



VMware Cloud Foundation su NetApp

NetApp virtualization solutions

NetApp
January 12, 2026

Sommario

VMware Cloud Foundation su NetApp	1
Semplifica l'esperienza del cloud ibrido con VMware Cloud Foundation e ONTAP	1
Introduzione	1
Introduzione a NetApp ONTAP	1
Introduzione a VMware Cloud Foundation	1
Domini VCF	1
Archiviazione con VCF	2
Perché ONTAP per VCF	3
Informazioni aggiuntive:	4
Riepilogo	5
Risorse di documentazione	5
Opzioni di progettazione con VMware Cloud Foundation e ONTAP	6
Opzioni di archiviazione	6
Progetti	6
Configurare ambienti cloud privati con VMware Cloud Foundation e ONTAP	11
Distribuisci una nuova istanza VCF 9	11
Convergere i componenti esistenti in VCF 9	13
Aggiorna un ambiente VCF esistente a VCF 9	14
Implementazione del Disaster Recovery con NetApp Disaster Recovery	14
Iniziare	15
Configurazione NetApp Disaster Recovery	17
Configurazione della replicazione dello storage tra l'array del sito di origine e l'array del sito di destinazione	18
Come impostare le relazioni di replica per NetApp Disaster Recovery	18
Cosa può fare per te NetApp Disaster Recovery ?	18
Failover di prova	23
Operazione di test di failover di pulizia	25
Migrazione pianificata e failover	25
Rifasamento	27
Monitoraggio e dashboard	28
Convertire i cluster vSphere esistenti in VCF	29
Scopri come convertire un ambiente vSphere con datastore esistenti in un dominio di gestione VCF	30
Flusso di lavoro di distribuzione per la conversione delle istanze del server vCenter in domini di gestione VCF con datastore NFS	32
Flusso di lavoro di distribuzione per la conversione delle istanze del server vCenter in domini di gestione VCF con datastore Fibre Channel	32
Fornire VCF con storage principale	33
Fornire un ambiente VCF con ONTAP come soluzione di archiviazione principale	33
Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per il dominio di gestione VCF	33
Utilizzare un datastore NFS su ONTAP come storage principale per il dominio di gestione VCF	34
Utilizzare un datastore VMFS basato su FC su ONTAP come storage principale per un dominio di carico di lavoro VI	36

Utilizzare un datastore NFS su ONTAP come storage principale per un dominio di carico di lavoro VI	38
Espandi VCF con spazio di archiviazione supplementare	59
Scopri come espandere lo storage per un ambiente VCF utilizzando storage supplementare	59
Espandi i domini di gestione con iSCSI	61
Aggiungere un datastore VMFS basato su FC come storage supplementare per un dominio di gestione utilizzando gli ONTAP tools for VMware vSphere	83
Espandi i domini del carico di lavoro VI con vVols iSCSI	84
Espandi i domini del carico di lavoro VI con vVols NFS	112
Espandi i domini del carico di lavoro VI con NVMe/TCP	138
Aggiungere un datastore VMFS basato su FC come storage supplementare ai domini di carico di lavoro VI	160
Proteggi VCF con SnapCenter	161
Scopri come proteggere i domini dei carichi di lavoro VCF con il plug-in SnapCenter per VMware vSphere	161
Proteggi un dominio di carico di lavoro VCF con il plug-in SnapCenter per VMware vSphere	161
Proteggere i domini di gestione e carico di lavoro VCF utilizzando il plug-in SnapCenter per VMware vSphere	196
Proteggi i domini dei carichi di lavoro VCF con l'archiviazione NVMe su TCP e il plug-in SnapCenter per VMware vSphere	209
Proteggi i carichi di lavoro con vSphere Metro Storage Cluster	216
Scopri come integrare l'alta disponibilità ONTAP con VMware vSphere Metro Storage Cluster (vMSC)	216
Configurare un cluster esteso per un dominio di gestione VCF utilizzando MetroCluster	217
Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando MetroCluster	228
Configurare un cluster esteso per un dominio di gestione VCF utilizzando SnapMirror Active Sync	240
Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando SnapMirror Active Sync	242
Migrazione delle VM da VMware vSphere ai datastore ONTAP	244
Requisiti di rete	245
Scenari di migrazione delle VM	246
Scenari di migrazione dei modelli di VM	270
Casi d'uso	277
Risorse aggiuntive	278
Protezione autonoma contro i ransomware per l'archiviazione NFS	278
Monitora l'archiviazione on-premise con Data Infrastructure Insights	288
Monitoraggio dell'archiviazione locale con Data Infrastructure Insights	288
Panoramica sulla distribuzione della soluzione	288
Prerequisiti	289
Distribuzione della soluzione	289
Conclusione	306
Informazioni aggiuntive	306

VMware Cloud Foundation su NetApp

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

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

Introduzione

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

Introduzione a NetApp ONTAP

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

Introduzione a VMware Cloud Foundation

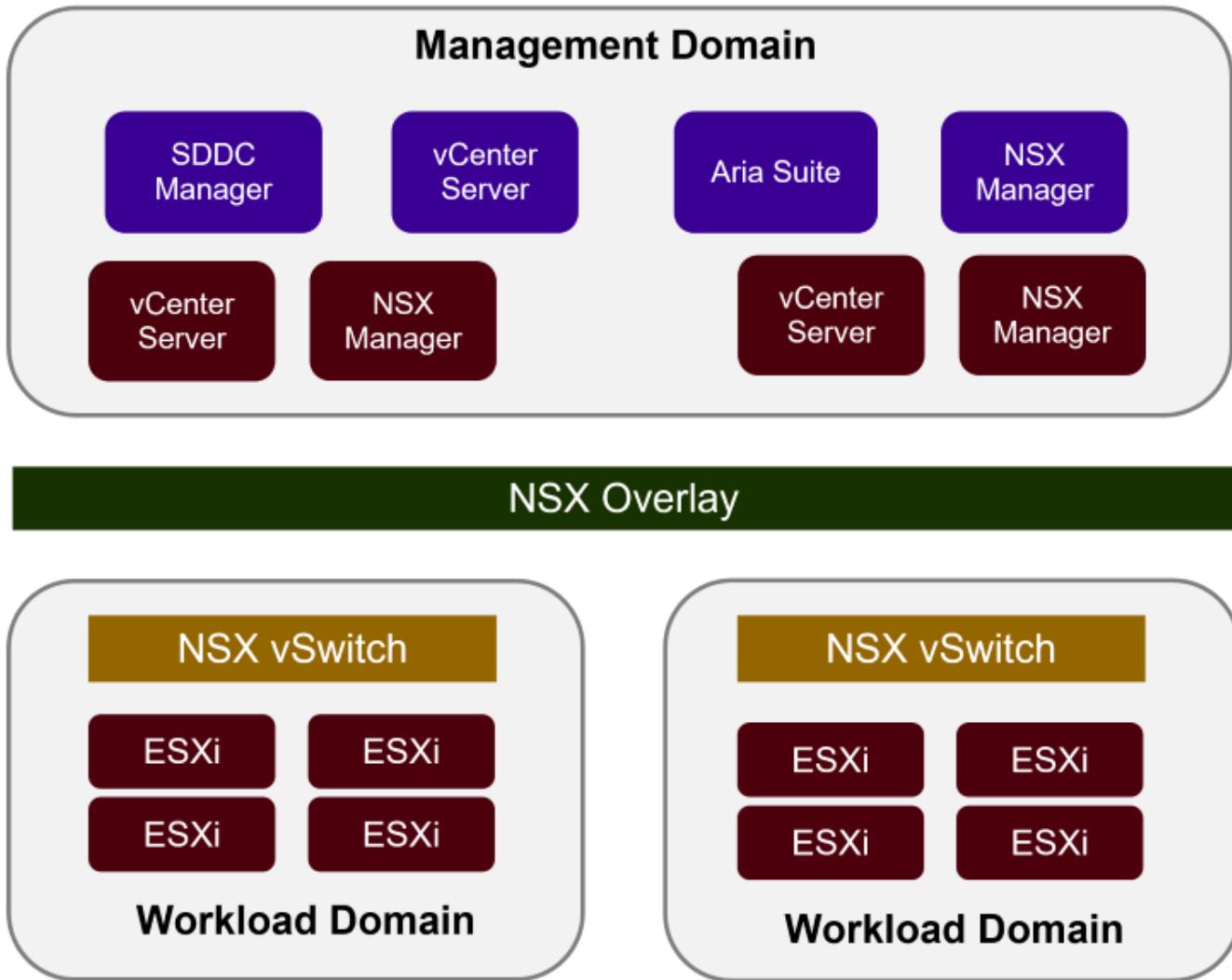
VCF integra le offerte di elaborazione, rete e storage con i prodotti VMware e le integrazioni di terze parti, facilitando sia i carichi di lavoro nativi Kubernetes sia quelli basati su macchine virtuali. Questa piattaforma software include componenti chiave quali VMware vSphere, NSX, Aria Suite Enterprise,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



Domini VCF

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

di elaborazione, rete e storage.



Esistono due tipi principali di domini con VCF:

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

Archiviazione con VCF

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

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

Esistono due tipi principali di archiviazione con VCF:

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

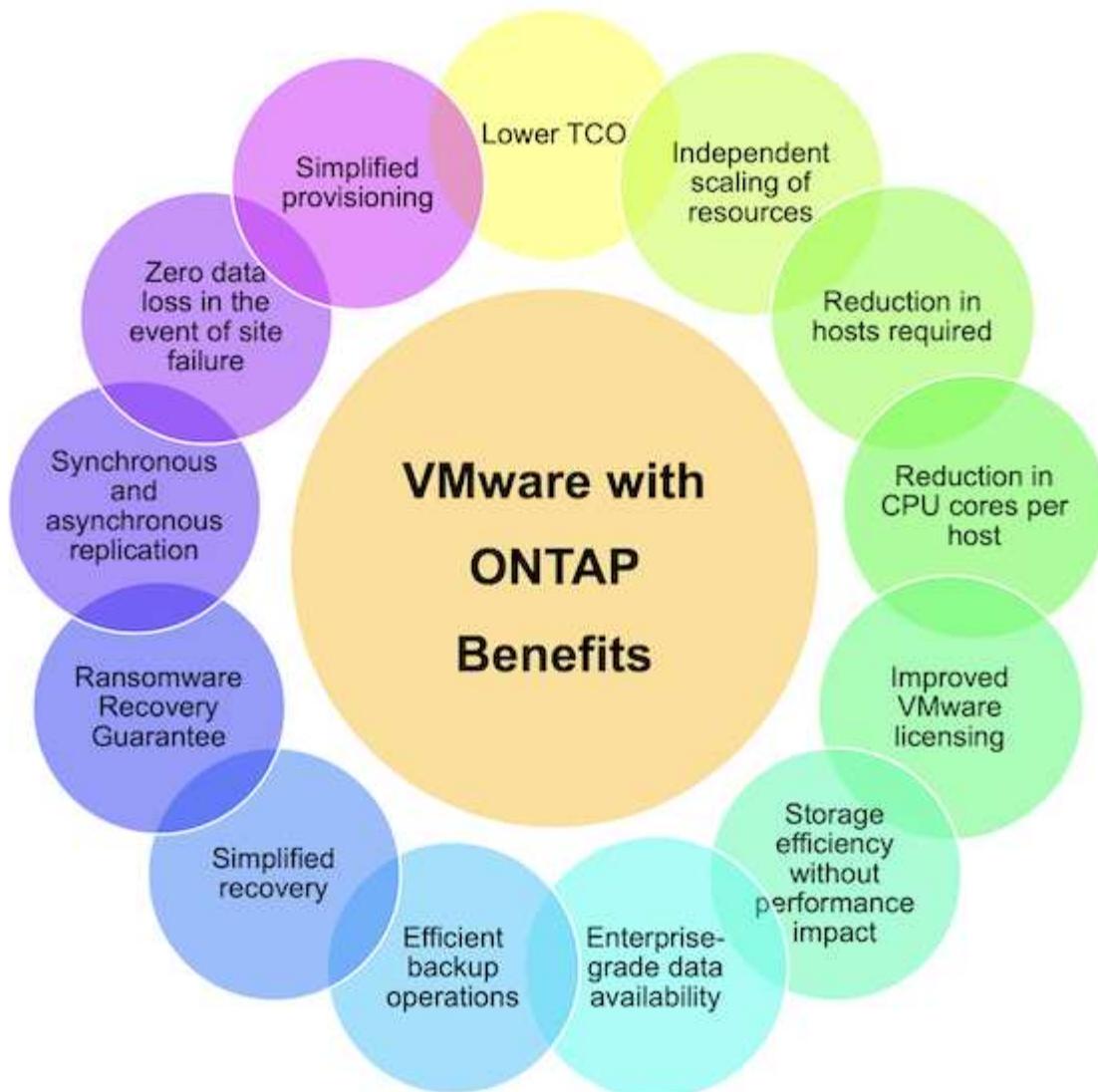
Supporta i tipi di archiviazione VCF

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

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

Perché ONTAP per VCF

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



Per ulteriori informazioni sui principali vantaggi ONTAP per VMware VCF identificati di seguito, vedere "[Perché ONTAP per VMware](#)" .

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

Informazioni aggiuntive:

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

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

Riepilogo

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

Risorse di documentazione

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

Documentazione di VMware Cloud Foundation

- "Documentazione di VMware Cloud Foundation"

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

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

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

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

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

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

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

Opzioni di progettazione con VMware Cloud Foundation e ONTAP

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

Opzioni di archiviazione

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

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

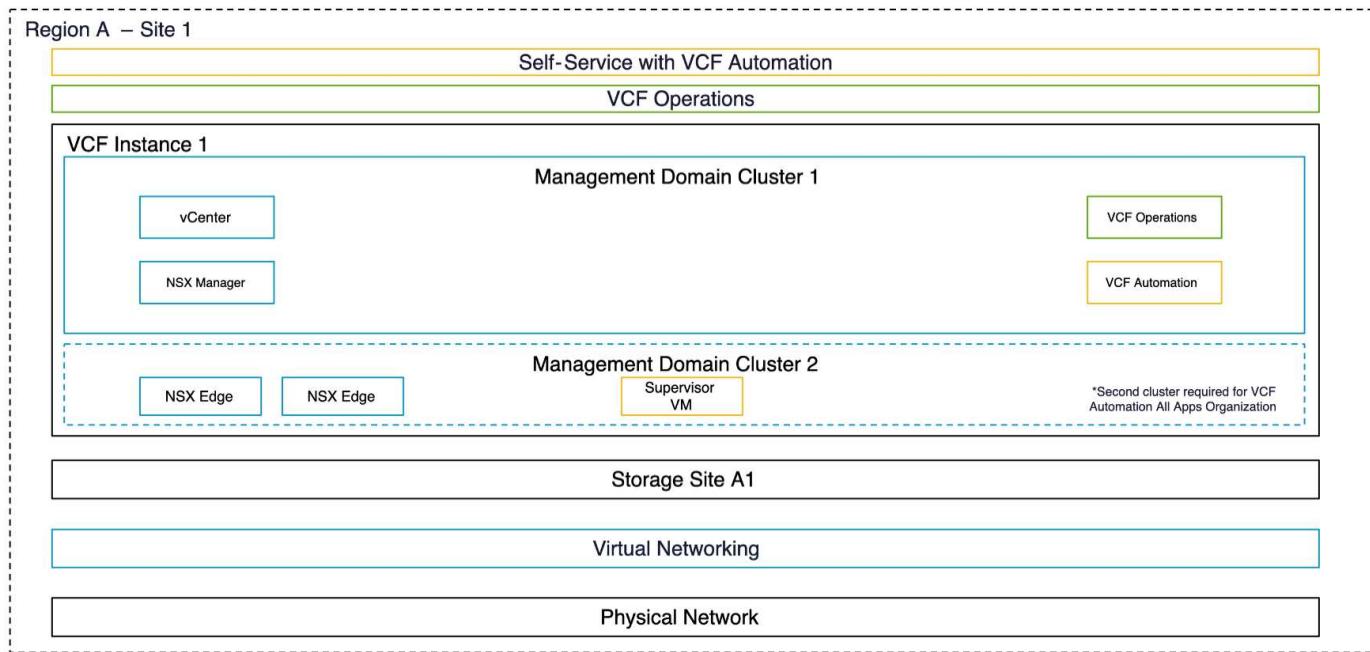
Famiglia di prodotti	VMFS su FC	VMFS su iSCSI	VMFS su NVMe-oF	NFSv3	NFSv4.1
ASA serie A e serie C	Sì	Sì	Sì	NO	NO
Serie A e serie C AFF	Sì	Sì	Sì	Sì	Sì
FAS	Sì	Sì	Sì	Sì	Sì

Progetti

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

Flotta VCF in un unico sito con ingombro minimo

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



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



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

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

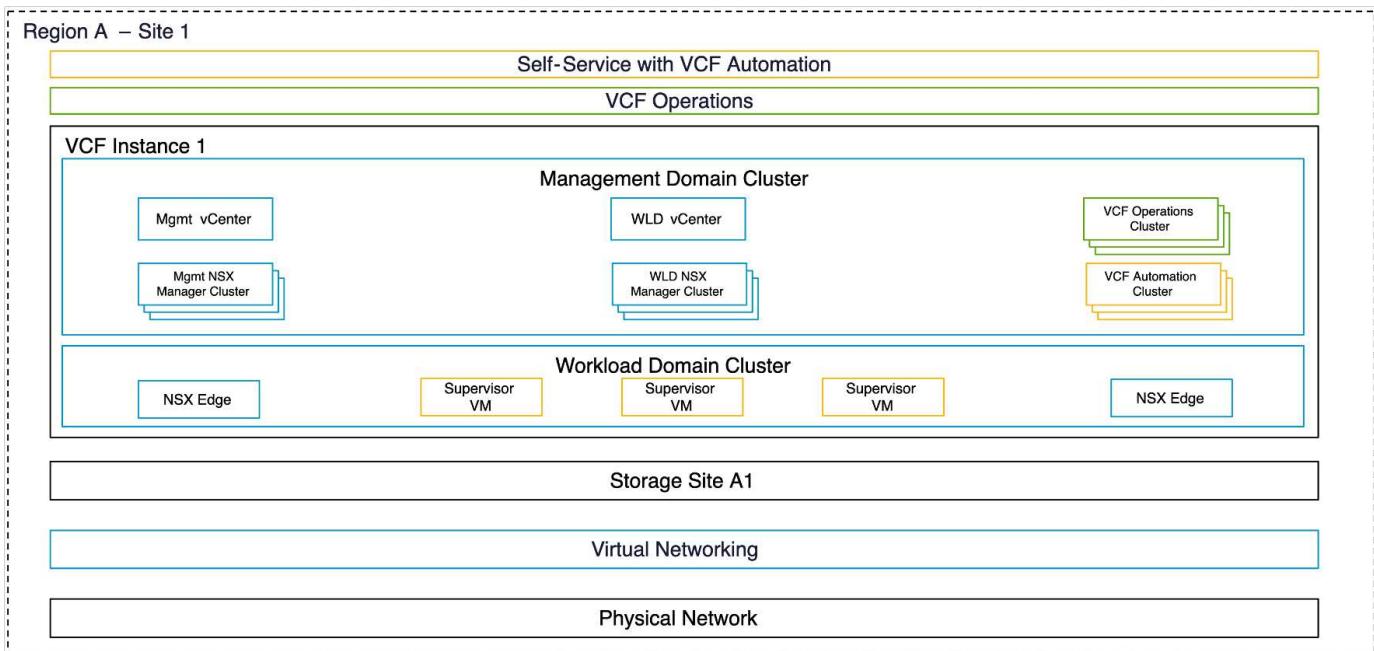
Flotta VCF in un unico sito

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

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



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



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

[Archivio dati supplementare VCF con strumenti ONTAP](#)

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

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

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

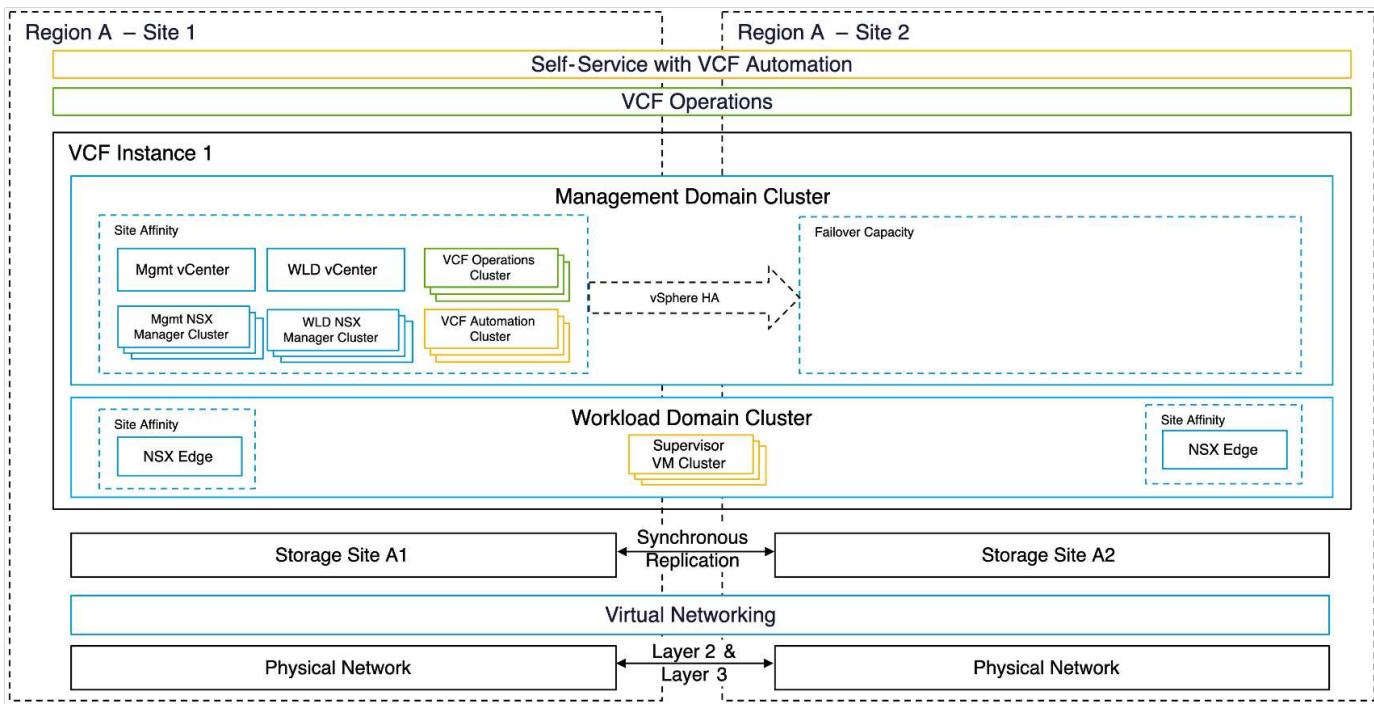
Flotta VCF con più siti in una singola regione

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

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

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

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



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

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

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

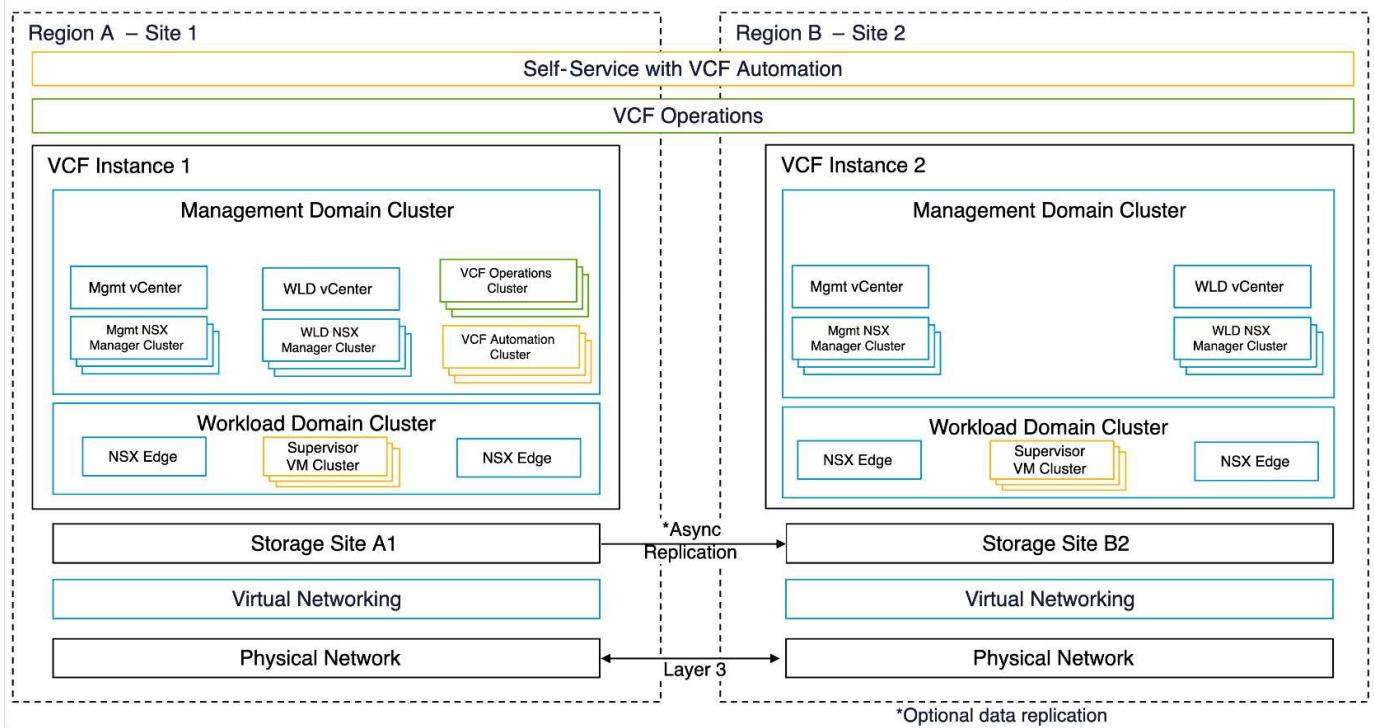
Per maggiori informazioni, consultare il "["Documentazione tecnica Broadcom sulla flotta VCF con più siti in una singola regione"](#)" .

Flotta VCF con più sedi in più regioni

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

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

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



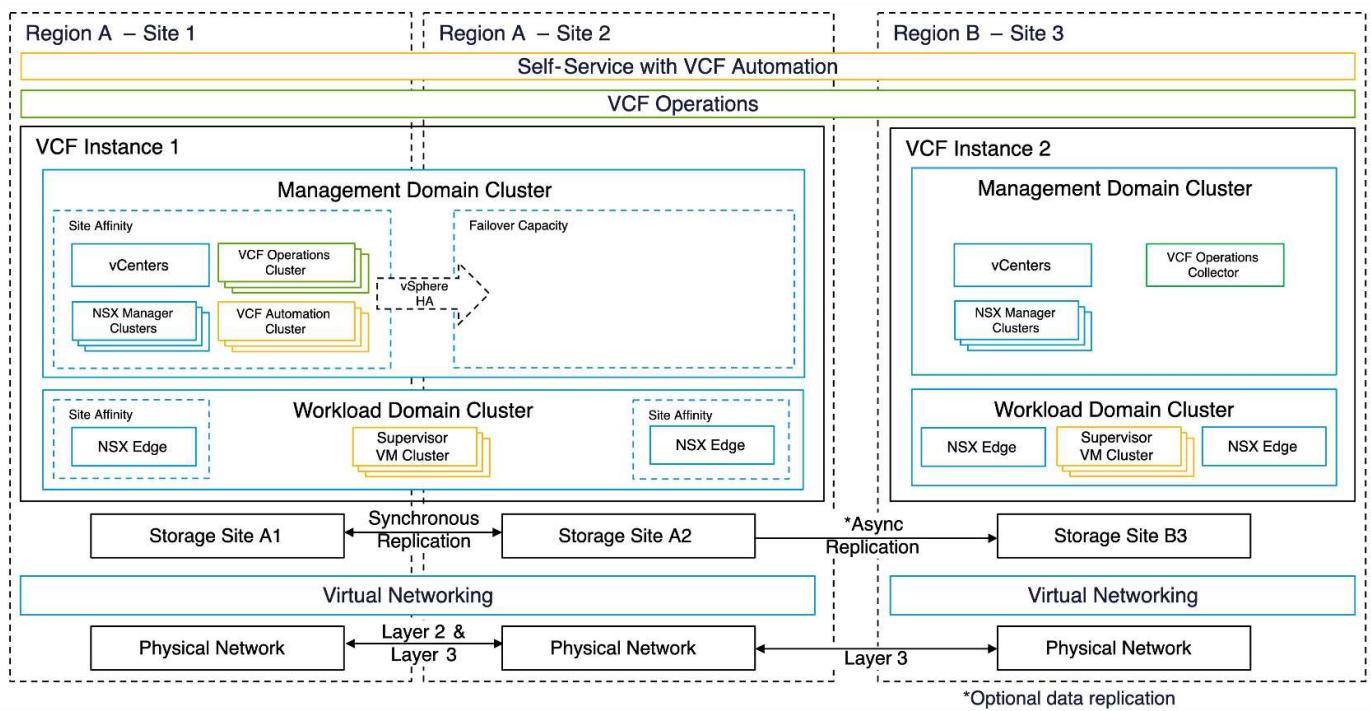
Gli strumenti ONTAP forniscono un'interfaccia utente per la configurazione della replicazione del datastore. NetApp Console può essere utilizzato anche per la replica tra array di storage. Il SnapCenter Plug-in for VMware vSphere utilizza le relazioni SnapMirror esistenti per gli SnapShot.

Per maggiori informazioni, consultare il "["Documentazione tecnica Broadcom sulla flotta VCF con più siti in più regioni"](#)" .

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

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

ASA, AFF e FAS supportano questa opzione di progettazione.



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

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

Configurare ambienti cloud privati con VMware Cloud Foundation e ONTAP

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

Distribuisci una nuova istanza VCF 9

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

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

Passi

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

VMFS su FC

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



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

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

NFSv3

1. Creare un'interfaccia VMkernel su un host ESXi.
2. Assicurare il "[SVM ha NFS abilitato](#)" E "[vStorage su NFS è abilitato](#)".
3. Creare un volume ed esportarlo con una policy che consenta gli host ESXi.
4. Regolare le autorizzazioni secondo necessità.
5. Distribuire l' ONTAP NFS VAAI VIB e includerlo nell'immagine vLCM. Per esempio: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip`. (Scaricare il file ZIP dal sito di supporto NetApp .)
6. Montare il volume NFS sull'host in cui è stata creata l'interfaccia VMkernel. Per esempio: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-c101-nfs01`.



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

1. Al termine della fase **Verifica riepilogo distribuzione e revisione passaggi successivi** nella fase **Distribuzione flotta VCF**, completare quanto segue:

- a. Distribuisci gli strumenti ONTAP

- "[Scarica gli strumenti ONTAP 10.x](#)"dal sito di supporto NetApp .
- Creare record DNS per gli strumenti ONTAP Manager, i nodi e l'IP virtuale utilizzato per la comunicazione interna.
- Distribuire l'OVA sul server di gestione vCenter.
- "[Registrare il dominio di gestione vCenter](#)"con ONTAP Tools Manager.
- "[Aggiungere il backend di archiviazione](#)"utilizzando l'interfaccia utente di vSphere Client.
- "[Creare un datastore supplementare](#)"(includerne uno per il registro dei contenuti).
- Creare il registro dei contenuti se si pianifica una distribuzione HA.
- "[Abilita HA](#)"nel gestore degli strumenti ONTAP .

- b. Distribuisci il plug-in SnapCenter

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

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

Convergere i componenti esistenti in VCF 9

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

Prerequisiti

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

Passi

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

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

Aggiorna un ambiente VCF esistente a VCF 9

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

Prerequisiti

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

Passi

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

Implementazione del Disaster Recovery con NetApp Disaster Recovery

Soluzione di disaster recovery VCF per datastore NFS con NetApp SnapMirror e NetApp Disaster Recovery

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

Per ulteriori informazioni, vedere quanto segue "[Documentazione NetApp Disaster Recovery](#)" .

Questa sezione descrive la configurazione di NetApp Disaster Recovery per stabilire il DR per le macchine virtuali VMware locali.

La configurazione include:

- Creazione di un account NetApp Console e distribuzione di un agente.
- Aggiunta di array ONTAP alla NetApp Console sui sistemi in gestione per facilitare la comunicazione tra VMware vCenter e lo storage ONTAP .
- Configurazione della replica tra siti tramite SnapMirror.
- Impostazione e test di un piano di ripristino per convalidare la prontezza al failover.

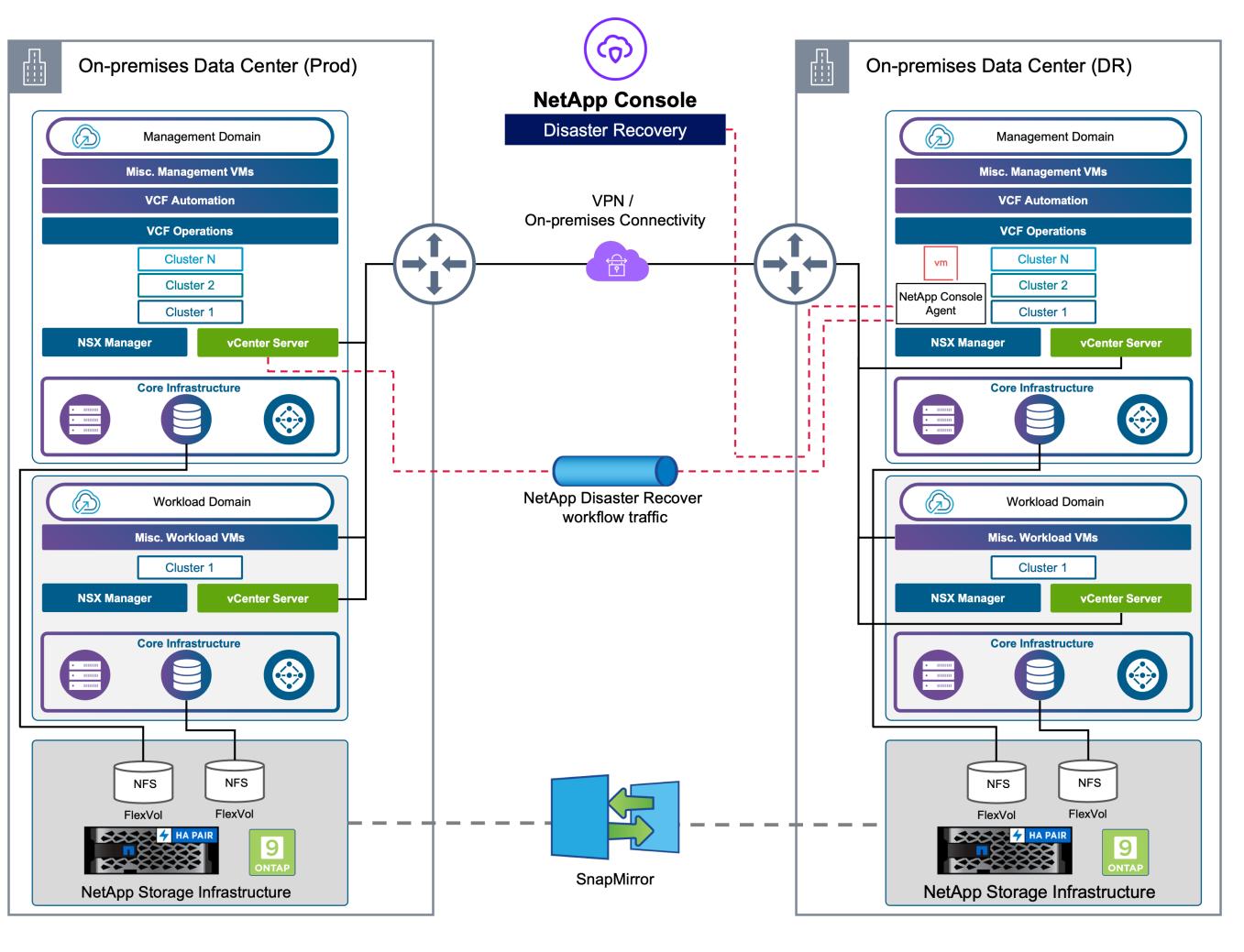
NetApp Disaster Recovery, integrato nella NetApp Console, consente alle organizzazioni di individuare senza

problemi i propri sistemi di storage VMware vCenter e ONTAP in sede. Una volta individuate, le risorse possono essere definite dagli amministratori, creare piani di disaster recovery, associarle alle risorse appropriate e avviare o testare le operazioni di failover e fallback. NetApp SnapMirror fornisce un'efficiente replica a livello di blocco, garantendo che il sito DR rimanga sincronizzato con l'ambiente di produzione tramite aggiornamenti incrementali. Ciò consente un Recovery Point Objective (RPO) di appena cinque minuti.

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

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

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



Iniziare

Per iniziare a utilizzare NetApp Disaster Recovery, utilizzare NetApp Console e quindi accedere al servizio.

1. Accedi alla NetApp Console.
2. Dal menu di navigazione a sinistra della NetApp Console , selezionare Protezione > Disaster Recovery.
3. Viene visualizzata la dashboard NetApp Disaster Recovery .

The screenshot shows the NetApp Console interface. On the left, there's a navigation sidebar with icons for Home, Storage, Protection (which is selected and highlighted with a red box), Governance, Health, Workloads, Mobility, and Administration. The main content area has several sections: 'Backup and Recovery' (implement a complete data protection strategy for all ONTAP workloads), 'Disaster Recovery' (execute a complete disaster protection solution for your VMware workloads, which is also highlighted with a red box), 'Replication' (replicate data for backup, disaster recovery, and migration between on-premises and cloud ONTAP systems), 'Ransomware Resilience' (implement robust ransomware defense at the storage layer to protect data and automate workflows), and a summary of storage capacity: 12.6 GiB Used Capacity and 197.61 GiB Available. To the right, there's a 'System Manager' panel showing 'ONTAP version 9.16.1P1' and 'View release notes', and an 'Information' panel displaying details like 'On-Premises ONTAP', 'Cluster Management IP: 192.168.0.101', 'Serial Number: 70', 'System ID: 4053517501', and 'Replication Licenses: snapmirror, snapvault'.

Prima di configurare il piano di disaster recovery, assicurarsi di quanto segue "[prerequisiti](#)" sono soddisfatte:

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

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

Nota: NetApp consiglia di distribuire l'agente Console nel sito di destinazione o in un terzo sito, in modo che l'agente possa comunicare tramite la rete con le risorse di origine e di destinazione.

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

Configurazione NetApp Disaster Recovery

Il primo passo nella preparazione al disaster recovery è individuare e aggiungere le risorse di origine vCenter e storage a NetApp Disaster Recovery.

Aprire NetApp Console e selezionare Protezione > Disaster Recovery dal menu di navigazione a sinistra. Selezionare Siti e quindi scegliere Aggiungi. Inserisci un nome per il nuovo sito di origine e le sue posizioni. Ripetere il passaggio per aggiungere il sito e la posizione di destinazione.

Add site

A site is a collection of vCenter servers, either on-premises or in the cloud.

Site

Location

Add **Cancel**

Aggiungere le seguenti piattaforme:

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

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

Configurazione della replicazione dello storage tra l'array del sito di origine e l'array del sito di destinazione

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

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



Se la relazione SnapMirror è già configurata per il volume tramite CLI o System Manager, NetApp Disaster Recovery rileva la relazione e continua con le restanti operazioni del flusso di lavoro.

Come impostare le relazioni di replica per NetApp Disaster Recovery

Il processo di base per creare la replica SnapMirror rimane lo stesso per qualsiasi applicazione. Il modo più semplice è sfruttare NetApp Disaster Recovery , che automatizzerà il flusso di lavoro di replicazione a condizione che siano soddisfatti i due criteri seguenti: Il processo può essere manuale o automatizzato. Il modo più semplice consiste nell'utilizzare NetApp Disaster Recovery, che automatizza il flusso di lavoro di replica a condizione che vengano soddisfatti i due criteri seguenti:

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

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

Cosa può fare per te NetApp Disaster Recovery ?

Dopo aver aggiunto i siti di origine e di destinazione, NetApp Disaster Recovery esegue automaticamente un'analisi approfondita e visualizza le VM insieme ai metadati associati. NetApp Disaster Recovery rileva inoltre automaticamente le reti e i gruppi di porte utilizzati dalle VM e li popola.

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a sidebar with navigation links: Disaster Recovery, Dashboard, Sites (selected), Replication plans, Resource groups, and Job monitoring. The main area displays 'Sites (2)'. SiteA (IP 192.168.0.31) contains 3 VMs, 3 Datastores, and 0 Resource groups, with an Engineering Agent. SiteB (IP 192.168.0.32) contains 1 VM, 3 Datastores, and 0 Resource groups, also with an Engineering Agent. A top banner indicates a 'Free trial (29 days left) - View details'.

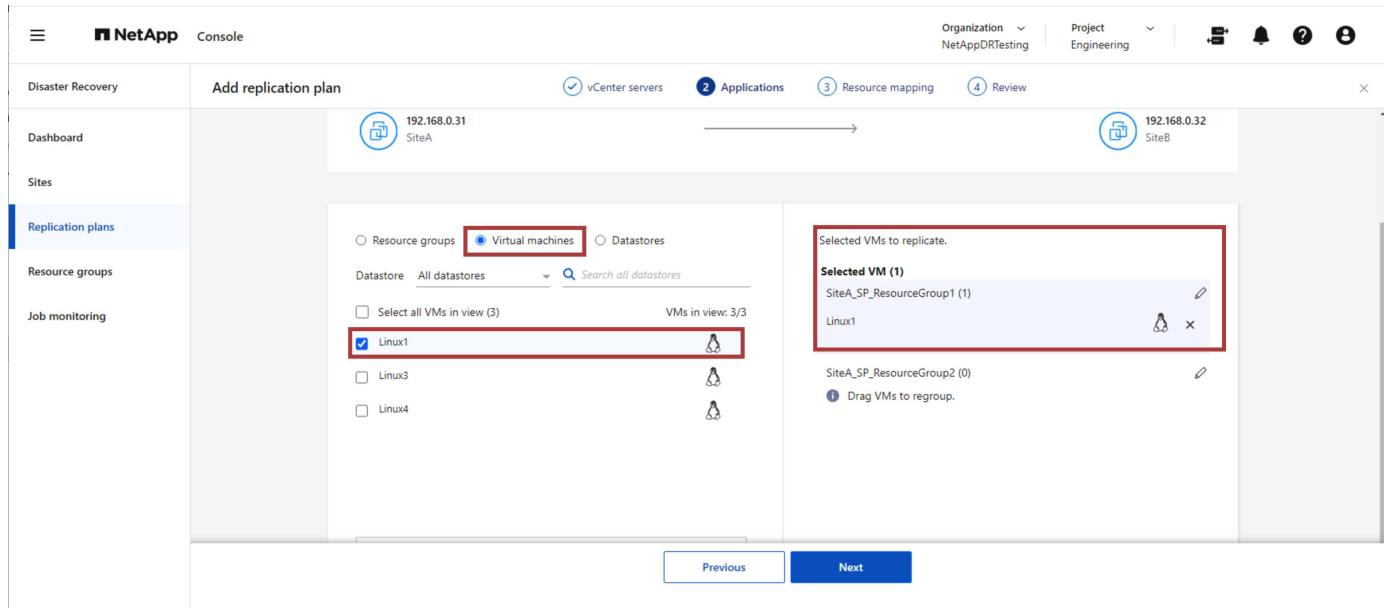
Dopo aver aggiunto i siti, configurare il piano di replica selezionando le piattaforme vCenter di origine e di destinazione e scegliere i gruppi di risorse da includere nel piano, insieme al raggruppamento delle modalità di ripristino e accensione delle applicazioni e alla mappatura di cluster e reti.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

In questa fase, le VM possono essere raggruppate in gruppi di risorse. I gruppi di risorse NetApp Disaster Recovery consentono di raggruppare un set di VM dipendenti in gruppi logici che contengono i relativi ordini di avvio e ritardi di avvio che possono essere eseguiti al momento del ripristino. I gruppi di risorse possono essere creati durante la creazione del piano di replicazione oppure utilizzando la scheda Gruppo di risorse nella barra di navigazione a sinistra.

Per prima cosa, assegna un nome al piano di replica e seleziona il vCenter di origine e il vCenter di destinazione.

The screenshot shows the 'Add replication plan' wizard. Step 1: vCenter servers. It shows a 'Replication plan name' input field containing 'SiteA_SP'. Below it is a 'vCenter servers' section with two host icons. A red box highlights the 'Replication plan name' field and the 'Source vCenter' dropdown, which is set to '192.168.0.31'. The 'Target vCenter' dropdown is set to '192.168.0.32'. The top navigation bar shows the steps: 1 vCenter servers, 2 Applications, 3 Resource mapping, 4 Review.

Il passaggio successivo consiste nello scegliere se creare un piano di replica con gruppi di risorse, macchine virtuali o datastore. Selezionare un gruppo di risorse esistente e, se non viene creato alcun gruppo di risorse, la procedura guidata aiuta a raggruppare le macchine virtuali richieste (in pratica a creare gruppi di risorse funzionali) in base agli obiettivi di ripristino. Ciò aiuta anche a definire la sequenza operativa di come devono essere ripristinate le macchine virtuali delle applicazioni.



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

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

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

Disaster Recovery Add replication plan vCenter servers Applications Resource mapping Review

Dashboard Sites Replication plans Resource groups Job monitoring

Failover mappings Test mappings

Compute resources Mapped

Virtual networks Mapped

Virtual machines Mapped

Datastores Mapped

Previous Next

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

Disaster Recovery Add replication plan vCenter servers Applications Resource mapping Review

Dashboard Sites Replication plans Resource groups Job monitoring

192.168.0.31 SiteA → 192.168.0.32 SiteB

Plan details Failover mapping Virtual machines

	Source	Target
Datastores	nfs1	nfs1 Export policy : default Preferred NFS LIF : 192.168.0.141
Compute resource	Datacenter1 : Cluster1	Datacenter : Datacenter2 Cluster : Cluster2
Virtual networks	VM Network	VM Network

Previous Add plan

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



The screenshot shows the NetApp Disaster Recovery Console interface. On the left sidebar, under the 'Replication plans' section, there is a single entry for 'SiteA_SP'. This entry is highlighted with a red border. The details show it is 'Healthy' and 'Ready', with 'SiteA' as the 'Protected site' and 'SiteB' as the 'Failover site'. The 'Resource groups' column lists 'SiteA_SP_ResourceGroup1'. A 'More' button (three dots) is also visible.

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

The screenshot shows the 'Job monitoring' section of the NetApp Disaster Recovery Console. It displays a summary of 9 jobs completed successfully over the last 12 hours. Below this, a detailed table lists each job with its ID, status (all marked as 'Success'), workload, name, start time, end time, and action taken.

ID	Status	Workload	Name	Start time	End time	Action
018d8b44-c951-4113-a91c-	Success	Compliance	Compliance check for replication plan 'SiteA_SP'	11/04/2025, 06:44:33 PM	11/04/2025, 06:44:36 PM	
d79b74c1-c4ea-4473-bf22-	Success	Compliance	Initialize Compliance of SiteA_SP for every 180 mi...	11/04/2025, 06:44:32 PM	11/04/2025, 06:44:33 PM	
bfc453ac-83f7-4669-a821-9	Success	DRCleanupSecondaryBackups	Initialize DRCleanupSecondaryBackups of Cleanu...	11/04/2025, 06:44:30 PM	11/04/2025, 06:44:31 PM	
b654a09f-6b1a-41d0-9885-	Success	DRReplicationPlan	Replication plan modification for 'SiteA_SP'	11/04/2025, 06:44:28 PM	11/04/2025, 06:44:31 PM	
85e8e7d-67eb-4e48-88ca-	Success	Discovery	Discovery of resources in host 192.168.0.32	11/04/2025, 06:34:37 PM	11/04/2025, 06:34:44 PM	

NetApp Disaster Recovery è costituito dai seguenti flussi di lavoro:

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

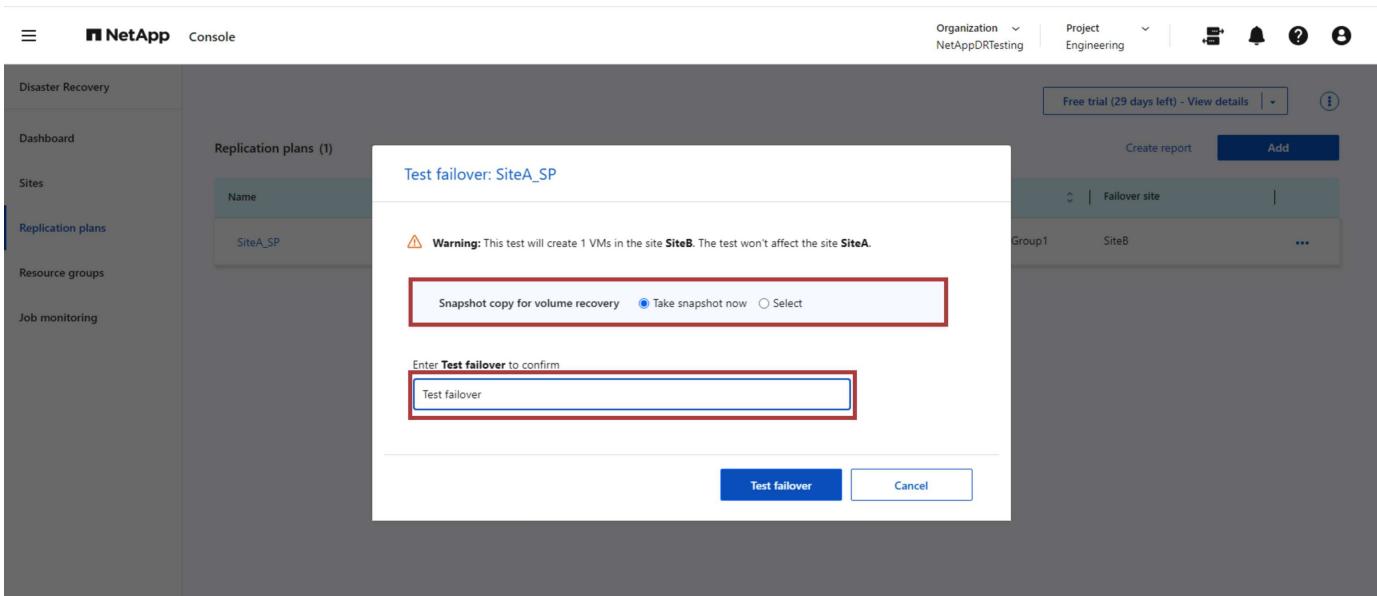
The screenshot shows the NetApp Disaster Recovery console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (which is selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)'. It lists a single plan: SiteA_SP, which is healthy and ready. The protected site is SiteA, and the resource group is SiteA_SP_ResourceGroup1. The failover site is SiteB. A context menu is open over the SiteA_SP row, with the 'Test failover' option highlighted.

Failover di prova

Il failover di prova in NetApp Disaster Recovery è una procedura operativa che consente agli amministratori VMware di convalidare completamente i propri piani di ripristino senza interrompere gli ambienti di produzione.

This screenshot is identical to the one above, showing the NetApp Disaster Recovery console with the 'Replication plans' section selected. It displays a single replication plan named SiteA_SP. The context menu over the plan is open, and the 'Test failover' option is highlighted with a red box.

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



Quando l'amministratore VMware esegue un'operazione di failover di prova, NetApp Disaster Recovery automatizza le seguenti attività:

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

Name	Status	Start time	End time	ID
Test failover for replication plan 'SiteA_SP'	Completed	11/18/2025, 06:09:55 PM	11/18/2025, 06:12:46 PM	87ca8b8c-2c89-4bc1-8271-d16ec1924e0d
^ Prerequisite Checks	Completed	11/18/2025, 06:09:55 PM	11/18/2025, 06:09:56 PM	748c5d89-1d0d-49fd-8fe9-e...
^ Launch ondemand snapshot	Completed	11/18/2025, 06:09:56 PM	11/18/2025, 06:09:57 PM	7aae807a-754e-4521-8471-...
^ Tracking ondemand snapshot	Completed	11/18/2025, 06:09:57 PM	11/18/2025, 06:10:57 PM	1b6510df-3bcf-486c-87a9-c...
^ Create Clone Volume(s)	Completed	11/18/2025, 06:10:58 PM	11/18/2025, 06:11:33 PM	0fc95ee6-aa80-4d77-acdc-3...
^ Datastore Mount	Completed	11/18/2025, 06:11:33 PM	11/18/2025, 06:11:36 PM	3505dc8d-061e-4a79-bc60-...
^ Register Virtual Machine(s)	Completed	11/18/2025, 06:11:36 PM	11/18/2025, 06:11:37 PM	bcf8088c-24ce-4307-acec-8...

Operazione di test di failover di pulizia

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

The screenshot shows the NetApp Disaster Recovery console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (which is selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)' and shows a table with one row. The row details are: Name (SiteA_SP), Compliance status (Healthy), Plan status (Test failover), Protected site (SiteA), Resource groups (SiteA_SP_ResourceGroup1), and Failover site (SiteB). A context menu is open over the SiteA_SP row, listing options such as View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up test failover (which is highlighted with a red box), Fail over, Fail back, Migrate, Edit schedules, and Take snapshot now. At the top right of the main area, there are buttons for Free trial (29 days left) - View details, Create report, and Add.

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

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

Migrazione pianificata e failover

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

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)'. It lists a single plan named 'SiteA_SP' with columns for Name, Compliance status (Healthy), Plan status (Ready), Protected site (SiteA), Resource groups (SiteA_SP_ResourceGroup1), and Failover site (SiteB). A context menu is open over the 'SiteA_SP' row, with 'Test failover' highlighted.

The screenshot shows the 'Failover: SiteA_SP' dialog. It includes a warning message about disrupting client access during failover and another about powered-on source VMs. It has options for 'Snapshot copy for volume recovery' (radio buttons for 'Take snapshot now' and 'Select'). There are also checkboxes for 'Force failover' and 'Skip protection'. A text input field for 'Enter Failover to confirm' contains the word 'Failover'. At the bottom are 'Failover' and 'Cancel' buttons, with 'Failover' highlighted by a red box.

Quando l'amministratore VMware esegue un'operazione di failover, NetApp Disaster Recovery automatizza le seguenti attività:

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

Recent Tasks

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Power On virtual machine	Linux1	Completed	Powering on the new Virtual Machine	DEMO.LOCAL\Administrator	6 ms	11/18/2025, 7:32:46 PM	11/18/2025, 7:32:51 PM	vc2.demo.netapp.com

Rifasamento

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

Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Failed over	SiteA	SiteA_SP_ResourceGroup1	SiteB

Fail back

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



NetApp Disaster Recovery replica (risincronizza) tutte le modifiche sulla macchina virtuale di origine prima di invertire la direzione della replica.

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

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

The screenshot shows the vSphere Client interface for the vCenter server vc2.demo.netapp.com. The left sidebar shows the navigation tree with Datacenter2 and Cluster2 selected. The main pane displays the vCenter Details section, which includes the version (8.0.3), build (24322831), last updated (Dec 19, 2024, 4:46 PM), and scheduled tasks (Last File-Based Backup: Not scheduled). To the right is the Capacity and Usage section, showing resource utilization for CPU, Memory, and Storage.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Remove datastore	nfs1	Completed		DEMO.LOCAL\Administrator	5 ms	11/18/2025, 7:56:12 PM	11/18/2025, 7:56:13 PM	vc2.demo.netapp.com
Unregister virtual machine	Linux1	Completed		DEMO.LOCAL\Administrator	9 ms	11/18/2025, 7:56:12 PM	11/18/2025, 7:56:12 PM	vc2.demo.netapp.com
Initiate guest OS shutdown	Linux1	Completed		DEMO.LOCAL\Administrator	12 ms	11/18/2025, 7:53:14 PM	11/18/2025, 7:53:14 PM	vc2.demo.netapp.com

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

The screenshot shows the vSphere Client interface for the cluster Cluster1 under Datacenter1. The left sidebar shows the navigation tree with Datacenter1 and Cluster1 selected. The main pane displays the Cluster Details section, which includes the total processors (8) and total vMotion migrations (0). To the right is the Capacity and Usage section, showing resource utilization for CPU, Memory, and Storage.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Power On virtual machine	Linux1	Completed	Powering on the new Virtual Machine	DEMO.LOCAL\Administrator	5 ms	11/18/2025, 7:55:07 PM	11/18/2025, 7:55:08 PM	vc1.demo.netapp.com
Reconfigure virtual machine	Linux1	Completed		DEMO.LOCAL\Administrator	7 ms	11/18/2025, 7:55:05 PM	11/18/2025, 7:55:06 PM	vc1.demo.netapp.com

Per maggiori dettagli sull'accesso e la configurazione NetApp Disaster Recovery, vedere ["Scopri di più su NetApp Disaster Recovery per VMware"](#).

Monitoraggio e dashboard

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

Last updated: November 18, 2025, 8:08 PM

Jobs (38)

ID	Status	Workload	Name	Start time	End time	Action
da2efd87-674c-4013-b00a-...	Success	Reconciliation	Backup reconciliation for plan SiteA_SP	11/18/2025, 07:59:25 PM	11/18/2025, 07:59:28 PM	
34d261a2-371a-4a82-9f61-...	Success	Discovery	Discovery of resources in host 192.168.0.31	11/18/2025, 07:58:25 PM	11/18/2025, 07:58:32 PM	
569fb8ea-fcbd-44b8-8f40-4...	Success	Discovery	Discovery of resources in host 192.168.0.32	11/18/2025, 07:58:25 PM	11/18/2025, 07:58:31 PM	
b68e14b0-e11d-4656-bbdc...	Success	DRBackupRetention	Backup retention for plan SiteA_SP	11/18/2025, 07:54:20 PM	11/18/2025, 07:54:21 PM	



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

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

Activity (Last 12 hours)

- Backup reconciliation for plan SiteA_SP 14 m ago
- Discovery of resources in host 192.168.0.31 15 m ago
- Discovery of resources in host 192.168.0.32 15 m ago
- Backup retention for plan SiteA_SP 20 m ago
- Backup for replication plan 'SiteA_SP' 20 m ago

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

Convertire i cluster vSphere esistenti in VCF

Scopri come convertire un ambiente vSphere con datastore esistenti in un dominio di gestione VCF

La conversione di un ambiente vSphere con datastore Fibre Channel o NFS esistenti su ONTAP implica l'integrazione dell'infrastruttura attuale in una moderna architettura cloud privata.

Panoramica della soluzione

Questa soluzione dimostra come i datastore FC o NFS esistenti in vSphere diventano storage principale quando il cluster viene convertito in un dominio di gestione VCF.

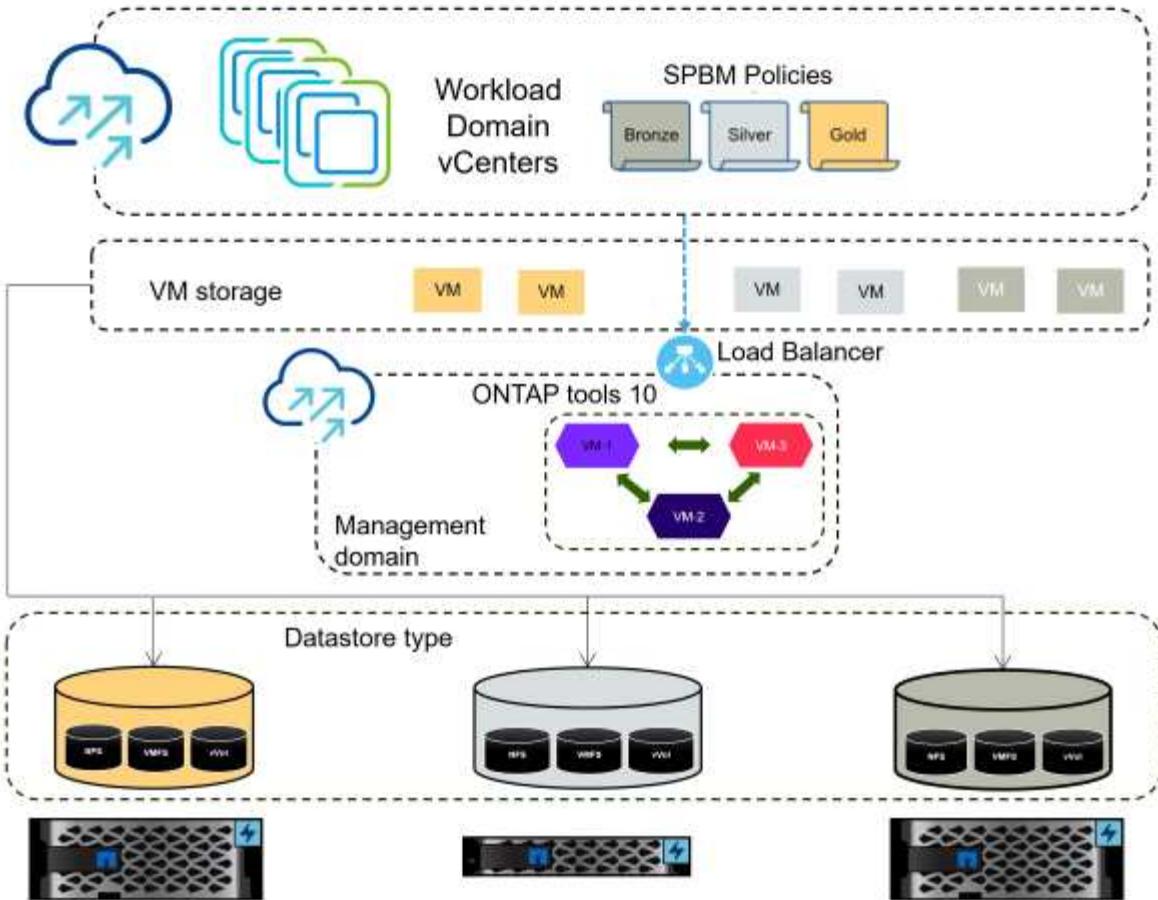
Questo processo trae vantaggio dalla robustezza e dalla flessibilità dell'archiviazione ONTAP per garantire un accesso e una gestione dei dati senza interruzioni. Dopo aver stabilito un dominio di gestione VCF tramite il processo di conversione, gli amministratori possono importare in modo efficiente altri ambienti vSphere, compresi quelli che utilizzano sia datastore FC che NFS, nell'ecosistema VCF.

Questa integrazione non solo migliora l'utilizzo delle risorse, ma semplifica anche la gestione dell'infrastruttura cloud privata, garantendo una transizione fluida con un'interruzione minima dei carichi di lavoro esistenti.

Panoramica dell'architettura

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

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



Soluzioni supportate per la conversione di un ambiente vSphere

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

- ["Convertire un'istanza vCenter nel dominio di gestione VCF \(datastore NFS\)"](#)
- ["Convertire l'istanza vCenter nel dominio di gestione VCF \(datastore FC\)"](#)

Informazioni aggiuntive

- Per demo video di queste soluzioni, fare riferimento a ["Provisioning del datastore VMware con ONTAP"](#) .
- Per una panoramica del processo di conversione, fare riferimento a ["Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation"](#) .
- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a ["Documentazione ONTAP 9"](#) .
- Per informazioni sulla configurazione di VCF, fare riferimento a ["Documentazione di VMware Cloud Foundation"](#) .
- Per informazioni sullo storage supportato e altre considerazioni sulla conversione o l'importazione di vSphere in VCF 5.2, fare riferimento a ["Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation"](#) .

Flusso di lavoro di distribuzione per la conversione delle istanze del server vCenter in domini di gestione VCF con datastore NFS

Convertire un cluster vSphere 8 esistente con datastore NFS NetApp ONTAP in un dominio di gestione VMware Cloud Foundation. Esaminerai i requisiti di configurazione, implementerai gli strumenti ONTAP e fornirai datastore NFS, e utilizzerai lo strumento di importazione VCF per convalidare e convertire il cluster.

Per una panoramica del processo di conversione, fare riferimento alla documentazione VMware: "[Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation](#)" .

1

"Rivedere i requisiti di configurazione"

Esaminare i requisiti chiave per la conversione delle istanze del server vCenter in domini di gestione VCF utilizzando datastore NFS.

2

"Distribuisci gli strumenti ONTAP e fornisci un datastore NFS"

Distribuisci gli ONTAP tools for VMware vSphere e fornisci un datastore NFS.

3

"Convertire il cluster vSphere in dominio di gestione VCF"

Utilizzare lo strumento di importazione VCF per convalidare e convertire vSphere 8 nel dominio di gestione VCF.

Flusso di lavoro di distribuzione per la conversione delle istanze del server vCenter in domini di gestione VCF con datastore Fibre Channel

Converti un cluster vSphere 8 esistente con datastore Fibre Channel (FC) NetApp ONTAP in un dominio di gestione VMware Cloud Foundation. Esaminerai i requisiti di configurazione, implementerai gli strumenti ONTAP e fornirai gli archivi dati FC, e utilizzerai lo strumento di importazione VCF per convalidare e convertire il cluster.

Per una panoramica del processo di conversione, fare riferimento alla documentazione VMware: "[Convertire un ambiente vSphere in un dominio di gestione o importare un ambiente vSphere come dominio di carico di lavoro VI in VMware Cloud Foundation](#)" .

1

"Rivedere i requisiti di configurazione"

Esaminare i requisiti chiave per la conversione delle istanze del server vCenter in domini di gestione VCF utilizzando datastore FC.

2

"Distribuisci gli strumenti ONTAP e fornisci un datastore FC"

Distribuisci gli ONTAP tools for VMware vSphere e fornisci un datastore FC.

3

"Convertire il cluster vSphere in dominio di gestione VCF"

Utilizzare lo strumento di importazione VCF per convalidare e convertire il cluster vSphere 8 nel dominio di gestione VCF.

Fornire VCF con storage principale

Fornire un ambiente VCF con ONTAP come soluzione di archiviazione principale

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

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

- ["Dominio di gestione con FC"](#)
- ["Dominio di gestione con NFS"](#)
- ["Dominio del carico di lavoro dell'infrastruttura virtuale con FC"](#)
- ["Dominio del carico di lavoro dell'infrastruttura virtuale con NFS"](#)

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

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

Introduzione

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

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



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



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

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

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

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#)" centro.

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

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

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

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

Dominio di gestione - Cluster aggiuntivo

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

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

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#)" centro.

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

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

In questo caso d'uso descriviamo la procedura per utilizzare un datastore NFS esistente su ONTAP come storage primario per i domini di gestione VMware Cloud Foundation

(VCF). Questa procedura riassume i componenti richiesti, i passaggi di configurazione e il processo di distribuzione.

Introduzione

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

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

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

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

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

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

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

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

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

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

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

Dominio di gestione - Cluster aggiuntivo

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

- Avere un cluster aggiuntivo nell'ambiente vSphere e utilizzare lo strumento di importazione brownfield VCF per convertire l'ambiente vSphere nel dominio di gestione. "[ONTAP tools for VMware vSphere](#)" "[Gestore di sistema o API ONTAP](#)" può essere utilizzato per distribuire il datastore NFS nel cluster vSphere.
- Utilizzare l'API SDDC per distribuire cluster aggiuntivi. Gli host vSphere devono avere configurato il datastore NFS. Utilizzo "[Gestore di sistema o API ONTAP](#)" per distribuire LUN sugli host vSphere.
- Utilizzare l'interfaccia utente di SDDC Manager per distribuire cluster aggiuntivi. Questa opzione, tuttavia, crea solo datastore vSAN con versioni precedenti alla 5.2.x.

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

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

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

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

Vantaggi del Fibre Channel

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

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

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

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

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

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

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

sistema di archiviazione ONTAP .

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



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

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

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



NetApp consiglia il multipath per le LUN FC.

Fasi di distribuzione

Dominio di gestione - Cluster predefinito

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

Dominio di gestione - Cluster aggiuntivo

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

Dominio del carico di lavoro VI - Cluster predefinito

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

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

Dominio del carico di lavoro VI - Cluster aggiuntivo

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

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

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

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

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

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

Vantaggi di NFS

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

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

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

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

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

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

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



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

Prerequisiti

In questo scenario vengono utilizzati i seguenti componenti e configurazioni:

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

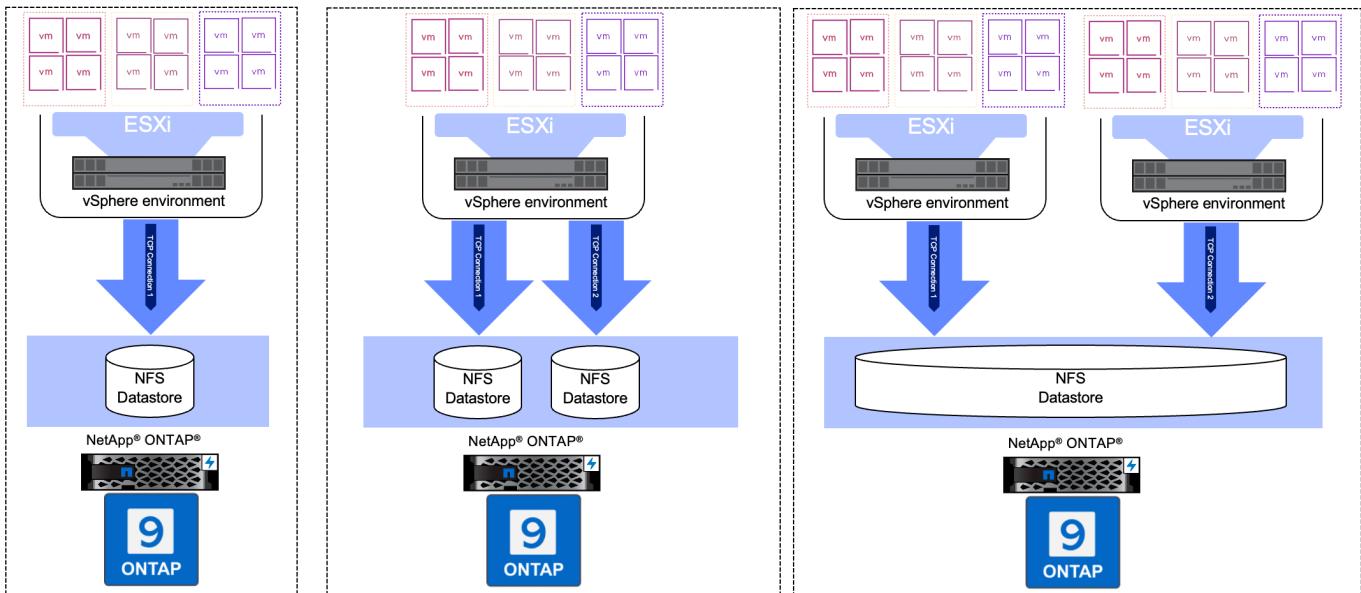


Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario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

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#) centro.

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

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



Fasi di distribuzione

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

Verifica della rete per ONTAP SVM

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

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

The screenshot shows the ONTAP System Manager interface. On the left, the navigation pane is visible with sections like DASHBOARD, INSIGHTS, STORAGE (Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas), Storage VMs (selected), Tiers, NETWORK (selected), and EVENTS & JOBS. The main panel is titled 'Storage VMs' and shows a list of SVMs: EHC_iSCSI, EHC_NFS (selected), HMC_187, HMC_3510, HMC_iSCSI_3510, infra_svm_a300, JS_EHC_iSCSI, OTVtest, svm0, Temp_3510_N1, and zoneb. To the right, there's a detailed view for the selected SVM ('EHC_NFS'). Under 'OVERVIEW', there's a section for 'NETWORK IP INTERFACES' with a sub-section for 'NFS'. This section lists several IP addresses: 172.21.253.117, 172.21.253.118, 172.21.253.116, 172.21.253.112, 172.21.253.113, 172.21.118.163, and 172.21.118.164. A blue callout box highlights this list.

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

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

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

```
vmkping <IP Address>
```



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

Crea criteri di esportazione per la condivisione del volume NFS

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

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

The screenshot shows the ONTAP System Manager interface. On the left, the navigation sidebar is open, showing categories like DASHBOARD, INSIGHTS, STORAGE, and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main content area is titled 'Storage VMs' and shows a list of VMs: EHC_ISCSI, EHC_NFS (selected), HMC_187, HMC_3510, HMC_ISCSI_3510, infra_svm_a300, JS_EHC_ISCSI, OTVtest, svm0, and Temp_3510_N1. To the right of the list, there are tabs for Overview, Settings (which is selected), SnapMirror (Local or Remote), and File System. Below the tabs, a section titled 'Pinned' lists 'Export Policies': default (41 Rules), JetStream_NFS_v02 (0.0.0.0 for Any), and JetStream_NFS_v03 (0.0.0.0 for Any). A hand cursor is hovering over the 'Add Rule' button (a blue square with a white plus sign) in the 'Export Policies' section.

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

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

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) (i)	<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



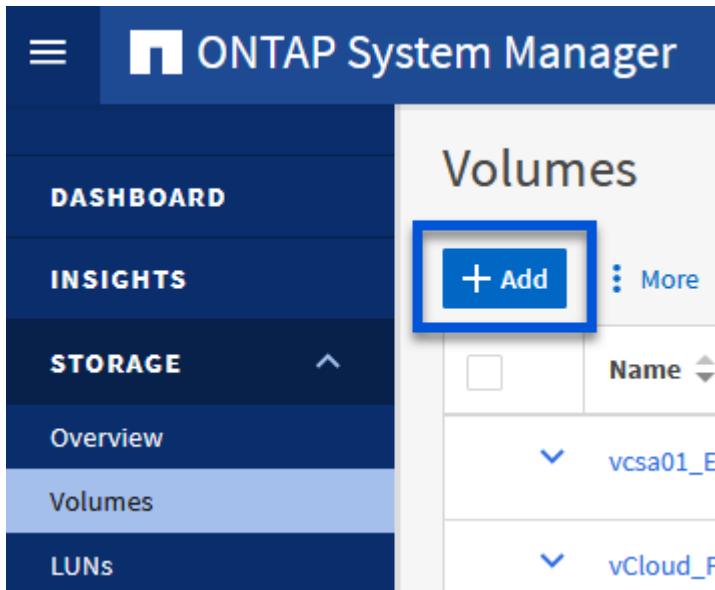
Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario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

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

Crea volume NFS

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

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



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

Add Volume

X

NAME

CAPACITY



STORAGE VM



Export via NFS

[More Options](#)

[Cancel](#)

[Save](#)

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

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, 172.21.2

+



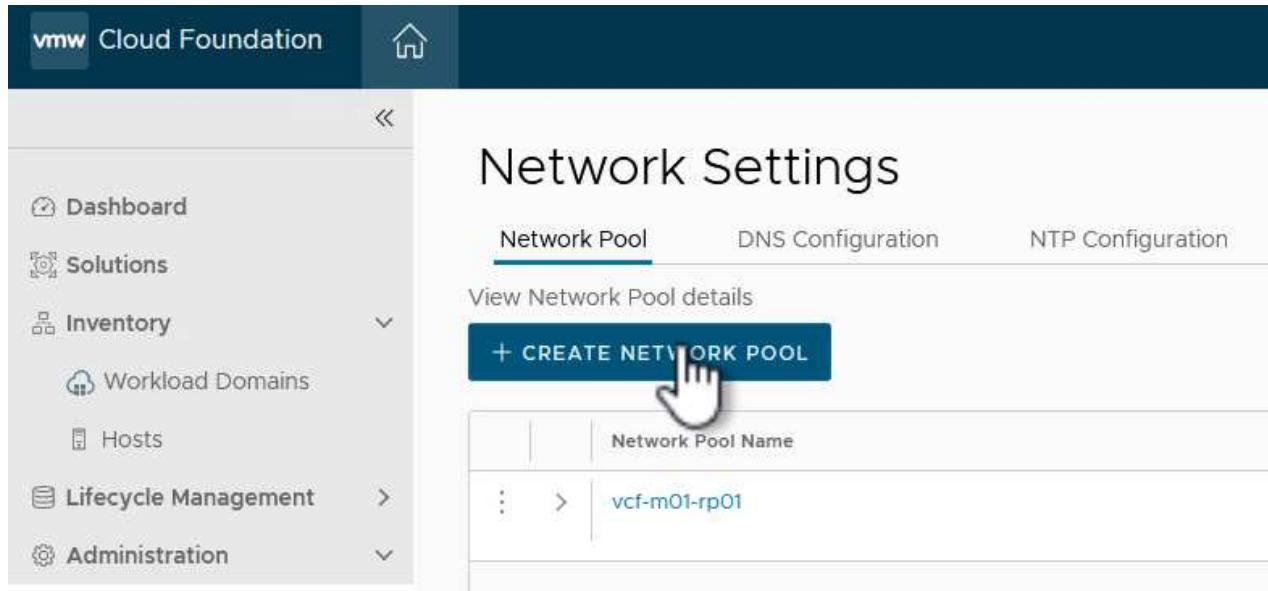
Durante la distribuzione di un dominio di carico di lavoro VI, VCF convalida la connettività al server NFS. Questa operazione viene eseguita utilizzando l'adattatore di gestione sugli host ESXi prima che venga aggiunto qualsiasi adattatore vmkernel aggiuntivo con l'indirizzo IP NFS. Pertanto, è necessario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

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

Crea pool di rete in SDDC Manager

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

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



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

The screenshot shows the 'Network Settings' section of the VMware Cloud Foundation interface. On the left, a sidebar lists various management categories like Dashboard, Solutions, Inventory, Workload Domains, Hosts, Lifecycle Management, Administration, and more. The 'Network Settings' category is currently selected.

The main area is titled 'Create Network Pool'. It includes tabs for 'Network Pool' (selected), 'DNS Configuration', and 'NTP Configuration'. A note at the top says: 'Ensure that all required networks are selected based on their usage for workload domains.'

The 'Network Pool Name' is set to 'NFS_NP01'. Under 'Network Type', 'VSAN' is unselected, while 'NFS', 'iSCSI', and 'vMotion' are selected. Below this are two sections: 'NFS Network Information' and 'vMotion Network Information', each containing fields for VLAN ID, MTU, Network, Subnet Mask, and Default Gateway.

Below these sections is a table for 'Included IP Address Ranges'. It shows two ranges: '172.21.118.145 To 172.21.118.148' and '172.21.167.121 To 172.21.167.124'. There are 'REMOVE' and 'ADD' buttons for each row.

At the bottom are 'CANCEL' and 'SAVE' buttons.

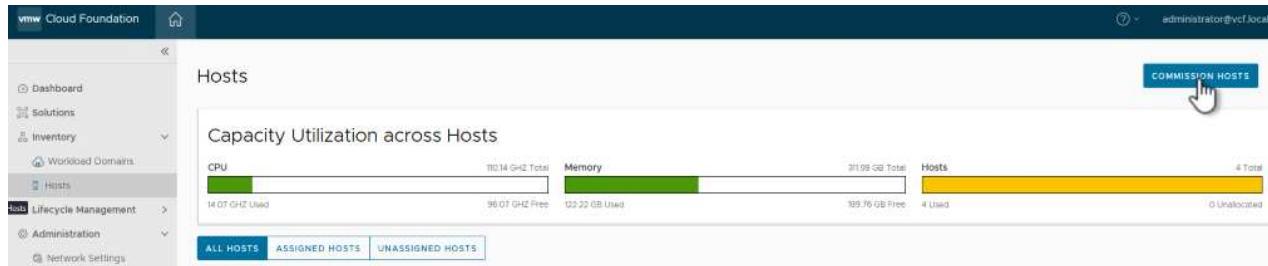
3. Fare clic sul pulsante **Salva** per completare la creazione del pool di rete.

Host della Commissione

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

Per maggiori informazioni vedere "[Host della Commissione](#)" nella Guida all'amministrazione VCF.

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



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

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

Commission Hosts

1 Host Addition and Validation

2 Review

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: vcf-wkld-esx02.sddc.netapp.com

Storage Type: vSAN NFS VMFS on FC vVol

Network Pool Name:

User Name: root

Password:

ADD 

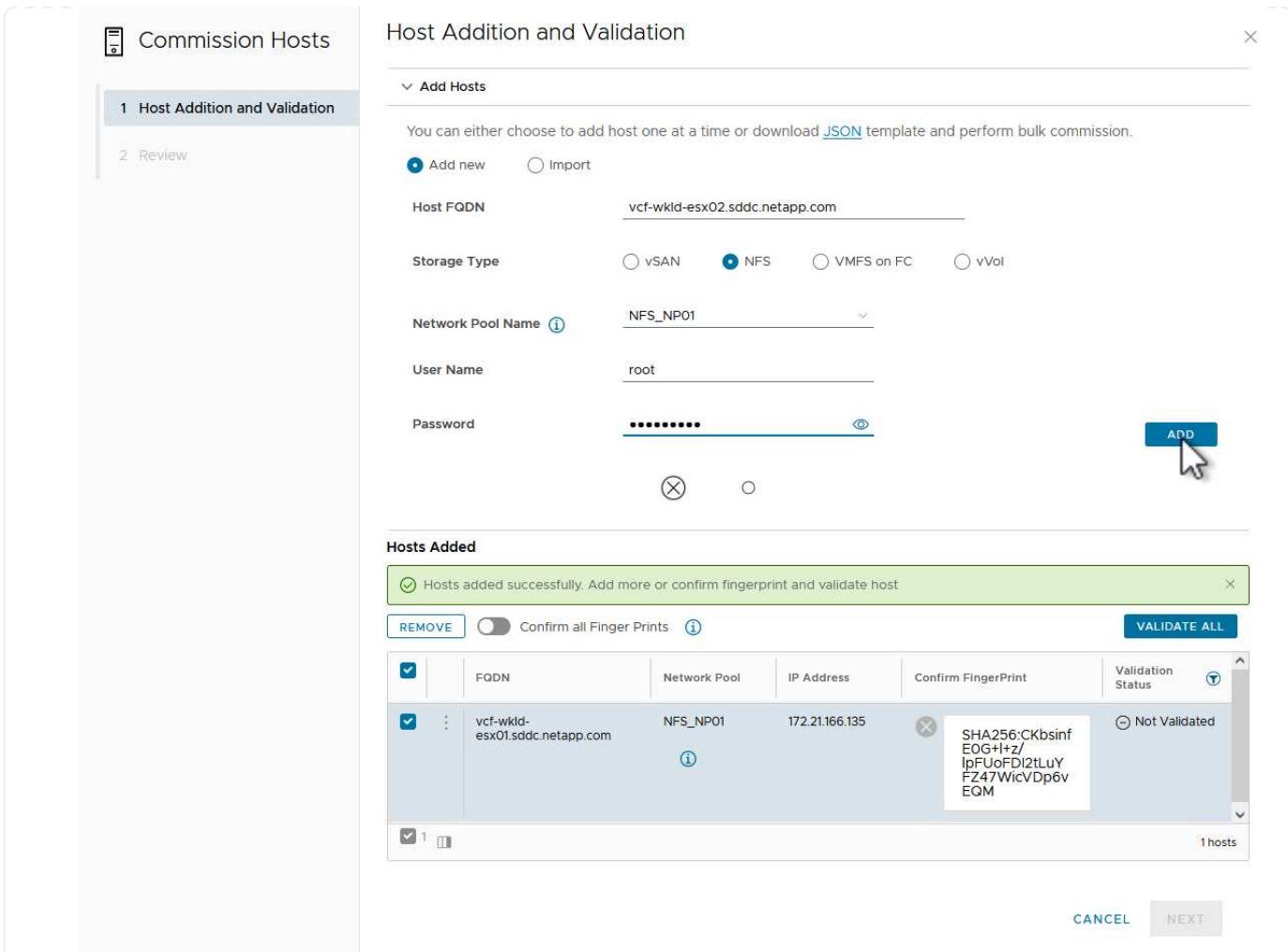
Hosts Added

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

<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		 Not Validated

SHA256:CKbsinfEOG+Hz/lpFUoFDl2tLuYFZ47WicVDp6vEQM

CANCEL **NEXT**



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

Hosts Added

Host Validated Successfully.

[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-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2IOwZDPFH+z0	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	SHA256:AMhyR60OpTQIYYq0DjhqVbj/M/GvrQaqUy7Ce+M4IWY	Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	SHA256:CKbsinfEOG+l+z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	Valid

[CANCEL](#)

[NEXT](#)



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

Commission Hosts

1 Host Addition and Validation

2 Review

Review

Skip failed hosts during commissioning On

▼ Validated Host(s)

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

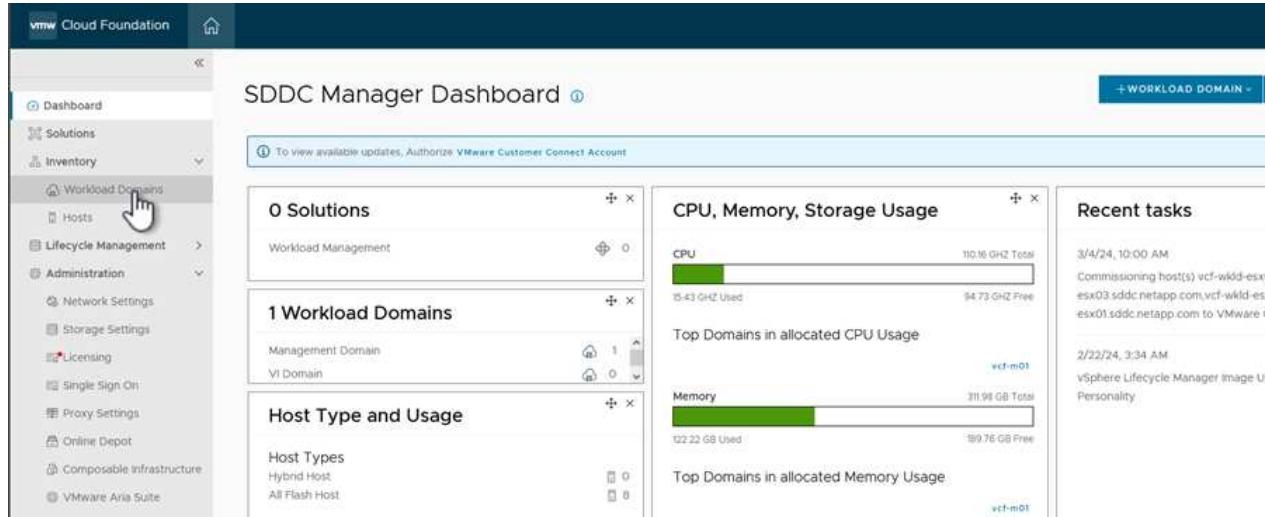
CANCEL BACK COMMISSION 

Distribuisci il dominio del carico di lavoro VI

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

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

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



The screenshot shows the SDDC Manager Dashboard. On the left, there is a sidebar with various navigation options. A hand cursor is hovering over the 'Workload Domains' section under the 'Hosts' category. The main area displays three cards: '0 Solutions', '1 Workload Domains', and 'Host Type and Usage'. The '1 Workload Domains' card shows one Management Domain and one VI Domain. To the right, there are two charts: 'CPU, Memory, Storage Usage' and 'Recent tasks'. The 'CPU' chart shows 10.16 GHz Total, 15.43 GHz Used, and 84.73 GHz Free. The 'Memory' chart shows 311.98 GB Total, 122.22 GB Used, and 189.76 GB Free. The 'Recent tasks' section lists two entries: 'Commissioning host(s) vcf-wld0-esx0 esx03.sddc.netapp.com, vcf-wld0-esx01.sddc.netapp.com to VMware CI' and 'vSphere Lifecycle Manager Image Up Personality'.

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

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

VI Configuration

The screenshot shows the 'VI Configuration' wizard with the following steps visible:

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

A '+' sign is located at the bottom left of the list.

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

The screenshot shows the 'NFS Storage' configuration screen with the following details:

VI Configuration		NFS Storage
1 General Info	NFS Share Details	
2 Cluster	Datastore Name <small>(i)</small>	VCF_WKLD_01
3 Compute	Folder <small>(i)</small>	/VCF_WKLD_01
4 Networking	NFS Server IP Address <small>(i)</small>	172.21.118.163
5 Host Selection		
6 NFS Storage		

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

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

Installare il plug-in NetApp NFS per VMware VAAI

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

Per istruzioni dettagliate sulla distribuzione del plug-in NetApp NFS per VMware VAAI, seguire le istruzioni riportate in "[Installare il plug-in NetApp NFS per VMware VAAI](#)" .

Demo video per questa soluzione

[Datastore NFS come storage principale per domini di carichi di lavoro VCF](#)

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

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

Espandi VCF con spazio di archiviazione supplementare

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

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

Gli ONTAP tools for VMware vSphere forniscono una soluzione efficiente per questa espansione, integrando perfettamente lo storage NetApp nell'ambiente VCF.

Gli strumenti ONTAP semplificano la configurazione e la gestione degli archivi dati, consentendo agli amministratori di eseguire il provisioning e gestire lo storage direttamente da vSphere Client. Le funzionalità avanzate di ONTAP, come snapshot, clonazione e protezione dei dati, migliorano le prestazioni di archiviazione, l'efficienza e la scalabilità nell'ambiente VCF.

Protocolli supportati per l'espansione dello storage

Gli ambienti VCF possono essere ampliati utilizzando diversi protocolli di archiviazione, ognuno dei quali offre vantaggi e casi d'uso unici.

È possibile utilizzare i seguenti protocolli per espandere lo storage nei domini di gestione VCF e nei domini di carico di lavoro VI. Scegli l'opzione migliore per il tuo ambiente per integrare senza problemi lo storage supplementare nella tua distribuzione VCF.

iSCSI

Protocollo basato su blocchi che utilizza reti Ethernet standard. Ideale per ambienti che richiedono elevate prestazioni, flessibilità e scalabilità a costi contenuti.

iSCSI è ampiamente utilizzato per i datastore VMFS e supporta funzionalità ONTAP avanzate, come snapshot e clonazione.

- **Prestazioni elevate:** offre prestazioni elevate per garantire velocità di trasferimento dati rapide ed efficienti e bassa latenza. Ideale per applicazioni aziendali esigenti e ambienti virtualizzati.
- **Facilità di gestione:** semplifica la gestione dell'archiviazione utilizzando strumenti e protocolli basati su IP noti.
- **Conveniente:** utilizza l'infrastruttura Ethernet esistente, riducendo la necessità di hardware specializzato e consentendo alle organizzazioni di ottenere soluzioni di archiviazione affidabili e scalabili.

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

Canale in fibra (FC)

Protocollo ad alta velocità e bassa latenza che utilizza reti FC dedicate. FC è preferibile per carichi di lavoro critici che richiedono affidabilità, larghezza di banda dedicata e correzione degli errori affidabile. Viene comunemente utilizzato per gli archivi dati VMFS in ambienti aziendali.

- **Prestazioni elevate:** FC garantisce velocità di trasferimento dati elevate, rendendolo ideale per applicazioni che richiedono un accesso rapido e affidabile a grandi quantità di dati.
- **Bassa latenza:** Latenza molto bassa, fondamentale per le applicazioni che richiedono prestazioni elevate, come database e ambienti virtualizzati.

- **Affidabilità:** le reti FC sono note per la loro robustezza e affidabilità, con funzionalità quali ridondanza integrata e correzione degli errori.
- **Larghezza di banda dedicata:** FC fornisce larghezza di banda dedicata per il traffico di archiviazione, riducendo il rischio di congestione della rete.

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

NFS (sistema di file di rete)

Protocollo basato su file che consente una facile condivisione e gestione dei file tra host. NFS è semplice da configurare e scalabile in modo efficiente, il che lo rende adatto a carichi di lavoro virtualizzati e ambienti che richiedono un accesso flessibile ai file.

Gli archivi dati NFS sono supportati da ONTAP e vSphere sia per i domini di gestione che per quelli dei carichi di lavoro.

- **Semplicità e facilità d'uso:** NFS è semplice da configurare e gestire, il che lo rende una scelta eccellente per gli ambienti che richiedono una condivisione dei file rapida e semplice.
- **Scalabilità:** l'architettura di ONTAP consente a NFS di scalare in modo efficiente, supportando le crescenti esigenze di dati senza modifiche significative all'infrastruttura.
- **Flessibilità:** NFS supporta un'ampia gamma di applicazioni e carichi di lavoro, rendendolo versatile per vari casi d'uso, inclusi gli ambienti virtualizzati.

Per ulteriori informazioni, fare riferimento al "["Guida di riferimento NFS v3 per vSphere 8"](#)" .

NVMe/TCP

Protocollo moderno che garantisce elevate prestazioni e bassa latenza su reti Ethernet standard utilizzando TCP/IP. NVMe/TCP è ideale per applicazioni complesse e operazioni di dati su larga scala, poiché garantisce scalabilità ed efficienza dei costi senza richiedere hardware specializzato.

- **Prestazioni elevate:** offre prestazioni eccezionali con bassa latenza e velocità di trasferimento dati elevate. Ciò è fondamentale per le applicazioni più esigenti e le operazioni sui dati su larga scala.
- **Scalabilità:** supporta configurazioni scalabili, consentendo agli amministratori IT di espandere la propria infrastruttura senza problemi man mano che aumentano i requisiti dei dati.
- **Conveniente:** funziona tramite switch Ethernet standard ed è encapsulato all'interno di datagrammi TCP. Non sono richieste attrezzature speciali per l'implementazione.

Per maggiori informazioni sui vantaggi di NVMe, fare riferimento a "["Che cos'è NVME?"](#)" .

Casi d'uso per l'aggiunta di spazio di archiviazione supplementare

I seguenti casi d'uso dimostrano come aggiungere storage supplementare ai domini di gestione VCF e ai domini di carico di lavoro dell'infrastruttura virtuale (VI) utilizzando protocolli e configurazioni diversi.

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

Espandi i domini di gestione con iSCSI

Flusso di lavoro di distribuzione per l'aggiunta di un datastore iSCSI come storage supplementare in un dominio di gestione VCF

Inizia aggiungendo un datastore iSCSI come storage supplementare per un dominio di gestione VMware Cloud Foundation (VCF). Imposterai una Storage Virtual Machine (SVM) con interfacce logiche (LIF) per iSCSI, configurerai la rete iSCSI sugli host ESXi, implementerai gli ONTAP tools for VMware vSphere e creerai un datastore VMFS.

1

"Esaminare i requisiti di distribuzione"

Esaminare i requisiti per l'aggiunta di datastore iSCSI come storage supplementare al dominio di gestione VCF.

2

"Creare SVM e LIF"

Creare una SVM con più LIF per il traffico iSCSI.

3

"Configurare la rete"

Configurare la rete per iSCSI sugli host ESXi.

4

"Configurare l'archiviazione"

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

Requisiti di distribuzione per l'aggiunta di un datastore iSCSI a un dominio di gestione VCF

Esaminare i requisiti per l'aggiunta di datastore iSCSI come storage supplementare a un dominio di gestione VMware Cloud Foundation (VCF).

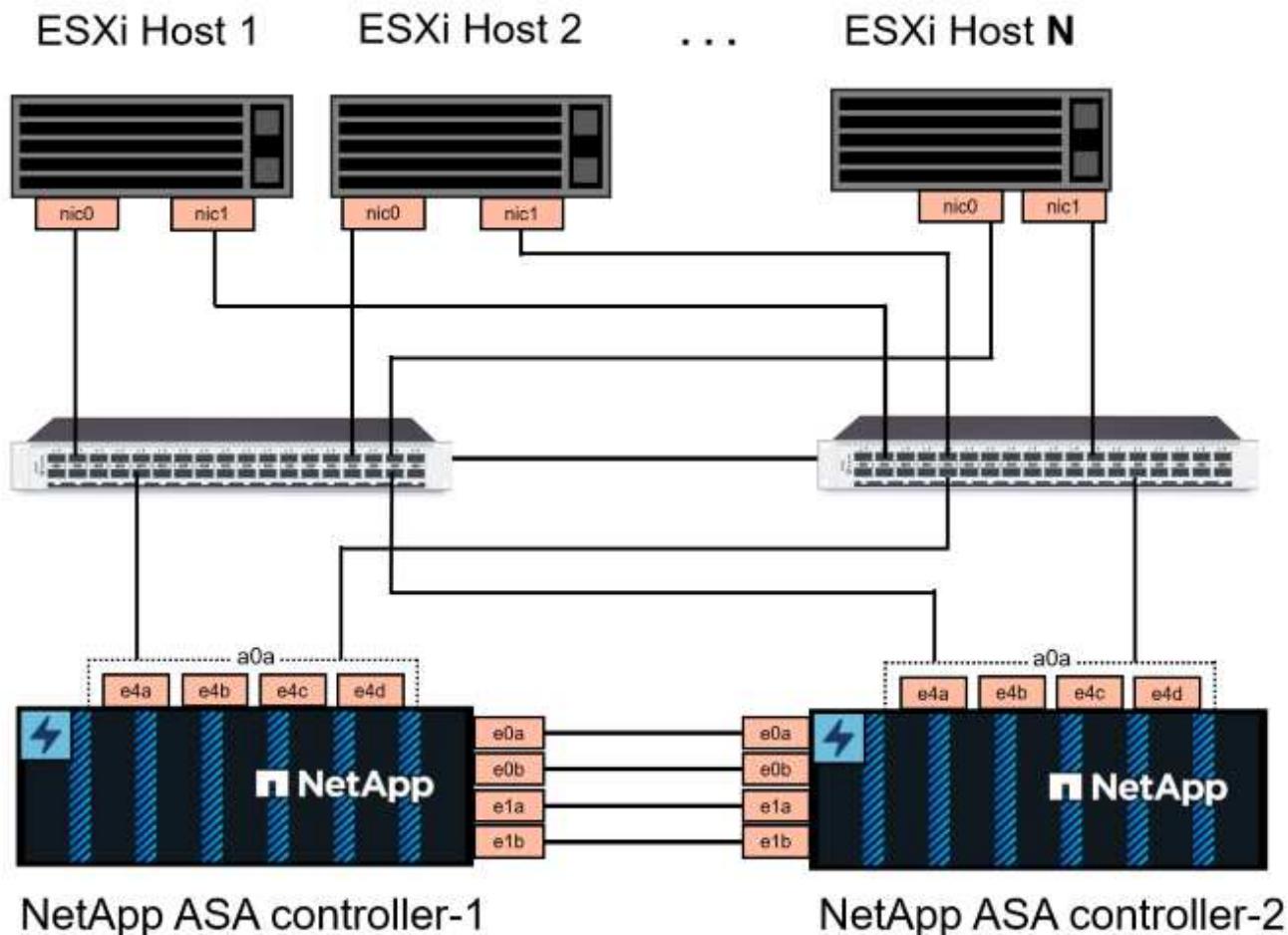
Requisiti infrastrutturali

Assicurarsi che i seguenti componenti e configurazioni siano presenti.

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

Progettazione di rete iSCSI consigliata

È necessario configurare progetti di rete completamente ridondanti per iSCSI. Il diagramma seguente mostra un esempio di configurazione ridondante, che garantisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. Fare riferimento a NetApp "[Riferimento alla configurazione SAN](#)" per ulteriori informazioni.



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

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

Cosa succederà ora?

Dopo aver esaminato i requisiti di distribuzione, "[creare SVM e LIF](#)" .

Creare SVM e LIF per datastore iSCSI in un dominio di gestione VCF

Creare una macchina virtuale di archiviazione (SVM) con più interfacce logiche (LIF) per fornire connettività iSCSI per i domini di gestione VMware Cloud Foundation.

Configurerai l'SVM con il supporto del protocollo iSCSI e imposta i più LIF su reti Ethernet separate per abilitare il multipathing e il failover per prestazioni e disponibilità ottimali.

Per aggiungere nuovi LIF a un SVM esistente, fare riferimento alla documentazione ONTAP : "[Creare ONTAP LIF](#)" .

Passi

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

Mostra esempio

The screenshot shows the ONTAP System Manager interface. The left sidebar has a 'Storage' section with various options: Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas, Storage VMs (which is selected and highlighted in blue), and Tiers. The main panel is titled 'Storage VMs' and contains a list of existing SVMs. A blue-bordered button labeled '+ Add' is located at the top left of the list area. The list includes the following items:

Name
EHC_iSCSI
EHC
HMC_187
HMC_3510
HMC_iSCSI_3510
infra_svm_a300
JS_EHC_iSCSI
OTVtest

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

Mostra esempio

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 **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, è possibile utilizzare impostazioni individuali oppure abilitare la casella di controllo per utilizzare impostazioni comuni per tutti i LIF rimanenti.



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

Mostra esempio

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

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

IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374

IP ADDRESS	PORT
172.21.119.180	a0a-3375

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

Mostra esempio

Storage VM Administration

Manage administrator account

Save

Cancel

Cosa succederà ora?

Dopo aver creato SVM e LIF, "configurare la rete per iSCSI sugli host ESXi".

Configurare la rete per iSCSI su host ESXi in un dominio di gestione VCF

Configurare la rete iSCSI sugli host ESXi nei domini di gestione VMware Cloud Foundation per abilitare la connettività ai sistemi di storage ONTAP. Creerai gruppi di porte distribuiti con separazione VLAN, configurerai il teaming uplink per la ridondanza e imposta gli adattatori VMkernel su ciascun host ESXi per stabilire percorsi iSCSI dedicati per le funzionalità di failover.

Eseguire questi passaggi sul cluster del dominio di gestione VCF utilizzando il client vSphere.

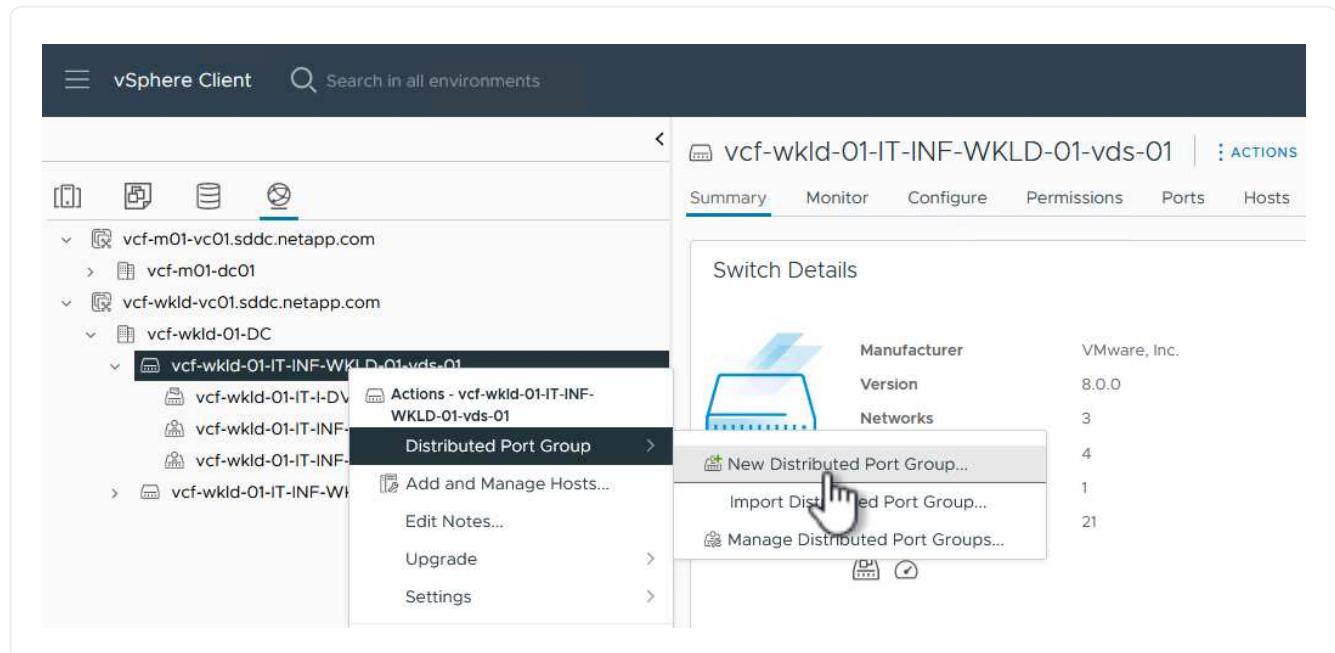
Passaggio 1: creare gruppi di porte distribuiti per il traffico iSCSI

Completare i seguenti passaggi per creare un nuovo gruppo di porte distribuite per ciascuna rete iSCSI:

Passi

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

Mostra esempio



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

Mostra esempio

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 (1)

Number of ports: 8

Network resource pool: (default)

VLAN

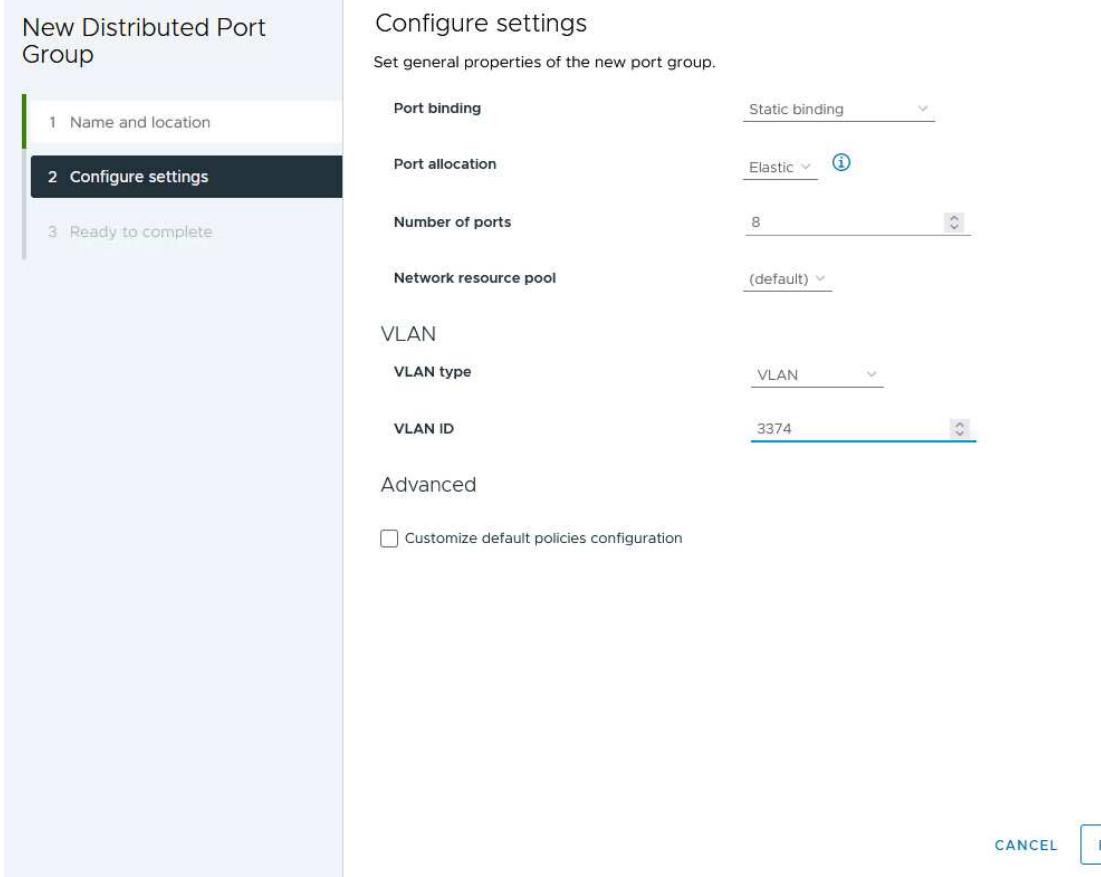
VLAN type: VLAN

VLAN ID: 3374

Advanced

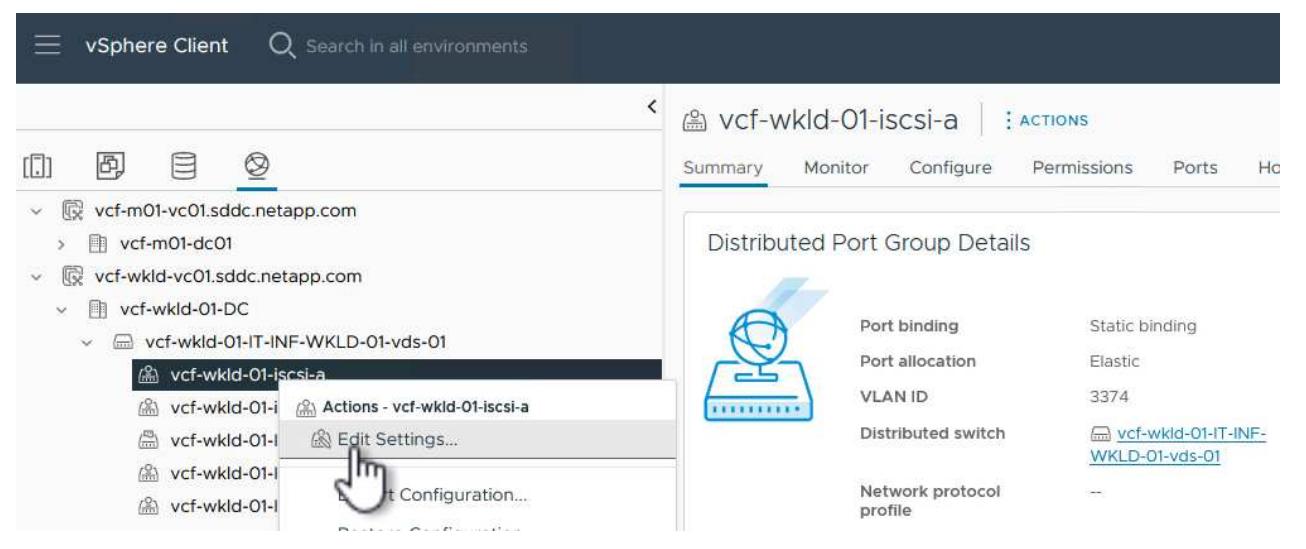
Customize default policies configuration

CANCEL BACK NEXT 



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

Mostra esempio



vSphere Client Search in all environments

vcf-wkld-01-iscsi-a ACTIONS

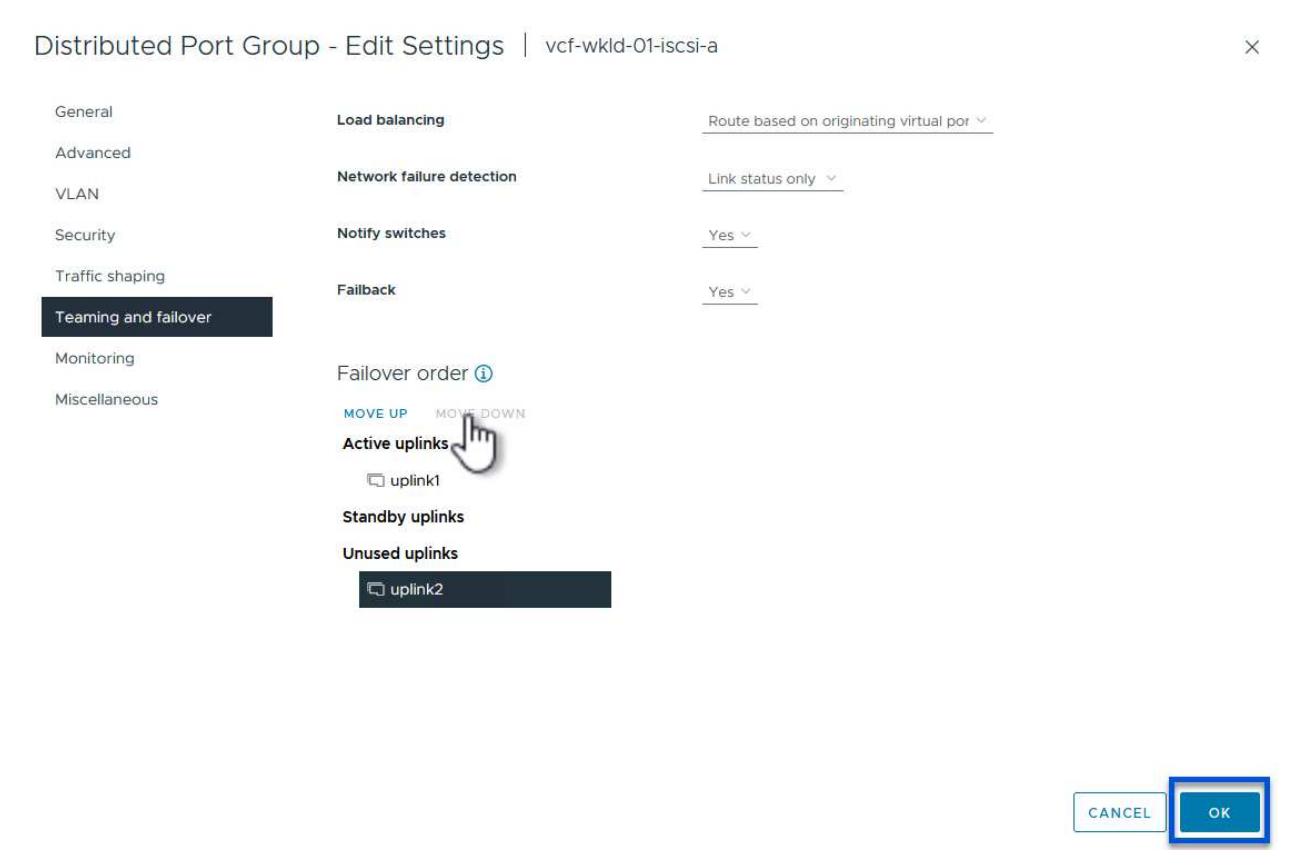
Summary Monitor Configure Permissions Ports Hc

Distributed Port Group Details

Port binding Static binding
Port allocation Elastic
VLAN ID 3374
Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile --

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

Mostra esempio



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

General Load balancing Route based on originating virtual port
Advanced Network failure detection Link status only
VLAN Notify switches Yes
Security Fallback Yes
Traffic shaping
Teaming and failover
Monitoring Failover order ⓘ
Miscellaneous Active uplinks MOVE UP MOVE DOWN
uplink1
Standby uplinks
Unused uplinks uplink2

CANCEL OK

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

Mostra esempio

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

The screenshot shows the 'Teaming and failover' tab selected in the Distributed Port Group settings. It displays the 'Failover order' section where 'uplink1' is highlighted. A hand cursor is shown clicking the 'MOVE DOWN' button next to 'uplink2'. Other options like 'Standby uplinks' and 'Unused uplinks' are also visible.

Passaggio 2: creare adattatori VMkernel su ciascun host ESXi

Creare adattatori VMkernel su ciascun host ESXi nel dominio di gestione.

Passi

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

Mostra esempio

The screenshot shows the vSphere Client interface with the host 'vcf-wkld-esx01.sddc.netapp.com' selected. In the 'Networking' section, the 'VMkernel adapters' tab is active. A hand cursor is clicking the 'ADD NETWORKING...' button. A table lists existing VMkernel adapters: vmk0 (vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt), vmk1 (vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion), vmk2 (vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs), and vmk10 (empty).

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

continuare.

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select connection type'. A sidebar on the left lists steps: 1. Select connection type (highlighted in dark grey), 2. Select target device, 3. Port properties, 4. IPv4 settings, 5. Ready to complete. The main panel contains three options:

- VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select target device'. A sidebar on the left lists steps: 1. Select connection type, 2. Select target device (highlighted in dark grey), 3. Port properties, 4. IPv4 settings, 5. Ready to complete. The main panel contains a 'Quick Filter' input field and a table of target devices:

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

At the bottom right, there are 'NEXT' and 'BACK' buttons, with 'NEXT' being highlighted and a hand cursor icon pointing at it.

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

Mostra esempio

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: vcf-wkld-01-iscsi-a (vcf-wkld-01-T-INF-WKLD-01-vds-01)

MTU: Get MTU from switch 9000

TCP/IP stack: Default

Available services

Enabled services:

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

5. Nella pagina **Impostazioni IPv4**, compilare **Indirizzo IP**, **Maschera di sottorete** e fornire un nuovo indirizzo IP del gateway (solo se richiesto). Fare clic su **Avanti** per continuare.

Mostra esempio

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: 172.21.118.127

Subnet mask: 255.255.255.0

Default gateway: Override default gateway for this adapter
172.21.166.1

DNS server addresses: 10.61.185.231

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard at step 5, 'Ready to complete'. On the left, a sidebar lists steps 1 through 5. Step 5 is highlighted with a dark background. The main area displays configuration details:

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

At the bottom right, there are 'CANCEL', 'BACK', and 'FINISH' buttons. The 'FINISH' button is highlighted with a green background and has a hand cursor icon pointing to it.

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

Cosa succederà ora?

Dopo aver configurato la rete per iSCSI su tutti gli host ESXi nel dominio del carico di lavoro, ["configurare l'archiviazione per iSCSI sugli host ESXi"](#).

Configurare l'archiviazione iSCSI in un dominio di gestione VCF utilizzando gli strumenti ONTAP

Configurare uno storage iSCSI supplementare per espandere i domini di gestione di VMware Cloud Foundation. Distribuirai gli strumenti ONTAP , configurerai un datastore iSCSI sul dominio di gestione e migrerai le VM di gestione al nuovo datastore.

Eseguire i seguenti passaggi sul cluster del dominio di gestione VCF utilizzando il client vSphere.

Passaggio 1: distribuire gli ONTAP tools for VMware vSphere

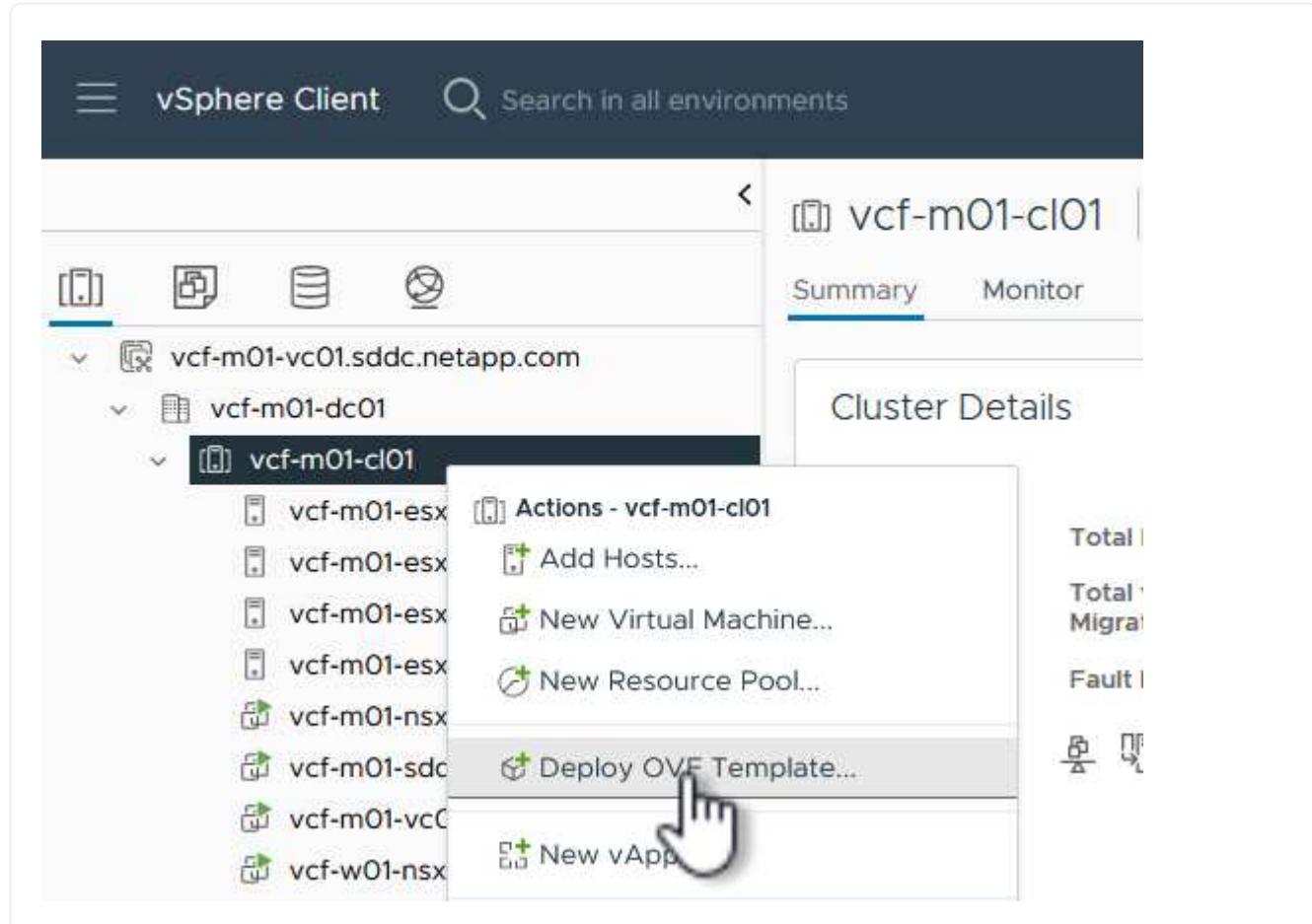
Gli ONTAP tools for VMware vSphere (OTV) vengono distribuiti come appliance VM e forniscono un'interfaccia utente vCenter integrata per la gestione dello storage ONTAP .

Passi

- Ottieni l'immagine OVA degli strumenti ONTAP da ["Sito di supporto NetApp"](#) e scaricarlo in una cartella locale.

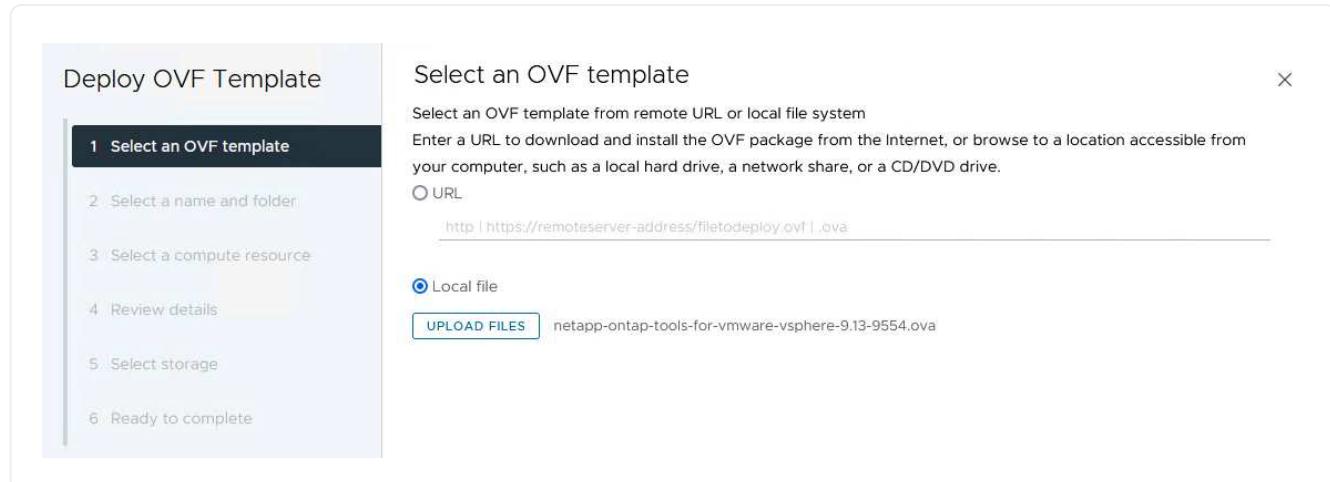
2. Accedere all'appliance vCenter per il dominio di gestione VCF.
3. Dall'interfaccia dell'appliance vCenter, fare clic con il pulsante destro del mouse sul cluster di gestione e selezionare **Distribuisci modello OVF...**

Mostra esempio



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

Mostra esempio



5. Per i passaggi da 2 a 5 della procedura guidata, seleziona un nome e una cartella per la VM, seleziona la

risorsa di elaborazione, rivedi i dettagli e accetta 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.

Mostra esempio

Name	Storage Compatibility	Capacity	Provisioned	Free
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB

7. Nella pagina **Selezione rete**, seleziona la rete utilizzata per la gestione del traffico.

Mostra esempio

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

8. Nella pagina **Personalizza modello**, inserisci tutte le informazioni richieste:

- Password da utilizzare per l'accesso amministrativo agli strumenti ONTAP .
- Indirizzo IP del server NTP.
- Password dell'account di manutenzione degli strumenti ONTAP .
- Password del database Derby degli strumenti ONTAP .
- Non selezionare la casella per **Abilitare VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire storage supplementare.

- FQDN o indirizzo IP dell’appliance vCenter per il **dominio del carico di lavoro VI**
 - Credenziali per l’appliance vCenter del **VI Workload Domain**
 - Proprietà di rete richieste.
9. Fare clic su **Avanti** per continuare.

Mostra esempio

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template**
- Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration 4 settings

Application User Password (*) 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:

Confirm Password:

NTP Servers 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

Maintenance User Password (*) Password to assign to maint user account.

Password:

Confirm Password:

Configure vCenter or Enable VCF 3 settings

Enable VMware Cloud Foundation (VCF) vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*) Specify the IP address/hostname of an existing vCenter to register to.
cf-wkld-vc01.sddc.netapp.com

Port (*) Specify the HTTPS port of an existing vCenter to register to.
443

Username (*) Specify the username of an existing vCenter to register to.
administrator@vsphere.local

Password (*) Specify the password of an existing vCenter to register to.

Password:

Confirm Password:

Network Properties 8 settings

Host Name Specify the hostname for the appliance. (Leave blank if DHCP is desired)
vcf-w01-otv9

IP Address Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL **BACK** **NEXT**

10. Esaminare tutte le informazioni nella pagina **Pronto per il completamento**, quindi fare clic su **Fine** per iniziare a distribuire l'appliance degli strumenti ONTAP .

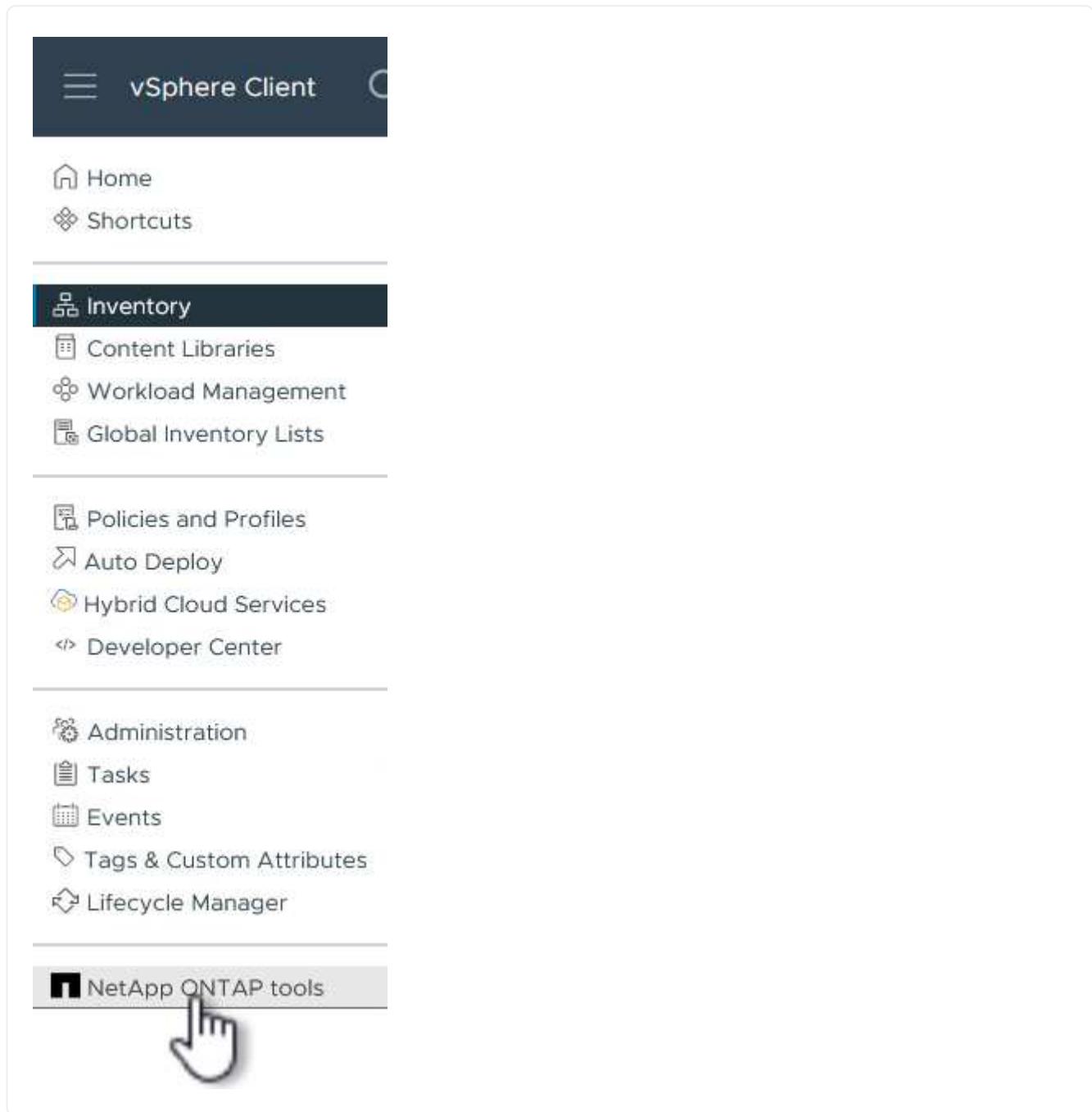
Passaggio 2: aggiungere un sistema di archiviazione

Per aggiungere un sistema di archiviazione utilizzando gli strumenti ONTAP , procedere come segue.

Passi

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

Mostra esempio



- Una volta in **Strumenti ONTAP ***, dalla pagina **Introduzione** (o da ***Sistemi di archiviazione**), fare clic su **Aggiungi** per aggiungere un nuovo sistema di archiviazione.

Mostra esempio

The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". Below the title bar, it says "NetApp ONTAP tools INSTANCE 172.21.166.139:8443". The main content area is titled "ONTAP tools for VMware vSphere" and includes tabs for "Getting Started", "Traditional Dashboard", and "vVols Dashboard". The "Getting Started" tab is selected. It displays instructions for adding storage systems and provisioning datastores, with large "ADD" and "PROVISION" buttons. A sidebar on the left lists "Overview", "Storage Systems", "Storage capability profile", "Storage Mapping", "Settings", and a "Reports" section containing "Datastore Report", "Virtual Machine Report", "vVols Datastore Report", "vVols Virtual Machine Report", and "Log Integrity Report". On the right, there are "Next Steps" sections for "View Dashboard" and "Settings". A "What's new?" section dated September 4, 2023, lists updates like support for ONTAP 9.13.1 and enhanced SCPs. A "Resources" section links to documentation for ONTAP tools and RBAC User Creator.

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

Mostra esempio

Add Storage System

i 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

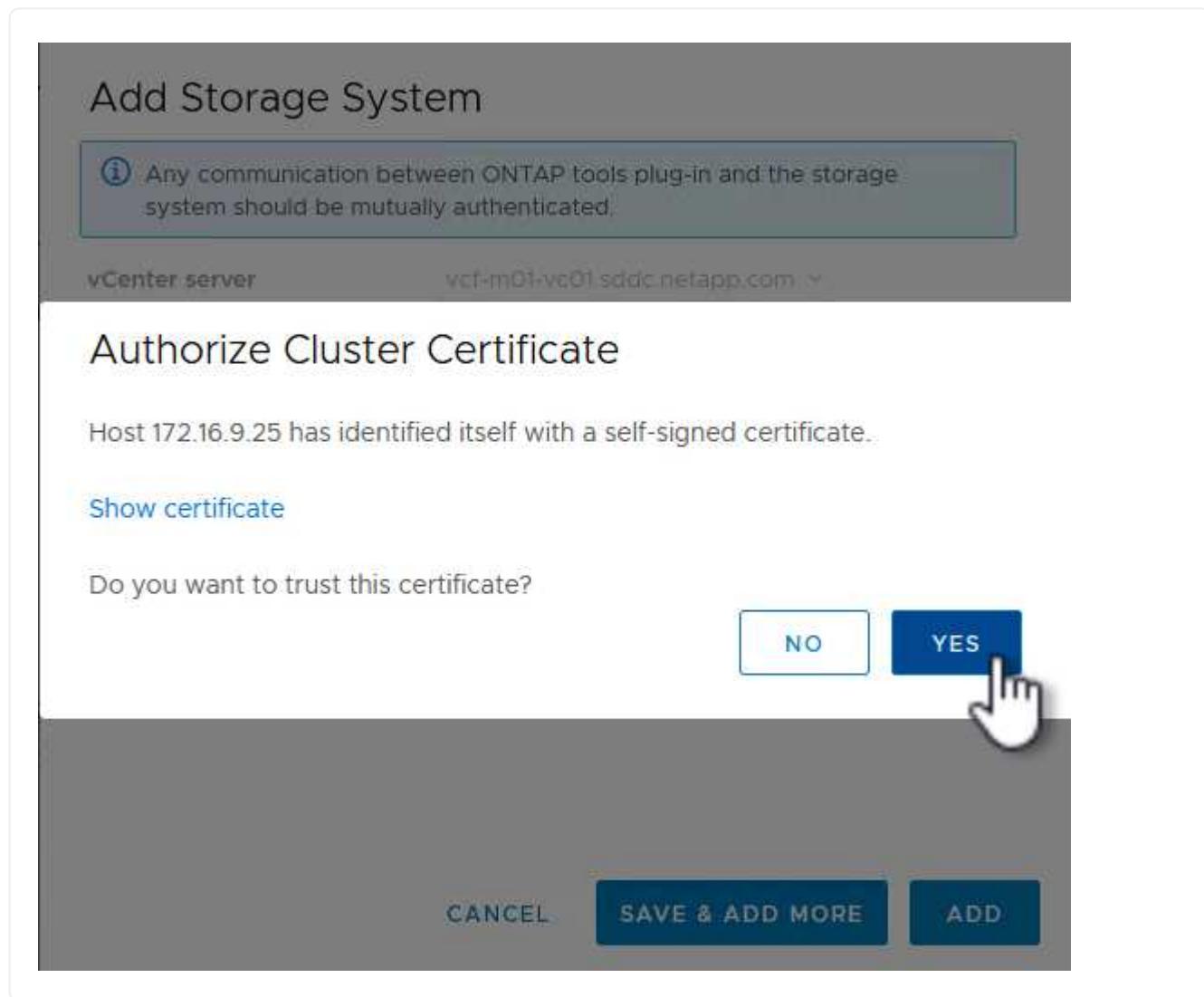
SAVE & ADD MORE

ADD



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

Mostra esempio



Facoltativo: migrare le VM di gestione al datastore iSCSI

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

Passi

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

Mostra esempio

The screenshot shows the vSphere Client interface. In the left sidebar, there's a tree view with nodes like 'vcf-m01-vc01.sddc.netapp.com' and 'vcf-m01-cl01'. Under 'vcf-m01-cl01', several virtual machines are listed: 'vcf-m01-esx01.sddc.netapp.com', 'vcf-m01-esx02.sddc.netapp.com', 'vcf-m01-esx03.sddc.netapp.com', 'vcf-m01-esx04.sddc.netapp.com', 'vcf-m01-nsx01a', 'vcf-m01-nsx01b', 'vcf-m01-otv9', 'vcf-m01-sddcm01', 'vcf-m01-vc01', 'vcf-w01-nsx01', 'vcf-w01-nsx02', 'vcf-w01-nsx03', and 'vcf-wkld-vc01'. The 'vcf-m01-cl01' node is expanded. In the main content area, the 'VMs' tab is selected. A context menu is open over the 'vcf-m01-nsx01a' VM, with the 'Migrate...' option highlighted by a cursor icon.

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

Mostra esempio

The screenshot shows the 'Select a migration type' step of the vSphere Migration wizard. On the left, a sidebar lists steps: 1. Select a migration type (highlighted), 2. Select storage, and 3. Ready to complete. The main area is titled 'Select a migration type' with the sub-instruction 'Change the virtual machines' compute resource, storage, or both.' Below are four radio button options:

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

4. Nella pagina **Selezione storage**, seleziona il datastore iSCSI e seleziona **Avanti** per continuare.

Mostra esempio

The screenshot shows the 'Select storage' step of the migration wizard. On the left, a sidebar lists steps: 1. Select a migration type, 2. Select storage (which is highlighted in dark blue), and 3. Ready to complete. The main area is titled 'Select storage' and contains the instruction 'Select the destination storage for the virtual machine migration.' Below this are two tabs: 'BATCH CONFIGURE' (selected) and 'CONFIGURE PER DISK'. Underneath are settings for 'Select virtual disk format' (set to 'Same format as source') and 'VM Storage Policy' (set to 'Datastore Default'). A checkbox for 'Disable Storage DRS for this virtual machine' is also present. A table lists available storage resources:

Name	Storage Compatibility	Capacity	Provisioned	Free	T
mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	V
vcf-m01-cl01-ds-vsang01	--	999.97 GB	7.28 TB	52.38 GB	V

Below the table, a compatibility section states: 'Compatibility checks succeeded.' with a green checkmark icon. At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons, with 'NEXT' being the one currently being clicked.

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

Mostra esempio

Recent Tasks	Alarms		
Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	<div style="width: 38%;">38%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	<div style="width: 42%;">42%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	<div style="width: 36%;">36%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	<div style="width: 49%;">49%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	<div style="width: 47%;">47%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	<div style="width: 39%;">39%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	<div style="width: 42%;">42%</div>	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	<div style="width: 44%;">44%</div>	Migrating Virtual Machine active state

Informazioni aggiuntive

- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a "[Documentazione ONTAP 9](#)" .
- Per informazioni sulla configurazione di VCF, fare riferimento a "[Documentazione di VMware Cloud Foundation](#)" .
- Per informazioni sull'utilizzo di datastore iSCSI VMFS con VMware, fare riferimento a "[vSphere VMFS datastore - backend di archiviazione iSCSI con ONTAP](#)" .
- Per demo video di questa soluzione, fare riferimento a "[Provisioning del datastore VMware](#)" .

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

In questo caso d'uso descriviamo in dettaglio come configurare un datastore VMFS su Fibre Channel (FC) come storage supplementare per il dominio di gestione VMware Cloud Foundation (VCF). Questa procedura riassume i passaggi per distribuire gli strumenti ONTAP sul dominio di gestione, aggiungere un backend di archiviazione e predisporre il datastore.

Prima di iniziare

Assicurarsi che i seguenti componenti e configurazioni siano presenti.

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



- Utilizzare l’interfaccia logica FC SVM nella configurazione della zona anziché le porte FC fisiche sui sistemi ONTAP .
- Utilizzare multipath per FC LUN.

Passi

1. Distribuire gli strumenti ONTAP sul dominio di gestione seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Distribuire gli strumenti ONTAP sul dominio di gestione](#)" .

Gli ONTAP tools for VMware vSphere vengono distribuiti come un singolo nodo di piccole dimensioni con servizi principali per supportare i datastore NFS e VMFS.

2. Aggiungere un backend di storage utilizzando l’interfaccia client vSphere seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Definisci il backend di archiviazione utilizzando l’interfaccia client vSphere](#)" .

L’aggiunta di un backend di archiviazione consente di integrare un cluster ONTAP .

3. Eseguire il provisioning di VMFS su FC seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Provisioning VMFS su FC](#)" .

Informazioni aggiuntive

- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a"[Documentazione ONTAP 9](#)" .
- Per informazioni sulla configurazione di VCF, fare riferimento a"[Documentazione di VMware Cloud Foundation](#)" .
- Per informazioni sulla configurazione di Fibre Channel sui sistemi di archiviazione ONTAP , fare riferimento alla documentazione di ONTAP 9 "[Gestione dello storage SAN](#)" .
- Per ulteriori informazioni sull’utilizzo di VMFS con sistemi di archiviazione ONTAP , fare riferimento a"[Guida alla distribuzione per VMFS](#)" .
- Per demo video di questa soluzione, fare riferimento a"[Provisioning del datastore VMware](#)" .

Espandi i domini del carico di lavoro VI con vVols iSCSI

Flusso di lavoro di distribuzione per l’aggiunta di un datastore iSCSI vVols come storage supplementare in un dominio di carico di lavoro VI

Inizia a configurare un datastore iSCSI vVols come storage supplementare in un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Creerai SVM e LIF, configurerai la rete iSCSI, implementerai gli ONTAP tools for VMware vSphere e configurerai lo storage.

1

["Esaminare i requisiti di distribuzione"](#)

Esaminare i requisiti per distribuire iSCSI vVols in un dominio di carico di lavoro VMware Cloud Foundation VI.

2

["Creare SVM e LIF"](#)

Creare una SVM con più LIF per il traffico iSCSI.

3

"Configurare la rete"

Configurare la rete per iSCSI sugli host ESXi.

4

"Configurare l'archiviazione"

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

Requisiti di distribuzione per iSCSI vVols in un dominio di carico di lavoro VI

Esaminare i requisiti di progettazione e infrastruttura di rete consigliati per distribuire iSCSI vVols in un dominio di carico di lavoro VMware Cloud Foundation VI. È necessario un sistema di archiviazione ONTAP AFF o ASA completamente configurato, un dominio di gestione VCF completato e un dominio di carico di lavoro VI esistente.

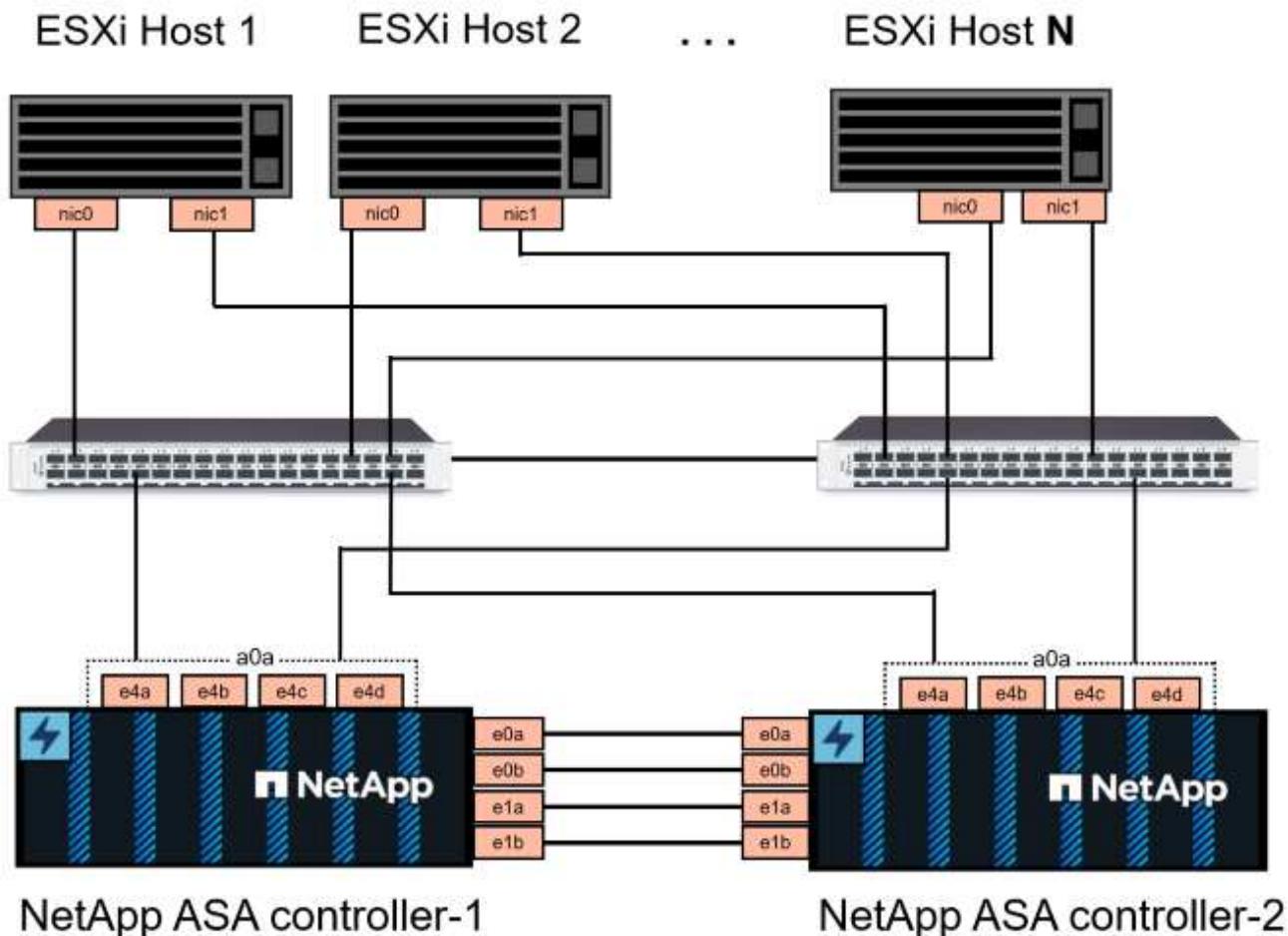
Requisiti infrastrutturali

Assicurarsi che i seguenti componenti e configurazioni siano presenti.

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

Progettazione di rete iSCSI consigliata

È necessario configurare progetti di rete completamente ridondanti per iSCSI. Il diagramma seguente illustra un esempio di configurazione ridondante. Fornisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. Per ulteriori informazioni, fare riferimento a NetApp "[Riferimento alla configurazione SAN](#)".



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



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

Cosa succederà ora?

Dopo aver esaminato i requisiti di distribuzione, "[creare SVM e LIF](#)" .

Creare SVM e LIF per datastore iSCSI vVols in un dominio di carico di lavoro VCF VI

Creare una Storage Virtual Machine (SVM) e più interfacce logiche (LIF) su un sistema ONTAP per supportare il traffico iSCSI per i datastore vVols in un dominio di carico di lavoro VMware Cloud Foundation VI. Aggiungerai una nuova SVM, abiliterai iSCSI, configurerai i LIF e, facoltativamente, abiliterai l'account di amministrazione della VM di archiviazione.

Per aggiungere nuovi LIF a un SVM esistente, fare riferimento alla documentazione ONTAP :"[Creare ONTAP](#)

LIF".

Passi

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

Mostra esempio

The screenshot shows the ONTAP System Manager interface. On the left, there's a sidebar with a navigation menu:

- DASHBOARD
- INSIGHTS
- STORAGE ▾
 - Overview
 - Volumes
 - LUNs
 - Consistency Groups
 - NVMe Namespaces
 - Shares
 - Buckets
 - Qtrees
 - Quotas
- Storage VMs
- Tiers

The main panel is titled "Storage VMs" and contains a list of existing SVMs. A blue box highlights the "+ Add" button. Below it is a table with a single column labeled "Name", containing the following entries:

Name
EHC_iSCSI
EHC
HMC_187
HMC_3510
HMC_iSCSI_3510
infra_svm_a300
JS_EHC_iSCSI
OTVtest

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

Mostra esempio

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 **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, è possibile utilizzare impostazioni individuali oppure abilitare la casella di controllo per utilizzare impostazioni comuni per tutti i LIF rimanenti.



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

Mostra esempio

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
172.21.118.179	24	Add optional gateway	NFS_iSCSI

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

IP ADDRESS	PORT
172.21.119.179	a0a-3375

ntaphci-a300-02

IP ADDRESS	PORT
172.21.118.180	a0a-3374

IP ADDRESS	PORT
172.21.119.180	a0a-3375

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

Mostra esempio

Storage VM Administration

Manage administrator account

Save

Cancel

Cosa succederà ora?

Dopo aver creato SVM e LIF, "configurare la rete per iSCSI sugli host ESXi" .

Configurare la rete per iSCSI su host ESXi in un dominio di carico di lavoro VCF VI

Configurare la rete per l'archiviazione iSCSI sugli host ESXi in un dominio di carico di lavoro VI. Creerai gruppi di porte distribuiti per il traffico iSCSI e configurerai gli adattatori VMkernel utilizzando il client vSphere per abilitare connettività affidabile e multipathing.

Utilizzare il client vSphere con vCenter Single Sign-On per eseguire questi passaggi sul cluster VI Workload Domain. Lo stesso client vSphere gestisce sia il dominio di gestione che quello del carico di lavoro.

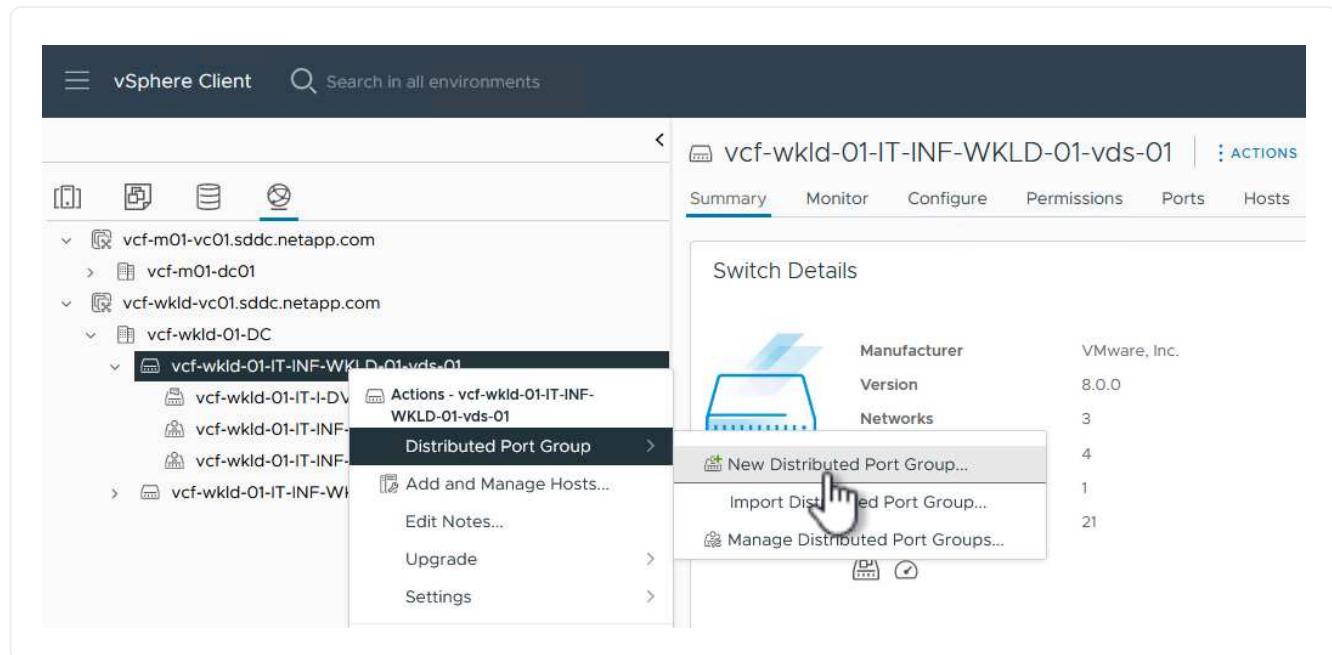
Passaggio 1: creare gruppi di porte distribuiti per il traffico iSCSI

Completare i seguenti passaggi per creare un nuovo gruppo di porte distribuite per ciascuna rete iSCSI.

Passi

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

Mostra esempio



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

Mostra esempio

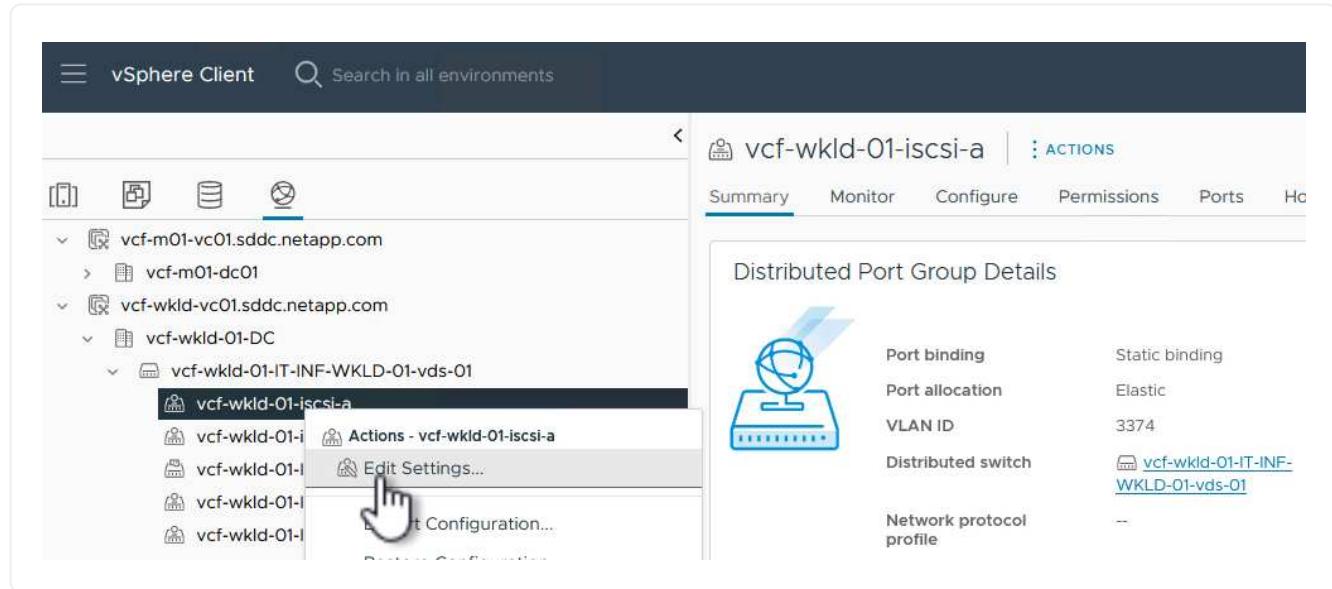
The screenshot shows a configuration interface for creating a new distributed port group. On the left, a vertical navigation bar lists three steps: 1. Name and location, 2. Configure settings (which is selected and highlighted in dark grey), and 3. Ready to complete. The main panel is titled 'Configure settings' and contains the following fields:

- Port binding:** Static binding
- Port allocation:** Elastic (with a help icon)
- Number of ports:** 8
- Network resource pool:** (default)
- VLAN:**
 - VLAN type:** VLAN
 - VLAN ID:** 3374
- Advanced:** A checkbox labeled 'Customize default policies configuration' is unchecked.

At the bottom right, there are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT' (highlighted with a blue border and a hand cursor icon).

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

Mostra esempio



vSphere Client Search in all environments

vcf-wkld-01-iscsi-a ACTIONS

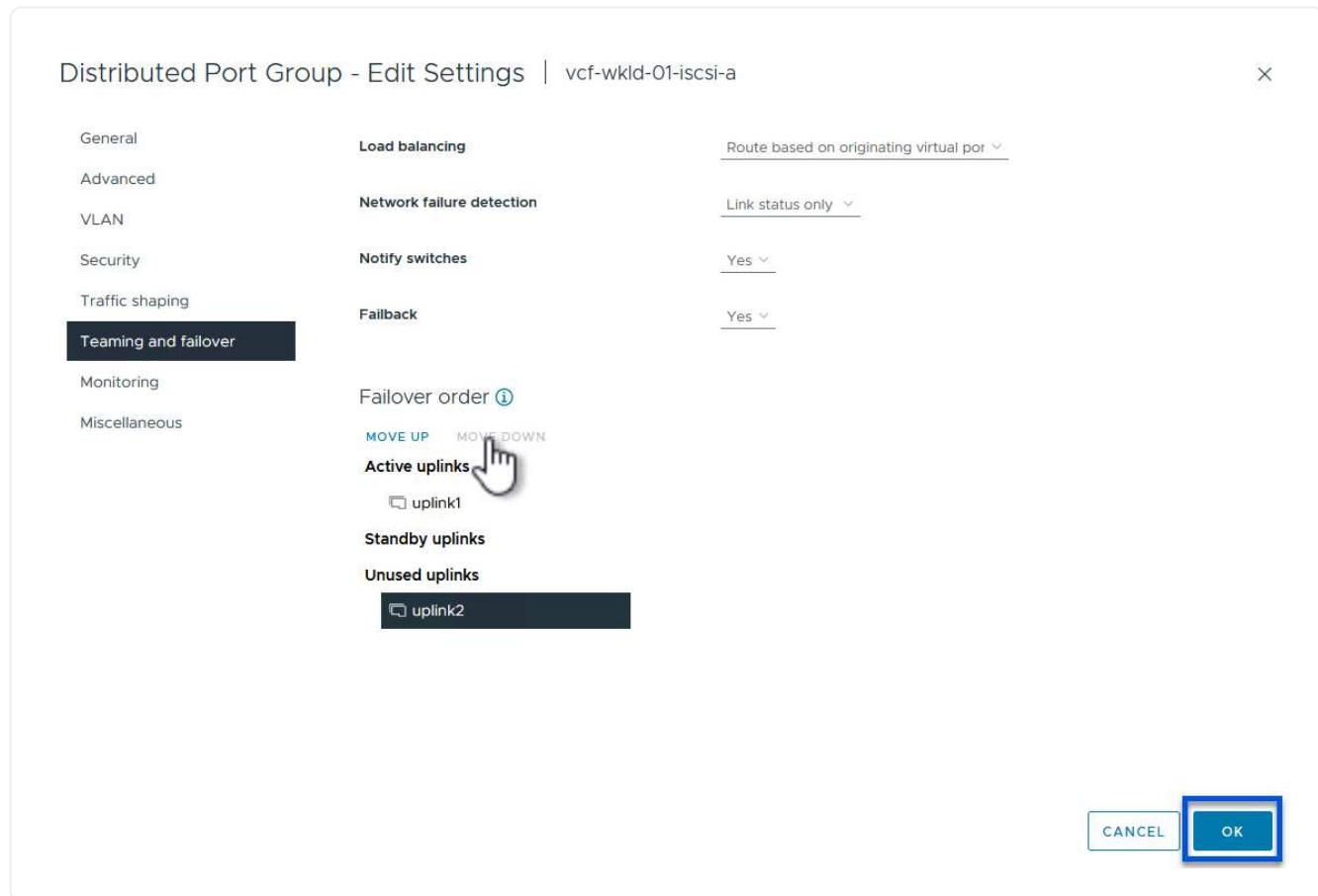
Summary Monitor Configure Permissions Ports Hc

Distributed Port Group Details

Port binding Static binding
Port allocation Elastic
VLAN ID 3374
Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile --

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

Mostra esempio



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

General Load balancing Route based on originating virtual port
Advanced Network failure detection Link status only
VLAN Notify switches Yes
Security Fallback Yes
Traffic shaping
Teaming and failover
Monitoring Failover order ⓘ
Miscellaneous Active uplinks MOVE UP MOVE DOWN
uplink1
Standby uplinks
Unused uplinks uplink2

CANCEL OK

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

Mostra esempio

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

General Advanced VLAN Security Traffic shaping Teaming and failover Monitoring Miscellaneous

Load balancing Network failure detection Notify switches Fallback

Route based on originating virtual port ▾ Link status only ▾ Yes ▾ Yes ▾

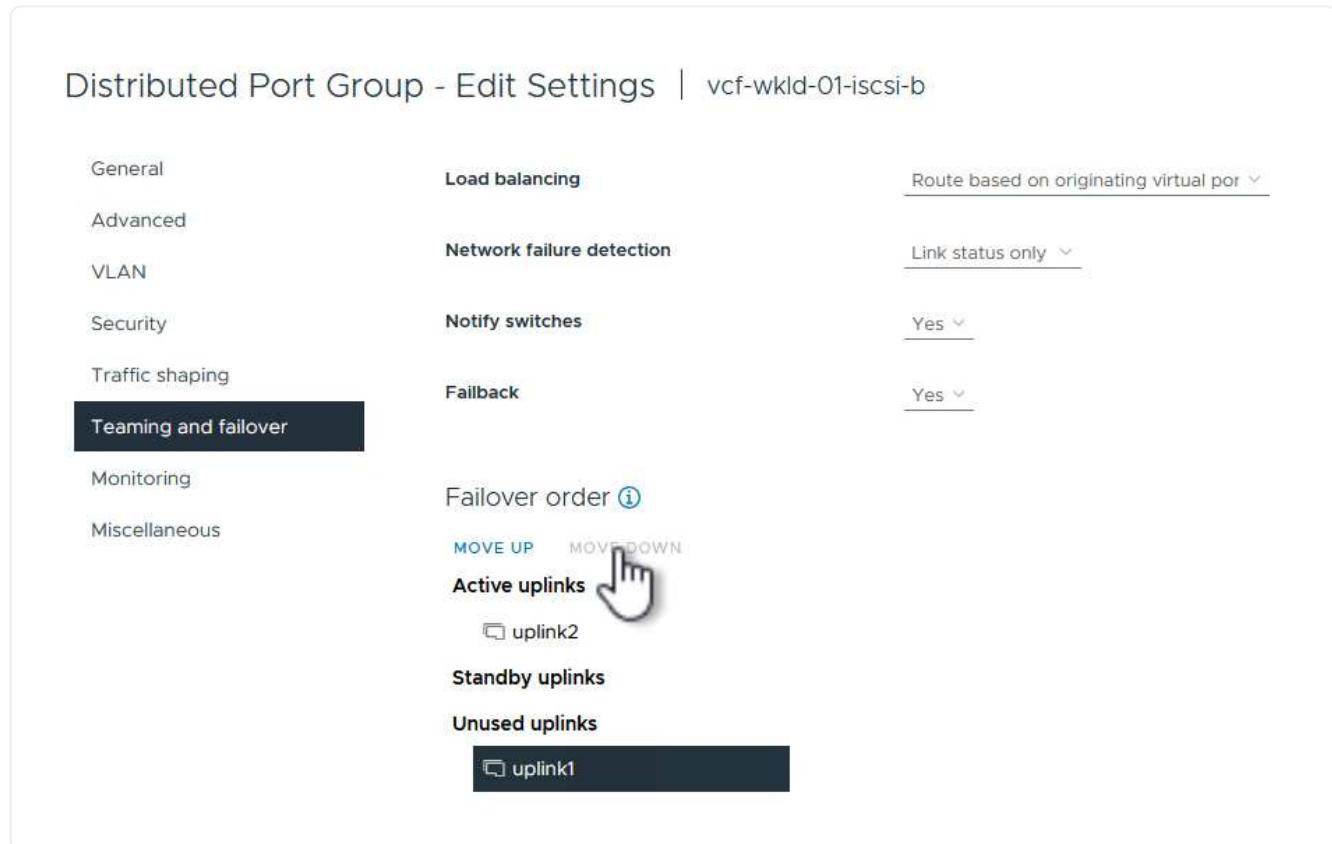
Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks  uplink2

Standby uplinks

Unused uplinks uplink1



Passaggio 2: creare adattatori VMkernel su ciascun host ESXi

Eseguire i seguenti passaggi su ciascun host ESXi nel dominio del carico di lavoro utilizzando il client vSphere.

Passi

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

Mostra esempio

vSphere Client Search in all environments

vcf-wkld-esx01.sddc.netapp.com ACTIONS

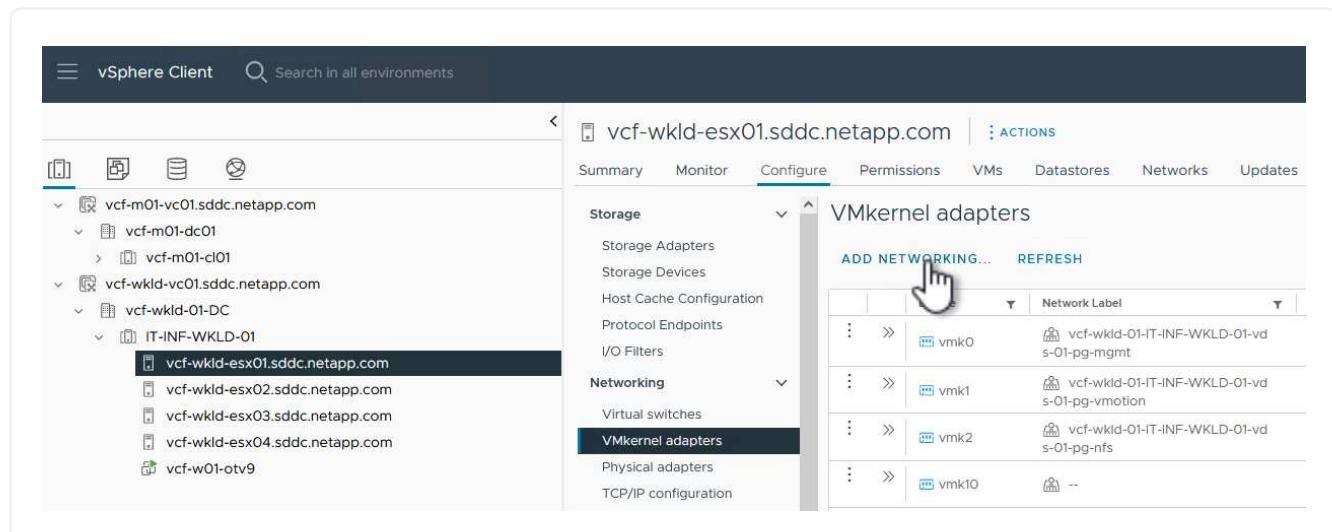
Summary Monitor Configure Permissions VMs Datastores Networks Updates

Storage Storage Adapters Storage Devices Host Cache Configuration Protocol Endpoints I/O Filters

Networking Virtual switches VMkernel adapters

ADD NETWORKING... REFRESH

		Network Label
⋮	»	vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt
⋮	»	vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion
⋮	»	vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs
⋮	»	vmk10 --



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

continuare.

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select connection type'. A sidebar on the left lists steps: 1. Select connection type (highlighted in dark grey), 2. Select target device, 3. Port properties, 4. IPv4 settings, 5. Ready to complete. The main panel contains three options:

- VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select target device'. A sidebar on the left lists steps: 1. Select connection type, 2. Select target device (highlighted in dark grey), 3. Port properties, 4. IPv4 settings, 5. Ready to complete. The main panel contains a 'Quick Filter' input field and a table of target devices:

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-it-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-it-INF-WKLD-01-vds-01
vcf-wkld-01-it-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-it-INF-WKLD-01-vds-01
vcf-wkld-01-it-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-it-INF-WKLD-01-vds-02
vcf-wkld-01-it-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-it-INF-WKLD-01-vds-01

At the bottom right, there are 'NEXT' and 'BACK' buttons, with 'NEXT' being highlighted and a hand cursor icon pointing at it.

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

Mostra esempio

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: vcf-wkld-01-iscsi-a (vcf-wkld-01-T-INF-WKLD-01-vds-01)

MTU: Get MTU from switch 9000

TCP/IP stack: Default

Available services

Enabled services:

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

5. Nella pagina **Impostazioni IPv4**, compilare **Indirizzo IP**, **Maschera di sottorete** e fornire un nuovo indirizzo IP del gateway (solo se richiesto). Fare clic su **Avanti** per continuare.

Mostra esempio

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: 172.21.118.127

Subnet mask: 255.255.255.0

Default gateway: Override default gateway for this adapter
172.21.166.1

DNS server addresses: 10.61.185.231

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard at step 5: Ready to complete. On the left, a sidebar lists steps 1 through 5. Step 5 is highlighted with a dark background. The main area displays configuration details:

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

At the bottom right, there are 'CANCEL', 'BACK', and 'FINISH' buttons. The 'FINISH' button is highlighted with a green background and has a hand cursor icon pointing to it.

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

Cosa succederà ora?

Dopo aver configurato la rete per iSCSI su tutti gli host ESXi nel dominio del carico di lavoro, "configurare l'archiviazione per iSCSI vVols".

Configurare l'archiviazione iSCSI vVols in un dominio di carico di lavoro VCF VI utilizzando gli strumenti ONTAP

Configurare l'archiviazione iSCSI vVols in un dominio di carico di lavoro VI utilizzando gli strumenti ONTAP . Distribuirai gli ONTAP tools for VMware vSphere, registrerai un sistema di storage, creerai un profilo di capacità di storage e fornirai un datastore vVols nel client vSphere.

Passaggio 1: distribuire gli ONTAP tools for VMware vSphere

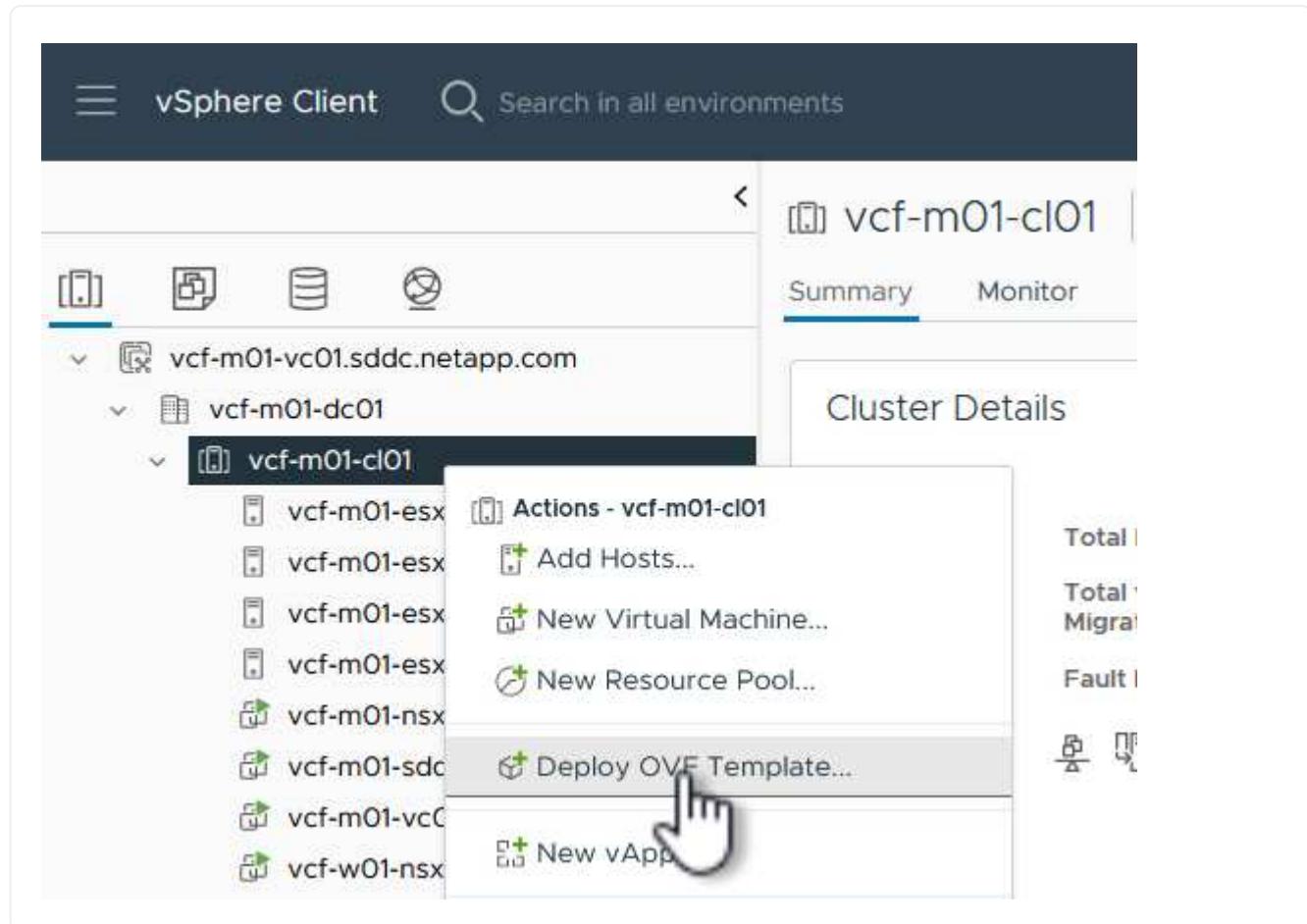
Per i domini del carico di lavoro VI, gli strumenti ONTAP vengono installati nel cluster di gestione VCF ma registrati con il vCenter associato al dominio del carico di lavoro VI.

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

Passi

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

Mostra esempio



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

Mostra esempio

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
http://remoteserver-address/filetodeploy.ovf|.ova

Local file
UPLOAD FILES netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Per i passaggi da 2 a 5 della procedura guidata, seleziona un nome e una cartella per la VM, seleziona la risorsa di elaborazione, rivedi i dettagli e accetta 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.

Mostra esempio

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

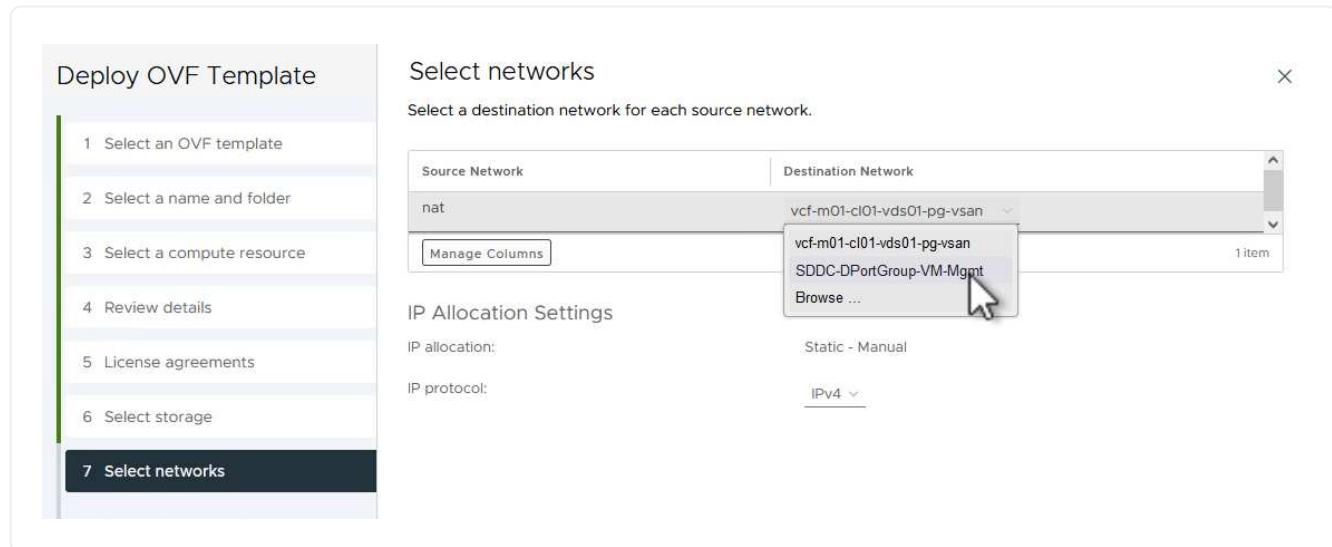
Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	...
vcf-m01-cl01-ds-vs01	--	999.97 GB	7.17 TB	225.72 GB	V
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
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 **Selezione rete**, seleziona la rete utilizzata per la gestione del traffico.

Mostra esempio



8. Nella pagina **Personalizza modello**, inserisci tutte le informazioni richieste:

- Password da utilizzare per l'accesso amministrativo agli strumenti ONTAP .
- Indirizzo IP del server NTP.
- Password dell'account di manutenzione degli strumenti ONTAP .
- Password del database Derby degli strumenti ONTAP .
- Non selezionare la casella per **Abilitare VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire storage supplementare.
- FQDN o indirizzo IP dell'appliance vCenter per il **dominio del carico di lavoro VI**
- Credenziali per l'appliance vCenter del **VI Workload Domain**
- Proprietà di rete richieste.

9. Fare clic su **Avanti** per continuare.

Mostra esempio

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template**
- Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration 4 settings

Application User Password (*) 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:

Confirm Password:

NTP Servers 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

Maintenance User Password (*) Password to assign to maint user account.

Password:

Confirm Password:

Configure vCenter or Enable VCF 3 settings

Enable VMware Cloud Foundation (VCF) vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*) Specify the IP address/hostname of an existing vCenter to register to.
cf-wkld-vc01.sddc.netapp.com

Port (*) Specify the HTTPS port of an existing vCenter to register to.
443

Username (*) Specify the username of an existing vCenter to register to.
administrator@vsphere.local

Password (*) Specify the password of an existing vCenter to register to.

Password:

Confirm Password:

Network Properties 8 settings

Host Name Specify the hostname for the appliance. (Leave blank if DHCP is desired)
vcf-w01-otv9

IP Address Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL **BACK** **NEXT**

10. Esaminare tutte le informazioni nella pagina **Pronto per il completamento**, quindi fare clic su **Fine** per iniziare a distribuire l'appliance degli strumenti ONTAP .

Passaggio 2: aggiungere un sistema di archiviazione

Per aggiungere un sistema di archiviazione utilizzando gli strumenti ONTAP , procedere come segue.

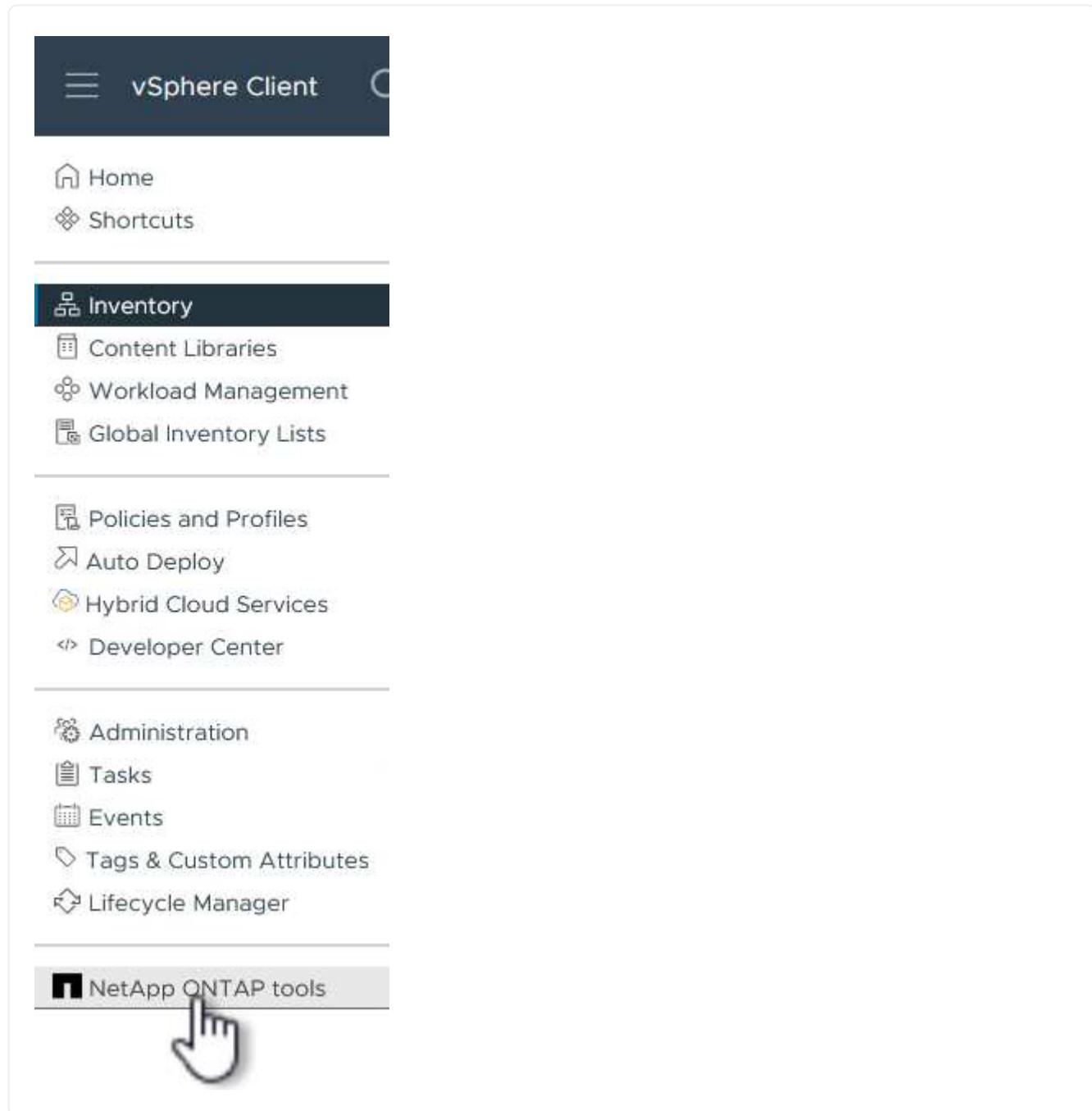


vVol richiede le credenziali del cluster ONTAP anziché le credenziali SVM. Per ulteriori informazioni, fare riferimento alla documentazione degli ONTAP tools for VMware vSphere : ["Aggiungere sistemi di archiviazione"](#) .

Passi

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

Mostra esempio



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

Mostra esempio

The screenshot shows the vSphere Client interface with the NetApp ONTAP tools plugin. The left sidebar has 'Overview' selected. The main content area is titled 'ONTAP tools for VMware vSphere' and includes sections for 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. The 'Getting Started' section contains two main buttons: 'Add Storage System' and 'Provision Datastore'. Below these buttons, there are links to add storage systems and create traditional or vVols datastores. A 'What's new?' section is present, dated September 4, 2023, listing recent changes such as support for ONTAP 9.13.1 and enhanced SCPs. To the right, there are 'Next Steps' and 'Resources' sections.

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

Mostra esempio

Add Storage System

i 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 **Sì** per autorizzare il certificato del cluster e aggiungere il sistema di archiviazione.

Mostra esempio

The screenshot shows a 'vCenter server' configuration screen with a 'vCenter server' dropdown set to 'vcf-m01-vc01.sddc.netapp.com'. Below it, the title 'Add Storage System' is displayed, followed by a note: 'Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.' A section titled 'Authorize Cluster Certificate' contains the message 'Host 172.16.9.25 has identified itself with a self-signed certificate.' with a 'Show certificate' link. A question 'Do you want to trust this certificate?' is followed by 'NO' and 'YES' buttons, with 'YES' being highlighted and a hand cursor icon pointing at it. At the bottom are 'CANCEL', 'SAVE & ADD MORE' (highlighted), and 'ADD' buttons.

Passaggio 3: creare un profilo di capacità di archiviazione negli strumenti ONTAP

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

Passi

1. Negli strumenti ONTAP , seleziona **Profilo capacità di archiviazione** dal menu a sinistra e poi premi **Crea**.

Mostra esempio

The screenshot shows the vSphere Client interface. At the top, there is a dark header bar with the "vSphere Client" logo and a search bar labeled "Search in all environments". Below the header, the title "NetApp ONTAP tools" and "INSTANCE 172.21.166.149:8443" are displayed. The main content area has a sidebar on the left with three items: "Overview", "Storage Systems", and "Storage capability profile", with "Storage capability profile" being the active tab. The main panel is titled "Storage Capability Profiles" and contains a blue "CREATE" button. Below the button, there is a section labeled "Name".

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

Mostra esempio

The screenshot shows the "Create Storage Capability Profile" wizard. On the left, a vertical navigation bar lists steps: 1 General (highlighted in grey), 2 Platform, 3 Protocol, 4 Performance, 5 Storage attributes, and 6 Summary. The main panel is titled "General" and contains the instruction "Specify a name and description for the storage capability profile." Below this, there are two input fields: "Name:" with the value "Gold ASA iSCSI" and "Description:" with an empty text area. At the bottom right, there are "CANCEL" and "NEXT" buttons.

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

Mostra esempio

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Platform

Platform: Performance

Asymmetric: OFF

CANCEL BACK NEXT

4. Seleziona il protocollo che preferisci oppure seleziona **Qualsiasi** per consentire tutti i protocolli possibili.
5. Fare clic su **Avanti** per continuare.

Mostra esempio

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

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

Mostra esempio

The screenshot shows the 'Create Storage Capability Profile' wizard. The left sidebar lists steps 1 through 6, with step 4 ('Performance') highlighted. The main area is titled 'Performance' and contains the following configuration:

- Radio button for 'None' (disabled)
- Radio button for 'QoS policy group' (selected)
- Text input for 'Min IOPS':
- Text input for 'Max IOPS':
- Check box for 'Unlimited' (

At the bottom right are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT'.

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

Mostra esempio

The screenshot shows the 'Create Storage Capability Profile' wizard. The left sidebar lists steps 1 through 6, with step 5 ('Storage attributes') highlighted. The main area is titled 'Storage attributes' and contains the following settings:

Deduplication:	Yes
Compression:	Yes
Space reserve:	Thin
Encryption:	No
Tiering policy (FabricPool):	None

At the bottom right are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT'.

8. Rivedi il riepilogo e clicca su **Fine** per creare il profilo.

Mostra esempio

The screenshot shows the 'Create Storage Capability Profile' wizard. On the left, a vertical navigation bar lists steps 1 through 6: General, Platform, Protocol, Performance, Storage attributes, and Summary. Step 6 is highlighted. The main area is titled 'Summary' and displays the following configuration:

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

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'FINISH'. A hand cursor is hovering over the 'FINISH' button.

Passaggio 4: creare un datastore vVols negli strumenti ONTAP

Per creare un datastore vVols negli strumenti ONTAP , completare i seguenti passaggi.

Passi

1. Negli strumenti ONTAP , selezionare **Panoramica** e dalla scheda **Introduzione** fare clic su **Provisioning** per avviare la procedura guidata.

Mostra esempio

The screenshot shows the 'NetApp ONTAP tools' interface. The left sidebar includes links for 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), and Help. The main area is titled 'ONTAP tools for VMware vSphere' and features a 'Getting Started' section. It includes a brief description: 'ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments.' Below this are two main buttons: 'Add Storage System' (with a plus icon) and 'Provision Datastore' (with a plus icon). At the bottom, there are two calls-to-action: 'ADD' and 'PROVISION'. The 'PROVISION' button is highlighted with a blue border.

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

Mostra esempio

New Datastore

General

Specify the details of the datastore to provision [?](#)

Provisioning destination: [IT-INF-WKLD-01](#) [BROWSE](#)

Type: NFS VMFS vVols

Name: VCF_WKLD_02_VVOLS

Description:

Protocol: NFS iSCSI FC / FCoE NVMe/FC

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

5. Nella pagina **Sistema di archiviazione**, seleziona un profilo di capacità di archiviazione, il sistema di archiviazione e la VM.
6. Fare clic su **Avanti** per continuare.

Mostra esempio

New Datastore

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](#)

- Nella pagina **Attributi di archiviazione**, seleziona l'opzione per creare un nuovo volume per il datastore e immetti gli attributi di archiviazione del volume che desideri creare.
- Fare clic su **Aggiungi** per creare il volume e quindi su **Avanti** per continuare.

Mostra esempio

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) <small>①</small>	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHC Aggr02 - (27053.3 GE)	Thin

ADD CANCEL BACK NEXT

- Rivedere il riepilogo e fare clic su **Fine** per avviare il processo di creazione del datastore vVol.

Mostra esempio

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	EHC Aggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL BACK **FINISH**

Informazioni aggiuntive

- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a "[Documentazione ONTAP 9](#)" .

- Per informazioni sulla configurazione di VCF, fare riferimento a "[Documentazione di VMware Cloud Foundation](#)" .
- Per informazioni sull'utilizzo di datastore iSCSI VMFS con VMware, fare riferimento a "[vSphere VMFS datastore - backend di archiviazione iSCSI con ONTAP](#)" .
- Per demo video di questa soluzione, fare riferimento a "[Provisioning del datastore VMware](#)" .

Espandi i domini del carico di lavoro VI con vVols NFS

Flusso di lavoro di distribuzione per l'aggiunta di datastore NFS vVols come storage supplementare in un dominio di carico di lavoro VI

Inizia ad aggiungere datastore NFS vVols come storage supplementare in domini di carichi di lavoro VI utilizzando gli ONTAP tools for VMware vSphere. Esaminerai i requisiti di distribuzione, distribuirai gli ONTAP tools for VMware vSphere, configurerai l'SVM con interfacce logiche e configurerai l'archiviazione.

1

["Esaminare i requisiti di distribuzione"](#)

Esaminare i requisiti per distribuire NFS vVols in un dominio di gestione VMware Cloud Foundation.

2

["Creare SVM e LIF"](#)

Creare una SVM con più LIF per il traffico NFS.

3

["Configurare la rete"](#)

Configurare la rete per NFS sugli host ESXi.

4

["Configurare l'archiviazione"](#)

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

Requisiti di distribuzione per l'aggiunta vVols NFS in un dominio di carico di lavoro VI

Esaminare i requisiti di progettazione e infrastruttura di rete consigliati per distribuire NFS vVols in un dominio di carico di lavoro VMware Cloud Foundation VI. È necessario un sistema di archiviazione ONTAP AFF o ASA completamente configurato, un dominio di gestione VCF completato e un dominio di carico di lavoro VI esistente.

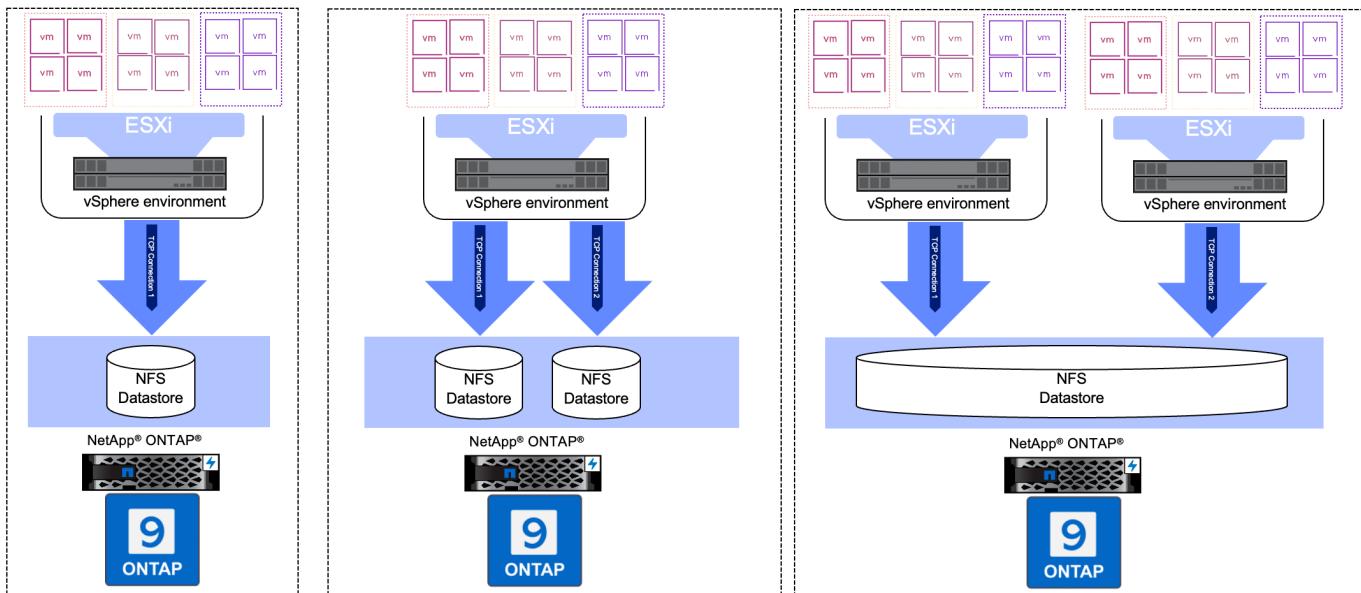
Requisiti infrastrutturali

Assicurarsi che i seguenti componenti e configurazioni siano presenti.

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

Progettazione di rete NFS consigliata

Configurare progetti di rete ridondanti per NFS per garantire tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host. È comune distribuire NFS con una singola subnet o più subnet, a seconda dei requisiti architettonici.



Informazioni aggiuntive

- Per informazioni dettagliate specifiche su VMware vSphere, fare riferimento a "[Procedure consigliate per l'esecuzione di NFS con VMware vSphere](#)" .
- Per indicazioni di rete sull'utilizzo di ONTAP con VMware vSphere, fare riferimento a "[Configurazione di rete - NFS](#)" sezione della documentazione delle applicazioni aziendali NetApp .

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

- Per informazioni complete sull'utilizzo di NFS con cluster vSphere, fare riferimento a "[Guida di riferimento NFS v3 per vSphere 8](#)" .

Cosa succederà ora?

Dopo aver esaminato i requisiti, "[creare SVM e LIF](#)" .

Creare SVM e LIF per datastore NFS vVols in un dominio di carico di lavoro VCF VI

Creare una Storage Virtual Machine (SVM) e più interfacce logiche (LIF) su un sistema ONTAP per supportare il traffico NFS per i datastore vVols in un dominio di carico di lavoro VMware Cloud Foundation VI.

Per aggiungere nuovi LIF a un SVM esistente, fare riferimento alla documentazione ONTAP : "[Creare ONTAP LIF](#)" .

Passi

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

Mostra esempio

The screenshot shows the ONTAP System Manager interface. On the left, there is a navigation sidebar with sections: DASHBOARD, INSIGHTS, STORAGE (expanded), Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas, Storage VMs (selected and highlighted in blue), and Tiers. The main content area is titled "Storage VMs". It features a large blue button labeled "+ Add" which is highlighted with a red box. Below this button is a table with a header row containing a checkbox and the word "Name". The table lists several SVM names: EHC_iSCSI, EHC, HMC_187, HMC_3510, HMC_iSCSI_3510, infra_svm_a300, JS_EHC_iSCSI, and OTVtest.

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

Mostra esempio

Add Storage VM

STORAGE VM NAME

IPSPACE

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

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

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)



Non è necessario selezionare la casella di controllo **Consenti accesso client NFS**. Gli ONTAP tools for VMware vSphere verranno utilizzati per automatizzare il processo di distribuzione del datastore, che include la fornitura dell'accesso client per gli host ESXi.

3. Nella sezione **Interfaccia di rete**, compilare **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, è possibile utilizzare impostazioni individuali oppure abilitare la casella di controllo per utilizzare impostazioni comuni per tutti i LIF rimanenti.

Mostra esempio

NETWORK INTERFACE
Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS: 172.21.118.119
SUBNET MASK: 24
GATEWAY: Add optional gateway
BROADCAST DOMAIN AND PORT: NFS_iSCSI

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

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS: 172.21.118.120
PORT: a0a-3374

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

Mostra esempio

Storage VM Administration

Manage administrator account

Save Cancel

Cosa succederà ora?

Dopo aver creato SVM e LIF, "[configurare la rete per NFS sugli host ESXi](#)" .

Configurare la rete per NFS su host ESXi in un dominio di carico di lavoro VCF VI

Configurare la rete NFS sugli host ESXi nei domini di gestione VMware Cloud Foundation per abilitare la connettività ai sistemi di archiviazione ONTAP . Creerai gruppi di porte

distribuiti con separazione VLAN, configurerai il teaming uplink per la ridondanza e imposterai gli adattatori VMkernel su ciascun host ESXi per stabilire percorsi NFS dedicati per le funzionalità di failover.

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

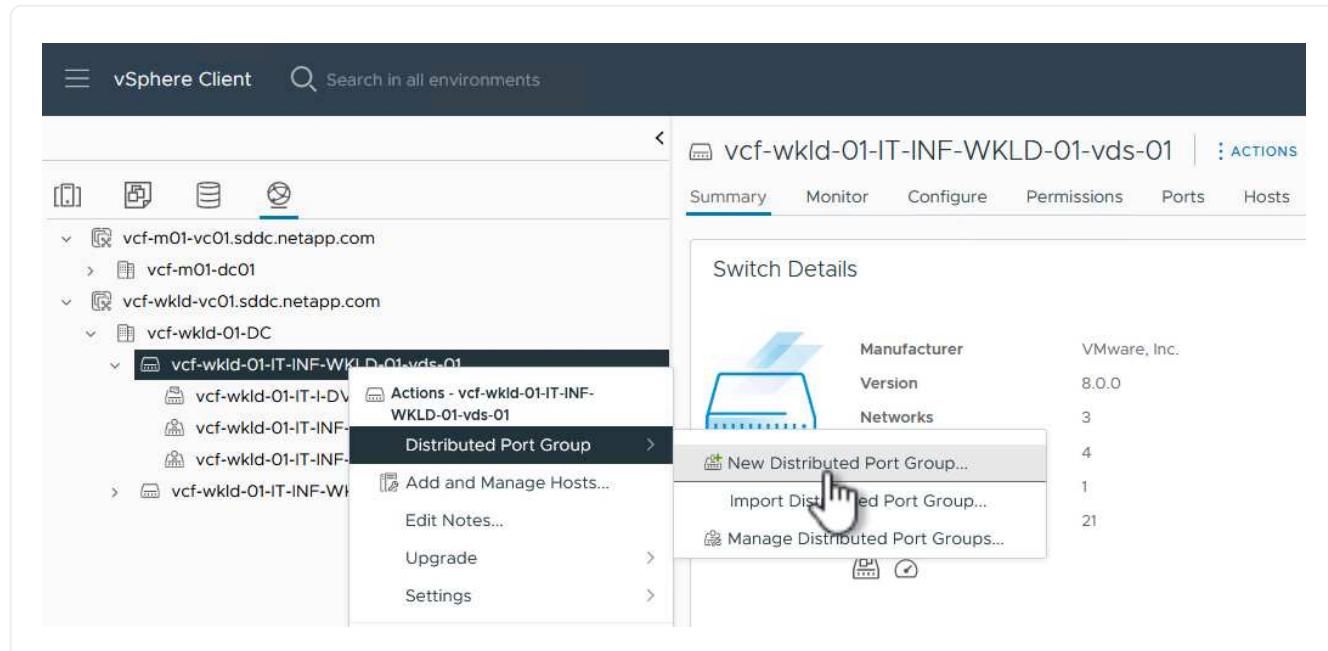
Passaggio 1: creare un gruppo di porte distribuito per il traffico NFS

Completare i seguenti passaggi per creare un nuovo gruppo di porte distribuito affinché la rete trasporti il traffico NFS.

Passi

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

Mostra esempio



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

Mostra esempio

The screenshot shows a configuration interface for creating a new distributed port group. On the left, a vertical navigation bar lists three steps: 1. Name and location, 2. Configure settings (which is selected and highlighted in dark grey), and 3. Ready to complete. The main panel is titled 'Configure settings' and contains the following fields:

- Port binding:** Static binding
- Port allocation:** Elastic (with a help icon)
- Number of ports:** 8
- Network resource pool:** (default)
- VLAN:**
 - VLAN type:** VLAN
 - VLAN ID:** 3374
- Advanced:** A checkbox labeled 'Customize default policies configuration' is unchecked.

At the bottom right of the main panel, there are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT' (highlighted with a blue border and a hand cursor icon).

- Nella pagina **Pronto per il completamento**, rivedere le modifiche e fare clic su **Fine** per creare il nuovo gruppo di porte distribuite.
- Una volta creato il gruppo di porte, accedi al gruppo di porte e seleziona l'azione **Modifica impostazioni...**.

Mostra esempio

The screenshot shows the vSphere Client interface. In the left sidebar, under the 'Network' category, there is a tree view of network resources. One item, 'vcf-wkld-01-nfs', is highlighted with a black rectangle and has a blue rectangular callout box pointing to it with the text 'Actions - vcf-wkld-01-nfs'. Inside this callout box, the 'Edit Settings...' option is also highlighted with a blue rectangle. On the right side of the screen, a detailed view of the selected port group is displayed. The title bar says 'vcf-wkld-01-nfs' and 'ACTIONS'. Below the title, there are tabs for 'Summary', 'Monitor', 'Configure', and 'Perf'. The 'Summary' tab is selected. A large section titled 'Distributed Port Group Details' contains several items, each with an icon and a label: 'Port binding' (switch icon), 'Port allocation' (switch icon), 'VLAN ID' (switch icon), 'Distributed switch' (switch icon), 'Network protocol profile' (gear icon), 'Network resource pool' (pool icon), 'Ports' (port icon), and 'Virtual machines' (vm icon). The 'vcf-wkld-01-nfs' item is also listed here.

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

Mostra esempio

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

General Load balancing Route based on originating virtual port

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
- uplink1

Standby uplinks

Unused uplinks

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

Passaggio 2: creare un adattatore VMkernel su ciascun host ESXi

Creare un adattatore VMkernel su ciascun host ESXi nel dominio del carico di lavoro.

Passi

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

Mostra esempio

vSphere Client Search in all environments

vcf-wkld-esx01.sddc.netapp.com ACTIONS

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Storage Storage Adapters Storage Devices Host Cache Configuration Protocol Endpoints I/O Filters

Networking Virtual switches VMkernel adapters

ADD NETWORKING... REFRESH

		Network Label
⋮	⇒	vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt
⋮	⇒	vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-motion
⋮	⇒	vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs
⋮	⇒	vmk10 --

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

Mostra esempio

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select connection type

Select a connection type to create.

VMkernel Network Adapter
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

Virtual Machine Port Group for a Standard Switch
A port group handles the virtual machine traffic on standard switch.

Physical Network Adapter
A physical network adapter handles the network traffic to other hosts on the network.

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

Mostra esempio

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		
<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-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input 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		8 items	

CANCEL **BACK** **NEXT**

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard. On the left, a vertical navigation bar lists steps 1 through 5: 'Select connection type', 'Select target device', 'Port properties', 'IPv4 settings' (which is highlighted in dark blue), and 'Ready to complete'. The main panel is titled 'IPv4 settings' with the sub-instruction 'Specify VMkernel IPv4 settings.' It contains the following configuration:

<input type="radio"/> Obtain IPv4 settings automatically	
<input checked="" type="radio"/> Use static IPv4 settings	
IPv4 address	172.21.118.145
Subnet mask	255.255.255.0
Default gateway	<input type="checkbox"/> Override default gateway for this adapter 172.21.166.1
DNS server addresses	10.61.185.231

At the bottom right are three buttons: 'CANCEL', 'BACK' (disabled), and 'NEXT'.

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard. The left navigation bar highlights 'Ready to complete'. The main panel is titled 'Ready to complete' with the sub-instruction 'Review your selections before finishing the wizard'. It displays the following summary of selected port properties:

Select target device	
Distributed port group	vcf-wkld-01-nfs
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Port properties	
New port group	vcf-wkld-01-nfs (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

At the bottom right are three buttons: 'CANCEL', 'BACK' (disabled), and 'FINISH'.

Cosa succederà ora?

Dopo aver configurato la rete per NFS su tutti gli host ESXi nel dominio del carico di lavoro, "[configurare l'archiviazione per NFS vVols](#)" .

Configurare l'archiviazione NFS vVols in un dominio di carico di lavoro VCF VI utilizzando gli strumenti ONTAP

Configurare l'archiviazione NFS vVols in un dominio di carico di lavoro VI. Dopo aver distribuito gli ONTAP tools for VMware vSphere, utilizzerai l'interfaccia client vSphere per aggiungere il sistema di storage, creare un profilo di capacità di storage e predisporre un datastore vVols .

Passaggio 1: distribuire gli ONTAP tools for VMware vSphere

Per i domini del carico di lavoro VI, gli strumenti ONTAP vengono installati nel cluster di gestione VCF ma registrati con il vCenter associato al dominio del carico di lavoro VI.

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

Passi

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

Mostra esempio

The screenshot shows the vSphere Client interface. In the left navigation pane, under 'vcf-m01-vc01.sddc.netapp.com' > 'vcf-m01-dc01', the 'vcf-m01-cl01' cluster is selected. A context menu is open over the cluster name, listing actions: 'Actions - vcf-m01-cl01', 'Add Hosts...', 'New Virtual Machine...', 'New Resource Pool...', 'Deploy OVF Template...', and 'New vApp'. The 'Deploy OVF Template...' option is highlighted with a mouse cursor.

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

Mostra esempio

The screenshot shows the 'Deploy OVF Template' wizard. Step 1, 'Select an OVF template', is active. It displays instructions to select an OVF template from a remote URL or local file system. Two options are shown: 'URL' (with a field containing 'http://remoteserver-address/filetodeploy.ovf') and 'Local file' (with a 'UPLOAD FILES' button and a file path 'netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova').

5. Per i passaggi da 2 a 5 della procedura guidata, seleziona un nome e una cartella per la VM, seleziona la risorsa di elaborazione, rivedi i dettagli e accetta 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.

Mostra esempio

The screenshot shows the 'Deploy OVF Template' wizard at step 6: 'Select storage'. A table lists storage options:

Name	Storage Compatibility	Capacity	Provisioned	Free	Type
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	Virtual Machine Disk
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	Virtual Machine Disk
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	Virtual Machine Disk
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	Virtual Machine Disk
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	Virtual Machine Disk

Buttons at the bottom include 'Manage Columns', 'Items per page: 10', and '5 items'.

7. Nella pagina **Selezione rete**, seleziona la rete utilizzata per la gestione del traffico.

Mostra esempio

The screenshot shows the 'Deploy OVF Template' wizard at step 7: 'Select networks'. A table maps source networks to destination networks:

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan vcf-m01-cl01-vds01-pg-vsan SDDC-DPortGroup-VM-Mgmt Browse ...

Buttons at the bottom include 'Manage Columns' and '1 item'.

8. Nella pagina **Personalizza modello**, inserisci tutte le informazioni richieste:

- Password da utilizzare per l'accesso amministrativo agli strumenti ONTAP .
- Indirizzo IP del server NTP.
- Password dell'account di manutenzione degli strumenti ONTAP .
- Password del database Derby degli strumenti ONTAP .
- Non selezionare la casella per **Abilitare VMware Cloud Foundation (VCF)**. La modalità VCF non è richiesta per distribuire storage supplementare.
- FQDN o indirizzo IP dell'appliance vCenter per il **dominio del carico di lavoro VI**
- Credenziali per l'appliance vCenter del **VI Workload Domain**
- Proprietà di rete richieste.

9. Fare clic su **Avanti** per continuare.

Mostra esempio

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template**
- Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration 4 settings

Application User Password (*) 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:

Confirm Password:

NTP Servers 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

Maintenance User Password (*) Password to assign to maint user account.

Password:

Confirm Password:

Configure vCenter or Enable VCF 3 settings

Enable VMware Cloud Foundation (VCF) vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*) Specify the IP address/hostname of an existing vCenter to register to.
cf-wkld-vc01.sddc.netapp.com

Port (*) Specify the HTTPS port of an existing vCenter to register to.
443

Username (*) Specify the username of an existing vCenter to register to.
administrator@vsphere.local

Password (*) Specify the password of an existing vCenter to register to.

Password:

Confirm Password:

Network Properties 8 settings

Host Name Specify the hostname for the appliance. (Leave blank if DHCP is desired)
vcf-w01-otv9

IP Address Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL **BACK** **NEXT**

10. Esaminare tutte le informazioni nella pagina **Pronto per il completamento**, quindi fare clic su **Fine** per iniziare a distribuire l'appliance degli strumenti ONTAP .

Passaggio 2: aggiungere un sistema di archiviazione

Per aggiungere un sistema di archiviazione utilizzando gli strumenti ONTAP , procedere come segue.

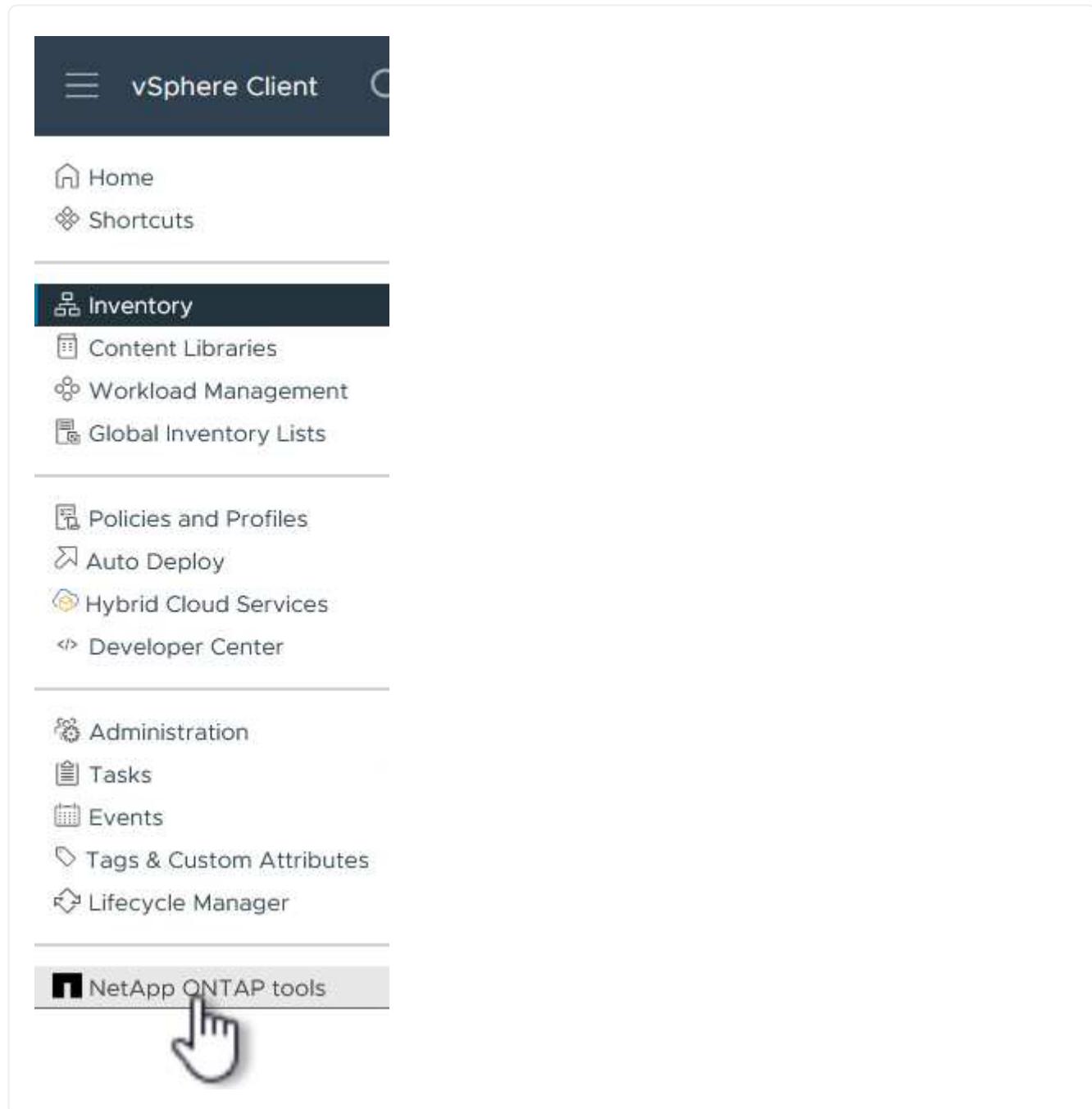


vVol richiede le credenziali del cluster ONTAP anziché le credenziali SVM. Per ulteriori informazioni, fare riferimento alla documentazione degli ONTAP tools for VMware vSphere : ["Aggiungere sistemi di archiviazione"](#) .

Passi

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

Mostra esempio



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

Mostra esempio

The screenshot shows the vSphere Client interface with the following details:

- Header:** vSphere Client, Search in all environments, and user account information.
- Breadcrumbs:** NetApp ONTAP tools INSTANCE 172.21.166.139:8443
- Left Sidebar (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
- Main Content Area:**
 - Section Title:** ONTAP tools for VMware vSphere
 - Sub-sections:** Getting Started, Traditional Dashboard, vVols Dashboard
 - Description:** 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.
 - Buttons:** Add Storage System (with a hand cursor icon), Provision Datastore (green button).
 - Links:** Add storage systems to ONTAP tools for VMware vSphere, Create traditional or vVols datastores.
 - 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
 - Next Steps:**
 - View Dashboard**: View and monitor the datastores in ONTAP tools for VMware vSphere.
 - Settings**: Configure administrative settings such as credentials, alarm thresholds.
 - Resources:**
 - ONTAP tools for VMware vSphere Documentation Resources
 - RBAC User Creator for Data ONTAP
 - ONTAP tools for VMware vSphere REST API Documentation

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

Mostra esempio

Add Storage System

i 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

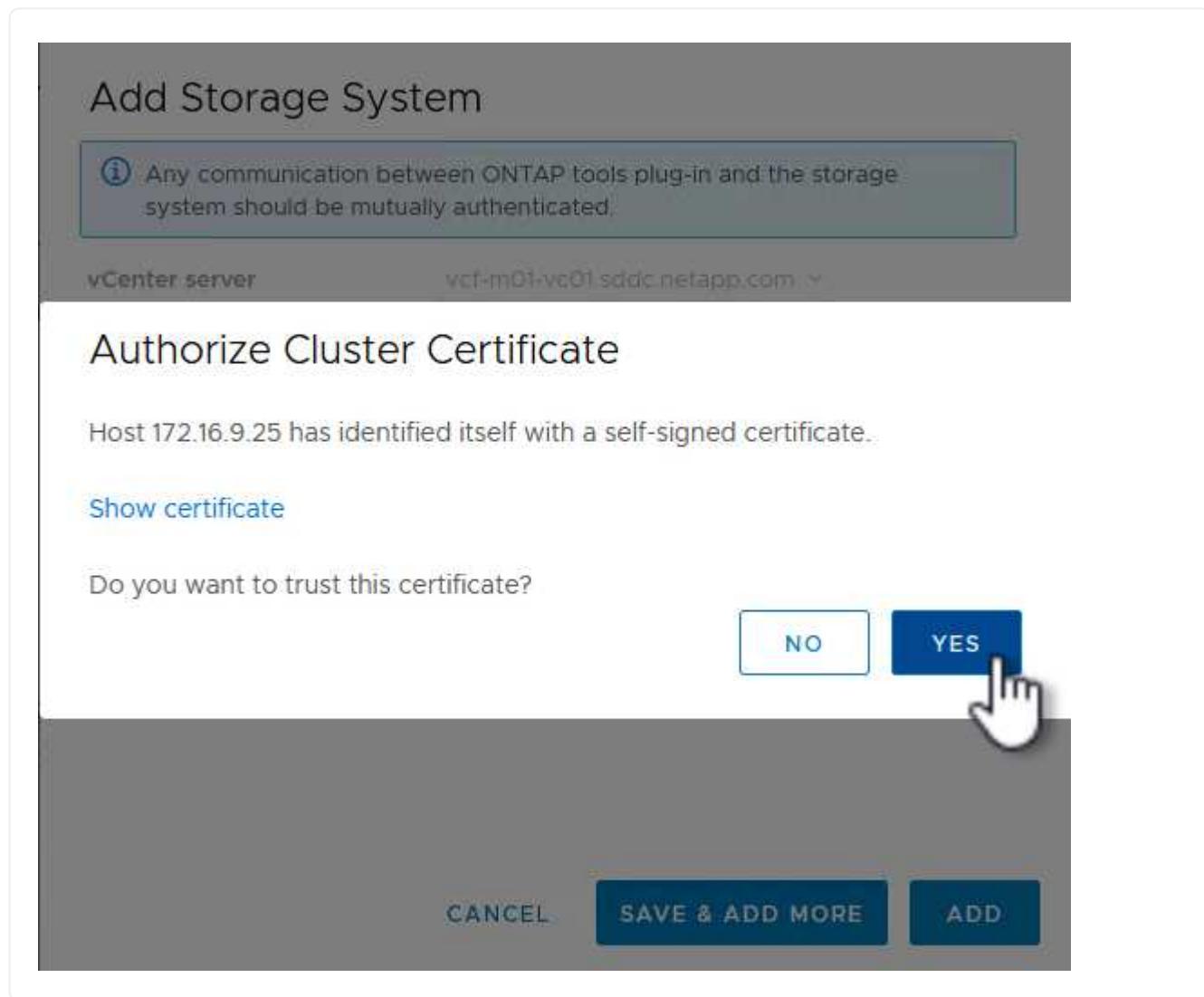
SAVE & ADD MORE

ADD



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

Mostra esempio



Passaggio 3: creare un datastore NFS negli strumenti ONTAP

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

Passi

1. Negli strumenti ONTAP selezionare **Panoramica** e dalla scheda **Introduzione** fare clic su **Provisioning** per avviare la procedura guidata.

Mostra esempio

The screenshot shows the vSphere Client interface with the NetApp ONTAP tools plugin. The left sidebar has a tree view with 'Overview' selected. The main content area is titled 'ONTAP tools for VMware vSphere' and includes tabs for 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. Below the tabs, there's a brief description of the plugin. Two large buttons are present: 'Add Storage System' and 'Provision Datastore'. The 'Provision Datastore' button is highlighted with a blue border.

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



Selezionando **Distribuisci i dati del datastore nel cluster**, il volume sottostante verrà creato come volume FlexGroup , il che impedisce l'utilizzo dei profili di capacità di archiviazione. Fare riferimento a "[Configurazioni supportate e non supportate per i volumi FlexGroup](#)" per ulteriori informazioni sull'utilizzo di FlexGroup Volumes.

Mostra esempio

The screenshot shows the 'General' step of the 'New Datastore' wizard. On the left, a navigation bar lists steps 1 through 4. Step 1, 'General', is selected and highlighted in blue. The main area is titled 'General' and contains the following fields:

- Provisioning destination:** vcf-wkld-01-DC [BROWSE](#)
- Type:** NFS VMFS vVols
- Name:** VCF_WKLD_05_NFS
- Size:** 2 TB
- Protocol:** NFS 3 NFS 4.1
- Distribute datastore data across the ONTAP cluster.
- Use storage capability profile for provisioning

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

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

Mostra esempio

The screenshot shows the 'Storage system' step of the 'New Datastore' wizard. The navigation bar on the left shows step 2, 'Storage system', is selected. The main area is titled 'Storage system' and contains the following fields:

- Storage capability profile:** Platinum_AFF_A
- Storage system:** ntaphci-a300e9u25 (172.16.9.25)
- Storage VM:** VCF_NFS

7. Nella pagina **Attributi di archiviazione**, seleziona l'aggregato da utilizzare, quindi fai clic su **Avanti** per continuare.

Mostra esempio

The screenshot shows the 'Storage attributes' step of the 'New Datastore' wizard. On the left, a vertical navigation bar lists steps 1 through 4: General, Storage system, Storage attributes (which is selected and highlighted in blue), and Summary. The main pane is titled 'Storage attributes' and contains the instruction 'Specify the storage details for provisioning the datastore.' It shows an 'Aggregate:' dropdown set to 'EHCAggr02 - (25350.17 GB Free)', a 'Volumes:' dropdown set to 'Automatically creates a new volume.', and a link 'Advanced options >'. A green vertical bar on the left indicates the current step.

8. Rivedere il **Riepilogo** e fare clic su **Fine** per iniziare a creare il datastore NFS.

Mostra esempio

The screenshot shows the 'Summary' step of the 'New Datastore' wizard. The left navigation bar shows steps 1 through 4: General, Storage system, Storage attributes (selected and highlighted in blue), and Summary. The main pane is titled 'Summary' and contains three sections: 'General', 'Storage system details', and 'Storage attributes'. The 'General' section lists: vCenter server: vcf-wkld-vc01.sddc.netapp.com, Provisioning destination: vcf-wkld-01-DC, Datastore name: VCF_WKLD_05_NFS, Datastore size: 2 TB, Datastore type: NFS, Protocol: NFS 3, Datastore cluster: None, and Storage capability profile: Platinum_AFF_A. The 'Storage system details' section lists: Storage system: ntaphci-a300e9u25 and SVM: VCF_NFS. The 'Storage attributes' section lists: Aggregate: EHCAggr02. At the bottom right are 'CANCEL', 'BACK', and 'FINISH' buttons.

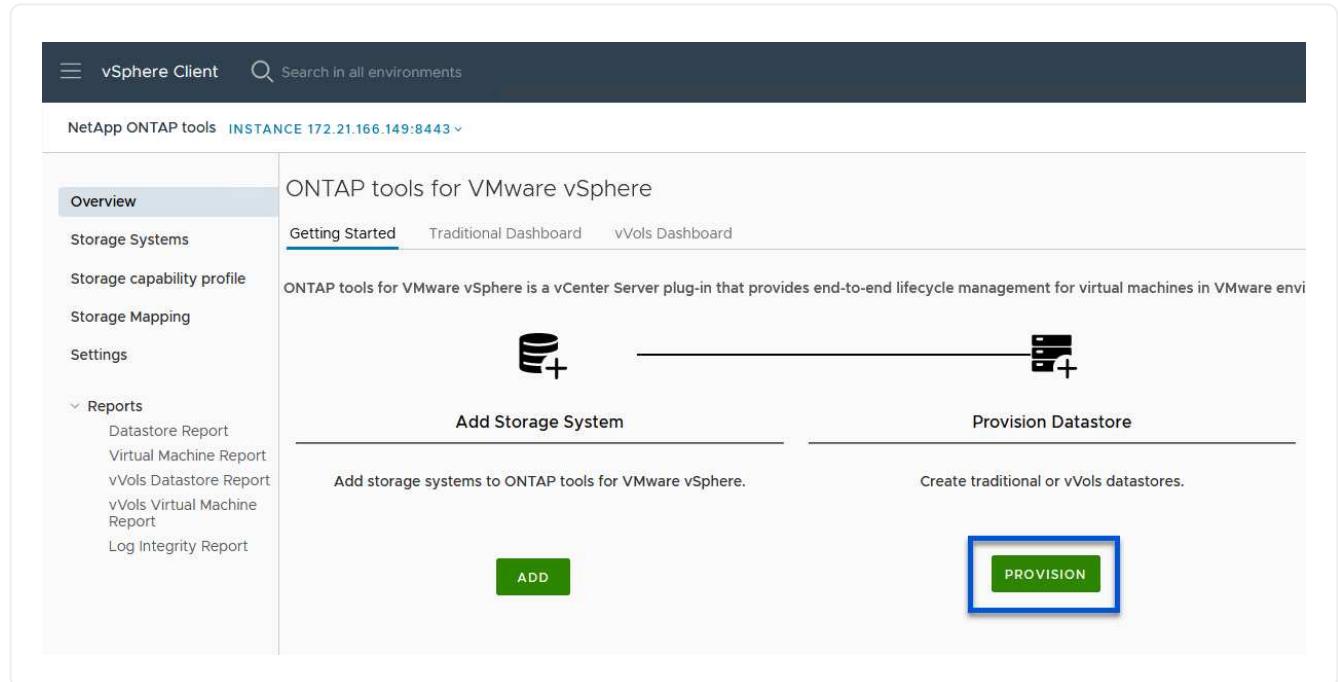
Passaggio 4: creare un datastore vVols negli strumenti ONTAP

Per creare un datastore vVols negli strumenti ONTAP , completare i seguenti passaggi.

Passi

1. Negli strumenti ONTAP , selezionare **Panoramica** e dalla scheda **Introduzione** fare clic su **Provisioning** per avviare la procedura guidata.

Mostra esempio



NetApp ONTAP tools INSTANCE 172.21.166.149:8443

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

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

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

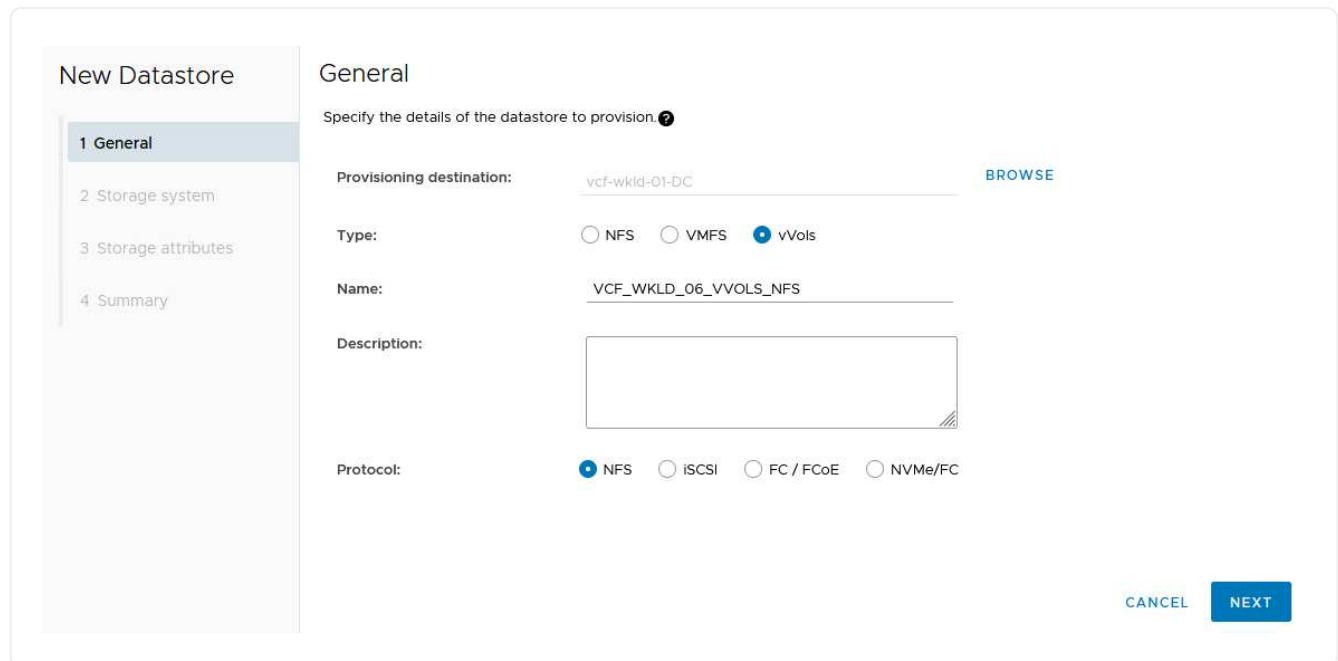
Add Storage System Provision Datastore

Add storage systems to ONTAP tools for VMware vSphere. Create traditional or vVols datastores.

ADD PROVISION

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

Mostra esempio



New Datastore

General

Specify the details of the datastore to provision. [?](#)

Provisioning destination: vcf-wkld-01-DC [BROWSE](#)

Type: NFS VMFS vVols

Name: VCF_WKLD_06_VVOLS_NFS

Description:

Protocol: NFS iSCSI FC / FCoE NVMe/FC

CANCEL NEXT

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

Mostra esempio

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 profile: Platinum_AFF_A

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_NFS

7. Nella pagina **Attributi di archiviazione**, seleziona **Crea nuovi volumi** e immetti gli attributi di archiviazione del volume da creare.

Mostra esempio

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vv	2000	Platinum_AFF_A	EHCAGgr02 - (25404 GB)	Thin

ADD

8. Fare clic su **Aggiungi** per creare il volume e quindi su **Avanti** per continuare.

Mostra esempio

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
vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCAGgr02

1 - 1 of 1 item

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCAGgr02 - (25407.15 G)	Thin

Default storage capability profile: Platinum_AFF_A

ADD

NEXT

9. Rivedere la pagina **Riepilogo** e fare clic su **Fine** per avviare il processo di creazione del datastore vVol.

Mostra esempio

The screenshot shows the 'Summary' step of a 'New Datastore' wizard. On the left, a vertical navigation bar lists steps: 1 General, 2 Storage system, 3 Storage attributes, and 4 Summary (which is highlighted). The main area displays 'General' settings:

vCenter server:	vcf-wkld-vc01.sddc.netapp.com
Provisioning destination:	vcf-wkld-01-DC
Datastore name:	VCF_WKLD_06_VVOLS_NFS
Datastore type:	vVols
Protocol:	NFS
Storage capability profile:	Platinum_AFF_A

Below this are sections for 'Storage system details' and 'Storage attributes'. The 'Storage attributes' section contains four tabs: 'New FlexVol Name' (selected), 'New FlexVol Size', 'Aggregate', and 'Storage Capability Profile'. At the bottom right are 'CANCEL', 'BACK', and 'FINISH' buttons.

Informazioni aggiuntive

- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a "[Documentazione ONTAP 9](#)" .
- Per informazioni sulla configurazione di VCF, fare riferimento a "[Documentazione di VMware Cloud Foundation](#)" .
- Per informazioni sulla distribuzione e l'utilizzo degli strumenti ONTAP in più ambienti vCenter, fare riferimento a "[Requisiti per la registrazione degli strumenti ONTAP in più ambienti server vCenter](#)" .
- Per demo video di questa soluzione, fare riferimento a "[Provisioning del datastore VMware](#)" .

Espandi i domini del carico di lavoro VI con NVMe/TCP

Flusso di lavoro di distribuzione per l'aggiunta di datastore vVols NVMe come storage supplementare in un dominio di carico di lavoro VI

Inizia aggiungendo datastore NVMe/TCP vVols come storage supplementare per un dominio di carico di lavoro VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Esaminerai i requisiti di distribuzione, configurerai SVM e LIF abilitati per NVMe/TCP, configurerai la rete host ESXi e distribuirai il datastore NVMe/TCP.

1

"[Esaminare i requisiti di distribuzione](#)"

Esaminare i requisiti per distribuire un datastore NVMe/TCP in un dominio di carico di lavoro VMware Cloud Foundation VI.

2

"[Creare SVM e LIF e lo spazio dei nomi NVMe](#)"

Creare una macchina virtuale di archiviazione con interfacce logiche e lo spazio dei nomi NVMe per il traffico

NVMe/TCP.

3

"Configurare la rete"

Creare gruppi di porte distribuiti e adattatori vmkernel sugli host ESXi per il dominio del carico di lavoro VI.

4

"Configurare l'archiviazione"

Distribuire il datastore NVMe/TCP.

Requisiti di distribuzione per NVMe vVols in un dominio di carico di lavoro VI

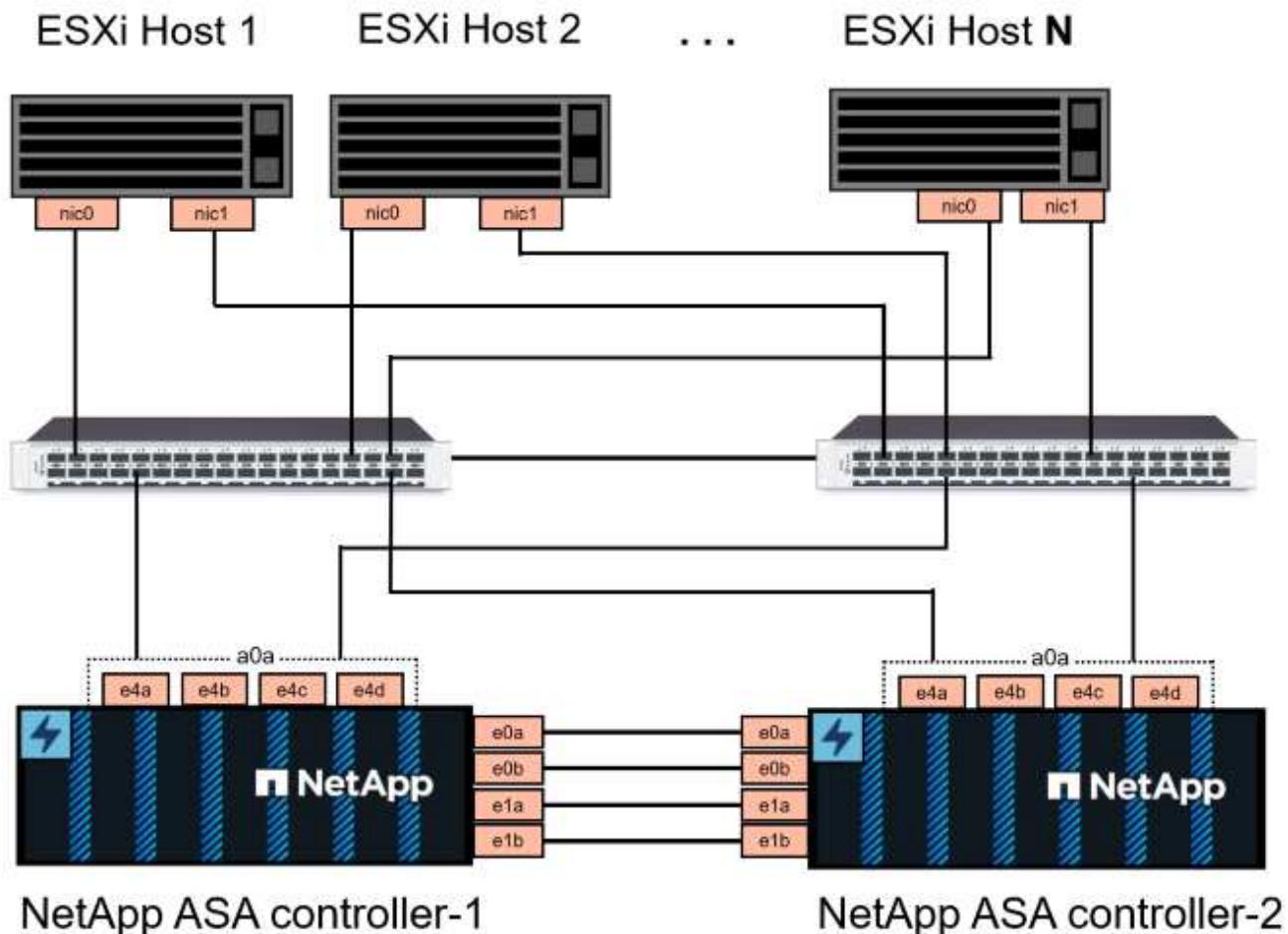
Esaminare i requisiti di progettazione e infrastruttura di rete consigliati per distribuire NVMe vVols in un dominio di carico di lavoro VMware Cloud Foundation VI. È necessario un sistema di archiviazione ONTAP AFF o ASA completamente configurato, un dominio di gestione VCF distribuito e un dominio di carico di lavoro VI esistente.

Requisiti infrastrutturali

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

Progettazione di rete NVMe/TCP consigliata

NetApp consiglia progettazioni di rete completamente ridondanti per NVMe/TCP. Il diagramma seguente illustra un esempio di configurazione ridondante, che garantisce tolleranza agli errori per sistemi di archiviazione, switch, adattatori di rete e sistemi host.



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

Cosa succederà ora?

Dopo aver esaminato i requisiti di distribuzione, ["creare SVM e LIF"](#) .

Creare SVM e LIF e lo spazio dei nomi NVMe per i datastore NVMe/TCP vVols in un dominio di carico di lavoro VCF VI

Crea una macchina virtuale di archiviazione (SVM) con più interfacce logiche (LIF) per fornire connettività NVMe ai domini di carico di lavoro VMware Cloud Foundation. Questa procedura riassume la configurazione di una SVM e di LIF abilitati per NVMe/TCP e la creazione degli spazi dei nomi NVMe.

Passaggio 1: creare gli SVM e i LIF

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

Per aggiungere nuovi LIF a un SVM esistente, fare riferimento alla documentazione ONTAP :["Creare ONTAP LIF"](#) .

Passi

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

Mostra esempio

The screenshot shows the ONTAP System Manager interface. On the left, there's a sidebar with sections: DASHBOARD, INSIGHTS, STORAGE (with Overview, Volumes, LUNs, Consistency Groups, NVMe Namespaces, Shares, Buckets, Qtrees, Quotas, Storage VMs, and Tiers), and a bottom section for Tiers. The Storage VMs section is highlighted with a blue background. The main area is titled "Storage VMs" and contains a list of existing SVMs. A large blue button labeled "+ Add" is positioned above the list. The list includes: EHC_iSCSI, EHC, HMC_187, HMC_3510, HMC_iSCSI_3510, infra_svm_a300, JS_EHC_iSCSI, and OTVtest. Each item in the list has a small checkbox icon to its left.

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

[Mostra esempio](#)

Add Storage VM

X

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**, immettere **Indirizzo IP**, **Maschera di sottorete** e **Dominio di broadcast e porta** per il primo LIF. Per i LIF successivi, è possibile utilizzare impostazioni individuali oppure abilitare la casella di controllo per utilizzare impostazioni comuni per tutti i LIF rimanenti.



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

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

[Mostra esempio](#)

Storage VM Administration

Manage administrator account

Save

[Cancel](#)

Passaggio 2: creare lo spazio dei nomi NVMe

Gli spazi dei nomi NVMe sono analoghi ai LUN per iSCSi o FC. È necessario creare lo spazio dei nomi NVMe

prima di poter distribuire un datastore VMFS da vSphere Client.

Per creare lo spazio dei nomi NVMe, ottenere il nome qualificato NVMe (NQN) da ciascun host ESXi nel cluster. ONTAP utilizza l'NQN per fornire il controllo di accesso allo spazio dei nomi.

Passi

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

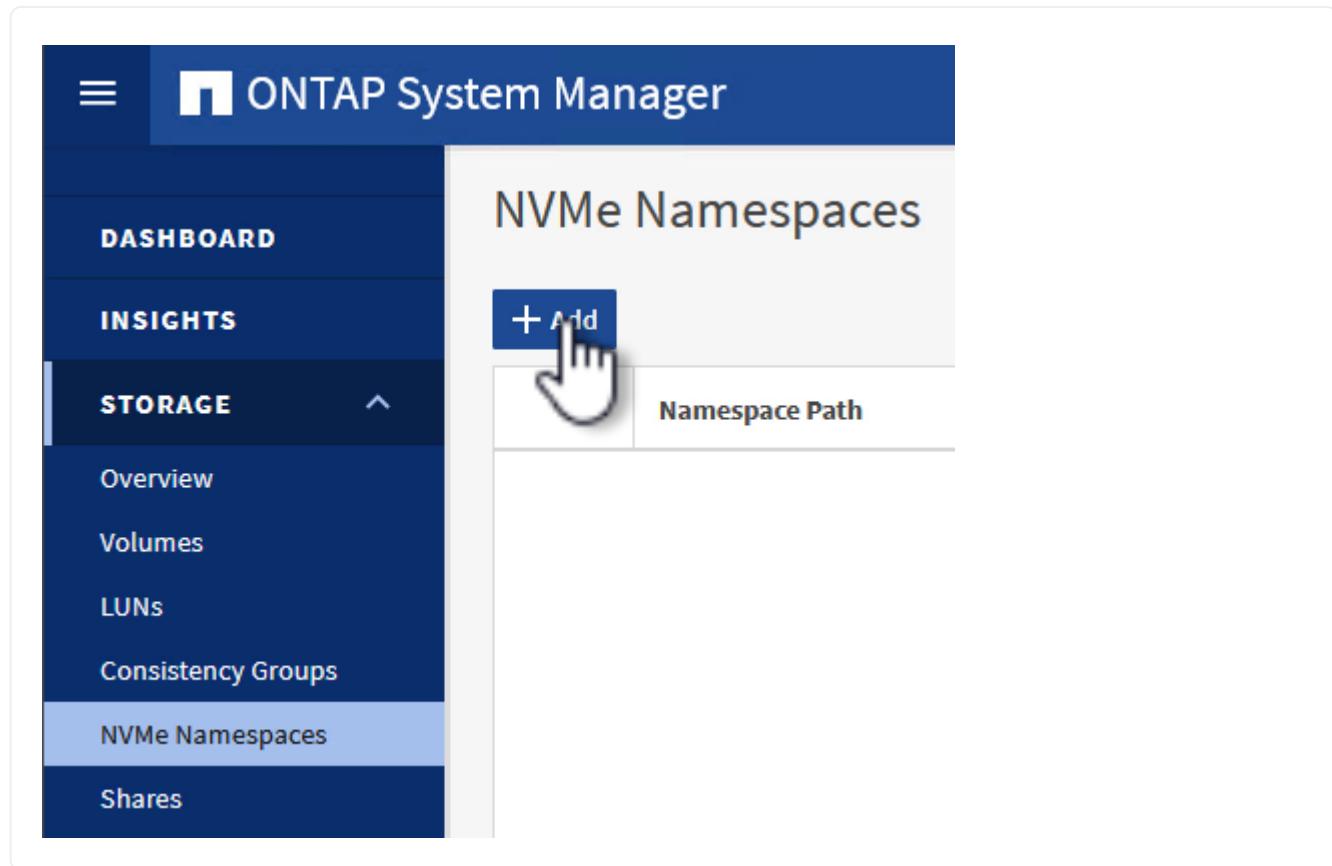
```
esxcli nvme info get
```

Dovrebbe essere visualizzato un output simile al seguente esempio:

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

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

Mostra esempio



4. Nella pagina **Aggiungi spazio dei nomi NVMe**, inserisci un prefisso del nome, il numero di spazi dei nomi da creare, la dimensione dello spazio dei nomi e il sistema operativo host che accederà allo spazio dei nomi.
5. Nella sezione **Host NQN**, creare un elenco separato da virgole degli NQN precedentemente raccolti dagli

host ESXi che accederanno agli spazi dei nomi.

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

Mostra esempio

The screenshot shows the ONTAP System Manager interface. The left sidebar has a 'DASHBOARD' section, followed by 'INSIGHTS', 'STORAGE' (which is expanded to show 'Overview', 'Volumes', 'LUNs', 'Consistency Groups', 'NVMe Namespaces', and 'Shares'). The 'NVMe Namespaces' item is highlighted with a blue background. The main content area is titled 'NVMe Namespaces' and features a large '+ Add' button with a hand cursor icon over it. Below the button is a 'Namespace Path' field.

Cosa succederà ora?

Dopo aver creato SVM e LIF, "configurare la rete per NVMe/TCP (NVMe/TCP) vVols".

Configurare la rete per NVMe/TCP su host ESXi in un dominio di carico di lavoro VCF VI

Configurare la rete per l'archiviazione NVMe su TCP (NVMe/TCP) sugli host ESXi in un dominio di carico di lavoro VI. Creerai gruppi di porte distribuiti per il traffico NVMe, configurerai adattatori VMkernel su ciascun host ESXi e aggiungerai un adattatore NVMe/TCP per abilitare connettività affidabile e multipathing.

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

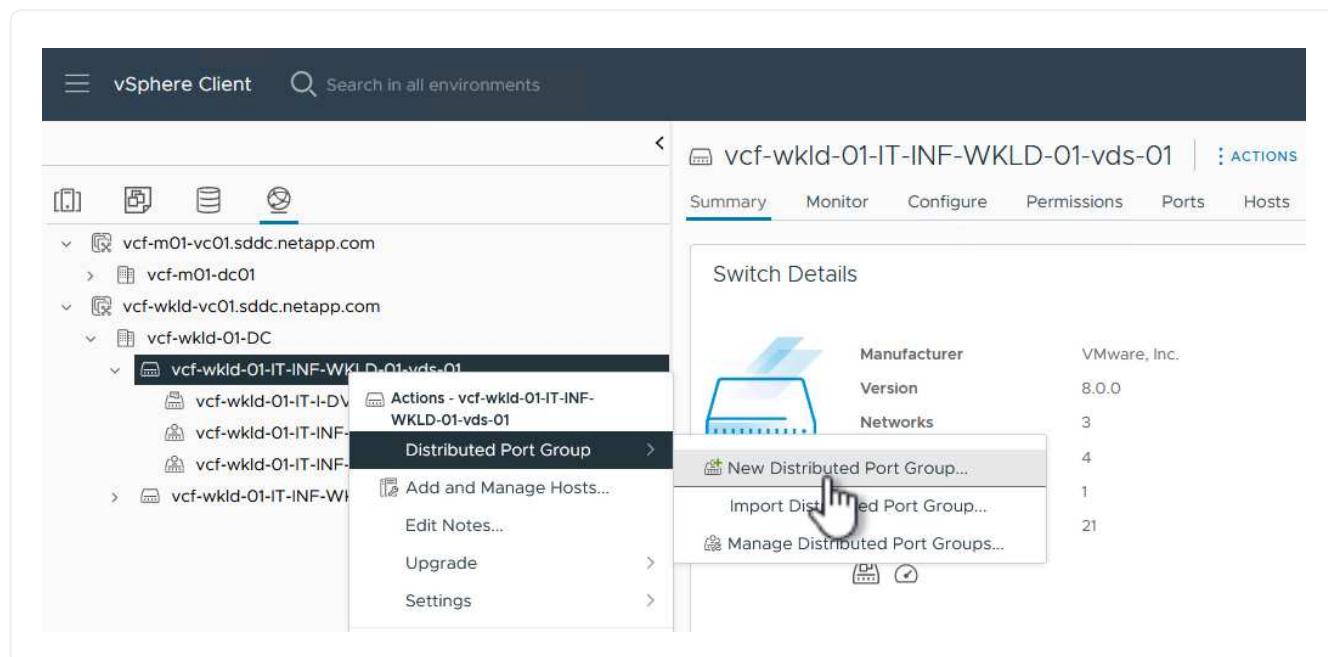
Passaggio 1: creare gruppi di porte distribuiti per il traffico NVME/TCP

Completare i seguenti passaggi per creare un nuovo gruppo di porte distribuito per ciascuna rete NVMe/TCP.

Passi

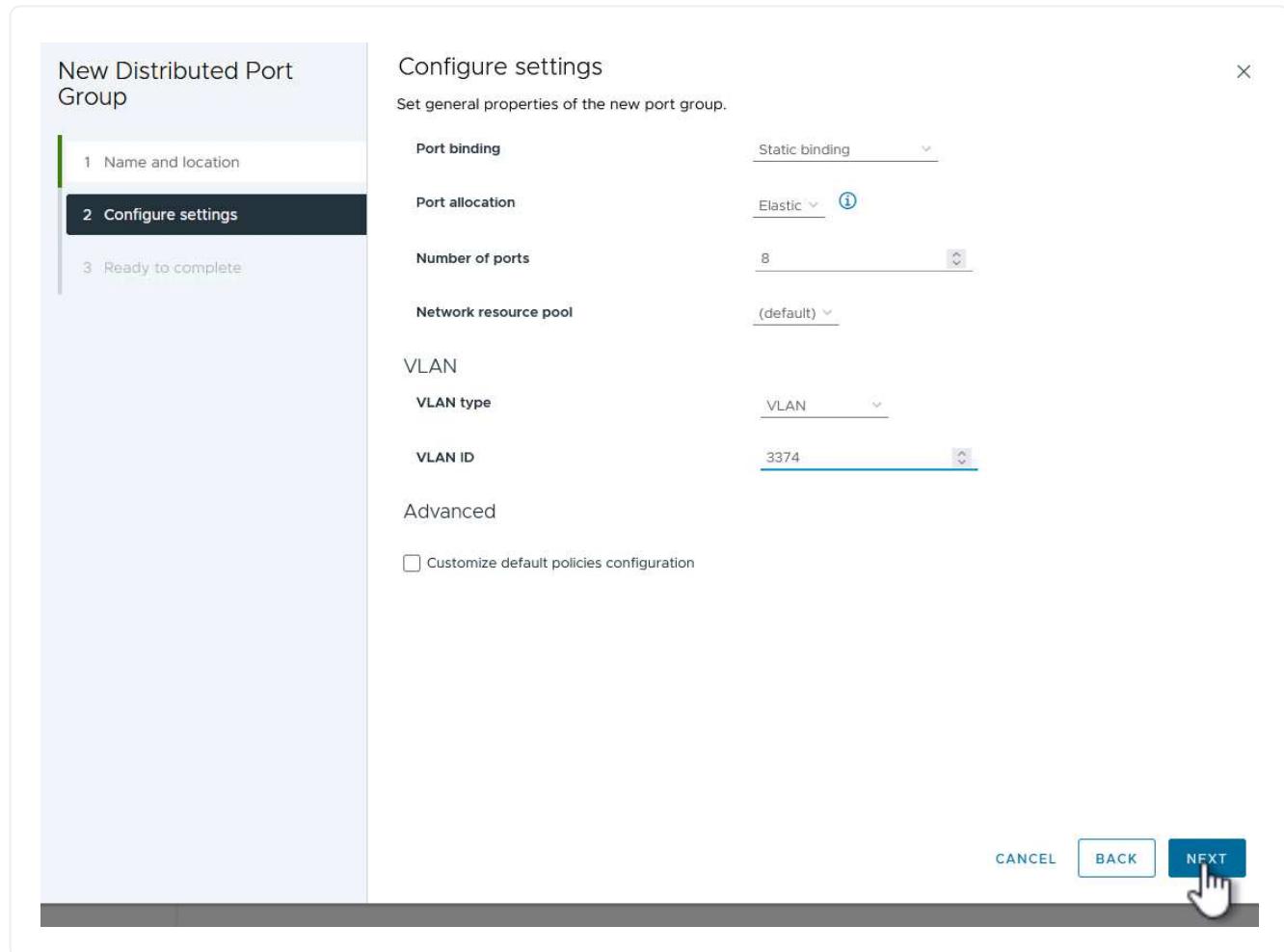
1. Dal client vSphere, accedere a **Inventario > Rete** per il dominio del carico di lavoro. Passare allo switch distribuito esistente e scegliere l'azione per creare **Nuovo gruppo di porte distribuite....**

Mostra esempio



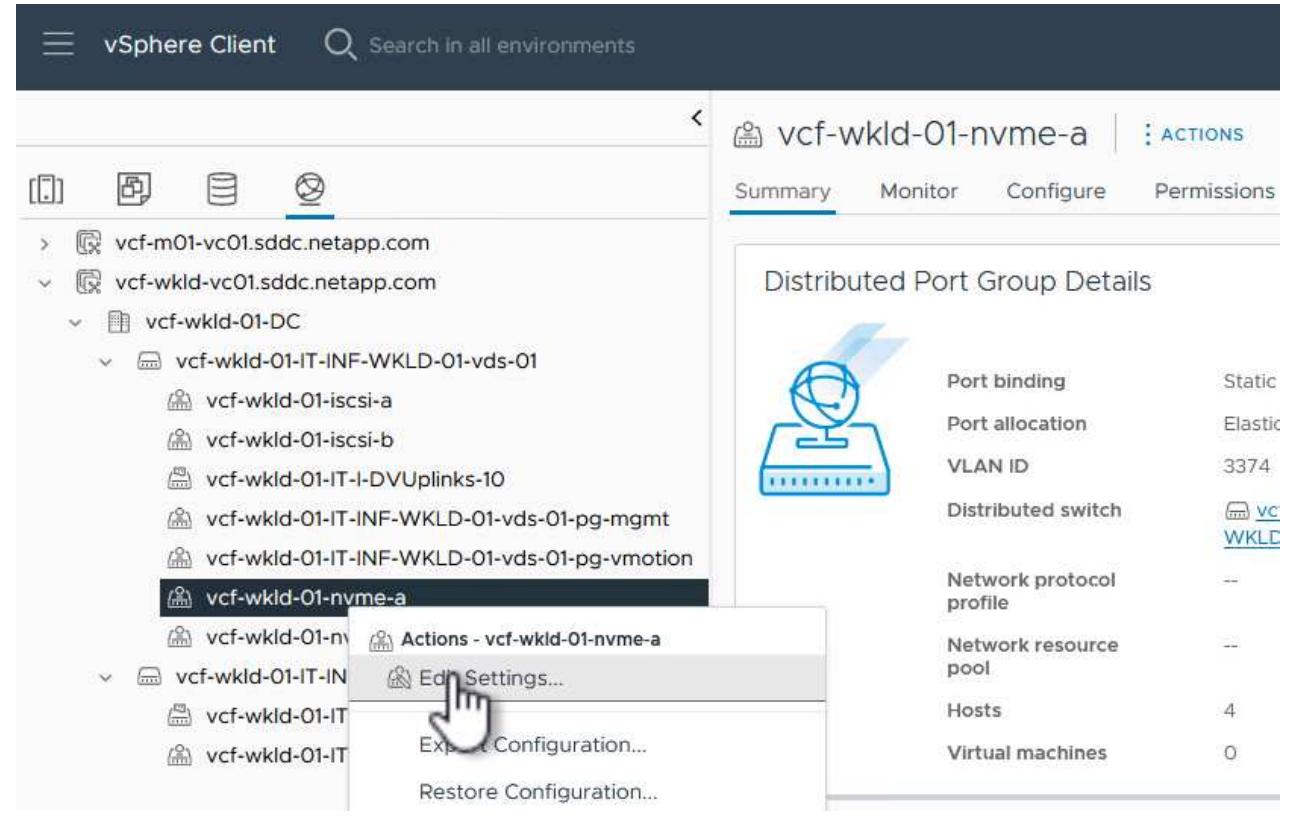
2. Nella procedura guidata **Nuovo gruppo di porte distribuite**, inserisci un nome per il nuovo gruppo di porte e fai clic su **Avanti** per continuare.
3. Nella pagina **Configura impostazioni**, compila tutte le impostazioni. Se si utilizzano le VLAN, assicurarsi di fornire l'ID VLAN corretto. Fare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

Mostra esempio



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

Mostra esempio



The screenshot shows the vSphere Client interface. On the left, a navigation tree lists various hosts and datacenters. In the center, a detailed view of a 'Distributed Port Group Details' for 'vcf-wkld-01-nvme-a' is displayed. On the right, a context menu titled 'Actions - vcf-wkld-01-nvme-a' is open, with 'Edit Settings...' being selected. The 'Edit Settings...' option is highlighted with a blue rectangle and has a hand cursor icon pointing at it.

Setting	Value
Port binding	Static
Port allocation	Elastic
VLAN ID	3374
Distributed switch	VC WKLD
Network protocol profile	--
Network resource pool	--
Hosts	4
Virtual machines	0

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

Mostra esempio

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-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	Failover order ⓘ	
Miscellaneous	MOVE UP MOVE DOWN	
	Active uplinks	
	uplink1	
	Standby uplinks	
	Unused uplinks	
	uplink2	

8. Ripetere questo passaggio per il secondo gruppo di porte NVMe/TCP. Questa volta, sposta **uplink1** in basso a **Uplink non utilizzati**.

Mostra esempio

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

General	Load balancing	Route based on originating virtual port
Advanced	Network failure detection	Link status only
VLAN	Notify switches	Yes
Security	Fallback	Yes
Traffic shaping		
Teaming and failover		
Monitoring	Failover order ①	
Miscellaneous	MOVE UP MOVE DOWN	
	Active uplinks	
	uplink2	
	Standby uplinks	
	Unused uplinks	
	uplink1	

Passaggio 2: creare gli adattatori VMkernel su ciascun host ESXi

Creare gli adattatori VMkernel su ciascun host ESXi nel dominio del carico di lavoro.

Passi

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

Mostra esempio

vSphere Client Search in all environments

vcf-wkld-esx01.sddc.netapp.com ACTIONS

Summary	Monitor	Configure	Permissions	VMs	Datastores	Networks	Updates															
Storage																						
Storage Adapters																						
Storage Devices																						
Host Cache Configuration																						
Protocol Endpoints																						
I/O Filters																						
Networking																						
Virtual switches																						
VMkernel adapters																						
ADD NETWORKING... REFRESH																						
<table border="1"><thead><tr><th></th><th></th><th>Network Label</th></tr></thead><tbody><tr><td>:</td><td>>></td><td>vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nmgt</td></tr><tr><td>:</td><td>>></td><td>vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion</td></tr><tr><td>:</td><td>>></td><td>vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs</td></tr><tr><td>:</td><td>>></td><td>vmk10 --</td></tr></tbody></table>										Network Label	:	>>	vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nmgt	:	>>	vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion	:	>>	vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs	:	>>	vmk10 --
		Network Label																				
:	>>	vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nmgt																				
:	>>	vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion																				
:	>>	vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs																				
:	>>	vmk10 --																				

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

continuare.

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select connection type'. A sidebar on the left lists steps: 1. Select connection type (highlighted in dark grey), 2. Select target device, 3. Port properties, 4. IPv4 settings, and 5. Ready to complete. The main panel displays three options:

- VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard with the title 'Select target device'. A sidebar on the left lists steps: 1. Select connection type, 2. Select target device (highlighted in dark grey), 3. Port properties, 4. IPv4 settings, and 5. Ready to complete. The main panel displays a 'Quick Filter' input field and a table of target devices:

Name	NSX Port Group ID	Distributed Switch
vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nmgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
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
vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons. The 'NEXT' button has a hand cursor icon pointing at it.

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

Mostra esempio

The screenshot shows the 'Port properties' step of the 'Add Networking' wizard. On the left, a vertical navigation bar lists steps 1 through 5. Step 3, 'Port properties', is highlighted with a dark background. The main panel contains fields for 'Network label' (set to 'vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)'), 'MTU' (set to 'Get MTU from switch' with a value of 9000), and 'TCP/IP stack' (set to 'Default'). Below these, a section titled 'Available services' lists several options with checkboxes. The 'vSphere Replication over TCP' checkbox is checked. At the bottom right, there are 'CANCEL', 'BACK', and 'NEXT' buttons, with a hand cursor pointing at the 'NEXT' button.

5. Nella pagina **Impostazioni IPv4**, compilare **Indirizzo IP** e **Maschera di sottorete** e fornire un nuovo indirizzo IP del gateway (solo se necessario). Fare clic su **Avanti** per continuare.

Mostra esempio

The screenshot shows the 'IPv4 settings' step of the 'Add Networking' wizard. The left navigation bar highlights step 4, 'IPv4 settings'. The main panel shows 'Specify VMkernel IPv4 settings' with the 'Use static IPv4 settings' option selected. It includes fields for 'IPv4 address' (172.21.118.191), 'Subnet mask' (255.255.255.0), 'Default gateway' (172.21.166.1), and 'DNS server addresses' (10.61.185.231). At the bottom right, there are 'BACK' and 'NEXT' buttons, with a hand cursor pointing at the 'NEXT' button.

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

Mostra esempio

The screenshot shows the 'Add Networking' wizard in progress, specifically step 5: Ready to complete. The left sidebar lists steps 1 through 5. The right panel displays the configuration settings:

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

At the bottom right, there are 'CANCEL', 'BACK', and 'FINISH' buttons. The 'FINISH' button is highlighted with a green background and a white mouse cursor is positioned over it.

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

Passaggio 3: aggiungere l'adattatore NVMe/TCP

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

Per installare gli adattatori NVMe/TCP e rilevare i controller NVMe, completare i seguenti passaggi.

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

Mostra esempio

The screenshot shows the vSphere Client interface. The left sidebar lists hosts: vcf-m01-vc01.sddc.netapp.com, vcf-wkld-vc01.sddc.netapp.com, vcf-wkld-01-DC, IT-INF-WKLD-01, vcf-wkld-esx01.sddc.netapp.com, vcf-wkld-esx02.sddc.netapp.com, vcf-wkld-esx03.sddc.netapp.com, vcf-wkld-esx04.sddc.netapp.com, OracleSrv_01, OracleSrv_02, OracleSrv_03, and OracleSrv_04. The host vcf-wkld-esx01.sddc.netapp.com is selected. The main pane shows the 'Configure' tab selected, with the 'Storage' sub-tab active. On the right, the 'Storage Adapters' section is visible, featuring a 'Storage Adapters' dropdown, a 'Storage Devices' link, a 'Host Cache Configuration' link, a 'Protocol Endpoints' link, and an 'I/O Filters' link. Below this is a 'Networking' dropdown with links for 'Virtual switches', 'VMkernel adapters', 'Physical adapters', and 'TCP/IP configuration'. A context menu is open over the 'Add NVMe over TCP adapter' option in the 'Storage Adapters' list, with a hand cursor pointing at it.

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

Mostra esempio

The screenshot shows the 'Add Software NVMe over TCP adapter' dialog box. The title bar says 'Add Software NVMe over TCP adapter' and the host name 'vcf-wkld-esx01.sddc.netapp.com'. The main area contains the text 'Enable software NVMe adapter on the selected physical network adapter.' Below this is a 'Physical Network Adapter' list with four items: 'vmnic1/nvmlxnet3', 'vmnic1/nvmlxnet3', 'vmnic2/nvmlxnet3', and 'vmnic3/nvmlxnet3'. A hand cursor points at the first item in the list. At the bottom right are 'CANCEL' and 'OK' buttons.

4. Ripetere questa procedura per la seconda rete assegnata al traffico NVMe/TCP, assegnando l'adattatore fisico corretto.
5. Selezionare uno degli adattatori NVMe/TCP appena installati. Nella scheda **Controller**, seleziona **Aggiungi controller**.

Mostra esempio

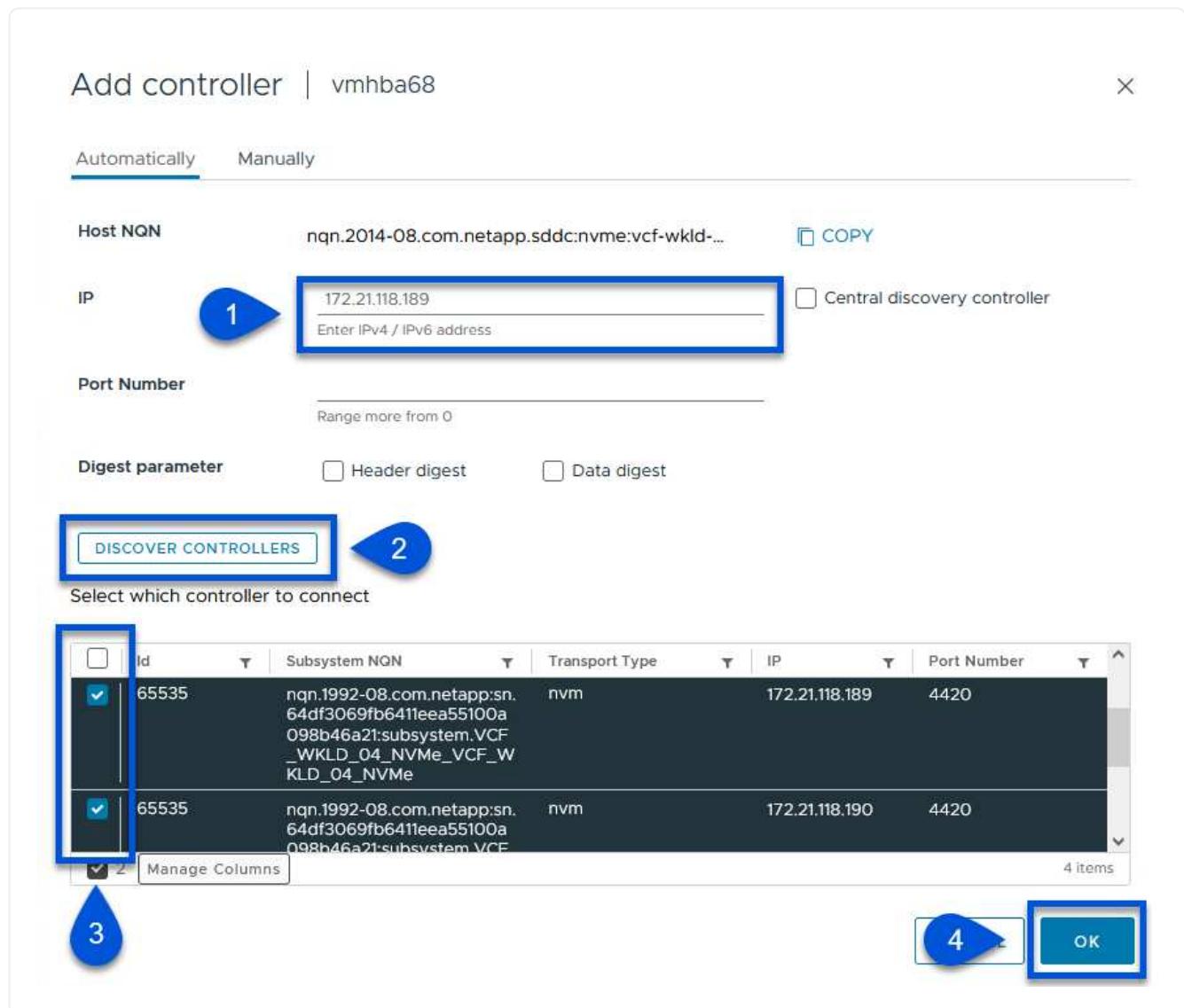
The screenshot shows the vSphere Client interface for managing storage adapters. The left sidebar shows a tree view of hosts and datastores. The main pane is titled 'vcf-wkld-esx01.sddc.netapp.com' and has tabs for Summary, Monitor, Configure, Permissions, VMs, Datastores, Networks, and Updates. The 'Configure' tab is selected. Under 'Storage', the 'Storage Adapters' section is active. A table lists the following adapters:

Adapter	Model	Type
vmhba65	iSCSI Software Adapter	iSCSI
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
vmhba0	PVSCSI SCSI Controller	SCSI
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP

Below the table are buttons for Manage Columns and Export. At the bottom, there are tabs for Properties, Devices, Paths, Namespaces, and Controllers. The 'Controllers' tab is selected. An 'ADD CONTROLLER' button is visible, and a hand cursor is pointing at the 'Name' input field.

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

Mostra esempio



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

Mostra esempio

The screenshot shows the vSphere Client interface. At the top, there's a toolbar with buttons for ADD SOFTWARE ADAPTER, REFRESH, RESCAN STORAGE, RESCAN ADAPTER, and REMOVE. Below the toolbar is a table titled "Storage Adapters" with columns: Adapter, Model, Type, Status, Identifier, Targets, Devices, and Paths. The table lists several adapters, including "vmhba65" (iSCSI Software Adapter), "vmhba1" (PIIX4 for 430TX/440BX/MX IDE Controller), "vmhba64" (PIIX4 for 430TX/440BX/MX IDE Controller), "vmhba0" (PVSCSI SCSI Controller), "vmhba68" (selected, VMware NVMe over TCP Storage Adapter), and "vmhba69" (VMware NVMe over TCP Storage Adapter). The "vmhba68" row is highlighted with a dark background. Below the table are buttons for Manage Columns and Export.

Below the adapter table is a section titled "Properties" with tabs for Devices, Paths, Namespaces, and Controllers. The "Devices" tab is selected and has a sub-menu with buttons for REFRESH, ATTACH (highlighted with a blue border), DETACH, and RENAME. Under the "Devices" tab, there's another table with columns: Name, LUN, Type, Capacity, Datastore, Operational State, Hardware Acceleration, Drive Type, and Transport. One item is listed: "NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)".

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

Cosa succederà ora?

Dopo aver configurato la rete, ["configurare l'archiviazione per NVMe vVols"](#).

Configurare l'archiviazione NVMe/TCP vVols in un dominio di carico di lavoro VCF VI

Configurare l'archiviazione NVMe/TCP vVols in un dominio di carico di lavoro VMware Cloud Foundation VI. Distribuirai gli strumenti ONTAP, registrerai un sistema di storage, creerai un profilo di capacità di storage e fornirai un datastore vVols nel client vSphere.

Passi

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

Mostra esempio

The screenshot shows the vSphere Client interface. On the left, the navigation tree displays several hosts under the root node 'vcf-m01-vc01.sddc.netapp.com'. One host, 'vcf-wkld-esx01.sddc.netapp.com', is selected and expanded, showing its children: 'vcf-wkld-vc01.sddc.netapp.com', 'vcf-wkld-01-DC', and 'IT-INF-WKLD-01'. 'IT-INF-WKLD-01' is further expanded to show 'vcf-wkld-esx01.sddc.netapp.com' and a list of virtual machines: OracleSrv_01 through OracleSrv_04, and SQLSRV_01 through SQLSRV_04. The main pane shows 'Host Details' for 'vcf-wkld-esx01.sddc.netapp.com'. The 'Actions' menu is open on the right, with 'Storage' selected. A hand cursor is hovering over the 'Rescan Storage' button.

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

Mostra esempio

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partizione configuration

5 Ready to complete

Name and device selection

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

Name

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V Si
<input checked="" type="radio"/>	NVMe TCP Disk (uuid:929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcfce42d230340deb66036)	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 ▾

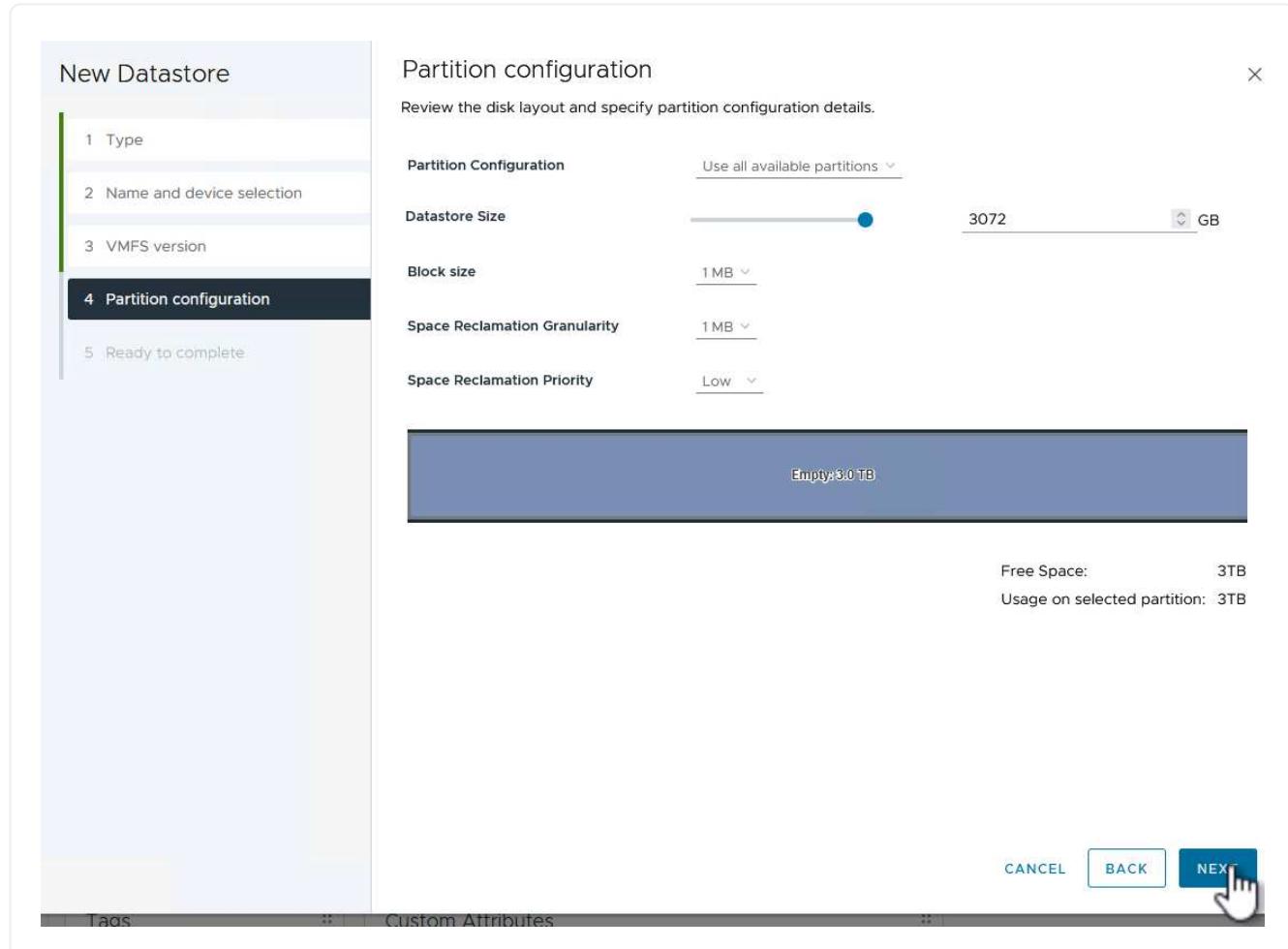
3 items

CANCEL BACK **NEXT** 

Tags Custom Attributes

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

Mostra esempio



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

Mostra esempio

Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
vcf-wkld-esx01.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	15%	13%	Connected (Secondary)	19 days
vcf-wkld-esx02.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	9%	15%	Running (Primary)	19 days
vcf-wkld-esx03.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	9%	21%	Connected (Secondary)	19 days
vcf-wkld-esx04.sddc.netapp.co	Connected	Normal	IT-INF-WKLD-0	11%	4%	Connected (Secondary)	19 days

Informazioni aggiuntive

- Per ulteriori informazioni sulla configurazione SAN per la ridondanza, fare riferimento a "Riferimento alla configurazione SAN NetApp".

- Per ulteriori informazioni sulle considerazioni di progettazione NVMe per i sistemi di archiviazione ONTAP , fare riferimento a "[Configurazione, supporto e limitazioni NVMe](#)" .
- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a "[Documentazione ONTAP 9](#)" .
- Per informazioni sulla configurazione di VCF, fare riferimento a "[Documentazione di VMware Cloud Foundation](#)" .

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

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

Prima di iniziare

Assicurarsi che i seguenti componenti e configurazioni siano presenti.

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

-  • Utilizzare l'interfaccia logica FC SVM nella configurazione della zona anziché le porte FC fisiche sui sistemi ONTAP .
• Utilizzare multipath per FC LUN.

Passi

1. Registrare il carico di lavoro VI vCenter seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Registra il carico di lavoro VI vCenter](#)" .

La registrazione del carico di lavoro VI vCenter abilita il plugin vCenter.

2. Aggiungere un backend di storage utilizzando l'interfaccia client vSphere seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Definisci il backend di archiviazione utilizzando l'interfaccia client vSphere](#)" .

L'aggiunta di un backend di archiviazione consente di integrare un cluster ONTAP .

3. Eseguire il provisioning di VMFS su Fibre Channel (FC) seguendo le istruzioni nella documentazione degli ONTAP tools for VMware vSphere :"[Provisioning VMFS su FC](#)" .

Informazioni aggiuntive

- Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP , fare riferimento a "[Documentazione ONTAP 9](#)" .

- Per informazioni sulla configurazione di VCF, fare riferimento a "[Documentazione di VMware Cloud Foundation](#)" .
- Per informazioni sulla configurazione di Fibre Channel sui sistemi di archiviazione ONTAP , fare riferimento a "[Gestione dello storage SAN](#)" nella documentazione ONTAP 9.
- Per informazioni sull'utilizzo di VMFS con sistemi di archiviazione ONTAP , fare riferimento a "[Guida alla distribuzione per VMFS](#)" .
- Per demo video di questa soluzione, fare riferimento a "[Provisioning del datastore VMware](#)" .

Proteggi VCF con SnapCenter

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

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

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

Per maggiori dettagli fare riferimento alle seguenti soluzioni.

- "[Proteggi il dominio del carico di lavoro VCF](#)"
- "[Proteggere più domini di carico di lavoro VCF](#)"
- "[Proteggi il dominio del carico di lavoro VCF con NVMe](#)"

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

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

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

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuire il SnapCenter Plug-in for VMware vSphere (SCV) sul dominio del carico di lavoro VI.
- Aggiungere sistemi di archiviazione a SCV.
- Creare policy di backup in SCV.
- Creare gruppi di risorse in SCV.

- Utilizzare SCV per eseguire il backup di datastore o VM specifiche.
- Utilizzare SCV per ripristinare le VM in una posizione alternativa nel cluster.
- Utilizzare SCV per ripristinare i file in un file system Windows.

Prerequisiti

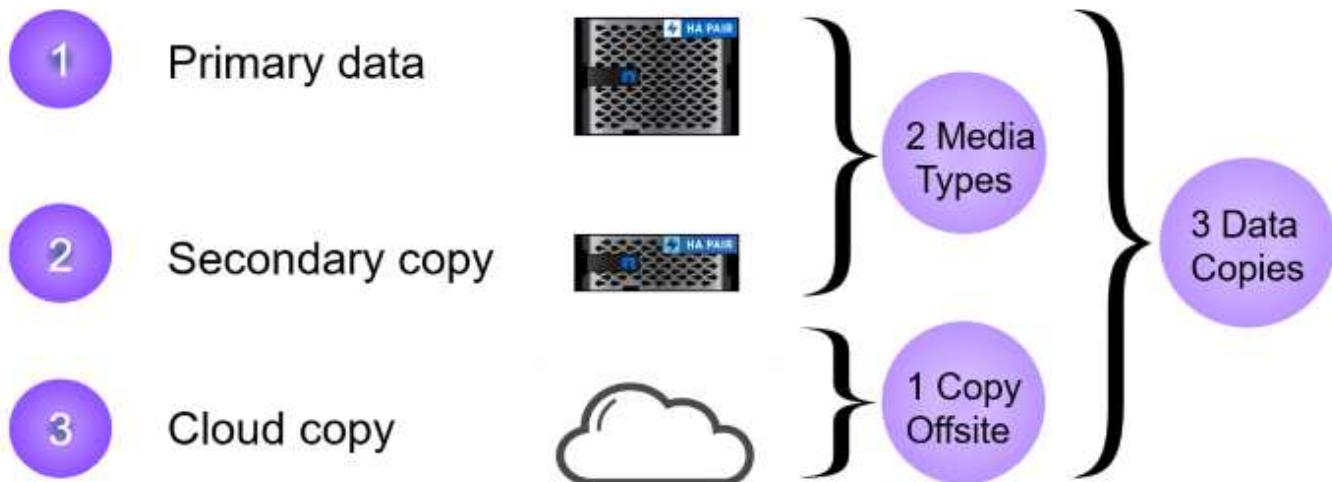
Questo scenario richiede i seguenti componenti e configurazioni:

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

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



Oltre a replicare i backup eseguiti con SCV su un archivio secondario, è possibile effettuare copie offsite dei dati su un archivio di oggetti su uno dei tre (3) principali provider cloud utilizzando NetApp Backup and Recovery per VM. Per maggiori informazioni fare riferimento a questa offerta "[Documentazione NetApp Backup and Recovery](#)".



Fasi di distribuzione

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

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

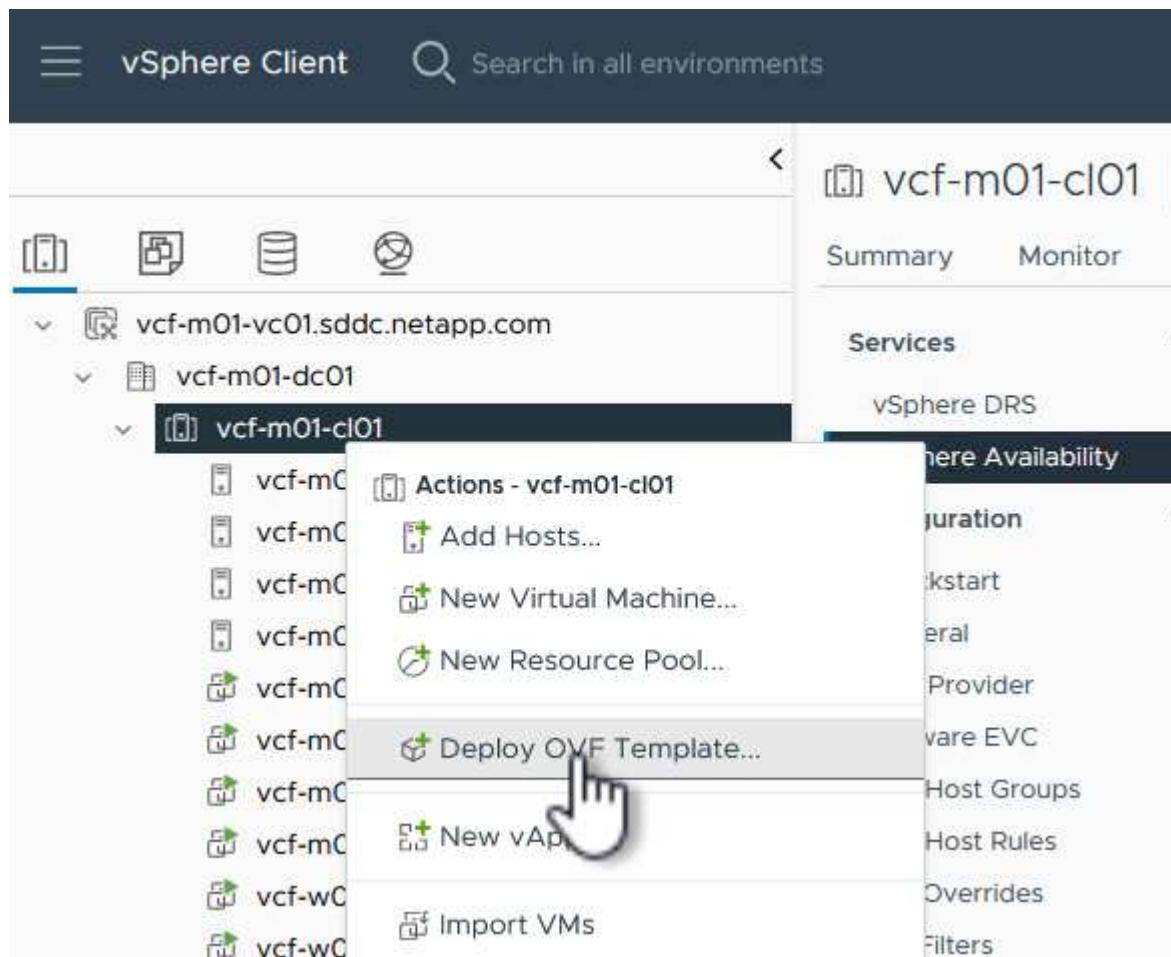
Completare i seguenti passaggi per distribuire, configurare e utilizzare SCV per proteggere i dati in un dominio di carico di lavoro VI:

Distribuisci il SnapCenter Plug-in for VMware vSphere

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

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

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



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

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 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
<http://https://remoteserver-address/filetodeploy.ovf> .ova

Local file
scv-5.0P2-240310_1514.ova

UPLOAD FILES

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

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 (i)

Select virtual disk format **Thin Provision**

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	3.71 TB	2.5 TB	V
<input type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 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

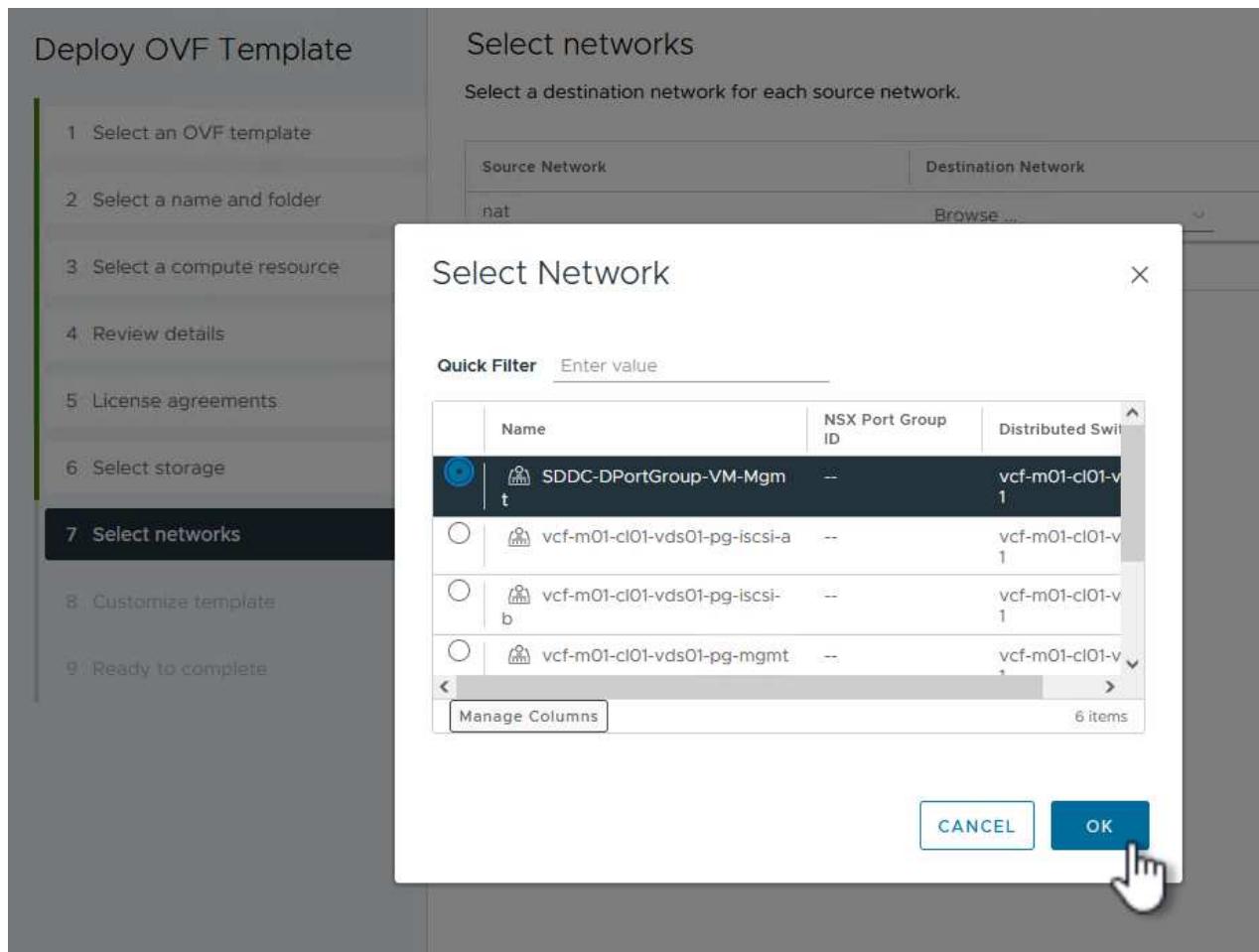
Manage Columns Items per page 10 6 items

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 di storage ONTAP primario e secondario.



9. Nella pagina **Personalizza modello** compila tutte le informazioni richieste per la distribuzione:

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

Fare clic su **Avanti** per continuare.

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com	
1.2 vCenter username	administrator@vcf.local	
1.3 vCenter password	Password	***** (?)
	Confirm Password	***** (?)
1.4 vCenter port	443	
2. Create SCV Credentials		2 settings
2.1 Username	admin	
2.2 Password	Password	***** (?)
	Confirm Password	***** (?)
3. System Configuration		1 settings

Deploy OVF Template

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

Customize template

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

5. Setup Date and Time

2 settings

5.1 NTP servers (optional)

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

5.2 Time Zone setting

Sets the selected timezone setting for the VM

America/New_York

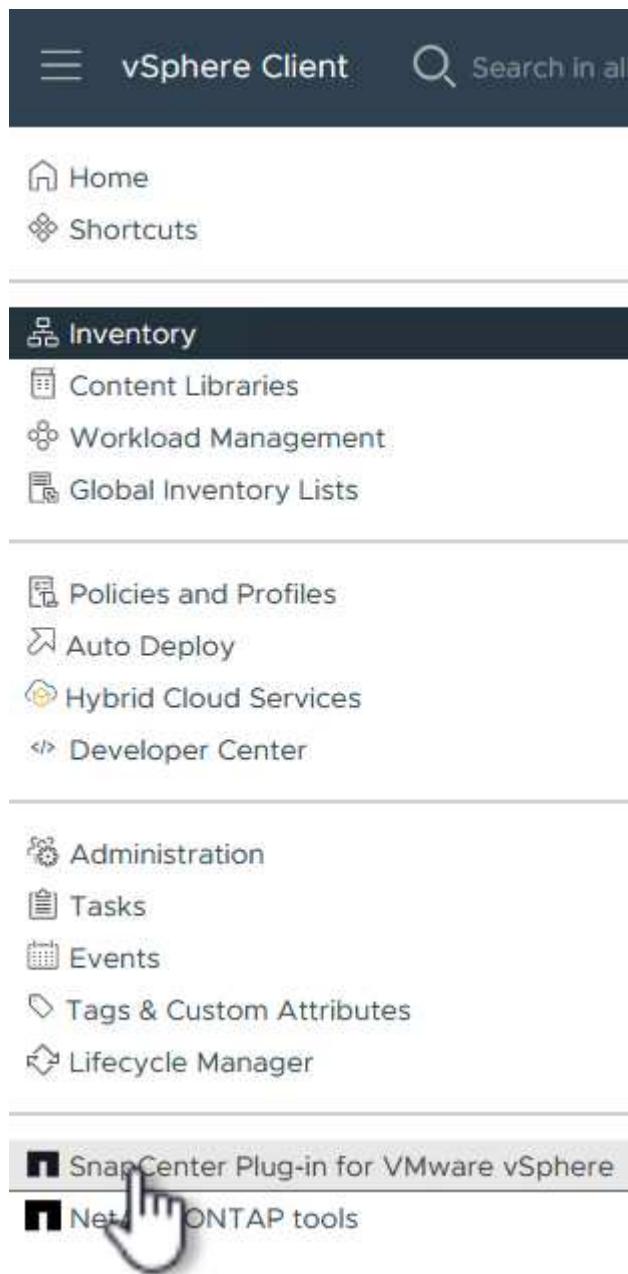
CANCEL BACK NEXT

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

Aggiungere sistemi di archiviazione a SCV

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

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



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



vSphere Client



Search in all environments

SnapCenter Plug-in for VMware vSphere

INSTANCE 172.21.166.148:8080 ▾

[Dashboard](#)[Settings](#)

Dashboard

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



vSphere Client



Search in all environments

SnapCenter Plug-in for VMware vSphere

INSTANCE 172.21.166.148:8080 ▾

[Dashboard](#)[Settings](#)[Resource Groups](#)[Policies](#)[**Storage Systems**](#)[Guest File Restore](#)

Storage Systems

[+ Add](#)[Edit](#)[Delete](#)[Export](#)

Name

Display Name

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

Add Storage System

X

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

Event Management System(EMS) & AutoSupport Setting

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

CANCEL

ADD



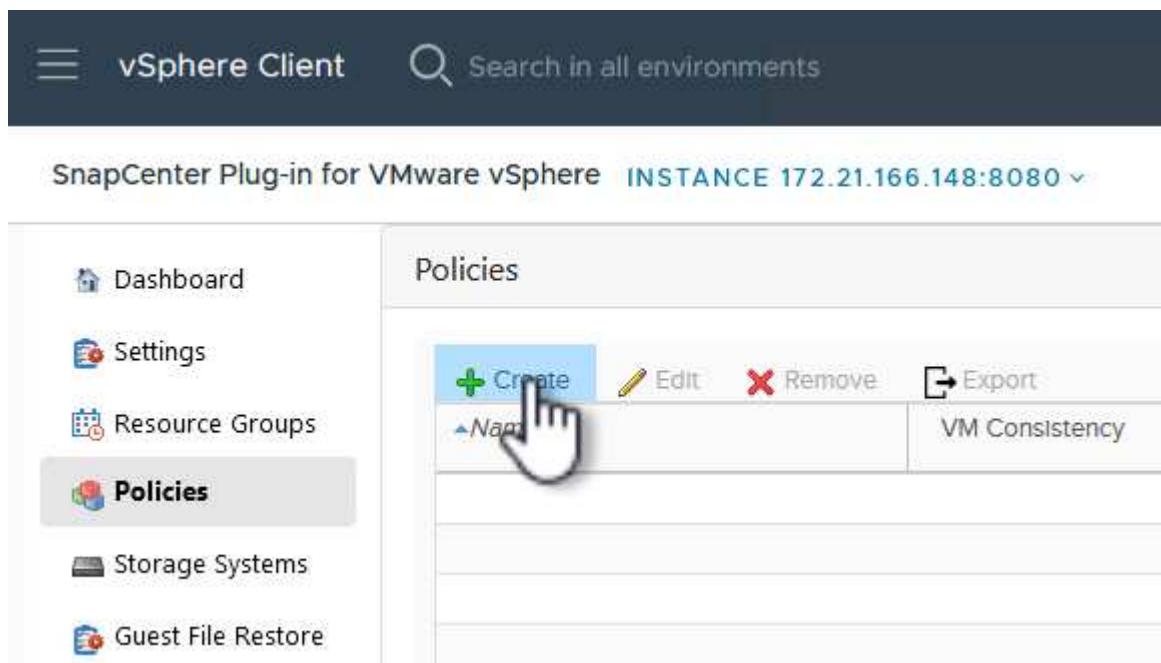
5. Ripetere questa procedura per tutti gli altri sistemi di archiviazione da gestire, compresi quelli da utilizzare come destinazioni di backup secondarie.

Configurare i criteri di backup in SCV

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

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

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



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

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

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



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

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

New Backup Policy

X

Name	Daily_Snapmirror		
Description	description		
Frequency	Daily	▼	
Locking Period	<input type="checkbox"/> Enable Snapshot Locking <small>i</small>		
Retention	Days to keep	▼	15 <small>▲ ▼ i</small>
Replication	<input checked="" type="checkbox"/> Update SnapMirror after backup <small>i</small> <input type="checkbox"/> Update SnapVault after backup <small>i</small>		
	Snapshot label <input type="text"/>		
Advanced <small>▼</small>	<input type="checkbox"/> VM consistency <small>i</small> <input type="checkbox"/> Include datastores with independent disks		
Scripts <small>i</small>	<input type="text" value="Enter script path"/>		

CANCEL

ADD

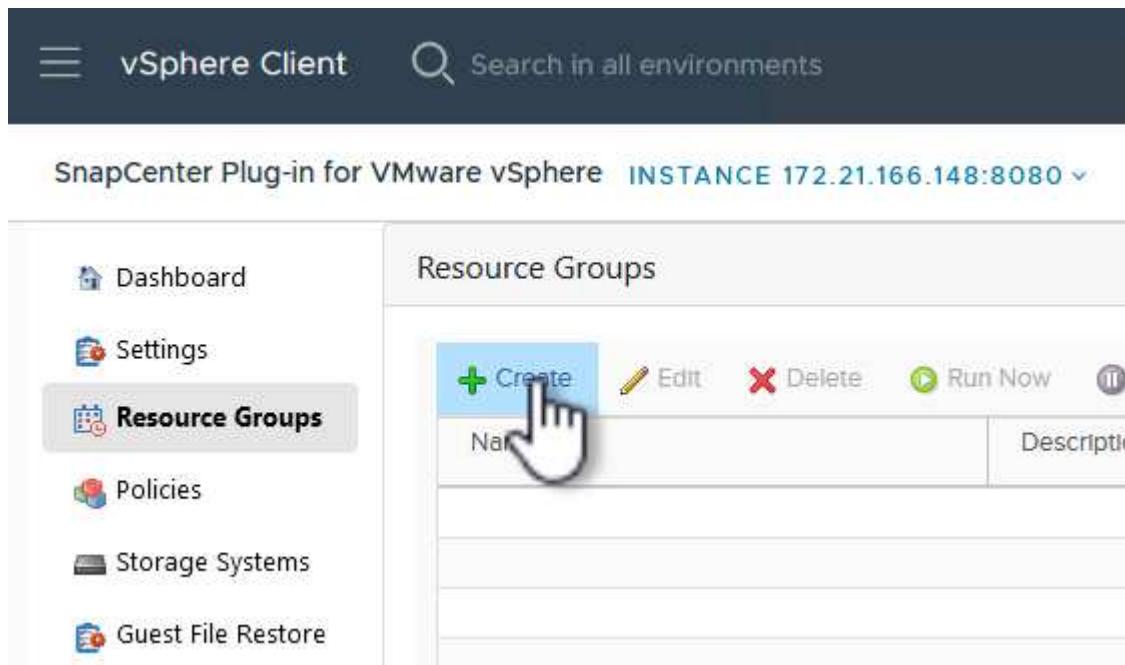


Creare gruppi di risorse in SCV

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

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

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



The screenshot shows the vSphere Client interface with the title bar "vSphere Client" and a search bar "Search in all environments". Below the title bar, it says "SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080". On the left, there's a sidebar with icons for Dashboard, Settings, Resource Groups (which is selected and highlighted in grey), Policies, Storage Systems, and Guest File Restore. The main panel is titled "Resource Groups" and contains a table with columns for Name, Description, and Actions (Edit, Delete, Run Now). At the top of this table, there are buttons for "+ Create", "Edit", "Delete", "Run Now", and "Details". A hand cursor is pointing at the "+ Create" button.

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



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

Create Resource Group

✓ 1. General info & notification

Scope: Virtual Machines

2. Resource

Parent entity: VCF_WKLD_03_ISCSI

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Available entities

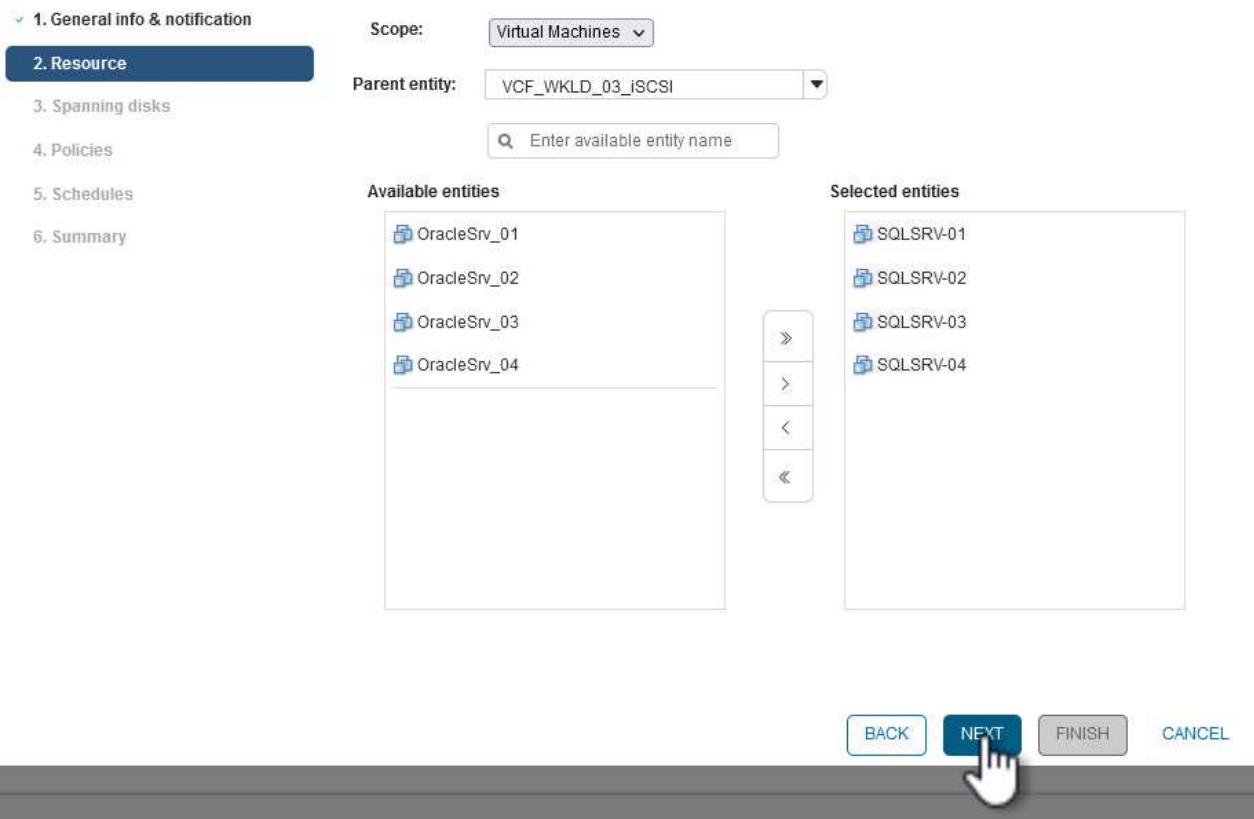
- OracleSrv_01
- OracleSrv_02
- OracleSrv_03
- OracleSrv_04

Selected entities

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

Enter available entity name

BACK NEXT FINISH CANCEL



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

Create Resource Group

- ✓ 1. General info & notification
 - 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
 - ✓ 2. Resource
 - 3. Spanning disks**
 - 4. Policies
 - 5. Schedules
 - 6. Summary
- 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 i
You will need to modify the list every time new VMs are added

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



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

Create Resource Group

- ## ✓ 1. General info & notification

- ## ✓ 2. Resource

- ### ✓ 3. Spanning disks

4. Policies

5. Schedules

6. Summary

+ Create

BACK

NEXT

FINISH

CANCEL



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

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource Daily_Snapmi... ▾ Type Daily

✓ 3. Spanning disks Every 1 Day(s)

✓ 4. Policies Starting 04/04/2024

5. Schedules

At 04 : 45 PM

6. Summary

BACK **NEXT** FINISH CANCEL



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

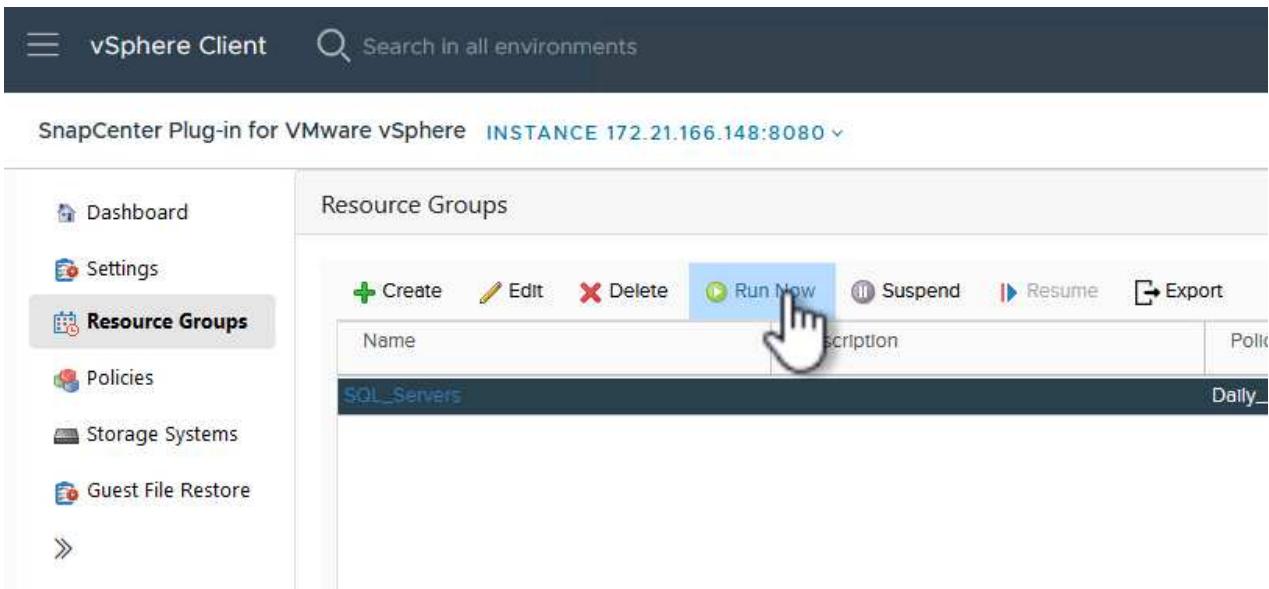
Create Resource Group

- ✓ 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	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.



vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

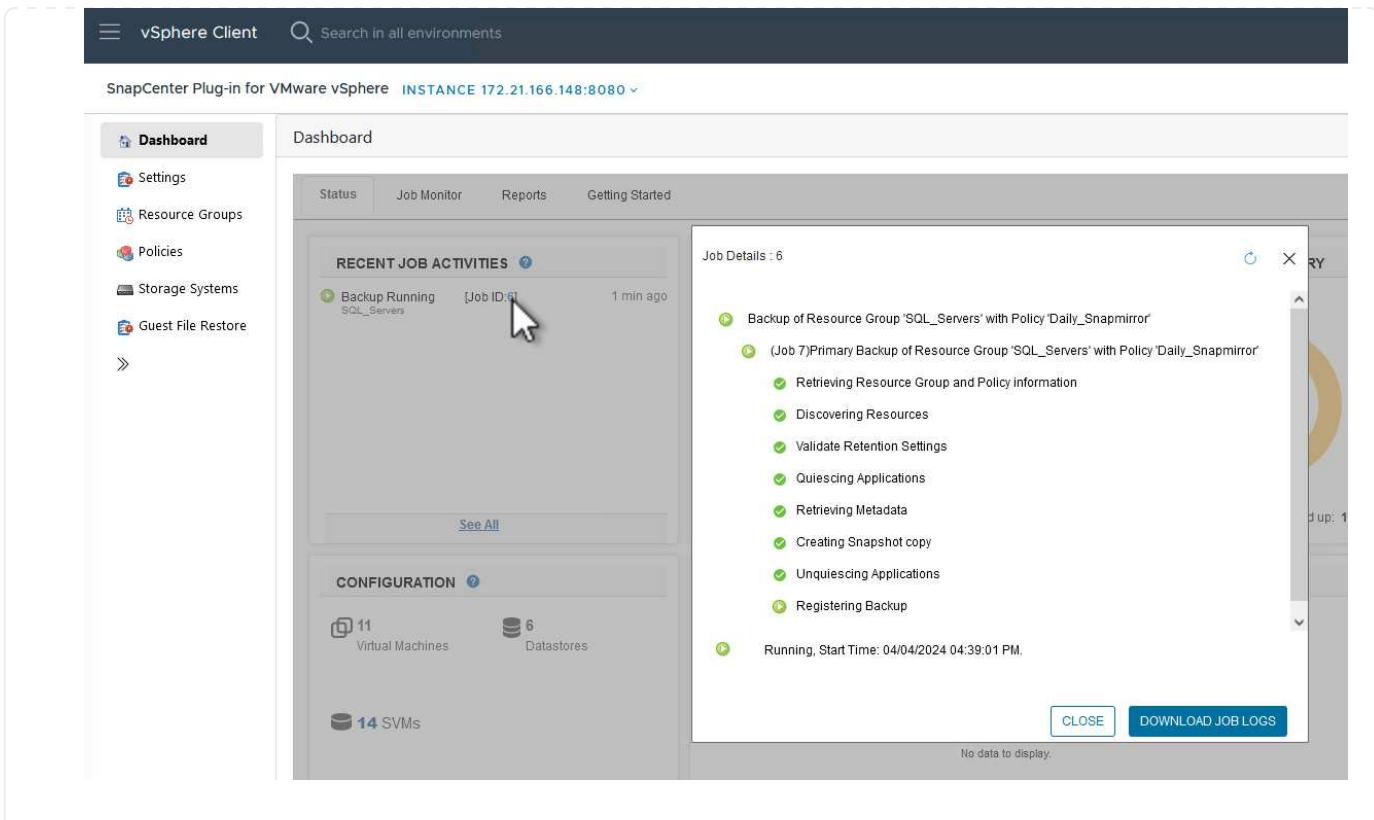
Resource Groups

Dashboard Settings **Resource Groups** Policies Storage Systems Guest File Restore

Run Now 

Name	Description	Policy
SQL_Servers		Daily...

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



Utilizzare SCV per ripristinare VM, VMDK e file

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

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

Le VM vVol possono essere ripristinate sull'host originale.

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

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

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

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

Ripristina le VM utilizzando il plug-in SnapCenter

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

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

vSphere Client Search in all environments

OracleSrv_04

Summary Monitor Configure Permissions

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

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

Detach Virtual Disk(s)

Restore

File Restore

Recent Tasks

Task Name

Manage Columns Run

SnapCenter Plug-in for VMware vSphere

4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision (VCF_WKLD_03_iSCSI)
(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f1
Disconnected
ESXi 7.0 U2 and later (VM vers)



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

vSphere Client Search in all environments

Administrator@VCF.LOCAL

VCF_WKLD_03_iSCSI

1

2

3

4

Actions

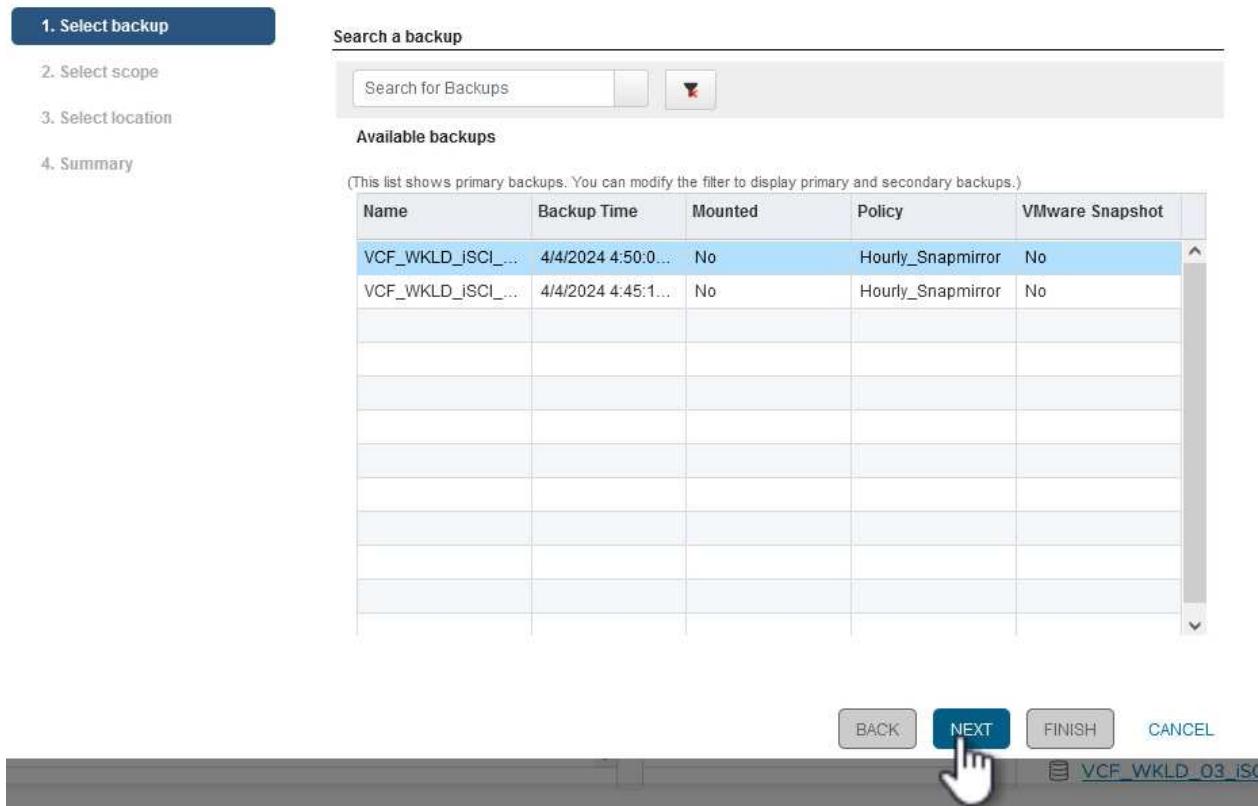
Summary Monitor Configure Permissions Files Hosts VMs

Backups

Name	Status	Locations	Snapshot Loc.	Created Time	Mounted	Policy	VMware Sn...
VCF_WKLD_ISCSI_Destore_04-12-2024_12_50_01.0083	Completed	Primary & Secondary	-	4/12/2024 12:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_11_50_01.0083	Completed	Primary & Secondary	-	4/12/2024 11:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_10_50_01.0014	Completed	Primary & Secondary	-	4/12/2024 10:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_09_50_01.0087	Completed	Primary & Secondary	-	4/12/2024 9:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_08_50_01.0050	Completed	Primary & Secondary	-	4/12/2024 8:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_07_50_01.0237	Completed	Primary & Secondary	-	4/12/2024 7:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_06_50_01.0068	Completed	Primary & Secondary	-	4/12/2024 6:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_05_50_01.0025	Completed	Primary & Secondary	-	4/12/2024 5:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_04_50_01.0062	Completed	Primary & Secondary	-	4/12/2024 4:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_03_50_01.0035	Completed	Primary & Secondary	-	4/12/2024 3:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_02_50_01.0122	Completed	Primary & Secondary	-	4/12/2024 2:50:08 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_01_50_01.0136	Completed	Primary & Secondary	-	4/12/2024 1:50:07 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-12-2024_00_50_01.0067	Completed	Primary & Secondary	-	4/12/2024 0:50:06 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-11-2024_23_50_01.0062	Completed	Primary & Secondary	-	4/11/2024 11:50:06 PM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCSI_Destore_04-11-2024_22_50_01.0000	Completed	Primary & Secondary	-	4/11/2024 10:50:06 PM	No	Hourly_Snapmirror	No

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

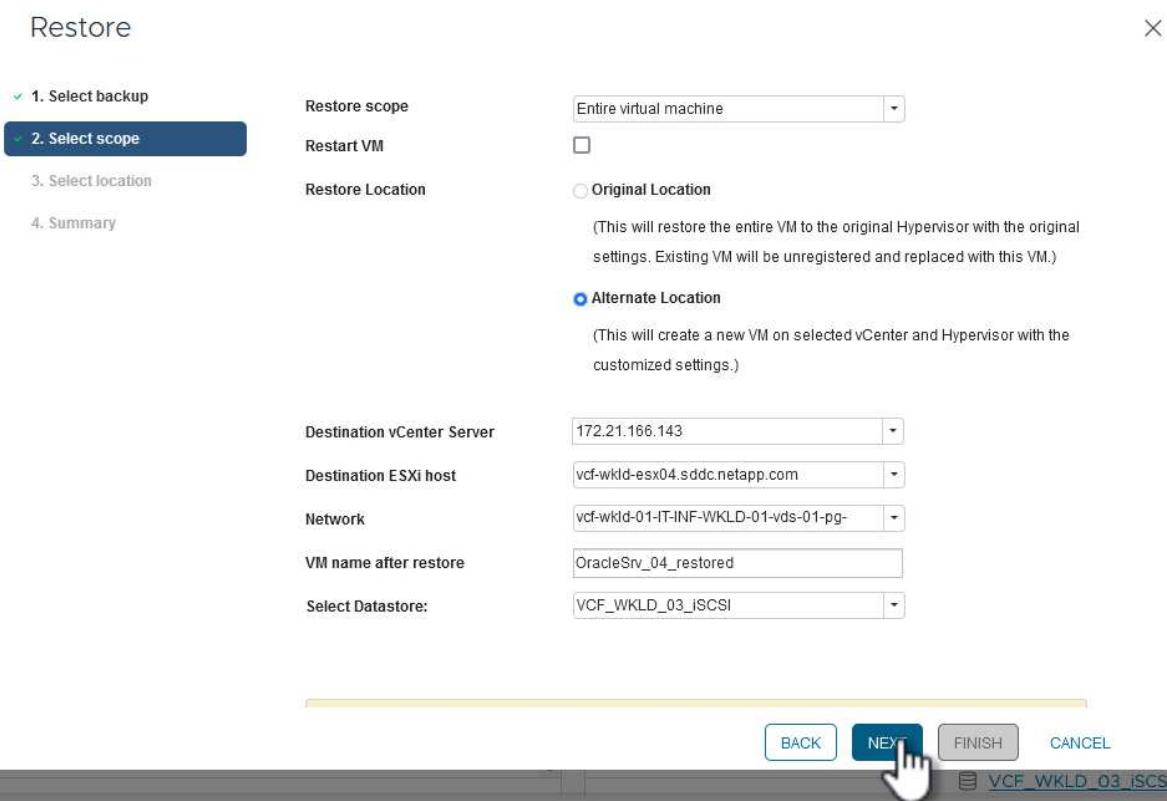
Restore



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

- **Ripristina ambito:** seleziona per ripristinare l'intera macchina virtuale.
- **Riavvia VM:** scegli se avviare la VM dopo il ripristino.
- **Ripristina posizione:** scegli se ripristinare la posizione originale o una posizione alternativa.
Quando si sceglie una posizione alternativa, selezionare le opzioni da ciascuno dei campi:

- **Server vCenter di destinazione:** vCenter locale o vCenter alternativo in modalità collegata
- **Host ESXi di destinazione**
- **Rete**
- **Nome della VM dopo il ripristino**
- **Seleziona datastore:**



Fare clic su **Avanti** per continuare.

4. Nella pagina **Selezione posizione**, scegli di ripristinare la VM dal sistema di archiviazione 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, rivedere il **Riepilogo** e fare clic su **Fine** per avviare il processo di ripristino.

Restore

- ✓ 1. Select backup
 - ✓ 2. Select scope
 - ✓ 3. Select location

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



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

WKLD_03

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

vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] VCF_WKLD_ISCI_Datastore_04-04-20... 1 min ago
- Backup Successful [Job ID:15] VCF_WKLD_ISCI_Datastore 8 min ago
- Backup Successful [Job ID:12] VCF_WKLD_ISCI_Datastore 13 min ago
- Backup Successful [Job ID:9] SQL_Servers 13 min ago
- Backup Successful [Job ID:6] SQL_Servers 19 min ago

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.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	[vcf-wkld-esx04.sdd c.netapp.com]	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	[vcf-wkld-esx04.sdd c.netapp.com]	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

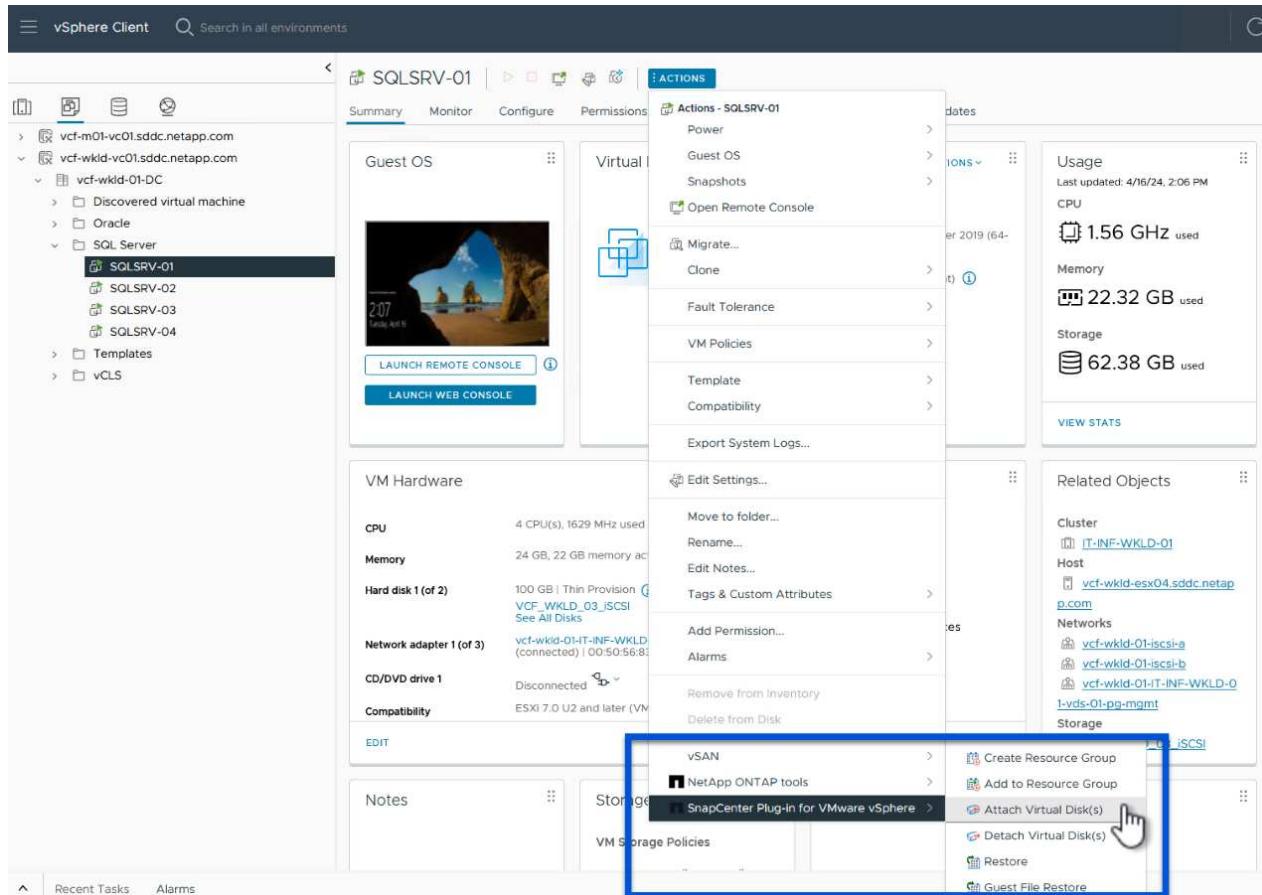
Manage Columns Running More Tasks

Ripristinare i VMDK utilizzando il plug-in SnapCenter

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

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

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



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

Attach Virtual Disk(s)

X

[Click here to attach to alternate VM](#)

Backup

(This list shows primary backups. [1](#) Click here to modify the filter to display primary and secondary backups.)

Search for 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

<input type="checkbox"/> 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.C
<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.C



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

Attach Virtual Disk(s)

X

[Click here to attach to alternate VM](#)

Backup

(This list shows primary backup

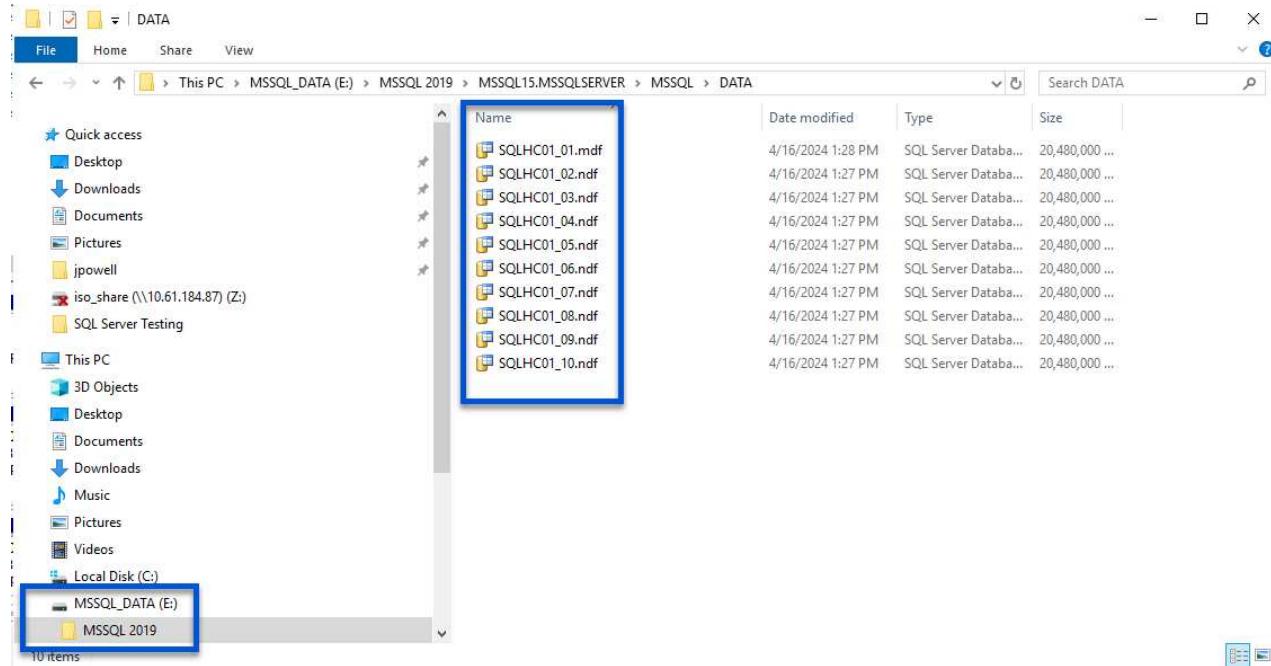
Search for Backups

Name	Time range	From <input type="text" value="04/17/2024"/>	To <input type="text"/>	VMware snapshot <input type="text" value="Yes"/>	Mounted <input type="text" value="No"/>	Location <input type="text" value="Primary/Secondary"/>
		12 <input type="button" value="Hour"/> 00 <input type="button" value="Minute"/> 00 <input type="button" value="Second"/> AM <input type="button" value="AM/PM"/>				
		12 <input type="button" value="Hour"/> 00 <input type="button" value="Minute"/> 00 <input type="button" value="Second"/> AM <input type="button" value="AM/PM"/>				
		<input type="button" value="CLEAR"/> <input type="button" value="OK"/>				

CANCEL

ATTACH

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



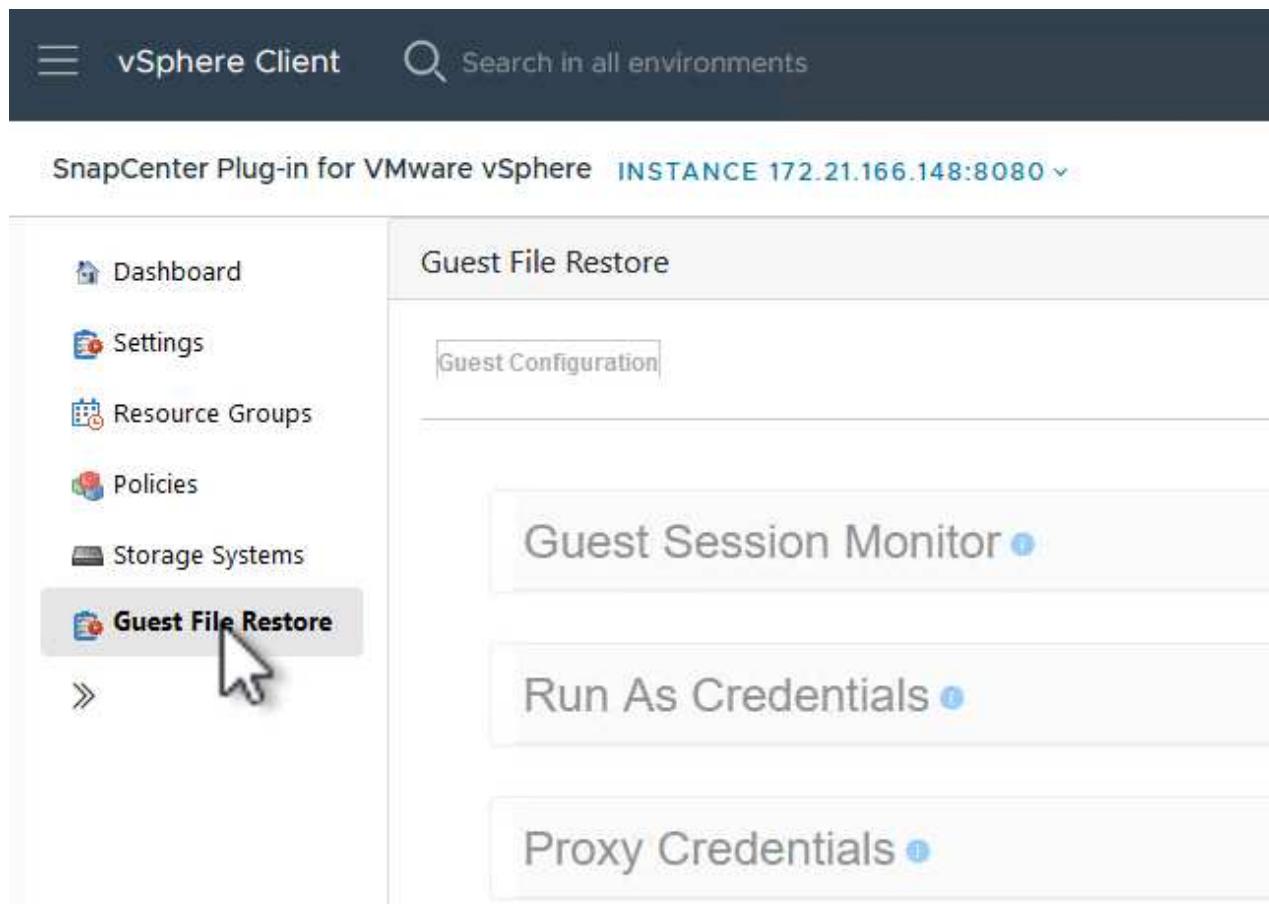
Ripristino del file system guest tramite il plug-in SnapCenter

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

Per informazioni dettagliate fare riferimento a "[Ripristina file e cartelle degli ospiti](#)" sul sito di documentazione SCV.

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

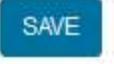
- Il primo passo è creare le credenziali Run As per fornire l'accesso al sistema host Windows. Nel vSphere Client, accedere all'interfaccia del plug-in CSV e fare clic su **Guest File Restore** nel menu principale.



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

Run As Credentials



Run As Name	Administrator	
Username	administrator	
Password	*****	
Authentication Mode	Windows	
VM Name	<input type="text"/>	
		 CANCEL  SAVE

ripristino.

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

Proxy VM



VM Name

SQLSRV-01

Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

SQLSRV-01

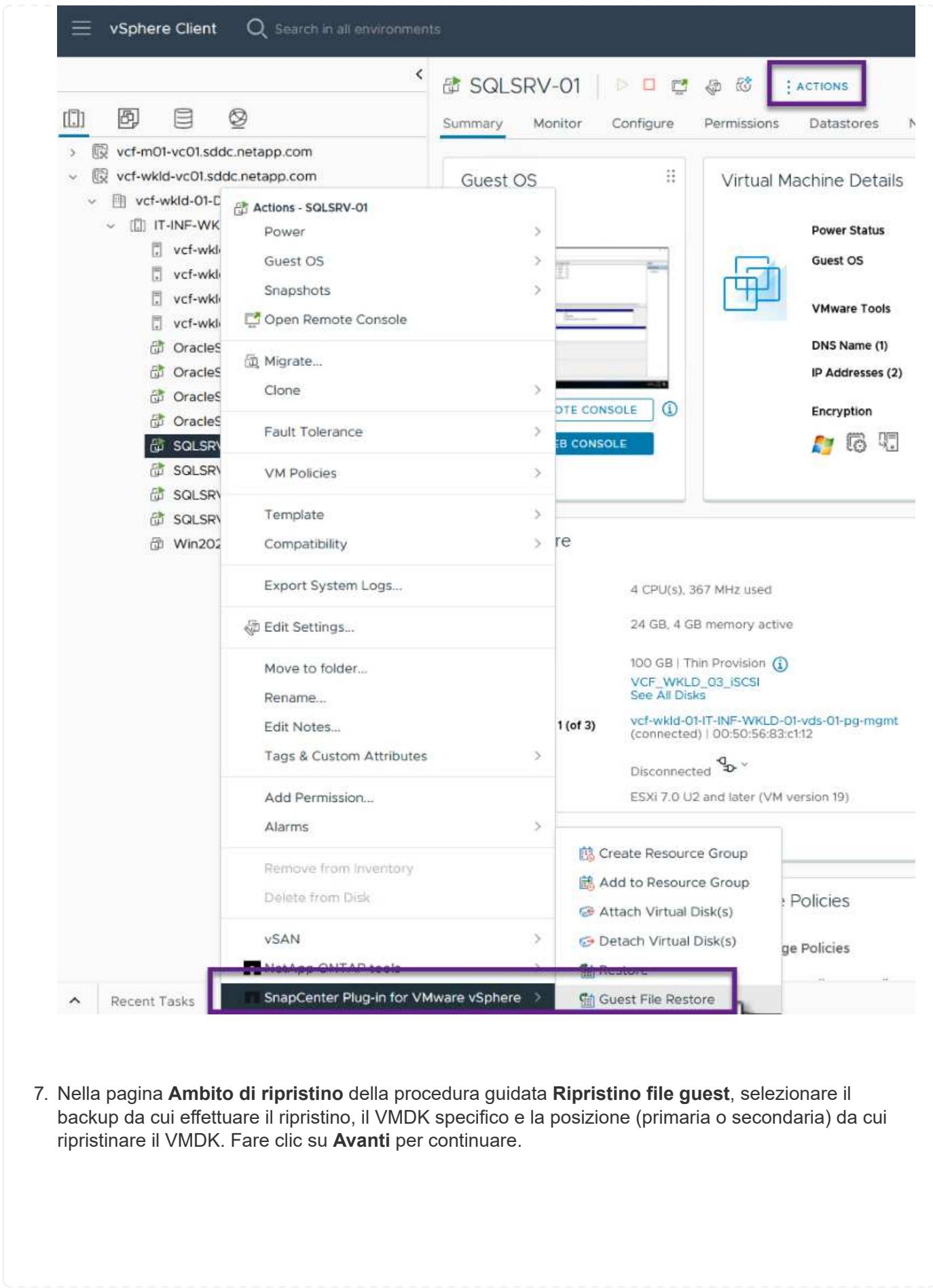
Search by Virtual Machine name

CANCEL

SAVE



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



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

Guest File Restore

X

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

Storage

VCF_WKLD_03_iSCSI

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

Guest File Restore

X

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: Guest File Restore

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

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

vSphere Client Search in all environments

SnapCenter Plug-in for VMware vSphere INSTANCE 172.21.166.148:8080

Administrator@VCF.LOCAL

Guest File Restore

Guest Configuration

Guest Session Monitor

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_iSCSI(sc-202404161419...)	E:\	23h:58m	

Run As Credentials

Proxy Credentials

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

Guest File Browse

X

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

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		<input type="button" value="Delete"/>
Selected 0 Files / 1 Directory			
Name	Path	Size	Delete
MSSQL 2019	E:\MSSQL 2019		<input type="button" value="Delete"/>

Select Restore Location

^

Select address family for UNC path:

IPv4

IPv6

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE

Select Restore Location

Select address family for UNC path:

IPv4

IPv6

Restore to path

\172.21.166.16\c\$

Provide UNC path to the guest where files will be restored. eg:\
\10.60.136.65\c\$

Run As Credentials while triggering the Guest File Restore workflow
will be used to connect to the UNC path

If original file(s) exist:

Always overwrite

Always skip

Disconnect Guest Session after successful restore

CANCEL

RESTORE



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

Informazioni aggiuntive

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

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

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

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

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

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

Introduzione

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

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

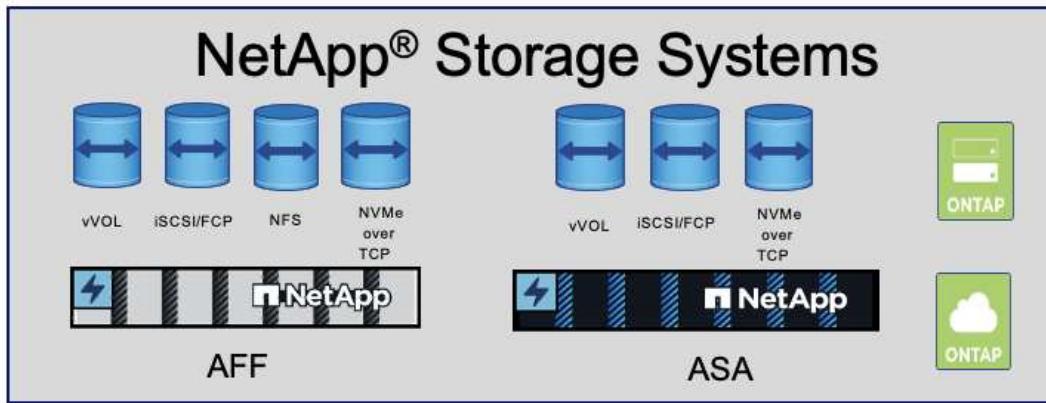
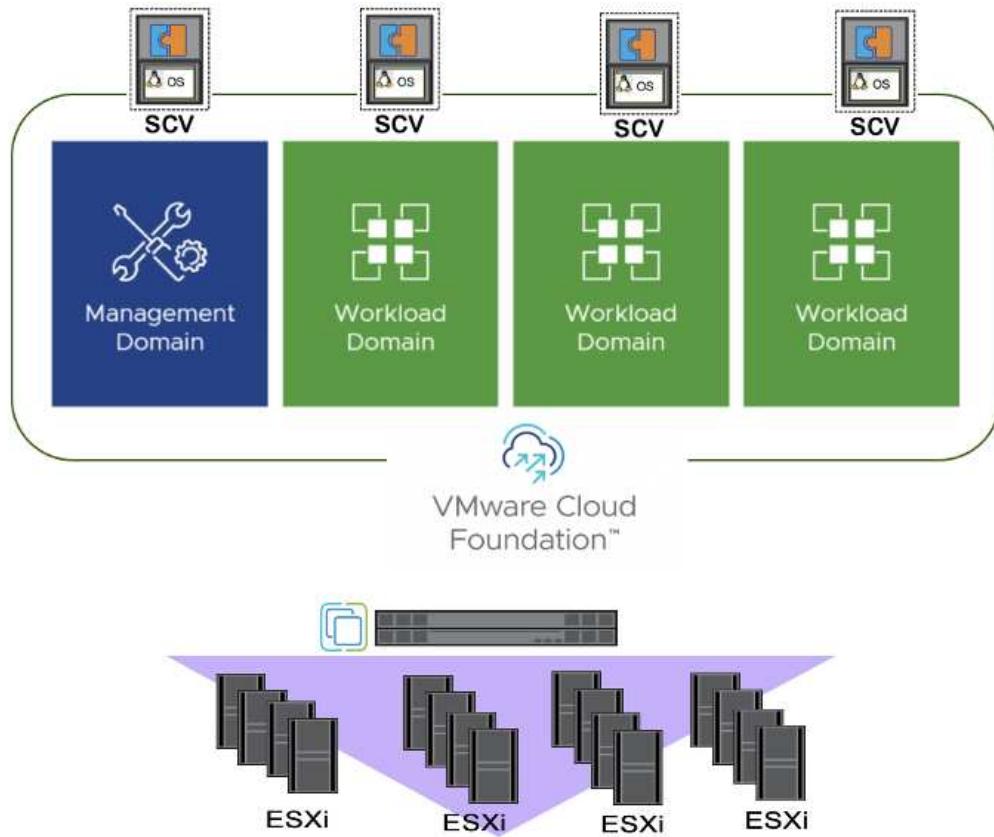
Pubblico

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

Panoramica dell'architettura

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

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



La regola di backup 3-2-1 è una strategia di protezione dei dati che prevede la creazione di tre copie dei dati, la loro archiviazione su due tipi diversi di supporti e la conservazione di una copia fuori sede. NetApp Backup and Recovery è uno strumento basato su cloud per la gestione dei dati che fornisce un unico piano di controllo per un'ampia gamma di operazioni di backup e ripristino sia in ambienti on-premise che cloud. Per maggiori dettagli, controlla "[Documentazione NetApp Backup and Recovery](#)".

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

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

The screenshot shows the vSphere Web Client interface with the 'Workload Domains' dashboard selected. The left sidebar contains navigation links for Home, Hosts & Clusters, Datacenters, Workload Domains, Datastores, Virtual Machines, and Network. The main content area is titled 'Workload Domains' and shows a summary for 'VMware Private AI Foundation with NVIDIA'. It includes a summary card with metrics like CPU, Memory, and Storage usage, and a table showing detailed resource utilization across hosts.

Fasi di distribuzione, configurazione e ripristino SCV

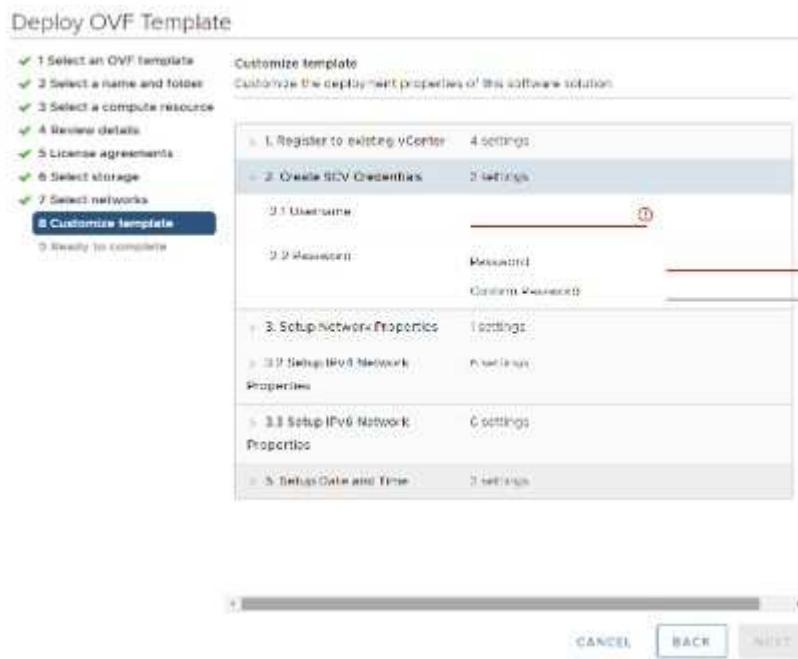
In base al numero di domini di carico di lavoro e al dominio di gestione, è necessario distribuire più SCV. Con due domini di carico di lavoro e un dominio di gestione, l'esempio seguente mostra tre SCV distribuiti sul dominio di gestione VCF vCenter.



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

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

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



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

```

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

Enter your choice: 10

Generating MFA Token... Your MFA Token is : 435164
Press ENTER to continue...

```

sistema.

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

Name (FQDN) or IP	vcf-wkld-vc01.sddc.netapp.com	Port	443
Username	administrator@vsphere.local		
Password	*****		

Plug-in Details:

- Service: Enabled
- SSH: Enabled
- Status: Connected

Configurare SCV

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

Getting Started with SnapCenter Plug-in for VMware vSphere



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

New Backup Policy

X

Name	wkld01
Description	description
Frequency	Daily
Locking Period	<input checked="" type="checkbox"/> Enable Snapshot Locking <small>i</small> 1 Days
Retention	Days to keep <input type="button" value="7"/>
Replication	<input type="checkbox"/> Update SnapMirror after backup <small>i</small> <input type="checkbox"/> Update SnapVault after backup <small>i</small>
Snapshot label	<input type="text"/>

[Advanced >](#)

CANCEL

ADD

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

Create Resource Group

X

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

Name	wkld01RG				
Description					
Send email	Never				
Latest Snapshot name	None <small>?</small>				
Custom snapshot format	None <small>?</small>				
Entities	wkld01				
Spanning	True				
Policies	Name	Frequency	Snapshot Locking Period		
	wkld01	Daily	1 Day		

BACK

NEXT

FINISH

CANCEL

Ripristina la macchina virtuale e il backup di file o cartelle

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

Passaggi di ripristino della VM

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

Restore

1. Select backup	Virtual machine to be restored	win2022
2. Select scope	Backup name	wkld02_recent
3. Select location	Restart virtual machine	No
4. Summary	Restore Location	Alternate Location
	Destination vCenter Server	172.21.166.202
	ESXi host to be used to mount the backup	vcf-wkld-esx07.sddc.netapp.com
	VM Network	vcf-m01wk-vc02-vcf-wkld02-vds-01-pg-mgmt
	Destination datastore	wkld02
	VM name after restore	win2022.1

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

BACK NEXT FINISH CANCEL

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

Passaggi di ripristino del datastore

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

Mount Datastore

ESXi host name

Backup

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
wkld02_recent	2/9/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-09-202...	2/9/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-08-2025_20.0...	2/8/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-08-202...	2/8/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-07-2025_20.0...	2/7/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-07-202...	2/7/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-06-2025_20.0...	2/6/2025 8:00:01 PM	No	wkld02	Yes

Backup location

Backup type	Location
Primary	172.21.118.118:vcf_md_wkld02:wkld02_recent

Passaggi per il ripristino di file e cartelle

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

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

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

specifici o singoli file.

Demo video per proteggere più domini VCF con SCV

[Proteggi più domini VMware VCF con NetApp SCV](#)

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

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

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

Introduzione

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

Vantaggi di NVMe rispetto a TCP

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

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

Pubblico

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

Panoramica dell'architettura

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

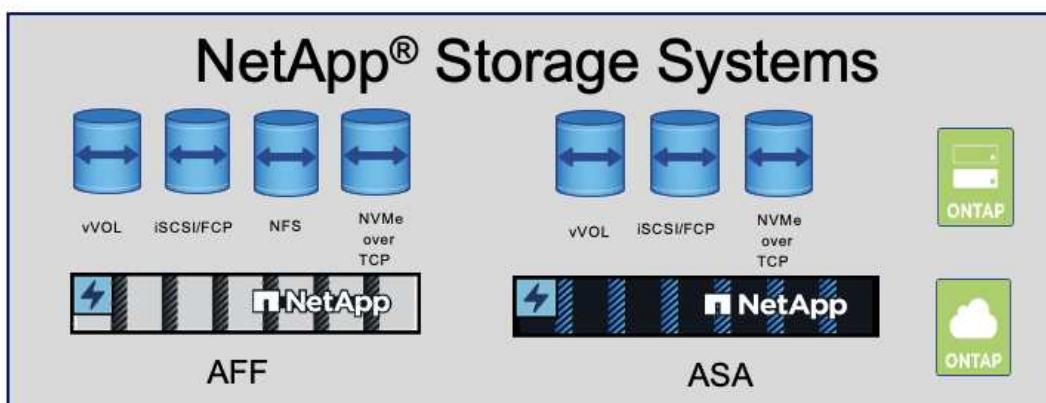
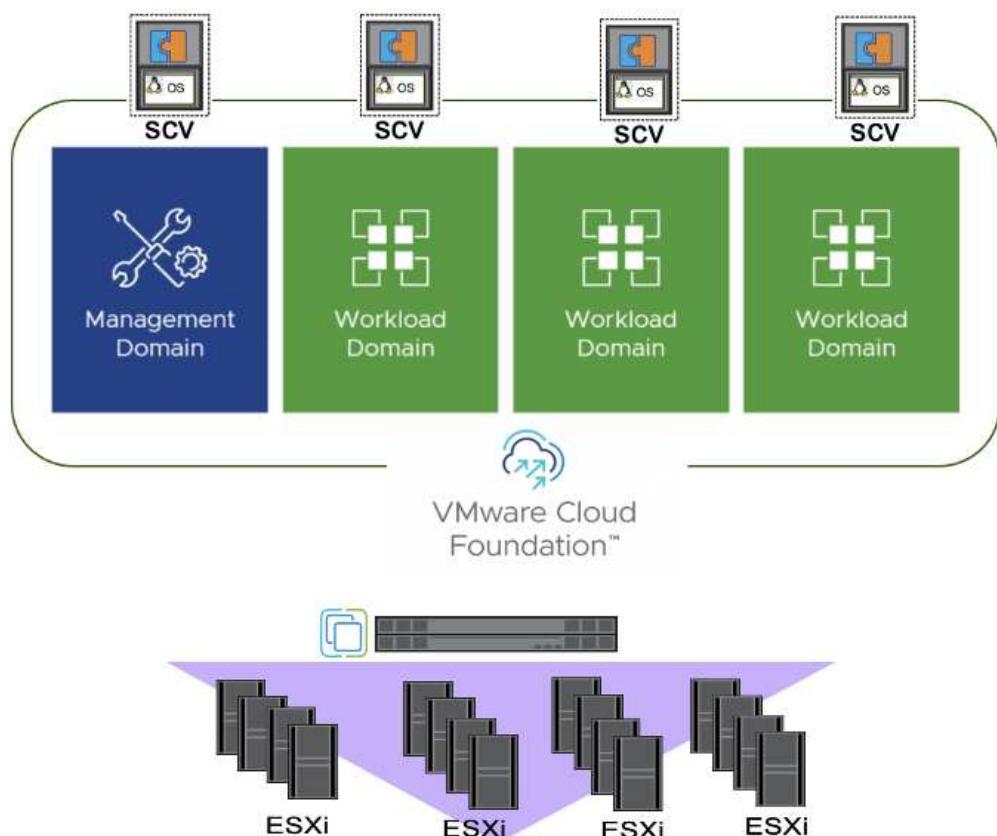
Architettura di distribuzione SCV

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

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

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

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



La regola di backup 3-2-1 è una strategia di protezione dei dati che prevede la creazione di tre copie dei dati, la loro archiviazione su due tipi diversi di supporti e la conservazione di una copia fuori sede. NetApp Backup and Recovery è uno strumento basato su cloud per la gestione dei dati che fornisce un unico piano di controllo per un'ampia gamma di operazioni di backup e ripristino sia in ambienti on-premise che cloud. Per maggiori dettagli, controlla "[Documentazione NetApp Backup and Recovery](#)".

Passaggi di distribuzione SCV per VCF su NVMe

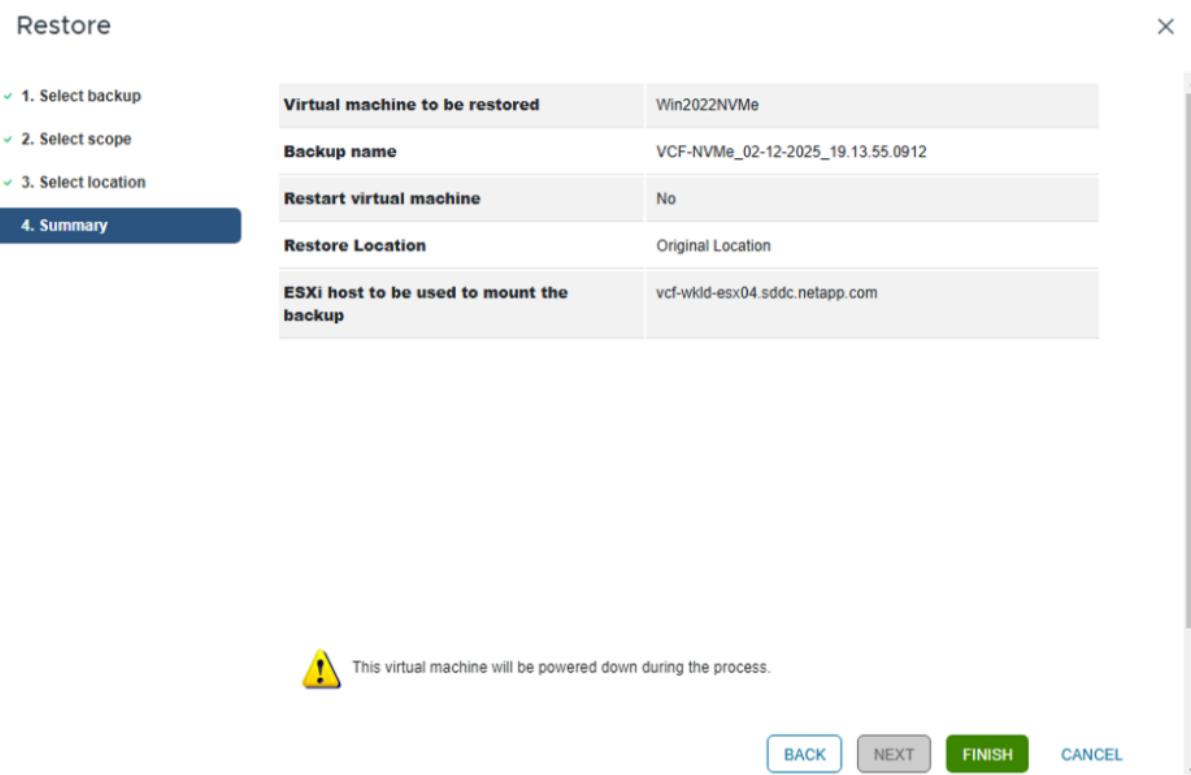
Il "[ONTAP tools for VMware vSphere](#)" (OTV) fornisce una soluzione potente ed efficiente per la gestione dello storage NetApp negli ambienti VMware. Integrandosi direttamente con vCenter Server, OTV semplifica la gestione dello storage, migliora la protezione dei dati e ottimizza le prestazioni. Sebbene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

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

Ripristina VM, datastore, disco virtuale e file o cartelle

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

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



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

Mount Datastore

X

ESXi host name vcf-wkld-esx03.sddc.netapp.com ▾

Backup

Search for Backups



(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-19-2025_...	2/19/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-18-2025_...	2/18/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-17-2025_...	2/17/2025 6:57:01 PM	Yes	wkld01	No
VCF-NVMe_02-16-2025_...	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_...	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_...	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_...	2/13/2025 6:57:01 PM	No	wkld01	No

Backup location

Backup type	Location
Primary	VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-19-2025_18.57.02.0052

CANCEL

MOUNT

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

Attach Virtual Disk(s) X

[Click here to attach to alternate VM](#)

Backup

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-17-2025_18....	2/17/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-16-2025_18....	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_18....	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_18....	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_18....	2/13/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-12-2025_19....	2/12/2025 7:13:55 PM	No	wkld01	No

Select disks

<input type="checkbox"/> Virtual disk	Location
<input checked="" type="checkbox"/>	[VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-17-2025_18.57.02.0697
<input type="checkbox"/>	

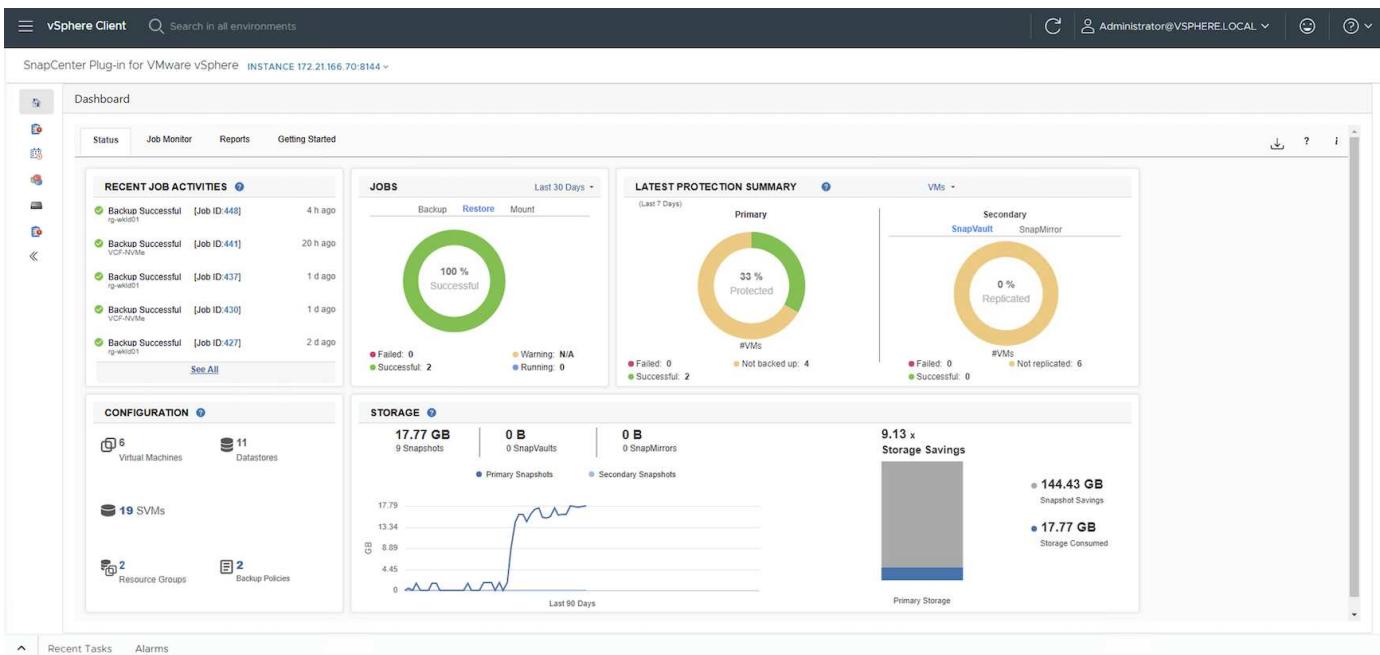
[CANCEL](#) [ATTACH](#)

- Fasi di ripristino di file e cartelle È possibile ripristinare singoli file e cartelle in una sessione di ripristino file guest, che allega una copia di backup di un disco virtuale e quindi ripristina i file o le cartelle selezionati. È possibile ripristinare anche file e cartelle. Maggiori dettagli controllano "Ripristino di file e cartelle SnapCenter ."
 - a. Quando si collega un disco virtuale per operazioni di ripristino di file o cartelle guest, la macchina virtuale di destinazione per il collegamento deve disporre di credenziali configurate prima del ripristino. Dal SnapCenter Plug-in for VMware vSphere , nella sezione plug-in, selezionare Ripristino file guest ed Esegui come credenziali, quindi immettere le credenziali utente. Per Nome utente, devi inserire "Amministratore".

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

Monitorare e segnalare

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



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

Proteggi i carichi di lavoro con vSphere Metro Storage Cluster

Scopri come integrare l'alta disponibilità ONTAP con VMware vSphere Metro Storage Cluster (vMSC)

Scopri le soluzioni NetApp che puoi utilizzare per integrare l'elevata disponibilità NetApp ONTAP con VMware vSphere Metro Storage Cluster (vMSC). Ciò fornisce soluzioni robuste per la gestione di VMware Cloud Foundation (VCF) e per i domini dei carichi di lavoro VI.

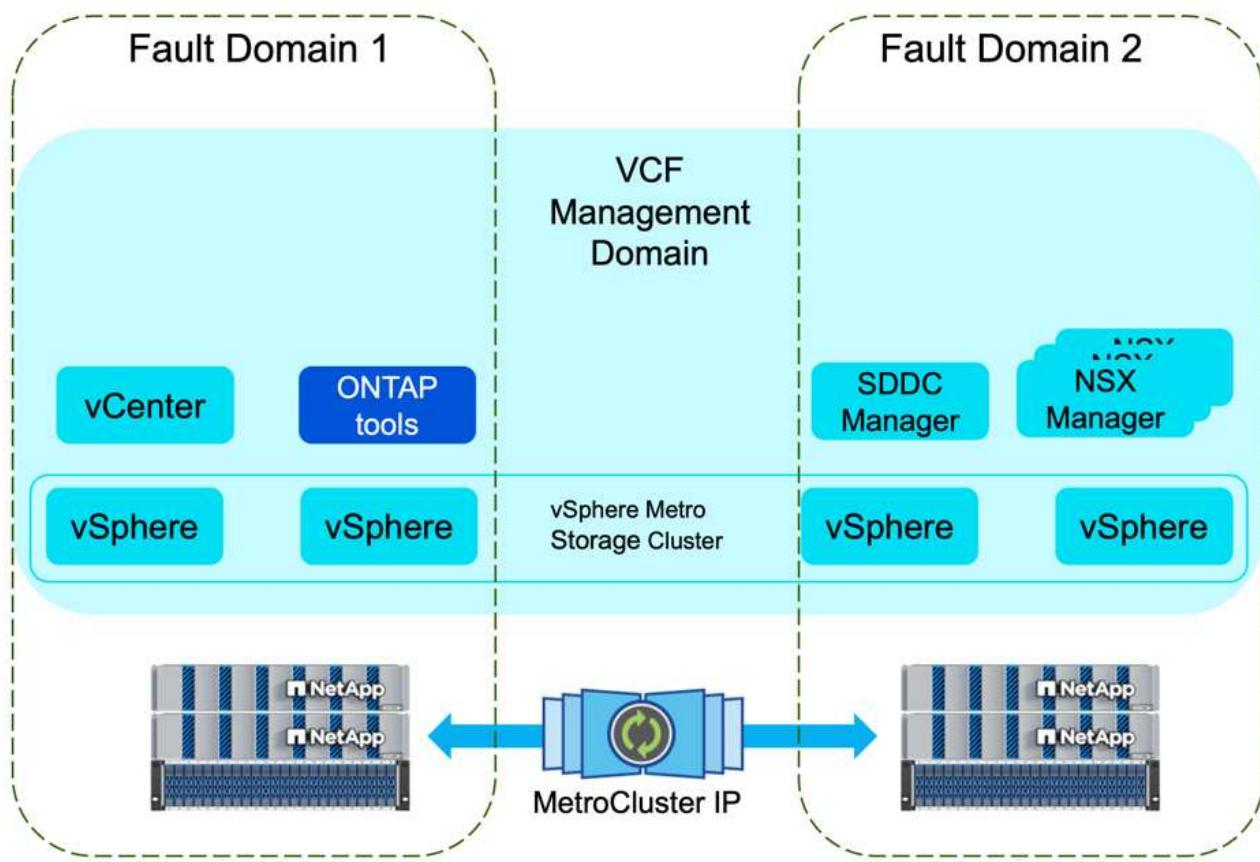
Questa combinazione garantisce la disponibilità continua dei dati, il failover senza interruzioni e il disaster recovery in siti geograficamente dispersi, migliorando la resilienza e la continuità operativa per i carichi di lavoro critici. La sincronizzazione attiva SnapMirror consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Non è necessario alcun intervento manuale o scripting personalizzato per attivare un failover con ActiveSync SnapMirror .

Per maggiori dettagli fare riferimento alle seguenti soluzioni.

- ["Cluster esteso per dominio di gestione mediante sincronizzazione attiva SnapMirror"](#)
- ["Cluster esteso per dominio di gestione tramite MetroCluster"](#)
- ["Cluster esteso per dominio del carico di lavoro VI utilizzando SnapMirror ActiveSync"](#)
- ["Stretch Cluster per il dominio del carico di lavoro VI utilizzando MetroCluster"](#)

Configurare un cluster esteso per un dominio di gestione VCF utilizzando MetroCluster

In questo caso d'uso descriviamo la procedura per configurare un cluster esteso per il dominio di gestione VMware Cloud Foundation (VCF) utilizzando ONTAP MetroCluster con NFS come datastore primario. Questa procedura include la distribuzione di host vSphere e vCenter Server, il provisioning di datastore NFS, la convalida del cluster con VCF Import Tool, la configurazione delle impostazioni NSX e la conversione dell'ambiente in un dominio di gestione VCF.



Introduzione

In questa soluzione mostreremo come implementare Stretched VCF Management Domain con NFS come Principal Datastore utilizzando ONTAP MetroCluster.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci host vSphere e server vCenter.
- Fornire il datastore NFS agli host vSphere.
- Distribuire SDDC Manager nel cluster vSphere.
- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.

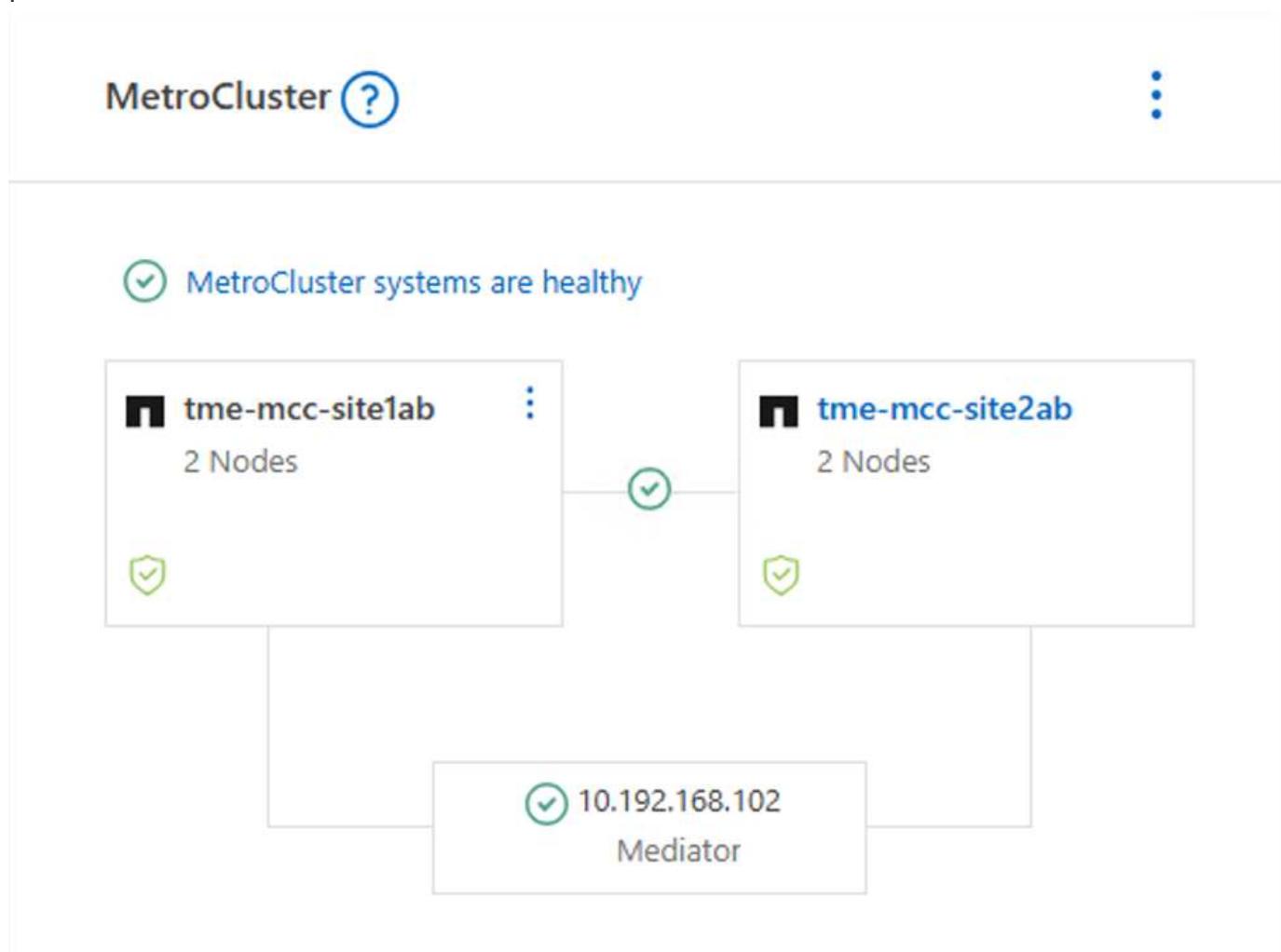
- Configurare un file JSON per creare un NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per convertire l'ambiente vSphere 8 in un dominio di gestione VCF.

Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Configurazione ONTAP MetroCluster supportata
- Macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi connessi allo switch di rete.
- Scarica il software necessario per la conversione VCF.

Ecco uno screenshot di esempio di System Manager che mostra la configurazione MetroCluster



ed ecco le interfacce di rete SVM da entrambi i domini di errore.

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a	
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a	
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b	
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b	

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node	↑
<input type="text"/>		<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>	
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a	
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a	
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b	
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b	

[NOTA] SVM sarà attivo su uno dei domini di errore in MetroCluster.

NetApp ONTAP System Manager | tme-mcc-site1ab

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	

NetApp ONTAP System Manager | tme-mcc-site2ab

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	

Fare riferimento "vMSC con MetroCluster".

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

Prima di creare un cluster vSphere che verrà convertito in VCF Management Domain, fare riferimento "["Considerazioni NSX su vSphere Cluster"](#)"

Per il software richiesto fare riferimento a "["Scarica il software per convertire o importare ambienti vSphere esistenti"](#)" .

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#)" centro.

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

Fasi di distribuzione

Per distribuire VCF Stretched Management Domain con NFS come Principal Datastore,

Completare i seguenti passaggi:

- Distribuisci host vSphere e vCenter.
- Creare un cluster vSphere.
- Fornire un datastore NFS.
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Distribuire la VM del gestore SDDC sul cluster vCenter.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di conversione.
- Caricare il software richiesto nel gestore SDDC.
- Convertire il cluster vSphere in un dominio di gestione VCF.

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

Distribuisci host vSphere e vCenter

Distribuisci vSphere sugli host utilizzando l'ISO scaricato dal portale di supporto Broadcom oppure utilizza l'opzione di distribuzione esistente per l'host vSphere.

Montare NFS Datastore per ospitare le VM

In questo passaggio creiamo il volume NFS e lo montiamo come Datastore per ospitare le VM.

1. Utilizzando System Manager, creare un volume e collegarlo alla policy di esportazione che include la subnet IP dell'host vSphere.

Add volume

Name
NFS01

Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity
1024 GiB

Performance service level
Extreme

Not sure? [Get help selecting type](#)

Optimization options

Distribute volume data across the cluster (FlexGroup) [?](#)

Advanced capacity balancing
ONTAP distributes file data to maintain balance as files grow.

Access permissions

Export via NFS

GRANT ACCESS TO HOST
default

Create a new export policy, or select an existing export policy.

2. Eseguire l'SSH sull'host vSphere e montare il datastore NFS.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name Host Share Vmknic Accessible Mounted Connections Read-Only isPE Hardware Acceleration
----- -----
NFS01 10.192.164.225 /NFS01 None true true 4 false false Not Supported
[root@SiteA-vs01:~]
```

3. Ripetere i passaggi precedenti per ogni ulteriore necessità di datastore e assicurarsi che l'accelerazione hardware sia supportata.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name Host Share Vmknic Accessible Mounted Connections Read-Only isPE Hardware Acceleration
----- -----
NFS02 10.192.164.230 /NFS02 None true true 4 false false Supported
NFS01 10.192.164.225 /NFS01 None true true 4 false false Supported
[root@MCCA01:~]
```

Distribuisci vCenter su NFS Datastore. Assicurarsi che SSH e Bash shell siano abilitati sull'appliance vCenter.

Crea un cluster vSphere

1. Accedi al client Web vSphere, crea il DataCenter e il cluster vSphere aggiungendo uno degli host in cui è distribuito NFS VAAI. Abbiamo scelto di gestire tutti gli host nel cluster con l'opzione immagine singola. [SUGGERIMENTO] Non selezionare Gestisci configurazione a livello di cluster. Per ulteriori dettagli, fare riferimento "[Considerazioni NSX su vSphere Cluster](#)". Per le best practice vMSC con ONTAP MetroCluster, controlla "[Linee guida per la progettazione e l'implementazione di vMSC](#)"
2. Aggiungere altri host vSphere al cluster.
3. Creare uno switch distribuito e aggiungere i gruppi di porte.
4. "[Migrazione della rete da vSwitch standard a switch distribuito.](#)"

Convertire l'ambiente vSphere in un dominio di gestione VCF

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

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

Per ulteriori informazioni, consulta "[Opzioni e parametri dello strumento di importazione VCF](#)" .

Copia ed estrai lo strumento di importazione VCF

Lo strumento di importazione VCF viene utilizzato sull'appliance vCenter per convalidare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

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

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

Convalida l'appliance vCenter

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

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

```
[root@mcc-vc01 ~]/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset # python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,001] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Pre-checks started for vCenter: mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...
[2025-03-20 23:02:06,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] EUM ring topology check...
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] MCP import check...
[2025-03-20 23:02:10,880] [INFO] vc_precheck: Pre-checks completed successfully
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
[root@mcc-vc01 ~]/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset #
```

Distribuire SDDC Manager

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

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

The screenshot shows the vSphere Client interface. On the left, the navigation tree is visible with 'mcc-vc01.sddc.netapp.com' expanded, showing 'RTP' and 'vMSC' subfolders. The 'vMSC' folder is currently selected. The right panel displays 'Cluster Details' for the selected cluster, showing metrics like 'Total Processors: 32' and 'Total vMotion Migrations: 4'. The top bar shows the title 'vSphere Client' and a search bar.

Fare riferimento a ["Distribuire l'appliance SDDC Manager sul vCenter di destinazione"](#).

Creare un file JSON per la distribuzione NSX

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



Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzato il segmento supportato da NSX VLAN. Per maggiori dettagli sulle limitazioni del segmento supportato da NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a ["Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation"](#).

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

```
{  
    "deploy_without_license_keys": true,  
    "form_factor": "small",  
    "admin_password": "*****",  
    "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-  
133764.zip",  
    "cluster_ip": "10.61.185.114",  
    "cluster_fqdn": "mcc-nsx.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "mcc-nsxa.sddc.netapp.com",  
            "name": "mcc-nsxa",  
            "ip_address": "10.61.185.111",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-nsxb.sddc.netapp.com",  
            "name": "mcc-nsxb",  
            "ip_address": "10.61.185.112",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-nsxc.sddc.netapp.com",  
            "name": "mcc-nsxc",  
            "ip_address": "10.61.185.113",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

Copiare il file JSON nella cartella home dell'utente vcf su SDDC Manager.

Carica il software su SDDC Manager

Copiare lo strumento di importazione VCF nella cartella home dell'utente vcf e il bundle di distribuzione NSX nella cartella /nfs/vmware/vcf/nfs-mount/bundle/ su SDDC Manager.

Vedere "[Caricare il software richiesto sull'appliance SDDC Manager](#)" per istruzioni dettagliate.

Controllo dettagliato su vCenter prima della conversione

Prima di eseguire un'operazione di conversione del dominio di gestione o un'operazione di importazione del dominio del carico di lavoro VI, è necessario eseguire un controllo dettagliato per assicurarsi che la configurazione dell'ambiente vSphere esistente sia supportata per la conversione o l'importazione. . Eseguire l'accesso SSH all'appliance SDDC Manager come utente vcf. . Passare alla directory in cui è stato copiato lo strumento di importazione VCF. . Eseguire il seguente comando per verificare che l'ambiente vSphere possa essere convertito

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user  
'<sso-user>' --sso-password '*****' --local-admin-password  
'*****' --accept-trust
```

Convertire il cluster vSphere in dominio di gestione VCF

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF.

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

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user '' --sso-password '*****' --vcenter-root-password '*****' --local-admin-password '*****' --backup-password '*****' --domain-name '<Mgmt-domain-name>' --accept-trust --nsx-deployment-spec-path /home/vcf/nsx.json
```

Quando sull'host vSphere sono disponibili più Datastore, viene richiesto quale Datastore deve essere considerato come Datastore primario su quali VM NSX verranno distribuite per impostazione predefinita.

```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: =====
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: =====
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
[2025-03-24 19:29:25,193] [INFO] discover_domain: =====
```

Per istruzioni complete, fare riferimento a ["Procedura di conversione VCF"](#).

Le VM NSX verranno distribuite su vCenter.

The screenshot shows the vSphere Client interface. On the left, there is a navigation tree with the following structure:

- mcc-vc01.sddc.netapp.com
 - RTP
 - vMSC
 - vmSC-mgmt-001
 - mcc-nsxa
 - mcc-nsxb
 - mcc-nsxc
 - mcc-vc01
 - mcc-vcf01

The "vMSC" item is selected and highlighted in blue. To the right of the navigation tree, there is a "Cluster Details" panel. The panel title is "vMSC". Below the title, there is a summary section with the following data:

Total Processors:	32
Total vMotion Migrations:	5

Below the summary, there are two small icons: a bar chart icon and a gear icon.

SDDC Manager mostra il dominio di gestione creato con il nome fornito e NFS come

Datastore.

The screenshot shows the vSphere Cloud Foundation interface. The left sidebar is expanded to show the 'Lifecycle Management' section. The main content area is titled 'Workload Domains' and displays a summary of capacity utilization across domains. It includes four progress bars: CPU (73.44 GHz Total, 6.88 GHz Used), Memory (511.98 GB Total, 470.5 GB Used), vSAN Storage Usage (57%), and NFS Storage (3 TB Total, 1.7 TB Used). Below these bars is a detailed table of workload domains. One row is selected, showing 'MCC_Mig...' as the domain, 'MAN...' as the type, and various usage metrics like CPU Usage (8%), Memory Usage (8%), and vVol Storage Usage (57%). The table also includes columns for Configuration Status (ACTIVE), Cluster (1 Cluster), Hosts (4), and Updates Available (Up-to-date). A note at the bottom right indicates 1 domain.

Domain	Type	CPU Usage	Memory Usage	vSAN Storage Usage	NFS Storage Usage	vMFS on FC Storage Usage	vVol Storage Usage	Configuration Status	Cluster	Hosts	Updates Available
MCC_Mig...	MAN...	8%	8%	-	57%	-	-	ACTIVE	1 Cluster	4	Up-to-date

Durante l'ispezione del cluster, vengono fornite le informazioni del datastore NFS.

The screenshot shows the vSphere Cloud Foundation interface. The left sidebar is expanded to show the 'Lifecycle Management' section. The main content area is titled 'vMSC' and shows the 'Summary' tab. It displays resource usage for CPU (24.61 GHz used of 73.44 GHz) and Memory (89.68 GB used of 511.98 GB). Below this is a 'Storage' section for an NFS datastore. It lists two entries: 'NFS01' (Server: 10.192.164.225, Folder: /NFS01) and 'NFS02' (Server: 10.192.164.230, Folder: /NFS02). On the right side, there is a 'Tags' panel with a single tag 'vft_imported' and a 'ASSIGN' button.

Aggiungere la licenza al VCF

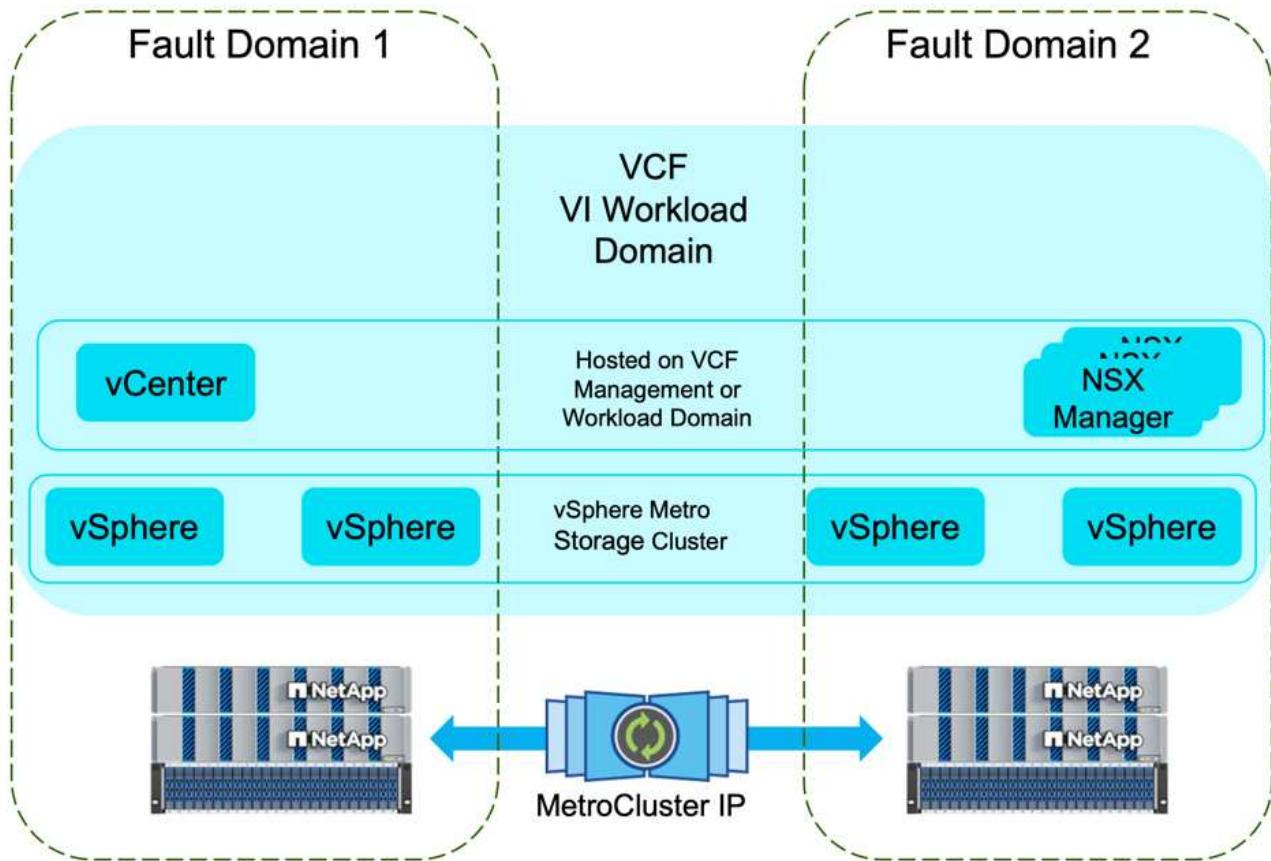
Dopo aver completato la conversione, è necessario aggiungere la licenza all'ambiente.

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

Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando MetroCluster

In questo caso d'uso descriviamo la procedura per configurare il dominio del carico di lavoro VCF VI esteso con NFS come datastore principale utilizzando ONTAP MetroCluster. Questa procedura include la distribuzione di host vSphere e vCenter Server, il provisioning di datastore NFS, la convalida del cluster vSphere, la configurazione di NSX durante la conversione VCF e l'importazione dell'ambiente vSphere in un dominio di gestione VCF esistente.

I carichi di lavoro su VCF sono protetti da vSphere Metro Storage Cluster (vMSC). ONTAP MetroCluster con distribuzione FC o IP viene in genere utilizzato per garantire la tolleranza agli errori dei datastore VMFS e NFS.



Introduzione

In questa soluzione mostreremo come implementare il dominio del carico di lavoro VCF VI esteso con NFS come datastore principale utilizzando ONTAP MetroCluster. Il dominio del carico di lavoro VI può essere distribuito tramite SDDC Manager oppure importando un ambiente vSphere esistente come dominio del carico di lavoro VI.

Panoramica dello scenario

Questo scenario comprende i seguenti passaggi di alto livello:

- Distribuisci host vSphere e server vCenter.
- Fornire il datastore NFS agli host vSphere.
- Utilizzare lo strumento di importazione VCF per convalidare il cluster vSphere.
- Configurare un file JSON per creare un NSX durante la conversione VCF.
- Utilizzare lo strumento di importazione VCF per importare l'ambiente vSphere 8 come dominio del carico di lavoro VCF VI in un dominio di gestione VCF esistente.

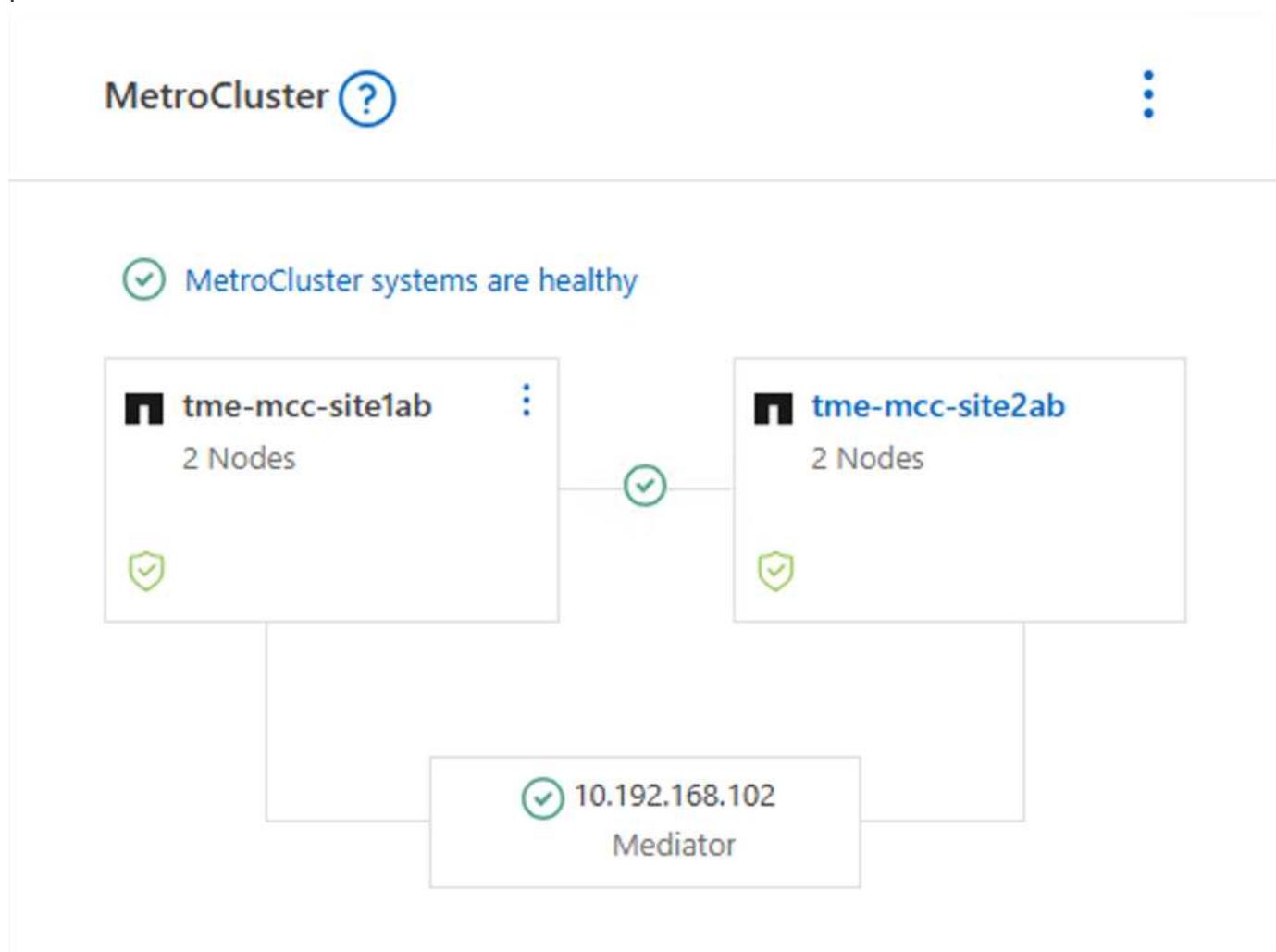
Prerequisiti

Questo scenario richiede i seguenti componenti e configurazioni:

- Configurazione ONTAP MetroCluster supportata

- Macchina virtuale di archiviazione (SVM) configurata per consentire il traffico NFS.
- È stata creata un'interfaccia logica (LIF) sulla rete IP che deve trasportare il traffico NFS ed è associata all'SVM.
- Un cluster vSphere 8 con 4 host ESXi connessi allo switch di rete.
- Scarica il software necessario per la conversione VCF.

Ecco uno screenshot di esempio di System Manager che mostra la configurazione MetroCluster



ed ecco le interfacce di rete SVM da entrambi i domini di errore.

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
<input type="text"/>	<input type="checkbox"/>	<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc02_8775	!	ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118	✓	ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778	!	ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783	✓	ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
<input type="text"/>	<input type="checkbox"/>	<input type="text"/> ch-svm	<input type="text"/>	<input type="text"/>	<input type="text"/>
lif_ch-svm-mcc01_3118	!	ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775	✓	ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783	!	ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778	✓	ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] SVM sarà attivo su uno dei domini di errore in MetroCluster.

NetApp ONTAP System Manager | tme-mcc-site1ab

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	<input type="radio"/>
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	<input type="radio"/>

NetApp ONTAP System Manager | tme-mcc-site2ab

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	<input type="radio"/>
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	<input type="radio"/>

Fare riferimento "vMSC con MetroCluster".

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

Prima di creare un cluster vSphere che verrà convertito in VCF Management Domain, fare riferimento "["Considerazioni NSX su vSphere Cluster"](#)" .

Per il software richiesto fare riferimento a "["Scarica il software per convertire o importare ambienti vSphere esistenti"](#)" .

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#)" centro.

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

Fasi di distribuzione

Per distribuire VCF Stretched Management Domain con NFS come Principal Datastore,

Completare i seguenti passaggi:

- Distribuisci host vSphere e vCenter.
- Creare un cluster vSphere.
- Fornire un datastore NFS.
- Copiare lo strumento di importazione VCF nell'appliance vCenter.
- Eseguire un controllo preliminare sull'appliance vCenter utilizzando lo strumento di importazione VCF.
- Creare un file JSON per un cluster NSX da distribuire durante il processo di importazione.
- Caricare il software richiesto nel gestore SDDC.
- Convertire il cluster vSphere in un dominio di carico di lavoro VCF VI.

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

Distribuisci host vSphere e vCenter

Distribuisci vSphere sugli host utilizzando l'ISO scaricato dal portale di supporto Broadcom oppure utilizza l'opzione di distribuzione esistente per l'host vSphere.

Montare NFS Datastore per ospitare le VM

In questo passaggio creiamo il volume NFS e lo montiamo come Datastore per ospitare le VM.

1. Utilizzando System Manager, creare un volume e collegarlo alla policy di esportazione che include la subnet IP dell'host vSphere.

Add volume

Name
WLD01_DS01

Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity
500 GiB

Performance service level
Extreme

Not sure? [Get help selecting type](#)

Optimization options
 Distribute volume data across the cluster (FlexGroup) [?](#)

Access permissions

Export via NFS

GRANT ACCESS TO HOST
default

Create a new export policy, or select an existing export policy.

Rule index	Clients	Access protocols	Read-only rule	Re
9	0.0.0.0/0	NFSv3, NFSv4, SMB/CIFS, NFS	Any	Any

2. Eseguire l'SSH sull'host vSphere e montare il datastore NFS.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

Distribuisci vCenter su NFS Datastore. Assicurarsi che SSH e Bash shell siano abilitati sull'appliance vCenter.

The screenshot shows the vSphere Client interface. On the left, there's a navigation sidebar with icons for hosts, datacenters, clusters, and datastores. Below this is a tree view of hosts under a cluster named RTP. The host 'siteb-vs02.sddc.netapp.com' is selected and highlighted in blue. At the top right, there's a search bar and a 'Search in all environments' button. The main pane shows the host details for 'siteb-vs02.sddc.netapp.com'. The 'Host Details' section includes a summary card with a server icon and the host's name. To the right, a table provides specific hardware information:

Hypervisor:	VMware ESXi, 8.0.3, 24280767
Model:	
Processor Type:	Intel(R) Xeon(R) Gold 5120 C PU @ 2.20GHz
Logical Processors:	12
NICs:	2
Virtual Machines:	1
State:	Connected
Uptime:	19 hours

Crea un cluster vSphere

1. Accedi al webclient vSphere, crea il DataCenter e il cluster vSphere aggiungendo uno degli host in cui è distribuito NFS VAAI. Abbiamo scelto di gestire tutti gli host nel cluster con l'opzione immagine singola. [SUGGERIMENTO] Non selezionare Gestisci configurazione a livello di cluster. Per ulteriori dettagli, fare riferimento "[Considerazioni NSX su vSphere Cluster](#)". Per le best practice vMSC con ONTAP MetroCluster, controlla "[Linee guida per la progettazione e l'implementazione di vMSC](#)"
2. Aggiungere altri host vSphere al cluster.
3. Creare uno switch distribuito e aggiungere i gruppi di porte.
4. "[Migrazione della rete da vSwitch standard a switch distribuito.](#)"

Convertire l'ambiente vSphere in un dominio di carico di lavoro VCF VI

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

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

Per ulteriori informazioni, consulta "[Opzioni e parametri dello strumento di importazione VCF](#)" .

Copia ed estrai lo strumento di importazione VCF

Lo strumento di importazione VCF viene utilizzato sull'appliance vCenter per convalidare che il cluster vSphere sia in uno stato di integrità per il processo di conversione o importazione VCF.

Completare i seguenti passaggi:

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

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

Convalida l'appliance vCenter

Utilizzare lo strumento di importazione VCF per convalidare l'appliance vCenter prima dell'importazione come dominio del carico di lavoro VI.

1. Segui i passaggi a ["Eseguire un pre-controllo sul vCenter di destinazione prima della conversione"](#) per eseguire la convalida.

Creare un file JSON per la distribuzione NSX

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



Quando si distribuisce un cluster NSX Manager in un'operazione di conversione o importazione, viene utilizzato il segmento supportato da NSX VLAN. Per maggiori dettagli sulle limitazioni del segmento supportato da NSX-VLAN, fare riferimento alla sezione "Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation". Per informazioni sulle limitazioni di rete NSX-VLAN, fare riferimento a ["Considerazioni prima di convertire o importare ambienti vSphere esistenti in VMware Cloud Foundation"](#).

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

```
{  
    "deploy_without_license_keys": true,  
    "form_factor": "small",  
    "admin_password": "*****",  
    "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-  
133764.zip",  
    "cluster_ip": "10.61.185.105",  
    "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",  
    "manager_specs": [  
        {  
            "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",  
            "name": "mcc-wld01-nsxa",  
            "ip_address": "10.61.185.106",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",  
            "name": "mcc-wld01-nsxb",  
            "ip_address": "10.61.185.107",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        },  
        {  
            "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",  
            "name": "mcc-wld01-nsxc",  
            "ip_address": "10.61.185.108",  
            "gateway": "10.61.185.1",  
            "subnet_mask": "255.255.255.0"  
        }]  
}
```

Copiare il file JSON nella cartella home dell'utente vcf su SDDC Manager.

Carica il software su SDDC Manager

Copiare lo strumento di importazione VCF nella cartella home dell'utente vcf e il bundle di distribuzione NSX nella cartella /nfs/vmware/vcf/nfs-mount/bundle/ su SDDC Manager.

Vedere ["Caricare il software richiesto sull'appliance SDDC Manager"](#) per istruzioni dettagliate.

Controllo dettagliato su vCenter prima della conversione

Prima di eseguire un'operazione di conversione del dominio di gestione o un'operazione di importazione del dominio del carico di lavoro VI, è necessario eseguire un controllo dettagliato per assicurarsi che la configurazione dell'ambiente vSphere esistente sia supportata per la conversione o l'importazione. . Eseguire l'accesso SSH all'appliance SDDC Manager come utente vcf. . Passare alla directory in cui è stato copiato lo strumento di importazione VCF. . Eseguire il seguente comando per verificare che l'ambiente vSphere possa essere convertito

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user '' --sso-password '*****' --local-admin-password '*****' --accept-trust
```

```
[root@vcf ~]# cd vcf-brownfield-import-5.2.1.2-24494570/vcf_brownfield_toolset/
[vcf ~]# ./vcf_brownfield-import-5.2.1.2-24494570/vcf_brownfield-toolset ls python3 vcf_brownfield.py check
[2025-03-23 17:48:44,979] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:48:44,980] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Usage: vcf_brownfield.py check [-h] --vcenter VCENTER_ADDRESS --sso-user SSO_USERNAME [-sso-password SSO_PASSWORD] [-l local-admin-password LOCAL_ADMIN_PASSWORD] [-skip-nsx-deployment-checks] [-accept-trust]
vcf_brownfield.py check [-h] --vcenter VCENTER_ADDRESS --sso-user SSO_USERNAME [-sso-password SSO_PASSWORD] [-l local-admin-password LOCAL_ADMIN_PASSWORD] [-skip-nsx-deployment-checks] [-accept-trust]
[2025-03-23 17:41:46,491] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-23 17:41:46,492] [INFO] vcf_brownfield: Generating SDDC Manager public API token
[2025-03-23 17:41:46,490] [INFO] vcf_brownfield: Using cached SDDC Manager controller info
[2025-03-23 17:41:46,001] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:46,941] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:46,940] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:46,939] [INFO] vcf_brownfield: Response status from retrieving domain: 200
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Retrieving SDDC Manager controller info
[2025-03-23 17:41:47,016] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:47,511] [INFO] request_helper: Response status from SDDC Manager controller info retrieval: 200
[2025-03-23 17:41:47,510] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,504] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,505] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47,661] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47,660] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:48,114] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:48,115] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:48,080] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:48,079] [INFO] sddc_manager_helper: Adding new trusted certificate for alias: 9ca849d6698cc841d51adace980eb7f85c4a0b7f with thumbprint: DA:6F:94:90:D9:83:66:6E:7:CD:68:49:EC:9B:2:E:03:EA:A0:S7:ED:8B:EC:03:5C:31:8C:40:4C:10:48:4F:4F
[2025-03-23 17:41:48,085] [INFO] sddc_manager_certificate_utils: Adding new trusted certificate for alias: mce-vc02.sddc.netapp.com with thumbprint: 94:F3:C7:05:DF:FF:E6:C9:68:66:5B:92:3C:B7:7D:15:85:6B:3B:A1:FD:27:2B:56:60:85:FA:D5:82:AE:3C:46
[2025-03-23 17:41:50,085] [INFO] sddc_manager_helper: Importing trusted certificates to SDDC Manager trust store
[2025-03-23 17:41:50,074] [INFO] request_helper: Response status from certificates import: 200
[2025-03-23 17:41:53,381] [INFO] request_helper: Response status from certificates import: 200
```

Convertire il cluster vSphere in un dominio di carico di lavoro VCF VI

Per eseguire il processo di conversione viene utilizzato lo strumento di importazione VCF.

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

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user '' --sso-password '*****' --vcenter-root-password '*****' --local-admin-password '*****' --backup-password '*****' --domain-name '<Mgmt-domain-name>' --accept-trust --nsx-deployment-spec-path /home/vcf/nsx.json
```

Anche se sull'host vSphere sono disponibili più Datastore, non è necessario specificare quale Datastore deve essere considerato come Datastore primario.

Per istruzioni complete, fare riferimento a "[Procedura di conversione VCF](#)" .

Le VM NSX verranno distribuite su vCenter.

The screenshot shows the vSphere Client interface. The left sidebar displays a tree view of hosts and datastores under the 'RTP' category. One host, 'siteb-vs02.sddc.netapp.com', is selected and highlighted with a black border. The main pane shows the 'Host Details' for this selected host. The 'Actions' tab is visible at the top right of the main pane. The 'Host Details' section contains the following information:

Host Details
Hypervisor: VMware ESXi, 8.0.3, 24280767
Model: Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Logical Processors: 12
NICs: 2
Virtual Machines: 2
State: Connected
Uptime: 20 hours

SDDC Manager mostra il dominio del carico di lavoro VI creato con il nome fornito e NFS come Datastore.

Workload Domains

Capacity Utilization across Domains

	CPU	Memory	NFS Storage
Total	177.84 GHz Total 35.67 GHz Used	1,023.97 GB Total 184.45 GB Used	3.98 TB Total 1.76 TB Used
Free	128.17 GHz Free	905.52 GB Free	2.22 TB Free

Domain Type CPU Usage Memory Usage vSAN Storage Usage NFS Storage Usage VMFS on FC Storage Usage vVol Storage Usage Configuration Status Cluster Hosts Updates Available

Domain	Type	CPU Usage	Memory Usage	vSAN Storage Usage	NFS Storage Usage	VMFS on FC Storage Usage	vVol Storage Usage	Configuration Status	Cluster	Hosts	Updates Available
MCC-Mg_	MANAGED	36%	18%	-	58%	-	-	ACTIVE	1 Cluster	4	✓ Up-to-date
WLD01	VMWARE	13%	6%	-	2%	-	-	ACTIVE	1 Cluster	4	✓ Up-to-date

Show Or Hide Column

Durante l'ispezione del cluster, vengono fornite le informazioni sui datastore NFS.

BACK TO WLD01

Stretch Cluster

ACTIONS Managed by image

ACTIVE

Summary Network Hosts

Resource Usage

CPU	Memory
13.16 GHz used of 104.4 GHz (91.24 GHz free)	28.69 GB used of 511.99 GB (483.3 GB free)

Tags

- vft_IMPORTED_VCF_IMPORTED_CLUSTER

ASSIGN

Storage

NFS

Datastore Name	Server	Folder
DS02	10.192.164.230	/WLD01_DS02
DS01	10.192.164.225	/WLD01_DS01

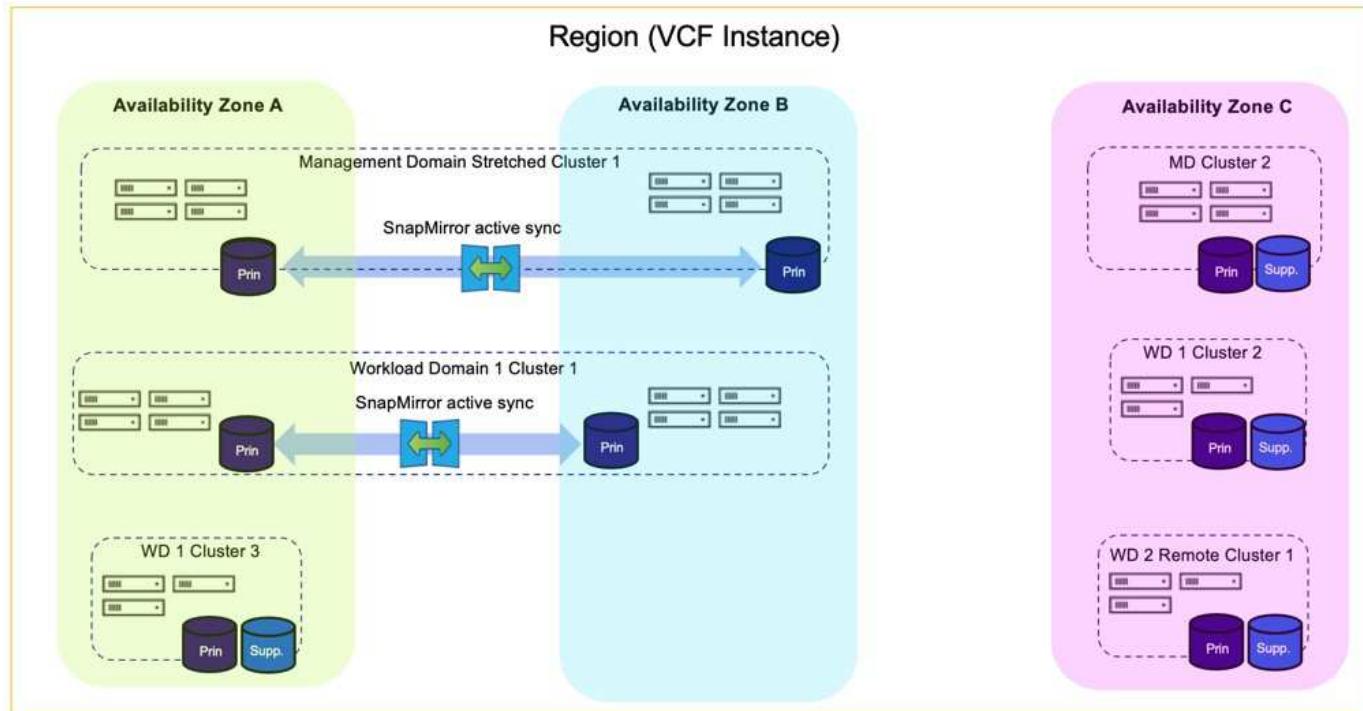
Aggiungere la licenza al VCF

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

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

Configurare un cluster esteso per un dominio di gestione VCF utilizzando SnapMirror Active Sync

In questo caso d'uso descriviamo la procedura per utilizzare gli ONTAP tools for VMware vSphere per configurare un cluster esteso per un dominio di gestione VCF. Questa procedura include la distribuzione di host vSphere e vCenter Server, l'installazione di strumenti ONTAP , la protezione dei datastore con SnapMirror Active Sync, la migrazione delle VM verso datastore protetti e la configurazione di storage supplementare.

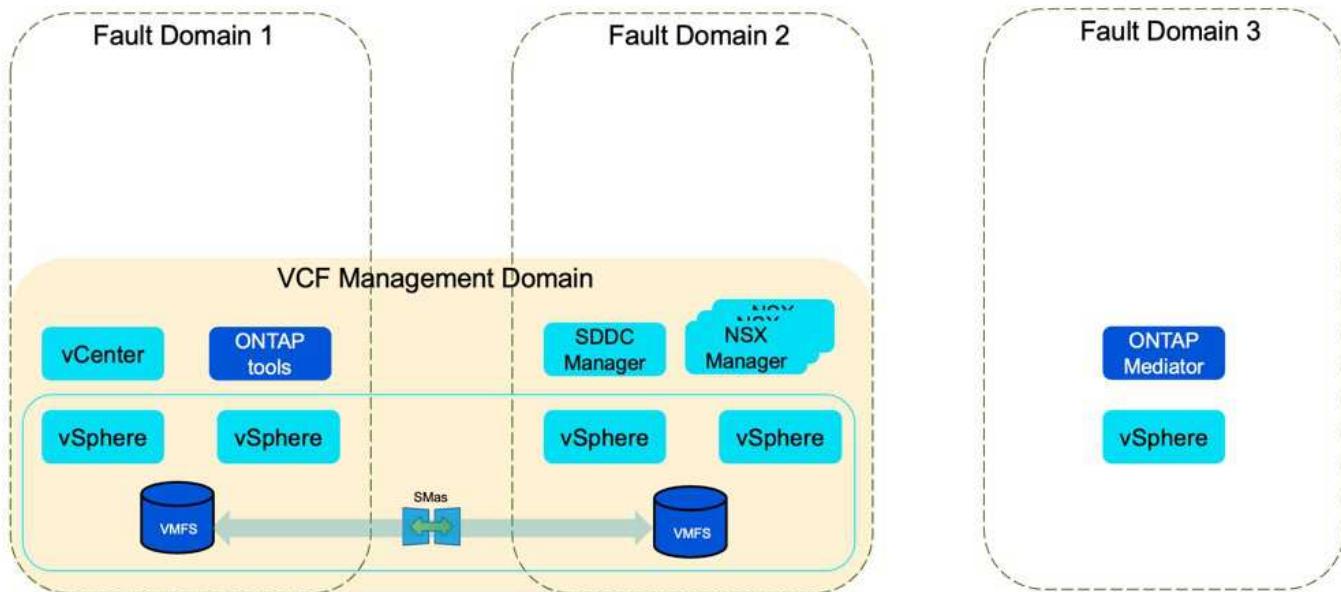


Panoramica dello scenario

La soluzione Stretch Cluster può essere implementata sul cluster predefinito o su un cluster aggiuntivo nei domini di gestione o di carico di lavoro VCF. VMFS su FC è supportato sia sul datastore principale che sui

datastore supplementari. VMFS su iSCSI è supportato solo con datastore supplementari. Fare riferimento a IMT per il supporto di VMFS su NVMe-oF con SnapMirror ActiveSync.

VMFS with FC



Archiviazione principale sul dominio di gestione

A partire da VCF 5.2, il dominio di gestione può essere distribuito senza VSAN utilizzando lo strumento di importazione VCF. L'opzione di conversione dello strumento di importazione VCF consente "[una distribuzione vCenter esistente in un dominio di gestione](#)". Tutti i cluster in vCenter diventeranno parte del dominio di gestione.

1. Distribuisci host vSphere
2. Distribuire il server vCenter sul datastore locale (vCenter deve coesistere sugli host vSphere che verranno convertiti nel dominio di gestione)
3. Distribuisci gli ONTAP tools for VMware vSphere
4. Distribuisci il plug-in SnapCenter per VMware vSphere (facoltativo)
5. Creare un datastore (la configurazione della zona FC deve essere a posto)
6. Proteggere il cluster vSphere
7. Migrare le VM al datastore appena creato



Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Archiviazione supplementare sul dominio di gestione

Una volta che il dominio di gestione è attivo e funzionante, è possibile creare datastore aggiuntivi utilizzando gli strumenti ONTAP che attiveranno l'espansione del gruppo di coerenza.



Se un cluster vSphere è protetto, saranno protetti tutti i datastore nel cluster.

Se l'ambiente VCF viene distribuito con lo strumento Cloud Builder, per creare l'archiviazione supplementare con iSCSI, distribuire gli strumenti ONTAP per creare il datastore iSCSI e proteggere il cluster vSphere.



Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "[Documentazione ONTAP 9](#)" centro.

Per informazioni sulla configurazione di VCF fare riferimento a "[Documentazione di VMware Cloud Foundation 5.2](#)".

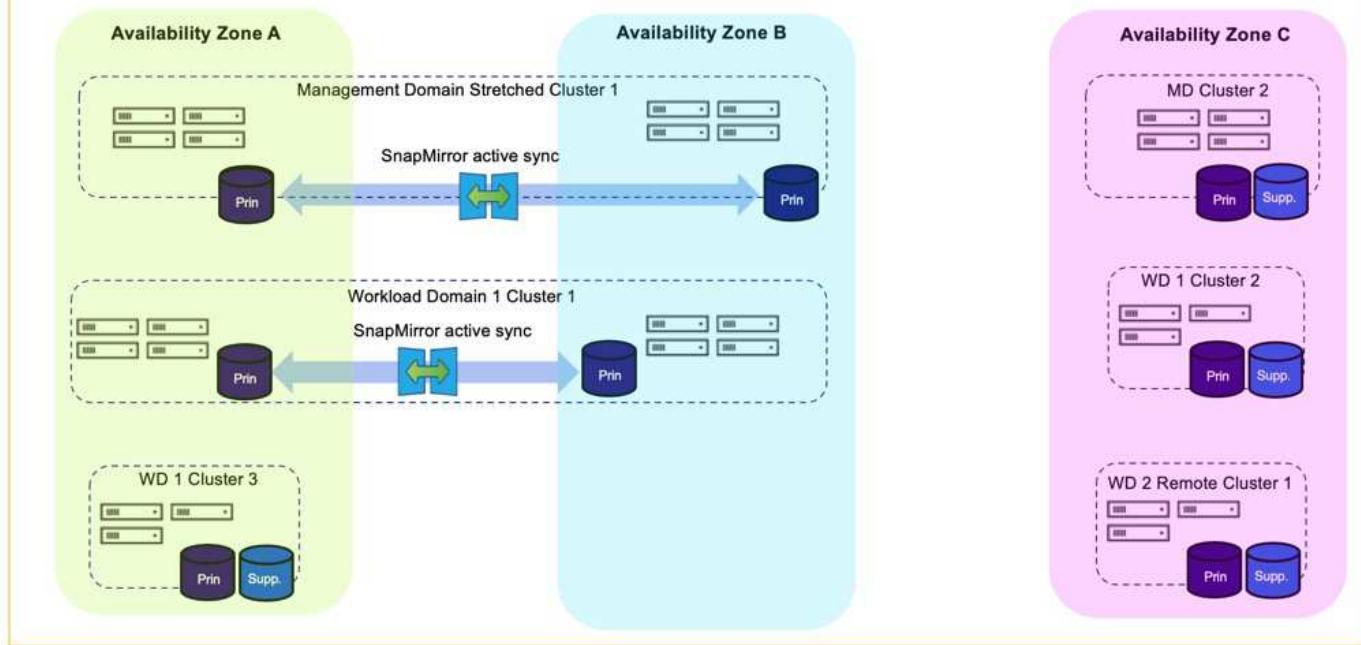
Demo video per questa soluzione

[Cluster di allungamento per VCF con strumenti ONTAP](#)

Configurare un cluster esteso per un dominio di carico di lavoro VI utilizzando SnapMirror Active Sync

In questo caso d'uso descriviamo la procedura per configurare un cluster esteso per un dominio di carico di lavoro di un'infrastruttura virtuale (VI) utilizzando SnapMirror Active Sync con ONTAP tools for VMware vSphere. Questa procedura include la creazione di un dominio di carico di lavoro VCF con VMFS su Fibre Channel, la registrazione di vCenter con strumenti ONTAP, la registrazione dei sistemi di storage e la protezione del cluster vSphere.

Region (VCF Instance)



Panoramica dello scenario

Gli archivi dati sul dominio VCF Workload possono essere protetti con SnapMirror ActiveSync per fornire una soluzione di cluster estensibile. La protezione è abilitata a livello di cluster vSphere e tutti i datastore a blocchi ONTAP nel cluster saranno protetti.

Archiviazione principale sul dominio del carico di lavoro

Il dominio del carico di lavoro può essere creato importandolo tramite lo strumento di importazione VCF oppure distribuendolo tramite il gestore SDDC. L'implementazione con SDDC Manager fornirà più opzioni di rete rispetto all'importazione di un ambiente esistente.

1. Crea un dominio di carico di lavoro con VMFS su FC
2. ["Registra il dominio del carico di lavoro vCenter nel gestore degli strumenti ONTAP per distribuire il plug-in vCenter"](#)
3. ["Registrare i sistemi di archiviazione sugli strumenti ONTAP"](#)
4. ["Proteggere il cluster vSphere"](#)



Ogni volta che il cluster viene espanso o ridotto, è necessario aggiornare la relazione Host Cluster sugli strumenti ONTAP per il cluster, per indicare le modifiche apportate all'origine o alla destinazione.

Archiviazione supplementare sul dominio del carico di lavoro

Una volta che il dominio del carico di lavoro è attivo e funzionante, è possibile creare datastore aggiuntivi utilizzando gli strumenti ONTAP che attiveranno l'espansione del gruppo di coerenza.



Se un cluster vSphere è protetto, saranno protetti tutti i datastore nel cluster.

Informazioni aggiuntive

Per informazioni sulla configurazione dei sistemi di archiviazione ONTAP fare riferimento a "["Documentazione ONTAP 9"](#) centro.

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

Demo video per questa soluzione

[Cluster di allungamento per VCF con strumenti ONTAP](#)

Migrazione delle VM da VMware vSphere ai datastore ONTAP

Gli ambienti VMware vSphere possono trarre notevoli vantaggi dalla migrazione delle macchine virtuali verso datastore supportati NetApp ONTAP. Che tu stia passando da vSAN a sistemi di archiviazione di terze parti o aggiornando la tua infrastruttura esistente, esplora vari scenari vMotion e strategie di migrazione per trasferire senza problemi le tue VM ai datastore ONTAP. Ciò garantisce la continuità aziendale sfruttando al contempo le funzionalità di archiviazione di classe enterprise di ONTAP.

VMware vSphere di Broadcom supporta i datastore VMFS, NFS e vVol per l'hosting di macchine virtuali. I clienti hanno la possibilità di creare tali datastore con infrastrutture iperconvergenti o con sistemi di storage condivisi centralizzati.

I clienti spesso riscontrano il valore dell'hosting su sistemi di storage basati su ONTAP per fornire snapshot e cloni di macchine virtuali efficienti in termini di spazio, flessibilità nella scelta di vari modelli di distribuzione nei data center e nei cloud, efficienza operativa con strumenti di monitoraggio e avviso, sicurezza, governance e strumenti di conformità opzionali per ispezionare i dati delle macchine virtuali e così via.

Le VM ospitate su datastore ONTAP possono essere protette utilizzando il plug-in SnapCenter per VMware vSphere (SCV). SCV crea snapshot basati sull'archiviazione e li replica anche sul sistema di archiviazione ONTAP remoto. I ripristini possono essere eseguiti sia dai sistemi di archiviazione primari che da quelli secondari.

I clienti hanno la flessibilità di scegliere Cloud Insights o Aria Operations o una combinazione di entrambi o altri strumenti di terze parti che utilizzano l'API ONTAP per la risoluzione dei problemi, il monitoraggio delle prestazioni, la creazione di report e le funzionalità di notifica degli avvisi.

I clienti possono facilmente effettuare il provisioning del datastore utilizzando il plug-in vCenter ONTAP Tools o la sua API e le VM possono essere migrate nei datastore ONTAP anche mentre sono accesi.

 Alcune VM distribuite con strumenti di gestione esterni come VCF Automation, vSphere Supervisor (o altre versioni di Kubernetes) dipendono solitamente dalla policy di archiviazione della VM. Se si esegue la migrazione tra gli archivi dati all'interno della stessa policy di archiviazione della VM, l'impatto sulle applicazioni dovrebbe essere minore. Verificare con i proprietari dell'applicazione la corretta migrazione di tali VM al nuovo datastore. Introduzione di vSphere 8 "["Notifiche vSphere vMotion per applicazioni sensibili alla latenza"](#) per preparare le applicazioni per vMotion.

Requisiti di rete

Migrazione di VM con vMotion

Si presume che sia già presente una rete di archiviazione doppia per il datastore ONTAP , per garantire connettività, tolleranza agli errori e aumento delle prestazioni.

Anche la migrazione delle VM tra gli host vSphere viene gestita dall'interfaccia VMKernel dell'host vSphere. Per la migrazione a caldo (VM accese), viene utilizzata l'interfaccia VMKernel con il servizio vMotion abilitato, mentre per la migrazione a freddo (VM spente), viene utilizzata l'interfaccia VMKernel con il servizio Provisioning abilitato per spostare i dati. Se non viene trovata alcuna interfaccia valida, verrà utilizzata l'interfaccia di gestione per spostare i dati, il che potrebbe non essere auspicabile per determinati casi d'uso.

Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion
vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

Quando si modifica l'interfaccia VMKernel, ecco l'opzione per abilitare i servizi richiesti.

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



Assicurarsi che siano disponibili almeno due schede di rete uplink attive ad alta velocità per il portgroup utilizzato dalle interfacce vMotion e Provisioning VMkernel.

Scenari di migrazione delle VM

vMotion viene spesso utilizzato per migrare le VM indipendentemente dal loro stato di alimentazione. Di seguito sono disponibili ulteriori considerazioni e procedure di migrazione per scenari specifici.



Capire "[Condizioni e limitazioni della VM di vSphere vMotion](#)" prima di procedere con qualsiasi opzione di migrazione della VM.

Migrazione di VM da uno specifico vSphere Datastore

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

1. Con vSphere Web Client, seleziona il Datastore dall'inventario di storage e fai clic sulla scheda VMs.

The screenshot shows the vSphere Client interface. At the top, there's a search bar labeled 'Search in all environments'. Below it, the inventory tree shows 'vcsa-hc.sddc.netapp.com' and 'Datacenter'. The 'vsanDatastore' is selected. In the top navigation bar, the 'VMs' tab is highlighted. The main area displays a list of virtual machines: 'gke-admin-ws-1-28-repeat', 'gke-admin-ws-asv', 'hammerdb-01', 'hammerdb-02', 'hammerdb-03', and 'hammerdb-04'. The 'hammerdb' series are selected, indicated by a checked checkbox icon.

2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

This screenshot shows the 'Actions - 4 Objects' context menu for the selected VMs. The menu includes options like Power, Guest OS, Snapshots, and Migrate... (which is highlighted with a blue box). Other visible options include VM Policies and Template. To the right of the menu, a table lists the selected VMs with their names and sizes: 'hammerdb-01' (16.31 GB), 'hammerdb-02' (15.55 GB), 'hammerdb-03' (15.44 GB), and 'hammerdb-04' (18.41 GB).

VM Name	Size
hammerdb-01	16.31 GB
hammerdb-02	15.55 GB
hammerdb-03	15.44 GB
hammerdb-04	18.41 GB

3. Scegli l'opzione per modificare solo l'archiviazione, fai clic su Avanti

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only
Migrate the virtual machines to another host or cluster.

Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL **NEXT**

4. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.

4 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: Thin Provision

VM Storage Policy: NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB
DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB
destination	Incompatible	250 GB	31.8 MB	249.97 GB
DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB
E13A400_ISCSI	Incompatible	2 TB	858.66 GB	1.85 TB

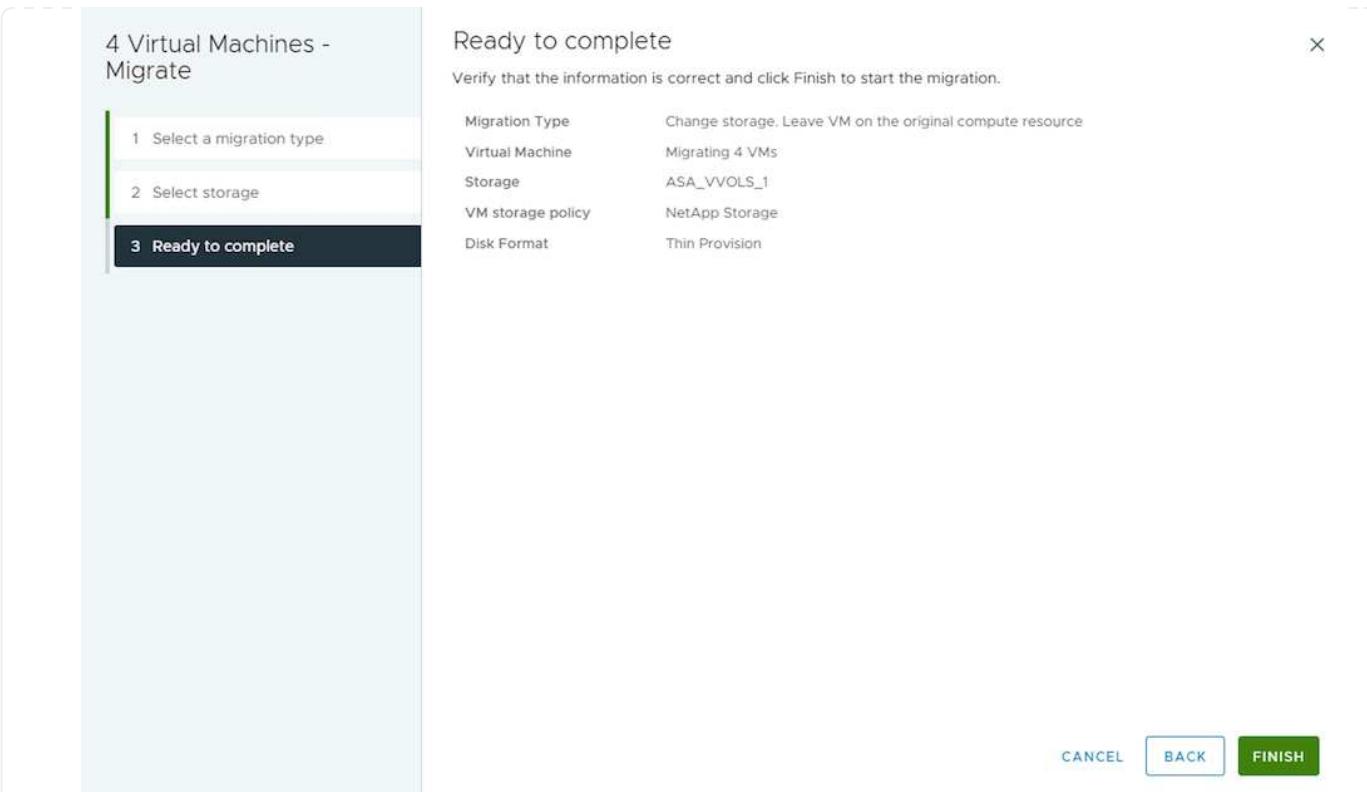
Manage Columns Items per page: 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

5. Rivedi e clicca su Fine.



Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

Migrazione di VM nello stesso cluster vSphere

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VMs.

The screenshot shows the vSphere Client interface. At the top, there's a search bar and tabs for Summary, Monitor, Configure, Permissions, Hosts, VMs (which is highlighted), Datastores, Networks, and Updates. Below the tabs, there's a navigation tree with nodes like vcf-m01-vc01.sddc.netapp.com, vcf-m01-dc01, and vcf-m01-cl01. Under vcf-m01-cl01, several VMs are listed: gke-admin-ws-1-28-repeat, gke-admin-ws-asv, hammerdb-01, hammerdb-02, hammerdb-03, and hammerdb-04. The hammerdb-01, hammerdb-02, hammerdb-03, and hammerdb-04 VMs have checkboxes checked next to them.

2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

This screenshot shows the Actions menu for four selected VMs: hammerdb-01, hammerdb-02, hammerdb-03, and hammerdb-04. The menu includes options like Power, Guest OS, Snapshots, Migrate..., VM Policies, and Template. The 'Migrate...' option is highlighted with a blue box.

VM Name	Size
gke-admin-ws-1-28-repeat	32.78 GB
gke-admin-ws-asv	46.51 GB
hammerdb-01	16.31 GB
hammerdb-02	15.55 GB
hammerdb-03	15.44 GB
hammerdb-04	18.41 GB

3. Scegli l'opzione per modificare solo l'archiviazione, fai clic su Avanti

This screenshot shows the 'Select a migration type' step of the migration wizard. On the left, a sidebar lists steps: 1. Select a migration type (which is highlighted in dark blue), 2. Select storage, and 3. Ready to complete. The main area shows a title 'Select a migration type' and a sub-instruction 'Change the virtual machines' compute resource, storage, or both.' Below this are four radio button options:

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

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

4. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format: Thin Provision
VM Storage Policy: NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB
DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB
destination	Incompatible	250 GB	31.8 MB	249.97 GB
DRAaSTest	Incompatible	1 TB	201.13 GB	880.86 GB
E13A400_JSCSI	Incompatible	2 TB	858.66 GB	1.85 TB

Manage Columns Items per page: 5 1 - 5 of 14 items | 1 / 3 > >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

5. Rivedi e clicca su Fine.

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL **BACK** **FINISH**

Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-c101' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```



Quando Datastore Cluster è in uso con DRS (Dynamic Resource Scheduling) di archiviazione completamente automatizzato ed entrambi i datastore (di origine e di destinazione) sono dello stesso tipo (VMFS/NFS/vVol), mantenere entrambi i datastore nello stesso cluster di archiviazione ed eseguire la migrazione delle VM dal datastore di origine abilitando la modalità di manutenzione sull'origine. L'esperienza sarà simile a quella che si ha quando si gestiscono gli host di elaborazione per la manutenzione.

Migrazione di VM su più cluster vSphere



Fare riferimento "Compatibilità CPU e compatibilità vSphere Enhanced vMotion" quando gli host di origine e di destinazione appartengono a famiglie o modelli di CPU diversi.

Per migrare le VM al nuovo Datastore tramite l'interfaccia utente, seguire la procedura seguente.

1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VMs.

The screenshot shows the vSphere Web Client interface. At the top, there's a navigation bar with tabs for Summary, Monitor, Configure, Permissions, Hosts, VMs (which is currently selected), Datastores, Networks, and Updates. Below the navigation bar is a search bar labeled 'Search in all environments'. The main content area displays a tree view of hosts and clusters. Under 'vcf-m01', there are two clusters: 'vcf-m01-dc01' and 'vcf-m01-cl01'. Under 'vcf-m01-cl01', there are several virtual machines listed. A quick filter bar is at the bottom of the main area.

2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

The screenshot shows the 'Actions - 4 Objects' menu for four selected virtual machines: 'hammerdb-01', 'hammerdb-02', 'hammerdb-03', and 'hammerdb-04'. The menu includes options for Power, Guest OS, Snapshots, Migrate..., VM Policies, and Template. The 'Migrate...' option is highlighted with a blue box. To the right of the menu, resource usage statistics are displayed for each VM: '32.78 GE', '46.51 GB', '16.31 GB', '15.55 GB', '15.44 GB', and '18.41 GB'.

3. Scegli l'opzione per modificare le risorse di elaborazione e di archiviazione, fai clic su Avanti

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Esplora e seleziona il cluster giusto da migrare.

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ✓ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ✓ vcf-wkld-vc01.sddc.netapp.com
 - > vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

Name	Storage Compatibility	Capacity	Provisioned	Free
VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB
vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns

Items per page: 10 7 items

Compatibility:

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. Selezionare la cartella VM in cui posizionare le VM di destinazione.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
- Discovered virtual machine
- vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. Selezionare il gruppo di porte di destinazione.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Rivedi e clicca su Fine.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage, Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-c101' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

Migrazione di VM tra server vCenter nello stesso dominio SSO

Per migrare le VM sul nuovo server vCenter elencato nella stessa interfaccia utente di vSphere Client, seguire la procedura seguente.



Per requisiti aggiuntivi come le versioni di vCenter di origine e di destinazione, ecc., controllare ["Documentazione vSphere sui requisiti per vMotion tra le istanze del server vCenter"](#)

1. Con vSphere Web Client, seleziona il cluster dall'inventario host e cluster e fai clic sulla scheda VM.

The screenshot shows the vSphere Client interface. At the top, there's a navigation bar with 'vSphere Client' and a search bar. Below it, a sidebar lists inventories: 'vcf-m01-vc01.sddc.netapp.com' (expanded) and 'vcf-m01-dc01' (expanded). Under 'vcf-m01-dc01', 'vcf-m01-cl01' is selected. The main content area has tabs: Summary, Monitor, Configure, Permissions, Hosts, VMs (which is underlined), Datastores, Networks, and Updates. The 'VMs' tab is active, showing a list of VMs: 'gke-admin-ws-1-28-repeat', 'gke-admin-ws-asv', 'hammerdb-01', 'hammerdb-02', 'hammerdb-03', and 'hammerdb-04'. A 'Quick Filter' input field is at the bottom.

2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migra.

This screenshot shows the same vSphere Client interface as the previous one, but with a context menu open over the selected VMs ('hammerdb-01', 'hammerdb-02', 'hammerdb-03', and 'hammerdb-04'). The menu is titled 'Actions - 4 Objects' and includes options: Power, Guest OS, Snapshots, Migrate..., VM Policies, and Template. The 'Migrate...' option is highlighted with a blue rounded rectangle.

VM	Size
gke-admin-ws-1-28-repeat	32.78 GE
gke-admin-ws-asv	46.51 GB
hammerdb-01	16.31 GB
hammerdb-02	15.55 GB
hammerdb-03	15.44 GB
hammerdb-04	18.41 GB

3. Scegli l'opzione per modificare le risorse di elaborazione e di archiviazione, fai clic su Avanti

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Selezionare il cluster di destinazione nel server vCenter di destinazione.

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a compute resource
- 3 Select storage
- 4 Select networks
- 5 Select vMotion priority
- 6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ✓ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ✓ vcf-wkld-vc01.sddc.netapp.com
 - > vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

- ✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Selezionare la policy di archiviazione della VM desiderata e scegliere il datastore compatibile. Fare clic su Avanti.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

Name	Storage Compatibility	Capacity	Provisioned	Free
VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB
VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB
vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Manage Columns

Items per page: 10 7 items

Compatibility:

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. Selezionare la cartella VM in cui posizionare le VM di destinazione.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select folder

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
- Discovered virtual machine
- vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. Selezionare il gruppo di porte di destinazione.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Esaminare le opzioni di migrazione e fare clic su Fine.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage, Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

Migrazione di VM tra server vCenter in diversi domini SSO



Questo scenario presuppone che la comunicazione esista tra i server vCenter. In caso contrario, controllare lo scenario di ubicazione dei data center elencato di seguito. Per i prerequisiti, controllare "Documentazione vSphere su Advanced Cross vCenter vMotion"

Per migrare le VM su diversi server vCenter tramite l'interfaccia utente, seguire la procedura seguente.

1. Con vSphere Web Client, seleziona il server vCenter di origine e fai clic sulla scheda VM.

The screenshot shows the vSphere Client interface with the title bar 'vSphere Client' and a search bar 'Search in all environments'. The URL 'vcsa-hc.sddc.netapp.com' is visible. The navigation bar includes 'Summary', 'Monitor', 'Configure', 'Permissions', 'Datacenters', 'Hosts & Clusters', 'VMs' (which is highlighted in blue), 'Datastores', 'Networks', 'Linked vCenter Server Systems', 'Extensions', and 'Updates'. Below the navigation bar, there's a tree view under 'vcsa-hc.sddc.netapp.com' showing 'Datacenter' and 'HMC Cluster'. The main content area is titled 'Virtual Machines' with tabs for 'Virtual Machines', 'VM Templates', and 'vApps'. A 'Quick Filter' and 'Enter value' field are at the bottom of this section.

2. Selezionare le VM da migrare e fare clic con il pulsante destro del mouse per selezionare l'opzione Migrata.

The screenshot shows the vSphere Client interface with the 'VMs' tab selected. On the left, a list of VMs is shown with checkboxes next to them. The VMs listed are 'gke-admin-ws-1-28-repeat', 'gke-admin-ws-asv', 'hammerdb-01' (selected), 'hammerdb-02' (selected), 'hammerdb-03' (selected), and 'hammerdb-04'. On the right, a context menu titled 'Actions - 4 Objects' is open, listing 'Power', 'Guest OS', 'Snapshots', 'Migrate...', 'VM Policies', and 'Template'. The 'Migrate...' option is highlighted with a blue rounded rectangle.

VM Name	Size
gke-admin-ws-1-28-repeat	32.78 GB
gke-admin-ws-asv	46.51 GB
hammerdb-01	16.31 GB
hammerdb-02	15.55 GB
hammerdb-03	15.44 GB
hammerdb-04	18.41 GB

3. Scegli l'opzione Esportazione tra server vCenter, fai clic su Avanti

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 - Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL NEXT



La VM può anche essere importata dal server vCenter di destinazione. Per tale procedura, controllare "[Importa o clona una macchina virtuale con Advanced Cross vCenter vMotion](#)"

4. Fornire i dettagli delle credenziali vCenter e fare clic su Accedi.

Migrate | SQLSRV-05

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS **NEW VCENTER SERVER**

vCenter Server address: vcf-wkld-vc01.sddc.netapp.com
vCenter Server FQDN or IP address.

Username: administrator@vcf.local
example@domain.local

Password:

Save vCenter Server address

LOGIN

CANCEL BACK NEXT

5. Conferma e accetta l'impronta digitale del certificato SSL del server vCenter

Security Alert



Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:



17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

Connect anyway?

Click Yes if you trust the vCenter Server.

Click No to cancel connecting to the vCenter Server.

NO

YES

6. Espandi il vCenter di destinazione e seleziona il cluster di elaborazione di destinazione.

Migrate | SQLSRV-05

- Select a migration type
- Select a target vCenter Server
- Select a compute resource**
- Select storage
- Select networks
- Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

VM ORIGIN ⓘ

- vcf-wkld-vc01.sddc.netapp.com
 - vcf-wkld-01-DC
 - IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. Selezionare il datastore di destinazione in base ai criteri di archiviazione della VM.

Migrate | SQLSRV-05

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format: Thin Provision

VM Storage Policy: NFS

Name	Storage Compatibility	Capacity	Provisioned	Free	Total
VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB	
VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB	
VCF_WKLD_03_ISCSI	Incompatible	3 TB	1.35 TB	2.59 TB	
vcf-wkld-esx01-esx5x-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
vcf-wkld-esx02-esx5x-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Selezionare la cartella della macchina virtuale di destinazione.

Migrate | SQLSRV-05

Select folder

Select the destination virtual machine folder for the virtual machine migration.

VM ORIGIN

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine
 - Oracle
 - SQL Server**
 - vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

9. Selezionare il portgroup VM per ogni mappatura della scheda di interfaccia di rete.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks**
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» Mgmt_181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
» Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
» Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

3 items

ADVANCED >

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

10. Rivedere e fare clic su Fine per avviare vMotion sul server vCenter.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

VM ORIGIN ⓘ

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

CANCEL BACK FINISH

Per migrare le VM tramite PowerCLI, ecco lo script di esempio.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

Migrazione di VM tra le sedi dei data center

- Quando il traffico di Livello 2 viene distribuito su più data center tramite NSX Federation o altre opzioni, seguire la procedura per la migrazione delle VM su più server vCenter.
- HCX fornisce vari "tipi di migrazione" inclusa la Replication Assisted vMotion nei data center per spostare le VM senza tempi di inattività.
- "Site Recovery Manager (SRM)" è in genere destinato a scopi di Disaster Recovery e spesso utilizzato anche per la migrazione pianificata mediante replica basata su array di archiviazione.
- I prodotti di protezione continua dei dati (CDP) utilizzano "API vSphere per IO (VAIO)" per intercettare i dati e inviarne una copia a una posizione remota per una soluzione RPO prossima allo zero.
- È possibile utilizzare anche prodotti di backup e ripristino. Ma spesso si traduce in un RTO più lungo.
- "Ripristino di emergenza NetApp" utilizza la replica basata su array di archiviazione e automatizza determinate attività per ripristinare le VM nel sito di destinazione.

Migrazione di VM in ambiente cloud ibrido

- "Configura la modalità ibrida collegata" e seguire la procedura di "[Migrazione di VM tra server vCenter nello stesso dominio SSO](#)"
- HCX fornisce vari "tipi di migrazione" incluso Replication Assisted vMotion nei data center per spostare la VM mentre è accesa.
 - "TR 4942: Migrazione dei carichi di lavoro al datastore FSx ONTAP utilizzando VMware HCX"
 - "TR-4940: Migrazione dei carichi di lavoro al datastore di Azure NetApp Files tramite VMware HCX - Guida introduttiva"
 - "Migrazione dei carichi di lavoro al datastore Google Cloud NetApp Volumes su Google Cloud VMware Engine utilizzando VMware HCX - Guida introduttiva"
- "[NetApp Disaster Recovery](#)" utilizza la replica basata su array di archiviazione e automatizza determinate attività per ripristinare le VM nel sito di destinazione.
- Con prodotti CDP (Continous Data Protection) supportati che utilizzano "[API vSphere per IO \(VAIO\)](#)" per intercettare i dati e inviarne una copia a una posizione remota per una soluzione RPO prossima allo zero.



Quando la VM di origine risiede sul datastore vVol a blocchi, può essere replicata con SnapMirror su Amazon FSx ONTAP o Cloud Volumes ONTAP (CVO) presso altri provider cloud supportati e utilizzata come volume iSCSI con VM cloud native.

Scenari di migrazione dei modelli di VM

I modelli di VM possono essere gestiti da vCenter Server o da una libreria di contenuti. La distribuzione di modelli VM, modelli OVF e OVA e altri tipi di file viene gestita pubblicandoli nella libreria di contenuti locale e le librerie di contenuti remote possono sottoscriverli.

- I modelli di VM archiviati nell'inventario vCenter possono essere convertiti in VM e utilizzare le opzioni di migrazione VM.
- I modelli OVF e OVA e altri tipi di file memorizzati nella libreria di contenuti possono essere clonati in altre librerie di contenuti.
- I modelli VM della libreria di contenuti possono essere ospitati su qualsiasi datastore e devono essere aggiunti alla nuova libreria di contenuti.

Migrazione dei modelli di VM ospitati sul datastore

1. In vSphere Web Client, fare clic con il pulsante destro del mouse sul modello VM nella vista cartelle VM e modelli e selezionare l'opzione per convertire in VM.

The screenshot shows the vSphere Web Client interface. On the left, there's a navigation sidebar with categories like Oracle, RTP, SQL Server, Tanzu, and Templates. Under Templates, several items are listed: ESXi-8.0-U1a, vdbench template, win10-template (which is selected and highlighted in black), win2019 template, and win2022-template. The main content area displays 'VM Template Details' for 'win10-template'. It shows the Guest OS as Microsoft Windows, VMware Tools status as 'Not running, version:123', DNS Name as DESKTOP-HGNBVPL, and IP Addresses and Encryption details. Below this, a context menu is open with options: New VM from This Template..., Convert to Virtual Machine... (which is highlighted with a blue oval), Clone to Template..., Clone to Library..., Move to folder..., Rename..., Edit Notes..., Tags & Custom Attributes, Add Permission..., Alarms, Remove from Inventory, Delete from Disk, vSAN, and NetApp ONTAP tools. A notes section on the right says 'No note'.

2. Una volta convertito in VM, seguire le opzioni di migrazione della VM.

Clonazione degli elementi della libreria dei contenuti

1. In vSphere Web Client, seleziona Librerie di contenuti



vSphere Client



Search in all en



Home



Content Libraries



2. Seleziona la libreria di contenuti in cui si trova l'elemento che desideri clonare
3. Fare clic con il tasto destro del mouse sull'elemento e fare clic su Clona elemento.

The screenshot shows the vSphere Client interface with the 'CL01' library selected. A context menu is open over a specific item, and the 'Clone item...' option is highlighted with a blue oval. The menu also includes other options like 'Update item...', 'Export item...', 'Edit Notes...', 'Rename...', 'Tags', and 'Delete'.



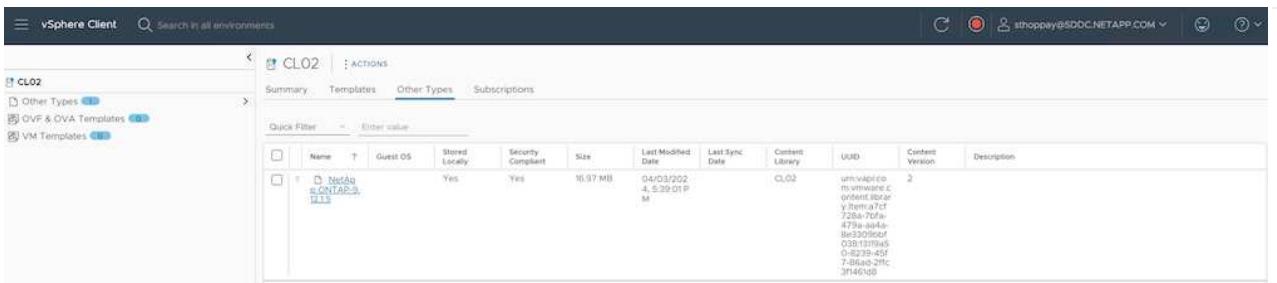
Se si utilizza il menu Azione, assicurarsi che sia elencato l'oggetto di destinazione corretto per eseguire l'azione.

4. Selezionare la libreria di contenuti di destinazione e fare clic su OK.

Clone Library Item | NetApp ONTAP-9.12.1.5
X

Name	NetApp ONTAP-9.12.1.5									
Notes	<input type="text"/>									
Select a content library where to clone the library item.										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Name</th> <th>Notes</th> <th>Creation Date</th> </tr> </thead> <tbody> <tr> <td>CL01</td> <td></td> <td>9/26/2023, 5:02:03 PM</td> </tr> <tr style="background-color: #0070C0; color: white;"> <td>CL02</td> <td></td> <td>4/1/2024, 12:37:51 PM</td> </tr> </tbody> </table>		Name	Notes	Creation Date	CL01		9/26/2023, 5:02:03 PM	CL02		4/1/2024, 12:37:51 PM
Name	Notes	Creation Date								
CL01		9/26/2023, 5:02:03 PM								
CL02		4/1/2024, 12:37:51 PM								
<input type="button" value="CANCEL"/> <input type="button" value="OK"/>										

5. Verificare che l'elemento sia disponibile nella libreria di contenuti di destinazione.



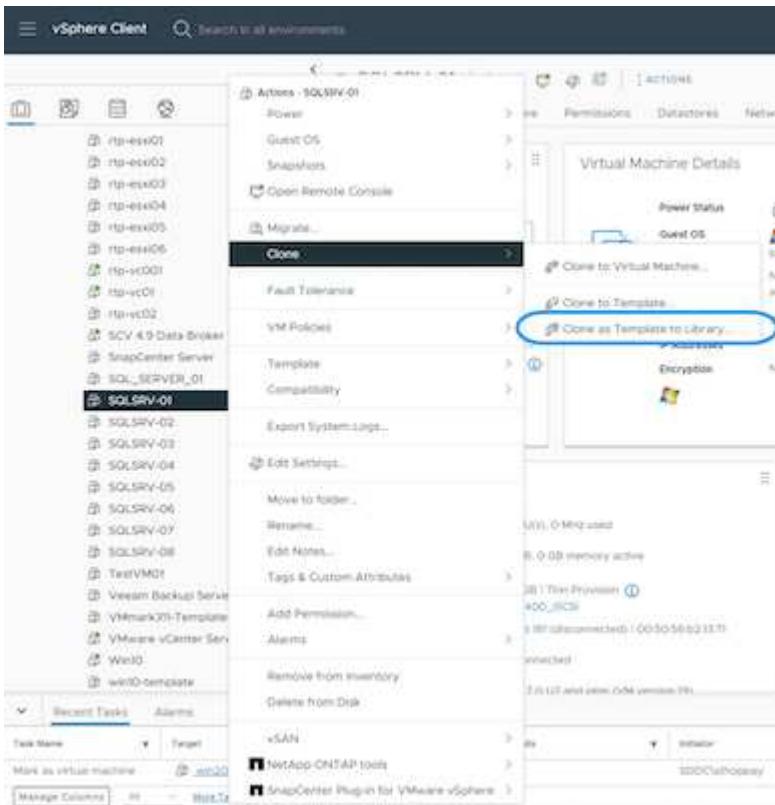
Ecco un esempio di script PowerCLI per copiare gli elementi della libreria di contenuti dalla libreria di contenuti CL01 a CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

Aggiunta di VM come modelli nella libreria dei contenuti

1. In vSphere Web Client, seleziona la VM e fai clic con il pulsante destro del mouse per scegliere Clona come modello nella libreria



Quando si seleziona il modello VM per la clonazione nella libreria, è possibile memorizzarlo solo come modello OVF e OVA e non come modello VM.

2. Verificare che il tipo di modello selezionato sia Modello VM e seguire le istruzioni della procedura guidata per completare l'operazione.

SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information

2 Location
3 Select a compute resource
4 Select storage
5 Ready to complete

Basic information

Template type **VM Template**

Name: SQLSRV-01

Notes:

Select a folder for the template

vcsa-hc.sddc.netapp.com
Datacenter

CANCEL **NEXT**



Per ulteriori dettagli sui modelli VM nella libreria di contenuti, controllare "[Guida all'amministrazione della VM vSphere](#)"

Casi d'uso

Migrazione da sistemi di archiviazione di terze parti (incluso vSAN) a datastore ONTAP .

- In base a dove è predisposto il datastore ONTAP , seleziona le opzioni di migrazione della VM sopra indicate.

Migrazione dalla versione precedente alla versione più recente di vSphere.

- Se l'aggiornamento sul posto non è possibile, è possibile creare un nuovo ambiente e utilizzare le opzioni di migrazione sopra indicate.



Nell'opzione di migrazione tra vCenter, importa dalla destinazione se l'opzione di esportazione non è disponibile sulla sorgente. Per tale procedura, controllare "[Importa o clona una macchina virtuale con Advanced Cross vCenter vMotion](#)"

Migrazione al dominio del carico di lavoro VCF.

- Migrare le VM da ciascun cluster vSphere al dominio del carico di lavoro di destinazione.



Per consentire la comunicazione di rete con le VM esistenti su altri cluster sul vCenter di origine, estendere il segmento NSX aggiungendo gli host vCenter vSphere di origine alla zona di trasporto oppure utilizzare il bridge L2 sull'edge per consentire la comunicazione L2 nella VLAN. Controllare la documentazione NSX di "["Configurare una VM Edge per il bridging"](#)

Risorse aggiuntive

- ["Migrazione della macchina virtuale vSphere"](#)
- ["Migrazione di macchine virtuali con vSphere vMotion"](#)
- ["Configurazioni del gateway di livello 0 nella federazione NSX"](#)
- ["Guida utente HCX 4.8"](#)
- ["Documentazione di VMware Live Recovery"](#)
- ["NetApp Disaster Recovery per VMware"](#)

Protezione autonoma contro i ransomware per l'archiviazione NFS

Rilevare il ransomware il prima possibile è fondamentale per prevenirne la diffusione ed evitare costosi tempi di inattività. Una strategia efficace per il rilevamento dei ransomware deve integrare più livelli di protezione a livello di host ESXi e di VM guest. Sebbene vengano implementate molteplici misure di sicurezza per creare una difesa completa contro gli attacchi ransomware, ONTAP consente di aggiungere ulteriori livelli di protezione all'approccio di difesa complessivo. Per citarne alcune, si inizia con gli snapshot, la protezione autonoma dai ransomware, gli snapshot a prova di manomissione e così via.

Diamo un'occhiata a come le funzionalità sopra menzionate interagiscono con VMware per proteggere e recuperare i dati dal ransomware. Per proteggere vSphere e le VM guest dagli attacchi, è essenziale adottare diverse misure, tra cui la segmentazione, l'utilizzo di EDR/XDR/SIEM per gli endpoint, l'installazione di aggiornamenti di sicurezza e il rispetto delle linee guida di rafforzamento appropriate. Ogni macchina virtuale residente su un datastore ospita anche un sistema operativo standard. Assicurarsi che le suite di prodotti antimalware sui server aziendali siano installate e aggiornate regolarmente, il che rappresenta un componente essenziale della strategia di protezione anti-ransomware multilivello. Oltre a ciò, abilitare la protezione autonoma contro i ransomware (ARP) sul volume NFS che alimenta il datastore. ARP sfrutta l'apprendimento automatico integrato che analizza l'attività del carico di lavoro e l'entropia dei dati per rilevare automaticamente il ransomware. ARP è configurabile tramite l'interfaccia di gestione integrata ONTAP o il System Manager ed è abilitato in base al volume.

The screenshot shows the ONTAP System Manager interface. On the left, a sidebar lists categories like DASHBOARD, INSIGHTS, STORAGE, NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER. Under STORAGE, 'Volumes' is selected. The main area displays a table of volumes with columns for Name and Status. One row is highlighted for 'Src_NFS_Vol01'. To the right of the table, there's a detailed view for 'Src_NFS_Vol01' with tabs for Overview, Snapshot copies, SnapMirror, Back up to cloud, Security (which is selected), File system, and Quota Reports. Below the tabs, there's a section titled 'Anti-ransomware' with a status switch labeled 'Disabled'. A tooltip says: 'Enable anti-ransomware if you're running applications on this NFS volume.' At the bottom right of the main area, there's a link to 'Activate Windows'.

i Con il nuovo NetApp ARP/AI, attualmente in anteprima tecnologica, non è necessaria una modalità di apprendimento. Può invece passare direttamente alla modalità attiva grazie alla sua capacità di rilevamento ransomware basata sull'intelligenza artificiale.

i Con ONTAP One, tutte queste funzionalità sono completamente gratuite. Accedi alla solida suite di protezione dei dati e sicurezza di NetApp e a tutte le funzionalità offerte da ONTAP senza preoccuparti degli ostacoli legati alle licenze.

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

The screenshot shows the ONTAP System Manager interface. In the left sidebar, under the 'STORAGE' category, there is a list of volumes: Src_NFS_DS01, NFSARPDemo02, NFSDS02ARP, nimpra, SQLDatavol, Src_25G_Vol01, Src_iSCSI_D005, Src_iSCSI_D0502, Src_iSCSI_D0504, Src_iSCSI_D0506, Src_NFS_D002, Src_NFS_D003, and Src_NFS_DS04. The 'Src_NFS_DS04' volume is selected. In the main content area, the 'Volumes' tab is selected. The 'Security' tab is highlighted with a red box. Under the 'Anti-ransomware' section, there is a toggle switch labeled 'Enabled in active mode' which is turned on, also highlighted with a red box.

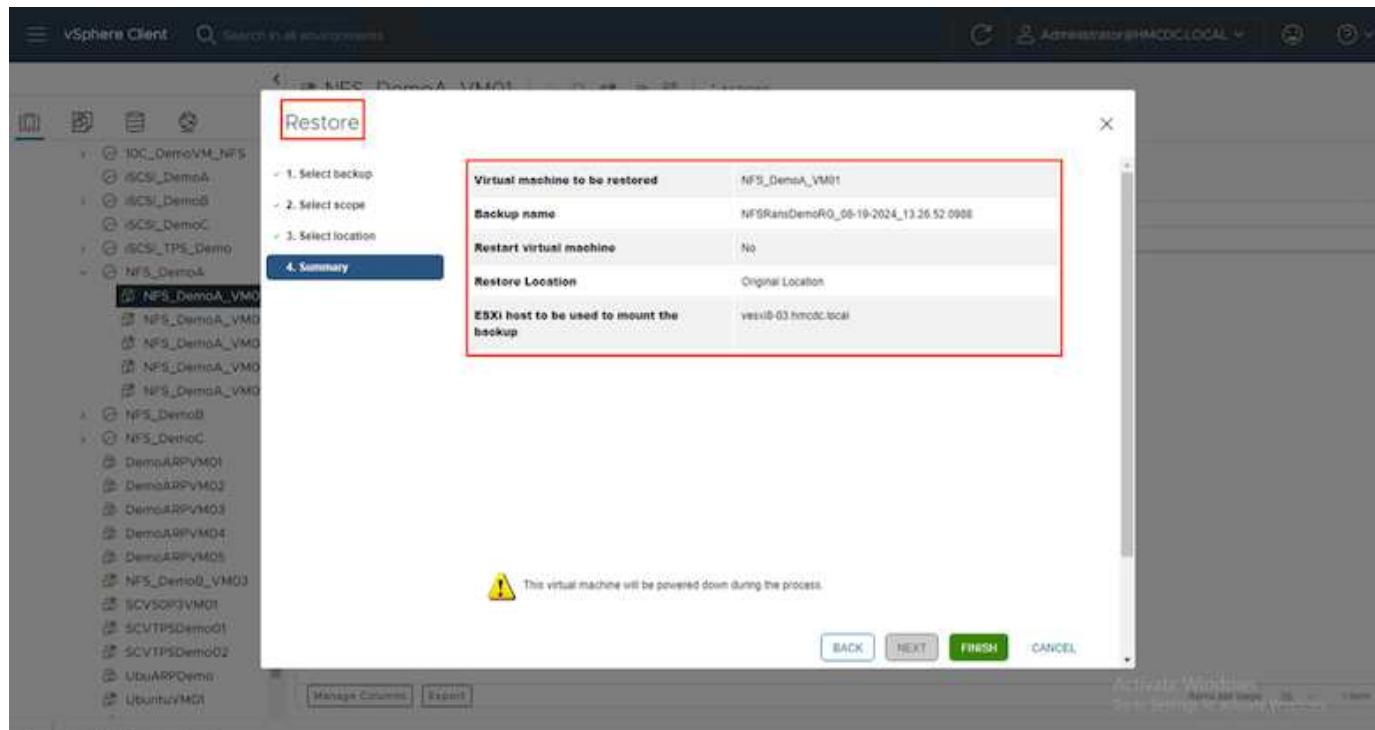
Se un attacco ransomware prende di mira la macchina virtuale (VM) e modifica i file al suo interno senza apportare modifiche all'esterno, Advanced Ransomware Protection (ARP) rileverà comunque la minaccia se l'entropia predefinita della VM è bassa, ad esempio per tipi di file come .txt, .docx o .mp4.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

Per informazioni dettagliate, fare riferimento alla sezione "ARP e macchine virtuali" in "[Casi d'uso e considerazioni ARP](#)" .

Passando dai file ai dati di backup, gli attacchi ransomware prendono sempre più di mira i backup e i punti di ripristino degli snapshot, cercando di eliminarli prima di iniziare a crittografare i file. Tuttavia, con ONTAP, questo può essere prevenuto creando snapshot a prova di manomissione sui sistemi primari o secondari con "[Blocco della copia snapshot NetApp](#)" .

The screenshot shows the vSphere Client interface. On the left, there is a sidebar with options like Dashboard, Settings, Resource Groups, Policies, Storage Systems, and Guest File Restore. The 'Policies' option is selected. In the main area, there is a table of policies, and a specific policy named 'Pol_NFSDS04' is selected. A modal dialog box titled 'Edit - Pol_NFSDS04' is open. Inside the dialog, under the 'Locking Period' section, there is a checkbox labeled 'Enable Snapshot Locking' which is checked. This checkbox is highlighted with a red box. Below it, there is a dropdown menu for 'Days to keep' and a dropdown menu for 'Days'.

Queste copie Snapshot non possono essere eliminate o modificate da aggressori ransomware o amministratori non autorizzati, quindi sono disponibili anche dopo un attacco. Se il datastore o specifiche macchine virtuali sono interessati, SnapCenter è in grado di recuperare i dati delle macchine virtuali in pochi secondi, riducendo al minimo i tempi di inattività dell'organizzazione.



Quanto sopra dimostra come l'archiviazione ONTAP aggiunga un ulteriore livello alle tecniche esistenti, migliorando la protezione futura dell'ambiente.

Per ulteriori informazioni, consultare la guida per "[Soluzioni NetApp per il ransomware](#)".

Ora, se tutto questo deve essere orchestrato e integrato con strumenti SIEM, è possibile utilizzare un servizio offtap come NetApp Ransomware Resilience. Si tratta di un servizio progettato per proteggere i dati dal ransomware. Questo servizio offre protezione per carichi di lavoro basati su applicazioni quali Oracle, MySQL, datastore VM e condivisioni di file su storage NFS locali.

In questo esempio, il datastore NFS "Src_NFS_DS04" è protetto tramite NetApp Ransomware Resilience.



I passaggi descritti di seguito sono con BlueXP. Il flusso di lavoro è simile a quello della NetApp Console.

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_NFS_DS02	VM datastore	G1SABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	<button>Edit protection</button>
Drasa_src_test_3130	VM file share	G1SABXPConn	Standard	At risk	None	None	None	n/a	<button>Protect</button>
Nfsd02arp_804	VM file share	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	<button>Edit protection</button>
Drasa_src_7027	VM file share	G1SABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	<button>Protect</button>
Src_NFS_Vol01_7948	VM file share	G1SABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	<button>Protect</button>
Src_NFS_DS03	VM datastore	G1SABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	<button>Protect</button>
Src_NFS_DS04	VM datastore	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	<button>Edit protection</button>
Src_NFS_DS04	File share	G1SABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	<button>Edit protection</button>
Testvol_1787	File share	G1SABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	<button>Edit protection</button>
Nfsarpdemo02_1419	File share	G1SABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	<button>Edit protection</button>

Standard Importance	Protection	Storage
Protected Protection health Edit protection	0 Alerts	Not marked for recovery Recovery
Protection These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload. Pol_NFSDS04 Snapshot policy 1 Year Daily LTR Backup policy	VM datastore Location: urn:scv:scvmUI:Resou... vCenter server: vvcasb-01.hmcidc.local Connector: G1SABXPConn	Storage Cluster id: add38d26-348c-11ef-8... Working Env name: NTAP915_Src Storage VM name: svm_NFS Volume name: Src_NFS_DS04 Used size: 29 GiB

Per informazioni dettagliate sulla configurazione NetApp Ransomware Resilience, fare riferimento a "Imposta NetAp Ransomware Resilience" E "Configurare le impostazioni di NetAp Ransomware Resilience".

È il momento di analizzare la questione con un esempio. In questa procedura dettagliata, è interessato il datastore "Src_NFS_DS04".

VM Disk files under Ransomware Attack and VM affected

File browser interface showing a list of files and folders. The 'NFS_DemoB_VM01' folder is selected. The 'Manage Content' button is highlighted.

Name	Type	Size	Modified
SO_DemoVM1scoreBoard	File	8 KB	08/05/2024, 1:02:39 AM
SO_DMW/VM1scoreboard	File	8 KB	08/09/2024, 9:51:11 AM
NFS_DemoB_VM01.vmem	File	4,194,304 KB	07/31/2024, 5:59:48 AM
NFS_DemoB_VM01.vmdk	File	0.09 KB	08/05/2024, 1:02:39 AM
NFS_DemoB_VM01-29f5a031.vmdk	File	0.01 KB	08/05/2024, 1:02:39 AM
NFS_DemoB_VM01.vmx	Virtual Machine	3.4 KB	08/09/2024, 9:08:46 AM
NFS_DemoB_VM01.vmdk	File	0 KB	08/05/2024, 1:02:39 AM
NFS_DemoB_VM01.vmem	File	0.07 KB	08/09/2024, 9:31:22 AM
NFS_DemoB_VM01-3-1c9.vmdk	File	940.54 KB	08/09/2024, 9:31:22 AM
NFS_DemoB_VM01-3-f1a1.vmdk	File	10,485.36 KB	08/09/2024, 9:31:22 AM
NFS_DemoB_VM01-3.vmdk	File	0.64 KB	08/09/2024, 9:31:22 AM

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

NetApp Snapshot triggered during suspected abnormal activity

Name	Snapshot copy creation time	Snapshot restore size
snapmirror.e2ad5432-3537-11ef-bd57-00a0b0f6d346_21	Aug/9/2024 9:05 AM	50.5 GB
59491296_2024-08-09_160500		
Anti_ransomware_backup.2024-08-09_1326	Aug/9/2024 6:26 AM	44.5 GB
RG_NFSD504_08-09-2024_08.08.16.0981	Aug/9/2024 5:08 AM	27.8 GB
RG_NFSD504_08-09-2024_07.54.48.0205	Aug/9/2024 4:55 AM	27.7 GB
RG_NFSD504_08-09-2024_06.27.18.0190	Aug/9/2024 3:27 AM	27.6 GB
RG_NFSD504_08-09-2024_05.00.28.0747	Aug/9/2024 2:00 AM	27.7 GB

The screenshot shows the ONTAP System Manager interface. In the top right corner, a blue banner displays the message: "ARP detects abnormal activity on the Volume". The main area shows a section titled "Anti-ransomware" with a status indicator: "Enabled in active mode". It also displays a warning message: "Abnormal volume activity detected on 09 Aug 2024 5:53 AM". Below this, there is a list of "SUSPECTED RANSOMWARE FILES" with a count of "10 files". A button labeled "View suspected file type" is present. On the right side of the banner, there are buttons for "Pause anti-ransomware" and "Event severity settings". The left sidebar contains navigation links for DASHBOARD, INSIGHTS, STORAGE (Overview, Volumes, LUNs, NVMe namespaces, Consistency groups, Shares, Qtree, Quotas, Storage VMs, Tiers), NETWORK, EVENTS & JOBS, PROTECTION, HOSTS, and CLUSTER.

Una volta completata l'analisi forense, i ripristini possono essere eseguiti in modo rapido e senza problemi utilizzando SnapCenter o NetApp Ransomware Resilience. Con SnapCenter, accedi alle macchine virtuali interessate e seleziona lo snapshot appropriato da ripristinare.

The screenshot shows the vSphere Client interface. A blue banner at the top right says: "Select the VM to be restored within the backup". The main window displays a list of VMs under the heading "RESTORE". One specific VM, "NFS_DemoB_VM01", is highlighted in the list. The "Backup" tab is selected in the ribbon. The left sidebar shows a tree view of the vCenter inventory, including hosts, clusters, and datastores. At the bottom, there are buttons for "Recent Tasks" and "Activate Windows".

Entry Name	Quiescent	UUID	Location
NFS_DemoB_VM02	Yes	50121588-4E78-a11e-7211-77095866e0c7	[Src_NFS_D504] NFS_DemoB_VM02[NFS_DemoB_VM02.vmx]
NFS_DemoB_VM01	Yes	50125aa9-70cc-41be-82de-a480149359d5	[Src_NFS_D504] NFS_DemoB_VM01[NFS_DemoB_VM01.vmx]
NFS_DemoB_VM03	Yes	50126818-4F55-4465-787a-4a4434991020	[Src_NFS_D504] NFS_DemoB_VM03[NFS_DemoB_VM03.vmx]
NFS_DemoB_VM05	Yes	5012ab48-e254-b333-2d6d-00137a651f1f	[Src_NFS_D504] NFS_DemoB_VM05[NFS_DemoB_VM05.vmx]
NFS_DemoB_VM04	Yes	50125d7a-e4ec-a4c3-3253-2b2937a0f18	[Src_NFS_D504] NFS_DemoB_VM04[NFS_DemoB_VM04.vmx]
Src_NFS_D504	No	netfs://172.21.168.161/iscsi_NFS_D504	src_NFS_ivsSrc_NFS_D504

Questa sezione esamina il modo in cui NetApp Ransomware Resilience orchestra il ripristino da un incidente ransomware in cui i file della VM sono crittografati.



Se la VM è gestita da SnapCenter, NetApp Ransomware Resilience ripristina la VM allo stato precedente utilizzando il processo coerente con la VM.

1. Accedi a NetApp Ransomware Resilience e un avviso verrà visualizzato nella dashboard NetApp Ransomware Resilience .
2. Fare clic sull'avviso per rivedere gli incidenti su quel volume specifico per l'avviso generato

Protection View specific to the NFS Volume

Src_NFS_DS04

Protection		VM datastore	Storage
Standard Importance	Protected	Location: urn:scv:scvmUI:Resou... vCenter server: vvcalls-01.hmedc.local Connector: GISABXPConn	Cluster id: add38d26-348c-11ef-8... Working Env name: NTAP915_src Storage VM name: svm_NFS Volume name: Src_NFS_DS04 Used size: 29 GiB
PoI_NFS0504 Snapshot policy	1 Year Daily LTR Backup policy		

3. Contrassegna l'incidente ransomware come pronto per il ripristino (dopo che gli incidenti sono stati neutralizzati) selezionando "Contrassegna come ripristino necessario"

Mark the alert for "restore needed"

alert12198

Workload: Src_NFS_DS04 | Location: urn:scv:scvmUI:Resou... | Type: VM datastore | Connector: GISABXPConn

Mark restore needed

Incident ID	Volume	SVM	Working environment	Type	Status	First detected	Evidence	Automated responses
Inc12198	Src_NFS_DS04	svm_NFS	NTAP915_src	Potential attack	New	4 hours ago	1 new extensions detected	2 Snapshot copies



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

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

Workload	Location	Type	Connector	Snapshot and backup...	Recovery status	Progress	Importance	Total data	Action
Nfsds02arpj_004	10.61.187.61	VM file share	GSA8XPConn	n/a	Restore needed	n/a	Standard	228 GiB	<button>Restore</button>
Src_nfs_ds04	urn:scv:scvml:Resource:n...	VM datastore	GSA8XPConn	SnapCenter for VMware	Restore needed	n/a	Standard	29 GiB	<button>Restore</button>

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

Restore point	Type	Date
RG_NFS0504_08-09-2024_06:08:16.0981	snapshot	August 9, 2024, 1:08 PM
RG_NFS0504_08-09-2024_07:54:48.0206	snapshot	August 9, 2024, 12:54 PM
RG_NFS0504_08-09-2024_06:27:18.0190	snapshot	August 9, 2024, 11:27 AM
RG_NFS0504_08-09-2024_05:00:28.0747	snapshot	August 9, 2024, 10:00 AM

6. Selezionare il punto di ripristino da utilizzare per ripristinare i dati, selezionare Destinazione e fare clic su Ripristina.

The screenshot shows the 'Review' step of a restore operation for 'Src_NFS_DS04'. The table details the source VM (NFS_DemoB_VM02) and the destination environment (NTAP915_Src). The destination SVM is 'svm_NFS' and the destination VM is 'NFS_DemoB_VM02'. The 'Restore' button is highlighted.

- Dal menu in alto, seleziona Ripristino per esaminare il carico di lavoro nella pagina Ripristino, dove lo stato dell'operazione scorre tra gli stati. Una volta completato il ripristino, i file della VM vengono ripristinati come mostrato di seguito.

The screenshot shows the 'Verify the restored VM files' dialog in the vSphere Client. It lists restored files for 'NFS_DemoB_VM02' in the 'File' tab. The table includes columns for Name, Size, Modified, Type, and Age. The files listed are related to the restored VM, such as 'NFS_DemoB_VM02.vmdk', 'NFS_DemoB_VM02.vmsd', and various log files like 'vmware-1.log' and 'vmware-2.log'.



Il ripristino può essere eseguito da SnapCenter per VMware o dal plugin SnapCenter , a seconda dell'applicazione.

La soluzione NetApp fornisce diversi strumenti efficaci per la visibilità, il rilevamento e la correzione, aiutandoti a individuare tempestivamente il ransomware, a prevenirne la diffusione e a ripristinare rapidamente, se necessario, per evitare costosi tempi di inattività. Le soluzioni di difesa tradizionali a più livelli continuano a

essere prevalenti, così come le soluzioni di terze parti e partner per la visibilità e il rilevamento. Una bonifica efficace resta una parte fondamentale della risposta a qualsiasi minaccia.

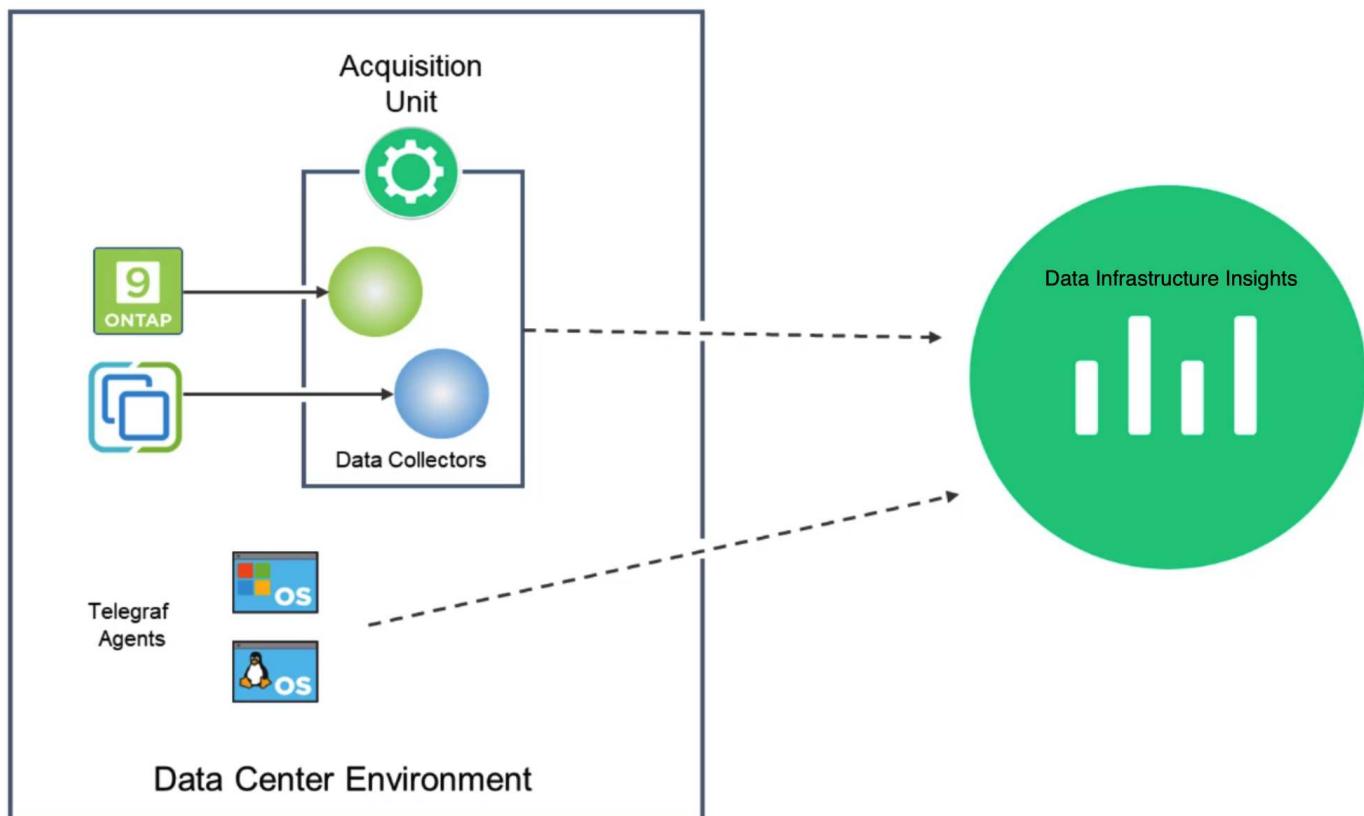
Monitora l'archiviazione on-premise con Data Infrastructure Insights

NetApp Data Infrastructure Insights (in precedenza Cloud Insights) è una piattaforma basata su cloud progettata per monitorare e analizzare le prestazioni, lo stato di salute e i costi delle infrastrutture IT, sia on-premise che nel cloud. Scopri come distribuire strumenti di raccolta dati, analizzare le metriche delle prestazioni e utilizzare dashboard per identificare problemi e ottimizzare le risorse.

Monitoraggio dell'archiviazione locale con Data Infrastructure Insights

Data Infrastructure Insights funziona tramite il software Acquisition Unit, configurato con collettori di dati per asset quali i sistemi di storage VMware vSphere e NetApp ONTAP. Questi collettori raccolgono i dati e li trasmettono a Data Infrastructure Insights. La piattaforma utilizza quindi una serie di dashboard, widget e query metriche per organizzare i dati in analisi approfondite che gli utenti possono interpretare.

Diagramma dell'architettura Data Infrastructure Insights :



Panoramica sulla distribuzione della soluzione

Questa soluzione fornisce un'introduzione al monitoraggio dei sistemi di storage VMware vSphere e ONTAP on-premise mediante Data Infrastructure Insights.

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

1. Configurare Data Collector per un cluster vSphere.
2. Configurare Data Collector per un sistema di archiviazione ONTAP .
3. Utilizzare le regole di annotazione per contrassegnare le risorse.
4. Esplora e correla le risorse.
5. Utilizzare una dashboard Top VM Latency per isolare i vicini rumorosi.
6. Identificare le opportunità per dimensionare correttamente le VM.
7. Utilizzare le query per isolare e ordinare le metriche.

Prerequisiti

Questa soluzione utilizza i seguenti componenti:

1. NetApp SAN All-Flash NetApp A400 con ONTAP 9.13.
2. Cluster VMware vSphere 8.0.
3. Account NetApp Console .
4. Software NetApp Data Infrastructure Insights Acquisition Unit installato su una VM locale con connettività di rete alle risorse per la raccolta dati.

Distribuzione della soluzione

Configurare i raccoglitori di dati

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

Aggiungere un Data Collector per un sistema di archiviazione ONTAP

1. Dopo aver effettuato l'accesso a Data Infrastructure Insights, vai su **Observability > Collectors > Data Collectors** e premi il pulsante per installare un nuovo Data Collector.

The screenshot shows the 'Data Collectors' page in NetApp Cloud Insights. The left sidebar has 'Observability' selected. The main area shows 84 data collectors. At the top right, there are buttons for 'Data Collectors' (7), 'Acquisition Units' (3), and 'Kubernetes Collectors'. Below these are 'Bulk Actions' and a 'Filter...' button. A prominent purple box highlights the '+ Data Collector' button.

2. Da qui cerca * ONTAP* e clicca su *Software di gestione dati ONTAP*.

The screenshot shows a search results page for 'ontap'. It lists four options: 'FSx for NetApp ONTAP', 'Cloud Volumes ONTAP', 'ONTAP Data Management Software' (which is highlighted with a purple box and has a cursor arrow pointing to it), and 'ONTAP Select'.

3. Nella pagina **Configura Collector**, inserisci un nome per il collector, specifica l'**Unità di acquisizione** corretta e fornisci le credenziali per il sistema di archiviazione ONTAP . Fare clic su **Salva e continua** e poi su **Completa configurazione** in fondo alla pagina per completare la configurazione.



The screenshot shows the 'Configure Collector' page for ONTAP Data Management Software. It includes fields for 'Name' (ntaphci-a300e9u25), 'Acquisition Unit' (bxp-au01), 'NetApp Management IP Address' (10.61.185.145), 'User Name' (admin), 'Password' (redacted), and checkboxes for 'Advanced Configuration' and 'Test Connection'. A purple box highlights the 'Save and Continue' button at the bottom left.

Aggiungere un Data Collector per un cluster VMware vSphere

1. Ancora una volta, vai su **Observability > Collectors > Data Collectors** e premi il pulsante per installare un nuovo Data Collector.

The screenshot shows the NetApp Cloud Insights interface. The left sidebar has 'Observability' selected. The main area shows 'Data Collectors (84)' with a search bar and filters for 'Name ↑', 'Status', 'Type', 'Acquisition Unit', and 'IP'. A blue button labeled '+ Data Collector' is highlighted with a red box. Other tabs include 'Acquisition Units' (0) and 'Kubernetes Collectors'.

2. Da qui cerca **vSphere** e clicca su **VMware vSphere**.

The screenshot shows the 'Add Data Collector' page. The left sidebar has 'Collectors' selected. The main area has a search bar with 'vsphere' typed in. Below it, a box labeled 'vmware' with 'vsphere' underneath has a hand cursor icon pointing at it.

3. Nella pagina **Configura Collector**, inserisci un nome per il collector, specifica l'**Unità di acquisizione** corretta e fornisci le credenziali per il server vCenter. Fare clic su **Salva e continua** e poi su **Completa configurazione** in fondo alla pagina per completare la configurazione.

Select a Data Collector

Configure Data Collector

Configure Collector

Add credentials and required settings Need Help?

Name ? VCSA7	Acquisition Unit bxp-au01
Virtual Center IP Address 10.61.181.210	User Name administrator@vsphere.local
Password *****	
Complete Setup Test Connection	
<input type="checkbox"/> Advanced Configuration	
Collecting:	
<input checked="" type="checkbox"/> Inventory	
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> Collect basic performance metrics only	
Complete Setup Test Connection	

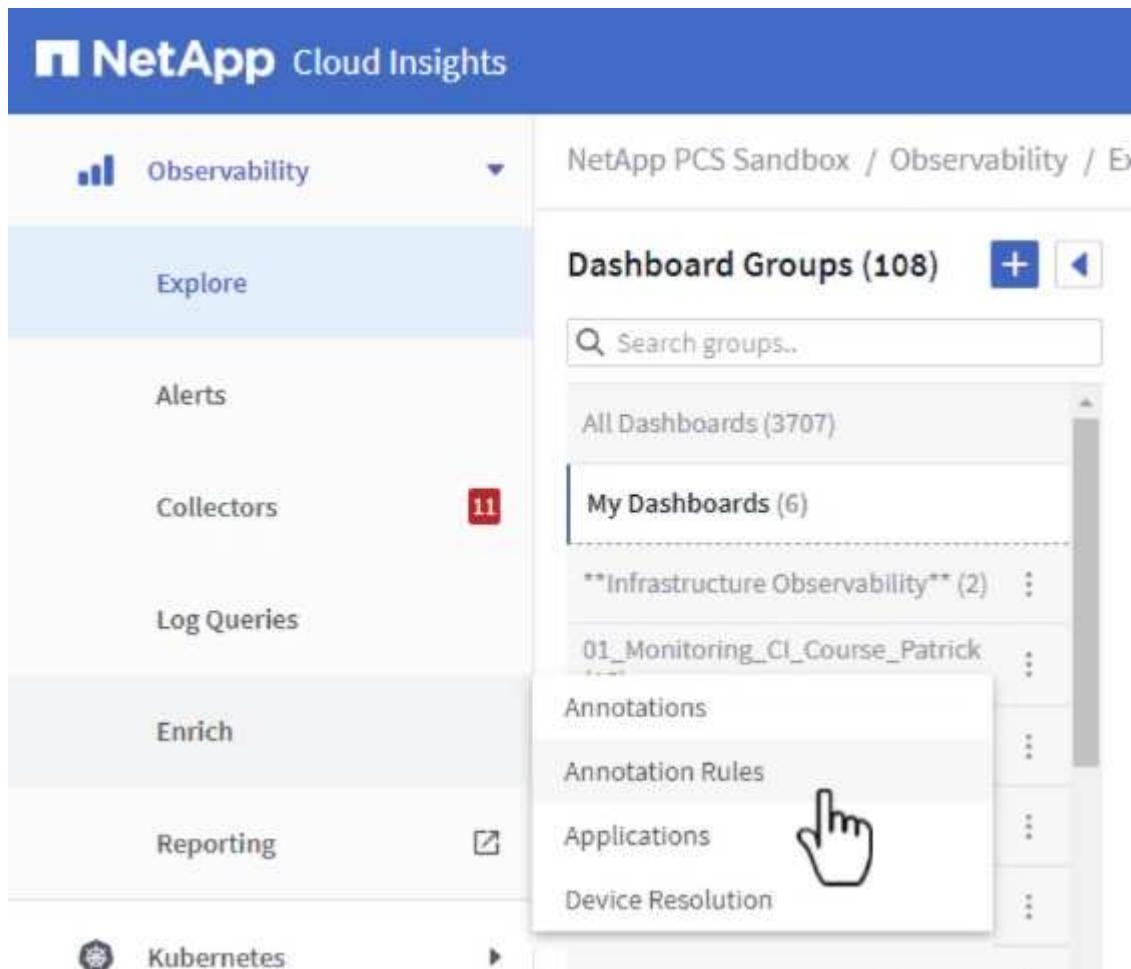
Aggiungi annotazioni alle risorse

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

In questa sezione verranno aggiunte annotazioni alle risorse della macchina virtuale per il filtraggio in base al **Data Center**.

Utilizzare le regole di annotazione per taggare le risorse

- Nel menu a sinistra, vai su **Osservabilità > Arricchisci > Regole di annotazione** e clicca sul pulsante **+ Regola** in alto a destra per aggiungere una nuova regola.



- Nella finestra di dialogo **Aggiungi regola**, inserisci un nome per la regola, individua una query a cui verrà applicata la regola, il campo di annotazione interessato e il valore da popolare.

Add Rule

Name

Query

Annotation

Value

Cancel
Save

3. Infine, nell'angolo in alto a destra della pagina **Regole di annotazione**, fare clic su **Esegui tutte le regole** per eseguire la regola e applicare l'annotazione alle risorse.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Annotation rules (217)
Rules running...
Run All Rules

Name	Resource Type	Query	Annotation	Value	⋮
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 1	⋮
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggr0) for Tier...	Tier	Tier 2	⋮

Esplora e correla le risorse

Cloud Insights trae conclusioni logiche sulle risorse in esecuzione contemporaneamente sui sistemi di storage e sui cluster vSphere.

Questa sezione illustra come utilizzare i dashboard per correlare le risorse.

Correlazione delle risorse da una dashboard delle prestazioni di archiviazione

1. Nel menu a sinistra, vai su **Osservabilità > Esplora > Tutte le dashboard**.

The screenshot shows the NetApp Cloud Insights interface. The top navigation bar has the NetApp logo and 'Cloud Insights'. Below it, the 'Observability' menu is open, showing 'Explore', 'Alerts', and 'Collectors'. A context menu is displayed over the 'Collectors' button, containing options like 'Home Dashboard', 'All Dashboards', '+ New Dashboard' (with a hand cursor pointing at it), 'Metric Queries', and 'Infrastructure Insights'. The 'Collectors' button has a red badge with the number '17'.

2. Fare clic sul pulsante **+ Dalla galleria** per visualizzare un elenco di dashboard già pronte che possono essere importate.

The screenshot shows the 'Dashboards' page under the 'Explore' section. It displays 'Dashboard Groups (108)' and 'All Dashboards (3,708)'. A search bar is present, along with a sorting option 'Name ↑'. Two dashboard entries are listed:

- # Internal Volumes by IOPS Range (do not set as Home Page!) - Owner: Workneh Hilina
- # Internal Volumes by IOPS Range - Owner: Simon Wu

A red box highlights the '+ From Gallery' button in the top right corner of the table header.

3. Scegli dall'elenco una dashboard per le prestazioni FlexVol e clicca sul pulsante **Aggiungi dashboard** in fondo alla 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?

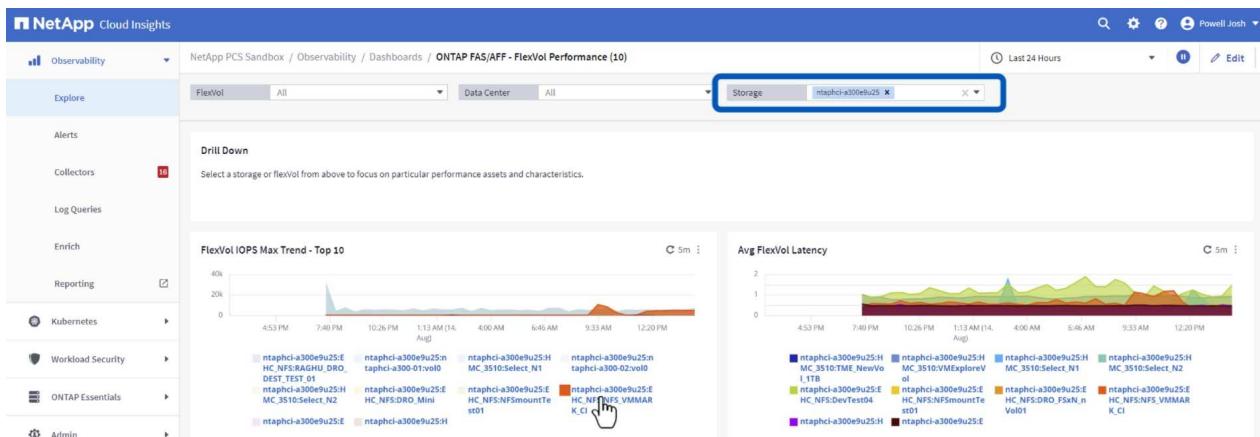
Additional Dashboards (13)

These dashboards require additional data collectors to be installed. [Add More](#)

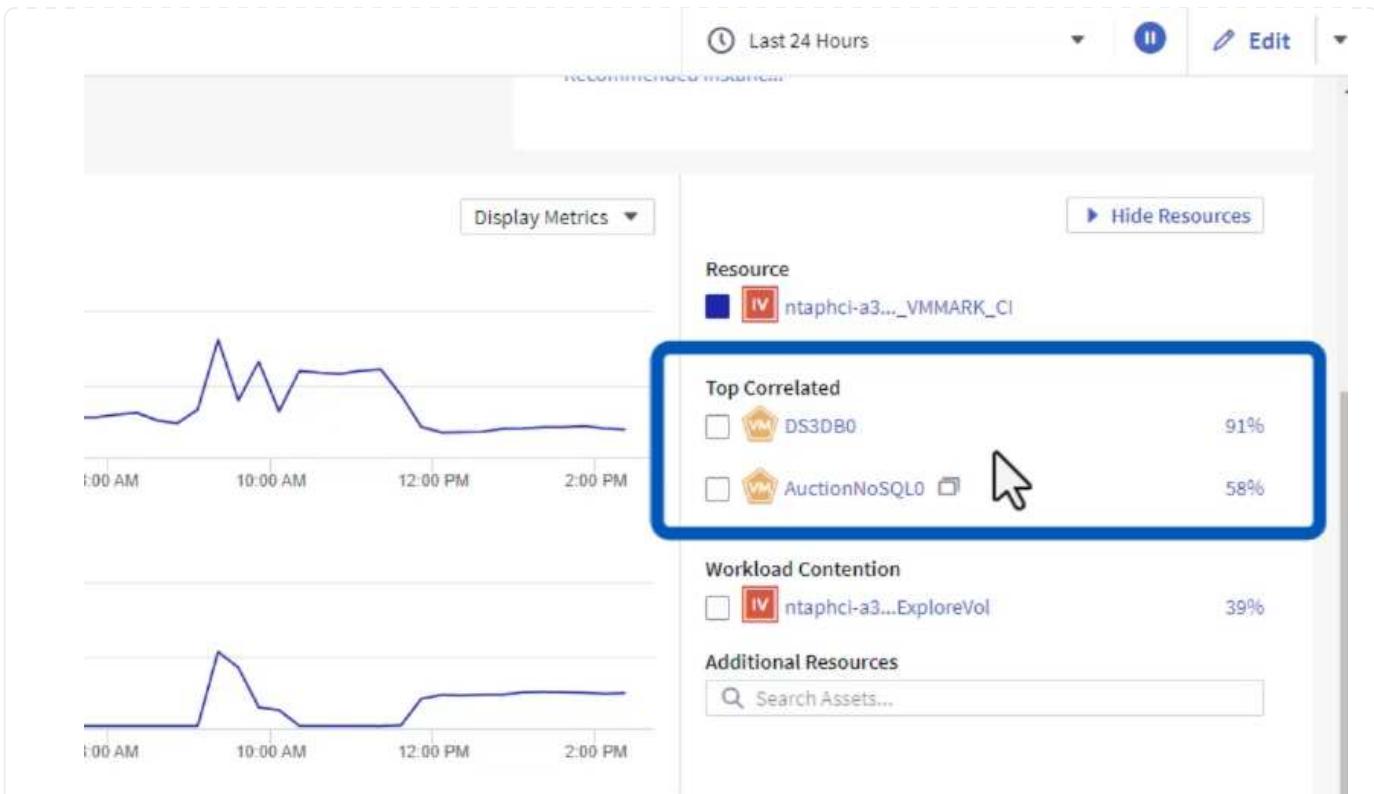
[Add Dashboards](#)

[Go Back](#)

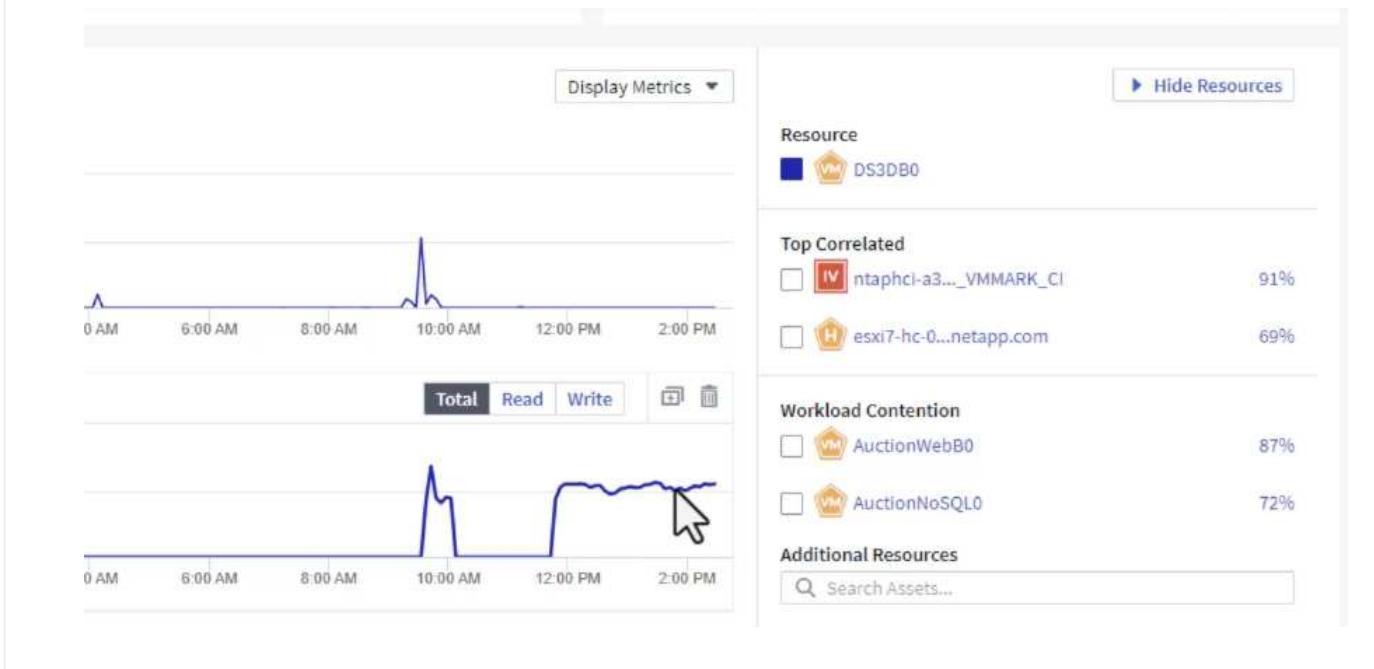
- Una volta importato, apri la dashboard. Da qui puoi vedere vari widget con dati dettagliati sulle prestazioni. Aggiungi un filtro per visualizzare un singolo sistema di archiviazione e seleziona un volume di archiviazione per analizzarne i dettagli.



- Da questa vista è possibile visualizzare varie metriche relative a questo volume di archiviazione e alle macchine virtuali più utilizzate e correlate in esecuzione sul volume.



6. Facendo clic sulla VM con il più alto utilizzo, si accede alle metriche per quella VM per visualizzare eventuali problemi.



Utilizza Cloud Insights per identificare i vicini rumorosi

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

Utilizzare una dashboard Top VM Latency per isolare i vicini rumorosi

1. In questo esempio accedi a una dashboard disponibile nella **Galleria** denominata **VMware Admin - Dove trovo la latenza della VM?**

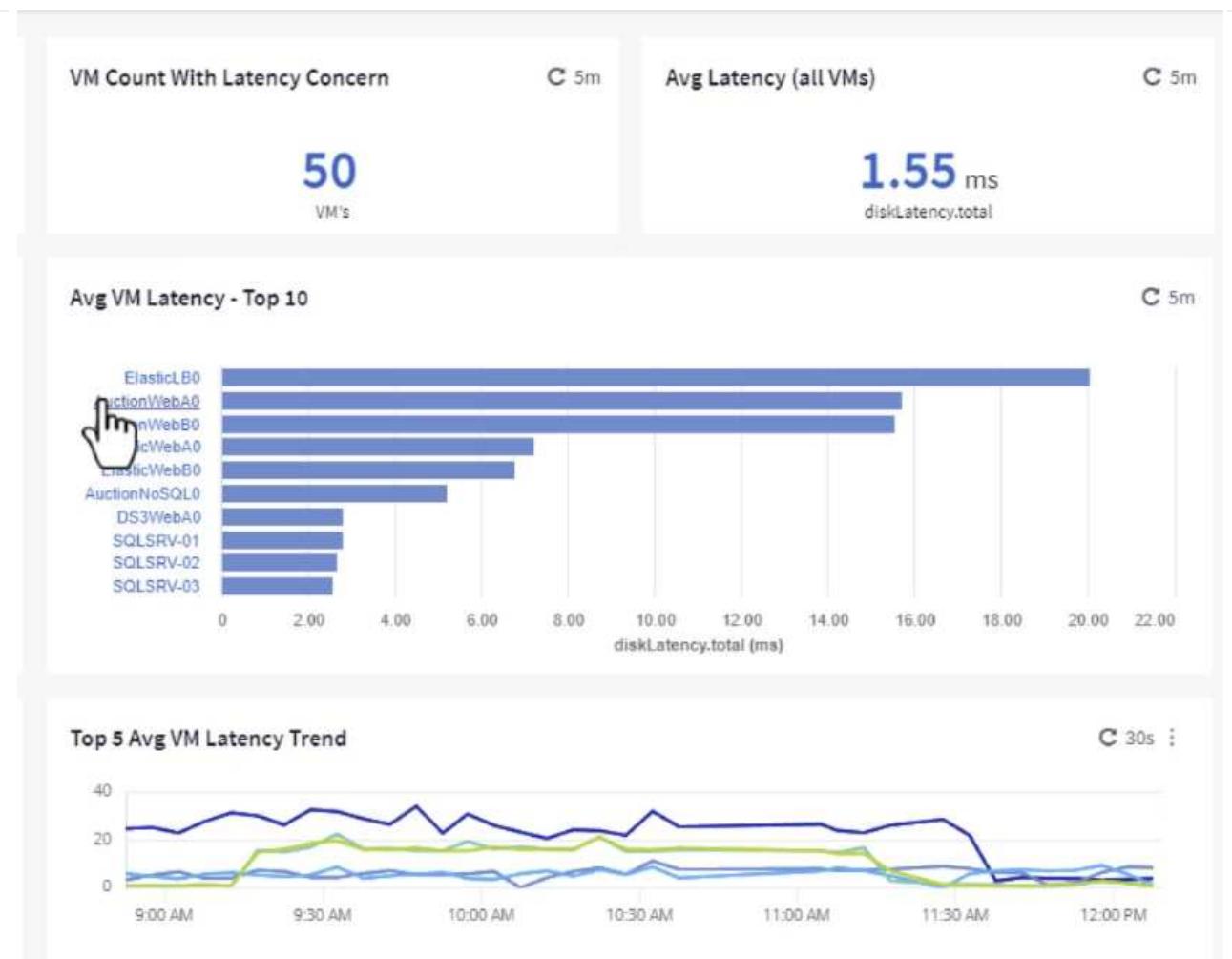
The screenshot shows the 'Dashboards' section of the NetApp PCS Sandbox Observability interface. On the left, there's a sidebar with 'Dashboard Groups (108)' and a search bar. The main area is titled 'My Dashboards (6)'. It lists six dashboards with their names and owners:

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
VMware Admin - Where do I have VM Latency? (9)	Powell Josh

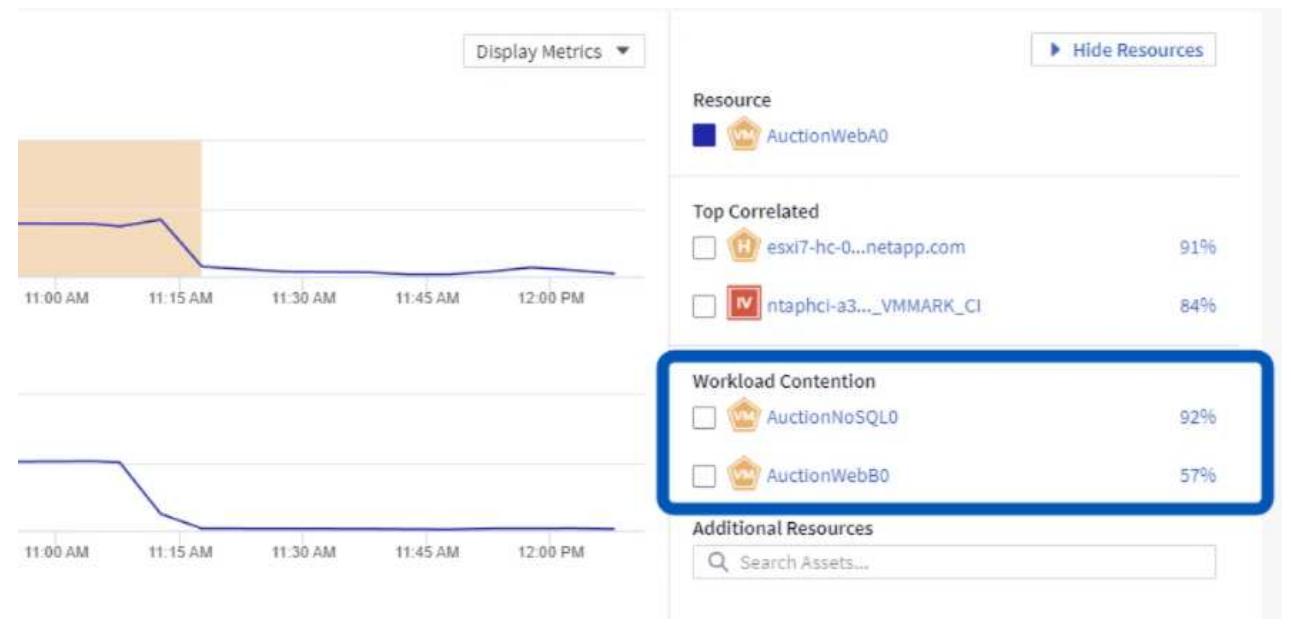
2. Successivamente, filtra in base all'annotazione **Data Center** creata in un passaggio precedente per visualizzare un sottoinsieme di risorse.

The screenshot shows the 'VMware Admin - Where do I have VM Latency?' dashboard. At the top, there's a filter bar with several dropdowns and a search bar. The 'Data Center' dropdown is highlighted with a purple box and has a cursor pointing at it. Other dropdowns include 'VirtualMachine', 'All', 'Solutions Engineering', and 'diskLatency.total'. Below the filter bar, there are four time-series cards showing 'Avg Latency (all hypervisors)', 'VM Count With Latency Concern', and 'Avg Latency (all VMs)' over the last 5 minutes.

3. Questa dashboard mostra un elenco delle 10 VM più performanti in base alla latenza media. Da qui fare clic sulla VM interessata per approfondirne i dettagli.



- Le VM che potrebbero causare conflitti di carico di lavoro sono elencate e disponibili. Analizza attentamente le metriche delle prestazioni di queste VM per individuare eventuali problemi.



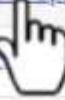
Visualizza le risorse sovra e sottoutilizzate in Cloud Insights

Abbinando le risorse delle VM ai requisiti effettivi del carico di lavoro, è possibile ottimizzare l'utilizzo delle risorse, con conseguente risparmio sui costi dell'infrastruttura e dei servizi cloud. I dati in Cloud Insights possono essere personalizzati per visualizzare facilmente le VM sovra o sotto utilizzate.

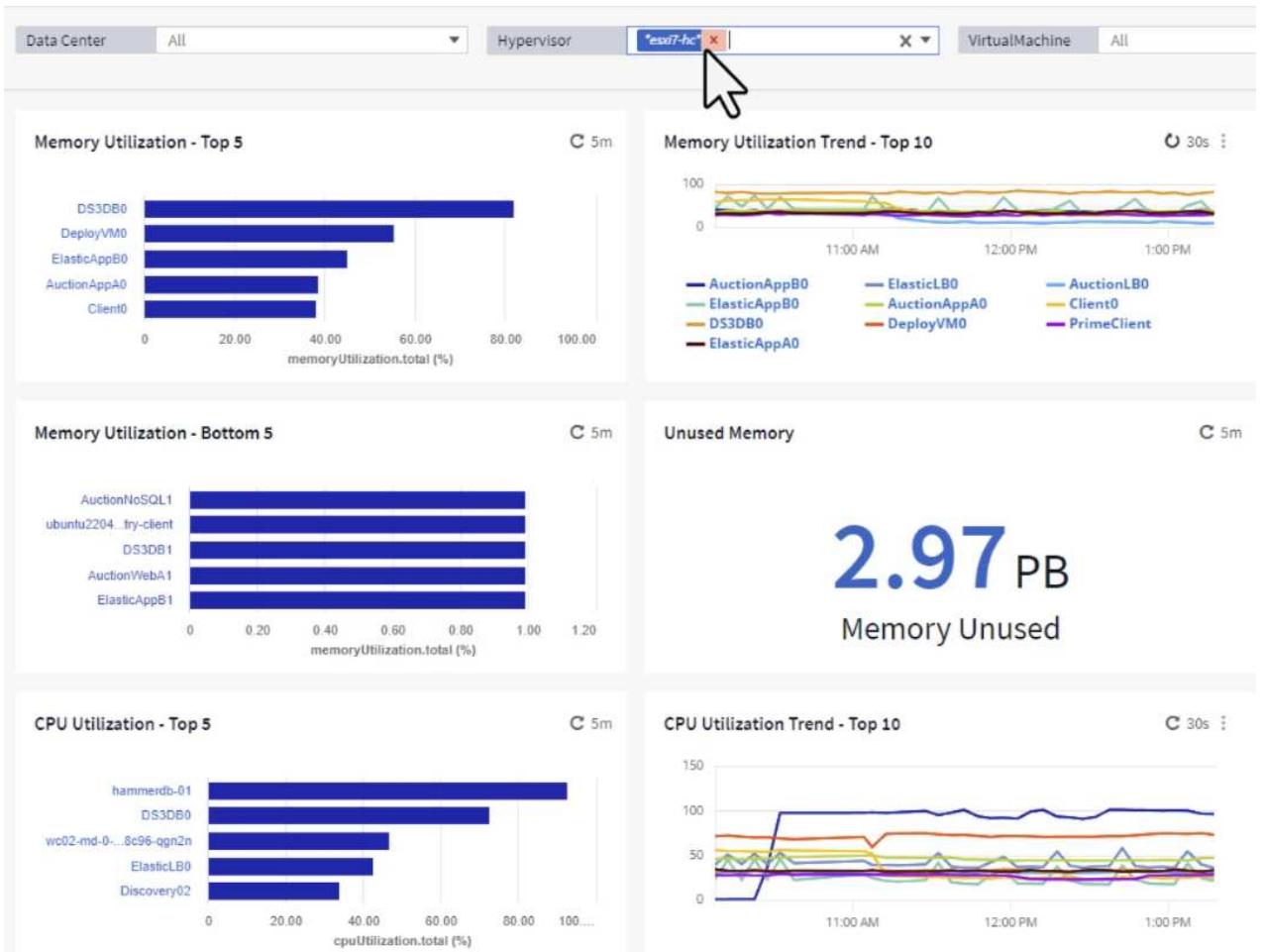
Identificare le opportunità per dimensionare correttamente le VM

1. In questo esempio accedi a una dashboard disponibile nella **Galleria** denominata **VMware Admin - Dove sono le opportunità da dimensionare correttamente?**

My Dashboards (6)

<input type="checkbox"/>	Name ↑
	All SAN Array Status (2)
	Cloud Volumes ONTAP - FlexVol Performance (6)
	ONTAP - Volume Workload Performance (Frontend) (7)
<input type="checkbox"/> ⭐	<u>VMware Admin - Where are opportunities to right size? (37)</u>
	VMware Admin - Where can I potentially reclaim waste? (11) 
	VMware Admin - Where do I have VM Latency? (9)

2. Per prima cosa filtrare in base a tutti gli host ESXi nel cluster. È quindi possibile visualizzare la classifica delle VM migliori e peggiori in base all'utilizzo di memoria e CPU.



3. Le tabelle consentono di ordinare e forniscono maggiori dettagli in base alle colonne di dati scelte.

Memory Usage

C 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

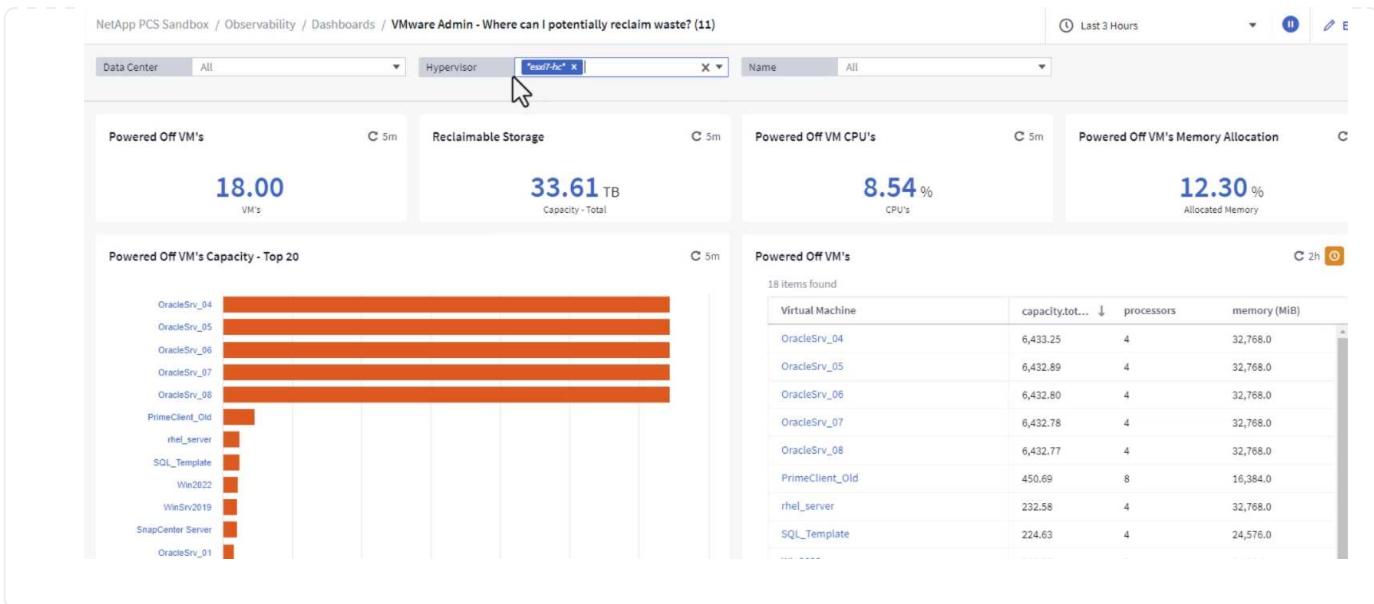
CPU Utilization

C 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'altra dashboard denominata **VMware Admin - Dove posso potenzialmente recuperare gli sprechi?** mostra le VM spente ordinate in base alla loro capacità di utilizzo.

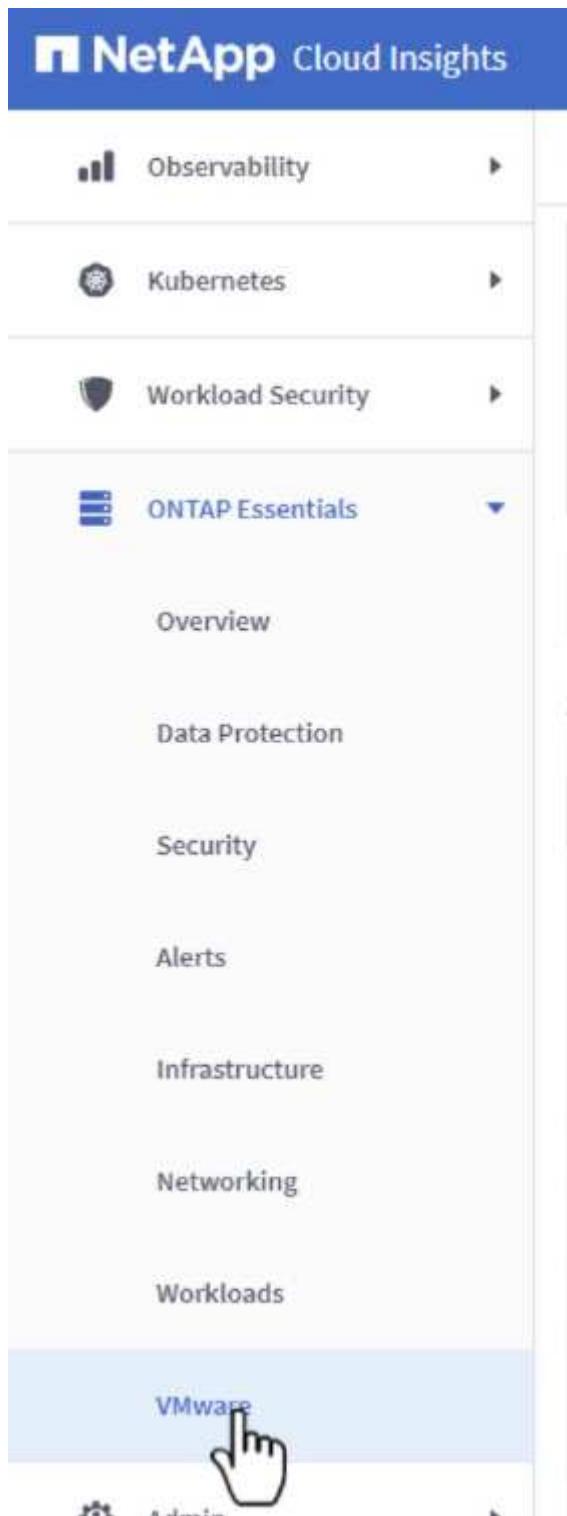


Utilizzare query per isolare e ordinare le metriche

La quantità di dati acquisiti da Cloud Insights è piuttosto ampia. Le query metriche rappresentano un modo efficace per ordinare e organizzare grandi quantità di dati in modo utile.

Visualizza una query VMware dettagliata in ONTAP Essentials

1. Passare a * ONTAP Essentials > VMware* per accedere a una query completa sulle metriche VMware.



2. In questa vista vengono presentate diverse opzioni per filtrare e raggruppare i dati nella parte superiore. Tutte le colonne di dati sono personalizzabili e possono essere aggiunte facilmente altre colonne.

The screenshot shows a detailed view of a table within the NetApp Cloud Insights interface. The table lists 281 items found, specifically virtual machines, grouped by 'Virtual Machine'. The columns include: name, powerState, capacity.used (GiB), capacity.total (GiB), capacityRatio.us..., diskIops.total (IO/s), diskLatency.total..., and diskThroughput.... The table header also includes 'Metrics & Attributes' and 'Table Row Grouping' options.

Virtual Machine	name	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (IO/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

Conclusioni

Questa soluzione è stata progettata come introduzione per imparare a usare NetApp Cloud Insights e mostrare alcune delle potenti funzionalità che questa soluzione di osservabilità può offrire. Il prodotto è dotato di centinaia di dashboard e query metriche integrate, che consentono di iniziare subito a utilizzarlo. La versione completa di Cloud Insights è disponibile come prova di 30 giorni, mentre la versione base è disponibile gratuitamente per i clienti NetApp .

Informazioni aggiuntive

Per saperne di più sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- ["Pagina di destinazione NetApp Console"](#)
- ["Pagina di destinazione NetApp Data Infrastructure Insights"](#)
- ["Documentazione NetApp Data Infrastructure Insights"](#)

Informazioni sul copyright

Copyright © 2026 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 COMMERCIALITÀ 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.