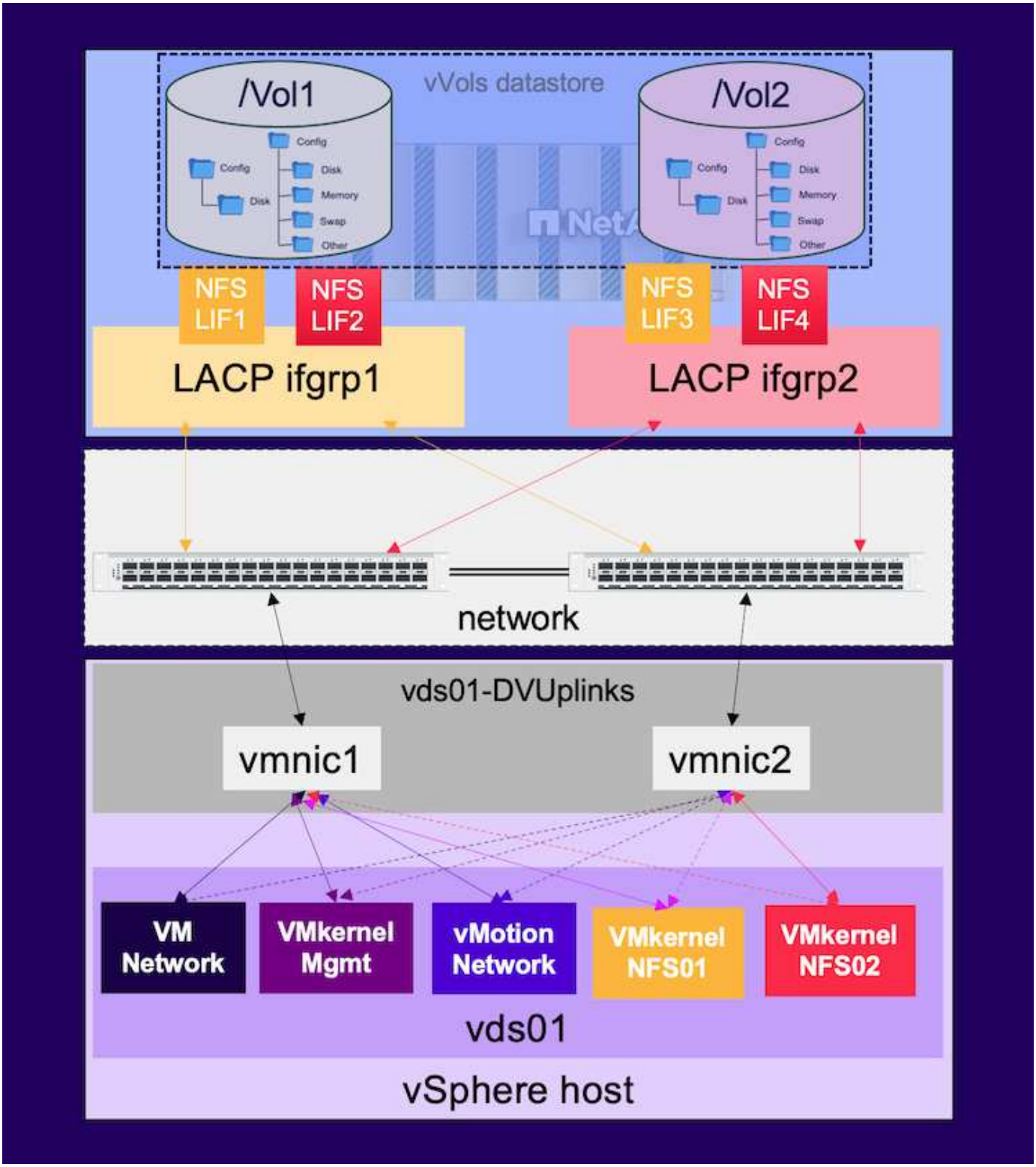
- Gli amministratori di storage hanno la possibilità di monitorare a livello di disco della VM.

Opzioni di connettività

In genere, per le reti di storage si consiglia un ambiente a doppia struttura, per soddisfare i requisiti di elevata disponibilità, prestazioni e tolleranza agli errori. I vVols sono supportati con iSCSI, FC, NFSv3 e NVMe/FC. NOTA: fare riferimento"Strumento di matrice di interoperabilità (IMT)" per la versione supportata dello strumento ONTAP

L'opzione di connettività rimane coerente con le opzioni del datastore VMFS o del datastore NFS. Di seguito è riportato 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

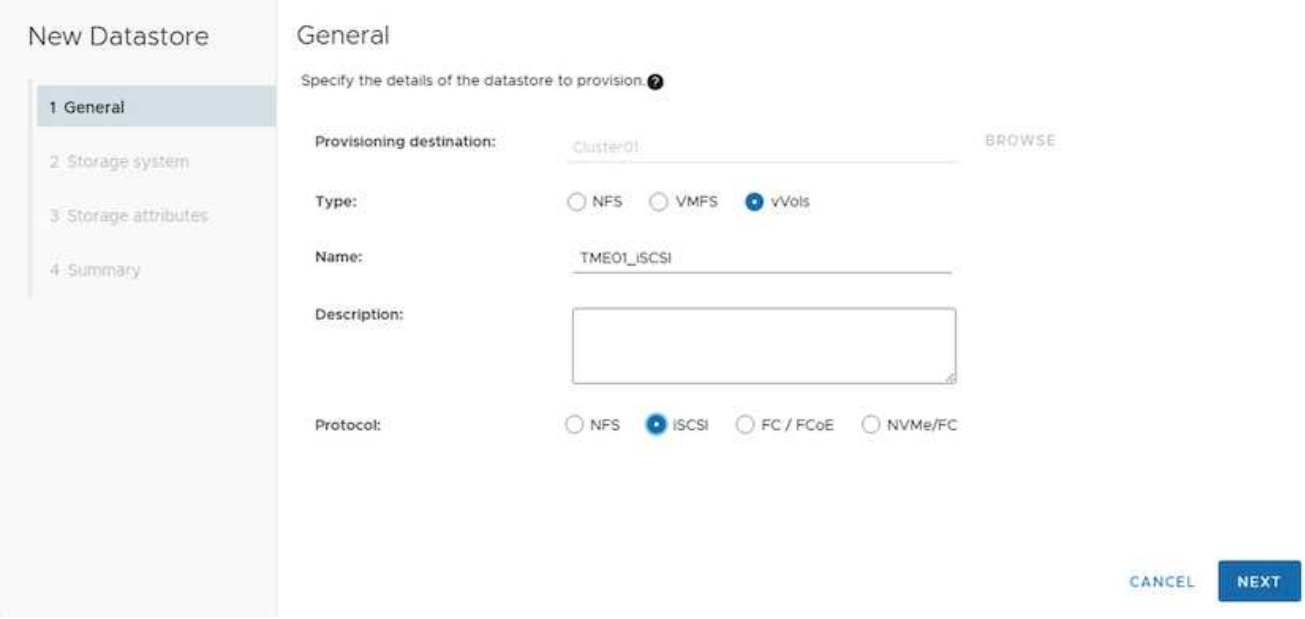


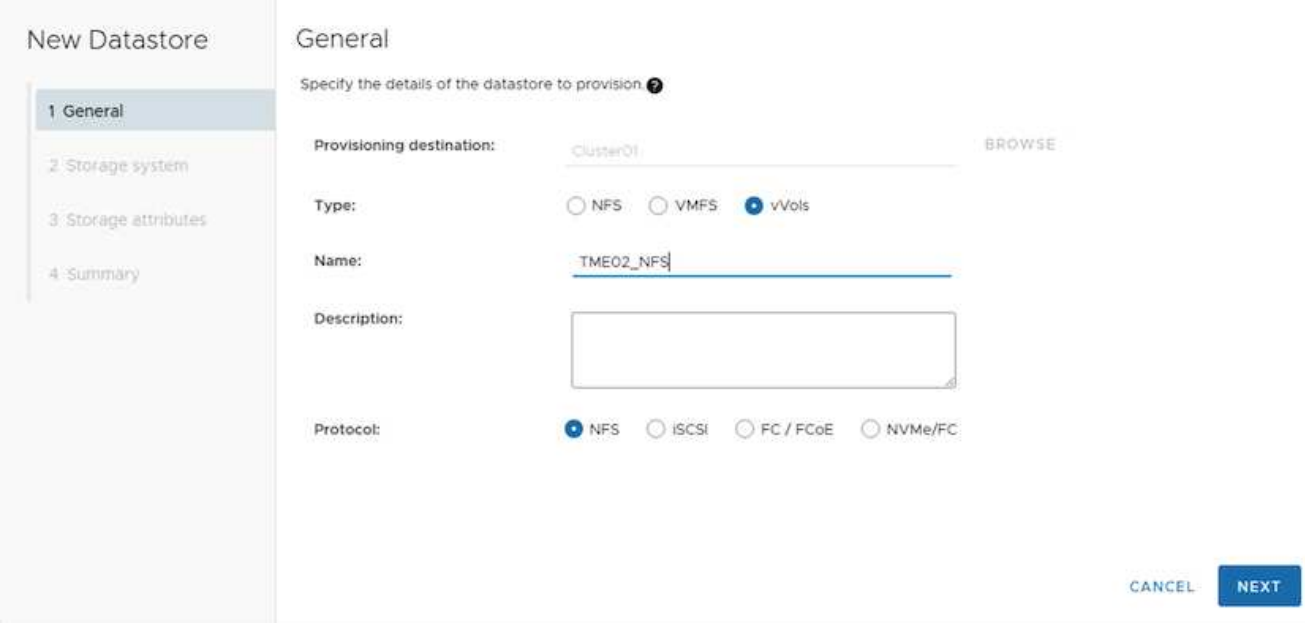
Provisioning tramite ONTAP tools for VMware vSphere

Il datastore vVol può essere fornito in modo simile al datastore VMFS o NFS utilizzando gli strumenti ONTAP . Se il plug-in degli strumenti ONTAP non è disponibile nell'interfaccia utente del client vSphere, fare riferimento alla sezione Come iniziare riportata di seguito.

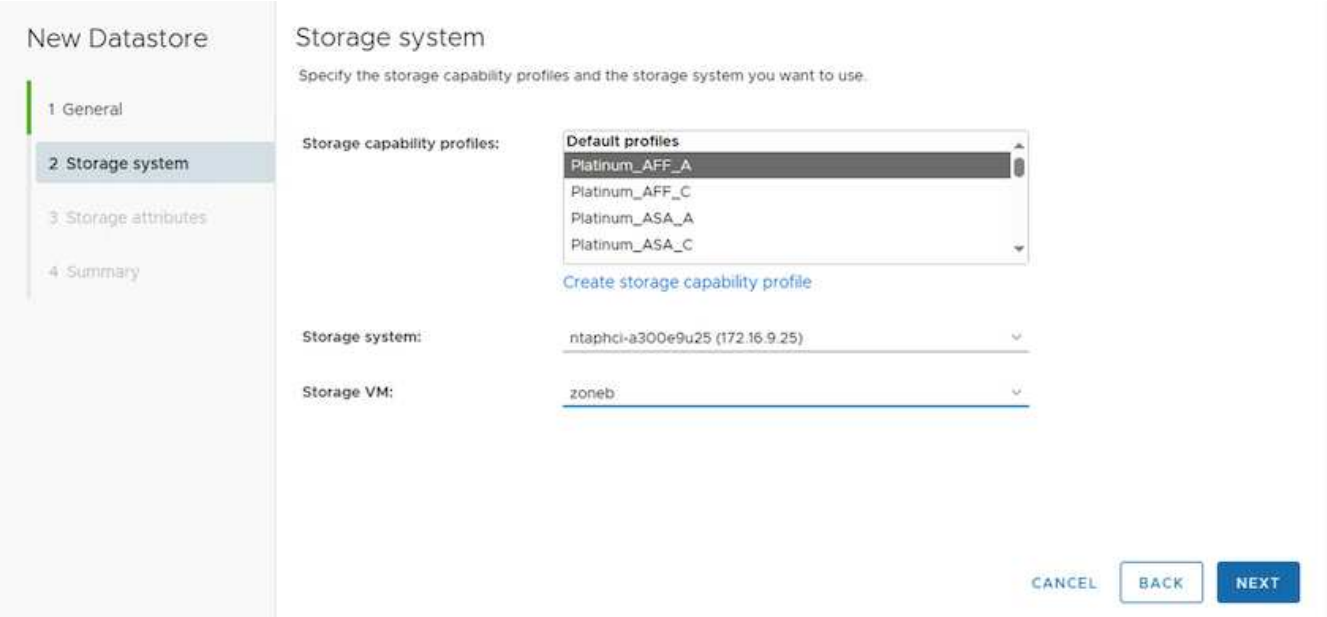
Con gli strumenti ONTAP 9.13

1. Fare clic con il pulsante destro del mouse sul cluster o sull'host vSphere e selezionare Provision Datastore in Strumenti NetApp ONTAP .
2. Mantieni il tipo come vVols, fornisci un nome per il datastore e seleziona il protocollo desiderato

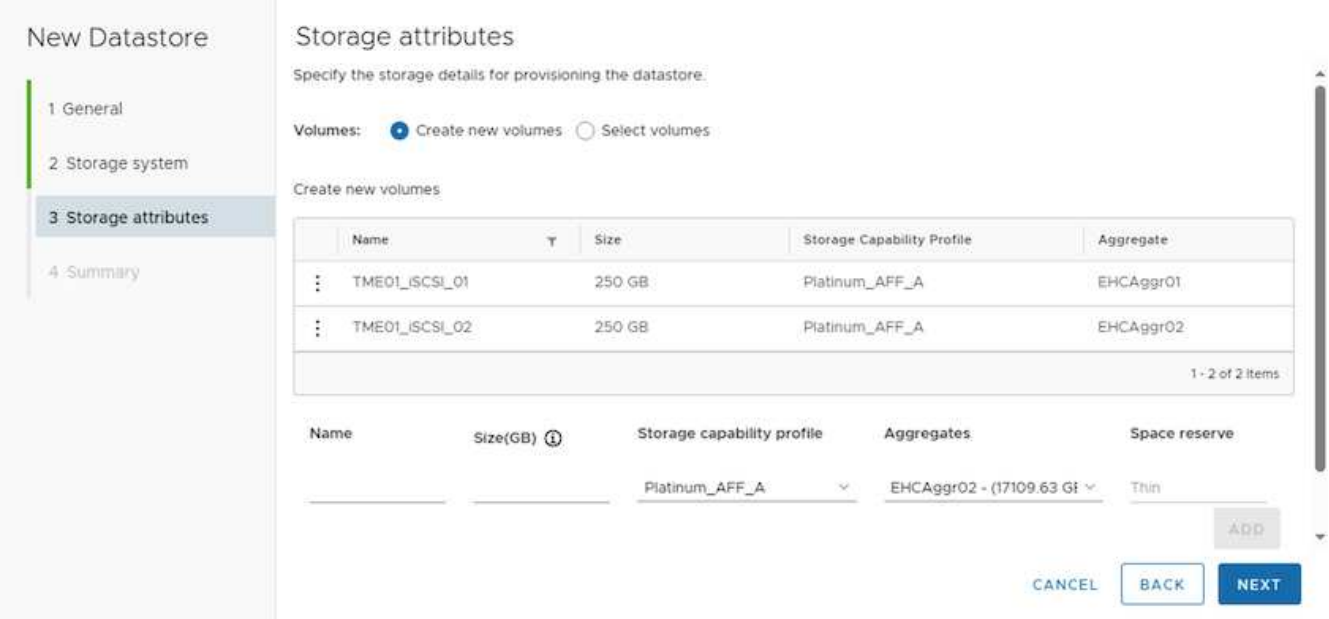




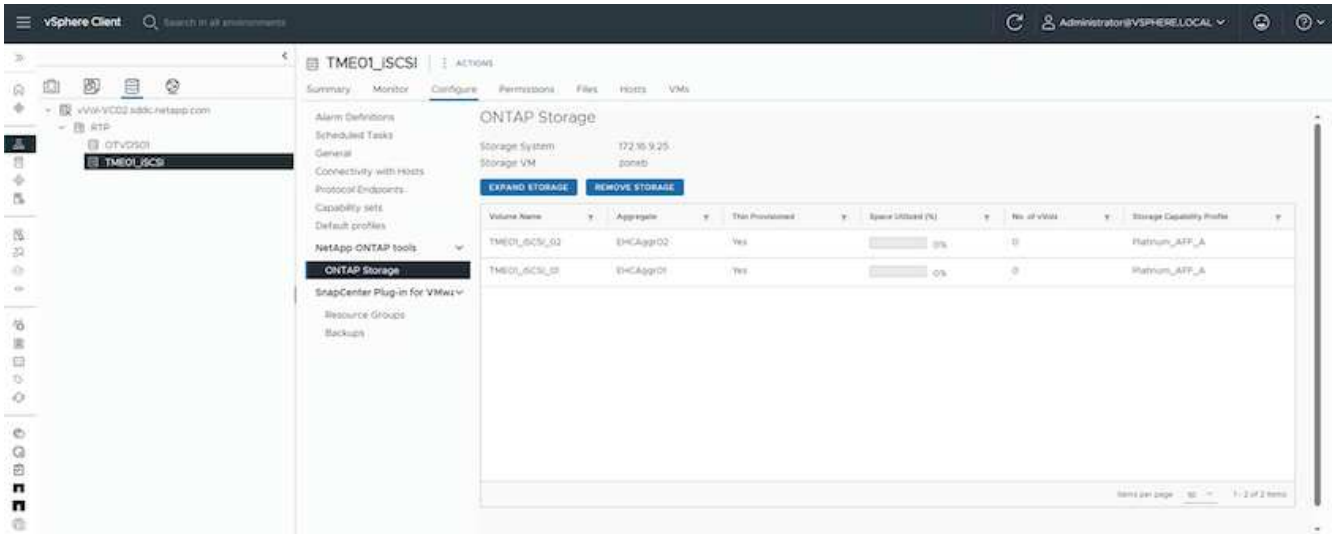
3. Selezionare il profilo di capacità di archiviazione desiderato, scegliere il sistema di archiviazione e l'SVM.



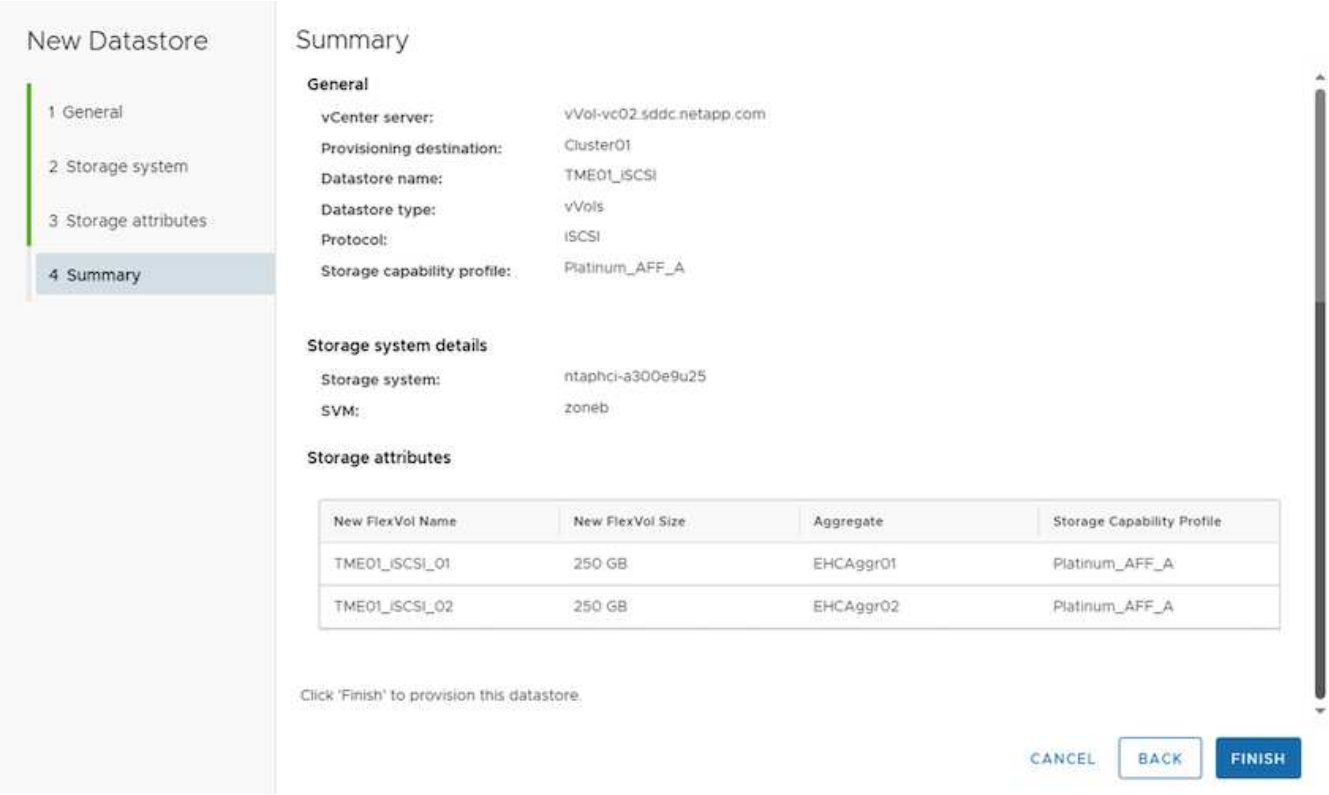
4. Crea nuovi volumi ONTAP o selezionane uno esistente per il datastore vVol.



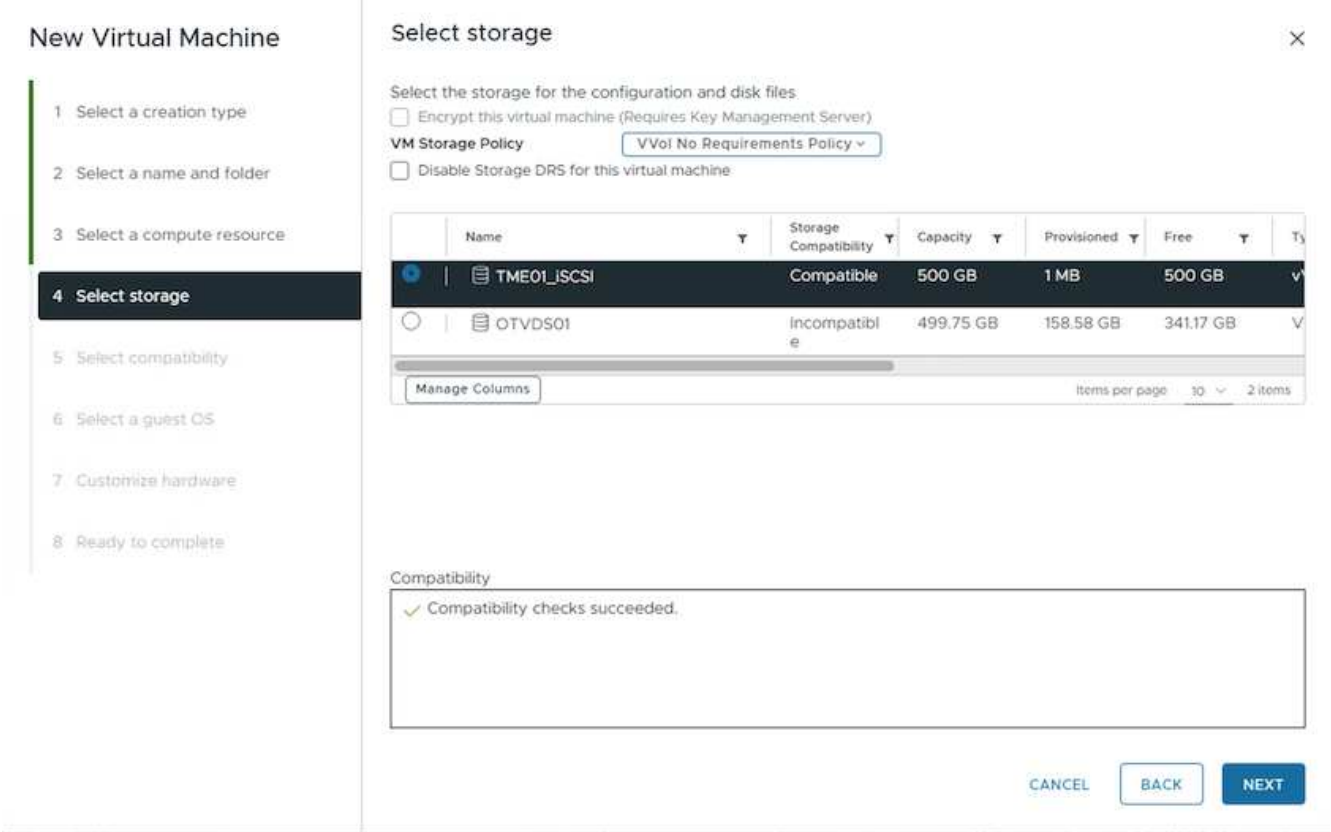
I volumi ONTAP possono essere visualizzati o modificati in seguito tramite l'opzione datastore.



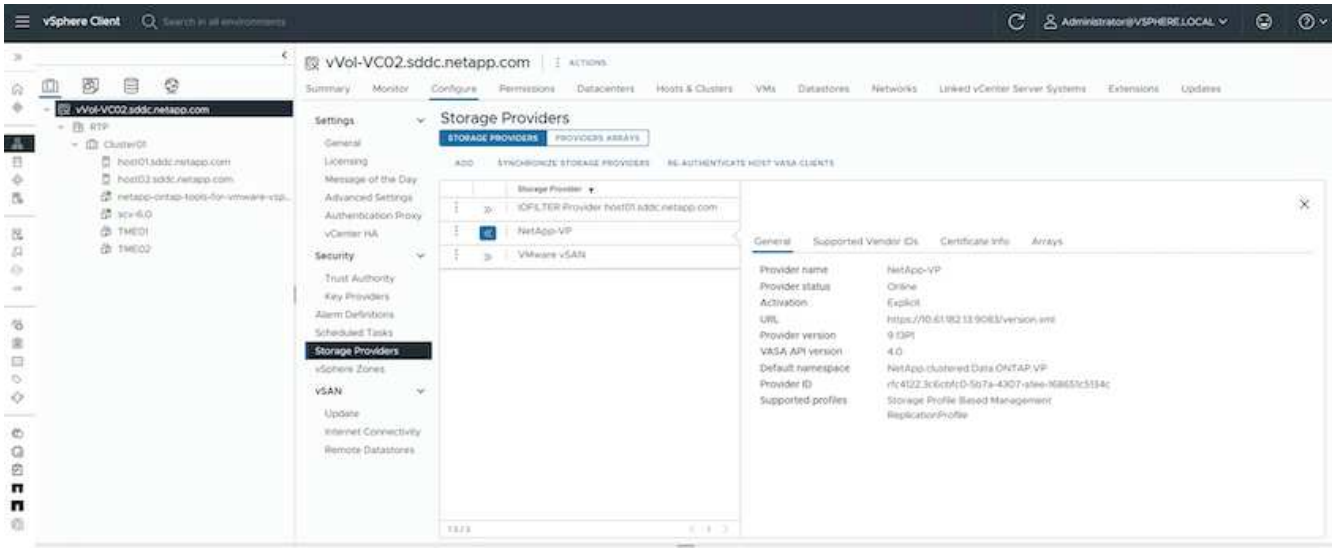
5. Rivedere il riepilogo e fare clic su Fine per creare il datastore vVol.



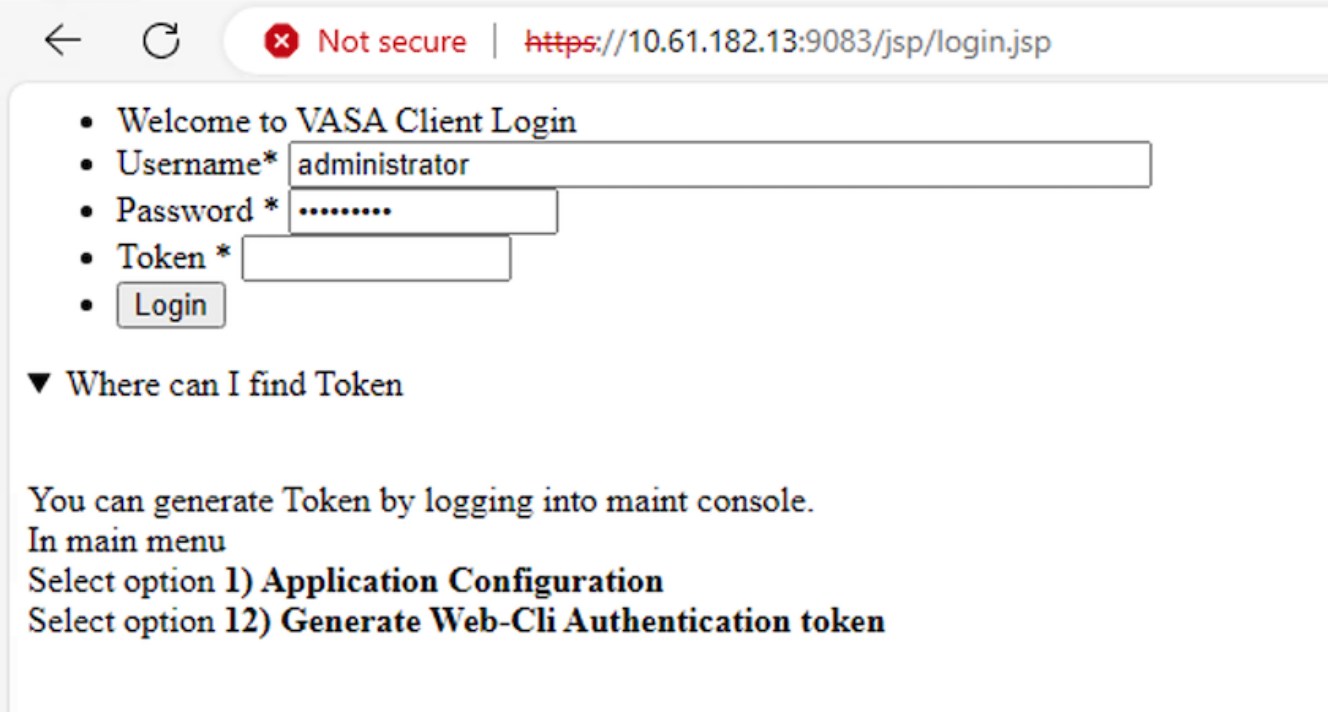
6. Una volta creato, il datastore vVol può essere utilizzato come qualsiasi altro datastore. Ecco un esempio di assegnazione di un datastore in base ai criteri di archiviazione della VM a una VM in fase di creazione.



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



Le credenziali devono corrispondere alle informazioni utilizzate durante la fornitura degli strumenti ONTAP



oppure utilizzare la password aggiornata con la console di manutenzione degli strumenti ONTAP .

```
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:

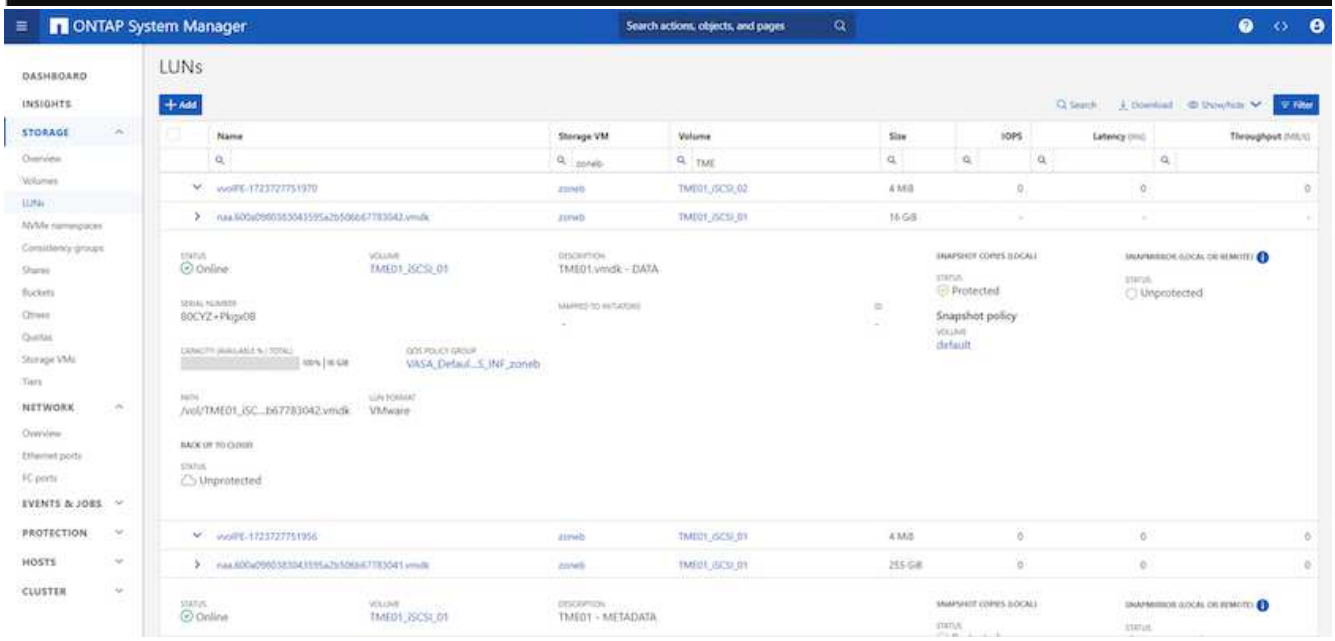
Operation	Description
Web based CLI interface	Web based access to the command line interface for administrative tasks
Inventory	Listing of all objects and information currently known in Unified Virtual Appliance database
Statistics	Listing of all counters and information regarding internal state
Right 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

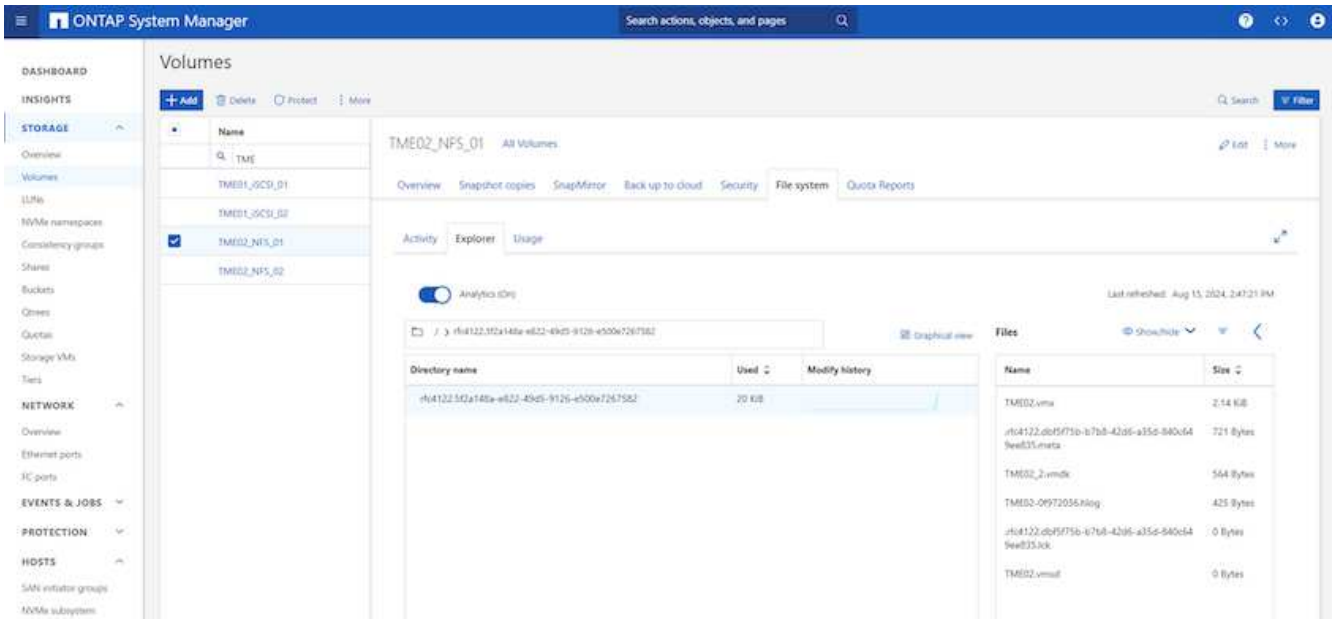
Digitare il comando desiderato dall'elenco dei comandi disponibili. Per elencare i dettagli vVol insieme alle informazioni di archiviazione sottostanti, provare vvol list -
verbose=true

Per i sistemi basati su LUN, è possibile utilizzare anche ONTAP CLI 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
```

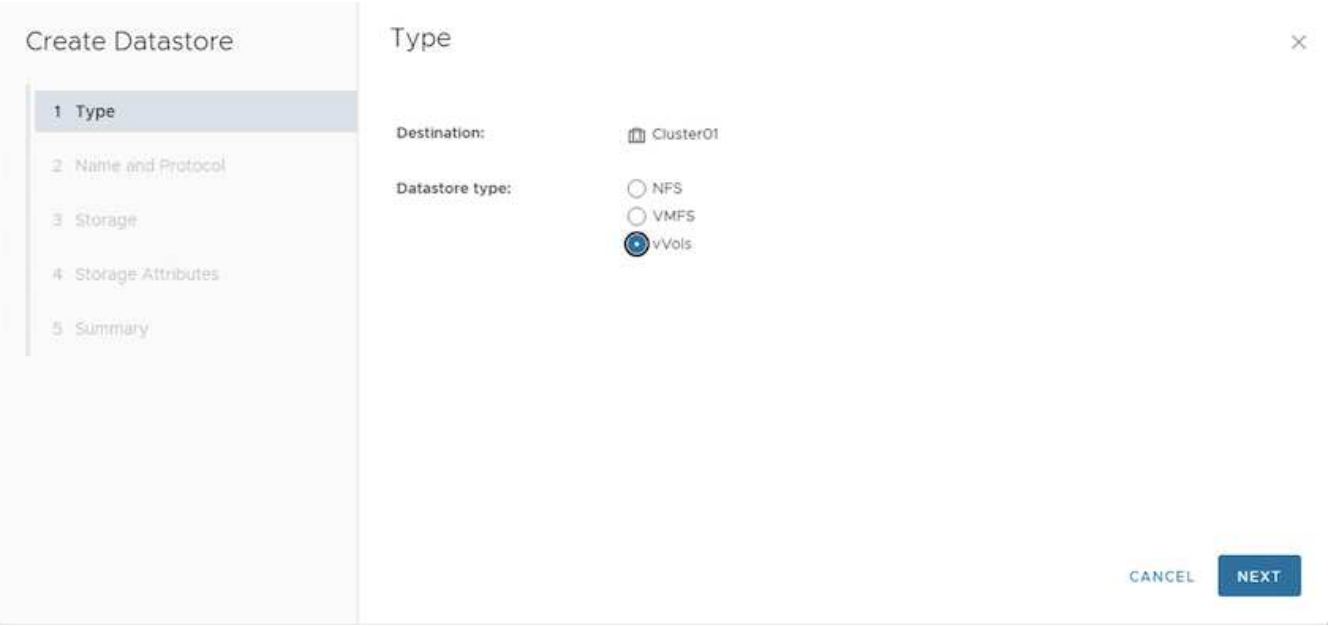


Per i sistemi basati su NFS, è possibile utilizzare System Manager per esplorare il datastore.

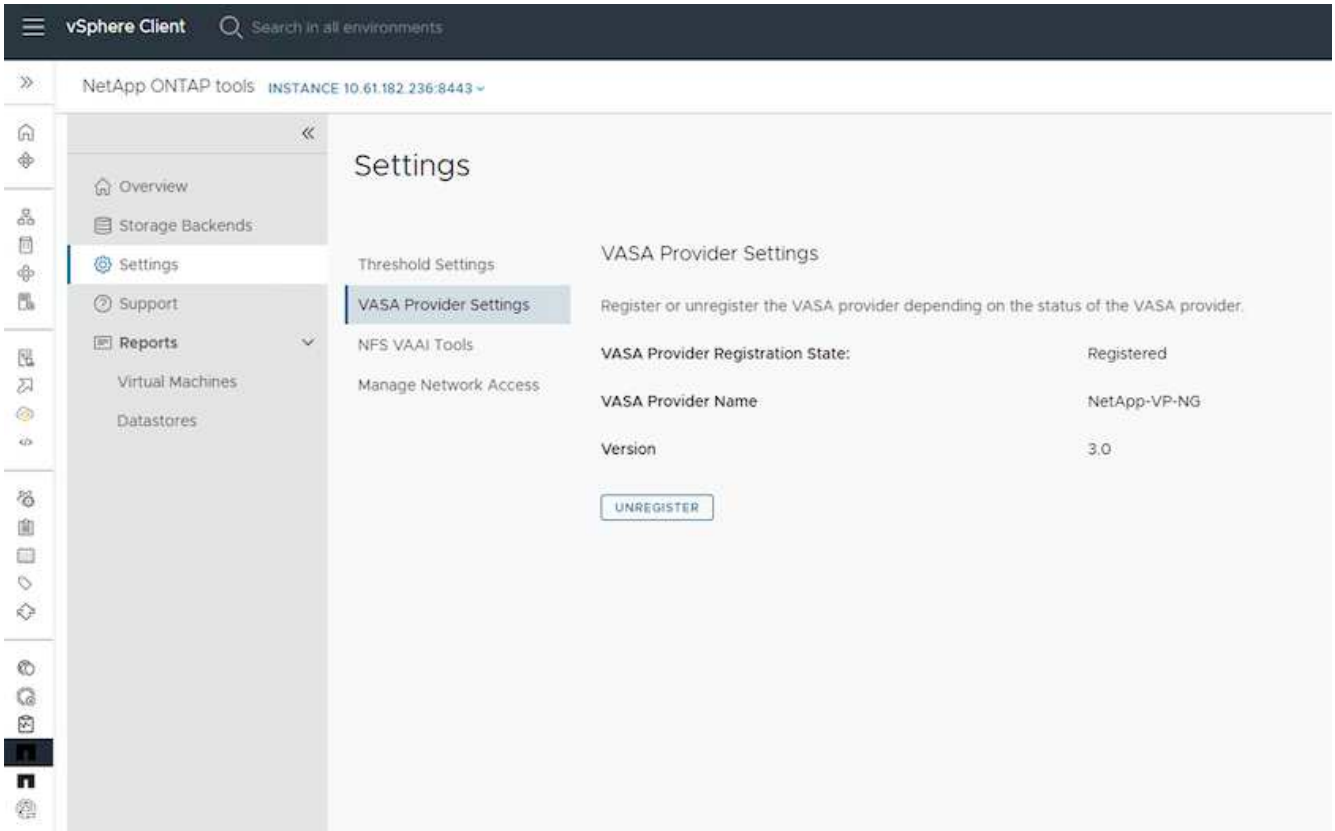


Con gli strumenti ONTAP 10.1

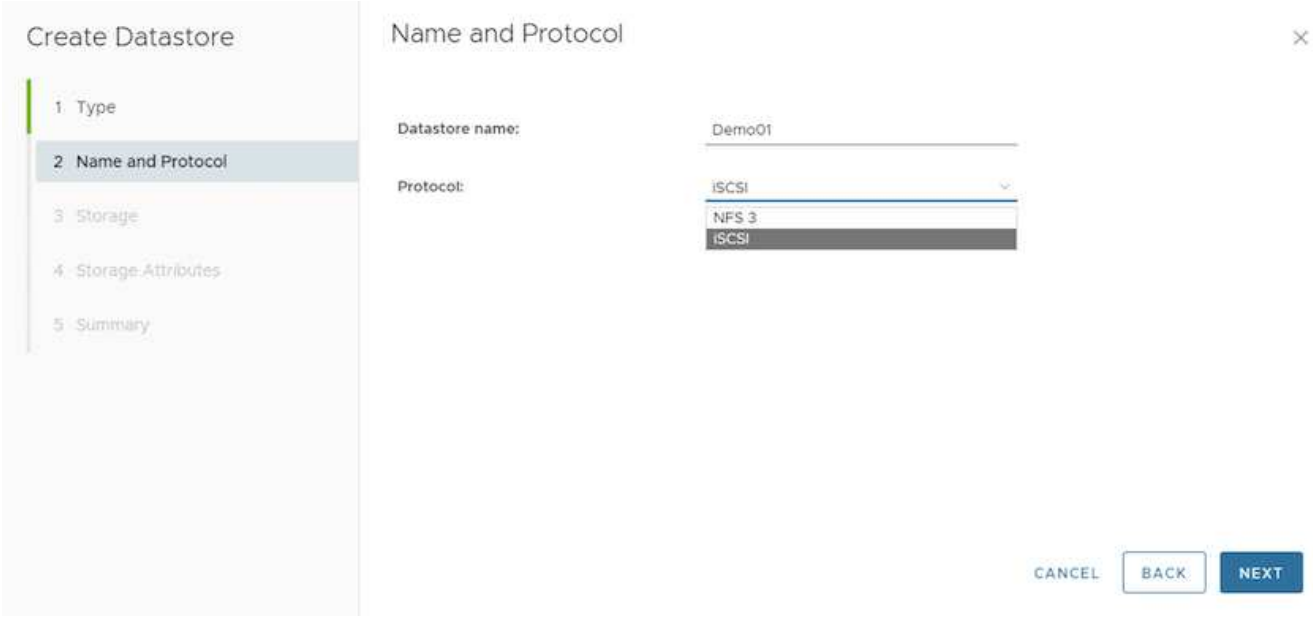
1. Fare clic con il pulsante destro del mouse sul cluster o sull'host vSphere e selezionare Crea datastore (10.1) in Strumenti NetApp ONTAP .
2. Selezionare il tipo di datastore come vVols.



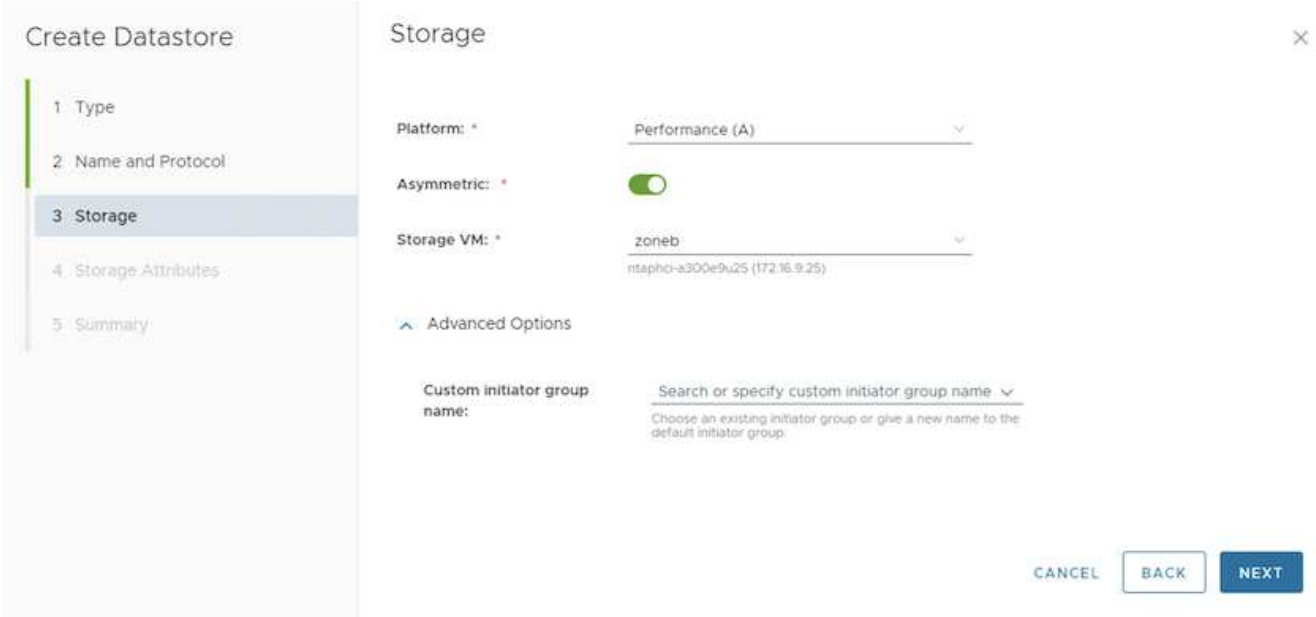
Se l'opzione vVols non è disponibile, assicurarsi che il provider VASA sia registrato.



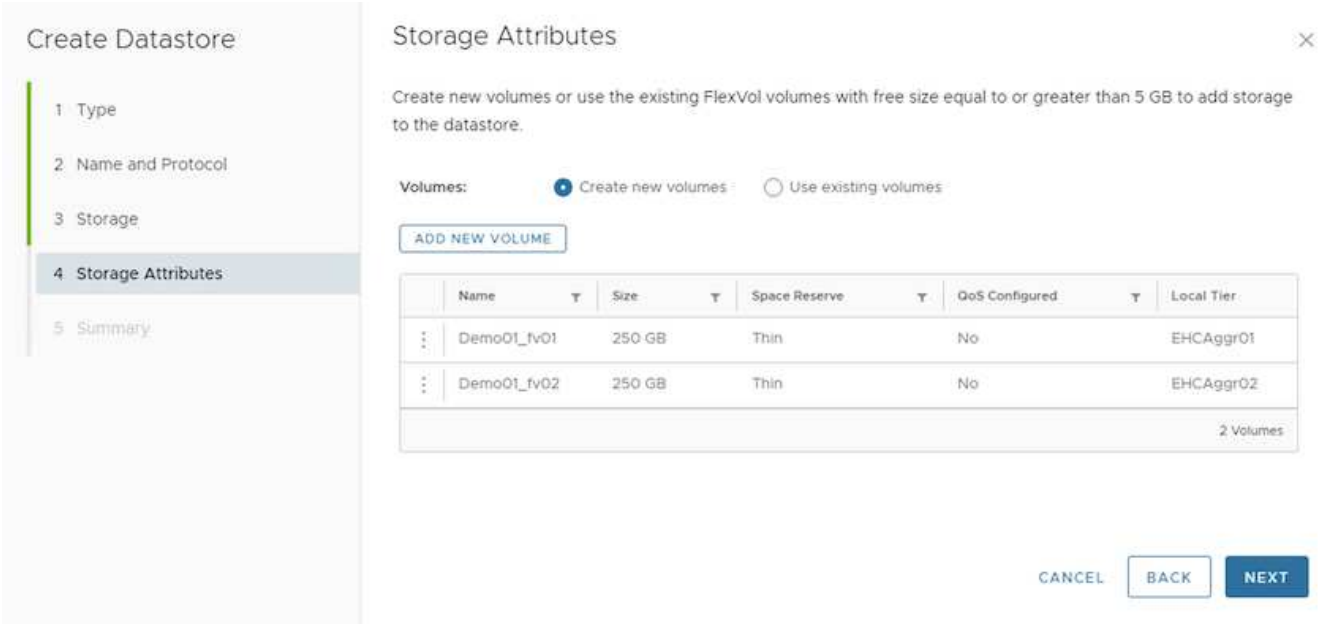
3. Fornire il nome del datastore vVol e selezionare il protocollo di trasporto.



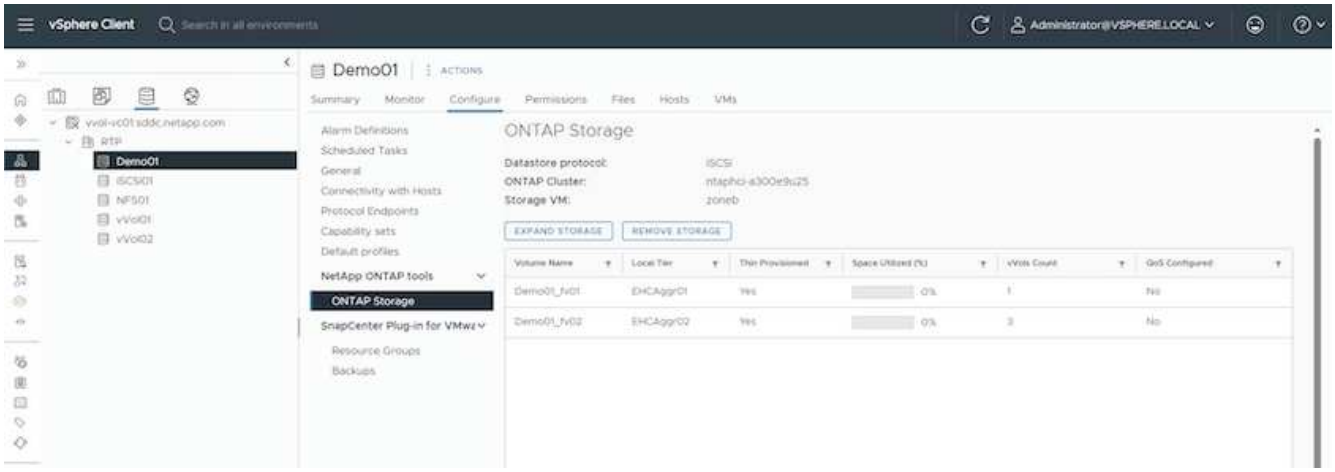
4. Selezionare la piattaforma e la VM di archiviazione.



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

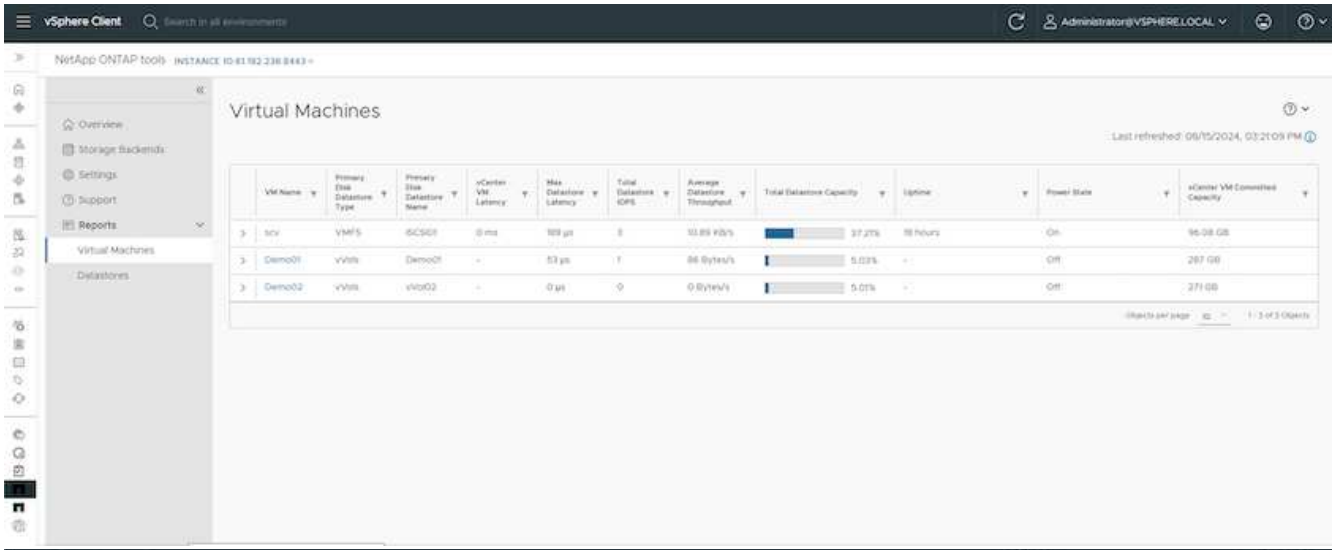


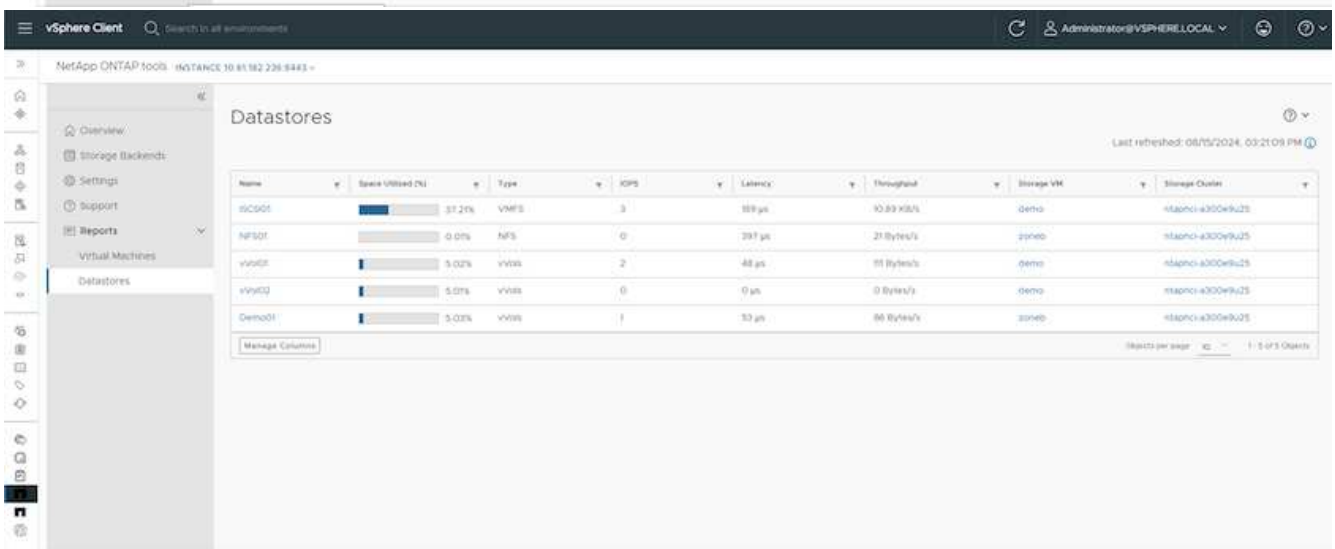
I volumi ONTAP possono essere visualizzati o aggiornati in un secondo momento dalla configurazione del datastore.



6. Una volta eseguito il provisioning, il datastore vVol può essere utilizzato come qualsiasi altro datastore.

7. Gli strumenti ONTAP forniscono il report VM e Datastore.

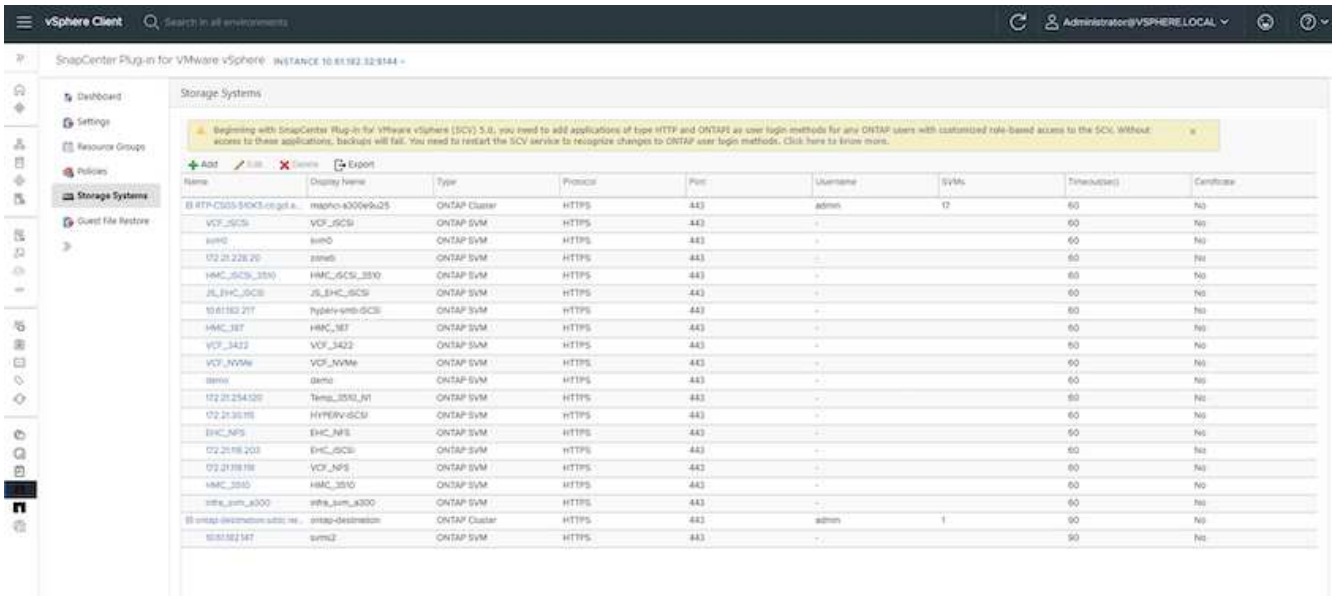




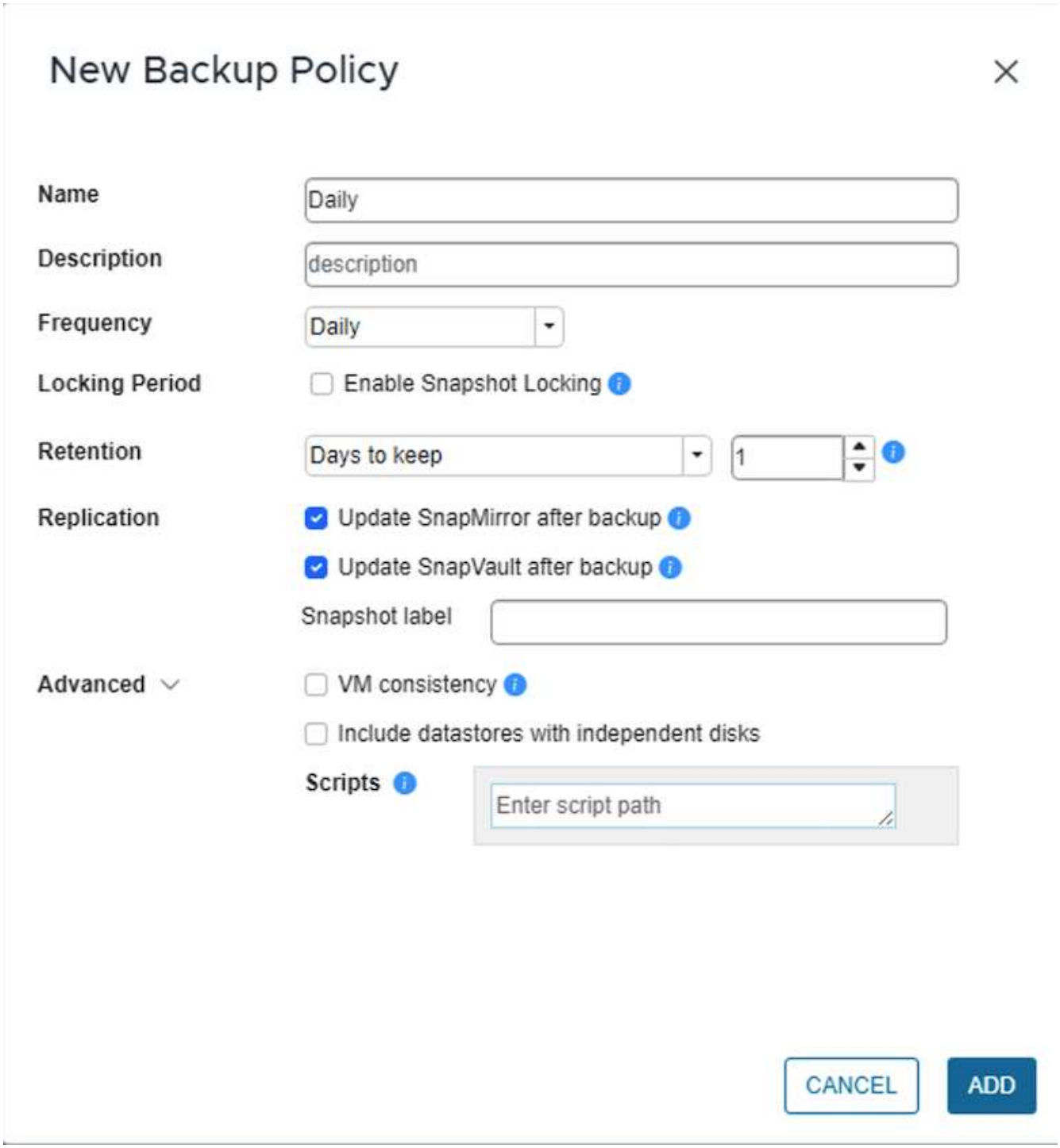
Protezione dei dati delle VM sul datastore vVol

Una panoramica della protezione dei dati delle VM sul datastore vVol è disponibile all'indirizzo"protezione vVols" .

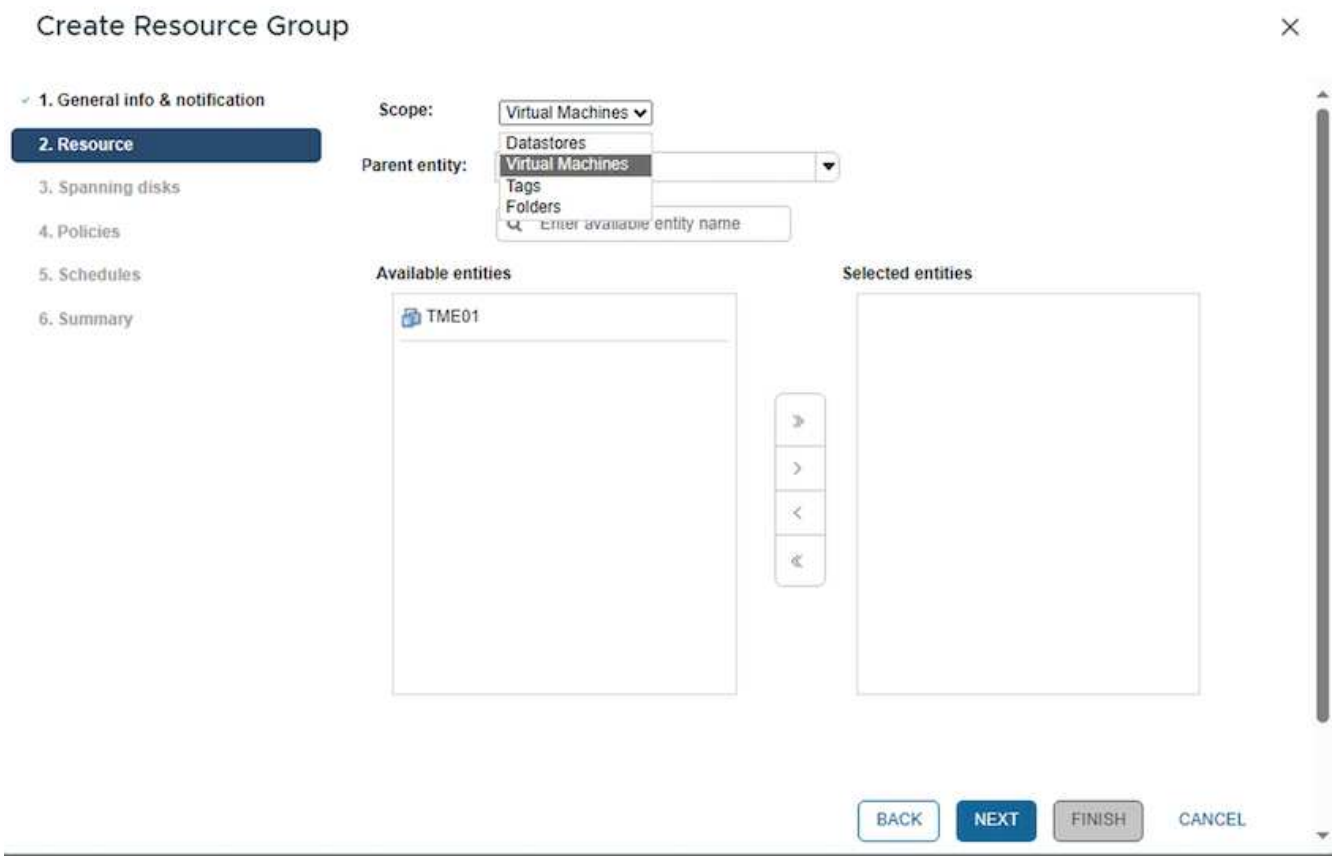
1. Registrare il sistema di archiviazione che ospita il datastore vVol e tutti i partner di replicazione.



2. Creare una policy con gli attributi richiesti.

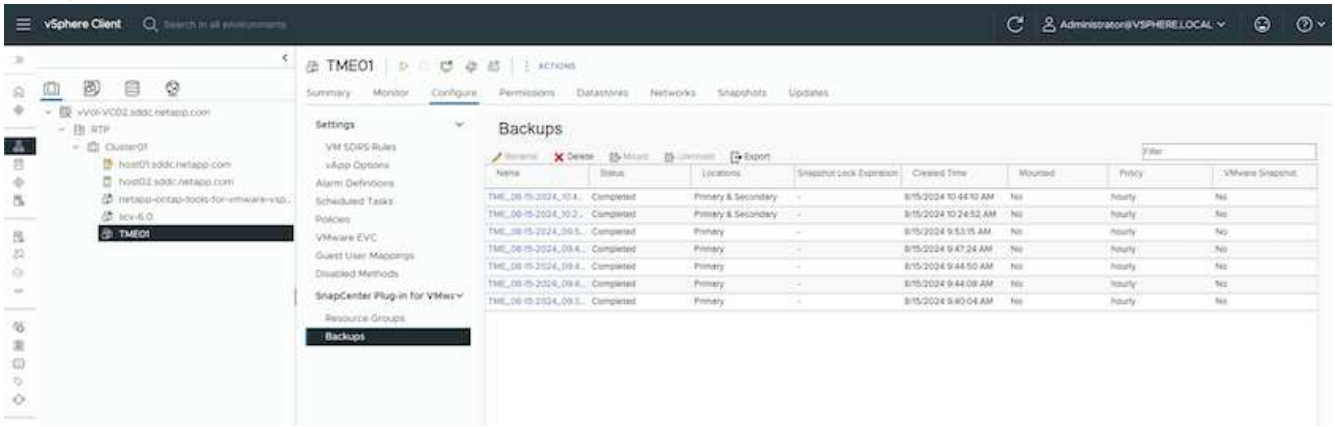


3. Crea un gruppo di risorse e associalo alla policy (o alle Policy).



NOTA: per il datastore vVol, è necessario proteggerlo 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 nella scheda di configurazione.



5. La macchina virtuale può essere ripristinata dalla sua posizione primaria o secondaria.

Fare riferimento"Documentazione del plug-in SnapCenter" per ulteriori casi d'uso.

Migrazione delle VM dai datastore tradizionali al datastore vVol

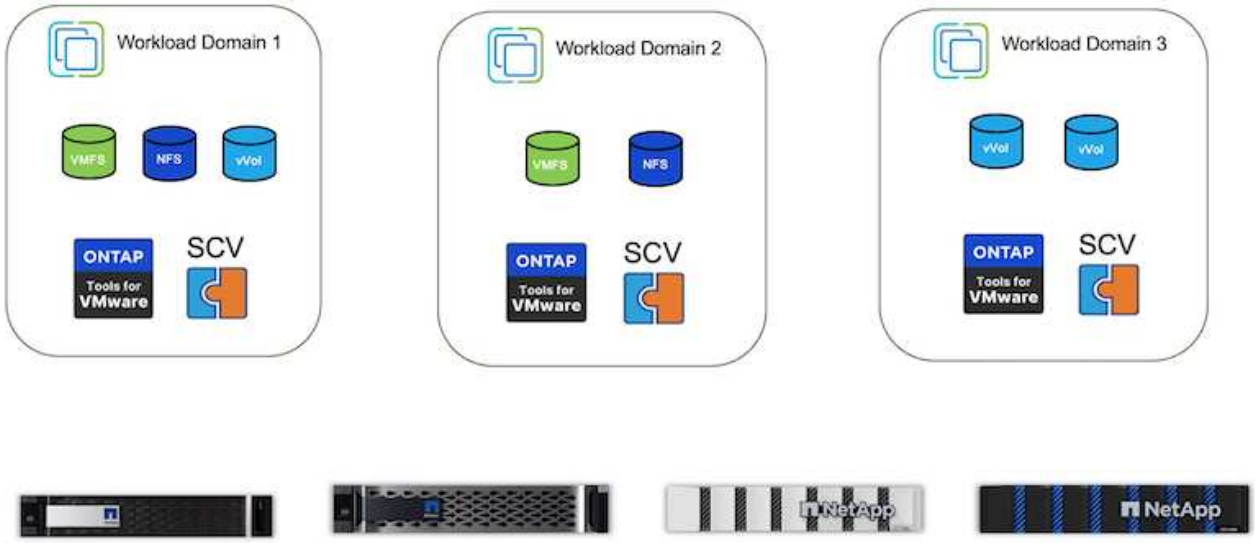
Per migrare le VM da altri datastore a un datastore vVol, sono disponibili varie opzioni in base allo scenario. Può variare da una semplice operazione di storage vMotion alla migrazione tramite HCX. Fare riferimento"migrare le VM al datastore ONTAP" per maggiori dettagli.

Migrazione di VM tra datastore vVol

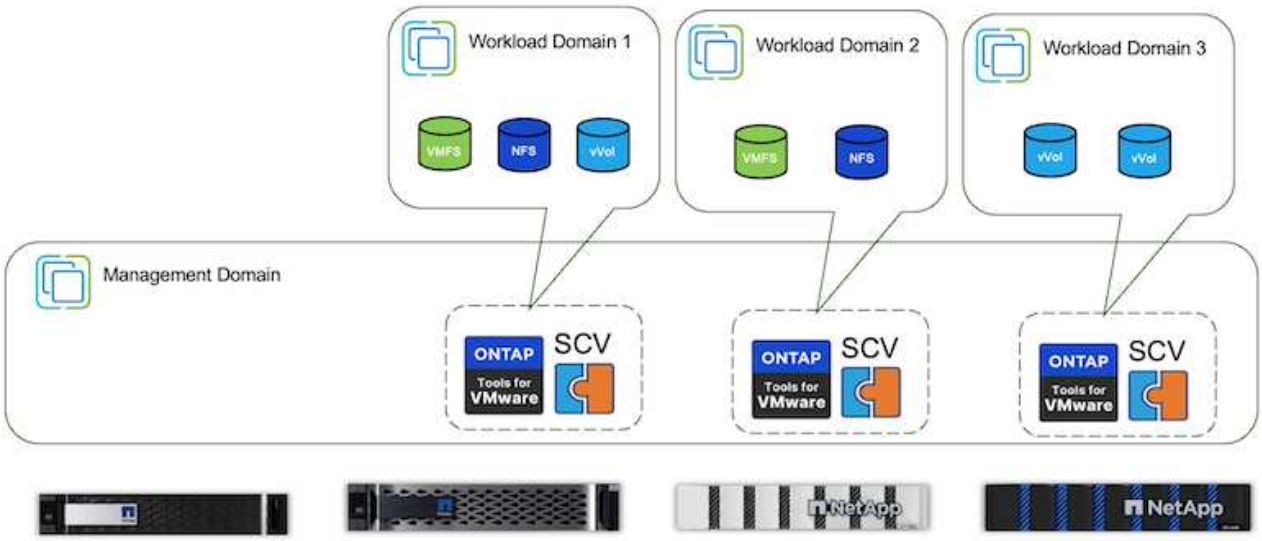
Per la migrazione in blocco delle VM tra datastore vVol, verificare"migrare le VM al datastore ONTAP" .

Esempio di architettura di riferimento

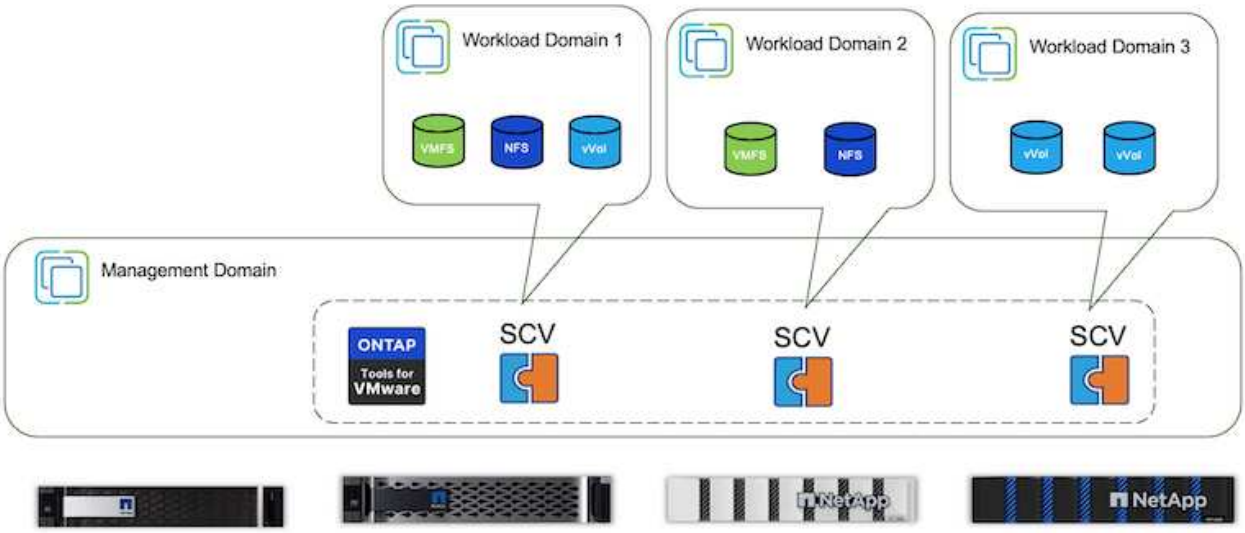
Gli ONTAP tools for VMware vSphere e SCV possono essere installati sullo stesso vCenter che gestiscono o su un server vCenter diverso. È meglio evitare di ospitare sul datastore vVol che gestisce.



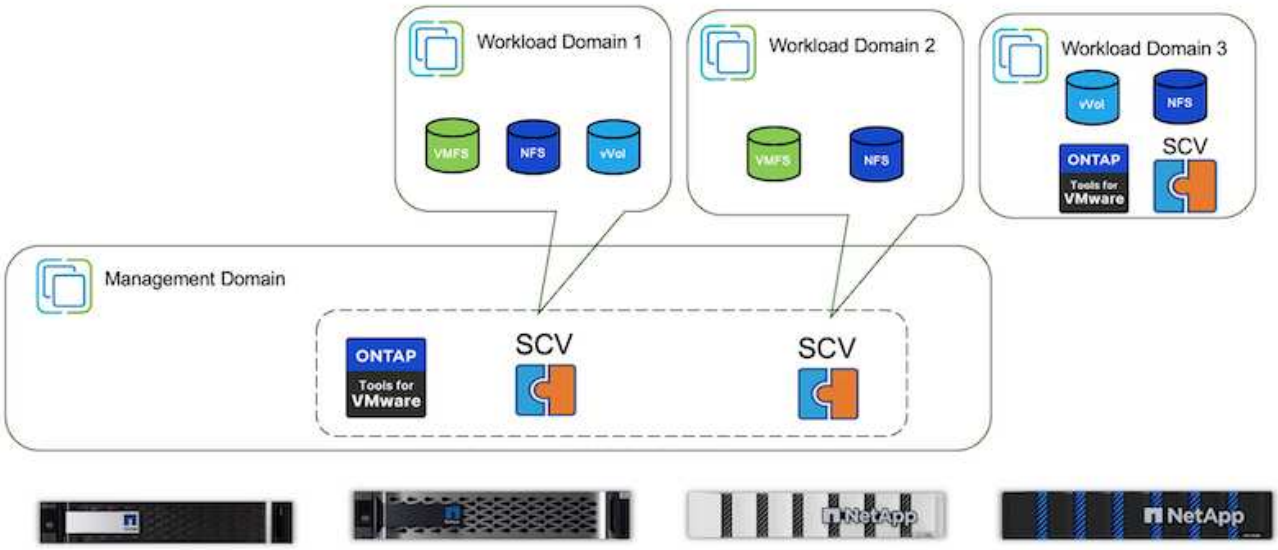
Poiché molti clienti ospitano i propri server vCenter su un server diverso da quello che gestiscono, si consiglia un approccio simile anche per gli strumenti ONTAP e SCV.



Con gli strumenti ONTAP 10.x, una singola istanza può gestire più ambienti vCenter. I sistemi di storage vengono registrati a livello globale con credenziali di cluster e le SVM vengono assegnate a ciascun server vCenter tenant.



È supportato anche il mix di modelli dedicati e condivisi.



Come iniziare

Se gli strumenti ONTAP non sono installati nel tuo ambiente, scaricali da"Sito di supporto NetApp" e seguire le istruzioni disponibili su"utilizzo di vVols con ONTAP" .

Raccogli dati con Virtual Machine Data Collector

Scopri come valutare la tua infrastruttura VMware utilizzando Virtual Machine Data Collector

Virtual Machine Data Collector (VMDC) è uno strumento gratuito e leggero con un’interfaccia grafica utente progettata per gli ambienti VMware. Raccoglie dati di

inventario e prestazioni su VM, host, storage e reti, offrendo informazioni utili per l'ottimizzazione delle risorse e la pianificazione della capacità.

Introduzione

Virtual Machine Data Collector (VMDC) è un toolkit gratuito, leggero e semplice basato su GUI per ambienti VMware che consente agli utenti di raccogliere informazioni di inventario dettagliate sulle proprie macchine virtuali (VM), host, storage e reti.

Per ulteriori informazioni su Virtual Machine Data Collector, vedere"Documentazione del raccoglitore dati della macchina virtuale" .

Capacità VMDC

VMDC è solo un trampolino di lancio per raccogliere statistiche rapide e istantanee per la proiezione delle possibilità di ottimizzazione per le licenze core VMWare insieme a vCPU e RAM. NetApp Data Infrastructure Insights , che richiede l'installazione di AU e collettori di dati, dovrebbe essere il passo successivo ovvio per comprendere la topologia dettagliata delle VM, il raggruppamento delle VM tramite annotazione, in modo da dimensionare correttamente i carichi di lavoro e rendere l'infrastruttura a prova di futuro.

Campionamento delle metriche raccolte con VMDC:

- Informazioni sulla macchina virtuale
  - Nome della macchina virtuale
  - Stato di alimentazione della VM
  - Informazioni sulla CPU della VM
  - Informazioni sulla memoria della VM
  - Posizione della macchina virtuale
  - Informazioni sulla rete VM
  - e altro ancora
- Prestazioni della VM
  - Dati sulle prestazioni per le VM all'intervallo selezionato
  - Informazioni di lettura/scrittura della VM
  - Informazioni IOPS VM
  - Latenza della VM
  - e altro ancora
- Informazioni sull'host ESXi
  - Informazioni sul datacenter host
  - Informazioni sul cluster host
  - Informazioni sul modello host
  - Informazioni sulla CPU host
  - Informazioni sulla memoria host
  - e altro ancora

Raccoglitore dati macchina virtuale (VMDC)

Virtual Machine Data Collector (VMDC) è un toolkit gratuito, leggero e semplice basato su GUI per ambienti VMware che consente agli utenti di raccogliere informazioni di inventario dettagliate sulle proprie macchine virtuali (VM), host, storage e reti.

Questa è una versione di anteprima di VMDC.

Panoramica

La funzione principale di VMDC è la segnalazione della configurazione di vCenter, dei server ESXi e delle macchine virtuali (VM) che risiedono in un ambiente vSphere, inclusi i dati di configurazione del cluster, di rete, di storage e sulle prestazioni. Una volta raccolti dati ambientali completi, è possibile utilizzarli per produrre informazioni approfondite sull'infrastruttura. La visualizzazione dell'output del report è un'interfaccia grafica utente (GUI) in stile foglio di calcolo con più schede per le varie sezioni. Fornisce report di facile lettura e aiuta a ottimizzare l'utilizzo delle risorse e a pianificare la capacità.

VMDC è solo un trampolino di lancio per raccogliere statistiche rapide e istantanee per la proiezione delle possibilità di ottimizzazione per le licenze core VMWare insieme a vCPU e RAM. "Data Infrastructure Insights NetApp" che richiede l'installazione di AU e collettori di dati dovrebbe essere il passo successivo ovvio per comprendere la topologia dettagliata delle VM, il raggruppamento delle VM tramite annotazione in modo da dimensionare correttamente i carichi di lavoro e rendere l'infrastruttura a prova di futuro.

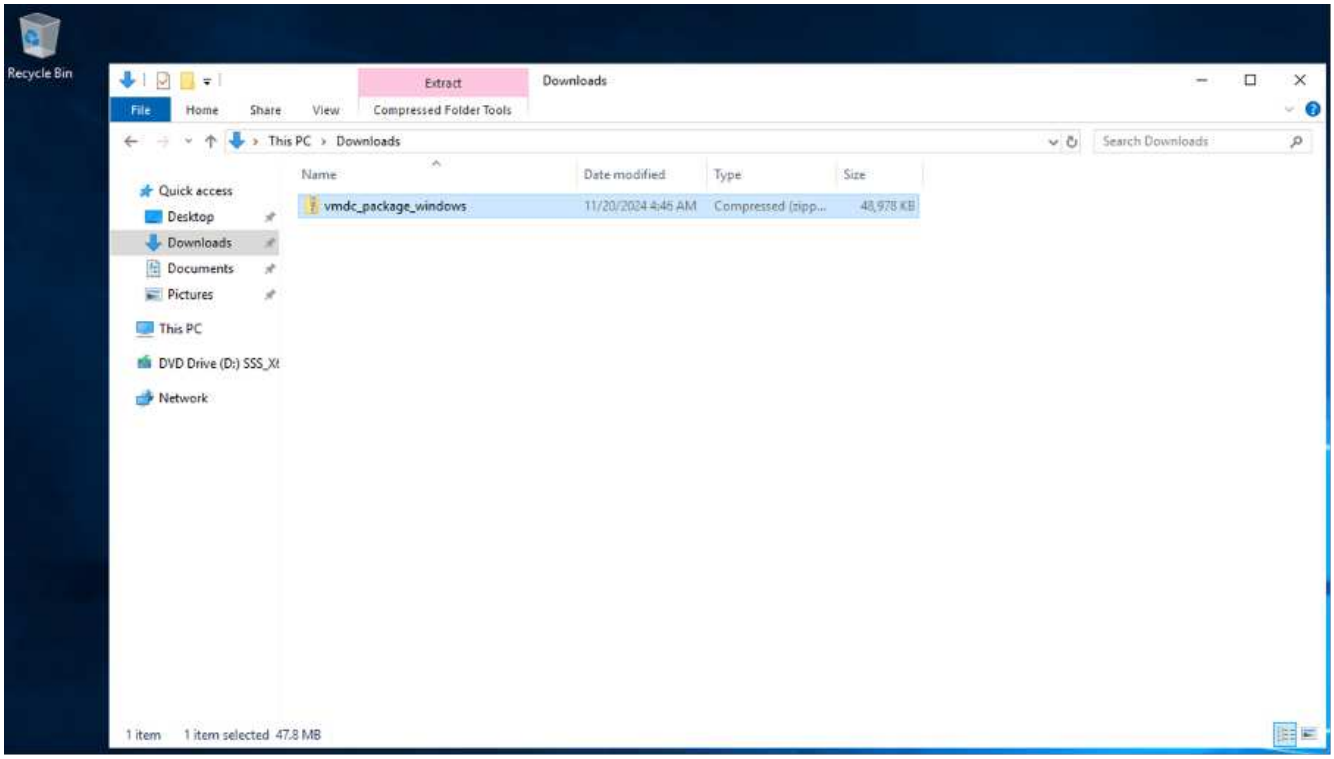
VMDC può essere scaricato"Qui" ed è disponibile solo per i sistemi Windows.

Installazione e configurazione di VMDC

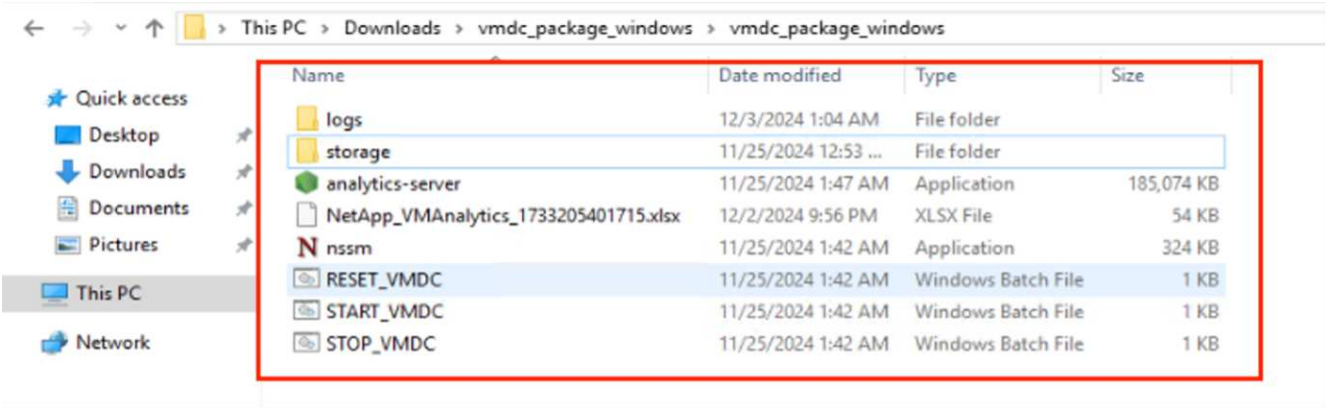
VMDC può essere eseguito su Windows versione 2019 e 2022. Il prerequisito è disporre di connettività di rete dall'istanza VMDC ai server vCenter designati. Una volta verificato, scarica il pacchetto VMDC da"NetApp Toolchest" quindi decomprimere il pacchetto ed eseguire il file batch per installare e avviare il servizio.

Una volta installato VMDC, accedere all'interfaccia utente utilizzando l'indirizzo IP indicato durante l'installazione. Verrà visualizzata l'interfaccia di accesso VMDC, dove è possibile aggiungere vCenter immettendo l'indirizzo IP o il nome DNS e le credenziali di un vCenter Server.

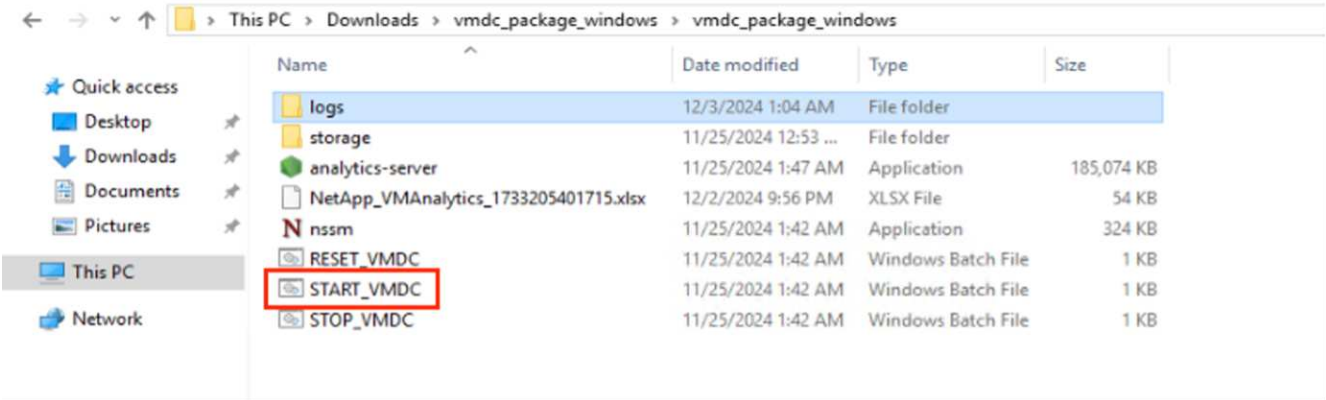
1. Scaricamento"Pacchetto VMDC" .



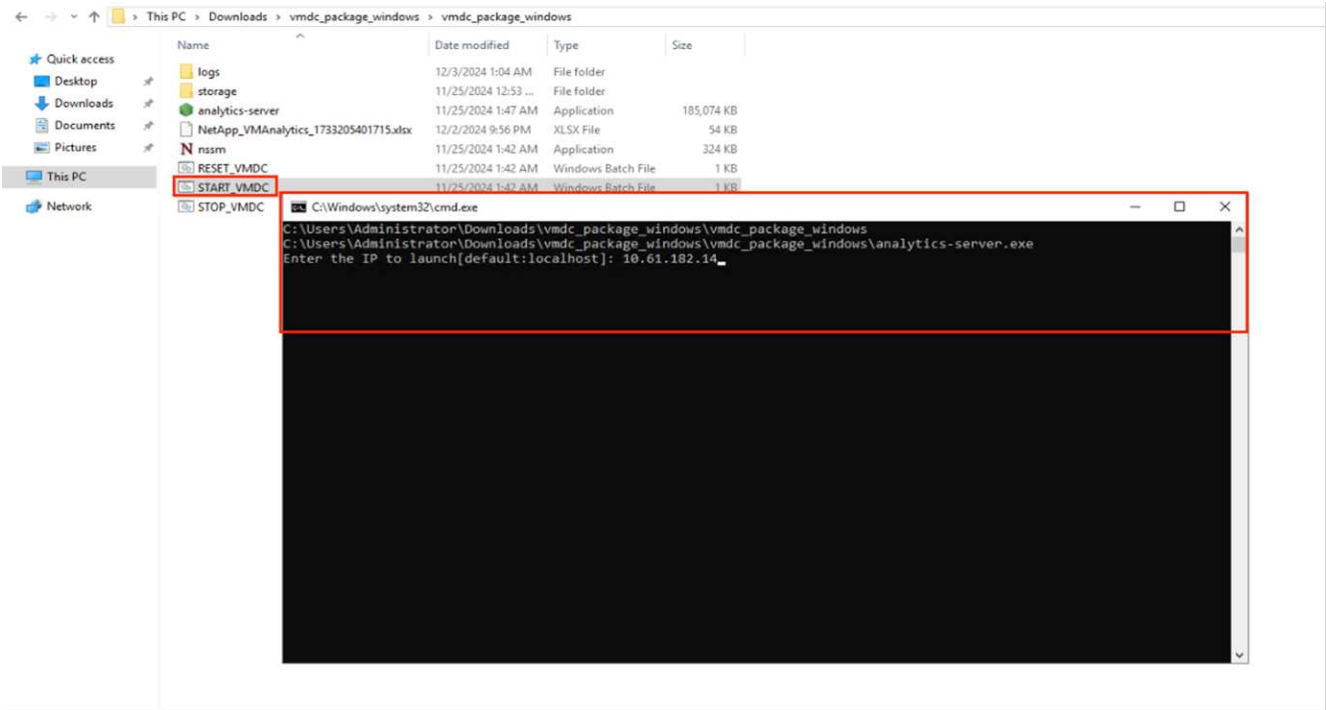
2. Estrarre il pacchetto nella cartella designata.

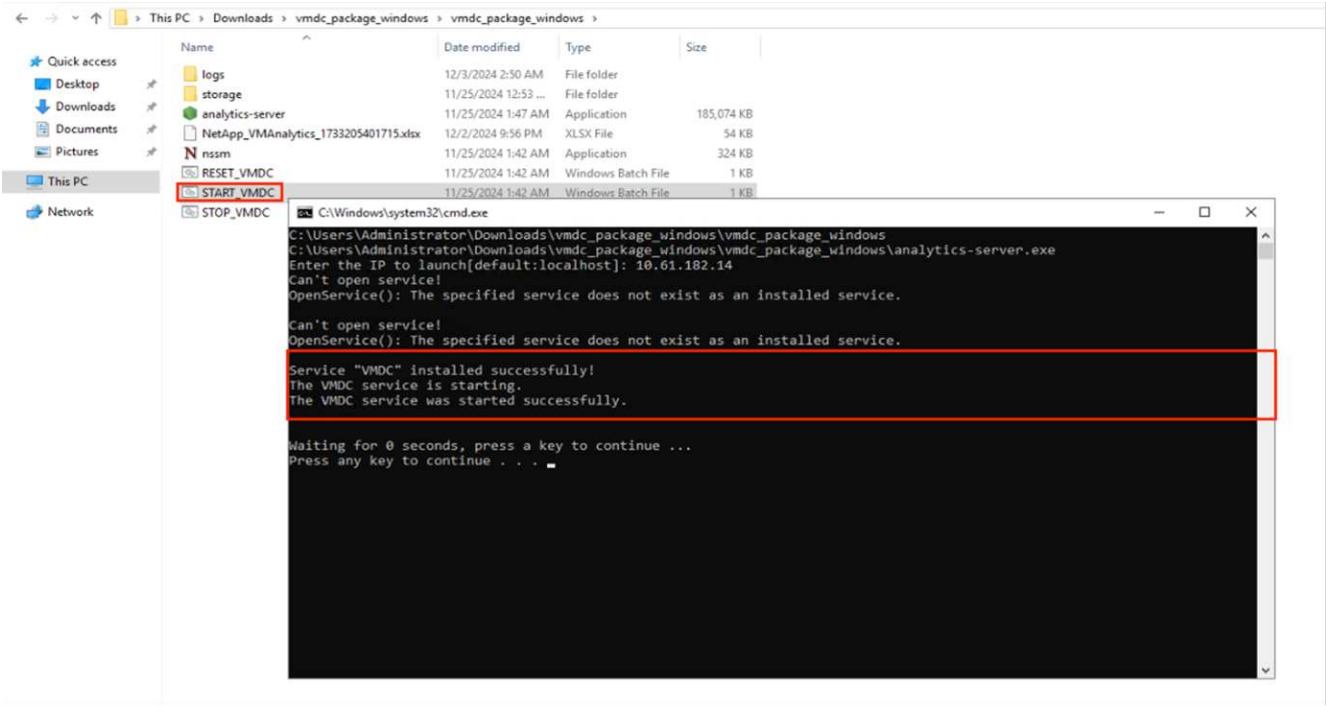


3. Eseguire il pacchetto VMDC facendo clic sul file batch Start_VMDC. Verrà aperto il prompt dei comandi e verrà richiesto di immettere l'indirizzo IP.

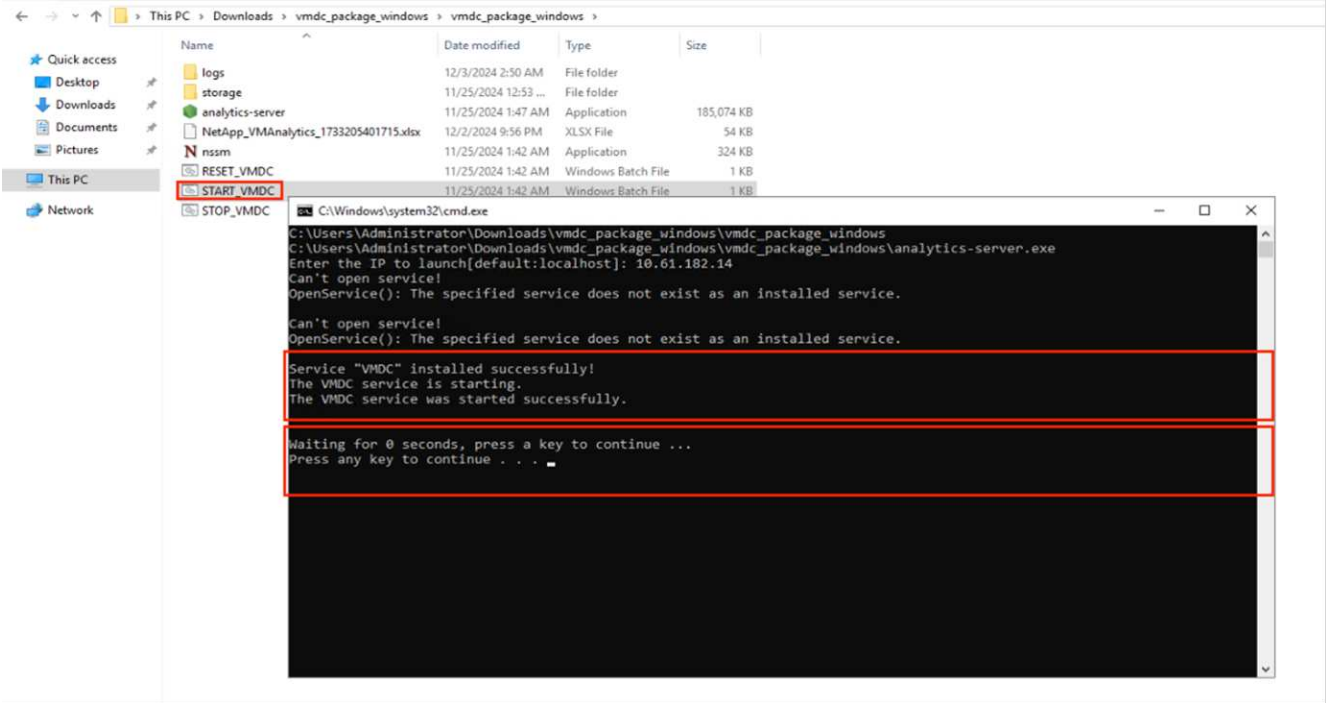


4. Il programma di installazione avvierà il processo di installazione e il servizio VMDC.



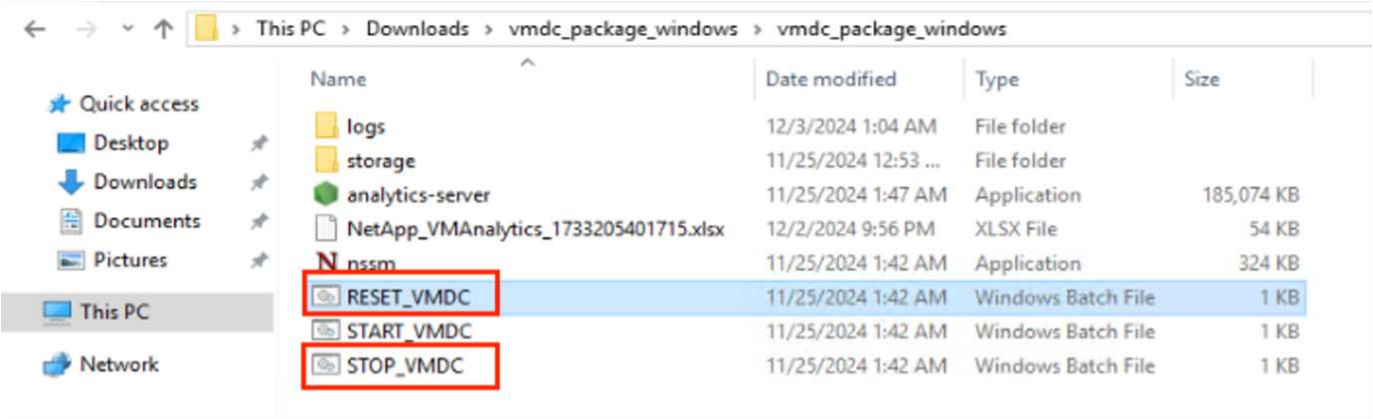


5. Una volta fatto, "Premi un tasto qualsiasi per continuare" per chiudere il prompt dei comandi.



Per interrompere la raccolta dei dati, fare clic sul file batch Stop_VMDC.

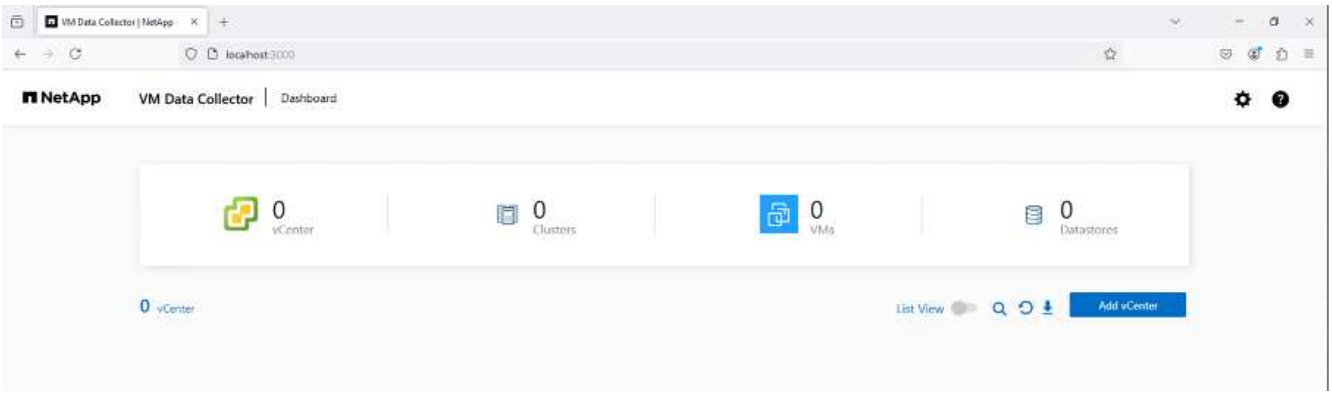
Per rimuovere i dati raccolti e reimpostare VMDC, eseguire il file batch reset_VMDC. Tieni presente che l'esecuzione di reset bat file eliminerà tutti i dati esistenti e ripartirà da zero.



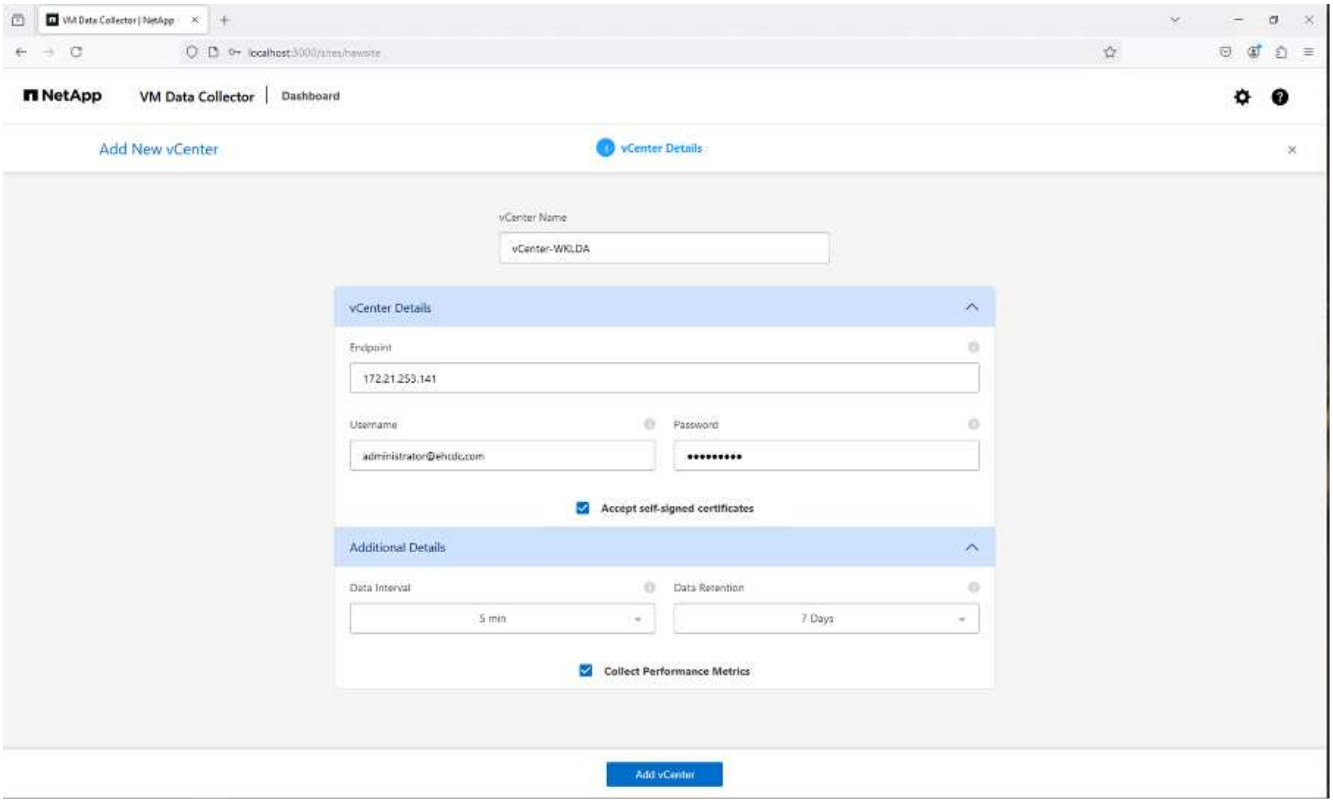
Utilizzo della GUI

Esegui VMDC

- Utilizzando il browser, accedi all'interfaccia utente di VMDC



- Aggiungere il vCenter designato utilizzando l'opzione "Aggiungi vCenter"
  - Nome vCenter: fornire un nome per vCenter
  - Endpoint: immettere l'indirizzo IP o il nome di dominio completo del server vCenter
  - Nome utente: nome utente per accedere a vCenter (in formato UPN: nomeutente@dominio.com)
  - Password
- Modificare i "Dettagli aggiuntivi" in base ai requisiti
  - Intervallo dati: specifica l'intervallo di tempo di aggregazione del campione. Il valore predefinito è 5 minuti, ma può essere modificato in 30 secondi o 1 minuto, a seconda delle esigenze.
  - Conservazione dei dati: specifica il periodo di conservazione per archiviare le metriche storiche.
  - Raccogli metriche sulle prestazioni: se abilitata, raccoglie le metriche sulle prestazioni per ogni VM. Se non selezionato, VMDC fornisce funzionalità simili a RVtools, fornendo solo i dettagli della VM, dell'host e del datastore.
- Una volta fatto, clicca su "Aggiungi vCenter"



La raccolta dei dati inizia immediatamente dopo l'aggiunta di vCenter. Non è necessario pianificare un orario per la raccolta, poiché il processo recupererebbe i dati disponibili nel database vCenter e inizierebbe ad aggregarli in base all'"intervallo di tempo dei dati" specificato.

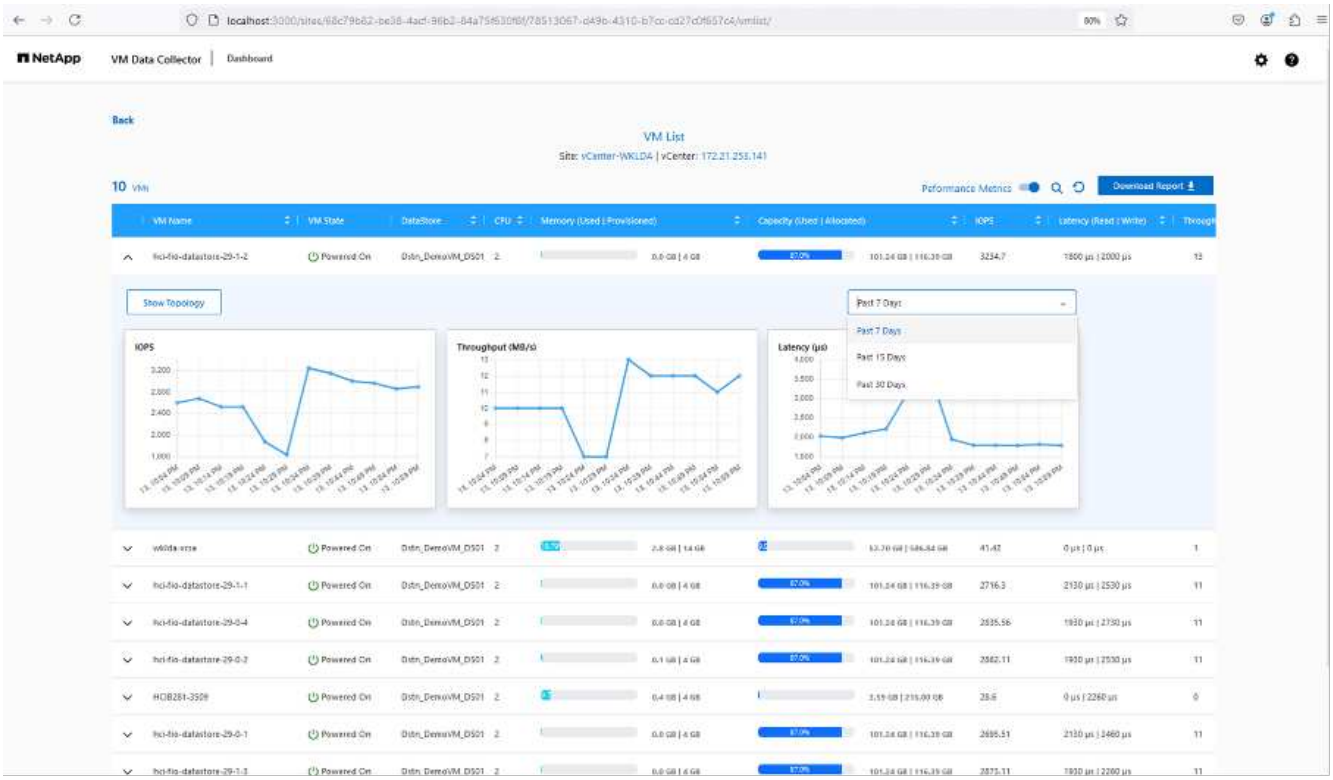
Per visualizzare i dati di un vCenter specifico, andare alla dashboard e fare clic su "Visualizza inventario" accanto al nome del vCenter appropriato. La pagina visualizzerà l'inventario delle VM insieme ai relativi attributi. Per impostazione predefinita, "Performance Metrics" è disabilitato nell'interfaccia utente, ma può essere attivato tramite l'opzione di attivazione/disattivazione. Una volta abilitate le metriche delle prestazioni, verranno visualizzati i dati sulle prestazioni per ogni VM. Per informazioni sulle performance dal vivo, clicca sul pulsante Aggiorna.

Visualizza la topologia della VM

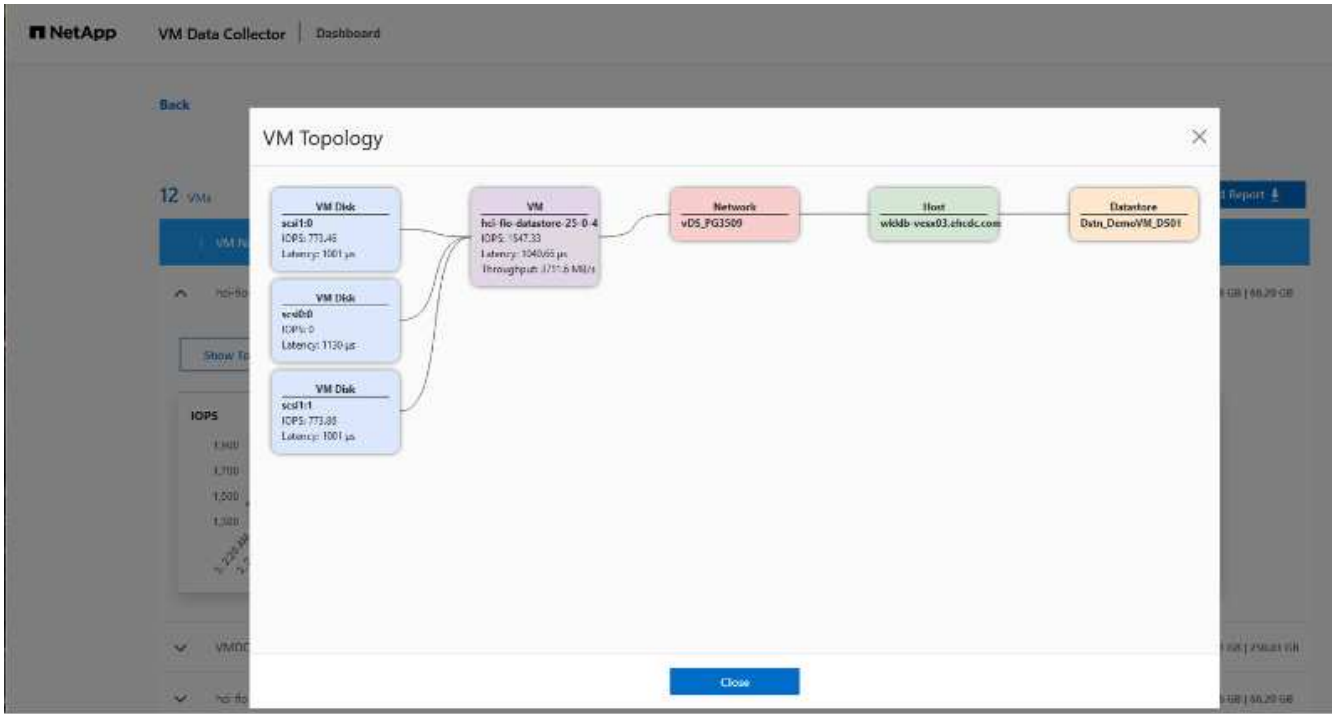
VMDC fornisce l'opzione "Mostra topologia" per ogni VM, che fornisce un'interfaccia interattiva per visualizzare le risorse e le relative relazioni rispetto al disco della VM, alla VM, all'host ESXi, ai datastore e alle reti. Aiuta a gestire e monitorare con informazioni approfondite dai dati sulle prestazioni raccolti. La topologia aiuta a eseguire diagnosi di base e a risolvere problemi utilizzando i dati correnti. Per una risoluzione dei problemi dettagliata e un MTTR rapido, utilizzare"Data Infrastructure Insights NetApp" che fornisce una vista topologica dettagliata con mappatura delle dipendenze end-to-end.

Per accedere alla vista topologica, seguire i passaggi seguenti:

- Accedi alla dashboard VMDC.
- Selezionare il nome del vCenter e fare clic su "Visualizza inventario".



- Selezionare la VM e fare clic su "Mostra topologia".

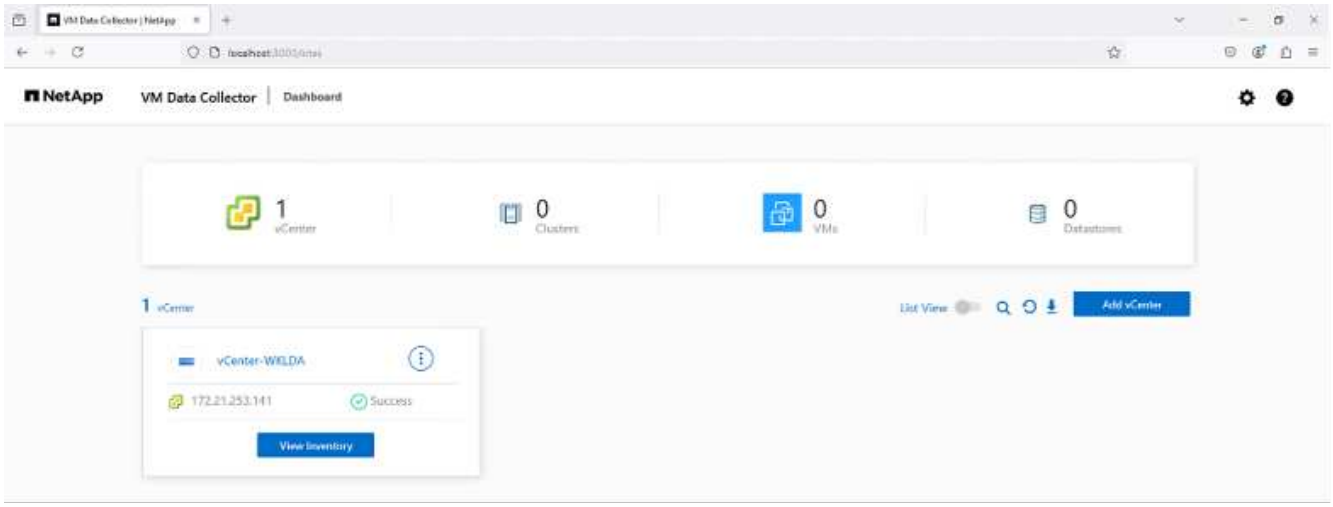


Esporta in Excel

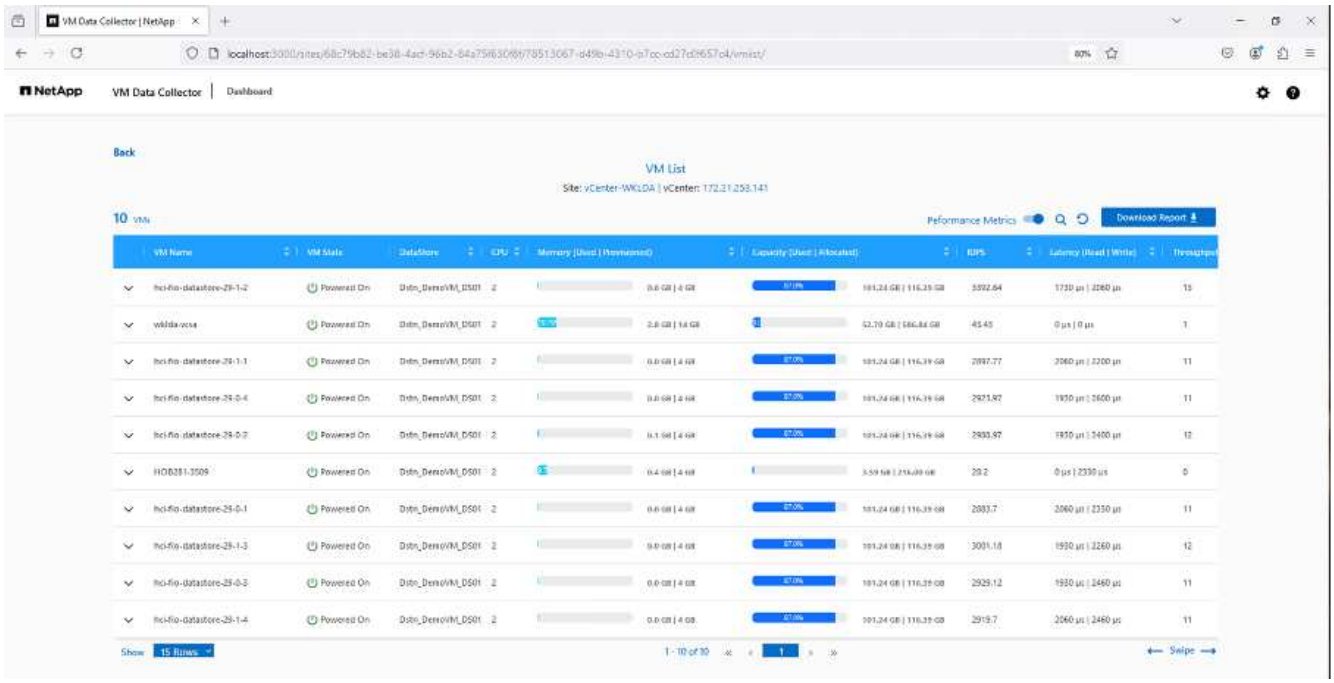
Per acquisire i dati raccolti in un formato utilizzabile, utilizzare l'opzione "Scarica report" per scaricare il file XLSX.

Per scaricare il report, seguire i passaggi seguenti:

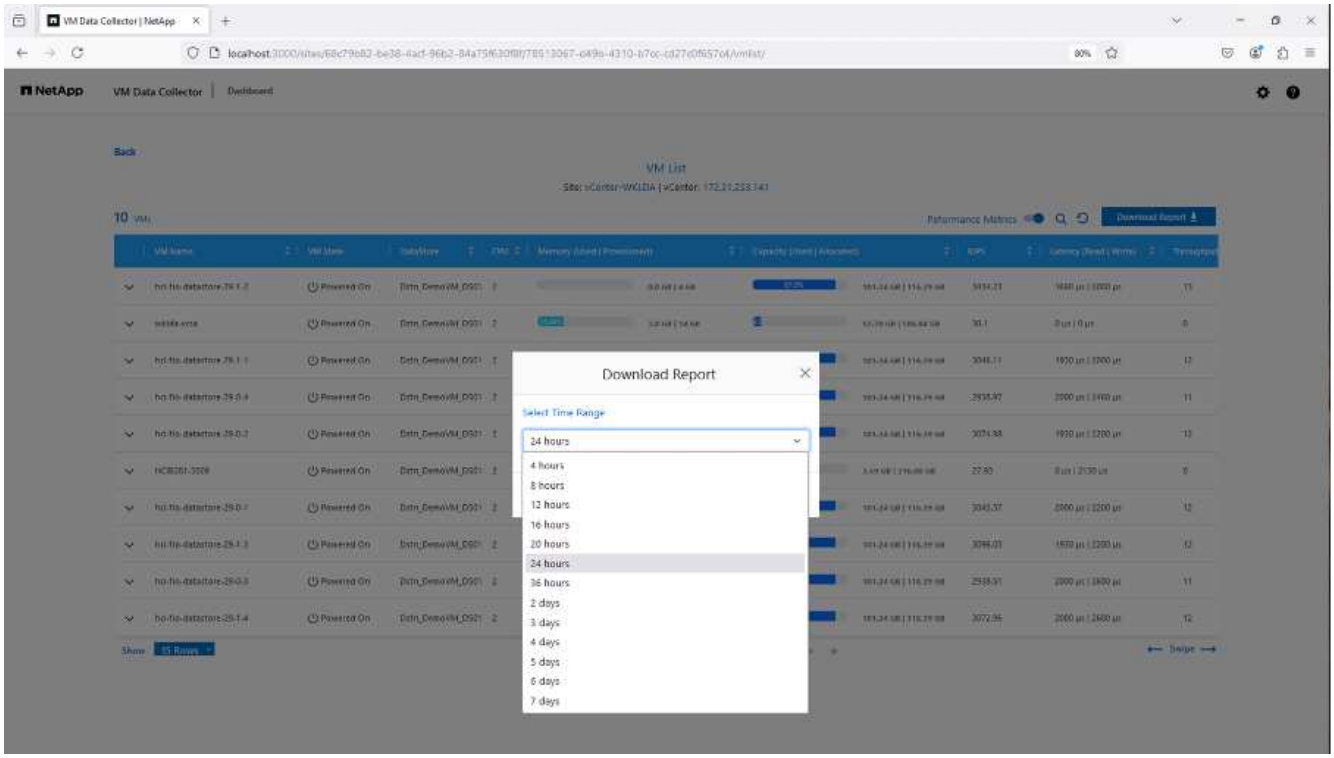
- Accedi alla dashboard VMDC.
- Selezionare il nome del vCenter e fare clic su "Visualizza inventario".



- Seleziona l'opzione "Scarica rapporto"



- Seleziona l’intervallo di tempo. L’intervallo di tempo offre molteplici opzioni, da 4 ore a 7 giorni.



Ad esempio, se i dati richiesti riguardano le ultime 4 ore, selezionare 4 oppure selezionare il valore appropriato per acquisire i dati per quel dato periodo. I dati generati vengono aggregati in modo continuo. Quindi, seleziona l’intervallo di tempo per garantire che il report generato catturi le statistiche necessarie sul carico di lavoro.

Contatori dati VMDC

Una volta scaricato, il primo foglio visualizzato da VMDC è "VM Info", un foglio che contiene informazioni sulle VM che risiedono nell’ambiente vSphere. Vengono visualizzate informazioni generiche sulle macchine virtuali:

nome della VM, stato di alimentazione, CPU, memoria fornita (MB), memoria utilizzata (MB), capacità fornita (GB), capacità utilizzata (GB), versione degli strumenti VMware, versione del sistema operativo, tipo di ambiente, data center, cluster, host, cartella, datastore primario, dischi, schede di rete, ID VM e UUID VM.

La scheda "Prestazioni VM" acquisisce i dati sulle prestazioni per ciascuna VM campionata al livello di intervallo selezionato (l'impostazione predefinita è 5 minuti). Il campione di ciascuna macchina virtuale comprende: IOPS di lettura medi, IOPS di scrittura medi, IOPS medi totali, IOPS di lettura di picco, IOPS di scrittura di picco, IOPS di picco totali, throughput di lettura medio (KB/s), throughput di scrittura medio (KB/s), throughput medio totale (KB/s), throughput di lettura di picco (KB/s), throughput di scrittura di picco (KB/s), throughput di picco totale (KB/s), latenza di lettura media (ms), latenza di scrittura media (ms), latenza media totale (ms), latenza di lettura di picco (ms), latenza di scrittura di picco (ms) e latenza di picco totale (ms).

La scheda "Informazioni host ESXi" per ciascun host acquisisce: Datacenter, vCenter, Cluster, SO, Produttore, Modello, Socket CPU, Core CPU, Velocità di clock di rete (GHz), Velocità di clock CPU (GHz), Thread CPU, Memoria (GB), Memoria utilizzata (%), Utilizzo CPU (%), Numero di VM guest e Numero di NIC.

Prossimi passi

Utilizzare il file XLSX scaricato per esercizi di ottimizzazione e refactoring.

Descrizione degli attributi VMDC

Questa sezione del documento riguarda la definizione di ciascun contatore utilizzato nel foglio Excel.

Scheda informativa VM

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
CPUs	The number of vCPUs provisioned on the Guest Virtual Machine
Memory Provisioned (MB)	The Memory Provisioned on the Guest Virtual Machine. Units MB
Memory Utilized (MB)	Active Memory Utilized by the Guest Virtual Machine during the phase of metrics collection. Units MB
Capacity Provisioned (GB)	Total Capacity of the Virtual Disks provisioned on the Guest Virtual Machine. Units GB
Capacity Utilized (GB)	Total Utilized Virtual Disks capacity on the Guest Virtual Machine. Units GB
VMware tools version	Version of the Vmware Tools installed on the Guest Virtual machine
OS Version	The Operating System installed on the Guest Virtual Machine
Environment Type	
Datacenter	Name of the Datacenter containing the Guest Virtual Machine
Cluster	Name of the Cluster containing the Guest Virtual Machine
Host	Name of the ESXi Server on which the Guest Virtual Machine is hosted
Folder	Name of the folder under the VMs Tab containing the Guest Virtual Machine
Primary Datastore	Name of the Datastore on which the Guest Virtual Machine's disks reside
Disks	Number of Virtual Disks connected to the Guest Virtual Machine
NICs	Number of Virtual Network Interface connections to the Guest Virtual Machine
VM ID	The Guest Virtual Machine Identifier String within the scope of vCenter Server Monitoring
VM UUID	The Unique Identifier value for the Guest Virtual Machine

Scheda delle prestazioni della VM

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
Number of CPUs	Number of vCPUs provisioned on the Guest Virtual Machine
Average CPU (%)	Average vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Peak CPU (%)	Maximum vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Average Read IOPS	Average read IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Write IOPS	Average Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Average IOPS	Combined Average Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Read IOPS	Maximum Read IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Write IOPS	Maximum Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Peak IOPS	Combined Maximum Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Read Throughput (KB/s)	Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Write Throughput (KB/s)	Average rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Average Throughput (KB/s)	Combined Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Read Throughput (KB/s)	Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Write Throughput (KB/s)	Peak rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Peak Throughput (KB/s)	Combined Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Read Latency (ms)	Average Read latency for the Guest Virtual Machine. Units milliseconds
Average Write Latency (ms)	Average Write latency for the Guest Virtual Machine. Units milliseconds
Total Average Latency (ms)	Combined Average Read & Write latency for the Guest Virtual Machine. Units milliseconds
Peak Read Latency (ms)	Maximum Read latency for the Guest Virtual Machine. Units milliseconds
Peak Write Latency (ms)	Maximum Write latency for the Guest Virtual Machine. Units milliseconds
Total Peak Latency (ms)	Combined Maximum Read & Write latency for the Guest Virtual Machine. Units milliseconds

Informazioni sull'host ESXi

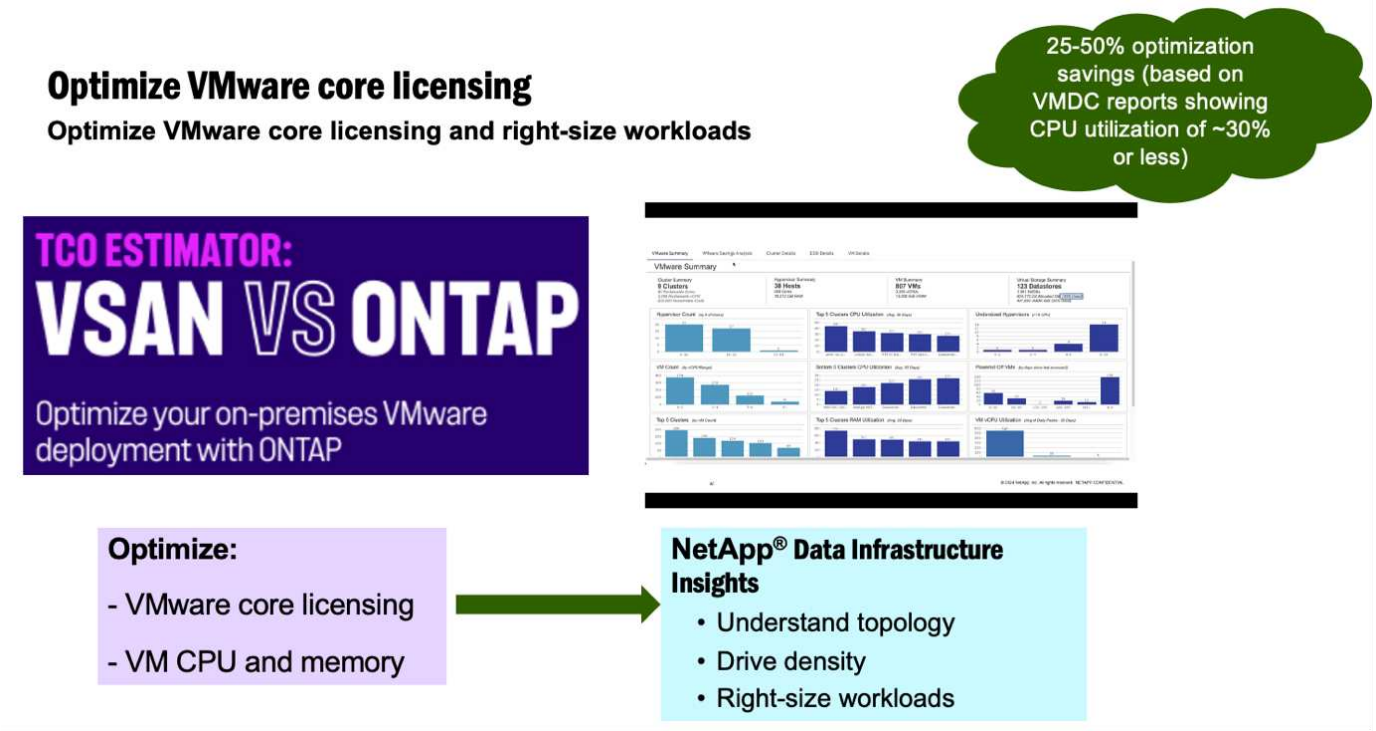
Counter Name	Counter Description
Host	Hostname of the ESXi Hypervisor Server
Datacenter	Virtual DataCenter Name under which the ESXi Hypervisor Hosts exists
vCenter	Version of the VMware vCenter Server used to Manage & Monitor the ESXi Hosts
Cluster	Name of the Cluster under which the ESXi Hypervisor Hosts exists
OS	Version of VMware ESXi Hypervisor that is installed on the Host / Server
Manufacturer	Vendor Company name of the Physical Server of the Host
Model	Server Model / Model Number of the Physical Server
CPU Sockets	Total number of CPU Sockets installed on the Physical Server
CPU Cores	Total number of Cores across all CPU Sockets installed on the Physical Server
CPU Description	Vendor Company & Model Information of the CPU Type installed on the Physical Server
Net Clock Speed (GHz)	Sum of CPU Clock Speed of all CPU cores running on the Physical Server. Units GHz
CPU Clock Speed (GHz)	Clock Speed of each CPU core running on the Physical Server. Units GHz
CPU Threads	Total Number of threads supported for all Cores on the Physical Server
Memory (GB)	Total RAM installed on the Physical Server. Units GB
Memory Used (%)	Percentage of Memory Used on the Physical Server / Host
CPU usage (%)	Percentage of CPU Used on the Physical Server / Host
Guest VM Count	Total Number of Guest Virtual Machines running on the Physical Server / Host
Number of NICs	Total Number of Network Interface Connection Ports on the Physical Hypervisor Server / Host

Conclusione

Con le imminenti modifiche alle licenze, le organizzazioni stanno affrontando in modo proattivo il potenziale aumento del costo totale di proprietà (TCO). Stanno ottimizzando strategicamente la loro infrastruttura VMware attraverso una gestione aggressiva delle risorse e un dimensionamento corretto per migliorare l'utilizzo delle risorse e semplificare 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 complessive di licenza. VMDC offre la possibilità di raccogliere rapidamente dati VM che possono essere suddivisi per creare report e ottimizzare l'ambiente esistente.

Utilizzando VMDC, esegui una valutazione rapida per individuare le risorse sottoutilizzate e quindi utilizza NetApp Data Infrastructure Insights (DII) per fornire analisi dettagliate e raccomandazioni per il recupero delle VM. Ciò consente ai clienti di comprendere i potenziali risparmi sui costi e l'ottimizzazione durante l'implementazione e la configurazione di NetApp Data Infrastructure Insights (DII). NetApp Data Infrastructure Insights (DII) può aiutare le aziende a prendere decisioni informate sull'ottimizzazione del loro ambiente VM. È in grado di identificare dove è possibile recuperare risorse o dismettere host con un impatto minimo sulla produzione, aiutando le aziende a gestire i cambiamenti apportati dall'acquisizione di VMware da parte di Broadcom in modo ponderato e strategico. In altre parole, VMDC e DII, in quanto meccanismi di analisi dettagliata, aiutano le aziende a eliminare l'aspetto emotivo dalle decisioni. Invece di reagire ai cambiamenti con panico o frustrazione, possono utilizzare le informazioni fornite da questi due strumenti per prendere decisioni razionali e strategiche che bilancino l'ottimizzazione dei costi con l'efficienza operativa e la produttività.

Con NetApp, ridimensiona correttamente i tuoi ambienti virtualizzati e introduci prestazioni di storage flash convenienti, insieme a soluzioni semplificate per la gestione dei dati e il ransomware, per garantire che le organizzazioni siano pronte per il nuovo modello di abbonamento, ottimizzando al contempo le risorse IT attualmente disponibili.



Prossimi passi

Scarica il pacchetto VMDC e raccogli i dati e utilizzali"Stimatore TCO vSAN" per una facile proiezione e quindi utilizzare"DII" per fornire costantemente l'intelligence, influenzando l'IT ora e in futuro, per garantire che possa adattarsi alle nuove esigenze che emergono.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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