



# Virtualizzazione con VMware

## NetApp Solutions

NetApp  
May 10, 2024

This PDF was generated from <https://docs.netapp.com/it-it/netapp-solutionshttps://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html> on May 10, 2024. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Sommario

- Soluzioni NetApp per la virtualizzazione con VMware di Broadcom ..... 1
  - VMware Cloud Foundation ..... 1
  - Introduzione all'automazione per ONTAP e vSphere ..... 139
  - Multicloud ibrido NetApp con soluzioni VMware ..... 151
  - Casi d'utilizzo di multicloud ibrido di VMware ..... 151
  - Desktop virtuali ..... 152
  - Array SAN all-flash NetApp con VMware vSphere 8 ..... 192
  - Demo ed esercitazioni ..... 237

# Soluzioni NetApp per la virtualizzazione con VMware di Broadcom

## VMware Cloud Foundation

### VMware Cloud Foundation con NetApp All-Flash SAN Array

Autore: Josh Powell

#### VMware Cloud Foundation con NetApp All-Flash SAN Array

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

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

#### Casi di utilizzo

Casi d'utilizzo illustrati nella presente documentazione:

- Opzioni di storage per i clienti che cercano ambienti uniformi su cloud pubblici e privati.
- Soluzione automatizzata per l'implementazione dell'infrastruttura virtuale per i domini di carico di lavoro.
- Soluzione storage scalabile realizzata su misura per soddisfare esigenze in evoluzione, anche se non allineata direttamente ai requisiti delle risorse di calcolo.
- Distribuire storage supplementare ai domini di gestione e carico di lavoro VI utilizzando ONTAP Tools per VMware vSphere.
- Proteggi macchine virtuali e datastore utilizzando il plug-in SnapCenter per VMware vSphere.

#### Pubblico

Questa soluzione è destinata alle seguenti persone:

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

## Panoramica sulla tecnologia

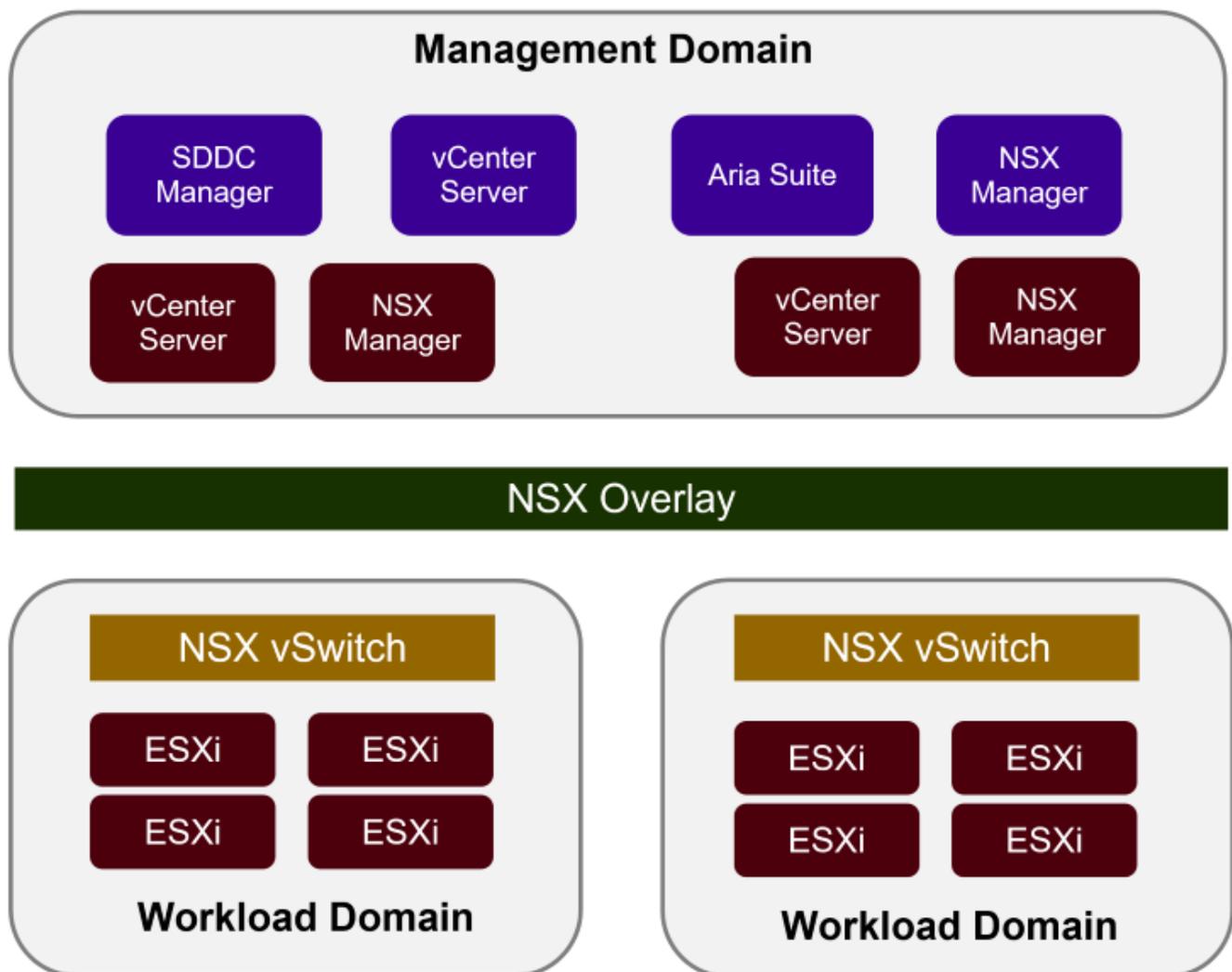
La soluzione VCF con NetApp ASA comprende i seguenti componenti principali:

### VMware Cloud Foundation

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

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

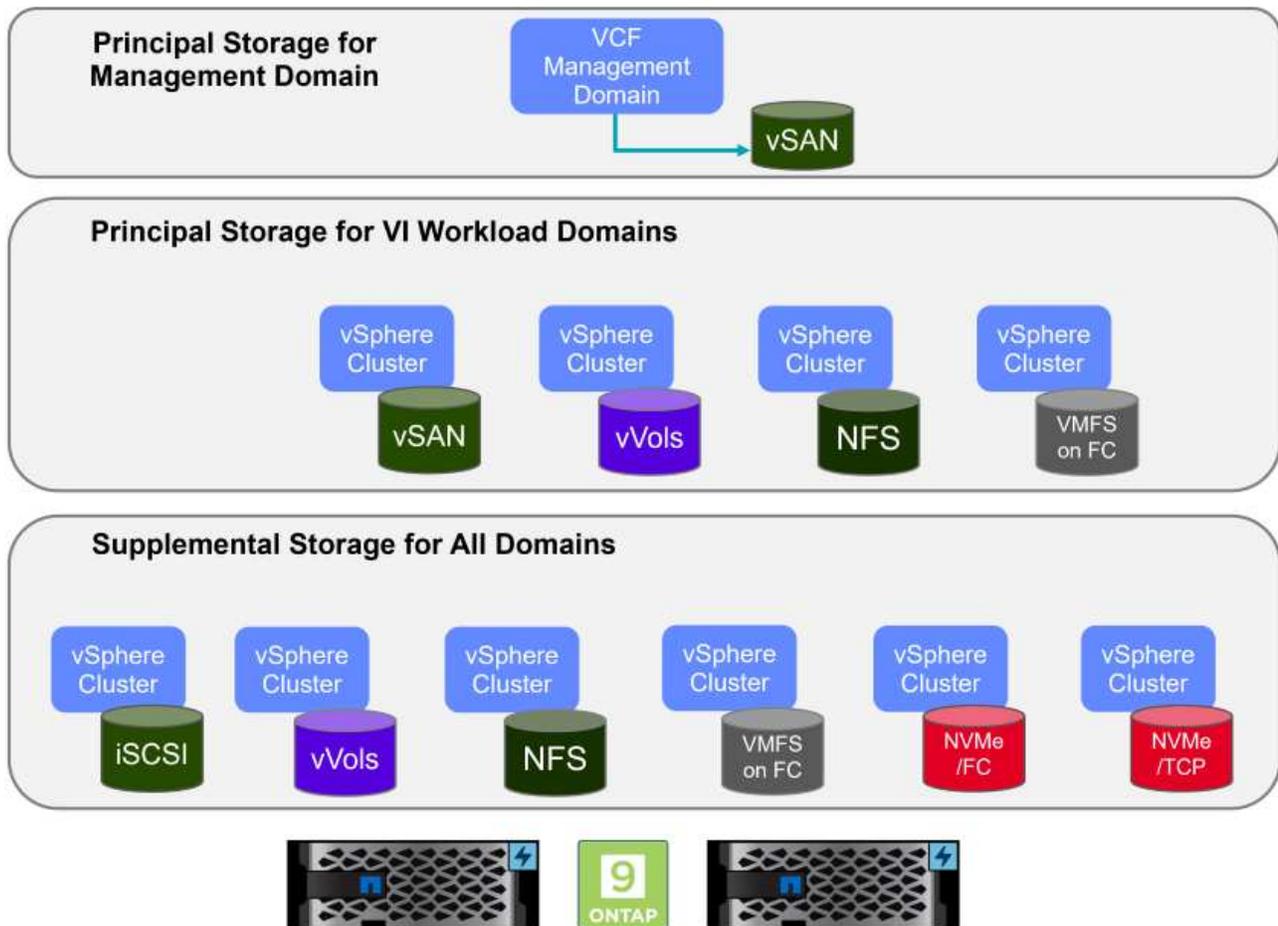
VCF è costituito da un singolo dominio di gestione e fino a 24 domini di workload VI che rappresentano ciascuno un'unità di infrastruttura predisposta per le applicazioni. Un dominio del carico di lavoro è costituito da uno o più cluster vSphere gestiti da una singola istanza vCenter.



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

## Opzioni di archiviazione VCF

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



### Archiviazione principale per i domini del carico di lavoro

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

### Archiviazione supplementare per domini di gestione e carico di lavoro

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

Ulteriori risorse di documentazione per VMware Cloud Foundation:

\* ["Documentazione di VMware Cloud Foundation"](#)

\* ["Tipi di storage supportati per VMware Cloud Foundation"](#)

\* ["Gestione dello storage in VMware Cloud Foundation"](#)

### Array SAN all-flash NetApp

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

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

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



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



Per informazioni dettagliate, consultare la ["Landing page di NetApp ASA"](#).

### Supporto dei protocolli di storage

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

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

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

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

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

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

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

## Tecnologia Active-Active

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

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

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

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

## Garanzie di archiviazione

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

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

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

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

Vedere ["Portale dei prodotti NetApp ASA"](#) per ulteriori informazioni.

## Strumenti NetApp ONTAP per VMware vSphere

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

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

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

Per ulteriori informazioni sugli strumenti NetApp ONTAP, vedere ["Strumenti ONTAP per la documentazione VMware vSphere"](#) pagina.

## Plug-in SnapCenter per VMware vSphere

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

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

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

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

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

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

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

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

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

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

## Panoramica della soluzione

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

Scenari trattati nella presente documentazione:

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

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

Autore: Josh Powell

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

### Panoramica dello scenario

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

Questo scenario copre i seguenti passaggi di alto livello:

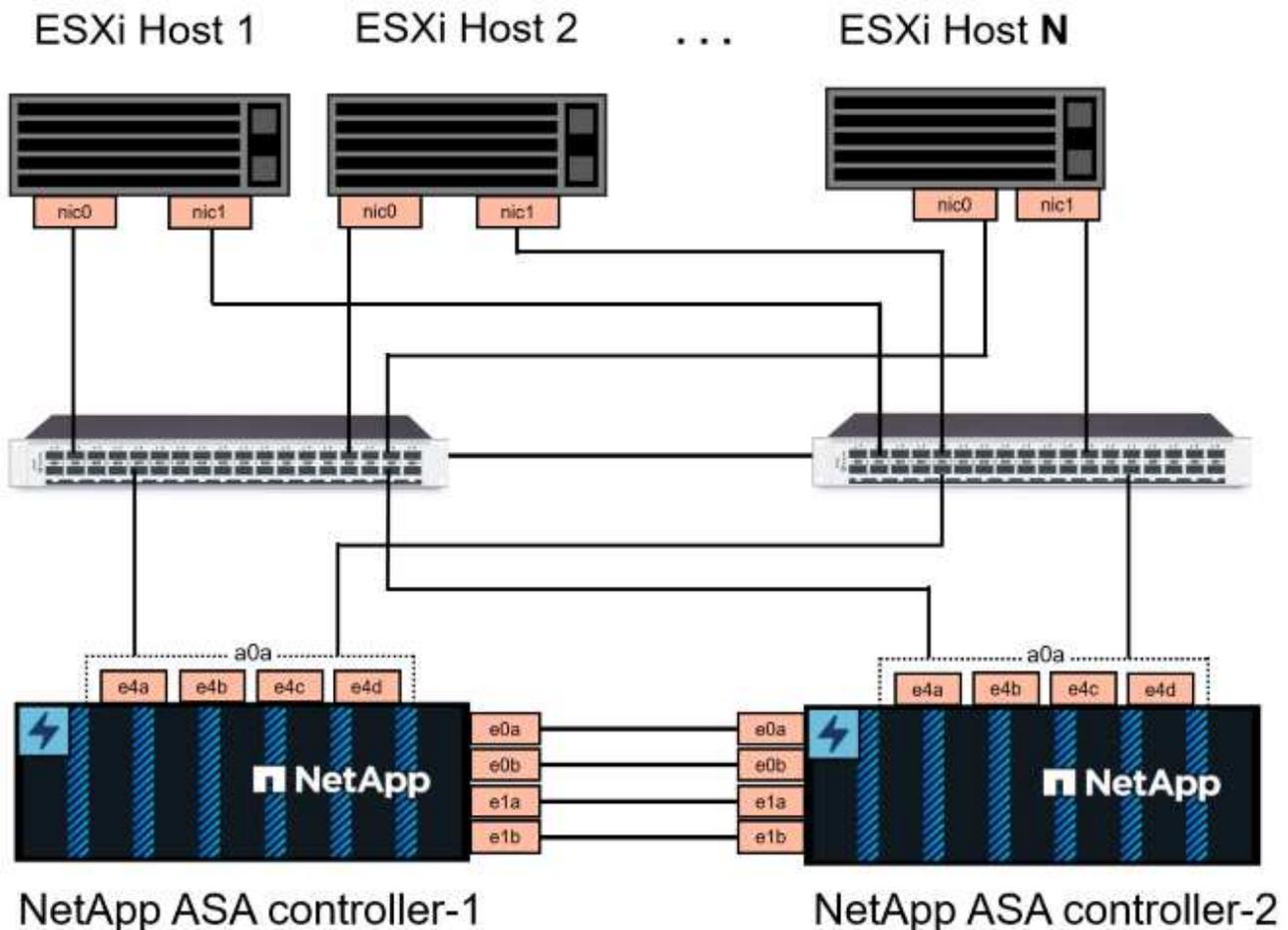
- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio di gestione VCF.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio di gestione VCF.
- Distribuire gli strumenti ONTAP nel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

### Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

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

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



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

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

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



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

## Fasi di implementazione

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

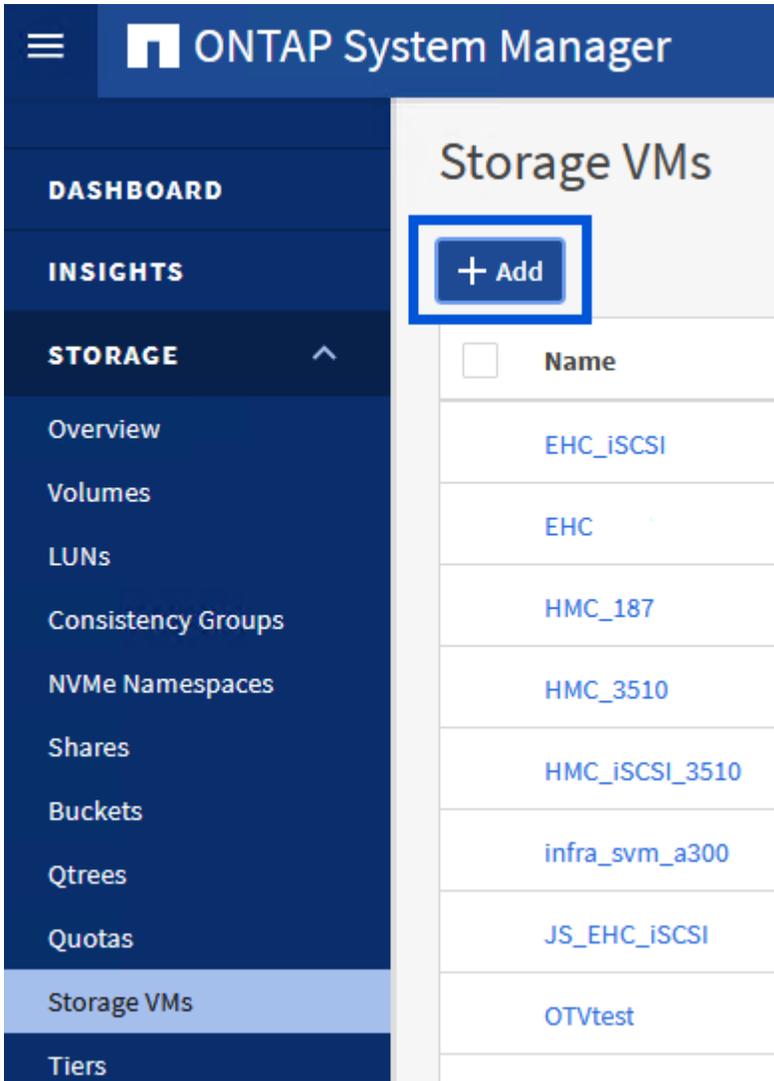
## **Crea SVM e LIF su un sistema storage ONTAP**

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

## Creazione di LIF e macchine virtuali storage

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

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



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

## Add Storage VM



STORAGE VM NAME

SVM\_ISCSI

IPSPACE

Default

### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

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



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

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS\_iSCSI

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

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

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

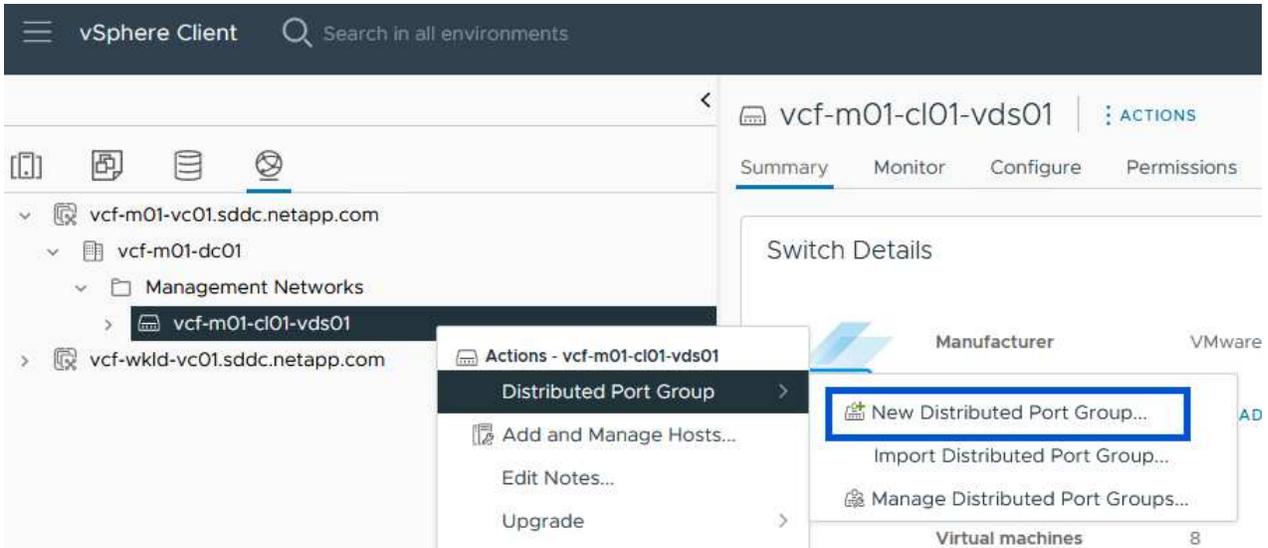
## Configurare il networking per iSCSI sugli host ESXi

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

## Creare gruppi di porte distribuite per il traffico iSCSI

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

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



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

## New Distributed Port Group

- 1 Name and location
- 2 Configure settings
- 3 Ready to complete

## Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL BACK NEXT

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

The screenshot shows the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search bar. The main content area is divided into a left-hand navigation pane and a right-hand details pane. The left pane shows a tree view of the environment, with the following path highlighted: vcf-m01-vc01.sddc.netapp.com > vcf-m01-dc01 > Management Networks > vcf-m01-cl01-vds01 > vcf-m01-cl01-vds01-pg-iscsi-a. A context menu is open over the selected item, with the 'Edit Settings...' option highlighted. The right-hand pane shows the 'Distributed Port Group Details' for the selected port group. The details are as follows:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds01
Network protocol profile	--
Network resource pool	--
Hosts	4

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

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General	<b>Load balancing</b>	Route based on originating virtual por ▾
Advanced	<b>Network failure detection</b>	Link status only ▾
VLAN	<b>Notify switches</b>	Yes ▾
Security	<b>Failback</b>	Yes ▾
Traffic shaping		
<b>Teaming and failover</b>		
Monitoring		
Miscellaneous		

**Failover order** ⓘ

MOVE UP MOVE DOWN

**Active uplinks**

uplink1

**Standby uplinks**

**Unused uplinks**

uplink2

CANCEL OK

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

# Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

## Load balancing

Route based on originating virtual por 

## Network failure detection

Link status only 

## Notify switches

Yes 

## Failback

Yes 

## Failover order

MOVE UP MOVE DOWN

### Active uplinks

 uplink2

### Standby uplinks

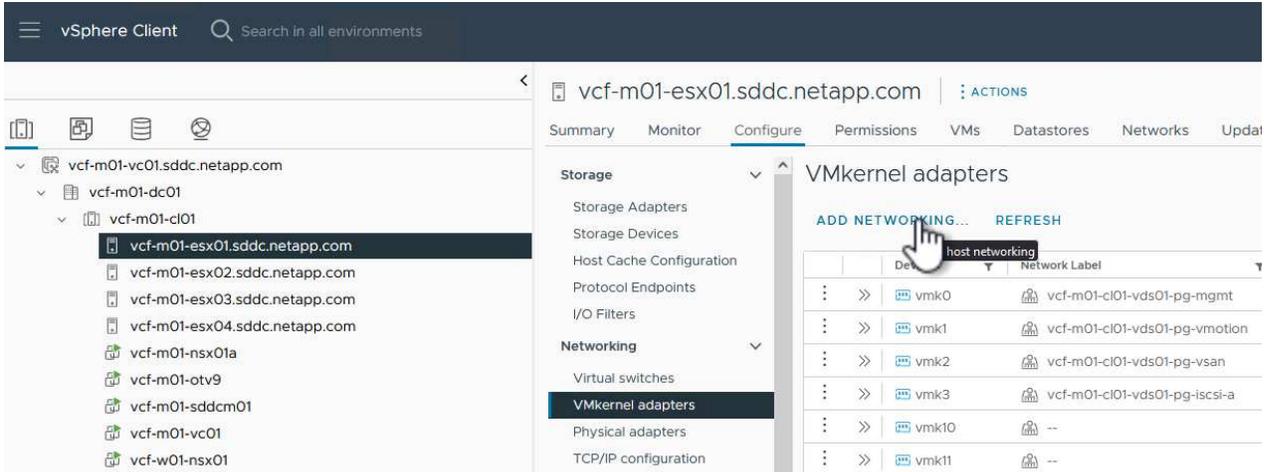
### Unused uplinks

 uplink1

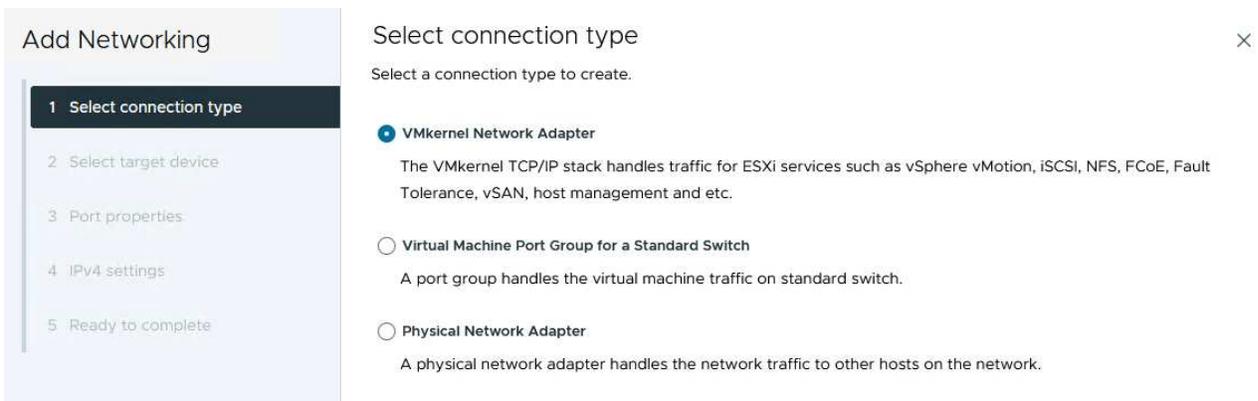
## Creare adattatori VMkernel su ciascun host ESXi

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

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



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



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

### 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

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-ci01-vds01
<input checked="" type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-a	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-b	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-mgmt	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vmotion	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vsan	--	vcf-m01-ci01-vds01

6 items

CANCEL BACK NEXT

4. Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e 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

### Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

- vMotion
- vSphere Replication NFC
- NVMe over RDMA
- Provisioning
- vSAN
- Fault Tolerance logging
- vSAN Witness
- Management
- vSphere Backup NFC
- vSphere Replication
- NVMe over TCP

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**

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

### Add Networking

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

### Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-m01-cl01-vds01-pg-iscsi-a

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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

## **Implementazione e utilizzo degli strumenti di ONTAP per configurare lo storage**

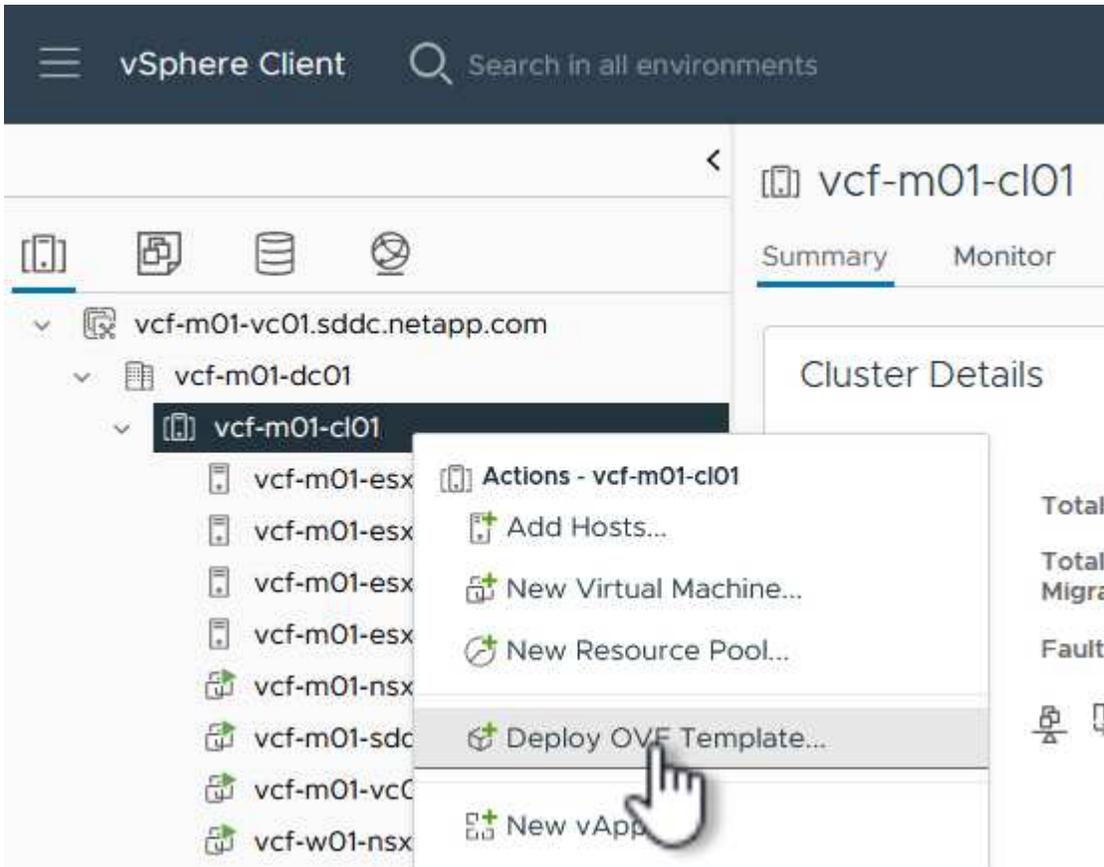
I seguenti passaggi vengono eseguiti sul cluster del dominio di gestione VCF utilizzando il client vSphere e prevedono la distribuzione di OTV, la creazione di un datastore iSCSI VMFS e la migrazione delle VM di gestione al nuovo datastore.

## Implementa i tool ONTAP per VMware vSphere

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

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

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



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

## 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

- 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.
- Per la posizione di archiviazione dei file di configurazione e del disco, selezionare il datastore vSAN del cluster del dominio di gestione VCF.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

**6 Select storage**

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

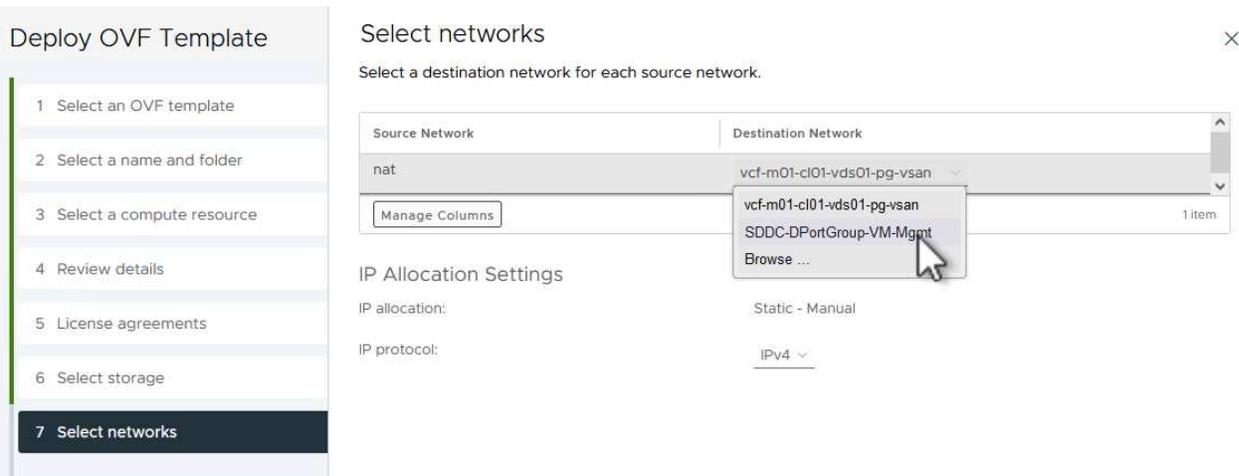
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsant01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Items per page 10 5 items

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



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

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

Fare clic su **Avanti** per continuare.

## Deploy OVF Template

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

## Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values X

System Configuration	4 settings
<b>Application User Password (*)</b>	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>
<b>NTP Servers</b>	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>
<b>Maintenance User Password (*)</b>	Password to assign to maint user account.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

## Deploy OVF Template

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

## Customize template

Configure vCenter or Enable VCF	5 settings
<b>Enable VMware Cloud Foundation (VCF)</b>	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
<b>vCenter Server Address (*)</b>	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/>
<b>Port (*)</b>	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
<b>Username (*)</b>	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
<b>Password (*)</b>	Specify the password of an existing vCenter to register to.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

Network Properties	8 settings
<b>Host Name</b>	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-m01-otv9"/>
<b>IP Address</b>	Specify the IP address for the appliance. (Leave blank if DHCP is

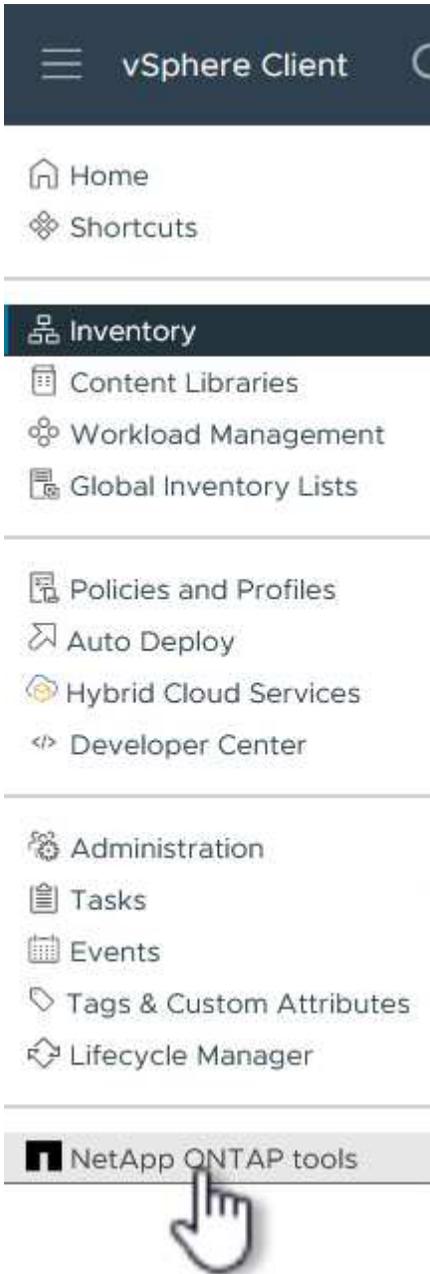
CANCEL BACK NEXT

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

## Configurare un datastore iSCSI VMFS sul dominio di gestione utilizzando OTV

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

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



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

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

### ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

#### Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.



#### Provision Datastore

Create traditional or vVols datastores.



#### Next Steps

  
[View Dashboard](#)  
View and monitor the datastores in ONTAP tools for VMware vSphere.

  
[Settings](#)  
Configure administrative settings such as credentials, alarm thresholds.

#### What's new?

September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

#### Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

Overview

- Storage Systems
- Storage capability profile
- Storage Mapping
- Settings
- Reports
  - Datastore Report
  - Virtual Machine Report
  - vVols Datastore Report
  - vVols Virtual Machine Report
  - Log Integrity Report

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

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	vcf-m01-vc01.sddc.netapp.com 
Name or IP address:	172.16.9.25
Username:	admin
Password:	●●●●●●●●
Port:	443
Advanced options	

CANCEL

SAVE & ADD MORE

ADD 

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

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

### Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

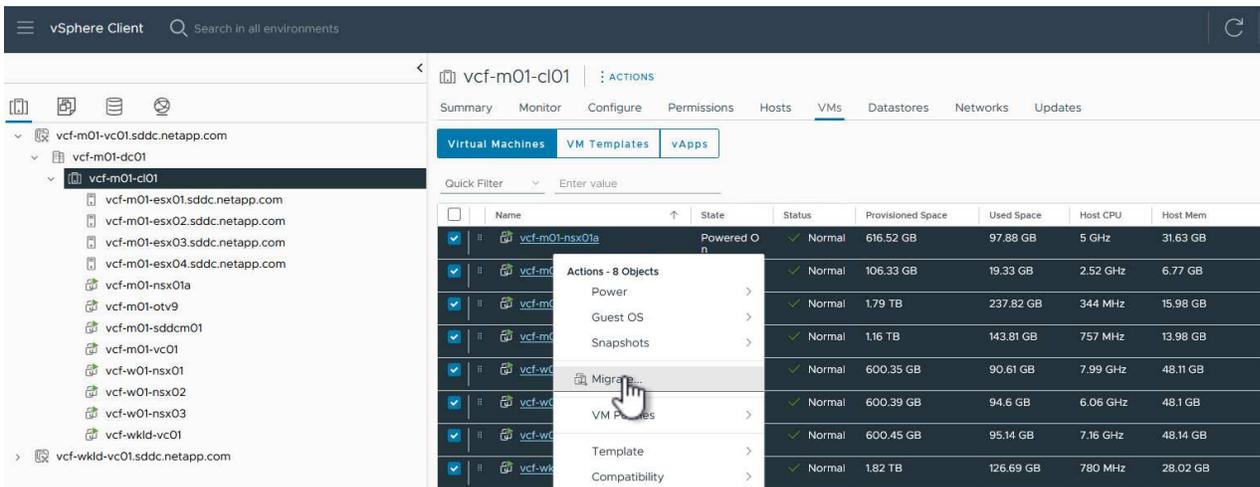
ADD

## Migrazione di VM di gestione's al datastore iSCSI

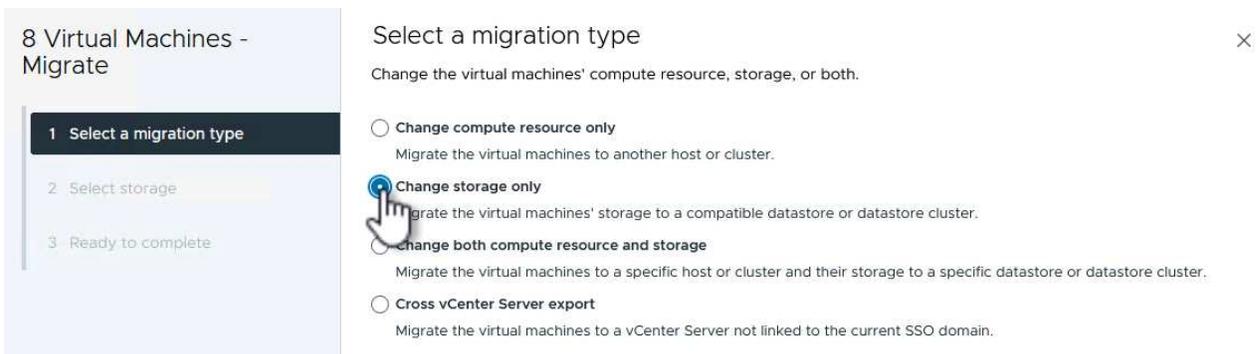
Nei casi in cui si preferisce utilizzare lo storage ONTAP per proteggere la VM di gestione VCF, vMotion può essere utilizzato per migrare la VM nel datastore iSCSI appena creato.

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

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



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



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

## 8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

### Select storage



Select the destination storage for the virtual machine migration.

**BATCH CONFIGURE** CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	
<input type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	

Manage Columns Items per page 10 2 items

#### Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Rivedere le selezioni e fare clic su **fine** per avviare la migrazione.

6. Lo stato di rilocalizzazione può essere visualizzato dal riquadro **attività recenti**.

Task Name	Target	Status	Details
Relocate virtual machine	<a href="#">vcf-w01-nsx03</a>	38%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-wkld-vc01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-otv9</a>	36%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-nsx01a</a>	49%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx02</a>	47%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-sddcm01</a>	39%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-vc01</a>	44%	Migrating Virtual Machine active state

## Ulteriori informazioni

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

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

## Video dimostrativo per questa soluzione

[Archivi dati iSCSI come archiviazione supplementare per i domini di gestione VCF](#)

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

Autore: Josh Powell

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

## Panoramica dello scenario

In questo scenario dimostreremo come implementare e utilizzare ONTAP Tools per VMware vSphere (OTV) per configurare un datastore **vVol** per un dominio del carico di lavoro VCF.

**iSCSI** viene utilizzato come protocollo storage per il datastore vVol.

Questo scenario copre i seguenti passaggi di alto livello:

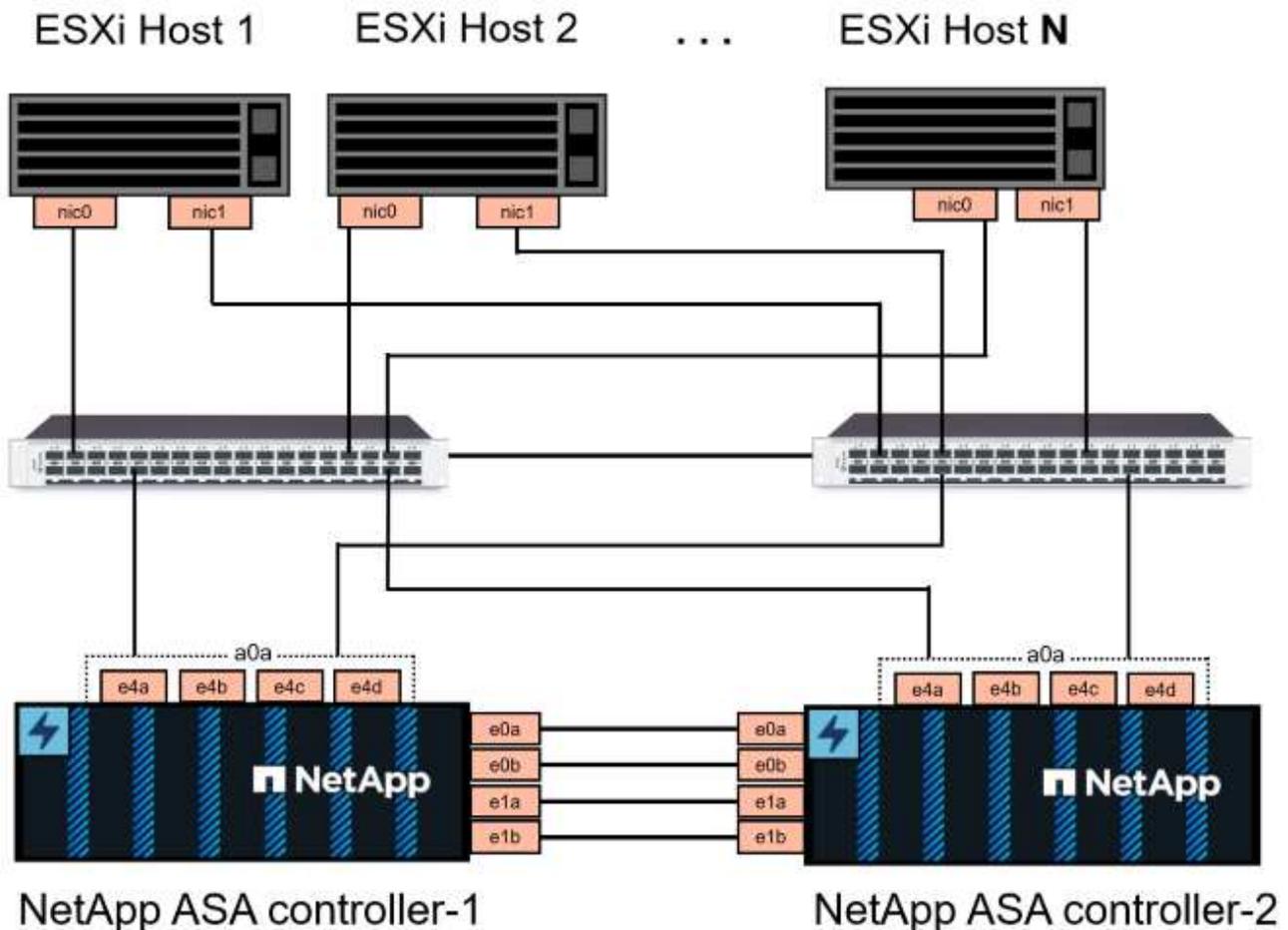
- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico iSCSI.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Distribuire gli strumenti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

## Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

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

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



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

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



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

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

### Fasi di implementazione

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

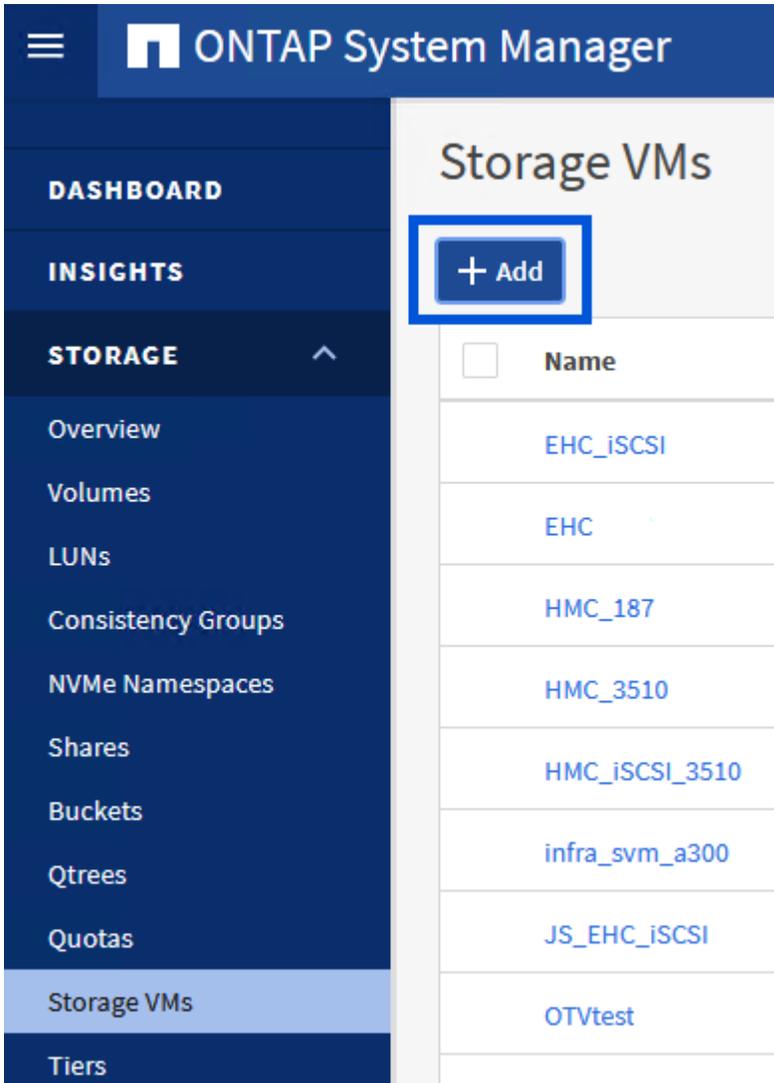
## **Crea SVM e LIF su un sistema storage ONTAP**

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

## Creazione di LIF e macchine virtuali storage

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

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



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

## Add Storage VM



STORAGE VM NAME

SVM\_ISCSI

IPSPACE

Default

### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

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



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

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS\_iSCSI

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

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

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

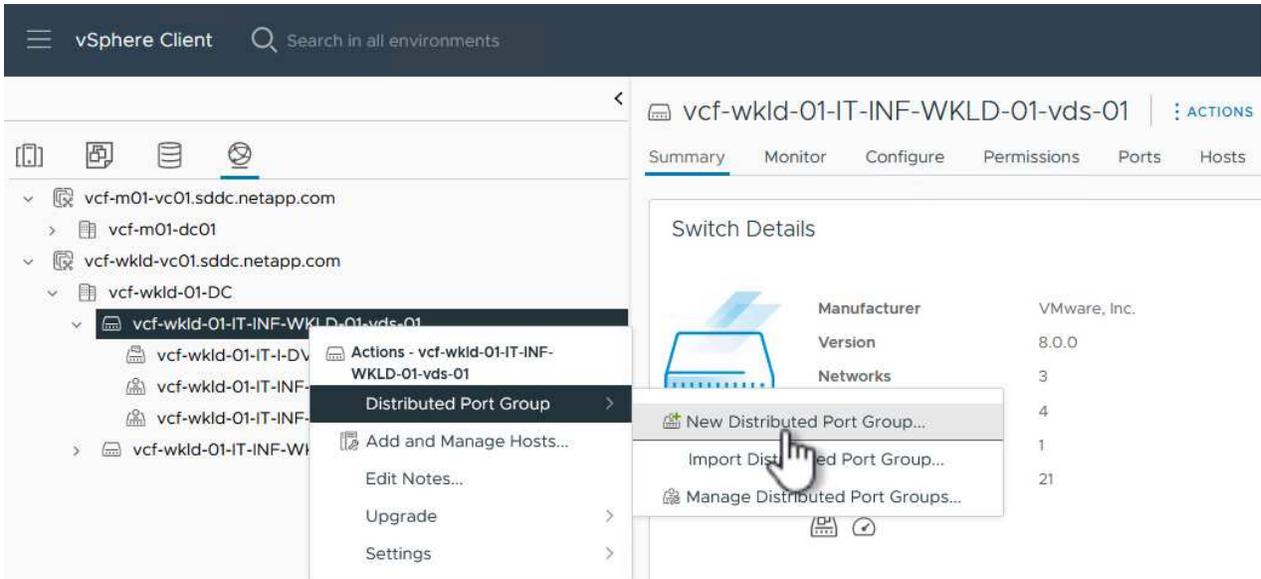
## Configurare il networking per iSCSI sugli host ESXi

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

## Creare gruppi di porte distribuite per il traffico iSCSI

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

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



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

## New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

## Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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

The screenshot shows the vSphere Client interface. On the left, a tree view displays the environment structure, with the path **vcf-wkld-01-iscsi-a** selected. A context menu is open over this selection, showing options like **Actions - vcf-wkld-01-iscsi-a** and **Edit Settings...**. On the right, the **Distributed Port Group Details** panel is visible, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	<a href="#">vcf-wkld-01-IT-INF-WKLD-01-vds-01</a>
Network protocol profile	--

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

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a

General Load balancing Route based on originating virtual por ▼

Advanced Network failure detection Link status only ▼

VLAN Notify switches Yes ▼

Security Fallback Yes ▼

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL OK

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

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General Load balancing Route based on originating virtual por ▼

Advanced Network failure detection Link status only ▼

VLAN Notify switches Yes ▼

Security Fallback Yes ▼

Traffic shaping

**Teaming and failover**

Monitoring

Miscellaneous

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

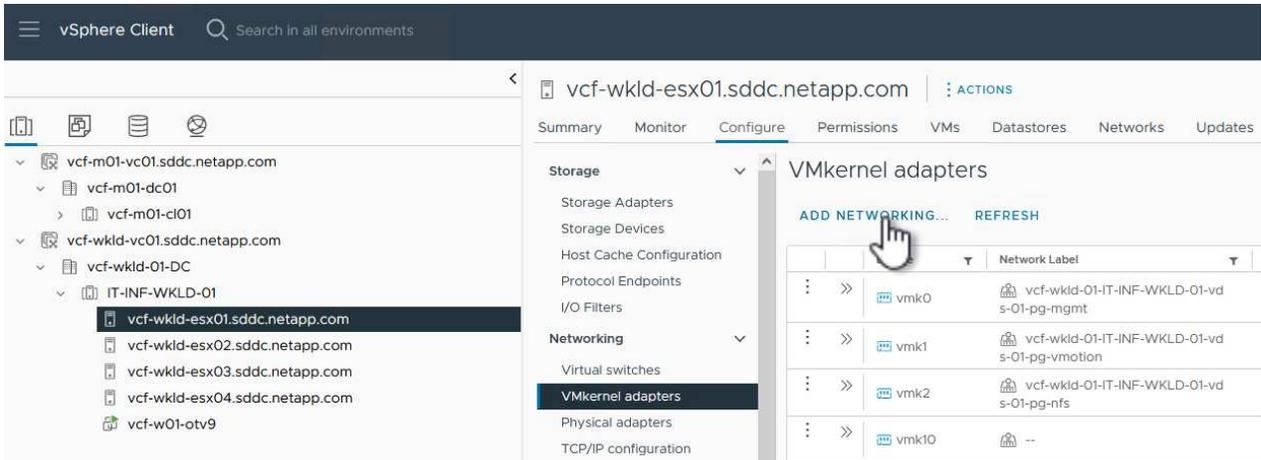
Unused uplinks

uplink1

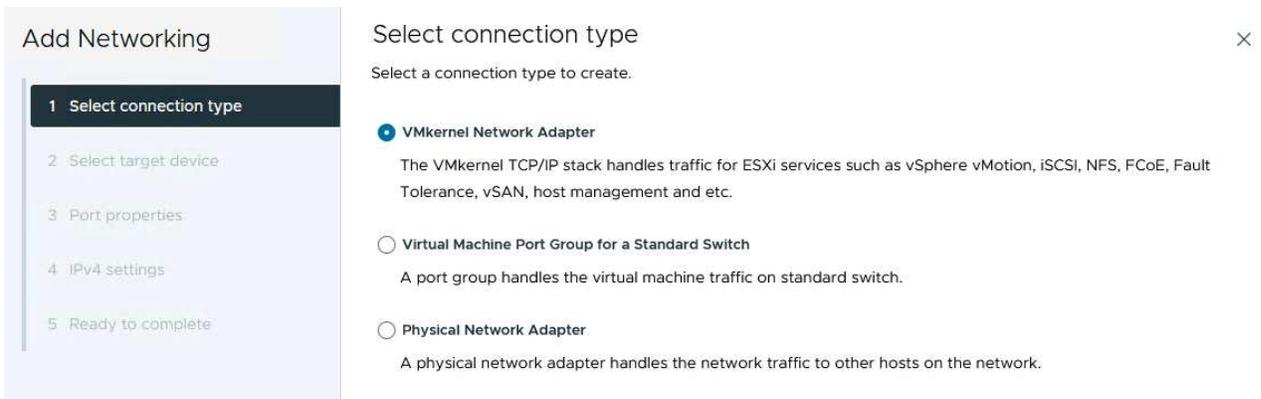
## Creare adattatori VMkernel su ciascun host ESXi

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

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



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



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

## 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 checked="" type="radio"/>	 vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 5 items

CANCEL

BACK

NEXT

- Nella pagina **Proprietà porta** mantenere le impostazioni predefinite e 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

## Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

### Available services

- Enabled services
- vMotion
  - Provisioning
  - Fault Tolerance logging
  - Management
  - vSphere Replication
  - vSphere Replication NFC
  - vSAN
  - vSAN Witness
  - vSphere Backup NFC
  - NVMe over TCP
  - NVMe over RDMA

- 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**

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

### Add Networking

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

### Ready to complete

Review your selections before finishing the wizard

- ▼ **Select target device**

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ **Port properties**

New port group vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ **IPv4 settings**

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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

## **Implementazione e utilizzo degli strumenti di ONTAP per configurare lo storage**

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

Per i domini di carico di lavoro VI, OTV viene installato nel cluster di gestione VCF ma registrato con vCenter associato al dominio del carico di lavoro VI.

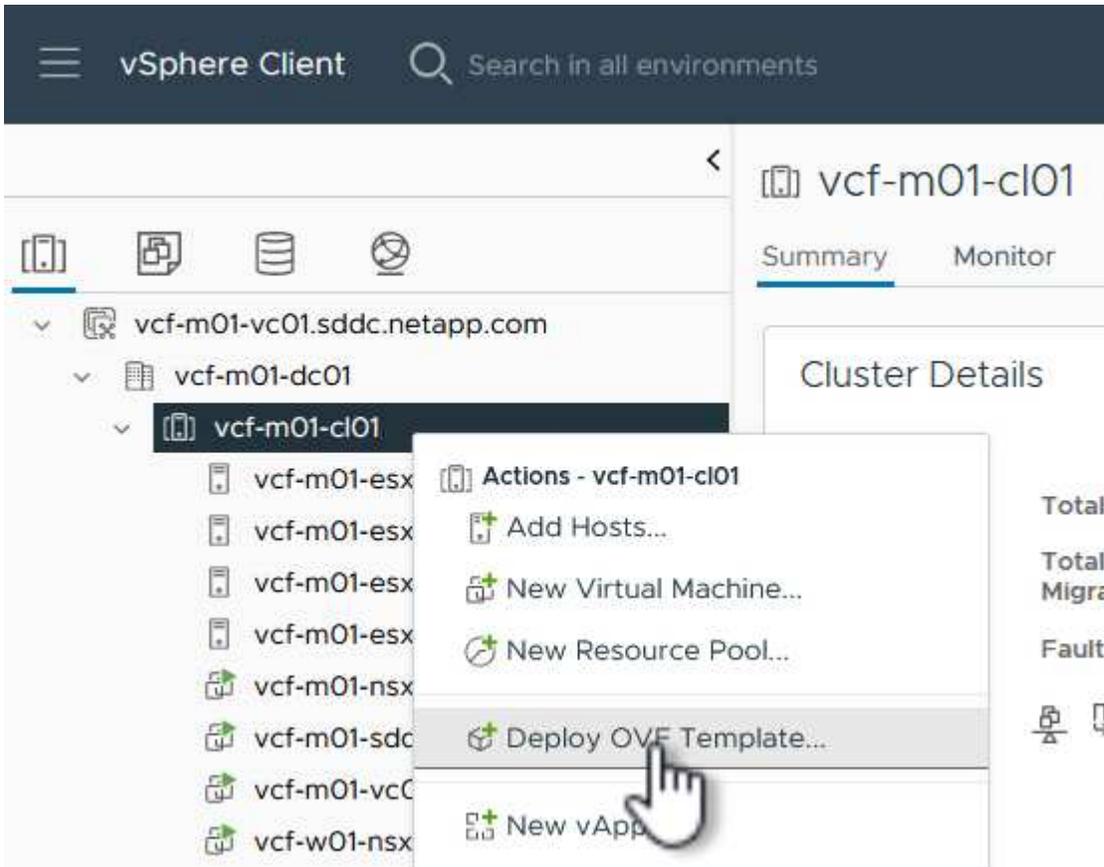
Per ulteriori informazioni sulla distribuzione e l'utilizzo degli strumenti ONTAP in un ambiente vCenter multiplo, fare riferimento a ["Requisiti per la registrazione degli strumenti ONTAP in più ambienti vCenter Server"](#).

## Implementa i tool ONTAP per VMware vSphere

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

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

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



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

## 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 di archiviazione dei file di configurazione e del disco, selezionare il datastore vSAN del cluster del dominio di gestione VCF.

## Deploy OVF Template

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

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format As defined in the VM storage policy

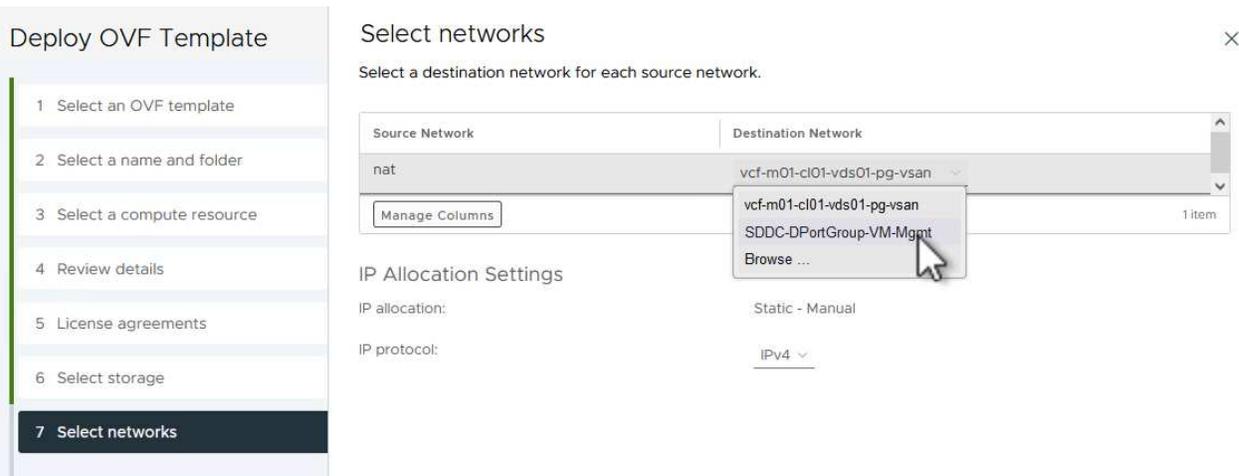
VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	v
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	v

Manage Columns Items per page 10 5 items

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



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

- Password da utilizzare per l'accesso amministrativo a OTV.
- Indirizzo IP del server NTP.
- Password dell'account di manutenzione OTV.
- Password DB Derby OTV.
- Non selezionare la casella di controllo **Abilita VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire lo storage supplementare.
- FQDN o indirizzo IP dell'appliance vCenter per **VI workload Domain**
- Credenziali per l'appliance vCenter del **VI workload Domain**
- Specificare i campi delle proprietà di rete richiesti.

Fare clic su **Avanti** per continuare.

## Deploy OVF Template

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

## Customize template

Customize the deployment properties of this software solution.

❗ 2 properties have invalid values ✕

System Configuration		4 settings
<b>Application User Password (*)</b>		Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
<b>NTP Servers</b>		A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1
<b>Maintenance User Password (*)</b>		Password to assign to maint user account.
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>

## Deploy OVF Template

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

## Customize template

❗ 2 properties have invalid values ✕

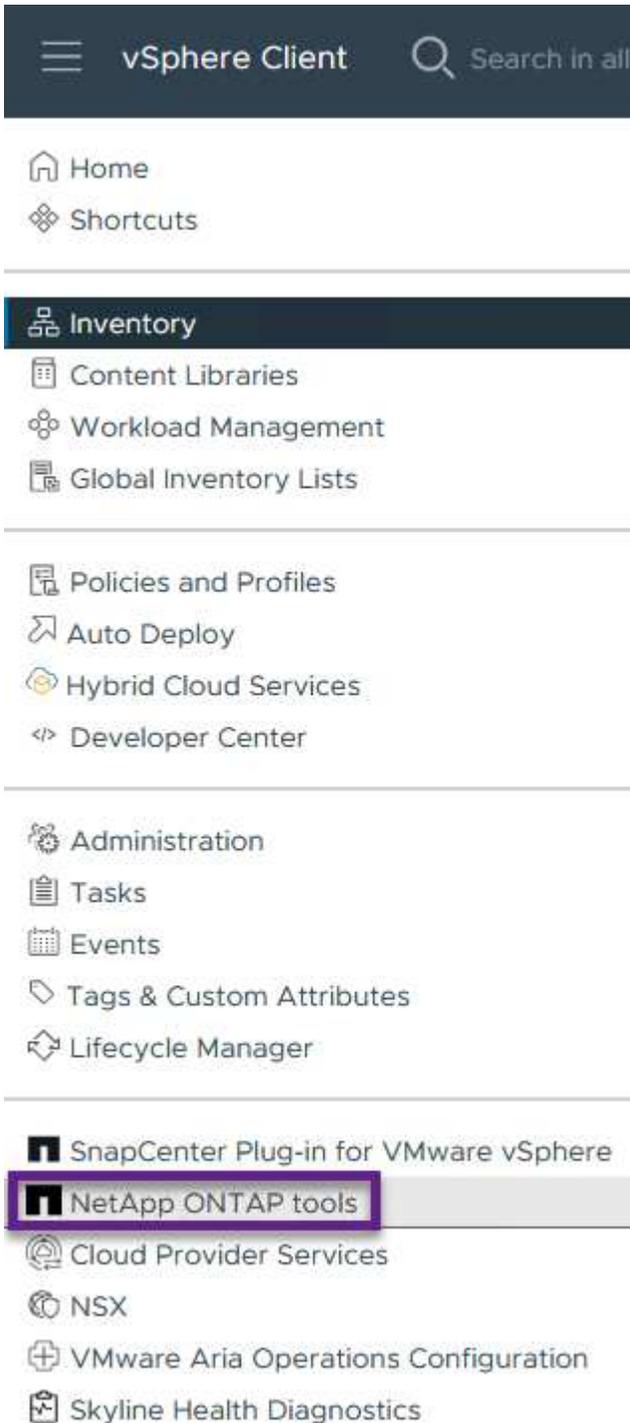
Configure vCenter or Enable vCenter		3 settings
<b>Enable VMware Cloud Foundation (VCF)</b>		vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
<b>vCenter Server Address (*)</b>		Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com
<b>Port (*)</b>		Specify the HTTPS port of an existing vCenter to register to. 443
<b>Username (*)</b>		Specify the username of an existing vCenter to register to. administrator@vsphere.local
<b>Password (*)</b>		Specify the password of an existing vCenter to register to.
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
Network Properties		8 settings
<b>Host Name</b>		Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9
<b>IP Address</b>		Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

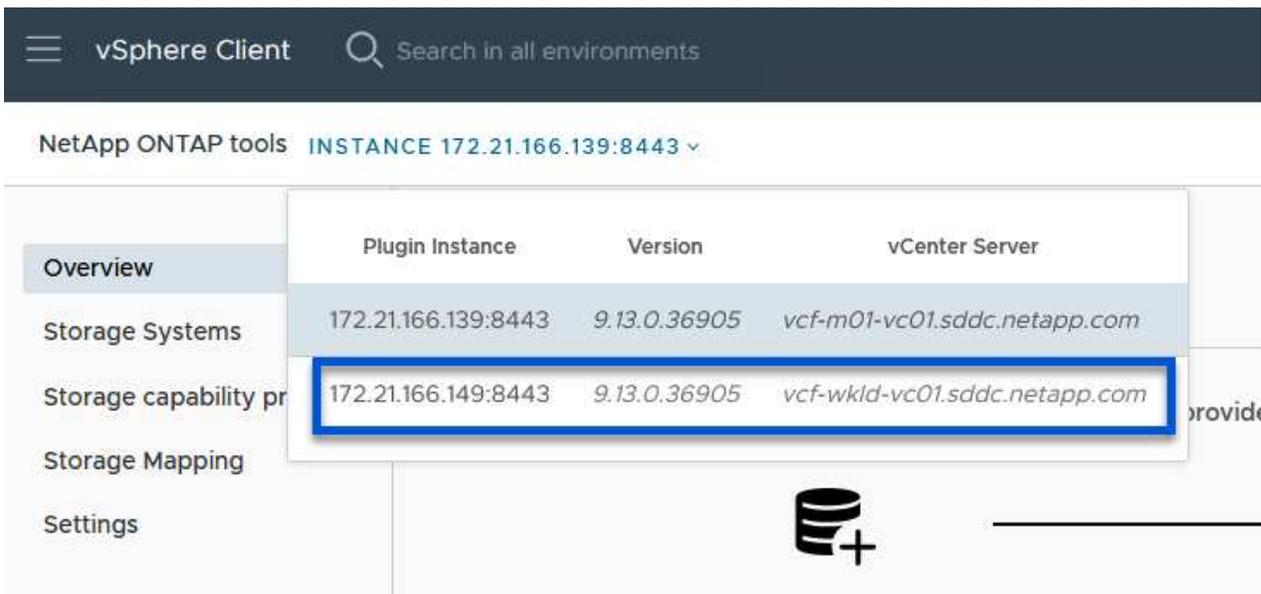
9. Leggere tutte le informazioni sulla pagina Pronto per il completamento e fare clic su fine per iniziare a implementare l'apparecchio OTV.

## Aggiunta di un sistema di storage ai tool ONTAP.

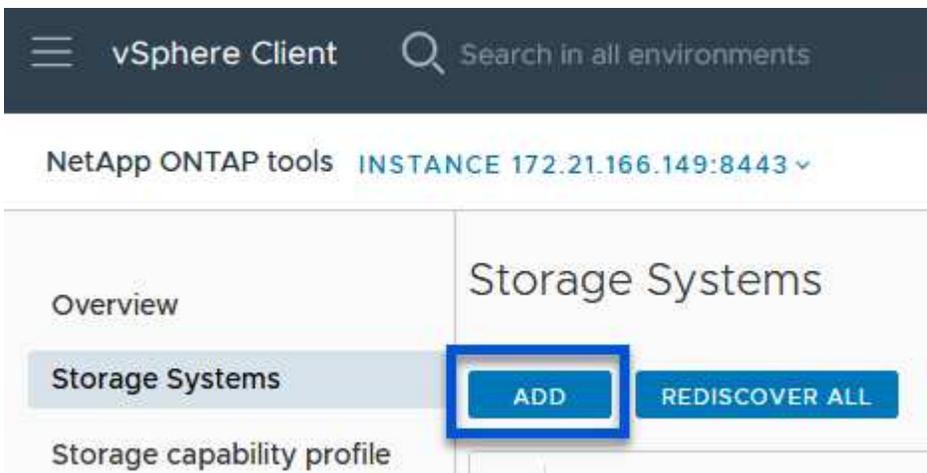
1. Accedere agli strumenti NetApp ONTAP selezionandoli dal menu principale del client vSphere.



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



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



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



VVol richiede le credenziali del cluster ONTAP al posto delle credenziali SVM. Per ulteriori informazioni, fare riferimento a ["Aggiungere sistemi storage"](#) Nella documentazione relativa agli strumenti ONTAP.

## Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server vcf-m01-vc01.sddc.netapp.com 

**Name or IP address:** 172.16.9.25

**Username:** admin

**Password:** ●●●●●●●●

**Port:** 443

Advanced options 

**ONTAP Cluster Certificate:**  Automatically fetch  Manually upload

CANCEL

SAVE & ADD MORE

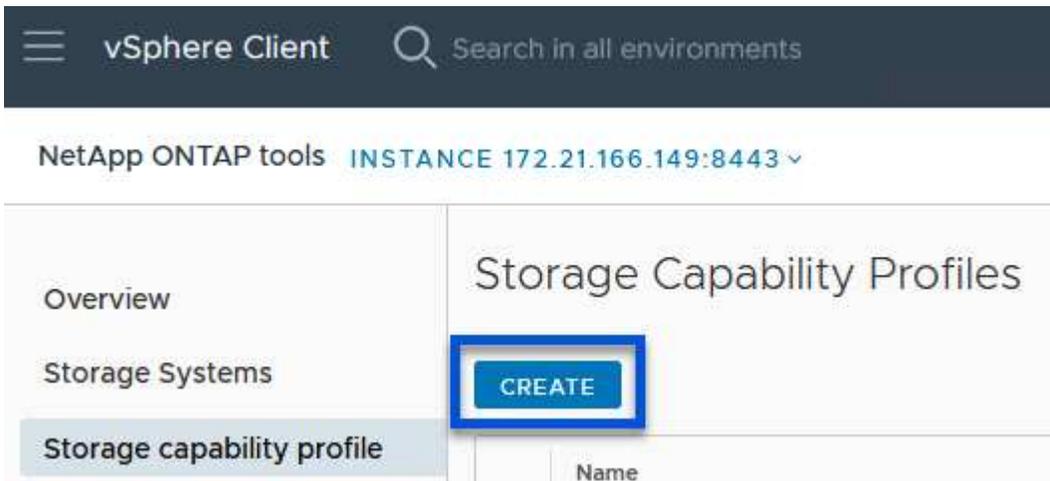
ADD

## Creare un profilo di funzionalità di storage in ONTAP Tools

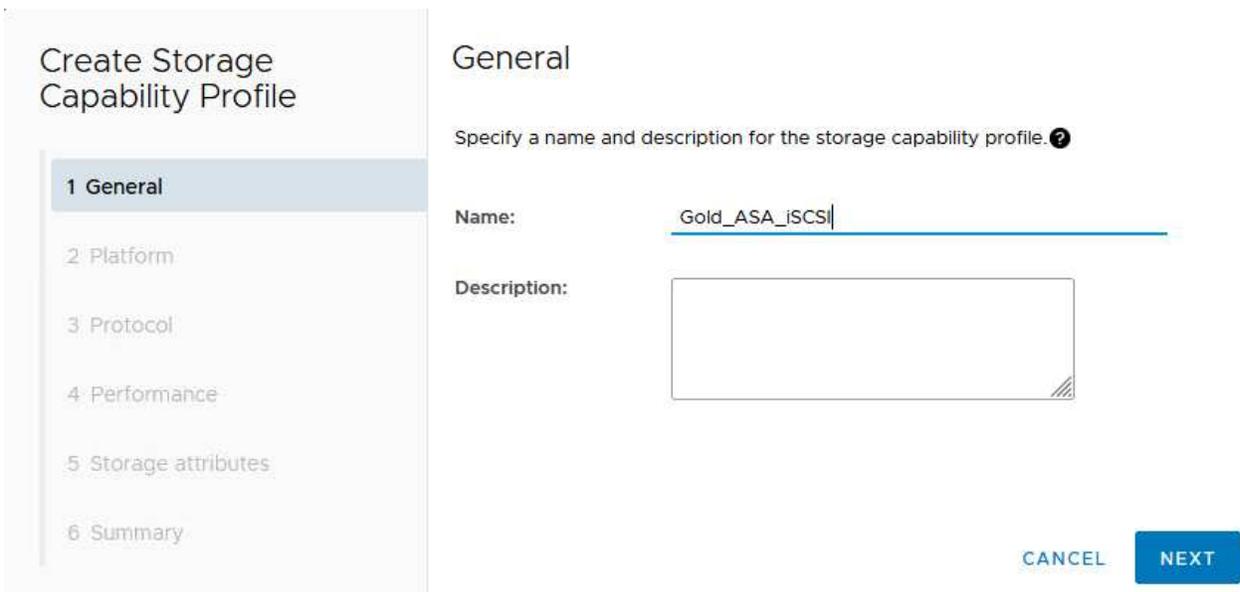
I profili di capacità dello storage descrivono le funzionalità fornite da uno storage array o da un sistema storage. Includono le definizioni della qualità del servizio e vengono utilizzate per selezionare i sistemi storage che soddisfano i parametri definiti nel profilo. È possibile utilizzare uno dei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

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

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



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



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

## Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

## Summary

Name:	ASA_Gold_iSCSI
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	None

CANCEL

BACK

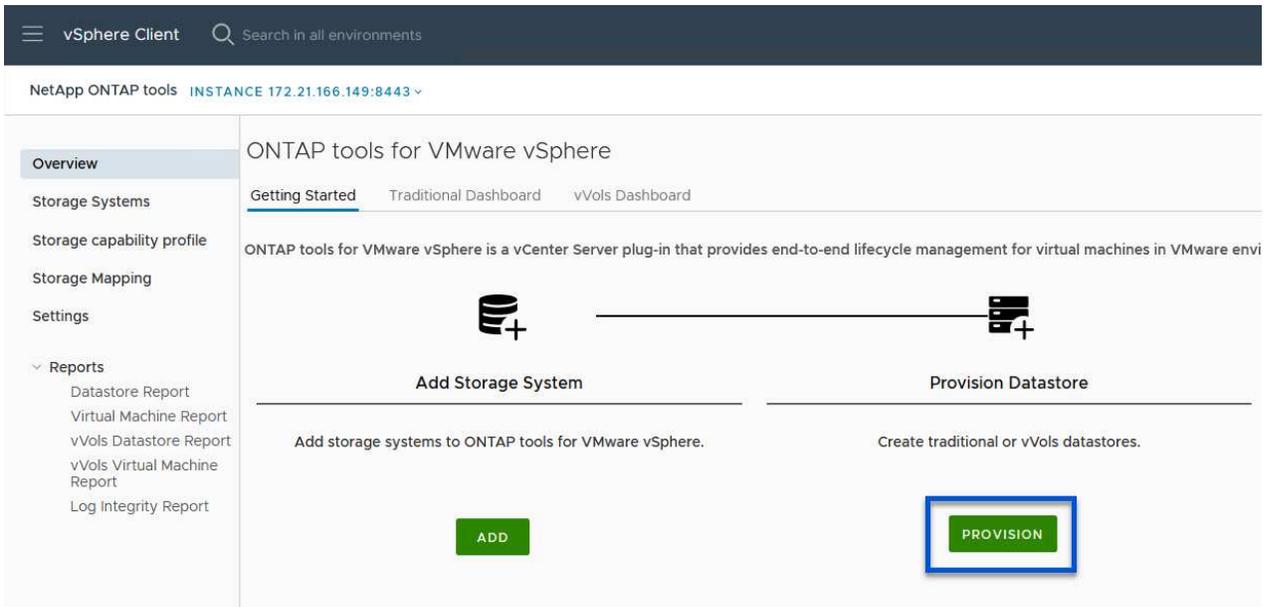
FINISH



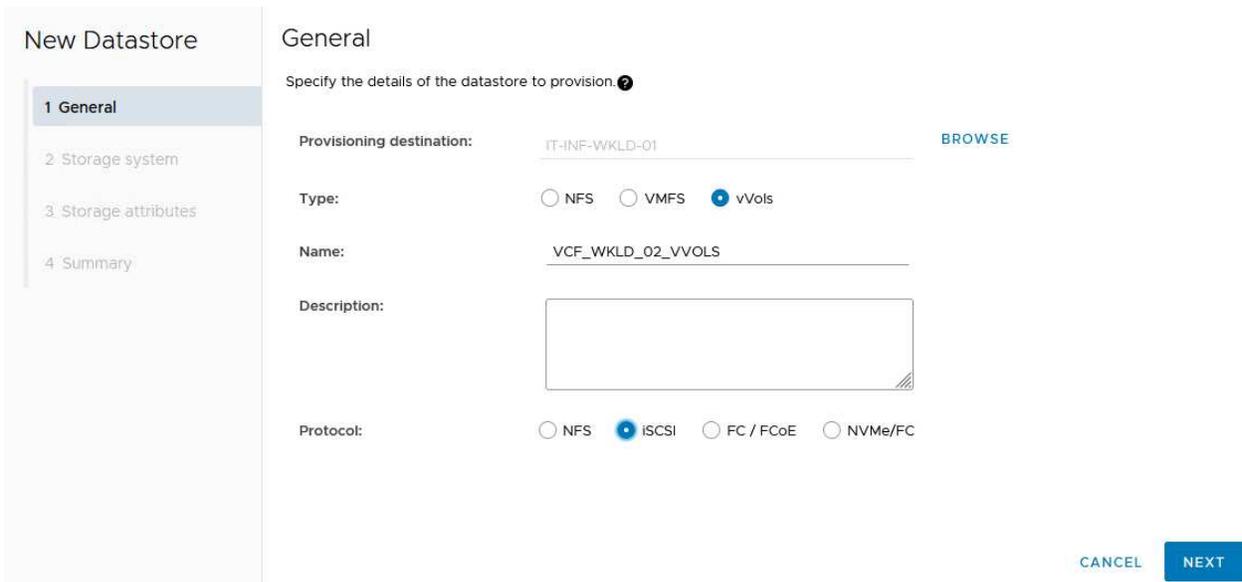
## Creare un datastore vVol in ONTAP Tools

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

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



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



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

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF\_Encrypted\_Min50\_ASA\_A
- FAS\_Default
- FAS\_Max20
- Custom profiles
- ASA\_Gold\_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF\_iSCSI

CANCEL BACK NEXT

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

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE)	Thin

ADD

CANCEL BACK NEXT

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

### New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Summary

**Datastore type:** vVols  
**Protocol:** iSCSI  
**Storage capability profile:** ASA\_Gold\_iSCSI

**Storage system details**

**Storage system:** ntaphci-a300e9u25  
**SVM:** VCF\_iSCSI

**Storage attributes**

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL
BACK
FINISH

## Ulteriori informazioni

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

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

## Configurare lo storage supplementare NVMe/TCP per i domini del carico di lavoro VCF

Autore: Josh Powell

### Configurare lo storage supplementare NVMe/TCP per i domini del carico di lavoro VCF

#### Panoramica dello scenario

In questo scenario, dimostreremo come configurare lo storage supplementare NVMe/TCP per un dominio di carico di lavoro VCF.

Questo scenario copre i seguenti passaggi di alto livello:

- Crea una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per il traffico NVMe/TCP.
- Creare gruppi di porte distribuite per le reti iSCSI nel dominio del carico di lavoro VI.
- Creare adattatori vmkernel per iSCSI sugli host ESXi per il dominio del carico di lavoro VI.
- Aggiungere adattatori NVMe/TCP sugli host ESXi.
- Implementa il datastore NVMe/TCP.

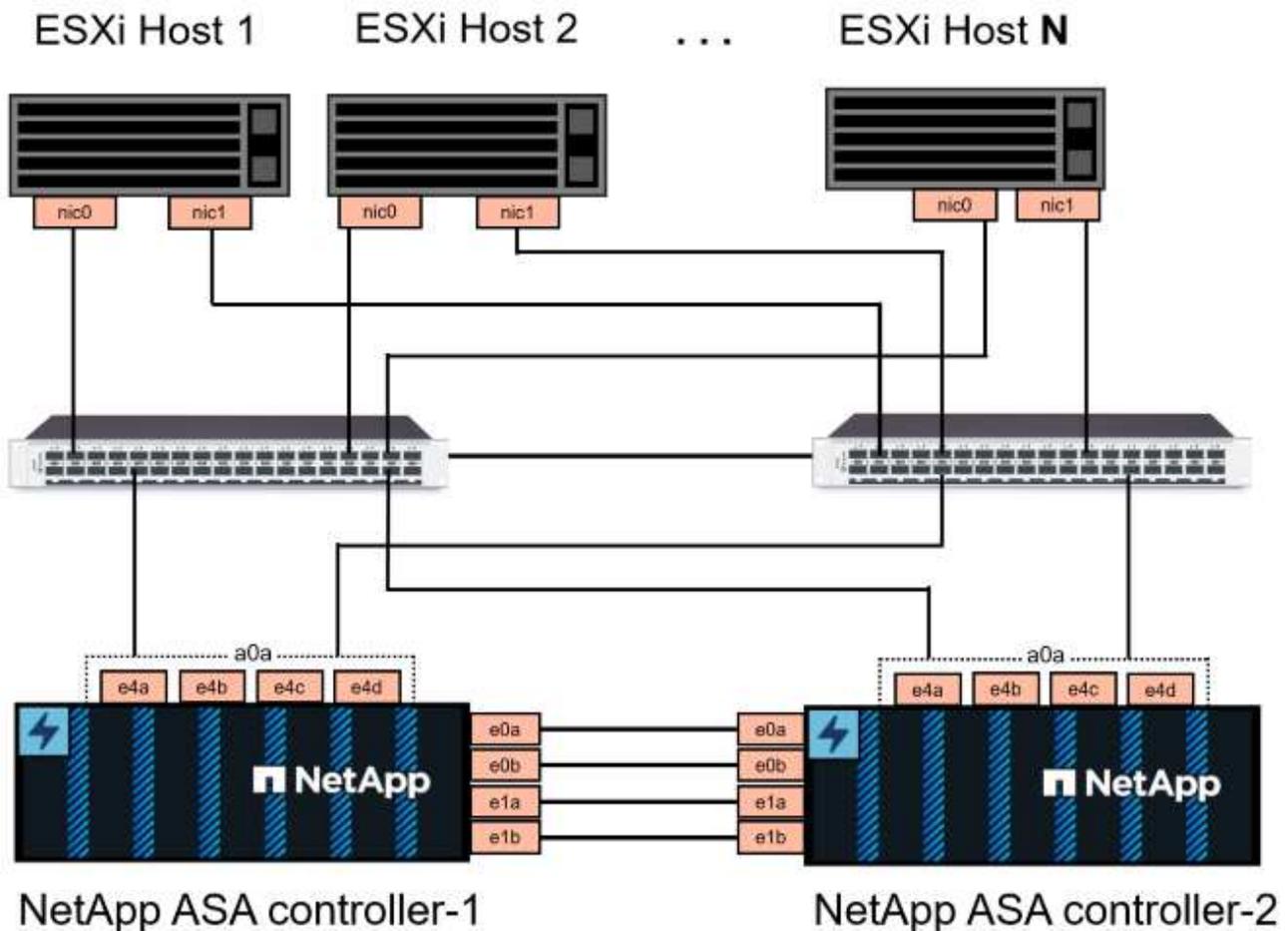
#### Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con porte per dati fisici su switch ethernet dedicati al traffico di storage.

- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.

NetApp consiglia design di rete completamente ridondanti per NVMe/TCP. Il diagramma seguente illustra un esempio di configurazione ridondante, che fornisce tolleranza agli errori per sistemi di archiviazione, switch, schede di rete e sistemi host. Consultare il NetApp ["Riferimento alla configurazione SAN"](#) per ulteriori informazioni.



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

Questa documentazione illustra il processo di creazione di una nuova SVM e specifica delle informazioni dell'indirizzo IP per creare LIF multipli per il traffico NVMe/TCP. Per aggiungere nuove LIF a una SVM esistente, fare riferimento a ["Creazione di una LIF \(interfaccia di rete\)"](#).

Per ulteriori informazioni sulle considerazioni sulla progettazione NVMe per i sistemi storage ONTAP, fare riferimento a ["Configurazione, supporto e limitazioni NVMe"](#).

### Fasi di implementazione

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

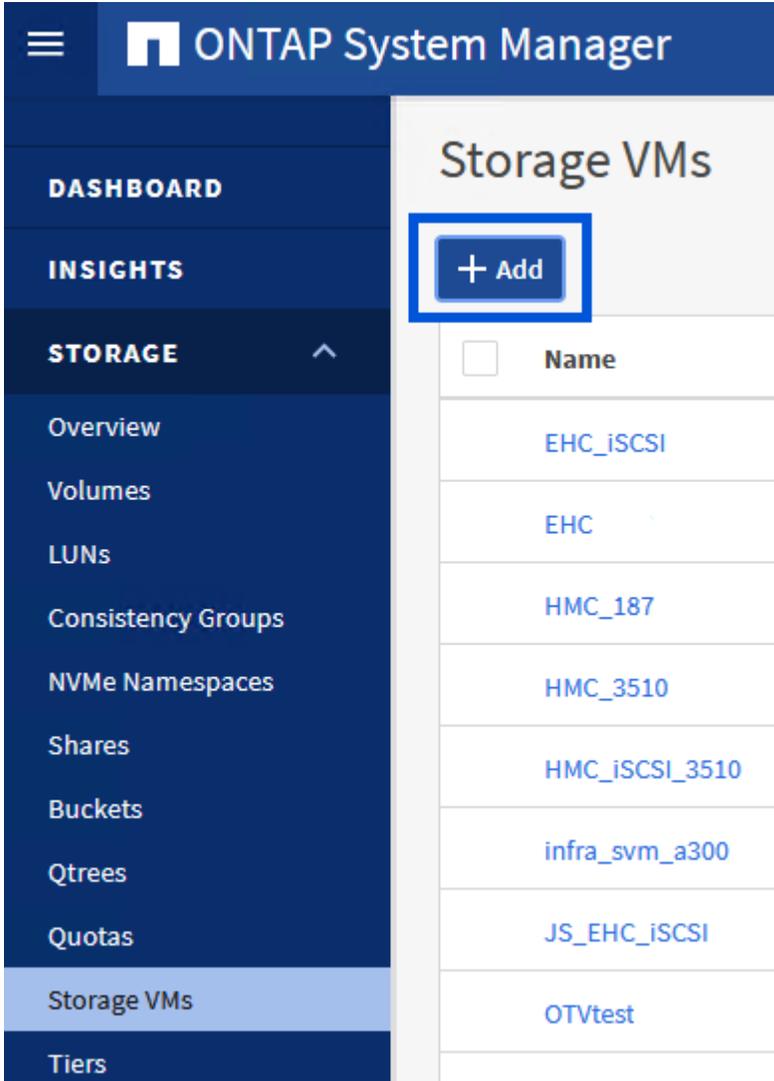
## **Crea SVM, LIF e namespace NVMe su un sistema storage ONTAP**

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

## Creazione di LIF e macchine virtuali storage

Completa i seguenti passaggi per creare una SVM insieme a LIF multipli per traffico NVMe/TCP.

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



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

## Add Storage VM



STORAGE VM NAME

VCF\_NVMe

IPSPACE

Default

### Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

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



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

## NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT 

NFS\_iSCSI 

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

IP ADDRESS

172.21.119.189

PORT

a0a-3375 

ntaphci-a300-02

IP ADDRESS

172.21.118.190

PORT

a0a-3374 

IP ADDRESS

172.21.119.190

PORT

a0a-3375 

## Storage VM Administration

Manage administrator account

Save

Cancel

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

## Storage VM Administration

Manage administrator account

Save

Cancel

## Creare il namespace NVMe

I namespace NVMe sono analoghi alle LUN per iSCSI o FC. È necessario creare il namespace NVMe prima di poter implementare un datastore VMFS da vSphere Client. Per creare il namespace NVMe, occorre prima ottenere il NVMe Qualified Name (NQN) da ogni host ESXi nel cluster. L'NQN viene utilizzato da ONTAP per fornire il controllo dell'accesso allo spazio dei nomi.

Completare i seguenti passaggi per creare un namespace NVMe:

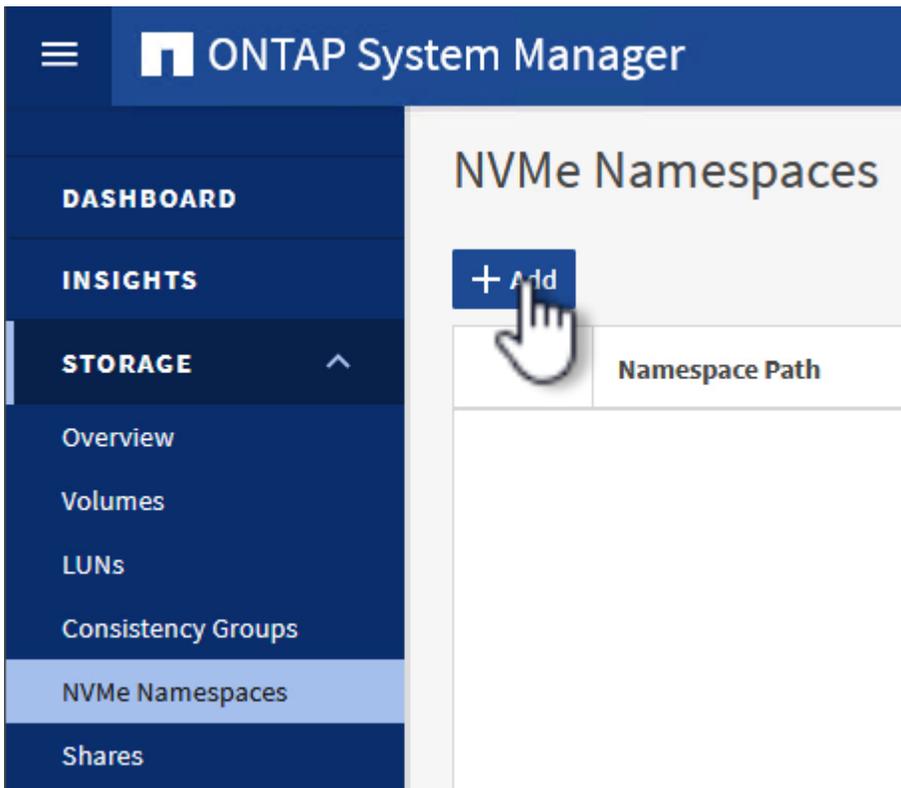
1. Aprire una sessione SSH con un host ESXi nel cluster per ottenere il proprio NQN. Utilizzare il seguente comando dall'interfaccia CLI:

```
esxcli nvme info get
```

Dovrebbe essere visualizzato un output simile al seguente:

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

2. Registrare l'NQN per ciascun host ESXi nel cluster
3. Da Gestione di sistema di ONTAP, accedere a **NVMe Namespaces** nel menu a sinistra e fare clic su **+ Aggiungi** per iniziare.

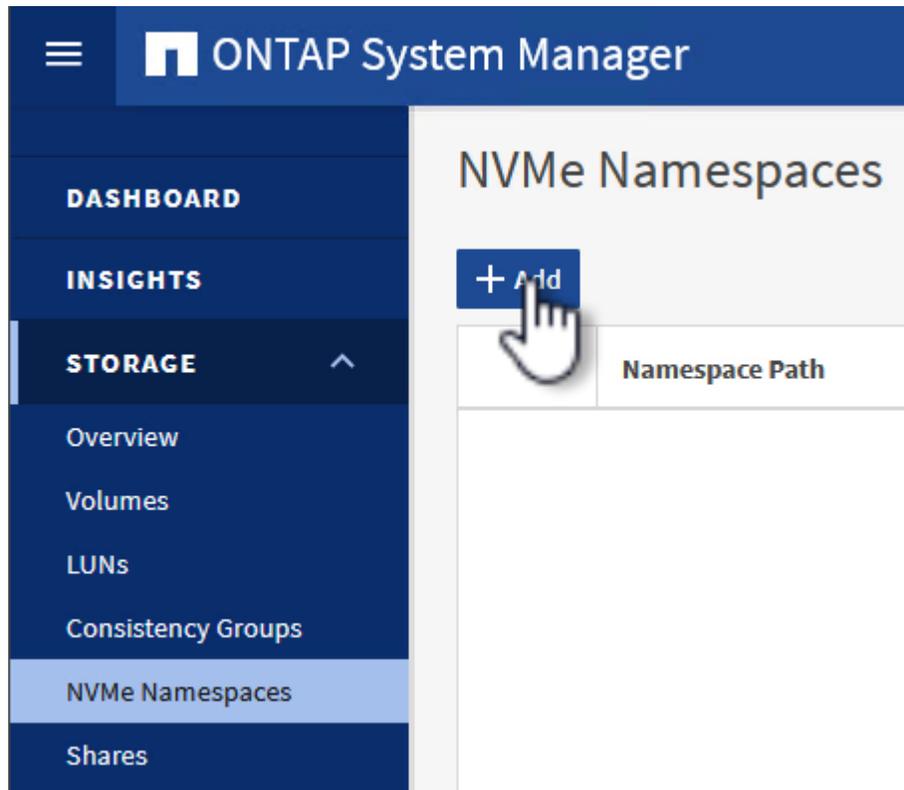


4. Nella pagina **Add NVMe Namespace**, inserire un prefisso nome, il numero di namespace da creare, le dimensioni dello spazio dei nomi e il sistema operativo host che accederà allo spazio dei nomi.

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

Fare clic su **altre opzioni** per configurare elementi aggiuntivi come il criterio di protezione delle istantanee. Infine, fare clic su **Save** per creare lo spazio dei nomi NVMe.

+



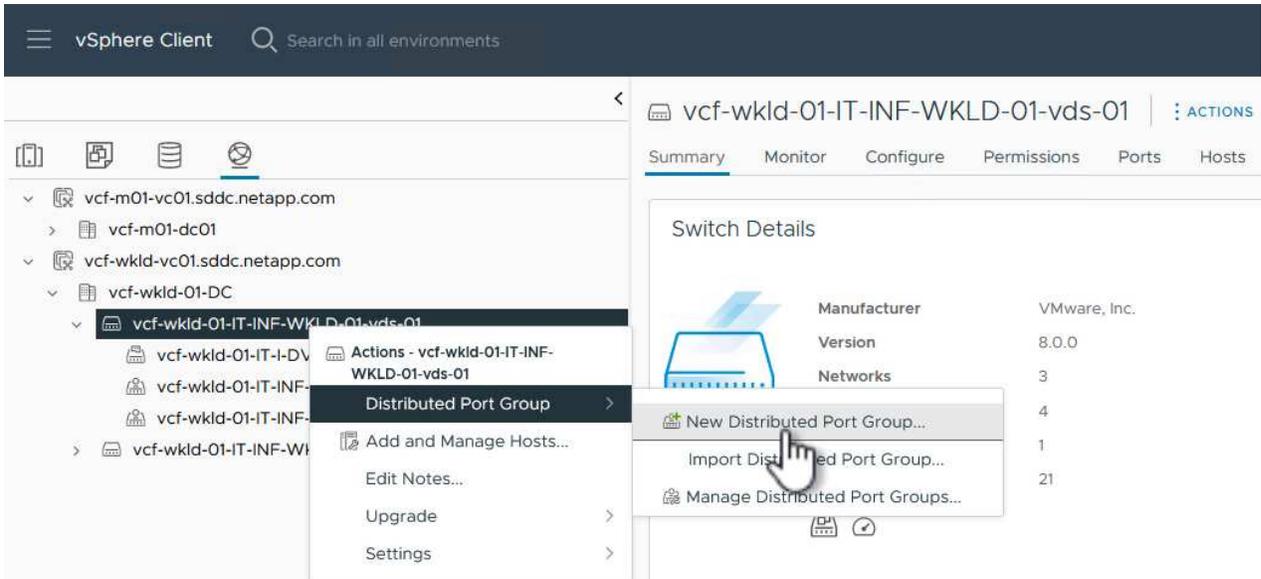
### Configurare le schede di rete e il software NVMe sugli host ESXi

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

## Creare gruppi di porte distribuite per il traffico NVMe/TCP

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

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



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

## New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

### Configure settings

Set general properties of the new port group.

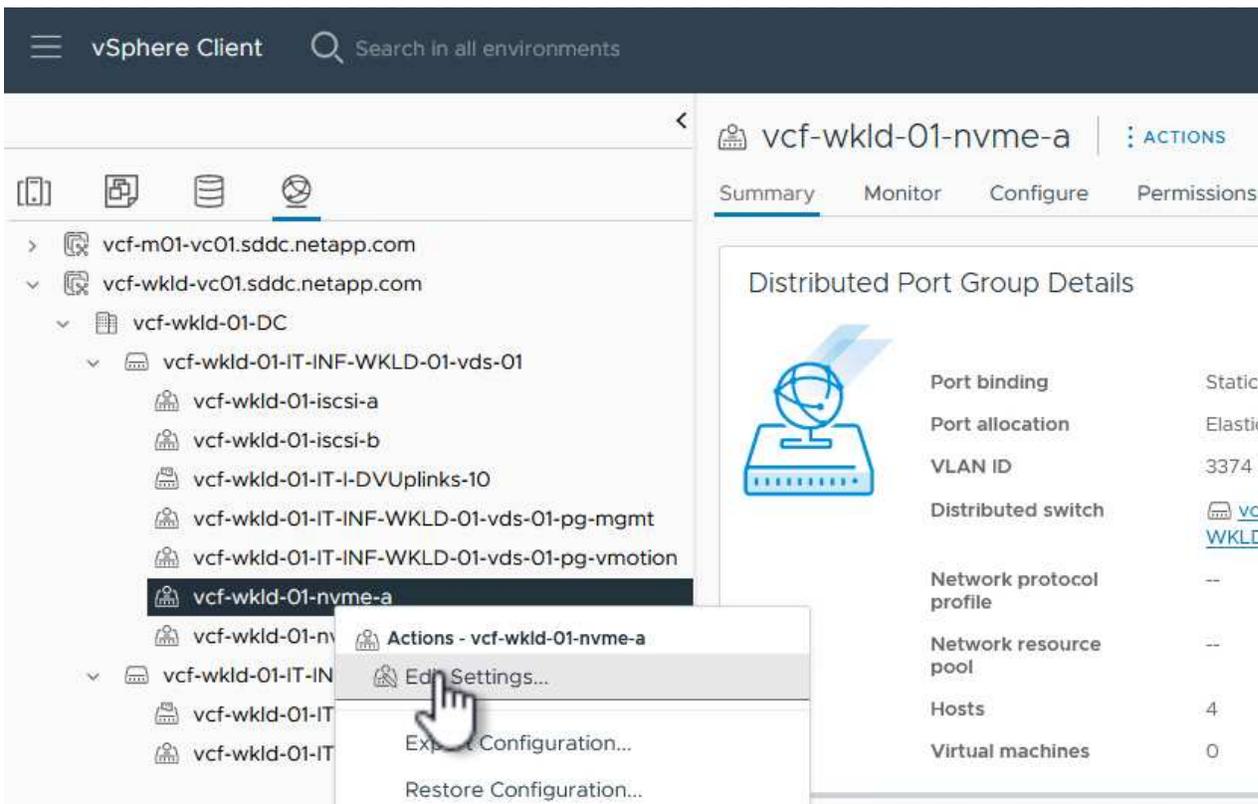
Port binding	Static binding
Port allocation	Elastic <span>?</span>
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

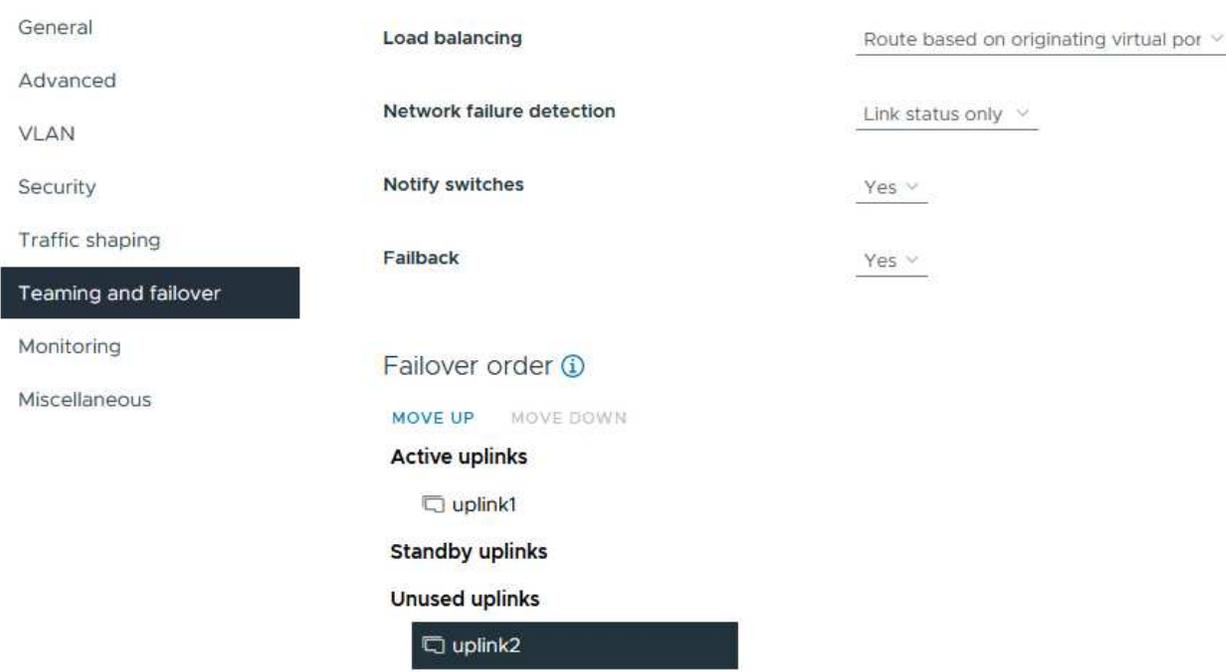
**NEXT**

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



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

### Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a



8. Ripetere questo passo per il secondo gruppo di porte NVMe/TCP. Tuttavia, questa volta si sposta

**uplink1** verso il basso in **uplink non utilizzati**.

## Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and fallover**

Monitoring

Miscellaneous

**Load balancing**

Route based on originating virtual por ▼

**Network failure detection**

Link status only ▼

**Notify switches**

Yes ▼

**Failback**

Yes ▼

Failover order ⓘ

[MOVE UP](#) [MOVE DOWN](#)

**Active uplinks**

uplink2

**Standby uplinks**

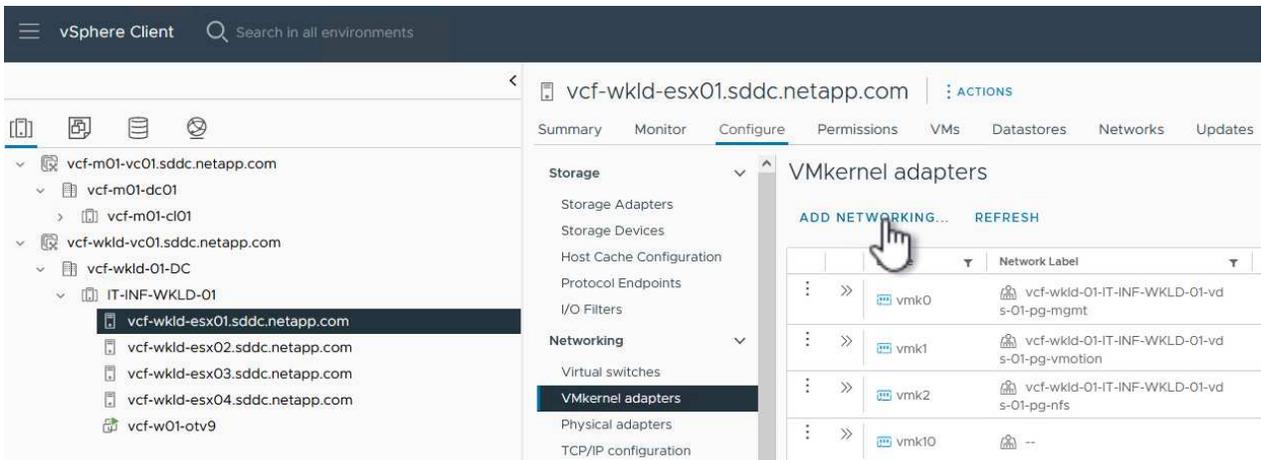
**Unused uplinks**

uplink1

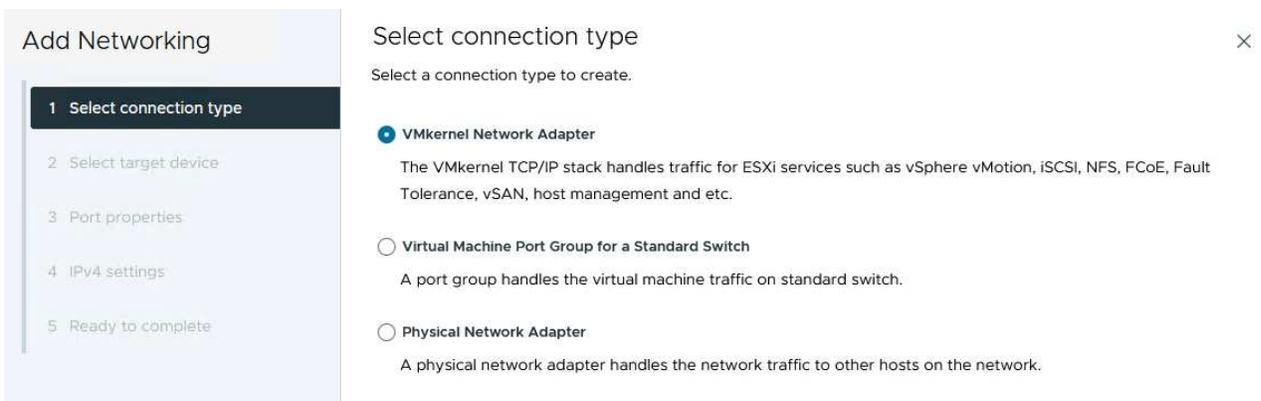
## Creare adattatori VMkernel su ciascun host ESXi

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

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



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



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

## 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"/>	 vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	 vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 7 Items

CANCEL

BACK

NEXT

Packages

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

### Port properties ✕

Specify VMkernel port settings.

**Network label**

**MTU**

**TCP/IP stack**

**Available services**

**Enabled services**

<input checked="" type="checkbox"/> vMotion	<input type="checkbox"/> vSphere Replication NFC	<input type="checkbox"/> NVMe over RDMA
<input type="checkbox"/> Provisioning	<input type="checkbox"/> vSAN	
<input type="checkbox"/> Fault Tolerance logging	<input type="checkbox"/> vSAN Witness	
<input type="checkbox"/> Management	<input type="checkbox"/> vSphere Backup NFC	
<input type="checkbox"/> vSphere Replication	<input checked="" type="checkbox"/> NVMe over TCP	

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**

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

## Add Networking

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

## Ready to complete

Review your selections before finishing the wizard

### ▼ Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

### ▼ Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

### ▼ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL

BACK

FINISH

Packages

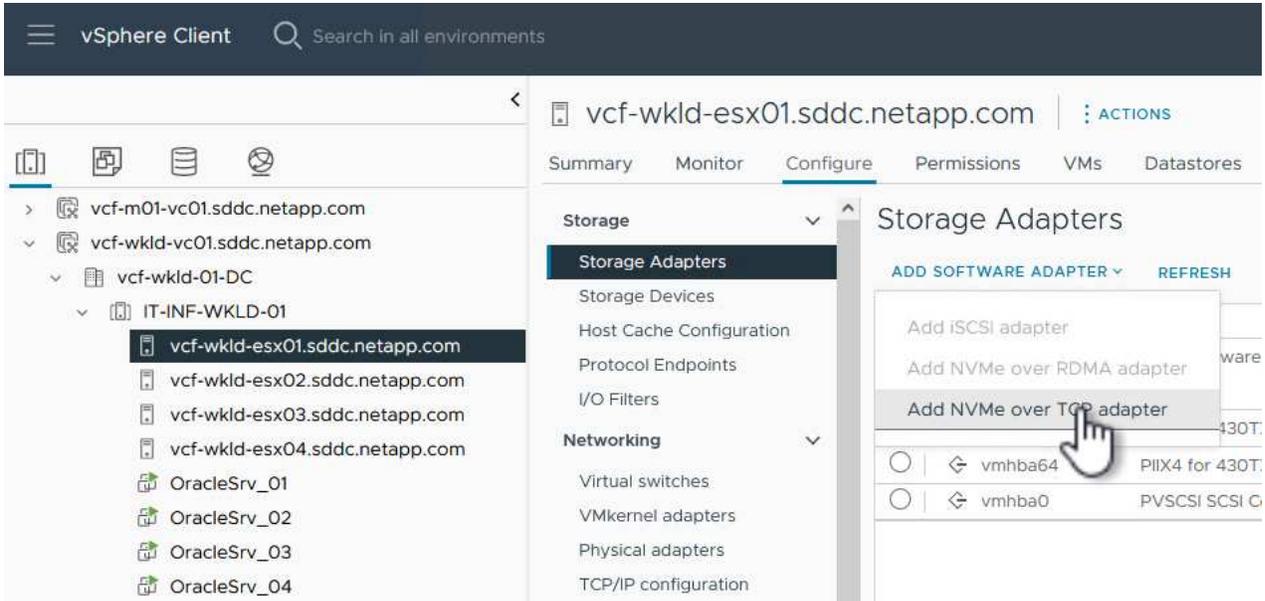
7. Ripetere questa procedura per creare un adattatore VMkernel per la seconda rete iSCSI.

## Aggiungi adattatore NVMe over TCP

Ogni host ESXi nel cluster del dominio del carico di lavoro deve avere installato un adattatore software NVMe over TCP per ogni rete NVMe/TCP consolidata dedicata al traffico storage.

Per installare gli adattatori NVMe over TCP e rilevare i controller NVMe, attenersi alla seguente procedura:

1. Nel client vSphere, accedere a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dalla scheda **Configure** (Configura), fare clic su **Storage Adapters** (schede di memoria) nel menu a discesa **Add Software Adapter** (Aggiungi scheda software) e selezionare **Add NVMe over TCP adapter** (Aggiungi scheda NVMe su TCP).



2. Nella finestra **Add Software NVMe over TCP adapter** (Aggiungi adattatore NVMe su TCP), accedere al menu a discesa **Physical Network Adapter** (scheda di rete fisica) e selezionare l'adattatore di rete fisico corretto su cui abilitare l'adattatore NVMe.

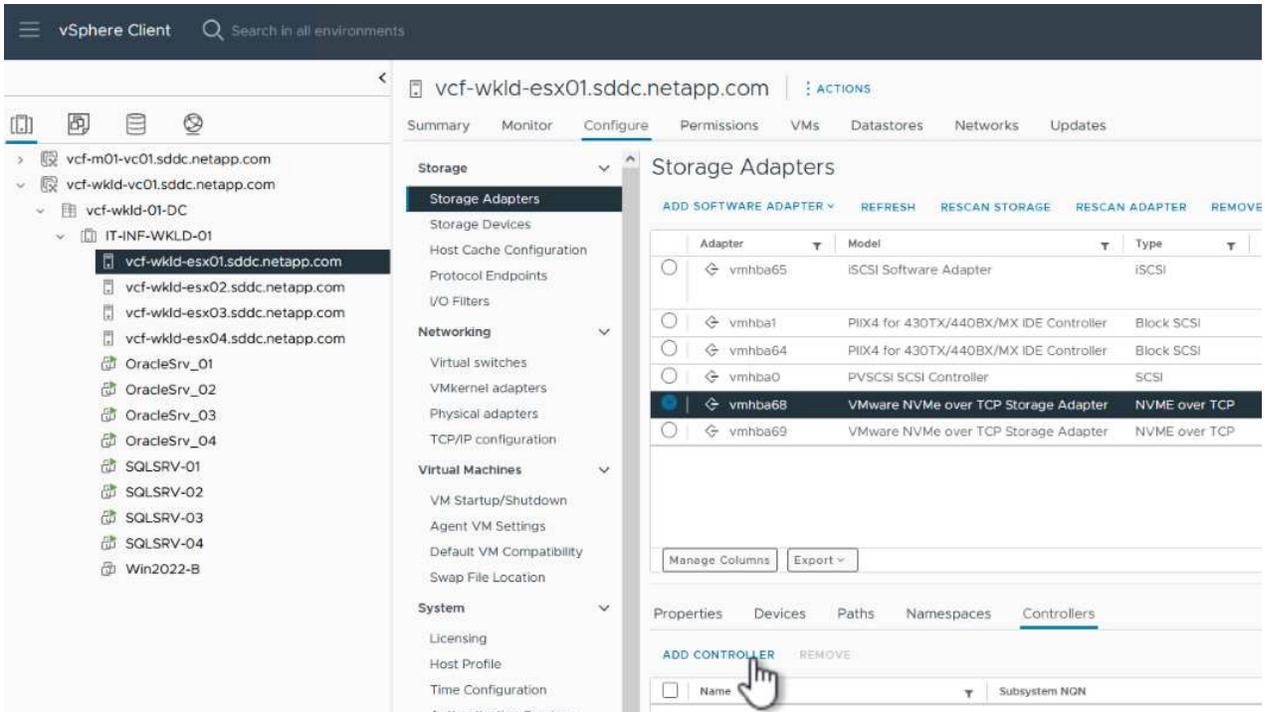
Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



3. Ripetere questa procedura per la seconda rete assegnata al traffico NVMe su TCP, assegnando l'adattatore fisico corretto.
4. Selezionare una delle schede NVMe over TCP appena installate e, nella scheda **Controller**, selezionare **Aggiungi controller**.



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

## Add controller | vmhba68



Automatically Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP

172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS

Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvme	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvme	172.21.118.190	4420

4 items

3

4

OK

6. Dopo qualche secondo dovresti vedere il namespace NVMe nella scheda Devices (dispositivi).

### Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(ign.1998-01.com.vmware:vcf-wkld-esx01.sddc.netapp.com:794177624:65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
<b>vmhba68</b>	<b>VMware NVMe over TCP Storage Adapter</b>	<b>NVMe over TCP</b>	<b>Online</b>	--	<b>1</b>	<b>1</b>	<b>1</b>
vmhba69	VMware NVMe over TCP Storage Adapter	NVMe over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties Devices Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

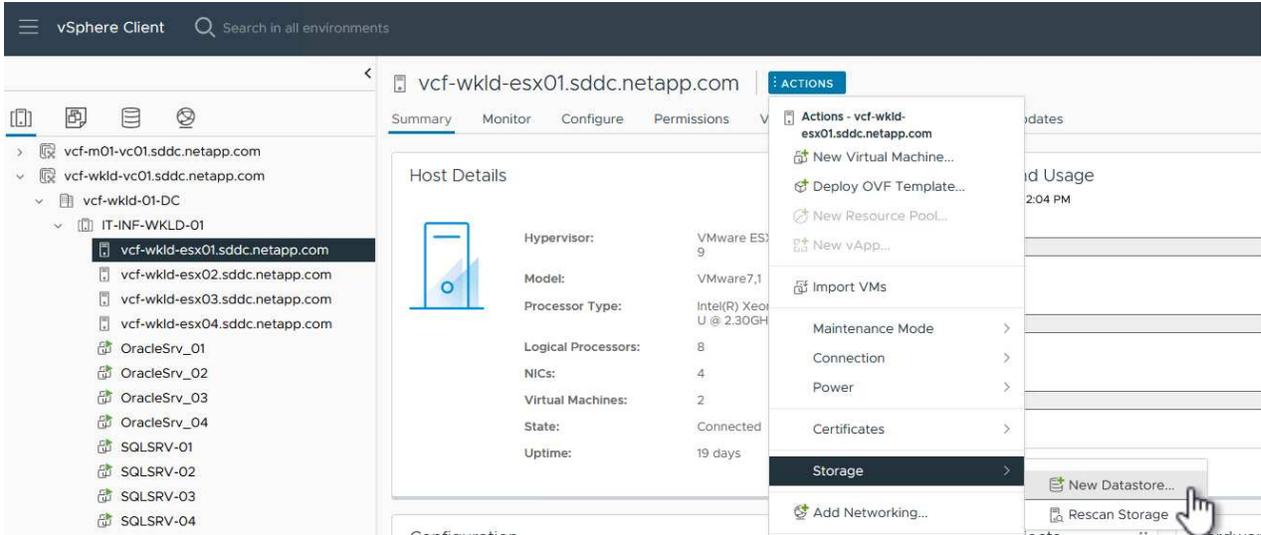
<input type="checkbox"/>	Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
<input type="checkbox"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPRTRAN

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

## Implementa datastore NVMe su TCP

Per creare un datastore VMFS nel namespace NVMe, completa i seguenti passaggi:

1. Nel client vSphere, accedere a uno degli host ESXi nel cluster del dominio del carico di lavoro. Dal menu **azioni**, selezionare **archiviazione > nuovo archivio dati....**



2. Nella procedura guidata **nuovo datastore**, selezionare **VMFS** come tipo. Fare clic su **Avanti** per continuare.
3. Nella pagina **selezione nome e dispositivo**, fornire un nome per l'archivio dati e selezionare lo spazio dei nomi NVMe dall'elenco dei dispositivi disponibili.

## New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

## Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name VCF\_WKLD\_04\_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V S
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcfe42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

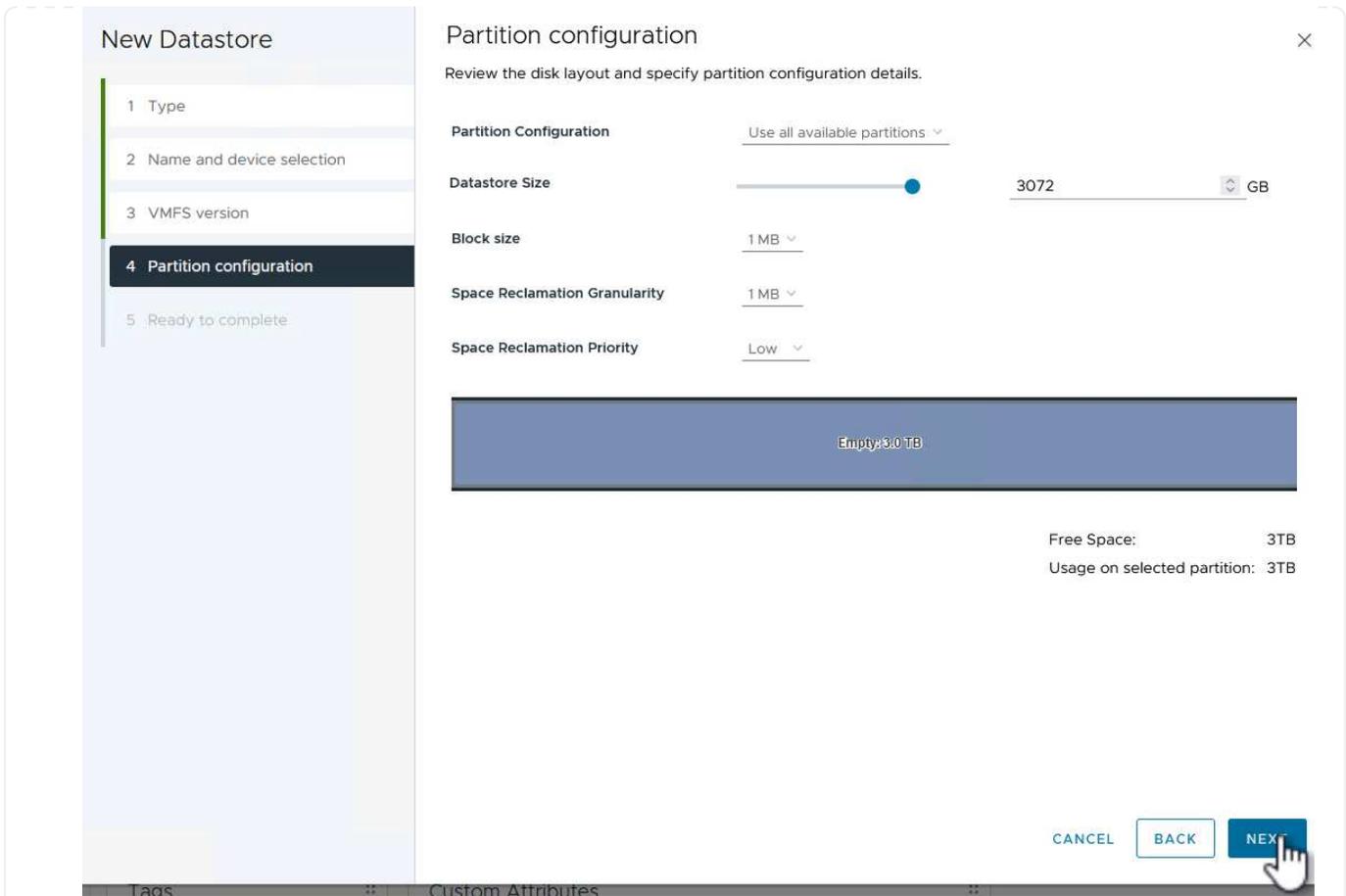
Manage Columns Export 3 items

CANCEL

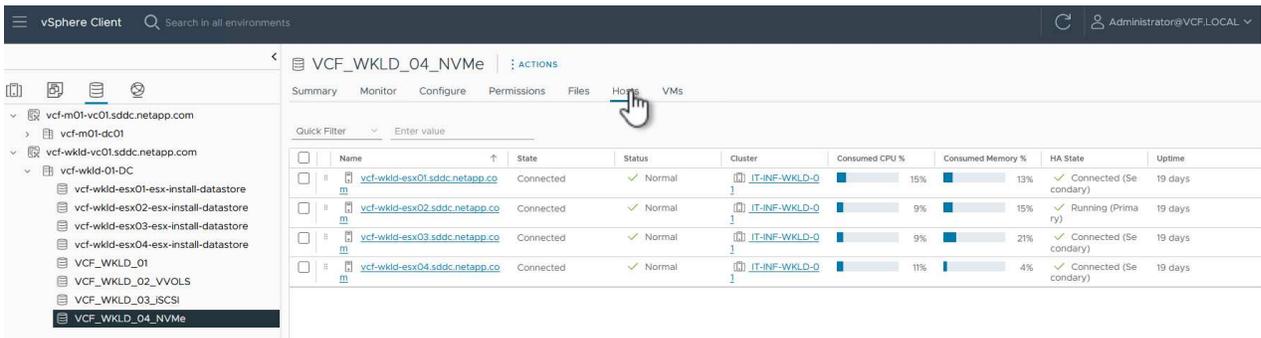
BACK

NEXT

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



6. Nella pagina **Pronto per il completamento**, rivedere il riepilogo e fare clic su **fine** per creare il datastore.
7. Accedere al nuovo datastore nell'inventario e fare clic sulla scheda **hosts**. Se configurato correttamente, tutti gli host ESXi nel cluster devono essere elencati e avere accesso al nuovo datastore.



## Ulteriori informazioni

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

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

## **Utilizza il plug-in SnapCenter per VMware vSphere per proteggere le VM nei domini del carico di lavoro VCF**

Autore: Josh Powell

**Utilizza il plug-in SnapCenter per VMware vSphere per proteggere le VM nei domini del carico di lavoro VCF**

### **Panoramica dello scenario**

In questo scenario dimostreremo come implementare e utilizzare il plug-in SnapCenter per VMware vSphere (SCV) per eseguire il backup e il ripristino di VM e datastore in un dominio di carico di lavoro VCF. SCV utilizza la tecnologia Snapshot di ONTAP per eseguire copie di backup veloci ed efficienti dei volumi di storage ONTAP che ospitano i datastore vSphere. Le tecnologie SnapMirror e SnapVault vengono utilizzate per creare backup secondari su un sistema storage separato e con policy di conservazione che simulano il volume originale o possono essere indipendenti dal volume originale per la conservazione a lungo termine.

**ISCSI** viene utilizzato come protocollo storage per il datastore VMFS in questa soluzione.

Questo scenario copre i seguenti passaggi di alto livello:

- Distribuire il plug-in SnapCenter per VMware vSphere (SCV) nel dominio del carico di lavoro VI.
- Aggiungere i sistemi di stoccaggio al distributore idraulico.
- Creare criteri di backup in SCV.
- Creare gruppi di risorse in SCV.
- Utilizzare SCV per eseguire il backup di datastore o macchine virtuali specifiche.
- Utilizzare SCV per ripristinare le macchine virtuali in una posizione alternativa nel quadro strumenti.
- Utilizzare SCV per ripristinare i file in un file system Windows.

### **Prerequisiti**

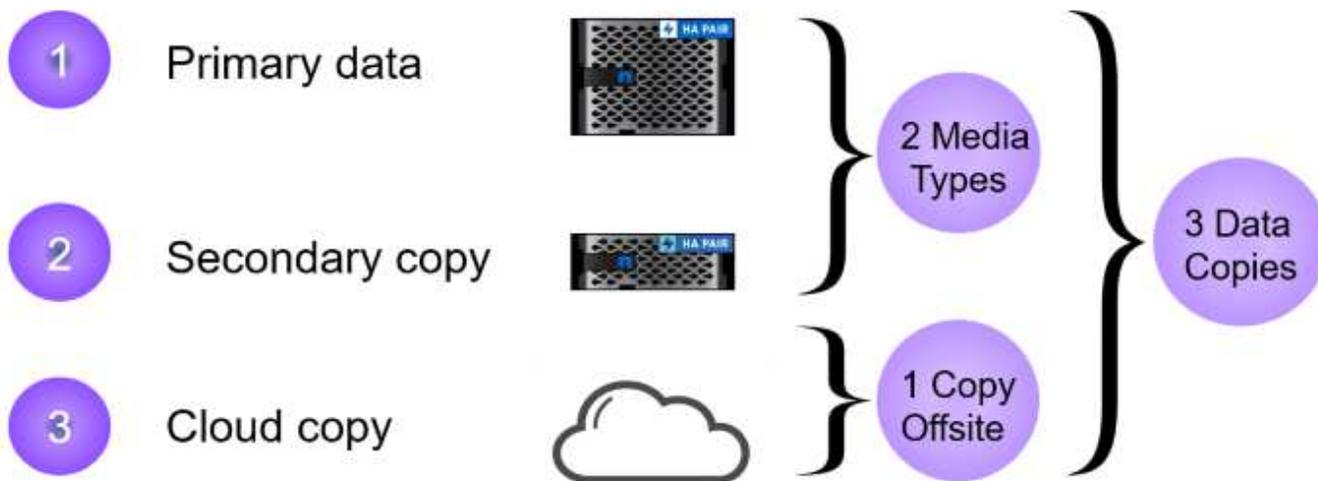
Questo scenario richiede i seguenti componenti e configurazioni:

- Un sistema di storage ONTAP ASA con archivi dati VMFS iSCSI allocati al cluster di dominio del carico di lavoro.
- Un sistema di storage ONTAP secondario configurato per ricevere backup secondari utilizzando SnapMirror.
- La distribuzione del dominio di gestione VCF è stata completata e il client vSphere è accessibile.
- Un dominio del carico di lavoro VI è stato distribuito in precedenza.
- Le macchine virtuali sono presenti sul gruppo SCV è designato come protezione.

Per informazioni sulla configurazione degli archivi dati VMFS iSCSI come storage supplementare, fare riferimento a. ["ISCSI come archiviazione supplementare per i domini di gestione"](#) ivi descritti. Il processo per utilizzare OTV per implementare i datastore è identico per i domini di gestione e carico di lavoro.



Oltre alla replica dei backup eseguiti con SCV nello storage secondario, è possibile realizzare copie offsite dei dati nello storage a oggetti su uno dei tre (3) cloud provider leader, utilizzando il backup e recovery di NetApp BlueXP per le VM. Per ulteriori informazioni, consultare la soluzione ["Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM"](#).



### Fasi di implementazione

Per implementare il plug-in SnapCenter e utilizzarlo per creare backup e ripristinare macchine virtuali e datastore, attenersi alla seguente procedura:

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

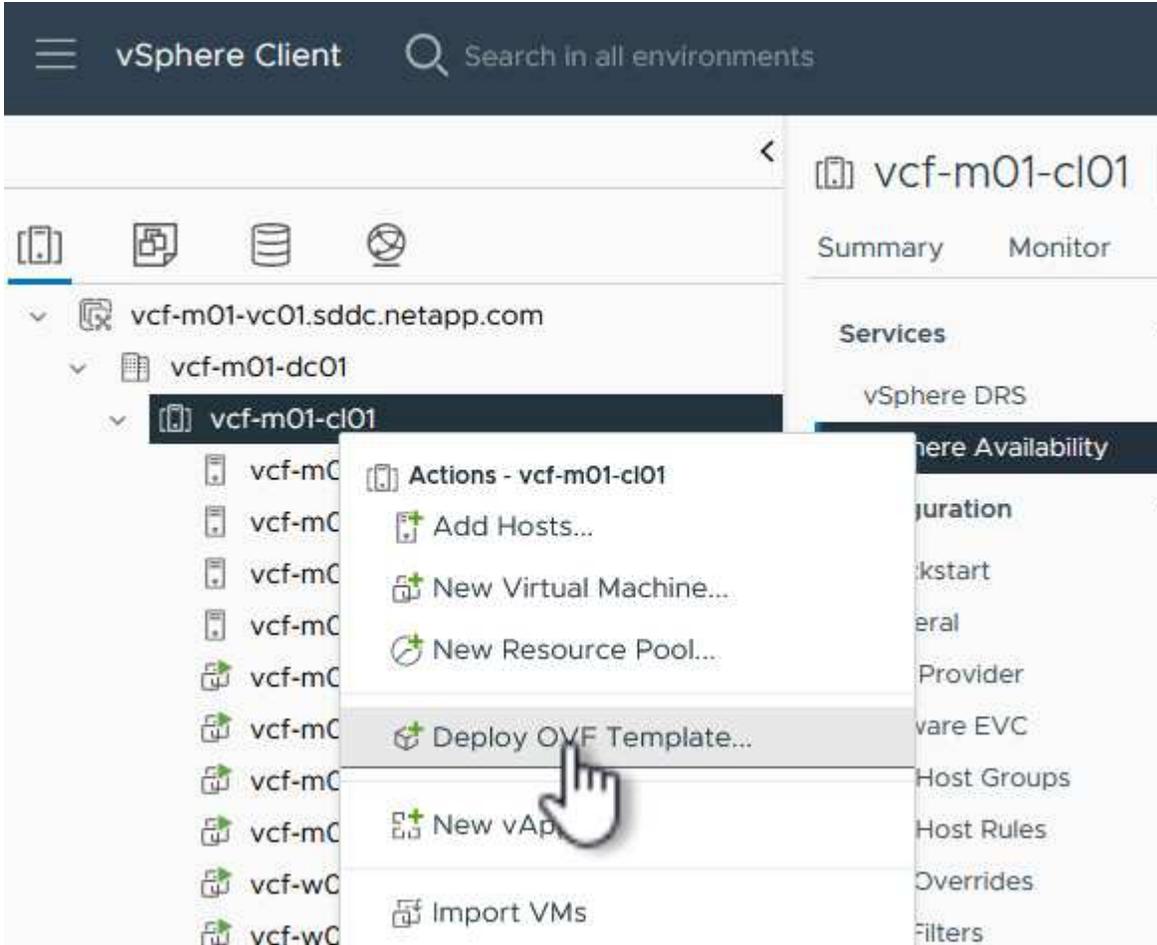
Completare i seguenti passaggi per distribuire, configurare e utilizzare SCV per proteggere i dati in un dominio del carico di lavoro VI:

## Implementa il plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter è ospitato nel dominio di gestione VCF ma registrato in vCenter per il dominio del carico di lavoro VI. È necessaria un'istanza SCV per ciascuna istanza di vCenter e, tenere presente che un dominio del carico di lavoro può includere cluster multipli gestiti da una singola istanza di vCenter.

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

1. Scaricare il file OVA per l'implementazione dei distributori idraulici dall'area di download del sito di assistenza NetApp "QUI".
2. Dal client vCenter del dominio di gestione, selezionare **Deploy OVF Template...**



3. Nella procedura guidata **Deploy OVF Template**, fare clic sul pulsante di opzione **Local file**, quindi selezionare per caricare il modello OVF scaricato in precedenza. Fare clic su **Avanti** per continuare.

## 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

scv-5.OP2-240310\_1514.ova

4. Nella pagina **Select name and folder** (Seleziona nome e cartella\*), fornire un nome per la VM del broker di dati SCV e una cartella nel dominio di gestione. Fare clic su **Avanti** per continuare.
5. Nella pagina **selezionare una risorsa di calcolo**, selezionare il cluster del dominio di gestione o l'host ESXi specifico all'interno del cluster in cui installare la VM.
6. Esaminare le informazioni relative al modello OVF nella pagina **Dettagli revisione** e accettare i termini di licenza nella pagina **contratti di licenza**.
7. Nella pagina **Select storage** (Seleziona storage), scegliere il datastore in cui verrà installata la macchina virtuale e selezionare **virtual disk format** (formato disco virtuale) e **VM Storage Policy** (criterio archiviazione VM). In questa soluzione, la macchina virtuale verrà installata in un datastore VMFS iSCSI situato in un sistema storage ONTAP, come precedentemente implementato in una sezione separata di questa documentazione. Fare clic su **Avanti** per continuare.

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

## 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	
<input checked="" type="radio"/> mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	
<input type="radio"/> vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 GB	
<input type="radio"/> vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	

Manage Columns Items per page: 10 6 items

### Compatibility

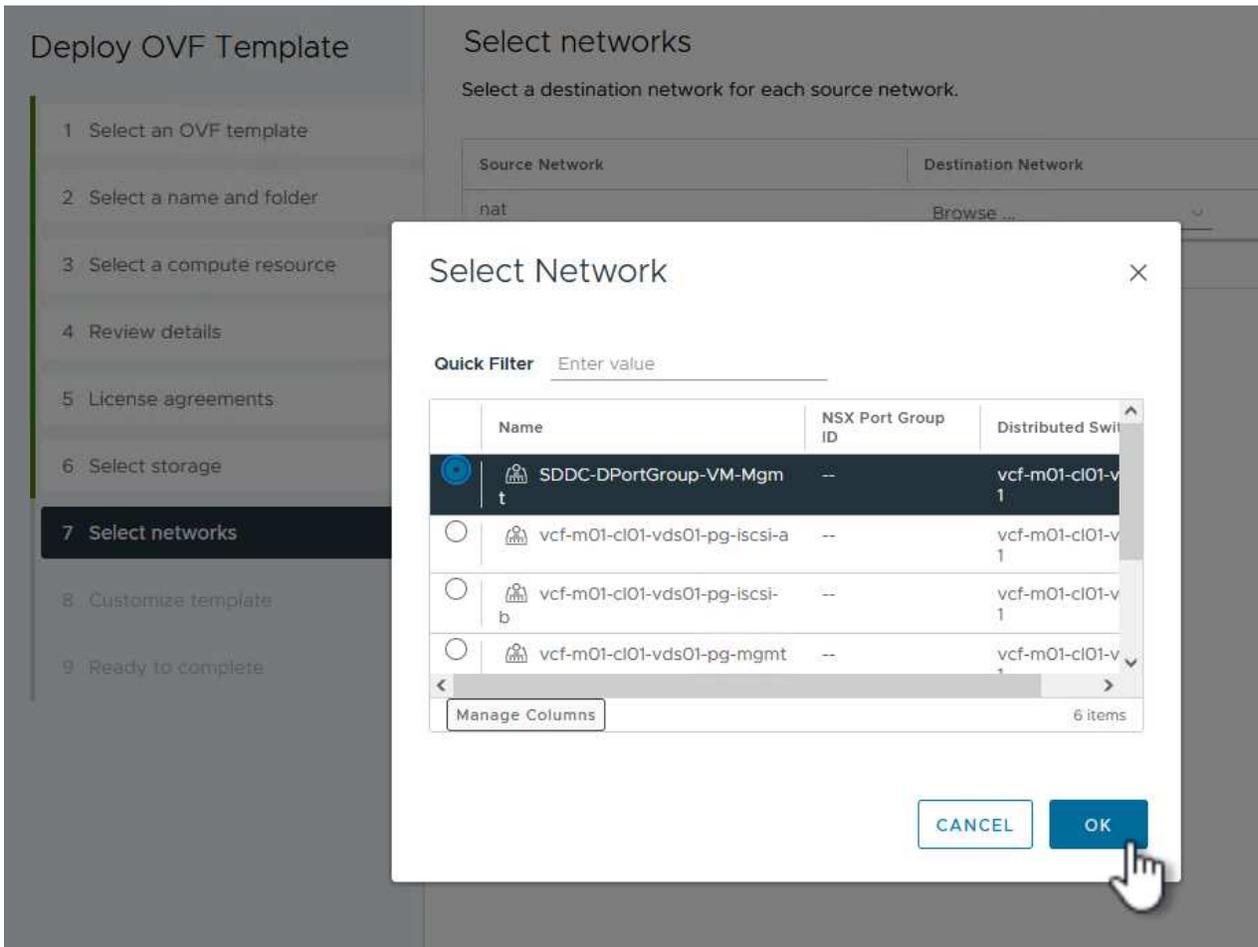
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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



9. Nella pagina **Personalizza modello** compilare tutte le informazioni necessarie per la distribuzione:

- FQDN o IP e credenziali per l'appliance vCenter del dominio del carico di lavoro.
- Credenziali per l'account amministrativo SCV.
- Credenziali per l'account di manutenzione SCV.
- IPv4 informazioni dettagliate sulle proprietà di rete (è possibile utilizzare anche IPv6).
- Impostazioni di data e ora.

Fare clic su **Avanti** per continuare.

## Deploy OVF Template

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

## Customize template

Customize the deployment properties of this software solution.

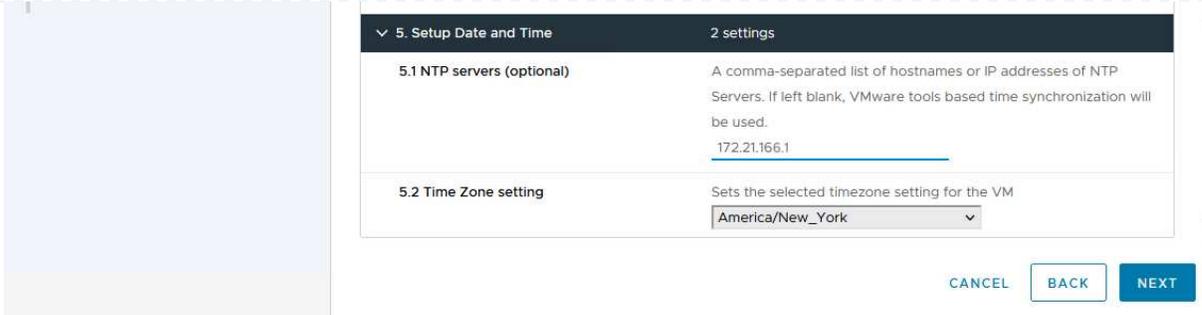
<b>1. Register to existing vCenter</b>		4 settings
1.1 vCenter Name(FQDN) or IP Address	<input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>	
1.2 vCenter username	<input type="text" value="administrator@vcf.local"/>	
1.3 vCenter password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
1.4 vCenter port	<input type="text" value="443"/>	
<b>2. Create SCV Credentials</b>		2 settings
2.1 Username	<input type="text" value="admin"/>	
2.2 Password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
<b>3. System Configuration</b>		1 settings

## Deploy OVF Template

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

## Customize template

<b>4.2 Setup IPv4 Network Properties</b>		6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.148"/>	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/>	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/>	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/>	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="10.61.186.231"/>	
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) <input type="text" value="netapp.com,sddc.netapp.com"/>	
<b>3.3 Setup IPv6 Network Properties</b>		6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/>	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/>	

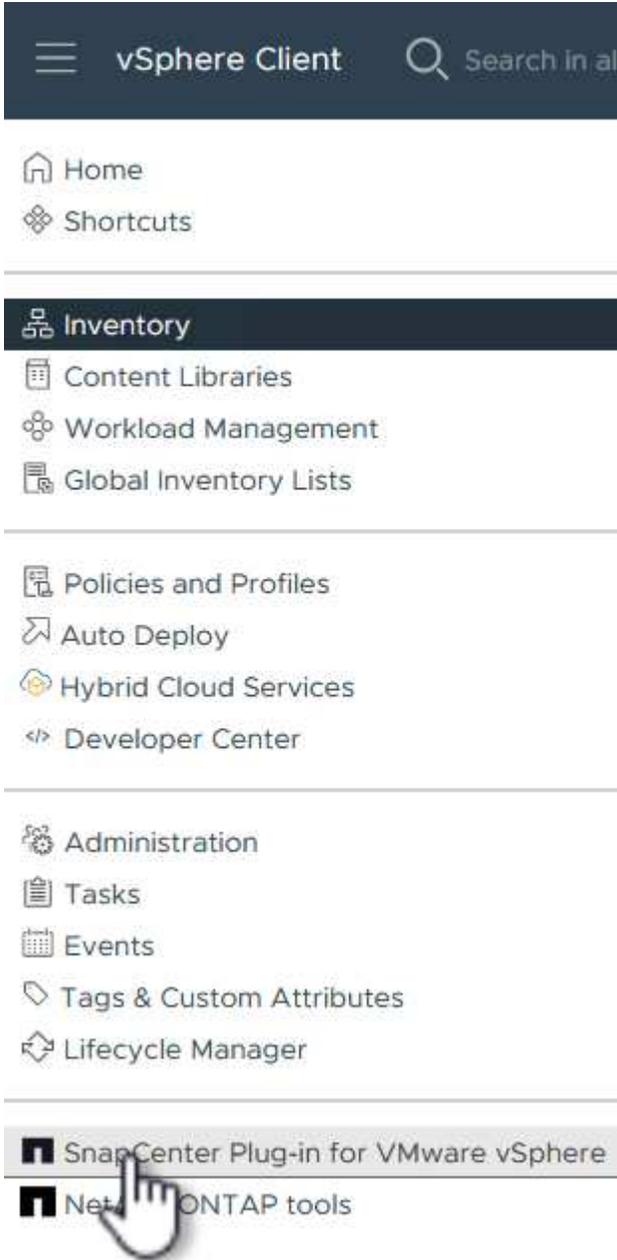


10. Infine, nella pagina **Pronto per il completamento**, esaminare tutte le impostazioni e fare clic su fine per avviare la distribuzione.

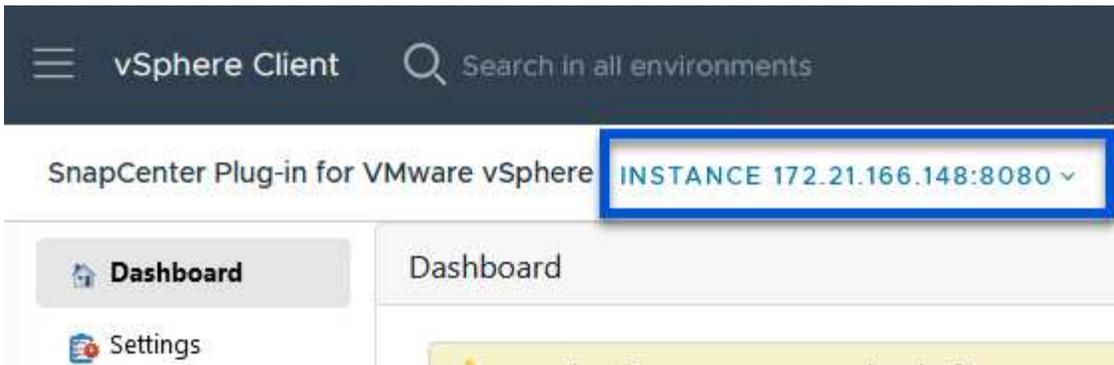
## Aggiungere i sistemi di stoccaggio al distributore idraulico

Una volta installato il plug-in SnapCenter, completare i seguenti passaggi per aggiungere i sistemi di stoccaggio al distributore idraulico:

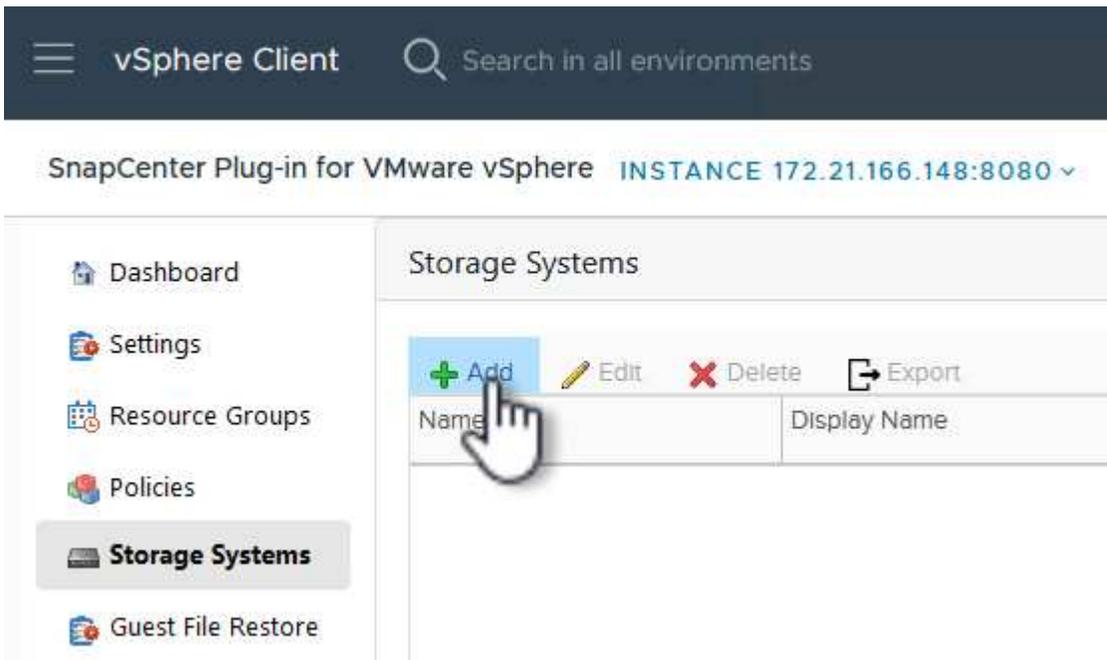
1. SCV è accessibile dal menu principale di vSphere Client.



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



3. Accedere a **Storage Systems** nel menu a sinistra e fare clic su **Add** per iniziare.



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

## Add Storage System



Storage System	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

### Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system



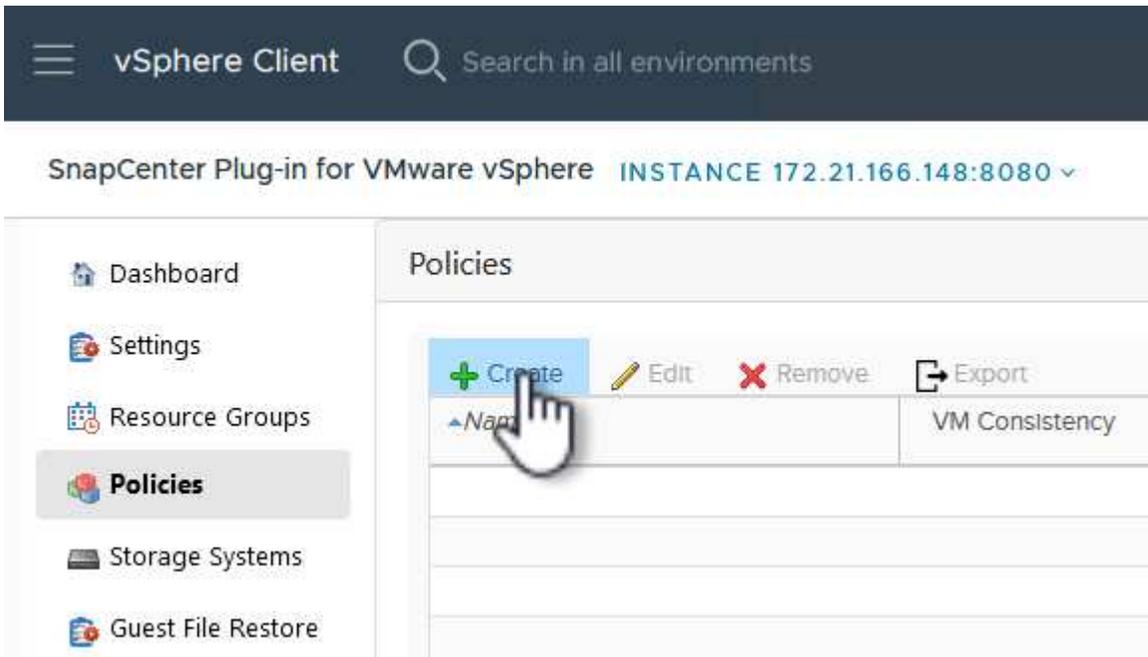
5. Ripetere questa procedura per tutti i sistemi di storage aggiuntivi da gestire, inclusi tutti i sistemi da utilizzare come destinazioni di backup secondarie.

## Configurare i criteri di backup in SCV

Per ulteriori informazioni sulla creazione delle politiche di backup dei distributori idraulici, fare riferimento a ["Creare policy di backup per macchine virtuali e datastore"](#).

Completare i seguenti passaggi per creare un nuovo criterio di backup:

1. Dal menu a sinistra, selezionare **Policies** e fare clic su **Create** per iniziare.



2. Nel modulo **Nuova policy di backup**, fornire un **Nome** e **Descrizione** per il criterio, la **frequenza** in cui verranno eseguiti i backup e il periodo **conservazione** che specifica la durata di conservazione del backup.

**Periodo di blocco** abilita la funzione ONTAP SnapLock per creare istantanee antimanomissione e consente la configurazione del periodo di blocco.

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



Le repliche di SnapMirror e SnapVault sono simili in quanto utilizzano la tecnologia ONTAP SnapMirror per replicare in modo asincrono i volumi storage in un sistema storage secondario, per una maggiore protezione e sicurezza. Per le relazioni di SnapMirror, il programma di conservazione specificato nella politica di backup dei distributori idraulici regolerà la conservazione per il volume primario e secondario. Con le relazioni di SnapVault, è possibile stabilire un piano di conservazione separato sul sistema di storage secondario per pianificazioni di conservazione a lungo termine o diverse. In questo caso, l'etichetta dell'istantanea viene specificata nella politica di backup dei distributori idraulici e nella politica associata al volume secondario, per identificare i volumi a cui applicare la pianificazione di conservazione indipendente.

Scegliere eventuali opzioni avanzate aggiuntive e fare clic su **Aggiungi** per creare il criterio.

# New Backup Policy



**Name**

**Description**

**Frequency**

**Locking Period**  Enable Snapshot Locking ⓘ

**Retention**   ⓘ

**Replication**  Update SnapMirror after backup ⓘ

Update SnapVault after backup ⓘ

Snapshot label

**Advanced** ▾

VM consistency ⓘ

Include datastores with independent disks

**Scripts** ⓘ

CANCEL

ADD

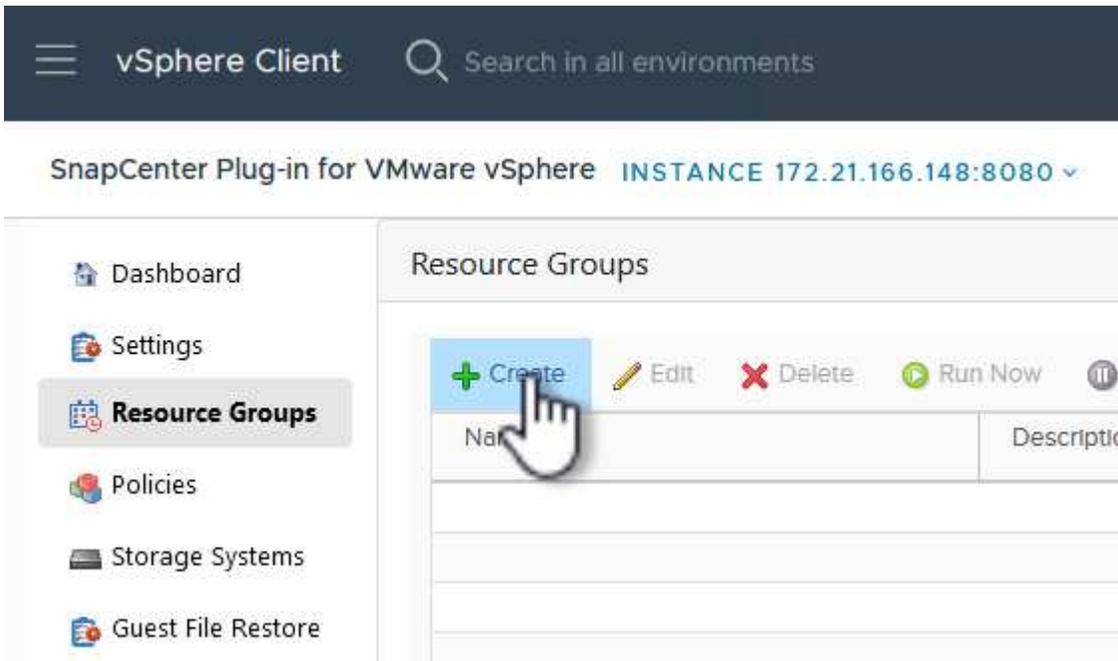


## Creare gruppi di risorse in SCV

Per ulteriori informazioni sulla creazione di gruppi di risorse SCV, fare riferimento a ["Creare gruppi di risorse"](#).

Completare i seguenti passaggi per creare un nuovo gruppo di risorse:

1. Dal menu a sinistra, selezionare **gruppi di risorse** e fare clic su **Crea** per iniziare.



2. Nella pagina **informazioni generali e notifica**, fornire un nome per il gruppo di risorse, le impostazioni di notifica e le eventuali opzioni aggiuntive per la denominazione delle istantanee.
3. Nella pagina **risorsa** selezionare gli archivi dati e le VM da proteggere nel gruppo di risorse. Fare clic su **Avanti** per continuare.



Anche quando sono selezionate solo macchine virtuali specifiche, viene sempre eseguito il backup dell'intero datastore. Ciò è dovuto al fatto che ONTAP crea snapshot del volume che ospita il datastore. Tuttavia, la selezione solo di macchine virtuali specifiche per il backup limita la possibilità di ripristino solo a queste macchine virtuali.

## Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF\_WKLD\_03\_iSCSI

Enter available entity name

Available entities

OracleSrv\_01  
OracleSrv\_02  
OracleSrv\_03  
OracleSrv\_04

Selected entities

SQLSRV-01  
SQLSRV-02  
SQLSRV-03  
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

4. Nella pagina **dischi di spanning** selezionare l'opzione per la gestione delle macchine virtuali con VMDK che coprono più archivi dati. Fare clic su **Avanti** per continuare.

## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK

NEXT

FINISH

CANCEL

5. Nella pagina **Criteri**, selezionare uno o più criteri creati in precedenza da utilizzare con questo gruppo di risorse. Fare clic su **Avanti** per continuare.



## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily\_Snapmi... ▼

Type Daily

Every 1 Day(s)

Starting 04/04/2024

At 04 45 PM

BACK

NEXT

FINISH

CANCEL

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

## Create Resource Group

- 1. General info & notification
- 2. Resource
- 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary**

Name	SQL_Servers						
Description							
Send email	Never						
Latest Snapshot name	None ⓘ						
Custom snapshot format	None ⓘ						
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04						
Spanning	False						
Policies	<table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>Daily_Snapmir...</td><td>Daily</td><td>-</td></tr></tbody></table>	Name	Frequency	Snapshot Locking Period	Daily_Snapmir...	Daily	-
Name	Frequency	Snapshot Locking Period					
Daily_Snapmir...	Daily	-					

BACK

NEXT

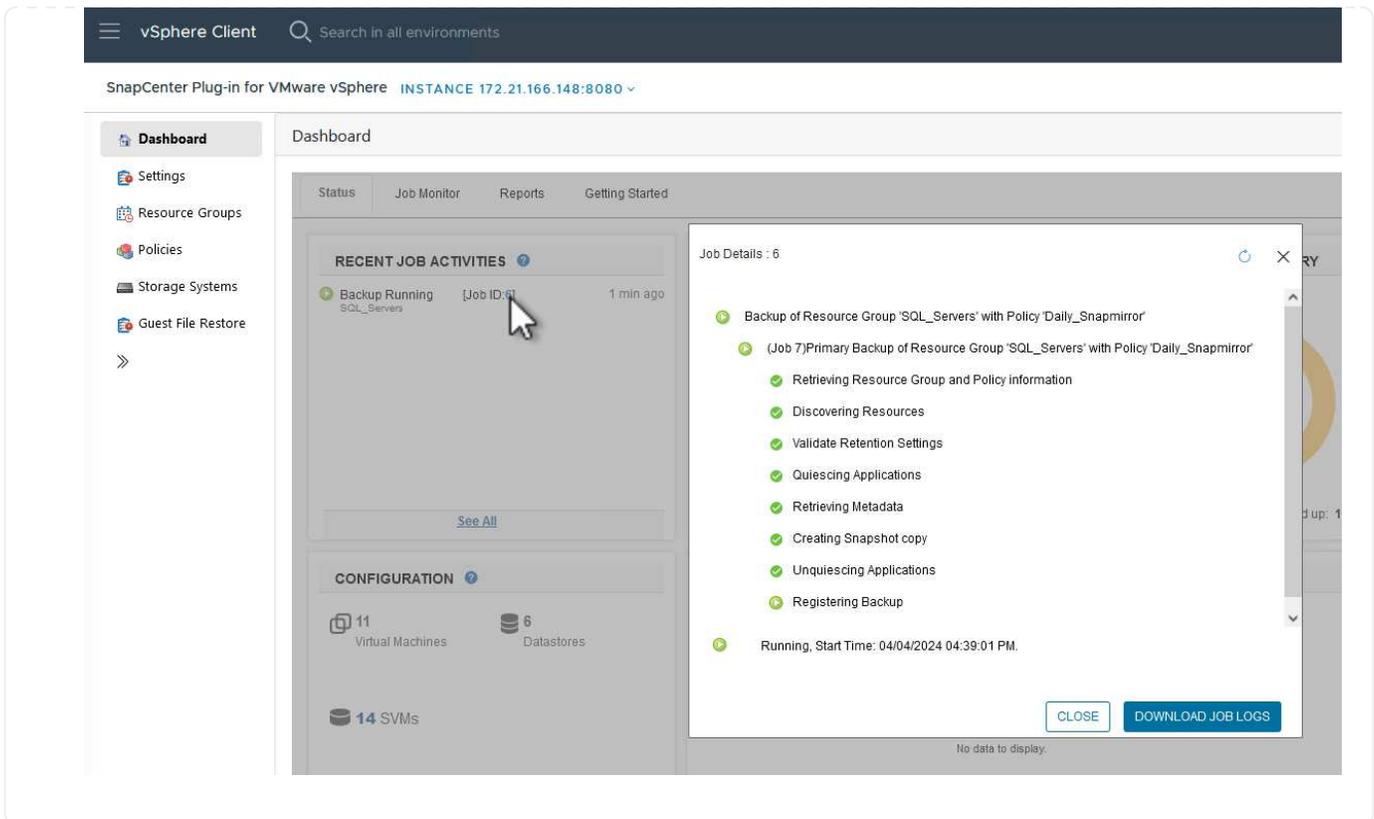
FINISH

CANCEL

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

The screenshot shows the vSphere Client interface. At the top, there is a search bar and a dropdown menu for the SnapCenter Plug-in for VMware vSphere, set to instance 172.21.166.148:8080. On the left, a navigation sidebar lists various options, with 'Resource Groups' highlighted. The main area displays a table of Resource Groups. The table has columns for Name, Description, and Policy. One resource group, 'SQL\_Servers', is listed. Above the table, there are several action buttons: '+ Create', 'Edit', 'Delete', 'Run Now', 'Suspend', 'Resume', and 'Export'. A hand cursor is pointing at the 'Run Now' button.

9. Accedere al **Dashboard** e, in **Recent Job Activities**, fare clic sul numero accanto a **Job ID** per aprire il monitoraggio del processo e visualizzare l'avanzamento del processo in esecuzione.



## Utilizzare SCV per ripristinare VM, VMDK e file

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

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

Le macchine virtuali vVol possono essere ripristinate sull'host originale.

I VMDK delle macchine virtuali tradizionali possono essere ripristinati nel datastore originale o in un datastore alternativo.

I VMDK delle macchine virtuali vVol possono essere ripristinati nel datastore originale.

È possibile ripristinare singoli file e cartelle in una sessione di ripristino dei file guest, allegando una copia di backup di un disco virtuale e ripristinando i file o le cartelle selezionati.

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

## Ripristino delle VM con il plug-in SnapCenter

Completare i seguenti passaggi per ripristinare una VM con SCV:

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

OracleSrv\_04 | Summary Monitor Configure Permissions

Guest OS Virtual Mac

**Actions - OracleSrv\_04**

- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- vSAN
- NetApp ONTAP tools
- SnapCenter Plug-in for VMware vSphere
  - Create Resource Group
  - Add to Resource Group
  - Attach Virtual Disk(s)
  - Detach Virtual Disk(s)
  - Restore
  - File Restore

4 CPU(s), 22 MHz used  
32 GB, 0 GB memory active  
100 GB | Thin Provision  
VCF\_WKLD\_03\_ISCSI  
(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f  
Disconnected  
ESXI 7.0 U2 and later (VM vers

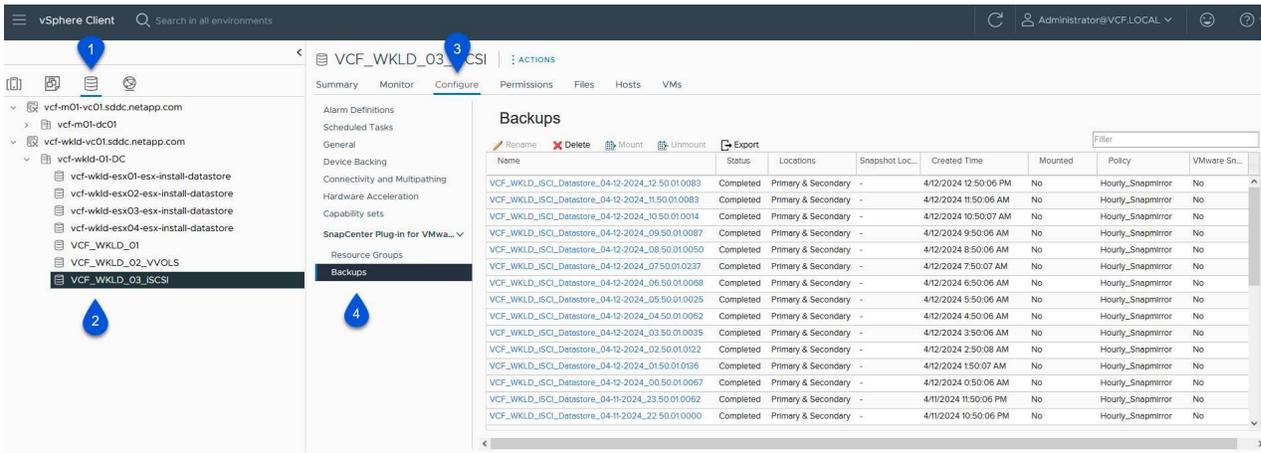
Recent Tasks

Task Name

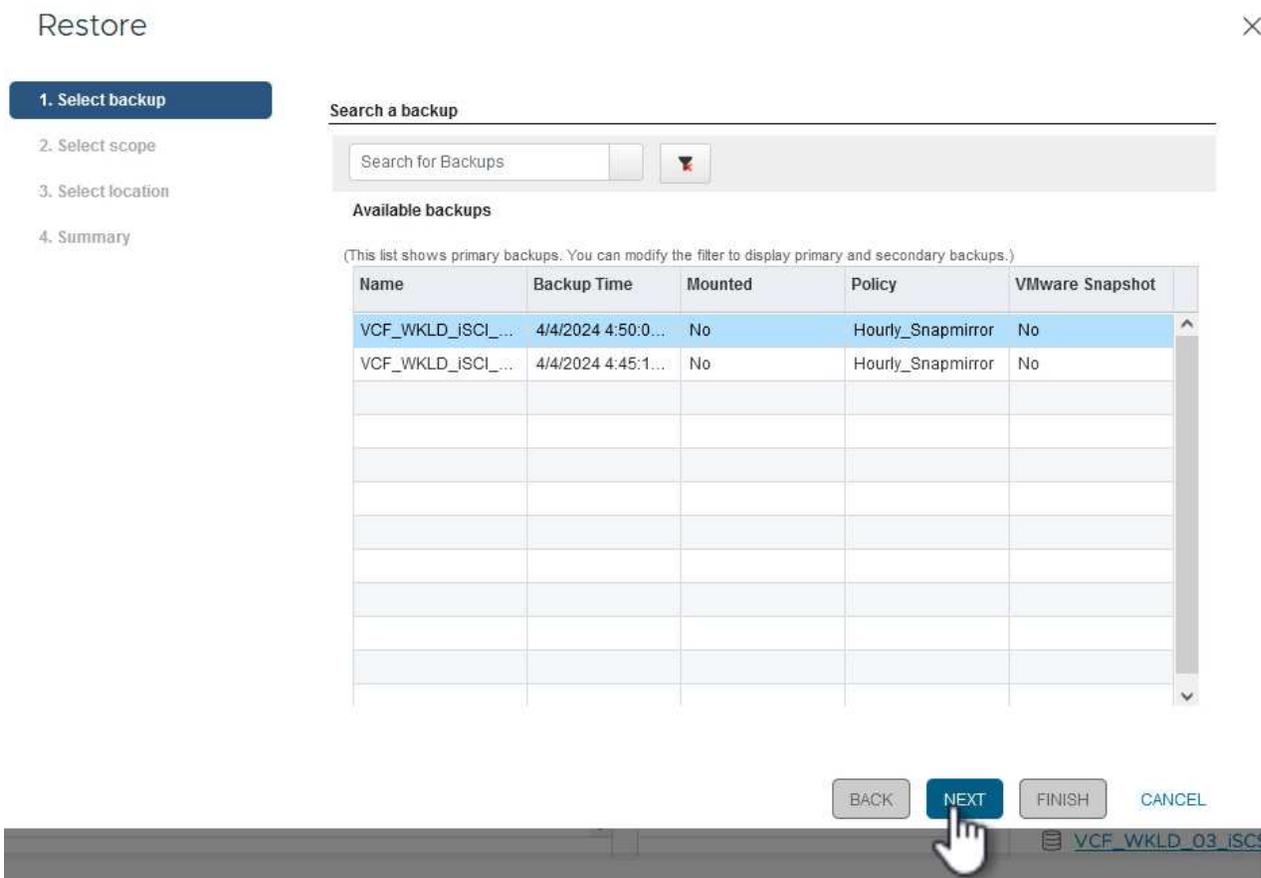
Manage Columns Run



Un'alternativa è accedere al datastore nell'inventario, quindi nella scheda **Configura** andare a **plug-in SnapCenter per VMware vSphere > Backup**. Dal backup scelto, selezionare le VM da ripristinare.



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



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

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

Restore ✕

1. Select backup  
 **2. Select scope**  
 3. Select location  
 4. Summary

**Restore scope**: Entire virtual machine  
**Restart VM**:   
**Restore Location**:
 

- Original Location**  
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)
- Alternate Location**  
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

**Destination vCenter Server**: 172.21.166.143  
**Destination ESXi host**: vcf-wkld-esx04.sddc.netapp.com  
**Network**: vcf-wkld-01-HT-INF-WKLD-01-vds-01-pg-  
**VM name after restore**: OracleSrv\_04\_restored  
**Select Datastore**: VCF\_WKLD\_03\_iSCSI

VCF\_WKLD\_03\_iSCSI

Fare clic su **Avanti** per continuare.

4. Nella pagina **Seleziona posizione**, scegliere di ripristinare la macchina virtuale dal sistema di storage ONTAP primario o secondario. Fare clic su **Avanti** per continuare.

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest
	< >

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

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

<b>Virtual machine to be restored</b>	OracleSrv_04
<b>Backup name</b>	VCF_WKLD_iSCSI_Datastore_04-04-2024_16.50.00.0940
<b>Restart virtual machine</b>	No
<b>Restore Location</b>	Alternate Location
<b>Destination vCenter Server</b>	172.21.166.143
<b>ESXi host to be used to mount the backup</b>	vcf-wkld-esx04.sddc.netapp.com
<b>VM Network</b>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
<b>Destination datastore</b>	VCF_WKLD_03_iSCSI
<b>VM name after restore</b>	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

**FINISH**

CANCEL

6. L'avanzamento del processo di ripristino può essere monitorato dal riquadro **Recent Tasks** (attività recenti) nel client vSphere e dal monitoraggio dei processi in SCV.

- Dashboard
- Settings
- Resource Groups
- Policies
- Storage Systems
- Guest File Restore
- >>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago  
VCF\_WKLD\_ISCI\_Datastore\_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:12] 13 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:9] 13 min ago  
SQL\_Servers
- Backup Successful [Job ID:6] 19 min ago  
SQL\_Servers

[See All](#)

CONFIGURATION

11 Virtual Machines    6 Datastores

14 SVMs

2 Resource Groups    2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF\_WKLD\_ISCI\_Datastore\_04-04-2024\_16:50:00.0940
- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	<a href="#">vcf-wkld-esx04.sdd</a> <a href="#">c.netapp.com</a>	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 P M
NetApp Restore	<a href="#">vcf-wkld-esx04.sdd</a> <a href="#">c.netapp.com</a>	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 P M

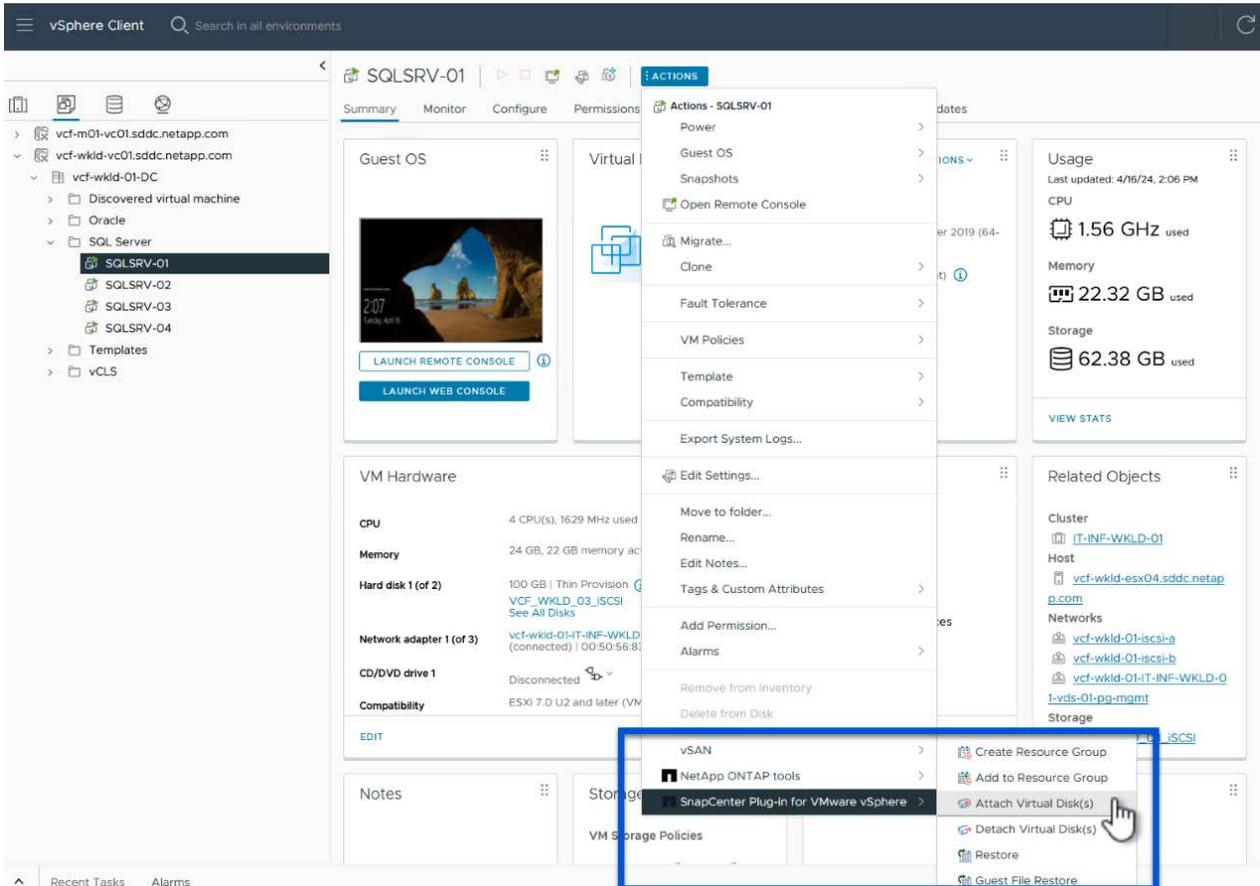
Manage Columns Running More Tasks

## Ripristinare VMDK utilizzando il plug-in SnapCenter

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

Per collegare un VMDK da un backup, attenersi alla seguente procedura:

1. Nel client vSphere, passare a una VM e, dal menu **azioni**, selezionare **Plug-in SnapCenter per VMware vSphere > Allega dischi virtuali**.



2. Nella procedura guidata **Allega dischi virtuali**, selezionare l'istanza di backup da utilizzare e il VMDK specifico da collegare.

# Attach Virtual Disk(s)



Click here to attach to alternate VM

## Backup

(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Le opzioni dei filtri consentono di individuare i backup e visualizzare i backup dei sistemi di storage primario e secondario.

# Attach Virtual Disk(s)



Click here to attach to alternate VM

## Backup

(This list shows primary backups)

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Time range

From

Hour  Minute  Second

To

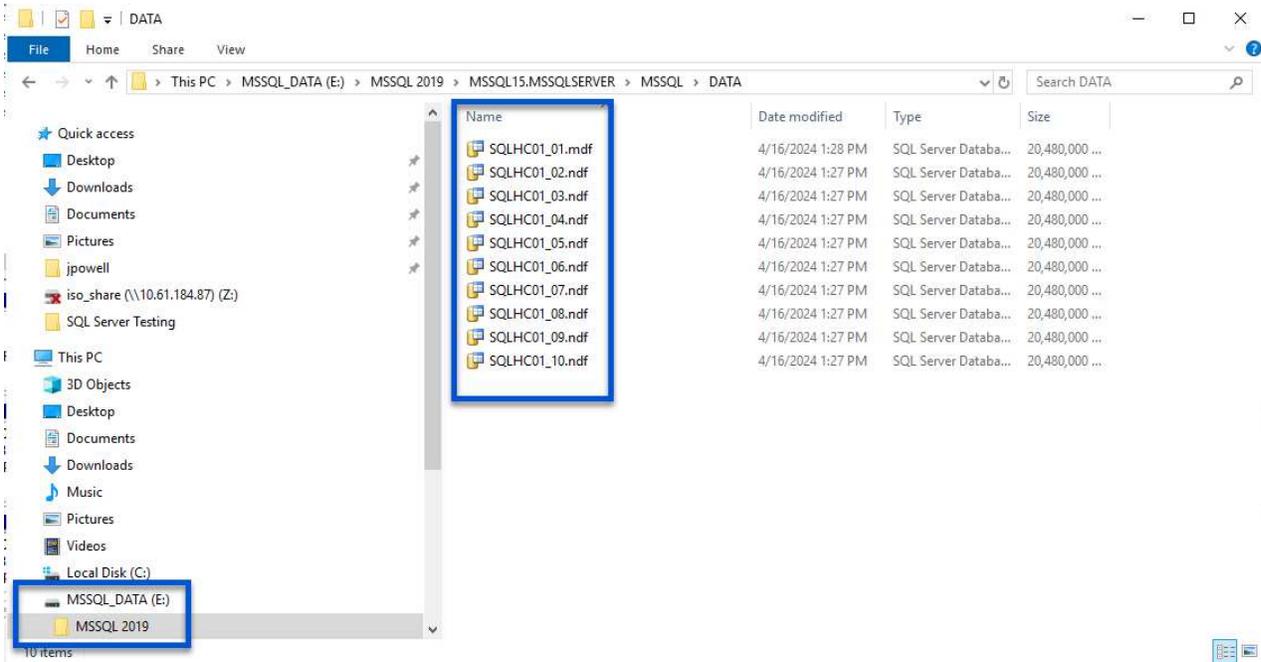
Hour  Minute  Second

VMware snapshot

Mounted

Location

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



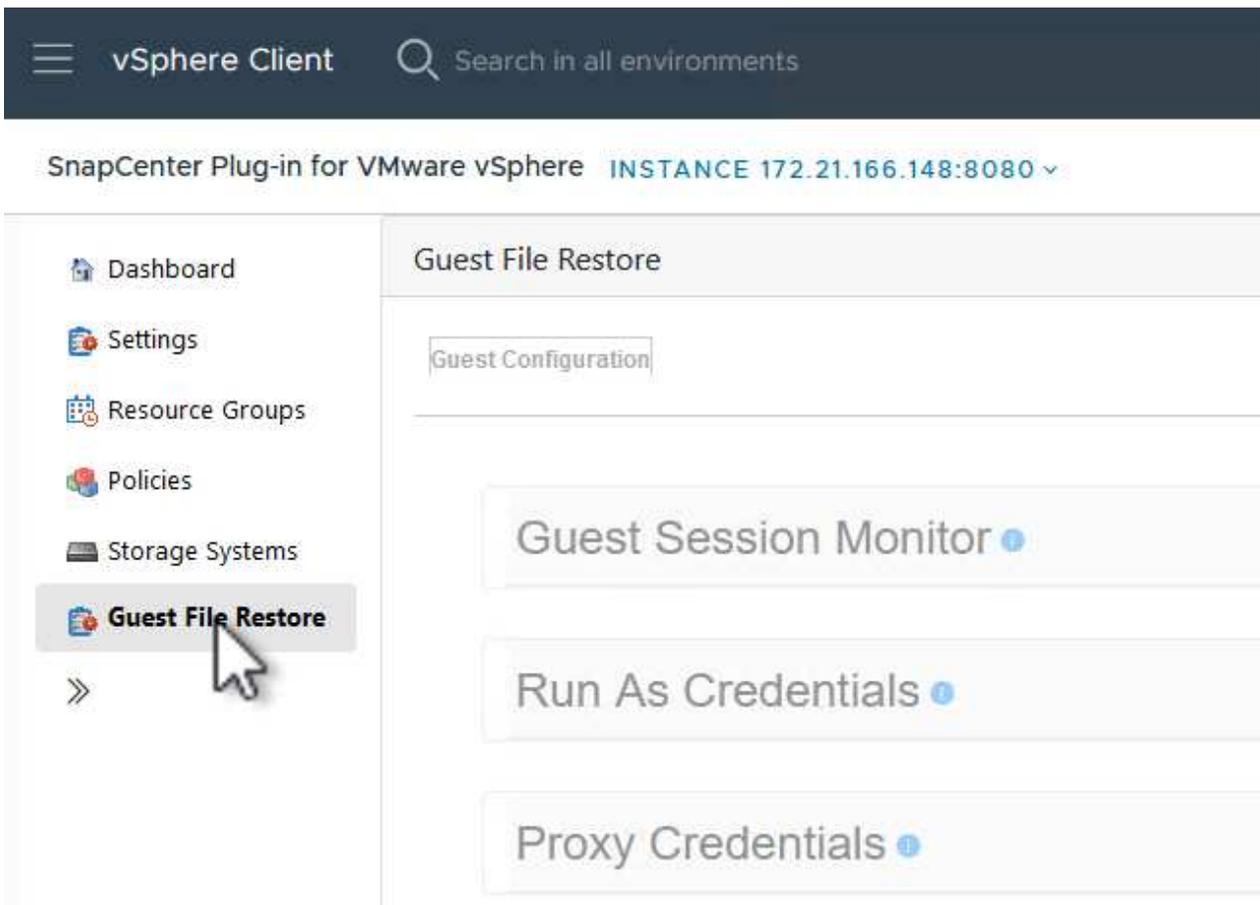
## Ripristino del file system guest mediante il plug-in SnapCenter

ONTAP Tools consente di eseguire il ripristino del file system guest da un VMDK sui sistemi operativi Windows Server. Questo è preformato centralmente dall'interfaccia del plug-in SnapCenter.

Per informazioni dettagliate, fare riferimento a. "[Ripristinare file e cartelle guest](#)" Sul sito della documentazione del distributore idraulico.

Per eseguire un ripristino del file system guest per un sistema Windows, attenersi alla seguente procedura:

1. Il primo passaggio consiste nel creare credenziali Esegui come per fornire l'accesso al sistema host Windows. Nel client vSphere, accedere all'interfaccia del plug-in CSV e fare clic su **Guest file Restore** nel menu principale.



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

## Run As Credentials



Run As Name	<input type="text" value="Administrator"/>	
Username	<input type="text" value="administrator"/>	
Password	<input type="password" value="••••••••"/>	
Authentication Mode	<input type="text" value="Windows"/>	
VM Name	<input type="text"/>	



<input type="button" value="CANCEL"/>	<input type="button" value="SAVE"/>
---------------------------------------	-------------------------------------

4. Nella pagina Proxy VM, fornire un nome per la VM e individuarla ricercando per host ESXi o per nome. Una volta selezionata, fare clic su **Salva**.

## Proxy VM



VM Name

Search by ESXi Host

ESXi Host

Virtual Machine

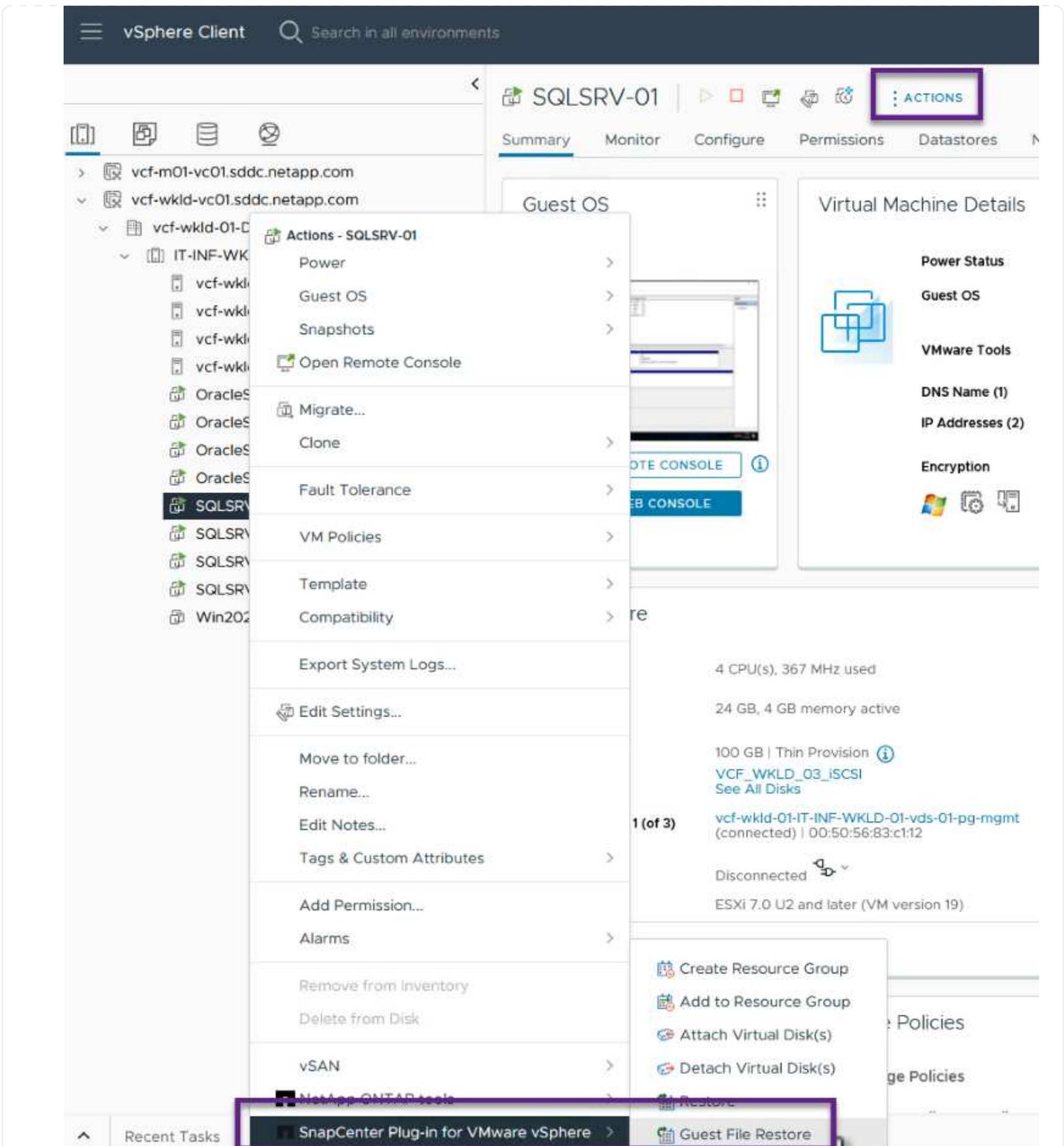
Search by Virtual Machine name

CANCEL

SAVE



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



7. Nella pagina **Restore Scope** della procedura guidata **Guest file Restore**, selezionare il backup da cui eseguire il ripristino, il VMDK specifico e la posizione (primaria o secondaria) da cui ripristinare il VMDK. Fare clic su **Avanti** per continuare.

## Guest File Restore



### 1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iscsi_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK NEXT FINISH CANCEL



8. Nella pagina **Dettagli ospite**, selezionare per utilizzare **Guest VM** o **Use gues file Restore proxy VM** per il ripristino. Inoltre, se lo si desidera, compilare qui le impostazioni per le notifiche e-mail. Fare clic su **Avanti** per continuare.

## Guest File Restore



### 1. Restore Scope

### 2. Guest Details

### 3. Summary

#### Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

#### Use Guest File Restore proxy VM

#### Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

9. Infine, esaminare la pagina **Riepilogo** e fare clic su **fine** per avviare la sessione Ripristino configurazione di sistema file guest.
10. Nell'interfaccia del plug-in SnapCenter, accedere nuovamente a **Ripristino file guest** e visualizzare la sessione in esecuzione in **monitoraggio sessione guest**. Fare clic sull'icona sotto **Sfogliare file** per continuare.

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_JSCSI(sc-202404161419...	E:\	23h:58m	

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

## Guest File Browse



### Select File(s)/Folder(s) to Restore



E:\MSSQL 2019

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		^
			v

Selected 0 Files / 1 Directory

Name	Path	Size	Delete	
MSSQL 2019	E:\MSSQL 2019			^
				v

### Select Restore Location



Select address family for UNC path:

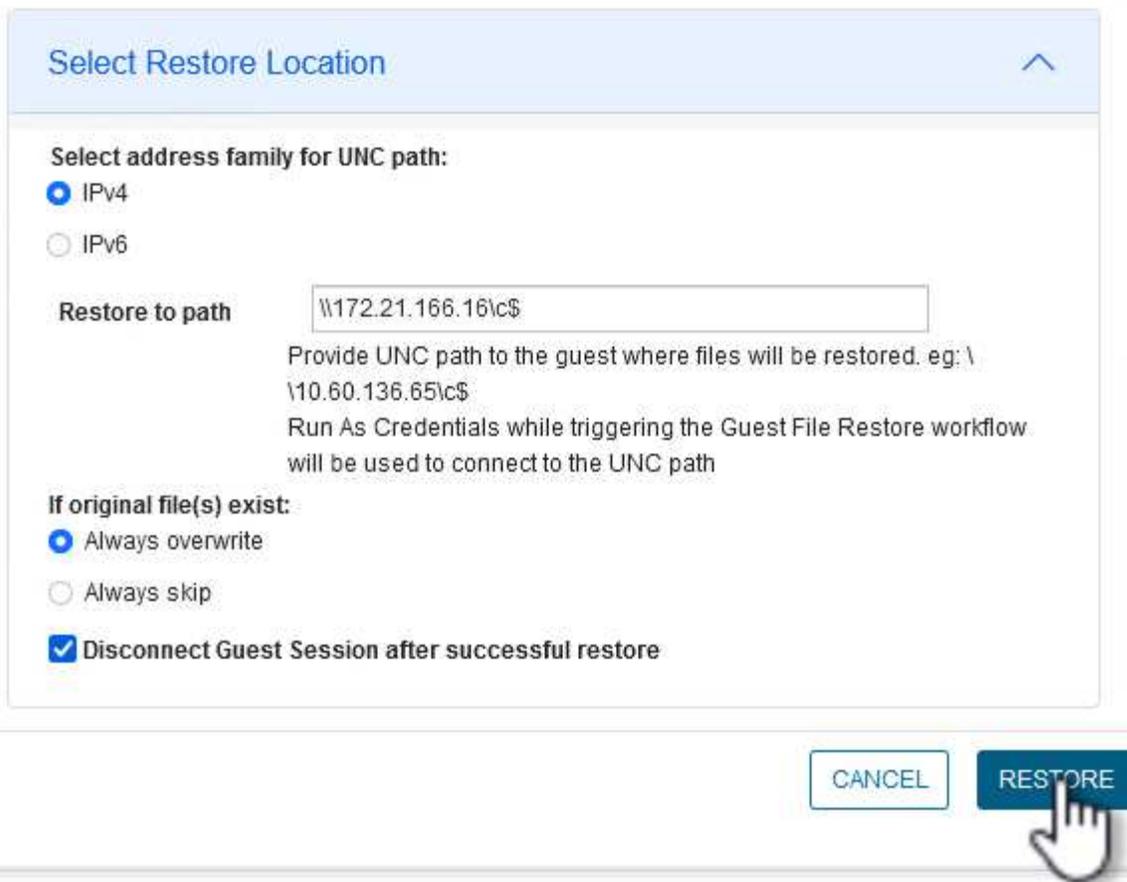
IPv4

IPv6

**Either Files to Restore or Restore Location is not selected!**

CANCEL

RESTORE



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

### Ulteriori informazioni

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

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

Per informazioni sull'utilizzo del plug-in SnapCenter per VMware vSphere, consultare la ["Plug-in SnapCenter per la documentazione di VMware vSphere"](#).

## VMware Cloud Foundation con array NetApp AFF

Autore: Josh Powell, Ravi BCB

### VMware Cloud Foundation con array NetApp AFF

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

Il presente documento fornisce informazioni sulle opzioni di storage disponibili per VMware Cloud Foundation utilizzando il sistema storage AFF all-flash di NetApp. Le opzioni di storage supportate sono coperte da istruzioni specifiche per la creazione di domini di workload con datastore NFS e vVol come storage principale, oltre a una gamma di opzioni di storage supplementari.

### **Casi di utilizzo**

Casi d'utilizzo illustrati nella presente documentazione:

- Opzioni di storage per i clienti che cercano ambienti uniformi su cloud pubblici e privati.
- Soluzione automatizzata per l'implementazione dell'infrastruttura virtuale per i domini di carico di lavoro.
- Soluzione storage scalabile realizzata su misura per soddisfare esigenze in evoluzione, anche se non allineata direttamente ai requisiti delle risorse di calcolo.
- Distribuire i domini del carico di lavoro VCF VI utilizzando ONTAP come storage principale.
- Distribuire lo storage supplementare ai domini del carico di lavoro VI utilizzando gli strumenti ONTAP per VMware vSphere.

### **Pubblico**

Questa soluzione è destinata alle seguenti persone:

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

### **Panoramica sulla tecnologia**

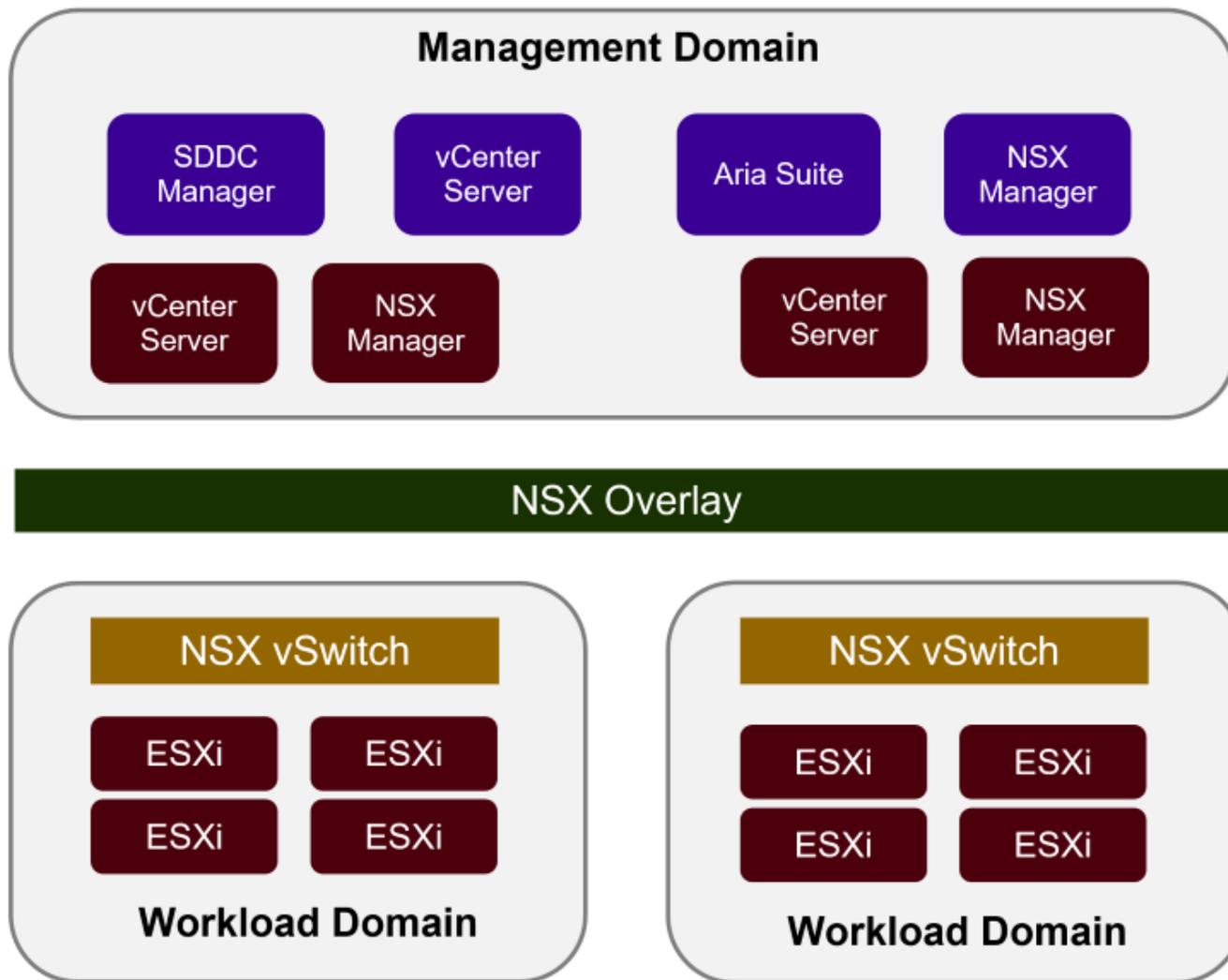
La soluzione VCF con NetApp AFF comprende i seguenti componenti principali:

#### **VMware Cloud Foundation**

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

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

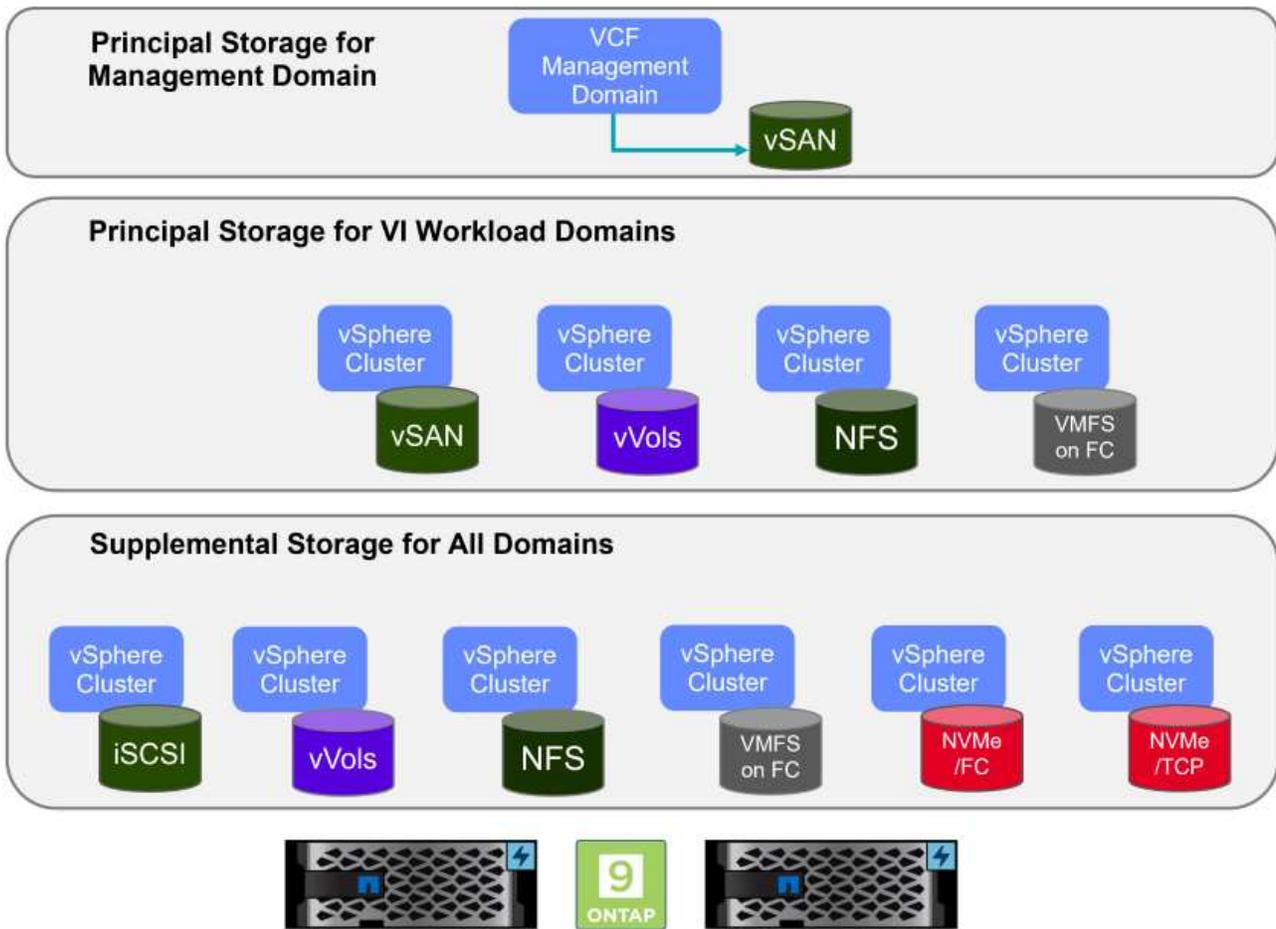
VCF è costituito da un singolo dominio di gestione e fino a 24 domini del carico di lavoro VI che rappresentano ciascuna un'unità di infrastruttura predisposta per le applicazioni. Un dominio del carico di lavoro è costituito da uno o più cluster vSphere gestiti da una singola istanza vCenter.



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

### Opzioni di archiviazione VCF

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



### Archiviazione principale per i domini del carico di lavoro

L'archiviazione principale si riferisce a qualsiasi tipo di archiviazione che può essere collegata direttamente a un dominio del carico di lavoro VI durante il processo di installazione in SDDC Manager. Lo storage principale è il primo datastore configurato per un dominio del carico di lavoro e include vSAN, vVol (VMFS), NFS e VMFS su Fibre Channel.

### Archiviazione supplementare per domini di gestione e carico di lavoro

Lo storage supplementare è il tipo di storage che è possibile aggiungere ai domini di gestione o del carico di lavoro in qualsiasi momento dopo la creazione del cluster. Lo storage supplementare rappresenta la più ampia gamma di opzioni di storage supportate, tutte supportate dagli array NetApp AFF.

Ulteriori risorse di documentazione per VMware Cloud Foundation:

- \* ["Documentazione di VMware Cloud Foundation"](#)
- \* ["Tipi di storage supportati per VMware Cloud Foundation"](#)
- \* ["Gestione dello storage in VMware Cloud Foundation"](#)

### Array storage all-flash NetApp

Gli array NetApp AFF (All Flash FAS) sono soluzioni storage ad alte performance progettate per sfruttare la velocità e l'efficienza della tecnologia flash. Gli array AFF incorporano funzionalità di gestione integrata dei dati quali backup basati su snapshot, replica, thin provisioning e funzionalità di protezione dei dati.

Gli array NetApp AFF utilizzano il sistema operativo per lo storage ONTAP, offrendo un supporto completo del

protocollo di storage per tutte le opzioni di storage compatibili con VCF, il tutto all'interno di un'architettura unificata.

Gli storage array NetApp AFF sono disponibili nella serie A dalle performance più elevate e in una serie C QLC basata su flash. Entrambe le serie utilizzano dischi flash NVMe.

Per ulteriori informazioni sugli storage array NetApp AFF A-Series, consultare la ["NetApp AFF A-Series" landing page](#).

Per ulteriori informazioni sugli storage array NetApp C-Series, consultare la ["NetApp AFF C-Series" landing page](#).

### Strumenti NetApp ONTAP per VMware vSphere

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

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

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

Per ulteriori informazioni sugli strumenti NetApp ONTAP, vedere ["Strumenti ONTAP per la documentazione VMware vSphere"](#) pagina.

### Panoramica della soluzione

Negli scenari presentati in questa documentazione, verrà illustrato come utilizzare i sistemi di storage ONTAP come storage principale per le implementazioni del dominio di carico di lavoro VCF VI. Inoltre, installeremo e utilizzeremo gli strumenti ONTAP per VMware vSphere per configurare datastore supplementari per i domini del carico di lavoro VI.

Scenari trattati nella presente documentazione:

- **Configurare e utilizzare un datastore NFS come storage principale durante la distribuzione del dominio del carico di lavoro VI.** fare clic ["qui"](#) per le fasi di implementazione.
- **Installare e dimostrare l'uso degli strumenti ONTAP per configurare e montare gli archivi dati NFS come archiviazione supplementare nei domini del carico di lavoro VI.** fare clic su ["qui"](#) per le fasi di implementazione.

### NFS come storage principale per i domini del carico di lavoro VI

Autore: Josh Powell, Ravi BCB

NFS come storage principale per i domini del carico di lavoro VI

## Panoramica dello scenario

In questo scenario verrà illustrato come configurare un datastore NFS come storage principale per la distribuzione di un dominio del carico di lavoro VI in VCF. Se necessario, faremo riferimento alla documentazione esterna per le operazioni che devono essere eseguite in SDDC Manager di VCF e descriveremo le operazioni specifiche per la parte relativa alla configurazione dello storage.

Questo scenario copre i seguenti passaggi di alto livello:

- Verifica dell'networking per la Storage Virtual Machine (SVM) di ONTAP e della presenza di un'interfaccia logica (LIF) per il traffico NFS.
- Creare una policy di esportazione per consentire agli host ESXi di accedere al volume NFS.
- Crea un volume NFS sul sistema storage ONTAP.
- Creare un pool di rete per il traffico NFS e vMotion in SDDC Manager.
- Commissione di host in VCF per l'utilizzo in un dominio del carico di lavoro VI.
- Implementare un dominio del carico di lavoro VI in VCF utilizzando un datastore NFS come storage principale.
- Installare il plug-in NetApp NFS per VMware VAAI

## Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Sistema storage NetApp AFF con una Storage Virtual Machine (SVM) configurata per consentire il traffico NFS.
- L'interfaccia logica (LIF) è stata creata nella rete IP per il trasporto del traffico NFS e associata alla SVM.
- La distribuzione del dominio di gestione VCF è completa e l'interfaccia di SDDC Manager è accessibile.
- 4 host ESXi configurati per la comunicazione sulla rete di gestione VCF.
- Indirizzi IP riservati per il traffico di storage vMotion e NFS sulla VLAN o sul segmento di rete stabilito a tale scopo.



Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

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

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

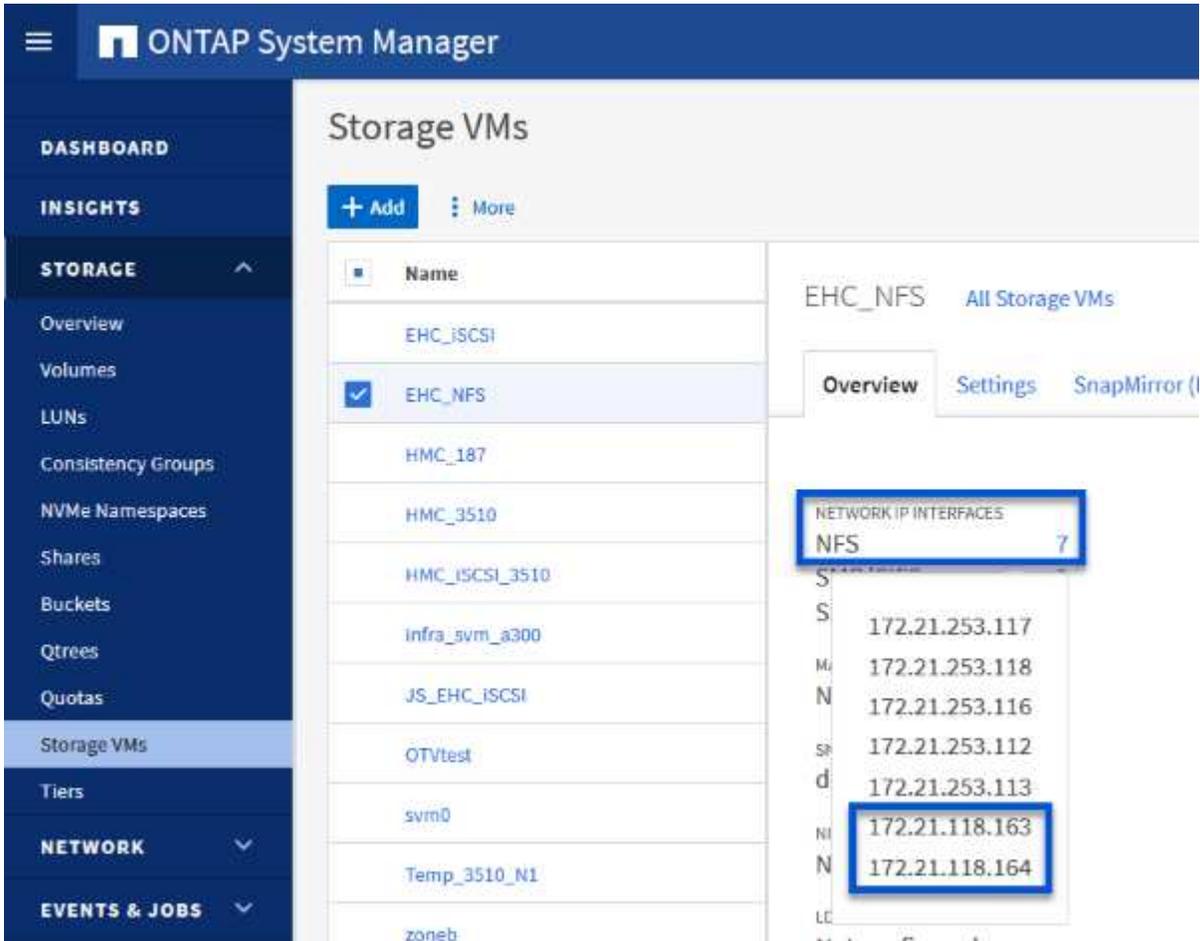
## Fasi di implementazione

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

## Verifica della rete per ONTAP SVM

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

1. Da Gestione di sistema di ONTAP, accedere a **Storage VM** nel menu a sinistra e fare clic sulla SVM da utilizzare per il traffico NFS. Nella scheda **Panoramica**, sotto **NETWORK IP INTERFACES**, clicca sul valore numerico a destra di **NFS**. Nell'elenco, verifica che siano elencati gli indirizzi IP LIF richiesti.



The screenshot shows the ONTAP System Manager interface. On the left is a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE (expanded), and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main area displays a list of Storage VMs. The 'EHC\_NFS' SVM is selected and highlighted. To the right of the list, there are tabs for 'Overview', 'Settings', and 'SnapMirror (0)'. The 'Overview' tab is active, showing a 'NETWORK IP INTERFACES' section. Under this section, the 'NFS' interface is highlighted, and a dropdown menu is open showing a list of IP addresses. Two IP addresses, '172.21.118.163' and '172.21.118.164', are highlighted with blue boxes.

Name
EHC_ISCSI
<input checked="" type="checkbox"/> EHC_NFS
HMC_187
HMC_3510
HMC_ISCSI_3510
infra_svm_a300
JS_EHC_ISCSI
OTVtest
svm0
Temp_3510_N1
zoneb

NETWORK IP INTERFACES

Interface	IP Address
NFS	7
S	172.21.253.117
S	172.21.253.118
M	172.21.253.118
N	172.21.253.116
SP	172.21.253.112
d	172.21.253.113
N	172.21.118.163
N	172.21.118.164

In alternativa, verifica le LIF associate a una SVM dalla CLI di ONTAP utilizzando il seguente comando:

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

1. Verificare che gli host ESXi siano in grado di comunicare con il server NFS ONTAP. Accedere all'host ESXi tramite SSH e eseguire il ping della LIF SVM:

```
vmkping <IP Address>
```

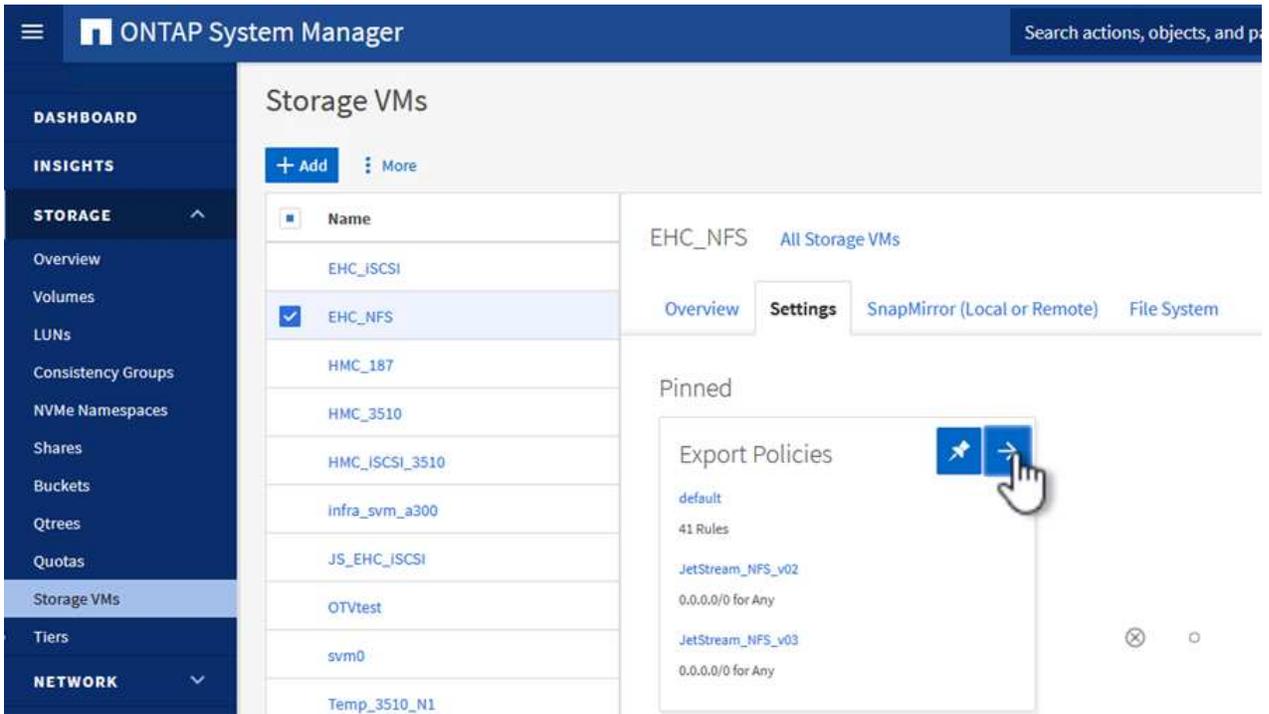


Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

## Crea una policy di esportazione per la condivisione del volume NFS

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

1. In Gestione sistema di ONTAP, fare clic su **Storage VM** nel menu a sinistra e selezionare una SVM dall'elenco.
2. Nella scheda **Impostazioni** individuare **Esporta criteri** e fare clic sulla freccia per accedere.



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

## New export policy

NAME

WKLD\_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Immettere gli indirizzi IP, l'intervallo degli indirizzi IP o la rete che si desidera includere nella regola. Deselezionare le caselle **SMB/CIFS** e **FlexCache** e selezionare i dettagli di accesso riportati di seguito. La selezione delle caselle UNIX è sufficiente per l'accesso all'host ESXi.

## New Rule



### CLIENT SPECIFICATION

172.21.166.0/24

### ACCESS PROTOCOLS

SMB/CIFS

FlexCache

NFS  NFSv3  NFSv4

### ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



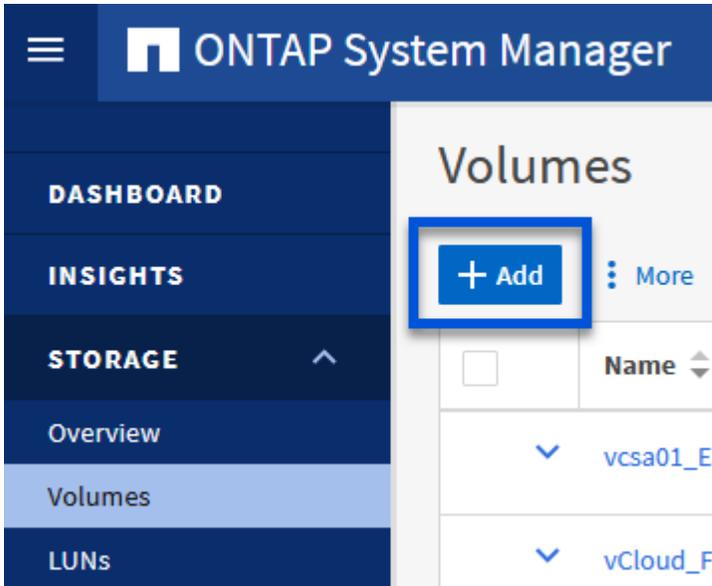
Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario garantire che il criterio di esportazione includa la rete di gestione VCF per consentire la convalida.

- Una volta immesse tutte le regole, fare clic sul pulsante **Salva** per salvare la nuova politica di esportazione.
- In alternativa, è possibile creare criteri e regole di esportazione nella CLI di ONTAP. Fare riferimento alla procedura per la creazione di un criterio di esportazione e l'aggiunta di regole nella documentazione di ONTAP.
  - Utilizzare l'interfaccia CLI di ONTAP per ["Creare una policy di esportazione"](#).
  - Utilizzare l'interfaccia CLI di ONTAP per ["Aggiungere una regola a un criterio di esportazione"](#).

## Creazione di un volume NFS

Creare un volume NFS sul sistema storage ONTAP da utilizzare come datastore nell'implementazione del dominio dei carichi di lavoro.

1. Da Gestione di sistema di ONTAP, accedere a **archiviazione > volumi** nel menu a sinistra e fare clic su **+Aggiungi** per creare un nuovo volume.



2. Aggiungi un nome per il volume, compila la capacità desiderata e seleziona la VM di archiviazione che ospiterà il volume. Fare clic su **altre opzioni** per continuare.

## Add Volume



NAME

VCF\_WKLD\_01

CAPACITY

5



TiB



STORAGE VM

EHC\_NFS



Export via NFS

[More Options](#)

Cancel

Save

3. In autorizzazioni di accesso, selezionare il criterio di esportazione che include la rete di gestione VCF o l'indirizzo IP e gli indirizzi IP di rete NFS che verranno utilizzati per la convalida del traffico NFS Server e NFS.

## Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default 

JetStream\_NFS\_v04  
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01  
3 rules

NFSmountTestReno01  
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols  
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv\_VPN  
Clients : 172.21.254.0/24 | Access protocols : Any

VCF\_WKLD  
2 rules

WKLD\_DM01  
2 rules

Wkld01\_NFS  
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



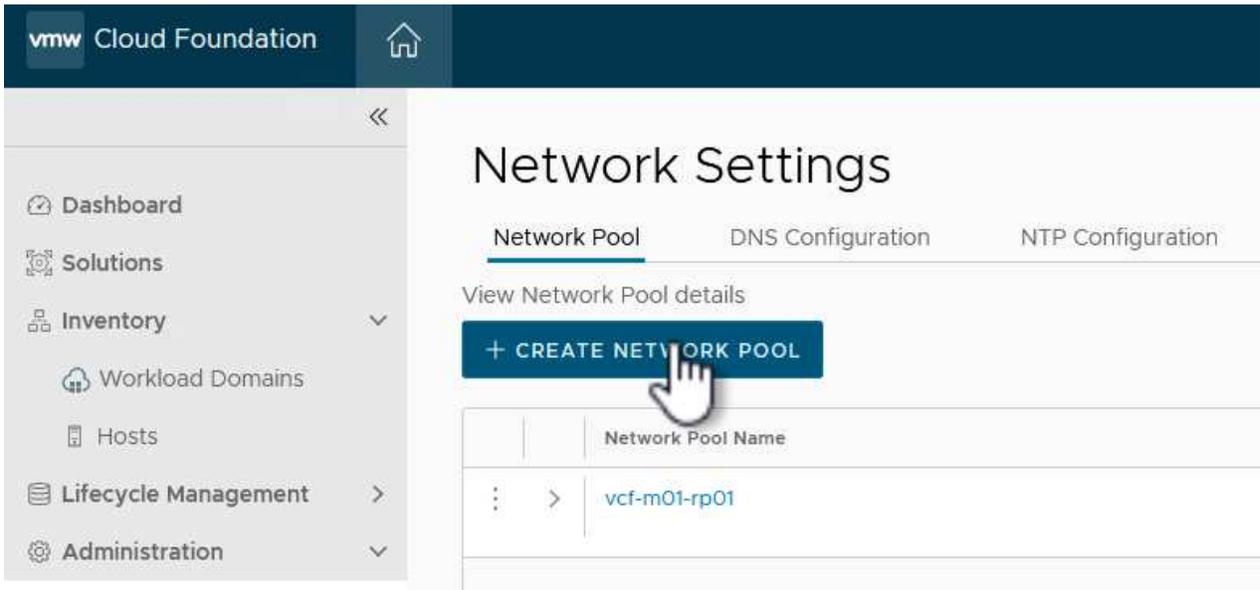
Quando si distribuisce un dominio del carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima di aggiungere qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario verificare che 1) la rete di gestione sia instradabile al server NFS o 2) una LIF per la rete di gestione sia stata aggiunta alla SVM che ospita il volume del datastore NFS, per garantire che la convalida possa procedere.

1. In alternativa, è possibile creare volumi ONTAP nella CLI di ONTAP. Per ulteriori informazioni, fare riferimento a "[lun create \(crea lun\)](#)" Nella documentazione dei comandi ONTAP.

## Creare un pool di rete in SDDC Manager

Il pool di rete deve essere creato in SDDC Manager prima di mettere in funzione gli host ESXi, come preparazione per la loro distribuzione in un dominio del carico di lavoro VI. Il pool di rete deve includere le informazioni di rete e gli intervalli di indirizzi IP affinché gli adattatori VMkernel possano essere utilizzati per la comunicazione con il server NFS.

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



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

The screenshot shows the VMware Cloud Foundation interface for creating a network pool. The left sidebar contains navigation options like Dashboard, Solutions, Inventory, Lifecycle Management, Administration, Network Settings, Storage Settings, Licensing, Single Sign On, Proxy Settings, Online Depot, Composable Infrastructure, VMware Aria Suite, Backup, VMware CEP, Security, Password Management, Certificate Authority, and Developer Center. The main content area is titled 'Network Settings' and 'Create Network Pool'. It includes a 'Network Pool Name' field with the value 'NFS\_NPOOL' and 'Network Type' options: vSAN, NFS (checked), iSCSI, and vMotion (checked). Below are two panels: 'NFS Network Information' and 'vMotion Network Information'. Each panel contains fields for VLAN ID, MTU, Network, Subnet Mask, and Default Gateway. The NFS panel has values: VLAN ID 3374, MTU 9000, Network 172.21.118.0, Subnet Mask 255.255.255.0, and Default Gateway 172.21.118.1. The vMotion panel has values: VLAN ID 3423, MTU 9000, Network 172.21.167.0, Subnet Mask 255.255.255.0, and Default Gateway 172.21.167.1. Both panels also have an 'Included IP Address Ranges' section with a table of IP ranges and a 'REMOVE' button. At the bottom, there are 'CANCEL' and 'SAVE' buttons.

Field	NFS Network Information	vMotion Network Information
VLAN ID	3374	3423
MTU	9000	9000
Network	172.21.118.0	172.21.167.0
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	172.21.118.1	172.21.167.1

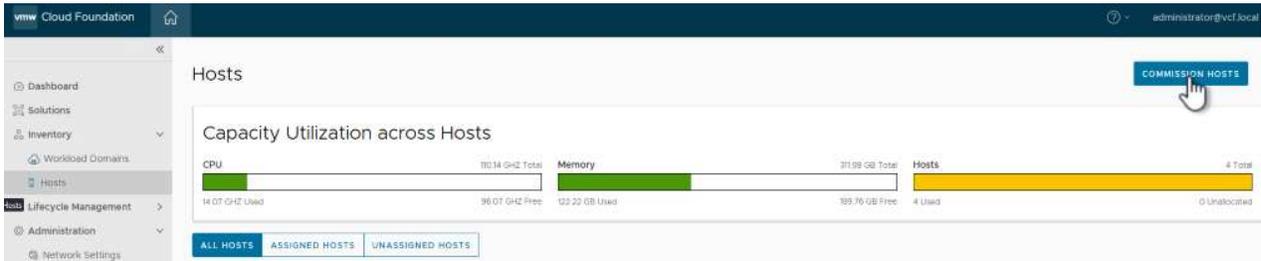
3. Fare clic sul pulsante **Salva** per completare la creazione del pool di rete.

## La commissione ospita

Prima di poter distribuire gli host ESXi come dominio del carico di lavoro, è necessario aggiungerli all'inventario di SDDC Manager. Ciò comporta la fornitura delle informazioni richieste, il superamento della convalida e l'avvio del processo di messa in funzione.

Per ulteriori informazioni, vedere ["La commissione ospita"](#) Nella Guida all'amministrazione di VCF.

1. Dall'interfaccia di SDDC Manager, accedere a **hosts** nel menu a sinistra e fare clic sul pulsante **Commission hosts**.



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

## Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- Select All**
- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for vSAN workload domain are associated with vSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

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

## Host Addition and Validation

## Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new  Import

Host FQDN

Storage Type  vSAN  NFS  VMFS on FC  vVol

Network Pool Name

User Name

Password

ADD

## Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

Confirm all Finger Prints

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVDp6v EGM	<input type="checkbox"/> Not Validated

1 hosts

CANCEL

NEXT

- Una volta aggiunti tutti gli host da convalidare, fare clic sul pulsante **convalida tutto** per continuare.
- Presupponendo che tutti gli host siano convalidati, fare clic su **Avanti** per continuare.

## Hosts Added

✔ Host Validated Successfully. ✕

REMOVE  Confirm all Finger Prints (i) VALIDATE ALL

<input checked="" type="checkbox"/>	FGDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.138	<input checked="" type="checkbox"/> SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	<input checked="" type="checkbox"/> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.137	<input checked="" type="checkbox"/> SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2IOWZDPFH+z0	<input checked="" type="checkbox"/> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.136	<input checked="" type="checkbox"/> SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4IWY	<input checked="" type="checkbox"/> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinfEOG+ +z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	<input checked="" type="checkbox"/> Valid

CANCEL NEXT

- Rivedere l'elenco degli host da mettere in servizio e fare clic sul pulsante **Commissione** per avviare il processo. Monitorare il processo di messa in funzione dal Task pane in SDDC Manager.

## Commission Hosts

1 Host Addition and Validation

2 **Review**

## Review

Skip failed hosts during commissioning   On

Validated Host(s)	
vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

CANCEL

BACK

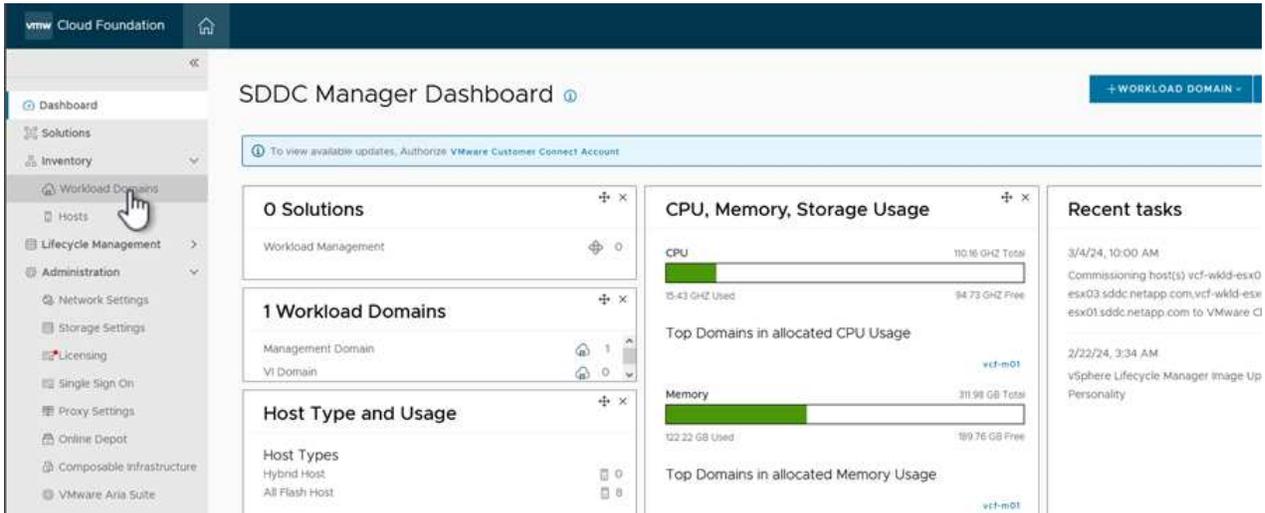
COMMISSION

## Distribuire il dominio del carico di lavoro VI

La distribuzione dei domini del carico di lavoro VI viene eseguita utilizzando l'interfaccia di VCF Cloud Manager. Qui verranno presentate solo le fasi relative alla configurazione dello storage.

Per istruzioni dettagliate sull'implementazione di un dominio del carico di lavoro VI, fare riferimento a ["Distribuire un dominio del carico di lavoro VI utilizzando l'interfaccia utente di SDDC Manager"](#).

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



2. Nella procedura guidata di configurazione vi compilare le sezioni **informazioni generali, cluster, elaborazione, rete** e **selezione host** secondo necessità.

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

+

# VI Configuration

## 1 General Info

## 2 Cluster

## 3 Compute

## 4 Networking

## 5 Host Selection

## 6 NFS Storage

## 7 Switch Configuration

## 8 License

## 9 Review

1. Nella sezione Storage NFS compilare il Nome datastore, il punto di montaggio della cartella del volume NFS e l'indirizzo IP della LIF delle macchine virtuali di storage NFS di ONTAP.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage**

### NFS Storage

**NFS Share Details**

Datastore Name ⓘ	VCF_WKLD_01
Folder ⓘ	/VCF_WKLD_01
NFS Server IP Address ⓘ	172.21.118.163

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

### VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review

### Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxc101.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL
BACK
FINISH

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

### Installare il plug-in NetApp NFS per VMware VAAI

Il plug-in NFS di NetApp per VMware VAAI integra le librerie di dischi virtuali VMware installate sull'host ESXi e offre operazioni di cloning con performance più elevate e completate più rapidamente. Questa è una procedura consigliata quando si utilizzano i sistemi storage ONTAP con VMware vSphere.

Per istruzioni dettagliate sull'implementazione del plug-in NFS NetApp per VMware VAAI, seguire le istruzioni sul sito ["Installare il plug-in NetApp NFS per VMware VAAI"](#).

### Video dimostrativo per questa soluzione

[Archivi dati NFS come archiviazione principale per i domini del carico di lavoro VCF](#)

## Introduzione all'automazione per ONTAP e vSphere

### Automazione VMware

L'automazione è parte integrante della gestione degli ambienti VMware fin dai primi giorni di VMware ESX. La capacità di implementare l'infrastruttura come codice ed estendere le pratiche alle operazioni del cloud privato

aiuta ad alleviare i problemi legati a scalabilità, flessibilità, self-provisioning ed efficienza.

L'automazione può essere organizzata nelle seguenti categorie:

- **Implementazione dell'infrastruttura virtuale**
- **Operazioni della macchina guest**
- **Operazioni cloud**

Gli amministratori hanno a disposizione numerose opzioni per l'automazione dell'infrastruttura. Sia attraverso l'utilizzo di funzionalità vSphere native come profili host o specifiche di personalizzazione per le macchine virtuali alle API disponibili sui componenti software VMware, sui sistemi operativi e sui sistemi storage NetApp, sono disponibili documentazione e indicazioni significative.

Data ONTAP 8.0.1 e versioni successive supportano alcune API VMware vSphere per l'integrazione degli array (VAAI) quando l'host ESX esegue ESX 4.1 o versioni successive. VAAI è un insieme di API che consentono la comunicazione tra host VMware vSphere ESXi e dispositivi di storage. Queste funzionalità consentono di trasferire le operazioni dall'host ESX al sistema storage e aumentare il throughput di rete. L'host ESX attiva automaticamente le funzioni nell'ambiente corretto. È possibile determinare la misura in cui il sistema utilizza le funzioni VAAI controllando le statistiche contenute nei contatori VAAI.

Il punto di partenza più comune per l'automazione dell'implementazione di un ambiente VMware è il provisioning di datastore a blocchi o basati su file. È importante definire i requisiti delle attività effettive prima di sviluppare l'automazione corrispondente.

Per ulteriori informazioni sull'automazione degli ambienti VMware, consultare le seguenti risorse:

- ["Il NetApp Pub"](#). Automazione e gestione della configurazione NetApp.
- ["La community Ansible Galaxy per VMware"](#). Una raccolta di risorse Ansible per VMware.
- ["Risorse VMware {code}"](#). Risorse necessarie per progettare soluzioni per il data center software-defined, inclusi forum, standard di progettazione, codice di esempio e tool per sviluppatori.

## Provisioning tradizionale dello storage a blocchi vSphere con ONTAP

VMware vSphere supporta le seguenti opzioni di datastore VMFS con il supporto del protocollo SAN ONTAP indicato.

Opzioni datastore VMFS	Supporto del protocollo SAN ONTAP
<a href="#">"Fibre Channel (FC)"</a>	sì
<a href="#">"Fibre Channel over Ethernet (FCoE)"</a>	sì
<a href="#">"iSCSI"</a>	sì
Estensioni iSCSI per RDMA (iSER)	no
<a href="#">"NVMe su fabric con FC (NVMe/FC)"</a>	sì
NVMe su fabric con RDMA su Ethernet convergente (NVMe/RoCE)	no



Se è richiesto iSER o NVMe/RoCE VMFS, controllare i sistemi storage basati su SANtricity.

## Datastore vSphere VMFS - backend dello storage Fibre Channel con ONTAP

### A proposito di questa attività

In questa sezione viene illustrata la creazione di un datastore VMFS con lo storage Fibre Channel (FC) ONTAP.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con ONTAP 9,8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente e password)
- WWPN ONTAP di host, destinazione e informazioni su SVM e LUN
- ["Il foglio di lavoro di configurazione FC completo"](#)
- Credenziali vCenter Server
- Informazioni sugli host vSphere
  - VSphere 7,0 o versione successiva
- Switch fabric
  - Con porte dati ONTAP FC e host vSphere collegati
  - Con la funzione NPIV (N\_Port ID Virtualization) attivata
  - Creare una singola zona di destinazione dell'iniziatore.
    - Creare una zona per ciascun iniziatore (singola zona iniziatore).
    - Per ciascuna zona, includere una destinazione che sia l'interfaccia logica FC ONTAP (WWPN) per le SVM. Devono essere presenti almeno due interfacce logiche per nodo per SVM. Non utilizzare la WWPN delle porte fisiche.
- Un tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso.

### Provisioning di un datastore VMFS

Per eseguire il provisioning di un datastore VMFS, attenersi alla seguente procedura:

1. Verificare la compatibilità con ["Tool di matrice di interoperabilità \(IMT\)"](#)
2. Verificare che il ["Configurazione FCP supportata"](#).

### Attività di ONTAP

1. ["Verificare di disporre di una licenza ONTAP per FCP."](#)
  - a. Utilizzare `system license show` Per verificare che FCP sia presente nell'elenco.
  - b. Utilizzare `licen se add -license-code <license code>` per aggiungere la licenza.
2. Assicurarsi che il protocollo FCP sia attivato su SVM.
  - a. ["Verificare l'FCP su una SVM esistente."](#)

- b. ["Configurare l'FCP su una SVM esistente."](#)
  - c. ["Crea la nuova SVM con FCP."](#)
3. Assicurarsi che le interfacce logiche FCP siano disponibili su una SVM.
  - a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.
  - b. Quando viene creata una SVM con la GUI, le interfacce logiche fanno parte di tale processo.
  - c. Per rinominare le interfacce di rete, utilizzare `Network Interface modify`.
4. ["Creare e mappare un LUN."](#) Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere.

### Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili in ["Informazioni sull'adattatore di storage"](#).
2. ["Eseguire il provisioning di un datastore VMFS con gli strumenti ONTAP"](#).

### Datastore vSphere VMFS - protocollo storage Fibre Channel over Ethernet con ONTAP

#### A proposito di questa attività

In questa sezione viene illustrata la creazione di un datastore VMFS con il protocollo di trasporto Fibre Channel over Ethernet (FCoE) allo storage ONTAP.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

#### Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select) che esegue ONTAP 9,8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente e password)
- ["Una combinazione FCoE supportata"](#)
- ["Un foglio di lavoro di configurazione completo"](#)
- Credenziali vCenter Server
- Informazioni sugli host vSphere
  - vSphere 7,0 o versione successiva
- Switch fabric
  - Con porte dati ONTAP FC o host vSphere collegati
  - Con la funzione NPIV (N\_Port ID Virtualization) attivata
  - Creare una singola zona di destinazione dell'iniziatore.
  - ["Zoning FC/FCoE configurato"](#)
- Switch di rete
  - Supporto FCoE
  - Supporto DCB
  - ["Frame jumbo per FCoE"](#)
- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

## Eeguire il provisioning di un datastore VMFS

- Verificare la compatibilità con ["Tool di matrice di interoperabilità \(IMT\)"](#).
- ["Verificare che la configurazione FCoE sia supportata"](#).

## Attività di ONTAP

1. ["Verificare la licenza ONTAP per FCP."](#)
  - a. Utilizzare `system license show` Per verificare che l'FCP sia presente nell'elenco.
  - b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. Verificare che il protocollo FCP sia attivato su SVM.
  - a. ["Verificare l'FCP su una SVM esistente."](#)
  - b. ["Configurare l'FCP su una SVM esistente."](#)
  - c. ["Creare una nuova SVM con FCP."](#)
3. Verificare che le interfacce logiche FCP siano disponibili su SVM.
  - a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.
  - b. Quando la SVM viene creata con la GUI, le interfacce logiche fanno parte di tale processo.
  - c. Per rinominare l'interfaccia di rete, utilizzare `Network Interface modify`.
4. ["Creare e mappare un LUN"](#); Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere.

## Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili in ["informazioni sull'adattatore di storage"](#).
2. ["Eeguire il provisioning di un datastore VMFS con gli strumenti ONTAP"](#).

## Datastore vSphere VMFS - backend storage iSCSI con ONTAP

### A proposito di questa attività

In questa sezione viene descritta la creazione di un datastore VMFS con lo storage iSCSI ONTAP.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con ONTAP 9,8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente e password)
- Informazioni su porta di rete ONTAP, SVM e LUN per iSCSI
- ["Un foglio di lavoro di configurazione iSCSI completo"](#)
- Credenziali vCenter Server
- Informazioni sugli host vSphere
  - vSphere 7,0 o versione successiva
- Informazioni IP adattatore VMkernel iSCSI

- Switch di rete
  - Con porte dati di rete del sistema ONTAP e host vSphere collegati
  - VLAN configurate per iSCSI
  - (Opzionale) link aggregation configurato per le porte dati di rete ONTAP
- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

## Fasi

1. Verificare la compatibilità con "Tool di matrice di interoperabilità (IMT)".
2. "Verificare che la configurazione iSCSI sia supportata."
3. Completare le seguenti attività di ONTAP e vSphere.

## Attività di ONTAP

1. "Verificare la licenza ONTAP per iSCSI".
  - a. Utilizzare `system license show` Comando per verificare se iSCSI è presente nell'elenco.
  - b. Utilizzare `license add -license-code <license code>` per aggiungere la licenza.
2. "Verificare che il protocollo iSCSI sia attivato su SVM."
3. Verificare che le interfacce logiche di rete iSCSI siano disponibili su SVM.



Quando si crea una SVM utilizzando la GUI, vengono create anche le interfacce di rete iSCSI.

4. Utilizzare `Network interface` per visualizzare o apportare modifiche all'interfaccia di rete.



Si consigliano due interfacce di rete iSCSI per nodo.

5. "Creare un'interfaccia di rete iSCSI." È possibile utilizzare la policy di servizio `default-data-block`.
6. "Verificare che il servizio dati-iscsi sia incluso nella politica di servizio." È possibile utilizzare `network interface service-policy show` per verificare.
7. "Verificare che i frame jumbo siano attivati."
8. "Creare e mappare il LUN." Saltare questo passaggio se si utilizzano i tool ONTAP per VMware vSphere. Ripetere questo passaggio per ogni LUN.

## Attività di VMware vSphere

1. Verificare che almeno una NIC sia disponibile per la VLAN iSCSI. Due schede di rete sono preferite per migliorare le performance e la tolleranza agli errori.
2. "Identificare il numero di NIC fisiche disponibili sull'host vSphere."
3. "Configurare iSCSI Initiator." Un caso d'utilizzo tipico è un iniziatore iSCSI software.
4. "Verificare che lo stack TCP/IP per iSCSI sia disponibile".
5. "Verificare che i portgroup iSCSI siano disponibili".
  - In genere utilizziamo un singolo switch virtuale con più porte di uplink.
  - Utilizzare la mappatura dell'adattatore 1:1.

6. Verificare che gli adattatori VMkernel iSCSI siano abilitati per corrispondere al numero di NIC e che gli IP siano assegnati.
7. ["Collegare l'adattatore software iSCSI agli adattatori VMkernel iSCSI."](#)
8. ["Eseguire il provisioning del datastore VMFS con gli strumenti ONTAP"](#). Ripetere questo passaggio per tutti gli archivi dati.
9. ["Verificare il supporto dell'accelerazione hardware."](#)

#### Quali sono le prossime novità?

Una volta completate queste attività, il datastore VMFS è pronto per il provisioning delle macchine virtuali.

#### Ansible Playbook

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
    - name: Generate a Session ID for ONTAP tools with vCenter
      uri:
        url: "https://{{ ontap_tools_ip
        }}:8143/api/rest/2.0/security/user/login"
        validate_certs: false
        method: POST
        return_content: yes
        body_format: json
        body:
          vcenterUserName: "{{ vcenter_username }}"
          vcenterPassword: "{{ vcenter_password }}"
      register: login

    # Get existing registered ONTAP Cluster info with ONTAP tools
```

```

- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false
    method: GET
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      cluster-id: "{{ ontap_svm_id }}"
  when: ontap_svm_id != ''
  register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:
    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
  vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB

```

```

    set_fact:
        datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
  uri:
    url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
    validate_certs: false
    method: GET
    return_content: yes
    body_format: json
    headers:
        vmware-api-session-id: "{{ vcllogin.json.value }}"
  when: vsphere_cluster != ''
  register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]
    body_format: json
    body:
        traditionalDatastoreRequest:
            name: "{{ iscsi_datastore_name }}"
            datastoreType: VMFS
            protocol: ISCSI
            spaceReserve: Thin
            clusterID: "{{ ontap_cluster_id }}"
            svmID: "{{ ontap_svm_id }}"
            targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
            datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
            vmfsFileSystem: VMFS6
            aggrName: "{{ aggr_name }}"
            existingFlexVolName: ""
            volumeStyle: FLEXVOL
            datastoreClusterMoref: ""
    headers:
        vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''

```

```
register: result
changed_when: result.status == 200
```

## Archivio dati vSphere VMFS - NVMe/FC con ONTAP

### A proposito di questa attività

In questa sezione viene descritta la creazione di un datastore VMFS con storage ONTAP utilizzando NVMe/FC.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o. [\[Terraform\]](#).

### Di cosa hai bisogno

- Competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- ["Comprensione di base di NVMe/FC"](#).
- Un sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/ASA) con ONTAP 9,8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente e password)
- WWPN ONTAP per informazioni su host, destinazione, SVM e LUN
- ["Un foglio di lavoro di configurazione FC completo"](#)
- Server vCenter
- Informazioni sugli host vSphere (vSphere 7,0 o versioni successive)
- Switch fabric
  - Con porte dati ONTAP FC e host vSphere collegati.
  - Con la funzione NPIV (N\_Port ID Virtualization) attivata.
  - Creare una singola zona di destinazione dell'iniziatore.
  - Creare una zona per ciascun iniziatore (singola zona iniziatore).
  - Per ciascuna zona, includere una destinazione che sia l'interfaccia logica FC ONTAP (WWPN) per le SVM. Devono essere presenti almeno due interfacce logiche per nodo per SVM. Non utilizzare la WWPN delle porte fisiche.

### Provisioning del datastore VMFS

1. Verificare la compatibilità con ["Tool di matrice di interoperabilità \(IMT\)"](#).
2. ["Verificare che la configurazione NVMe/FC sia supportata."](#)

### Attività di ONTAP

1. ["Verificare la licenza ONTAP per FCP."](#) Utilizzare `system license show` E verificare se NVMe\_of è elencato. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. Verificare che il protocollo NVMe sia attivato sulla SVM.
  - a. ["Configurare le SVM per NVMe."](#)
3. Verificare che le interfacce logiche NVMe/FC siano disponibili sulle SVM.
  - a. Utilizzare `Network Interface show` Per verificare l'adattatore FCP.

- b. Quando si crea una SVM con la GUI, le interfacce logiche fanno parte di tale processo.
  - c. Per rinominare l'interfaccia di rete, utilizzare il comando `Network Interface modify`.
4. ["Creare lo spazio dei nomi e il sottosistema NVMe"](#)

#### Attività di VMware vSphere

1. Verificare che i driver HBA siano installati. Gli HBA supportati da VMware dispongono di driver implementati e devono essere visibili all'indirizzo ["Informazioni sull'adattatore di storage"](#)
2. ["Eseguire l'installazione del driver vSphere host NVMe e le attività di convalida"](#)
3. ["Crea datastore VMFS"](#)

## Provisioning tradizionale dello storage di file vSphere con ONTAP

VMware vSphere supporta i seguenti protocolli NFS, entrambi compatibili con ONTAP.

- ["NFS versione 3"](#)
- ["NFS versione 4.1"](#)

Se hai bisogno di aiuto per selezionare la versione NFS corretta per vSphere, controlla ["Questo confronto tra le versioni dei client NFS"](#).

#### Riferimento

["Caratteristiche del datastore e del protocollo vSphere: NFS"](#)

### Datastore vSphere NFS - versione 3 con ONTAP

#### A proposito di questa attività

Creazione di datastore NFS versione 3 con storage NAS ONTAP.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

#### Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP.
- Un sistema storage ONTAP (file FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp) con ONTAP 9.8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente, password)
- Informazioni su porta di rete ONTAP, SVM e LUN per NFS
  - ["Un foglio di lavoro di configurazione NFS completo"](#)
- Credenziali vCenter Server
- Informazioni sugli host vSphere per vSphere 7.0 o versioni successive
- NFS VMkernel adapter IP information
- Switch di rete
  - Con porte dati di rete del sistema ONTAP e host vSphere collegati
  - VLAN configurate per NFS

- (Opzionale) link aggregation configurato per le porte dati di rete ONTAP
- Tool ONTAP per VMware vSphere implementato, configurato e pronto all'uso

## Fasi

- Verificare la compatibilità con ["Tool di matrice di interoperabilità \(IMT\)"](#)
  - ["Verificare che la configurazione NFS sia supportata."](#)
- Completare le seguenti attività di ONTAP e vSphere.

## Attività di ONTAP

1. ["Verificare la licenza ONTAP per NFS."](#)
  - a. Utilizzare `system license show` Controllare che NFS sia presente nell'elenco.
  - b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. ["Seguire il workflow di configurazione di NFS."](#)

## Attività di VMware vSphere

["Seguire il flusso di lavoro per la configurazione del client NFS per vSphere."](#)

## Riferimento

["Caratteristiche del datastore e del protocollo vSphere: NFS"](#)

## Quali sono le prossime novità?

Una volta completate queste attività, il datastore NFS è pronto per il provisioning delle macchine virtuali.

## Archivio dati vSphere NFS - versione 4.1 con ONTAP

### A proposito di questa attività

Questa sezione descrive la creazione di un datastore NFS versione 4.1 con storage NAS ONTAP.

Per il provisioning automatizzato, utilizzare uno dei seguenti script: [\[PowerShell\]](#), [\[Ansible\]](#), o [\[Terraform\]](#).

### Di cosa hai bisogno

- Le competenze di base necessarie per gestire un ambiente vSphere e ONTAP
- Sistema storage ONTAP (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) con ONTAP 9,8 o versione successiva
- Credenziali ONTAP (nome SVM, ID utente, password)
- Informazioni su porta di rete ONTAP, SVM e LUN per NFS
- ["Un foglio di lavoro di configurazione NFS completo"](#)
- Credenziali vCenter Server
- Informazioni sugli host vSphere 7,0 o versioni successive
- NFS VMkernel adapter IP information
- Switch di rete

- Con porte dati di rete del sistema ONTAP, host vSphere e connessi
- VLAN configurate per NFS
- (Opzionale) link aggregation configurato per le porte dati di rete ONTAP
- Tool ONTAP per VMware vSphere implementati, configurati e pronti all'uso

#### Fasi

- Verificare la compatibilità con ["Tool di matrice di interoperabilità \(IMT\)."](#)
  - ["Verificare che la configurazione NFS sia supportata."](#)
- Completare le attività ONTAP e vSphere fornite di seguito.

#### Attività di ONTAP

1. ["Verificare la licenza ONTAP per NFS"](#)
  - a. Usare il `system license show` Comando per verificare se NFS è elencato.
  - b. Utilizzare `license add -license-code <license code>` per aggiungere una licenza.
2. ["Seguire il workflow di configurazione di NFS"](#)

#### Attività di VMware vSphere

["Seguire il flusso di lavoro Configurazione client NFS per vSphere."](#)

#### Quali sono le prossime novità?

Una volta completate queste attività, il datastore NFS è pronto per il provisioning delle macchine virtuali.

## Multicloud ibrido NetApp con soluzioni VMware

### Casi d'utilizzo di multicloud ibrido di VMware

#### Casi di utilizzo per NetApp Hybrid Multicloud con VMware

Panoramica dei casi di utilizzo importanti per l'organizzazione IT durante la pianificazione di implementazioni cloud ibrido o cloud-first.

#### Casi di utilizzo più comuni

I casi di utilizzo includono:

- Disaster recovery,
- Hosting dei carichi di lavoro durante la manutenzione del data center, \* rapida esplosione in cui sono richieste risorse aggiuntive oltre a quanto previsto nel data center locale,
- Espansione del sito VMware,
- Migrazione rapida al cloud,
- Dev/test, e.
- Modernizzazione delle applicazioni sfruttando le tecnologie supplementari del cloud.

In questa documentazione, i riferimenti al workload cloud verranno dettagliati utilizzando i casi di utilizzo di VMware. Questi casi di utilizzo sono:

- Protect (include disaster recovery e backup/ripristino)
- Migrare
- Estendi

### **Dentro il percorso DELL'IT**

La maggior parte delle organizzazioni è in viaggio verso la trasformazione e la modernizzazione. Nell'ambito di questo processo, le aziende stanno cercando di utilizzare gli investimenti VMware esistenti, sfruttando al contempo i vantaggi del cloud e esplorando i modi per rendere il processo di migrazione il più possibile perfetto. Questo approccio renderebbe molto semplice il loro impegno di modernizzazione perché i dati sono già nel cloud.

La risposta più semplice a questo scenario è rappresentata dalle offerte VMware in ogni hyperscaler. Come NetApp® Cloud Volumes, VMware offre un modo per spostare o estendere ambienti VMware on-premise su qualsiasi cloud, consentendo di mantenere risorse, competenze e strumenti on-premise esistenti durante l'esecuzione nativa dei carichi di lavoro nel cloud. Questo riduce i rischi perché non ci saranno interruzioni di servizio o necessità di modifiche IP e offre al team IT la possibilità di operare nel modo in cui si svolgono on-premise utilizzando le competenze e gli strumenti esistenti. Questo può portare a migrazioni del cloud accelerate e a una transizione molto più fluida verso un'architettura multicloud ibrida.

### **Comprendere l'importanza delle opzioni di storage NFS supplementari**

Mentre VMware in qualsiasi cloud offre funzionalità ibride uniche a tutti i clienti, opzioni di storage NFS supplementari limitate hanno limitato la sua utilità per le organizzazioni con carichi di lavoro elevati in termini di storage. Poiché lo storage è direttamente legato agli host, l'unico modo per scalare lo storage è aggiungere più host, e questo può aumentare i costi del 35-40% o più per i carichi di lavoro a elevato utilizzo dello storage. Questi carichi di lavoro necessitano solo di storage aggiuntivo, non di potenza aggiuntiva. Ma ciò significa pagare per altri host.

Consideriamo questo scenario:

Un cliente richiede solo cinque host per CPU e memoria, ma ha molte esigenze di storage e ha bisogno di 12 host per soddisfare i requisiti di storage. Questo requisito finisce per mettere a punto la scala finanziaria dovendo acquistare la potenza aggiuntiva, quando è necessario solo incrementare lo storage.

Quando stai pianificando l'adozione e la migrazione del cloud, è sempre importante valutare l'approccio migliore e seguire il percorso più semplice per ridurre gli investimenti totali. L'approccio più comune e più semplice per qualsiasi migrazione applicativa è il rehosting (noto anche come Lift and Shift) in cui non esiste una macchina virtuale (VM) o una conversione dei dati. L'utilizzo di NetApp Cloud Volumes con il software-defined data center (SDDC) VMware, integrando al contempo vSAN, offre un'opzione semplice di "lift-and-shift".

## **Desktop virtuali**

### **Virtual Desktop Services (VDS)**

#### **TR-4861: Cloud ibrido VDI con Virtual Desktop Service**

Suresh Thoppay, NetApp

NetApp Virtual Desktop Service (VDS) consente di orchestrare Remote Desktop Services (RDS) nei principali cloud pubblici e nei cloud privati. VDS supporta Windows Virtual Desktop (WVD) su Microsoft Azure. VDS automatizza molte attività che devono essere eseguite dopo l'implementazione di WVD o RDS, tra cui la configurazione delle condivisioni di file SMB (per profili utente, dati condivisi e disco principale utente), l'abilitazione delle funzionalità Windows, l'installazione di applicazioni e agenti, firewall e policy e così via.

Gli utenti utilizzano VDS per desktop dedicati, desktop condivisi e applicazioni remote. VDS fornisce eventi con script per l'automazione della gestione delle applicazioni per i desktop e riduce il numero di immagini da gestire.

VDS offre un singolo portale di gestione per la gestione delle implementazioni in ambienti cloud pubblici e privati.

### **Valore per il cliente**

L'esplosione della forza lavoro remota del 2020 ha cambiato i requisiti di business continuity. I reparti IT devono affrontare nuove sfide per il provisioning rapido di desktop virtuali e quindi richiedere agilità di provisioning, gestione remota e i vantaggi TCO di un cloud ibrido che semplifica il provisioning on-premise e delle risorse cloud. Hanno bisogno di una soluzione di cloud ibrido che:

- Affronta la realtà dello spazio di lavoro post-COVID per consentire modelli di lavoro flessibili con dinamiche globali
- Consente di eseguire turni di lavoro semplificando e accelerando l'implementazione degli ambienti di lavoro per tutti i dipendenti, dai task worker agli utenti più esigenti
- Mobilizza la forza lavoro fornendo risorse VDI ricche e sicure indipendentemente dalla posizione fisica
- Semplifica l'implementazione del cloud ibrido
- Automatizza e semplifica la gestione della riduzione dei rischi

### **Casi di utilizzo**

L'infrastruttura VDI ibrida con NetApp VDS consente ai service provider e agli amministratori dei desktop virtuali aziendali di espandere facilmente le risorse in altri ambienti cloud senza influire sugli utenti. La disponibilità di risorse on-premise offre un migliore controllo delle risorse e un'ampia scelta di opzioni (calcolo, GPU, storage e rete) per soddisfare la domanda.

Questa soluzione si applica ai seguenti casi di utilizzo:

- Nel cloud per i picchi della domanda di desktop e applicazioni remoti
- Riduzione del TCO per applicazioni e desktop remoti a esecuzione prolungata ospitandoli on-premise con storage flash e risorse GPU
- Facilità di gestione di desktop e applicazioni remoti negli ambienti cloud
- Sperimenta desktop e applicazioni remoti utilizzando un modello software-as-a-service con risorse on-premise

## **Pubblico di destinazione**

Il pubblico di riferimento per la soluzione comprende i seguenti gruppi:

- EUC/VDI Architect che vogliono comprendere i requisiti per un VDS ibrido
- Partner NetApp che desiderano assistere i clienti nelle loro esigenze di desktop remoto e applicazioni
- Clienti NetApp HCI esistenti che desiderano soddisfare le esigenze di desktop remoto e applicazioni

## **Panoramica del servizio Virtual Desktop di NetApp**

NetApp offre numerosi servizi cloud, tra cui il provisioning rapido di desktop virtuale con applicazioni WVD o remote e la rapida integrazione con Azure NetApp Files.

Tradizionalmente, il provisioning e l'erogazione di servizi desktop remoti ai clienti richiedono settimane. Oltre al provisioning, può essere difficile gestire applicazioni, profili utente, dati condivisi e oggetti di policy di gruppo per applicare le policy. Le regole del firewall possono aumentare la complessità e richiedere un set di competenze e strumenti separati.

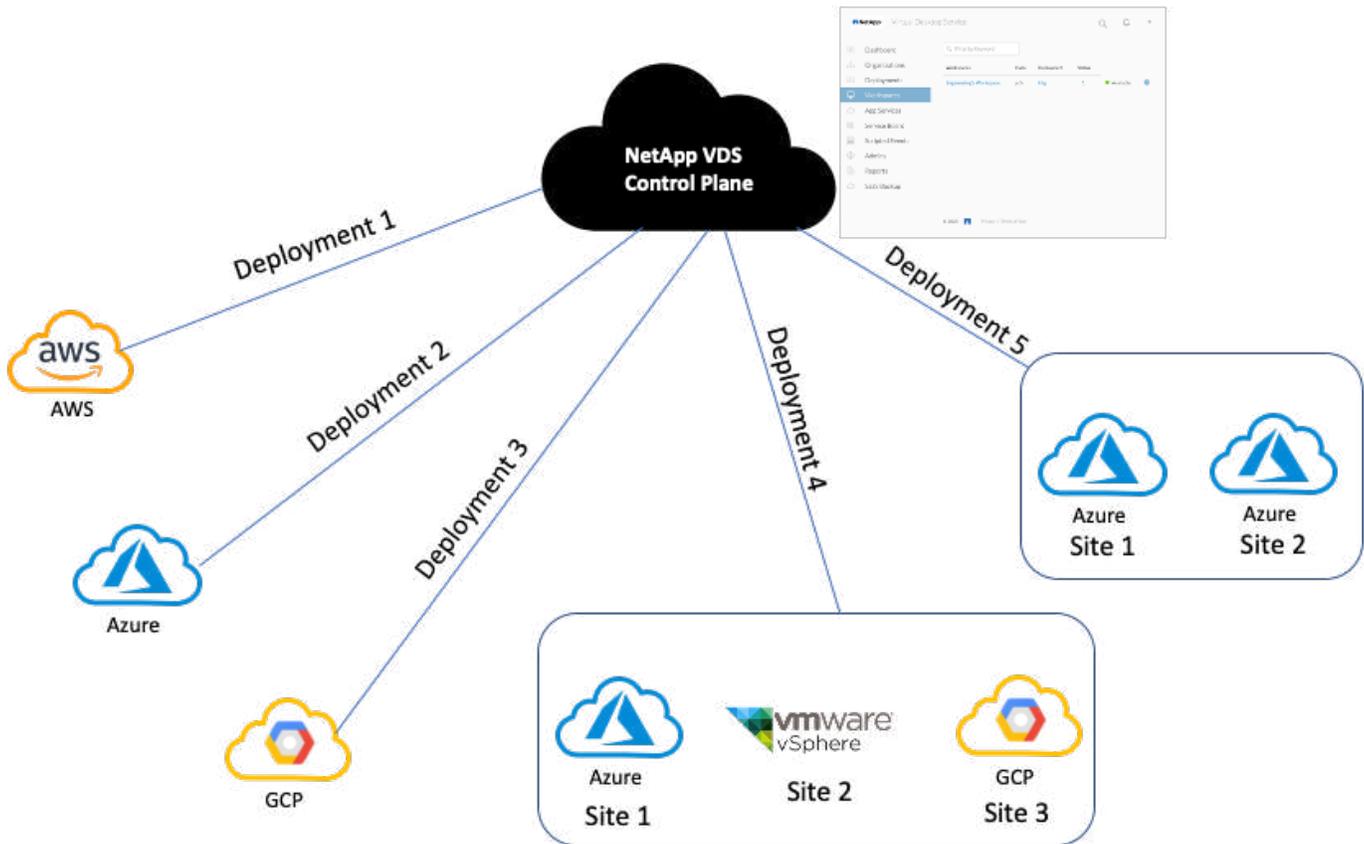
Con il servizio Microsoft Azure Windows Virtual Desktop, Microsoft si occupa della manutenzione dei componenti di Remote Desktop Services, consentendo ai clienti di concentrarsi sul provisioning delle aree di lavoro nel cloud. I clienti devono eseguire il provisioning e gestire lo stack completo, che richiede competenze speciali per gestire gli ambienti VDI.

Con NetApp VDS, i clienti possono implementare rapidamente desktop virtuali senza doversi preoccupare di dove installare i componenti dell'architettura come broker, gateway, agenti e così via. I clienti che richiedono il controllo completo del proprio ambiente possono collaborare con un team di servizi professionali per raggiungere i propri obiettivi. I clienti utilizzano i VDS come servizio e possono quindi concentrarsi sulle principali sfide aziendali.

NetApp VDS è un'offerta software-as-a-service per la gestione centralizzata di implementazioni multiple in ambienti AWS, Azure, GCP o cloud privato. Microsoft Windows Virtual Desktop è disponibile solo su Microsoft Azure. NetApp VDS consente di orchestrare i servizi di desktop remoto Microsoft in altri ambienti.

Microsoft offre sessioni multiple su Windows 10 esclusivamente per ambienti Windows Virtual Desktop su Azure. L'autenticazione e l'identità sono gestite dalla tecnologia dei desktop virtuali; WVD richiede Azure Active Directory sincronizzato (con ad Connect) con Active Directory e le VM di sessione collegate ad Active Directory. RDS richiede Active Directory per l'identità e l'autenticazione dell'utente e l'Unione e la gestione del dominio delle macchine virtuali.

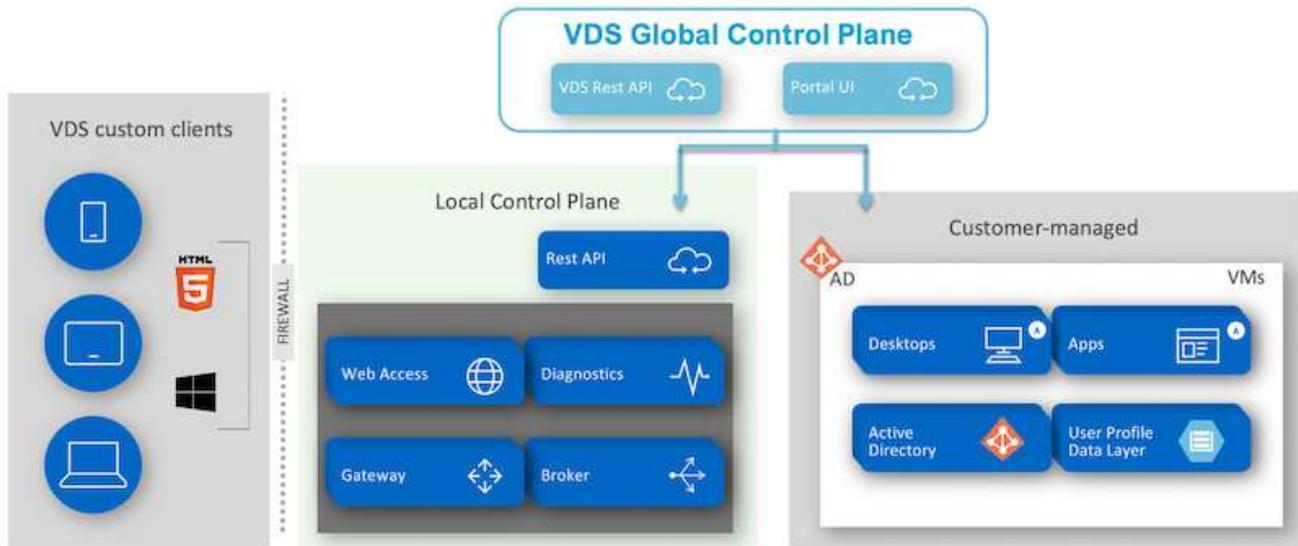
Nella figura seguente viene illustrata una topologia di implementazione di esempio.



Ogni implementazione è associata a un dominio Active Directory e fornisce ai client un punto di accesso per aree di lavoro e applicazioni. Un provider di servizi o un'azienda che dispone di più domini Active Directory ha in genere più implementazioni. Un singolo dominio Active Directory che si estende in più regioni ha in genere una singola implementazione con più siti.

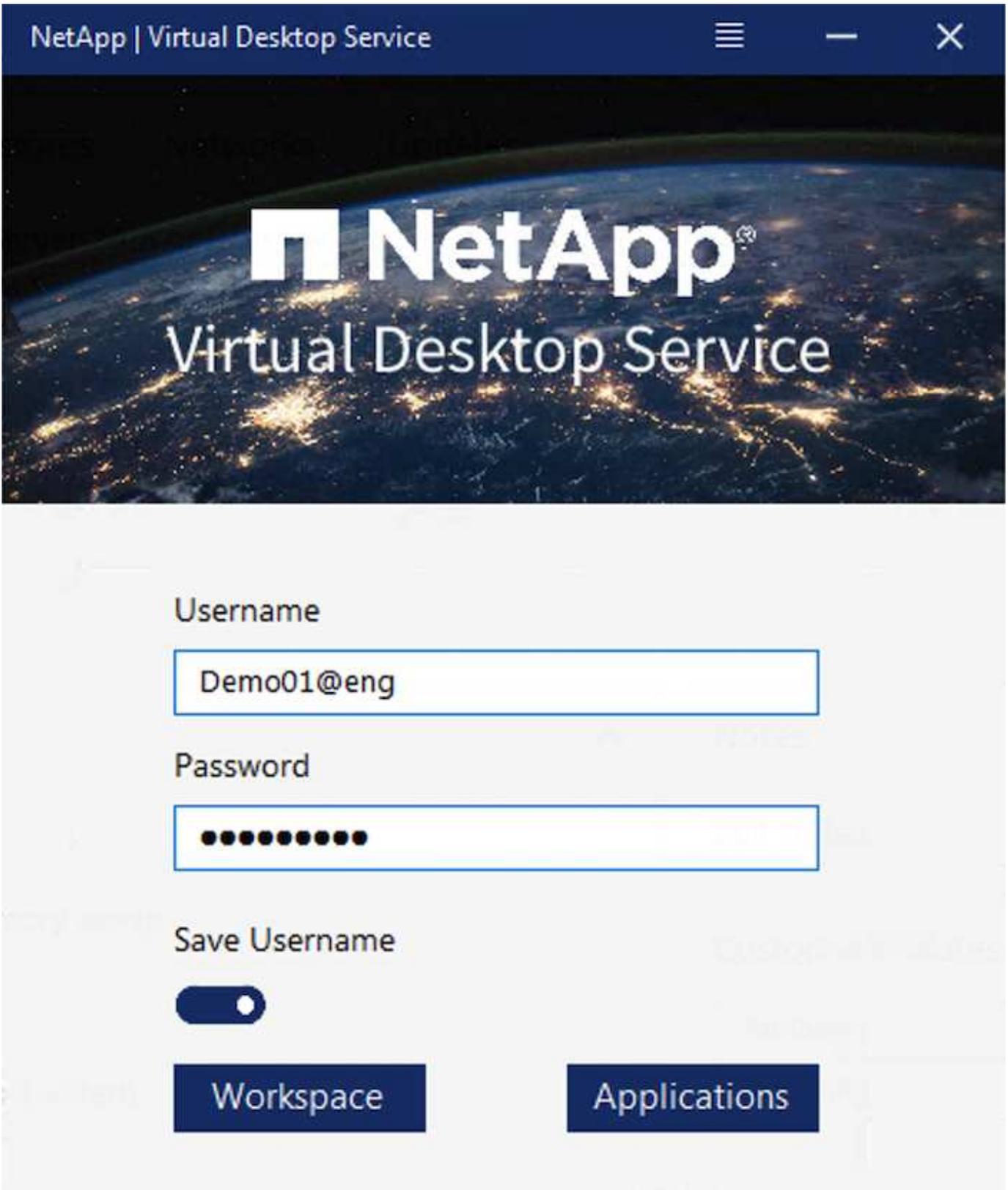
Per WVD in Azure, Microsoft fornisce un servizio Platform-as-a-Service utilizzato da NetApp VDS. Per altri ambienti, NetApp VDS orchestrerà l'implementazione e la configurazione dei servizi di desktop remoto Microsoft. NetApp VDS supporta sia WVD Classic che WVD ARM e può essere utilizzato anche per aggiornare le versioni esistenti.

Ogni implementazione dispone di servizi per la propria piattaforma, che comprendono Cloud Workspace Manager (endpoint REST API), un gateway HTML 5 (connessione alle macchine virtuali da un portale di gestione VDS), RDS Gateway (Access Point per i client) e un controller di dominio. La figura seguente mostra l'architettura del piano di controllo VDS per l'implementazione RDS.



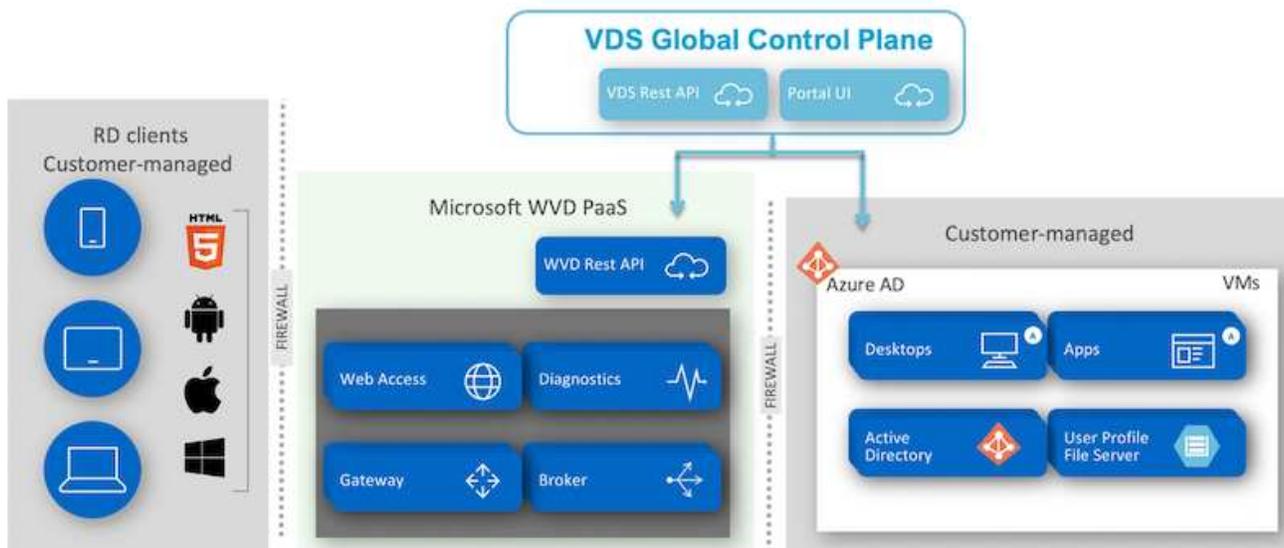
Per le implementazioni RDS, NetApp VDS può essere facilmente accessibile da Windows e dai browser utilizzando software client che può essere personalizzato per includere logo e immagini del cliente. In base alle credenziali dell'utente, fornisce all'utente l'accesso a aree di lavoro e applicazioni approvate. Non è necessario configurare i dettagli del gateway.

La figura seguente mostra il client NetApp VDS.



Nell'implementazione di Azure WVD, Microsoft gestisce l'access point per i client e può essere utilizzato da un client Microsoft WVD disponibile in modalità nativa per diversi sistemi operativi. È inoltre possibile accedervi da un portale basato su web. La configurazione del software client deve essere gestita dall'oggetto Criteri di gruppo (GPO) o in altri modi preferiti dai clienti.

La seguente figura illustra l'architettura del piano di controllo VDS per le implementazioni di Azure WVD.



Oltre all'implementazione e alla configurazione dei componenti richiesti, NetApp VDS gestisce anche la gestione degli utenti, la gestione delle applicazioni, la scalabilità delle risorse e l'ottimizzazione.

NetApp VDS può creare utenti o concedere agli account utente esistenti l'accesso allo spazio di lavoro cloud o ai servizi applicativi. Il portale può essere utilizzato anche per la reimpostazione delle password e la delega dell'amministrazione di un sottoinsieme di componenti. Gli amministratori dell'helpdesk o i tecnici di livello 3 possono affiancare le sessioni degli utenti per la risoluzione dei problemi o connettersi ai server dall'interno del portale.

NetApp VDS può utilizzare i modelli di immagine creati dall'utente oppure quelli esistenti sul mercato per il provisioning basato sul cloud. Per ridurre il numero di immagini da gestire, è possibile utilizzare un'immagine di base e il provisioning di eventuali applicazioni aggiuntive necessarie utilizzando il framework fornito per includere qualsiasi tool della riga di comando come chocolatey, MSIX app attach, PowerShell e così via. Anche gli script personalizzati possono essere utilizzati come parte degli eventi del ciclo di vita delle macchine.

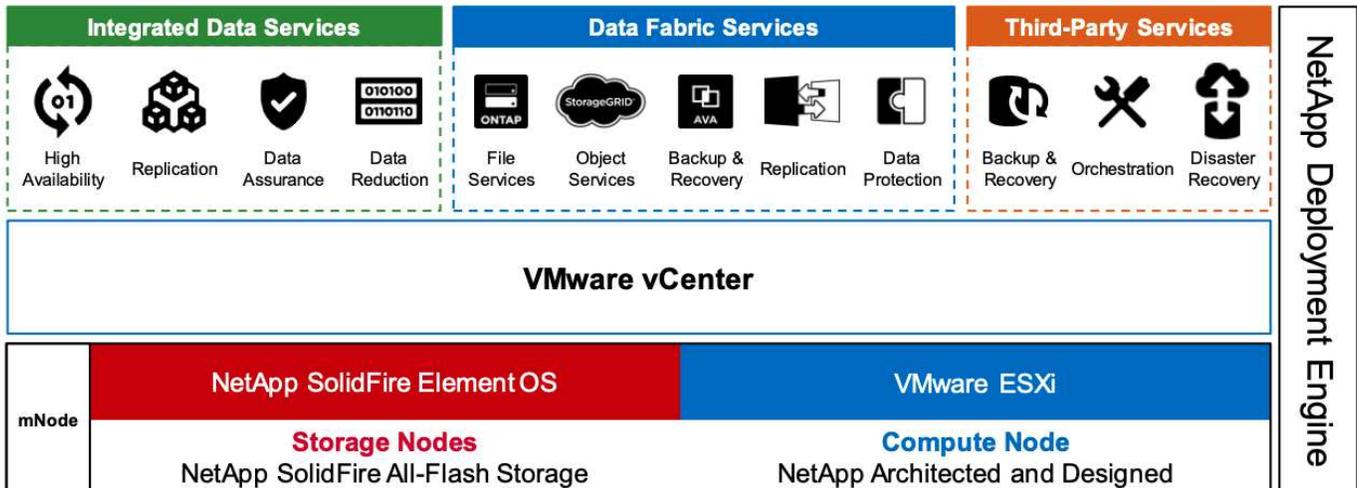
### Panoramica di NetApp HCI

NetApp HCI è un'infrastruttura di cloud ibrido costituita da una combinazione di nodi di storage e nodi di calcolo. È disponibile come unità a due rack o come unità a rack singolo, a seconda del modello. L'installazione e la configurazione necessarie per implementare le macchine virtuali sono automatizzate con NetApp Deployment Engine (NDE). I cluster di calcolo vengono gestiti con VMware vCenter e i cluster di storage vengono gestiti con il plug-in vCenter implementato con NDE. Una VM di gestione chiamata mNode viene implementata come parte di NDE.

NetApp HCI gestisce le seguenti funzioni:

- Aggiornamenti della versione
- Invio di eventi a vCenter
- Gestione del plug-in vCenter
- Tunnel VPN per il supporto
- NetApp Active IQ Collector

- L'estensione dei NetApp Cloud Services on-premise, consentendo un'infrastruttura di cloud ibrido. La figura seguente mostra i componenti HCI.



### Nodi di storage

I nodi di storage sono disponibili come unità rack a mezza larghezza o a larghezza intera. Inizialmente sono necessari almeno quattro nodi di storage e un cluster può espandersi fino a 40 nodi. Un cluster di storage può essere condiviso tra più cluster di calcolo. Tutti i nodi di storage contengono un controller della cache per migliorare le performance di scrittura. Un singolo nodo fornisce 50.000 o 100.000 IOPS con una dimensione del blocco 4K.

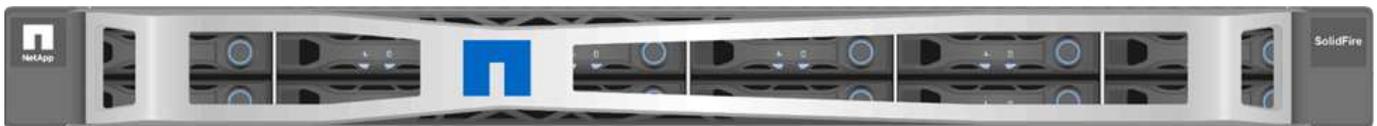
I nodi di storage NetApp HCI eseguono il software NetApp Element, che fornisce limiti di QoS minimi, massimi e burst. Il cluster di storage supporta una combinazione di nodi di storage, anche se un nodo di storage non può superare un terzo della capacità totale.

### Nodi di calcolo



NetApp supporta lo storage connesso a qualsiasi server di calcolo elencato nella ["Guida alla compatibilità VMware"](#).

I nodi di calcolo sono disponibili in metà larghezza, larghezza completa e due dimensioni di unità rack. I modelli NetApp HCI H410C e H610C sono basati su processori scalabili Intel Skylake. H615C è basato su processori scalabili Intel Cascade Lake di seconda generazione. Esistono due modelli di calcolo che contengono GPU: Il modello H610C contiene due schede NVIDIA M10 e il modello H615C contiene tre schede NVIDIA T4.



NVIDIA T4 dispone di 40 core RT che forniscono la potenza di calcolo necessaria per fornire il ray tracing in tempo reale. Lo stesso modello di server utilizzato da progettisti e ingegneri può ora essere utilizzato anche dagli artisti per creare immagini fotorealistiche con luce che rimbalza dalle superfici proprio come nella vita reale. Questa GPU compatibile con RTX produce prestazioni di ray tracing in tempo reale fino a cinque Giga raggi al secondo. NVIDIA T4, se combinata con il software quadro Virtual Data Center Workstation (quadro VDWS), consente agli artisti di creare design fotorealistici con ombre, riflessi e rifrazioni precise su qualsiasi dispositivo da qualsiasi posizione.

I core Tensor ti consentono di eseguire carichi di lavoro di deduzione per l'apprendimento approfondito. Durante l'esecuzione di questi carichi di lavoro, NVIDIA T4 con quadro VDWS offre prestazioni fino a 25 volte più veloci rispetto a una macchina virtuale gestita da un server solo CPU. NetApp H615C con tre schede NVIDIA T4 in un'unità rack è la soluzione ideale per la grafica e i carichi di lavoro a elaborazione intensiva.

La figura seguente elenca le schede NVIDIA GPU e ne confronta le caratteristiche.

NVIDIA GPUs Recommended for Virtualization						
	V100S	RTX 8000	RTX 6000	T4	M10	P6
GPU	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
CUDA Cores	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
Tensor Cores	640	576	576	320	—	—
RT Cores	—	72	72	40	—	—
Guaranteed QoS (GPU Scheduler)	✓	✓	✓	✓	—	✓
Live Migration	✓	✓	✓	✓	✓	✓
Multi-vGPU	✓	✓	✓	✓	✓	✓
Memory Size	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
vGPU Profiles	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
Form Factor	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
Power	250 W /300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
Thermal	passive	passive	passive	passive	passive	bare board
vGPU Software Support	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
Use Case	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to high-end 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multi-monitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

La GPU M10 rimane la migliore soluzione TCO per i casi di utilizzo dei knowledge worker. Tuttavia, il T4 rappresenta un'ottima alternativa quando si desidera standardizzare su una GPU che può essere utilizzata in diversi casi di utilizzo, come workstation virtuali, performance grafiche, rendering interattivo in tempo reale e deduzione. Con il T4, l'IT può sfruttare le stesse risorse GPU per eseguire carichi di lavoro misti—ad esempio, eseguendo VDI durante il giorno e riutilizzando le risorse per eseguire i carichi di lavoro di calcolo di notte.

Il nodo di calcolo H610C è costituito da due unità rack; il modello H615C è un'unità rack di dimensioni pari a una e consuma meno energia. Il modello H615C supporta la codifica e la decodifica H.264 e H.265 (High Efficiency Video Coding [HEVC]) 4:4:4. Supporta anche il decoder VP9 sempre più diffuso; anche il pacchetto container WebM fornito da YouTube utilizza il codec VP9 per il video.

Il numero di nodi in un cluster di calcolo è determinato da VMware; attualmente è 96 con VMware vSphere 7.0 Update 1. La combinazione di diversi modelli di nodi di calcolo in un cluster è supportata quando è attivata la compatibilità vMotion avanzata (EVC).

### Licenze NVIDIA

Quando si utilizza un H610C o H615C, la licenza per la GPU deve essere acquistata dai partner NVIDIA autorizzati a rivendere le licenze. È possibile trovare i partner NVIDIA con ["ricerca partner"](#). Cerca competenze come GPU virtuale (vGPU) o Tesla.

Il software NVIDIA vGPU è disponibile in quattro edizioni:

- NVIDIA GRID Virtual PC (GRID VPC)

- Applicazioni virtuali NVIDIA GRID (GRID vApps)
- Workstation NVIDIA quadro Virtual Data Center (quadro VDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

## PC virtuale GRID

Questo prodotto è ideale per gli utenti che desiderano un desktop virtuale che offra un'esperienza utente ottimale per applicazioni Microsoft Windows, browser, video ad alta definizione e supporto multi-monitor. NVIDIA GRID Virtual PC offre un'esperienza nativa in un ambiente virtuale, consentendo di eseguire tutte le applicazioni del PC a piene performance.

## APPLICAZIONI Grid Virtual

LE APPLICAZIONI GRID vApps sono destinate alle organizzazioni che implementano un Remote Desktop Session host (RDSH) o altre soluzioni basate su sessioni o streaming di applicazioni. Progettati per offrire applicazioni Microsoft Windows alle massime performance, i desktop RDSH ospitati da Windows Server sono supportati anche DA GRID vApps.

## Quadro Virtual Data Center Workstation

Questa edizione è ideale per i designer mainstream e high-end che utilizzano potenti applicazioni per la creazione di contenuti 3D come Dassault CATIA, SOLIDWORKS, 3Dexcite, Siemens NX, PTC Creo, Schlumberger Petrel, o Autodesk Maya. NVIDIA quadro VDWS consente agli utenti di accedere alle proprie applicazioni grafiche professionali con funzionalità e prestazioni complete, ovunque si trovino su qualsiasi dispositivo.

## NVIDIA Virtual ComputeServer

Molte organizzazioni eseguono carichi di lavoro server a elaborazione intensiva come intelligenza artificiale (ai), deep learning (DL) e data science. In questi casi di utilizzo, il software NVIDIA vComputeServer virtualizza la GPU NVIDIA, che accelera i carichi di lavoro dei server a elaborazione intensiva con funzionalità come codice di correzione degli errori, eliminazione delle pagine, peer-to-peer su NVLink e multi-vGPU.



Una licenza quadro VDWS consente di utilizzare GRID VPC e NVIDIA vComputeServer.

## Implementazione

NetApp VDS può essere implementato su Microsoft Azure utilizzando un'applicazione di configurazione disponibile in base alla base di codice richiesta. La versione corrente è disponibile ["qui"](#) e la release di anteprima del prodotto in arrivo è disponibile ["qui"](#).

Vedere ["questo video"](#) per le istruzioni di implementazione.



# NetApp Virtual Desktop Service

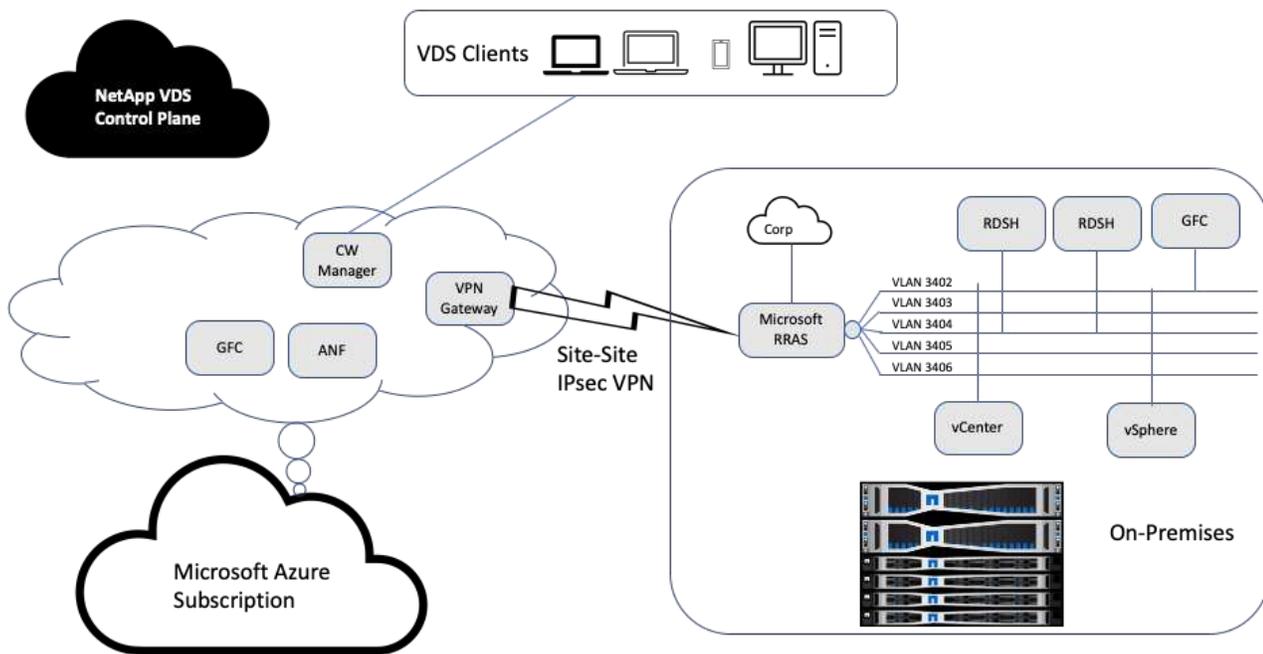
## Deployment & AD Connect

Toby vanRoojen  
Product Marketing Manager  
June, 2020

### Ambiente di cloud ibrido

NetApp Virtual Desktop Service può essere esteso a on-premise quando esiste una connettività tra risorse on-premise e risorse cloud. Le aziende possono stabilire il collegamento a Microsoft Azure utilizzando Express Route o una connessione VPN IPSec site-to-site. È inoltre possibile creare collegamenti ad altri cloud in modo simile utilizzando un collegamento dedicato o un tunnel VPN IPSec.

Per la convalida della soluzione, abbiamo utilizzato l'ambiente illustrato nella figura seguente.



On-premise, avevamo più VLAN per la gestione, host di sessione desktop remoto e così via. Si trovavano nella subnet 172.21.146-150.0/24 e venivano instradati alla rete aziendale utilizzando il servizio di accesso di routing remoto Microsoft. Abbiamo anche eseguito le seguenti attività:

1. Abbiamo preso nota dell'IP pubblico di Microsoft Routing and Remote Access Server (RRAS), identificato con IPchicken.com.
2. Abbiamo creato una risorsa Virtual Network Gateway (VPN basata su routing) con Azure Subscription.
3. È stata creata la connessione che fornisce l'indirizzo del gateway di rete locale per l'IP pubblico del server Microsoft RRAS.
4. Abbiamo completato la configurazione VPN su RRAS per creare un'interfaccia virtuale utilizzando l'autenticazione pre-condivisa fornita durante la creazione del gateway VPN. Se configurata correttamente, la VPN deve trovarsi nello stato connesso. Invece di Microsoft RRAS, è possibile utilizzare pfSense o altri strumenti pertinenti per creare il tunnel VPN IPsec sito-sito. Poiché è basato su route, il tunnel reindirizza il traffico in base alle subnet specifiche configurate.

Microsoft Azure Active Directory fornisce l'autenticazione dell'identità basata su OAuth. Le autenticazioni dei client aziendali richiedono in genere l'autenticazione basata su NTLM o Kerberos. I servizi di dominio Active Directory di Microsoft Azure eseguono la sincronizzazione dell'hash delle password tra Azure Active Directory e i controller di dominio on-premise utilizzando ADConnect.

Per la convalida di questa soluzione VDS ibrida, abbiamo inizialmente implementato Microsoft Azure e aggiunto un sito aggiuntivo con vSphere. Il vantaggio di questo approccio è che i servizi della piattaforma sono stati implementati in Microsoft Azure e quindi sono stati prontamente sottoposti a backup utilizzando il portale. È quindi possibile accedere facilmente ai servizi da qualsiasi luogo, anche se il collegamento VPN del sito non è attivo.

Per aggiungere un altro sito, abbiamo utilizzato uno strumento chiamato DCConfig. Il collegamento a tale applicazione è disponibile sul desktop della macchina virtuale CWMgr (Cloud Workspace Manager). Una volta avviata l'applicazione, accedere alla scheda DataCenter Sites (Siti DataCenter), aggiungere il nuovo sito del

data center e inserire le informazioni richieste come mostrato di seguito. L'URL punta all'IP vCenter. Assicurarsi che la macchina virtuale CWMgr possa comunicare con vCenter prima di aggiungere la configurazione.



Assicurarsi che vSphere PowerCLI 5.1 su CloudWorkspace Manager sia installato per consentire la comunicazione con l'ambiente VMware vSphere.

La seguente figura illustra la configurazione del sito del data center on-premise.

The screenshot displays the Configuration interface for DataCenter Sites. On the left, a table lists the configured sites:

DataCenter Site	Type	Is Primary	DataCenter Site Detail
Site 1	AzureRM	<input checked="" type="checkbox"/>	
Site 2	vSphere	<input type="checkbox"/>	

Below the table, a red message states: "To delete DataCenter Site(s), Select it and right click to delete".

The right side of the interface shows the configuration details for Site 2:

- DataCenter Site:** Site 2
- Hypervisor:** vSphere
- General Settings:**
  - Local VM Account:** Username: Administrator, Password: [masked]
  - Hypervisor Account:** Username: Administrator@vsphere, Password: [masked]
  - URL:** https://172.21.146.150/sdk/
  - VM Name Prefix:** [empty]
  - Max Concurrent Create Server:** 20
  - Subnet Mask:** 255.255.255.0
  - Default Gateway:** 172.21.148.250
  - Is Primary Hypervisor?:**  Yes  No
  - Must Set IpAddress Of VM:**  Yes  No
- DNS:**
  - Primary DNS:** 10.67.78.11
  - Secondary DNS:** [empty]
  - Set DNS Address:**  Yes  No
- VSphere:**
  - Data Center:** NetApp-HCI-Datacenter
  - Cluster:** [empty]
  - Resource Pool:** [empty]
  - Host Name:** [empty]
  - VM Folder:** VDS
  - Max VMs In Datastore:** -1
  - Min HD Free Space In Datastore GB:** -1
  - Min Ram Free GB:** -1

At the bottom, there are checkboxes for "Exclude VSphere DataStore" and "Exclude VSphere ResourcePools".

Tenere presente che sono disponibili opzioni di filtraggio per le risorse di calcolo in base al cluster specifico, al nome host o allo spazio libero della RAM. Le opzioni di filtraggio per le risorse di storage includono lo spazio libero minimo sugli archivi dati o il numero massimo di macchine virtuali per archivio dati. Gli archivi di dati possono essere esclusi utilizzando espressioni regolari. Fare clic sul pulsante Save (Salva) per salvare la configurazione.

Per convalidare la configurazione, fare clic sul pulsante Test o fare clic su Load Hypervisor (carica hypervisor) e selezionare un menu a discesa nella sezione vSphere. Deve essere compilato con i valori appropriati. È consigliabile mantenere l'hypervisor primario impostato su yes per il sito di provisioning predefinito.

I modelli di macchine virtuali creati su VMware vSphere vengono utilizzati come raccolte di provisioning su VDS. Le raccolte di provisioning sono disponibili in due forme: Condivisa e VDI. Il tipo di raccolta di

provisioning condiviso viene utilizzato per i servizi di desktop remoto per i quali viene applicata una singola policy di risorse a tutti i server. Il tipo di VDI viene utilizzato per le istanze di WVD per le quali il criterio di risorsa viene assegnato singolarmente. Ai server di una raccolta di provisioning può essere assegnato uno dei tre ruoli seguenti:

- **TSDATA.** combinazione di servizi terminal e ruolo del server dati.
- **TS.** servizi terminal (host di sessione).
- **DATA.** file server o database server. Quando si definisce il ruolo del server, è necessario scegliere il modello di macchina virtuale e lo storage (datastore). Il datastore scelto può essere limitato a un datastore specifico oppure è possibile utilizzare l'opzione meno utilizzata in cui il datastore viene scelto in base all'utilizzo dei dati.

Ogni implementazione dispone di risorse VM predefinite per l'allocazione delle risorse cloud in base a utenti attivi, fissi, carico del server o numero di utenti.

#### Test di carico di un singolo server con Login VSI

Il NetApp Virtual Desktop Service utilizza il protocollo Microsoft Remote Desktop per accedere alle sessioni e alle applicazioni del desktop virtuale, mentre il tool Login VSI determina il numero massimo di utenti che possono essere ospitati su un modello di server specifico. Login VSI simula l'accesso dell'utente a intervalli specifici ed esegue operazioni dell'utente come l'apertura di documenti, la lettura e la composizione di e-mail, l'utilizzo di Excel e PowerPoint, la stampa di documenti, la compressione dei file e l'esecuzione di interruzioni casuali. Quindi, misura i tempi di risposta. I tempi di risposta dell'utente sono bassi quando l'utilizzo del server è basso e aumentano quando vengono aggiunte più sessioni dell'utente. Login VSI determina la linea di base in base alle sessioni di accesso utente iniziali e riporta la sessione utente massima quando la risposta dell'utente supera i 2 secondi dalla linea di base.

NetApp Virtual Desktop Service utilizza Microsoft Remote Desktop Protocol per accedere alle applicazioni e alle sessioni di Virtual Desktop. Per determinare il numero massimo di utenti che possono essere ospitati su un modello di server specifico, è stato utilizzato il tool Login VSI. Login VSI simula l'accesso dell'utente a intervalli specifici ed esegue operazioni dell'utente come l'apertura di documenti, la lettura e la composizione di e-mail, l'utilizzo di Excel e PowerPoint, la stampa di documenti, la compressione di file, l'esecuzione di interruzioni casuali e così via. Inoltre, misura i tempi di risposta. I tempi di risposta dell'utente sono bassi quando l'utilizzo del server è basso e aumentano quando vengono aggiunte più sessioni dell'utente. Login VSI determina la linea di base in base alle sessioni di accesso utente iniziali e riporta il numero massimo di sessioni utente quando la risposta dell'utente supera i 2 secondi dalla linea di base.

La seguente tabella contiene l'hardware utilizzato per questa convalida.

Modello	Conta	Descrizione
NetApp HCI H610C	4	Tre in un cluster per i lanciatori, ad, DHCP e così via. Un server per il test del carico.
NetApp HCI H615C	1	2 x 24 C Intel Xeon Gold 6282 @2,1 GHz. 1,5 TB DI RAM.

La seguente tabella contiene il software utilizzato per la convalida.

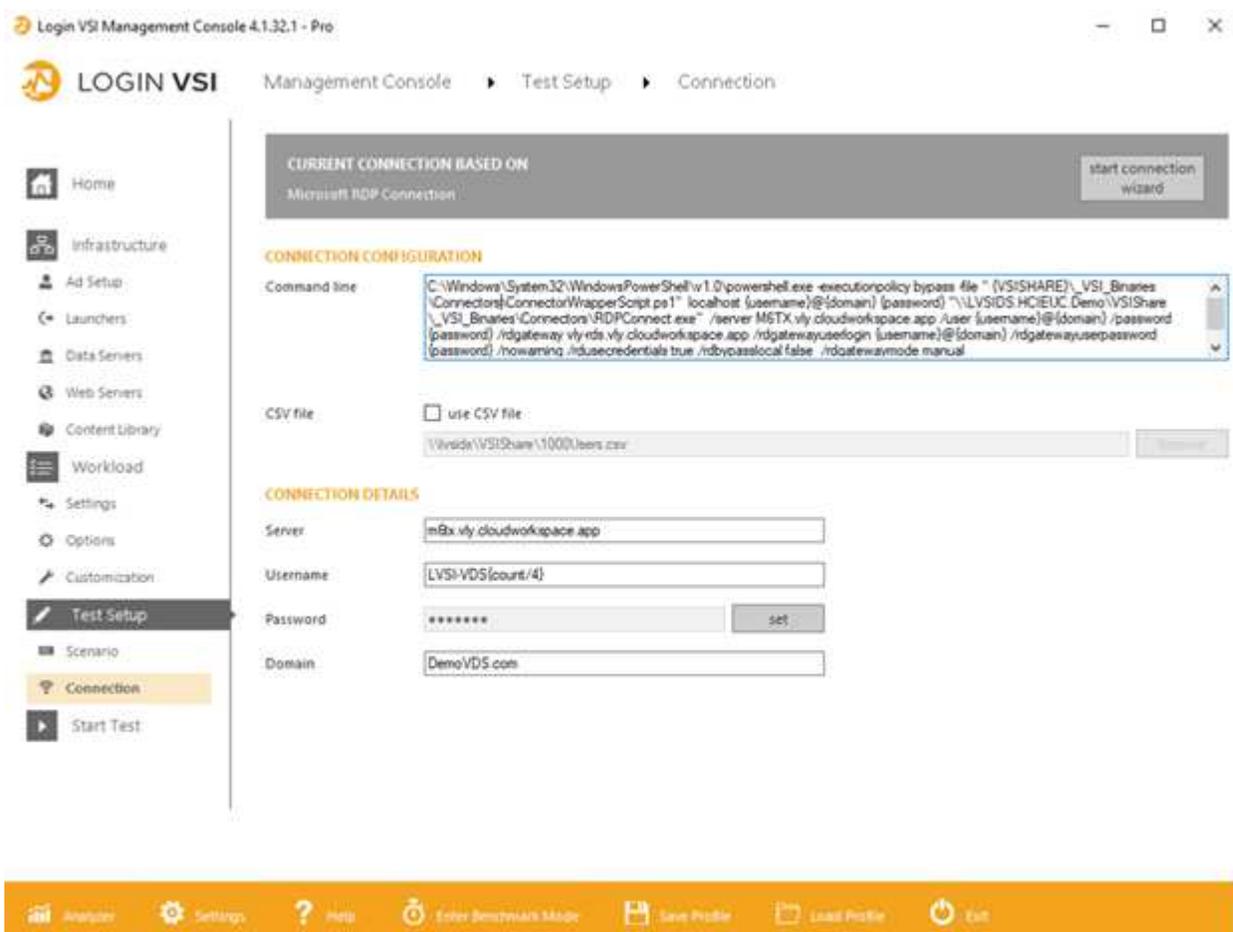
Prodotto	Descrizione
NetApp VDS 5.4	Orchestrazione
Modelli di macchine virtuali Windows 2019 1809	Sistema operativo server per RDSH
Accedere a VSI	4.1.32.1
VMware vSphere 6.7 Update 3	Hypervisor
VMware vCenter 6.7 Update 3f	Tool di gestione VMware

I risultati del test Login VSI sono i seguenti:

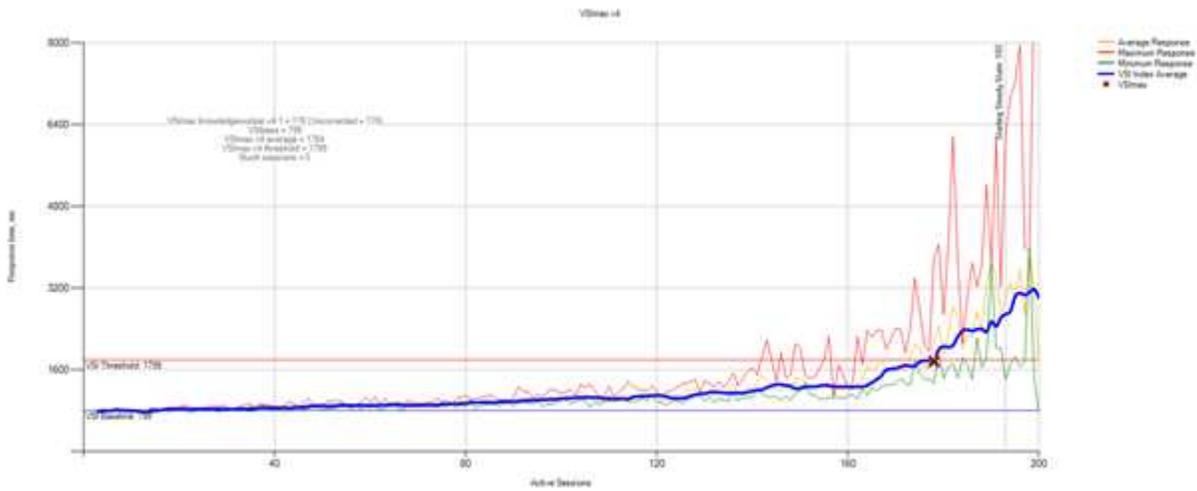
Modello	Configurazione delle macchine virtuali	Accesso VSI baseline	Accesso VSI Max
H610C	8 vCPU, 48 GB di RAM, disco da 75 GB, profilo 8Q vGPU	799	178
H615C	12 vCPU, 128 GB di RAM, disco da 75 GB	763	272

Considerando i limiti inferiori a NUMA e l'hyperthreading, le otto macchine virtuali scelte per il test e la configurazione delle macchine virtuali dipendono dai core disponibili sull'host.

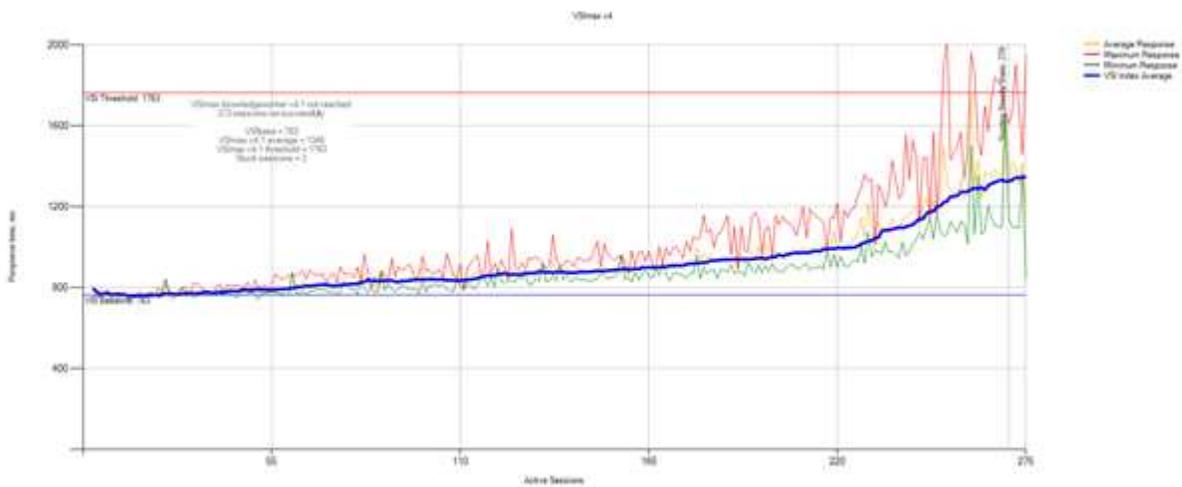
Abbiamo utilizzato 10 macchine virtuali di avvio sull'H610C, che utilizzavano il protocollo RDP per connettersi alla sessione utente. La figura seguente mostra le informazioni di connessione Login VSI.



La figura seguente mostra il tempo di risposta di Login VSI rispetto alle sessioni attive per H610C.



La figura seguente mostra il tempo di risposta di Login VSI rispetto alle sessioni attive per H615C.



Le metriche delle performance di Cloud Insights durante il test VSI di accesso H615C per host vSphere e macchine virtuali sono illustrate nella figura seguente.



## Portale di gestione

È disponibile il portale NetApp VDS Cloud Workspace Management Suite "qui" e la prossima versione è disponibile "qui".

Il portale consente la gestione centralizzata di varie implementazioni VDS, tra cui una con siti definiti per utenti on-premise, amministrativi, catalogo di applicazioni ed eventi con script. Il portale viene utilizzato anche dagli utenti amministrativi per il provisioning manuale delle applicazioni, se necessario, e per la connessione a qualsiasi computer per la risoluzione dei problemi.

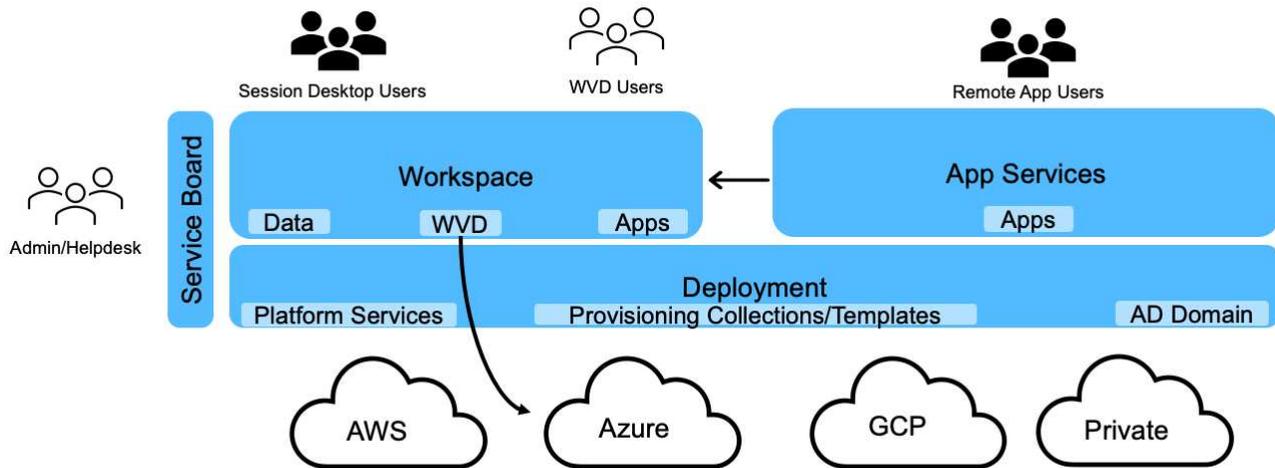
I service provider possono utilizzare questo portale per aggiungere i propri partner di canale e consentire loro di gestire i propri client.

## Gestione utenti

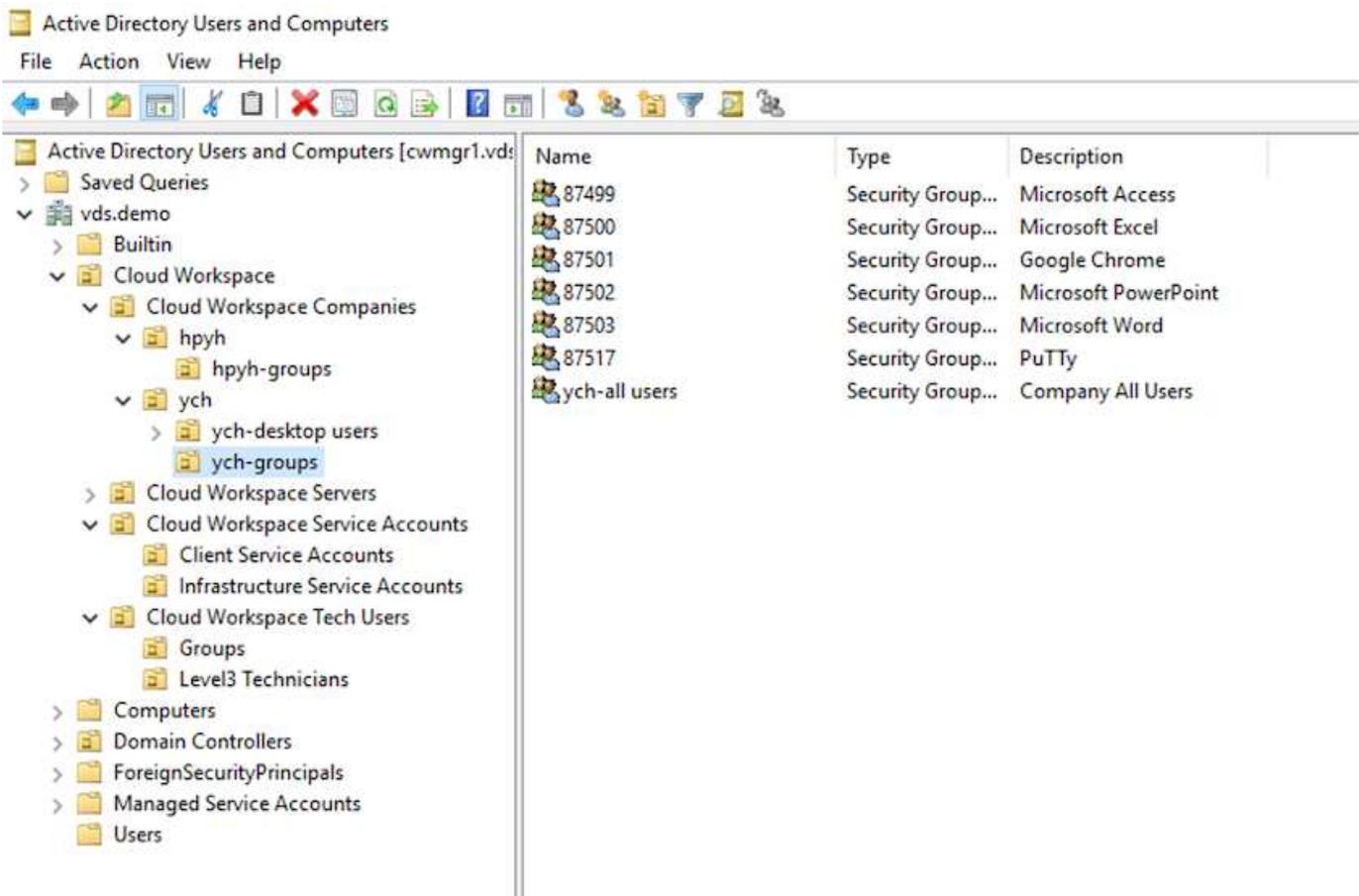
NetApp VDS utilizza Azure Active Directory per l'autenticazione dell'identità e Azure Active Directory Domain Services per l'autenticazione NTLM/Kerberos. Lo strumento ADConnect può essere utilizzato per sincronizzare un dominio Active Directory on-premise con Azure Active Directory.

È possibile aggiungere nuovi utenti dal portale oppure attivare lo spazio di lavoro cloud per gli utenti esistenti. Le autorizzazioni per le aree di lavoro e i servizi applicativi possono essere controllate da singoli utenti o da gruppi. Dal portale di gestione, è possibile definire gli utenti amministrativi per controllare le autorizzazioni per il portale, le aree di lavoro e così via.

La seguente figura illustra la gestione degli utenti in NetApp VDS.



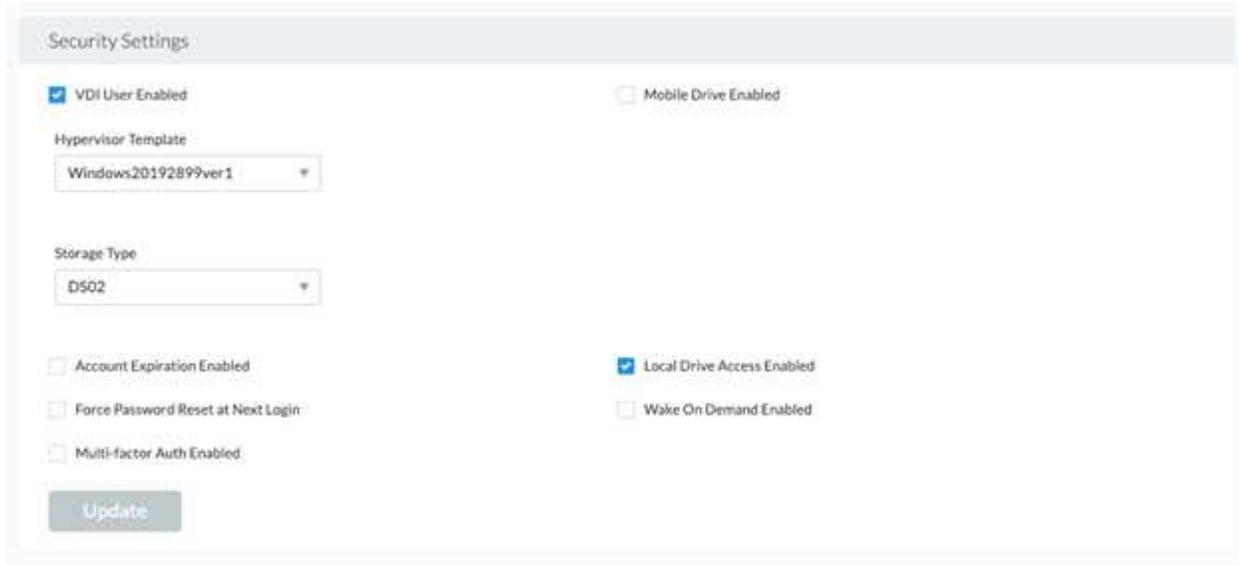
Ogni area di lavoro risiede nella propria unità organizzativa (OU) di Active Directory sotto l'unità organizzativa Cloud Workspace, come illustrato nella figura seguente.



Per ulteriori informazioni, vedere ["questo video"](#) Sulle autorizzazioni degli utenti e sulla gestione degli utenti in NetApp VDS.

Quando un gruppo Active Directory viene definito come CRAUserGroup utilizzando una chiamata API per il data center, tutti gli utenti di tale gruppo vengono importati in CloudWorkspace per la gestione mediante l'interfaccia utente. Quando l'area di lavoro cloud è attivata per l'utente, VDS crea le cartelle principali dell'utente, i permessi delle impostazioni, gli aggiornamenti delle proprietà dell'utente e così via.

Se l'opzione VDI User Enabled (utente VDI abilitato) è selezionata, VDS crea una macchina RDS a sessione singola dedicata a tale utente. Richiede il provisioning del modello e del datastore.



The screenshot shows a 'Security Settings' window with the following configuration:

- VDI User Enabled
- Mobile Drive Enabled
- Hypervisor Template: Windows20192899ver1
- Storage Type: DS02
- Account Expiration Enabled
- Local Drive Access Enabled
- Force Password Reset at Next Login
- Wake On Demand Enabled
- Multi-factor Auth Enabled

An 'Update' button is located at the bottom left of the settings panel.

### Gestione dell'area di lavoro

Un'area di lavoro è costituita da un ambiente desktop, che può essere condiviso in sessioni di desktop remoto ospitate on-premise o in qualsiasi ambiente cloud supportato. Con Microsoft Azure, l'ambiente desktop può essere persistente con i desktop virtuali Windows. Ogni area di lavoro è associata a un'organizzazione o a un client specifico. Le opzioni disponibili durante la creazione di una nuova area di lavoro sono illustrate nella figura seguente.

## New Workspace

Client & Settings
Choose Applications
Add Users
Review & Provision

Select a Client [Add](#)

No Clients Added.

**Workspace Settings**

Company Name

Primary Notification Email

**Application Settings**

Enable Remote App

Enable App Locker

Enable Application Usage Tracking

**Device Settings**

Disable Printing Access

Enable Workspace User Data Storage

**Security Settings**

Require Complex User Password

Enable MFA for All Users

Permit Access To Task Manager

Cancel
Continue



Ogni area di lavoro è associata a un'implementazione specifica.

Le aree di lavoro contengono applicazioni e servizi app associati, cartelle di dati condivise, server e un'istanza WVD. Ogni area di lavoro può controllare le opzioni di sicurezza come l'applicazione della complessità delle password, l'autenticazione a più fattori, i controlli dei file e così via.

Le aree di lavoro possono controllare la pianificazione del carico di lavoro per accendere server aggiuntivi, limitare il numero di utenti per server o impostare la pianificazione delle risorse disponibili per un determinato periodo (sempre acceso/spento). Le risorse possono anche essere configurate per l'attivazione on-demand.

Se necessario, lo spazio di lavoro può sostituire le impostazioni predefinite delle risorse delle macchine virtuali di implementazione. Per WVD, i pool di host WVD (che contengono host di sessione e gruppi di applicazioni) e le aree di lavoro WVD possono essere gestiti anche dal portale della suite di gestione dell'area di lavoro cloud. Per ulteriori informazioni sul pool di host WVD, consultare questa sezione ["video"](#).

### Gestione delle applicazioni

I task worker possono avviare rapidamente un'applicazione dall'elenco di applicazioni disponibili. I servizi app pubblicano le applicazioni dagli host della sessione di servizi Desktop remoto. Con WVD, i gruppi di applicazioni offrono funzionalità simili dai pool di host di Windows 10 a più sessioni.

Per consentire agli impiegati di potenziare gli utenti, è possibile eseguire il provisioning manuale delle applicazioni necessarie utilizzando una scheda di servizio oppure eseguire il provisioning automatico utilizzando la funzionalità di script degli eventi di NetApp VDS.

Per ulteriori informazioni, consultare ["Pagina NetApp Application Entitlement"](#).

## Funzionalità di ONTAP per il servizio di desktop virtuale

Le seguenti funzionalità di ONTAP lo rendono una scelta interessante da utilizzare con un servizio di desktop virtuale.

- **Filesystem scale-out.** i volumi ONTAP FlexGroup possono crescere fino a oltre 20 PB e possono contenere più di 400 miliardi di file all'interno di un singolo namespace. Il cluster può contenere fino a 24 nodi di storage, ciascuno con un numero flessibile di schede di interfaccia di rete a seconda del modello utilizzato.

I desktop virtuali, le cartelle home, i container dei profili utente, i dati condivisi e così via possono crescere in base alla domanda senza alcuna preoccupazione per le limitazioni del file system.

- **Analisi del file system.** puoi utilizzare il tool XCP per ottenere informazioni sui dati condivisi. Con ONTAP 9.8+ e ActiveIQ Unified Manager, è possibile eseguire query e recuperare facilmente le informazioni sui metadati dei file e identificare i dati cold.
- **Cloud Tiering.** puoi migrare i dati cold in un archivio di oggetti nel cloud o in qualsiasi storage compatibile con S3 nel tuo data center.
- **Versioni dei file.** gli utenti possono ripristinare i file protetti dalle copie Snapshot di NetApp ONTAP. Le copie Snapshot di ONTAP sono molto efficienti in termini di spazio perché registrano solo i blocchi modificati.
- **Namespace globale.** la tecnologia ONTAP FlexCache consente il caching remoto dello storage dei file, semplificando la gestione dei dati condivisi tra ubicazioni contenenti sistemi di storage ONTAP.
- **Supporto multi-tenancy sicuro.** Un singolo cluster di storage fisico può essere presentato come più array di storage virtuali ciascuno con i propri volumi, protocolli di storage, interfacce di rete logiche, dominio di identità e autenticazione, utenti di gestione e così via. Pertanto, è possibile condividere l'array di storage tra più business unit o ambienti, come test, sviluppo e produzione.

Per garantire le performance, è possibile utilizzare la QoS adattiva per impostare i livelli di performance in base allo spazio utilizzato o allocato e controllare la capacità dello storage utilizzando le quote.

- **Integrazione VMware.** i tool ONTAP per VMware vSphere forniscono un plug-in vCenter per il provisioning dei datastore, l'implementazione delle Best practice per gli host vSphere e il monitoraggio delle risorse ONTAP.

ONTAP supporta le API vStorage per l'integrazione degli array (VAAI) per l'offload delle operazioni SCSI/file nell'array di storage. ONTAP supporta inoltre le API vStorage per la consapevolezza dello storage (VASA) e il supporto dei volumi virtuali per protocolli a blocchi e file.

Il plug-in SnapCenter per VMware vSphere offre un metodo semplice per eseguire il backup e il ripristino delle macchine virtuali utilizzando la funzione Snapshot su un array di storage.

ActiveIQ Unified Manager offre visibilità della rete storage end-to-end in un ambiente vSphere. Gli amministratori possono identificare facilmente qualsiasi problema di latenza che potrebbe verificarsi negli ambienti di desktop virtuali ospitati su ONTAP.

- **Conformità alla sicurezza.** con ActiveIQ Unified Manager, è possibile monitorare più sistemi ONTAP con avvisi per eventuali violazioni delle policy.
- **Supporto multiprotocollo.** ONTAP supporta blocchi (iSCSI, FC, FCoE e NVMe/FC), file (NFSv3, NFSv4.1, SMB2.x e SMB3.x) e protocolli di storage a oggetti (S3).

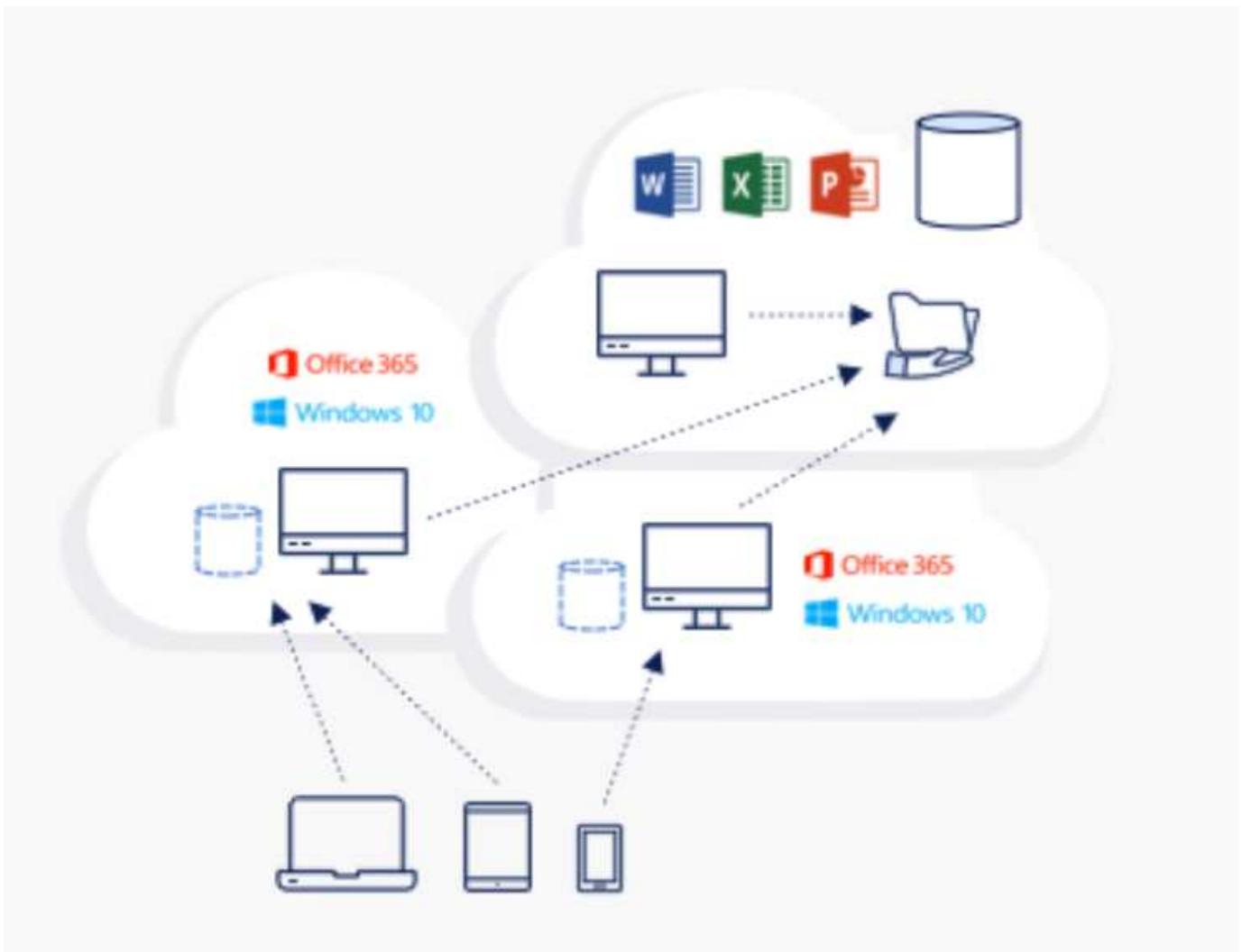
- **Supporto per l'automazione.** ONTAP fornisce moduli REST API, Ansible e PowerShell per automatizzare le attività con il portale di gestione VDS.

### Gestione dei dati

Come parte dell'implementazione, è possibile scegliere il metodo di file-service per ospitare il profilo utente, i dati condivisi e la cartella del disco principale. Le opzioni disponibili sono file server, Azure Files o Azure NetApp Files. Tuttavia, dopo l'implementazione, è possibile modificare questa scelta con il tool Command Center per puntare a qualsiasi condivisione SMB. ["L'hosting con NetApp ONTAP offre diversi vantaggi"](#). Per informazioni su come modificare la condivisione SMB, consulta ["Modifica livello dati"](#).

### Global file cache

Quando gli utenti sono distribuiti in più siti all'interno di uno spazio dei nomi globale, Global file cache può contribuire a ridurre la latenza per i dati ad accesso frequente. L'implementazione di Global file cache può essere automatizzata utilizzando una raccolta di provisioning ed eventi con script. Global file cache gestisce le cache di lettura e scrittura a livello locale e mantiene i blocchi dei file in diverse posizioni. Global file cache può funzionare con qualsiasi file server SMB, incluso Azure NetApp Files.



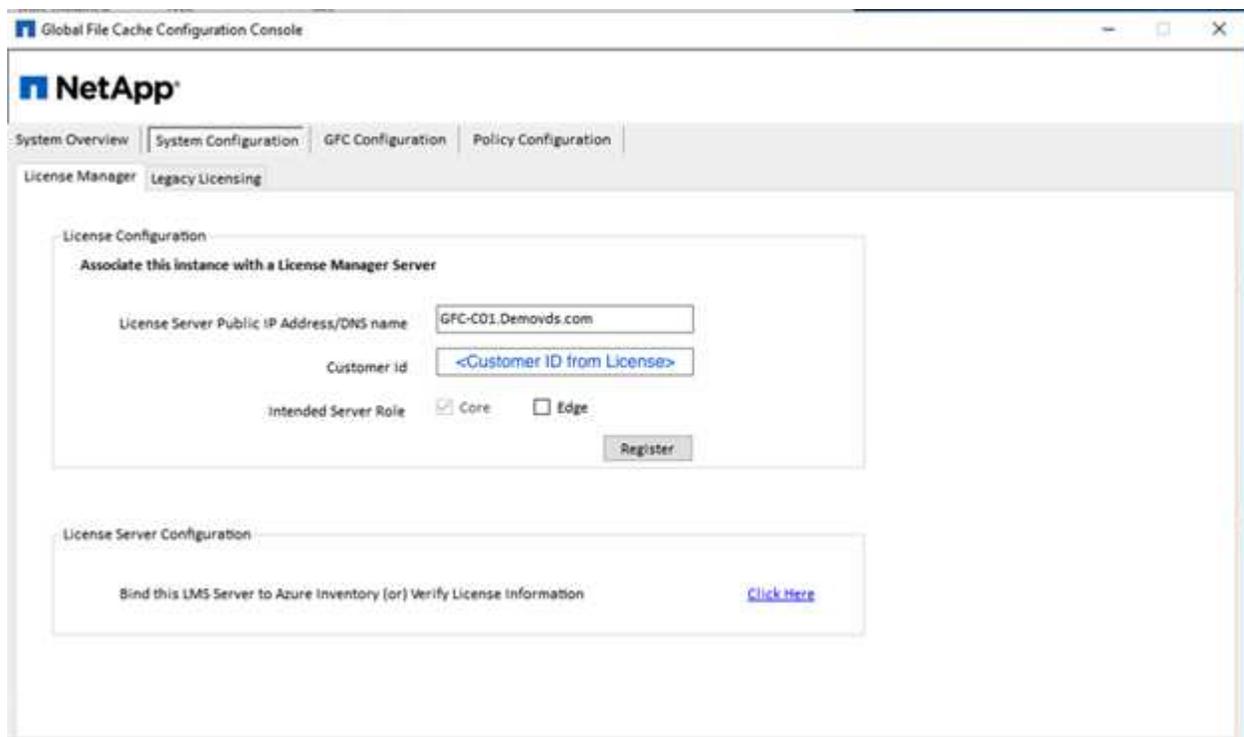
Global file cache richiede quanto segue:

- Server di gestione (server di gestione delle licenze)
- Core
- Edge con capacità disco sufficiente per memorizzare i dati nella cache

Per scaricare il software e calcolare la capacità della cache del disco per Edge, consultare "[Documentazione GFC](#)".

Per la nostra convalida, abbiamo implementato le risorse di base e di gestione sulla stessa macchina virtuale in Azure e le risorse edge in NetApp HCI. Si noti che il core è il luogo in cui è richiesto l'accesso ai dati per volumi elevati e l'edge è un sottoinsieme del core. Una volta installato il software, è necessario attivare la licenza attivata prima dell'uso. A tale scopo, attenersi alla seguente procedura:

1. Nella sezione License Configuration (Configurazione licenza), utilizzare il collegamento fare clic qui per completare l'attivazione della licenza. Quindi registrare il core.

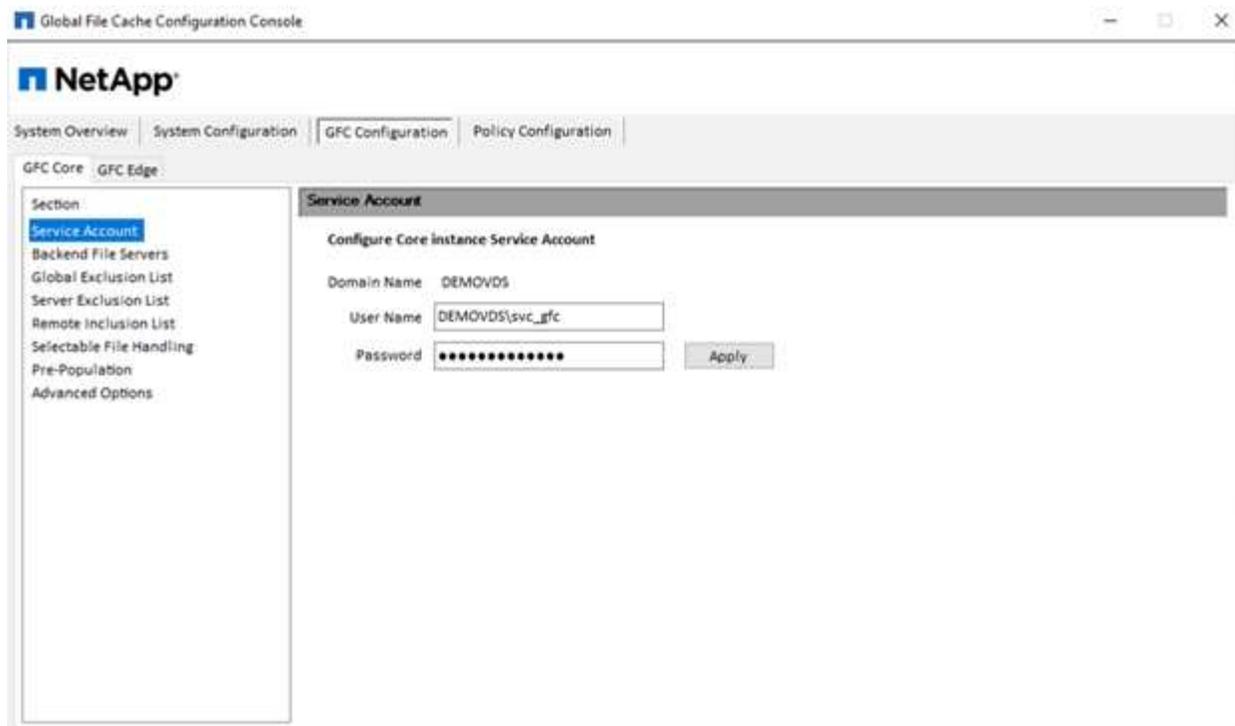


The screenshot displays the NetApp Global File Cache Configuration Console. The interface includes a navigation menu with tabs for System Overview, System Configuration, GFC Configuration, and Policy Configuration. The current view is under License Manager > Legacy Licensing. The main content area is titled 'License Configuration' and contains the following fields and options:

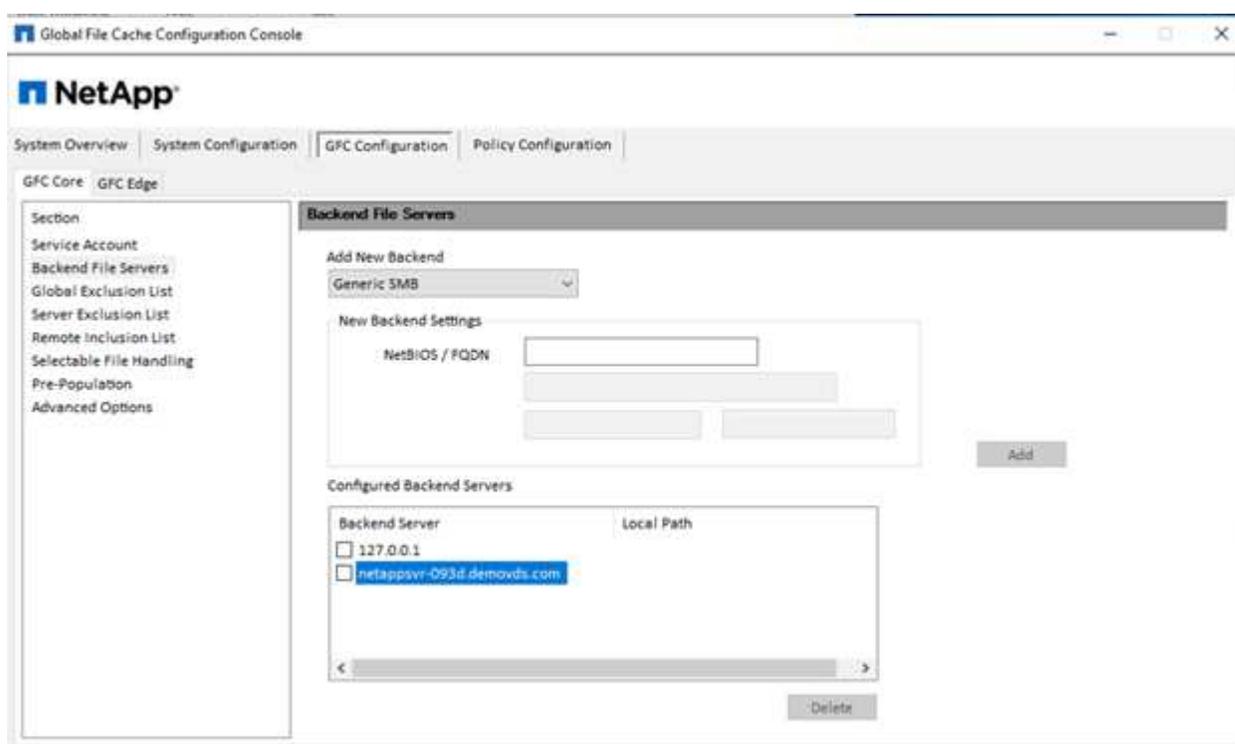
- Associate this instance with a License Manager Server**
- License Server Public IP Address/DNS name:
- Customer id:
- Intended Server Role:  Core  Edge
- 

Below this section is a 'License Server Configuration' box with the text 'Bind this LMS Server to Azure Inventory (or) Verify License Information' and a blue link labeled 'Click here'.

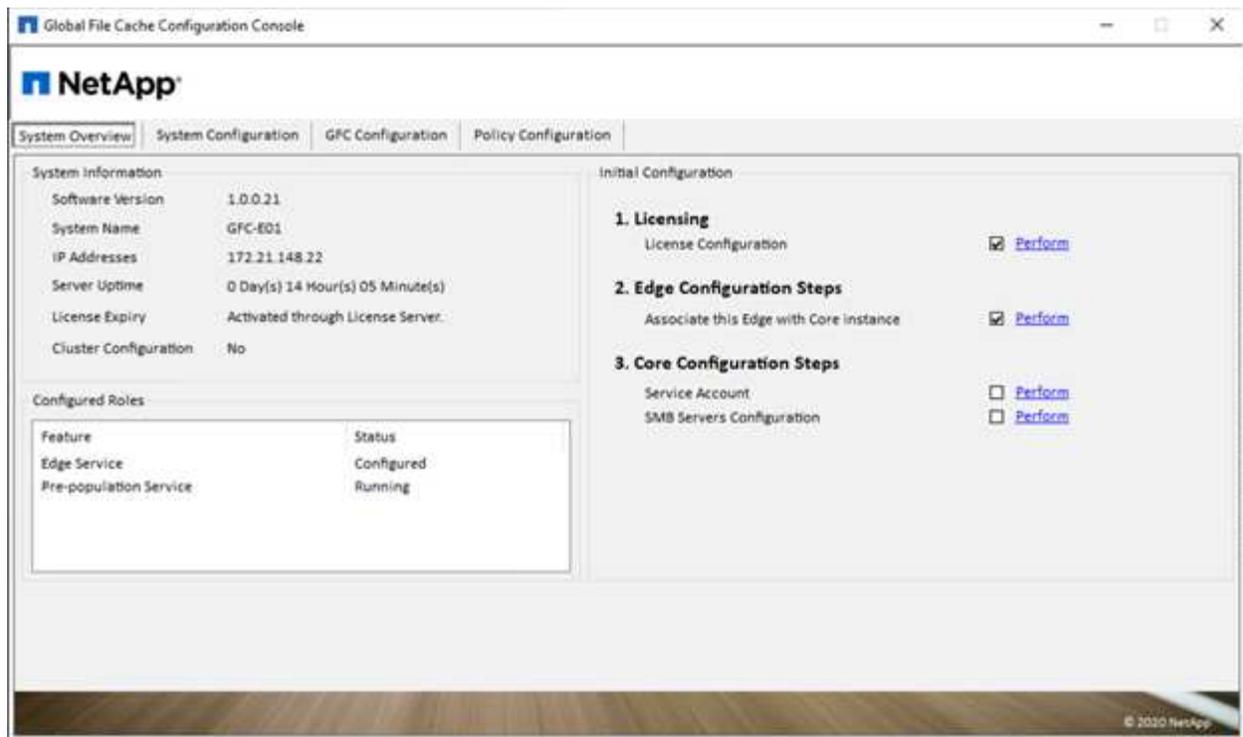
2. Fornire l'account di servizio da utilizzare per Global file cache. Per le autorizzazioni richieste per questo account, consultare "[Documentazione GFC](#)".



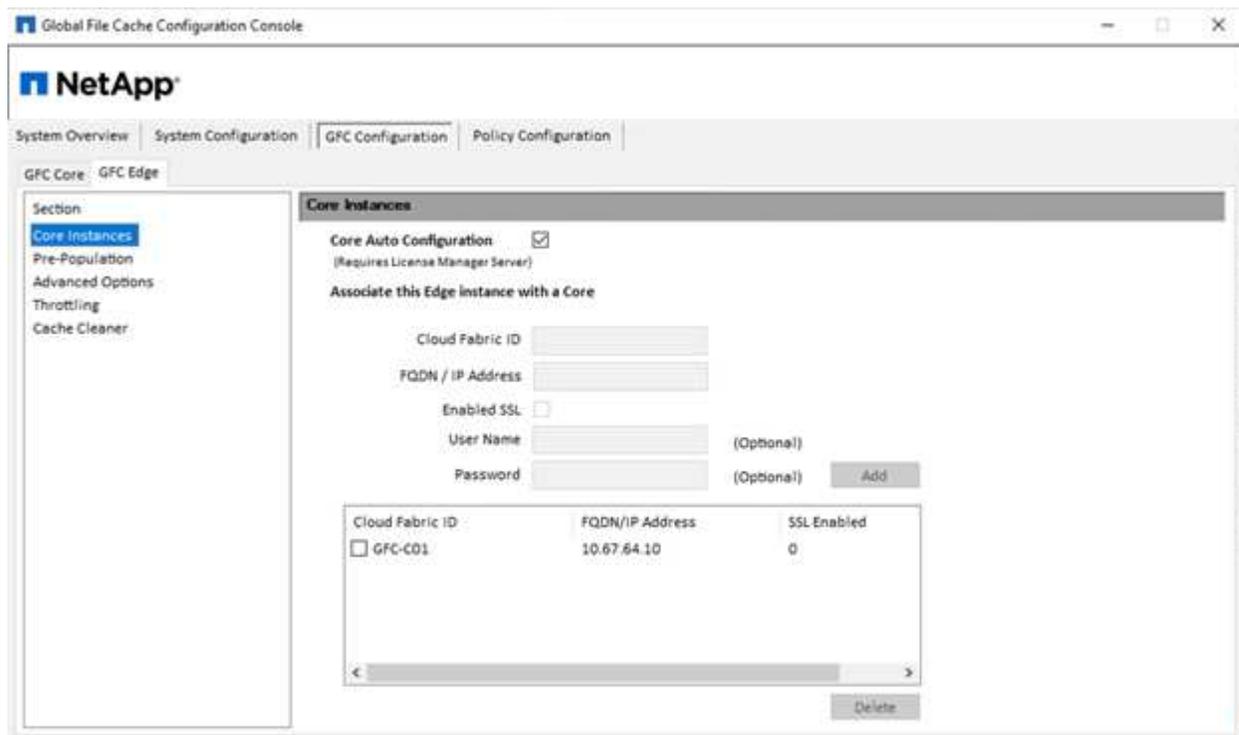
3. Aggiungere un nuovo file server back-end e fornire il nome del file server o l'IP.



4. Sul bordo, l'unità cache deve avere la lettera D. In caso contrario, utilizzare diskpart.exe per selezionare il volume e modificare la lettera dell'unità. Effettuare la registrazione con il server di licenza come edge.

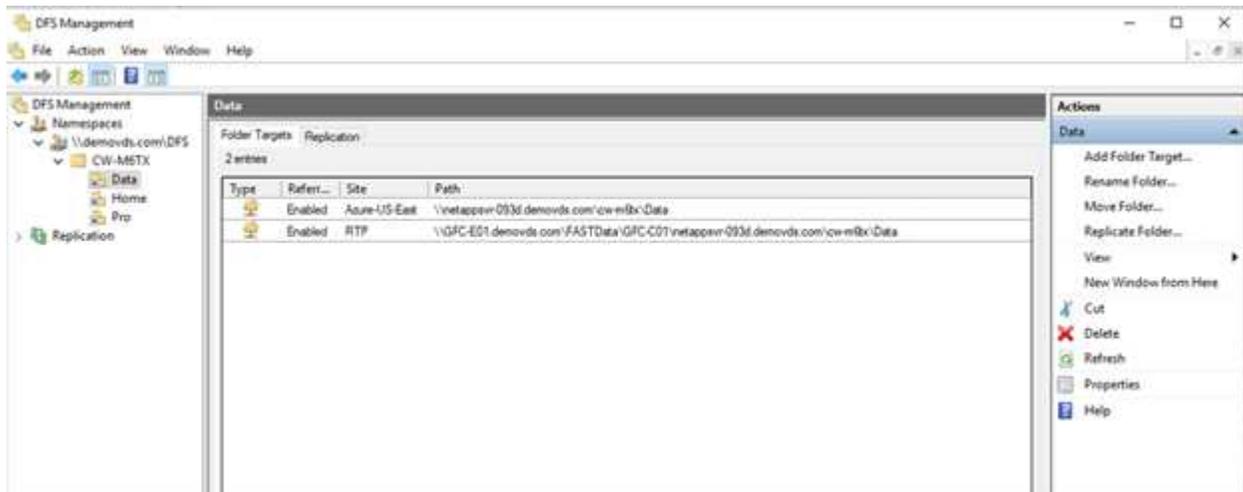


Se la configurazione automatica principale è attivata, le informazioni principali vengono recuperate automaticamente dal server di gestione delle licenze.

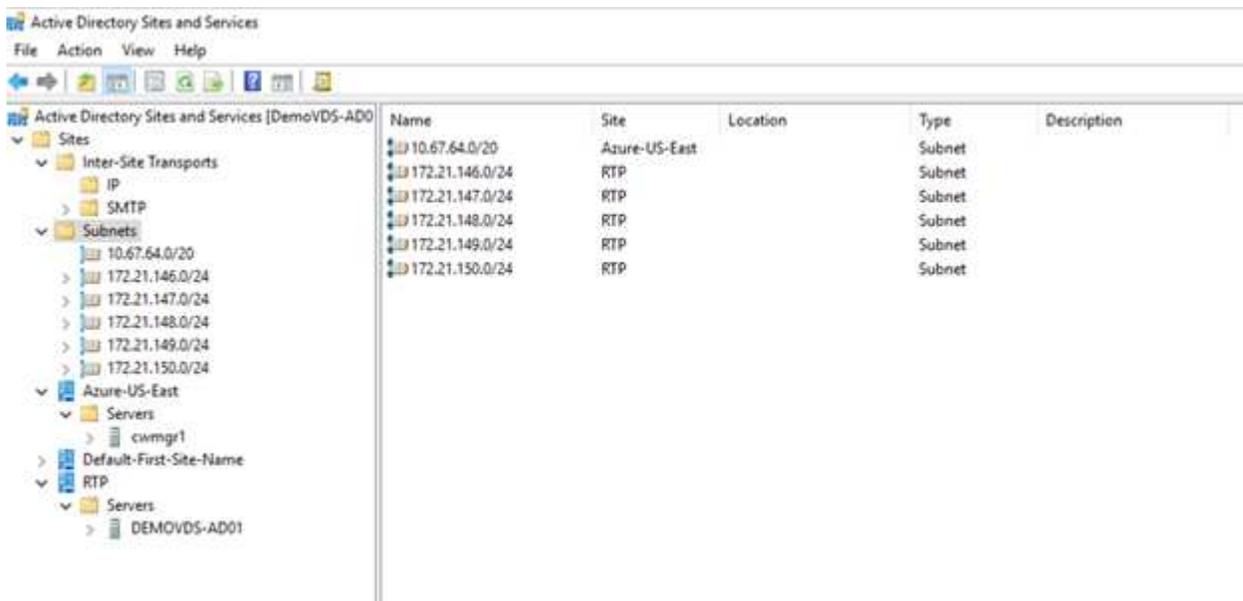


Da qualsiasi computer client, gli amministratori che hanno utilizzato per accedere alla condivisione sul file server possono accedervi con GFC edge utilizzando UNC Path `\\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>`. Gli amministratori possono includere questo percorso nello script di accesso utente o nell'oggetto Criteri di gruppo per la mappatura dei dischi degli utenti nella posizione edge.

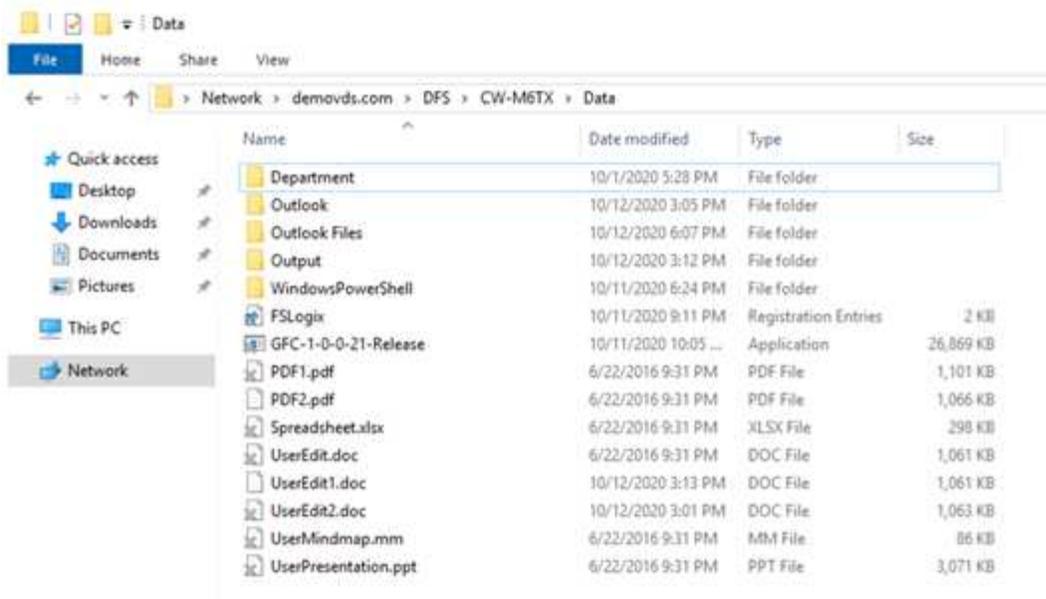
Per fornire un accesso trasparente agli utenti di tutto il mondo, un amministratore può configurare il Microsoft Distributed Filesystem (DFS) con collegamenti che puntano alle condivisioni del file server e alle ubicazioni edge.



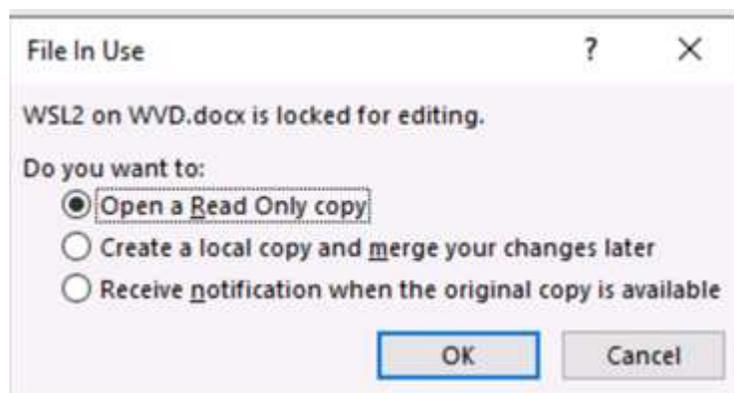
Quando gli utenti accedono con credenziali Active Directory in base alle subnet associate al sito, il client DFS utilizza il collegamento appropriato per accedere ai dati.



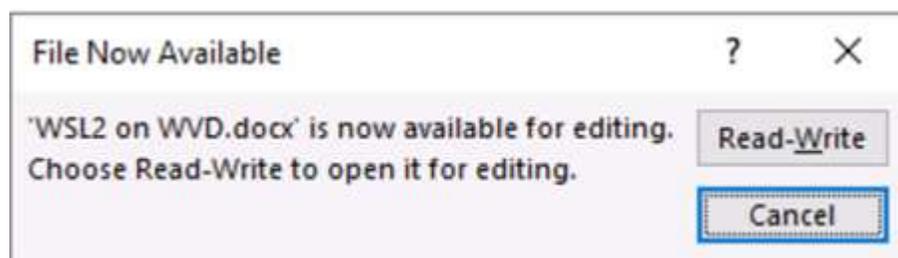
Le icone dei file cambiano a seconda che un file venga memorizzato nella cache; i file non memorizzati nella cache hanno una X grigia nell'angolo inferiore sinistro dell'icona. Dopo che un utente in una posizione edge accede a un file, tale file viene memorizzato nella cache e l'icona cambia.



Quando un file è aperto e un altro utente sta tentando di aprire lo stesso file da una posizione edge, all'utente viene richiesto di selezionare la seguente opzione:



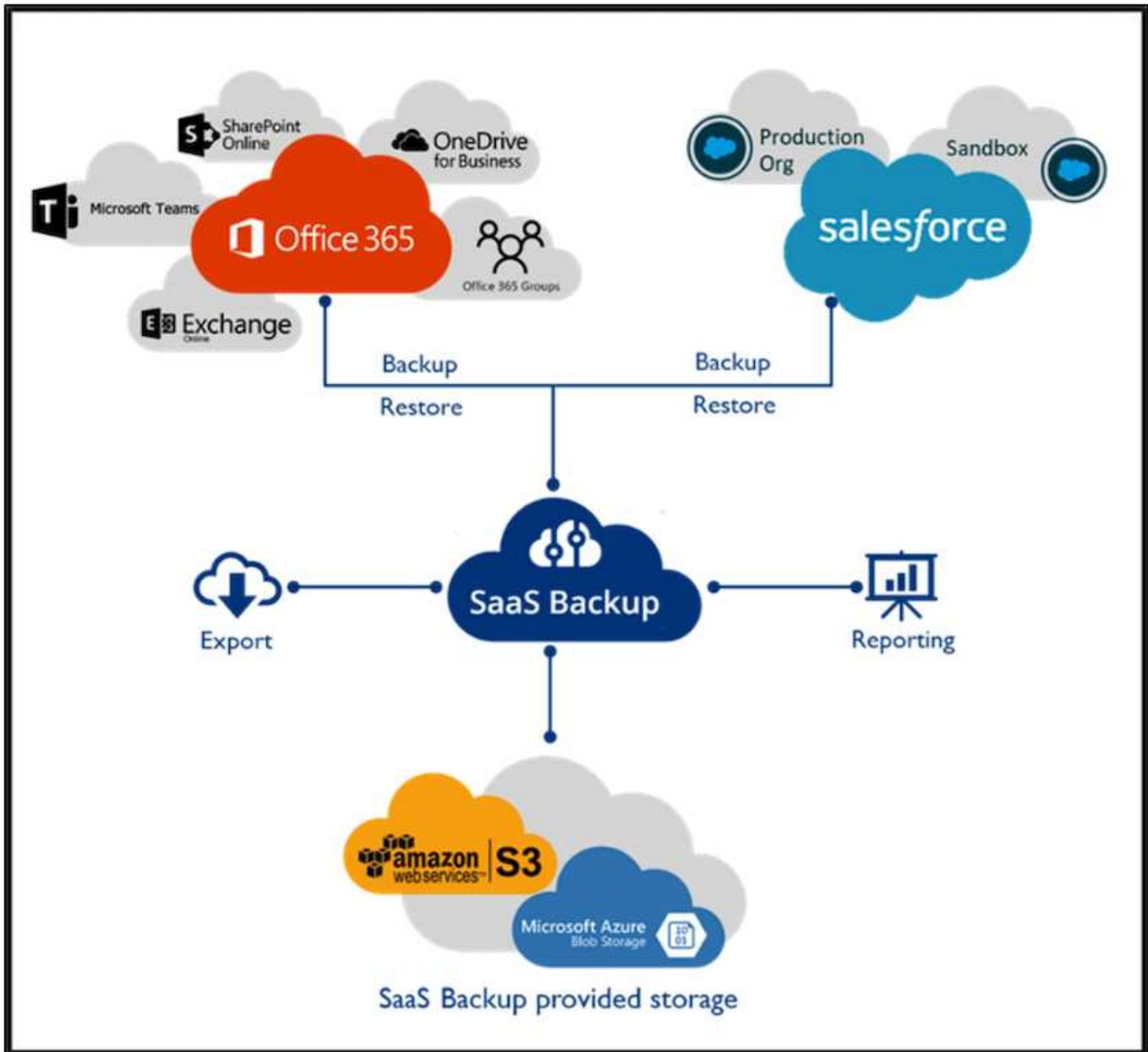
Se l'utente seleziona l'opzione per ricevere una notifica quando la copia originale è disponibile, l'utente riceve una notifica come segue:



Per ulteriori informazioni, consulta questa sezione ["Video sull'implementazione di Talon e Azure NetApp Files"](#).

## Backup SaaS

NetApp VDS offre protezione dei dati per Salesforce e Microsoft Office 365, inclusi Exchange, SharePoint e Microsoft OneDrive. La figura seguente mostra come NetApp VDS fornisce SaaS Backup per questi servizi dati.



Per una dimostrazione della protezione dei dati di Microsoft Office 365, vedere ["questo video"](#).

Per una dimostrazione della protezione dei dati di Salesforce, consulta ["questo video"](#).

#### Gestione delle operazioni

Con NetApp VDS, gli amministratori possono delegare le attività ad altri. Possono connettersi ai server implementati per risolvere i problemi, visualizzare i log ed eseguire i report di audit. Mentre assistono i clienti, l'helpdesk o i tecnici di livello 3 possono affiancare le sessioni degli utenti, visualizzare gli elenchi dei processi e, se necessario, eliminare i processi.

Per informazioni sui file di log VDS, consultare ["Risoluzione dei problemi della pagina azioni VDA non riuscite"](#).

Per ulteriori informazioni sulle autorizzazioni minime richieste, vedere ["Pagina componenti e autorizzazioni VDA"](#).

Se si desidera clonare manualmente un server, vedere ["Pagina cloning Virtual Machines"](#).

Per aumentare automaticamente le dimensioni del disco della macchina virtuale, consultare ["Pagina delle funzionalità di aumento automatico dello spazio su disco"](#).

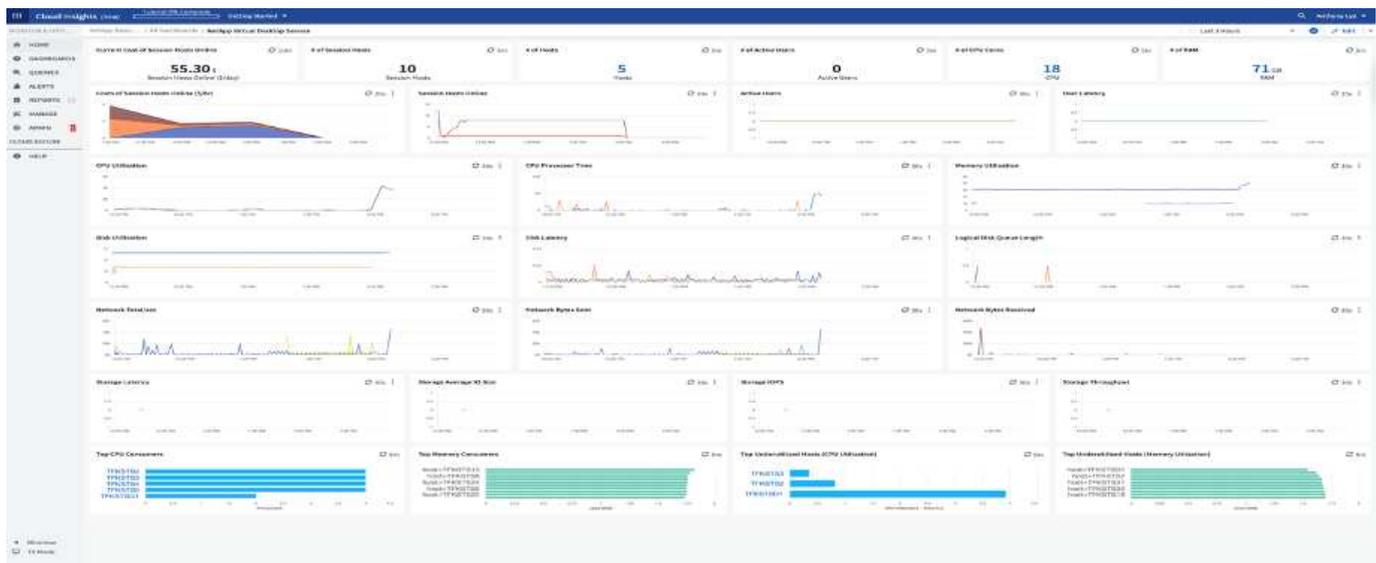
Per identificare l'indirizzo del gateway per la configurazione manuale del client, consultare ["Pagina dei requisiti per l'utente finale"](#).

## Cloud Insights

NetApp Cloud Insights è uno strumento di monitoraggio basato su web che offre una visibilità completa dell'infrastruttura e delle applicazioni eseguite su NetApp e su altri componenti dell'infrastruttura di terze parti. Cloud Insights supporta cloud privati e pubblici per il monitoraggio, la risoluzione dei problemi e l'ottimizzazione delle risorse.

Solo la macchina virtuale dell'unità di acquisizione (può essere Windows o Linux) deve essere installata su un cloud privato per raccogliere le metriche dai data colleer senza la necessità di agenti. I data raccoglitori basati su agenti consentono di ottenere metriche personalizzate da Windows Performance Monitor o da qualsiasi agente di input supportato da Telegraf.

La figura seguente mostra la dashboard di Cloud Insights VDS.



Per ulteriori informazioni su NetApp Cloud Insights, vedere ["questo video"](#).

## Strumenti e registri

### Tool DCCconfig

Lo strumento DCCconfig supporta le seguenti opzioni di hypervisor per l'aggiunta di un sito:

DataCenter Site

DataCenter Site

Hypervisor

Cancel New Save

Load Hypervisor Test

Select Hypervisor

- Aws
- AzureClassic
- AzureRM
- ComputeEngine
- HyperV
- ProfitBricks
- vCloud
- vCloudRest
- vSphere
- XenServer

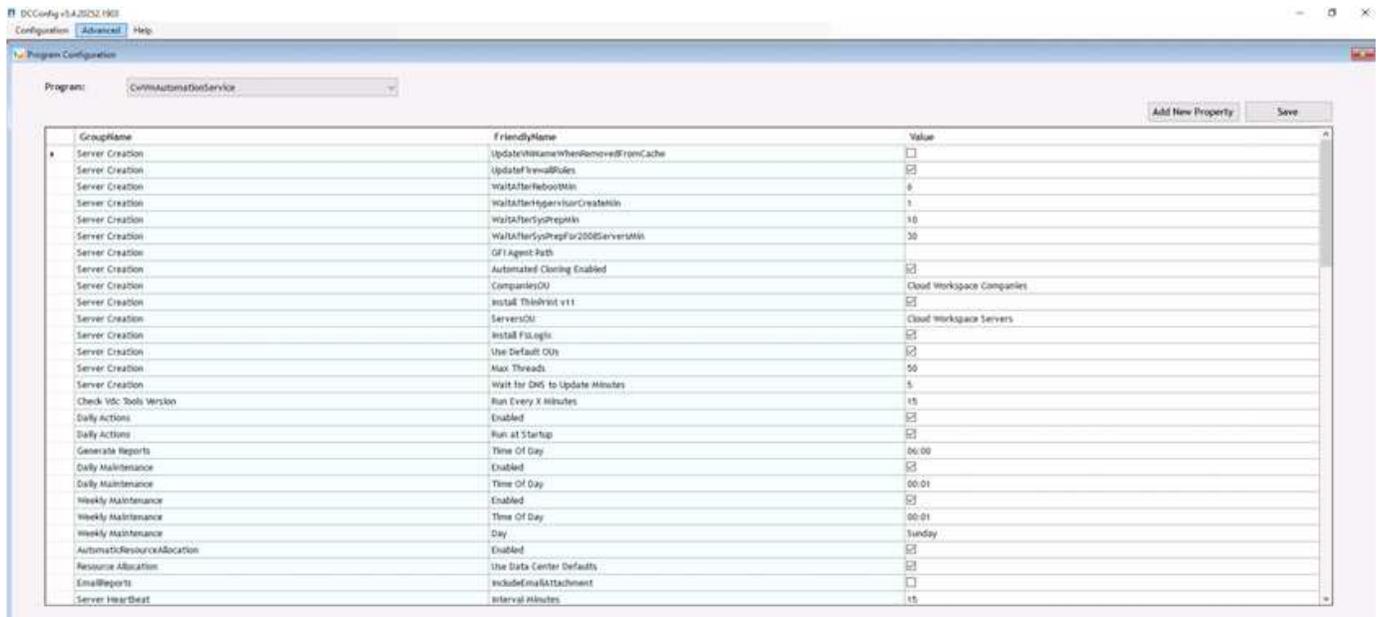
Configuration

DataCenter Accounts Email DatabaseConnection Exclude DataCenter Sites Product Keys Static IpAddress Drive Mapping

Save

	Description	DriveLetter
	Shared Data	P
	FTP	F
▶	User Home	H

È possibile gestire la mappatura delle lettere di unità specifiche dell'area di lavoro per i dati condivisi utilizzando l'oggetto Criteri di gruppo. Professional Services o il team di supporto possono utilizzare la scheda Advanced per personalizzare impostazioni come i nomi delle unità organizzative di Active Directory, l'opzione per attivare o disattivare la distribuzione di FSLogix, vari valori di timeout e così via.

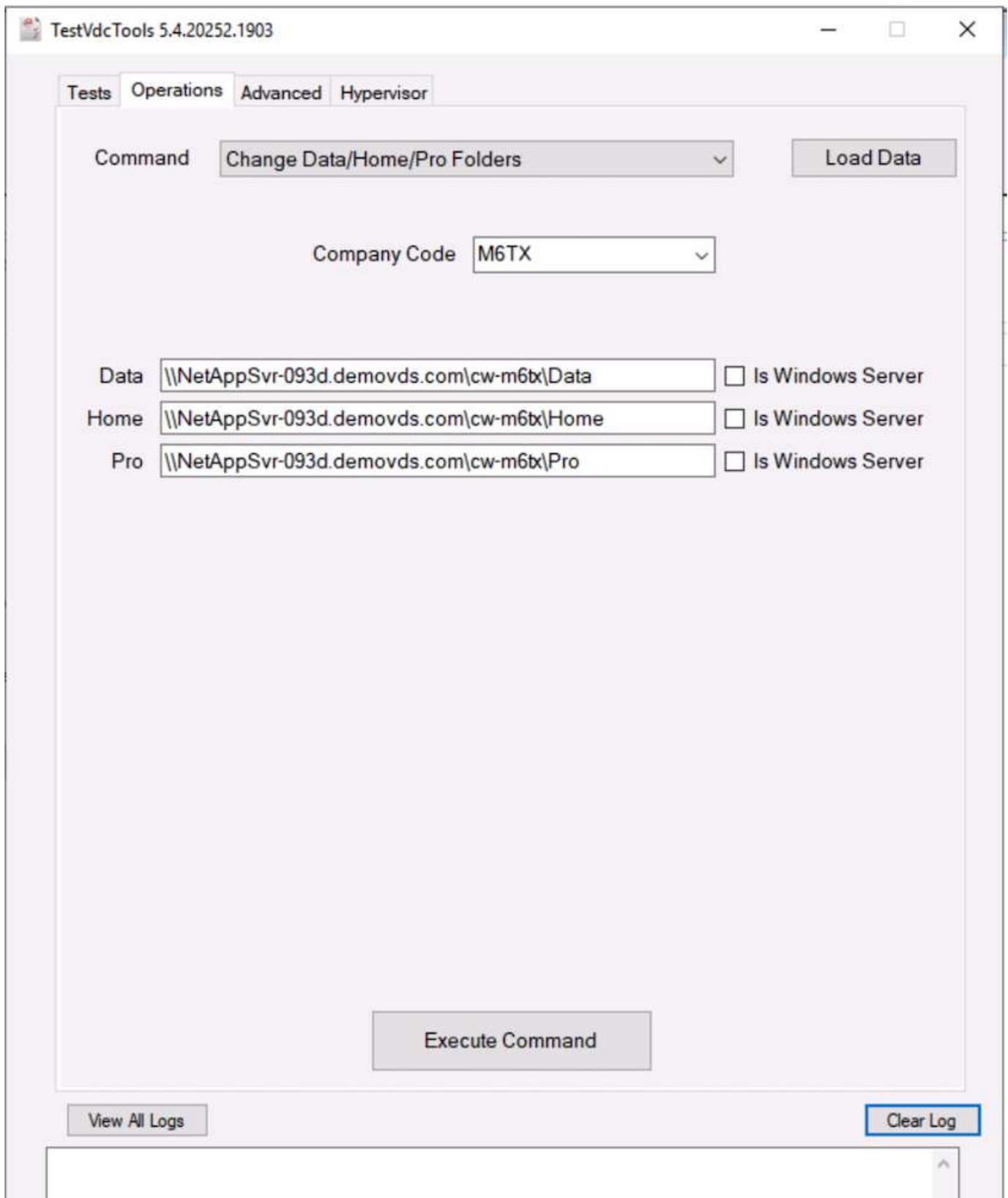


## Command Center (precedentemente noto come TestVdc Tools)

Per avviare Command Center e il ruolo richiesto, vedere ["Panoramica del Command Center"](#).

È possibile eseguire le seguenti operazioni:

- Modificare il percorso SMB per un'area di lavoro.



- Modificare il sito per la raccolta di provisioning.

Tests Operations **Advanced** Hypervisor

Command Edit Provisioning Collection ▾

Load Data

Provisioning Collection **Windows2019** ▾

Description On vSphere Site 2

Share Drive P ▾

Minimum Cache Level 1 ▾

Operating System Windows Server 2019 ▾

Collection Type Shared ▾

	Data Center Site	Role	Template	Storage
▶	Site 2 ▾	TSDData ▾	Windows2019 ▾	DS01
*	▾	▾	▾	▾

Execute Command

View All Logs

Clear Log

File di log

Name	Date modified	Type	Size
 CwAgent	9/19/2020 12:35 PM	File folder	
 CWAutomationService	9/19/2020 12:34 PM	File folder	
 CWManagerX	9/19/2020 12:53 PM	File folder	
 CwVmAutomationService	9/19/2020 12:34 PM	File folder	
 TestVdcTools	9/22/2020 8:20 PM	File folder	
 report	9/19/2020 12:18 PM	Executable Jar File	705 KB

Controllare "[log di automazione](#)" per ulteriori informazioni.

### Considerazioni sulla GPU

Le GPU vengono generalmente utilizzate per la visualizzazione grafica (rendering) eseguendo calcoli aritmetici ripetitivi. Questa funzionalità di calcolo ripetitivo viene spesso utilizzata per i casi di utilizzo di ai e deep learning.

Per le applicazioni ad uso intensivo di grafica, Microsoft Azure offre la serie NV basata sulla scheda NVIDIA Tesla M60 con una o quattro GPU per macchina virtuale. Ogni scheda NVIDIA Tesla M60 include due GPU basate su Maxwell, ciascuna con 8 GB di memoria GDDR5 per un totale di 16 GB.



La serie NV include una licenza NVIDIA.

TechPowerUp GPU-Z 2.36.0

Graphics Card | Sensors | Advanced | Validation

Name: NVIDIA Tesla M60 [Lookup](#)

GPU: GM204 Revision: FF

Technology: 28 nm Die Size: 398 mm<sup>2</sup>

Release Date: Aug 30, 2015 Transistors: 5200M

BIOS Version: 84.04.85.00.03  UEFI

Subvendor: NVIDIA Device ID: 10DE 13F2 - 10DE 115E

ROPs/TMUs: 64 / 128 Bus Interface: PCI ?

Shaders: 2048 Unified DirectX Support: 12 (12\_1)

Pixel Fillrate: 75.4 GPixel/s Texture Fillrate: 150.8 GTexel/s

Memory Type: GDDR5 (Hynix) Bus Width: 256 bit

Memory Size: 8192 MB Bandwidth: 160.4 GB/s

Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date: Oct 22, 2020 Digital Signature: WHQL

GPU Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

Default Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

NVIDIA SLI: Disabled

Computing  OpenCL  CUDA  DirectCompute  DirectML

Technologies  Vulkan  Ray Tracing  PhysX  OpenGL 4.6

NVIDIA Tesla M60 [Close](#)

Con NetApp HCI, la GPU H615C contiene tre schede NVIDIA Tesla T4. Ogni scheda NVIDIA Tesla T4 dispone di una GPU basata su Turing con 16 GB di memoria GDDR6. Se utilizzate in un ambiente VMware vSphere, le macchine virtuali sono in grado di condividere la GPU, con ogni macchina virtuale dotata di una memoria frame buffer dedicata. Il ray tracing è disponibile con le GPU sul NetApp HCI H615C per produrre immagini realistiche, inclusi i riflessi della luce. Tenere presente che è necessario disporre di un server di licenza NVIDIA

con una licenza per le funzioni GPU.

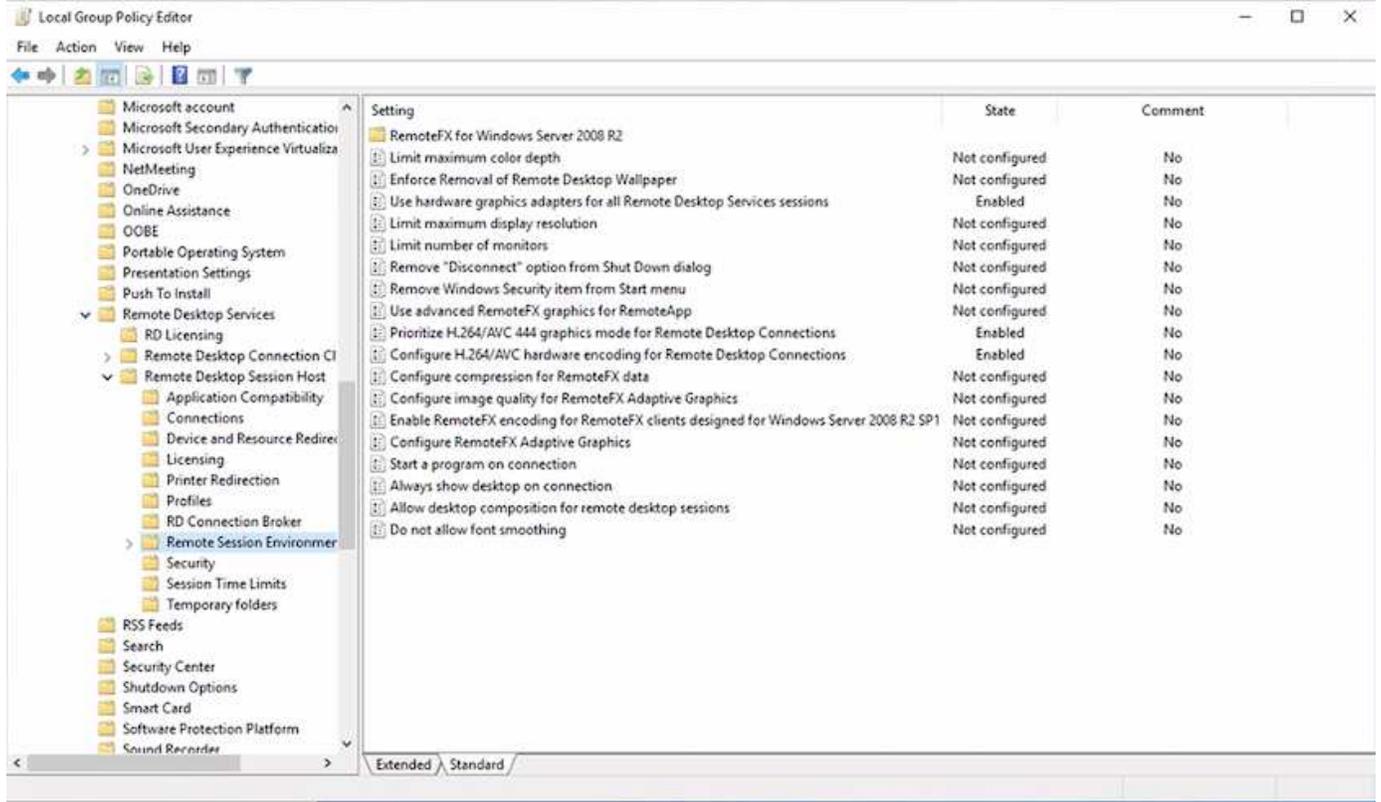
The screenshot shows the TechPowerUp GPU-Z 2.36.0 application window. The main content area displays the following information for the NVIDIA GRID T4-8Q GPU:

- Name:** NVIDIA GRID T4-8Q
- GPU:** TU104, **Revision:** A1
- Technology:** 12 nm, **Die Size:** 545 mm<sup>2</sup>
- Release Date:** Sep 13, 2018, **Transistors:** 13600M
- BIOS Version:** 0.00.00.00.00
- Subvendor:** NVIDIA, **Device ID:** 10DE 1EB8 - 10DE 130F
- ROPs/TMUs:** 8 / 160, **Bus Interface:** PCI
- Shaders:** 2560 Unified, **DirectX Support:** 12 (12\_2)
- Pixel Fillrate:** 4.7 GPixel/s, **Texture Fillrate:** 93.6 GTexel/s
- Memory Type:** GDDR6, **Bus Width:** 256 bit
- Memory Size:** 8192 MB, **Bandwidth:** Unknown
- Driver Version:** 27.21.14.5257 (NVIDIA 452.57) / 2016
- Driver Date:** Oct 22, 2020, **Digital Signature:** WHQL
- GPU Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- Default Clock:** 585 MHz, **Memory:** 0 MHz, **Shader:** N/A
- NVIDIA SLI:** Disabled
- Computing Technologies:**  OpenCL,  CUDA,  DirectCompute,  DirectML
- Technologies:**  Vulkan,  Ray Tracing,  PhysX,  OpenGL 4.6

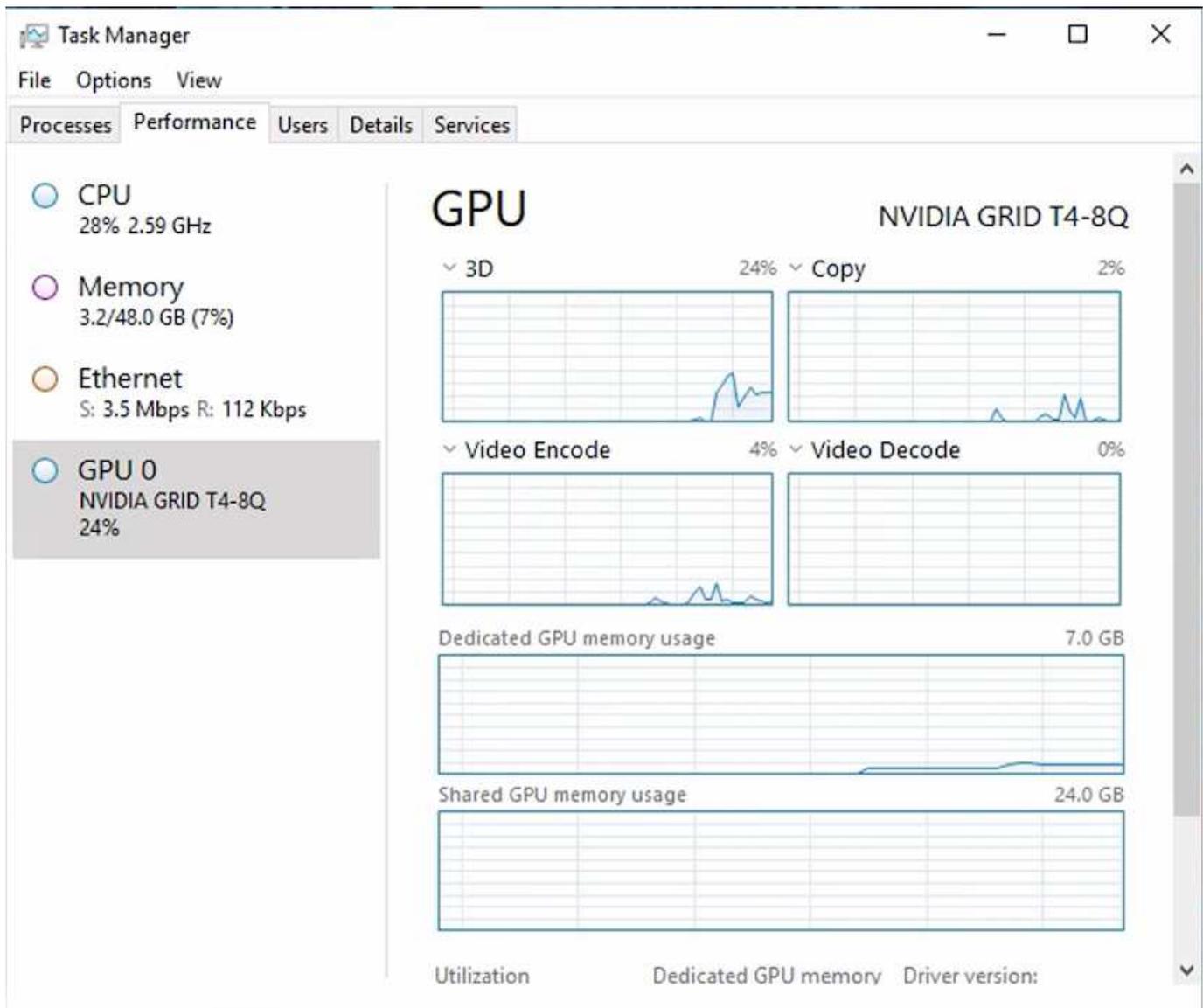
The application window includes a 'Look up' button, an NVIDIA logo, and a 'Close' button at the bottom right. The GPU name 'NVIDIA GRID T4-8Q' is also displayed in a dropdown menu at the bottom left.

Per utilizzare la GPU, è necessario installare il driver appropriato, che può essere scaricato dal portale di licenza NVIDIA. In un ambiente Azure, il driver NVIDIA è disponibile come estensione del driver GPU. Quindi, i criteri di gruppo nella seguente schermata devono essere aggiornati per utilizzare l'hardware GPU per le

sessioni di servizio di desktop remoto. È necessario assegnare la priorità alla modalità grafica H.264 e attivare la funzionalità del codificatore.



Convalidare il monitoraggio delle performance della GPU con Task Manager o utilizzando nvidia-smi CLI quando si eseguono esempi WebGL. Assicurarsi che le risorse della GPU, della memoria e dell'encoder siano in uso.



Per assicurarsi che la macchina virtuale venga implementata in NetApp HCI H615C con servizio di desktop virtuale, definire un sito con la risorsa di cluster vCenter che dispone di host H615C. Il modello di macchina virtuale deve avere il profilo vGPU richiesto allegato.

Per gli ambienti multi-sessione condivisi, considerare l'allocazione di più profili vGPU omogenei. Tuttavia, per le applicazioni grafiche professionali di fascia alta, è meglio avere ogni macchina virtuale dedicata a un utente per mantenere le macchine virtuali isolate.

Il processore GPU può essere controllato da una policy QoS e ciascun profilo vGPU può avere frame buffer dedicati. Tuttavia, l'encoder e il decoder sono condivisi per ogni scheda. Il posizionamento di un profilo vGPU su una scheda GPU è controllato dalla policy di assegnazione della GPU host di vSphere, che può enfatizzare le performance (macchine virtuali distribuite) o il consolidamento (macchine virtuali di gruppo).

#### Soluzioni per il settore

Le workstation grafiche sono generalmente utilizzate in settori come produzione, sanità, energia, media e intrattenimento, istruzione, e così via. La mobilità è spesso limitata per le applicazioni a uso intensivo di grafica.

Per risolvere il problema della mobilità, i servizi di desktop virtuale offrono un ambiente desktop per tutti i tipi di lavoratori, dai task worker agli utenti esperti, utilizzando risorse hardware nel cloud o con NetApp HCI, incluse le opzioni per configurazioni flessibili della GPU. VDS consente agli utenti di accedere al proprio ambiente di lavoro da qualsiasi luogo con laptop, tablet e altri dispositivi mobili.

Per eseguire carichi di lavoro di produzione con software come ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX e così via, Le GPU disponibili su diversi cloud (a gennaio 2021) sono elencate nella seguente tabella.

Modello GPU	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	On-premise (NetApp HCI)
NVIDIA M60	Sì	Sì	Sì	No
NVIDIA T4	No	Sì	Sì	Sì
NVIDIA P100	No	Sì	No	No
NVIDIA P4	No	Sì	No	No

Sono inoltre disponibili sessioni desktop condivise con altri utenti e desktop personali dedicati. I desktop virtuali possono avere da una a quattro GPU o utilizzare GPU parziali con NetApp HCI. NVIDIA T4 è una scheda GPU versatile in grado di soddisfare le esigenze di un'ampia gamma di carichi di lavoro degli utenti. Ogni scheda GPU su NetApp HCI H615C dispone di 16 GB di memoria frame buffer e tre schede per server. Il numero di utenti che possono essere ospitati su un singolo server H615C dipende dal carico di lavoro dell'utente.

Utenti/Server	Leggero (4 GB)	Media (8 GB)	Pesante (16 GB)
H615C	12	6	3

Per determinare il tipo di utente, eseguire il profiler GPU mentre gli utenti lavorano con le applicazioni che eseguono attività tipiche. Il profiler GPU acquisisce le richieste di memoria, il numero di display e la risoluzione richiesta dagli utenti. È quindi possibile scegliere il profilo vGPU che soddisfa i requisiti.

I desktop virtuali con GPU possono supportare una risoluzione dello schermo fino a 8K, mentre l'utility nView può suddividere un singolo monitor in regioni per lavorare con diversi set di dati.

Con lo storage di file ONTAP, puoi ottenere i seguenti vantaggi:

- Un singolo namespace in grado di crescere fino a 20 PB di storage con 400 miliardi di file, senza molti input amministrativi
- Uno spazio dei nomi che può estendersi a livello globale con una Global file cache
- Multi-tenancy sicura con lo storage NetApp gestito
- Migrazione dei dati cold in archivi di oggetti utilizzando NetApp FabricPool
- Statistiche rapide sui file con analisi del file system
- Scalabilità di un cluster di storage fino a 24 nodi per aumentare capacità e performance
- Possibilità di controllare lo spazio di storage utilizzando quote e performance garantite con limiti di QoS
- Protezione dei dati con crittografia
- Soddisfare i più ampi requisiti di protezione e conformità dei dati
- Offrire opzioni flessibili di business continuity

## Conclusione

NetApp Virtual Desktop Service offre un ambiente di applicazioni e desktop virtuali di facile utilizzo, con un'attenzione particolare alle sfide aziendali. Estendendo i VDS con l'ambiente ONTAP on-premise, è possibile utilizzare le potenti funzionalità NetApp in un ambiente VDS, tra cui cloni rapidi, deduplica in-line, compaction, thin provisioning, e compressione. Queste funzionalità consentono di risparmiare sui costi di storage e migliorare le performance con lo storage all-flash. Con l'hypervisor VMware vSphere, che riduce al minimo i tempi di provisioning dei server utilizzando Virtual Volumes e vSphere API per l'integrazione degli array. Utilizzando il cloud ibrido, i clienti possono scegliere l'ambiente giusto per i carichi di lavoro esigenti e risparmiare denaro. La sessione desktop in esecuzione on-premise può accedere alle risorse cloud in base alle policy.

## Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- ["Cloud di NetApp"](#)
- ["Documentazione sui prodotti NetApp VDS"](#)
- ["Connetti la tua rete on-premise ad Azure con VPN Gateway"](#)
- ["Portale Azure"](#)
- ["Desktop virtuale Microsoft Windows"](#)
- ["Registrazione Azure NetApp Files"](#)

## VMware Horizon

### **NVA-1132-DESIGN: VMware end-user computing con NetApp HCI**

Suresh Thoppay, NetApp

VMware End-User Computing con NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive la progettazione architeturale e le Best practice per l'implementazione della soluzione su scala di produzione in modo affidabile e privo di rischi.

["NVA-1132-DESIGN: VMware end-user computing con NetApp HCI"](#)

### **NVA-1129-DESIGN: Calcolo per l'utente finale VMware con GPU NetApp HCI e NVIDIA**

Suresh Thoppay, NetApp

VMware End-User Computing con NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive la progettazione architeturale e le Best practice per l'implementazione della soluzione su scala di produzione in modo affidabile e privo di

rischi.

["NVA-1129-DESIGN: Calcolo per l'utente finale VMware con GPU NetApp HCI e NVIDIA"](#)

## **NVA-1129-DEPLOY: VMware end-user computing con GPU NetApp HCI e NVIDIA**

Suresh Thoppay, NetApp

VMware End-User Computing with NetApp HCI è un'architettura di data center pre-validata e Best-practice per l'implementazione di workload di desktop virtuali su scala aziendale. Questo documento descrive come implementare la soluzione su scala di produzione in modo affidabile e privo di rischi

["NVA-1129-DEPLOY: VMware end-user computing con GPU NetApp HCI e NVIDIA"](#)

## **NetApp HCI per l'infrastruttura di desktop virtuale con VMware Horizon 7: Potenzia i tuoi utenti più esperti con la grafica 3D**

Suresh Thoppay, NetApp

TR-4792 fornisce indicazioni sull'utilizzo del nodo di calcolo NetApp H615C per carichi di lavoro di grafica 3D in un ambiente VMware Horizon con unità di elaborazione grafica NVIDIA (GPU) e software di virtualizzazione. Fornisce inoltre i risultati dei test preliminari di SPECviewperf 13 per H615C.

["NetApp HCI per l'infrastruttura di desktop virtuale con VMware Horizon 7: Potenzia i tuoi utenti più esperti con la grafica 3D"](#)

## **Soluzioni di virtualizzazione desktop FlexPod**

Per ulteriori informazioni sulle soluzioni di virtualizzazione FlexPod, consulta la ["Guida alla progettazione di FlexPod"](#)

# **Array SAN all-flash NetApp con VMware vSphere 8**

Autore: Josh Powell - NetApp Solutions Engineering

## **Panoramica della soluzione**

### **Introduzione**

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

## Scopo del presente documento

In questo documento tratteremo il valore esclusivo dell'utilizzo dei sistemi storage NetApp ASA con VMware vSphere e forniremo una panoramica della tecnologia dell'array SAN all-flash NetApp. Inoltre, esamineremo strumenti aggiuntivi per semplificare il provisioning dello storage, la protezione dei dati e il monitoraggio del data center VMware e ONTAP.

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

## Panoramica sulla tecnologia

Questa soluzione include tecnologie innovative di VMware e NetApp.

### VMware vSphere 8,0

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

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

### Nuovi miglioramenti in vSphere 8,0

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

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

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

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

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

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

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

Per ulteriori informazioni, consultare il blog, ["Novità di vSphere 8"](#).

### Volumi virtuali VMware (vVol)

I vVol sono un nuovo rivoluzionario approccio alla gestione dello storage nei cluster vSphere, che offre una gestione semplificata e un controllo più granulare delle risorse storage. Ciascun disco virtuale di un datastore di vVol è un vVol e diventa un oggetto LUN nativo nel sistema storage. L'integrazione del sistema storage e di vSphere avviene tramite il provider **VMware API per Storage Awareness (VASA)** e consente al sistema

storage di essere consapevole dei dati delle VM e di gestirli di conseguenza. Le policy di storage definite nel client vCenter vengono utilizzate per allocare e gestire le risorse di storage.

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

Per ulteriori informazioni sui vVol, vedere la ["Guida introduttiva di vVol"](#).

## NVMe over Fabrics

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

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

---

## NetApp ONTAP

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

### Funzioni di base di ONTAP

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

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

l'automazione e sfruttando i moduli Ansible per una perfetta gestione della configurazione dei sistemi ONTAP. I moduli Ansible offrono una comoda soluzione per gestire in modo efficiente le configurazioni dei sistemi ONTAP. La combinazione di questi potenti strumenti consente di ottimizzare i flussi di lavoro e migliorare la gestione globale dell'infrastruttura storage.

### Funzionalità di disaster recovery ONTAP

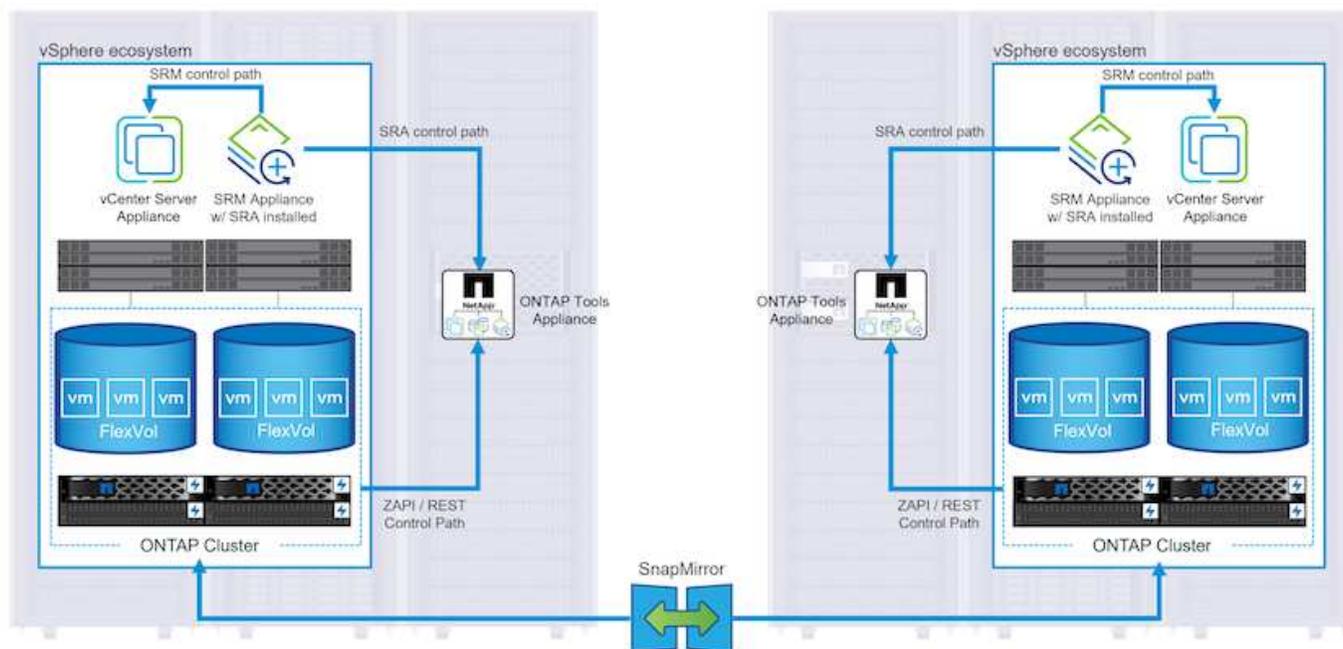
NetApp ONTAP offre solide soluzioni di disaster recovery per gli ambienti VMware. Queste soluzioni sfruttano tecnologie di replica SnapMirror tra sistemi di storage primario e secondario per consentire il failover e il recovery rapido in caso di guasto.

### Scheda di replica archiviazione:

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

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

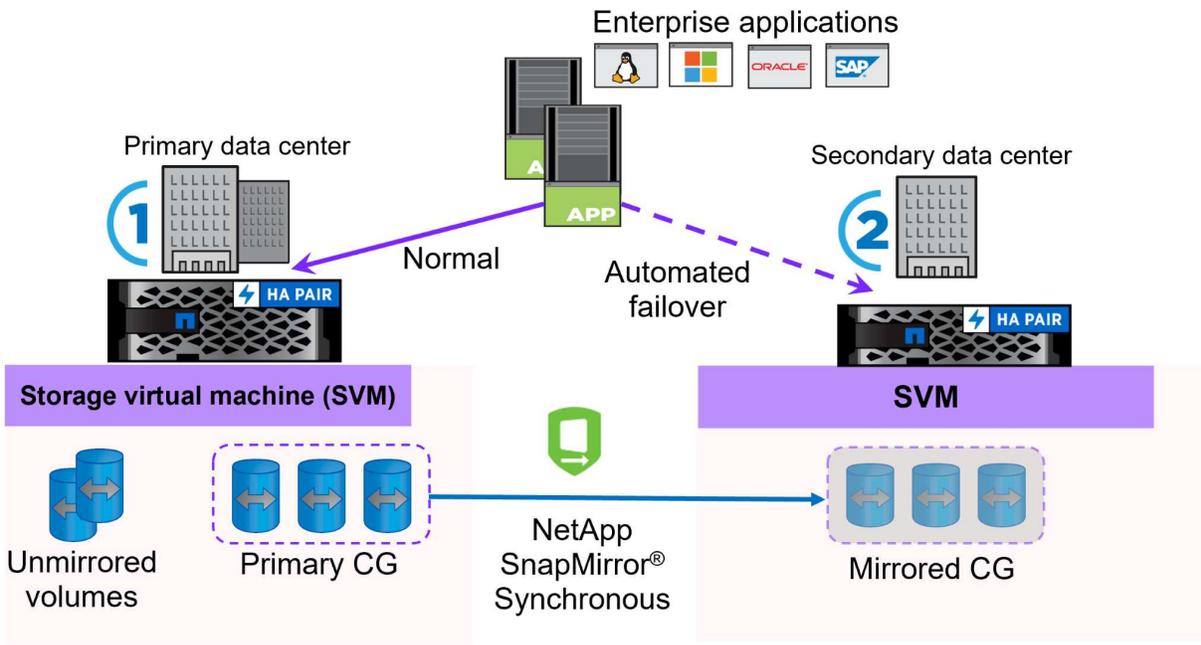
NetApp SRA viene installato come parte degli strumenti ONTAP per VMware vSphere.



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

### Business Continuity SnapMirror:

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



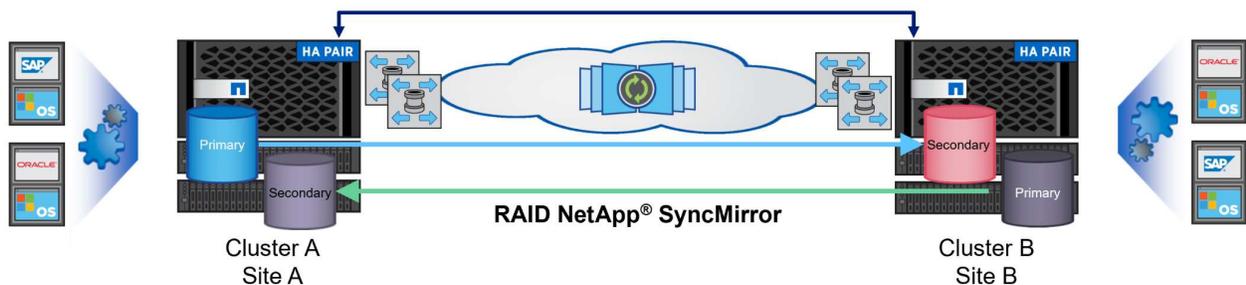
Per ulteriori informazioni, fare riferimento a SnapMirror ["Panoramica sulla continuità del business"](#).

### NetApp MetroCluster:

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

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

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



Per informazioni dettagliate sull'architettura e la configurazione di MetroCluster, consultare la ["Sito di documentazione MetroCluster"](#).

## Modello di licenza ONTAP One

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

La licenza ONTAP ONE include tutte le seguenti funzioni:

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

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

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

**SnapRestore** – consente il ripristino rapido dei dati dalle istantanee.

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

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

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

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

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

---

## Array SAN all-flash NetApp

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

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

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



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



Per informazioni dettagliate, consultare la ["Landing page di NetApp ASA"](#).

#### Caratteristiche di NetApp ASA

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

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

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

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

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

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

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

### Supporto del protocollo

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

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

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

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

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

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

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

### Tecnologia Active-Active

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

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

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

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

## Garanzie di archiviazione

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

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

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

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

Vedere ["Portale dei prodotti NetApp ASA"](#) per ulteriori informazioni.

---

## Plug-in NetApp per VMware vSphere

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

### Strumenti ONTAP per VMware vSphere

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

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

Gli strumenti ONTAP includono i seguenti componenti:

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

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

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

Per ulteriori informazioni sugli strumenti NetApp ONTAP per VMware, vedere ["Strumenti ONTAP per la documentazione VMware vSphere"](#).

### Plug-in SnapCenter per VMware vSphere

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

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

con il client vSphere:

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

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

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

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

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

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

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

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

---

## NetApp Cloud Insights

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

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

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

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

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

## Array SAN all-flash NetApp con VMware vSphere 8

Autore: Josh Powell - NetApp Solutions Engineering

## Gestire lo storage a blocchi con tool ONTAP per VMware vSphere

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

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

Gli strumenti ONTAP includono i seguenti componenti:

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

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

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

Per ulteriori informazioni sugli strumenti NetApp ONTAP per VMware, vedere ["Strumenti ONTAP per la documentazione VMware vSphere"](#).

### Panoramica sull'implementazione della soluzione

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

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

Per informazioni dettagliate sui vVol con ONTAP, fare riferimento a ["vVol di volumi virtuali\) con ONTAP"](#).

Questa soluzione copre i seguenti passaggi di alto livello:

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

### Prerequisiti

In questa soluzione sono stati utilizzati i seguenti componenti:

1. Array SAN all-flash NetApp A400 con ONTAP 9,13.

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

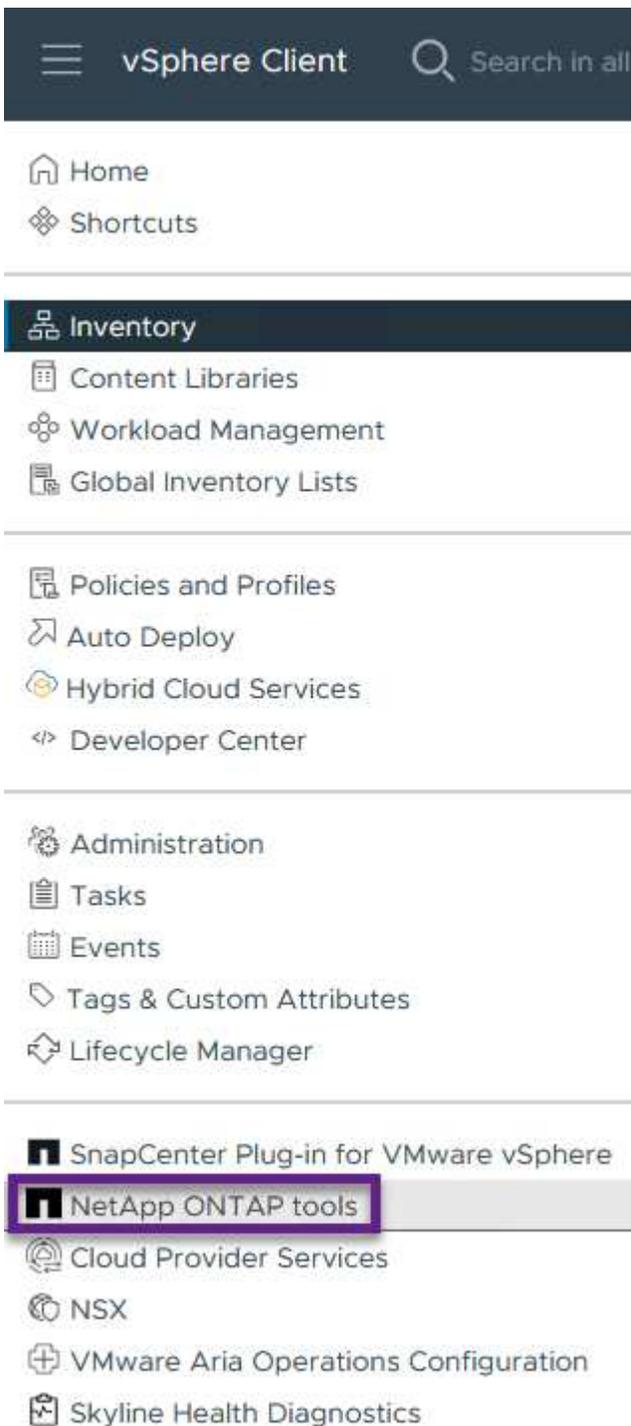
#### **Implementazione della soluzione**

##### **Creare un datastore vVol in ONTAP Tools**

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

## Aggiunta di un sistema di storage ai tool ONTAP.

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



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



NetApp ONTAP tools INSTANCE 10.61.181.154:8443 ▾

Overview

## Storage Systems

Storage Systems

ADD

REDISCOVER ALL

Storage capability profile

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

## Add Storage System



Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.61.181.205 ▾

Name or IP address:

10.192.102.103

Username:

admin

Password:

●●●●●●●●

Port:

443

Advanced options ^

ONTAP Cluster Certificate:



Automatically fetch



Manually upload

CANCEL

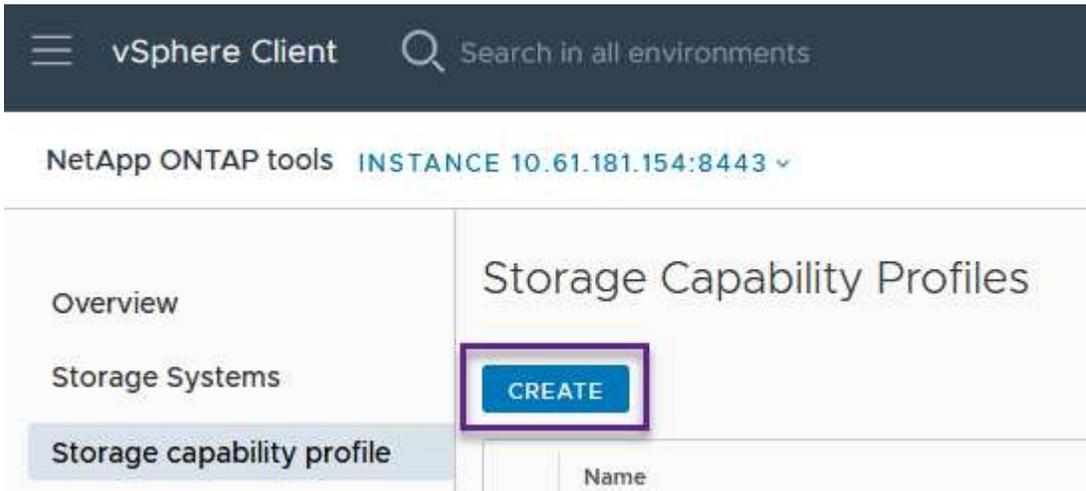
ADD

## Creare un profilo di funzionalità di storage in ONTAP Tools

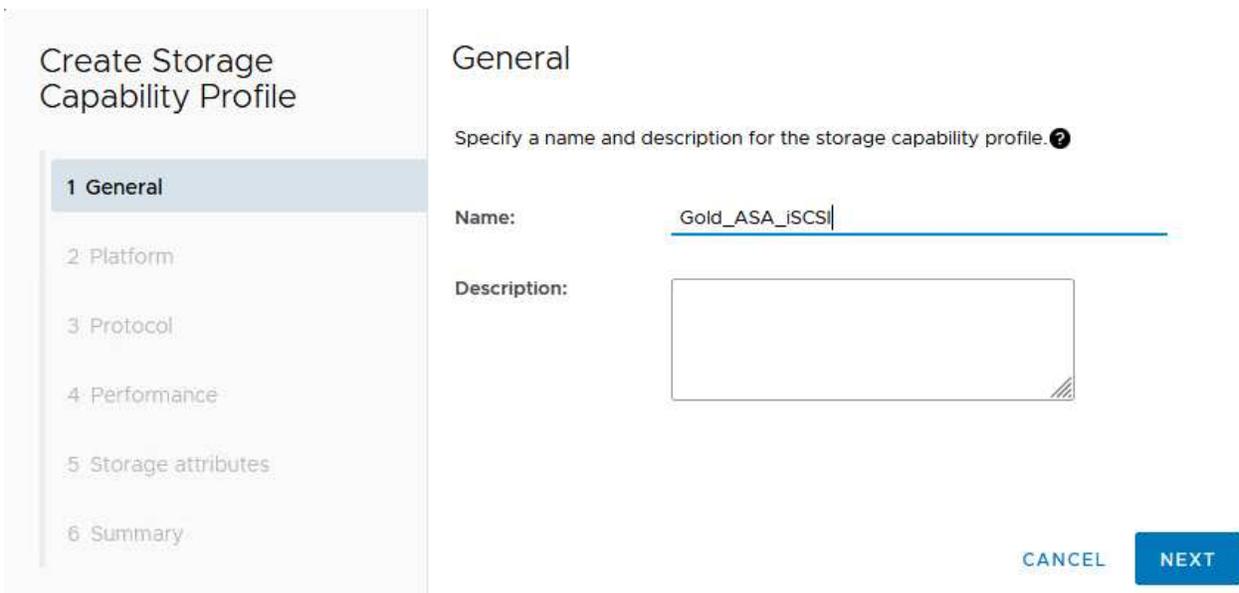
I profili di capacità dello storage descrivono le funzionalità fornite da uno storage array o da un sistema storage. Includono le definizioni della qualità del servizio e vengono utilizzate per selezionare i sistemi storage che soddisfano i parametri definiti nel profilo.

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

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



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



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

## Create Storage Capability Profile

- 1 General
- 2 Platform**
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

### Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

## Summary

Name:	ASA_Gold
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	No
Tiering policy (FabricPool):	None

CANCEL

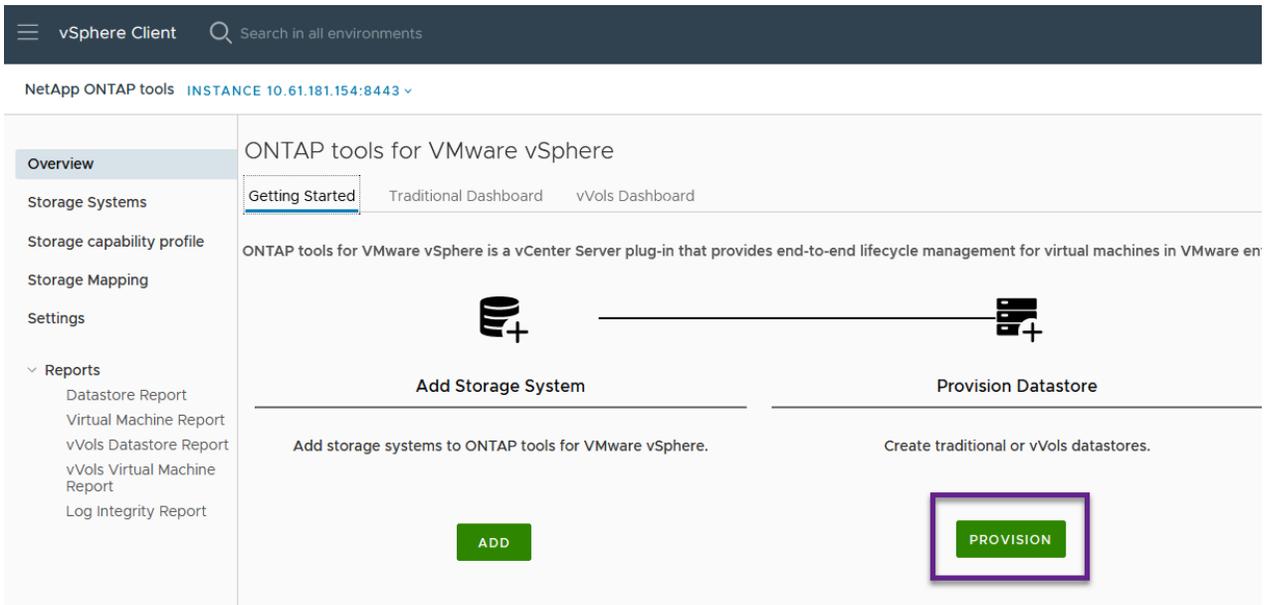
BACK

FINISH

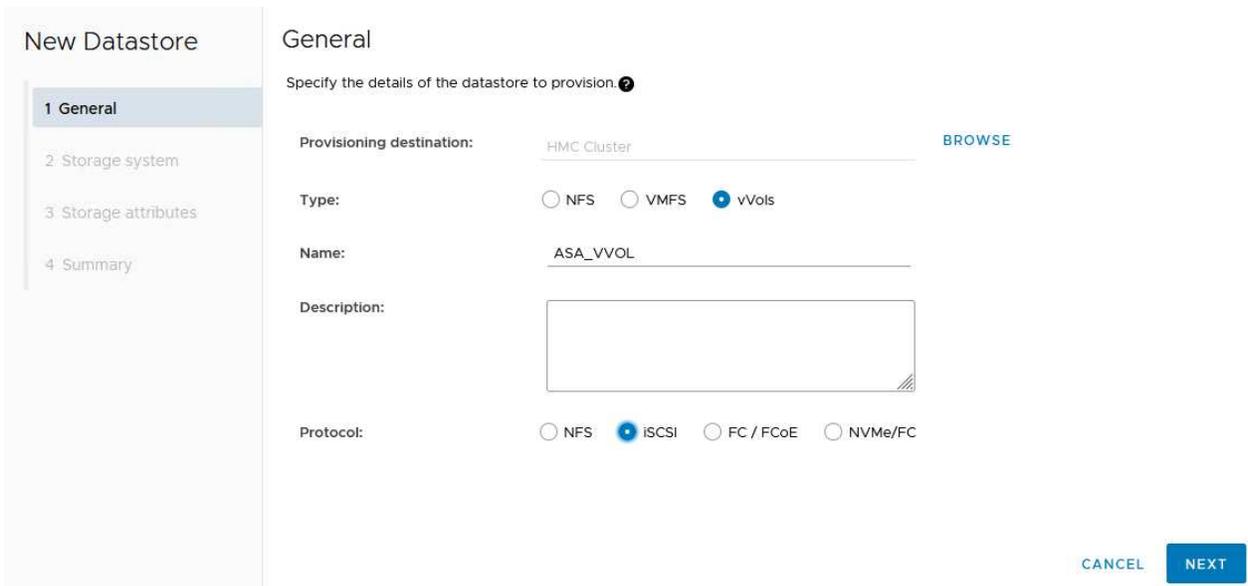
## Creare un datastore vVol in ONTAP Tools

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

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



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



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

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

## Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

FAS\_Default  
FAS\_Max20  
**Custom profiles**  
Gold\_ASA\_JSCSI  
Gold\_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

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

## New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

## Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVMe	Thin

ADD

CANCEL

BACK

NEXT

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

### New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

### Summary

**General**

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA\_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold\_ASA

**Storage system details**

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

**Storage attributes**

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

## Creare una policy di storage delle macchine virtuali nel client vSphere

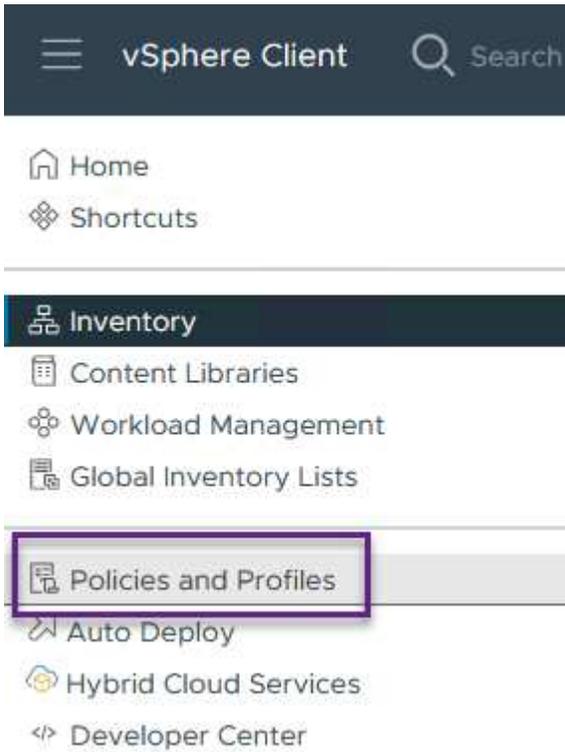
Un criterio di storage delle macchine virtuali è un insieme di regole e requisiti che definiscono le modalità di archiviazione e gestione dei dati delle macchine virtuali. Specifica le caratteristiche di storage desiderate, come performance, disponibilità e servizi dati, per una VM specifica.

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

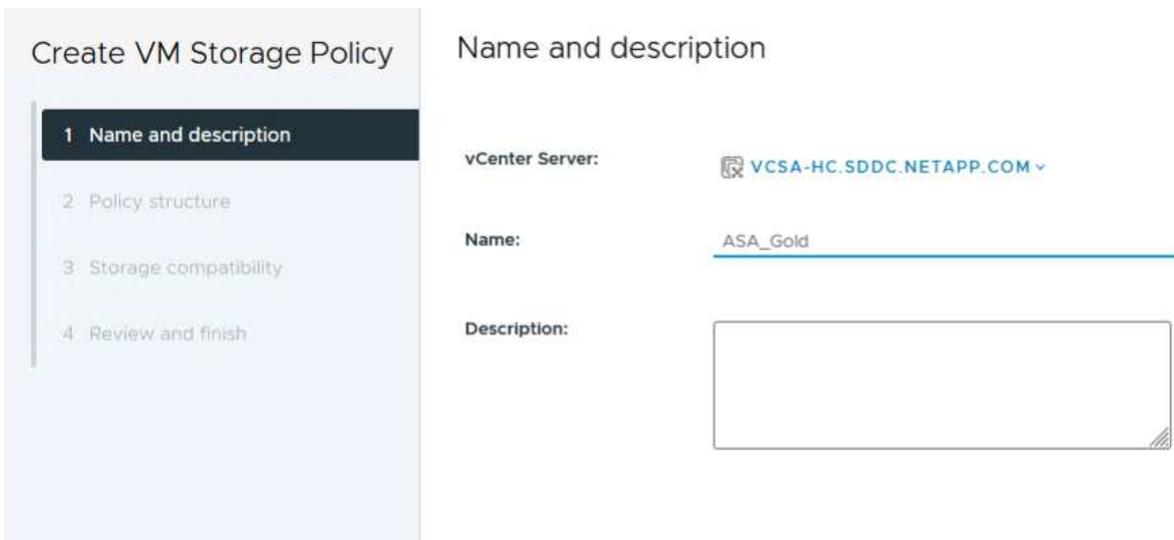
## Crea una policy di storage delle macchine virtuali

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

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



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

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a vertical sidebar with four steps: '1 Name and description' (highlighted in dark blue), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server:' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name:' with a text input field containing 'ASA\_Gold', and 'Description:' with a large empty text area.

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

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

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

## Creare una policy di storage delle macchine virtuali nel client vSphere

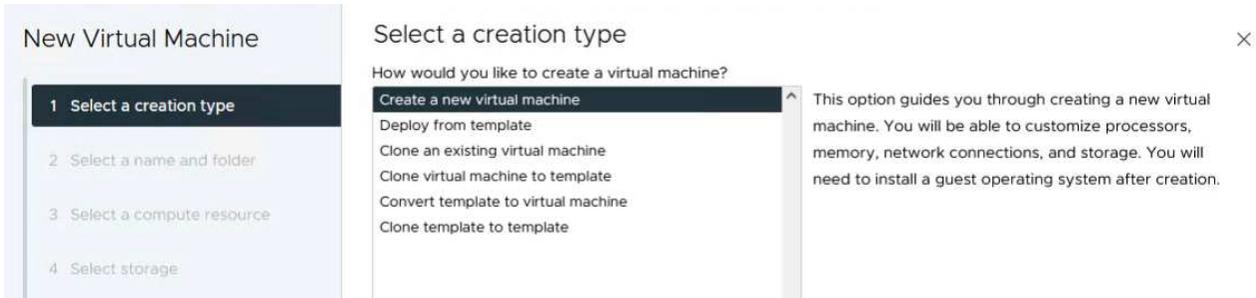
Un criterio di storage delle macchine virtuali è un insieme di regole e requisiti che definiscono le modalità di archiviazione e gestione dei dati delle macchine virtuali. Specifica le caratteristiche di storage desiderate, come performance, disponibilità e servizi dati, per una VM specifica.

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

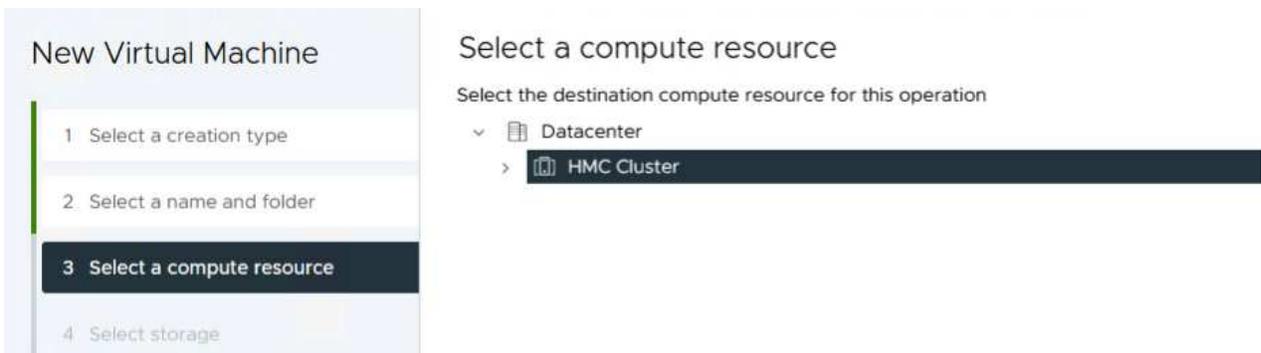
## Creare una macchina virtuale su un datastore vVol

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

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



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



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

## New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

VM Storage Policy

ASA\_Gold ▾

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	V
<input type="radio"/>	ASA400_ISCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	V
<input type="radio"/>	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
<input type="radio"/>	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
<input type="radio"/>	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-03 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V

Manage Columns      Items per page: 10      1 - 10 of 15 items      1 / 2

Compatibility

Validating...

CANCEL

BACK

NEXT

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

### New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Customize hardware

Configure the virtual machine hardware

Virtual Hardware   VM Options   Advanced Parameters

[ADD NEW DEVICE](#) ▾

> CPU *	4	▼ ⓘ
> Memory *	32	▼ GB ▼
> New Hard disk *	150	▼ GB ▼

**Maximum Size** 1.95 TB

**VM storage policy** ASA\_Gold ▾

**Location** Store with the virtual machine ▾

**Disk Provisioning** Thin Provision ▾

**Sharing** Unspecified ▾

**Disk Mode** Dependent ▾

**Virtual Device Node** New SCSI controller ▾ SCSI(0:0) New Hard disk ▾

> New SCSI controller LSI Logic SAS

> New Network VM Network  Connected

CANCEL
BACK
NEXT

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

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

## Array SAN all-flash NetApp con VMware vSphere 8

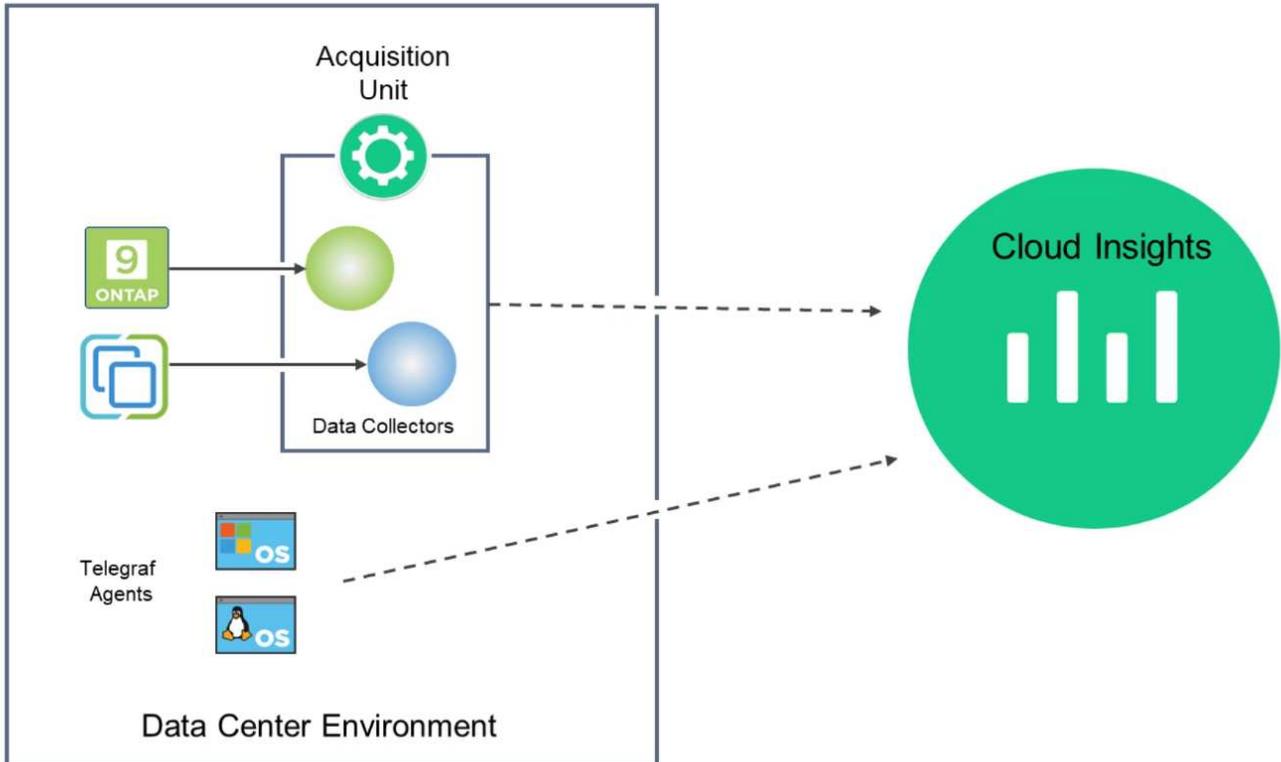
Autore: Josh Powell - NetApp Solutions Engineering

### Monitoraggio dello storage on-premise con NetApp Cloud Insights

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

NetApp Cloud Insights opera attraverso il software dell'unità di acquisizione, che è configurato con i raccoglitori di dati per asset come VMware vSphere e i sistemi storage NetApp ONTAP. Questi raccoglitori raccolgono i dati e li trasmettono a Cloud Insights. La piattaforma utilizza quindi una varietà di dashboard, widget e query di metrica per organizzare i dati in analisi approfondite che gli utenti possono interpretare.

Schema dell'architettura Cloud Insights:



### Panoramica sull'implementazione della soluzione

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

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

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

### Prerequisiti

Questa soluzione utilizza i seguenti componenti:

1. Array SAN all-flash NetApp A400 con ONTAP 9,13.
2. Cluster VMware vSphere 8,0.
3. Account NetApp Cloud Insights.
4. Software dell'unità di acquisizione NetApp Cloud Insights installato su una macchina virtuale locale con

connettività di rete agli asset per la raccolta dei dati.

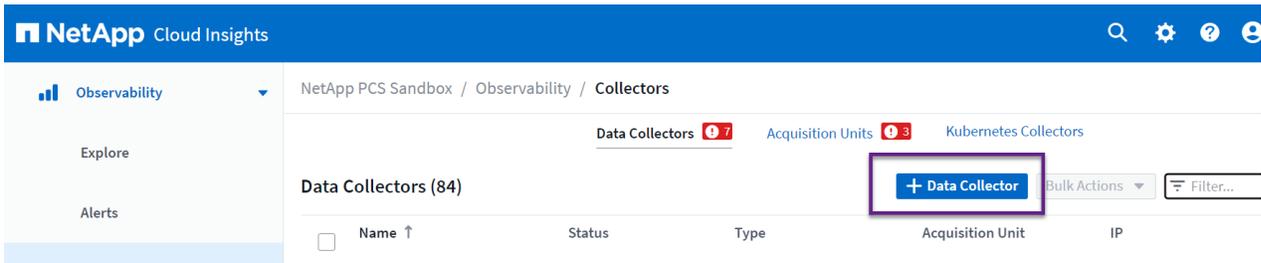
## **Implementazione della soluzione**

### **Configurare Data Collector**

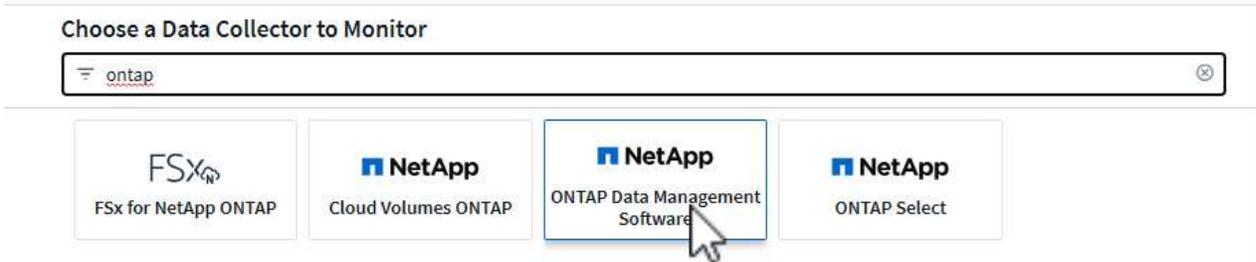
Per configurare Data Collector per i sistemi di storage VMware vSphere e ONTAP, completare i seguenti passaggi:

## Aggiunta di un Data Collector per un sistema di archiviazione ONTAP

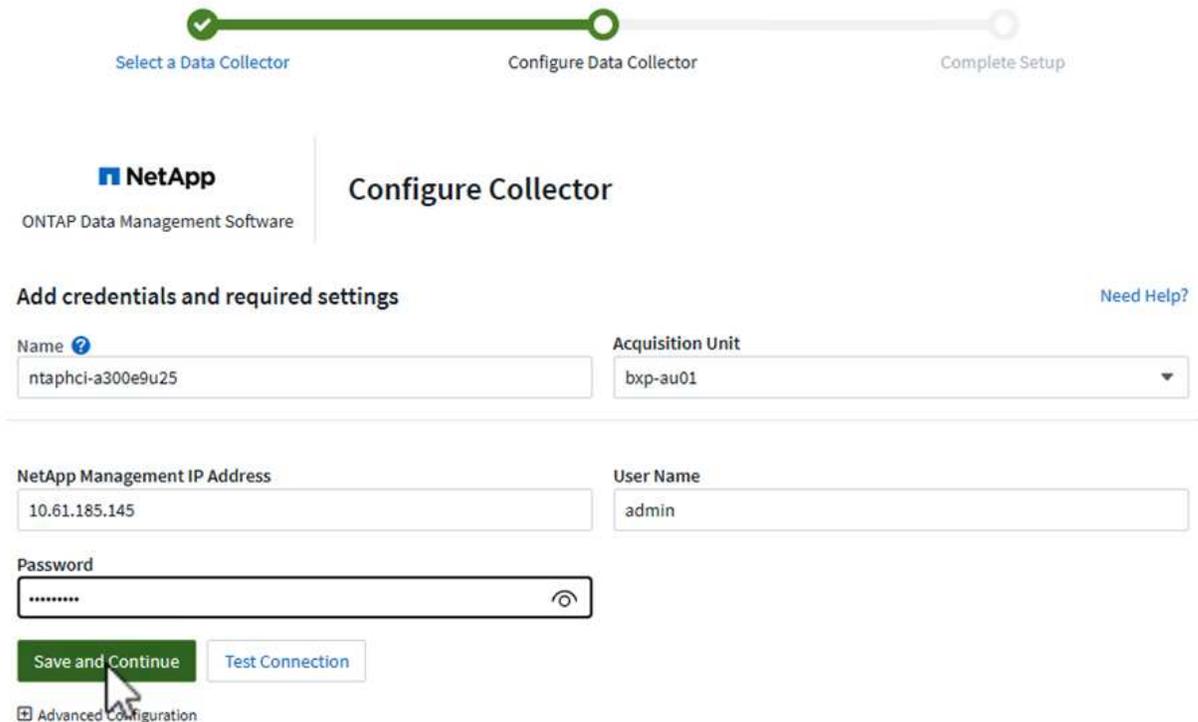
1. Una volta effettuato l'accesso a Cloud Insights, accedere a **osservabilità > Collector > Data Collector** e premere il pulsante per installare un nuovo Data Collector.



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

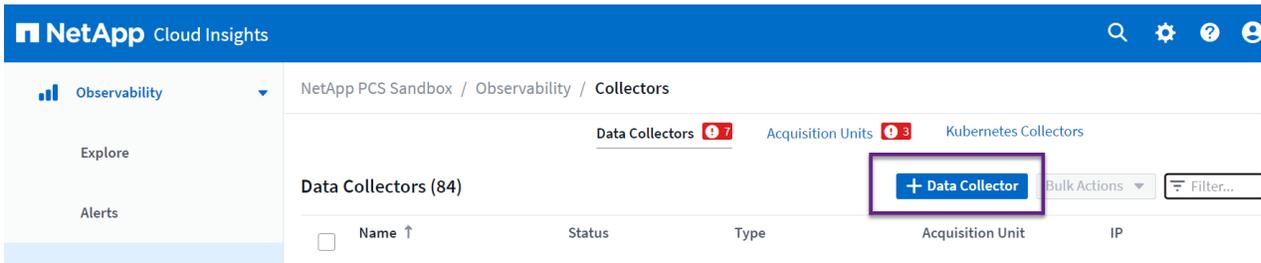


3. Nella pagina **Configure Collector** (Configura modulo di raccolta) compilare un nome per il raccogliatore, specificare l'unità di acquisizione \* corretta e fornire le credenziali per il sistema di archiviazione ONTAP. Fare clic su **Salva e continua**, quindi su **completa installazione** nella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

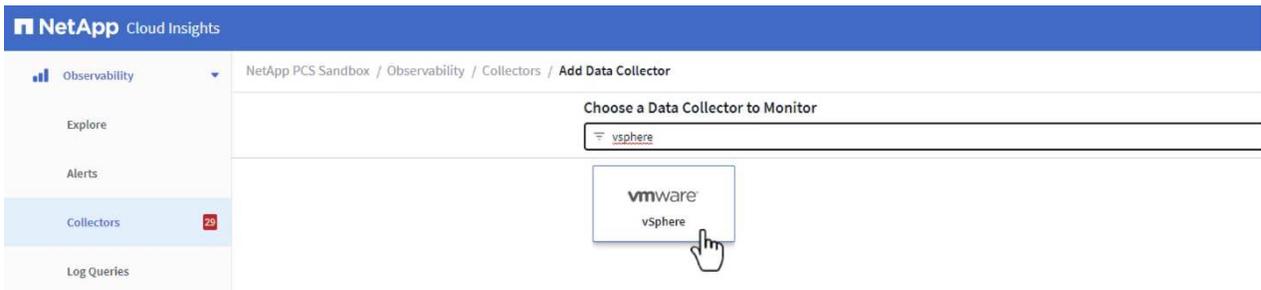


## Aggiunta di un Data Collector per un cluster VMware vSphere

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



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



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



## Configure Collector

### Add credentials and required settings

[Need Help?](#)

Name <a href="#">?</a> VCSA7	Acquisition Unit bxp-au01
---------------------------------	------------------------------

Virtual Center IP Address 10.61.181.210	User Name administrator@vsphere.local
--------------------------------------------	------------------------------------------

Password *****
-------------------

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
-----------------------------------------------	------------------------------------------------

#### Advanced Configuration

##### Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min) 20	Communication Port 443
-------------------------------------	---------------------------

Filter VMs by ESX_HOST	Choose 'Exclude' or 'Include' to Specify a List Exclude
---------------------------	------------------------------------------------------------

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)	Performance Poll Interval (sec) 300
-----------------------------------------------------------------------------------------------------	----------------------------------------

 Collect basic performance metrics only

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
-----------------------------------------------	------------------------------------------------

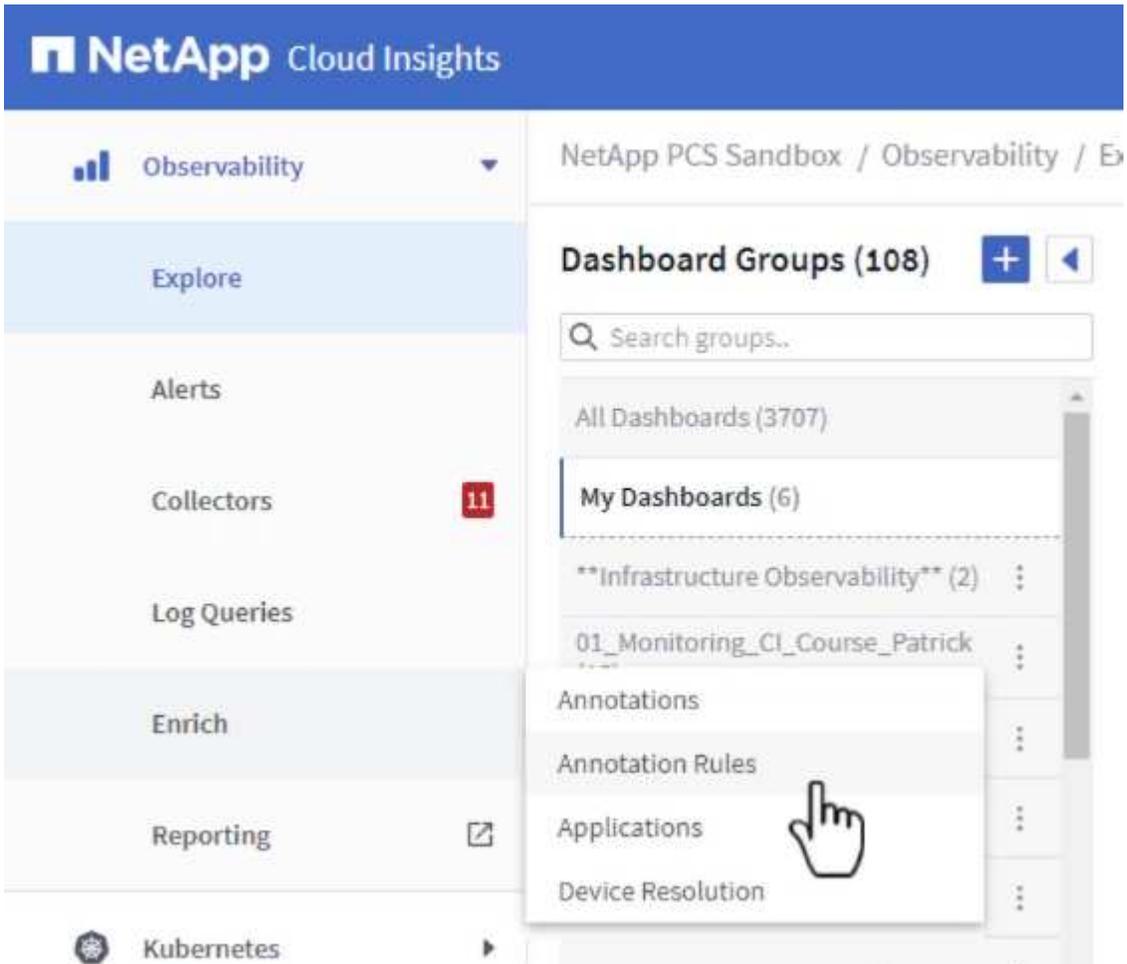
## Aggiungere annotazioni alle risorse

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

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

## Utilizzare le regole di annotazione per contrassegnare le risorse

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



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

**Add Rule**
✕

**Name**

**Query**

**Annotation**

**Value**

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

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Rules running... **Run All Rules**

**Annotation rules (217)**

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 2

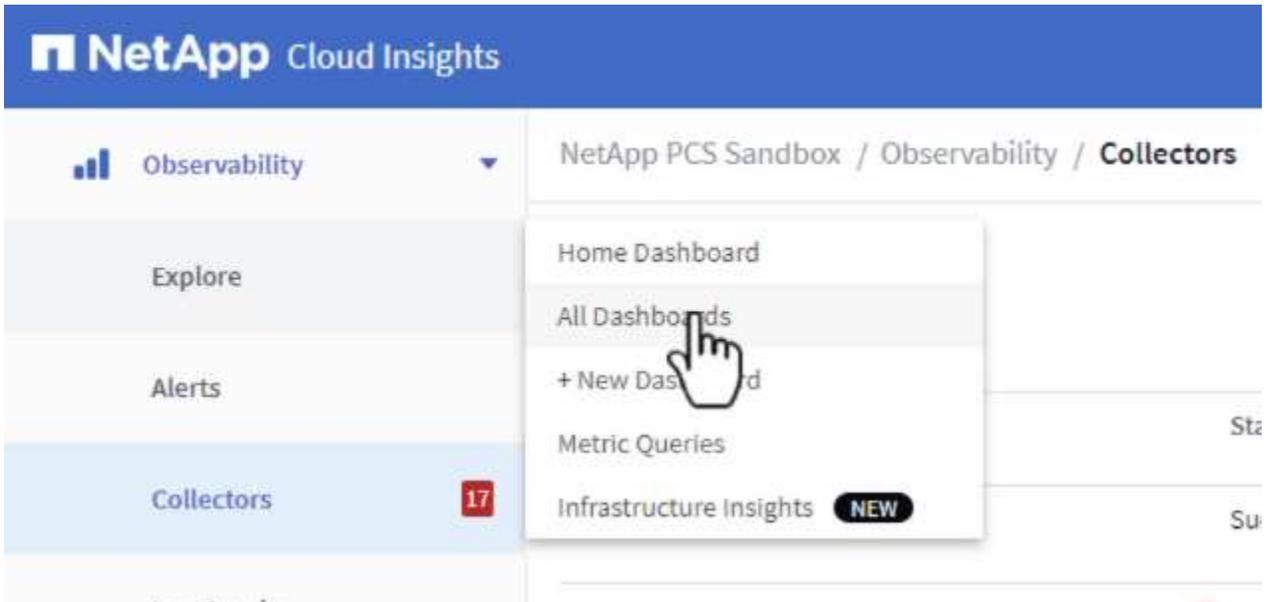
### Esplorare e correlare le risorse

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

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

## Correlazione delle risorse da una dashboard delle performance dello storage

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



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

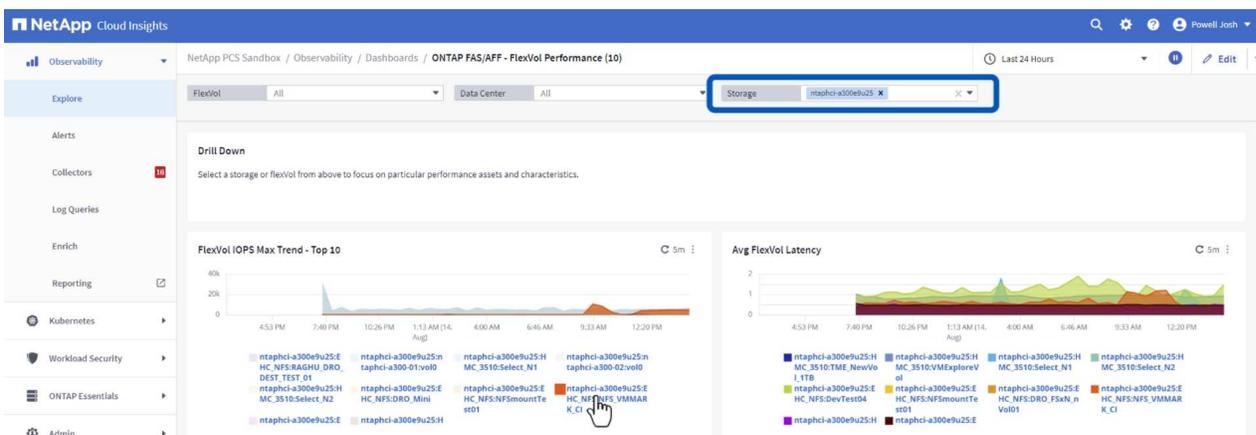


3. Scegliere un dashboard per le prestazioni FlexVol dall'elenco e fare clic sul pulsante **Aggiungi dashboard** nella parte inferiore della pagina.

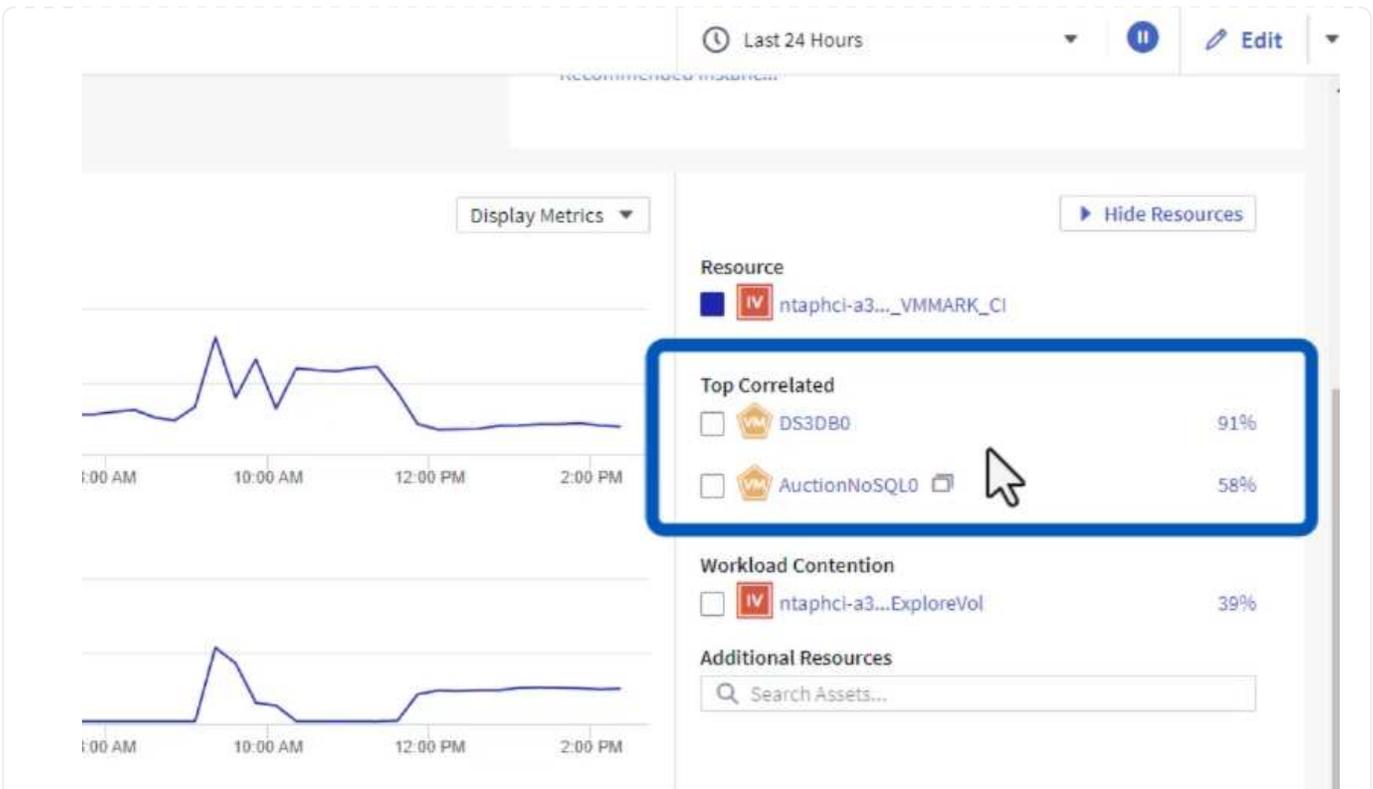
- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- StorageGRID - Capacity Summary
- StorageGRID - ILM Performance Monitoring
- StorageGRID - MetaData Usage
- StorageGRID - S3 Performance Monitoring
- VMware Admin - ESX Hosts Overview
- VMware Admin - Overview
- VMware Admin - VM Performance
- VMware Admin - Where are opportunities to right size?
- VMware Admin - Where can I potentially reclaim waste?
- VMware Admin - Where do I have VM Latency?

**+ Additional Dashboards (13)**  
 These dashboards require additional data collectors to be installed. [Add More](#)

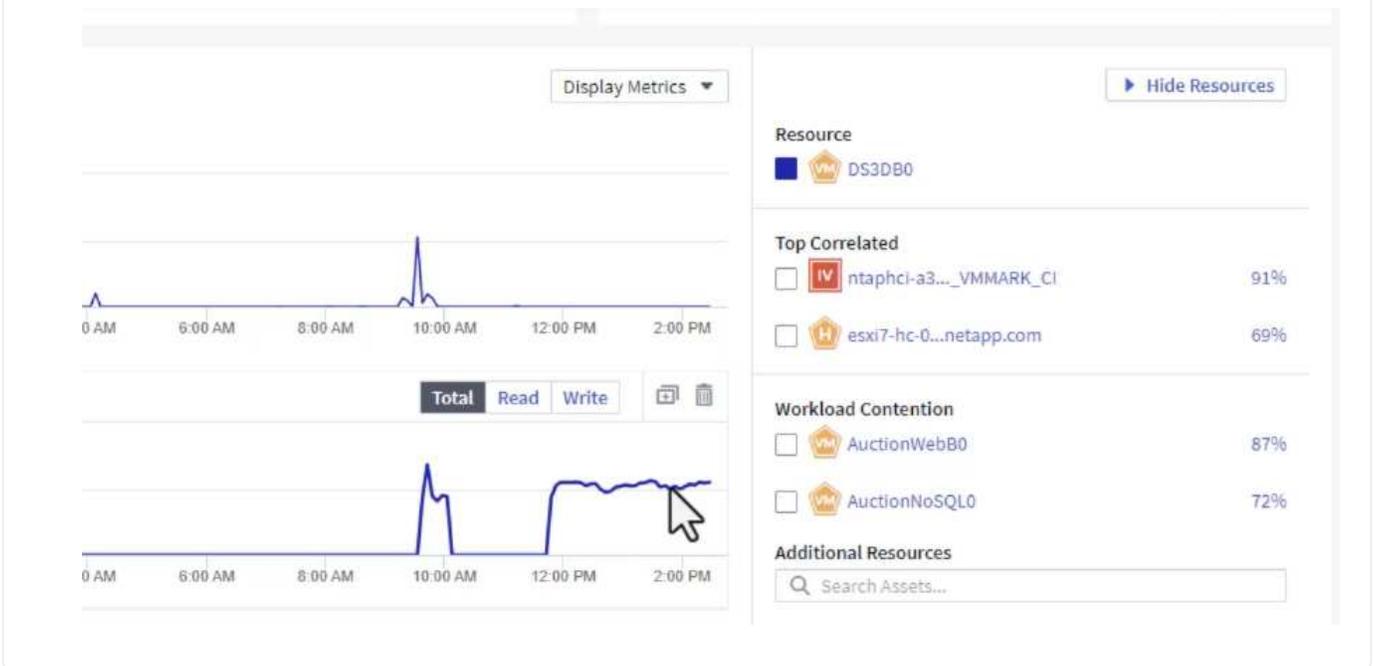
4. Una volta importata, aprire la dashboard. Da qui è possibile visualizzare vari widget con dati dettagliati sulle prestazioni. Aggiungi un filtro per visualizzare un singolo sistema di storage e seleziona un volume di storage per analizzare i dettagli.



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



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



### USA Cloud Insights per identificare i noisy neighbor

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

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

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

NetApp PCS Sandbox / Observability / Explore / Dashboards

Dashboard Groups (108) + My Dashboards (6) + From Gallery + Dashboard

Search groups..

All Dashboards (3709)

My Dashboards (6)

- \*\*Infrastructure Observability\*\* (2)
- 01\_Monitoring\_CI\_Course\_Patrick (15)
- 02\_Monitoring\_CI\_Course\_Vish (5)
- 1\_Str Dashboards (8)

Name ↑	Owner
All SAN Array Status (2)	Powell Josh
Cloud Volumes ONTAP - FlexVol Performance (6)	Powell Josh
ONTAP - Volume Workload Performance (Frontend) (7)	Powell Josh
VMware Admin - Where are opportunities to right size? (37)	Powell Josh
VMware Admin - Where can I potentially reclaim waste? (11)	Powell Josh
<input checked="" type="checkbox"/> VMware Admin - Where do I have VM Latency? (9)	Powell Josh

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

/ VMware Admin - Where do I have VM Latency? (9) Last 3 Hours

VirtualMachine All Data Center Solutions Engineering X diskLatency.total ≥ All

! 5m Avg Latency (all hypervisors) C 5m VM Count With Latency Concern C 5m Avg Latency (all VMs)

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

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

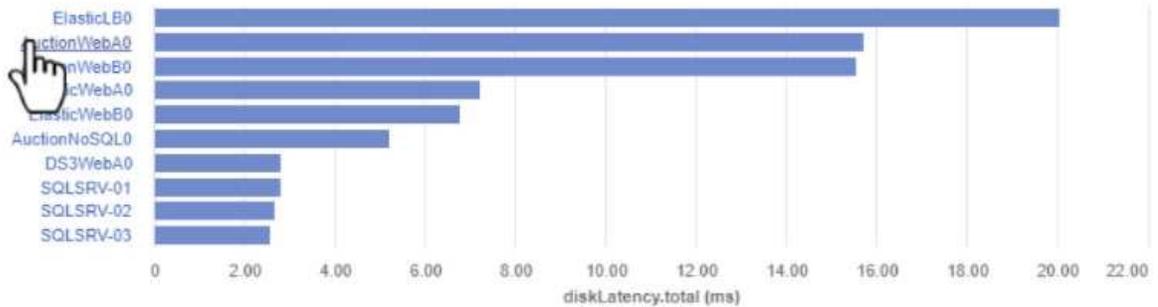
5m

1.55 ms

diskLatency.total

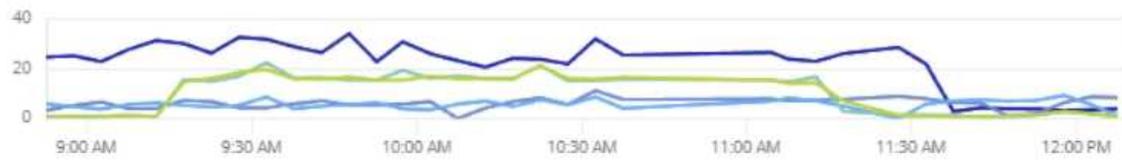
Avg VM Latency - Top 10

5m

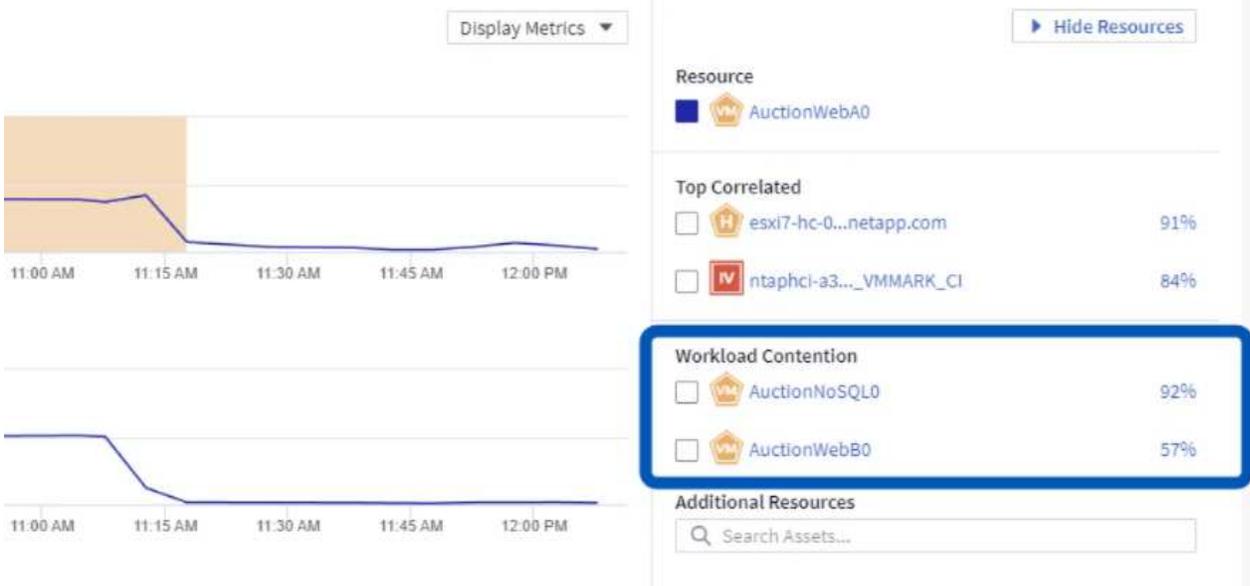


Top 5 Avg VM Latency Trend

30s



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



## **Visualizzare le risorse sottoutilizzate in Cloud Insights**

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

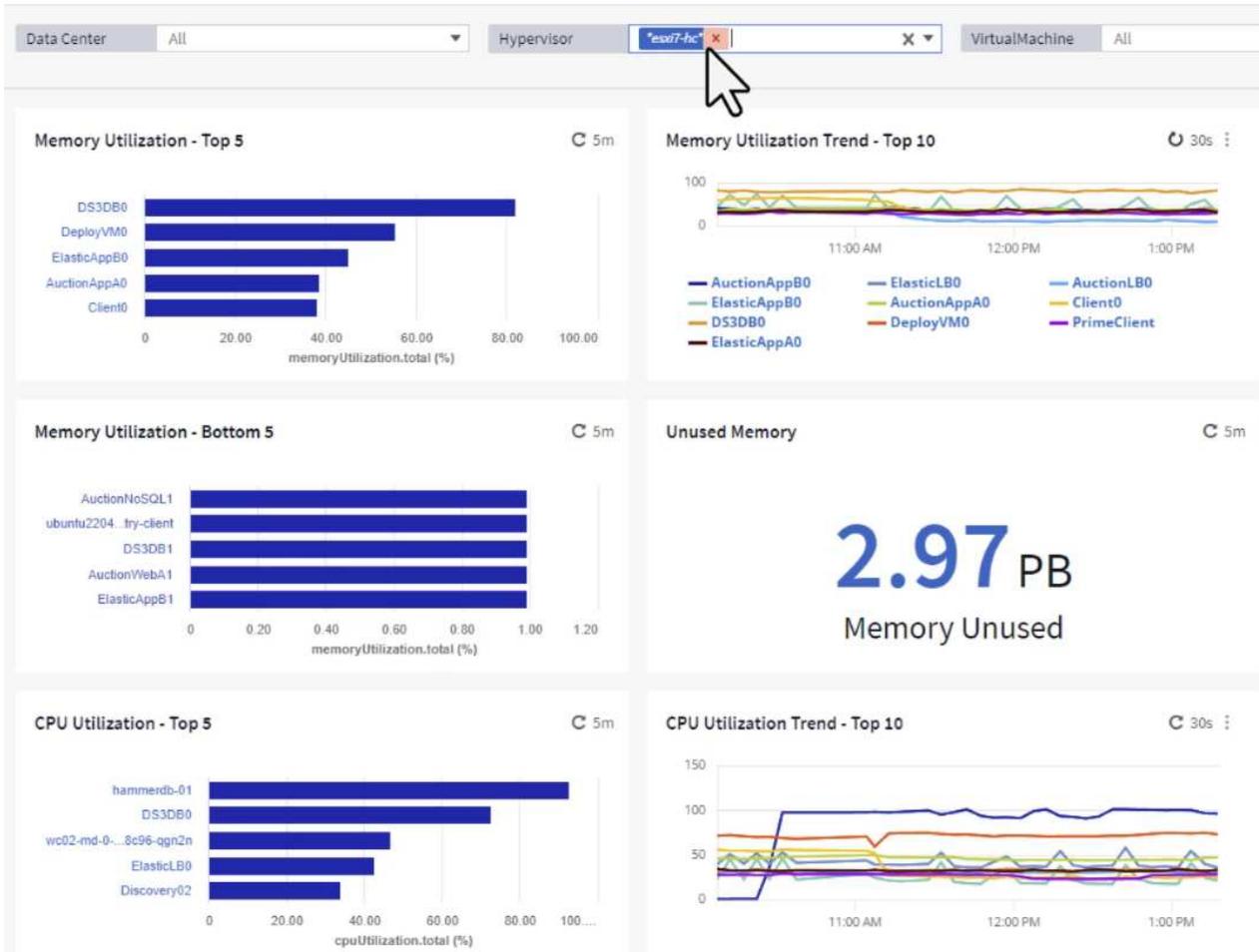
## Identifica le opportunità per il corretto dimensionamento delle macchine virtuali

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

### My Dashboards (6)

<input type="checkbox"/>	Name ↑
	<a href="#">All SAN Array Status (2)</a>
	<a href="#">Cloud Volumes ONTAP - FlexVol Performance (6)</a>
	<a href="#">ONTAP - Volume Workload Performance (Frontend) (7)</a>
<input type="checkbox"/>	<a href="#">VMware Admin - Where are opportunities to right size? (37)</a>
	<a href="#">VMware Admin - Where do I potentially reclaim waste? (11)</a>
	<a href="#">VMware Admin - Where do I have VM Latency? (9)</a>

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



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

## Memory Usage

5m

121 items found

Virtual Machine	memory (MiB)	memoryUt... ↓
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

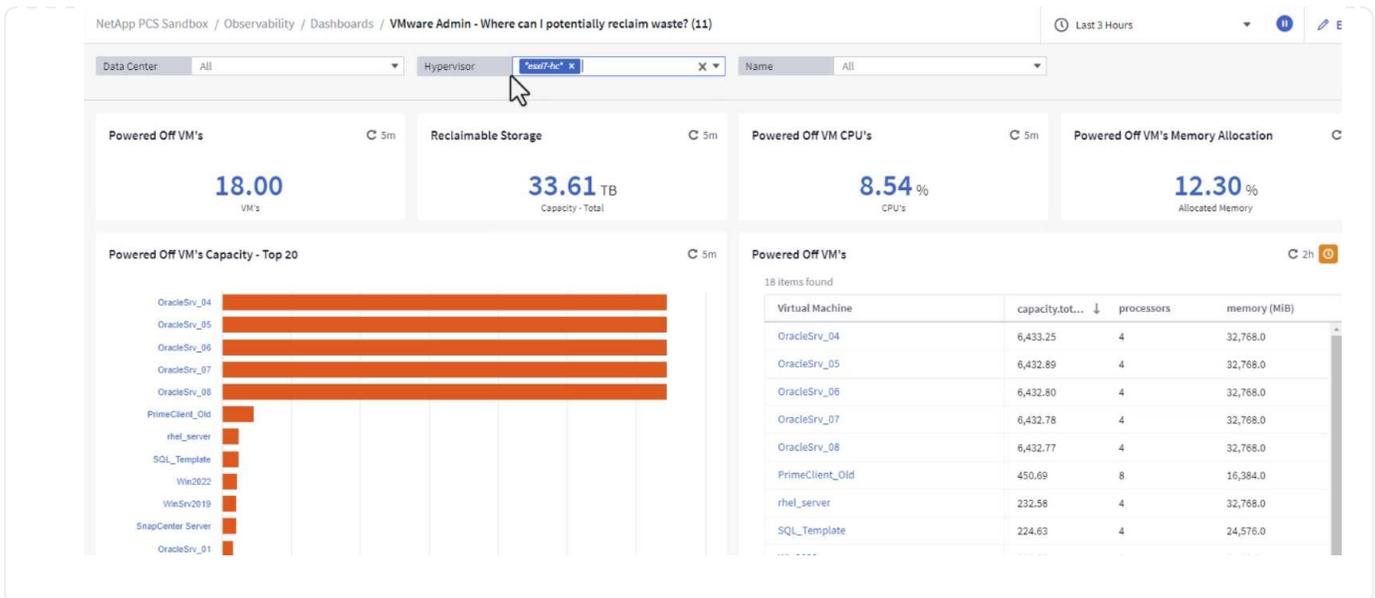
## CPU Utilization

5m

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

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

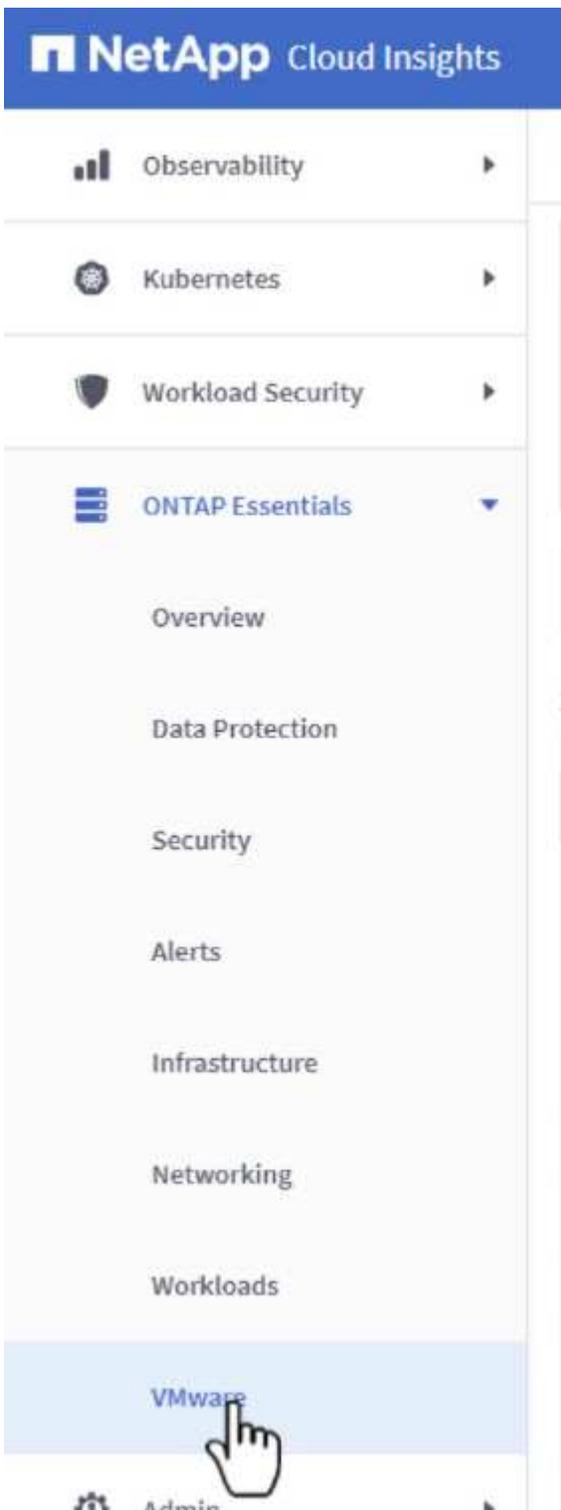


## Utilizzare le query per isolare e ordinare le metriche

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

## Visualizzate una query VMware dettagliata in ONTAP Essentials

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



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

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacity.ratio.us...	diskIops.total (I/O/s)	diskLatency.total...	diskThroughput...
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

## Conclusion

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

## Ulteriori informazioni

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

- ["Landing page di NetApp BlueXP e Cloud Insights"](#)
- ["Documentazione NetApp Cloud Insights"](#)

# Demo ed esercitazioni

## Video e demo sulla virtualizzazione

Guarda i seguenti video e demo che illustrano le funzionalità specifiche delle soluzioni di cloud ibrido, virtualizzazione e container.

### Strumenti NetApp ONTAP per VMware vSphere

[Strumenti ONTAP per VMware - Panoramica](#)

[Provisioning di archivi dati VMware iSCSI con ONTAP](#)

[Provisioning di archivi dati VMware NFS con ONTAP](#)

## Plug-in SnapCenter per VMware vSphere

Il software NetApp SnapCenter è una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system.

Il plug-in SnapCenter per VMware vSphere consente di eseguire operazioni di backup, ripristino e collegamento per macchine virtuali e operazioni di backup e montaggio per datastore registrati con SnapCenter direttamente in VMware vCenter.

Per ulteriori informazioni sul plug-in NetApp SnapCenter per VMware vSphere, consultare la "[Panoramica del plug-in NetApp SnapCenter per VMware vSphere](#)".

[Plug-in SnapCenter per VMware vSphere - prerequisiti della soluzione](#)

[Plug-in SnapCenter per VMware vSphere - implementazione](#)

[Plug-in SnapCenter per VMware vSphere - flusso di lavoro di backup](#)

[Plug-in SnapCenter per VMware vSphere - flusso di lavoro di ripristino](#)

[SnapCenter - flusso di lavoro di ripristino SQL](#)

## Soluzioni per la protezione dei dati 3-2-1

Le soluzioni per la protezione dei dati 3-2-1 combinano backup primari e secondari on-premise, utilizzando la tecnologia SnapMirror, con copie replicate sullo storage a oggetti utilizzando il backup e recovery di BlueXP.

[Protezione dei dati 3-2-1 per datastore VMFS con plug-in SnapCenter per backup e recovery di VMware vSphere e BlueXP per macchine virtuali](#)

## VMware Cloud su AWS con AWS FSX per NetApp ONTAP

[Storage connesso guest Windows con FSX ONTAP utilizzando iSCSI](#)

[Storage connesso guest Linux con FSX ONTAP con NFS](#)

[Risparmi sul TCO di VMware Cloud su AWS con Amazon FSX per NetApp ONTAP](#)

[Archivio dati supplementare VMware Cloud su AWS con Amazon FSX per NetApp ONTAP](#)

[Installazione della configurazione e dell'implementazione di VMware HCX per VMC](#)

[Dimostrazione della migrazione a VMotion con VMware HCX per VMC e FSxN](#)

[Dimostrazione della migrazione a freddo con VMware HCX per VMC e FSxN](#)

## **Azure servizi VMware su Azure con Azure NetApp Files (ANF)**

[Panoramica del datastore supplementare della soluzione VMware Azure con Azure NetApp Files](#)

[Soluzione VMware Azure DR con Cloud Volumes ONTAP, SnapCenter e JetStream](#)

[Dimostrazione della migrazione a freddo con VMware HCX per AVS e ANF](#)

[Dimostrazione di VMotion con VMware HCX per AVS e ANF](#)

[Dimostrazione della migrazione in blocco con VMware HCX per AVS e ANF](#)

## **VMware Cloud Foundation con NetApp ONTAP**

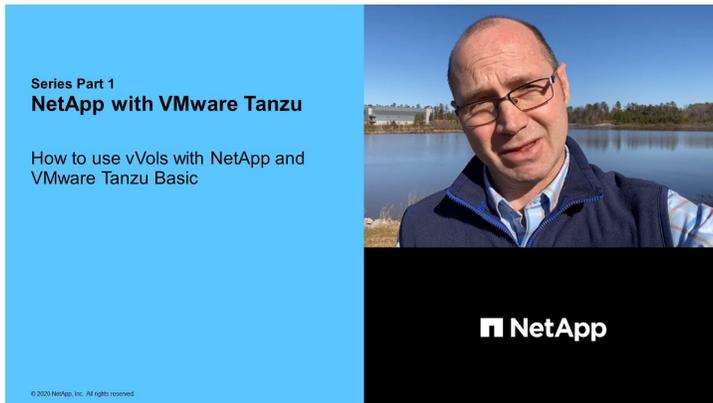
[Archivi dati NFS come archiviazione principale per i domini del carico di lavoro VCF](#)

[Archivi dati iSCSI come archiviazione supplementare per i domini di gestione VCF](#)

## NetApp con VMware Tanzu

VMware Tanzu consente ai clienti di implementare, amministrare e gestire il proprio ambiente Kubernetes tramite vSphere o VMware Cloud Foundation. Questo portfolio di prodotti VMware consente ai clienti di gestire tutti i cluster Kubernetes pertinenti da un singolo piano di controllo scegliendo l'edizione VMware Tanzu più adatta alle loro esigenze.

Per ulteriori informazioni su VMware Tanzu, consultare ["Panoramica di VMware Tanzu"](#). Questa recensione illustra i casi d'utilizzo, le aggiunte disponibili e molto altro ancora su VMware Tanzu.



Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 1



Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 2



Come utilizzare vVol con NetApp e VMware Tanzu Basic, parte 3

## NetApp Cloud Insights

NetApp Cloud Insights è una piattaforma completa di monitoring e analytics progettata per fornire visibilità e controllo sulla tua infrastruttura cloud e on-premise.

[NetApp Cloud Insights - osservabilità per il moderno data center](#)

## 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.