



# **NFS Reference Guide for vSphere 8**

NetApp Solutions

NetApp  
August 24, 2024

# Sommario

- NFS 3,1 - Guida di riferimento per vSphere 8 ..... 1
  - Utilizzo di NFS 3,1 con vSphere 8 e dei sistemi storage ONTAP ..... 1
  - Panoramica sulla tecnologia ..... 1
  - Funzionalità NFS nConnect con NetApp e VMware ..... 9
  - Utilizza i tool ONTAP 10 per configurare datastore NFS per vSphere 8 ..... 13
  - Utilizza VMware Site Recovery Manager per il disaster recovery dei datastore NFS ..... 44
  - Protezione autonoma dal ransomware per lo storage NFS ..... 70

# NFS 3,1 - Guida di riferimento per vSphere 8

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

## Utilizzo di NFS 3,1 con vSphere 8 e dei sistemi storage ONTAP

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

### Casi di utilizzo

Casi d'utilizzo illustrati nella presente documentazione:

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

### Pubblico

Questa soluzione è destinata alle seguenti persone:

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

## Panoramica sulla tecnologia

La guida di riferimento VCF di NFS 3,1 per vSphere 8 comprende i seguenti componenti principali:

## VMware vSphere Foundation (Fondazione VMware vSphere)

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

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

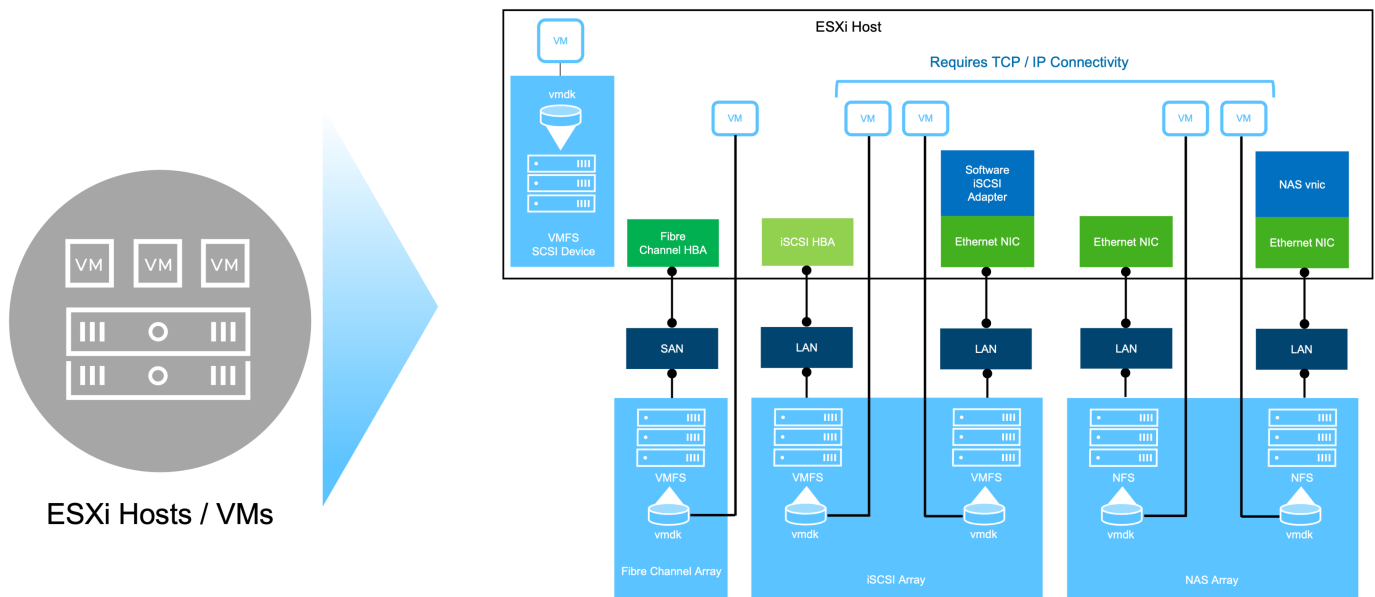
- VMware vSphere
- VMware vSAN
- Aria standard
- VMware Tanzu Kubernetes Grid Service per vSphere
- Switch distribuito vSphere

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

## Opzioni di archiviazione VVF

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

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



Per "[Introduzione allo storage nell'ambiente vSphere](#)" ulteriori informazioni sui tipi di storage supportati per

VMware vSphere Foundation, fare riferimento a .

## NetApp ONTAP

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

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

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

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

L'utilizzo di ONTAP insieme a vSphere è un'ottima combinazione che consente di ridurre le spese relative all'hardware host e al software VMware. Puoi anche proteggere i tuoi dati a un costo inferiore con performance elevate e costanti. Poiché i carichi di lavoro virtualizzati sono mobili, è possibile esplorare diversi approcci utilizzando Storage vMotion per spostare le macchine virtuali tra datastore VMFS, NFS o vVol, tutti sullo stesso sistema storage.

## Array All-Flash NetApp

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

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

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

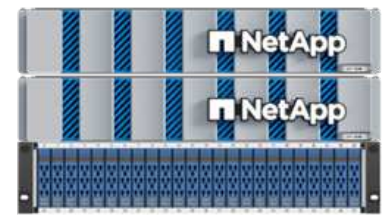
## AFF A70



## AFF A90



## AFF A1K



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

## AFF C250



## AFF C400



## AFF C800



### Supporto dei protocolli di storage

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

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

Per informazioni sulla progettazione delle configurazioni NFS, fare riferimento alla ["Documentazione di gestione dello storage NAS"](#).

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

Per istruzioni sulla progettazione delle configurazioni iSCSI, fare riferimento alla ["Documentazione di riferimento per la configurazione SAN"](#).

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

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

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

Per informazioni sulla progettazione su NVMe, fare riferimento a ["Configurazione, supporto e limitazioni NVMe"](#).

## Tecnologia Active-Active

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

Per ulteriori informazioni, consultare ["Data Protection e disaster recovery"](#) la documentazione.

## Garanzie di archiviazione

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

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

Per informazioni dettagliate, vedere ["Landing page di NetApp AFF"](#).

## Strumenti NetApp ONTAP per VMware vSphere

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

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

Strumenti ONTAP completi 10 risorse sono disponibili ["Strumenti ONTAP per le risorse di documentazione di VMware vSphere"](#).

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

## Plug-in NetApp NFS per VMware VAAI

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

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

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

## Plug-in SnapCenter per VMware vSphere

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

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

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

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

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

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

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

Per ulteriori informazioni, fare riferimento a ["Plug-in SnapCenter per la documentazione di VMware vSphere"](#).

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

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

Per istruzioni dettagliate sull'implementazione del plug-in SnapCenter, fare riferimento alla soluzione ["Utilizza il plug-in SnapCenter per VMware vSphere per proteggere le VM nei domini del carico di lavoro VCF"](#).

## Considerazioni sullo storage

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

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



Per informazioni dettagliate su nConnect, fare riferimento a ["Funzionalità NFS nConnect con VMware e NetApp"](#).

**Session trunking for NFS:** a partire da ONTAP 9.14.1, i client che utilizzano NFSv4.1 possono sfruttare il trunking di sessione per stabilire connessioni multiple a varie LIF sul server NFS. In questo modo è possibile trasferire i dati più velocemente e migliorare la resilienza utilizzando il multipathing. Il trunking risulta particolarmente vantaggioso quando si esportano volumi FlexVol in client che supportano il trunking, come i client VMware e Linux, o quando si utilizza NFS su protocolli RDMA, TCP o pNFS.

Per ulteriori informazioni, fare riferimento ["Panoramica del trunking NFS"](#) a.

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

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

## Protezione ransomware

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

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

Per ulteriori informazioni sulla garanzia di ripristino dal ransomware, consulta: ["Garanzia di recupero Ransomware"](#).

Per ["Panoramica della protezione ransomware autonoma"](#) ulteriori informazioni dettagliate, fare riferimento alla

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

## Considerazioni sul disaster recovery

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

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

Per ulteriori informazioni, fare riferimento alla ["Panoramica di VMware Site Recovery Manager"](#).

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

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

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

## Panoramica delle soluzioni

Soluzioni descritte nella presente documentazione:

- **NFS nConnect con NetApp e VMware.** Fare clic su ["qui"](#) per i passaggi di distribuzione.
  - **Utilizzare gli strumenti ONTAP 10 per configurare gli archivi dati NFS per vSphere 8.** Fare clic su ["qui"](#) per i passaggi di distribuzione.
  - **Distribuire e utilizzare il plug-in SnapCenter per VMware vSphere per proteggere e ripristinare le VM.** Fare clic su ["qui"](#) per i passaggi di distribuzione.
  - **Disaster Recovery di archivi dati NFS con VMware Site Recovery Manager.** Fare clic su ["qui"](#) per i passaggi di distribuzione.

- **Protezione autonoma da ransomware per lo storage NFS.** Fare clic su ["qui"](#) per i passaggi di distribuzione.

## Funzionalità NFS nConnect con NetApp e VMware

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



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

### Casi di utilizzo

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

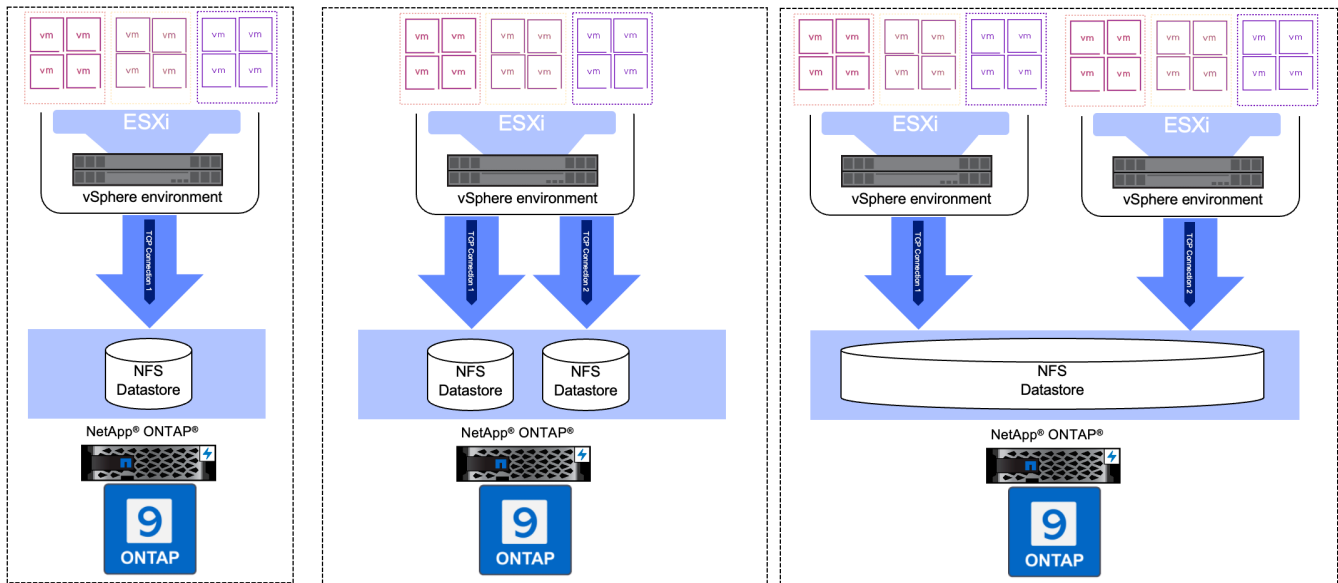
### Dettagli tecnici

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

### Datastore NFS predefinito

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

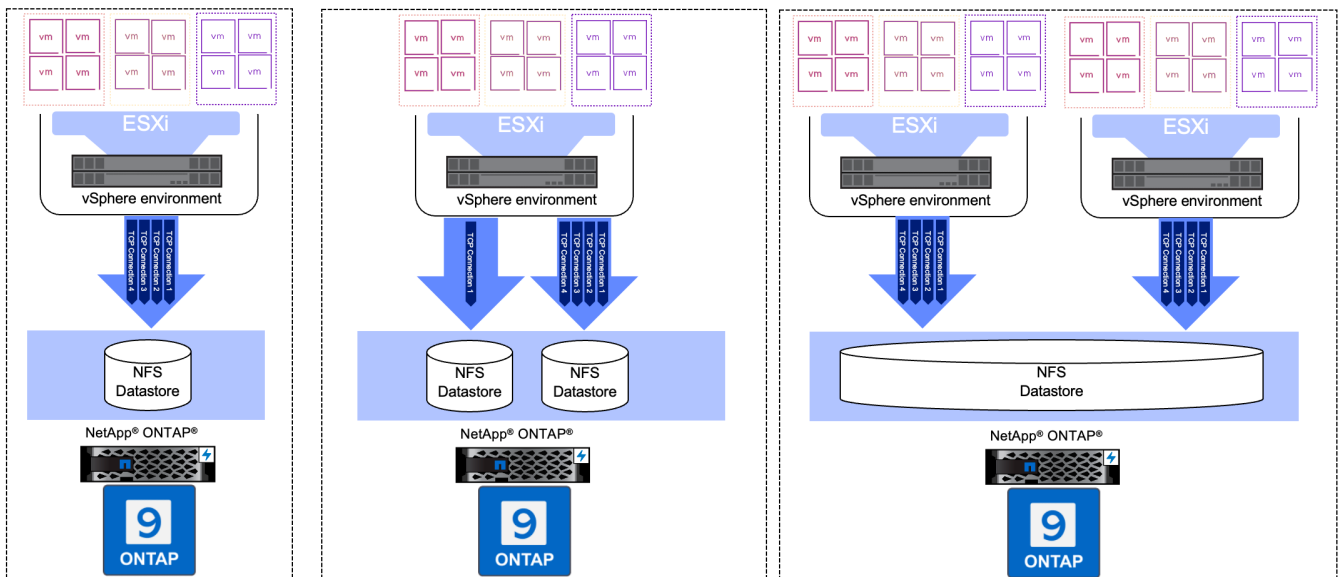
## Without nConnect feature with NetApp and VMware



### Con nConnect NFS Datastore

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

## With nConnect feature with NetApp and VMware



### Prerequisito

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

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

## Aggiornare il numero di connessione al datastore NFS

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

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

Oppure utilizzare PowerCLI come illustrato di seguito

```

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

```

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

```

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

```

Fare riferimento a ["Articolo della KB di VMware 91497"](#) per ulteriori informazioni.

## Considerazioni di progettazione

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

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

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



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

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

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

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

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

#### Panoramica della soluzione

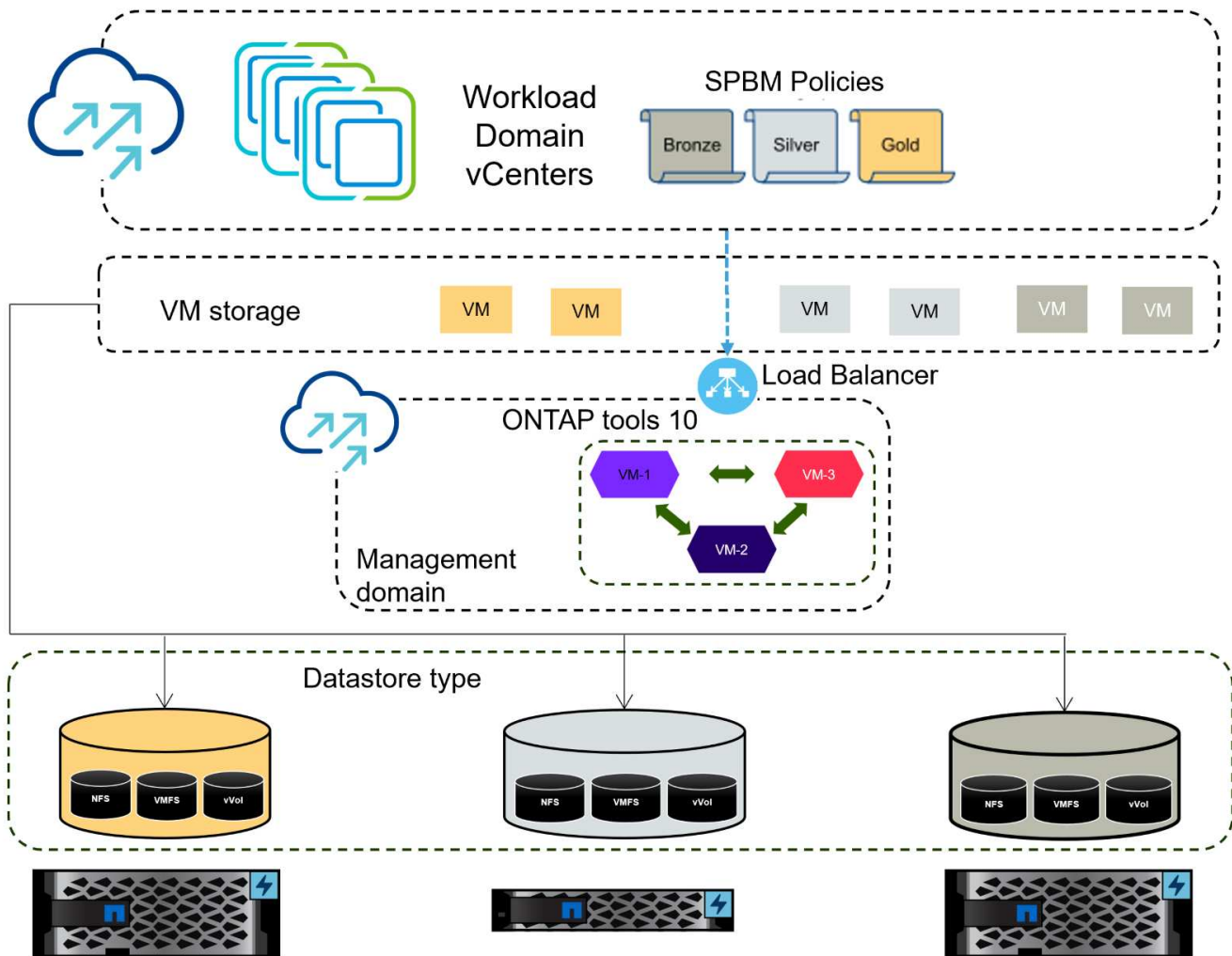
Questo scenario copre i seguenti passaggi di alto livello:

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

#### Architettura

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





## Prerequisiti

Questa soluzione richiede i seguenti componenti e configurazioni:

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

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

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

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

Strumenti ONTAP completi 10 risorse sono disponibili ["Strumenti ONTAP per le risorse di documentazione di VMware vSphere"](#).



## **Fasi di implementazione**

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

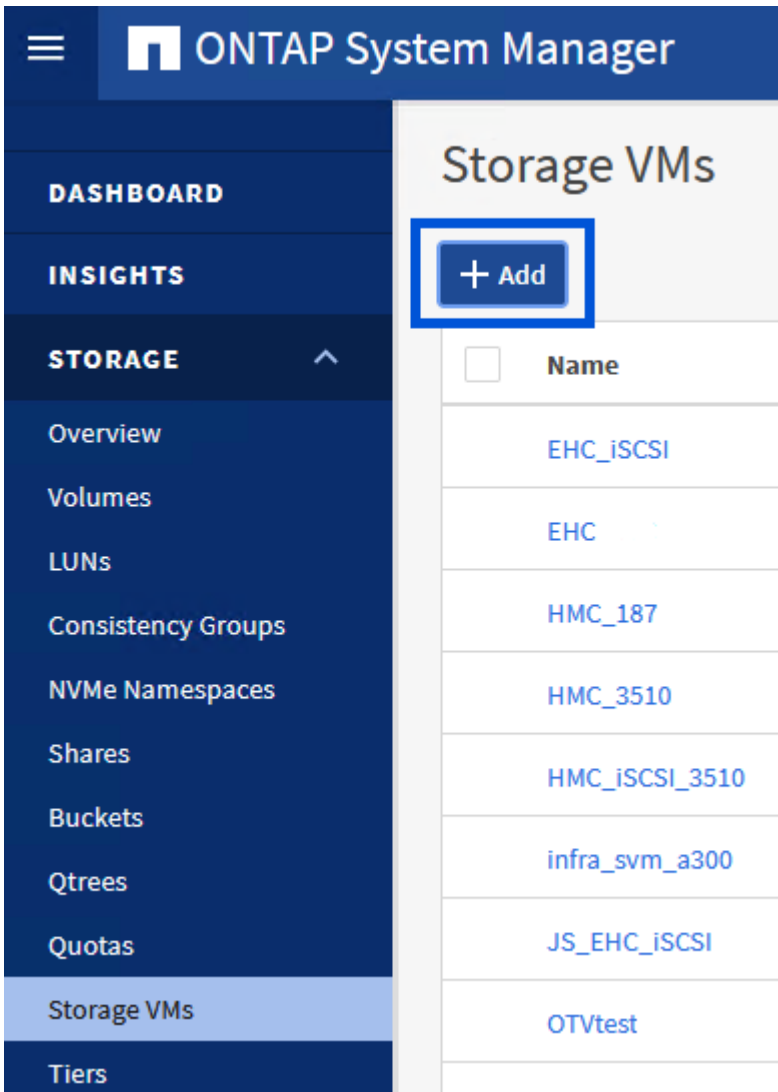
### **Crea SVM e LIF su un sistema storage ONTAP**

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

## Creazione di LIF e macchine virtuali storage

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

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



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

## Add Storage VM



STORAGE VM NAME

VCF\_NFS

IPSPACE

Default


### Access Protocol

SMB/CIFS, NFS, S3  iSCSI  FC  NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf\_8



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

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

## NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS\_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

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

## Storage VM Administration

Manage administrator account

Save

Cancel

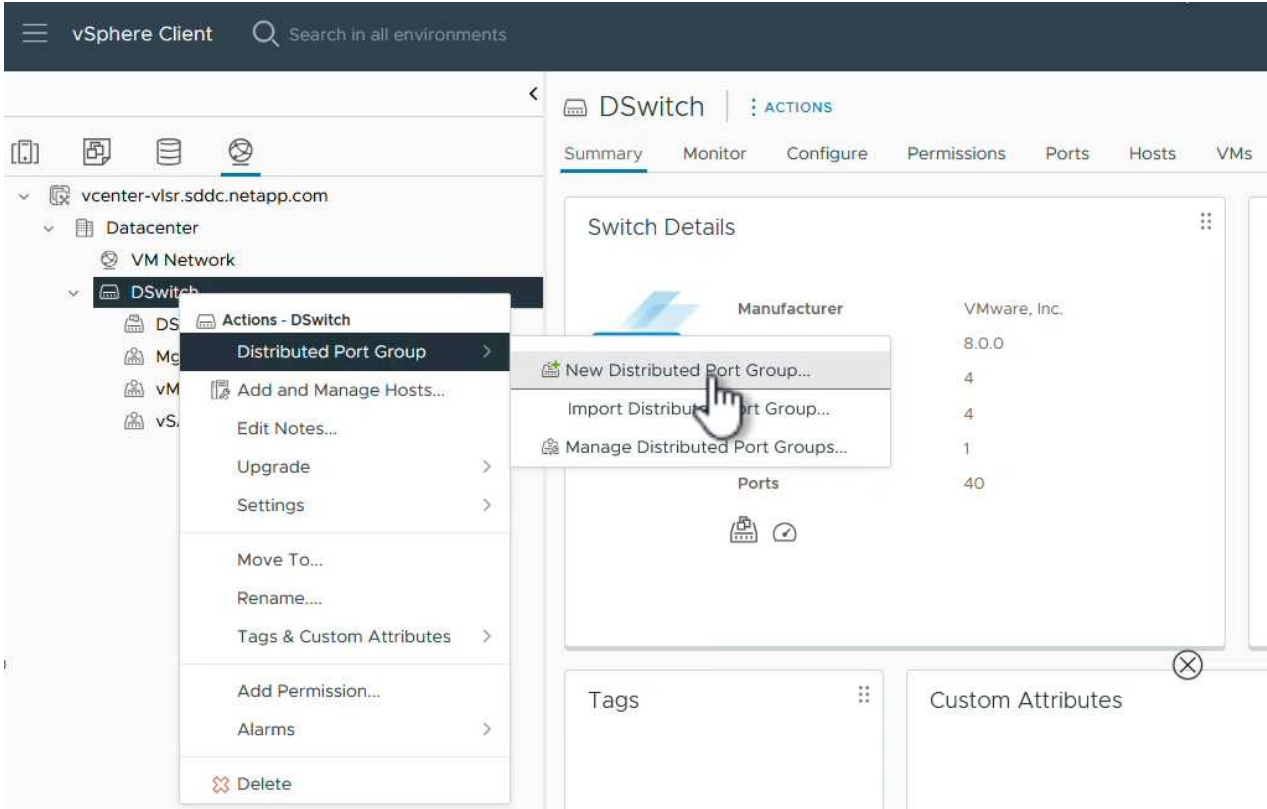
### Configurare il networking per NFS sugli host ESXi

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

## Creare un gruppo di porte distribuite per il traffico NFS

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

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



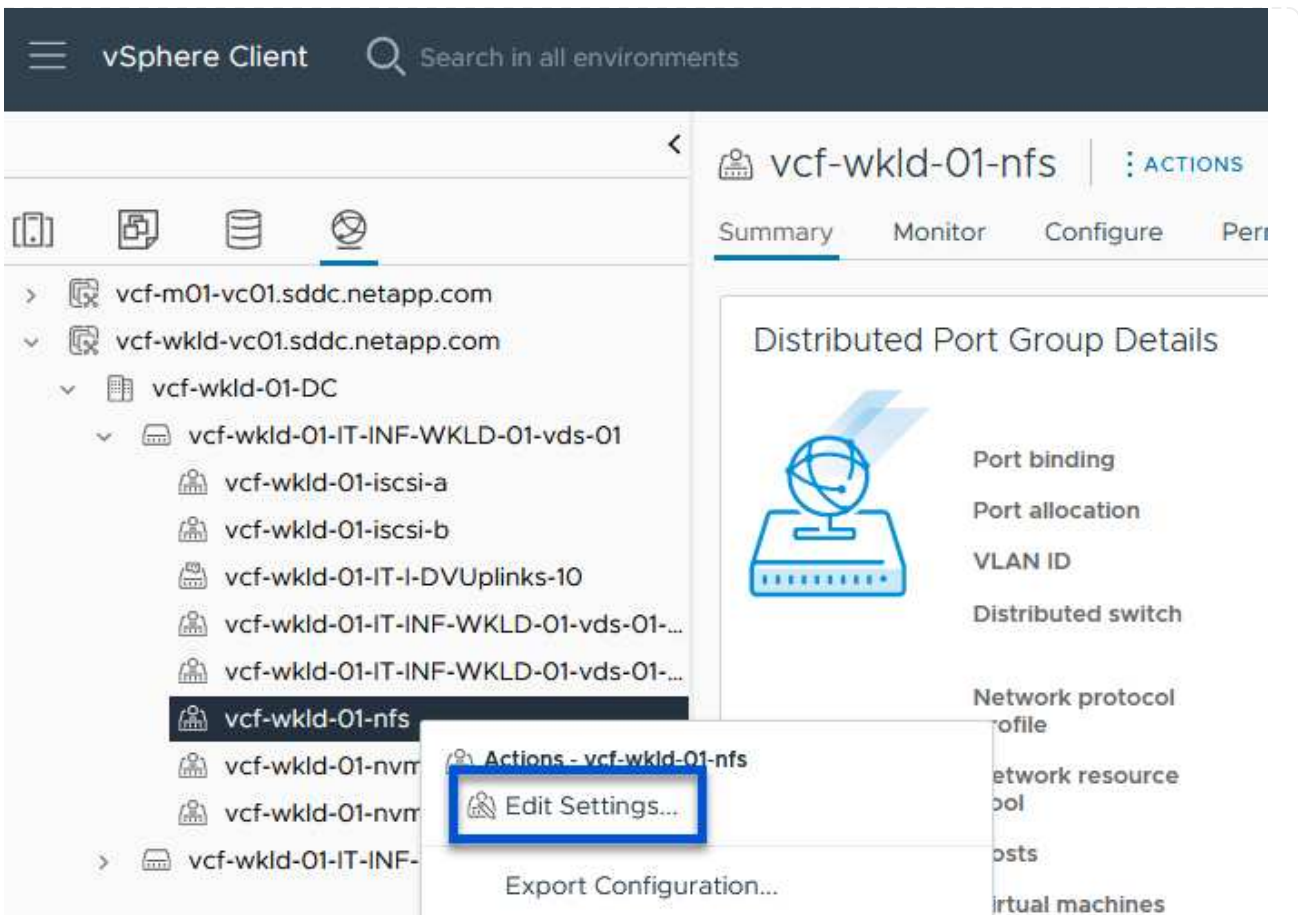
2. Nella procedura guidata **nuovo gruppo di porte distribuite** inserire un nome per il nuovo gruppo di porte e fare clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni** completare tutte le impostazioni. Se si utilizzano VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare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

The screenshot shows a configuration wizard for a 'New Distributed Port Group'. The left sidebar has three steps: '1 Name and location', '2 Configure settings' (highlighted), and '3 Ready to complete'. The main area is titled 'Configure settings' and contains the following fields:

- Port binding:** Static binding (dropdown)
- Port allocation:** Elastic (dropdown with an info icon)
- Number of ports:** 8 (input field)
- Network resource pool:** (default) (dropdown)
- VLAN:**
  - VLAN type:** VLAN (dropdown)
  - VLAN ID:** 3374 (input field)
- Advanced:**
  - Customize default policies configuration

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking on the 'NEXT' button.

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



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

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

OK

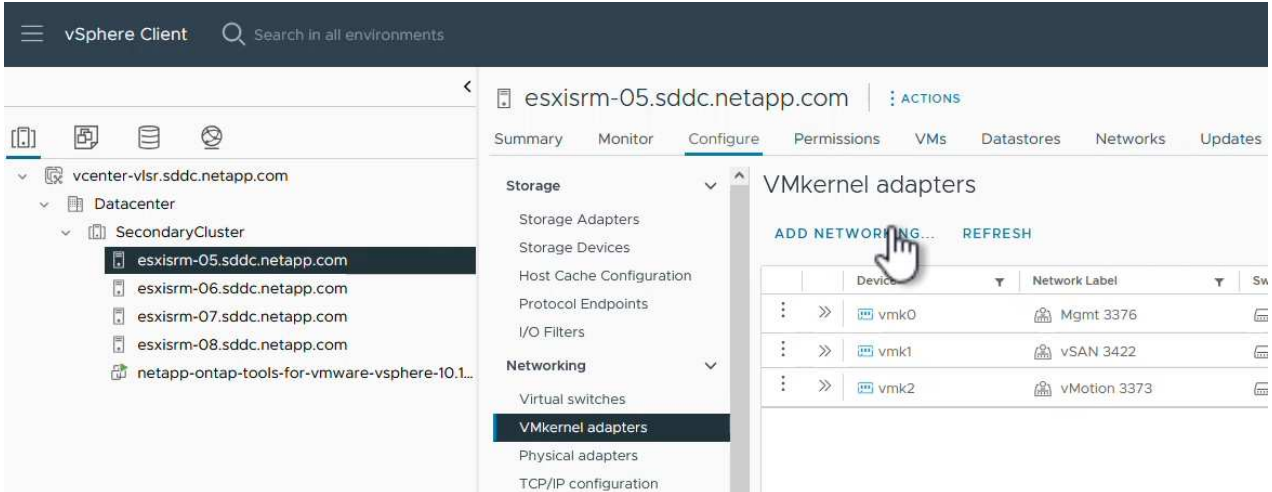
7. Ripetere questa procedura per ogni host ESXi nel cluster.



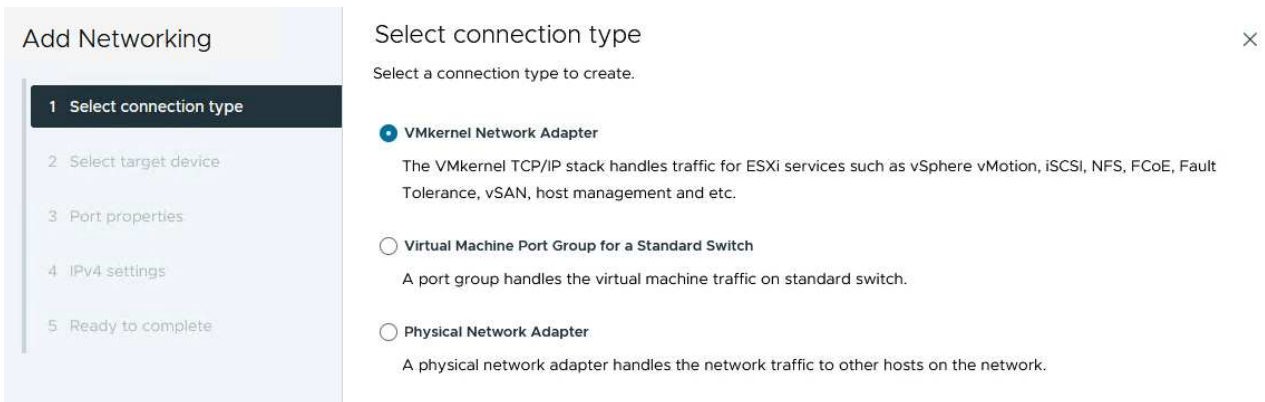
## Creare un adattatore VMkernel su ciascun host ESXi

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

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



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



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

## Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

## Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	Mgmt 3376	--	DSwitch
<input checked="" type="radio"/>	NFS 3374	--	DSwitch
<input type="radio"/>	vMotion 3373	--	DSwitch
<input type="radio"/>	vSAN 3422	--	DSwitch

Manage Columns 4 items

CANCEL

BACK

NEXT

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

## Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings**
- 5 Ready to complete

## IPv4 settings



Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway  Override default gateway for this adapter

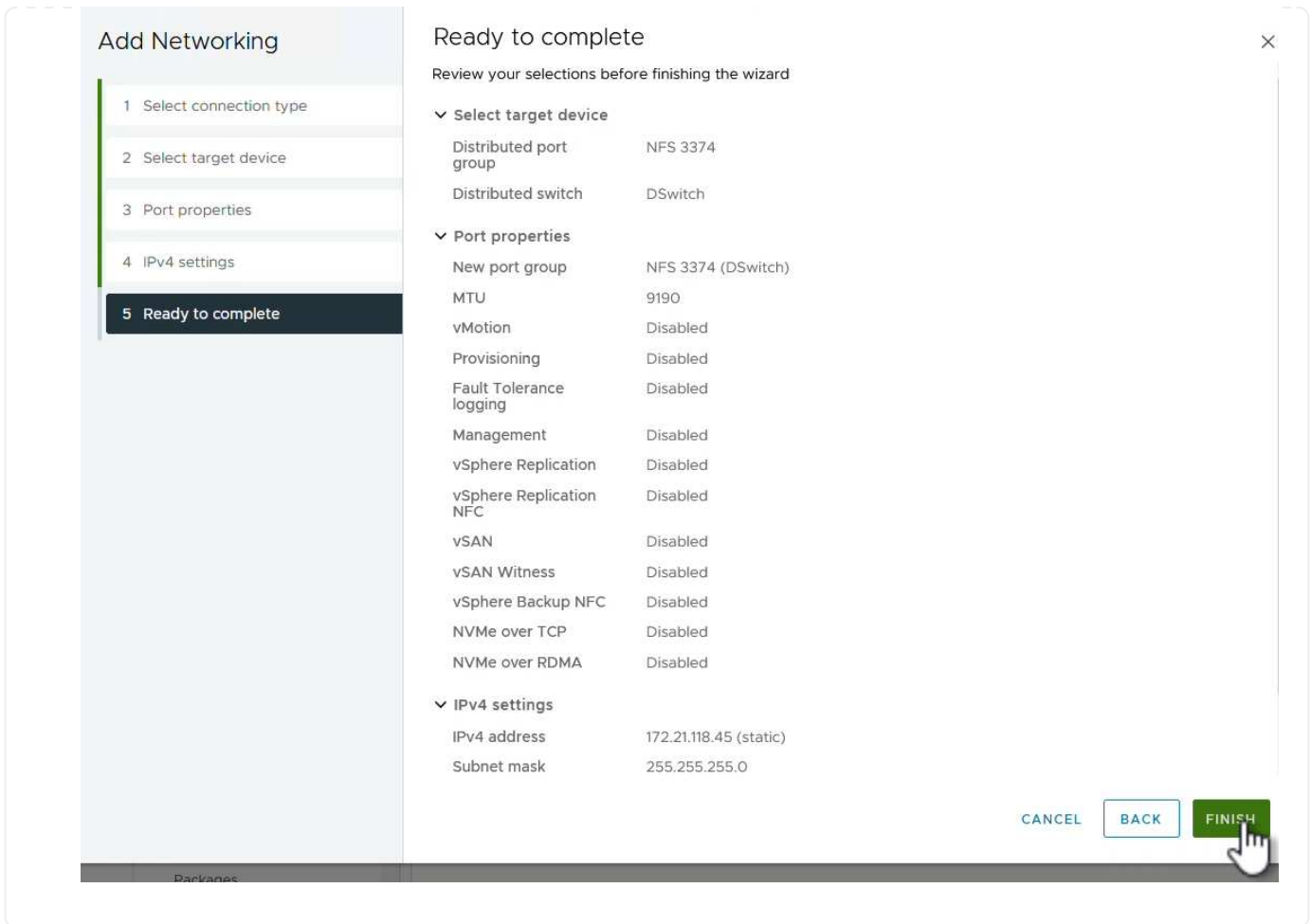
DNS server addresses

CANCEL

BACK

NEXT

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



## Implementare e utilizzare gli strumenti ONTAP 10 per configurare lo storage

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

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

## Implementa i tool ONTAP per VMware vSphere 10

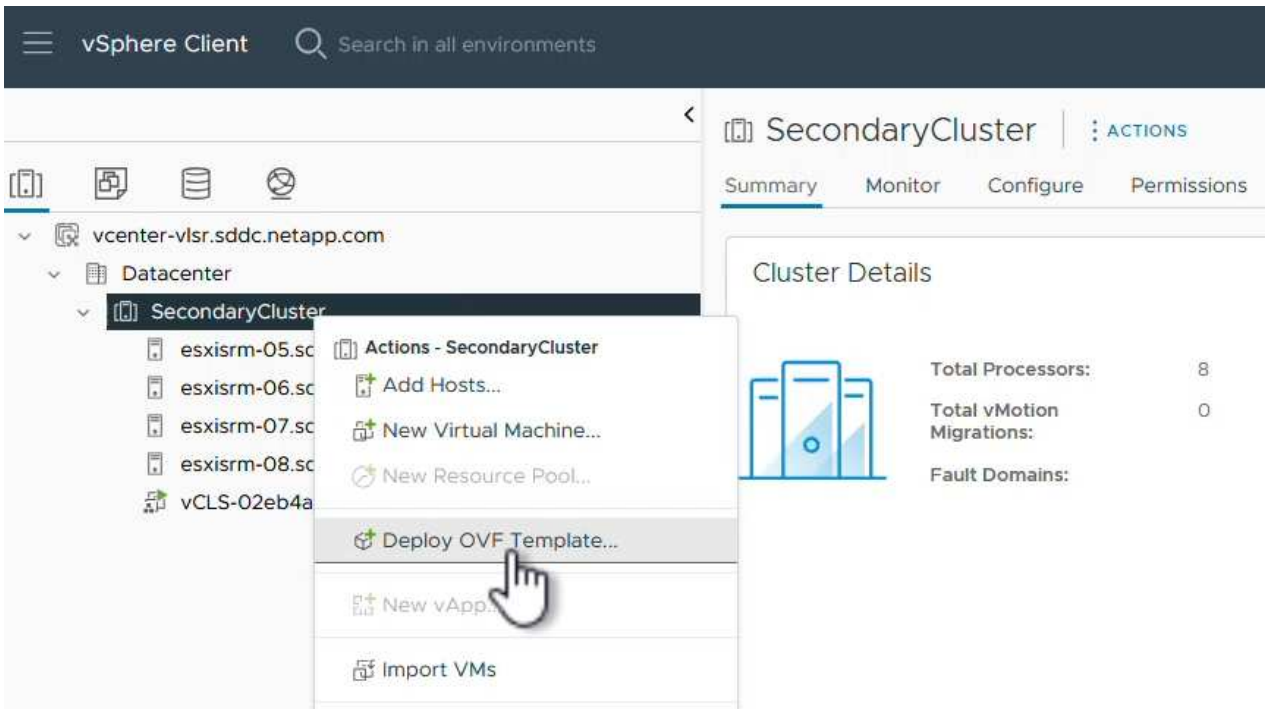
I tool ONTAP per VMware vSphere 10 vengono implementati come appliance delle macchine virtuali e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP. Strumenti ONTAP 10 è dotato di un nuovo portale di gestione globale per la gestione delle connessioni a più server vCenter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



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

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

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



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

## Deploy OVF Template

### 1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

## Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

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

## Deploy OVF Template

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

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

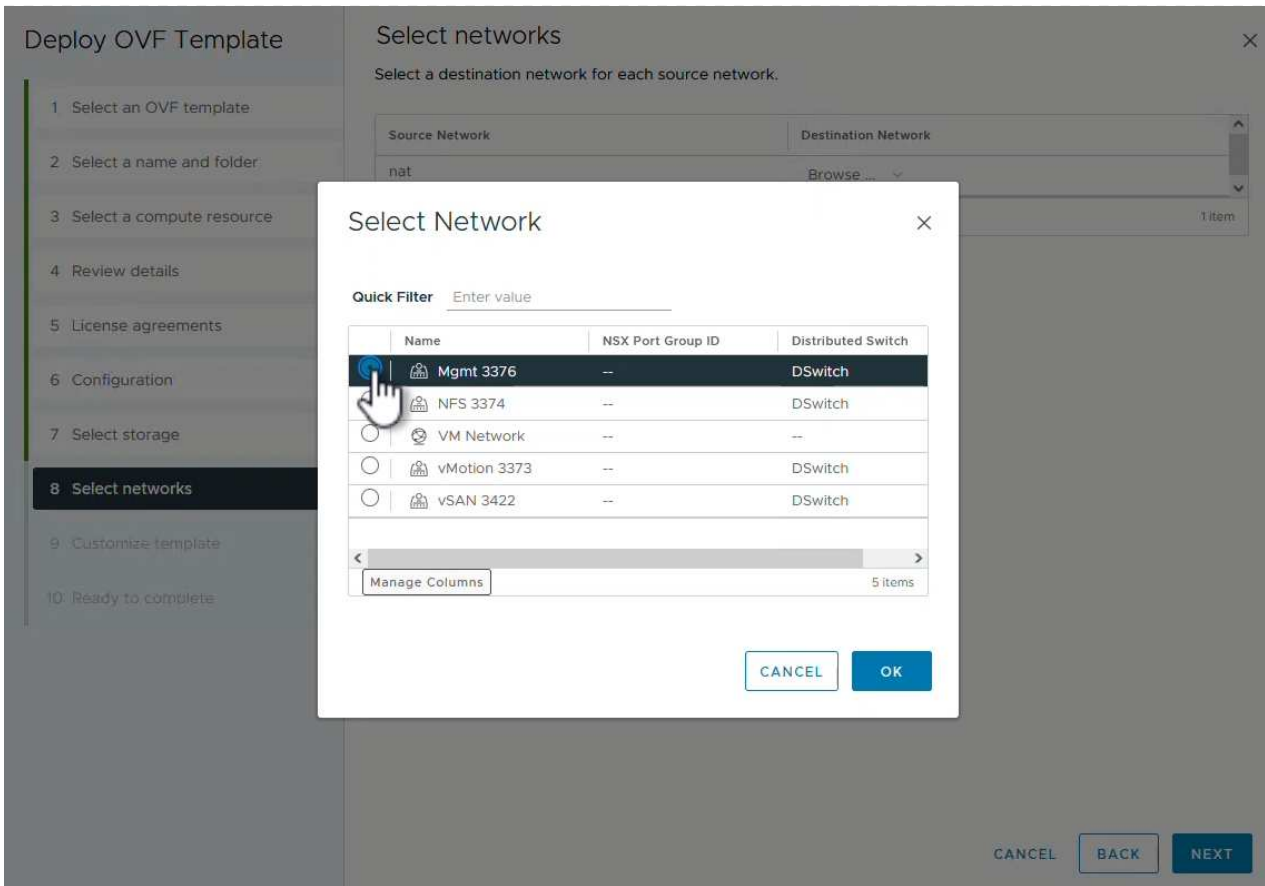
VM Storage Policy

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	
vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB	

Compatibility

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



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



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

## Deploy OVF Template

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

## Configuration

Select a deployment configuration

	Description
<input checked="" type="radio"/> Easy deployment (S)	Deploy local provisioner Non-HA Small single node instance of ONTAP tools
<input type="radio"/> Easy deployment (M)	
<input type="radio"/> Advanced deployment (S)	
<input type="radio"/> Advanced deployment (M)	
<input type="radio"/> High-Availability deployment (S)	
<input type="radio"/> High-Availability deployment (M)	
<input type="radio"/> High-Availability deployment (L)	
<input type="radio"/> Recovery	

8 Items

CANCEL

BACK

NEXT

9. Nella pagina Personalizza modello compilare tutte le informazioni richieste:

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

Fare clic su **Avanti** per continuare.



## Deploy OVF Template

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

## Customize template

Customize the deployment properties of this software solution.

! 10 properties have invalid values X

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

CANCEL BACK NEXT

## Deploy OVF Template

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

## Customize template

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

CANCEL BACK NEXT

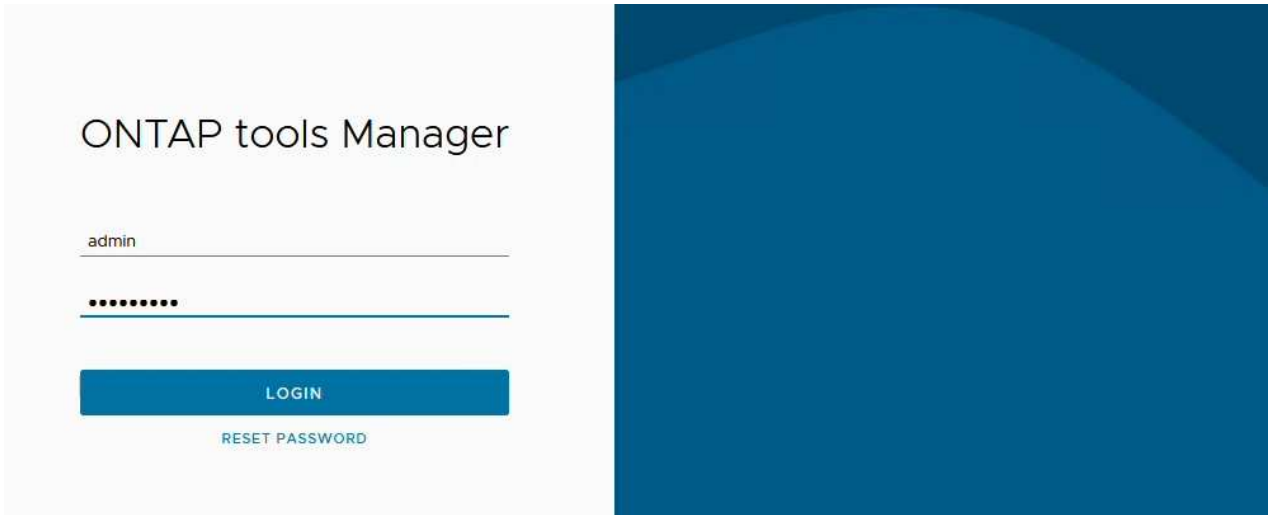
10. Esaminare tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare

a distribuire l'appliance ONTAP Tools.

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

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

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



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

# Getting Started



ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.



## Storage Backends

Add, modify, and remove storage backends.

[Go to Storage Backends](#)



## vCenters

Add, modify, and remove vCenters and associate storage backends with them.

[Go to vCenters](#)



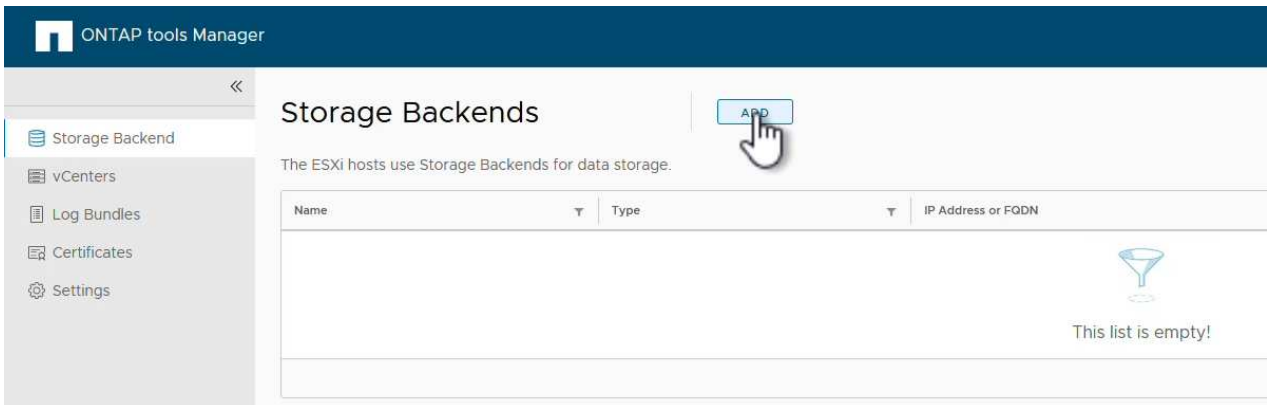
## Log Bundles

Generate and download log bundles for support purposes.

[Go to Log Bundles](#)

Don't show again

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




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

## Add Storage Backend

Hostname: \* 172.16.9.25

Username: \* admin

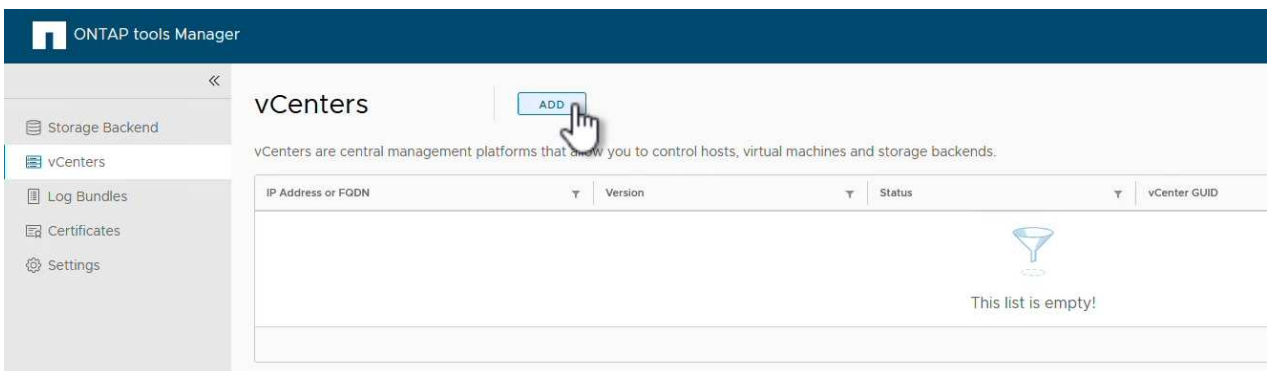
Password: \* ●●●●●●●● 

Port: \* 443

CANCEL

ADD 

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



The screenshot shows the ONTAP tools Manager interface. The top navigation bar is dark blue with the ONTAP logo and the text "ONTAP tools Manager". On the left, there is a sidebar menu with a back arrow and several items: "Storage Backend", "vCenters" (highlighted in blue), "Log Bundles", "Certificates", and "Settings". The main content area is titled "vCenters" and has an "ADD" button with a hand cursor pointing to it. Below the title, there is a descriptive sentence: "vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends." Underneath is a table with columns for "IP Address or FQDN", "Version", "Status", and "vCenter GUID". The table is currently empty, and a message "This list is empty!" is displayed in the center of the table area.

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

## Add vCenter

Server IP Address or FQDN: \*

Username: \*

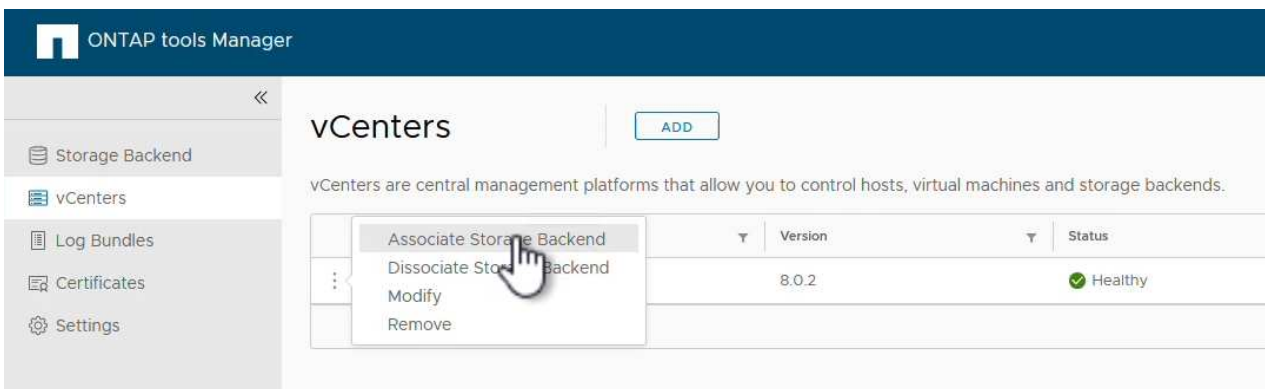
Password: \*  

Port: \*

CANCEL

ADD 



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



ONTAP tools Manager

vCenters ADD

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

	Version	Status
 Associate Storage Backend Dissociate Storage Backend Modify Remove	8.0.2	 Healthy

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

## Associate Storage Backend

vcenter-vlsr.sddc.netapp.com



Storage Backend

ntaphci-a300e9u25

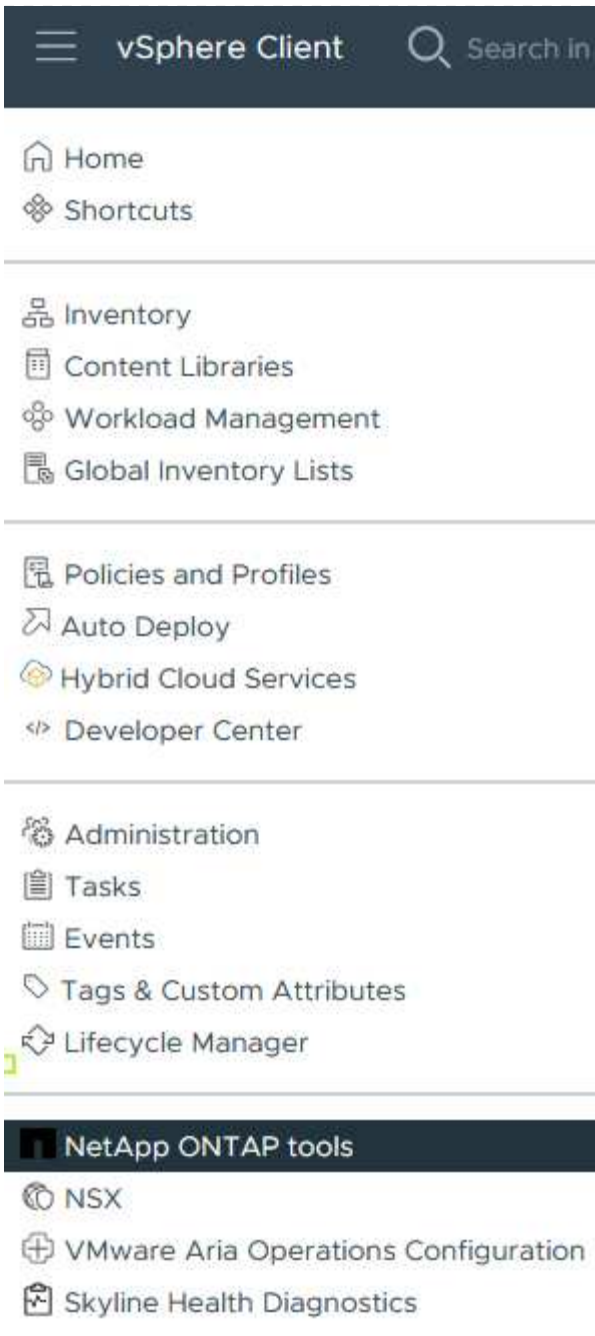


CANCEL

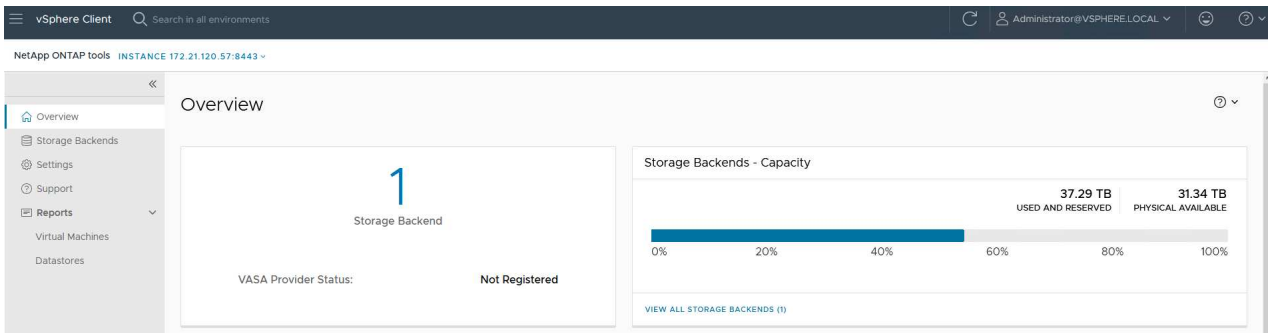
ASSOCIATE



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



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



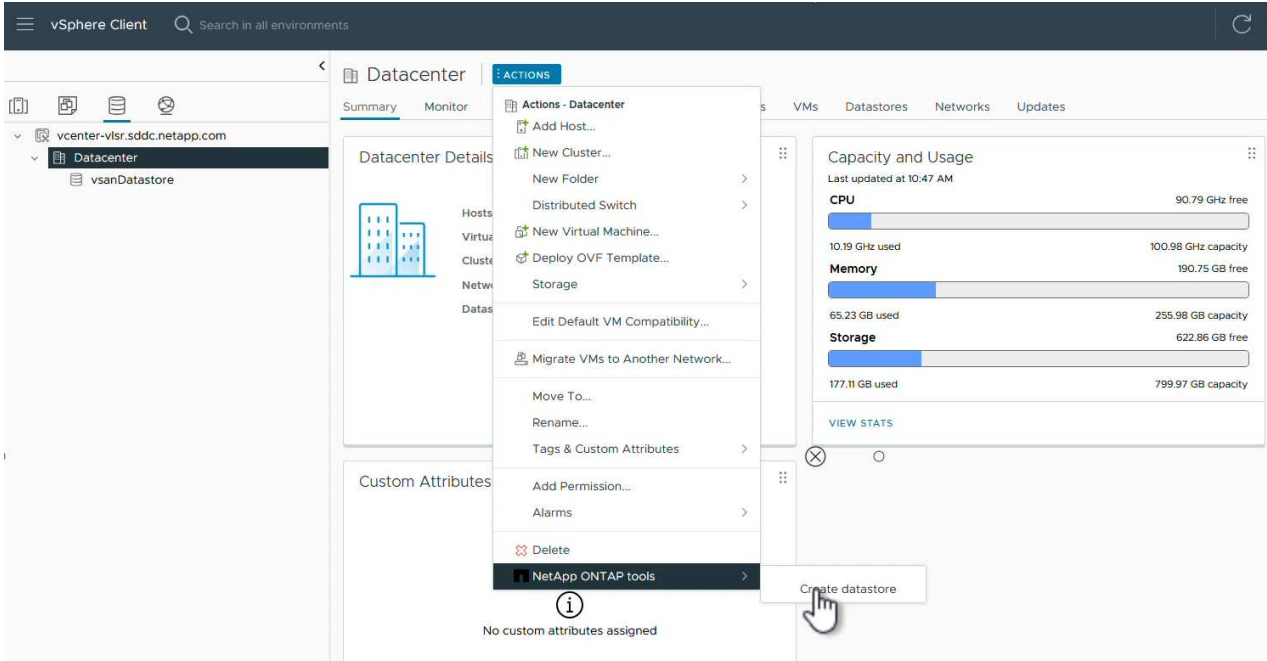




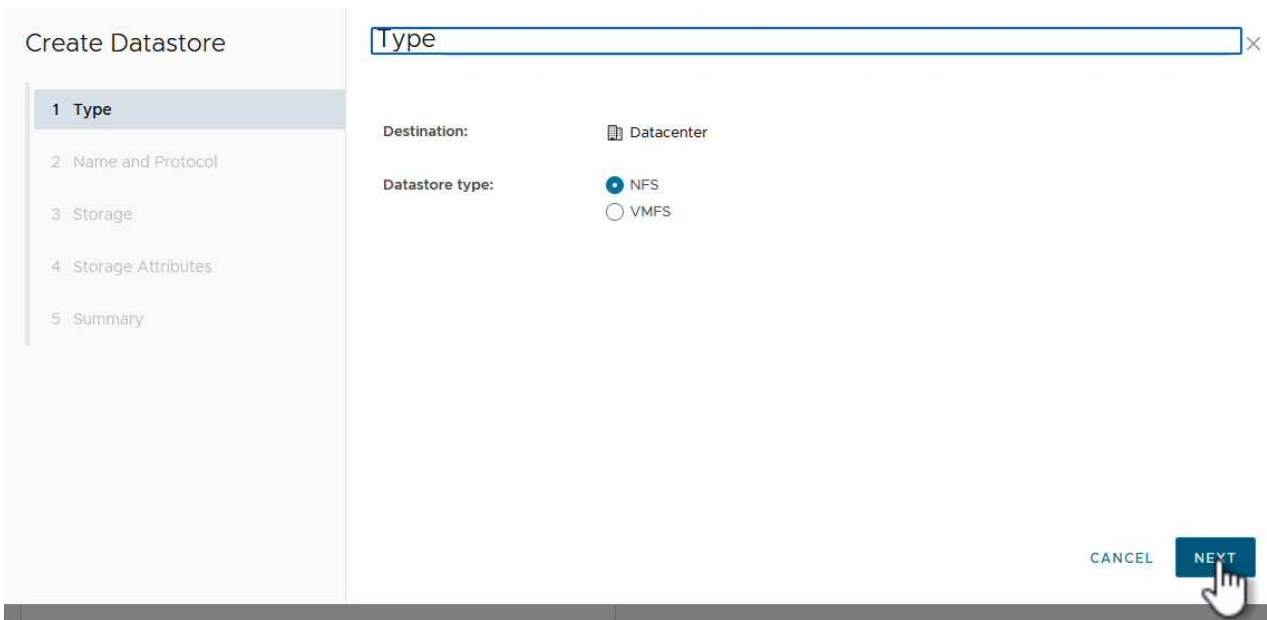
## Creare un datastore NFS utilizzando gli strumenti ONTAP 10

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

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



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



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

The screenshot shows the 'Create Datastore' wizard in the 'Name and Protocol' step. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol (highlighted), 3 Storage, 4 Storage Attributes, and 5 Summary. The main area is titled 'Name and Protocol' and contains the following fields:

- Datastore name:** NFS\_DS1
- Size:** 2 TB (with a note: 'Minimum supported size is 1 GB.')
- Protocol:** NFS 3
- Advanced Options:** (expanded)
- Datastore Cluster:** (empty dropdown)

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

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

The screenshot shows the 'Create Datastore' wizard in the 'Storage' step. On the left, the sidebar lists five steps: 1 Type, 2 Name and Protocol, 3 Storage (highlighted), 4 Storage Attributes, and 5 Summary. The main area is titled 'Storage' and contains the following fields:

- Platform: \*** Performance (A)
- Storage VM: \*** VCF\_NFS (with IP address: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** (expanded)
- Custom Export Policy:** Search or specify policy name (with a note: 'Choose an existing policy or give a new name to the default policy.')

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

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

## Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 **Storage Attributes**
- 5 Summary

## Storage Attributes

Specify the storage details for provisioning the datastore.

**Aggregate:** \* EHCaggr02 (16.61 TB Free) ▾

**Volume:** A new volume will be created automatically.

^ Advanced Options

**Space Reserve:** \* Thin ▾

**Enable QoS**

CANCEL

BACK

NEXT

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

## Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 **Summary**

## Summary

A new datastore will be created with these settings.

### Type

**Destination:** Datacenter  
**Datastore type:** NFS

### Name and Protocol

**Datastore name:** NFS\_DS1  
**Size:** 2 TB  
**Protocol:** NFS 3

### Storage

**Platform:** Performance (A)  
**Storage VM:** VCF\_NFS

CANCEL

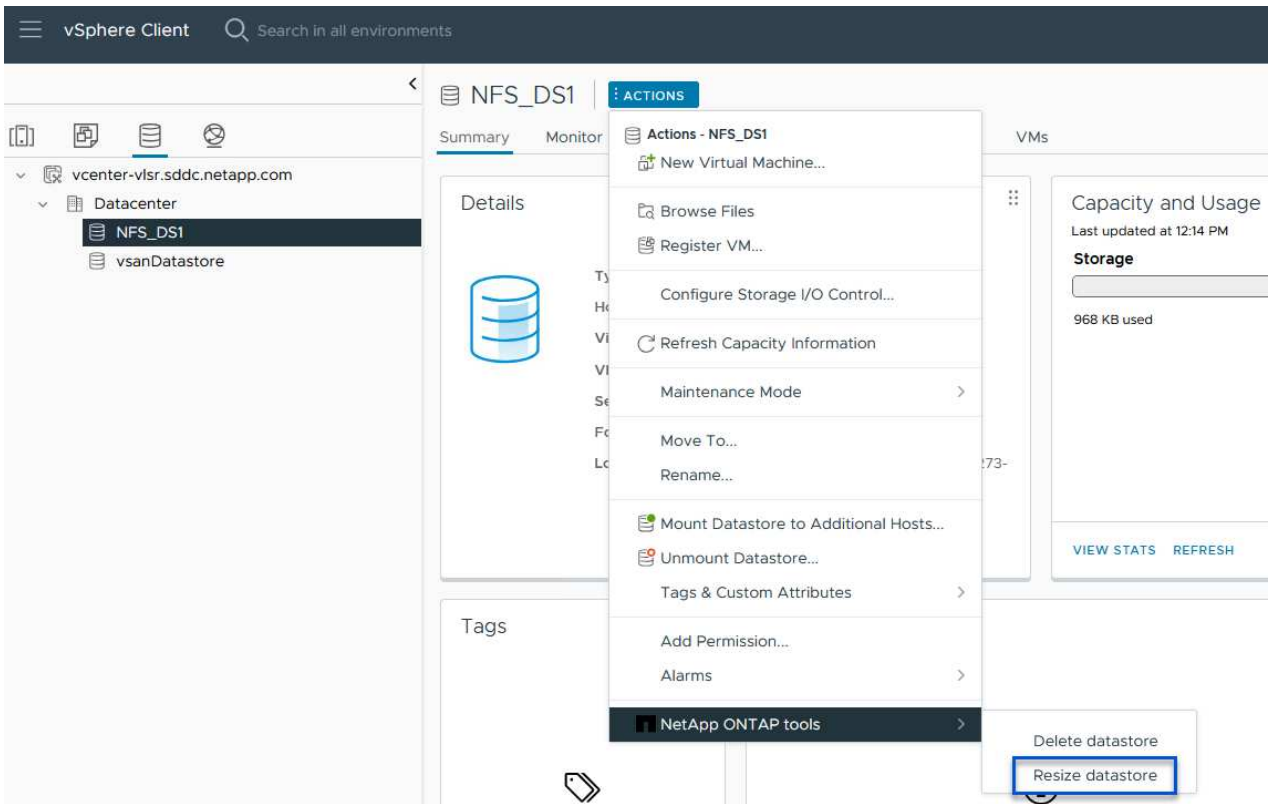
BACK

FINISH

## Ridimensionamento di un datastore NFS utilizzando strumenti ONTAP 10

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

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



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

## Resize Datastore | NFS\_DS1

### Volume Details

Volume Name:	NFS_DS1
Total Size:	2.1 TB
Used Size:	968 KB
Snapshot Reserve (%):	5
Thin Provisioned:	Yes

### Size

Current Datastore Size:	2 TB
New Datastore Size (GB): *	3000

CANCEL

RESIZE

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

Recent Tasks		Alarms	
Task Name	Target	Status	Details
Expand Datastore	<a href="https://vcenter-vlsr.sddc.net/app.com">vcenter-vlsr.sddc.net app.com</a>	100%	Expand datastore initiated with job id 2807

### Ulteriori informazioni

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

Per ulteriori informazioni sulla configurazione dei sistemi storage ONTAP, consultare il ["Documentazione di ONTAP 10"](#) centro dati.

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

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

L'utilizzo degli strumenti ONTAP per VMware vSphere 10 e Site Replication Adapter (SRA) insieme a VMware Site Recovery Manager (SRM) apporta un valore significativo alle attività di disaster recovery. I tool ONTAP 10 offrono solide funzionalità di storage, tra cui high Availability e scalabilità native per il provider VASA, con supporto per vVol iSCSI

e NFS. Ciò garantisce la disponibilità dei dati e semplifica la gestione di più server VMware vCenter e cluster ONTAP. Utilizzando SRA con VMware Site Recovery Manager, le organizzazioni possono ottenere una replica e un failover perfetti delle macchine virtuali e dei dati tra i siti, consentendo processi di disaster recovery efficienti. La combinazione di tool ONTAP e SRA permette alle aziende di proteggere i workload critici, ridurre al minimo il downtime e mantenere la business continuity in caso di eventi imprevisti o disastri.

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

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

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

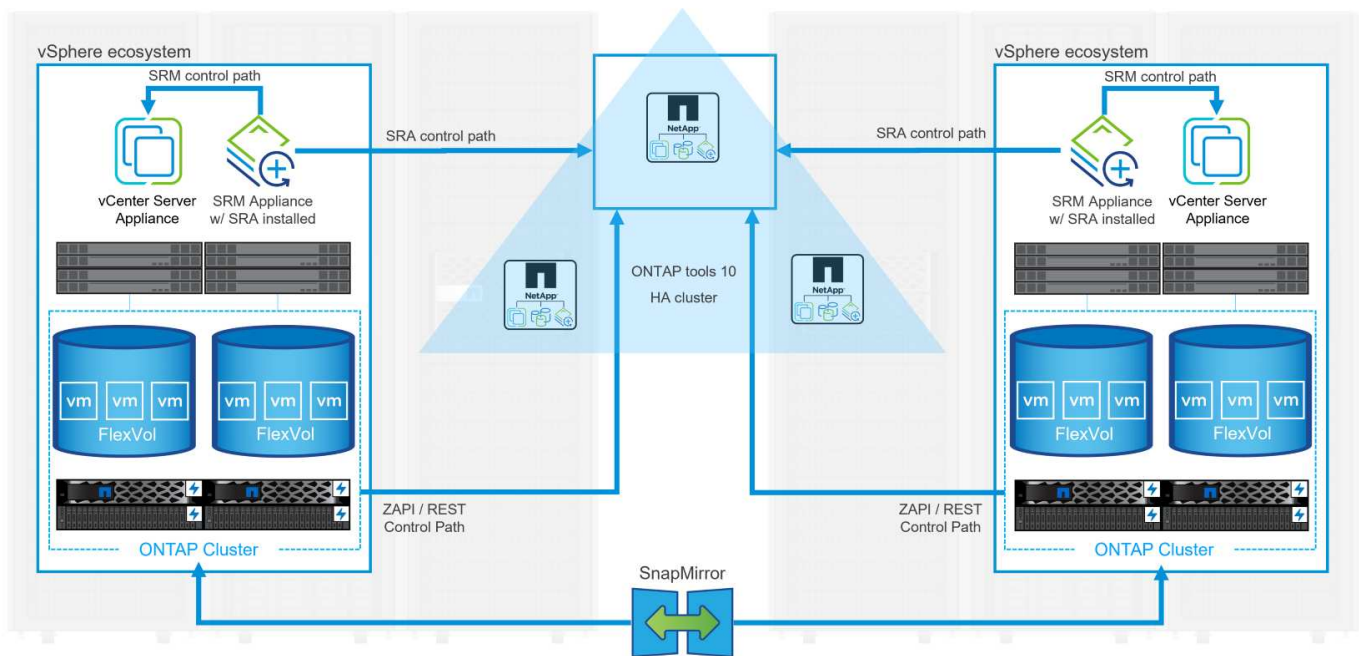
## **Panoramica dello scenario**

Questo scenario copre i seguenti passaggi di alto livello:

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

## **Architettura**

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



## Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

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

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

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

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

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

## Fasi di implementazione

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



## **Crea una relazione di SnapMirror tra i sistemi storage ONTAP**

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

Per ["QUI"](#) informazioni complete sulla creazione di relazioni di SnapMirror per ONTAP Volumes, consulta la documentazione di ONTAP.

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

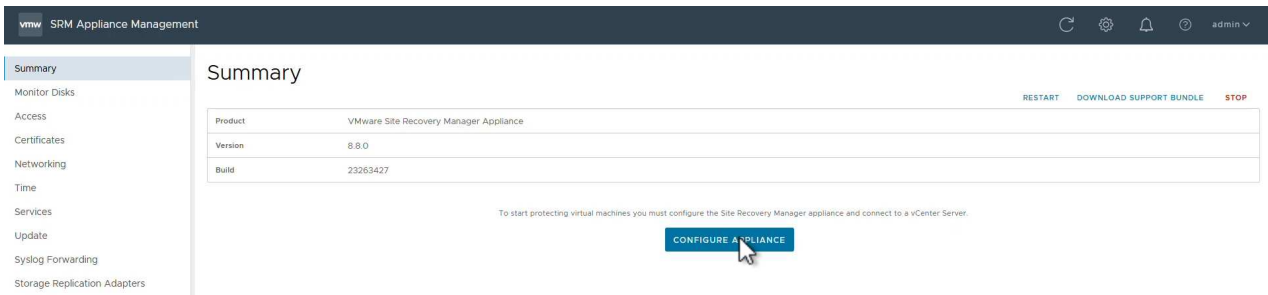
## **Configurare l'appliance SRM**

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

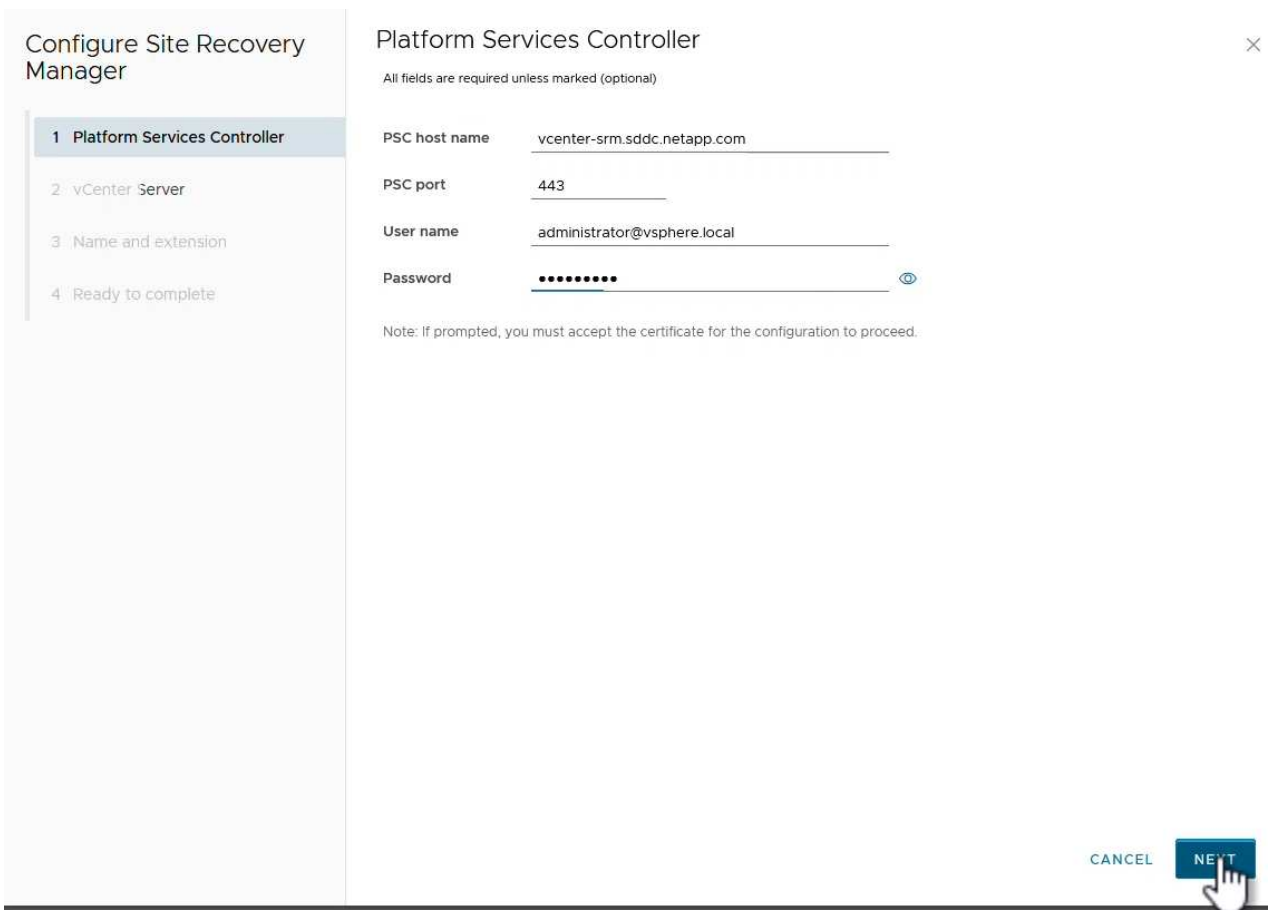
## Collegare l'appliance SRM per i siti primario e secondario

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

1. In un browser Web, [https://<SRM\\_appliance\\_IP>:5480](https://<SRM_appliance_IP>:5480) accedere a e accedere. Fare clic su **Configure Appliance** per iniziare.



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



3. Nella pagina **vCenter Server**, visualizzare il Vserver connesso e fare clic su **Avanti** per continuare.
4. Nella pagina **Nome ed estensione**, immettere un nome per il sito SRM, un indirizzo e-mail degli

amministratori e l'host locale che verrà utilizzato da SRM. Fare clic su **Avanti** per continuare.

### Configure Site Recovery Manager

- 1 Platform Services Controller
- 2 vCenter Server
- 3 Name and extension**
- 4 Ready to complete

#### Name and extension

All fields are required unless marked (optional)

Enter name and extension for Site Recovery Manager

**Site name**   
A unique display name for this Site Recovery Manager site.

**Administrator email**   
An email address to use for system notifications.

**Local host**  ▼  
The address on the local host to be used by Site Recovery Manager.

**Extension ID**  
 Default extension ID (com.vmware.vcDr)  
 Custom extension ID  
The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair.

Extension ID

Organization

Description

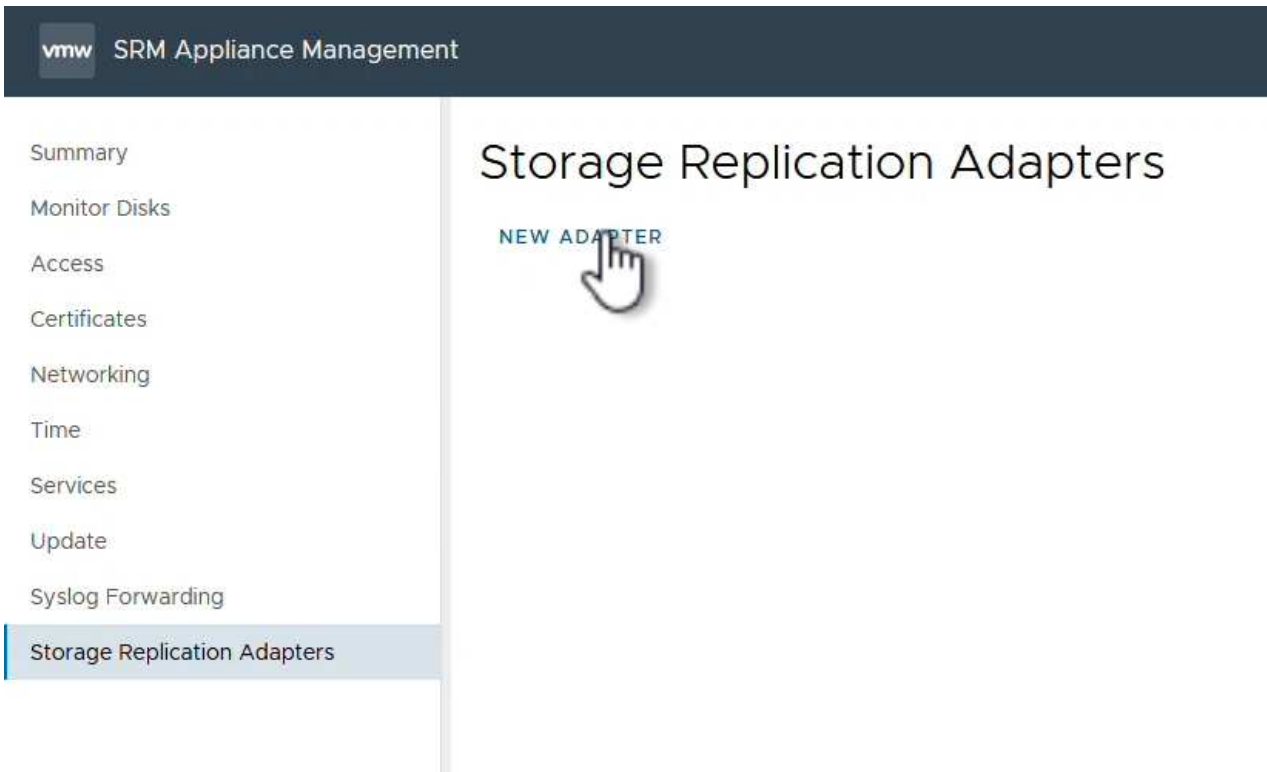
[CANCEL](#) [BACK](#) [NEXT](#)

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

## Configurare SRA sull'appliance SRM

Completare i seguenti passaggi per configurare SRA sul dispositivo SRM:

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



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

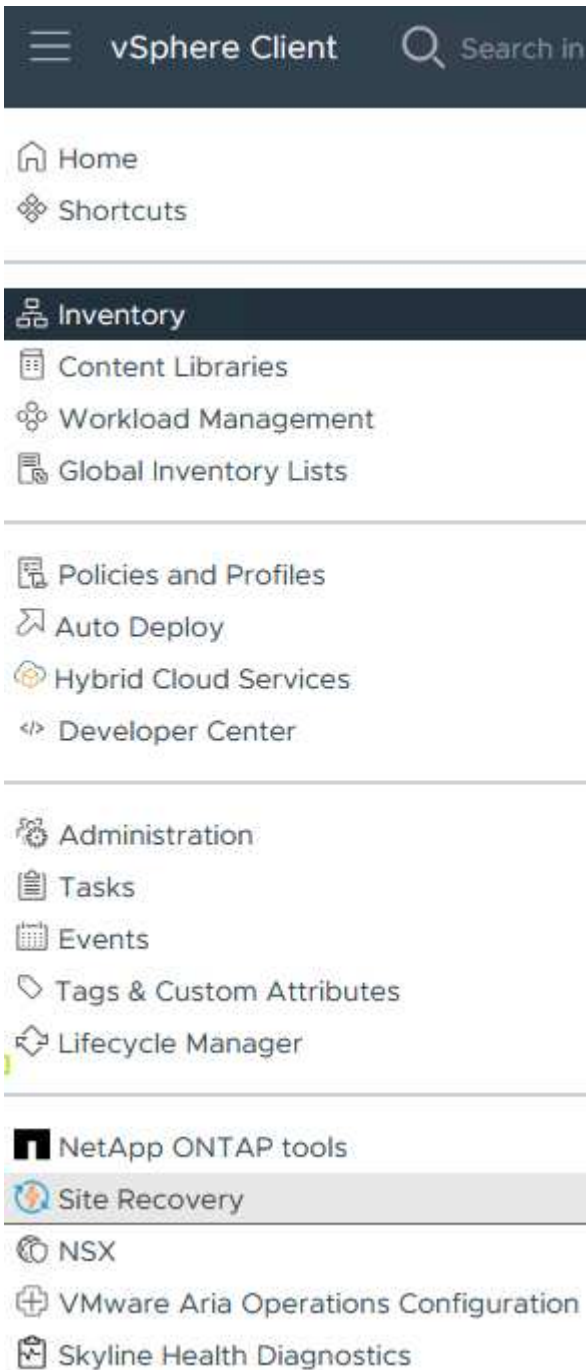
## Configurare Site Recovery per SRM

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

## Configurare l'associazione del sito per SRM

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

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



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

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

[NEW SITE PAIR](#)[Learn More](#)

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

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Pair type

Select a local vCenter Server:

vCenter Server

vcenter-vlsr.sddc.netapp.com

Pair type

Pair with a peer vCenter Server located in a different SSO domain

Pair with a peer vCenter Server located in the same SSO domain

CANCEL NEXT

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

## New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

## Peer vCenter Server



All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name

PSC port

User name

Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

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

## New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

## Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

Service	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
<input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

CANCEL

BACK

NEXT

6. Nella pagina **Pronto per il completamento**, esaminare la configurazione proposta e quindi fare clic sul pulsante **fine** per creare l'associazione del sito

7. La nuova coppia di siti e il relativo riepilogo possono essere visualizzati nella pagina Riepilogo.

### Summary

RECONNECT

BREAK SITE PAIR



vCenter Server: [vcenter-vlsr.sddc.netapp.com](#) [vcenter-srm.sddc.netapp.com](#)  
vCenter Version: 8.0.2, 22385739 8.0.2, 22385739  
vCenter Host Name: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443  
Platform Services Controller: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443

### Site Recovery Manager

EXPORT/IMPORT SRM CONFIGURATION

Protection Groups:0 Recovery Plans:0

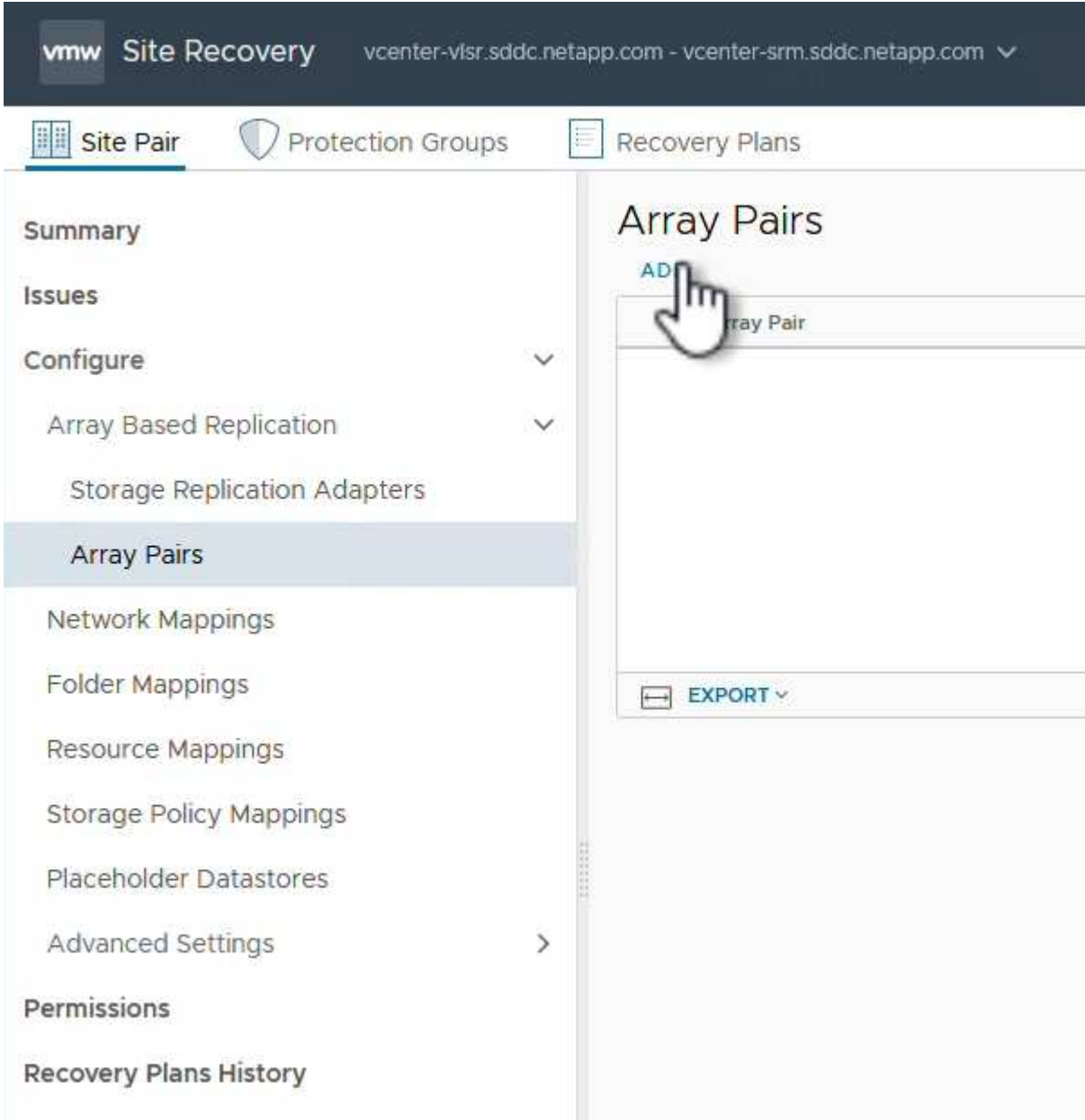
Name	Site 1 <a href="#">RENAME</a>	Site 2 <a href="#">RENAME</a>
Server	srm-site1.sddc.netapp.com:443 <a href="#">ACTIONS</a>	srm-site2.sddc.netapp.com:443 <a href="#">ACTIONS</a>
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected



## Aggiungere una coppia di array per SRM

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

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



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

## Add Array Pair

### 1 Storage replication adapter

- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

## Storage replication adapter

Select a storage replication adapter (SRA):

	Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
>	NetApp Storage Replication Ada...	OK	NetApp	10.1	Not Support...

Items per page: AUTO 1 items

CANCEL

NEXT

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

## Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

## Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com":

### Storage Array Parameters

Storage System connection parameters

**Storage Management IP Address or Hostname**   
Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

**NFS Hostnames or IP Addresses**   
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

**Storage Virtual Machine(SVM) Name**   
Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

**Volume include list**   
Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

**Volume exclude list**   
Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

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

## Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

## Remote array manager



Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com":

Array\_2

### Storage Array Parameters

Storage System connection parameters

**Storage Management IP Address or Hostname**

ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

**NFS Hostnames or IP Addresses**

172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

**Storage Virtual Machine(SVM) Name**

SRM\_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

**Volume include list**

|

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

**Volume exclude list**

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT



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

## Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs**
- 5 Ready to complete

## Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
<input checked="" type="checkbox"/>	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

1 1 items

CANCEL

BACK

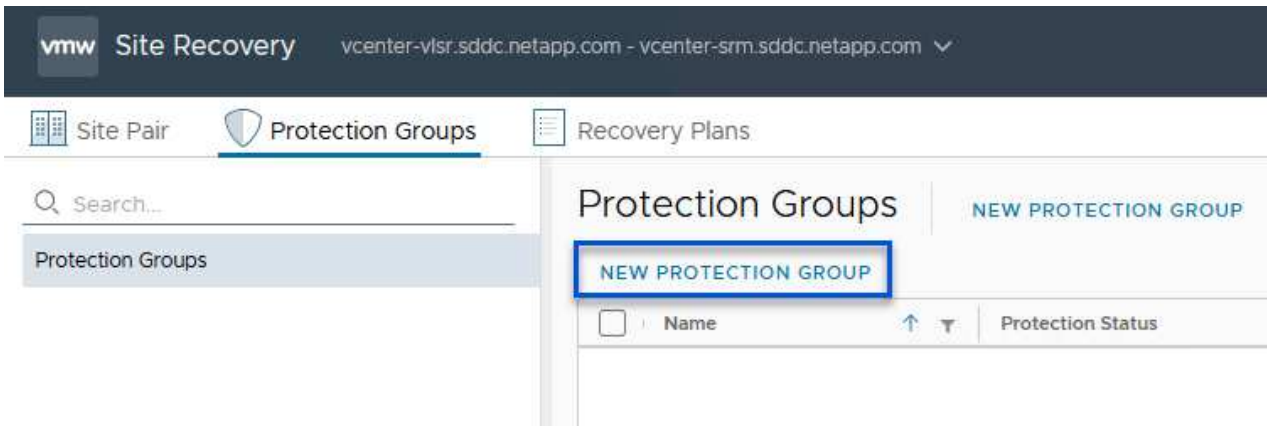
NEXT

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

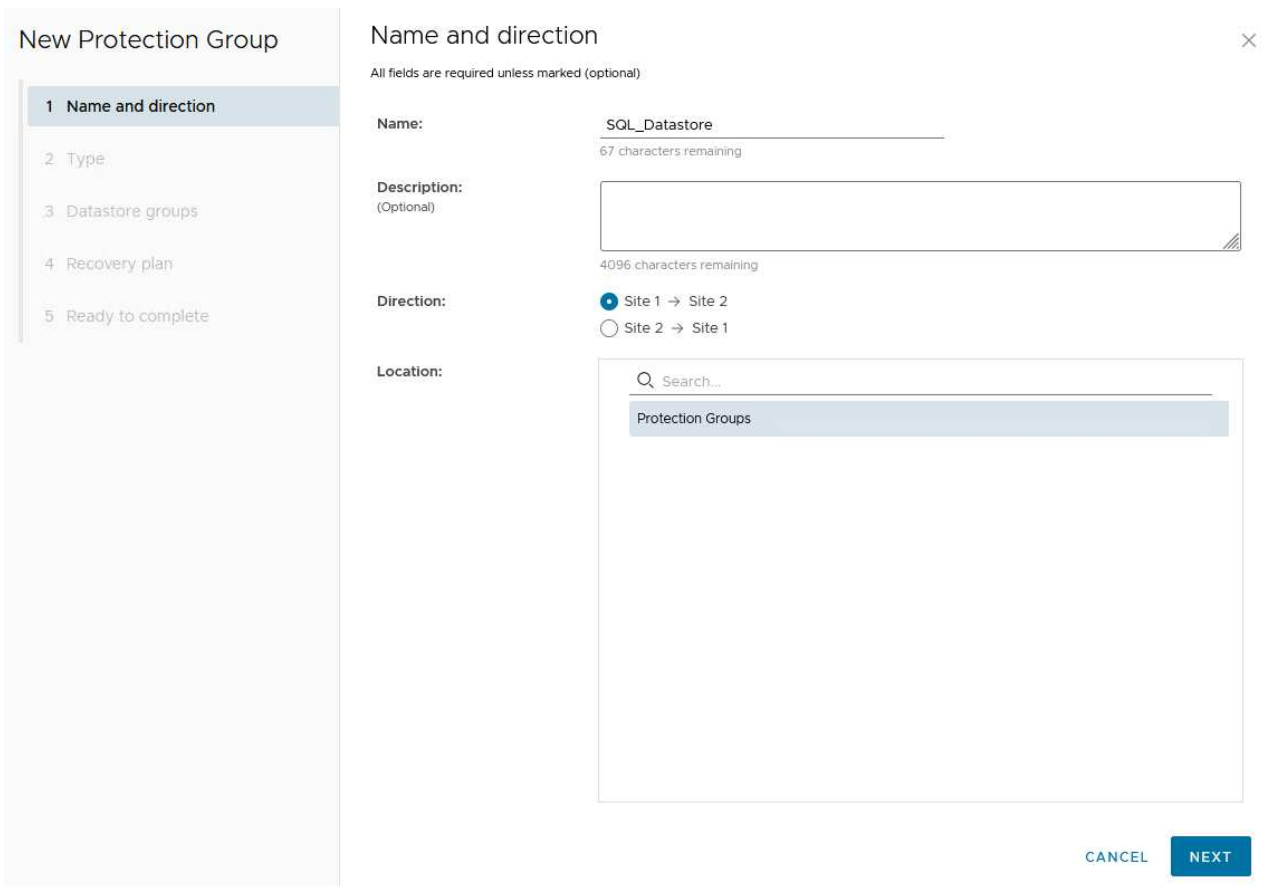
## Configurare i gruppi di protezione per SRM

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

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



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

The screenshot shows the 'New Protection Group' wizard. On the left, there's a sidebar with five steps: '1 Name and direction', '2 Type', '3 Datastore groups', '4 Recovery plan', and '5 Ready to complete'. The '1 Name and direction' step is selected. The main area is titled 'Name and direction' and contains the following fields:

- Name:** 'SQL\_Datastore' (67 characters remaining)
- Description:** (Optional) (4096 characters remaining)
- Direction:** Radio buttons for 'Site 1 -> Site 2' (selected) and 'Site 2 -> Site 1'.
- Location:** A search bar with 'Protection Groups' selected in the dropdown.

At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

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

**New Protection Group**

- 1 Name and direction
- 2 Type**
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

**Type**

Select the type of protection group you want to create:

- Datastore groups (array-based replication)**  
Protect all virtual machines which are on specific datastores.
- Individual VMs (vSphere Replication)  
Protect specific virtual machines, regardless of the datastores.
- Virtual Volumes (vVol replication)  
Protect virtual machines which are on replicated vVol storage.

Select array pair

Array Pair	Array Manager Pair
<input checked="" type="radio"/> ✓ ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> ✓ ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page: AUTO 2 array pairs

**CANCEL** **BACK** **NEXT**

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

## New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups**
- 4 Recovery plan
- 5 Ready to complete

## Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together.

[SELECT ALL](#) [CLEAR SELECTION](#)

<input checked="" type="checkbox"/>	Datastore Group	Status
<input checked="" type="checkbox"/>	NFS_DS1	Add to this protection group

1 Items per page: [AUTO](#) 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
SQLSRV-01	NFS_DS1	Add to this protection group
SQLSRV-03	NFS_DS1	Add to this protection group
SQLSRV-02	NFS_DS1	Add to this protection group

[CANCEL](#) [BACK](#) [NEXT](#)

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



## New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

## Recovery plan



You can optionally add this protection group to a recovery plan.

- Add to existing recovery plan
- Add to new recovery plan
- Do not add to recovery plan now

 The protection group cannot be recovered unless it is added to a recovery plan.

CANCEL

BACK

NEXT

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

## New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete**

## Ready to complete



Review your selected settings.

<b>Name</b>	SQL_Datastore
<b>Description</b>	
<b>Protected site</b>	Site 1
<b>Recovery site</b>	Site 2
<b>Location</b>	Protection Groups
<b>Protection group type</b>	Datastore groups (array-based replication)
<b>Array pair</b>	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2)
<b>Datastore groups</b>	NFS_DS1
<b>Total virtual machines</b>	3
<b>Recovery plan</b>	none

CANCEL

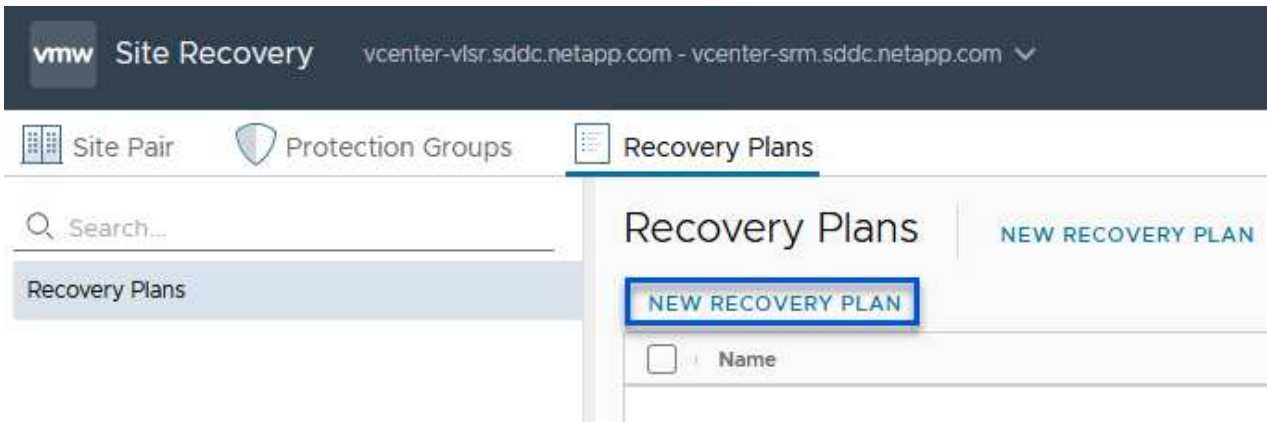
BACK

FINISH

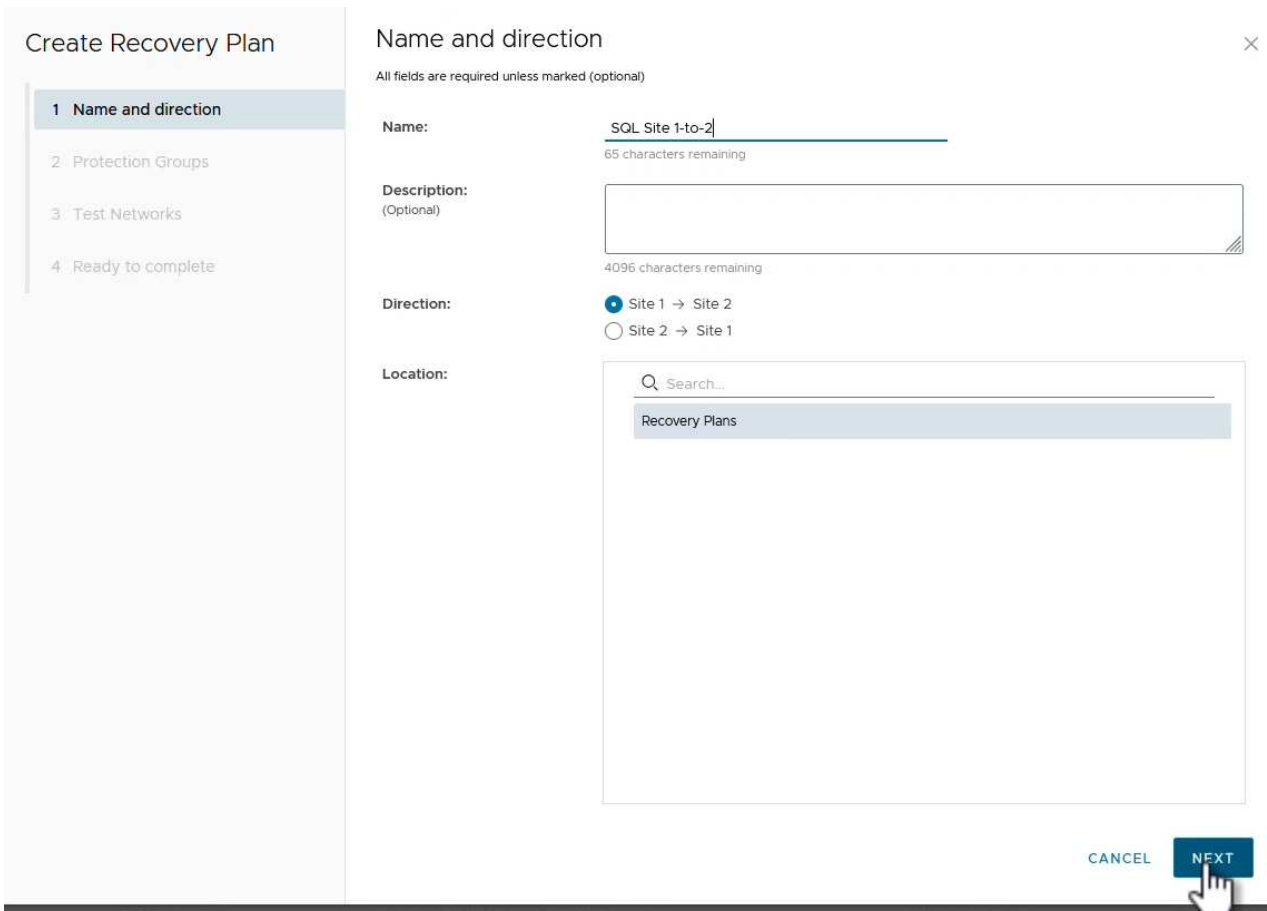
## Configurare il piano di ripristino per SRM

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

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



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



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

The screenshot shows the 'Create Recovery Plan' wizard in step 2, 'Protection Groups'. On the left, a sidebar lists the steps: 1. Name and direction, 2. Protection Groups (highlighted), 3. Test Networks, and 4. Ready to complete. The main area is titled 'Protection Groups' and shows a table with columns 'Name' and 'Description'. A single row is visible, 'SQL\_Datastore', with a checkmark in the selection column. Below the table, there are controls for 'Items per page' (set to 'AUTO') and '1 group(s)'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking the 'NEXT' button.

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

### Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups
- 3 Test Networks
- 4 Ready to complete

### Test Networks ×

Select the networks to use while running tests of this plan.

i If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	↑ ↓	Test Network	
<span style="font-size: 0.8em;">Datacenter &gt; DPortGroup</span>	☰	<span style="font-size: 0.8em;">Use site-level mapping</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; Mgmt 3376</span>	☰	<span style="font-size: 0.8em;">Mgmt 3376</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; NFS 3374</span>	☰	<span style="font-size: 0.8em;">NFS 3374</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; VLAN 181</span>	☰	<span style="font-size: 0.8em;">Use site-level mapping</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; VM Network</span>	☰	<span style="font-size: 0.8em;">Use site-level mapping</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; vMotion 3373</span>	☰	<span style="font-size: 0.8em;">Use site-level mapping</span>	<span style="font-size: 0.8em;">CHANGE</span>
<span style="font-size: 0.8em;">Datacenter &gt; vSAN 3422</span>	☰	<span style="font-size: 0.8em;">Use site-level mapping</span>	<span style="font-size: 0.8em;">CHANGE</span>

7 network(s)

CANCEL
BACK
NEXT

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

## Operazioni di disaster recovery con SRM

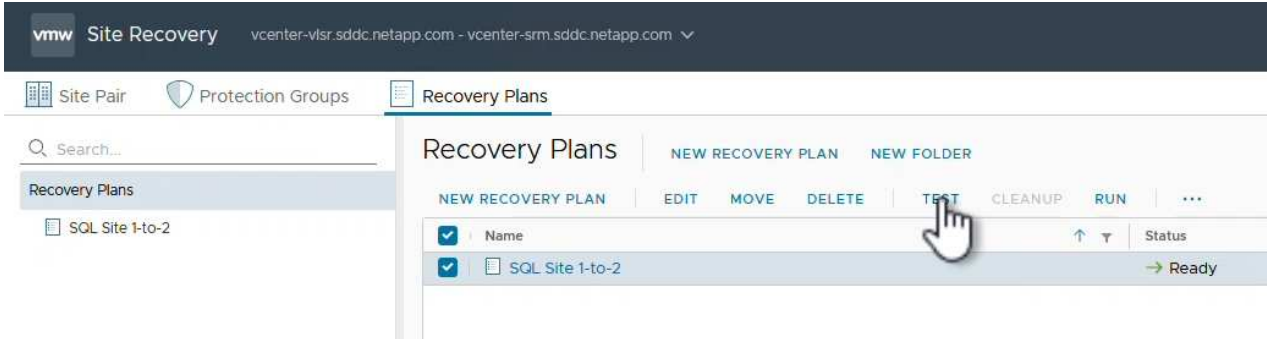
In questa sezione verranno trattate varie funzioni dell'utilizzo del disaster recovery con SRM, tra cui il test del failover, l'esecuzione del failover, la riprotezione e il failback.

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

## Verifica del failover con SRM

Il passaggio seguente viene completato nell'interfaccia Site Recovery.

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

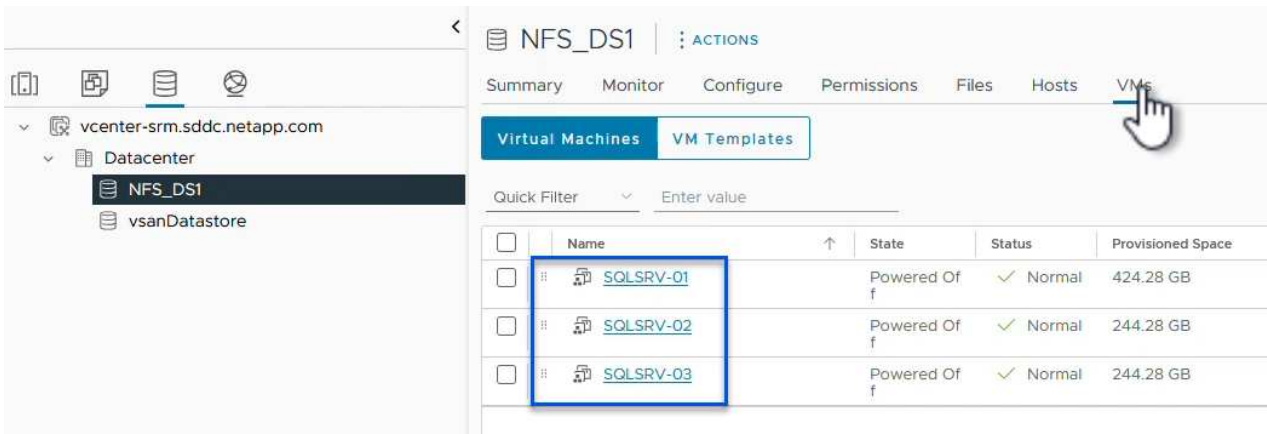


2. È possibile visualizzare l'avanzamento del test dal riquadro attività di Site Recovery e dal riquadro attività di vCenter.

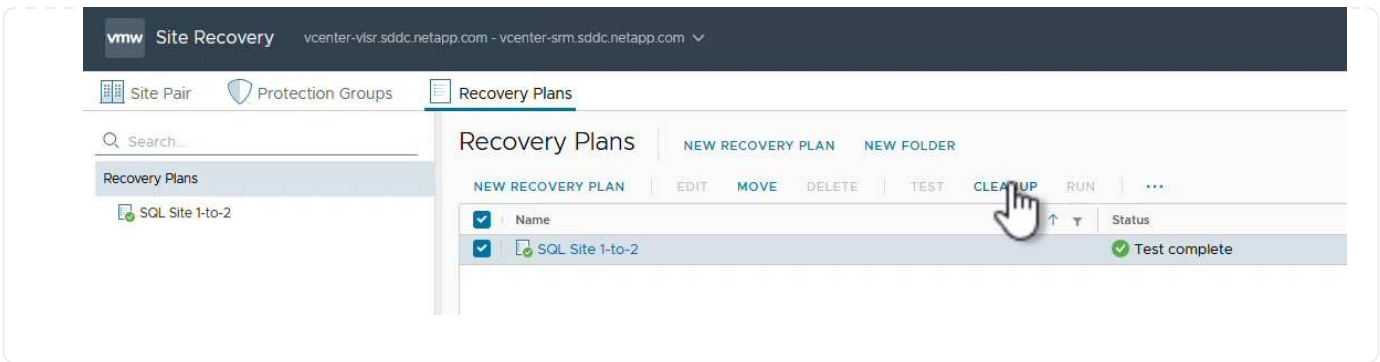
The screenshot shows the 'Recent Tasks' window in vCenter. It displays a table of tasks with columns for Task Name, Target, Status, Initiator, and Queued For. The 'Test Recovery Plan' task is highlighted, showing a progress bar at 6%.

Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERELOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	Completed	VSPHERELOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	Completed	VSPHERELOCAL\SRM-d1369bbb-62c6...	4 ms
Set virtual machine custom value	SQLSRV-01	Completed	VSPHERELOCAL\SRM-d1369bbb-62c6...	3 ms

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



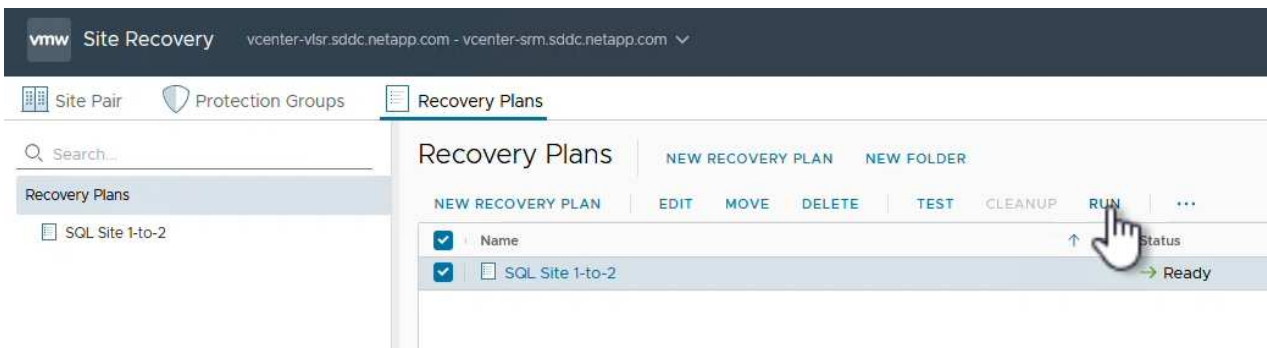
4. Una volta completato il test, fare clic su **Cleanup** per disinstallare il datastore e tornare all'ambiente originale.



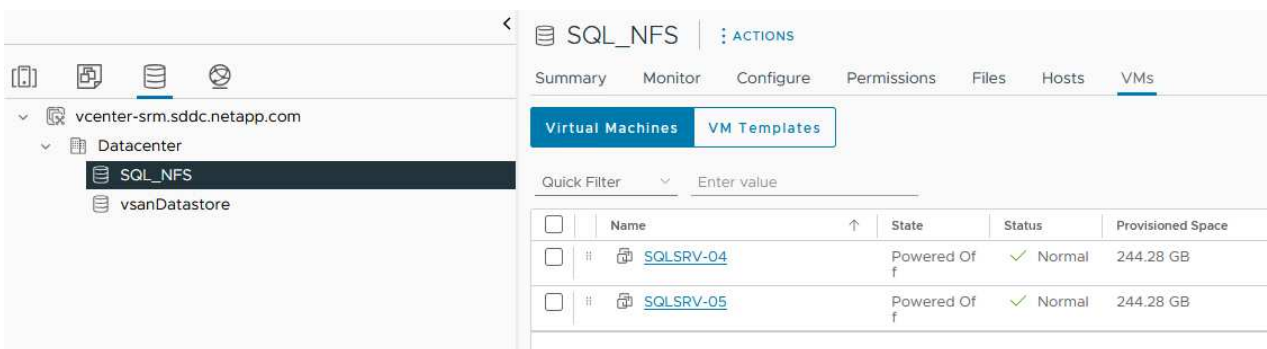
## Esecuzione di un piano di ripristino con SRM

Eeguire un ripristino completo e il failover sul sito secondario.

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



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



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

**Reprotezione:** Una volta completato il processo di ripristino, il sito di ripristino precedentemente designato assume il ruolo del nuovo sito di produzione. Tuttavia, è importante notare che la replica di SnapMirror viene interrotta durante l'operazione di ripristino, lasciando il nuovo sito di produzione vulnerabile a futuri disastri. Per garantire una protezione continua, si consiglia di stabilire una nuova protezione per il nuovo sito di produzione replicandolo in un altro sito. Nei casi in cui il sito di produzione originale rimane operativo, l'amministratore

VMware può riutilizzarlo come nuovo sito di ripristino, invertendo effettivamente la direzione della protezione. È fondamentale sottolineare che la ri-protezione è possibile solo in caso di guasti non catastrofici, che richiedono l'eventuale recuperabilità dei server vCenter originali, dei server ESXi, dei server SRM e dei rispettivi database. Se questi componenti non sono disponibili, diventa necessaria la creazione di un nuovo gruppo di protezione e di un nuovo piano di ripristino.

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

## Ulteriori informazioni

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

Per informazioni sulla configurazione dei sistemi storage ONTAP, consultare la ["Documentazione di ONTAP 9"](#) centro.

Per informazioni sulla configurazione di VCF, fare riferimento a ["Documentazione di VMware Cloud Foundation"](#).

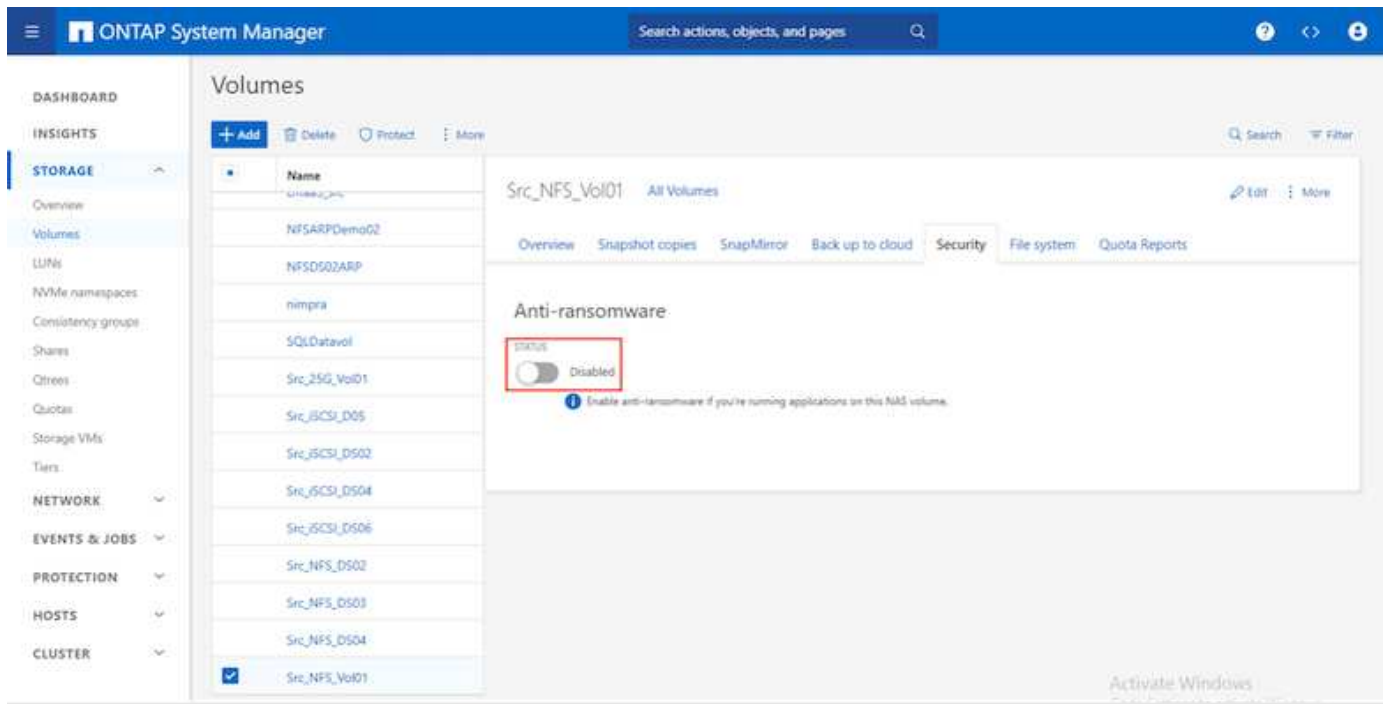
# Protezione autonoma dal ransomware per lo storage NFS

## Protezione autonoma dal ransomware per lo storage NFS

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

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



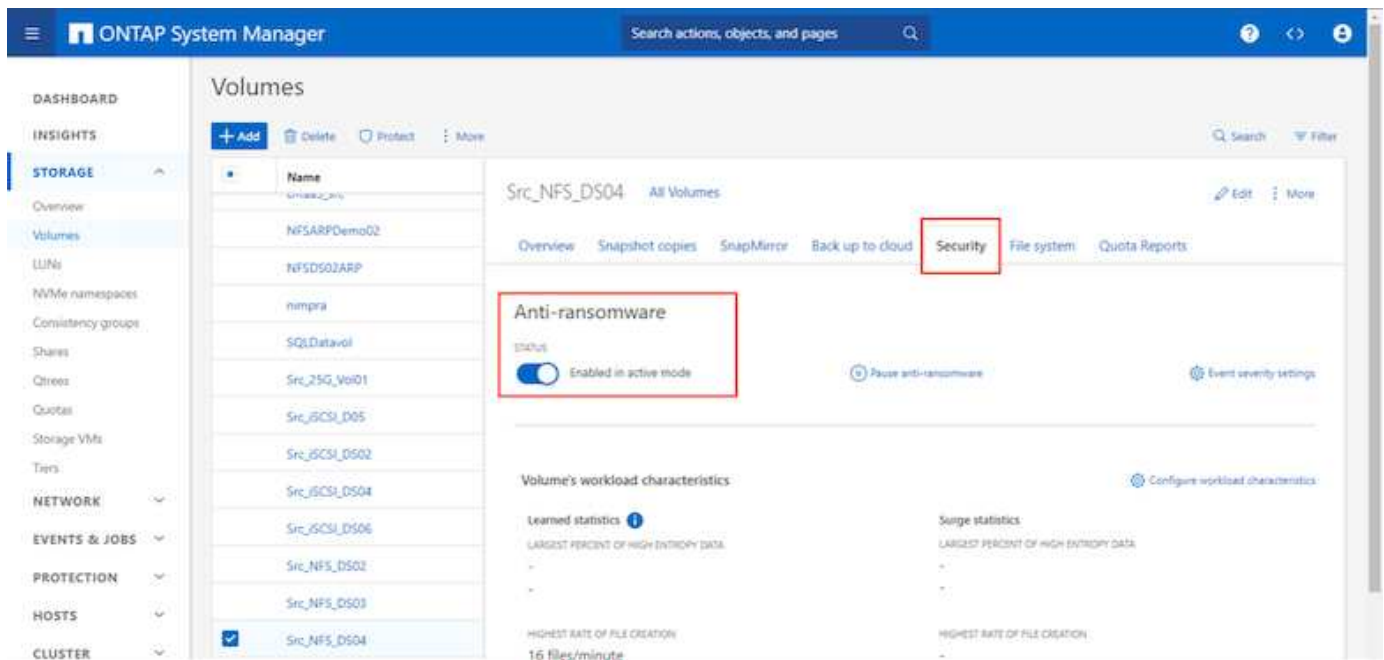


Con il nuovo NetApp ARP/ai, che è attualmente in anteprima tecnologica, non c'è bisogno di una modalità di apprendimento. Invece, può passare direttamente alla modalità attiva con la sua funzionalità di rilevamento ransomware basata su ai.



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

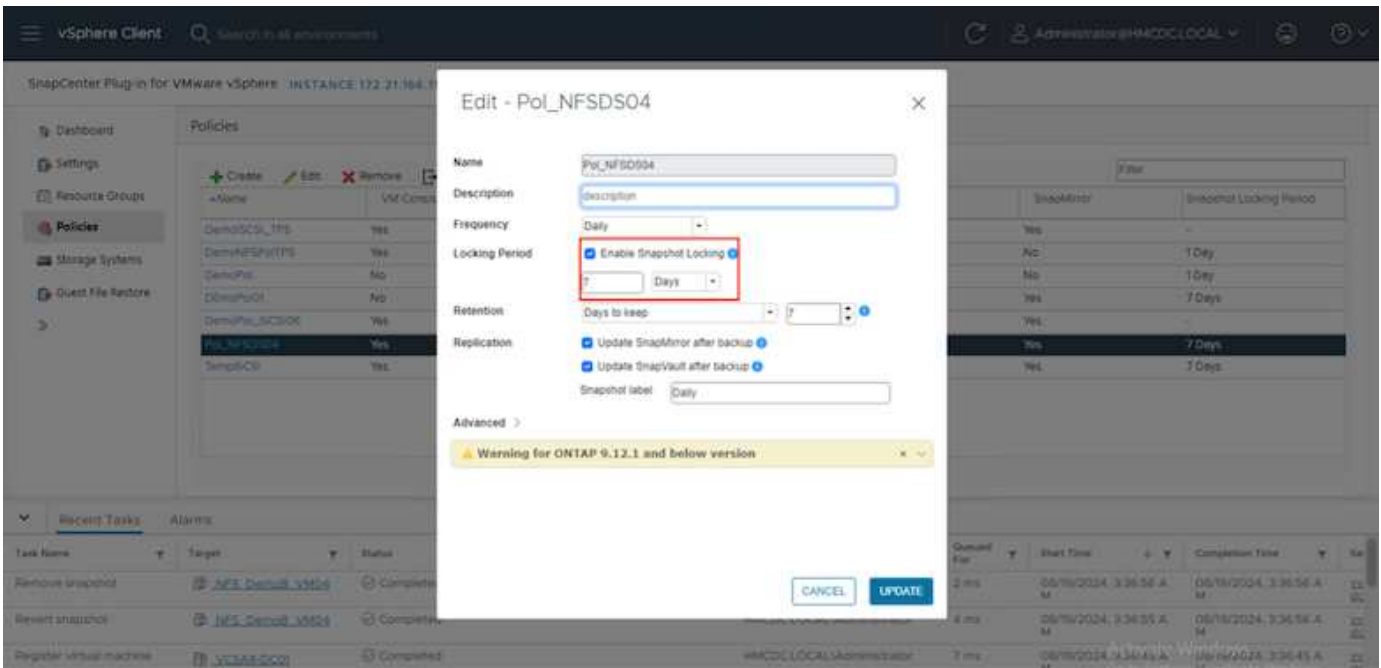
Una volta in modalità attiva, inizia a cercare l'attività anomala del volume che potrebbe essere un ransomware. Se viene rilevata un'attività anomala, viene immediatamente creata una copia Snapshot automatica che fornisce un punto di ripristino il più vicino possibile all'infezione dei file. ARP è in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



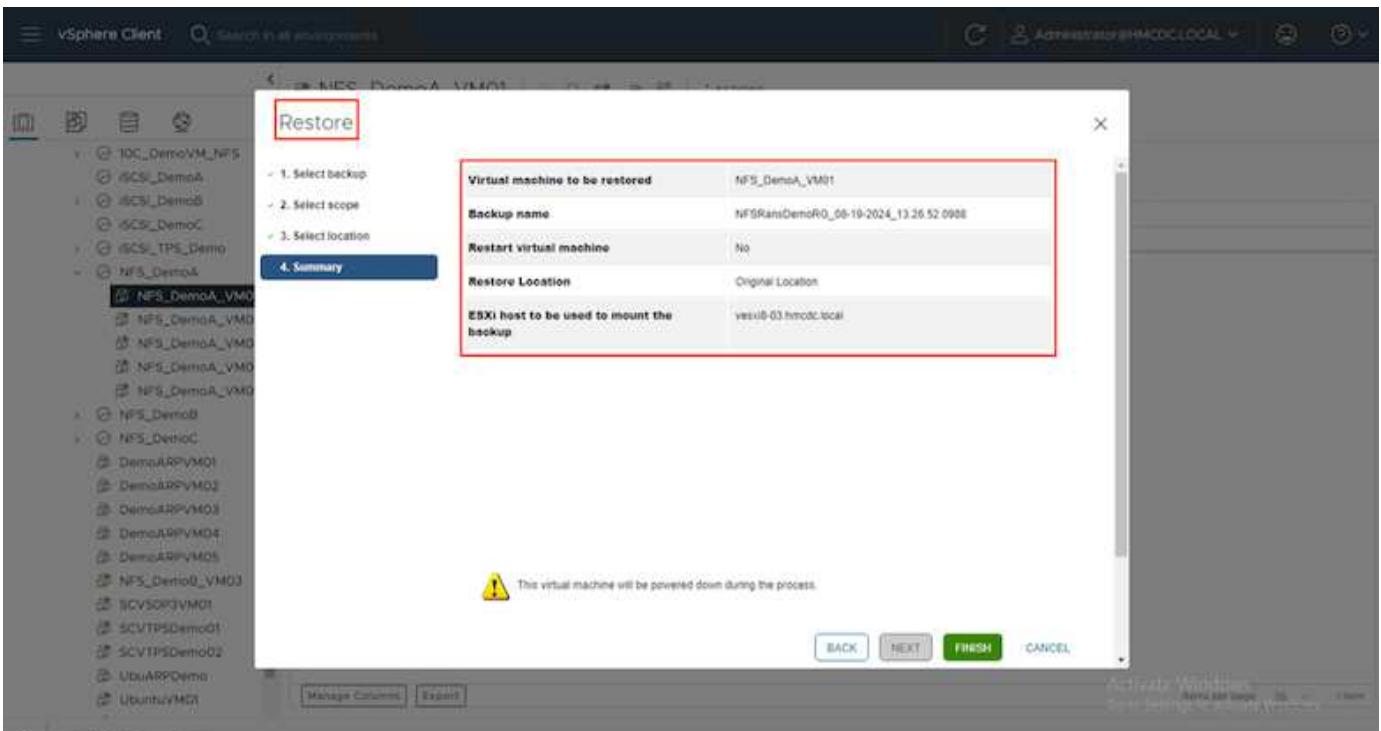
Se un attacco ransomware riguarda la macchina virtuale (VM) e altera i file all'interno della macchina virtuale senza apportare modifiche all'esterno della macchina virtuale, l'Advanced ransomware Protection (ARP) rileverà comunque la minaccia se l'entropia predefinita della macchina virtuale è bassa,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

Per informazioni dettagliate, fare riferimento alla sezione "ARP e macchine virtuali" nel ["ARP usecases e considerazioni"](#).

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



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



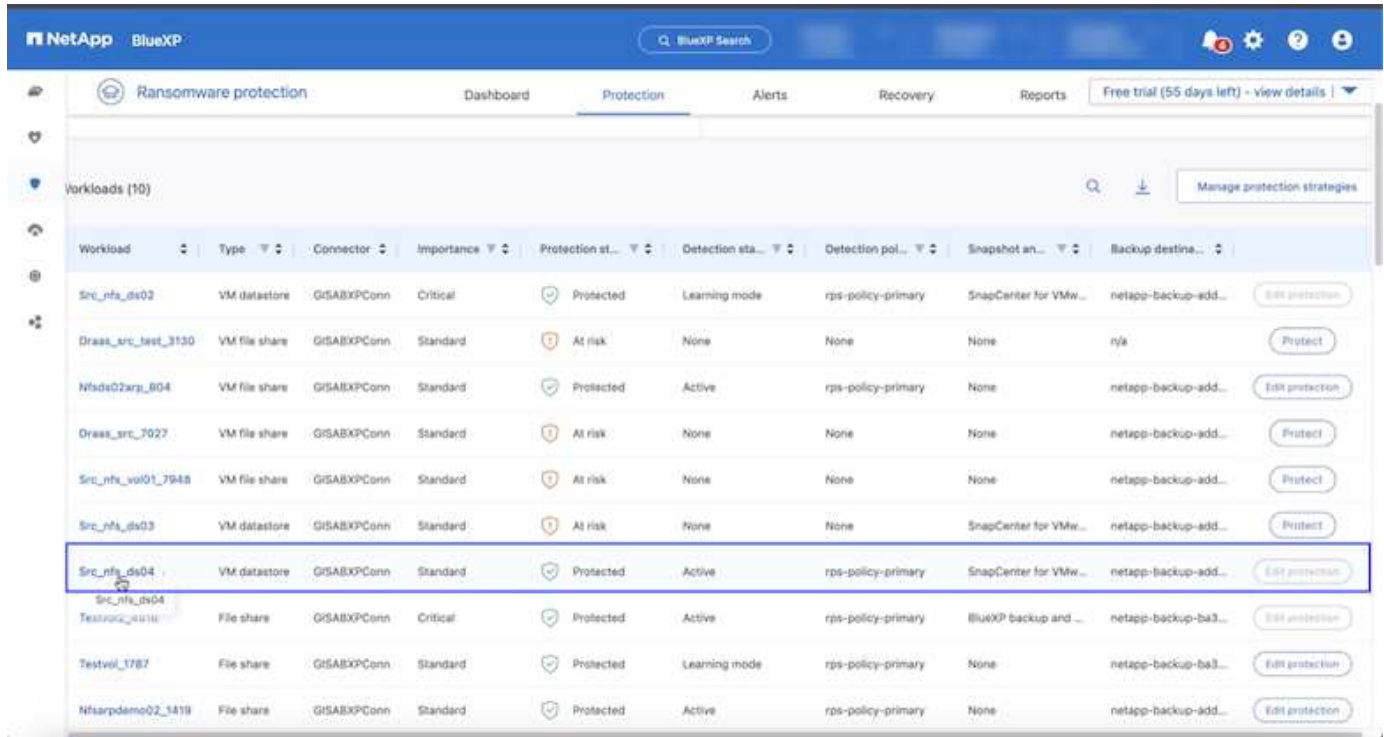
Quanto sopra dimostra in che modo lo storage ONTAP aggiunge un ulteriore livello alle tecniche esistenti, migliorando la predisposizione per il futuro dell'ambiente.

Per ulteriori informazioni, visualizzare le istruzioni per ["Soluzioni NetApp per il ransomware"](#).

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

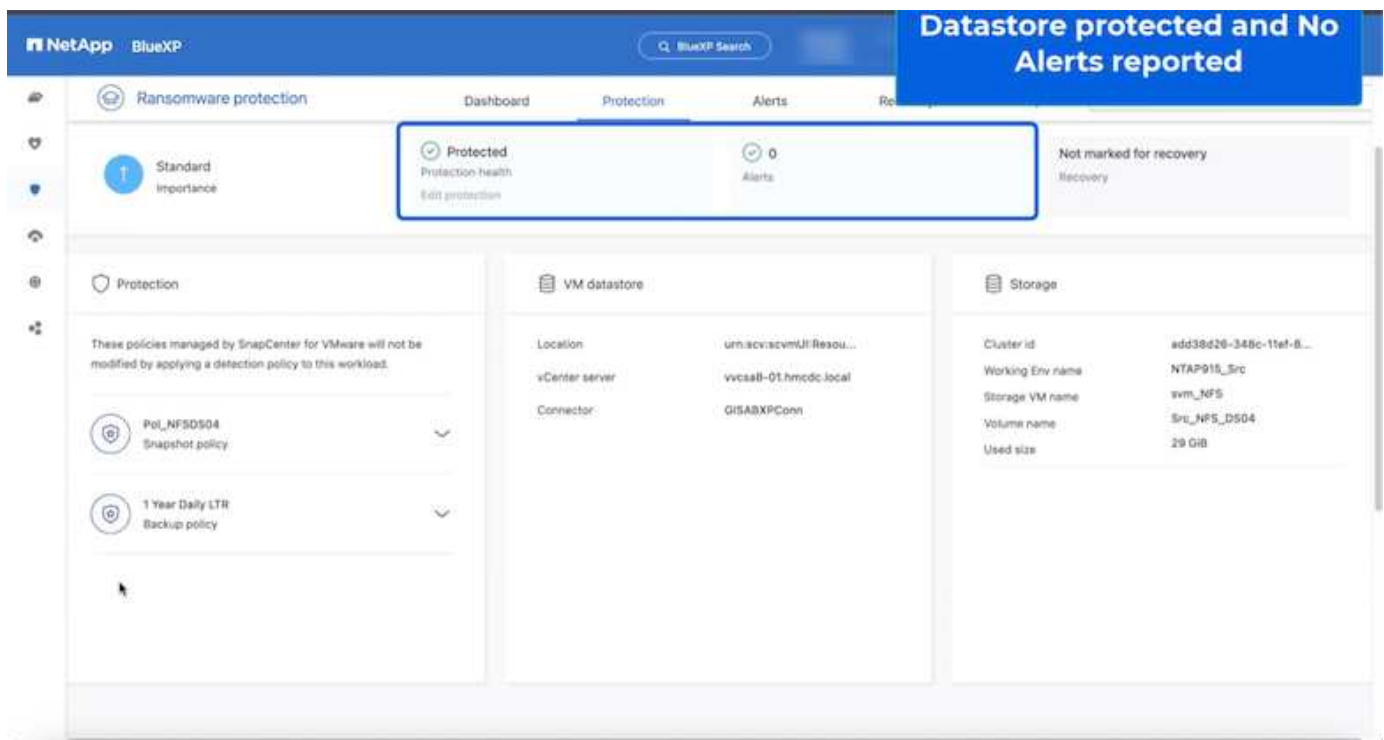
ransomware. Questo servizio offre protezione per i workload basati sulle applicazioni come Oracle, MySQL, datastore VM e file share sullo storage NFS on-premise.

In questo esempio, il datastore NFS "Src\_NFS\_DS04" è protetto tramite la protezione ransomware BlueXP .



The screenshot shows the NetApp BlueXP Ransomware protection dashboard. The 'Workloads (10)' section contains a table with the following data:

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02arp_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vol01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_3419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection



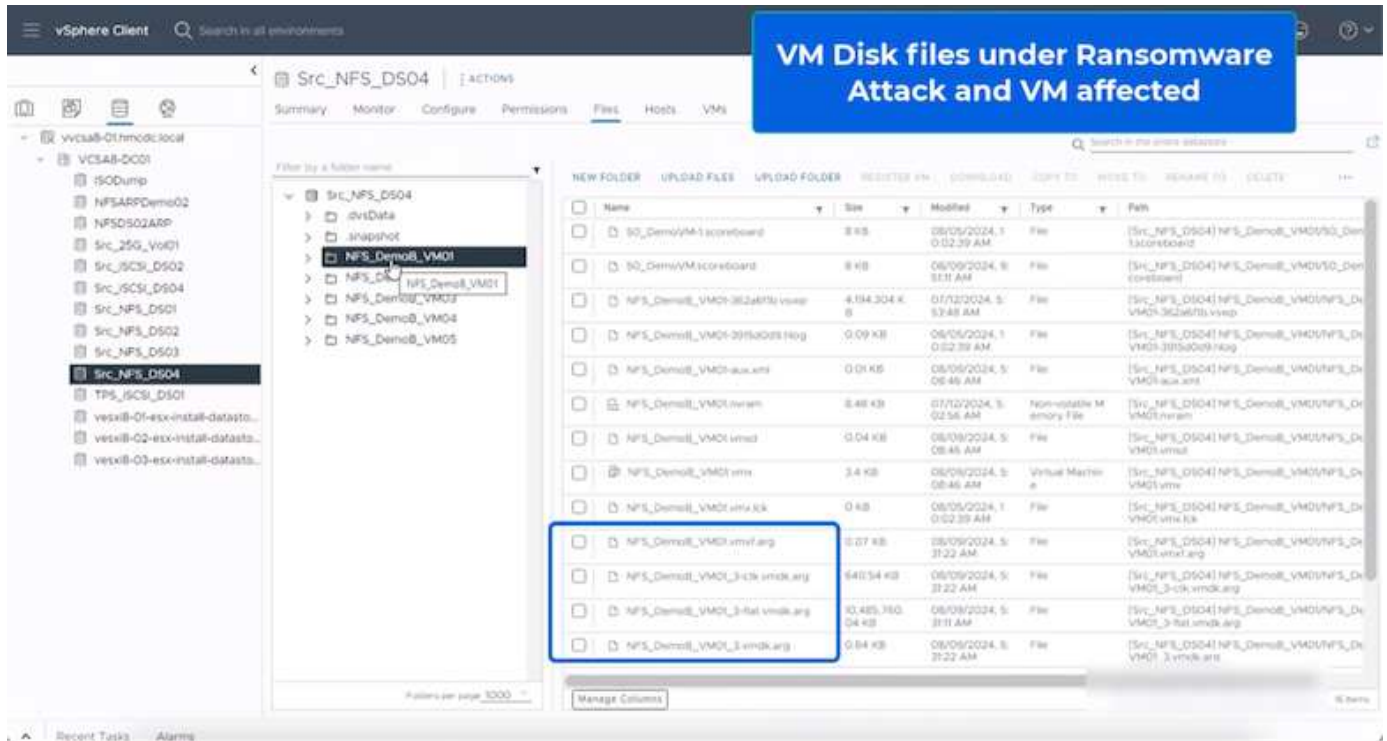
The screenshot shows the NetApp BlueXP Ransomware protection dashboard with a blue banner at the top right that reads "Datastore protected and No Alerts reported". The dashboard displays the following information:

- Standard Importance**: A blue circle with an upward arrow.
- Protected**: A green checkmark icon with the text "Protected Protection health" and "Alerts 0".
- Not marked for recovery**: A grey box with the text "Not marked for recovery Recovery".
- Protection**: A section titled "These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload." containing two policies: "Pol\_NFS0504 Snapshot policy" and "1 Year Daily LTR Backup policy".
- VM datastore**: A section with the following details:
  - Location: urn:scv:scvmUI:Resou...
  - vCenter server: vvcas8-01.hmcdc.local
  - Connector: GISABXPConn
- Storage**: A section with the following details:
  - Cluster id: add38d26-348c-11ef-8...
  - Working Env name: NTAP915\_Src
  - Storage VM name: svm\_nfs
  - Volume name: Src\_NFS\_DS04
  - Used size: 29 GiB

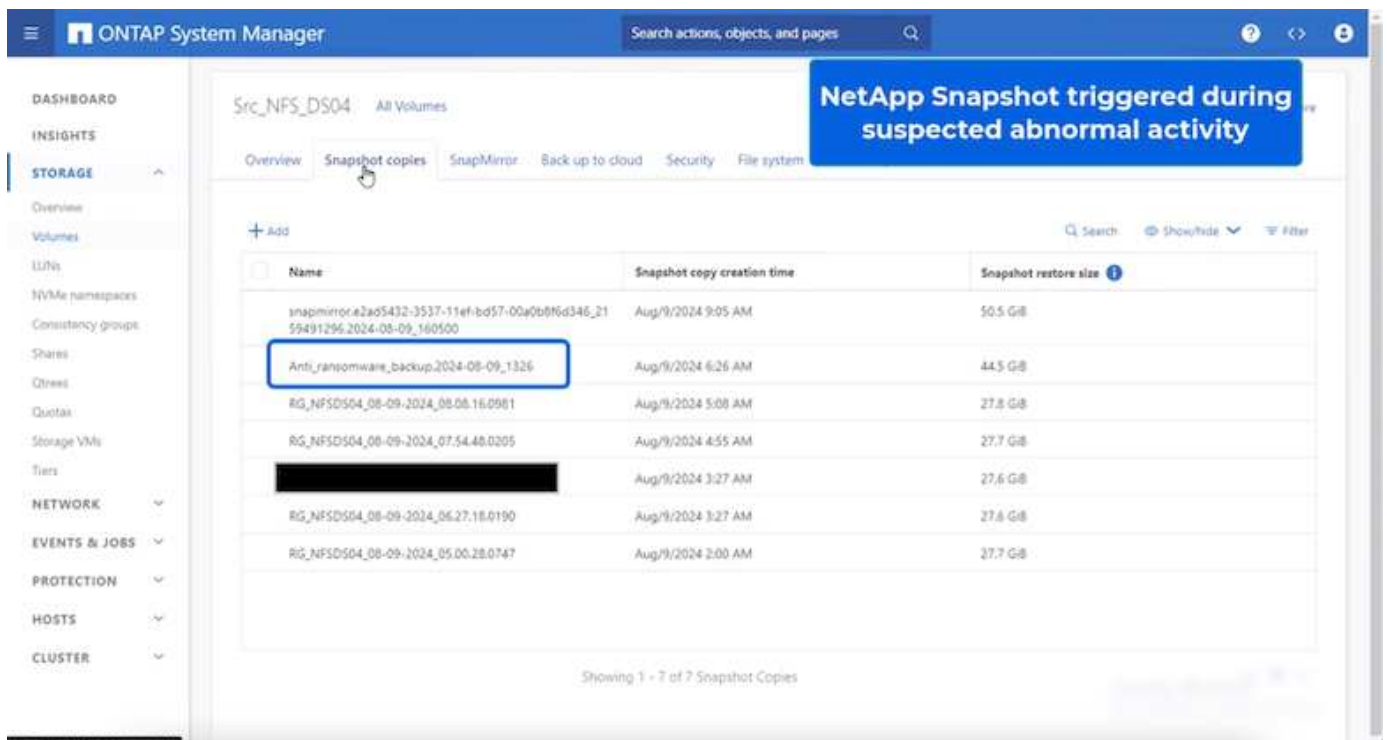
Per informazioni dettagliate sulla configurazione della protezione ransomware BlueXP , fare riferimento a "Imposta la protezione dal ransomware BlueXP " e "Configurare le impostazioni di protezione dal ransomware BlueXP".

È giunto il momento di descrivere questo concetto con un esempio. In questa procedura dettagliata, il

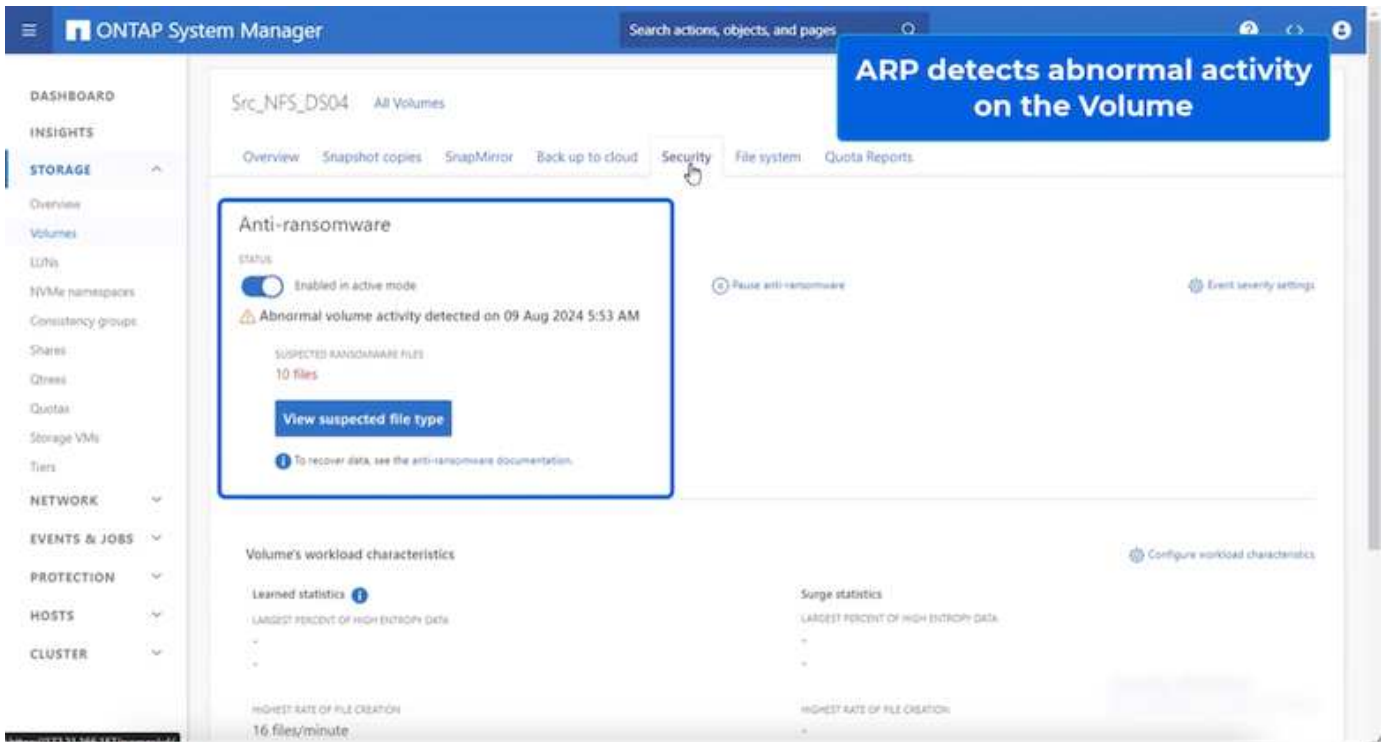
datastore "Src\_NFS\_DS04" è interessato.



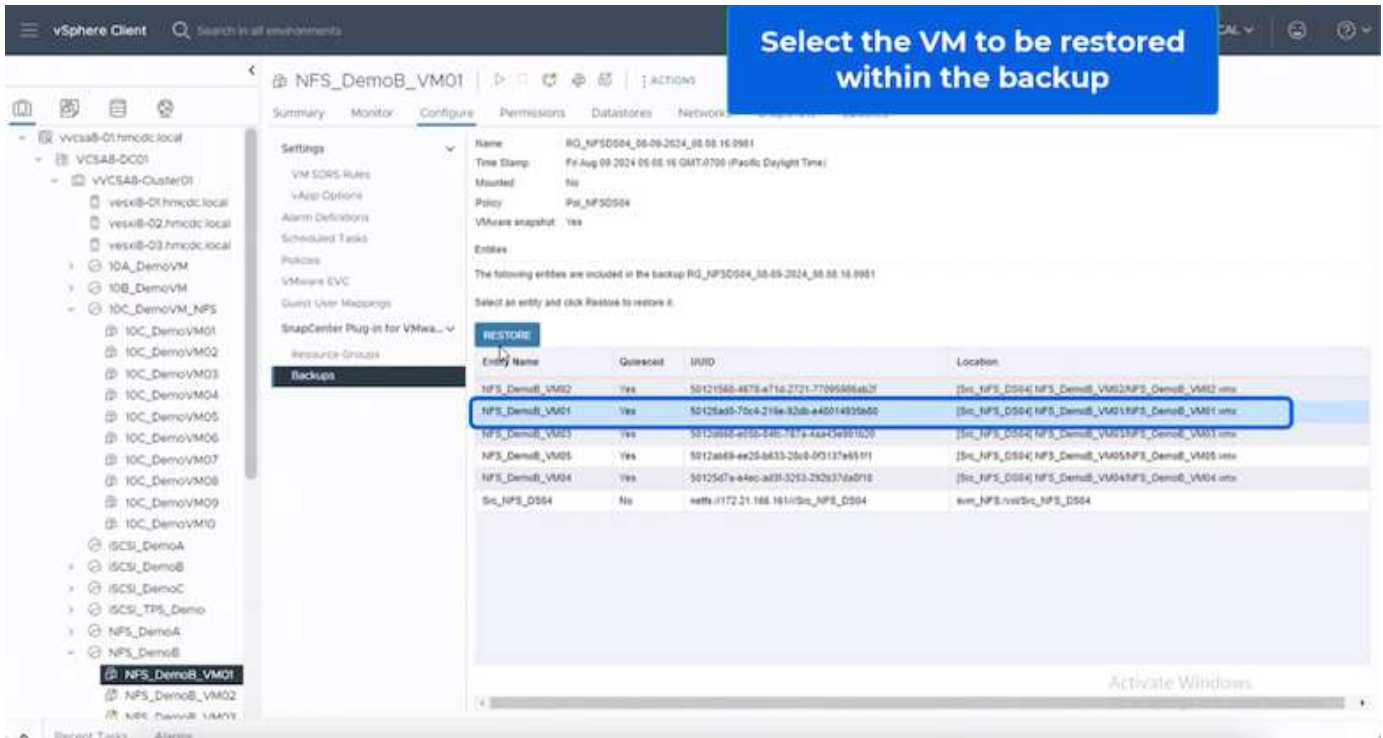
ARP ha immediatamente attivato uno snapshot sul volume al momento del rilevamento.







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

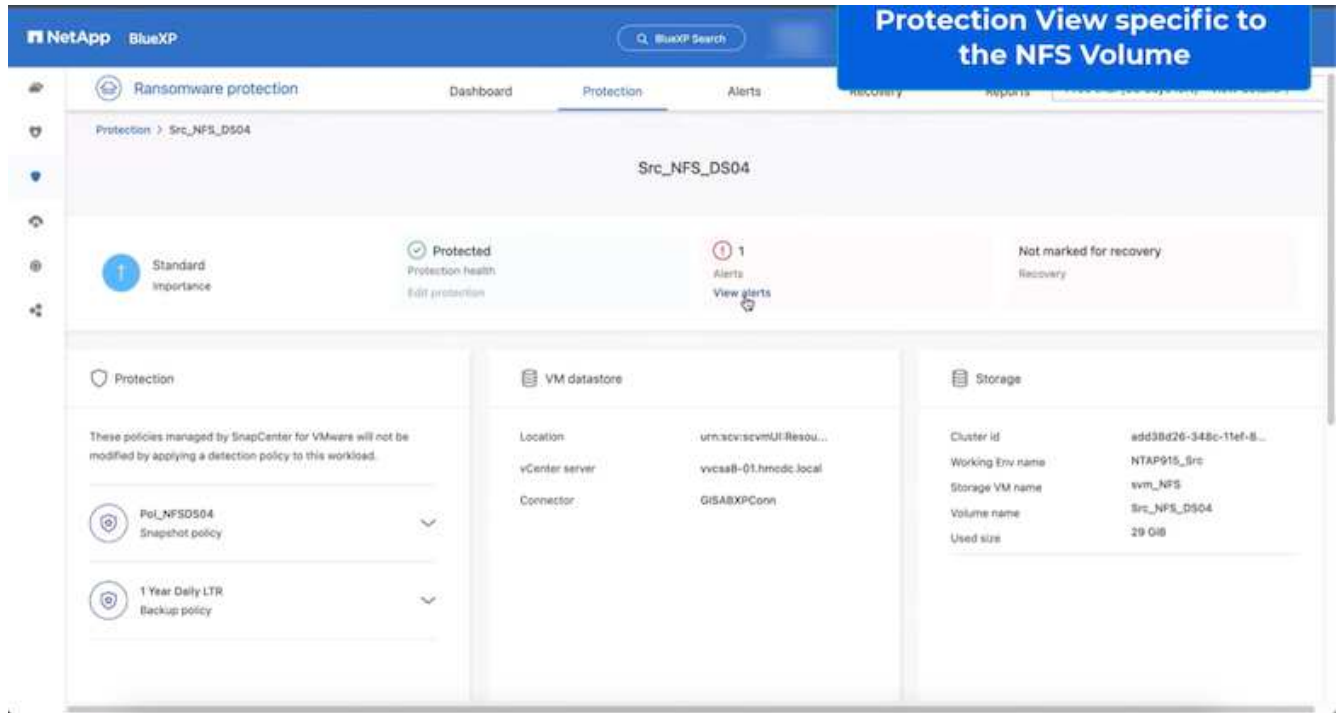


Questa sezione analizza il modo in cui la protezione ransomware BlueXP orchestra il recovery da un incidente ransomware in cui i file delle VM sono crittografati.

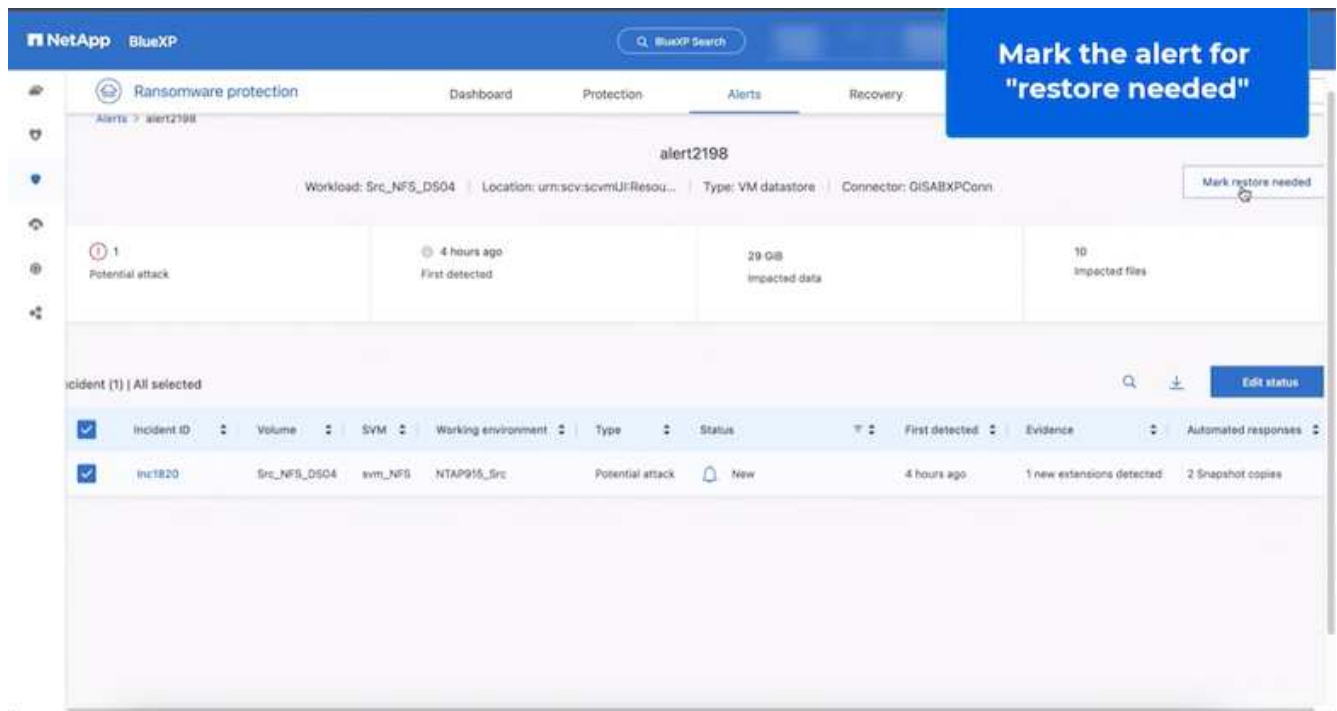


Se la macchina virtuale è gestita da SnapCenter, la protezione anti-ransomware BlueXP ripristina lo stato precedente della macchina virtuale utilizzando il processo coerente con la macchina virtuale.

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



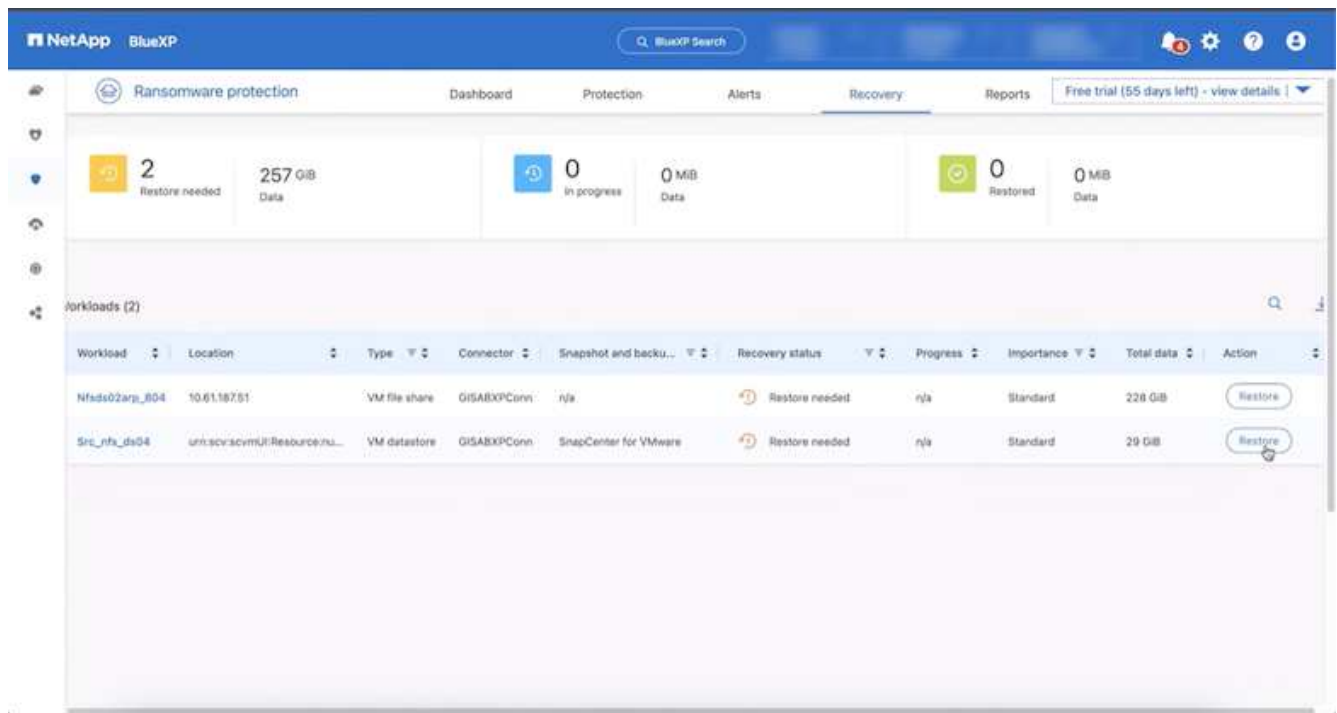
3. Contrassegna l'incidente ransomware come pronto per il recovery (dopo la neutralizzazione degli incidenti) selezionando "Mark restore needed"



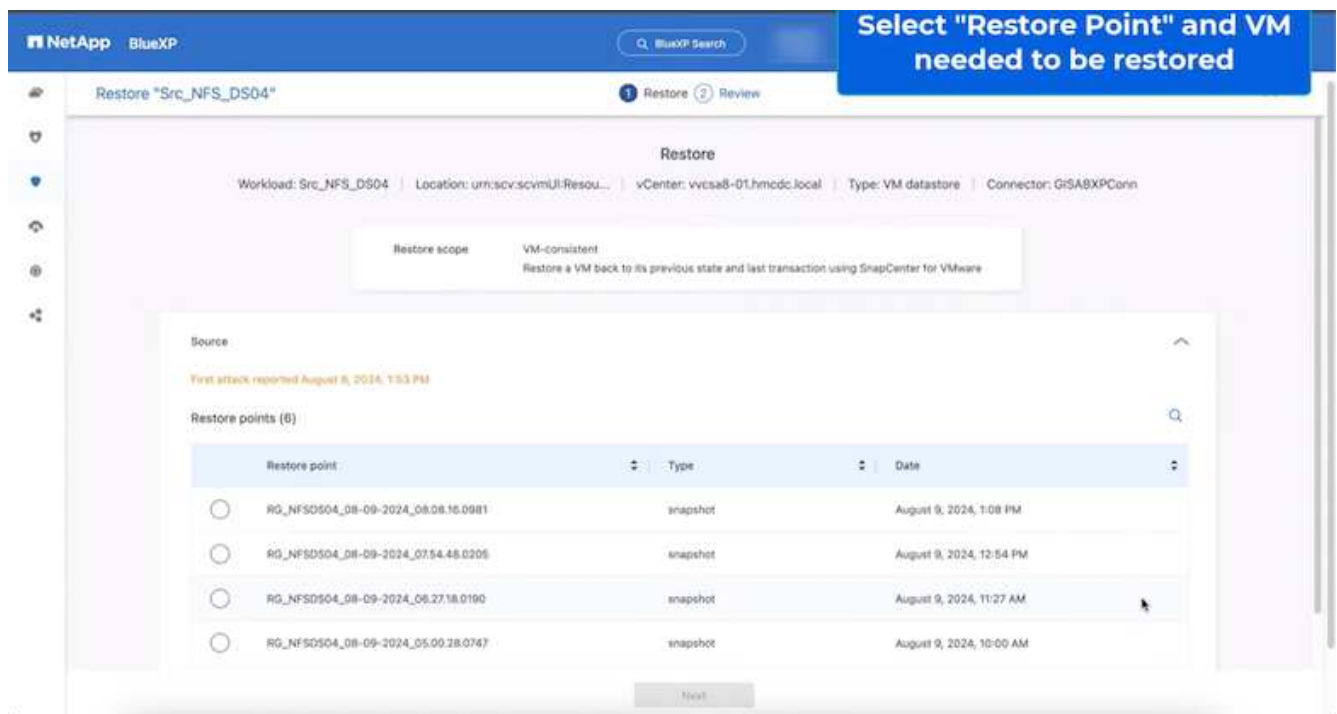


L'avviso può essere ignorato se l'incidente risulta falso positivo.

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

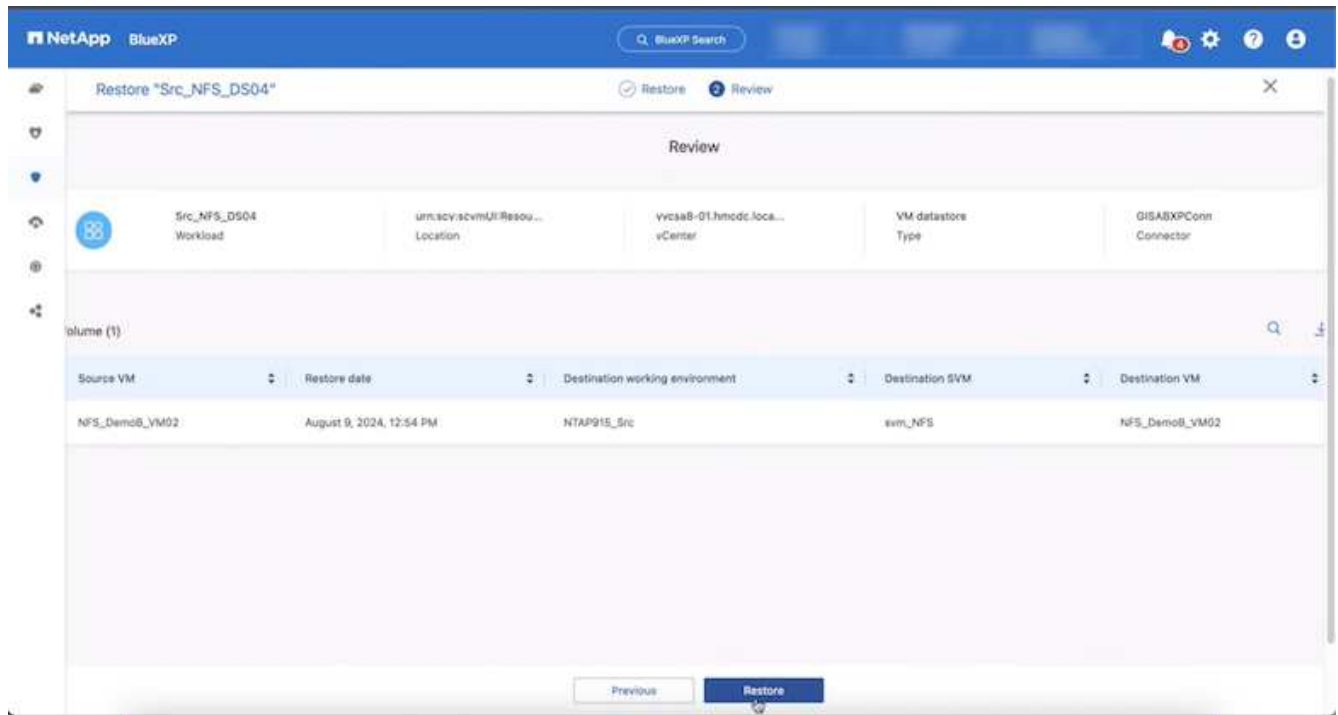


5. In questo caso, l'ambito del ripristino è "da VM" (per SnapCenter per VM, l'ambito del ripristino è "da VM")

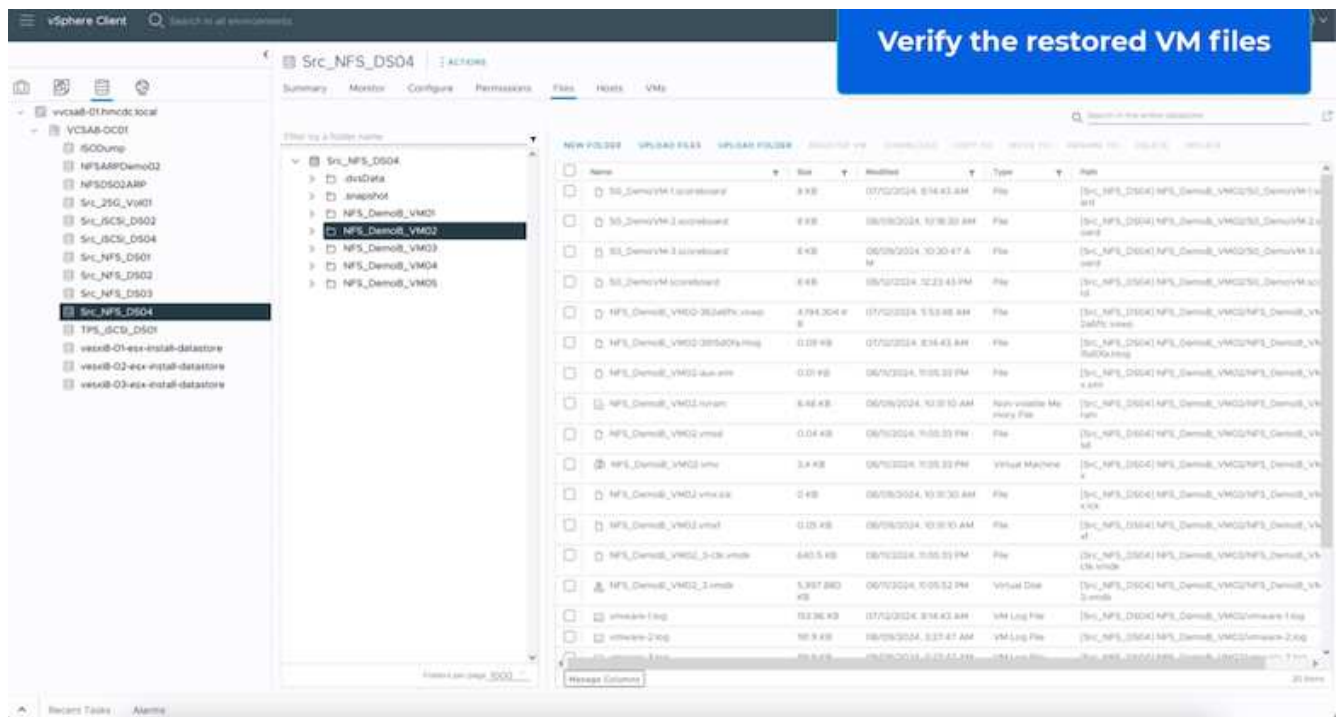


6. Scegliere il punto di ripristino da utilizzare per ripristinare i dati, quindi selezionare destinazione e fare clic su Ripristina.





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



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

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

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

## Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.