# VMware

## Enterprise applications

NetApp
May 09, 2024

# Sommario

# VMware

# VMware vSphere con ONTAP

## VMware vSphere con ONTAP

ONTAP è da quasi vent'anni una soluzione di storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione e ridurre i costi. Questo documento presenta la soluzione ONTAP per vSphere, incluse le informazioni più recenti sui prodotti e le Best practice, per ottimizzare l'implementazione, ridurre i rischi e semplificare la gestione.

Questa documentazione sostituisce i report tecnici precedentemente pubblicati *TR-4597: VMware vSphere for ONTAP*

Le Best practice integrano altri documenti come guide ed elenchi di compatibilità. Sono sviluppati in base a test di laboratorio e a un'ampia esperienza sul campo da parte di tecnici e clienti NetApp. Potrebbero non essere le uniche pratiche supportate che funzionano in ogni ambiente, ma sono generalmente le soluzioni più semplici che soddisfano le esigenze della maggior parte dei clienti.

Questo documento si concentra sulle funzionalità delle versioni recenti di ONTAP (9.x) in esecuzione su vSphere 7,0 o versioni successive. Vedere "Tool di matrice di interoperabilità NetApp" e. "Guida alla compatibilità VMware" per dettagli relativi a release specifiche.

#### Perché scegliere ONTAP per vSphere?

Sono molti i motivi per cui decine di migliaia di clienti hanno scelto ONTAP come soluzione storage per vSphere, ad esempio un sistema storage unificato che supporta protocolli SAN e NAS, solide funzionalità di protezione dei dati che utilizzano snapshot efficienti in termini di spazio e molti strumenti per aiutarti a gestire i dati delle applicazioni. L'utilizzo di un sistema storage separato dall'hypervisor consente di trasferire molte funzioni e massimizzare l'investimento nei sistemi host vSphere. Questo approccio non solo garantisce che le risorse host siano incentrate sui carichi di lavoro delle applicazioni, ma evita anche effetti casuali sulle performance delle applicazioni derivanti dalle operazioni di storage.

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

Ecco i fattori chiave che i clienti apprezzano oggi:

- **Storage unificato.** i sistemi che eseguono il software ONTAP sono unificati in diversi modi significativi. In origine, questo approccio si riferiva ai protocolli NAS e SAN e ONTAP continua a essere una piattaforma leader per SAN insieme alla sua forza originale nel NAS. Nel mondo vSphere, questo approccio potrebbe anche significare un sistema unificato per l'infrastruttura di desktop virtuale (VDI) insieme all'infrastruttura di server virtuale (VSI). I sistemi che eseguono il software ONTAP sono in genere meno costosi per VSI rispetto agli array aziendali tradizionali e dispongono tuttavia di funzionalità avanzate di efficienza dello storage per gestire VDI nello stesso sistema. ONTAP unifica inoltre una vasta gamma di supporti storage, da SSD a SATA, e può estenderli facilmente nel cloud. Non è necessario acquistare un flash array per le performance, un array SATA per gli archivi e sistemi separati per il cloud. ONTAP li lega tutti insieme.

- **Volumi virtuali e gestione basata su policy dello storage.** NetApp è stato un partner di progettazione iniziale di VMware nello sviluppo di vVol (vSphere Virtual Volumes), che offre input architetturali e supporto precoce di vVol e API di VMware vSphere per Storage Awareness (VASA). Questo approccio non solo ha portato a VMFS una gestione granulare dello storage delle macchine virtuali, ma ha anche supportato l'automazione del provisioning dello storage tramite la gestione basata su criteri dello storage. Questo approccio consente agli architetti dello storage di progettare pool di storage con diverse funzionalità che possono essere facilmente utilizzate dagli amministratori delle macchine virtuali. ONTAP è leader nel settore dello storage in termini di scalabilità vVol, supportando centinaia di migliaia di vVol in un singolo cluster, mentre i vendor di array Enterprise e flash array più piccoli supportano solo diverse migliaia di vVol per array. NetApp sta inoltre guidando l'evoluzione della gestione granulare delle macchine virtuali con funzionalità imminenti a supporto di vVol 3.0.
- **Efficienza dello storage.** sebbene NetApp sia stata la prima a fornire la deduplica per carichi di lavoro di produzione, questa innovazione non è stata la prima o l'ultima in quest'area. Il prodotto è partito dalle snapshot, un meccanismo di protezione dei dati efficiente in termini di spazio, senza effetti sulle performance, e dalla tecnologia FlexClone per creare istantaneamente copie in lettura/scrittura delle macchine virtuali per l'utilizzo in produzione e nel backup. NetApp ha continuato a offrire funzionalità inline, tra cui deduplica, compressione e deduplica a blocchi zero, per eliminare il maggior numero di storage dai costosi SSD. Più di recente, ONTAP ha aggiunto la possibilità di inserire file e operazioni i/o più piccole in un blocco di dischi utilizzando la compattazione. La combinazione di queste funzionalità ha consentito ai clienti di ottenere risparmi fino a 5:1 per VSI e fino a 30:1 per VDI.
- **Cloud ibrido.** sia che venga utilizzato per il cloud privato on-premise, l'infrastruttura di cloud pubblico o un cloud ibrido che combina il meglio di entrambi, le soluzioni ONTAP ti aiutano a costruire il tuo data fabric per ottimizzare e ottimizzare la gestione dei dati. Inizia con i sistemi all-flash dalle performance elevate, quindi accoppiali con sistemi di storage su disco o cloud per la protezione dei dati e il cloud computing. Scegli tra cloud Azure, AWS, IBM o Google per ottimizzare i costi ed evitare il lock-in. Sfrutta il supporto avanzato per le tecnologie OpenStack e container in base alle esigenze. NetApp offre inoltre backup basato sul cloud (SnapMirror Cloud, Cloud Backup Service e Cloud Sync) e tool di archiviazione e tiering dello storage (FabricPool) per ONTAP per ridurre le spese operative e sfruttare l'ampia portata del cloud.
- **E altro ancora.** sfrutta le performance estreme degli array NetApp AFF Serie A per accelerare l'infrastruttura virtualizzata e gestire i costi. Operazioni senza interruzioni, dalla manutenzione agli aggiornamenti fino alla sostituzione completa del sistema storage, utilizzando cluster ONTAP scale-out. Proteggi i dati inattivi con le funzionalità di crittografia NetApp senza costi aggiuntivi. Assicurati che le performance soddisfino i livelli di servizio di business grazie a funzionalità di qualità dei servizi. Fanno tutti parte dell'ampia gamma di funzionalità offerte da ONTAP, il software di Enterprise data management leader del settore.

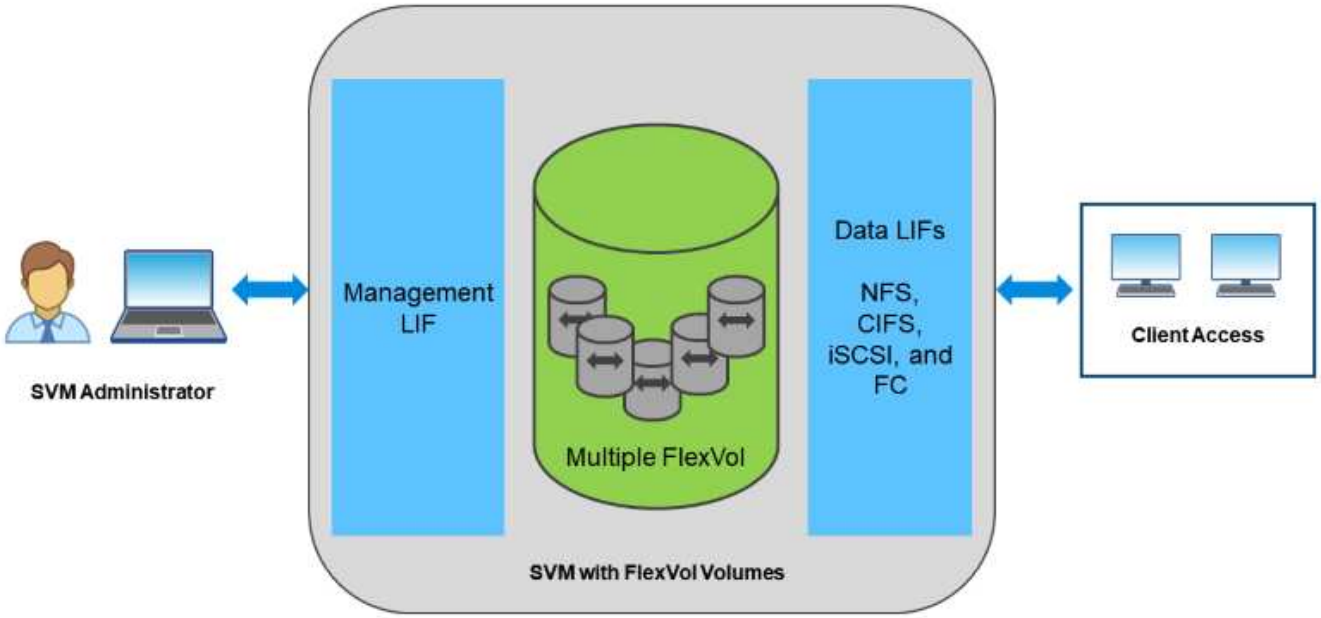
## Storage unificato

NetApp ONTAP unifica lo storage tramite un approccio software-defined semplificato per una gestione sicura ed efficiente, performance migliorate e una perfetta scalabilità. Questo approccio migliora la protezione dei dati e consente un uso efficace delle risorse cloud.

In origine, questo approccio unificato ha indicato il supporto dei protocolli NAS e SAN su un unico sistema di storage e ONTAP continua a essere una piattaforma leader per SAN e la sua forza originale nel campo delle NAS. ONTAP ora fornisce anche il supporto del protocollo a oggetti S3. Sebbene S3 non sia utilizzato per i datastore, è possibile utilizzarlo per le applicazioni in-guest. Per ulteriori informazioni sul supporto del protocollo S3 in ONTAP, consultare la sezione "Panoramica della configurazione S3".

Una Storage Virtual Machine (SVM) è l'unità di multi-tenancy sicura in ONTAP. Si tratta di un costrutto logico che consente l'accesso client ai sistemi che eseguono il software ONTAP. Le SVM possono servire i dati contemporaneamente attraverso più protocolli di accesso ai dati tramite le interfacce logiche (LIF). Le SVM

forniscono l'accesso ai dati a livello di file attraverso protocolli NAS, come CIFS e NFS, e l'accesso ai dati a livello di blocco attraverso protocolli SAN, come iSCSI, FC/FCoE e NVMe. Le SVM possono fornire dati ai client SAN e NAS in modo indipendente e con S3.




Nel mondo vSphere, questo approccio potrebbe anche significare un sistema unificato per l'infrastruttura di desktop virtuale (VDI) insieme all'infrastruttura di server virtuale (VSI). I sistemi che eseguono il software ONTAP sono in genere meno costosi per VSI rispetto agli array aziendali tradizionali e dispongono tuttavia di funzionalità avanzate di efficienza dello storage per gestire VDI nello stesso sistema. ONTAP unifica inoltre una vasta gamma di supporti storage, da SSD a SATA, e può estenderli facilmente nel cloud. Non è necessario acquistare un flash array per le performance, un array SATA per gli archivi e sistemi separati per il cloud. ONTAP li lega tutti insieme.

**NOTA:** per ulteriori informazioni sulle SVM, sullo storage unificato e sull'accesso dei client, vedere "Virtualizzazione dello storage" Nel centro di documentazione di ONTAP 9.

## Strumenti di virtualizzazione per ONTAP

NetApp offre diversi tool software standalone che possono essere utilizzati insieme a ONTAP e vSphere per gestire l'ambiente virtualizzato.

I seguenti strumenti sono inclusi con la licenza ONTAP senza costi aggiuntivi. Vedere la Figura 1 per un'illustrazione del funzionamento di questi strumenti nell'ambiente vSphere.

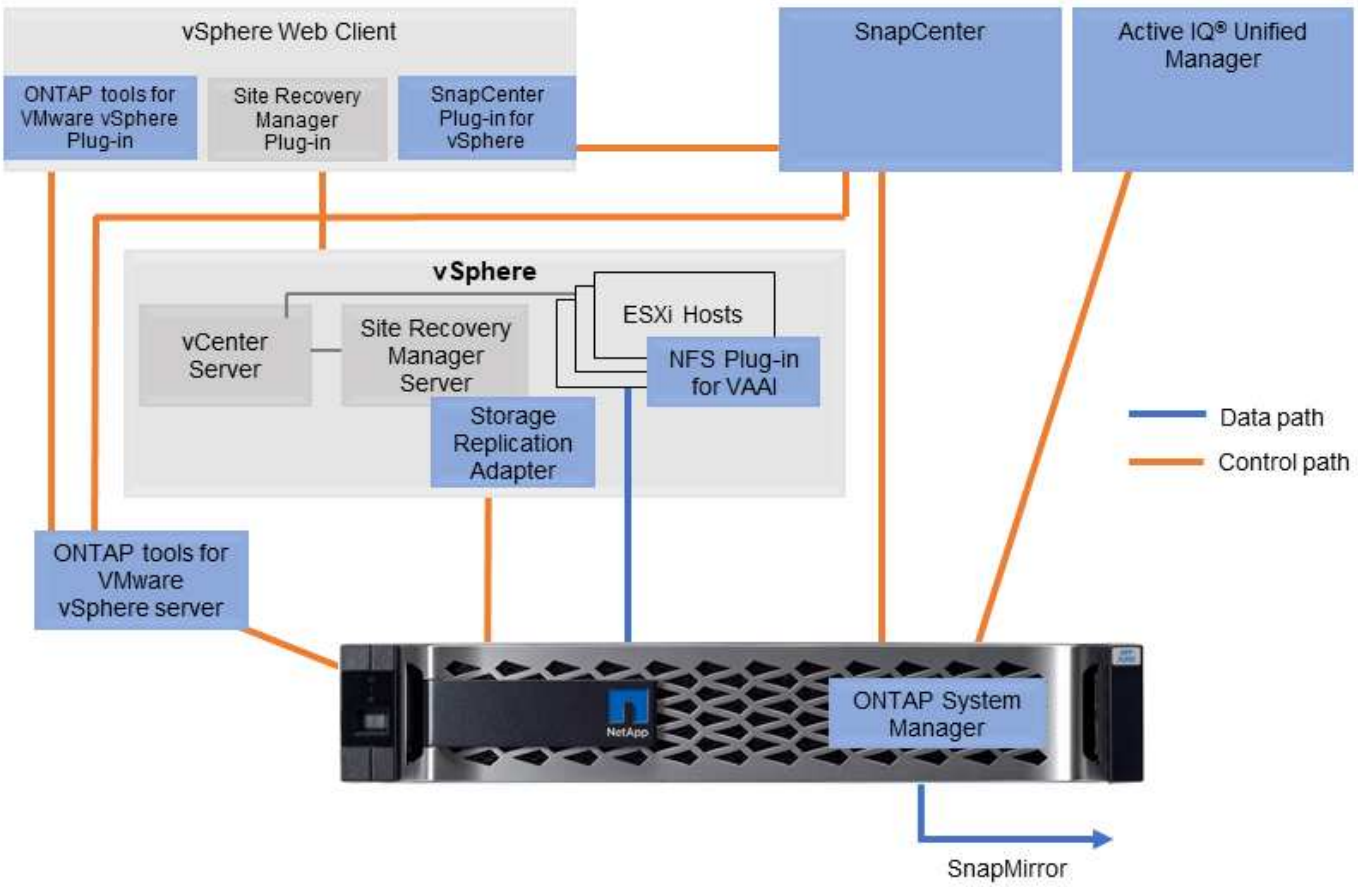
### Strumenti ONTAP per VMware vSphere

ONTAP Tools per VMware vSphere è un insieme di strumenti per l'utilizzo dello storage ONTAP insieme a vSphere. Il plug-in vCenter, precedentemente noto come Virtual Storage Console (VSC), semplifica le funzionalità di gestione ed efficienza dello storage, migliora la disponibilità e riduce i costi di storage e l'overhead operativo, sia che si utilizzi SAN che NAS. Utilizza le Best practice per il provisioning degli archivi dati e ottimizza le impostazioni degli host ESXi per gli ambienti di storage a blocchi e NFS. Per tutti questi

vantaggi, NetApp consiglia di utilizzare questi tool ONTAP come Best practice quando si utilizza vSphere con sistemi che eseguono il software ONTAP. Include un'appliance server, estensioni dell'interfaccia utente per vCenter, VASA Provider e Storage Replication Adapter. Quasi tutto ciò che è contenuto negli strumenti ONTAP può essere automatizzato utilizzando semplici API REST, utilizzabili dalla maggior parte dei moderni strumenti di automazione.

- Le estensioni dell'interfaccia utente di vCenter.* le estensioni dell'interfaccia utente di ONTAP Tools semplificano il lavoro dei team operativi e degli amministratori di vCenter, integrando menu facili da utilizzare e sensibili al contesto per la gestione di host e storage, portlet informativi e funzionalità di avviso native direttamente nell'interfaccia utente di vCenter per flussi di lavoro semplificati.
- **Provider VASA per ONTAP.** il provider VASA per ONTAP supporta il framework VMware vStorage API for Storage Awareness (VASA). Viene fornito come parte dei tool ONTAP per VMware vSphere come singola appliance virtuale per una maggiore facilità di implementazione. IL provider VASA connette vCenter Server a ONTAP per facilitare il provisioning e il monitoraggio dello storage delle macchine virtuali. Consente il supporto di VMware Virtual Volumes (vVol), la gestione dei profili di capacità dello storage e delle performance di VM vVol individuali e gli allarmi per il monitoraggio della capacità e della conformità con i profili.
- **Storage Replication Adapter.** SRA viene utilizzato insieme a VMware Site Recovery Manager (SRM) per gestire la replica dei dati tra siti di produzione e disaster recovery e testare le repliche DR senza interruzioni. Consente di automatizzare le attività di rilevamento, ripristino e protezione. Include un'appliance server SRA e adattatori SRA per server SRM Windows e appliance SRM.

La figura seguente mostra gli strumenti ONTAP per vSphere.



#### Plug-in NFS per VMware VAAI

Il plug-in NetApp NFS per VMware VAAI è un plug-in per gli host ESXi che consente loro di utilizzare le funzionalità VAAI con gli archivi dati NFS su ONTAP. Supporta l'offload delle copie per le operazioni di cloning, lo space reservation per i file di dischi virtuali con thick provisioning e l'offload delle snapshot. L'offload delle operazioni di copia sullo storage non è necessariamente più veloce da completare, ma riduce i requisiti di larghezza di banda della rete e scarica le risorse host come cicli CPU, buffer e code. È possibile utilizzare i tool ONTAP per VMware vSphere per installare il plug-in sugli host ESXi o, se supportato, vSphere Lifecycle Manager (vLCM).

## Virtual Volumes (vVol) e Storage Policy Based Management (SPBM)

NetApp è stato un primo partner di progettazione di VMware nello sviluppo di vVol (vSphere Virtual Volumes), fornendo input architetturale e supporto iniziale per vVol e API VMware vSphere per la consapevolezza dello storage (VASA). Questo approccio non solo ha portato la gestione granulare dello storage delle macchine virtuali a VMFS, ma ha anche supportato l'automazione del provisioning dello storage tramite Storage Policy Based Management (SPBM).

SPBM fornisce un framework che funge da layer di astrazione tra i servizi di storage disponibili per l'ambiente di virtualizzazione e gli elementi di storage sottoposti a provisioning tramite policy. Questo approccio consente agli architetti dello storage di progettare pool di storage con diverse funzionalità che possono essere facilmente utilizzate dagli amministratori delle macchine virtuali. Gli amministratori possono quindi associare i requisiti di carico di lavoro delle macchine virtuali ai pool di storage con provisioning, consentendo un controllo granulare delle varie impostazioni a livello di macchina virtuale o disco virtuale.

ONTAP è leader nel settore dello storage in termini di scalabilità vVol, supportando centinaia di migliaia di vVol in un singolo cluster, mentre i vendor di array Enterprise e flash array più piccoli supportano solo diverse migliaia di vVol per array. NetApp sta inoltre guidando l'evoluzione della gestione granulare delle macchine virtuali con funzionalità imminenti a supporto di vVol 3.0.

Per ulteriori informazioni su VMware vSphere Virtual Volumes, SPBM e ONTAP, vedere "TR-4400: Volumi virtuali VMware vSphere con ONTAP".

## Datastore e protocolli

#### Panoramica delle funzionalità del datastore e del protocollo di vSphere

Per collegare VMware vSphere a datastore su un sistema con software ONTAP vengono utilizzati sette protocolli:

- FCP
- FCoE
- NVMe/FC
- NVMe/TCP
- ISCSI
- NFS v3
- NFS v4,1

FCP, FCoE, NVMe/FC, NVMe/TCP e iSCSI sono protocolli a blocchi che utilizzano il file system della macchina virtuale vSphere per memorizzare le macchine virtuali all'interno di LUN ONTAP o spazi dei nomi NVMe contenuti in un volume ONTAP FlexVol. A partire da vSphere 7.0, VMware non supporta più il software FCoE negli ambienti di produzione. NFS è un protocollo di file che inserisce le macchine virtuali in datastore (che sono semplicemente volumi ONTAP) senza la necessità di VMFS. SMB (CIFS), iSCSI, NVMe/TCP o NFS possono essere utilizzati anche direttamente da un sistema operativo guest a ONTAP.

Le tabelle seguenti presentano le funzionalità tradizionali del datastore supportate da vSphere con ONTAP. Queste informazioni non si applicano agli archivi dati vVol, ma in genere si applicano a vSphere 6.x e alle versioni successive che utilizzano le versioni supportate di ONTAP. È inoltre possibile consultare "Valori massimi di configurazione VMware" Per release specifiche di vSphere per confermare limiti specifici.

| Funzionalità | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| Formato | VMFS o RDM (raw device mapping) | VMFS o RDM | VMFS | N/A. |
| Numero massimo di datastore o LUN | 1024 LUN per host | 1024 LUN per server | 256 namespeces per server | 256 supporti Default NFS (NFS predefinito). MaxVolumes è 8. Utilizza i tool ONTAP per VMware vSphere per aumentare fino a 256. |
| Dimensione massima datastore | 64 TB | 64 TB | 64 TB | 100 TB di volume FlexVol o superiore con volume FlexGroup |
| Dimensione massima del file del datastore | 62 TB | 62 TB | 62 TB | 62TB con ONTAP 9.12.1P2 e versioni successive |
| Profondità ottimale della coda per LUN o file system | 64-256 | 64-256 | Negoziazione automatica | Fare riferimento a NFS.MaxQueueDefe lse in "Host ESXi consigliato e altre impostazioni ONTAP". |

La seguente tabella elenca le funzionalità supportate relative allo storage VMware.

| Capacità/funzionali tà | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| VMotion | Sì | Sì | Sì | Sì |
| Storage vMotion | Sì | Sì | Sì | Sì |
| VMware ha | Sì | Sì | Sì | Sì |
| SDR (Storage Distributed Resource Scheduler) | Sì | Sì | Sì | Sì |

| Capacità/funzionalità | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| Software di backup abilitato VADP (VMware vStorage API for Data Protection) | Sì | Sì | Sì | Sì |
| Microsoft Cluster Service (MSCS) o clustering di failover all'interno di una macchina virtuale | Sì | Sì* | Sì* | Non supportato |
| Tolleranza agli errori | Sì | Sì | Sì | Sì |
| Site Recovery Manager | Sì | Sì | No** | Solo V3** |
| Macchine virtuali con thin provisioning (dischi virtuali) | Sì | Sì | Sì | Sì<br>Si tratta dell'impostazione predefinita per tutte le macchine virtuali su NFS quando non si utilizza VAAI. |
| Multipathing nativo di VMware | Sì | Sì | Sì, utilizzando il nuovo plug-in ad alte prestazioni (HPP) | Il trunking di sessione NFS v4,1 richiede ONTAP 9.14.1 e versioni successive |

La tabella seguente elenca le funzionalità di gestione dello storage ONTAP supportate.

| Funzionalità | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| Deduplica dei dati | Risparmi nell'array | Risparmi nell'array | Risparmi nell'array | Risparmi nel datastore |
| Thin provisioning | Datastore o RDM | Datastore o RDM | Datastore | Datastore |
| Ridimensiona datastore | Crescere solo | Crescere solo | Crescere solo | Crescita, crescita automatica e riduzione |
| Plug-in SnapCenter per applicazioni Windows e Linux (in guest) | Sì | Sì | No | Sì |
| Monitoraggio e configurazione dell'host con gli strumenti ONTAP per VMware vSphere | Sì | Sì | No | Sì |

| Funzionalità | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| Provisioning con gli strumenti ONTAP per VMware vSphere | Sì | Sì | No | Sì |

La tabella seguente elenca le funzionalità di backup supportate.

| Funzionalità | FC/FCoE | ISCSI | NVMe-of | NFS |
|---|---|---|---|---|
| Istantanee di ONTAP | Sì | Sì | Sì | Sì |
| SRM supportato da backup replicati | Sì | Sì | No** | Solo V3** |
| Volume SnapMirror | Sì | Sì | Sì | Sì |
| Accesso all'immagine VMDK | Software di backup abilitato per VADP | Software di backup abilitato per VADP | Software di backup abilitato per VADP | Software di backup abilitato VADP, vSphere Client e il browser datastore di vSphere Web Client |
| Accesso a livello di file VMDK | Software di backup abilitato VADP, solo Windows | Software di backup abilitato VADP, solo Windows | Software di backup abilitato VADP, solo Windows | Software di backup abilitato VADP e applicazioni di terze parti |
| Granularità NDMP | Datastore | Datastore | Datastore | Datastore o macchina virtuale |

*NetApp consiglia di utilizzare iSCSI in-guest per cluster Microsoft piuttosto che VMDK abilitati per il multi-writer in un datastore VMFS. Questo approccio è completamente supportato da Microsoft e VMware, offre grande flessibilità con ONTAP (SnapMirror per sistemi ONTAP on-premise o nel cloud), è facile da configurare e automatizzare e può essere protetto con SnapCenter. VSphere 7 aggiunge una nuova opzione VMDK in cluster. Si tratta di un'operazione diversa dai VMDK abilitati per il multi-writer, che richiede un datastore presentato tramite il protocollo FC che ha attivato il supporto VMDK in cluster. Sono previste altre restrizioni. Vedere VMware "Configurazione per il clustering di failover di Windows Server" documentazione per le linee guida di configurazione.

**I datastore che utilizzano NVMe-of e NFS v4.1 richiedono la replica vSphere. La replica basata su array non è supportata da SRM.

#### Selezione di un protocollo di storage

I sistemi che eseguono il software ONTAP supportano tutti i principali protocolli di storage, in modo che i clienti possano scegliere ciò che meglio si adatta al proprio ambiente, a seconda dell'infrastruttura di rete esistente e pianificata e delle competenze dello staff. I test di NetApp hanno generalmente mostrato poca differenza tra i protocolli eseguiti a velocità di linea simili, pertanto è meglio concentrarsi sull'infrastruttura di rete e sulle funzionalità del personale rispetto alle performance del protocollo raw.

I seguenti fattori potrebbero essere utili per valutare una scelta di protocollo:

- **Ambiente attuale del cliente.** sebbene i team IT siano generalmente esperti nella gestione dell'infrastruttura IP Ethernet, non tutti sono esperti nella gestione di un fabric SAN FC. Tuttavia, l'utilizzo di

una rete IP generica non progettata per il traffico di storage potrebbe non funzionare bene. Prendi in considerazione l'infrastruttura di rete in uso, gli eventuali miglioramenti pianificati e le competenze e la disponibilità del personale per gestirli.

- **Facilità di configurazione.** oltre alla configurazione iniziale del fabric FC (switch e cablaggio aggiuntivi, zoning e verifica dell'interoperabilità di HBA e firmware), i protocolli a blocchi richiedono anche la creazione e la mappatura di LUN e il rilevamento e la formattazione da parte del sistema operativo guest. Una volta creati ed esportati, i volumi NFS vengono montati dall'host ESXi e pronti all'uso. NFS non dispone di specifiche qualifiche hardware o firmware da gestire.
- **Facilità di gestione.** con i protocolli SAN, se è necessario più spazio, sono necessari diversi passaggi, tra cui la crescita di un LUN, la ricerca di nuove dimensioni e la crescita del file system). Sebbene sia possibile aumentare un LUN, non è possibile ridurre le dimensioni di un LUN e il ripristino dello spazio inutilizzato può richiedere ulteriore impegno. NFS consente un facile dimensionamento in alto o in basso e questo ridimensionamento può essere automatizzato dal sistema storage. LA SAN offre la bonifica dello spazio attraverso i comandi TRIM/UNMAP del sistema operativo guest, consentendo di restituire spazio dai file cancellati all'array. Questo tipo di recupero dello spazio è più difficile con gli archivi dati NFS.
- **Trasparenza dello spazio di storage.** l'utilizzo dello storage è in genere più semplice da visualizzare negli ambienti NFS perché il thin provisioning restituisce immediatamente risparmi. Allo stesso modo, i risparmi di deduplica e clonazione sono immediatamente disponibili per altre macchine virtuali nello stesso datastore o per altri volumi di sistemi storage. La densità delle macchine virtuali è in genere maggiore anche in un datastore NFS, che può migliorare i risparmi della deduplica e ridurre i costi di gestione grazie a un numero inferiore di datastore da gestire.

#### Layout del datastore

I sistemi storage ONTAP offrono una grande flessibilità nella creazione di datastore per macchine virtuali e dischi virtuali. Sebbene vengano applicate molte Best practice ONTAP quando si utilizza VSC per il provisioning dei datastore per vSphere (elencate nella sezione "Host ESXi consigliato e altre impostazioni ONTAP"), ecco alcune linee guida aggiuntive da prendere in considerazione:

- L'implementazione di vSphere con datastore NFS di ONTAP offre un'implementazione facile da gestire e dalle performance elevate che offre rapporti VM-datastore che non possono essere ottenuti con protocolli di storage basati su blocchi. Questa architettura può comportare un aumento di dieci volte della densità degli archivi dati con una conseguente riduzione del numero di archivi dati. Anche se un datastore più grande può trarre beneficio dall'efficienza dello storage e offrire vantaggi operativi, è consigliabile utilizzare almeno quattro datastore (volumi FlexVol) per memorizzare le macchine virtuali su un singolo controller ONTAP per ottenere le massime prestazioni dalle risorse hardware. Questo approccio consente inoltre di stabilire datastore con policy di recovery diverse. Alcuni possono essere sottoposti a backup o replicati più frequentemente rispetto ad altri in base alle esigenze aziendali. I volumi FlexGroup non richiedono più datastore per le performance, in quanto sono scalabili in base alla progettazione.
- NetApp consiglia di utilizzare i volumi FlexVol per la maggior parte dei datastore NFS. A partire da ONTAP 9,8, l'utilizzo dei volumi FlexGroup è supportato anche come datastore e generalmente è consigliato per alcuni casi d'utilizzo. Gli altri container di storage ONTAP, come i qtree, non sono generalmente consigliati, in quanto al momento non sono supportati dai tool ONTAP per VMware vSphere o dal plug-in NetApp SnapCenter per VMware vSphere. Ciò detto, implementare datastore come qtree multiple in un singolo volume potrebbe essere utile per ambienti altamente automatizzati, che possono trarre beneficio da quote a livello di datastore o cloni dei file delle macchine virtuali.
- Una buona dimensione per un datastore di volumi FlexVol è di circa 4TB - 8TB. Queste dimensioni rappresentano un buon punto di equilibrio per le performance, la facilità di gestione e la protezione dei dati. Inizia in piccolo (ad esempio, 4 TB) e fai crescere il datastore in base alle necessità (fino a un massimo di 100 TB). I datastore più piccoli sono più veloci da ripristinare dal backup o dopo un disastro e possono essere spostati rapidamente nel cluster. Prendere in considerazione l'utilizzo della funzione di dimensionamento automatico di ONTAP per aumentare e ridurre automaticamente il volume in base alle

modifiche dello spazio utilizzato. Per impostazione predefinita, i tool ONTAP per il provisioning guidato degli archivi dati VMware vSphere utilizzano la dimensione automatica per i nuovi archivi dati. È possibile personalizzare ulteriormente le soglie di aumento e riduzione e le dimensioni massime e minime con System Manager o la riga di comando.

- In alternativa, gli archivi dati VMFS possono essere configurati con LUN accessibili da FC, iSCSI o FCoE. VMFS consente l'accesso simultaneo alle LUN tradizionali da parte di ogni server ESX in un cluster. Gli archivi di dati VMFS possono avere dimensioni fino a 64 TB e sono costituiti da un massimo di 32 LUN da 2 TB (VMFS 3) o un singolo LUN da 64 TB (VMFS 5). La dimensione massima del LUN ONTAP è 16 TB sulla maggior parte dei sistemi e 128 TB sui sistemi all-SAN-array. Pertanto, è possibile creare un datastore VMFS 5 di dimensioni massime sulla maggior parte dei sistemi ONTAP utilizzando quattro LUN da 16 TB. Sebbene i carichi di lavoro con i/o elevati possano offrire un vantaggio in termini di performance con più LUN (con sistemi FAS o AFF high-end), questo vantaggio è compensato dalla complessità di gestione aggiunta per creare, gestire e proteggere le LUN degli archivi dati e dall'aumento del rischio di disponibilità. In genere, NetApp consiglia di utilizzare un singolo LUN di grandi dimensioni per ciascun datastore e solo se è necessario andare oltre un datastore da 16 TB. Come per NFS, puoi utilizzare più datastore (volumi) per massimizzare le performance su un singolo controller ONTAP.
- I sistemi operativi guest precedenti necessitavano di un allineamento con il sistema storage per ottenere le migliori performance ed efficienza dello storage. Tuttavia, i moderni sistemi operativi supportati dai vendor dei distributori Microsoft e Linux come Red Hat non richiedono più modifiche per allineare la partizione del file system con i blocchi del sistema storage sottostante in un ambiente virtuale. Se si utilizza un sistema operativo precedente che potrebbe richiedere l'allineamento, cercare gli articoli nella Knowledge base del supporto NetApp utilizzando "allineamento delle macchine virtuali" o richiedere una copia di TR-3747 a un contatto commerciale o partner di NetApp.
- Evitare l'uso di utilità di deframmentazione all'interno del sistema operativo guest, poiché ciò non offre vantaggi in termini di prestazioni e influisce sull'efficienza dello storage e sull'utilizzo dello spazio snapshot. È inoltre consigliabile disattivare l'indicizzazione della ricerca nel sistema operativo guest per i desktop virtuali.
- ONTAP ha guidato il settore con innovative funzionalità di efficienza dello storage, che ti consentono di sfruttare al massimo lo spazio su disco utilizzabile. I sistemi AFF aumentano ulteriormente questa efficienza con la deduplica e la compressione inline predefinite. I dati vengono deduplicati in tutti i volumi in un aggregato, quindi non è più necessario raggruppare sistemi operativi simili e applicazioni simili in un singolo datastore per massimizzare i risparmi.
- In alcuni casi, potrebbe non essere necessario un datastore. Per ottenere performance e gestibilità ottimali, evitare di utilizzare un datastore per applicazioni con i/o elevato, come database e alcune applicazioni. Si consiglia invece di prendere in considerazione file system di proprietà degli ospiti, come NFS o iSCSI, gestiti dal guest o con RDM. Per indicazioni specifiche sulle applicazioni, consulta i report tecnici NetApp relativi alla tua applicazione. Ad esempio, "Database Oracle su ONTAP" contiene una sezione sulla virtualizzazione con informazioni utili.
- I dischi di prima classe (o dischi virtuali migliorati) consentono dischi gestiti da vCenter indipendenti da una macchina virtuale con vSphere 6.5 e versioni successive. Anche se gestiti principalmente da API, possono essere utili con vVol, soprattutto se gestiti da OpenStack o Kubernetes tools. Sono supportati da ONTAP e dai tool ONTAP per VMware vSphere.

#### Migrazione di datastore e macchine virtuali

Quando si esegue la migrazione delle macchine virtuali da un datastore esistente su un altro sistema storage a ONTAP, è necessario tenere presente alcune procedure:

- Utilizzare Storage vMotion per spostare la maggior parte delle macchine virtuali su ONTAP. Questo approccio non solo non è disgregativo per l'esecuzione di macchine virtuali, ma consente anche funzionalità di efficienza dello storage ONTAP come la deduplica inline e la compressione per elaborare i dati durante la migrazione. Prendere in considerazione l'utilizzo delle funzionalità di vCenter per

selezionare più macchine virtuali dall'elenco di inventario e quindi pianificare la migrazione (utilizzare il tasto Ctrl mentre si fa clic su azioni) in un momento appropriato.

- Sebbene sia possibile pianificare con attenzione una migrazione verso datastore di destinazione appropriati, spesso è più semplice eseguire la migrazione in blocco e poi organizzarla in un secondo momento. Potresti voler utilizzare questo approccio per guidare la migrazione verso datastore diversi, se hai esigenze specifiche di data Protection, come ad esempio diverse pianificazioni Snapshot.
- La maggior parte delle macchine virtuali e del relativo storage può essere migrata durante l'esecuzione (a caldo), ma la migrazione dello storage collegato (non nel datastore) come gli ISO, i LUN o i volumi NFS da un altro sistema storage potrebbe richiedere la migrazione a freddo.
- Le macchine virtuali che richiedono una migrazione più accurata includono database e applicazioni che utilizzano lo storage collegato. In generale, considerare l'utilizzo degli strumenti dell'applicazione per gestire la migrazione. Per Oracle, prendere in considerazione l'utilizzo di strumenti Oracle come RMAN o ASM per migrare i file di database. Vedere "TR-4534" per ulteriori informazioni. Allo stesso modo, per SQL Server, prendere in considerazione l'utilizzo di SQL Server Management Studio o di strumenti NetApp come SnapManager per SQL Server o SnapCenter.

#### Strumenti ONTAP per VMware vSphere

La Best practice più importante per l'utilizzo di vSphere con i sistemi che eseguono il software ONTAP consiste nell'installare e utilizzare i tool ONTAP per il plug-in di VMware vSphere (precedentemente noto come console di storage virtuale). Questo plug-in vCenter semplifica la gestione dello storage, migliora la disponibilità e riduce i costi di storage e l'overhead operativo, sia che si utilizzi SAN che NAS. Utilizza le Best practice per il provisioning degli archivi di dati e ottimizza le impostazioni degli host ESXi per i timeout multipath e HBA (descritti nell'Appendice B). Poiché si tratta di un plug-in vCenter, è disponibile per tutti i client web vSphere che si connettono al server vCenter.

Il plug-in consente inoltre di utilizzare altri strumenti ONTAP in ambienti vSphere. Il prodotto consente di installare il plug-in NFS per VMware VAAI, che consente l'offload delle copie in ONTAP per le operazioni di cloning delle macchine virtuali, lo space reservation per i file di dischi virtuali con thick provisioning e l'offload delle snapshot ONTAP.

Il plug-in è anche l'interfaccia di gestione per molte funzioni del provider VASA per ONTAP, supportando la gestione basata su policy di storage con vVol. Una volta registrati i tool ONTAP per VMware vSphere, utilizzali per creare profili di capacità storage, mapparli allo storage e garantire la conformità dei datastore con i profili nel tempo. Il provider VASA fornisce anche un'interfaccia per creare e gestire datastore vVol.

In generale, NetApp consiglia di utilizzare i tool ONTAP per l'interfaccia di VMware vSphere all'interno di vCenter per eseguire il provisioning di datastore tradizionali e vVol per garantire il rispetto delle Best practice.

#### Rete generale

La configurazione delle impostazioni di rete quando si utilizza vSphere con sistemi che eseguono il software ONTAP è semplice e simile ad altre configurazioni di rete. Ecco alcuni aspetti da considerare:

- Separare il traffico di rete dello storage dalle altre reti. È possibile ottenere una rete separata utilizzando una VLAN dedicata o switch separati per lo storage. Se la rete di storage condivide percorsi fisici come gli uplink, potrebbe essere necessario QoS o porte di uplink aggiuntive per garantire una larghezza di banda sufficiente. Non connettere gli host direttamente allo storage; utilizzare gli switch per disporre di percorsi ridondanti e consentire a VMware ha di funzionare senza alcun intervento. Vedere "Connessione di rete diretta" per ulteriori informazioni.
- I frame jumbo possono essere utilizzati se lo si desidera e supportati dalla rete, in particolare quando si utilizza iSCSI. Se vengono utilizzati, assicurarsi che siano configurati in modo identico su tutti i dispositivi di rete, VLAN e così via nel percorso tra lo storage e l'host ESXi. In caso contrario, potrebbero verificarsi

problemi di connessione o di prestazioni. La MTU deve essere impostata in modo identico anche sullo switch virtuale ESXi, sulla porta VMkernel e anche sulle porte fisiche o sui gruppi di interfacce di ciascun nodo ONTAP.

- NetApp consiglia di disattivare il controllo del flusso di rete solo sulle porte di rete del cluster all'interno di un cluster ONTAP. NetApp non fornisce altri consigli sulle Best practice per le restanti porte di rete utilizzate per il traffico dati. Attivare o disattivare secondo necessità. Vedere "TR-4182" per ulteriori informazioni sul controllo di flusso.
- Quando gli array di storage ESXi e ONTAP sono collegati a reti di storage Ethernet, NetApp consiglia di configurare le porte Ethernet a cui questi sistemi si connettono come porte edge RSTP (Rapid Spanning Tree Protocol) o utilizzando la funzione PortFast di Cisco. NetApp consiglia di abilitare la funzione di trunk PortFast Spanning-Tree in ambienti che utilizzano la funzionalità Cisco PortFast e che dispongono di un trunking VLAN 802.1Q abilitato per il server ESXi o gli array di storage ONTAP.
- NetApp consiglia le seguenti Best practice per l'aggregazione dei collegamenti:
  - Utilizzare switch che supportano l'aggregazione di collegamenti di porte su due chassis switch separati utilizzando un approccio a gruppi di aggregazione di collegamenti multi-chassis, ad esempio Virtual PortChannel (VPC) di Cisco.
  - Disattivare LACP per le porte dello switch connesse a ESXi, a meno che non si utilizzi dvSwitch 5.1 o versioni successive con LACP configurato.
  - Utilizza LACP per creare aggregati di link per sistemi di storage ONTAP con gruppi di interfacce dinamiche multimode con hash porta o IP. Fare riferimento a. "Gestione della rete" per ulteriori indicazioni.
  - Utilizzare un criterio di raggruppamento hash IP su ESXi quando si utilizza l'aggregazione di collegamenti statici (ad esempio, EtherChannel) e vSwitch standard o l'aggregazione di collegamenti basata su LACP con gli switch distribuiti vSphere. Se non si utilizza l'aggregazione dei collegamenti, utilizzare invece "Route based on the origining virtual port ID" (percorso basato sull'ID della porta virtuale di origine).

La seguente tabella fornisce un riepilogo degli elementi di configurazione di rete e indica la posizione in cui vengono applicate le impostazioni.

| Elemento | ESXi | Switch | Nodo | SVM |
|---|---|---|---|---|
| Indirizzo IP | VMkernel | No** | No** | Sì |
| Aggregazione dei collegamenti | Switch virtuale | Sì | Sì | No* |
| VLAN | Gruppi di porte VMkernel e VM | Sì | Sì | No* |
| Controllo di flusso | NIC | Sì | Sì | No* |
| Spanning tree | No | Sì | No | No |
| MTU (per frame jumbo) | Switch virtuale e porta VMkernel (9000) | Sì (impostato su max) | Sì (9000) | No* |
| Gruppi di failover | No | No | Sì (creare) | Sì (selezionare) |

*Le LIF SVM si connettono a porte, gruppi di interfacce o interfacce VLAN con VLAN, MTU e altre impostazioni. Tuttavia, le impostazioni non vengono gestite a livello di SVM.

**Questi dispositivi dispongono di indirizzi IP propri per la gestione, ma non vengono utilizzati nel contesto

dello storage di rete ESXi.

**SAN (FC, FCoE, NVMe/FC, iSCSI), RDM**

NetApp ONTAP offre storage a blocchi di livello Enterprise per VMware vSphere utilizzando iSCSI, Fibre Channel Protocol (FCP o FC in breve) e NVMe over Fabrics (NVMe-of). Di seguito sono riportate le Best practice per l'implementazione dei protocolli a blocchi per lo storage delle macchine virtuali con vSphere e ONTAP.

In vSphere, esistono tre modi per utilizzare le LUN dello storage a blocchi:

- Con datastore VMFS
- Con RDM (raw device mapping)
- Come LUN accessibile e controllato da un iniziatore software da un sistema operativo guest VM

VMFS è un file system in cluster dalle performance elevate che fornisce datastore che sono pool di storage condivisi. Gli archivi dati VMFS possono essere configurati con LUN accessibili tramite FC, iSCSI, FCoE o namespace NVMe accessibili tramite i protocolli NVMe/FC o NVMe/TCP. VMFS consente l'accesso simultaneo allo storage da parte di ogni server ESX in un cluster. Le dimensioni massime del LUN sono generalmente di 128TB GB a partire da ONTAP 9.12.1P2 (e versioni precedenti con i sistemi ASA); pertanto, è possibile creare un datastore VMFS 5 o 6 di 64TB GB di dimensioni massime utilizzando un singolo LUN.

VSphere include il supporto integrato per più percorsi verso i dispositivi storage, definito NMP (Native Multipathing). NMP è in grado di rilevare il tipo di storage per i sistemi storage supportati e di configurare automaticamente lo stack NMP per supportare le funzionalità del sistema storage in uso.

Sia NMP che ONTAP supportano l'ALUA (Asymmetric Logical Unit Access) per negoziare percorsi ottimizzati e non ottimizzati. In ONTAP, un percorso ottimizzato per ALUA segue un percorso di dati diretto, utilizzando una porta di destinazione sul nodo che ospita il LUN a cui si accede. ALUA è attivato per impostazione predefinita sia in vSphere che in ONTAP. NMP riconosce il cluster ONTAP come ALUA e utilizza il plug-in del tipo di array di storage ALUA (`VMW_SATP_ALUA`) e seleziona il plug-in di selezione del percorso round robin ( `VMW_PSP_RR`).

ESXi 6 supporta fino a 256 LUN e fino a 1,024 percorsi totali verso LUN. ESXi non vede LUN o percorsi oltre questi limiti. Supponendo il numero massimo di LUN, il limite di percorso consente quattro percorsi per LUN. In un cluster ONTAP più grande, è possibile raggiungere il limite di percorso prima del limite di LUN. Per risolvere questo limite, ONTAP supporta la mappa LUN selettiva (SLM) nella versione 8.3 e successive.

SLM limita i nodi che pubblicizzano i percorsi a una determinata LUN. È una Best practice di NetApp avere almeno una LIF per nodo per SVM e utilizzare SLM per limitare i percorsi pubblicizzati al nodo che ospita la LUN e il suo partner ha. Sebbene esistano altri percorsi, essi non vengono pubblicizzati per impostazione predefinita. È possibile modificare i percorsi pubblicizzati con gli argomenti del nodo di reporting add e remove all'interno di SLM. Tenere presente che le LUN create nelle release precedenti alla 8.3 pubblicizzano tutti i percorsi e devono essere modificate solo per pubblicizzare i percorsi alla coppia ha di hosting. Per ulteriori informazioni su SLM, vedere la sezione 5.9 di "TR-4080". Il precedente metodo di portset può essere utilizzato anche per ridurre ulteriormente i percorsi disponibili per un LUN. I portset aiutano a ridurre il numero di percorsi visibili attraverso i quali gli iniziatori in un igroup possono vedere le LUN.

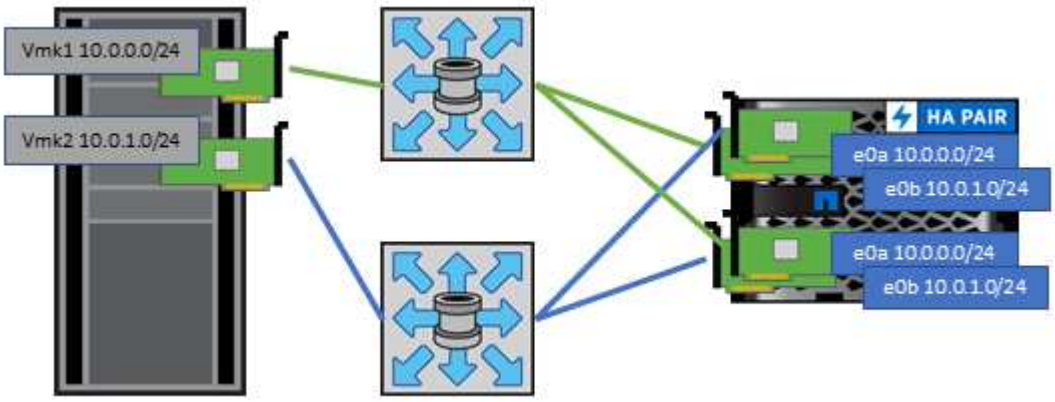
- SLM è attivato per impostazione predefinita. A meno che non si utilizzino portset, non è necessaria alcuna configurazione aggiuntiva.
- Per i LUN creati prima di Data ONTAP 8.3, applicare manualmente SLM eseguendo `lun mapping remove-reporting-nodes` Comando per rimuovere i nodi di reporting del LUN e limitare l'accesso del

LUN al nodo proprietario del LUN e al partner ha.

I protocolli a blocchi (iSCSI, FC e FCoE) accedono alle LUN utilizzando ID LUN e numeri di serie, insieme a nomi univoci. FC e FCoE utilizzano nomi in tutto il mondo (WWNN e WWPN), mentre iSCSI utilizza nomi iSCSI qualificati (IQN). Il percorso delle LUN all'interno dello storage è privo di significato per i protocolli a blocchi e non viene presentato in alcun punto del protocollo. Pertanto, un volume che contiene solo LUN non deve essere montato internamente e non è necessario un percorso di giunzione per i volumi che contengono LUN utilizzati negli archivi dati. Il sottosistema NVMe in ONTAP funziona in modo simile.

Altre Best practice da prendere in considerazione:

- Assicurarsi che venga creata un'interfaccia logica (LIF) per ogni SVM su ciascun nodo del cluster ONTAP per garantire la massima disponibilità e mobilità. La Best practice PER LE SAN ONTAP consiste nell'utilizzare due porte fisiche e LIF per nodo, una per ciascun fabric. ALUA viene utilizzato per analizzare i percorsi e identificare i percorsi attivi ottimizzati (diretti) rispetto ai percorsi attivi non ottimizzati. ALUA viene utilizzato per FC, FCoE e iSCSI.
- Per le reti iSCSI, utilizzare più interfacce di rete VMkernel su diverse subnet di rete con raggruppamento NIC quando sono presenti più switch virtuali. È inoltre possibile utilizzare più NIC fisiche collegate a più switch fisici per fornire ha e un throughput maggiore. La figura seguente mostra un esempio di connettività multipath. In ONTAP, configurare un gruppo di interfacce single-mode per il failover con due o più collegamenti connessi a due o più switch oppure utilizzare LACP o un'altra tecnologia di aggregazione dei collegamenti con gruppi di interfacce multimodali per fornire ha e i vantaggi dell'aggregazione dei collegamenti.
- Se il protocollo CHAP (Challenge-Handshake Authentication Protocol) viene utilizzato in ESXi per l'autenticazione di destinazione, deve essere configurato anche in ONTAP utilizzando la CLI (`vserver iscsi security create`) O con System Manager (modificare Initiator Security in Storage > SVM > SVM Settings > Protocols > iSCSI).
- Utilizza i tool ONTAP per VMware vSphere per creare e gestire LUN e igroups. Il plug-in determina automaticamente le WWPN dei server e crea gli igroups appropriati. Inoltre, configura i LUN in base alle Best practice e li associa agli igroups corretti.
- Utilizzare con cautela gli RDM poiché possono essere più difficili da gestire e utilizzano anche percorsi limitati come descritto in precedenza. I LUN ONTAP supportano entrambi "modalità di compatibilità fisica e virtuale" RDM.
- Per ulteriori informazioni sull'utilizzo di NVMe/FC con vSphere 7.0, consulta questo articolo "Guida alla configurazione degli host NVMe/FC di ONTAP" e. "TR-4684"La figura seguente mostra la connettività multipath da un host vSphere a un LUN ONTAP.



### NFS

NetApp ONTAP è, tra l'altro, un array NAS scale-out di livello Enterprise. ONTAP consente a VMware vSphere di accedere contemporaneamente agli archivi dati connessi a NFS da numerosi host ESXi, superando di gran lunga i limiti imposti ai file system VMFS. L'utilizzo di NFS con vSphere offre alcuni benefici in termini di facilità di utilizzo e di visibilità dell'efficienza dello storage, come menzionato nella "datastore" sezione.

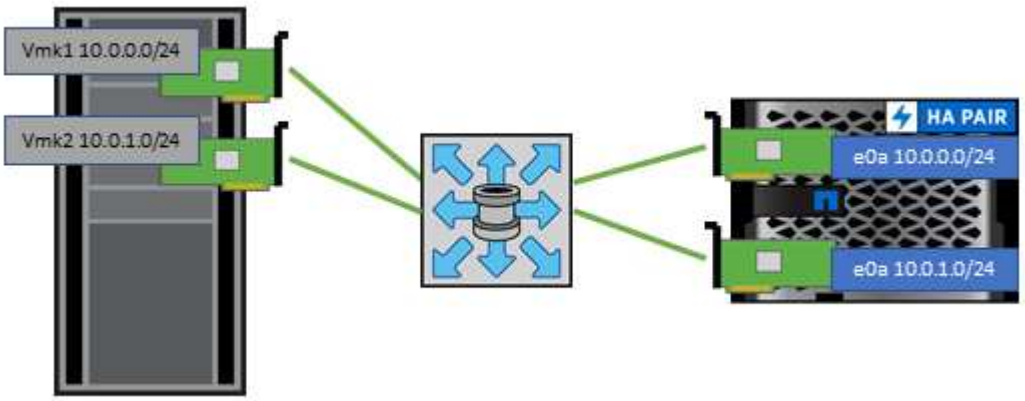
Quando si utilizza ONTAP NFS con vSphere, si consiglia di seguire le seguenti Best practice:

- Utilizzare una singola interfaccia logica (LIF) per ogni SVM su ciascun nodo del cluster ONTAP. Le raccomandazioni precedenti di un LIF per datastore non sono più necessarie. Benché l'accesso diretto (LIF e datastore sullo stesso nodo) sia migliore, non preoccuparti dell'accesso indiretto perché l'effetto sulle performance è generalmente minimo (microsecondi).
- VMware supporta NFSv3 da VMware Infrastructure 3. VSphere 6.0 ha aggiunto il supporto per NFSv4.1, che abilita alcune funzionalità avanzate come la sicurezza Kerberos. Dove NFSv3 utilizza il blocco lato client, NFSv4.1 utilizza il blocco lato server. Anche se un volume ONTAP può essere esportato attraverso entrambi i protocolli, ESXi può essere montato solo attraverso un protocollo. Questo montaggio di protocollo singolo non impedisce ad altri host ESXi di montare lo stesso datastore attraverso una versione diversa. Assicurarsi di specificare la versione del protocollo da utilizzare durante il montaggio in modo che tutti gli host utilizzino la stessa versione e, di conseguenza, lo stesso stile di blocco. Non mischiare versioni NFS tra gli host. Se possibile, utilizzare i profili host per verificare la conformità.
  - Poiché non esiste alcuna conversione automatica del datastore tra NFSv3 e NFSv4.1, creare un nuovo datastore NFSv4.1 e utilizzare Storage vMotion per migrare le macchine virtuali nel nuovo datastore.
  - Fare riferimento alle note della tabella di interoperabilità NFS v4.1 nella "Tool NetApp Interoperability Matrix" Per i livelli di patch ESXi specifici richiesti per il supporto.
  - VMware supporta nconnect con NFSv3 a partire da vSphere 8.0U2. Ulteriori informazioni su nconnect sono disponibili sul sito "Funzione NFSv3 nConnect con NetApp e VMware"
- Le policy di esportazione NFS vengono utilizzate per controllare l'accesso da parte degli host vSphere. È possibile utilizzare un criterio con più volumi (datastore). Con NFSv3, ESXi utilizza lo stile di sicurezza sys (UNIX) e richiede l'opzione di montaggio root per eseguire le macchine virtuali. In ONTAP, questa opzione viene definita superutente e, quando viene utilizzata l'opzione superutente, non è necessario specificare l'ID utente anonimo. Tenere presente che le regole dei criteri di esportazione con valori diversi per `-anon` e. `-allow-suid` Può causare problemi di rilevamento SVM con gli strumenti ONTAP. Ecco un esempio di politica:
  - Access Protocol: nfs (che include sia nfs3 che nfs4)
  - Specifiche di corrispondenza del client: 192.168.42.21
  - Regola di accesso RO: SIS
  - RW Access Rule (regola di accesso RW): SIS
  - UID anonimo
  - Superutente: SIS
- Se si utilizza il plug-in NetApp NFS per VMware VAAI, il protocollo deve essere impostato su `nfs` invece di `nfs3` quando viene creata o modificata la regola dei criteri di esportazione. La funzionalità di offload delle oopie di VAAI richiede il protocollo NFSv4 per funzionare, anche se il protocollo dati è NFSv3. Specificando il protocollo come `nfs` Include entrambe le versioni NFSv3 e NFSv4.
- I volumi del datastore NFS vengono svincoli dal volume root di SVM; pertanto, ESXi deve anche avere accesso al volume root per navigare e montare i volumi del datastore. La policy di esportazione per il

volume root e per qualsiasi altro volume in cui la giunzione del volume del datastore è nidificata deve includere una regola o regole per i server ESXi che concedono loro l'accesso in sola lettura. Ecco un esempio di policy per il volume root, utilizzando anche il plug-in VAAI:

  - Access Protocol: nfs (che include sia nfs3 che nfs4)
  - Specifiche di corrispondenza del client: 192.168.42.21
  - Regola di accesso RO: SIS
  - RW Access Rule: Never (miglior sicurezza per il volume root)
  - UID anonimo
  - Superutente: SYS (richiesto anche per il volume root con VAAI)

- Utilizza i tool ONTAP per VMware vSphere (la Best practice più importante):
  - Utilizza i tool ONTAP per VMware vSphere per eseguire il provisioning degli archivi dati, poiché semplifica automaticamente la gestione delle policy di esportazione.
  - Quando si creano datastore per cluster VMware con il plug-in, selezionare il cluster anziché un singolo server ESX. Questa opzione attiva il montaggio automatico del datastore su tutti gli host del cluster.
  - Utilizzare la funzione di montaggio del plug-in per applicare i datastore esistenti ai nuovi server.
  - Quando non si utilizzano gli strumenti ONTAP per VMware vSphere, utilizzare una singola policy di esportazione per tutti i server o per ciascun cluster di server in cui è necessario un controllo aggiuntivo degli accessi.
- Sebbene ONTAP offra una struttura flessibile dello spazio dei nomi dei volumi per organizzare i volumi in un albero utilizzando le giunzioni, questo approccio non ha alcun valore per vSphere. Crea una directory per ogni VM nella directory principale dell'archivio dati, indipendentemente dalla gerarchia dello spazio dei nomi dello storage. Pertanto, la Best practice consiste nel montare semplicemente il percorso di giunzione per i volumi per vSphere nel volume root della SVM, che è il modo in cui i tool ONTAP per VMware vSphere prevedono il provisioning dei datastore. La mancanza di percorsi di giunzione nidificati significa anche che nessun volume dipende da un volume diverso dal volume root e che la sua eliminazione o la sua eliminazione, anche intenzionalmente, non influisce sul percorso verso altri volumi.
- Una dimensione del blocco di 4K è adatta per le partizioni NTFS negli archivi dati NFS. La figura seguente mostra la connettività da un host vSphere a un datastore NFS ONTAP.




La seguente tabella elenca le versioni di NFS e le funzionalità supportate.

| Funzionalità di vSphere | NFSv3 | NFSv4,1 |
|---|---|---|
| VMotion e Storage vMotion | Sì | Sì |

| Funzionalità di vSphere | NFSv3 | NFSv4,1 |
|---|---|---|
| Alta disponibilità | Sì | Sì |
| Tolleranza agli errori | Sì | Sì |
| DRS | Sì | Sì |
| Profili host | Sì | Sì |
| DRS dello storage | Sì | No |
| Controllo i/o dello storage | Sì | No |
| SRM | Sì | No |
| Volumi virtuali | Sì | No |
| Accelerazione hardware (VAAI) | Sì | Sì |
| Autenticazione Kerberos | No | Sì (ottimizzato con vSphere 6.5 e versioni successive per supportare AES, krb5i) |
| Supporto multipathing | No | Sì |

### Volumi FlexGroup

## Utilizza volumi ONTAP e FlexGroup con VMware vSphere per datastore semplici e scalabili che sfruttano tutta la potenza di un intero cluster ONTAP.

ONTAP 9,8, insieme ai tool ONTAP per VMware vSphere 9,8 e al plug-in SnapCenter per VMware 4,4, ha aggiunto il supporto per i datastore basati su volumi FlexGroup in vSphere. I volumi FlexGroup semplificano la creazione di datastore di grandi dimensioni e creano automaticamente i volumi costituenti distribuiti necessari nel cluster ONTAP, per ottenere le massime performance da un sistema ONTAP.

Scopri di più su FlexGroup Volumes in "Report tecnici sui volumi FlexCache e FlexGroup".

Utilizza i volumi FlexGroup con vSphere se desideri un singolo datastore vSphere scalabile con la potenza di un cluster ONTAP completo o se disponi di carichi di lavoro di cloning molto grandi che possono sfruttare il nuovo meccanismo di cloning di FlexGroup.

#### Offload delle copie

Oltre agli estesi test di sistema con i carichi di lavoro vSphere, ONTAP 9,8 ha aggiunto un nuovo meccanismo di offload delle copie per i datastore FlexGroup. Questo nuovo sistema utilizza un motore di copia migliorato per replicare i file tra i componenti in background consentendo l'accesso sia all'origine che alla destinazione. La cache locale viene quindi utilizzata per creare rapidamente istanze dei cloni delle macchine virtuali on-demand.

Per attivare l'offload delle copie ottimizzato per FlexGroup, fare riferimento alla sezione "Come configurare ONTAP FlexGroup per consentire l'offload delle copie VAAI"

Potresti accorgerti che se utilizzi il cloning VAAI, ma non quello per mantenere calda la cache, i cloni potrebbero non essere più veloci di una copia basata su host. In questo caso, è possibile regolare il timeout della cache per soddisfare meglio le proprie esigenze.

Considerare il seguente scenario:

- Hai creato un nuovo FlexGroup con 8 componenti
- Il timeout della cache per il nuovo FlexGroup è impostato su 160 minuti

In questo scenario, i primi 8 cloni da completare saranno copie complete, non cloni di file locali. Qualsiasi clonazione aggiuntiva di tale macchina virtuale prima della scadenza del timeout di 160 secondi utilizzerà il motore di clonazione file all'interno di ciascun componente in modo round-robin per creare copie quasi immediate distribuite uniformemente tra i volumi costituenti.

Ogni nuovo processo di clonazione che un volume riceve ripristina il timeout. Se un volume costituente nel FlexGroup di esempio non riceve una richiesta di clone prima del timeout, la cache di quella particolare VM verrà cancellata e il volume dovrà essere popolato di nuovo. Inoltre, se l'origine del clone originale cambia (ad esempio, è stato aggiornato il modello), la cache locale di ciascun componente verrà invalidata per evitare conflitti. Come indicato in precedenza, la cache può essere regolata in base alle esigenze dell'ambiente.

Per ulteriori informazioni sull'utilizzo di FlexGroup con VAAI, fare riferimento a questo articolo della KB: "VAAI: Come funziona il caching con i volumi FlexGroup?"

In ambienti in cui non è possibile sfruttare al meglio la cache FlexGroup, ma è comunque necessario un rapido cloning cross-volume, prendere in considerazione l'utilizzo di vVol. Il cloning tra volumi con vVol è molto più rapido rispetto ai datastore tradizionali, senza fare affidamento su una cache.

#### Impostazioni QoS

È supportata la configurazione della qualità del servizio a livello di FlexGroup utilizzando ONTAP System Manager o la shell del cluster, ma non fornisce consapevolezza delle macchine virtuali o integrazione di vCenter.

La qualità del servizio (IOPS max/min) può essere impostata su singole macchine virtuali o su tutte le macchine virtuali di un datastore in quel momento nell'interfaccia utente di vCenter o tramite API REST utilizzando i tool ONTAP. L'impostazione della QoS su tutte le macchine virtuali sostituisce le impostazioni separate per ogni macchina virtuale. Le impostazioni non si estendono alle macchine virtuali nuove o migrate in futuro; impostare la QoS sulle nuove macchine virtuali o riapplicare la QoS a tutte le macchine virtuali nel datastore.

Si noti che VMware vSphere considera tutti i/o di un datastore NFS come una singola coda per host e la limitazione della QoS su una VM può influire sulle performance per altre VM nello stesso datastore. Questo contrasta con i vVol, che possono mantenere le proprie impostazioni di policy di QoS se migrano in un altro datastore e non influiscono sull'io di altre macchine virtuali quando rallentano.

#### Metriche

ONTAP 9,8 ha inoltre aggiunto nuove metriche di performance basate su file (IOPS, throughput e latenza) per i file FlexGroup, che possono essere visualizzate nei tool ONTAP per la dashboard e i report delle macchine virtuali di VMware vSphere. Il plug-in ONTAP Tools per VMware vSphere consente inoltre di impostare le regole di qualità del servizio (QoS) utilizzando una combinazione di IOPS massimo e/o minimo. Questi possono essere impostati su tutte le macchine virtuali in un datastore o singolarmente per macchine virtuali specifiche.

#### Best practice

- Utilizza i tool ONTAP per creare datastore FlexGroup, per assicurarti che FlexGroup venga creato in modo ottimale e che le policy di esportazione siano configurate in modo da corrispondere al tuo ambiente vSphere. Tuttavia, dopo aver creato il volume FlexGroup con i tool ONTAP, tutti i nodi del cluster vSphere utilizzano un singolo indirizzo IP per montare il datastore. Ciò potrebbe causare un collo di bottiglia sulla porta di rete. Per evitare questo problema, smontare il datastore, quindi rimontarlo utilizzando la procedura

guidata standard del datastore vSphere utilizzando un nome DNS round-robin che offre bilanciamento del carico tra le LIF della SVM. Dopo il rimontaggio, gli strumenti ONTAP saranno nuovamente in grado di gestire il datastore. Se gli strumenti ONTAP non sono disponibili, utilizzare i valori predefiniti di FlexGroup e creare il criterio di esportazione seguendo le linee guida riportate in "Datastore e protocolli: NFS".

- Quando si ridimensiona un datastore FlexGroup, tenere presente che FlexGroup è costituito da più volumi FlexVol più piccoli che creano uno spazio dei nomi più grande. Pertanto, dimensionare il datastore in modo che sia almeno 8x MB (si suppongano i 8 componenti predefiniti) delle dimensioni del file VMDK più il 10-20% di spazio inutilizzato, per garantire flessibilità nel ribilanciamento. Ad esempio, se nell'ambiente è presente un VMDK di 6TB GB, dimensionare il datastore FlexGroup non inferiore a 52,8TB GB (6x8+10%).
- VMware e NetApp supportano il trunking di sessione NFSv4,1 a partire da ONTAP 9.14.1. Per informazioni dettagliate sulle versioni specifiche, fare riferimento alle note della matrice di interoperabilità NFS 4,1 di NetApp. NFSv3 non supporta percorsi fisici multipli a un volume ma supporta nconnect beginning in vSphere 8.0U2. Ulteriori informazioni su nconnect sono disponibili sul sito "Funzione NFSv3 nConnect con NetApp e VMware".
- Utilizzare il plug-in NFS per VMware VAAI per l'offload delle copie. Si noti che mentre il cloning è migliorato all'interno di un datastore FlexGroup, come menzionato in precedenza, ONTAP non offre significativi vantaggi in termini di performance rispetto alla copia dell'host ESXi quando si copiano le macchine virtuali tra volumi FlexVol e/o FlexGroup. Prendi in considerazione, pertanto, i workload di cloning al momento di decidere di utilizzare VAAI o FlexGroup. La modifica del numero di volumi costituenti è un modo per ottimizzare il cloning basato su FlexGroup. Come per l'ottimizzazione del timeout della cache menzionato in precedenza.
- Utilizza i tool ONTAP per VMware vSphere 9,8 o versione successiva per monitorare le performance delle macchine virtuali FlexGroup utilizzando le metriche ONTAP (dashboard e report VM) e per gestire la QoS sulle singole macchine virtuali. Queste metriche non sono attualmente disponibili tramite i comandi o le API ONTAP.
- Il plug-in SnapCenter per VMware vSphere versione 4,4 e successive supporta il backup e recovery delle macchine virtuali in un datastore FlexGroup nel sistema storage primario. SCV 4,6 aggiunge il supporto di SnapMirror per datastore basati su FlexGroup. L'utilizzo di snapshot e replica basate su array è il modo più efficiente per proteggere i dati.

## Configurazione di rete

La configurazione delle impostazioni di rete quando si utilizza vSphere con sistemi che eseguono il software ONTAP è semplice e simile ad altre configurazioni di rete.

Ecco alcuni aspetti da considerare:

- Separare il traffico di rete dello storage dalle altre reti. È possibile ottenere una rete separata utilizzando una VLAN dedicata o switch separati per lo storage. Se la rete di storage condivide percorsi fisici come gli uplink, potrebbe essere necessario QoS o porte di uplink aggiuntive per garantire una larghezza di banda sufficiente. Non connettere gli host direttamente allo storage; utilizzare gli switch per disporre di percorsi ridondanti e consentire a VMware ha di funzionare senza alcun intervento. Vedere "Connessione di rete diretta" per ulteriori informazioni.
- I frame jumbo possono essere utilizzati se lo si desidera e supportati dalla rete, in particolare quando si utilizza iSCSI. Se vengono utilizzati, assicurarsi che siano configurati in modo identico su tutti i dispositivi di rete, VLAN e così via nel percorso tra lo storage e l'host ESXi. In caso contrario, potrebbero verificarsi problemi di connessione o di prestazioni. La MTU deve essere impostata in modo identico anche sullo switch virtuale ESXi, sulla porta VMkernel e anche sulle porte fisiche o sui gruppi di interfacce di ciascun nodo ONTAP.
- NetApp consiglia di disattivare il controllo del flusso di rete solo sulle porte di rete del cluster all'interno di un cluster ONTAP. NetApp non fornisce altri consigli sulle Best practice per le restanti porte di rete

utilizzate per il traffico dati. Se necessario, è necessario attivarlo o disattivarlo. Vedere "TR-4182" per ulteriori informazioni sul controllo di flusso.

- Quando gli array di storage ESXi e ONTAP sono collegati a reti di storage Ethernet, NetApp consiglia di configurare le porte Ethernet a cui questi sistemi si connettono come porte edge RSTP (Rapid Spanning Tree Protocol) o utilizzando la funzione PortFast di Cisco. NetApp consiglia di abilitare la funzione di trunk PortFast Spanning-Tree in ambienti che utilizzano la funzionalità Cisco PortFast e che dispongono di un trunking VLAN 802.1Q abilitato per il server ESXi o gli array di storage ONTAP.
- NetApp consiglia le seguenti Best practice per l'aggregazione dei collegamenti:
  - Utilizzare switch che supportano l'aggregazione di collegamenti di porte su due chassis switch separati utilizzando un approccio a gruppi di aggregazione di collegamenti multi-chassis, ad esempio Virtual PortChannel (VPC) di Cisco.
  - Disattivare LACP per le porte dello switch connesse a ESXi, a meno che non si utilizzi dvSwitch 5.1 o versioni successive con LACP configurato.
  - Utilizzare LACP per creare aggregati di link per sistemi storage ONTAP con gruppi di interfacce multimodali dinamiche con hash IP.
  - Utilizzare un criterio di raggruppamento hash IP su ESXi.

La seguente tabella fornisce un riepilogo degli elementi di configurazione di rete e indica la posizione in cui vengono applicate le impostazioni.

| Elemento | ESXi | Switch | Nodo | SVM |
|---|---|---|---|---|
| Indirizzo IP | VMkernel | No** | No** | Sì |
| Aggregazione dei collegamenti | Switch virtuale | Sì | Sì | No* |
| VLAN | Gruppi di porte VMkernel e VM | Sì | Sì | No* |
| Controllo di flusso | NIC | Sì | Sì | No* |
| Spanning tree | No | Sì | No | No |
| MTU (per frame jumbo) | Switch virtuale e porta VMkernel (9000) | Sì (impostato su max) | Sì (9000) | No* |
| Gruppi di failover | No | No | Sì (creare) | Sì (selezionare) |

*Le LIF SVM si connettono a porte, gruppi di interfacce o interfacce VLAN con VLAN, MTU e altre impostazioni. Tuttavia, le impostazioni non vengono gestite a livello di SVM.

**Questi dispositivi dispongono di indirizzi IP propri per la gestione, ma non vengono utilizzati nel contesto dello storage di rete ESXi.

#### SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

In vSphere, esistono tre modi per utilizzare le LUN dello storage a blocchi:

- Con datastore VMFS
- Con RDM (raw device mapping)
- Come LUN accessibile e controllato da un iniziatore software da un sistema operativo guest VM

VMFS è un file system in cluster dalle performance elevate che fornisce datastore che sono pool di storage condivisi. Gli archivi dati VMFS possono essere configurati con LUN a cui si accede utilizzando spazi dei nomi FC, iSCSI, FCoE o NVMe a cui si accede dal protocollo NVMe/FC. VMFS consente l'accesso simultaneo alle LUN tradizionali da parte di ogni server ESX in un cluster. La dimensione massima del LUN ONTAP è generalmente di 16 TB; pertanto, un datastore VMFS 5 di 64 TB (vedere la prima tabella di questa sezione) viene creato utilizzando quattro LUN da 16 TB (tutti i sistemi array SAN supportano la dimensione massima del LUN VMFS di 64 TB). Poiché l'architettura LUN di ONTAP non ha una profondità di coda singola ridotta, gli archivi dati VMFS in ONTAP possono scalare in maniera relativamente semplice rispetto alle architetture di array tradizionali.

VSphere include il supporto integrato per più percorsi verso i dispositivi storage, definito NMP (Native Multipathing). NMP è in grado di rilevare il tipo di storage per i sistemi storage supportati e di configurare automaticamente lo stack NMP per supportare le funzionalità del sistema storage in uso.

Sia NMP che ONTAP supportano l'ALUA (Asymmetric Logical Unit Access) per negoziare percorsi ottimizzati e non ottimizzati. In ONTAP, un percorso ottimizzato per ALUA segue un percorso di dati diretto, utilizzando una porta di destinazione sul nodo che ospita il LUN a cui si accede. ALUA è attivato per impostazione predefinita sia in vSphere che in ONTAP. NMP riconosce il cluster ONTAP come ALUA e utilizza il plug-in del tipo di array di storage ALUA (`VMW_SATP_ALUA`) e seleziona il plug-in di selezione del percorso round-robin ( `VMW_PSP_RR`).

ESXi 6 supporta fino a 256 LUN e fino a 1,024 percorsi totali verso LUN. I LUN o i percorsi che superano questi limiti non sono visti da ESXi. Supponendo il numero massimo di LUN, il limite di percorso consente quattro percorsi per LUN. In un cluster ONTAP più grande, è possibile raggiungere il limite di percorso prima del limite di LUN. Per risolvere questo limite, ONTAP supporta la mappa LUN selettiva (SLM) nella versione 8.3 e successive.

SLM limita i nodi che pubblicizzano i percorsi a una determinata LUN. È una Best practice di NetApp avere almeno una LIF per nodo per SVM e utilizzare SLM per limitare i percorsi pubblicizzati al nodo che ospita la LUN e il suo partner ha. Sebbene esistano altri percorsi, essi non vengono pubblicizzati per impostazione predefinita. È possibile modificare i percorsi pubblicizzati con gli argomenti del nodo di reporting add e remove all'interno di SLM. Si noti che i LUN creati nelle release precedenti alla 8,3 pubblicizzano tutti i percorsi e devono essere modificati solo per pubblicizzare i percorsi alla coppia ha di hosting. Per ulteriori informazioni su SLM, vedere la sezione 5.9 di "TR-4080". Il precedente metodo di portset può essere utilizzato anche per ridurre ulteriormente i percorsi disponibili per un LUN. I portset aiutano a ridurre il numero di percorsi visibili attraverso i quali gli iniziatori in un igroup possono vedere le LUN.

- SLM è attivato per impostazione predefinita. A meno che non si utilizzino portset, non è necessaria alcuna configurazione aggiuntiva.
- Per i LUN creati prima di Data ONTAP 8,3, applicare manualmente SLM eseguendo `lun mapping remove-reporting-nodes` Comando per rimuovere i nodi di reporting del LUN e limitare l'accesso del LUN al nodo proprietario del LUN e al partner ha.

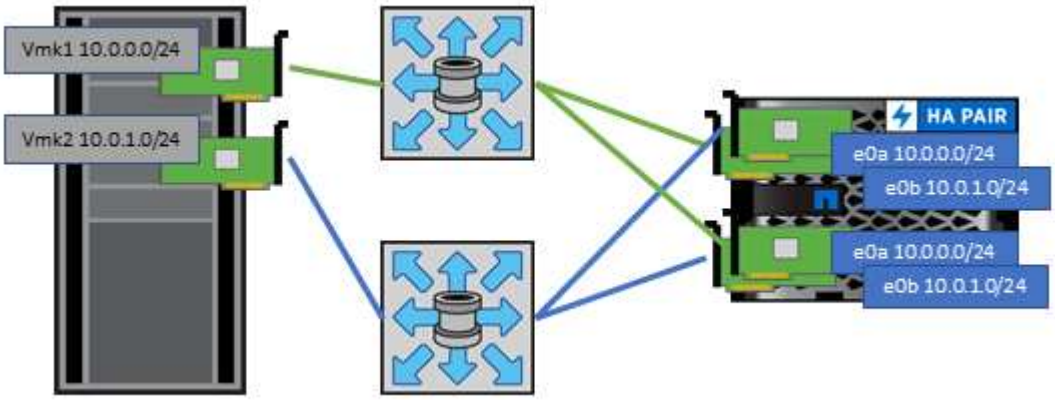
I protocolli a blocchi (iSCSI, FC e FCoE) accedono alle LUN utilizzando ID LUN e numeri di serie, insieme a nomi univoci. FC e FCoE utilizzano nomi in tutto il mondo (WWNN e WWPN), mentre iSCSI utilizza nomi iSCSI qualificati (IQN). Il percorso delle LUN all'interno dello storage è privo di significato per i protocolli a blocchi e non viene presentato in alcun punto del protocollo. Pertanto, un volume che contiene solo LUN non deve essere montato internamente e non è necessario un percorso di giunzione per i volumi che contengono LUN utilizzati negli archivi dati. Il sottosistema NVMe in ONTAP funziona in modo simile.

Altre Best practice da prendere in considerazione:

- Assicurarsi che venga creata un'interfaccia logica (LIF) per ogni SVM su ciascun nodo del cluster ONTAP per garantire la massima disponibilità e mobilità. La Best practice PER LE SAN ONTAP consiste

nell'utilizzare due porte fisiche e LIF per nodo, una per ciascun fabric. ALUA viene utilizzato per analizzare i percorsi e identificare i percorsi attivi ottimizzati (diretti) rispetto ai percorsi attivi non ottimizzati. ALUA viene utilizzato per FC, FCoE e iSCSI.

- Per le reti iSCSI, utilizzare più interfacce di rete VMkernel su diverse subnet di rete con raggruppamento NIC quando sono presenti più switch virtuali. È inoltre possibile utilizzare più NIC fisiche collegate a più switch fisici per fornire ha e un throughput maggiore. La figura seguente mostra un esempio di connettività multipath. In ONTAP, è possibile utilizzare un gruppo di interfacce a modalità singola con più collegamenti a switch diversi o LACP con gruppi di interfacce multimodali per ottenere vantaggi di elevata disponibilità e aggregazione dei collegamenti.
- Se il protocollo CHAP (Challenge-Handshake Authentication Protocol) viene utilizzato in ESXi per l'autenticazione di destinazione, deve essere configurato anche in ONTAP utilizzando la CLI (`vserver iscsi security create`) O con System Manager (modificare Initiator Security in Storage > SVM > SVM Settings > Protocols > iSCSI).
- Utilizza i tool ONTAP per VMware vSphere per creare e gestire LUN e igroups. Il plug-in determina automaticamente le WWPN dei server e crea gli igroups appropriati. Inoltre, configura i LUN in base alle Best practice e li associa agli igroups corretti.
- Utilizzare con cautela gli RDM poiché possono essere più difficili da gestire e utilizzano anche percorsi limitati come descritto in precedenza. I LUN ONTAP supportano entrambi "modalità di compatibilità fisica e virtuale" RDM.
- Per ulteriori informazioni sull'utilizzo di NVMe/FC con vSphere 7.0, consulta questo articolo "Guida alla configurazione degli host NVMe/FC di ONTAP" e. "TR-4684". La figura seguente illustra la connettività multipath da un host vSphere a una LUN ONTAP.




### NFS

VSphere consente ai clienti di utilizzare array NFS di livello Enterprise per fornire l'accesso simultaneo agli archivi dati a tutti i nodi di un cluster ESXi. Come indicato nella sezione datastore, l'utilizzo di NFS con vSphere offre alcuni vantaggi in termini di facilità d'uso e visibilità dell'efficienza dello storage.

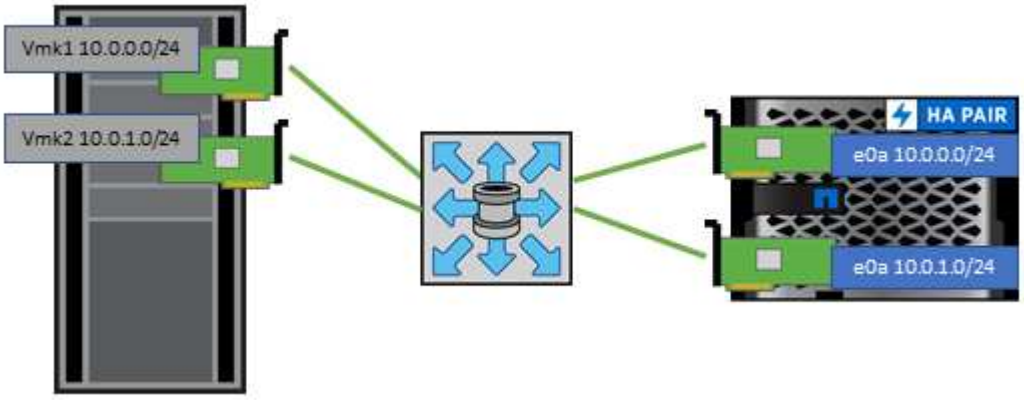
Quando si utilizza ONTAP NFS con vSphere, si consiglia di seguire le seguenti Best practice:

- Utilizzare una singola interfaccia logica (LIF) per ogni SVM su ciascun nodo del cluster ONTAP. Le raccomandazioni precedenti di un LIF per datastore non sono più necessarie. Benché l'accesso diretto (LIF e datastore nello stesso nodo) sia migliore, non preoccuparti dell'accesso indiretto perché l'effetto sulle performance è generalmente minimo (microsecondi).
- Tutte le versioni di VMware vSphere attualmente supportate possono utilizzare sia NFS v3 che v4,1. Il supporto ufficiale per nconnect è stato aggiunto a vSphere 8,0 update 2 per NFS v3. Per NFS v4,1, vSphere continua a supportare il trunking della sessione, l'autenticazione Kerberos e l'autenticazione

Kerberos con integrità. È importante notare che il trunking della sessione richiede ONTAP 9.14.1 o una versione successiva. Ulteriori informazioni sulla funzione nconnect e su come migliora le prestazioni "Funzione NFSv3 nConnect con NetApp e VMware".

Vale la pena notare che NFSv3 e NFSv4,1 utilizzano meccanismi di bloccaggio diversi. NFSv3 utilizza il blocco lato client, mentre NFSv4,1 utilizza il blocco lato server. Anche se un volume ONTAP può essere esportato tramite entrambi i protocolli, ESXi può montare un datastore solo attraverso un protocollo. Tuttavia, ciò non significa che altri host ESXi non possano montare lo stesso datastore attraverso una versione diversa. Per evitare qualsiasi problema, è essenziale specificare la versione del protocollo da utilizzare durante il montaggio, assicurandosi che tutti gli host utilizzino la stessa versione e, quindi, lo stesso stile di blocco. È fondamentale evitare di mischiare versioni NFS tra gli host. Se possibile, utilizzare i profili host per verificare la conformità.
**Poiché non esiste alcuna conversione automatica del datastore tra NFSv3 e NFSv4,1, creare un nuovo datastore NFSv4,1 e utilizzare Storage vMotion per migrare le macchine virtuali nel nuovo datastore.**
Fare riferimento alle note della tabella di interoperabilità NFS v4,1 nella "Tool NetApp Interoperability Matrix"
Per i livelli di patch ESXi specifici richiesti per il supporto.
* Le policy di esportazione NFS vengono utilizzate per controllare l'accesso da parte degli host vSphere. È possibile utilizzare un criterio con più volumi (datastore). Con NFSv3, ESXi utilizza lo stile di sicurezza sys (UNIX) e richiede l'opzione di montaggio root per eseguire le macchine virtuali. In ONTAP, questa opzione viene definita superutente e, quando viene utilizzata l'opzione superutente, non è necessario specificare l'ID utente anonimo. Tenere presente che le regole dei criteri di esportazione con valori diversi per `-anon` e. `-allow-suid` Può causare problemi di rilevamento SVM con gli strumenti ONTAP. Ecco un esempio di politica:
**Protocollo di accesso: nfs3**
Specifiche di corrispondenza client: 192.168.42.21
**RO regola di accesso: SYS**
RW regola di accesso: SYS
**UID anonimo**
Superutente: SYS
* Se si utilizza il plug-in NFS NetApp per VMware VAAI, il protocollo deve essere impostato su `nfs` quando viene creata o modificata la regola dei criteri di esportazione. Il protocollo NFSv4 è necessario per l'offload delle copie VAAI e per specificare il protocollo come `nfs` Include automaticamente le versioni NFSv3 e NFSv4.
* I volumi del datastore NFS sono collegati dal volume root della SVM; pertanto, ESXi deve avere accesso al volume root per navigare e montare i volumi del datastore. La policy di esportazione per il volume root e per qualsiasi altro volume in cui la giunzione del volume del datastore è nidificata deve includere una regola o regole per i server ESXi che concedono loro l'accesso in sola lettura. Ecco un esempio di policy per il volume root, utilizzando anche il plug-in VAAI:
**Protocollo di accesso: nfs (che include sia nfs3 che nfs4)**
Specifiche di corrispondenza client: 192.168.42.21
**RO regola di accesso: SYS**
RW regola di accesso: Mai (massima sicurezza per il volume root)
**UID anonimo**
Superuser: SYS (richiesto anche per il volume root con VAAI)
* Utilizza i tool ONTAP per VMware vSphere (la Best practice più importante):
**Utilizza i tool ONTAP per VMware vSphere per il provisioning dei datastore in quanto semplifica la gestione automatica delle policy di esportazione.**
Quando si creano datastore per cluster VMware con il plug-in, selezionare il cluster piuttosto che un singolo server ESX. Questa opzione attiva il montaggio automatico del datastore su tutti gli host del cluster.
**Utilizzare la funzione di montaggio dei plug-in per applicare i datastore esistenti ai nuovi server.**
Quando non si utilizzano gli strumenti ONTAP per VMware vSphere, utilizzare un unico criterio di esportazione per tutti i server o per ogni cluster di server in cui è necessario un ulteriore controllo dell'accesso.
* Sebbene ONTAP offra una struttura flessibile dello spazio dei nomi dei volumi per disporre i volumi in una struttura ad albero utilizzando le giunzioni, questo approccio non ha alcun valore per vSphere. Crea una directory per ogni VM nella directory principale dell'archivio dati, indipendentemente dalla gerarchia dello

spazio dei nomi dello storage. Pertanto, la Best practice consiste nel montare semplicemente il percorso di giunzione per i volumi per vSphere nel volume root della SVM, che è il modo in cui i tool ONTAP per VMware vSphere prevedono il provisioning dei datastore. La mancanza di percorsi di giunzione nidificati significa anche che nessun volume dipende da un volume diverso dal volume root e che la sua eliminazione o la sua eliminazione, anche intenzionalmente, non influisce sul percorso verso altri volumi.
* Per le partizioni NTFS sui datastore NFS è consigliabile Un blocco di 4K KB. La figura seguente mostra la connettività da un host vSphere a un datastore NFS ONTAP.




La seguente tabella elenca le versioni di NFS e le funzionalità supportate.

| Funzionalità di vSphere | NFSv3 | NFSv4,1 |
|---|---|---|
| VMotion e Storage vMotion | Sì | Sì |
| Alta disponibilità | Sì | Sì |
| Tolleranza agli errori | Sì | Sì |
| DRS | Sì | Sì |
| Profili host | Sì | Sì |
| DRS dello storage | Sì | No |
| Controllo i/o dello storage | Sì | No |
| SRM | Sì | No |
| Volumi virtuali | Sì | No |
| Accelerazione hardware (VAAI) | Sì | Sì |
| Autenticazione Kerberos | No | Sì (ottimizzato con vSphere 6.5 e versioni successive per supportare AES, krb5i) |
| Supporto multipathing | No | Sì (ONTAP 9.14.1) |

### Connessione di rete diretta

Gli amministratori dello storage a volte preferiscono semplificare le loro infrastrutture rimuovendo gli switch di rete dalla configurazione. Questo può essere supportato in alcuni scenari.

#### ISCSI e NVMe/TCP

Un host che utilizza iSCSI o NVMe/TCP può essere collegato direttamente a un sistema storage e funzionare normalmente. La ragione è la pedata. Le connessioni dirette a due storage controller differenti offrono due percorsi indipendenti per il flusso di dati. La perdita di percorso, porta o controller non impedisce l'utilizzo dell'altro percorso.

#### NFS

È possibile utilizzare lo storage NFS con connessione diretta, ma con una limitazione significativa: Il failover non funzionerà senza una significativa attività di scripting, che sarà responsabilità del cliente.

Il motivo per cui il failover senza interruzioni è complicato con lo storage NFS connesso direttamente è il routing che si verifica sul sistema operativo locale. Ad esempio, si supponga che un host abbia un indirizzo IP 192.168.1.1/24 e che sia collegato direttamente a un controller ONTAP con un indirizzo IP 192.168.1.50/24. Durante il failover, l'indirizzo 192.168.1.50 può eseguire il failover sull'altro controller e sarà disponibile per l'host, ma in che modo l'host rileva la sua presenza? L'indirizzo 192.168.1.1 originale esiste ancora sulla scheda di rete host che non si connette più a un sistema operativo. Il traffico destinato a 192.168.1.50 continuerebbe ad essere inviato a una porta di rete inutilizzabile.

La seconda scheda NIC del sistema operativo potrebbe essere configurata come 19 2.168.1.2 e sarebbe in grado di comunicare con l'indirizzo 192.168.1.50 non riuscito, ma le tabelle di routing locali avrebbero un valore predefinito di utilizzo di un solo indirizzo **e di un solo indirizzo** per comunicare con la subnet 192.168.1.0/24. Un amministratore di sistema potrebbe creare un framework di script che rilevi una connessione di rete non riuscita e alteri le tabelle di routing locali o che porti le interfacce verso l'alto e verso il basso. La procedura esatta dipende dal sistema operativo in uso.

In pratica, i clienti NetApp dispongono di NFS con connessione diretta, ma in genere solo per i workload in cui le pause io durante i failover sono accettabili. Quando si utilizzano i supporti rigidi, non devono verificarsi errori di i/o durante tali pause. L'io dovrebbe bloccarsi finché i servizi non vengono ripristinati, mediante failback o intervento manuale, per spostare gli indirizzi IP tra le schede NIC dell'host.

#### Connessione diretta FC

Non è possibile connettere direttamente un host a un sistema storage ONTAP utilizzando il protocollo FC. Il motivo è l'uso di NPIV. Il WWN che identifica una porta FC ONTAP per la rete FC utilizza un tipo di virtualizzazione chiamato NPIV. Qualsiasi dispositivo collegato a un sistema ONTAP deve essere in grado di riconoscere un WWN NPIV. Attualmente non vi sono fornitori di HBA che offrono un HBA che può essere installato in un host in grado di supportare un target NPIV.

## Clonazione di VM e datastore

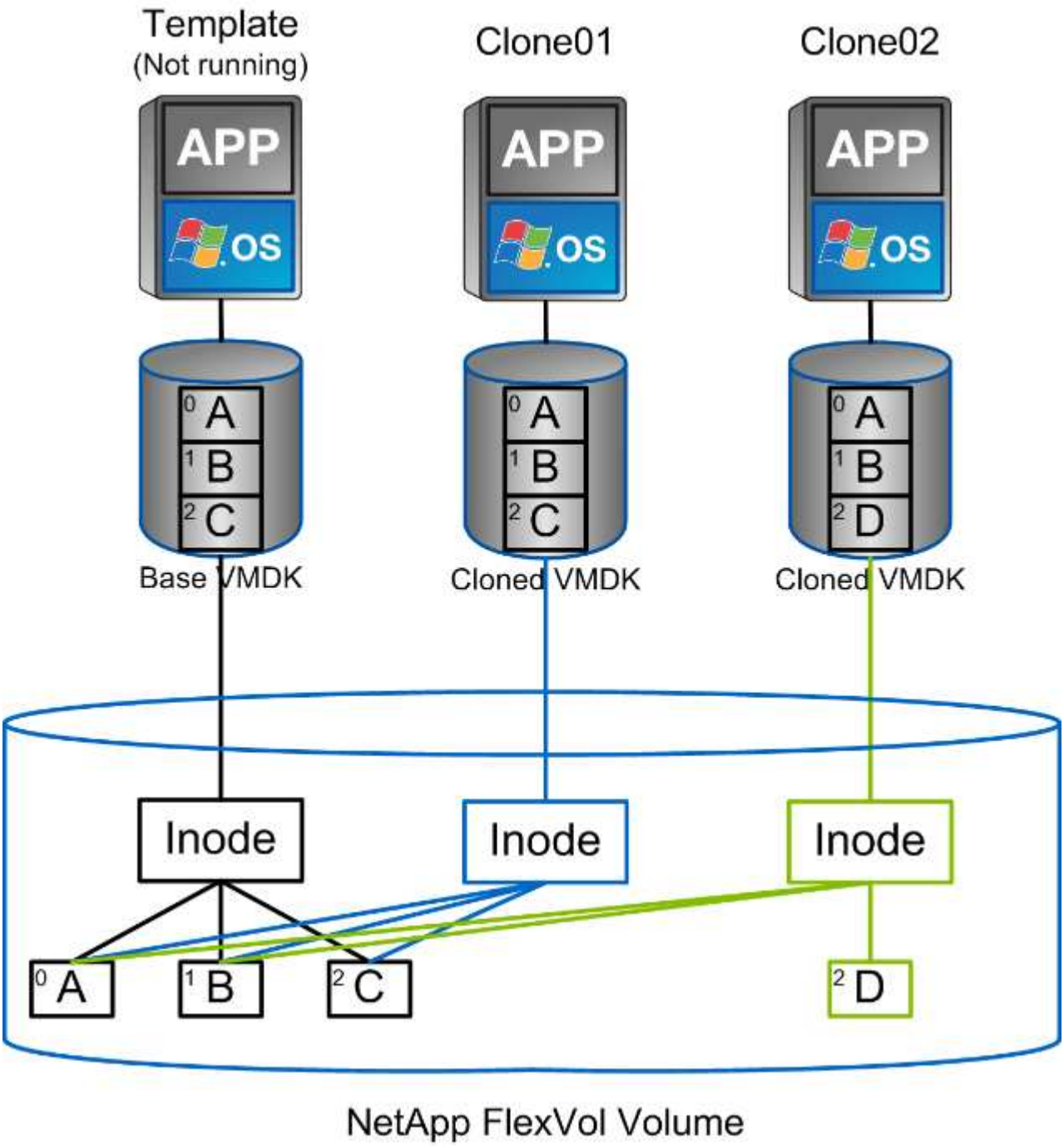
La clonazione di un oggetto storage consente di creare rapidamente copie da utilizzare ulteriormente, ad esempio il provisioning di macchine virtuali aggiuntive, operazioni di backup/recovery e così via.

In vSphere, è possibile clonare una macchina virtuale, un disco virtuale, un vVol o un datastore. Dopo essere stato clonato, l'oggetto può essere ulteriormente personalizzato, spesso attraverso un processo automatizzato. VSphere supporta entrambi i cloni di copia completa e i cloni collegati, in cui tiene traccia delle modifiche separatamente dall'oggetto originale.

I cloni collegati sono ideali per risparmiare spazio, ma aumentano la quantità di i/o che vSphere gestisce per la macchina virtuale, influenzando le performance di quella macchina virtuale e forse dell'host in generale. Ecco perché i clienti di NetApp spesso utilizzano cloni basati su sistemi storage per ottenere il meglio di entrambi i

mondi: Un utilizzo efficiente dello storage e maggiori performance.

La seguente figura illustra la clonazione ONTAP.




La clonazione può essere scaricata su sistemi che eseguono il software ONTAP attraverso diversi meccanismi, in genere a livello di VM, vVol o datastore. Questi includono quanto segue:

- VVol che utilizzano le API di NetApp vSphere per il provider di consapevolezza dello storage (VASA). I cloni ONTAP sono utilizzati per supportare le snapshot vVol gestite da vCenter, che sono efficienti in termini di spazio con effetto i/o minimo per crearle ed eliminarle. Le VM possono anche essere clonate utilizzando vCenter e vengono anche trasferite in ONTAP, sia all'interno di un singolo datastore/volume che tra datastore/volumi.
- Clonazione e migrazione di vSphere con API vSphere – integrazione array (VAAI). Le operazioni di cloning

delle macchine virtuali possono essere trasferite su ONTAP in ambienti SAN e NAS (NetApp fornisce un plug-in ESXi per abilitare VAAI per NFS). VSphere scarica solo le operazioni su macchine virtuali fredde (spente) in un datastore NAS, mentre le operazioni su macchine virtuali hot (cloning e storage vMotion) vengono anche scaricate per LA SAN. ONTAP utilizza l'approccio più efficiente in base all'origine, alla destinazione e alle licenze dei prodotti installate. Questa funzionalità viene utilizzata anche da VMware Horizon View.

- SRA (utilizzato con VMware Site Recovery Manager). In questo caso, i cloni vengono utilizzati per testare il ripristino della replica DR senza interruzioni.
- Backup e recovery con strumenti NetApp come SnapCenter. I cloni delle macchine virtuali vengono utilizzati per verificare le operazioni di backup e per montare un backup delle macchine virtuali in modo che i singoli file possano essere copiati.

La clonazione offload di ONTAP può essere invocata da VMware, NetApp e da strumenti di terze parti. I cloni che vengono scaricati su ONTAP presentano diversi vantaggi. Nella maggior parte dei casi, sono efficienti in termini di spazio e richiedono storage solo per le modifiche all'oggetto; non vi sono effetti aggiuntivi sulle performance per la lettura e la scrittura e in alcuni casi le performance sono migliorate grazie alla condivisione dei blocchi nelle cache ad alta velocità. Inoltre, consentono di trasferire cicli CPU e i/o di rete dal server ESXi. L'offload delle copie all'interno di un datastore tradizionale utilizzando un volume FlexVol può essere rapido ed efficiente con FlexClone concesso in licenza, ma le copie tra volumi FlexVol potrebbero essere più lente. Se si mantengono i modelli di macchine virtuali come origine dei cloni, è consigliabile posizionarli all'interno del volume datastore (utilizzare cartelle o librerie di contenuti per organizzarli) per cloni veloci ed efficienti in termini di spazio.

È inoltre possibile clonare un volume o un LUN direttamente in ONTAP per clonare un datastore. Con gli archivi di dati NFS, la tecnologia FlexClone può clonare un intero volume e il clone può essere esportato da ONTAP e montato da ESXi come altro archivio di dati. Per gli archivi di dati VMFS, ONTAP può clonare un LUN all'interno di un volume o di un intero volume, inclusi uno o più LUN. Un LUN contenente un VMFS deve essere mappato a un gruppo di iniziatori ESXi (igroup) e quindi rassegnato da ESXi per essere montato e utilizzato come datastore regolare. Per alcuni casi di utilizzo temporaneo, è possibile montare un VMFS clonato senza disdire. Dopo aver clonato un datastore, è possibile registrare, riconfigurare e personalizzare le macchine virtuali all'interno dell'IT come se fossero macchine virtuali clonate singolarmente.

In alcuni casi, è possibile utilizzare funzionalità aggiuntive con licenza per migliorare la clonazione, ad esempio SnapRestore per il backup o FlexClone. Queste licenze sono spesso incluse nei bundle di licenze senza costi aggiuntivi. È necessaria una licenza FlexClone per le operazioni di cloning di vVol e per supportare le snapshot gestite di un vVol (offload dall'hypervisor a ONTAP). Una licenza FlexClone può anche migliorare alcuni cloni basati su VAAI se utilizzati all'interno di un datastore/volume (crea copie istantanee ed efficienti in termini di spazio invece di copie a blocchi). Viene inoltre utilizzato dall'SRA per il test del ripristino di una replica DR e da SnapCenter per le operazioni di clonazione e per sfogliare le copie di backup per ripristinare singoli file.

## Protezione dei dati

Il backup delle macchine virtuali e il loro rapido ripristino sono tra i grandi punti di forza di ONTAP per vSphere ed è facile gestirla all'interno di vCenter con il plug-in SnapCenter per VMware vSphere.

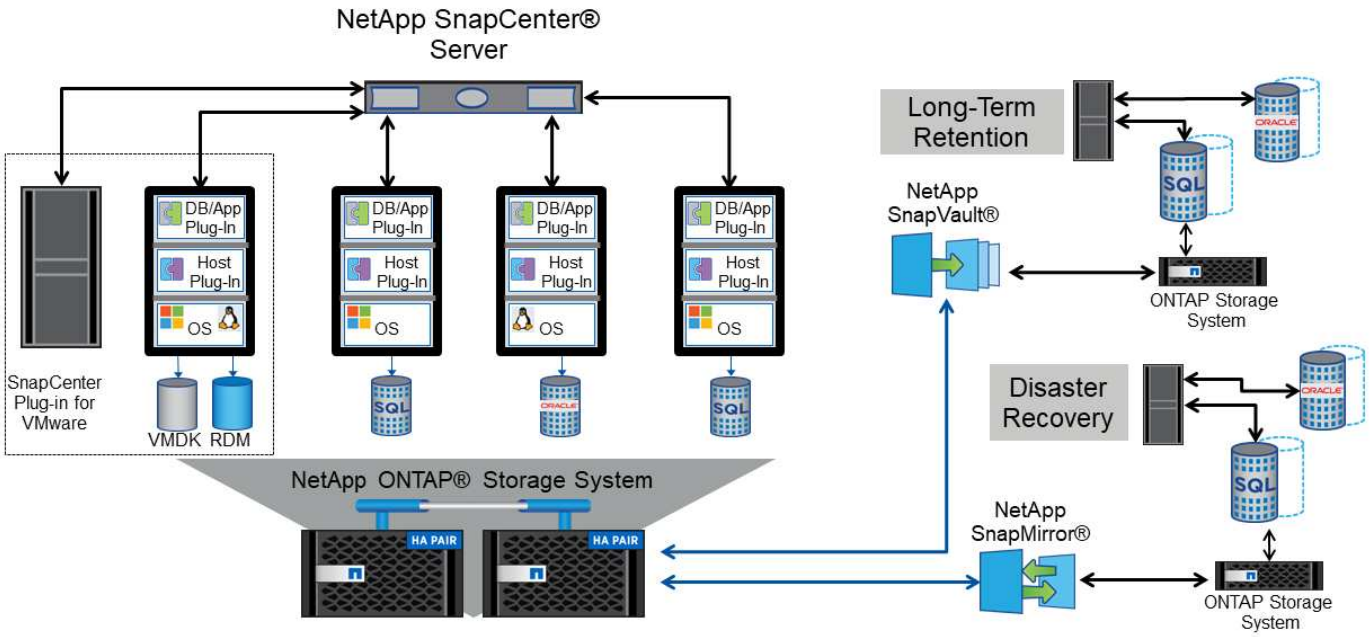
Utilizza le snapshot per creare copie rapide della tua macchina virtuale o del datastore senza influire sulle performance, quindi inviale a un sistema secondario utilizzando SnapMirror per la data Protection off-site a lungo termine. Questo approccio riduce al minimo lo spazio di storage e la larghezza di banda della rete memorizzando solo le informazioni modificate.

SnapCenter consente di creare policy di backup che possono essere applicate a più processi. Questi criteri possono definire pianificazione, conservazione, replica e altre funzionalità. Essi consentono una selezione

opzionale di snapshot coerenti con le macchine virtuali, che sfrutta la capacità dell'hypervisor di mettere in pausa l'i/o prima di scattare una snapshot VMware. Tuttavia, a causa dell'effetto delle performance delle snapshot VMware, in genere non sono consigliate, a meno che non sia necessario interrompere il file system guest. Utilizza invece le snapshot per la protezione generale e utilizza strumenti applicativi come i plug-in SnapCenter per proteggere i dati transazionali come SQL Server o Oracle. Questi snapshot sono diversi dalle snapshot VMware (coerenza) e sono adatti per una protezione a lungo termine. Le snapshot VMware sono solo "consigliato" per uso a breve termine a causa delle performance e di altri effetti.

Questi plug-in offrono funzionalità estese per proteggere i database in ambienti fisici e virtuali. Con vSphere, è possibile utilizzarli per proteggere i database SQL Server o Oracle in cui i dati vengono memorizzati su LUN RDM, LUN iSCSI direttamente connessi al sistema operativo guest o file VMDK su datastore VMFS o NFS. I plug-in consentono di specificare diversi tipi di backup del database, supportando backup online o offline e proteggendo i file di database insieme ai file di log. Oltre al backup e al ripristino, i plug-in supportano anche la clonazione dei database a scopo di sviluppo o test.

La figura seguente mostra un esempio di implementazione di SnapCenter.




Per funzionalità avanzate di disaster recovery, è consigliabile utilizzare NetApp SRA per ONTAP con VMware Site Recovery Manager. Oltre al supporto per la replica di datastore in un sito di DR, consente anche test senza interruzioni nell'ambiente di DR mediante il cloning dei datastore replicati. Anche il ripristino da un disastro e la riconprotezione della produzione dopo la risoluzione dell'interruzione sono semplificabili grazie all'automazione integrata in SRA.

Infine, per ottenere il massimo livello di protezione dei dati, prendere in considerazione una configurazione vMSC (Metro Storage Cluster) di VMware vSphere che utilizza NetApp MetroCluster. VMSC è una soluzione certificata da VMware che combina la replica sincrona con il clustering basato su array, offrendo gli stessi vantaggi di un cluster ad alta disponibilità ma distribuito su siti separati per la protezione dai disastri del sito. NetApp MetroCluster offre configurazioni convenienti per la replica sincrona con ripristino trasparente da qualsiasi guasto a un singolo componente dello storage e ripristino a comando singolo in caso di disastro del sito. VMSC è descritto in maggiore dettaglio nella "TR-4128".

## Qualità del servizio (QoS)

I sistemi che eseguono il software ONTAP possono utilizzare la funzione QoS dello

storage ONTAP per limitare il throughput in Mbps e/o i/o al secondo (IOPS) per diversi oggetti di storage come file, LUN, volumi o intere SVM.

I limiti di throughput sono utili per controllare i carichi di lavoro sconosciuti o di test prima della distribuzione per assicurarsi che non influiscano su altri carichi di lavoro. Possono anche essere utilizzati per limitare un carico di lavoro ingombrante dopo l'identificazione. Sono supportati anche i livelli minimi di servizio basati sugli IOPS per fornire performance costanti per gli oggetti SAN in ONTAP 9.2 e per gli oggetti NAS in ONTAP 9.3.

Con un datastore NFS, è possibile applicare una policy di QoS all'intero volume FlexVol o ai singoli file VMDK al suo interno. Con gli archivi di dati VMFS che utilizzano LUN ONTAP, è possibile applicare i criteri di qualità del servizio al volume FlexVol che contiene LUN o LUN singoli, ma non singoli file VMDK, poiché ONTAP non è consapevole del file system VMFS. Quando si utilizza vVol, è possibile impostare la QoS minima e/o massima su singole macchine virtuali utilizzando il profilo di capacità dello storage e la policy di storage delle macchine virtuali.

Il limite massimo di throughput QoS su un oggetto può essere impostato in Mbps e/o IOPS. Se vengono utilizzati entrambi, il primo limite raggiunto viene applicato da ONTAP. Un carico di lavoro può contenere più oggetti e una policy QoS può essere applicata a uno o più carichi di lavoro. Quando una policy viene applicata a più carichi di lavoro, i carichi di lavoro condividono il limite totale della policy. Gli oggetti nidificati non sono supportati (ad esempio, i file all'interno di un volume non possono avere una propria policy). I valori minimi di QoS possono essere impostati solo in IOPS.

I seguenti strumenti sono attualmente disponibili per la gestione delle policy di qualità del servizio ONTAP e per applicarle agli oggetti:

- CLI ONTAP
- Gestore di sistema di ONTAP
- OnCommand Workflow Automation
- Active IQ Unified Manager
- Kit di strumenti NetApp PowerShell per ONTAP
- Strumenti ONTAP per il provider VMware vSphere VASA

Per assegnare un criterio QoS a un VMDK su NFS, attenersi alle seguenti linee guida:

- La policy deve essere applicata a `vmname- flat.vmdk` che contiene l'immagine effettiva del disco virtuale, non il `vmname.vmdk` (file di descrizione del disco virtuale) o. `vmname.vmx` (File descrittore VM).
- Non applicare policy ad altri file di macchine virtuali, ad esempio file di swap virtuali (`vmname.vswp`).
- Quando si utilizza il client Web vSphere per trovare i percorsi di file (datastore > file), tenere presente che combina le informazioni di `- flat.vmdk` e. `. vmdk` e mostra semplicemente un file con il nome di `. vmdk` ma le dimensioni di `- flat.vmdk`. Aggiungi `-flat` nel nome del file per ottenere il percorso corretto.

Per assegnare una policy di QoS a un LUN, inclusi VMFS e RDM, è possibile ottenere la SVM di ONTAP (visualizzata come Vserver), il percorso del LUN e il numero di serie dal menu dei sistemi storage nella home page degli strumenti ONTAP per VMware vSphere. Seleziona il sistema storage (SVM), quindi gli oggetti correlati > SAN. Utilizzare questo approccio quando si specifica la qualità del servizio utilizzando uno degli strumenti ONTAP.

La QoS massima e minima può essere facilmente assegnata a una macchina virtuale basata su vVol con gli strumenti ONTAP per VMware vSphere o la console di storage virtuale 7.1 e versioni successive. Durante la creazione di un profilo di capacità storage per il container vVol, specifica un valore IOPS max e/o min in termini

di performance, quindi fai riferimento a questo SCP con la policy storage delle macchine virtuali. Utilizzare questo criterio quando si crea la macchina virtuale o si applica il criterio a una macchina virtuale esistente.

Gli archivi dati FlexGroup offrono funzionalità QoS avanzate quando si utilizzano gli strumenti ONTAP per VMware vSphere 9.8 e versioni successive. È possibile impostare facilmente la QoS su tutte le macchine virtuali di un datastore o su macchine virtuali specifiche. Per ulteriori informazioni, consultare la sezione FlexGroup di questo report.

### QoS ONTAP e SIOC VMware

Il QoS di ONTAP e il controllo i/o dello storage VMware vSphere sono tecnologie complementari che vSphere e gli amministratori dello storage possono utilizzare insieme per gestire le performance delle macchine virtuali vSphere ospitate su sistemi che eseguono il software ONTAP. Ogni strumento ha i propri punti di forza, come mostrato nella tabella seguente. A causa dei diversi ambiti di VMware vCenter e ONTAP, alcuni oggetti possono essere visti e gestiti da un sistema e non dall'altro.

| Proprietà | QoS ONTAP | VMware SIOC |
|---|---|---|
| Se attivo | La policy è sempre attiva | Attivo quando esiste un conflitto (latenza dell'archivio dati oltre la soglia) |
| Tipo di unità | IOPS, Mbps | IOPS, condivisioni |
| VCenter o ambito applicativo | Più ambienti vCenter, altri hypervisor e applicazioni | Singolo server vCenter |
| Impostare QoS su VM? | VMDK solo su NFS | VMDK su NFS o VMFS |
| Impostare QoS su LUN (RDM)? | Sì | No |
| Impostare la qualità del servizio su LUN (VMFS)? | Sì | No |
| Impostare QoS sul volume (datastore NFS)? | Sì | No |
| Impostare QoS su SVM (tenant)? | Sì | No |
| Approccio basato su policy? | Sì; può essere condiviso da tutti i carichi di lavoro della policy o applicato in toto a ciascun carico di lavoro della policy. | Sì, con vSphere 6.5 e versioni successive. |
| Licenza richiesta | Incluso con ONTAP | Enterprise Plus |

### VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDR) è una funzionalità vSphere che consente di posizionare le macchine virtuali sullo storage in base alla latenza i/o corrente e all'utilizzo dello spazio. Quindi, sposta le VM o i VMDK senza interruzioni tra gli archivi dati in un cluster di datastore (noto anche come pod), selezionando il migliore datastore in cui posizionare le VM o i VMDK nel cluster di datastore. Un cluster di datastore è un insieme di datastore simili che vengono aggregati in una singola unità di consumo dal punto di vista dell'amministratore di vSphere.

Quando si utilizzano DSP con strumenti ONTAP per VMware vSphere, è necessario prima creare un datastore con il plug-in, utilizzare vCenter per creare il cluster di datastore e quindi aggiungere il datastore. Una volta creato il cluster di datastore, è possibile aggiungere ulteriori datastore al cluster di datastore direttamente dalla

procedura guidata di provisioning nella pagina Dettagli.

Altre Best practice ONTAP per I DSP includono:

- Tutti gli archivi dati del cluster devono utilizzare lo stesso tipo di storage (ad esempio SAS, SATA o SSD), tutti gli archivi dati VMFS o NFS e avere le stesse impostazioni di replica e protezione.
- Considerare l'utilizzo DEGLI SDR in modalità predefinita (manuale). Questo approccio consente di rivedere i suggerimenti e decidere se applicarli o meno. Tenere presente i seguenti effetti delle migrazioni VMDK:
  - Quando GLI SDR spostano i VMDK tra datastore, qualsiasi risparmio di spazio derivante dalla clonazione o deduplica ONTAP viene perso. È possibile rieseguire la deduplica per recuperare questi risparmi.
  - Dopo che LE SDR spostano i VMDK, NetApp consiglia di ricreare gli snapshot nel datastore di origine, poiché lo spazio è altrimenti bloccato dalla VM che è stata spostata.
  - Lo spostamento di VMDK tra datastore sullo stesso aggregato ha pochi benefici e GLI SDR non hanno visibilità su altri carichi di lavoro che potrebbero condividere l'aggregato.

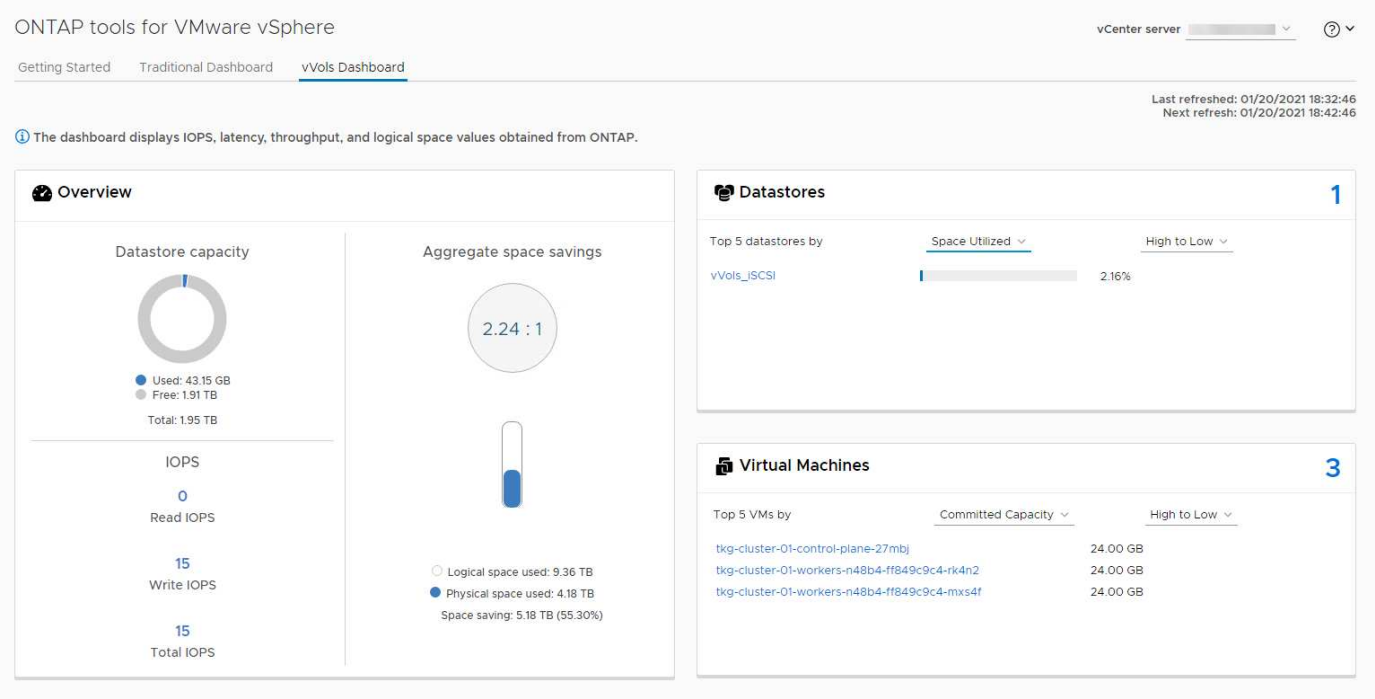
**Gestione basata su criteri di archiviazione e vVol**

Le API VMware vSphere per Storage Awareness (VASA) semplificano la configurazione dei datastore da parte di un amministratore dello storage con funzionalità ben definite e consentono all'amministratore delle macchine virtuali di utilizzarle quando necessario per eseguire il provisioning delle macchine virtuali senza dover interagire tra loro. Vale la pena di dare un'occhiata a questo approccio per scoprire in che modo può semplificare le operazioni di virtualizzazione dello storage ed evitare un lavoro molto banale.

Prima di VASA, gli amministratori delle macchine virtuali potevano definire le policy di storage delle macchine virtuali, ma dovevano collaborare con l'amministratore dello storage per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o le convenzioni di denominazione. Con VASA, l'amministratore dello storage può definire una serie di funzionalità di storage, tra cui performance, tiering, crittografia e replica. Un insieme di funzionalità per un volume o un set di volumi viene definito SCP (Storage Capability Profile).

SCP supporta la qualità del servizio minima e/o massima per i vVol di dati di una VM. La QoS minima è supportata solo sui sistemi AFF. Gli strumenti ONTAP per VMware vSphere includono una dashboard che visualizza le performance granulari delle macchine virtuali e la capacità logica per i vVol sui sistemi ONTAP.

La figura seguente mostra i tool ONTAP per il dashboard di VMware vSphere 9.8 vVol.




Una volta definito il profilo di capacità dello storage, è possibile utilizzarlo per eseguire il provisioning delle macchine virtuali utilizzando la policy di storage che ne identifica i requisiti. La mappatura tra il criterio di storage delle macchine virtuali e il profilo di capacità dello storage del datastore consente a vCenter di visualizzare un elenco di datastore compatibili per la selezione. Questo approccio è noto come gestione basata su criteri di storage.

VASA offre la tecnologia per eseguire query sullo storage e restituire un set di funzionalità di storage a vCenter. I vendor provider VASA forniscono la traduzione tra le API e i costrutti del sistema storage e le API VMware comprese da vCenter. Il provider VASA di NetApp per ONTAP viene offerto come parte dei tool ONTAP per macchina virtuale dell'appliance VMware vSphere, mentre il plug-in vCenter fornisce l'interfaccia per il provisioning e la gestione dei datastore vVol, nonché la capacità di definire profili di funzionalità dello storage (SCP).

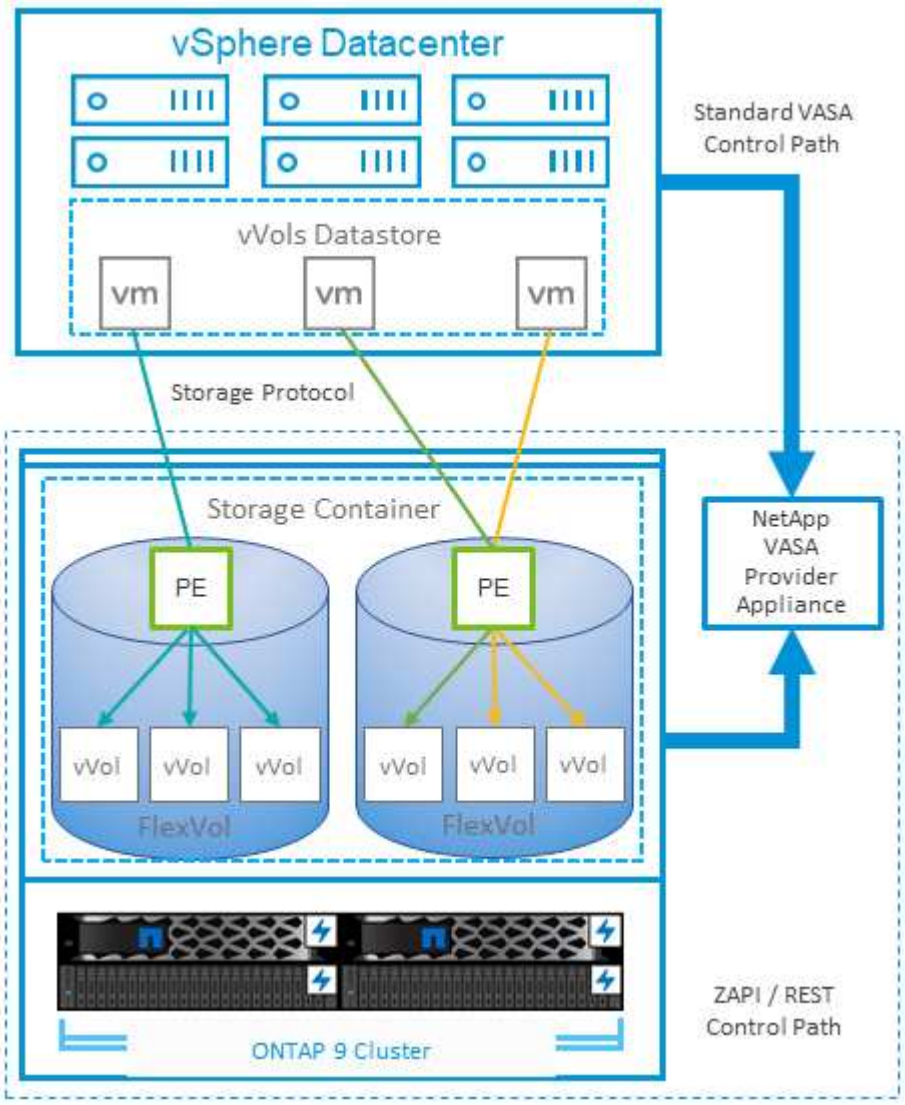
ONTAP supporta gli archivi dati VMFS e NFS vVol. L'utilizzo di vVol con datastore SAN offre alcuni dei vantaggi di NFS, come la granularità a livello di macchine virtuali. Di seguito sono riportate alcune Best practice da prendere in considerazione e ulteriori informazioni sono disponibili in "TR-4400":

- Un datastore vVol può essere costituito da più volumi FlexVol su più nodi del cluster. L'approccio più semplice è un singolo datastore, anche quando i volumi hanno funzionalità diverse. SPBM garantisce l'utilizzo di un volume compatibile per la macchina virtuale. Tuttavia, tutti i volumi devono far parte di una singola SVM ONTAP e devono essere accessibili utilizzando un singolo protocollo. È sufficiente una LIF per nodo per ogni protocollo. Evitare di utilizzare più release di ONTAP all'interno di un singolo datastore vVol, poiché le funzionalità dello storage potrebbero variare tra le varie release.
- Utilizza i tool ONTAP per il plug-in VMware vSphere per creare e gestire datastore vVol. Oltre a gestire il datastore e il relativo profilo, crea automaticamente un endpoint del protocollo per accedere ai vVol, se necessario. Se si utilizzano LUN, tenere presente che i LUN PES vengono mappati utilizzando LUN ID 300 e superiori. Verificare che l'impostazione di sistema avanzata dell'host ESXi sia corretta `Disk.MaxLUN` Consente un numero di ID LUN superiore a 300 (il valore predefinito è 1,024). Eseguire questa operazione selezionando l'host ESXi in vCenter, quindi la scheda Configura e trova `Disk.MaxLUN` Nell'elenco delle Advanced System Settings (Impostazioni di sistema avanzate).
- Non installare o migrare il provider VASA, il server vCenter (basato su appliance o Windows) o i tool ONTAP per VMware vSphere in sé su un datastore vVols, perché in tal caso sono dipendenti

reciprocamente, limitando la possibilità di gestirli in caso di interruzione dell'alimentazione o di altre interruzioni del data center.

- Eseguire regolarmente il backup della VM del provider VASA. Crea almeno snapshot orarie del datastore tradizionale che contiene il provider VASA. Per ulteriori informazioni sulla protezione e il ripristino del provider VASA, consulta questa sezione "Articolo della Knowledge base".

La figura seguente mostra i componenti di vVol.




**Migrazione e backup del cloud**

Un altro punto di forza di ONTAP è l'ampio supporto per il cloud ibrido, che unisce i sistemi nel tuo cloud privato on-premise con funzionalità di cloud pubblico. Ecco alcune soluzioni cloud NetApp che possono essere utilizzate insieme a vSphere:

- **Cloud Volumes** NetApp Cloud Volumes Service per Amazon Web Services o Google Cloud Platform e Azure NetApp Files per ANF offrono servizi di storage gestiti multiprotocollo dalle performance elevate negli ambienti di cloud pubblico leader. Possono essere utilizzati direttamente dai guest delle macchine virtuali VMware Cloud.
- **Cloud Volumes ONTAP.** il software per la gestione dei dati NetApp Cloud Volumes ONTAP offre controllo, protezione, flessibilità ed efficienza ai tuoi dati sul cloud di tua scelta. Cloud Volumes ONTAP è un software

di gestione dei dati nativo del cloud basato sullo storage ONTAP. Utilizzare insieme a Cloud Manager per implementare e gestire le istanze di Cloud Volumes ONTAP insieme ai sistemi ONTAP on-premise. Sfrutta le funzionalità NAS e SAN iSCSI avanzate insieme a una gestione dei dati unificata, incluse le snapshot e la replica SnapMirror.

- **Servizi cloud.** Usa Cloud Backup Service o SnapMirror Cloud per proteggere i dati dai sistemi on-premise utilizzando lo storage di cloud pubblico. Cloud Sync consente di migrare e mantenere sincronizzati i dati tra NAS, archivi di oggetti e storage Cloud Volumes Service.
- **FabricPool.** FabricPool offre tiering rapido e semplice per i dati ONTAP. È possibile migrare i blocchi cold in un archivio di oggetti nei cloud pubblici o in un archivio di oggetti StorageGRID privato e vengono richiamati automaticamente quando si accede nuovamente ai dati ONTAP. Oppure utilizzare il Tier di oggetti come terzo livello di protezione per i dati già gestiti da SnapVault. Questo approccio può consentirti di farlo "Memorizzazione di più snapshot delle macchine virtuali" Sui sistemi storage ONTAP primari e/o secondari.
- **ONTAP Select.** utilizza lo storage software-defined di NetApp per estendere il tuo cloud privato attraverso Internet a sedi e uffici remoti, dove puoi utilizzare ONTAP Select per supportare i servizi di file e blocchi e le stesse funzionalità di gestione dei dati vSphere presenti nel tuo data center aziendale.

Quando si progettano le applicazioni basate su macchine virtuali, considerare la futura mobilità del cloud. Ad esempio, invece di mettere insieme file di applicazioni e dati, utilizza un'esportazione LUN o NFS separata per i dati. Ciò consente di migrare la macchina virtuale e i dati separatamente ai servizi cloud.

#### Crittografia per i dati vSphere

Oggi, la necessità di proteggere i dati inattivi è in aumento grazie alla crittografia. Sebbene l'attenzione iniziale fosse concentrata sulle informazioni finanziarie e sanitarie, c'è sempre più interesse a proteggere tutte le informazioni, che siano archiviate in file, database o altri tipi di dati.

I sistemi che eseguono il software ONTAP semplificano la protezione dei dati con la crittografia a riposo. NetApp Storage Encryption (NSE) utilizza dischi con crittografia automatica e ONTAP per proteggere i dati SAN e NAS. NetApp offre inoltre NetApp Volume Encryption e NetApp aggregate Encryption come approccio semplice e basato su software per crittografare i volumi su qualsiasi disco. Questa crittografia software non richiede unità disco speciali o gestori di chiavi esterne ed è disponibile per i clienti ONTAP senza costi aggiuntivi. È possibile eseguire l'upgrade e iniziare a utilizzarlo senza alcuna interruzione per i client o le applicazioni e sono validati in base allo standard FIPS 140-2 livello 1, incluso il gestore delle chiavi integrato.

Esistono diversi approcci per la protezione dei dati delle applicazioni virtualizzate in esecuzione su VMware vSphere. Un approccio consiste nel proteggere i dati con il software all'interno della macchina virtuale a livello di sistema operativo guest. Gli hypervisor più recenti, come vSphere 6.5, ora supportano la crittografia a livello di VM come alternativa. Tuttavia, la crittografia del software NetApp è semplice e offre i seguenti vantaggi:

- **Nessun effetto sulla CPU del server virtuale.** alcuni ambienti di server virtuali richiedono ogni ciclo di CPU disponibile per le proprie applicazioni, tuttavia i test hanno dimostrato che sono necessarie fino a 5 risorse di CPU con crittografia a livello di hypervisor. Anche se il software di crittografia supporta il set di istruzioni AES-NI di Intel per l'offload del carico di lavoro di crittografia (come fa la crittografia del software NetApp), questo approccio potrebbe non essere fattibile a causa del requisito di nuove CPU che non sono compatibili con i server meno recenti.
- **Onboard Key Manager incluso.** la crittografia software NetApp include un gestore delle chiavi integrato senza costi aggiuntivi, il che rende semplice iniziare senza server di gestione delle chiavi ad alta disponibilità complessi da acquistare e utilizzare.
- **Nessun effetto sull'efficienza dello storage.** le tecniche di efficienza dello storage, come deduplica e compressione, sono ampiamente utilizzate oggi e sono fondamentali per utilizzare i supporti su disco flash in modo conveniente. Tuttavia, i dati crittografati non possono in genere essere deduplicati o compressi. La

crittografia dello storage e dell'hardware NetApp opera a un livello inferiore e consente l'utilizzo completo delle funzionalità di efficienza dello storage NetApp leader del settore, a differenza di altri approcci.

- **Crittografia granulare semplice del datastore.** con NetApp Volume Encryption, ogni volume ottiene la propria chiave AES a 256 bit. Se è necessario modificarlo, è possibile farlo con un singolo comando. Questo approccio è ideale se hai più tenant o hai bisogno di dimostrare una crittografia indipendente per diversi reparti o applicazioni. Questa crittografia viene gestita a livello di datastore, il che è molto più semplice della gestione di singole macchine virtuali.

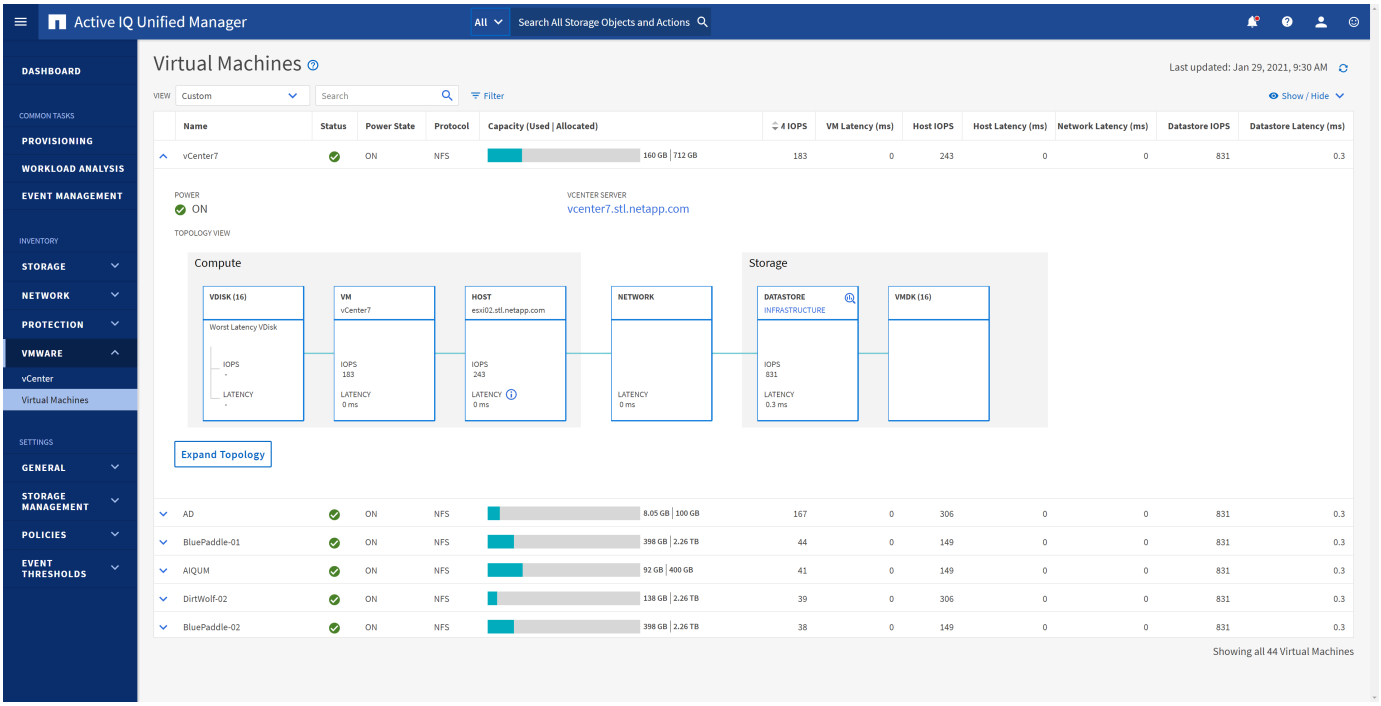
Iniziare a utilizzare la crittografia del software è semplice. Una volta installata la licenza, è sufficiente configurare il gestore delle chiavi integrato specificando una passphrase e quindi creare un nuovo volume o spostare un volume lato storage per abilitare la crittografia. NetApp sta lavorando per aggiungere un supporto più integrato per le funzionalità di crittografia nelle versioni future dei suoi strumenti VMware.

### Active IQ Unified Manager

Active IQ Unified Manager offre visibilità sulle macchine virtuali dell'infrastruttura virtuale e consente il monitoraggio e la risoluzione dei problemi relativi a storage e performance nell'ambiente virtuale.

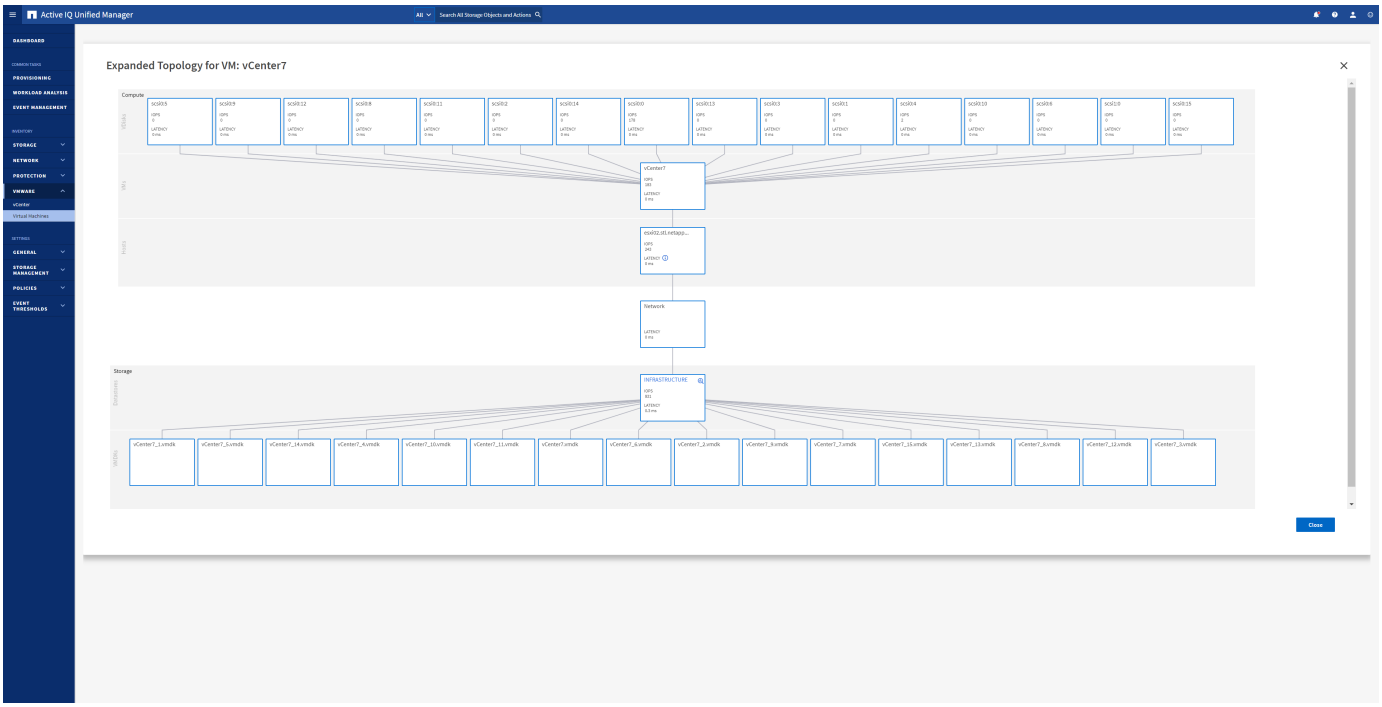
Una tipica implementazione di un'infrastruttura virtuale su ONTAP include diversi componenti distribuiti tra livelli di calcolo, rete e storage. Eventuali ritardi nelle performance in un'applicazione VM potrebbero verificarsi a causa di una combinazione di latenze affrontate dai vari componenti nei rispettivi layer.

La seguente schermata mostra la vista macchine virtuali Active IQ Unified Manager.




Unified Manager presenta il sottosistema sottostante di un ambiente virtuale in una vista topologica per determinare se si è verificato un problema di latenza nel nodo di calcolo, nella rete o nello storage. La vista evidenzia anche l'oggetto specifico che causa il ritardo delle performance per l'adozione di misure correttive e la risoluzione del problema sottostante.

La seguente schermata mostra la topologia espansa di AIQUM.




## Gestione basata su criteri di archiviazione e vVol

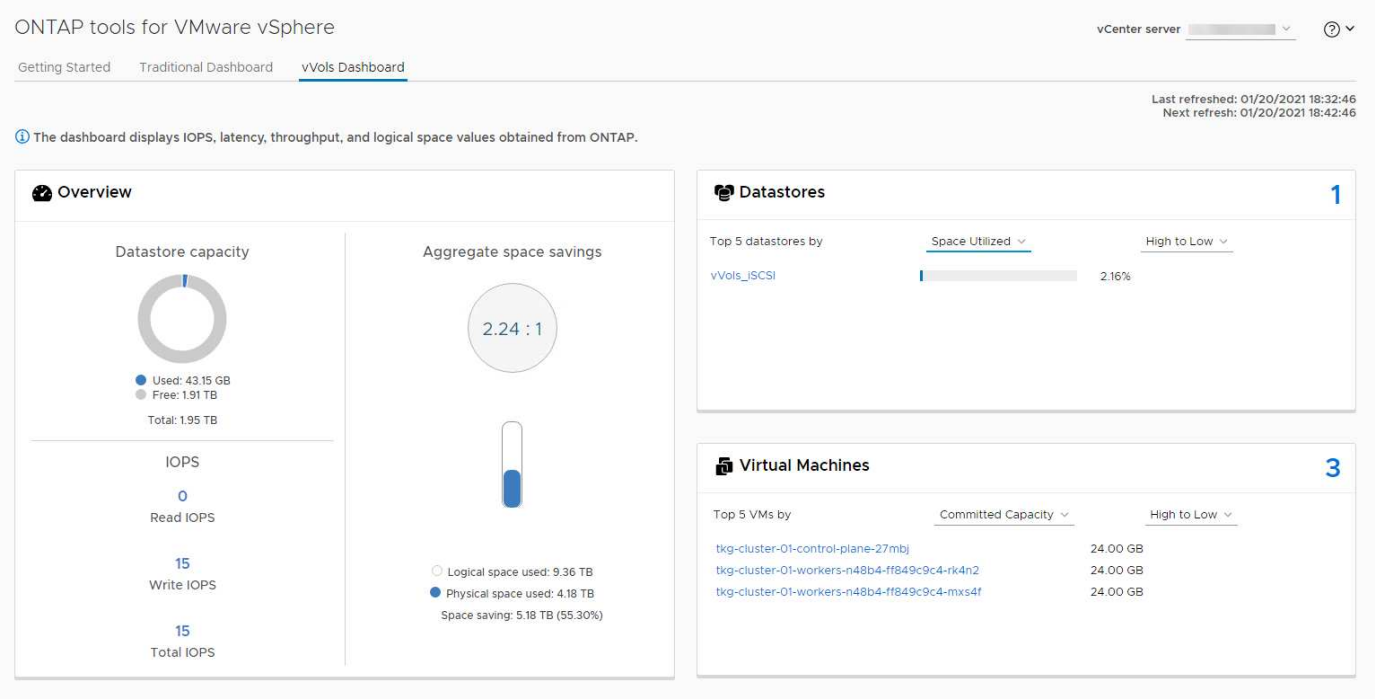
Le API VMware vSphere per Storage Awareness (VASA) semplificano la configurazione dei datastore da parte di un amministratore dello storage con funzionalità ben definite e consentono all'amministratore delle macchine virtuali di utilizzarle quando necessario per eseguire il provisioning delle macchine virtuali senza dover interagire tra loro.

Vale la pena di dare un'occhiata a questo approccio per scoprire in che modo può semplificare le operazioni di virtualizzazione dello storage ed evitare un lavoro molto banale.

Prima di VASA, gli amministratori delle macchine virtuali potevano definire le policy di storage delle macchine virtuali, ma dovevano collaborare con l'amministratore dello storage per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o le convenzioni di denominazione. Con VASA, l'amministratore dello storage può definire una serie di funzionalità di storage, tra cui performance, tiering, crittografia e replica. Un insieme di funzionalità per un volume o un set di volumi viene definito SCP (Storage Capability Profile).

SCP supporta la qualità del servizio minima e/o massima per i vVol di dati di una VM. La QoS minima è supportata solo sui sistemi AFF. Gli strumenti ONTAP per VMware vSphere includono una dashboard che visualizza le performance granulari delle macchine virtuali e la capacità logica per i vVol sui sistemi ONTAP.

La figura seguente mostra i tool ONTAP per il dashboard di VMware vSphere 9.8 vVol.




Una volta definito il profilo di capacità dello storage, è possibile utilizzarlo per eseguire il provisioning delle macchine virtuali utilizzando la policy di storage che ne identifica i requisiti. La mappatura tra il criterio di storage delle macchine virtuali e il profilo di capacità dello storage del datastore consente a vCenter di visualizzare un elenco di datastore compatibili per la selezione. Questo approccio è noto come gestione basata su criteri di storage.

VASA offre la tecnologia per eseguire query sullo storage e restituire un set di funzionalità di storage a vCenter. I vendor provider VASA forniscono la traduzione tra le API e i costrutti del sistema storage e le API VMware comprese da vCenter. Il provider VASA di NetApp per ONTAP viene offerto come parte dei tool ONTAP per macchina virtuale dell'appliance VMware vSphere, mentre il plug-in vCenter fornisce l'interfaccia per il provisioning e la gestione dei datastore vVol, nonché la capacità di definire profili di funzionalità dello storage (SCP).

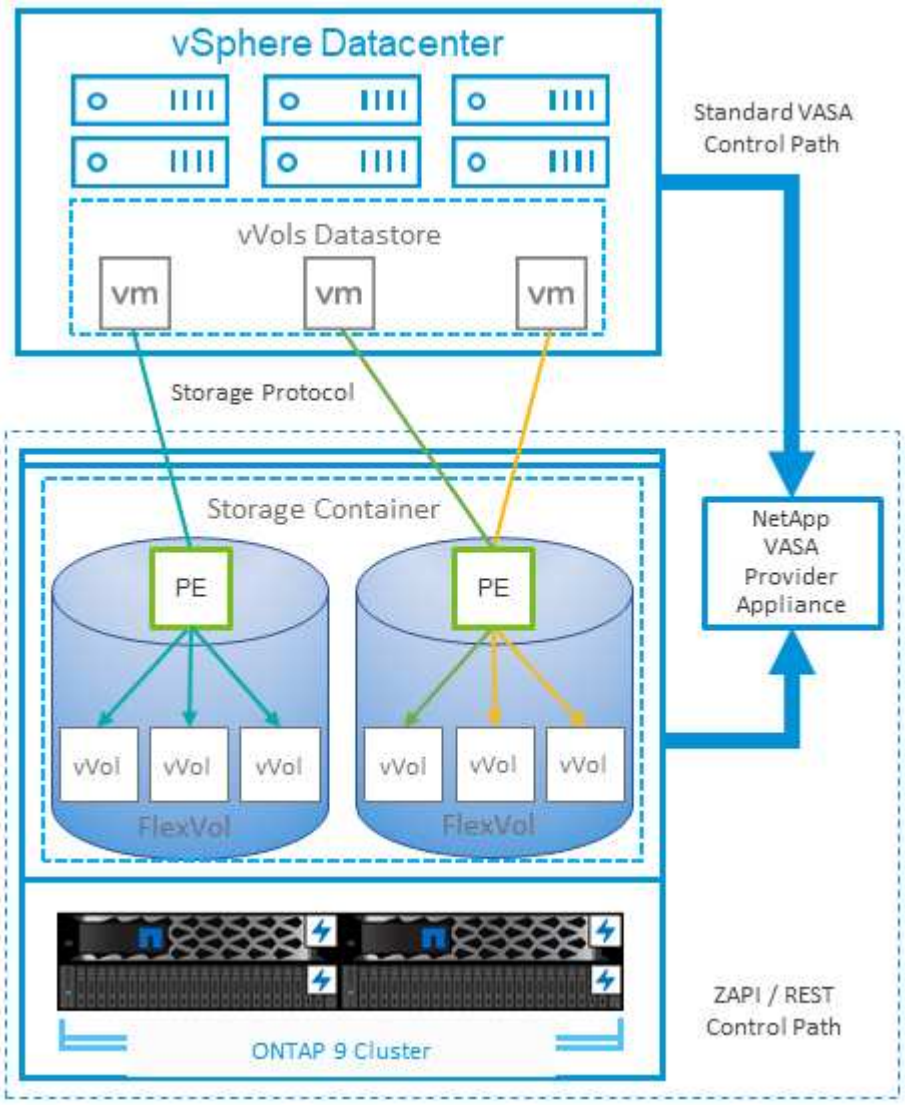
ONTAP supporta gli archivi dati VMFS e NFS vVol. L'utilizzo di vVol con datastore SAN offre alcuni dei vantaggi di NFS, come la granularità a livello di macchine virtuali. Di seguito sono riportate alcune Best practice da prendere in considerazione e ulteriori informazioni sono disponibili in "TR-4400":

- Un datastore vVol può essere costituito da più volumi FlexVol su più nodi del cluster. L'approccio più semplice è un singolo datastore, anche quando i volumi hanno funzionalità diverse. SPBM garantisce l'utilizzo di un volume compatibile per la macchina virtuale. Tuttavia, tutti i volumi devono far parte di una singola SVM ONTAP e devono essere accessibili utilizzando un singolo protocollo. È sufficiente una LIF per nodo per ogni protocollo. Evitare di utilizzare più release di ONTAP all'interno di un singolo datastore vVol, poiché le funzionalità dello storage potrebbero variare tra le varie release.
- Utilizza i tool ONTAP per il plug-in VMware vSphere per creare e gestire datastore vVol. Oltre a gestire il datastore e il relativo profilo, crea automaticamente un endpoint del protocollo per accedere ai vVol, se necessario. Se si utilizzano LUN, tenere presente che i LUN PES vengono mappati utilizzando LUN ID 300 e superiori. Verificare che l'impostazione di sistema avanzata dell'host ESXi sia corretta `Disk.MaxLUN` Consente un numero di ID LUN superiore a 300 (il valore predefinito è 1,024). Eseguire questa operazione selezionando l'host ESXi in vCenter, quindi la scheda Configura e trova `Disk.MaxLUN` Nell'elenco delle Advanced System Settings (Impostazioni di sistema avanzate).
- Non installare o migrare il provider VASA, il server vCenter (basato su appliance o Windows) o i tool ONTAP per VMware vSphere in sé su un datastore vVols, perché in tal caso sono dipendenti

reciprocamente, limitando la possibilità di gestirli in caso di interruzione dell'alimentazione o di altre interruzioni del data center.

- Eseguire regolarmente il backup della VM del provider VASA. Crea almeno snapshot orarie del datastore tradizionale che contiene il provider VASA. Per ulteriori informazioni sulla protezione e il ripristino del provider VASA, consulta questa sezione "Articolo della Knowledge base".

La figura seguente mostra i componenti di vVol.




## VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDR) è una funzionalità vSphere che consente di posizionare le macchine virtuali sullo storage in base alla latenza i/o corrente e all'utilizzo dello spazio.

Quindi, sposta le VM o i VMDK senza interruzioni tra gli archivi dati in un cluster di datastore (noto anche come pod), selezionando il migliore datastore in cui posizionare le VM o i VMDK nel cluster di datastore. Un cluster di datastore è un insieme di datastore simili che vengono aggregati in una singola unità di consumo dal punto di vista dell'amministratore di vSphere.

Quando si utilizzano DSP con strumenti ONTAP per VMware vSphere, è necessario prima creare un datastore

con il plug-in, utilizzare vCenter per creare il cluster di datastore e quindi aggiungere il datastore. Una volta creato il cluster di datastore, è possibile aggiungere ulteriori datastore al cluster di datastore direttamente dalla procedura guidata di provisioning nella pagina Dettagli.

Altre Best practice ONTAP per I DSP includono:

- Tutti gli archivi dati del cluster devono utilizzare lo stesso tipo di storage (ad esempio SAS, SATA o SSD), tutti gli archivi dati VMFS o NFS e avere le stesse impostazioni di replica e protezione.
- Considerare l'utilizzo DEGLI SDR in modalità predefinita (manuale). Questo approccio consente di rivedere i suggerimenti e decidere se applicarli o meno. Tenere presente i seguenti effetti delle migrazioni VMDK:
  - Quando GLI SDR spostano i VMDK tra datastore, qualsiasi risparmio di spazio derivante dalla clonazione o deduplica ONTAP viene perso. È possibile rieseguire la deduplica per recuperare questi risparmi.
  - Dopo che LE SDR spostano i VMDK, NetApp consiglia di ricreare gli snapshot nel datastore di origine, poiché lo spazio è altrimenti bloccato dalla VM che è stata spostata.
  - Lo spostamento di VMDK tra datastore sullo stesso aggregato ha pochi benefici e GLI SDR non hanno visibilità su altri carichi di lavoro che potrebbero condividere l'aggregato.

## Host ESXi consigliato e altre impostazioni ONTAP

NetApp ha sviluppato una serie di impostazioni ottimali per l'host ESXi sia per protocolli NFS sia per protocolli a blocchi. Sono inoltre fornite indicazioni specifiche per le impostazioni di multipathing e timeout HBA per un corretto comportamento con ONTAP in base ai test interni di NetApp e VMware.

Questi valori possono essere impostati facilmente utilizzando gli strumenti ONTAP per VMware vSphere: Dal dashboard Riepilogo, fare clic su Modifica impostazioni nel portlet sistemi host o fare clic con il pulsante destro del mouse sull'host in vCenter, quindi accedere a Strumenti ONTAP > Imposta valori consigliati.

Di seguito sono riportate le impostazioni dell'host attualmente consigliate per le versioni 9,8-9,13.

| Impostazione host | Valore consigliato da NetApp | Riavvio richiesto |
|---|---|---|
| **Configurazione avanzata ESXi** | | |
| VMFS3.HardwareAcceleratedLocking | Mantieni predefinito (1) | No |
| VMFS3.EnableBlockDelete | Mantenere l'impostazione predefinita (0), ma può essere modificata se necessario.<br>Per ulteriori informazioni, vedere "Tastiera VMware 2007427" | No |
| VMFS3.EnableVMFS6Unmap | Mantieni predefinito (1)<br>Per ulteriori informazioni, vedere "API VMware vSphere: Integrazione degli array (VAAI)" | No |
| **Impostazioni NFS** | | |

| | | |
|---|---|---|
| NET.TcpipelHeapSize | VSphere 6.0 o versione successiva, impostato su 32.<br>Tutte le altre configurazioni NFS, impostate su 30 | Sì |
| NET.TcpipelHeapMax | Impostato su 512 MB per la maggior parte delle release di vSphere 6.X.<br>Impostare su 1024 MB per 6.5U3, 6.7U3 e 7.0 o versioni successive. | Sì |
| NFS.MaxVolumes | VSphere 6,0 o versioni successive, impostare su 256<br>Tutte le altre configurazioni NFS sono impostate su 64. | No |
| NFS41.MaxVolumes | VSphere 6,0 o versioni successive, impostare su 256. | No |
| NFS.MaxQueueDepth[1] | VSphere 6.0 o versione successiva, impostato su 128 | Sì |
| NFS.HeartbeatMaxFailures | Impostare su 10 per tutte le configurazioni NFS | No |
| NFS.HeartbeatFrequency | Impostato su 12 per tutte le configurazioni NFS | No |
| NFS.HeartbeatTimeout | Impostare su 5 per tutte le configurazioni NFS. | No |
| SunRPC.MaxConnPerIP | VSphere 7,0 o versioni successive, impostare su 128. | No |
| **Impostazioni FC/FCoE** | | |
| Policy di selezione del percorso | Impostare su RR (round robin) quando si utilizzano percorsi FC con ALUA. Impostare su FISSO per tutte le altre configurazioni.<br>L'impostazione di questo valore su RR consente di fornire il bilanciamento del carico in tutti i percorsi attivi/ottimizzati.<br>Il valore FISSO è per le configurazioni precedenti non ALUA e aiuta a prevenire i/o proxy In altre parole, consente di evitare che l'i/o venga collegato all'altro nodo di una coppia ad alta disponibilità (ha) in un ambiente con Data ONTAP in 7-Mode | No |
| Disk.QFullSampleSize | Impostare su 32 per tutte le configurazioni.<br>L'impostazione di questo valore aiuta a prevenire gli errori di i/O. | No |

| | | |
|---|---|---|
| Disk.QFullThreshold | Impostare su 8 per tutte le configurazioni.<br>L'impostazione di questo valore aiuta a prevenire gli errori di i/O. | No |
| Timeout HBA FC Emulex | Utilizzare il valore predefinito. | No |
| Timeout HBA FC QLogic | Utilizzare il valore predefinito. | No |
| **Impostazioni iSCSI** | | |
| Policy di selezione del percorso | Impostare su RR (round robin) per tutti i percorsi iSCSI.<br>L'impostazione di questo valore su RR consente di fornire il bilanciamento del carico in tutti i percorsi attivi/ottimizzati. | No |
| Disk.QFullSampleSize | Impostare su 32 per tutte le configurazioni.<br>L'impostazione di questo valore aiuta a prevenire gli errori di i/O. | No |
| Disk.QFullThreshold | Impostare su 8 per tutte le configurazioni.<br>L'impostazione di questo valore aiuta a prevenire gli errori di i/O. | No |

1 - l'opzione di configurazione avanzata di NFS MaxQueueDepth potrebbe non funzionare come previsto quando si utilizzano VMware vSphere ESXi 7.0.1 e VMware vSphere ESXi 7.0.2. Fare riferimento a. "Tastiera VMware 86331" per ulteriori informazioni.

Gli strumenti ONTAP specificano anche alcune impostazioni predefinite durante la creazione di ONTAP FlexVol Volumes e LUN:

| **Strumento ONTAP** | **Impostazione predefinita** |
|---|---|
| Riserva di Snapshot (-percento-spazio-snapshot) | 0 |
| Riserva frazionaria (-riserva frazionaria) | 0 |
| Access time update (-atime-update) | Falso |
| Readahead minimo (-min-readahead) | Falso |
| Istantanee pianificate | Nessuno |
| Efficienza dello storage | Attivato |
| Garanzia di volume | Nessuno (con thin provisioning) |
| Dimensionamento automatico del volume | grow_shrink |
| Prenotazione di spazio LUN | Disattivato |
| Allocazione dello spazio del LUN | Attivato |

#### Impostazioni multipath per performance superiori

Sebbene non sia attualmente configurato dagli strumenti ONTAP disponibili, NetApp suggerisce le seguenti opzioni di configurazione:

- In ambienti dalle performance elevate o quando si testano le performance con un singolo datastore LUN, si consiglia di modificare l'impostazione del bilanciamento del carico del criterio di selezione del percorso (PSP) round-robin (VMW_PSP_RR) dall'impostazione IOPS predefinita di 1000 a un valore di 1. Consulta la Knowledge base di VMware "2069356" per ulteriori informazioni.
- In vSphere 6.7 Update 1, VMware ha introdotto un nuovo meccanismo di bilanciamento del carico di latenza per la PSP Round Robin. La nuova opzione prende in considerazione la larghezza di banda i/o e la latenza del percorso quando si seleziona il percorso ottimale per i/O. Potresti trarre vantaggio dall'utilizzo in ambienti con una connettività di percorso non equivalente, ad esempio casi in cui sono presenti più hop di rete su un percorso piuttosto che su un altro, o quando utilizzi un sistema NetApp All SAN Array. Vedere "Plug-in e policy per la selezione del percorso" per ulteriori informazioni.

#### Documentazione aggiuntiva

Per FCP e iSCSI con vSphere 7, è possibile trovare ulteriori dettagli all'indirizzo "Utilizzo di VMware vSphere 7.x con ONTAP"
Per FCP e iSCSI con vSphere 8, è possibile trovare ulteriori dettagli all'indirizzo "Utilizzo di VMware vSphere 8.x con ONTAP"
Per NVMe-of con vSphere 7, è possibile trovare ulteriori dettagli all'indirizzo "Per NVMe-of, ulteriori dettagli sono disponibili nella pagina NVMe-of host Configuration per ESXi 7.x con ONTAP"
Per NVMe-of con vSphere 8, è possibile trovare ulteriori dettagli all'indirizzo "Per NVMe-of, ulteriori dettagli sono disponibili nella pagina NVMe-of host Configuration per ESXi 8.x con ONTAP"

# Volumi virtuali (vVol) con ONTAP

## Panoramica

ONTAP è stata una soluzione storage leader per gli ambienti VMware vSphere da oltre vent'anni e continua ad aggiungere funzionalità innovative per semplificare la gestione e ridurre i costi.

Questo documento tratta le funzionalità di ONTAP per i volumi virtuali VMware vSphere (vVol), incluse le informazioni più recenti sui prodotti e i casi di utilizzo, oltre a Best practice e altre informazioni per semplificare l'implementazione e ridurre gli errori.

Questa documentazione sostituisce i report tecnici precedentemente pubblicati *TR-4400: Volumi virtuali VMware vSphere (vVol) con ONTAP*

Le Best practice integrano altri documenti come guide ed elenchi di compatibilità. Sono sviluppati in base a test di laboratorio e a un'ampia esperienza sul campo da parte di tecnici e clienti NetApp. Potrebbero non essere le uniche pratiche che funzionano o sono supportate, ma sono generalmente le soluzioni più semplici che soddisfano le esigenze della maggior parte dei clienti.

Questo documento è stato aggiornato per includere le nuove funzionalità vVol di vSphere 8.0 update 1, supportate con la release 9.12 di ONTAP Tools.

### Panoramica dei volumi virtuali (vVol)

Nel 2012, NetApp ha iniziato a collaborare con VMware per supportare le API vSphere per la consapevolezza dello storage (VASA) per vSphere 5. Questo primo provider VASA consentiva la definizione delle funzionalità di storage in un profilo che poteva essere utilizzato per filtrare i datastore durante il provisioning e per verificare successivamente la conformità con la policy. Nel corso del tempo, questo si è evoluto per aggiungere nuove funzionalità per consentire una maggiore automazione nel provisioning, oltre all'aggiunta di volumi virtuali o vVol, in cui i singoli oggetti storage vengono utilizzati per i file delle macchine virtuali e i dischi virtuali. Questi oggetti potrebbero essere LUN, file, e ora con vSphere 8 - NVMe namespaces.NetApp ha lavorato a stretto contatto con VMware come partner di riferimento per vVol rilasciato con vSphere 6 nel 2015, e ancora come partner di progettazione per vVol utilizzando NVMe su fabric in vSphere 8. NetApp continua a migliorare vVol per sfruttare le più recenti funzionalità di ONTAP.

Esistono diversi componenti di cui tenere conto:

| **Provider VASA** |
| --- |
| Questo è il componente software che gestisce la comunicazione tra VMware vSphere e il sistema storage. Per ONTAP, il provider VASA viene eseguito in un'appliance nota come tool ONTAP per VMware vSphere (in breve, strumenti ONTAP). Gli strumenti ONTAP includono anche un plugin vCenter, un adattatore per la replica dello storage (SRA) per VMware Site Recovery Manager e un server API REST per la creazione di automazione. Una volta configurati e registrati gli strumenti ONTAP con vCenter, non è più necessario interagire direttamente con il sistema ONTAP, poiché quasi tutte le esigenze di storage possono essere gestite direttamente dall'interfaccia utente di vCenter o tramite l'automazione delle API REST. |
| **Protocol Endpoint (PE)** |
| L'endpoint del protocollo è un proxy per i/o tra gli host ESXi e il datastore vVols. Il provider ONTAP VASA crea automaticamente questi elementi, scegliendo una LUN endpoint di protocollo (4MB GB) per volume FlexVol del datastore vVol o un punto di montaggio NFS per interfaccia NFS (LIF) sul nodo storage che ospita un volume FlexVol nel datastore. L'host ESXi monta questi endpoint di protocollo direttamente piuttosto che singoli LUN vVol e file di dischi virtuali. Non è necessario gestire gli endpoint del protocollo poiché vengono creati, montati, rimossi ed eliminati automaticamente dal provider VASA, insieme a eventuali gruppi di interfacce o policy di esportazione necessari. |
| **Virtual Protocol Endpoint (VPE)** |
| Novità di vSphere 8: Quando si utilizza NVMe over Fabrics (NVMe-of) con vVol, il concetto di endpoint del protocollo non è più rilevante in ONTAP. Al contrario, l'host ESXi crea automaticamente un'istanza di PE virtuale per ciascun gruppo ANA non appena viene accesa la prima macchina virtuale. ONTAP crea automaticamente gruppi ANA per ogni volume FlexVol utilizzato dall'archivio dati.<br><br>Un ulteriore vantaggio dell'utilizzo di NVMe-of per vVol è che non sono richieste di bind da parte del provider VASA. L'host ESXi gestisce invece la funzionalità di binding vVol internamente in base a VPE. In questo modo si riduce l'opportunità di un vVol bind storm di impatto sul servizio.<br><br>Per ulteriori informazioni, vedere "NVMe e volumi virtuali" acceso "vmware.com" |
| **Archivio dati volume virtuale** |

| |
|---|
| Il datastore del volume virtuale è una rappresentazione logica del datastore di un container vVol creato e gestito da un provider VASA. Il container rappresenta un pool di capacità di storage fornito dai sistemi storage gestiti dal provider VASA. Gli strumenti ONTAP supportano l'allocazione di più volumi FlexVol (noti come volumi di backup) a un singolo datastore vVols e questi datastore vVols possono estendersi su più nodi in un cluster ONTAP, combinando sistemi flash e ibridi con funzionalità diverse. L'amministratore può creare nuovi volumi FlexVol utilizzando la procedura guidata di provisioning o l'API REST oppure selezionare volumi FlexVol pre-creati per il backup dello storage, se disponibili. |
| **Volumi virtuali (vVol)** |
| I vVol sono i file e i dischi della macchina virtuale memorizzati nel datastore vVols. Il termine vVol (singolo) si riferisce a un singolo file, LUN o namespace specifico. ONTAP crea spazi dei nomi NVMe, LUN o file a seconda del protocollo utilizzato dal datastore. Esistono diversi tipi distinti di vVol; i più comuni sono Config (file di metadati), Data (disco virtuale o VMDK) e Swap (creato all'accensione della macchina virtuale). I vVol protetti dalla crittografia delle macchine virtuali VMware sono di tipo Altro. La crittografia di VMware VM non deve essere confusa con la crittografia aggregata o del volume ONTAP. |

**Gestione basata su criteri**

Le API VMware vSphere per la consapevolezza dello storage (VASA) semplificano l'utilizzo da parte di un amministratore delle macchine virtuali delle funzionalità di storage necessarie per il provisioning delle macchine virtuali senza dover interagire con il proprio team di storage. Prima di VASA, gli amministratori delle macchine virtuali potevano definire le policy di storage delle macchine virtuali, ma dovevano collaborare con gli amministratori dello storage per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o le convenzioni di denominazione. Con VASA, gli amministratori di vCenter con le autorizzazioni appropriate possono definire una serie di funzionalità di storage che gli utenti di vCenter possono utilizzare per eseguire il provisioning delle macchine virtuali. La mappatura tra policy di storage delle macchine virtuali e profilo di funzionalità di storage del datastore consente a vCenter di visualizzare un elenco di datastore compatibili per la selezione, nonché di abilitare altre tecnologie come aria (precedentemente nota come vRealize) Automation o Tanzu Kubernetes Grid per selezionare automaticamente lo storage da una policy assegnata. Questo approccio è noto come gestione basata su criteri di storage. Anche se i profili e le policy delle funzionalità di storage possono essere utilizzati anche con i datastore tradizionali, la nostra attenzione qui è dedicata agli archivi dati vVols.

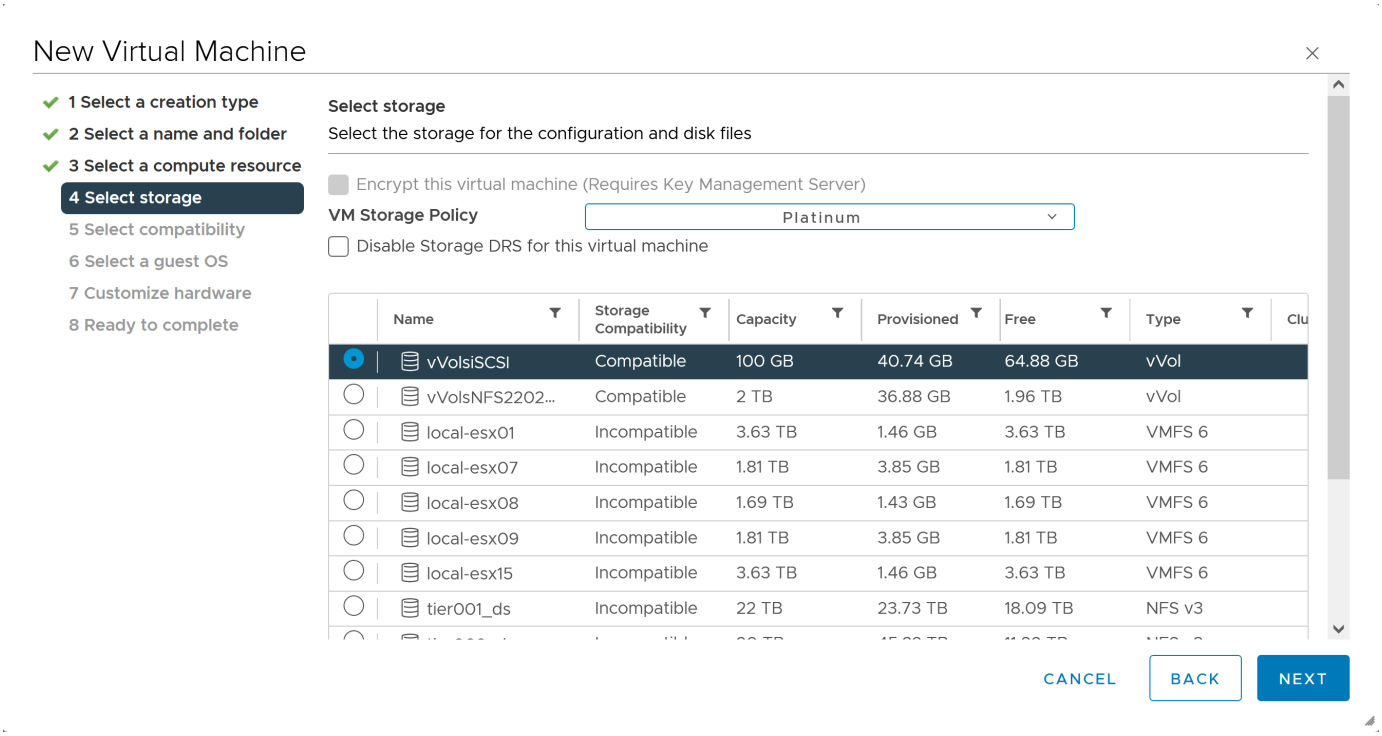
Esistono due elementi:

| |
|---|
| **Storage Capability Profile (SCP)** |
| Un SCP (Storage Capability Profile) è un modello di storage che consente all'amministratore di vCenter di definire le funzionalità di storage necessarie senza dover comprendere come gestire tali funzionalità in ONTAP. Adottando un approccio basato su modelli, l'amministratore può fornire facilmente servizi di storage in modo coerente e prevedibile. Le funzionalità descritte in un SCP includono performance, protocollo, efficienza dello storage e altre funzionalità. Le funzionalità specifiche variano in base alla versione. Vengono creati utilizzando il menu ONTAP Tools per VMware vSphere all'interno dell'interfaccia utente di vCenter. È inoltre possibile utilizzare le API REST per creare SCP. Possono essere creati manualmente selezionando singole funzionalità o generati automaticamente da datastore esistenti (tradizionali). |
| **Criterio di storage delle macchine virtuali** |
| I criteri di storage delle macchine virtuali vengono creati in vCenter in Criteri e profili. Per i vVol, creare un set di regole utilizzando le regole del provider del tipo di storage NetApp vVols. Gli strumenti di ONTAP offrono un approccio semplificato, consentendo di selezionare semplicemente un SCP piuttosto che obbligare a specificare singole regole. |

Come indicato in precedenza, l'utilizzo delle policy consente di ottimizzare l'attività di provisioning di un

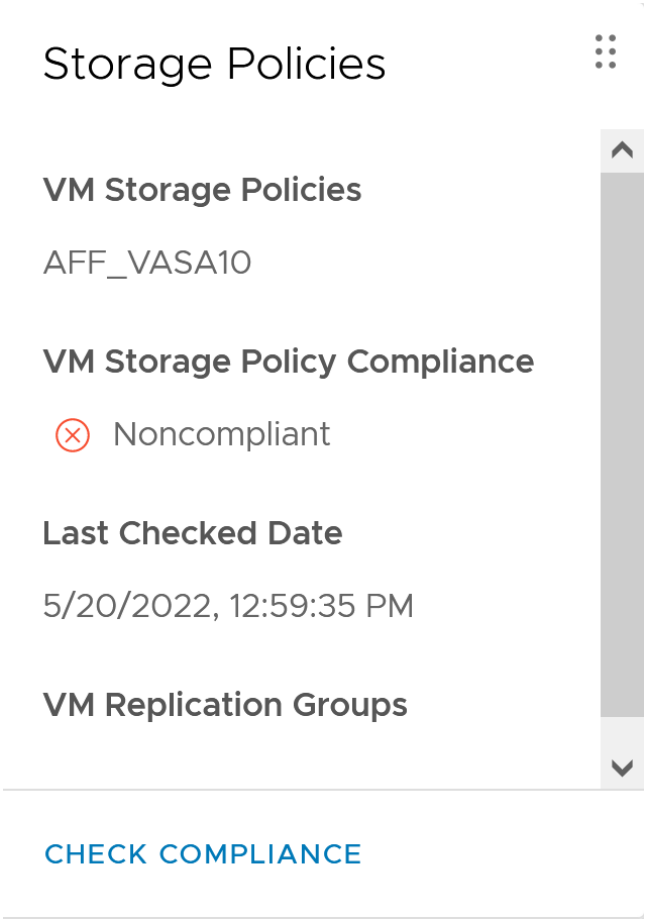
volume. È sufficiente selezionare una policy appropriata e il provider VASA mostrerà gli archivi dati vVol che supportano tale policy e inserirà vVol in un singolo volume FlexVol conforme (Figura 1).

**Implementare la macchina virtuale utilizzando i criteri di storage**




Una volta eseguito il provisioning di una macchina virtuale, il provider VASA continua a controllare la conformità e avvisa l'amministratore della macchina virtuale con un allarme in vCenter quando il volume di backup non è più conforme al criterio (Figura 2).

**Conformità delle policy di storage delle macchine virtuali**




### Supporto vVol NetApp

ONTAP ha supportato la specifica VASA dalla sua versione iniziale nel 2012. Sebbene altri sistemi storage NetApp possano supportare VASA, questo documento si concentra sulle versioni attualmente supportate di ONTAP 9.

#### ONTAP

Oltre a ONTAP 9 su sistemi AFF, ASA e FAS, NetApp supporta i carichi di lavoro VMware su ONTAP Select, Amazon FSX per NetApp con VMware Cloud su AWS, la soluzione Azure NetApp Files con Azure VMware, Cloud Volumes Service con Google Cloud VMware Engine e NetApp Private Storage in Equinix, tuttavia, le funzionalità specifiche possono variare in base al provider di servizi e alla connettività di rete disponibile. È inoltre disponibile l'accesso dai guest vSphere ai dati memorizzati in tali configurazioni e a Cloud Volumes ONTAP.

Al momento della pubblicazione, gli ambienti hyperscaler sono limitati solo agli archivi dati NFS v3 tradizionali, pertanto i vVol sono disponibili solo con sistemi ONTAP on-premise o con sistemi connessi al cloud che offrono la funzionalità completa di sistemi on-premise come quelli ospitati da partner e provider di servizi NetApp in tutto il mondo.

*Per ulteriori informazioni su ONTAP, vedere "Documentazione del prodotto ONTAP"*

*Per ulteriori informazioni sulle Best practice di ONTAP e VMware vSphere, vedere "TR-4597"*

### Vantaggi dell'utilizzo di vVol con ONTAP

Quando VMware ha introdotto il supporto vVol con VASA 2.0 nel 2015, lo ha descritto come "un framework di

integrazione e gestione che offre un nuovo modello operativo per lo storage esterno (SAN/NAS)". Questo modello operativo offre diversi vantaggi insieme allo storage ONTAP.

#### Gestione basata su criteri

Come descritto nella sezione 1,2, la gestione basata su criteri consente di eseguire il provisioning delle macchine virtuali e di gestirle successivamente utilizzando criteri predefiniti. Questo può aiutare le operazioni IT in diversi modi:

- **Aumentare la velocità.** i tool ONTAP eliminano il requisito per l'amministratore di vCenter di aprire i ticket con il team di storage per le attività di provisioning dello storage. Tuttavia, i ruoli RBAC dei tool ONTAP in vCenter e nel sistema ONTAP consentono ancora ai team indipendenti (come i team di storage) o alle attività indipendenti dello stesso team limitando l'accesso a funzioni specifiche, se necessario.
- **Provisioning più intelligente.** le funzionalità del sistema di storage possono essere esposte attraverso le API VASA, consentendo ai flussi di lavoro di provisioning di sfruttare funzionalità avanzate senza che l'amministratore delle macchine virtuali debba comprendere come gestire il sistema di storage.
- **Provisioning più rapido.** diverse funzionalità di storage possono essere supportate in un singolo datastore e selezionate automaticamente in base alla policy della macchina virtuale.
- **Evitare errori.** le policy di storage e macchine virtuali vengono sviluppate in anticipo e applicate in base alle necessità senza dover personalizzare lo storage ogni volta che viene eseguito il provisioning di una macchina virtuale. Gli allarmi di compliance vengono generati quando le funzionalità dello storage si scostano dalle policy definite. Come accennato in precedenza, gli SCP rendono il provisioning iniziale prevedibile e ripetibile, mentre basare le policy di storage delle macchine virtuali sugli SCP garantisce un posizionamento preciso.
- **Migliore gestione della capacità.** i tool VASA e ONTAP consentono di visualizzare la capacità dello storage fino al livello di aggregato induviale, se necessario, e di fornire più livelli di avviso nel caso in cui la capacità inizi a diminuire.

#### Gestione granulare delle macchine virtuali nella moderna SAN

I sistemi storage SAN che utilizzano Fibre Channel e iSCSI sono stati i primi ad essere supportati da VMware per ESX, ma non hanno la capacità di gestire singoli file e dischi VM dal sistema storage. Al contrario, vengono forniti i LUN e VMFS gestisce i singoli file. Questo rende difficile per il sistema storage gestire direttamente le performance, la clonazione e la protezione dello storage delle singole macchine virtuali. VVol offre una granularità dello storage di cui già godono i clienti che utilizzano lo storage NFS, con le solide funzionalità SAN ad alte performance di ONTAP.

Ora, con gli strumenti vSphere 8 e ONTAP per VMware vSphere 9.12 e versioni successive, gli stessi controlli granulari utilizzati da vVol per i protocolli basati su SCSI legacy sono ora disponibili nella MODERNA SAN Fibre Channel che utilizza NVMe over Fabrics per ottenere performance ancora maggiori su larga scala. Con vSphere 8.0 update 1, è ora possibile implementare una soluzione NVMe end-to-end completa utilizzando vVol senza alcuna traduzione i/o nello stack di storage dell'hypervisor.

#### Maggiori funzionalità di offload dello storage

Mentre VAAI offre una varietà di operazioni che vengono trasferite allo storage, ci sono alcune lacune che vengono affrontate dal provider VASA. SAN VAAI non è in grado di trasferire le snapshot gestite da VMware al sistema storage. NFS VAAI è in grado di trasferire le snapshot gestite da macchine virtuali, ma esistono dei limiti per una macchina virtuale con snapshot native dello storage. Poiché i vVol utilizzano LUN, spazi dei nomi o file singoli per i dischi delle macchine virtuali, ONTAP può clonare in modo rapido ed efficiente i file o le LUN per creare snapshot granulari delle macchine virtuali che non richiedono più file delta. Inoltre, NFS VAAI non supporta operazioni di offload dei cloni per le migrazioni vMotion di storage a caldo (attivate). La macchina virtuale deve essere spenta per consentire l'offload della migrazione quando si utilizza VAAI con datastore

NFS tradizionali. Il provider VASA negli strumenti ONTAP consente cloni quasi istantanei ed efficienti in termini di storage per le migrazioni a caldo e a freddo e supporta anche copie quasi istantanee per le migrazioni tra volumi di vVol. Grazie a questi significativi vantaggi in termini di efficienza dello storage, è possibile sfruttare al meglio i carichi di lavoro vVol in base a. "Garanzia di efficienza" programma. Allo stesso modo, se i cloni cross-volume con VAAI non soddisfano i tuoi requisiti, sarai in grado di risolvere le sfide per il tuo business grazie ai miglioramenti nell'esperienza di copia con i vVol.

#### Casi di utilizzo comuni per i vVol

Oltre a questi vantaggi, vediamo anche questi casi di utilizzo comuni per lo storage vVol:

- **Provisioning su richiesta delle VM**
  - Cloud privato o provider di servizi IaaS.
  - Sfrutta l'automazione e l'orchestrazione tramite la suite aria (in precedenza vRealize), OpenStack, ecc.
- **Dischi di prima classe (FCD)**
  - VMware Tanzu Kubernetes Grid [TKG] volumi persistenti.
  - Fornire servizi di Amazon EBS attraverso una gestione indipendente del ciclo di vita VMDK.
- **Provisioning on-demand delle macchine virtuali temporanee**
  - Laboratori di test/sviluppo
  - Ambienti di training

#### Vantaggi comuni con vVol

Se utilizzato a pieno vantaggio, come nei casi di utilizzo precedenti, i vVol forniscono i seguenti miglioramenti specifici:

- I cloni vengono creati rapidamente all'interno di un singolo volume o su più volumi in un cluster ONTAP, un vantaggio rispetto ai cloni abilitati VAAI tradizionali. Sono inoltre efficienti in termini di storage. I cloni all'interno di un volume utilizzano il clone del file ONTAP, simile ai volumi FlexClone, e memorizzano solo le modifiche dal file/LUN/namespace vVol di origine. In questo modo, le macchine virtuali a lungo termine per la produzione o altri scopi applicativi vengono create rapidamente, occupano poco spazio e possono beneficiare della protezione a livello di macchine virtuali (utilizzando il plug-in NetApp SnapCenter per VMware vSphere, le snapshot gestite da VMware o il backup VADP) e della gestione delle performance (con QoS ONTAP).
- I vVol sono la tecnologia di storage ideale quando si utilizza TKG con vSphere CSI, fornendo classi di storage e capacità discrete gestite dall'amministratore di vCenter.
- Amazon EBS-like Services può essere fornito attraverso FCD perché un FCD VMDK, come suggerisce il nome, è un cittadino di prima classe in vSphere e ha un ciclo di vita che può essere gestito in modo indipendente separato dalle macchine virtuali a cui potrebbe essere collegato.

## Utilizzo di vVol con ONTAP

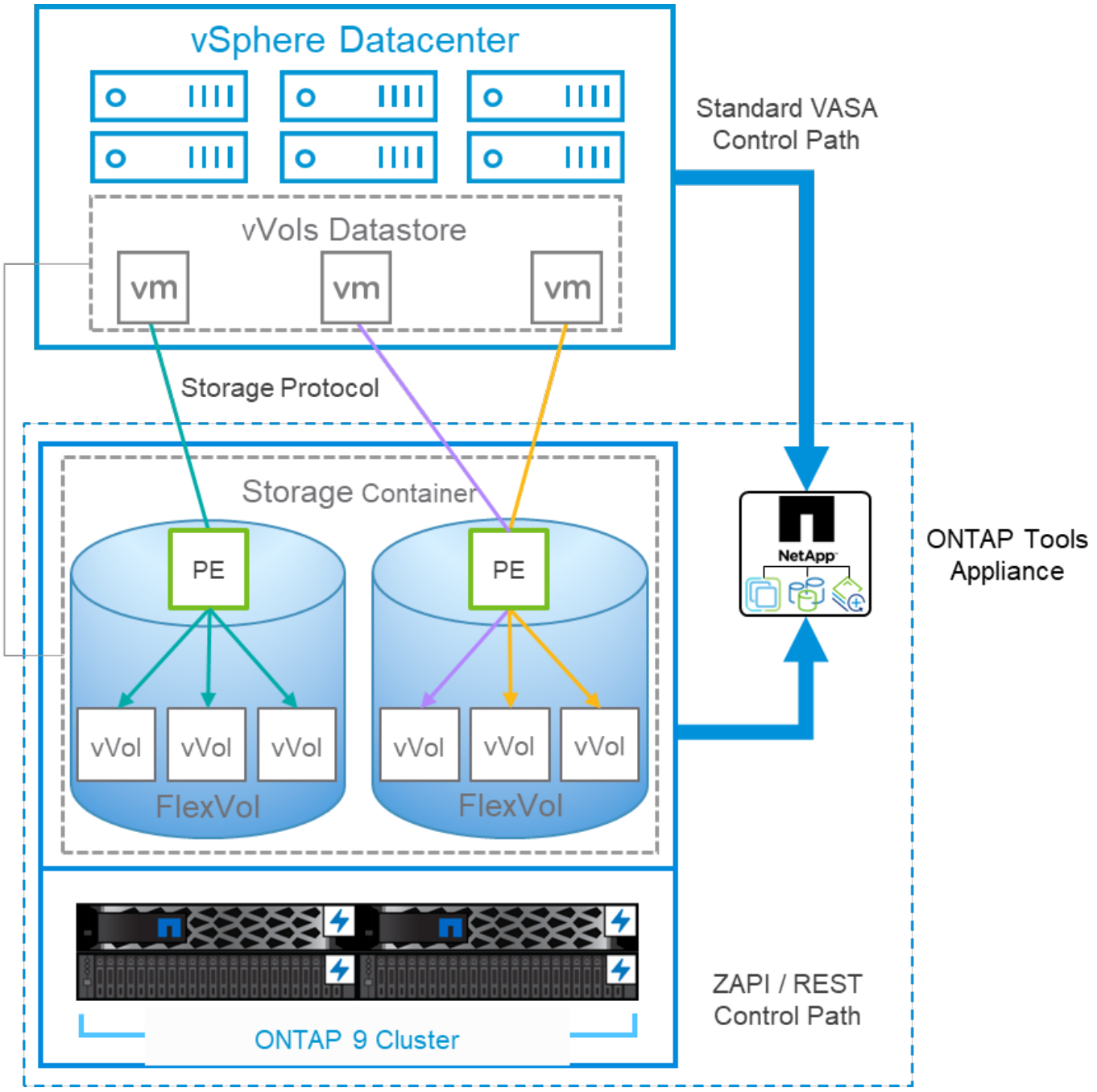
La chiave per utilizzare vVol con ONTAP è il software del provider VASA incluso negli strumenti ONTAP per l'appliance virtuale VMware vSphere.

Gli strumenti ONTAP includono anche le estensioni dell'interfaccia utente di vCenter, il server REST API, l'adattatore di replica dello storage per VMware Site Recovery Manager, i tool di monitoraggio e configurazione degli host e una serie di report che consentono di gestire al meglio l'ambiente VMware.

### Prodotti e documentazione

La licenza FlexClone di ONTAP (inclusa in ONTAP One) e l'appliance ONTAP Tools sono gli unici prodotti aggiuntivi necessari per utilizzare vVol con ONTAP. Le release recenti dei tool ONTAP sono fornite come singola appliance unificata che viene eseguita su ESXi, fornendo le funzionalità di quelle che in precedenza erano tre appliance e server diversi. Per i vVol, è importante utilizzare le estensioni dell'interfaccia utente di vCenter o LE API REST degli strumenti ONTAP come strumenti di gestione generali e interfacce utente per le funzioni ONTAP con vSphere, insieme al provider VASA che fornisce funzionalità vVol specifiche. Il componente SRA è incluso per gli archivi dati tradizionali, ma VMware Site Recovery Manager non utilizza SRA per vVol, implementando invece nuovi servizi in SRM 8.3 e versioni successive che sfruttano il provider VASA per la replica di vVol.

#### ONTAP Tools architettura del provider VASA quando si utilizza iSCSI o FCP



#### Installazione del prodotto

Per le nuove installazioni, implementa l'appliance virtuale nel tuo ambiente vSphere. Le versioni correnti dei tool ONTAP si registreranno automaticamente con vCenter e abiliteranno il provider VASA per impostazione predefinita. Oltre alle informazioni su host ESXi e vCenter Server, sono necessari anche i dettagli di configurazione dell'indirizzo IP per l'appliance. Come indicato in precedenza, il provider VASA richiede che la licenza FlexClone di ONTAP sia già installata su qualsiasi cluster ONTAP che si intende utilizzare per vVol. L'appliance dispone di un watchdog integrato per garantire la disponibilità e, come Best practice, deve essere configurata con le funzionalità VMware High Availability e, facoltativamente, Fault Tolerance. Per ulteriori dettagli, vedere la sezione 4.1. Non installare o spostare l'appliance ONTAP Tools o l'appliance vCenter Server (VCSA) sullo storage vVol, in quanto ciò potrebbe impedire il riavvio delle appliance.

Gli aggiornamenti in-place dei tool ONTAP sono supportati utilizzando il file ISO di aggiornamento disponibile per il download sul sito del supporto NetApp (NSS). Per aggiornare l'appliance, seguire le istruzioni della Guida all'installazione e alla distribuzione.

Per il dimensionamento dell'appliance virtuale e la comprensione dei limiti di configurazione, consultare questo articolo della Knowledge base: "Guida al dimensionamento degli strumenti ONTAP per VMware vSphere"

#### Documentazione del prodotto

La seguente documentazione è disponibile per facilitare l'implementazione degli strumenti ONTAP.

"Per il repository completo della documentazione;#44; visitare questo link a docs.netapp.com"

### Inizia subito

- "Note di rilascio"
- "Scopri i tool ONTAP per VMware vSphere"
- "ONTAP Tools Avvio rapido"
- "Implementare gli strumenti ONTAP"
- "Aggiornare i tool ONTAP"

### Utilizzare gli strumenti ONTAP

- "Provisioning di datastore tradizionali"
- "Provisioning degli archivi dati vVol"
- "Configurare il controllo degli accessi in base al ruolo"
- "Configurare la diagnostica remota"
- "Configurare la disponibilità elevata"

### Proteggere e gestire i datastore

- "Proteggere i datastore tradizionali" Con SRM
- "Proteggere le macchine virtuali basate su vVol" Con SRM
- "Monitoraggio di datastore e macchine virtuali tradizionali"
- "Monitorare datastore e macchine virtuali di vVol"

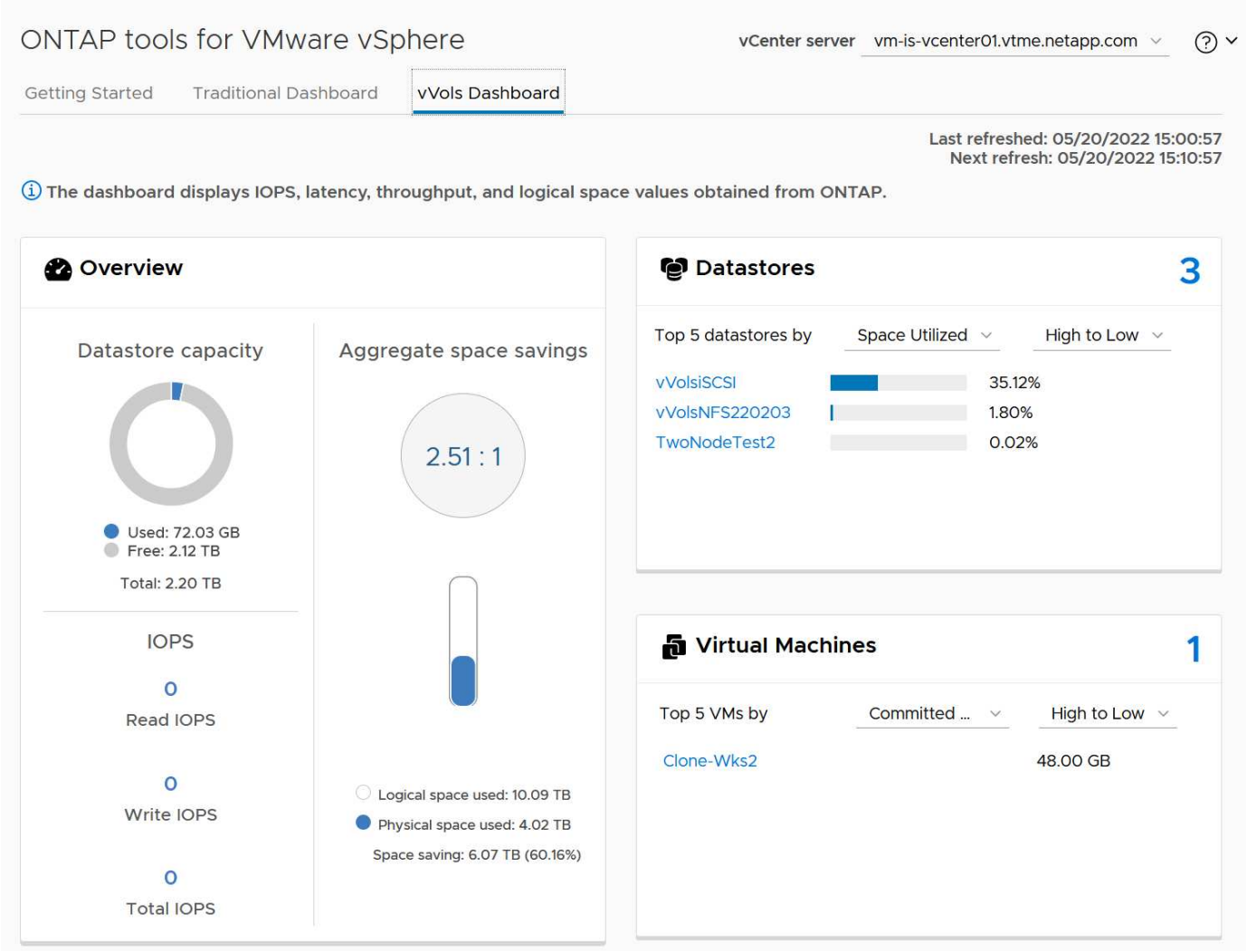
Oltre alla documentazione del prodotto, sono disponibili articoli della Knowledge base di supporto che potrebbero essere utili.

- "Come eseguire un Disaster Recovery provider VASA - Guida alla risoluzione"

#### Dashboard del provider VASA

Il provider VASA include una dashboard con informazioni su performance e capacità per le singole VM vVol. Queste informazioni provengono direttamente da ONTAP per i file vVol e le LUN, tra cui latenza, IOPS, throughput e uptime per le prime 5 macchine virtuali, latenza e IOPS per i primi 5 datastore. Questa opzione è attivata per impostazione predefinita quando si utilizza ONTAP 9.7 o versione successiva. Il recupero e la visualizzazione dei dati iniziali nella dashboard possono richiedere fino a 30 minuti.

### Dashboard di ONTAP Tools vVol




### Best Practice

L'utilizzo di ONTAP vVol con vSphere è semplice e segue i metodi vSphere pubblicati (per la versione di ESXi in uso, vedere utilizzo dei volumi virtuali in vSphere Storage nella documentazione VMware). Di seguito sono riportate alcune procedure aggiuntive da prendere in considerazione in combinazione con ONTAP.

### Limiti

In generale, ONTAP supporta i limiti vVol definiti da VMware (vedere pubblicato "Valori massimi di configurazione"). La seguente tabella riassume i limiti ONTAP specifici in termini di dimensione e numero di vVol. Controllare sempre "NetApp Hardware Universe" Per i limiti aggiornati su numeri e dimensioni di LUN e

file.

**Limiti di ONTAP vVol**

| Capacità/funzionalità | SAN (SCSI o NVMe-of) | NFS |
|---|---|---|
| Dimensione massima vVol | 62 TIB* | 62 TIB* |
| Numero massimo di vVol per volume FlexVol | 1024 | 2 miliardi |
| Numero massimo di vVol per nodo ONTAP | Fino a 12,288** | 50 miliardi di dollari |
| Numero massimo di vVol per coppia ONTAP | Fino a 24.576** | 50 miliardi di dollari |
| Numero massimo di vVol per cluster ONTAP | Fino a 98.304** | Nessun limite specifico del cluster |
| Numero massimo di oggetti QoS (gruppo di policy condiviso e livello di servizio vVol singolo) | Da 12,000 a ONTAP 9.3; 40,000 con ONTAP 9.4 e versioni successive | |

- Limite di dimensione basato sui sistemi ASA o AFF e FAS con ONTAP 9.12.1P2 e versioni successive.
  - Il numero di vVol SAN (NVMe namespace o LUN) varia in base alla piattaforma. Controllare sempre "NetApp Hardware Universe" Per i limiti aggiornati su numeri e dimensioni di LUN e file.

**Utilizzare i tool ONTAP per le estensioni dell'interfaccia utente di VMware vSphere o le API REST per eseguire il provisioning degli archivi dati vVol e degli endpoint del protocollo.**

Anche se è possibile creare datastore vVol con l'interfaccia generale vSphere, utilizzando i tool ONTAP sarà possibile creare automaticamente gli endpoint del protocollo in base alle necessità, e creare volumi FlexVol utilizzando le Best practice ONTAP e in conformità con i profili di funzionalità dello storage definiti. È sufficiente fare clic con il pulsante destro del mouse sull'host/cluster/data center, quindi selezionare *ONTAP tools* e *provisioning datastore*. Da qui, è sufficiente scegliere le opzioni vVol desiderate nella procedura guidata.

**Non memorizzare mai l'appliance ONTAP Tools o l'appliance vCenter Server (VCSA) su un datastore vVol gestito.**

Questo può causare una "situazione a base di uova e pollo" se occorre riavviare le appliance perché non saranno in grado di ricollegare i propri vVol durante il riavvio. È possibile memorizzarli in un datastore vVol gestito da un diverso tool ONTAP e da una distribuzione vCenter.

**Evitare le operazioni vVol in diverse release di ONTAP.**

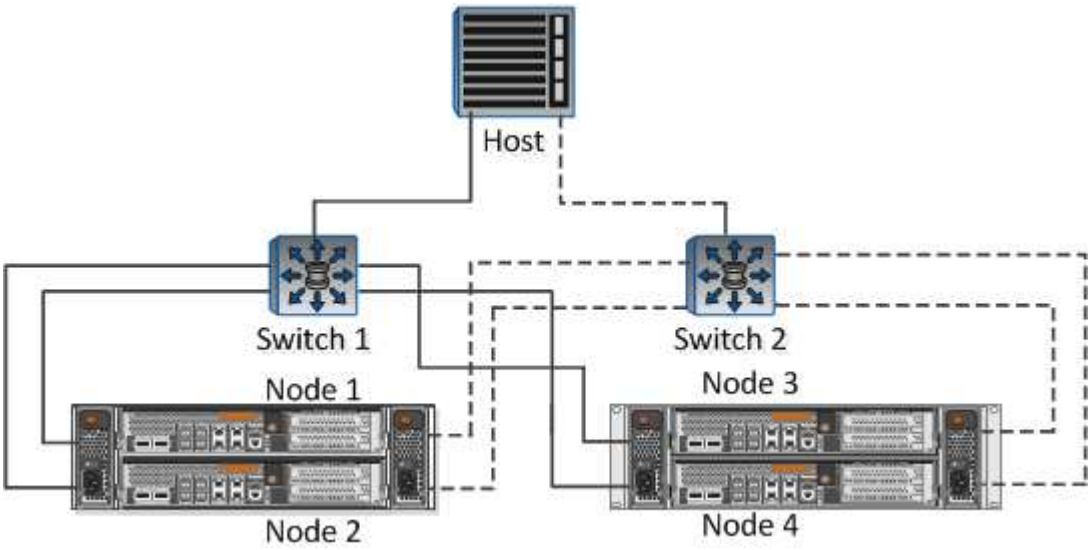
Le funzionalità di storage supportate, come QoS, personalità e molto altro, sono cambiate in varie versioni del provider VASA e alcune dipendono dalla release di ONTAP. L'utilizzo di release diverse in un cluster ONTAP o lo spostamento di vVol tra cluster con release diverse può causare comportamenti imprevisti o allarmi di compliance.

**Prima di utilizzare NVMe/FC o FCP per i vVol, è necessario eseguire un'area del fabric Fibre Channel.**

Il provider ONTAP Tools VASA si occupa della gestione degli igroup FCP e iSCSI, nonché dei sottosistemi NVMe in ONTAP in base agli iniziatori rilevati degli host ESXi gestiti. Tuttavia, non si integra con gli switch Fibre Channel per gestire lo zoning. Lo zoning deve essere eseguito in base alle Best practice prima di eseguire qualsiasi provisioning. Di seguito è riportato un esempio di zoning a initiator singolo per quattro

sistemi ONTAP:

Zoning a initiator singolo:




Fare riferimento ai seguenti documenti per ulteriori Best practice:

"*TR-4080 Best practice per la MODERNA SAN ONTAP 9*"

"*TR-4684 implementazione e configurazione delle moderne SAN con NVMe-of*"

**Pianificare FlexVol di supporto in base alle proprie esigenze.**

È consigliabile aggiungere diversi volumi di backup al datastore vVol per distribuire il carico di lavoro nel cluster ONTAP, supportare diverse opzioni di policy o aumentare il numero di LUN o file consentiti. Tuttavia, se è richiesta la massima efficienza dello storage, posizionare tutti i volumi di backup su un singolo aggregato. In alternativa, se sono richieste le massime prestazioni di cloning, prendere in considerazione l'utilizzo di un singolo volume FlexVol e la conservazione dei modelli o della libreria di contenuti nello stesso volume. Il provider VASA trasferisce molte operazioni di storage vVol a ONTAP, tra cui migrazione, cloning e snapshot. Quando questa operazione viene eseguita all'interno di un singolo volume FlexVol, vengono utilizzati cloni di file efficienti in termini di spazio e sono quasi immediatamente disponibili. Quando questo viene eseguito su volumi FlexVol, le copie sono rapidamente disponibili e utilizzano la deduplica e la compressione inline, ma la massima efficienza dello storage potrebbe non essere ripristinata fino a quando i processi in background non vengono eseguiti su volumi che utilizzano la deduplica e la compressione in background. A seconda dell'origine e della destinazione, un certo livello di efficienza potrebbe risultare degradato.

**Mantieni semplici gli SCP (Storage Capability Profiles).**

Evitare di specificare le funzionalità non necessarie impostandole su nessuna. In questo modo si riducono al minimo i problemi durante la selezione o la creazione di volumi FlexVol. Ad esempio, con il provider VASA 7.1 e versioni precedenti, se la compressione viene lasciata all'impostazione SCP predefinita No, tenterà di disattivare la compressione, anche su un sistema AFF.

**Utilizzare gli SCP predefiniti come modelli di esempio per creare i propri.**

Gli SCP inclusi sono adatti per la maggior parte degli usi generici, ma i requisiti potrebbero essere diversi.

**Prendere in considerazione l'utilizzo di IOPS massimi per controllare macchine virtuali sconosciute o di test.**

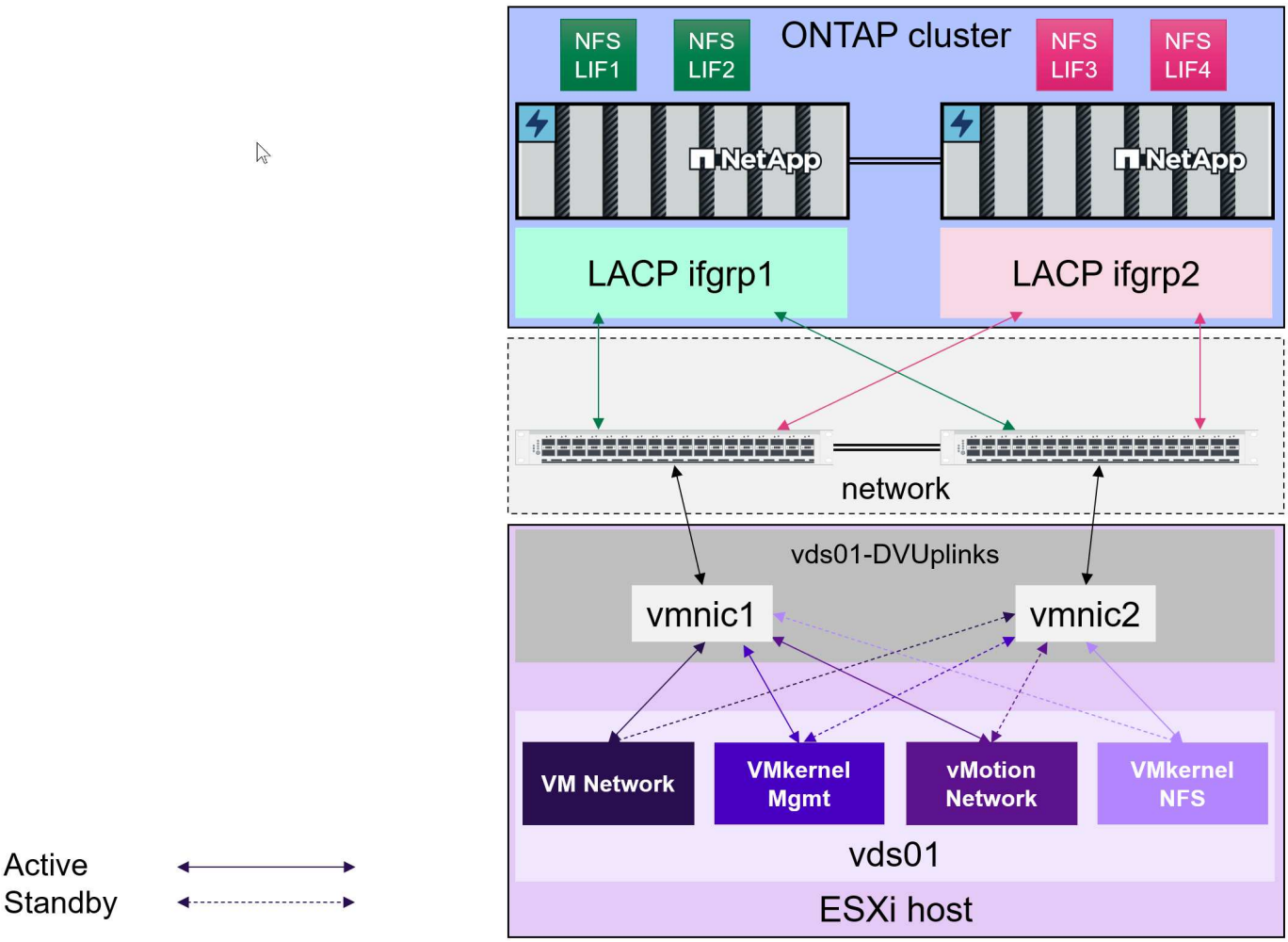
Per la prima volta disponibile nel provider VASA 7.1, è possibile utilizzare il massimo IOPS per limitare gli IOPS a un vVol specifico per un carico di lavoro sconosciuto, in modo da evitare impatti su altri carichi di lavoro più critici. Per ulteriori informazioni sulla gestione delle performance, vedere la Tabella 4.

**Assicurarsi di disporre di LIF di dati sufficienti.**
Creare almeno due LIF per nodo per coppia ha. In base al carico di lavoro, potrebbe essere necessario un numero maggiore di risorse.

**Seguire tutte le Best practice del protocollo.**

Fare riferimento alle altre guide alle Best practice di NetApp e VMware specifiche per il protocollo selezionato. In generale, non vi sono modifiche diverse da quelle già menzionate.

**Esempio di configurazione di rete utilizzando vVol su NFS v3**




## Implementazione dello storage vVol

La creazione dello storage vVol per le macchine virtuali prevede diversi passaggi.

I primi due passaggi potrebbero non essere necessari per un ambiente vSphere esistente che utilizza ONTAP per i datastore tradizionali. Potreste già utilizzare strumenti ONTAP per gestire, automatizzare e creare rapporti con il vostro sistema di storage basato su VMFS o su NFS tradizionale. Questi passaggi sono descritti in modo più dettagliato nella sezione seguente.

1. Creare la Storage Virtual Machine (SVM) e la relativa configurazione del protocollo. È possibile selezionare NVMe/FC, NFSv3, NFSv4,1, iSCSI, FCP, o un mix di queste opzioni. È possibile utilizzare le procedure guidate di ONTAP System Manager o la riga di comando della shell del cluster.
    - Almeno un LIF per nodo per ogni connessione switch/fabric. Come Best practice, creare due o più per nodo per i protocolli basati su FCP, iSCSI o NVMe.
    - È possibile creare i volumi in questo momento, ma è più semplice consentire la creazione guidata *Provision Datastore*. L'unica eccezione a questa regola è rappresentata dall'utilizzo della replica vVol con VMware Site Recovery Manager. Questa operazione è più semplice da configurare con volumi FlexVol preesistenti con relazioni SnapMirror esistenti. Prestare attenzione a non abilitare la qualità del servizio su alcun volume da utilizzare per i vVol, in quanto questa operazione deve essere gestita dai tool SPBM e ONTAP.
2. Implementare i tool ONTAP per VMware vSphere utilizzando il software OVA scaricato dal sito del supporto NetApp.
3. Configurare gli strumenti ONTAP per il proprio ambiente.
    - Aggiungere il cluster ONTAP agli strumenti ONTAP in *sistemi storage*
        - Mentre gli strumenti e gli SRA di ONTAP supportano sia le credenziali a livello di cluster che quelle a livello di SVM, il provider VASA supporta solo le credenziali a livello di cluster per i sistemi storage. Ciò è dovuto al fatto che molte delle API utilizzate per i vVol sono disponibili solo a livello di cluster. Pertanto, se intendi utilizzare vVol, devi aggiungere i cluster ONTAP utilizzando credenziali cluster-scoped.
    - Se i dati ONTAP si trovano su sottoreti diverse dagli adattatori VMkernel, è necessario aggiungere le subnet dell'adattatore VMkernel all'elenco delle subnet selezionate nel menu delle impostazioni degli strumenti ONTAP. Per impostazione predefinita, gli strumenti ONTAP proteggono il traffico di storage consentendo solo l'accesso alla subnet locale.
    - Gli strumenti ONTAP sono dotati di diverse policy predefinite che è possibile utilizzare o vedere Gestione delle VM mediante policy Per istruzioni sulla creazione di SCP.
4. Utilizzare il menu *ONTAP tools* di vCenter per avviare la procedura guidata *provisioning datastore*.
5. Fornire un nome significativo e selezionare il protocollo desiderato. È anche possibile fornire una descrizione del datastore.
6. Selezionare uno o più SCP da supportare dal datastore vVols. In questo modo, i sistemi ONTAP che non sono in grado di corrispondere al profilo verranno filtrati. Dall'elenco visualizzato, selezionare il cluster e la SVM desiderati.
7. Utilizzare la procedura guidata per creare nuovi volumi FlexVol per ciascuno degli SCP specificati o utilizzare volumi esistenti selezionando il pulsante di opzione appropriato.
8. Creare policy VM per ogni SCP che verrà utilizzato nell'archivio dati dal menu *Policies and Profiles* dell'interfaccia utente di vCenter.
9. Scegliere il set di regole di storage "NetApp.Clustered.Data.ONTAP.VP.vvol". Il set di regole di storage "NetApp.Clustered.Data.ONTAP.VP.VASA10" è per il supporto SPBM con datastore non vVols
10. Quando si crea un criterio di storage VM, specificare il profilo di capacità dello storage in base al nome. In questa fase, è possibile configurare anche la corrispondenza dei criteri di SnapMirror utilizzando la scheda di replica e la corrispondenza basata su tag utilizzando la scheda dei tag. Tenere presente che i tag devono essere già creati per essere selezionabili.
11. Creare le macchine virtuali, selezionando la policy di storage delle macchine virtuali e il datastore compatibile in Select storage (Seleziona storage).

### Migrazione di macchine virtuali da datastore tradizionali a vVol

La migrazione delle macchine virtuali dai datastore tradizionali a un datastore vVol è semplice quanto lo spostamento delle macchine virtuali tra datastore tradizionali. È sufficiente selezionare le macchine virtuali, quindi Migrate (Migra) dall'elenco delle azioni e selezionare un tipo di migrazione di *change storage only*. Le operazioni di copia della migrazione verranno trasferite con vSphere 6.0 e versioni successive per le migrazioni DA SAN VMFS a vVol, ma non da NAS VMDK a vVol.

### Gestione delle VM mediante policy

Per automatizzare il provisioning dello storage con una gestione basata su criteri, dobbiamo:

- Definire le funzionalità dello storage (nodo ONTAP e volume FlexVol) con SCP (Storage Capability Profiles).
- Creare policy di storage delle macchine virtuali mappate alle SCP definite.

NetApp ha semplificato le funzionalità e la mappatura a partire dal provider VASA 7.2 con continui miglioramenti nelle versioni successive. Questa sezione si concentra su questo nuovo approccio. Le versioni precedenti supportavano un maggior numero di funzionalità e consentiva di mapparle singolarmente alle policy di storage, ma questo approccio non è più supportato.

#### Funzionalità di profilo della capacità dello storage con la release di tool ONTAP

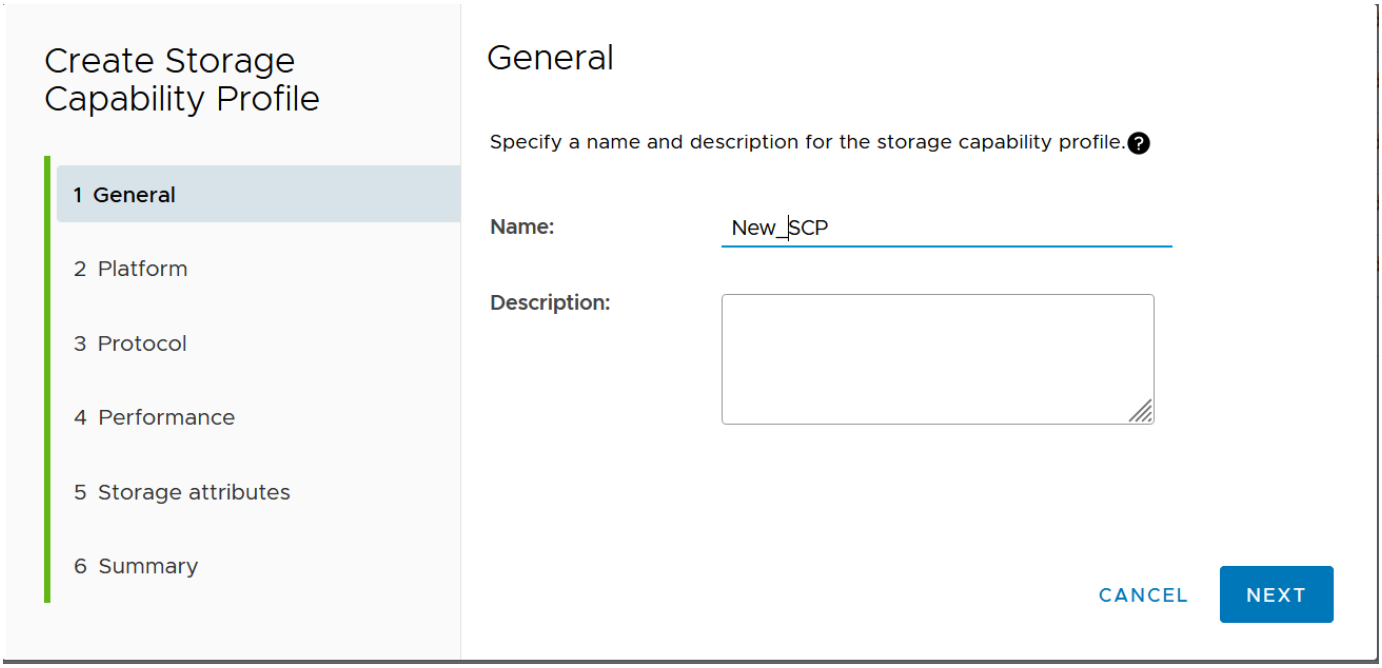
| Funzionalità SCP | Valori di capacità | Versione supportata | Note |
|---|---|---|---|
| **Compressione** | Sì, No, qualsiasi | Tutto | Obbligatorio per AFF nel 7.2 e versioni successive. |
| **Deduplica** | Sì, No, qualsiasi | Tutto | M andatory for AFF nel 7.2 e versioni successive. |
| **Crittografia** | Sì, No, qualsiasi | 7,2 e successivi | Seleziona/crea un volume FlexVol crittografato. È richiesta la licenza ONTAP. |
| **IOPS max** | <number> | 7.1 e versioni successive, ma le differenze | Elencato in QoS Policy Group per 7.2 e versioni successive. Vedere Gestione delle performance con gli strumenti ONTAP 9.10 e versioni successive per ulteriori informazioni. |
| **Personalità** | A FF, FAS | 7,2 e successivi | FAS include anche altri sistemi non AFF, come ONTAP Select. AFF include ASA. |
| **Protocollo** | NFS, NFS 4.1, iSCSI, FCP, NVMe/FC, Qualsiasi | 7.1 e versioni precedenti, 9.10 e versioni successive | 7.2-9.8 è effettivamente "qualsiasi". Ricominciare dal 9.10, dove NFS 4.1 e NVMe/FC sono stati aggiunti all'elenco originale. |

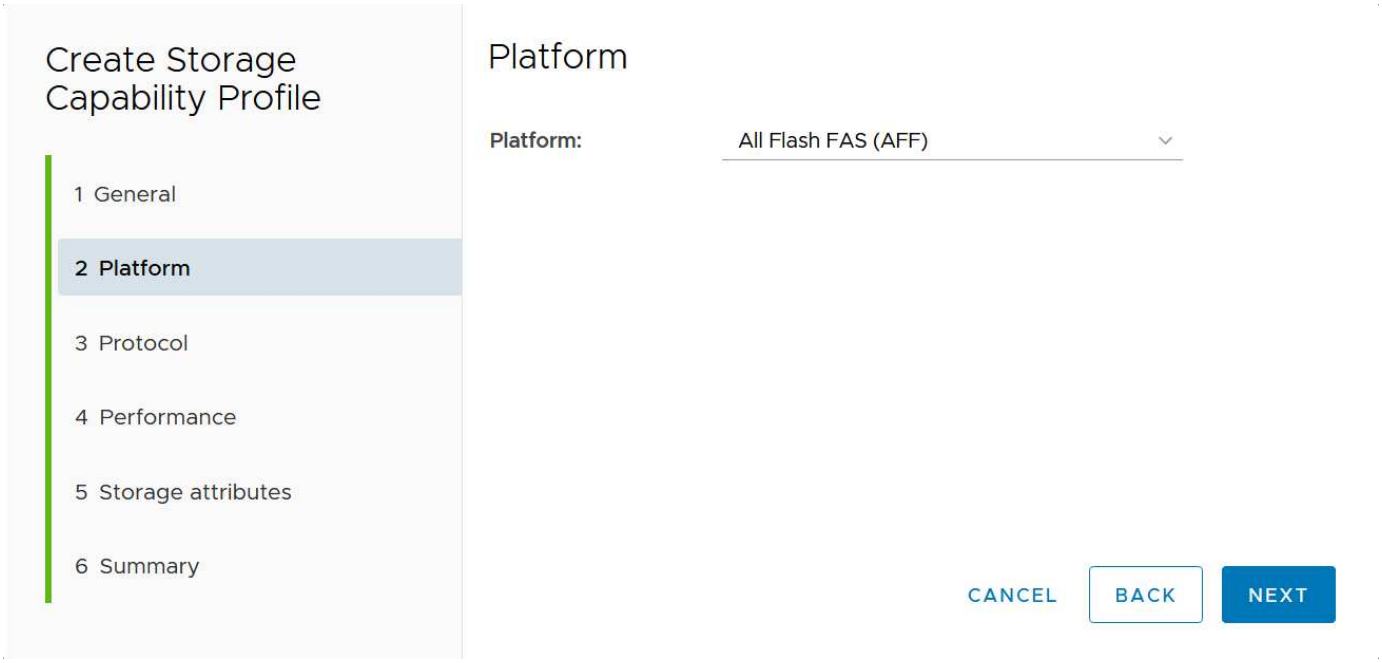
| Funzionalità SCP | Valori di capacità | Versione supportata | Note |
|---|---|---|---|
| **Riserva di spazio (Thin Provisioning)** | Sottile, spesso (qualsiasi) | Tutto, ma le differenze | Definito Thin Provisioning nel 7.1 e nelle versioni precedenti, che consentiva anche il valore di qualsiasi. Chiamata Space Reserve nel 7.2. Per impostazione predefinita, tutte le release sono impostate su Thin. |
| **Policy di tiering** | Qualsiasi, Nessuno, Snapshot, Auto | 7,2 e successivi | Utilizzato per FabricPool - richiede AFF o ASA con ONTAP 9,4 o versione successiva. Si consiglia di utilizzare solo Snapshot, a meno che non si utilizzi una soluzione S3 on-premise come NetApp StorageGRID. |

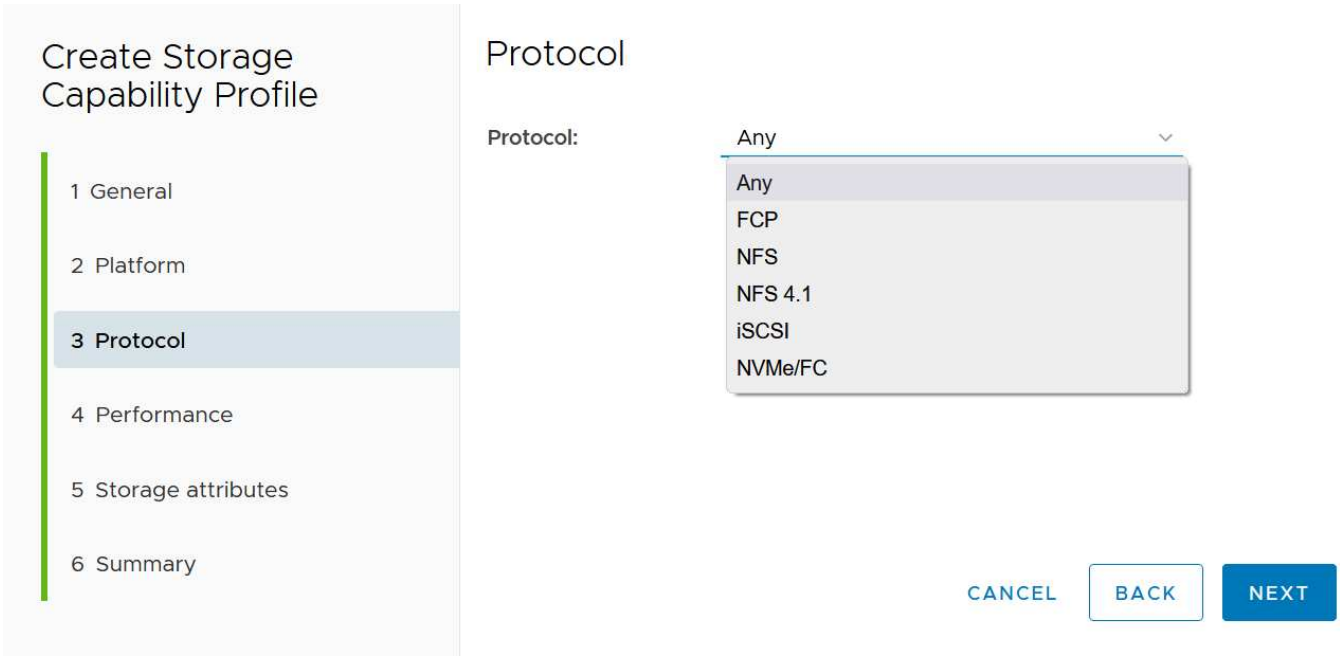
### Creazione di profili di funzionalità storage

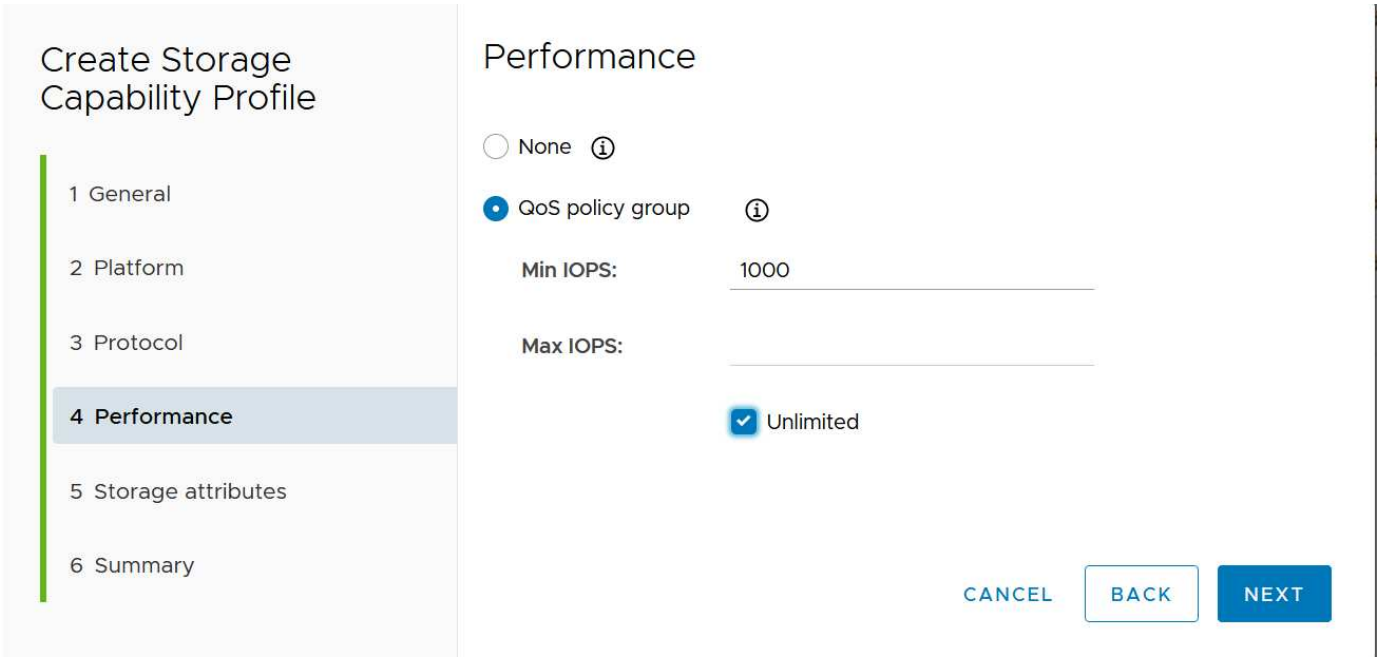
Il NetApp VASA Provider viene fornito con diversi SCP predefiniti. I nuovi SCP possono essere creati manualmente, utilizzando l'interfaccia utente di vCenter o tramite automazione utilizzando le API REST. Specificando le funzionalità in un nuovo profilo, clonando un profilo esistente o generando automaticamente profili da datastore tradizionali esistenti. Questa operazione viene eseguita utilizzando i menu in ONTAP Tools (Strumenti di Windows). Utilizzare *Storage Capability Profiles* per creare o clonare un profilo e *Storage Mapping* per generare automaticamente un profilo.

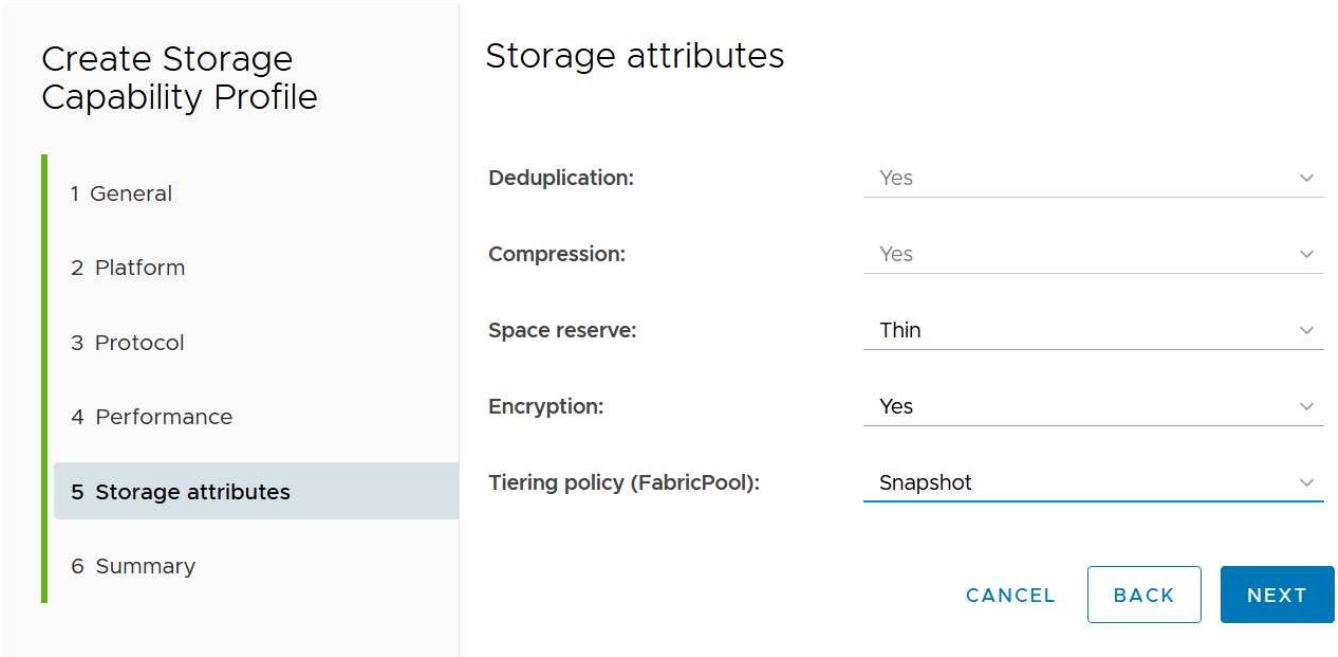
### Funzionalità di storage per gli strumenti ONTAP 9.10 e versioni successive

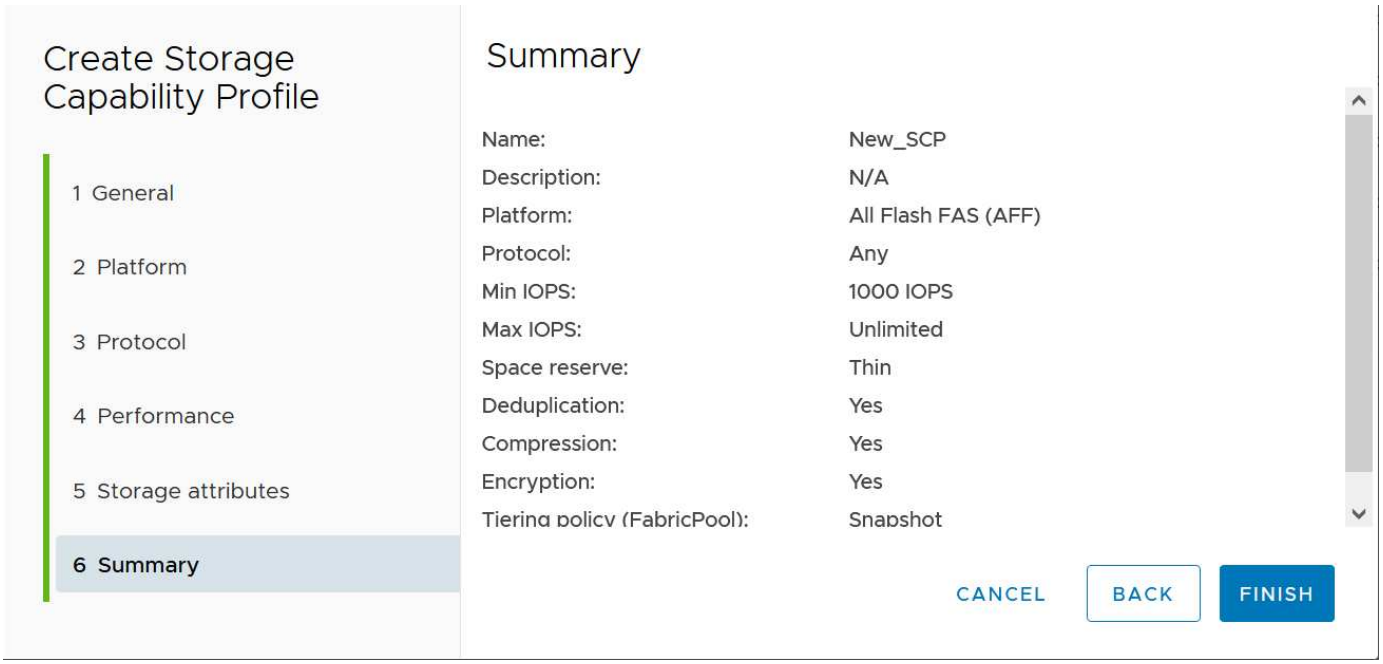



Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Platform
Platform:
All Flash FAS (AFF)
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Protocol
Protocol:
Any
Any
FCP
NFS
NFS 4.1
iSCSI
NVMe/FC
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Performance
None
QoS policy group
Min IOPS:
1000
Max IOPS:
Unlimited
CANCEL
BACK
NEXT


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Storage attributes
Deduplication:
Yes
Compression:
Yes
Space reserve:
Thin
Encryption:
Yes
Tiering policy (FabricPool):
Snapshot
CANCEL
BACK
NEXT




**Creazione di archivi dati vVol**

Una volta creati, gli SCP necessari possono essere utilizzati per creare il datastore vVols (e, facoltativamente, i volumi FlexVol per il datastore). Fare clic con il pulsante destro del mouse sull'host, sul cluster o sul data center su cui si desidera creare il datastore vVols, quindi selezionare *ONTAP Tools* > *Provision Datastore*. Selezionare uno o più SCP da supportare dall'archivio dati, quindi scegliere tra i volumi FlexVol esistenti e/o eseguire il provisioning di nuovi volumi FlexVol per l'archivio dati. Infine, specificare l'SCP predefinito per l'archivio dati, che verrà utilizzato per le macchine virtuali che non dispongono di un SCP specificato dal criterio, nonché per i vVol di swap (che non richiedono uno storage dalle performance elevate).

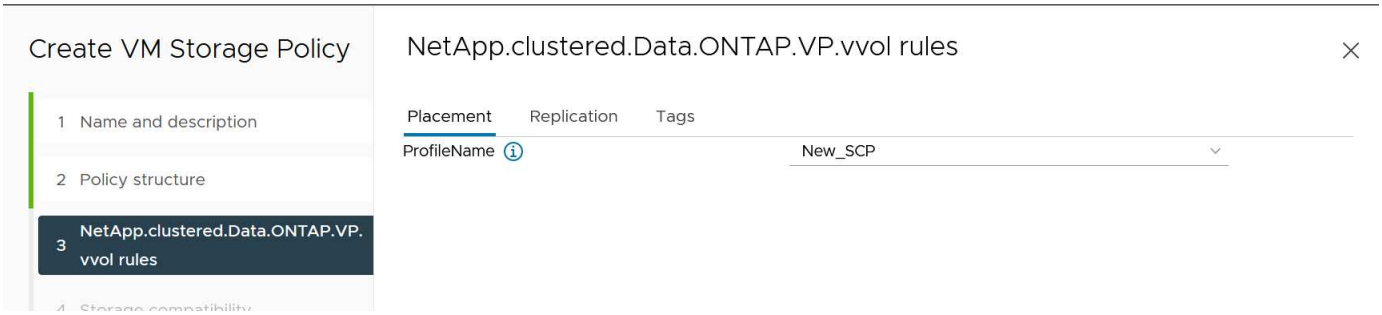
#### Creazione di policy di storage delle macchine virtuali

Le policy di storage delle macchine virtuali vengono utilizzate in vSphere per gestire funzionalità opzionali come Storage i/o Control o vSphere Encryption. Vengono inoltre utilizzati con vVol per applicare funzionalità di storage specifiche alla macchina virtuale. Utilizzare il tipo di storage "NetApp.Clustered.Data.ONTAP.VP.vvol" e la regola "ProfileName" per applicare un SCP specifico alle macchine virtuali attraverso l'utilizzo del criterio. Consulta esempio di configurazione di rete con vVol su NFS v3 per un esempio con il provider VASA degli strumenti ONTAP. Le regole per lo storage "NetApp.Clustered.Data.ONTAP.VP.VASA10" devono essere utilizzate con datastore non basati su vVol.

Le versioni precedenti sono simili, ma come menzionato in Funzionalità di profilo della capacità dello storage con la release di tool ONTAP, le opzioni disponibili variano.

Una volta creata la policy di storage, è possibile utilizzarla per il provisioning di nuove macchine virtuali, come illustrato nella "Implementare la macchina virtuale utilizzando i criteri di storage". Le linee guida per l'utilizzo delle funzionalità di gestione delle prestazioni con VASA Provider 7,2 sono illustrate nella Gestione delle performance con gli strumenti ONTAP 9.10 e versioni successive.

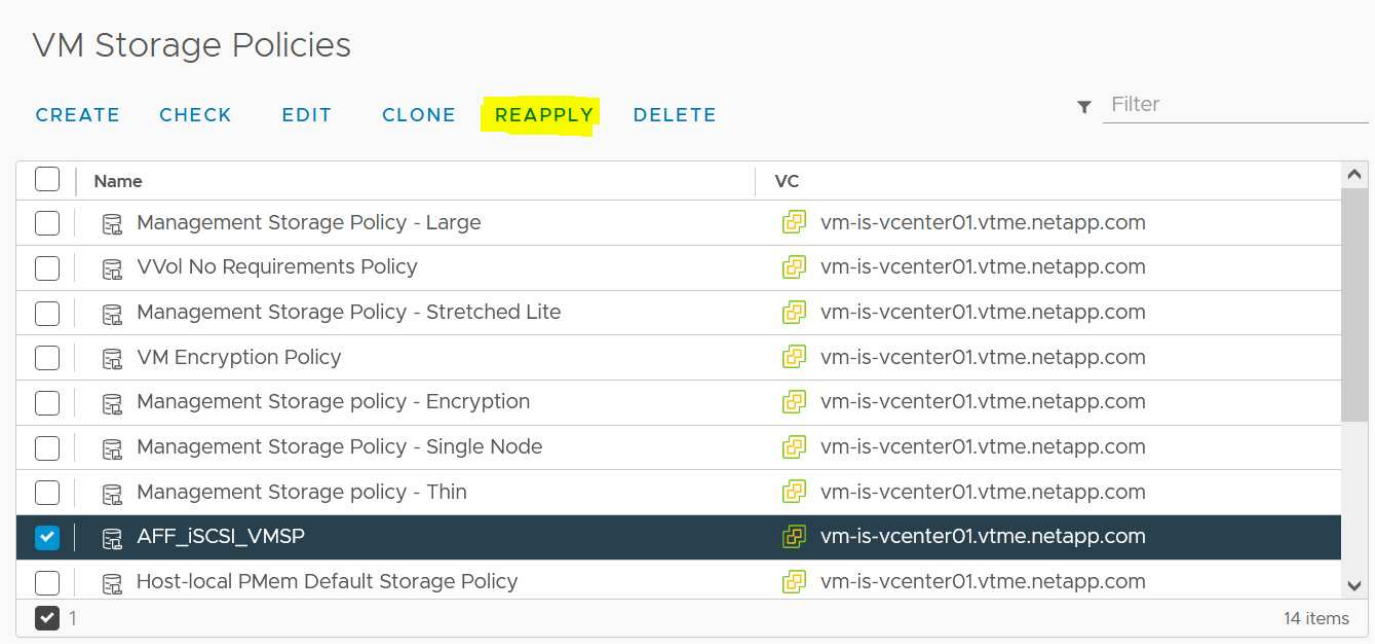
**Creazione di policy di storage delle macchine virtuali con tool ONTAP VASA Provider 9,10**




### Gestione delle performance con gli strumenti ONTAP 9.10 e versioni successive

- ONTAP Tools 9.10 utilizza il proprio algoritmo di posizionamento bilanciato per inserire un nuovo vVol nel miglior volume FlexVol all'interno di un datastore vVol. Il posizionamento si basa sui volumi SCP specificati e FlexVol corrispondenti. In questo modo si garantisce che il datastore e lo storage di backup soddisfino i requisiti di performance specificati.
- La modifica delle funzionalità delle performance, ad esempio IOPS min e max, richiede un'attenzione particolare alla configurazione specifica.
  - **I valori minimo e massimo di IOPS** possono essere specificati in un SCP e utilizzati in una policy VM.
    - La modifica degli IOPS in SCP non modificherà la QoS sui vVol fino a quando il criterio della VM non viene modificato e quindi riapplicato alle VM che lo utilizzano (vedere la) Funzionalità di storage per gli strumenti ONTAP 9.10 e versioni successive). Oppure creare un nuovo SCP con gli IOPS desiderati e modificare il criterio per utilizzarlo (e riapplicarlo alle macchine virtuali). In genere, si consiglia di definire semplicemente criteri di storage di SCP e VM separati per diversi livelli di servizio e di modificare semplicemente la policy di storage delle macchine virtuali sulla macchina virtuale.
    - Le personalità AFF e FAS hanno impostazioni IOPS diverse. Sia min che Max sono disponibili su AFF. Tuttavia, i sistemi non AFF possono utilizzare solo le impostazioni relative al numero massimo di IOPS.
- In alcuni casi, potrebbe essere necessario migrare un vVol dopo una modifica di policy (manualmente o automaticamente dal provider VASA e da ONTAP):
  - Alcune modifiche non richiedono alcuna migrazione (ad esempio, la modifica di Max IOPS, che può essere applicata immediatamente alla macchina virtuale come descritto sopra).
  - Se la modifica del criterio non può essere supportata dal volume FlexVol corrente che memorizza il vVol (ad esempio, la piattaforma non supporta il criterio di crittografia o di tiering richiesto), sarà necessario migrare manualmente la macchina virtuale in vCenter.
- Gli strumenti ONTAP creano policy QoS individuali non condivise con le versioni attualmente supportate di ONTAP. Pertanto, ogni singolo VMDK riceverà la propria allocazione di IOPS.

### Riapplicazione dei criteri di storage delle macchine virtuali




## Protezione di vVol

Nelle seguenti sezioni vengono illustrate le procedure e le Best practice per l'utilizzo di vVol VMware con lo storage ONTAP.

### ALTA disponibilità del provider VASA

NetApp VASA Provider viene eseguito come parte dell'appliance virtuale insieme al plug-in vCenter, al server REST API (precedentemente noto come Virtual Storage Console [VSC]) e allo Storage Replication Adapter. Se il provider VASA non è disponibile, le VM che utilizzano vVol continueranno a funzionare. Tuttavia, non è possibile creare nuovi datastore vVol e non è possibile creare o vinare vVol da vSphere. Ciò significa che le macchine virtuali che utilizzano vVol non possono essere attivate poiché vCenter non sarà in grado di richiedere la creazione dello swap vVol. Inoltre, le macchine virtuali in esecuzione non possono utilizzare vMotion per la migrazione a un altro host perché i vVol non possono essere associati al nuovo host.

VASA Provider 7.1 e versioni successive supportano nuove funzionalità per garantire la disponibilità dei servizi quando necessario. Include nuovi processi di controllo che monitorano il provider VASA e i servizi di database integrati. Se rileva un errore, aggiorna i file di registro e riavvia automaticamente i servizi.

L'amministratore di vSphere deve configurare un'ulteriore protezione utilizzando le stesse funzionalità di disponibilità utilizzate per proteggere le altre macchine virtuali mission-critical da guasti del software, dell'hardware host e della rete. Non è richiesta alcuna configurazione aggiuntiva sull'appliance virtuale per utilizzare queste funzionalità; è sufficiente configurarle utilizzando gli approcci standard vSphere. Sono stati testati e supportati da NetApp.

VSphere High Availability è facilmente configurabile per riavviare una macchina virtuale su un altro host nel cluster host in caso di guasto. VSphere Fault Tolerance offre una maggiore disponibilità creando una macchina virtuale secondaria che viene continuamente replicata e che può assumere il controllo in qualsiasi momento. Ulteriori informazioni su queste funzioni sono disponibili nella "Strumenti ONTAP per la documentazione di VMware vSphere (configurare l'alta disponibilità per i tool ONTAP)", Oltre alla documentazione VMware vSphere (cercare vSphere Availability sotto ESXi e vCenter Server).

Il provider VASA di ONTAP Tools esegue automaticamente il backup della configurazione vVol in tempo reale sui sistemi ONTAP gestiti in cui le informazioni vVol vengono memorizzate nei metadati dei volumi FlexVol. Nel

caso in cui l'appliance ONTAP Tools non fosse disponibile per qualsiasi motivo, è possibile implementarne una nuova e importarne la configurazione in modo semplice e rapido. Fare riferimento a questo articolo della Knowledge base per ulteriori informazioni sulle fasi di ripristino del provider VASA:

"Come eseguire un Disaster Recovery provider VASA - Guida alla risoluzione"

### Replica di vVol

Molti clienti ONTAP replicano i propri datastore tradizionali su sistemi storage secondari utilizzando NetApp SnapMirror, quindi utilizzano il sistema secondario per ripristinare singole macchine virtuali o un intero sito in caso di disastro. Nella maggior parte dei casi, i clienti utilizzano uno strumento software per la gestione di questo tipo, ad esempio un prodotto software di backup come il plug-in NetApp SnapCenter per VMware vSphere o una soluzione di disaster recovery come Site Recovery Manager di VMware (insieme all'adattatore di replica dello storage negli strumenti ONTAP).

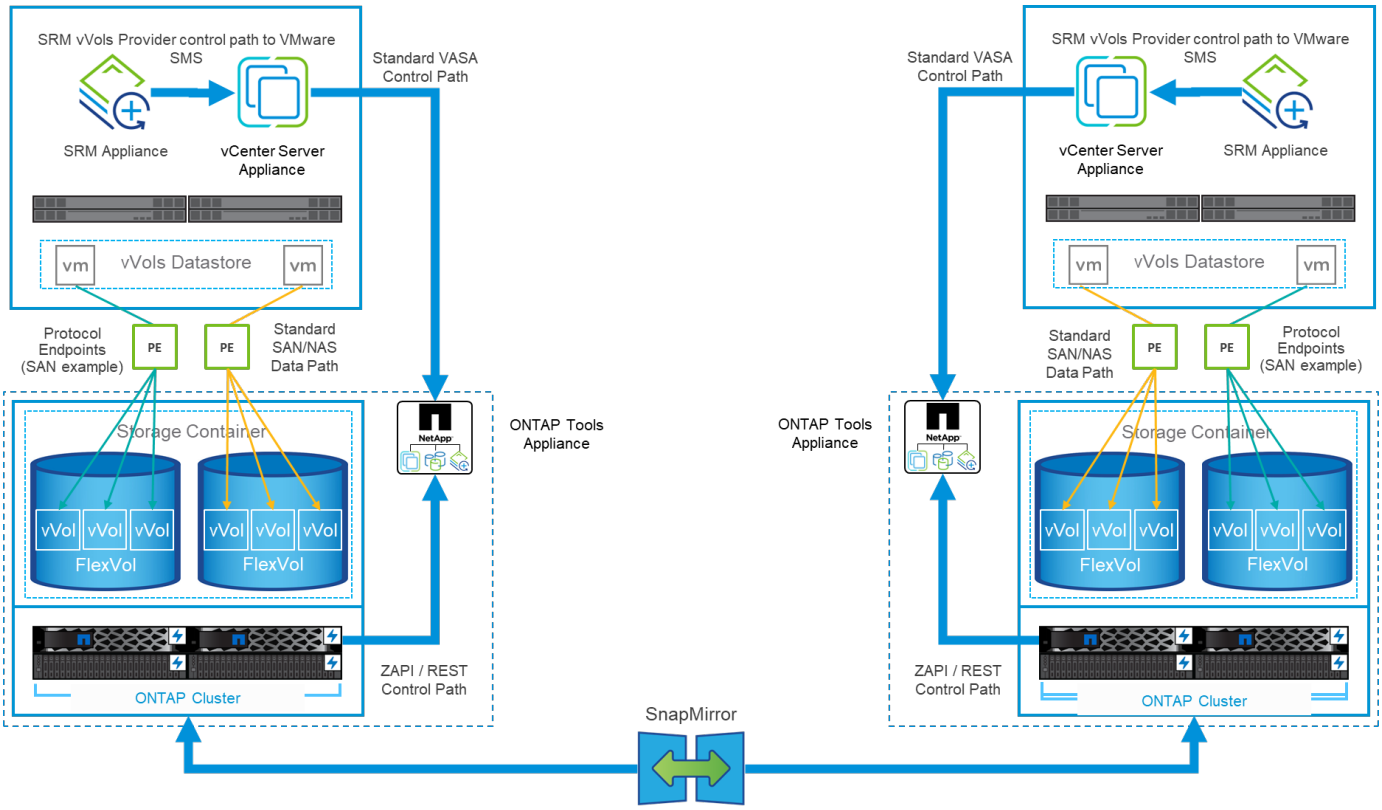
Questo requisito per uno strumento software è ancora più importante per gestire la replica di vVol. Sebbene alcuni aspetti possano essere gestiti da funzionalità native (ad esempio, le snapshot gestite da VMware di vVol vengono trasferite su ONTAP, che utilizza cloni di file o LUN rapidi ed efficienti), in generale l'orchestrazione è necessaria per gestire la replica e il ripristino. I metadati relativi ai vVol sono protetti da ONTAP e dal provider VASA, ma è necessaria un'ulteriore elaborazione per utilizzarli in un sito secondario.

I tool ONTAP 9.7.1, insieme alla release 8.3 di VMware Site Recovery Manager (SRM), hanno aggiunto il supporto per il disaster recovery e l'orchestrazione del flusso di lavoro di migrazione sfruttando la tecnologia SnapMirror di NetApp.

Nella versione iniziale del supporto SRM con i tool ONTAP 9.7.1 era necessario pre-creare FlexVol e abilitare la protezione SnapMirror prima di utilizzarli come volumi di backup per un datastore vVol. A partire dagli strumenti ONTAP 9.10, questo processo non è più necessario. È ora possibile aggiungere la protezione SnapMirror ai volumi di backup esistenti e aggiornare le policy di storage delle macchine virtuali per sfruttare la gestione basata su policy con disaster recovery, orchestrazione e automazione della migrazione integrate con SRM.

Attualmente, VMware SRM è l'unica soluzione di disaster recovery e automazione della migrazione per vVol supportata da NetApp e i tool ONTAP verificheranno l'esistenza di un server SRM 8.3 o successivo registrato con vCenter prima di consentire la replica di vVol, Sebbene sia possibile sfruttare le API REST degli strumenti ONTAP per creare i propri servizi.

#### Replica di vVol con SRM




### Supporto MetroCluster

Sebbene gli strumenti ONTAP non siano in grado di attivare uno switchover MetroCluster, supportano i sistemi NetApp MetroCluster per il backup dei volumi in una configurazione vMSC (vSphere Metro Storage Cluster) uniforme. La commutazione di un sistema MetroCluster viene gestita normalmente.

Anche se NetApp SnapMirror Business Continuity (SM-BC) può essere utilizzato come base per una configurazione vMSC, al momento non è supportato con vVol.

Consulta queste guide per ulteriori informazioni su NetApp MetroCluster:

"*Architettura e progettazione della soluzione IP TR-4689 MetroCluster*"

"*TR-4705 architettura e progettazione della soluzione NetApp MetroCluster*"

"*VMware KB 2031038 supporto VMware vSphere con NetApp MetroCluster*"

### Panoramica del backup di vVol

Esistono diversi approcci per la protezione delle macchine virtuali, ad esempio l'utilizzo di agenti di backup in-guest, l'aggiunta di file di dati delle macchine virtuali a un proxy di backup o l'utilizzo di API definite come VMware VADP. I vVol possono essere protetti utilizzando gli stessi meccanismi e molti partner NetApp supportano i backup delle macchine virtuali, inclusi i vVol.

Come accennato in precedenza, le snapshot gestite da VMware vCenter vengono trasferite a cloni di file/LUN ONTAP efficienti in termini di spazio e veloci. Questi possono essere utilizzati per backup manuali e rapidi, ma sono limitati da vCenter a un massimo di 32 snapshot. È possibile utilizzare vCenter per creare snapshot e ripristinarli in base alle necessità.

A partire dal plug-in SnapCenter per VMware vSphere (SCV) 4.6, se utilizzato insieme ai tool ONTAP 9.10 e versioni successive, aggiunge il supporto per backup e ripristino coerenti in caso di crash delle macchine

virtuali basate su vVol, sfruttando le snapshot dei volumi ONTAP FlexVol con il supporto per SnapMirror e la replica SnapVault. Sono supportati fino a 1023 snapshot per volume. SCV può anche memorizzare più snapshot con una maggiore conservazione sui volumi secondari utilizzando SnapMirror con una policy di vault mirror.

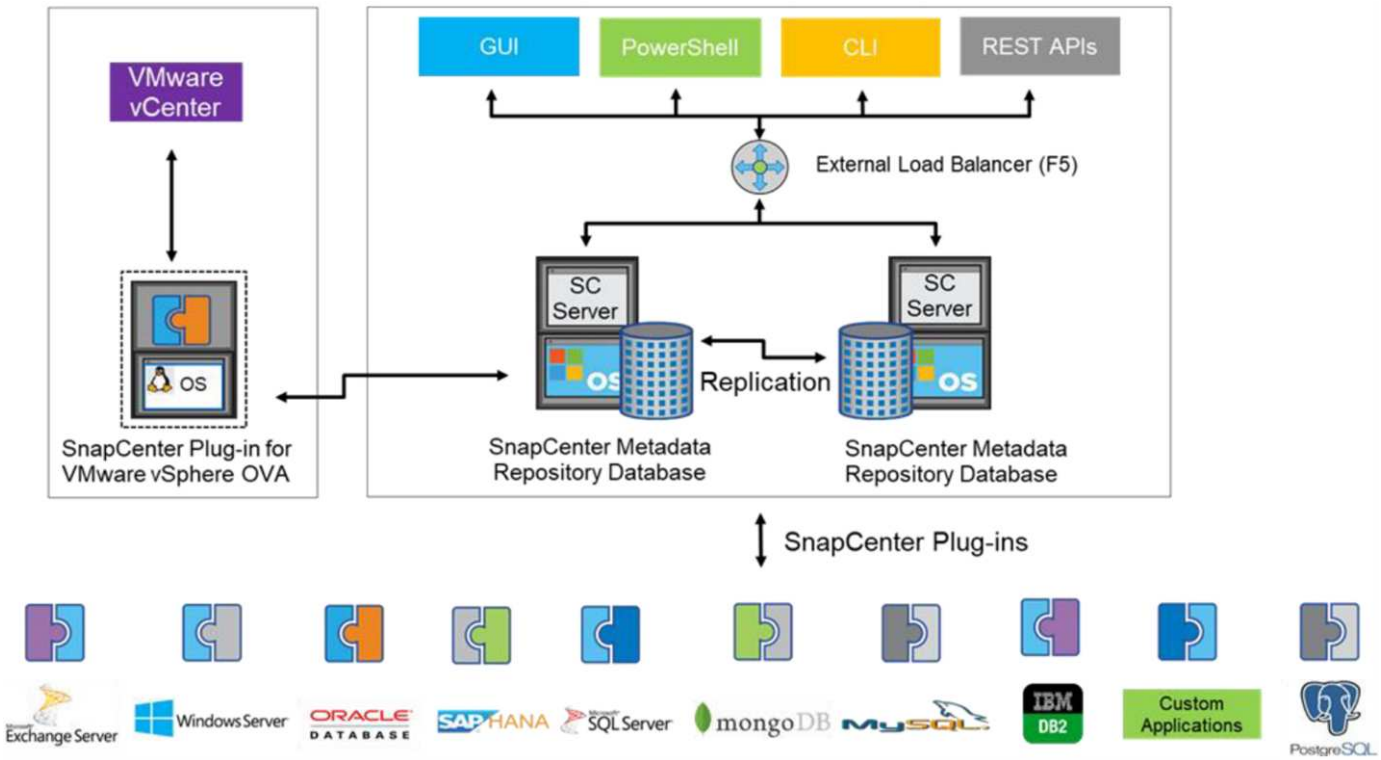
Il supporto di vSphere 8.0 è stato introdotto con SCV 4.7, che utilizzava un'architettura di plug-in locale isolata. Il supporto di vSphere 8.0U1 è stato aggiunto a SCV 4.8, che ha completato la transizione alla nuova architettura di plug-in remoto.

### Backup vVol con plug-in SnapCenter per VMware vSphere

Con NetApp SnapCenter puoi ora creare gruppi di risorse per i vVol basati su tag e/o cartelle per sfruttare automaticamente le snapshot basate su FlexVol di ONTAP per macchine virtuali basate su vVol. Ciò consente di definire servizi di backup e ripristino che proteggeranno automaticamente le macchine virtuali man mano che vengono sottoposte a provisioning dinamico all'interno dell'ambiente.

Il plug-in SnapCenter per VMware vSphere viene implementato come appliance standalone registrata come estensione vCenter, gestita tramite l'interfaccia utente di vCenter o tramite API REST per l'automazione dei servizi di backup e recovery.

#### Architettura SnapCenter




Poiché gli altri plug-in di SnapCenter non supportano ancora i vVol al momento di questa scrittura, in questo documento ci concentreremo sul modello di distribuzione standalone.

Poiché SnapCenter utilizza snapshot ONTAP FlexVol, non è previsto alcun overhead su vSphere, né penalità in termini di performance, come si può vedere con le macchine virtuali tradizionali che utilizzano snapshot gestite da vCenter. Inoltre, poiché le funzionalità di SCV sono esposte attraverso le API REST, è semplice creare workflow automatizzati utilizzando tool come VMware aria Automation, Ansible, Terraform e virtualmente qualsiasi altro tool di automazione in grado di utilizzare le API REST standard.

Per informazioni sulle API REST di SnapCenter, vedere "Panoramica delle API REST"

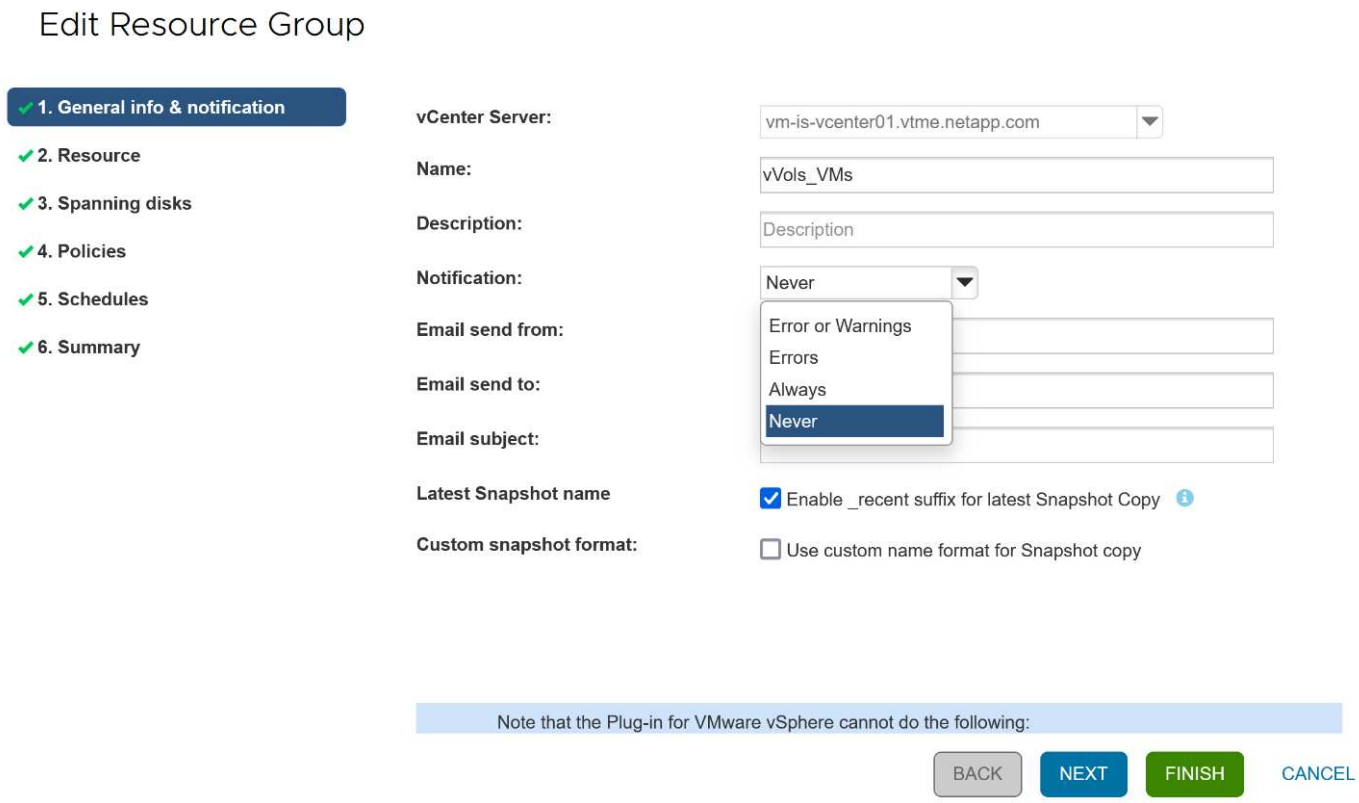
Per informazioni sulle API REST del plug-in SnapCenter per VMware vSphere, vedere "Plug-in SnapCenter per le API REST di VMware vSphere"

#### Best Practice

Le seguenti Best practice possono aiutarti a ottenere il massimo dalla tua implementazione SnapCenter.

- SCV supporta sia vCenter Server RBAC che ONTAP RBAC e include ruoli vCenter predefiniti che vengono creati automaticamente al momento della registrazione del plug-in. Ulteriori informazioni sui tipi di RBAC supportati "qui."
  - Utilizzare l'interfaccia utente di vCenter per assegnare l'accesso agli account con privilegi minimi utilizzando i ruoli predefiniti descritti "qui".
  - Se si utilizza SCV con il server SnapCenter, è necessario assegnare il ruolo *SnapCenterAdmin*.
  - ONTAP RBAC si riferisce all'account utente utilizzato per aggiungere e gestire i sistemi di storage utilizzati da SCV. Il role-based access control ONTAP non si applica ai backup basati su vVol. Scopri di più su ONTAP RBAC e SCV "qui".
- Replica i set di dati di backup su un secondo sistema utilizzando SnapMirror per repliche complete dei volumi di origine. Come indicato in precedenza, è anche possibile utilizzare policy di vault mirror per la conservazione a lungo termine dei dati di backup indipendentemente dalle impostazioni di conservazione delle snapshot del volume di origine. Entrambi i meccanismi sono supportati con vVol.
- Poiché SCV richiede anche strumenti ONTAP per la funzionalità vVol di VMware vSphere, controllare sempre lo strumento matrice di interoperabilità NetApp (IMT) per verificare la compatibilità delle versioni specifiche
- Se si utilizza la replica vVol con VMware SRM, prestare attenzione all'RPO delle policy e alla pianificazione del backup
- Progettare le policy di backup con impostazioni di conservazione che soddisfino gli obiettivi dei punti di ripristino (RPO) definiti dall'organizzazione
- Configurare le impostazioni di notifica sui gruppi di risorse per ricevere una notifica dello stato durante l'esecuzione dei backup (vedere la figura 10 di seguito)

#### Opzioni di notifica del gruppo di risorse




**Iniziare a utilizzare SCV utilizzando questi documenti**

"Scopri di più sul plug-in SnapCenter per VMware vSphere"

"Implementare il plug-in SnapCenter per VMware vSphere"

## Risoluzione dei problemi

Sono disponibili diverse risorse per la risoluzione dei problemi con ulteriori informazioni.

### Sito di supporto NetApp

Oltre a una serie di articoli della Knowledge base per i prodotti di virtualizzazione NetApp, il sito del supporto NetApp offre anche una comoda landing page per "Strumenti ONTAP per VMware vSphere" prodotto. Questo portale fornisce link ad articoli, download, report tecnici e discussioni sulle soluzioni VMware sulla community NetApp. È disponibile all'indirizzo:

"*Sito di supporto NetApp*"

La documentazione aggiuntiva sulla soluzione è disponibile qui:

"*Soluzioni NetApp per la virtualizzazione*"

### Risoluzione dei problemi del prodotto

I vari componenti degli strumenti ONTAP, come il plugin vCenter, il provider VASA e l'adattatore di replica dello storage, sono tutti documentati insieme nell'archivio dei documenti NetApp. Tuttavia, ciascuno di essi dispone di una sottosezione separata della Knowledge base e può disporre di procedure specifiche per la risoluzione dei problemi. Queste soluzioni risolvono i problemi più comuni che potrebbero verificarsi con il provider VASA.

#### Problemi dell'interfaccia utente del provider VASA

Occasionalmente, il client Web vCenter vSphere incontra problemi con i componenti di Serenity, causando la mancata visualizzazione delle voci di menu del provider VASA per ONTAP. Consultare la sezione risoluzione dei problemi di registrazione del provider VASA nella Guida all'implementazione o nella presente Knowledge base "articolo".

#### Il provisioning del datastore di vVol non riesce

Occasionalmente, i servizi vCenter potrebbero subire un timeout durante la creazione del datastore vVols. Per correggerlo, riavviare il servizio vmware-sps e rimontare il datastore vVols utilizzando i menu vCenter (Storage > New Datastore). Questo argomento viene trattato in vVols datastore provisioning fails with vCenter Server 6.5 nella Administration Guide.

#### L'aggiornamento di Unified Appliance non riesce a montare ISO

A causa di un bug in vCenter, l'ISO utilizzato per aggiornare Unified Appliance da una release alla successiva potrebbe non essere in grado di eseguire il montaggio. Se è possibile collegare l'ISO all'appliance in vCenter, seguire la procedura descritta in questa Knowledge base "articolo" per risolvere il problema.

# VMware Site Recovery Manager con ONTAP

## VMware Site Recovery Manager con ONTAP

Sin dall'introduzione nel moderno data center nel 2002, ONTAP è una soluzione storage leader per gli ambienti VMware vSphere e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo i costi.

In questo documento viene presentata la soluzione ONTAP per VMware Site Recovery Manager (SRM), il software di disaster recovery (DR) leader del settore di VMware, che include le informazioni più recenti sui prodotti e le Best practice per semplificare la distribuzione, ridurre i rischi e semplificare la gestione continua.

> Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4900: VMware Site Recovery Manager con ONTAP*

Le Best practice integrano altri documenti come guide e strumenti di compatibilità. Sono sviluppati in base a test di laboratorio e a un'ampia esperienza sul campo da parte di tecnici e clienti NetApp. In alcuni casi, le Best practice consigliate potrebbero non essere adatte al tuo ambiente; tuttavia, sono generalmente le soluzioni più semplici che soddisfano le esigenze della maggior parte dei clienti.

Questo documento è incentrato sulle funzionalità delle recenti release di ONTAP 9, se utilizzato insieme ai tool ONTAP per VMware vSphere 9.12 (che include l'adattatore per la replica dello storage NetApp [SRA] e il provider VASA [VP]), nonché VMware Site Recovery Manager 8.7.

### Perché utilizzare ONTAP con SRM?

Le piattaforme di gestione dei dati NetApp basate sul software ONTAP sono alcune delle soluzioni di storage più diffuse per SRM. I motivi sono molteplici: Una piattaforma per la gestione dei dati sicura, dalle performance elevate e protocollo unificato (NAS e SAN insieme) che offre efficienza dello storage definita dal settore, multitenancy, controlli della qualità del servizio, protezione dei dati con snapshot efficienti in termini di spazio e replica con SnapMirror. Tutto questo sfrutta l'integrazione multi-cloud ibrida nativa per la protezione dei carichi di lavoro VMware e una vasta gamma di strumenti di automazione e orchestrazione a portata di mano.

Utilizzando SnapMirror per la replica basata su array è possibile sfruttare una delle tecnologie ONTAP più comprovate e mature. SnapMirror offre il vantaggio di trasferimenti di dati sicuri ed altamente efficienti, copiando solo i blocchi di file system modificati, non intere macchine virtuali o datastore. Anche questi blocchi sfruttano il risparmio di spazio, come deduplica, compressione e compattazione. I moderni sistemi ONTAP utilizzano ora SnapMirror indipendente dalla versione, consentendo di scegliere i cluster di origine e di destinazione in modo flessibile. SnapMirror è diventato uno dei tool più potenti disponibili per il disaster recovery.

Sia che stiate utilizzando datastore collegati a NFS, iSCSI o Fibre Channel tradizionali (ora con supporto per datastore vVol), SRM offre una solida offerta di prima parte che sfrutta il meglio delle funzionalità ONTAP per il disaster recovery o la pianificazione e l'orchestrazione della migrazione dei data center.

**In che modo SRM sfrutta ONTAP 9**

SRM sfrutta le tecnologie avanzate di gestione dei dati dei sistemi ONTAP integrandosi con i tool ONTAP per VMware vSphere, un'appliance virtuale che include tre componenti principali:

- Il plug-in vCenter, precedentemente noto come Virtual Storage Console (VSC), semplifica le funzionalità di gestione ed efficienza dello storage, migliora la disponibilità e riduce i costi di storage e l'overhead operativo, sia che si utilizzi SAN che NAS. Utilizza le Best practice per il provisioning degli archivi dati e ottimizza le impostazioni degli host ESXi per gli ambienti di storage a blocchi e NFS. Per tutti questi vantaggi, NetApp consiglia questo plug-in quando si utilizza vSphere con sistemi che eseguono il software ONTAP.
- Il provider VASA per ONTAP supporta il framework VMware vStorage API for Storage Awareness (VASA). IL provider VASA connette vCenter Server a ONTAP per facilitare il provisioning e il monitoraggio dello storage delle macchine virtuali. Consente il supporto di VMware Virtual Volumes (vVol) e la gestione dei profili di capacità dello storage (incluse le funzionalità di replica di vVol) e delle performance di VM vVol individuali. Fornisce inoltre allarmi per il monitoraggio della capacità e della conformità con i profili. Se utilizzato in combinazione con SRM, il provider VASA per ONTAP consente il supporto delle macchine virtuali basate su vVol senza richiedere l'installazione di un adattatore SRA sul server SRM.
- SRA viene utilizzato insieme a SRM per gestire la replica dei dati delle macchine virtuali tra siti di produzione e disaster recovery per datastore VMFS e NFS tradizionali e per il test senza interruzioni delle repliche DR. Consente di automatizzare le attività di rilevamento, ripristino e protezione. Include un'appliance server SRA e adattatori SRA per server SRM Windows e appliance SRM.

Dopo aver installato e configurato gli adattatori SRA sul server SRM per proteggere gli archivi dati non vVols e/o aver abilitato la replica vVols nelle impostazioni del provider VASA, è possibile iniziare l'attività di configurazione dell'ambiente vSphere per il disaster recovery.

I provider SRA e VASA offrono un'interfaccia di controllo e comando per il server SRM per gestire i FlexVol ONTAP che contengono le macchine virtuali VMware e la replica SnapMirror che li protegge.

A partire da SRM 8.3, nel server SRM è stato introdotto un nuovo percorso di controllo SRM vVols Provider, che consente di comunicare con il server vCenter e, attraverso di esso, con il provider VASA senza la necessità di un SRA. Ciò ha consentito al server SRM di sfruttare un controllo molto più approfondito sul cluster ONTAP rispetto a quanto era possibile in precedenza, perché VASA offre un'API completa per un'integrazione strettamente accoppiata.

SRM può verificare il vostro piano DR senza interruzioni utilizzando la tecnologia proprietaria FlexClone di NetApp per creare cloni quasi istantanei dei datastore protetti nel sito DR. SRM crea un sandbox per eseguire test in modo sicuro in modo che la tua organizzazione e i tuoi clienti siano protetti in caso di disastro reale, offrendo la sicurezza della capacità delle organizzazioni di eseguire un failover durante un disastro.

In caso di disastro reale o persino di migrazione pianificata, SRM consente di inviare eventuali modifiche

dell'ultimo minuto al dataset tramite un aggiornamento finale di SnapMirror (se si sceglie di farlo). Quindi, interrompe il mirror e monta il datastore sugli host DR. A questo punto, le VM possono essere alimentate automaticamente in qualsiasi ordine in base alla strategia prepianificata.

#### SRM con ONTAP e altri casi di utilizzo: Cloud ibrido e migrazione

L'integrazione dell'implementazione SRM con le funzionalità avanzate di gestione dei dati di ONTAP consente di migliorare notevolmente scalabilità e performance rispetto alle opzioni di storage locale. Ma oltre a questo, offre la flessibilità del cloud ibrido. Il cloud ibrido ti consente di risparmiare denaro tiering dei blocchi di dati inutilizzati dal tuo array dalle performance elevate all'hyperscaler preferito utilizzando FabricPool, che potrebbe essere un store S3 on-premise come NetApp StorageGRID. È inoltre possibile utilizzare SnapMirror per sistemi edge con software-defined ONTAP Select o DR basata su cloud utilizzando Cloud Volumes ONTAP (CVO) o. "Storage privato NetApp in Equinix" Per Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP) per creare uno stack di storage, networking e servizi di calcolo completamente integrato nel cloud.

Quindi, grazie a FlexClone, è possibile eseguire un failover di test nel data center di un cloud service provider con un impatto dello storage prossimo allo zero. Proteggere la tua organizzazione può ora costare meno che mai.

SRM può anche essere utilizzato per eseguire migrazioni pianificate sfruttando SnapMirror per trasferire in modo efficiente le macchine virtuali da un data center all'altro o anche all'interno dello stesso data center, sia esso il tuo, o tramite un numero qualsiasi di partner service provider NetApp.

## Best practice per l'implementazione

Nelle sezioni seguenti vengono illustrate le Best practice per la distribuzione con ONTAP e VMware SRM.

#### Layout e segmentazione SVM per SMT

Con ONTAP, il concetto di storage virtual machine (SVM) offre una segmentazione rigorosa in ambienti multi-tenant sicuri. Gli utenti SVM su una SVM non possono accedere o gestire le risorse da un'altra. In questo modo, è possibile sfruttare la tecnologia ONTAP creando SVM separate per diverse business unit che gestiscono i propri flussi di lavoro SRM sullo stesso cluster per una maggiore efficienza dello storage globale.

Valutare la possibilità di gestire ONTAP utilizzando account con ambito SVM e LIF di gestione SVM per non solo migliorare i controlli di sicurezza, ma anche le performance. Le performance sono intrinsecamente maggiori quando si utilizzano connessioni con ambito SVM perché l'SRA non è richiesto per elaborare tutte le risorse di un intero cluster, incluse le risorse fisiche. Al contrario, l'IT deve solo comprendere le risorse logiche astratte dalla specifica SVM.

Quando si utilizzano solo i protocolli NAS (senza accesso SAN), è anche possibile sfruttare la nuova modalità NAS ottimizzata impostando il seguente parametro (si noti che il nome è tale perché SRA e VASA utilizzano gli stessi servizi di back-end nell'appliance):

1. Accedere al pannello di controllo all'indirizzo `https://<IP address>:9083` E fare clic su interfaccia CLI basata su Web.
2. Eseguire il comando `vp updateconfig -key=enable.qtree.discovery -value=true`.
3. Eseguire il comando `vp updateconfig -key=enable.optimised.sra -value=true`.
4. Eseguire il comando `vp reloadconfig`.

#### Implementare gli strumenti e le considerazioni di ONTAP per i vVol

Se si intende utilizzare SRM con vVol, è necessario gestire lo storage utilizzando credenziali con ambito cluster e una LIF di gestione del cluster. Questo perché il provider VASA deve comprendere l'architettura fisica sottostante per soddisfare le policy richieste per le policy di storage delle macchine virtuali. Ad esempio, se si dispone di una policy che richiede storage all-flash, il provider VASA deve essere in grado di vedere quali sistemi sono tutti flash.

Un'altra Best practice per l'implementazione consiste nel non memorizzare mai l'appliance ONTAP Tools su un datastore vVols gestito dall'IT. Ciò potrebbe causare l'impossibilità di accendere il provider VASA perché non è possibile creare lo swap vVol per l'appliance perché l'appliance non è in linea.

#### Best practice per la gestione dei sistemi ONTAP 9

Come indicato in precedenza, è possibile gestire i cluster ONTAP utilizzando credenziali cluster o SVM con ambito e LIF di gestione. Per performance ottimali, puoi prendere in considerazione l'utilizzo delle credenziali con ambito SVM ogni volta che non utilizzi vVol. Tuttavia, in questo modo, è necessario conoscere alcuni requisiti e perdere alcune funzionalità.

- L'account SVM vsadmin predefinito non dispone del livello di accesso richiesto per eseguire le attività degli strumenti ONTAP. Pertanto, è necessario creare un nuovo account SVM.
- Se si utilizza ONTAP 9,8 o versione successiva, NetApp consiglia di creare un account utente RBAC con privilegi minimi utilizzando il menu utenti di ONTAP System Manager insieme al file JSON disponibile nell'appliance ONTAP Tools all'indirizzo `https://<IP address>:9083/vsc/config/`. Utilizzare la password di amministratore per scaricare il file JSON. Può essere utilizzato per account SVM o con ambito cluster.

  Se si utilizza ONTAP 9.6 o versioni precedenti, utilizzare lo strumento RBAC User Creator (RUC) disponibile in "Toolchest del sito di supporto NetApp".

- Poiché il plug-in dell'interfaccia utente di vCenter, il provider VASA e il server SRA sono tutti servizi completamente integrati, è necessario aggiungere storage all'adattatore SRM nello stesso modo in cui si aggiunge storage nell'interfaccia utente di vCenter per gli strumenti ONTAP. In caso contrario, il server SRA potrebbe non riconoscere le richieste inviate da SRM tramite l'adattatore SRA.
- Il controllo del percorso NFS non viene eseguito quando si utilizzano credenziali con ambito SVM. Questo perché la posizione fisica è logicamente astratta dalla SVM. Tuttavia, questo non è motivo di preoccupazione, in quanto i sistemi ONTAP moderni non subiscono più alcun calo significativo delle performance quando si utilizzano percorsi indiretti.
- Il risparmio di spazio aggregato dovuto all'efficienza dello storage potrebbe non essere segnalato.
- Se supportati, i mirror di condivisione del carico non possono essere aggiornati.
- La registrazione EMS potrebbe non essere eseguita sui sistemi ONTAP gestiti con credenziali SVM con ambito.

## Best practice operative

Nelle seguenti sezioni vengono illustrate le Best practice operative per lo storage SRM e ONTAP di VMware.

#### Datastore e protocolli

- Se possibile, utilizza sempre gli strumenti ONTAP per eseguire il provisioning di datastore e volumi. In questo modo si garantisce che volumi, percorsi di giunzione, LUN, igroups, policy di esportazione, e altre

impostazioni sono configurate in modo compatibile.

- SRM supporta iSCSI, Fibre Channel e NFS versione 3 con ONTAP 9 quando si utilizza la replica basata su array tramite SRA. SRM non supporta la replica basata su array per NFS versione 4.1 con datastore tradizionali o vVols.
- Per confermare la connettività, verificare sempre che sia possibile montare e smontare un nuovo datastore di test sul sito DR dal cluster ONTAP di destinazione. Verificare ogni protocollo che si intende utilizzare per la connettività del datastore. Una Best practice consiste nell'utilizzare gli strumenti ONTAP per creare il datastore di test, poiché sta eseguendo tutta l'automazione del datastore come indicato da SRM.
- I protocolli SAN devono essere omogenei per ciascun sito. È possibile combinare NFS e SAN, ma i protocolli SAN non devono essere combinati all'interno di un sito. Ad esempio, è possibile utilizzare FCP nel sito A e iSCSI nel sito B. Non utilizzare sia FCP che iSCSI nel sito A. Il motivo è che l'SRA non crea gruppi igroup misti nel sito di ripristino e l'SRM non filtra l'elenco di iniziatori fornito all'SRA.
- Le guide precedenti hanno consigliato la creazione di una LIF in una località dati. Vale a dire, montare sempre un datastore utilizzando una LIF situata sul nodo che fisicamente possiede il volume. Questo non è più un requisito nelle versioni moderne di ONTAP 9. Quando possibile e se specifiche credenziali di ambito del cluster, i tool ONTAP continueranno a scegliere di bilanciare il carico tra le LIF locali dei dati, ma non è un requisito di high Availability o performance.
- ONTAP 9 può essere configurato in modo da rimuovere automaticamente le istantanee per preservare l'uptime in caso di esaurimento dello spazio quando il dimensionamento automatico non è in grado di fornire una capacità di emergenza sufficiente. L'impostazione predefinita di questa funzionalità non elimina automaticamente le snapshot create da SnapMirror. Se le snapshot SnapMirror vengono eliminate, il servizio SRA di NetApp non può invertire e risincronizzare la replica per il volume interessato. Per impedire a ONTAP di eliminare snapshot di SnapMirror, configurare la funzionalità di eliminazione automatica Snapshot in modo da provare.

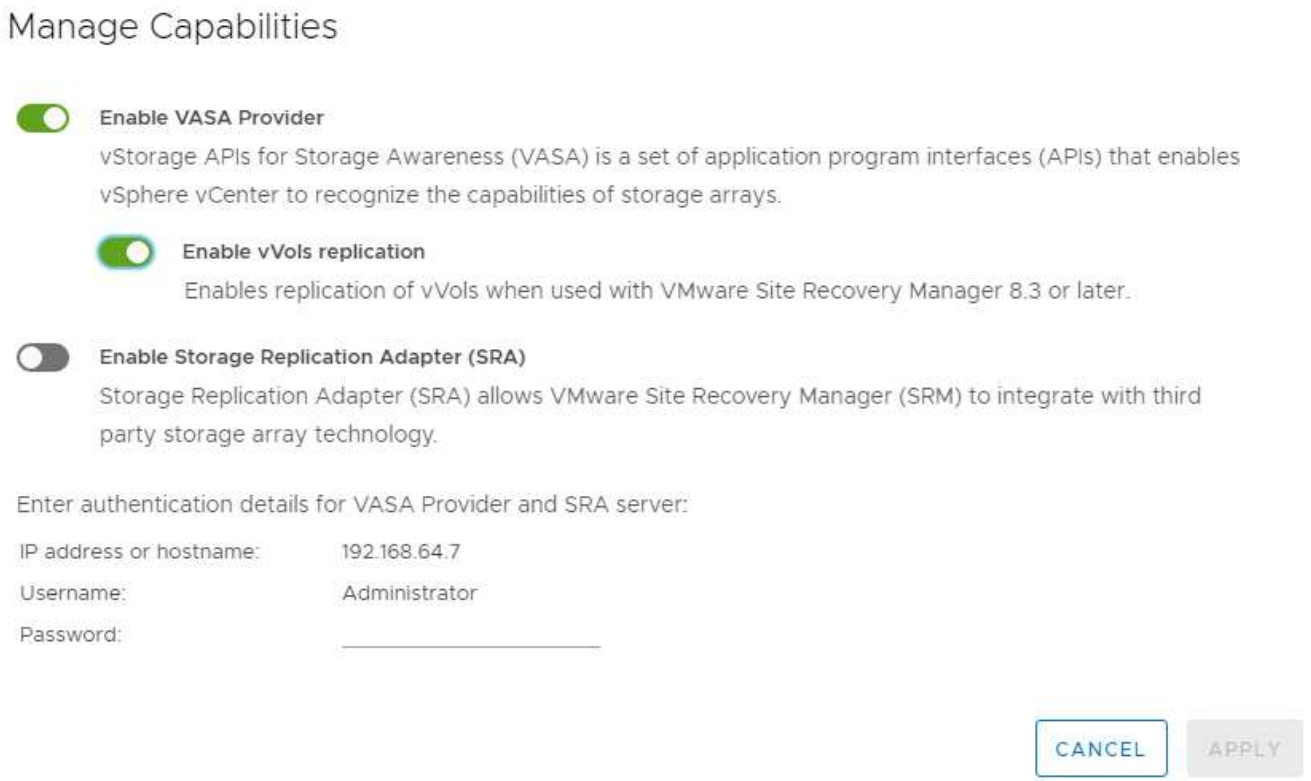
```
snap autodelete modify -volume -commitment try
```

- La dimensione automatica del volume deve essere impostata su `grow` Per volumi contenenti datastore SAN e. `grow_shrink` Per datastore NFS. Scopri di più "configurazione automatica dell'aumento o della riduzione dei volumi".
- SRM funziona al meglio quando il numero di datastore e quindi di gruppi di protezione viene ridotto al minimo nei piani di ripristino. È quindi opportuno prendere in considerazione l'ottimizzazione della densità delle macchine virtuali negli ambienti protetti con SRM in cui l'RTO è fondamentale.
- Utilizza DRS (Distributed Resource Scheduler) per bilanciare il carico sui cluster ESXi protetti e di recovery. Tenere presente che se si prevede di eseguire il failback, quando si esegue una nuova protezione i cluster precedentemente protetti diventeranno i nuovi cluster di ripristino. Il DRS aiuterà a bilanciare il posizionamento in entrambe le direzioni.
- Ove possibile, evitare di utilizzare la personalizzazione IP con SRM, poiché ciò può aumentare il vostro RTO.

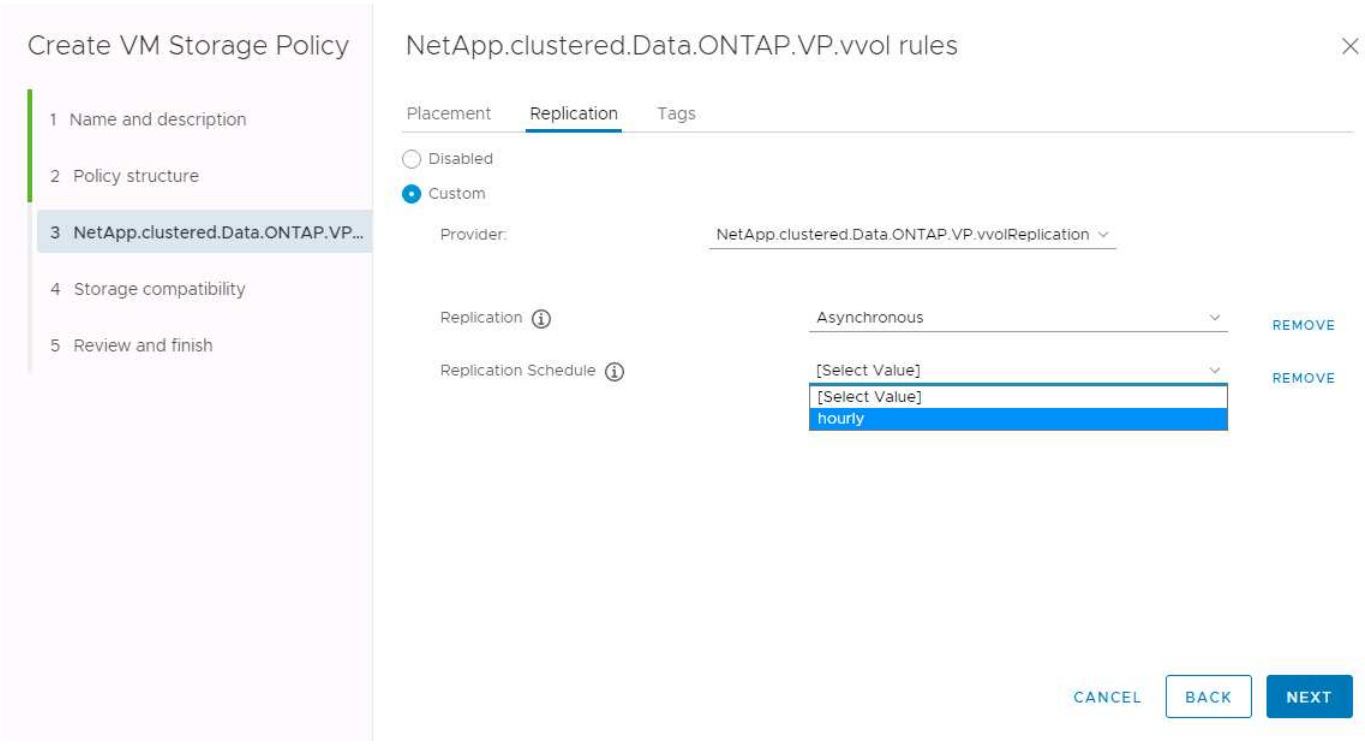
#### Gestione basata su criteri storage (SPBM, Storage Policy Based Management) e vVol

A partire da SRM 8,3, è supportata la protezione delle macchine virtuali che utilizzano gli archivi dati vVol. Le pianificazioni di SnapMirror sono esposte ai criteri di storage delle macchine virtuali dal provider VASA quando la replica di vVol è attivata nel menu delle impostazioni degli strumenti di ONTAP, come mostrato nelle seguenti schermate.

Nell'esempio riportato di seguito viene illustrata l'attivazione della replica vVol.

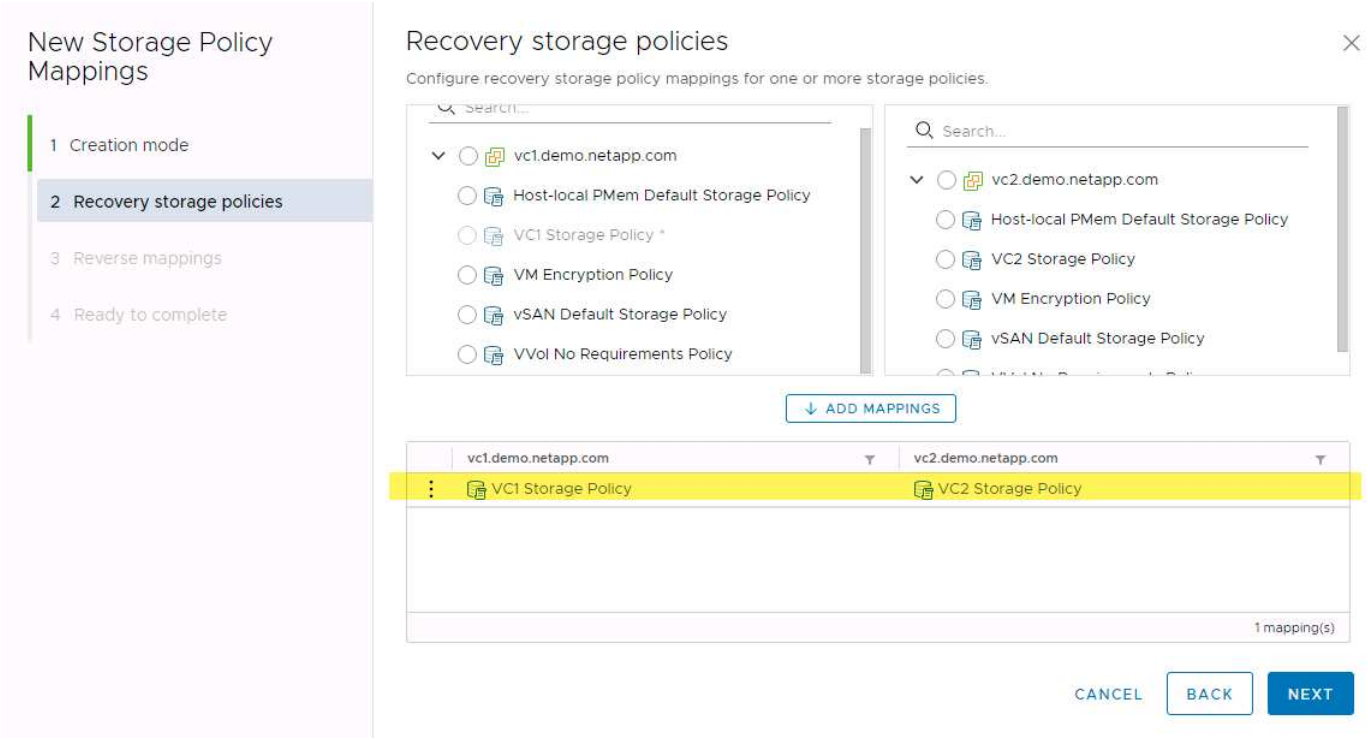



La seguente schermata fornisce un esempio di pianificazioni SnapMirror visualizzate nella procedura guidata Crea policy di storage VM.




Il provider VASA di ONTAP supporta il failover su storage diverso. Ad esempio, il sistema può eseguire il failover da ONTAP Select in una posizione periferica a un sistema AFF nel data center principale. Indipendentemente dalla somiglianza dello storage, è necessario configurare sempre le mappature dei criteri di storage e le mappature inverse per le policy di storage delle macchine virtuali abilitate alla replica per

garantire che i servizi forniti nel sito di recovery soddisfino le aspettative e i requisiti. La seguente schermata evidenzia un esempio di mappatura dei criteri.




**Creare volumi replicati per gli archivi dati vVols**

A differenza dei datastore vVols precedenti, gli archivi dati vVols replicati devono essere creati dall'inizio con la replica abilitata e devono utilizzare volumi pre-creati sui sistemi ONTAP con relazioni SnapMirror. Ciò richiede la preconfigurazione di elementi come il peering dei cluster e il peering SVM. Queste attività devono essere eseguite dall'amministratore ONTAP, in quanto ciò facilita una rigorosa separazione delle responsabilità tra coloro che gestiscono i sistemi ONTAP in più siti e coloro che sono i principali responsabili delle operazioni vSphere.

Questo viene fornito con un nuovo requisito per conto dell'amministratore di vSphere. Poiché i volumi vengono creati al di fuori dell'ambito degli strumenti di ONTAP, non è a conoscenza delle modifiche apportate dall'amministratore di ONTAP fino al periodo di riscoperta regolarmente pianificato. Per questo motivo, è consigliabile eseguire sempre la risDiscovery ogni volta che si crea un volume o una relazione SnapMirror da utilizzare con i vVol. È sufficiente fare clic con il pulsante destro del mouse sull'host o sul cluster e selezionare ONTAP tools > Update host and Storage Data (Strumenti > Aggiorna dati host e archiviazione), come illustrato nella seguente schermata.

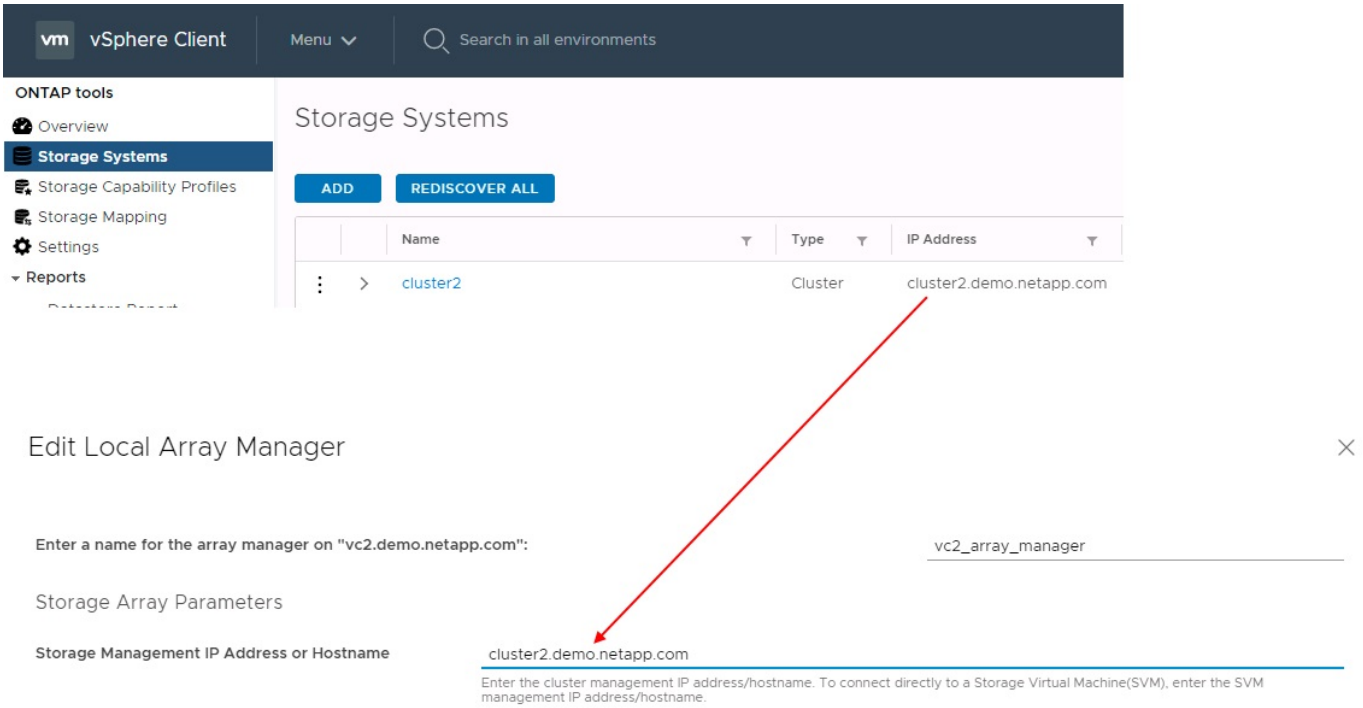

Si consiglia di prestare attenzione quando si tratta di vVol e SRM. Non mischiare mai macchine virtuali protette e non protette nello stesso datastore vVols. Il motivo è che quando si utilizza SRM per eseguire il failover sul sito DR, solo le macchine virtuali che fanno parte del gruppo di protezione vengono messe in linea nel DR. Pertanto, quando si esegue una nuova protezione (reverse SnapMirror dal DR di nuovo alla produzione), è possibile sovrascrivere le macchine virtuali che non hanno eseguito il failover e che potrebbero contenere dati

preziosi.

### Informazioni sulle coppie di array

Viene creato un gestore di array per ogni coppia di array. Con gli strumenti SRM e ONTAP, ogni accoppiamento di array viene eseguito con l'ambito di una SVM, anche se si utilizzano le credenziali del cluster. Ciò consente di segmentare i flussi di lavoro DR tra tenant in base alle SVM assegnate per la gestione. È possibile creare più array manager per un determinato cluster e possono essere asimmetrici. È possibile eseguire il fan-out o il fan-in tra diversi cluster di ONTAP 9. Ad esempio, è possibile utilizzare SVM-A e SVM-B nel cluster-1 in replica su SVM-C nel cluster-2, SVM-D nel cluster-3 o viceversa.

Quando si configurano le coppie di array in SRM, è necessario aggiungerle sempre in SRM nello stesso modo in cui sono state aggiunte agli strumenti ONTAP, ovvero devono utilizzare lo stesso nome utente, password e LIF di gestione. Questo requisito garantisce che SRA comunichi correttamente con l'array. La seguente schermata illustra come potrebbe essere visualizzato un cluster negli strumenti ONTAP e come potrebbe essere aggiunto a un gestore di array.




### Informazioni sui gruppi di replica

I gruppi di replica contengono raccolte logiche di macchine virtuali che vengono ripristinate insieme. Il provider VASA di ONTAP Tools crea automaticamente i gruppi di replica. Poiché la replica di ONTAP SnapMirror avviene a livello di volume, tutte le macchine virtuali di un volume si trovano nello stesso gruppo di replica.

Esistono diversi fattori da considerare per i gruppi di replica e il modo in cui si distribuiscono le macchine virtuali tra i volumi FlexVol. Il raggruppamento di macchine virtuali simili nello stesso volume può aumentare l'efficienza dello storage con i sistemi ONTAP meno recenti che non dispongono di una deduplica a livello di aggregato, ma il raggruppamento aumenta la dimensione del volume e riduce l'simultaneità dell'i/O. Il miglior equilibrio tra performance ed efficienza dello storage si può ottenere negli attuali sistemi ONTAP distribuendo le VM su volumi FlexVol nello stesso aggregato, sfruttando così la deduplica a livello di aggregato e ottenendo una maggiore parallelizzazione i/o su più volumi. È possibile ripristinare le macchine virtuali nei volumi insieme perché un gruppo di protezione (discusso di seguito) può contenere più gruppi di replica. Lo svantaggio di questo layout è che i blocchi potrebbero essere trasmessi più volte via cavo perché SnapMirror per i volumi non prende in considerazione la deduplica degli aggregati.

Un'ultima considerazione per i gruppi di replica è che ciascuno di essi è per sua natura un gruppo di coerenza logica (da non confondere con i gruppi di coerenza SRM). Questo perché tutte le VM nel volume vengono trasferite insieme utilizzando lo stesso snapshot. Pertanto, se si dispone di macchine virtuali che devono essere coerenti tra loro, è consigliabile memorizzarle nello stesso FlexVol.

### A proposito dei gruppi di protezione

I gruppi di protezione definiscono macchine virtuali e datastore in gruppi che vengono ripristinati insieme dal sito protetto. Il sito protetto è il luogo in cui esistono le macchine virtuali configurate in un gruppo di protezione durante le normali operazioni in stato stazionario. È importante notare che anche se SRM potrebbe visualizzare più gestori di array per un gruppo di protezione, un gruppo di protezione non può estendersi a più gestori di array. Per questo motivo, non è necessario estendere i file delle macchine virtuali tra gli archivi dati su macchine virtuali SVM diverse.

### Sui piani di recovery

I piani di recovery definiscono quali gruppi di protezione vengono ripristinati nello stesso processo. È possibile configurare più gruppi di protezione nello stesso piano di ripristino. Inoltre, per abilitare più opzioni per l'esecuzione dei piani di ripristino, è possibile includere un singolo gruppo di protezione in più piani di ripristino.

I piani di recovery consentono agli amministratori SRM di definire i flussi di lavoro di recovery assegnando le macchine virtuali a un gruppo di priorità da 1 (massimo) a 5 (minimo), con 3 (medio) come valore predefinito. All'interno di un gruppo di priorità, le VM possono essere configurate per le dipendenze.

Ad esempio, la tua azienda potrebbe disporre di un'applicazione business-critical Tier 1 che si affida a un server Microsoft SQL per il proprio database. Quindi, si decide di inserire le macchine virtuali nel gruppo di priorità 1. All'interno del gruppo di priorità 1, si inizia a pianificare l'ordine per visualizzare i servizi. Probabilmente si desidera che il controller di dominio Microsoft Windows venga avviato prima del server Microsoft SQL, che deve essere online prima del server dell'applicazione e così via. È necessario aggiungere tutte queste macchine virtuali al gruppo di priorità e quindi impostare le dipendenze perché le dipendenze si applicano solo all'interno di un determinato gruppo di priorità.

NetApp consiglia vivamente di collaborare con i team delle applicazioni per comprendere l'ordine delle operazioni richieste in uno scenario di failover e per costruire di conseguenza i piani di recovery.

### Test del failover

Come Best practice, eseguire sempre un test di failover ogni volta che viene apportata una modifica alla configurazione di uno storage VM protetto. In questo modo, in caso di emergenza, è possibile verificare che Site Recovery Manager sia in grado di ripristinare i servizi entro la destinazione RTO prevista.

NetApp consiglia inoltre di confermare occasionalmente la funzionalità delle applicazioni in-guest, soprattutto dopo la riconfigurazione dello storage delle macchine virtuali.

Quando viene eseguita un'operazione di test recovery, viene creata una rete bubble di test privata sull'host ESXi per le macchine virtuali. Tuttavia, questa rete non è connessa automaticamente ad alcun adattatore di rete fisico e pertanto non fornisce connettività tra gli host ESXi. Per consentire la comunicazione tra macchine virtuali in esecuzione su host ESXi diversi durante il test di DR, viene creata una rete fisica privata tra gli host ESXi nel sito di DR. Per verificare che la rete di test sia privata, è possibile separare fisicamente la rete a bolle di test oppure utilizzando VLAN o tag VLAN. Questa rete deve essere separata dalla rete di produzione, in quanto non è possibile posizionare le macchine virtuali sulla rete di produzione con indirizzi IP che potrebbero entrare in conflitto con i sistemi di produzione effettivi. Quando viene creato un piano di ripristino in SRM, la rete di test creata può essere selezionata come rete privata a cui connettere le macchine virtuali durante il test.

Una volta convalidato il test e non più necessario, eseguire un'operazione di pulizia. L'esecuzione della pulizia

riporta le macchine virtuali protette al loro stato iniziale e ripristina il piano di ripristino allo stato Pronta.

### Considerazioni sul failover

Oltre all'ordine delle operazioni indicato in questa guida, è necessario considerare anche altri aspetti relativi al failover di un sito.

Un problema che potrebbe essere dovuto affrontare è rappresentato dalle differenze di rete tra i siti. Alcuni ambienti potrebbero essere in grado di utilizzare gli stessi indirizzi IP di rete sia nel sito primario che nel sito di DR. Questa capacità viene definita come una LAN virtuale estesa (VLAN) o una configurazione di rete estesa. Altri ambienti potrebbero richiedere l'utilizzo di indirizzi IP di rete diversi (ad esempio, in VLAN diverse) nel sito primario rispetto al sito di DR.

VMware offre diversi modi per risolvere questo problema. Per prima cosa, le tecnologie di virtualizzazione di rete come VMware NSX-T Data Center astraggono l'intero stack di rete dai livelli 2 fino a 7 dall'ambiente operativo, consentendo soluzioni più portatili. Scopri di più "Opzioni NSX-T con SRM".

SRM consente inoltre di modificare la configurazione di rete di una macchina virtuale durante il ripristino. Questa riconfigurazione include impostazioni quali indirizzi IP, indirizzi gateway e impostazioni del server DNS. È possibile specificare diverse impostazioni di rete, che vengono applicate alle singole macchine virtuali non appena vengono recuperate, nelle impostazioni della proprietà di una macchina virtuale nel piano di ripristino.

Per configurare SRM in modo che applichi impostazioni di rete diverse a più macchine virtuali senza dover modificare le proprietà di ciascuna di esse nel piano di ripristino, VMware fornisce uno strumento chiamato dr-ip-customizer. Per informazioni sull'utilizzo di questa utilità, fare riferimento alla sezione "Documentazione di VMware".

### Proteggere di nuovo

Dopo un ripristino, il sito di ripristino diventa il nuovo sito di produzione. Poiché l'operazione di ripristino ha rotto la replica di SnapMirror, il nuovo sito di produzione non è protetto da eventuali disastri futuri. Una Best practice consiste nel proteggere il nuovo sito di produzione in un altro sito immediatamente dopo un ripristino. Se il sito di produzione originale è operativo, l'amministratore di VMware può utilizzare il sito di produzione originale come nuovo sito di ripristino per proteggere il nuovo sito di produzione, invertendo efficacemente la direzione della protezione. La protezione è disponibile solo in caso di guasti non catastrofici. Pertanto, i server vCenter originali, i server ESXi, i server SRM e i database corrispondenti devono essere ripristinabili. Se non sono disponibili, è necessario creare un nuovo gruppo di protezione e un nuovo piano di ripristino.

### Failback

Un'operazione di failback è fondamentalmente un failover in una direzione diversa rispetto a prima. Come Best practice, prima di tentare di eseguire il failback o, in altre parole, di eseguire il failover sul sito originale, è necessario verificare che il sito originale sia tornato a livelli di funzionalità accettabili. Se il sito originale è ancora compromesso, è necessario ritardare il failback fino a quando il guasto non viene risolto in modo adeguato.

Un'altra Best practice per il failback consiste nell'eseguire sempre un failover di test dopo aver completato la protezione e prima di eseguire il failback finale. In questo modo si verifica che i sistemi installati presso il sito originale possano completare l'operazione.

### Protezione del sito originale

Dopo il failback, è necessario confermare con tutti gli stakeholder che i loro servizi sono stati riportati alla normalità prima di eseguire nuovamente la funzione di protezione,

L’esecuzione di una nuova protezione dopo il failback riporta sostanzialmente l’ambiente nello stato in cui si trovava all’inizio, con la replica di SnapMirror nuovamente in esecuzione dal sito di produzione al sito di ripristino.

## Topologie di replica

In ONTAP 9, i componenti fisici di un cluster sono visibili agli amministratori del cluster, ma non sono direttamente visibili alle applicazioni e agli host che utilizzano il cluster. I componenti fisici forniscono un pool di risorse condivise da cui vengono costruite le risorse del cluster logico. Le applicazioni e gli host accedono ai dati solo tramite SVM che contengono volumi e LIF.

Ogni SVM NetApp viene trattata come array in VMware vCenter Site Recovery Manager. SRM supporta determinati layout di replica array-to-array (o SVM-to-SVM).

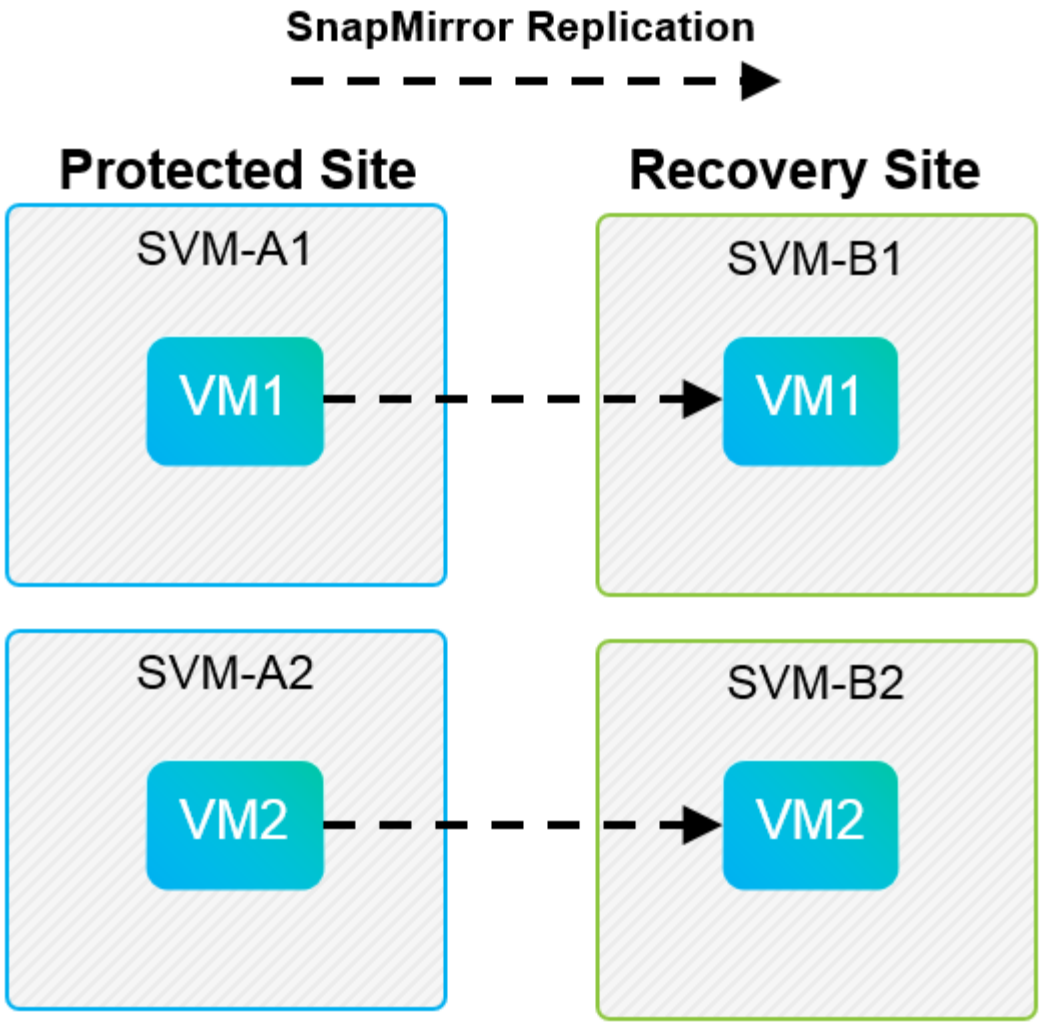
Una singola macchina virtuale non è in grado di gestire i dati (VMDK) o RDM) su più array SRM per i seguenti motivi:

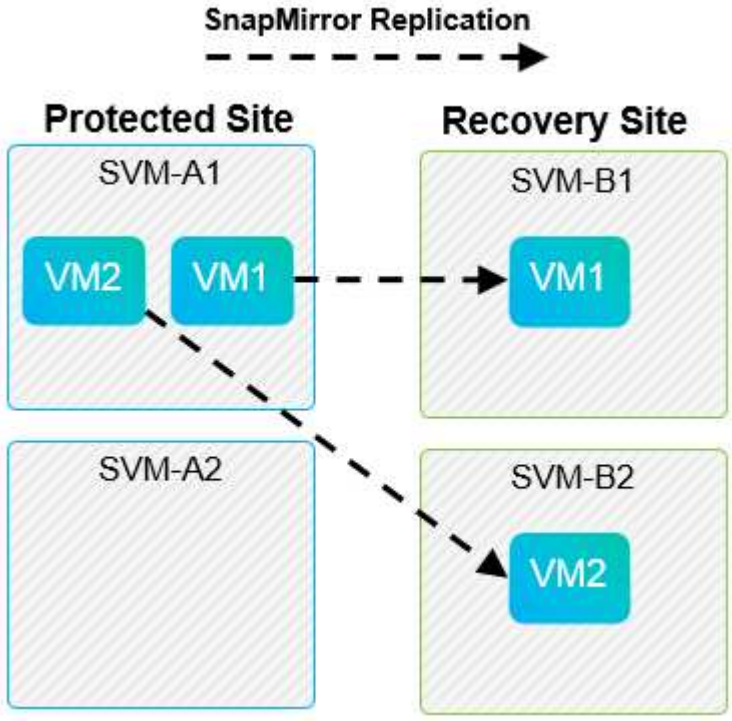
- SRM vede solo la SVM, non un singolo controller fisico.
- Una SVM può controllare LUN e volumi che si estendono su più nodi in un cluster.

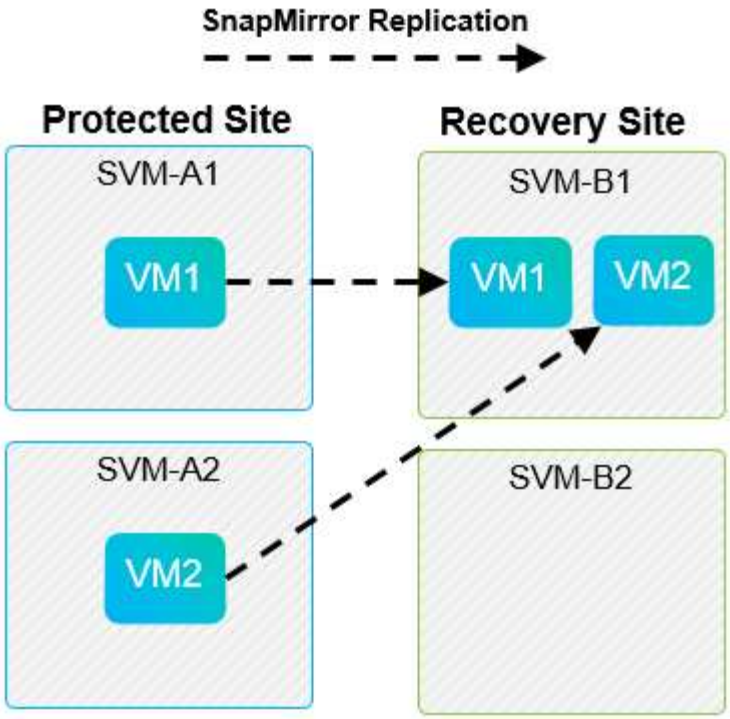
| **Best practice** |
| --- |
| Per determinare la supportabilità, tenere presente questa regola: Per proteggere una macchina virtuale utilizzando SRM e NetApp SRA, tutte le parti della macchina virtuale devono esistere su un solo SVM. Questa regola si applica sia al sito protetto che al sito di ripristino. |

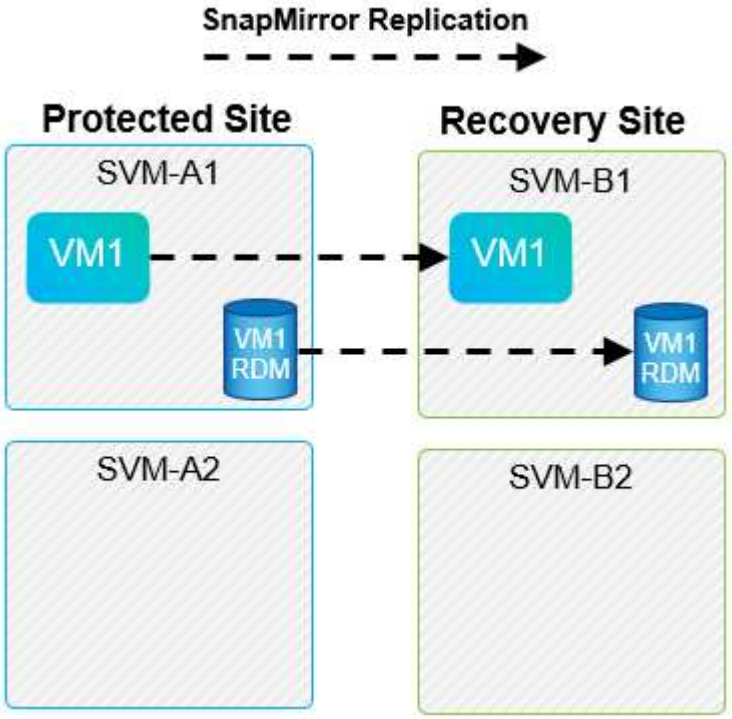
### Layout SnapMirror supportati

Le seguenti figure mostrano gli scenari di layout delle relazioni SnapMirror supportati da SRM e SRA. Ogni macchina virtuale nei volumi replicati possiede i dati su un solo array SRM (SVM) in ogni sito.


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2

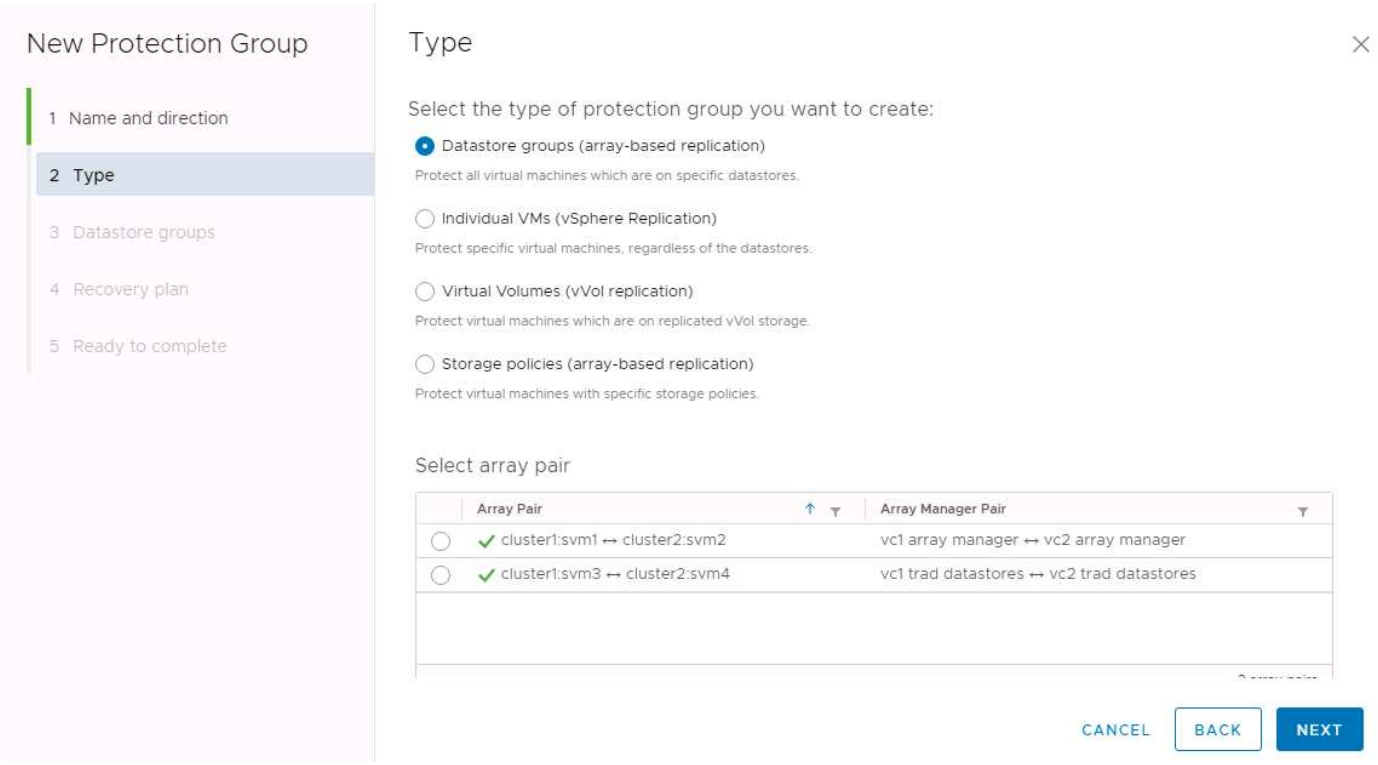

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2



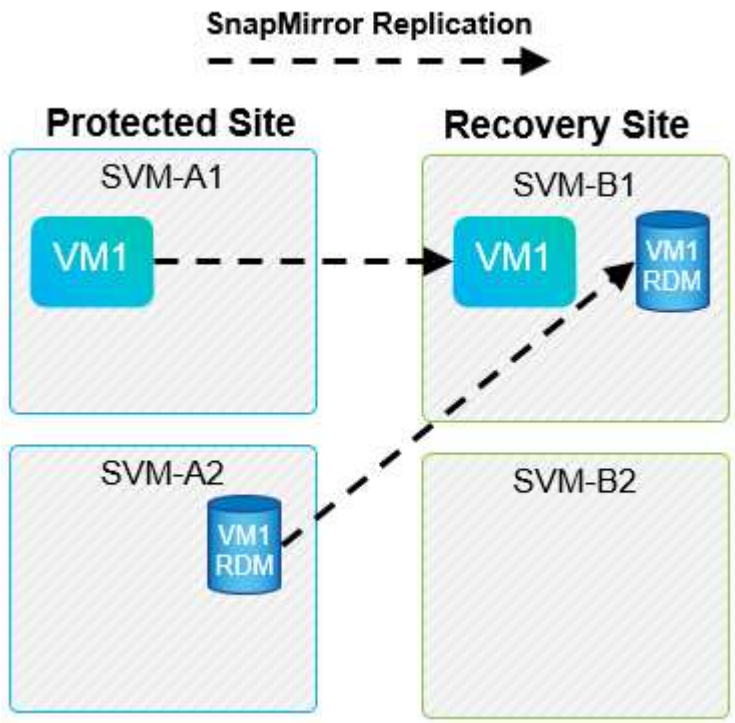

**Layout di Array Manager supportati**

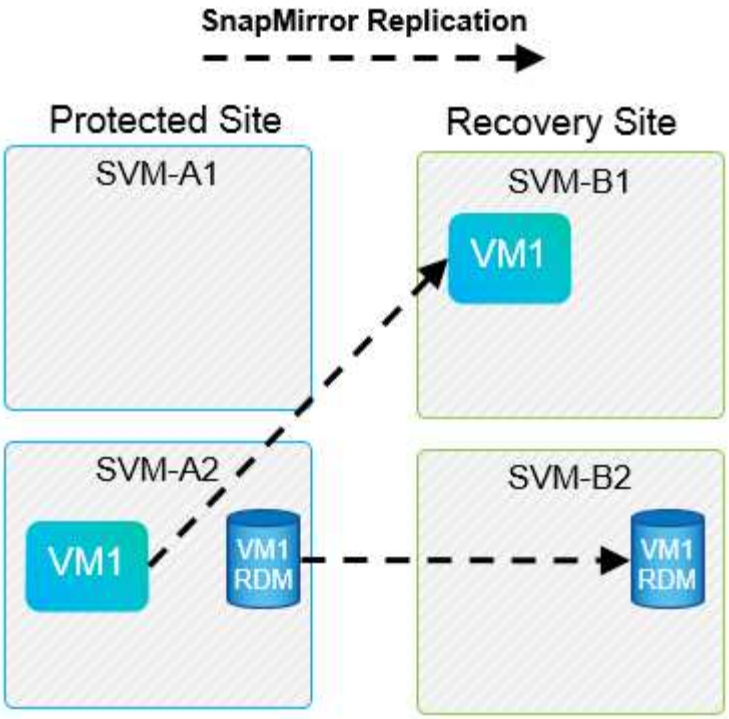
Quando si utilizza la replica basata su array (ABR) in SRM, i gruppi di protezione vengono isolati in una singola coppia di array, come illustrato nella seguente schermata. In questo scenario, `SVM1` e. `SVM2` sono in coppia con `SVM3` e. `SVM4` presso il sito di recovery. Tuttavia, è possibile selezionare solo una delle due coppie di array quando si crea un gruppo di protezione.



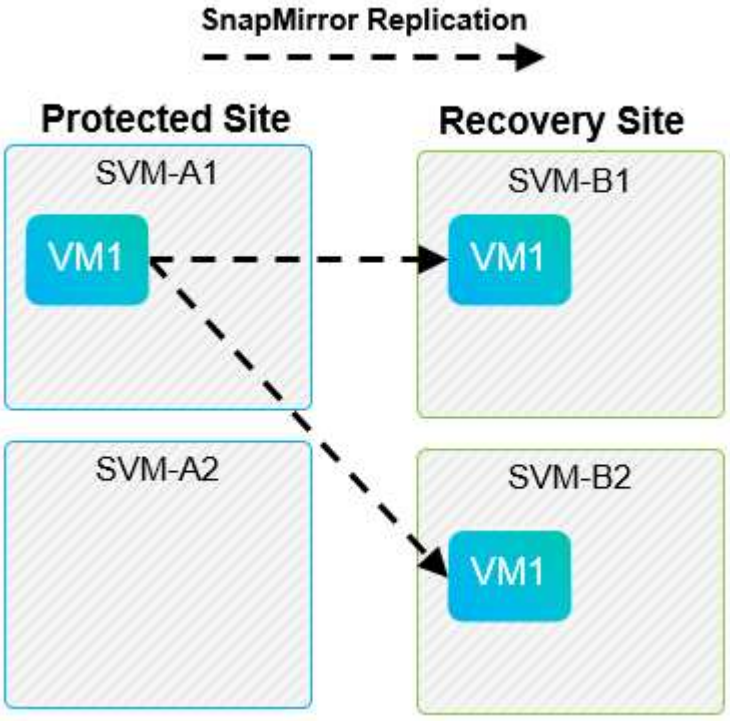

### Layout non supportati

Le configurazioni non supportate dispongono di dati (VMDK o RDM) su più SVM di proprietà di una singola macchina virtuale. Negli esempi illustrati nelle seguenti figure, `VM1` Impossibile configurare la protezione con SRM perché `VM1` Dispone di dati su due SVM.





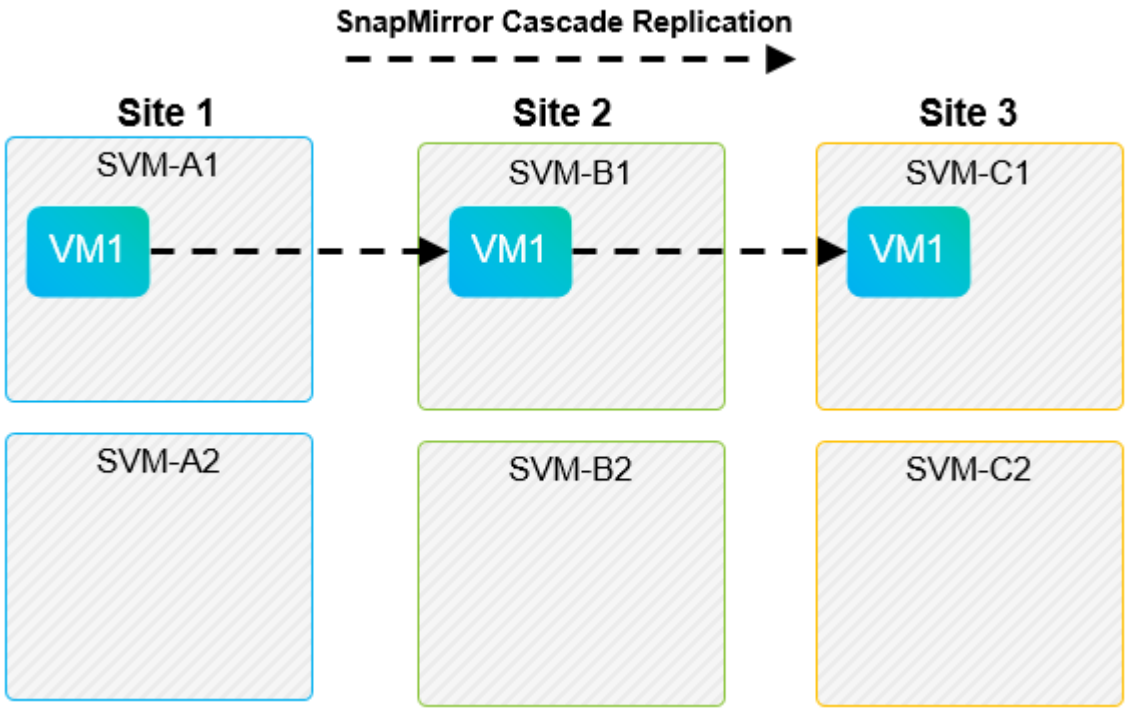

Qualsiasi relazione di replica in cui un singolo volume NetApp viene replicato da una SVM di origine a più destinazioni nella stessa SVM o in SVM differenti viene definita fan-out di SnapMirror. Fan-out non supportato con SRM. Nell'esempio illustrato nella figura seguente, `VM1` Impossibile configurare la protezione in SRM perché viene replicata con SnapMirror in due posizioni diverse.




**Cascata di SnapMirror**

SRM non supporta la sovrapposizione delle relazioni SnapMirror, in cui un volume di origine viene replicato in un volume di destinazione e tale volume di destinazione viene replicato anche con SnapMirror in un altro volume di destinazione. Nello scenario illustrato nella figura seguente, SRM non può essere utilizzato per il

failover tra siti.




**SnapMirror e SnapVault**

Il software NetApp SnapVault consente il backup basato su disco dei dati aziendali tra i sistemi storage NetApp. SnapVault e SnapMirror possono coesistere nello stesso ambiente; tuttavia, SRM supporta il failover solo delle relazioni SnapMirror.

NetApp SRA supporta `mirror-vault` tipo di policy.

SnapVault è stato ricostruito da zero per ONTAP 8.2. Anche se gli utenti di Data ONTAP 7-Mode precedenti dovrebbero trovare delle analogie, in questa versione di SnapVault sono stati apportati importanti miglioramenti. Un importante progresso è la capacità di preservare l'efficienza dello storage sui dati primari durante i trasferimenti SnapVault.

Un'importante modifica architetturale è che SnapVault in ONTAP 9 replica a livello di volume anziché a livello di qtree, come nel caso di 7-Mode SnapVault. Questa configurazione indica che l'origine di una relazione SnapVault deve essere un volume e che tale volume deve replicarsi nel proprio volume sul sistema secondario SnapVault.

In un ambiente in cui viene utilizzato SnapVault, vengono create snapshot specificatamente denominate sul sistema di storage primario. A seconda della configurazione implementata, gli snapshot denominati possono essere creati sul sistema primario da una pianificazione SnapVault o da un'applicazione come NetApp Active IQ Unified Manager. Gli Snapshot con nome creati sul sistema primario vengono quindi replicati nella destinazione SnapMirror, da dove vengono trasferiti in un vault nella destinazione SnapVault.

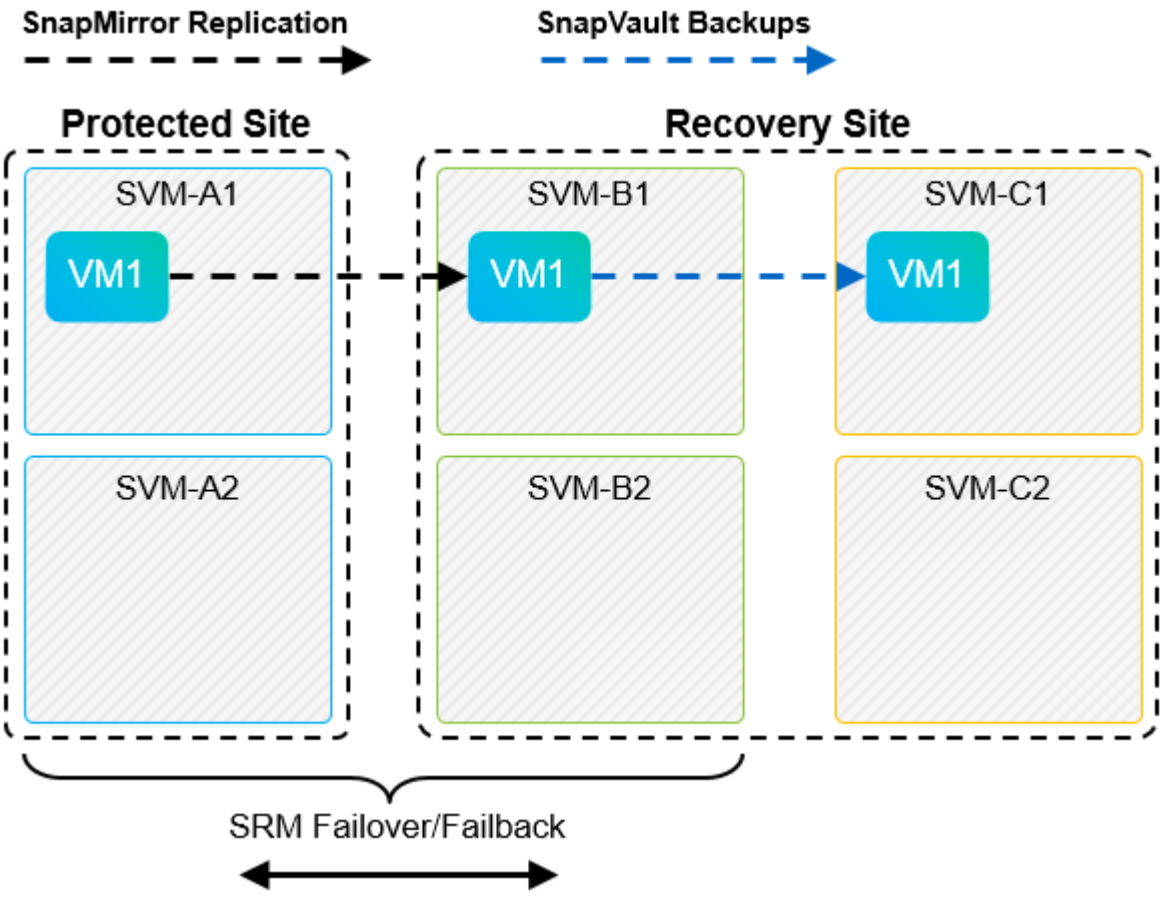
È possibile creare un volume di origine in una configurazione a cascata in cui un volume viene replicato in una destinazione SnapMirror nel sito DR e da qui viene vault in una destinazione SnapVault. È possibile creare un volume di origine anche in una relazione fan-out in cui una destinazione è una destinazione SnapMirror e l'altra destinazione è una destinazione SnapVault. Tuttavia, SRA non riconfigurerà automaticamente la relazione SnapVault per utilizzare il volume di destinazione SnapMirror come origine per il vault quando si verifica il failover SRM o l'inversione della replica.

Per informazioni aggiornate su SnapMirror e SnapVault per ONTAP 9, vedere "Guida alle Best practice per la configurazione di SnapMirror TR-4015 per ONTAP 9."

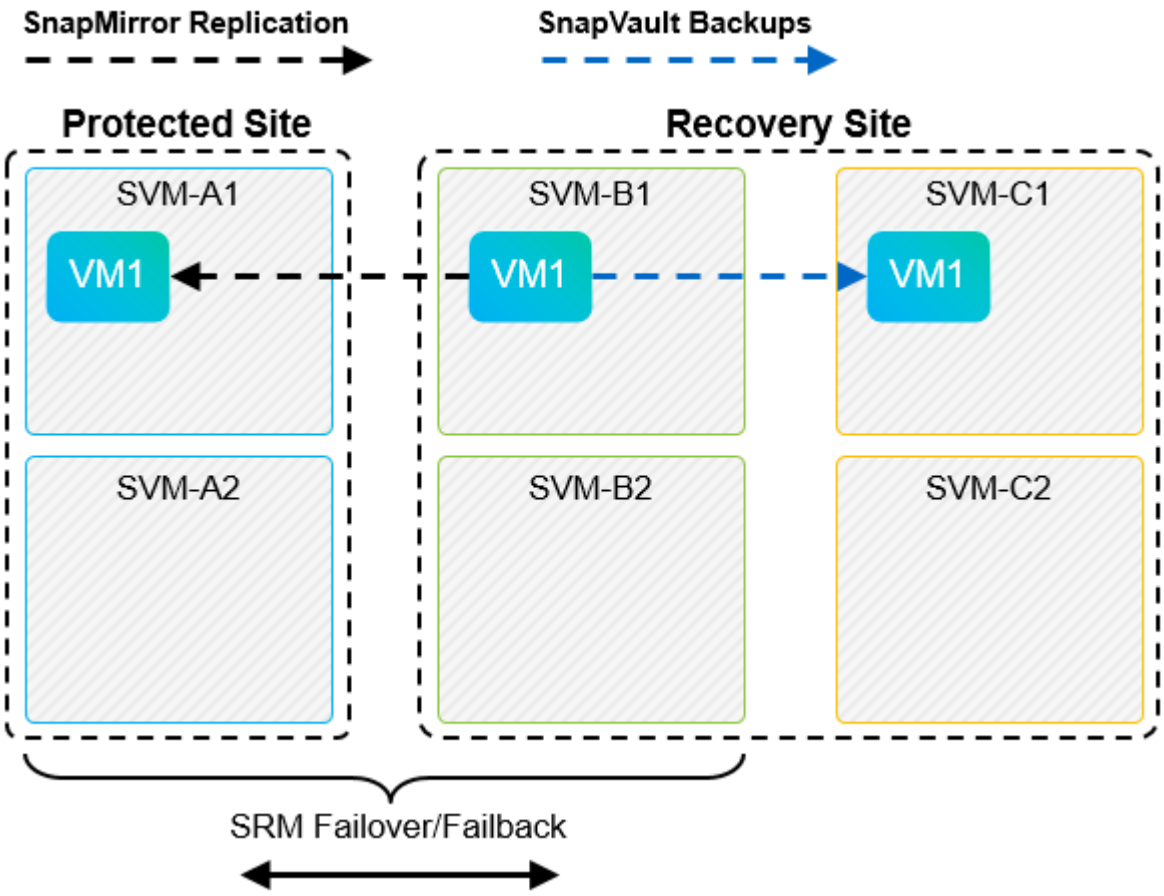
| Best practice |
| --- |
| Se SnapVault e SRM vengono utilizzati nello stesso ambiente, NetApp consiglia di utilizzare una configurazione a cascata da SnapMirror a SnapVault in cui i backup di SnapVault vengono normalmente eseguiti dalla destinazione di SnapMirror nel sito di DR. In caso di disastro, questa configurazione rende il sito primario inaccessibile. Mantenendo la destinazione SnapVault nel sito di recovery, è possibile riconfigurare i backup SnapVault dopo il failover in modo che i backup SnapVault possano continuare mentre si opera nel sito di recovery. |

In un ambiente VMware, ogni datastore dispone di un UUID (Universal Unique Identifier) e ogni VM dispone di un MOID (Managed Object ID) univoco. Questi ID non vengono gestiti da SRM durante il failover o il failback. Poiché gli UUID degli archivi di dati e i MOID delle macchine virtuali non vengono mantenuti durante il failover da SRM, tutte le applicazioni che dipendono da questi ID devono essere riconfigurate dopo il failover di SRM. Un'applicazione di esempio è NetApp Active IQ Unified Manager, che coordina la replica SnapVault con l'ambiente vSphere.

La figura seguente mostra una configurazione a cascata da SnapMirror a SnapVault. Se la destinazione SnapVault si trova nel sito di DR o in un sito terzo che non è interessato da un'interruzione nel sito primario, l'ambiente può essere riconfigurato per consentire ai backup di continuare dopo il failover.




La seguente figura illustra la configurazione dopo l'utilizzo di SRM per eseguire il reverse della replica di SnapMirror nel sito primario. L'ambiente è stato anche riconfigurato in modo che i backup di SnapVault si verifichino da quella che ora è l'origine di SnapMirror. Questa configurazione è una configurazione fan-out di SnapMirror SnapVault.




Dopo che SRM esegue il failback e una seconda inversione delle relazioni SnapMirror, i dati di produzione vengono ripristinati nel sito primario. Questi dati sono ora protetti nello stesso modo in cui erano prima del failover al sito di DR, tramite i backup SnapMirror e SnapVault.

### Utilizzo di Qtree in ambienti Site Recovery Manager

I qtree sono directory speciali che consentono l'applicazione delle quote del file system per NAS. ONTAP 9 consente la creazione di qtree e qtree possono esistere in volumi replicati con SnapMirror. Tuttavia, SnapMirror non consente la replica di singoli qtree o replica a livello di qtree. Tutte le repliche di SnapMirror sono solo a livello di volume. Per questo motivo, NetApp sconsiglia l'utilizzo di qtree con SRM.

### Ambienti misti FC e iSCSI

Con i protocolli SAN supportati (FC, FCoE e iSCSI), ONTAP 9 offre servizi LUN, ovvero la possibilità di creare e mappare LUN agli host collegati. Poiché il cluster è costituito da più controller, esistono più percorsi logici gestiti da i/o multipath verso qualsiasi LUN individuale. L'ALUA (Asymmetric Logical Unit Access) viene utilizzato sugli host in modo che il percorso ottimizzato per un LUN sia selezionato e reso attivo per il trasferimento dei dati. Se il percorso ottimizzato per qualsiasi LUN cambia (ad esempio, perché il volume contenente viene spostato), ONTAP 9 riconosce automaticamente e regola senza interruzioni per questa modifica. Se il percorso ottimizzato non è disponibile, ONTAP può passare senza interruzioni a qualsiasi altro percorso disponibile.

VMware SRM e NetApp SRA supportano l'utilizzo del protocollo FC in un sito e del protocollo iSCSI nell'altro. Tuttavia, non supporta la combinazione di datastore FC-attached e datastore iSCSI-attached nello stesso host ESXi o in host diversi nello stesso cluster. Questa configurazione non è supportata con SRM perché, durante il failover SRM o il failover di test, SRM include tutti gli iniziatori FC e iSCSI negli host ESXi nella richiesta.

| Best practice |
| --- |
| SRM e SRA supportano protocolli FC e iSCSI misti tra i siti protetti e di ripristino. Tuttavia, ogni sito deve essere configurato con un solo protocollo, FC o iSCSI, non entrambi nello stesso sito. Se esiste un requisito per la configurazione dei protocolli FC e iSCSI nello stesso sito, NetApp consiglia che alcuni host utilizzino iSCSI e altri host utilizzino FC. In questo caso, NetApp consiglia anche di configurare le mappature delle risorse SRM in modo che le macchine virtuali siano configurate per il failover in un gruppo di host o nell'altro. |

## Risoluzione dei problemi di SRM quando si utilizza la replica vVol

Il flusso di lavoro all'interno di SRM è significativamente diverso quando si utilizza la replica vVol da quello utilizzato con SRA e datastore tradizionali. Ad esempio, non esiste alcun concetto di gestore di array. In quanto tale, `discoverarrays` e. `discoverdevices` i comandi non vengono mai visualizzati.

Durante la risoluzione dei problemi, è utile comprendere i nuovi flussi di lavoro, elencati di seguito:

1. QueryReplicationPeer: Rileva gli accordi di replica tra due domini di errore.
2. QueryFaultDomain: Rileva la gerarchia di dominio di errore.
3. QueryReplicationGroup: Consente di individuare i gruppi di replica presenti nei domini di origine o di destinazione.
4. SyncReplicationGroup: Sincronizza i dati tra origine e destinazione.
5. QueryPointInTimeReplica: Consente di rilevare le repliche point-in-time di una destinazione.
6. TestFailoverReplicationGroupStart: Avvia il failover del test.
7. TestFailoverReplicationGroupStop: Termina il failover del test.
8. PromoteReplicationGroup: Promuove un gruppo attualmente in fase di test in produzione.
9. PrepareFailoverReplicationGroup: Prepara per un disaster recovery.
10. FailoverReplicationGroup: Esegue il disaster recovery.
11. ReverseReplicateGroup: Avvia la replica inversa.
12. QueryMatchingContainer: Trova i container (insieme agli host o ai gruppi di replica) che potrebbero soddisfare una richiesta di provisioning con una determinata policy.
13. QueryResourceMetadata: Rileva i metadati di tutte le risorse dal provider VASA, l'utilizzo delle risorse può essere restituito come risposta alla funzione QueryMatchingContainer.

L'errore più comune riscontrato durante la configurazione della replica di vVol è il mancato rilevamento delle relazioni di SnapMirror. Ciò si verifica perché i volumi e le relazioni di SnapMirror vengono creati al di fuori dell'ambito di applicazione degli strumenti ONTAP. Pertanto, è consigliabile assicurarsi sempre che la relazione di SnapMirror sia completamente inizializzata e che sia stata eseguita una riscoperta negli strumenti ONTAP in entrambi i siti prima di tentare di creare un datastore vVol replicato.

## Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- TR-4597: VMware vSphere per ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"

- TR-4400: Volumi virtuali VMware vSphere con ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- Guida alle Best practice per la configurazione di SnapMirror TR-4015 per ONTAP 9
  https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- Creatore utente RBAC per ONTAP
  "https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- Strumenti ONTAP per le risorse VMware vSphere
  "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- Documentazione di VMware Site Recovery Manager
  "https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

Fare riferimento a. "Tool di matrice di interoperabilità (IMT)" Sul sito del supporto NetApp per verificare che le versioni esatte dei prodotti e delle funzionalità descritte in questo documento siano supportate per il tuo ambiente specifico. NetApp IMT definisce i componenti e le versioni dei prodotti che possono essere utilizzati per costruire configurazioni supportate da NetApp. I risultati specifici dipendono dall'installazione di ciascun cliente in conformità alle specifiche pubblicate.

# VSphere Metro Storage Cluster con ONTAP

## VSphere Metro Storage Cluster con ONTAP

L'hypervisor vSphere leader del settore di VMware può essere implementato come cluster stretched indicato come vSphere Metro Storage Cluster (vMSC).

Le soluzioni vMSC sono supportate sia con NetApp® MetroCluster™ che con SnapMirror Active Sync (precedentemente noto come SnapMirror Business Continuity o SMBC) e forniscono una business continuity avanzata se uno o più domini di errore subiscono un'interruzione totale. La resilienza alle diverse modalità di errore dipende dalle opzioni di configurazione scelte.

#### Soluzioni di disponibilità continua per ambienti vSphere

L'architettura ONTAP è una piattaforma di storage flessibile e scalabile che fornisce servizi SAN (FCP, iSCSI e NVMe-of) e NAS (NFS v3 e v4,1) per datastore. I sistemi storage NetApp AFF, ASA e FAS utilizzano il sistema operativo ONTAP per offrire protocolli aggiuntivi per l'accesso allo storage guest, come S3 e SMB/CIFS.

NetApp MetroCluster utilizza la funzione di ha (failover del controller o CFO) di NetApp per la protezione dai guasti dei controller. Include inoltre la tecnologia SyncMirror locale, il failover cluster in caso di disastro (failover controller on-demand o CFOD), la ridondanza hardware e la separazione geografica per ottenere livelli elevati di disponibilità. SyncMirror esegue il mirroring sincrono dei dati tra le due metà della configurazione MetroCluster scrivendo i dati su due plessi: Il plesso locale (sullo shelf locale) fornendo attivamente i dati e il plesso remoto (sullo shelf remoto) normalmente non fornendo i dati. La ridondanza hardware viene implementata per tutti i componenti MetroCluster, come controller, storage, cavi, switch (utilizzati con Fabric MetroCluster) e adattatori.

La sincronizzazione attiva di NetApp SnapMirror fornisce una protezione granulare dei datastore con protocolli SAN FCP e iSCSI, permettendoti di proteggere in modo selettivo solo i carichi di lavoro ad alta priorità. Offre l'accesso Active-Active ai siti locali e remoti, a differenza di NetApp MetroCluster, che è una soluzione Active-standby. Attualmente, la sincronizzazione attiva è una soluzione asimmetrica in cui un lato è preferito rispetto all'altro, fornendo prestazioni migliori. Ciò si ottiene utilizzando la funzionalità ALUA (Asymmetric Logical Unit Access) che informa automaticamente l'host ESXi, quali controller preferire. Tuttavia, NetApp ha annunciato che la sincronizzazione attiva presto abiliterà l'accesso completamente simmetrico.

Per creare un cluster VMware ha/DRS su due siti, gli host ESXi vengono utilizzati e gestiti da un'appliance vCenter Server (VCSA). Le reti di gestione vSphere, vMotion® e delle macchine virtuali sono collegate tramite una rete ridondante tra i due siti. VCenter Server che gestisce il cluster ha/DRS può connettersi agli host ESXi in entrambi i siti e deve essere configurato utilizzando vCenter ha.

Fare riferimento a. "Come creare e configurare i cluster nel client vSphere" Per configurare vCenter ha.

Fare riferimento anche alla sezione "Procedure consigliate per VMware vSphere Metro Storage Cluster".

**Che cos'è vSphere Metro Storage Cluster?**

VSphere Metro Storage Cluster (vMSC) è una configurazione certificata che protegge le macchine virtuali (VM) e i container dai guasti. Ciò si ottiene utilizzando concetti di storage estesi insieme ai cluster di host ESXi, distribuiti in diversi domini di errore come rack, edifici, campus o persino città. Le tecnologie di storage Active Sync di NetApp MetroCluster e SnapMirror vengono utilizzate per fornire ai cluster host una protezione rispettivamente con RPO=0 o near RPO=0. La configurazione vMSC è progettata per garantire che i dati siano sempre disponibili, anche in caso di errore di un "sito" fisico o logico completo. Un dispositivo di storage che fa parte della configurazione vMSC deve essere certificato dopo aver superato un processo di certificazione vMSC di successo. Tutti i dispositivi di archiviazione supportati sono disponibili nella "Guida alla compatibilità dello storage VMware".

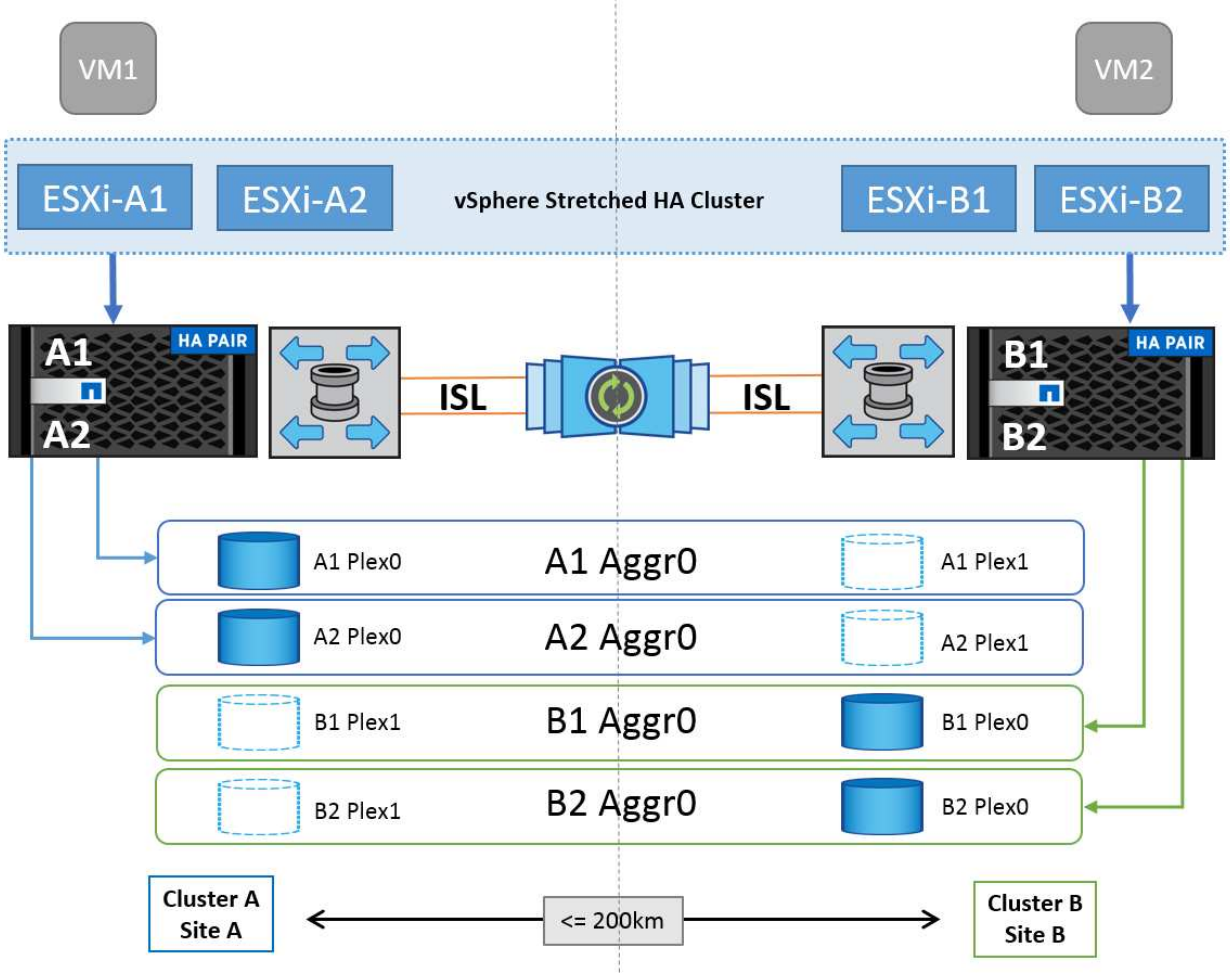
Per ulteriori informazioni sulle linee guida di progettazione per vSphere Metro Storage Cluster, consultare la seguente documentazione:

- "Supporto di VMware vSphere con NetApp MetroCluster"
- "Supporto di VMware vSphere con business continuity di NetApp SnapMirror" (Adesso noto come SnapMirror Active Sync)

A seconda delle considerazioni sulla latenza, NetApp MetroCluster può essere implementato in due diverse configurazioni da utilizzare con vSphere:

- Stretch MetroCluster
- Fabric MetroCluster

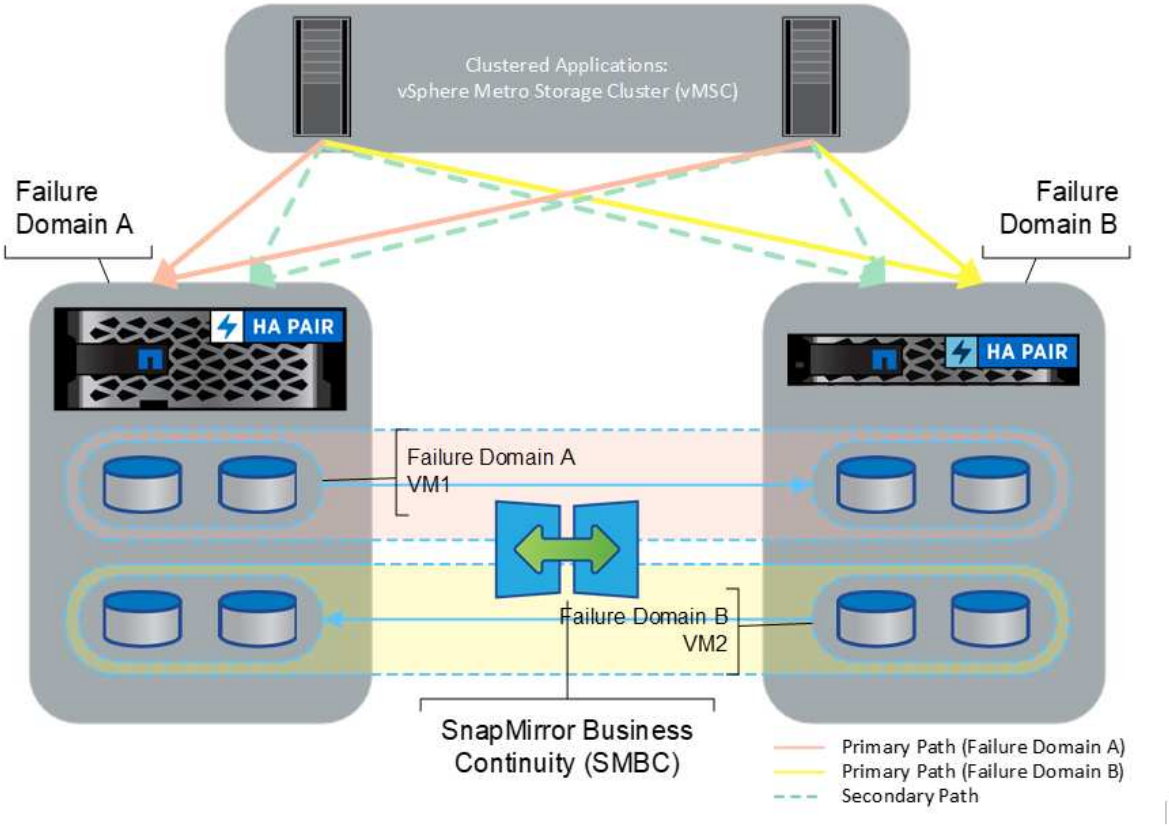
Di seguito viene illustrato uno schema topologico di alto livello di Stretch MetroCluster.




Fare riferimento a. "Documentazione MetroCluster" Per informazioni specifiche sulla progettazione e la distribuzione di MetroCluster.

SnapMirror Active Sync può anche essere implementato in due modi diversi.

- Asimmetrico
- Simmetrico (anteprima privata in ONTAP 9.14.1)




Fare riferimento a. "Documenti NetApp" Per informazioni specifiche sulla progettazione e la distribuzione per la sincronizzazione attiva di SnapMirror.

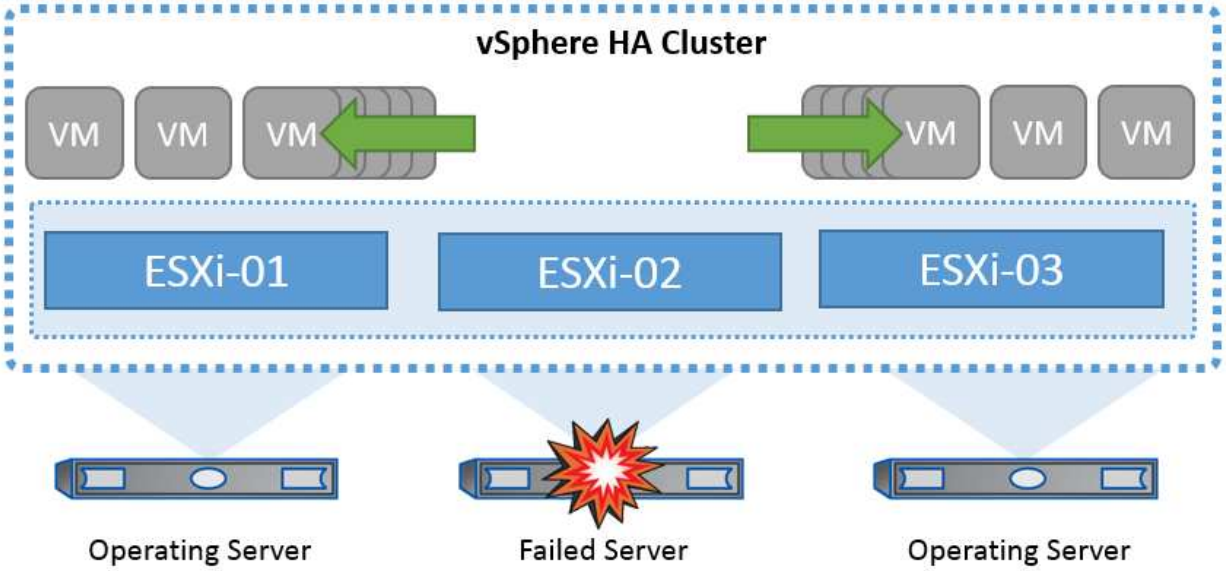
## Panoramica della soluzione VMware vSphere

VCenter Server Appliance (VCSA) è un potente sistema di gestione centralizzato e un singolo pannello di controllo per vSphere che consente agli amministratori di utilizzare in modo efficace i cluster ESXi. Agevola le funzioni chiave come provisioning delle macchine virtuali, funzionamento di vMotion, alta disponibilità (ha), Distributed Resource Scheduler (DRS), Tanzu Kubernetes Grid e altro ancora. Si tratta di un componente essenziale negli ambienti cloud VMware e deve essere progettato tenendo presente la disponibilità del servizio.

### Alta disponibilità vSphere

La tecnologia cluster di VMware raggruppa i server ESXi in pool di risorse condivise per le macchine virtuali e offre vSphere High Availability (ha). VSphere ha offre alta disponibilità e facile da utilizzare per le applicazioni eseguite su macchine virtuali. Quando la funzionalità ha è abilitata sul cluster, ogni server ESXi mantiene la comunicazione con altri host in modo che, se un host ESXi non risponde o si isola, il cluster di ha può negoziare il recovery delle macchine virtuali in esecuzione sull'host ESXi tra gli host sopravvissuti nel cluster. In caso di errore del sistema operativo guest, vSphere ha riavvia la macchina virtuale interessata sullo stesso server fisico. VSphere ha consente di ridurre i downtime pianificati, prevenire i downtime non pianificati e eseguire un rapido ripristino in caso di interruzioni.

Cluster vSphere ha in grado di ripristinare le VM dal server guasto.




È importante comprendere che VMware vSphere non conosce NetApp MetroCluster o SnapMirror Active Sync e vede tutti gli host ESXi nel cluster vSphere come host idonei per le operazioni del cluster ha in base alle configurazioni di affinità dei gruppi VM e host.

**Rilevamento errori host**

Non appena viene creato il cluster ha, tutti gli host nel cluster partecipano alle elezioni e uno degli host diventa un master. Ogni slave esegue heartbeat di rete al master, e il master a sua volta esegue heartbeat di rete su tutti gli host slave. L'host master di un cluster vSphere ha è responsabile del rilevamento del guasto degli host slave.

A seconda del tipo di errore rilevato, potrebbe essere necessario eseguire il failover delle macchine virtuali in esecuzione sugli host.

In un cluster vSphere ha, vengono rilevati tre tipi di errore dell'host:

- Errore - Un host smette di funzionare.
- Isolamento - Un host diventa isolato dalla rete.
- Partizione - Un host perde la connettività di rete con l'host master.

L'host master monitora gli host slave nel cluster. Questa comunicazione viene fatta attraverso lo scambio di heartbeat di rete ogni secondo. Quando l'host master smette di ricevere questi heartbeat da un host slave, controlla la liveness dell'host prima di dichiarare che l'host non è riuscito. Il controllo liveness che l'ospite principale effettua è di determinare se l'ospite secondario sta scambiando i heartbeat con uno dei datastore. Inoltre, l'host master verifica se l'host risponde ai ping ICMP inviati ai propri indirizzi IP di gestione per rilevare se è semplicemente isolato dal suo nodo master o completamente isolato dalla rete. Per farlo, eseguire il ping del gateway predefinito. È possibile specificare manualmente uno o più indirizzi di isolamento per migliorare l'affidabilità della convalida dell'isolamento.

*Best practice*

NetApp consiglia di specificare un minimo di due indirizzi di isolamento aggiuntivi e che ciascuno di questi indirizzi sia locale al sito. Ciò migliorerà l'affidabilità della convalida dell'isolamento.

### Risposta di isolamento dell'host

Risposta di isolamento è un'impostazione in vSphere ha che determina l'azione attivata sulle macchine virtuali quando un host in un cluster vSphere ha perde le connessioni di rete di gestione ma continua a essere eseguito. Sono disponibili tre opzioni per questa impostazione: "Disabilitato", "Arresta e riavvia le macchine virtuali" e "Spegni e riavvia le macchine virtuali".

Lo "spegnimento" è migliore dello "spegnimento", che non svuota le modifiche più recenti al disco o esegue il commit delle transazioni. Se le macchine virtuali non si sono arrestate entro 300 secondi, vengono spente. Per modificare il tempo di attesa, utilizzare l'opzione avanzata das.isolationshutdowntimeout.

Prima che ha avvii la risposta di isolamento, verifica prima se l'agente master ha vSphere è proprietario del datastore che contiene i file di configurazione della VM. In caso contrario, l'host non attiverà la risposta di isolamento, poiché non vi è alcun master per riavviare le VM. L'host controllerà periodicamente lo stato del datastore per determinare se viene richiesto da un agente vSphere ha che detiene il ruolo master.

*Best practice*

NetApp consiglia di impostare la risposta di isolamento dell'host su Disabilitato.

Una condizione split-brain può verificarsi se un host viene isolato o partizionato dall'host master vSphere ha e il master non è in grado di comunicare tramite datastore heartbeat o tramite ping. Il master dichiara l'host isolato inattivo e riavvia le macchine virtuali su altri host nel cluster. Esiste ora una condizione split-brain perché esistono due istanze della macchina virtuale in esecuzione, una sola delle quali è in grado di leggere o scrivere i dischi virtuali. Le condizioni split-brain possono ora essere evitate configurando VMCP (VM Component Protection).

### Protezione dei componenti VM (VMCP)

Uno dei miglioramenti delle funzionalità di vSphere 6, relativi all'ha, è VMCP. VMCP fornisce una protezione avanzata da APD (All Path Down) e PDL (Permanent Device Loss) per lo storage a blocchi (FC, iSCSI, FCoE) e a file (NFS).

#### Perdita permanente del dispositivo (PDL)

PDL è una condizione che si verifica quando un dispositivo di memorizzazione si guasta in modo permanente o viene rimosso amministrativamente e non deve essere restituito. L'array di storage NetApp invia un codice di rilevamento SCSI a ESXi dichiarando che il dispositivo è perso in modo permanente. Nella sezione Condizioni di guasto e Risposta VM di vSphere ha, è possibile configurare la risposta che deve essere dopo il rilevamento di una condizione PDL.

*Best practice*

NetApp consiglia di impostare "Risposta per datastore con PDL" su "**Spegni e riavvia VM**". Quando viene rilevata questa condizione, una VM viene riavviata istantaneamente su un host integro all'interno del cluster vSphere ha.

#### Tutti i percorsi verso il basso (APD)

APD è una condizione che si verifica quando un dispositivo di archiviazione diventa inaccessibile all'host e non sono disponibili percorsi all'array. ESXi considera questo un problema temporaneo con il dispositivo e si aspetta che diventi nuovamente disponibile.

Quando viene rilevata una condizione APD, viene avviato un timer. Dopo 140 secondi, la condizione APD viene dichiarata ufficialmente e il dispositivo viene contrassegnato come timeout APD. Una volta trascorsi i 140

secondi, ha inizia il conteggio dei minuti specificati nell'APD Delay for VM failover. Una volta trascorso il tempo specificato, ha riavvia le macchine virtuali interessate. È possibile configurare VMCP in modo che risponda in modo diverso, se lo si desidera (Disattivato, Eventi problema o Spegni e riavvia le macchine virtuali).

*Best practice*

NetApp consiglia di configurare "Risposta per datastore con APD" su "**Spegni e riavvia le VM (conservative)**".

Conservative si riferisce alla probabilità che ha sia in grado di riavviare le VM. Quando è impostata su Conservative, ha riavvia la VM interessata dall'APD solo se sa che un altro host può riavviarla. In caso di problemi aggressivi, ha tenterà di riavviare la macchina virtuale anche se non conosce lo stato degli altri host. Ciò può comportare il mancato riavvio delle VM se non vi è alcun host con accesso al datastore su cui si trova.

Se lo stato APD viene risolto e l'accesso allo storage viene ripristinato prima del termine del timeout, l'ha non riavvia inutilmente la macchina virtuale a meno che non sia stata configurata esplicitamente. Se si desidera una risposta anche quando l'ambiente è stato ripristinato dalla condizione APD, è necessario configurare la risposta per il ripristino APD dopo il timeout APD in modo da ripristinare le VM.

*Best practice*

NetApp consiglia di configurare la risposta per il ripristino APD dopo il timeout APD su Disabilitato.

**Implementazione VMware DRS per NetApp MetroCluster**

VMware DRS è una funzionalità che aggrega le risorse host in un cluster e viene utilizzata principalmente per il bilanciamento del carico all'interno di un cluster in un'infrastruttura virtuale. VMware DRS calcola principalmente le risorse di CPU e memoria per eseguire il bilanciamento del carico in un cluster. Poiché vSphere non è consapevole del clustering allungato, considera tutti gli host in entrambi i siti durante il bilanciamento del carico. Per evitare il traffico tra siti, NetApp consiglia di configurare le regole di affinità DRS per gestire una separazione logica delle VM. In questo modo si garantisce che, a meno che non si verifichi un errore completo del sito, ha e DRS utilizzino solo host locali.

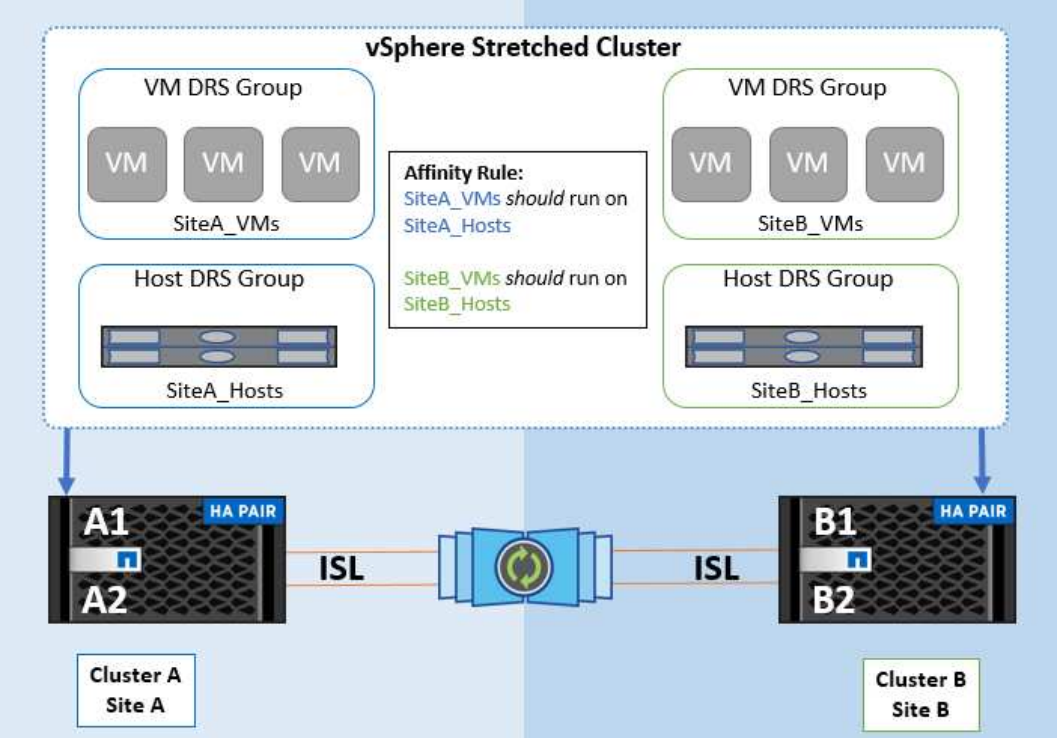
Se si crea una regola di affinità DRS per il cluster, è possibile specificare in che modo vSphere applica tale regola durante il failover di una macchina virtuale.

Esistono due tipi di regole che è possibile specificare il comportamento di failover di vSphere ha:

- Le regole di anti-affinità delle macchine virtuali costringono le macchine virtuali specificate a rimanere separate durante le azioni di failover.
- Le regole di affinità degli host VM collocano macchine virtuali specifiche su un host specifico o su un membro di un gruppo definito di host durante le azioni di failover.

Utilizzando le regole di affinità degli host delle macchine virtuali in VMware DRS, si può avere una separazione logica tra il sito A e il sito B in modo che la macchina virtuale venga eseguita sull'host nello stesso sito dell'array configurato come controller di lettura/scrittura principale per un determinato datastore. Inoltre, le regole di affinità degli host delle macchine virtuali consentono alle macchine virtuali di rimanere locali rispetto allo storage, il che a sua volta determina la connessione della macchina virtuale in caso di errori di rete tra i siti.

Di seguito è riportato un esempio di gruppi di host VM e regole di affinità.




*Best practice*

NetApp consiglia di implementare le regole "should" invece di quelle "must", in quanto vengono violate da vSphere ha in caso di errore. L'utilizzo di regole "must" può potenzialmente causare interruzioni del servizio.

La disponibilità dei servizi dovrebbe sempre prevalere sulle prestazioni. Nello scenario in cui si verifica un guasto di un data center completo, le regole "must" devono scegliere gli host dal gruppo di affinità degli host VM e, quando il data center non è disponibile, le macchine virtuali non verranno riavviate.

### Implementazione di VMware Storage DRS con NetApp MetroCluster

La funzione VMware Storage DRS consente l'aggregazione di datastore in una singola unità e bilancia i dischi della macchina virtuale quando vengono superate le soglie di controllo i/o di storage.

Il controllo i/o dello storage è abilitato per impostazione predefinita sui cluster DRS abilitati per Storage DRS. Il controllo i/o dello storage consente a un amministratore di controllare la quantità di i/o dello storage allocata alle macchine virtuali nei periodi di congestione dell'i/o e di conseguenza le macchine virtuali più importanti possono preferire le macchine virtuali meno importanti per l'allocazione delle risorse i/O.

Storage DRS utilizza Storage vMotion per migrare le macchine virtuali in datastore diversi all'interno di un cluster di datastore. In un ambiente NetApp MetroCluster, la migrazione di una macchina virtuale deve essere controllata all'interno dei datastore di quel sito. Ad esempio, la macchina virtuale A, in esecuzione su un host nel sito A, dovrebbe idealmente migrare all'interno dei datastore della SVM nel sito A. In caso contrario, la macchina virtuale continuerà a funzionare ma con prestazioni ridotte, poiché la lettura/scrittura del disco virtuale avverrà dal sito B attraverso collegamenti tra siti.

*Best practice*

NetApp consiglia di creare cluster di datastore in relazione all'affinità con i siti storage. In altre parole, i datastore con affinità con i siti per il sito A non devono essere mescolati con i cluster di datastore con datastore con affinità con i siti per il sito B.

Ogni volta che viene eseguito il provisioning o la migrazione di una macchina virtuale mediante Storage vMotion, NetApp consiglia di aggiornare manualmente tutte le regole VMware DRS specifiche di tali macchine virtuali. In questo modo, si verificherà l'affinità della macchina virtuale a livello di sito per host e datastore, riducendo così l'overhead di rete e storage.

## Linee guida per la progettazione e l'implementazione di vMSC

Questo documento delinea le linee guida di progettazione e implementazione per vMSC con i sistemi di storage ONTAP.

### Configurazione dello storage NetApp

Le istruzioni per l'installazione di NetApp MetroCluster (definite configurazione MCC) sono disponibili all'indirizzo "Documentazione MetroCluster". Le istruzioni per la sincronizzazione attiva di SnapMirror sono disponibili all'indirizzo "Panoramica di SnapMirror Business Continuity".

Una volta configurato MetroCluster, gestirlo è come gestire un ambiente ONTAP tradizionale. Puoi configurare Storage Virtual Machine (SVM) utilizzando vari strumenti come l'interfaccia a riga di comando (CLI), System Manager o Ansible. Una volta configurate le SVM, occorre creare nel cluster interfacce logiche (LIF), volumi e LUN (Logical Unit Number) da utilizzare per le normali operazioni. Questi oggetti verranno replicati automaticamente sull'altro cluster utilizzando la rete di peering del cluster.

Se non utilizzi MetroCluster, puoi usare SnapMirror Active Sync che offre protezione granulare dei datastore e accesso Active-Active su diversi cluster ONTAP in diversi domini di errore. SnapMirror Active Sync utilizza gruppi di coerenza per garantire la coerenza dell'ordine di scrittura in uno o più datastore. Puoi creare più gruppi di coerenza in base ai requisiti di applicazioni e datastore. I gruppi di coerenza sono particolarmente utili per le applicazioni che richiedono la sincronizzazione dei dati tra datastore multipli. La sincronizzazione attiva di SnapMirror supporta inoltre RDM (Raw Device Mapping) e storage connesso al guest con initiator iSCSI in-guest. Per ulteriori informazioni sui gruppi di coerenza, visitare il sito Web all'indirizzo "Panoramica dei gruppi di coerenza".

Esiste una certa differenza nella gestione di una configurazione vMSC con sincronizzazione attiva SnapMirror rispetto a una MetroCluster. In primo luogo, si tratta DI una configurazione solo SAN, ma non è possibile proteggere datastore NFS con la sincronizzazione attiva di SnapMirror. In secondo luogo, è necessario mappare entrambe le copie delle LUN agli host ESXi per accedere ai datastore replicati in entrambi i domini di errore.

### VMware vSphere ha

#### Creare un cluster vSphere ha

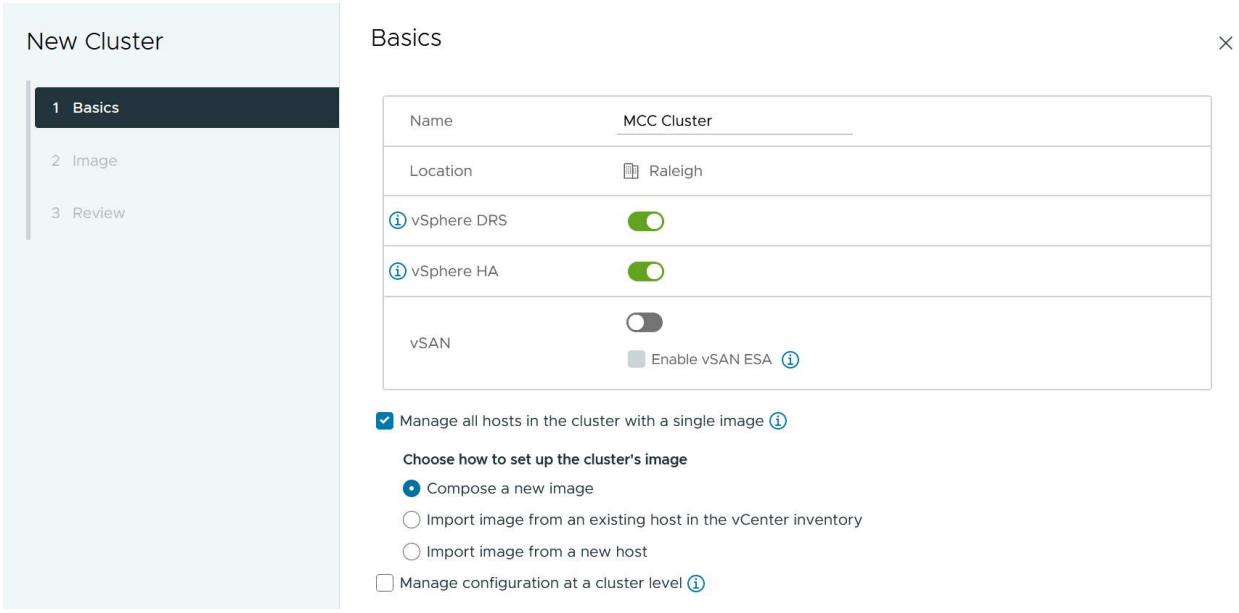
La creazione di un cluster vSphere ha è un processo in più fasi documentato all'indirizzo "Come creare e configurare i cluster nel client vSphere su docs.vmware.com". In poche parole, devi prima creare un cluster vuoto, quindi, utilizzando vCenter, devi aggiungere host e specificare l'ha vSphere del cluster e le altre impostazioni.

**Nota:** nulla di quanto contenuto nel presente documento sostituisce "Procedure consigliate per VMware vSphere Metro Storage Cluster"

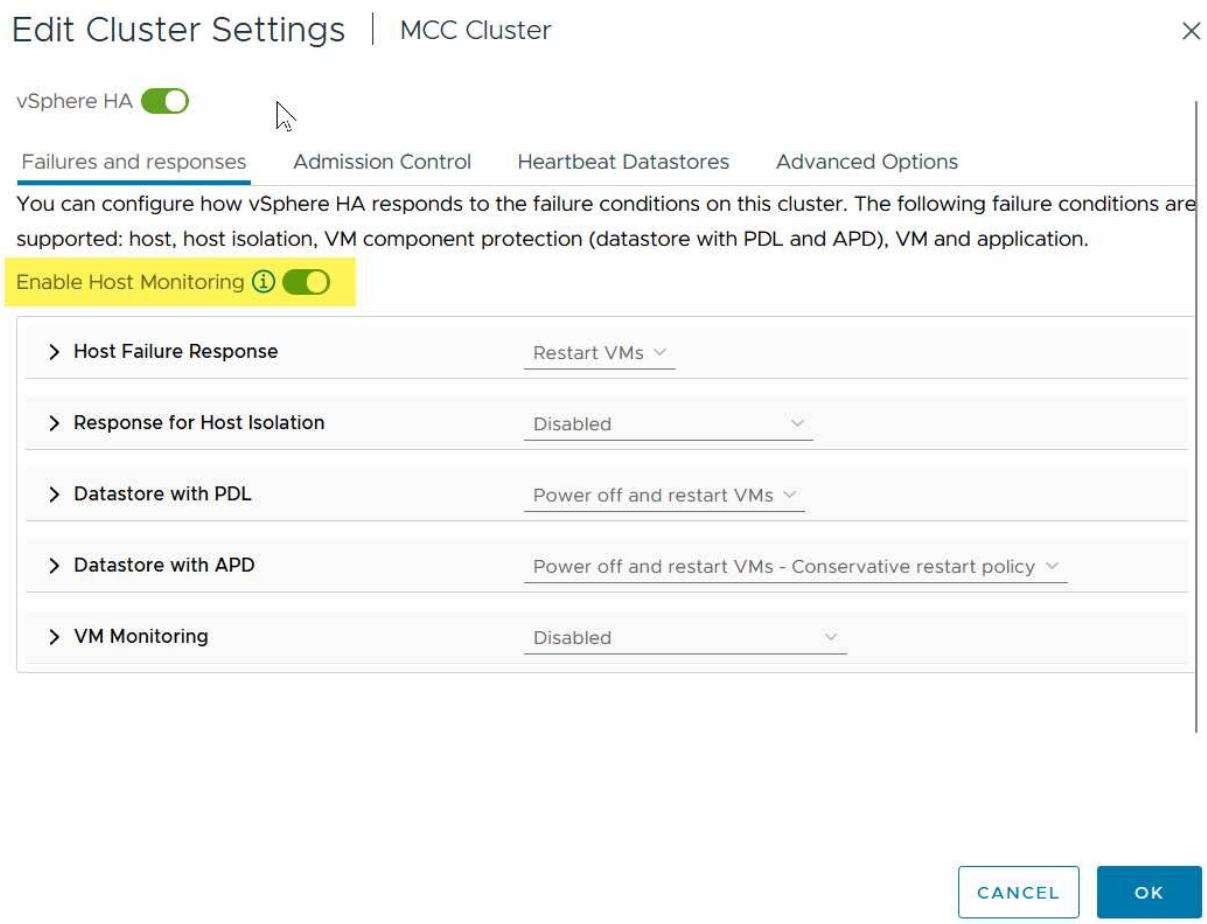
Per configurare un cluster ha, completare i seguenti passaggi:

1. Connettersi all'interfaccia utente di vCenter.
2. In host e cluster, individuare il data center in cui si desidera creare il cluster ha.

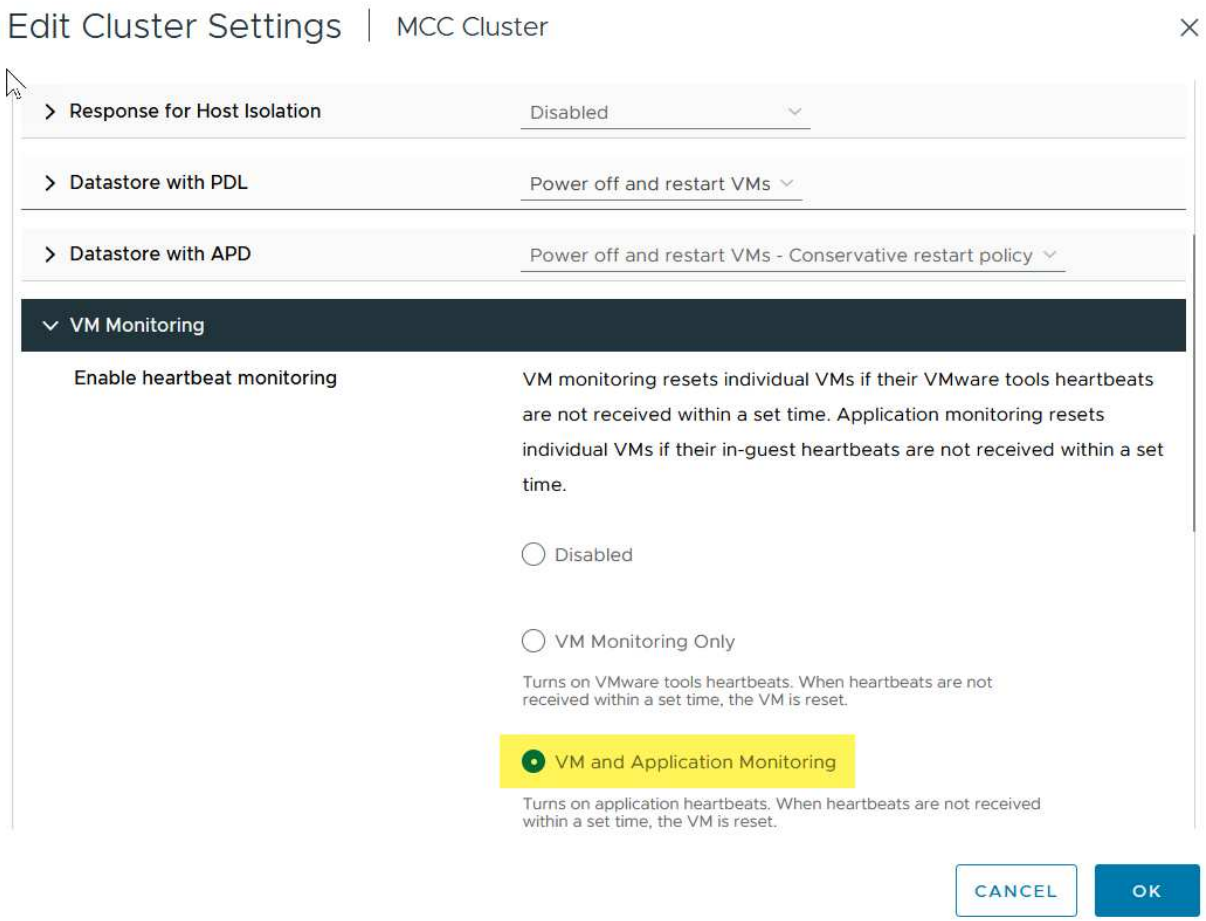
3. Fare clic con il pulsante destro del mouse sull'oggetto del data center e selezionare nuovo cluster. In base alle nozioni di base, assicurarsi di aver abilitato vSphere DRS e vSphere ha. Completare la procedura guidata.



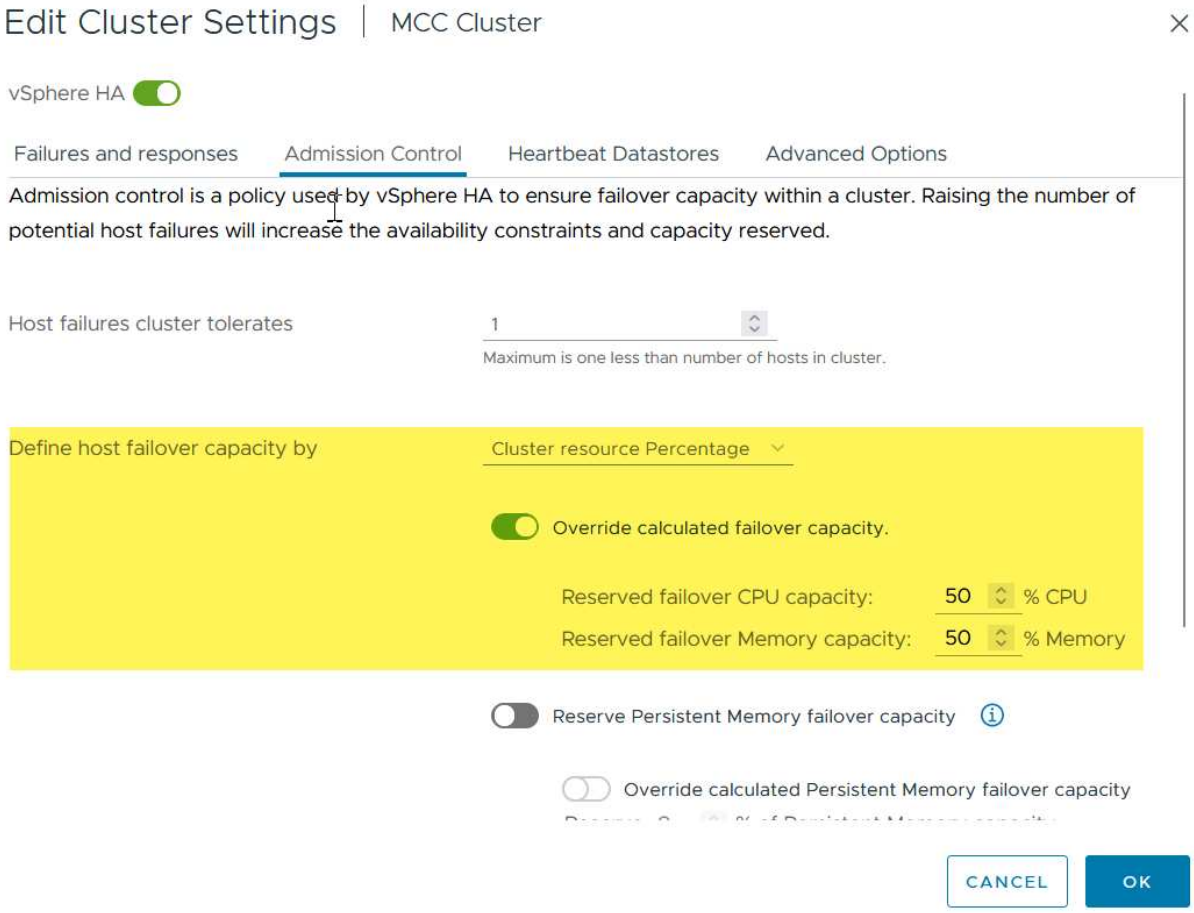

1. Selezionare il cluster e accedere alla scheda di configurazione. Selezionare vSphere ha e fare clic su Modifica.
2. In monitoraggio host, selezionare l'opzione attiva monitoraggio host.



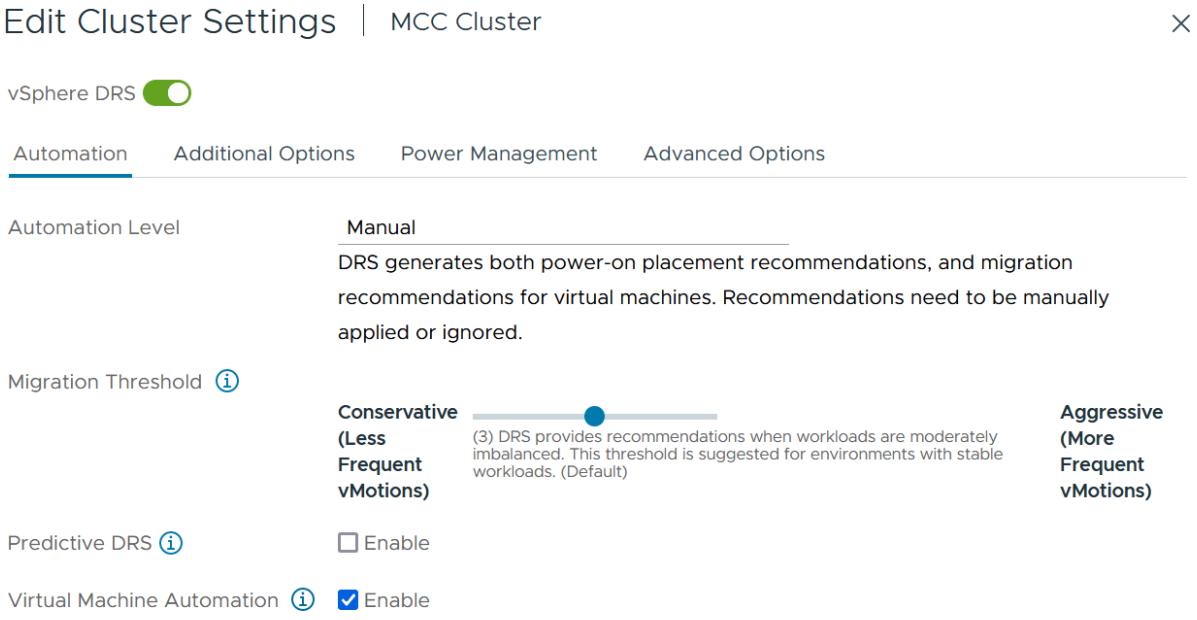
1. Nella scheda guasti e risposte, in monitoraggio VM, selezionare l'opzione solo monitoraggio VM o monitoraggio VM e applicazione.




1. In controllo ammissione, impostare l'opzione di controllo ammissione ha su Cluster Resource Reserve; utilizzare 50% CPU/MEM.




1. Fare clic su "OK".
2. Selezionare DRS e fare clic su MODIFICA.
3. Impostare il livello di automazione su manuale, a meno che non sia richiesto dalle applicazioni.



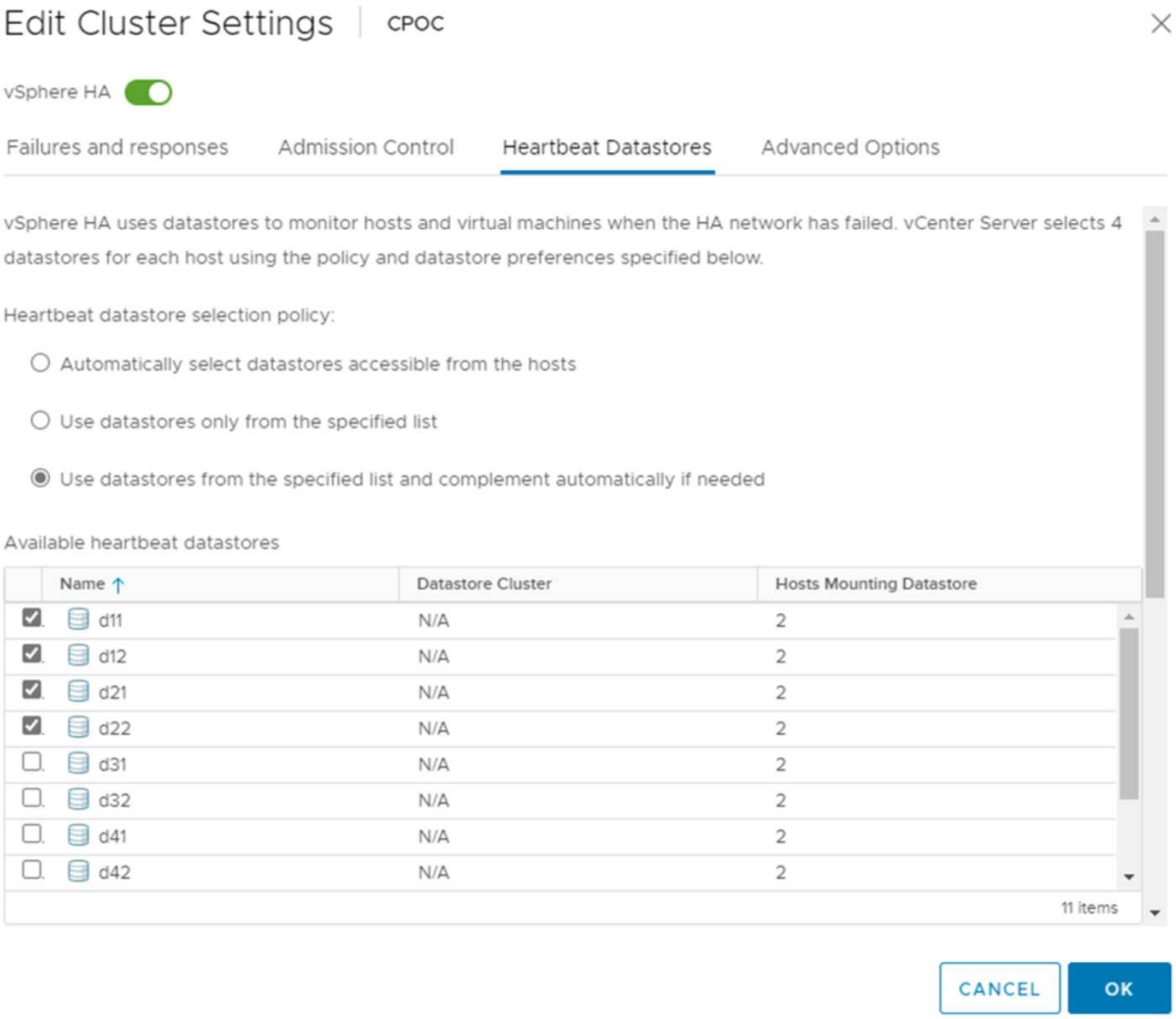
1. Abilitare la protezione dei componenti VM, fare riferimento a. "docs.vmware.com".
2. Le seguenti impostazioni aggiuntive di vSphere ha sono consigliate per vMSC con MCC:

| Guasto | Risposta |
|---|---|
| Errore host | Riavviare le VM |
| Isolamento degli host | Disattivato |
| Datastore con perdita permanente di dispositivi (PDL) | Spegnere e riavviare le macchine virtuali |
| Datastore con tutti i percorsi verso il basso (APD) | Spegnere e riavviare le macchine virtuali |
| L'ospite non batte il cuore | Ripristinare le VM |
| Policy di riavvio della VM | Determinato dall'importanza della VM |
| Risposta per l'isolamento dell'host | Arrestare e riavviare le VM |
| Risposta per il datastore con PDL | Spegnere e riavviare le macchine virtuali |
| Risposta per datastore con APD | Spegnere e riavviare le macchine virtuali (conservative) |
| Ritardo del failover delle macchine virtuali per APD | 3 minuti |
| Risposta per il ripristino APD con timeout APD | Disattivato |
| Sensibilità di monitoraggio VM | Preimpostazione alta |

#### Configurare gli archivi dati per Heartbeating

VSphere ha utilizza i datastore per monitorare gli host e le macchine virtuali in caso di guasto alla rete di gestione. È possibile configurare in che modo vCenter seleziona i datastore heartbeat. Per configurare gli archivi dati per il heartbeat, completare i seguenti passaggi:

1. Nella sezione Heartbeating del datastore, selezionare Usa archivi dati dall'elenco specificato e completare automaticamente se necessario.
2. Seleziona i datastore che desideri utilizzare vCenter da entrambi i siti e premi OK.

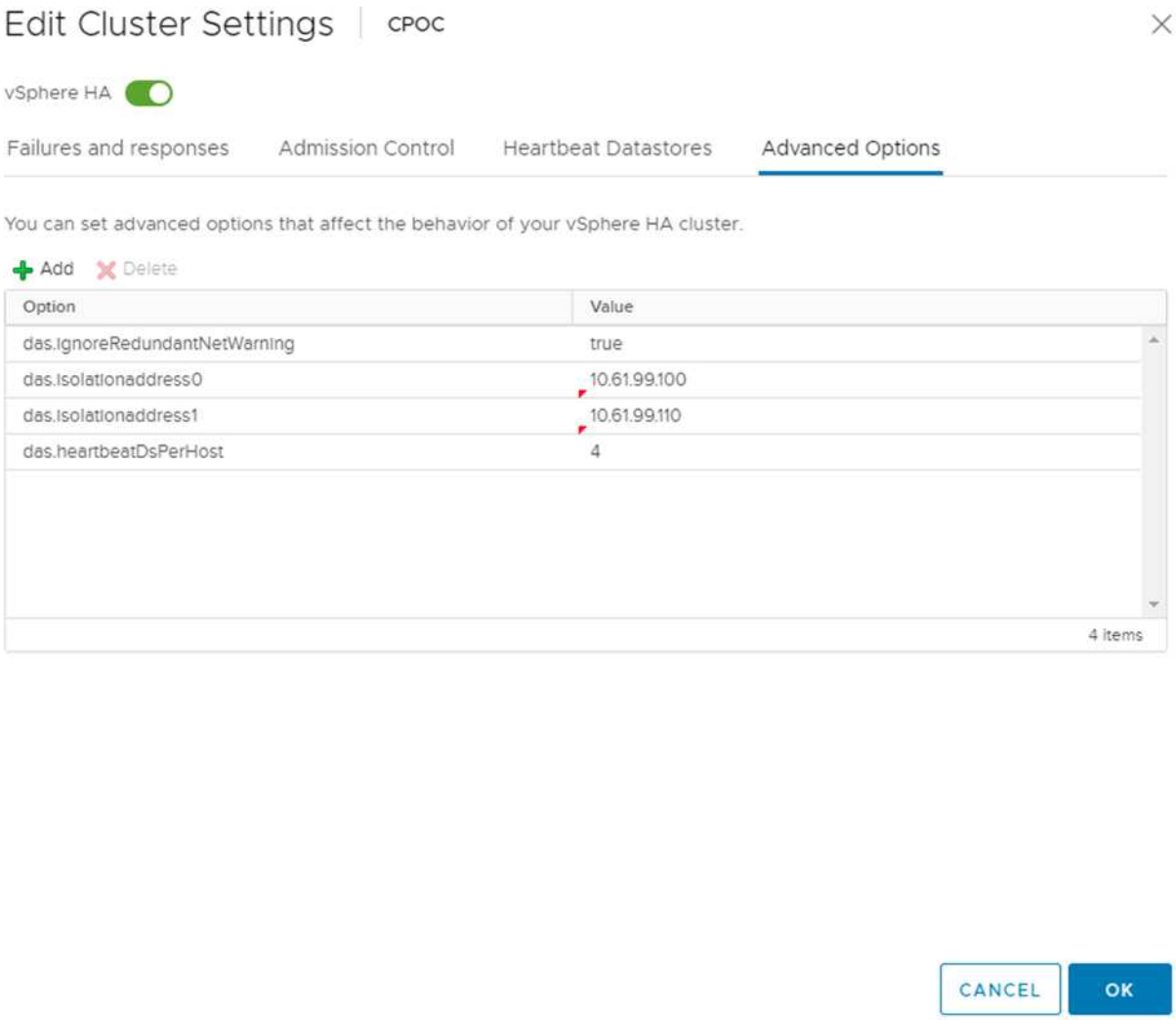



**Configurare le opzioni avanzate**

### Rilevamento errori host

Gli eventi di isolamento si verificano quando gli host all'interno di un cluster ha perdono la connettività alla rete o ad altri host nel cluster. Per impostazione predefinita, vSphere ha utilizzerà il gateway predefinito per la propria rete di gestione come indirizzo di isolamento predefinito. Tuttavia, è possibile specificare indirizzi di isolamento aggiuntivi per l'host al ping per determinare se deve essere attivata una risposta di isolamento. Aggiungere due IP di isolamento in grado di eseguire il ping, uno per sito. Non utilizzare l'indirizzo IP del gateway. L'impostazione avanzata vSphere ha utilizzata è das.isolationaddress. A tale scopo, è possibile utilizzare gli indirizzi IP ONTAP o Mediator.

Fare riferimento a. "core.vmware.com" per ulteriori informazioni.




L'aggiunta di un'impostazione avanzata denominata das.heartbeatDsPerHost può aumentare il numero di datastore heartbeat. Utilizzare quattro datastore heartbeat (HB DSS), due per sito. Utilizzare l'opzione "Select from List but complent" (Seleziona da elenco ma complimento). Questo è necessario perché se un sito non funziona, è necessario ancora due HB DSS. Tuttavia, questi elementi non devono essere protetti con la sincronizzazione attiva di MCC o SnapMirror.

Fare riferimento a. "core.vmware.com" per ulteriori informazioni.

Affinità con VMware DRS per NetApp MetroCluster

In questa sezione vengono creati gruppi DRS per VM e host per ciascun sito/cluster nell'ambiente MetroCluster. Quindi configuriamo le regole VM\host per allineare l'affinità dell'host VM con le risorse di storage locali. Ad esempio, il sito A fa parte del gruppo VM sitea_VM e gli host del sito A appartengono al gruppo host sitea_hosts. Successivamente, in VM\host Rules, si afferma che sitea_vm deve essere eseguito sugli host in sitea_hosts.

*Best practice*

- NetApp consiglia vivamente la specifica **deve essere eseguita sugli host nel gruppo** piuttosto che sulla specifica **deve essere eseguita sugli host nel gruppo**. In caso di guasto dell'host del sito A, è necessario riavviare le macchine virtuali del sito A sugli host del sito B attraverso vSphere ha, ma quest'ultima specifica non consente all'ha di riavviare le macchine virtuali sul sito B perché è una regola rigida. La

specifica precedente è una regola debole e viene violata in caso di ha, abilitando in tal modo la disponibilità anziché le prestazioni.

**Nota:** è possibile creare un allarme basato su eventi che viene attivato quando una macchina virtuale viola una regola di affinità VM-host. Nel client vSphere, aggiungere un nuovo allarme per la macchina virtuale e selezionare "VM viola la regola di affinità VM-host" come trigger dell'evento. Per ulteriori informazioni sulla creazione e la modifica degli allarmi, fare riferimento a. "Monitoraggio e performance di vSphere" documentazione.

#### Creare gruppi host DRS

Per creare gruppi di host DRS specifici per il sito A e il sito B, attenersi alla seguente procedura:

1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare Impostazioni.
2. Fare clic su VM\host Groups.
3. Fare clic su Aggiungi.
4. Digitare il nome del gruppo (ad esempio, sitea_hosts).
5. Dal menu tipo, selezionare Gruppo host.
6. Fare clic su Aggiungi e selezionare gli host desiderati dal sito A, quindi fare clic su OK.
7. Ripetere questi passaggi per aggiungere un altro gruppo di host per il sito B.
8. Fare clic su OK.

#### Creare gruppi DRS VM

Per creare gruppi di macchine virtuali DRS specifici per il sito A e il sito B, attenersi alla seguente procedura:

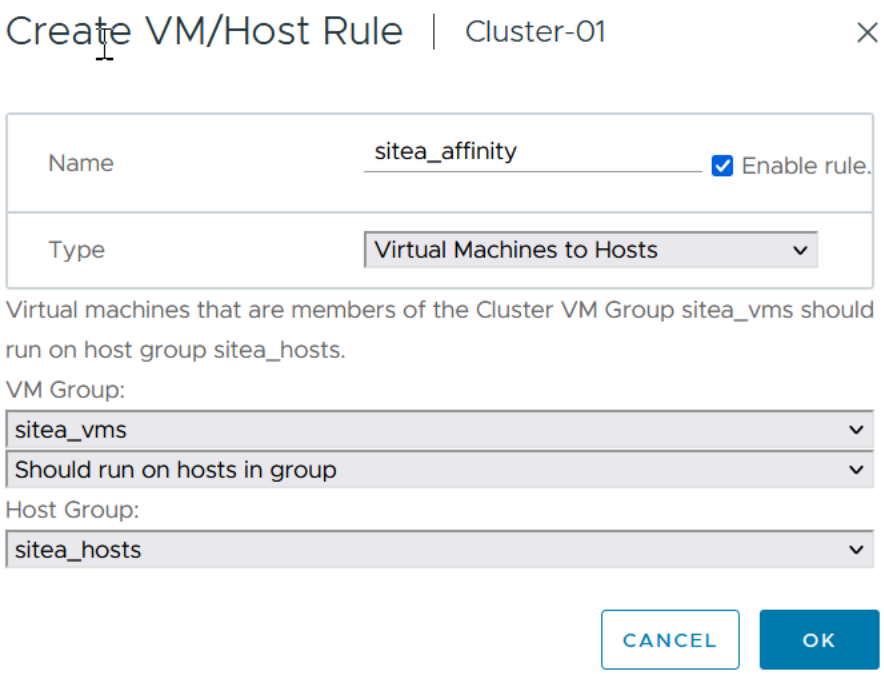
1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare Impostazioni.
2. Fare clic su VM\host Groups.
3. Fare clic su Aggiungi.
4. Digitare il nome del gruppo (ad esempio, sitea_vm).
5. Dal menu tipo, selezionare Gruppo VM.
6. Fare clic su Add (Aggiungi) e selezionare le VM desiderate dal sito A, quindi fare clic su OK.
7. Ripetere questi passaggi per aggiungere un altro gruppo di host per il sito B.
8. Fare clic su OK.

#### Crea regole host VM

Per creare regole di affinità DRS specifiche per il sito A e il sito B, completare i seguenti passaggi:

1. Nel client web vSphere, fare clic con il pulsante destro del mouse sul cluster nell'inventario e selezionare Impostazioni.
2. Fare clic su VM\host Rules.
3. Fare clic su Aggiungi.
4. Digitare il nome della regola (ad esempio, sitea_Affinity).

5. Verificare che l'opzione Enable Rule (attiva regola) sia selezionata.
6. Dal menu Type (tipo), selezionare Virtual Machines to hosts (macchine virtuali a host).
7. Selezionare il gruppo VM (ad esempio, sitea_vm).
8. Selezionare il gruppo host (ad esempio, sitea_hosts).
9. Ripetere questi passaggi per aggiungere un'altra VM\regola host per il sito B.
10. Fare clic su OK.




## VMware vSphere Storage DRS per NetApp MetroCluster

### Creare cluster di datastore

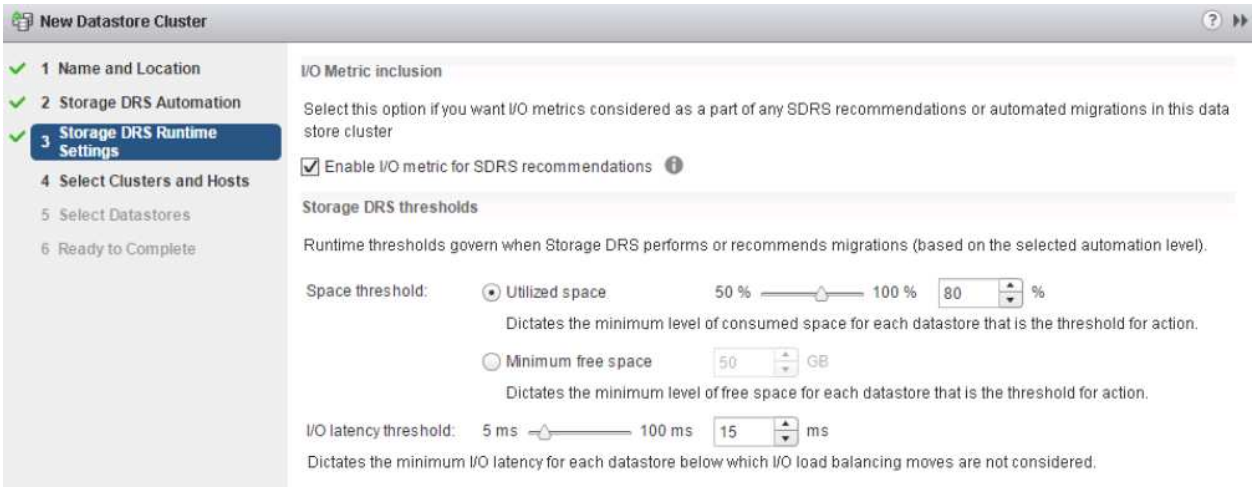
Per configurare un cluster di datastore per ciascun sito, attenersi alla seguente procedura:

1. Utilizzando il client web vSphere, individuare il data center in cui risiede il cluster ha in Storage.
2. Fare clic con il pulsante destro del mouse sull'oggetto del data center e selezionare Storage > New Datastore Cluster.
3. Selezionare l'opzione Turn ON Storage DRS (ATTIVA DRS archiviazione) e fare clic su Next (Avanti).
4. Impostare tutte le opzioni su Nessuna automazione (modalità manuale) e fare clic su Avanti.

*Best practice*

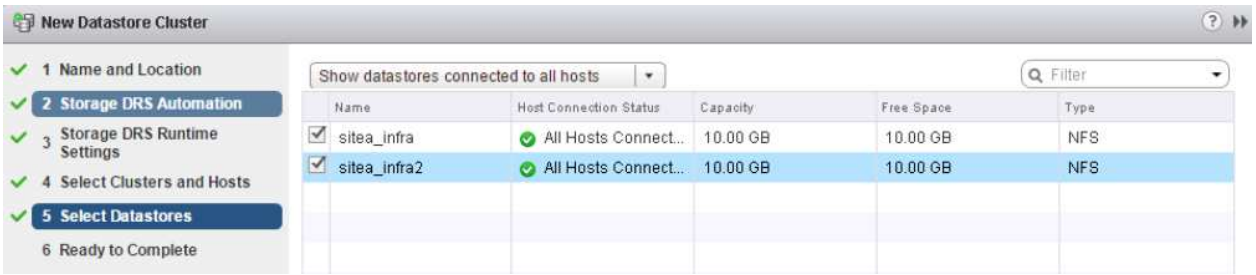
- NetApp consiglia di configurare i DRS dello storage in modalità manuale, in modo che l'amministratore possa decidere e controllare quando è necessario eseguire le migrazioni.


1. Verificare che la casella di controllo Enable i/o Metric for SDRS Recommendations (Abilita metriche i/o per raccomandazioni SDRS) sia selezionata; le impostazioni metriche possono essere lasciate con i valori predefiniti.




1. Selezionare il cluster ha e fare clic su Next.


1. Selezionare gli archivi dati appartenenti al sito A e fare clic su Avanti.




1. Rivedere le opzioni e fare clic su fine.
2. Ripetere questa procedura per creare il cluster di datastore del sito B e verificare che siano selezionati solo i datastore del sito B.

#### Disponibilità di vCenter Server

Le appliance vCenter Server (VCSA) devono essere protette con vCenter ha. VCenter ha ti consente di implementare due VCSA in una coppia ha Active-passive. Uno in ogni dominio di errore. Puoi leggere ulteriori informazioni su vCenter ha all'indirizzo "docs.vmware.com".

## Resilienza per eventi pianificati e non pianificati

NetApp MetroCluster e SnapMirror Active Sync sono potenti strumenti che migliorano l'alta disponibilità e le operazioni senza interruzioni dell'hardware NetApp e del software ONTAP®.

Questi strumenti garantiscono una protezione a livello di sito per l'intero ambiente di storage, garantendo che i tuoi dati siano sempre disponibili. Che si stiano utilizzando server standalone, cluster di server ad alta disponibilità, container Docker o server virtualizzati, la tecnologia NetApp permette di conservare perfettamente la disponibilità dello storage in caso di black-out totale causato da black-out, raffreddamento o connettività di rete, arresto dello storage array o errori operativi.

La sincronizzazione attiva di MetroCluster e SnapMirror offre tre metodi di base per la continuità dei dati in caso di eventi pianificati o non pianificati:

- Componenti ridondanti per la protezione contro i guasti a un singolo componente
- Takeover locale di ha in caso di eventi che colpiscono un singolo controller
- Protezione completa del sito: Rapida ripresa del servizio mediante il trasferimento dello storage e dell'accesso client dal cluster di origine al cluster di destinazione

Ciò significa che le operazioni continuano senza problemi in caso di guasto a un singolo componente e vengono ripristinate automaticamente al funzionamento ridondante una volta sostituito il componente guasto.

Tutti i cluster ONTAP, ad eccezione dei cluster a nodo singolo (in genere versioni software-defined, come ad esempio ONTAP Select), offrono funzionalità di ha integrate chiamate takeover e giveback. Ciascun controller del cluster è accoppiato con un altro controller in modo da formare una coppia ha. Queste coppie garantiscono che ogni nodo sia connesso localmente allo storage.

Il takeover è un processo automatizzato in cui un nodo assume il controllo dello storage dell'altro per la gestione dei servizi dati. Giveback è il processo inverso che ripristina il normale funzionamento. Il takeover può essere pianificato, ad esempio durante la manutenzione hardware o gli upgrade della ONTAP, o non pianificato, derivante da un nodo di panico o da un guasto dell'hardware.

Durante un takeover, le interfacce logiche NAS (Network Attached Storage) nelle configurazioni MetroCluster eseguono automaticamente il failover. Tuttavia, le LIF (SAN) di Storage Area Network non subiscono failover e continueranno a utilizzare il percorso diretto dei LUN (Logical Unit Number).

Per ulteriori informazioni sul takeover e lo sconto ha, consulta la "Panoramica sulla gestione delle coppie HA". È importante notare che questa funzionalità non è specifica per MetroCluster o SnapMirror Active Sync.

Lo switchover del sito con MetroCluster viene eseguito quando un sito è offline o come attività pianificata per la manutenzione di un intero sito. Il sito rimanente presuppone la proprietà delle risorse storage (dischi e aggregati) del cluster offline e le SVM del sito guasto vengono messe online e riavviate nel sito di disaster recovery, preservando la loro identità completa per l'accesso client e host.

Con la sincronizzazione attiva di SnapMirror, poiché entrambe le copie vengono utilizzate contemporaneamente in modo attivo, gli host esistenti continueranno a funzionare. Il NetApp Mediator è necessario per garantire che il failover del sito avvenga correttamente.

## Scenari di errore per vMSC con MCC

Nelle sezioni seguenti vengono illustrati i risultati attesi da vari scenari di guasto con i sistemi vMSC e NetApp MetroCluster.

### Errore singolo percorso di storage

In questo scenario, se componenti come la porta HBA, la porta di rete, la porta dello switch dati front-end o un cavo FC o Ethernet si guastano, quel particolare percorso al dispositivo di storage viene contrassegnato come inattivo dall'host ESXi. Se vengono configurati diversi percorsi per il dispositivo storage fornendo resilienza alla porta HBA/rete/switch, ESXi esegue uno switchover del percorso. Durante questo periodo, le macchine virtuali rimangono in esecuzione senza alcun impatto, perché la disponibilità dello storage viene garantita attraverso l'offerta di più percorsi al dispositivo di storage.

**Nota:** in questo scenario non vi è alcun cambiamento nel comportamento di MetroCluster, e tutti i datastore continuano ad essere intatti dai rispettivi siti.

*Best practice*

Negli ambienti in cui vengono utilizzati volumi NFS/iSCSI, NetApp consiglia di avere almeno due uplink di rete configurati per la porta vmkernel NFS nel vSwitch standard e lo stesso nel gruppo di porte in cui è mappata l'interfaccia vmkernel NFS per il vSwitch distribuito. Il raggruppamento NIC può essere configurato in modalità Active-Active o Active-standby.

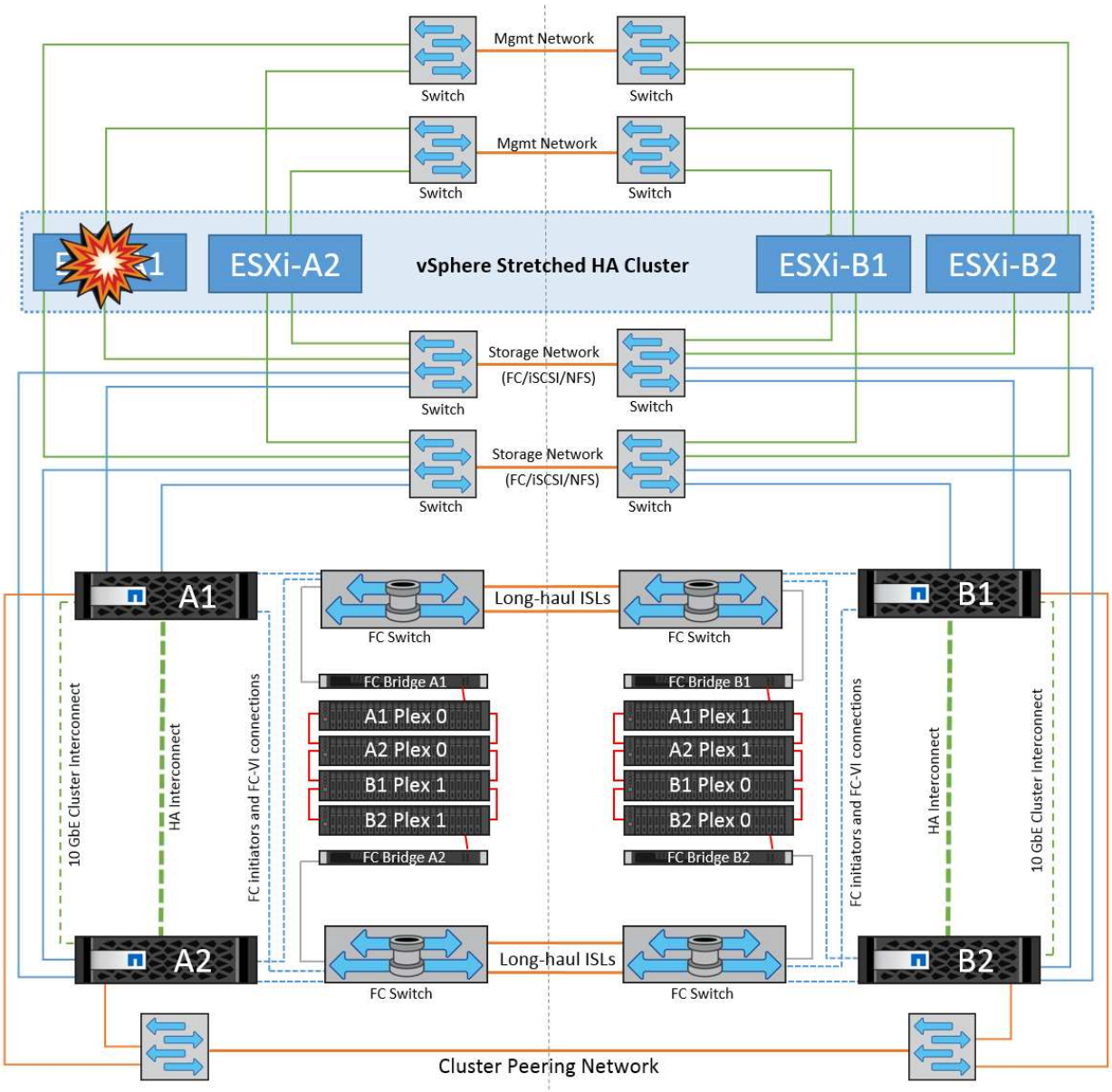
Inoltre, per i LUN iSCSI, il multipathing deve essere configurato legando le interfacce vmkernel agli adattatori di rete iSCSI. Per ulteriori informazioni, fai riferimento alla documentazione dello storage vSphere.

*Best practice*

Negli ambienti in cui vengono utilizzate le LUN Fibre Channel, NetApp consiglia di disporre di almeno due HBA, che garantiscono resilienza a livello di HBA/porta. NetApp consiglia inoltre di utilizzare lo zoning a destinazione singola come Best practice per la configurazione dello zoning.

È necessario utilizzare Virtual Storage Console (VSC) per impostare policy di multipathing, perché imposta policy per tutti i dispositivi storage NetApp nuovi ed esistenti.

### Errore host ESXi singolo



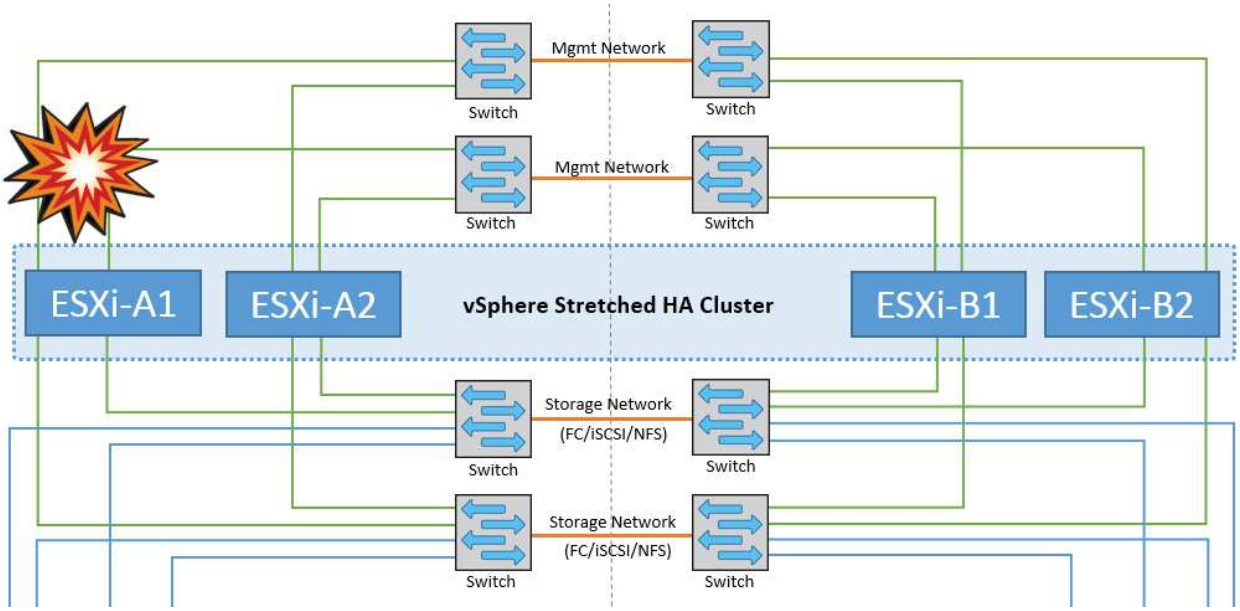

In questo scenario, se si verifica un guasto dell'host ESXi, il nodo master nel cluster VMware ha rileva il guasto dell'host in quanto non riceve più gli heartbeat di rete. Per determinare se l'host è effettivamente inattivo o solo una partizione di rete, il nodo master monitora gli heartbeat del datastore e, se sono assenti, esegue un controllo finale eseguendo il ping degli indirizzi IP di gestione dell'host guasto. Se tutti questi controlli sono negativi, il nodo master dichiara l'host un host guasto e tutte le macchine virtuali in esecuzione su questo host guasto vengono riavviate sull'host rimasto nel cluster.

Se sono state configurate le regole di affinità per DRS VM e host (le VM nel gruppo VM sitea_VM devono eseguire gli host nel gruppo host sitea_hosts), il master ha controlla prima le risorse disponibili nel sito A. Se non ci sono host disponibili nel sito A, il master tenta di riavviare le VM sugli host nel sito B.

È possibile che le macchine virtuali vengano avviate sugli host ESXi nell'altro sito se è presente un vincolo di risorse nel sito locale. Tuttavia, le regole di affinità definite per DRS VM e host verranno corrette in caso di violazione di regole mediante la migrazione delle macchine virtuali a qualsiasi host ESXi rimasto nel sito locale. Nei casi in cui DRS è impostato su manuale, NetApp consiglia di richiamare DRS e applicare le raccomandazioni per correggere il posizionamento della macchina virtuale.

In questo scenario, non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a essere intatti dai rispettivi siti.

### Isolamento dell'host ESXi

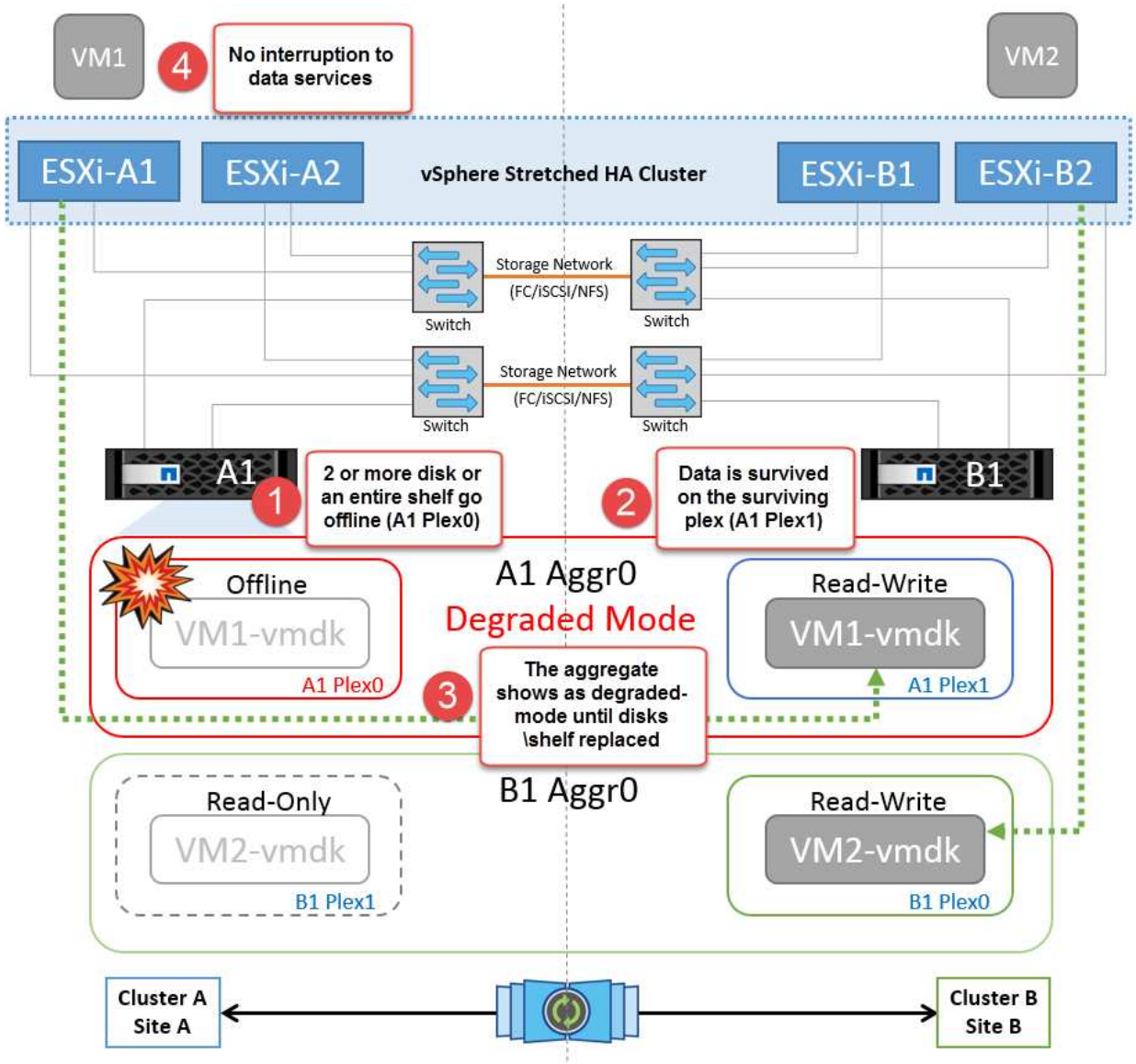



In questo scenario, se la rete di gestione dell'host ESXi non è attiva, il nodo master nel cluster ha non riceverà alcun heartbeat, pertanto l'host viene isolato nella rete. Per determinare se si è verificato un errore o se è solo isolato, il nodo master inizia a monitorare l'heartbeat del datastore. Se è presente, l'host viene dichiarato isolato dal nodo master. A seconda della risposta di isolamento configurata, l'host può scegliere di spegnere, spegnere le macchine virtuali o persino lasciare accese le macchine virtuali. L'intervallo predefinito per la risposta di isolamento è di 30 secondi.

In questo scenario, non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a essere intatti dai rispettivi siti.

### Guasto a shelf di dischi

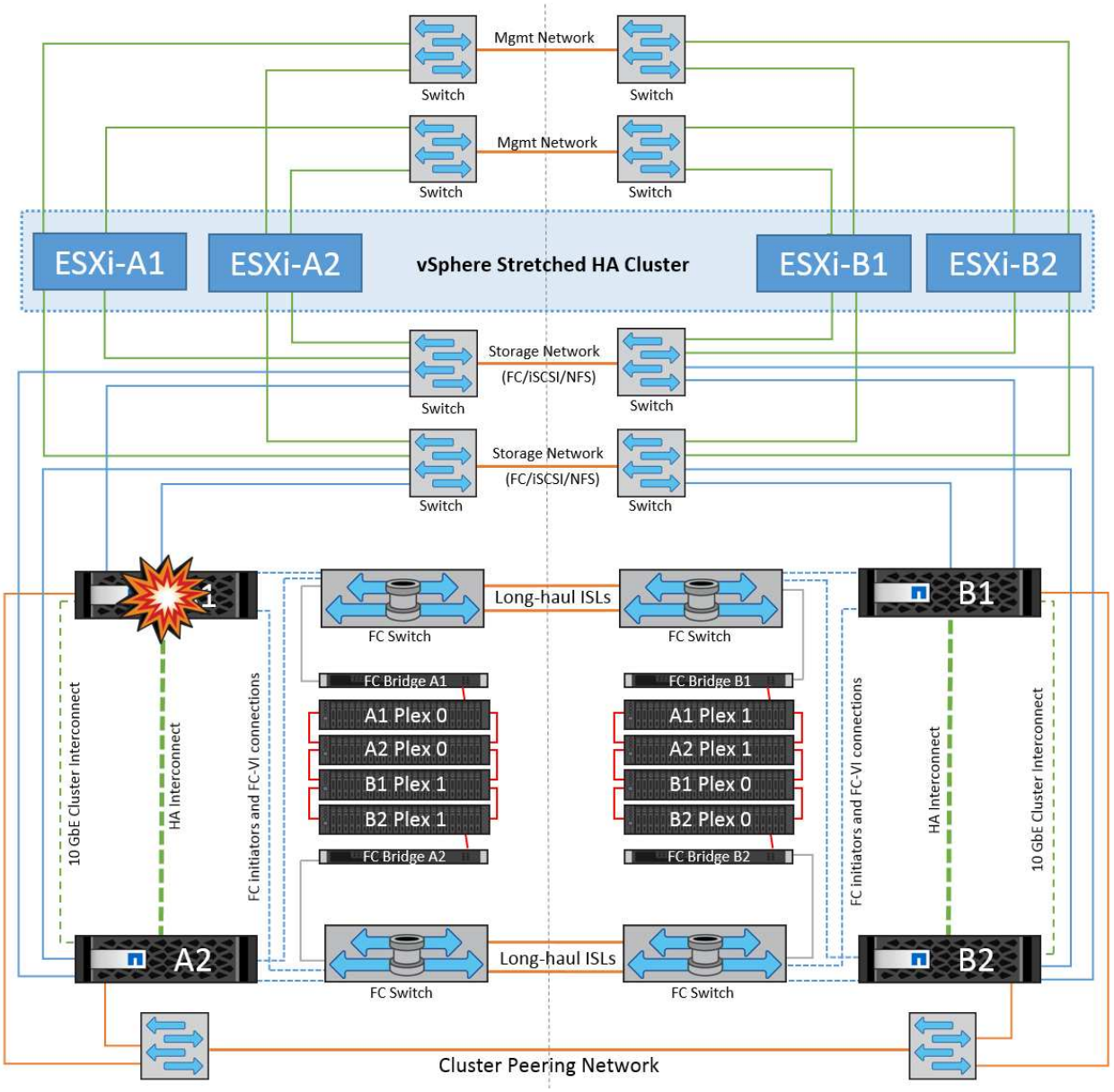
In questo scenario, si verifica un errore di più di due dischi o di un intero shelf. I dati vengono distribuiti dal plesso restante senza alcuna interruzione dei servizi dati. Il guasto del disco potrebbe influire su un plesso locale o remoto. Gli aggregati vengono visualizzati come modalità degradata perché è attivo un solo plesso. Una volta sostituiti i dischi guasti, gli aggregati interessati si risincronizzano automaticamente per ricostruire i dati. Dopo la risincronizzazione, gli aggregati tornano automaticamente alla normale modalità con mirroring. Se più di due dischi all'interno di un singolo gruppo RAID si sono guastati, il plex deve essere ricostruito da zero.




**Nota:** durante questo periodo, non si verifica alcun impatto sulle operazioni i/o della macchina virtuale, ma le prestazioni sono ridotte a causa dell'accesso ai dati dallo shelf di dischi remoto tramite collegamenti ISL.

### Guasto a un singolo storage controller

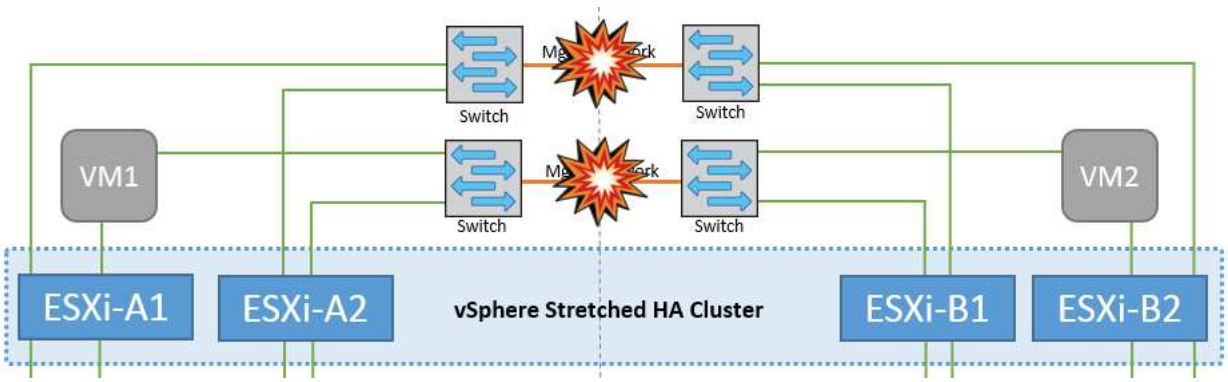
In questo scenario, uno dei due storage controller si guasta in un solo sito. Poiché è presente una coppia ha in ciascun sito, un guasto di un nodo attiva automaticamente il failover sull'altro nodo. Ad esempio, in caso di guasto al nodo A1, il relativo storage e carichi di lavoro vengono trasferiti automaticamente al nodo A2. Le macchine virtuali non saranno interessate perché tutti i plessi rimangono disponibili. I nodi del secondo sito (B1 e B2) non sono interessati. Inoltre, vSphere ha non intraprenderà alcuna azione perché il nodo master nel cluster riceverà comunque gli heartbeat di rete.




Se il failover fa parte di un rolling disaster (il nodo A1 esegue il failover su A2) e si verifica un successivo guasto di A2 o il guasto completo del sito A, è possibile eseguire lo switchover in seguito a un disastro nel sito B.

## Errori del collegamento interswitch

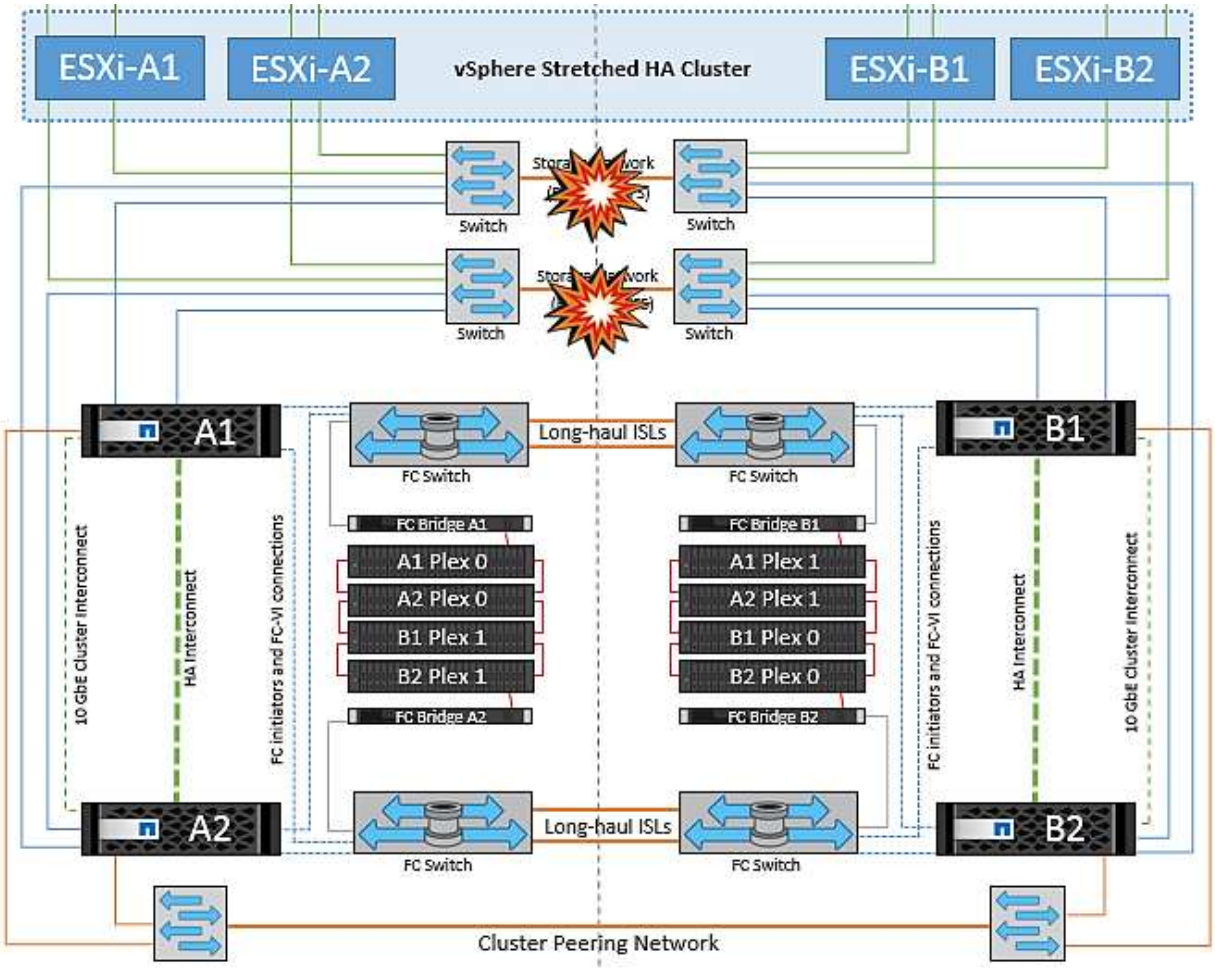
### Errore collegamento interswitch sulla rete di gestione



In questo scenario, se i collegamenti ISL nella rete di gestione host front-end si guastano, gli host ESXi nel sito A non saranno in grado di comunicare con gli host ESXi nel sito B. Ciò determina una partizione di rete poiché gli host ESXi in un determinato sito non sono in grado di inviare gli heartbeat di rete al nodo master nel cluster ha. Come tale, ci saranno due segmenti di rete a causa della partizione e vi sarà un nodo master in ogni segmento che proteggerà le VM da guasti host all'interno del sito specifico.

**Nota:** durante questo periodo, le macchine virtuali rimangono in esecuzione e non vi è alcuna modifica nel comportamento di MetroCluster in questo scenario. Tutti i datastore continuano a essere intatti dai rispettivi siti.

#### Errore collegamento interswitch sulla rete di storage

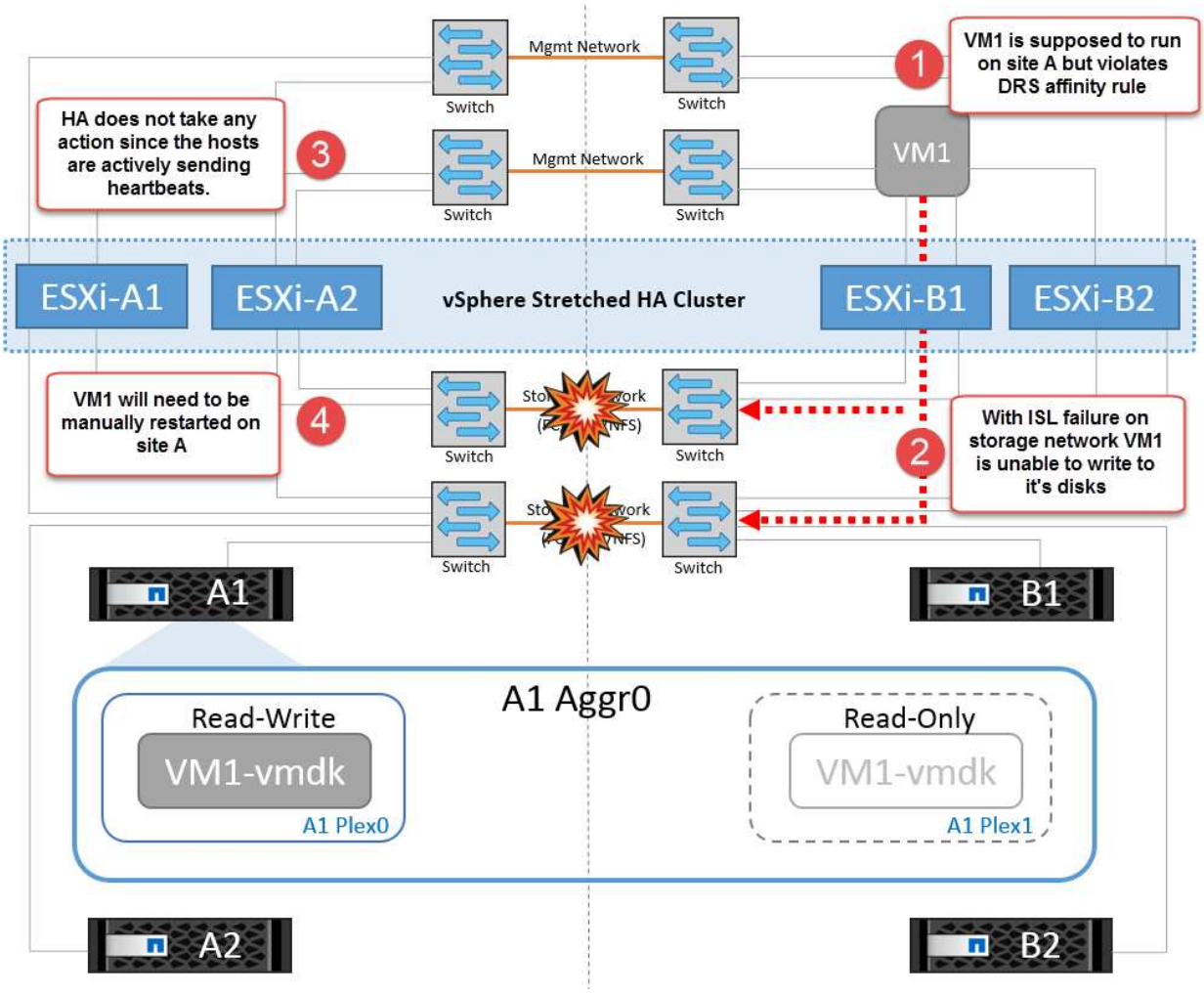



In questo scenario, se si verifica un errore nei collegamenti ISL nella rete di storage backend, gli host sul sito A perderanno l'accesso ai volumi di storage o alle LUN del cluster B nel sito B e viceversa. Le regole VMware DRS sono definite in modo che l'affinità tra il sito host e il sito di storage faciliti l'esecuzione delle macchine virtuali senza impatti all'interno del sito.

Durante questo periodo, le macchine virtuali rimangono in esecuzione nei rispettivi siti e in questo scenario non si verifica alcuna modifica nel comportamento di MetroCluster. Tutti i datastore continuano a essere intatti dai rispettivi siti.

Se per qualche motivo è stata violata la regola di affinità (ad esempio VM1, che doveva essere eseguito dal sito A in cui i dischi risiedono sui nodi del cluster locale A vengono eseguiti su un host nel sito B), il disco della macchina virtuale può essere acceduto in remoto tramite i link ISL. A causa di un errore del collegamento ISL, VM1 in esecuzione nel sito B non sarebbe in grado di scrivere sui propri dischi perché i percorsi del volume di storage non sono attivi e quella particolare macchina virtuale non è attiva. In queste situazioni, VMware ha non intraprende alcuna azione poiché gli host stanno inviando heartbeat. Tali macchine virtuali devono essere

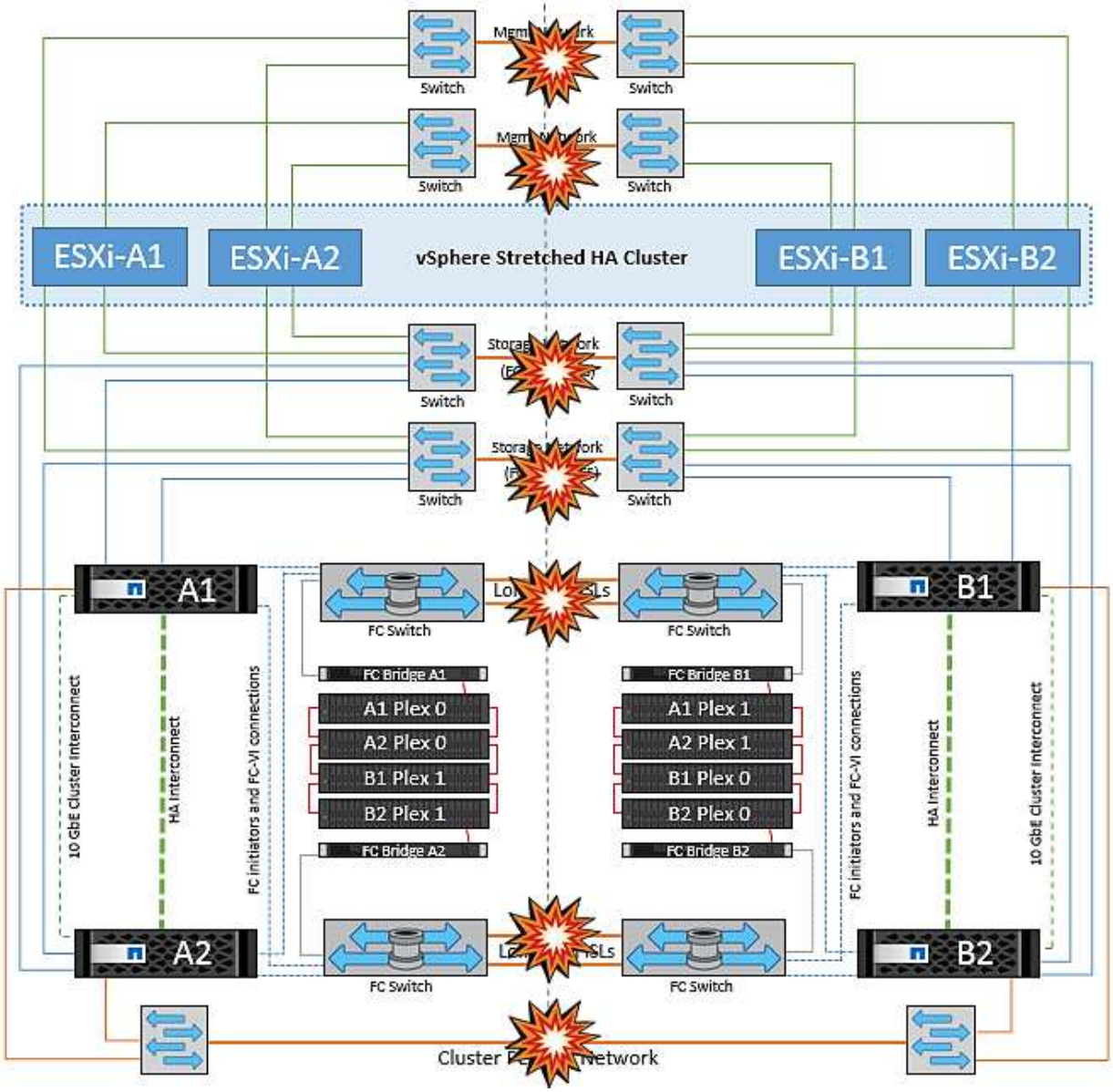
spente e attivate manualmente nei rispettivi siti. La figura seguente illustra una VM che viola una regola di affinità DRS.



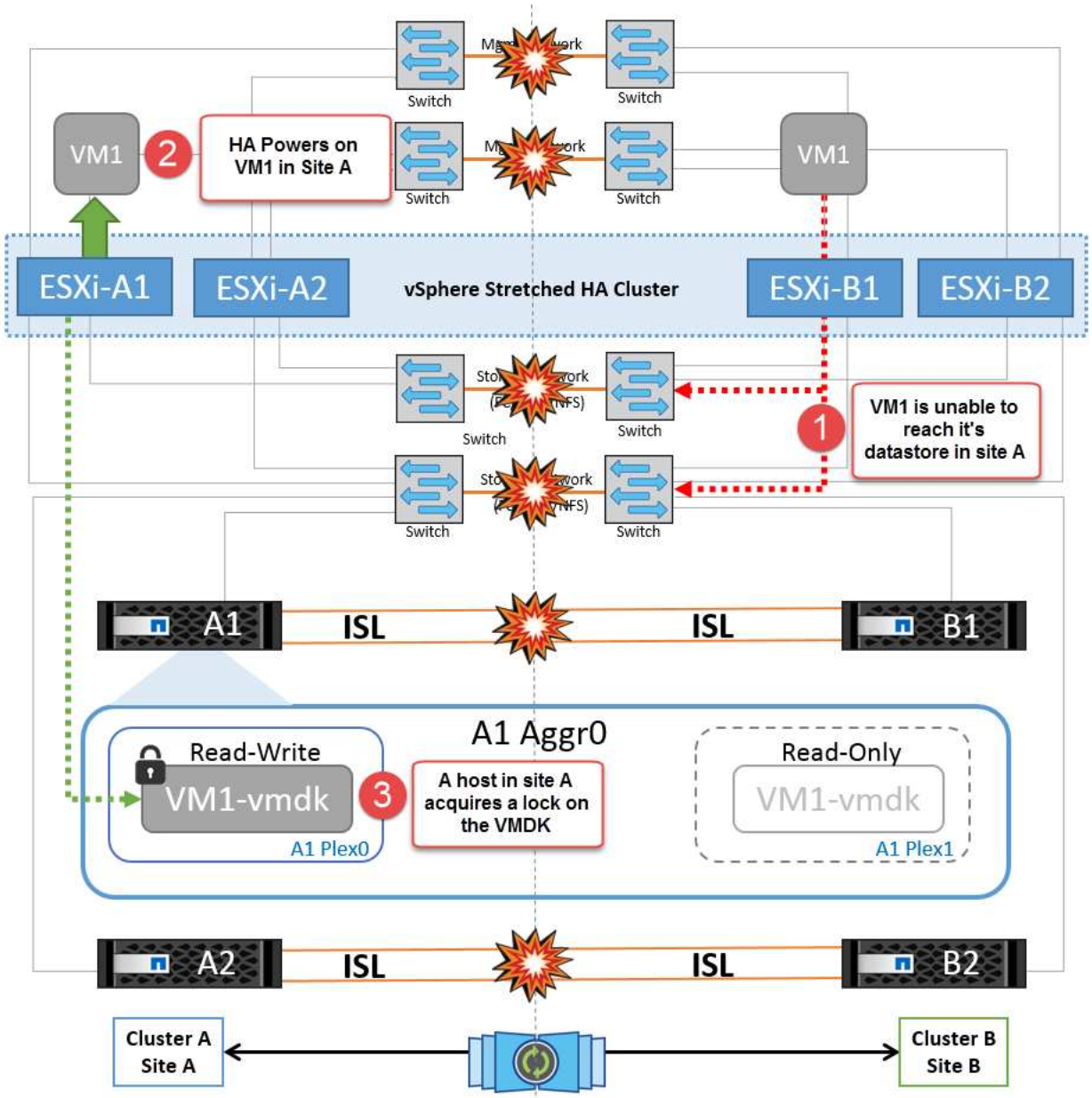

**Guasto a tutti gli interswitch o partizione completa del data center**

In questo scenario, tutti i collegamenti ISL tra i siti sono interrotti ed entrambi i siti sono isolati l'uno dall'altro. Come discusso in scenari precedenti, come ad esempio un errore ISL nella rete di gestione e nella rete di storage, le macchine virtuali non sono interessate da un errore ISL completo.

Dopo la partizione degli host ESXi tra i siti, l'agente vSphere ha controlla gli heartbeat del datastore e, in ciascun sito, gli host ESXi locali saranno in grado di aggiornare gli heartbeat del datastore nei rispettivi volumi/LUN di lettura/scrittura. Gli host nel sito A presumono che gli altri host ESXi nel sito B non abbiano avuto esito positivo perché non vi sono heartbeat di rete/datastore. VSphere ha nel sito A tenta di riavviare le macchine virtuali del sito B, operazione che alla fine ha esito negativo perché i datastore del sito B non saranno accessibili a causa di un guasto all'ISL di storage. Una situazione simile si ripete nel sito B.



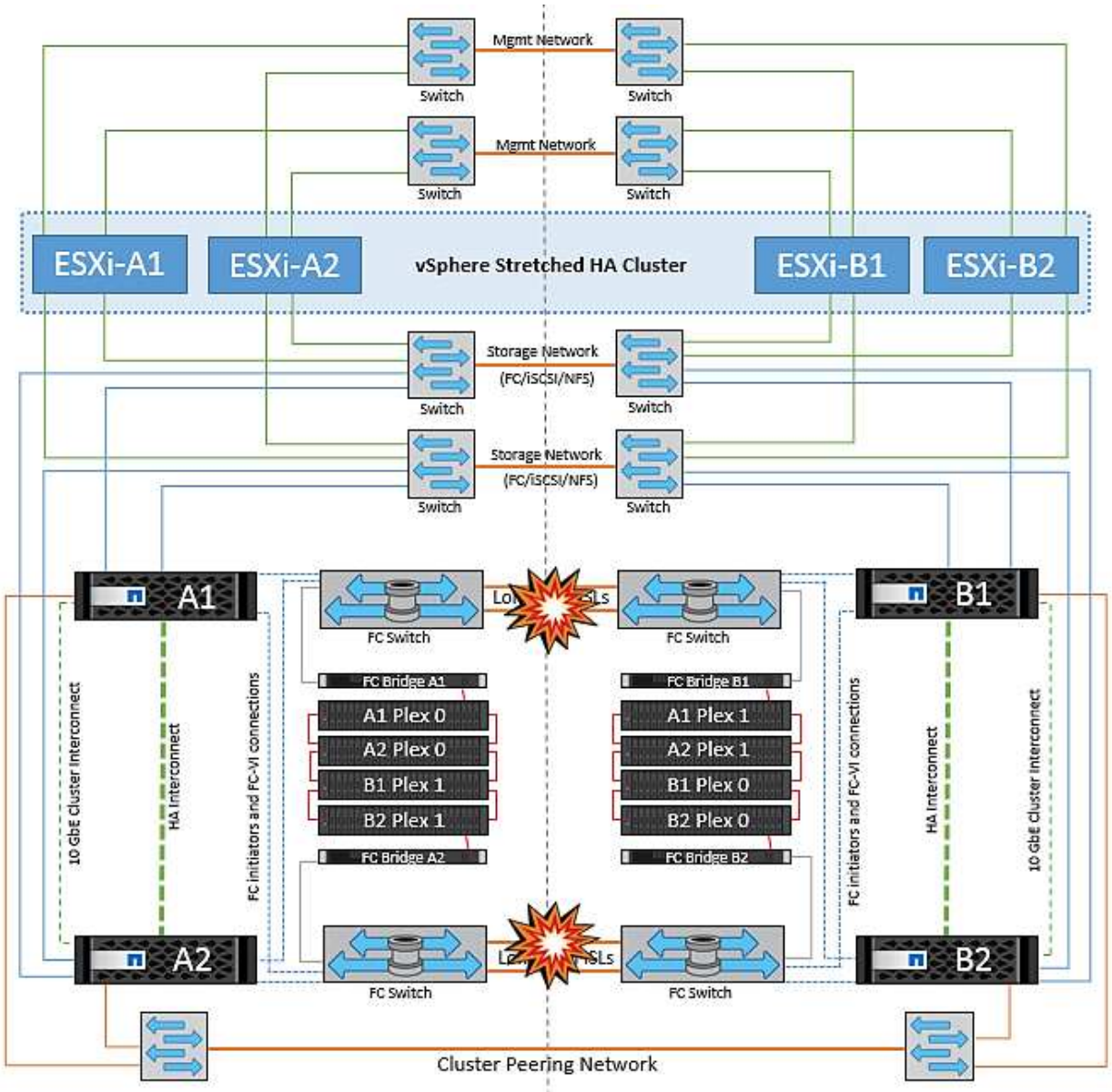

NetApp consiglia di determinare se una macchina virtuale ha violato le regole DRS. Tutte le macchine virtuali in esecuzione da un sito remoto non potranno accedere al datastore, quindi vSphere ha riavvia la macchina virtuale nel sito locale. Una volta che i collegamenti ISL sono tornati in linea, la macchina virtuale in esecuzione nel sito remoto verrà interrotta, poiché non possono esistere due istanze di macchine virtuali in esecuzione con gli stessi indirizzi MAC.




**Errore collegamento interswitch su entrambi i fabric in NetApp MetroCluster**

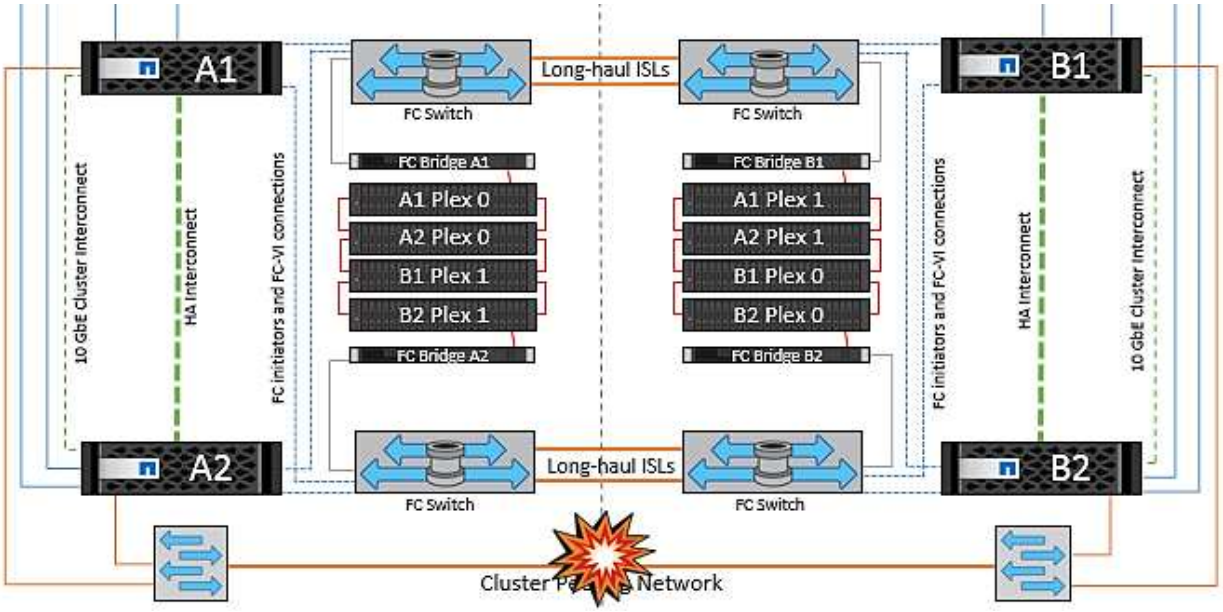
In uno scenario di errore di uno o più ISL, il traffico continua attraverso i collegamenti rimanenti. In caso di errore di tutti gli ISL su entrambi i fabric, in modo da eliminare un collegamento tra i siti per la replica di storage e NVRAM, ciascun controller continuerà a fornire i propri dati locali. Al ripristino di un minimo di un ISL, la risincronizzazione di tutti i plessi avviene automaticamente.

Eventuali scritture che si verificano dopo che tutti gli ISL sono inattivi non verranno mirrorate nell'altro sito. Uno switchover in caso di disastro, mentre la configurazione si trova in questo stato, causerebbe una perdita dei dati non sincronizzati. In questo caso, è necessario un intervento manuale per il ripristino dopo lo switchover. Se è probabile che non saranno disponibili ISL per un periodo prolungato, un amministratore può scegliere di arrestare tutti i servizi dati per evitare il rischio di perdita di dati se occorre eseguire uno switchover in caso di disastro. L'esecuzione di questa azione deve essere valutata rispetto alla probabilità che un evento disastroso richieda lo switchover prima che almeno un ISL diventi disponibile. In alternativa, in caso di errore degli ISL in uno scenario a cascata, un amministratore può attivare uno switchover pianificato verso uno dei siti prima che tutti i collegamenti abbiano avuto esito negativo.




**Errore collegamento cluster in peering**

In uno scenario di guasto al link del cluster in peering, poiché gli ISL del fabric sono ancora attivi, i servizi dati (letture e scritture) continuano in entrambi i siti verso entrambi i plessi. Eventuali modifiche alla configurazione del cluster, ad esempio l'aggiunta di una nuova SVM, il provisioning di un volume o di una LUN in una SVM esistente, non possono essere propagate all'altro sito. Questi vengono conservati nei volumi di metadati CRS locali e propagati automaticamente all'altro cluster al ripristino del collegamento di cluster sottoposto a peering. Se occorre uno switchover forzato prima del ripristino del link del cluster in peering, le modifiche alla configurazione del cluster in sospeso verranno riprodotte automaticamente dalla copia replicata remota dei volumi di metadati presenti nel sito rimasto nel processo di switchover.



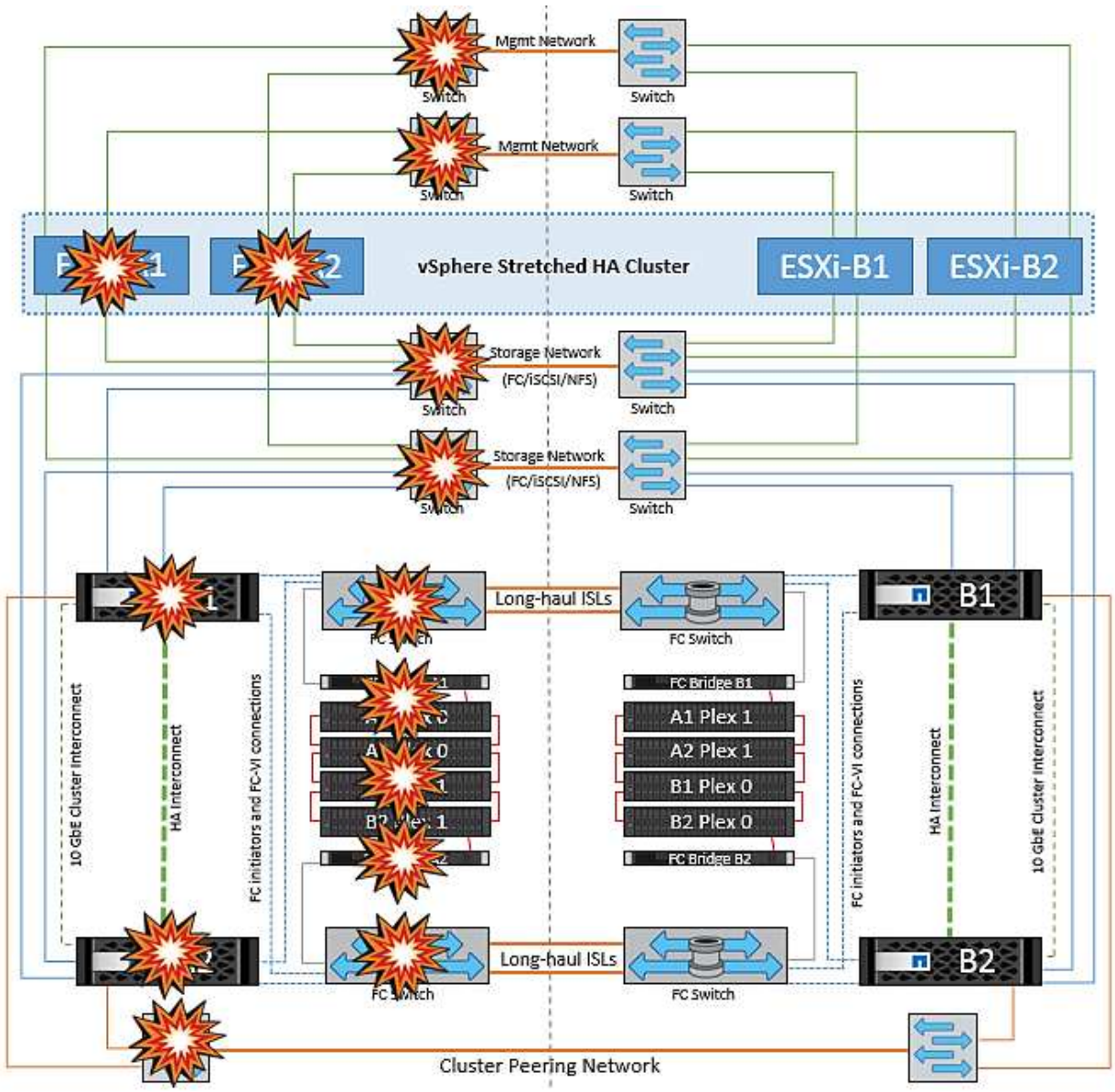

**Errore completo del sito**

In uno scenario di guasto completo del sito A, gli host ESXi nel sito B non otterranno l'heartbeat di rete dagli host ESXi nel sito A perché non sono attivi. Il master ha nel sito B verificherà che gli heartbeat del datastore non siano presenti, dichiarerà che gli host nel sito A non sono riusciti e tenterà di riavviare le macchine virtuali del sito A nel sito B. Durante questo periodo, l'amministratore dello storage esegue uno switchover per riprendere i servizi dei nodi guasti del sito rimasto e ripristinare i servizi di storage del sito A del sito B. Dopo che i volumi o le LUN del sito A sono disponibili nel sito B, l'agente master ha tenterà di riavviare le macchine virtuali del sito A nel sito B.

Se il tentativo dell'agente master vSphere ha di riavviare una VM (che comporta la registrazione e l'accensione) non riesce, il riavvio viene rieseguito dopo un ritardo. Il ritardo tra i riavvii può essere configurato fino a un massimo di 30 minuti. VSphere ha tenta di riavviare il sistema per un numero massimo di tentativi (sei tentativi per impostazione predefinita).

**Nota:** il master ha non inizia i tentativi di riavvio fino a quando il placement manager non trova lo spazio di archiviazione adeguato, quindi in caso di un guasto completo del sito, ciò avverrà dopo l'esecuzione dello switchover.

Se il sito A è stato sottoposto a switchover, un guasto successivo di uno dei nodi del sito B sopravvissuto può essere gestito senza problemi attraverso il failover verso il nodo rimasto. In questo caso, il lavoro di quattro nodi viene ora eseguito da un solo nodo. Il ripristino in questo caso consisterebbe nell'esecuzione di un giveback al nodo locale. Quindi, quando il sito A viene ripristinato, viene eseguita un'operazione di switchback per ripristinare il funzionamento regolare della configurazione.




# Sicurezza dei prodotti

## Strumenti ONTAP per VMware vSphere

La progettazione software con strumenti ONTAP per VMware vSphere si avvale delle seguenti attività di sviluppo sicure:

- **Modellazione delle minacce.** lo scopo della modellazione delle minacce è quello di individuare i difetti di sicurezza in una funzionalità, un componente o un prodotto nelle prime fasi del ciclo di vita dello sviluppo software. Un modello di minaccia è una rappresentazione strutturata di tutte le informazioni che influiscono sulla sicurezza di un'applicazione. In sostanza, si tratta di una vista dell'applicazione e del suo ambiente attraverso l'obiettivo della sicurezza.
- **Dynamic Application Security Testing (DAST).** questa tecnologia è progettata per rilevare le condizioni vulnerabili delle applicazioni in esecuzione. DAST testa le interfacce HTTP e HTML esposte delle applicazioni web-enable.
- **Valuta del codice di terze parti.** nell'ambito dello sviluppo di software con software open-source (OSS), è necessario risolvere le vulnerabilità di sicurezza che potrebbero essere associate a qualsiasi OSS

incorporato nel prodotto. Si tratta di un'operazione continua, in quanto una nuova versione di OSS potrebbe presentare una vulnerabilità scoperta di recente in qualsiasi momento.

- **Scansione delle vulnerabilità.** lo scopo della scansione delle vulnerabilità è quello di rilevare vulnerabilità di sicurezza comuni e note nei prodotti NetApp prima che vengano rilasciate ai clienti.
- Test di penetrazione.* il test di penetrazione è il processo di valutazione di un sistema, di un'applicazione Web o di una rete per individuare le vulnerabilità di sicurezza che potrebbero essere sfruttate da un utente malintenzionato. I test di penetrazione (test delle penne) di NetApp vengono condotti da un gruppo di aziende terze approvate e fidate. Il loro scopo di test include il lancio di attacchi contro un'applicazione o un software simile a intrusi o hacker ostili che utilizzano sofisticati metodi o strumenti di sfruttamento.

### Funzionalità di sicurezza del prodotto

I tool ONTAP per VMware vSphere includono le seguenti funzionalità di sicurezza in ciascuna release.

- **Login banner.** SSH è disattivato per impostazione predefinita e consente l'accesso una sola volta, se abilitato dalla console della macchina virtuale. Il seguente banner di accesso viene visualizzato dopo che l'utente ha inserito un nome utente nel prompt di accesso:

  **ATTENZIONE:** l'accesso non autorizzato a questo sistema è vietato e sarà perseguito dalla legge. Accedendo a questo sistema, l'utente accetta che le proprie azioni possano essere monitorate in caso di sospetto di utilizzo non autorizzato.

  Dopo che l'utente ha completato l'accesso tramite il canale SSH, viene visualizzato il seguente testo:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **RBAC (role-based access control).** due tipi di controlli RBAC sono associati ai tool ONTAP:
  - Privilegi vCenter Server nativi
  - Privilegi specifici del plug-in vCenter. Per ulteriori informazioni, vedere "questo link".
- **Canali di comunicazione crittografati.** tutte le comunicazioni esterne avvengono su HTTPS utilizzando la versione 1.2 di TLS.
- **Esposizione minima delle porte.** solo le porte necessarie sono aperte sul firewall.

  La seguente tabella descrive i dettagli della porta aperta.

| Porta TCP v4/v6 n. | Direzione | Funzione |
|---|---|---|
| 8143 | in entrata | Connessioni HTTPS per API REST |
| 8043 | in entrata | Connessioni HTTPS |

| Porta TCP v4/v6 n. | Direzione | Funzione |
|---|---|---|
| 9060 | in entrata | Connessioni HTTPS<br>Utilizzato per connessioni SOAP su https<br>Questa porta deve essere aperta per consentire a un client di connettersi al server API degli strumenti ONTAP. |
| 22 | in entrata | SSH (Disattivato per impostazione predefinita) |
| 9080 | in entrata | Connessioni HTTPS - VP e SRA - connessioni interne solo da loopback |
| 9083 | in entrata | Connessioni HTTPS - VP e SRA<br>Utilizzato per connessioni SOAP su https |
| 1162 | in entrata | Pacchetti di trap SNMP VP |
| 1527 | solo interno | Porta del database Derby, solo tra questo computer e se stesso, connessioni esterne non accettate — solo connessioni interne |
| 443 | bidirezionale | Utilizzato per le connessioni ai cluster ONTAP |

- **Supporto dei certificati firmati dall'autorità di certificazione (CA).** i tool ONTAP per VMware vSphere supportano i certificati firmati CA. Vedi questo "articolo della knowledge base" per ulteriori informazioni.
- **Registrazione audit.** i pacchetti di supporto possono essere scaricati e sono estremamente dettagliati. ONTAP Tools registra tutte le attività di login e logout degli utenti in un file di log separato. Le chiamate API VASA vengono registrate in un registro di controllo VASA dedicato (cxf.log locale).
- **Criteri per le password.** vengono seguite le seguenti policy per le password:
  - Le password non vengono registrate in alcun file di log.
  - Le password non vengono comunicate in testo normale.
  - Le password vengono configurate durante il processo di installazione.
  - La cronologia delle password è un parametro configurabile.
  - La durata minima della password è impostata su 24 ore.
  - Il completamento automatico dei campi della password è disattivato.
  - Gli strumenti ONTAP crittografano tutte le informazioni sulle credenziali memorizzate utilizzando l'hashing SHA256.

## Plug-in di SnapCenter per VMware vSphere

Il plug-in NetApp SnapCenter per il software engineering VMware vSphere utilizza le seguenti attività di sviluppo sicuro:

- **Modellazione delle minacce.** lo scopo della modellazione delle minacce è quello di individuare i difetti di sicurezza in una funzionalità, un componente o un prodotto nelle prime fasi del ciclo di vita dello sviluppo software. Un modello di minaccia è una rappresentazione strutturata di tutte le informazioni che influiscono sulla sicurezza di un'applicazione. In sostanza, si tratta di una vista dell'applicazione e del suo ambiente attraverso l'obiettivo della sicurezza.
- **Dynamic Application Security testing (DAST).** tecnologie progettate per rilevare condizioni vulnerabili sulle applicazioni in esecuzione. DAST testa le interfacce HTTP e HTML esposte delle applicazioni web-enable.
- **Valuta del codice di terze parti.** come parte dello sviluppo di software e dell'utilizzo di software open-source (OSS), è importante risolvere le vulnerabilità di sicurezza che potrebbero essere associate a OSS che è stato incorporato nel prodotto. Si tratta di un impegno continuo, in quanto la versione del componente OSS potrebbe presentare una vulnerabilità scoperta di recente in qualsiasi momento.
- **Scansione delle vulnerabilità.** lo scopo della scansione delle vulnerabilità è quello di rilevare vulnerabilità di sicurezza comuni e note nei prodotti NetApp prima che vengano rilasciate ai clienti.
- Test di penetrazione.* il test di penetrazione è il processo di valutazione di un sistema, di un'applicazione Web o di una rete per individuare le vulnerabilità della sicurezza che potrebbero essere sfruttate da un utente malintenzionato. I test di penetrazione (test delle penne) di NetApp vengono condotti da un gruppo di aziende terze approvate e fidate. Il loro scopo di test include il lancio di attacchi contro un'applicazione o un software come intrusi o hacker ostili che utilizzano sofisticati metodi o strumenti di sfruttamento.
- **Attività di risposta agli incidenti di sicurezza dei prodotti.** le vulnerabilità di sicurezza sono scoperte sia internamente che esternamente all'azienda e possono rappresentare un serio rischio per la reputazione di NetApp se non vengono affrontate in modo tempestivo. Per facilitare questo processo, un Product Security Incident Response Team (PSIRT) segnala e tiene traccia delle vulnerabilità.

**Funzionalità di sicurezza del prodotto**

Il plug-in NetApp SnapCenter per VMware vSphere include le seguenti funzionalità di sicurezza in ciascuna release:

- **Accesso limitato alla shell.** SSH è disattivato per impostazione predefinita e gli accessi una tantum sono consentiti solo se sono abilitati dalla console della macchina virtuale.
- **Avviso di accesso nel banner di accesso.** il seguente banner di accesso viene visualizzato dopo che l'utente ha inserito un nome utente nel prompt di accesso:

  **ATTENZIONE:** l'accesso non autorizzato a questo sistema è vietato e sarà perseguito dalla legge. Accedendo a questo sistema, l'utente accetta che le proprie azioni possano essere monitorate in caso di sospetto di utilizzo non autorizzato.

  Una volta completato l'accesso tramite il canale SSH, viene visualizzato il seguente output:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **RBAC (role-based access control).** due tipi di controlli RBAC sono associati ai tool ONTAP:

- Privilegi vCenter Server nativi.
- Privilegi specifici del plug-in VMware vCenter. Per ulteriori informazioni, vedere "RBAC (Role-Based Access Control)".

- **Canali di comunicazione crittografati.** tutte le comunicazioni esterne avvengono su HTTPS utilizzando TLS.
- **Esposizione minima delle porte.** solo le porte necessarie sono aperte sul firewall.

La seguente tabella fornisce i dettagli della porta aperta.

| Numero della porta TCP v4/v6 | Funzione |
|---|---|
| 8144 | Connessioni HTTPS per API REST |
| 8080 | Connessioni HTTPS per GUI OVA |
| 22 | SSH (disattivato per impostazione predefinita) |
| 3306 | MySQL (solo connessioni interne; connessioni esterne disattivate per impostazione predefinita) |
| 443 | Nginx (servizi di protezione dei dati) |

- **Supporto dei certificati firmati dall'autorità di certificazione (CA).** il plug-in SnapCenter per VMware vSphere supporta la funzione dei certificati firmati dalla CA. Vedere "Come creare e/o importare un certificato SSL nel plug-in SnapCenter per VMware vSphere (SCV)".
- **Password policy.** sono in vigore i seguenti criteri relativi alle password:
  - Le password non vengono registrate in alcun file di log.
  - Le password non vengono comunicate in testo normale.
  - Le password vengono configurate durante il processo di installazione.
  - Tutte le informazioni sulle credenziali vengono memorizzate utilizzando l'hashing SHA256.
- **Immagine del sistema operativo di base.** il prodotto viene fornito con il sistema operativo di base Debian per OVA con accesso limitato e accesso alla shell disattivato. In questo modo si riduce l'impatto degli attacchi. Ogni sistema operativo SnapCenter release base viene aggiornato con le ultime patch di sicurezza disponibili per la massima copertura di sicurezza.

NetApp sviluppa funzionalità software e patch di sicurezza per quanto riguarda il plug-in SnapCenter per l'appliance VMware vSphere e le rilascia ai clienti come piattaforma software integrata. Poiché queste appliance includono dipendenze specifiche del sistema operativo secondario Linux e il nostro software proprietario, NetApp consiglia di non apportare modifiche al sistema operativo secondario, in quanto questo potrebbe influire sull'appliance NetApp. Ciò potrebbe influire sulla capacità di NetApp di supportare l'appliance. NetApp consiglia di testare e implementare la versione più recente del codice per le appliance, perché vengono rilasciate per correggere eventuali problemi relativi alla sicurezza.

# Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere

## Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere

La guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere fornisce una serie completa di istruzioni per la configurazione delle impostazioni più sicure.

Queste guide si applicano sia alle applicazioni che al sistema operativo guest dell'appliance stessa.

## Verifica dell'integrità dei tool ONTAP per i pacchetti di installazione di VMware vSphere

Sono disponibili due metodi per verificare l'integrità dei pacchetti di installazione degli strumenti ONTAP.

1. Verifica dei checksum
2. Verifica della firma

I checksum sono disponibili nelle pagine di download dei pacchetti di installazione di OTV. Gli utenti devono verificare i checksum dei pacchetti scaricati in base al checksum fornito nella pagina di download.

### Verifica della firma degli strumenti ONTAP OVA

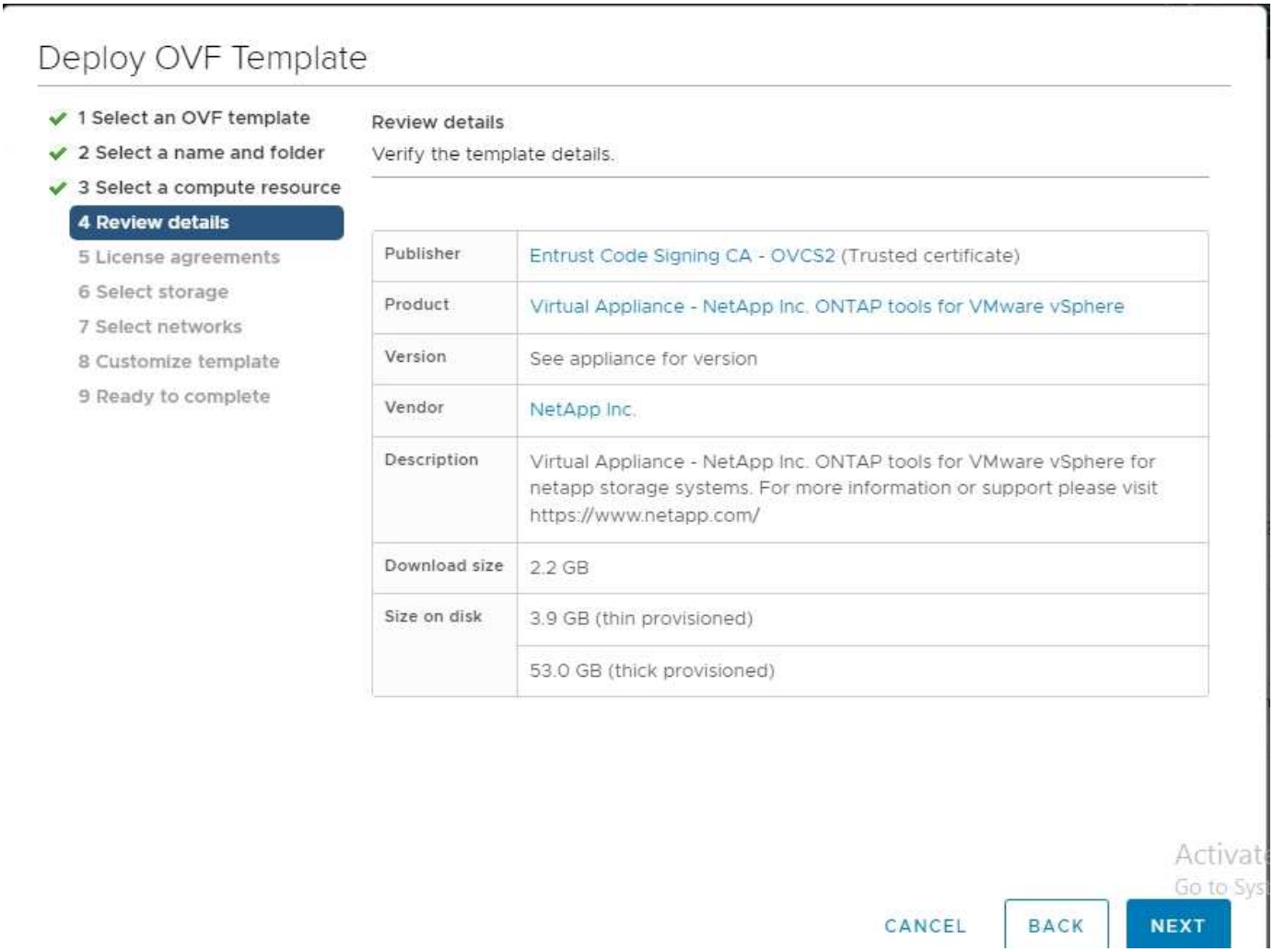
Il pacchetto di installazione vApp viene fornito sotto forma di tarball. Questo tarball contiene certificati intermedi e root per l'appliance virtuale insieme a un file README e un pacchetto OVA. Il file README guida gli utenti su come verificare l'integrità del pacchetto vApp OVA.

I clienti devono inoltre caricare il certificato root e intermedio fornito su vCenter versione 7.0U3E e successive. Per le versioni vCenter comprese tra 7.0.1 e 7,0.U3E, la funzionalità di verifica del certificato non è supportata da VMware. I clienti non devono caricare alcun certificato per le versioni 6.x. di vCenter

#### Caricamento del certificato root attendibile in vCenter

1. Accedere con il client VMware vSphere a vCenter Server.
2. Specificare il nome utente e la password per adminutator@vsphere.local o un altro membro del gruppo vCenter Single Sign-on Administrators. Se durante l'installazione è stato specificato un dominio diverso, accedere come Administrator@mydomain.
3. Accedere all'interfaccia utente di Gestione certificati: a. Dal menu principale, selezionare Amministrazione. b. Nella sezione certificati, fare clic su Gestione certificati.
4. Se richiesto dal sistema, immettere le credenziali di vCenter Server.
5. In certificati principali attendibili, fare clic su Aggiungi.
6. Fare clic su Sfoglia e selezionare la posizione del file .pem del certificato (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Fare clic su Aggiungi. Il certificato viene aggiunto al negozio.

Fare riferimento a. "Aggiungere un certificato radice attendibile all'archivio certificati" per ulteriori informazioni. Durante la distribuzione di una vApp (utilizzando il file OVA), la firma digitale per il pacchetto vApp può essere verificata nella pagina "Dettagli revisione". Se il pacchetto vApp scaricato è originale, nella colonna 'Publisher' viene visualizzato 'Trusted Certificate' (certificato attendibile) (come nella seguente schermata).




**Verifica della firma degli attrezzi ONTAP ISO e SRA tar.gz**

NetApp condivide il proprio certificato di firma del codice con i clienti nella pagina di download del prodotto, insieme ai file zip del prodotto per OTV-ISO e SRA.tgz.

Dal certificato di firma del codice, gli utenti possono estrarre la chiave pubblica nel modo seguente:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Quindi, utilizzare la chiave pubblica per verificare la firma per il
prodotto zip iso e tgz come indicato di seguito:
```

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Esempio:
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

## Porte e protocolli

Di seguito sono elencate le porte e i protocolli necessari per consentire la comunicazione tra gli strumenti ONTAP per il server VMware vSphere e altre entità come i sistemi di storage gestito, i server e altri componenti.

#### Porte in entrata e in uscita richieste per OTV

Tenere presente la tabella riportata di seguito che elenca le porte in entrata e in uscita necessarie per il corretto funzionamento degli strumenti ONTAP. È importante assicurarsi che solo le porte menzionate nella tabella siano aperte per i collegamenti da macchine remote, mentre tutte le altre porte devono essere bloccate per i collegamenti da macchine remote. In questo modo si garantisce la sicurezza e la sicurezza del sistema.

La seguente tabella descrive i dettagli della porta aperta.

| Porta TCP v4/V6 # | Direzione | Funzione |
|---|---|---|
| 8143 | in entrata | Connessioni HTTPS per API REST |
| 8043 | in entrata | Connessioni HTTPS |
| 9060 | in entrata | Connessioni HTTPS<br>Utilizzato per connessioni SOAP su HTTPS<br>Questa porta deve essere aperta per consentire a un client di connettersi al server API degli strumenti ONTAP. |
| 22 | in entrata | SSH (Disattivato per impostazione predefinita) |
| 9080 | in entrata | Connessioni HTTPS - VP e SRA - connessioni interne solo da loopback |
| 9083 | in entrata | Connessioni HTTPS - VP e SRA<br>Utilizzato per le connessioni SOAP su HTTPS |
| 1162 | in entrata | Pacchetti di trap SNMP VP |
| 8443 | in entrata | Plugin remoto |
| 1527 | solo interno | Porta del database Derby, solo tra questo computer e se stesso, connessioni esterne non accettate — solo connessioni interne |
| 8150 | solo interno | Il servizio integrità registro viene eseguito sulla porta |
| 443 | bidirezionale | Utilizzato per le connessioni ai cluster ONTAP |

### Controllo dell'accesso remoto al database Derby

Gli amministratori possono accedere al database derby con i seguenti comandi. È possibile accedervi tramite la VM locale degli strumenti ONTAP e un server remoto con i seguenti passaggi:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

**esempio:**

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                    |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                    |
SYS                 |SYSCHECKS                     |
SYS                 |SYSCOLPERMS                   |
SYS                 |SYSCOLUMNS                    |
SYS                 |SYSCONGLOMERATES              |
SYS                 |SYSCONSTRAINTS                |
SYS                 |SYSDEPENDS                    |
SYS                 |SYSFILES                      |
SYS                 |SYSFOREIGNKEYS                |
SYS                 |SYSKEYS                       |
SYS                 |SYSPERMS                      |
```

## Tool ONTAP per access point VMware vSphere (utenti)

L'installazione di ONTAP Tools per VMware vSphere consente di creare e utilizzare tre tipi di utenti:

1. System User (utente di sistema): L'account utente root
2. Utente dell'applicazione: Gli account utente amministratore, utente principale e utente di database
3. Support user: L'account utente diag

### 1. Utente di sistema

L'utente System(root) viene creato dall'installazione degli strumenti ONTAP sul sistema operativo sottostante (Debian).

- Un utente di sistema predefinito "root" viene creato su Debian tramite l'installazione degli strumenti ONTAP. L'impostazione predefinita è disattivata e può essere attivata ad hoc tramite la console 'Maint'.

### 2. Utente dell'applicazione

L'utente dell'applicazione viene denominato come utente locale negli strumenti di ONTAP. Si tratta di utenti creati nell'applicazione ONTAP Tools. Nella tabella seguente sono elencati i tipi di utenti dell'applicazione:

| Utente | Descrizione |
| --- | --- |
| Administrator User (utente amministratore) | Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. La password scadrà tra 90 giorni e gli utenti saranno tenuti a cambiarla. |
| Utente manutenzione | Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. Si tratta di un utente addetto alla manutenzione che viene creato per eseguire le operazioni della console di manutenzione. |
| Utente database | Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. La password scadrà tra 90 giorni e gli utenti saranno tenuti a cambiarla. |

**3. Utente di assistenza (utente diag)**

Durante l'installazione di ONTAP Tools, viene creato un utente di supporto. Questo utente può essere utilizzato per accedere agli strumenti ONTAP in caso di problemi o interruzioni del server e per raccogliere i registri. Per impostazione predefinita, questo utente è disattivato, ma può essere attivato su base adhoc tramite la console 'Maint'. È importante notare che l'utente verrà disattivato automaticamente dopo un determinato periodo di tempo.

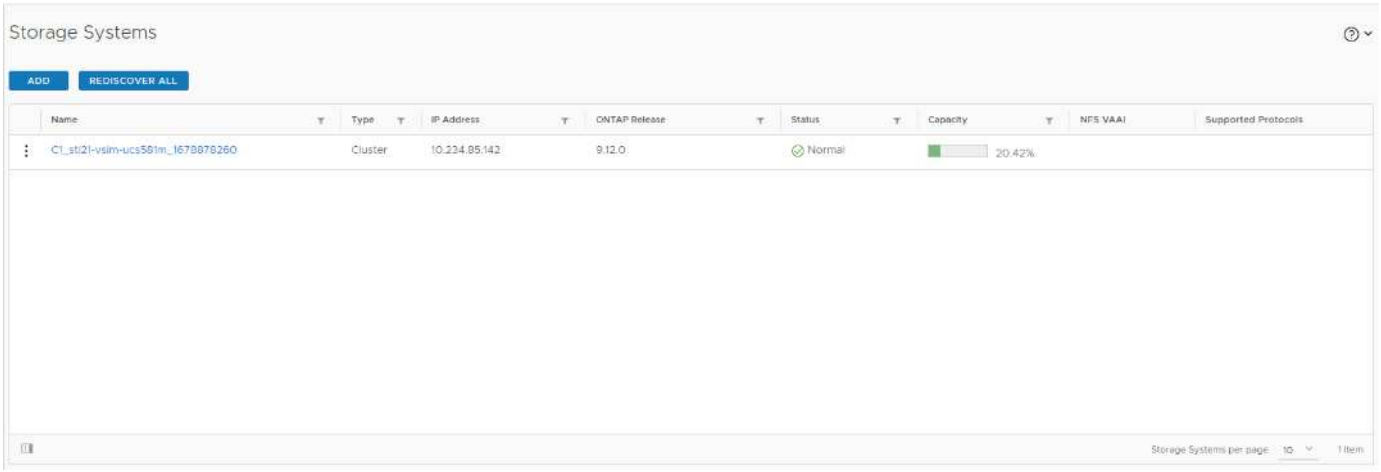
## Mutual TLS (autenticazione basata su certificato)

Le versioni ONTAP 9,7 e successive supportano la comunicazione mutua TLS. A partire dai tool ONTAP per VMware e vSphere 9,12, il TLS reciproco viene utilizzato per la comunicazione con i cluster appena aggiunti (in base alla versione di ONTAP).

**ONTAP**

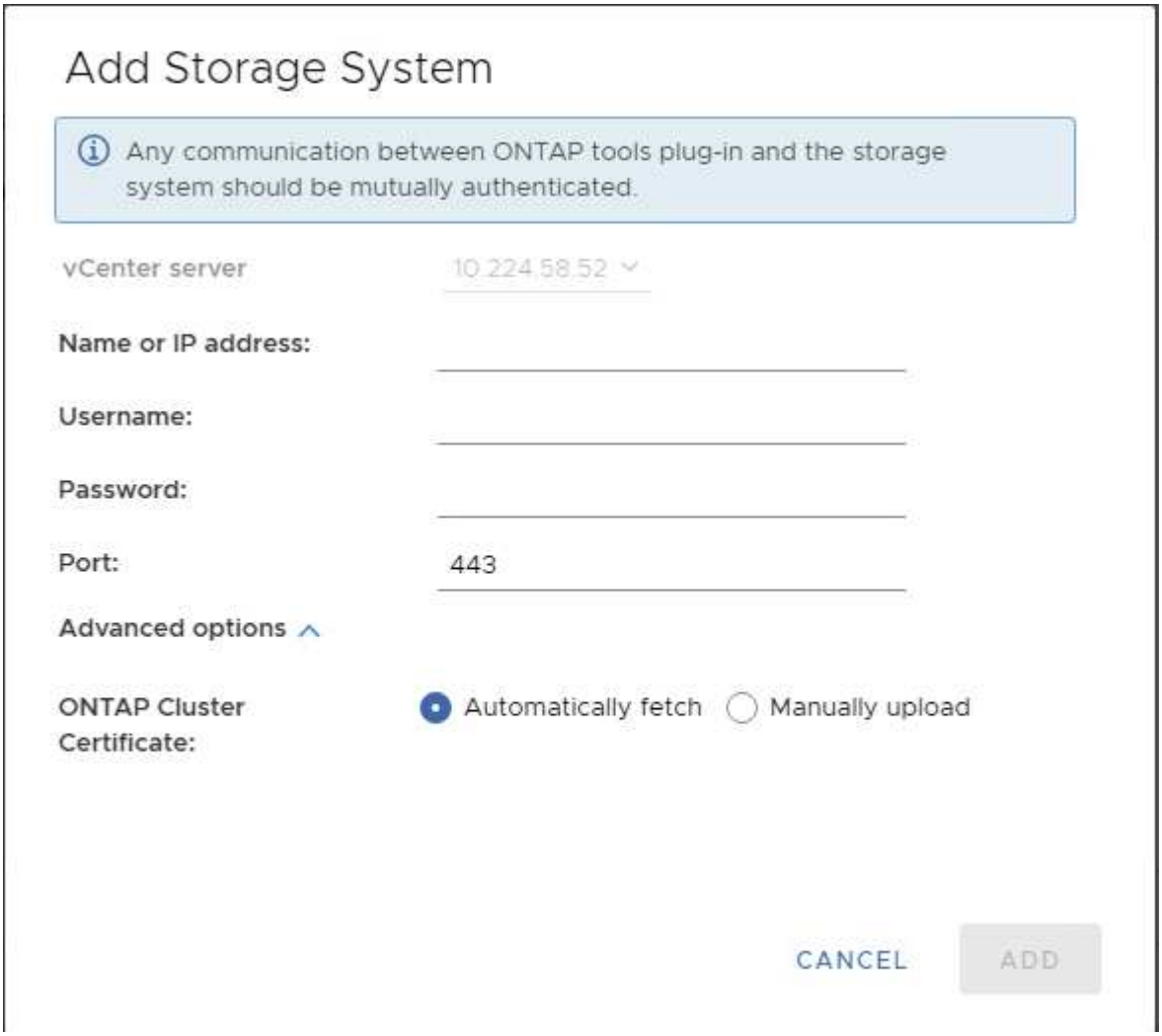
Per tutti i sistemi storage aggiunti in precedenza: Durante un aggiornamento, tutti i sistemi storage aggiunti diventeranno automaticamente attendibili e verranno configurati i meccanismi di autenticazione basati su certificato.

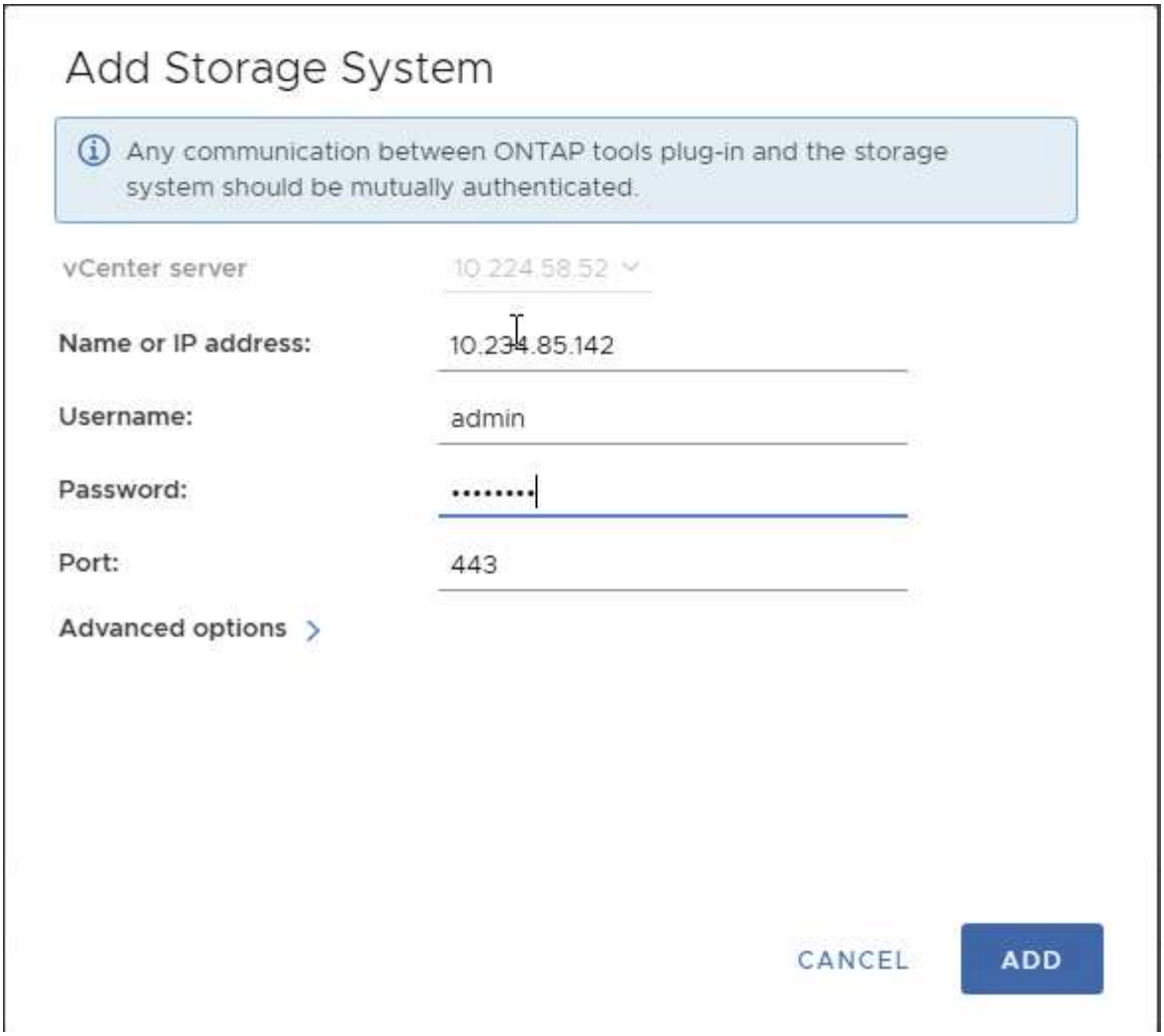
Come nella schermata riportata di seguito, nella pagina di configurazione del cluster viene visualizzato lo stato di Mutual TLS (autenticazione basata su certificato), configurato per ciascun cluster.

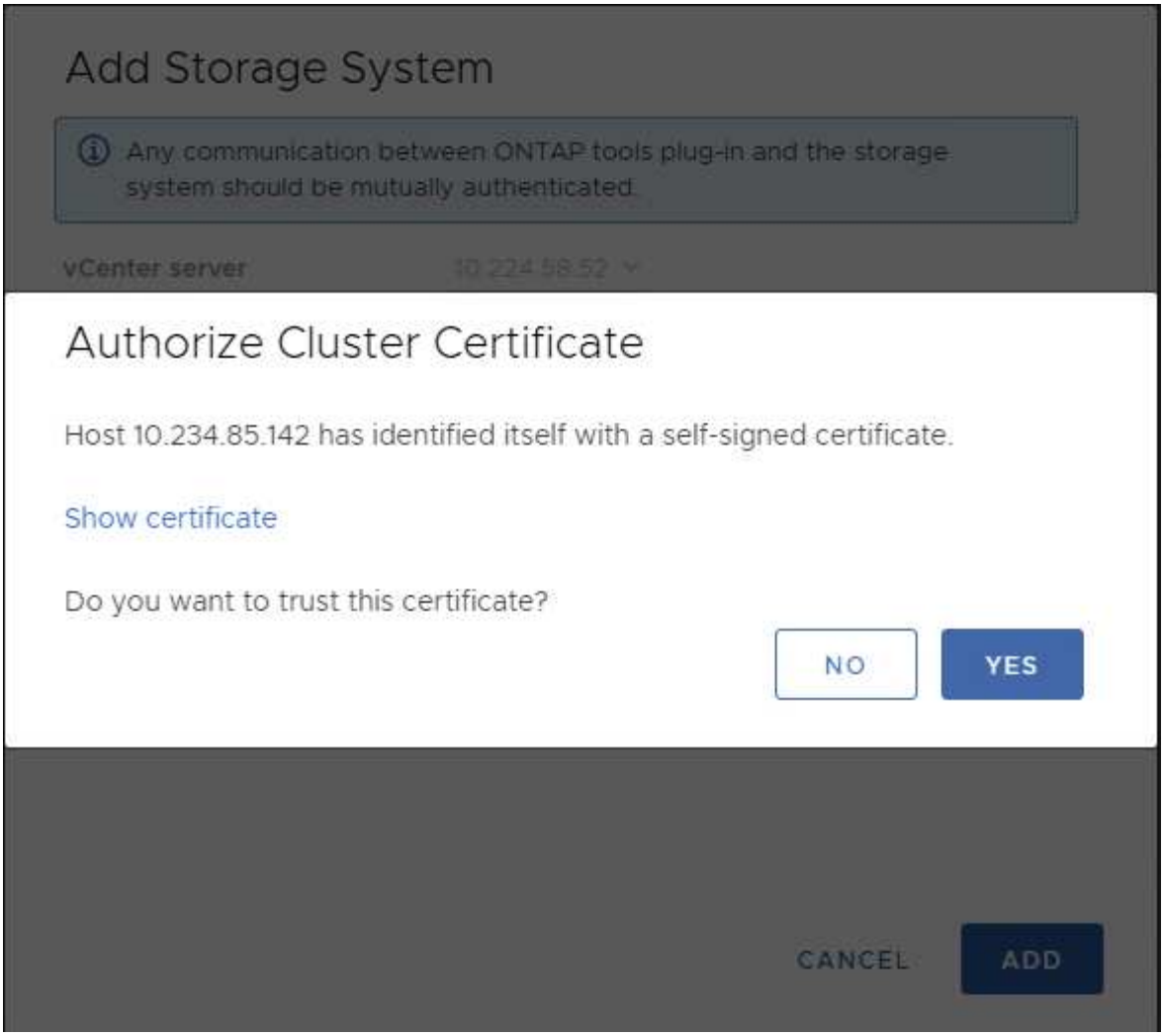


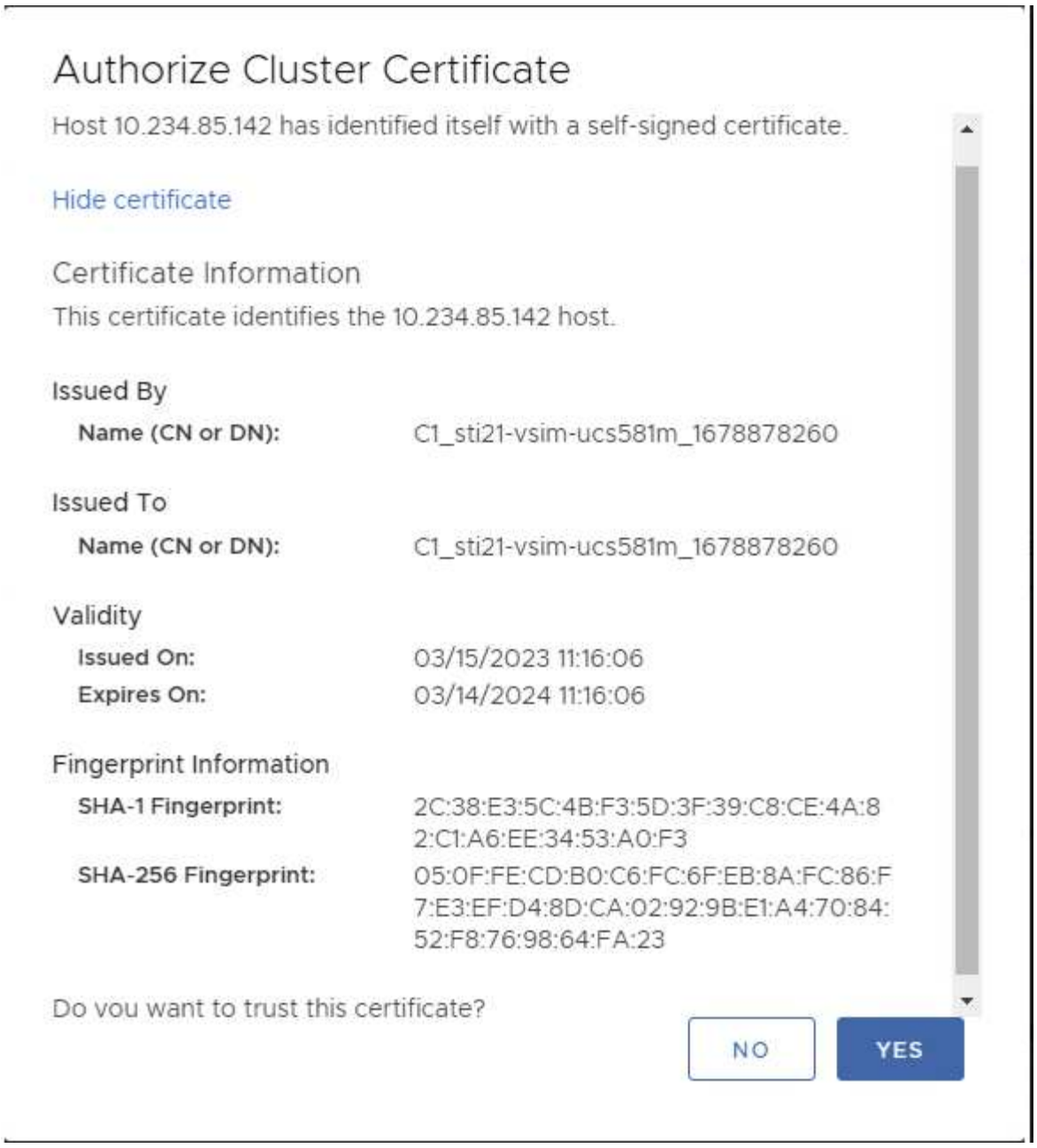

**Aggiunta cluster**

Durante il flusso di lavoro di aggiunta del cluster, se il cluster che viene aggiunto supporta MTLS, MTLS verrà configurato per impostazione predefinita. L'utente non deve eseguire alcuna configurazione per questo. La schermata riportata di seguito mostra la schermata presentata all'utente durante l'aggiunta del cluster.




Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

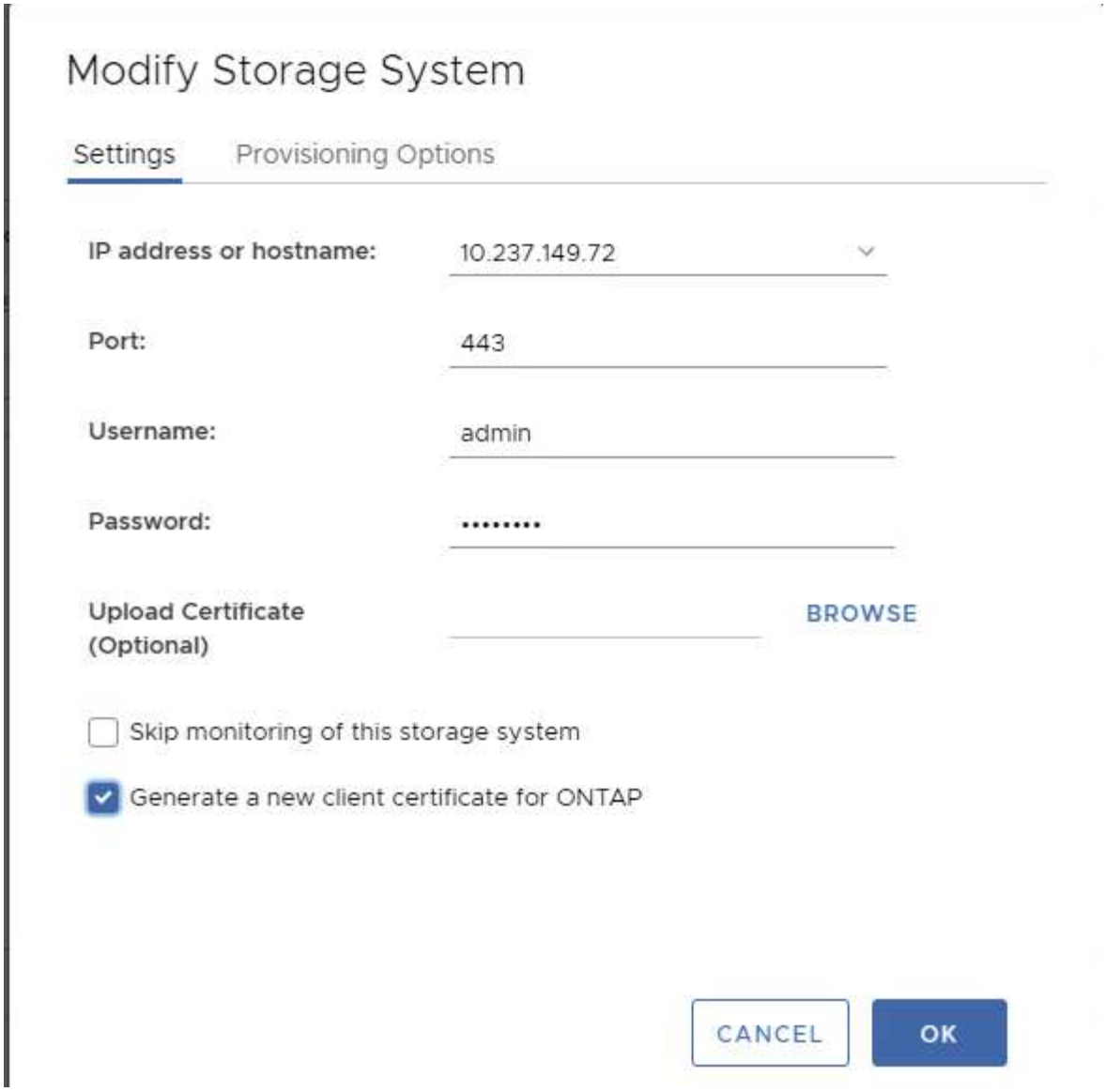

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

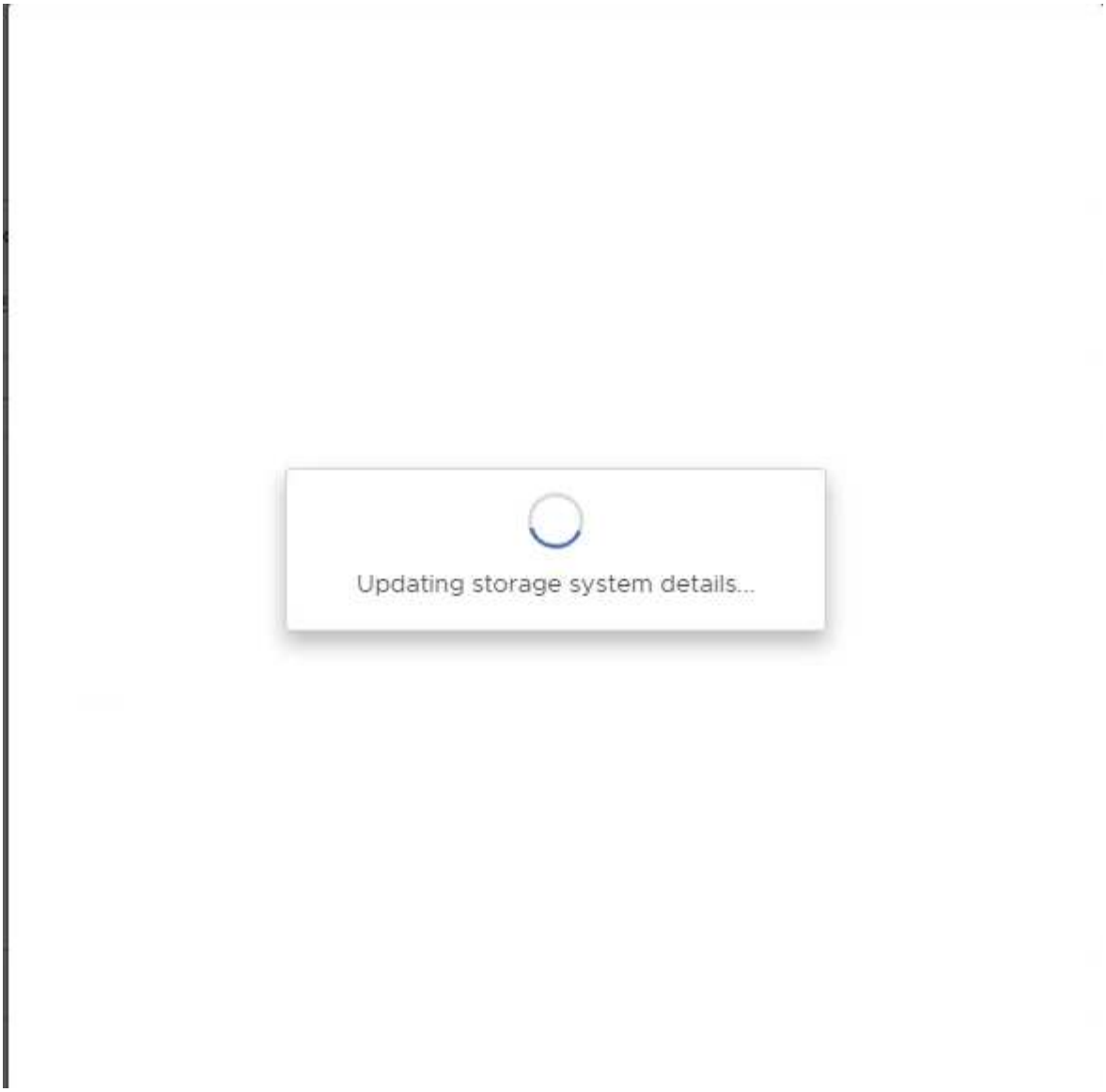



**Cluster Edit (Modifica cluster)**

Durante l'operazione di modifica del cluster, esistono due scenari:

- Se il certificato ONTAP scade, l'utente dovrà ottenere il nuovo certificato e caricarlo.
- Se il certificato OTV scade, l'utente può rigenerarlo selezionando la casella di controllo.
  - *Genera un nuovo certificato client per ONTAP.*


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK




## Certificato HTTPS degli strumenti ONTAP

Per impostazione predefinita, gli strumenti ONTAP utilizzano un certificato autofirmato creato automaticamente durante l'installazione per proteggere l'accesso HTTPS all'interfaccia utente Web. Gli strumenti ONTAP offrono le seguenti funzionalità:

1. Rigenerare il certificato HTTPS

Durante l'installazione degli strumenti ONTAP, viene installato un certificato CA HTTPS e il certificato viene memorizzato nell'archivio chiavi. L'utente può rigenerare il certificato HTTPS tramite la console principale.

È possibile accedere alle opzioni sopra riportate nella console *maint* accedendo a *'Configurazione applicazione' → 'rigenerare certificati'.*

## Banner di accesso

Il seguente banner di accesso viene visualizzato dopo che l'utente ha immesso un nome utente nel prompt di accesso. Tenere presente che SSH è disattivato per impostazione

predefinita e consente l'accesso una tantum solo se attivato dalla console VM.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Una volta completato l'accesso tramite il canale SSH, viene visualizzato il seguente testo:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

### Timeout di inattività

Per impedire l'accesso non autorizzato, viene impostato un timeout di inattività che disconnette automaticamente gli utenti inattivi per un determinato periodo di tempo durante l'utilizzo di risorse autorizzate. In questo modo, solo gli utenti autorizzati possono accedere alle risorse e mantenere la sicurezza.

- Per impostazione predefinita, le sessioni del client vSphere si chiudono dopo 120 minuti di inattività, richiedendo all'utente di accedere nuovamente per riprendere a utilizzare il client. È possibile modificare il valore di timeout modificando il file webclient.properties. È possibile configurare il timeout del client vSphere "Configurare il valore di timeout del client vSphere"
- Gli strumenti ONTAP hanno un tempo di disconnessione della sessione Web-cli di 30 minuti.

### Numero massimo di richieste simultanee per utente (protezione di rete :: Attacco DOS)

Per impostazione predefinita, il numero massimo di richieste simultanee per utente è 48. L'utente root negli strumenti ONTAP può modificare questo valore in base ai requisiti del proprio ambiente. **Questo valore non deve essere impostato su un valore molto alto in quanto fornisce un meccanismo contro gli attacchi DOS (Denial of Service).**

Gli utenti possono modificare il numero massimo di sessioni simultanee e altri parametri supportati nel file ***/opt/netapp/vscserver/etc/dosfilterParams.json***.

Possiamo configurare il filtro con i seguenti parametri :

- ***delayMS***: Il ritardo in millisecondi dato a tutte le richieste oltre il limite di velocità prima che vengano prese in considerazione. Dare -1 per respingere la richiesta.
- ***throttleMS***: Per quanto tempo attendere il semaforo in modalità asincrona.
- ***maxRequestMS***: Per quanto tempo consentire l'esecuzione di questa richiesta.
- ***ipWhitelist***: Un elenco separato da virgole di indirizzi IP che non saranno limitati dalla velocità. (Possono essere indirizzi IP vCenter, ESXi e SRA)
- ***maxRequestsPerSec***: Il numero massimo di richieste da una connessione al secondo.

**Valori predefiniti nel file *dosfilterParams*:**

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

## Network Time Protocol (NTP) Configuration (Configurazione NTP)

A volte, possono verificarsi problemi di protezione dovuti a discrepanze nelle configurazioni dell'ora di rete. È importante assicurarsi che tutti i dispositivi all'interno di una rete dispongano di impostazioni dell'ora precise per evitare tali problemi.

#### Virtual appliance

È possibile configurare i server NTP dalla console di manutenzione dell'appliance virtuale. Gli utenti possono aggiungere i dettagli del server NTP in *System Configuration* ⇒ *Add new NTP Server* option

Per impostazione predefinita, il servizio per NTP è ntpd. Si tratta di un servizio legacy che in alcuni casi non funziona bene per le macchine virtuali.

#### Debian

Su Debian, l'utente può accedere al file /etc/ntp.conf per i dettagli del server ntp.

## Criteri password

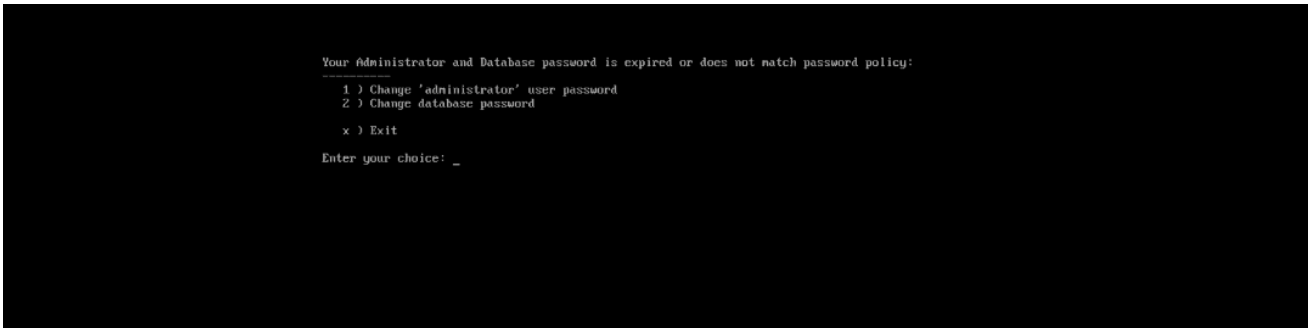
Gli utenti che distribuiscono gli strumenti ONTAP per la prima volta o che eseguono l'aggiornamento alla versione 9,12 o successiva dovranno seguire il criterio password complessa sia per gli utenti dell'amministratore che per quelli del database. Durante il processo di distribuzione, ai nuovi utenti verrà richiesto di immettere le password. Per gli utenti di brownfield che effettuano l'aggiornamento alla versione 9,12 o successiva, l'opzione per seguire il criterio password complessa sarà disponibile nella console di manutenzione.

- Una volta che l'utente accede alla console principale, le password verranno controllate in base al set di regole complesso e, se risulta non essere seguite, all'utente verrà chiesto di reimpostare lo stesso.
- La validità predefinita della password è di 90 giorni e dopo 75 giorni l'utente inizierà a ricevere la notifica di

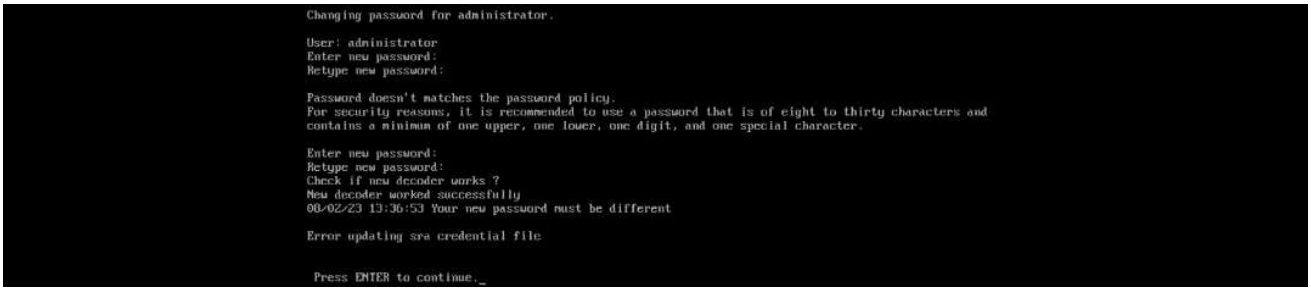
modifica della password.

- È necessario impostare una nuova password ad ogni ciclo; il sistema non utilizzerà l'ultima password come nuova password.
- Ogni volta che un utente accede alla console principale, prima di caricare il menu principale controlla i criteri delle password, come le schermate seguenti:


- Se non viene rilevato seguendo il criterio password o la relativa configurazione di aggiornamento da ONTAP Tools 9,11 o precedenti. L'utente visualizzerà quindi la seguente schermata per reimpostare la password:




- Se l'utente tenta di impostare una password debole o restituisce l'ultima password, viene visualizzato il seguente errore:



## Informazioni sul copyright



## Informazioni sul marchio commerciale