VMware Cloud Foundation su NetApp

NetApp virtualization solutions

NetApp
August 24, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html on August 24, 2025. Always check docs.netapp.com for the latest.

Sommario

VMware Cloud Foundation su NetApp . . . 1
- Semplifica l'esperienza del cloud ibrido con VMware Cloud Foundation e ONTAP . . . 1
- Introduzione . . . 1
  - Introduzione a NetApp ONTAP . . . 1
  - Introduzione a VMware Cloud Foundation . . . 1
  - Domini VCF . . . 1
  - Archiviazione con VCF . . . 2
  - Perché ONTAP per VCF . . . 3
  - Informazioni aggiuntive: . . . 4
  - Riepilogo . . . 5
  - Risorse di documentazione . . . 5
- Opzioni di progettazione con VMware Cloud Foundation e ONTAP . . . 6
  - Opzioni di archiviazione . . . 6
  - Progetti . . . 6
- Configurare ambienti cloud privati con VMware Cloud Foundation e ONTAP . . . 11
  - Distribuisci una nuova istanza VCF 9 . . . 11
  - Convergere i componenti esistenti in VCF 9 . . . 13
  - Aggiorna un ambiente VCF esistente a VCF 9 . . . 14
- Implementazione del Disaster Recovery con NetApp SnapMirror e BlueXP DRaaS . . . 14
  - Iniziare . . . 15
  - Configurazione BlueXP disaster recovery . . . 17
  - Configurazione della replica di archiviazione tra l'array del sito di origine e l'array del sito di destinazione . . . 17
  - Come configurarlo per VMware Disaster Recovery . . . 18
  - Cosa può fare per te il BlueXP disaster recovery ? . . . 18
  - Failover di prova . . . 23
  - Operazione di test di failover di pulizia . . . 25
  - Migrazione pianificata e failover . . . 26
  - Rifasamento . . . 27
  - Monitoraggio e dashboard . . . 29
- Convertire i cluster vSphere esistenti in VCF . . . 30
  - Scopri come convertire un ambiente vSphere con datastore esistenti in VCF . . . 30
  - Convertire l'istanza del server vCenter in dominio di gestione VCF (datastore NFS) . . . 30
  - Convertire l'istanza del server vCenter in dominio di gestione VCF (datastore FC) . . . 44
- Fornire VCF con storage principale . . . 58
  - Fornire un ambiente VCF con ONTAP come soluzione di archiviazione principale . . . 58
  - Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per il dominio di gestione VCF . . . 58
  - Utilizzare un datastore NFS su ONTAP come storage principale per il dominio di gestione VCF . . . 59
  - Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per un dominio di carico di lavoro VI . . . 61
  - Utilizzare un datastore NFS su ONTAP come storage principale per un dominio di carico di lavoro VI . . . 63
- Espandi VCF con spazio di archiviazione supplementare . . . 84

Scopri come espandere lo storage per un ambiente VCF utilizzando storage supplementare . . . 84
Aggiungere un datastore iSCSI come storage supplementare per un dominio di gestione utilizzando gli ONTAP tools for VMware vSphere . . . 84
Aggiungere un datastore VMFS basato su FC come storage supplementare per un dominio di gestione utilizzando gli ONTAP tools for VMware vSphere . . . 108
Aggiungere vVols come storage supplementare ai domini dei carichi di lavoro VI utilizzando gli ONTAP tools for VMware vSphere . . . 109
Aggiungere NFS e vVols come storage supplementare ai domini dei carichi di lavoro VI utilizzando gli ONTAP tools for VMware vSphere . . . 136
Aggiungere NVMe su TCP come storage supplementare ai domini dei carichi di lavoro VI . . . 161
Aggiungere un datastore VMFS basato su FC come storage supplementare ai domini dei carichi di lavoro VI . . . 185
Proteggi VCF con SnapCenter . . . 186
Scopri come proteggere i domini dei carichi di lavoro VCF con il plug-in SnapCenter per VMware vSphere . . . 186
Proteggi un dominio di carico di lavoro VCF con il plug-in SnapCenter per VMware vSphere . . . 187
Proteggere i domini di gestione e carico di lavoro VCF utilizzando il plug-in SnapCenter per VMware vSphere . . . 222
Proteggi i domini dei carichi di lavoro VCF con l'archiviazione NVMe su TCP e il plug-in SnapCenter per VMware vSphere . . . 235
Proteggi i datastore VMware con BlueXP . . . 242
Scopri come proteggere i datastore VMware utilizzando il BlueXP disaster recovery . . . 242
Configura la protezione dei dati 3-2-1 per VMware con il plug-in SnapCenter per il BlueXP backup and recovery . . . 242
Impostare il ripristino di emergenza per i datastore VMFS utilizzando il BlueXP disaster recovery . . . 287
Impostare il ripristino di emergenza per i datastore NFS utilizzando il BlueXP disaster recovery . . . 306
Proteggi i carichi di lavoro con vSphere Metro Storage Cluster . . . 327
Scopri come integrare l'alta disponibilità ONTAP con VMware vSphere Metro Storage Cluster (vMSC) 327
Configurare un cluster esteso per un dominio di gestione VCF utilizzando MetroCluster . . . 328
Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando MetroCluster . . . 339
Configurare un cluster esteso per un dominio di gestione VCF utilizzando SnapMirror Active Sync . . . 351
Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando SnapMirror Active Sync 353
Migrazione delle VM da VMware vSphere ai datastore ONTAP . . . 355
Requisiti di rete . . . 356
Scenari di migrazione delle VM . . . 357
Scenari di migrazione dei modelli di VM . . . 381
Casi d'uso . . . 388
Risorse aggiuntive . . . 389
Protezione autonoma contro i ransomware per l'archiviazione NFS . . . 389
Monitora l'archiviazione on-premise con Data Infrastructure Insights . . . 399
Monitoraggio dell'archiviazione locale con Data Infrastructure Insights . . . 399
Panoramica sulla distribuzione della soluzione . . . 399
Prerequisiti . . . 400
Distribuzione della soluzione . . . 400
Conclusione . . . 417

Informazioni aggiuntive 417

VMware Cloud Foundation su NetApp

Semplifica l’esperienza del cloud ibrido con VMware Cloud Foundation e ONTAP

NetApp ONTAP si integra con VMware Cloud Foundation (VCF) per offrire una soluzione di storage unificata che supporta sia protocolli a blocchi che a file. Questa integrazione semplifica le distribuzioni cloud ibride, migliora la gestione e le prestazioni dei dati e garantisce servizi dati coerenti negli ambienti on-premise e cloud.

Introduzione

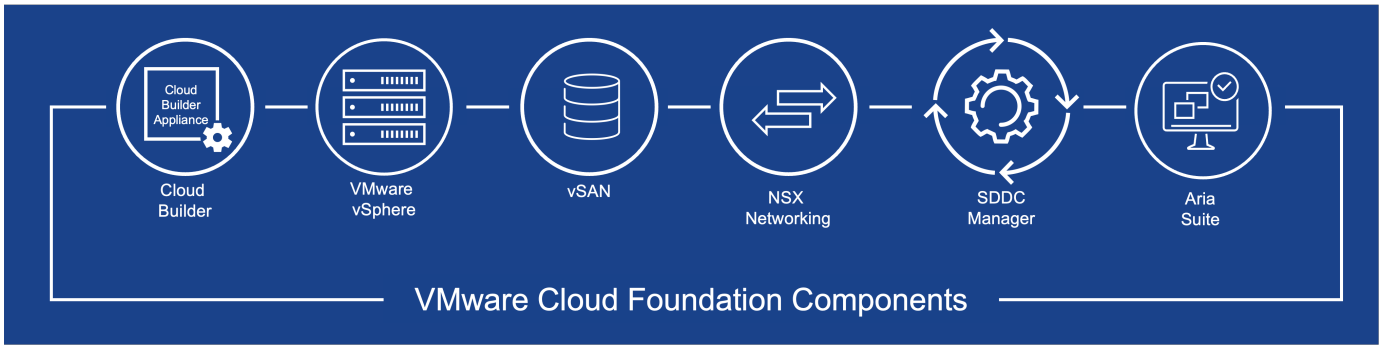
L’utilizzo NetApp con VCF migliora la gestione dei dati e l’efficienza dell’archiviazione tramite le funzionalità avanzate di NetApp, come deduplicazione, compressione e snapshot. Questa combinazione garantisce un’integrazione perfetta, prestazioni elevate e scalabilità per gli ambienti virtualizzati. Inoltre, semplifica le distribuzioni cloud ibride consentendo servizi dati e gestione coerenti tra infrastrutture on-premise e cloud.

Introduzione a NetApp ONTAP

NetApp ONTAP è un software completo per la gestione dei dati che offre funzionalità di storage avanzate su un’ampia gamma di prodotti. ONTAP è disponibile come storage definito dal software, come servizio di prima parte tramite i principali provider cloud e come sistema operativo di storage per le piattaforme NetApp ASA (All San Array), AFF (All-flash FAS) e FAS (Fabric-Attached Storage). ONTAP garantisce elevate prestazioni e bassa latenza per una varietà di casi d’uso, tra cui la virtualizzazione VMware, senza creare silos.

Introduzione a VMware Cloud Foundation

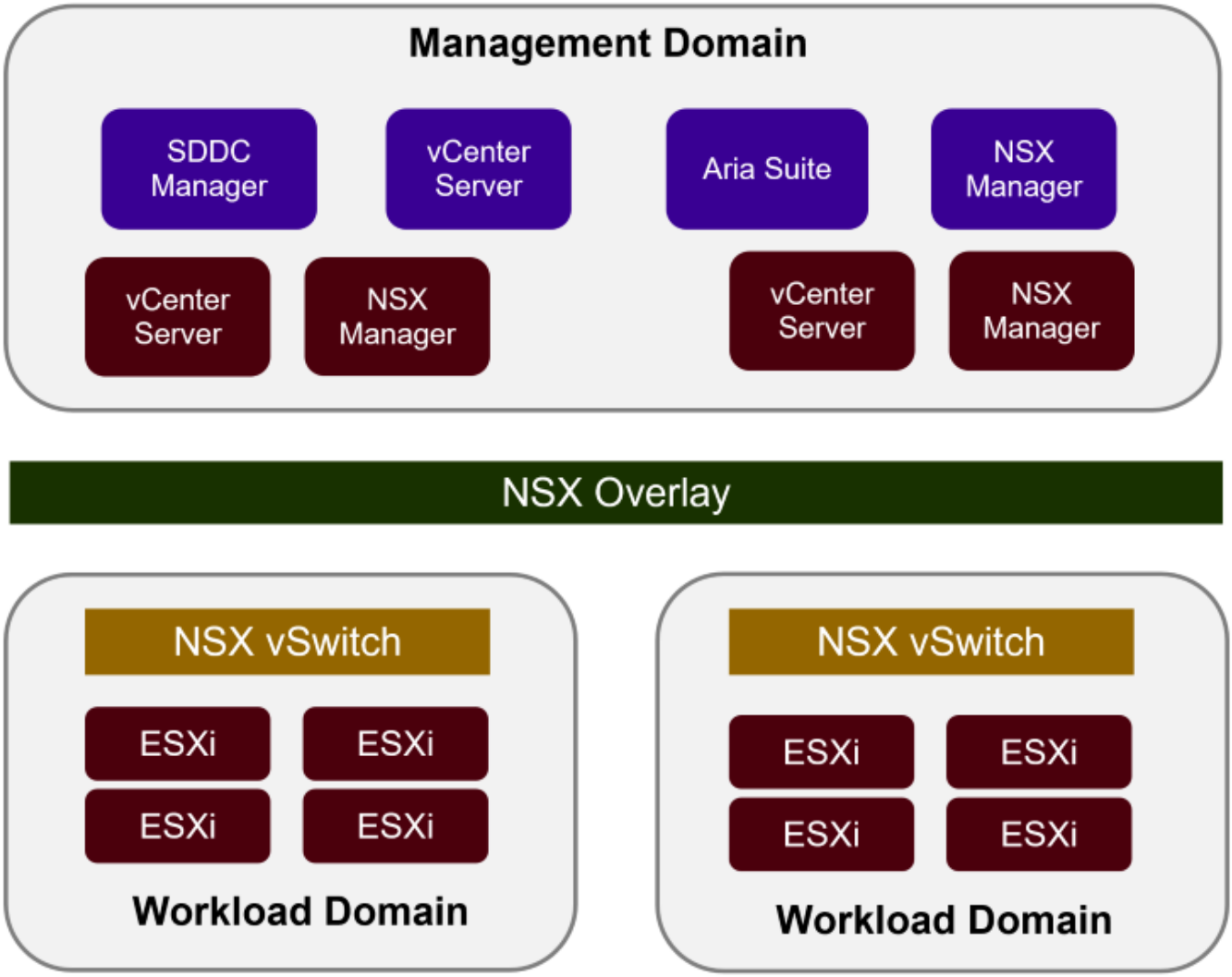
VCF integra le offerte di elaborazione, rete e storage con i prodotti VMware e le integrazioni di terze parti, facilitando sia i carichi di lavoro nativi Kubernetes sia quelli basati su macchine virtuali. Questa piattaforma software include componenti chiave quali VMware vSphere, NSX, Aria Suite Enterprise, Tanzu Kubernetes Grid, HCX Enterprise, SDDC Manager e capacità di archiviazione collegata ai core della CPU host tramite vSAN. NetApp ONTAP si integra perfettamente con una varietà di modelli di distribuzione VCF sia in locale che nel cloud pubblico.



Domini VCF

I domini sono una struttura fondamentale all’interno di VCF che consente di organizzare le risorse in raggruppamenti distinti e indipendenti. I domini aiutano a organizzare l’infrastruttura in modo più efficace, garantendo che le risorse vengano utilizzate in modo efficiente. Ogni dominio è distribuito con i propri elementi

di elaborazione, rete e storage.



Esistono due tipi principali di domini con VCF:

- **Dominio di gestione** – Il dominio di gestione include componenti responsabili delle funzioni principali dell'ambiente VCF. I componenti gestiscono attività essenziali quali provisioning delle risorse, monitoraggio e manutenzione e includono integrazioni di plug-in di terze parti come NetApp ONTAP Tools per VMware. I domini di gestione possono essere distribuiti utilizzando Cloud Builder Appliance per garantire il rispetto delle best practice, oppure è possibile convertire un ambiente vCenter esistente in un dominio di gestione VCF.
- **Dominio del carico di lavoro dell'infrastruttura virtuale** – I domini del carico di lavoro dell'infrastruttura virtuale sono progettati per essere pool di risorse dedicate a una specifica esigenza operativa, carico di lavoro o organizzazione. I domini dei carichi di lavoro vengono distribuiti facilmente tramite SDDC Manager, contribuendo ad automatizzare una serie di attività complesse. È possibile eseguire il provisioning fino a 24 domini di carico di lavoro in un ambiente VCF, ognuno dei quali rappresenta un'unità di infrastruttura pronta per l'applicazione.

Archiviazione con VCF

Fondamentale per la funzionalità dei domini è lo spazio di archiviazione che essi consumano. Sebbene VCF includa capacità vSAN basata su CPU-core per casi d'uso iperconvergenti, supporta anche un'ampia gamma

di soluzioni di archiviazione esterna. Questa flessibilità è fondamentale per le aziende che hanno effettuato investimenti significativi in array di storage esistenti o che hanno bisogno di supportare protocolli che vanno oltre quelli offerti da vSAN. VMware supporta più tipi di storage con VCF.

Esistono due tipi principali di archiviazione con VCF:

- **Archiviazione principale** – Questo tipo di archiviazione viene assegnato durante la creazione iniziale del dominio. Per i domini di gestione, questo archivio ospita i componenti amministrativi e operativi del VCF. Per i domini di carico di lavoro, questo storage è progettato per supportare i carichi di lavoro, le VM o i container per cui è stato distribuito il dominio.
- **Archiviazione supplementare** – È possibile aggiungere archiviazione supplementare a qualsiasi dominio di carico di lavoro dopo la distribuzione. Questo tipo di storage aiuta le organizzazioni a sfruttare gli investimenti esistenti nell'infrastruttura di storage e a integrare diverse tecnologie di storage per ottimizzare prestazioni, scalabilità ed efficienza dei costi.

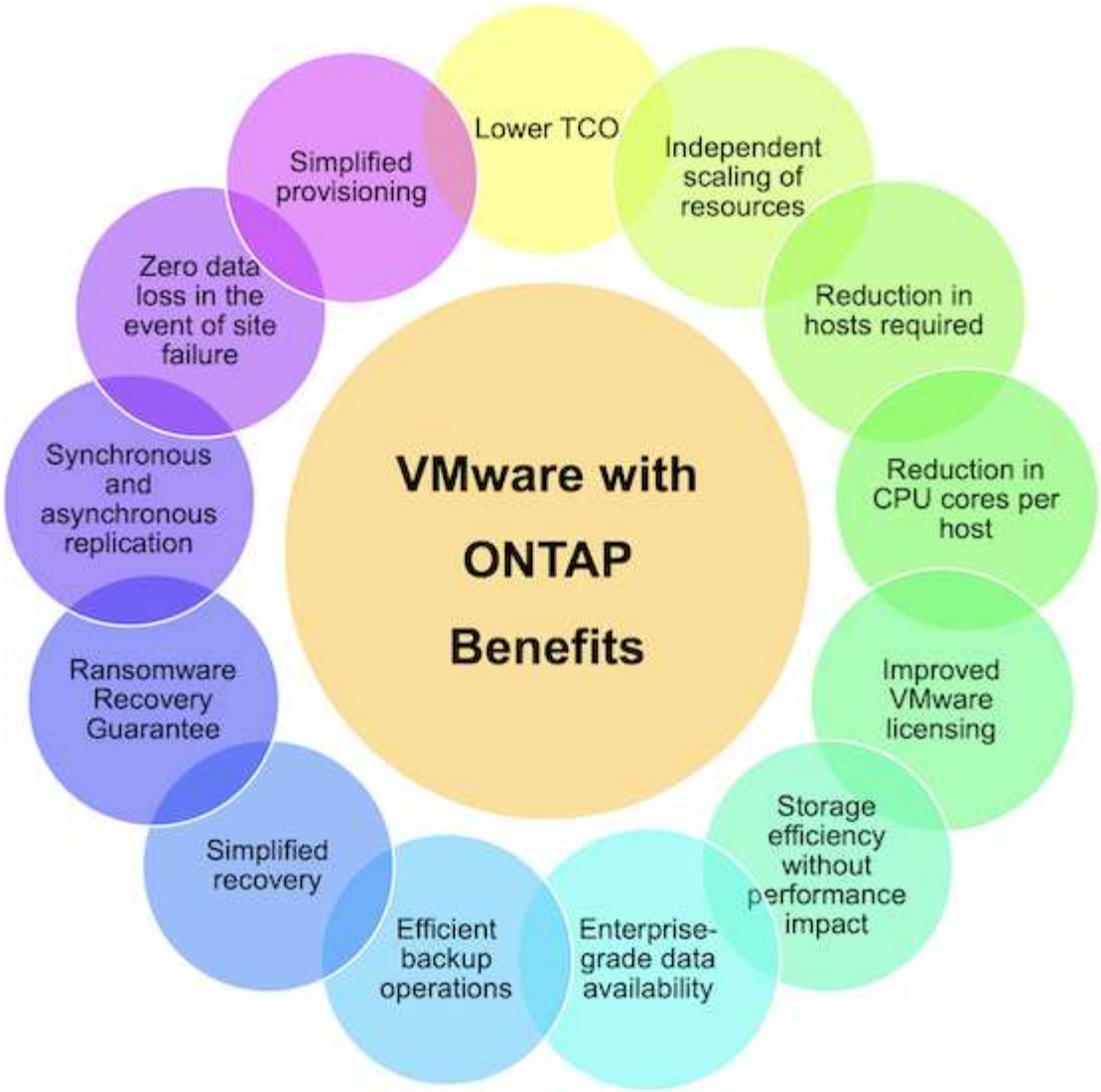
Supporta i tipi di archiviazione VCF

Tipo di dominio	Archiviazione principale	Spazio di archiviazione supplementare
Dominio di gestione	vSAN FC* NFS*	vVols (FC, iSCSI o NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
Dominio del carico di lavoro dell'infrastruttura virtuale	vSAN vVols (FC, iSCSI o NFS) FC NFS	vVols (FC, iSCSI o NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

Nota: * Supporto di protocollo specifico fornito quando si utilizza VCF Import Tool con ambienti vSphere esistenti.

Perché ONTAP per VCF

Oltre ai casi d'uso che riguardano la protezione degli investimenti e il supporto multiprotocollo, ci sono molti altri motivi per sfruttare i vantaggi dell'archiviazione condivisa esterna all'interno di un dominio di carico di lavoro VCF. Si può supporre che lo storage fornito per un dominio di carico di lavoro sia semplicemente un repository per ospitare VM e container. Tuttavia, le esigenze delle organizzazioni spesso superano le capacità della licenza e richiedono storage aziendale. Lo storage fornito da ONTAP, assegnato ai domini all'interno di VCF, è facile da implementare e offre una soluzione di storage condiviso a prova di futuro.



Per ulteriori informazioni sui principali vantaggi ONTAP per VMware VCF identificati di seguito, vedere"Perché ONTAP per VMware" .

- Flessibilità dal primo giorno e man mano che si cresce
- Trasferisci le attività di archiviazione a ONTAP
- La migliore efficienza di archiviazione della categoria
- Disponibilità dei dati di livello aziendale
- Operazioni di backup e ripristino efficienti
- Capacità di continuità aziendale olistica

Informazioni aggiuntive:

- "Opzioni di archiviazione NetApp"
- "Supporto vSphere Metro Storage Cluster (vMSC)"
- "Strumenti ONTAP per VMware vSphere"
- "Automazione VMware con ONTAP"

- "NetApp SnapCenter"
- "Multicloud ibrido con VMware e NetApp"
- "Sicurezza e protezione dal ransomware"
- "Facile migrazione dei carichi di lavoro VMware su NetApp"
- "Ripristino di emergenza BlueXP"
- "Approfondimenti sull'infrastruttura dati"
- "Raccoglitore dati VM"

Riepilogo

ONTAP fornisce una piattaforma che soddisfa tutti i requisiti dei carichi di lavoro, offrendo soluzioni di storage a blocchi personalizzate e offerte unificate per consentire risultati più rapidi per VM e applicazioni in modo affidabile e sicuro. ONTAP integra tecniche avanzate di riduzione e spostamento dei dati per ridurre al minimo l'ingombro del data center, garantendo al contempo una disponibilità a livello aziendale per mantenere online i carichi di lavoro critici. Inoltre, AWS, Azure e Google supportano l'archiviazione esterna basata su NetApp per migliorare l'archiviazione vSAN nei cluster basati su cloud VMware come parte delle loro offerte VMware-in-the-Cloud. Nel complesso, le capacità superiori di NetApp lo rendono una scelta più efficace per le distribuzioni VMware Cloud Foundation.

Risorse di documentazione

Per informazioni dettagliate sulle offerte NetApp per VMware Cloud Foundation, fare riferimento a quanto segue:

Documentazione di VMware Cloud Foundation

- "Documentazione di VMware Cloud Foundation"

Serie di blog in quattro (4) parti su VCF con NetApp

- "NetApp e VMware Cloud Foundation semplificati Parte 1: Introduzione"
- "NetApp e VMware Cloud Foundation semplificate Parte 2: VCF e storage principale ONTAP"
- "NetApp e VMware Cloud Foundation semplificate Parte 3: VCF e storage dei principali elementi"
- "NetApp e VMware Cloud Foundation semplificate - Parte 4: Strumenti ONTAP per VMware e storage supplementare"

*VMware Cloud Foundation con array SAN All-Flash NetApp *

- "VCF con array NetApp ASA , introduzione e panoramica della tecnologia"
- "Utilizzare ONTAP con FC come storage principale per i domini di gestione"
- "Utilizzare ONTAP con FC come storage principale per i domini dei carichi di lavoro VI"
- "Utilizzare Ontap Tools per distribuire datastore iSCSI in un dominio di gestione VCF"
- "Utilizzare Ontap Tools per distribuire datastore FC in un dominio di gestione VCF"
- "Utilizzare Ontap Tools per distribuire datastore vVols (iSCSI) in un dominio di carico di lavoro VI"
- "Configurare gli archivi dati NVMe su TCP per l'utilizzo in un dominio di carico di lavoro VI"
- "Distribuisci e utilizza il SnapCenter Plug-in for VMware vSphere per proteggere e ripristinare le VM in un dominio di carico di lavoro VI"

- "Distribuisci e utilizza il SnapCenter Plug-in for VMware vSphere per proteggere e ripristinare le VM in un dominio di carico di lavoro VI (datastore NVMe/TCP)"

*VMware Cloud Foundation con array NetApp All-Flash AFF *

- "VCF con array NetApp AFF , introduzione e panoramica della tecnologia"
- "Utilizzare ONTAP con NFS come storage principale per i domini di gestione"
- "Utilizzare ONTAP con NFS come storage principale per i domini di carico di lavoro VI"
- "Utilizzare gli strumenti ONTAP per distribuire datastore vVols (NFS) in un dominio di carico di lavoro VI"
- Soluzioni NetApp FlexPod per VMware Cloud Foundation*
- "Espansione del cloud ibrido FlexPod con VMware Cloud Foundation"
- "FlexPod come dominio di carico di lavoro per VMware Cloud Foundation"
- "FlexPod come dominio di carico di lavoro per VMware Cloud Foundation - Guida alla progettazione"

Opzioni di progettazione con VMware Cloud Foundation e ONTAP

È possibile ripartire da zero con VCF 9 o riutilizzare le distribuzioni esistenti per creare un ambiente Private Cloud utilizzando VCF 9 e ONTAP. Scopri i progetti di progettazione più diffusi per VCF 9 e come i prodotti NetApp aggiungono valore.

Opzioni di archiviazione

VMware Cloud Foundation con ONTAP supporta diverse configurazioni di storage per soddisfare diversi requisiti di prestazioni, scalabilità e disponibilità. Le tabelle seguenti riepilogano le opzioni di archiviazione principali e supplementari disponibili per il tuo ambiente.

Famiglia di prodotti	VMFS su FC	NFSv3
ASA serie A e serie C	SÌ	NO
Serie A e serie C AFF	SÌ	SÌ
FAS	SÌ	SÌ

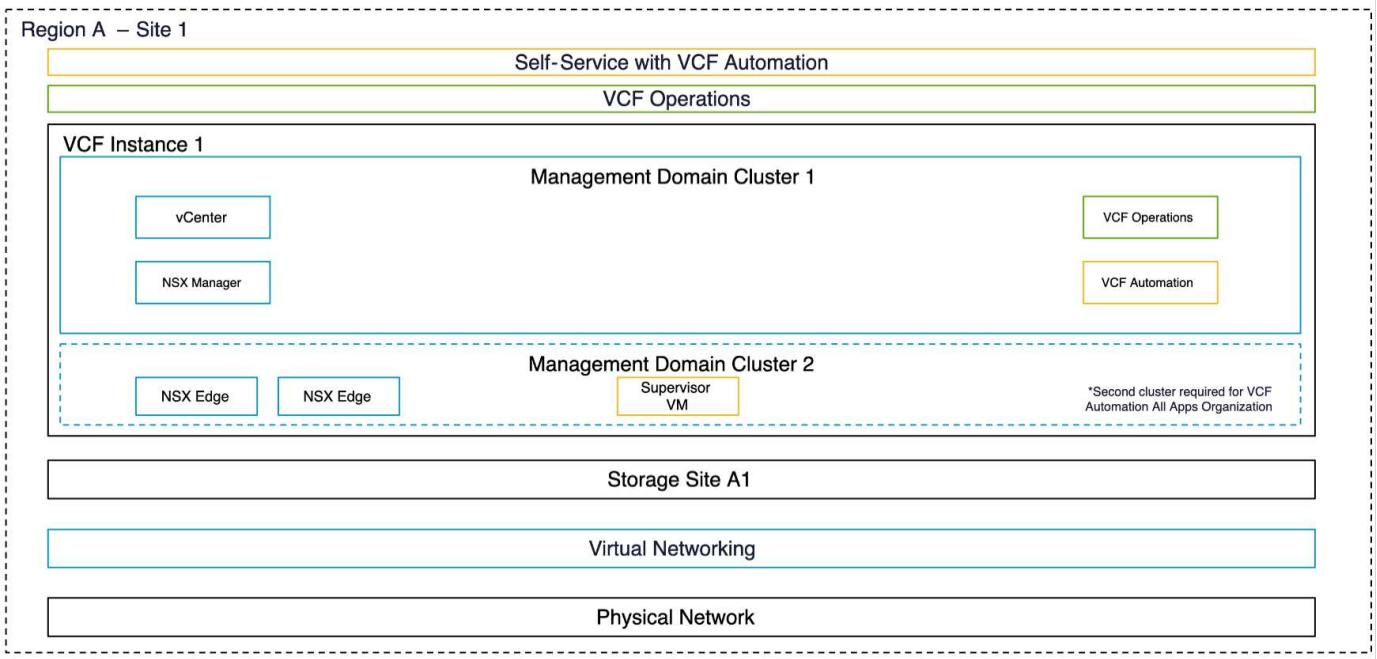
Famiglia di prodotti	VMFS su FC	VMFS su iSCSI	VMFS su NVMe-oF	NFSv3	NFSv4.1
ASA serie A e serie C	SÌ	SÌ	SÌ	NO	NO
Serie A e serie C AFF	SÌ	SÌ	SÌ	SÌ	SÌ
FAS	SÌ	SÌ	SÌ	SÌ	SÌ

Progetti

I seguenti progetti illustrano modelli di distribuzione comuni per VMware Cloud Foundation e ONTAP in vari scenari di siti e risorse.

Flotta VCF in un unico sito con ingombro minimo

Questo modello di progettazione è pensato per distribuire componenti di gestione e carico di lavoro in un singolo cluster vSphere con risorse minime. Supporta i principali datastore VMFS e NFSv3 e un'opzione di distribuzione semplice con una configurazione a due nodi. Se si prevede di utilizzare VCF Automation con il modello di organizzazione All Apps, è necessario un secondo cluster per distribuire i nodi vSphere Supervisor e NSX Edge.



Per ridurre al minimo il consumo di risorse, utilizzare, se possibile, un'istanza esistente degli strumenti ONTAP . Se non disponibile, è adatto un singolo nodo con un profilo piccolo. Il SnapCenter Plug-in for VMware vSphere protegge le macchine virtuali e i datastore utilizzando snapshot nativi e la replica su un altro array di storage ONTAP .

> Se non si dispone delle risorse necessarie per esplorare VCF, molti provider cloud offrono VCF come servizio e ONTAP è disponibile come servizio di prima parte dai provider cloud.

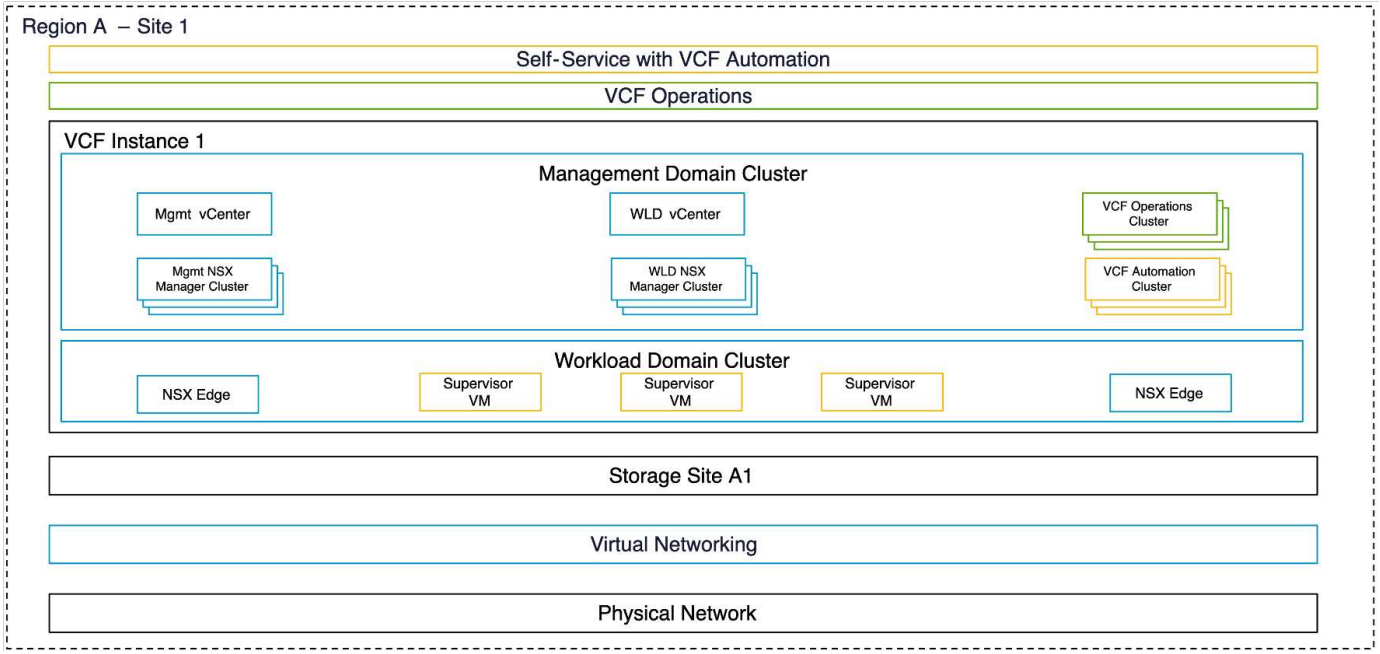
Per maggiori dettagli su questo progetto, fare riferimento al"Documentazione tecnica Broadcom sulla flotta VCF in un unico sito con ingombro minimo" .

Flotta VCF in un unico sito

Questo modello di progettazione è destinato ai clienti con un singolo data center primario che si affida all'alta disponibilità delle applicazioni. In genere, si tratta di un singolo ambiente VCF. È possibile utilizzare ASA per i carichi di lavoro a blocchi e AFF per i carichi di lavoro file/unificati.

Content Repository condivide modelli di VM e registri di container tra i domini VCF. Se ospitata su FlexGroup Volume, la funzionalità FlexCache è disponibile per il datastore in abbonamento.

> L'hosting di VM su FlexCache Datastore non è supportato.



Una singola istanza degli strumenti ONTAP in modalità HA può gestire tutti i vCenter nella flotta VCF. Fare riferimento al"Limiti di configurazione degli strumenti ONTAP" per maggiori informazioni. Gli strumenti ONTAP si integrano con il raggruppamento intelligente VCF SSO e VCF OPS per l'accesso multi-vCenter nella stessa interfaccia utente.

Archivio dati supplementare VCF con strumenti ONTAP

È necessario distribuire il plug-in SnapCenter su ogni istanza di vCenter per la protezione di VM e Datastore.

La gestione basata su policy di storage viene utilizzata con vSphere Supervisor per ospitare le VM di controllo di VKS. I tag sono gestiti centralmente presso VCF Ops. NetApp Trident CSI viene utilizzato con VKS per la protezione del backup delle applicazioni mediante funzionalità array native. Quando si utilizza vSphere CSI, i dettagli del volume persistente vengono visualizzati in VCF Automation.

Per maggiori dettagli su questo progetto, fare riferimento al"Documentazione tecnica Broadcom sulla flotta VCF in un unico sito" .

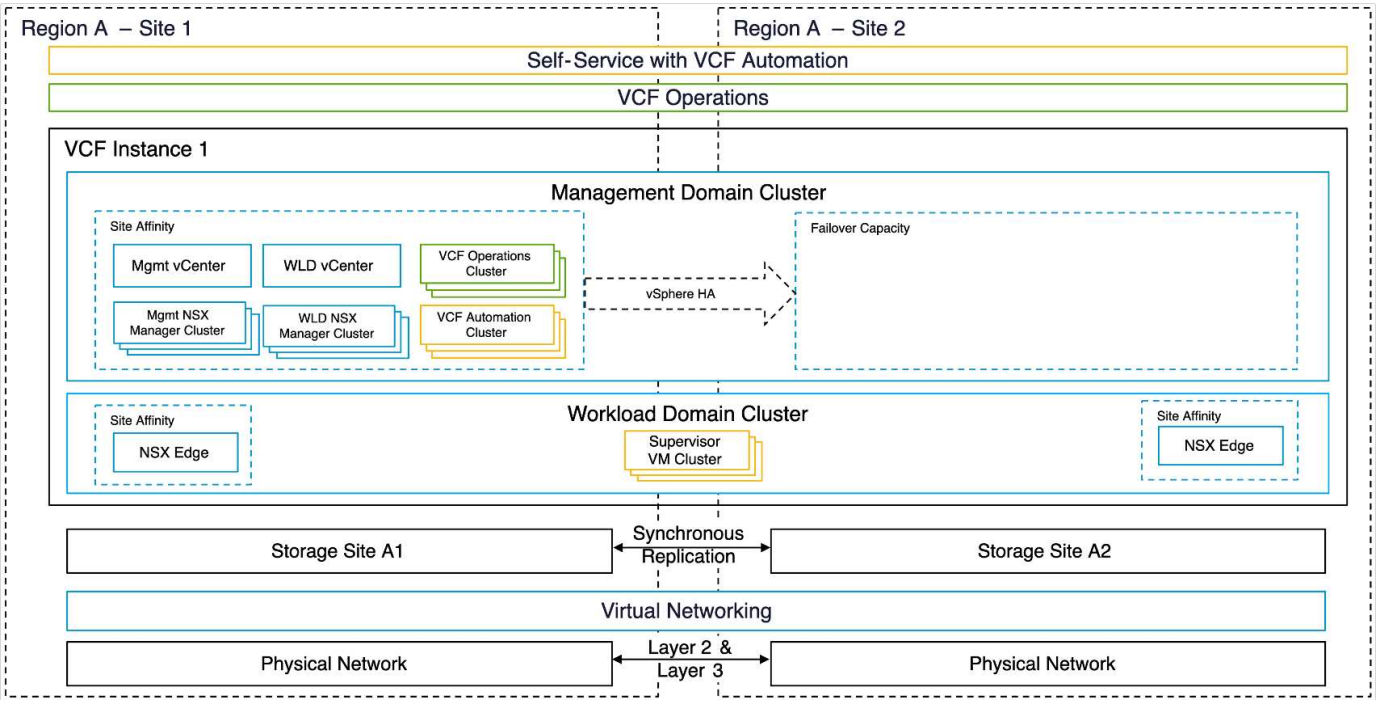
Flotta VCF con più siti in una singola regione

Questa progettazione è rivolta ai clienti che forniscono servizi simili al cloud con maggiore disponibilità distribuendo i carichi di lavoro su diversi domini di errore.

Per i datastore VMFS, SnapMirror Active Sync fornisce un'unità di archiviazione attiva-attiva da utilizzare con vSphere Metro Storage Cluster. La modalità di accesso uniforme offre un failover di archiviazione trasparente, mentre la modalità di accesso non uniforme richiede il riavvio della VM in caso di errore del dominio di errore.

Per i datastore NFS, ONTAP MetroCluster con vSphere Metro Storage Cluster garantisce un'elevata disponibilità. Un mediatore evita scenari di split-brain e ora può essere ospitato su BlueXP.

Le regole di posizionamento delle VM controllano le VM all'interno dello stesso dominio di errore per i componenti del dominio di gestione.



Gli strumenti ONTAP forniscono un'interfaccia utente per impostare le relazioni di sincronizzazione attiva SnapMirror . I sistemi di storage di entrambi i domini di errore devono essere registrati negli strumenti ONTAP e SnapCenter Plug-in for VMware vSphere.

È possibile implementare criteri di backup 3-2-1 utilizzando BlueXP Backup and Recovery per VM tramite SnapMirror e SnapMirror to Cloud. È possibile eseguire ripristini da una qualsiasi delle tre posizioni.

Trident Protect o BlueXP Backup and Recovery per Kubernetes proteggono le applicazioni del cluster VKS.

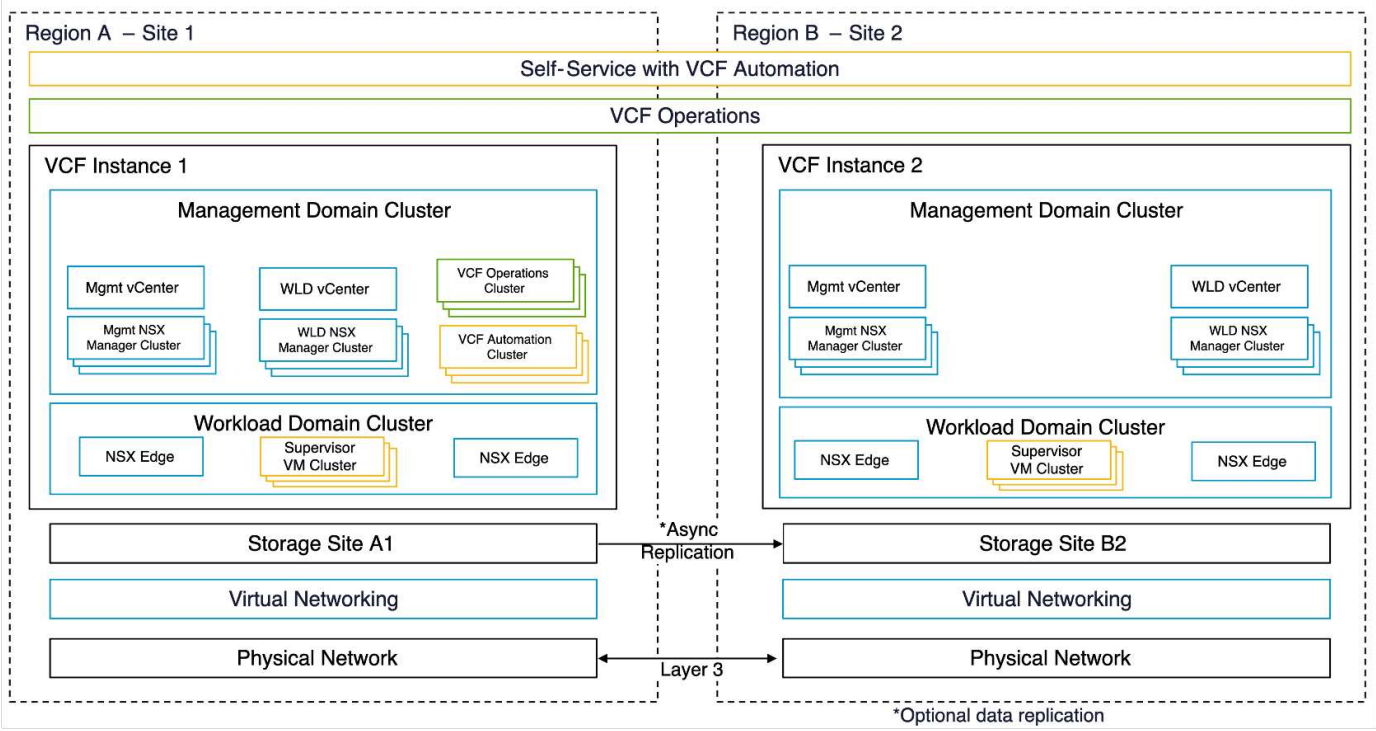
Per maggiori informazioni, consultare il"Documentazione tecnica Broadcom sulla flotta VCF con più siti in una singola regione" .

Flotta VCF con più sedi in più regioni

Questo progetto è rivolto a clienti distribuiti in tutto il mondo, che forniscono servizi in prossimità e soluzioni di disaster recovery.

È possibile gestire il Disaster Recovery per le VM con VMware Live Site Recovery o BlueXP Disaster Recovery as a Service. Gli strumenti ONTAP offrono l'SRA (Storage Replication Adapter) per orchestrare le operazioni di archiviazione con ONTAP.

Famiglia di prodotti	Sincronizzazione attiva SnapMirror	MetroCluster
ASA serie A e serie C	SÌ	SÌ
Serie A e serie C AFF	SÌ	SÌ
FAS	NO	SÌ



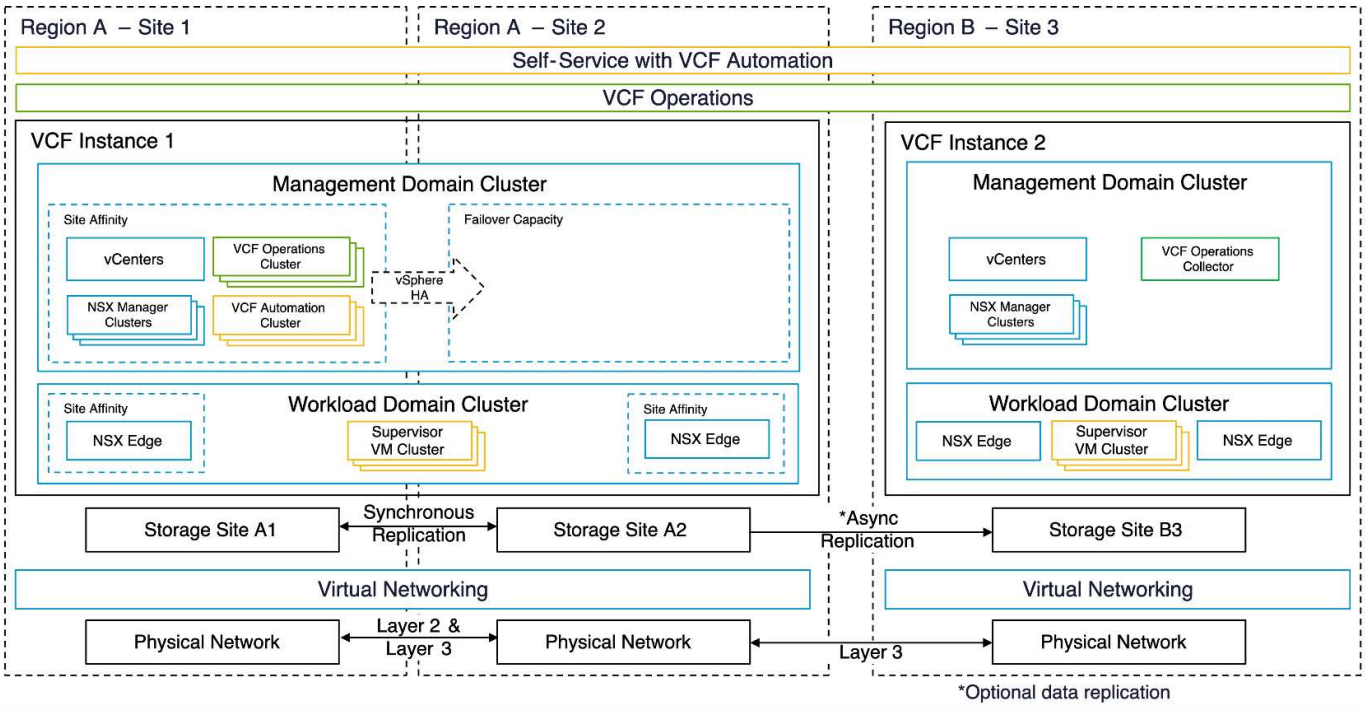
Gli strumenti ONTAP forniscono un'interfaccia utente per la configurazione della replicazione del datastore. BlueXP può essere utilizzato anche per la replica tra array di storage. Il SnapCenter Plug-in for VMware vSphere utilizza le relazioni SnapMirror esistenti per gli SnapShot.

Per maggiori informazioni, consultare il"Documentazione tecnica Broadcom sulla flotta VCF con più siti in più regioni" .

Flotta VCF con più siti in una singola regione più regioni aggiuntive

Questa progettazione affronta sia la disponibilità che il ripristino di emergenza delle VM e delle applicazioni VKS.

ASA, AFF e FAS supportano questa opzione di progettazione.



È possibile utilizzare gli strumenti ONTAP o BlueXP per impostare la relazione di replica.

Per ulteriori informazioni, consultare il sito "Documentazione tecnica Broadcom sulla flotta VCF con più siti in una singola regione più regioni aggiuntive" .

Configurare ambienti cloud privati con VMware Cloud Foundation e ONTAP

Distribuisci, fai convergere o aggiorna gli ambienti VMware Cloud Foundation 9 con ONTAP. Scopri come configurare nuovi ambienti VCF 9.0, far convergere istanze vCenter e datastore ONTAP esistenti e aggiornare le precedenti distribuzioni VCF.

Distribuisci una nuova istanza VCF 9

Utilizzare questo flusso di lavoro per distribuire un ambiente VMware Cloud Foundation (VCF) 9.0 pulito. Dopo la distribuzione, è possibile migrare i carichi di lavoro o iniziare a fornire applicazioni e servizi infrastrutturali.

Per i passaggi di alto livello, vedere"Build Journey: installa una nuova distribuzione VMware Cloud Foundation" .

Passi

1. Segui il"Passaggi di distribuzione di Broadcom VCF 9" .
2. Nella fase di preparazione della distribuzione, completa le attività per l'opzione di archiviazione principale.

VMFS su FC

1. Raccogliere i WWPN per tutti gli host ESXi. Puoi correre `esxcli storage san fc list`, utilizzare ESXi Host Client oppure PowerCLI.
2. Configurare la zonizzazione. Vedere "Configurazioni di zonizzazione FC consigliate per i sistemi ONTAP" .

> Utilizzare i WWPN delle interfacce logiche SVM (LIF), non i WWPN dell'adattatore fisico.

3. Creare una LUN e mapparla sugli host tramite WWPN utilizzando System Manager, ONTAP CLI o l'API.
4. Eseguire nuovamente la scansione dell'adattatore di archiviazione su ESXi e creare il datastore VMFS.

NFSv3

1. Creare un'interfaccia VMkernel su un host ESXi.
2. Assicurare il"SVM ha NFS abilitato" E"vStorage su NFS è abilitato" .
3. Creare un volume ed esportarlo con una policy che consenta gli host ESXi.
4. Regolare le autorizzazioni secondo necessità.
5. Distribuire l' ONTAP NFS VAAI VIB e includerlo nell'immagine vLCM. Per esempio: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip`. (Scaricare il file ZIP dal sito di supporto NetApp .)
6. Montare il volume NFS sull'host in cui è stata creata l'interfaccia VMkernel. Per esempio: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01`.

> IL `nConnect` il conteggio delle sessioni è per host. Aggiornare gli altri host dopo la distribuzione, se necessario.

1. Al termine della fase **Verifica riepilogo distribuzione e revisione passaggi successivi** nella fase **Distribuzione flotta VCF**, completare quanto segue:
   a. Distribuisci gli strumenti ONTAP
      - "Scarica gli strumenti ONTAP 10.x"dal sito di supporto NetApp .
      - Creare record DNS per gli strumenti ONTAP Manager, i nodi e l'IP virtuale utilizzato per la comunicazione interna.
      - Distribuire l'OVA sul server di gestione vCenter.
      - "Registrare il dominio di gestione vCenter"con ONTAP Tools Manager.
      - "Aggiungere il backend di archiviazione"utilizzando l'interfaccia utente di vSphere Client.
      - "Creare un datastore supplementare"(includerne uno per il registro dei contenuti).
      - Creare il registro dei contenuti se si pianifica una distribuzione HA.
      - "Abilita HA"nel gestore degli strumenti ONTAP .
   b. Distribuisci il plug-in SnapCenter

        - "Distribuisci il SnapCenter Plug-in for VMware vSphere" .
        - "Aggiungere il backend di archiviazione" .
        - "Creare policy di backup" .
        - "Creare gruppi di risorse" .
    c. Distribuisci il connettore BlueXP
        - "Scopri cosa puoi fare senza un connettore" .
        - "Distribuisci il connettore" .
    d. Utilizzare BlueXP per il backup e il ripristino
        - "Proteggere i carichi di lavoro VM" .
        - "Proteggere i carichi di lavoro VKS" .
2. Dopo aver importato vCenter come dominio del carico di lavoro nell'istanza VCF, completare le seguenti operazioni:
    a. Registra gli strumenti ONTAP
        - "Registra il dominio del carico di lavoro vCenter"con ONTAP Tools Manager.
        - "Aggiungere il backend di archiviazione"utilizzando l'interfaccia utente di vSphere Client.
        - "Creare un datastore supplementare" .
    b. Distribuisci il SnapCenter Plug-in for VMware vSphere
        - "Distribuisci il SnapCenter Plug-in for VMware vSphere" .
        - "Aggiungere il backend di archiviazione" .
        - "Creare policy di backup" .
        - "Creare gruppi di risorse" .
    c. Utilizzare BlueXP per il backup e il ripristino
        - "Proteggere i carichi di lavoro VM" .
        - "Proteggere i carichi di lavoro VKS" .

È possibile riutilizzare questi passaggi ogni volta che si crea un nuovo dominio del carico di lavoro.

Convergere i componenti esistenti in VCF 9

Potresti già disporre di alcuni componenti della flotta VCF e preferire riutilizzarli. Quando si riutilizza un'istanza vCenter, gli archivi dati vengono spesso forniti con strumenti ONTAP , che possono fungere da storage principale per VCF.

Prerequisiti

- Verificare che le istanze vCenter esistenti siano funzionanti.
- Verificare che i datastore forniti da ONTAP siano disponibili.
- Garantire l'accesso al"Matrice di interoperabilità" .

Passi

1. Rivedere il"scenari supportati per convergere verso VCF" .
2. Convergere un'istanza vCenter con datastore forniti da ONTAP come storage principale.

3. Verificare le versioni supportate utilizzando"Matrice di interoperabilità" .
4. Aggiornamento"Strumenti ONTAP" se necessario.
5. Aggiorna il"Plugin SnapCenter per VMware vSphere" se necessario.

Aggiorna un ambiente VCF esistente a VCF 9

Aggiornare una precedente distribuzione VCF alla versione 9.0 utilizzando la procedura di aggiornamento standard. Il risultato è un ambiente VCF che esegue la versione 9.0 con domini di gestione e di carico di lavoro aggiornati.

Prerequisiti

- Eseguire il backup del dominio di gestione e dei domini del carico di lavoro.
- Verificare la compatibilità degli strumenti ONTAP e del plug-in SnapCenter con VCF 9.0. Segui il"Matrice di interoperabilità" A"aggiornare gli strumenti ONTAP" E"Plugin SnapCenter per VMware vSphere" supportati per VCF 9.

Passi

1. Aggiornare il dominio di gestione VCF. Vedere"Aggiornare il dominio di gestione VCF a VCF 9" per istruzioni.
2. Aggiornare tutti i domini di carico di lavoro VCF 5.x. Vedere"Aggiorna il dominio del carico di lavoro VCF 5.x a VCF 9" per istruzioni.

Implementazione del Disaster Recovery con NetApp SnapMirror e BlueXP DRaaS

Soluzione di disaster recovery VCF per datastore NFS con NetApp SnapMirror e BlueXP DRaaS

La replica a livello di blocco da un sito di produzione a un sito di disaster recovery (DR) offre una strategia resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, inclusi gli attacchi ransomware. La replica di NetApp SnapMirror consente ai domini di carico di lavoro VMware VCF 9 in esecuzione su sistemi ONTAP locali, utilizzando datastore NFS o VMFS, di essere replicati su un sistema ONTAP secondario situato in un data center di ripristino designato in cui è distribuito anche VMware.

Questa sezione descrive la configurazione di BlueXP Disaster Recovery as a Service (DRaaS) per stabilire il DR per le macchine virtuali VMware locali.

La configurazione include:

- Creazione di un account BlueXP e distribuzione di un connettore BlueXP .
- Aggiunta di array ONTAP al canvas BlueXP per facilitare la comunicazione tra VMware vCenter e lo storage ONTAP .
- Configurazione della replica tra siti tramite SnapMirror.
- Impostazione e test di un piano di ripristino per convalidare la prontezza al failover.

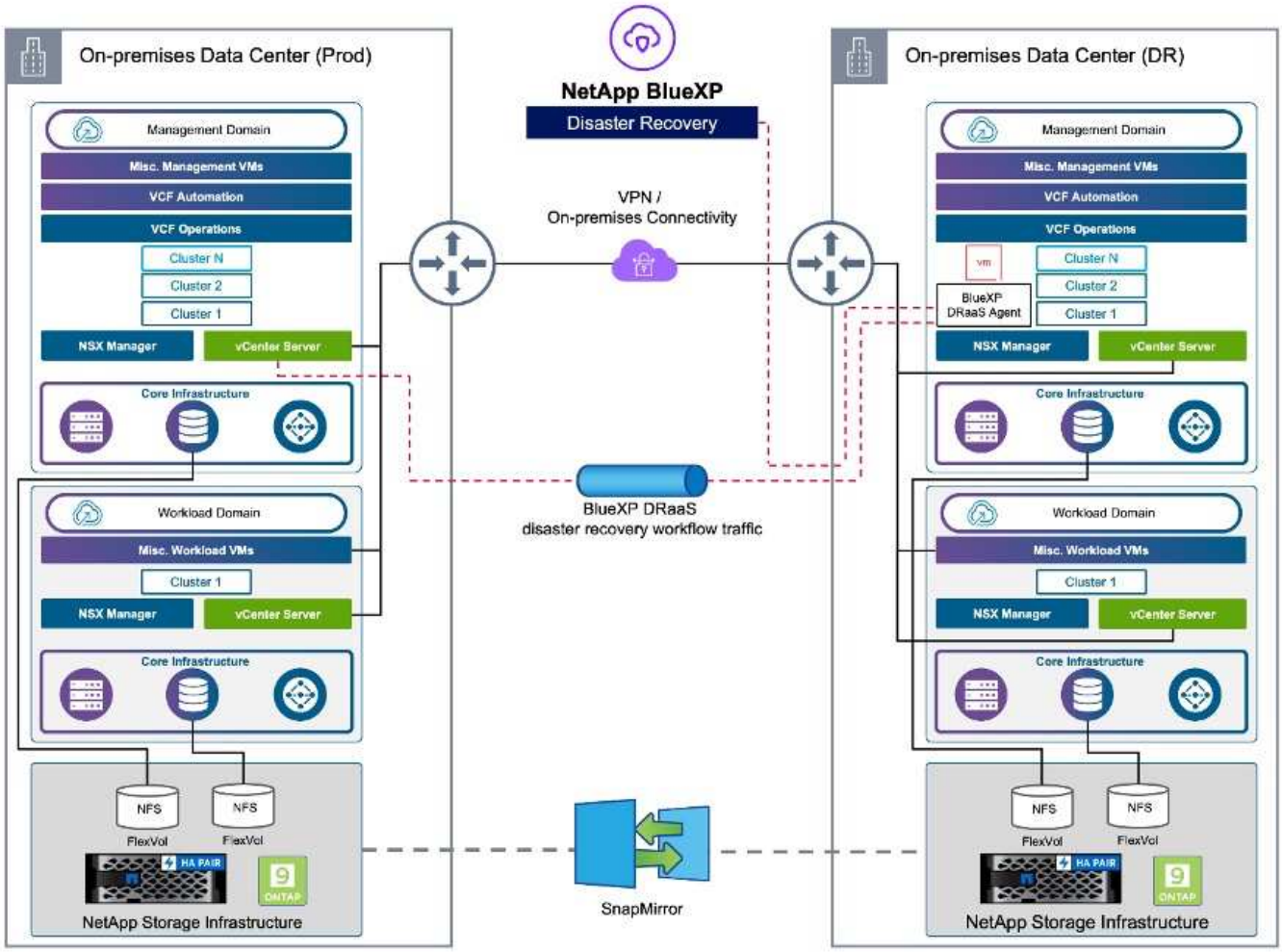
Il servizio BlueXP disaster recovery , integrato nella console NetApp BlueXP , consente alle organizzazioni di individuare senza problemi i propri sistemi di storage VMware vCenter e ONTAP in sede. Una volta individuate, le risorse possono essere definite dagli amministratori, creare piani di disaster recovery, associarle alle risorse

appropriate e avviare o testare le operazioni di failover e failback. NetApp SnapMirror fornisce un'efficiente replica a livello di blocco, garantendo che il sito DR rimanga sincronizzato con l'ambiente di produzione tramite aggiornamenti incrementali. Ciò consente un Recovery Point Objective (RPO) di appena cinque minuti.

BlueXP DRaaS supporta anche test di disaster recovery non-disruptive. Sfruttando la tecnologia FlexClone di ONTAP, vengono create copie temporanee e a basso consumo di spazio del datastore NFS dallo Snapshot replicato più recente, senza influire sui carichi di lavoro di produzione o comportare costi di archiviazione aggiuntivi. Dopo il test, l'ambiente può essere facilmente smantellato, preservando l'integrità dei dati replicati.

In caso di un failover effettivo, BlueXP orchestra il processo di ripristino, attivando automaticamente le macchine virtuali protette nel sito DR designato con un intervento minimo da parte dell'utente. Quando il sito primario viene ripristinato, il servizio inverte la relazione SnapMirror e replica tutte le modifiche sul sito originale, consentendo un failback fluido e controllato.

Tutte queste funzionalità vengono fornite a un costo notevolmente inferiore rispetto alle tradizionali soluzioni di disaster recovery.

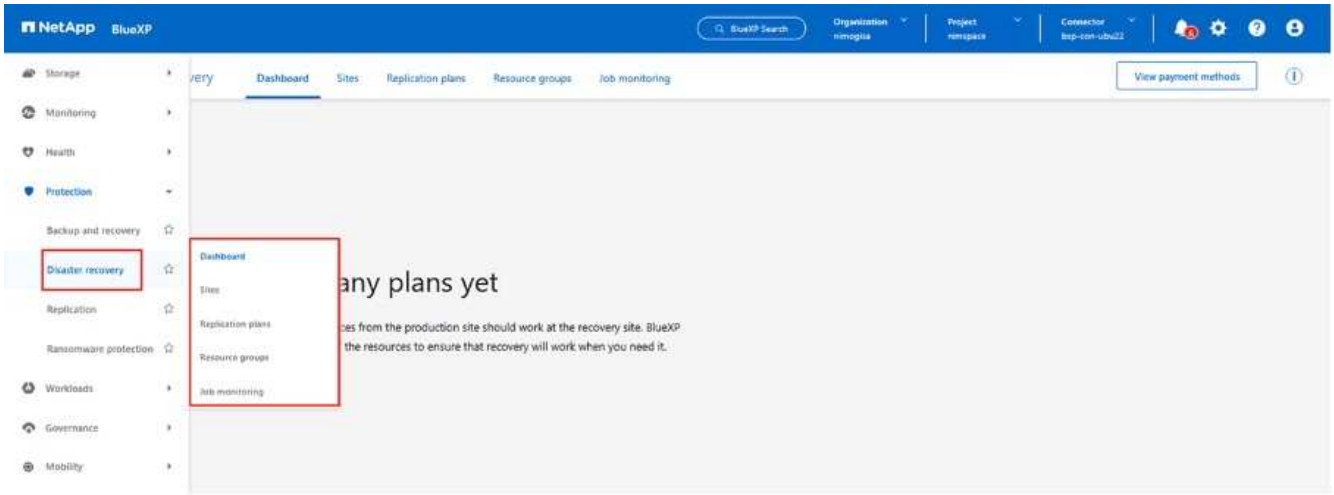


Iniziare

Per iniziare a utilizzare il BlueXP disaster recovery, utilizzare la console BlueXP e quindi accedere al servizio.

1. Accedi a BlueXP.
2. Dal menu di navigazione a sinistra BlueXP , seleziona Protezione > Ripristino di emergenza.

3. Viene visualizzata la Dashboard BlueXP disaster recovery .



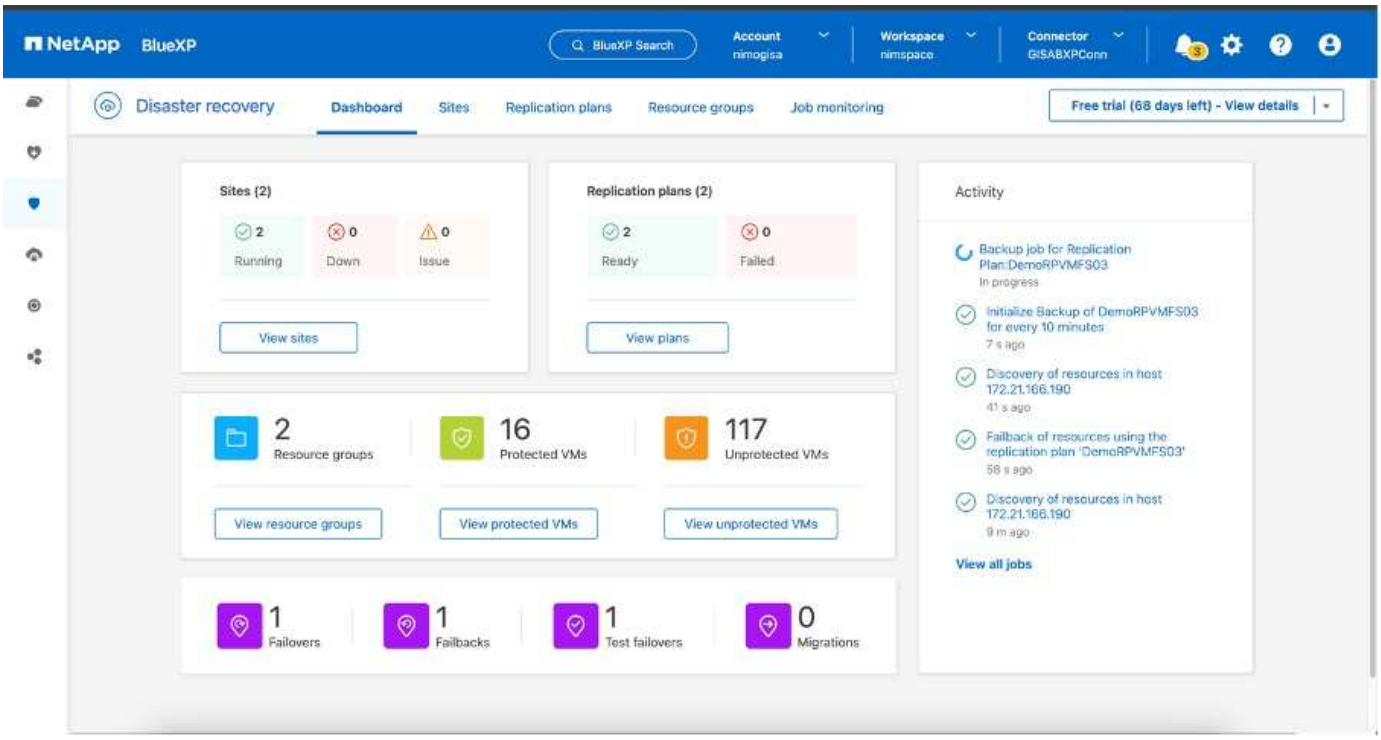
Prima di configurare il piano di ripristino di emergenza, assicurarsi di quanto segue"prerequisiti" sono soddisfatte:

- BlueXP Connector è configurato in NetApp BlueXP.
- L'istanza del connettore BlueXP dispone di connettività con il dominio del carico di lavoro di origine e di destinazione, vCenter e sistemi di archiviazione.
- Cluster NetApp Data ONTAP per fornire datastore di archiviazione NFS o VMFS.
- In BlueXP vengono aggiunti i sistemi di storage NetApp on-premise che ospitano datastore NFS o VMFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su NFS o VMFS designati.
- Assicurarsi che l'ambiente disponga di versioni supportate dei server vCenter Server ed ESXi.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere un paio di clic e circa 3-5 minuti.

Nota: NetApp consiglia di distribuire il connettore BlueXP nel sito di destinazione o in un terzo sito, in modo che il connettore BlueXP possa comunicare tramite la rete con le risorse di origine e di destinazione.

In questa dimostrazione, i domini del carico di lavoro sono configurati con storage ONTAP NFS. I passaggi in termini di flusso di lavoro rimangono gli stessi per i datastore basati su VMFS.



Configurazione BlueXP disaster recovery

Il primo passo nella preparazione al disaster recovery è individuare e aggiungere le risorse di archiviazione e vCenter di origine al BlueXP disaster recovery.

Aprire la console BlueXP e selezionare Protezione > Ripristino di emergenza dal menu di navigazione a sinistra. Selezionare Scopri server vCenter oppure utilizzare il menu in alto, selezionare Siti > Aggiungi > Aggiungi vCenter.

Aggiungere le seguenti piattaforme:

- Dominio del carico di lavoro di origine vCenter
- Dominio del carico di lavoro di destinazione vCenter.

Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra l'array del sito di origine e l'array del sito di destinazione

SnapMirror fornisce la replica dei dati in un ambiente NetApp . Basata sulla tecnologia NetApp Snapshot®, la replica SnapMirror è estremamente efficiente perché replica solo i blocchi che sono stati modificati o aggiunti dall'aggiornamento precedente. SnapMirror può essere facilmente configurato tramite NetApp OnCommand® System Manager o ONTAP CLI. BlueXP DRaaS crea anche la relazione SnapMirror a condizione che il cluster e il peering SVM siano configurati in anticipo.

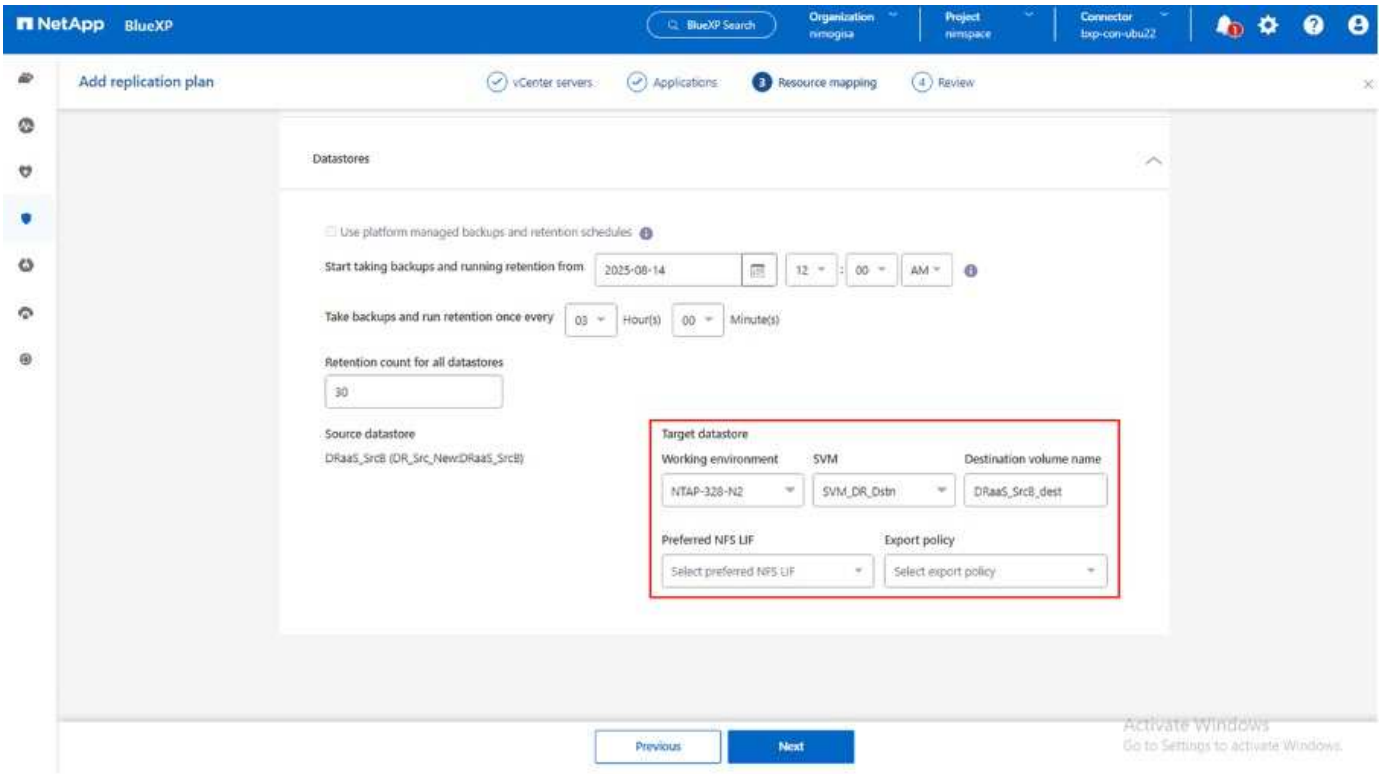
Nei casi in cui lo storage primario non è completamente perso, SnapMirror fornisce un mezzo efficiente per risincronizzare i siti primario e DR. SnapMirror può risincronizzare i due siti, trasferendo solo i dati modificati o nuovi dal sito DR al sito primario, semplicemente invertendo le relazioni SnapMirror . Ciò significa che i piani di replica in BlueXP DRaaS possono essere risincronizzati in entrambe le direzioni dopo un failover senza dover ricopiare l'intero volume. Se una relazione viene risincronizzata nella direzione inversa, solo i nuovi dati scritti dall'ultima sincronizzazione riuscita della copia Snapshot vengono inviati alla destinazione.

Se la relazione SnapMirror è già configurata per il volume tramite CLI o System Manager, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.

Come configurarlo per VMware Disaster Recovery

Il processo per creare una replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è sfruttare BlueXP DRaaS, che automatizzerà la stessa operazione a condizione che siano soddisfatti i due criteri seguenti:

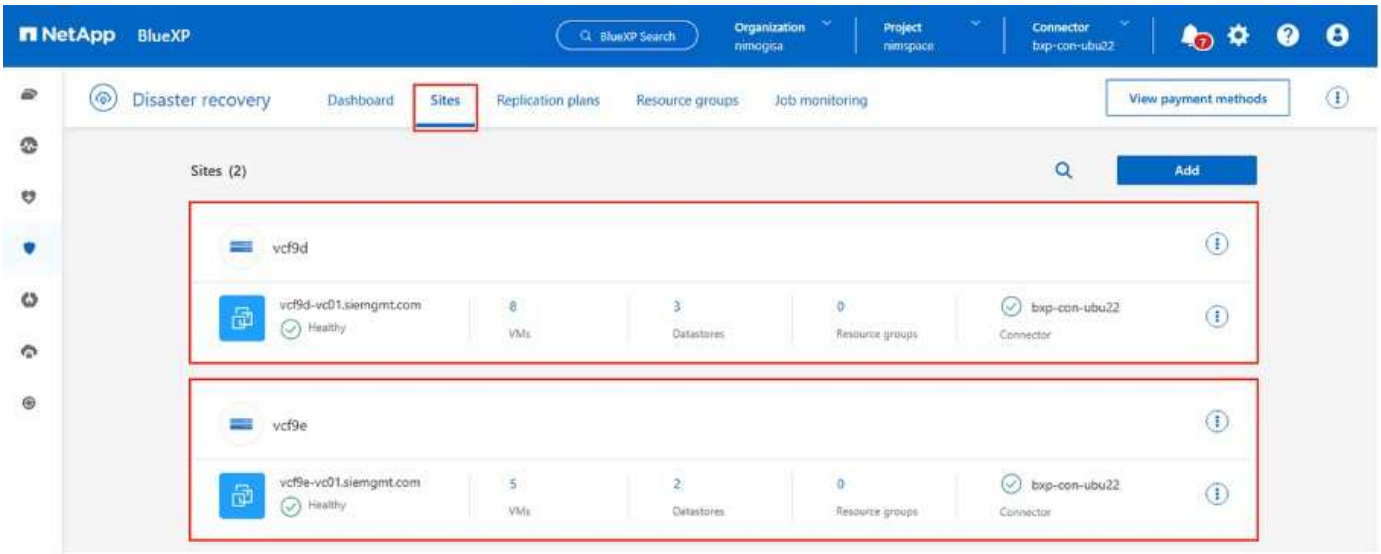
- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.



BlueXP fornisce anche un'opzione alternativa per configurare la replica SnapMirror mediante un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione per avviare la procedura guidata che guida attraverso il resto del processo.

Cosa può fare per te il BlueXP disaster recovery ?

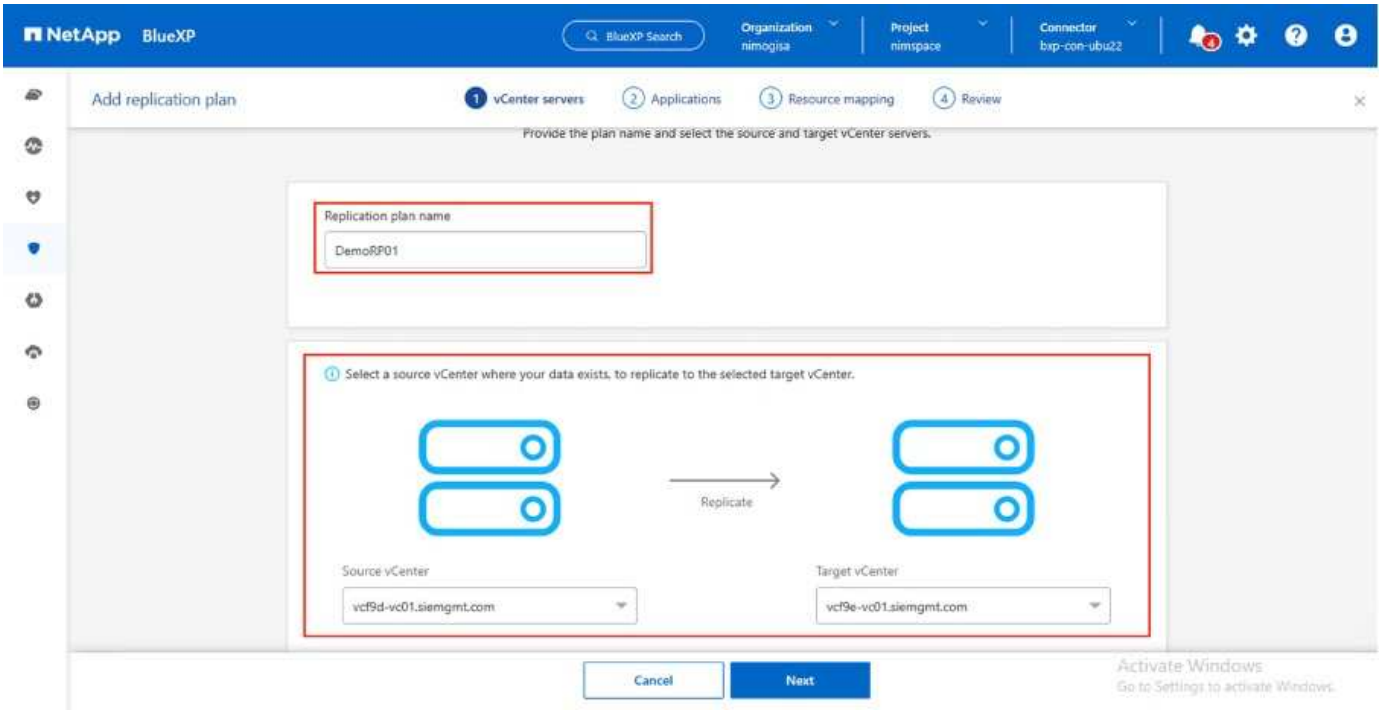
Dopo aver aggiunto i siti di origine e di destinazione, il BlueXP disaster recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. Il BlueXP disaster recovery rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle VM e li popola.



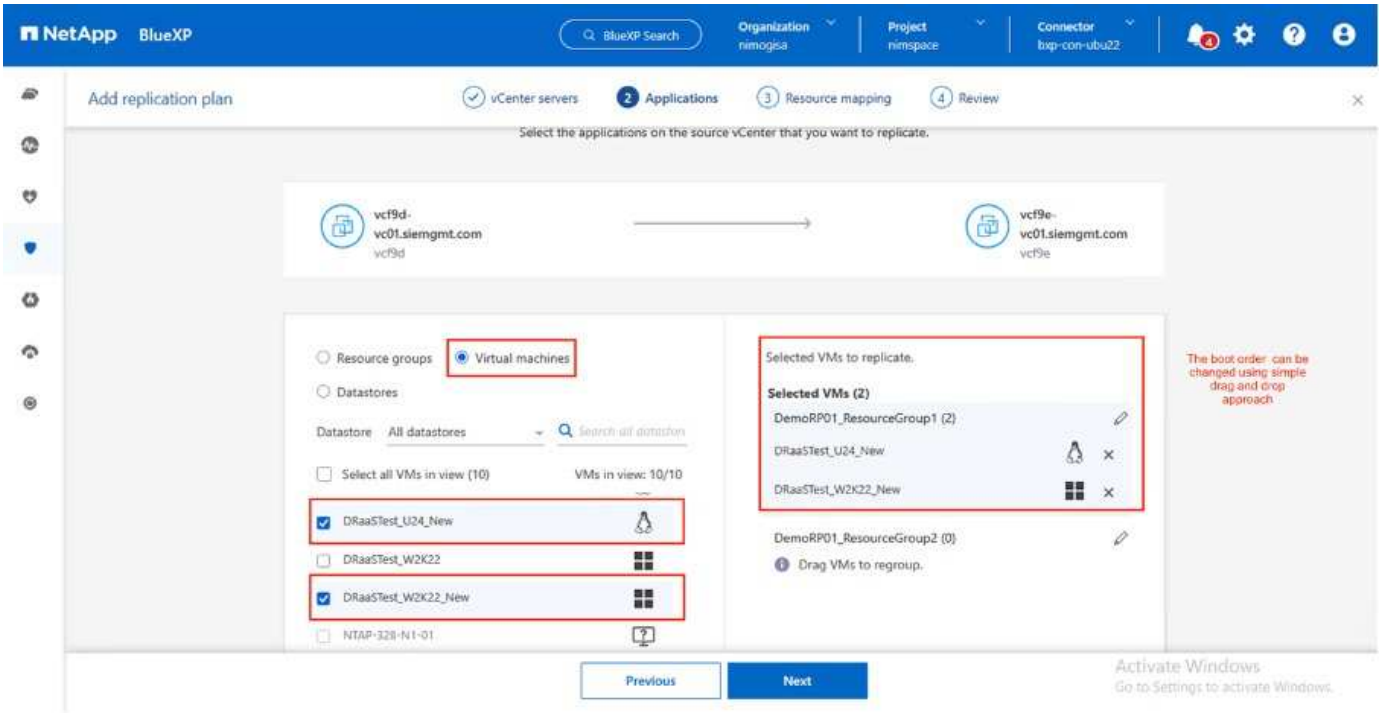
Dopo aver aggiunto i siti, configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Aggiungi piano**.

In questa fase, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse BlueXP disaster recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. Il gruppo di risorse può essere creato anche utilizzando la scheda Gruppo di risorse.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



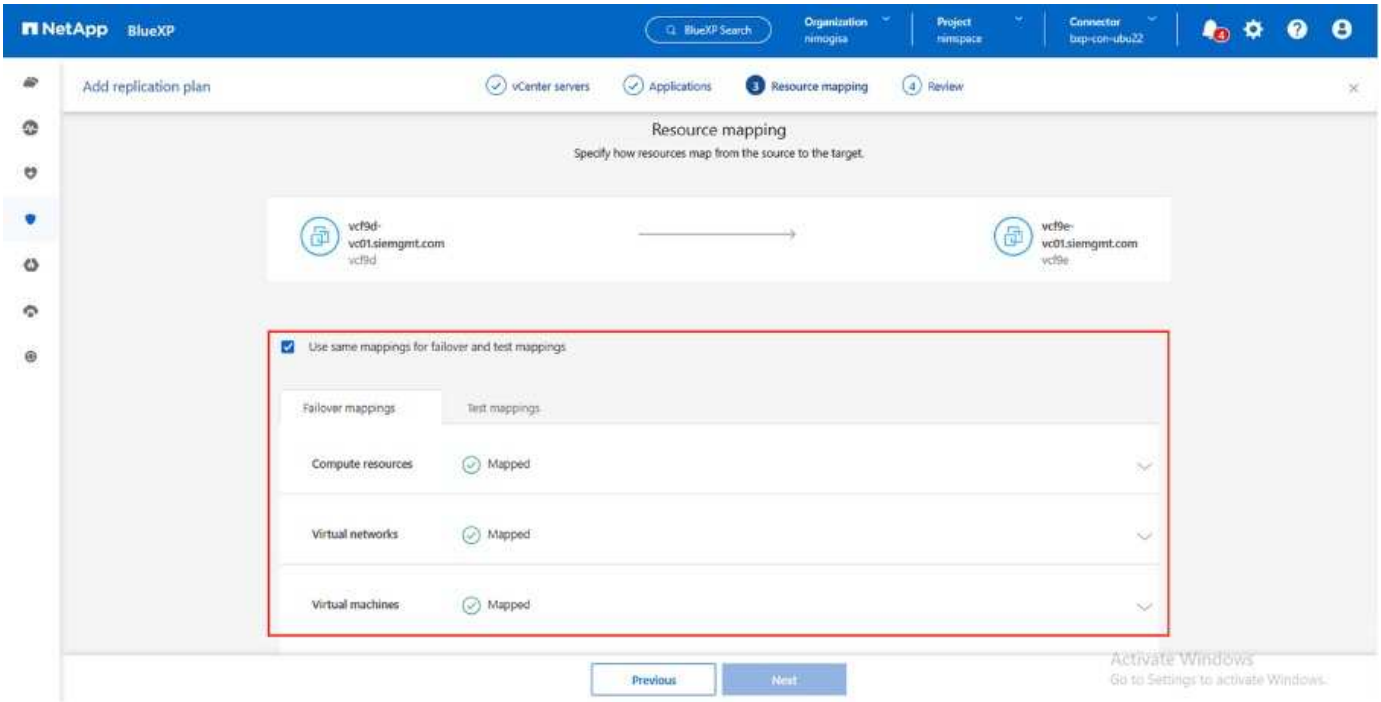
Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono essere ripristinate le macchine virtuali delle applicazioni.



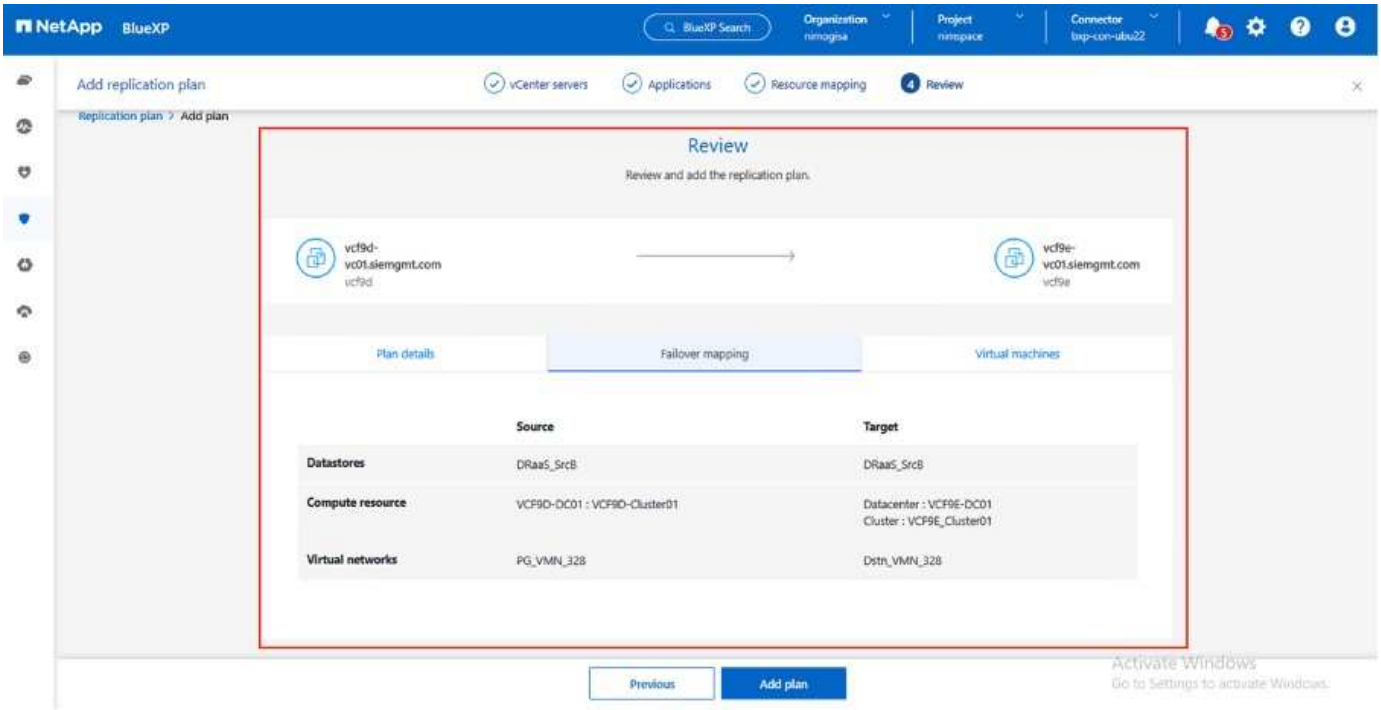
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

Una volta creati i gruppi di risorse tramite il piano di replica, il passaggio successivo consiste nel selezionare il progetto o una mappatura per ripristinare macchine virtuali e applicazioni in caso di disastro. In questo passaggio, specificare come le risorse dall'ambiente di origine vengono mappate alla destinazione. Ciò include risorse di elaborazione, reti virtuali, personalizzazione IP, pre- e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento a"Creare un piano di replicazione" . Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.

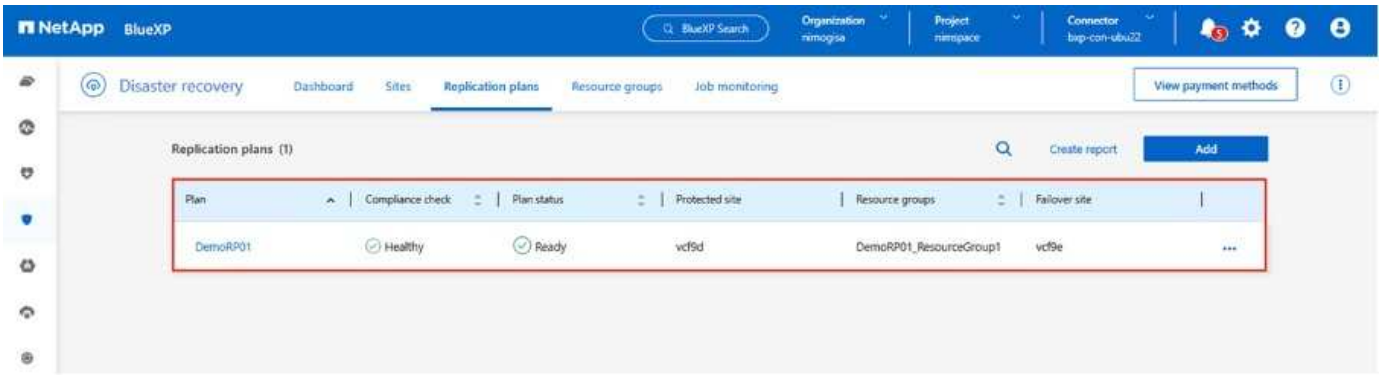
Nota: per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per impostare mapping diversi per l'ambiente di test, selezionare l'opzione Test mapping dopo aver deselezionato la casella di controllo "Usa gli stessi mapping per failover e test mapping". Una volta completata la mappatura delle risorse, fare clic su Avanti.



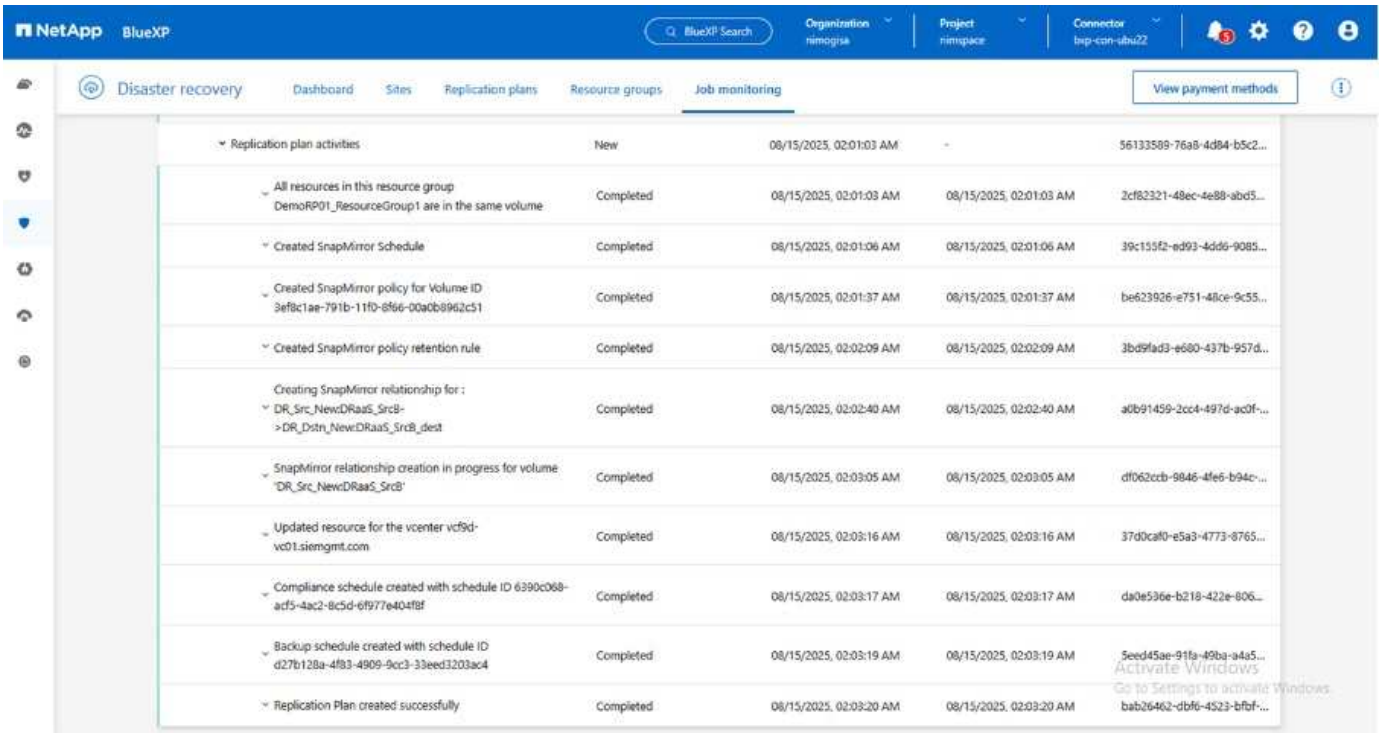
Una volta fatto, rivedi le mappature create e poi fai clic su Aggiungi piano.



In un piano di replicazione è possibile includere VM di volumi diversi e SVM. A seconda del posizionamento della VM (sia sullo stesso volume o su volumi separati all'interno della stessa SVM, volumi separati su SVM diverse), il BlueXP disaster recovery crea uno snapshot del gruppo di coerenza.

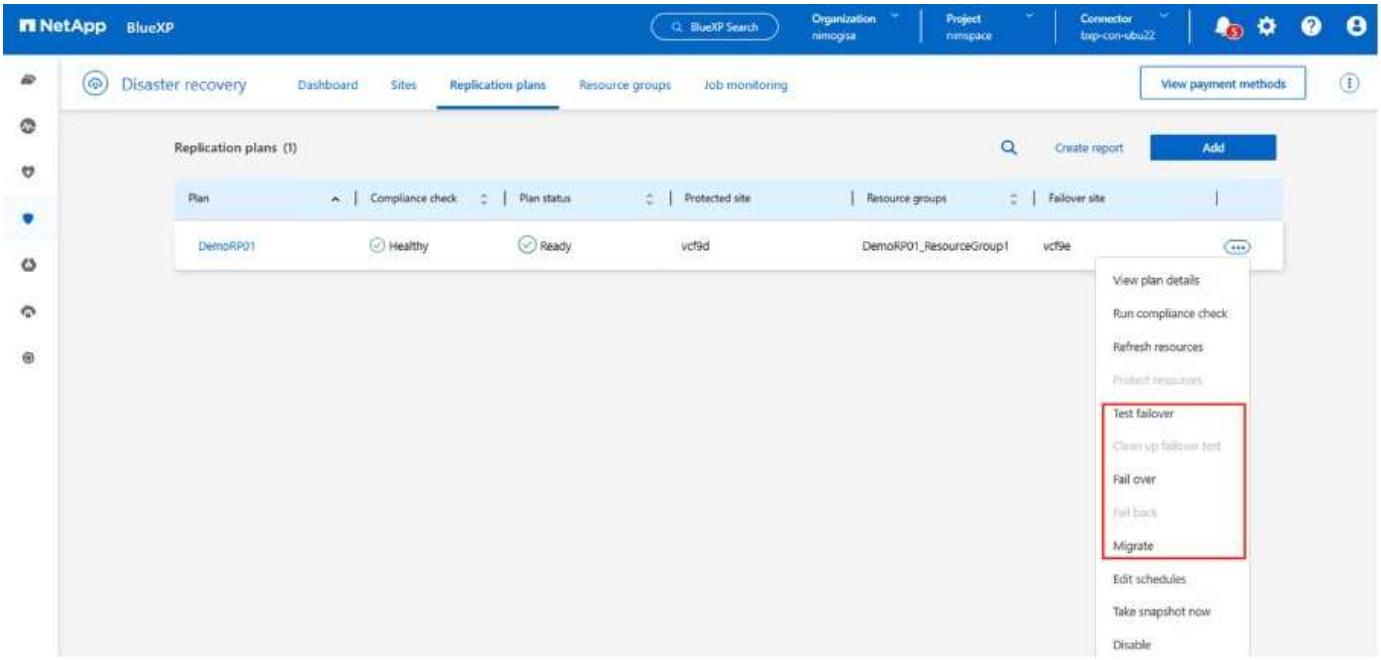


Non appena il piano viene creato, viene attivata una serie di convalide e la replica e le pianificazioni SnapMirror vengono configurate in base alla selezione.



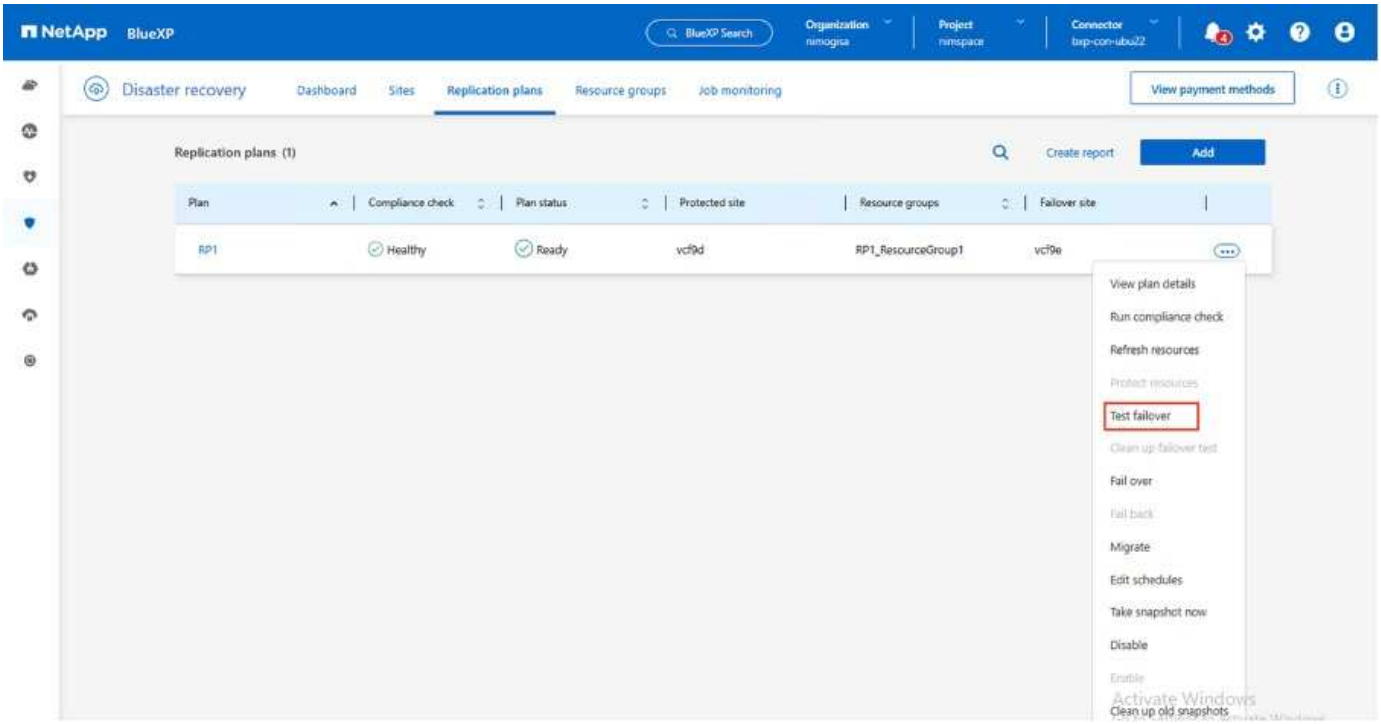
BlueXP DRaaS è costituito dai seguenti flussi di lavoro:

- Failover di test (incluse simulazioni automatiche periodiche)
- Test di failover di pulizia
- Failover:
  - Migrazione pianificata (estendere il caso d'uso per un failover una tantum)
  - Ripristino dopo un disastro
- Rifasamento

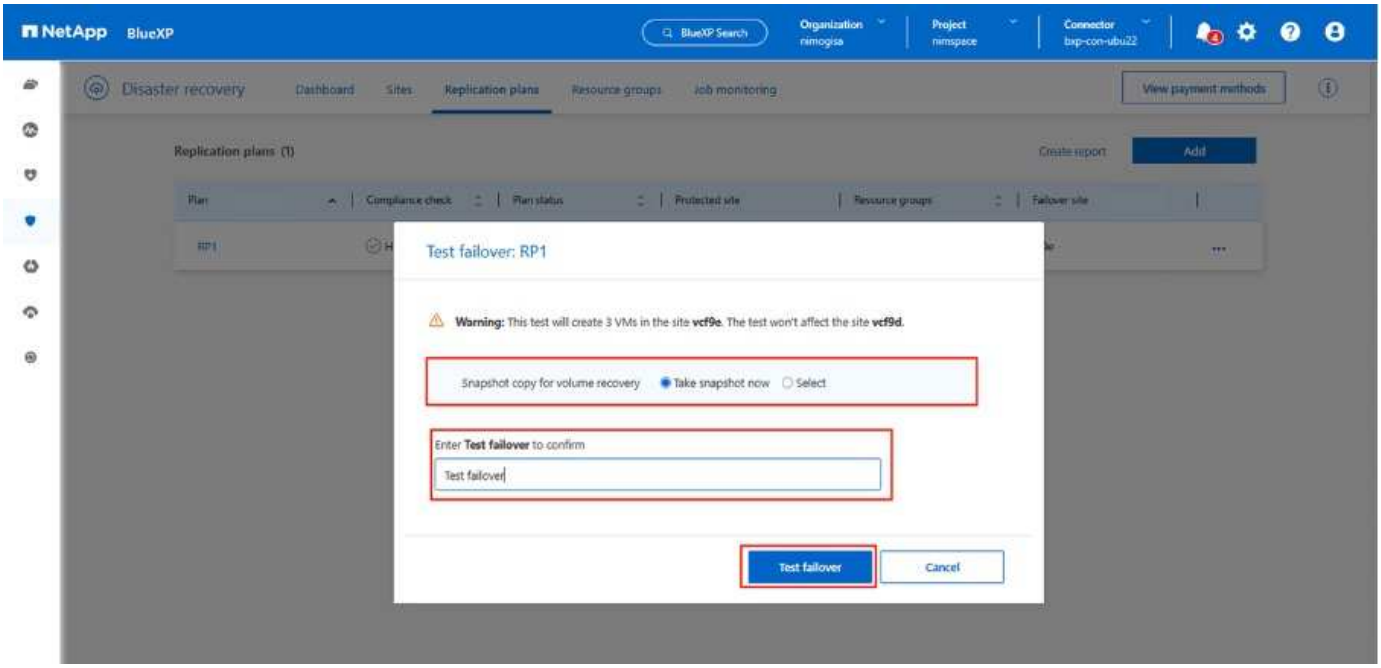


Failover di prova

Il failover di test in BlueXP DRaaS è una procedura operativa che consente agli amministratori VMware di convalidare completamente i propri piani di ripristino senza interrompere gli ambienti di produzione.

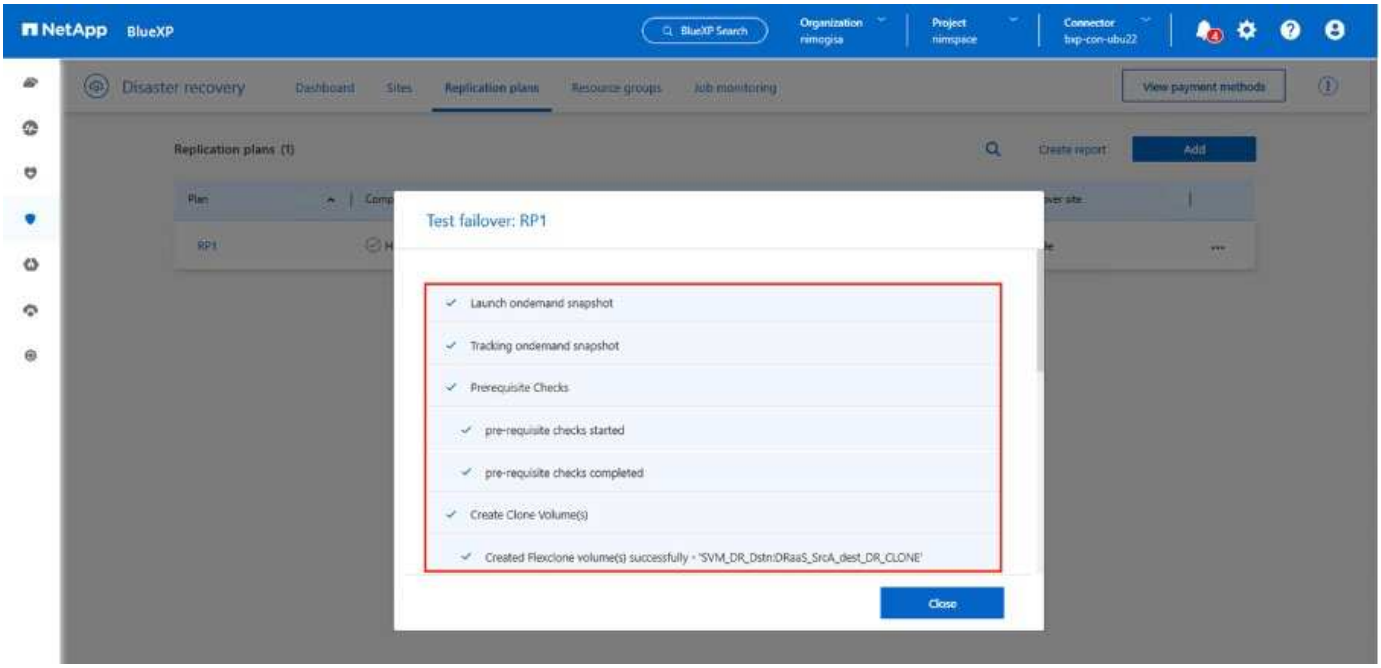


BlueXP DRaaS incorpora la possibilità di selezionare lo snapshot come funzionalità opzionale nell'operazione di failover di test. Questa funzionalità consente all'amministratore VMware di verificare che tutte le modifiche apportate di recente all'ambiente vengano replicate nel sito di destinazione e siano quindi presenti durante il test. Tali modifiche includono patch al sistema operativo guest della VM.



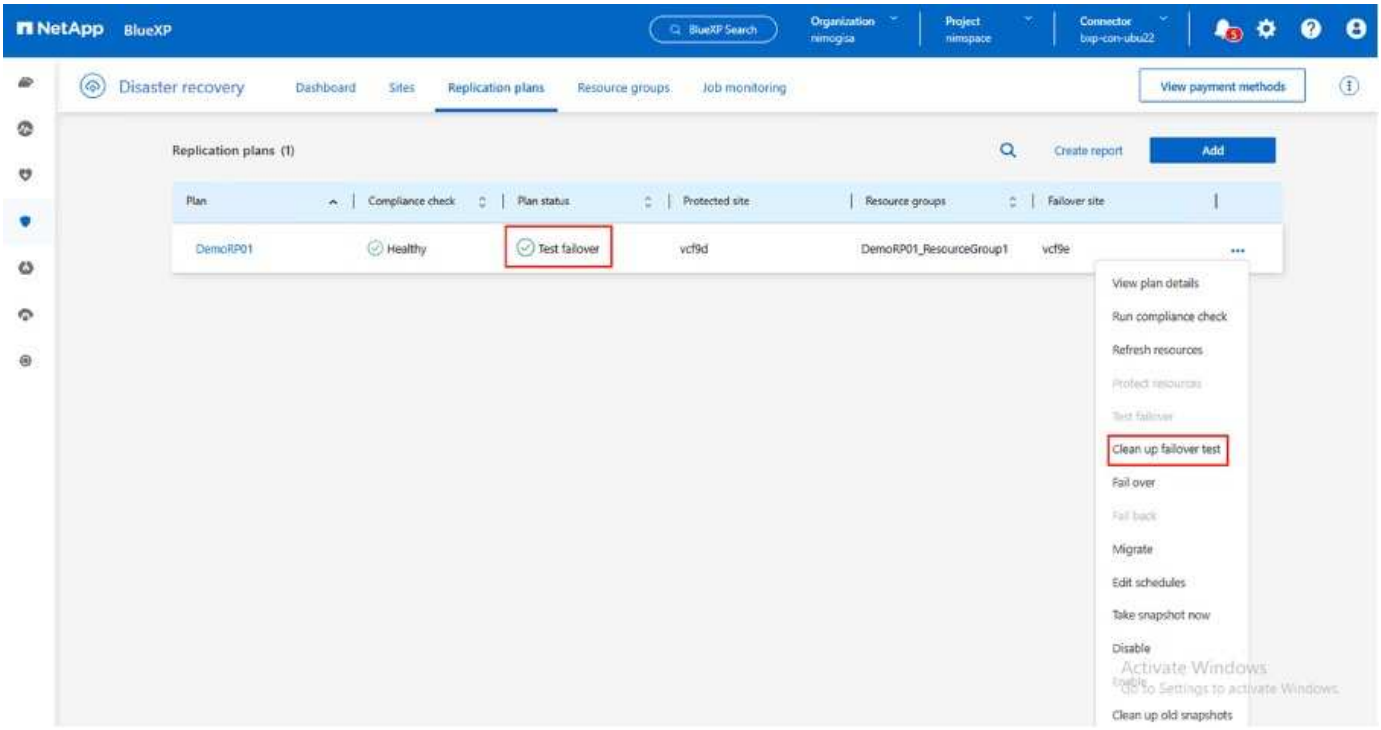
Quando l'amministratore VMware esegue un'operazione di failover di prova, BlueXP DRaaS automatizza le seguenti attività:

- Attivazione delle relazioni SnapMirror per aggiornare l'archiviazione nel sito di destinazione con tutte le modifiche recenti apportate nel sito di produzione.
- Creazione di volumi NetApp FlexClone dei volumi FlexVol sull'array di archiviazione DR.
- Collegamento dei datastore nei volumi FlexClone agli host ESXi nel sito DR.
- Collegamento degli adattatori di rete della VM alla rete di prova specificata durante la mappatura.
- Riconfigurazione delle impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito DR.
- Esecuzione di tutti i comandi personalizzati memorizzati nel piano di replicazione.
- Accensione delle VM nell'ordine definito nel piano di replica.



Operazione di test di failover di pulizia

L'operazione di test di failover di pulizia avviene dopo il completamento del test del piano di replica e quando l'amministratore VMware risponde al prompt di pulizia.

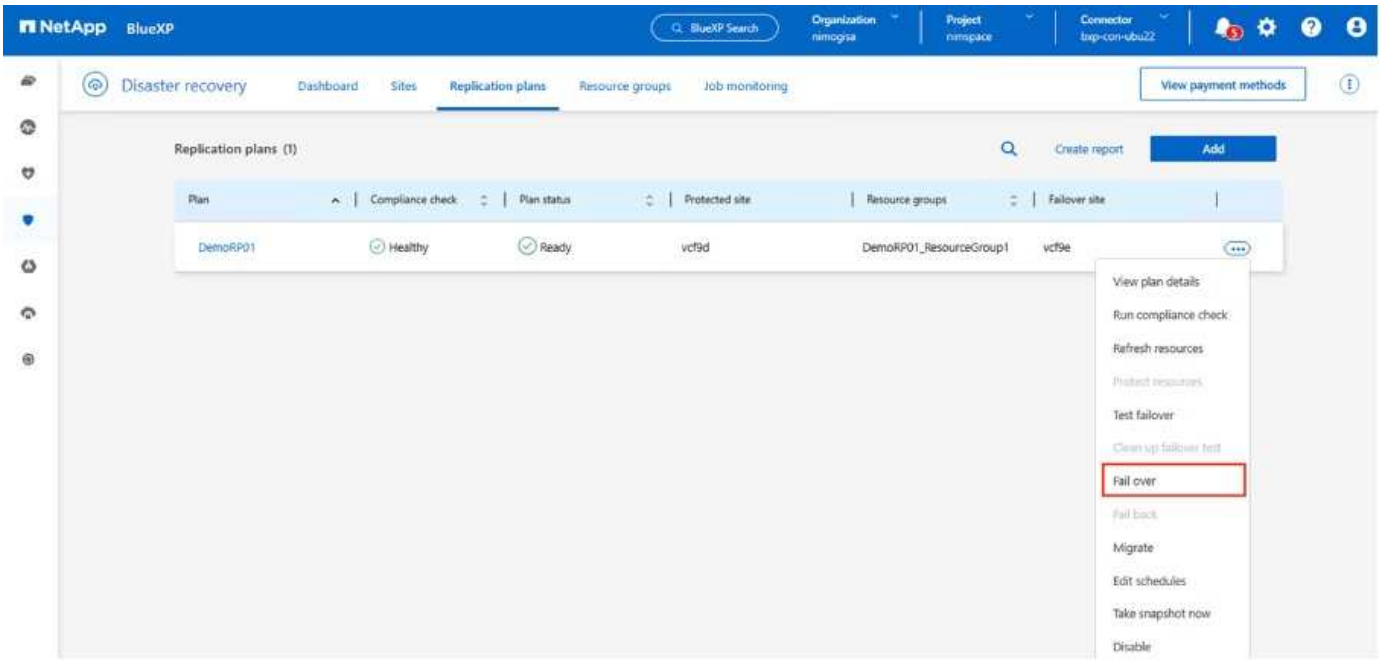


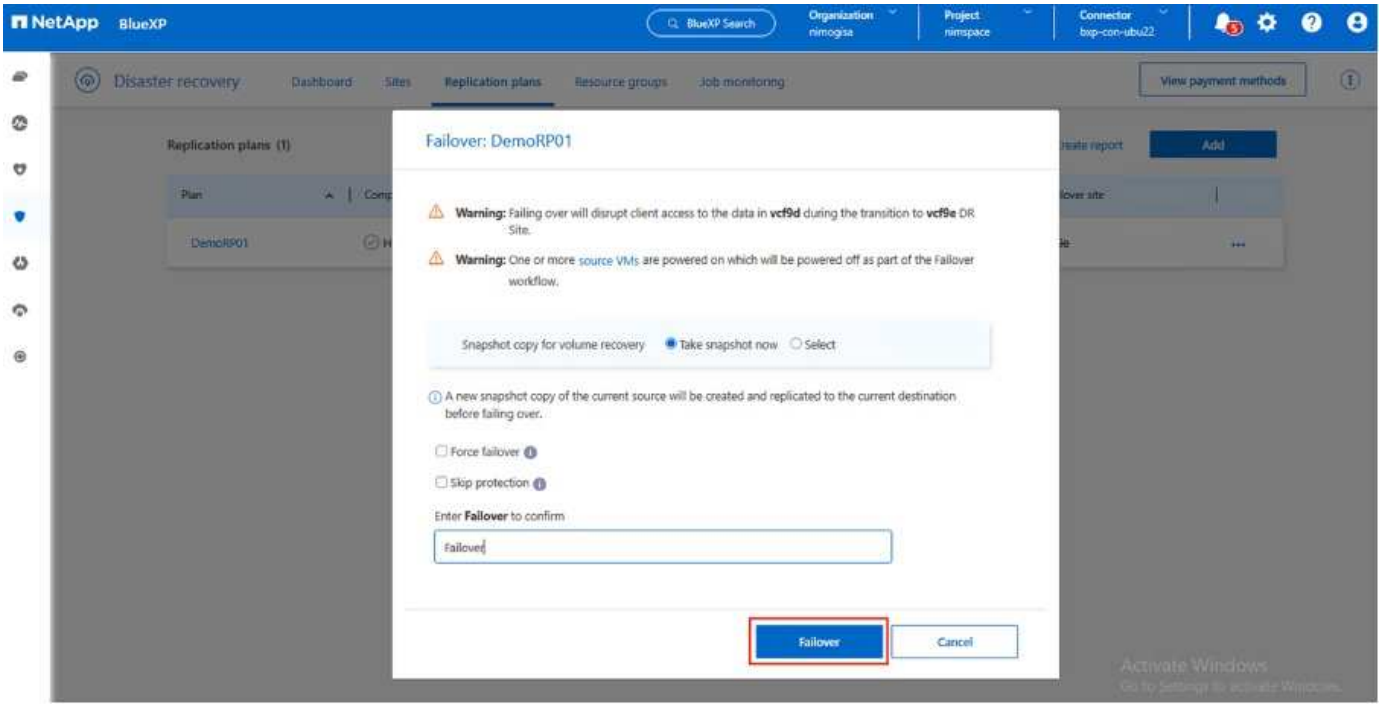
Questa azione reimposterà le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto. Quando l'amministratore VMware esegue un'operazione di ripristino, BlueXP DRaaS completa il seguente processo:

1. Spegne ogni VM recuperata nella copia FlexClone utilizzata per il test.
2. Elimina il volume FlexClone utilizzato per presentare le VM recuperate durante il test.

Migrazione pianificata e failover

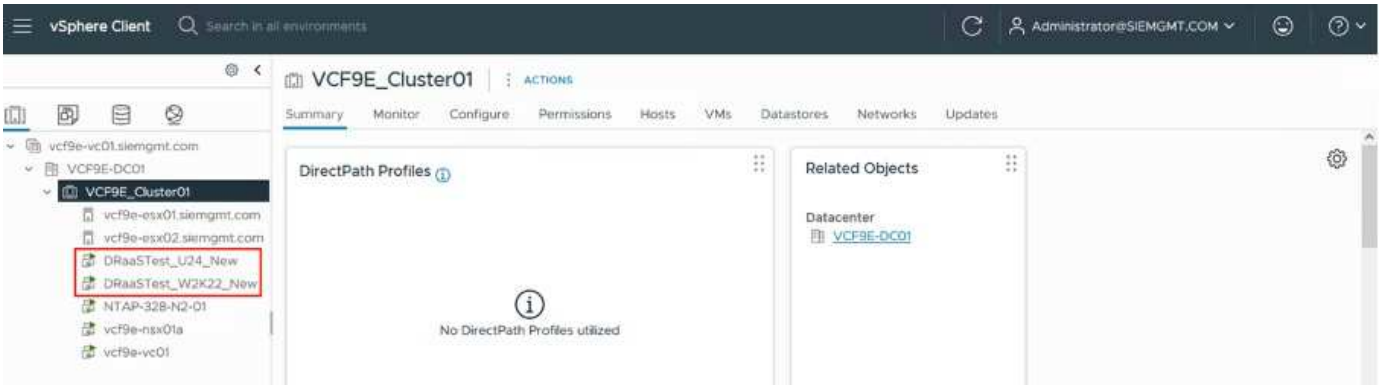
BlueXP DRaaS dispone di due metodi per eseguire un failover reale: migrazione pianificata e failover. Il primo metodo, la migrazione pianificata, incorpora l'arresto delle VM e la sincronizzazione della replicazione dello storage nel processo per ripristinare o spostare efficacemente le VM nel sito di destinazione. La migrazione pianificata richiede l'accesso al sito di origine. Il secondo metodo, il failover, è un failover pianificato/non pianificato in cui le VM vengono ripristinate nel sito di destinazione dall'ultimo intervallo di replicazione dell'archiviazione che è stato possibile completare. A seconda dell'RPO progettato nella soluzione, è possibile che si verifichi una certa perdita di dati nello scenario DR.





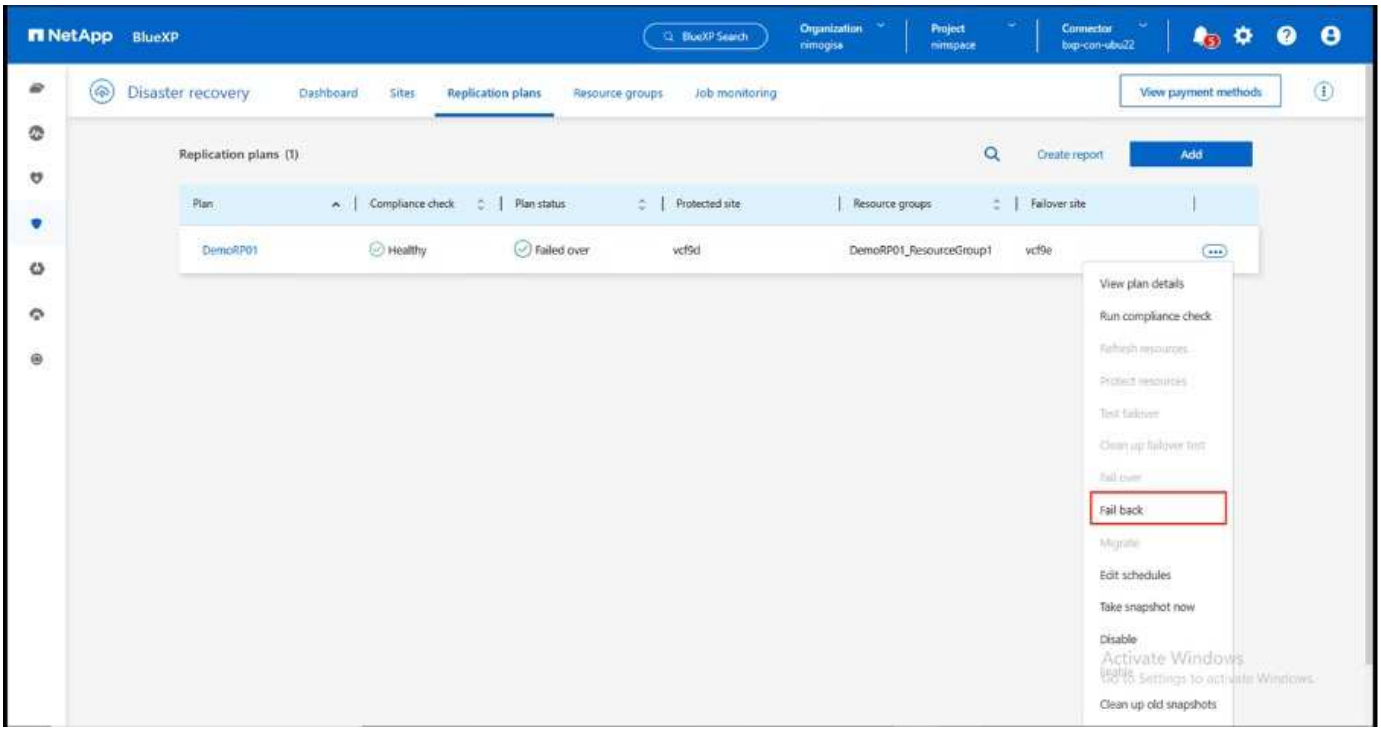
Quando l'amministratore VMware esegue un'operazione di failover, BlueXP DRaaS automatizza le seguenti attività:

- Interrompere ed eseguire il failover delle relazioni NetApp SnapMirror .
- Collegare i datastore replicati agli host ESXi nel sito DR.
- Collegare gli adattatori di rete della VM alla rete del sito di destinazione appropriata.
- Riconfigurare le impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito di destinazione.
- Eseguire eventuali comandi personalizzati memorizzati nel piano di replicazione.
- Accendere le VM nell'ordine definito nel piano di replica.



Rifasamento

Un failback è una procedura facoltativa che ripristina la configurazione originale dei siti di origine e di destinazione dopo un ripristino.

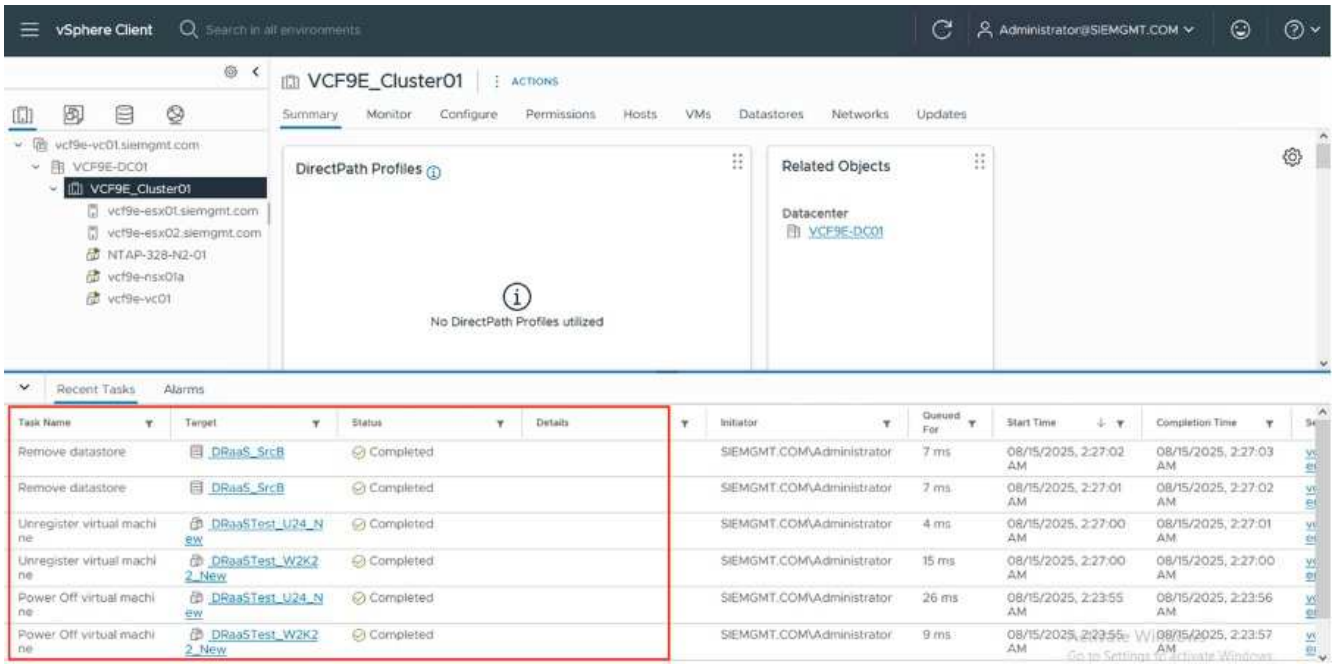


Gli amministratori VMware possono configurare ed eseguire una procedura di failback quando sono pronti a ripristinare i servizi sul sito di origine.

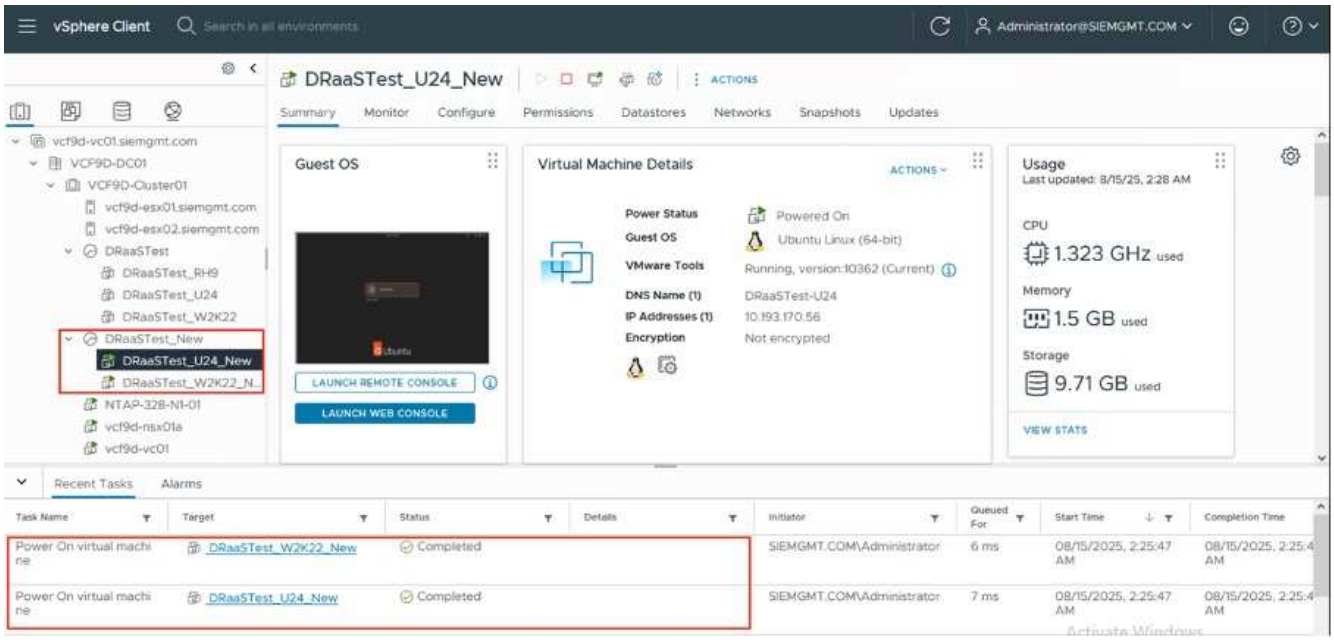
> BlueXP DRaaS replica (risincronizza) tutte le modifiche sulla macchina virtuale di origine prima di invertire la direzione della replica.

Questo processo inizia da una relazione che ha completato il failover verso una destinazione e prevede i seguenti passaggi:

- Spegnere e annullare la registrazione delle macchine virtuali e dei volumi sul sito di destinazione.



- Interrompere la relazione SnapMirror sulla sorgente originale per renderla di lettura/scrittura.
- Risincronizzare la relazione SnapMirror per invertire la replica.
- Montare il volume sulla sorgente, accendere e registrare le macchine virtuali di origine.

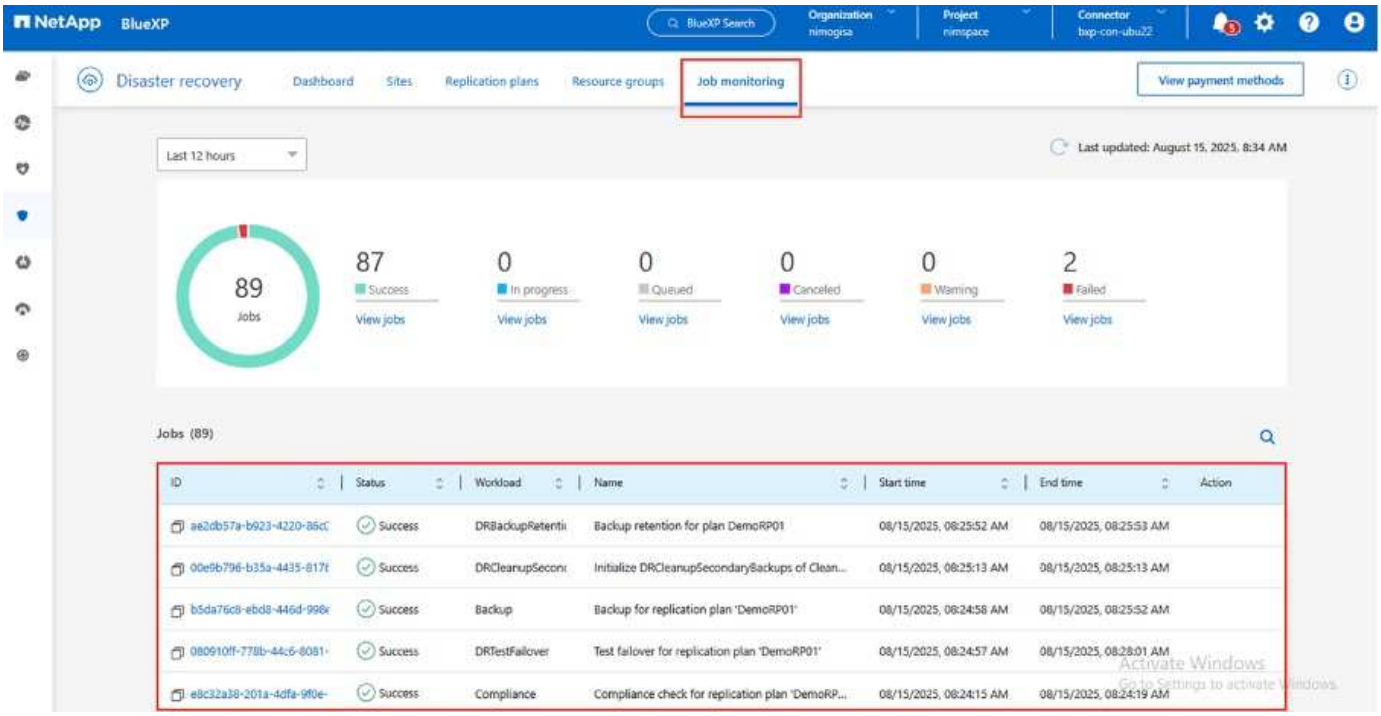


Per maggiori dettagli sull'accesso e la configurazione di BlueXP DRaaS, vedere"Scopri di più su BlueXP

Disaster Recovery per VMware" .

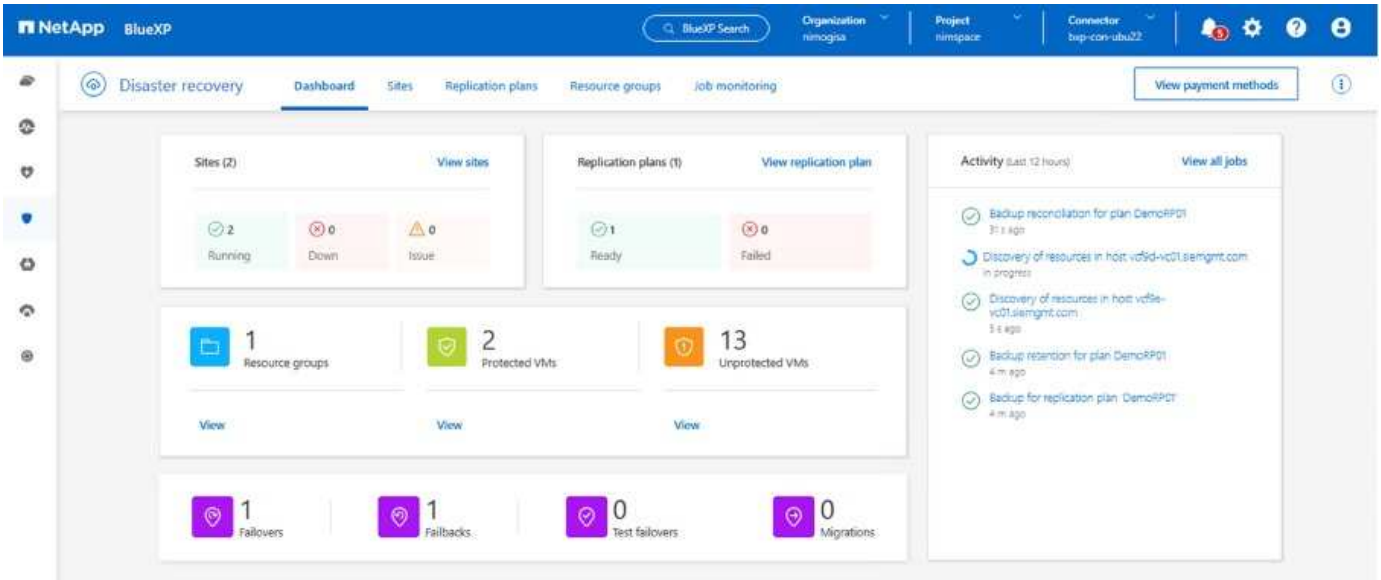
Monitoraggio e dashboard

Da BlueXP o dalla CLI ONTAP è possibile monitorare lo stato di integrità della replica per i volumi del datastore appropriati, mentre lo stato di un failover o di un failover di prova può essere monitorato tramite Job Monitoring.



Se un lavoro è in corso o in coda e si desidera interromperlo, è disponibile un'opzione per annullarlo.

Grazie alla dashboard BlueXP disaster recovery , puoi valutare con sicurezza lo stato dei siti di disaster recovery e dei piani di replica. Ciò consente agli amministratori di identificare rapidamente siti e piani integri, disconnessi o degradati.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Convertire i cluster vSphere esistenti in VCF

Scopri come convertire un ambiente vSphere con datastore esistenti in VCF

La conversione di un ambiente vSphere con datastore esistenti in esecuzione su ONTAP in un ambiente VMware Cloud Foundation (VCF) implica l'integrazione dell'infrastruttura attuale in una moderna architettura cloud privata.

Questo processo sfrutta la flessibilità dell'archiviazione ONTAP per un accesso e una gestione dei dati senza interruzioni. Una volta stabilito il dominio di gestione VCF, gli amministratori possono importare in modo efficiente altri ambienti vSphere nell'ecosistema VCF. Questa integrazione migliora l'utilizzo delle risorse, semplifica la gestione del cloud privato e garantisce una transizione fluida con un'interruzione minima dei carichi di lavoro esistenti.

Per i dettagli tecnici sulla conversione di un'istanza vCenter, fare riferimento alle seguenti soluzioni.

- "Convertire l'istanza vCenter esistente in dominio di gestione VCF (NFS)"
- "Convertire l'istanza vCenter (datastore FC) in dominio di gestione VCF"

Convertire l'istanza del server vCenter in dominio di gestione VCF (datastore NFS)

Converti un cluster vSphere 8 esistente con datastore NFS NetApp ONTAP in un dominio di gestione VMware Cloud Foundation (VCF). Questa procedura include il provisioning dello storage NFS, l'implementazione degli strumenti ONTAP per VMware e l'utilizzo dello strumento di importazione VCF per convertire il cluster per una gestione semplificata e un utilizzo ottimizzato delle risorse all'interno di VCF.

Introduzione

La conversione di un cluster con un datastore NFS esistente in esecuzione su ONTAP implica l'integrazione dell'infrastruttura esistente in una moderna architettura cloud privata. Questo processo trae vantaggio dalla flessibilità dell'archiviazione NFS, per garantire un accesso e una gestione dei dati senza interruzioni. Dopo aver stabilito un dominio di gestione VCF tramite il processo di conversione, gli amministratori possono importare in modo efficiente altri cluster vSphere, compresi quelli che utilizzano datastore NFS, nell'ecosistema VCF. Questa integrazione non solo migliora l'utilizzo delle risorse, ma semplifica anche la gestione dell'infrastruttura cloud privata, garantendo una transizione fluida con un'interruzione minima dei carichi di lavoro esistenti.

In questa soluzione mostreremo come un datastore NFS in vSphere 8 diventa un archivio principale quando il cluster viene convertito in un dominio di gestione VCF.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci gli ONTAP tools for VMware vSphere 10.
- Fornire un datastore NFS utilizzando gli strumenti ONTAP .

- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.
- Distribuire SDDC Manager nel cluster vSphere.
- Configurare un file JSON per creare NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per convertire il cluster vSphere 8 in VCF 5.2.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Sistema di archiviazione NetApp AFF con una macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi e un'appliance vCenter collocata sul cluster.
- Gruppo di porte distribuito configurato per il traffico di archiviazione vMotion e NFS sulle VLAN o sui segmenti di rete stabiliti a tale scopo.
- Scarica il software necessario per la conversione VCF.

Gli ONTAP tools for VMware vSphere 10 possono essere installati in configurazioni HA o non HA. Per informazioni complete sui prerequisiti per gli strumenti ONTAP fare riferimento a "Prerequisiti per gli ONTAP tools for VMware vSphere" .

Per l'archiviazione supportata e altre considerazioni per la conversione o l'importazione di vSphere in VCF 5.2, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Per il software richiesto, vai a "Portale di supporto Broadcom" .

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" .

Fasi di distribuzione

La soluzione prevede l'utilizzo di ONTAP tools for VMware vSphere per il provisioning di datastore NFS e il processo di conversione di un cluster vSphere 8 esistente in un dominio di gestione VCF.

Completare i seguenti passaggi:

- Distribuisci gli ONTAP tools for VMware vSphere 10.
- Fornire un datastore NFS utilizzando gli strumenti ONTAP .
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Distribuire la VM del gestore SDDC sul cluster vCenter.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di conversione.
- Caricare il software richiesto nel gestore SDDC.

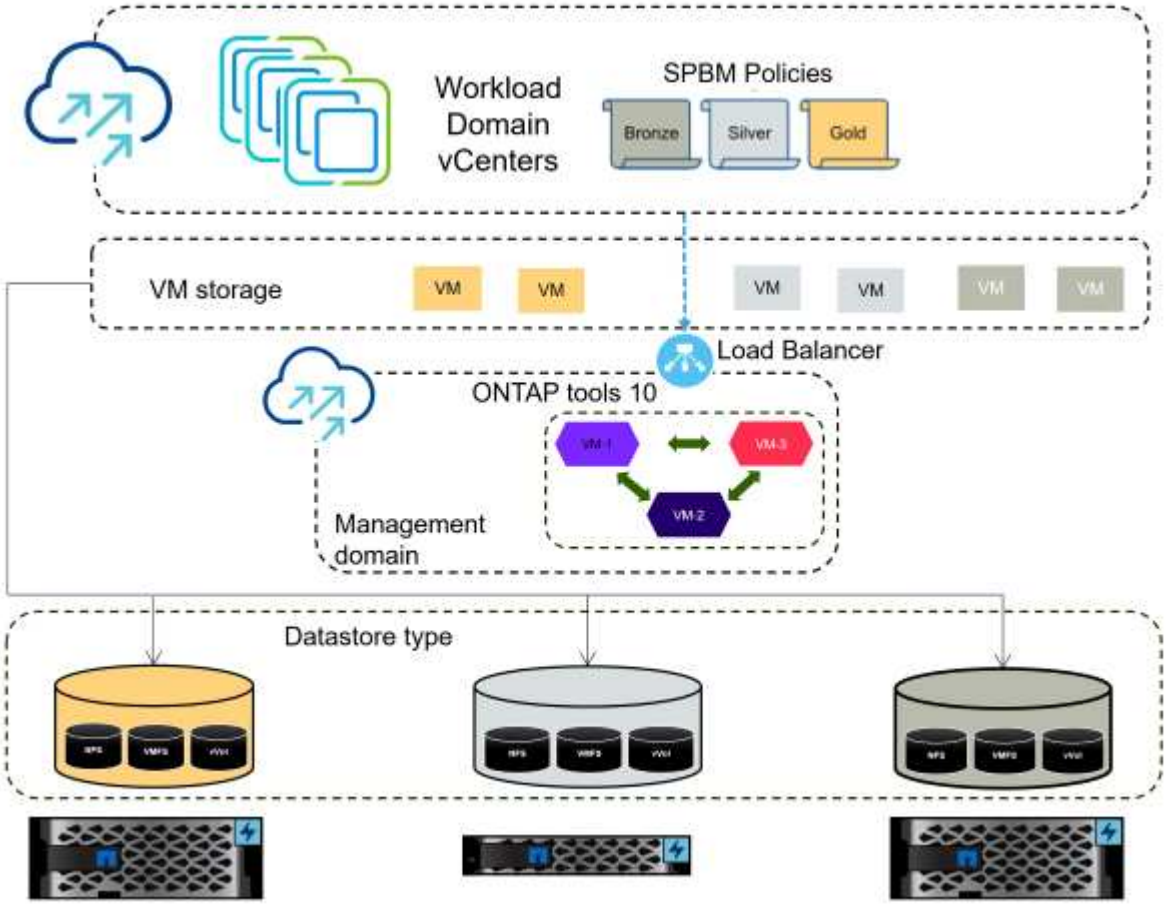
- Convertire il cluster vSphere nell'inventario del gestore SDDC.

Per una panoramica del processo di conversione, fare riferimento a "Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation" .

Distribuisci gli strumenti ONTAP e fornisci un datastore NFS

L'architettura degli strumenti ONTAP 10 è progettata per integrarsi perfettamente con gli ambienti VMware, sfruttando un framework modulare e scalabile che include i servizi degli strumenti ONTAP , il plug-in vSphere e le API REST per consentire una gestione efficiente dello storage, l'automazione e la protezione dei dati.

Gli ONTAP tools for VMware vSphere 10 possono essere installati in configurazioni HA o non HA.

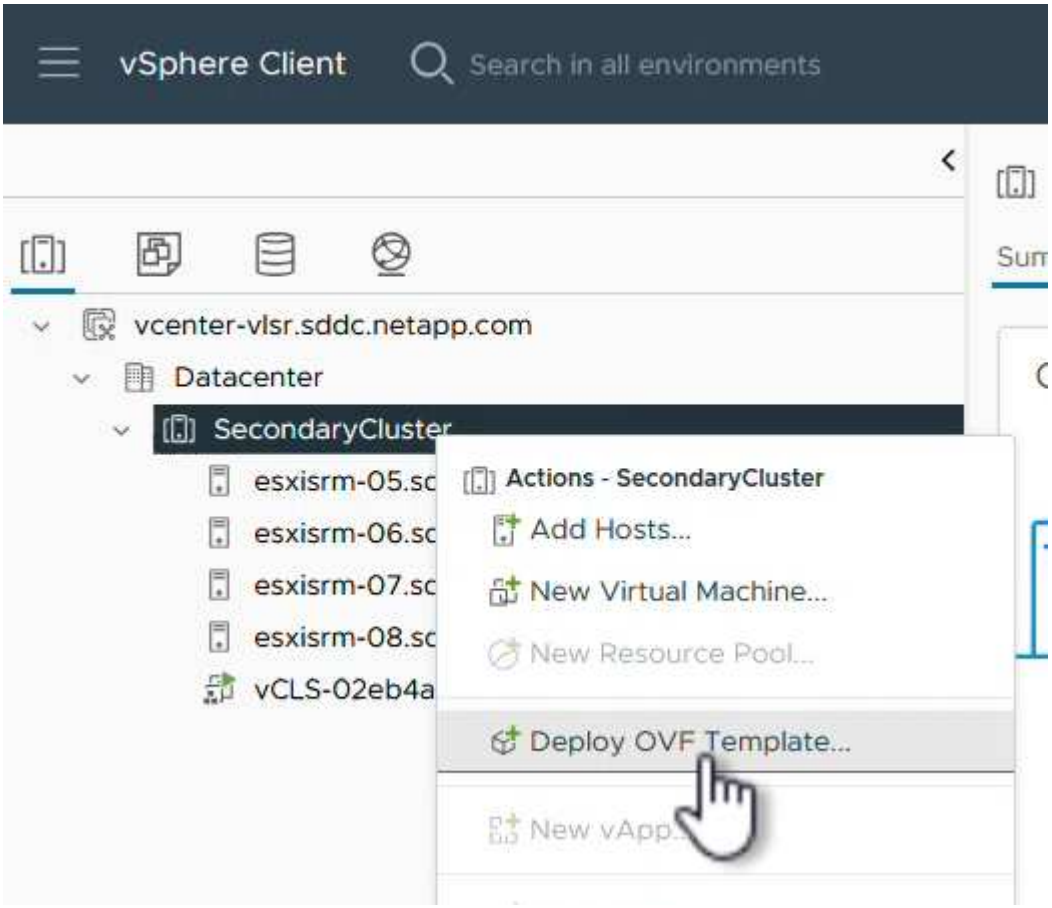


Distribuisci gli ONTAP tools for VMware vSphere 10

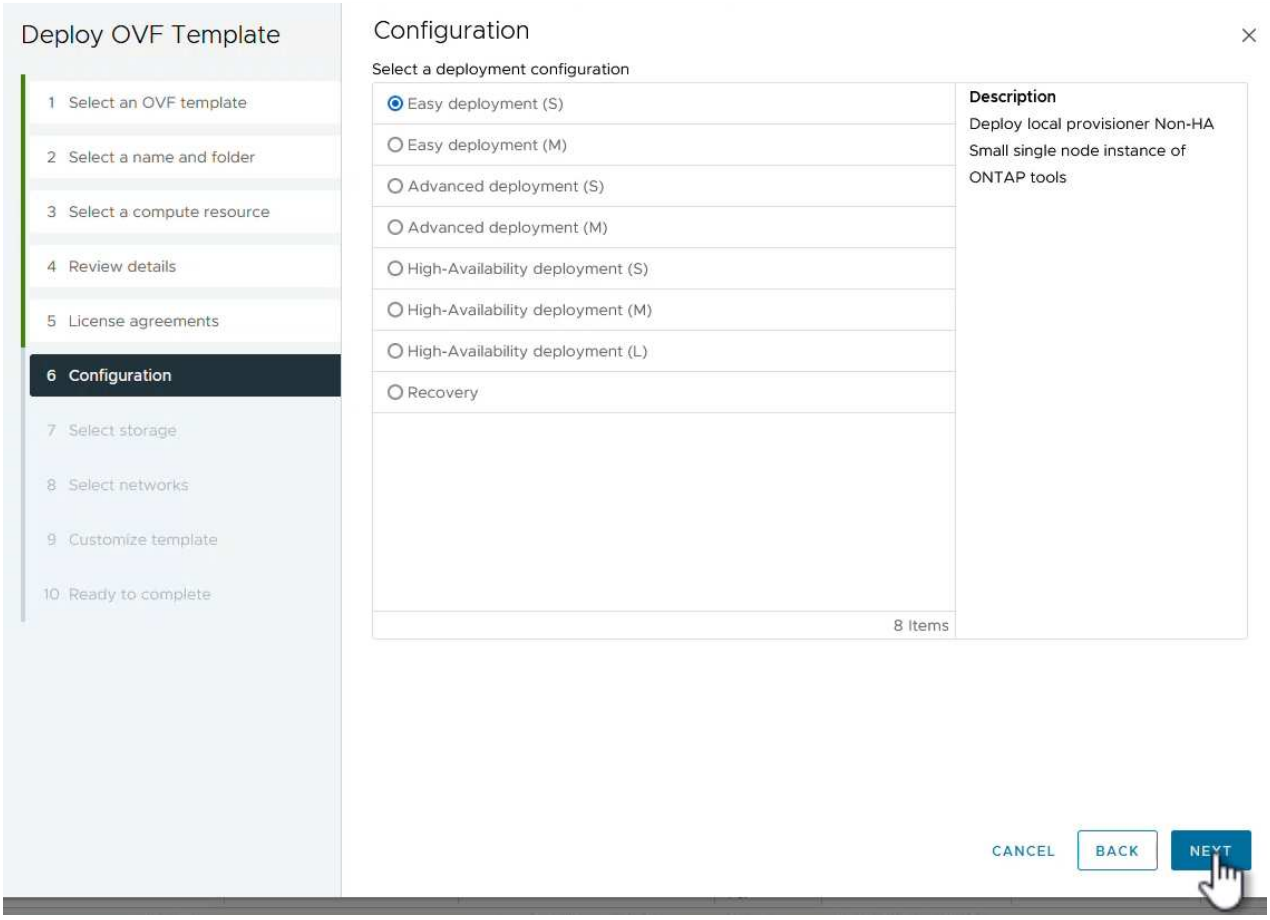
In questa fase gli strumenti ONTAP 10 vengono distribuiti con una configurazione non HA.

Per ulteriori dettagli sulla distribuzione delle configurazioni HA e non HA, fare riferimento a "Distribuisci gli ONTAP tools for VMware vSphere" .

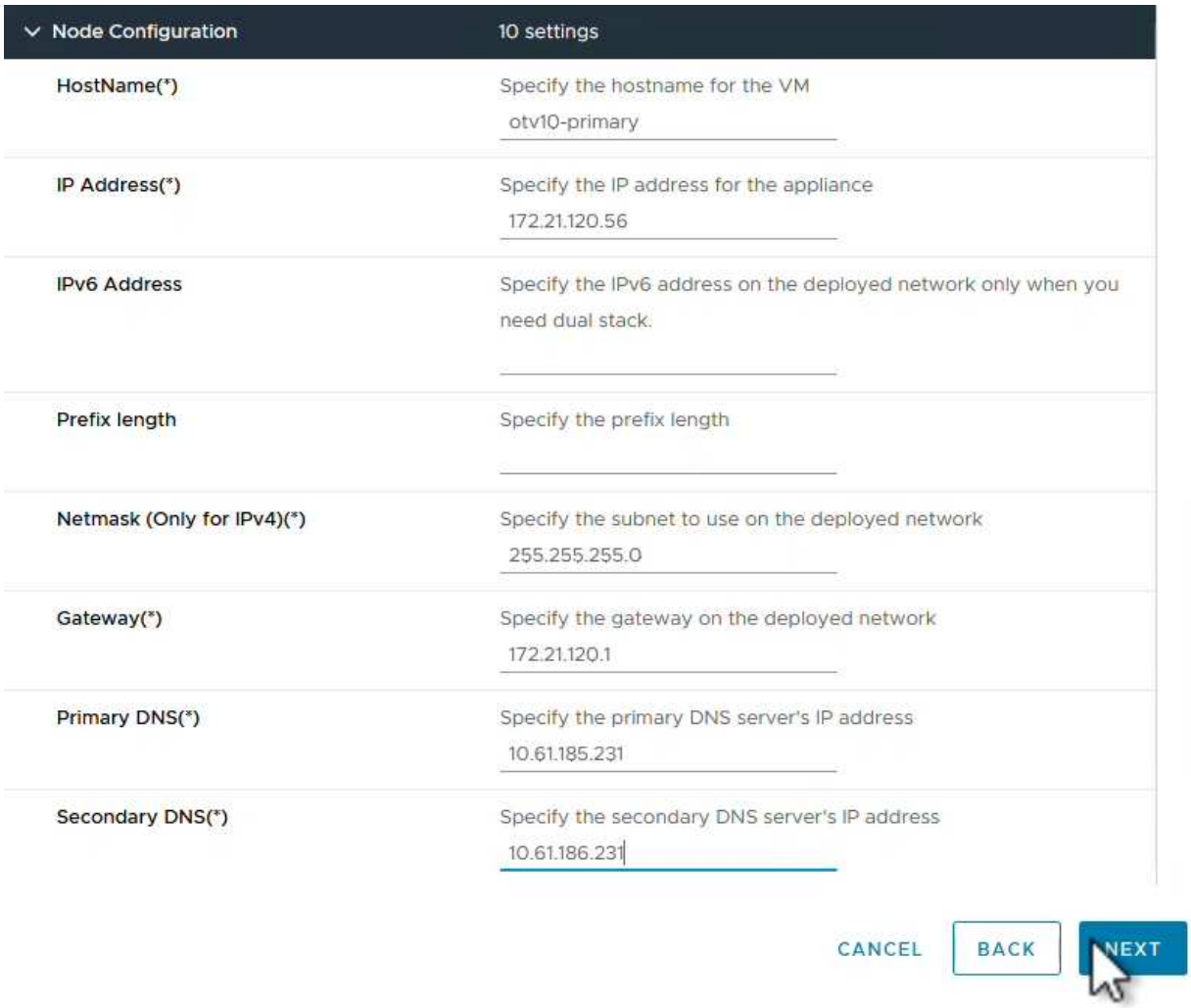
1. Scarica il modello OVA degli strumenti ONTAP 10 da "Sito di supporto NetApp" .
2. Nel client vSphere, fare clic con il pulsante destro del mouse sul cluster e fare clic su **Distribuisci modello OVF**



3. Nel **Modello di distribuzione OVF** completare i passaggi per:
   - Seleziona un modello OVF.
   - Seleziona un nome e una cartella.
   - Seleziona una risorsa di elaborazione.
   - Dettagli della recensione.
   - Accettare il contratto di licenza.
4. Nella pagina **Configurazione** del modello, selezionare il tipo di distribuzione, specificando se distribuire gli strumenti ONTAP in una configurazione HA. Fare clic su **Avanti** per continuare.



5. Nella pagina **Seleziona storage**, seleziona il datastore su cui installare la VM e fai clic su **Avanti**.
6. Selezionare la rete su cui comunicherà la VM degli strumenti ONTAP . Fare clic su **Avanti** per continuare.
7. Nella finestra "Personalizza modello", compila tutte le informazioni richieste.
    - Nome utente e password dell’applicazione
    - Scegliere se abilitare ASUP (supporto automatico) includendo un URL proxy.
    - Nome utente e password dell’amministratore.
    - Server NTP.
    - Nome utente e password di manutenzione (account di manutenzione utilizzato nella console).
    - Fornire gli indirizzi IP richiesti per la configurazione della distribuzione.
    - Fornire tutte le informazioni di rete per la configurazione del nodo.

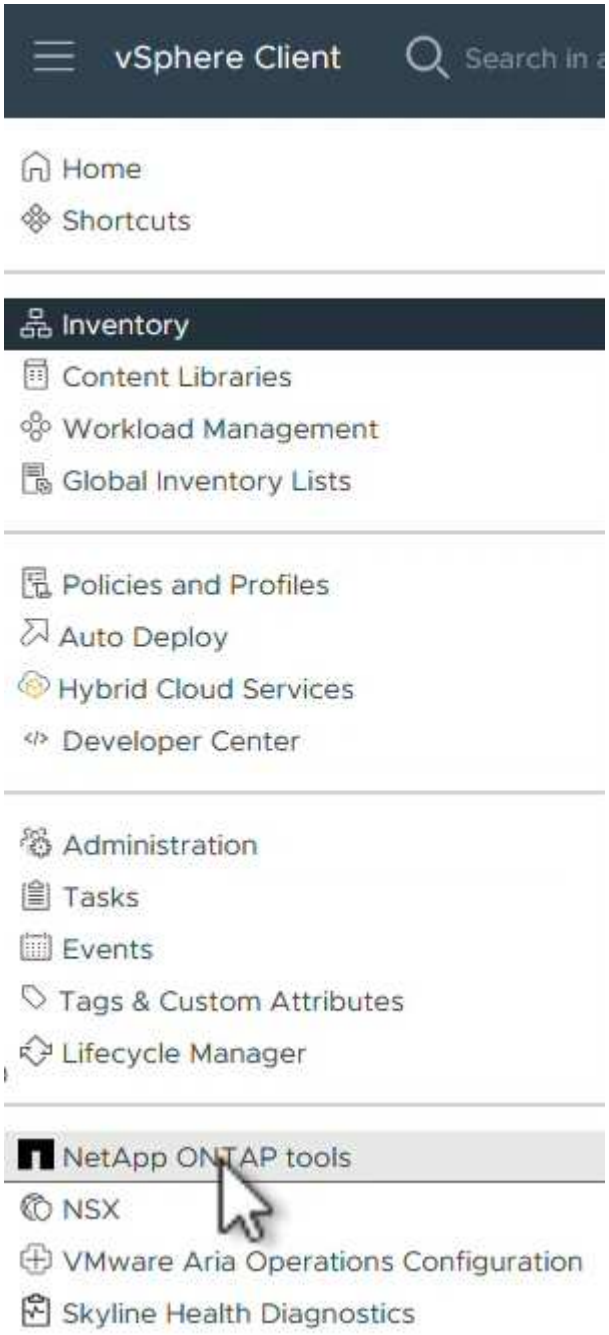


8. Infine, fare clic su **Avanti** per continuare e poi su **Fine** per iniziare la distribuzione.

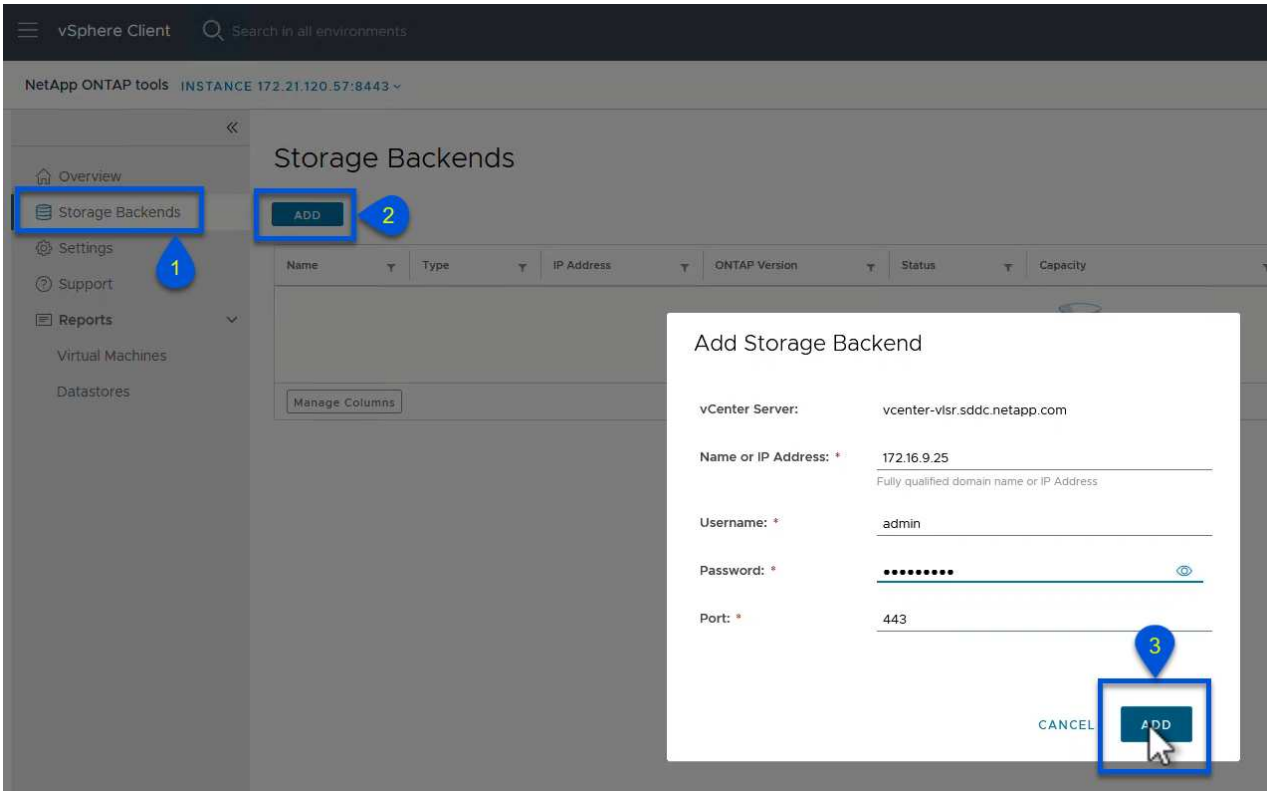
Configurare gli strumenti ONTAP

Una volta installata e avviata la VM degli strumenti ONTAP , saranno necessarie alcune configurazioni di base, come l'aggiunta di server vCenter e sistemi di storage ONTAP da gestire. Fare riferimento alla documentazione a "Documentazione ONTAP tools for VMware vSphere" per informazioni dettagliate.

1. Fare riferimento a "Aggiungi istanze vCenter" per configurare le istanze vCenter da gestire con gli strumenti ONTAP .
2. Per aggiungere un sistema di storage ONTAP , accedi al client vSphere e vai al menu principale a sinistra. Fare clic su *Strumenti NetApp ONTAP * per avviare l'interfaccia utente.



3. Vai su **Backend di archiviazione** nel menu a sinistra e clicca su **Aggiungi** per accedere alla finestra **Aggiungi backend di archiviazione**.
4. Compilare l'indirizzo IP e le credenziali per il sistema di archiviazione ONTAP da gestire. Fare clic su **Aggiungi** per terminare.

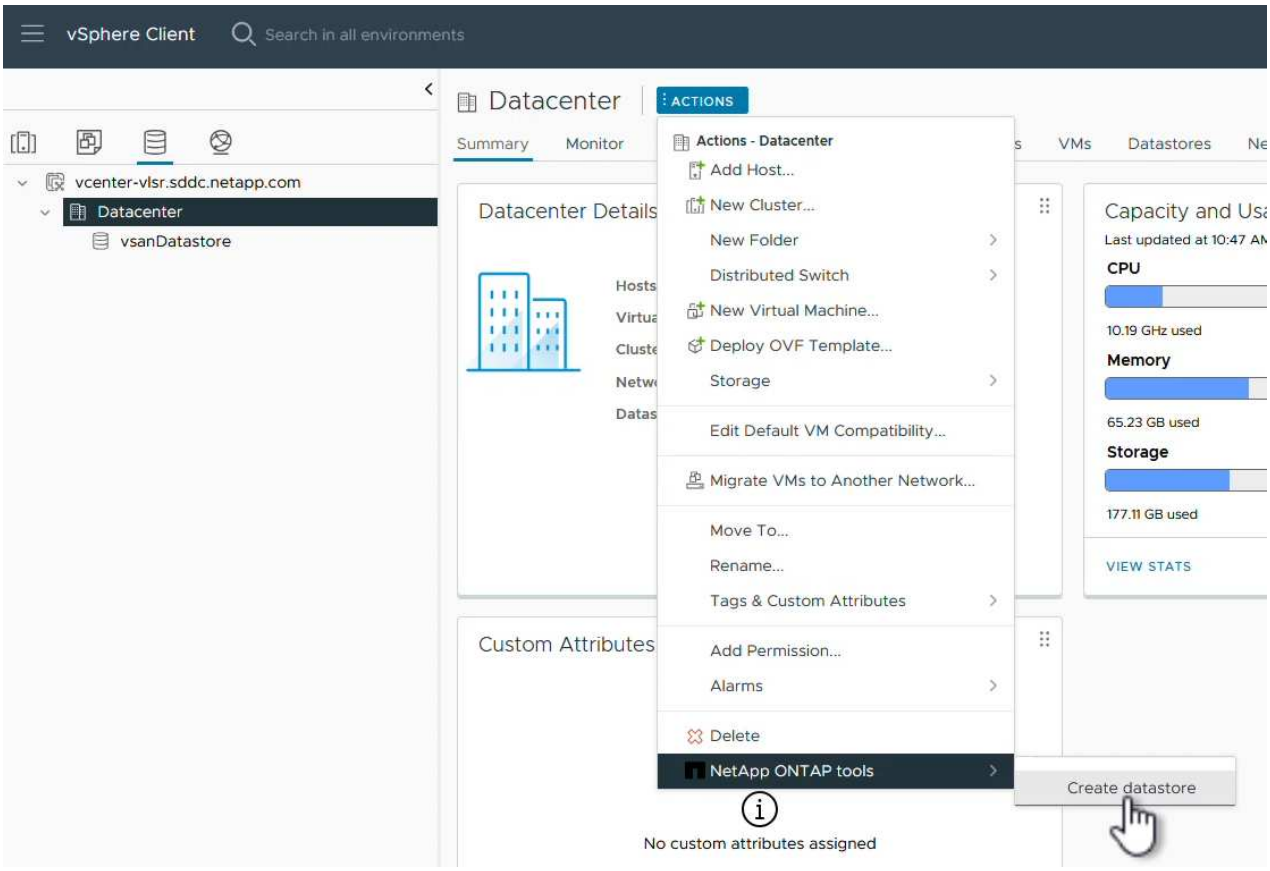


In questo caso, il backend di archiviazione viene aggiunto nell'interfaccia utente del client vSphere utilizzando l'indirizzo IP del cluster. Ciò consente la gestione completa di tutte le SVM nel sistema di archiviazione. In alternativa, il backend di archiviazione può essere aggiunto e associato a un'istanza vCenter utilizzando ONTAP Tools Manager in `https://loadBalanceIP:8443/virtualization/ui/` . Con questo metodo è possibile aggiungere solo le credenziali SVM all'interfaccia utente del client vSphere, garantendo un controllo più granulare sull'accesso allo storage.

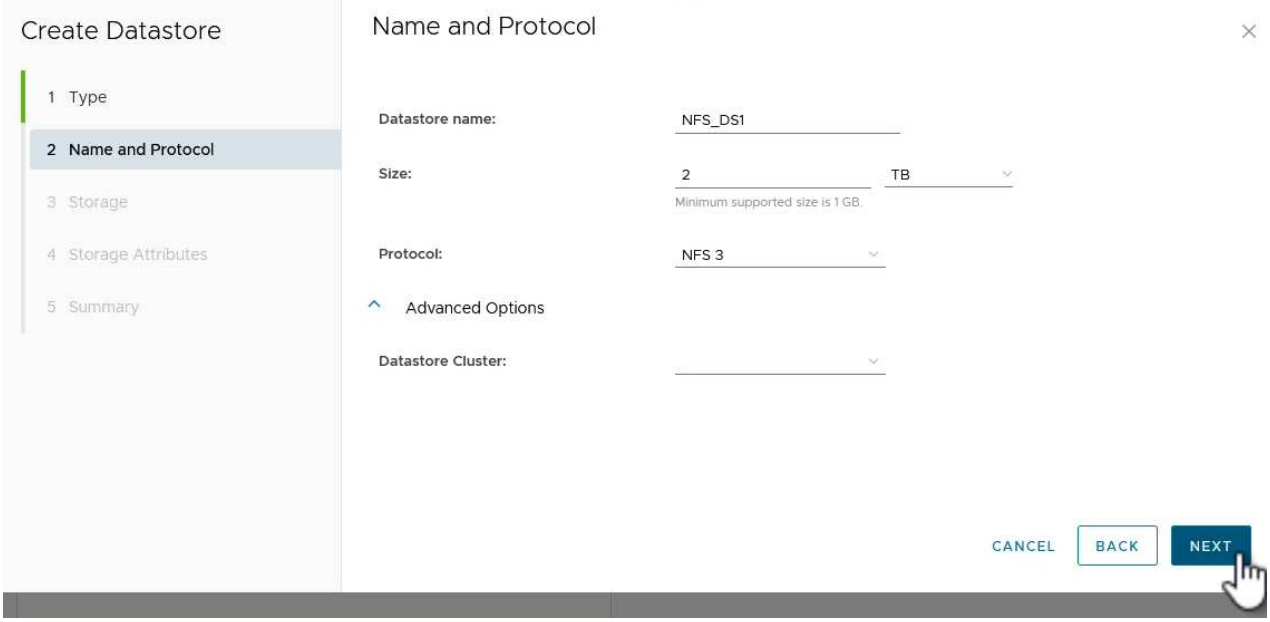
Fornire un datastore NFS con gli strumenti ONTAP

Gli strumenti ONTAP integrano le funzionalità nell'intera interfaccia utente del client vSphere. In questa fase verrà eseguito il provisioning di un datastore NFS dalla pagina dell'inventario di archiviazione.

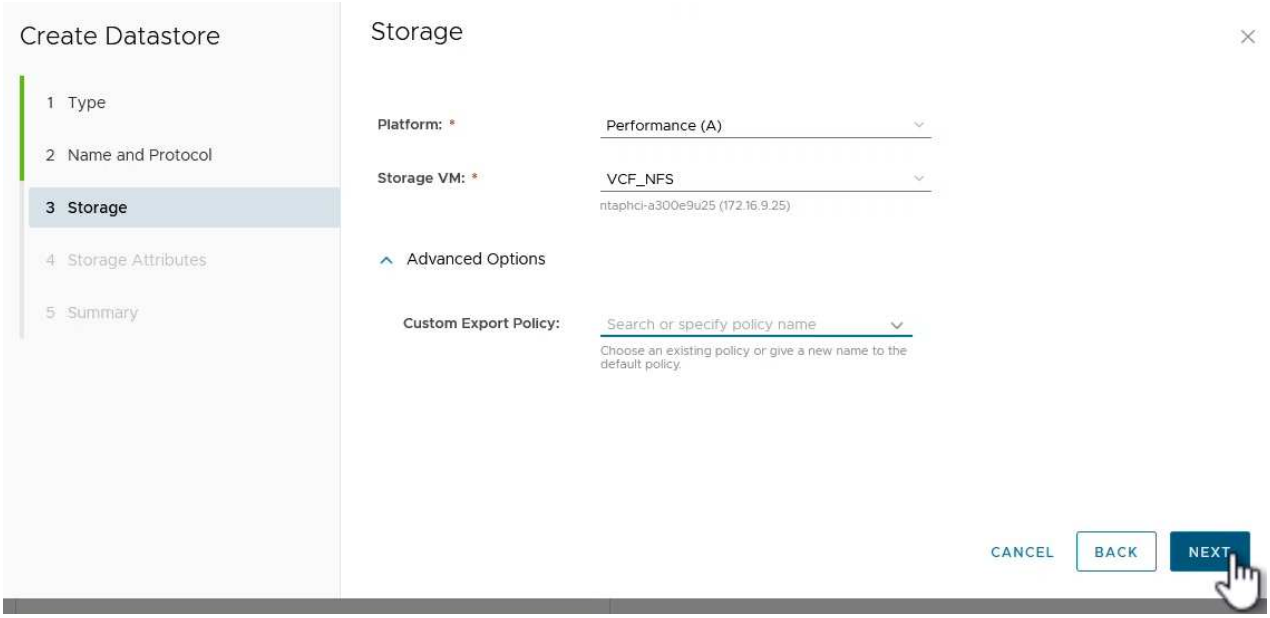
1. Nel client vSphere, accedere all'inventario di archiviazione.
2. Passare a **AZIONI > Strumenti NetApp ONTAP > Crea datastore**.



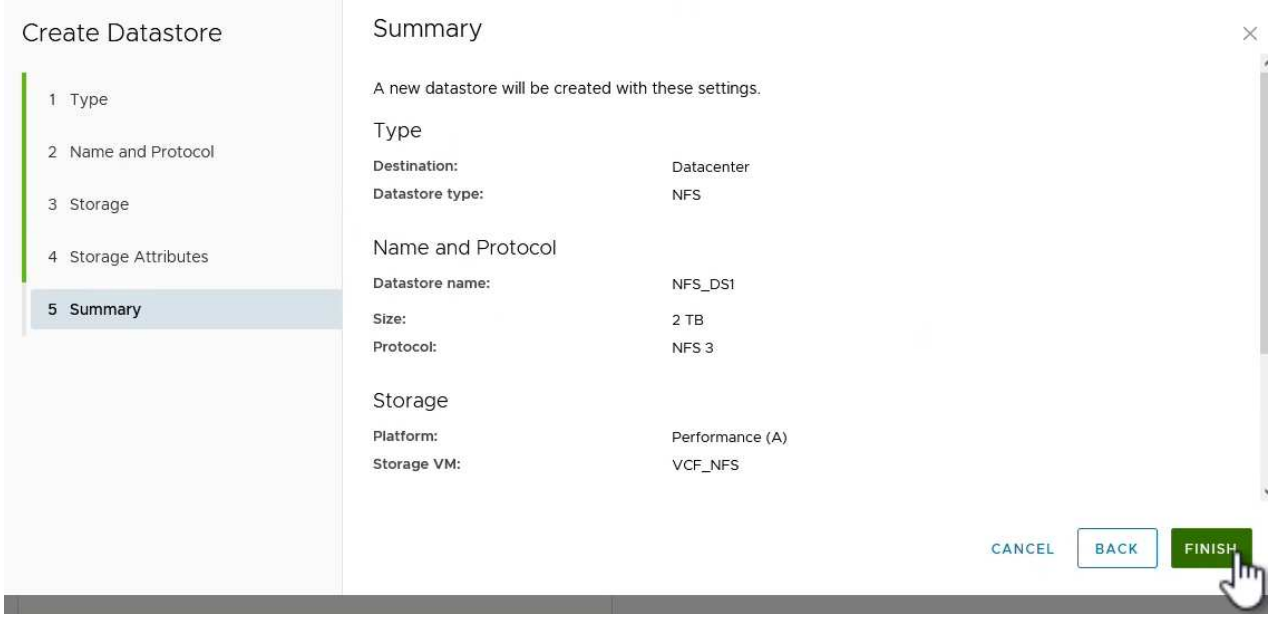
3. Nella procedura guidata **Crea datastore**, seleziona il tipo di datastore da creare. Le opzioni sono NFS o VMFS.
4. Nella pagina **Nome e protocollo**, inserisci un nome per il datastore, la dimensione e il protocollo NFS da utilizzare.



5. Nella pagina **Archiviazione**, selezionare la piattaforma di archiviazione ONTAP e la macchina virtuale di archiviazione (SVM). Qui puoi anche selezionare qualsiasi criterio di esportazione personalizzato disponibile. Fare clic su **Avanti** per continuare.



6. Nella pagina **Attributi di archiviazione** selezionare l'aggregato di archiviazione da utilizzare. Fare clic su **Avanti** per continuare.
7. Nella pagina **Riepilogo**, rivedere le informazioni e fare clic su **Fine** per avviare il processo di provisioning. Gli strumenti ONTAP creeranno un volume sul sistema di archiviazione ONTAP e lo monteranno come datastore NFS su tutti gli host ESXi nel cluster.



Convertire il cluster vSphere in VCF 5.2

Nella sezione seguente vengono illustrati i passaggi per distribuire il gestore SDDC e convertire il cluster vSphere 8 in un dominio di gestione VCF 5.2. Se del caso, per ulteriori dettagli si farà riferimento alla documentazione VMware.

VCF Import Tool, di VMware by Broadcom, è un'utilità utilizzata sia sull'appliance vCenter che sul gestore SDDC per convalidare le configurazioni e fornire servizi di conversione e importazione per gli ambienti vSphere e VCF.

Per ulteriori informazioni, consulta "Opzioni e parametri dello strumento di importazione VCF" .

Copia ed estrai lo strumento di importazione VCF

Gli strumenti di importazione VCF vengono utilizzati sull'appliance vCenter per verificare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

1. Segui i passaggi a "Copia lo strumento di importazione VCF nell'appliance vCenter di destinazione" in VMware Docs per copiare lo strumento di importazione VCF nella posizione corretta.
2. Estrarre il bundle utilizzando il seguente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Convalida l'appliance vCenter

Utilizzare lo strumento di importazione VCF per convalidare l'appliance vCenter prima della conversione.

1. Segui i passaggi a "Eseguire un pre-controllo sul vCenter di destinazione prima della conversione" per eseguire la convalida.
2. L'output seguente mostra che l'appliance vCenter ha superato il pre-controllo.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Distribuire SDDC Manager

Il gestore SDDC deve essere collocato sul cluster vSphere che verrà convertito in un dominio di gestione VCF.

Per completare la distribuzione, seguire le istruzioni di distribuzione in VMware Docs.

Fare riferimento a "Distribuire l'appliance SDDC Manager sul vCenter di destinazione" .

Per maggiori informazioni vedere"Host della Commissione" nella Guida all'amministrazione VCF.

Creare un file JSON per la distribuzione NSX

Per distribuire NSX Manager durante l'importazione o la conversione di un ambiente vSphere in VMware Cloud Foundation, creare una specifica di distribuzione NSX. Per la distribuzione di NSX sono necessari almeno 3 host.

> Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzata la rete NSX-VLAN. Per informazioni dettagliate sulle limitazioni della rete NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Di seguito è riportato un esempio di file JSON per la distribuzione NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copiare il file JSON in una directory su SDDC Manager.

Carica il software su SDDC Manager

Copiare lo strumento di importazione VCF e il bundle di distribuzione NSX nella directory /home/vcf/vcfimport su SDDC Manager.

Vedere "Caricare il software richiesto sull'appliance SDDC Manager" per istruzioni dettagliate.

Convertire il cluster vSphere in dominio di gestione VCF

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF. Eseguire il seguente comando dalla directory /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset per visualizzare una stampa delle funzioni dello strumento di importazione VCF:

```
python3 vcf_brownfield.py --help
```

Per convertire il cluster vSphere in un dominio di gestione VCF e distribuire il cluster NSX, eseguire il comando seguente:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Per istruzioni complete, fare riferimento a "Convertire o importare l'ambiente vSphere nell'inventario di SDDC Manager" .

Aggiungere la licenza al VCF

Dopo aver completato la conversione, è necessario aggiungere la licenza all'ambiente.

1. Accedi all'interfaccia utente di SDDC Manager.
2. Nel riquadro di navigazione, vai su **Amministrazione > Licenze**.
3. Fare clic su **+ Chiave di licenza**.
4. Scegli un prodotto dal menu a discesa.
5. Inserisci la chiave di licenza.
6. Fornire una descrizione della licenza.
7. Fare clic su **Aggiungi**.
8. Ripetere questi passaggi per ogni licenza.

Demo video per gli ONTAP tools for VMware vSphere 10

Datastore NFS con ONTAP tools for VMware vSphere 10

Convertire l’istanza del server vCenter in dominio di gestione VCF (datastore FC)

Convertire un cluster vSphere 8 utilizzando datastore ONTAP Fibre Channel in un dominio di gestione VMware Cloud Foundation. Questa procedura include il provisioning dello storage FC, l’implementazione degli strumenti ONTAP per VMware e l’utilizzo dello strumento di importazione VCF per migrare e gestire il cluster all’interno dell’ambiente VCF.

Introduzione

La conversione di un ambiente vSphere, con un datastore Fibre Channel (FC) esistente in esecuzione su ONTAP, implica l’integrazione dell’infrastruttura esistente in una moderna architettura cloud privata. Questo processo trae vantaggio dalla robustezza dell’archiviazione FC, per garantire un accesso e una gestione dei dati senza interruzioni. Dopo aver stabilito un dominio di gestione VCF tramite il processo di conversione, gli amministratori possono importare in modo efficiente altri ambienti vSphere, compresi quelli che utilizzano datastore FC, nell’ecosistema VCF. Questa integrazione non solo migliora l’utilizzo delle risorse, ma semplifica anche la gestione dell’infrastruttura cloud privata, garantendo una transizione fluida con un’interruzione minima dei carichi di lavoro esistenti.

In questa soluzione mostreremo come un datastore FC in vSphere 8 diventa un archivio principale quando il cluster viene convertito in un dominio di gestione VCF.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci gli ONTAP tools for VMware vSphere 10.
- Fornire un datastore FC utilizzando gli strumenti ONTAP .
- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.
- Distribuire SDDC Manager nel cluster vSphere.
- Configurare un file JSON per creare NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per convertire il cluster vSphere 8 in VCF 5.2.1

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Sistema di archiviazione NetApp ASA R2/ ASA/ AFF con una macchina virtuale di archiviazione (SVM) configurata per consentire il traffico Fibre Channel (FC).
- L’interfaccia logica (LIF) è stata creata per trasportare il traffico FC ed è associata all’SVM.
- La suddivisione in zone FC è stata configurata sugli switch designati per trasportare il traffico FC.
- Un cluster vSphere 8 con 4 host ESXi e un’appliance vCenter collocata sul cluster.
- Gruppo di porte distribuito configurato per vMotion sulle VLAN o sui segmenti di rete stabiliti a tale scopo.
- Scarica il software necessario per la conversione VCF.

Gli ONTAP tools for VMware vSphere 10 possono essere installati in configurazioni HA o non HA. Per informazioni complete sui prerequisiti per gli strumenti ONTAP fare riferimento a "Prerequisiti per gli ONTAP tools for VMware vSphere" .

Per l'archiviazione supportata e altre considerazioni per la conversione o l'importazione di vSphere in VCF 5.2, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Per il software richiesto fare riferimento a "Scarica il software per convertire o importare ambienti vSphere esistenti" .

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 5.2" .

Fasi di distribuzione

La soluzione prevede l'utilizzo di ONTAP tools for VMware vSphere per il provisioning di datastore FC e il processo di conversione di un cluster vSphere 8 esistente in un dominio di gestione VCF.

Completare i seguenti passaggi:

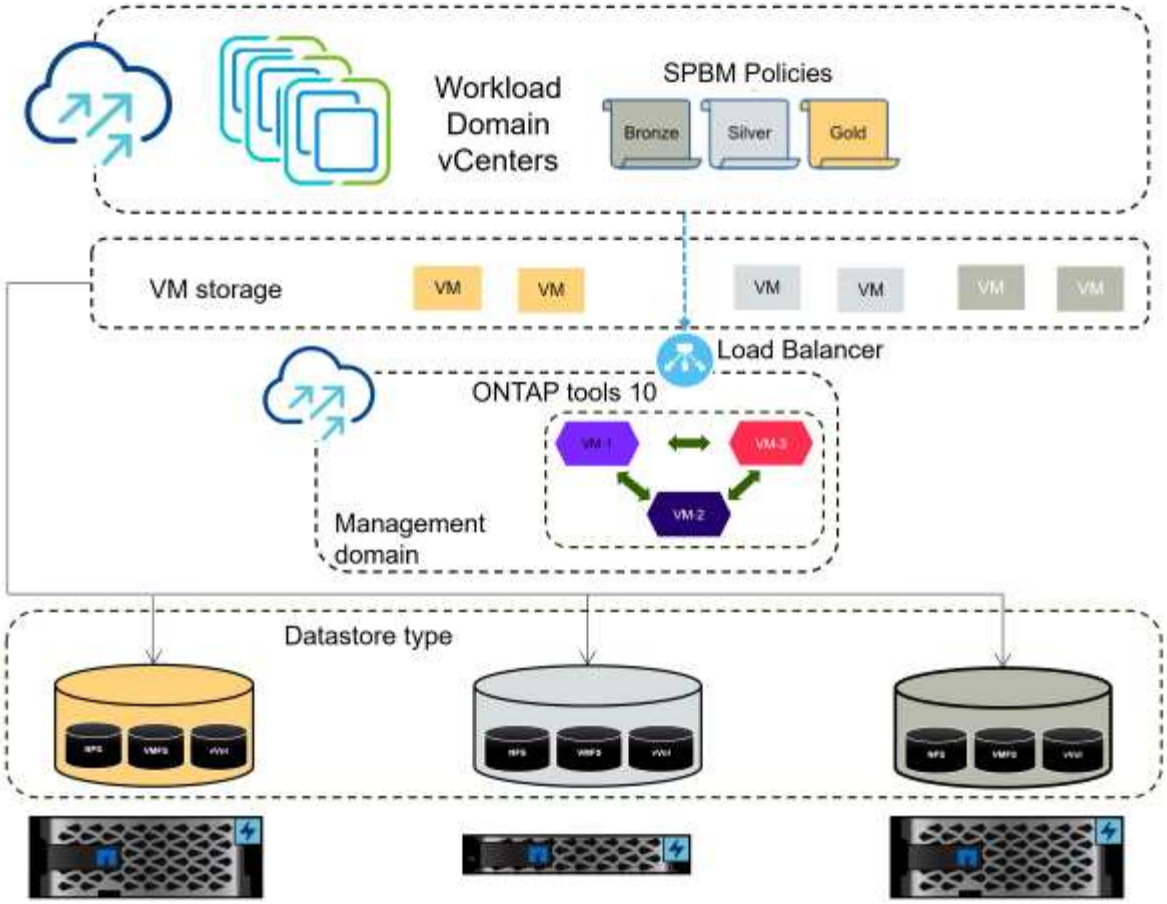
- Distribuisci gli ONTAP tools for VMware vSphere 10.
- Fornire un datastore FC utilizzando gli strumenti ONTAP .
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Distribuire la VM del gestore SDDC sul cluster vCenter.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di conversione.
- Caricare il software richiesto nel gestore SDDC.
- Convertire il cluster vSphere nell'inventario del gestore SDDC.

Per una panoramica del processo di conversione, fare riferimento a "Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation" .

Distribuisci gli strumenti ONTAP e fornisci un datastore FC

L'architettura degli strumenti ONTAP 10 è progettata per integrarsi perfettamente con gli ambienti VMware, sfruttando un framework modulare e scalabile che include i servizi degli strumenti ONTAP , il plug-in vSphere e le API REST per consentire una gestione efficiente dello storage, l'automazione e la protezione dei dati.

Gli ONTAP tools for VMware vSphere 10 possono essere installati in configurazioni HA o non HA.

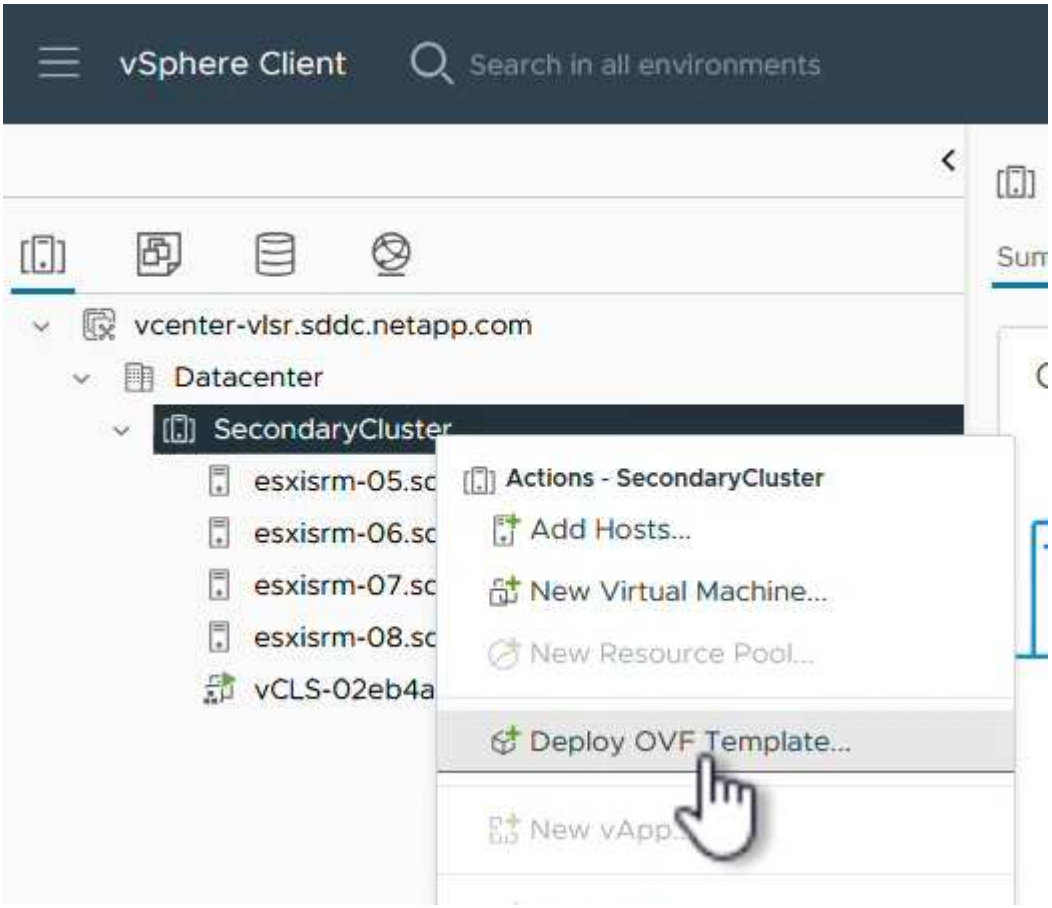

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

Distribuisci gli ONTAP tools for VMware vSphere 10

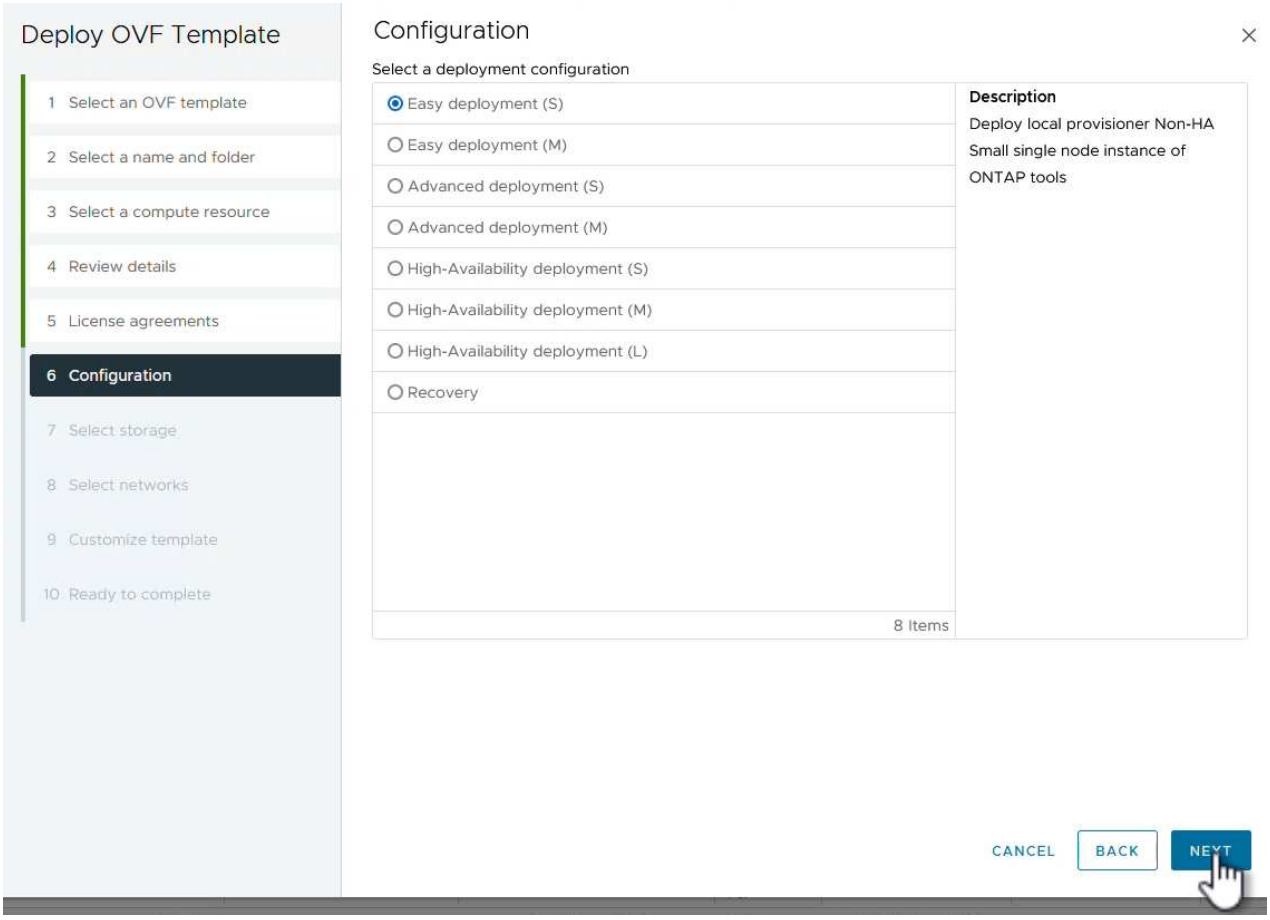
In questa fase gli strumenti ONTAP 10 vengono distribuiti con una configurazione non HA.

Per ulteriori dettagli sulla distribuzione delle configurazioni HA e non HA, fare riferimento a "Distribuisci gli ONTAP tools for VMware vSphere" .

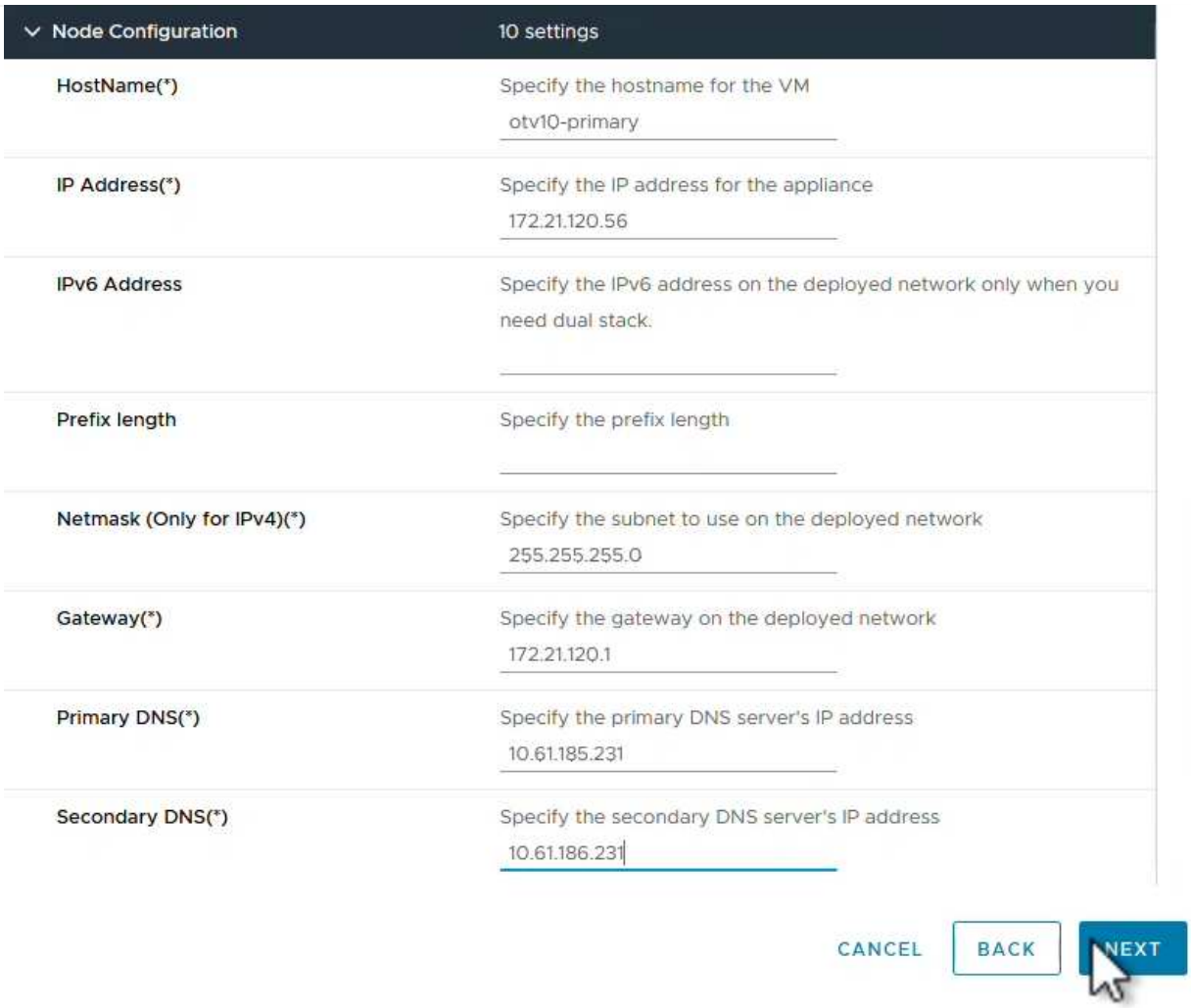
1. Scarica il modello OVA degli strumenti ONTAP 10 da "Sito di supporto NetApp" .
2. Nel client vSphere, fare clic con il pulsante destro del mouse sul cluster e fare clic su **Distribuisci modello OVF**



3. Nel **Modello di distribuzione OVF** completare i passaggi per:
   - Seleziona un modello OVF.
   - Seleziona un nome e una cartella.
   - Seleziona una risorsa di elaborazione.
   - Dettagli della recensione.
   - Accettare il contratto di licenza.
4. Nella pagina **Configurazione** del modello, selezionare il tipo di distribuzione, specificando se distribuire gli strumenti ONTAP in una configurazione HA. Fare clic su **Avanti** per continuare.



5. Nella pagina **Seleziona storage**, seleziona il datastore su cui installare la VM e fai clic su **Avanti**.
6. Selezionare la rete su cui comunicherà la VM degli strumenti ONTAP . Fare clic su **Avanti** per continuare.
7. Nella finestra "Personalizza modello", compila tutte le informazioni richieste.
    - Nome utente e password dell’applicazione
    - Scegliere se abilitare ASUP (supporto automatico) includendo un URL proxy.
    - Nome utente e password dell’amministratore.
    - Server NTP.
    - Nome utente e password di manutenzione (account di manutenzione utilizzato nella console).
    - Fornire gli indirizzi IP richiesti per la configurazione della distribuzione.
    - Fornire tutte le informazioni di rete per la configurazione del nodo.

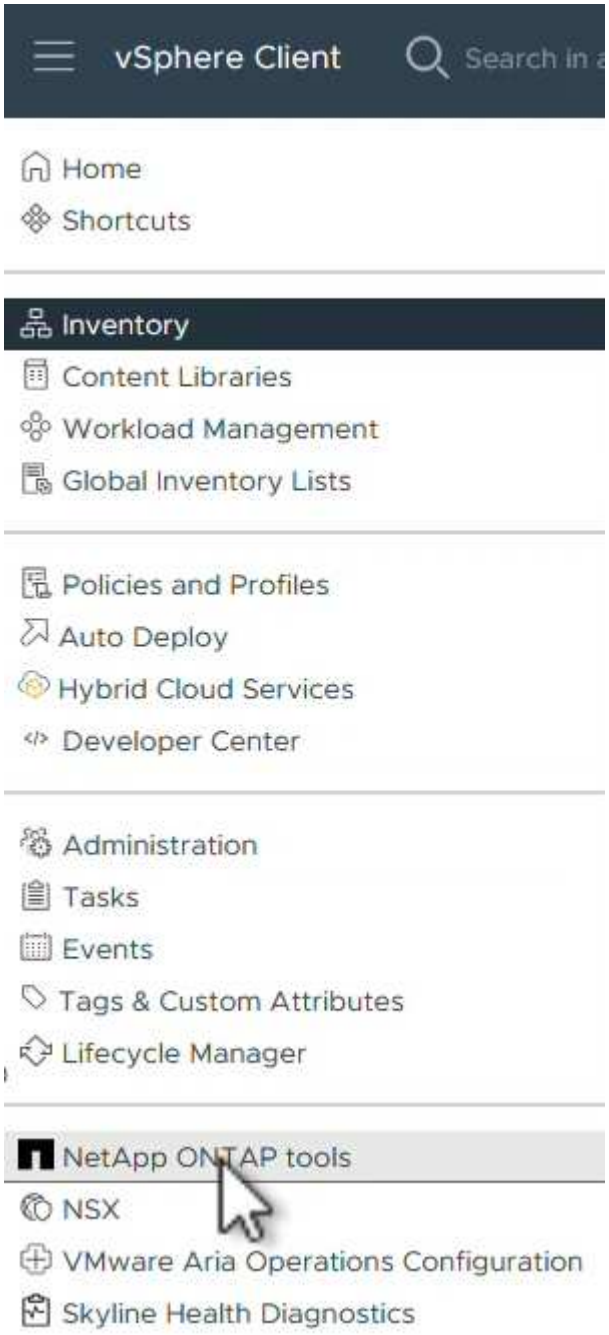


8. Infine, fare clic su **Avanti** per continuare e poi su **Fine** per iniziare la distribuzione.

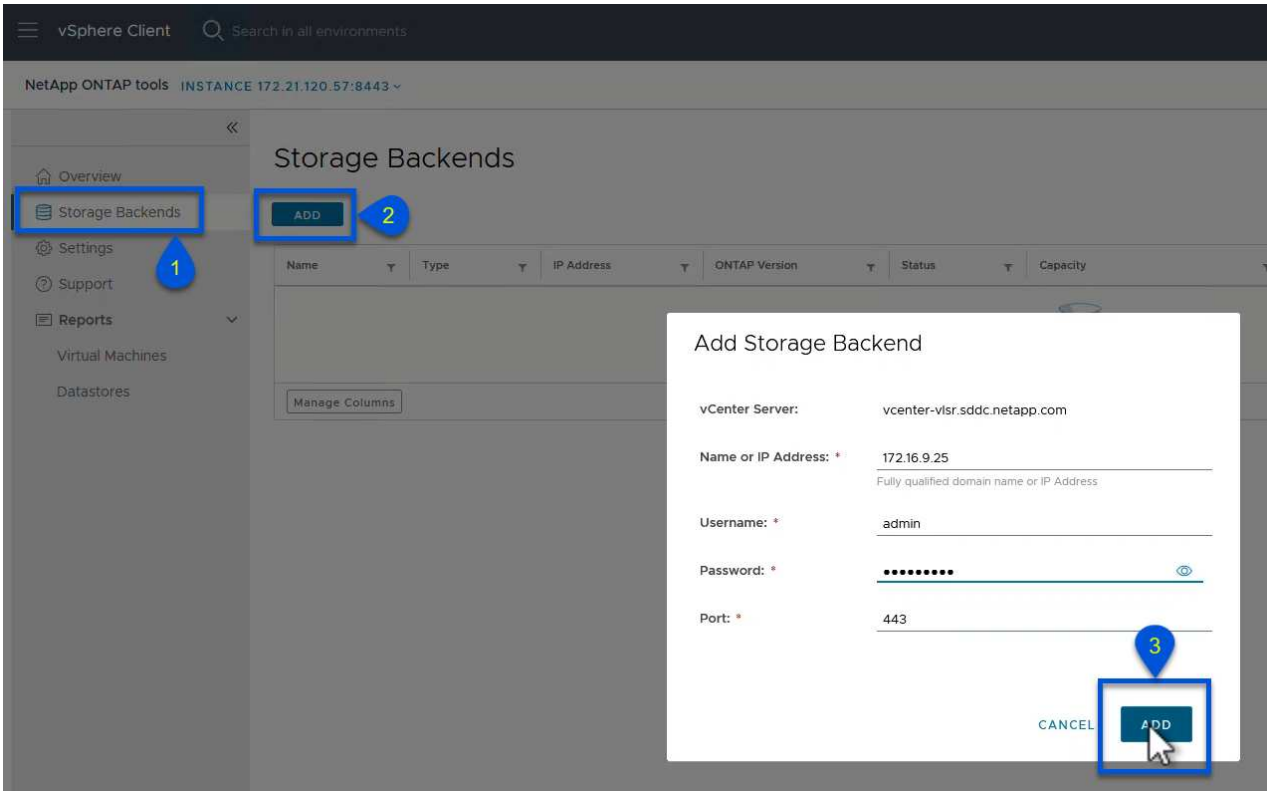
Configurare gli strumenti ONTAP

Una volta installata e avviata la VM degli strumenti ONTAP , saranno necessarie alcune configurazioni di base, come l'aggiunta di server vCenter e sistemi di storage ONTAP da gestire. Fare riferimento alla documentazione a "Documentazione ONTAP tools for VMware vSphere" per informazioni dettagliate.

1. Fare riferimento a "Aggiungi istanze vCenter" per configurare le istanze vCenter da gestire con gli strumenti ONTAP .
2. Per aggiungere un sistema di storage ONTAP , accedi al client vSphere e vai al menu principale a sinistra. Fare clic su *Strumenti NetApp ONTAP * per avviare l'interfaccia utente.



3. Vai su **Backend di archiviazione** nel menu a sinistra e clicca su **Aggiungi** per accedere alla finestra **Aggiungi backend di archiviazione**.
4. Compilare l'indirizzo IP e le credenziali per il sistema di archiviazione ONTAP da gestire. Fare clic su **Aggiungi** per terminare.

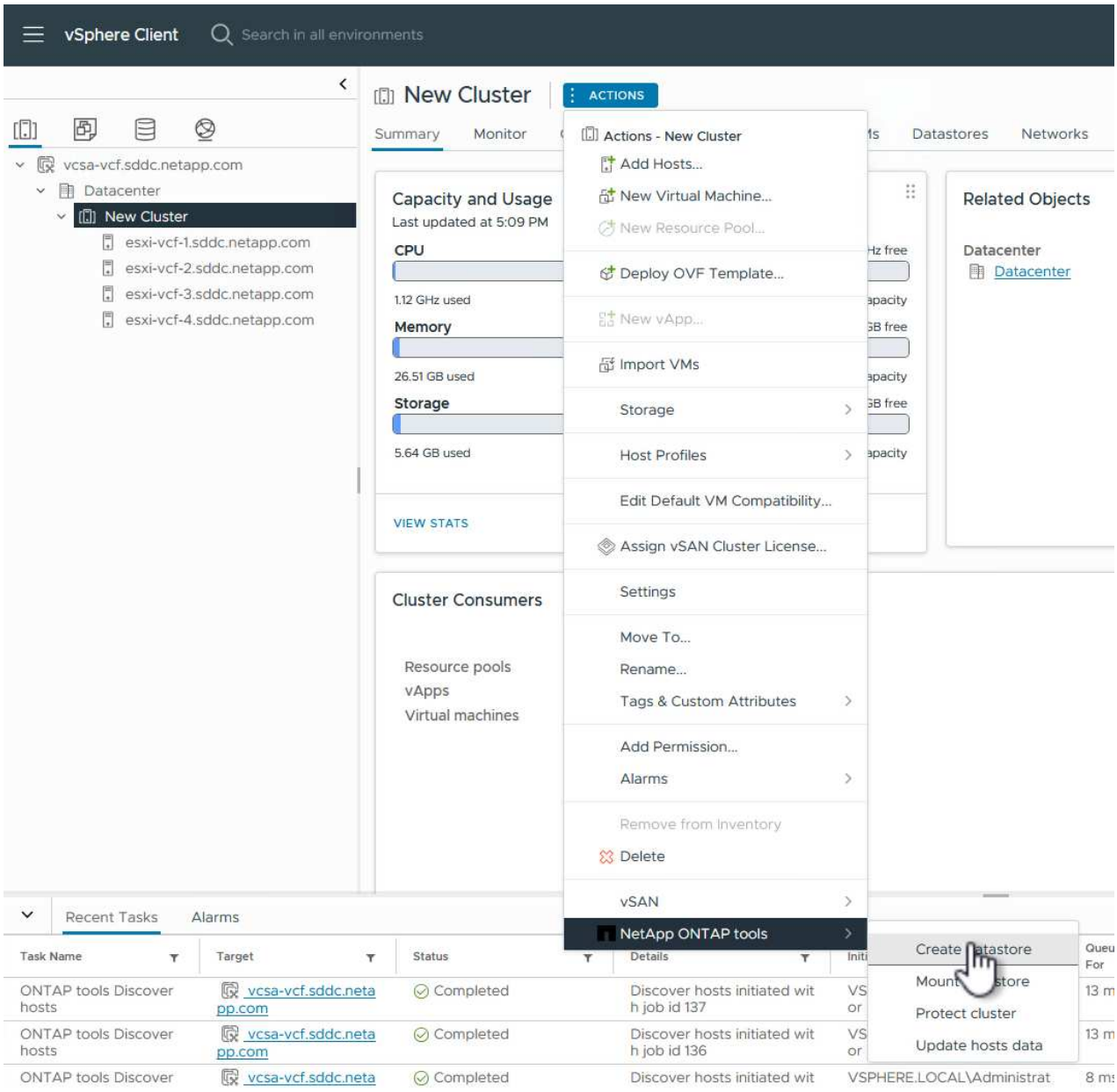


In questo caso, il backend di archiviazione viene aggiunto nell'interfaccia utente del client vSphere utilizzando l'indirizzo IP del cluster. Ciò consente la gestione completa di tutte le SVM nel sistema di archiviazione. In alternativa, il backend di archiviazione può essere aggiunto e associato a un'istanza vCenter utilizzando ONTAP Tools Manager in `https://loadBalanceIP:8443/virtualization/ui/` . Con questo metodo è possibile aggiungere solo le credenziali SVM all'interfaccia utente del client vSphere, garantendo un controllo più granulare sull'accesso allo storage.

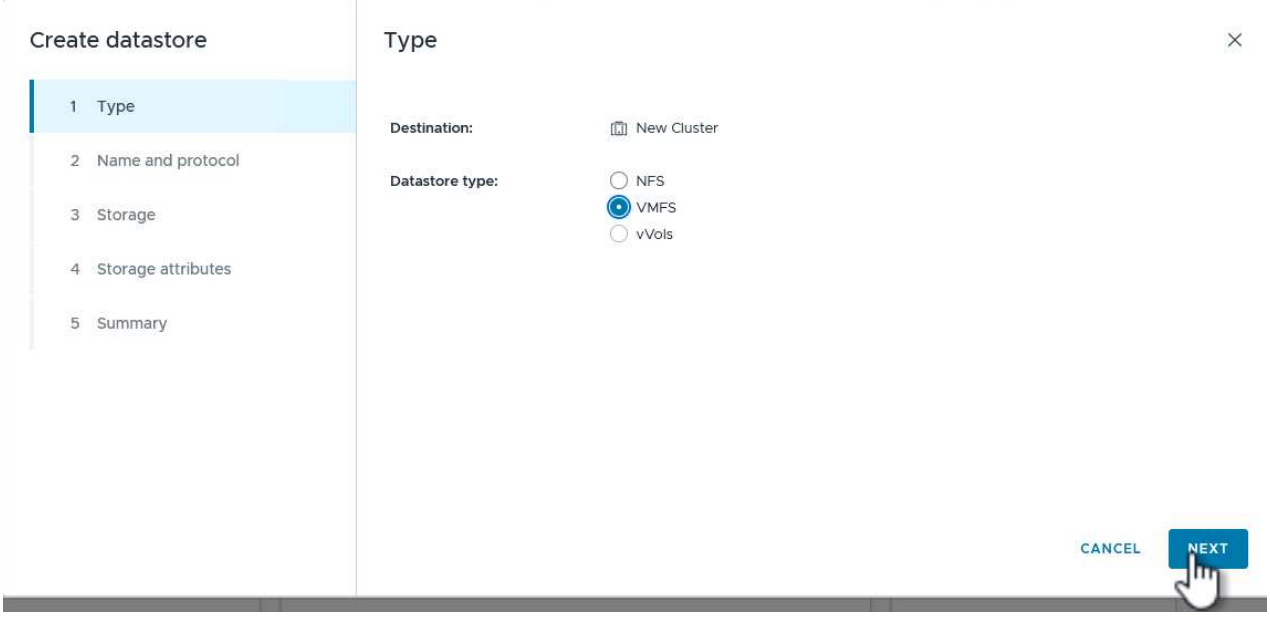
Fornire un datastore FC con strumenti ONTAP

Gli strumenti ONTAP integrano le funzionalità nell'intera interfaccia utente del client vSphere. In questa fase verrà eseguito il provisioning di un datastore FC dalla pagina dell'inventario degli host.

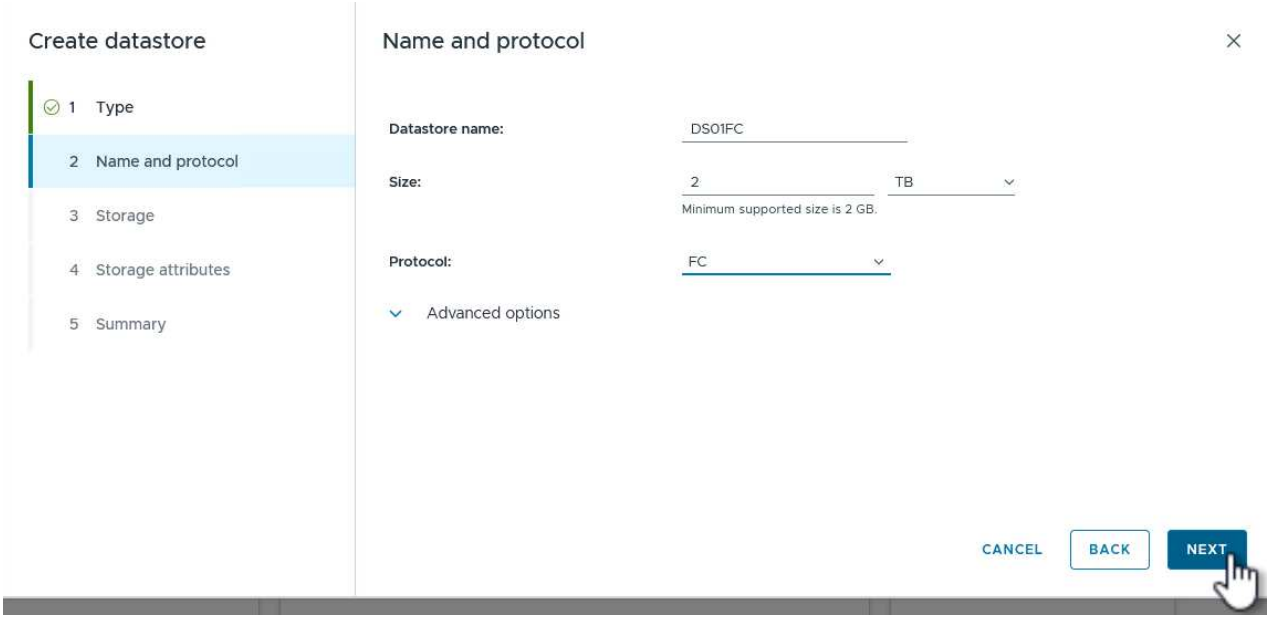
1. Nel client vSphere, accedere all'inventario degli host (o dello storage).
2. Passare a **AZIONI > Strumenti NetApp ONTAP > Crea datastore**.



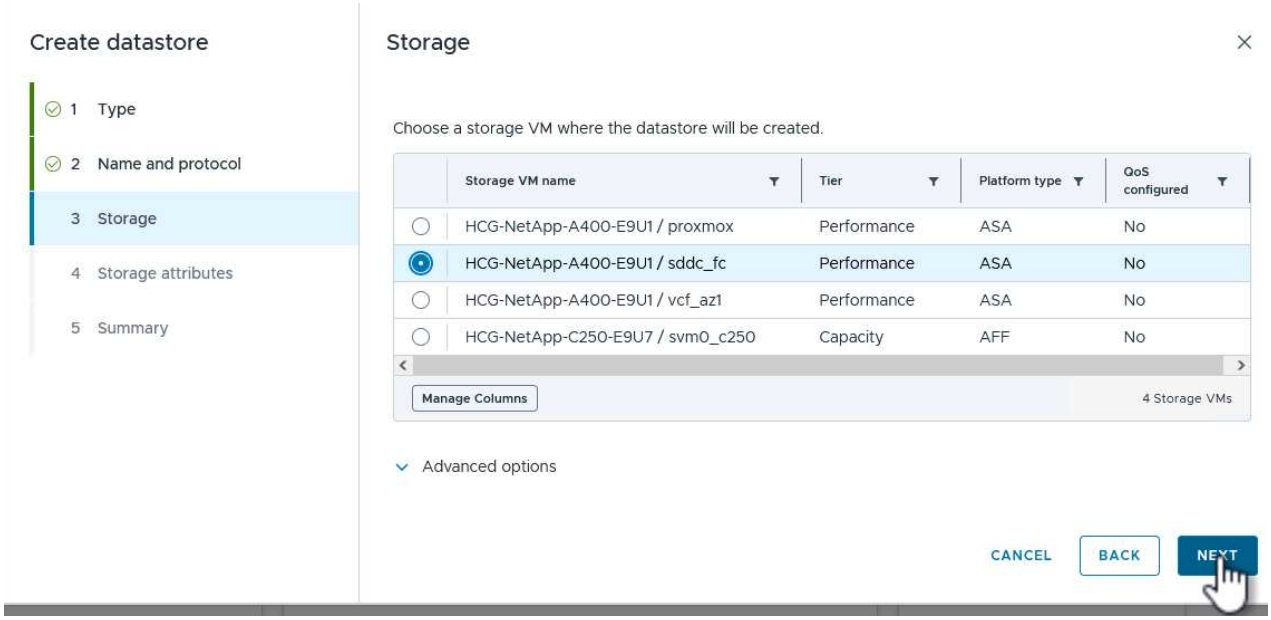
3. Nella procedura guidata **Crea datastore**, seleziona VMFS come tipo di datastore da creare.



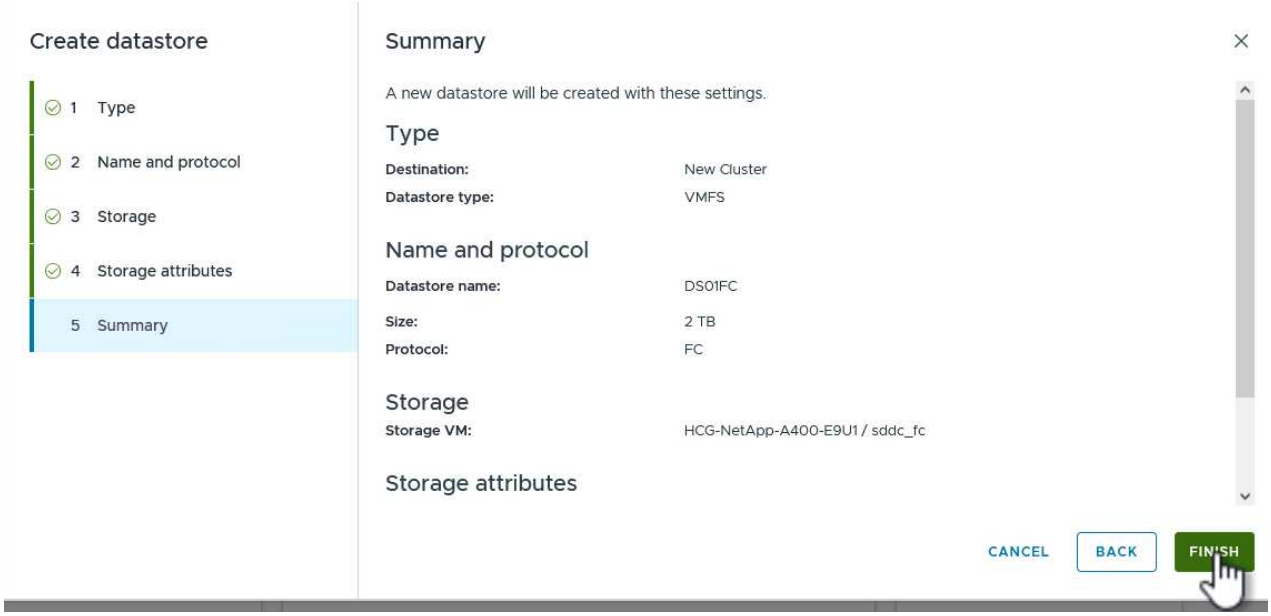
4. Nella pagina **Nome e protocollo**, inserisci un nome per il datastore, la dimensione e il protocollo FC da utilizzare.



5. Nella pagina **Archiviazione**, selezionare la piattaforma di archiviazione ONTAP e la macchina virtuale di archiviazione (SVM). Qui puoi anche selezionare qualsiasi criterio di esportazione personalizzato disponibile. Fare clic su **Avanti** per continuare.



6. Nella pagina **Attributi di archiviazione** selezionare l'aggregato di archiviazione da utilizzare. Fare clic su **Avanti** per continuare.
7. Nella pagina **Riepilogo**, rivedere le informazioni e fare clic su **Fine** per avviare il processo di provisioning. Gli strumenti ONTAP creeranno un volume sul sistema di archiviazione ONTAP e lo monteranno come datastore FC su tutti gli host ESXi nel cluster.



Convertire l'ambiente vSphere in VCF 5.2

Nella sezione seguente vengono illustrati i passaggi per distribuire il gestore SDDC e convertire il cluster vSphere 8 in un dominio di gestione VCF 5.2. Se del caso, per ulteriori dettagli si farà riferimento alla documentazione VMware.

VCF Import Tool, di VMware by Broadcom, è un'utilità utilizzata sia sull'appliance vCenter che sul gestore

SDDC per convalidare le configurazioni e fornire servizi di conversione e importazione per gli ambienti vSphere e VCF.

Per ulteriori informazioni, consulta "Opzioni e parametri dello strumento di importazione VCF" .

Copia ed estrai lo strumento di importazione VCF

Gli strumenti di importazione VCF vengono utilizzati sull'appliance vCenter per verificare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

1. Segui i passaggi a "Copia lo strumento di importazione VCF nell'appliance vCenter di destinazione" in VMware Docs per copiare lo strumento di importazione VCF nella posizione corretta.
2. Estrarre il bundle utilizzando il seguente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Convalida l'appliance vCenter

Utilizzare lo strumento di importazione VCF per convalidare l'appliance vCenter prima della conversione.

1. Segui i passaggi a "Eseguire un pre-controllo sul vCenter di destinazione prima della conversione" per eseguire la convalida.
2. L'output seguente mostra che l'appliance vCenter ha superato il pre-controllo.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Distribuire SDDC Manager

Il gestore SDDC deve essere collocato sul cluster vSphere che verrà convertito in un dominio di gestione VCF.

Per completare la distribuzione, seguire le istruzioni di distribuzione in VMware Docs.

Fare riferimento a "Distribuire l'appliance SDDC Manager sul vCenter di destinazione" .

Per maggiori informazioni vedere"Host della Commissione" nella Guida all'amministrazione VCF.

Creare un file JSON per la distribuzione NSX

Per distribuire NSX Manager durante l'importazione o la conversione di un ambiente vSphere in VMware Cloud Foundation, creare una specifica di distribuzione NSX. Per la distribuzione di NSX sono necessari almeno 3 host.

Per informazioni complete, fare riferimento a "Generare una specifica di distribuzione NSX per la conversione o l'importazione di ambienti vSphere esistenti" .

> Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzata la rete NSX-VLAN. Per informazioni dettagliate sulle limitazioni della rete NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Di seguito è riportato un esempio di file JSON per la distribuzione NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "************************",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copiare il file JSON in una directory su SDDC Manager.

Carica il software su SDDC Manager

Copiare lo strumento di importazione VCF e il bundle di distribuzione NSX nella directory /home/vcf/vcfimport su SDDC Manager.

Vedere "Caricare il software richiesto sull'appliance SDDC Manager" per istruzioni dettagliate.

Convertire il cluster vSphere in dominio di gestione VCF

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF. Eseguire il seguente comando dalla directory /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset per visualizzare una stampa delle funzioni dello strumento di importazione VCF:

```
python3 vcf_brownfield.py --help
```

Per convertire il cluster vSphere in un dominio di gestione VCF e distribuire il cluster NSX, eseguire il comando seguente:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Per istruzioni complete, fare riferimento a "Convertire o importare l'ambiente vSphere nell'inventario di SDDC Manager" .

Aggiungere la licenza al VCF

Dopo aver completato la conversione, è necessario aggiungere la licenza all'ambiente.

1. Accedi all'interfaccia utente di SDDC Manager.
2. Nel riquadro di navigazione, vai su **Amministrazione > Licenze**.
3. Fare clic su **+ Chiave di licenza**.
4. Scegli un prodotto dal menu a discesa.
5. Inserisci la chiave di licenza.
6. Fornire una descrizione della licenza.
7. Fare clic su **Aggiungi**.
8. Ripetere questi passaggi per ogni licenza.

Demo video per gli ONTAP tools for VMware vSphere 10

Datastore NFS con ONTAP tools for VMware vSphere 10

Fornire VCF con storage principale

Fornire un ambiente VCF con ONTAP come soluzione di archiviazione principale

Lo storage NetApp ONTAP è una soluzione di storage primaria ideale per la gestione di VMware Cloud Foundation (VCF) e per i domini di carico di lavoro di Virtual Infrastructure (VI). ONTAP offre elevate prestazioni, scalabilità, gestione avanzata dei dati e integrazione perfetta per migliorare l'efficienza operativa e la protezione dei dati.

Per i dettagli tecnici sul provisioning di un ambiente VCF nel dominio appropriato e con il protocollo appropriato, fare riferimento alle seguenti soluzioni.

- "Dominio di gestione con FC"
- "Dominio di gestione con NFS"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con FC"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con NFS"

Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per il dominio di gestione VCF

In questo caso d'uso descriviamo la procedura per utilizzare un datastore VMFS basato su FC esistente su ONTAP come storage primario per i domini di gestione VMware Cloud Foundation (VCF). Questa procedura riassume i componenti, le configurazioni e i passaggi di distribuzione richiesti.

Introduzione

Se opportuno, faremo riferimento alla documentazione esterna per i passaggi che devono essere eseguiti in SDDC Manager di VCF e faremo riferimento ai passaggi specifici della parte di configurazione dell'archiviazione.

Per informazioni sulla conversione di un ambiente vSphere basato su FC esistente con ONTAP, fare riferimento a"Convertire vSphere Environment (datastore FC) in VCF Management Domain" .

> La versione 5.2 di VCF ha introdotto la possibilità di convertire un ambiente vSphere 8 esistente in un dominio di gestione VCF o di importarlo come domini di carico di lavoro VCF VI. Prima di questa versione, VMware vSAN era l'unica opzione per l'archiviazione principale per il dominio di gestione VCF.

> Questa soluzione è applicabile alle piattaforme ONTAP che supportano l'archiviazione FC, tra cui NetApp ASA, AFF e FAS.

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

- Sistema di storage NetApp con una macchina virtuale di storage (SVM) configurata per consentire il traffico FC.

- Sono state create interfacce logiche (LIF) sulla struttura FC che deve trasportare il traffico FC ed è associata alla SVM.
- La suddivisione in zone è stata configurata per utilizzare la suddivisione in zone con singolo iniziatore-destinazione sugli switch FC per HBA host e destinazioni di archiviazione.

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" .

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

L'archiviazione principale FC sul cluster iniziale è supportata solo con lo strumento di importazione brownfield VCF. Se VCF viene distribuito con lo strumento Cloud Builder (prima della versione 5.2.x), è supportato solo vSAN.

Per ulteriori informazioni sull'utilizzo di un ambiente vSphere esistente, fare riferimento a "conversione dell'ambiente vSphere esistente in dominio di gestione" per maggiori informazioni.

Dominio di gestione - Cluster aggiuntivo

Il cluster vSphere aggiuntivo sul dominio di gestione può essere distribuito con le seguenti opzioni:

- Avere un cluster aggiuntivo nell'ambiente vSphere e utilizzare lo strumento di importazione brownfield VCF per convertire l'ambiente vSphere nel dominio di gestione. "ONTAP tools for VMware vSphere" "Gestore di sistema o API ONTAP" può essere utilizzato per distribuire il datastore VMFS nel cluster vSphere.
- Utilizzare l'API SDDC per distribuire cluster aggiuntivi. Gli host vSphere devono avere configurato il datastore VMFS. Utilizzo "Gestore di sistema o API ONTAP" per distribuire LUN sugli host vSphere.
- Utilizzare l'interfaccia utente di SDDC Manager per distribuire cluster aggiuntivi. Tuttavia, questa opzione crea solo datastore VSAN fino alla versione 5.2.x.

Informazioni aggiuntive

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" .

Utilizzare un datastore NFS su ONTAP come storage principale per il dominio di gestione VCF

In questo caso d'uso descriviamo la procedura per utilizzare un datastore NFS esistente su ONTAP come storage primario per i domini di gestione VMware Cloud Foundation (VCF). Questa procedura riassume i componenti richiesti, i passaggi di configurazione e il processo di distribuzione.

Introduzione

Se opportuno, faremo riferimento alla documentazione esterna per i passaggi che devono essere eseguiti in SDDC Manager di VCF e faremo riferimento ai passaggi specifici della parte di configurazione dell'archiviazione.

Per informazioni sulla conversione di un ambiente vSphere basato su NFS esistente con ONTAP, fare riferimento a"Convertire vSphere Environment (datastore NFS) in VCF Management Domain" .

> La versione 5.2 di VCF ha introdotto la possibilità di convertire un ambiente vSphere 8 esistente in un dominio di gestione VCF o di importarlo come domini di carico di lavoro VCF VI. Prima di questa versione, VMware vSAN era l'unica opzione per l'archiviazione principale per il dominio di gestione VCF.

> Questa soluzione è applicabile alle piattaforme ONTAP che supportano l'archiviazione NFS, inclusi NetApp AFF e FAS.

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

- Sistema di archiviazione NetApp con una macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi e un'appliance vCenter collocata sul cluster.
- Gruppo di porte distribuito configurato per il traffico di archiviazione vMotion e NFS sulle VLAN o sui segmenti di rete stabiliti a tale scopo.
- Scarica il software necessario per la conversione VCF.

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" .

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

L'archiviazione principale NFS sul cluster iniziale è supportata solo con lo strumento di importazione brownfield VCF. Se VCF viene distribuito con lo strumento Cloud Builder (fino alla versione 5.2.x), è supportato solo VSAN.

Per ulteriori informazioni sull'utilizzo di un ambiente vSphere esistente, fare riferimento a "conversione dell'ambiente vSphere esistente in dominio di gestione" per maggiori informazioni.

Dominio di gestione - Cluster aggiuntivo

Il cluster vSphere aggiuntivo sul dominio di gestione può essere distribuito con le seguenti opzioni:

- Avere un cluster aggiuntivo nell'ambiente vSphere e utilizzare lo strumento di importazione brownfield VCF

per convertire l'ambiente vSphere nel dominio di gestione. "ONTAP tools for VMware vSphere" "Gestore di sistema o API ONTAP" può essere utilizzato per distribuire il datastore NFS nel cluster vSphere.

- Utilizzare l'API SDDC per distribuire cluster aggiuntivi. Gli host vSphere devono avere configurato il datastore NFS. Utilizzo "Gestore di sistema o API ONTAP" per distribuire LUN sugli host vSphere.
- Utilizzare l'interfaccia utente di SDDC Manager per distribuire cluster aggiuntivi. Questa opzione, tuttavia, crea solo datastore vSAN con versioni precedenti alla 5.2.x.

Informazioni aggiuntive

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" .

Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per un dominio di carico di lavoro VI

In questo caso d'uso descriviamo la procedura per configurare un datastore VMFS Fibre Channel (FC) su ONTAP come soluzione di storage primaria per un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Questa procedura riassume i componenti richiesti, i passaggi di configurazione e il processo di distribuzione.

Vantaggi del Fibre Channel

Prestazioni elevate: FC garantisce velocità di trasferimento dati elevate, rendendolo ideale per applicazioni che richiedono un accesso rapido e affidabile a grandi quantità di dati.

Bassa latenza: Latenza molto bassa, fondamentale per le applicazioni che richiedono prestazioni elevate, come database e ambienti virtualizzati.

Affidabilità: le reti FC sono note per la loro robustezza e affidabilità, con funzionalità quali ridondanza integrata e correzione degli errori.

Larghezza di banda dedicata: FC fornisce larghezza di banda dedicata per il traffico di archiviazione, riducendo il rischio di congestione della rete.

Per ulteriori informazioni sull'utilizzo di Fibre Channel con i sistemi di storage NetApp , fare riferimento a "Provisioning SAN con FC" .

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Creare una macchina virtuale di archiviazione (SVM) con interfacce logiche (LIF) per il traffico FC.
- Raccogliere le informazioni WWPN degli host da distribuire e creare i gruppi di iniziatori corrispondenti sul sistema di archiviazione ONTAP .
- Creare un volume FC sul sistema di archiviazione ONTAP .
- Mappare i gruppi di iniziatori per creare il volume FC

- Utilizzare la suddivisione in zone con singolo iniziatore-target sugli switch FC. Creare una zona per ogni iniziatore (zona iniziatore singolo).
  - Per ogni zona, includere un target che sia l'interfaccia logica ONTAP FC (WWPN) per gli SVM. Dovrebbero esserci almeno due interfacce logiche per nodo per SVM. Non utilizzare il WWPN delle porte fisiche.
- Creare un pool di rete per il traffico vMotion in SDDC Manager.
- Host della Commissione in VCF per l'utilizzo in un dominio di carico di lavoro VI.
- Distribuisci un dominio di carico di lavoro VI in VCF utilizzando un datastore FC come storage principale.

> Questa soluzione è applicabile alle piattaforme ONTAP che supportano l'archiviazione NFS, inclusi NetApp AFF e FAS.

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o ASA con porte FC collegate a switch FC.
- SVM creato con FC lifs.
- vSphere con HBA FC collegati agli switch FC.
- Sugli switch FC è configurata la suddivisione in zone con singolo iniziatore-destinazione.

> NetApp consiglia il multipath per le LUN FC.

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

L'archiviazione principale FC sul cluster iniziale è supportata solo con lo strumento di importazione brownfield VCF. Se VCF viene distribuito con lo strumento CloudBuilder (fino alla versione 5.2.x), è supportato solo VSAN. Fare riferimento "conversione dell'ambiente vSphere esistente in dominio di gestione" per maggiori informazioni.

Dominio di gestione - Cluster aggiuntivo

Il cluster vSphere aggiuntivo sul dominio di gestione può essere distribuito con le seguenti opzioni: * Avere un cluster aggiuntivo nell'ambiente vSphere e utilizzare lo strumento di importazione brownfield VCF per convertire l'ambiente vSphere nel dominio di gestione. "ONTAP tools for VMware vSphere" , "Gestore di sistema o API ONTAP" può essere utilizzato per distribuire il datastore VMFS nel cluster vSphere. * Utilizzare l'API SDDC per distribuire cluster aggiuntivi. Gli host vSphere devono avere configurato il datastore VMFS. Utilizzo "Gestore di sistema o API ONTAP" per distribuire LUN sugli host vSphere. * Utilizzare l'interfaccia utente di SDDC Manager per distribuire cluster aggiuntivi. Tuttavia, questa opzione crea solo datastore VSAN fino alla versione 5.2.x.

Dominio del carico di lavoro VI - Cluster predefinito

Dopo che il dominio di gestione è attivo e funzionante, è possibile creare il dominio del carico di lavoro VI:

- Utilizzo dell'interfaccia utente di SDDC Manager. Gli host vSphere devono avere configurato il datastore VMFS. Utilizzare System Manager o l'API ONTAP per distribuire LUN sugli host vSphere.
- Importa un ambiente vSphere esistente come nuovo dominio del carico di lavoro VI. Per distribuire il

datastore VMFS nel cluster vSphere è possibile utilizzare gli ONTAP tools for VMware vSphere, System Manager o ONTAP API.

Dominio del carico di lavoro VI - Cluster aggiuntivo

Una volta che il carico di lavoro VI è attivo e funzionante, è possibile distribuire cluster aggiuntivi con VMFS su FC LUN utilizzando le seguenti opzioni.

- Cluster aggiuntivi nell'ambiente vSphere importati tramite lo strumento di importazione brownfield VCF. Per distribuire il datastore VMFS nel cluster vSphere è possibile utilizzare gli ONTAP tools for VMware vSphere, System Manager o ONTAP API.
- Utilizzo dell'interfaccia utente o dell'API di SDDC Manager per distribuire cluster aggiuntivi. Gli host vSphere devono avere configurato il datastore VMFS. Utilizzare System Manager o l'API ONTAP per distribuire LUN sugli host vSphere.

Informazioni aggiuntive

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" .

Utilizzare un datastore NFS su ONTAP come storage principale per un dominio di carico di lavoro VI

In questo caso d'uso descriviamo la procedura per configurare un datastore NFS su ONTAP come soluzione di storage primaria per un dominio di carico di lavoro di un'infrastruttura virtuale (VI) VMware Cloud Foundation (VCF). Questa procedura riassume i componenti richiesti, i passaggi di configurazione e il processo di distribuzione.

Vantaggi di NFS

Semplicità e facilità d'uso: NFS è semplice da configurare e gestire, il che lo rende una scelta eccellente per gli ambienti che richiedono una condivisione dei file rapida e semplice.

Scalabilità: l'architettura di ONTAP consente a NFS di scalare in modo efficiente, supportando le crescenti esigenze di dati senza modifiche significative all'infrastruttura.

Flessibilità: NFS supporta un'ampia gamma di applicazioni e carichi di lavoro, rendendolo versatile per vari casi d'uso, inclusi gli ambienti virtualizzati.

Per ulteriori informazioni, fare riferimento alla Guida di riferimento NFS v3 per vSphere 8.

Per ulteriori informazioni sull'utilizzo di Fibre Channel con i sistemi di storage NetApp , fare riferimento a"Guida di riferimento NFS v3 per vSphere 8" .

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Creare una macchina virtuale di archiviazione (SVM) con interfaccia logica (LIF) per NFS straffic

- Verificare la rete per la macchina virtuale di archiviazione ONTAP (SVM) e che sia presente un'interfaccia logica (LIF) per trasportare il traffico NFS.
- Creare una policy di esportazione per consentire agli host ESXi di accedere al volume NFS.
- Creare un volume NFS sul sistema di archiviazione ONTAP .
- Creare un pool di rete per il traffico NFS e vMotion in SDDC Manager.
- Host della Commissione in VCF per l'utilizzo in un dominio di carico di lavoro VI.
- Distribuisci un dominio di carico di lavoro VI in VCF utilizzando un datastore NFS come storage principale.
- Installa il plug-in NetApp NFS per VMware VAAI

> Questa soluzione è applicabile alle piattaforme ONTAP che supportano l'archiviazione NFS, inclusi NetApp AFF e FAS.

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

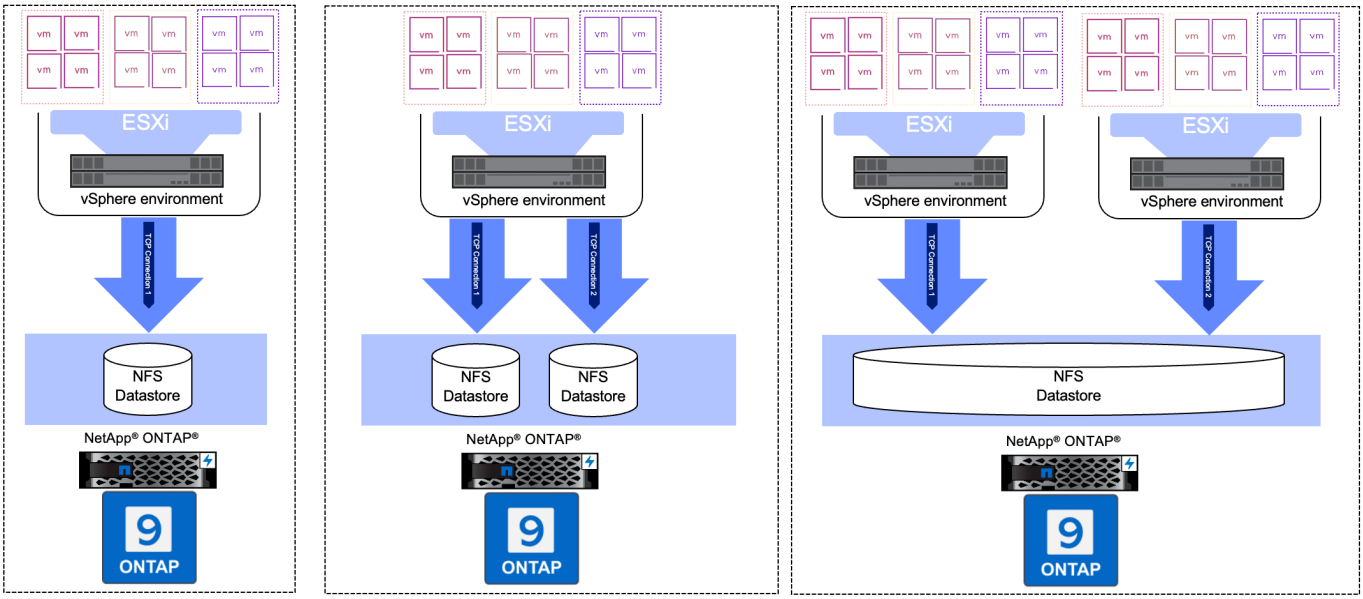
- Sistema di archiviazione NetApp AFF con una macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- La distribuzione del dominio di gestione VCF è completa e l'interfaccia di SDDC Manager è accessibile.
- 4 host ESXi configurati per la comunicazione sulla rete di gestione VCF.
- Indirizzi IP riservati per il traffico di archiviazione vMotion e NFS sulla VLAN o sul segmento di rete stabilito a tale scopo.

> Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario assicurarsi che 1) la rete di gestione sia instradabile verso il server NFS oppure 2) un LIF per la rete di gestione sia stato aggiunto all'SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

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" .

Per ulteriori informazioni sull'utilizzo di NFS con cluster vSphere, fare riferimento a"Guida di riferimento NFS v3 per vSphere 8" .



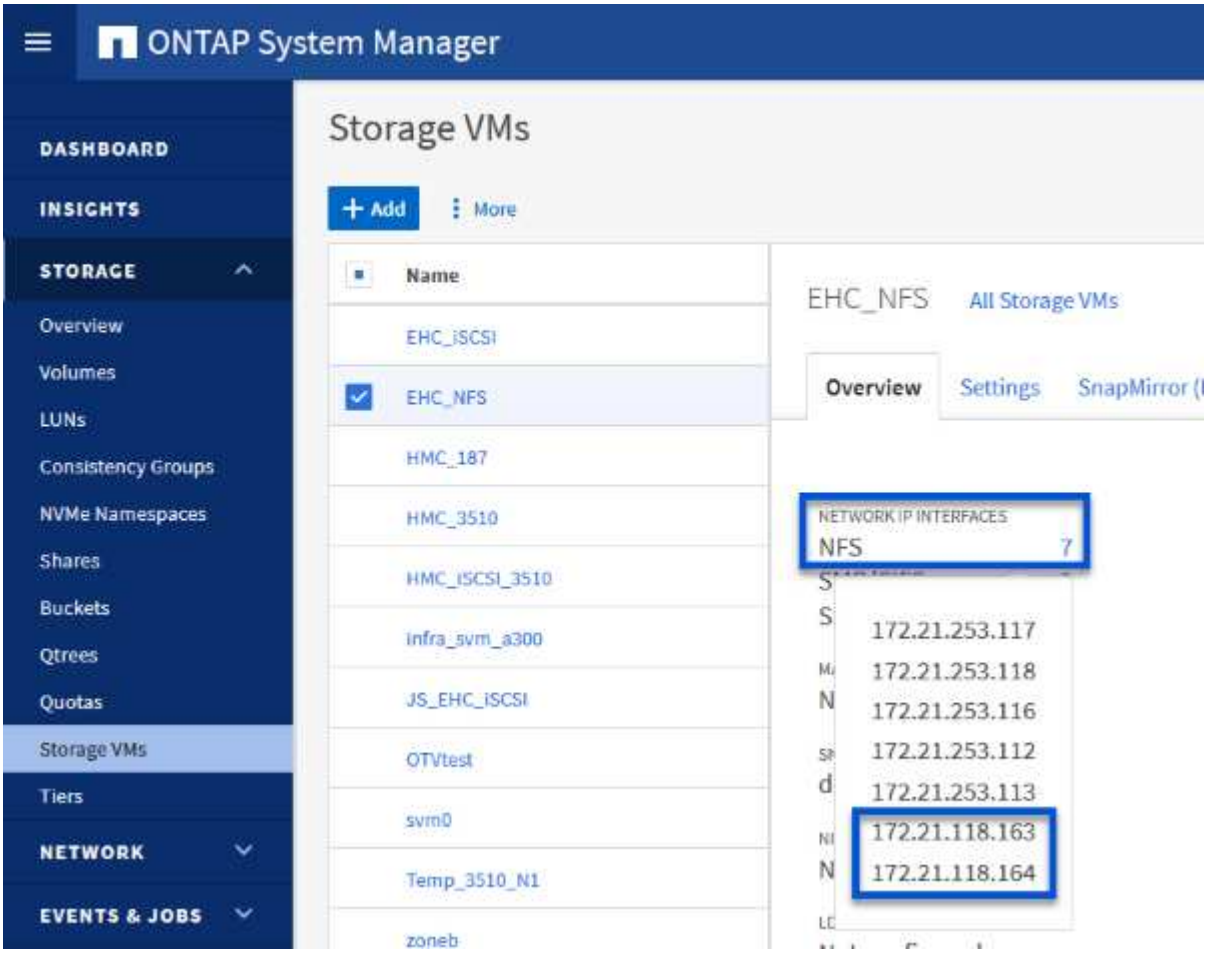
Fasi di distribuzione

Per distribuire un dominio di carico di lavoro VI con un datastore NFS come storage principale, completare i seguenti passaggi:

Verifica della rete per ONTAP SVM

Verificare che siano state stabilite le interfacce logiche richieste per la rete che trasporterà il traffico NFS tra il cluster di archiviazione ONTAP e il dominio del carico di lavoro VI.

1. Da ONTAP System Manager, accedere a **Storage VMs** nel menu a sinistra e fare clic sulla SVM da utilizzare per il traffico NFS. Nella scheda **Panoramica**, in **INTERFACCE IP DI RETE**, fare clic sul numero a destra di **NFS**. Nell'elenco verificare che siano elencati gli indirizzi IP LIF richiesti.



In alternativa, verificare i LIF associati a un SVM dalla CLI ONTAP con il seguente comando:

```
network interface show -vserver <SVM_NAME>
```

1. Verificare che gli host ESXi possano comunicare con il server NFS ONTAP . Accedi all'host ESXi tramite SSH ed esegui il ping dell'SVM LIF:

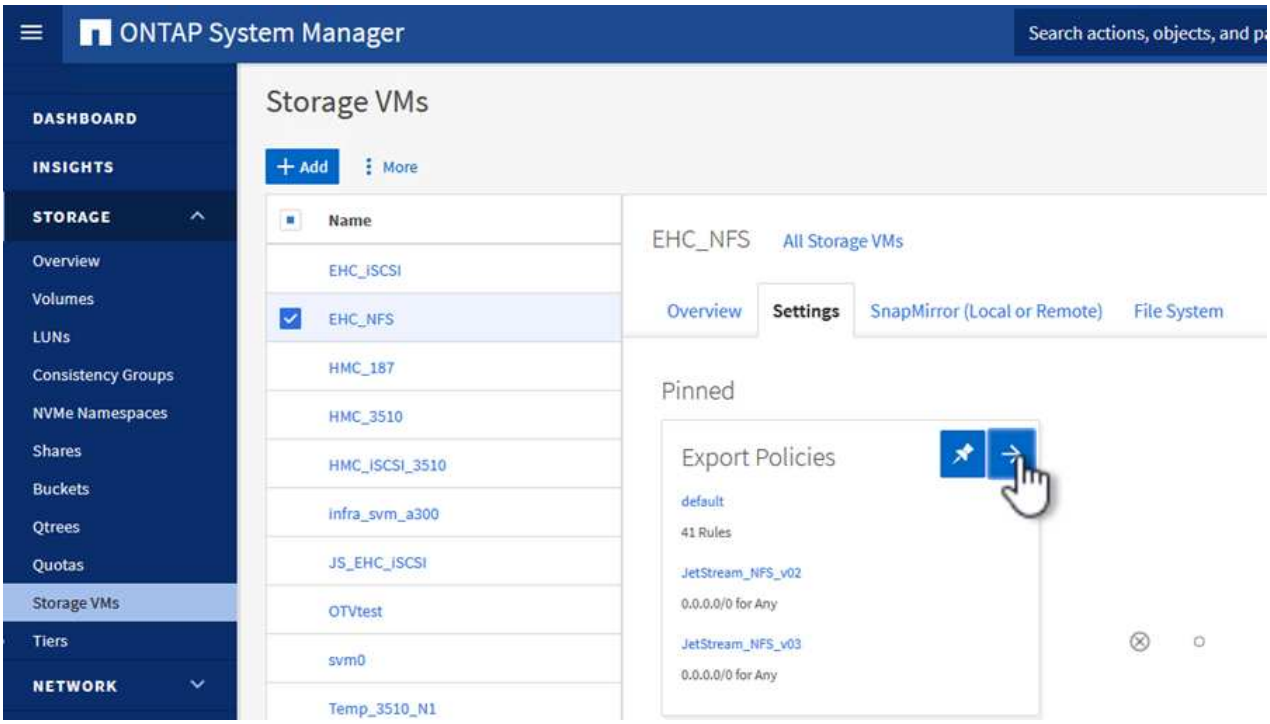
```
vmkping <IP Address>
```

Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario assicurarsi che 1) la rete di gestione sia instradabile verso il server NFS oppure 2) un LIF per la rete di gestione sia stato aggiunto all'SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

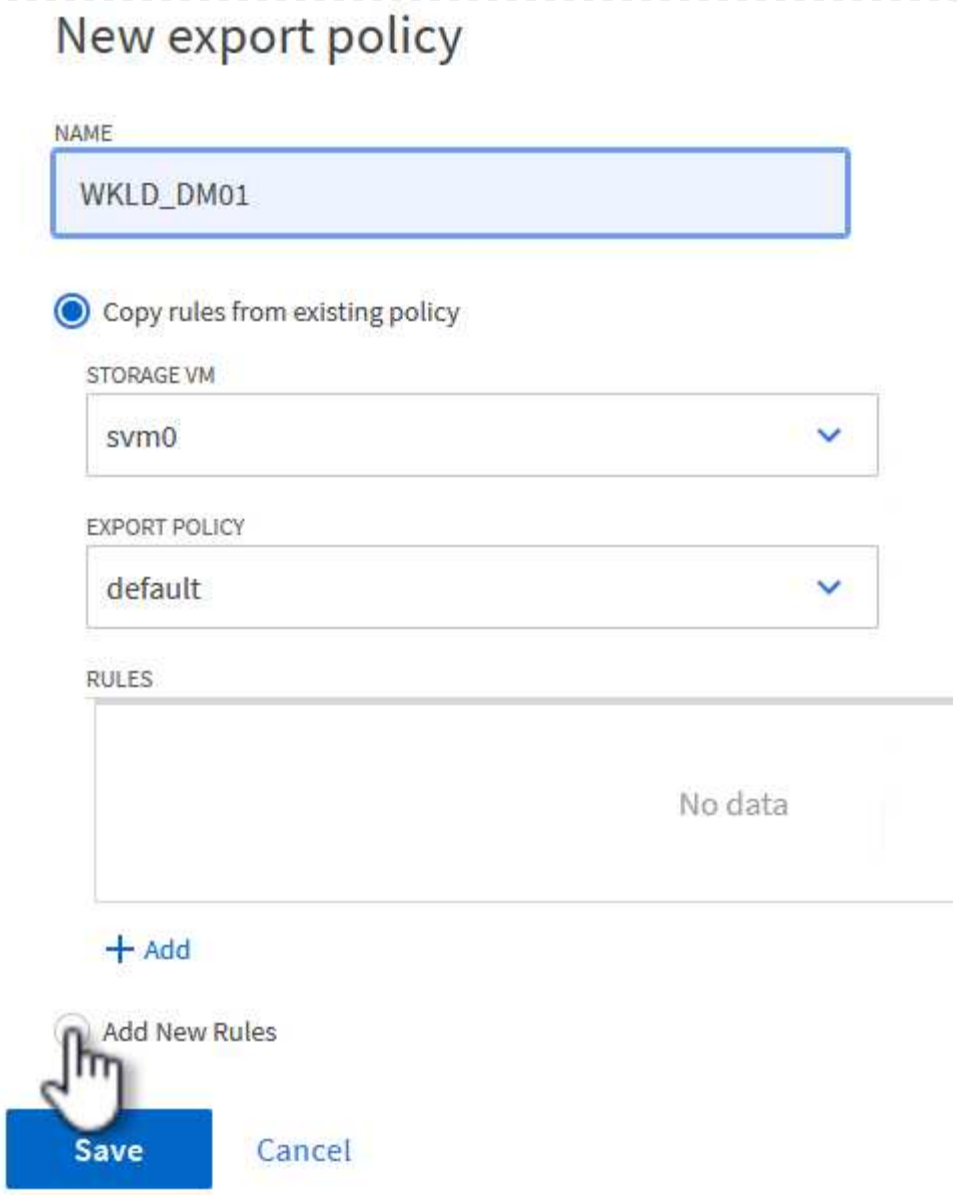
Crea criteri di esportazione per la condivisione del volume NFS

Creare una policy di esportazione in ONTAP System Manager per definire il controllo di accesso per i volumi NFS.

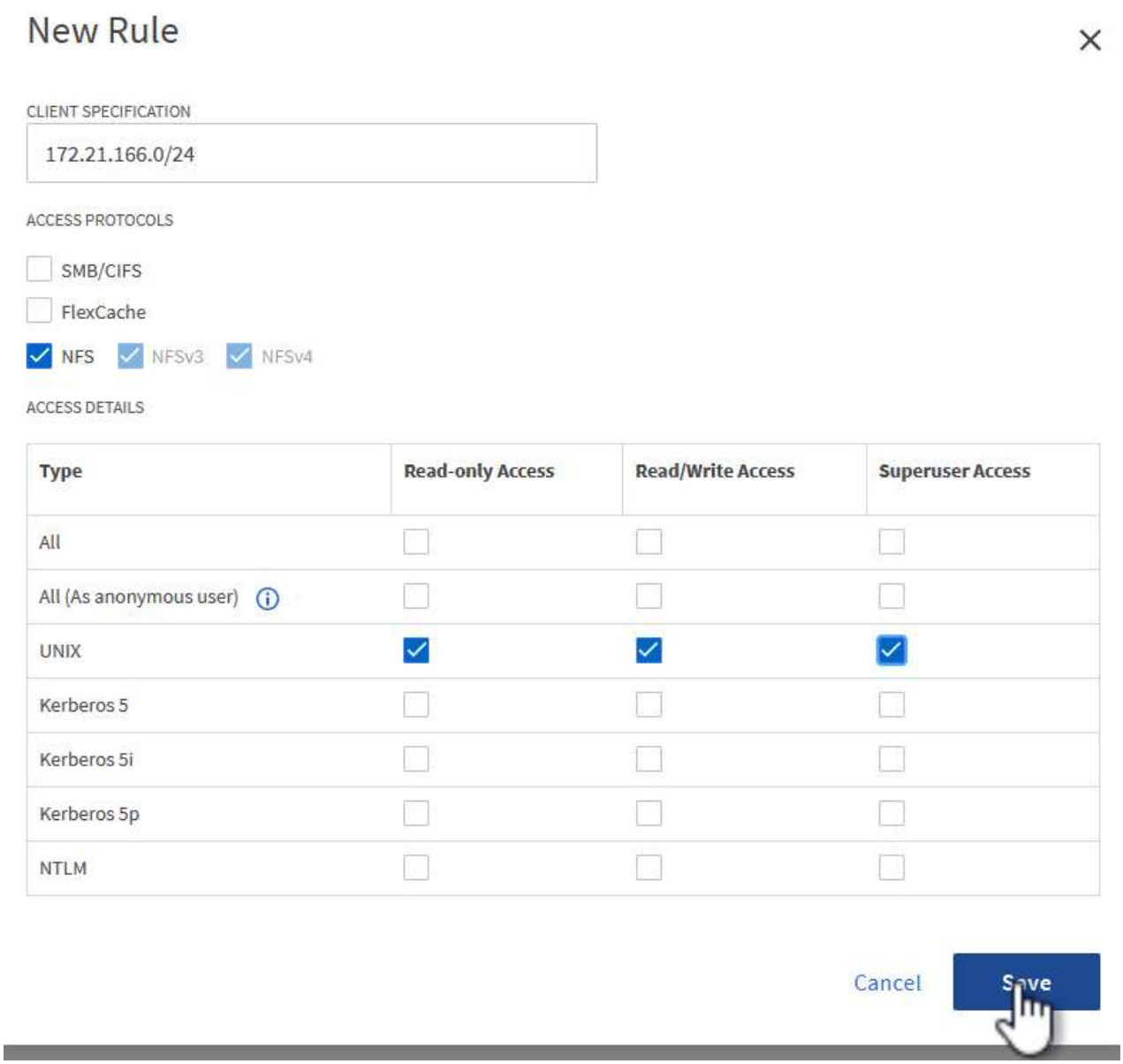
1. In ONTAP System Manager, fare clic su **Storage VMs** nel menu a sinistra e selezionare una SVM dall'elenco.
2. Nella scheda **Impostazioni** individua **Criteri di esportazione** e clicca sulla freccia per accedervi.



3. Nella finestra **Nuova policy di esportazione** aggiungere un nome per la policy, fare clic sul pulsante **Aggiungi nuove regole** e quindi sul pulsante **+Aggiungi** per iniziare ad aggiungere una nuova regola.



4. Inserisci gli indirizzi IP, l'intervallo di indirizzi IP o la rete che desideri includere nella regola. Deselezionare le caselle **SMB/Cifs** e * FlexCache* ed effettuare le selezioni per i dettagli di accesso di seguito. Per l'accesso all'host ESXi è sufficiente selezionare le caselle UNIX.



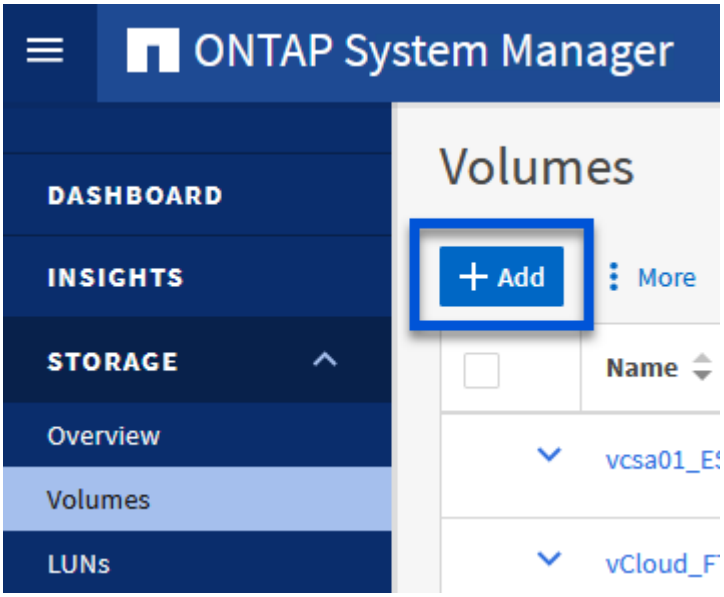
> Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario garantire che la politica di esportazione includa la rete di gestione VCF per consentire il proseguimento della convalida.

5. Una volta inserite tutte le regole, fare clic sul pulsante **Salva** per salvare la nuova politica di esportazione.
6. In alternativa, è possibile creare criteri e regole di esportazione nella CLI ONTAP . Fare riferimento ai passaggi per la creazione di una policy di esportazione e l'aggiunta di regole nella documentazione ONTAP .
   - Utilizzare ONTAP CLI per"Creare una politica di esportazione" .
   - Utilizzare ONTAP CLI per"Aggiungere una regola a un criterio di esportazione" .

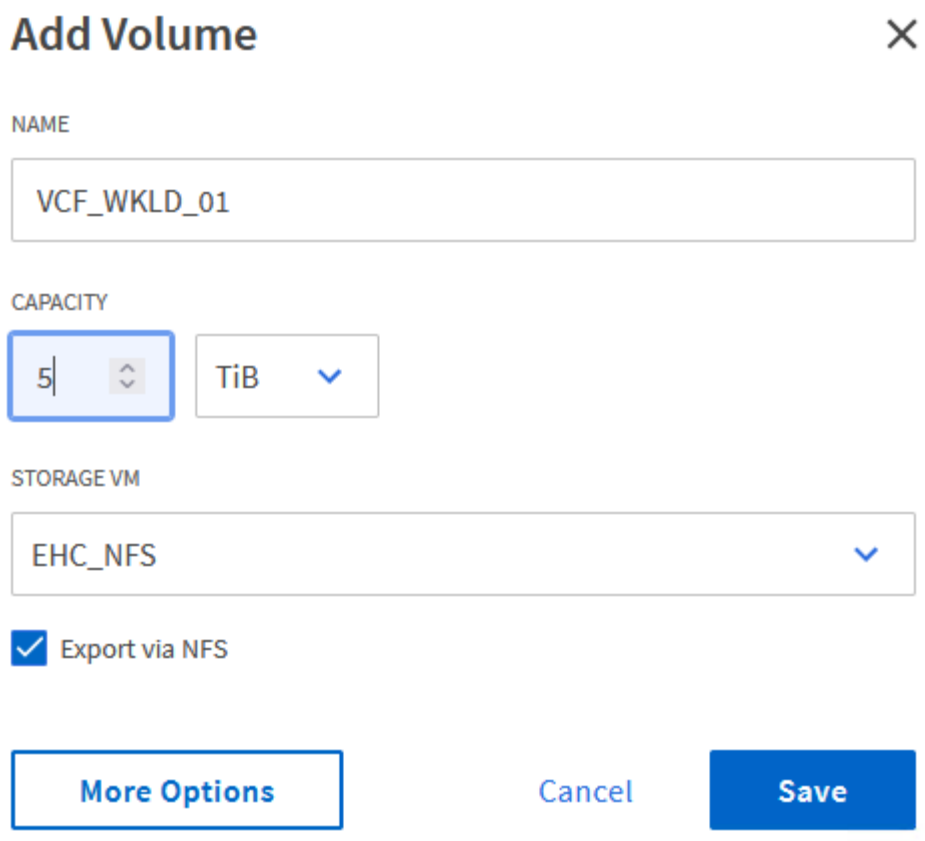
Crea volume NFS

Creare un volume NFS sul sistema di archiviazione ONTAP da utilizzare come datastore nella distribuzione del dominio del carico di lavoro.

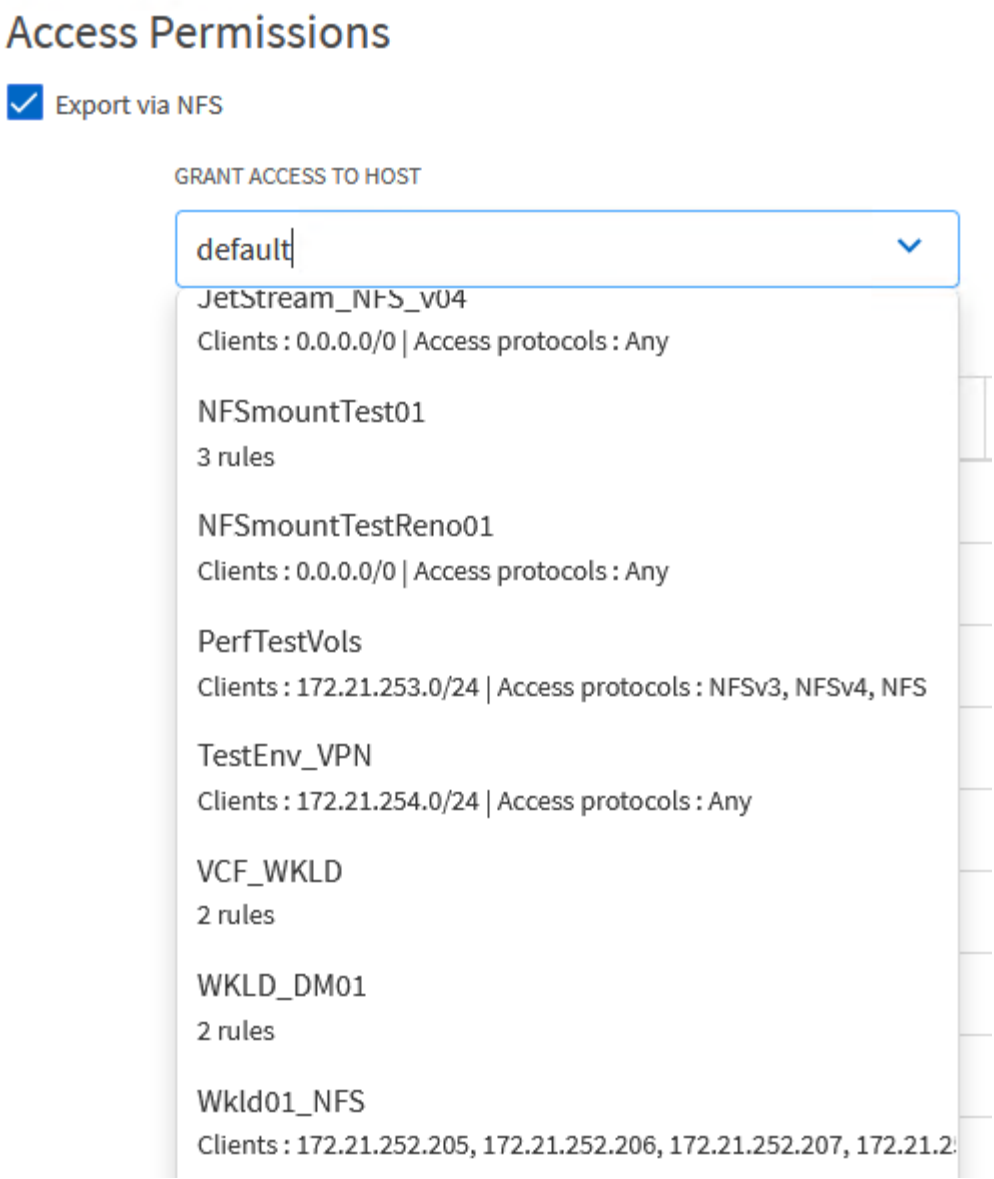
1. Da ONTAP System Manager, andare su **Archiviazione > Volumi** nel menu a sinistra e fare clic su **+Aggiungi** per creare un nuovo volume.



2. Aggiungere un nome per il volume, specificare la capacità desiderata e selezionare la VM di archiviazione che ospiterà il volume. Fare clic su **Altre opzioni** per continuare.



3. In Autorizzazioni di accesso, selezionare la Politica di esportazione che include la rete di gestione VCF o l'indirizzo IP e gli indirizzi IP della rete NFS che verranno utilizzati sia per la convalida del server NFS che per il traffico NFS.



+

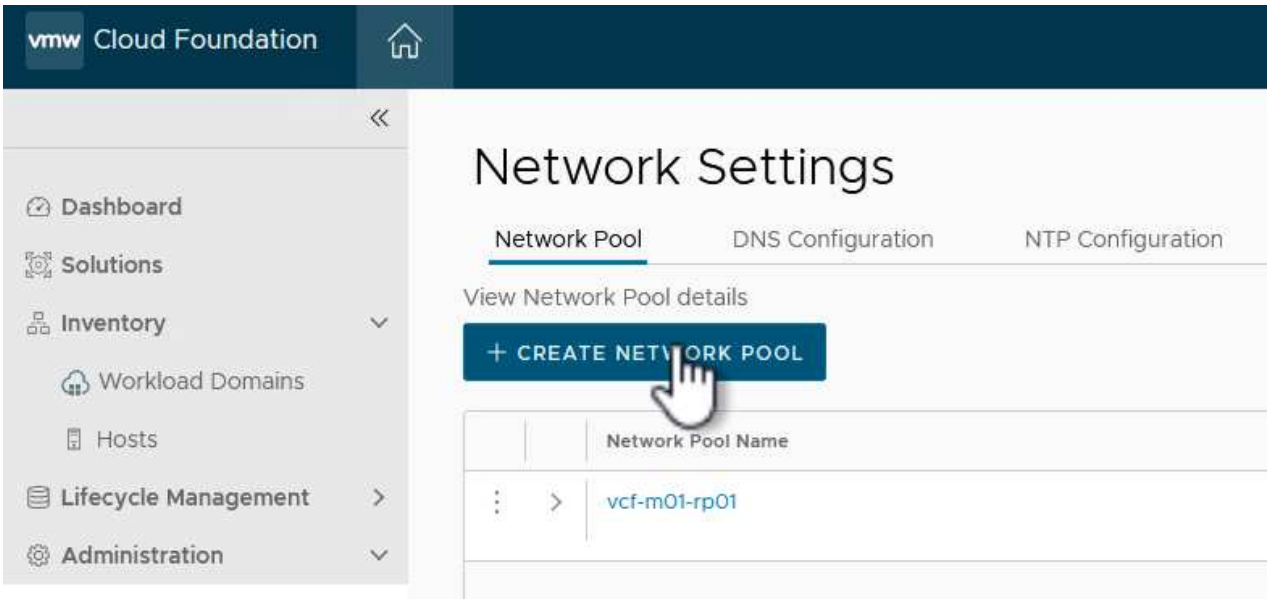
> Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario assicurarsi che 1) la rete di gestione sia instradabile verso il server NFS oppure 2) un LIF per la rete di gestione sia stato aggiunto all'SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

4. In alternativa, è possibile creare volumi ONTAP nella CLI ONTAP . Per maggiori informazioni fare riferimento al"lun crea" comando nella documentazione dei comandi ONTAP .

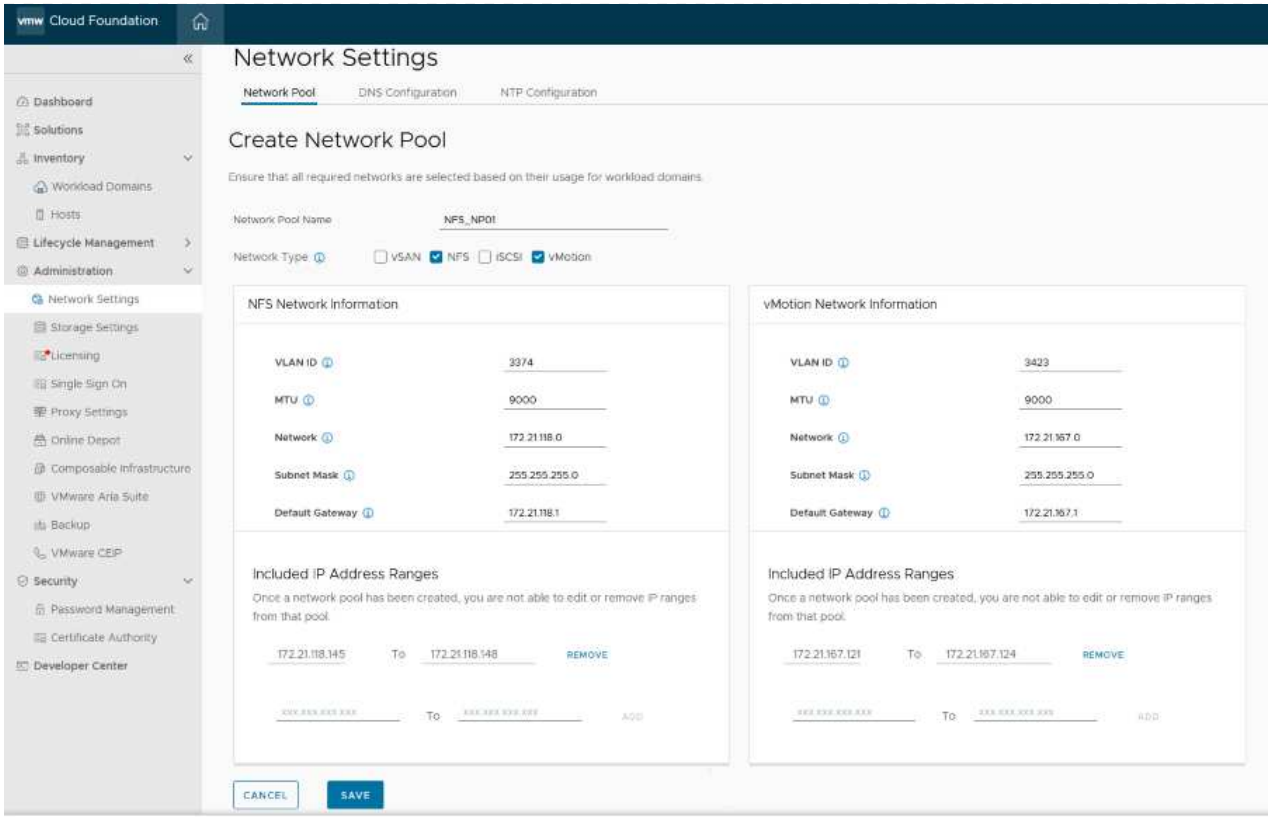
Crea pool di rete in SDDC Manager

È necessario creare un pool di rete in SDDC Manager prima di mettere in servizio gli host ESXi, come preparazione per la loro distribuzione in un dominio di carico di lavoro VI. Il pool di rete deve includere le informazioni di rete e gli intervalli di indirizzi IP per gli adattatori VMkernel da utilizzare per la comunicazione con il server NFS.

1. Dall'interfaccia web di SDDC Manager, accedere a **Impostazioni di rete** nel menu a sinistra e fare clic sul pulsante **+ Crea pool di rete**.



2. Inserire un nome per il pool di rete, selezionare la casella di controllo per NFS e compilare tutti i dettagli di rete. Ripetere questa operazione per le informazioni di rete vMotion.



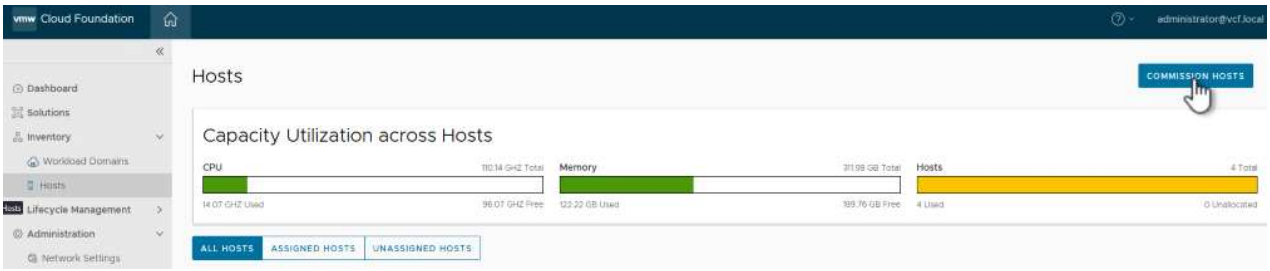
3. Fare clic sul pulsante **Salva** per completare la creazione del pool di rete.

Host della Commissione

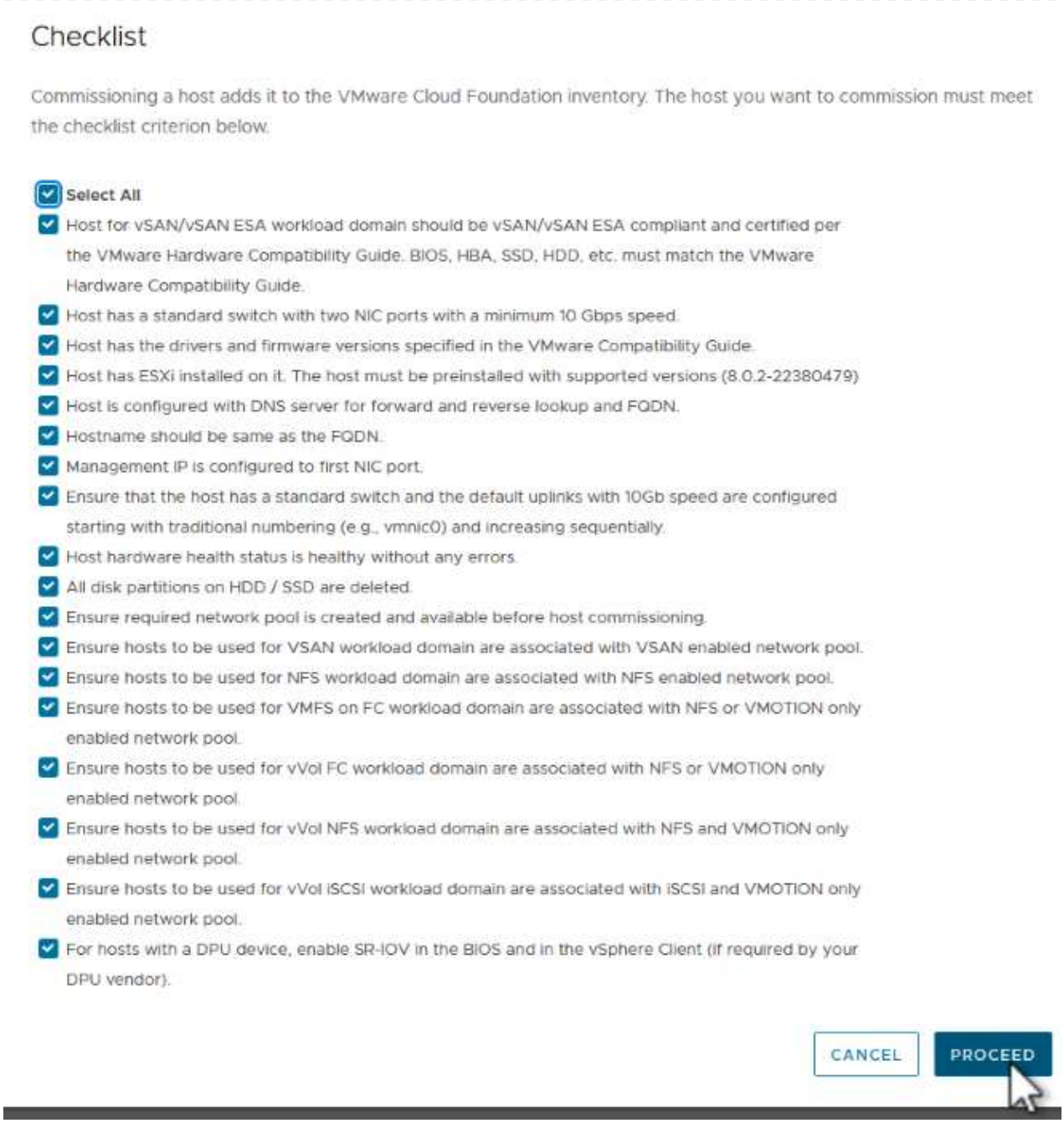
Prima che gli host ESXi possano essere distribuiti come dominio di carico di lavoro, devono essere aggiunti all'inventario di SDDC Manager. Ciò comporta la fornitura delle informazioni richieste, il superamento della convalida e l'avvio del processo di messa in servizio.

Per maggiori informazioni vedere"Host della Commissione" nella Guida all'amministrazione VCF.

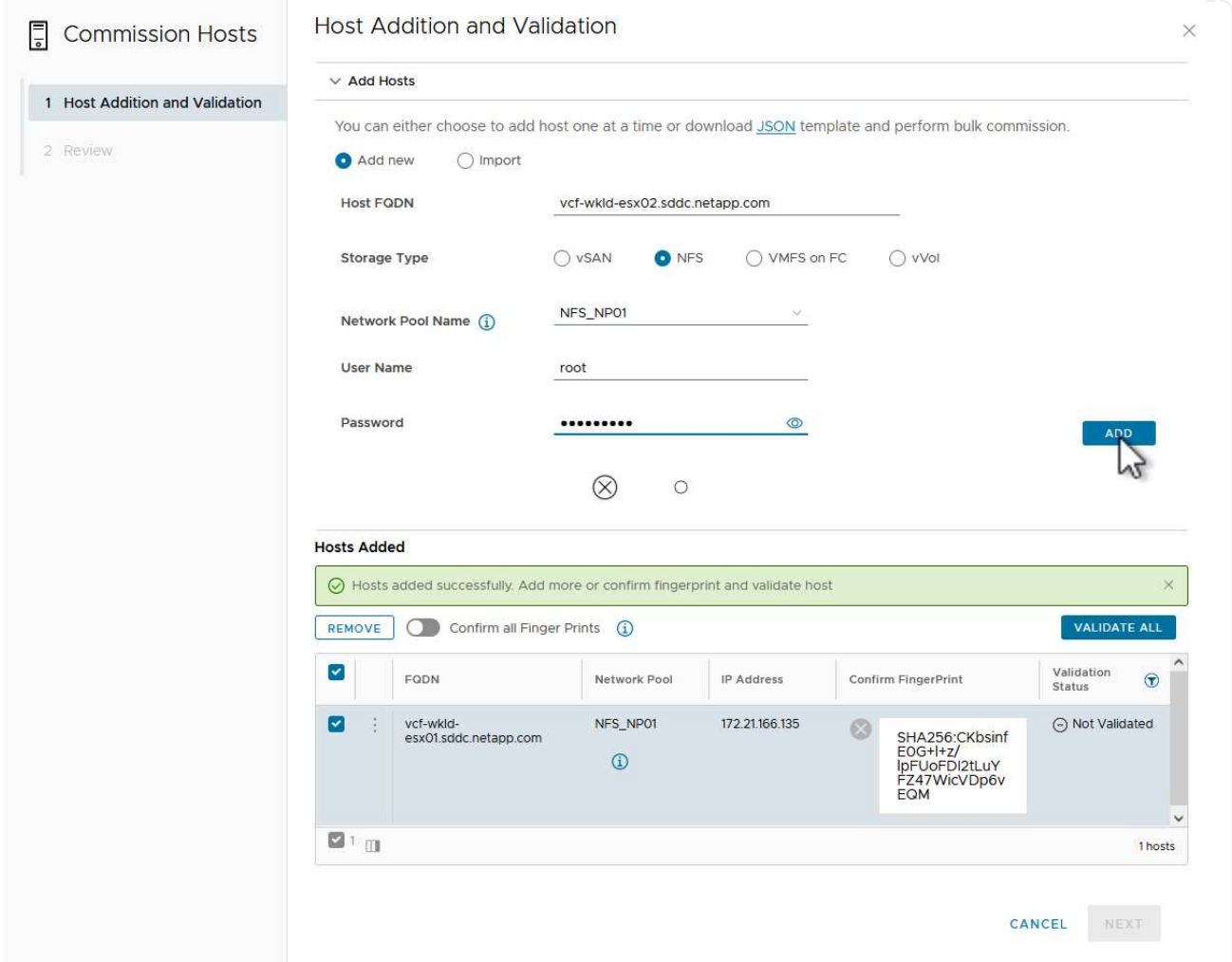
1. Dall'interfaccia di SDDC Manager, vai su **Host** nel menu a sinistra e clicca sul pulsante **Commission Hosts**.



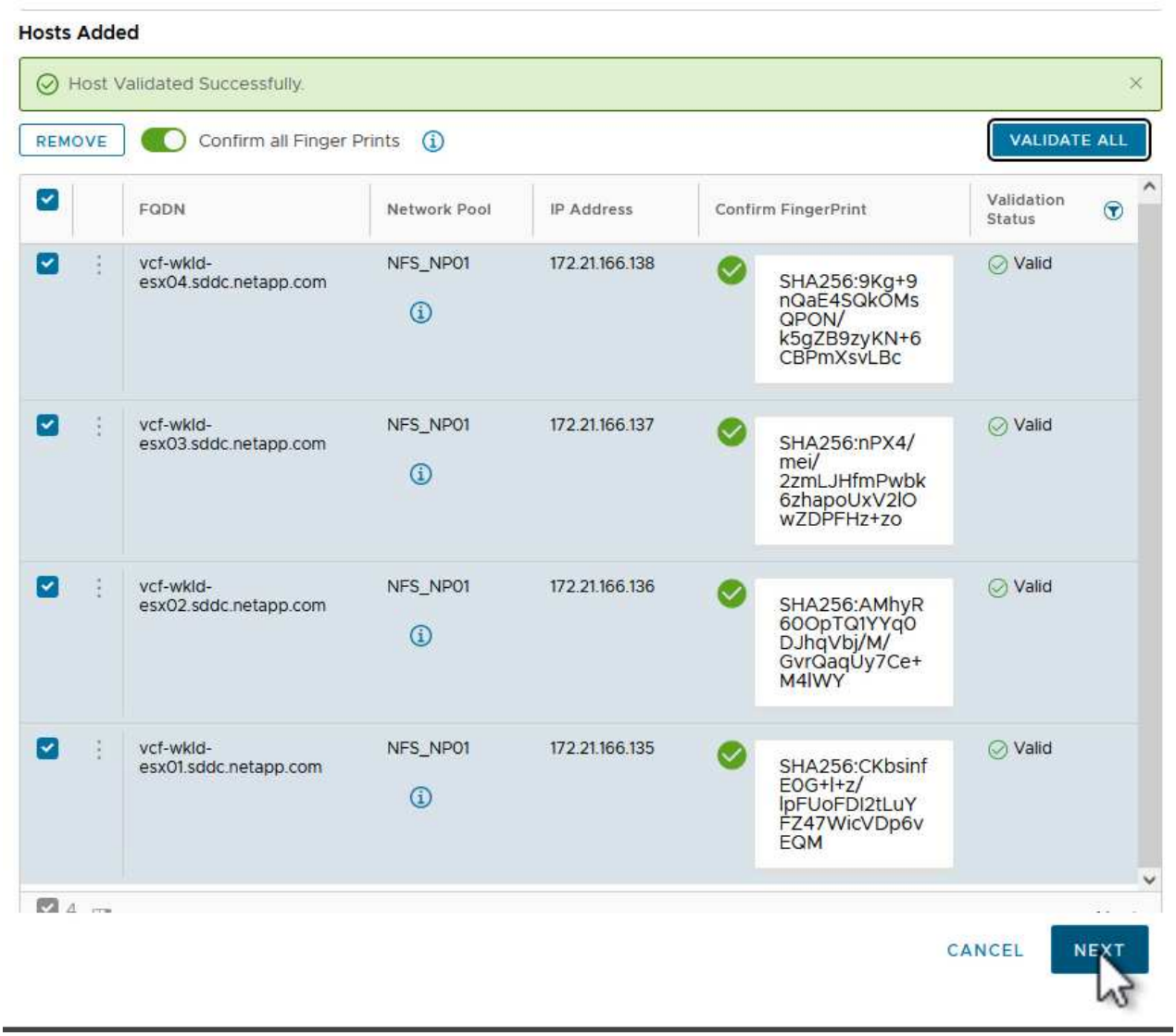
2. La prima pagina è una lista di controllo dei prerequisiti. Verificare nuovamente tutti i prerequisiti e selezionare tutte le caselle di controllo per procedere.



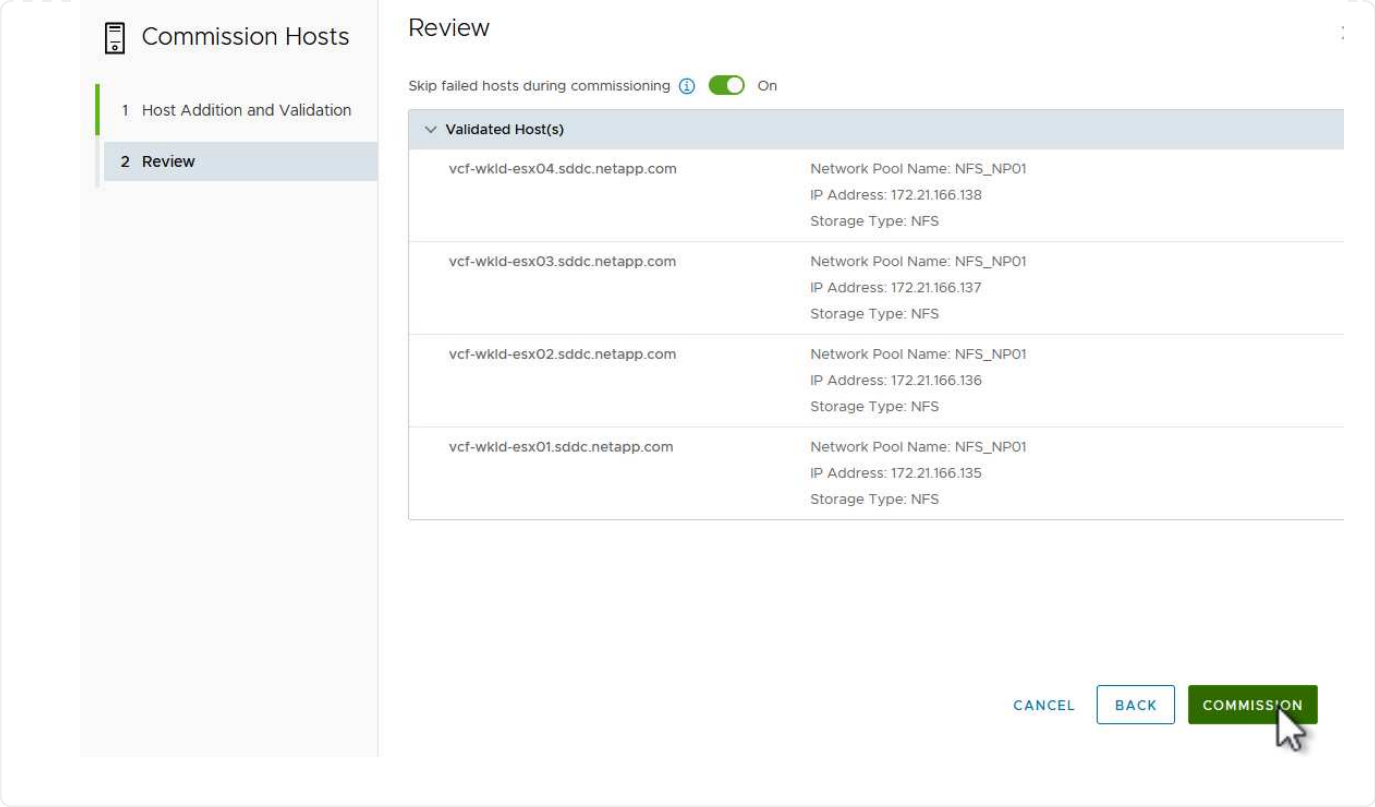
3. Nella finestra **Aggiunta e convalida host** compilare **FQDN host**, **Tipo di archiviazione**, il nome del **pool di rete** che include gli indirizzi IP di archiviazione vMotion e NFS da utilizzare per il dominio del carico di lavoro e le credenziali per accedere all'host ESXi. Fare clic su **Aggiungi** per aggiungere l'host al gruppo di host da convalidare.



4. Una volta aggiunti tutti gli host da convalidare, fare clic sul pulsante **Convalida tutti** per continuare.
5. Supponendo che tutti gli host siano convalidati, fare clic su **Avanti** per continuare.



6. Esaminare l'elenco degli host da commissionare e fare clic sul pulsante **Commission** per avviare il processo. Monitorare il processo di messa in servizio dal riquadro Attività in SDDC Manager.

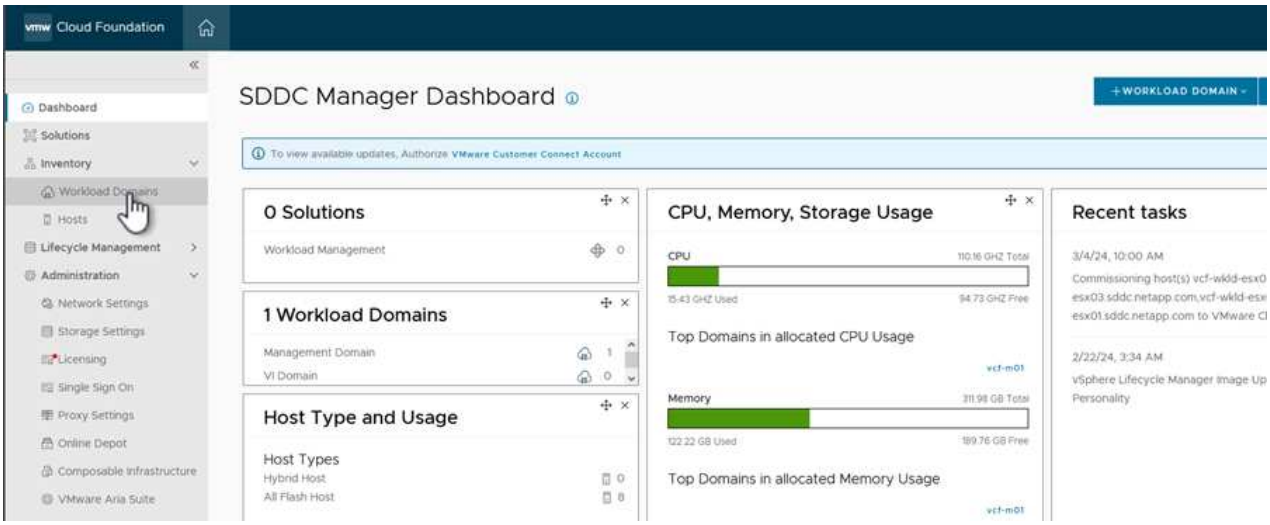

Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

Distribuisci il dominio del carico di lavoro VI

La distribuzione dei domini dei carichi di lavoro VI viene eseguita tramite l'interfaccia VCF Cloud Manager. Verranno qui presentati solo i passaggi relativi alla configurazione dell'archiviazione.

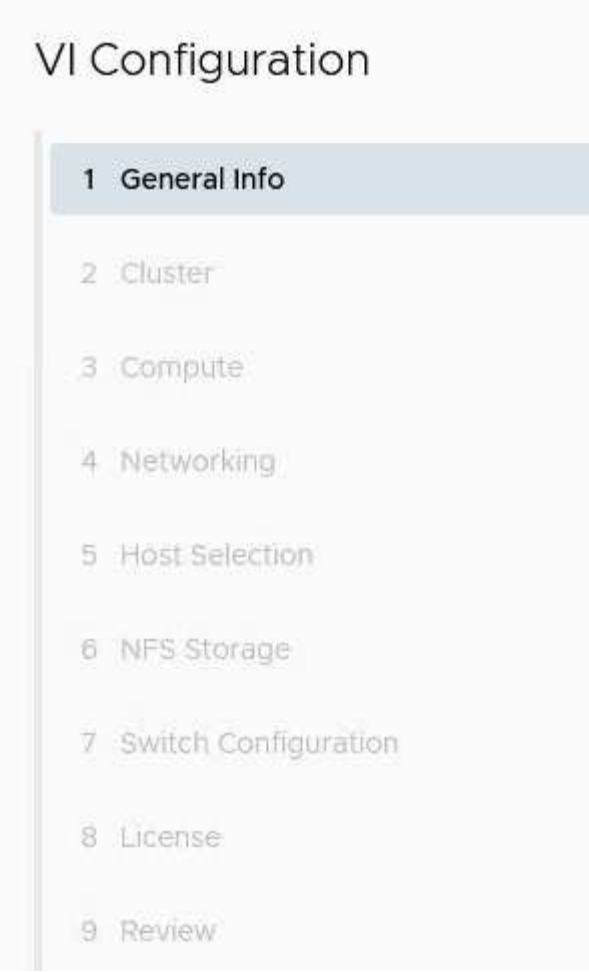
Per istruzioni dettagliate sulla distribuzione di un dominio di carico di lavoro VI, fare riferimento a"Distribuire un dominio di carico di lavoro VI utilizzando l'interfaccia utente di SDDC Manager" .

1. Dalla dashboard di SDDC Manager, fare clic su **+ Dominio del carico di lavoro** nell'angolo in alto a destra per creare un nuovo dominio del carico di lavoro.



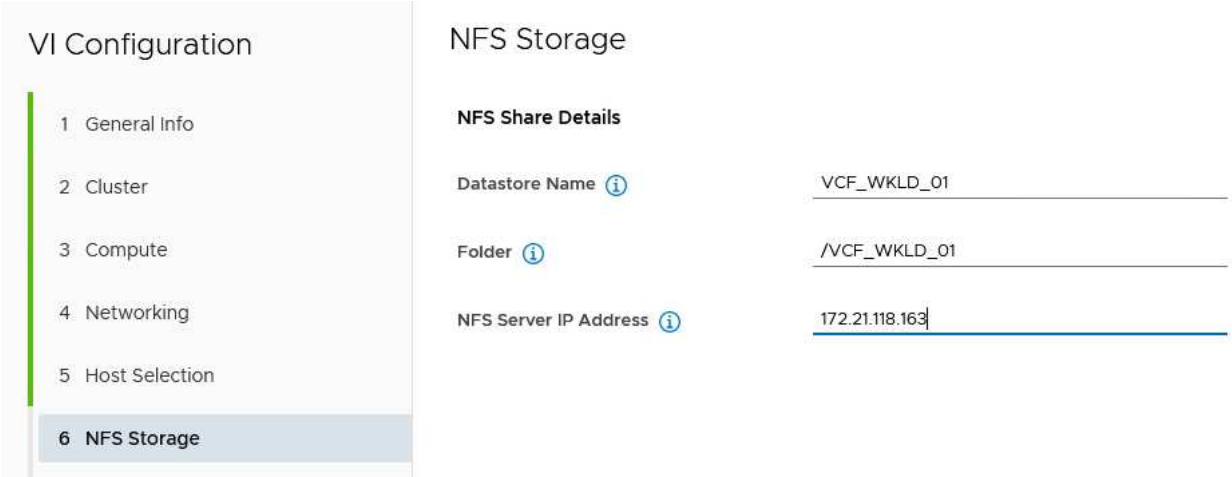
2. Nella procedura guidata di configurazione VI compilare le sezioni per **Informazioni generali, Cluster, Elaborazione, Rete** e **Selezione host** come richiesto.

Per informazioni sulla compilazione delle informazioni richieste nella procedura guidata di configurazione VI, fare riferimento a"Distribuire un dominio di carico di lavoro VI utilizzando l'interfaccia utente di SDDC Manager" .

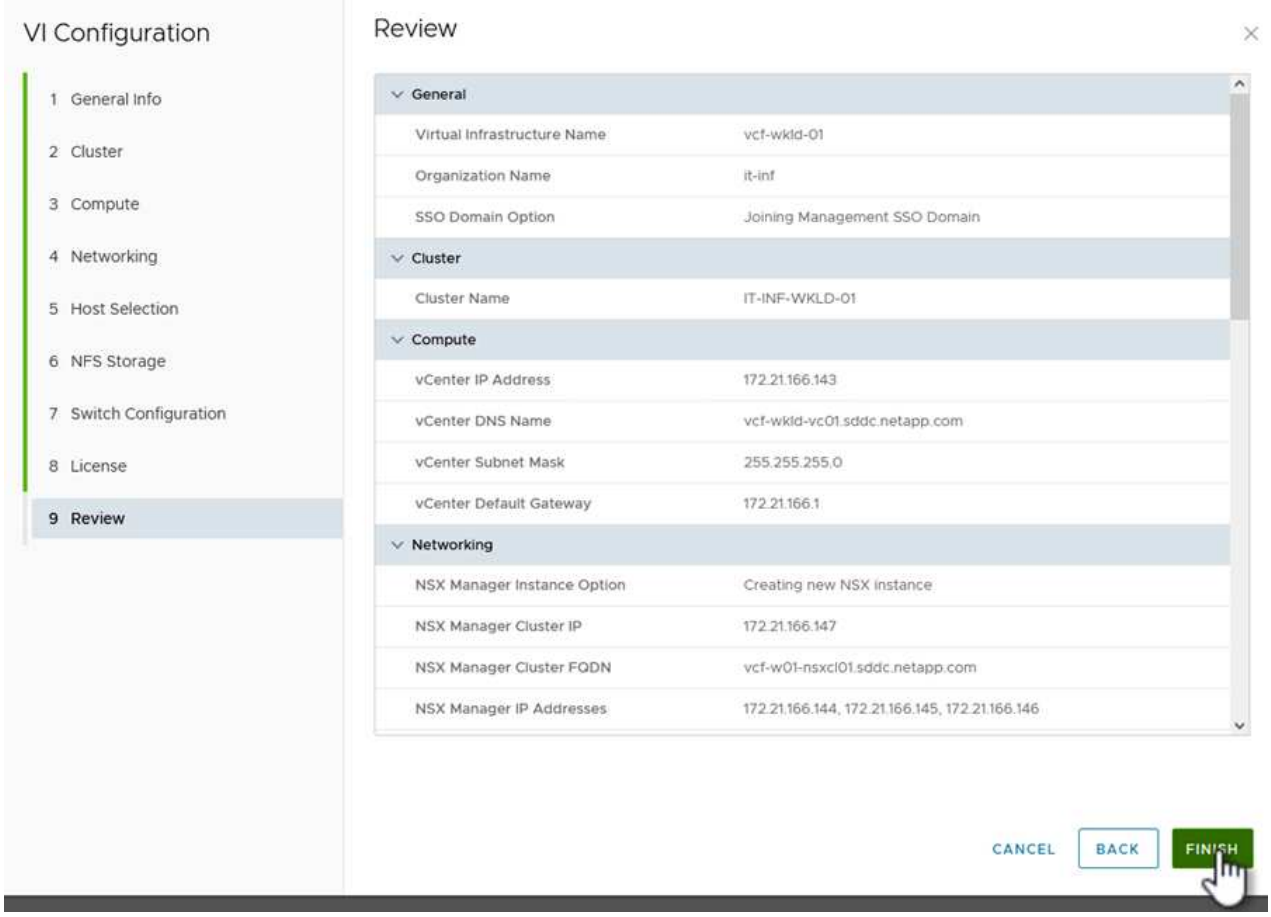


+

1. Nella sezione Archiviazione NFS, compilare il nome del datastore, il punto di montaggio della cartella del volume NFS e l'indirizzo IP della VM LIF di archiviazione NFS ONTAP .



2. Nella procedura guidata di configurazione VI, completare i passaggi di configurazione dello switch e licenza, quindi fare clic su **Fine** per avviare il processo di creazione del dominio del carico di lavoro.



3. Monitorare il processo e risolvere eventuali problemi di convalida che si presentano durante il processo.

Installa il plug-in NetApp NFS per VMware VAAI

Il plug-in NetApp NFS per VMware VAAI integra le librerie VMware Virtual Disk installate sull'host ESXi e fornisce operazioni di clonazione con prestazioni più elevate e tempi di completamento più rapidi. Questa è una procedura consigliata quando si utilizzano sistemi di archiviazione ONTAP con VMware vSphere.

Per istruzioni dettagliate sulla distribuzione del plug-in NetApp NFS per VMware VAAI, seguire le istruzioni riportate in"Installa il plug-in NetApp NFS per VMware VAAI" .

Demo video per questa soluzione

Datastore NFS come storage principale per domini di carichi di lavoro VCF

Informazioni aggiuntive

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" .

Espandi VCF con spazio di archiviazione supplementare

Scopri come espandere lo storage per un ambiente VCF utilizzando storage supplementare

VMware Cloud Foundation (VCF) supporta un'ampia gamma di opzioni di storage supplementari per espandere lo storage sui domini di gestione VCF e sui domini di carico di lavoro dell'infrastruttura virtuale (VI).

Gli strumenti ONTAP di NetApp per VMware vSphere offrono una soluzione efficiente per questa espansione, integrando perfettamente lo storage NetApp nell'ambiente VCF. Gli strumenti ONTAP semplificano la configurazione e la gestione degli archivi dati, consentendo agli amministratori di eseguire il provisioning e gestire lo storage direttamente da vSphere Client. Le funzionalità avanzate di ONTAP, quali snapshot, clonazione e protezione dei dati, migliorano le prestazioni di archiviazione, l'efficienza e la scalabilità nell'ambiente VCF.

Per i dettagli tecnici su come espandere l'ambiente VCF, fare riferimento alle seguenti soluzioni.

- "Dominio di gestione con iSCSI"
- "Dominio di gestione con FC"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con vVols (iSCSI)"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con vVols (NFS)"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con NVMe/TCP"
- "Dominio del carico di lavoro dell'infrastruttura virtuale con FC"

Aggiungere un datastore iSCSI come storage supplementare per un dominio di gestione utilizzando gli ONTAP tools for VMware vSphere

In questo caso d'uso descriviamo la procedura per aggiungere un datastore iSCSI come storage supplementare per un dominio di gestione VMware Cloud Foundation (VCF). Questa procedura riassume la configurazione di una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per iSCSI, la configurazione della rete iSCSI sugli host ESXi, la distribuzione di ONTAP Tools per VMware vSphere e la creazione di un datastore VMFS.

Vantaggi di iSCSI

Prestazioni elevate: offre prestazioni elevate per garantire velocità di trasferimento dati rapide ed efficienti e bassa latenza. Ideale per applicazioni aziendali esigenti e ambienti virtualizzati.

Facilità di gestione: semplifica la gestione dell'archiviazione utilizzando strumenti e protocolli basati su IP noti.

Conveniente: utilizza l'infrastruttura Ethernet esistente, riducendo la necessità di hardware specializzato e consentendo alle organizzazioni di ottenere soluzioni di archiviazione affidabili e scalabili.

Per ulteriori informazioni sull'utilizzo di iSCSI con i sistemi di storage NetApp , fare riferimento a "Provisioning SAN con iSCSI" .

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

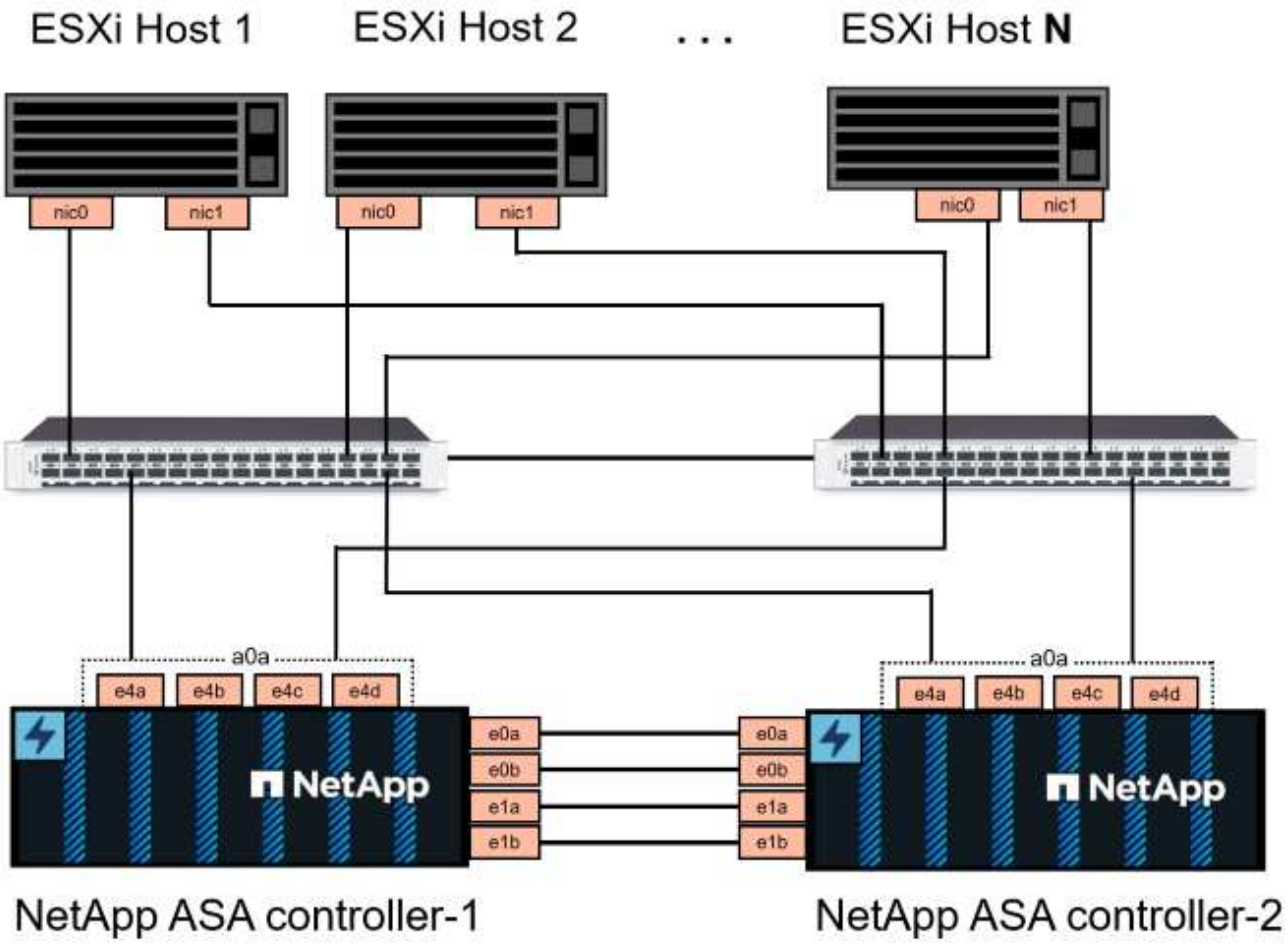
- Creare una macchina virtuale di archiviazione (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuiti per reti iSCSI sul dominio di gestione VCF.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio di gestione VCF.
- Distribuire gli strumenti ONTAP sul dominio di gestione VCF.
- Creare un nuovo datastore VMFS sul dominio di gestione VCF.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o ASA con porte dati fisiche su switch Ethernet dedicate al traffico di archiviazione.
- La distribuzione del dominio di gestione VCF è completa e il client vSphere è accessibile.

NetApp consiglia progetti di rete completamente ridondanti per iSCSI. Il diagramma seguente illustra un esempio di configurazione ridondante, che garantisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. Fare riferimento a NetApp"Riferimento alla configurazione SAN" per ulteriori informazioni.



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

Questa documentazione illustra il processo di creazione di una nuova SVM e di specifica delle informazioni sull'indirizzo IP per creare più LIF per il traffico iSCSI. Per aggiungere nuovi LIF a un SVM esistente, fare riferimento a"Creare un LIF (interfaccia di rete)" .

Per ulteriori informazioni sull'utilizzo di datastore iSCSI VMFS con VMware, fare riferimento a"vSphere VMFS Datastore - Backend di archiviazione iSCSI con ONTAP" .

> Nei casi in cui più adattatori VMkernel sono configurati sulla stessa rete IP, si consiglia di utilizzare il binding delle porte iSCSI software sugli host ESXi per garantire il bilanciamento del carico tra gli adattatori. Fare riferimento all'articolo della Knowledge Base"Considerazioni sull'utilizzo del binding delle porte iSCSI software in ESX/ESXi (2038869)" .

Fasi di distribuzione

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

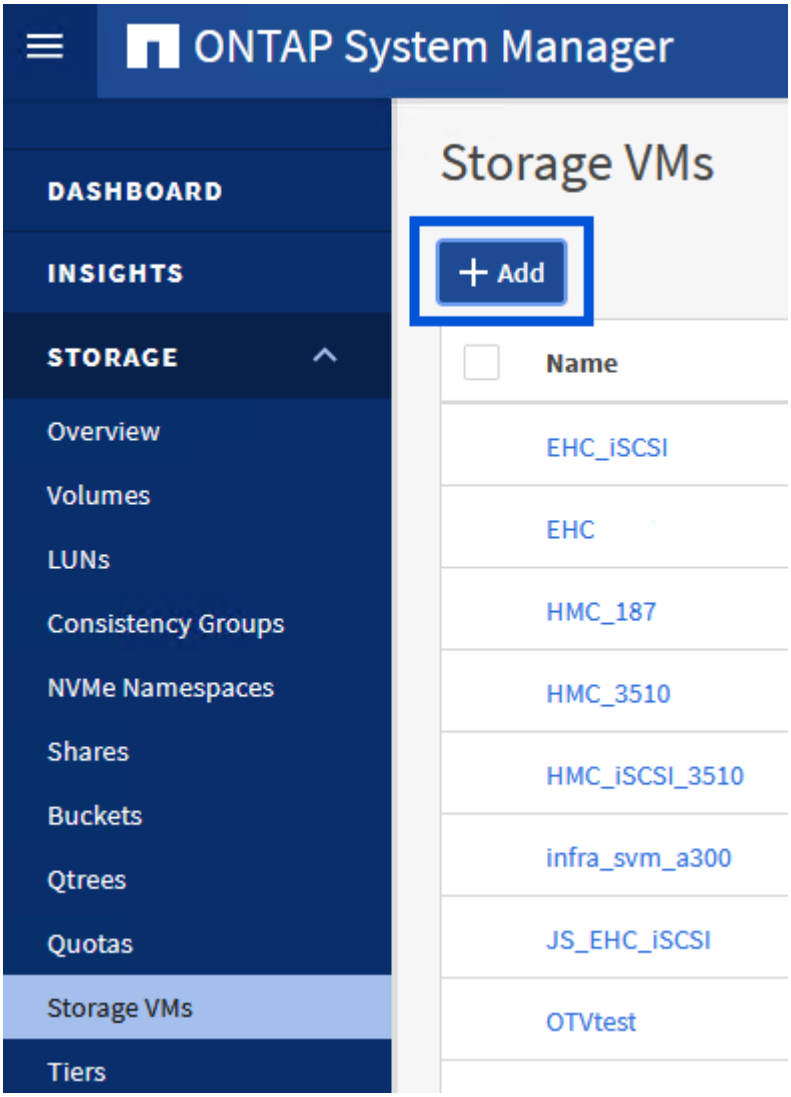
Creare SVM e LIF sul sistema di archiviazione ONTAP

Il passaggio successivo viene eseguito in ONTAP System Manager.

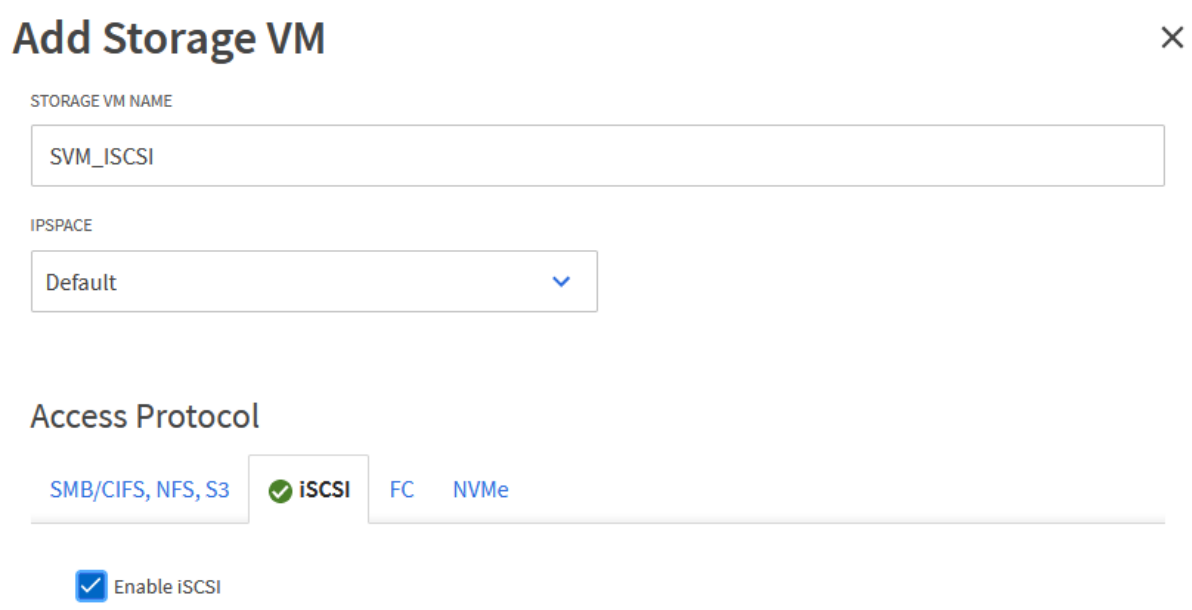
Creare la VM di archiviazione e i LIF

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

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

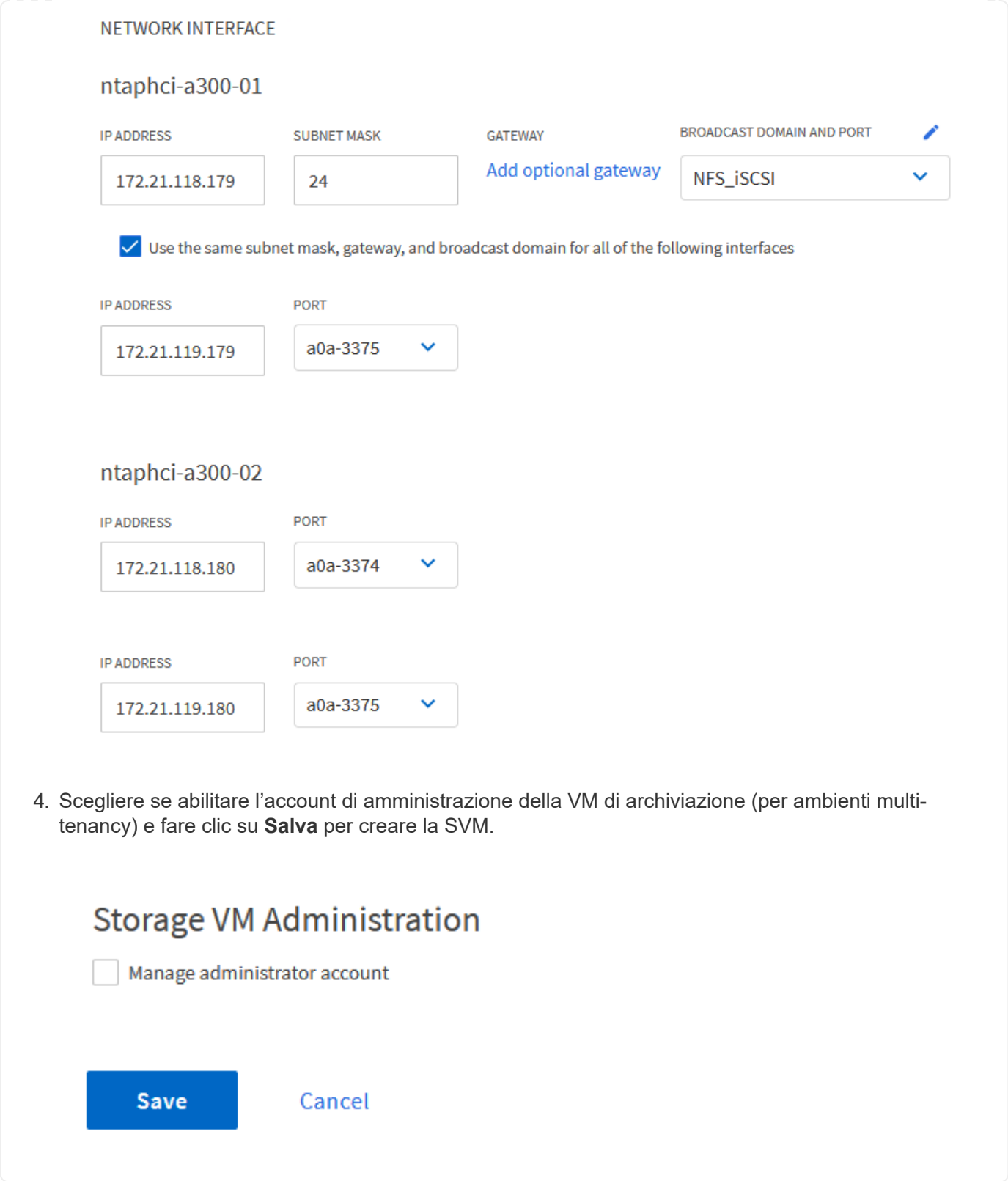


2. Nella procedura guidata **Aggiungi VM di archiviazione**, fornire un **Nome** per la SVM, selezionare lo **Spazio IP** e quindi, in **Protocollo di accesso, fare clic sulla scheda *iSCSI** e selezionare la casella per **Abilitare iSCSI**.



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.

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



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.

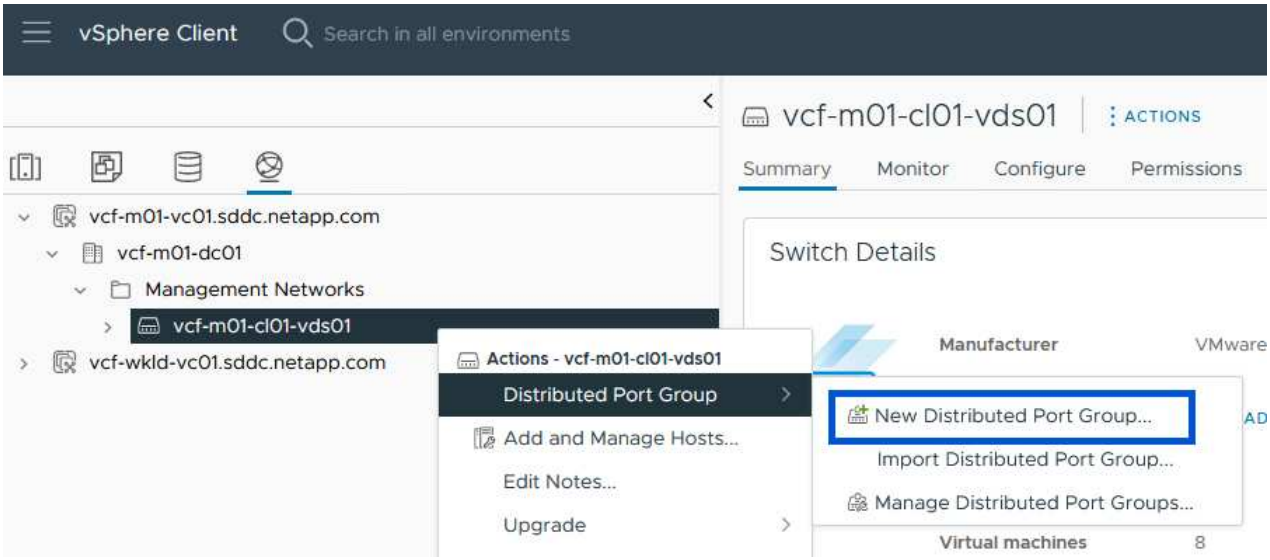
Configurazione della rete per iSCSI su host ESXi

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

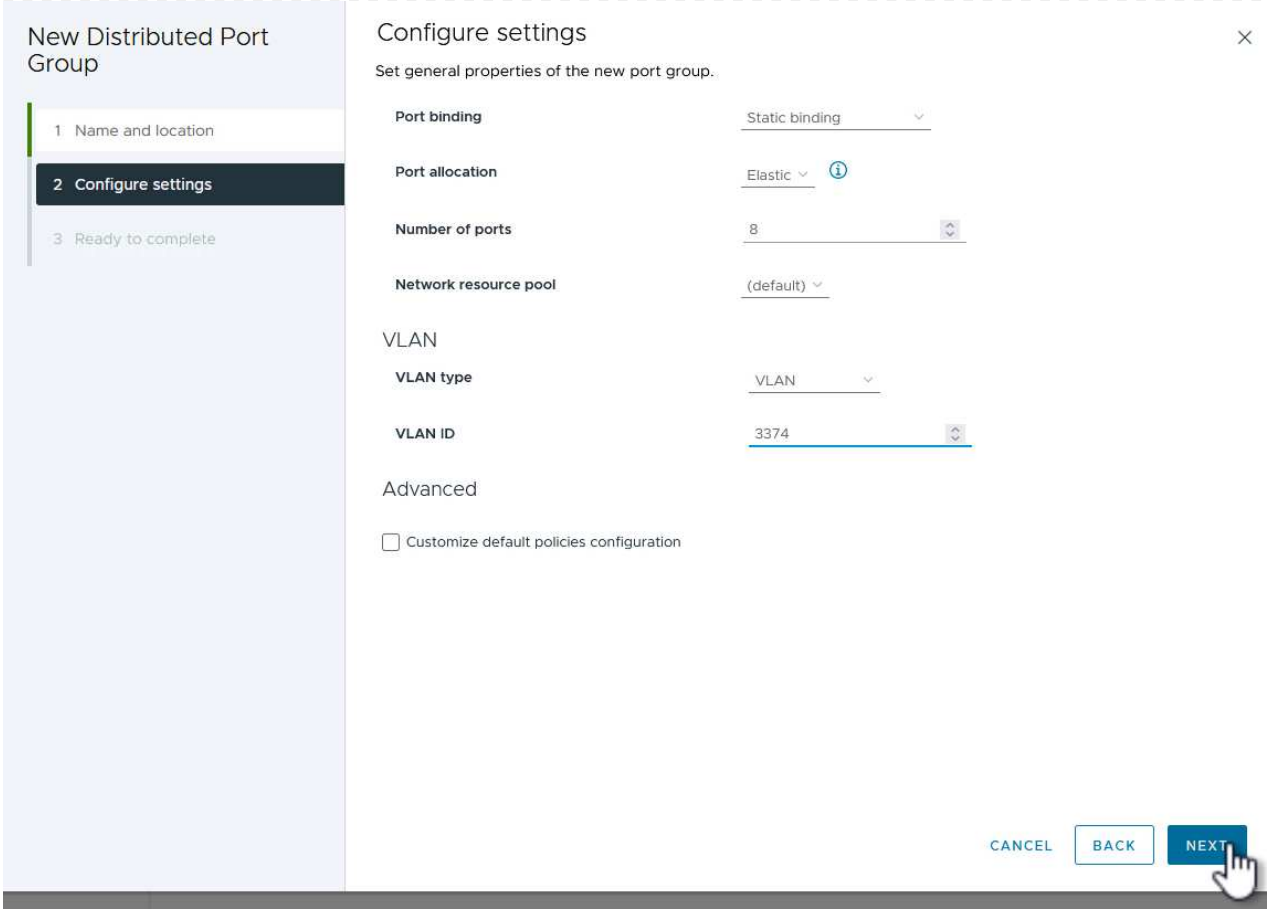
Creare gruppi di porte distribuiti per il traffico iSCSI

Completare la seguente procedura per creare un nuovo gruppo di porte distribuito per ogni rete iSCSI:

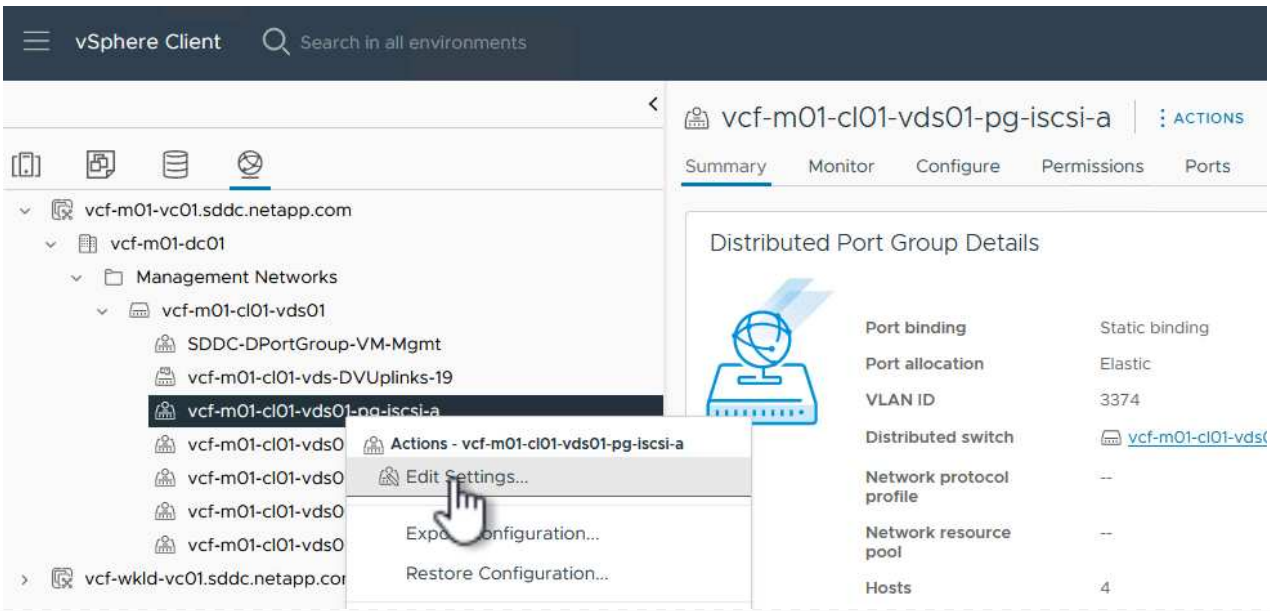
1. Dal client vSphere per il cluster del dominio di gestione, accedere a **Inventario > Rete**. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite…**.



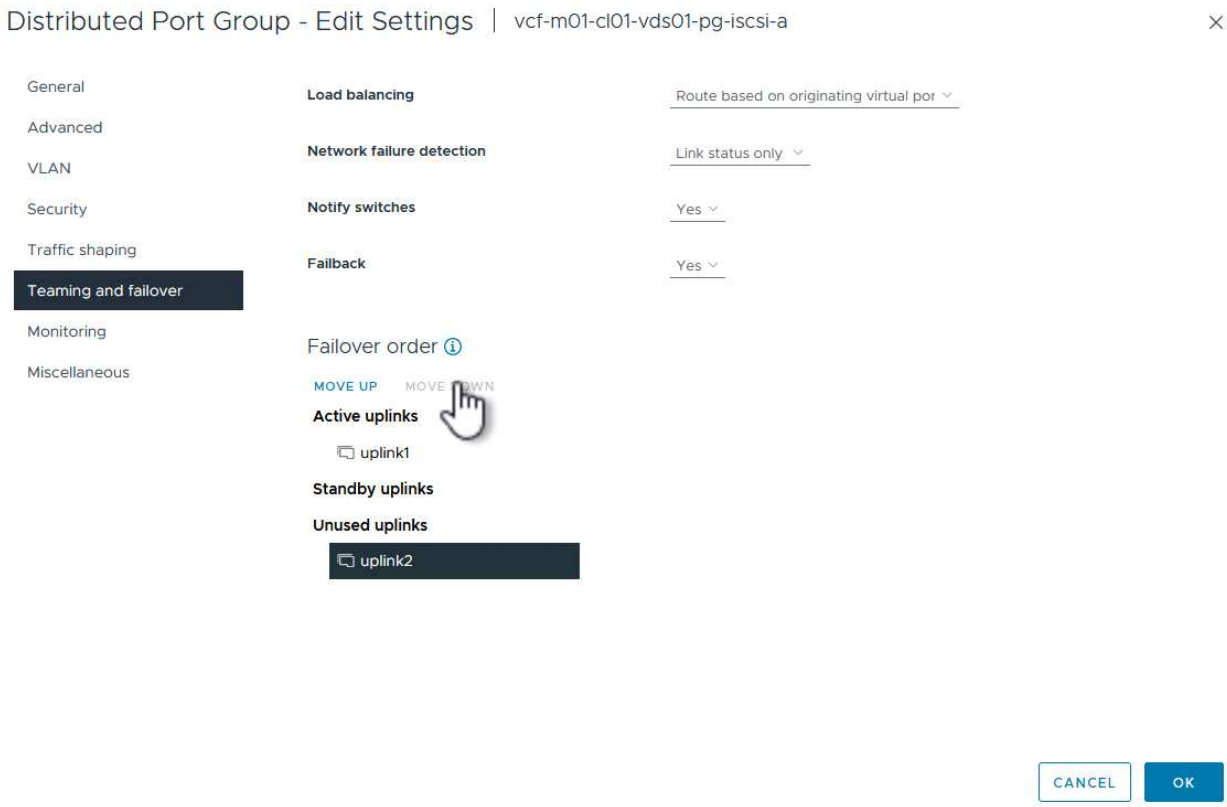
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, immettere un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare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



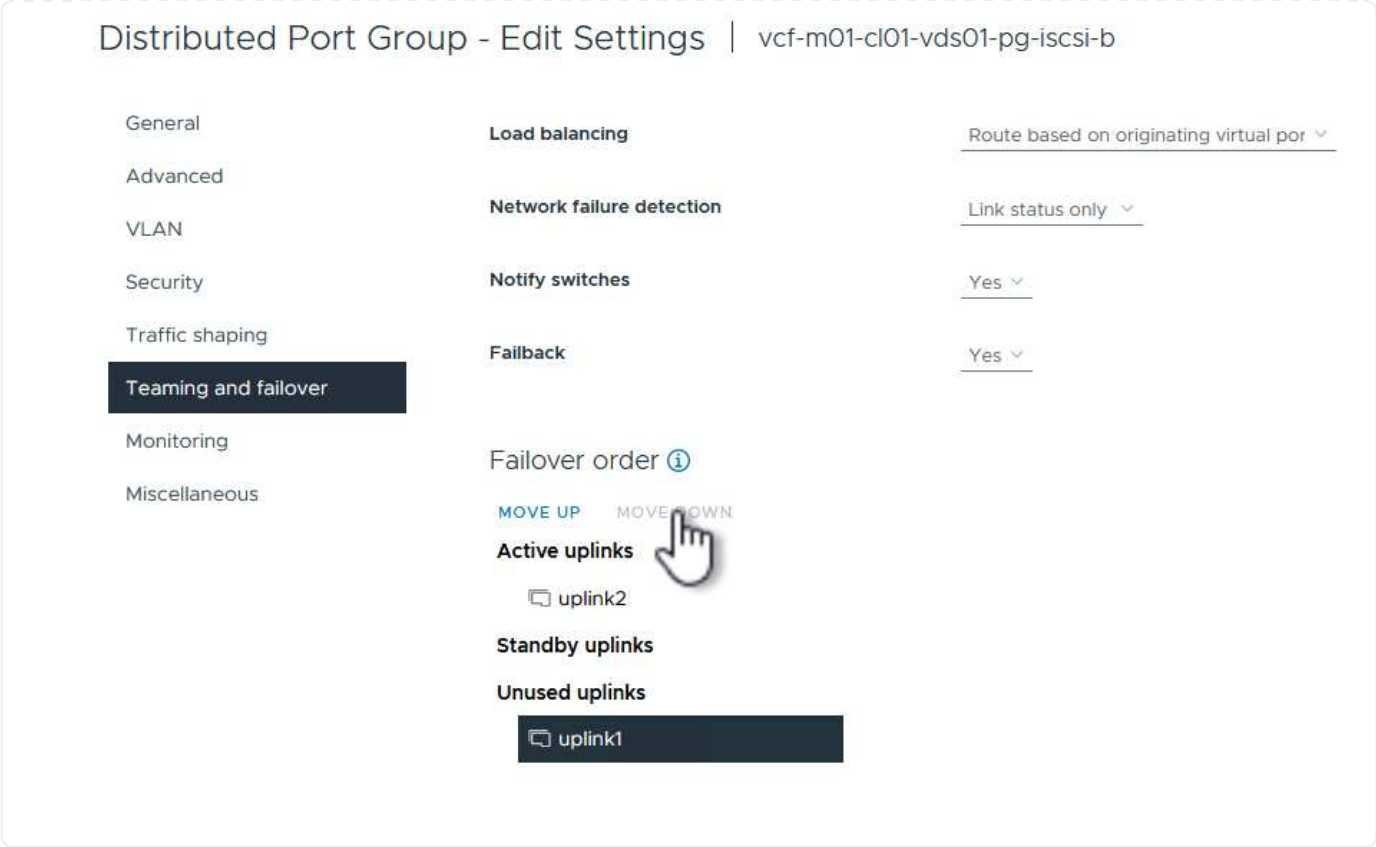
4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **Fine** per creare il nuovo gruppo di porte distribuite.
5. Ripetere questa procedura per creare un gruppo di porte distribuito per la seconda rete iSCSI utilizzata e assicurarsi di aver immesso l'**ID VLAN** corretto.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



7. Nella pagina **Gruppo di porte distribuite - Modifica impostazioni**, vai su **Teaming e failover** nel menu a sinistra e fai clic su **uplink2** per spostarlo in basso a **Uplink non utilizzati**.



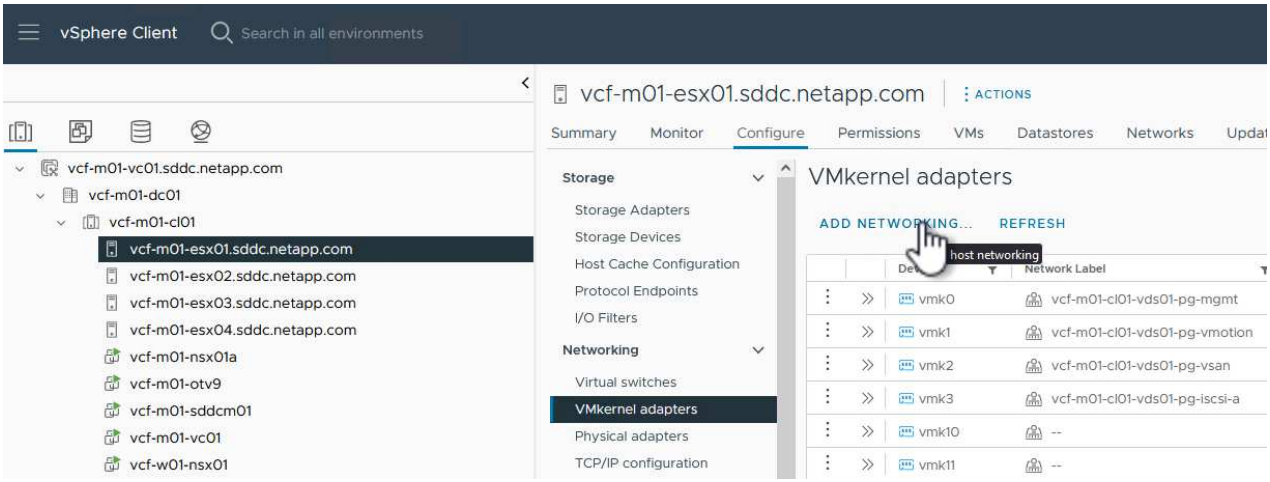
8. Ripetere questo passaggio per il secondo gruppo di porte iSCSI. Questa volta, però, sposta **uplink1** in **Uplink non utilizzati**.


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

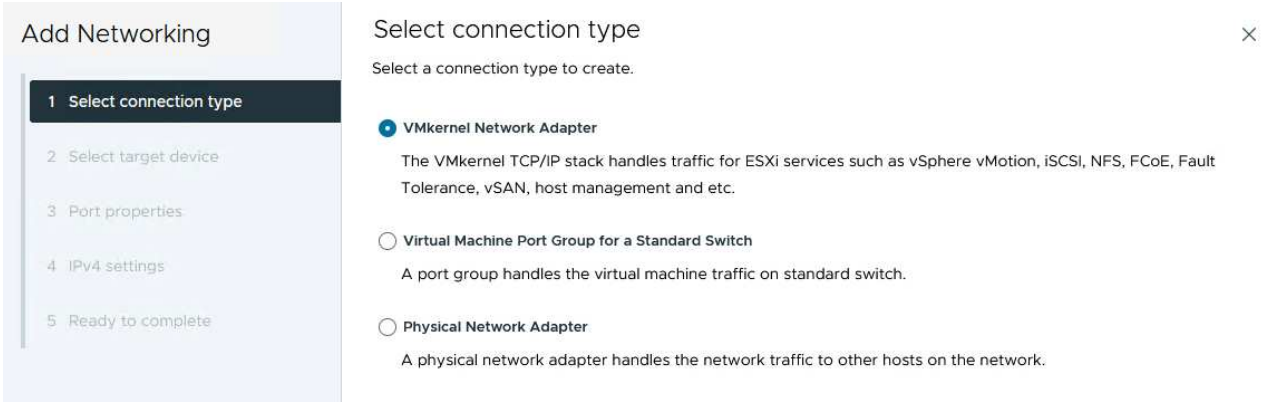
Creare adattatori VMkernel su ciascun host ESXi

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

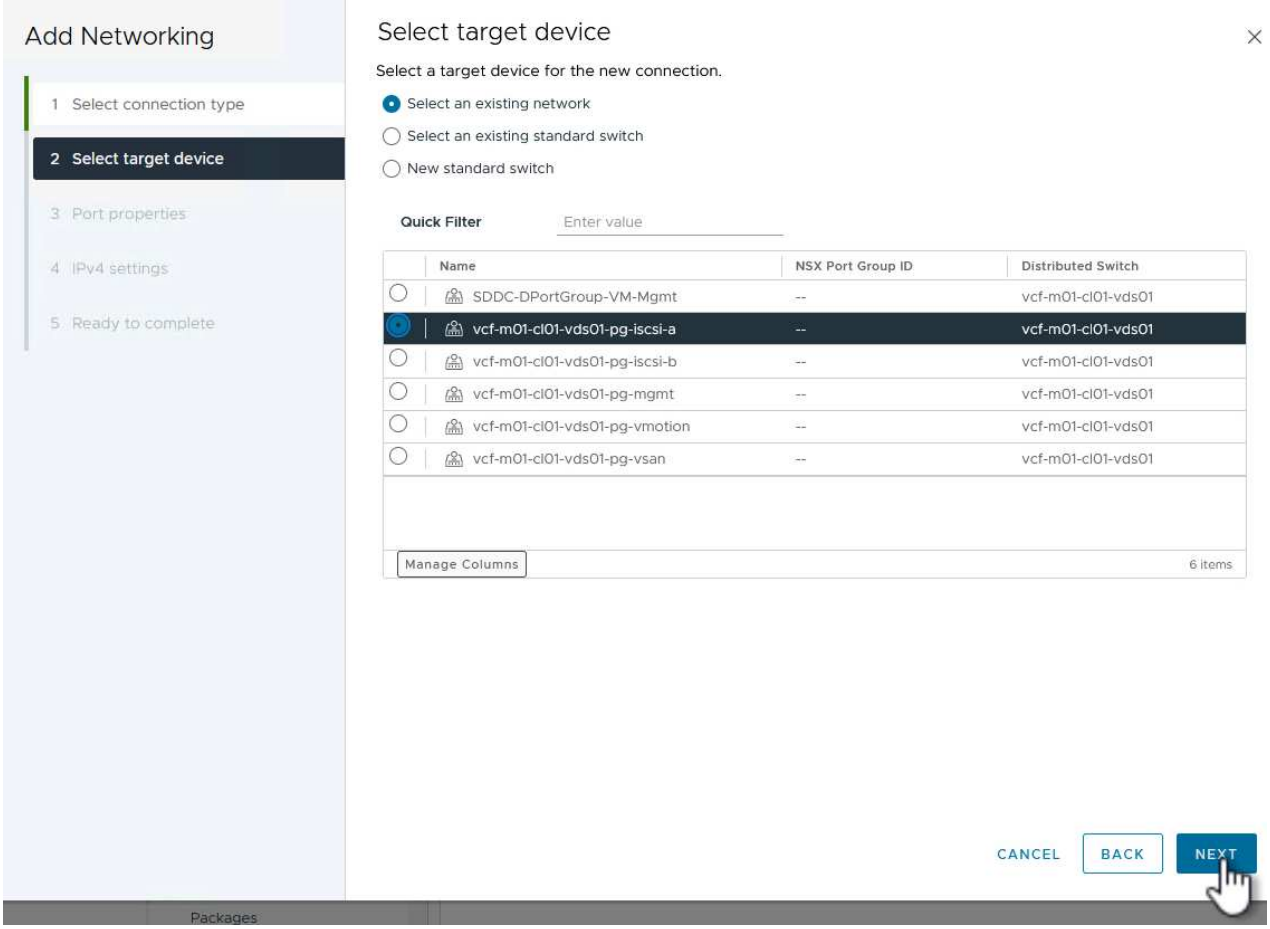
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio di gestione. Dalla scheda **Configura** seleziona **Schede VMkernel** e clicca su **Aggiungi rete…** per iniziare.



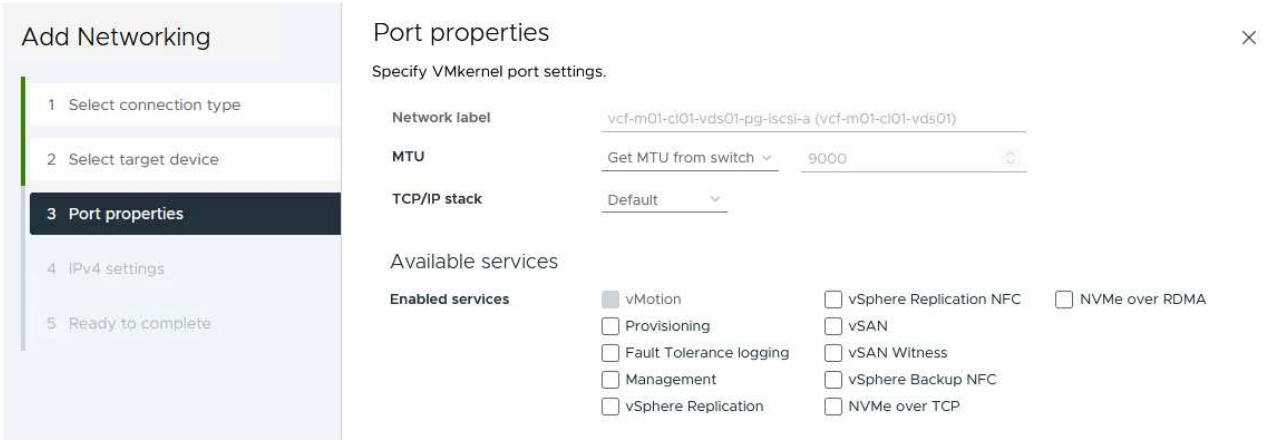
2. Nella finestra **Seleziona tipo di connessione** seleziona **Scheda di rete VMkernel** e fai clic su **Avanti** per continuare.



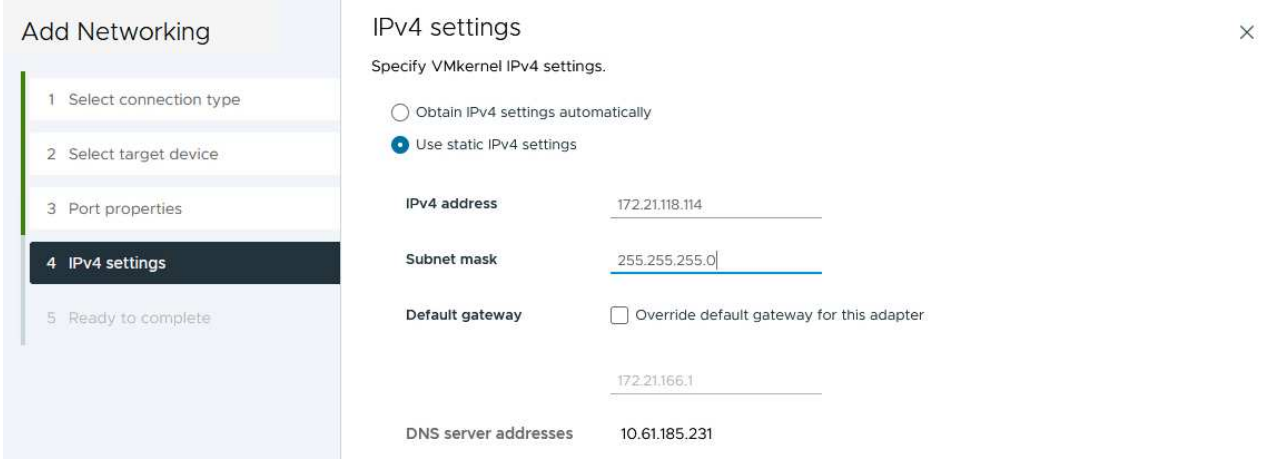
3. Nella pagina **Seleziona dispositivo di destinazione**, seleziona uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



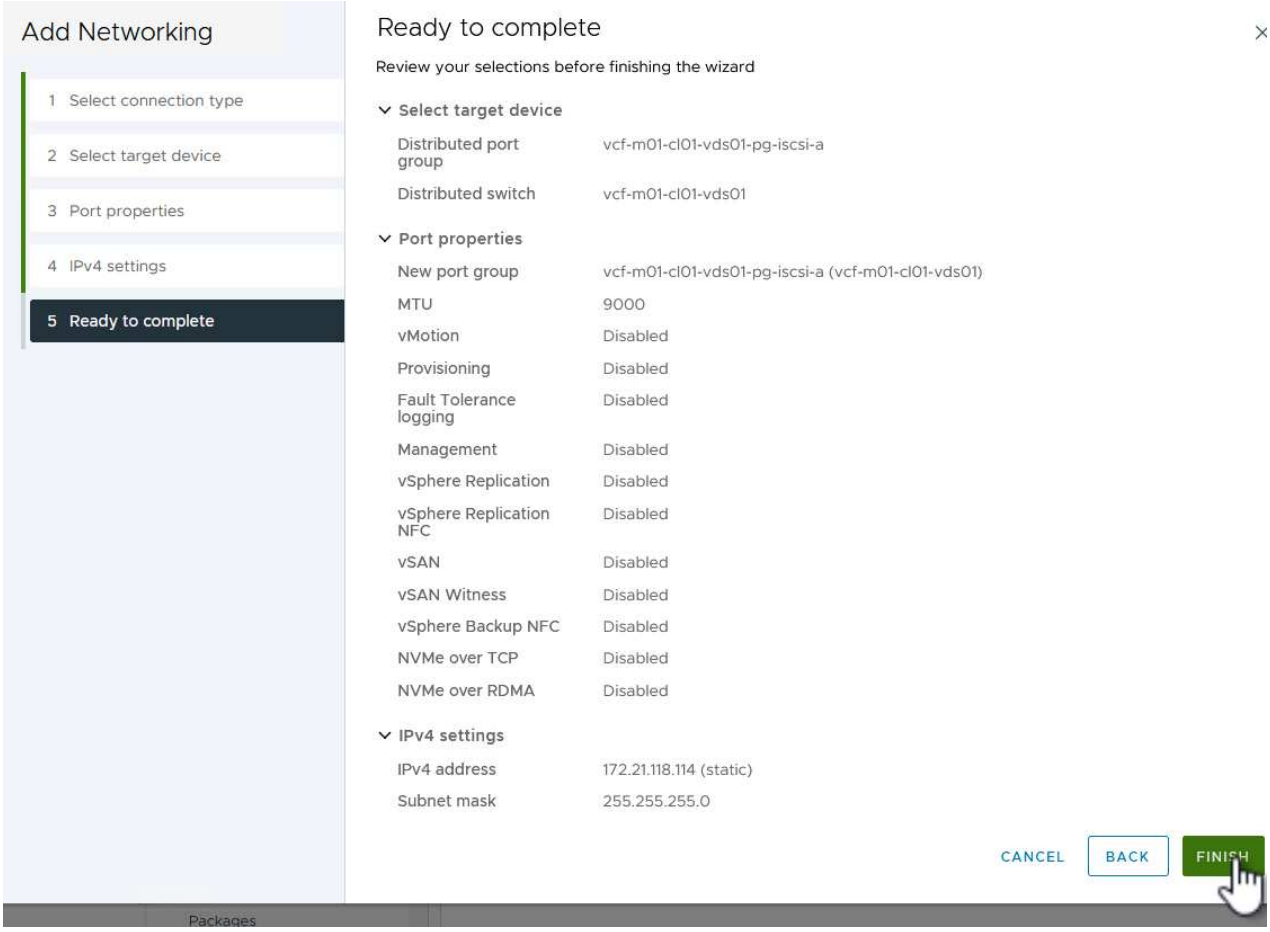
4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e fare clic su **Avanti** per continuare.



5. Nella pagina **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.



7. Ripetere questo processo per creare un adattatore VMkernel per la seconda rete iSCSI.

Distribuisci e usa gli strumenti ONTAP per configurare l’archiviazione

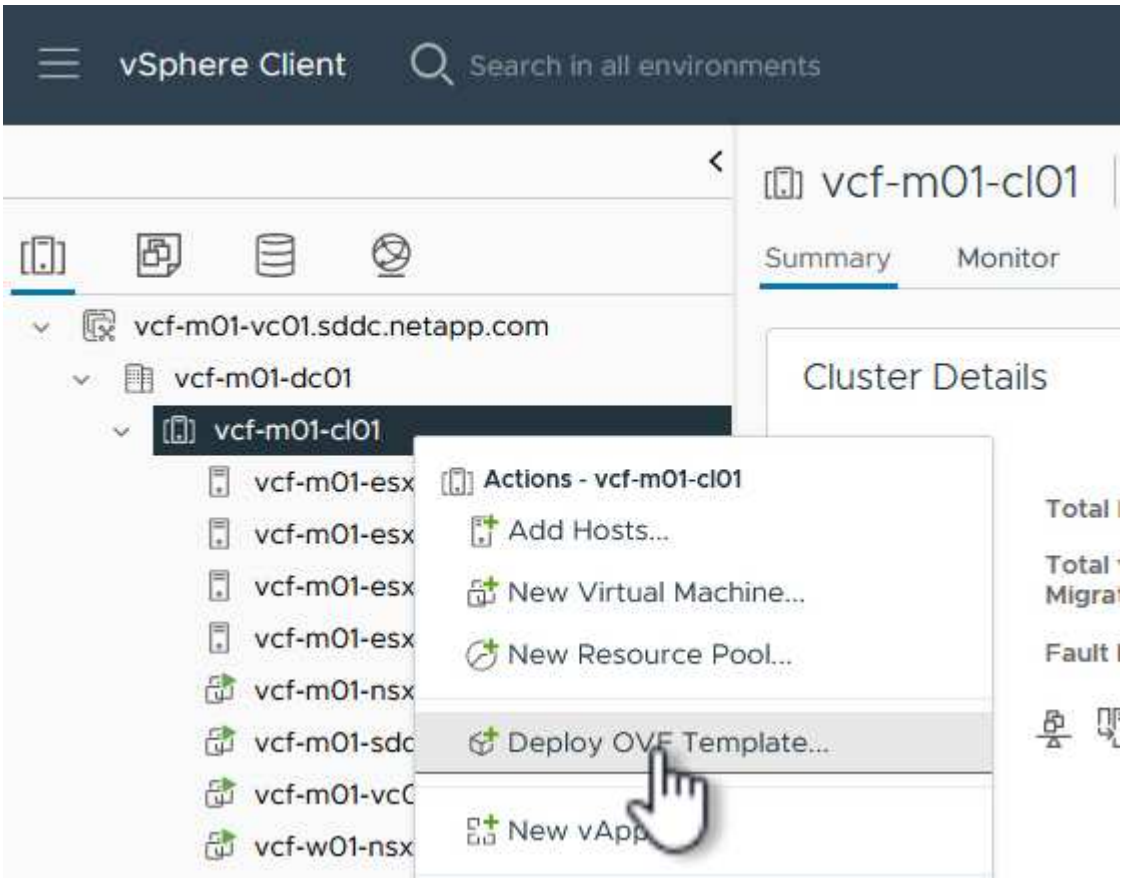
I passaggi seguenti vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere e comportano la distribuzione di OTV, la creazione di un datastore iSCSI VMFS e la migrazione delle VM di gestione al nuovo datastore.

Distribuisci gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere (OTV) vengono distribuiti come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP .

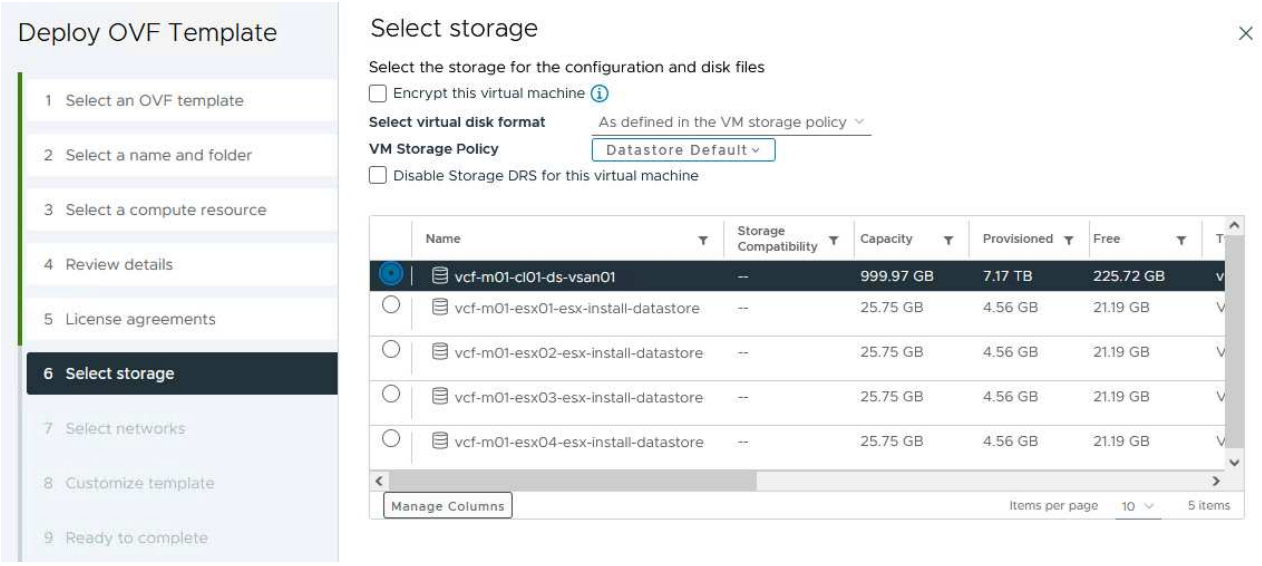
Completare quanto segue per distribuire gli ONTAP tools for VMware vSphere:

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 dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Distribuisci modello OVF…**

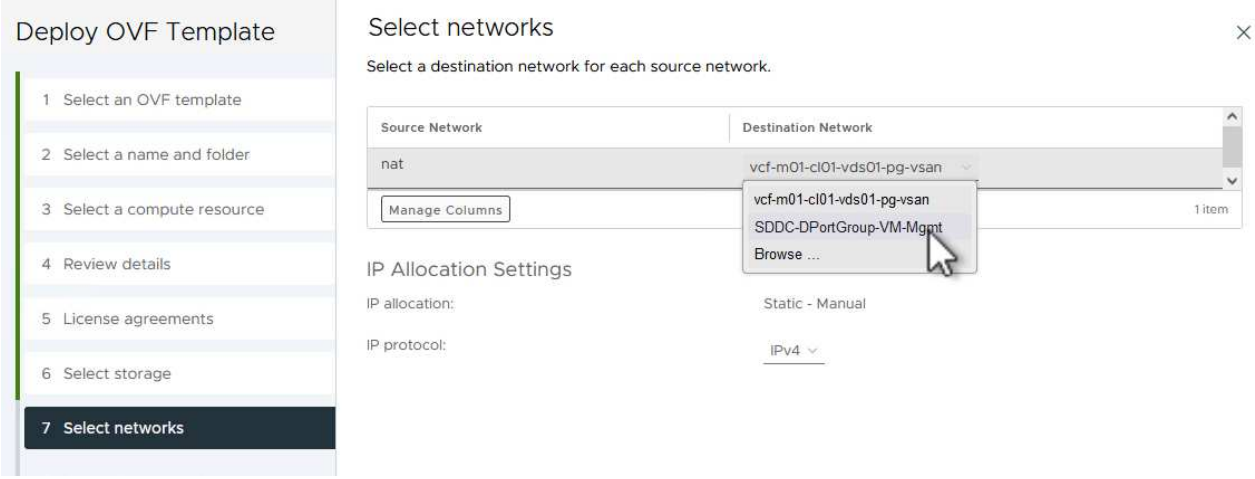


4. Nella procedura guidata **Distribuisci modello OVF**, fare clic sul pulsante di opzione **File locale** e selezionare il file OVA degli strumenti ONTAP scaricato nel passaggio precedente.

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 il datastore vSAN del cluster del dominio di gestione VCF.

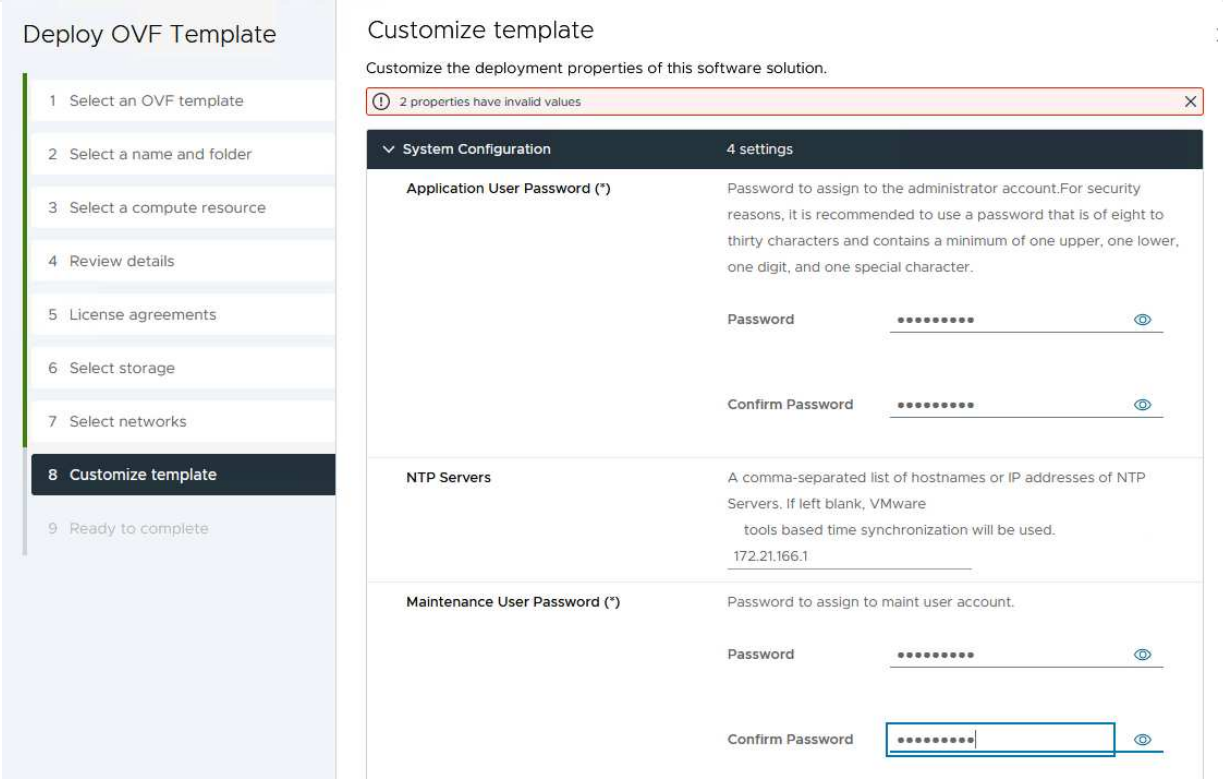


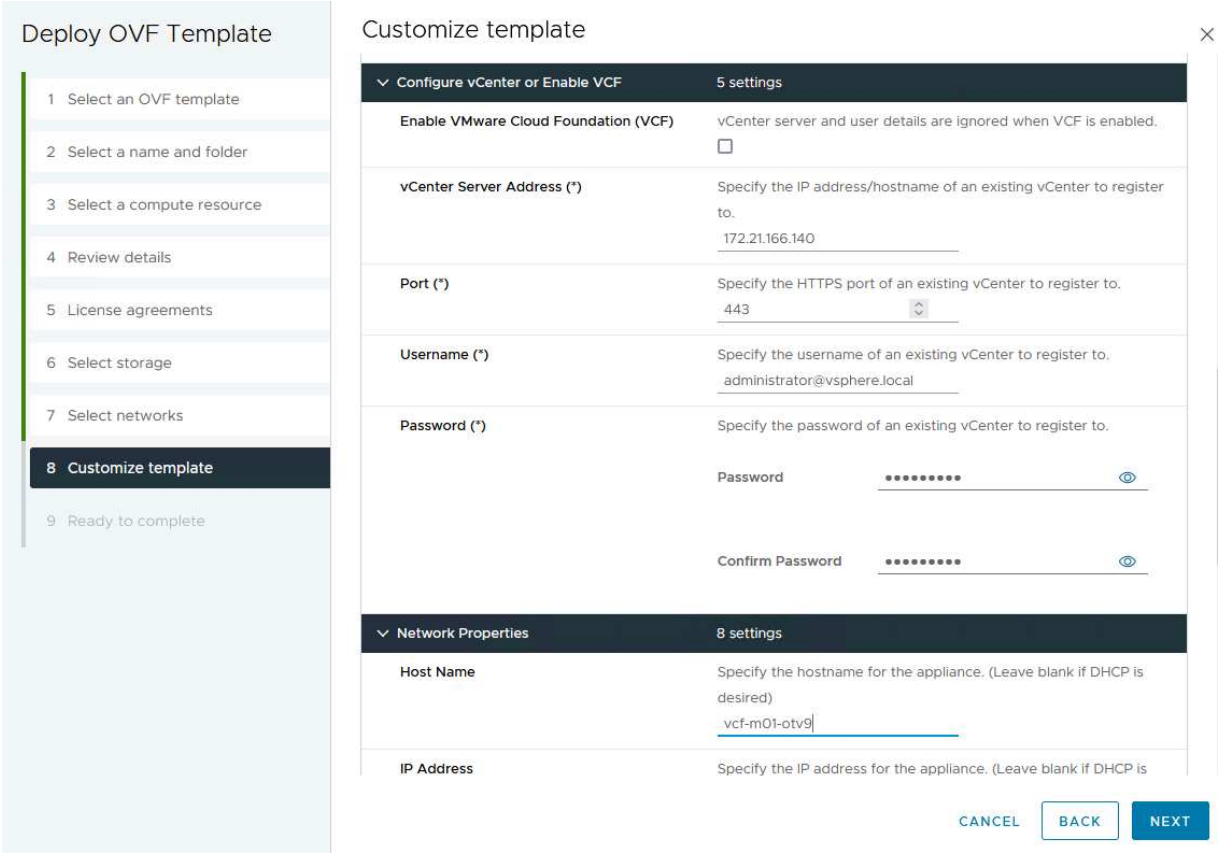
7. Nella pagina Seleziona rete seleziona la rete utilizzata per la gestione del traffico.



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

     Fare clic su **Avanti** per continuare.



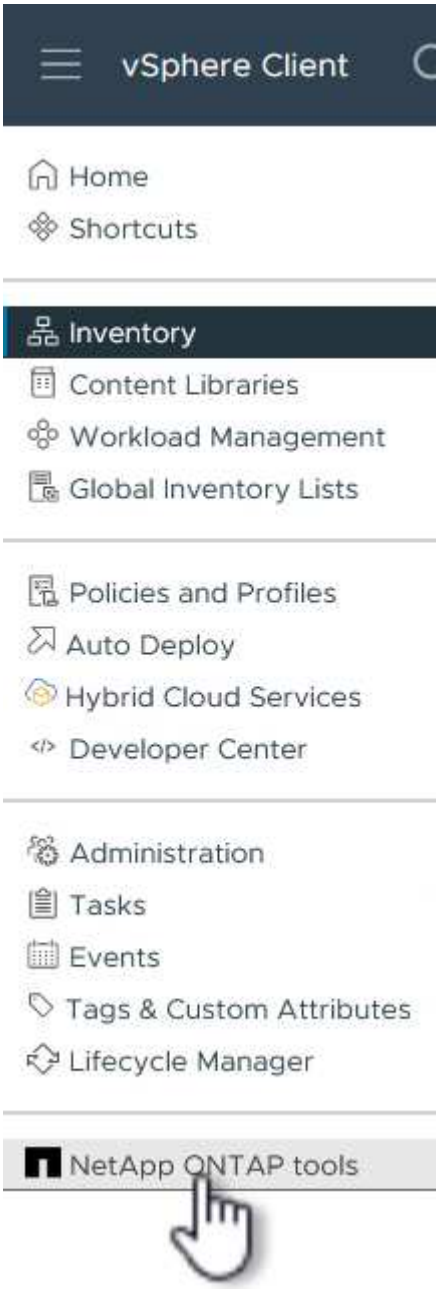


9. Rivedere tutte le informazioni nella pagina Pronto per il completamento e fare clic su Fine per iniziare a distribuire l'appliance OTV.

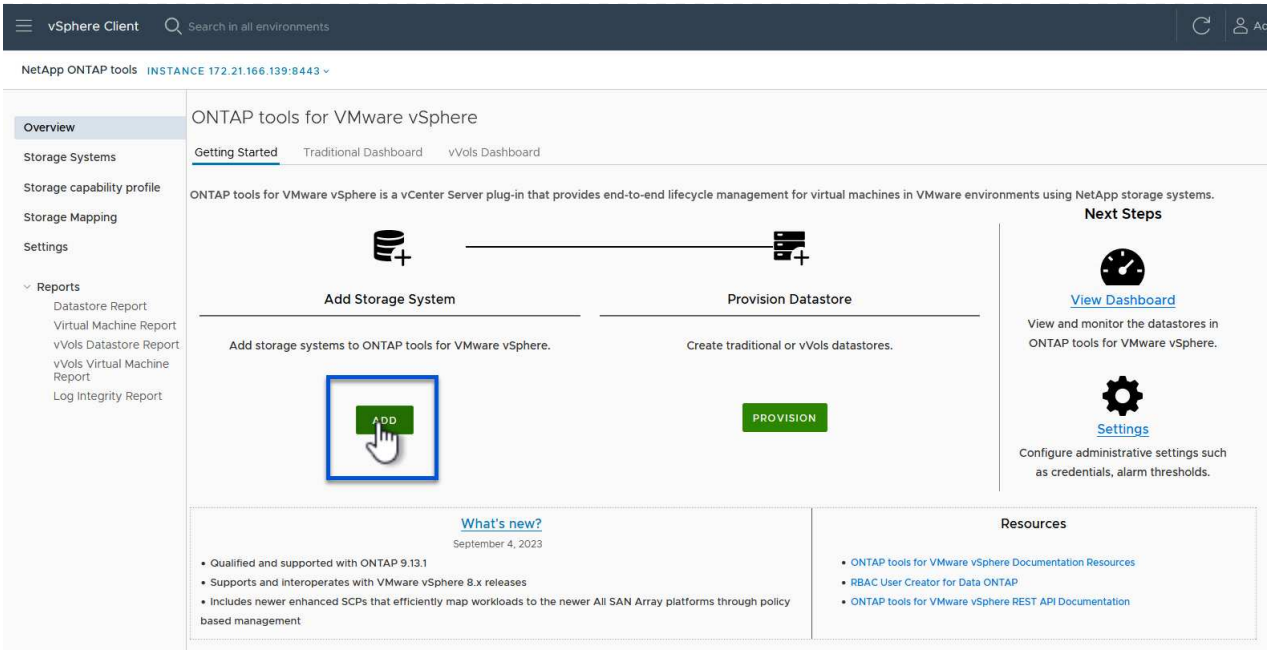
Configurare un datastore iSCSI VMFS sul dominio di gestione utilizzando OTV

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

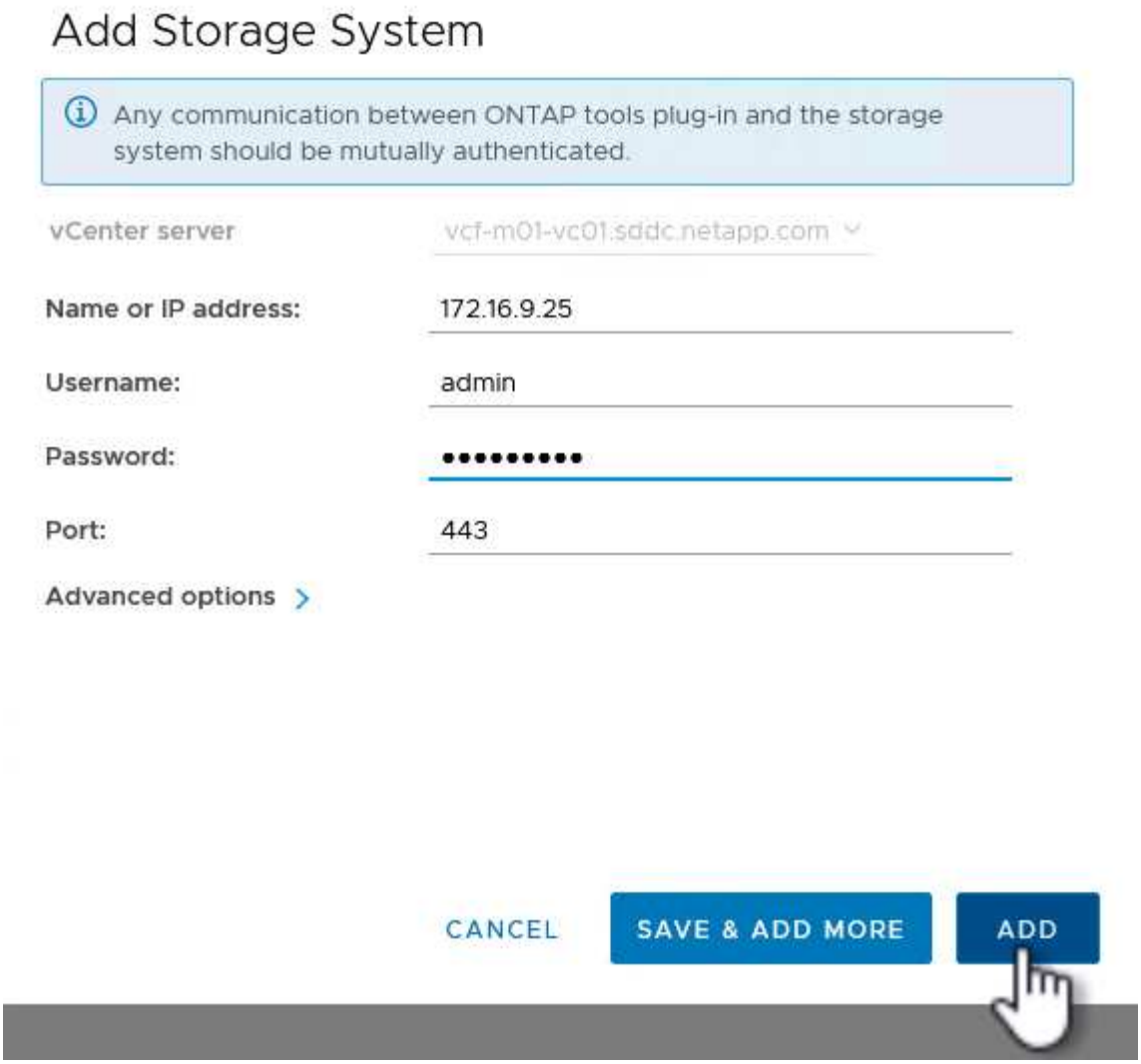
1. Nel client vSphere, accedere al menu principale e selezionare *Strumenti NetApp ONTAP *.



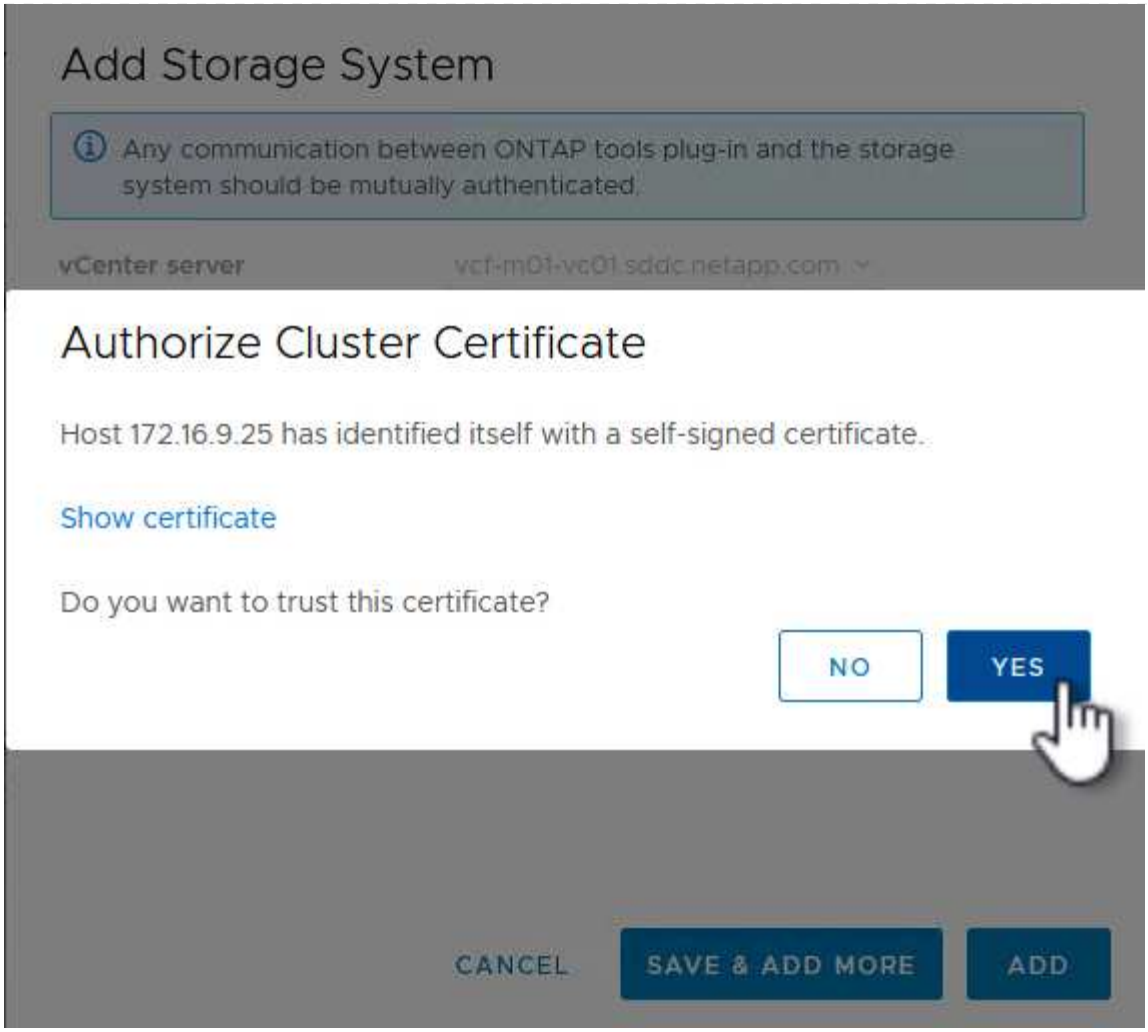
2. Una volta in * ONTAP Tools*, dalla pagina Getting Started (o da **Storage Systems**), fare clic su **Aggiungi** per aggiungere un nuovo sistema di archiviazione.



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



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

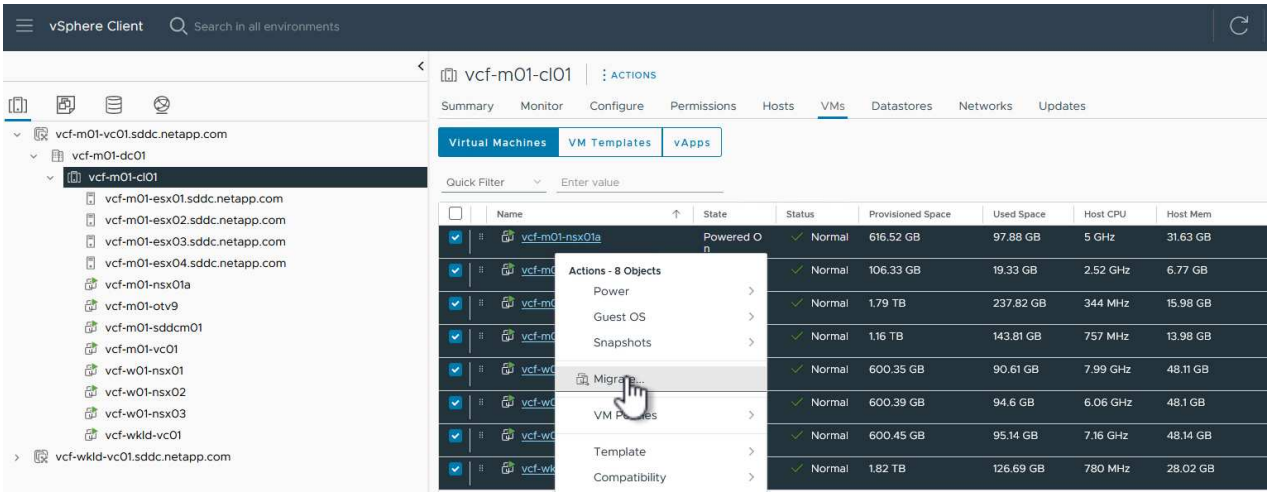

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust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

Migrazione delle VM di gestione su iSCSI Datastore

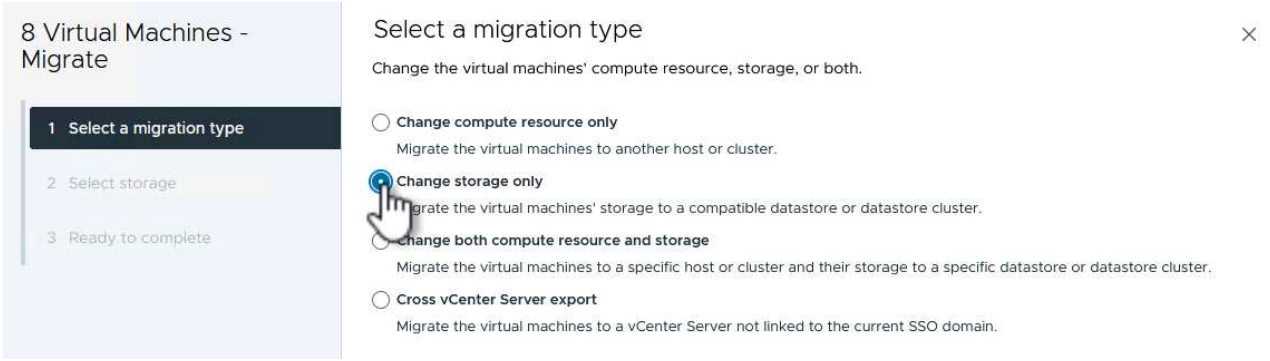
Nei casi in cui si preferisce utilizzare l'archiviazione ONTAP per proteggere le VM di gestione VCF, è possibile utilizzare vMotion per migrare le VM al datastore iSCSI appena creato.

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

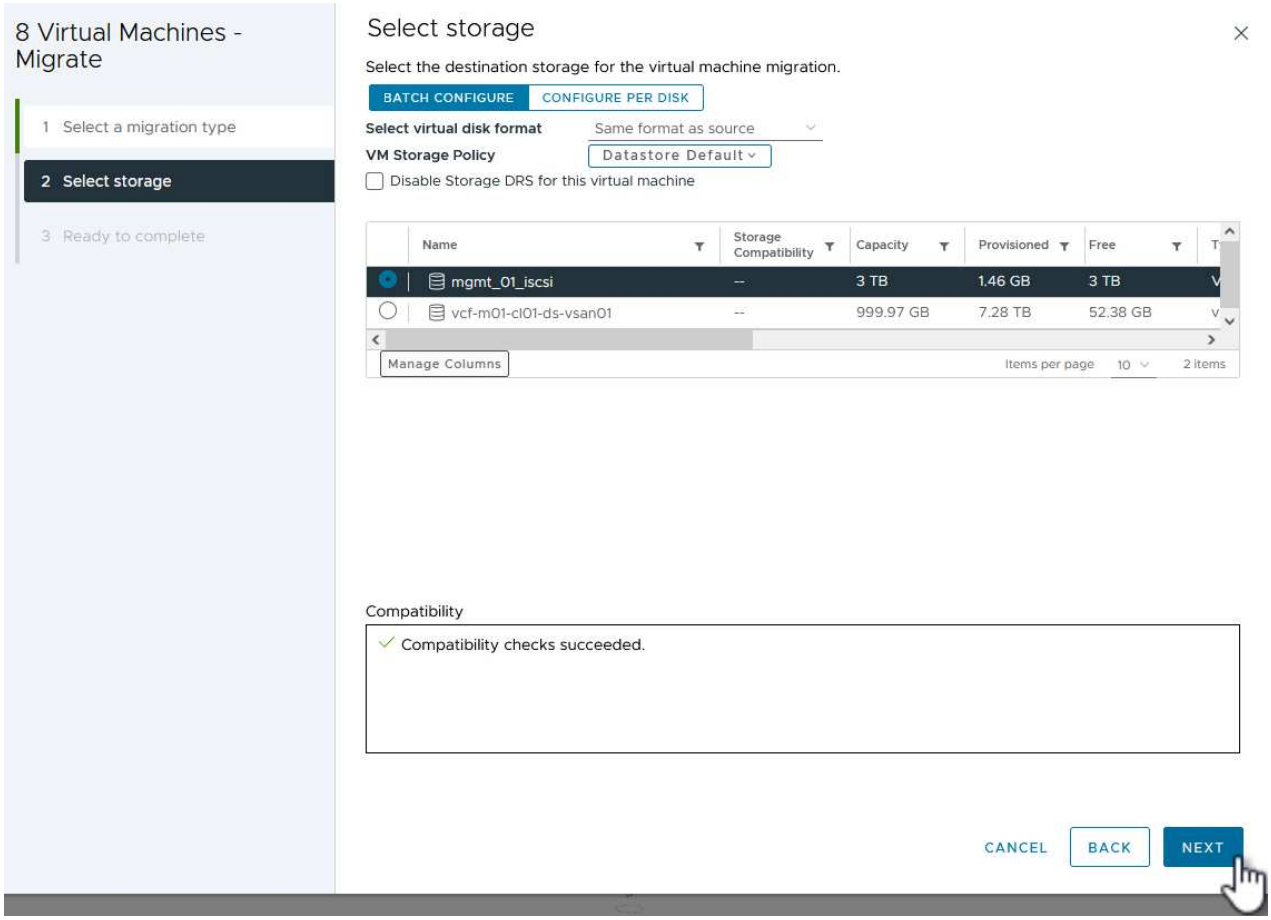
1. Da vSphere Client, accedere al cluster del dominio di gestione e fare clic sulla scheda **VM**.
2. Selezionare le VM da migrare nel datastore iSCSI, fare clic con il pulsante destro del mouse e selezionare **Migra...**.



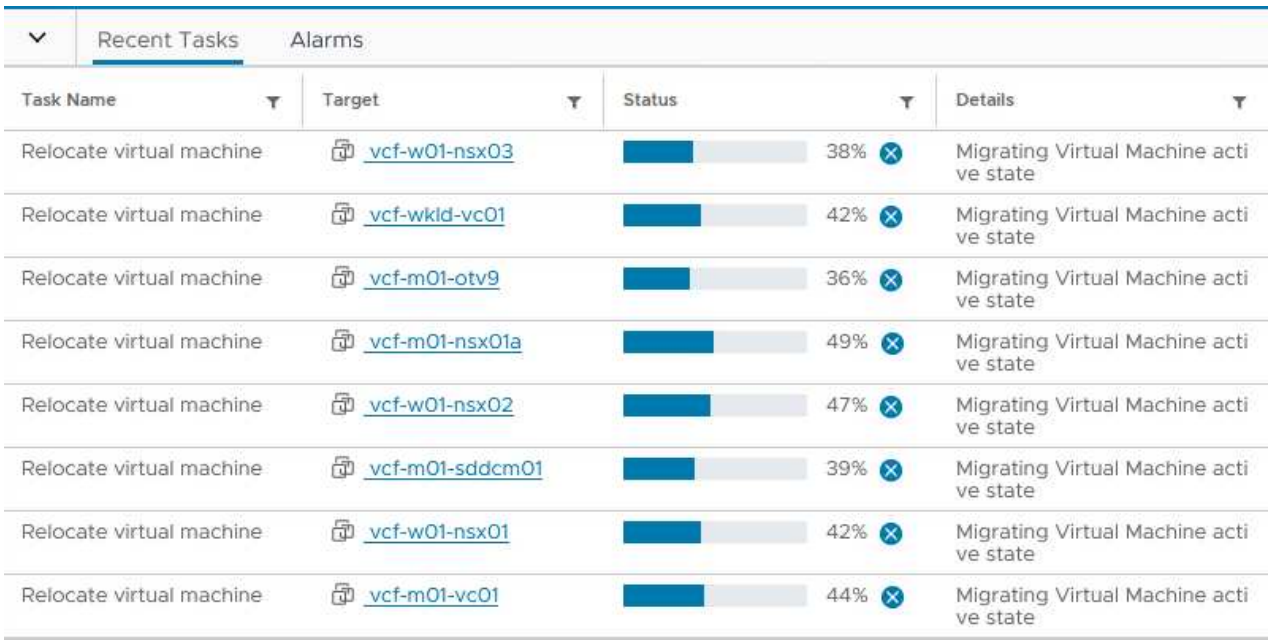
3. Nella procedura guidata **Macchine virtuali - Migrazione**, seleziona **Modifica solo archiviazione** come tipo di migrazione e fai clic su **Avanti** per continuare.



4. Nella pagina **Seleziona storage**, seleziona il datastore iSCSi e seleziona **Avanti** per continuare.



5. Rivedi le selezioni e clicca su **Fine** per avviare la migrazione.
6. Lo stato del trasferimento può essere visualizzato nel riquadro **Attività recenti**.



Informazioni aggiuntive

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" .

Demo video per questa soluzione

Datastore iSCSI come storage supplementare per domini di gestione VCF

Aggiungere un datastore VMFS basato su FC come storage supplementare per un dominio di gestione utilizzando gli ONTAP tools for VMware vSphere

In questo caso d'uso descriviamo la procedura per utilizzare ONTAP Tools per VMware per configurare un datastore VMFS su Fibre Channel (FC) come storage supplementare per il dominio di gestione VMware Cloud Foundation (VCF). Questa procedura riassume la distribuzione di ONTAP Tools per VMware vSphere, la registrazione dei server vCenter, la definizione del backend di storage e il provisioning del datastore FC.

Vantaggi del Fibre Channel

Prestazioni elevate: FC garantisce velocità di trasferimento dati elevate, rendendolo ideale per applicazioni che richiedono un accesso rapido e affidabile a grandi quantità di dati.

Bassa latenza: Latenza molto bassa, fondamentale per le applicazioni che richiedono prestazioni elevate, come database e ambienti virtualizzati.

Affidabilità: le reti FC sono note per la loro robustezza e affidabilità, con funzionalità quali ridondanza integrata e correzione degli errori.

Larghezza di banda dedicata: FC fornisce larghezza di banda dedicata per il traffico di archiviazione, riducendo il rischio di congestione della rete.

Per ulteriori informazioni sull'utilizzo di Fibre Channel con i sistemi di storage NetApp , fare riferimento a "Provisioning SAN con FC" .

Panoramica dello scenario

Il datastore supplementare VCF viene fornito come parte delle operazioni del giorno 2 tramite vCenter. Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuzione degli strumenti ONTAP sul dominio di gestione
- Registra i server vCenter del carico di lavoro VI negli strumenti ONTAP
- Definisci il backend di archiviazione sul plugin degli strumenti ONTAP per VMware vSphere
- Fornire VMFS sul trasporto FC

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP con porte FC collegate a switch FC.
- SVM creato con FC lifs.
- vSphere con HBA FC collegati agli switch FC.
- Sugli switch FC è configurata la suddivisione in zone con singolo iniziatore-destinazione.

> Utilizzare l'interfaccia logica FC SVM nella configurazione della zona anziché le porte FC fisiche sui sistemi ONTAP .

NetApp consiglia il multipath per le LUN FC.

Per informazioni complete sulla configurazione del canale in fibra sui sistemi di archiviazione ONTAP , fare riferimento a "Gestione dello storage SAN" nella documentazione ONTAP 9.

Per ulteriori informazioni sull'utilizzo di VMFS con sistemi di archiviazione ONTAP , fare riferimento a"Guida alla distribuzione per VMFS" .

Fasi di distribuzione per il dominio di gestione

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

- "Distribuire gli strumenti ONTAP sul dominio di gestione"
- "Definisci il backend di archiviazione utilizzando l'interfaccia client vSphere"
- "Provisioning VMFS su FC"

Informazioni aggiuntive

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" .

Demo video per questa soluzione

Datastore VMFS(FC) come storage supplementare per il dominio di gestione VCF

Aggiungere vVols come storage supplementare ai domini dei carichi di lavoro VI utilizzando gli ONTAP tools for VMware vSphere

In questo caso d'uso descriviamo la procedura per configurare un datastore vVols con iSCSI per l'archiviazione supplementare in un dominio di carico di lavoro di un'infrastruttura virtuale (VI) VMware Cloud Foundation (VCF). Questa procedura riassume la configurazione della rete iSCSI, l'implementazione di ONTAP Tools per VMware vSphere e il provisioning del datastore vVols .

iSCSI viene utilizzato come protocollo di archiviazione per il datastore vVols .

Vantaggi di iSCSI

Prestazioni elevate: offre prestazioni elevate per garantire velocità di trasferimento dati rapide ed efficienti e bassa latenza. Ideale per applicazioni aziendali esigenti e ambienti virtualizzati.

Facilità di gestione: semplifica la gestione dell'archiviazione utilizzando strumenti e protocolli basati su IP noti.

Conveniente: utilizza l'infrastruttura Ethernet esistente, riducendo la necessità di hardware specializzato e consentendo alle organizzazioni di ottenere soluzioni di archiviazione affidabili e scalabili.

Per ulteriori informazioni sull'utilizzo di iSCSI con i sistemi di storage NetApp , fare riferimento a "Provisioning SAN con iSCSI" .

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

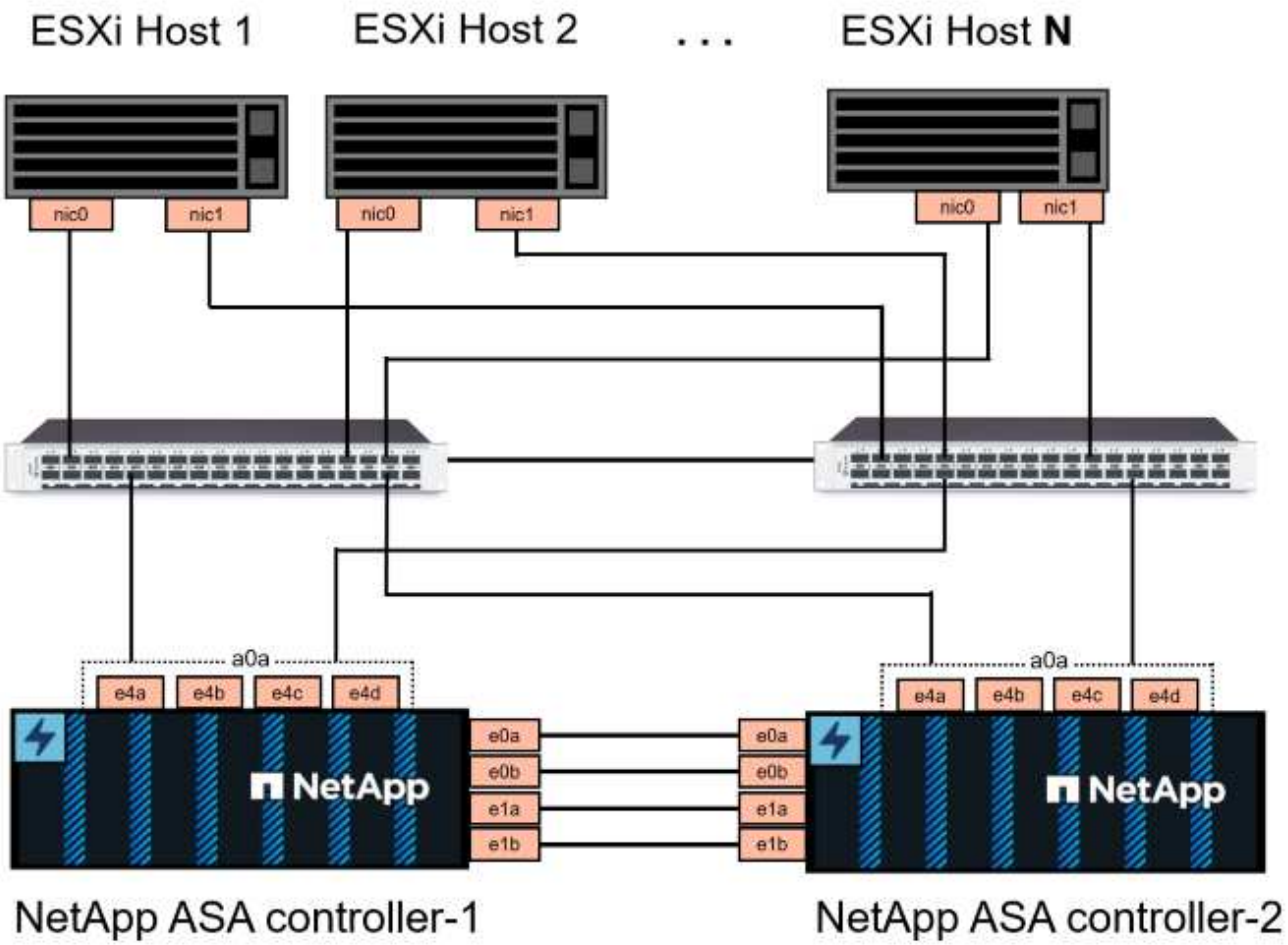
- Creare una macchina virtuale di archiviazione (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuiti per reti iSCSI sul dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Distribuire gli strumenti ONTAP sul dominio del carico di lavoro VI.
- Creare un nuovo datastore vVols sul dominio del carico di lavoro VI.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o ASA con porte dati fisiche su switch Ethernet dedicate al traffico di archiviazione.
- La distribuzione del dominio di gestione VCF è completa e il client vSphere è accessibile.
- In precedenza è stato distribuito un dominio di carico di lavoro VI.

NetApp consiglia progetti di rete completamente ridondanti per iSCSI. Il diagramma seguente illustra un esempio di configurazione ridondante, che garantisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. Fare riferimento a NetApp"Riferimento alla configurazione SAN" per ulteriori informazioni.



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

Questa documentazione illustra il processo di creazione di una nuova SVM e di specifica delle informazioni sull'indirizzo IP per creare più LIF per il traffico iSCSI. Per aggiungere nuovi LIF a un SVM esistente, fare riferimento a"Creare un LIF (interfaccia di rete)" .

> Nei casi in cui più adattatori VMkernel sono configurati sulla stessa rete IP, si consiglia di utilizzare il binding delle porte iSCSI software sugli host ESXi per garantire il bilanciamento del carico tra gli adattatori. Fare riferimento all'articolo della Knowledge Base"Considerazioni sull'utilizzo del binding delle porte iSCSI software in ESX/ESXi (2038869)" .

Per ulteriori informazioni sull'utilizzo di datastore iSCSI VMFS con VMware, fare riferimento a"vSphere VMFS Datastore - Backend di archiviazione iSCSI con ONTAP" .

Fasi di distribuzione

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

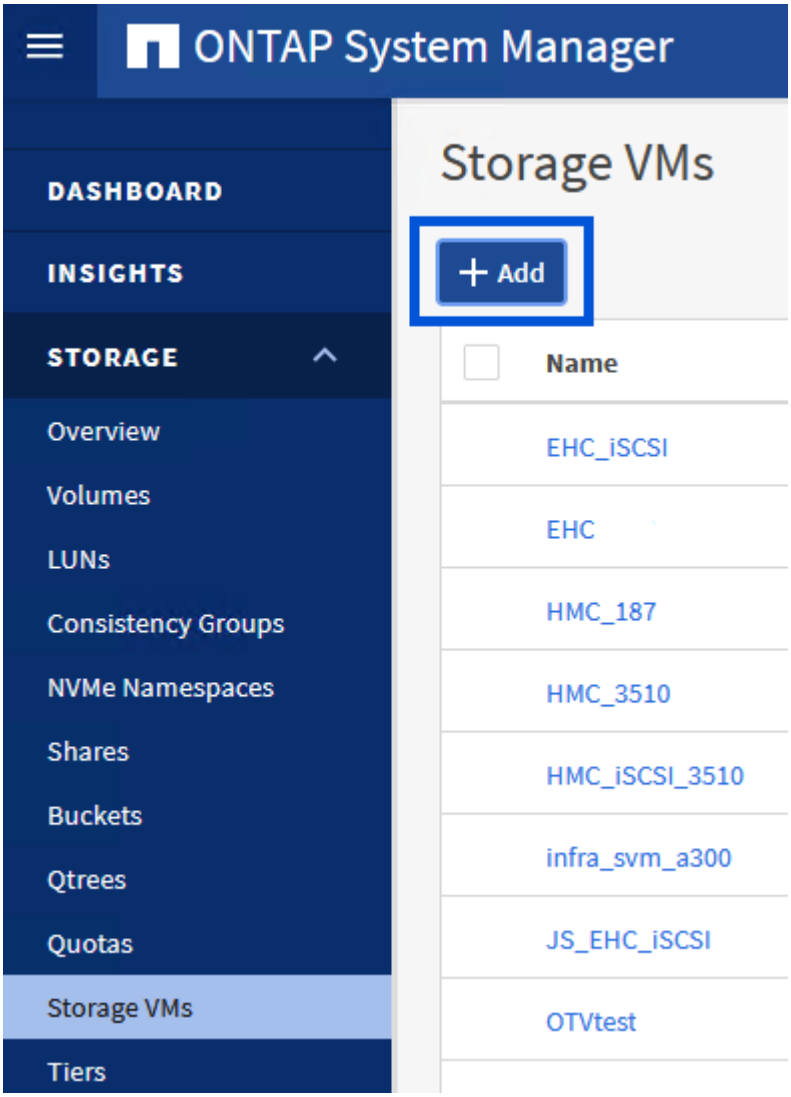
Creare SVM e LIF sul sistema di archiviazione ONTAP

Il passaggio seguente viene eseguito in ONTAP System Manager.

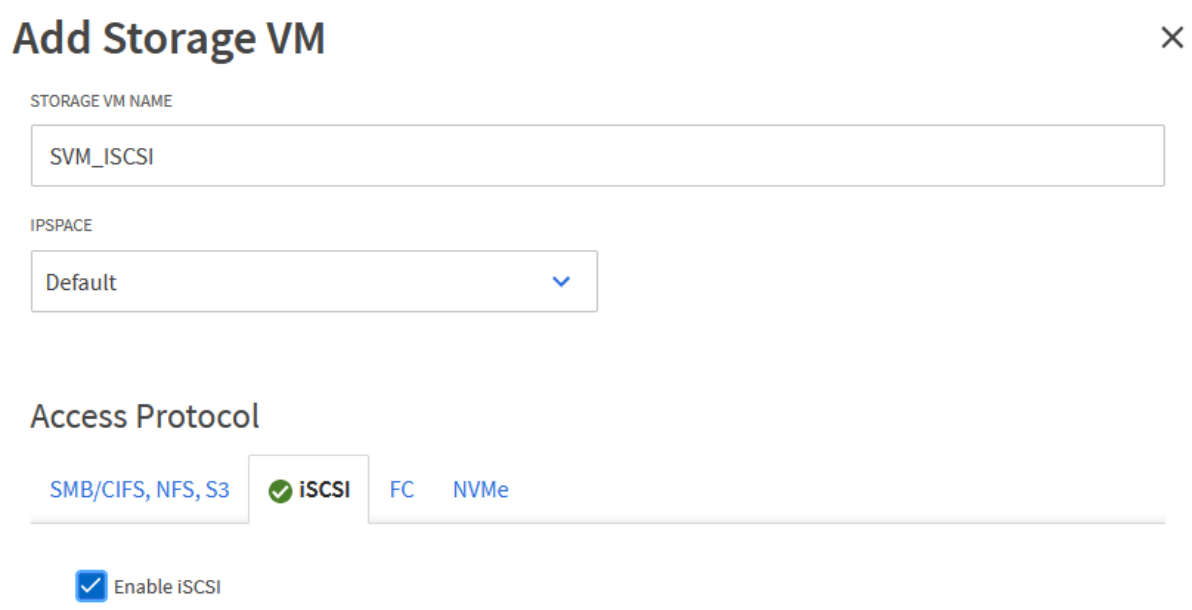
Creare la VM di archiviazione e i LIF

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

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

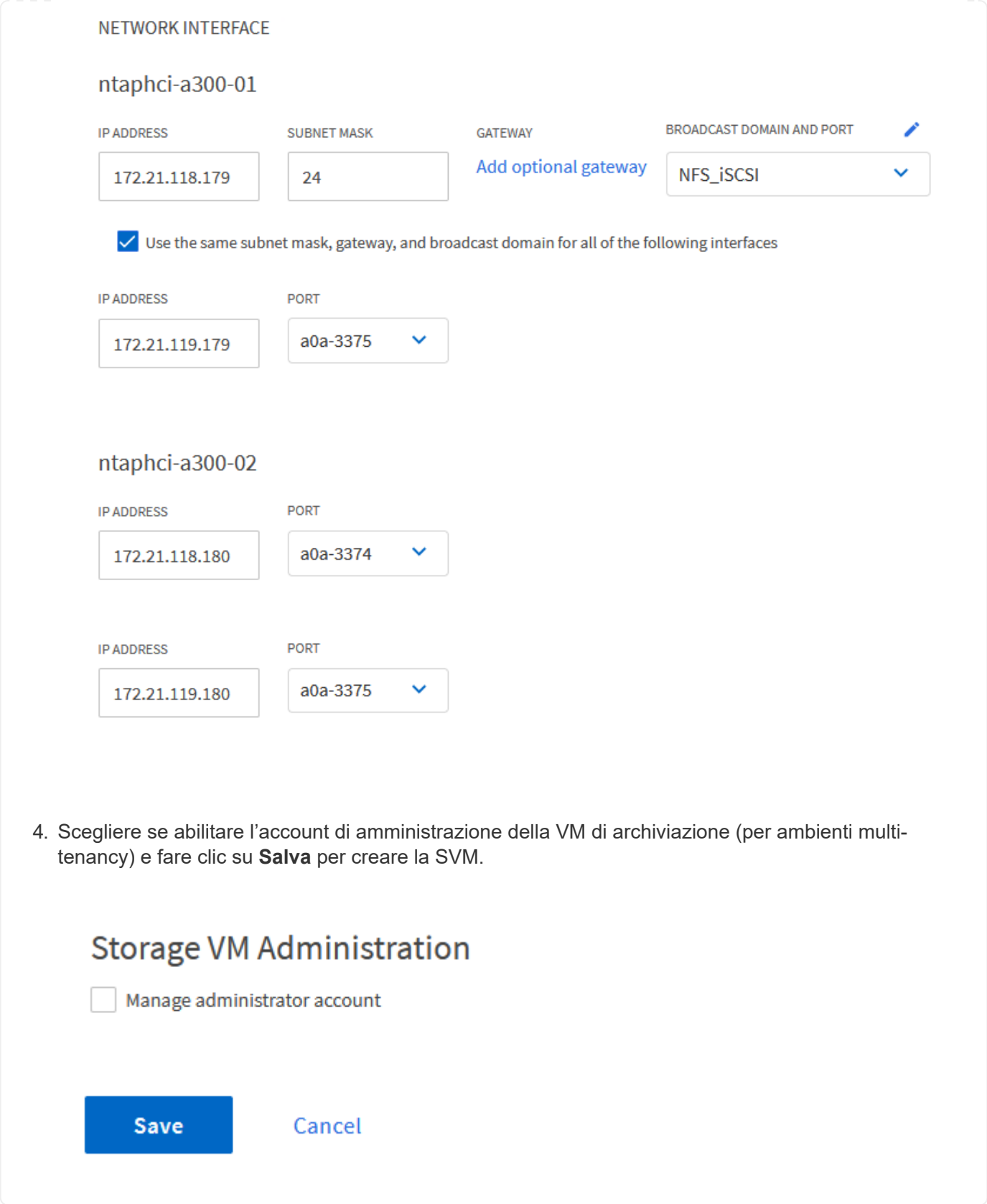


2. Nella procedura guidata **Aggiungi VM di archiviazione**, fornire un **Nome** per la SVM, selezionare lo **Spazio IP** e quindi, in **Protocollo di accesso**, fare clic sulla scheda **iSCSI** e selezionare la casella per **Abilitare iSCSI**.



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.

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



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.

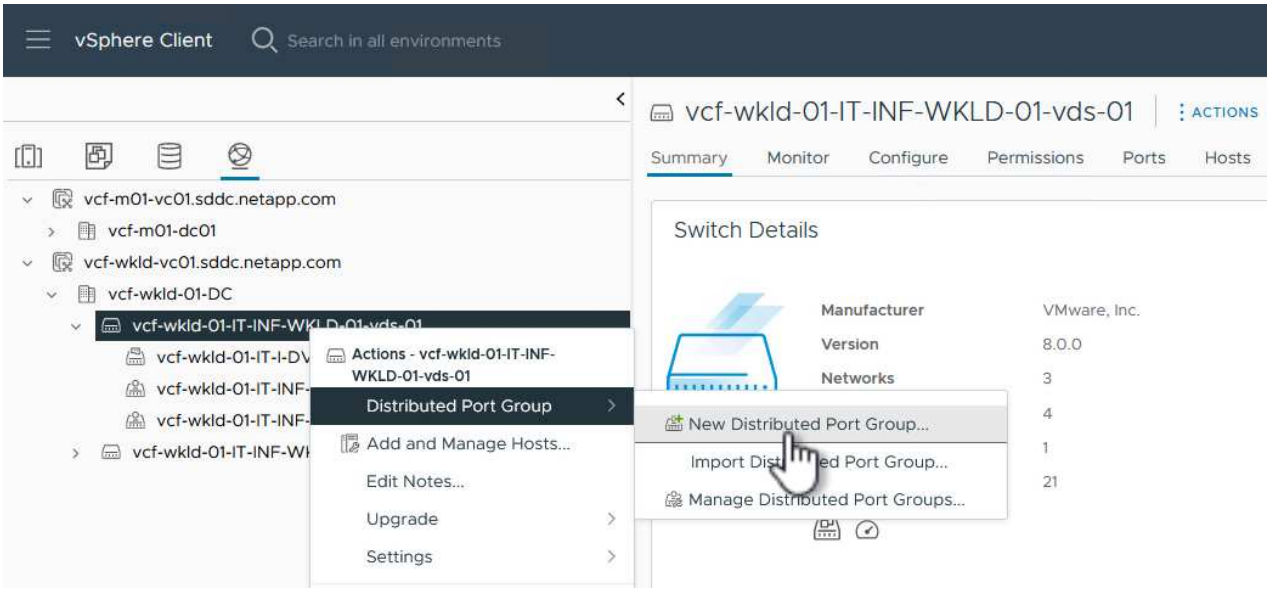
Configurazione della rete per iSCSI su host ESXi

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.

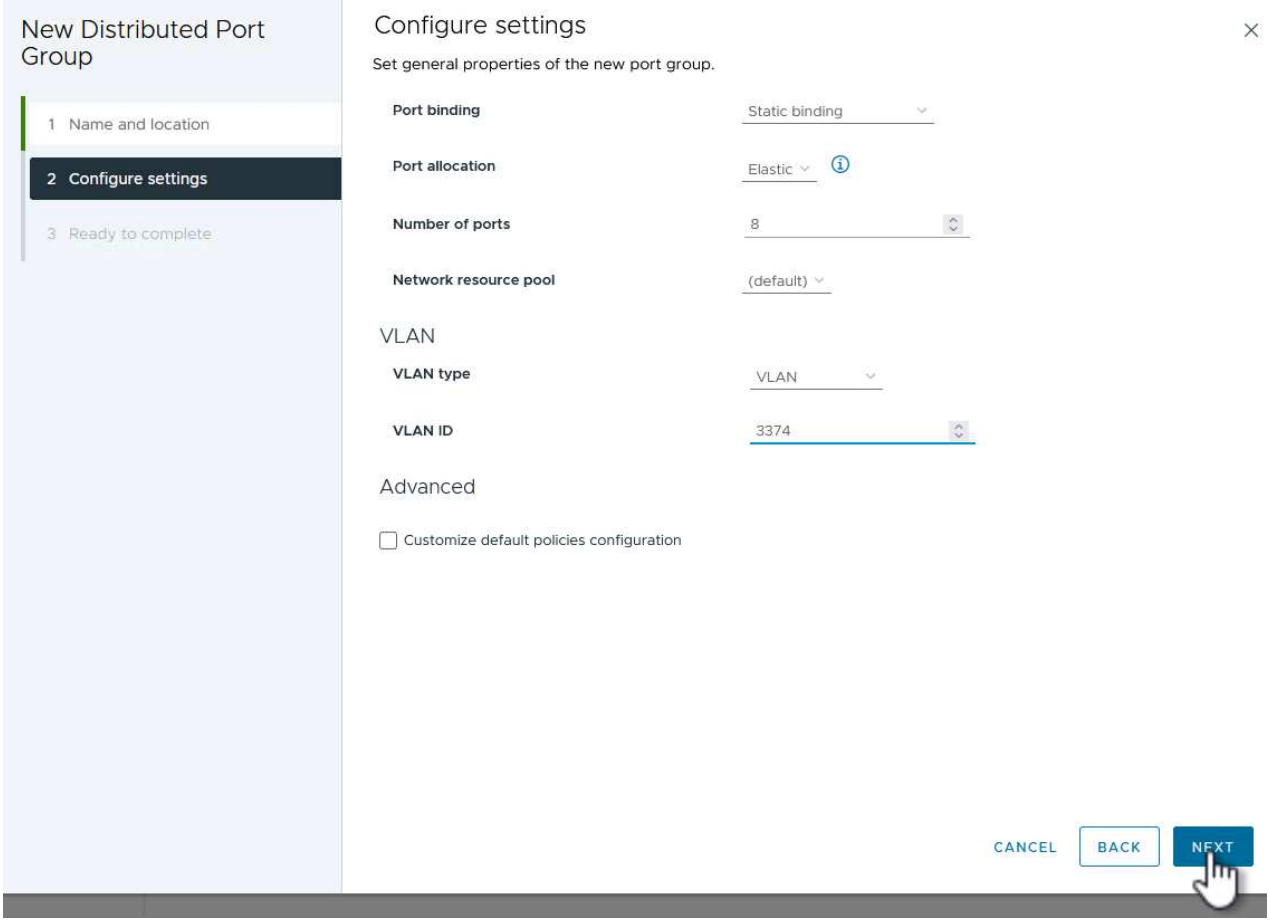
Creare gruppi di porte distribuiti per il traffico iSCSI

Completare la seguente procedura per creare un nuovo gruppo di porte distribuito per ogni rete iSCSI:

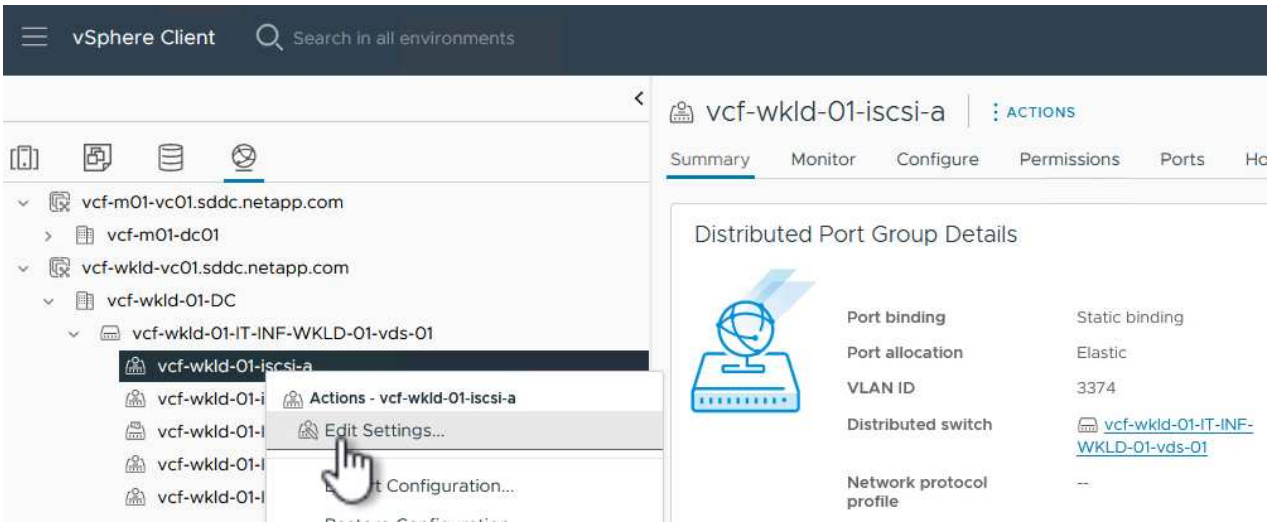
1. Dal client vSphere, accedere a **Inventario > Rete** per il dominio del carico di lavoro. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite…**.



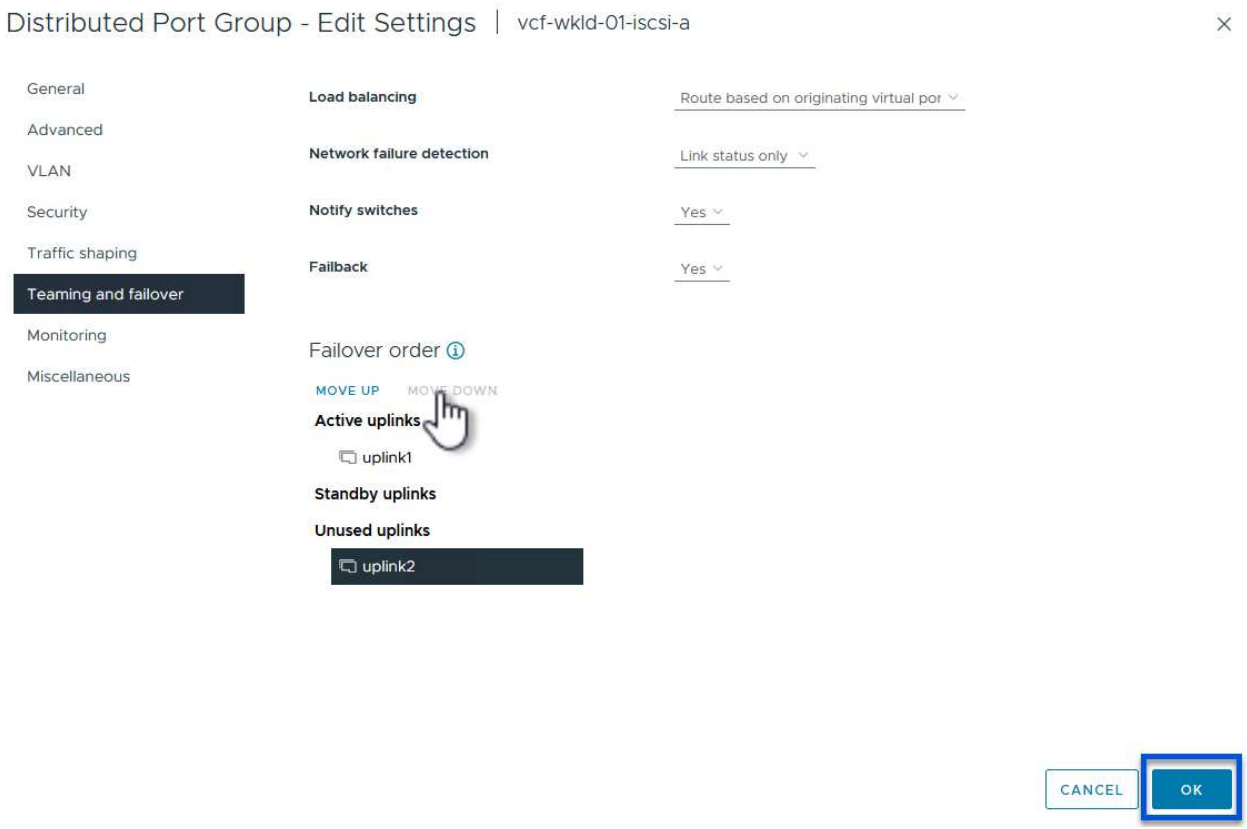
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, immettere un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare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



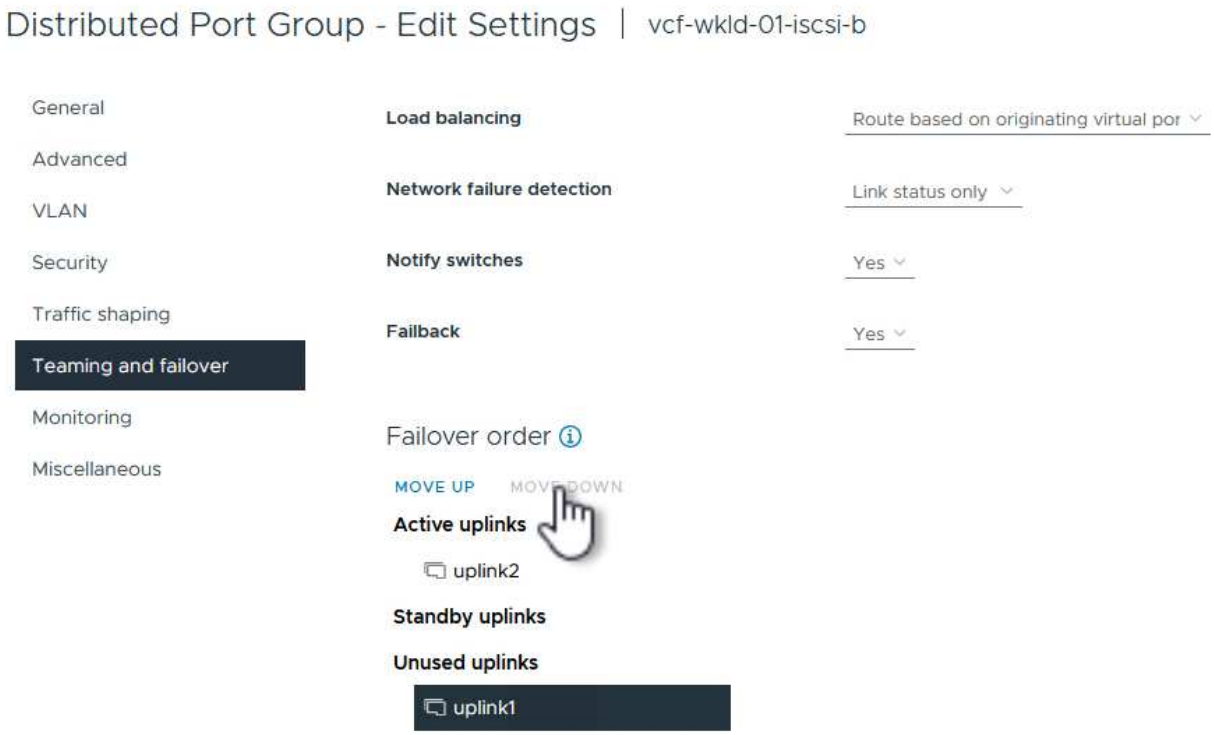
4. Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **Fine** per creare il nuovo gruppo di porte distribuite.
5. Ripetere questa procedura per creare un gruppo di porte distribuito per la seconda rete iSCSI utilizzata e assicurarsi di aver immesso l'**ID VLAN** corretto.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



7. Nella pagina **Gruppo di porte distribuite - Modifica impostazioni**, vai su **Teaming e failover** nel menu a sinistra e fai clic su **uplink2** per spostarlo in basso a **Uplink non utilizzati**.



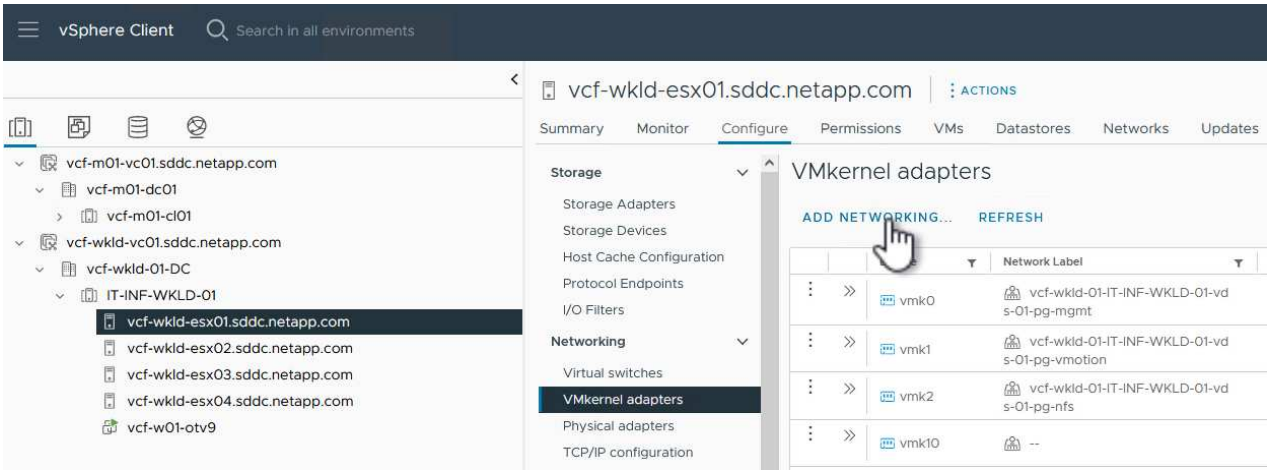
8. Ripetere questo passaggio per il secondo gruppo di porte iSCSI. Questa volta, però, sposta **uplink1** in **Uplink non utilizzati**.



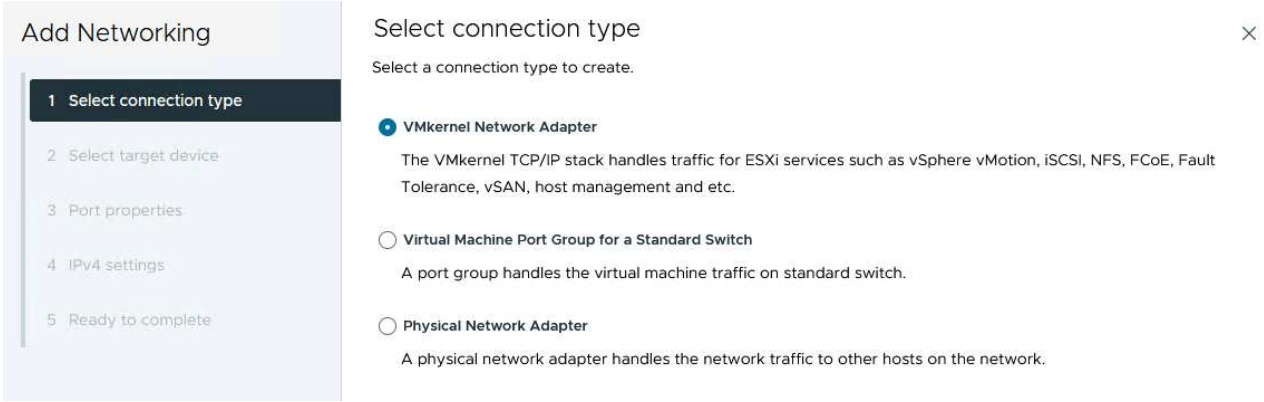
Creare adattatori VMkernel su ciascun host ESXi

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

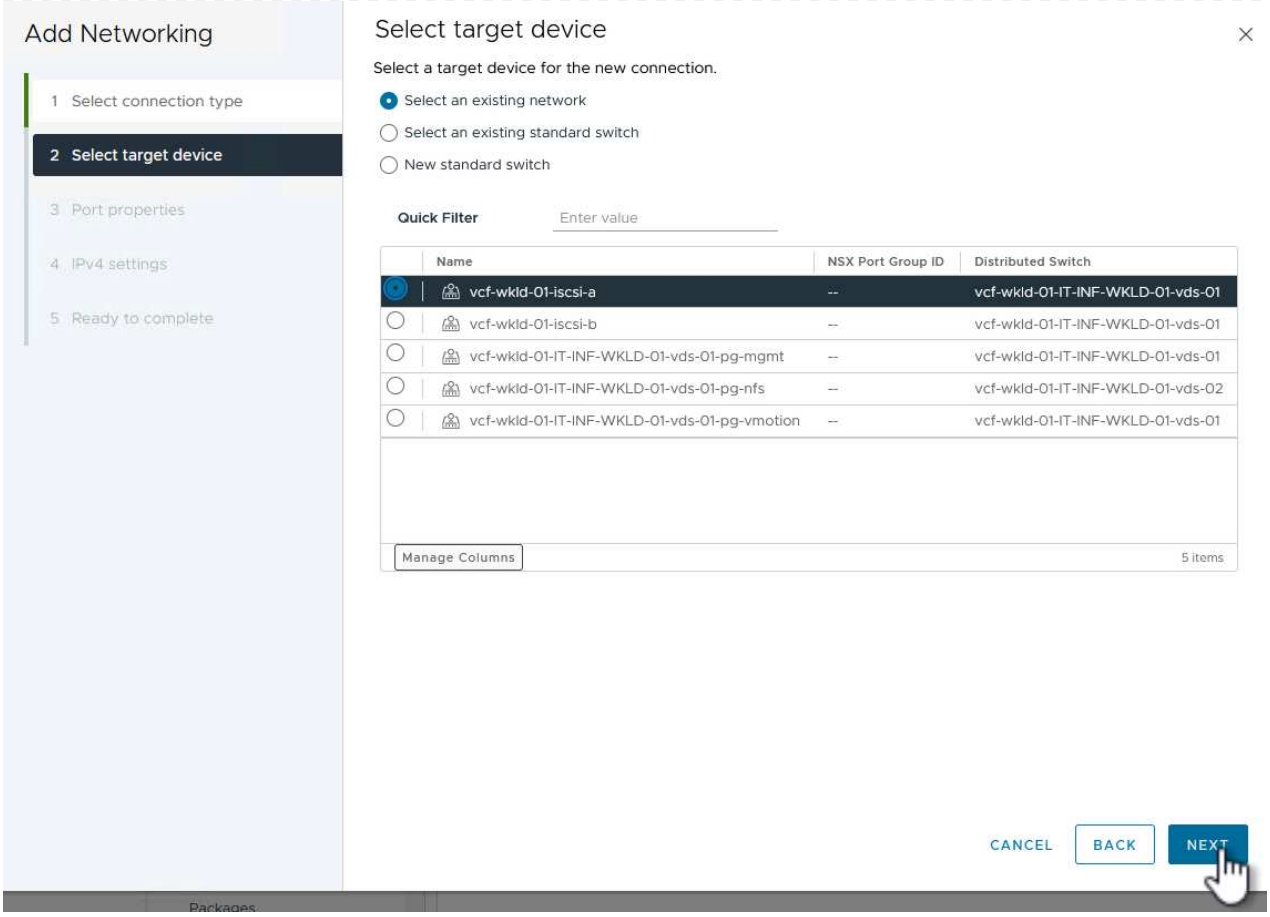
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configura** seleziona **Schede VMkernel** e clicca su **Aggiungi rete…** per iniziare.



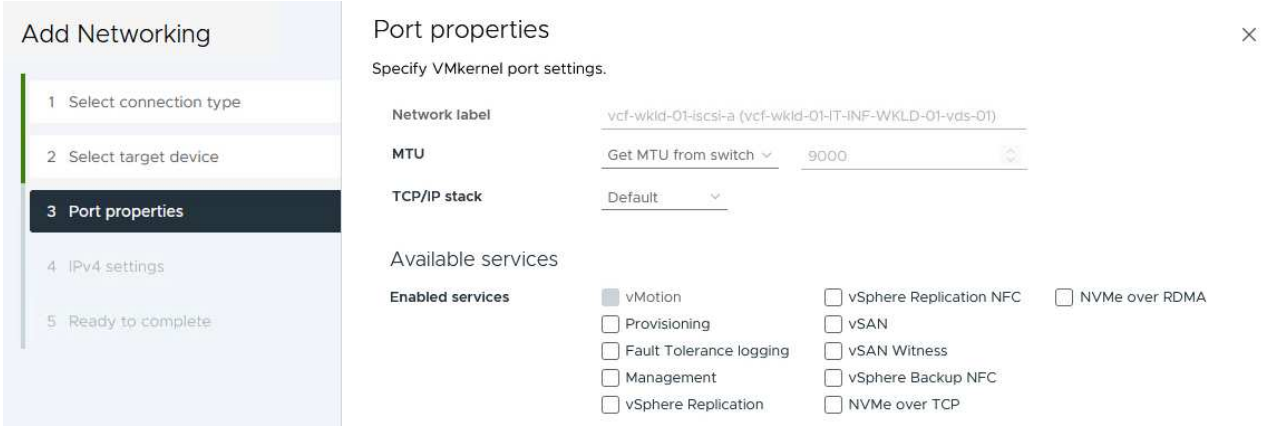
2. Nella finestra **Seleziona tipo di connessione** seleziona **Scheda di rete VMkernel** e fai clic su **Avanti** per continuare.



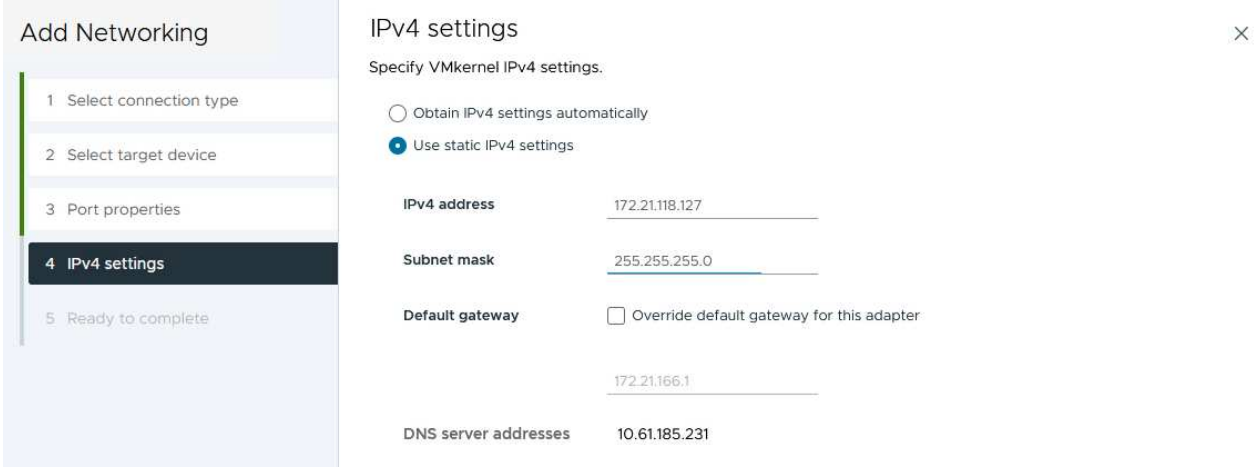
3. Nella pagina **Seleziona dispositivo di destinazione**, seleziona uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



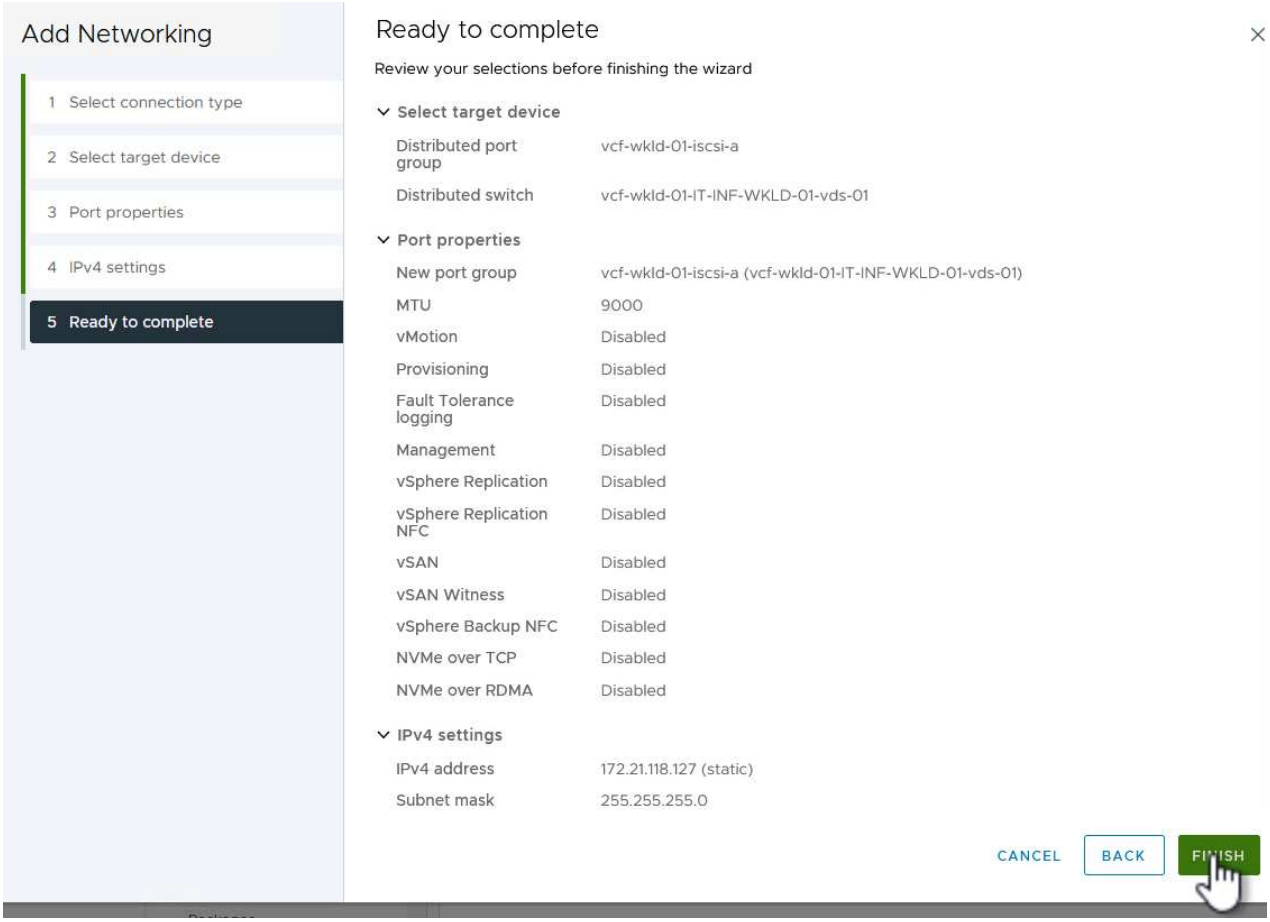
4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e fare clic su **Avanti** per continuare.



5. Nella pagina **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.



7. Ripetere questo processo per creare un adattatore VMkernel per la seconda rete iSCSI.

Distribuisci e usa gli strumenti ONTAP per configurare l'archiviazione

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

Per i domini del carico di lavoro VI, ONTAP Tools è installato nel VCF Management Cluster ma registrato con il vCenter associato al dominio del carico di lavoro VI.

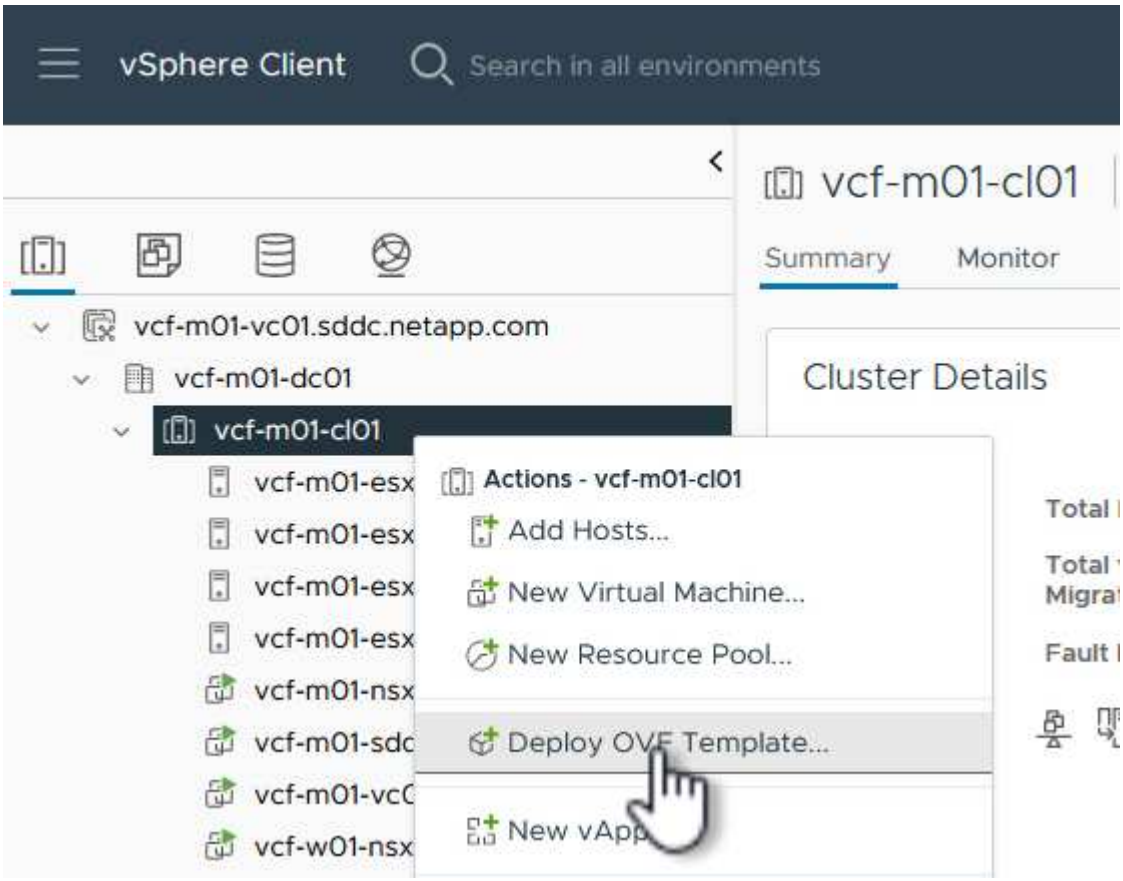
Per ulteriori informazioni sulla distribuzione e l'utilizzo di ONTAP Tools in un ambiente vCenter multiplo, fare riferimento a"Requisiti per la registrazione degli strumenti ONTAP in un ambiente con più vCenter Server" .

Distribuisci gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere vengono distribuiti come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP .

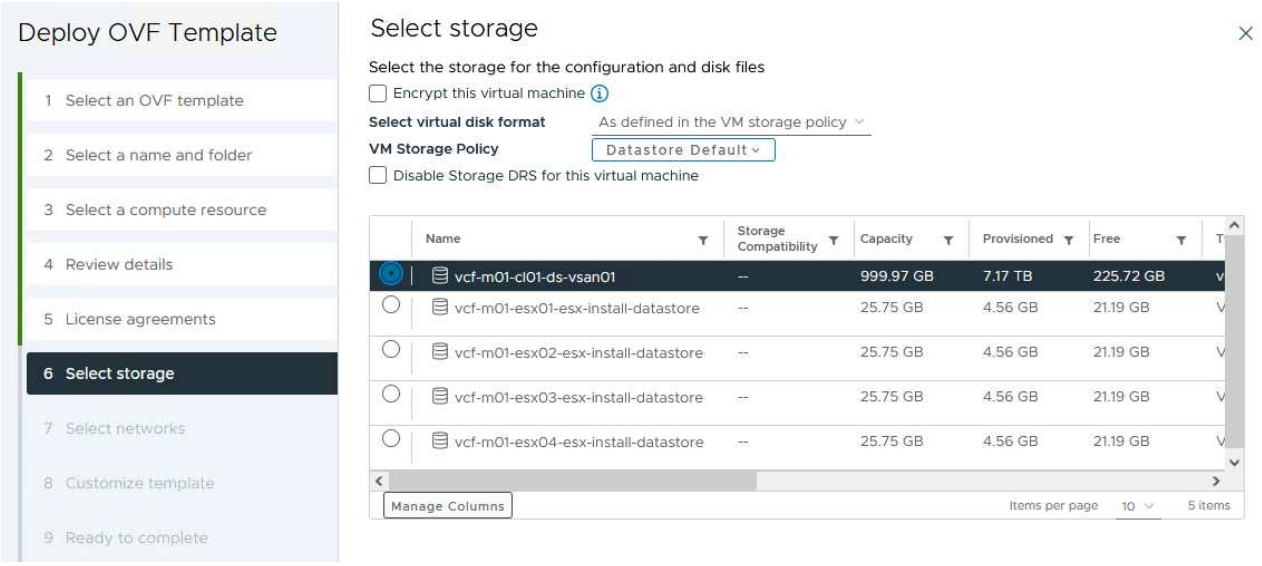
Completare quanto segue per distribuire gli ONTAP tools for VMware vSphere:

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 dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Distribuisci modello OVF…**

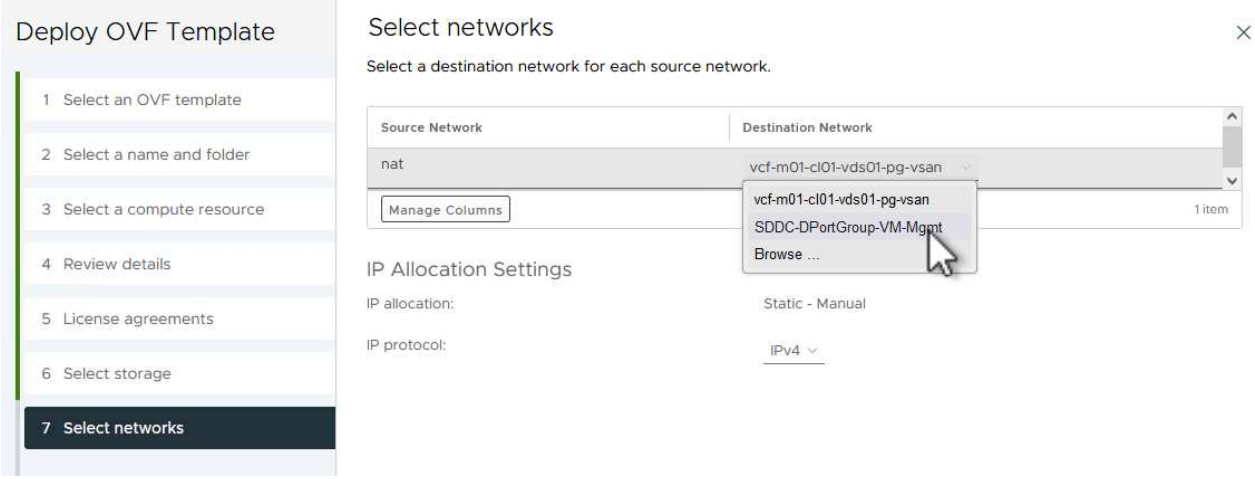


4. Nella procedura guidata **Distribuisci modello OVF**, fare clic sul pulsante di opzione **File locale** e selezionare il file OVA degli strumenti ONTAP scaricato nel passaggio precedente.

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 il datastore vSAN del cluster del dominio di gestione VCF.

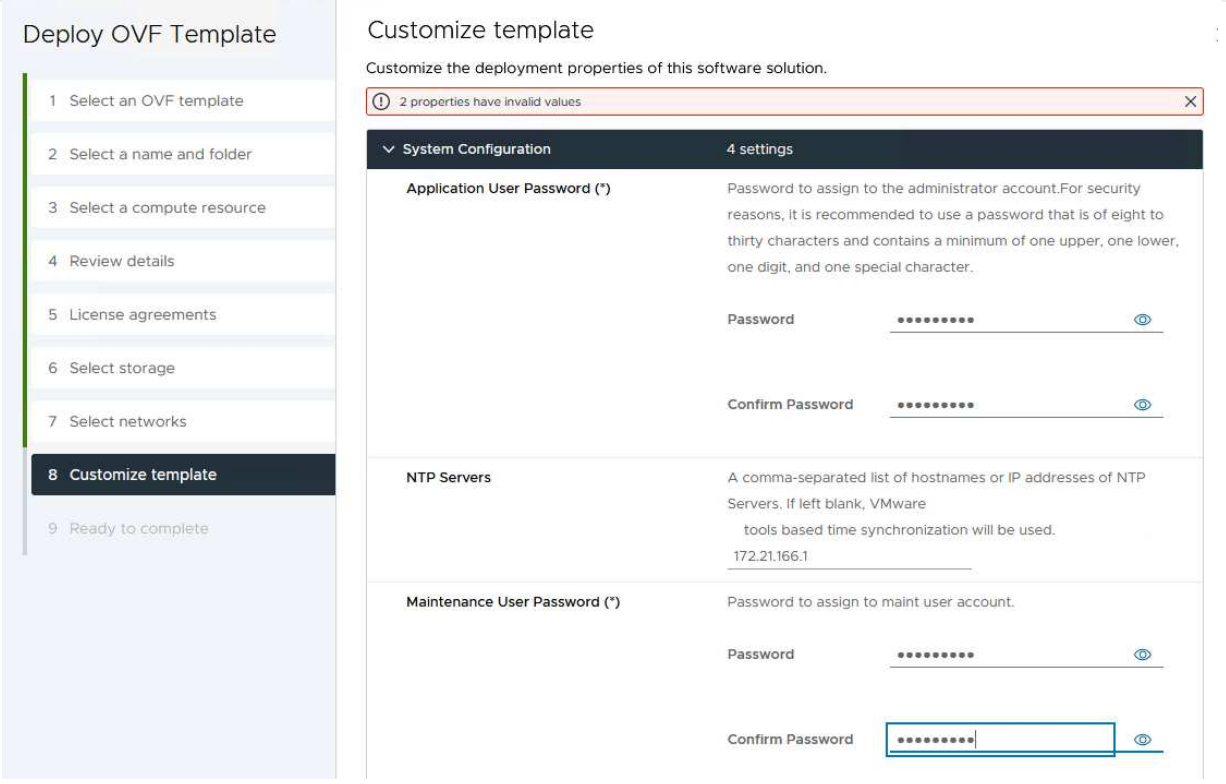


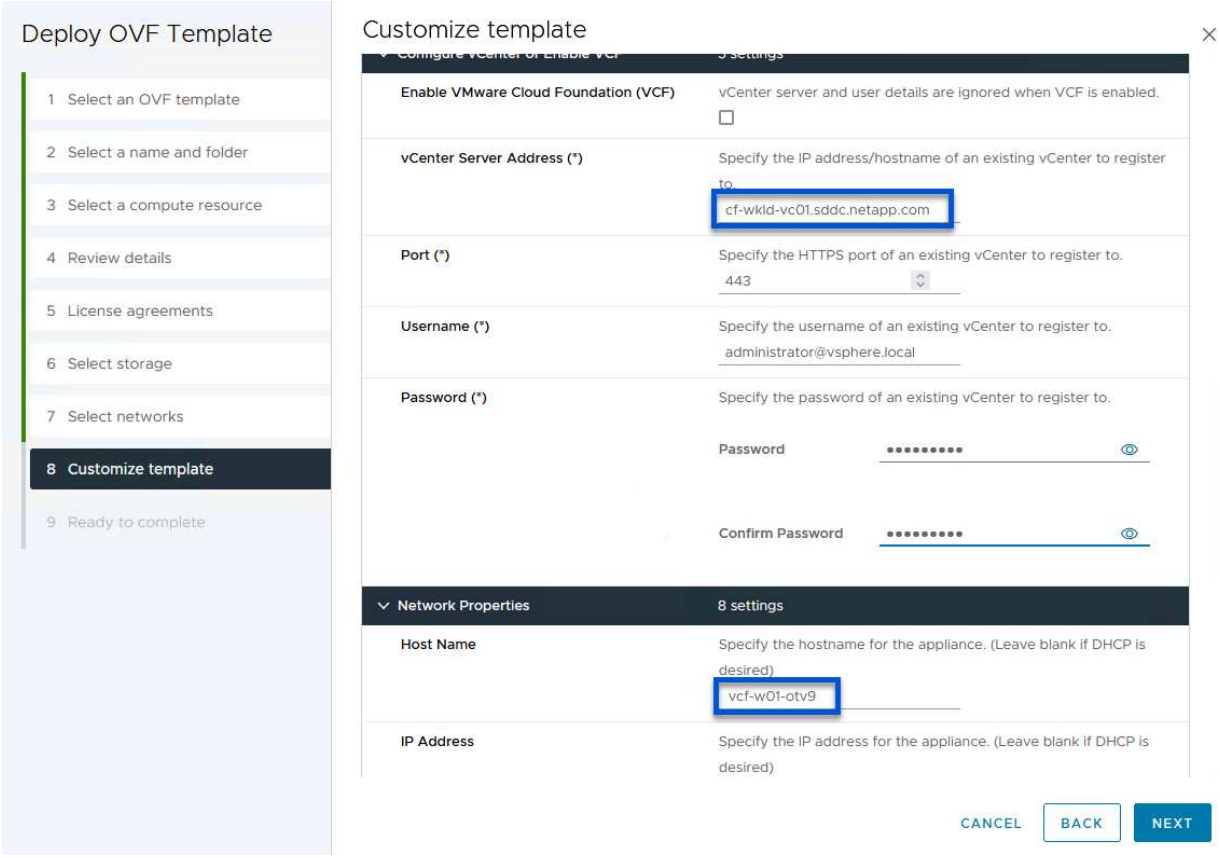
7. Nella pagina Seleziona rete seleziona la rete utilizzata per la gestione del traffico.



8. Nella pagina Personalizza modello compila tutte le informazioni richieste:
   - Password da utilizzare per l'accesso amministrativo a ONTAP Tools.
   - Indirizzo IP del server NTP.
   - Password dell'account di manutenzione degli strumenti ONTAP .
   - Password del database Derby ONTAP Tools.
   - Non selezionare la casella per **Abilitare VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire storage supplementare.
   - FQDN o indirizzo IP dell'appliance vCenter per il **dominio del carico di lavoro VI**
   - Credenziali per l'appliance vCenter del **VI Workload Domain**
   - Fornire i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.

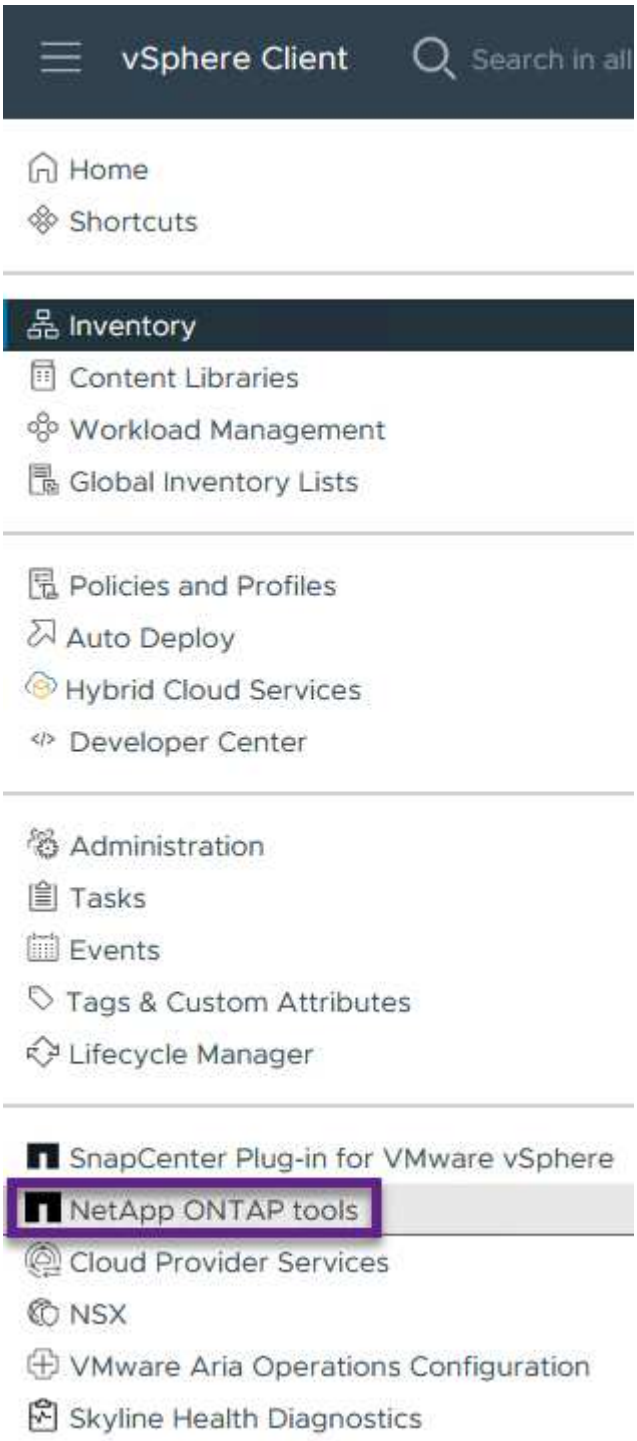




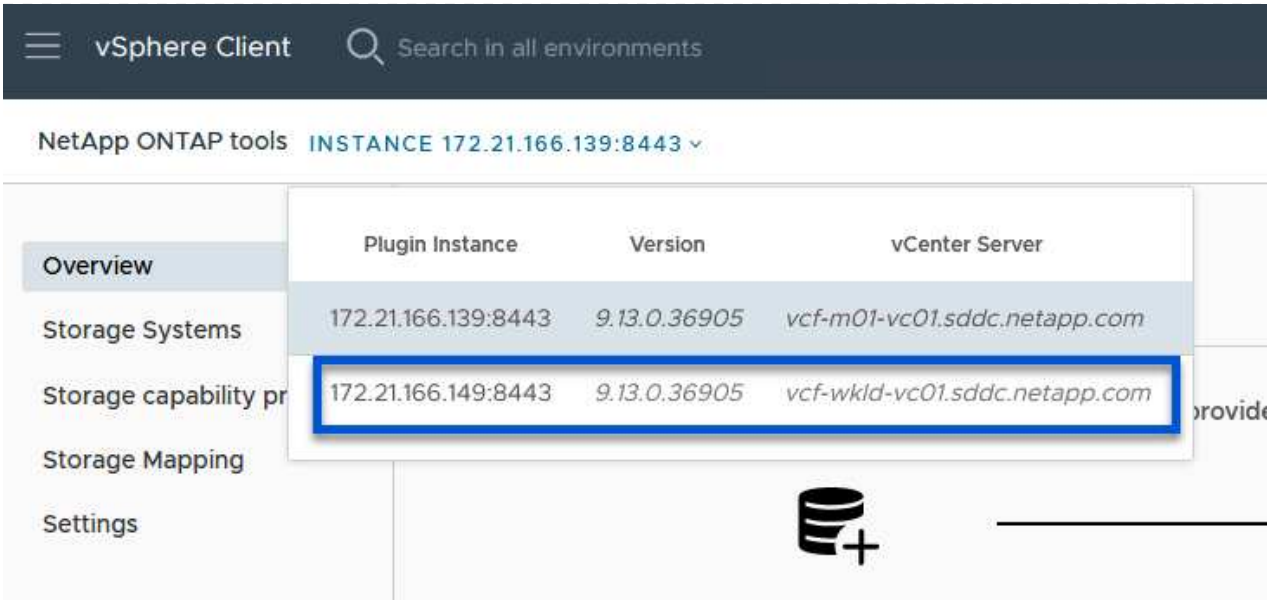
9. Esaminare tutte le informazioni nella pagina Pronto per il completamento e fare clic su Fine per iniziare a distribuire l'appliance ONTAP Tools.

Aggiungere un sistema di archiviazione a ONTAP Tools.

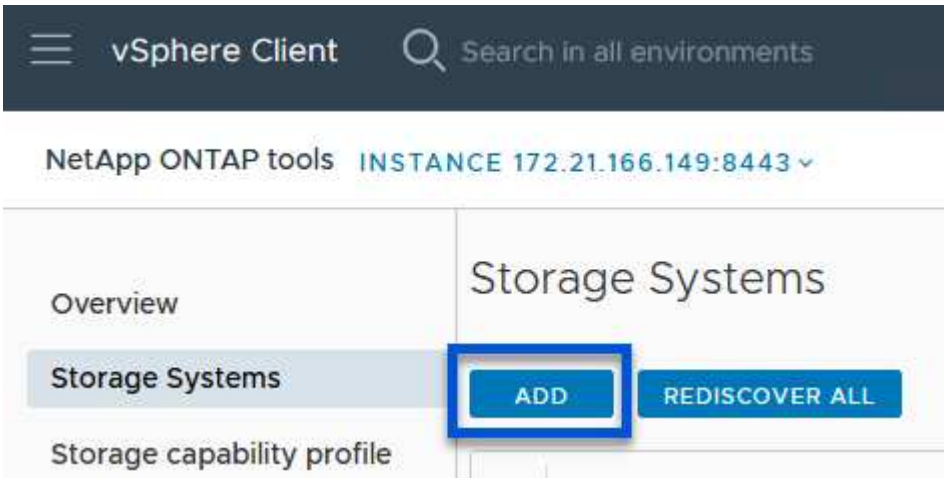
1. Accedi a NetApp ONTAP Tools selezionandolo dal menu principale nel client vSphere.



2. Dal menu a discesa **ISTANZA** nell'interfaccia dello strumento ONTAP , selezionare l'istanza dello strumento ONTAP associata al dominio del carico di lavoro da gestire.

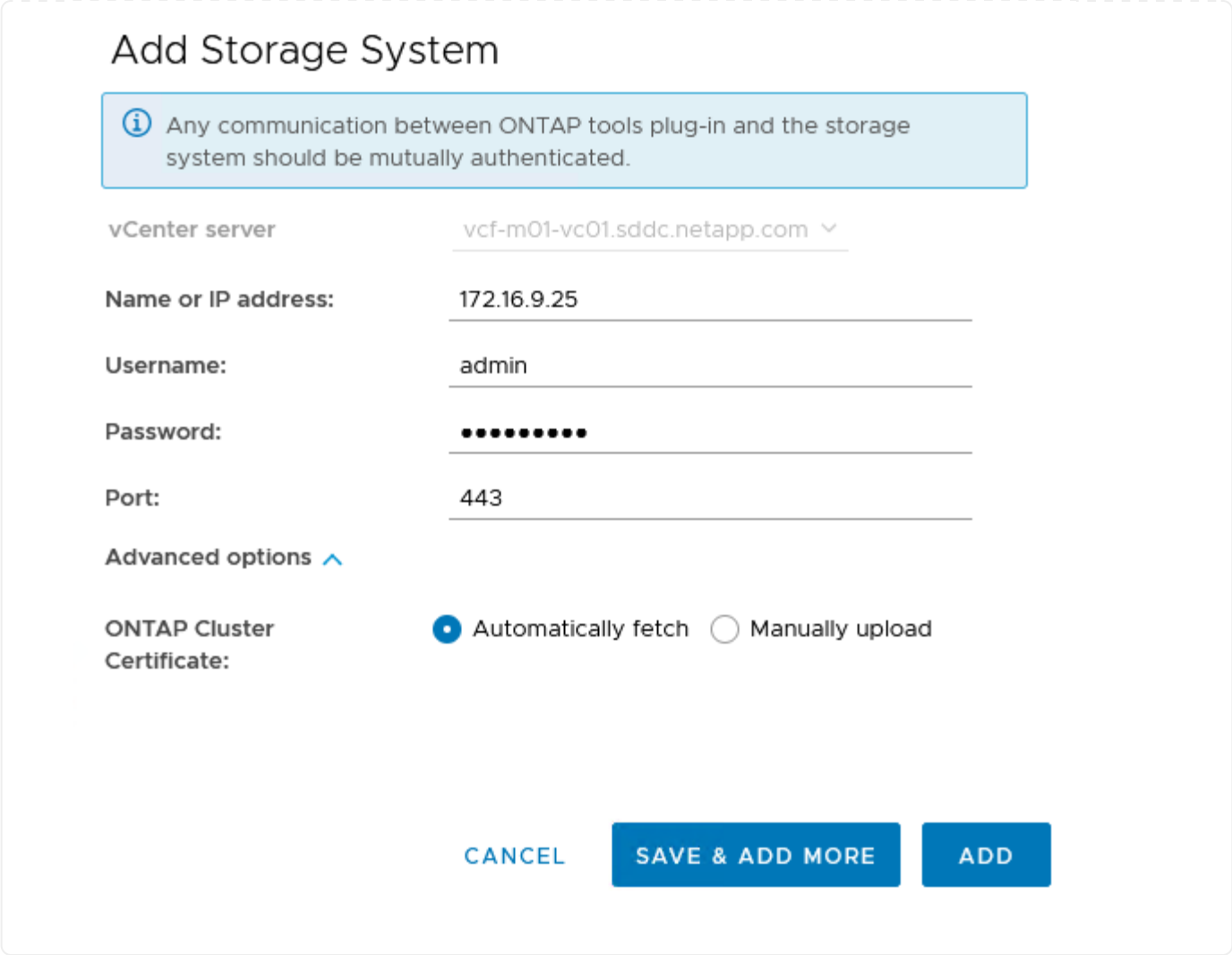


3. In ONTAP Tools seleziona **Storage Systems** dal menu a sinistra e poi premi **Aggiungi**.



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

> vVol richiede le credenziali del cluster ONTAP anziché le credenziali SVM. Per maggiori informazioni fare riferimento a "Aggiungere sistemi di archiviazione" Nella documentazione degli strumenti ONTAP .

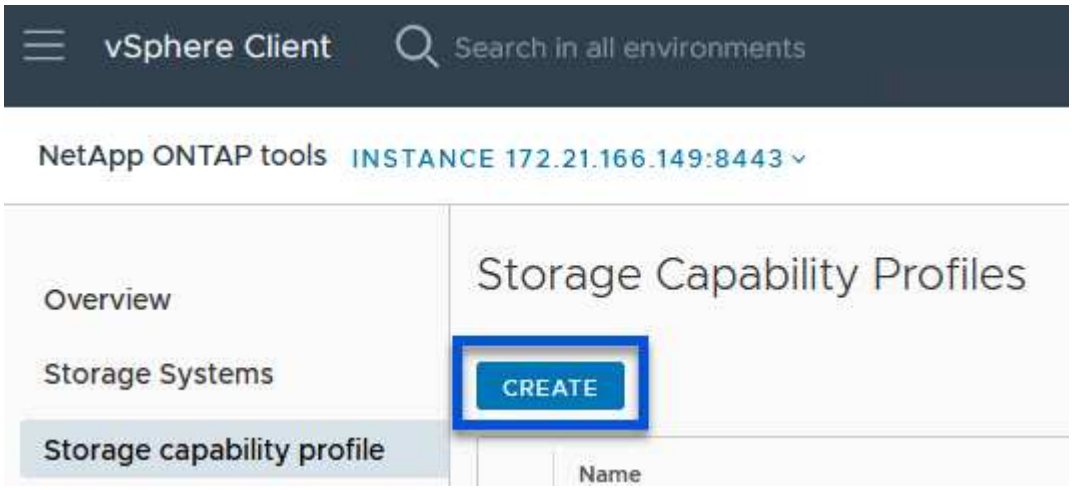

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Creare un profilo di capacità di archiviazione in ONTAP Tools

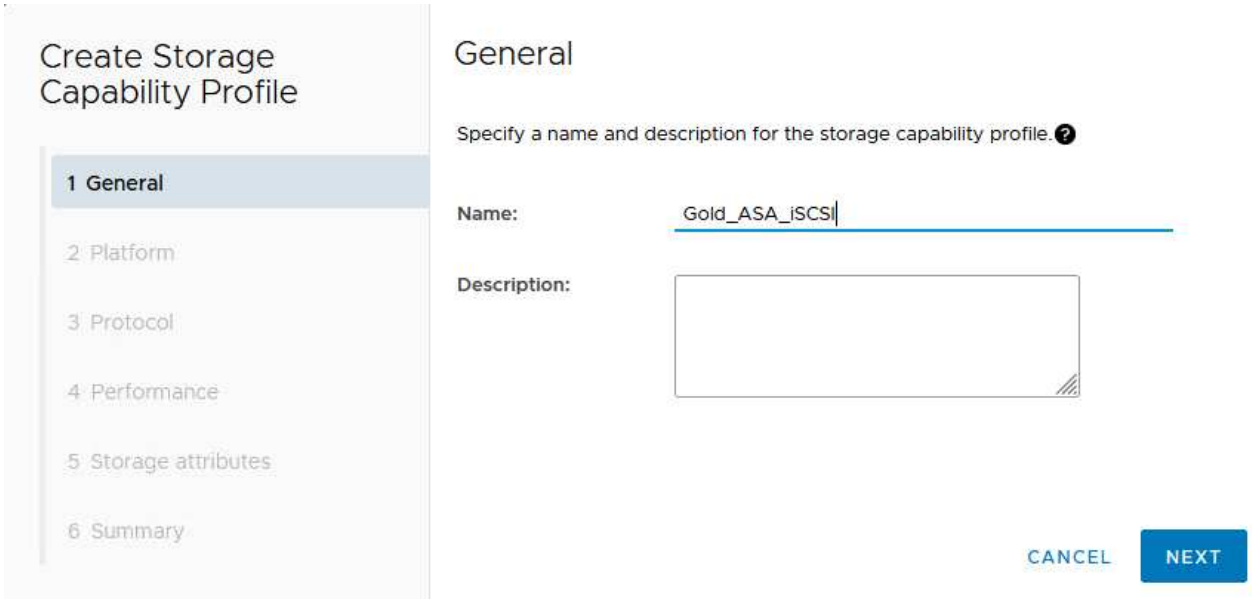
I profili di capacità di archiviazione descrivono le funzionalità fornite da un array di archiviazione o da un sistema di archiviazione. Includono definizioni di qualità del servizio e vengono utilizzate per selezionare i sistemi di archiviazione che soddisfano i parametri definiti nel profilo. È possibile utilizzare uno dei profili forniti oppure crearne di nuovi.

Per creare un profilo di capacità di archiviazione in ONTAP Tools, completare i seguenti passaggi:

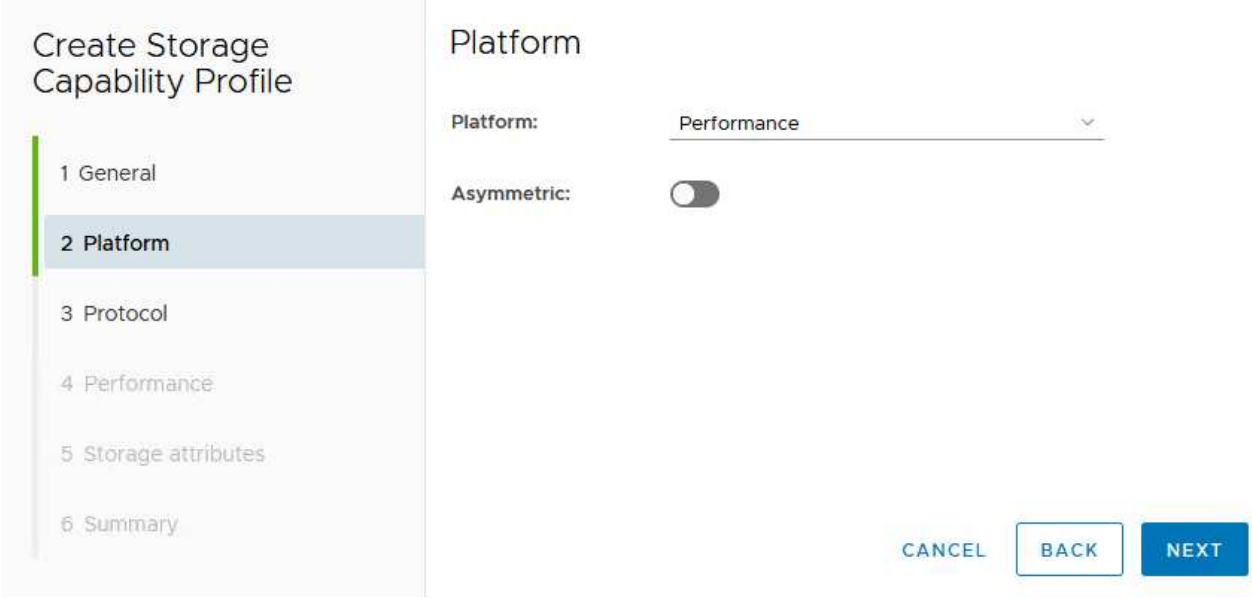
1. In ONTAP Tools seleziona **Profilo capacità di archiviazione** dal menu a sinistra e poi premi **Crea**.



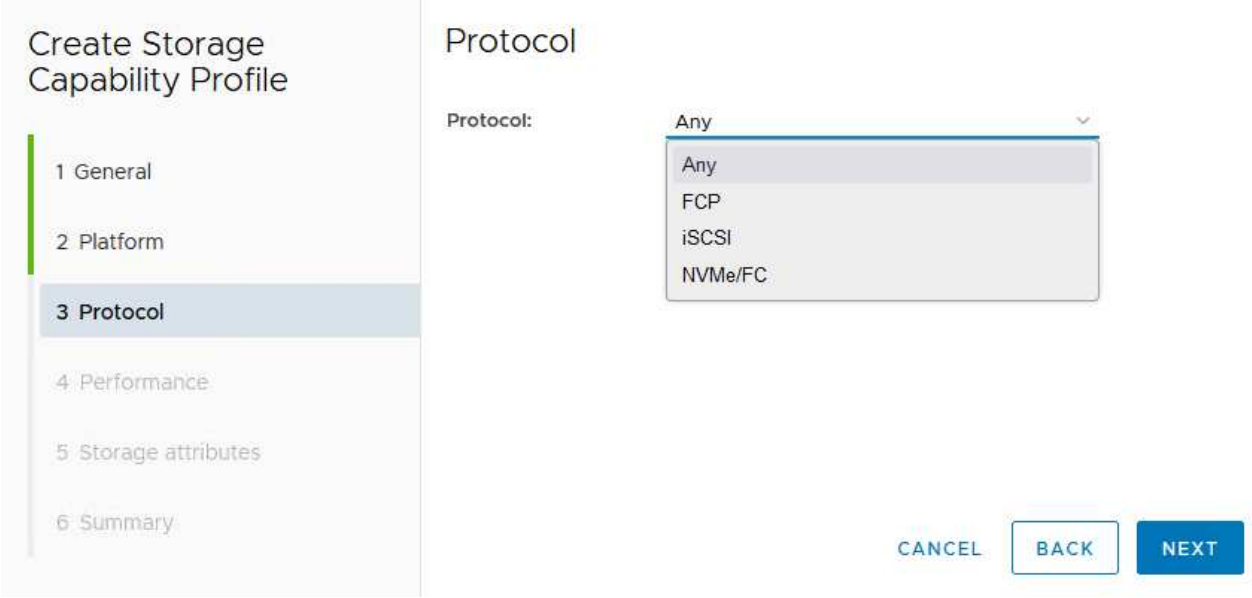
2. Nella procedura guidata **Crea profilo di capacità di archiviazione**, immettere un nome e una descrizione del profilo e fare clic su **Avanti**.



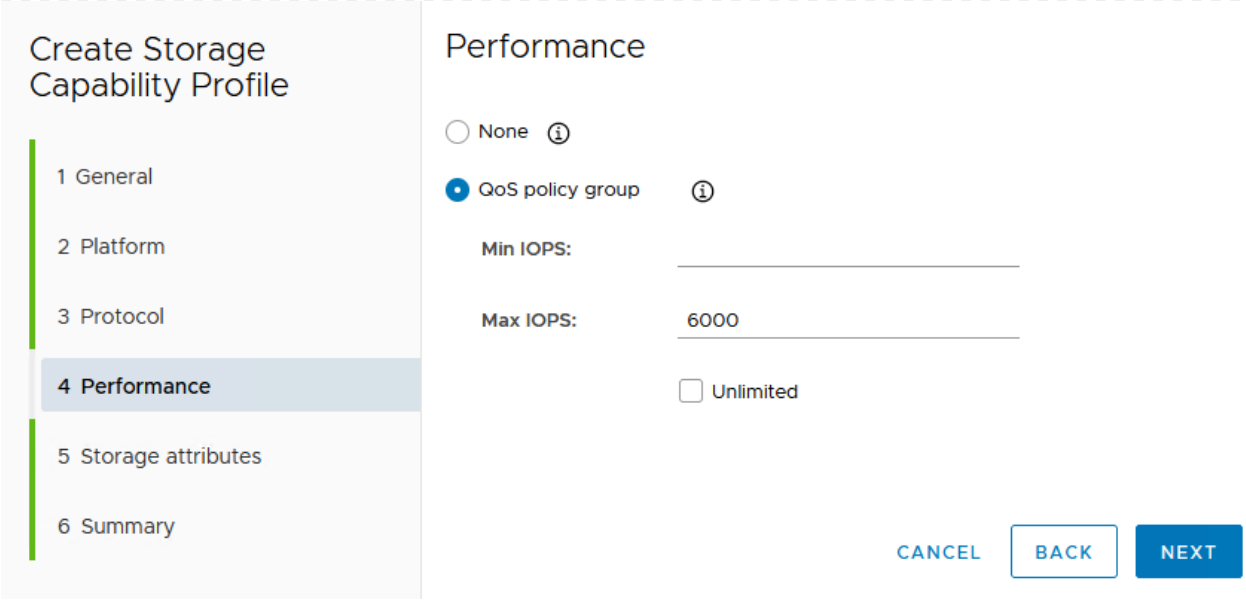
3. Selezionare il tipo di piattaforma e specificare che il sistema di archiviazione deve essere un array SAN All-Flash, impostare **Asymmetric** su false.



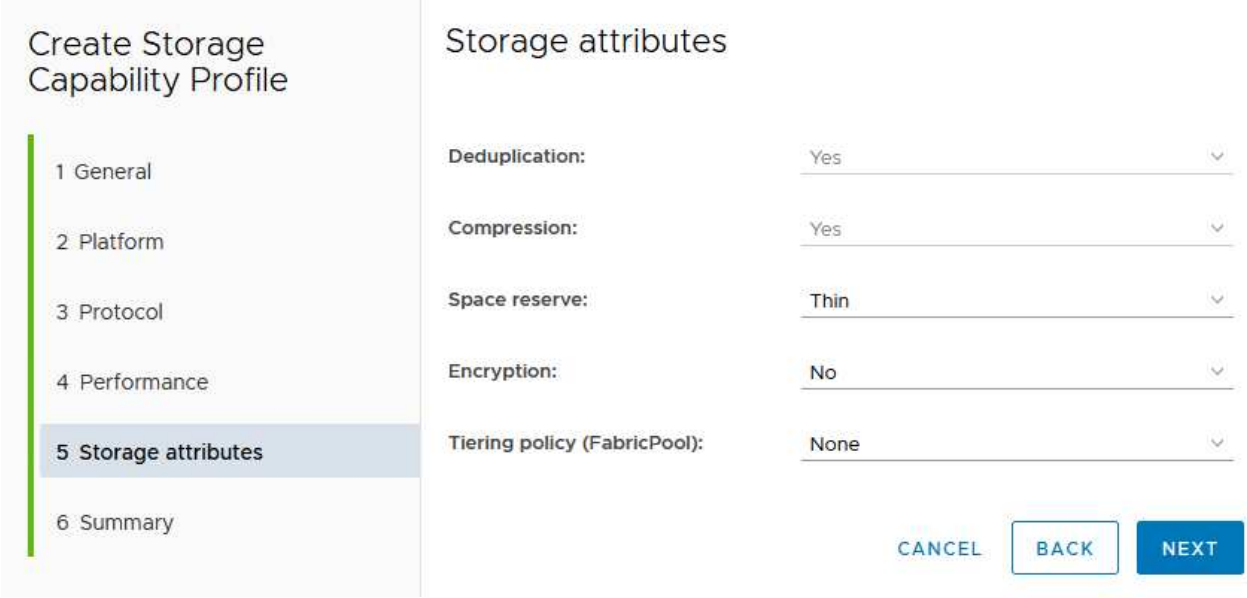
4. Successivamente, seleziona la scelta del protocollo o **Qualsiasi** per consentire tutti i protocolli possibili. Fare clic su **Avanti** per continuare.



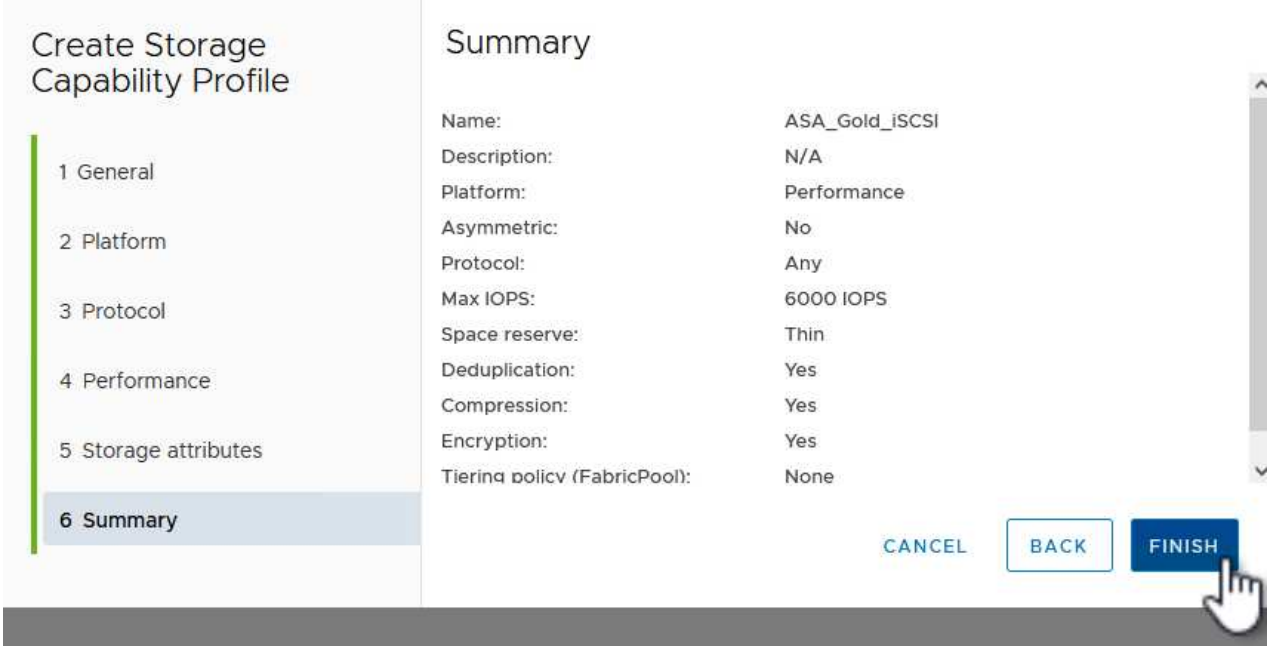
5. La pagina **prestazioni** consente di impostare la qualità del servizio sotto forma di IOP minimi e massimi consentiti.



6. Completare la pagina **attributi di archiviazione** selezionando l'efficienza di archiviazione, la prenotazione dello spazio, la crittografia e qualsiasi criterio di suddivisione in livelli, secondo necessità.



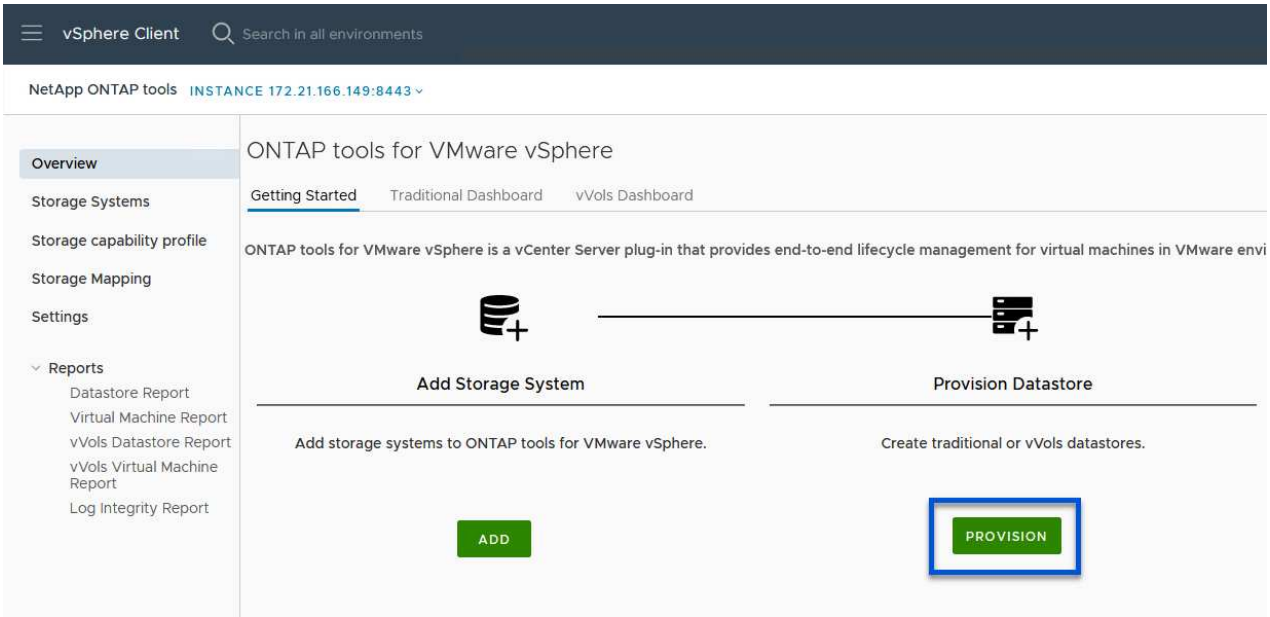
7. Infine, rivedi il riepilogo e clicca su Fine per creare il profilo.


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

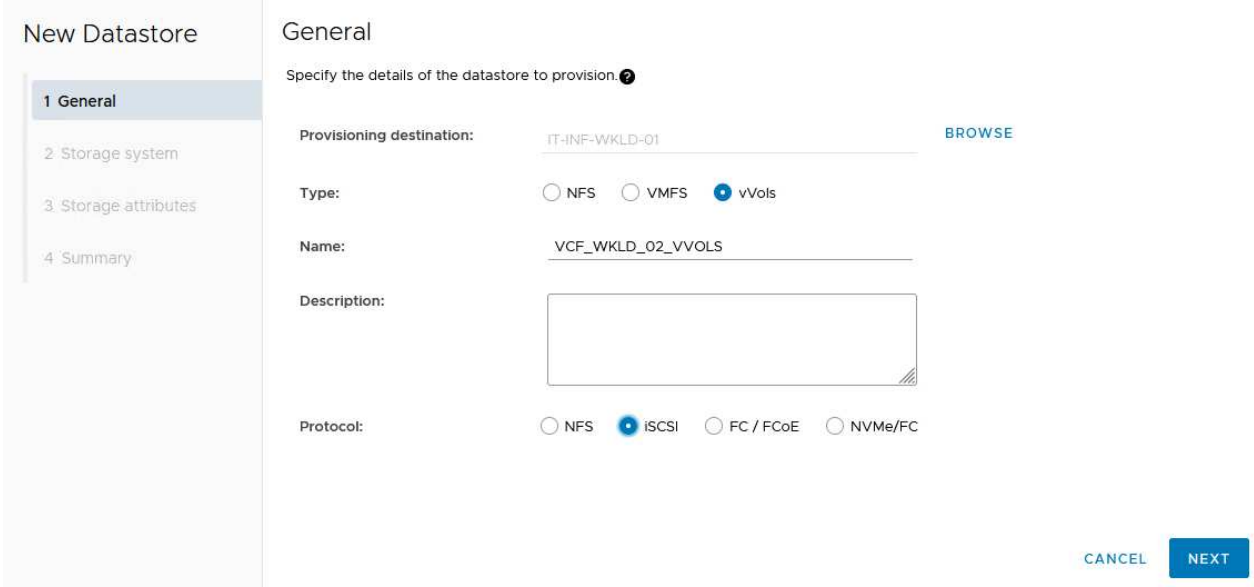
Creare un datastore vVols in ONTAP Tools

Per creare un datastore vVols in ONTAP Tools, completare i seguenti passaggi:

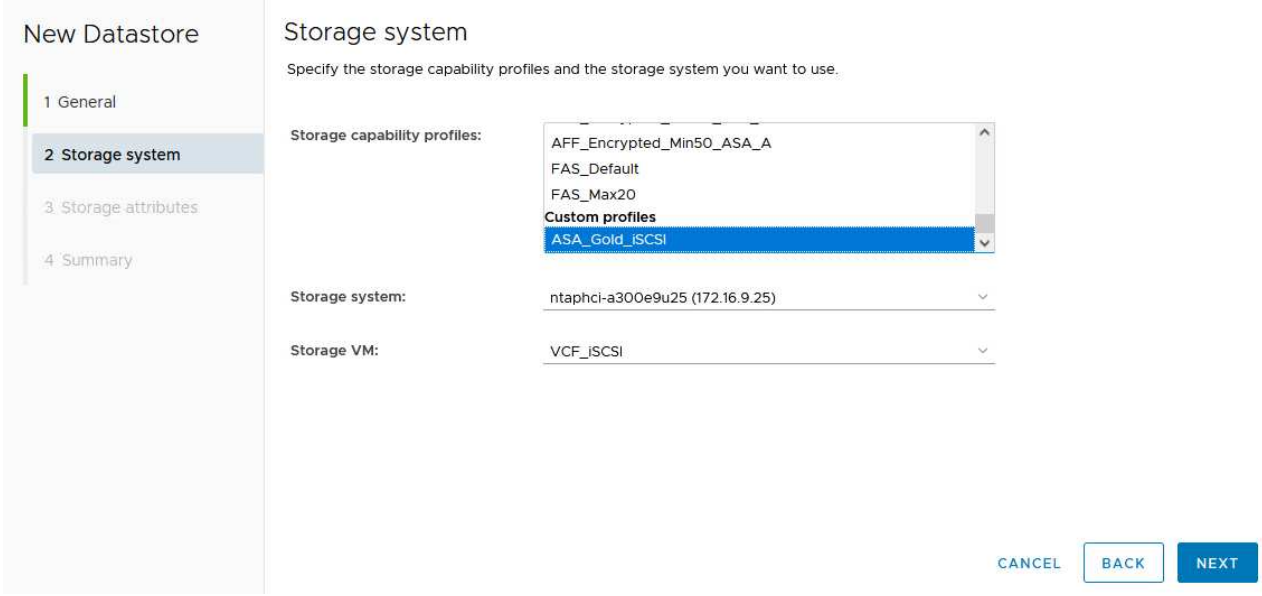
1. In ONTAP Tools seleziona **Panoramica** e dalla scheda **Introduzione** fai clic su **Provision** per avviare la procedura guidata.



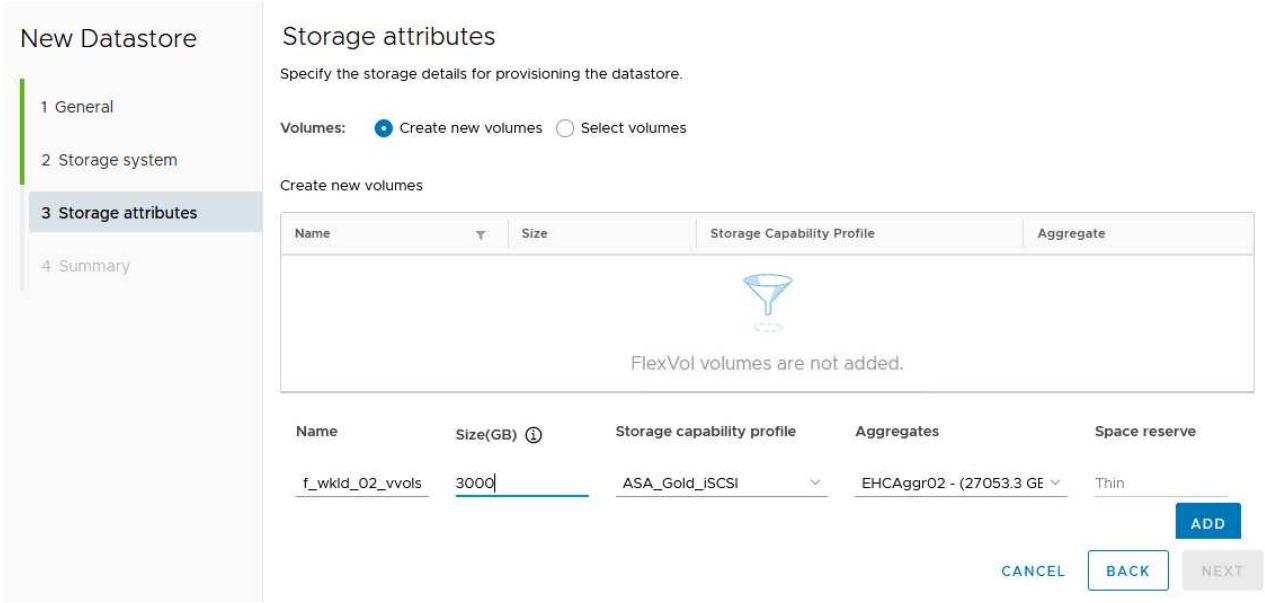
2. Nella pagina **Generale** della procedura guidata Nuovo datastore, selezionare la destinazione del data center o del cluster vSphere. Selezionare * vVols* come tipo di datastore, immettere un nome per il datastore e selezionare **iSCSI** come protocollo. Fare clic su **Avanti** per continuare.



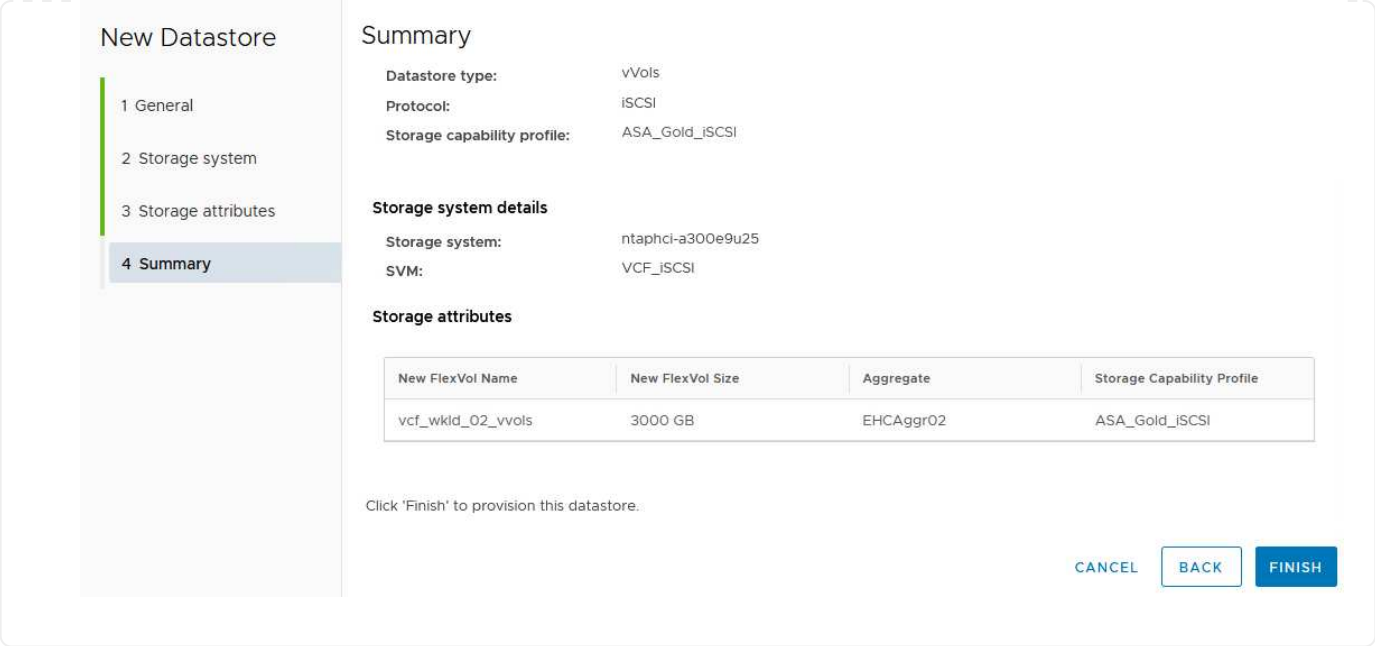
3. Nella pagina **Sistema di archiviazione** selezionare un profilo di capacità di archiviazione, il sistema di archiviazione e l'SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **Attributi di archiviazione** seleziona di creare un nuovo volume per il datastore e compila gli attributi di archiviazione del volume da creare. Fare clic su **Aggiungi** per creare il volume e poi su **Avanti** per continuare.



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



Informazioni aggiuntive

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" .

Aggiungere NFS e vVols come storage supplementare ai domini dei carichi di lavoro VI utilizzando gli ONTAP tools for VMware vSphere

In questo caso d'uso descriviamo la procedura per utilizzare ONTAP Tools per VMware per aggiungere datastore NFS e vVols come storage supplementare per un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Questa procedura riassume la distribuzione di ONTAP Tools per VMware vSphere, la configurazione di una Storage Virtual Machine (SVM) con interfacce logiche NFS e il provisioning di datastore NFS e vVols .

NFS viene utilizzato come protocollo di archiviazione per il datastore vVols .

Vantaggi di NFS

Semplicità e facilità d'uso: NFS è semplice da configurare e gestire, il che lo rende una scelta eccellente per gli ambienti che richiedono una condivisione dei file rapida e semplice.

Scalabilità: l'architettura di ONTAP consente a NFS di scalare in modo efficiente, supportando le crescenti esigenze di dati senza modifiche significative all'infrastruttura.

Flessibilità: NFS supporta un'ampia gamma di applicazioni e carichi di lavoro, rendendolo versatile per vari casi d'uso, inclusi gli ambienti virtualizzati.

Per ulteriori informazioni, fare riferimento al "Guida di riferimento NFS v3 per vSphere 8" .

Panoramica dello scenario

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 dominio del carico di lavoro VI.
- Creare un adattatore vmkernel per NFS sugli host ESXi per il dominio del carico di lavoro VI.
- Distribuire gli strumenti ONTAP sul dominio del carico di lavoro VI.
- Creare un nuovo datastore NFS sul dominio del carico di lavoro VI.
- Creare un nuovo datastore vVols sul dominio del carico di lavoro VI.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o FAS con porte dati fisiche su switch Ethernet dedicate al traffico di archiviazione.
- La distribuzione del dominio di gestione VCF è completa e il client vSphere è accessibile.
- In precedenza è stato distribuito un dominio di carico di lavoro VI.

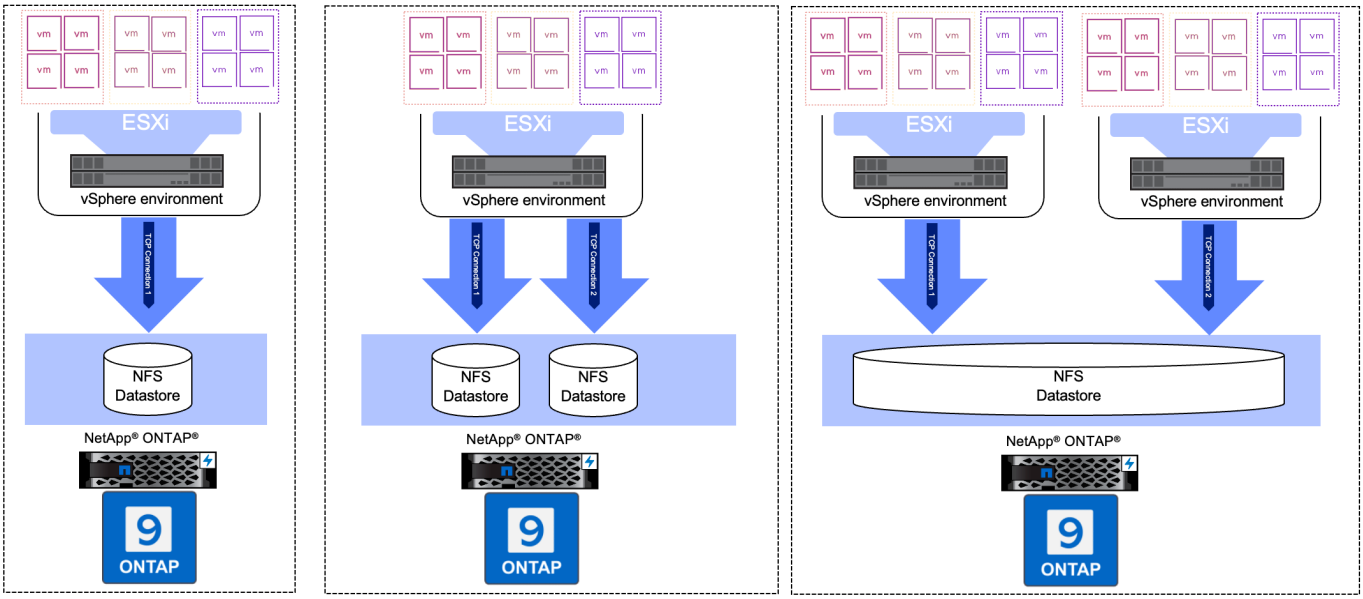
NetApp consiglia una progettazione di rete ridondante per NFS, che garantisca tolleranza agli errori per sistemi di storage, switch, adattatori di rete e sistemi host. È comune distribuire NFS con una singola subnet o più subnet a seconda dei requisiti architettonici.

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 .

Questa documentazione illustra il processo di creazione di un nuovo SVM e di specifica delle informazioni sull'indirizzo IP per creare più LIF per il traffico NFS. Per aggiungere nuovi LIF a un SVM esistente, fare riferimento a"Creare un LIF (interfaccia di rete)" .

Per informazioni complete sull'utilizzo di NFS con cluster vSphere, fare riferimento a"Guida di riferimento NFS v3 per vSphere 8" .



Fasi di distribuzione

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

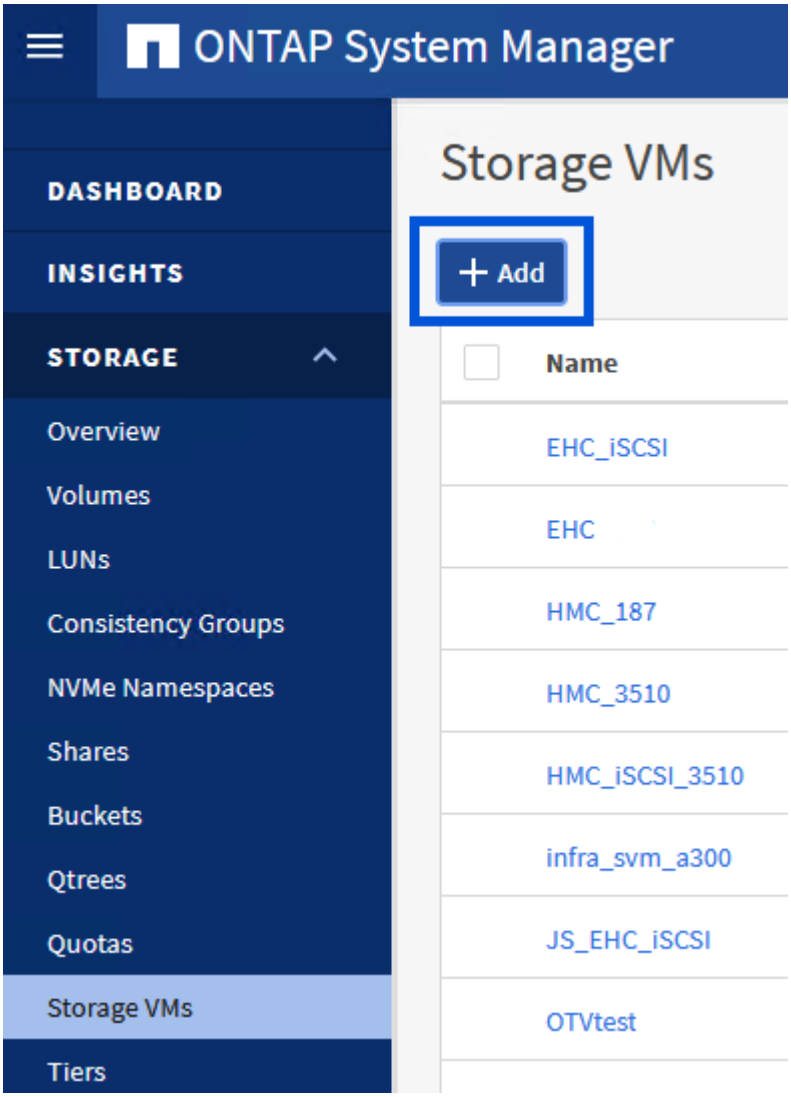
Creare SVM e LIF sul sistema di archiviazione ONTAP

Il passaggio seguente viene eseguito in ONTAP System Manager.

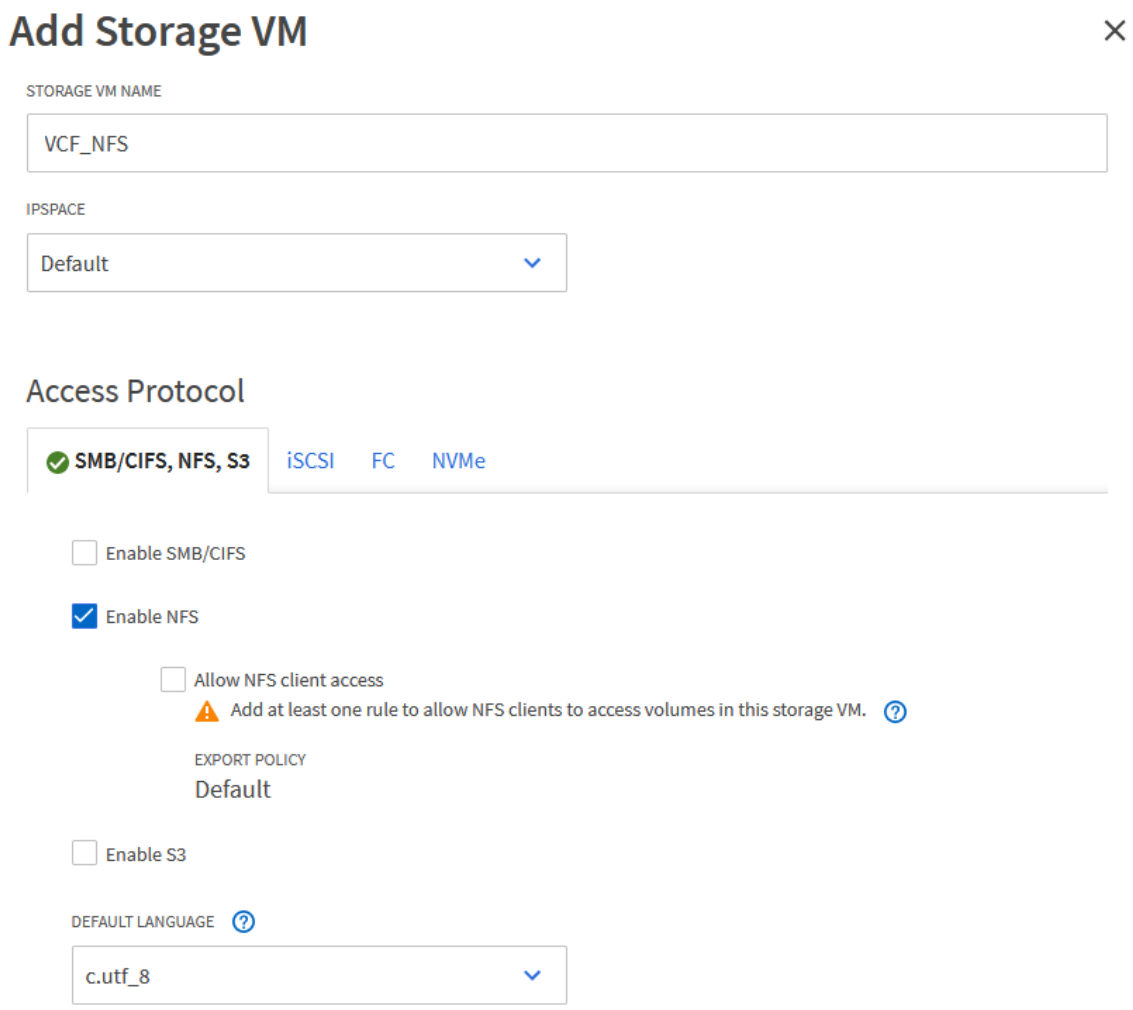
Creare la VM di archiviazione e i LIF

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.

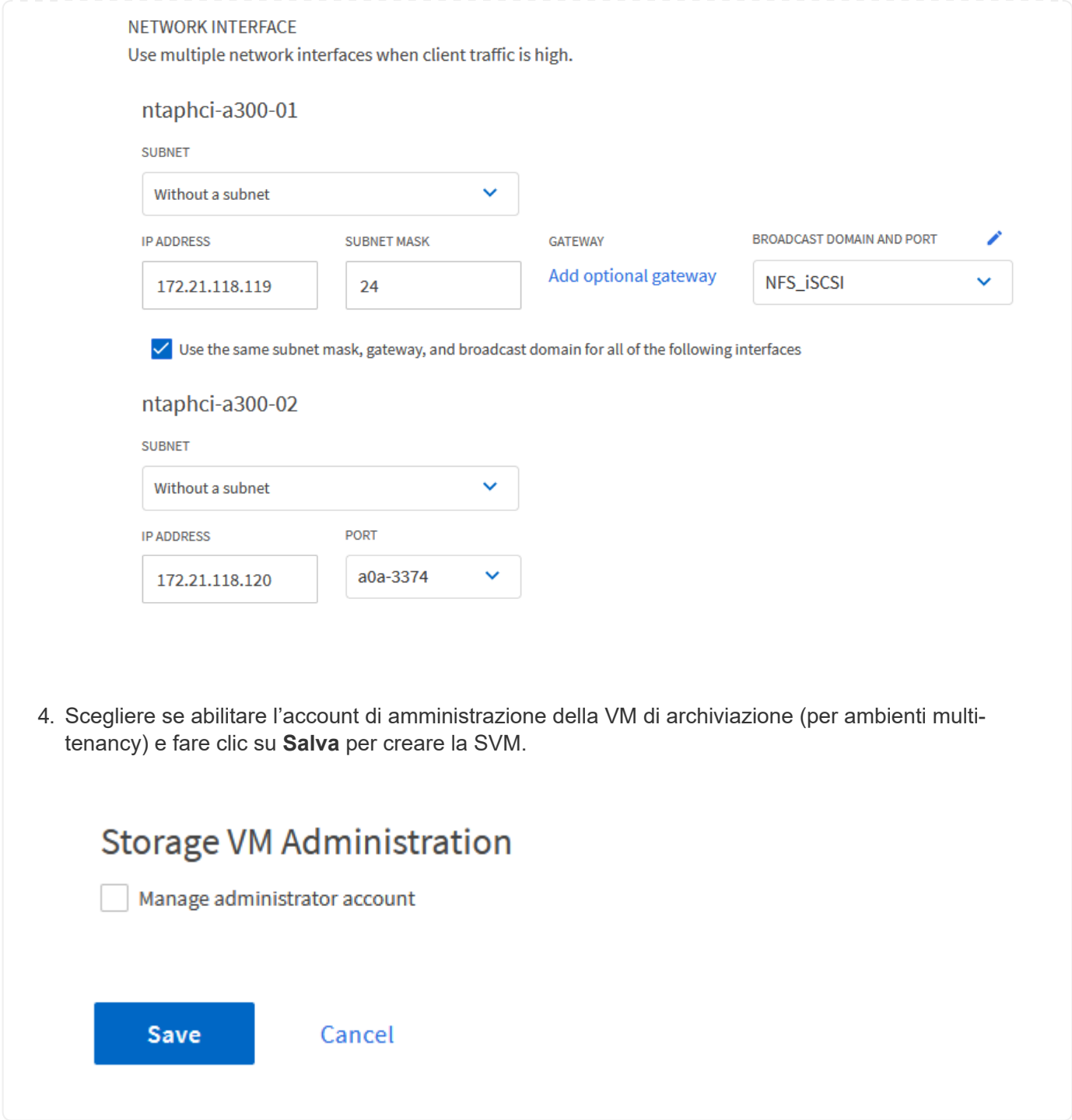


2. Nella procedura guidata **Aggiungi VM di archiviazione**, fornire un **Nome** per la SVM, selezionare lo **Spazio IP** e quindi, in **Protocollo di accesso**, fare clic sulla scheda **SMB/CIFS, NFS, S3** e selezionare la casella per **Abilitare NFS**.



Non è necessario selezionare il pulsante **Consenti accesso client NFS** in quanto Ontap Tools per VMware vSphere verrà utilizzato 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.

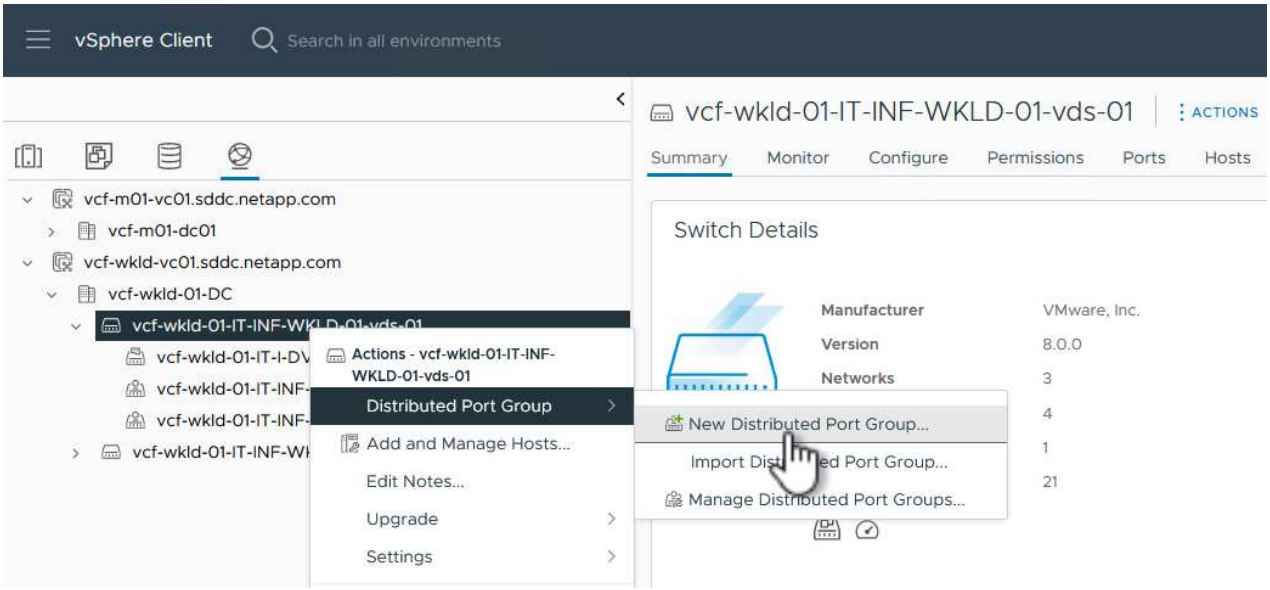
Configurare la rete per NFS sugli host ESXi

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.

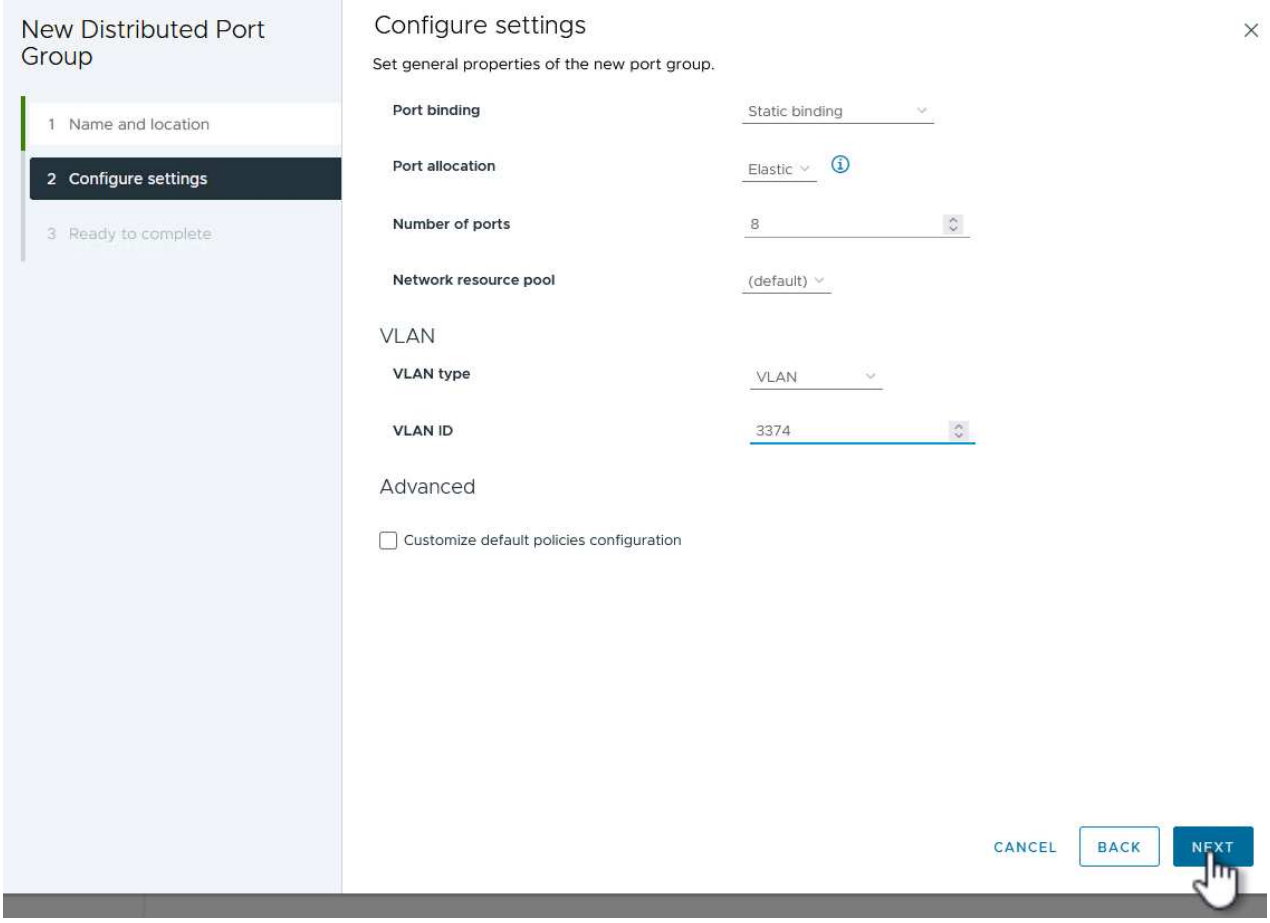
Creare un gruppo di porte distribuito per il traffico NFS

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

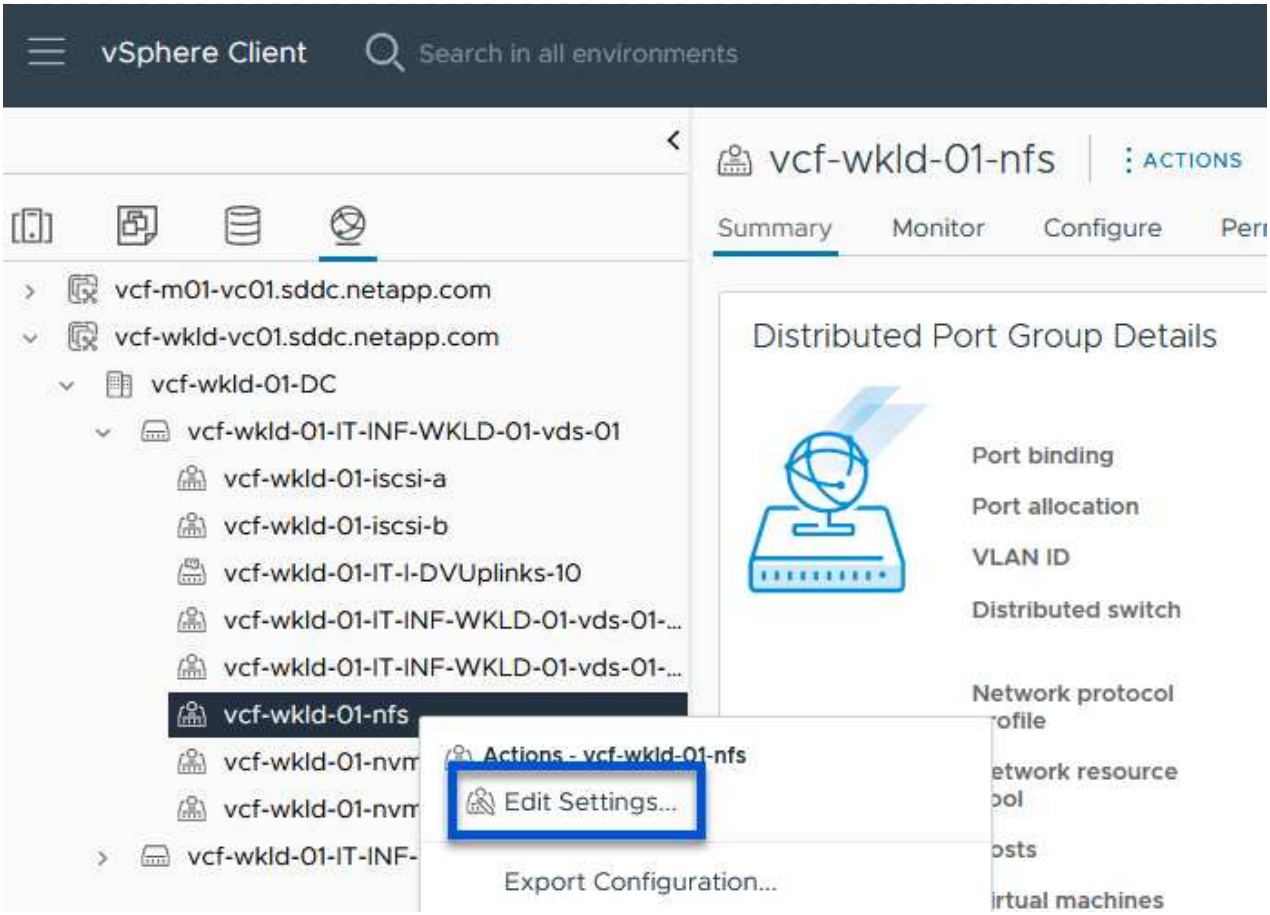
1. Dal client vSphere, accedere a **Inventario > Rete** per il dominio del carico di lavoro. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite…**.



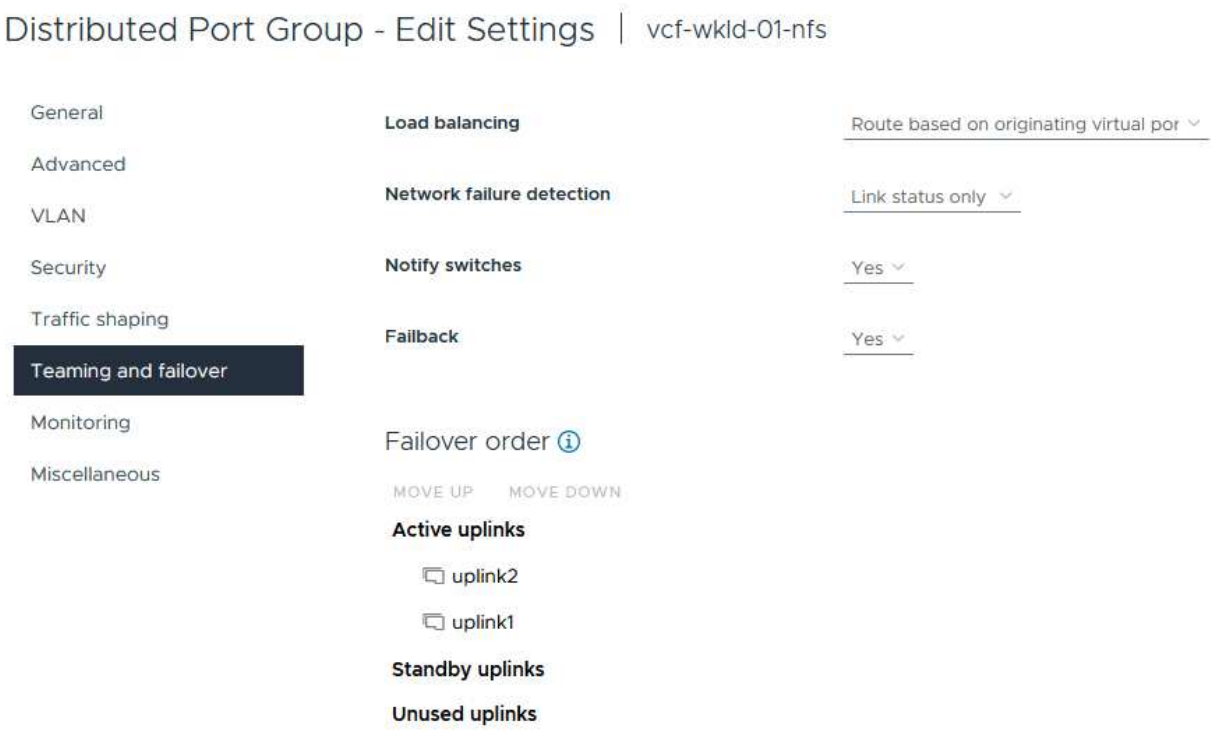
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, immettere un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare 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 insieme nell'area **Uplink attivi**. Sposta tutti gli uplink non utilizzati in **Uplink non utilizzati**.

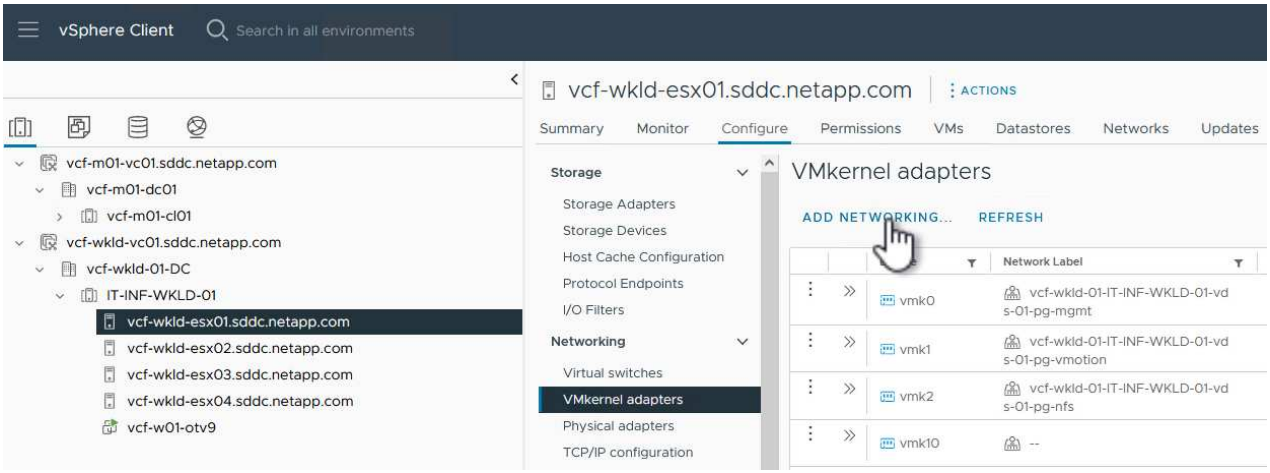


7. Ripetere questo processo per ogni host ESXi nel cluster.

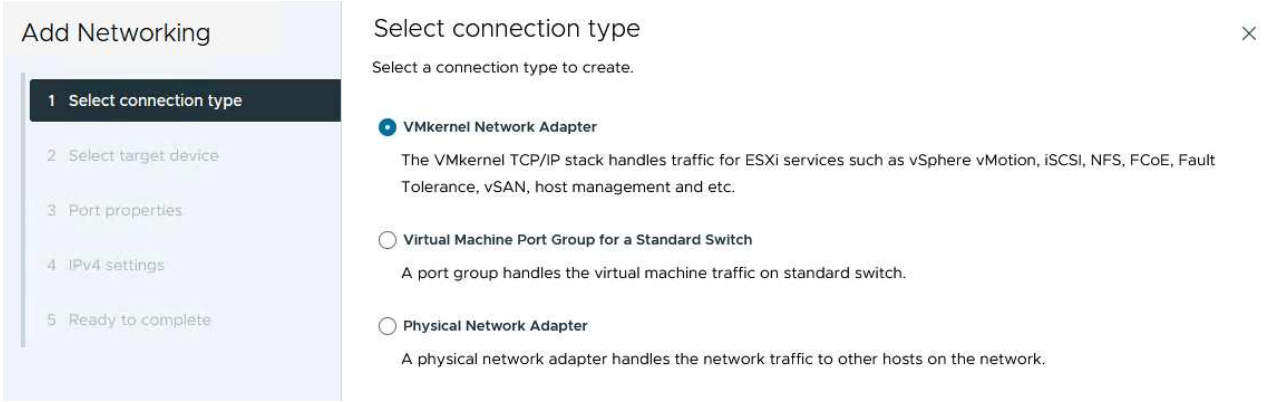
Creare un adattatore VMkernel su ciascun host ESXi

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

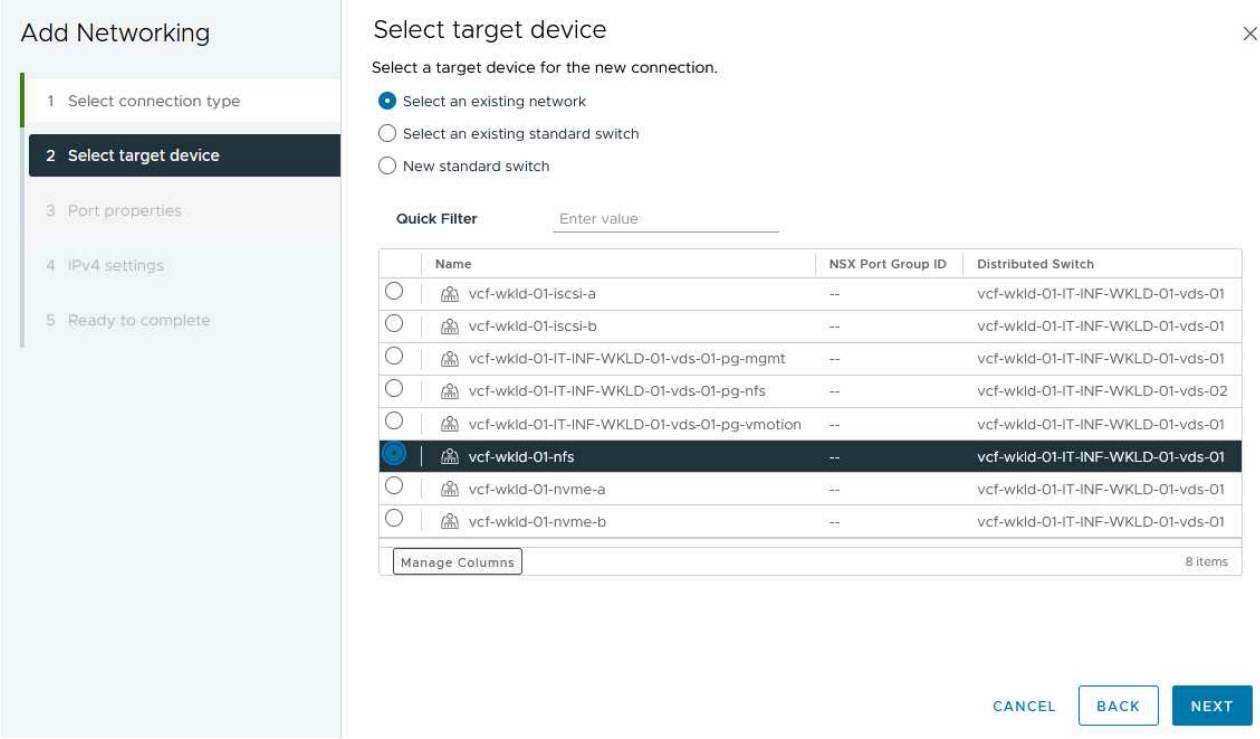
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configura** seleziona **Schede VMkernel** e clicca su **Aggiungi rete…** per iniziare.



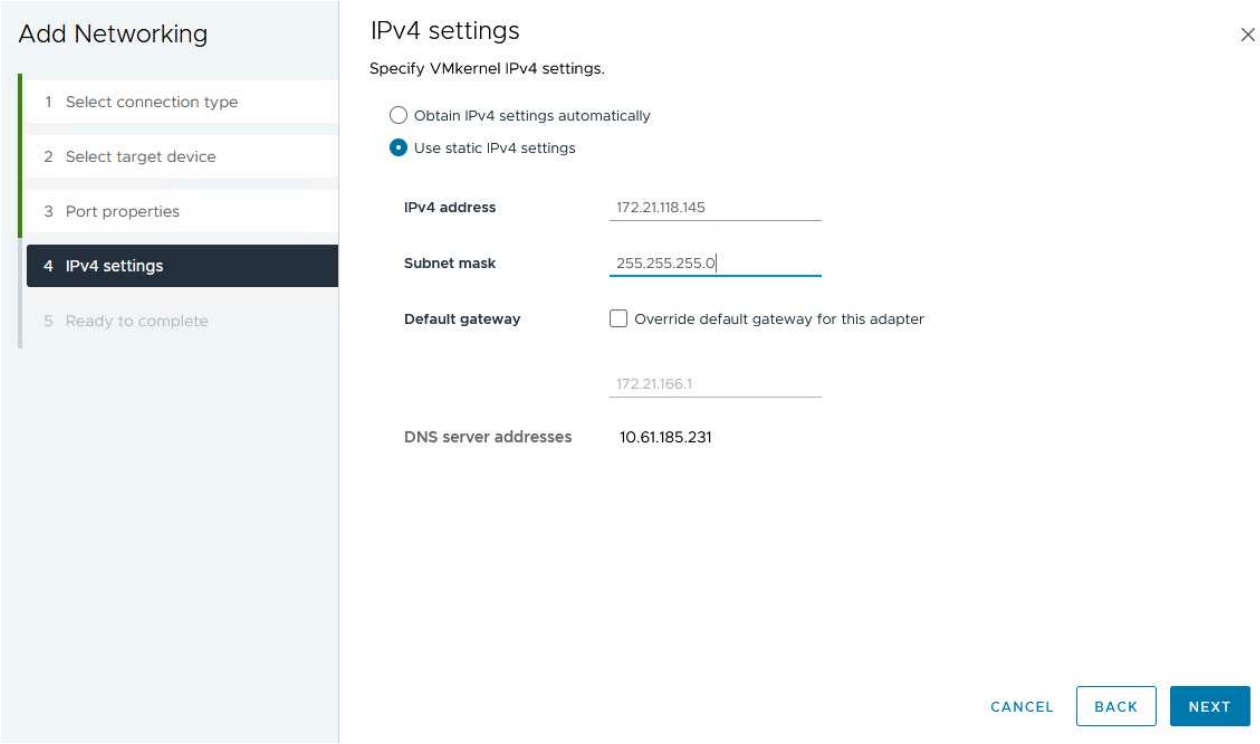
2. Nella finestra **Seleziona tipo di connessione** seleziona **Scheda di rete VMkernel** e fai clic su **Avanti** per continuare.



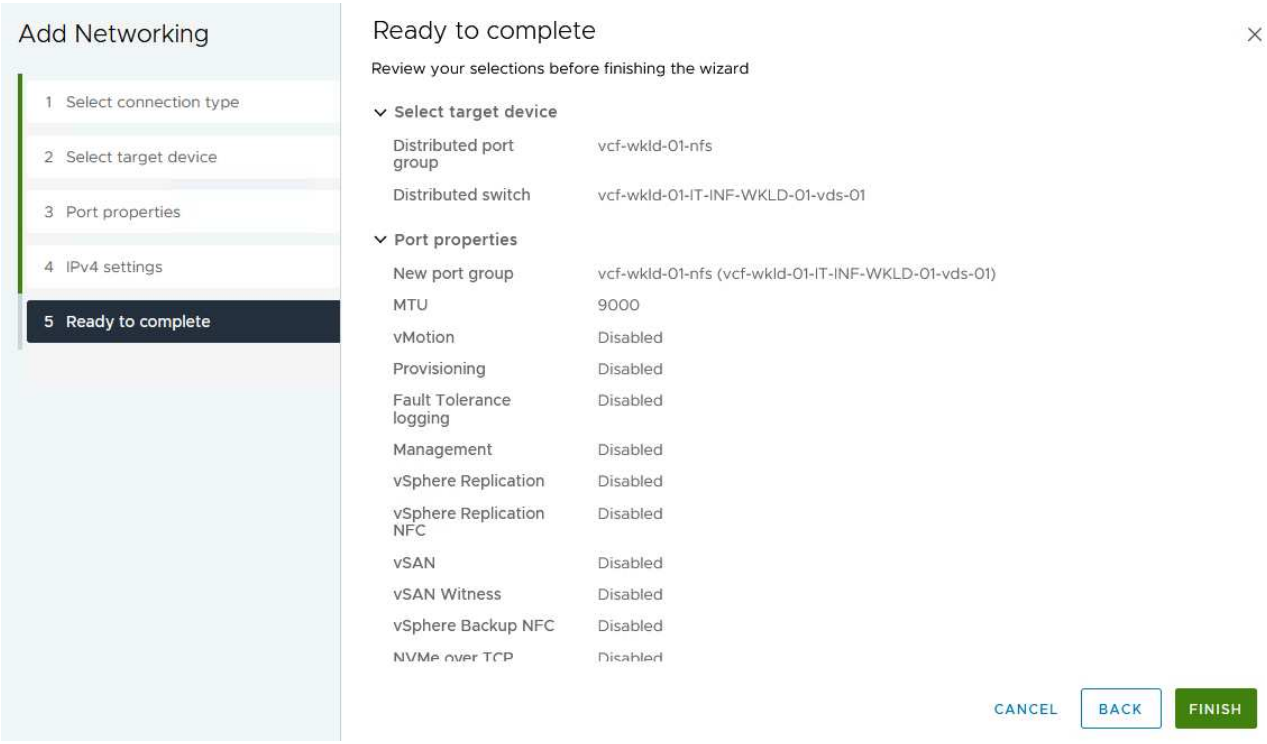
3. Nella pagina **Seleziona dispositivo di destinazione**, seleziona uno dei gruppi di porte distribuiti per NFS creati in precedenza.



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.



Distribuisci e usa gli strumenti ONTAP per configurare l'archiviazione

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

Per i domini del carico di lavoro VI, OTV è installato nel VCF Management Cluster ma registrato con il vCenter associato al dominio del carico di lavoro VI.

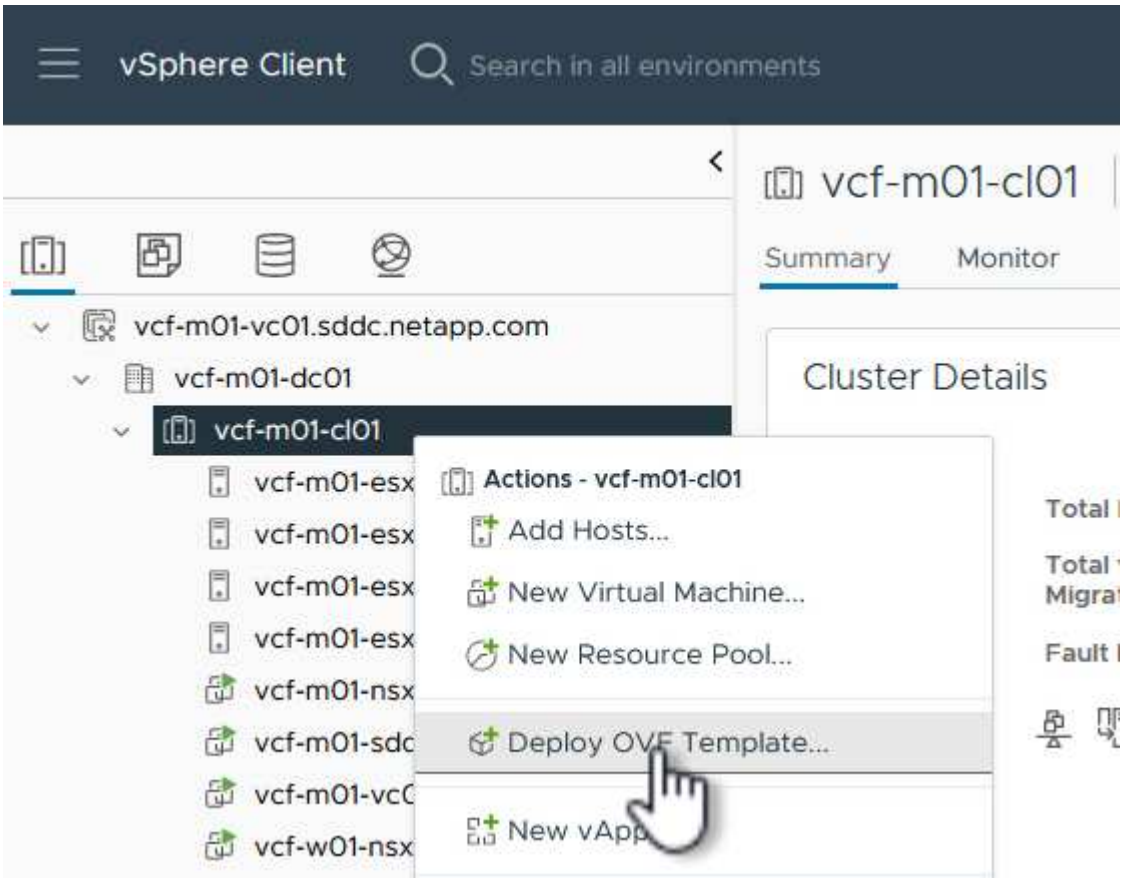
Per ulteriori informazioni sulla distribuzione e l'utilizzo di ONTAP Tools in un ambiente vCenter multiplo, fare riferimento a"Requisiti per la registrazione degli strumenti ONTAP in un ambiente con più vCenter Server" .

Distribuisci gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere (OTV) vengono distribuiti come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP .

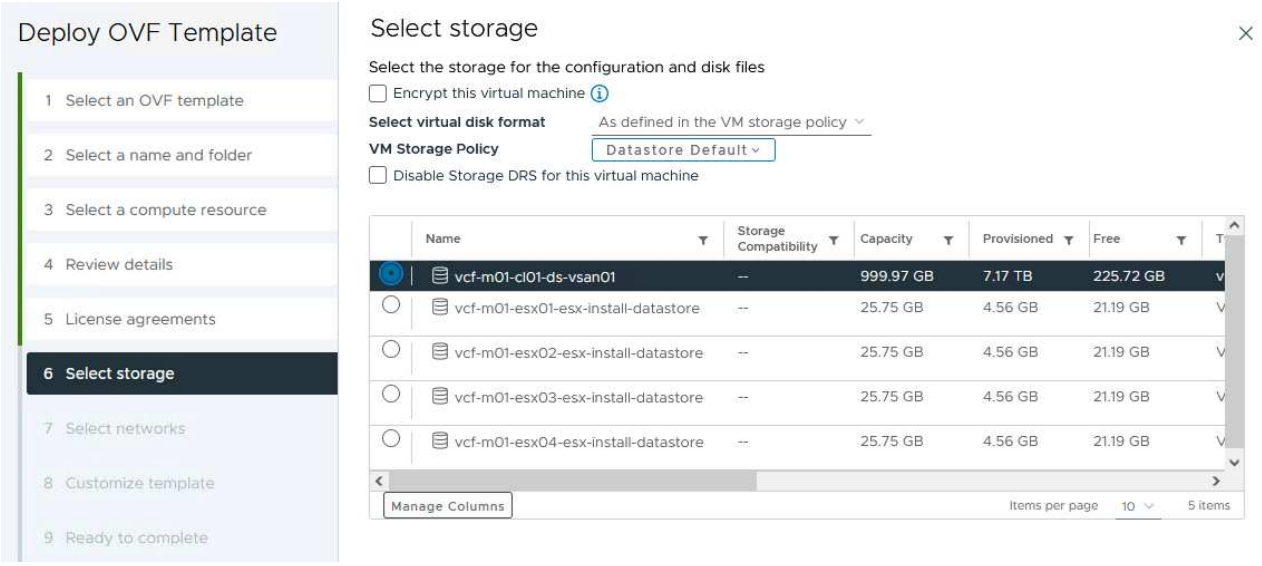
Completare quanto segue per distribuire gli ONTAP tools for VMware vSphere:

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 dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Distribuisci modello OVF…**

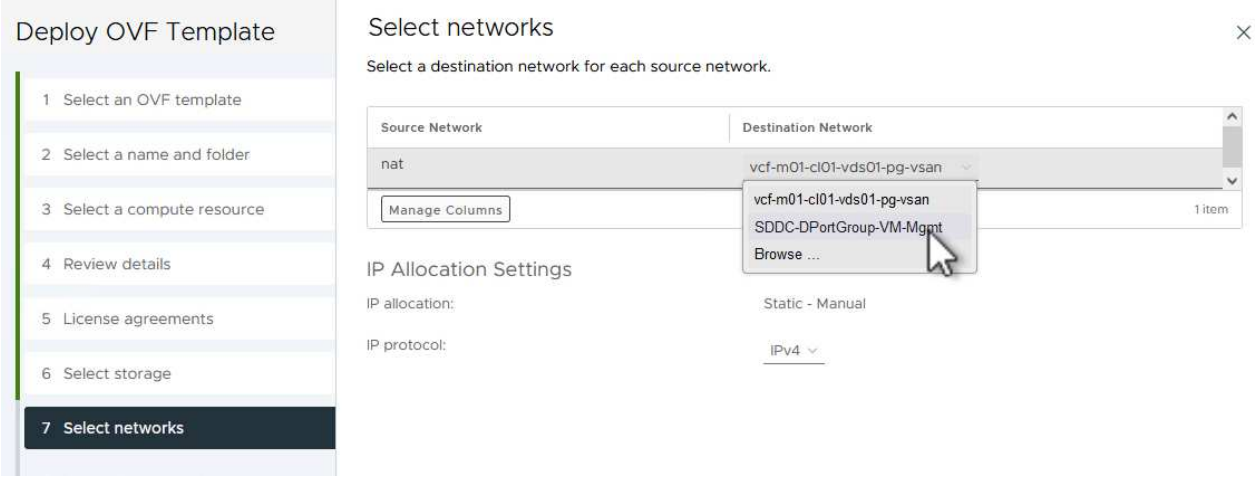


4. Nella procedura guidata **Distribuisci modello OVF**, fare clic sul pulsante di opzione **File locale** e selezionare il file OVA degli strumenti ONTAP scaricato nel passaggio precedente.

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 il datastore vSAN del cluster del dominio di gestione VCF.

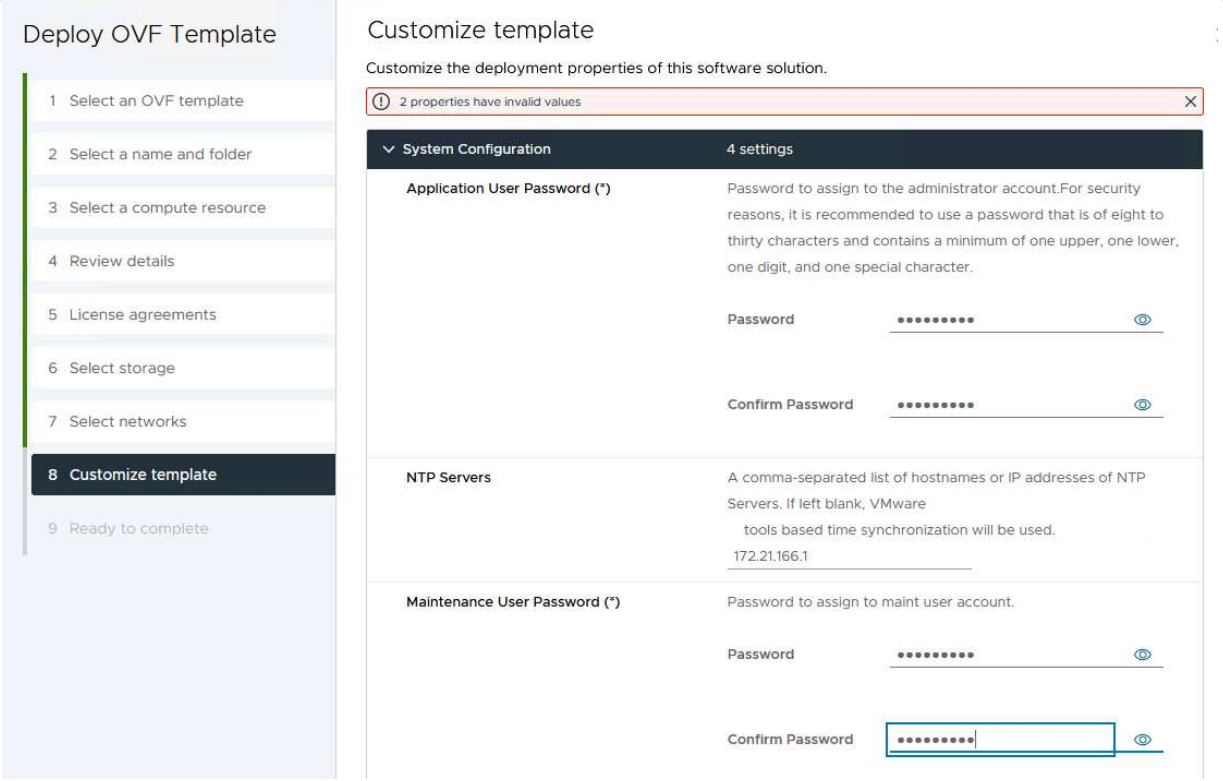


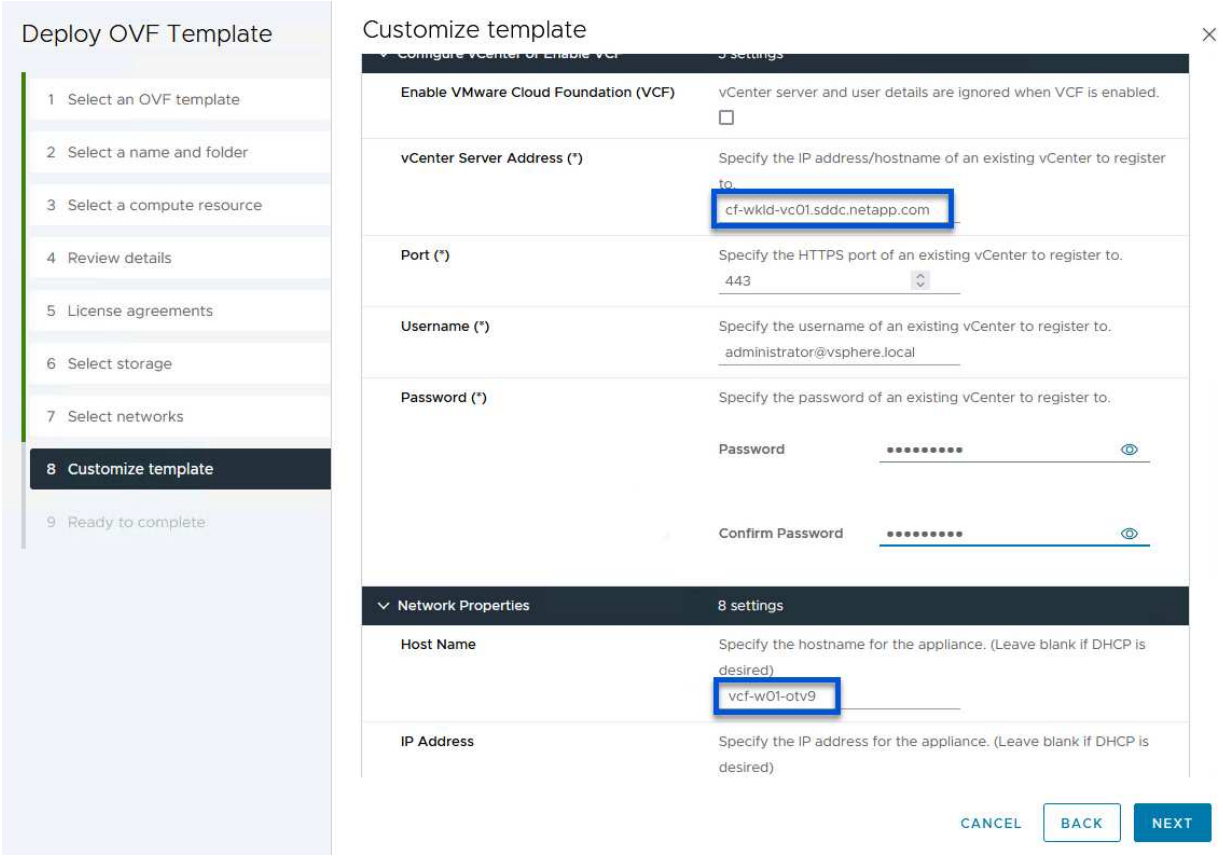
7. Nella pagina Seleziona rete seleziona la rete utilizzata per la gestione del traffico.



8. Nella pagina Personalizza modello compila tutte le informazioni richieste:
   - Password da utilizzare per l'accesso amministrativo a OTV.
   - Indirizzo IP del server NTP.
   - Password dell'account di manutenzione OTV.
   - Password del database OTV Derby.
   - Non selezionare la casella per **Abilitare VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire storage supplementare.
   - FQDN o indirizzo IP dell'appliance vCenter per il **dominio del carico di lavoro VI**
   - Credenziali per l'appliance vCenter del **VI Workload Domain**
   - Fornire i campi delle proprietà di rete richiesti.

     Fare clic su **Avanti** per continuare.

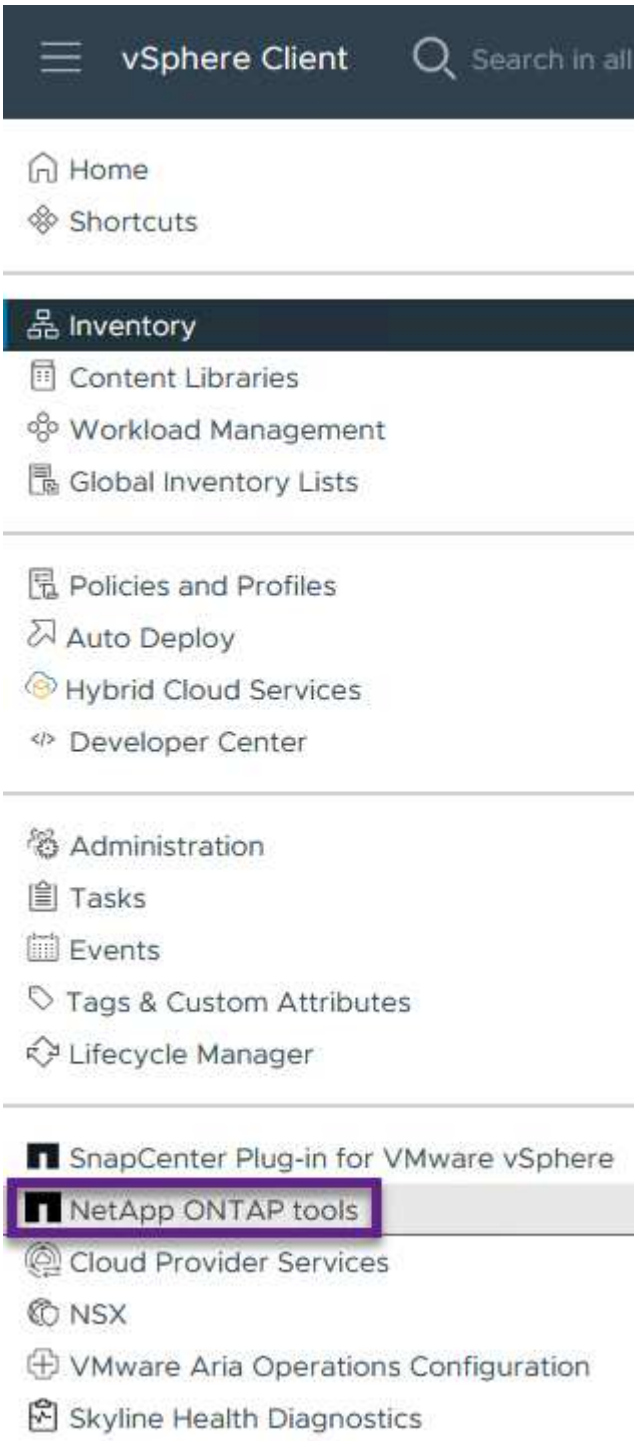




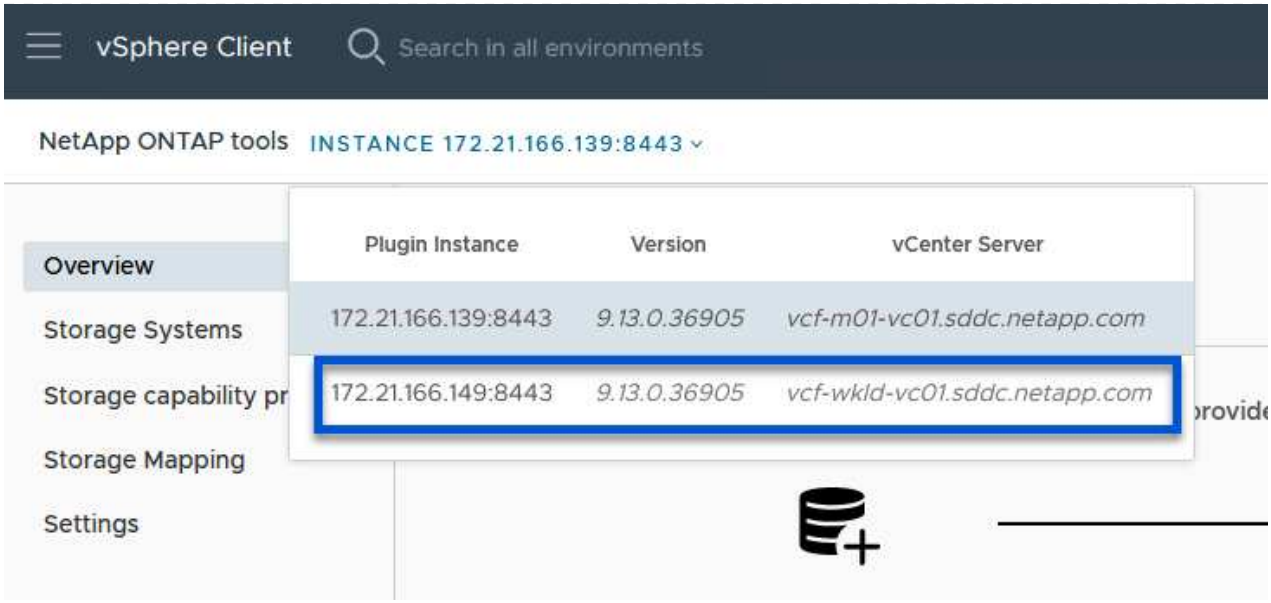
9. Rivedere tutte le informazioni nella pagina Pronto per il completamento e fare clic su Fine per iniziare a distribuire l'appliance OTV.

Aggiungere un sistema di archiviazione a ONTAP Tools.

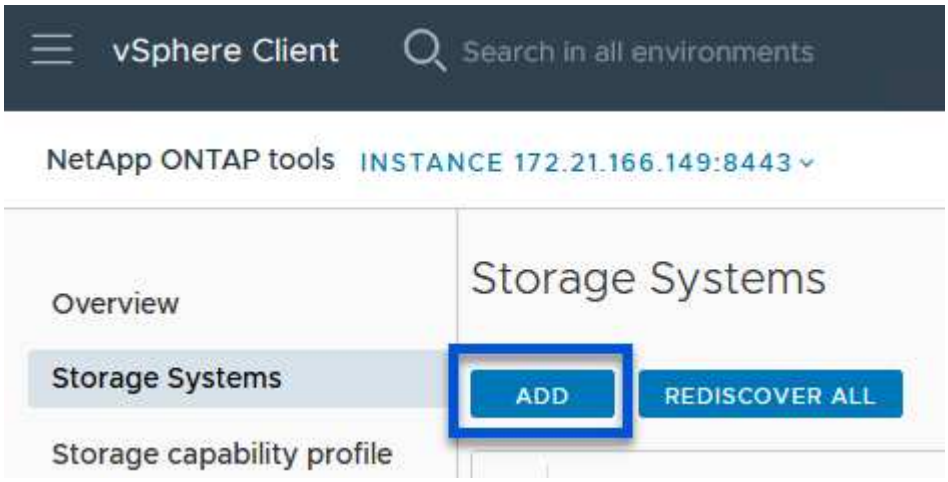
1. Accedi a NetApp ONTAP Tools selezionandolo dal menu principale nel client vSphere.



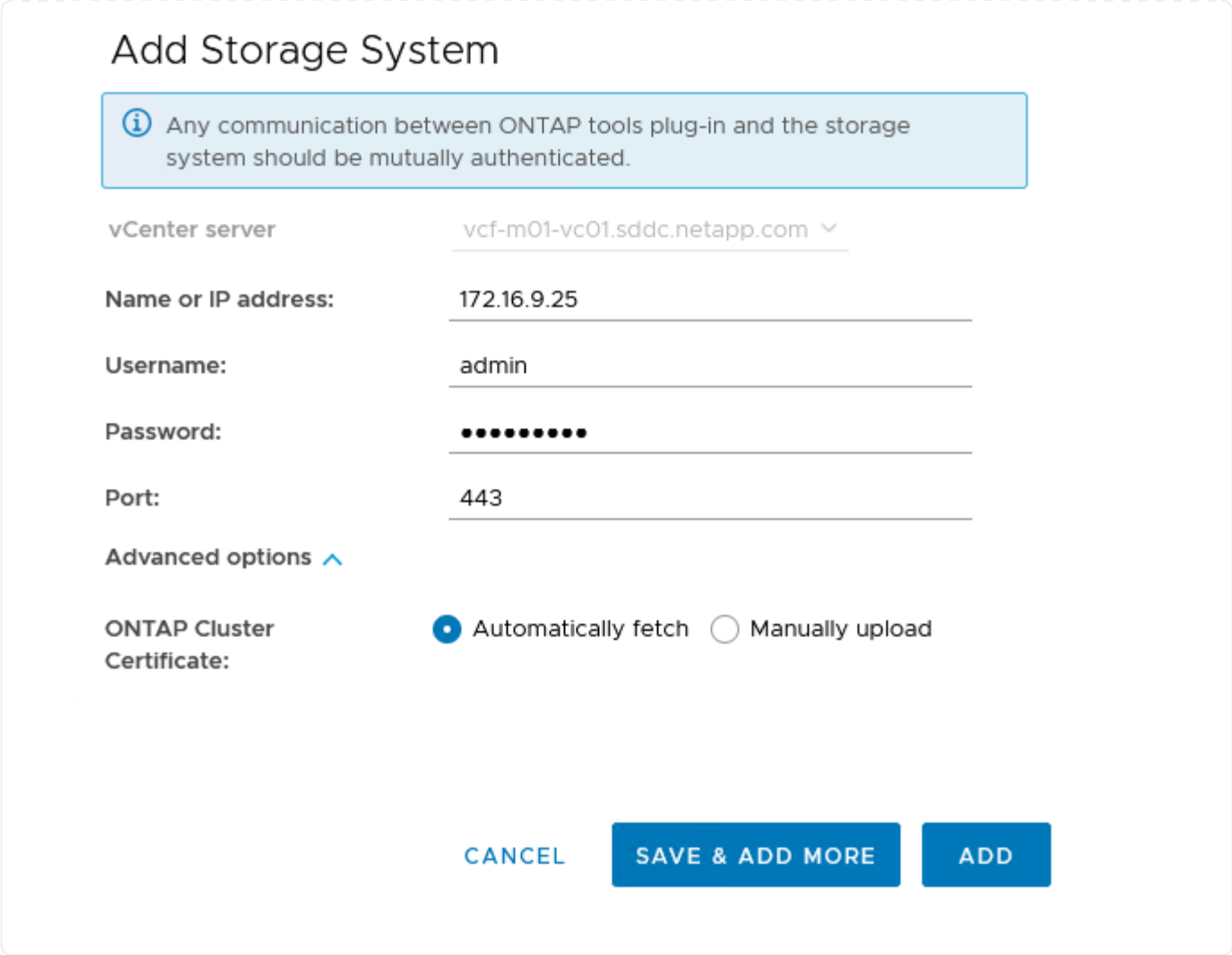
2. Dal menu a discesa **ISTANZA** nell'interfaccia dello strumento ONTAP , selezionare l'istanza OTV associata al dominio del carico di lavoro da gestire.



3. In ONTAP Tools seleziona **Storage Systems** dal menu a sinistra e poi premi **Aggiungi**.



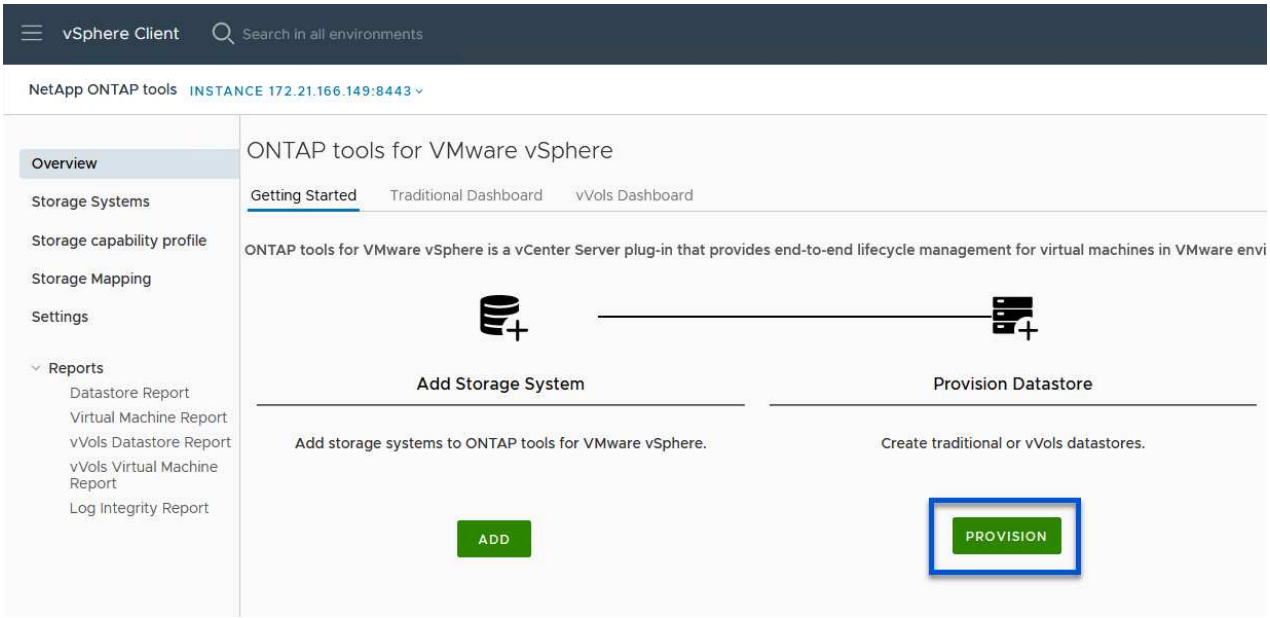
4. Compila l'indirizzo IP, le credenziali del sistema di archiviazione e il numero di porta. Fare clic su **Aggiungi** per avviare il processo di scoperta.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Creare un datastore NFS in ONTAP Tools

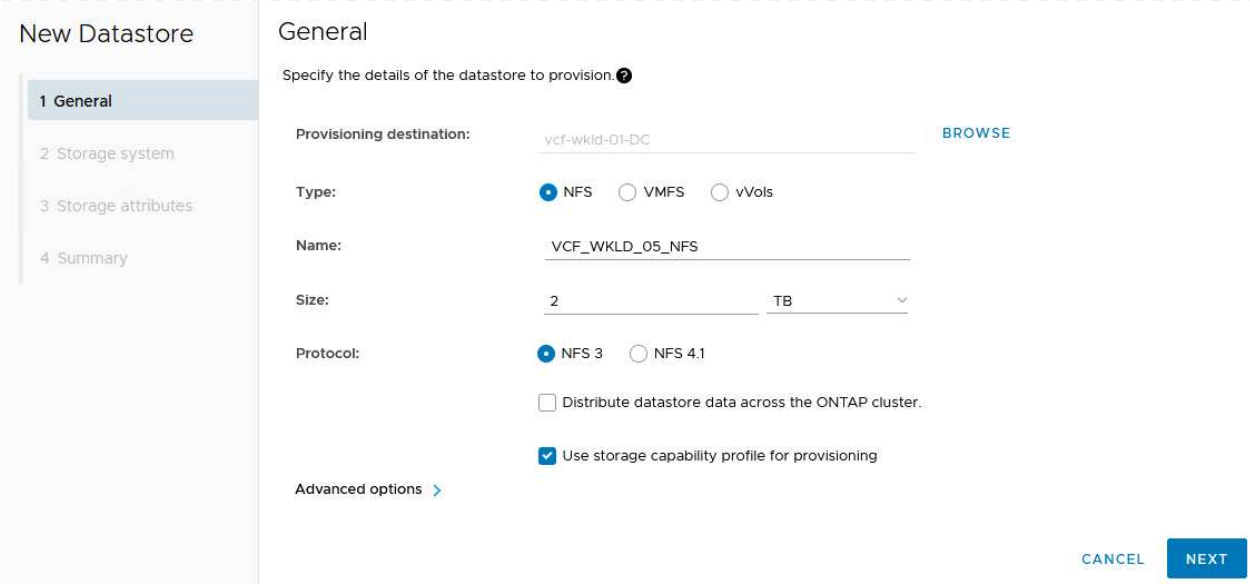
Completare i seguenti passaggi per distribuire un datastore ONTAP , in esecuzione su NFS, utilizzando ONTAP Tools.

1. In ONTAP Tools seleziona **Panoramica** e dalla scheda **Introduzione** fai clic su **Provision** per avviare la procedura guidata.

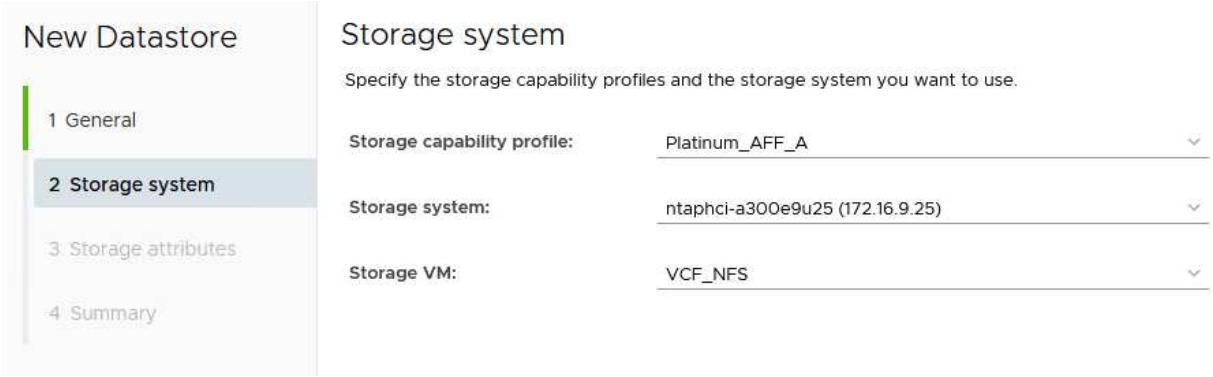


2. Nella pagina **Generale** della procedura guidata Nuovo datastore, selezionare la destinazione del data center o del cluster vSphere. Selezionare **NFS** come tipo di datastore, immettere un nome per il datastore e selezionare il protocollo. Scegliere se utilizzare volumi FlexGroup e se utilizzare un file di capacità di archiviazione per il provisioning. Fare clic su **Avanti** per continuare.

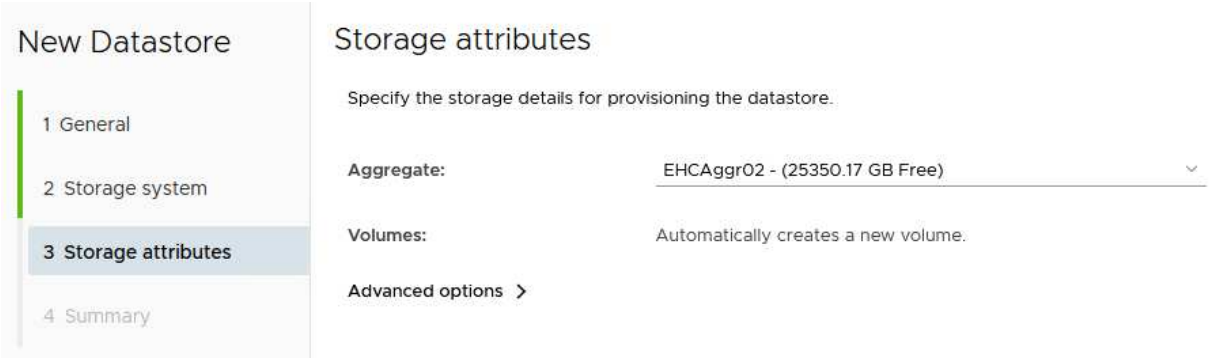
   Nota: selezionando **Distribuisci i dati del datastore nel cluster**, il volume sottostante verrà creato come volume FlexGroup , il che preclude l'utilizzo dei profili di capacità di archiviazione. Fare riferimento a "Configurazioni supportate e non supportate per i volumi FlexGroup" per ulteriori informazioni sull'utilizzo di FlexGroup Volumes.



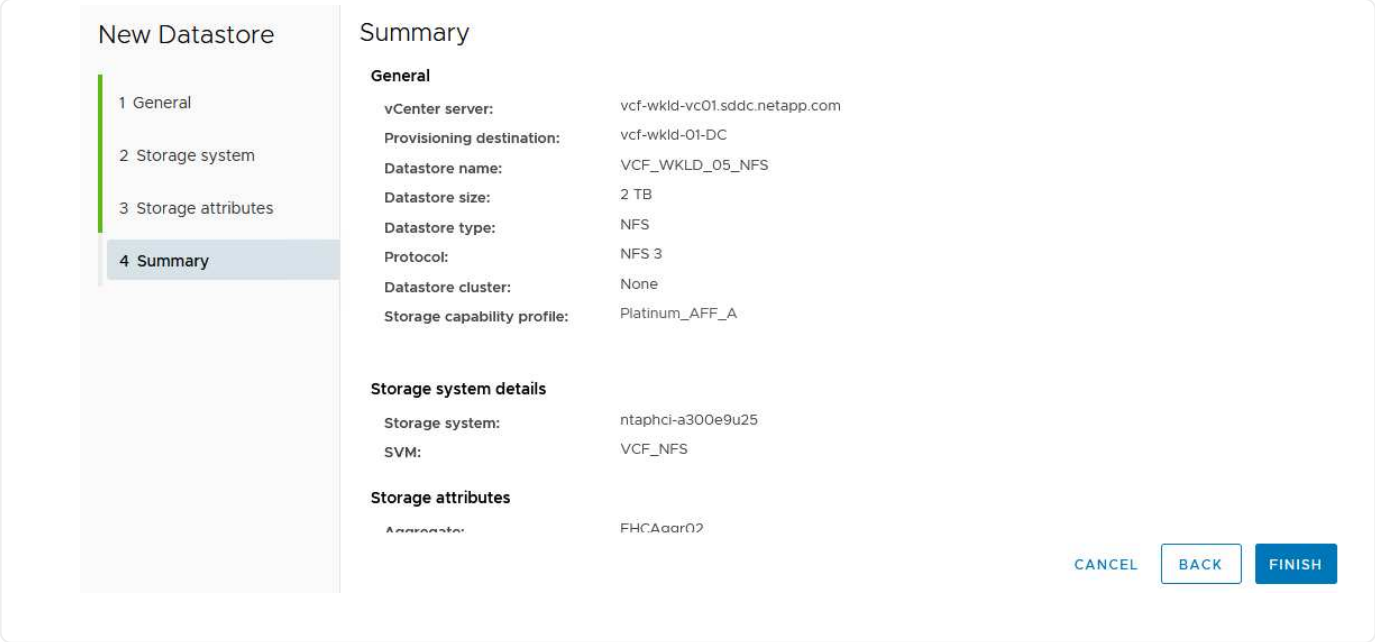
3. Nella pagina **Sistema di archiviazione** selezionare un profilo di capacità di archiviazione, il sistema di archiviazione e l'SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **Attributi di archiviazione** seleziona l'aggregato da utilizzare e poi clicca su **Avanti** per continuare.



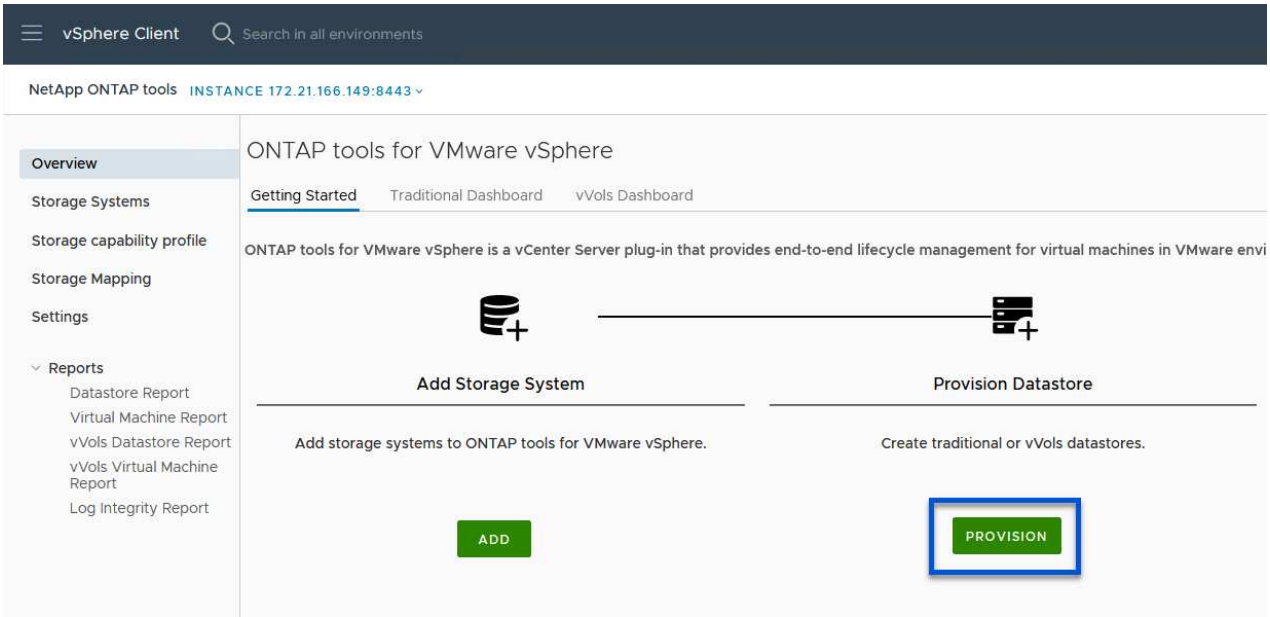
5. Infine, rivedere il **Riepilogo** e fare clic su Fine per iniziare a creare il datastore NFS.


New Datastore
1 General
2 Storage system
3 Storage attributes
4 Summary
Summary
General
vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_05_NFS
Datastore size: 2 TB
Datastore type: NFS
Protocol: NFS 3
Datastore cluster: None
Storage capability profile: Platinum_AFF_A
Storage system details
Storage system: ntaphci-a300e9u25
SVM: VCF_NFS
Storage attributes
CANCEL
BACK
FINISH

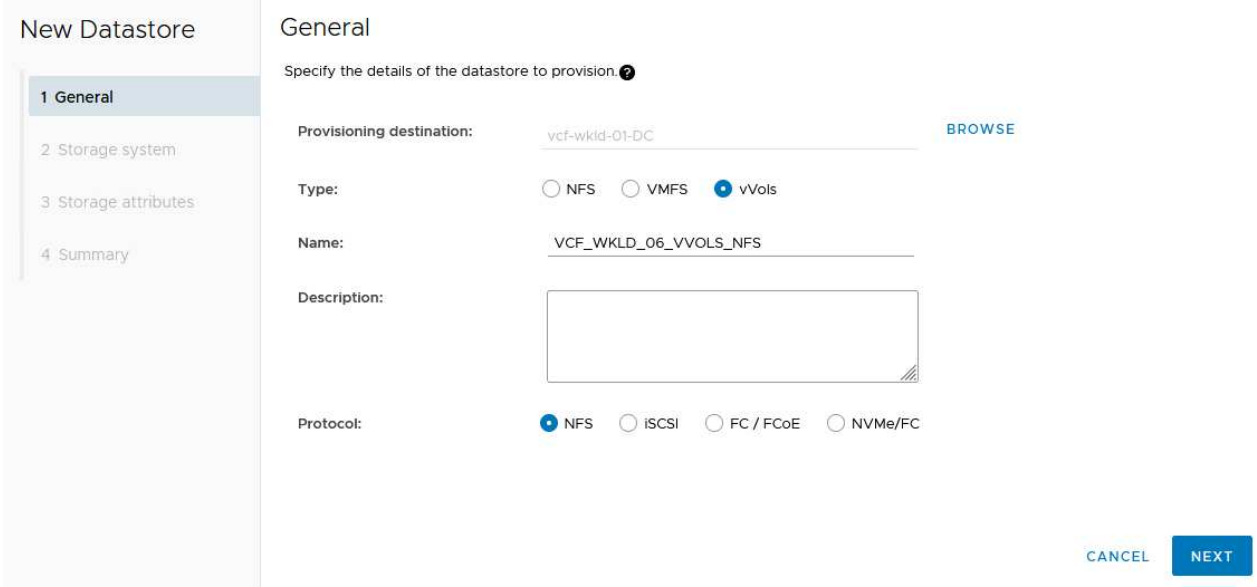
Creare un datastore vVols in ONTAP Tools

Per creare un datastore vVols in ONTAP Tools, completare i seguenti passaggi:

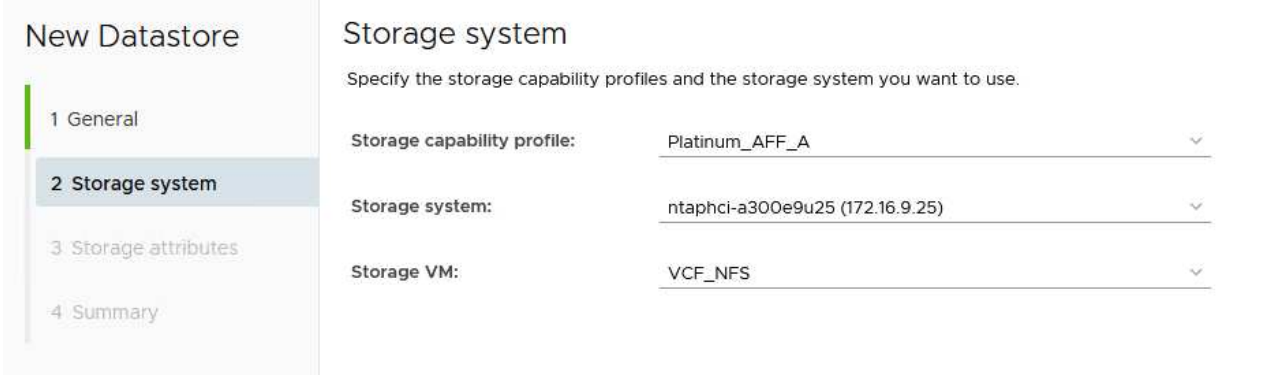
1. In ONTAP Tools seleziona **Panoramica** e dalla scheda **Introduzione** fai clic su **Provision** per avviare la procedura guidata.



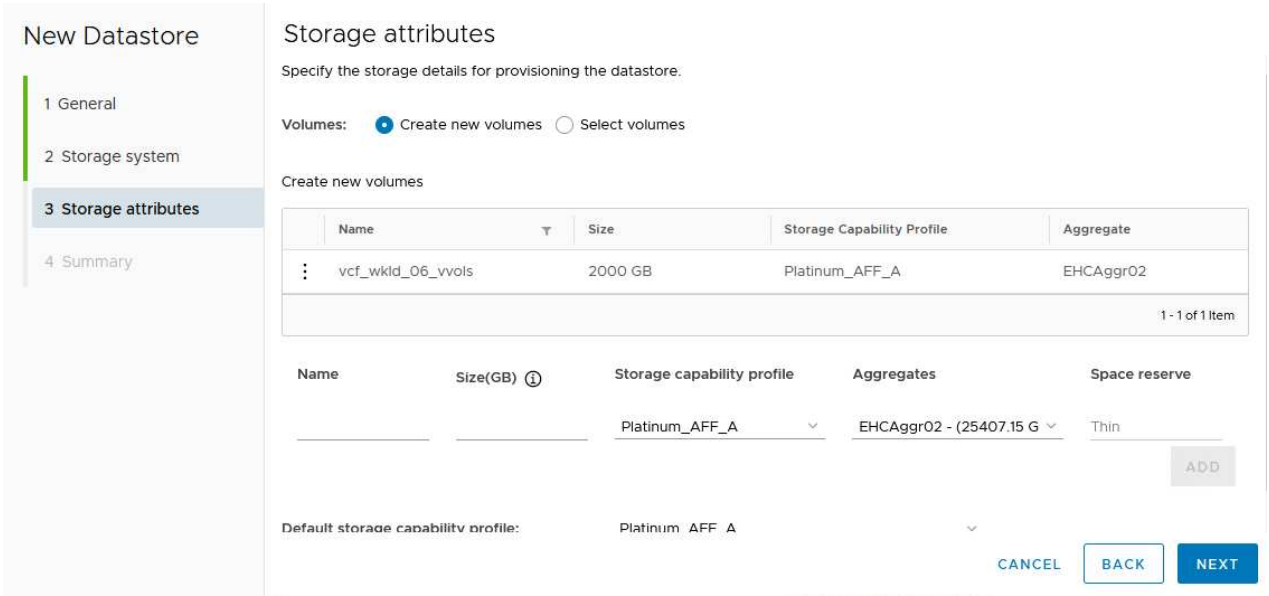
2. Nella pagina **Generale** della procedura guidata Nuovo datastore, selezionare la destinazione del data center o del cluster vSphere. Selezionare * vVols* come tipo di datastore, immettere un nome per il datastore e selezionare **NFS** come protocollo. Fare clic su **Avanti** per continuare.



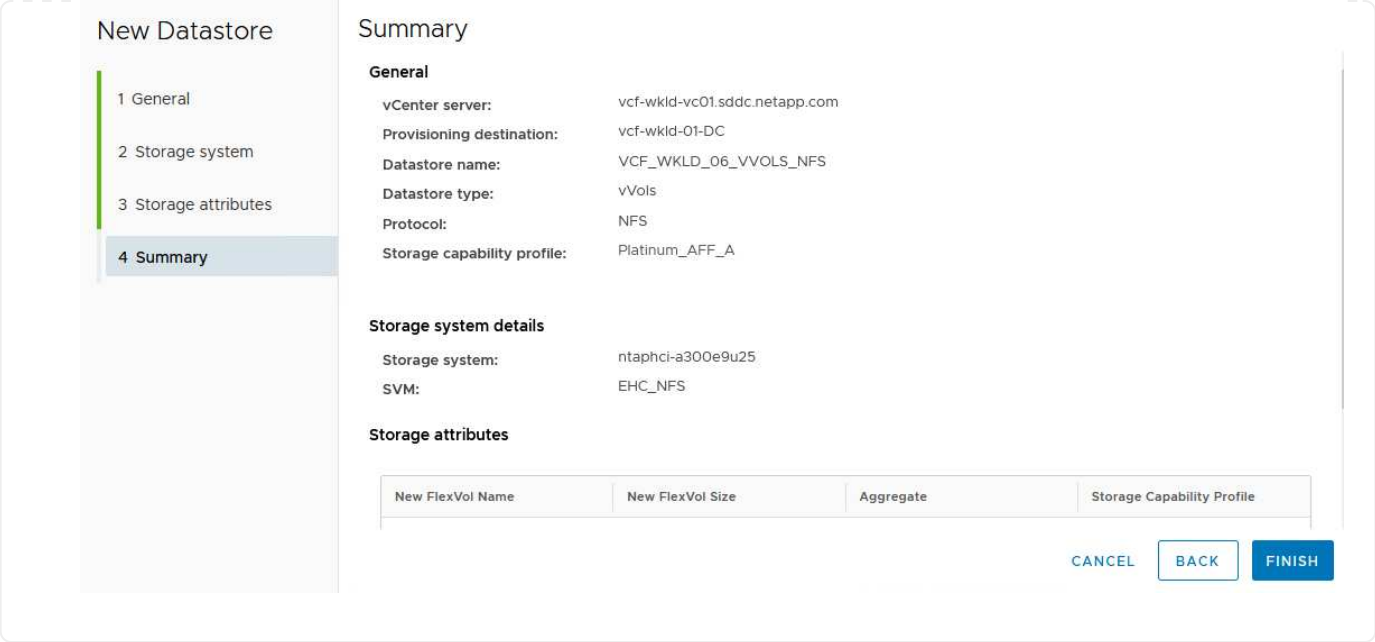
3. Nella pagina **Sistema di archiviazione** selezionare un profilo di capacità di archiviazione, il sistema di archiviazione e l'SVM. Fare clic su **Avanti** per continuare.



4. Nella pagina **Attributi di archiviazione** seleziona di creare un nuovo volume per il datastore e compila gli attributi di archiviazione del volume da creare. Fare clic su **Aggiungi** per creare il volume e poi su **Avanti** per continuare.



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



Informazioni aggiuntive

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" .

Aggiungere NVMe su TCP come storage supplementare ai domini dei carichi di lavoro VI

In questo caso d'uso descriviamo la procedura per utilizzare ONTAP Tools per VMware per configurare NVMe su TCP (NVMe/TCP) come storage supplementare per un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Questa procedura riassume la configurazione di una macchina virtuale di archiviazione (SVM) abilitata per NVMe/TCP, la creazione di namespace NVMe, la configurazione della rete host ESXi e la distribuzione di un datastore VMFS.

Vantaggi di NVMe rispetto a TCP

Prestazioni elevate: offre prestazioni eccezionali con bassa latenza e velocità di trasferimento dati elevate. Ciò è fondamentale per le applicazioni più esigenti e le operazioni sui dati su larga scala.

Scalabilità: supporta configurazioni scalabili, consentendo agli amministratori IT di espandere la propria infrastruttura senza problemi man mano che aumentano i requisiti dei dati.

Economico: funziona tramite switch Ethernet standard ed è incapsulato all'interno di datagrammi TCP. Non sono richieste attrezzature speciali per l'implementazione.

Per maggiori informazioni sui vantaggi di NVMe, fare riferimento a "Che cos'è NVME?"

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

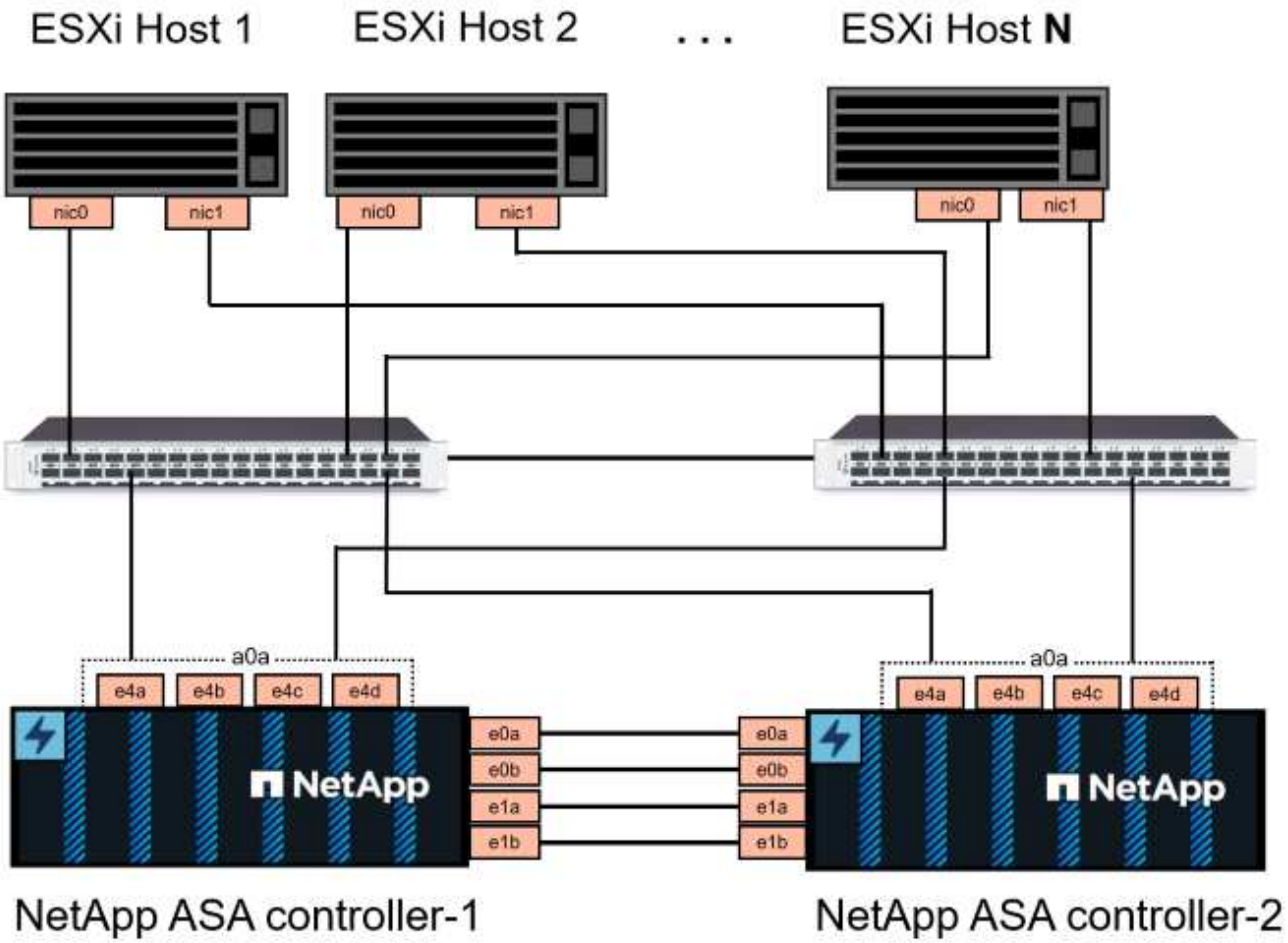
- Creare una macchina virtuale di archiviazione (SVM) con interfacce logiche (LIF) per il traffico NVMe/TCP.
- Creare gruppi di porte distribuiti per reti iSCSI sul dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Aggiungere adattatori NVMe/TCP sugli host ESXi.
- Distribuisci datastore NVMe/TCP.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o ASA con porte dati fisiche su switch Ethernet dedicate al traffico di archiviazione.
- La distribuzione del dominio di gestione VCF è completa e il client vSphere è accessibile.
- In precedenza è stato distribuito un dominio di carico di lavoro VI.

NetApp consiglia progettazioni di rete completamente ridondanti per NVMe/TCP. Il diagramma seguente illustra un esempio di configurazione ridondante, che garantisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. Fare riferimento a NetApp"Riferimento alla configurazione SAN" per ulteriori informazioni.



Per il multipathing e il failover su più percorsi, NetApp consiglia di disporre di almeno due LIF per nodo di storage in reti Ethernet separate per tutte le SVM nelle configurazioni NVMe/TCP.

Questa documentazione illustra il processo di creazione di una nuova SVM e di specifica delle informazioni sull'indirizzo IP per creare più LIF per il traffico NVMe/TCP. Per aggiungere nuovi LIF a un SVM esistente, fare riferimento a"Creare un LIF (interfaccia di rete)" .

Per ulteriori informazioni sulle considerazioni di progettazione NVMe per i sistemi di archiviazione ONTAP , fare riferimento a"Configurazione, supporto e limitazioni NVMe" .

Fasi di distribuzione

Per creare un datastore VMFS su un dominio di carico di lavoro VCF utilizzando NVMe/TCP, completare i seguenti passaggi.

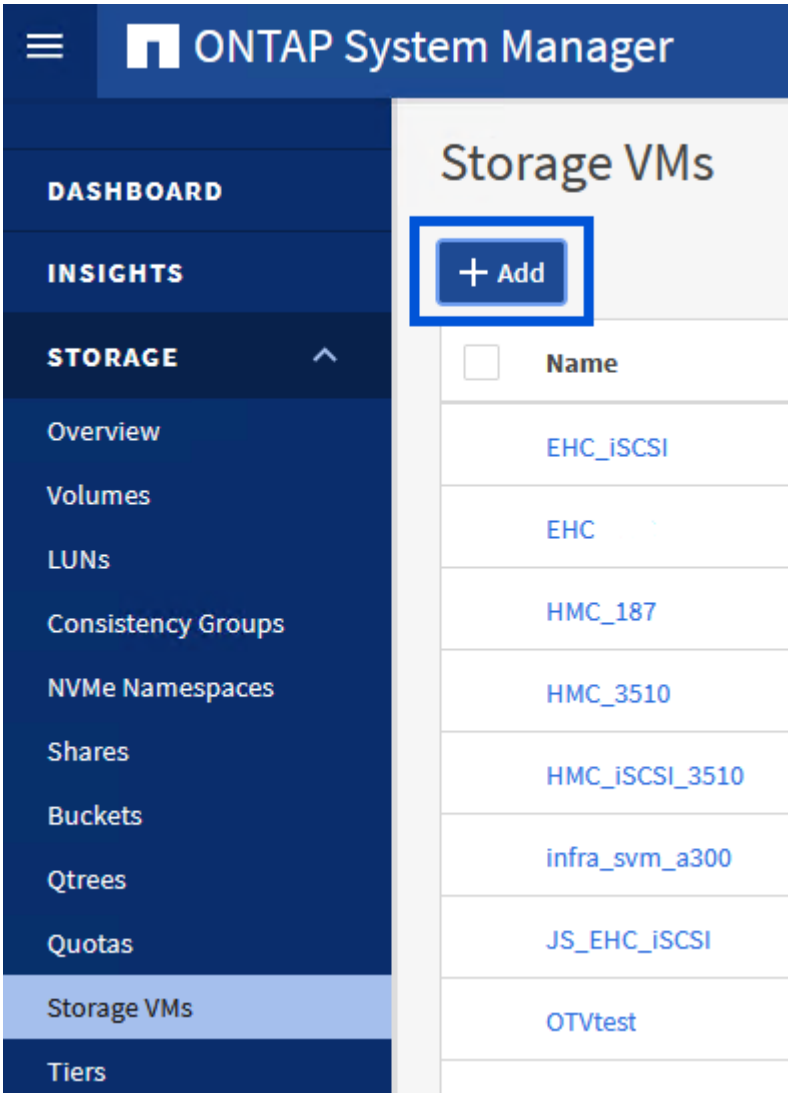
Crea SVM, LIF e namespace NVMe sul sistema di archiviazione ONTAP

Il passaggio seguente viene eseguito in ONTAP System Manager.

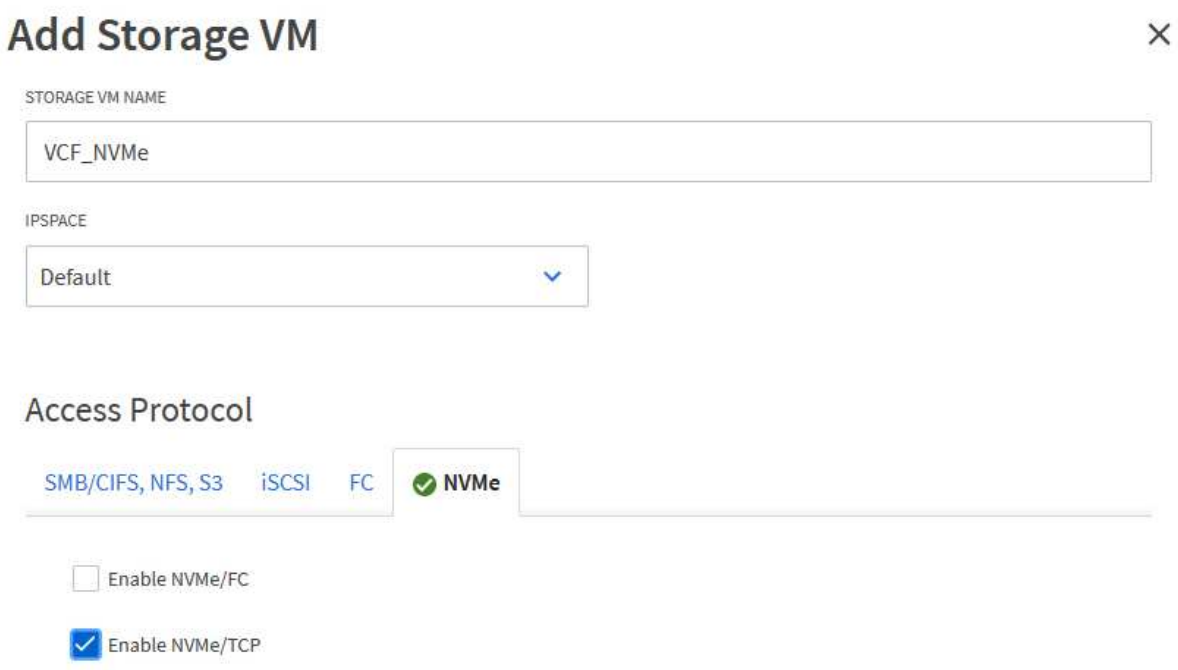
Creare la VM di archiviazione e i LIF

Completare i seguenti passaggi per creare una SVM insieme a più LIF per il traffico NVMe/TCP.

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

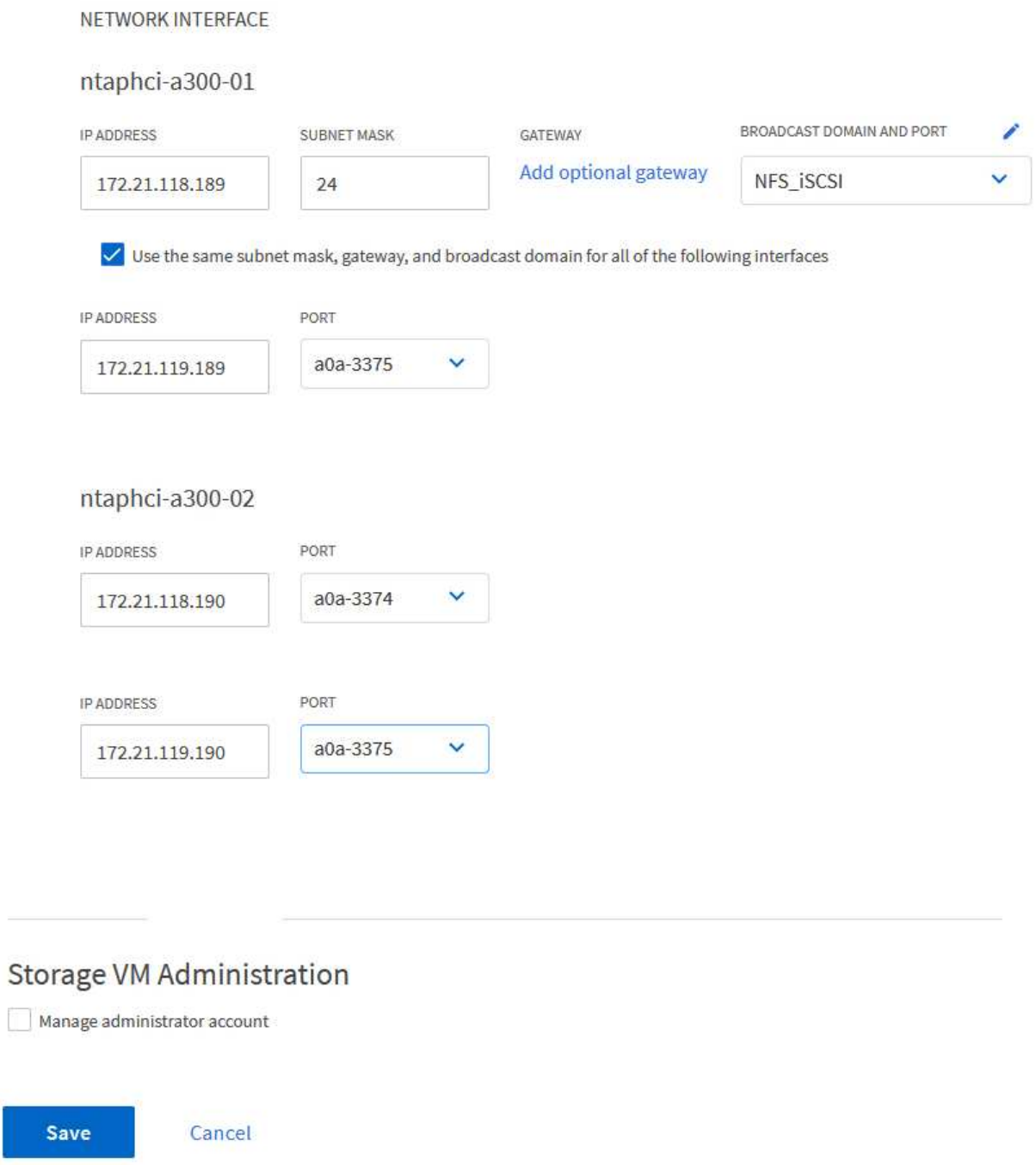


2. Nella procedura guidata **Aggiungi VM di archiviazione**, fornisci un **Nome** per la SVM, seleziona lo **Spazio IP** e quindi, in **Protocollo di accesso**, fai clic sulla scheda **NVMe** e seleziona la casella per **Abilita NVMe/TCP**.

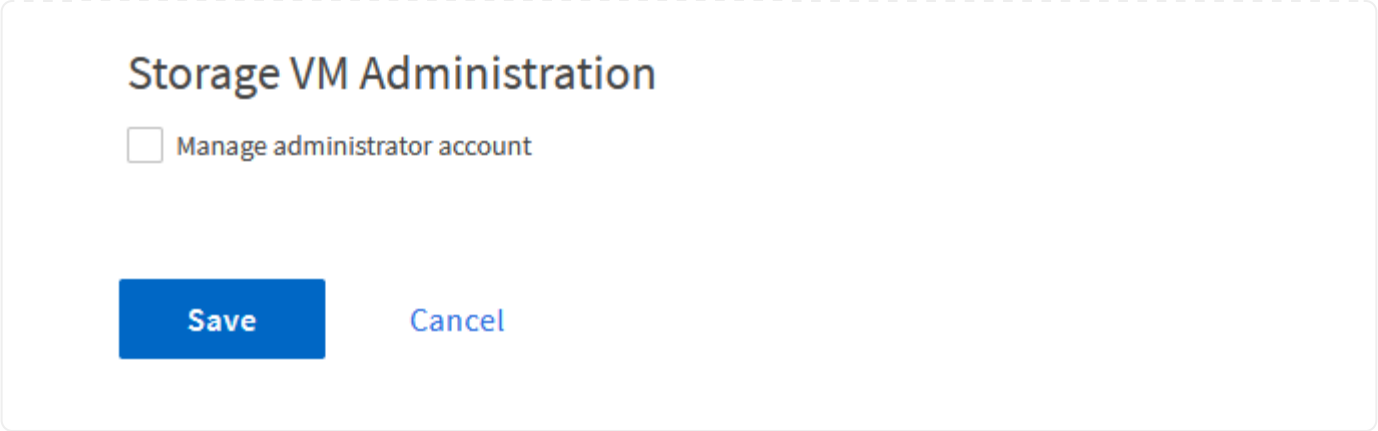


3. Nella sezione **Interfaccia di rete** compilare **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, la casella di controllo può essere abilitata per utilizzare impostazioni comuni a tutti i LIF rimanenti oppure per utilizzare impostazioni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

> Per il multipathing e il failover su più percorsi, NetApp consiglia di disporre di almeno due LIF per nodo di storage in reti Ethernet separate per tutte le SVM nelle configurazioni NVMe/TCP.



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.


Storage VM Administration
Manage administrator account
Save
Cancel

Creare lo spazio dei nomi NVMe

Gli spazi dei nomi NVMe sono analoghi ai LUN per iSCSi o FC. È necessario creare lo spazio dei nomi NVMe prima di poter distribuire un datastore VMFS da vSphere Client. Per creare lo spazio dei nomi NVMe, è necessario prima ottenere il nome qualificato NVMe (NQN) da ciascun host ESXi nel cluster. L'NQN viene utilizzato da ONTAP per fornire il controllo di accesso allo spazio dei nomi.

Per creare uno spazio dei nomi NVMe, completare i seguenti passaggi:

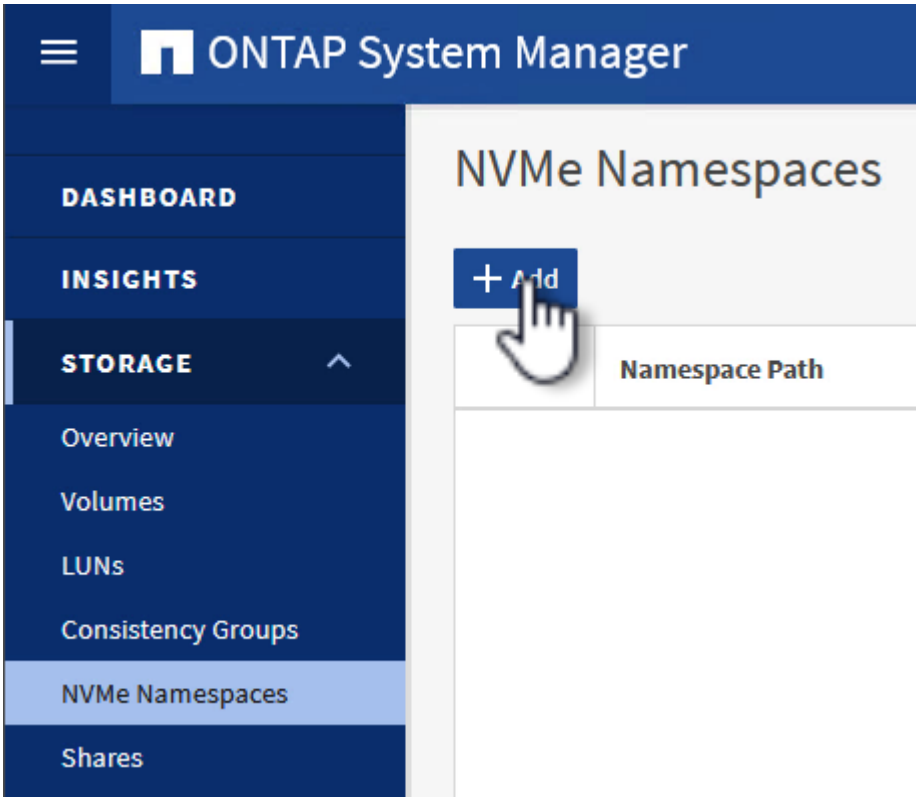
1. Aprire una sessione SSH con un host ESXi nel cluster per ottenere il suo NQN. Utilizzare il seguente comando dalla CLI:

   ```
   esxcli nvme info get
   ```

   Dovrebbe essere visualizzato un output simile al seguente:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

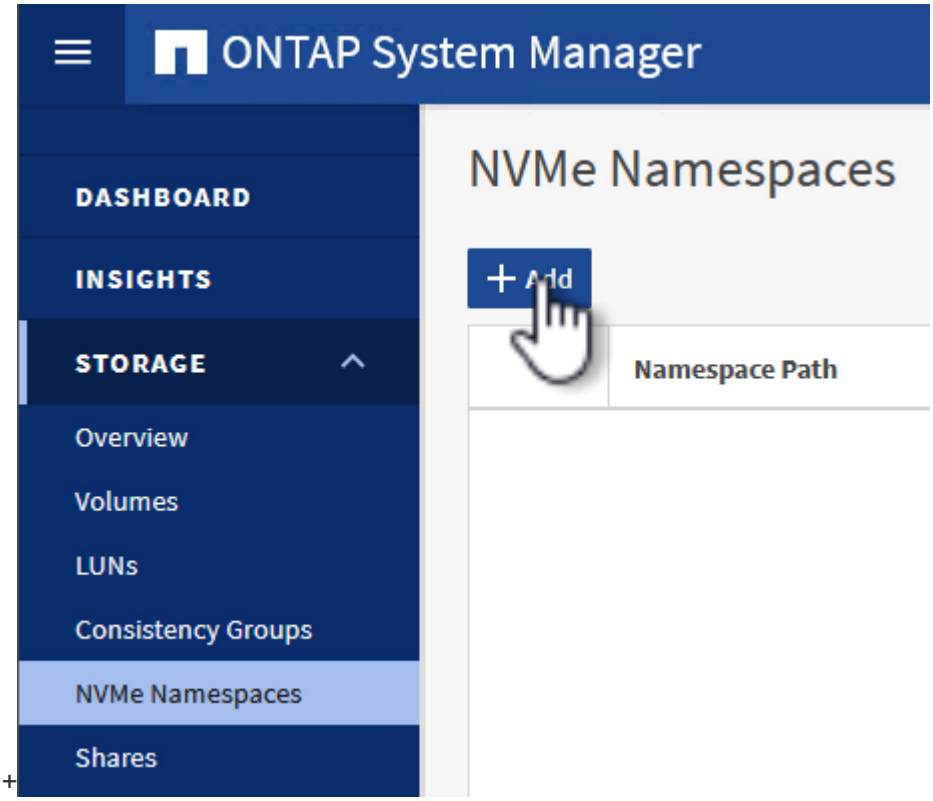
2. Registrare l'NQN per ciascun host ESXi nel cluster
3. Da ONTAP System Manager, vai su **NVMe Namespaces** nel menu a sinistra e clicca su **+ Aggiungi** per iniziare.



4. Nella pagina **Aggiungi spazio dei nomi NVMe**, inserisci un prefisso del nome, il numero di spazi dei nomi da creare, la dimensione dello spazio dei nomi e il sistema operativo host che accederà allo

spazio dei nomi. Nella sezione **Host NQN** creare un elenco separato da virgole degli NQN precedentemente raccolti dagli host ESXi che accederanno agli spazi dei nomi.

Fare clic su **Altre opzioni** per configurare elementi aggiuntivi, come il criterio di protezione degli snapshot. Infine, fare clic su **Salva** per creare lo spazio dei nomi NVMe.



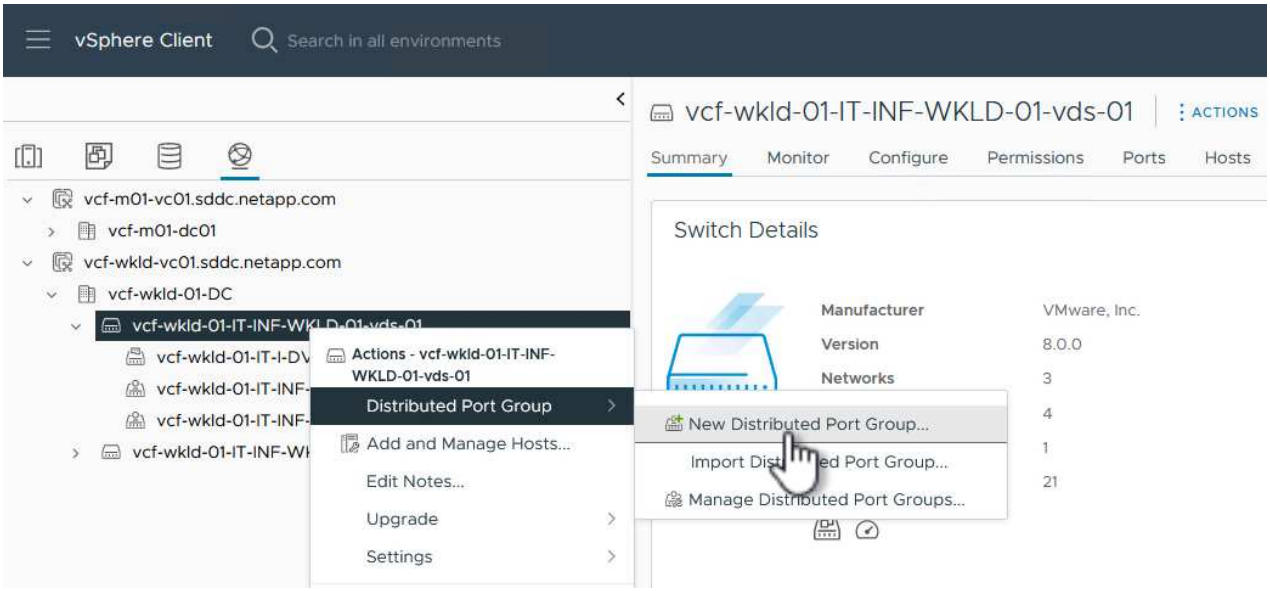
Configurare adattatori software di rete e NVMe sugli host ESXi

I passaggi seguenti vengono eseguiti sul cluster del dominio del carico di lavoro VI utilizzando il client vSphere. In questo caso viene utilizzato vCenter Single Sign-On, quindi il client vSphere è comune sia al dominio di gestione che a quello del carico di lavoro.

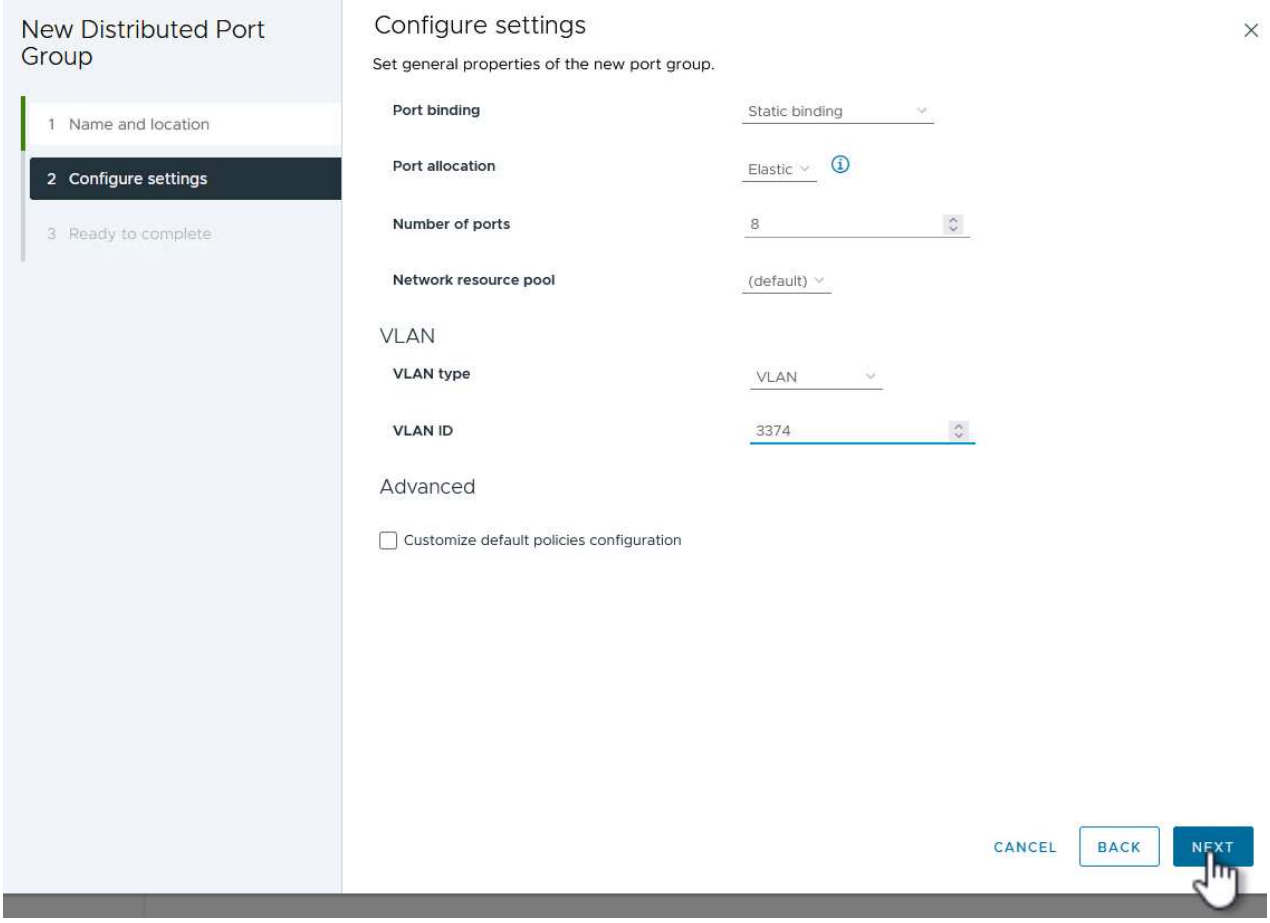
Creare gruppi di porte distribuiti per il traffico NVME/TCP

Completare quanto segue per creare un nuovo gruppo di porte distribuito per ogni rete NVMe/TCP:

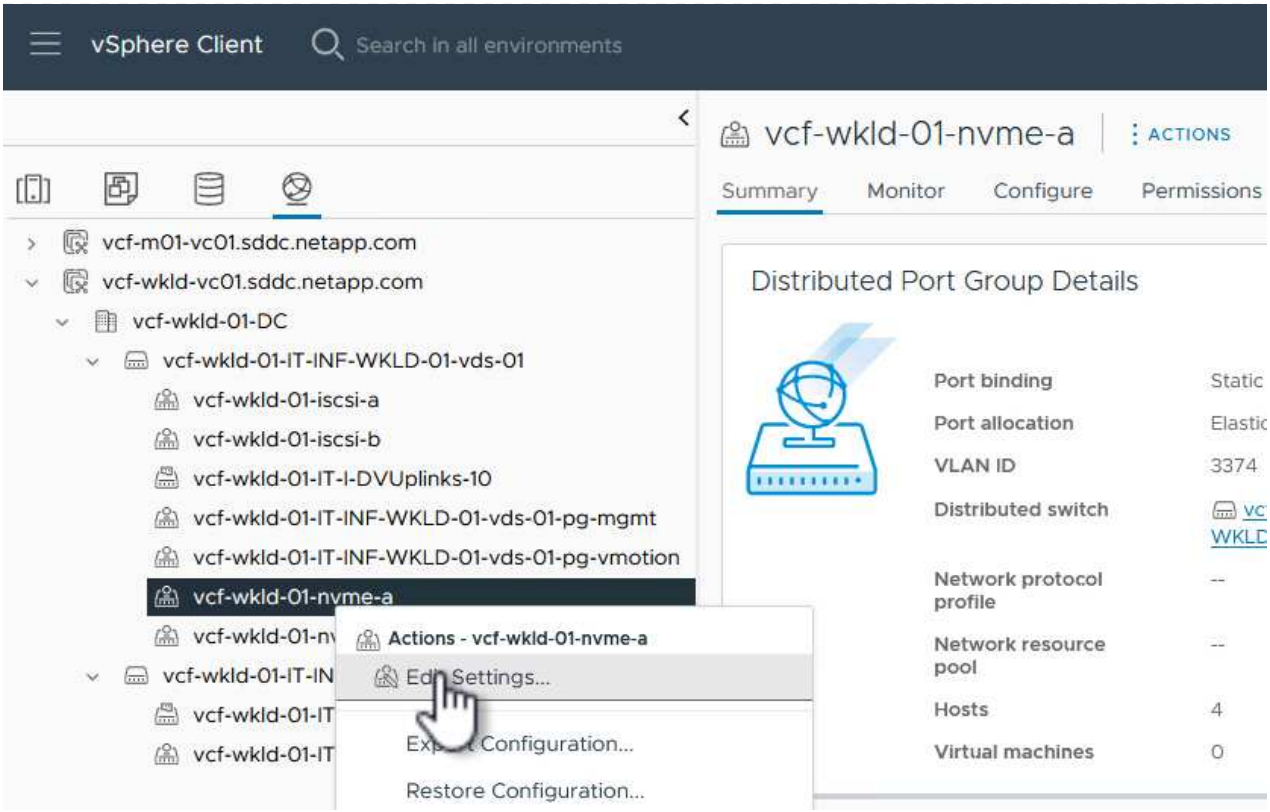
1. Dal client vSphere, accedere a **Inventario > Rete** per il dominio del carico di lavoro. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite…**.



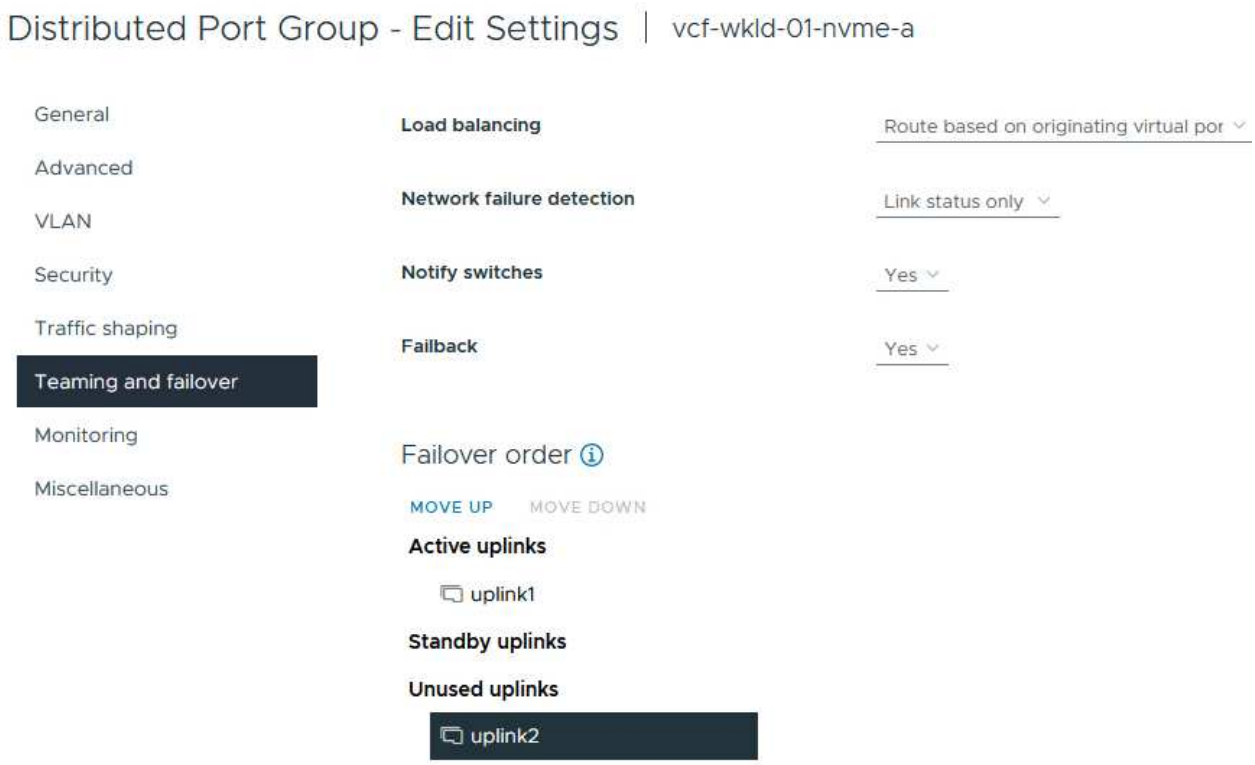
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, immettere un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare 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. Ripetere questa procedura per creare un gruppo di porte distribuito per la seconda rete NVMe/TCP utilizzata e assicurarsi di aver immesso l'**ID VLAN** corretto.
6. Una volta creati entrambi i gruppi di porte, passare al primo gruppo di porte e selezionare l'azione **Modifica impostazioni…**.

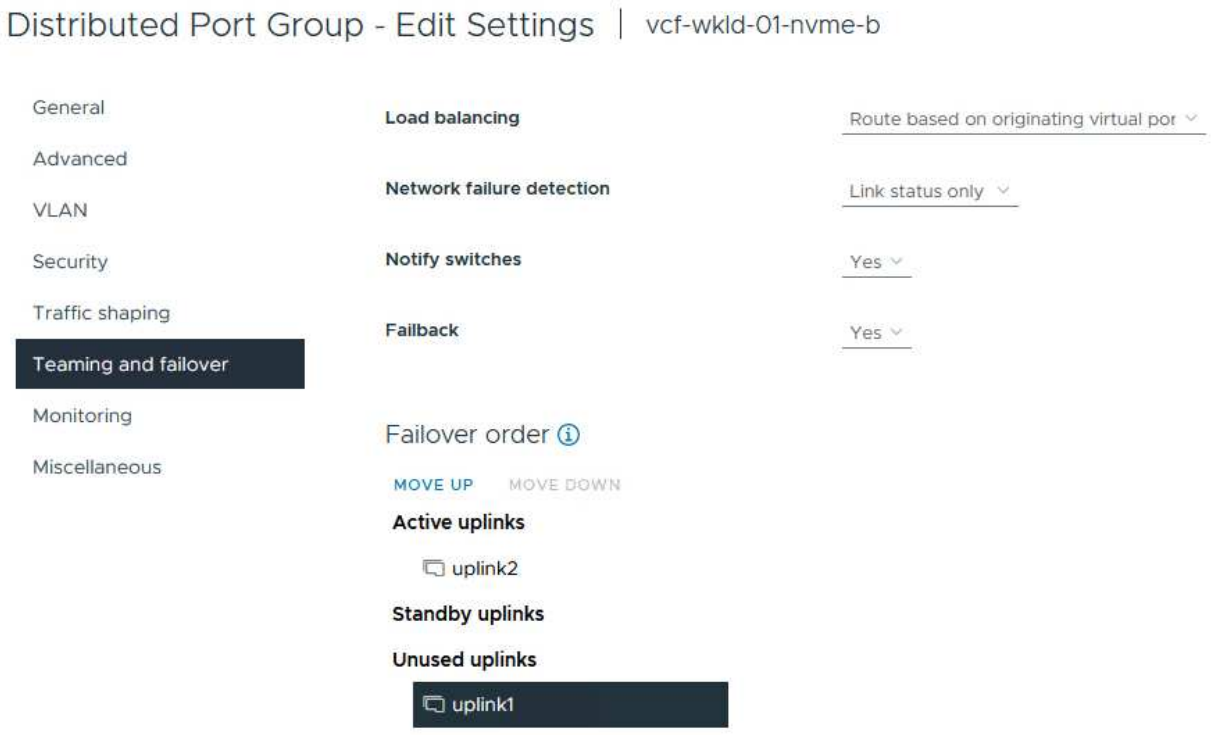


7. Nella pagina **Gruppo di porte distribuite - Modifica impostazioni**, vai su **Teaming e failover** nel menu a sinistra e fai clic su **uplink2** per spostarlo in basso a **Uplink non utilizzati**.



8. Ripetere questo passaggio per il secondo gruppo di porte NVMe/TCP. Questa volta, però, sposta

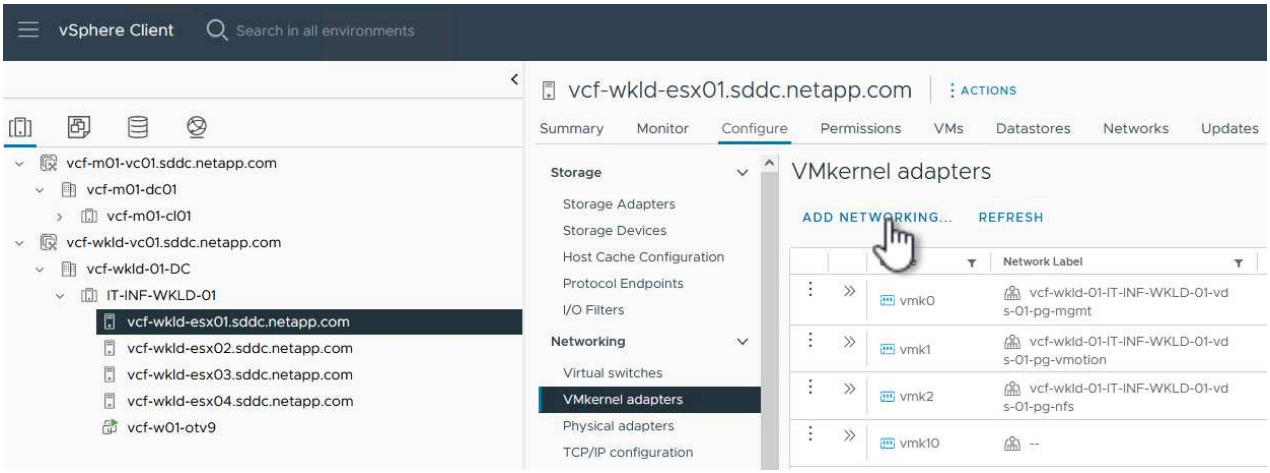
uplink1 in **Uplink non utilizzati**.



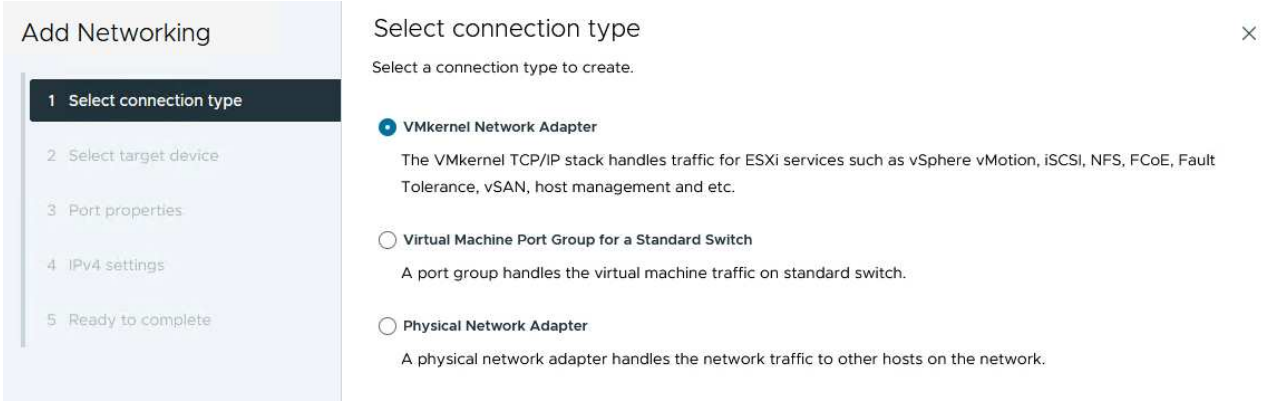
Creare adattatori VMkernel su ciascun host ESXi

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

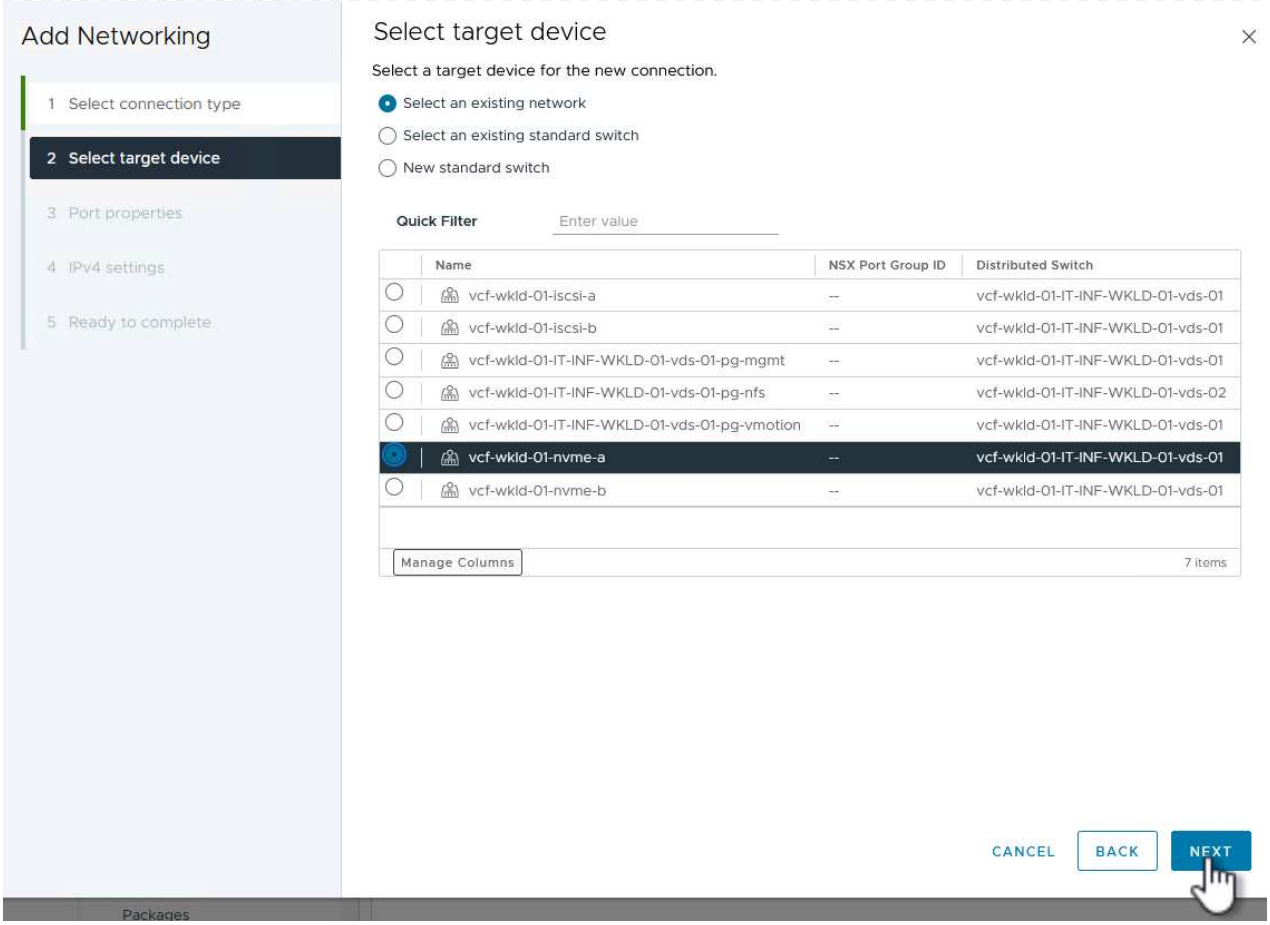
1. Dal client vSphere, passare a uno degli host ESXi nell'inventario del dominio del carico di lavoro. Dalla scheda **Configura** seleziona **Schede VMkernel** e clicca su **Aggiungi rete…** per iniziare.



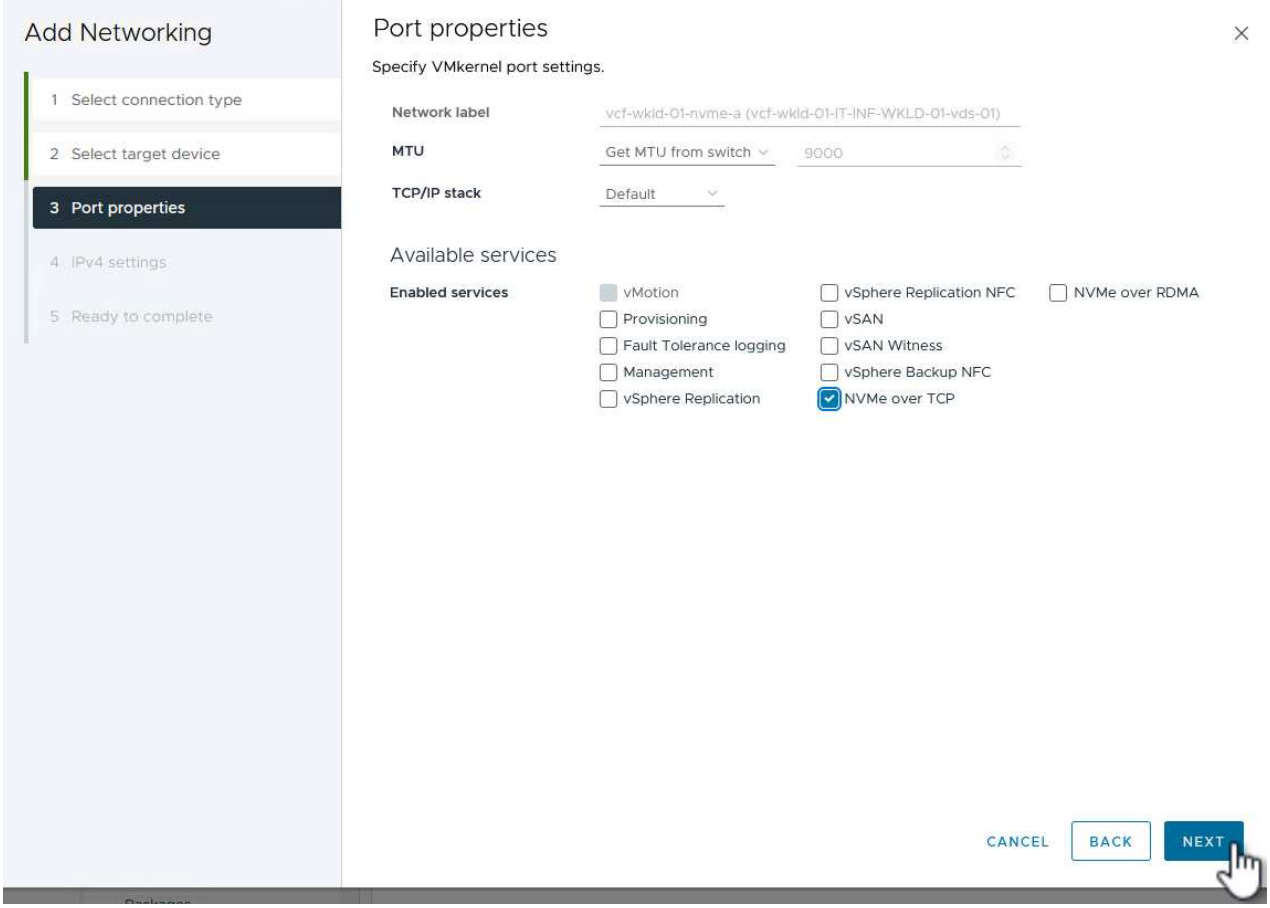
2. Nella finestra **Seleziona tipo di connessione** seleziona **Scheda di rete VMkernel** e fai clic su **Avanti** per continuare.



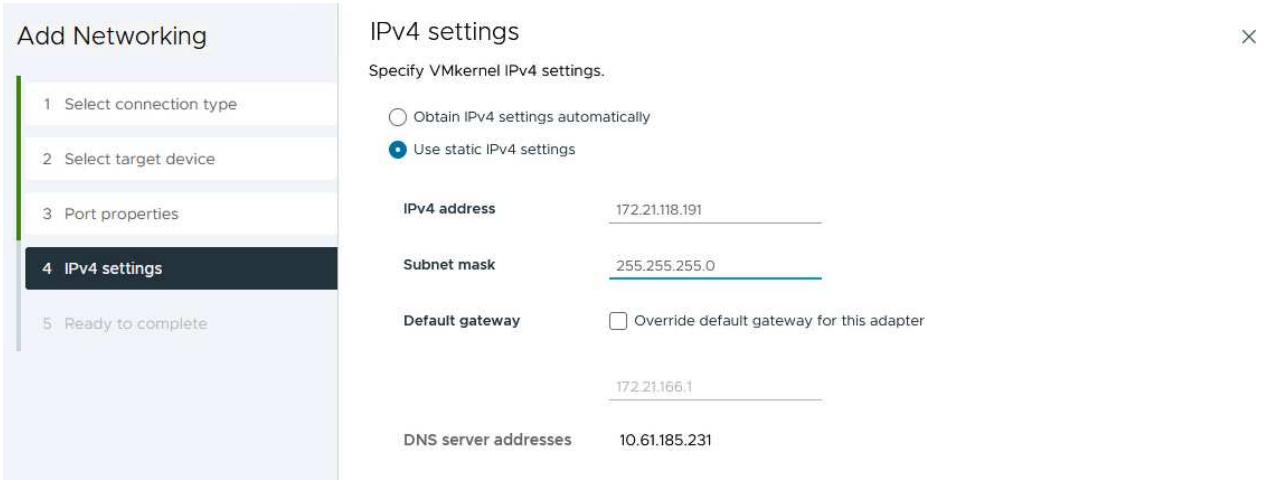
3. Nella pagina **Seleziona dispositivo di destinazione**, seleziona uno dei gruppi di porte distribuite per iSCSI creati in precedenza.



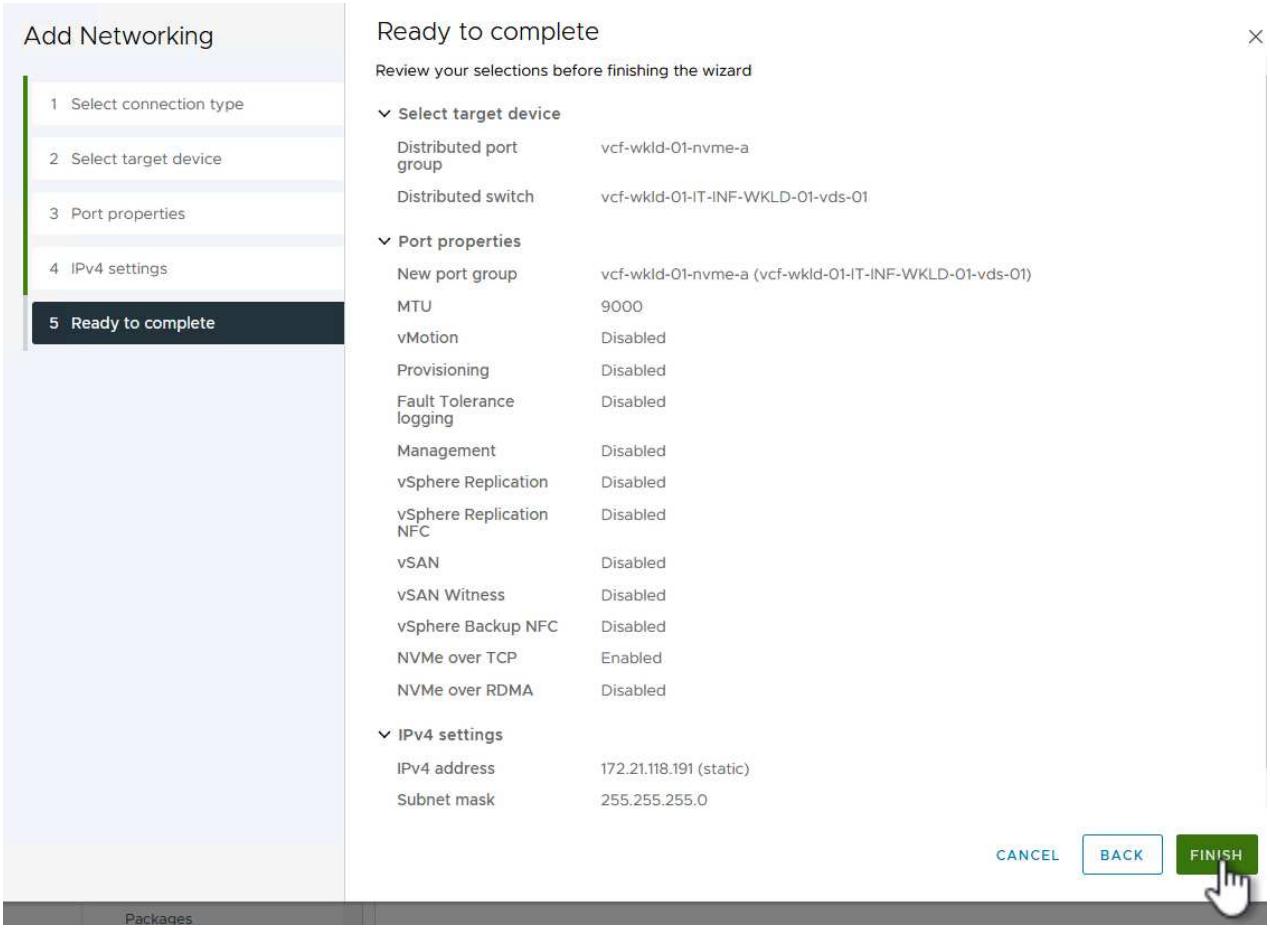
4. Nella pagina **Proprietà porta** fare clic sulla casella **NVMe su TCP** e fare clic su **Avanti** per continuare.



5. Nella pagina **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.



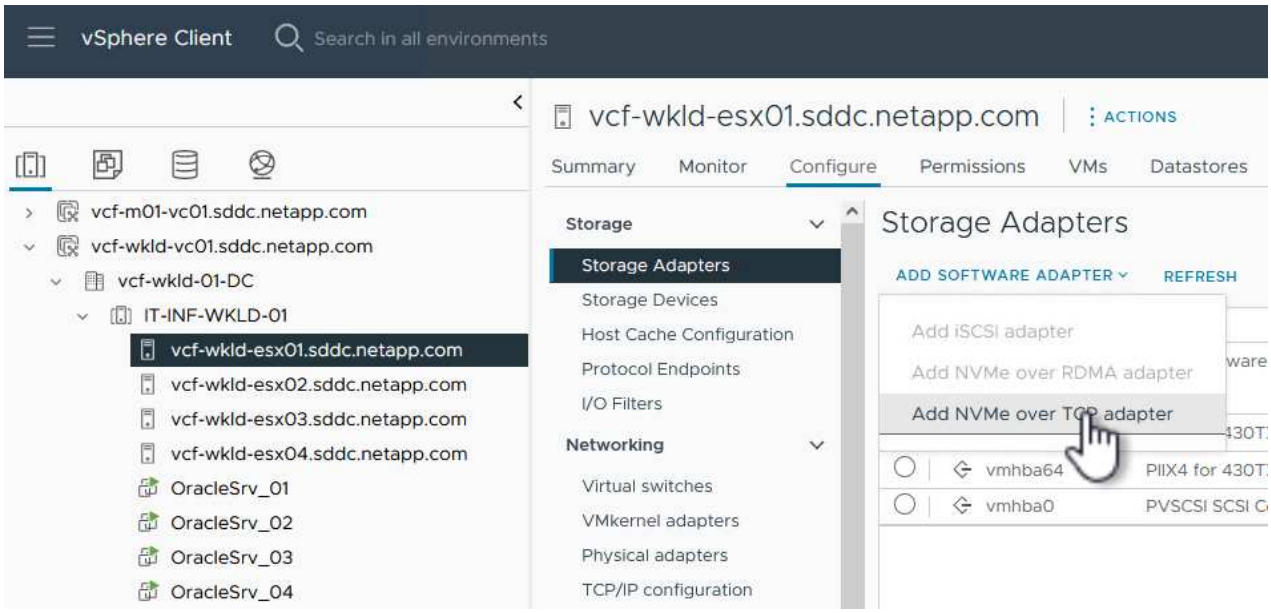
7. Ripetere questo processo per creare un adattatore VMkernel per la seconda rete iSCSI.

Aggiungi adattatore NVMe su TCP

Ogni host ESXi nel cluster del dominio del carico di lavoro deve disporre di un adattatore software NVMe su TCP installato per ogni rete NVMe/TCP stabilita dedicata al traffico di archiviazione.

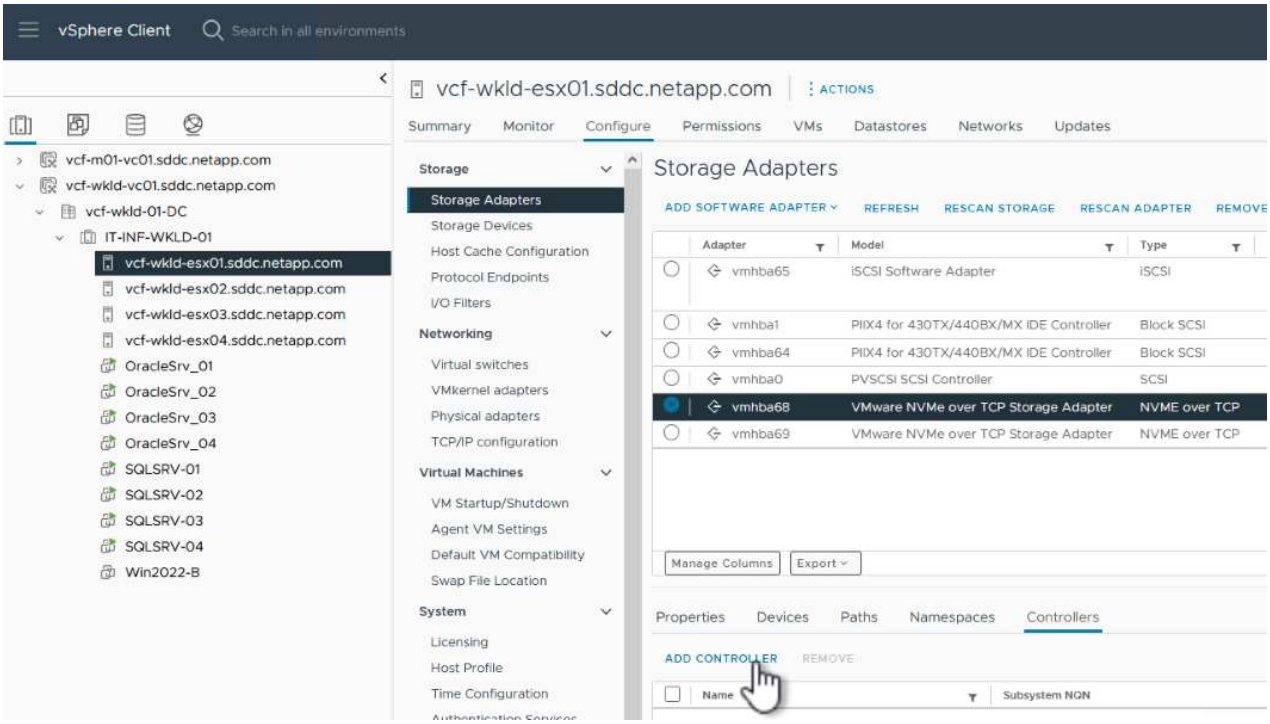
Per installare gli adattatori NVMe su TCP e rilevare i controller NVMe, completare i seguenti passaggi:

1. Nel client vSphere, passare a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dalla scheda **Configura** fare clic su **Schede di archiviazione** nel menu e quindi, dal menu a discesa **Aggiungi adattatore software**, selezionare **Aggiungi adattatore NVMe su TCP**.

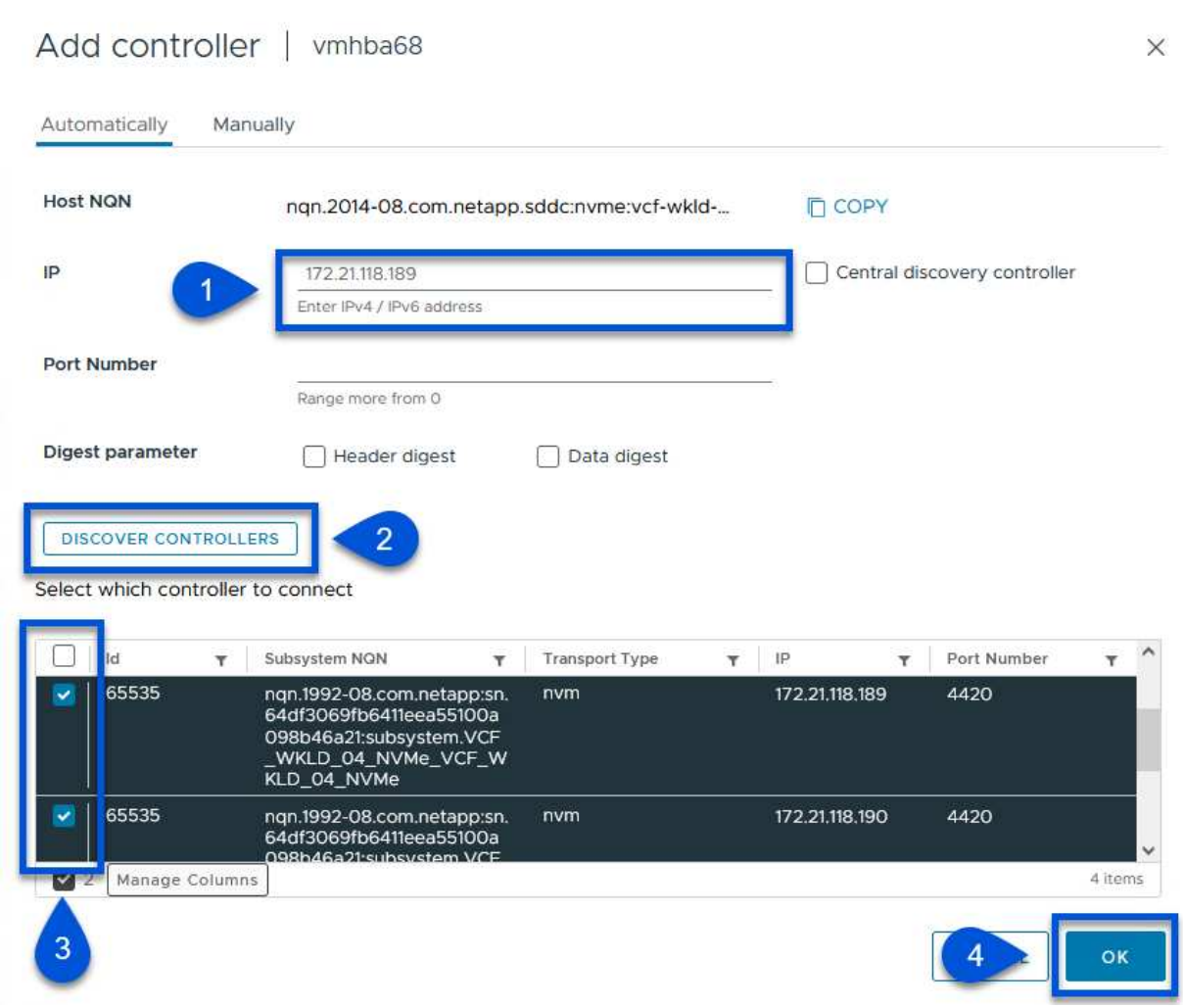


2. Nella finestra **Aggiungi adattatore software NVMe su TCP**, accedi al menu a discesa **Scheda di rete fisica** e seleziona la scheda di rete fisica corretta su cui abilitare l'adattatore NVMe.

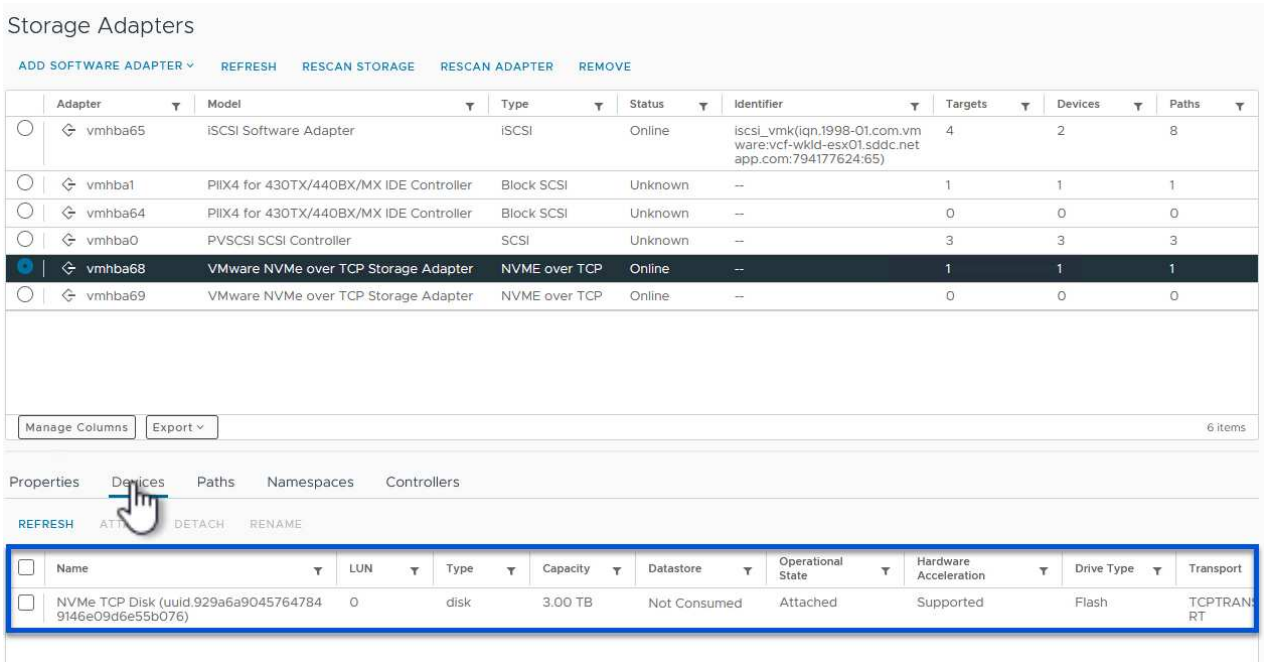
3. Ripetere questa procedura per la seconda rete assegnata a NVMe tramite traffico TCP, assegnando l'adattatore fisico corretto.
4. Selezionare uno degli adattatori NVMe su TCP appena installati e, nella scheda **Controller**, selezionare **Aggiungi controller**.



5. Nella finestra **Aggiungi controller**, seleziona la scheda **Automaticamente** e completa i seguenti passaggi.
   - Inserire un indirizzo IP per una delle interfacce logiche SVM sulla stessa rete dell'adattatore fisico assegnato a questo adattatore NVMe su TCP.
   - Fare clic sul pulsante **Scopri controller**.
   - Dall'elenco dei controller rilevati, fare clic sulla casella di controllo per i due controller con indirizzi di rete allineati con questo adattatore NVMe su TCP.
   - Fare clic sul pulsante **OK** per aggiungere i controller selezionati.



6. Dopo alcuni secondi dovresti vedere lo spazio dei nomi NVMe apparire nella scheda Dispositivi.

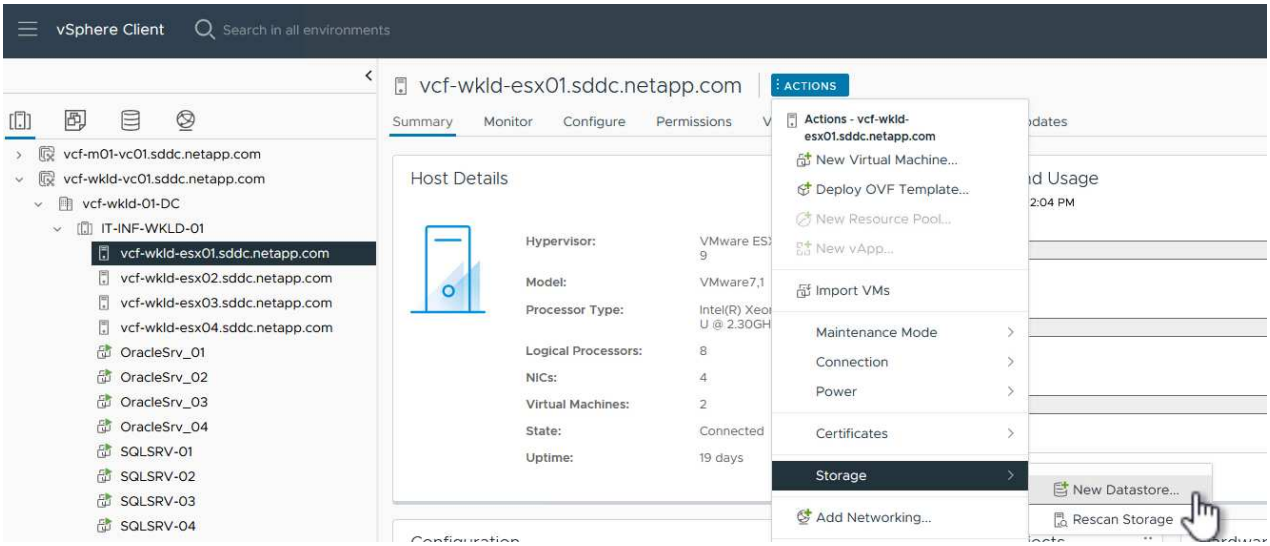


7. Ripetere questa procedura per creare un adattatore NVMe su TCP per la seconda rete stabilita per il traffico NVMe/TCP.

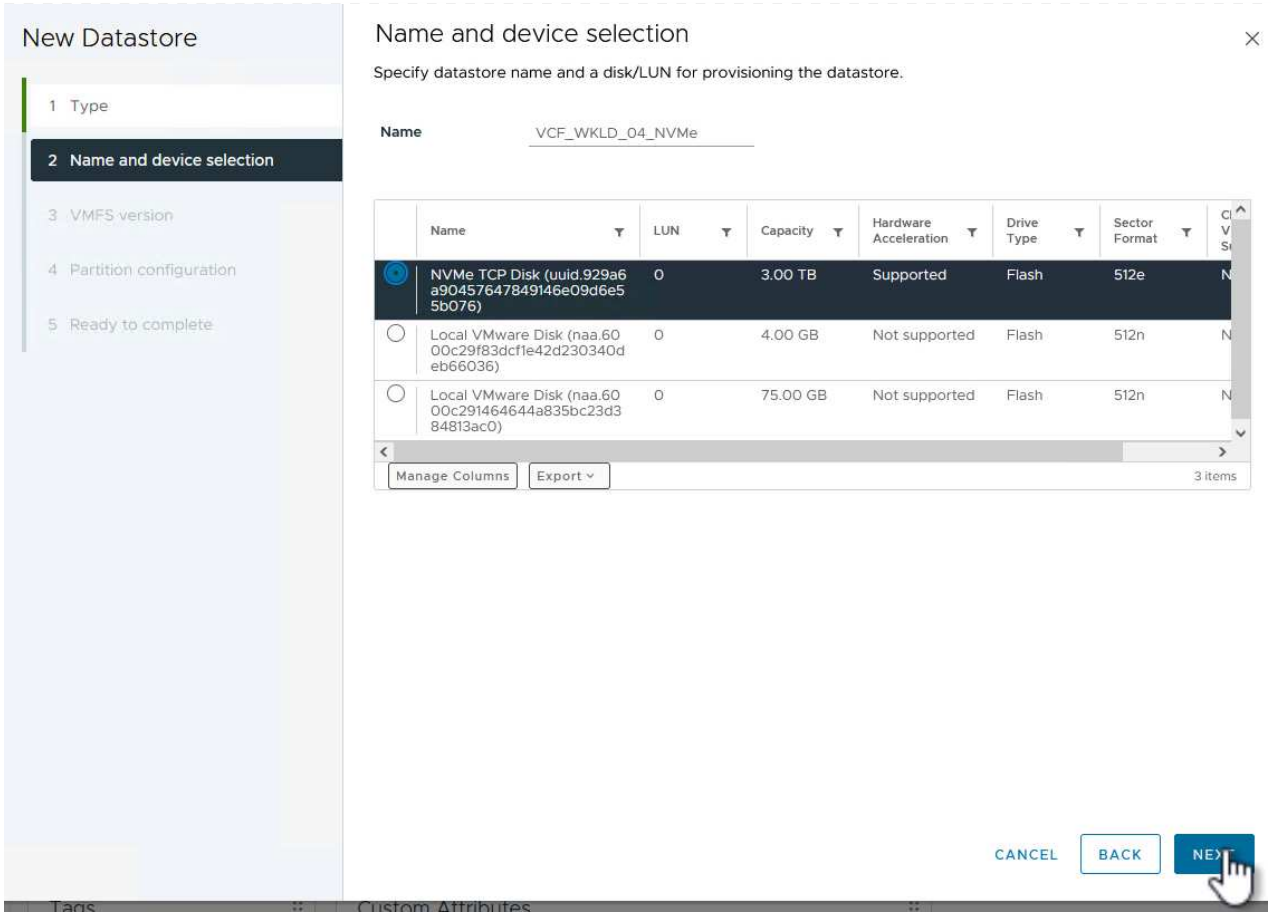
Distribuisci NVMe su datastore TCP

Per creare un datastore VMFS sullo spazio dei nomi NVMe, completare i seguenti passaggi:

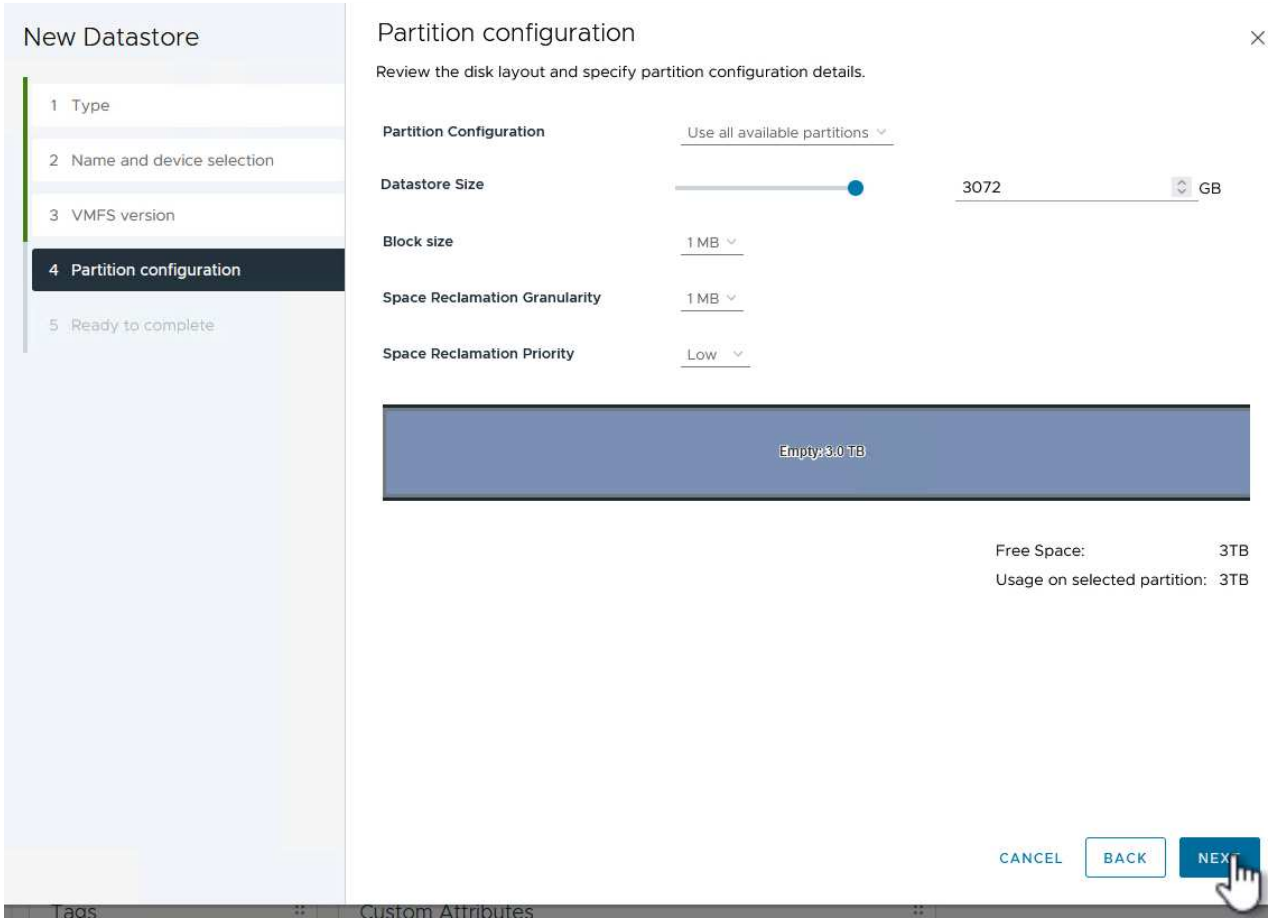
1. Nel client vSphere, passare a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dal menu **Azioni** selezionare **Archiviazione > Nuovo datastore…**.



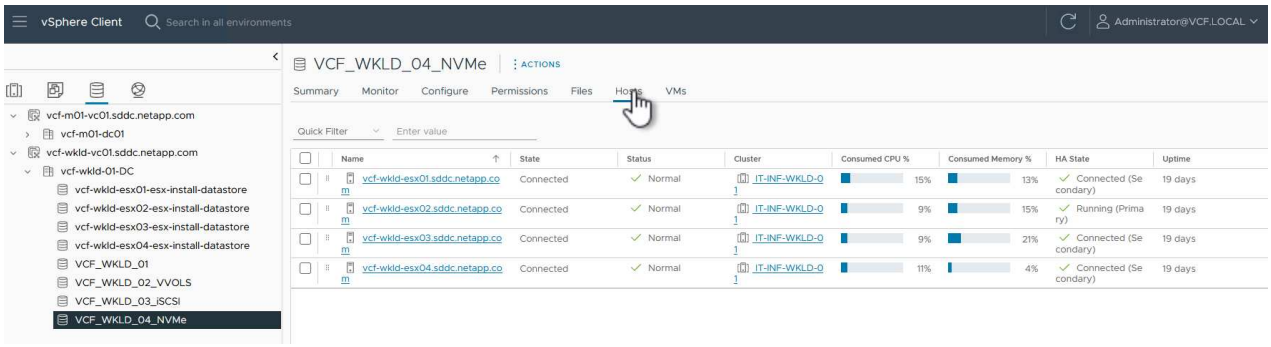
2. Nella procedura guidata **Nuovo datastore**, selezionare **VMFS** come tipo. Fare clic su **Avanti** per continuare.
3. Nella pagina **Selezione nome e dispositivo**, specificare un nome per il datastore e selezionare lo spazio dei nomi NVMe dall'elenco dei dispositivi disponibili.



4. Nella pagina **Versione VMFS** selezionare la versione di VMFS per il datastore.
5. Nella pagina **Configurazione partizione**, apportare le modifiche desiderate allo schema di partizione predefinito. Fare clic su **Avanti** per continuare.



6. Nella pagina **Pronto per il completamento**, rivedere il riepilogo e fare clic su **Fine** per creare il datastore.
7. Passare al nuovo datastore nell'inventario e fare clic sulla scheda **Host**. Se configurati correttamente, tutti gli host ESXi nel cluster dovrebbero essere elencati e avere accesso al nuovo datastore.



Informazioni aggiuntive

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" .

Aggiungere un datastore VMFS basato su FC come storage supplementare ai domini dei carichi di lavoro VI

In questo caso d'uso descriviamo la procedura per configurare un datastore VMFS utilizzando Fibre Channel (FC) come storage supplementare per un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Questa procedura riassume la distribuzione di ONTAP Tools per VMware vSphere, la registrazione del server vCenter del carico di lavoro VI, la definizione del backend di storage e il provisioning del datastore FC.

Vantaggi del Fibre Channel

Prestazioni elevate: FC garantisce velocità di trasferimento dati elevate, rendendolo ideale per applicazioni che richiedono un accesso rapido e affidabile a grandi quantità di dati.

Bassa latenza: Latenza molto bassa, fondamentale per le applicazioni che richiedono prestazioni elevate, come database e ambienti virtualizzati.

Affidabilità: le reti FC sono note per la loro robustezza e affidabilità, con funzionalità quali ridondanza integrata e correzione degli errori.

Larghezza di banda dedicata: FC fornisce larghezza di banda dedicata per il traffico di archiviazione, riducendo il rischio di congestione della rete.

Per ulteriori informazioni sull'utilizzo di Fibre Channel con i sistemi di storage NetApp , fare riferimento a "Provisioning SAN con FC" .

Panoramica dello scenario

Il datastore supplementare VCF viene fornito come parte delle operazioni del giorno 2 tramite vCenter. Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuzione degli strumenti ONTAP sul dominio di gestione
- Registra i server vCenter del carico di lavoro VI negli strumenti ONTAP
- Definisci il backend di archiviazione sul plugin degli strumenti ONTAP per VMware vSphere
- Fornire VMFS sul trasporto FC

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP AFF o ASA con porte FC collegate a switch FC.
- SVM creato con FC lifs.
- vSphere con HBA FC collegati agli switch FC.
- Sugli switch FC è configurata la suddivisione in zone con singolo iniziatore-destinazione.

> Utilizzare l'interfaccia logica FC SVM nella configurazione della zona anziché le porte FC fisiche sui sistemi ONTAP .

NetApp consiglia il multipath per le LUN FC.

Per informazioni complete sulla configurazione del canale in fibra sui sistemi di archiviazione ONTAP , fare riferimento a "Gestione dello storage SAN" nella documentazione ONTAP 9.

Per ulteriori informazioni sull'utilizzo di VMFS con sistemi di archiviazione ONTAP , fare riferimento a"Guida alla distribuzione per VMFS" .

Fasi di distribuzione per il dominio del carico di lavoro VI

Per distribuire ONTAP Tools e utilizzarlo per creare un datastore VMFS sul dominio del carico di lavoro VCF VI, completare i seguenti passaggi:

- "Registra il carico di lavoro VI vCenter per abilitare il plugin vCenter"
- "Definisci il backend di archiviazione utilizzando l'interfaccia client vSphere"
- "Provisioning VMFS su FC"

Informazioni aggiuntive

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" .

Demo video per questa soluzione

Datastore VMFS(FC) come storage supplementare per il dominio di gestione VCF

Proteggi VCF con SnapCenter

Scopri come proteggere i domini dei carichi di lavoro VCF con il plug-in SnapCenter per VMware vSphere

Scopri le soluzioni NetApp che puoi utilizzare per proteggere i carichi di lavoro VMware Cloud Foundation (VCF) con SnapCenter Plug-in for VMware vSphere. Questo plug-in semplifica il backup e il ripristino, garantendo backup coerenti con le applicazioni e ottimizzando lo storage con le tecnologie di efficienza di NetApp.

Supporta flussi di lavoro automatizzati e operazioni scalabili, garantendo al contempo un'integrazione perfetta con il client vSphere. Grazie alla replica SnapMirror che fornisce un backup secondario in sede o sul cloud, garantisce una solida protezione dei dati ed efficienza operativa negli ambienti virtualizzati.

Per maggiori dettagli fare riferimento alle seguenti soluzioni.

- "Proteggi il dominio del carico di lavoro VCF"
- "Proteggere più domini di carico di lavoro VCF"

- "Proteggi il dominio del carico di lavoro VCF con NVMe"
- "Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM"

Proteggi un dominio di carico di lavoro VCF con il plug-in SnapCenter per VMware vSphere

In questo caso d'uso descriviamo la procedura per utilizzare il plug-in SnapCenter per VMware vSphere per eseguire il backup e il ripristino di VM e datastore in un dominio di carico di lavoro VMware Cloud Foundation (VCF). Questa procedura riassume l'implementazione del plug-in SnapCenter per VMware vSphere, l'aggiunta di sistemi di storage, la creazione di policy di backup e l'esecuzione di ripristini di VM e file.

In questa soluzione, come protocollo di archiviazione per il datastore VMFS viene utilizzato **iSCSI**.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuire il SnapCenter Plug-in for VMware vSphere (SCV) sul dominio del carico di lavoro VI.
- Aggiungere sistemi di archiviazione a SCV.
- Creare policy di backup in SCV.
- Creare gruppi di risorse in SCV.
- Utilizzare SCV per eseguire il backup di datastore o VM specifiche.
- Utilizzare SCV per ripristinare le VM in una posizione alternativa nel cluster.
- Utilizzare SCV per ripristinare i file in un file system Windows.

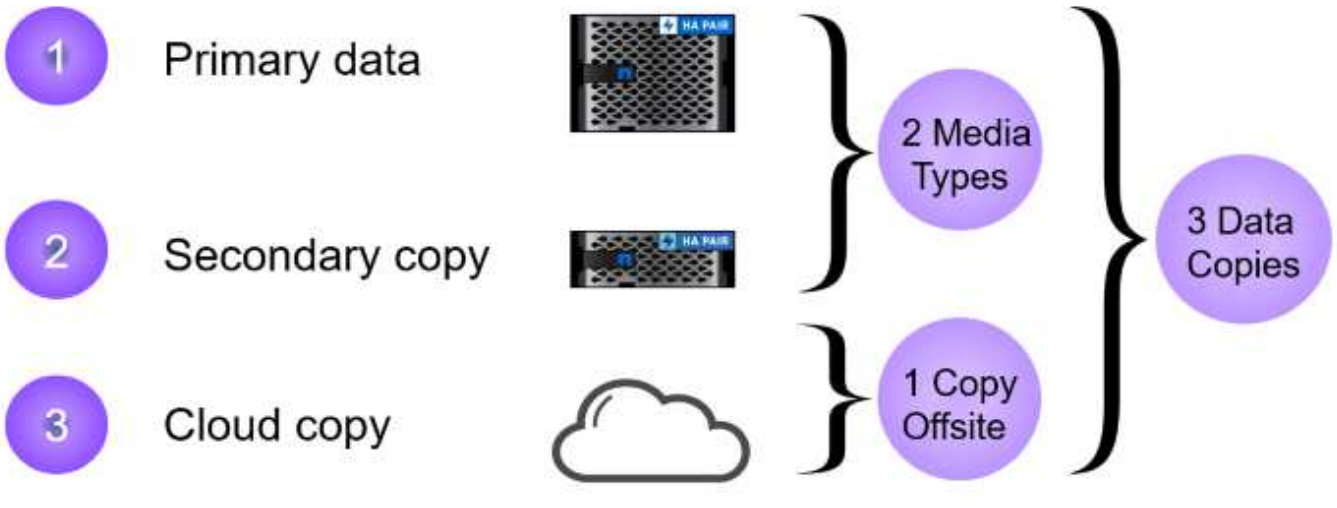
Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di archiviazione ONTAP ASA con datastore iSCSI VMFS assegnati al cluster del dominio del carico di lavoro.
- Un sistema di archiviazione ONTAP secondario configurato per ricevere backup secondari tramite SnapMirror.
- La distribuzione del dominio di gestione VCF è completa e il client vSphere è accessibile.
- In precedenza è stato distribuito un dominio di carico di lavoro VI.
- Le macchine virtuali sono presenti sul cluster che SCV è designato a proteggere.

Per informazioni sulla configurazione dei datastore iSCSI VMFS come storage supplementare, fare riferimento a"**iSCSI come storage supplementare per i domini di gestione che utilizzano ONTAP Tools per VMware**" in questa documentazione. Il processo per utilizzare OTV per distribuire gli archivi dati è identico per i domini di gestione e di carico di lavoro.

Oltre a replicare i backup eseguiti con SCV su un archivio secondario, è possibile effettuare copie offsite dei dati su un archivio di oggetti su uno dei tre (3) principali provider cloud utilizzando il BlueXP backup and recovery NetApp BlueXP per VM. Per maggiori informazioni fare riferimento alla soluzione"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM" .



Fasi di distribuzione

Per distribuire il plug-in SnapCenter e utilizzarlo per creare backup e ripristinare VM e datastore, completare i seguenti passaggi:

Distribuire e utilizzare SCV per proteggere i dati in un dominio di carico di lavoro VI

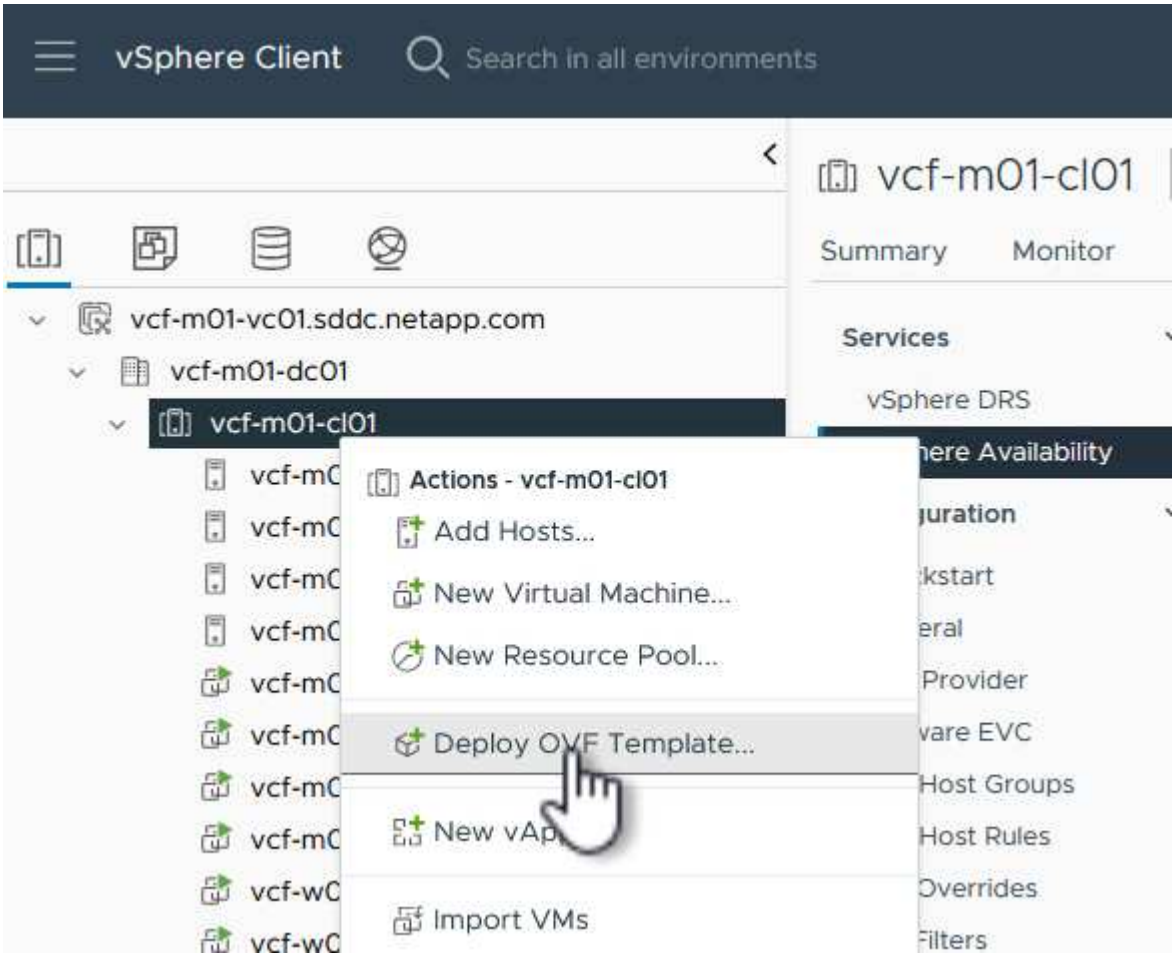
Completare i seguenti passaggi per distribuire, configurare e utilizzare SCV per proteggere i dati in un dominio di carico di lavoro VI:

Distribuisci il SnapCenter Plug-in for VMware vSphere

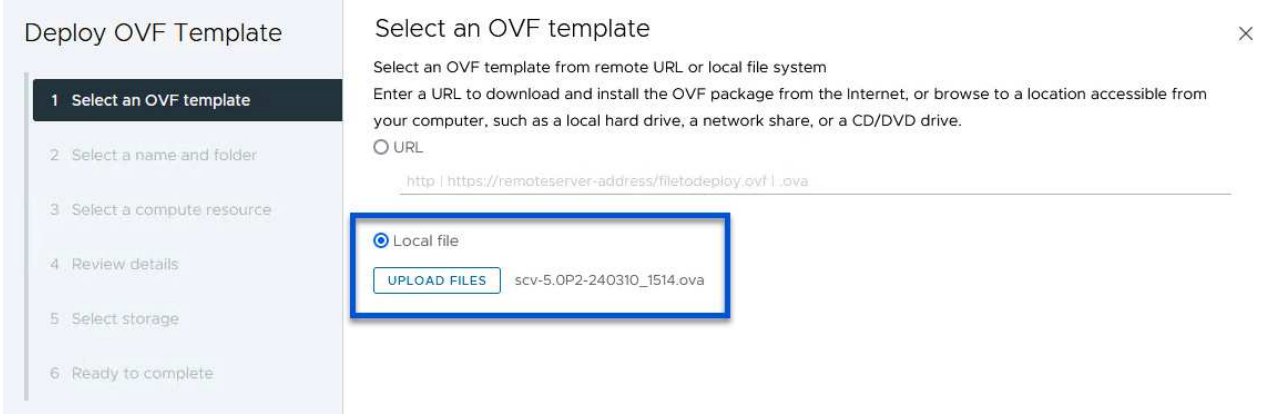
Il plug-in SnapCenter è ospitato sul dominio di gestione VCF ma registrato su vCenter per il dominio del carico di lavoro VI. Per ogni istanza vCenter è necessaria un'istanza SCV e, tieni presente che un dominio di carico di lavoro può includere più cluster gestiti da una singola istanza vCenter.

Completare i seguenti passaggi dal client vCenter per distribuire SCV nel dominio del carico di lavoro VI:

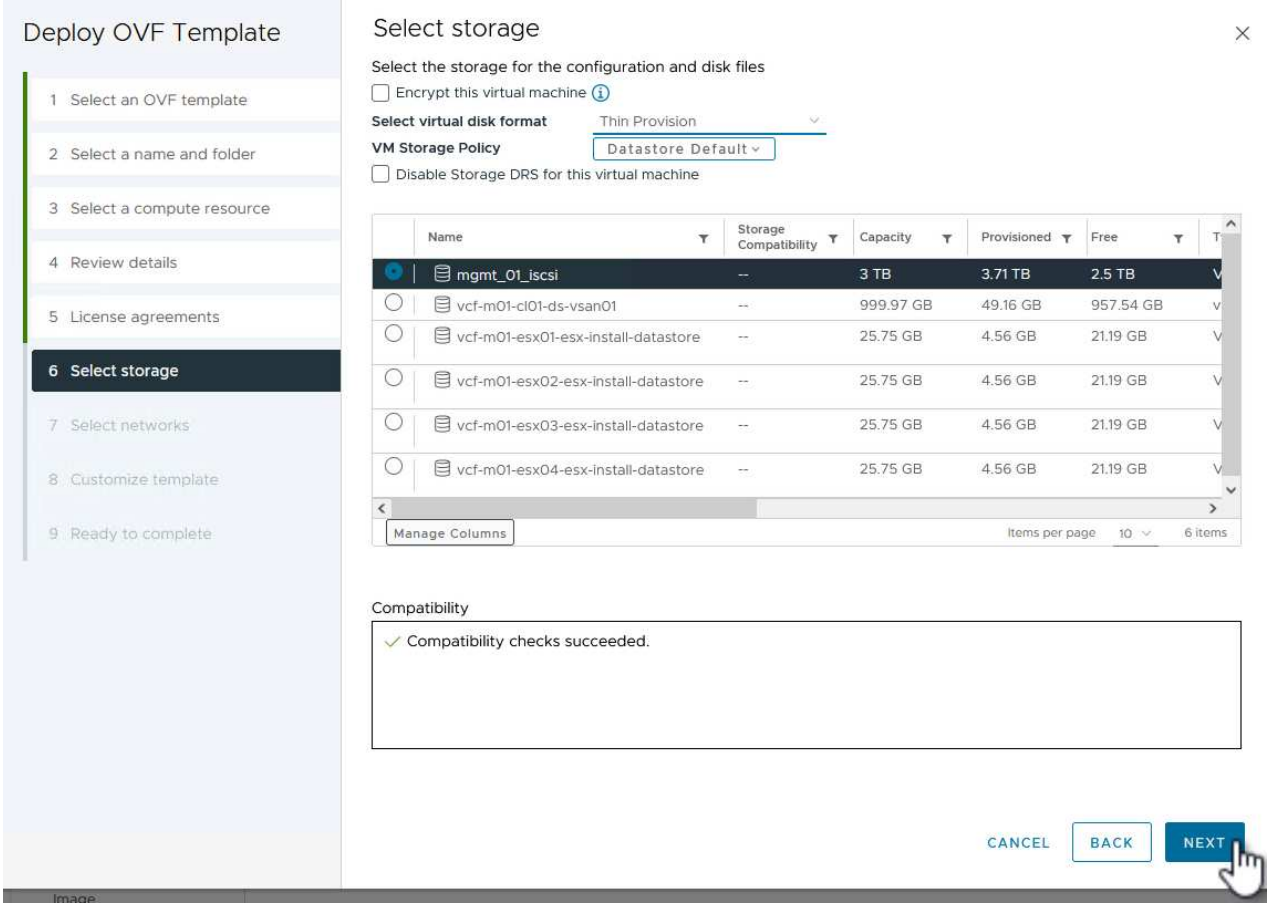
1. Scarica il file OVA per la distribuzione SCV dall'area download del sito di supporto NetApp"**QUI**" .
2. Dal dominio di gestione vCenter Client, selezionare **Distribuisci modello OVF…**.



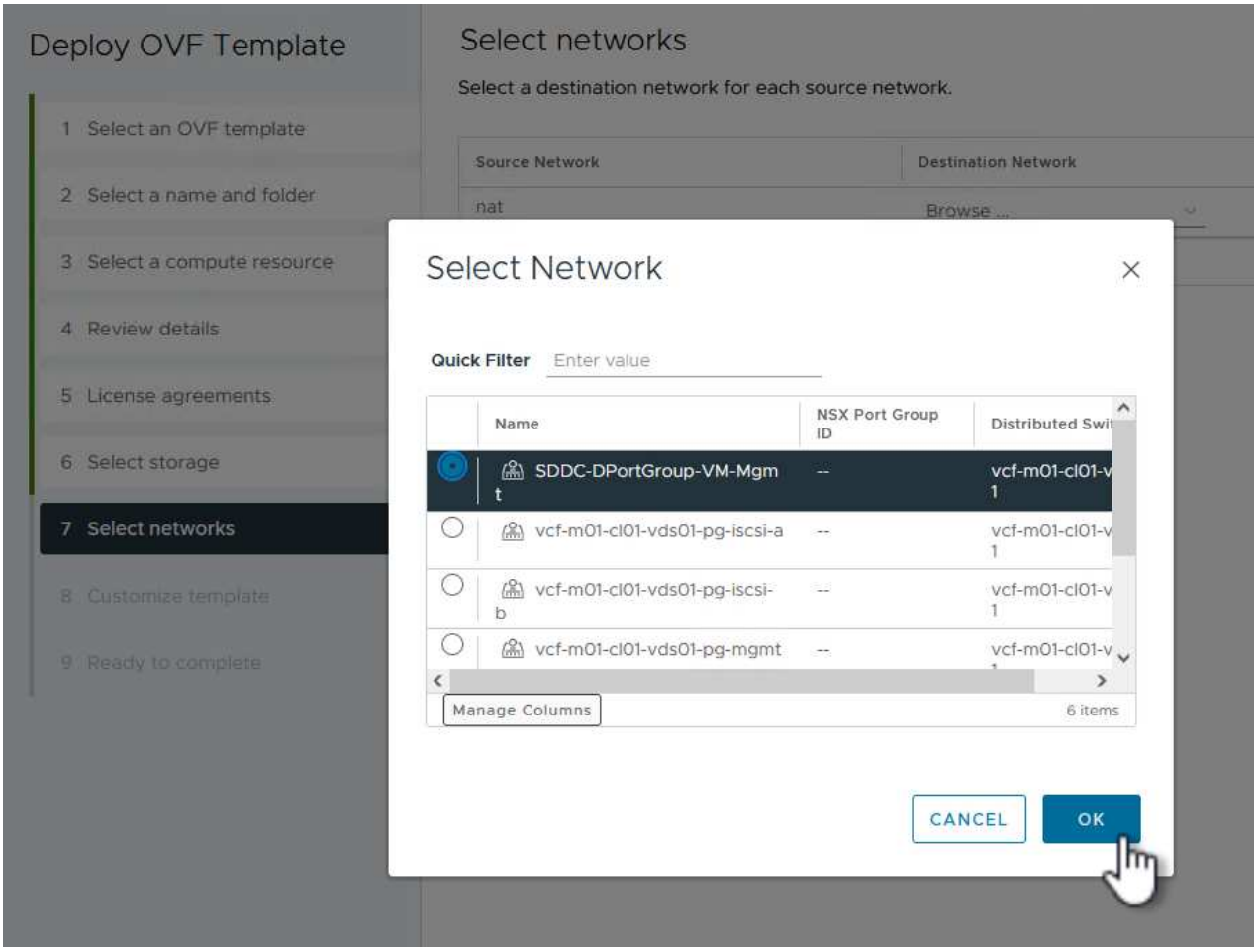
3. Nella procedura guidata **Distribuisci modello OVF**, fai clic sul pulsante di opzione **File locale** e seleziona quindi di caricare il modello OVF scaricato in precedenza. Fare clic su **Avanti** per continuare.



4. Nella pagina **Seleziona nome e cartella**, specificare un nome per la VM del broker dati SCV e una cartella nel dominio di gestione. Fare clic su **Avanti** per continuare.
5. Nella pagina **Seleziona una risorsa di elaborazione**, seleziona il cluster del dominio di gestione o l'host ESXi specifico all'interno del cluster su cui installare la VM.
6. Esaminare le informazioni relative al modello OVF nella pagina **Esamina dettagli** e accettare i termini di licenza nella pagina **Accordi di licenza**.
7. Nella pagina **Seleziona storage**, seleziona il datastore in cui verrà installata la VM e seleziona il **formato del disco virtuale** e i **criteri di storage della VM**. In questa soluzione, la VM verrà installata su un datastore iSCSI VMFS situato su un sistema di archiviazione ONTAP , come precedentemente distribuito in una sezione separata di questa documentazione. Fare clic su **Avanti** per continuare.

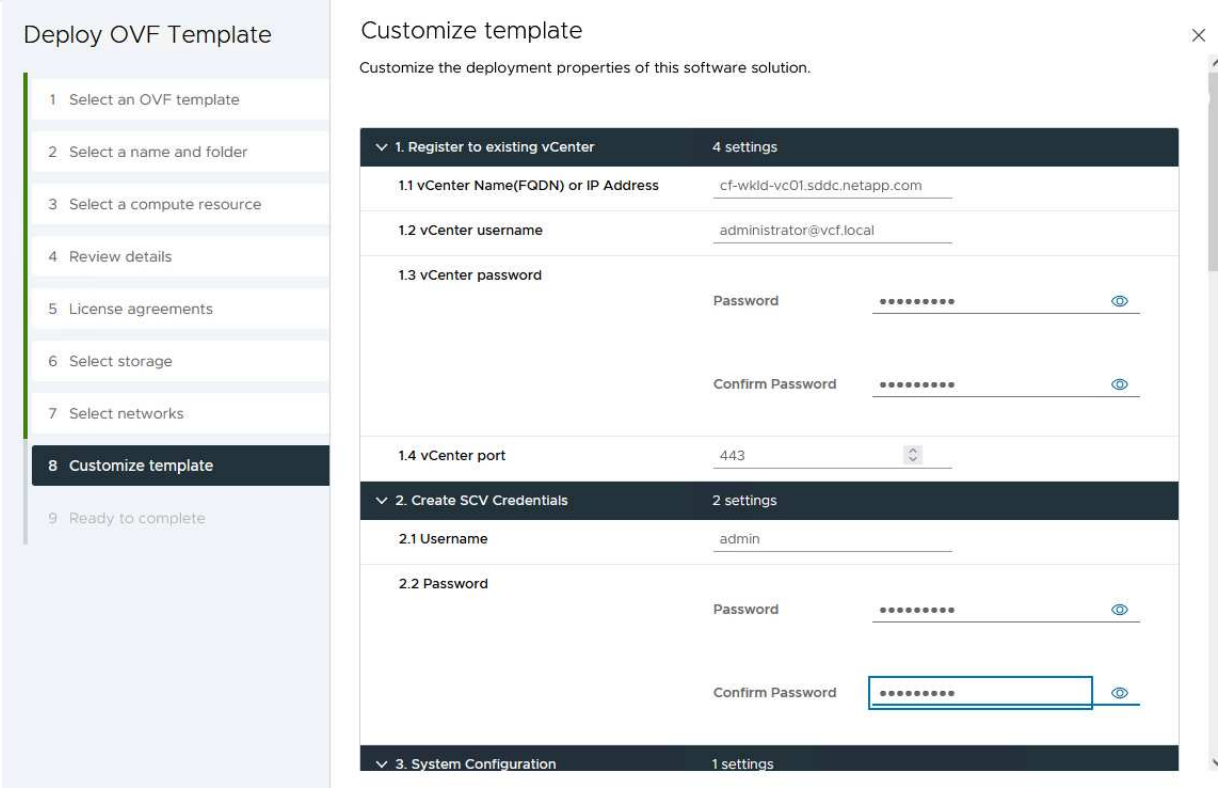


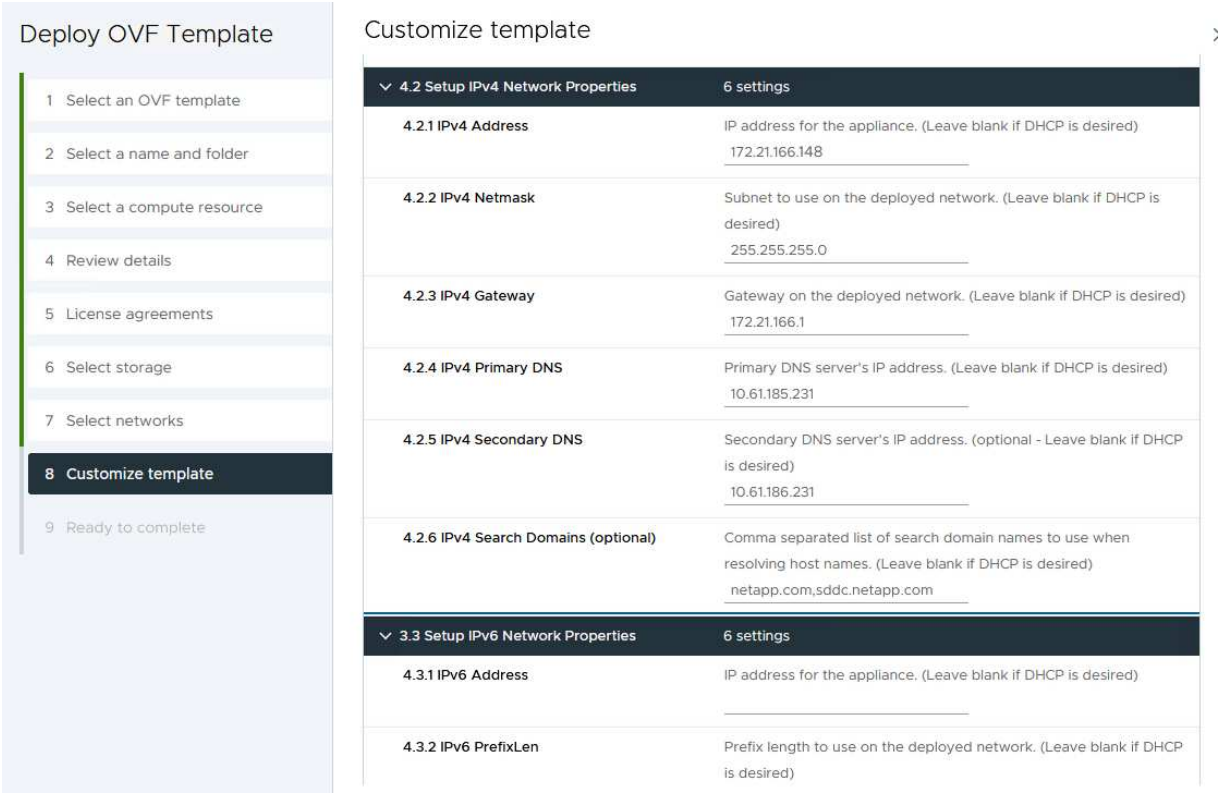
8. Nella pagina **Seleziona rete**, seleziona la rete di gestione in grado di comunicare con l'appliance vCenter del dominio del carico di lavoro e con i sistemi di storage ONTAP primario e secondario.

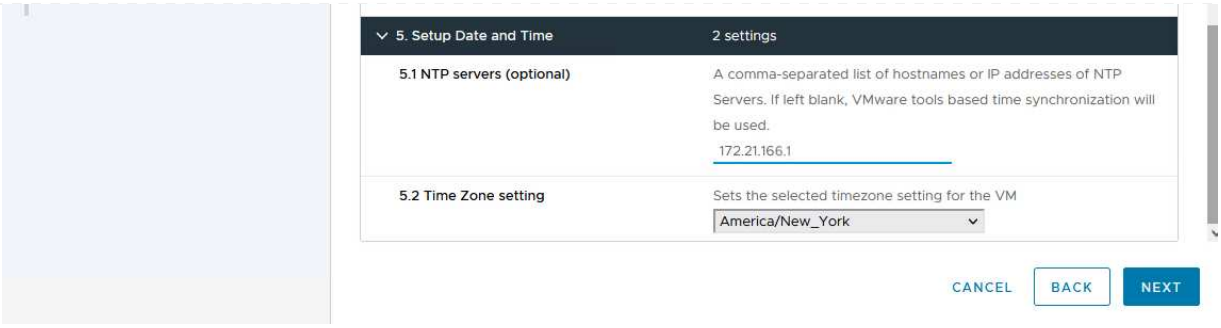


9. Nella pagina **Personalizza modello** compila tutte le informazioni richieste per la distribuzione:
   - FQDN o IP e credenziali per l'appliance vCenter del dominio del carico di lavoro.
   - Credenziali per l'account amministrativo SCV.
   - Credenziali per l'account di manutenzione SCV.
   - Dettagli sulle proprietà di rete IPv4 (è possibile utilizzare anche IPv6).
   - Impostazioni di data e ora.

   Fare clic su **Avanti** per continuare.


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
1. Register to existing vCenter
4 settings
1.1 vCenter Name(FQDN) or IP Address
cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username
administrator@vcf.local
1.3 vCenter password
Password
Confirm Password
1.4 vCenter port
443
2. Create SCV Credentials
2 settings
2.1 Username
admin
2.2 Password
Password
Confirm Password
3. System Configuration
1 settings


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
4.2 Setup IPv4 Network Properties
6 settings
4.2.1 IPv4 Address
IP address for the appliance. (Leave blank if DHCP is desired)
172.21.166.148
4.2.2 IPv4 Netmask
Subnet to use on the deployed network. (Leave blank if DHCP is desired)
255.255.255.0
4.2.3 IPv4 Gateway
Gateway on the deployed network. (Leave blank if DHCP is desired)
172.21.166.1
4.2.4 IPv4 Primary DNS
Primary DNS server's IP address. (Leave blank if DHCP is desired)
10.61.185.231
4.2.5 IPv4 Secondary DNS
Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired)
10.61.186.231
4.2.6 IPv4 Search Domains (optional)
Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired)
netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties
6 settings
4.3.1 IPv6 Address
IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen
Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

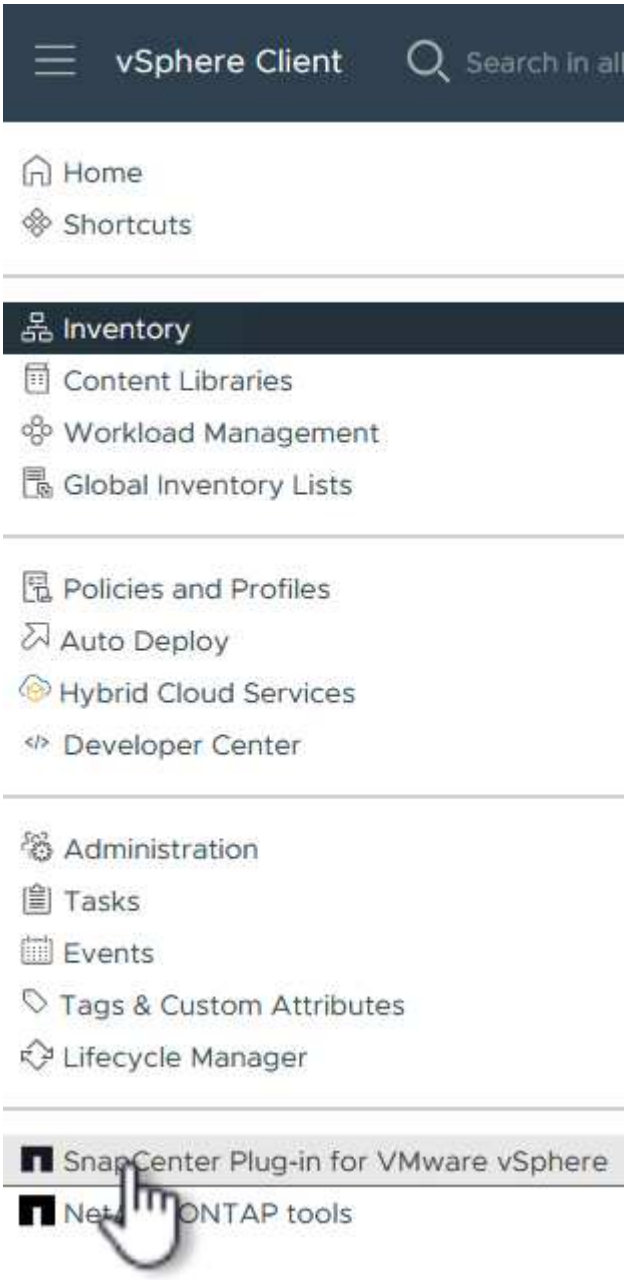


10. Infine, nella pagina **Pronto per il completamento**, rivedi tutte le impostazioni e fai clic su Fine per avviare la distribuzione.

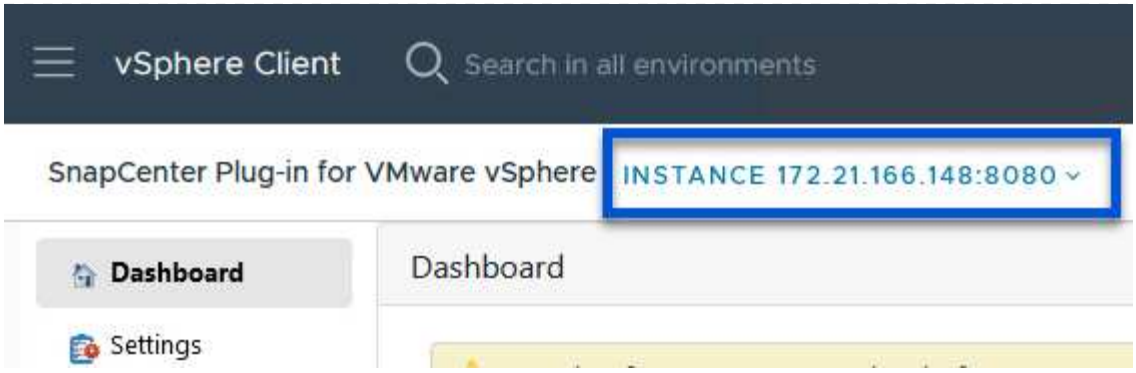
Aggiungere sistemi di archiviazione a SCV

Una volta installato il plug-in SnapCenter , completare i seguenti passaggi per aggiungere sistemi di archiviazione a SCV:

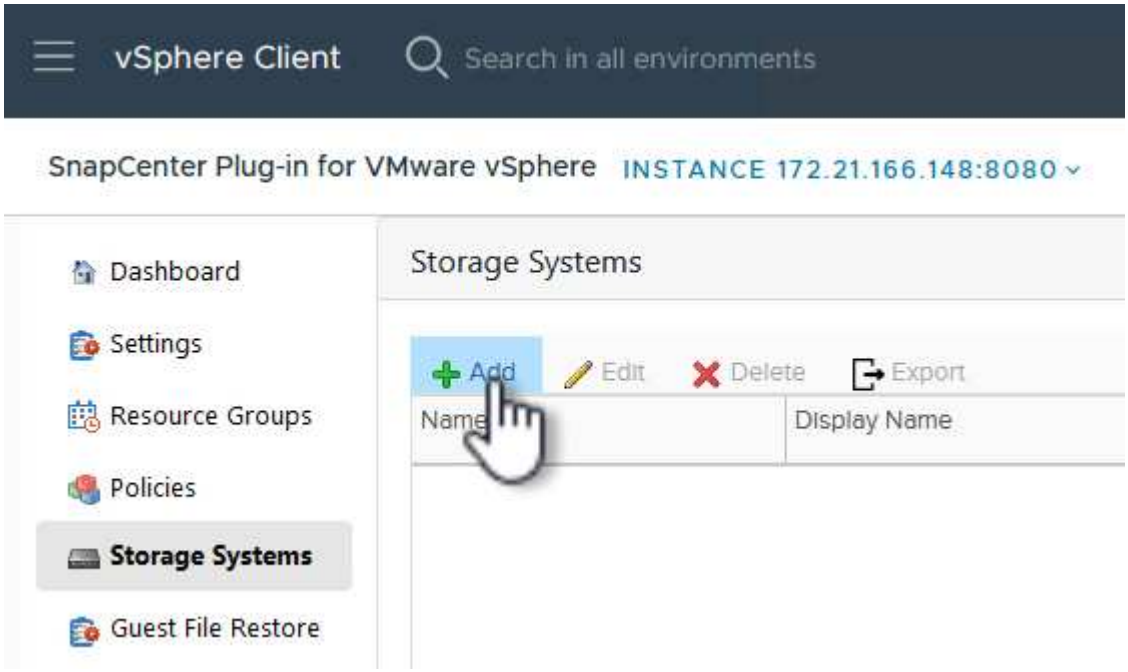
1. È possibile accedere a SCV dal menu principale di vSphere Client.



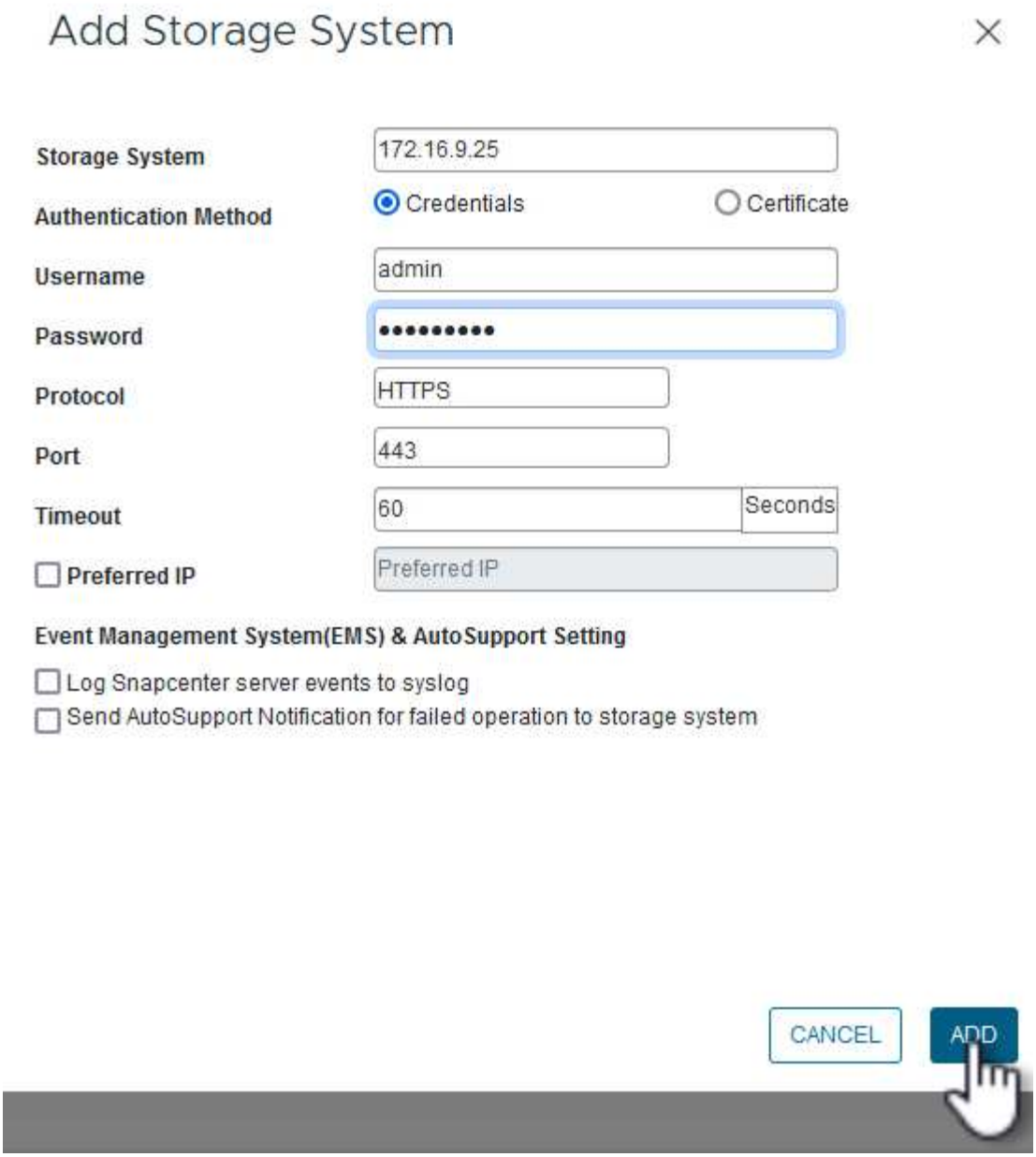
2. Nella parte superiore dell'interfaccia utente SCV, seleziona l'istanza SCV corretta che corrisponde al cluster vSphere da proteggere.



3. Vai su **Sistemi di archiviazione** nel menu a sinistra e clicca su **Aggiungi** per iniziare.



4. Nel modulo **Aggiungi sistema di archiviazione**, compilare l'indirizzo IP e le credenziali del sistema di archiviazione ONTAP da aggiungere e fare clic su **Aggiungi** per completare l'operazione.



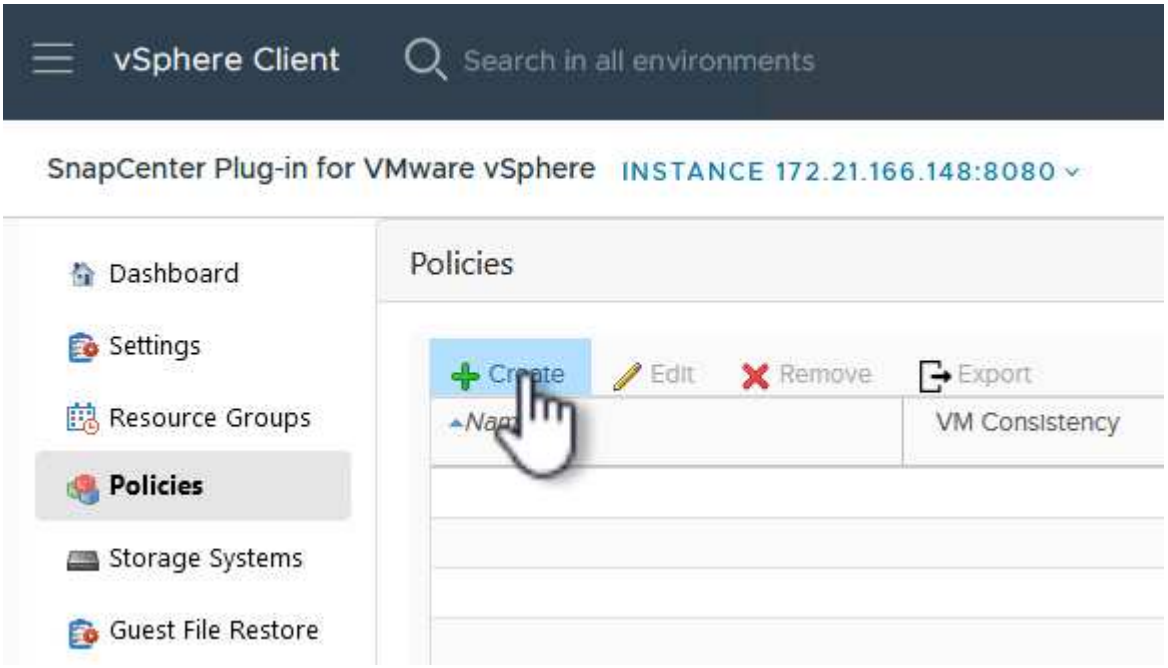
5. Ripetere questa procedura per tutti gli altri sistemi di archiviazione da gestire, compresi quelli da utilizzare come destinazioni di backup secondarie.

Configurare i criteri di backup in SCV

Per ulteriori informazioni sulla creazione di policy di backup SCV, fare riferimento a"Creare policy di backup per VM e datastore" .

Per creare un nuovo criterio di backup, completare i seguenti passaggi:

1. Dal menu a sinistra seleziona **Criteri** e clicca su **Crea** per iniziare.



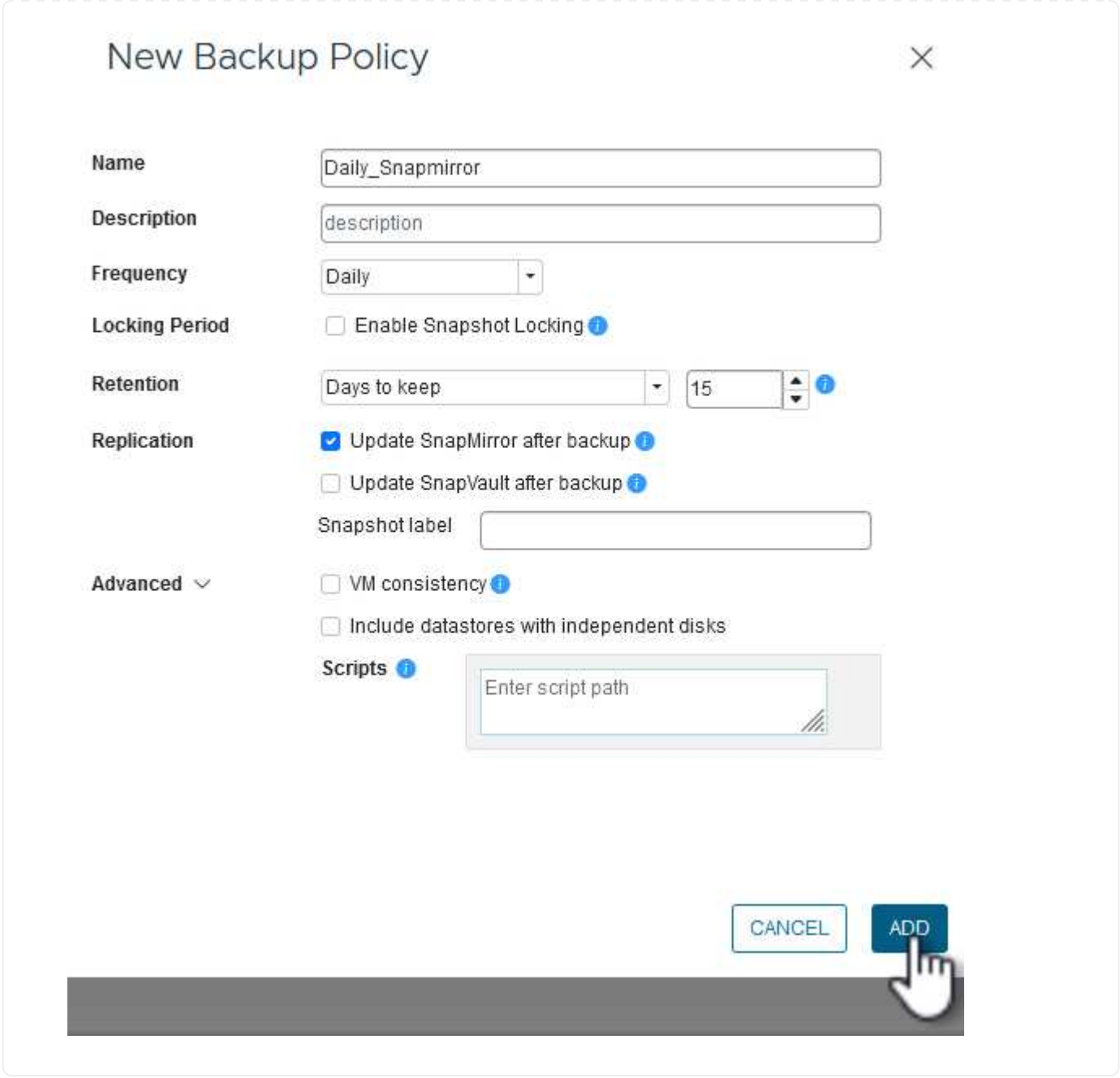
2. Nel modulo **Nuova politica di backup**, specificare un **Nome** e una **Descrizione** per la politica, la **Frequenza** con cui verranno eseguiti i backup e il **Periodo di conservazione** che specifica per quanto tempo verrà conservato il backup.

   Periodo di blocco consente alla funzione ONTAP SnapLock di creare snapshot a prova di manomissione e consente la configurazione del periodo di blocco.

   Per **Replica** selezionare per aggiornare le relazioni SnapMirror o SnapVault sottostanti per il volume di archiviazione ONTAP .

   > Le repliche SnapMirror e SnapVault sono simili in quanto entrambe utilizzano la tecnologia ONTAP SnapMirror per replicare in modo asincrono i volumi di archiviazione su un sistema di archiviazione secondario per una maggiore protezione e sicurezza. Per le relazioni SnapMirror , la pianificazione della conservazione specificata nella policy di backup SCV regolerà la conservazione sia per il volume primario che per quello secondario. Grazie alle relazioni SnapVault , è possibile stabilire un programma di conservazione separato sul sistema di archiviazione secondario per programmi di conservazione a lungo termine o diversi. In questo caso l'etichetta dello snapshot viene specificata nella policy di backup SCV e nella policy associata al volume secondario, per identificare a quali volumi applicare la pianificazione di conservazione indipendente.

   Seleziona eventuali opzioni avanzate aggiuntive e clicca su **Aggiungi** per creare la policy.

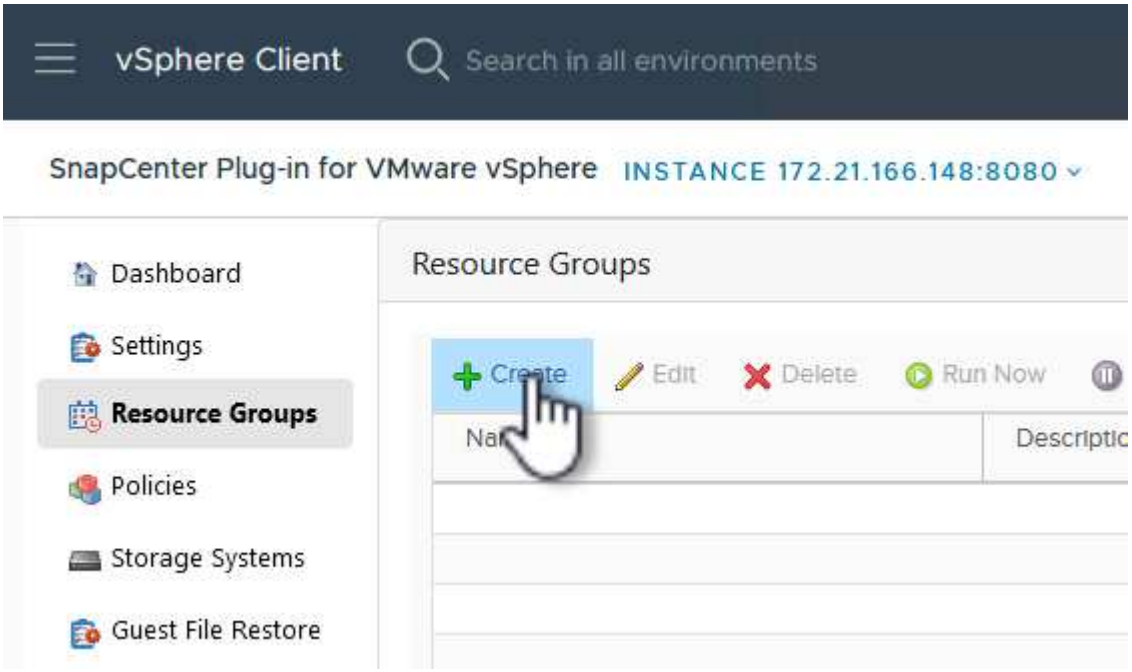

New Backup Policy
Name
Daily_Snapmirror
Description
description
Frequency
Daily
Locking Period
Enable Snapshot Locking
Retention
Days to keep
15
Replication
Update SnapMirror after backup
Update SnapVault after backup
Snapshot label
Advanced
VM consistency
Include datastores with independent disks
Scripts
Enter script path
CANCEL
ADD

Creare gruppi di risorse in SCV

Per ulteriori informazioni sulla creazione di gruppi di risorse SCV, fare riferimento a"Creare gruppi di risorse" .

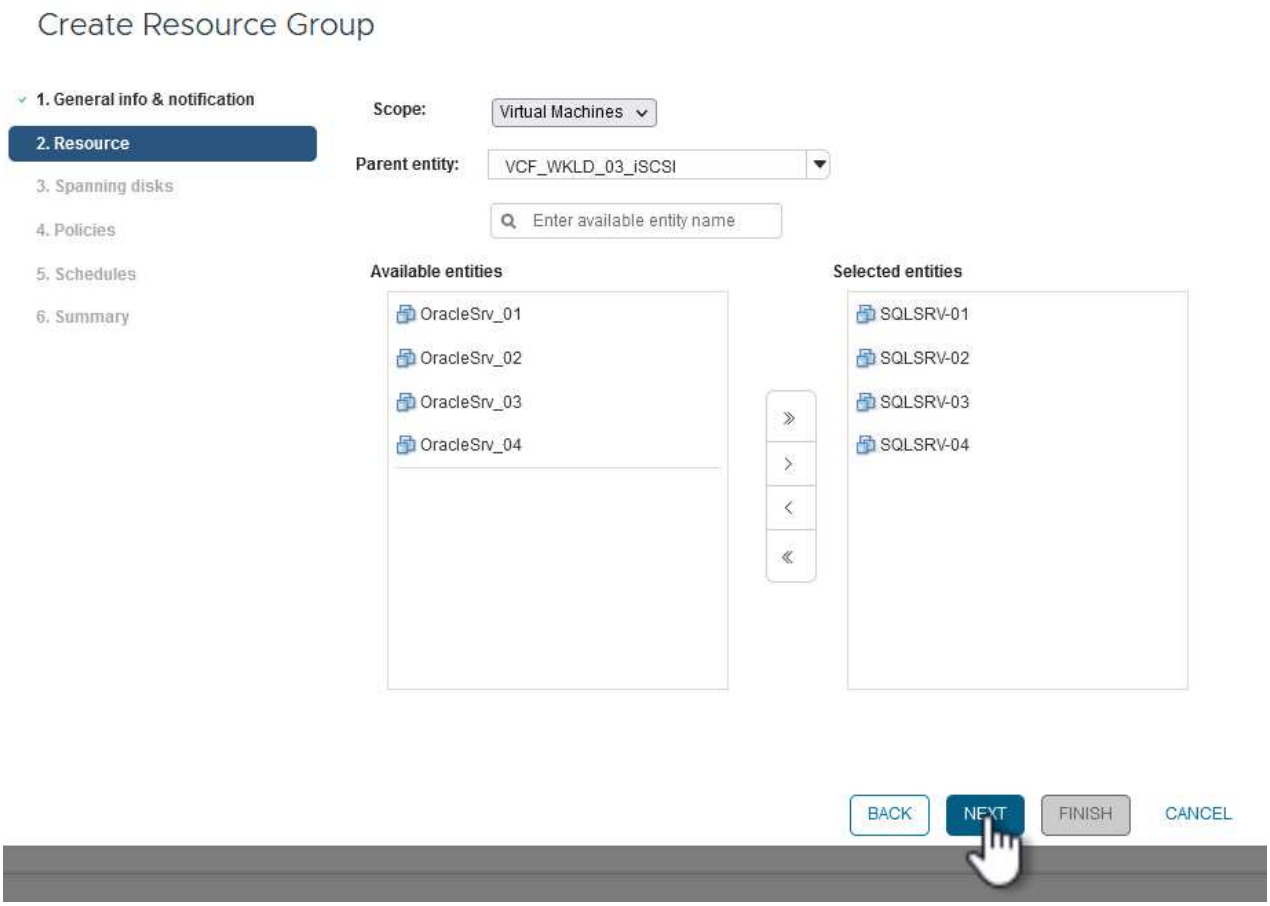
Per creare un nuovo gruppo di risorse, completa i seguenti passaggi:

1. Dal menu a sinistra seleziona **Gruppi di risorse** e clicca su **Crea** per iniziare.

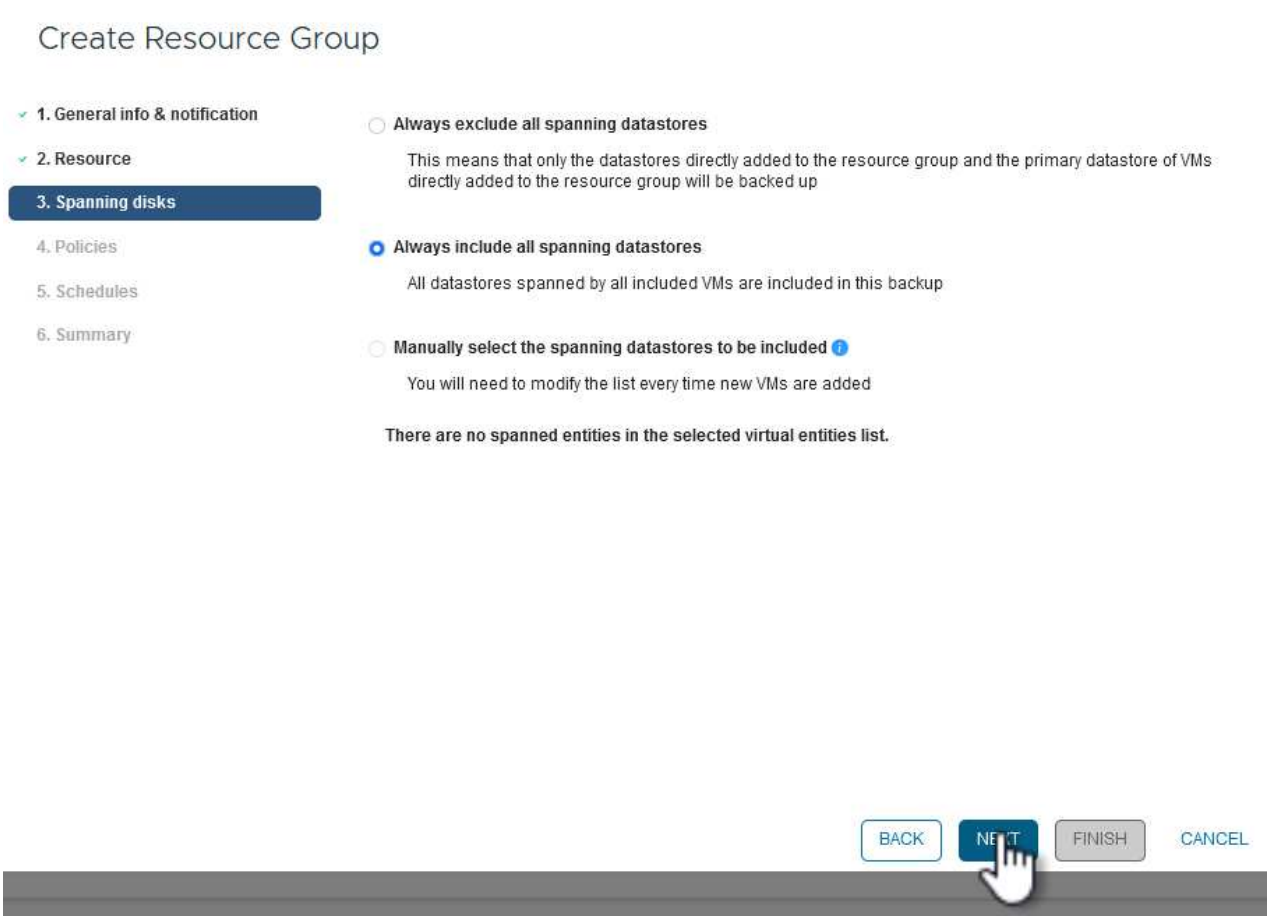


2. Nella pagina **Informazioni generali e notifiche**, specificare un nome per il gruppo di risorse, le impostazioni di notifica e qualsiasi altra opzione per la denominazione degli snapshot.
3. Nella pagina **Risorsa** selezionare i datastore e le VM da proteggere nel gruppo di risorse. Fare clic su **Avanti** per continuare.

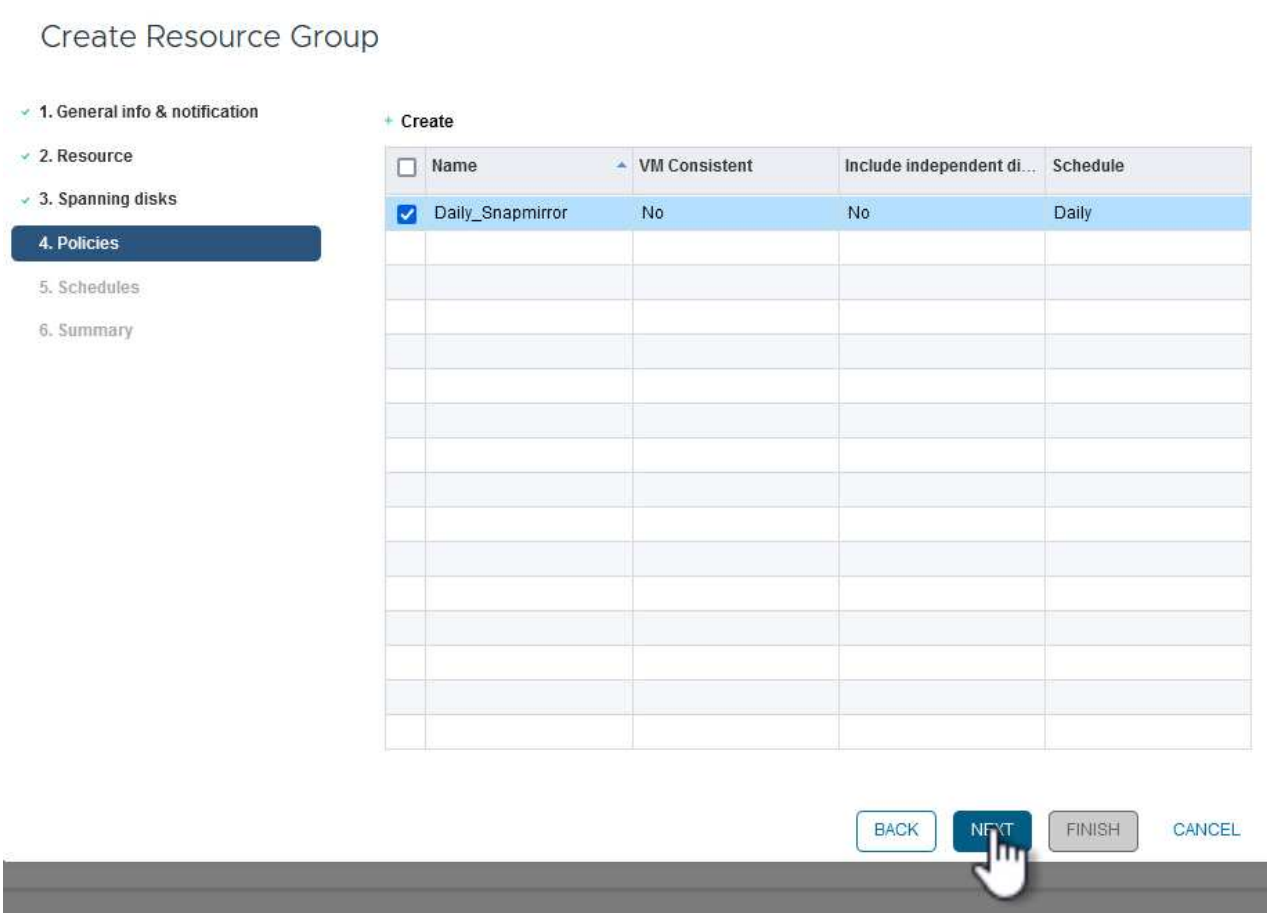
> Anche quando vengono selezionate solo VM specifiche, viene sempre eseguito il backup dell'intero datastore. Ciò avviene perché ONTAP esegue snapshot del volume che ospita il datastore. Tuttavia, tieni presente che selezionando solo VM specifiche per il backup si limita la possibilità di ripristinare solo quelle VM.



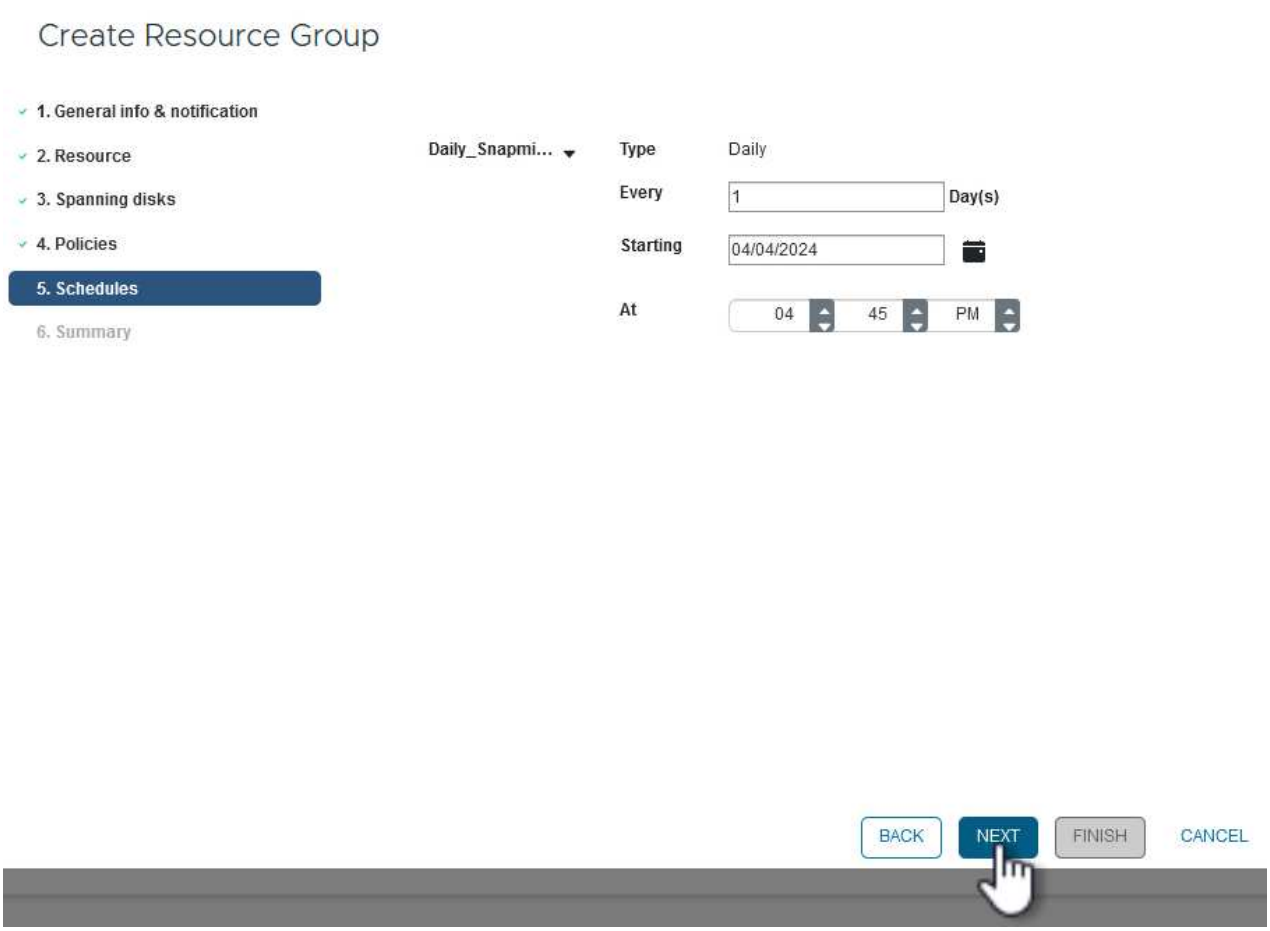
4. Nella pagina **Dischi distribuiti** selezionare l'opzione per la gestione delle VM con VMDK che si estendono su più datastore. Fare clic su **Avanti** per continuare.



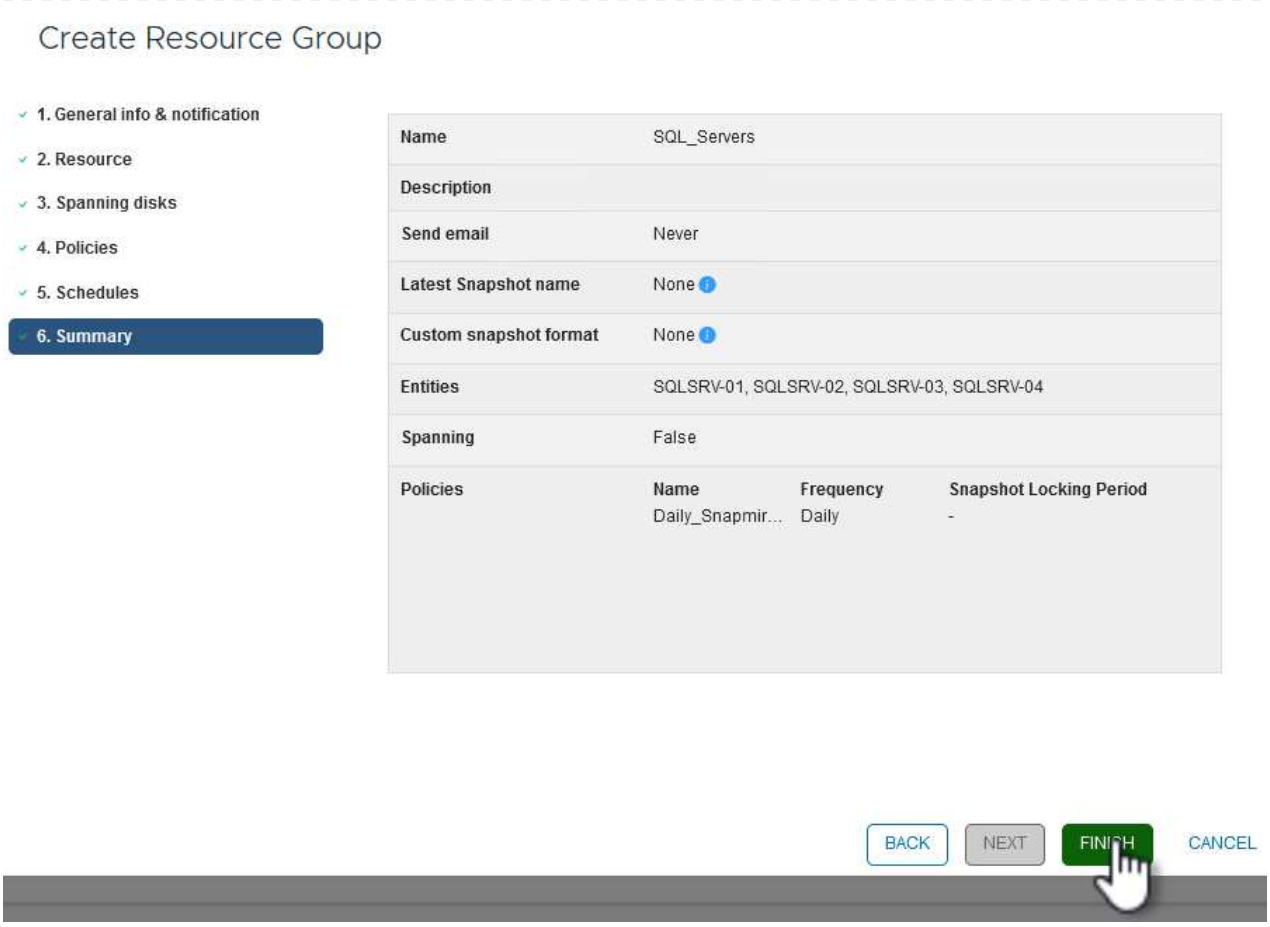
5. Nella pagina **Criteri** seleziona un criterio creato in precedenza o più criteri che verranno utilizzati con questo gruppo di risorse. Fare clic su **Avanti** per continuare.



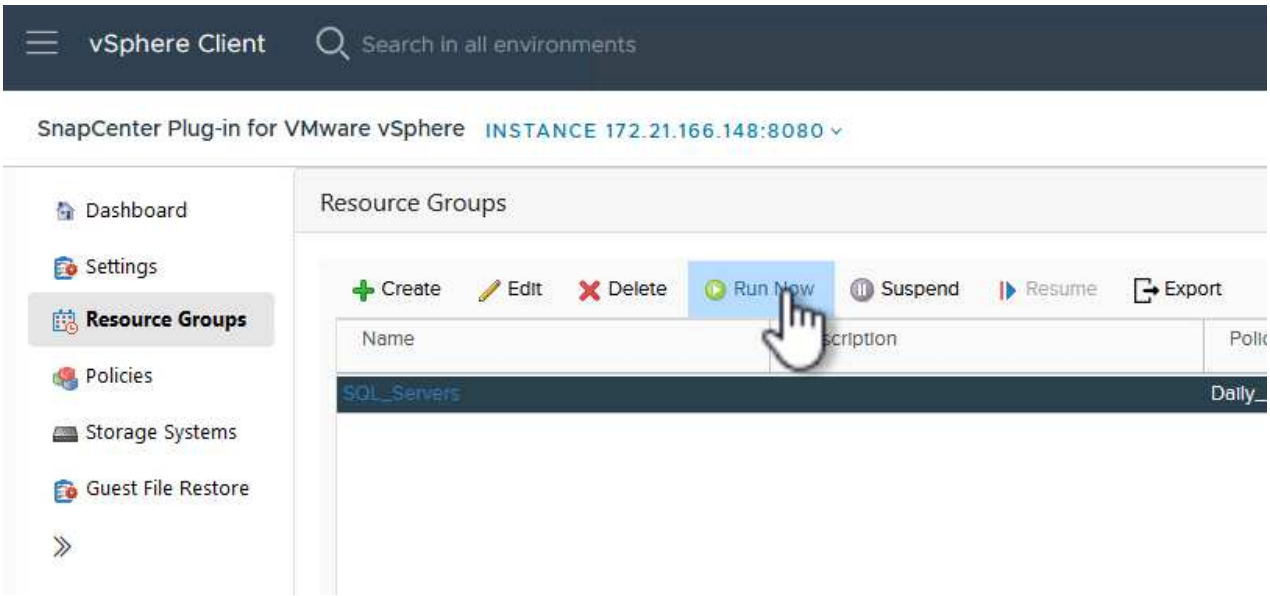
6. Nella pagina **Pianificazioni** stabilire quando verrà eseguito il backup configurando la ricorrenza e l'ora del giorno. Fare clic su **Avanti** per continuare.



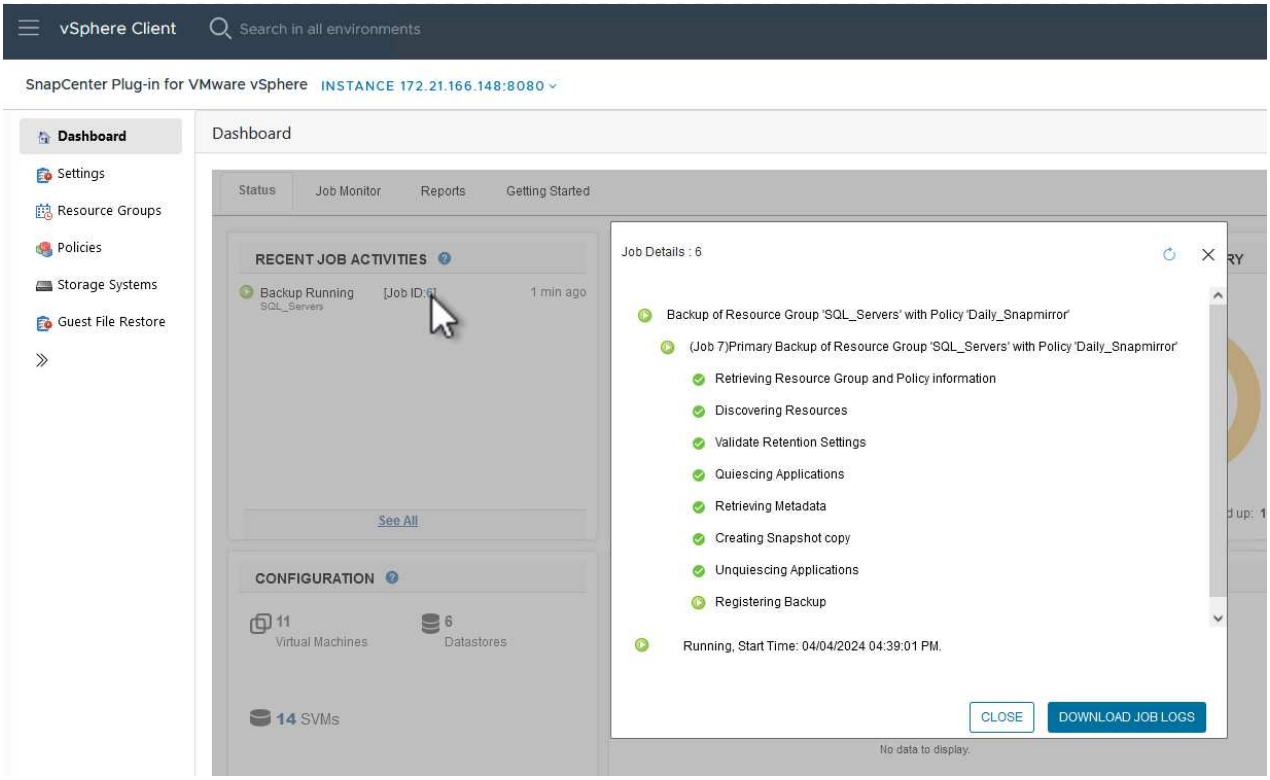
7. Infine, rivedere il **Riepilogo** e fare clic su **Fine** per creare il gruppo di risorse.



8. Dopo aver creato il gruppo di risorse, fare clic sul pulsante **Esegui ora** per eseguire il primo backup.



9. Vai alla **Dashboard** e, in **Attività recenti del lavoro**, clicca sul numero accanto a **ID lavoro** per aprire il monitor del lavoro e visualizzare l'avanzamento del lavoro in esecuzione.



Utilizzare SCV per ripristinare VM, VMDK e file

Il plug-in SnapCenter consente il ripristino di VM, VMDK, file e cartelle da backup primari o secondari.

Le VM possono essere ripristinate sull'host originale, su un host alternativo nello stesso vCenter Server o su un host ESXi alternativo gestito dallo stesso vCenter o da qualsiasi vCenter in modalità collegata.

Le VM vVol possono essere ripristinate sull'host originale.

I VMDK nelle VM tradizionali possono essere ripristinati nel datastore originale o in un datastore alternativo.

I VMDK nelle VM vVol possono essere ripristinati nel datastore originale.

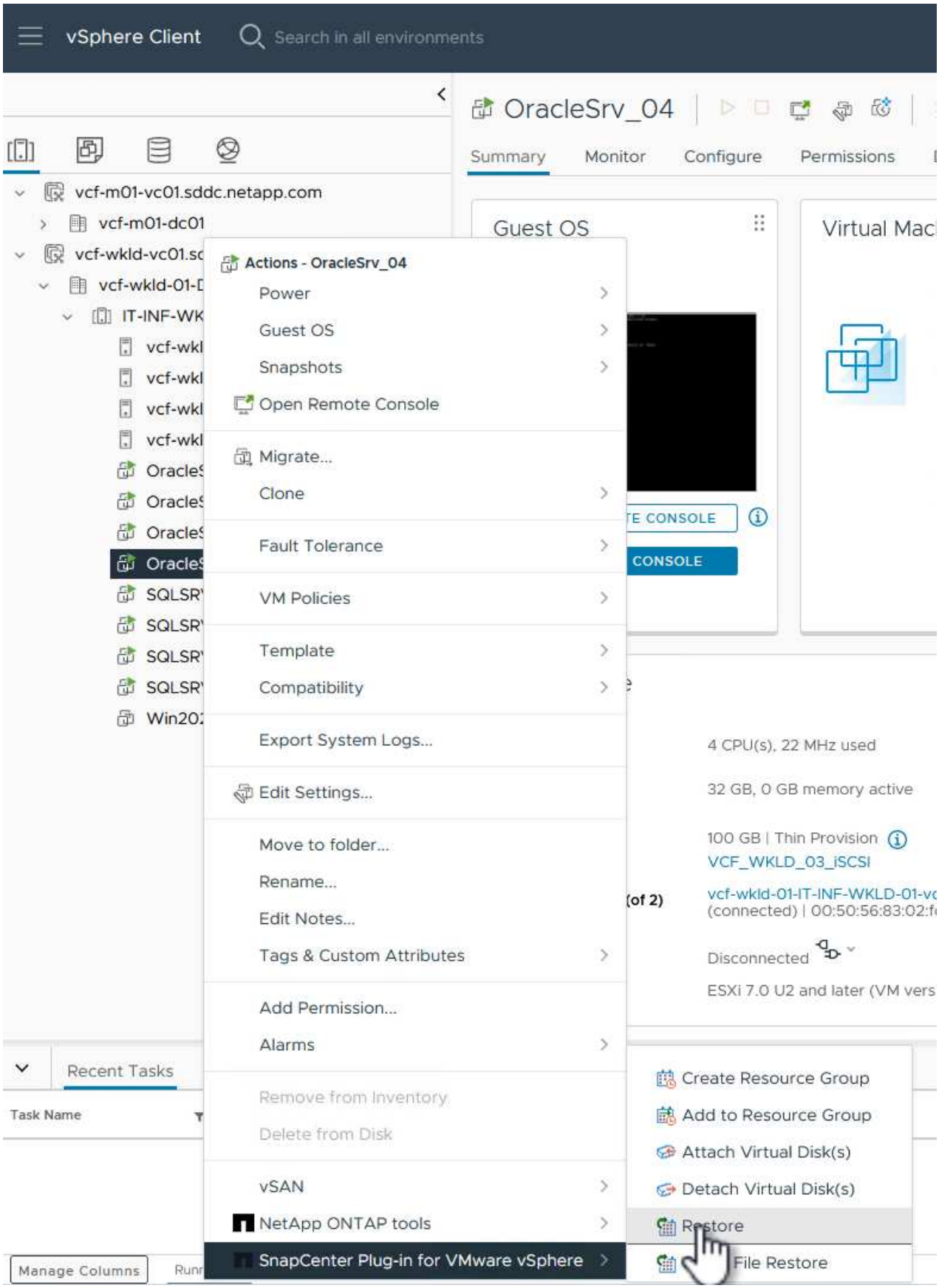
È possibile ripristinare singoli file e cartelle in una sessione di ripristino file guest, che allega una copia di backup di un disco virtuale e quindi ripristina i file o le cartelle selezionati.

Completare i seguenti passaggi per ripristinare VM, VMDK o singole cartelle.

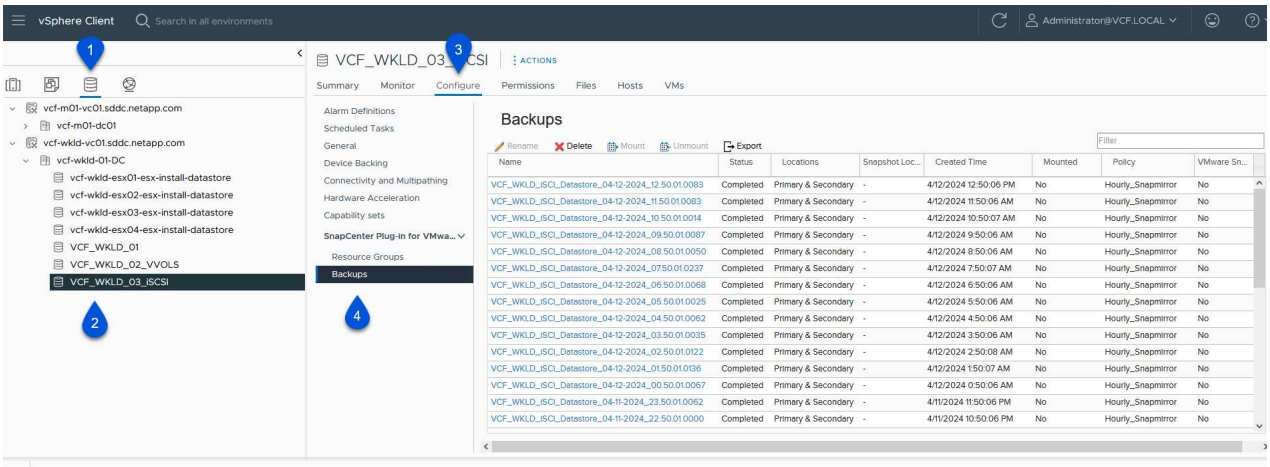
Ripristina le VM utilizzando il plug-in SnapCenter

Per ripristinare una VM con SCV, completare i seguenti passaggi:

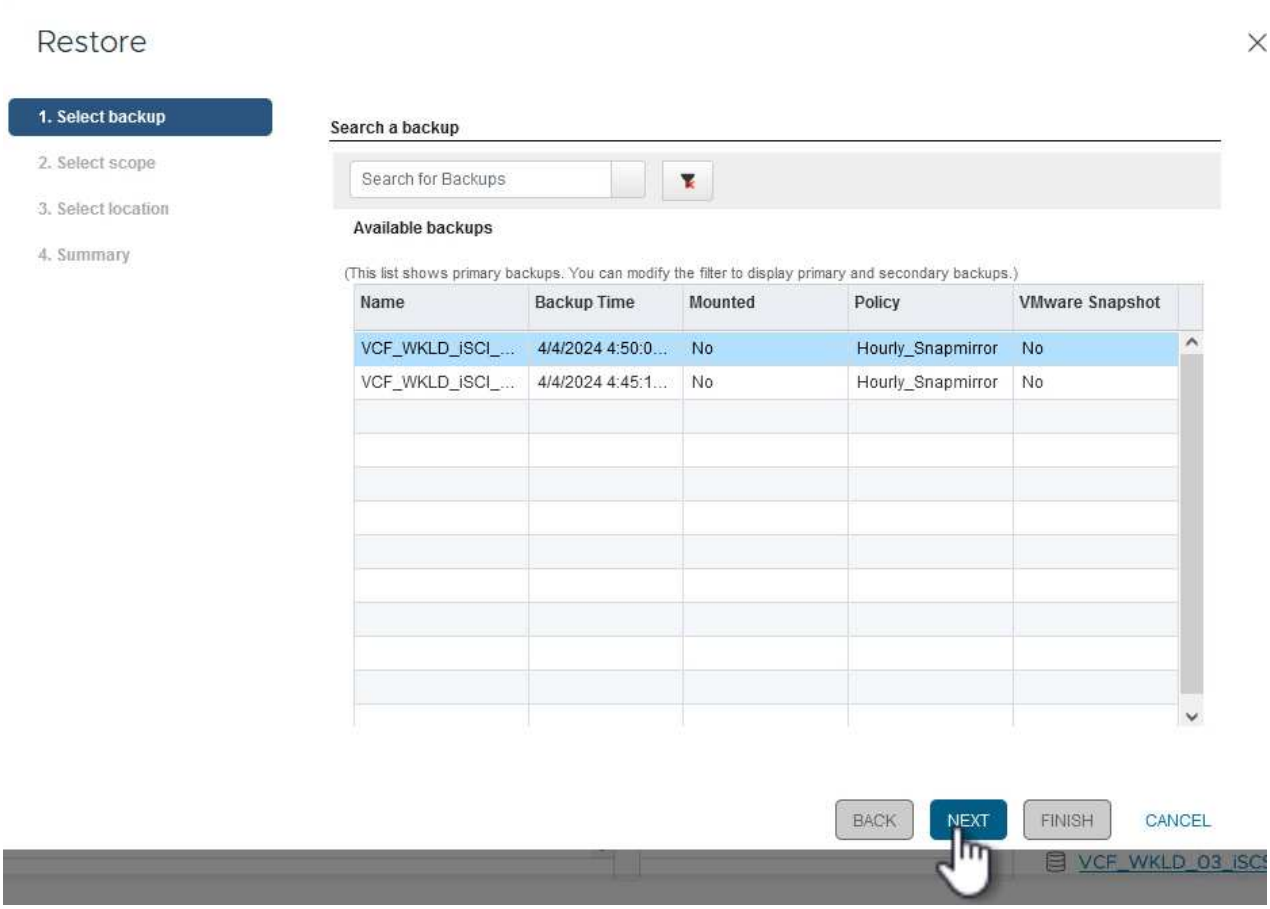
1. Passare alla VM da ripristinare nel client vSphere, fare clic con il pulsante destro del mouse e andare su * SnapCenter Plug-in for VMware vSphere*. Selezionare **Ripristina** dal sottomenu.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
Oracle
Oracle
Oracle
Oracle
SQLSR
SQLSR
SQLSR
SQLSR
Win20
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns

Un'alternativa è quella di accedere al datastore nell'inventario e quindi nella scheda **Configura** andare su * SnapCenter Plug-in for VMware vSphere > Backup*. Dal backup scelto, seleziona le VM da ripristinare.

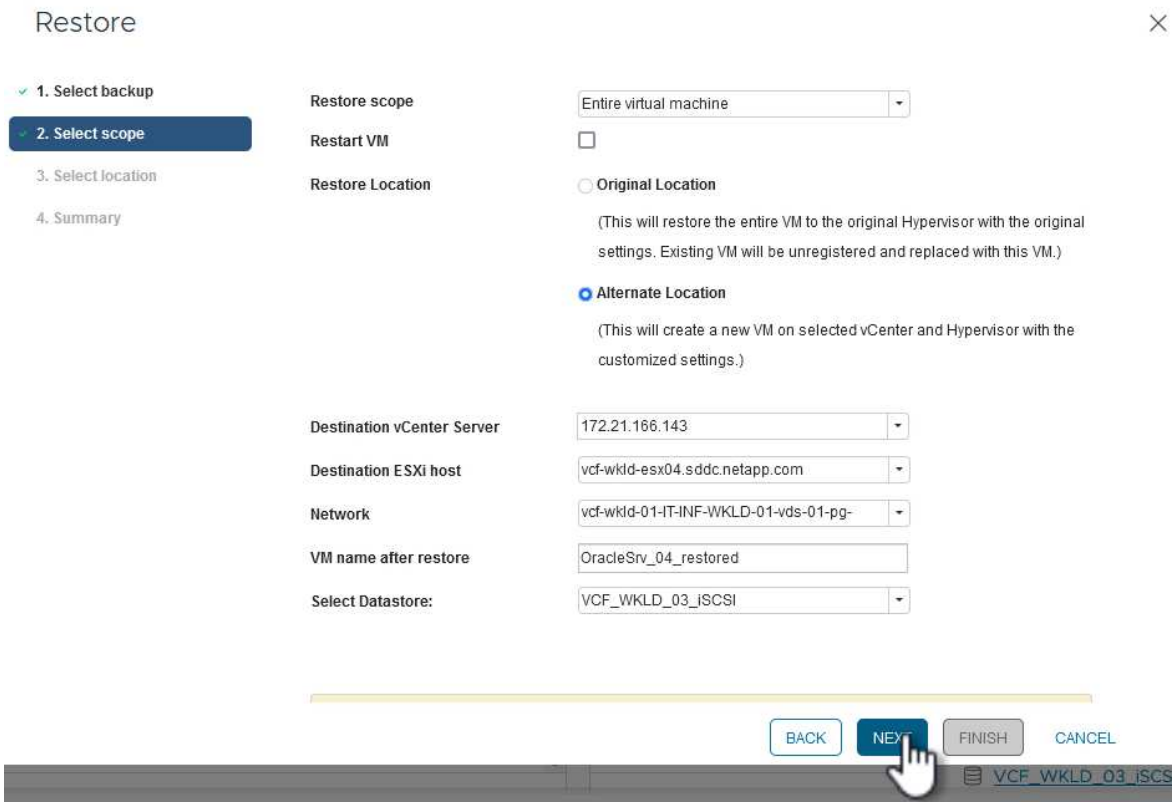


2. Nella procedura guidata **Ripristina** selezionare il backup da utilizzare. Fare clic su **Avanti** per continuare.



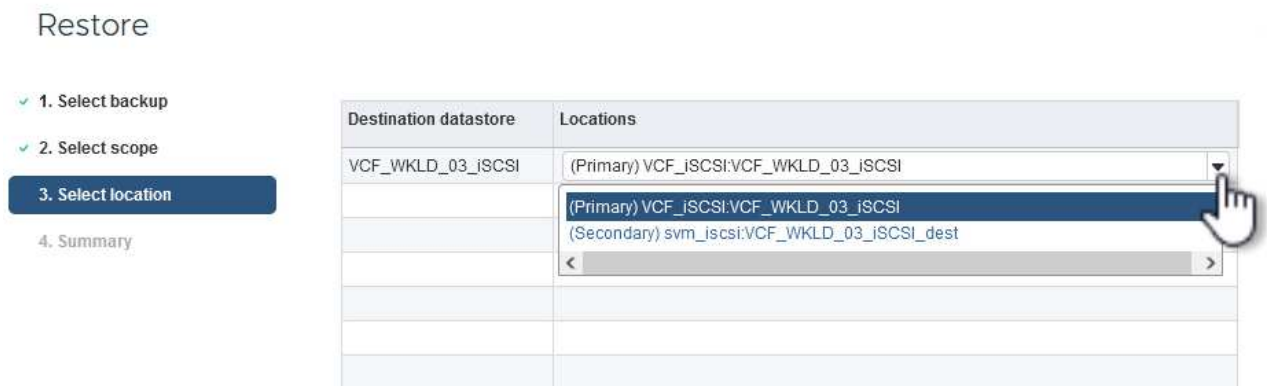
3. Nella pagina **Seleziona ambito** compila tutti i campi obbligatori:

- **Ripristina ambito**: seleziona per ripristinare l'intera macchina virtuale.
- **Riavvia VM**: scegli se avviare la VM dopo il ripristino.
- **Ripristina posizione**: scegli se ripristinare la posizione originale o una posizione alternativa. Quando si sceglie una posizione alternativa, selezionare le opzioni da ciascuno dei campi:
  - **Server vCenter di destinazione**: vCenter locale o vCenter alternativo in modalità collegata
  - **Host ESXi di destinazione**
  - **Rete**
  - **Nome della VM dopo il ripristino**
  - **Seleziona datastore:**

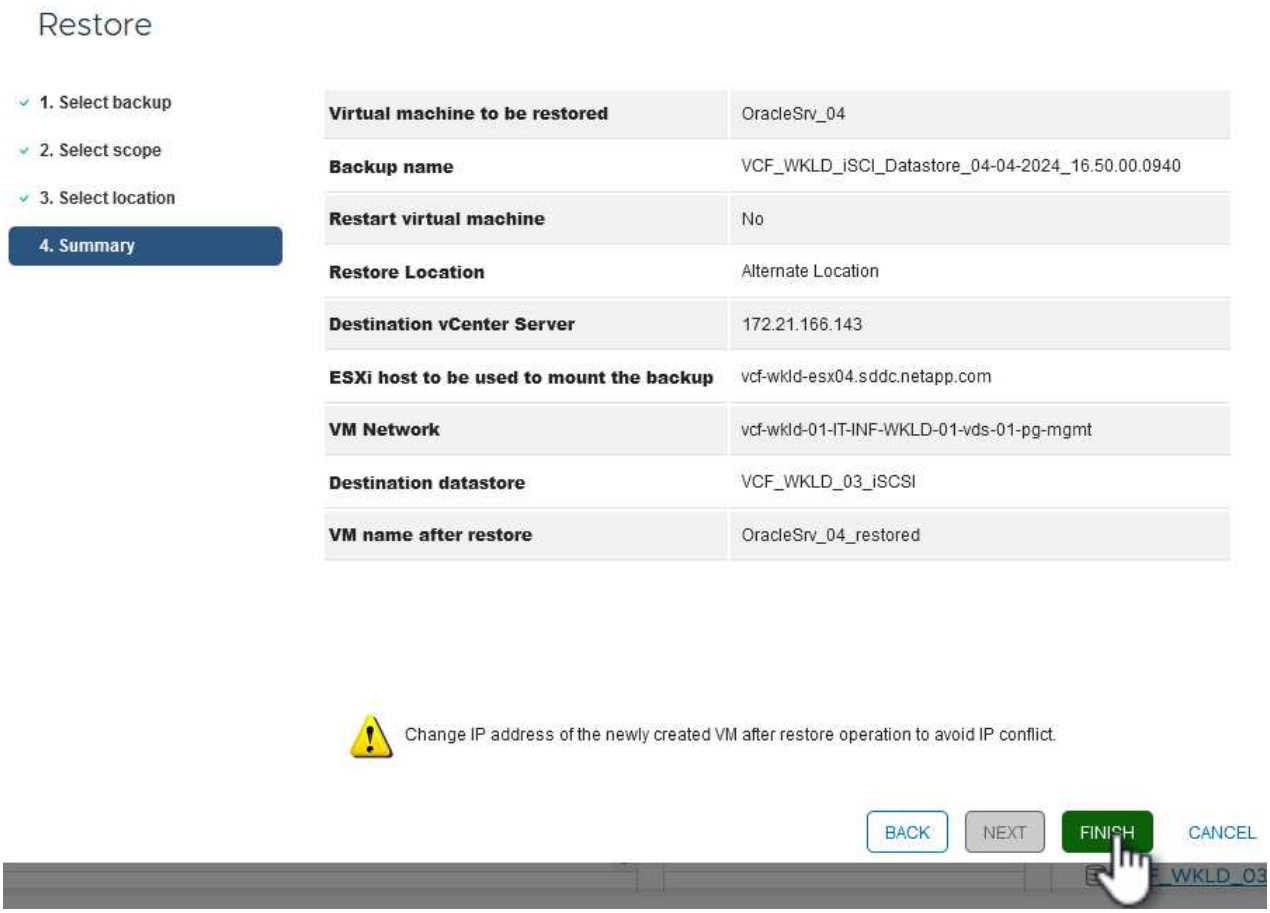


Fare clic su **Avanti** per continuare.

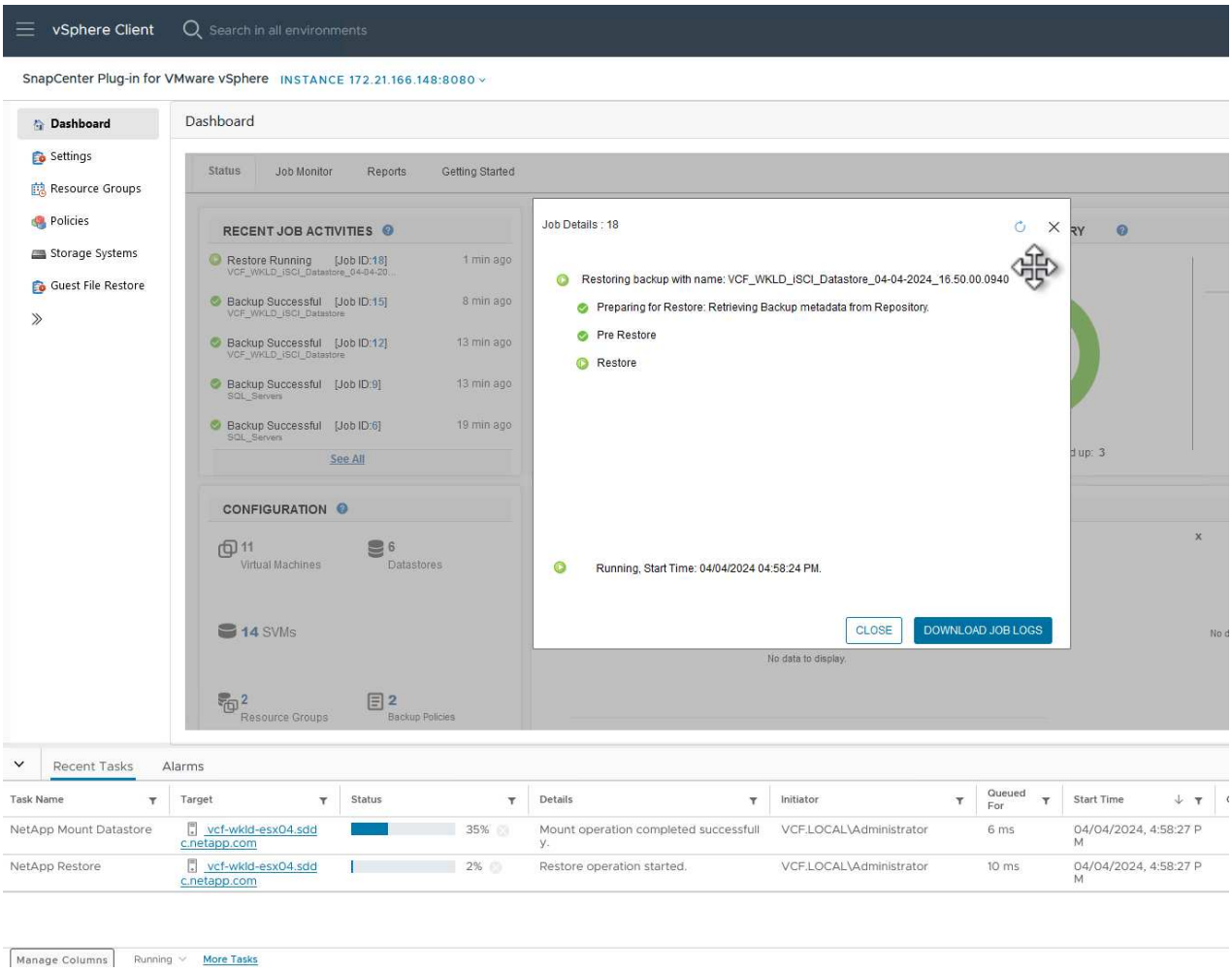
4. Nella pagina **Seleziona posizione**, scegli di ripristinare la VM dal sistema di archiviazione ONTAP primario o secondario. Fare clic su **Avanti** per continuare.



5. Infine, rivedere il **Riepilogo** e fare clic su **Fine** per avviare il processo di ripristino.



6. È possibile monitorare l'avanzamento del processo di ripristino dal riquadro **Attività recenti** in vSphere Client e dal monitoraggio dei processi in SCV.

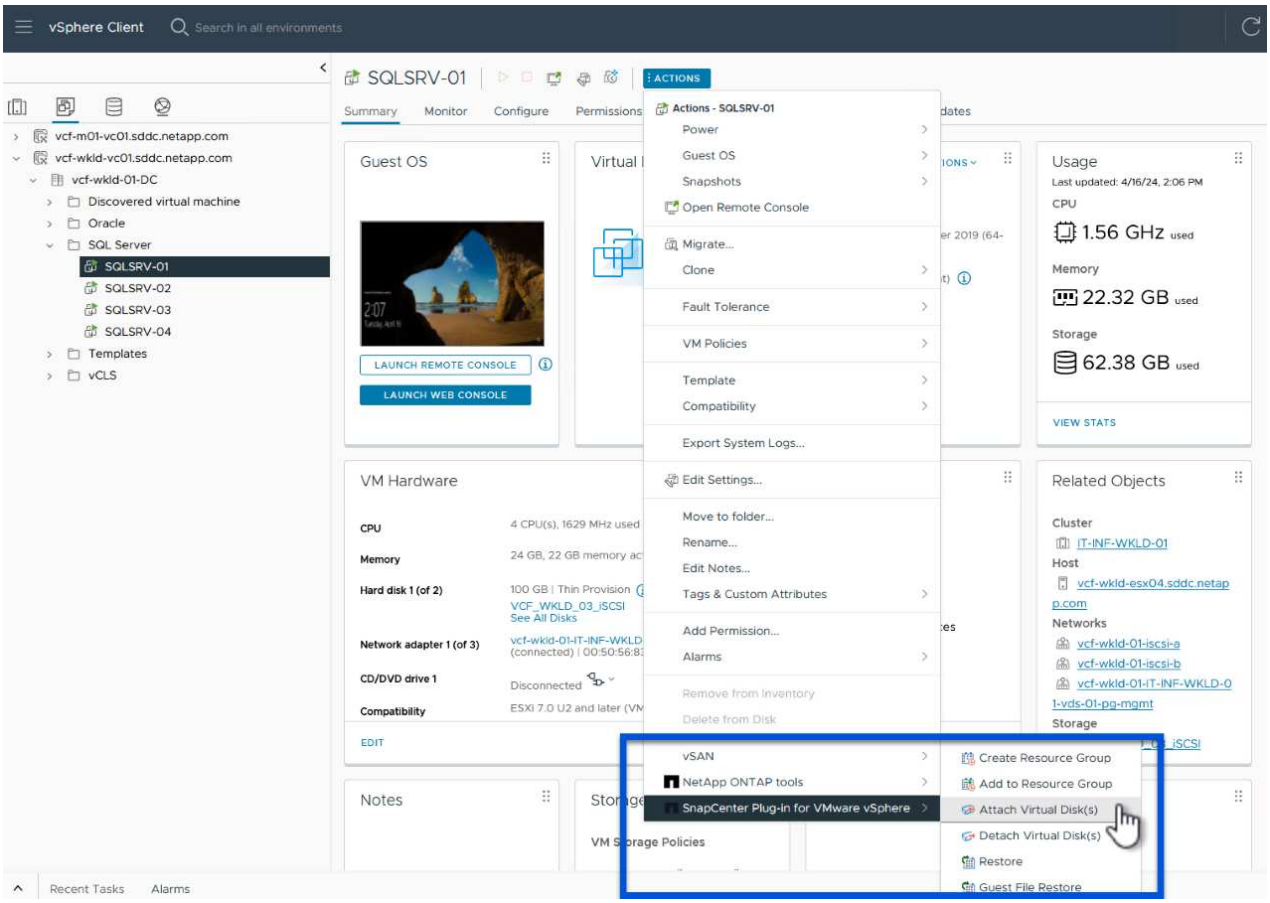

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

Ripristinare i VMDK utilizzando il plug-in SnapCenter

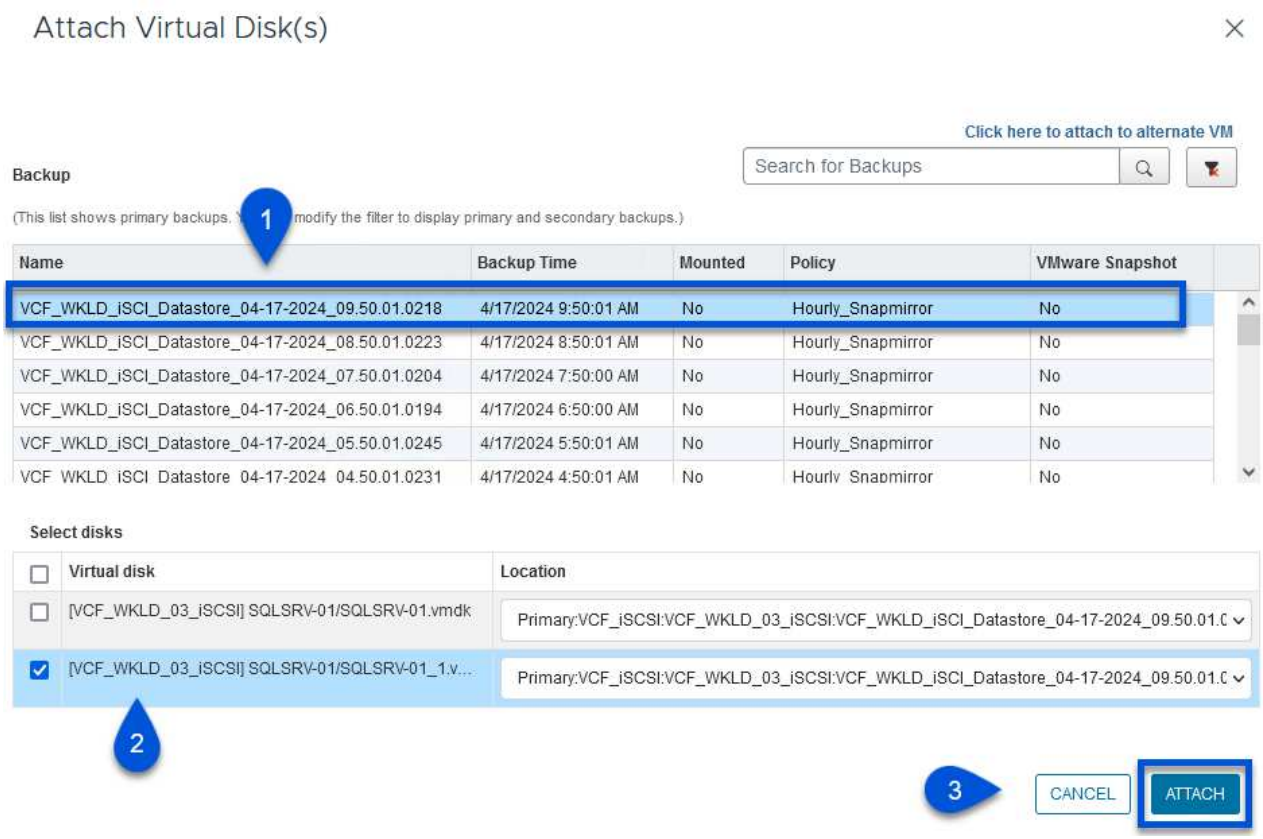
ONTAP Tools consente il ripristino completo dei VMDK nella loro posizione originale o la possibilità di collegare un VMDK come nuovo disco a un sistema host. In questo scenario, un VMDK verrà collegato a un host Windows per accedere al file system.

Per allegare un VMDK da un backup, completare i seguenti passaggi:

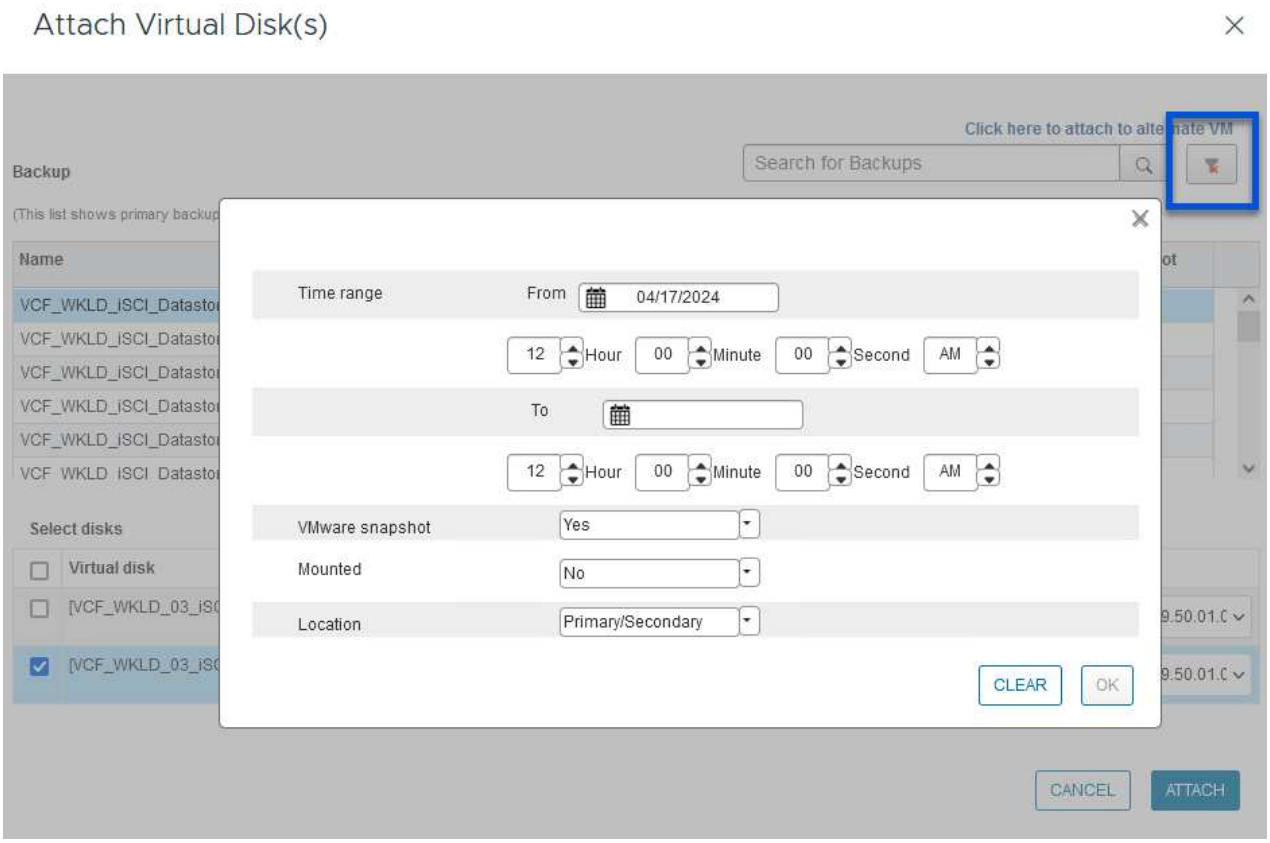
1. Nel vSphere Client, accedere a una VM e, dal menu **Azioni**, selezionare * SnapCenter Plug-in for VMware vSphere > Collega disco/i virtuale/i*.



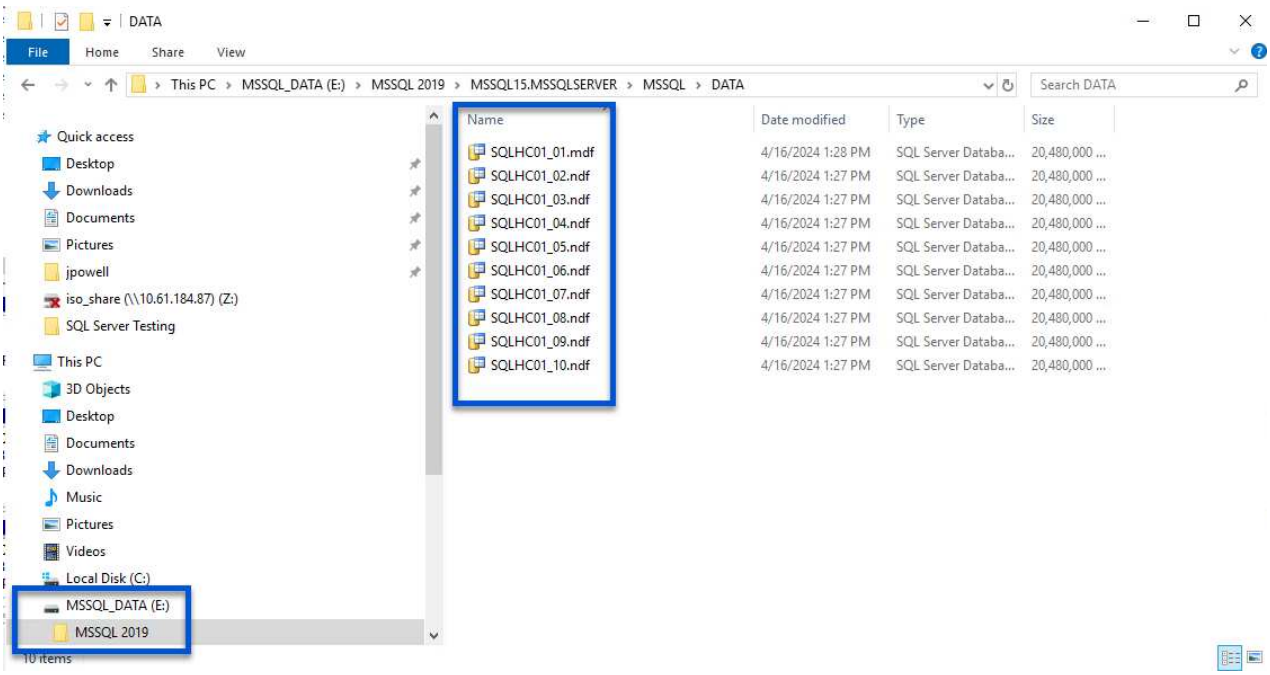
2. Nella procedura guidata **Collega disco/i virtuale/i**, seleziona l'istanza di backup da utilizzare e il VMDK specifico da collegare.



È possibile utilizzare le opzioni di filtro per individuare i backup e visualizzare i backup provenienti dai sistemi di archiviazione primari e secondari.



3. Dopo aver selezionato tutte le opzioni, fare clic sul pulsante **Allega** per avviare il processo di ripristino e allegare il VMDK all'host.
4. Una volta completata la procedura di collegamento, è possibile accedere al disco dal sistema operativo del sistema host. In questo caso SCV ha collegato il disco con il suo file system NTFS all'unità E: del nostro Windows SQL Server e i file del database SQL sul file system sono accessibili tramite Esplora file.



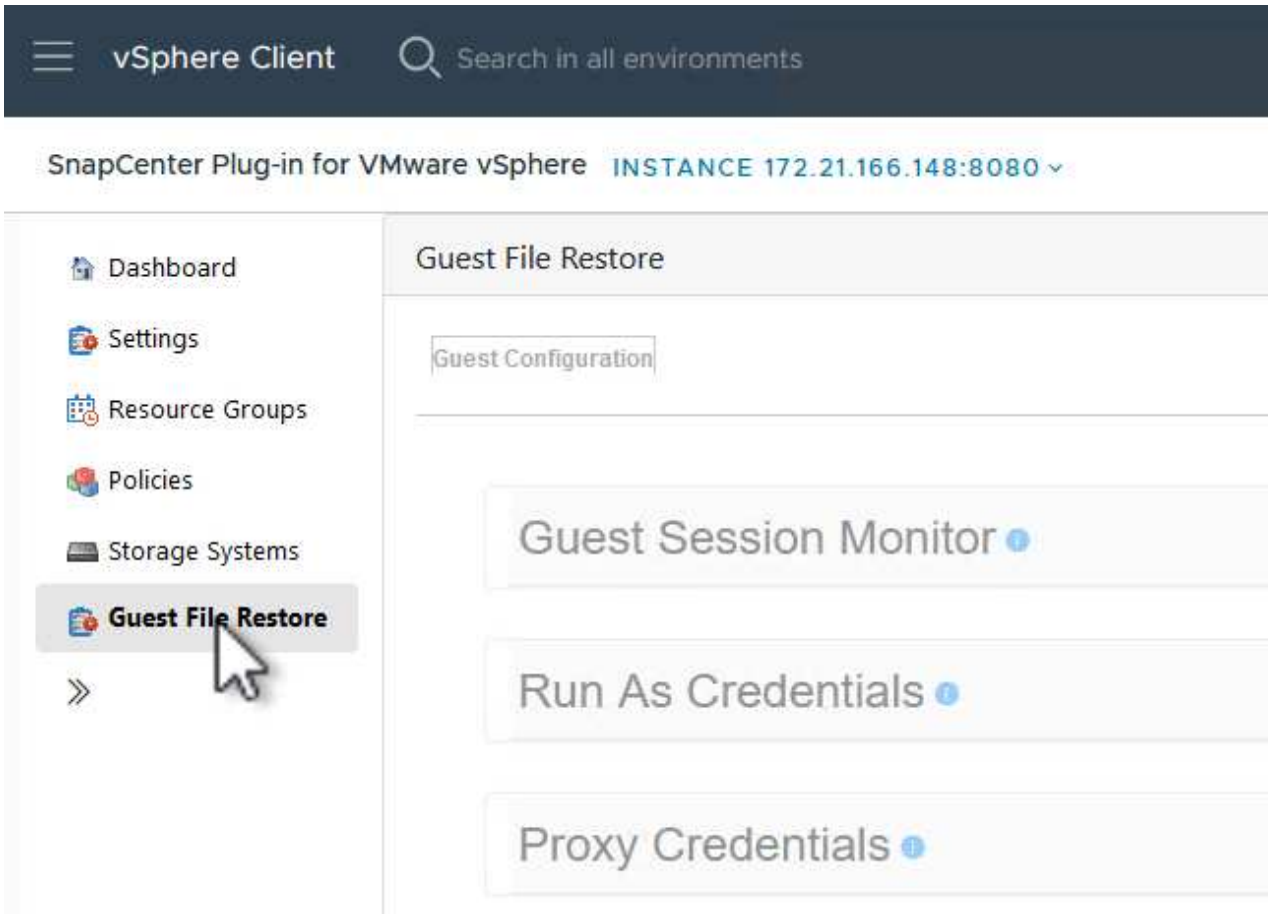
Ripristino del file system guest tramite il plug-in SnapCenter

ONTAP Tools consente di ripristinare il file system guest da un VMDK sui sistemi operativi Windows Server. Questa operazione viene eseguita centralmente dall'interfaccia del plug-in SnapCenter .

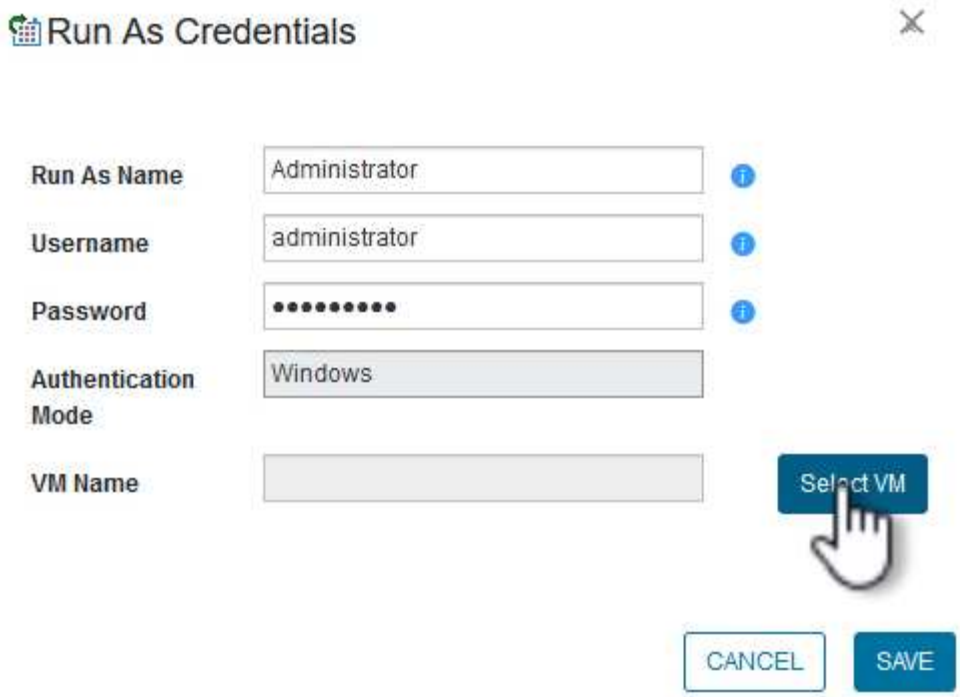
Per informazioni dettagliate fare riferimento a"Ripristina file e cartelle degli ospiti" sul sito di documentazione SCV.

Per eseguire un ripristino del file system guest per un sistema Windows, completare i seguenti passaggi:

1. Il primo passo è creare le credenziali Run As per fornire l'accesso al sistema host Windows. Nel vSphere Client, accedere all'interfaccia del plug-in CSV e fare clic su **Guest File Restore** nel menu principale.

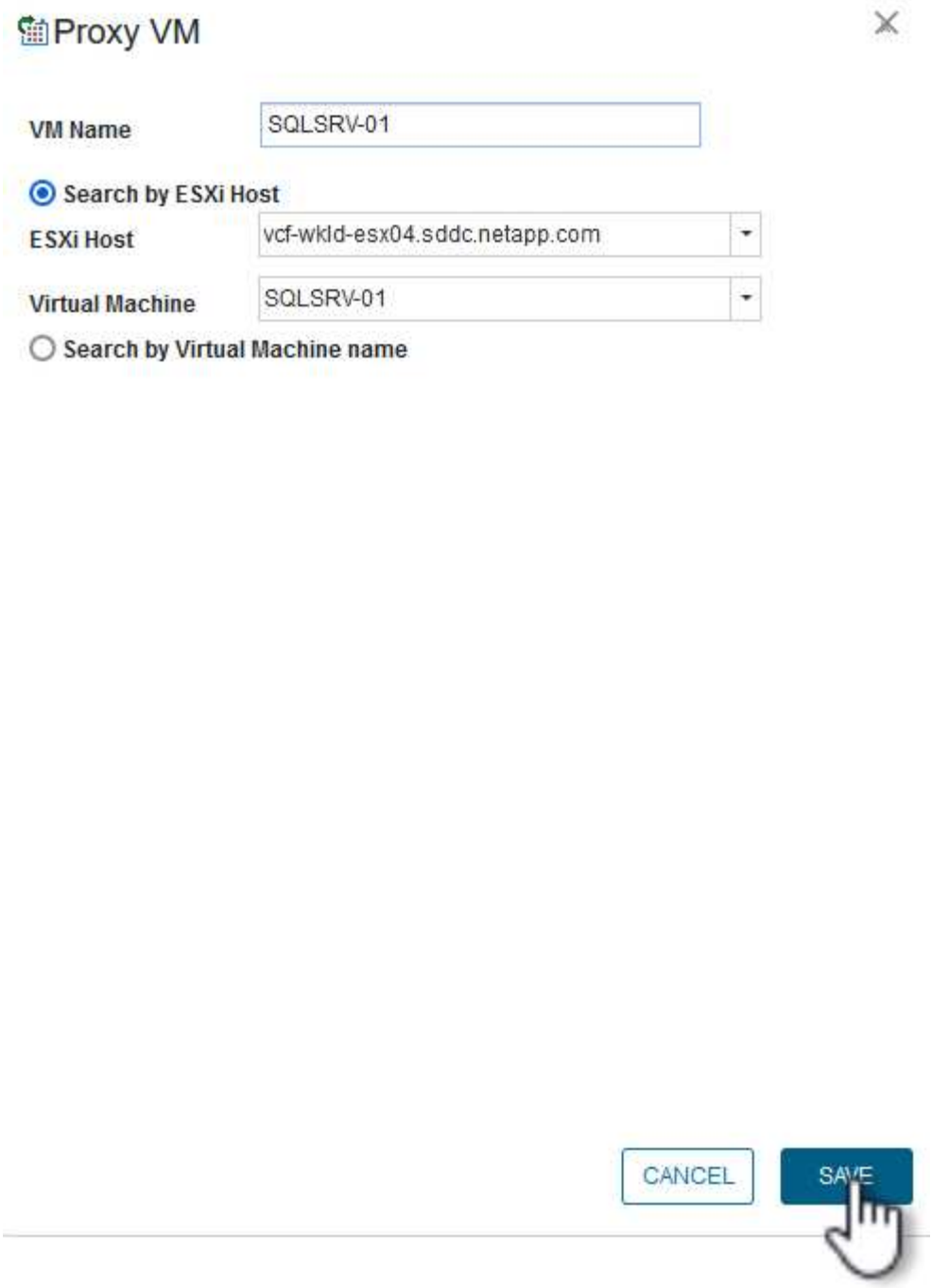


2. In **Esegui come credenziali** fare clic sull'icona **+** per aprire la finestra **Esegui come credenziali**.
3. Inserire un nome per il record delle credenziali, un nome utente e una password di amministratore per il sistema Windows, quindi fare clic sul pulsante **Seleziona VM** per selezionare una VM proxy facoltativa da utilizzare per il

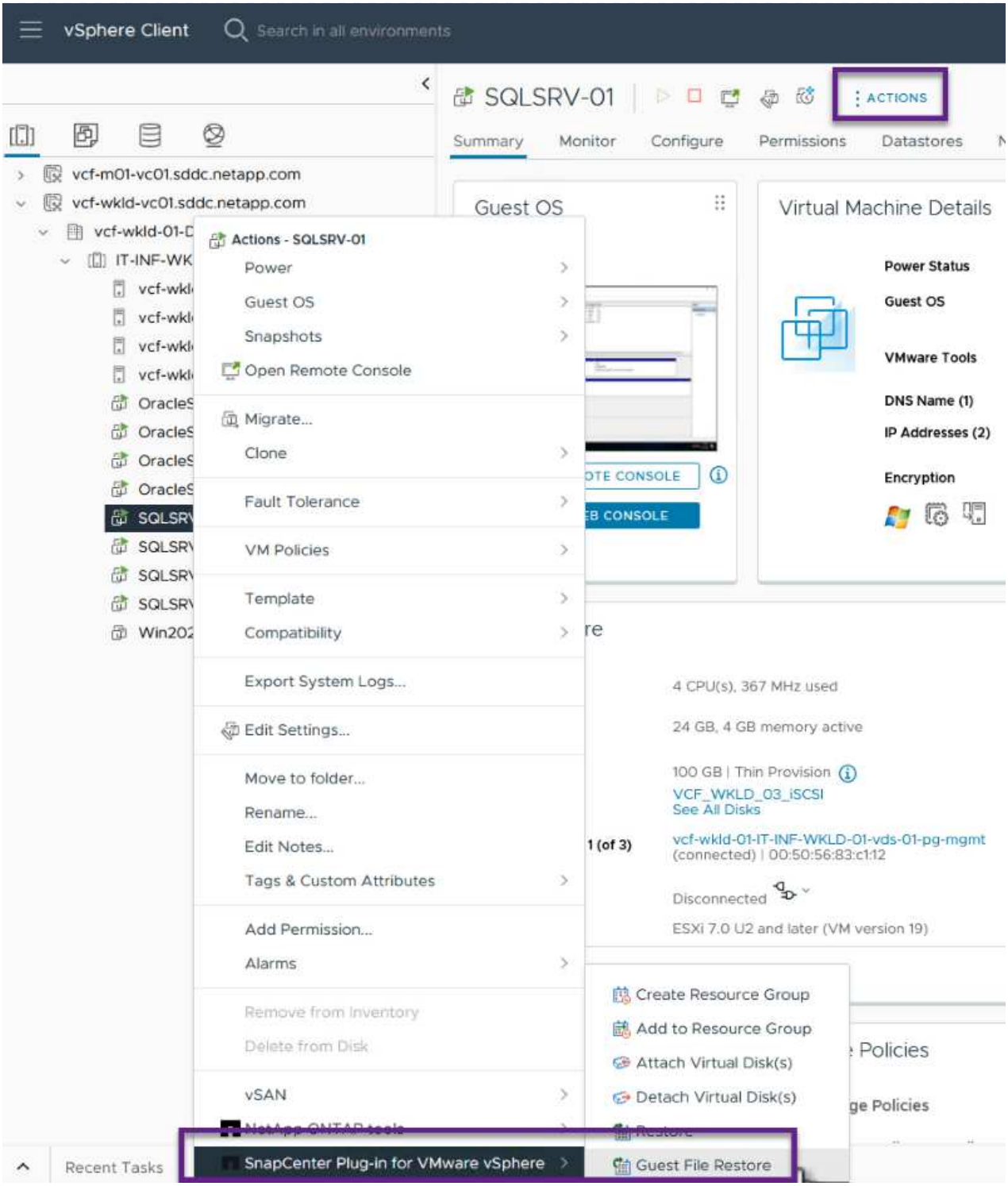


ripristino.

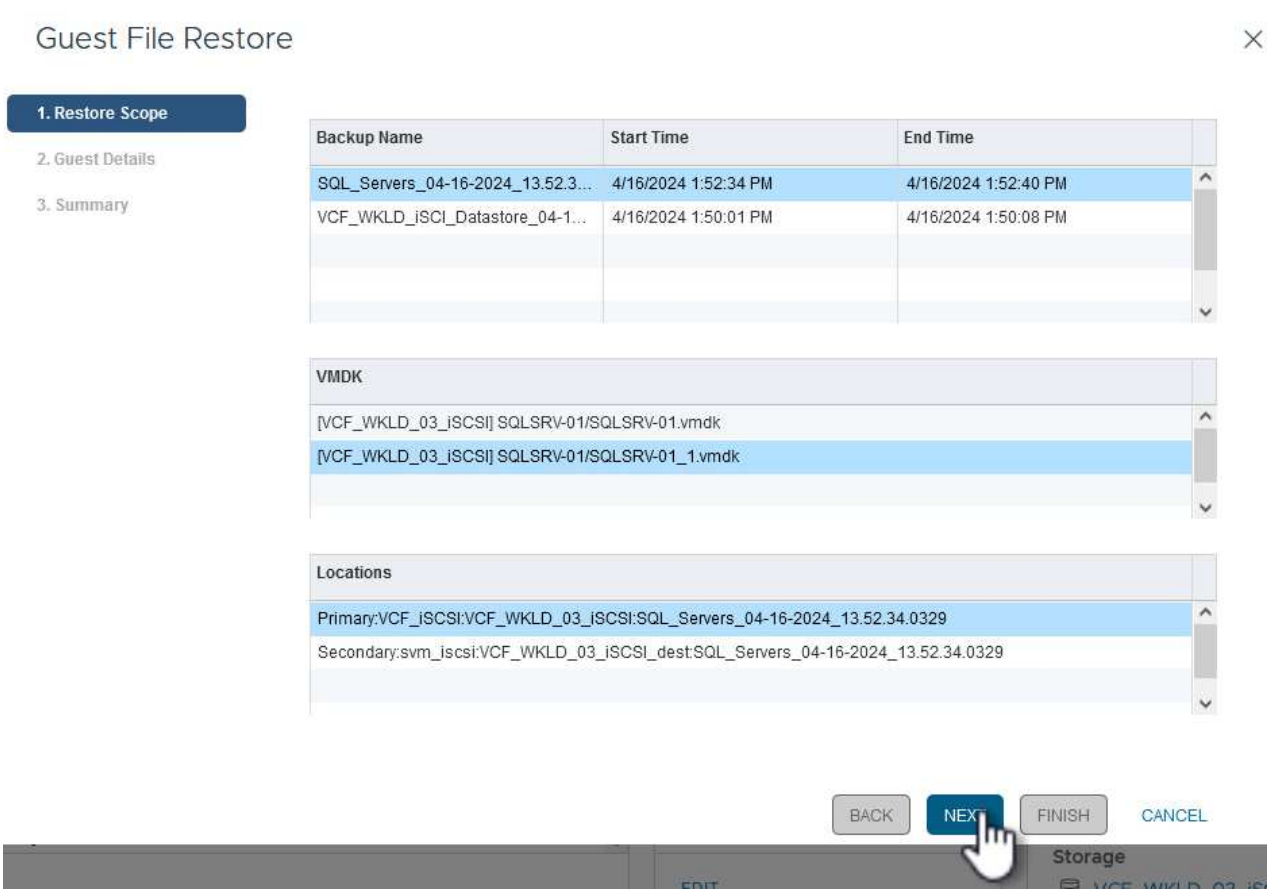
4. Nella pagina Proxy VM, fornire un nome per la VM e individuarla cercandola per host ESXi o per nome. Una volta selezionato, clicca su **Salva**.



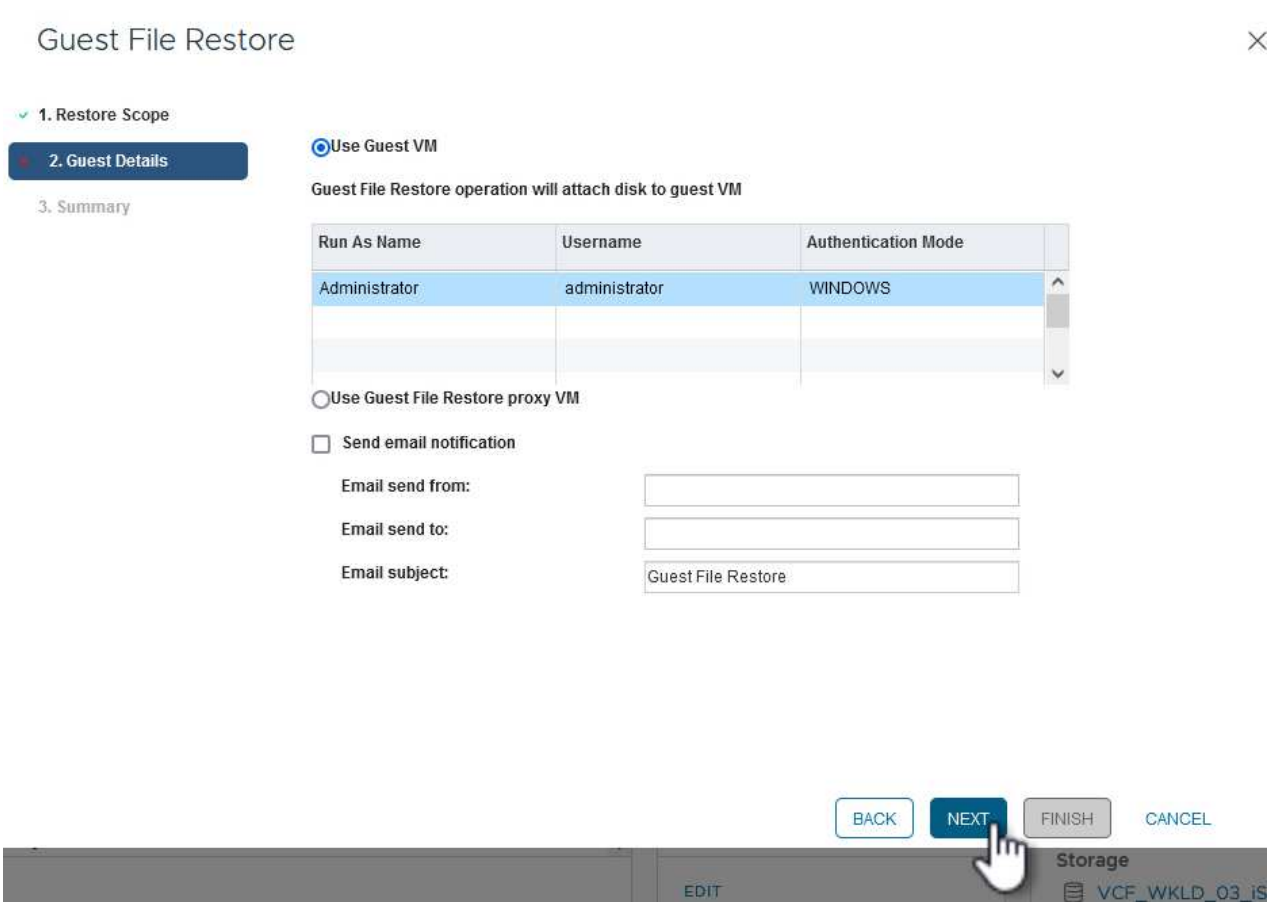
5. Fare nuovamente clic su **Salva** nella finestra **Esegui come credenziali** per completare il salvataggio del record.
6. Successivamente, accedi a una macchina virtuale nell'inventario. Dal menu **Azioni** o facendo clic con il pulsante destro del mouse sulla VM, selezionare * SnapCenter Plug-in for VMware vSphere > Ripristino file guest*.



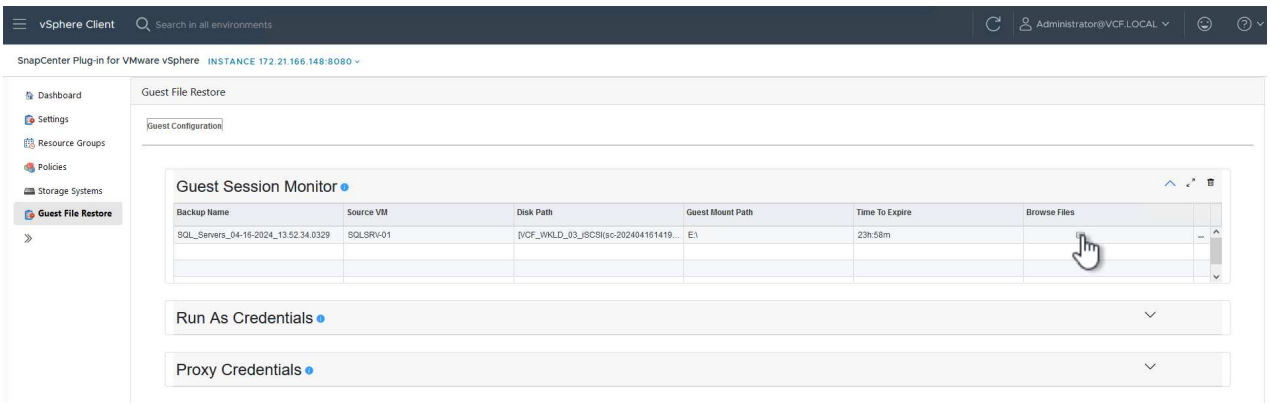
7. Nella pagina **Ambito di ripristino** della procedura guidata **Ripristino file guest**, selezionare il backup da cui effettuare il ripristino, il VMDK specifico e la posizione (primaria o secondaria) da cui ripristinare il VMDK. Fare clic su **Avanti** per continuare.



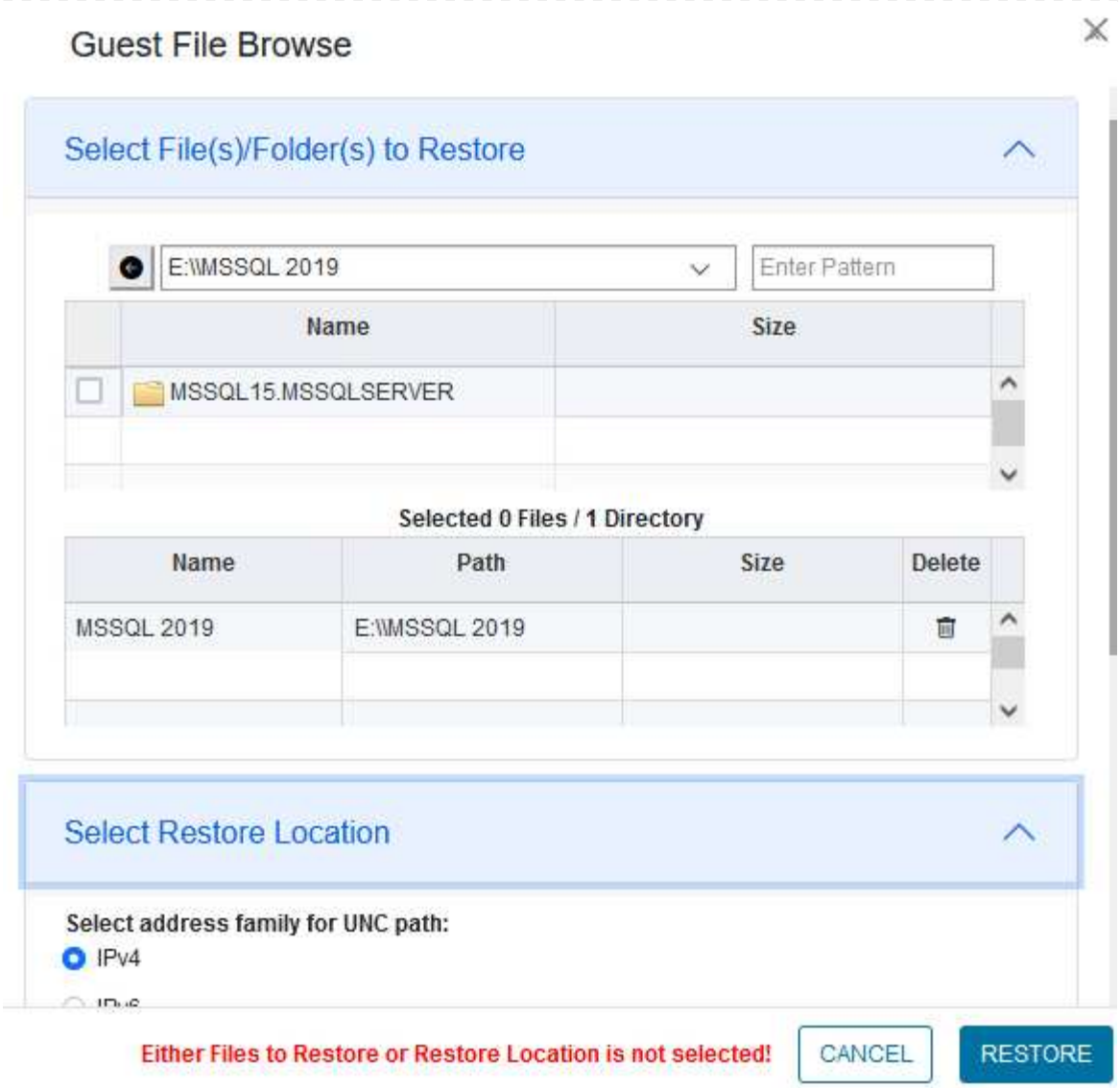
8. Nella pagina **Dettagli ospite**, seleziona se utilizzare **VM ospite** o **Utilizza VM proxy per il ripristino dei file ospite** per il ripristino. Se lo desideri, puoi anche compilare qui le impostazioni di notifica via email. Fare clic su **Avanti** per continuare.

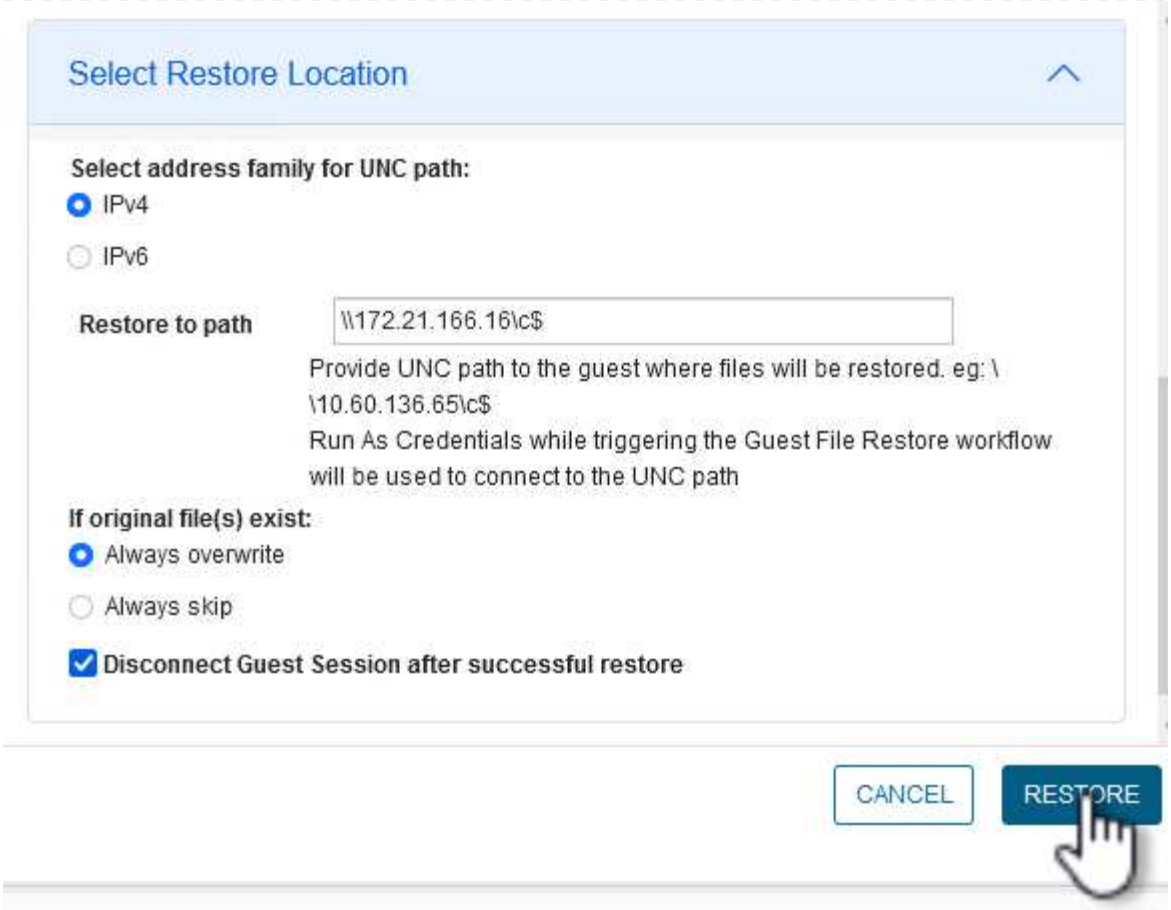


9. Infine, rivedere la pagina **Riepilogo** e fare clic su **Fine** per avviare la sessione di ripristino del file system guest.
10. Tornando all'interfaccia del plug-in SnapCenter , vai nuovamente a **Guest File Restore** e visualizza la sessione in esecuzione in **Guest Session Monitor**. Fare clic sull'icona sotto **Sfoglia file** per continuare.



11. Nella procedura guidata **Guest File Browse** seleziona la cartella o i file da ripristinare e la posizione del file system in cui ripristinarli. Infine, fare clic su **Ripristina** per avviare il processo di **Ripristino**.


Guest File Browse
Select File(s)/Folder(s) to Restore
E:\MSSQL 2019
Enter Pattern
Name
Size
MSSQL15.MSSQLSERVER
Selected 0 Files / 1 Directory
Name
Path
Size
Delete
MSSQL 2019
E:\MSSQL 2019
Select Restore Location
Select address family for UNC path:
IPv4
Either Files to Restore or Restore Location is not selected!
CANCEL
RESTORE



12. Il processo di ripristino può essere monitorato dal riquadro attività di vSphere Client.

Informazioni aggiuntive

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

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

Per informazioni sull'utilizzo del SnapCenter Plug-in for VMware vSphere, fare riferimento a "Documentazione SnapCenter Plug-in for VMware vSphere" .

Proteggere i domini di gestione e carico di lavoro VCF utilizzando il plug-in SnapCenter per VMware vSphere

Utilizzare il SnapCenter Plug-in for VMware vSphere per proteggere più domini VCF. Questa procedura include l'impostazione del plug-in per ciascun dominio, la configurazione dei criteri di backup e l'esecuzione delle operazioni di ripristino.

I domini dei carichi di lavoro VMware Cloud Foundation (VCF) consentono alle organizzazioni di separare logicamente le risorse in domini diversi per raggruppare carichi di lavoro diversi, migliorare la sicurezza e la tolleranza agli errori.

Introduzione

I domini possono essere scalati in modo indipendente, soddisfare specifiche conformità e fornire multi-tenancy. La protezione dei dati per VMware Cloud Foundation (VCF) è un aspetto fondamentale per garantire la disponibilità, l'integrità e la recuperabilità dei dati nel dominio di gestione e nei domini dei carichi di lavoro. NetApp SnapCenter Plug-in for VMware vSphere (SCV) è un potente strumento che integra le funzionalità di protezione dei dati di NetApp negli ambienti VMware. Semplifica il backup, il ripristino e la clonazione delle macchine virtuali (VM) VMware vSphere ospitate sullo storage NetApp .

Questo documento illustra i passaggi di distribuzione su come proteggere più domini VCF con SCV.

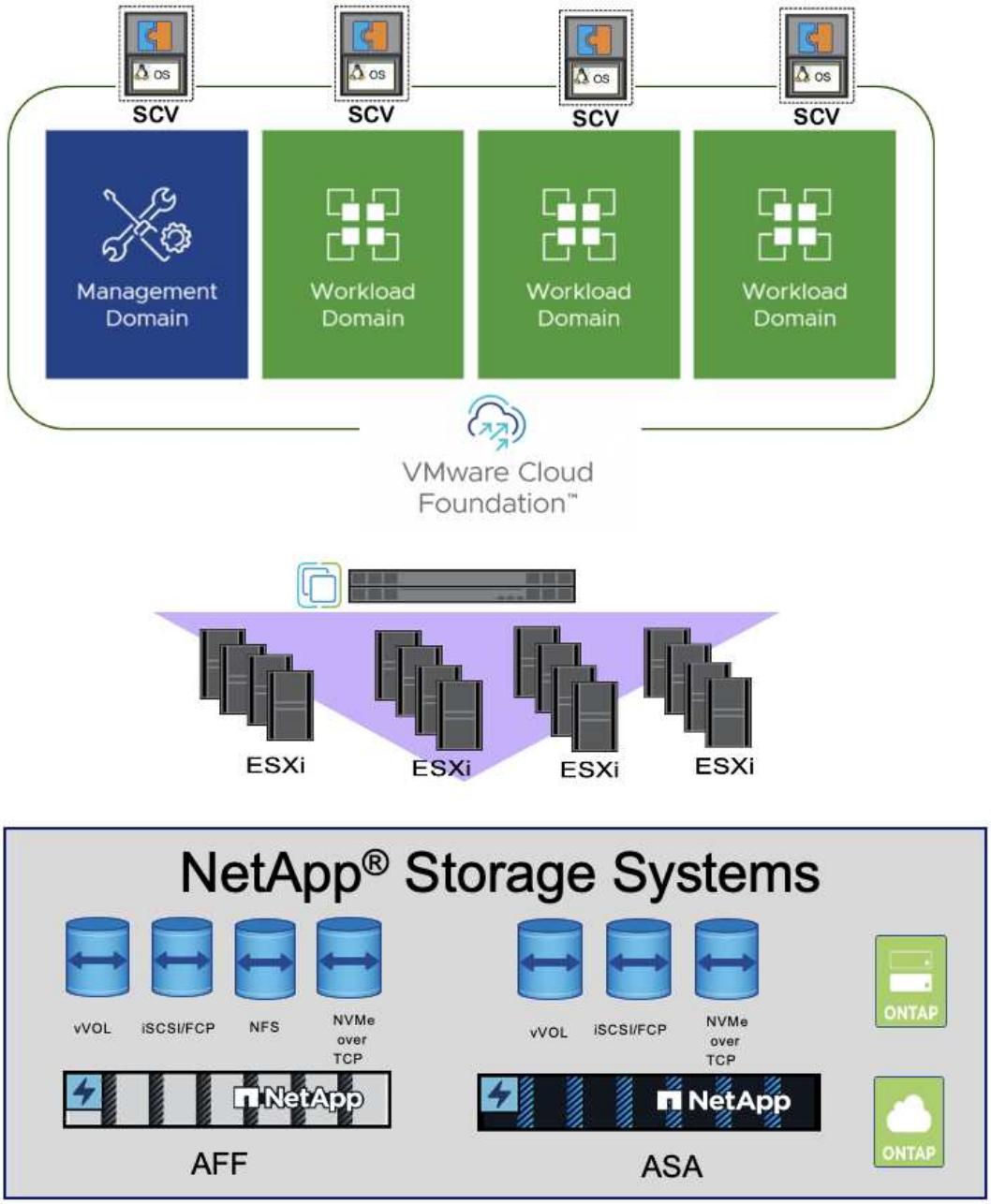
Pubblico

Architetti di soluzioni o amministratori di storage che garantiscono la protezione dei dati e il disaster recovery per i domini di carico di lavoro VMware VCF.

Panoramica dell'architettura

SCV viene distribuito come appliance virtuale Linux utilizzando un file OVA per fornire operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con la VM per VM, datastore, file e cartelle. SCV utilizza un'architettura plug-in remota. Erano presenti più SCV distribuiti e ospitati sul dominio di gestione VCF vCenter. Il dominio SCV e VCF ha una relazione uno a uno, pertanto il dominio di gestione VCF e ciascun dominio del carico di lavoro richiedono un SCV.

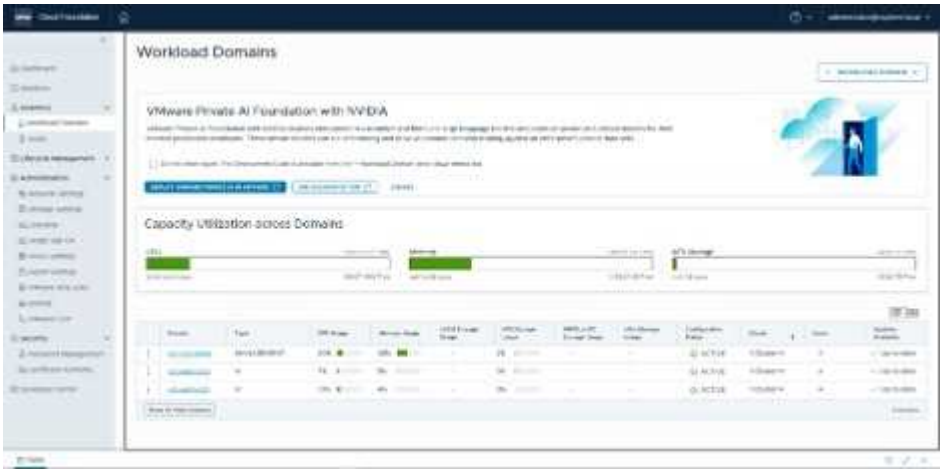
Dati presenti sui sistemi primari ONTAP FAS, AFF o All SAN Array (ASA) e replicati sui sistemi secondari ONTAP FAS, AFF o ASA . SCV funziona anche con SnapCenter Server per supportare operazioni di backup e ripristino basate su applicazioni in ambienti VMware per i plug-in specifici delle applicazioni SnapCenter . Per maggiori informazioni controlla,"Documentazione SnapCenter Plug-in for VMware vSphere ."



La regola di backup 3-2-1 è una strategia di protezione dei dati che prevede la creazione di tre copie dei dati, la loro archiviazione su due tipi diversi di supporti e la conservazione di una copia fuori sede. BlueXP backup and recovery è uno strumento basato su cloud per la gestione dei dati che fornisce un unico piano di controllo per un'ampia gamma di operazioni di backup e ripristino sia in ambienti locali che cloud. Una parte della suite BlueXP backup and recovery NetApp BlueXP è una funzionalità che si integra con SCV (on-premises) per estendere una copia dei dati all'archiviazione degli oggetti nel cloud. In questo modo viene creata una terza copia dei dati fuori sede, ricavata dai backup di archiviazione primari o secondari. Il BlueXP backup and recovery semplificano la configurazione di policy di archiviazione che trasferiscono copie dei dati da una di queste due posizioni locali. Per maggiori dettagli, controlla"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM" .

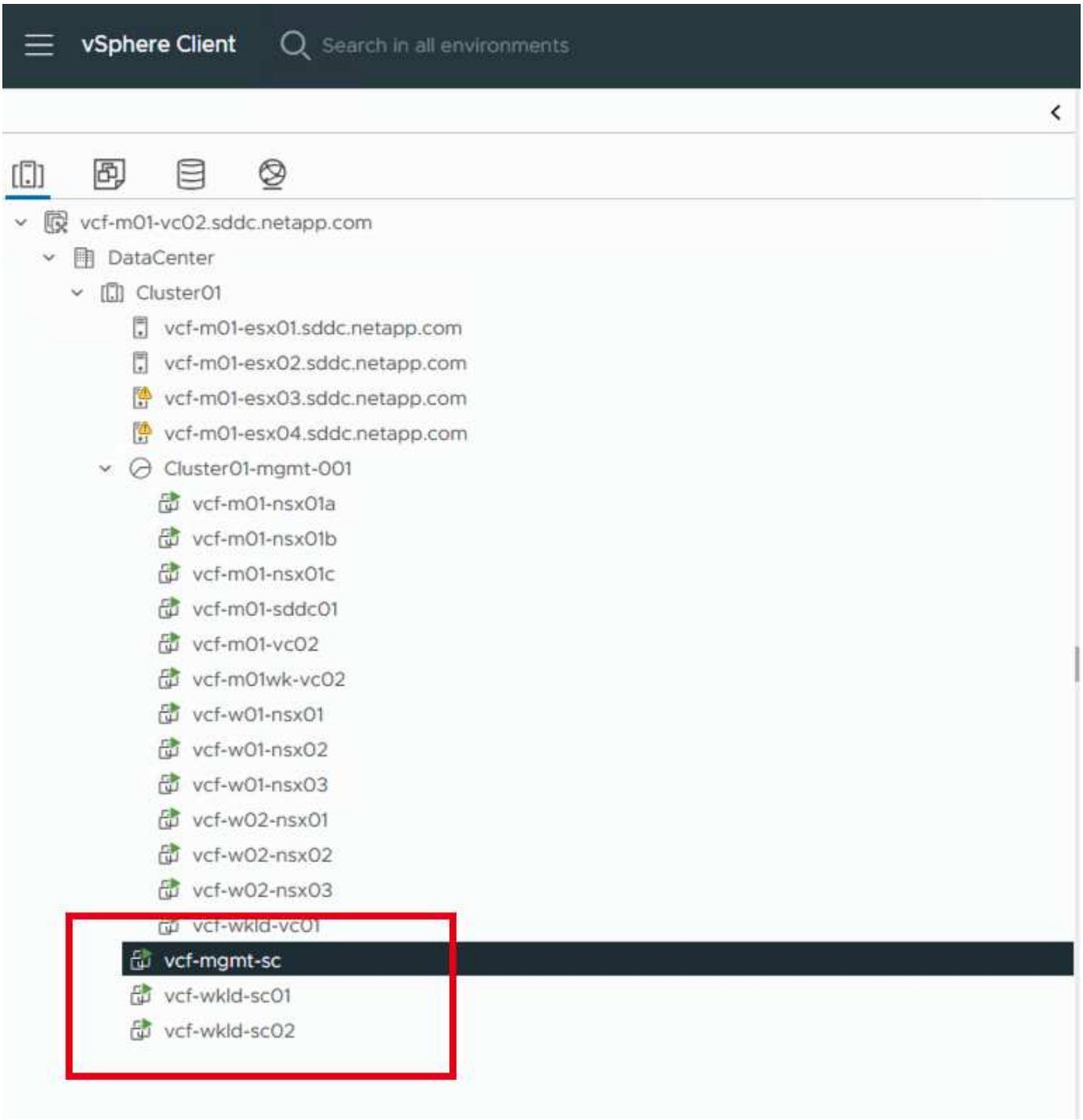
Distribuisci un VCF con dominio di gestione e più domini di carico di lavoro

Un dominio di carico di lavoro VCF è un gruppo di host ESXi con uno o più cluster vSphere, forniti da SDDC Manager e pronti per l'applicazione. Nell'esempio VCF riportato di seguito, sono stati distribuiti un dominio di gestione e due domini di carico di lavoro. Per maggiori dettagli su come distribuire VCF con lo storage NetApp , consultare"Documentazione sulla distribuzione di NetApp VCF."



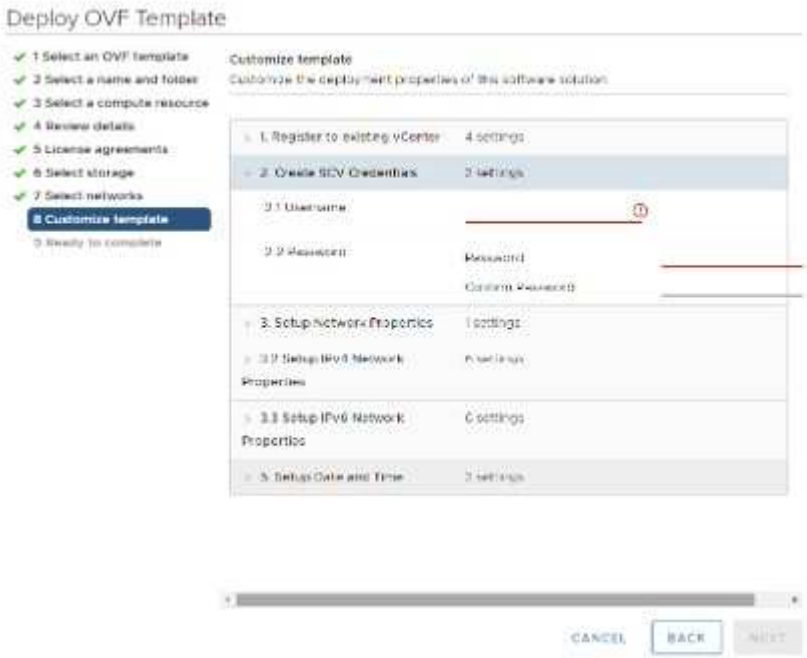
Fasi di distribuzione, configurazione e ripristino SCV

In base al numero di domini di carico di lavoro e al dominio di gestione, è necessario distribuire più SCV. Con due domini di carico di lavoro e un dominio di gestione, l'esempio seguente mostra tre SCV distribuiti sul dominio di gestione VCF
vCenter.


vSphere Client
Search in all environments
vcf-m01-vc02.sddc.netapp.com
DataCenter
Cluster01
vcf-m01-esx01.sddc.netapp.com
vcf-m01-esx02.sddc.netapp.com
vcf-m01-esx03.sddc.netapp.com
vcf-m01-esx04.sddc.netapp.com
Cluster01-mgmt-001
vcf-m01-nsx01a
vcf-m01-nsx01b
vcf-m01-nsx01c
vcf-m01-sddc01
vcf-m01-vc02
vcf-m01wk-vc02
vcf-w01-nsx01
vcf-w01-nsx02
vcf-w01-nsx03
vcf-w02-nsx01
vcf-w02-nsx02
vcf-w02-nsx03
vcf-wkld-vc01
vcf-mgmt-sc
vcf-wkld-sc01
vcf-wkld-sc02

Distribuisci SCV per il dominio di gestione e per ciascun dominio del carico di lavoro

1. "Scarica l'Open Virtual Appliance (OVA)."
2. Accedere al vCenter Server tramite vSphere Client. Vai su Amministrazione > Certificati > Gestione certificati. Aggiungere certificati radice attendibili e installare ciascun certificato nella cartella certs. Una volta installati i certificati, OVA può essere verificato e distribuito.
3. Accedi al dominio del carico di lavoro VCF vCenter e distribuisci il modello OVF per avviare la procedura guidata di distribuzione



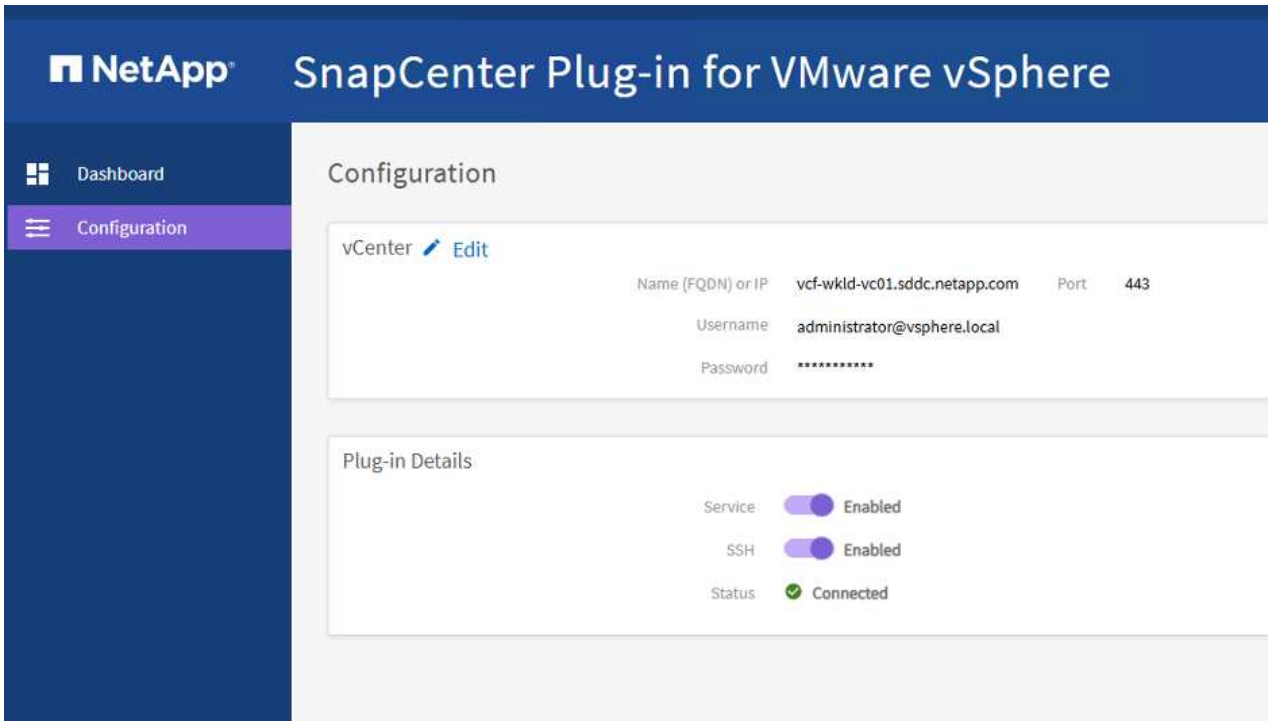
VMware.

4. Accendi OVA per avviare SCV, quindi fai clic su Installa strumenti VMware.
5. Generare il token MFA dalla console OVA, menu di configurazione del

sistema.

```
System Configuration Menu:
--------------------------
   1 ) Reboot virtual machine
   2 ) Shut down virtual machine
   3 ) Change 'maint' user password
   4 ) Change time zone
   5 ) Change NTP server
   6 ) Enable SSH access
   7 ) Increase jail disk size (/jail)
   8 ) Upgrade
   9 ) Install VMware Tools
  10 ) Generate MFA Token

   b ) Back
   x ) Exit

 Enter your choice: 10


Generating MFA Token... Your MFA Token is : 435164

 Press ENTER to continue._
```

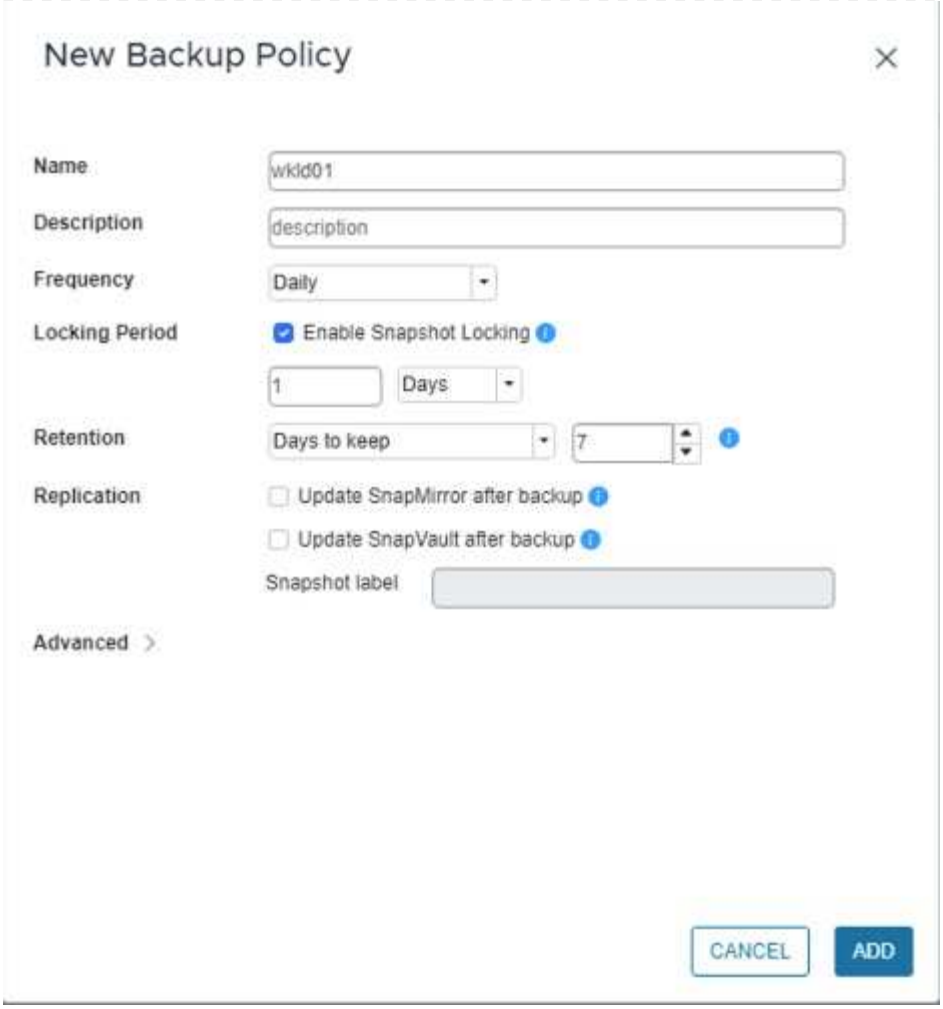
6. Accedere all'interfaccia utente grafica di gestione SCV con il nome utente e la password di amministratore impostati al momento della distribuzione e il token MFA generato tramite la console di manutenzione.
   `https://<appliance-IP-address>:8080` per accedere all'interfaccia grafica di gestione.



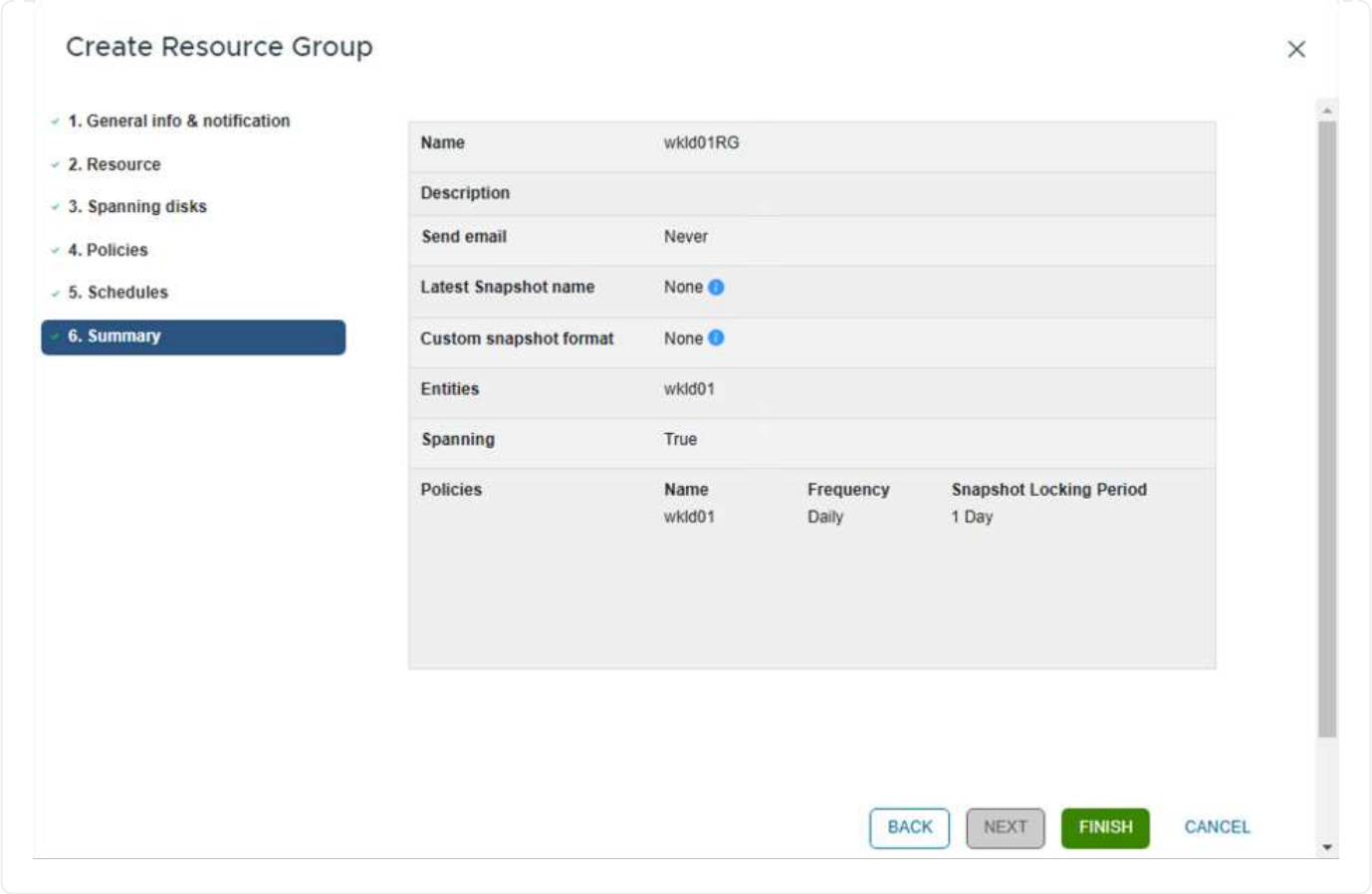
Configurare SCV

Per eseguire il backup o il ripristino delle VM, aggiungere prima i cluster di archiviazione o le VM che ospitano i datastore, quindi creare criteri di backup per la conservazione e la frequenza e impostare un gruppo di risorse per proteggere le
risorse.

1. Accedi al client Web vCenter e fai clic su Menu nella barra degli strumenti, quindi seleziona SnapCenter Plug-in for VMware vSphere e Aggiungi un archivio. Nel riquadro di navigazione sinistro del plug-in SCV, fare clic su Sistemi di archiviazione e quindi selezionare l'opzione Aggiungi. Nella finestra di dialogo Aggiungi sistema di archiviazione, immettere le informazioni di base sull'SVM o sul cluster e selezionare Aggiungi. Inserisci l'indirizzo IP dello storage NetApp ed effettua l'accesso.
2. Per creare un nuovo criterio di backup, nel riquadro di navigazione sinistro del plug-in SCV, fare clic su Criteri e selezionare Nuovo criterio. Nella pagina Nuovo criterio di backup, immettere le informazioni di configurazione del criterio e fare clic su Aggiungi.



3. Nel riquadro di navigazione sinistro del plug-in SCV, fare clic su Gruppi di risorse, quindi selezionare Crea. Immettere le informazioni richieste in ogni pagina della procedura guidata Crea gruppo di risorse, selezionare le VM e gli archivi dati da includere nel gruppo di risorse, quindi selezionare i criteri di backup da applicare al gruppo di risorse e specificare la pianificazione del backup.

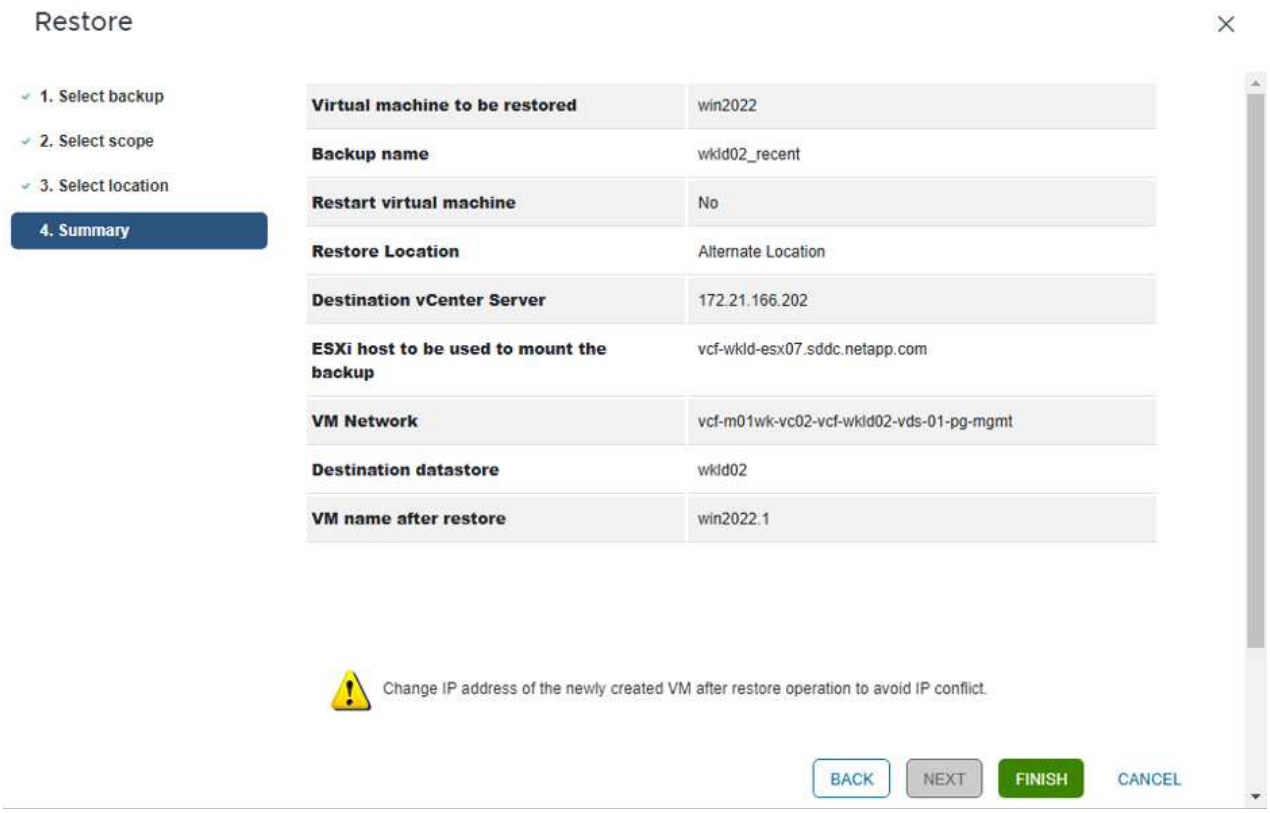

Create Resource Group
1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary
Name
wkld01RG
Description
Send email
Never
Latest Snapshot name
None
Custom snapshot format
None
Entities
wkld01
Spanning
True
Policies
Name
wkld01
Frequency
Daily
Snapshot Locking Period
1 Day
BACK
NEXT
FINISH
CANCEL

Ripristina la macchina virtuale e il backup di file o cartelle

È possibile ripristinare VM, VMDK, file e cartelle dai backup. La VM può essere ripristinata sull'host originale o su un host alternativo nello stesso vCenter Server oppure su un host ESXi alternativo gestito dallo stesso vCenter. È possibile montare un datastore tradizionale da un backup se si desidera accedere ai file nel backup. È possibile montare il backup sullo stesso host ESXi in cui è stato creato oppure su un host ESXi alternativo che abbia lo stesso tipo di configurazione host e VM. È possibile montare un datastore più volte su un host. È anche possibile ripristinare singoli file e cartelle in una sessione di ripristino file guest, che allega una copia di backup di un disco virtuale e quindi ripristina i file o le cartelle selezionati. È possibile ripristinare anche file e cartelle.

Passaggi di ripristino della VM

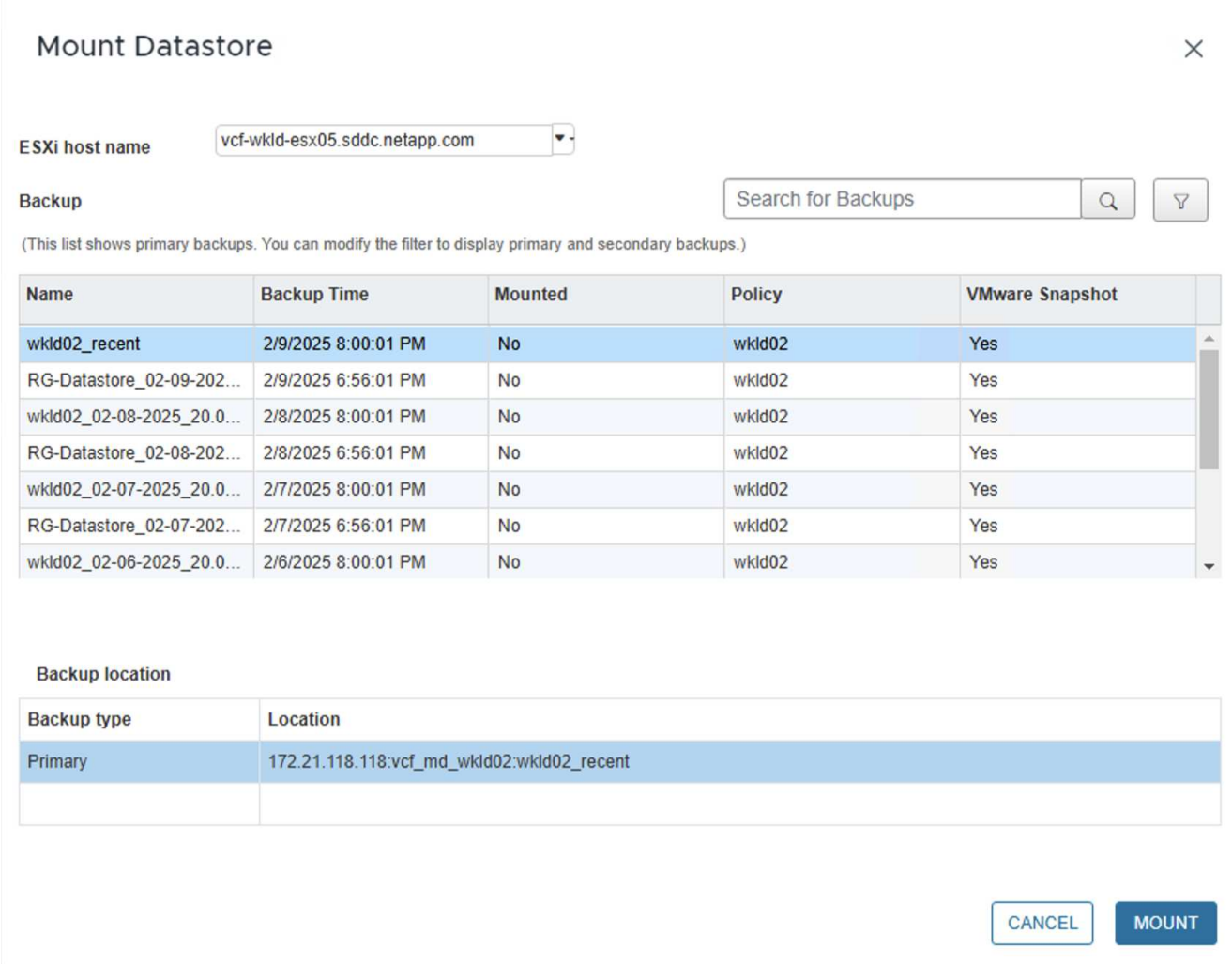
1. Nell'interfaccia utente grafica del client VMware vSphere, fare clic su Menu nella barra degli strumenti e selezionare VM e modelli dall'elenco a discesa, fare clic con il pulsante destro del mouse su una VM e selezionare SnapCenter Plug-in for VMware vSphere nell'elenco a discesa, quindi selezionare Ripristina nell'elenco a discesa secondario per avviare la procedura guidata.
2. Nella procedura guidata di ripristino, seleziona lo snapshot di backup che desideri ripristinare e seleziona Intera macchina virtuale nel campo Ambito di ripristino, seleziona la posizione di ripristino e quindi immetti le informazioni sulla destinazione in cui montare il backup. Nella pagina Seleziona posizione, seleziona la posizione per il datastore ripristinato. Rivedi la pagina Riepilogo e fai clic su Fine.



3. Monitorare l'avanzamento dell'operazione cliccando su Attività recenti nella parte inferiore dello schermo.

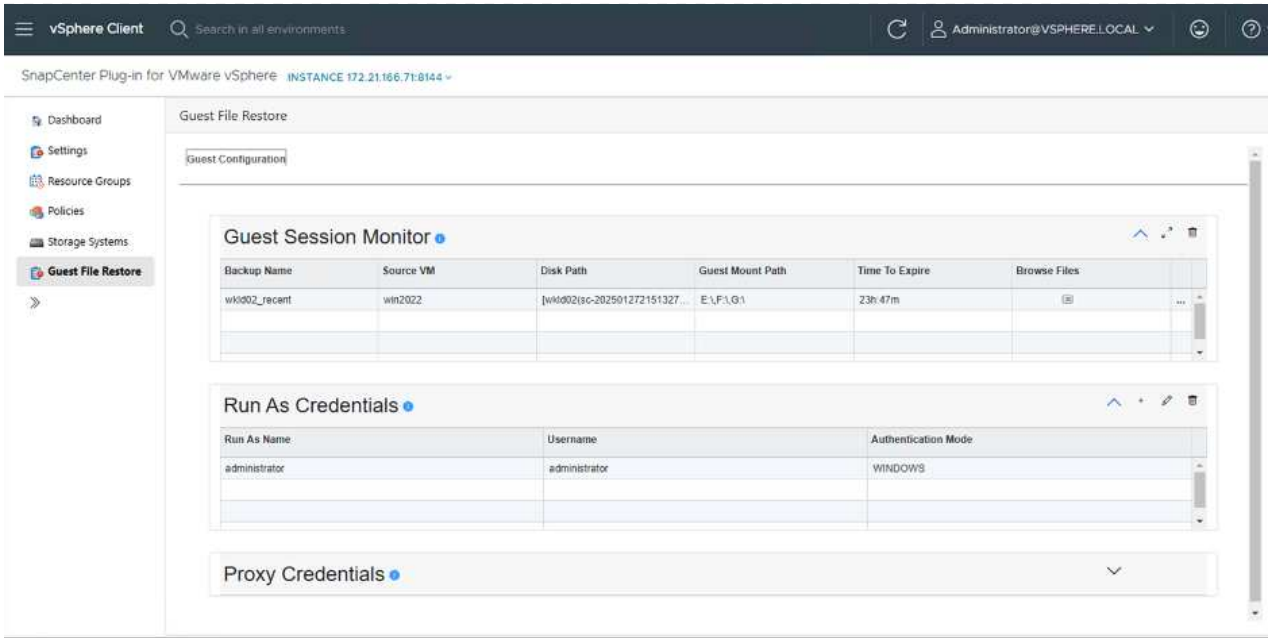
Passaggi di ripristino del datastore

1. Fare clic con il pulsante destro del mouse su un datastore e selezionare SnapCenter Plug-in for VMware vSphere > Monta backup.
2. Nella pagina Monta datastore, seleziona un backup e una posizione di backup (primaria o secondaria), quindi fai clic su Monta.

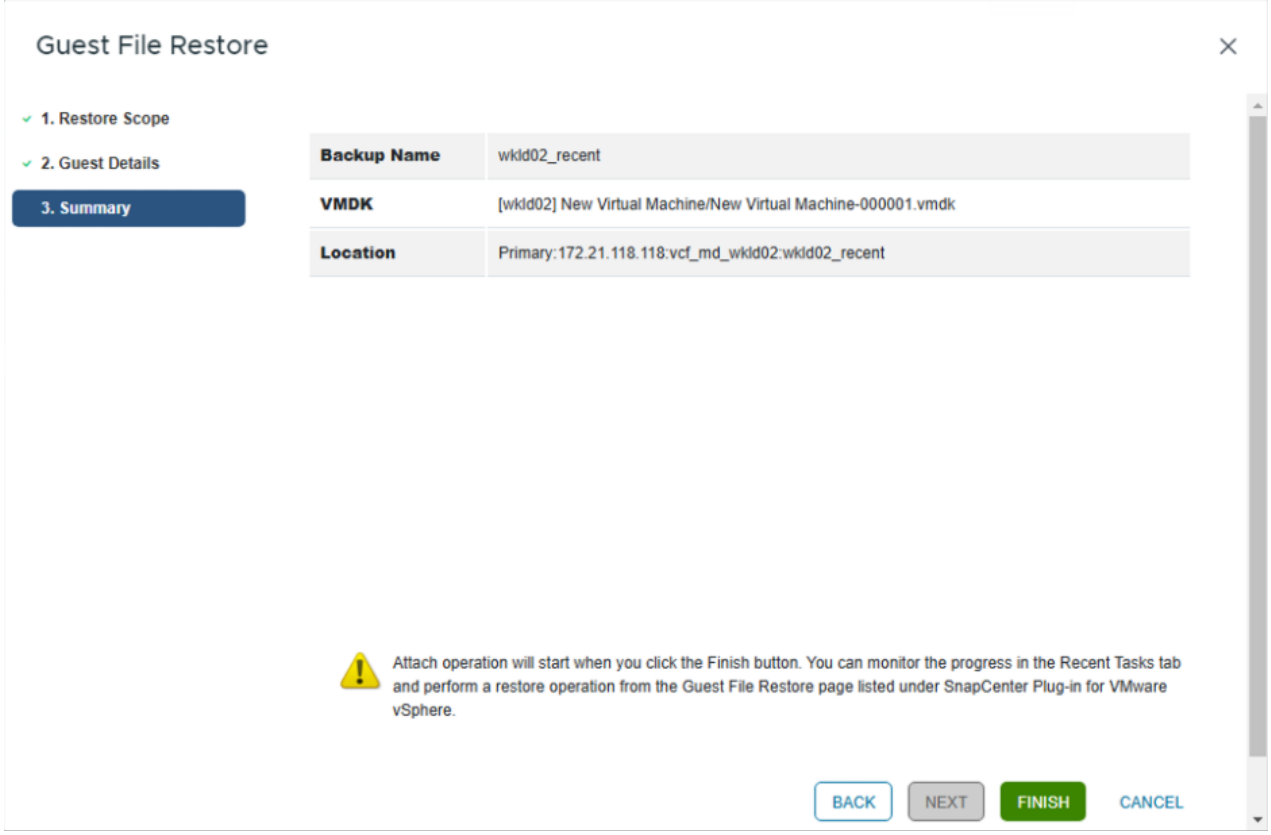


Passaggi per il ripristino di file e cartelle

1. Quando si collega un disco virtuale per operazioni di ripristino di file o cartelle guest, la macchina virtuale di destinazione per il collegamento deve disporre di credenziali configurate prima del ripristino. Dal SnapCenter Plug-in for VMware vSphere , nella sezione plug-in, selezionare Ripristino file guest ed Esegui come credenziali, quindi immettere le credenziali utente. Per Nome utente, devi inserire "Amministratore".



2. Fare clic con il pulsante destro del mouse sulla VM dal client vSphere e selezionare SnapCenter Plug-in for VMware vSphere > Ripristino file guest. Nella pagina Ambito di ripristino, specificare Nome backup, disco virtuale VMDK e Posizione: primaria o secondaria. Fare clic su Riepilogo per confermare.



NetApp SnapCenter per VCP multi-dominio centralizza la protezione dei dati, riduce in modo efficiente il tempo e lo spazio di archiviazione necessari per i backup utilizzando snapshot NetApp , supporta ambienti VMware su larga scala con solide funzionalità di backup e replica e consente il ripristino granulare di intere VM, VMDK

specifici o singoli file.

Demo video per proteggere più domini VCF con SCV

Proteggi più domini VMware VCF con NetApp SCV

Proteggi i domini dei carichi di lavoro VCF con l'archiviazione NVMe su TCP e il plug-in SnapCenter per VMware vSphere

Utilizzare il SnapCenter Plug-in for VMware vSphere per proteggere i domini dei carichi di lavoro VCF con NVMe. Questa procedura include l'impostazione del plug-in, la configurazione di NVMe su TCP per prestazioni ottimali e l'esecuzione di operazioni di backup, ripristino o clonazione.

NVMe (Non-Volatile Memory Express) su TCP è un protocollo di rete all'avanguardia che facilita il trasferimento dati ad alta velocità tra i server VMware Cloud Foundation ESXi e lo storage NetApp , inclusi All Flash FAS (AFF) e All SAN Array (ASA).

Introduzione

L'utilizzo di NVMe su TCP garantisce bassa latenza e throughput elevato per carichi di lavoro impegnativi. L'integrazione di NVMe su TCP con il SnapCenter Plug-in for VMware vSphere-in NetApp SnapCenter per VMware vSphere (SCV) offre una potente combinazione per una gestione efficiente dei dati, migliorando le operazioni di backup, ripristino e clonazione negli ambienti VMware.

Vantaggi di NVMe rispetto a TCP

- Alte prestazioni: offre prestazioni eccezionali con bassa latenza e velocità di trasferimento dati elevate. Ciò è fondamentale per le applicazioni più esigenti e le operazioni sui dati su larga scala.
- Scalabilità: supporta configurazioni scalabili, consentendo agli amministratori IT di espandere la propria infrastruttura senza problemi man mano che aumentano i requisiti dei dati.
- Efficienza: consente operazioni di backup e ripristino più rapide, riducendo i tempi di inattività e migliorando la disponibilità complessiva del sistema.

Questo documento illustra i passaggi per distribuire e gestire SCV negli ambienti VMware Cloud Foundation (VCF), con particolare attenzione allo sfruttamento di NVMe su TCP per prestazioni ottimali.

Pubblico

Architetti di soluzioni o amministratori di storage che garantiscono la protezione dei dati e il disaster recovery per i domini di carico di lavoro VMware VCF.

Panoramica dell'architettura

SCV è un potente strumento progettato per facilitare operazioni di backup e ripristino rapide, efficienti in termini di spazio, coerenti con gli arresti anomali e con le VM per VM, datastore, file e cartelle in ambienti VMware. SCV viene distribuito come appliance virtuale Linux utilizzando un file OVA e sfrutta un'architettura plug-in remota.

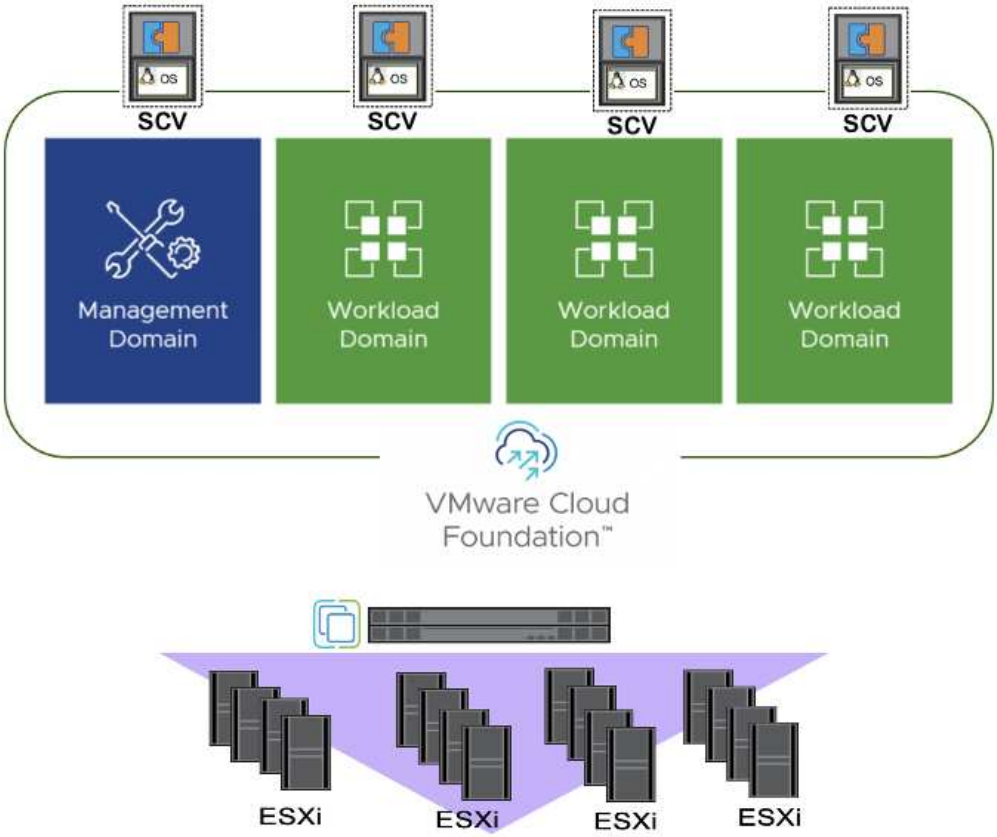
Architettura di distribuzione SCV

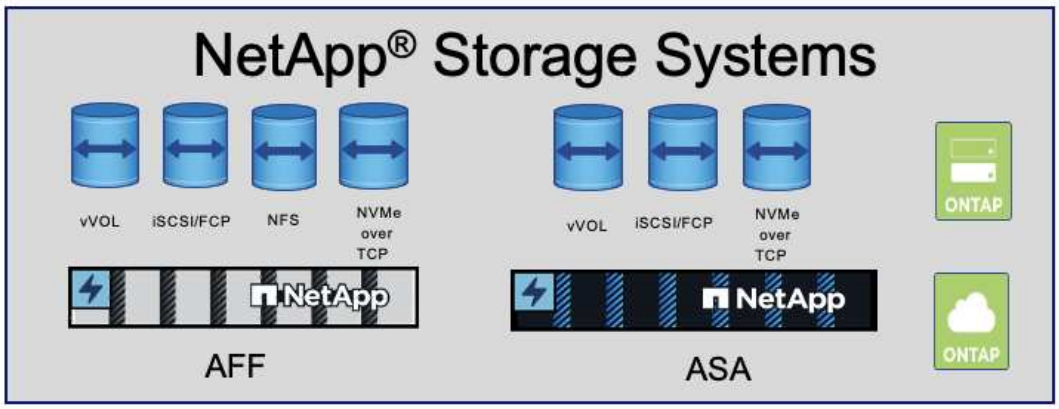
- Distribuzione di appliance virtuali: SCV viene distribuito come appliance virtuale Linux utilizzando un file

OVA. Questo metodo di distribuzione garantisce un processo di configurazione semplificato ed efficiente.

- Architettura plug-in remota: SCV utilizza un'architettura plug-in remota, consentendo scalabilità e flessibilità nella gestione di più istanze.
- Relazione uno a uno: ogni dominio VCF richiede un'istanza SCV dedicata, garantendo operazioni di backup e ripristino isolate ed efficienti.

Con ONTAP 9.10.1 e versioni successive, NetApp AFF e ASA supportano NVMe su TCP. Dati presenti sui sistemi primari AFF o ASA e che possono essere replicati sui sistemi secondari ONTAP AFF o ASA . SCV funziona anche con SnapCenter Server per supportare operazioni di backup e ripristino basate su applicazioni in ambienti VMware per i plug-in specifici delle applicazioni SnapCenter . Per maggiori informazioni controlla,"Documentazione SnapCenter Plug-in for VMware vSphere" E"Proteggi i carichi di lavoro con SnapCenter"





La regola di backup 3-2-1 è una strategia di protezione dei dati che prevede la creazione di tre copie dei dati, la loro archiviazione su due tipi diversi di supporti e la conservazione di una copia fuori sede. BlueXP backup and recovery è uno strumento basato su cloud per la gestione dei dati che fornisce un unico piano di controllo per un'ampia gamma di operazioni di backup e ripristino sia in ambienti locali che cloud. Una parte della suite BlueXP backup and recovery NetApp BlueXP è una funzionalità che si integra con SCV (on-premises) per estendere una copia dei dati all'archiviazione degli oggetti nel cloud. In questo modo viene creata una terza copia dei dati fuori sede, ricavata dai backup di archiviazione primari o secondari. Il BlueXP backup and recovery semplificano la configurazione di policy di archiviazione che trasferiscono copie dei dati da una di queste due posizioni locali. Per maggiori dettagli, controlla"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM" .

Passaggi di distribuzione SCV per VCF su NVMe

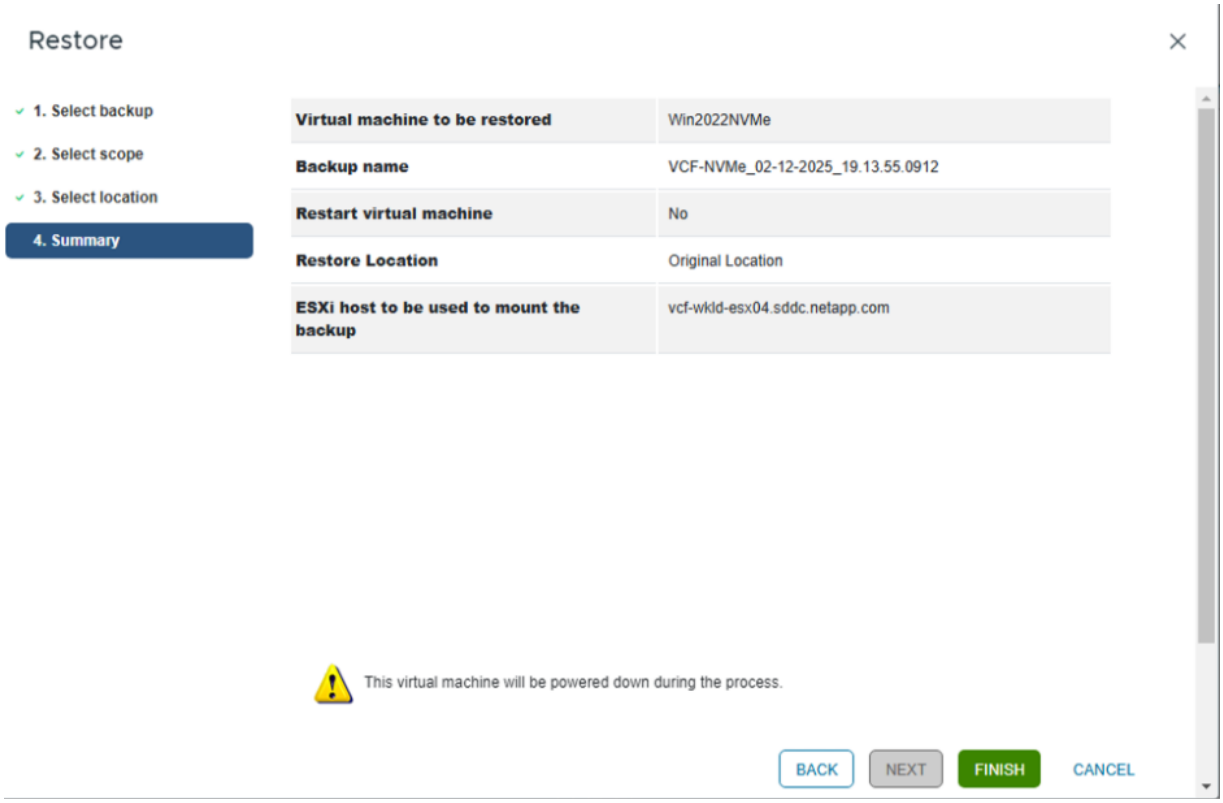
IL"ONTAP tools for VMware vSphere" (OTV) fornisce una soluzione potente ed efficiente per la gestione dello storage NetApp negli ambienti VMware. Integrandosi direttamente con vCenter Server, OTV semplifica la gestione dello storage, migliora la protezione dei dati e ottimizza le prestazioni. Sebbene facoltativa, l'implementazione di OTV può migliorare significativamente le capacità di gestione e l'efficienza complessiva degli ambienti VMware.

- "Creare uno storage NVMe/TCP per i domini di carico di lavoro VCF"
- "Configurare NetApp SnapCenter per VMware vSphere (SCV)"

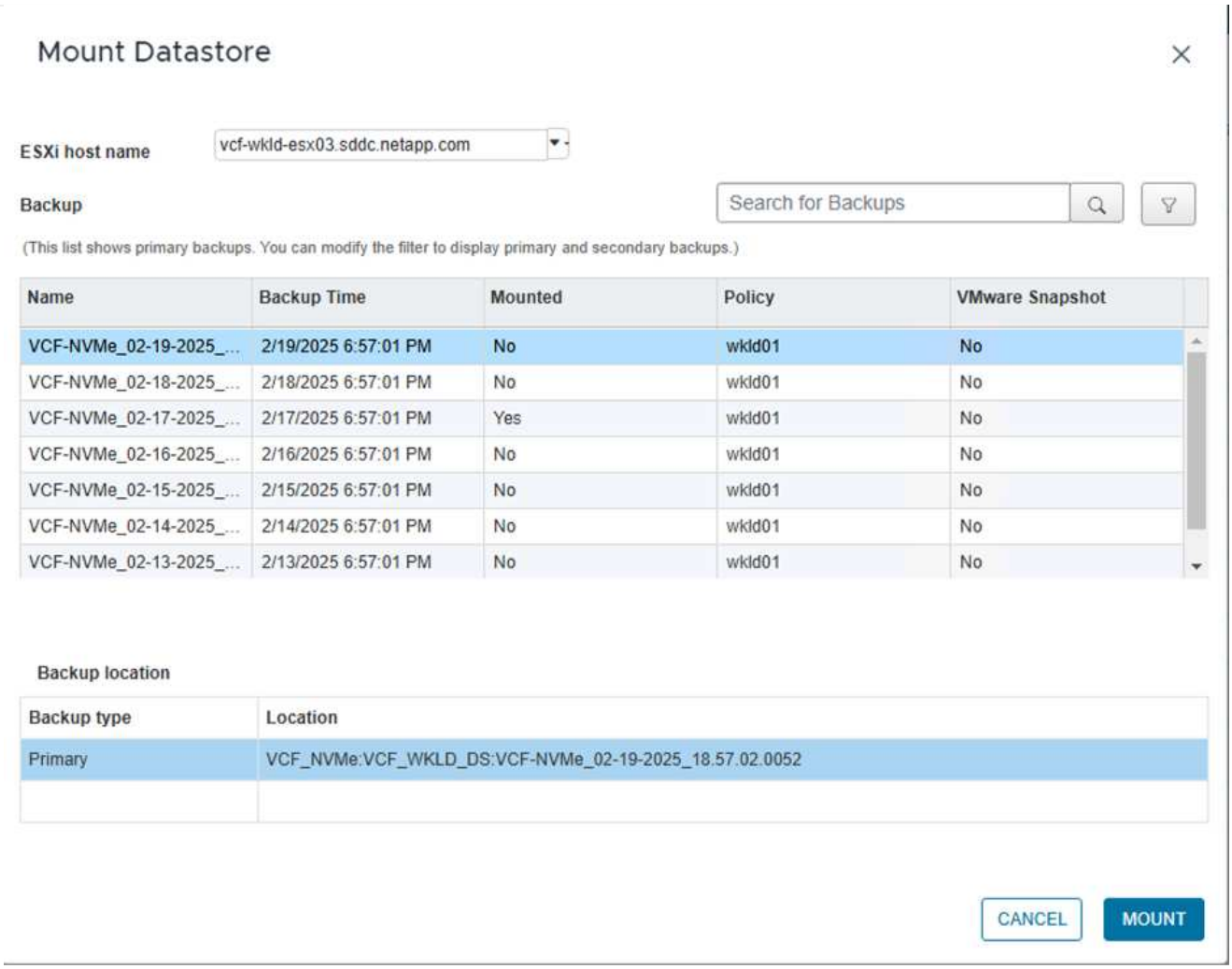
Ripristina VM, datastore, disco virtuale e file o cartelle

SCV offre funzionalità complete di backup e ripristino per gli ambienti VMware. Per gli ambienti VMFS, SCV utilizza operazioni di clonazione e montaggio insieme a Storage VMotion per eseguire operazioni di ripristino. Ciò garantisce un ripristino efficiente e senza interruzioni dei dati. Per maggiori dettagli controlla"come vengono eseguite le operazioni di ripristino."

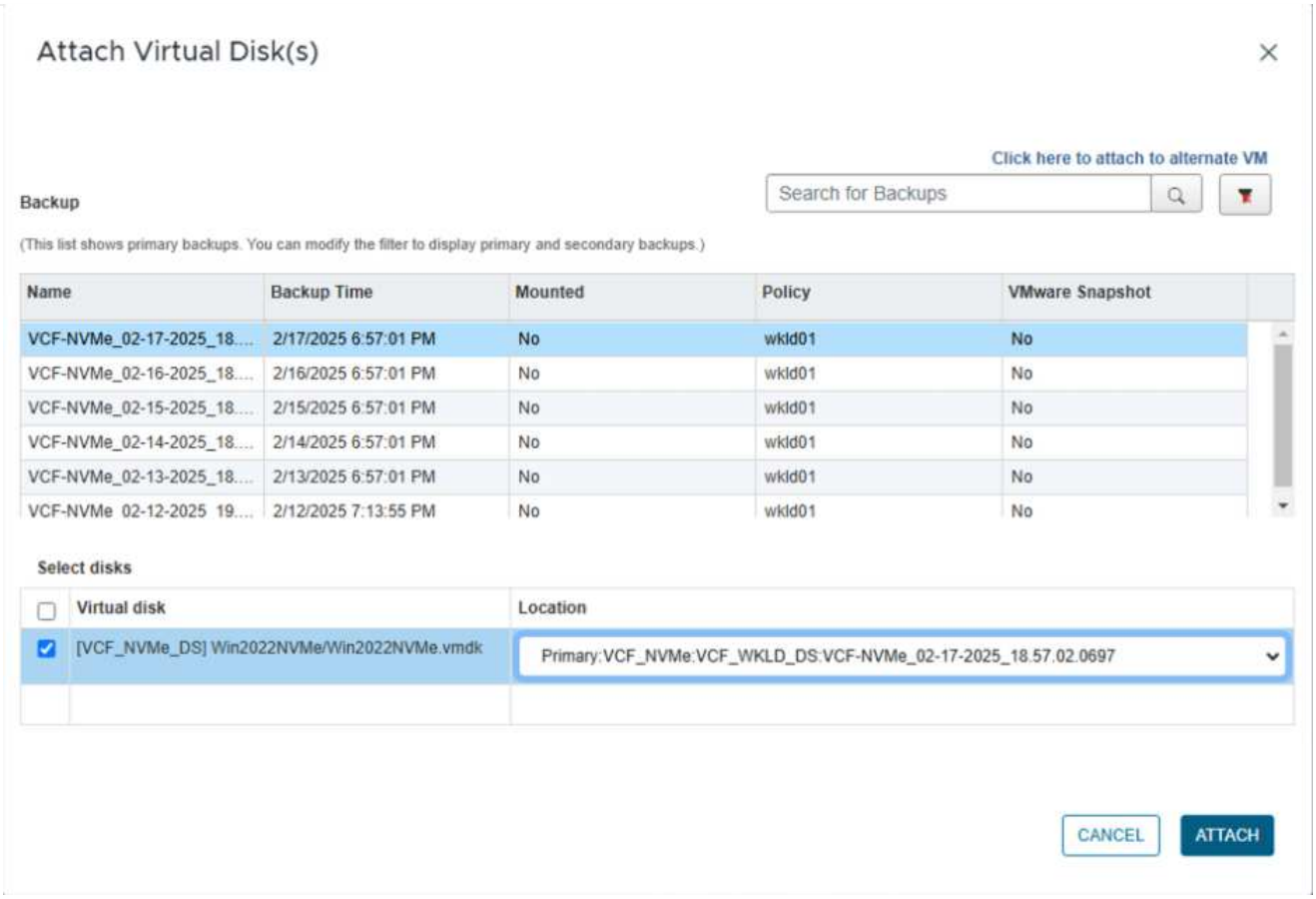
- Ripristino della VM È possibile ripristinare la VM sul suo host originale all'interno dello stesso vCenter Server o su un host ESXi alternativo gestito dallo stesso vCenter Server.
  a. Fare clic con il pulsante destro del mouse su una VM e selezionare SnapCenter Plug-in for VMware vSphere nell'elenco a discesa, quindi selezionare Ripristina nell'elenco a discesa secondario per avviare la procedura guidata.
  b. Nella procedura guidata di ripristino, seleziona lo snapshot di backup che desideri ripristinare e seleziona Intera macchina virtuale nel campo Ambito di ripristino, seleziona la posizione di ripristino e quindi immetti le informazioni sulla destinazione in cui montare il backup. Nella pagina Seleziona posizione, seleziona la posizione per il datastore ripristinato. Rivedi la pagina Riepilogo e fai clic su
  Fine.



- Montare un datastore È possibile montare un datastore tradizionale da un backup se si desidera accedere ai file nel backup. È possibile montare il backup sullo stesso host ESXi in cui è stato creato oppure su un host ESXi alternativo che abbia lo stesso tipo di configurazione host e VM. È possibile montare un datastore più volte su un host.
  a. Fare clic con il pulsante destro del mouse su un datastore e selezionare SnapCenter Plug-in for VMware vSphere > Monta backup.
  b. Nella pagina Monta datastore, seleziona un backup e una posizione di backup (primaria o secondaria), quindi fai clic su Monta.

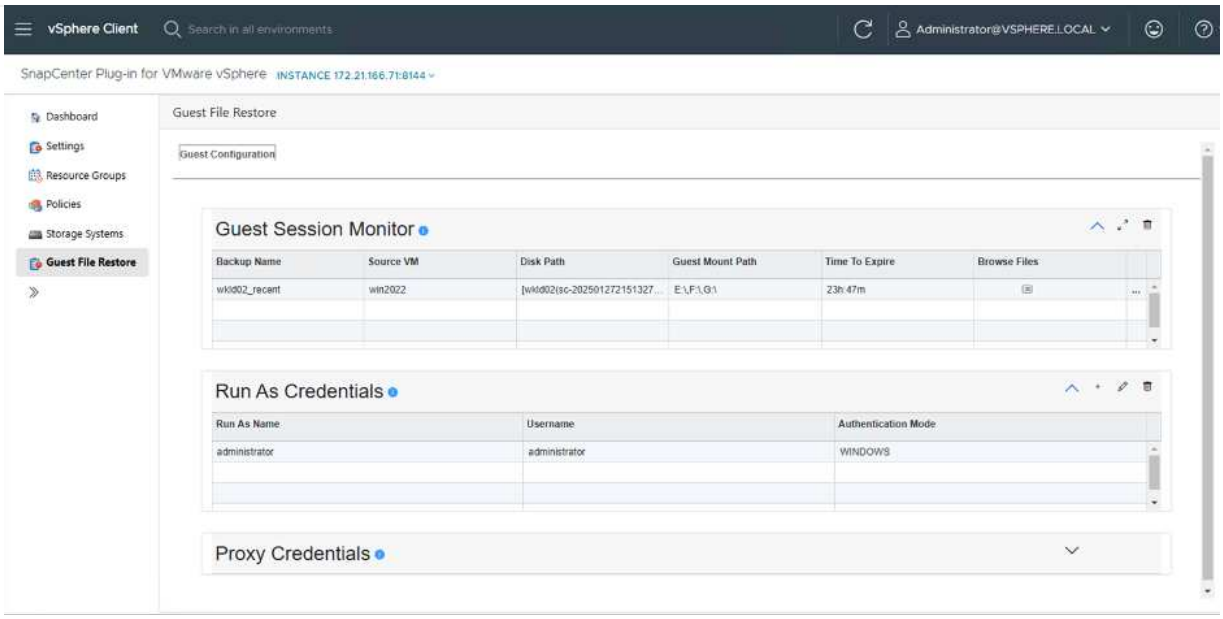


- Collegare un disco virtuale È possibile collegare uno o più VMDK da un backup alla VM padre, a una VM alternativa sullo stesso host ESXi o a una VM alternativa su un host ESXi alternativo gestito dallo stesso vCenter o da un vCenter diverso in modalità collegata.
  a. Fare clic con il pulsante destro del mouse su una VM, selezionare SnapCenter Plug-in for VMware vSphere > Collega disco/i virtuale/i.
  b. Nella finestra Collega disco virtuale, seleziona un backup, quindi seleziona uno o più dischi che desideri collegare e la posizione da cui desideri effettuare il collegamento (primario o secondario). Per impostazione predefinita, i dischi virtuali selezionati vengono collegati alla VM padre. Per collegare i dischi virtuali selezionati a una VM alternativa nello stesso host ESXi, selezionare Fai clic qui per collegare alla VM alternativa e specificare la VM alternativa. Fare clic su Allega.

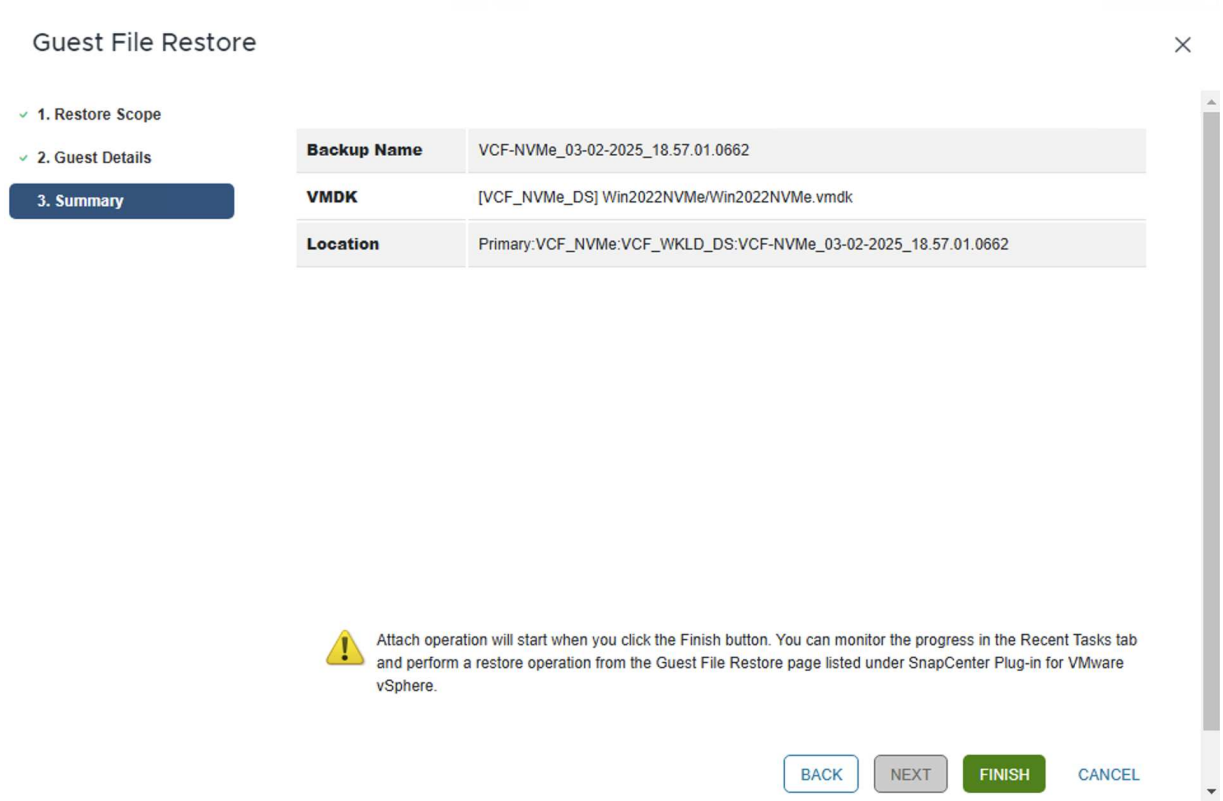


- Fasi di ripristino di file e cartelle È possibile ripristinare singoli file e cartelle in una sessione di ripristino file guest, che allega una copia di backup di un disco virtuale e quindi ripristina i file o le cartelle selezionati. È possibile ripristinare anche file e cartelle. Maggiori dettagli controllano"Ripristino di file e cartelle SnapCenter ."

  a. Quando si collega un disco virtuale per operazioni di ripristino di file o cartelle guest, la macchina virtuale di destinazione per il collegamento deve disporre di credenziali configurate prima del ripristino. Dal SnapCenter Plug-in for VMware vSphere , nella sezione plug-in, selezionare Ripristino file guest ed Esegui come credenziali, quindi immettere le credenziali utente. Per Nome utente, devi inserire "Amministratore".

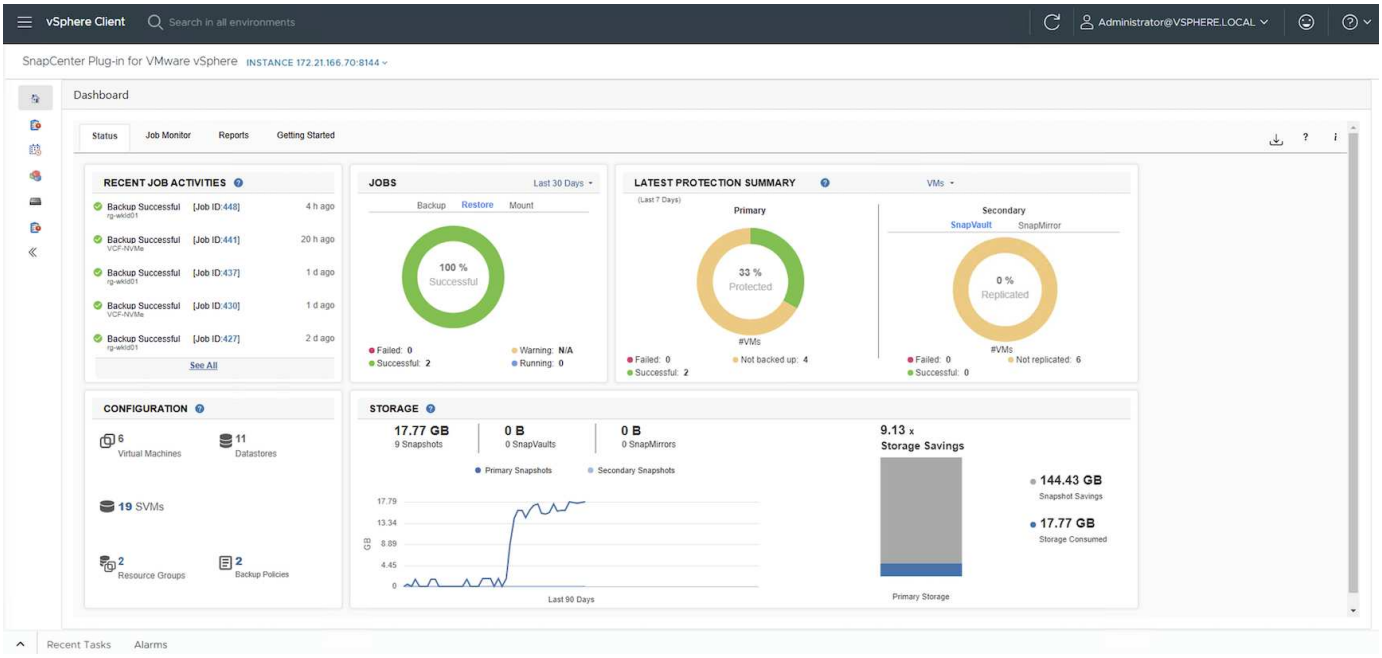


b. Fare clic con il pulsante destro del mouse sulla VM dal client vSphere e selezionare SnapCenter Plug-in for VMware vSphere > Ripristino file guest. Nella pagina Ambito di ripristino, specificare Nome backup, disco virtuale VMDK e Posizione: primaria o secondaria. Fare clic su Riepilogo per confermare.



Monitorare e segnalare

SCV offre solide funzionalità di monitoraggio e reporting per aiutare gli amministratori a gestire in modo efficiente le operazioni di backup e ripristino. È possibile visualizzare le informazioni sullo stato, monitorare i lavori, scaricare i registri dei lavori, accedere ai report, per maggiori dettagli controllare"Plug-in SnapCenter per VMware vSphere Monitor e Report."



Sfruttando la potenza di NVMe su TCP e SnapCenter Plug-in for VMware vSphere-in NetApp SnapCenter per VMware vSphere, le organizzazioni possono ottenere una protezione dei dati ad alte prestazioni e un disaster recovery per i domini di carico di lavoro di VMware Cloud Foundation. Questo approccio garantisce operazioni di backup e ripristino rapide e affidabili, riducendo al minimo i tempi di inattività e salvaguardando i dati critici.

Proteggi i datastore VMware con BlueXP

Scopri come proteggere i datastore VMware utilizzando il BlueXP disaster recovery

Scopri di più sulle soluzioni NetApp per il disaster recovery utilizzando BlueXP disaster recovery per VMware. Ciò fornisce soluzioni robuste per il disaster recovery mediante replica a livello di blocco da un sito primario a un sito di disaster recovery.

BlueXP DRaaS è un metodo efficace ed economico per proteggere i carichi di lavoro da guasti del sito e problemi di integrità dei dati, compresi gli attacchi ransomware. Inoltre, NetApp BlueXP DRaaS potenzia questa strategia fornendo una soluzione di disaster recovery gestita e basata sul cloud, che garantisce un ripristino rapido e tempi di inattività minimi durante i disastri.

Per i dettagli tecnici fare riferimento alle seguenti soluzioni.

- "DR tramite BlueXP DRaaS per datastore VMFS"
- "DR tramite BlueXP DRaaS per datastore NFS"

Configura la protezione dei dati 3-2-1 per VMware con il plug-in SnapCenter per il BlueXP backup and recovery

Configurare una strategia di protezione dei dati 3-2-1 per gli ambienti VMware utilizzando il plug-in SnapCenter per il BlueXP backup and recovery. Questa procedura include la configurazione di backup di VM e datastore su cluster ONTAP primari e secondari, la configurazione del plug-in e BlueXP e la gestione della replica dei dati su cloud o storage esterno per un ripristino affidabile.

La strategia di backup 3-2-1 è un metodo di protezione dei dati accettato dal settore, che fornisce un approccio completo alla salvaguardia dei dati preziosi. Questa strategia è affidabile e garantisce che, anche se si verificasse un disastro imprevisto, ci sarà comunque una copia dei dati disponibile.

Panoramica

La strategia si compone di tre regole fondamentali:

1. Conserva almeno tre copie dei tuoi dati. In questo modo si garantisce che, anche se una copia viene persa o danneggiata, saranno comunque disponibili almeno due copie su cui fare affidamento.
2. Conservare due copie di backup su supporti o dispositivi di archiviazione diversi. Diversificare i supporti di memorizzazione aiuta a proteggere da guasti specifici del dispositivo o del supporto. Se un dispositivo viene danneggiato o un tipo di supporto si guasta, l'altra copia di backup non subisce alcun danno.
3. Infine, assicurati che almeno una copia di backup sia fuori sede. L'archiviazione fuori sede funge da misura di sicurezza contro disastri localizzati, come incendi o inondazioni, che potrebbero rendere inutilizzabili le copie in loco.

Questo documento sulla soluzione riguarda una soluzione di backup 3-2-1 che utilizza il SnapCenter Plug-in for VMware vSphere (SCV) per creare backup primari e secondari delle nostre macchine virtuali on-premise e il BlueXP backup and recovery per le macchine virtuali per eseguire il backup di una copia dei nostri dati su un archivio cloud o StorageGRID.

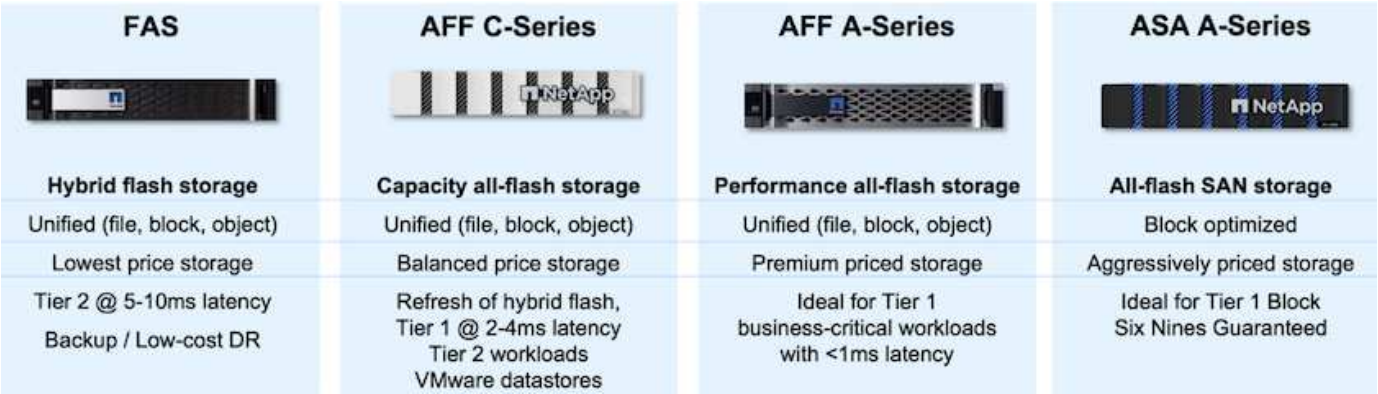
Casi d'uso

Questa soluzione affronta i seguenti casi d'uso:

- Backup e ripristino di macchine virtuali e datastore on-premise mediante il SnapCenter Plug-in for VMware vSphere.
- Backup e ripristino di macchine virtuali e datastore on-premise, ospitati su cluster ONTAP e sottoposti a backup su storage di oggetti tramite il BlueXP backup and recovery per macchine virtuali.

Archiviazione dati NetApp ONTAP

ONTAP è la soluzione di storage leader del settore di NetApp che offre storage unificato indipendentemente dall'accesso tramite protocolli SAN o NAS. La strategia di backup 3-2-1 garantisce la protezione dei dati in sede su più tipi di supporto e NetApp offre piattaforme che spaziano da flash ad alta velocità a supporti più economici.



Per maggiori informazioni su tutte le piattaforme hardware di NetApp, consulta "Archiviazione dati NetApp" .

SnapCenter Plug-in for VMware vSphere

Il plug-in SnapCenter per VMware vSphere è un'offerta di protezione dei dati strettamente integrata con VMware vSphere e consente una facile gestione del backup e del ripristino per le macchine virtuali. Come parte di questa soluzione, SnapMirror fornisce un metodo rapido e affidabile per creare una seconda copia di backup immutabile dei dati della macchina virtuale su un cluster di archiviazione ONTAP secondario. Grazie a questa architettura, le operazioni di ripristino delle macchine virtuali possono essere avviate facilmente dalle posizioni di backup primarie o secondarie.

SCV viene distribuito come appliance virtuale Linux utilizzando un file OVA. Il plug-in ora utilizza un'architettura di plug-in remoto. Il plug-in remoto viene eseguito all'esterno del server vCenter ed è ospitato sull'appliance virtuale SCV.

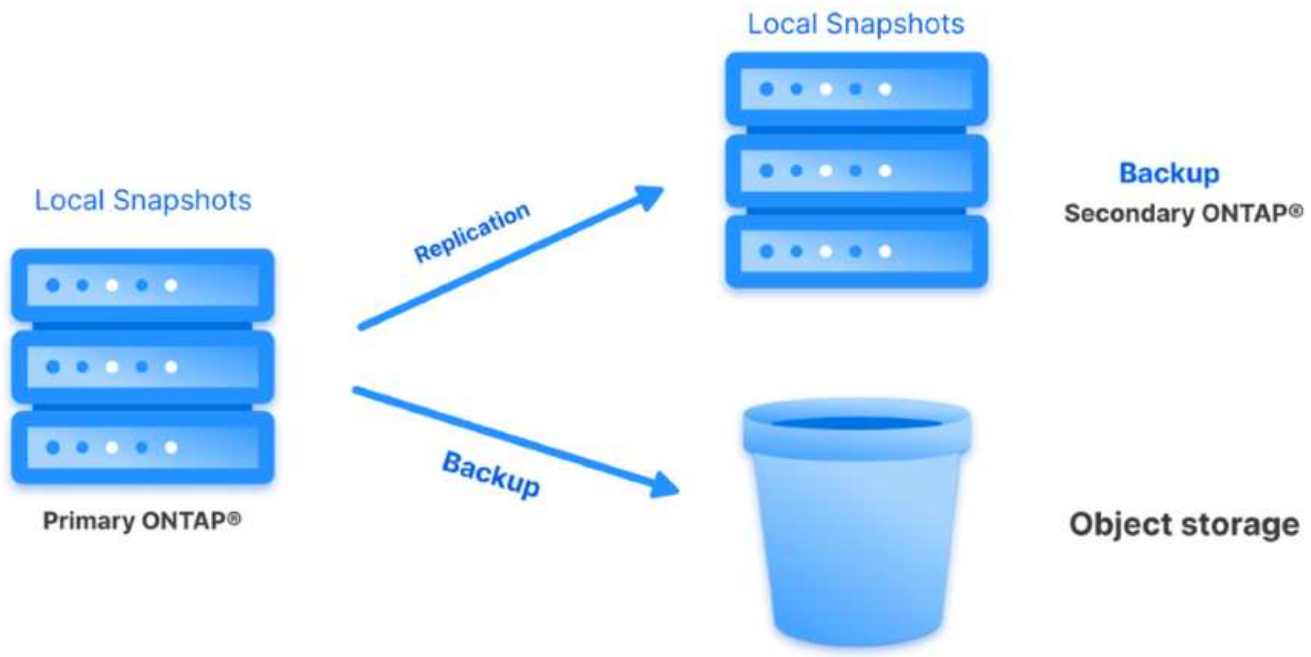
Per informazioni dettagliate su SCV fare riferimento a "Documentazione SnapCenter Plug-in for VMware vSphere" .

BlueXP backup and recovery per macchine virtuali

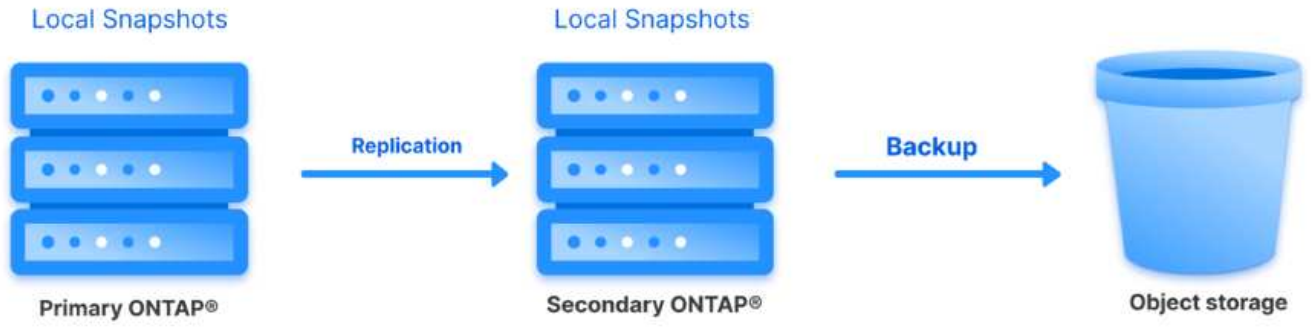
BlueXP backup and recovery è uno strumento basato su cloud per la gestione dei dati che fornisce un unico piano di controllo per un'ampia gamma di operazioni di backup e ripristino sia in ambienti locali che cloud. Una parte della suite BlueXP backup and recovery NetApp BlueXP è una funzionalità che si integra con il plug-in SnapCenter per VMware vSphere (on-premises) per estendere una copia dei dati all'archiviazione degli oggetti nel cloud. In questo modo viene creata una terza copia dei dati fuori sede, ricavata dai backup di archiviazione primari o secondari. Il BlueXP backup and recovery semplificano la configurazione di policy di archiviazione che trasferiscono copie dei dati da una di queste due posizioni locali.

La scelta tra backup primario e secondario come origine in BlueXP Backup and Recovery comporterà l'implementazione di una delle due topologie:

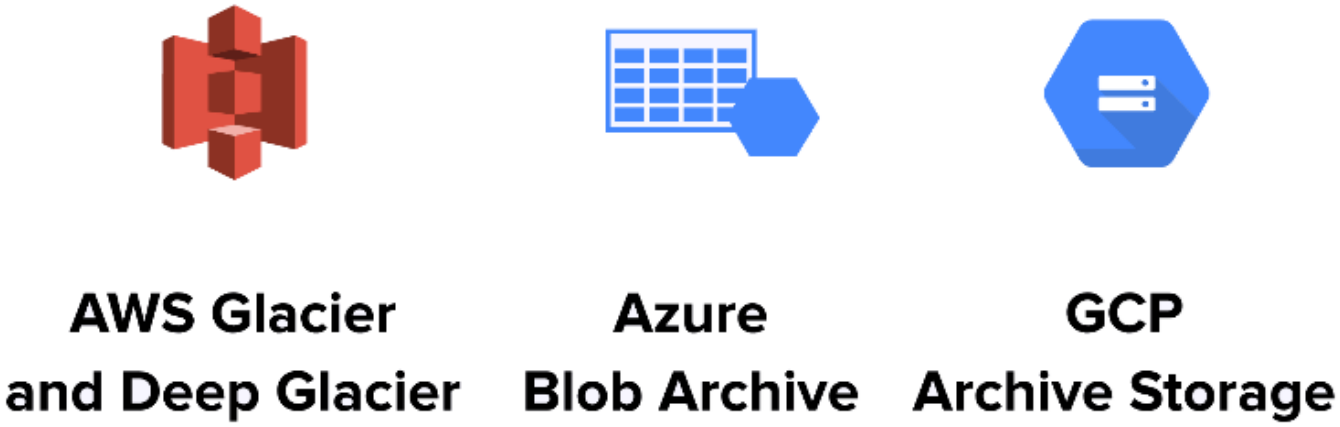
Topologia fan-out: quando un backup viene avviato dal SnapCenter Plug-in for VMware vSphere, viene immediatamente creato uno snapshot locale. SCV avvia quindi un'operazione SnapMirror che replica lo snapshot più recente sul cluster ONTAP secondario. In BlueXP Backup and Recovery, una policy specifica il cluster ONTAP primario come origine per una copia snapshot dei dati da trasferire all'archiviazione degli oggetti nel provider cloud scelto.



Topologia a cascata – La creazione delle copie dei dati primari e secondari tramite SCV è identica alla topologia fan-out menzionata sopra. Tuttavia, questa volta viene creata una policy in BlueXP Backup and Recovery che specifica che il backup nell'archivio oggetti avrà origine dal cluster ONTAP secondario.



Il BlueXP backup and recovery possono creare copie di backup di snapshot ONTAP locali su AWS Glacier, Azure Blob e GCP Archive.



Inoltre, è possibile utilizzare NetApp StorageGRID come destinazione di backup dell'archiviazione degli oggetti. Per maggiori informazioni su StorageGRID fare riferimento a "Pagina di destinazione StorageGRID" .

Panoramica sulla distribuzione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare questa soluzione ed eseguire operazioni di backup e ripristino da SCV e BlueXP backup and recovery:

1. Configurare la relazione SnapMirror tra i cluster ONTAP da utilizzare per le copie dei dati primari e secondari.
2. Configurare il plug-in SnapCenter per VMware vSphere.
   a. Aggiungi sistemi di archiviazione
   b. Creare policy di backup
   c. Creare gruppi di risorse
   d. Eseguire il backup prima dei processi di backup
3. Configurare il BlueXP backup and recovery per le macchine virtuali
   a. Aggiungi ambiente di lavoro
   b. Scopri gli apparecchi SCV e vCenter
   c. Creare policy di backup
   d. Attiva i backup
4. Ripristinare le macchine virtuali dallo storage primario e secondario utilizzando SCV.
5. Ripristina le macchine virtuali dall'archiviazione di oggetti utilizzando il backup e il ripristino BlueXP .

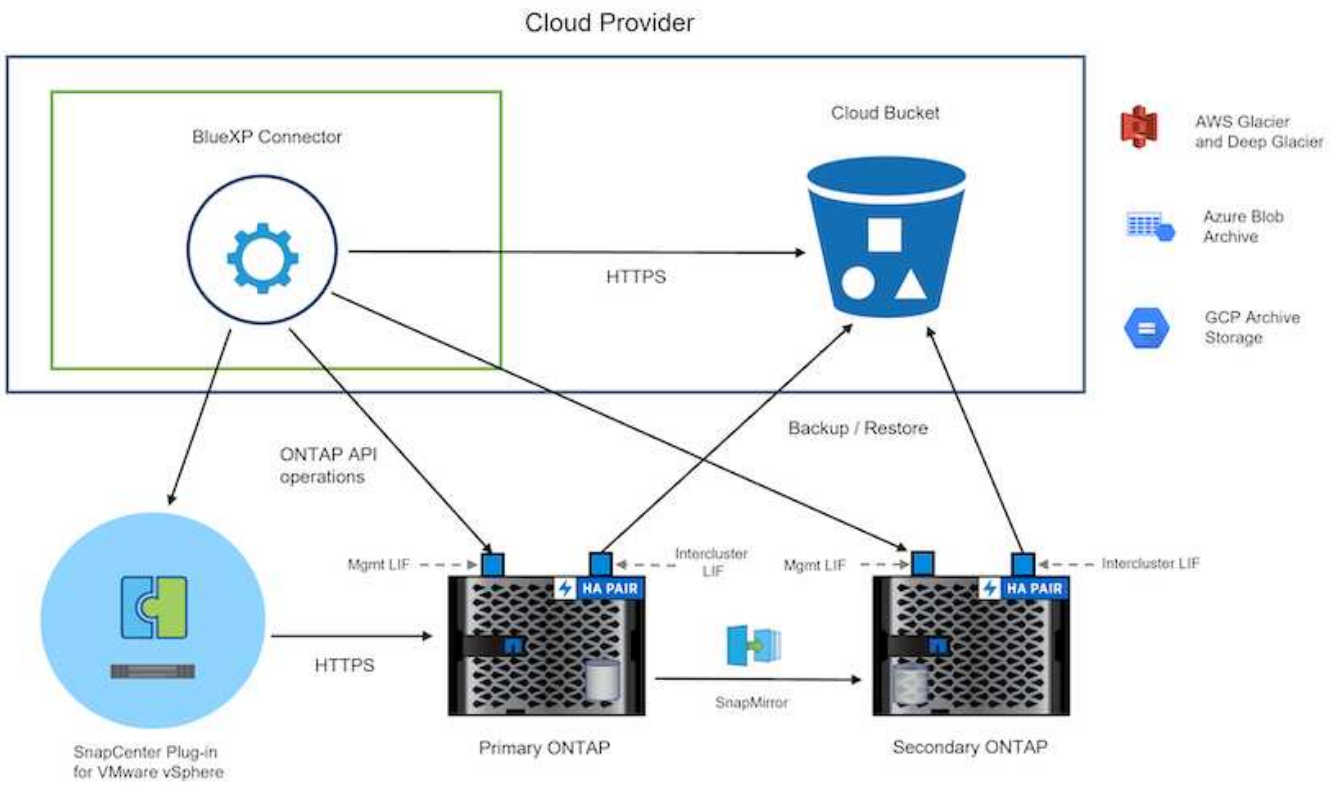
Prerequisiti

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware vSphere, nei domini di carico di lavoro VCF VI o nei domini di gestione VCF. Le macchine virtuali in questa soluzione sono ospitate su datastore NFS forniti da NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano configurati e pronti per l'uso:

1. Cluster di archiviazione ONTAP con datastore NFS o VMFS connessi a VMware vSphere. Sono supportati sia i datastore NFS che VMFS. Per questa soluzione sono stati utilizzati datastore NFS.
2. Cluster di archiviazione ONTAP secondario con relazioni SnapMirror stabilite per i volumi utilizzati per gli archivi dati NFS.
3. Connettore BlueXP installato per il provider cloud utilizzato per i backup di archiviazione di oggetti.
4. Le macchine virtuali da sottoporre a backup si trovano su datastore NFS residenti nel cluster di storage ONTAP primario.
5. Connettività di rete tra il connettore BlueXP e le interfacce di gestione del cluster di storage ONTAP in sede.
6. Connettività di rete tra il connettore BlueXP e la VM dell'appliance SCV locale e tra il connettore BlueXP e vCenter.
7. Connettività di rete tra i LIF intercluster ONTAP locali e il servizio di archiviazione degli oggetti.
8. DNS configurato per la gestione SVM sui cluster di storage ONTAP primari e secondari. Per maggiori informazioni fare riferimento a "Configurare il DNS per la risoluzione dei nomi host" .

Architettura di alto livello

Il test/la convalida di questa soluzione sono stati eseguiti in un laboratorio che potrebbe corrispondere o meno all'ambiente di distribuzione finale.



Distribuzione della soluzione

In questa soluzione forniamo istruzioni dettagliate per la distribuzione e la convalida di una soluzione che utilizza il SnapCenter Plug-in for VMware vSphere, insieme BlueXP backup and recovery, per eseguire il backup e il ripristino di macchine virtuali Windows e Linux all'interno di un cluster VMware vSphere situato in un data center locale. Le macchine virtuali in questa configurazione sono archiviate su datastore NFS ospitati da un cluster di storage ONTAP A300. Inoltre, un cluster di archiviazione ONTAP A300 separato funge da destinazione secondaria per i volumi replicati tramite SnapMirror. Inoltre, come destinazione per una terza copia dei dati sono stati utilizzati gli archivi di oggetti ospitati su Amazon Web Services e Azure Blob.

Esamineremo la creazione di relazioni SnapMirror per copie secondarie dei nostri backup gestiti da SCV e la configurazione dei processi di backup sia nel BlueXP backup and recovery.

Per informazioni dettagliate sul SnapCenter Plug-in for VMware vSphere, fare riferimento a "Documentazione SnapCenter Plug-in for VMware vSphere" .

Per informazioni dettagliate sul BlueXP backup and recovery fare riferimento a "Documentazione BlueXP backup and recovery" .

Stabilire relazioni SnapMirror tra cluster ONTAP

Il SnapCenter Plug-in for VMware vSphere utilizza la tecnologia ONTAP SnapMirror per gestire il trasporto di copie secondarie SnapMirror e/o SnapVault su un cluster ONTAP secondario.

I criteri di backup SCV hanno la possibilità di utilizzare relazioni SnapMirror o SnapVault . La differenza principale è che quando si utilizza l'opzione SnapMirror , la pianificazione di conservazione configurata per i backup nel criterio sarà la stessa nelle posizioni primaria e secondaria. SnapVault è progettato per l'archiviazione e quando si utilizza questa opzione è possibile stabilire una pianificazione di conservazione separata con la relazione SnapMirror per le copie snapshot sul cluster di archiviazione ONTAP secondario.

L’impostazione delle relazioni SnapMirror può essere effettuata in BlueXP, dove molti dei passaggi sono automatizzati, oppure può essere effettuata utilizzando System Manager e ONTAP CLI. Di seguito vengono illustrati tutti questi metodi.

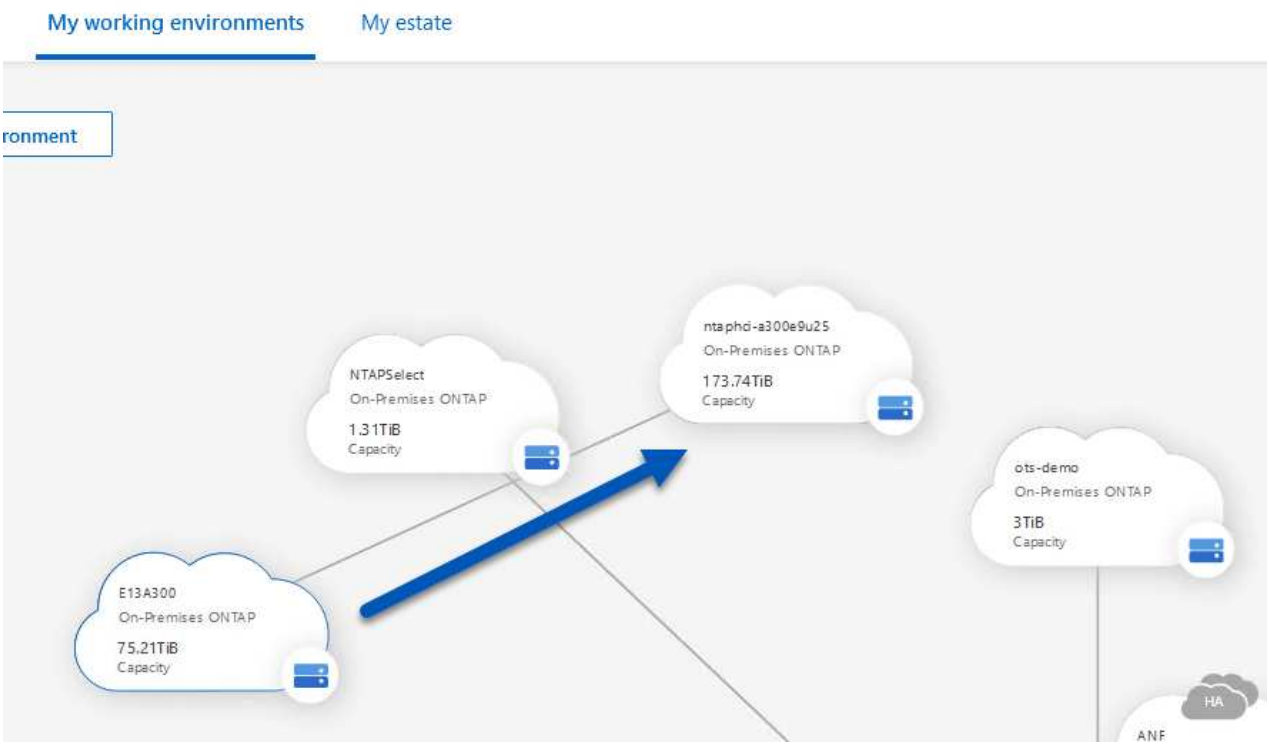
Stabilisci relazioni SnapMirror con BlueXP

I seguenti passaggi devono essere completati dalla console web BlueXP :

Configurazione della replica per sistemi di archiviazione ONTAP primari e secondari

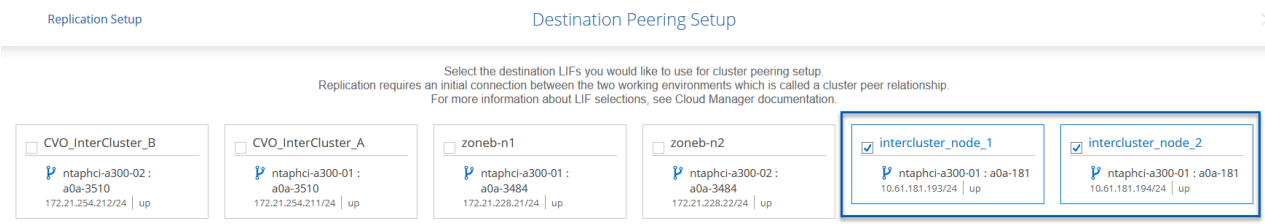
Per prima cosa accedi alla console web BlueXP e vai su Canvas.

1. Trascinare e rilasciare il sistema di archiviazione ONTAP di origine (primario) sul sistema di archiviazione ONTAP di destinazione (secondario).

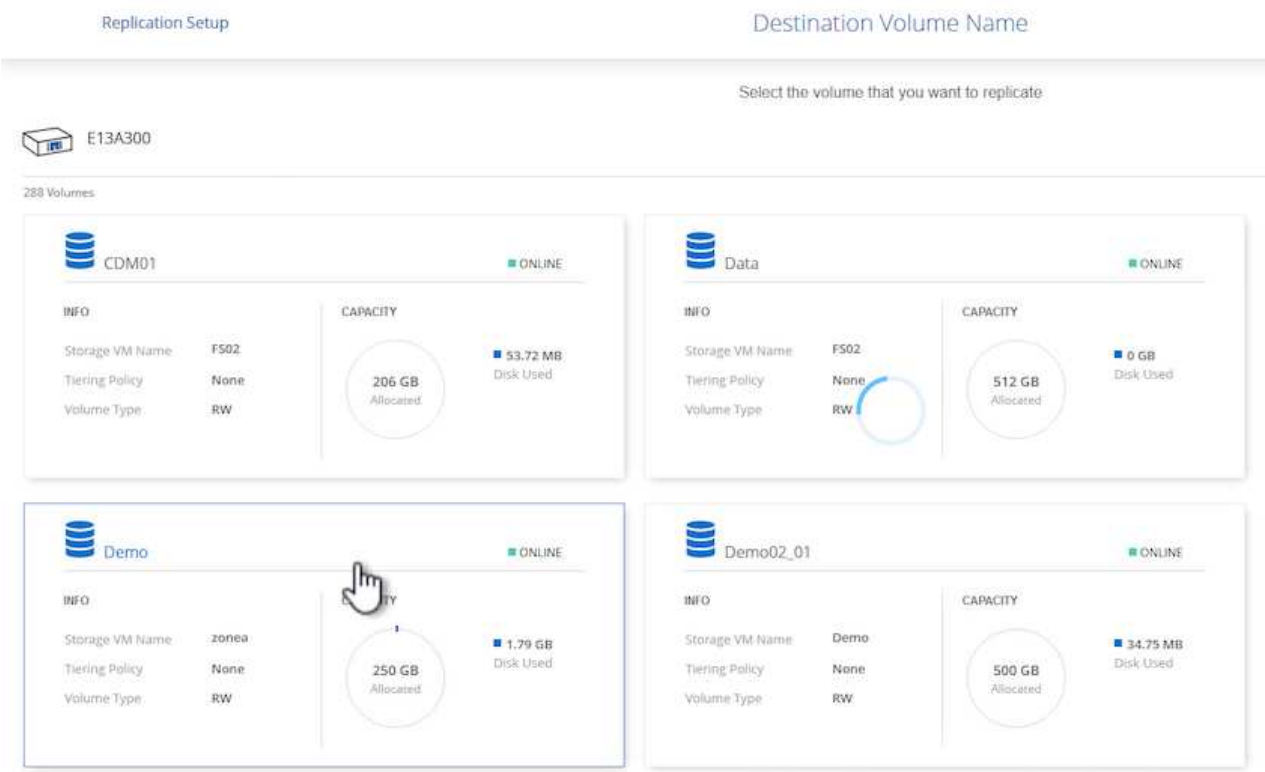


2. Dal menu che appare seleziona **Replicazione**.

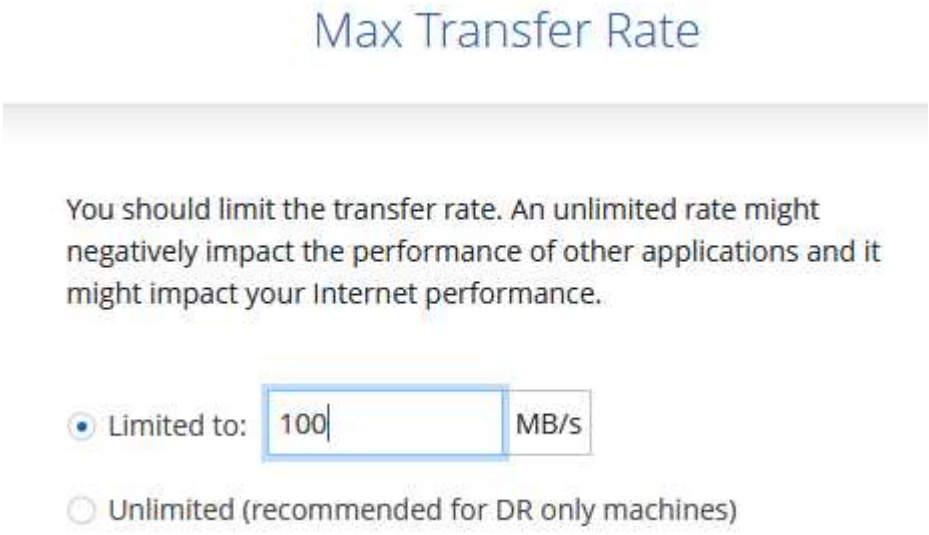
3. Nella pagina **Configurazione peering di destinazione** selezionare i LIF intercluster di destinazione da utilizzare per la connessione tra i sistemi di storage.



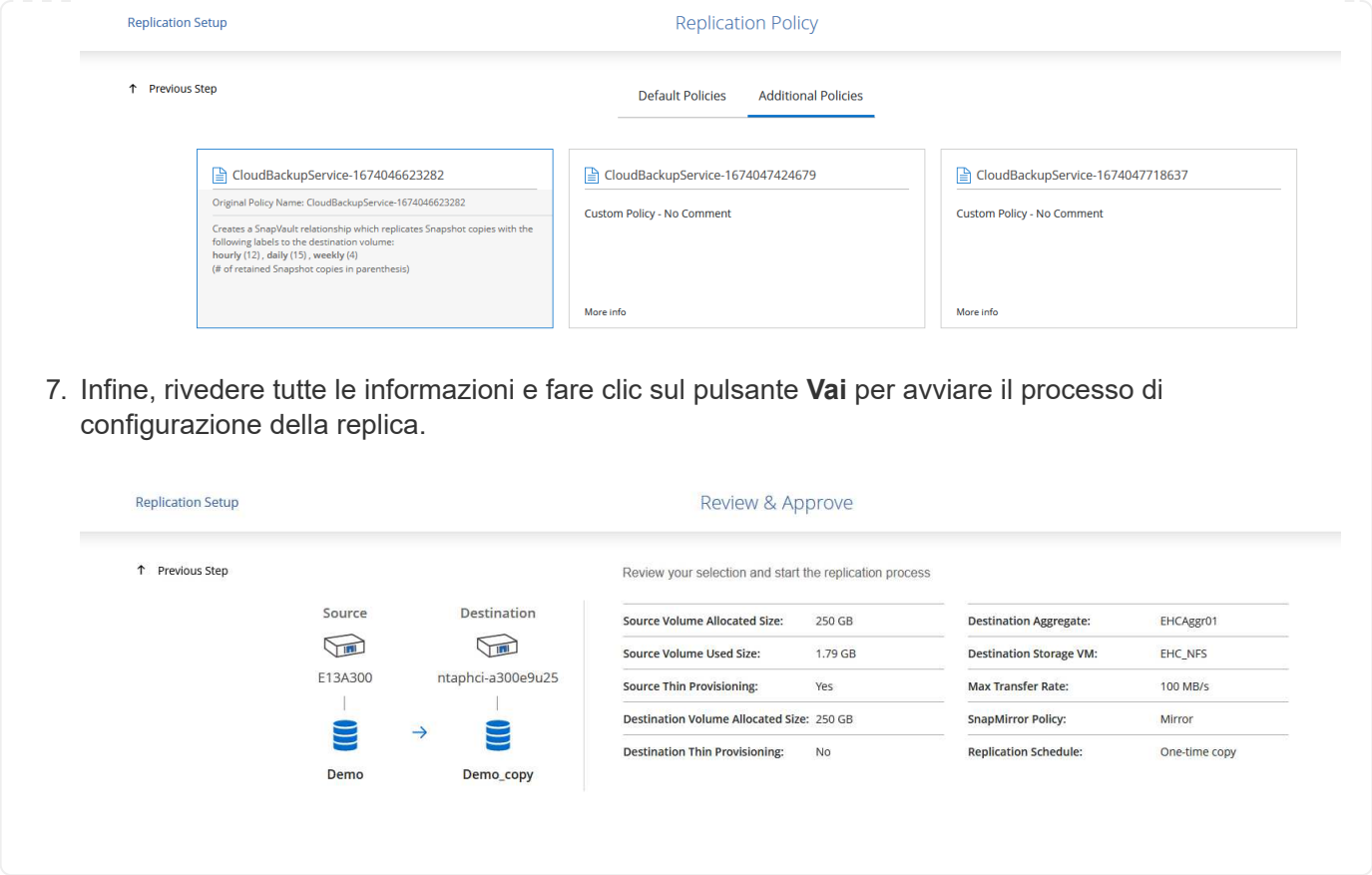
4. Nella pagina **Nome volume di destinazione**, seleziona prima il volume di origine, quindi compila il nome del volume di destinazione e seleziona l'SVM di destinazione e l'aggregato. Fare clic su **Avanti** per continuare.



5. Selezionare la velocità di trasferimento massima a cui deve avvenire la replica.



6. Selezionare il criterio che determinerà la pianificazione della conservazione per i backup secondari. Questa policy può essere creata in anticipo (vedere la procedura manuale riportata di seguito nel passaggio **Creare una policy di conservazione degli snapshot**) oppure può essere modificata in un secondo momento, se lo si desidera.



7. Infine, rivedere tutte le informazioni e fare clic sul pulsante **Vai** per avviare il processo di configurazione della replica.

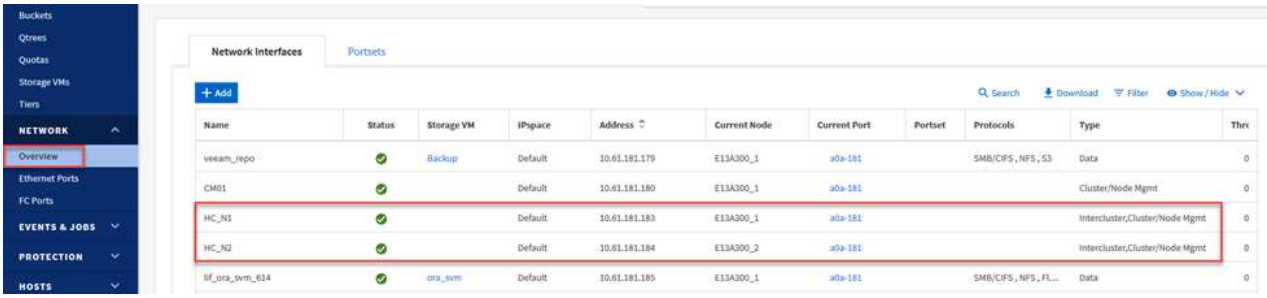
Stabilire relazioni SnapMirror con System Manager e ONTAP CLI

Tutti i passaggi necessari per stabilire relazioni SnapMirror possono essere eseguiti con System Manager o ONTAP CLI. La sezione seguente fornisce informazioni dettagliate per entrambi i metodi:

Registra le interfacce logiche Intercluster di origine e destinazione

Per i cluster ONTAP di origine e di destinazione, è possibile recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

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



2. Per recuperare gli indirizzi IP Intercluster tramite la CLI, eseguire il seguente comando:

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

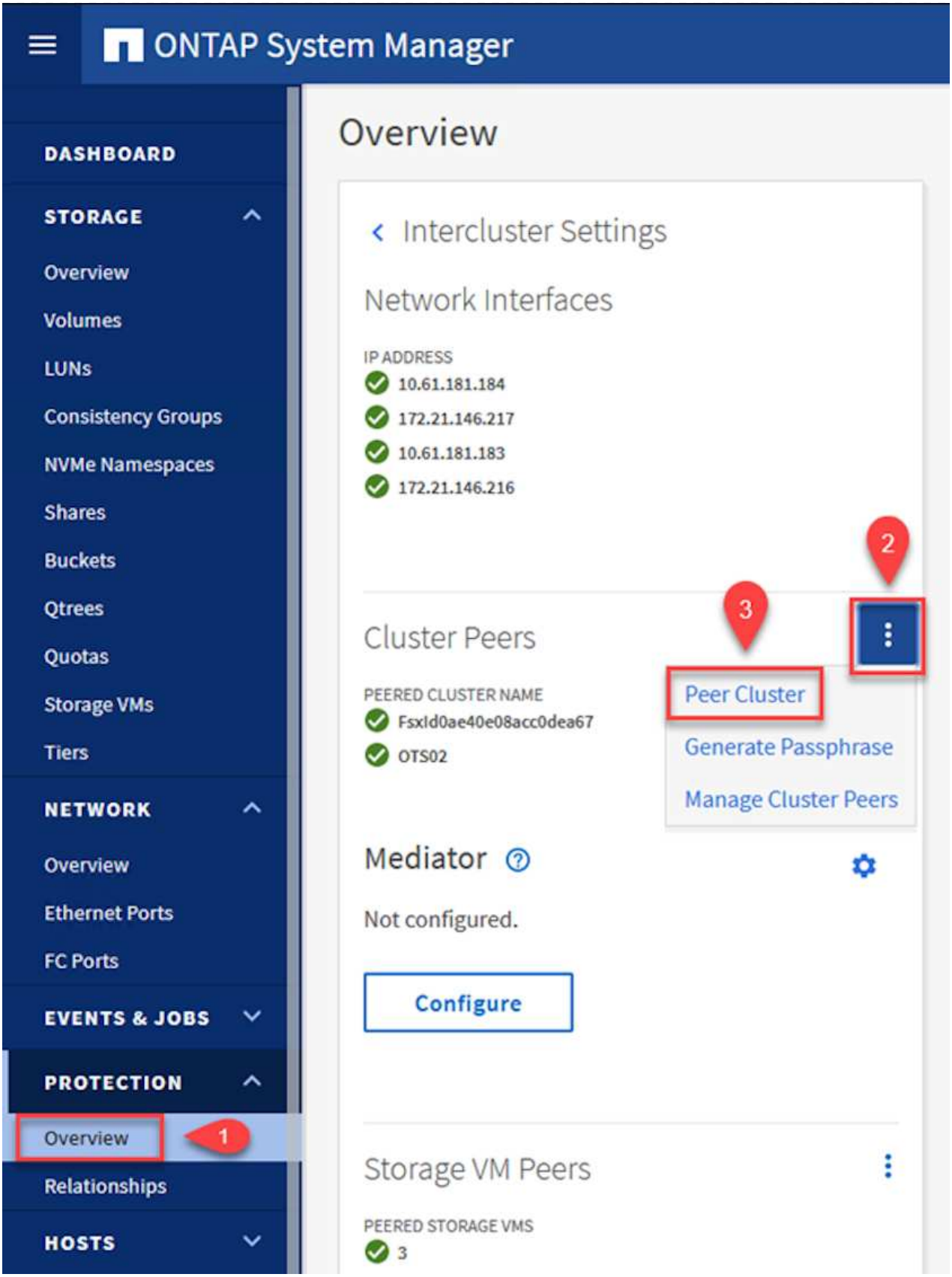
Stabilire il peering dei cluster tra i cluster ONTAP

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

1. Impostare il peering sul cluster ONTAP di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca che verrà utilizzata in seguito sul cluster di origine per finalizzare il processo di creazione.

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

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando ONTAP System Manager o la CLI. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Cluster.

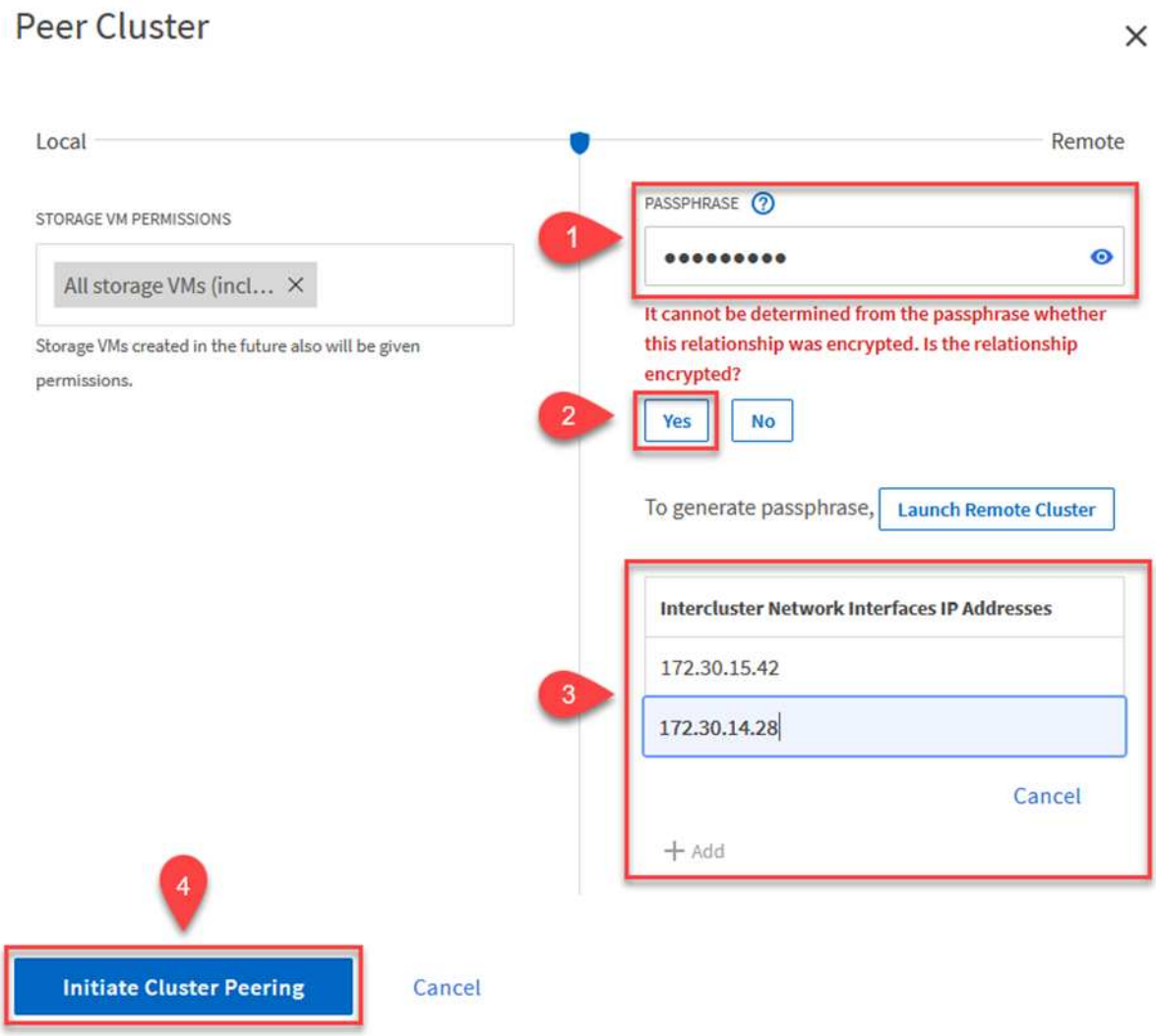


3. Nella finestra di dialogo Peer Cluster, compilare le informazioni richieste:
   a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer sul cluster ONTAP di destinazione.

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

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

d. Fare clic su Avvia peering cluster per finalizzare il processo.



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

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

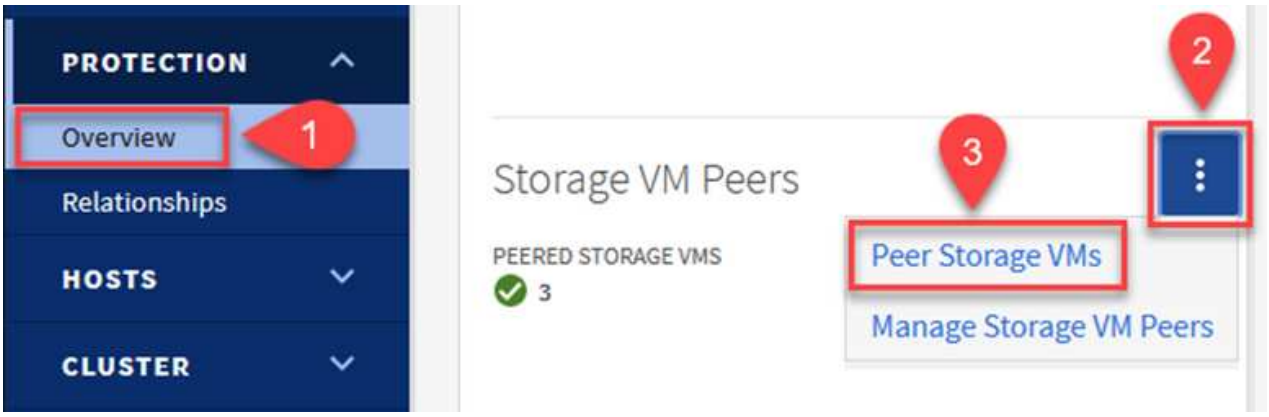
Stabilire una relazione di peering SVM

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

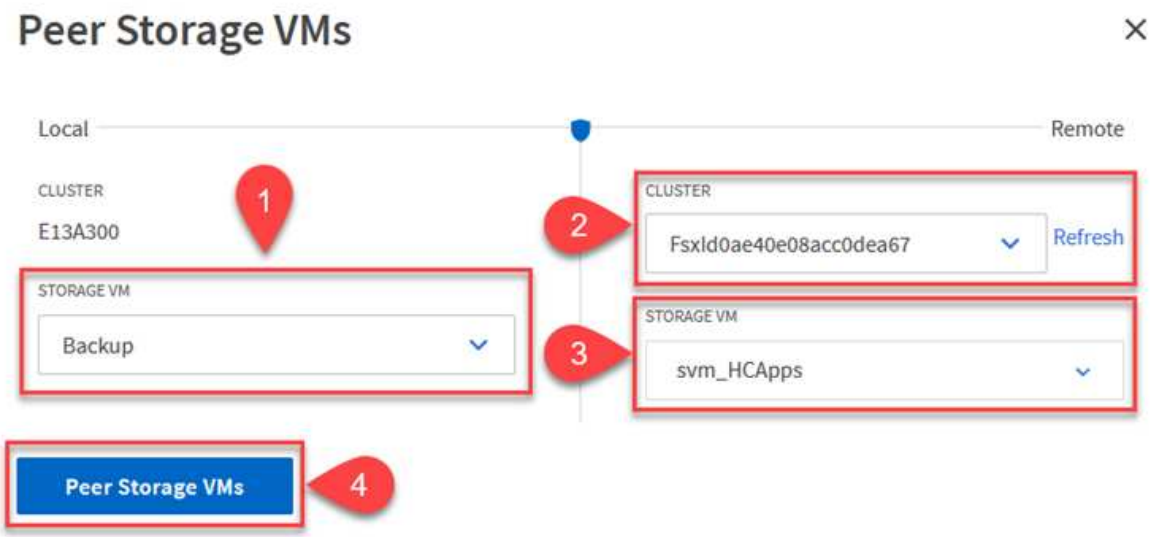
1. Dal cluster ONTAP di destinazione, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

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

2. Dal cluster ONTAP di origine, accettare la relazione di peering con ONTAP System Manager o con la CLI.
3. Da ONTAP System Manager, vai a Protezione > Panoramica e seleziona Peer Storage VM in Storage VM Peer.



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



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

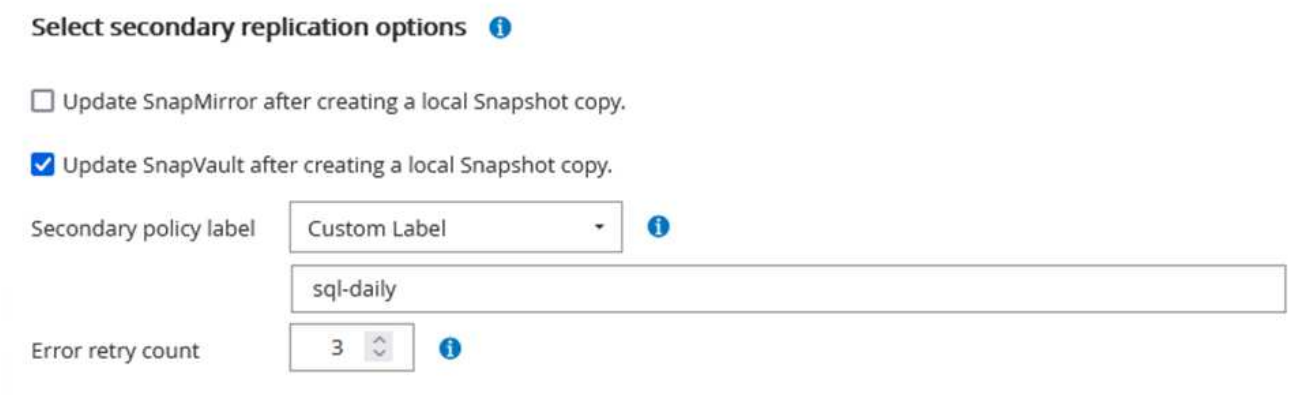
Creare un criterio di conservazione degli snapshot

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

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

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

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



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

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

1. Creare la policy SnapMirror sul cluster FSx.

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

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

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

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

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

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

Crea volumi di destinazione

Per creare un volume di destinazione su ONTAP che sarà il destinatario delle copie snapshot dai nostri volumi di origine, eseguire il seguente comando sul cluster ONTAP di destinazione:

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

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

Per creare una relazione SnapMirror tra un volume di origine e uno di destinazione, eseguire il seguente comando sul cluster ONTAP di destinazione:

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

Inizializza le relazioni SnapMirror

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

Per creare un volume, eseguire il seguente comando sul cluster ONTAP di destinazione:

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

Configurare il SnapCenter Plug-in for VMware vSphere

Una volta installato, è possibile accedere al SnapCenter Plug-in for VMware vSphere dall'interfaccia di gestione di vCenter Server Appliance. SCV gestirà i backup per i datastore NFS montati sugli host ESXi e che contengono le VM Windows e Linux.

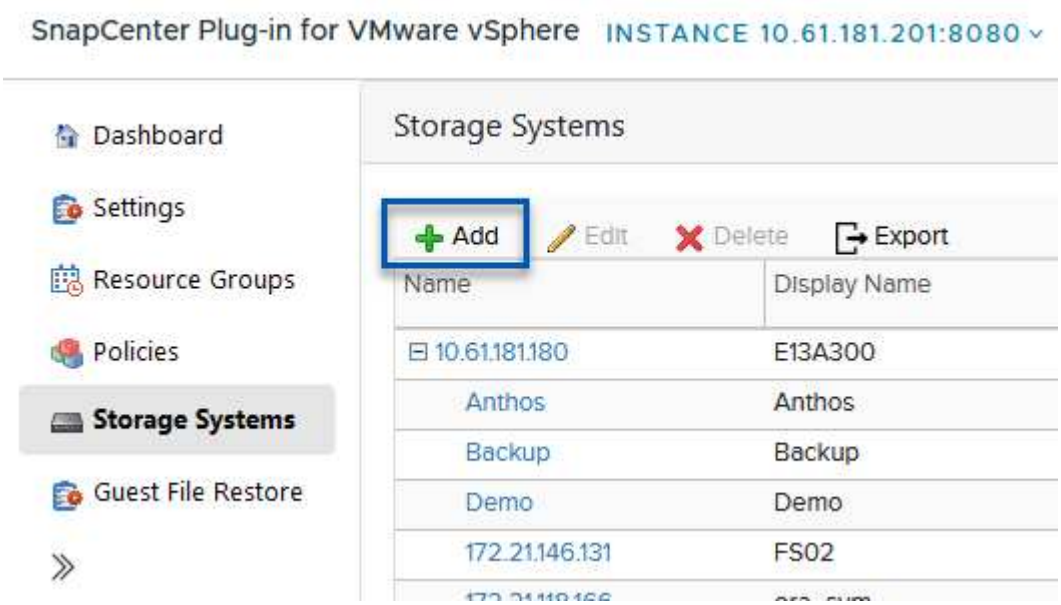
Rivedere il "Flusso di lavoro sulla protezione dei dati" sezione della documentazione SCV per maggiori informazioni sui passaggi necessari per configurare i backup.

Per configurare i backup delle macchine virtuali e degli archivi dati, è necessario completare i seguenti passaggi dall’interfaccia del plug-in.

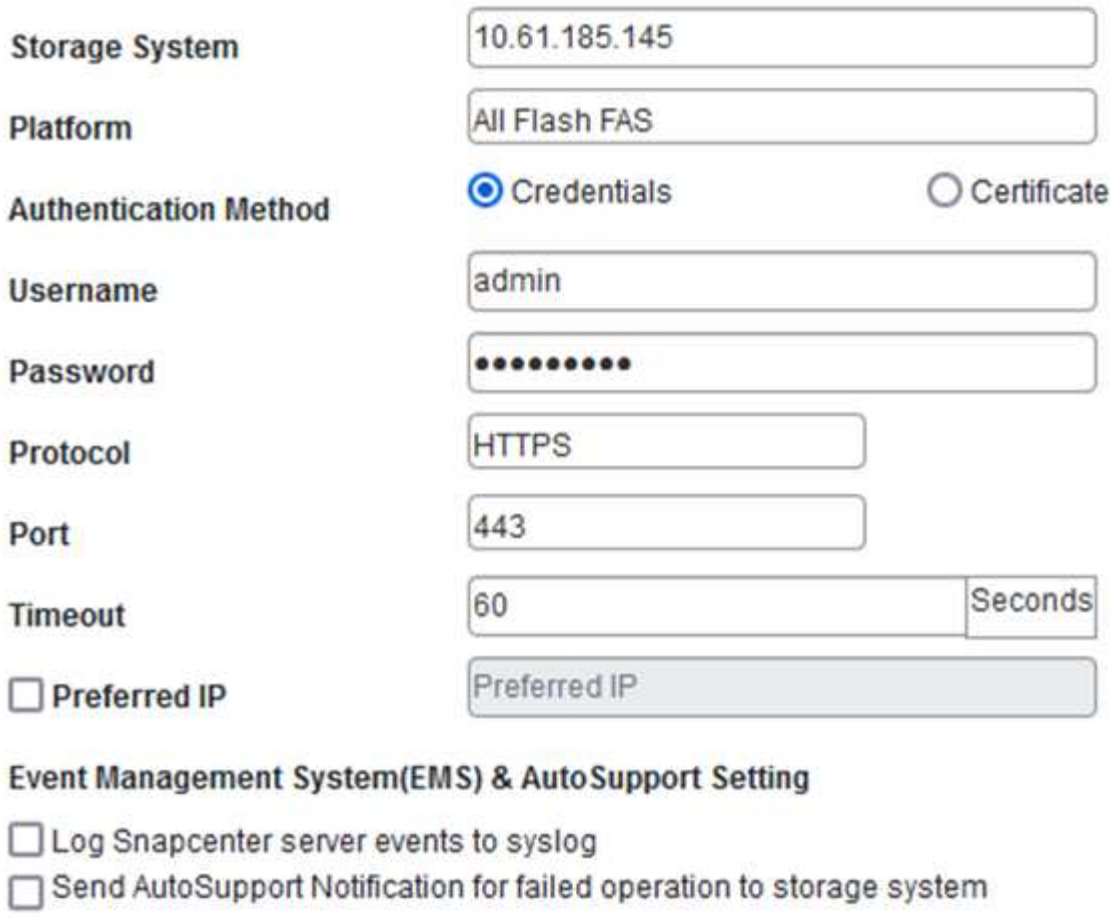
Sistemi di archiviazione Discovery ONTAP

Scopri i cluster di archiviazione ONTAP da utilizzare per i backup primari e secondari.

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Sistemi di storage** nel menu a sinistra e clicca sul pulsante **Aggiungi**.



2. Compila le credenziali e il tipo di piattaforma per il sistema di archiviazione ONTAP primario e fai clic su **Aggiungi**.



3. Ripetere questa procedura per il sistema di archiviazione ONTAP secondario.

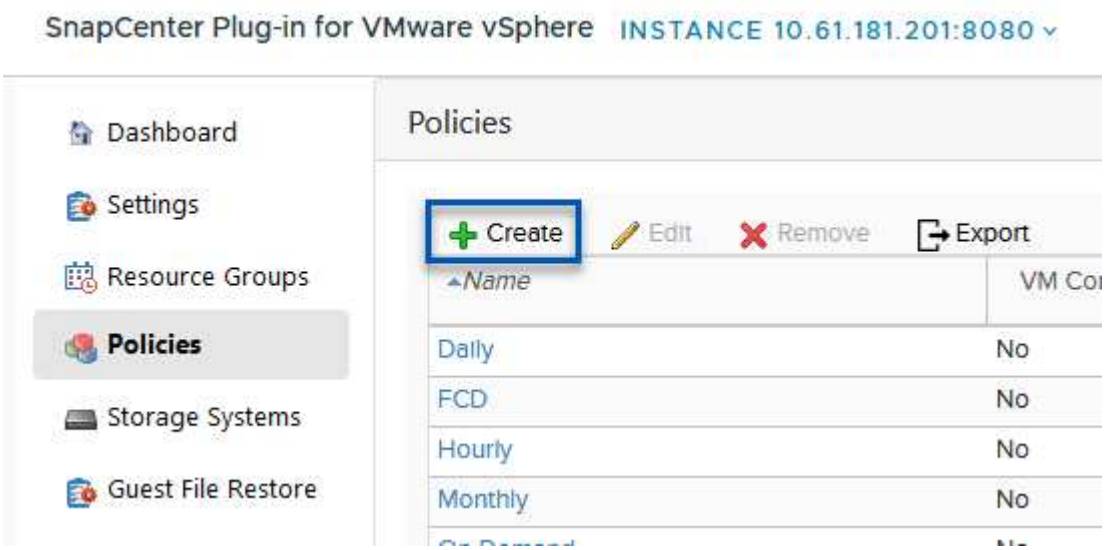
Creare policy di backup SCV

Le policy specificano il periodo di conservazione, la frequenza e le opzioni di replica per i backup gestiti da SCV.

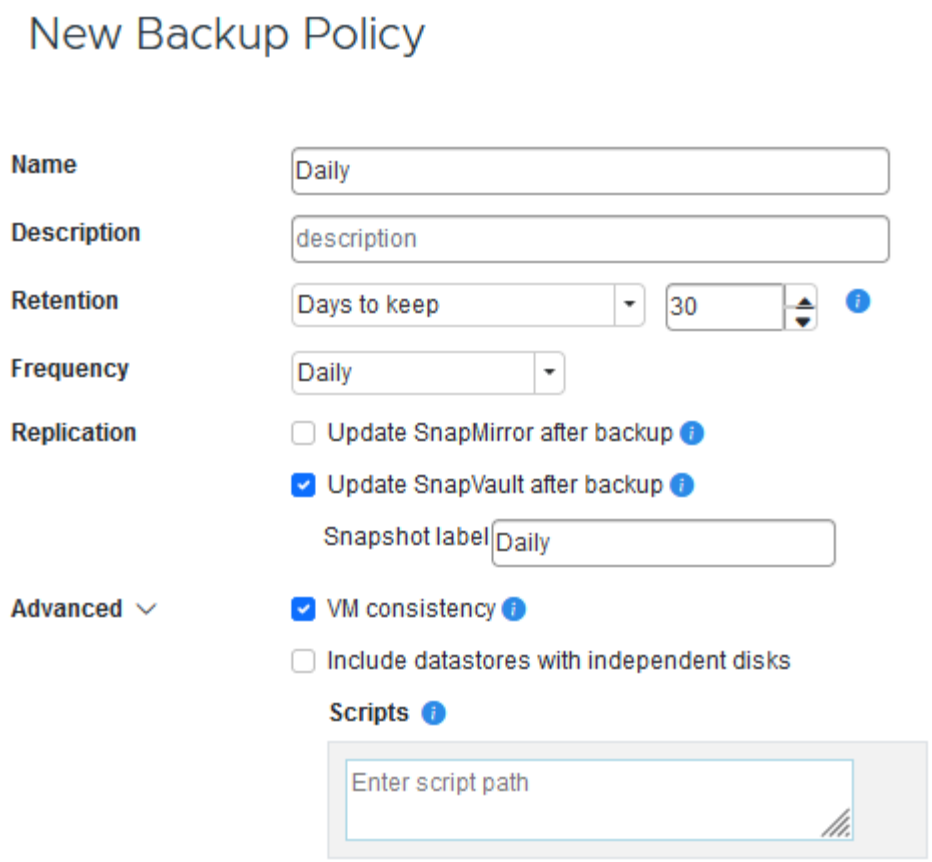
Rivedere il "Creare policy di backup per VM e datastore" sezione della documentazione per maggiori informazioni.

Per creare criteri di backup, completare i seguenti passaggi:

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Criteri** nel menu a sinistra e clicca sul pulsante **Crea**.



2. Specificare un nome per la policy, il periodo di conservazione, le opzioni di frequenza e replica e l'etichetta dello snapshot.



Quando si crea un criterio nel plug-in SnapCenter , verranno visualizzate le opzioni per SnapMirror e SnapVault. Se si sceglie SnapMirror, la pianificazione di conservazione specificata nel criterio sarà la stessa sia per gli snapshot primari che per quelli secondari. Se si sceglie SnapVault, la pianificazione della conservazione per lo snapshot secondario sarà basata su una pianificazione separata implementata con la relazione SnapMirror . Questa funzionalità è utile quando si desiderano periodi di conservazione più lunghi per i backup secondari.

Le etichette snapshot sono utili in quanto possono essere utilizzate per attuare policy con un periodo di conservazione specifico per le copie SnapVault replicate sul cluster ONTAP secondario. Quando SCV viene utilizzato con BlueXP Backup and Restore, il campo Etichetta snapshot deve essere vuoto o match l'etichetta specificata nella policy di backup BlueXP .

3. Ripetere la procedura per ogni polizza richiesta. Ad esempio, criteri separati per backup giornalieri, settimanali e mensili.

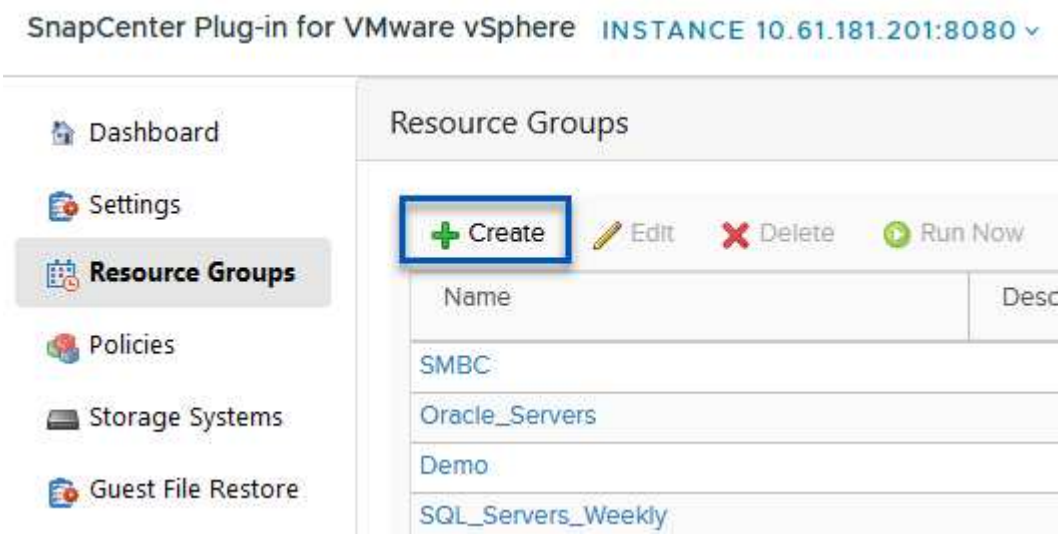
Creare gruppi di risorse

I gruppi di risorse contengono i datastore e le macchine virtuali da includere in un processo di backup, insieme ai criteri associati e alla pianificazione del backup.

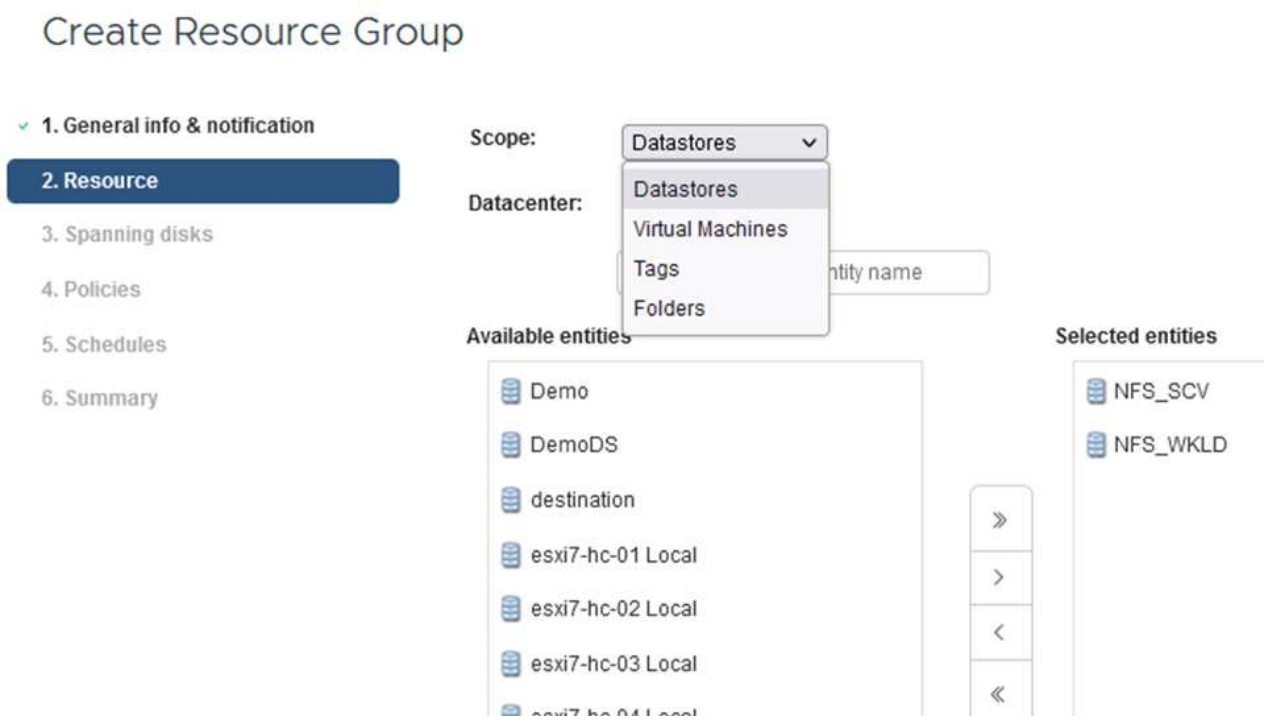
Rivedere il "Creare gruppi di risorse" sezione della documentazione per maggiori informazioni.

Per creare gruppi di risorse, completare i seguenti passaggi.

1. Nel SnapCenter Plug-in for VMware vSphere, vai su **Gruppi di risorse** nel menu a sinistra e clicca sul pulsante **Crea**.

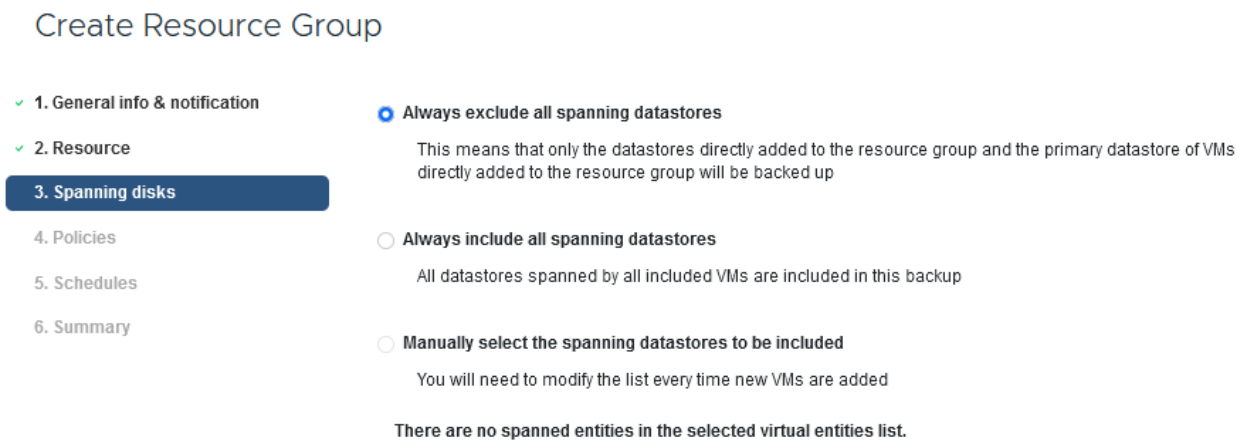


2. Nella procedura guidata Crea gruppo di risorse, immettere un nome e una descrizione per il gruppo, nonché le informazioni necessarie per ricevere le notifiche. Clicca su **Avanti**
3. Nella pagina successiva selezionare i datastore e le macchine virtuali che si desidera includere nel processo di backup, quindi fare clic su **Avanti**.



È possibile selezionare VM specifiche o interi datastore. Indipendentemente dalla scelta effettuata, viene eseguito il backup dell'intero volume (e del datastore), poiché il backup è il risultato dell'acquisizione di uno snapshot del volume sottostante. Nella maggior parte dei casi è più semplice scegliere l'intero datastore. Tuttavia, se si desidera limitare l'elenco delle VM disponibili durante il ripristino, è possibile scegliere solo un sottoinsieme di VM per il backup.

4. Selezionare le opzioni per l'estensione degli archivi dati per le VM con VMDK che risiedono su più archivi dati, quindi fare clic su **Avanti**.

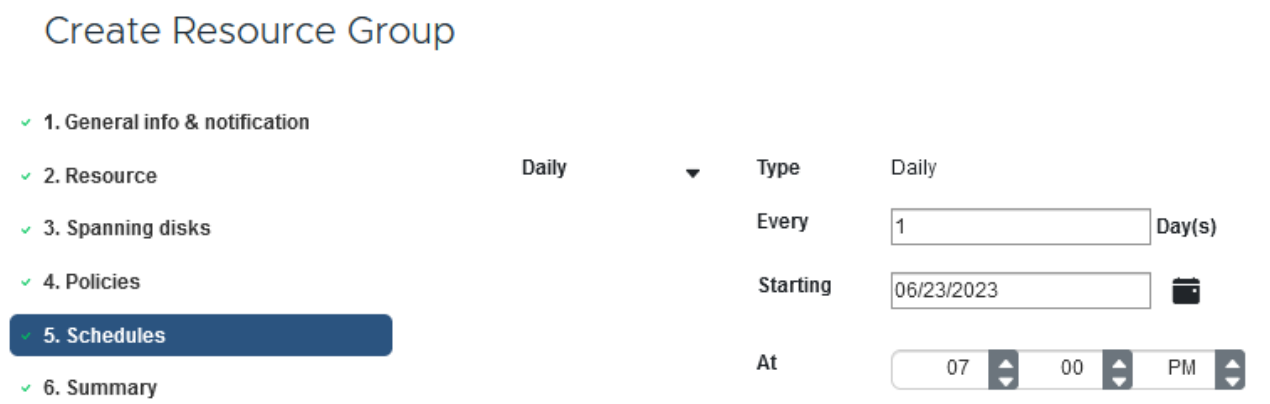


Attualmente, il BlueXP backup and recovery non supportano il backup di VM con VMDK che si estendono su più datastore.

5. Nella pagina successiva seleziona i criteri che saranno associati al gruppo di risorse e fai clic su **Avanti**.

Quando si esegue il backup di snapshot gestiti da SCV su un archivio di oggetti tramite BlueXP backup and recovery, ogni gruppo di risorse può essere associato a un solo criterio.

6. Selezionare una pianificazione che determinerà gli orari in cui verranno eseguiti i backup. Fare clic su **Avanti**.

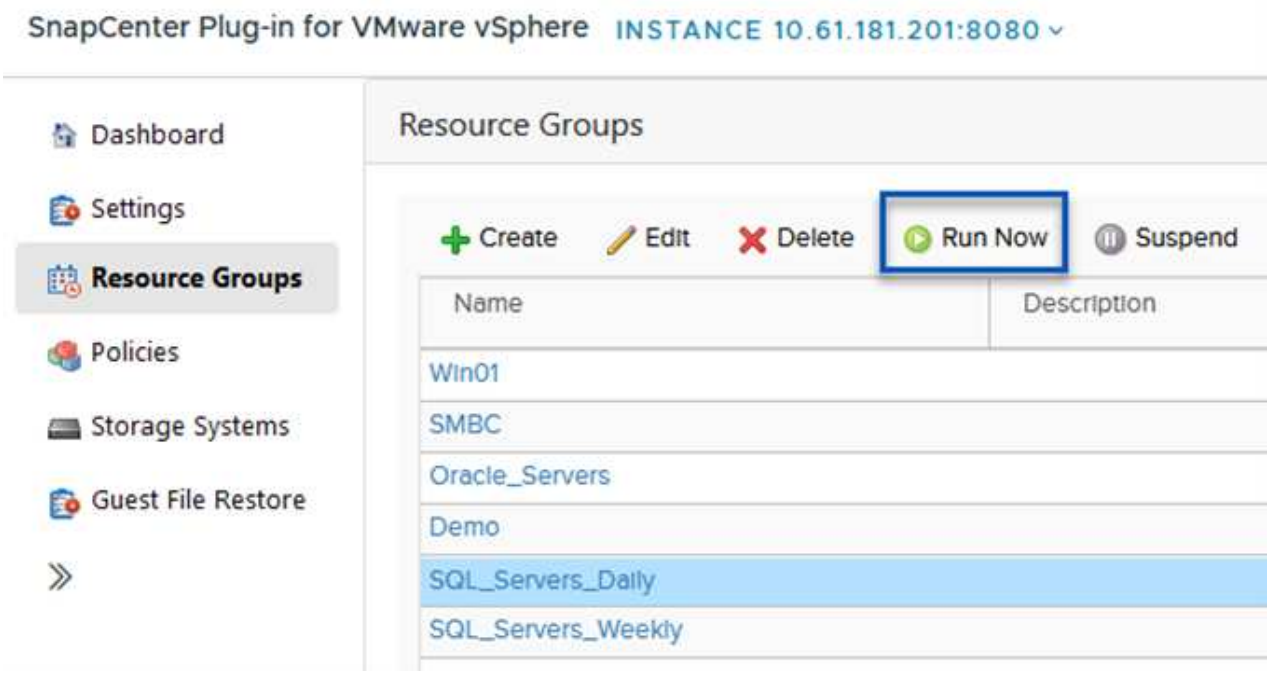


7. Infine, rivedere la pagina di riepilogo e quindi fare clic su **Fine** per completare la creazione del gruppo di risorse.

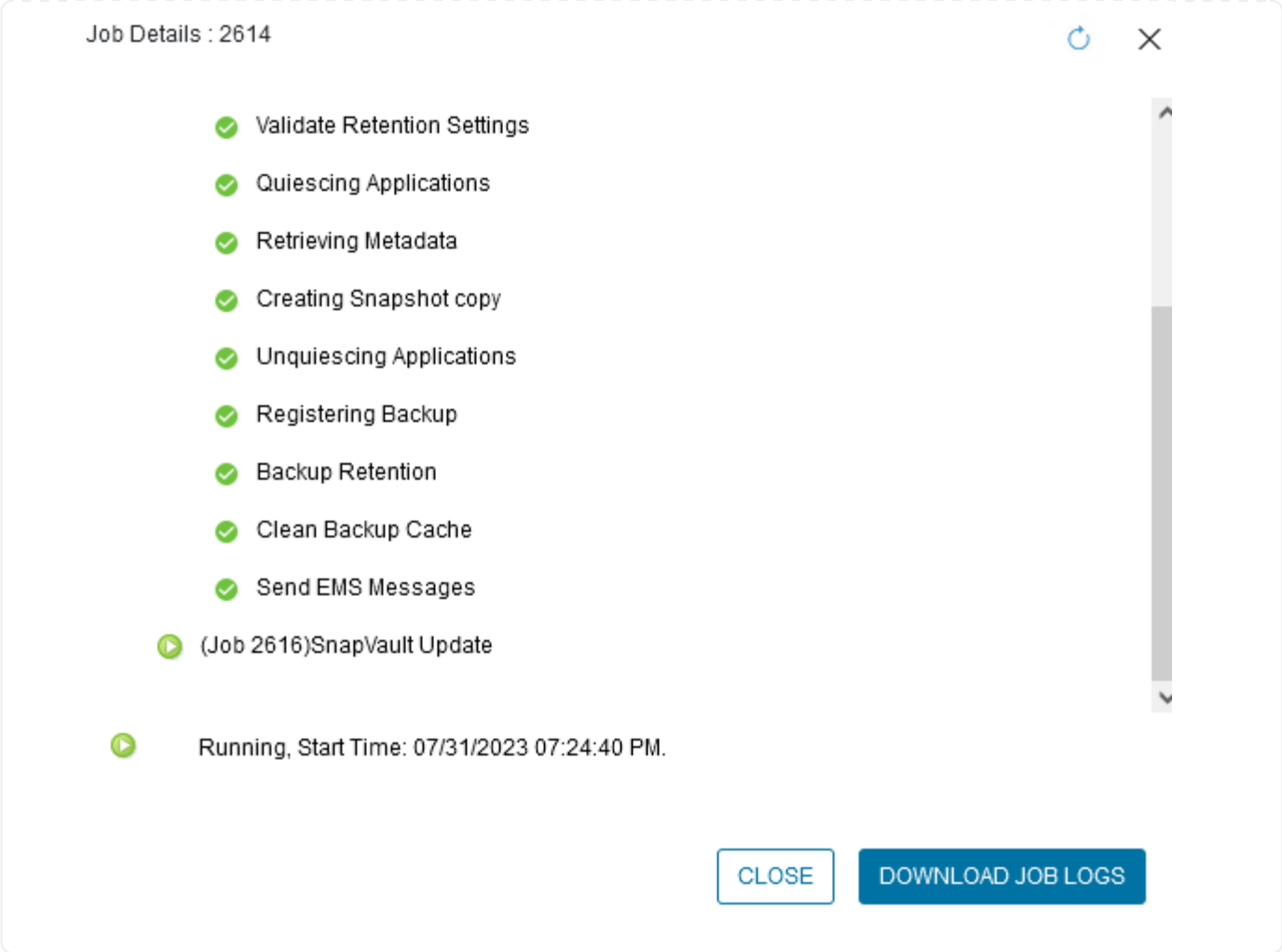
Eseguire un processo di backup

In questo passaggio finale, esegui un processo di backup e monitora il suo avanzamento. È necessario che almeno un processo di backup venga completato correttamente in SCV prima che le risorse possano essere rilevate dal BlueXP backup and recovery.

1. Nel SnapCenter Plug-in for VMware vSphere, accedere a **Gruppi di risorse** nel menu a sinistra.
2. Per avviare un processo di backup, selezionare il gruppo di risorse desiderato e fare clic sul pulsante **Esegui ora**.



3. Per monitorare il processo di backup, vai su **Dashboard** nel menu a sinistra. In **Attività recenti del lavoro** fare clic sul numero ID del lavoro per monitorare l'avanzamento del lavoro.



Configurare i backup su Object Storage nel BlueXP backup and recovery

Affinché BlueXP gestisca efficacemente l'infrastruttura dati, è necessaria l'installazione preventiva di un connettore. Il connettore esegue le azioni necessarie per individuare le risorse e gestire le operazioni sui dati.

Per maggiori informazioni sul connettore BlueXP fare riferimento a "Scopri di più sui connettori" nella documentazione BlueXP .

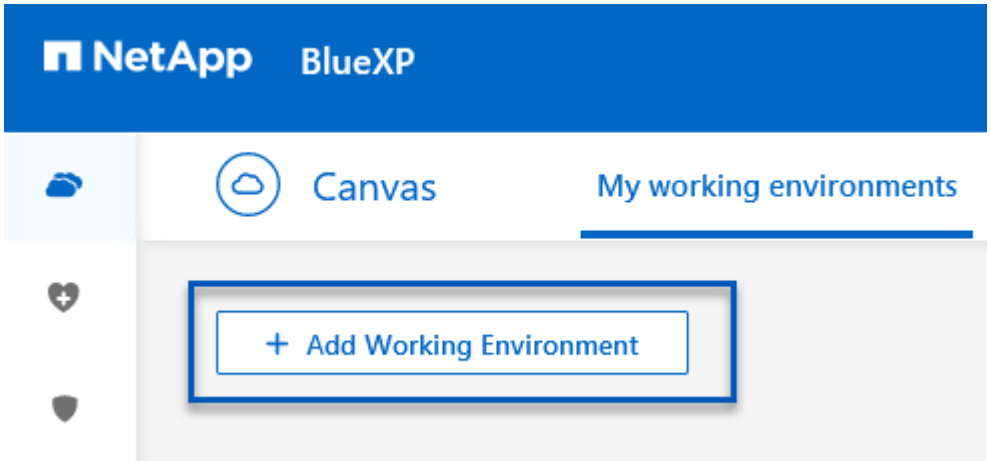
Una volta installato il connettore per il provider cloud utilizzato, sarà possibile visualizzare una rappresentazione grafica dell'archiviazione degli oggetti da Canvas.

Per configurare il BlueXP backup and recovery per eseguire il backup dei dati gestiti da SCV in locale, completare i seguenti passaggi:

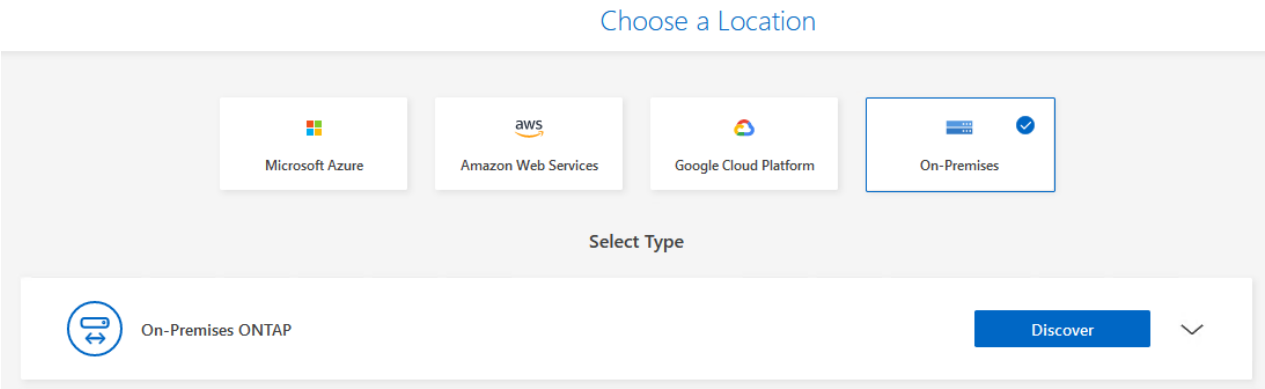
Aggiungi ambienti di lavoro alla tela

Il primo passo è aggiungere i sistemi di archiviazione ONTAP locali a BlueXP

1. Per iniziare, seleziona **Aggiungi ambiente di lavoro** dalla tela.



2. Seleziona **In sede** tra le posizioni disponibili e poi clicca sul pulsante **Scopri**.



3. Compila le credenziali per il sistema di archiviazione ONTAP e clicca sul pulsante **Scopri** per aggiungere l'ambiente di lavoro.

ONTAP Cluster IP

10.61.181.180

User Name

admin

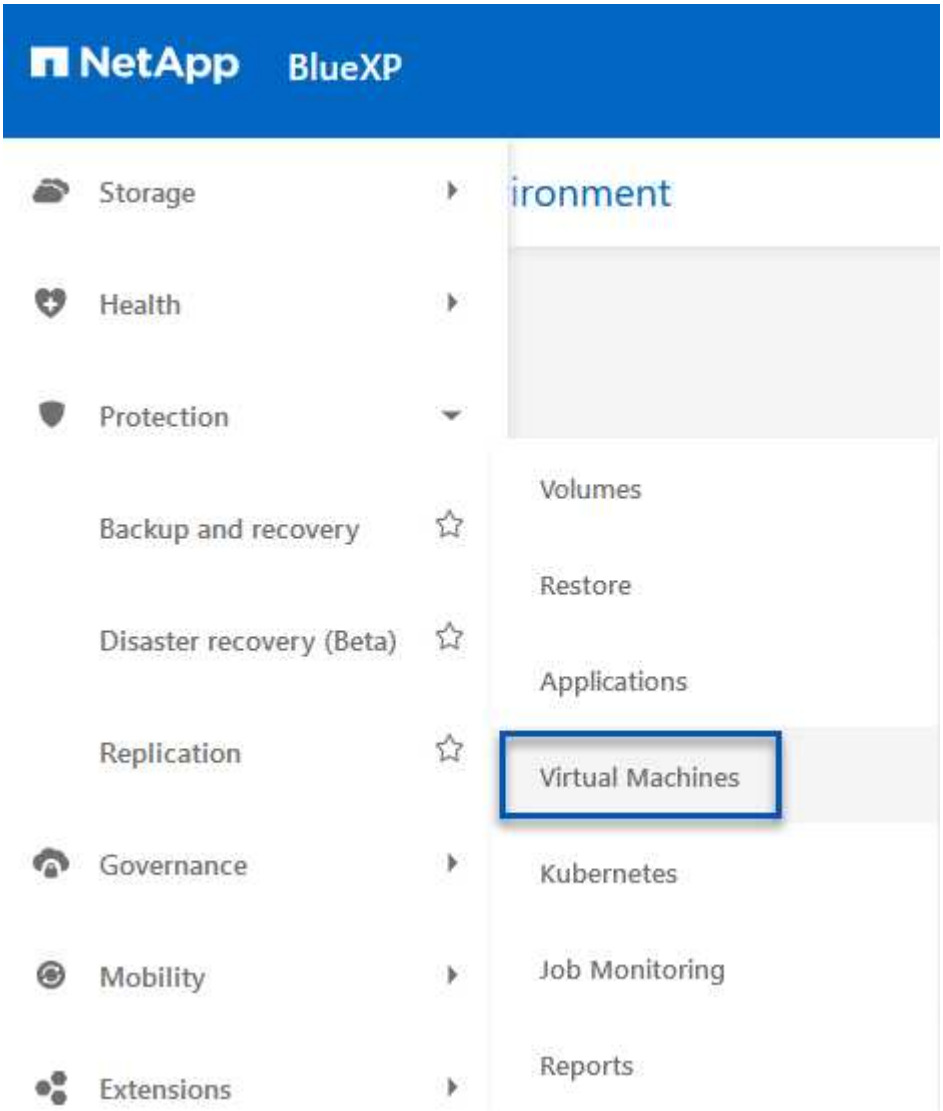
Password

••••••••••

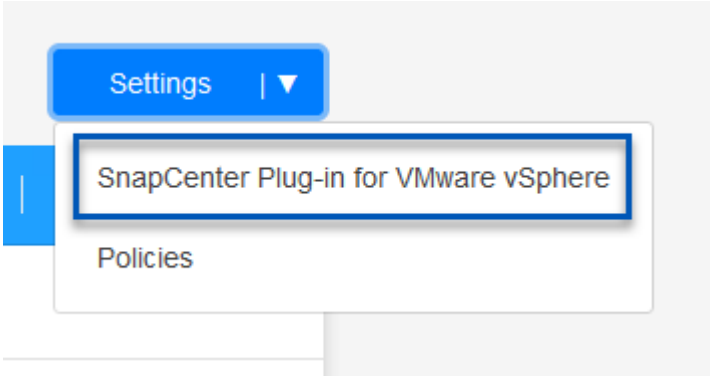
Scopri l'appliance SCV on-premise e vCenter

Per scoprire le risorse del datastore locale e della macchina virtuale, aggiungere le informazioni per il broker dati SCV e le credenziali per l'appliance di gestione vCenter.

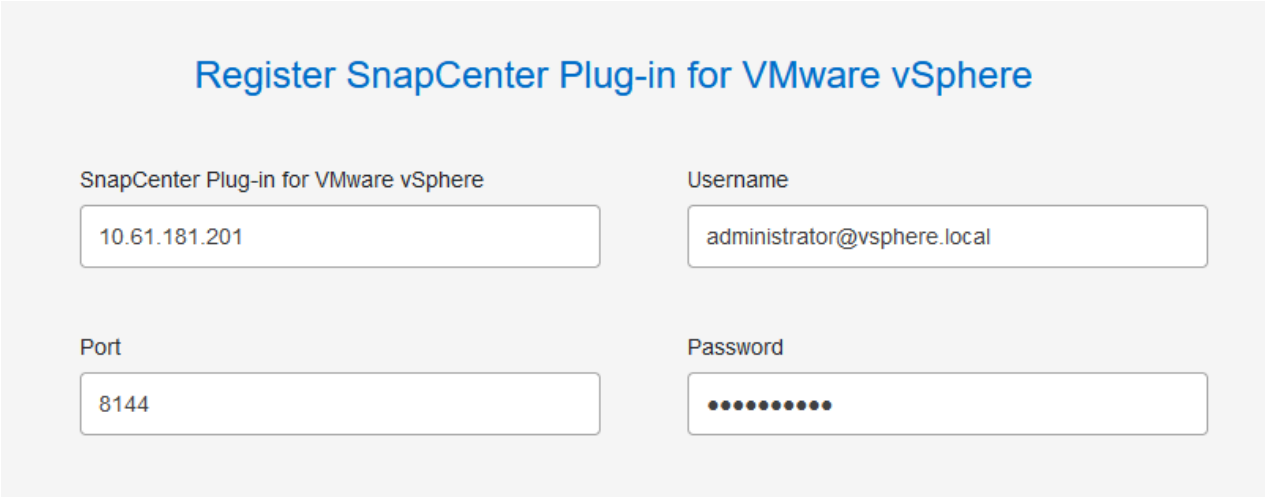
1. Dal menu di sinistra BlueXP selezionare **Protezione > Backup e ripristino > Macchine virtuali**



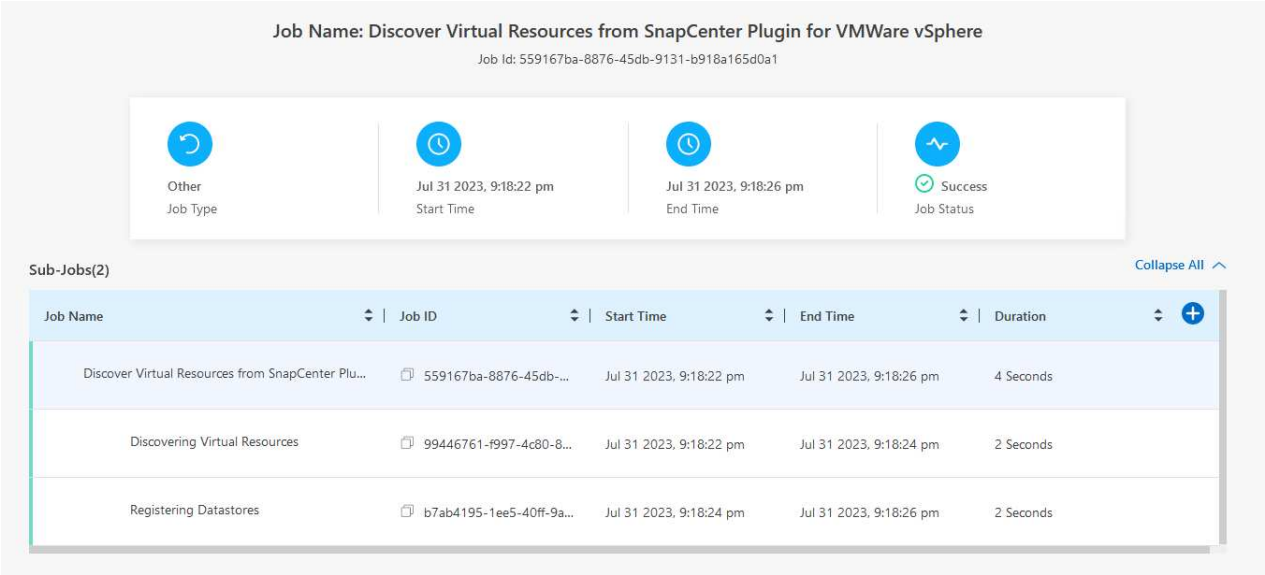
2. Dalla schermata principale Macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare * SnapCenter Plug-in for VMware vSphere*.



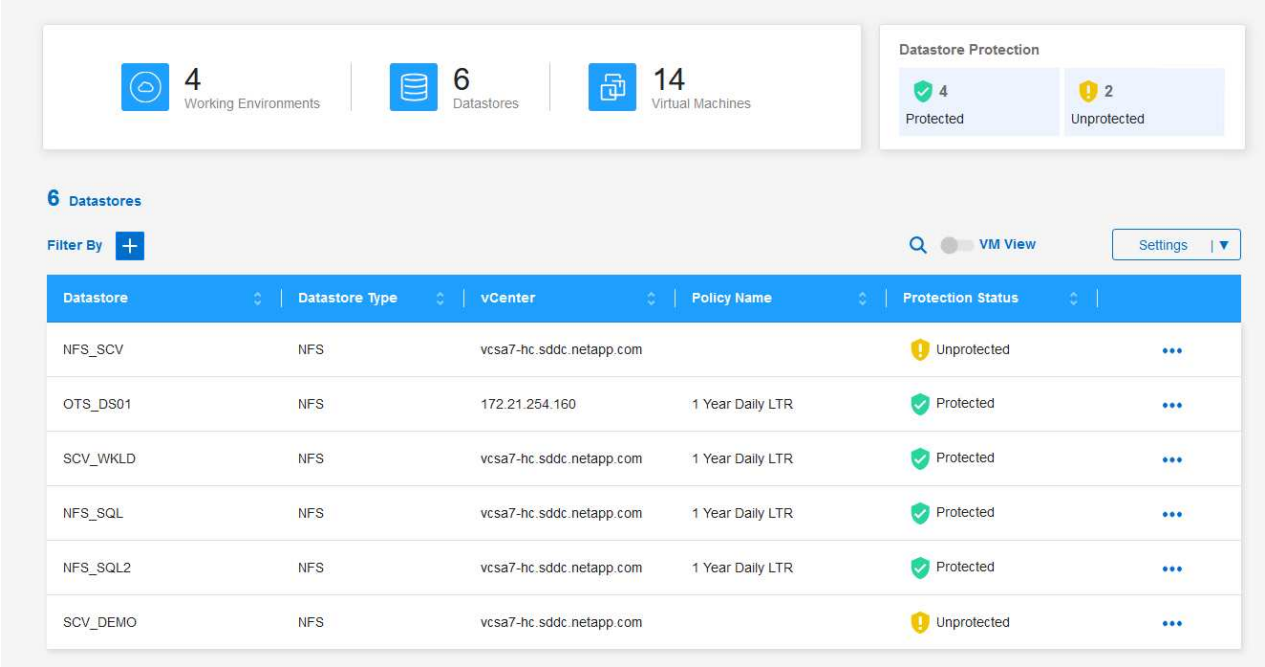
3. Fare clic sul pulsante **Registra**, quindi immettere l'indirizzo IP e il numero di porta per l'appliance SnapCenter Plug-in e il nome utente e la password per l'appliance di gestione vCenter. Fare clic sul pulsante **Registrati** per iniziare il processo di scoperta.



4. È possibile monitorare l'avanzamento dei lavori dalla scheda Monitoraggio lavori.



5. Una volta completata l'individuazione, sarà possibile visualizzare i datastore e le macchine virtuali in tutti gli appliance SCV individuati.

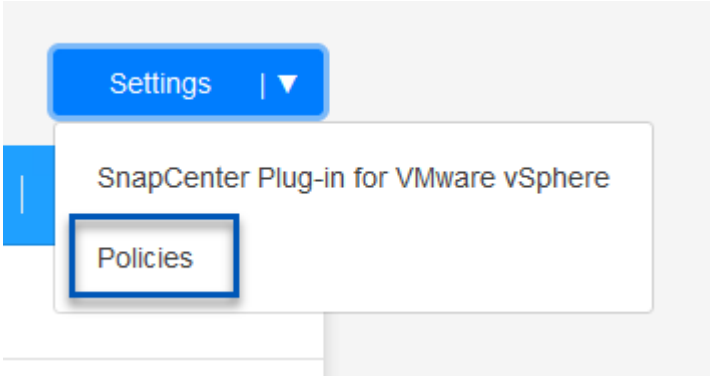

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

Creare policy di backup BlueXP

Nel BlueXP backup and recovery per macchine virtuali, creare criteri per specificare il periodo di conservazione, l'origine del backup e i criteri di archiviazione.

Per ulteriori informazioni sulla creazione di policy fare riferimento a "Creare una policy per eseguire il backup degli archivi dati" .

1. Dalla pagina principale di BlueXP backup and recovery per macchine virtuali, accedi al menu a discesa **Impostazioni** e seleziona **Criteri**.



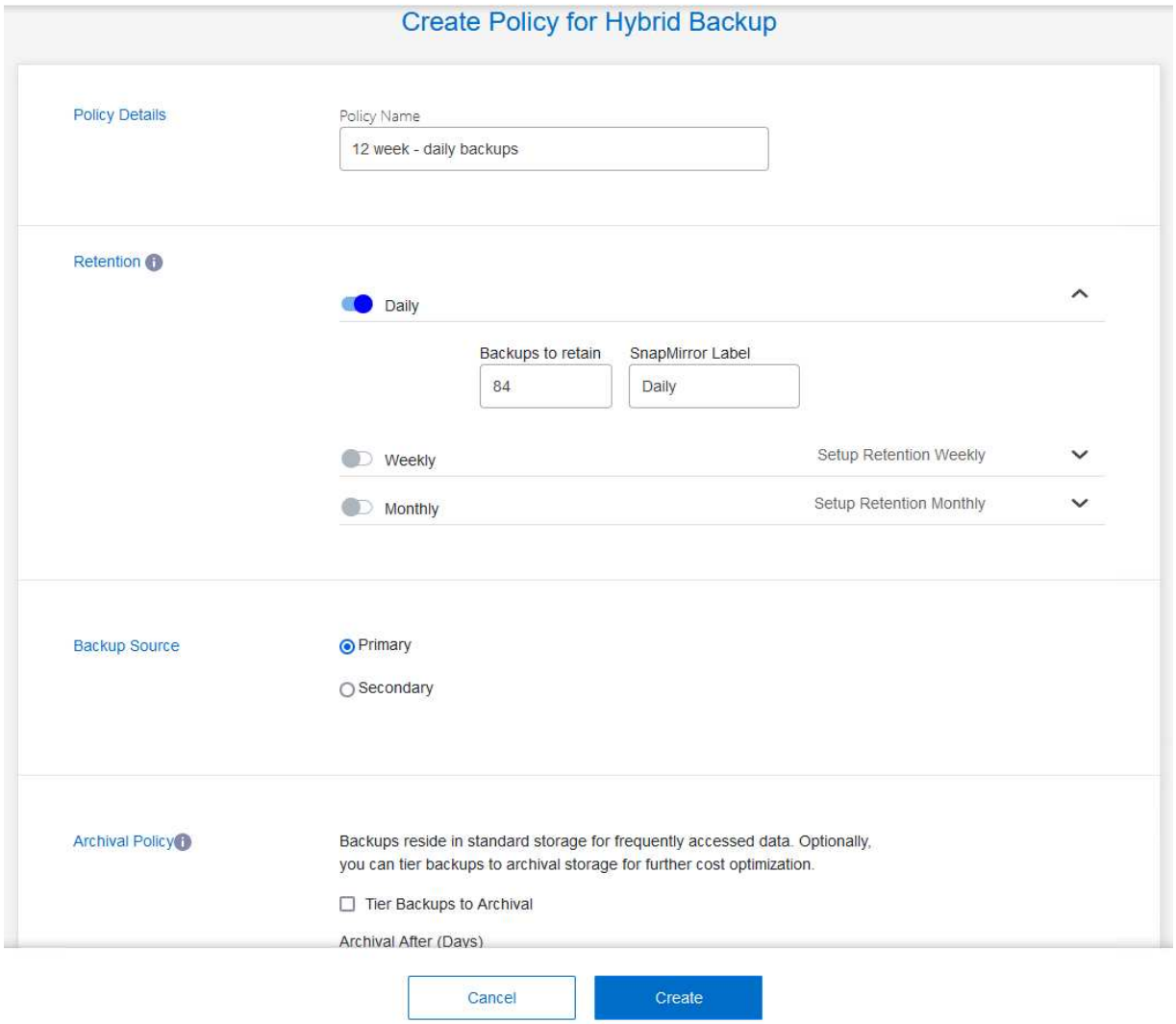
2. Fare clic su **Crea criterio** per accedere alla finestra **Crea criterio per backup ibrido**.

   a. Aggiungi un nome per la policy

   b. Seleziona il periodo di conservazione desiderato

   c. Selezionare se i backup verranno originati dal sistema di archiviazione ONTAP locale primario o secondario

   d. Facoltativamente, specificare dopo quale periodo di tempo i backup verranno archiviati in livelli diversi per un ulteriore risparmio sui costi.



L'etichetta SnapMirror immessa qui viene utilizzata per identificare a quali backup applicare la policy. Il nome dell'etichetta deve corrispondere al nome dell'etichetta nel criterio SCV locale corrispondente.

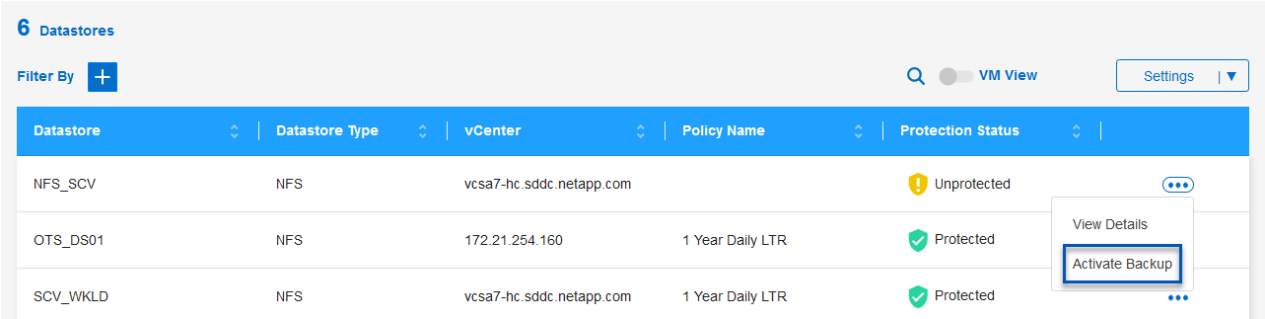
3. Fare clic su **Crea** per completare la creazione della policy.

Backup degli archivi dati su Amazon Web Services

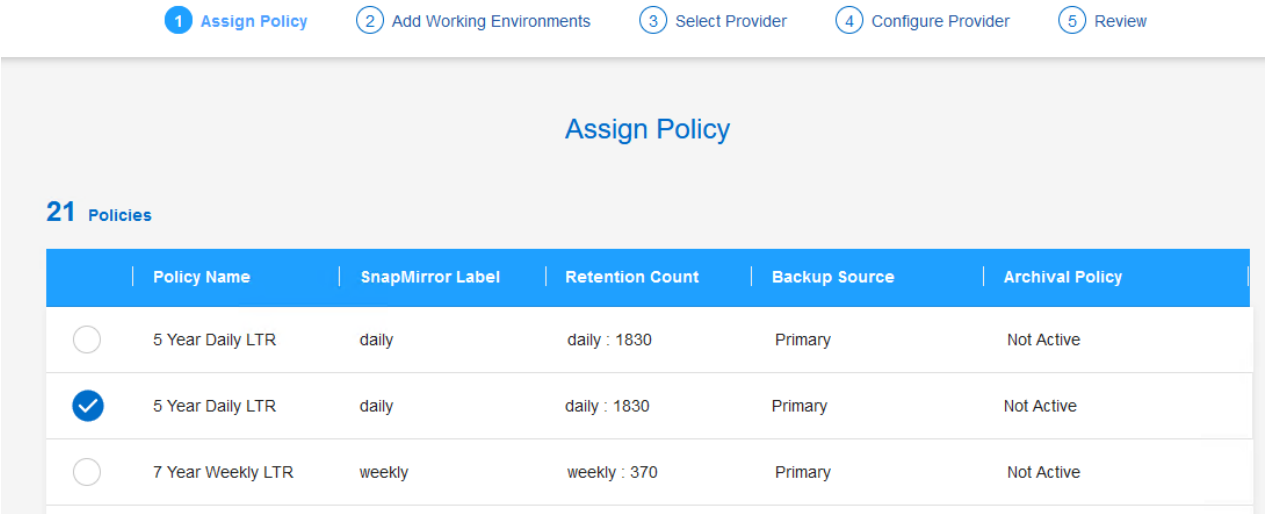
Il passaggio finale consiste nell'attivare la protezione dei dati per i singoli datastore e le macchine virtuali. I passaggi seguenti descrivono come attivare i backup su AWS.

Per maggiori informazioni fare riferimento a "Eseguire il backup degli archivi dati su Amazon Web Services" .

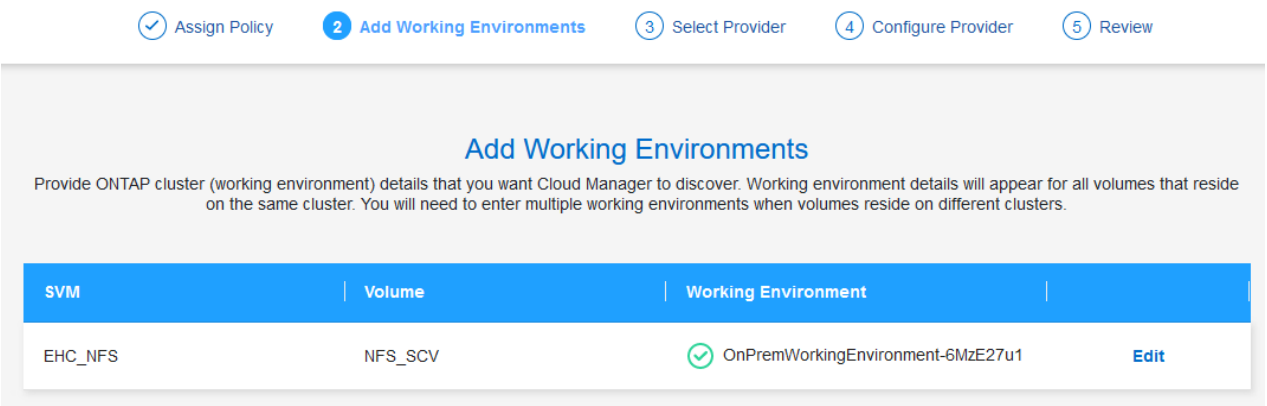
1. Dalla pagina principale di BlueXP backup and recovery per macchine virtuali, accedere al menu a discesa delle impostazioni per il datastore di cui eseguire il backup e selezionare **Attiva backup**.



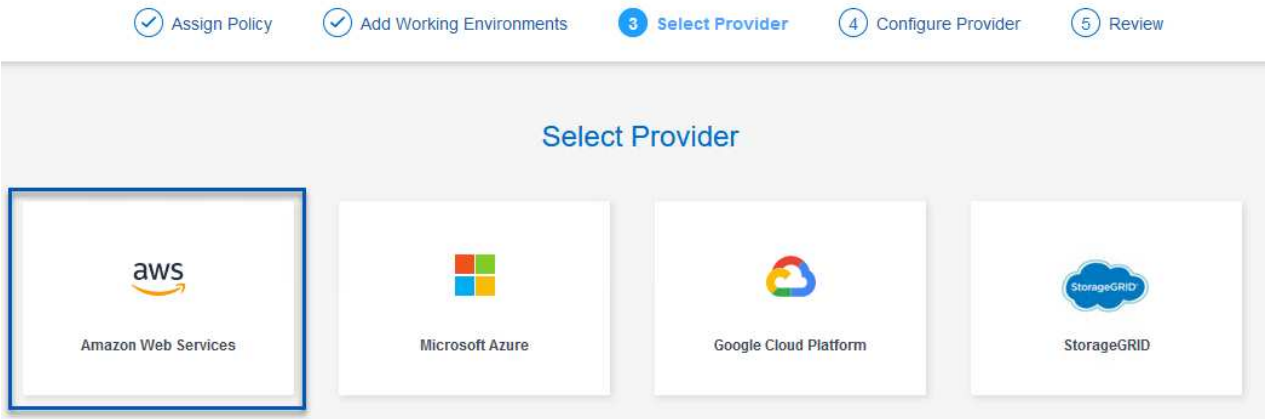
2. Assegnare la policy da utilizzare per l'operazione di protezione dei dati e fare clic su **Avanti**.



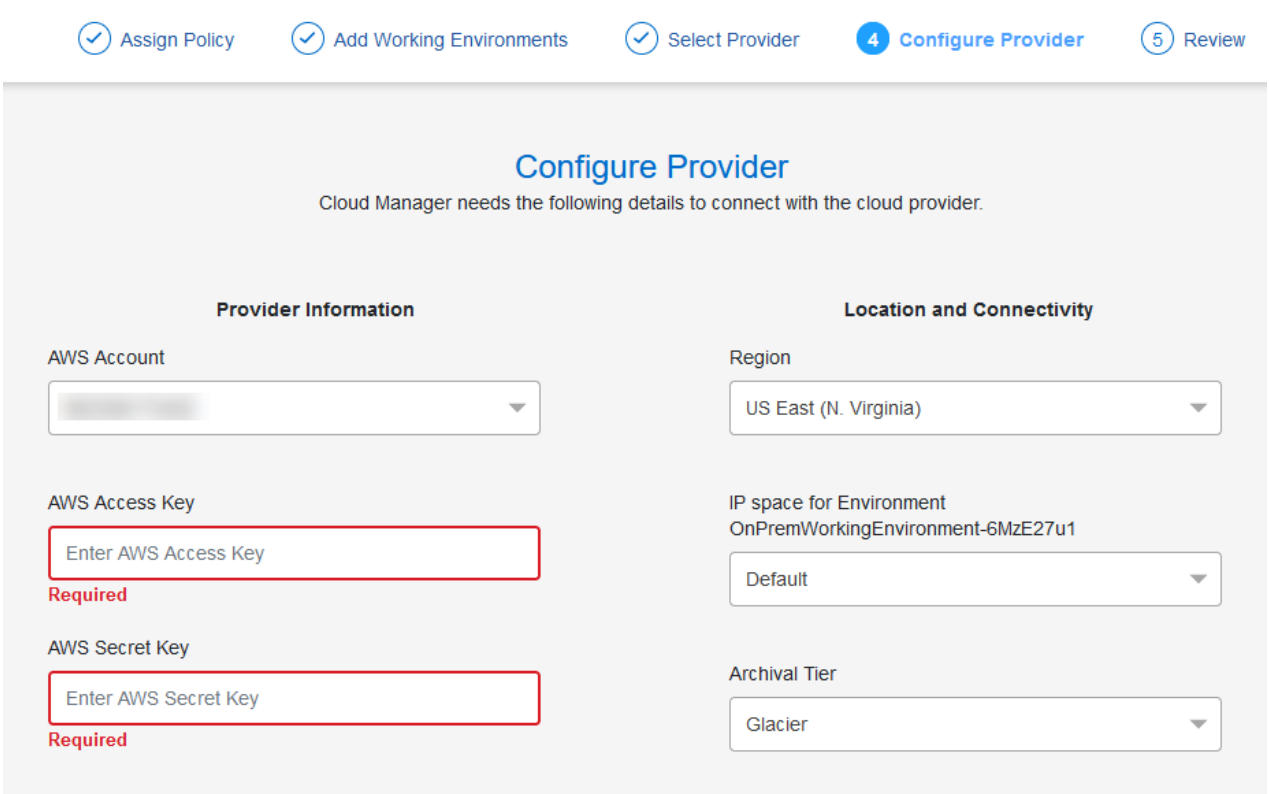
3. Nella pagina **Aggiungi ambienti di lavoro**, l'archivio dati e l'ambiente di lavoro con un segno di spunta dovrebbero apparire se l'ambiente di lavoro è stato precedentemente rilevato. Se l'ambiente di lavoro non è stato ancora scoperto, puoi aggiungerlo qui. Fare clic su **Avanti** per continuare.



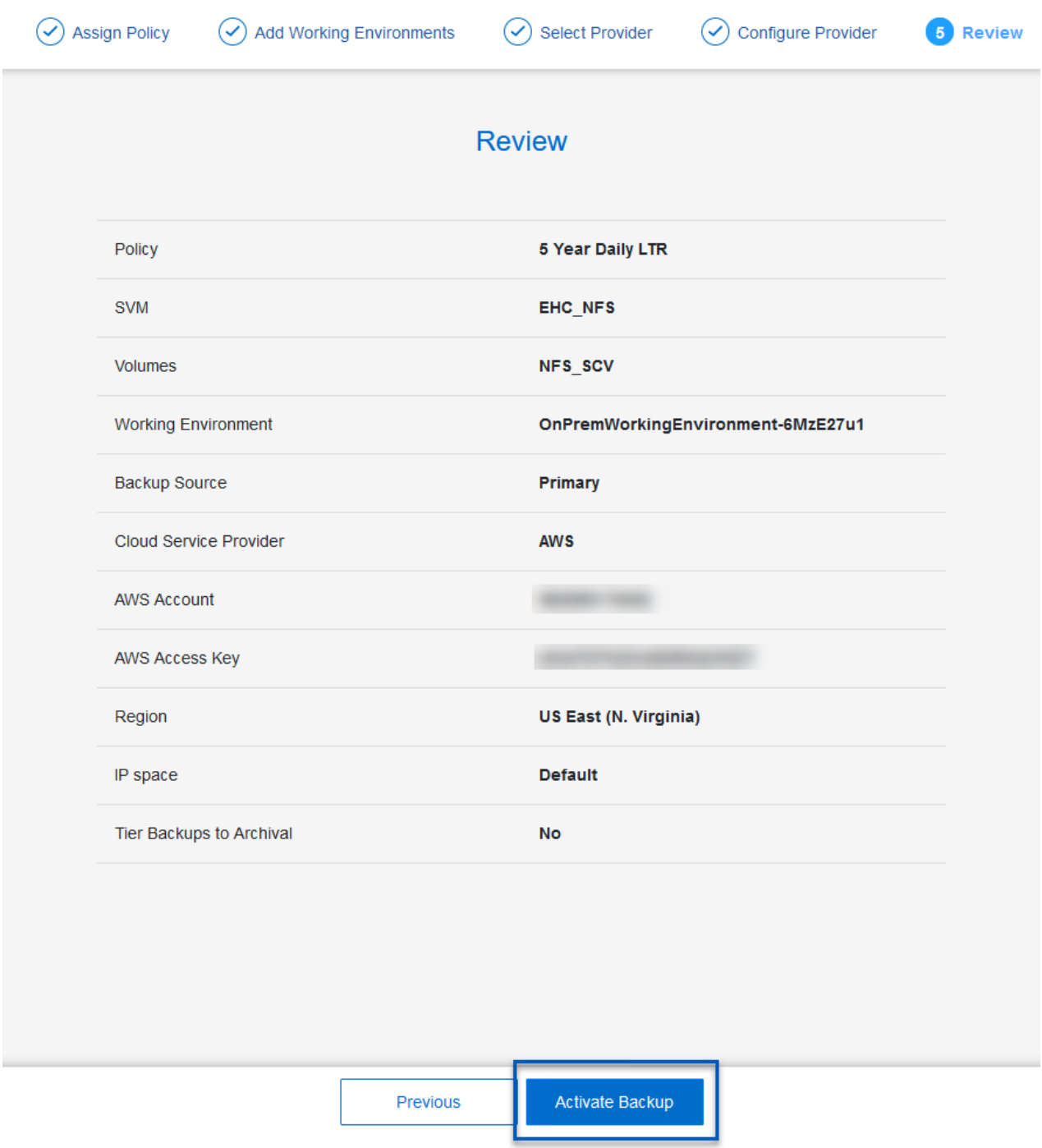
4. Nella pagina **Seleziona provider** clicca su AWS e poi clicca sul pulsante **Avanti** per continuare.



5. Compila le informazioni sulle credenziali specifiche del provider per AWS, tra cui la chiave di accesso e la chiave segreta AWS, la regione e il livello di archiviazione da utilizzare. Selezionare inoltre lo spazio IP ONTAP per il sistema di archiviazione ONTAP locale. Fare clic su **Avanti**.



6. Infine, rivedere i dettagli del processo di backup e fare clic sul pulsante **Attiva backup** per avviare la protezione dei dati del datastore.



A questo punto il trasferimento dei dati potrebbe non iniziare immediatamente. Ogni ora , la BlueXP backup and recovery esegue la scansione di eventuali snapshot in sospeso e li trasferisce nell'archivio oggetti.

Ripristino di macchine virtuali in caso di perdita di dati

Garantire la salvaguardia dei tuoi dati è solo uno degli aspetti di una protezione completa dei dati. Altrettanto cruciale è la capacità di ripristinare tempestivamente i dati da qualsiasi posizione in caso di perdita di dati o di attacco ransomware. Questa capacità è fondamentale per mantenere operazioni aziendali senza interruzioni e raggiungere gli obiettivi del punto di ripristino.

NetApp offre una strategia 3-2-1 altamente adattabile, che fornisce un controllo personalizzato sui programmi di conservazione nelle posizioni di archiviazione primaria, secondaria e degli oggetti. Questa strategia offre la flessibilità necessaria per adattare gli approcci alla protezione dei dati alle esigenze specifiche.

Questa sezione fornisce una panoramica del processo di ripristino dei dati sia dal SnapCenter Plug-in for VMware vSphere sia BlueXP backup and recovery per macchine virtuali.

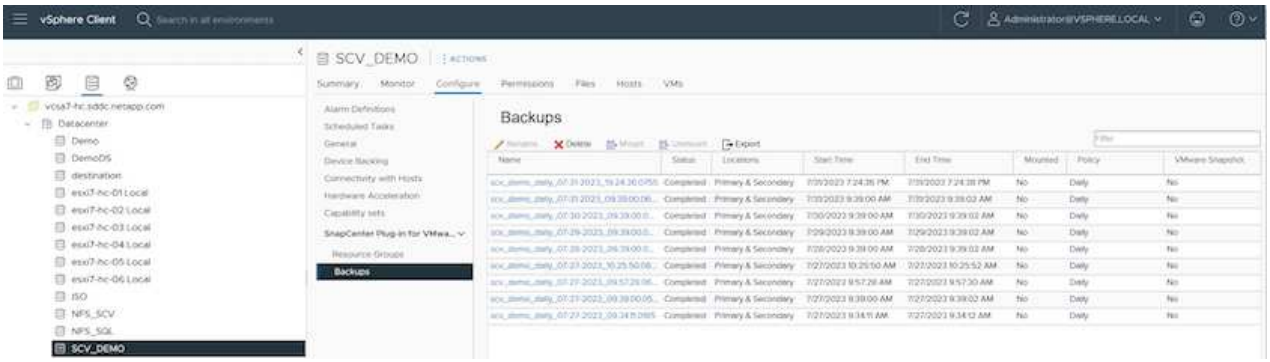
Ripristino di macchine virtuali dal SnapCenter Plug-in for VMware vSphere

Per questa soluzione le macchine virtuali sono state ripristinate nelle posizioni originali e alternative. Questa soluzione non copre tutti gli aspetti delle funzionalità di ripristino dei dati di SCV. Per informazioni approfondite su tutto ciò che SCV ha da offrire, fare riferimento al "Ripristinare le VM dai backup" nella documentazione del prodotto.

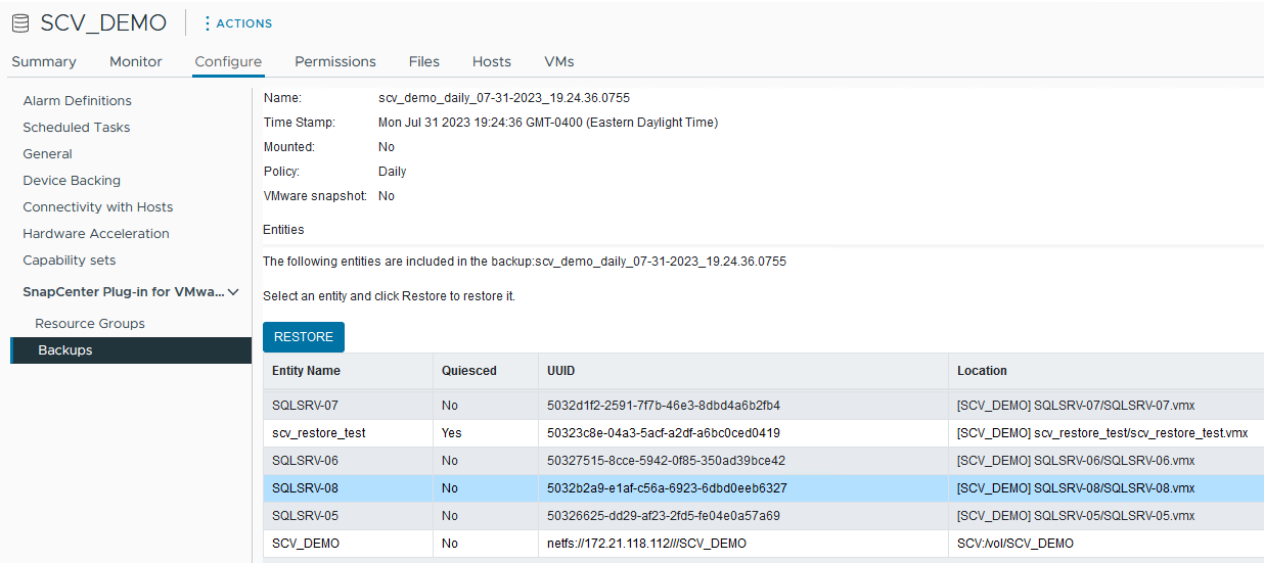
Ripristinare le macchine virtuali da SCV

Completare i seguenti passaggi per ripristinare una macchina virtuale da un archivio primario o secondario.

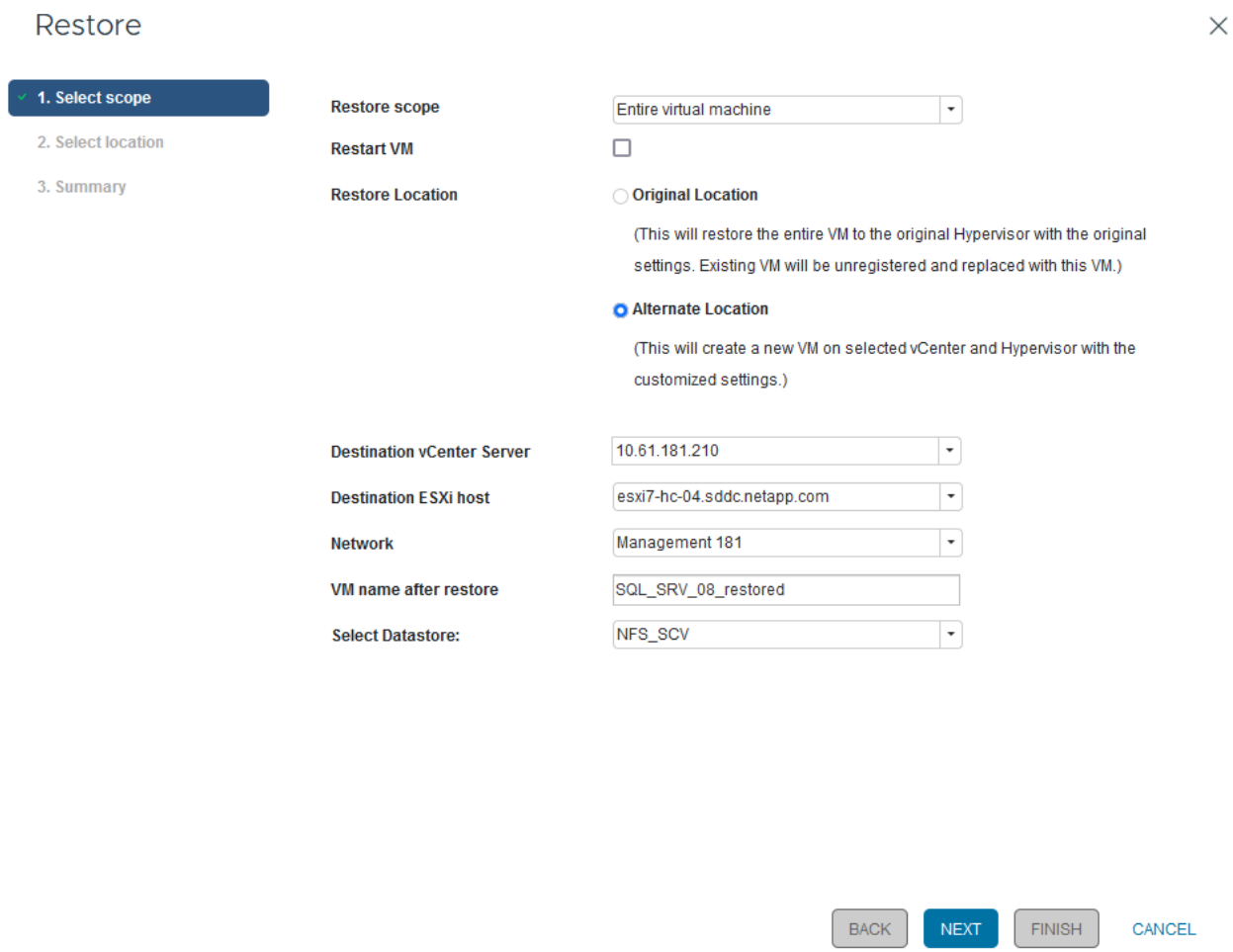
1. Dal client vCenter, vai su **Inventario > Archiviazione** e fai clic sul datastore che contiene le macchine virtuali che desideri ripristinare.
2. Dalla scheda **Configura** fare clic su **Backup** per accedere all'elenco dei backup disponibili.



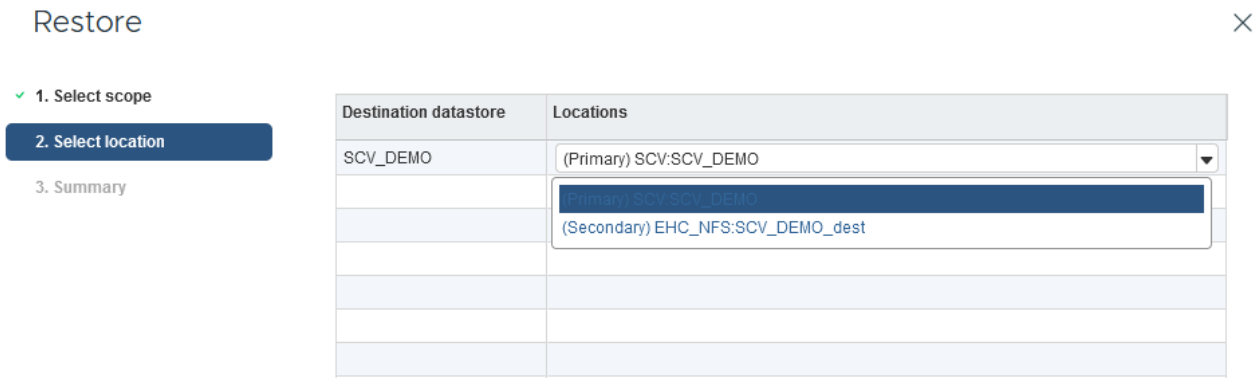
3. Fare clic su un backup per accedere all'elenco delle VM, quindi selezionare una VM da ripristinare. Fare clic su **Ripristina**.



4. Dalla procedura guidata di ripristino, seleziona se ripristinare l'intera macchina virtuale o un VMDK specifico. Selezionare se installare nella posizione originale o in una posizione alternativa, fornire il nome della VM dopo il ripristino e il datastore di destinazione. Fare clic su **Avanti**.



5. Scegliere se eseguire il backup dalla posizione di archiviazione primaria o secondaria.



6. Infine, rivedere un riepilogo del processo di backup e fare clic su Fine per avviare il processo di ripristino.

Ripristino di macchine virtuali dal BlueXP backup and recovery per macchine virtuali

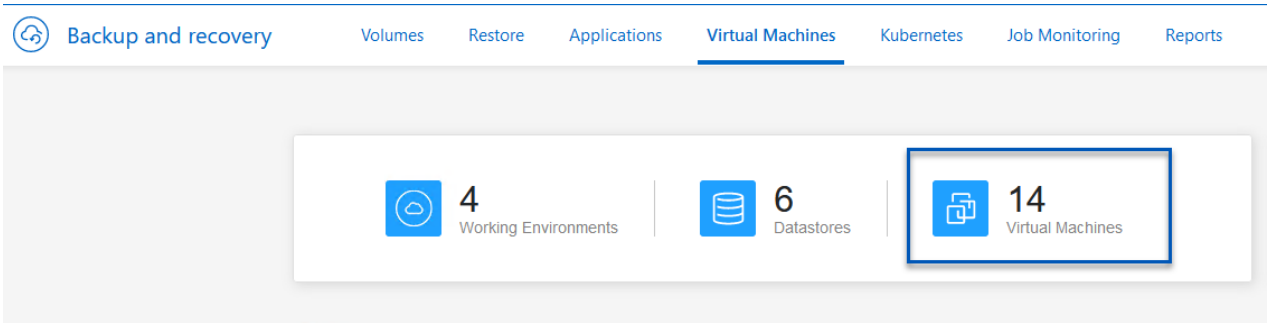
Il BlueXP backup and recovery per macchine virtuali consentono di ripristinare le macchine virtuali nella loro posizione originale. Le funzioni di ripristino sono accessibili tramite la console web BlueXP .

Per maggiori informazioni fare riferimento a "Ripristina i dati delle macchine virtuali dal cloud" .

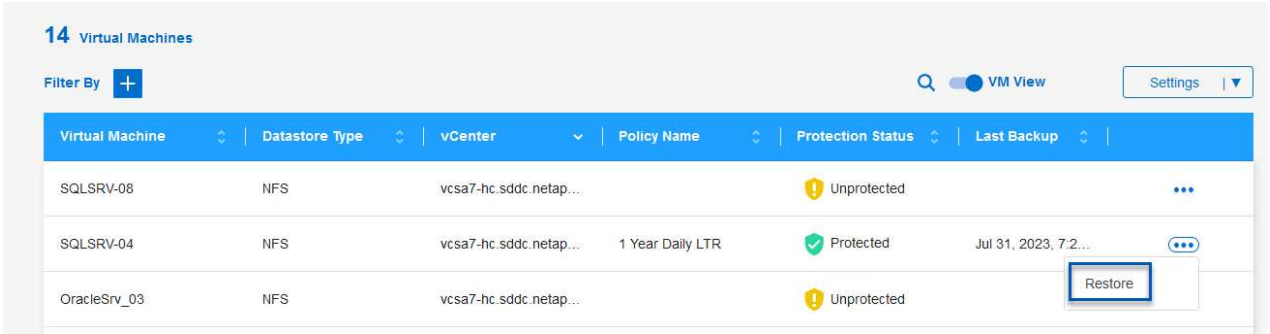
Ripristina macchine virtuali dal BlueXP backup and recovery

Per ripristinare una macchina virtuale dal BlueXP backup and recovery, completare i seguenti passaggi.

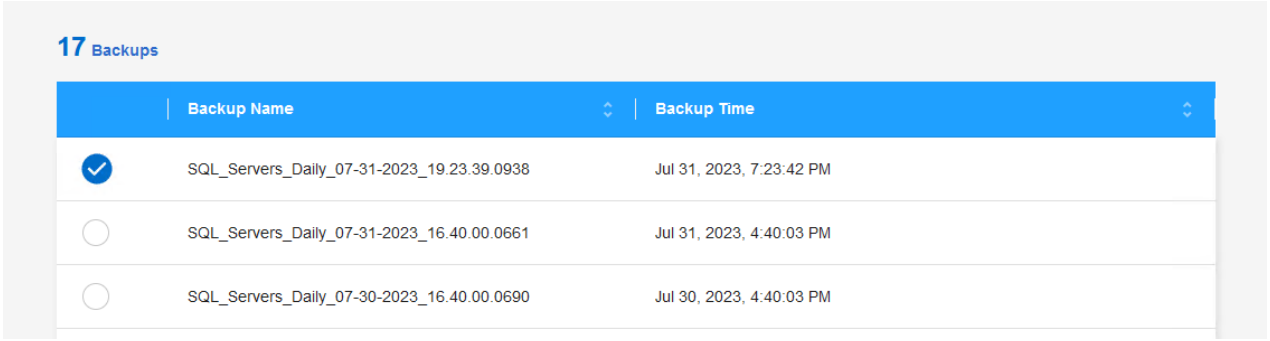
1. Passare a **Protezione > Backup e ripristino > Macchine virtuali** e fare clic su Macchine virtuali per visualizzare l'elenco delle macchine virtuali disponibili per il ripristino.



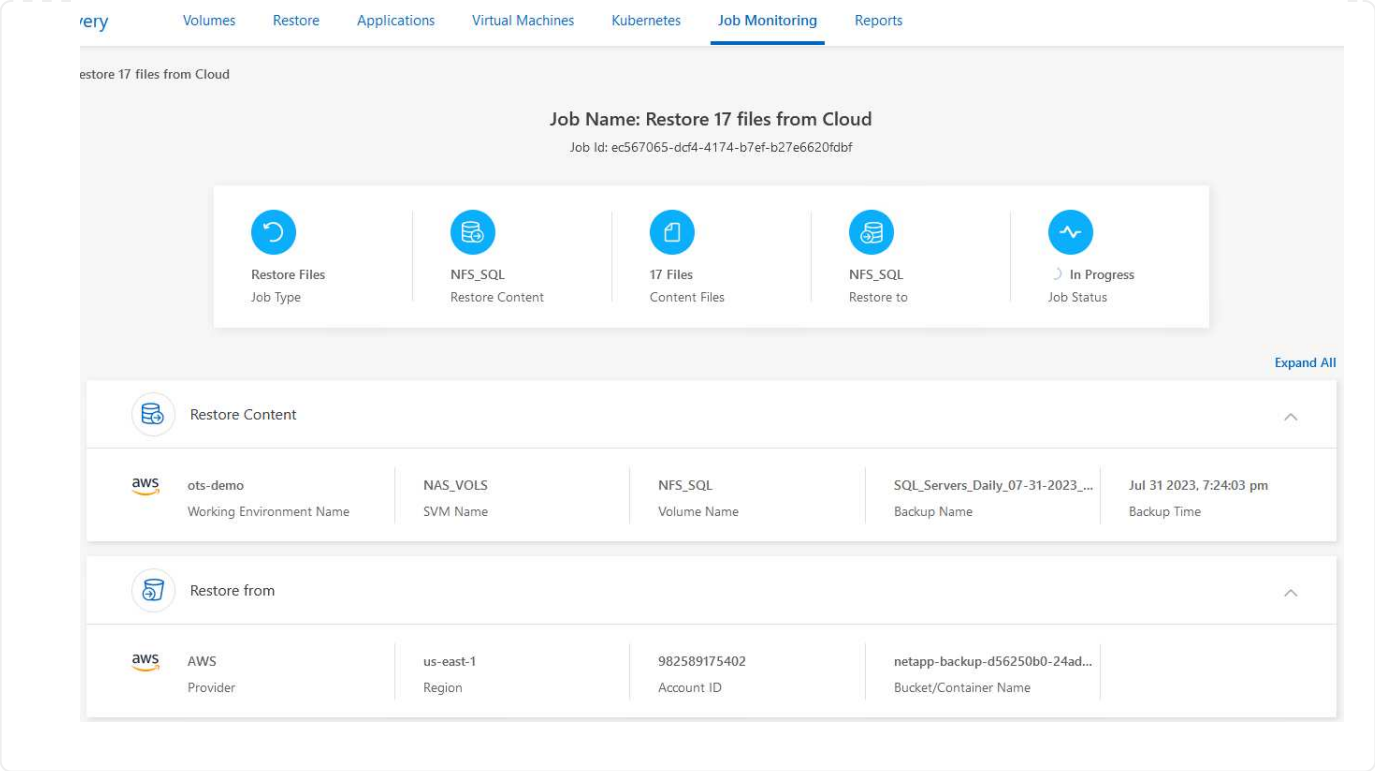
2. Accedi al menu a discesa delle impostazioni per la VM da ripristinare e seleziona



3. Selezionare il backup da cui effettuare il ripristino e fare clic su **Avanti**.



4. Esaminare un riepilogo del processo di backup e fare clic su **Ripristina** per avviare il processo di ripristino.
5. Monitorare l'avanzamento del processo di ripristino dalla scheda **Monitoraggio processo**.



Conclusione

La strategia di backup 3-2-1, se implementata con il SnapCenter Plug-in for VMware vSphere e il BlueXP backup and recovery per macchine virtuali, offre una soluzione solida, affidabile e conveniente per la protezione dei dati. Questa strategia non solo garantisce la ridondanza e l'accessibilità dei dati, ma offre anche la flessibilità di ripristinare i dati da qualsiasi posizione e sia dai sistemi di archiviazione ONTAP locali che dagli archivi di oggetti basati sul cloud.

Il caso d'uso presentato in questa documentazione si concentra su tecnologie di protezione dei dati comprovate che evidenziano l'integrazione tra NetApp, VMware e i principali provider cloud. Il SnapCenter Plug-in for VMware vSphere garantisce un'integrazione perfetta con VMware vSphere, consentendo una gestione efficiente e centralizzata delle operazioni di protezione dei dati. Questa integrazione semplifica i processi di backup e ripristino per le macchine virtuali, consentendo operazioni di pianificazione, monitoraggio e ripristino flessibili all'interno dell'ecosistema VMware. Il BlueXP backup and recovery per macchine virtuali forniscono l'uno (1) in 3-2-1 fornendo backup sicuri e air-gapped dei dati delle macchine virtuali su un archivio di oggetti basato su cloud. L'interfaccia intuitiva e il flusso di lavoro logico forniscono una piattaforma sicura per l'archiviazione a lungo termine dei dati critici.

Informazioni aggiuntive

Per saperne di più sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Documentazione SnapCenter Plug-in for VMware vSphere"
- "Documentazione BlueXP"

Impostare il ripristino di emergenza per i datastore VMFS utilizzando il BlueXP disaster recovery

In questo caso d'uso descriviamo la procedura per impostare il disaster recovery

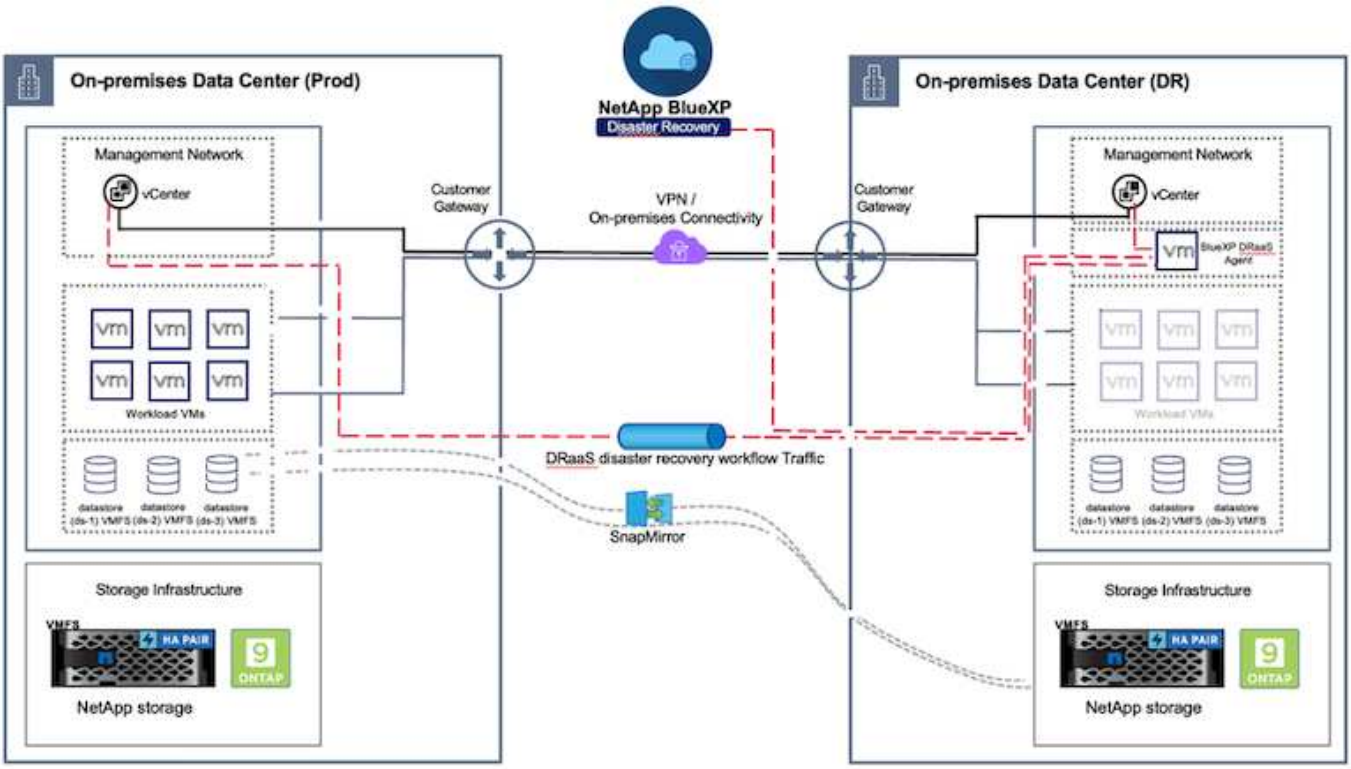
utilizzando BlueXP disaster recovery per le VM VMware on-premise che utilizzano datastore VMware Virtual Machine File System (VMFS). Questa procedura include la configurazione dell'account e del connettore BlueXP , la definizione della replica SnapMirror tra i sistemi ONTAP , l'integrazione con VMware vCenter e l'automazione delle operazioni di failover e failback.

Il disaster recovery mediante replica a livello di blocco dal sito di produzione al sito di disaster recovery è un modo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Con la replica NetApp SnapMirror , i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali che utilizzano datastore VMFS possono essere replicati su un altro sistema di storage ONTAP in un data center di ripristino designato in cui risiede VMware

Introduzione

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per impostare il disaster recovery per le VM VMware on-premise su un altro sito designato. Come parte di questa configurazione, l'account BlueXP , il connettore BlueXP e gli array ONTAP sono stati aggiunti all'interno dell'area di lavoro BlueXP , necessari per abilitare la comunicazione da VMware vCenter allo storage ONTAP . Inoltre, questo documento spiega nel dettaglio come configurare la replica tra siti e come impostare e testare un piano di ripristino. L'ultima sezione contiene istruzioni su come eseguire un failover completo del sito e su come effettuare il failback quando il sito primario viene ripristinato e acquistato online.

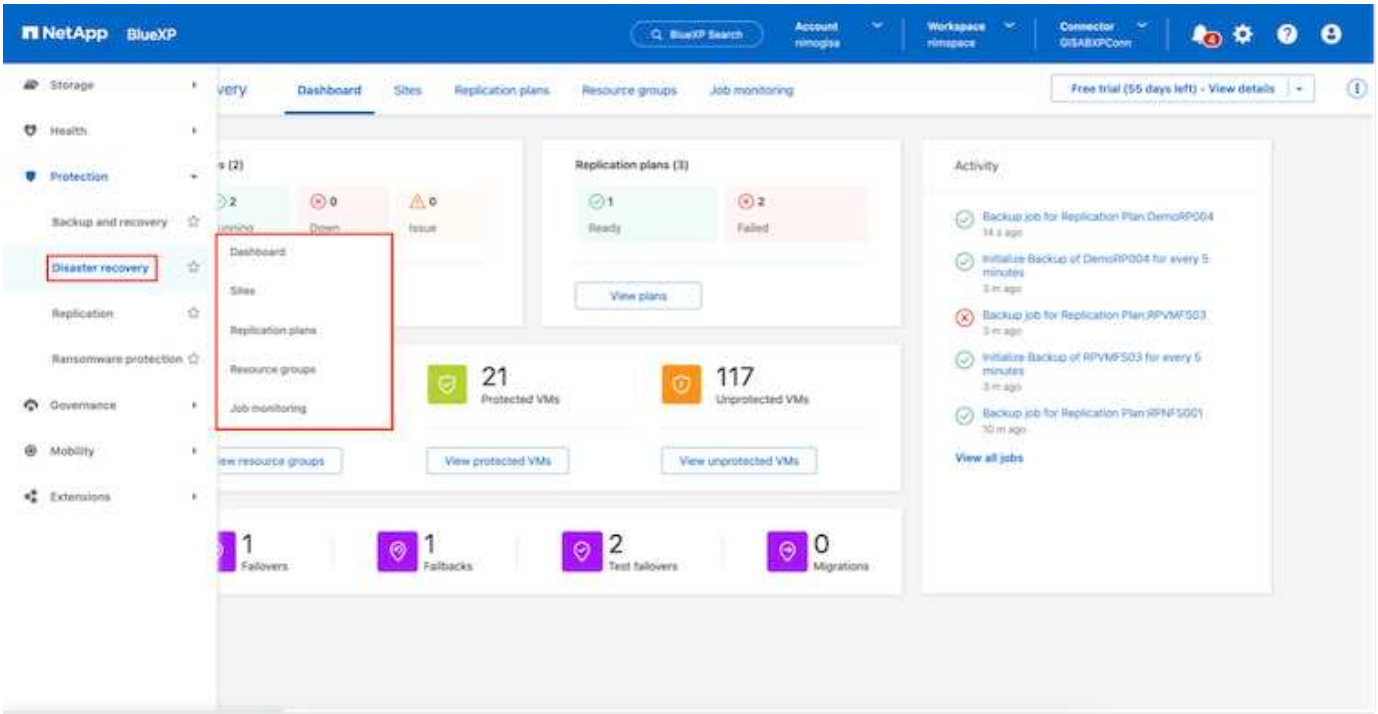
Utilizzando il servizio BlueXP disaster recovery , integrato nella console NetApp BlueXP , i clienti possono scoprire i propri VMware vCenter on-premise insieme allo storage ONTAP , creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e testare o eseguire failover e failback. SnapMirror fornisce la replicazione a blocchi a livello di storage per mantenere i due siti aggiornati con modifiche incrementali, con un RPO fino a 5 minuti. È anche possibile simulare le procedure DR come un'esercitazione regolare senza influire sulla produzione e sui datastore replicati o incorrere in costi di archiviazione aggiuntivi. Il BlueXP disaster recovery sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore VMFS dall'ultimo snapshot replicato sul sito DR. Una volta completato il test DR, i clienti possono semplicemente eliminare l'ambiente di test, sempre senza alcun impatto sulle risorse di produzione effettivamente replicate. Quando si verifica la necessità (pianificata o meno) di un failover effettivo, con pochi clic il servizio BlueXP disaster recovery organizzerà tutti i passaggi necessari per ripristinare automaticamente le macchine virtuali protette sul sito di disaster recovery designato. Il servizio invertirà anche la relazione SnapMirror con il sito primario e replicherà eventuali modifiche dal secondario al primario per un'operazione di failback, quando necessario. Tutto ciò può essere ottenuto con una frazione del costo rispetto ad altre alternative note.



Iniziare

Per iniziare a utilizzare il BlueXP disaster recovery, utilizzare la console BlueXP e quindi accedere al servizio.

1. Accedi a BlueXP.
2. Dal menu di navigazione a sinistra BlueXP , seleziona Protezione > Ripristino di emergenza.
3. Viene visualizzata la Dashboard BlueXP disaster recovery .

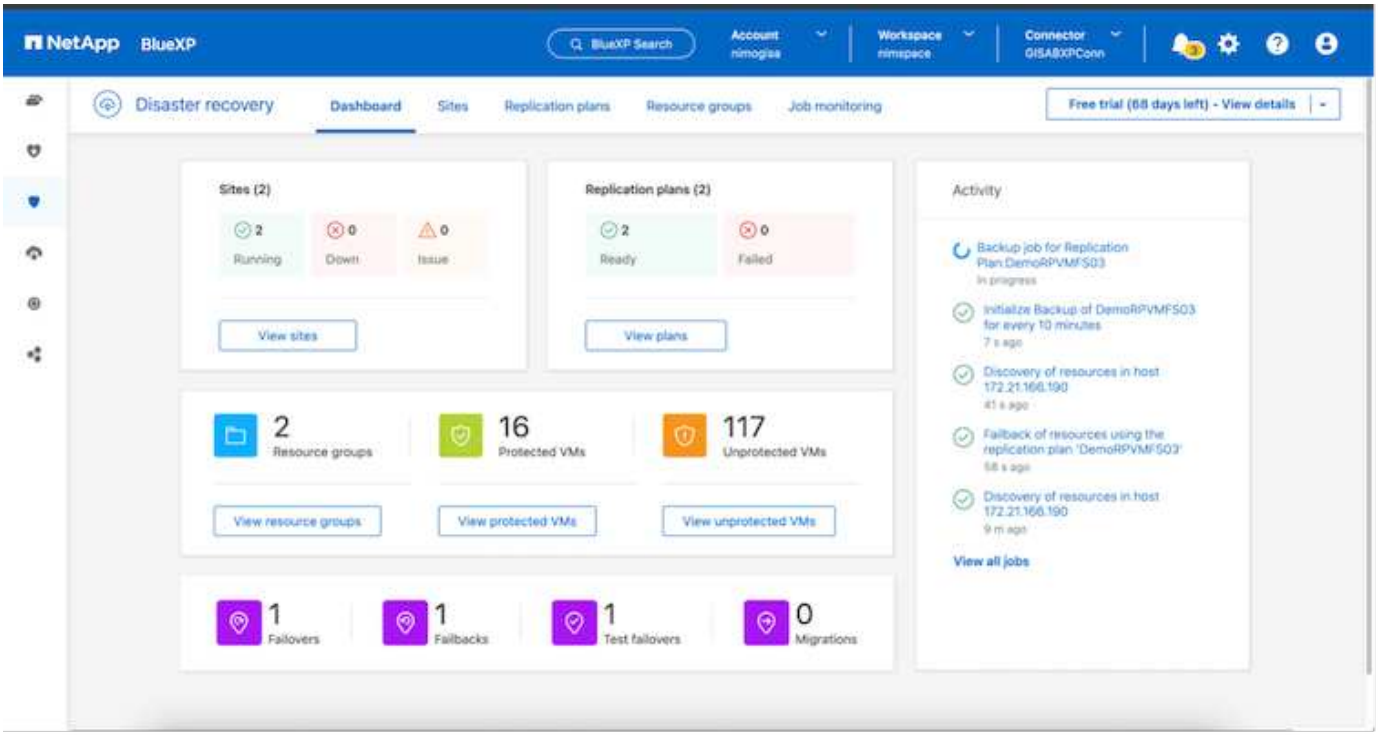


Prima di configurare il piano di disaster recovery, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è configurato in NetApp BlueXP. Il connettore deve essere distribuito in AWS VPC.
- Le istanze del connettore BlueXP dispongono di connettività con i sistemi di archiviazione e vCenter di origine e di destinazione.
- In BlueXP sono stati aggiunti sistemi di storage NetApp on-premise che ospitano datastore VMFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su VMFS designati.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere dai 3 ai 5 minuti.

NetApp consiglia di distribuire il connettore BlueXP nel sito di disaster recovery o in un terzo sito, in modo che il connettore BlueXP possa comunicare tramite la rete con le risorse di origine e di destinazione durante interruzioni reali o calamità naturali.

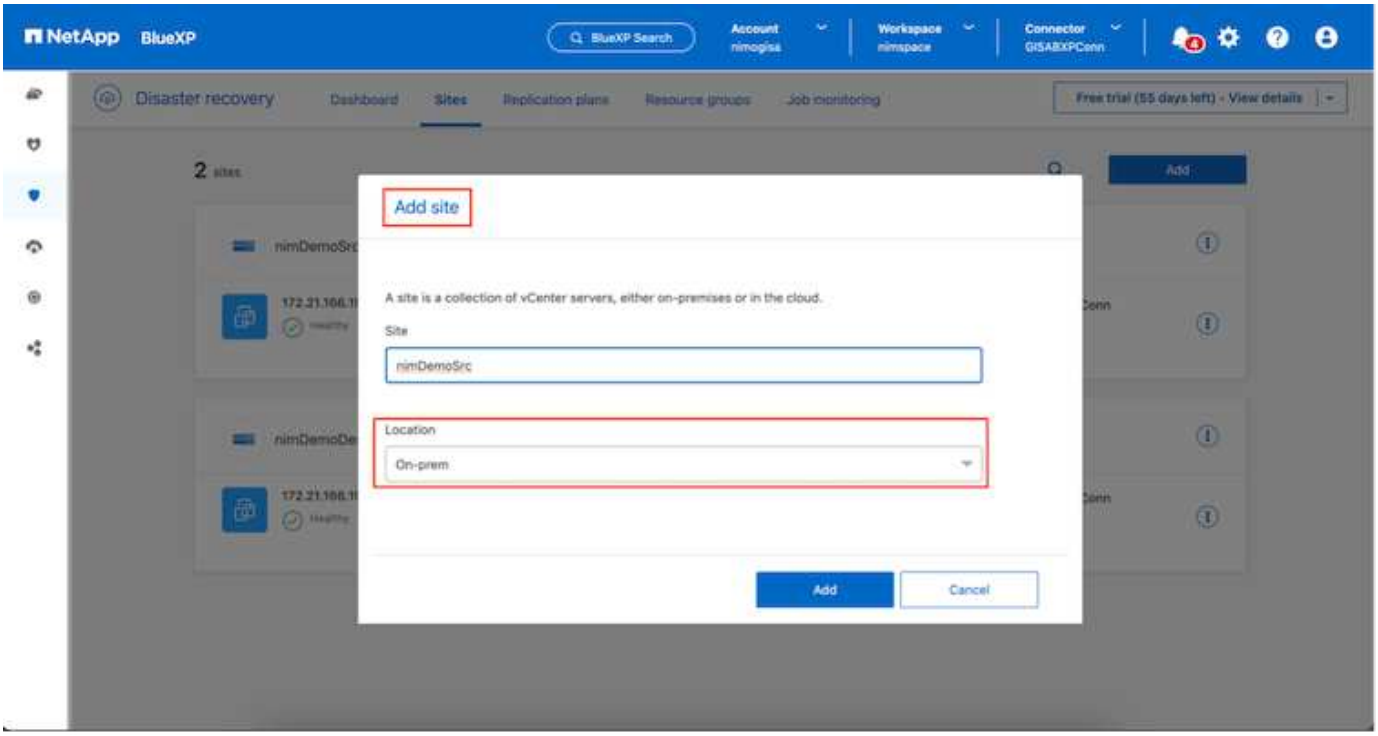


Al momento della stesura di questo documento, il supporto per i datastore VMFS da locale a locale è in fase di anteprima tecnologica. Questa funzionalità è supportata sia con i datastore VMFS basati sul protocollo FC che ISCSI.

Configurazione BlueXP disaster recovery

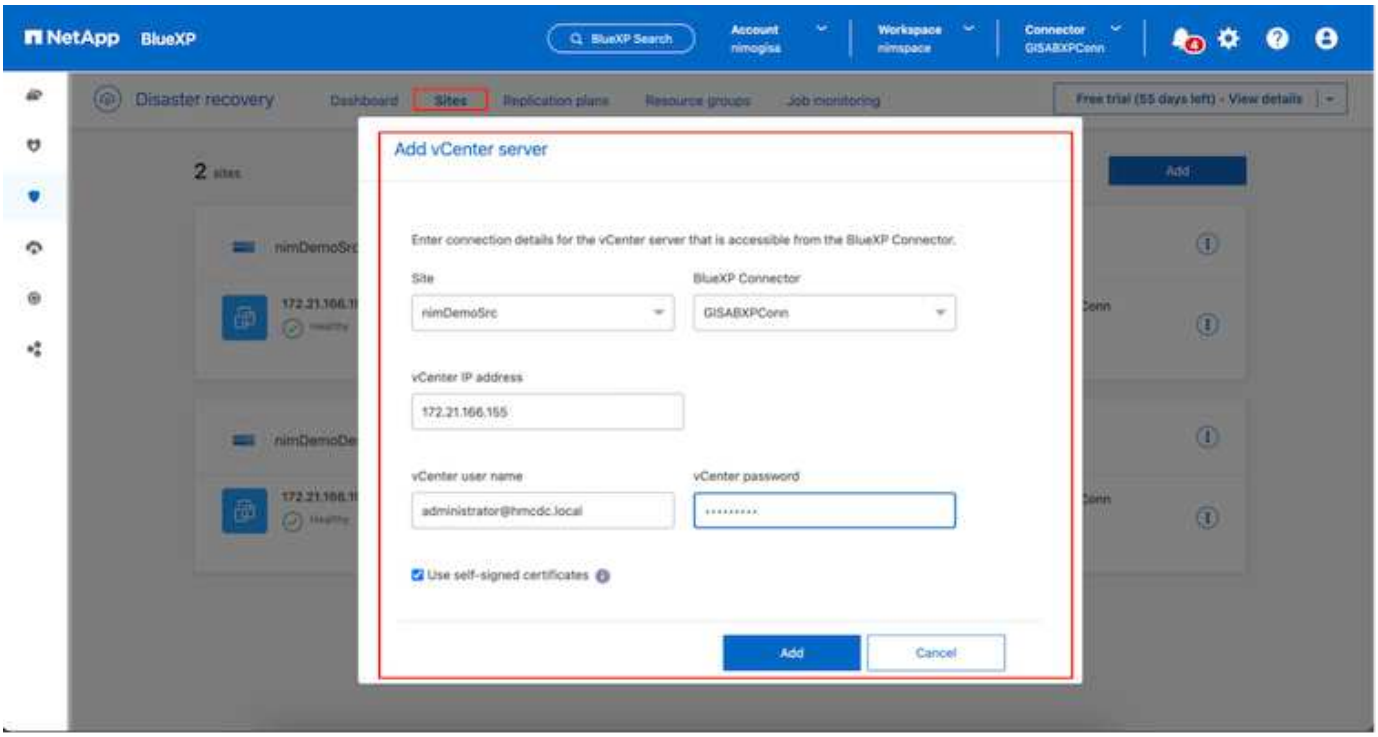
Il primo passo per prepararsi al disaster recovery è individuare e aggiungere le risorse di archiviazione e vCenter locali al BlueXP disaster recovery.

Assicurarsi che i sistemi di archiviazione ONTAP siano aggiunti all'ambiente di lavoro all'interno della tela. Aprire la console BlueXP e selezionare **Protezione > Ripristino di emergenza** dal menu di navigazione a sinistra. Selezionare **Scopri server vCenter** oppure utilizzare il menu in alto, selezionare **Siti > Aggiungi > Aggiungi vCenter**.

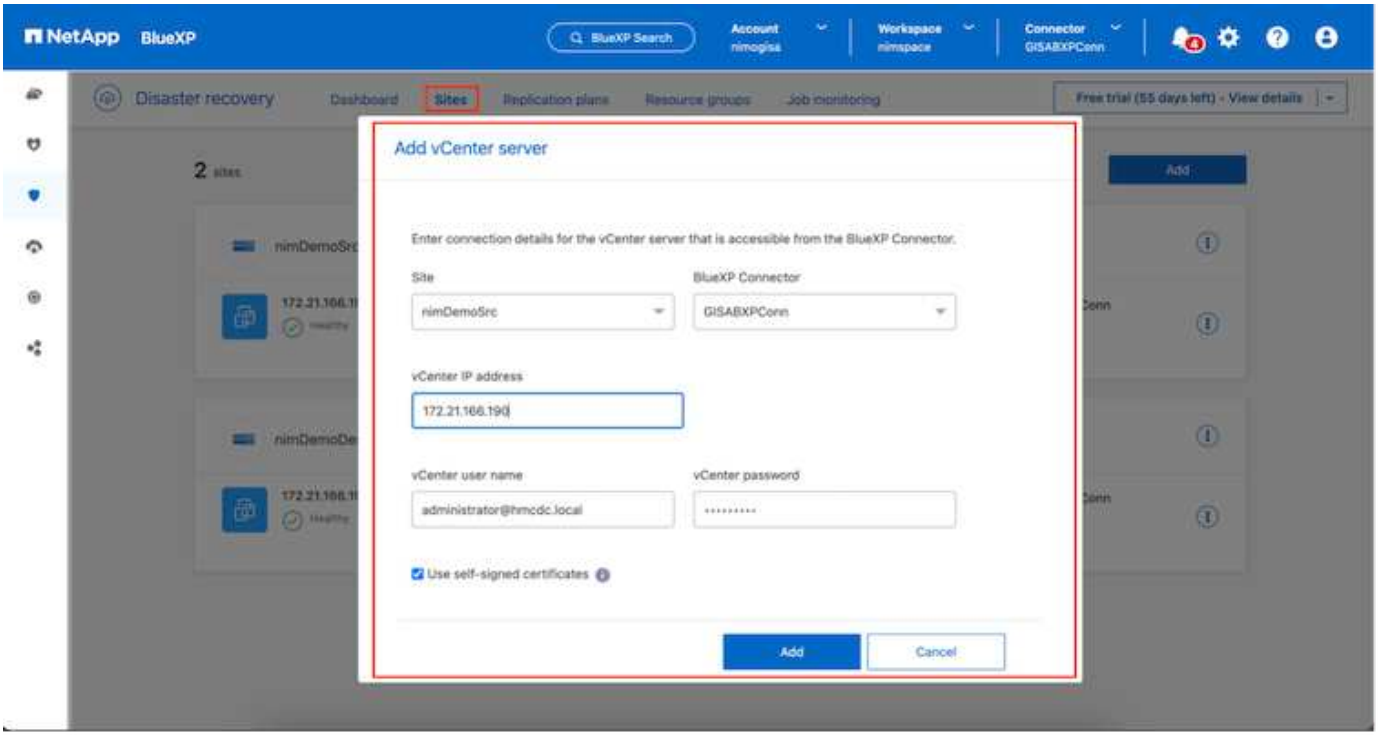


Aggiungere le seguenti piattaforme:

- **Fonte**. vCenter locale.



- **Destinazione**. VMC SDDC vCenter.



Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra il sito di origine e quello di destinazione

SnapMirror utilizza gli snapshot ONTAP per gestire il trasferimento dei dati da una posizione all'altra. Inizialmente, una copia completa basata su uno snapshot del volume di origine viene copiata sulla destinazione per eseguire una sincronizzazione di base. Quando si verificano modifiche ai dati all'origine, viene creato un nuovo snapshot e confrontato con lo snapshot di base. I blocchi che risultano modificati vengono quindi replicati nella destinazione, con lo snapshot più recente che diventa la baseline corrente o lo snapshot comune più recente. Ciò consente di ripetere il processo e di inviare aggiornamenti incrementali alla destinazione.

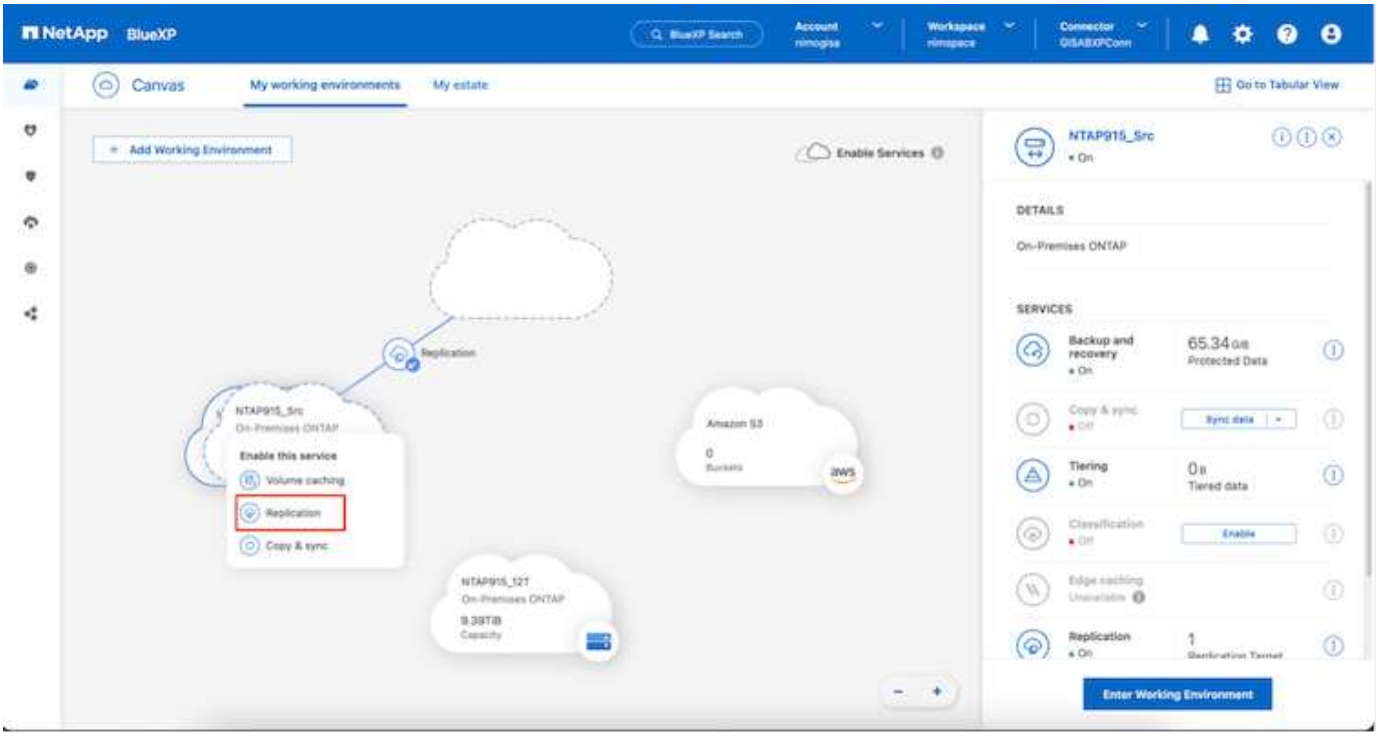
Una volta stabilita una relazione SnapMirror , il volume di destinazione è in uno stato di sola lettura online e quindi è ancora accessibile. SnapMirror funziona con blocchi fisici di archiviazione, anziché a livello di file o altro livello logico. Ciò significa che il volume di destinazione è una replica identica del volume di origine, inclusi snapshot, impostazioni del volume, ecc. Se il volume di origine utilizza funzionalità di efficienza dello spazio ONTAP , come la compressione dei dati e la deduplicazione dei dati, il volume replicato manterrà queste ottimizzazioni.

L'interruzione della relazione SnapMirror rende il volume di destinazione scrivibile e in genere viene utilizzato per eseguire un failover quando SnapMirror viene utilizzato per sincronizzare i dati in un ambiente DR. SnapMirror è sufficientemente sofisticato da consentire la risincronizzazione efficiente dei dati modificati nel sito di failover con il sistema primario, qualora questo dovesse tornare online in seguito, e quindi consentire il ripristino della relazione SnapMirror originale.

Come configurarlo per VMware Disaster Recovery

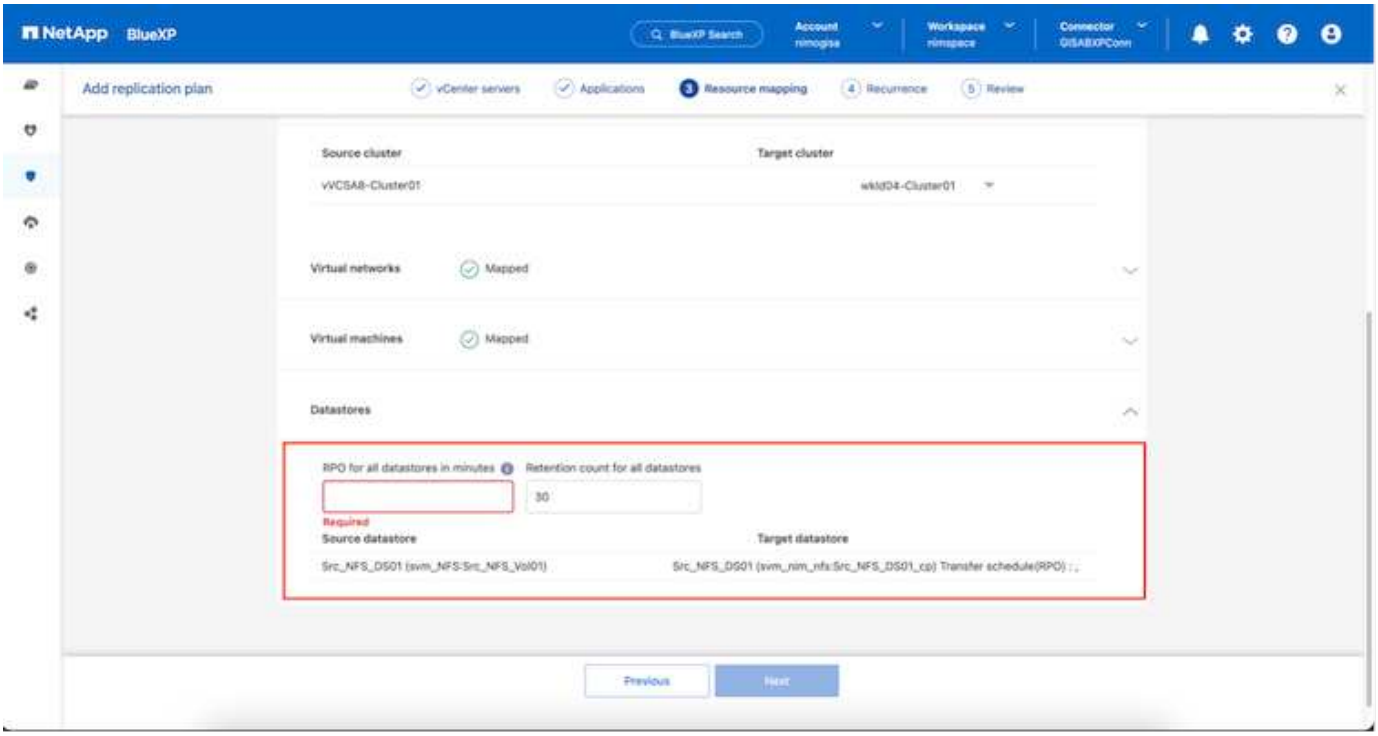
Il processo per creare una replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è sfruttare BlueXP per configurare la replica SnapMirror , utilizzando un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione per

avviare la procedura guidata che guida attraverso il resto del processo.



BlueXP DRaaS può anche automatizzare la stessa operazione, a condizione che siano soddisfatti i due criteri seguenti:

- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.

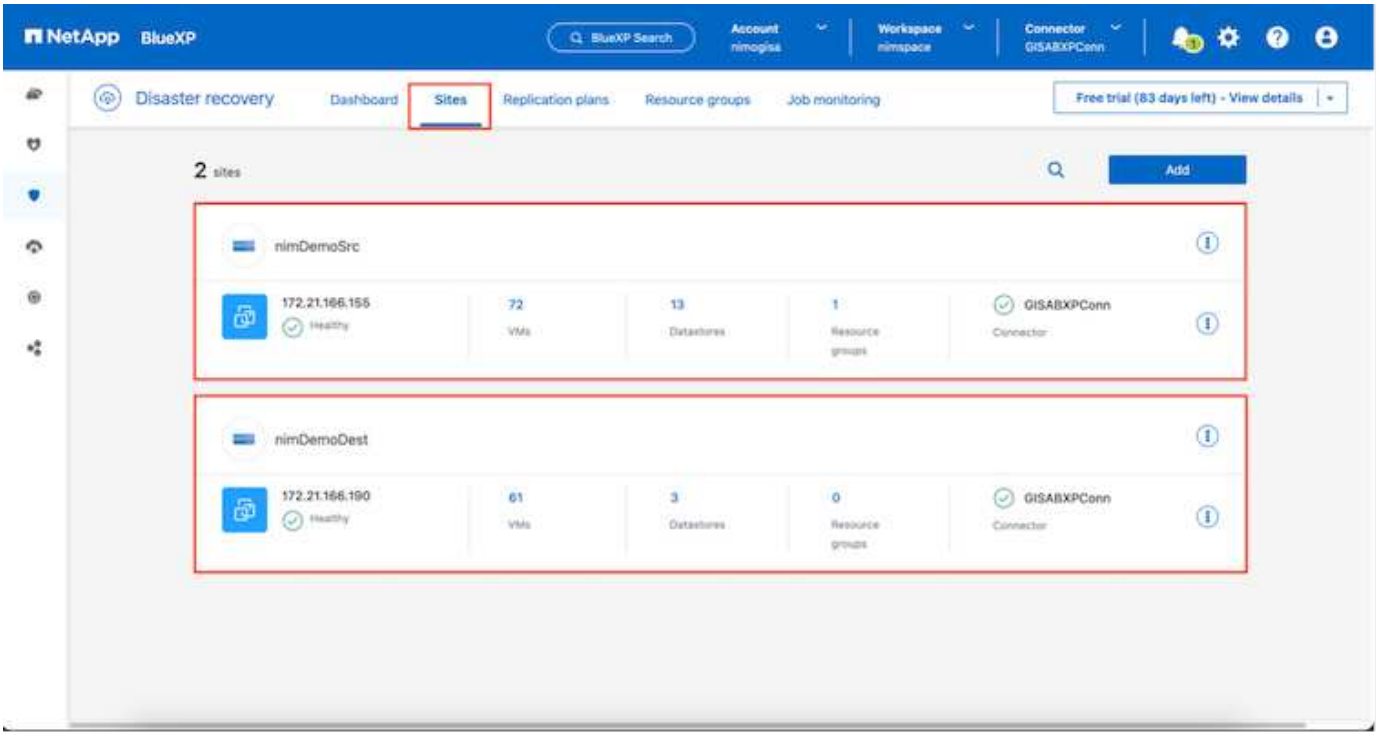


Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.

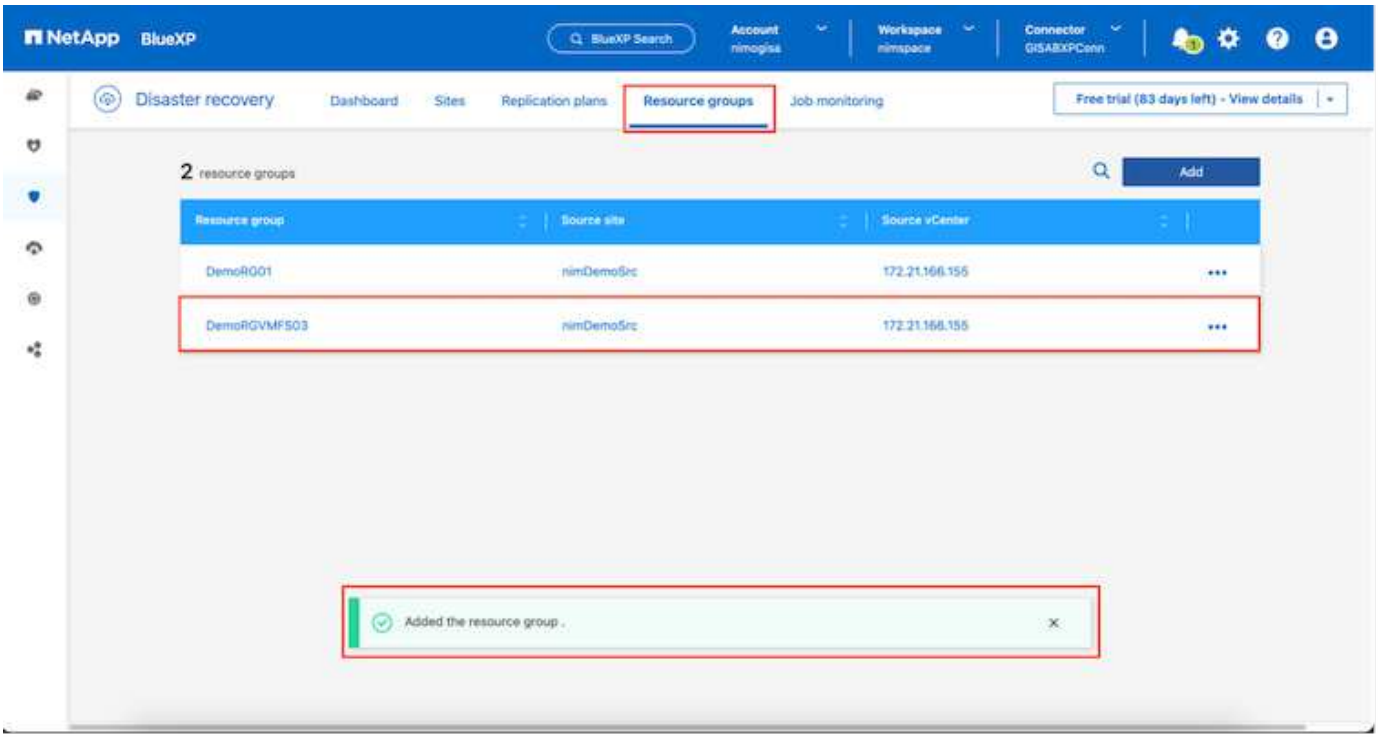
Oltre agli approcci sopra descritti, la replica SnapMirror può essere creata anche tramite ONTAP CLI o System Manager. Indipendentemente dall'approccio utilizzato per sincronizzare i dati tramite SnapMirror, BlueXP DRaaS orchestra il flusso di lavoro per operazioni di disaster recovery efficienti e senza interruzioni.

Cosa può fare per te il BlueXP disaster recovery ?

Dopo aver aggiunto i siti di origine e di destinazione, il BlueXP disaster recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. Il BlueXP disaster recovery rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle VM e li popola.

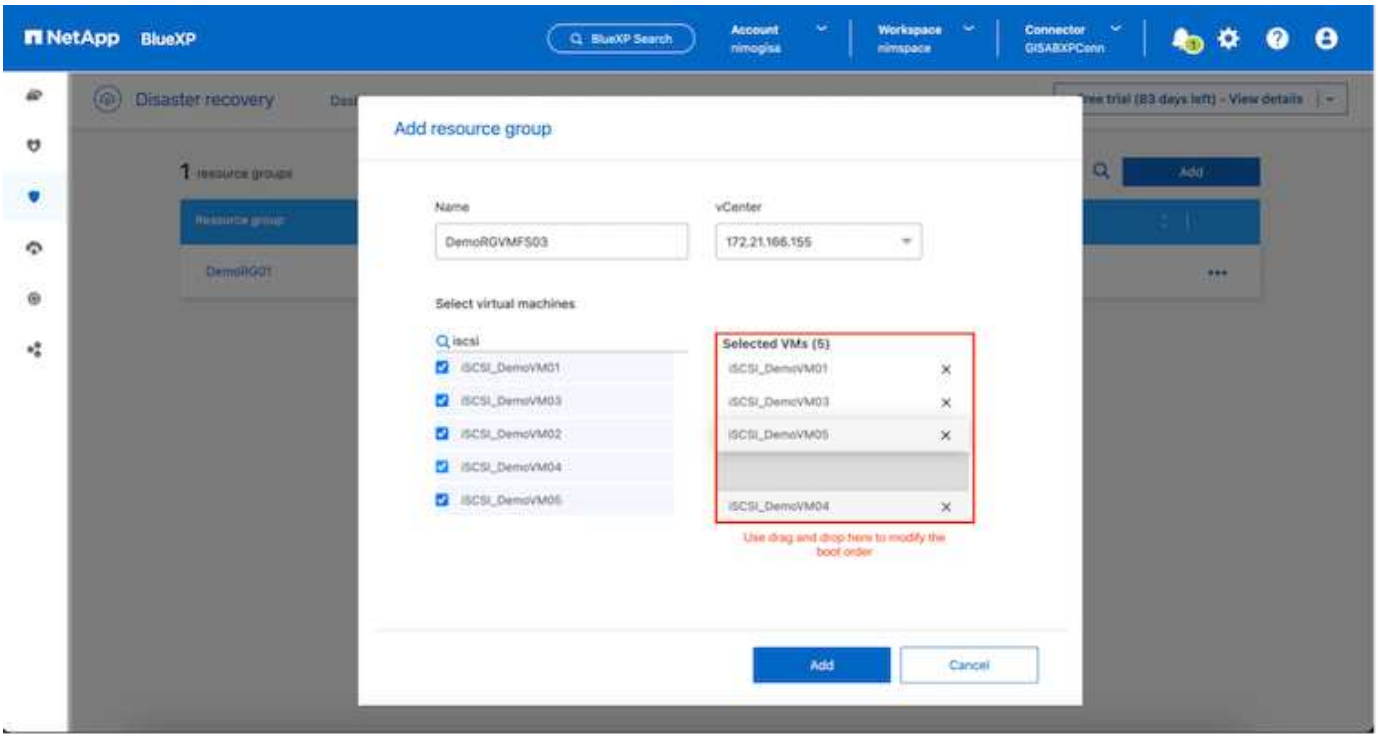


Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse BlueXP disaster recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, vai su **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.

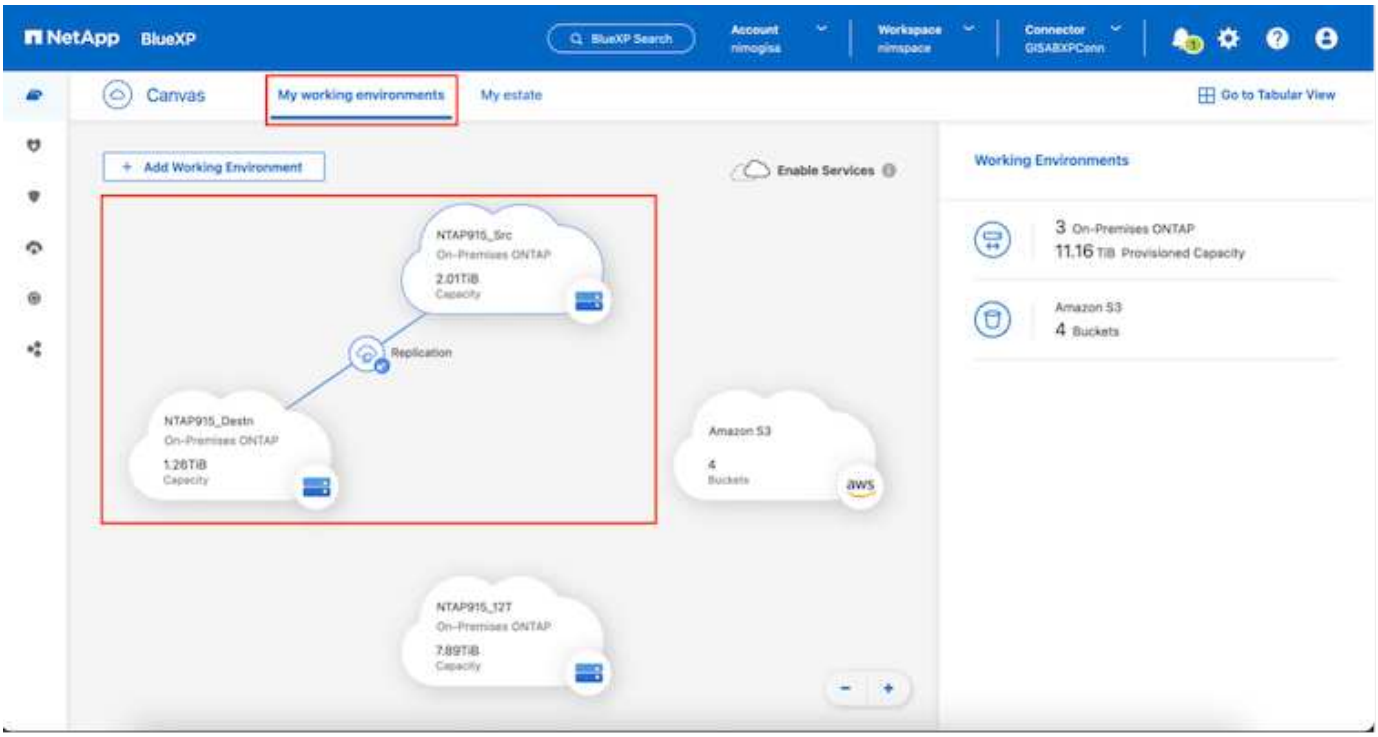


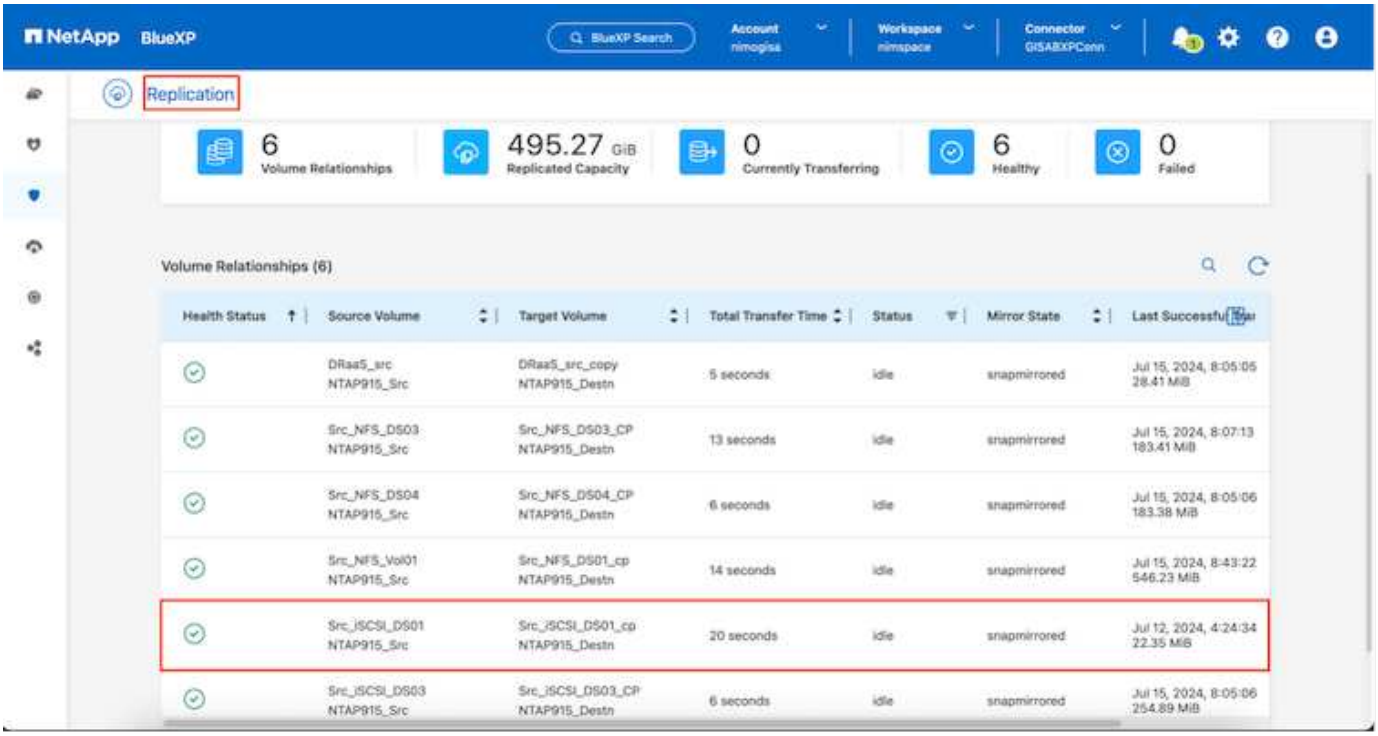
Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento della selezione.



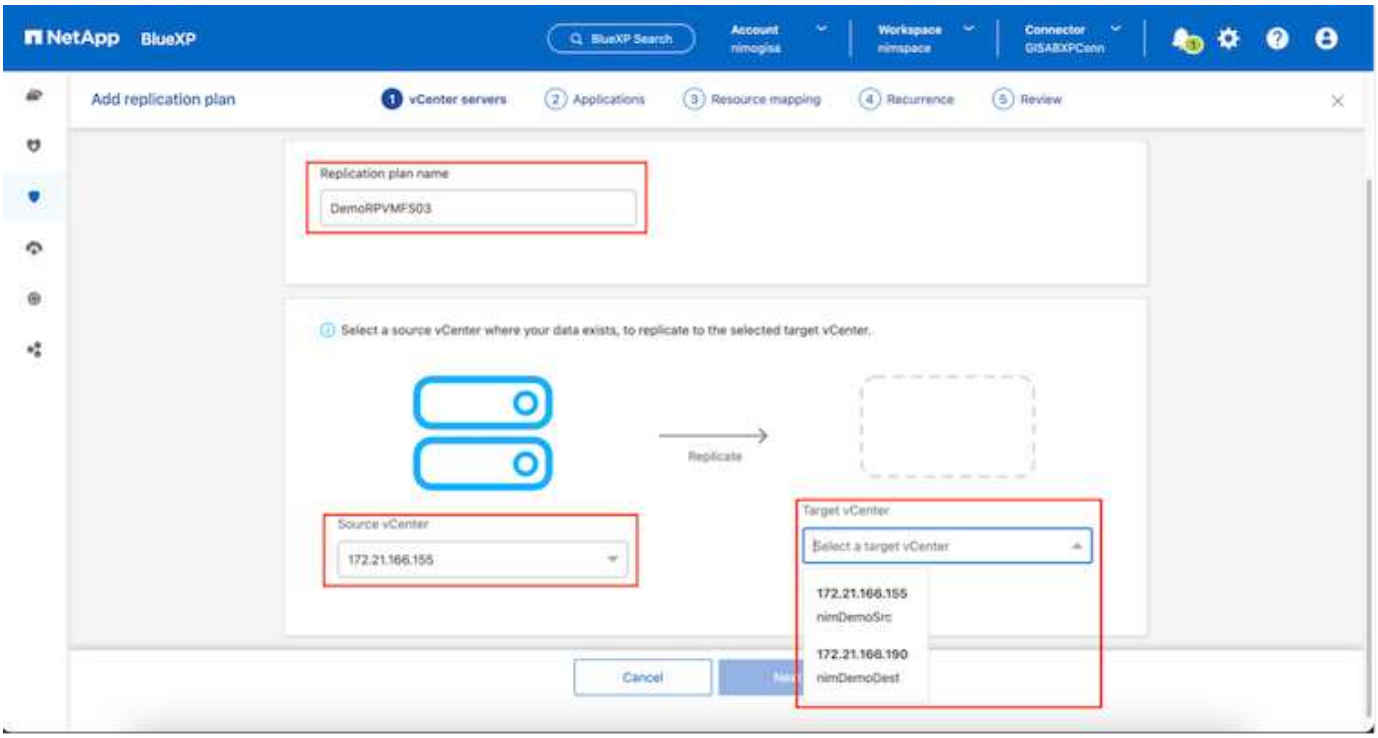
Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.



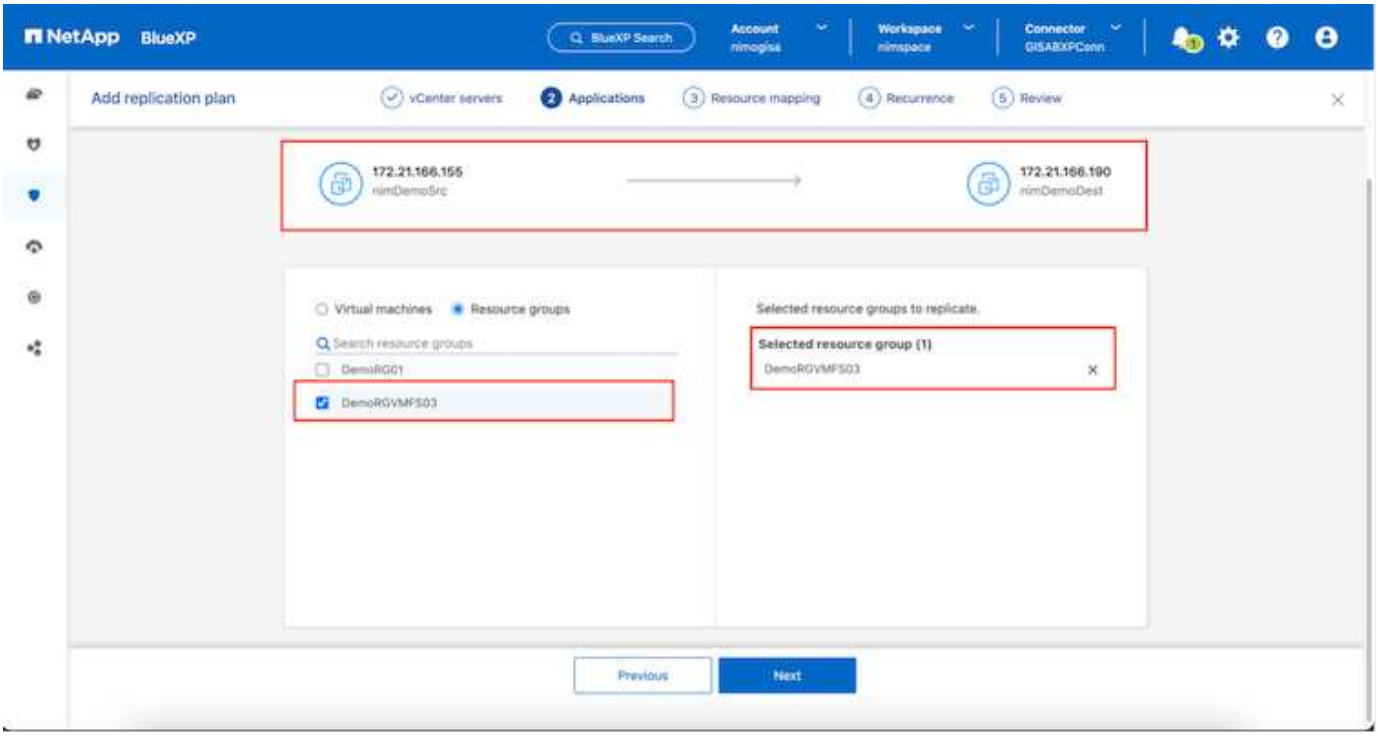


Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Aggiungi piano**.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



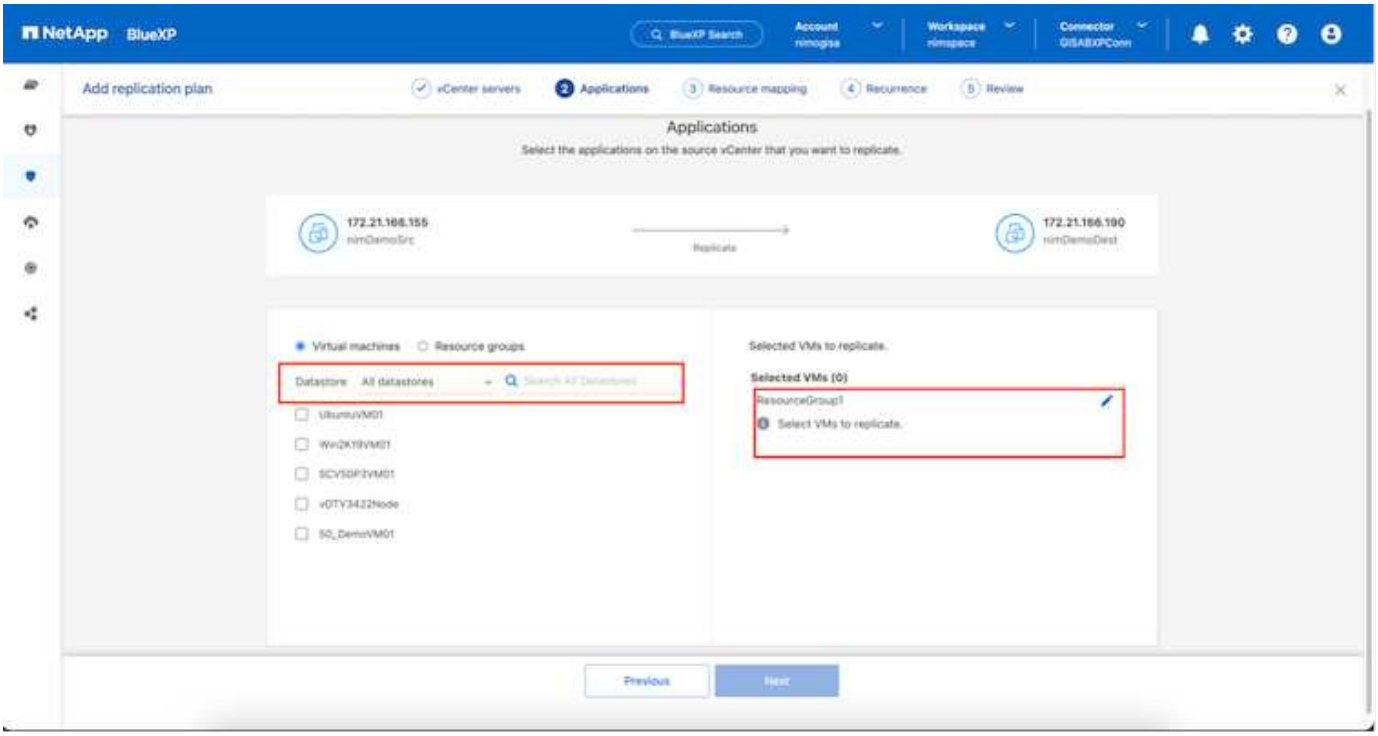
Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono essere ripristinate le macchine virtuali delle applicazioni.



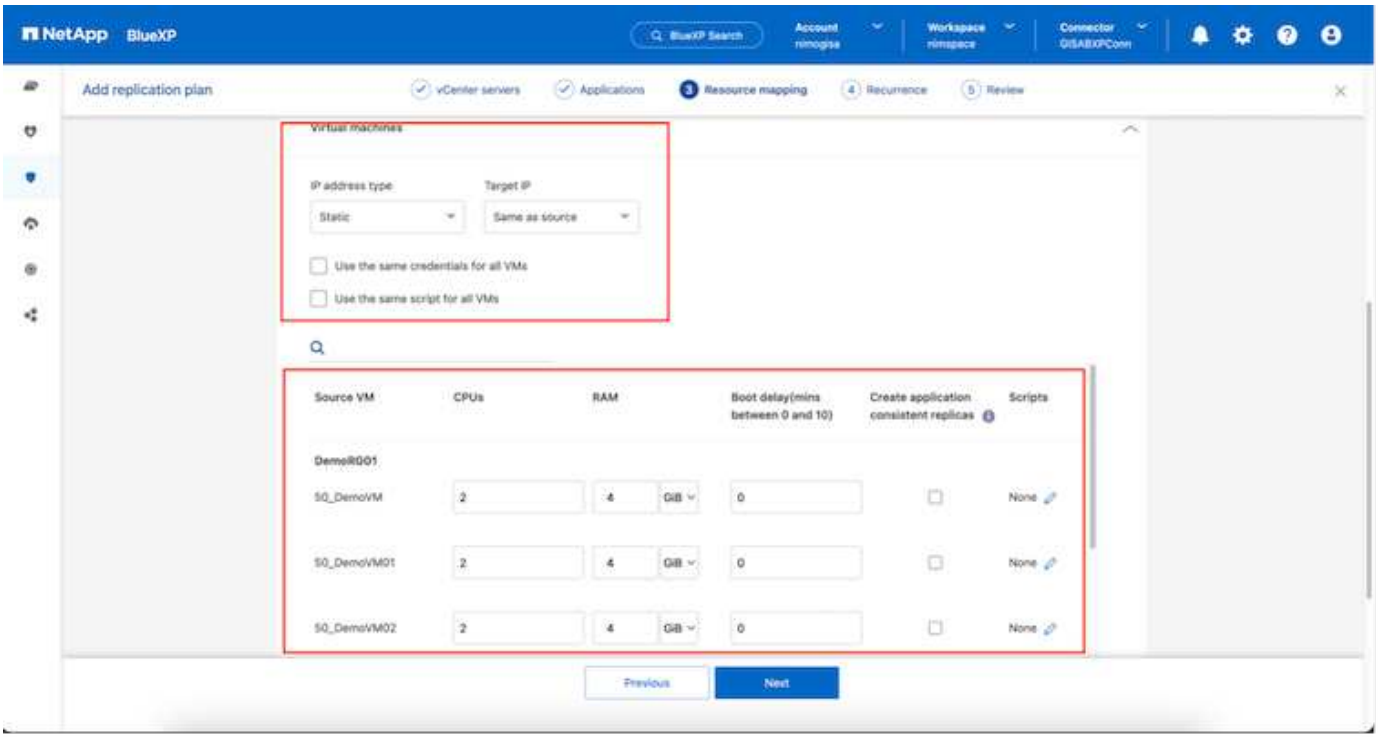
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Vengono avviati in parallelo due gruppi di risorse.

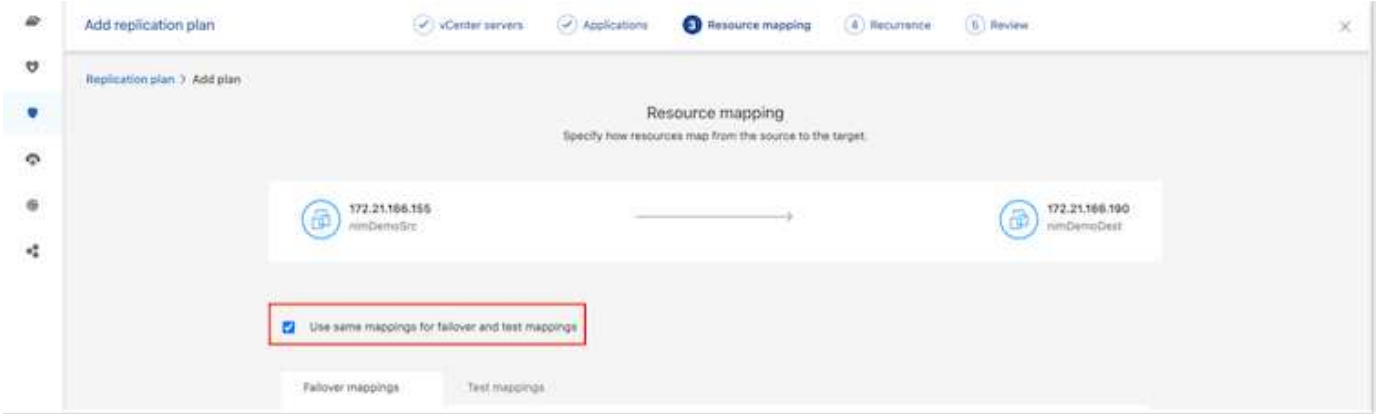
La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



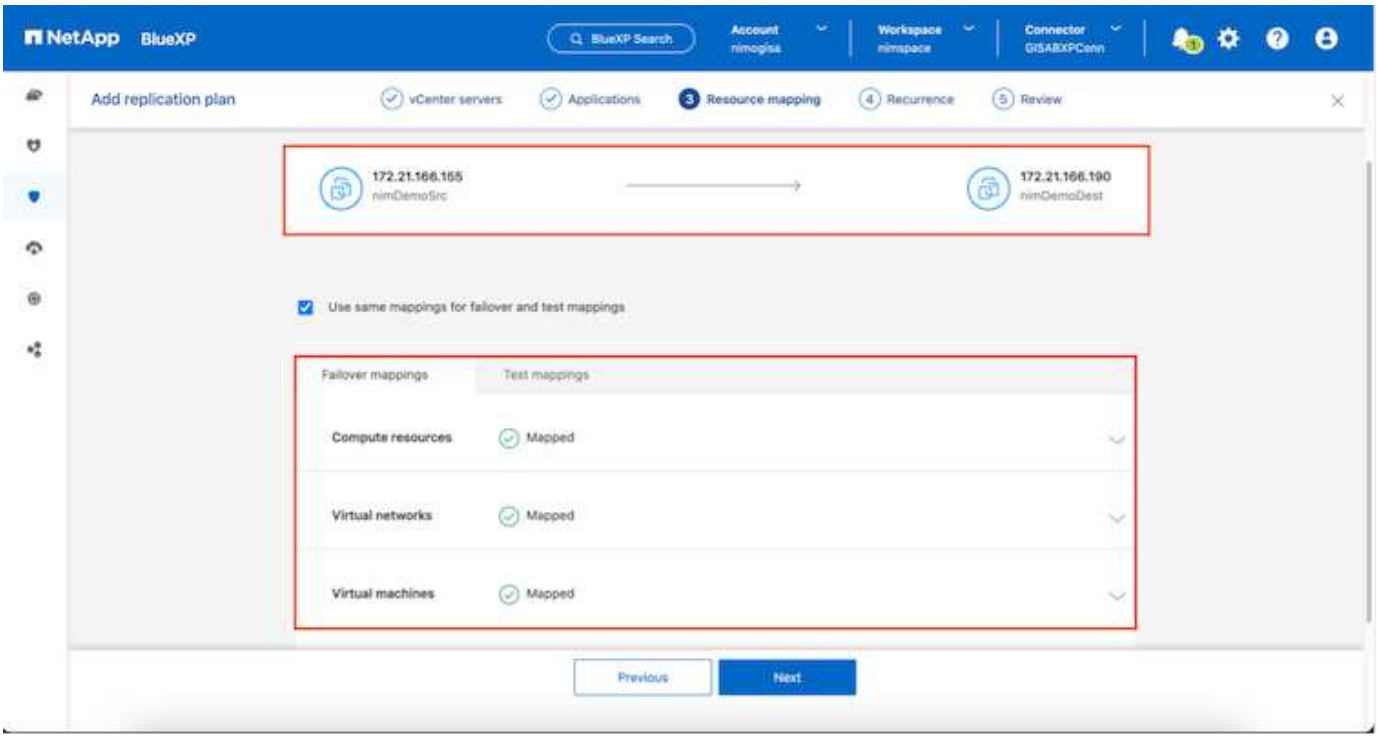
Una volta selezionati i gruppi di risorse, creare i mapping di failover. In questo passaggio, specificare come le risorse dall'ambiente di origine vengono mappate alla destinazione. Ciò include risorse di elaborazione e reti virtuali. Personalizzazione IP, pre- e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento a"Creare un piano di replicazione" .



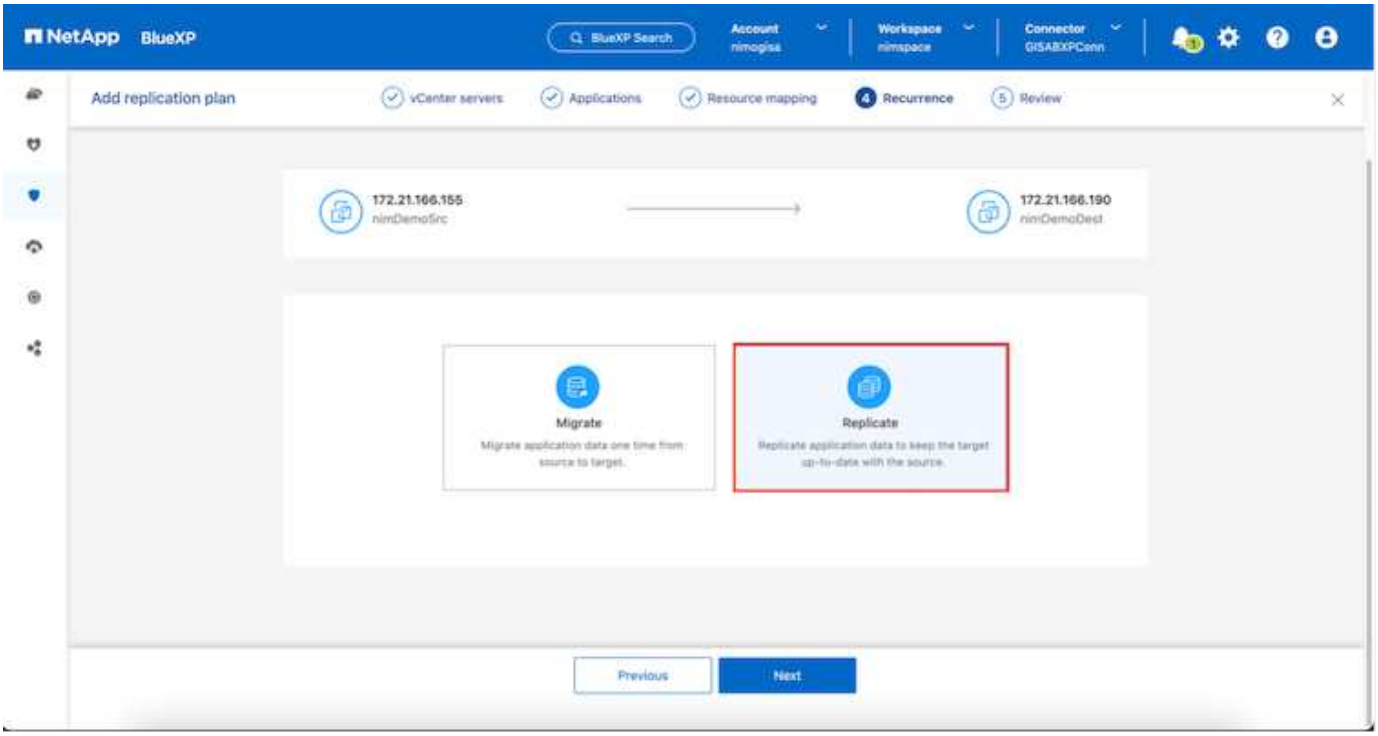
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per applicare mappature diverse per l'ambiente di test, selezionare l'opzione Mappatura test dopo aver deselezionato la casella di controllo come mostrato di seguito:



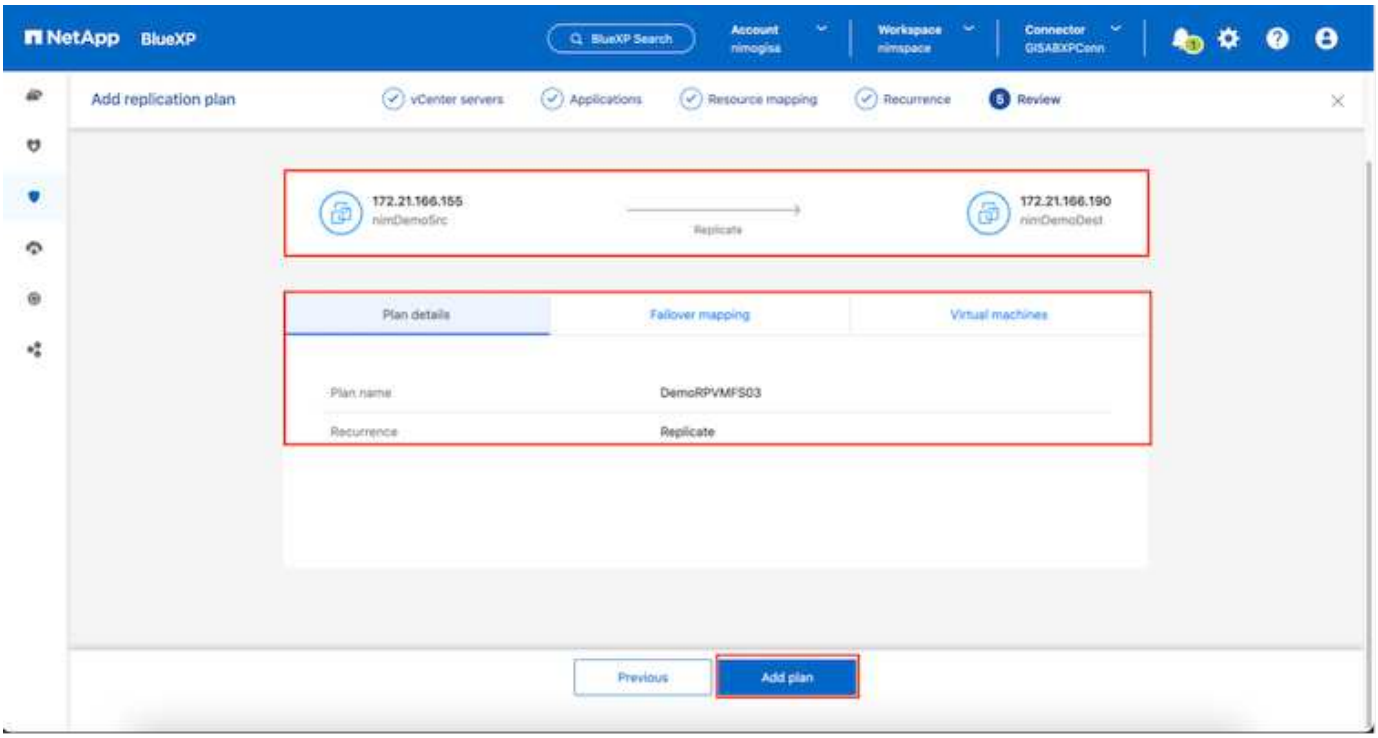
Una volta completata la mappatura delle risorse, fare clic su Avanti.

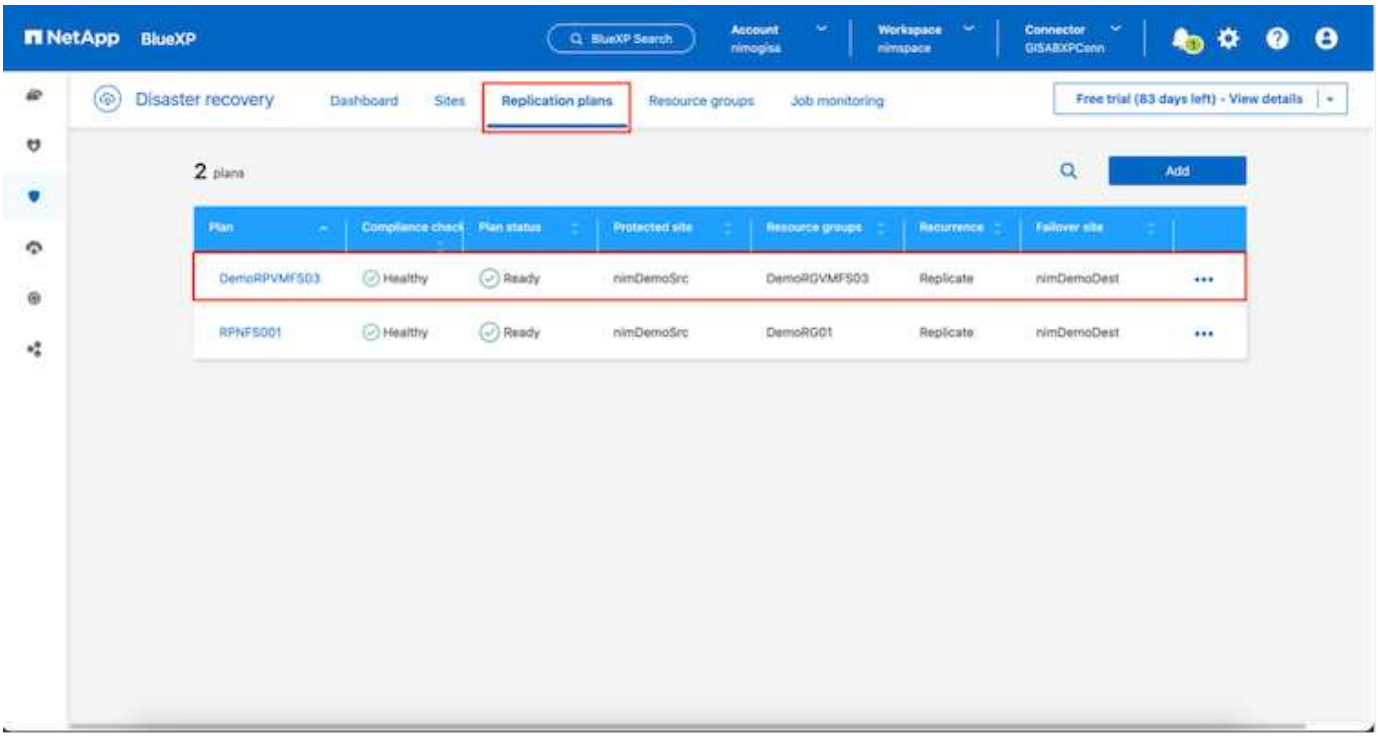


Selezionare il tipo di ricorrenza. In parole semplici, seleziona l'opzione Migra (migrazione una tantum tramite failover) o replica continua ricorrente. In questa procedura dettagliata è selezionata l'opzione Replica.

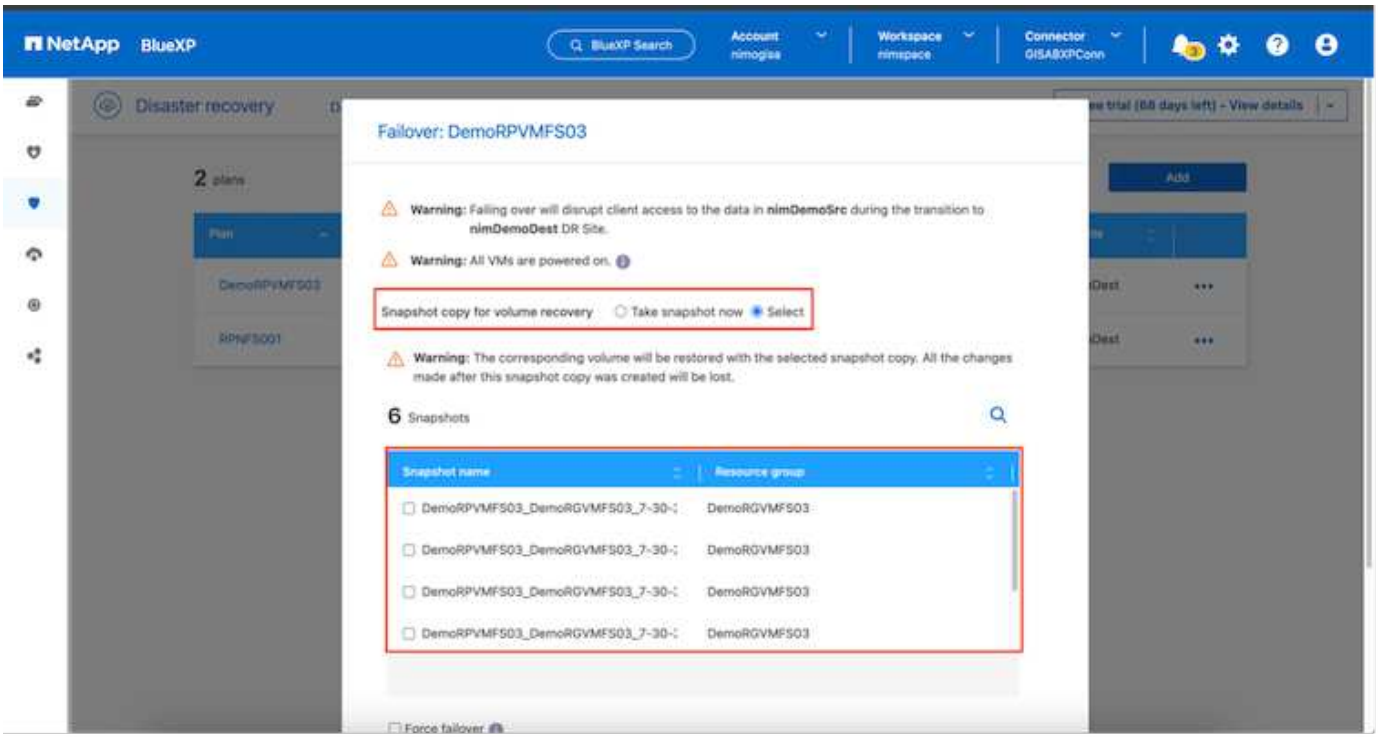


Una volta fatto, rivedi le mappature create e poi fai clic su Aggiungi piano.

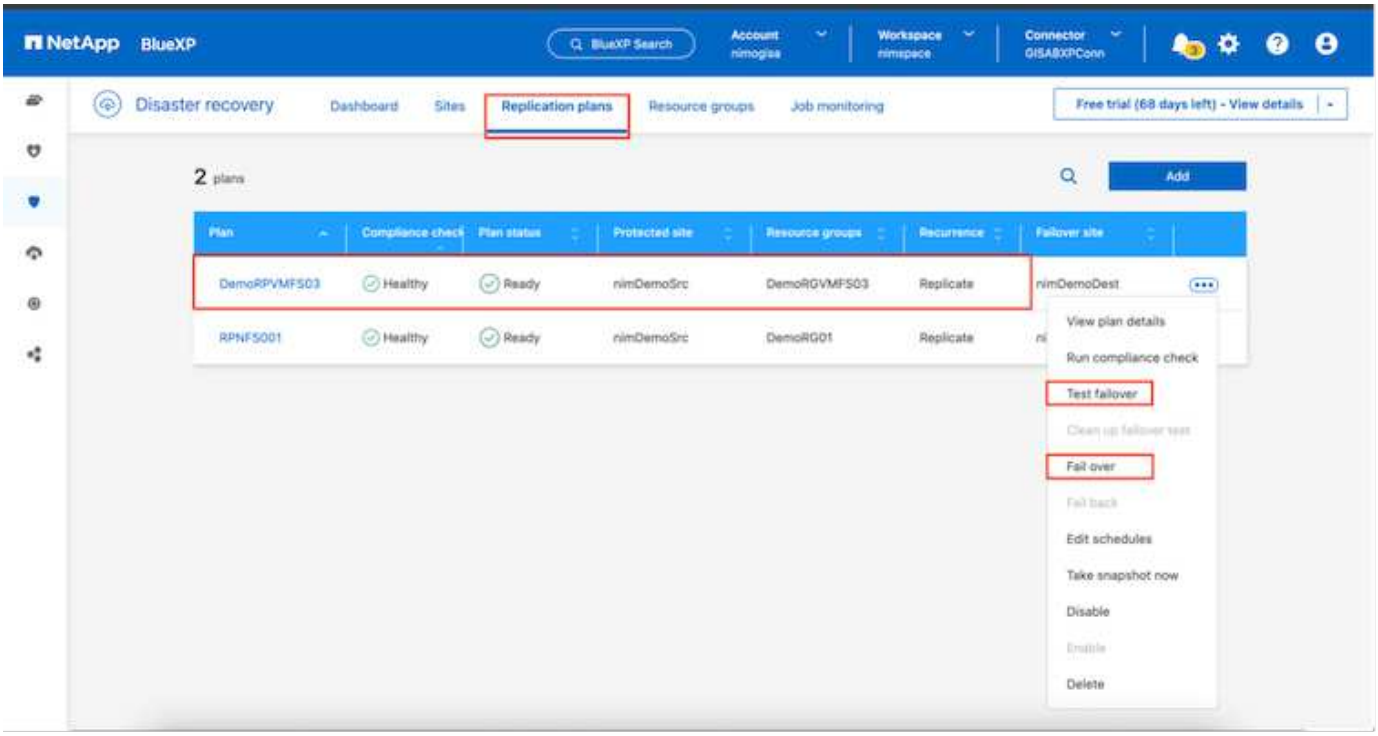




Una volta creato il piano di replicazione, è possibile eseguire il failover a seconda dei requisiti selezionando l'opzione failover, l'opzione test-failover o l'opzione migrate. Il BlueXP disaster recovery garantisce che il processo di replicazione venga eseguito secondo il piano ogni 30 minuti. Durante le opzioni di failover e test-failover, è possibile utilizzare la copia Snapshot SnapMirror più recente oppure selezionare una copia Snapshot specifica da una copia Snapshot di un determinato momento (in base ai criteri di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile in caso di un evento di corruzione come un ransomware, in cui le repliche più recenti sono già compromesse o crittografate. Il BlueXP disaster recovery mostra tutti i punti di ripristino disponibili.



Per attivare il failover o il failover di prova con la configurazione specificata nel piano di replica, fare clic su **Failover** o **Failover di prova**.

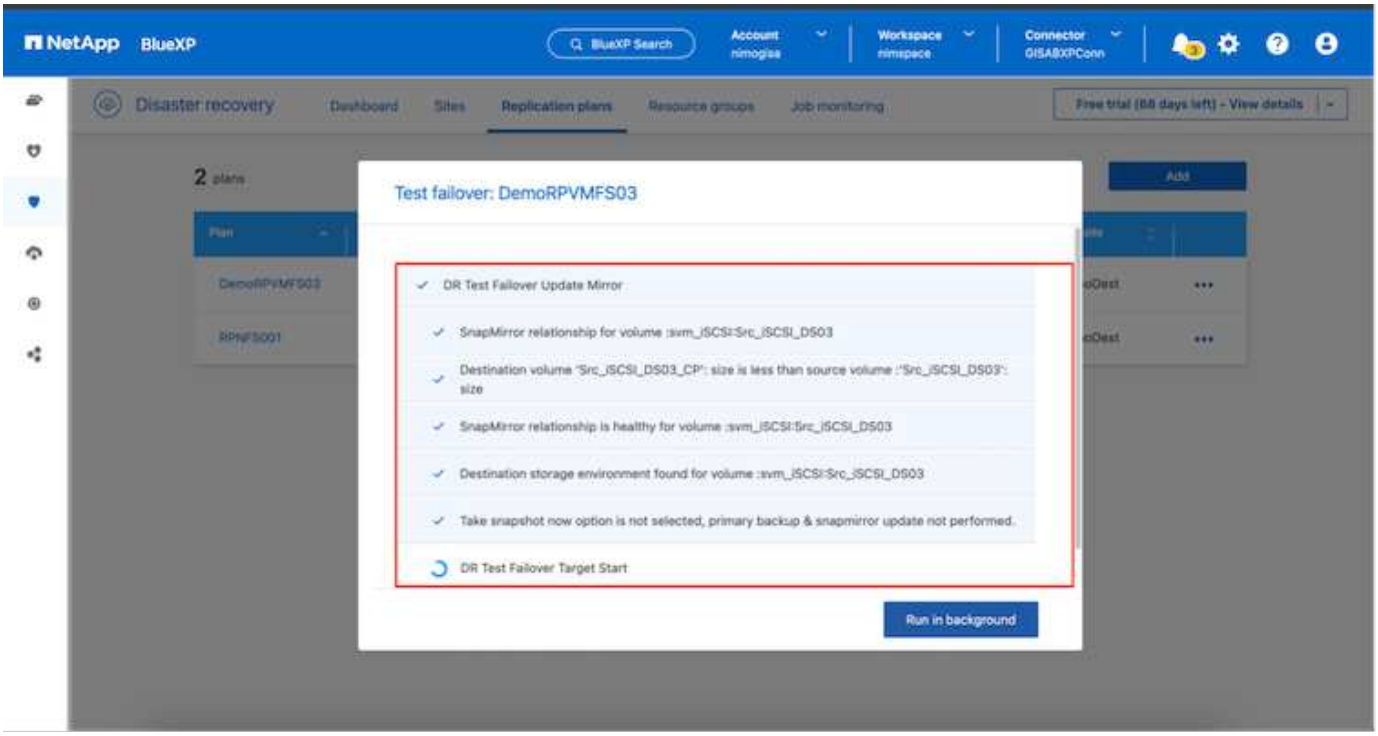


Cosa succede durante un’operazione di failover o di test failover?

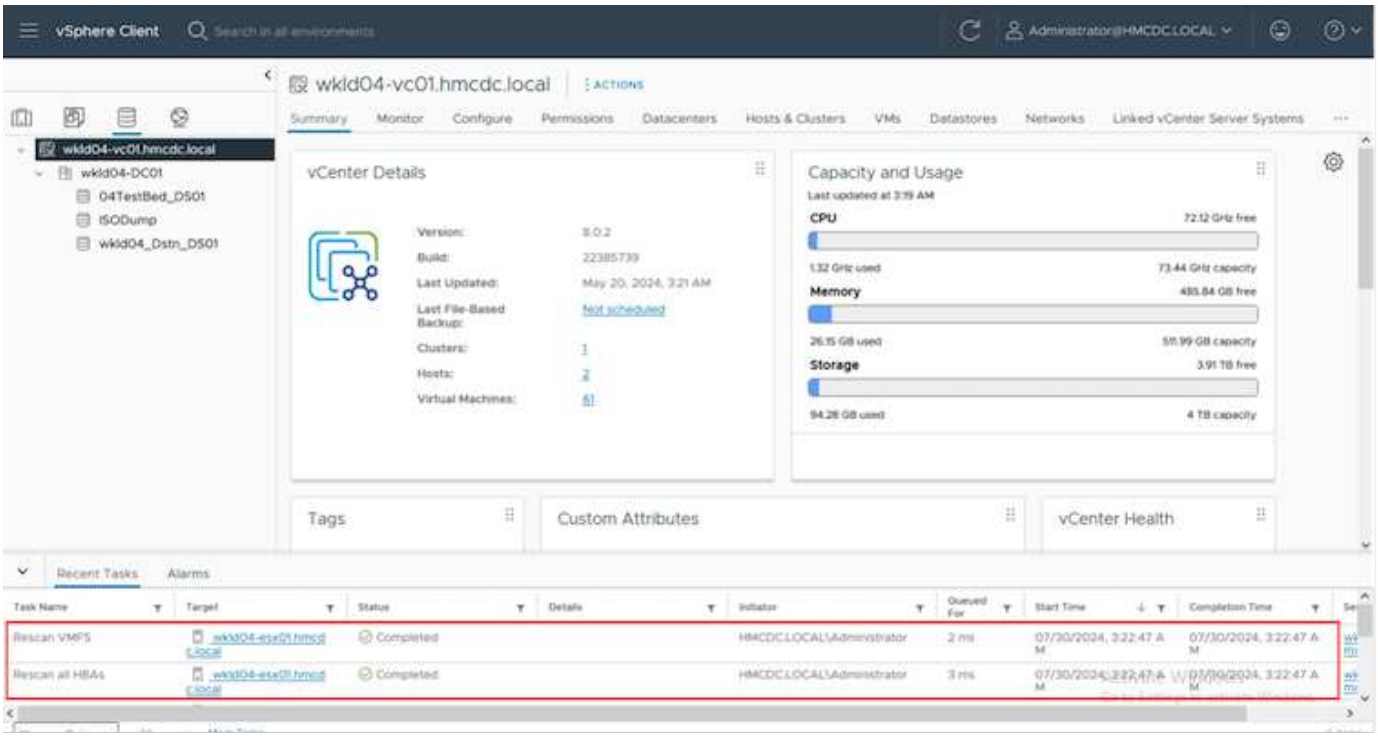
Durante un’operazione di failover di prova, il BlueXP disaster recovery crea un volume FlexClone sul sistema di archiviazione ONTAP di destinazione utilizzando la copia Snapshot più recente o uno snapshot selezionato del volume di destinazione.

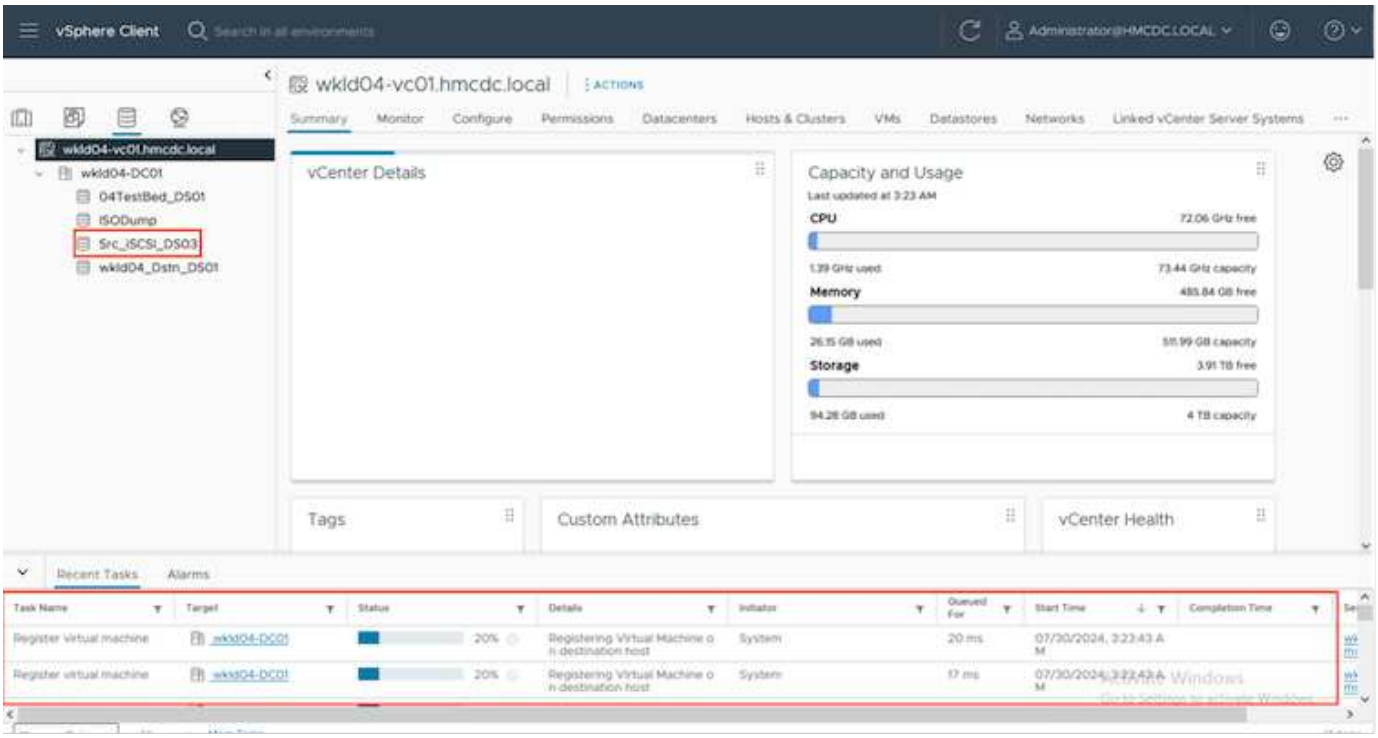
Un'operazione di failover di prova crea un volume clonato sul sistema di archiviazione ONTAP di destinazione.

L'esecuzione di un'operazione di ripristino di prova non influisce sulla replica SnapMirror .



Durante il processo, il BlueXP disaster recovery non mappa il volume di destinazione originale. Al contrario, crea un nuovo volume FlexClone dallo Snapshot selezionato e un datastore temporaneo che supporta il volume FlexClone viene mappato sugli host ESXi.

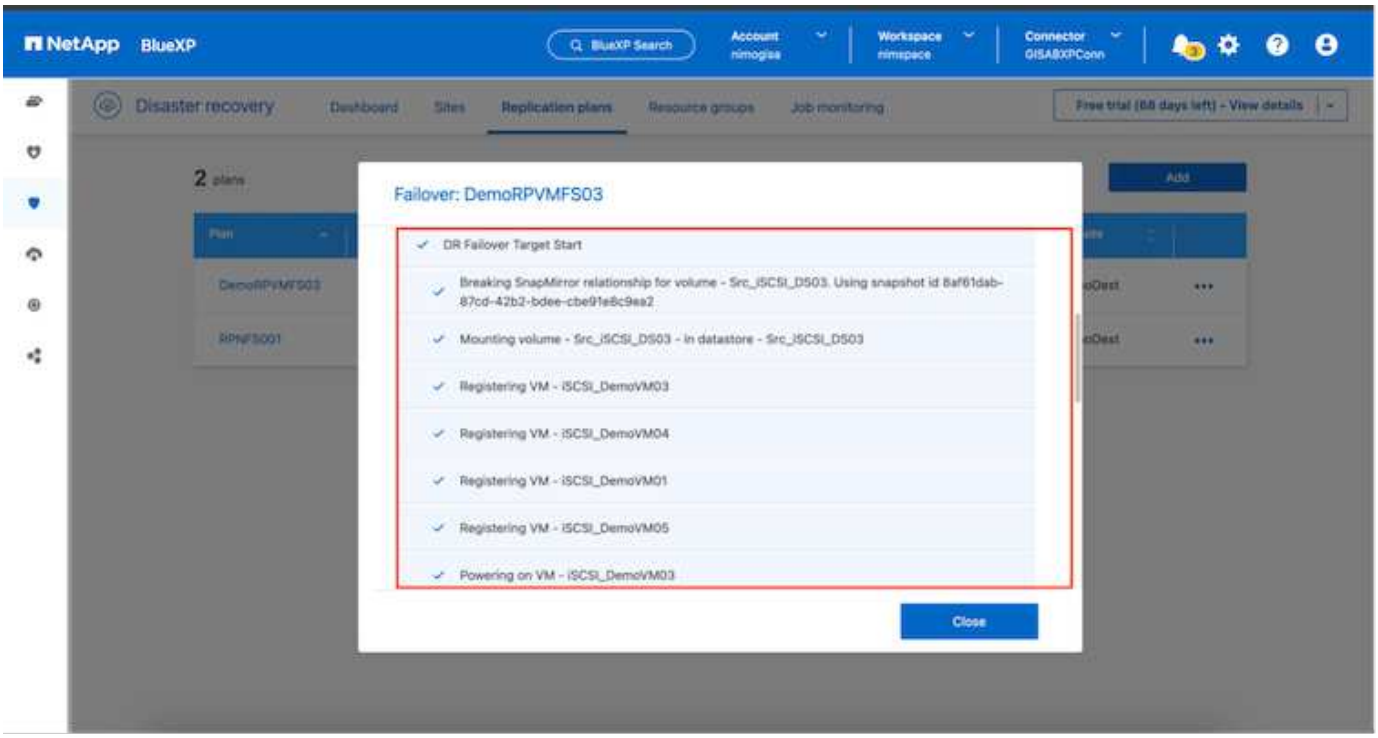




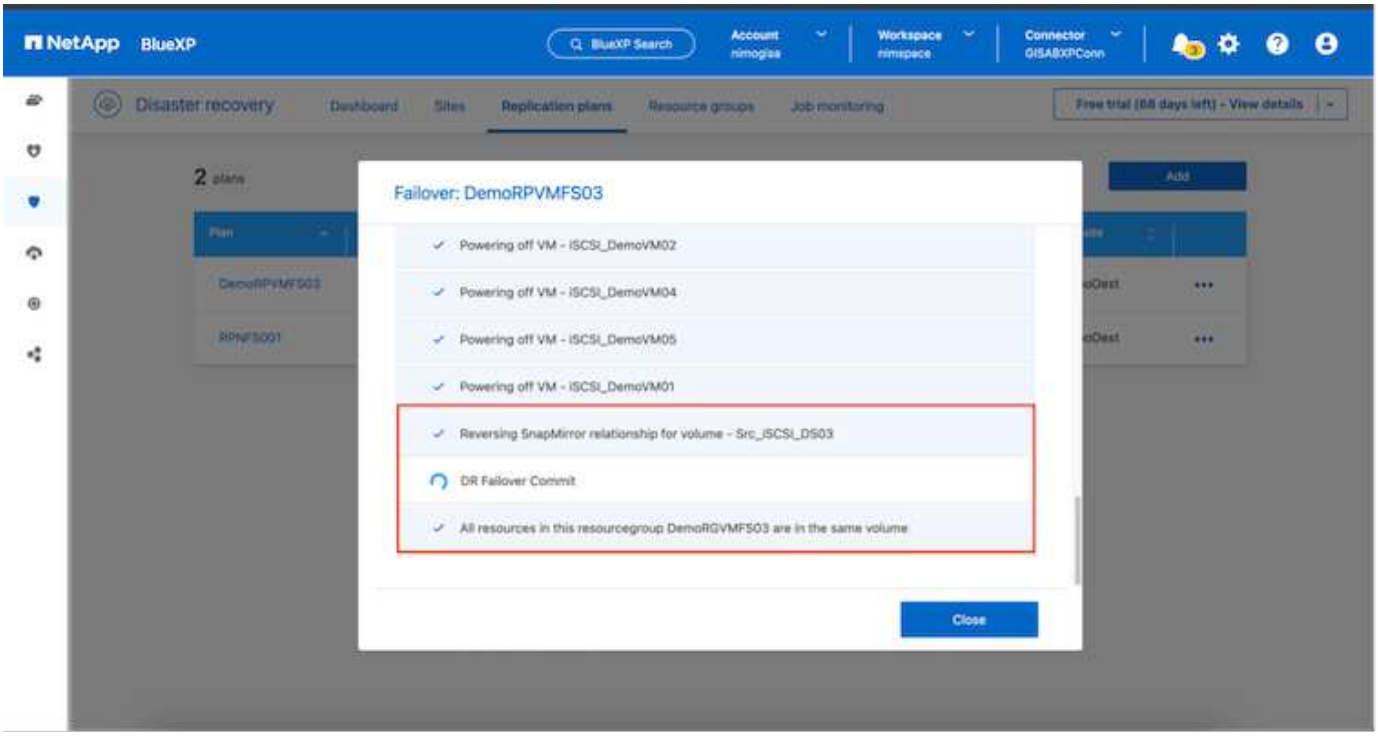
Una volta completata l’operazione di failover di prova, è possibile avviare l’operazione di pulizia utilizzando **"Clean Up failover test"**. Durante questa operazione, il BlueXP disaster recovery distrugge il volume FlexClone utilizzato nell’operazione.

In caso di un vero disastro, il BlueXP disaster recovery esegue i seguenti passaggi:

1. Interrompe la relazione SnapMirror tra i siti.
2. Monta il volume del datastore VMFS dopo la nuova firma per un utilizzo immediato.
3. Registrare le VM
4. Accendere le VM

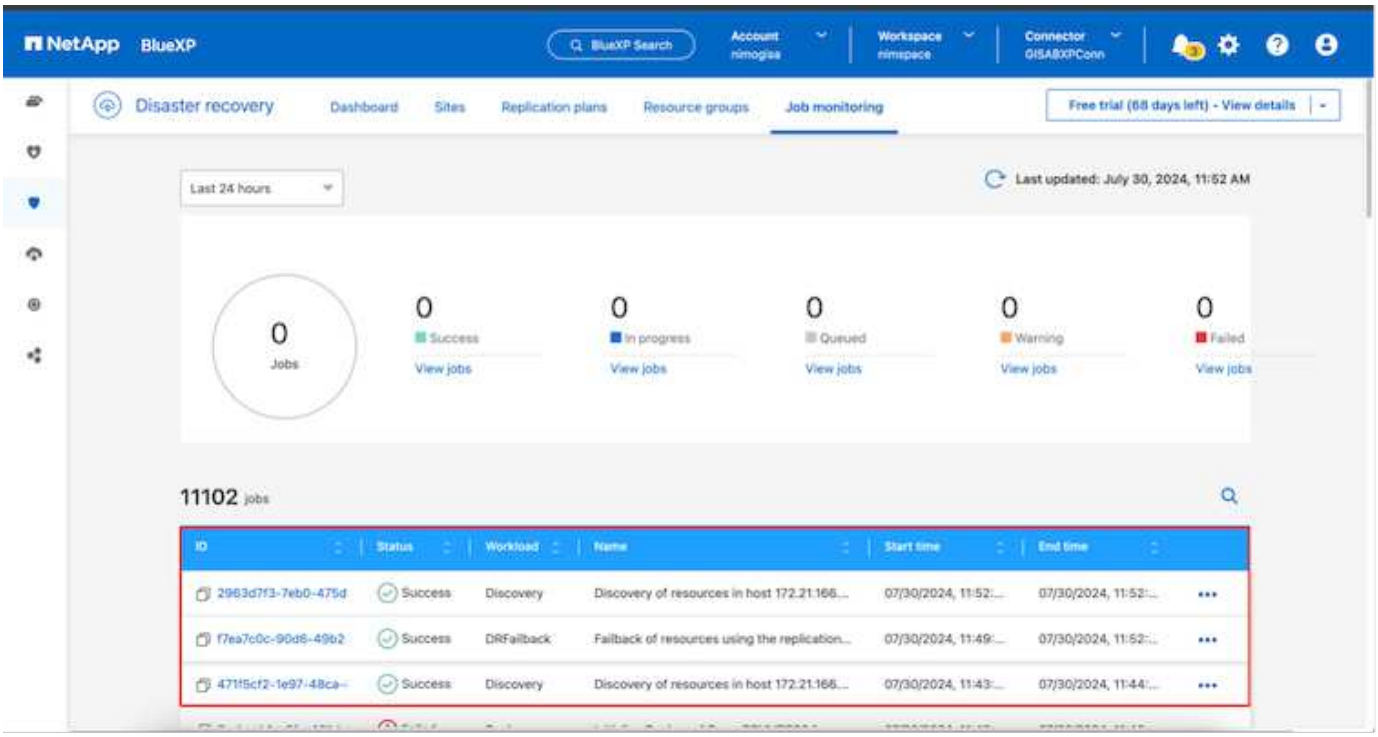


Una volta che il sito primario è attivo e funzionante, il BlueXP disaster recovery consente la risincronizzazione inversa per SnapMirror e abilita il failback, che può essere eseguito con un semplice clic.



Se si sceglie l'opzione di migrazione, questa viene considerata un evento di failover pianificato. In questo caso, viene attivato un ulteriore passaggio che consiste nello spegnimento delle macchine virtuali nel sito di origine. Il resto dei passaggi rimane lo stesso dell'evento di failover.

Da BlueXP o dalla CLI ONTAP è possibile monitorare lo stato di integrità della replica per i volumi del datastore appropriati, mentre lo stato di un failover o di un failover di prova può essere monitorato tramite Job Monitoring.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il"simulatore di soluzioni" .

Impostare il ripristino di emergenza per i datastore NFS utilizzando il BlueXP disaster recovery

In questo caso d'uso descriviamo la procedura per impostare il disaster recovery utilizzando BlueXP disaster recovery per le VM VMware on-premise che utilizzano datastore NFS. Questa procedura include la configurazione dell'account e del connettore BlueXP , l'aggiunta di array ONTAP per abilitare la comunicazione tra VMware vCenter e lo storage ONTAP , la configurazione della replica tra i siti e la creazione e il test dei piani di ripristino.

L'implementazione del disaster recovery tramite replica a livello di blocco dal sito di produzione al sito di disaster recovery è un metodo resiliente ed economico per proteggere i carichi di lavoro da interruzioni del sito ed eventi di danneggiamento dei dati, come gli attacchi ransomware. Utilizzando la replica NetApp SnapMirror , i carichi di lavoro VMware in esecuzione su sistemi ONTAP locali con datastore NFS possono essere replicati su un altro sistema di storage ONTAP situato in un data center di ripristino designato in cui è distribuito anche VMware.

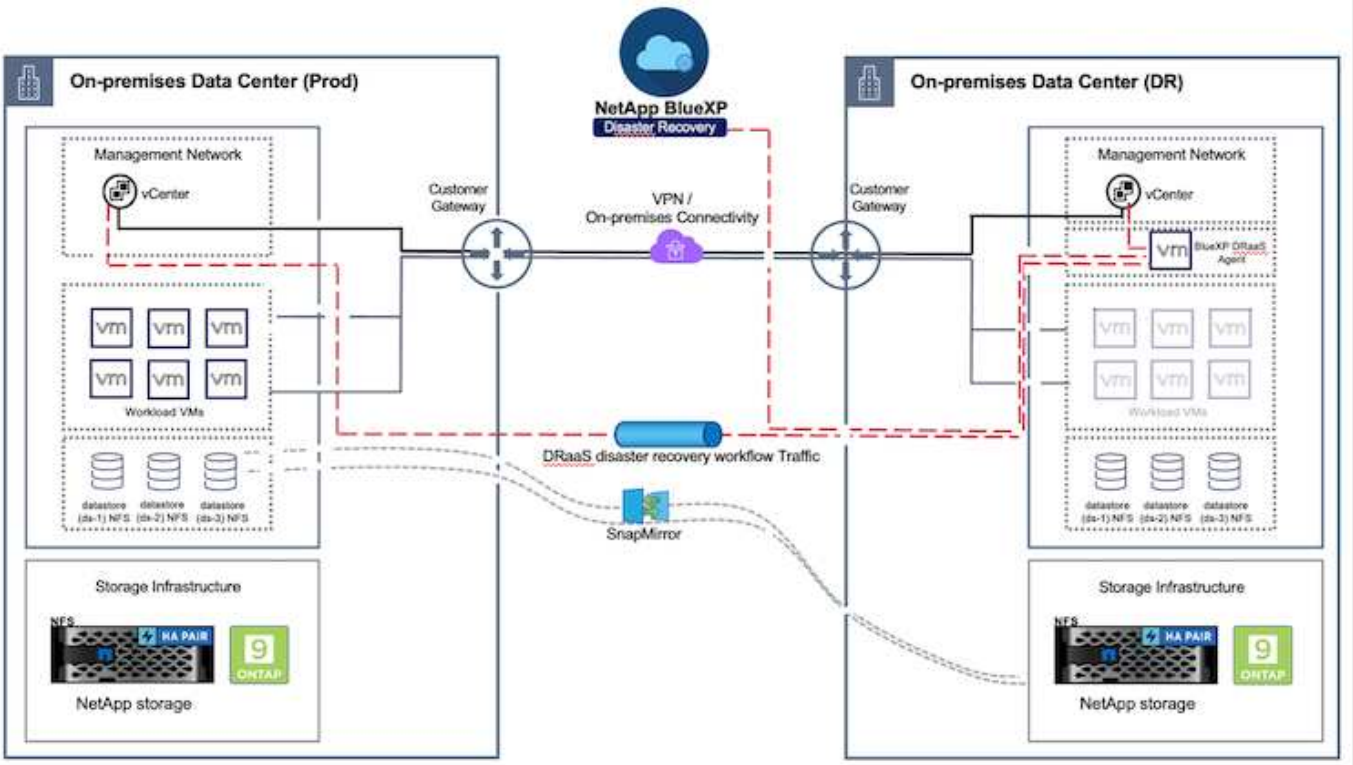
Introduzione

Questa sezione del documento descrive la configurazione di BlueXP DRaaS per impostare il disaster recovery per le VM VMware on-premise su un altro sito designato. Come parte di questa configurazione, l'account BlueXP , il connettore BlueXP e gli array ONTAP sono stati aggiunti all'interno dell'area di lavoro BlueXP , necessari per abilitare la comunicazione da VMware vCenter allo storage ONTAP . Inoltre, questo documento

spiega nel dettaglio come configurare la replica tra siti e come impostare e testare un piano di ripristino. L'ultima sezione contiene istruzioni su come eseguire un failover completo del sito e su come effettuare il failback quando il sito primario viene ripristinato e acquistato online.

Utilizzando il servizio BlueXP disaster recovery , integrato nella console NetApp BlueXP , le aziende possono individuare facilmente i propri VMware vCenter e storage ONTAP in sede. Le organizzazioni possono quindi creare raggruppamenti di risorse, creare un piano di disaster recovery, associarlo a gruppi di risorse e testare o eseguire failover e failback. SnapMirror fornisce la replicazione dei blocchi a livello di storage per mantenere i due siti aggiornati con modifiche incrementali, con un Recovery Point Objective (RPO) fino a 5 minuti. Inoltre, è possibile simulare procedure di disaster recovery senza compromettere la produzione o incorrere in costi di archiviazione aggiuntivi.

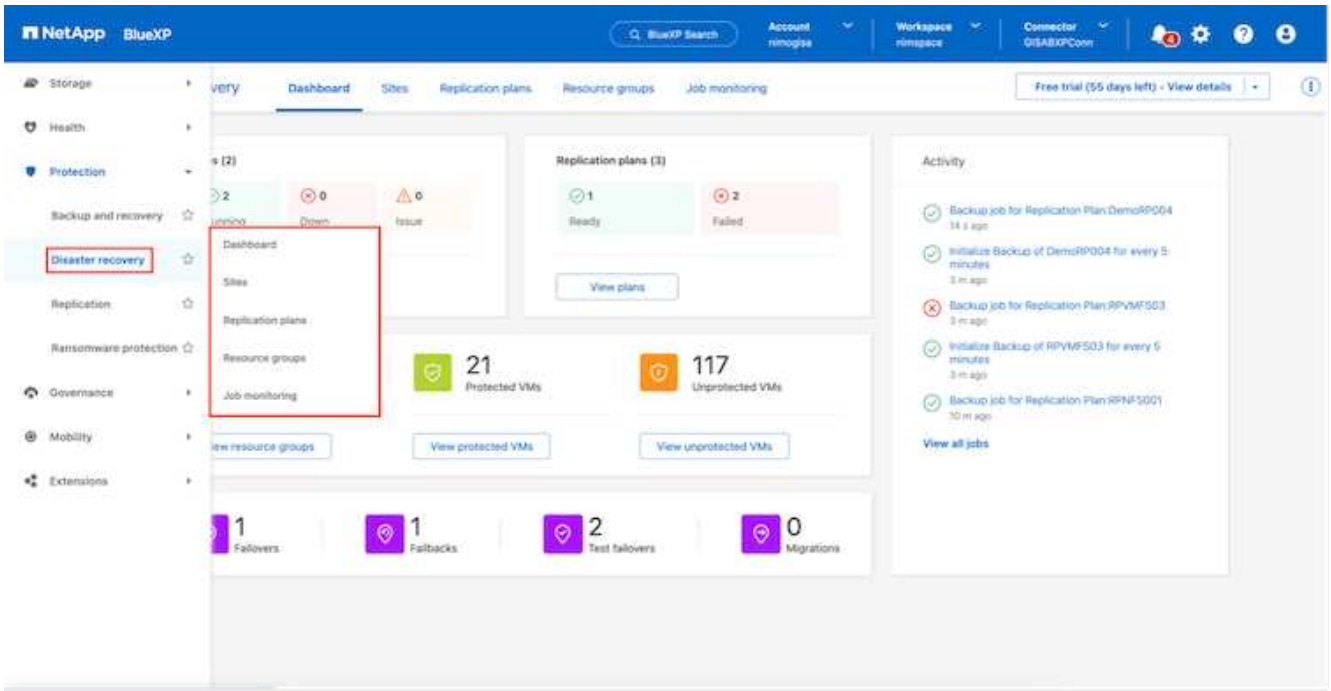
Il BlueXP disaster recovery sfrutta la tecnologia FlexClone di ONTAP per creare una copia efficiente in termini di spazio del datastore NFS dall'ultimo snapshot replicato sul sito di disaster recovery. Dopo aver completato il test di disaster recovery, i clienti possono facilmente eliminare l'ambiente di test senza influire sulle risorse di produzione effettivamente replicate. In caso di un failover effettivo, il servizio BlueXP disaster recovery orchestra tutti i passaggi necessari per ripristinare automaticamente le macchine virtuali protette sul sito di disaster recovery designato con pochi clic. Il servizio invertirà anche la relazione SnapMirror con il sito primario e replicherà eventuali modifiche dal secondario al primario per un'operazione di failback, quando necessario. Tutte queste funzionalità hanno un costo molto inferiore rispetto ad altre alternative note.



Iniziare

Per iniziare a utilizzare il BlueXP disaster recovery, utilizzare la console BlueXP e quindi accedere al servizio.

1. Accedi a BlueXP.
2. Dal menu di navigazione a sinistra BlueXP , seleziona Protezione > Ripristino di emergenza.
3. Viene visualizzata la Dashboard BlueXP disaster recovery .

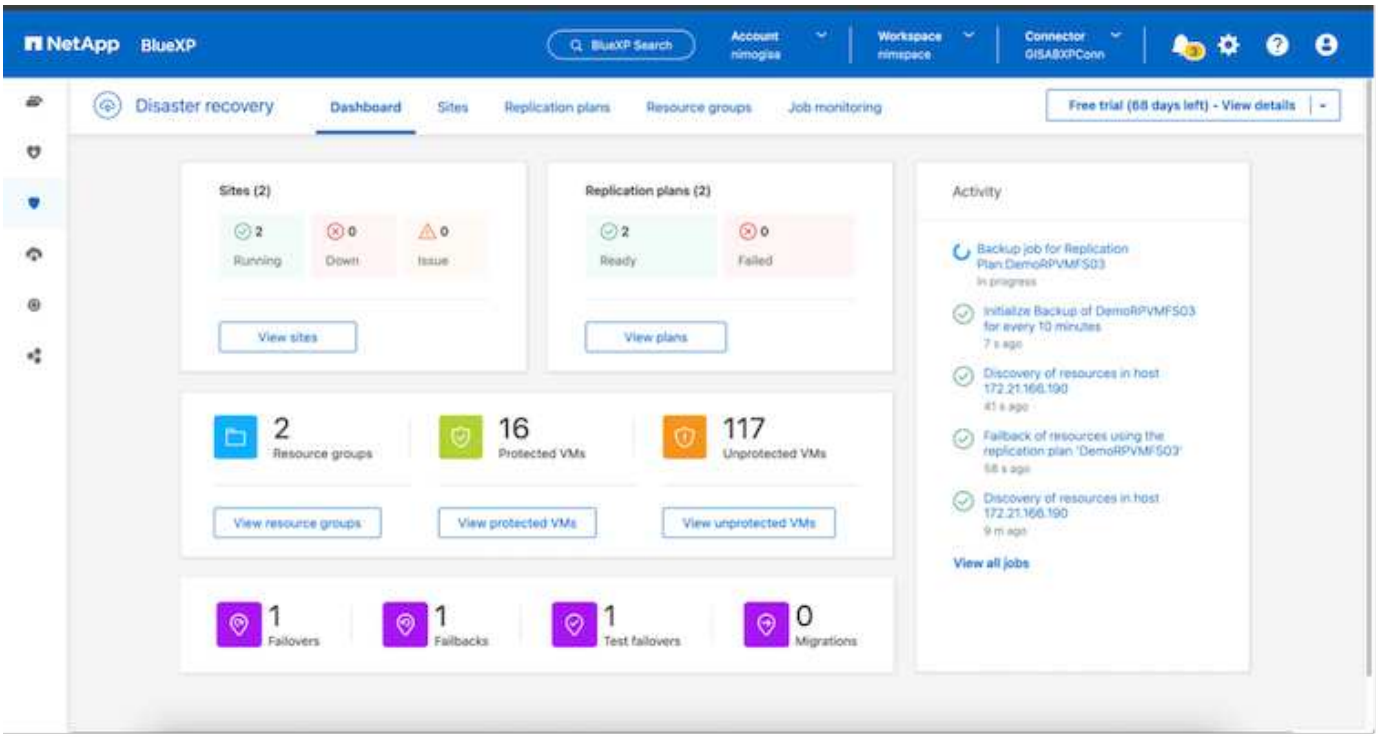


Prima di configurare il piano di disaster recovery, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- BlueXP Connector è configurato in NetApp BlueXP.
- Le istanze del connettore BlueXP dispongono di connettività con i sistemi di archiviazione e vCenter di origine e di destinazione.
- Cluster NetApp Data ONTAP per fornire datastore NFS di storage.
- In BlueXP sono stati aggiunti sistemi di storage NetApp on-premise che ospitano datastore NFS per VMware.
- Quando si utilizzano nomi DNS, è necessario che sia attiva la risoluzione DNS. In caso contrario, utilizzare gli indirizzi IP per vCenter.
- La replica SnapMirror è configurata per i volumi di datastore basati su NFS designati.
- Assicurarsi che l'ambiente disponga di versioni supportate dei server vCenter Server ed ESXi.

Una volta stabilita la connettività tra il sito di origine e quello di destinazione, procedere con la configurazione, che dovrebbe richiedere un paio di clic e circa 3-5 minuti.

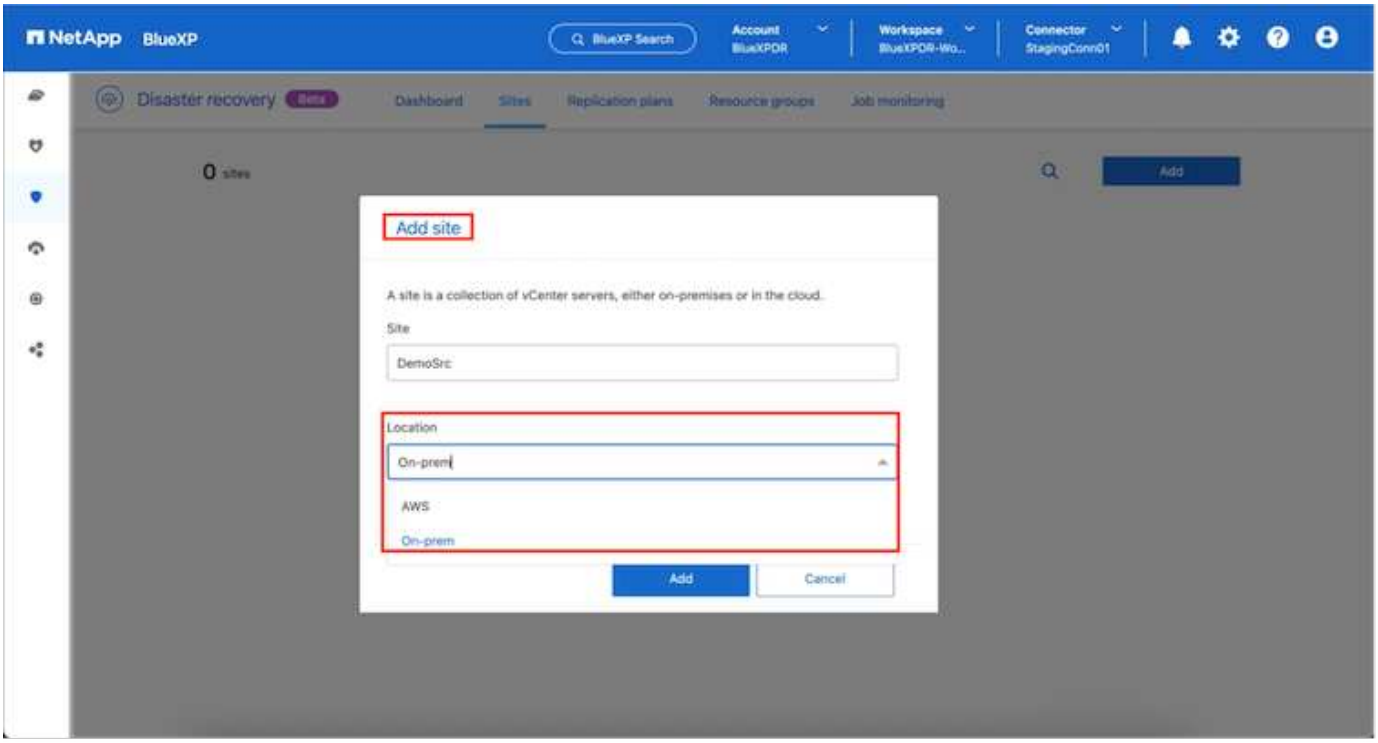
> NetApp consiglia di distribuire il connettore BlueXP nel sito di destinazione o in un terzo sito, in modo che il connettore BlueXP possa comunicare tramite la rete con le risorse di origine e di destinazione.



Configurazione BlueXP disaster recovery

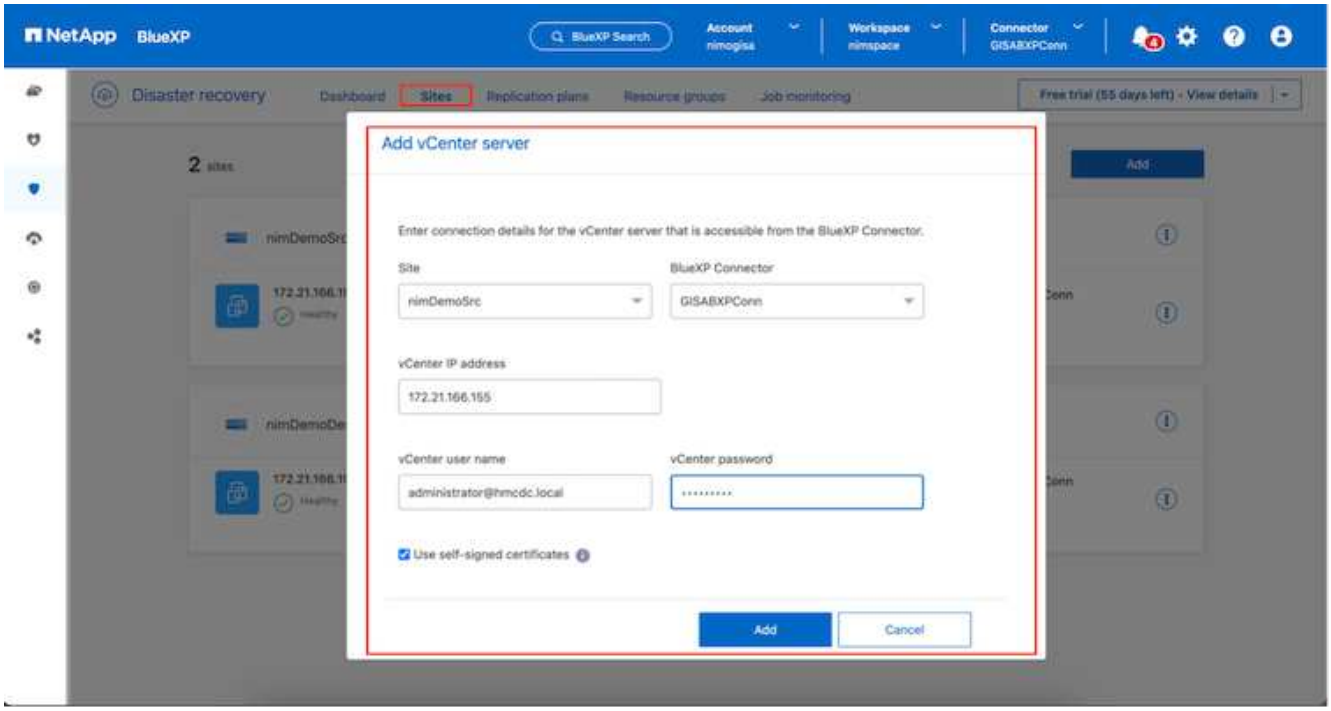
Il primo passo per prepararsi al disaster recovery è individuare e aggiungere le risorse di archiviazione e vCenter locali al BlueXP disaster recovery.

Aprire la console BlueXP e selezionare **Protezione > Ripristino di emergenza** dal menu di navigazione a sinistra. Selezionare **Scopri server vCenter** oppure utilizzare il menu in alto, selezionare **Siti > Aggiungi > Aggiungi vCenter**.

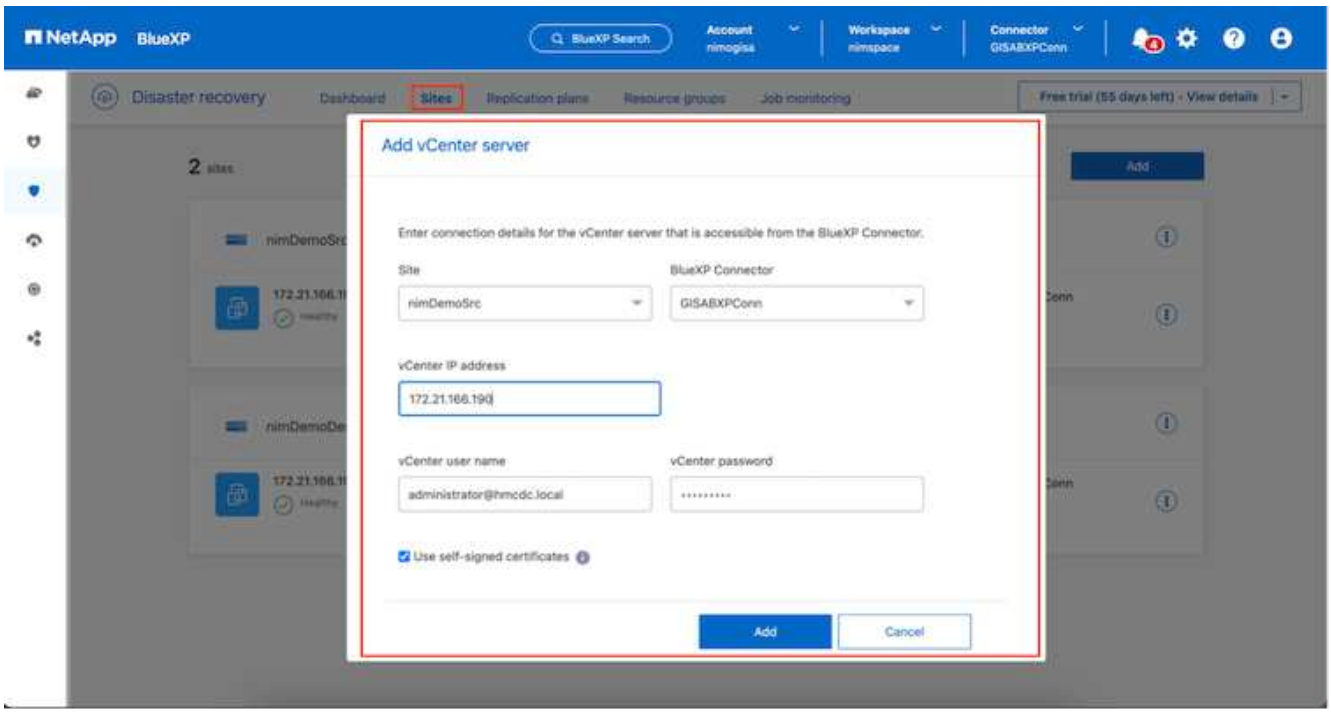


Aggiungere le seguenti piattaforme:

- **Fonte**. vCenter locale.



- **Destinazione**. VMC SDDC vCenter.



Una volta aggiunti i vCenter, viene attivata la rilevazione automatica.

Configurazione della replica di archiviazione tra l'array del sito di origine e l'array del sito di destinazione

SnapMirror fornisce la replica dei dati in un ambiente NetApp . Basata sulla tecnologia NetApp Snapshot, la replica SnapMirror è estremamente efficiente perché replica solo i blocchi che sono stati modificati o aggiunti

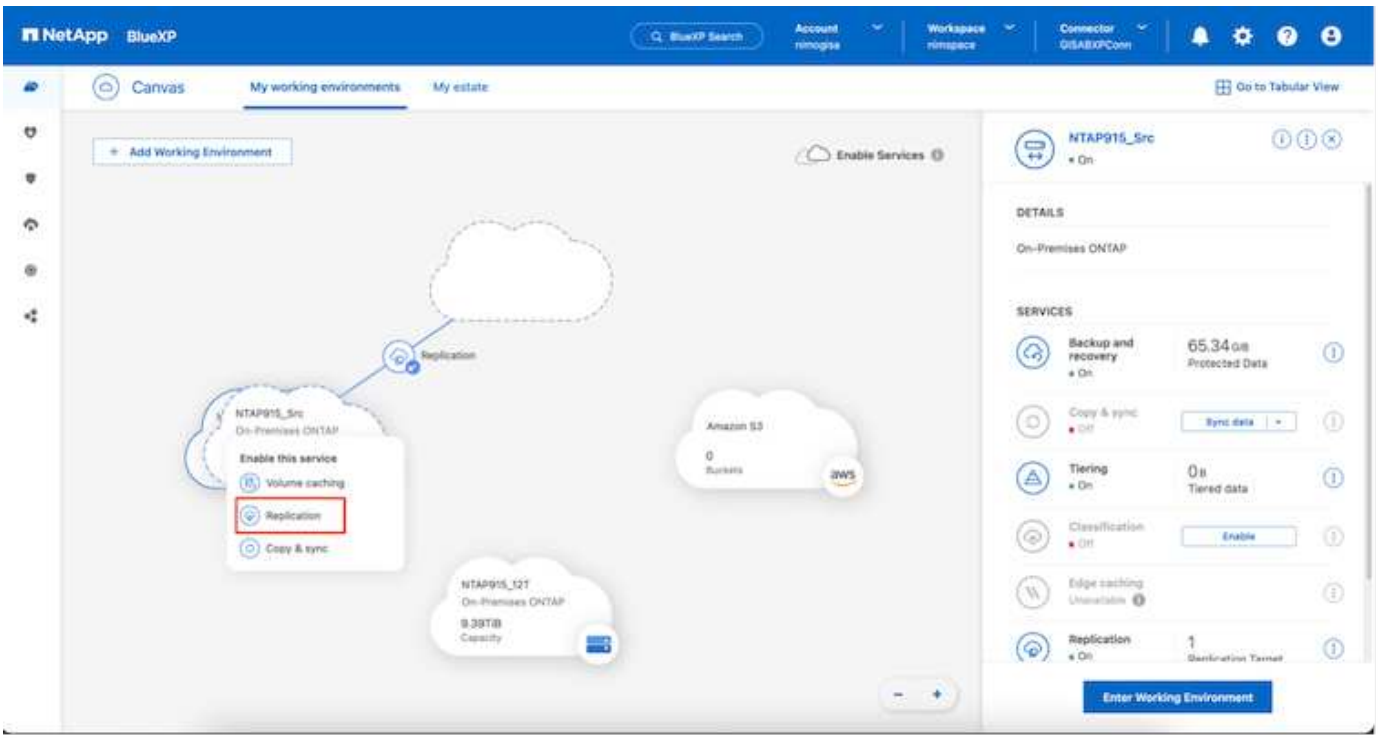
dall'aggiornamento precedente. SnapMirror può essere facilmente configurato tramite NetApp OnCommand System Manager o ONTAP CLI. BlueXP DRaaS crea anche la relazione SnapMirror a condizione che il cluster e il peering SVM siano configurati in anticipo.

Nei casi in cui lo storage primario non è completamente perso, SnapMirror fornisce un mezzo efficiente per risincronizzare i siti primario e DR. SnapMirror può risincronizzare i due siti, trasferendo solo i dati modificati o nuovi dal sito DR al sito primario, semplicemente invertendo le relazioni SnapMirror . Ciò significa che i piani di replica in BlueXP DRaaS possono essere risincronizzati in entrambe le direzioni dopo un failover senza dover ricopiare l'intero volume. Se una relazione viene risincronizzata nella direzione inversa, solo i nuovi dati scritti dall'ultima sincronizzazione riuscita della copia Snapshot vengono inviati alla destinazione.

> Se la relazione SnapMirror è già configurata per il volume tramite CLI o System Manager, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.

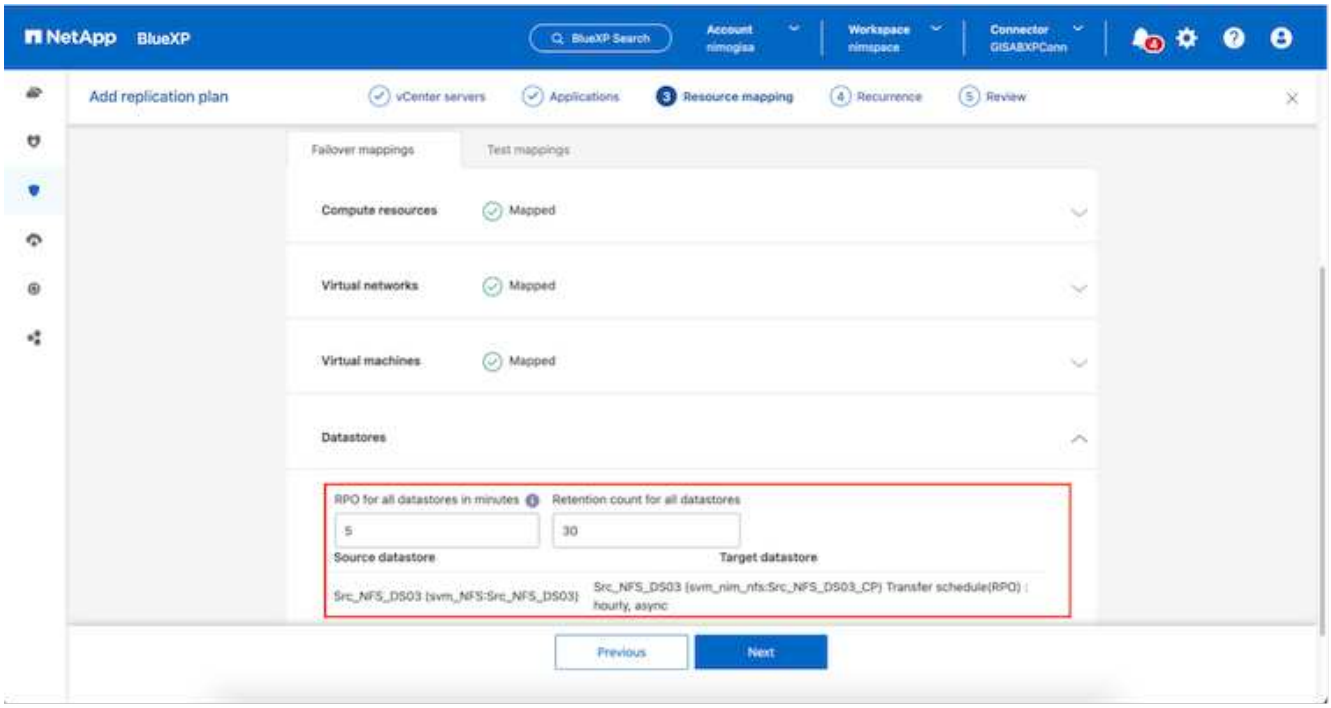
Come configurarlo per VMware Disaster Recovery

Il processo per creare una replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il processo può essere manuale o automatizzato. Il modo più semplice è sfruttare BlueXP per configurare la replica SnapMirror , utilizzando un semplice trascinamento del sistema ONTAP di origine nell'ambiente sulla destinazione per avviare la procedura guidata che guida attraverso il resto del processo.



BlueXP DRaaS può anche automatizzare la stessa operazione, a condizione che siano soddisfatti i due criteri seguenti:

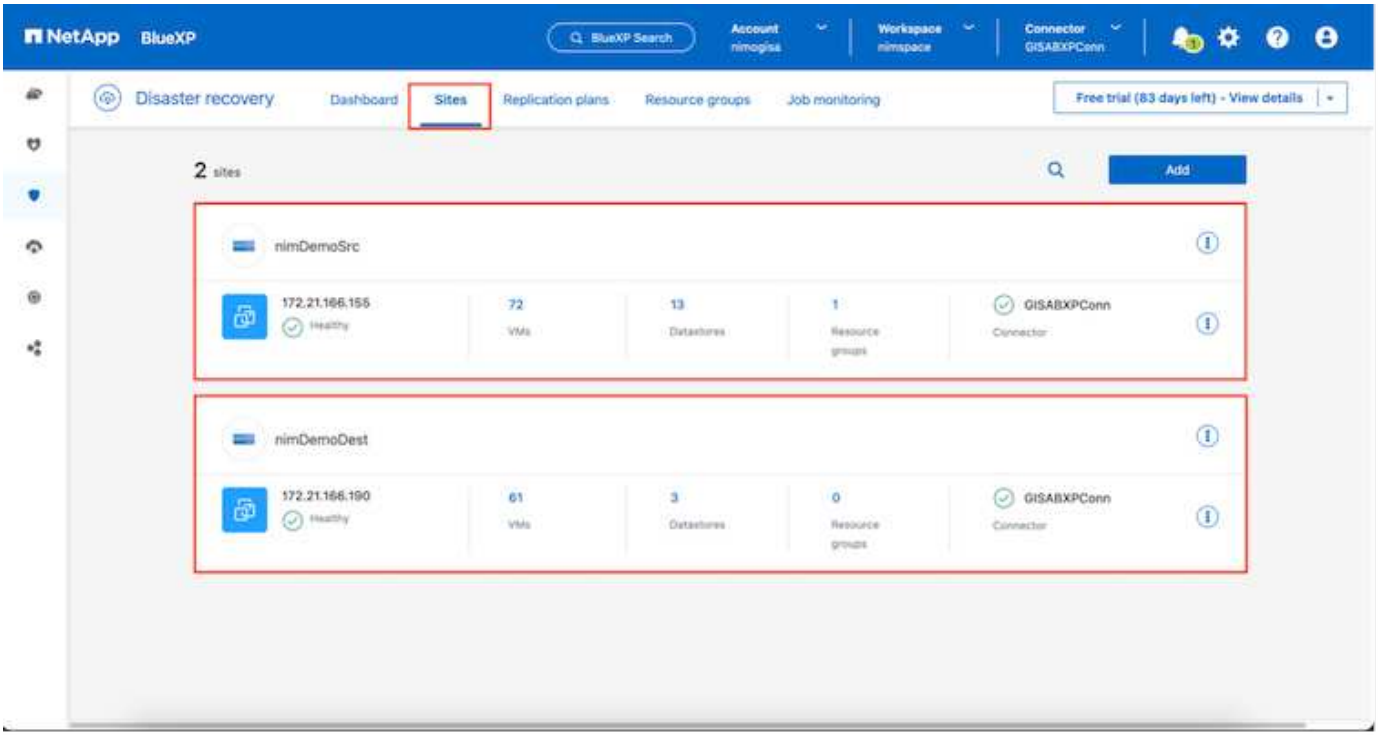
- I cluster di origine e di destinazione hanno una relazione peer.
- L'SVM di origine e l'SVM di destinazione hanno una relazione peer.



Se la relazione SnapMirror è già configurata per il volume tramite CLI, BlueXP DRaaS rileva la relazione e continua con il resto delle operazioni del flusso di lavoro.

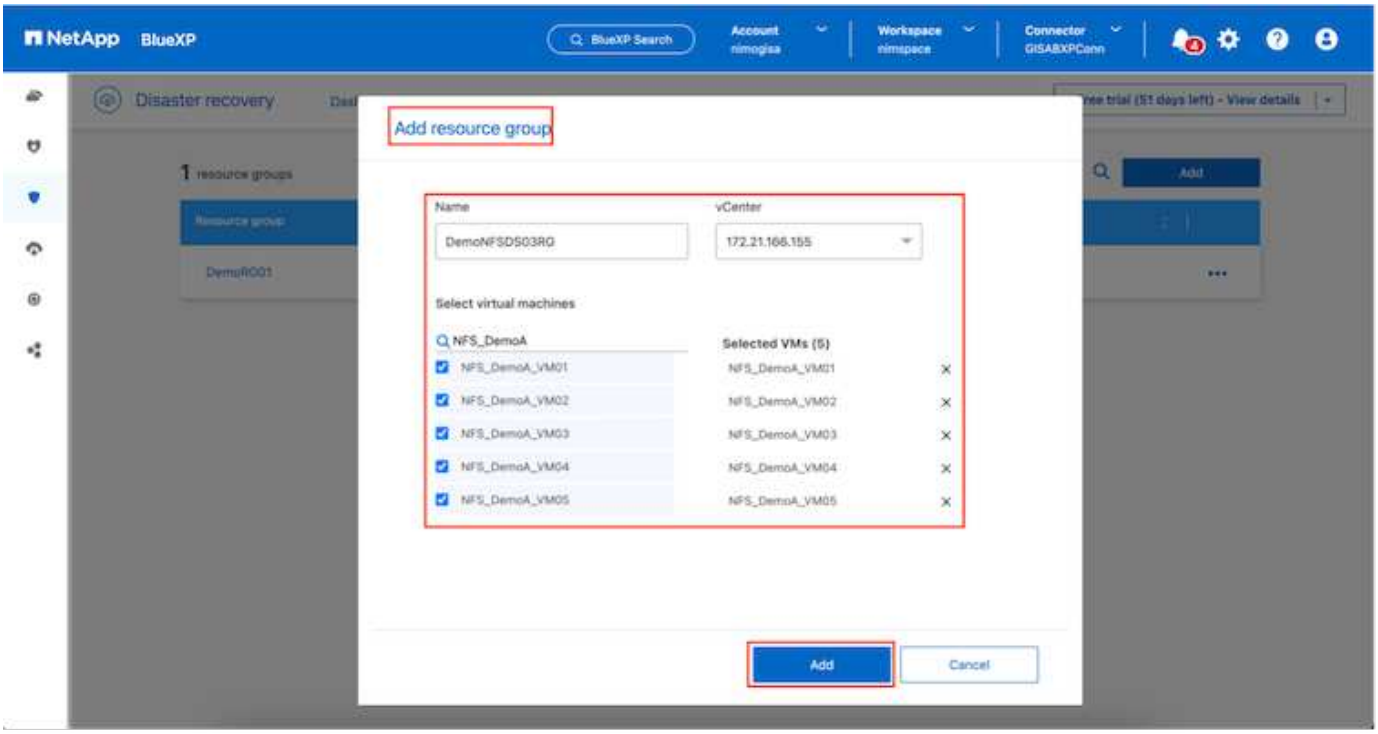
Cosa può fare per te il BlueXP disaster recovery ?

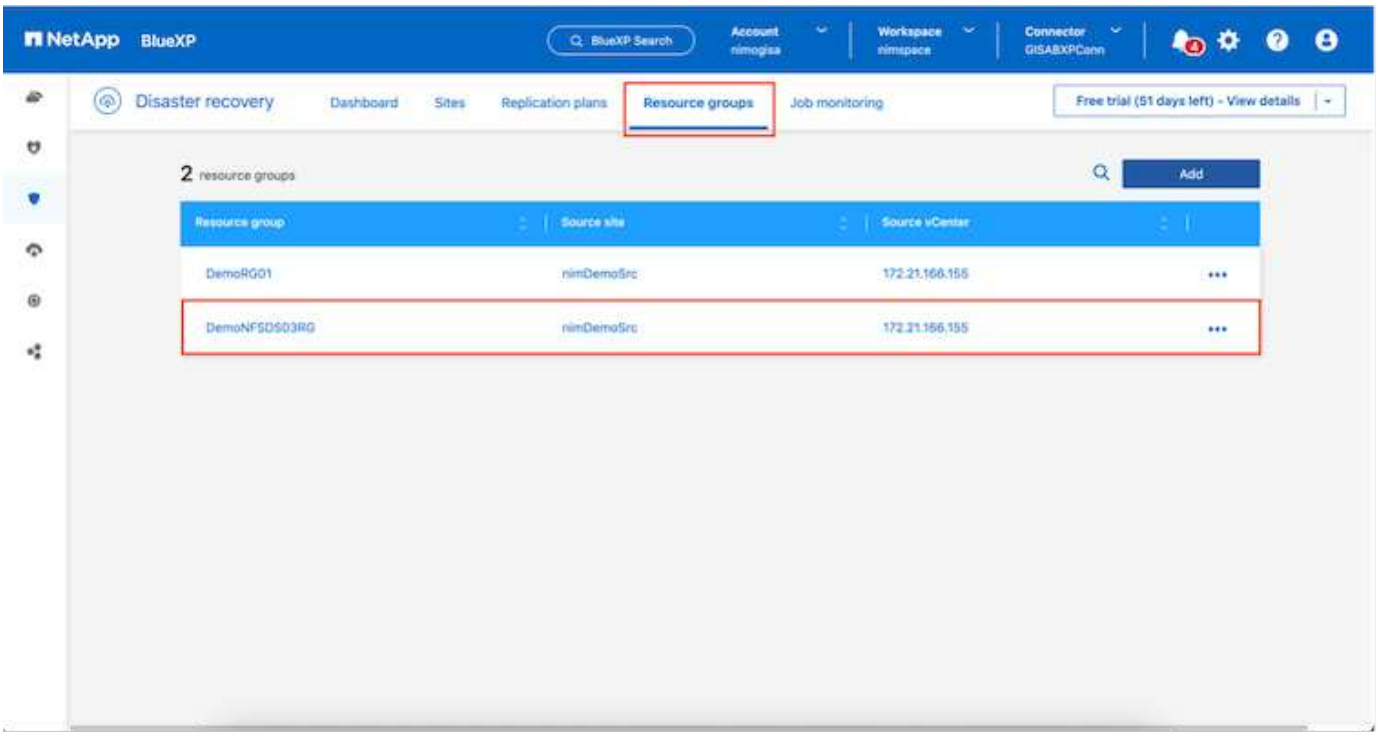
Dopo aver aggiunto i siti di origine e di destinazione, il BlueXP disaster recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. Il BlueXP disaster recovery rileva automaticamente anche le reti e i gruppi di porte utilizzati dalle VM e li popola.



Dopo aver aggiunto i siti, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse BlueXP

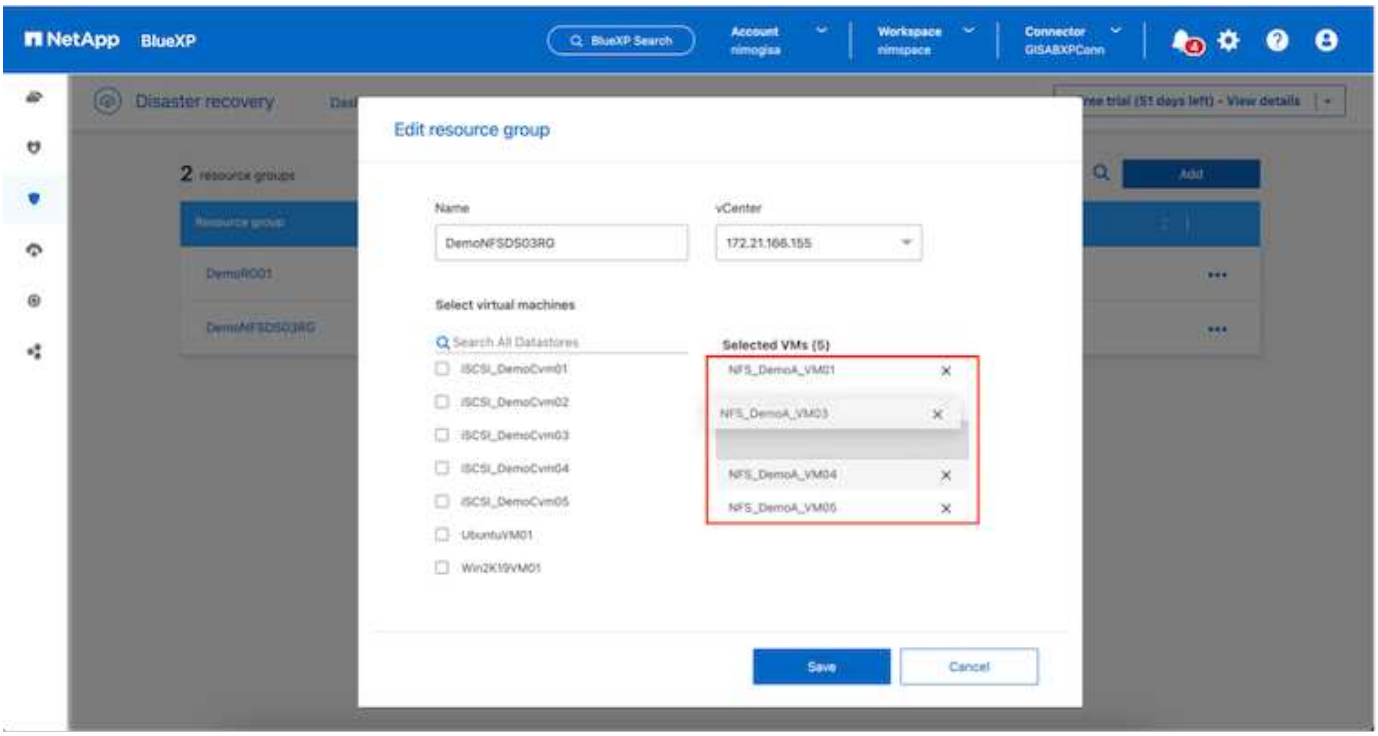
disaster recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. Per iniziare a creare gruppi di risorse, vai su **Gruppi di risorse** e fai clic su **Crea nuovo gruppo di risorse**.



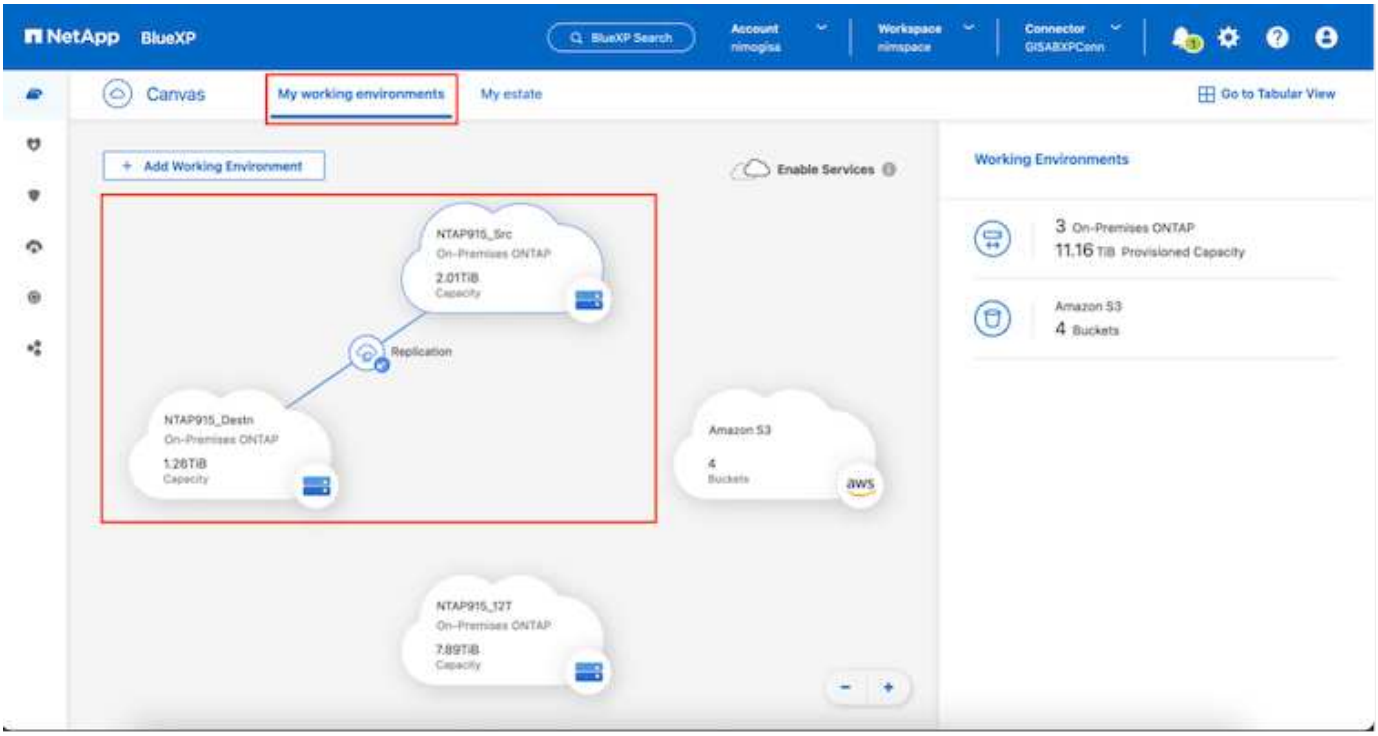


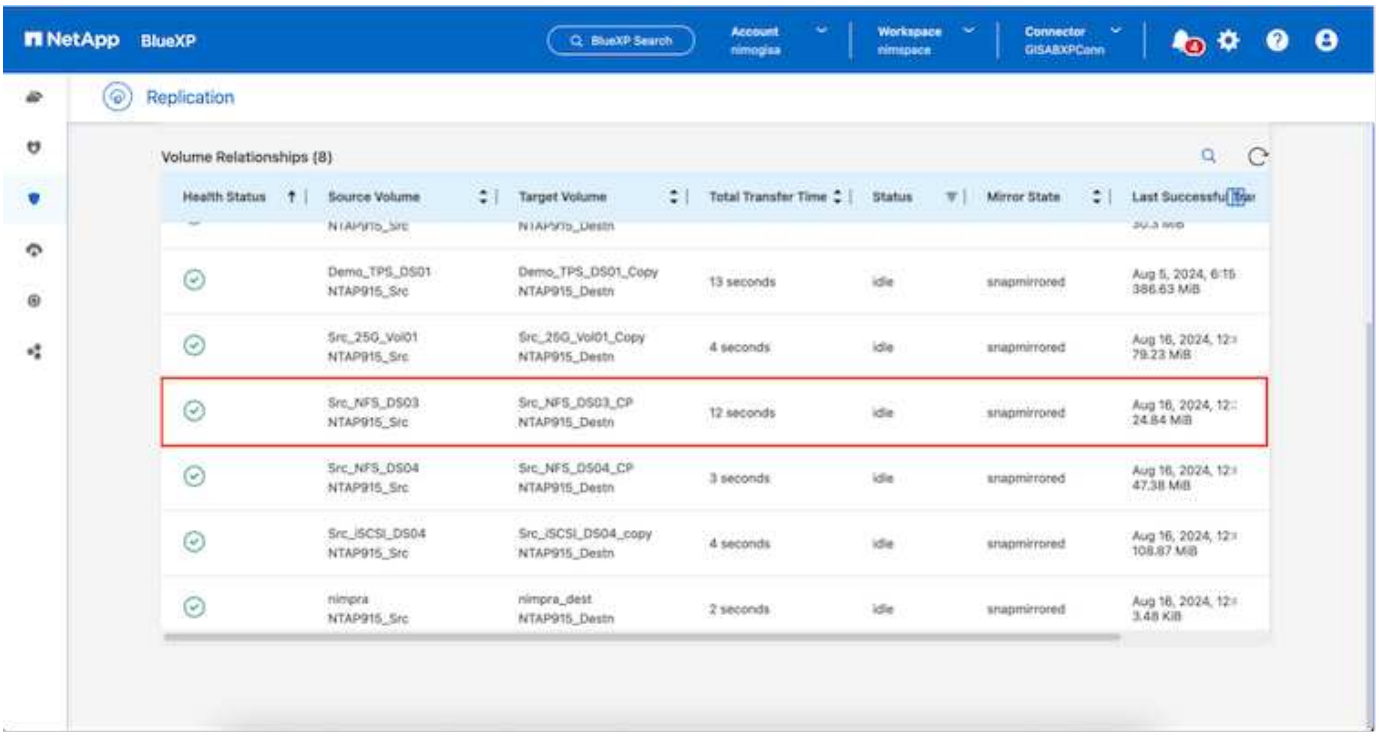
Il gruppo di risorse può essere creato anche durante la creazione di un piano di replica.

L'ordine di avvio delle VM può essere definito o modificato durante la creazione dei gruppi di risorse utilizzando un semplice meccanismo di trascinamento della selezione.



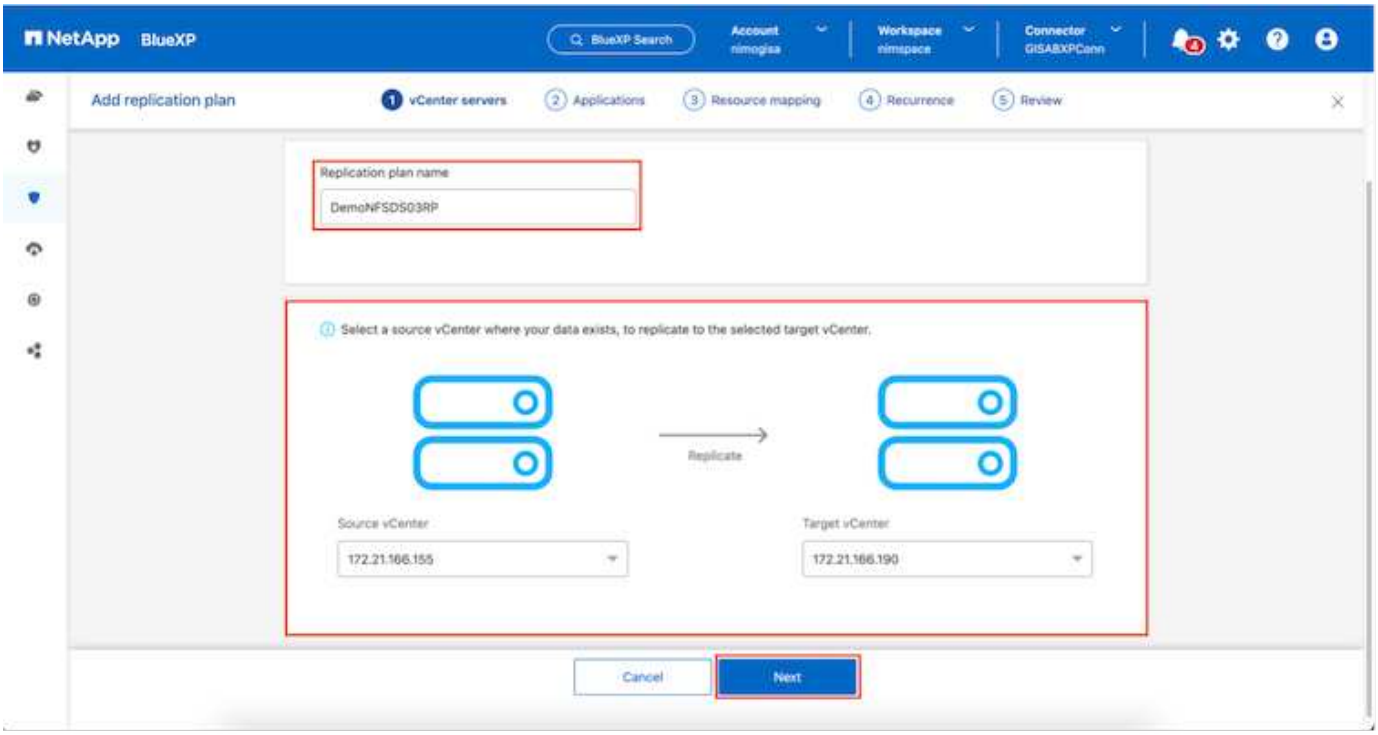
Una volta creati i gruppi di risorse, il passaggio successivo consiste nel creare il progetto di esecuzione o un piano per ripristinare macchine virtuali e applicazioni in caso di disastro. Come indicato nei prerequisiti, la replica SnapMirror può essere configurata in anticipo oppure DRaaS può configurarla utilizzando l'RPO e il conteggio di conservazione specificati durante la creazione del piano di replica.





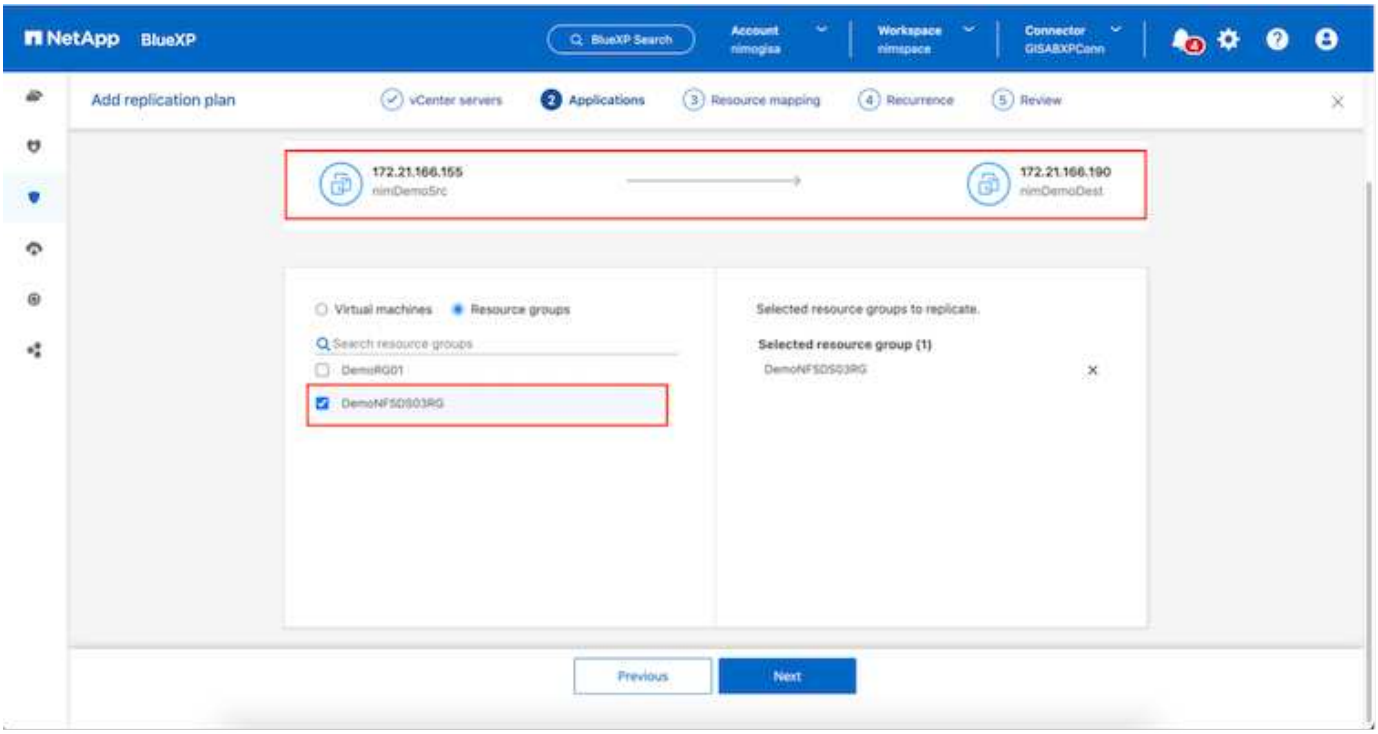
Configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione dal menu a discesa e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti. Per definire il piano di ripristino, accedere alla scheda **Piano di replica** e fare clic su **Aggiungi piano**.

Per prima cosa, seleziona il vCenter di origine e poi quello di destinazione.



Il passo successivo è selezionare i gruppi di risorse esistenti. Se non è stato creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono

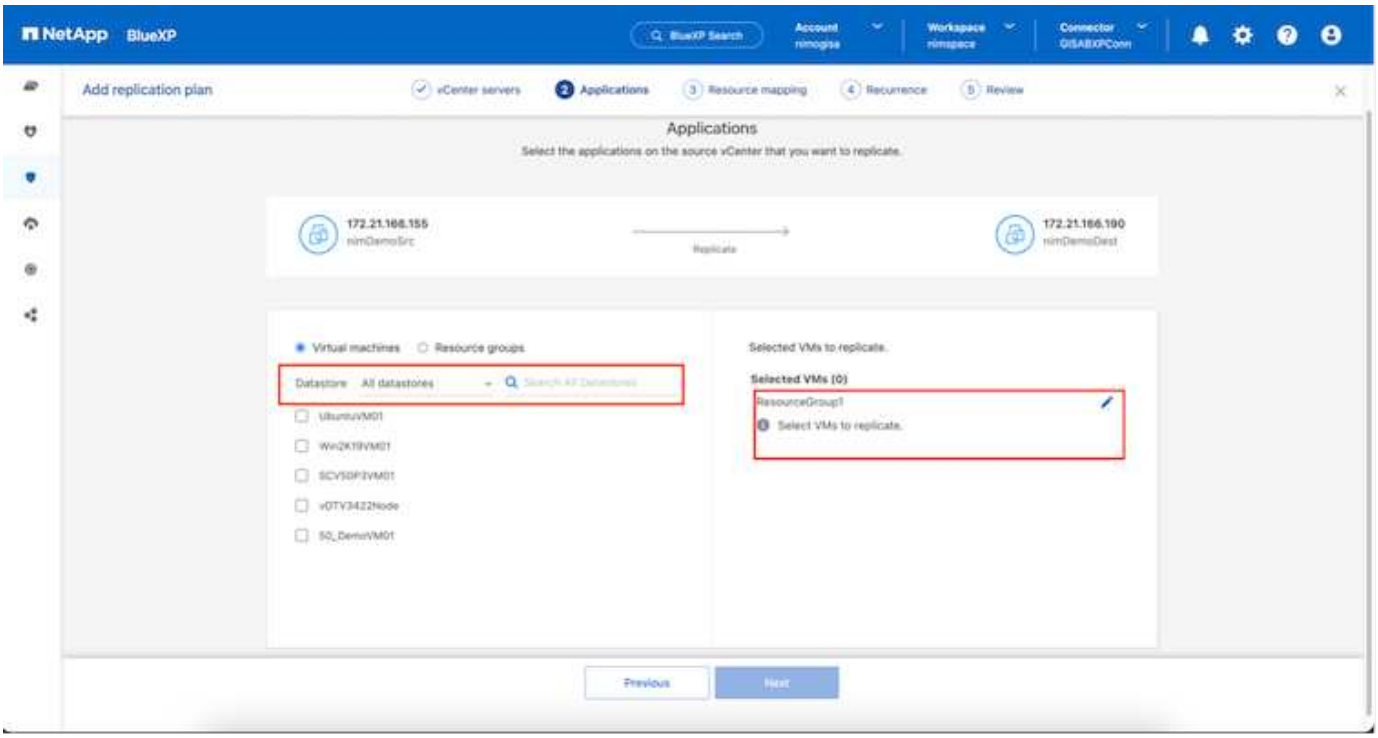
essere ripristinate le macchine virtuali delle applicazioni.



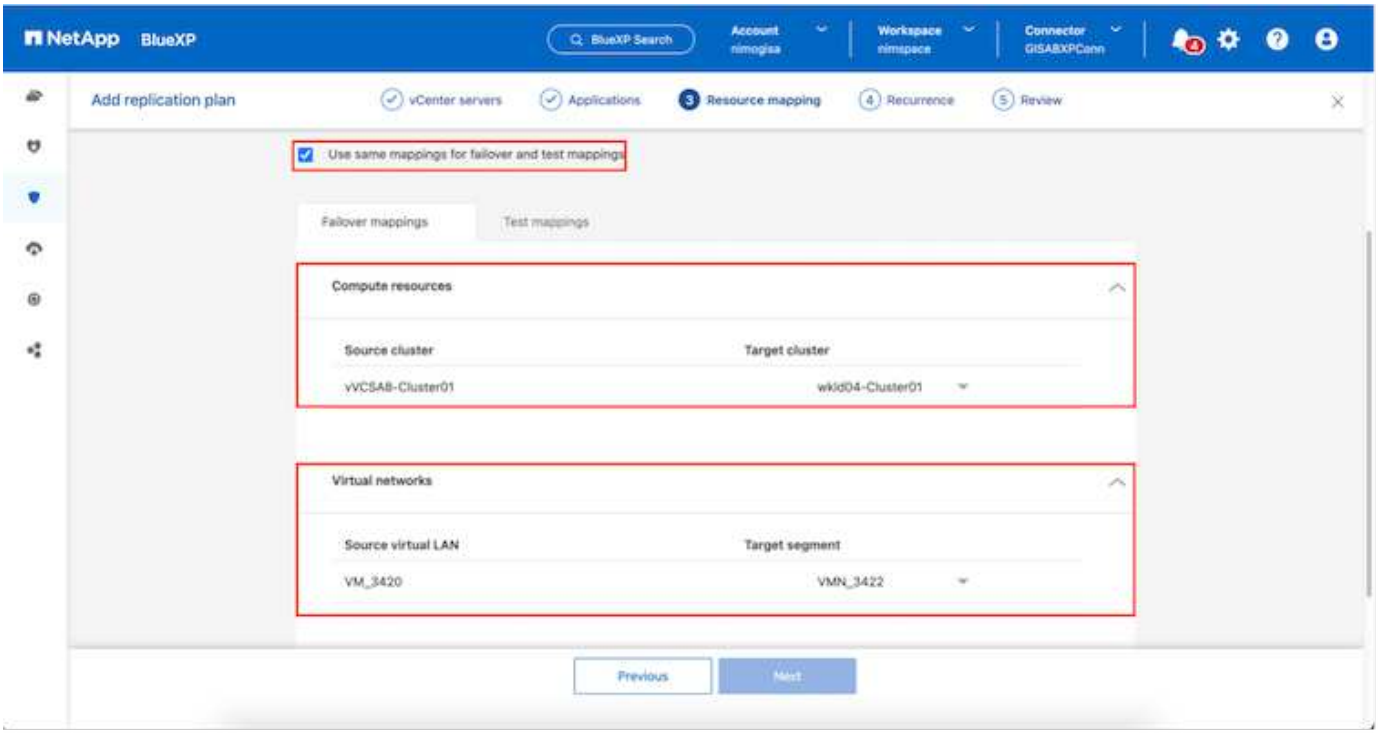
Il gruppo di risorse consente di impostare l'ordine di avvio utilizzando la funzionalità di trascinamento della selezione. Può essere utilizzato per modificare facilmente l'ordine in cui le VM verranno accese durante il processo di ripristino.

Ogni macchina virtuale all'interno di un gruppo di risorse viene avviata in sequenza in base all'ordine. Vengono avviati in parallelo due gruppi di risorse.

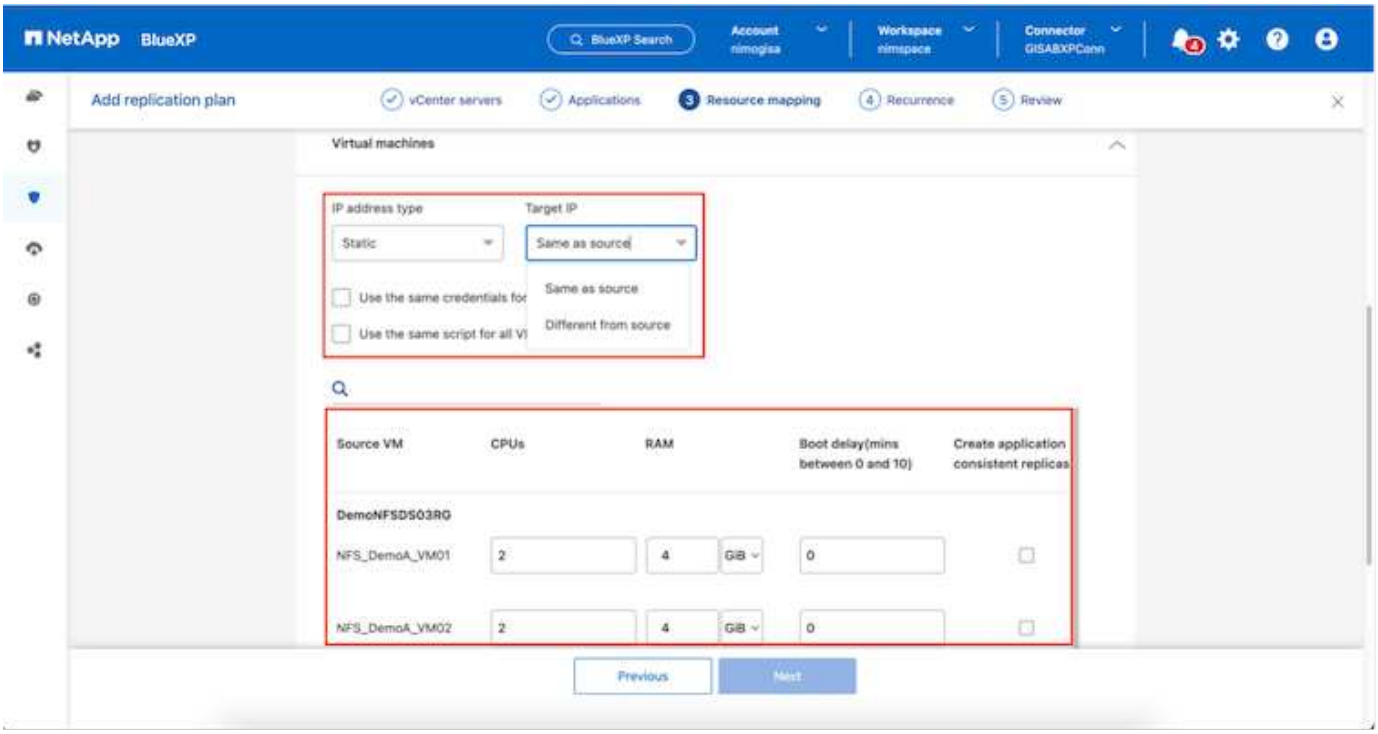
La schermata seguente mostra l'opzione per filtrare macchine virtuali o datastore specifici in base ai requisiti organizzativi se i gruppi di risorse non sono stati creati in precedenza.



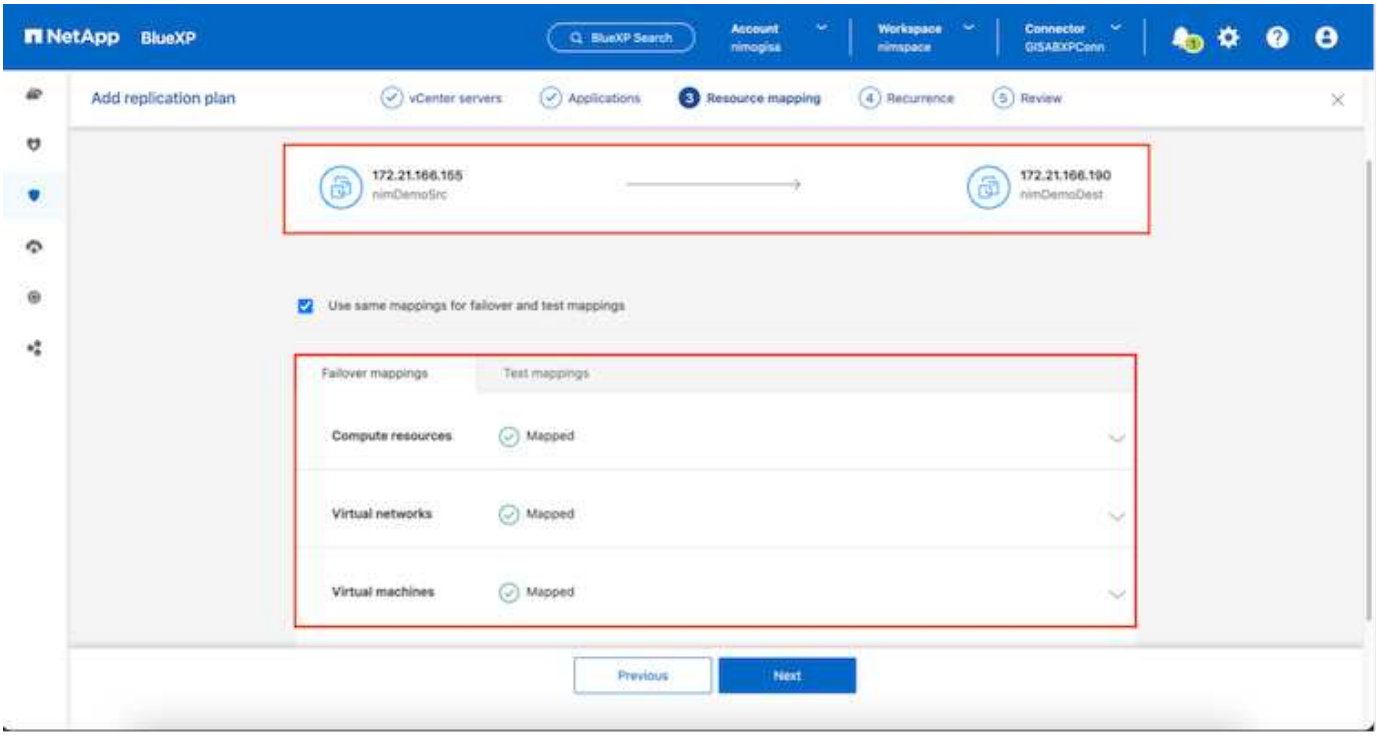
Una volta selezionati i gruppi di risorse, creare i mapping di failover. In questo passaggio, specificare come le risorse dall'ambiente di origine vengono mappate alla destinazione. Ciò include risorse di elaborazione e reti virtuali. Personalizzazione IP, pre- e post-script, ritardi di avvio, coerenza delle applicazioni e così via. Per informazioni dettagliate, fare riferimento a"Creare un piano di replicazione" .



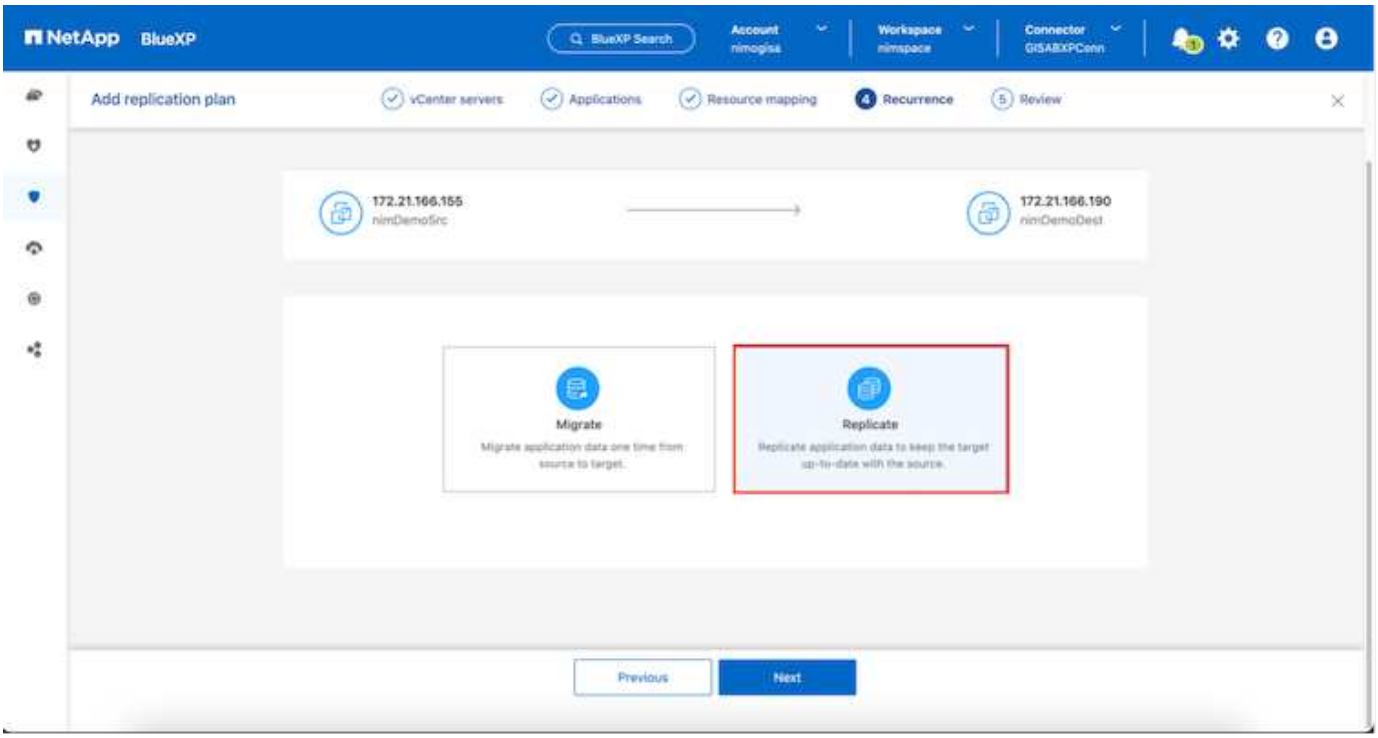
Per impostazione predefinita, vengono utilizzati gli stessi parametri di mappatura sia per le operazioni di test che per quelle di failover. Per impostare diverse mappature per l'ambiente di test, selezionare l'opzione Mappatura test dopo aver deselezionato la casella di controllo come mostrato di seguito:



Una volta completata la mappatura delle risorse, fare clic su Avanti.

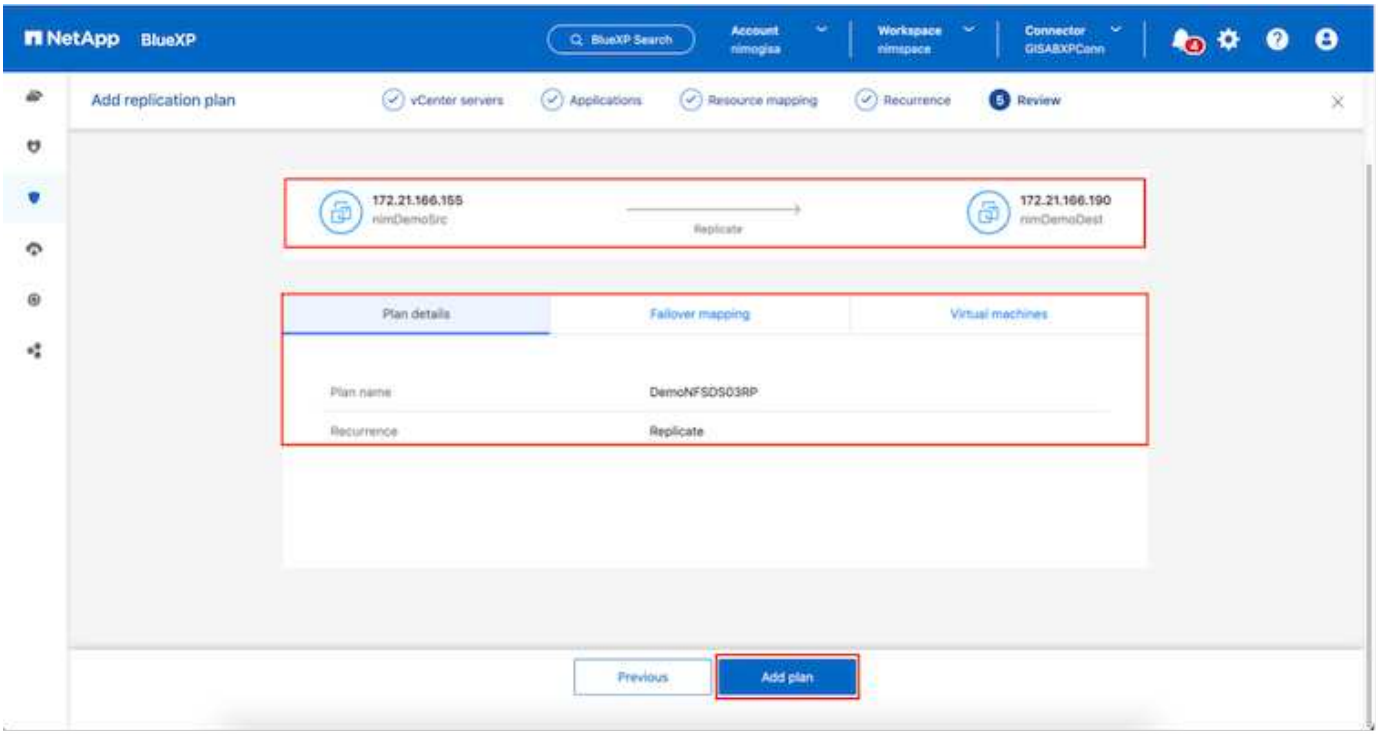


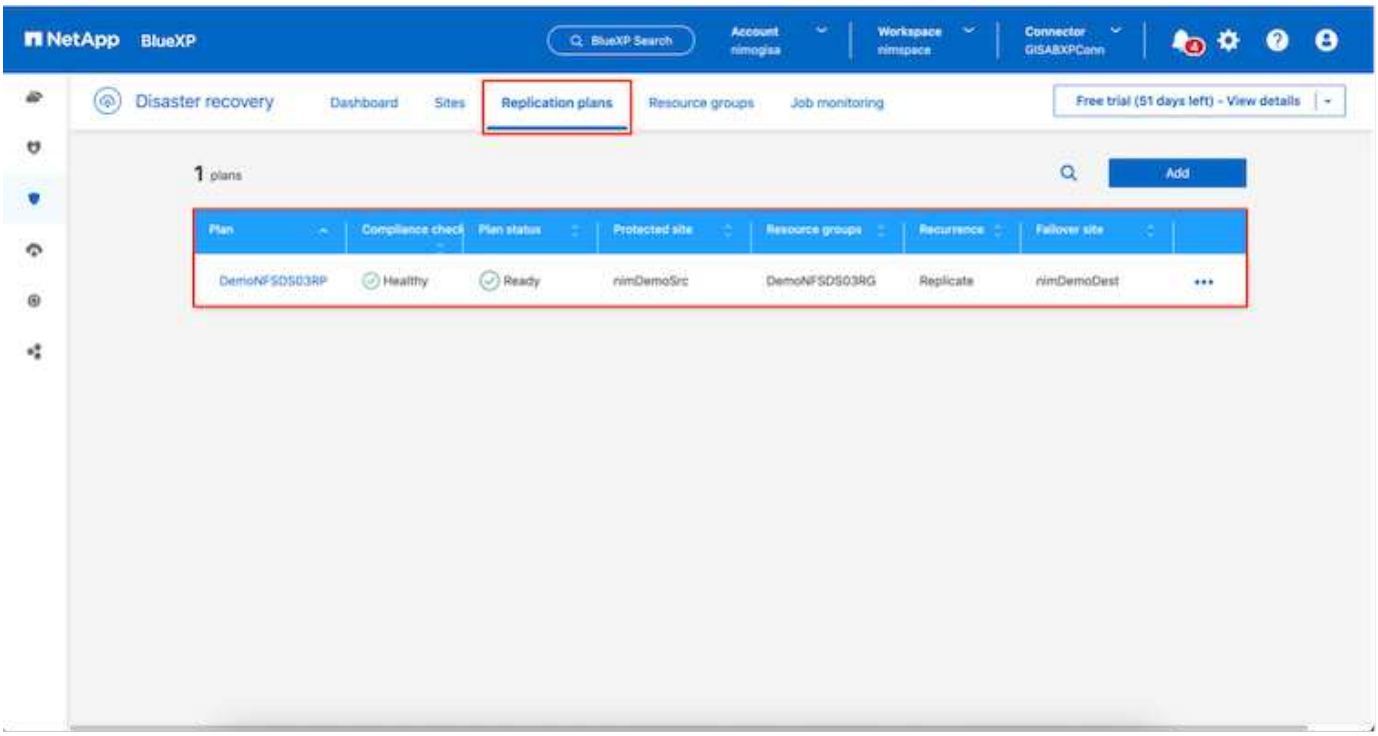
Selezionare il tipo di ricorrenza. In parole semplici, seleziona l'opzione Migra (migrazione una tantum tramite failover) o replica continua ricorrente. In questa procedura dettagliata è selezionata l'opzione Replica.



Una volta fatto, rivedi le mappature create e poi clicca su **Aggiungi piano**.

> In un piano di replicazione è possibile includere VM di volumi diversi e SVM. A seconda del posizionamento della VM (sia sullo stesso volume o su volumi separati all'interno della stessa SVM, volumi separati su SVM diverse), il BlueXP disaster recovery crea uno snapshot del gruppo di coerenza.



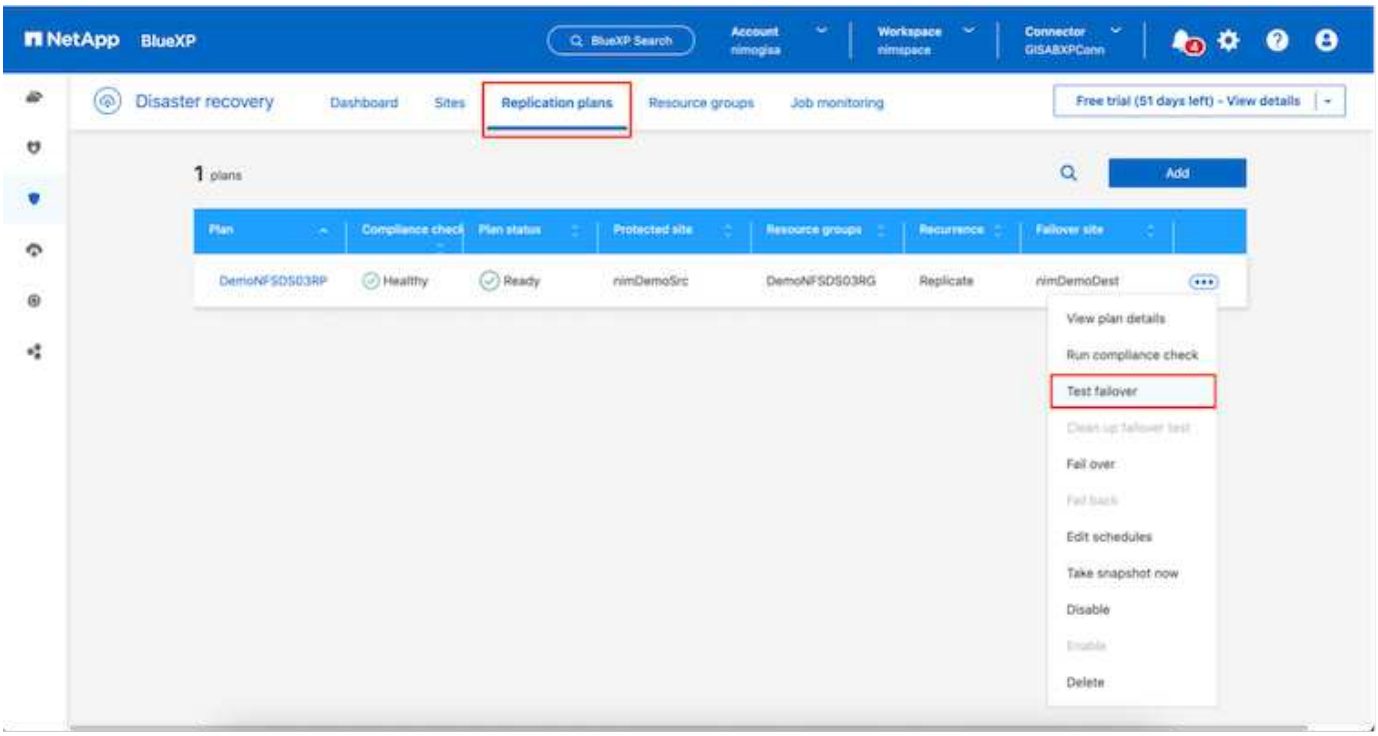


BlueXP DRaaS è costituito dai seguenti flussi di lavoro:

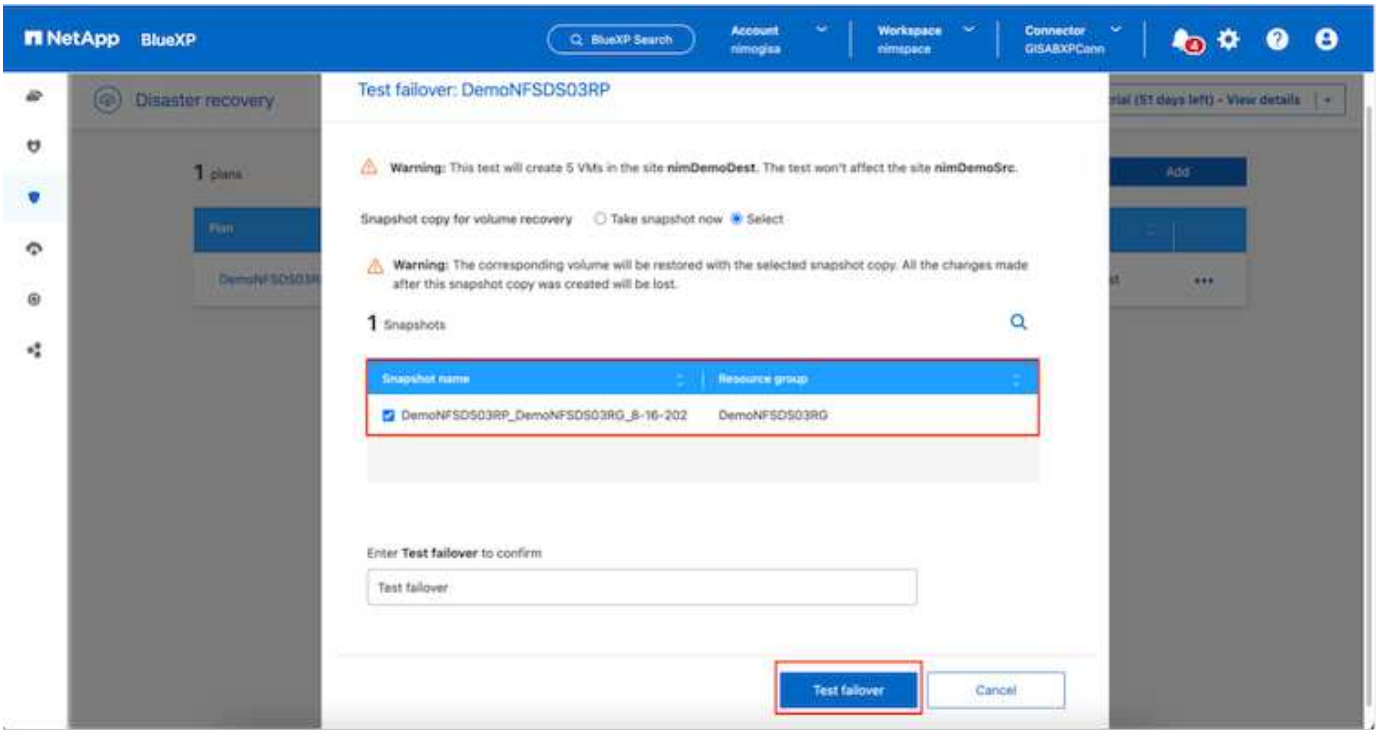
- Failover di test (incluse simulazioni automatiche periodiche)
- Test di failover di pulizia
- Failover
- Rifasamento

Failover di prova

Il failover di test in BlueXP DRaaS è una procedura operativa che consente agli amministratori VMware di convalidare completamente i propri piani di ripristino senza interrompere gli ambienti di produzione.



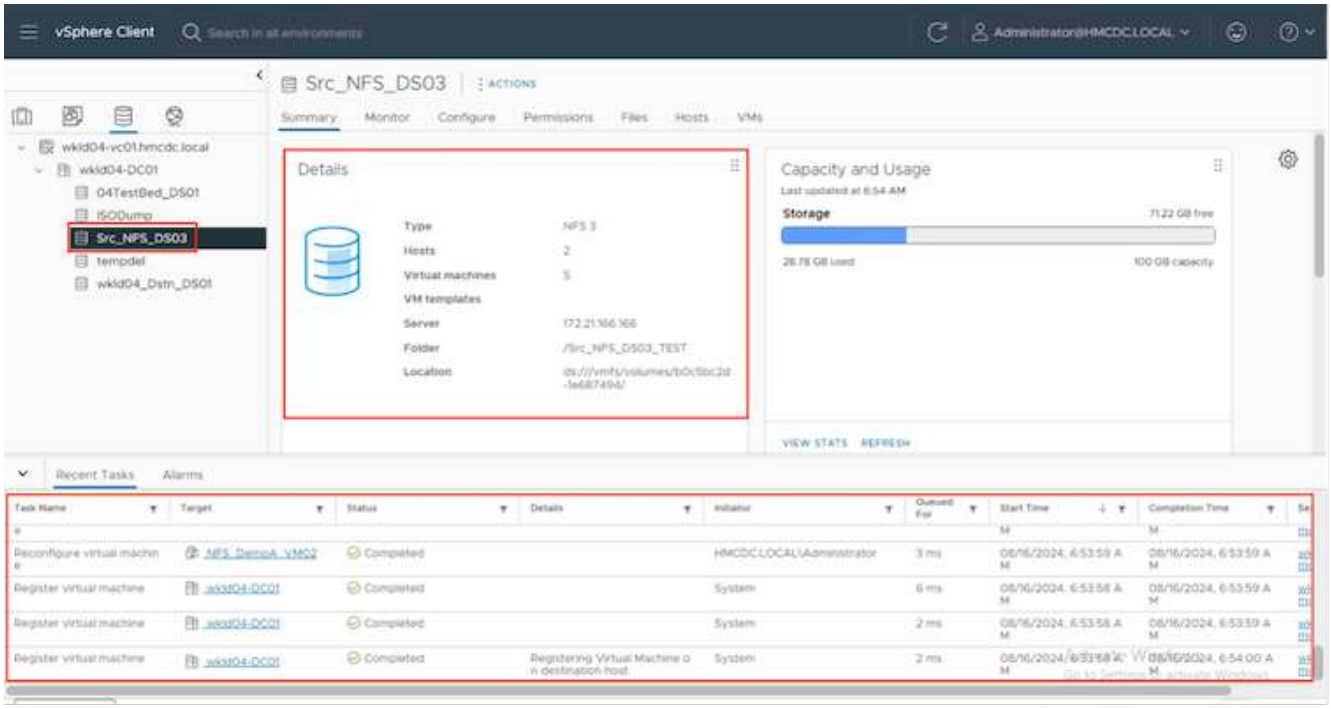
BlueXP DRaaS incorpora la possibilità di selezionare lo snapshot come funzionalità opzionale nell'operazione di failover di test. Questa funzionalità consente all'amministratore VMware di verificare che tutte le modifiche apportate di recente all'ambiente vengano replicate nel sito di destinazione e siano quindi presenti durante il test. Tali modifiche includono patch al sistema operativo guest della VM



Quando l'amministratore VMware esegue un'operazione di failover di prova, BlueXP DRaaS automatizza le seguenti attività:

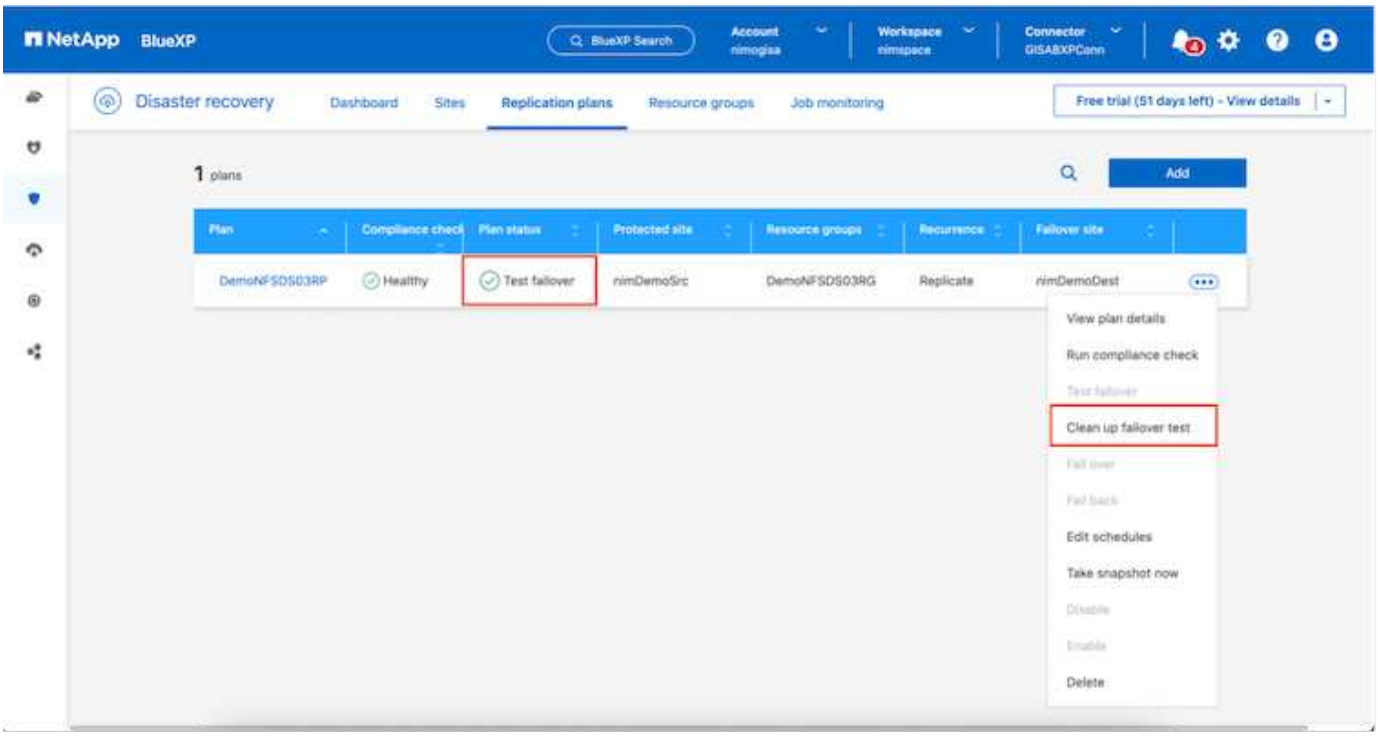
- Attivazione delle relazioni SnapMirror per aggiornare l'archiviazione nel sito di destinazione con tutte le modifiche recenti apportate nel sito di produzione.

- Creazione di volumi NetApp FlexClone dei volumi FlexVol sull'array di archiviazione DR.
- Collegamento dei datastore NFS nei volumi FlexClone agli host ESXi nel sito DR.
- Collegamento degli adattatori di rete della VM alla rete di prova specificata durante la mappatura.
- Riconfigurazione delle impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito DR.
- Esecuzione di tutti i comandi personalizzati memorizzati nel piano di replicazione.
- Accensione delle VM nell'ordine definito nel piano di replica.



Operazione di test di failover di pulizia

L'operazione di test di failover di pulizia avviene dopo il completamento del test del piano di replica e quando l'amministratore VMware risponde al prompt di pulizia.



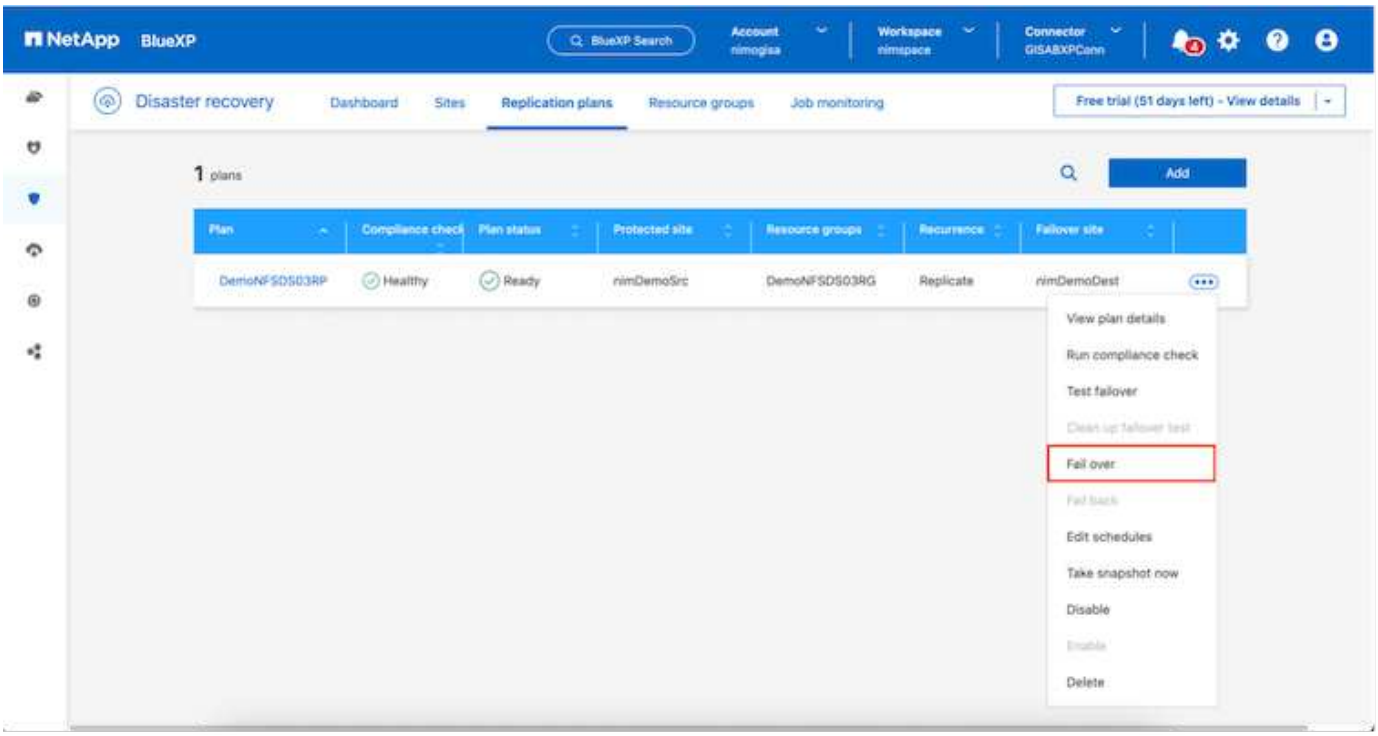
Questa azione reimposterà le macchine virtuali (VM) e lo stato del piano di replica allo stato pronto.

Quando l'amministratore VMware esegue un'operazione di ripristino, BlueXP DRaaS completa il seguente processo:

1. Spegne ogni VM recuperata nella copia FlexClone utilizzata per il test.
2. Elimina il volume FlexClone utilizzato per presentare le VM recuperate durante il test.

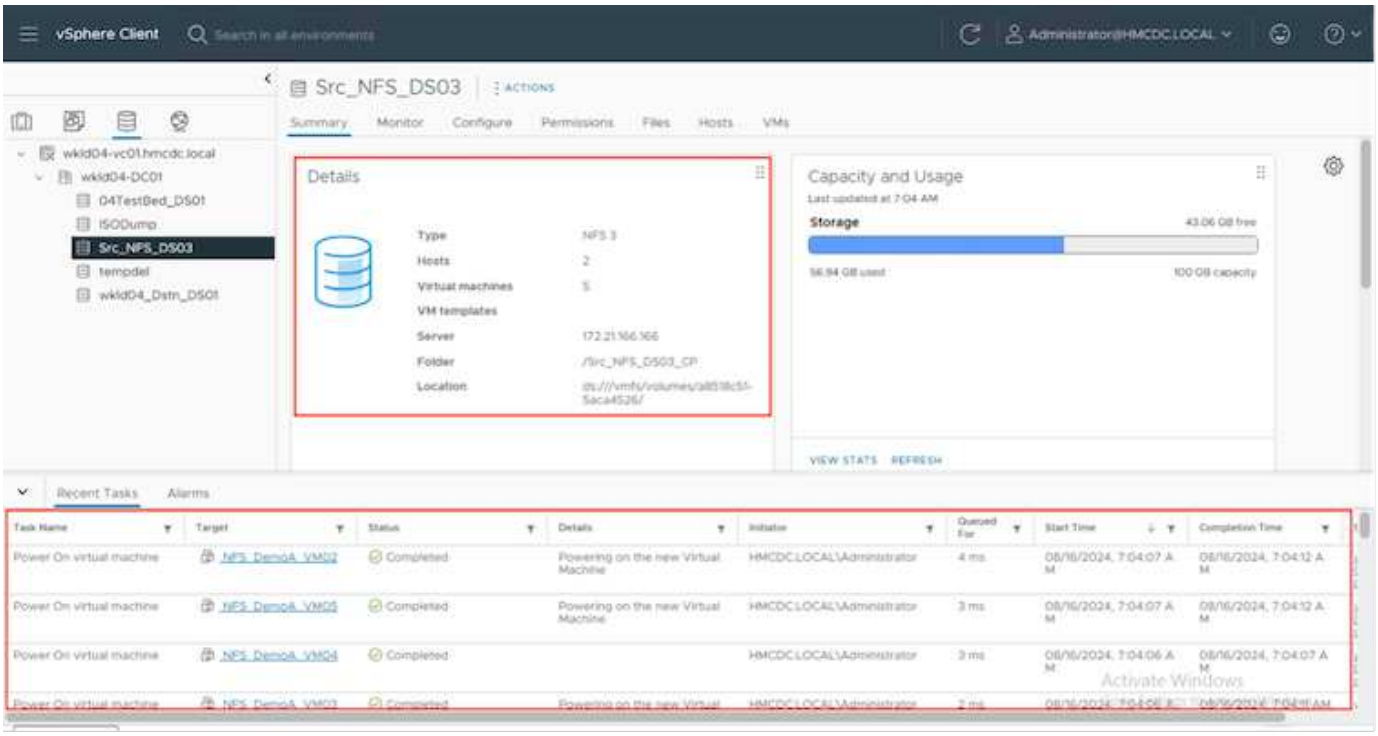
Migrazione pianificata e failover

BlueXP DRaaS dispone di due metodi per eseguire un failover reale: migrazione pianificata e failover. Il primo metodo, la migrazione pianificata, incorpora l'arresto delle VM e la sincronizzazione della replicazione dello storage nel processo per ripristinare o spostare efficacemente le VM nel sito di destinazione. La migrazione pianificata richiede l'accesso al sito di origine. Il secondo metodo, il failover, è un failover pianificato/non pianificato in cui le VM vengono ripristinate nel sito di destinazione dall'ultimo intervallo di replicazione dell'archiviazione che è stato possibile completare. A seconda dell'RPO progettato nella soluzione, è possibile che si verifichi una certa perdita di dati nello scenario DR.



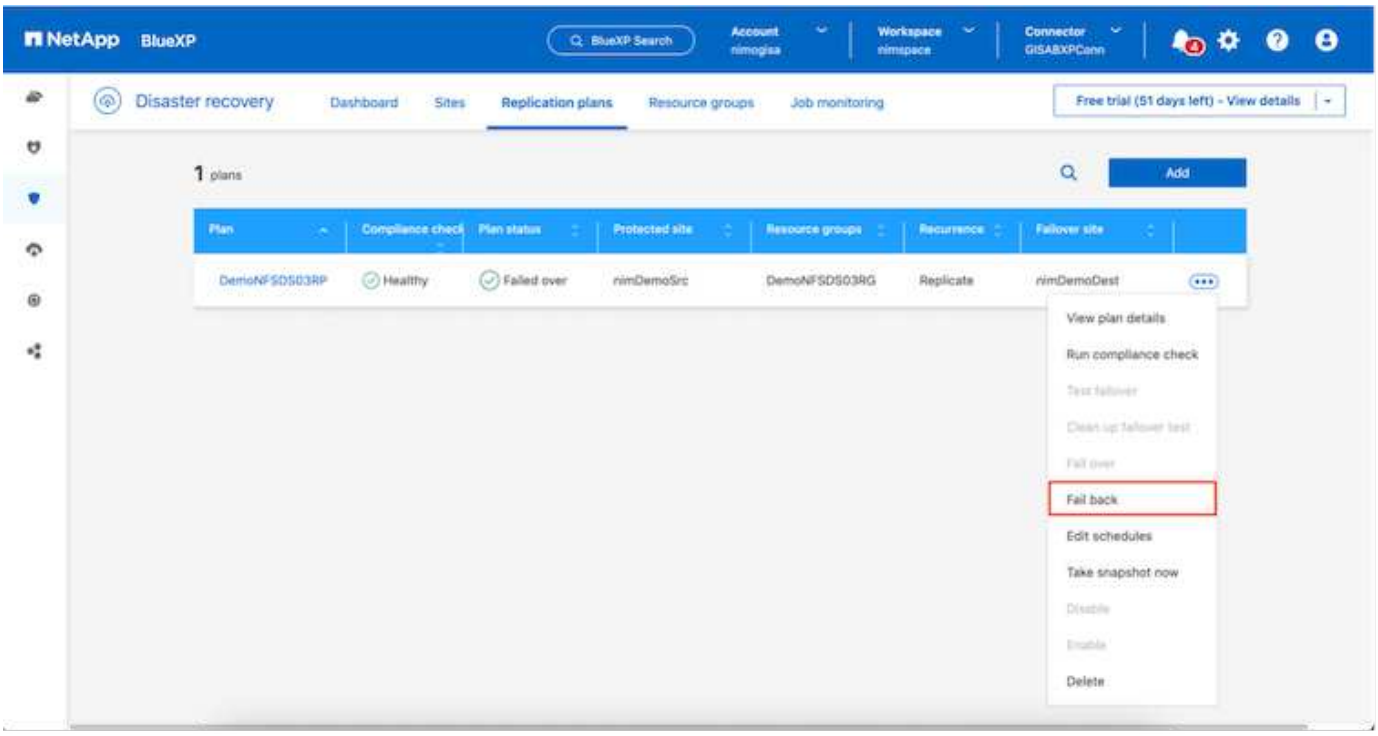
Quando l'amministratore VMware esegue un'operazione di failover, BlueXP DRaaS automatizza le seguenti attività:

- Interrompere ed eseguire il failover delle relazioni NetApp SnapMirror .
- Collegare i datastore NFS replicati agli host ESXi nel sito DR.
- Collegare gli adattatori di rete della VM alla rete del sito di destinazione appropriata.
- Riconfigurare le impostazioni di rete del sistema operativo guest della VM come definite per la rete nel sito di destinazione.
- Eseguire eventuali comandi personalizzati memorizzati nel piano di replicazione.
- Accendere le VM nell'ordine definito nel piano di replica.



Rifasamento

Un failback è una procedura facoltativa che ripristina la configurazione originale dei siti di origine e di destinazione dopo un ripristino.



Gli amministratori VMware possono configurare ed eseguire una procedura di failback quando sono pronti a ripristinare i servizi sul sito di origine.

NOTA: BlueXP DRaaS replica (risincronizza) tutte le modifiche sulla macchina virtuale di origine prima di invertire la direzione della replica. Questo processo inizia da una relazione che ha completato il failover verso

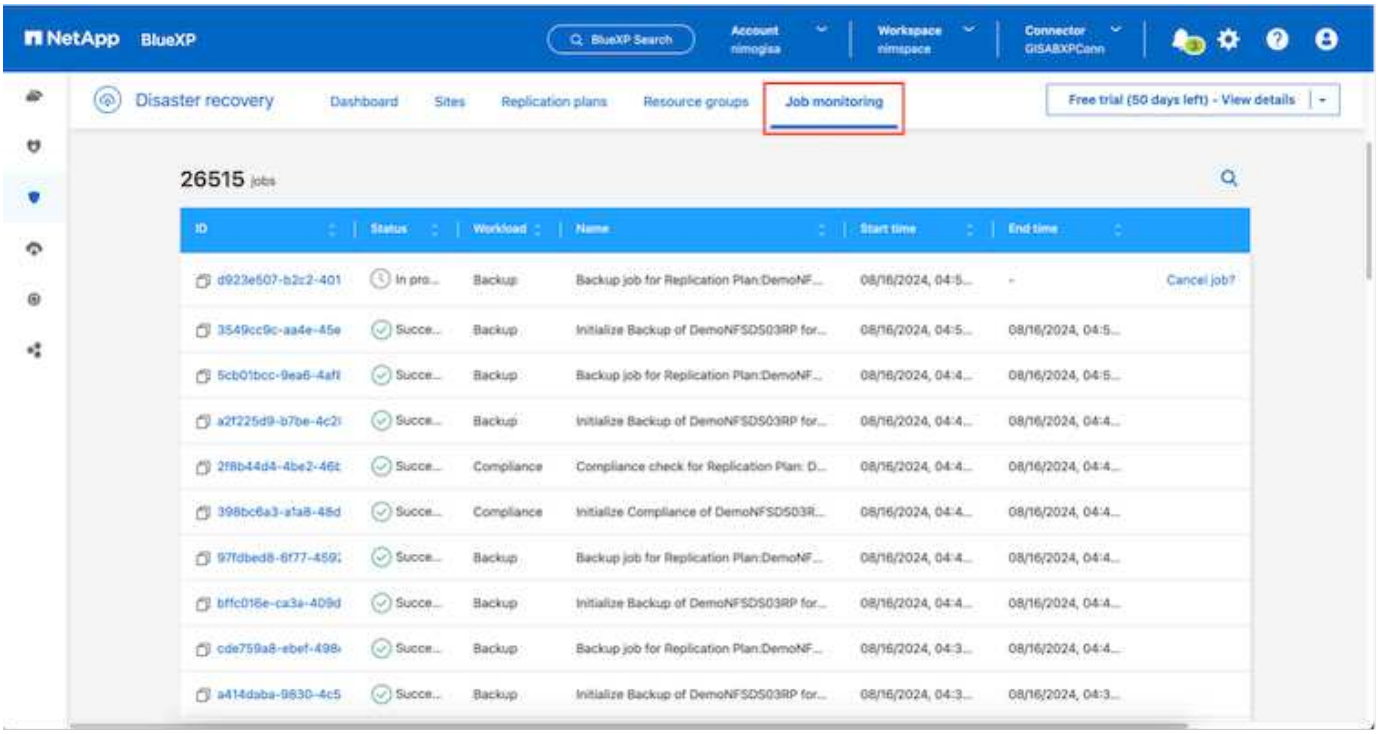
una destinazione e prevede i seguenti passaggi:

- Spegnere e annullare la registrazione delle macchine virtuali e dei volumi sul sito di destinazione.
- Interrompere la relazione SnapMirror sulla sorgente originale per renderla di lettura/scrittura.
- Risincronizzare la relazione SnapMirror per invertire la replica.
- Montare il volume sulla sorgente, accendere e registrare le macchine virtuali di origine.

Per maggiori dettagli sull'accesso e la configurazione di BlueXP DRaaS, vedere"Scopri di più su BlueXP Disaster Recovery per VMware" .

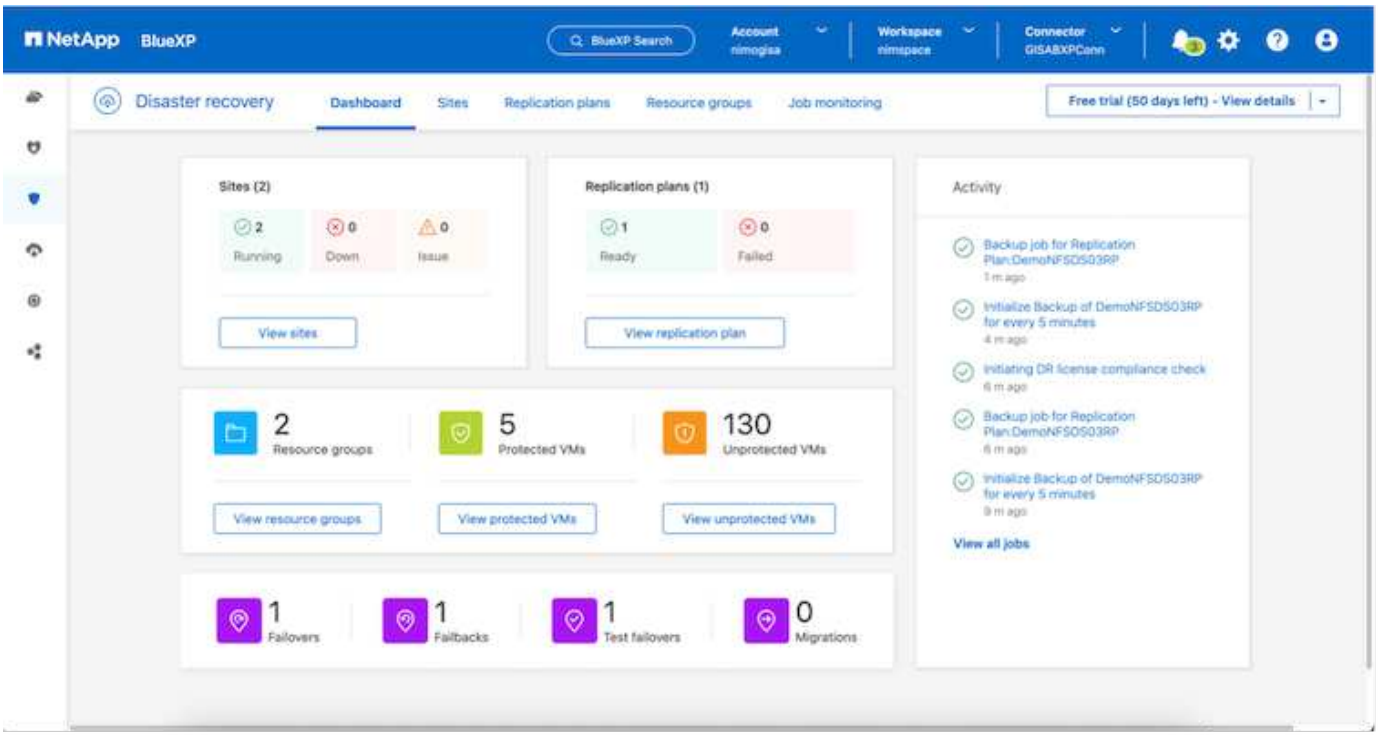
Monitoraggio e dashboard

Da BlueXP o dalla CLI ONTAP è possibile monitorare lo stato di integrità della replica per i volumi del datastore appropriati, mentre lo stato di un failover o di un failover di prova può essere monitorato tramite Job Monitoring.



Se un lavoro è in corso o in coda e si desidera interromperlo, è disponibile un'opzione per annullarlo.

Grazie alla dashboard BlueXP disaster recovery , puoi valutare con sicurezza lo stato dei siti di disaster recovery e dei piani di replica. Ciò consente agli amministratori di identificare rapidamente siti e piani integri, disconnessi o degradati.



Si tratta di una soluzione potente per gestire un piano di disaster recovery personalizzato e su misura. Il failover può essere eseguito come failover pianificato oppure con un clic su un pulsante quando si verifica un disastro e si decide di attivare il sito DR.

Per saperne di più su questo processo, sentiti libero di seguire il video dettagliato o di utilizzare il"simulatore di soluzioni" .

Proteggi i carichi di lavoro con vSphere Metro Storage Cluster

Scopri come integrare l'alta disponibilità ONTAP con VMware vSphere Metro Storage Cluster (vMSC)

Scopri le soluzioni NetApp che puoi utilizzare per integrare l'elevata disponibilità NetApp ONTAP con VMware vSphere Metro Storage Cluster (vMSC). Ciò fornisce soluzioni robuste per la gestione di VMware Cloud Foundation (VCF) e per i domini dei carichi di lavoro VI.

Questa combinazione garantisce la disponibilità continua dei dati, il failover senza interruzioni e il disaster recovery in siti geograficamente dispersi, migliorando la resilienza e la continuità operativa per i carichi di lavoro critici. La sincronizzazione attiva SnapMirror 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. Non è necessario alcun intervento manuale o scripting personalizzato per attivare un failover con ActiveSync SnapMirror .

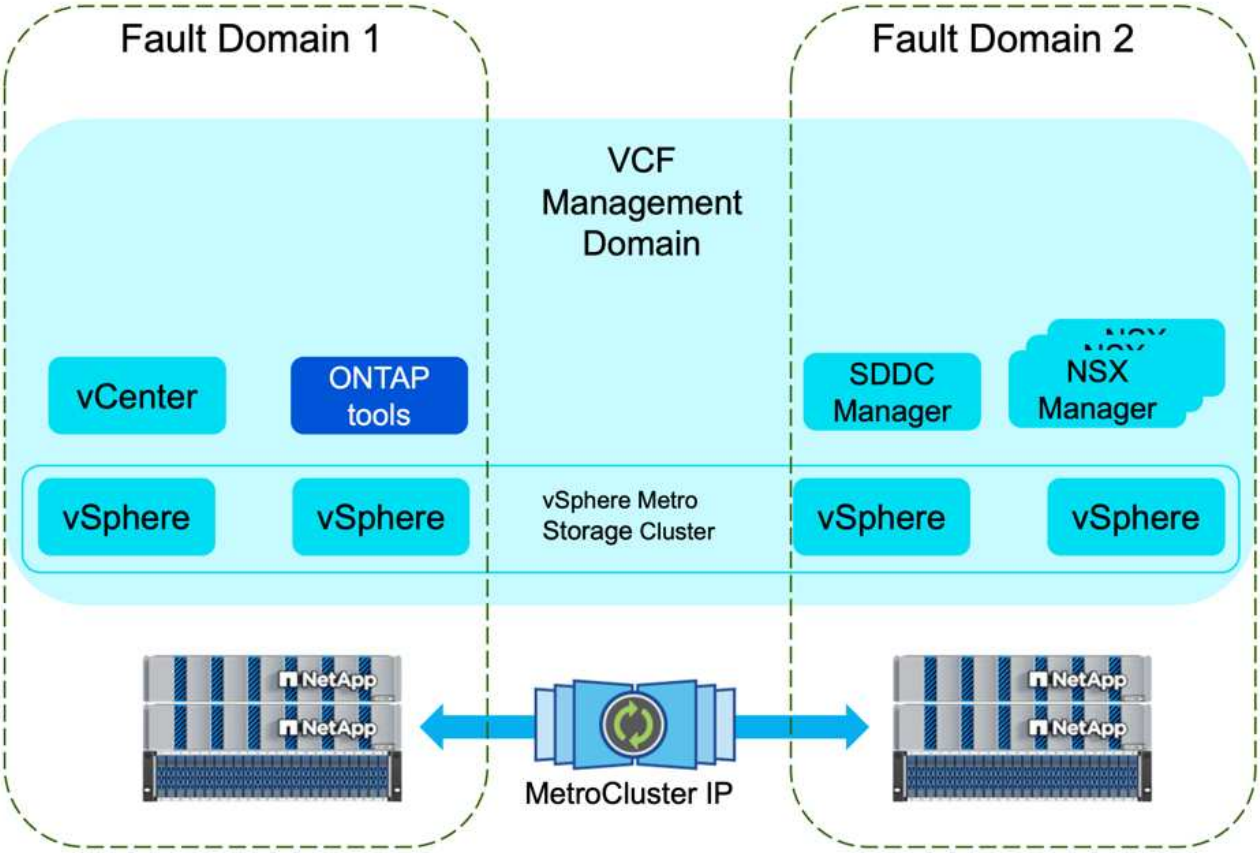
Per maggiori dettagli fare riferimento alle seguenti soluzioni.

- "Cluster esteso per dominio di gestione mediante sincronizzazione attiva SnapMirror"
- "Cluster esteso per dominio di gestione tramite MetroCluster"

- "Cluster esteso per dominio del carico di lavoro VI utilizzando SnapMirror ActiveSync"
- "Stretch Cluster per il dominio del carico di lavoro VI utilizzando MetroCluster"

Configurare un cluster esteso per un dominio di gestione VCF utilizzando MetroCluster

In questo caso d'uso descriviamo la procedura per configurare un cluster esteso per il dominio di gestione VMware Cloud Foundation (VCF) utilizzando ONTAP MetroCluster con NFS come datastore primario. Questa procedura include la distribuzione di host vSphere e vCenter Server, il provisioning di datastore NFS, la convalida del cluster con VCF Import Tool, la configurazione delle impostazioni NSX e la conversione dell'ambiente in un dominio di gestione VCF.



Introduzione

In questa soluzione mostreremo come implementare Stretched VCF Management Domain con NFS come Principal Datastore utilizzando ONTAP MetroCluster.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci host vSphere e server vCenter.
- Fornire il datastore NFS agli host vSphere.

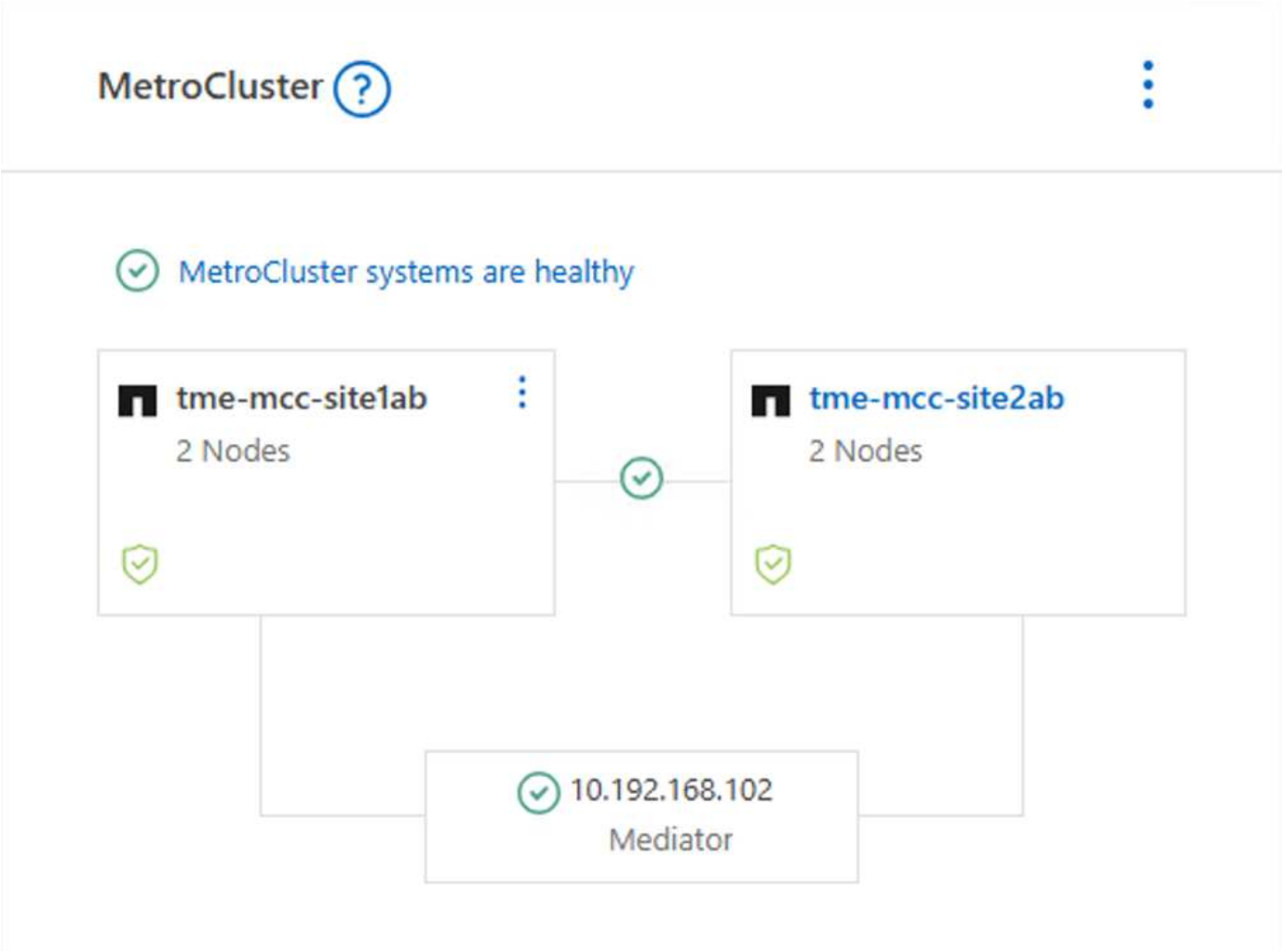
- Distribuire SDDC Manager nel cluster vSphere.
- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.
- Configurare un file JSON per creare un NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per convertire l'ambiente vSphere 8 in un dominio di gestione VCF.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Configurazione ONTAP MetroCluster supportata
- Macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi connessi allo switch di rete.
- Scarica il software necessario per la conversione VCF.

Ecco uno screenshot di esempio di System Manager che mostra la configurazione MetroCluster
.



ed ecco le interfacce di rete SVM da entrambi i domini di errore.

Network interfaces Subnets

+ Add

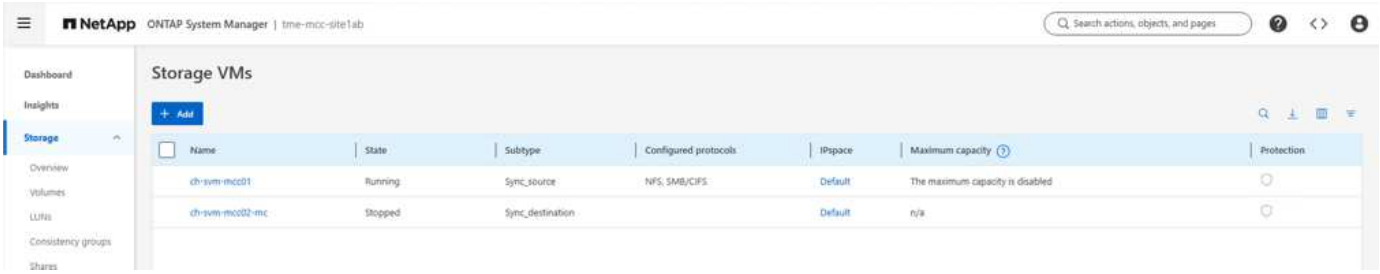
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

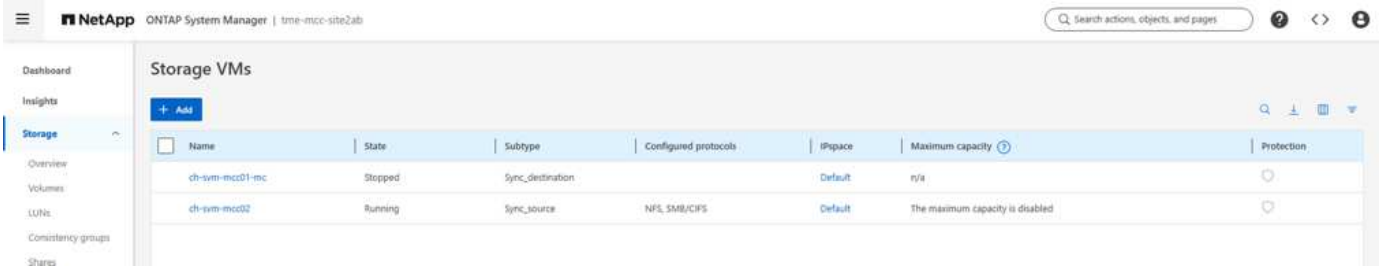
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] SVM sarà attivo su uno dei domini di errore in MetroCluster.





Fare riferimento "vMSC con MetroCluster" .

Per l'archiviazione supportata e altre considerazioni per la conversione o l'importazione di vSphere in VCF 5.2, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Prima di creare un cluster vSphere che verrà convertito in VCF Management Domain, fare riferimento "Considerazioni NSX su vSphere Cluster"

Per il software richiesto fare riferimento a "Scarica il software per convertire o importare ambienti vSphere esistenti" .

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" .

Fasi di distribuzione

Per distribuire VCF Stretched Management Domain con NFS come Principal Datastore,

Completare i seguenti passaggi:

- Distribuisci host vSphere e vCenter.
- Creare un cluster vSphere.
- Fornire un datastore NFS.
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Distribuire la VM del gestore SDDC sul cluster vCenter.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di conversione.
- Caricare il software richiesto nel gestore SDDC.
- Convertire il cluster vSphere in un dominio di gestione VCF.

Per una panoramica del processo di conversione, fare riferimento a "Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation" .

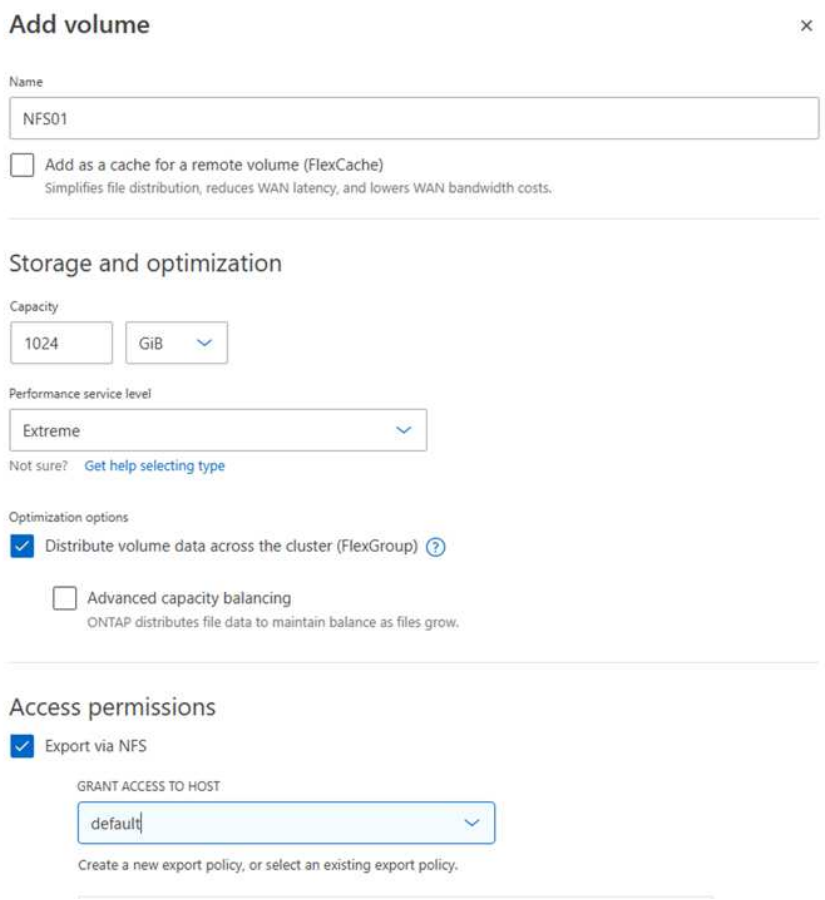
Distribuisci host vSphere e vCenter

Distribuisci vSphere sugli host utilizzando l'ISO scaricato dal portale di supporto Broadcom oppure utilizza l'opzione di distribuzione esistente per l'host vSphere.

Montare NFS Datastore per ospitare le VM

In questo passaggio creiamo il volume NFS e lo montiamo come Datastore per ospitare le VM.

1. Utilizzando System Manager, creare un volume e collegarlo alla policy di esportazione che includa la subnet IP dell'host vSphere.



2. Eseguire l'SSH sull'host vSphere e montare il datastore NFS.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

3. Ripetere i passaggi precedenti per ogni ulteriore necessità di datastore e assicurarsi che l'accelerazione hardware sia supportata.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~]
```

Distribuisci vCenter su NFS Datastore. Assicurarsi che SSH e Bash shell siano abilitati sull'appliance vCenter.

Crea un cluster vSphere

1. Accedi al client Web vSphere, crea il DataCenter e il cluster vSphere aggiungendo uno degli host in cui è distribuito NFS VAAI. Abbiamo scelto di gestire tutti gli host nel cluster con l'opzione immagine singola. [SUGGERIMENTO] Non selezionare Gestisci configurazione a livello di cluster. Per ulteriori dettagli, fare riferimento "Considerazioni NSX su vSphere Cluster" . Per le best practice vMSC con ONTAP MetroCluster, controlla "Linee guida per la progettazione e l'implementazione di vMSC"
2. Aggiungere altri host vSphere al cluster.
3. Creare uno switch distribuito e aggiungere i gruppi di porte.
4. "Migrazione della rete da vSwitch standard a switch distribuito."

Convertire l'ambiente vSphere in un dominio di gestione VCF

Nella sezione seguente vengono illustrati i passaggi per distribuire il gestore SDDC e convertire il cluster vSphere 8 in un dominio di gestione VCF 5.2. Se del caso, per ulteriori dettagli si farà riferimento alla documentazione VMware.

VCF Import Tool, di VMware by Broadcom, è un'utilità utilizzata sia sull'appliance vCenter che sul gestore SDDC per convalidare le configurazioni e fornire servizi di conversione e importazione per gli ambienti vSphere e VCF.

Per ulteriori informazioni, consulta "Opzioni e parametri dello strumento di importazione VCF" .

Copia ed estrai lo strumento di importazione VCF

Lo strumento di importazione VCF viene utilizzato sull'appliance vCenter per convalidare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

1. Segui i passaggi a "Copia lo strumento di importazione VCF nell'appliance vCenter di destinazione" in VMware Docs per copiare lo strumento di importazione VCF nella posizione corretta.
2. Estrarre il bundle utilizzando il seguente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Convalida l'appliance vCenter

Utilizzare lo strumento di importazione VCF per convalidare l'appliance vCenter prima della conversione.

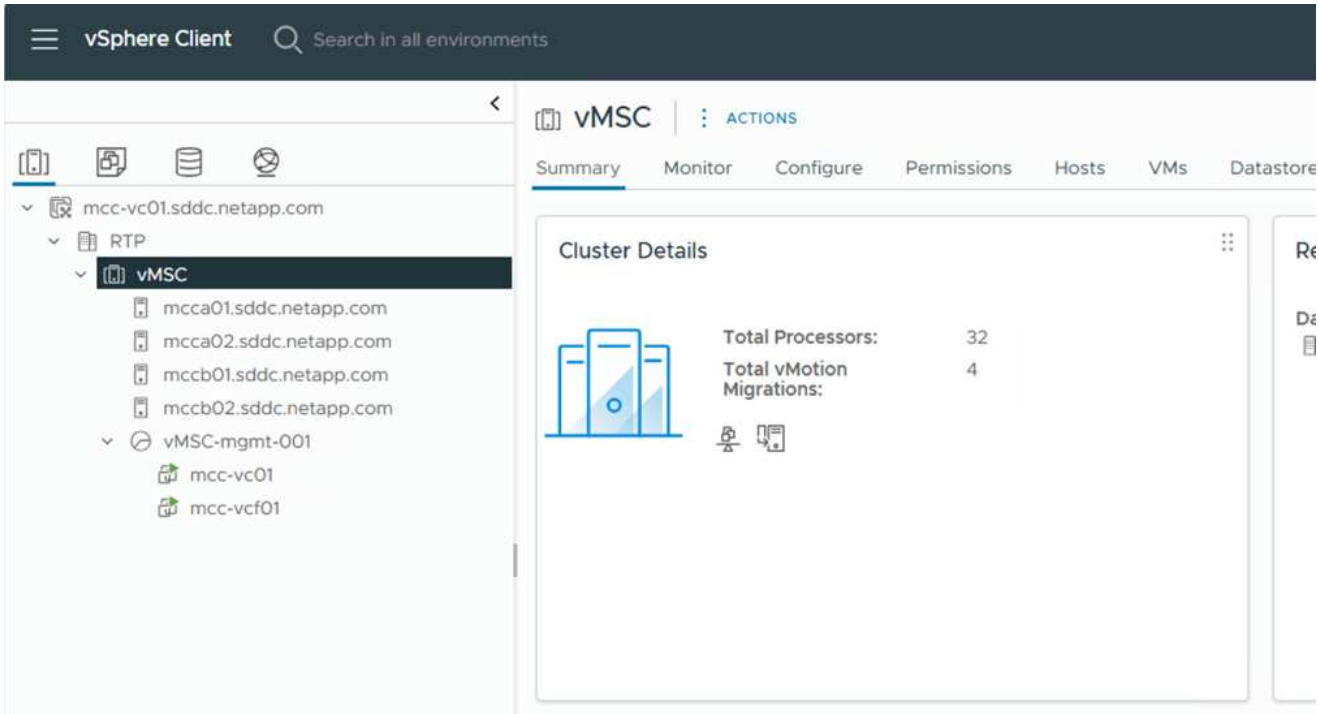
1. Segui i passaggi a "Eseguire un controllo preliminare sul vCenter di destinazione prima della conversione" per eseguire la convalida.
2. L'output seguente mostra che l'appliance vCenter ha superato il controllo preliminare.

```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

Distribuire SDDC Manager

Il gestore SDDC deve essere collocato sul cluster vSphere che verrà convertito in un dominio di gestione VCF.

Per completare la distribuzione, seguire le istruzioni di distribuzione in VMware Docs.



Fare riferimento a "Distribuire l'appliance SDDC Manager sul vCenter di destinazione" .

Creare un file JSON per la distribuzione NSX

Per distribuire NSX Manager durante l'importazione o la conversione di un ambiente vSphere in VMware Cloud Foundation, creare una specifica di distribuzione NSX. Per la distribuzione di NSX sono necessari almeno 3 host.

> Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzato il segmento supportato da NSX VLAN. Per maggiori dettagli sulle limitazioni del segmento supportato da NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Di seguito è riportato un esempio di file JSON per la distribuzione NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copiare il file JSON nella cartella home dell'utente vcf su SDDC Manager.

Carica il software su SDDC Manager

Copiare lo strumento di importazione VCF nella cartella home dell'utente vcf e il bundle di distribuzione NSX nella cartella /nfs/vmware/vcf/nfs-mount/bundle/ su SDDC Manager.

Vedere "Caricare il software richiesto sull'appliance SDDC Manager" per istruzioni dettagliate.

Controllo dettagliato su vCenter prima della conversione

Prima di eseguire un'operazione di conversione del dominio di gestione o un'operazione di importazione del dominio del carico di lavoro VI, è necessario eseguire un controllo dettagliato per assicurarsi che la configurazione dell'ambiente vSphere esistente sia supportata per la conversione o l'importazione. . Eseguire l'accesso SSH all'appliance SDDC Manager come utente vcf. . Passare alla directory in cui è stato copiato lo strumento di importazione VCF. . Eseguire il seguente comando per verificare che l'ambiente vSphere possa essere convertito

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

Convertire il cluster vSphere in dominio di gestione VCF

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF.

Per convertire il cluster vSphere in un dominio di gestione VCF e distribuire il cluster NSX, eseguire il comando seguente:

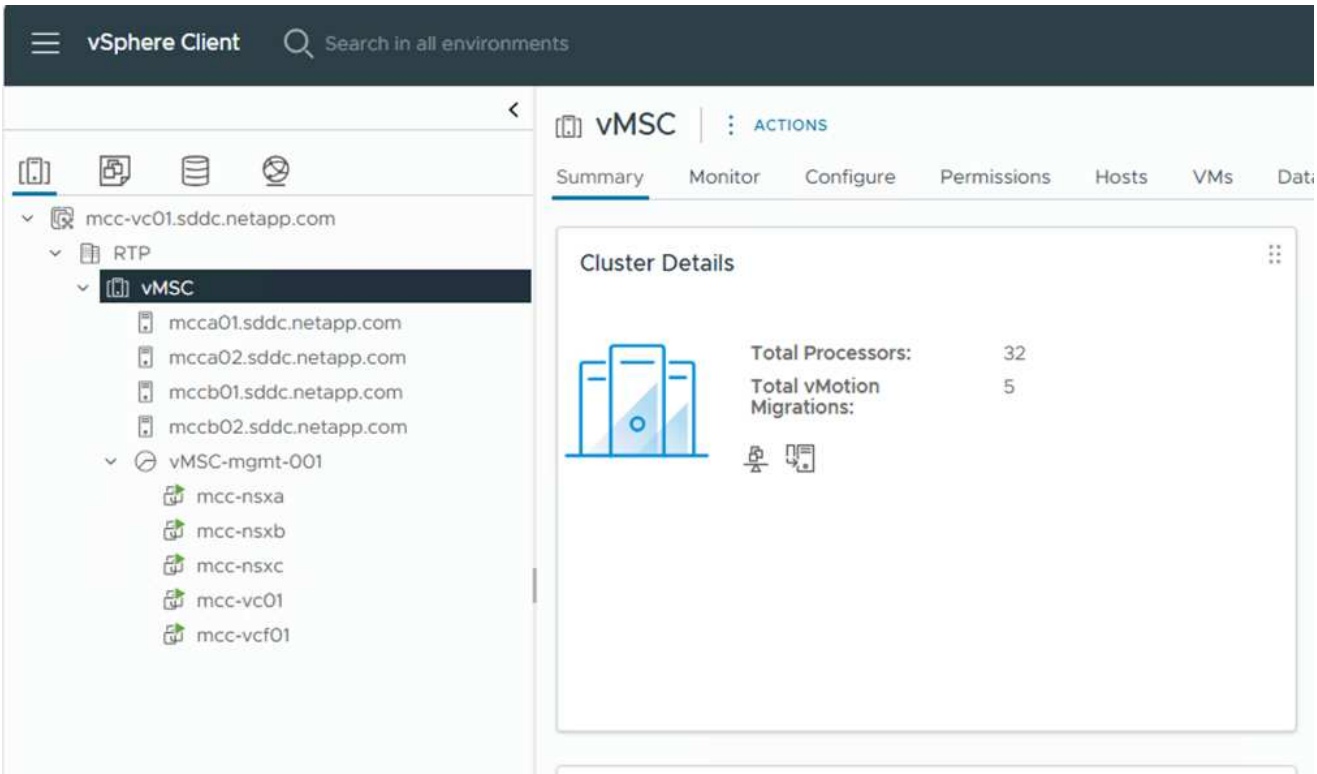
```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

Quando sull'host vSphere sono disponibili più Datastore, viene richiesto quale Datastore deve essere considerato come Datastore primario su quali VM NSX verranno distribuite per impostazione predefinita.

```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

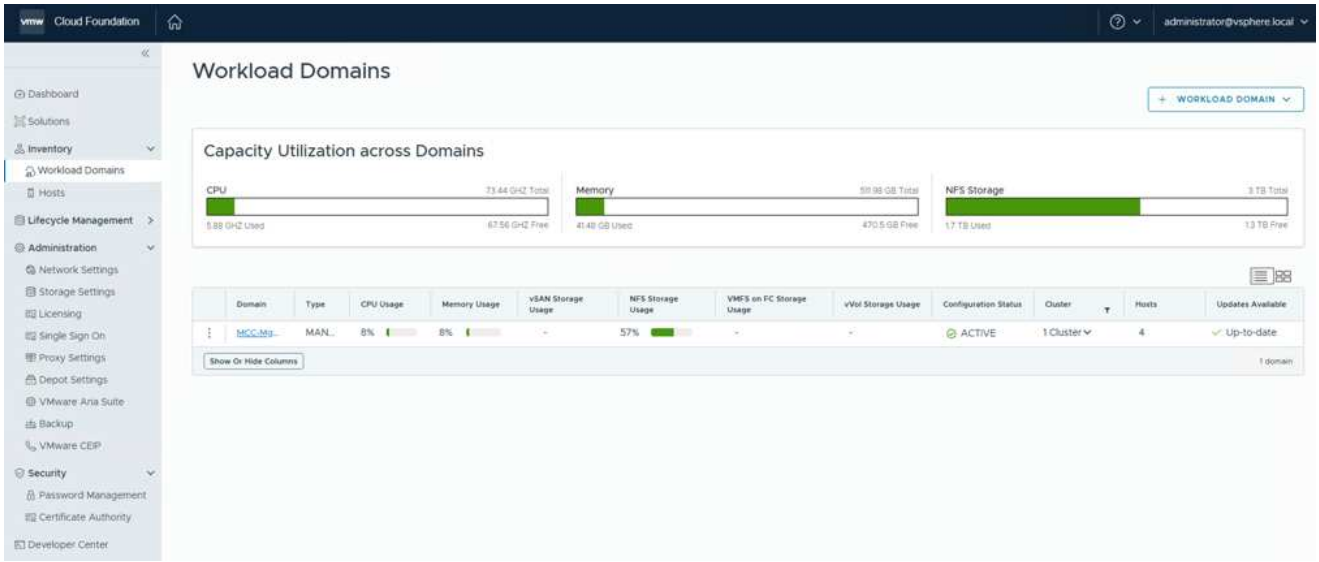
Per istruzioni complete, fare riferimento a "Procedura di conversione VCF" .

Le VM NSX verranno distribuite su vCenter.

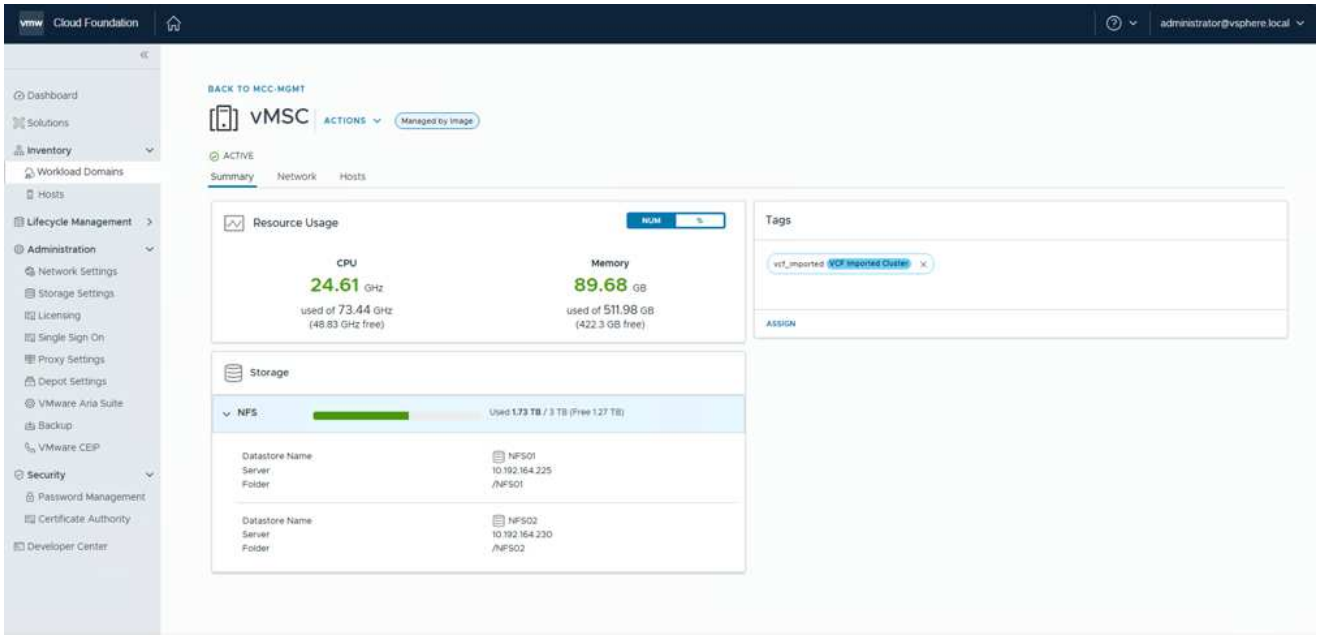


SDDC Manager mostra il dominio di gestione creato con il nome fornito e NFS come

Datastore.



Durante l’ispezione del cluster, vengono fornite le informazioni del datastore NFS.



Aggiungere la licenza al VCF

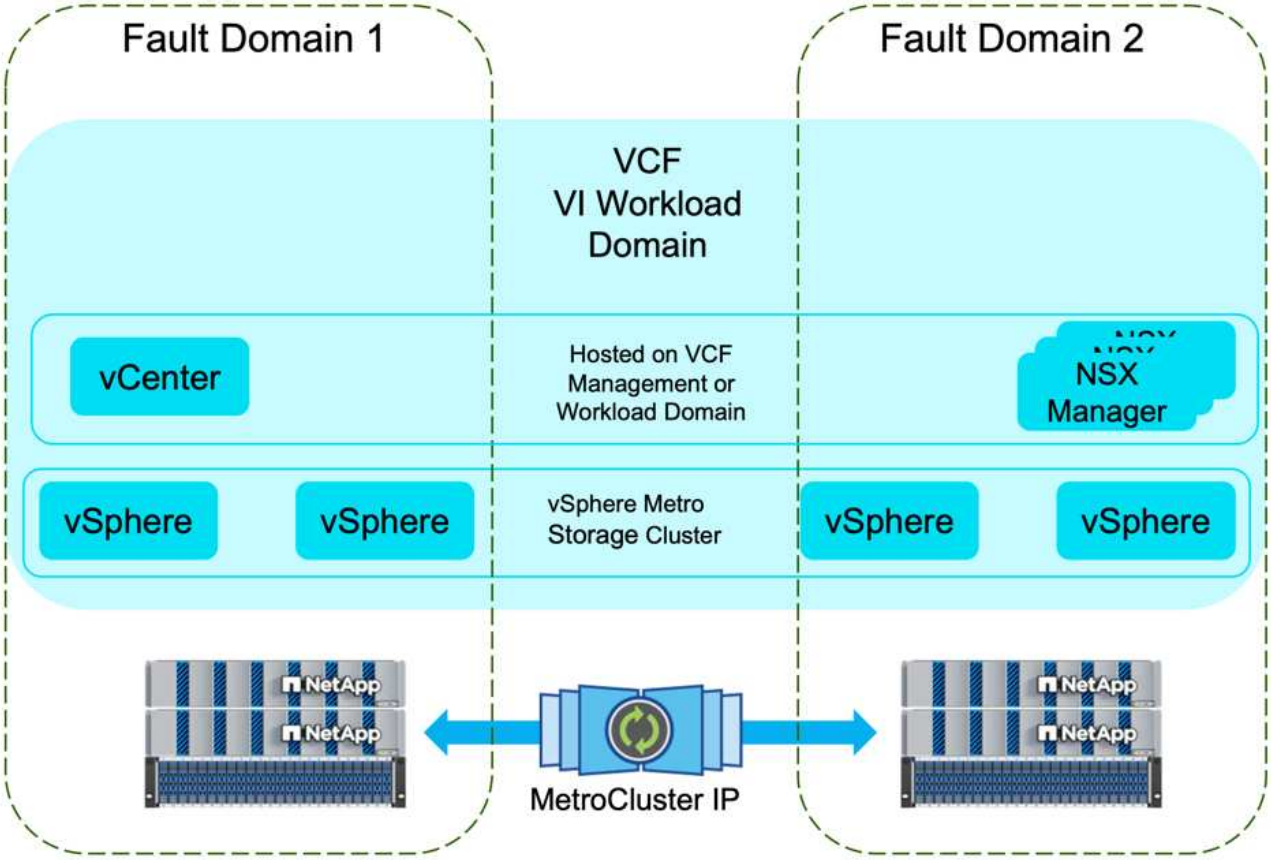
Dopo aver completato la conversione, è necessario aggiungere la licenza all'ambiente.

1. Accedi all'interfaccia utente di SDDC Manager.
2. Nel riquadro di navigazione, vai su **Amministrazione > Licenze**.
3. Fare clic su **+ Chiave di licenza**.
4. Scegli un prodotto dal menu a discesa.
5. Inserisci la chiave di licenza.
6. Fornire una descrizione della licenza.
7. Fare clic su **Aggiungi**.
8. Ripetere questi passaggi per ogni licenza.

Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando MetroCluster

In questo caso d'uso descriviamo la procedura per configurare il dominio del carico di lavoro VCF VI esteso con NFS come datastore principale utilizzando ONTAP MetroCluster. Questa procedura include la distribuzione di host vSphere e vCenter Server, il provisioning di datastore NFS, la convalida del cluster vSphere, la configurazione di NSX durante la conversione VCF e l'importazione dell'ambiente vSphere in un dominio di gestione VCF esistente.

I carichi di lavoro su VCF sono protetti da vSphere Metro Storage Cluster (vMSC). ONTAP MetroCluster con distribuzione FC o IP viene in genere utilizzato per garantire la tolleranza agli errori dei datastore VMFS e NFS.



Introduzione

In questa soluzione mostreremo come implementare il dominio del carico di lavoro VCF VI esteso con NFS come datastore principale utilizzando ONTAP MetroCluster. Il dominio del carico di lavoro VI può essere distribuito tramite SDDC Manager oppure importando un ambiente vSphere esistente come dominio del carico di lavoro VI.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci host vSphere e server vCenter.
- Fornire il datastore NFS agli host vSphere.
- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.
- Configurare un file JSON per creare un NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per importare l'ambiente vSphere 8 come dominio del carico di lavoro VCF VI in un dominio di gestione VCF esistente.

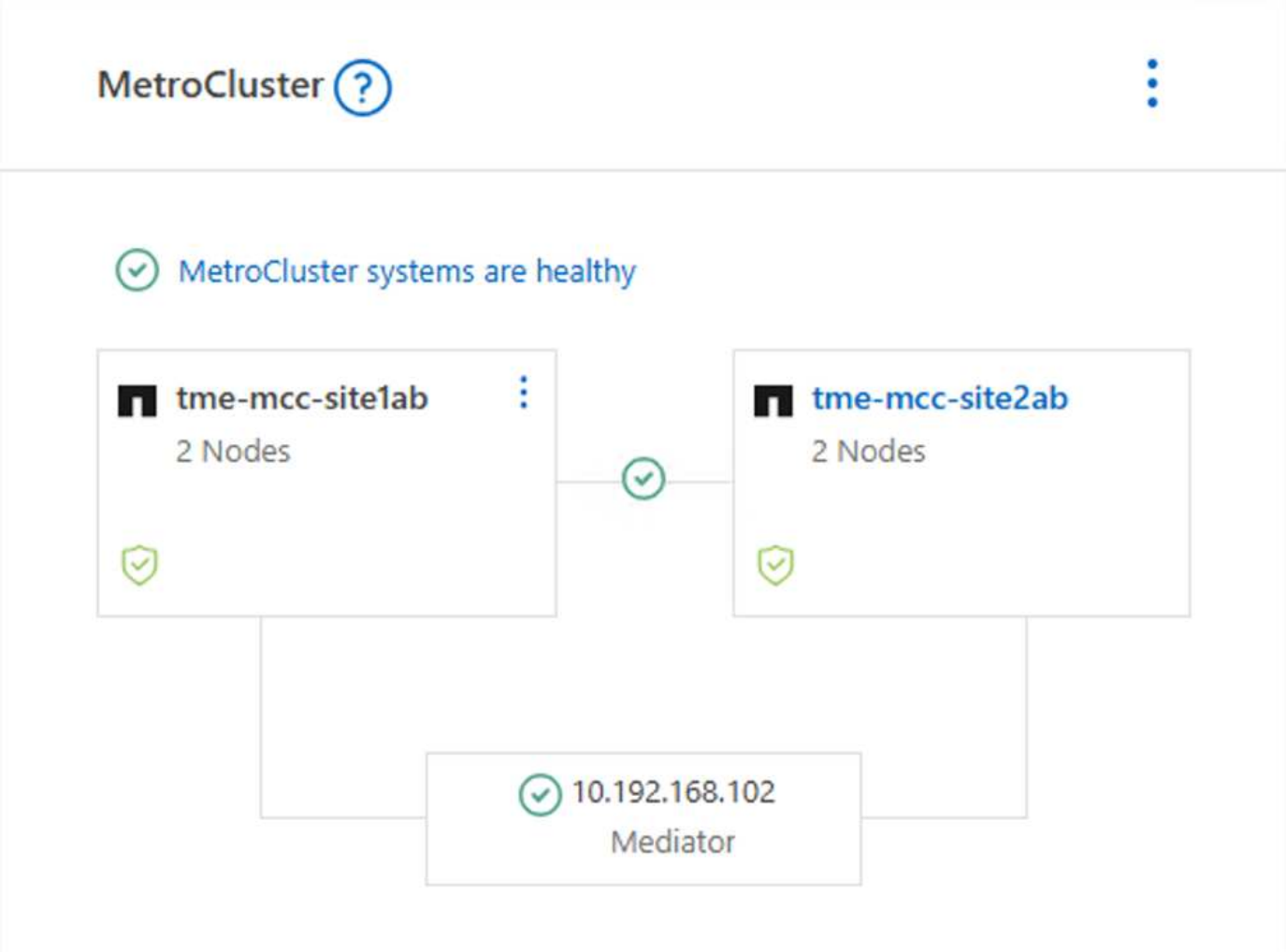
Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Configurazione ONTAP MetroCluster supportata

- Macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi connessi allo switch di rete.
- Scarica il software necessario per la conversione VCF.

Ecco uno screenshot di esempio di System Manager che mostra la configurazione MetroCluster
.



ed ecco le interfacce di rete SVM da entrambi i domini di errore.

Network interfaces Subnets

+ Add

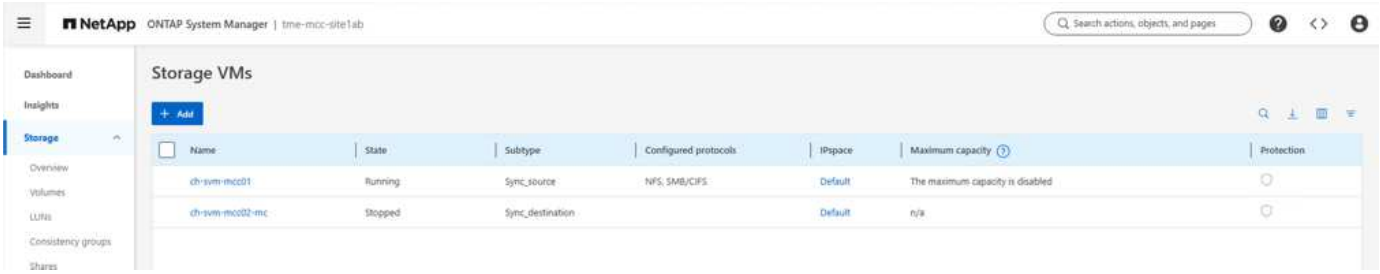
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

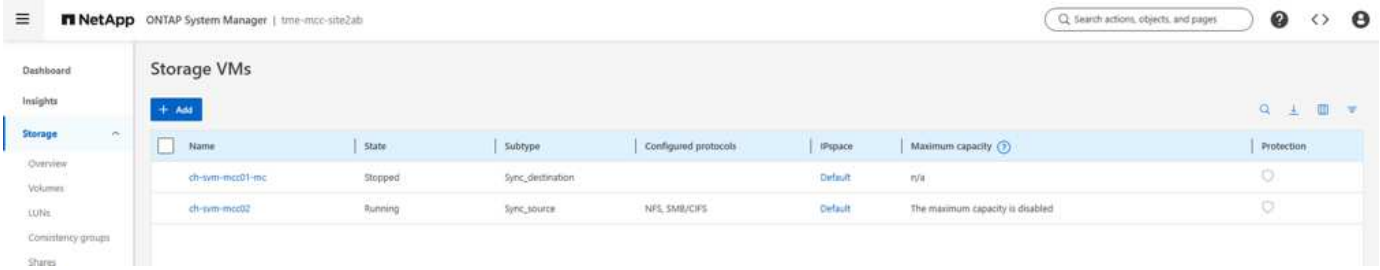
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] SVM sarà attivo su uno dei domini di errore in MetroCluster.





Fare riferimento "vMSC con MetroCluster" .

Per l'archiviazione supportata e altre considerazioni per la conversione o l'importazione di vSphere in VCF 5.2, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Prima di creare un cluster vSphere che verrà convertito in VCF Management Domain, fare riferimento "Considerazioni NSX su vSphere Cluster"

Per il software richiesto fare riferimento a "Scarica il software per convertire o importare ambienti vSphere esistenti" .

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" .

Fasi di distribuzione

Per distribuire VCF Stretched Management Domain con NFS come Principal Datastore,

Completare i seguenti passaggi:

- Distribuisci host vSphere e vCenter.
- Creare un cluster vSphere.
- Fornire un datastore NFS.
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di importazione.
- Caricare il software richiesto nel gestore SDDC.
- Convertire il cluster vSphere in un dominio di carico di lavoro VCF VI.

Per una panoramica del processo di conversione, fare riferimento a "Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation" .

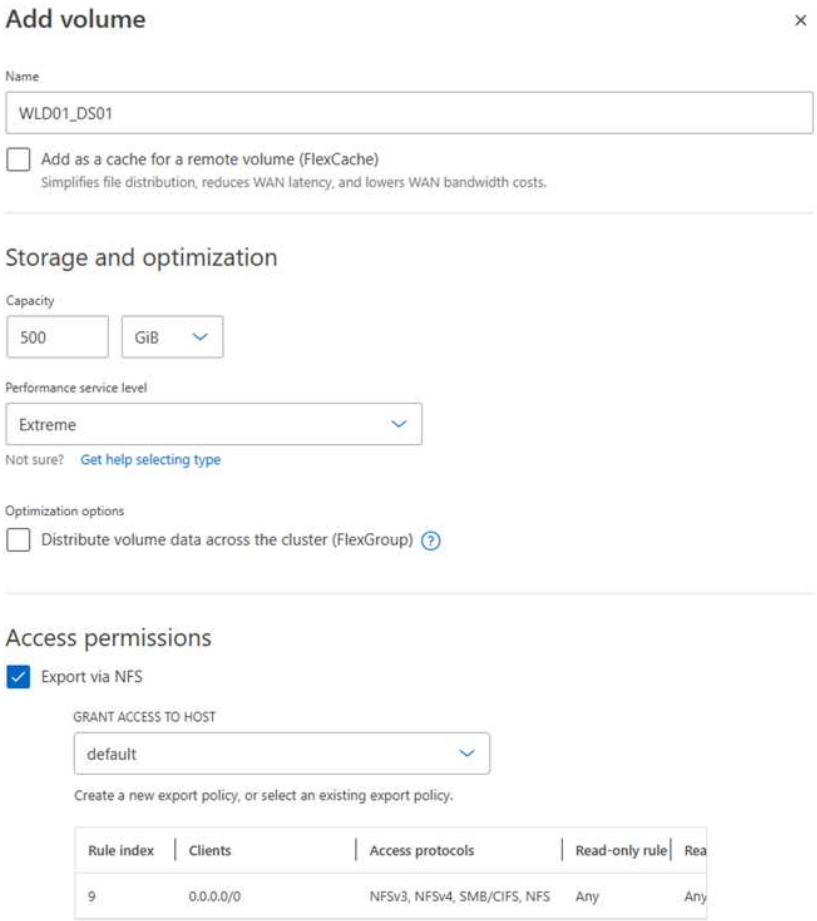
Distribuisci host vSphere e vCenter

Distribuisci vSphere sugli host utilizzando l'ISO scaricato dal portale di supporto Broadcom oppure utilizza l'opzione di distribuzione esistente per l'host vSphere.

Montare NFS Datastore per ospitare le VM

In questo passaggio creiamo il volume NFS e lo montiamo come Datastore per ospitare le VM.

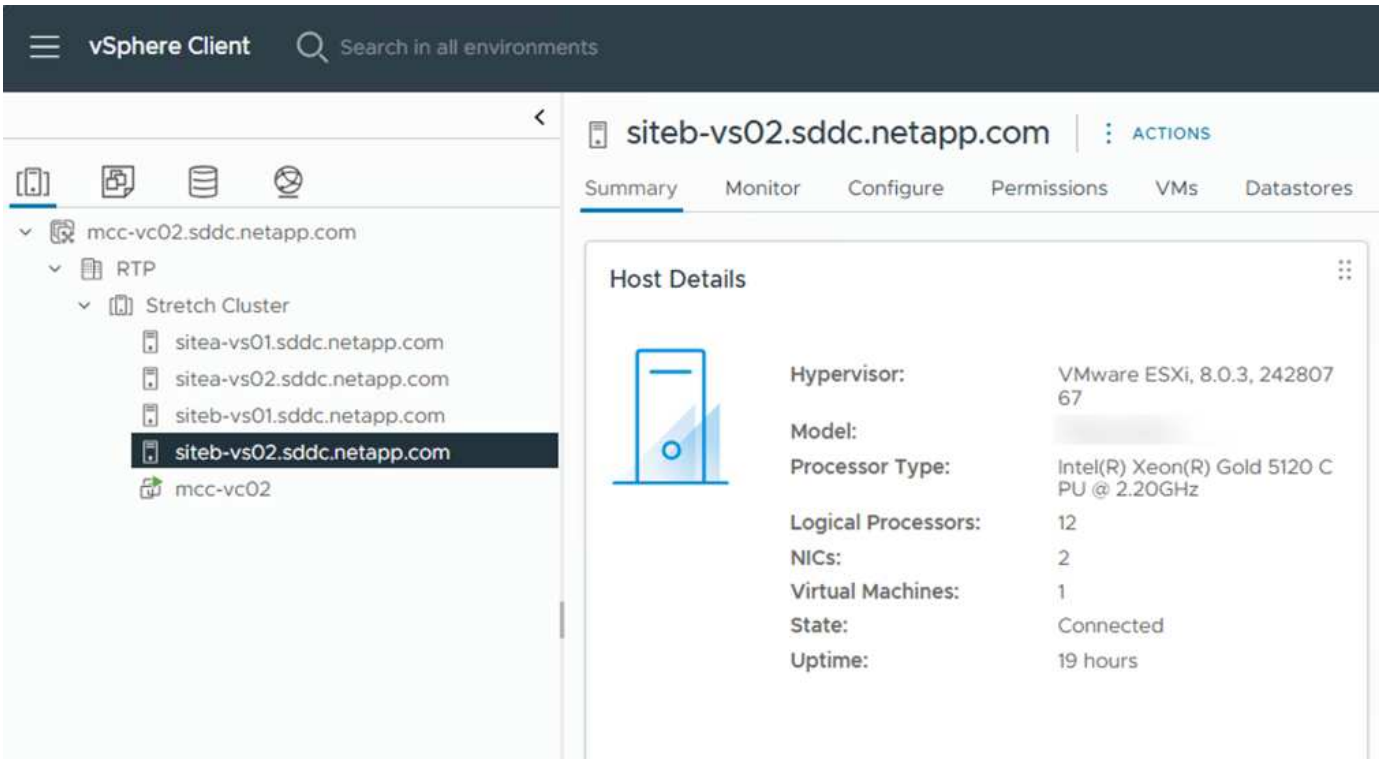
1. Utilizzando System Manager, creare un volume e collegarlo alla policy di esportazione che includa la subnet IP dell'host
vSphere.



2. Eseguire l'SSH sull'host vSphere e montare il datastore NFS.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

Distribuisci vCenter su NFS Datastore. Assicurarsi che SSH e Bash shell siano abilitati sull'appliance vCenter.



Crea un cluster vSphere

1. Accedi al webclient vSphere, crea il DataCenter e il cluster vSphere aggiungendo uno degli host in cui è distribuito NFS VAAI. Abbiamo scelto di gestire tutti gli host nel cluster con l'opzione immagine singola. [SUGGERIMENTO] Non selezionare Gestisci configurazione a livello di cluster. Per ulteriori dettagli, fare riferimento "Considerazioni NSX su vSphere Cluster" . Per le best practice vMSC con ONTAP MetroCluster, controlla "Linee guida per la progettazione e l'implementazione di vMSC"
2. Aggiungere altri host vSphere al cluster.
3. Creare uno switch distribuito e aggiungere i gruppi di porte.
4. "Migrazione della rete da vSwitch standard a switch distribuito."

Convertire l'ambiente vSphere in un dominio di carico di lavoro VCF VI

Nella sezione seguente vengono illustrati i passaggi per distribuire il gestore SDDC e convertire il cluster vSphere 8 in un dominio di gestione VCF 5.2. Se del caso, per ulteriori dettagli si farà riferimento alla documentazione VMware.

VCF Import Tool, di VMware by Broadcom, è un'utilità utilizzata sia sull'appliance vCenter che sul gestore SDDC per convalidare le configurazioni e fornire servizi di conversione e importazione per gli ambienti vSphere e VCF.

Per ulteriori informazioni, consulta "Opzioni e parametri dello strumento di importazione VCF" .

Copia ed estrai lo strumento di importazione VCF

Lo strumento di importazione VCF viene utilizzato sull'appliance vCenter per convalidare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

1. Segui i passaggi a "Copia lo strumento di importazione VCF nell'appliance vCenter di destinazione" in VMware Docs per copiare lo strumento di importazione VCF nella posizione corretta.
2. Estrarre il bundle utilizzando il seguente comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Convalida l'appliance vCenter

Utilizzare lo strumento di importazione VCF per convalidare l'appliance vCenter prima dell'importazione come dominio del carico di lavoro VI.

1. Segui i passaggi a "Eseguire un pre-controllo sul vCenter di destinazione prima della conversione" per eseguire la convalida.

Creare un file JSON per la distribuzione NSX

Per distribuire NSX Manager durante l'importazione o la conversione di un ambiente vSphere in VMware Cloud Foundation, creare una specifica di distribuzione NSX. Per la distribuzione di NSX sono necessari almeno 3 host.

> Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzato il segmento supportato da NSX VLAN. Per maggiori dettagli sulle limitazioni del segmento supportato da NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation" .

Di seguito è riportato un esempio di file JSON per la distribuzione NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copiare il file JSON nella cartella home dell'utente vcf su SDDC Manager.

Carica il software su SDDC Manager

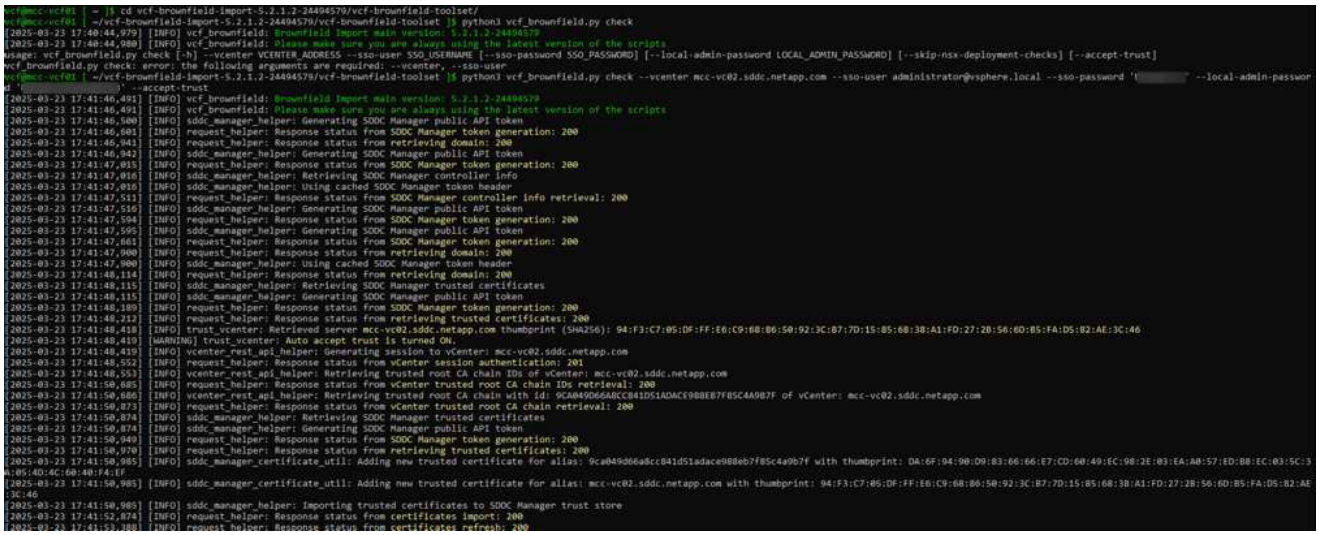
Copiare lo strumento di importazione VCF nella cartella home dell'utente vcf e il bundle di distribuzione NSX nella cartella /nfs/vmware/vcf/nfs-mount/bundle/ su SDDC Manager.

Vedere "Caricare il software richiesto sull'appliance SDDC Manager" per istruzioni dettagliate.

Controllo dettagliato su vCenter prima della conversione

Prima di eseguire un'operazione di conversione del dominio di gestione o un'operazione di importazione del dominio del carico di lavoro VI, è necessario eseguire un controllo dettagliato per assicurarsi che la configurazione dell'ambiente vSphere esistente sia supportata per la conversione o l'importazione. . Eseguire l'accesso SSH all'appliance SDDC Manager come utente vcf. . Passare alla directory in cui è stato copiato lo strumento di importazione VCF. . Eseguire il seguente comando per verificare che l'ambiente vSphere possa essere convertito

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



Convertire il cluster vSphere in un dominio di carico di lavoro VCF VI

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF.

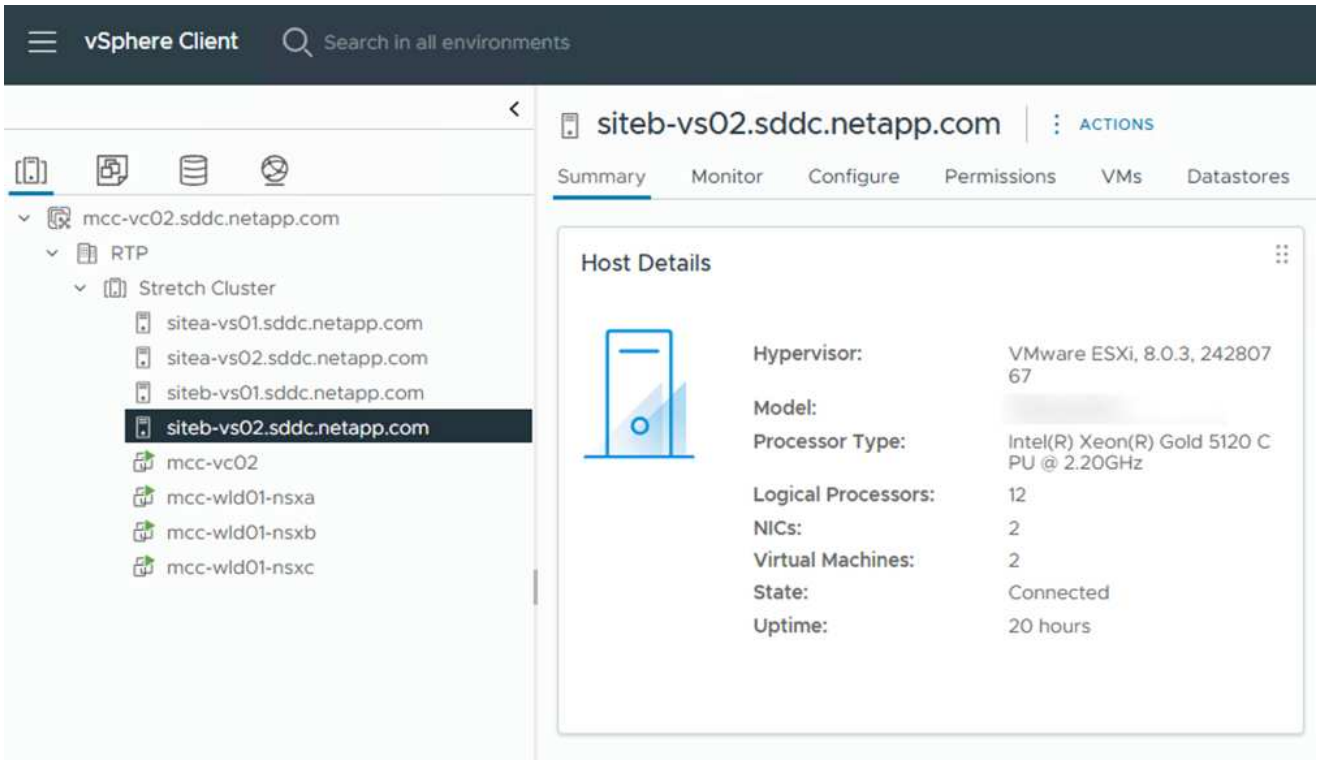
Per convertire il cluster vSphere in un dominio di gestione VCF e distribuire il cluster NSX, eseguire il comando seguente:

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

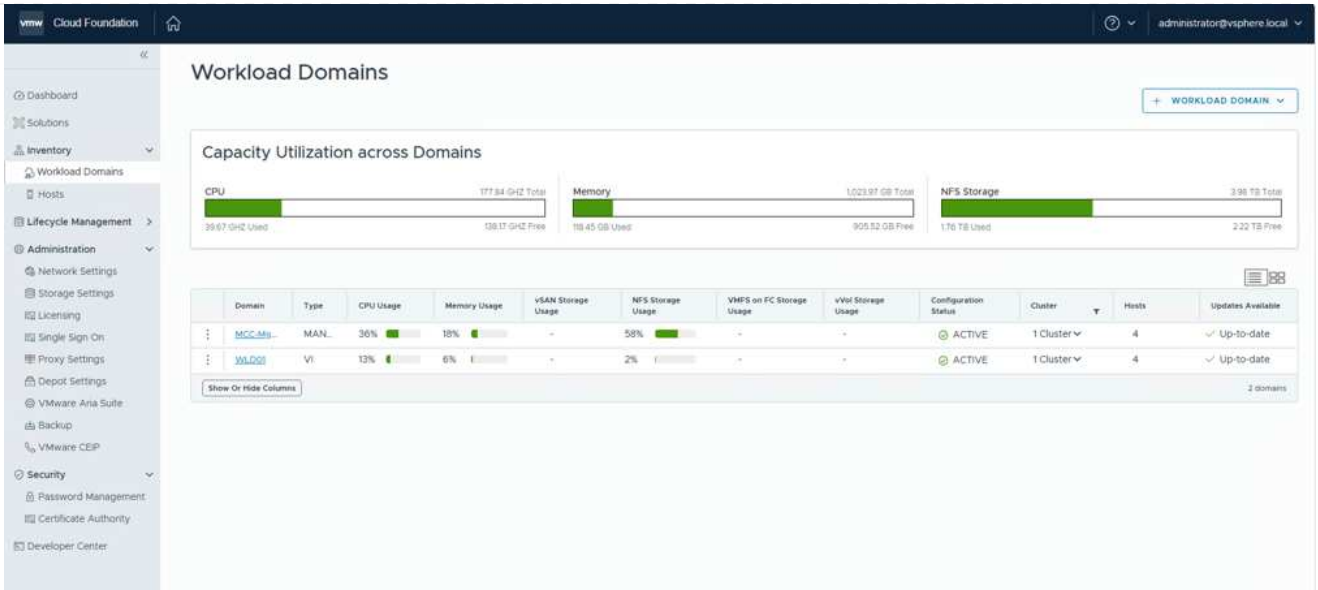
Anche se sull'host vSphere sono disponibili più Datastore, non è necessario specificare quale Datastore deve essere considerato come Datastore primario.

Per istruzioni complete, fare riferimento a "Procedura di conversione VCF" .

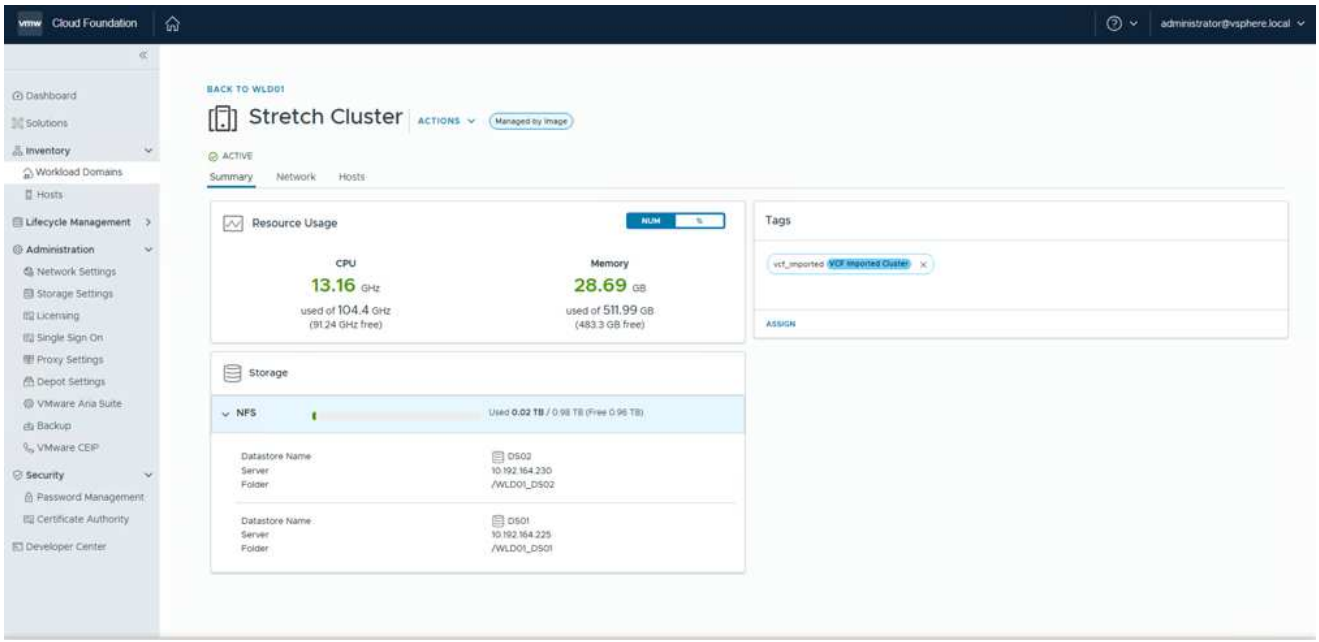
Le VM NSX verranno distribuite su vCenter.



SDDC Manager mostra il dominio del carico di lavoro VI creato con il nome fornito e NFS come Datastore.



Durante l’ispezione del cluster, vengono fornite le informazioni sui datastore NFS.



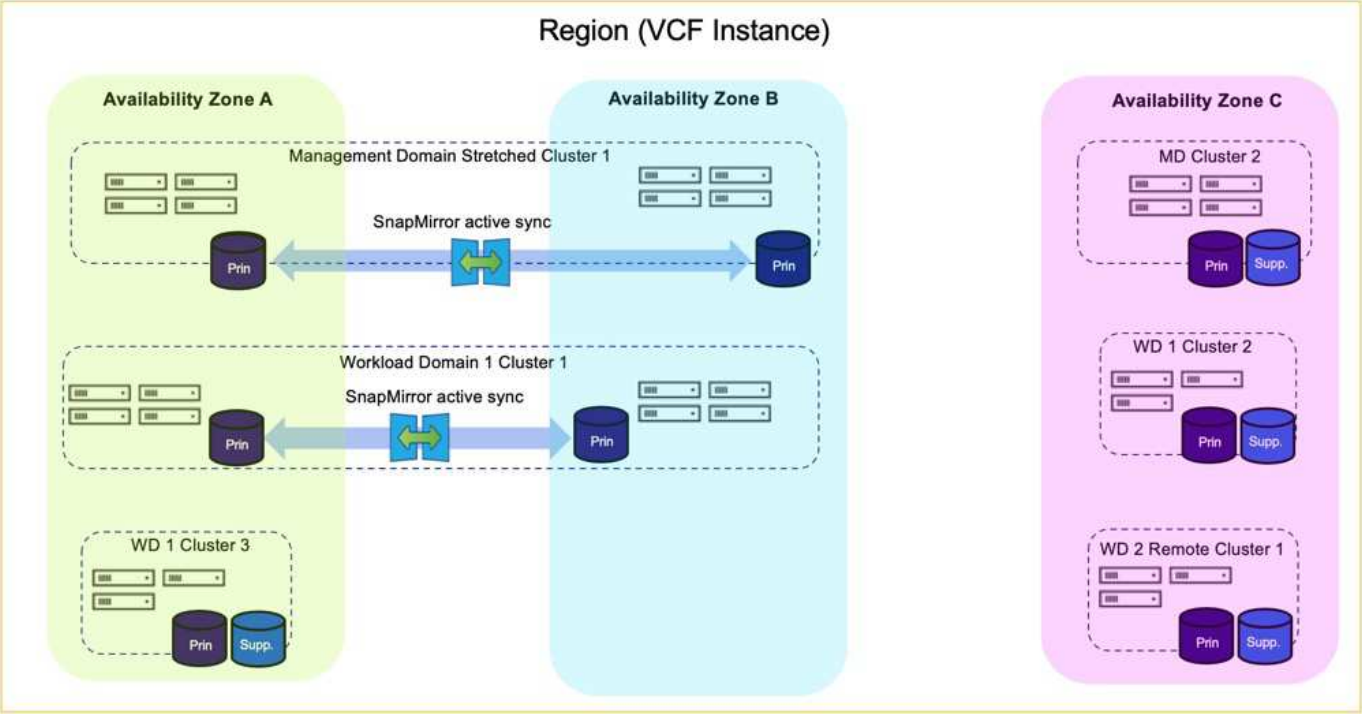
Aggiungere la licenza al VCF

Dopo aver completato la conversione, è necessario aggiungere la licenza all'ambiente.

1. Accedi all'interfaccia utente di SDDC Manager.
2. Nel riquadro di navigazione, vai su **Amministrazione > Licenze**.
3. Fare clic su **+ Chiave di licenza**.
4. Scegli un prodotto dal menu a discesa.
5. Inserisci la chiave di licenza.
6. Fornire una descrizione della licenza.
7. Fare clic su **Aggiungi**.
8. Ripetere questi passaggi per ogni licenza.

Configurare un cluster esteso per un dominio di gestione VCF utilizzando SnapMirror Active Sync

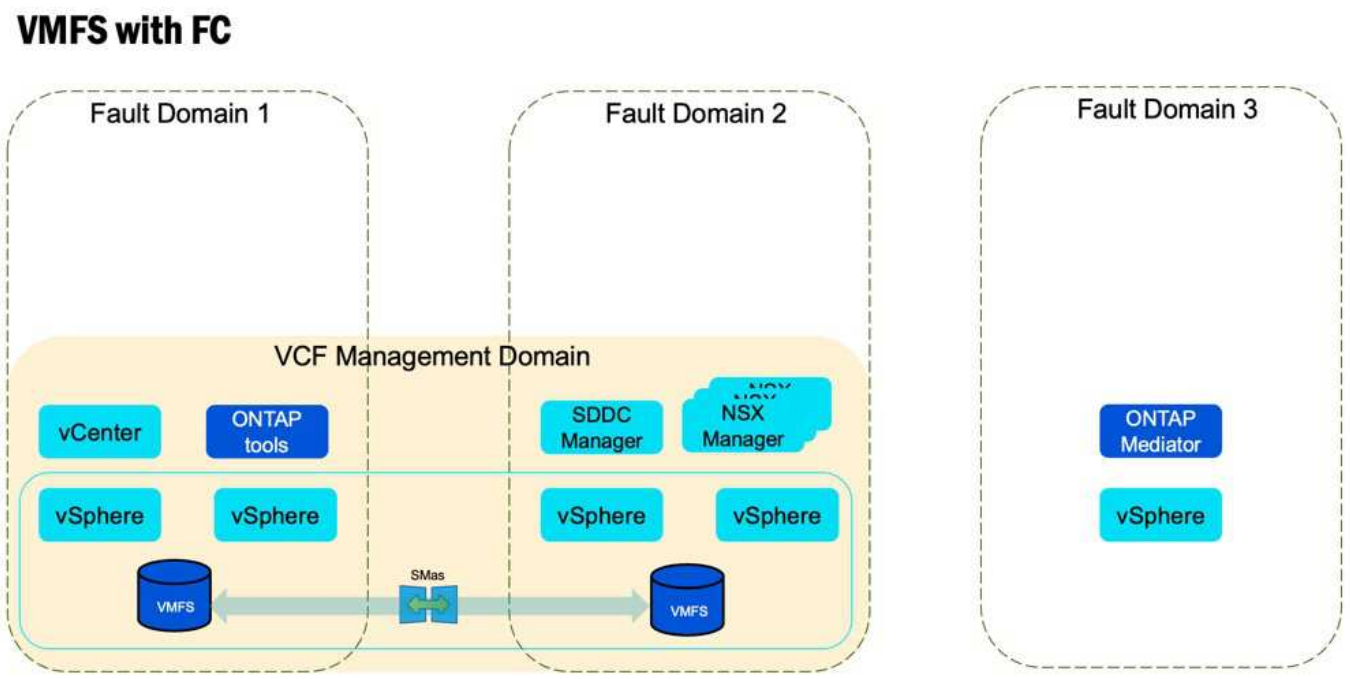
In questo caso d'uso descriviamo la procedura per utilizzare gli ONTAP tools for VMware vSphere per configurare un cluster esteso per un dominio di gestione VCF. Questa procedura include la distribuzione di host vSphere e vCenter Server, l'installazione di strumenti ONTAP , la protezione dei datastore con SnapMirror Active Sync, la migrazione delle VM verso datastore protetti e la configurazione di storage supplementare.



Panoramica dello scenario

La soluzione Stretch Cluster può essere implementata sul cluster predefinito o su un cluster aggiuntivo nei domini di gestione o di carico di lavoro VCF. VMFS su FC è supportato sia sul datastore principale che sui

datastore supplementari. VMFS su iSCSI è supportato solo con datastore supplementari. Fare riferimento a IMT per il supporto di VMFS su NVMe-oF con SnapMirror ActiveSync.



Archiviazione principale sul dominio di gestione

A partire da VCF 5.2, il dominio di gestione può essere distribuito senza VSAN utilizzando lo strumento di importazione VCF. L'opzione di conversione dello strumento di importazione VCF consente"una distribuzione vCenter esistente in un dominio di gestione" . Tutti i cluster in vCenter diventeranno parte del dominio di gestione.

1. Distribuisci host vSphere
2. Distribuire il server vCenter sul datastore locale (vCenter deve coesistere sugli host vSphere che verranno convertiti nel dominio di gestione)
3. Distribuisci gli ONTAP tools for VMware vSphere
4. Distribuisci il plug-in SnapCenter per VMware vSphere (facoltativo)
5. Creare un datastore (la configurazione della zona FC deve essere a posto)
6. Proteggere il cluster vSphere
7. Migrare le VM al datastore appena creato

Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Archiviazione supplementare sul dominio di gestione

Una volta che il dominio di gestione è attivo e funzionante, è possibile creare datastore aggiuntivi utilizzando gli strumenti ONTAP che attiveranno l'espansione del gruppo di coerenza.

> Se un cluster vSphere è protetto, saranno protetti tutti i datastore nel cluster.

Se l'ambiente VCF viene distribuito con lo strumento Cloud Builder, per creare l'archiviazione supplementare con iSCSI, distribuire gli strumenti ONTAP per creare il datastore iSCSI e proteggere il cluster vSphere.

> Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Informazioni aggiuntive

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

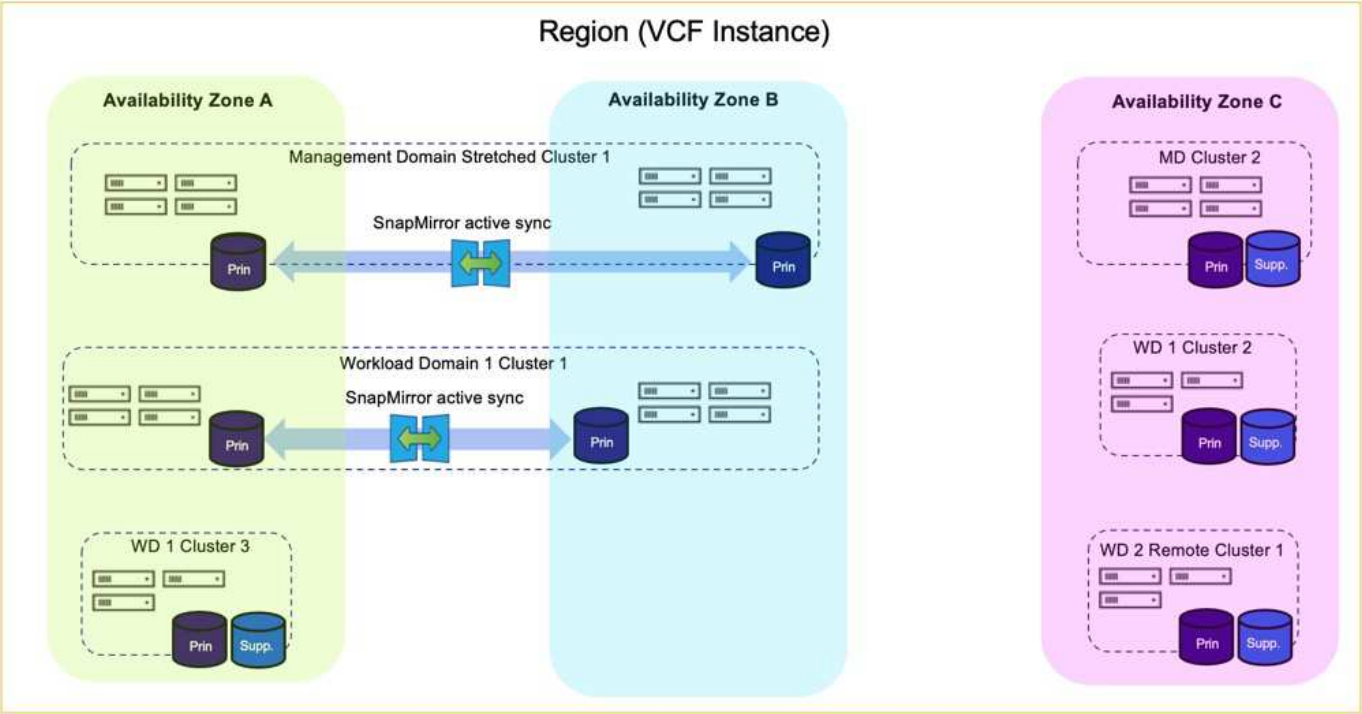
Per informazioni sulla configurazione di VCF fare riferimento a"Documentazione di VMware Cloud Foundation 5.2" .

Demo video per questa soluzione

Cluster di allungamento per VCF con strumenti ONTAP

Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando SnapMirror Active Sync

In questo caso d'uso descriviamo la procedura per configurare un cluster esteso per un dominio di carico di lavoro di un'infrastruttura virtuale (VI) utilizzando SnapMirror Active Sync con ONTAP tools for VMware vSphere. Questa procedura include la creazione di un dominio di carico di lavoro VCF con VMFS su Fibre Channel, la registrazione di vCenter con strumenti ONTAP , la registrazione dei sistemi di storage e la protezione del cluster vSphere.



Panoramica dello scenario

Gli archivi dati sul dominio VCF Workload possono essere protetti con SnapMirror ActiveSync per fornire una soluzione di cluster estensibile. La protezione è abilitata a livello di cluster vSphere e tutti i datastore a blocchi ONTAP nel cluster saranno protetti.

Archiviazione principale sul dominio del carico di lavoro

Il dominio del carico di lavoro può essere creato importandolo tramite lo strumento di importazione VCF oppure distribuendolo tramite il gestore SDDC. L'implementazione con SDDC Manager fornirà più opzioni di rete rispetto all'importazione di un ambiente esistente.

1. Crea un dominio di carico di lavoro con VMFS su FC
2. "Registra il dominio del carico di lavoro vCenter nel gestore degli strumenti ONTAP per distribuire il plug-in vCenter"
3. "Registrare i sistemi di archiviazione sugli strumenti ONTAP"
4. "Proteggere il cluster vSphere"

> Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Archiviazione supplementare sul dominio del carico di lavoro

Una volta che il dominio del carico di lavoro è attivo e funzionante, è possibile creare datastore aggiuntivi utilizzando gli strumenti ONTAP che attiveranno l'espansione del gruppo di coerenza.

> Se un cluster vSphere è protetto, saranno protetti tutti i datastore nel cluster.

Informazioni aggiuntive

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" .

Demo video per questa soluzione

Cluster di allungamento per VCF con strumenti ONTAP

Migrazione delle VM da VMware vSphere ai datastore ONTAP

Gli ambienti VMware vSphere possono trarre notevoli vantaggi dalla migrazione delle macchine virtuali verso datastore supportati NetApp ONTAP. Che tu stia passando da vSAN a sistemi di archiviazione di terze parti o aggiornando la tua infrastruttura esistente, esplora vari scenari vMotion e strategie di migrazione per trasferire senza problemi le tue VM ai datastore ONTAP . Ciò garantisce la continuità aziendale sfruttando al contempo le funzionalità di archiviazione di classe enterprise di ONTAP.

VMware vSphere di Broadcom supporta i datastore VMFS, NFS e vVol per l'hosting di macchine virtuali. I clienti hanno la possibilità di creare tali datastore con infrastrutture iperconvergenti o con sistemi di storage condivisi centralizzati.

I clienti spesso riscontrano il valore dell'hosting su sistemi di storage basati su ONTAP per fornire snapshot e cloni di macchine virtuali efficienti in termini di spazio, flessibilità nella scelta di vari modelli di distribuzione nei data center e nei cloud, efficienza operativa con strumenti di monitoraggio e avviso, sicurezza, governance e strumenti di conformità opzionali per ispezionare i dati delle macchine virtuali e così via.

Le VM ospitate su datastore ONTAP possono essere protette utilizzando il plug-in SnapCenter per VMware vSphere (SCV). SCV crea snapshot basati sull'archiviazione e li replica anche sul sistema di archiviazione ONTAP remoto. I ripristini possono essere eseguiti sia dai sistemi di archiviazione primari che da quelli secondari.

I clienti hanno la flessibilità di scegliere Cloud Insights o Aria Operations o una combinazione di entrambi o altri strumenti di terze parti che utilizzano l'API ONTAP per la risoluzione dei problemi, il monitoraggio delle prestazioni, la creazione di report e le funzionalità di notifica degli avvisi.

I clienti possono facilmente effettuare il provisioning del datastore utilizzando il plug-in vCenter ONTAP Tools o la sua API e le VM possono essere migrate nei datastore ONTAP anche mentre sono accesi.

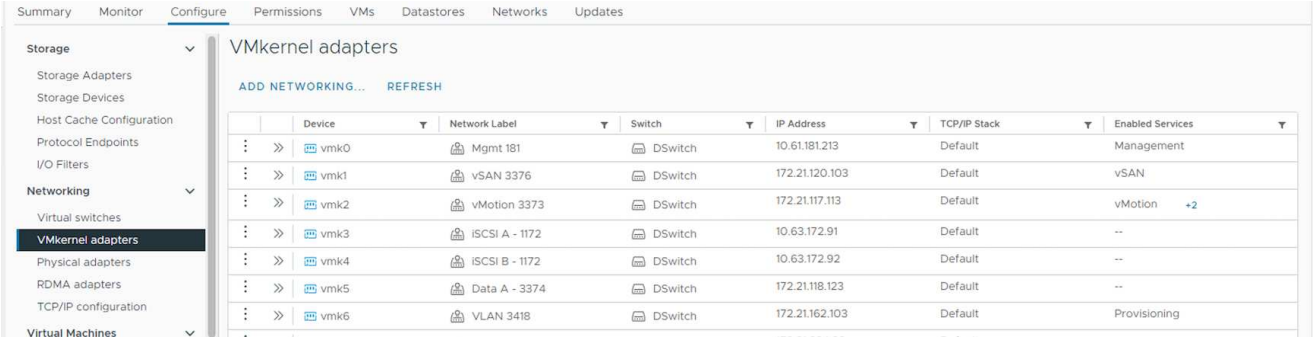
> Alcune VM distribuite con strumenti di gestione esterni come Aria Automation, Tanzu (o altre versioni di Kubernetes) dipendono solitamente dalla policy di archiviazione della VM. Se si esegue la migrazione tra gli archivi dati all'interno della stessa policy di archiviazione della VM, l'impatto sulle applicazioni dovrebbe essere minore. Verificare con i proprietari dell'applicazione la corretta migrazione di tali VM al nuovo datastore. Introduzione di vSphere 8 "Notifiche vSphere vMotion per applicazioni sensibili alla latenza" per preparare le applicazioni per vMotion.

Requisiti di rete

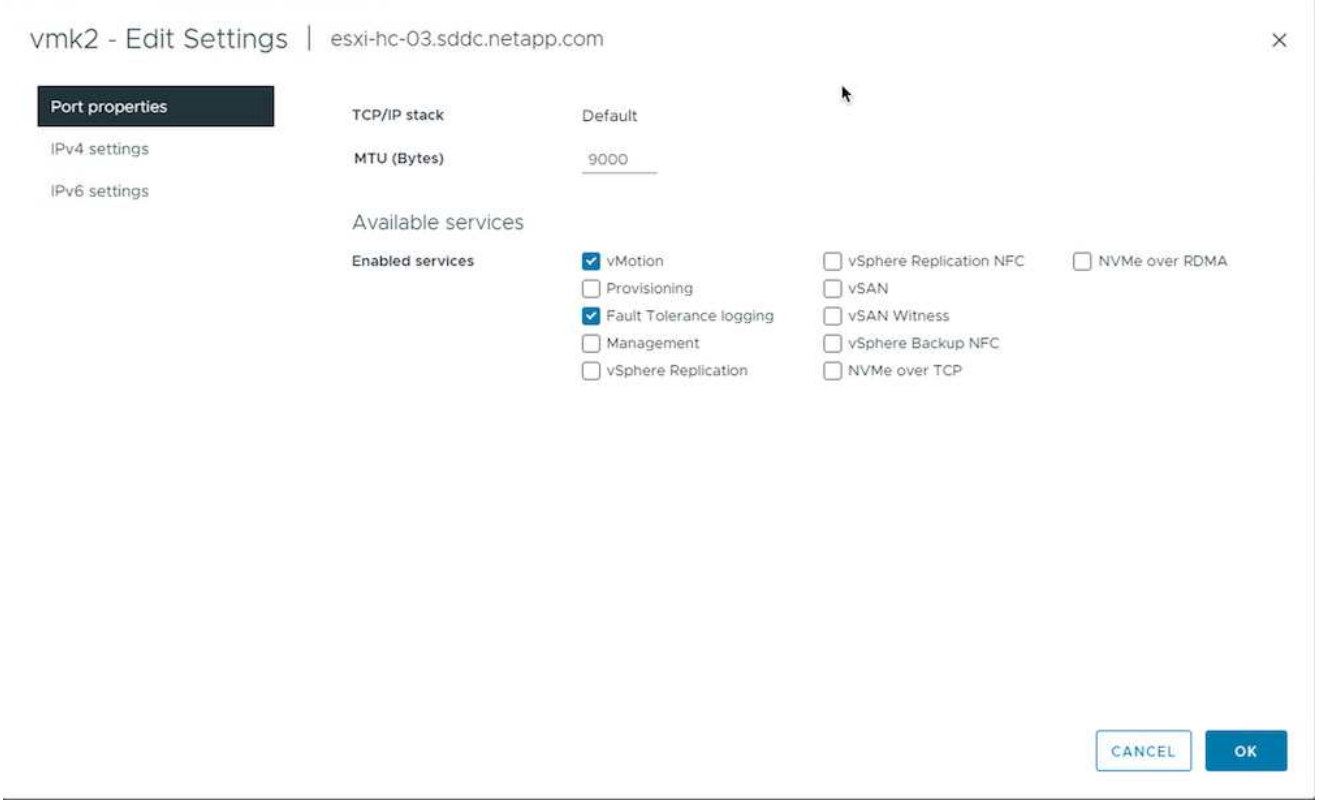
Migrazione di VM con vMotion

Si presume che sia già presente una rete di archiviazione doppia per il datastore ONTAP , per garantire connettività, tolleranza agli errori e aumento delle prestazioni.

Anche la migrazione delle VM tra gli host vSphere viene gestita dall'interfaccia VMKernel dell'host vSphere. Per la migrazione a caldo (VM accese), viene utilizzata l'interfaccia VMKernel con il servizio vMotion abilitato, mentre per la migrazione a freddo (VM spente), viene utilizzata l'interfaccia VMKernel con il servizio Provisioning abilitato per spostare i dati. Se non viene trovata alcuna interfaccia valida, verrà utilizzata l'interfaccia di gestione per spostare i dati, il che potrebbe non essere auspicabile per determinati casi d'uso.



Quando si modifica l'interfaccia VMKernel, ecco l'opzione per abilitare i servizi richiesti.



Assicurarsi che siano disponibili almeno due schede di rete uplink attive ad alta velocità per il portgroup utilizzato dalle interfacce vMotion e Provisioning VMkernel.

Scenari di migrazione delle VM

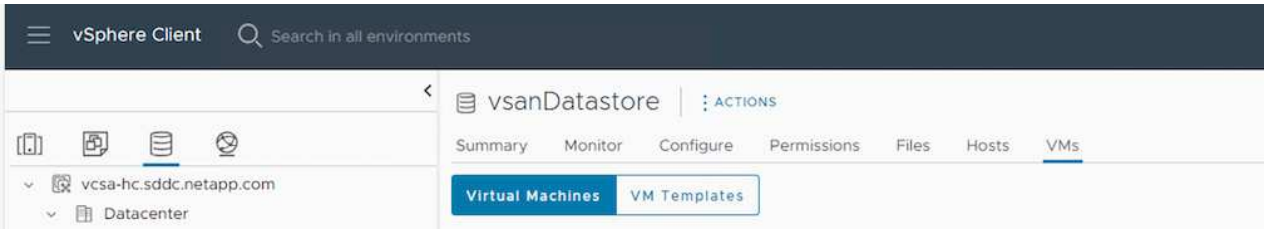
vMotion viene spesso utilizzato per migrare le VM indipendentemente dal loro stato di alimentazione. Di seguito sono disponibili ulteriori considerazioni e procedure di migrazione per scenari specifici.

> Capire "Condizioni e limitazioni della VM di vSphere vMotion" prima di procedere con qualsiasi opzione di migrazione della VM.

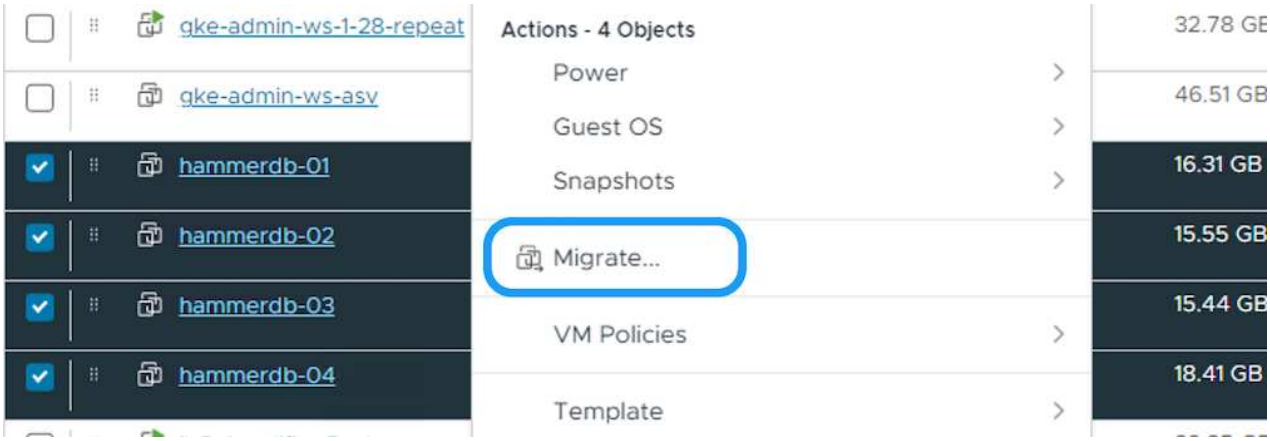
Migrazione di VM da uno specifico vSphere Datastore

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

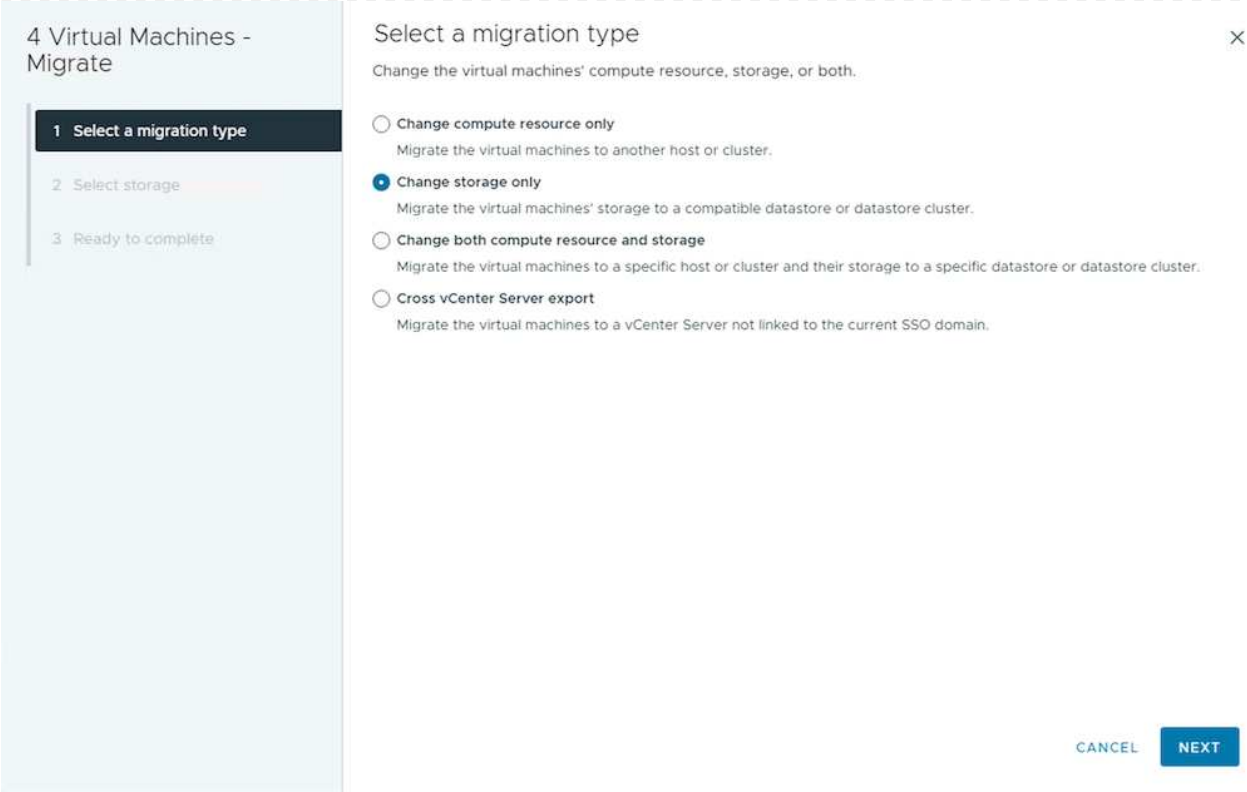
1. Con vSphere Web Client, seleziona il Datastore dall'inventario di storage e fai clic sulla scheda VM.



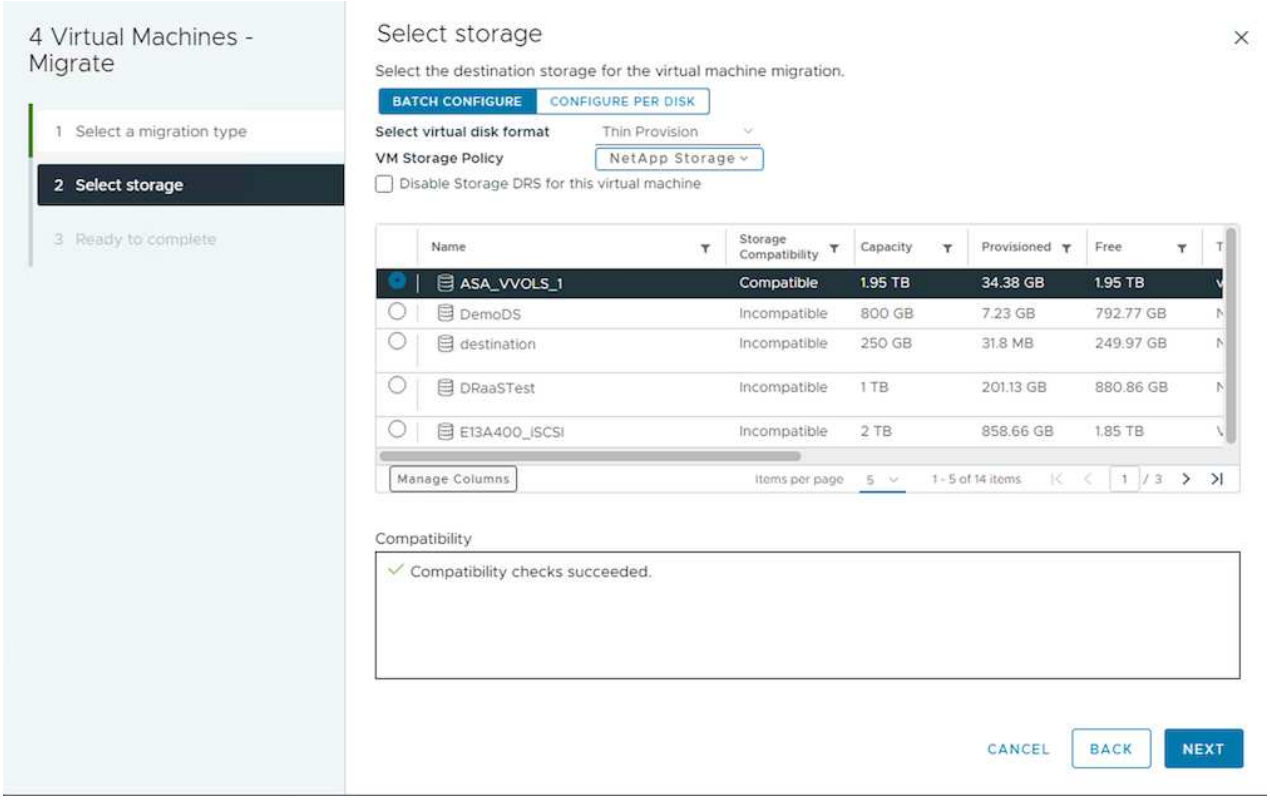
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



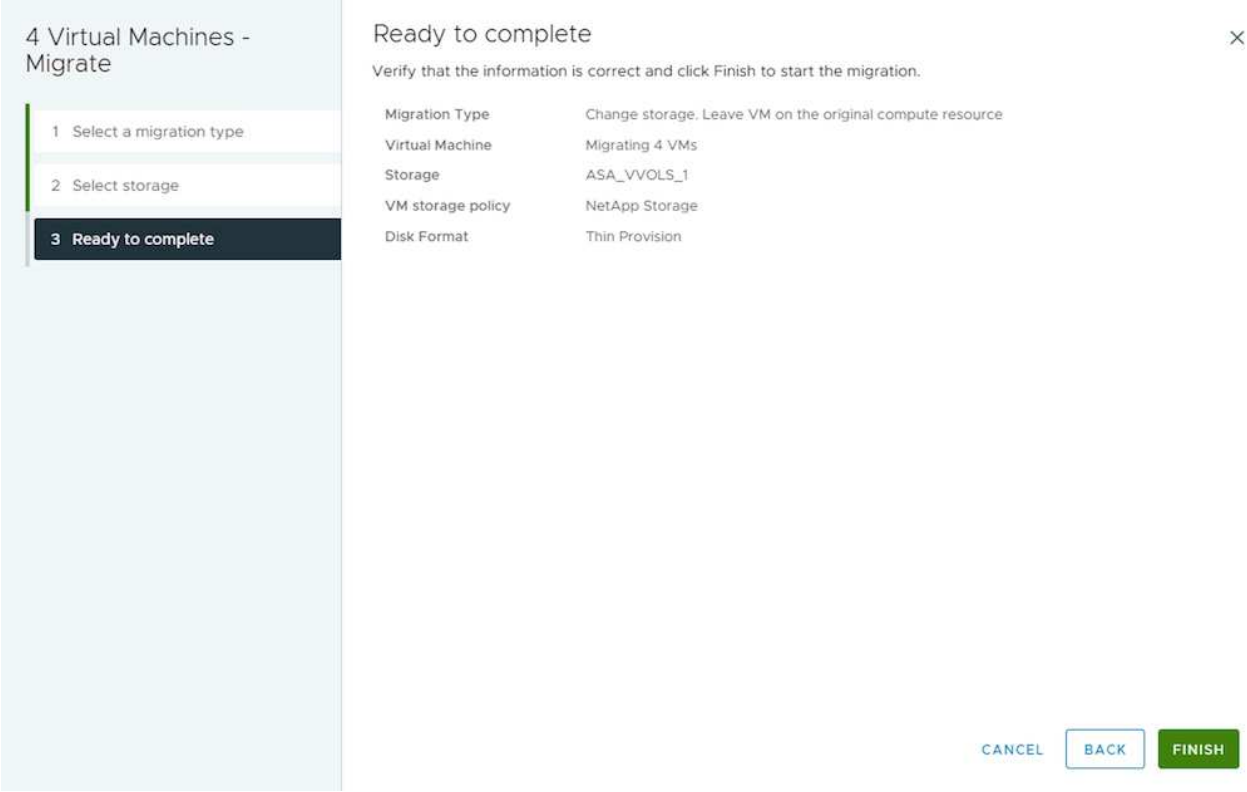
3. Scegli l'opzione per modificare solo l'archiviazione, fai clic su Avanti



4. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.



5. Rivedi e clicca su Fine.



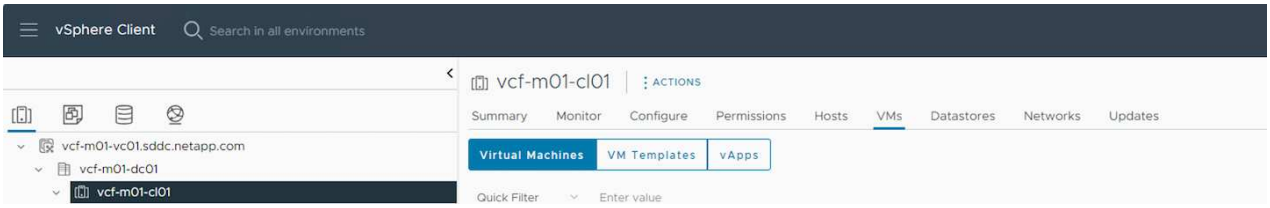
Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

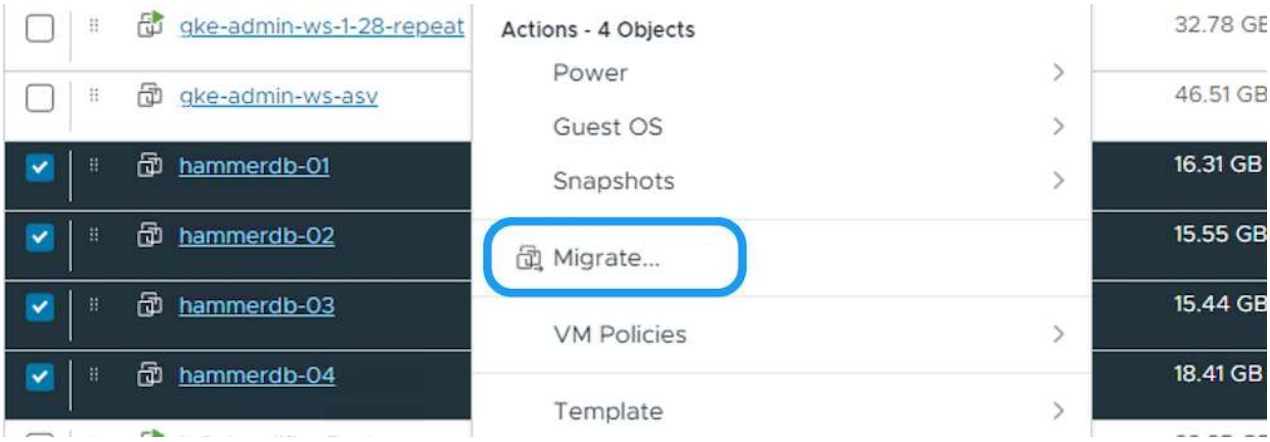
Migrazione di VM nello stesso cluster vSphere

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

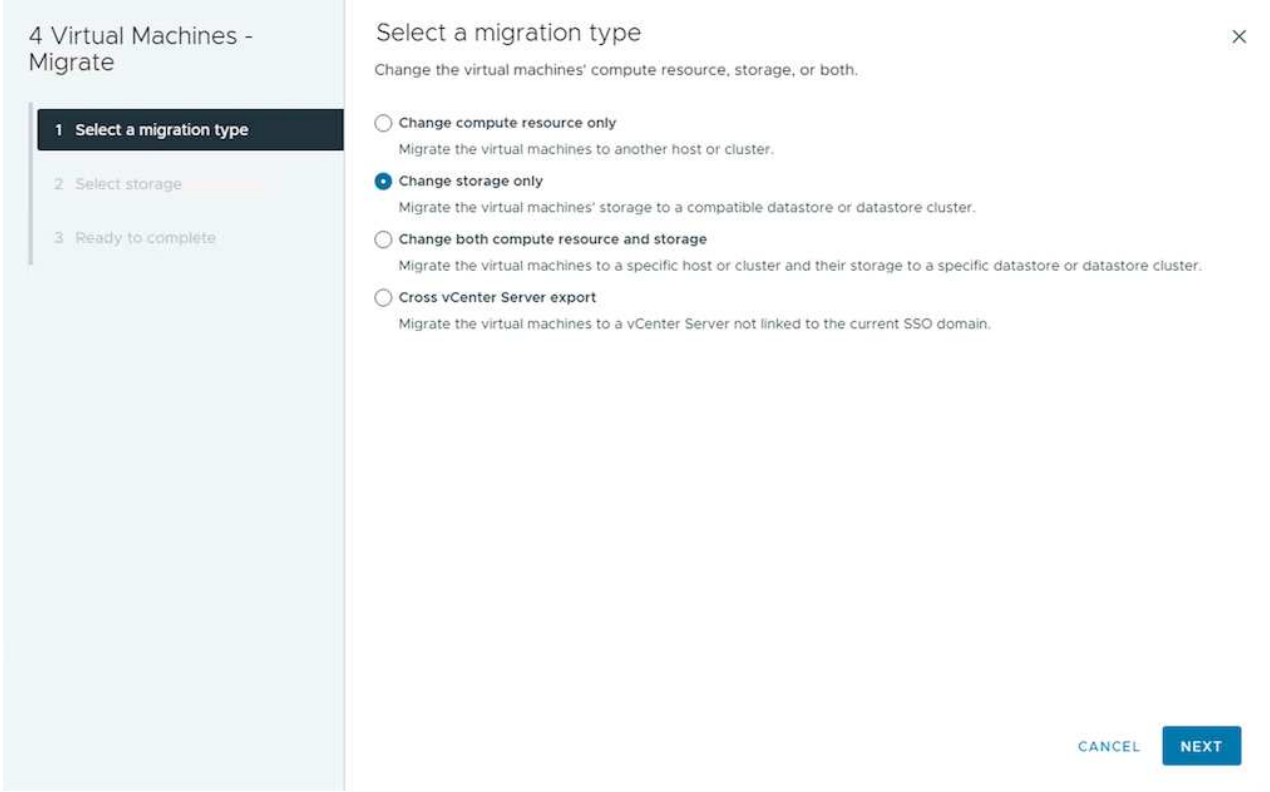
1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VM.



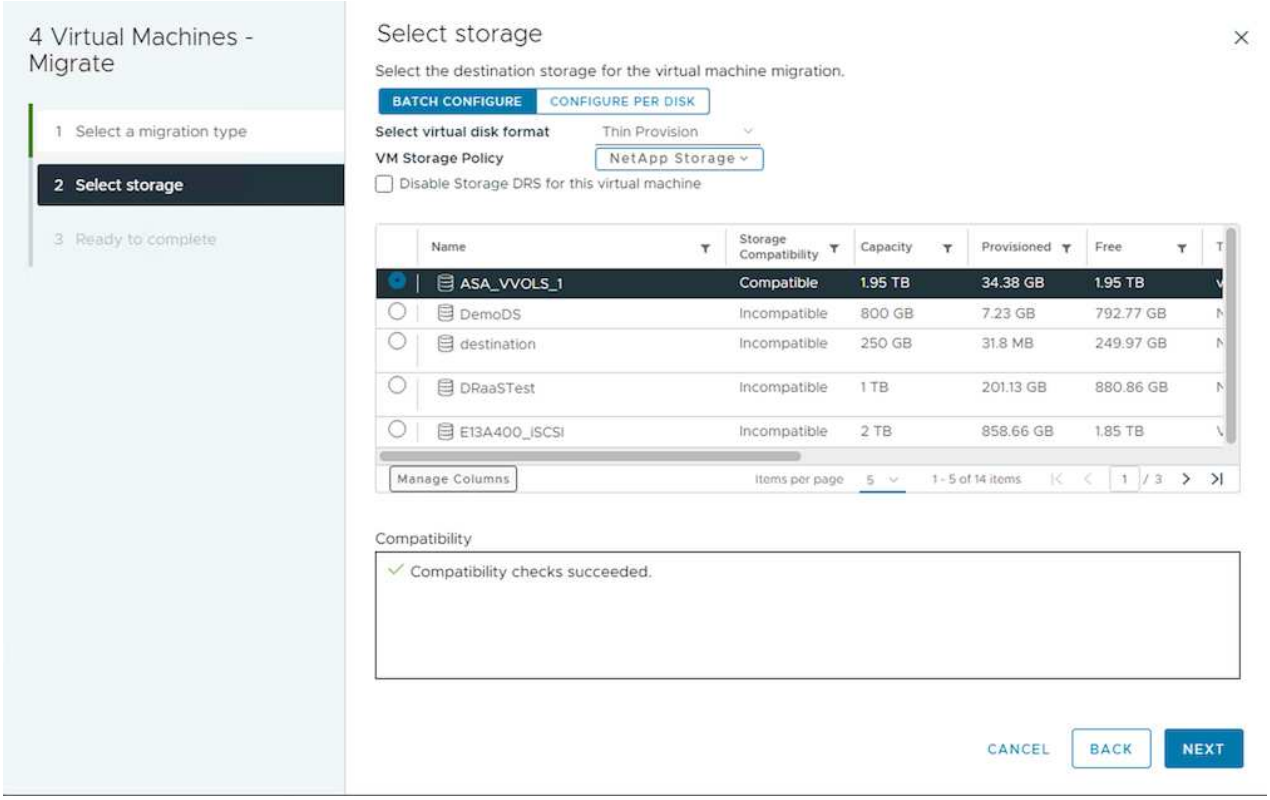
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



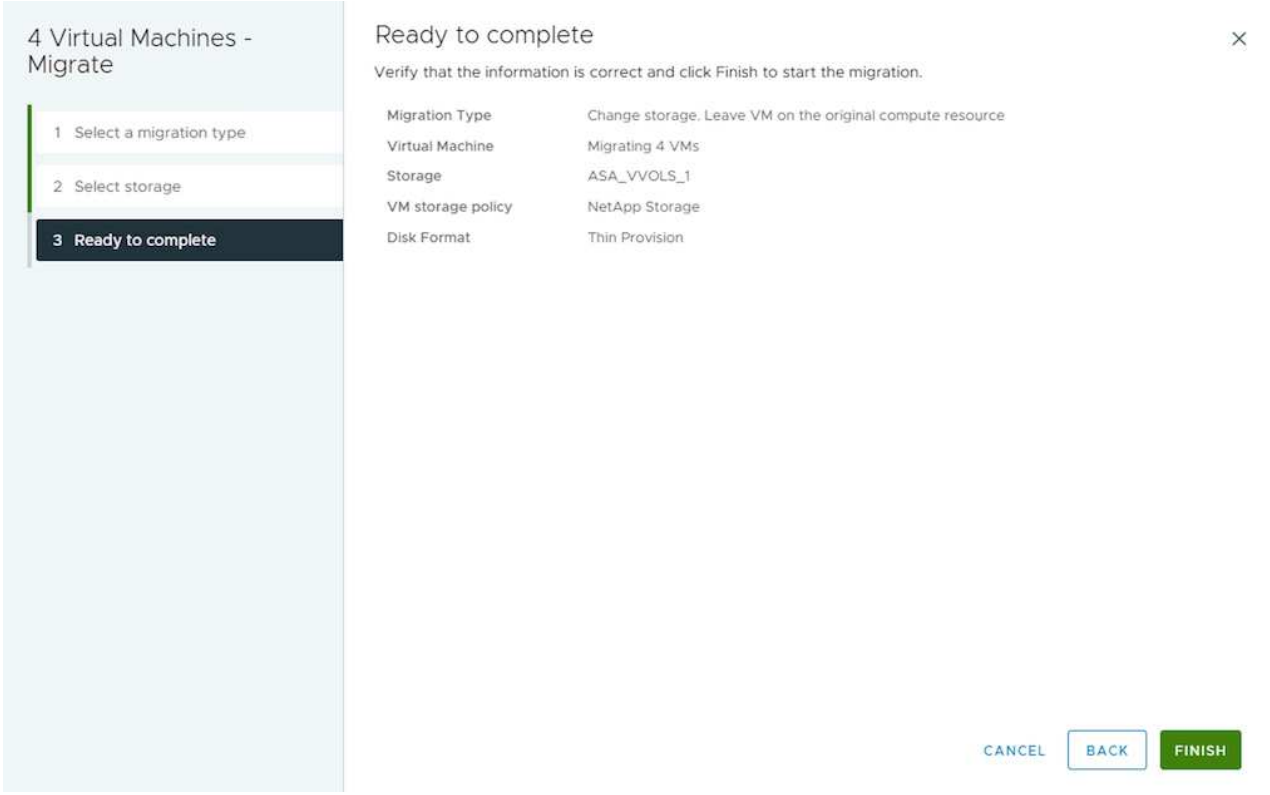
3. Scegli l'opzione per modificare solo l'archiviazione, fai clic su Avanti



4. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.



5. Rivedi e clicca su Fine.



Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

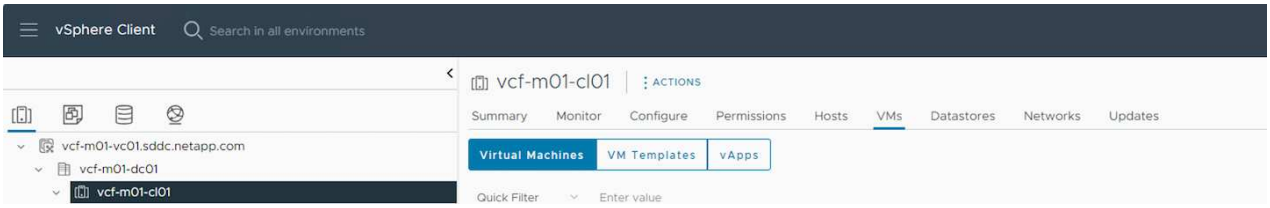
Quando Datastore Cluster è in uso con DRS (Dynamic Resource Scheduling) di archiviazione completamente automatizzato ed entrambi i datastore (di origine e di destinazione) sono dello stesso tipo (VMFS/NFS/vVol), mantenere entrambi i datastore nello stesso cluster di archiviazione ed eseguire la migrazione delle VM dal datastore di origine abilitando la modalità di manutenzione sull'origine. L'esperienza sarà simile a quella che si ha quando si gestiscono gli host di elaborazione per la manutenzione.

Migrazione di VM su più cluster vSphere

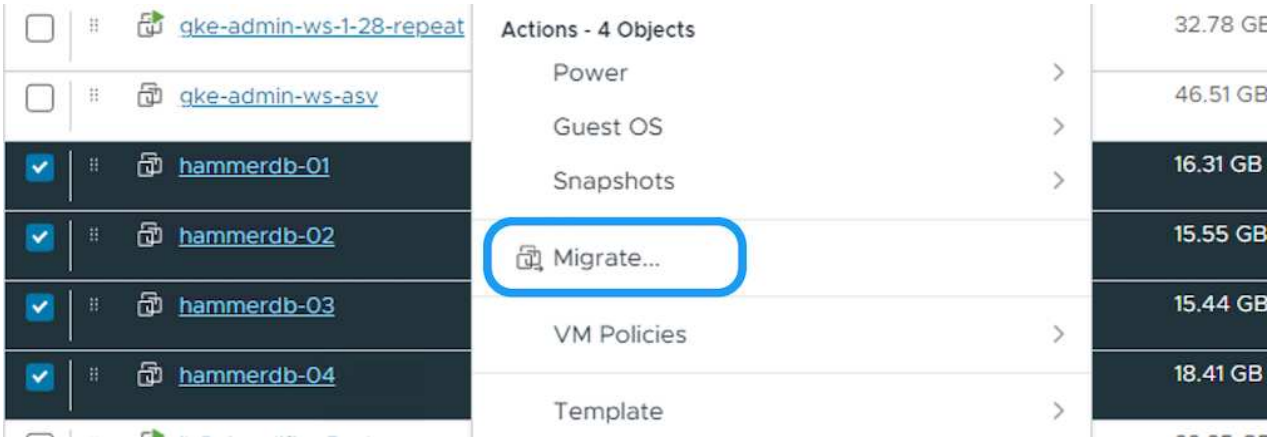
> Fare riferimento "Compatibilità CPU e compatibilità vSphere Enhanced vMotion" quando gli host di origine e di destinazione appartengono a famiglie o modelli di CPU diversi.

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

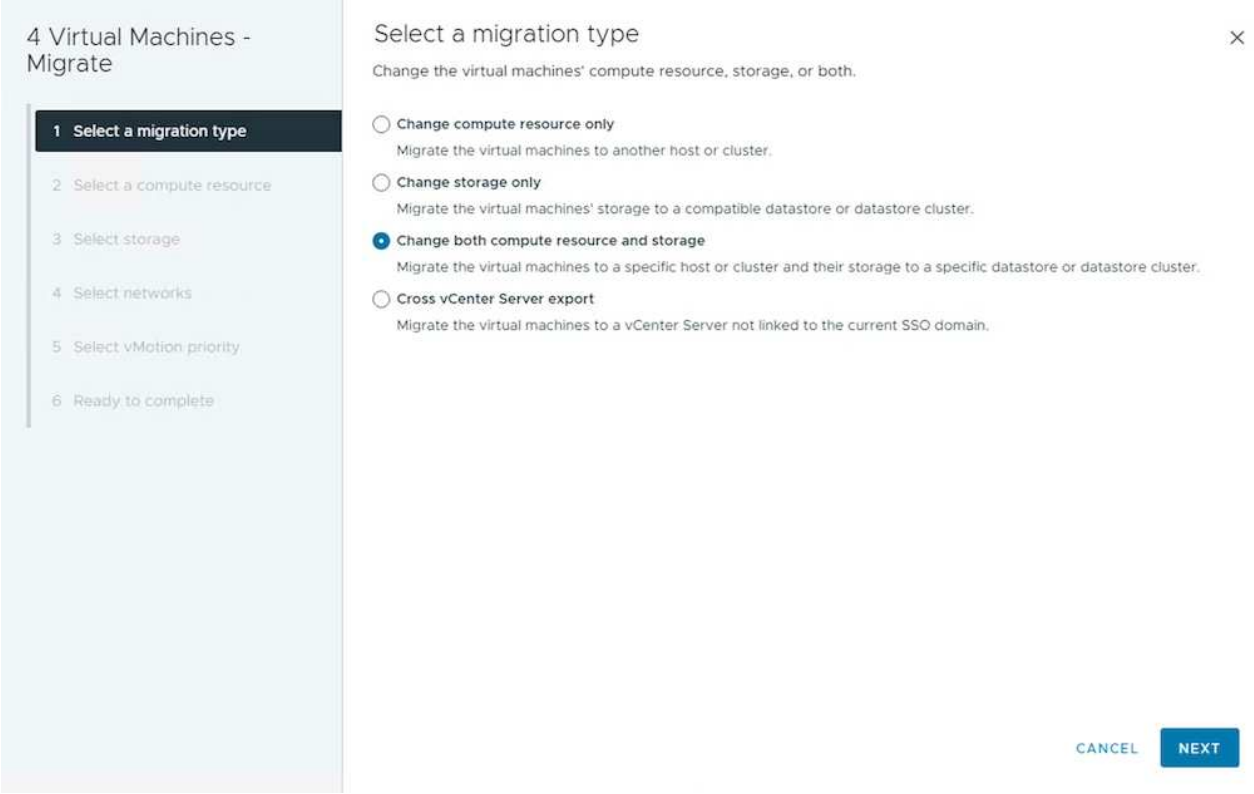
1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VM.



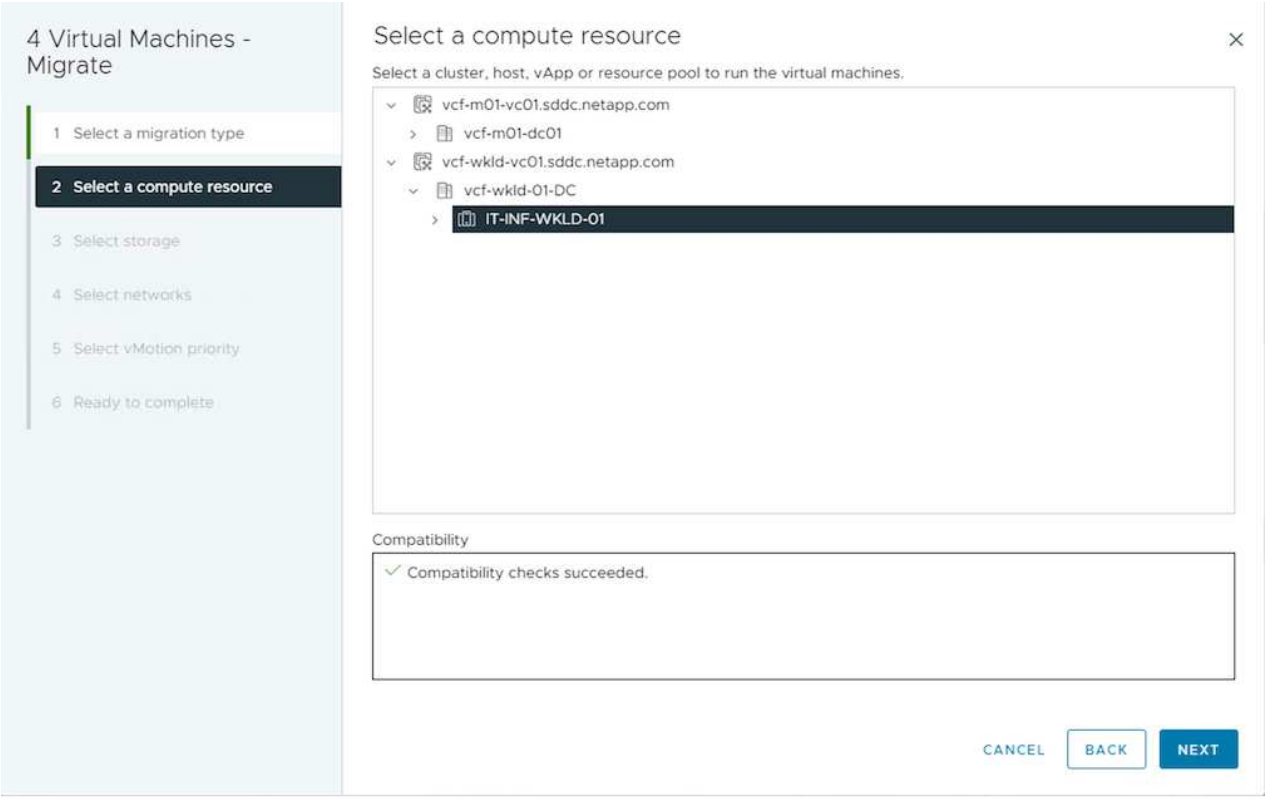
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



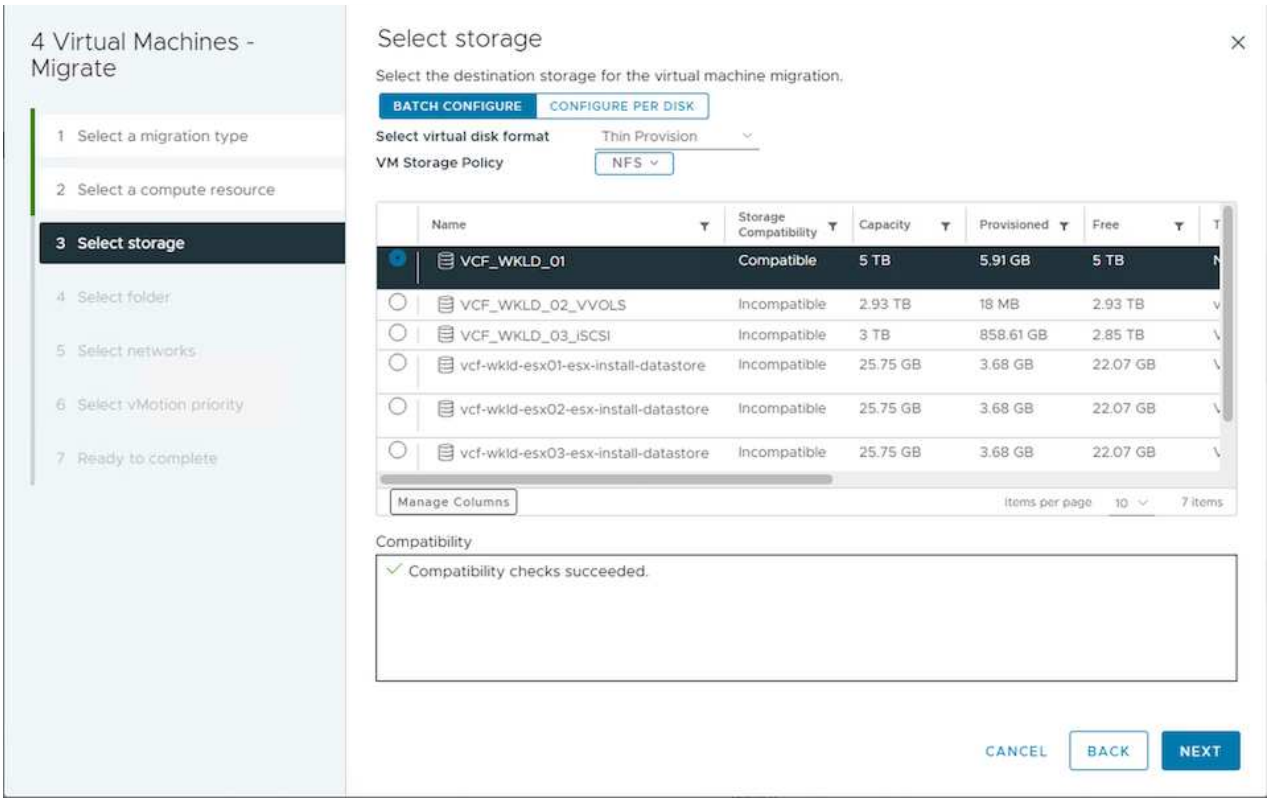
3. Scegli l'opzione per modificare le risorse di elaborazione e di archiviazione, fai clic su Avanti



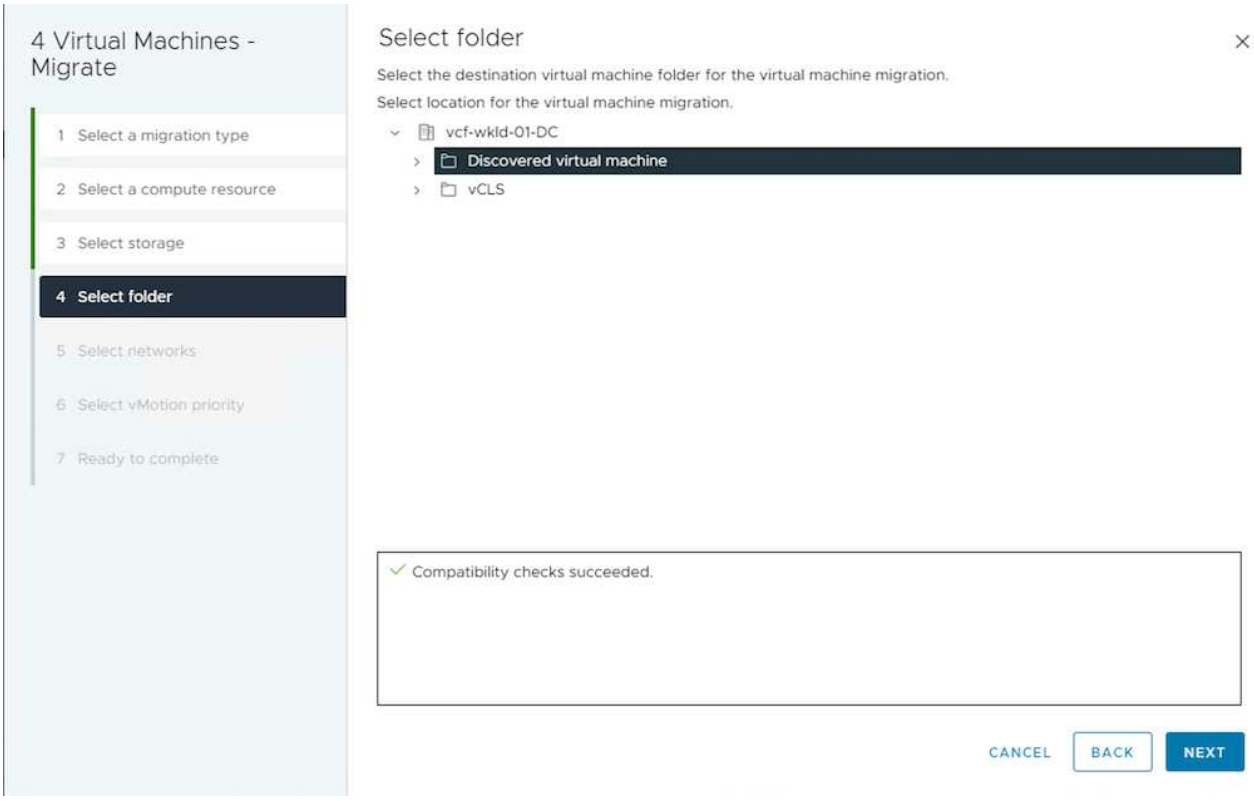
4. Esplora e seleziona il cluster giusto da migrare.



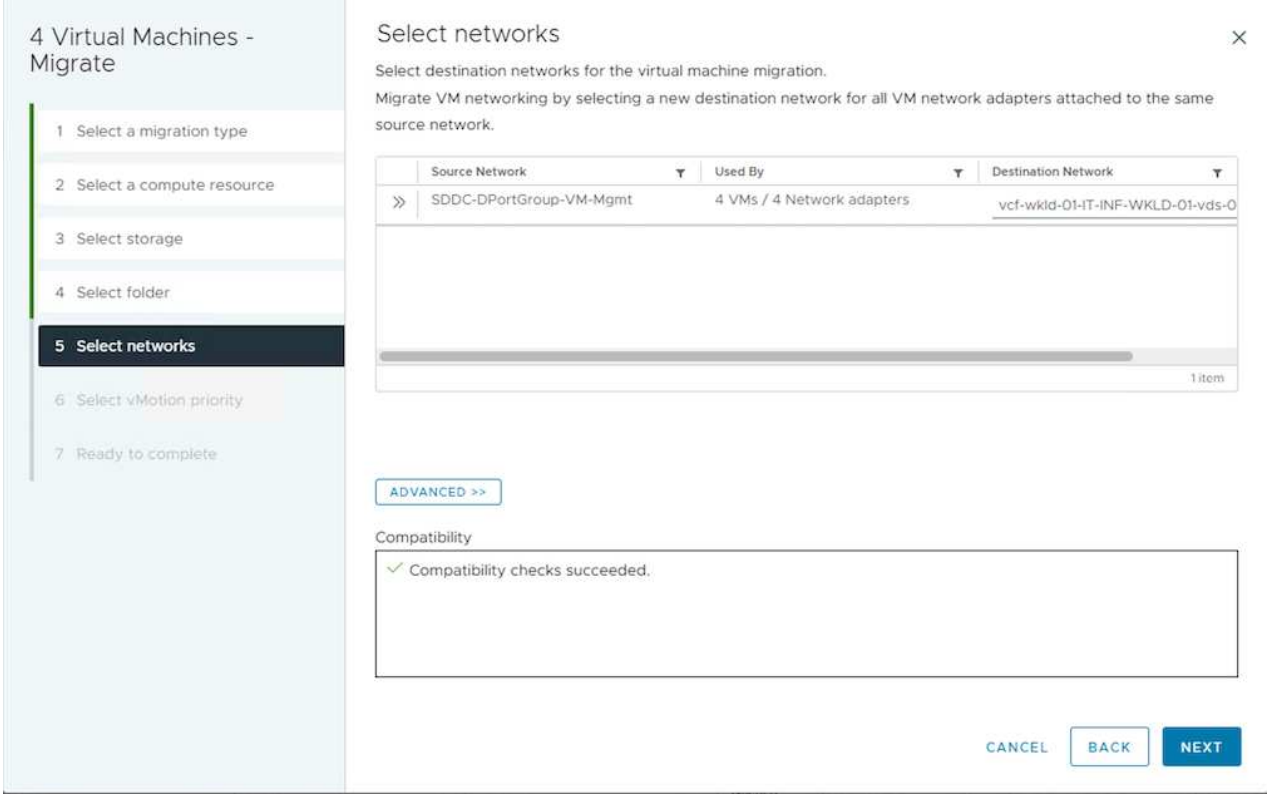
5. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.



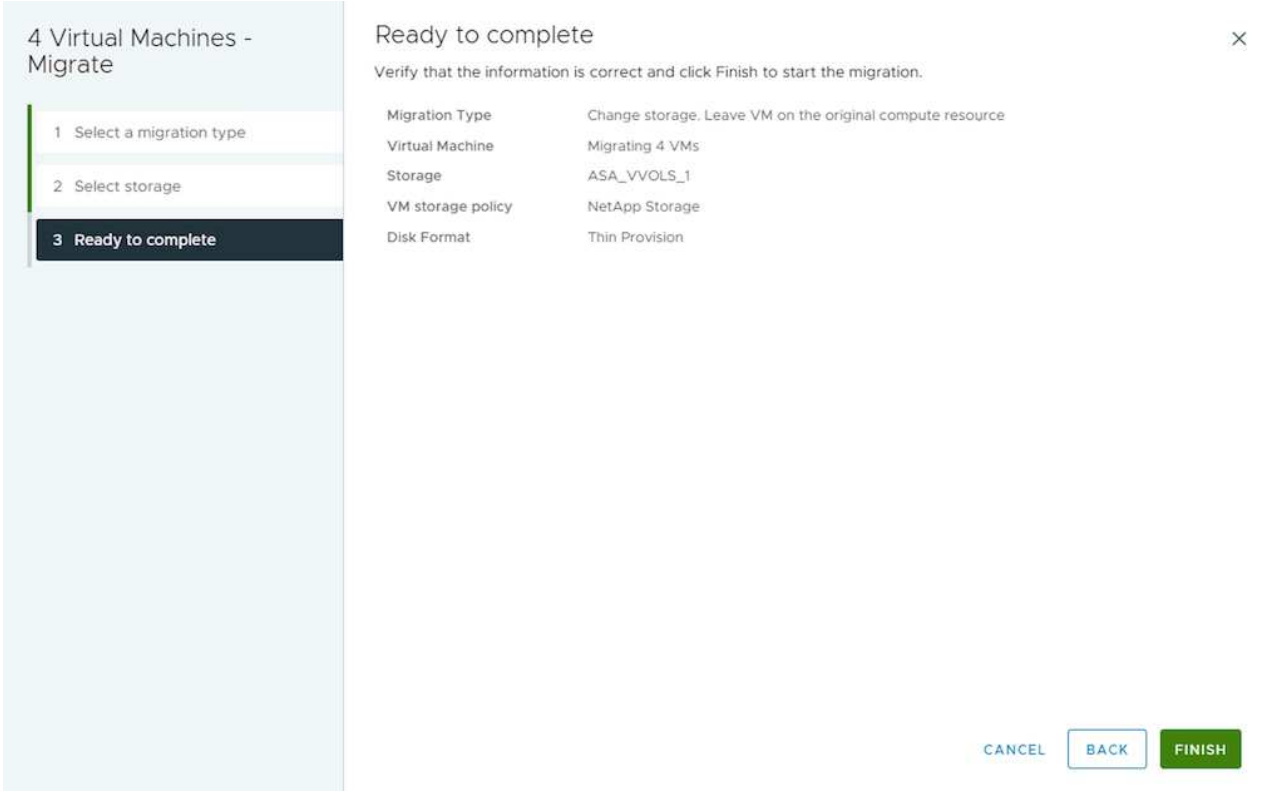
6. Selezionare la cartella VM in cui posizionare le VM di destinazione.



7. Selezionare il gruppo di porte di destinazione.



8. Rivedi e clicca su Fine.



Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

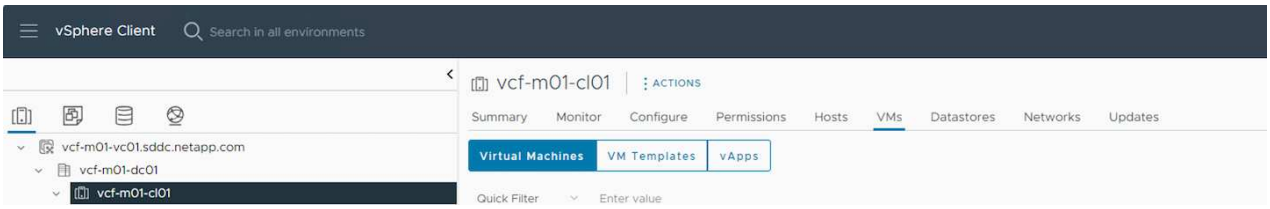
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migrazione di VM tra server vCenter nello stesso dominio SSO

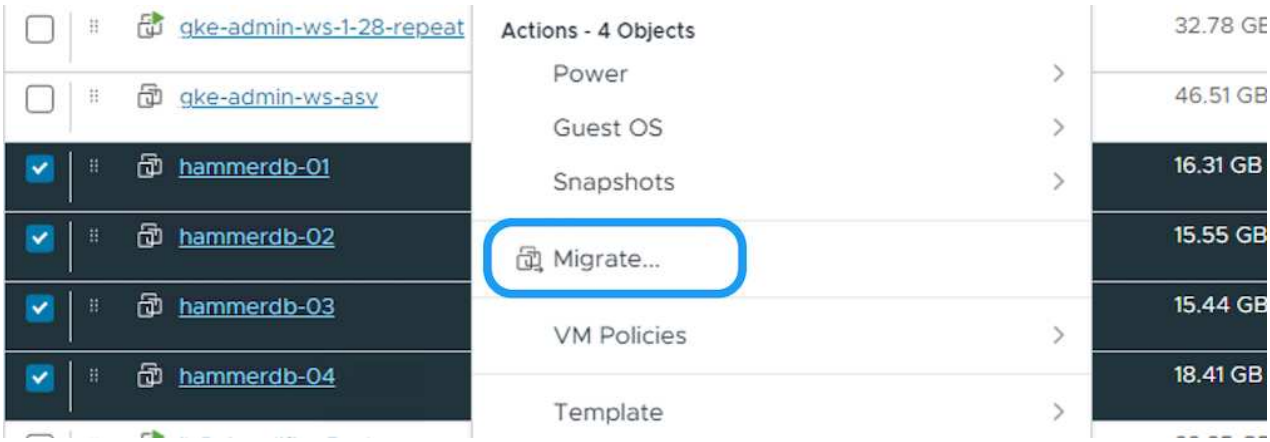
Per migrare le VM sul nuovo server vCenter elencato nella stessa interfaccia utente di vSphere Client, seguire la procedura seguente.

> Per requisiti aggiuntivi come le versioni di vCenter di origine e di destinazione, ecc., controllare "Documentazione vSphere sui requisiti per vMotion tra le istanze del server vCenter"

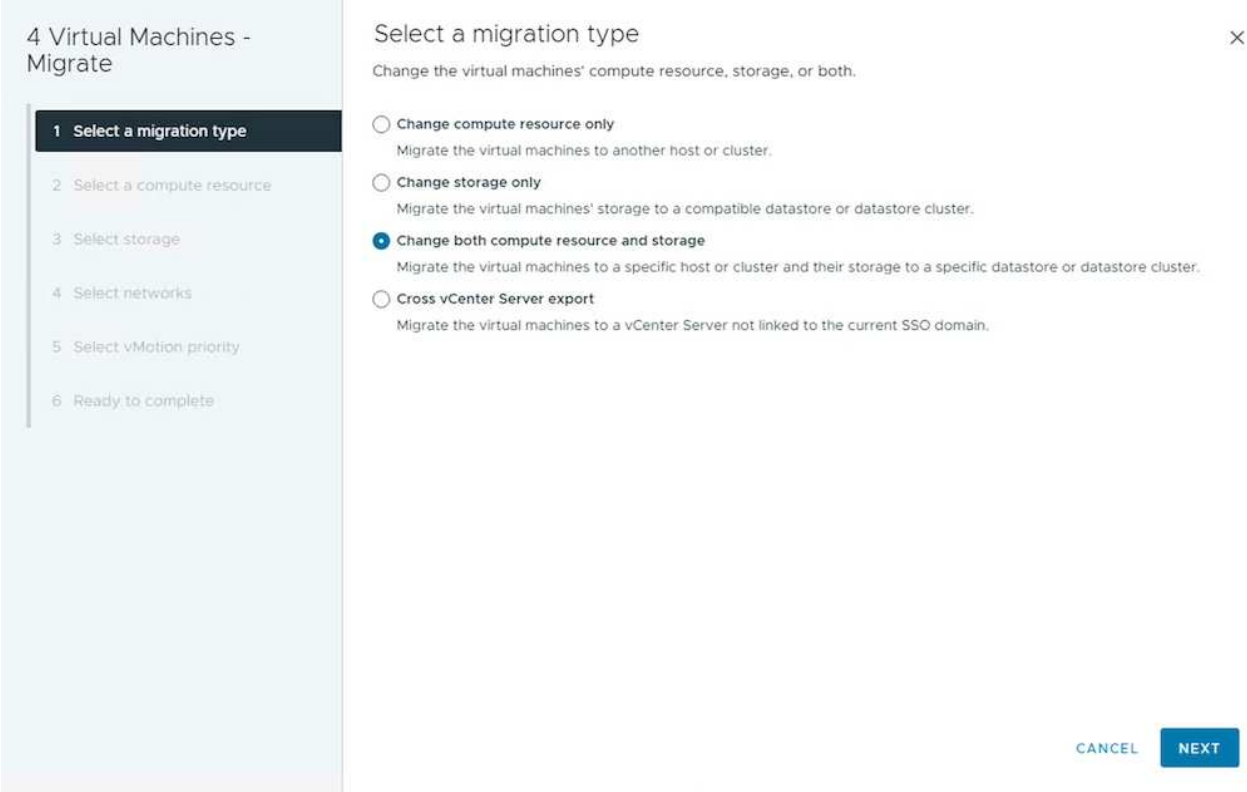
1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VM.



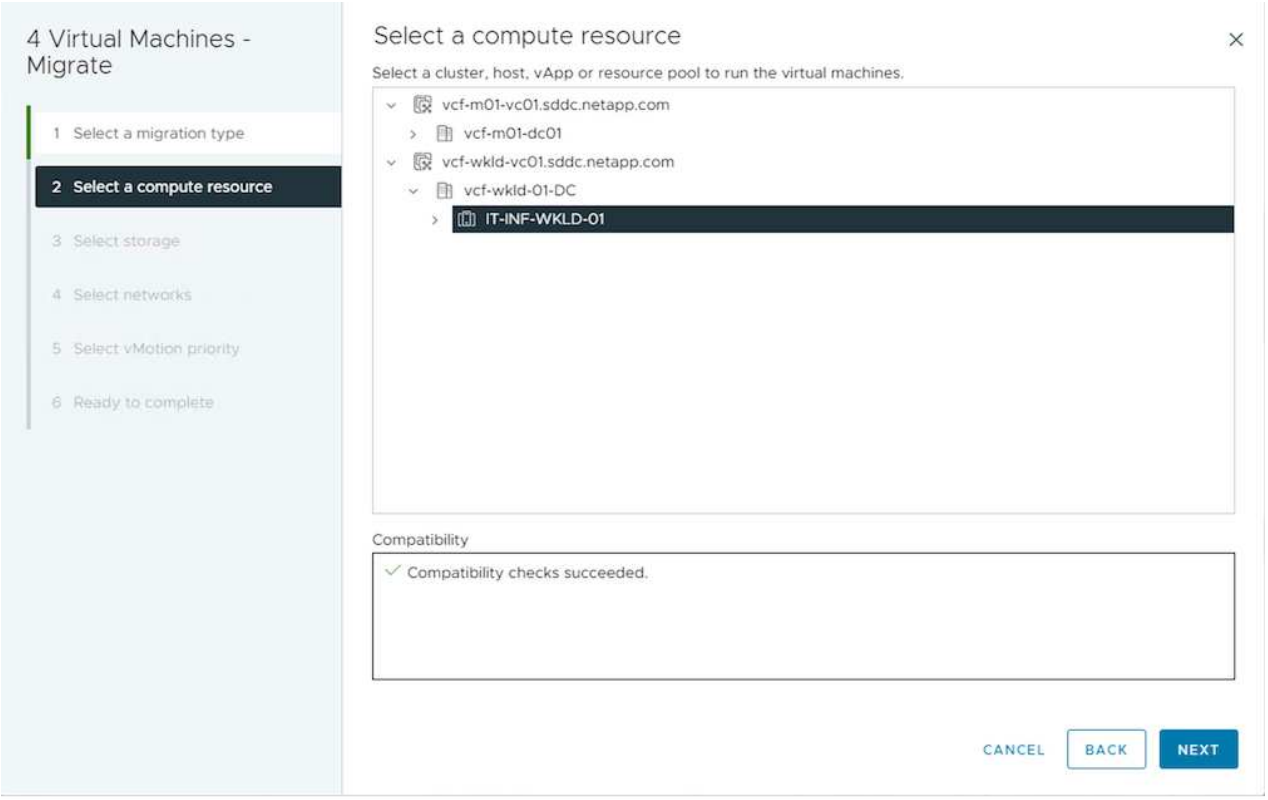
2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.



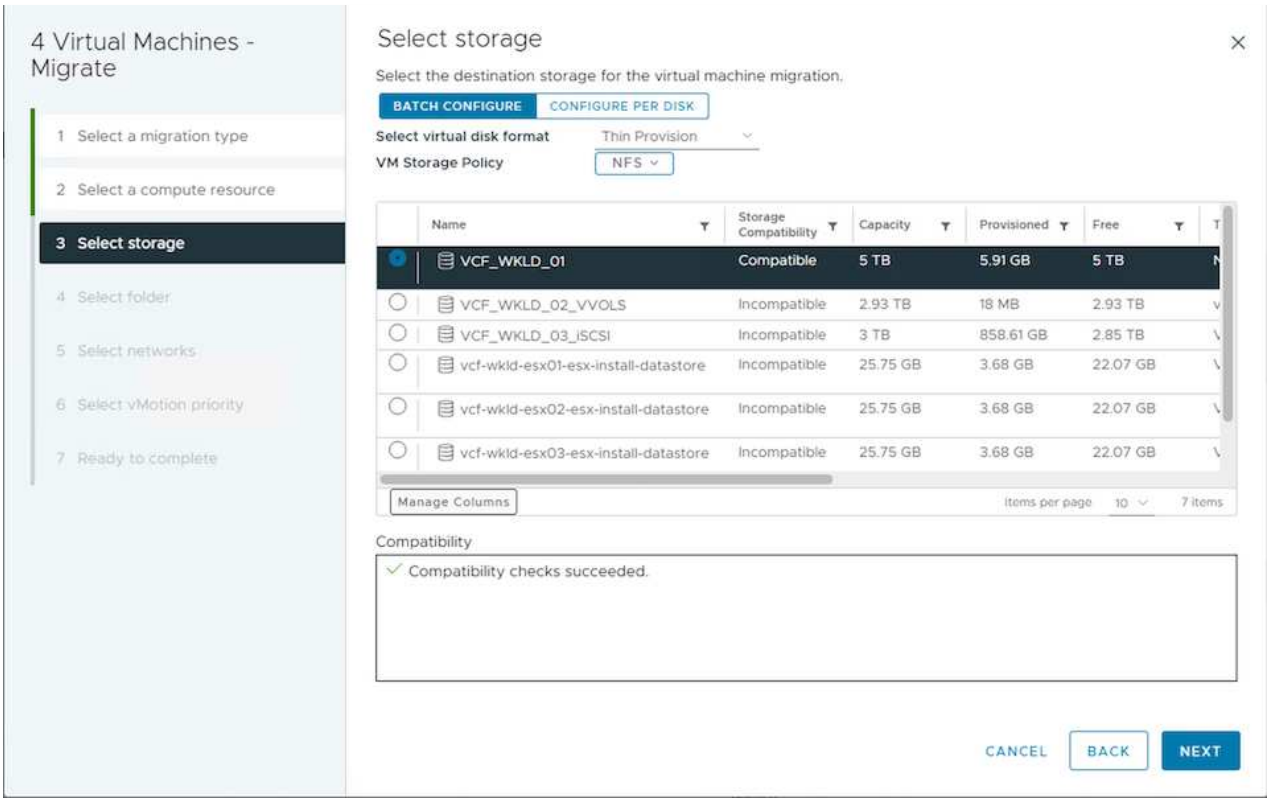
3. Scegli l'opzione per modificare le risorse di elaborazione e di archiviazione, fai clic su Avanti



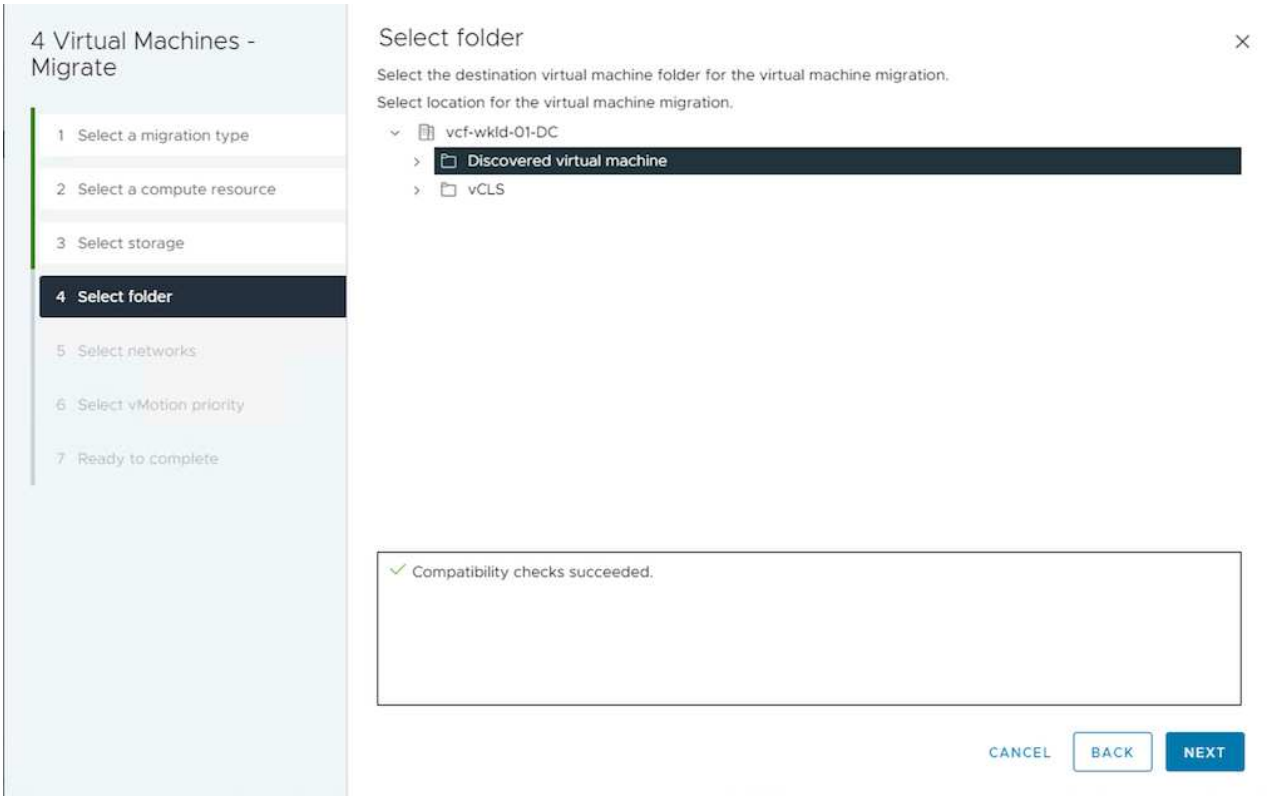
4. Selezionare il cluster di destinazione nel server vCenter di destinazione.



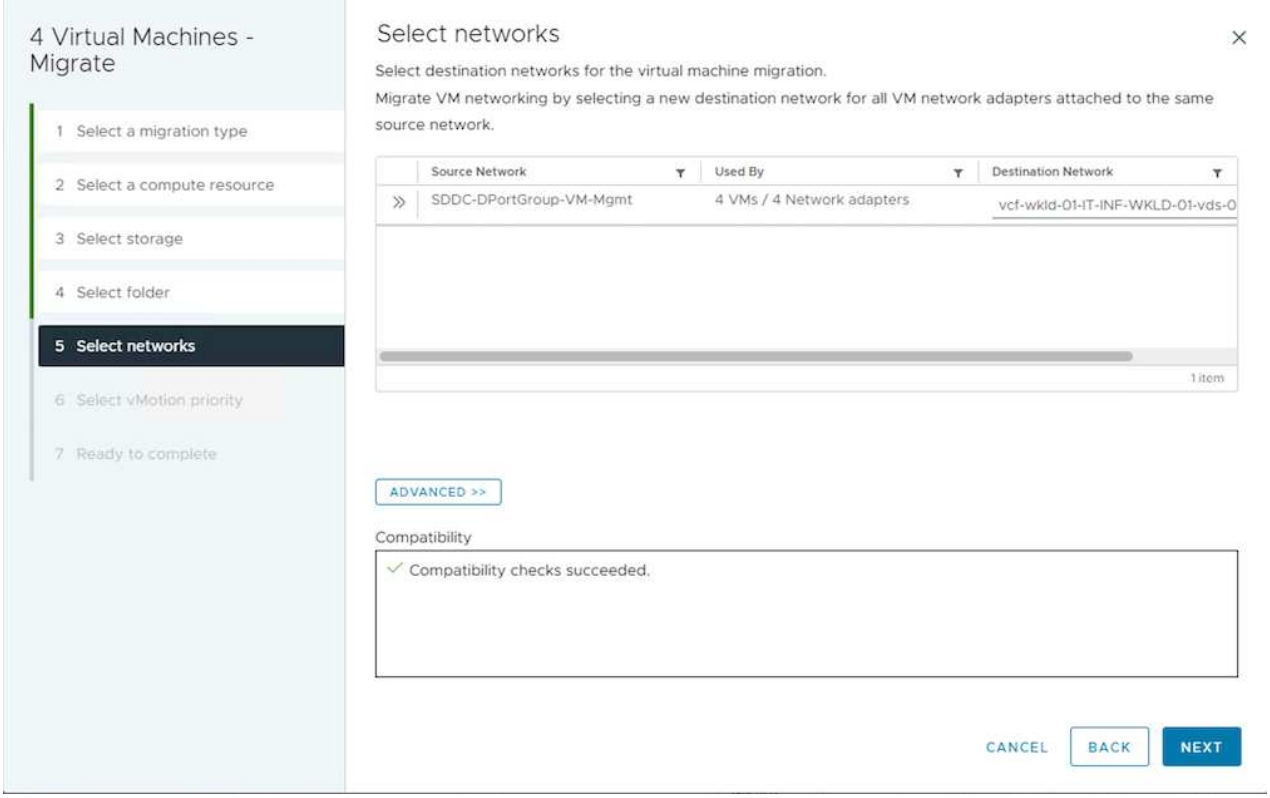
5. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.



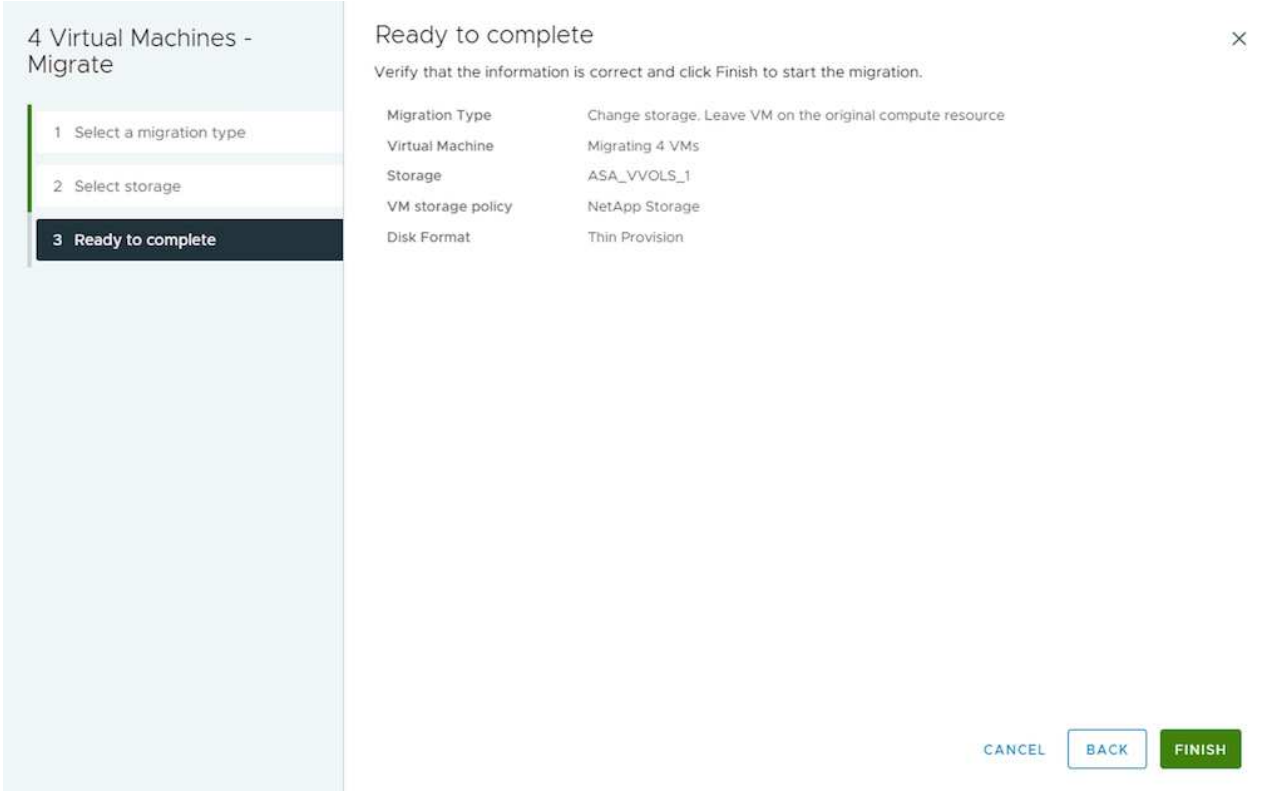
6. Selezionare la cartella VM in cui posizionare le VM di destinazione.



7. Selezionare il gruppo di porte di destinazione.



8. Esaminare le opzioni di migrazione e fare clic su Fine.



Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

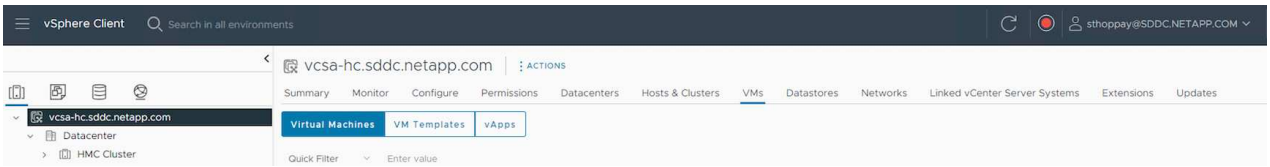
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migrazione di VM tra server vCenter in diversi domini SSO

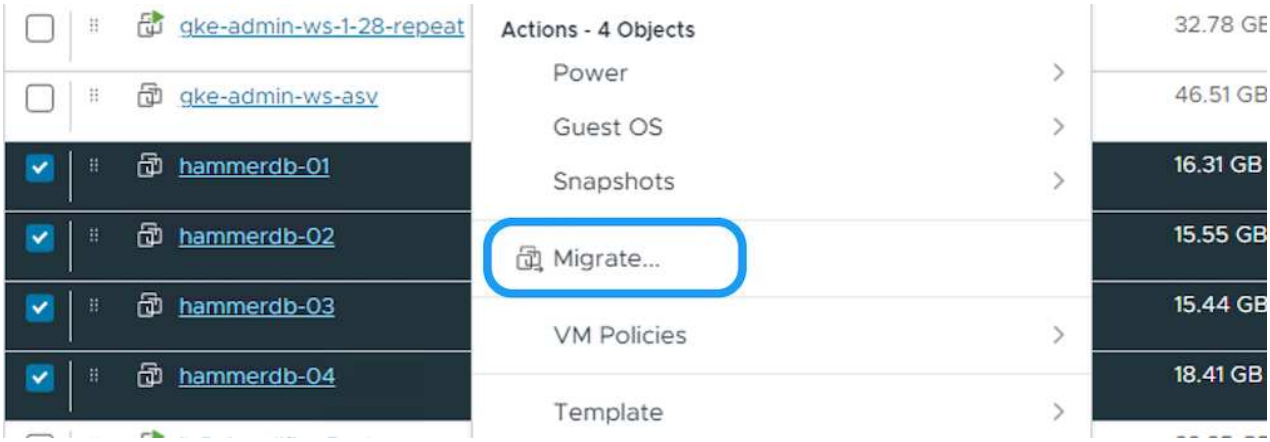
> Questo scenario presuppone che la comunicazione esista tra i server vCenter. In caso contrario, controllare lo scenario di ubicazione dei data center elencato di seguito. Per i prerequisiti, controllare "Documentazione vSphere su Advanced Cross vCenter vMotion"

Per migrare le VM su diversi server vCenter tramite l'interfaccia utente, seguire la procedura seguente.

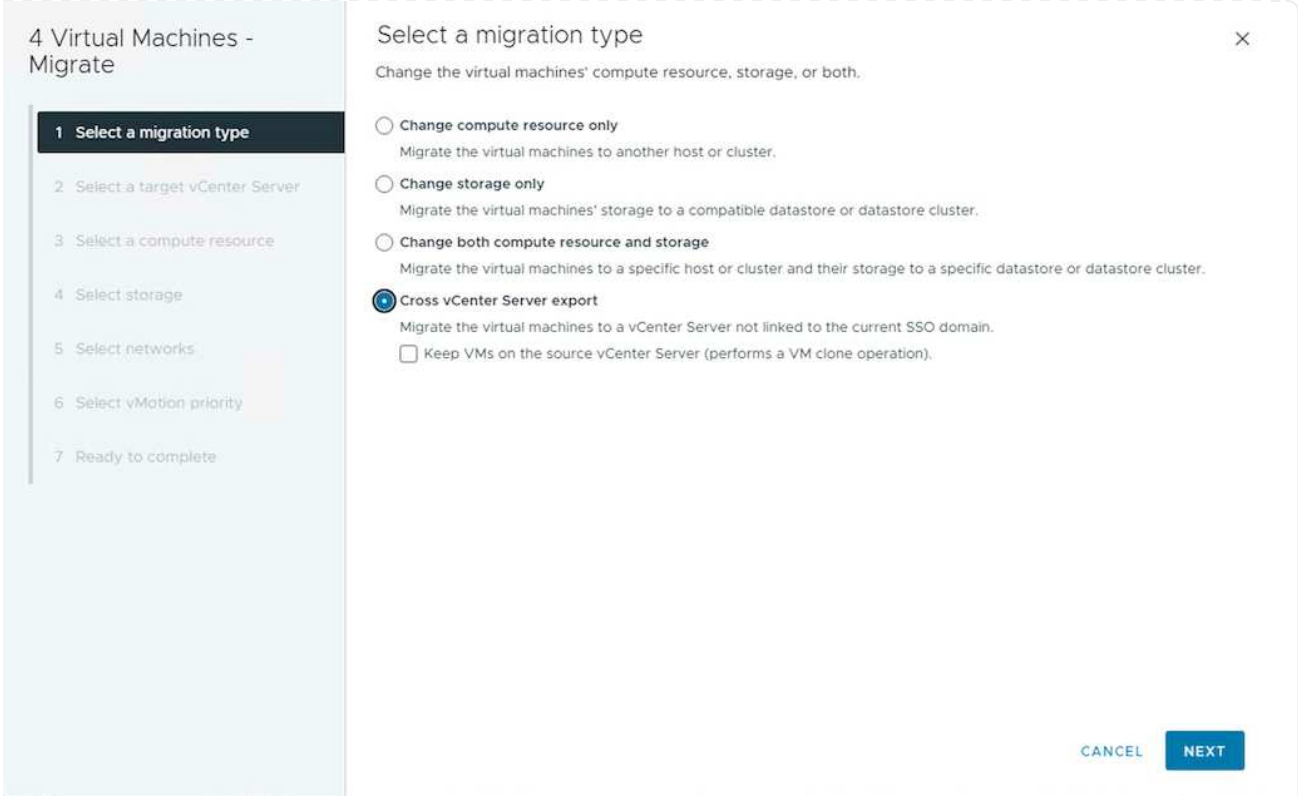
1. Con vSphere Web Client, seleziona il server vCenter di origine e fai clic sulla scheda VM.



2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

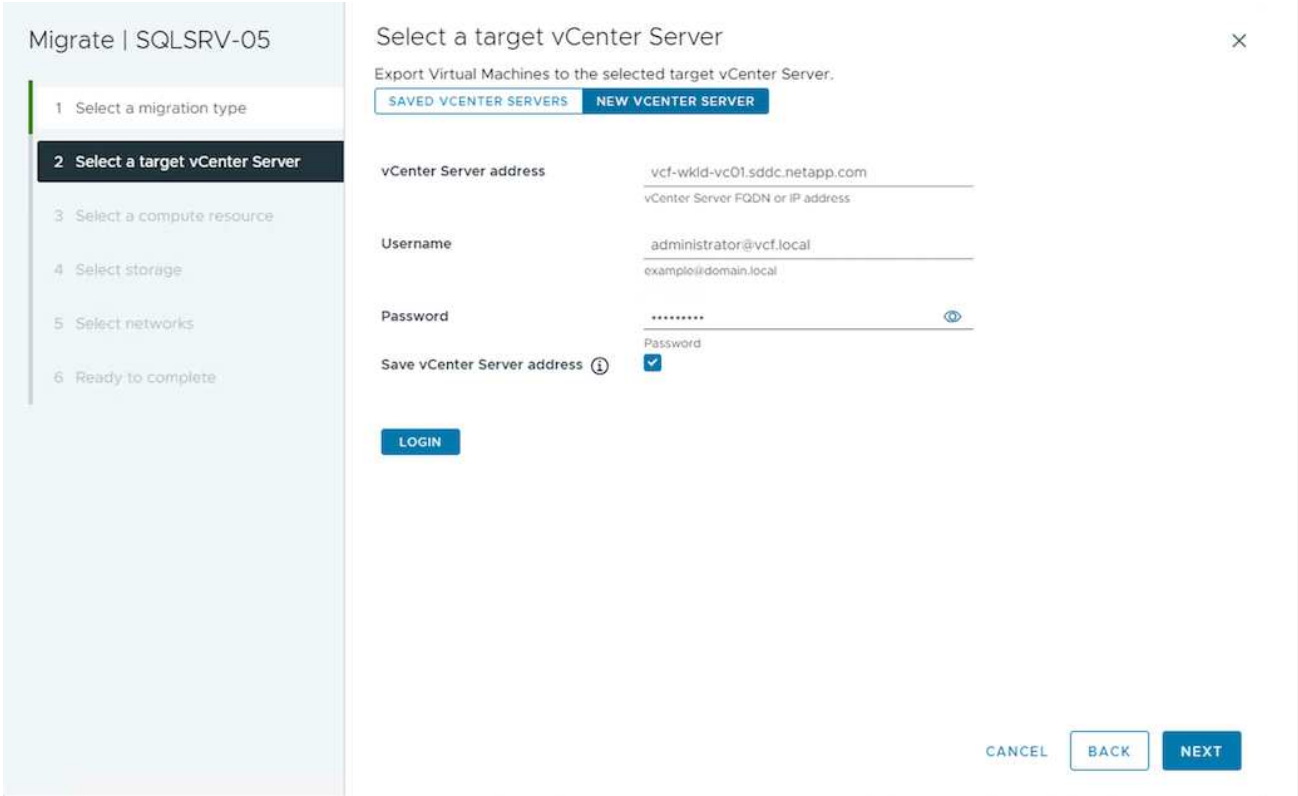


3. Scegli l'opzione Esportazione tra server vCenter, fai clic su Avanti

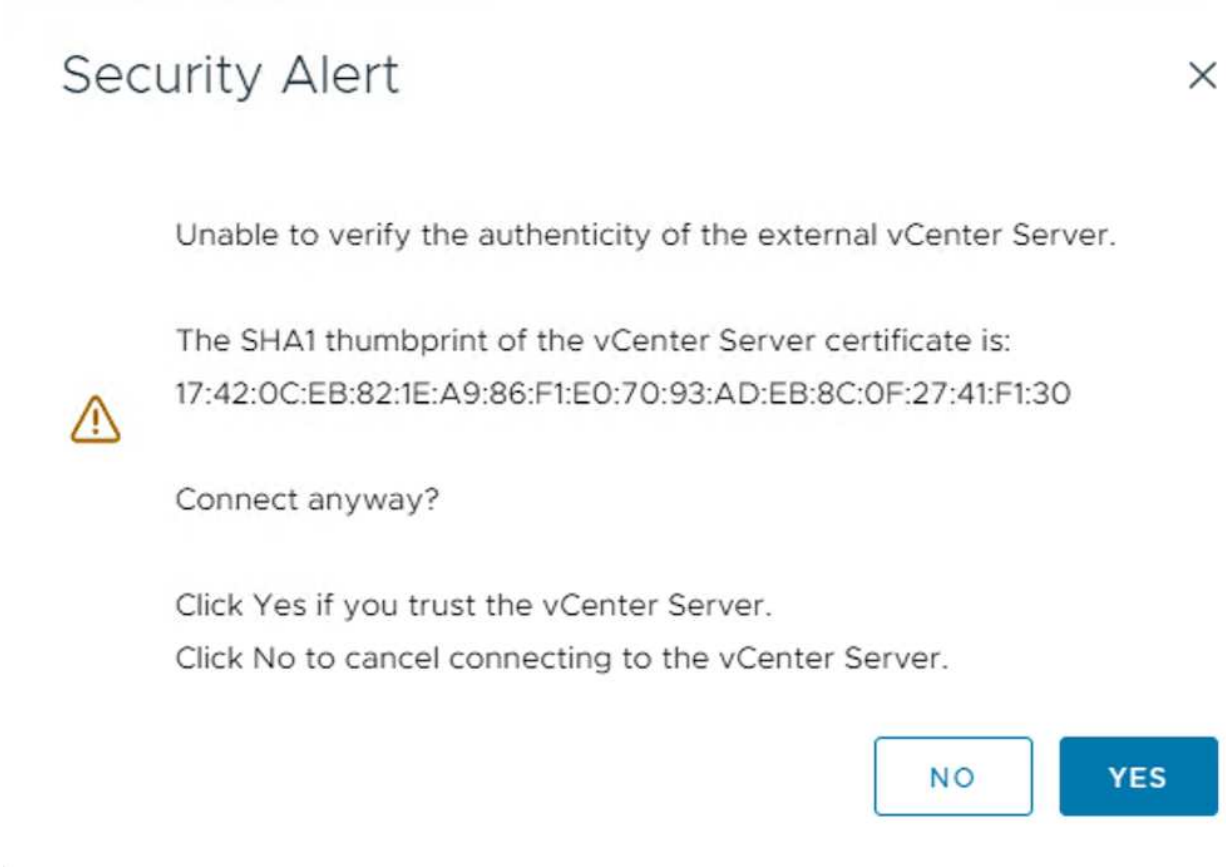


La VM può anche essere importata dal server vCenter di destinazione. Per tale procedura, controllare "Importa o clona una macchina virtuale con Advanced Cross vCenter vMotion"

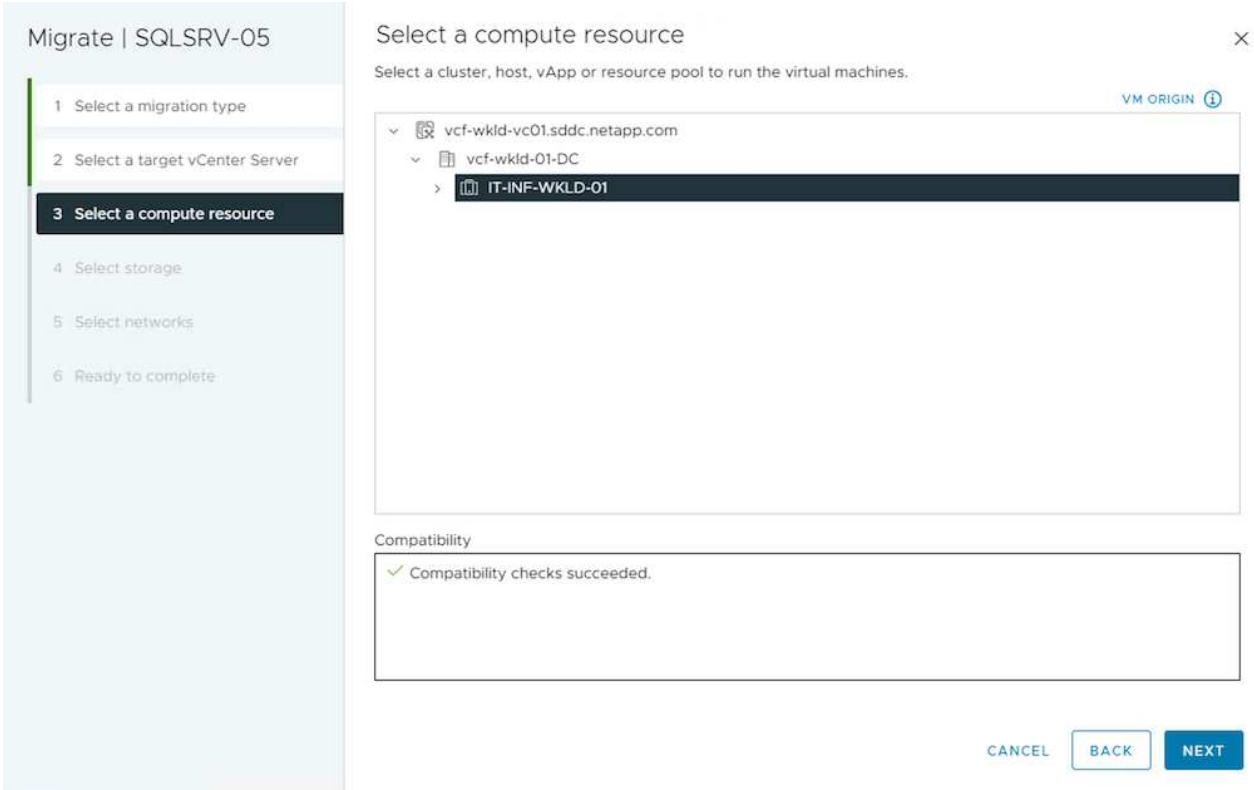
4. Fornire i dettagli delle credenziali vCenter e fare clic su Accedi.



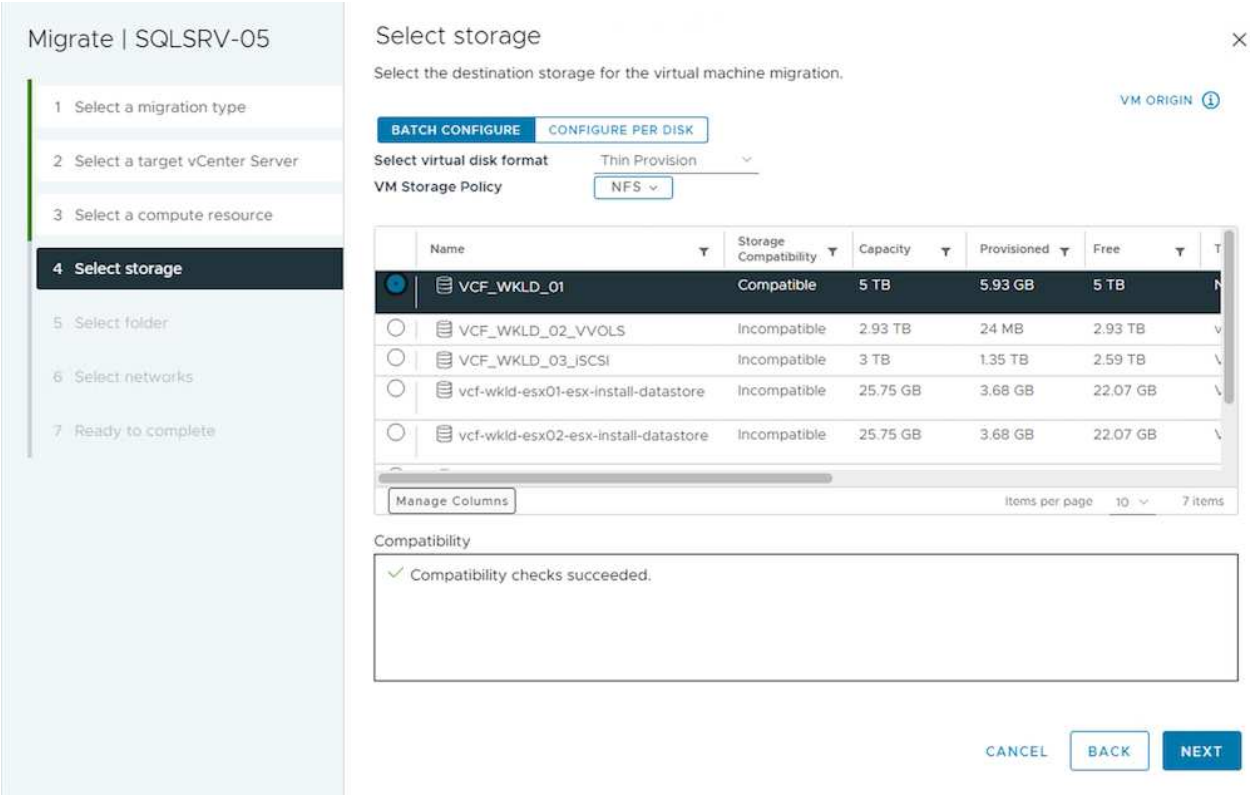
5. Conferma e accetta l'impronta digitale del certificato SSL del server vCenter



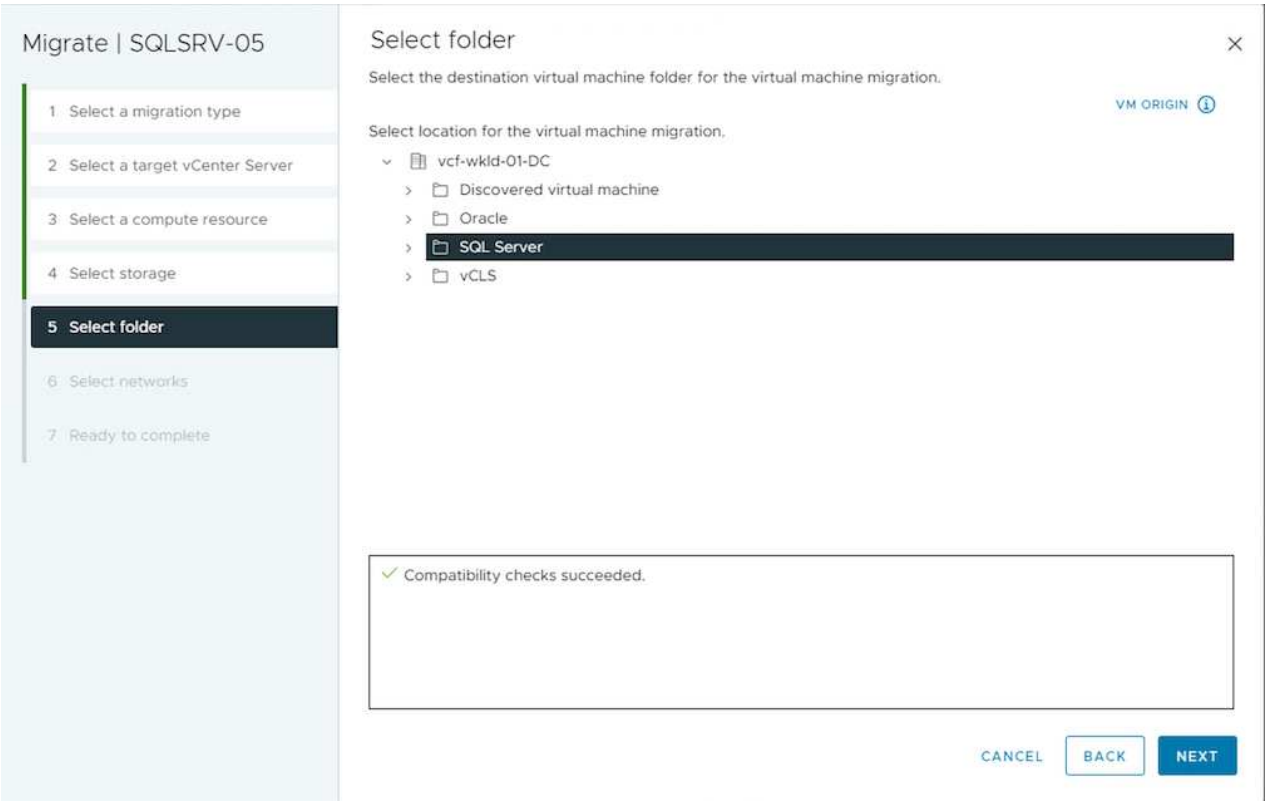
6. Espandi il vCenter di destinazione e seleziona il cluster di elaborazione di destinazione.



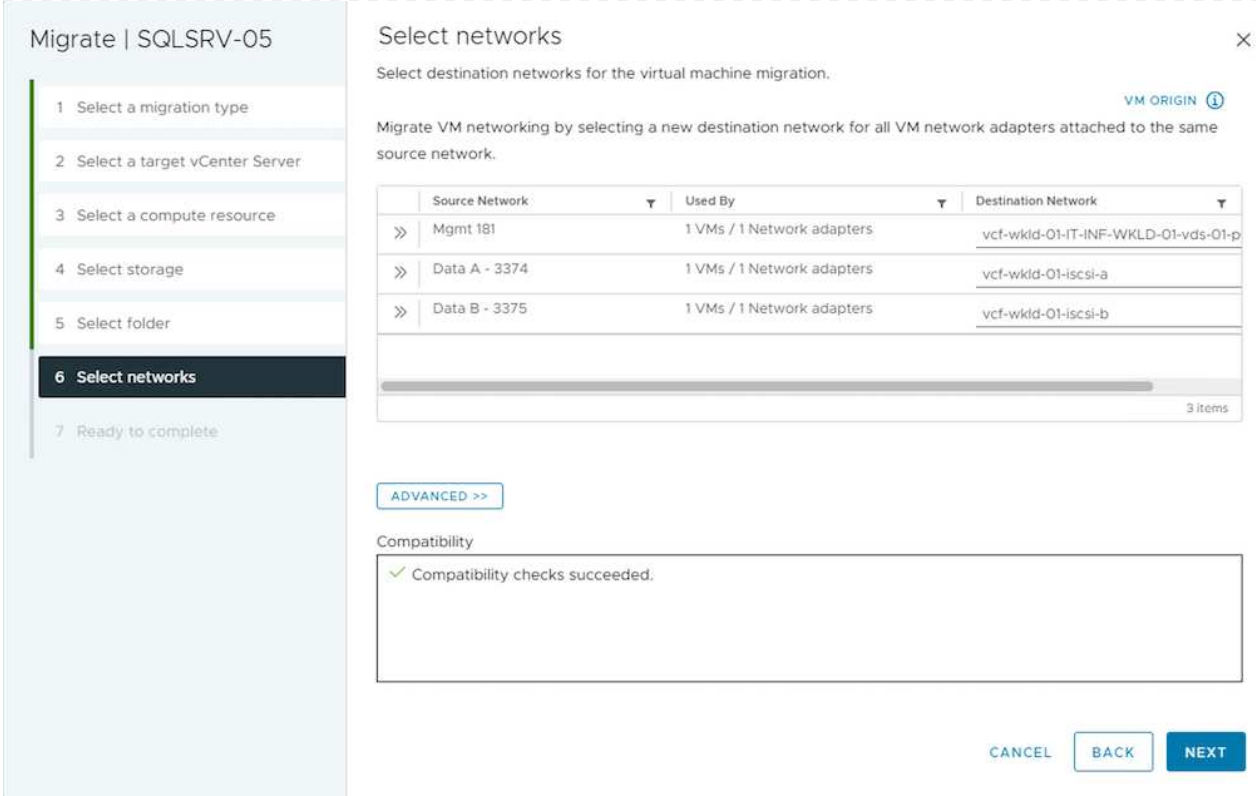
7. Selezionare il datastore di destinazione in base ai criteri di archiviazione della VM.



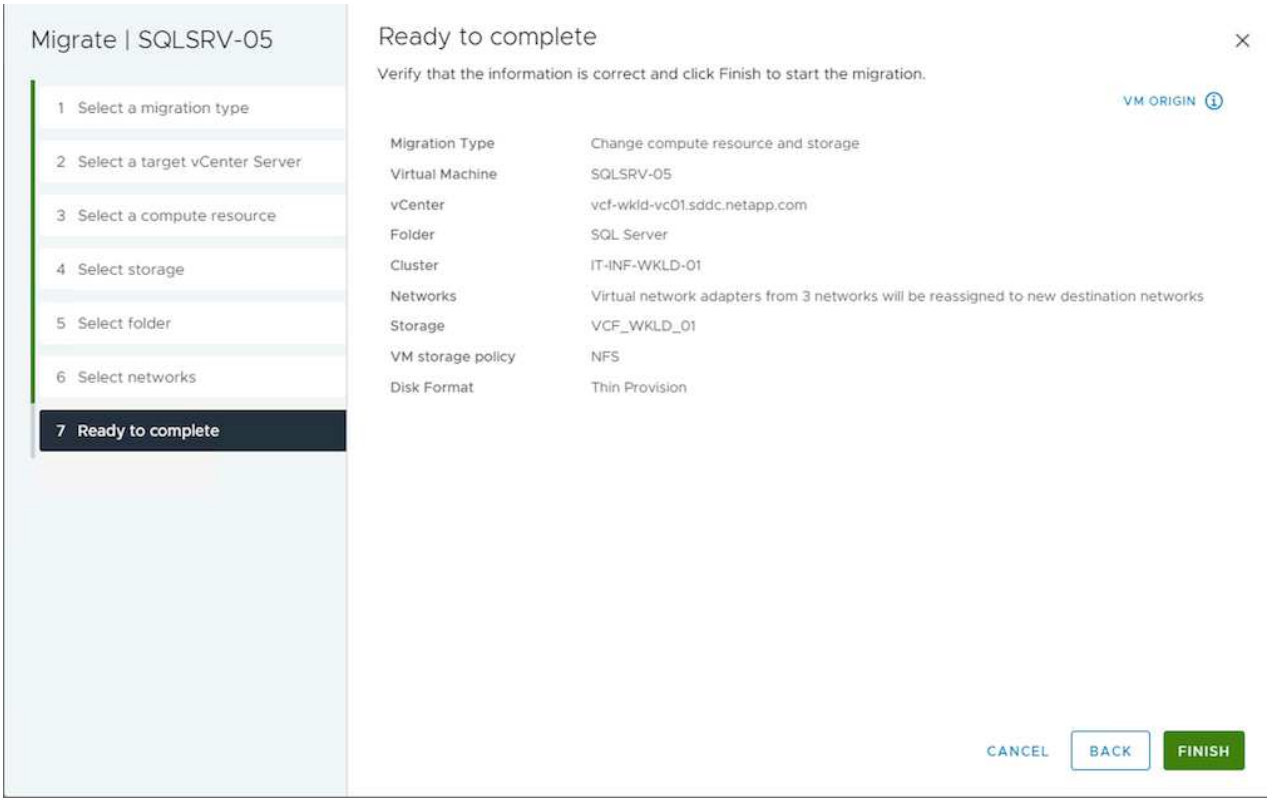
8. Selezionare la cartella della macchina virtuale di destinazione.



9. Selezionare il portgroup VM per ogni mappatura della scheda di interfaccia di rete.



10. Rivedere e fare clic su Fine per avviare vMotion sui server vCenter.



Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migrazione di VM tra le sedi dei data center

- Quando il traffico di Livello 2 viene distribuito su più data center tramite NSX Federation o altre opzioni, seguire la procedura per la migrazione delle VM su più server vCenter.
- HCX fornisce vari "tipi di migrazione" inclusa la Replication Assisted vMotion nei data center per spostare le VM senza tempi di inattività.
- "Site Recovery Manager (SRM)"è in genere destinato a scopi di Disaster Recovery e spesso utilizzato anche per la migrazione pianificata mediante replica basata su array di archiviazione.
- I prodotti di protezione continua dei dati (CDP) utilizzano "API vSphere per IO (VAIO)" per intercettare i dati e inviarne una copia a una posizione remota per una soluzione RPO prossima allo zero.
- È possibile utilizzare anche prodotti di backup e ripristino. Ma spesso si traduce in un RTO più lungo.
- "BlueXP Disaster Recovery come servizio (DRaaS)"utilizza la replica basata su array di archiviazione e automatizza determinate attività per ripristinare le VM nel sito di destinazione.

Migrazione di VM in ambiente cloud ibrido

- "Configura la modalità ibrida collegata"e seguire la procedura di"Migrazione di VM tra server vCenter nello stesso dominio SSO"
- HCX fornisce vari "tipi di migrazione" incluso Replication Assisted vMotion nei data center per spostare la VM mentre è accesa.
  - "TR 4942: Migrazione dei carichi di lavoro al datastore FSx ONTAP utilizzando VMware HCX"
  - "TR-4940: Migrazione dei carichi di lavoro al datastore di Azure NetApp Files tramite VMware HCX - Guida introduttiva"
  - "Migrazione dei carichi di lavoro al datastore Google Cloud NetApp Volumes su Google Cloud VMware Engine utilizzando VMware HCX - Guida introduttiva"
- "BlueXP Disaster Recovery come servizio (DRaaS)"utilizza la replica basata su array di archiviazione e automatizza determinate attività per ripristinare le VM nel sito di destinazione.
- Con prodotti CDP (Continous Data Protection) supportati che utilizzano "API vSphere per IO (VAIO)" per intercettare i dati e inviarne una copia a una posizione remota per una soluzione RPO prossima allo zero.

Quando la VM di origine risiede sul datastore vVol a blocchi, può essere replicata con SnapMirror su Amazon FSx ONTAP o Cloud Volumes ONTAP (CVO) presso altri provider cloud supportati e utilizzata come volume iSCSI con VM cloud native.

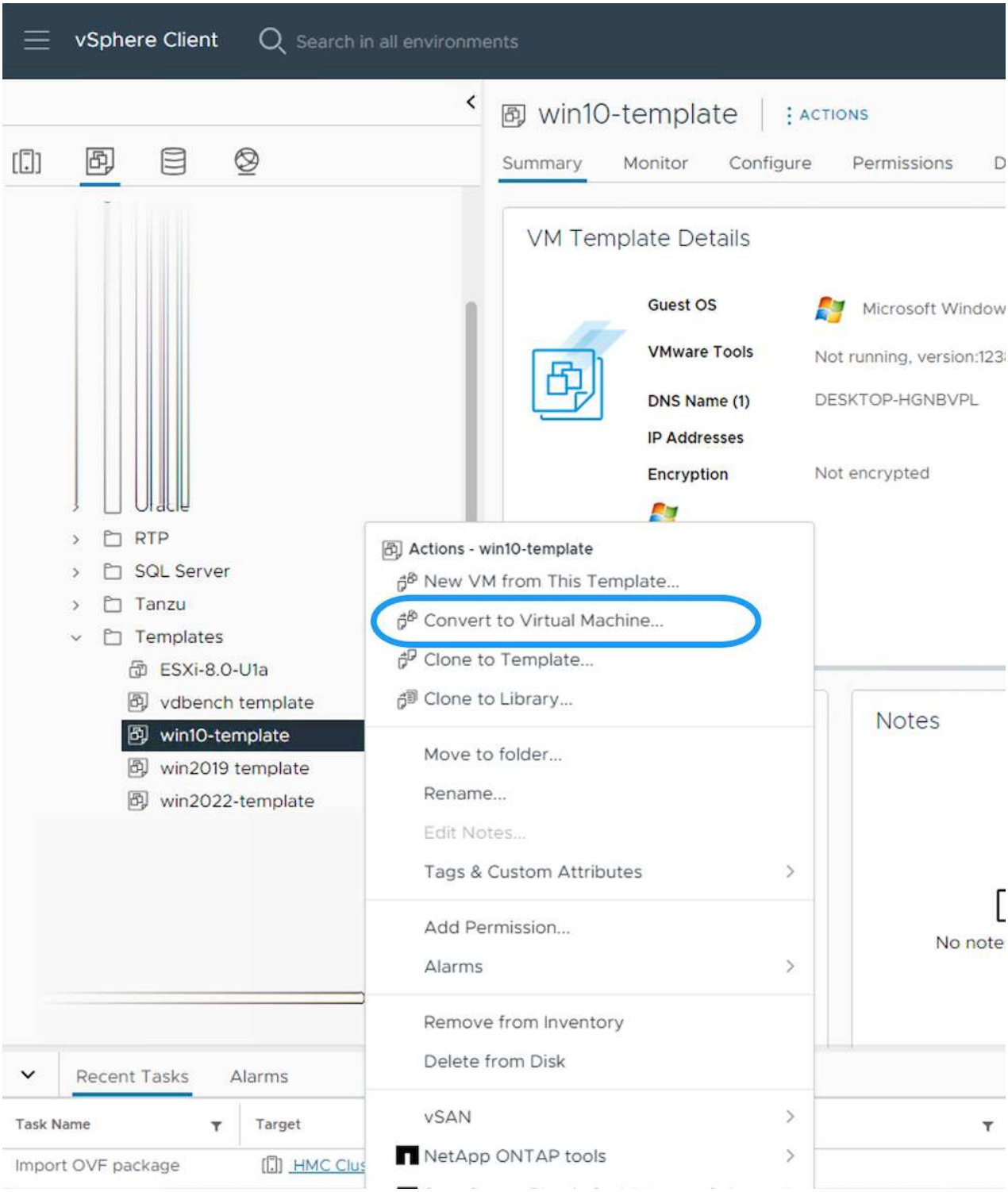
Scenari di migrazione dei modelli di VM

I modelli di VM possono essere gestiti da vCenter Server o da una libreria di contenuti. La distribuzione di modelli VM, modelli OVF e OVA e altri tipi di file viene gestita pubblicandoli nella libreria di contenuti locale e le librerie di contenuti remote possono sottoscriverli.

- I modelli di VM archiviati nell'inventario vCenter possono essere convertiti in VM e utilizzare le opzioni di migrazione VM.
- I modelli OVF e OVA e altri tipi di file memorizzati nella libreria di contenuti possono essere clonati in altre librerie di contenuti.
- I modelli VM della libreria di contenuti possono essere ospitati su qualsiasi datastore e devono essere aggiunti alla nuova libreria di contenuti.

Migrazione dei modelli di VM ospitati sul datastore

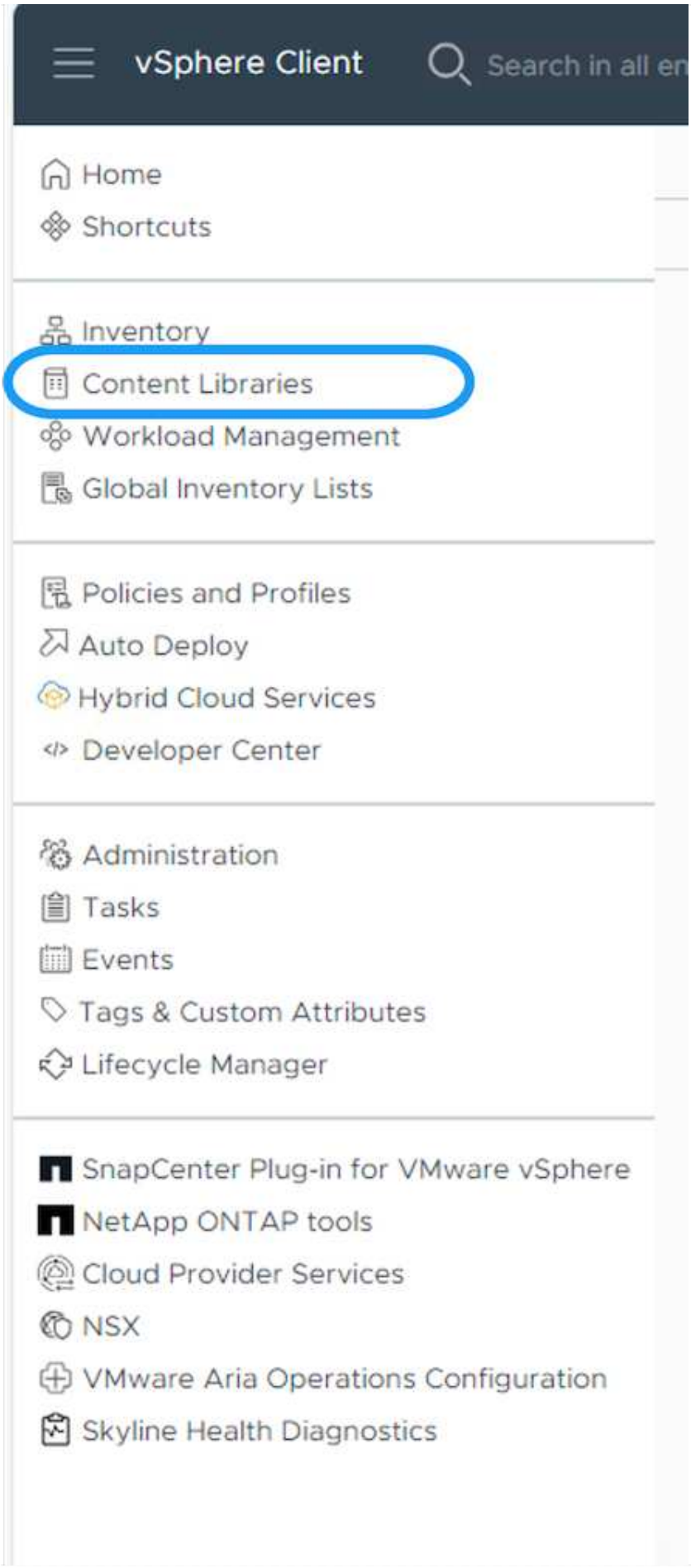
1. In vSphere Web Client, fare clic con il pulsante destro del mouse sul modello VM nella vista cartelle VM e modelli e selezionare l'opzione per convertire in VM.



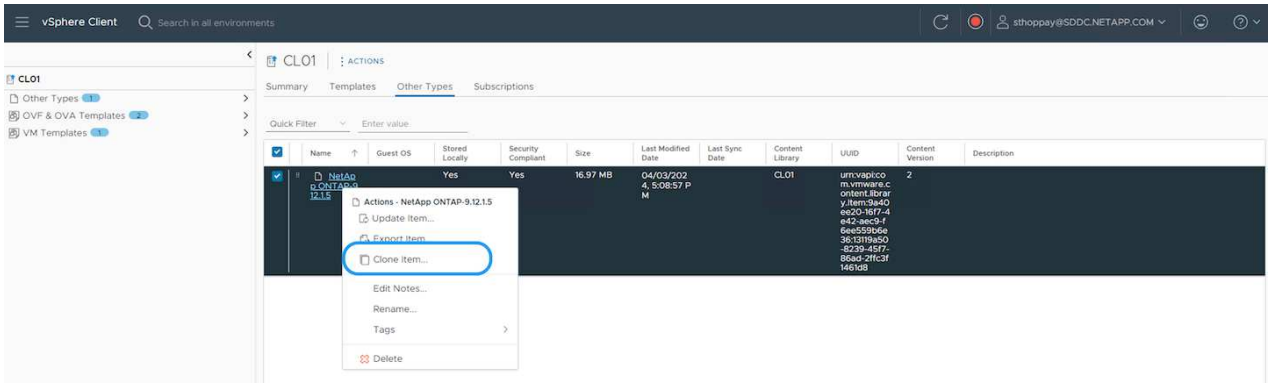
2. Una volta convertito in VM, seguire le opzioni di migrazione della VM.

Clonazione degli elementi della libreria dei contenuti

1. In vSphere Web Client, seleziona Librerie di contenuti

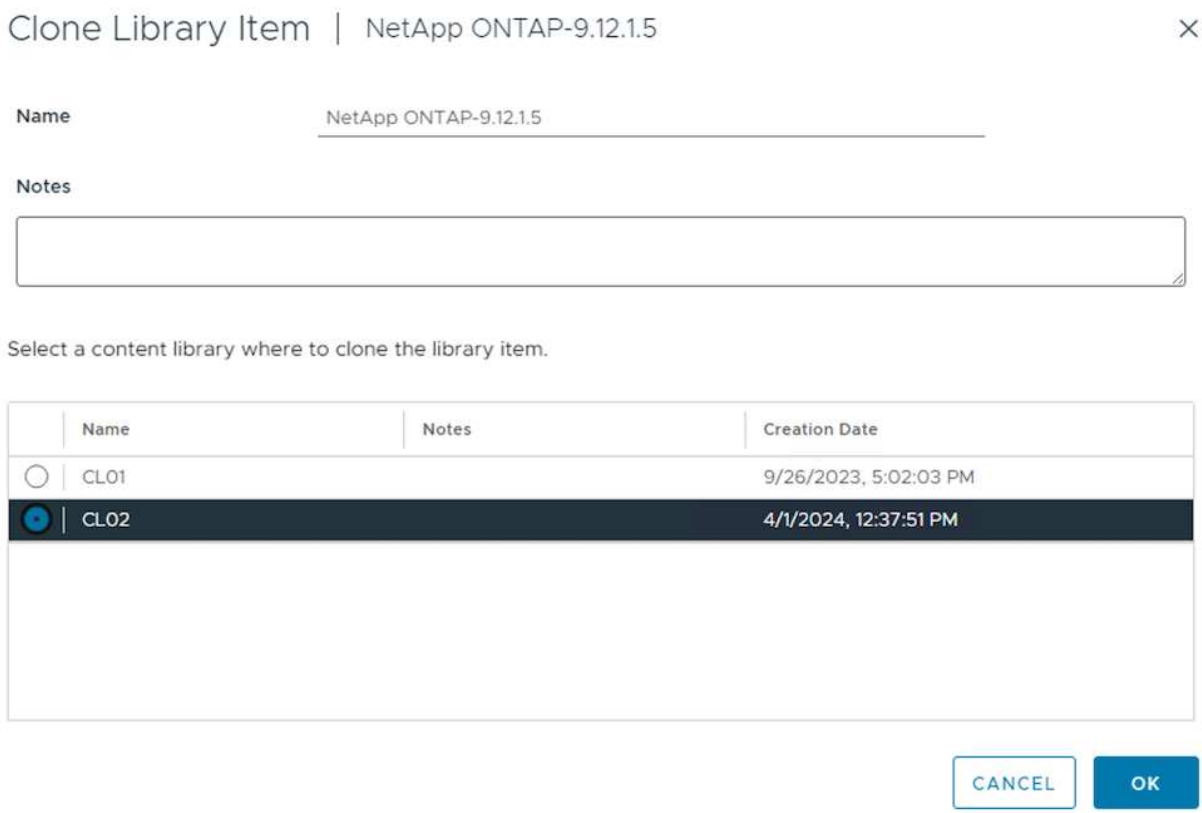

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. Seleziona la libreria di contenuti in cui si trova l'elemento che desideri clonare
3. Fare clic con il tasto destro del mouse sull'elemento e fare clic su Clona elemento.

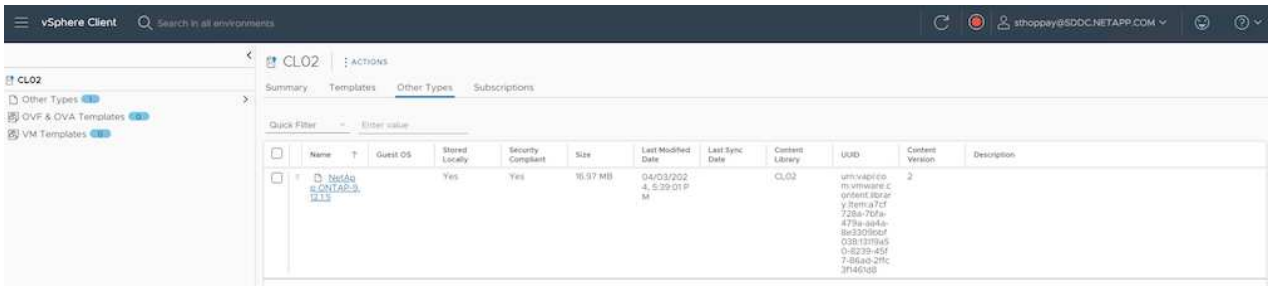


> Se si utilizza il menu Azione, assicurarsi che sia elencato l'oggetto di destinazione corretto per eseguire l'azione.

4. Selezionare la libreria di contenuti di destinazione e fare clic su OK.



5. Verificare che l'elemento sia disponibile nella libreria di contenuti di destinazione.

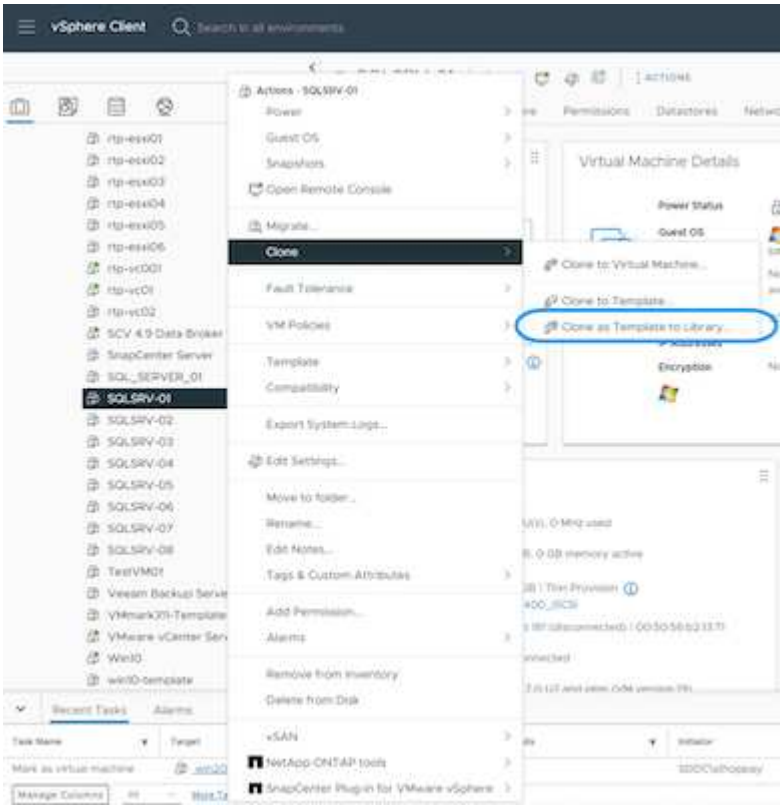


Ecco un esempio di script PowerCLI per copiare gli elementi della libreria di contenuti dalla libreria di contenuti CL01 a CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

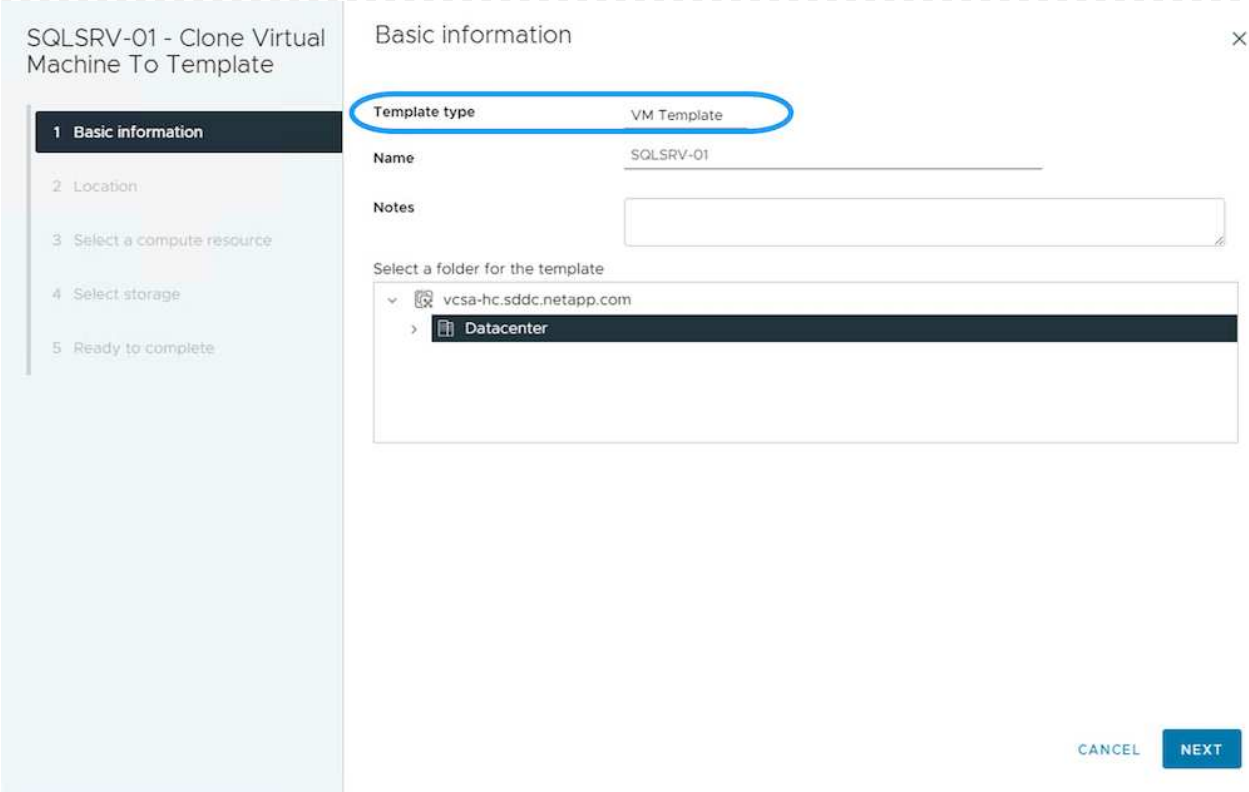
Aggiunta di VM come modelli nella libreria dei contenuti

1. In vSphere Web Client, seleziona la VM e fai clic con il pulsante destro del mouse per scegliere Clona come modello nella libreria



> Quando si seleziona il modello VM per la clonazione nella libreria, è possibile memorizzarlo solo come modello OVF e OVA e non come modello VM.

2. Verificare che il tipo di modello selezionato sia Modello VM e seguire le istruzioni della procedura guidata per completare l'operazione.



Per ulteriori dettagli sui modelli VM nella libreria di contenuti, controllare "Guida all'amministrazione della VM vSphere"

Casi d'uso

Migrazione da sistemi di archiviazione di terze parti (incluso vSAN) a datastore ONTAP .

- In base a dove è predisposto il datastore ONTAP , seleziona le opzioni di migrazione della VM sopra indicate.

Migrazione dalla versione precedente alla versione più recente di vSphere.

- Se l'aggiornamento sul posto non è possibile, è possibile creare un nuovo ambiente e utilizzare le opzioni di migrazione sopra indicate.

Nell'opzione di migrazione tra vCenter, importa dalla destinazione se l'opzione di esportazione non è disponibile sulla sorgente. Per tale procedura, controllare"Importa o clona una macchina virtuale con Advanced Cross vCenter vMotion"

Migrazione al dominio del carico di lavoro VCF.

- Migrare le VM da ciascun cluster vSphere al dominio del carico di lavoro di destinazione.

> Per consentire la comunicazione di rete con le VM esistenti su altri cluster sul vCenter di origine, estendere il segmento NSX aggiungendo gli host vCenter vSphere di origine alla zona di trasporto oppure utilizzare il bridge L2 sull'edge per consentire la comunicazione L2 nella VLAN. Controllare la documentazione NSX di "Configurare una VM Edge per il bridging"

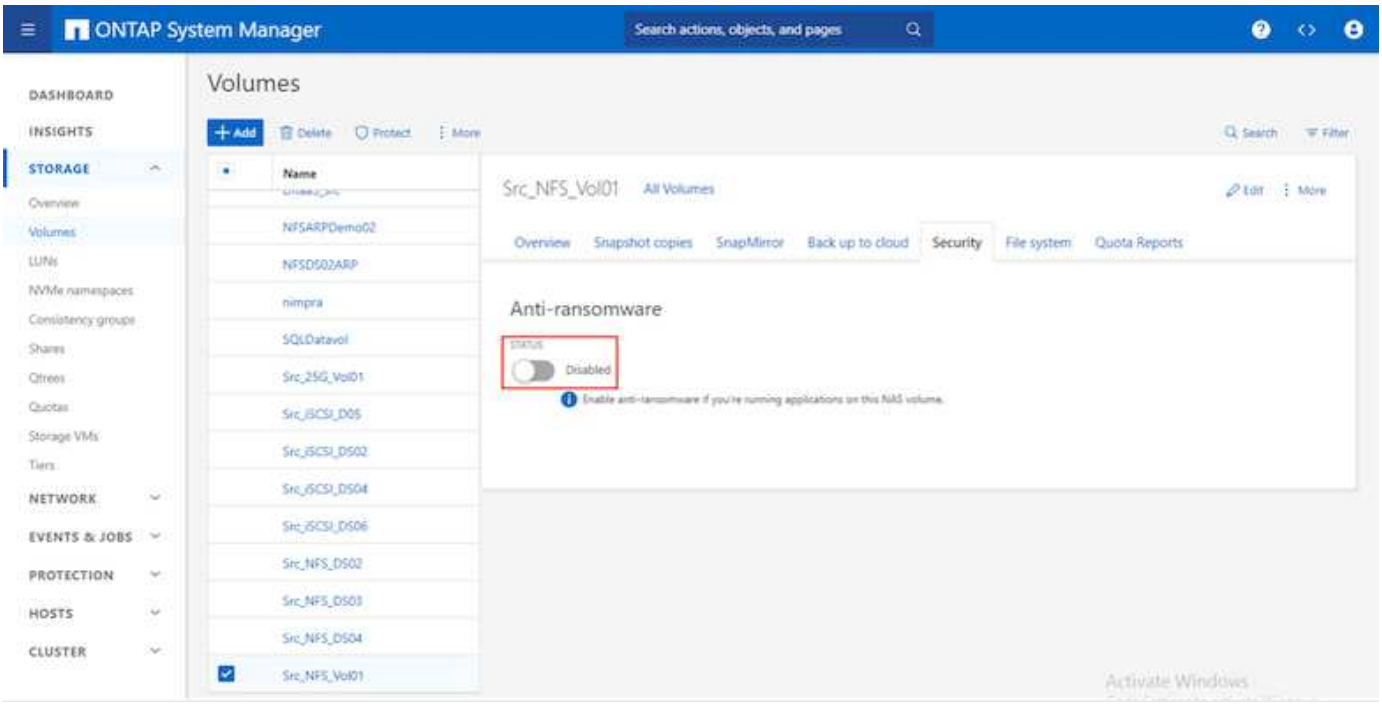
Risorse aggiuntive

- "Migrazione della macchina virtuale vSphere"
- "Migrazione di macchine virtuali con vSphere vMotion"
- "Configurazioni del gateway di livello 0 nella federazione NSX"
- "Guida utente HCX 4.8"
- "Documentazione di VMware Live Recovery"
- "BlueXP disaster recovery per VMware"

Protezione autonoma contro i ransomware per l'archiviazione NFS

Rilevare il ransomware il prima possibile è fondamentale per prevenirne la diffusione ed evitare costosi tempi di inattività. Una strategia efficace per il rilevamento dei ransomware deve integrare più livelli di protezione a livello di host ESXi e di VM guest. Sebbene vengano implementate molteplici misure di sicurezza per creare una difesa completa contro gli attacchi ransomware, ONTAP consente di aggiungere ulteriori livelli di protezione all'approccio di difesa complessivo. Per citarne alcune, si inizia con gli snapshot, la protezione autonoma dai ransomware, gli snapshot a prova di manomissione e così via.

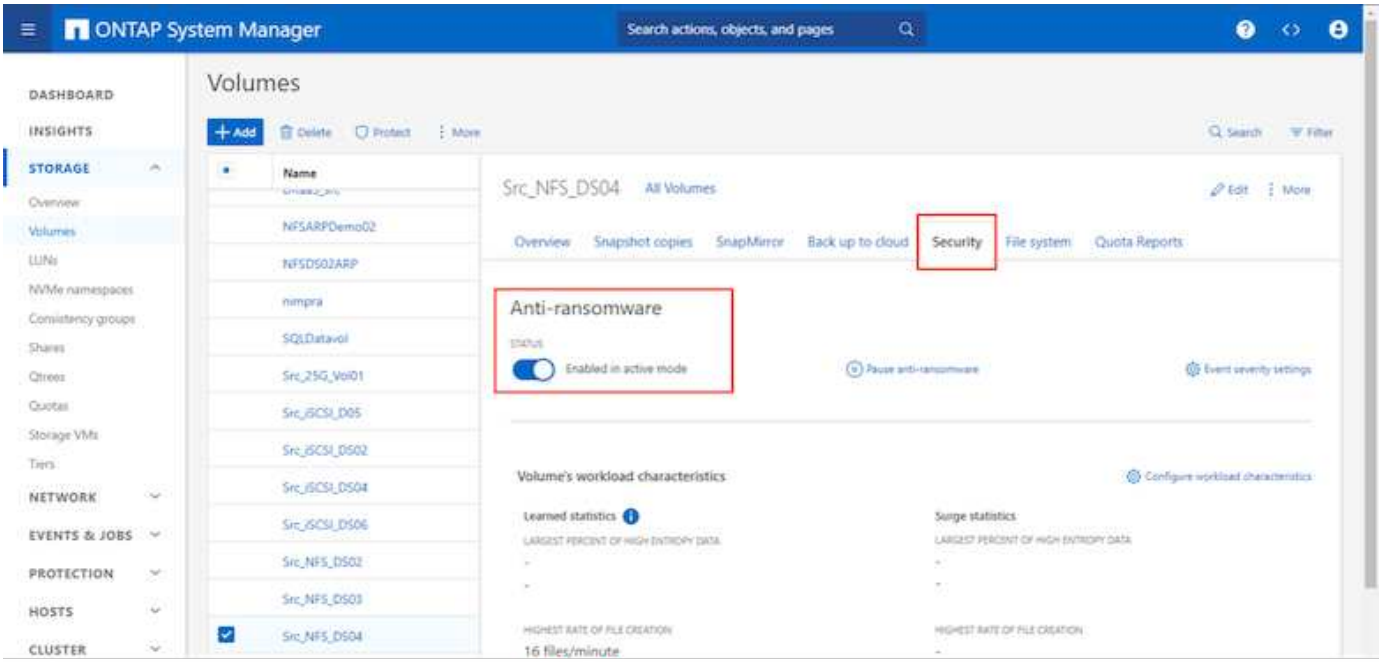
Diamo un'occhiata a come le funzionalità sopra menzionate interagiscono con VMware per proteggere e recuperare i dati dal ransomware. Per proteggere vSphere e le VM guest dagli attacchi, è essenziale adottare diverse misure, tra cui la segmentazione, l'utilizzo di EDR/XDR/SIEM per gli endpoint, l'installazione di aggiornamenti di sicurezza e il rispetto delle linee guida di rafforzamento appropriate. Ogni macchina virtuale residente su un datastore ospita anche 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, abilitare la protezione autonoma contro i ransomware (ARP) sul volume NFS che alimenta il datastore. ARP sfrutta l'apprendimento automatico integrato che analizza l'attività del carico di lavoro e l'entropia dei dati per rilevare automaticamente il ransomware. ARP è configurabile tramite l'interfaccia di gestione integrata ONTAP o il System Manager ed è abilitato in base al volume.



Con il nuovo NetApp ARP/AI, attualmente in anteprima tecnologica, non è necessaria una modalità di apprendimento. Può invece passare direttamente alla modalità attiva grazie alla sua capacità di rilevamento ransomware basata sull'intelligenza artificiale.

Con ONTAP One, tutte queste funzionalità sono completamente gratuite. Accedi alla solida suite di protezione dei dati e sicurezza di NetApp e a tutte le funzionalità offerte da ONTAP senza preoccuparti degli ostacoli legati alle licenze.

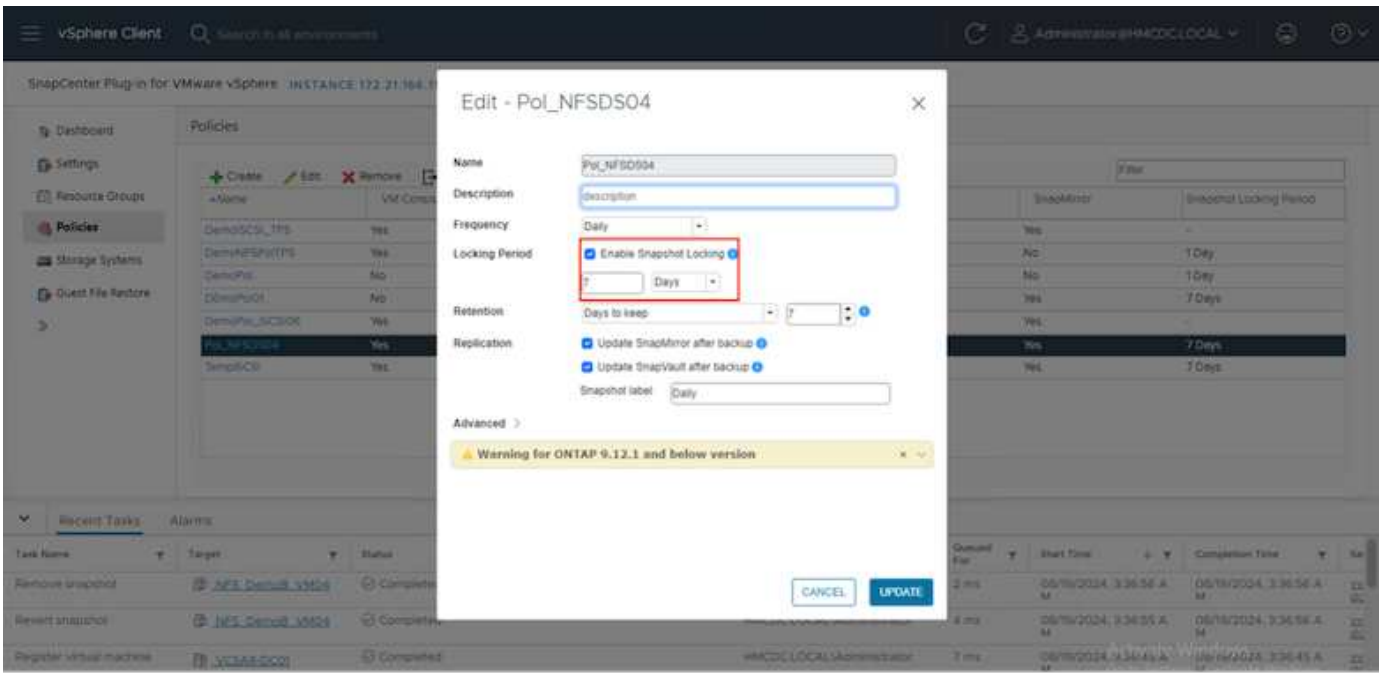
Una volta in modalità attiva, inizia a cercare attività anomale nel volume che potrebbero potenzialmente essere un ransomware. Se viene rilevata un'attività anomala, viene immediatamente eseguita una copia Snapshot automatica, che fornisce un punto di ripristino il più vicino possibile all'infezione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



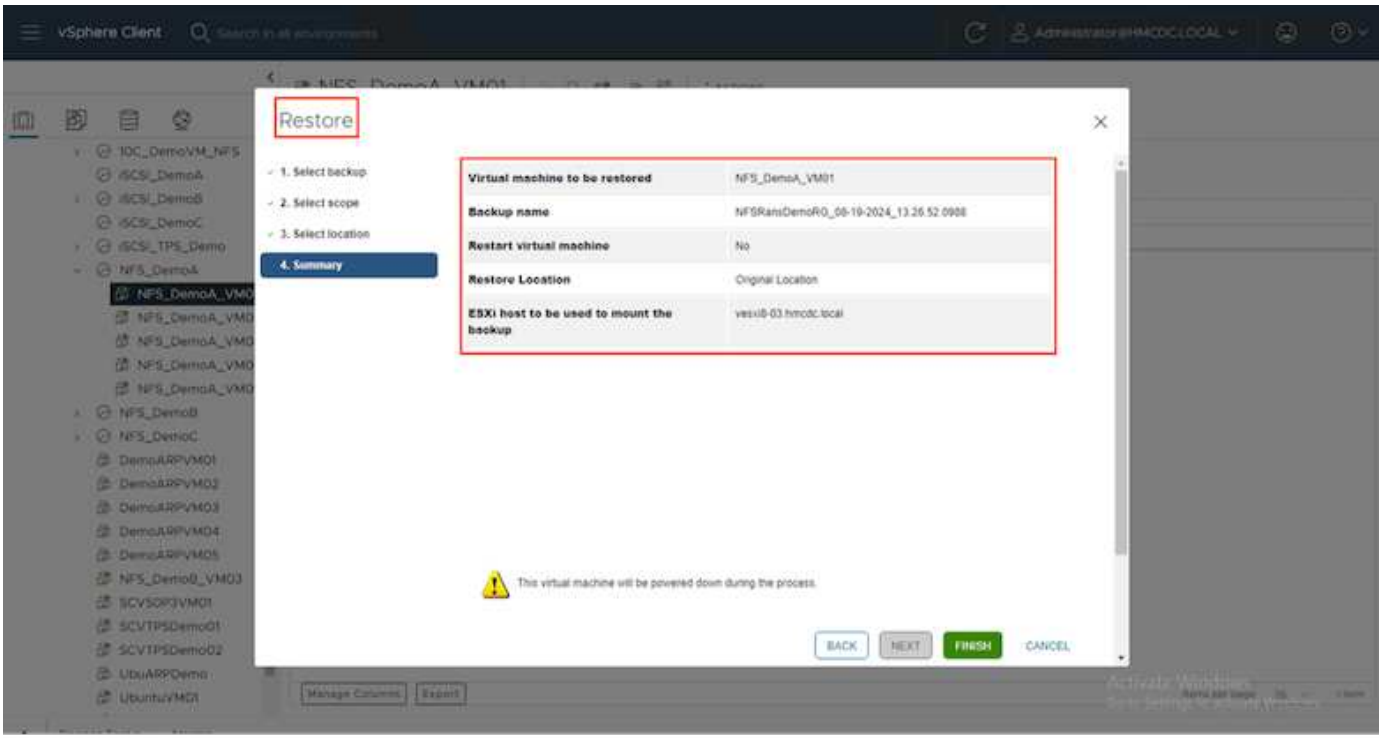
Se un attacco ransomware prende di mira la macchina virtuale (VM) e modifica i file al suo interno senza apportare modifiche all'esterno, Advanced Ransomware Protection (ARP) rileverà comunque la minaccia se l'entropia predefinita della VM è bassa, ad esempio per tipi di file come .txt, .docx o .mp4.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

Per informazioni dettagliate, fare riferimento alla sezione "ARP e macchine virtuali" in"Casi d'uso e considerazioni ARP" .

Passando dai file ai dati di backup, gli attacchi ransomware prendono sempre più di mira i backup e i punti di ripristino degli snapshot, cercando di eliminarli prima di iniziare a crittografare i file. Tuttavia, con ONTAP, questo può essere prevenuto creando snapshot a prova di manomissione sui sistemi primari o secondari con"Blocco della copia snapshot NetApp" .



Queste copie Snapshot non possono essere eliminate o modificate da aggressori ransomware o amministratori non autorizzati, quindi sono disponibili anche dopo un attacco. Se il datastore o specifiche macchine virtuali sono interessati, SnapCenter è in grado di recuperare i dati delle macchine virtuali in pochi secondi, riducendo al minimo i tempi di inattività dell'organizzazione.

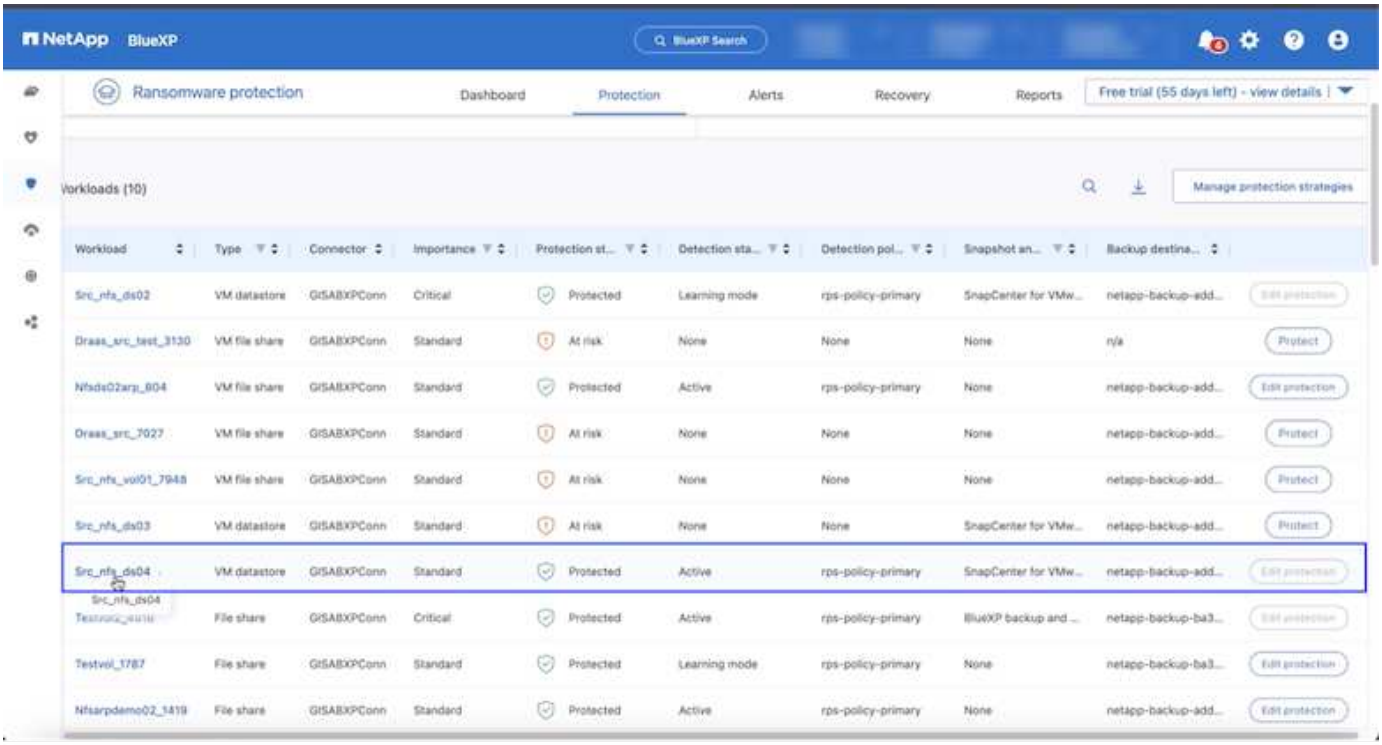


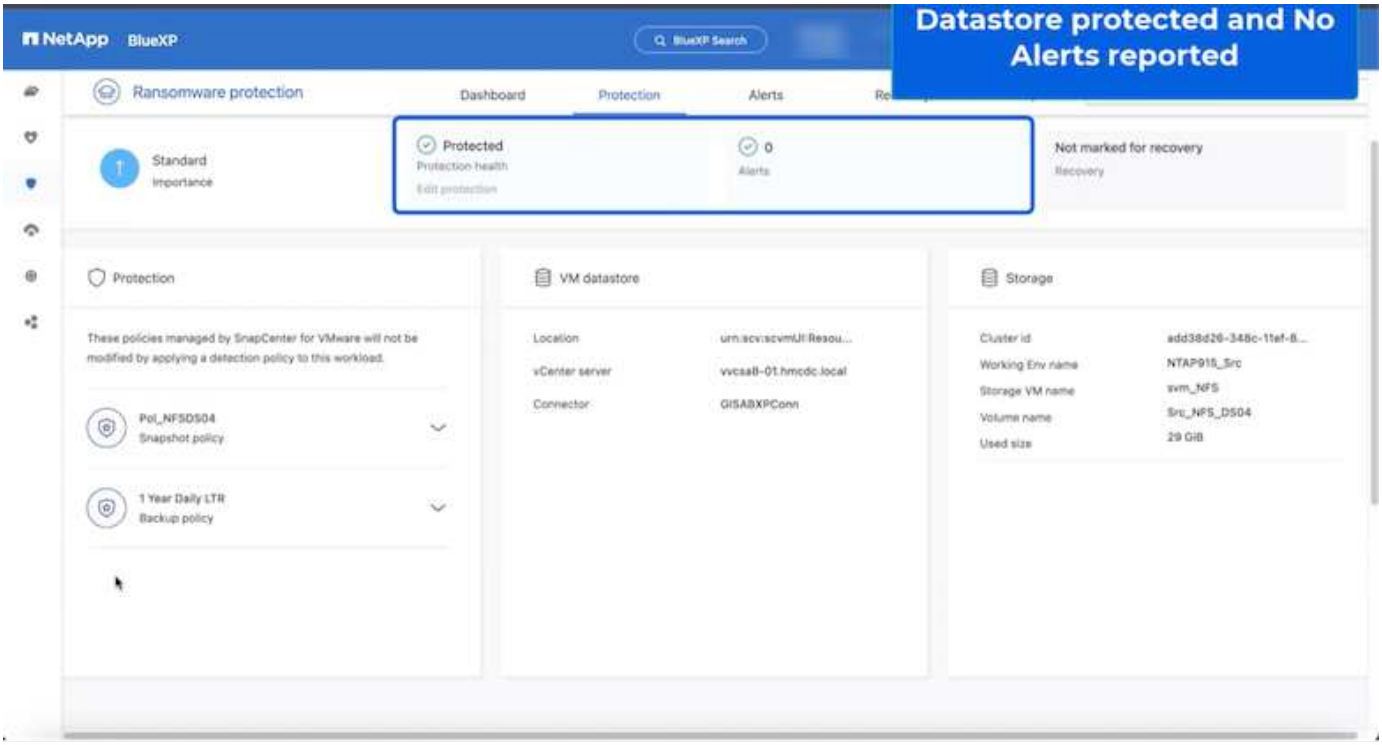
Quanto sopra dimostra come l'archiviazione ONTAP aggiunga un ulteriore livello alle tecniche esistenti, migliorando la protezione futura dell'ambiente.

Per ulteriori informazioni, consultare la guida per"Soluzioni NetApp per il ransomware" .

Ora, se tutto questo deve essere orchestrato e integrato con strumenti SIEM, è possibile utilizzare un servizio offtap come la BlueXP ransomware protection . Si tratta di un servizio progettato per proteggere i dati dal ransomware. Questo servizio offre protezione per carichi di lavoro basati su applicazioni quali Oracle, MySQL, datastore VM e condivisioni di file su storage NFS locali.

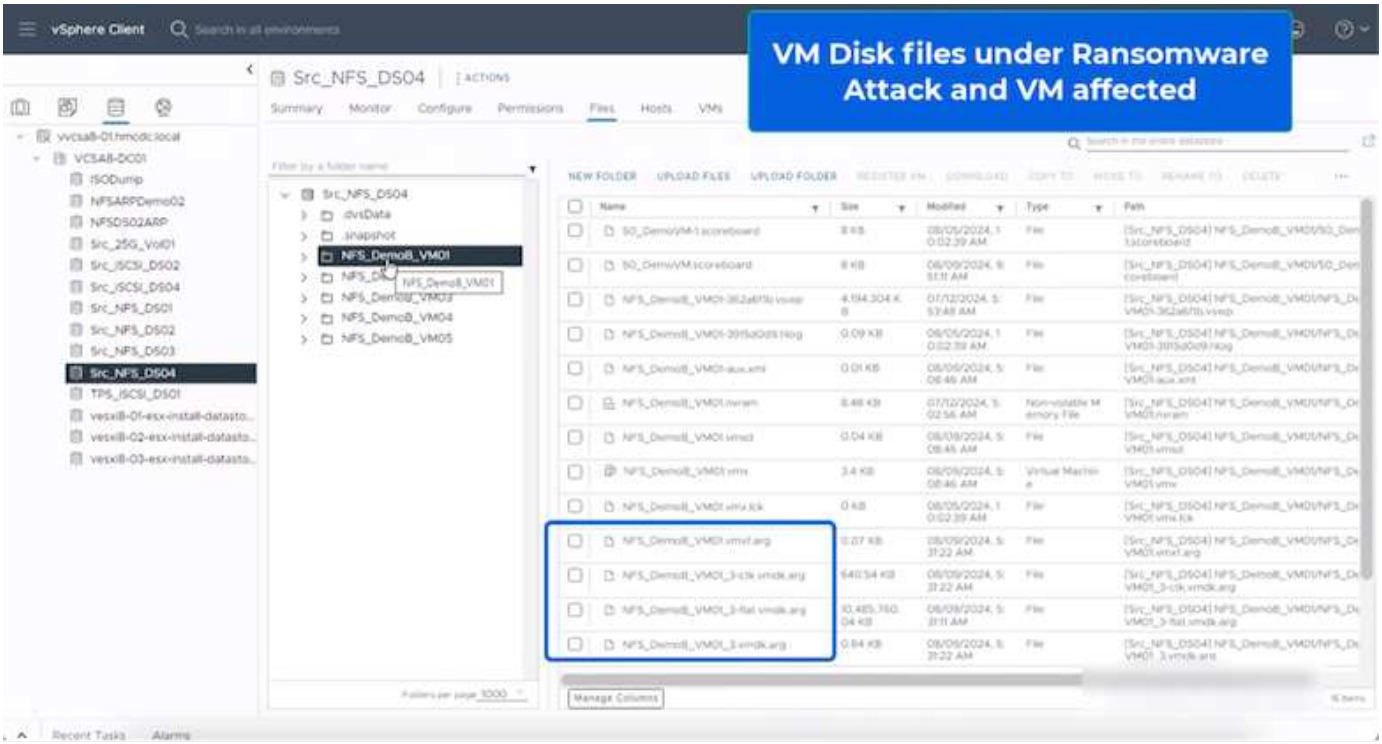
In questo esempio, il datastore NFS "Src_NFS_DS04" è protetto tramite la BlueXP ransomware protection.



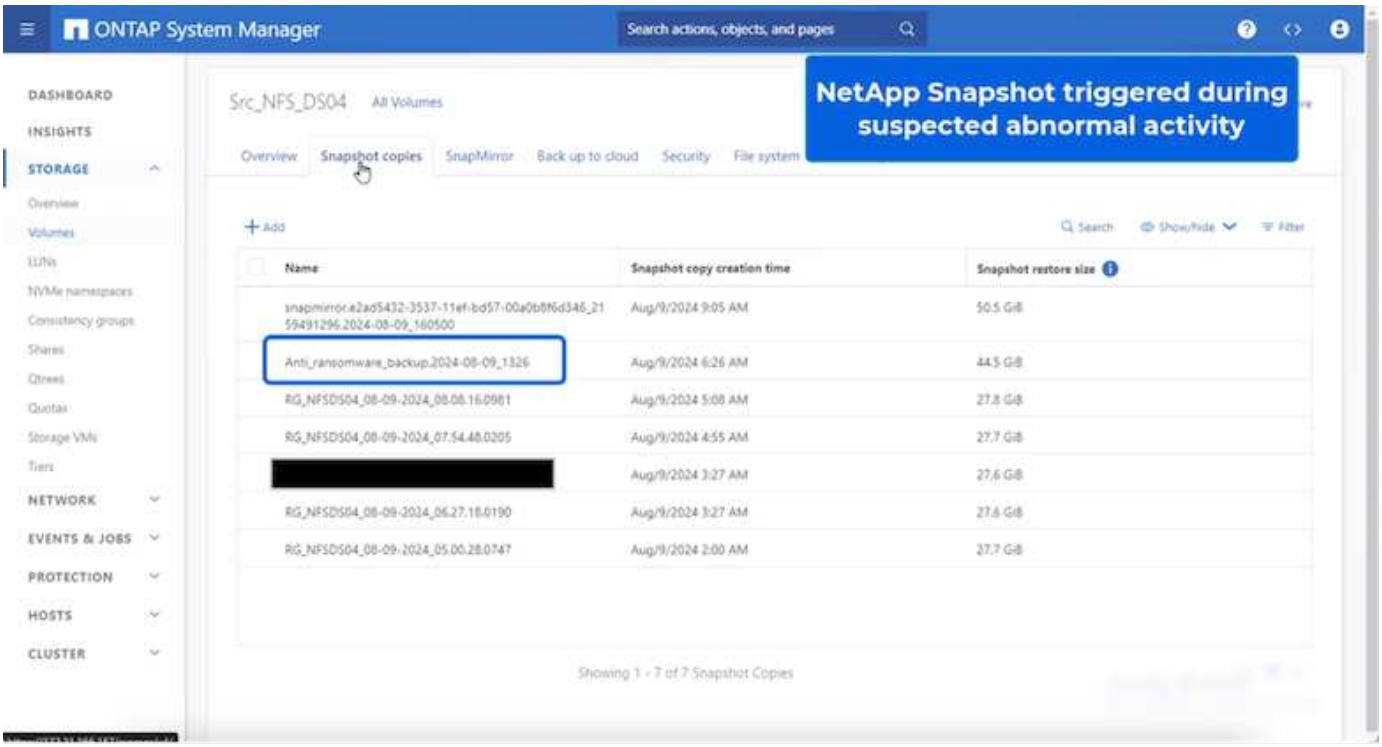


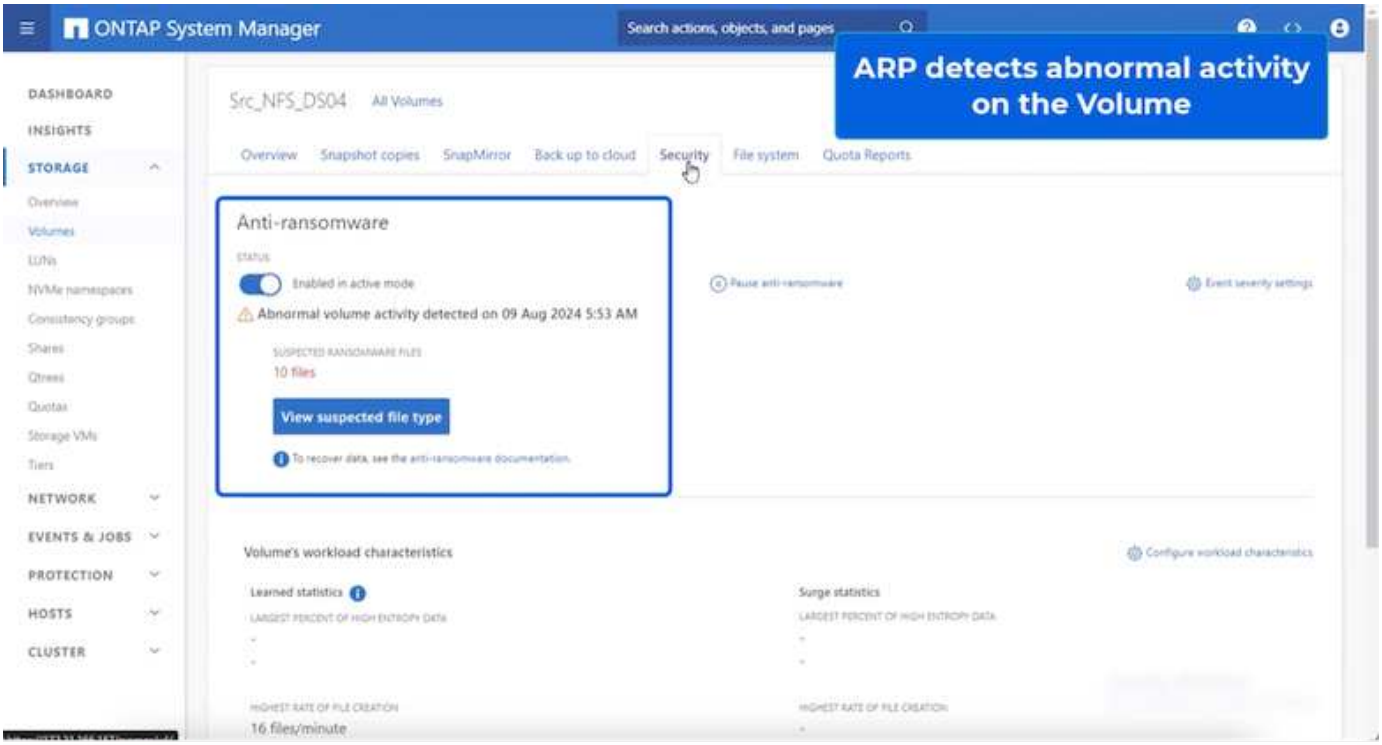
Per informazioni dettagliate su come configurare la BlueXP ransomware protection, fare riferimento a"Imposta la BlueXP ransomware protection" E"Configurare le impostazioni BlueXP ransomware protection" .

È il momento di analizzare la questione con un esempio. In questa procedura dettagliata, è interessato il datastore "Src_NFS_DS04".

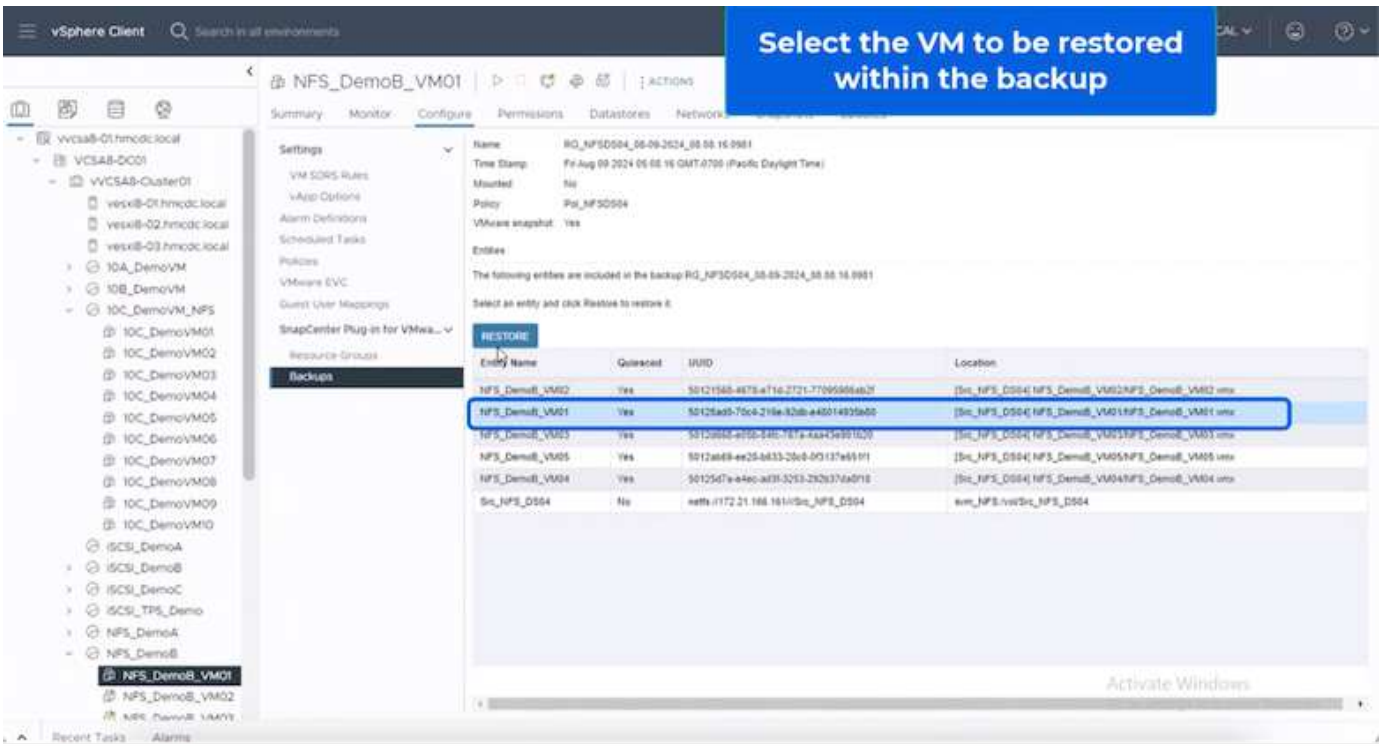


ARP ha immediatamente attivato uno snapshot sul volume al momento del rilevamento.





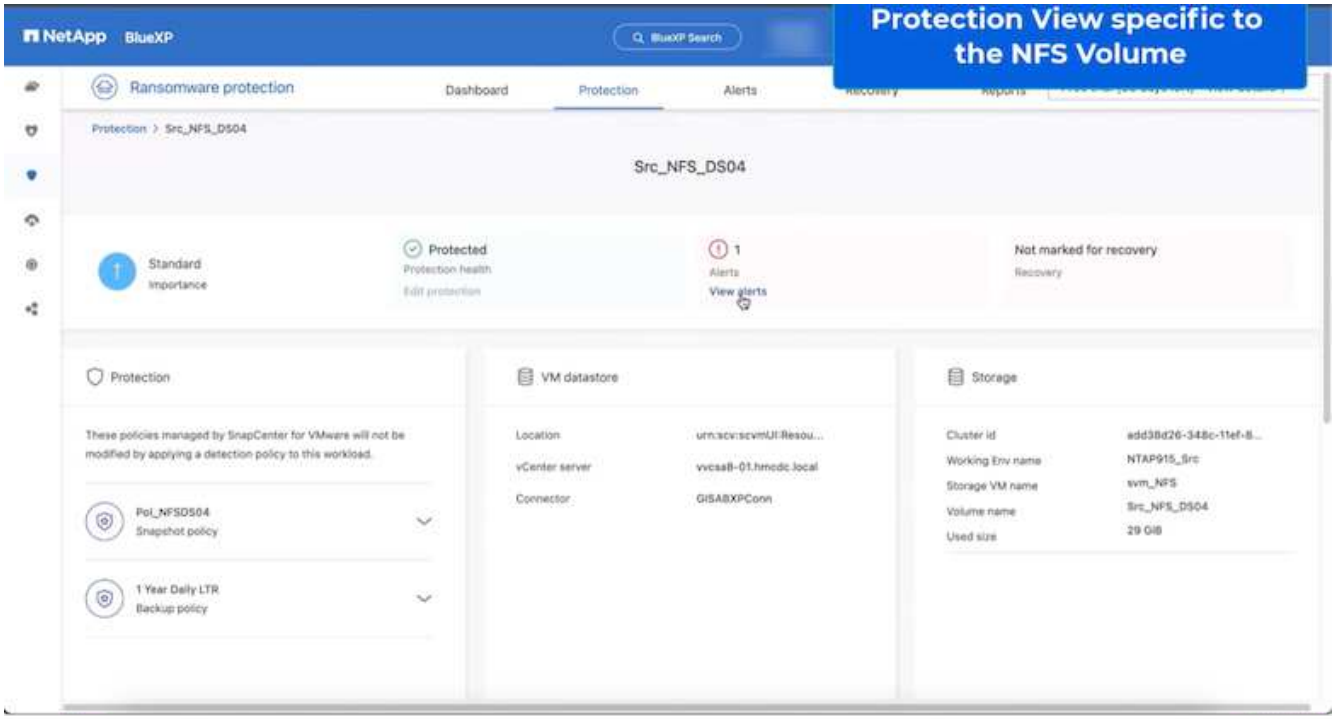
Una volta completata l'analisi forense, i ripristini possono essere eseguiti in modo rapido e senza problemi utilizzando la protezione ransomware SnapCenter o BlueXP ransomware protection. Con SnapCenter, accedi alle macchine virtuali interessate e seleziona lo snapshot appropriato da ripristinare.



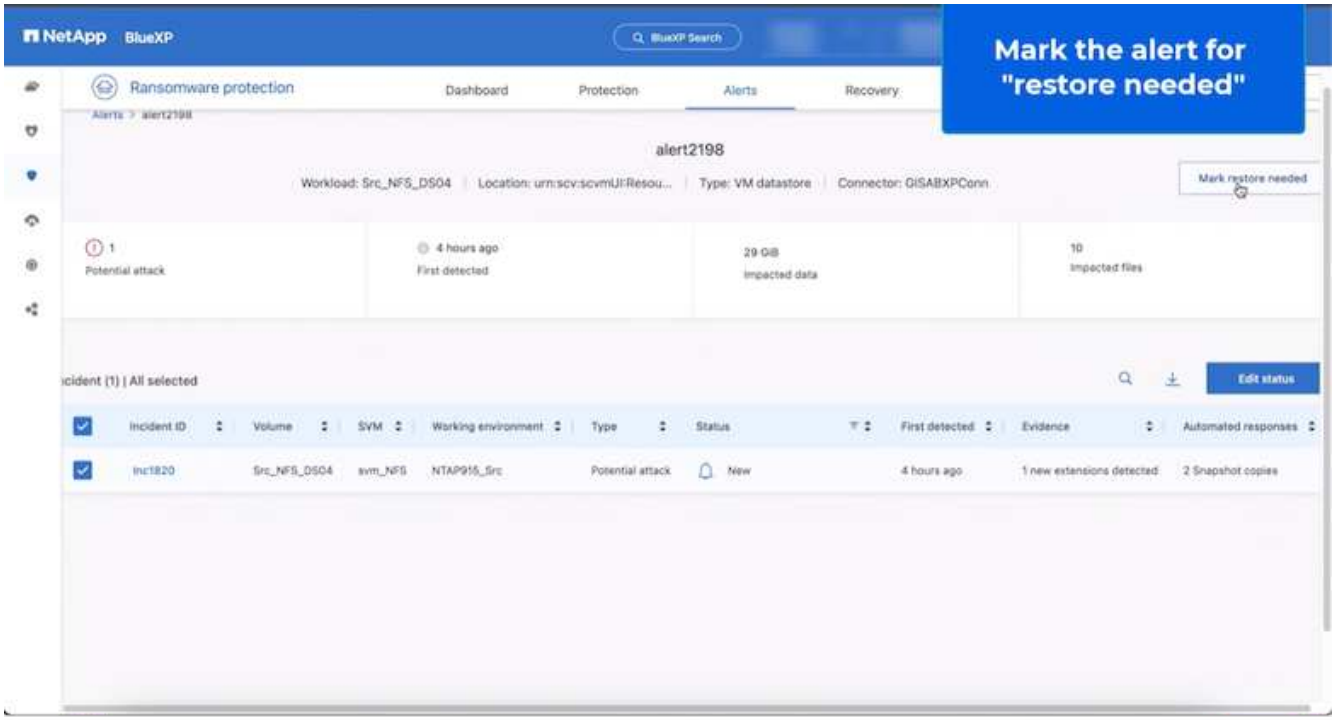
Questa sezione esamina il modo in cui la BlueXP ransomware protection orchestra il ripristino da un incidente ransomware in cui i file della macchina virtuale sono crittografati.

> Se la VM è gestita da SnapCenter, la BlueXP ransomware protection ripristina la VM allo stato precedente utilizzando il processo coerente con la VM.

1. Accedi BlueXP ransomware protection e un avviso apparirà sulla Dashboard BlueXP ransomware protection .
2. Fare clic sull'avviso per rivedere gli incidenti su quel volume specifico per l'avviso generato

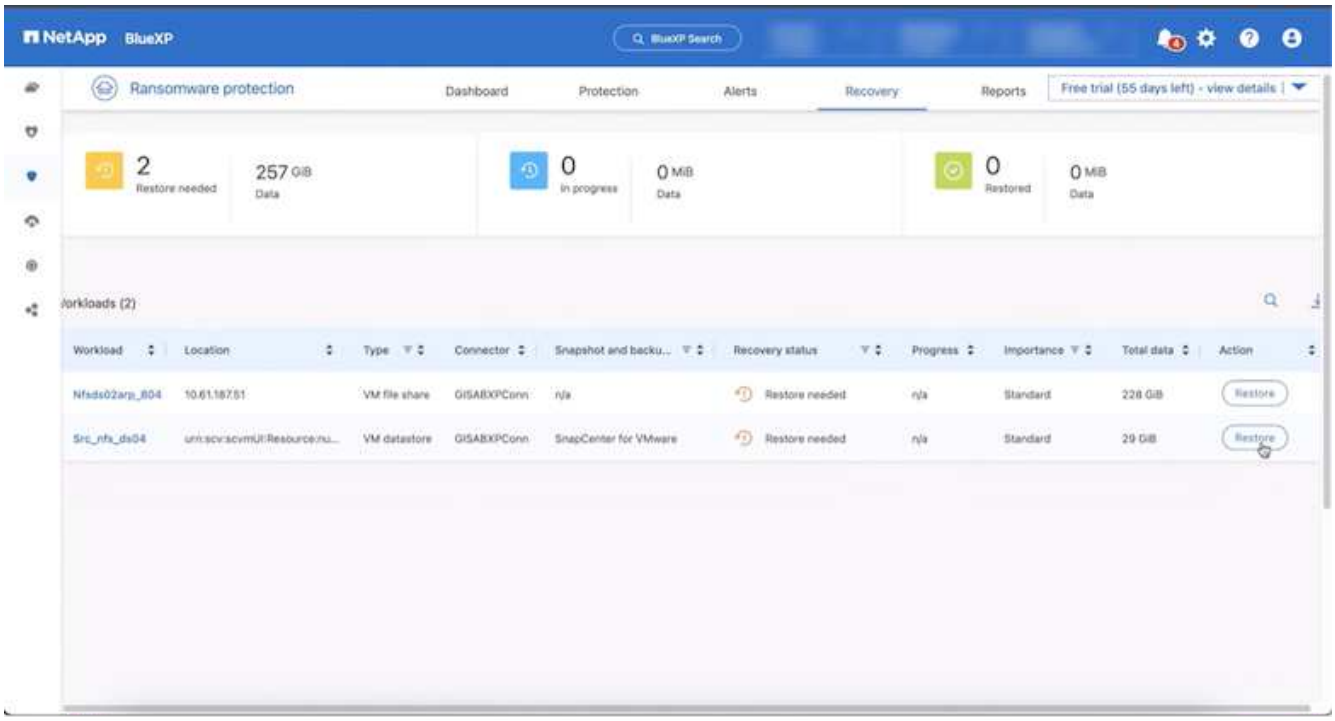


3. Contrassegna l'incidente ransomware come pronto per il ripristino (dopo che gli incidenti sono stati neutralizzati) selezionando "Contrassegna come ripristino necessario"

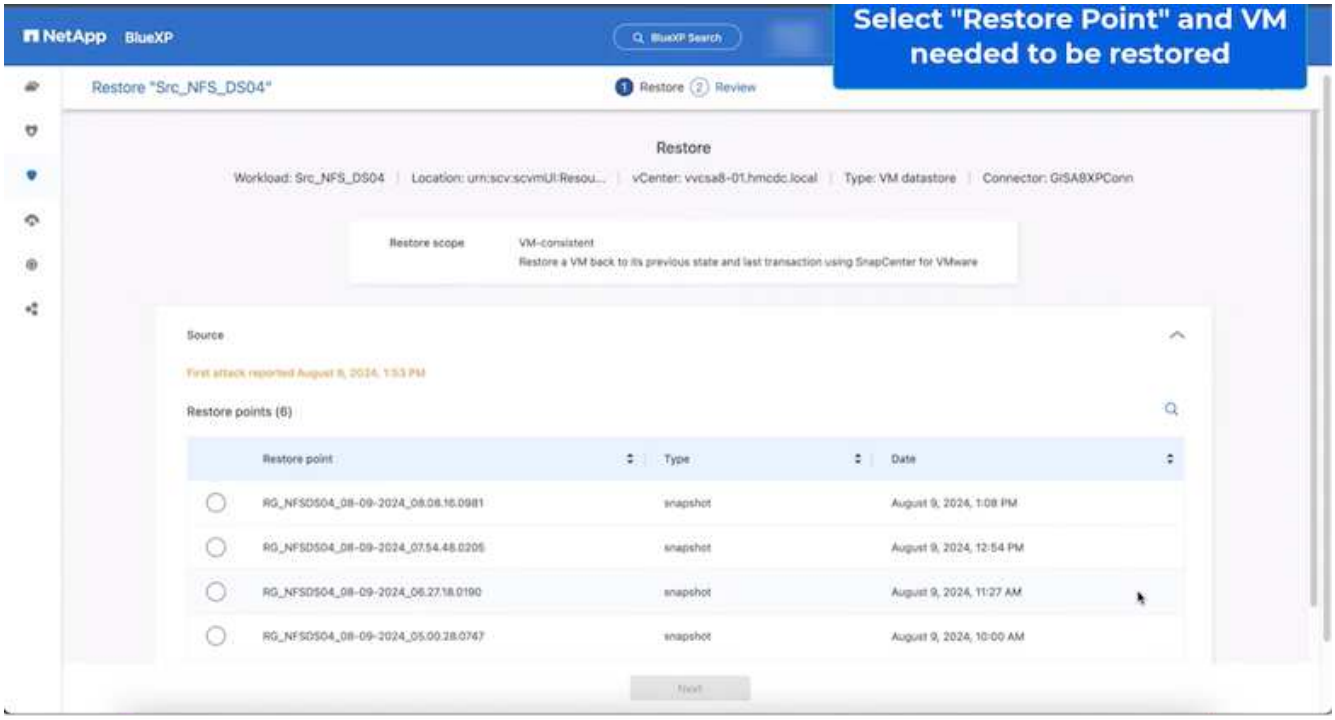


L'avviso può essere ignorato se l'incidente risulta essere un falso positivo.

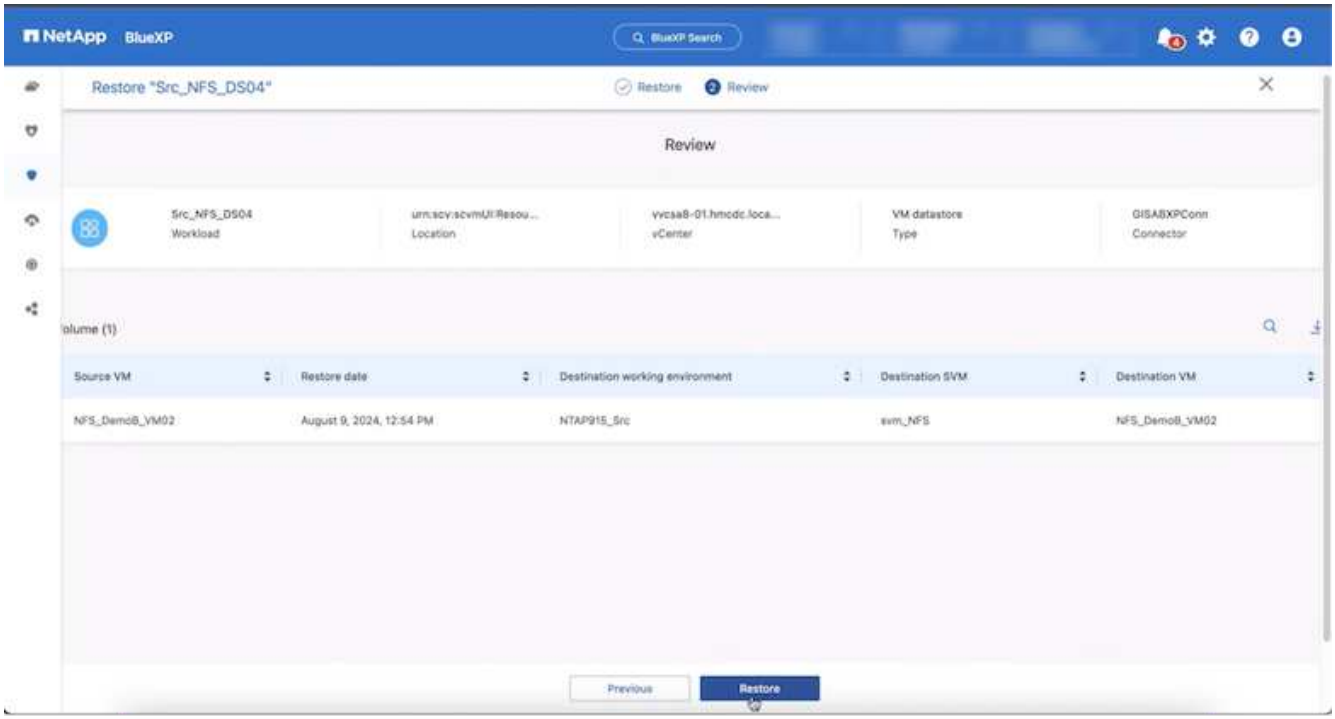
4. Accedere alla scheda Ripristino, rivedere le informazioni sul carico di lavoro nella pagina Ripristino, selezionare il volume del datastore che si trova nello stato "Ripristino necessario" e selezionare Ripristina.



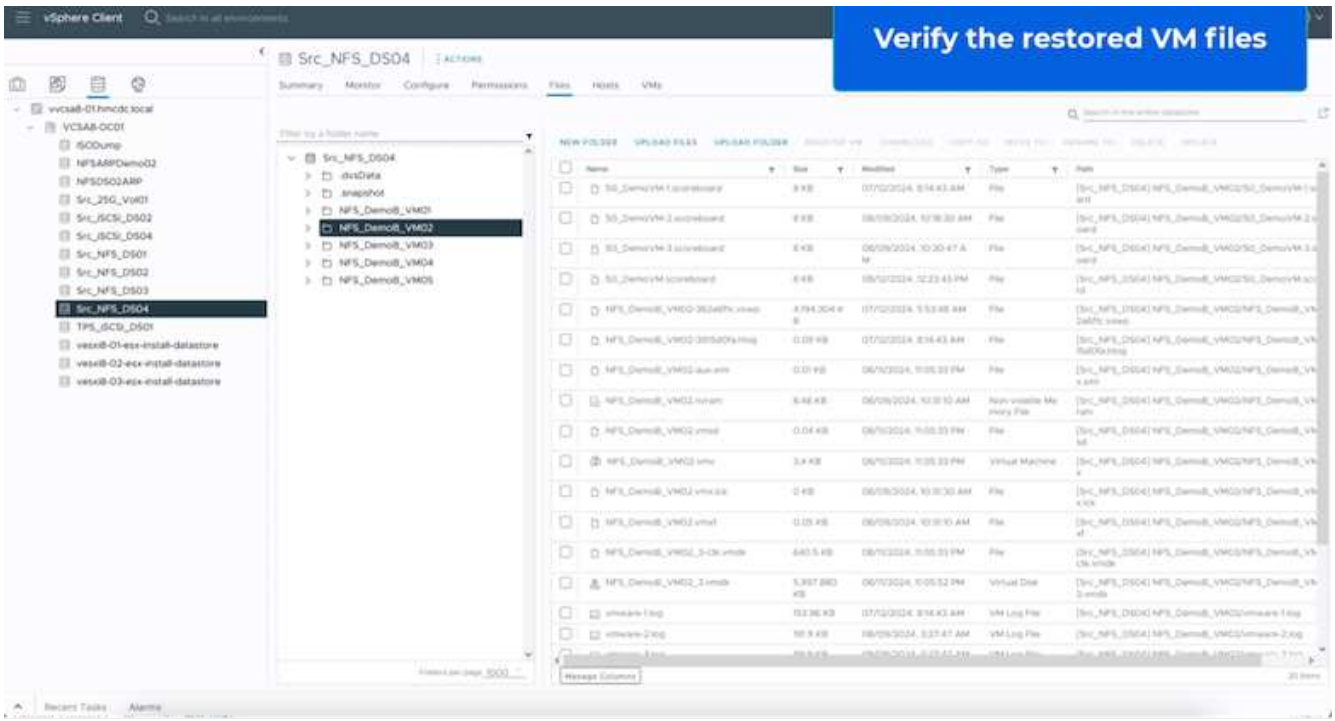
5. In questo caso, l'ambito di ripristino è "Per VM" (per SnapCenter per VM, l'ambito di ripristino è "Per VM")



6. Selezionare il punto di ripristino da utilizzare per ripristinare i dati, selezionare Destinazione e fare clic su Ripristina.



7. Dal menu in alto, seleziona Ripristino per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati. Una volta completato il ripristino, i file della VM vengono ripristinati come mostrato di seguito.



> Il ripristino può essere eseguito da SnapCenter per VMware o dal plugin SnapCenter , a seconda dell'applicazione.

La soluzione NetApp fornisce diversi strumenti efficaci per la visibilità, il rilevamento e la correzione, aiutandoti a individuare tempestivamente il ransomware, a prevenirne la diffusione e a ripristinare rapidamente, se necessario, per evitare costosi tempi di inattività. Le soluzioni di difesa tradizionali a più livelli continuano a

essere prevalenti, così come le soluzioni di terze parti e partner per la visibilità e il rilevamento. Una bonifica efficace resta una parte fondamentale della risposta a qualsiasi minaccia.

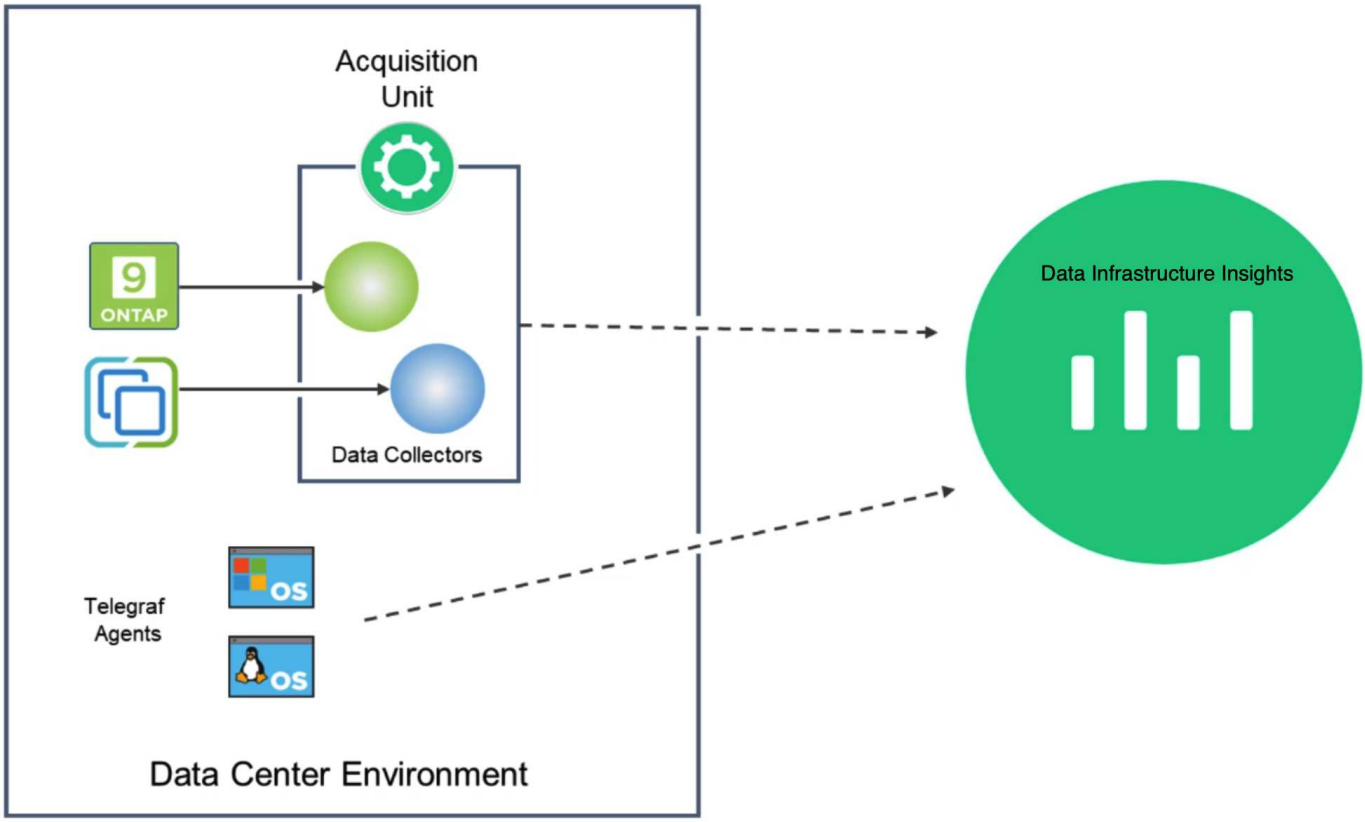
Monitora l'archiviazione on-premise con Data Infrastructure Insights

NetApp Data Infrastructure Insights (in precedenza Cloud Insights) è una piattaforma basata su cloud progettata per monitorare e analizzare le prestazioni, lo stato di salute e i costi delle infrastrutture IT, sia on-premise che nel cloud. Scopri come distribuire strumenti di raccolta dati, analizzare le metriche delle prestazioni e utilizzare dashboard per identificare problemi e ottimizzare le risorse.

Monitoraggio dell'archiviazione locale con Data Infrastructure Insights

Data Infrastructure Insights funziona tramite il software Acquisition Unit, configurato con collettori di dati per asset quali i sistemi di storage VMware vSphere e NetApp ONTAP . Questi collettori raccolgono i dati e li trasmettono a Data Infrastructure Insights. La piattaforma utilizza quindi una serie di dashboard, widget e query metriche per organizzare i dati in analisi approfondite che gli utenti possono interpretare.

Diagramma dell'architettura Data Infrastructure Insights :



Panoramica sulla distribuzione della soluzione

Questa soluzione fornisce un'introduzione al monitoraggio dei sistemi di storage VMware vSphere e ONTAP on-premise mediante Data Infrastructure Insights.

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

1. Configurare Data Collector per un cluster vSphere.
2. Configurare Data Collector per un sistema di archiviazione ONTAP .
3. Utilizzare le regole di annotazione per contrassegnare le risorse.
4. Esplora e correla le risorse.
5. Utilizzare una dashboard Top VM Latency per isolare i vicini rumorosi.
6. Identificare le opportunità per dimensionare correttamente le VM.
7. Utilizzare le query per isolare e ordinare le metriche.

Prerequisiti

Questa soluzione utilizza i seguenti componenti:

1. NetApp SAN All-Flash NetApp A400 con ONTAP 9.13.
2. Cluster VMware vSphere 8.0.
3. Account NetApp BlueXP .
4. Software NetApp Data Infrastructure Insights Acquisition Unit installato su una VM locale con connettività di rete alle risorse per la raccolta dati.

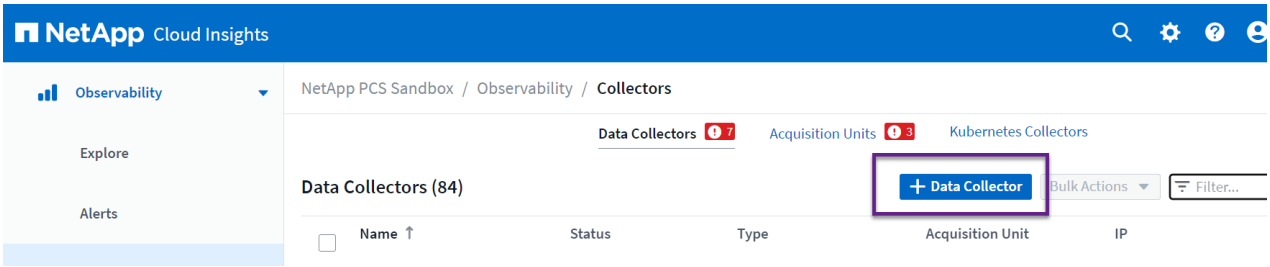
Distribuzione della soluzione

Configurare i raccoglitori di dati

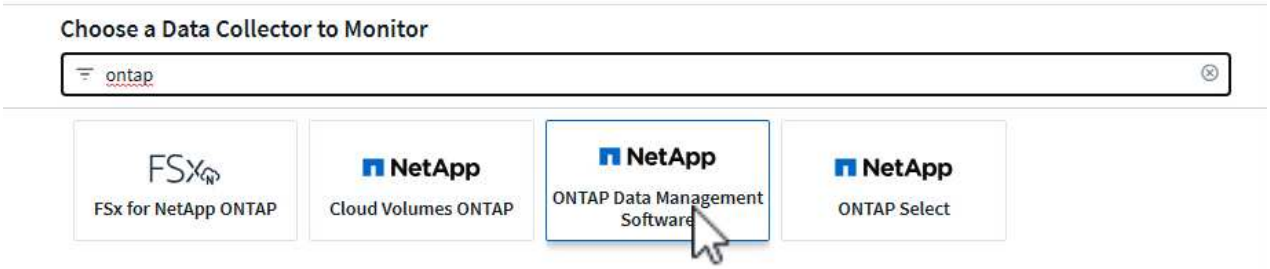
Per configurare i Data Collector per i sistemi di archiviazione VMware vSphere e ONTAP , completare i seguenti passaggi:

Aggiungere un Data Collector per un sistema di archiviazione ONTAP

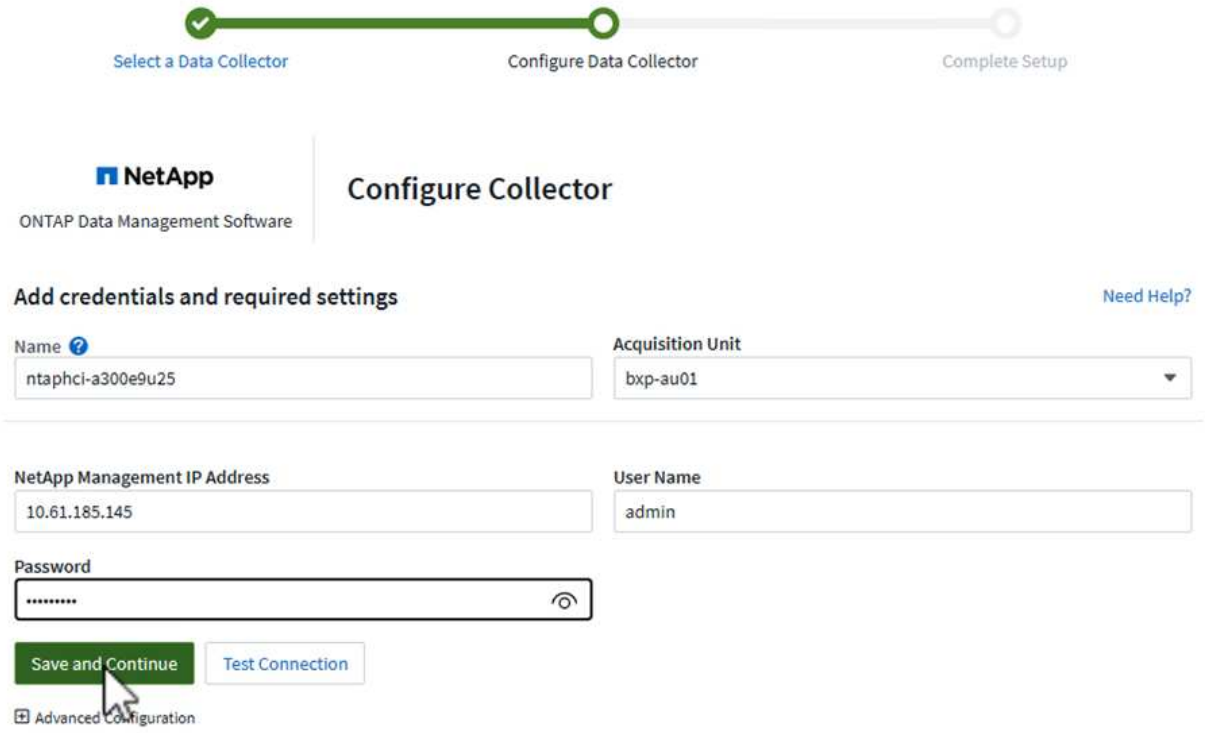
1. Dopo aver effettuato l'accesso a Data Infrastructure Insights, vai su **Observability > Collectors > Data Collectors** e premi il pulsante per installare un nuovo Data Collector.



2. Da qui cerca * ONTAP* e clicca su *Software di gestione dati ONTAP *.

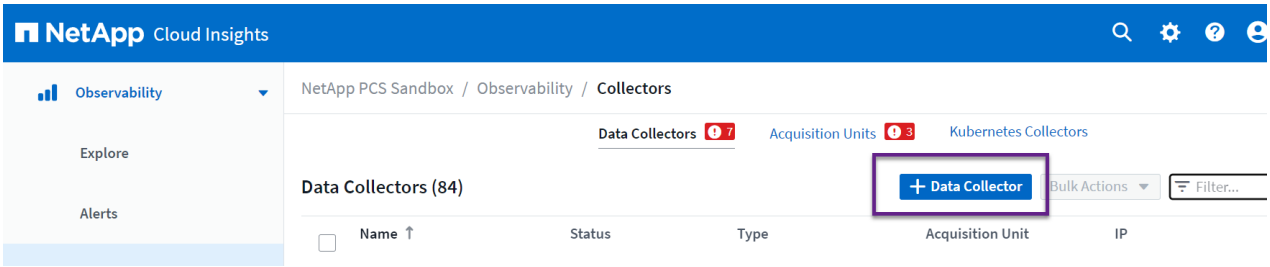


3. Nella pagina **Configura Collector**, inserisci un nome per il collector, specifica l'**Unità di acquisizione** corretta e fornisci le credenziali per il sistema di archiviazione ONTAP . Fare clic su **Salva e continua** e poi su **Completa configurazione** in fondo alla pagina per completare la configurazione.

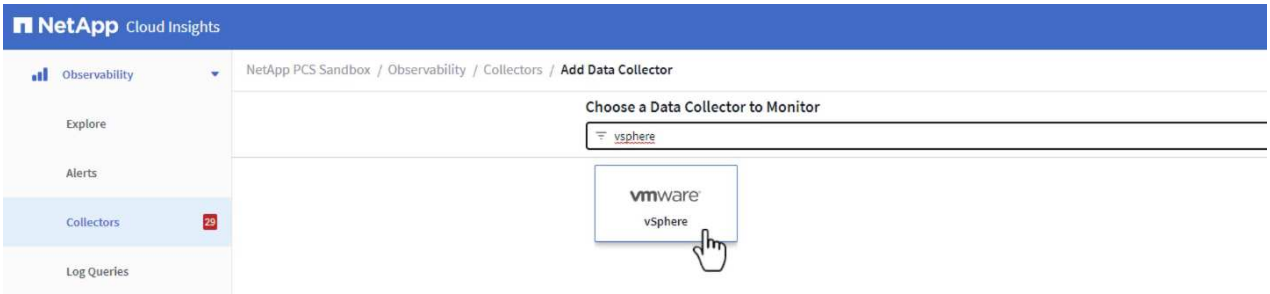


Aggiungere un Data Collector per un cluster VMware vSphere

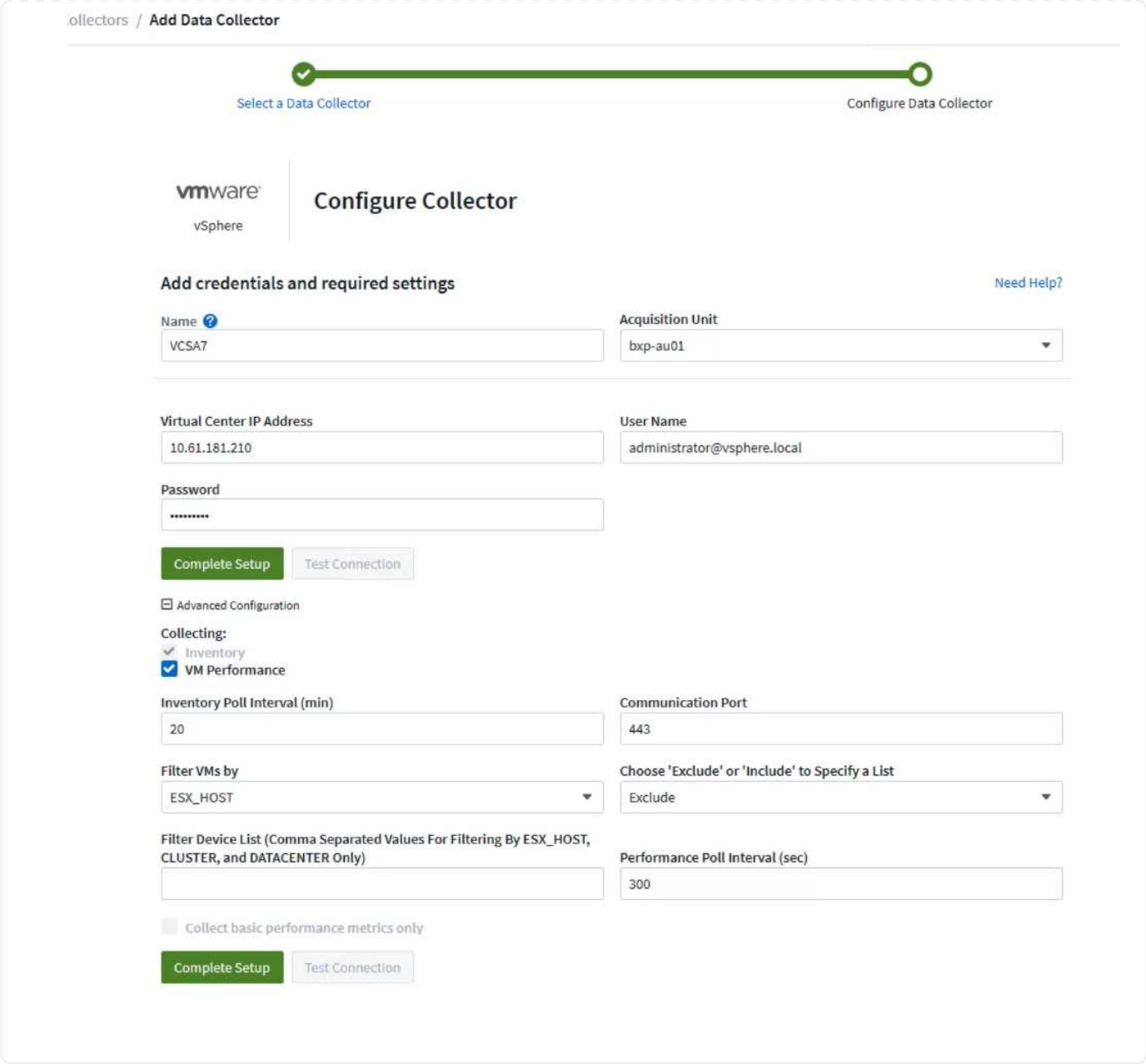
1. Ancora una volta, vai su **Observability > Collectors > Data Collectors** e premi il pulsante per installare un nuovo Data Collector.



2. Da qui cerca **vSphere** e clicca su **VMware vSphere**.



3. Nella pagina **Configura Collector**, inserisci un nome per il collector, specifica l'**Unità di acquisizione** corretta e fornisci le credenziali per il server vCenter. Fare clic su **Salva e continua** e poi su **Completa configurazione** in fondo alla pagina per completare la configurazione.



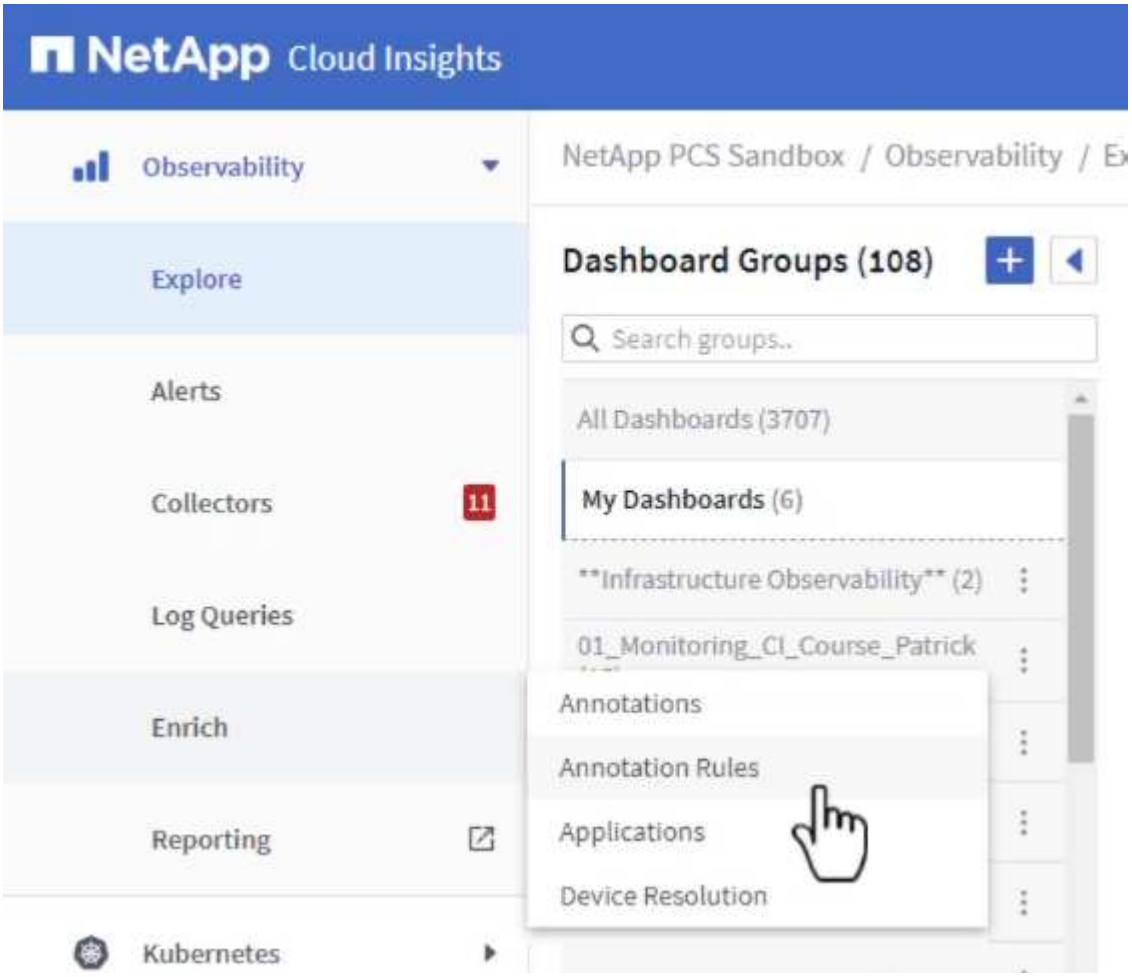
Aggiungi annotazioni alle risorse

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

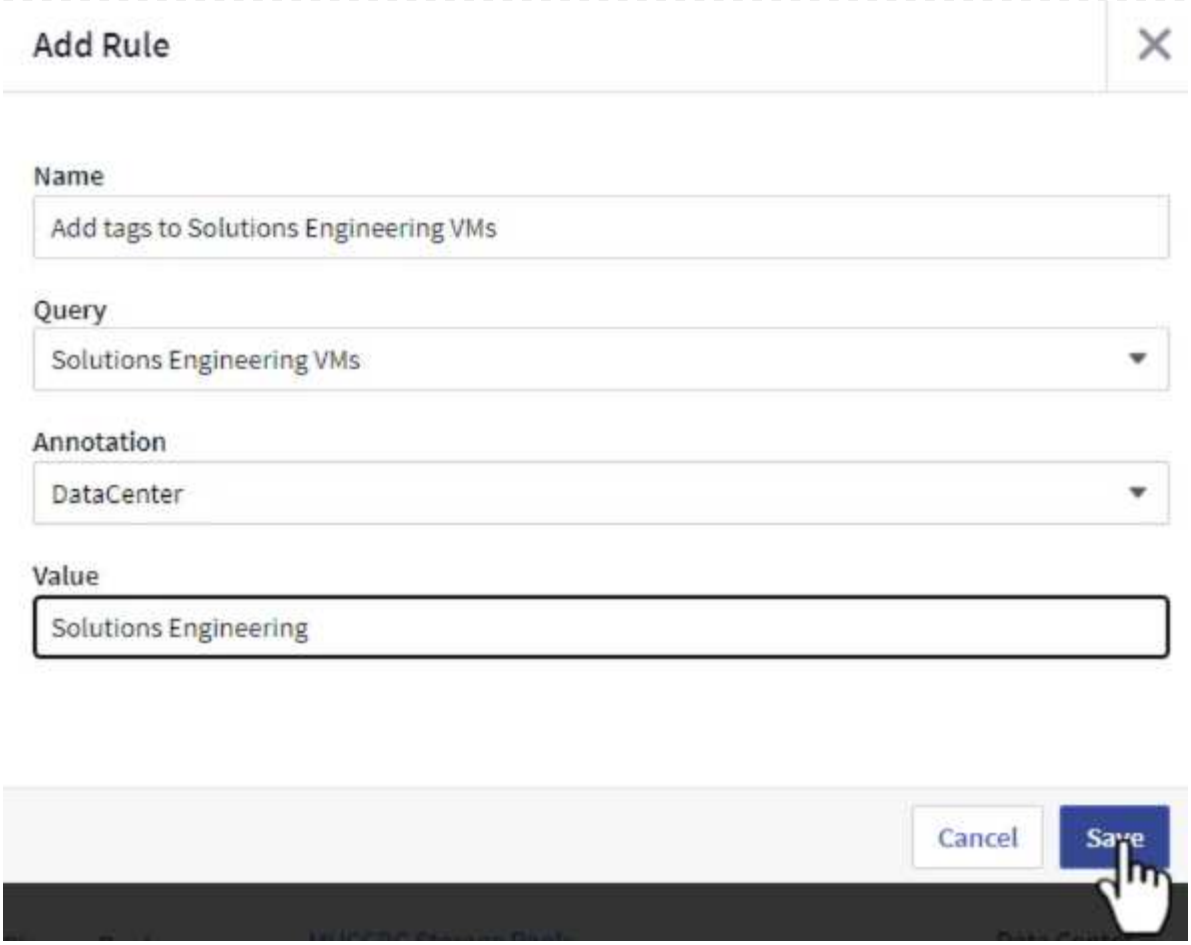
In questa sezione verranno aggiunte annotazioni alle risorse della macchina virtuale per il filtraggio in base al **Data Center**.

Utilizzare le regole di annotazione per taggare le risorse

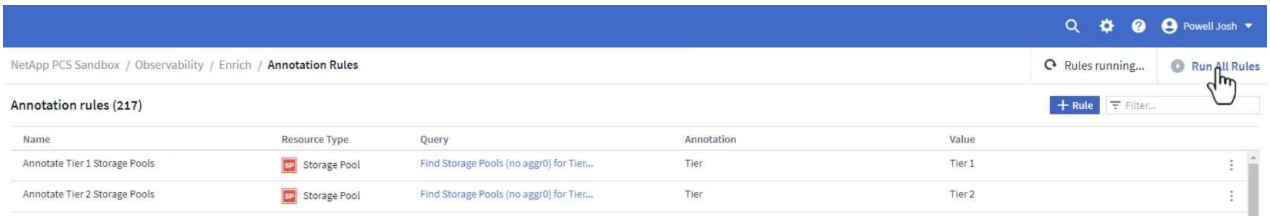
1. Nel menu a sinistra, vai su **Osservabilità > Arricchisci > Regole di annotazione** e clicca sul pulsante **+ Regola** in alto a destra per aggiungere una nuova regola.



2. Nella finestra di dialogo **Aggiungi regola**, inserisci un nome per la regola, individua una query a cui verrà applicata la regola, il campo di annotazione interessato e il valore da popolare.



3. Infine, nell'angolo in alto a destra della pagina **Regole di annotazione**, fare clic su **Esegui tutte le regole** per eseguire la regola e applicare l'annotazione alle risorse.



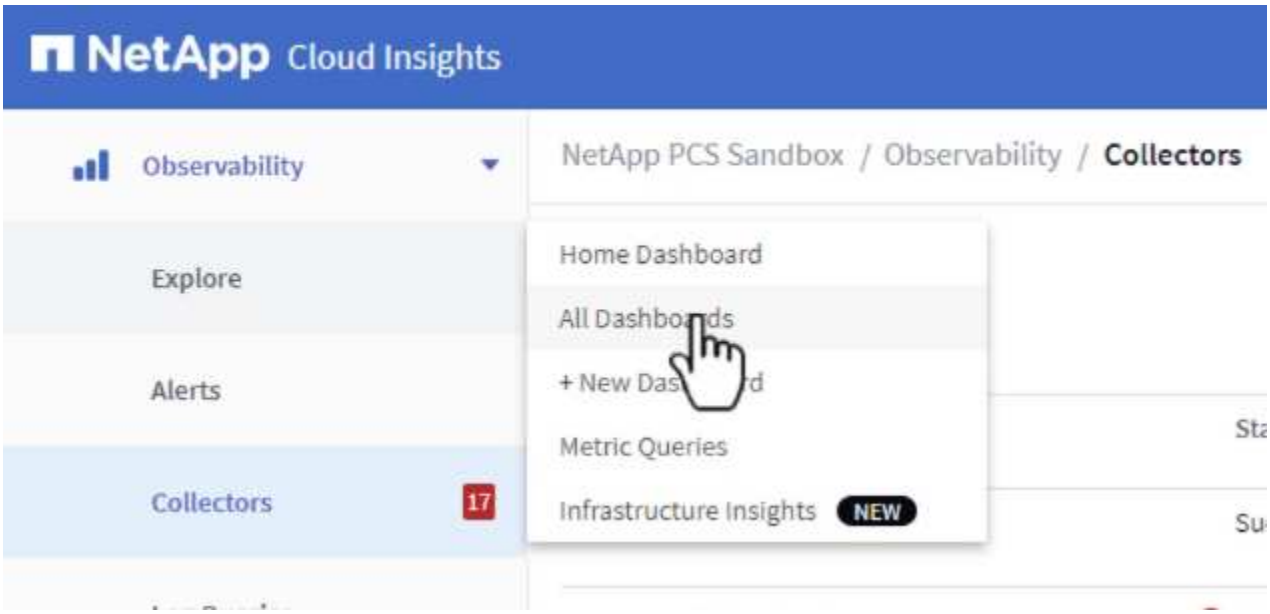
Esplora e correla le risorse

Cloud Insights trae conclusioni logiche sulle risorse in esecuzione contemporaneamente sui sistemi di storage e sui cluster vSphere.

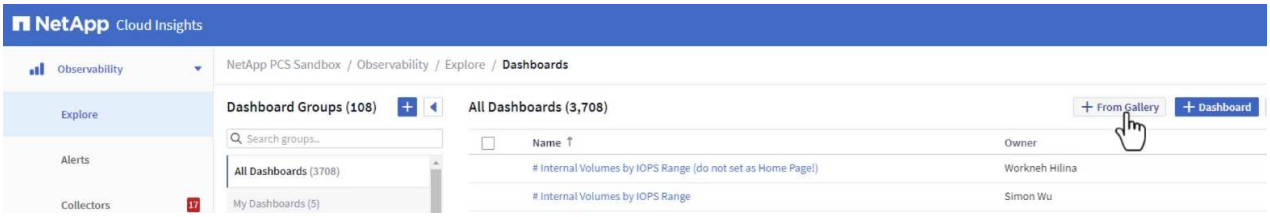
Questa sezione illustra come utilizzare i dashboard per correlare le risorse.

Correlazione delle risorse da una dashboard delle prestazioni di archiviazione

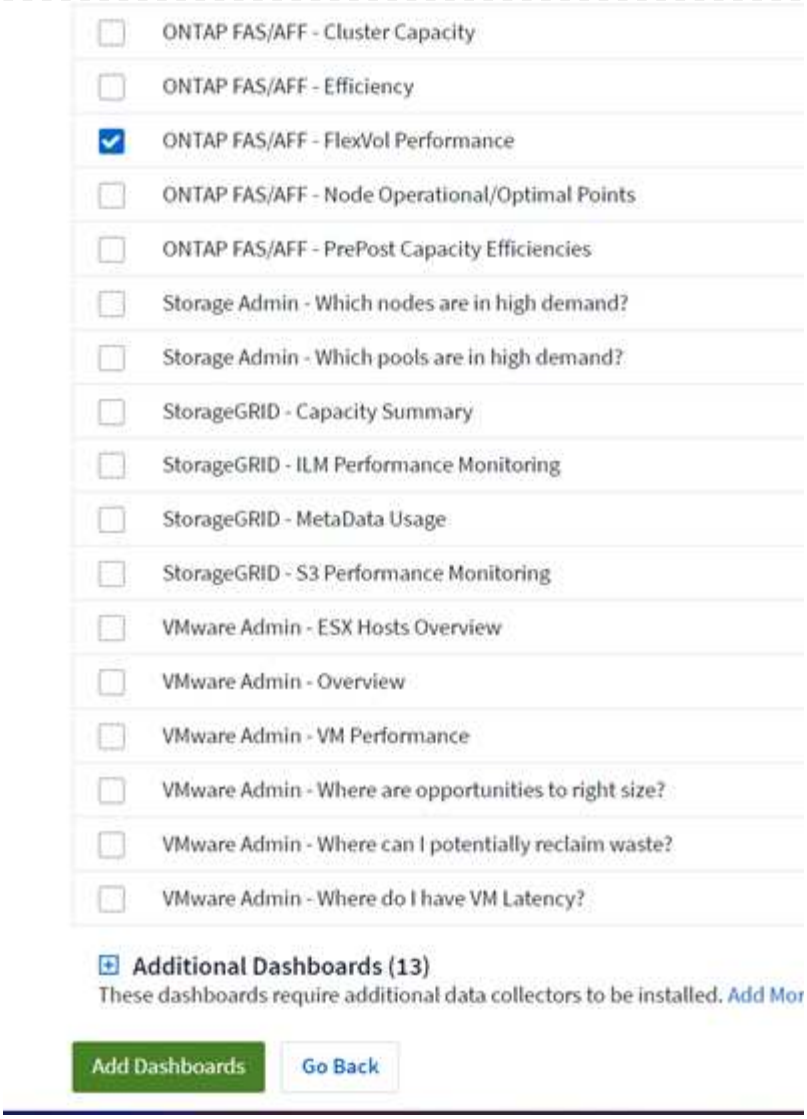
1. Nel menu a sinistra, vai su **Osservabilità > Esplora > Tutte le dashboard**.



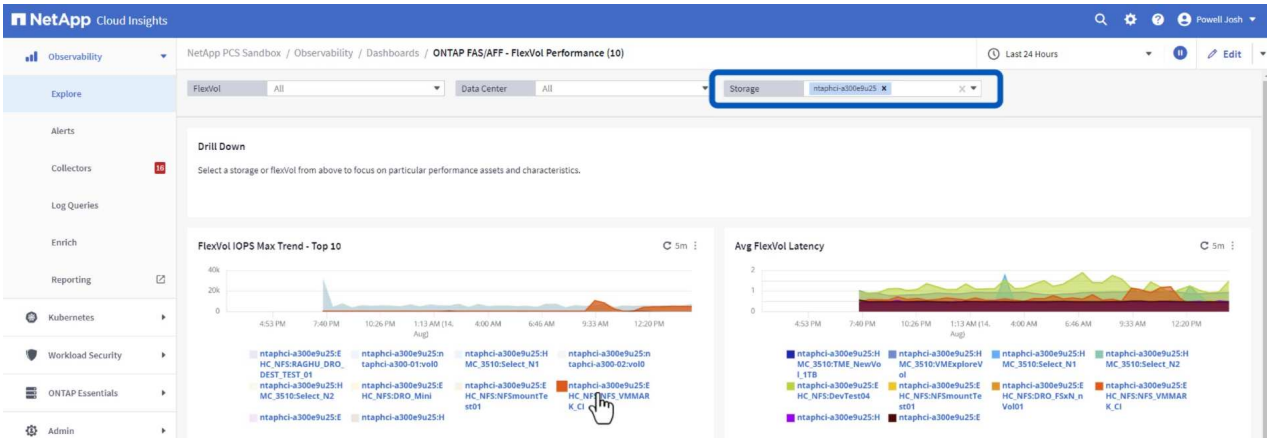
2. Fare clic sul pulsante **+ Dalla galleria** per visualizzare un elenco di dashboard già pronte che possono essere importate.



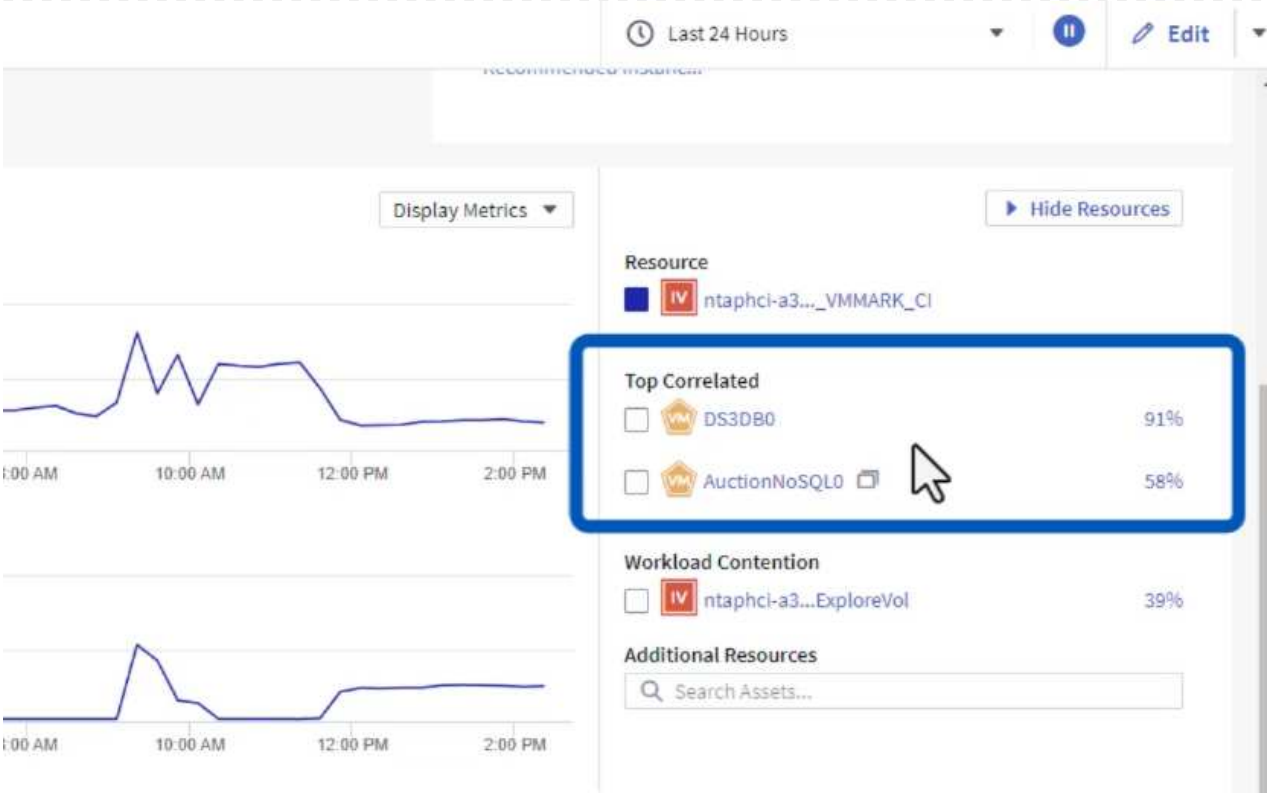
3. Scegli dall'elenco una dashboard per le prestazioni FlexVol e clicca sul pulsante **Aggiungi dashboard** in fondo alla pagina.



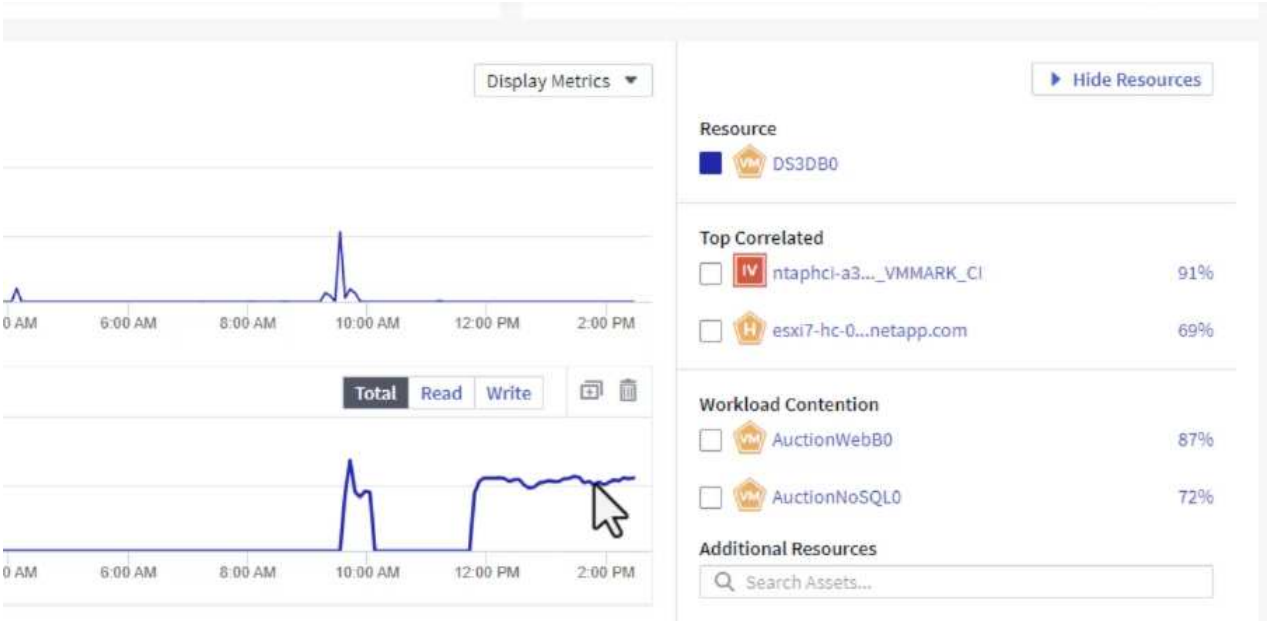
4. Una volta importato, apri la dashboard. Da qui puoi vedere vari widget con dati dettagliati sulle prestazioni. Aggiungi un filtro per visualizzare un singolo sistema di archiviazione e seleziona un volume di archiviazione per analizzarne i dettagli.



5. Da questa vista è possibile visualizzare varie metriche relative a questo volume di archiviazione e alle macchine virtuali più utilizzate e correlate in esecuzione sul volume.



6. Facendo clic sulla VM con il più alto utilizzo, si accede alle metriche per quella VM per visualizzare eventuali problemi.



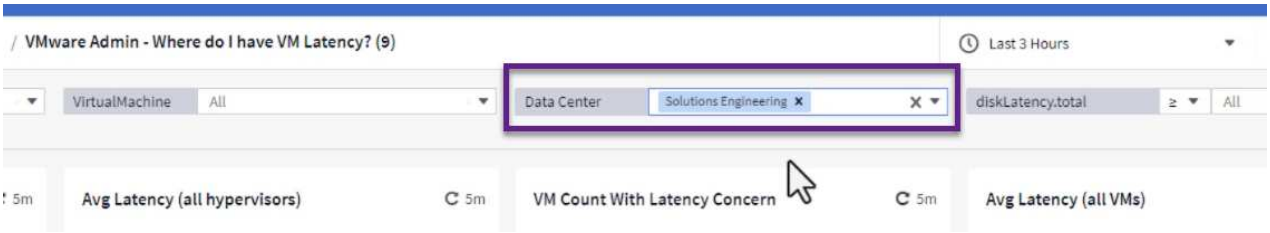
Utilizza Cloud Insights per identificare i vicini rumorosi

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

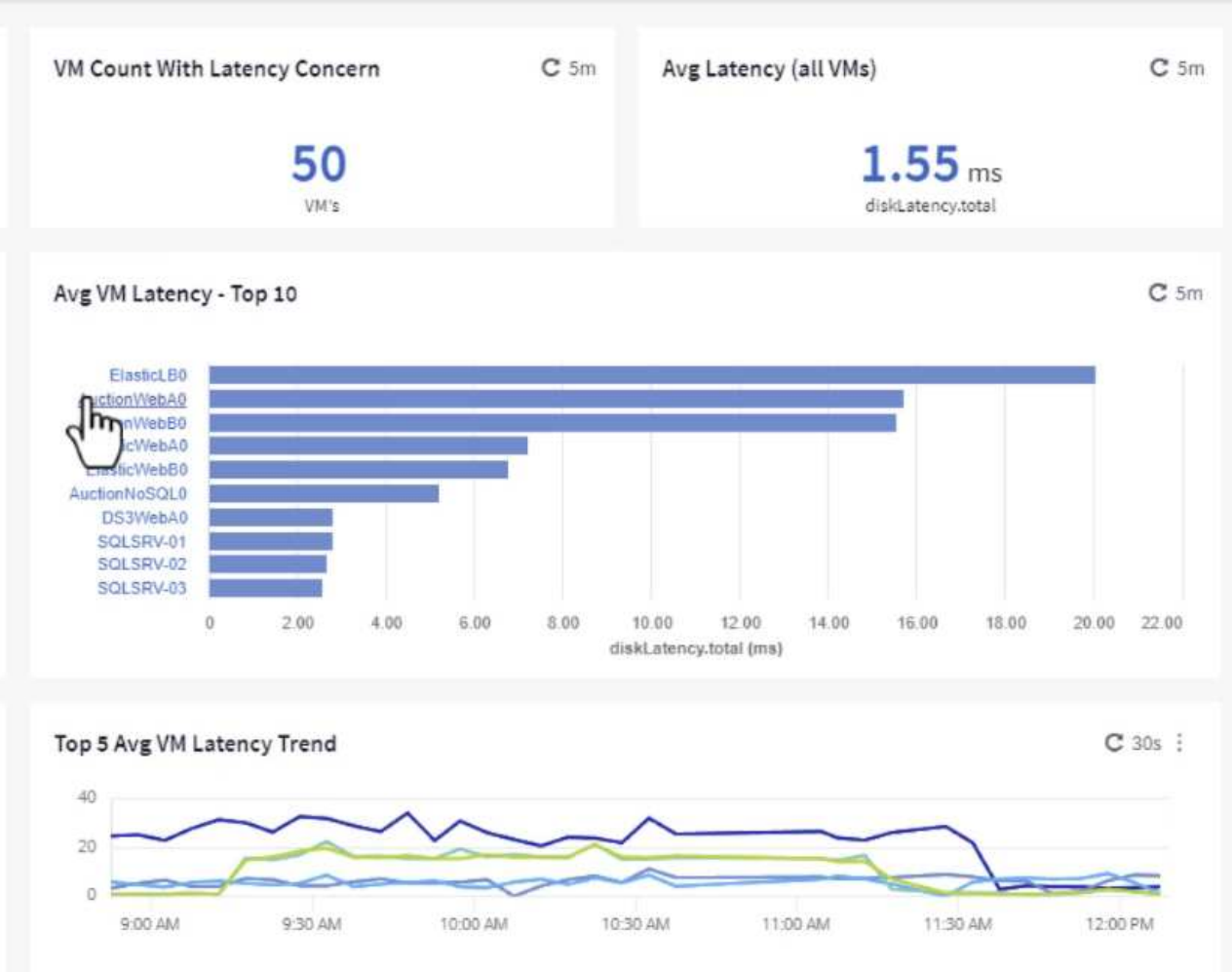
Utilizzare una dashboard Top VM Latency per isolare i vicini rumorosi

1. In questo esempio accedi a una dashboard disponibile nella **Galleria** denominata **VMware Admin - Dove trovo la latenza della VM?**

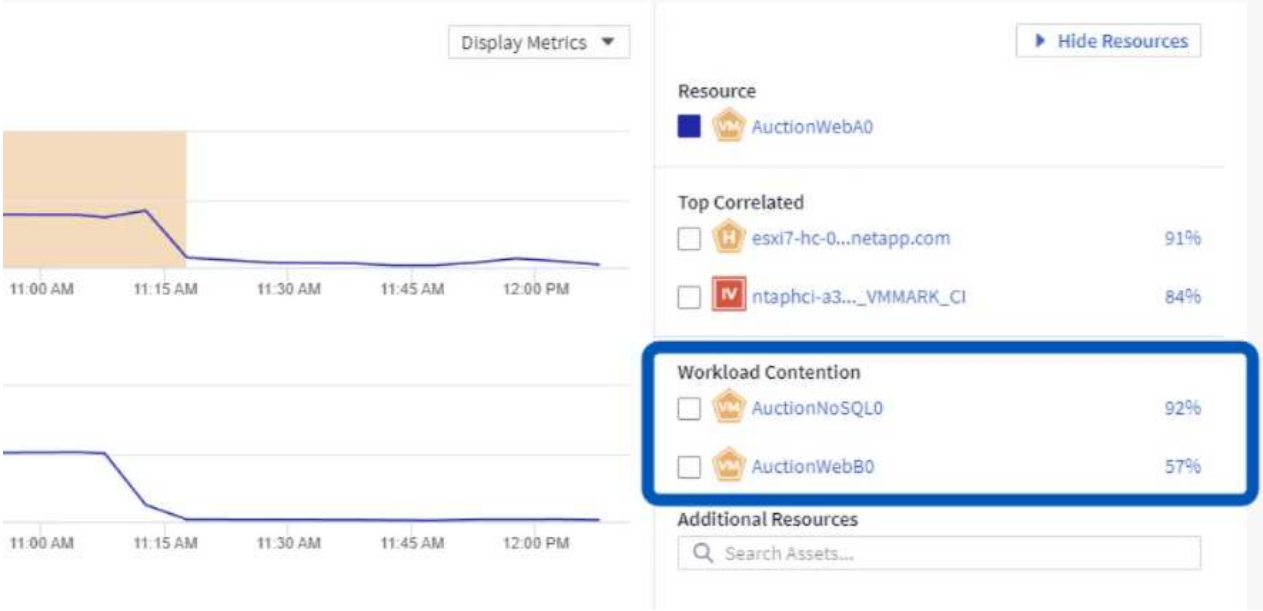
2. Successivamente, filtra in base all'annotazione **Data Center** creata in un passaggio precedente per visualizzare un sottoinsieme di risorse.



3. Questa dashboard mostra un elenco delle 10 VM più performanti in base alla latenza media. Da qui fare clic sulla VM interessata per approfondirne i dettagli.



4. Le VM che potrebbero causare conflitti di carico di lavoro sono elencate e disponibili. Analizza attentamente le metriche delle prestazioni di queste VM per individuare eventuali problemi.

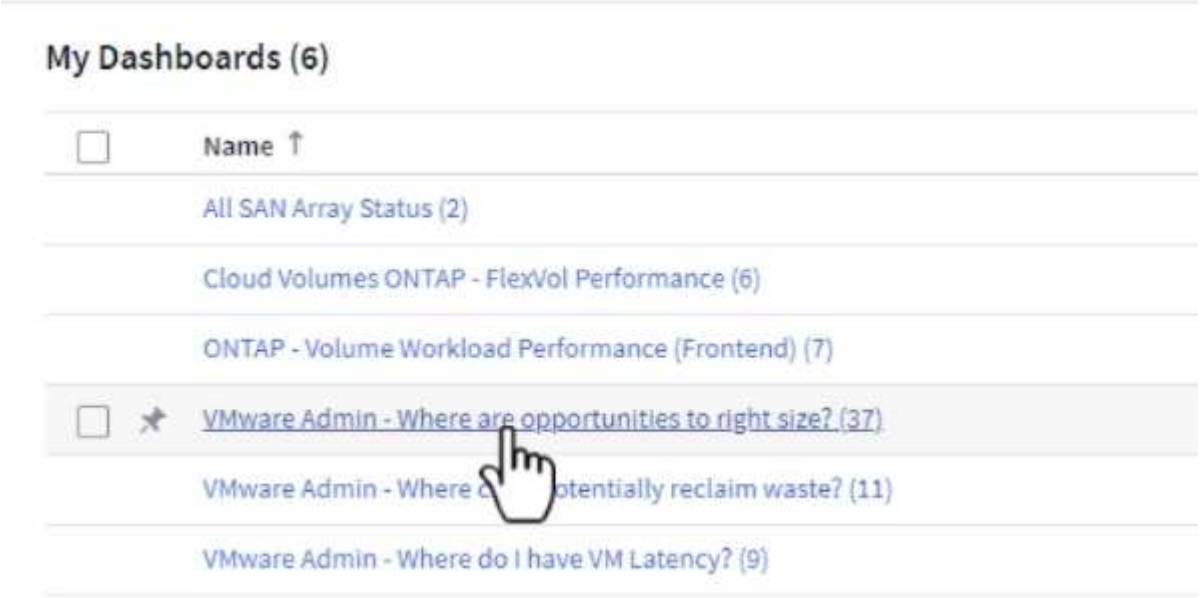


Visualizza le risorse sovra e sottoutilizzate in Cloud Insights

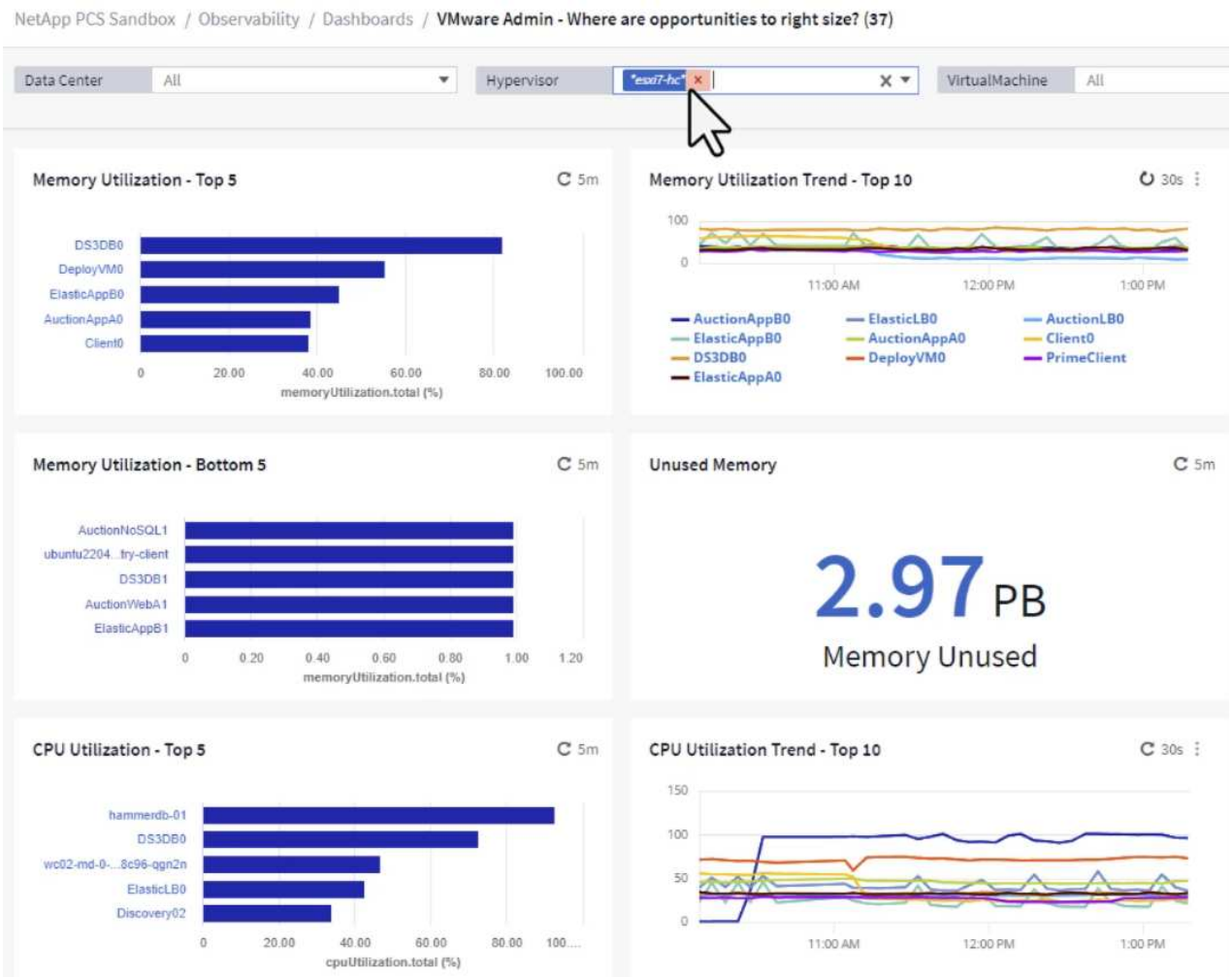
Abbinando le risorse delle VM ai requisiti effettivi del carico di lavoro, è possibile ottimizzare l'utilizzo delle risorse, con conseguente risparmio sui costi dell'infrastruttura e dei servizi cloud. I dati in Cloud Insights possono essere personalizzati per visualizzare facilmente le VM sovra o sotto utilizzate.

Identificare le opportunità per dimensionare correttamente le VM

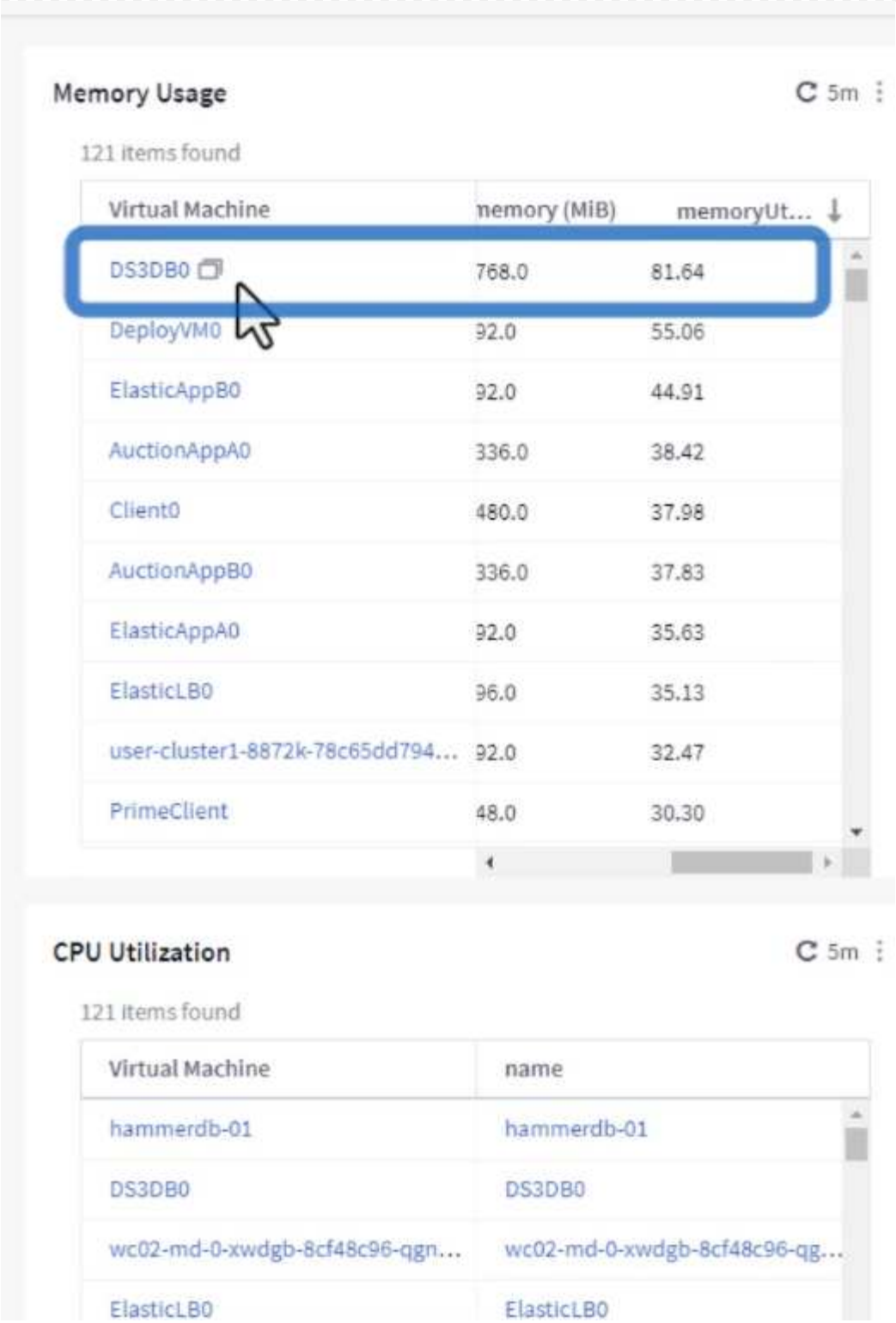
1. In questo esempio accedi a una dashboard disponibile nella **Galleria** denominata **VMware Admin - Dove sono le opportunità da dimensionare correttamente?**



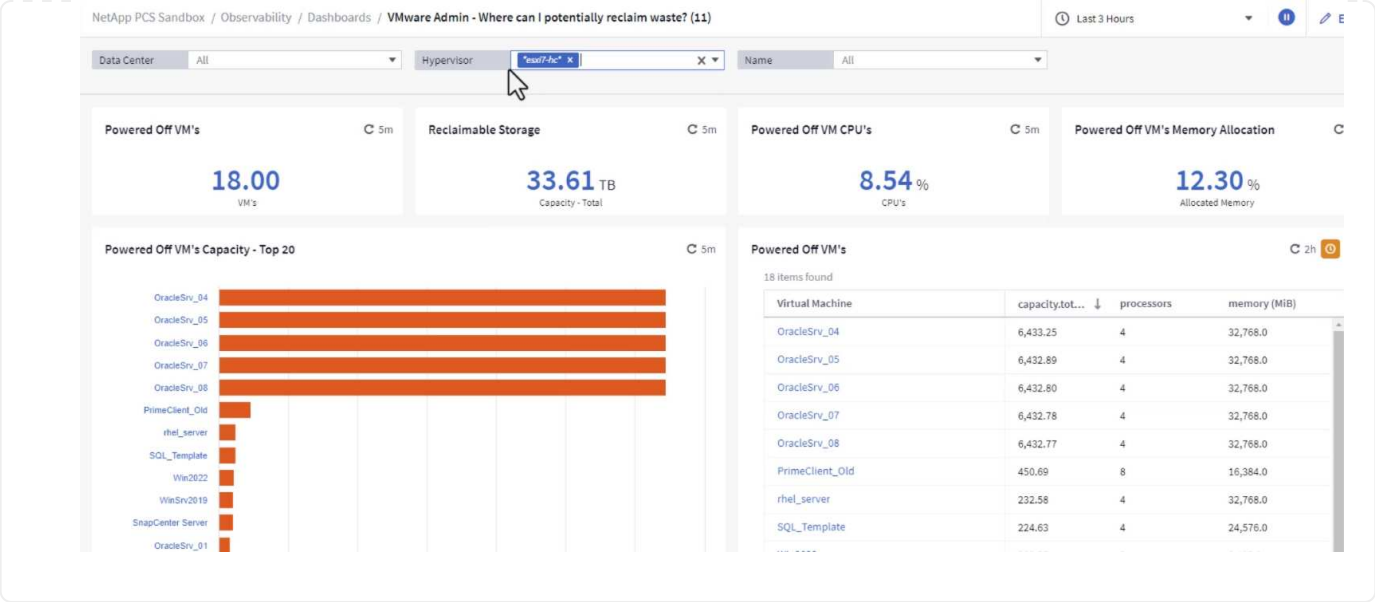
2. Per prima cosa filtrare in base a tutti gli host ESXi nel cluster. È quindi possibile visualizzare la classifica delle VM migliori e peggiori in base all'utilizzo di memoria e CPU.



3. Le tabelle consentono di ordinare e forniscono maggiori dettagli in base alle colonne di dati scelte.



4. Un'altra dashboard denominata **VMware Admin - Dove posso potenzialmente recuperare gli sprechi?** mostra le VM spente ordinate in base alla loro capacità di utilizzo.

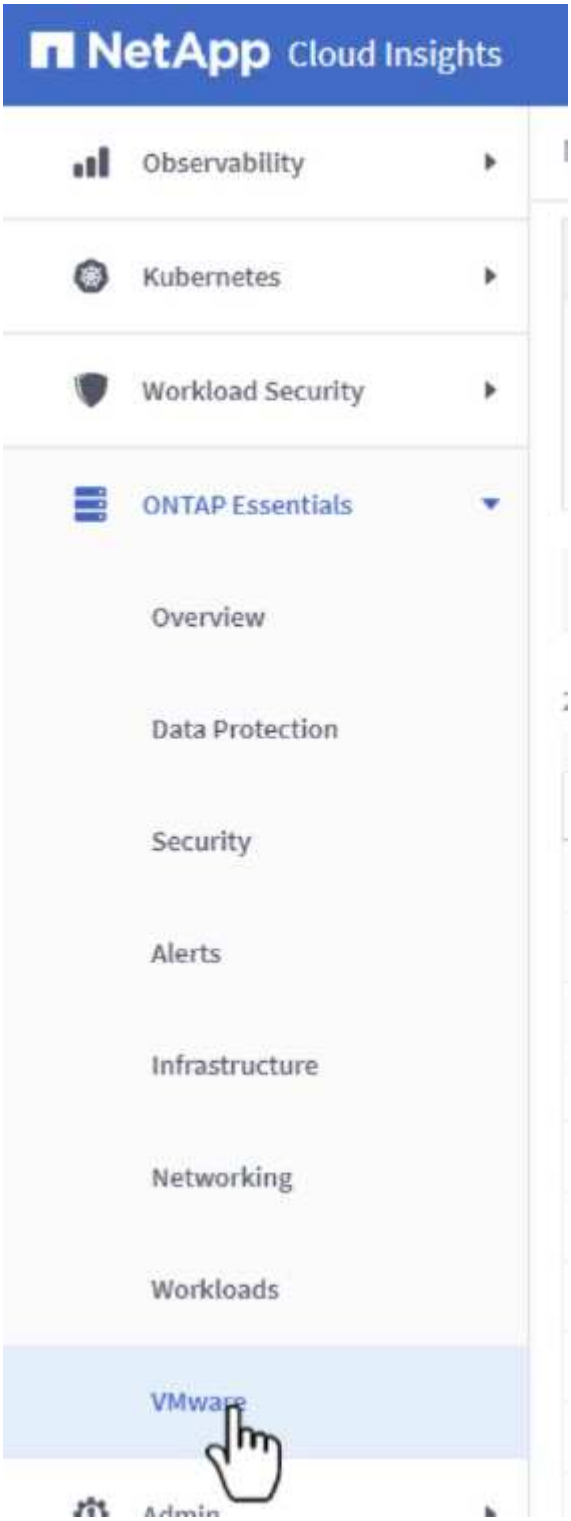


Utilizzare query per isolare e ordinare le metriche

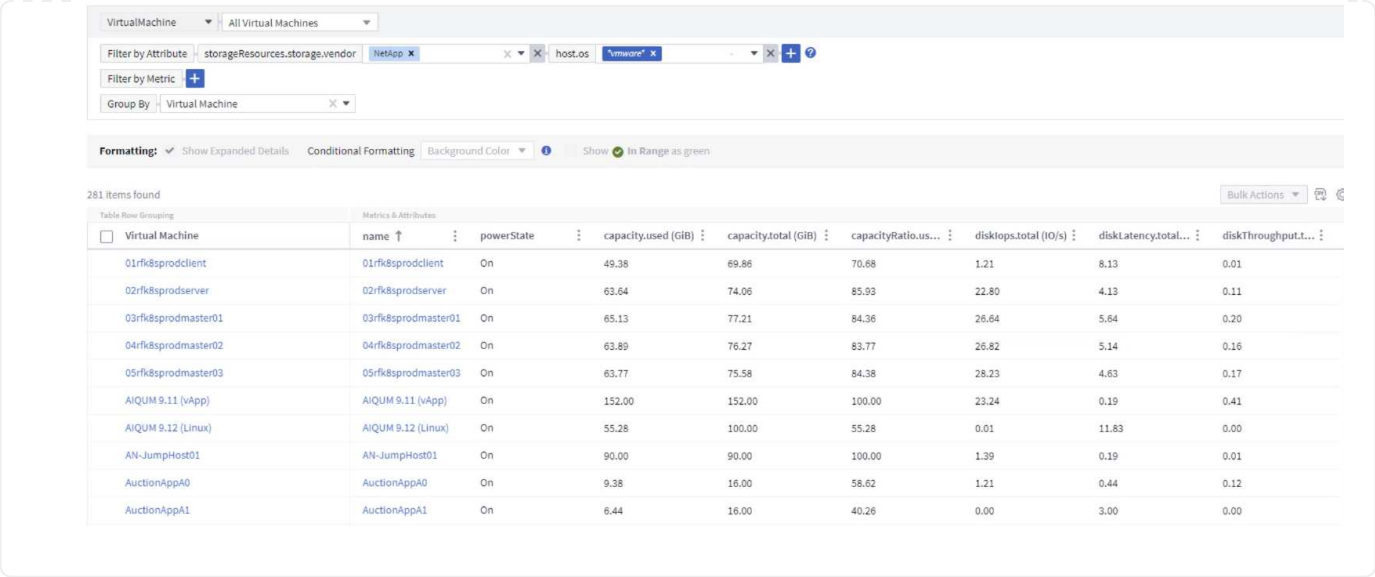
La quantità di dati acquisiti da Cloud Insights è piuttosto ampia. Le query metriche rappresentano un modo efficace per ordinare e organizzare grandi quantità di dati in modo utile.

Visualizza una query VMware dettagliata in ONTAP Essentials

1. Passare a * ONTAP Essentials > VMware* per accedere a una query completa sulle metriche VMware.



2. In questa vista vengono presentate diverse opzioni per filtrare e raggruppare i dati nella parte superiore. Tutte le colonne di dati sono personalizzabili e possono essere aggiunte facilmente altre colonne.



Conclusione

Questa soluzione è stata progettata come introduzione per imparare a usare NetApp Cloud Insights e mostrare alcune delle potenti funzionalità che questa soluzione di osservabilità può offrire. Il prodotto è dotato di centinaia di dashboard e query metriche integrate, che consentono di iniziare subito a utilizzarlo. La versione completa di Cloud Insights è disponibile come prova di 30 giorni, mentre la versione base è disponibile gratuitamente per i clienti NetApp .

Informazioni aggiuntive

Per saperne di più sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Pagina di destinazione di NetApp BlueXP e Data Infrastructure Insights"
- "Documentazione NetApp Data Infrastructure Insights"

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.