VMware

Enterprise applications

NetApp
January 12, 2026

Sommario

VMware

VMware vSphere con ONTAP

VMware vSphere con ONTAP

ONTAP è stata una soluzione storage leader per VMware vSphere e, più di recente, per gli ambienti Cloud Foundation dalla sua introduzione nel moderno data center nel 2002. Continua a introdurre funzionalità innovative che semplificano la gestione e riducono i costi.

In questo documento viene presentata la soluzione ONTAP per vSphere, che mette in evidenza le più recenti informazioni sui prodotti e le Best practice per semplificare la distribuzione, 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 (IMT)" e "Guida alla compatibilità VMware" per i dettagli relativi a versioni specifiche.

Perché scegliere ONTAP per VMware vSphere?

I clienti scelgono con fiducia ONTAP per vSphere sia per le soluzioni di storage SAN che NAS. La nuova architettura di storage disaggregato semplificata, presente negli ultimi All SAN Array, offre un'esperienza semplificata familiare agli amministratori di storage SAN, pur mantenendo la maggior parte delle integrazioni e delle funzionalità dei sistemi ONTAP tradizionali. I sistemi ONTAP forniscono un'eccezionale protezione snapshot e solidi strumenti di gestione. Trasferendo le funzioni su un archivio dedicato, ONTAP massimizza le risorse host, riduce i costi e mantiene prestazioni ottimali. Inoltre, i carichi di lavoro possono essere facilmente migrati tramite Storage vMotion su VMFS, NFS o vVols.

I vantaggi dell'utilizzo di 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 per l’hardware host e il software VMware. Puoi anche proteggere i tuoi dati a un costo inferiore mantenendo prestazioni elevate e costanti. Poiché i carichi di lavoro virtualizzati sono mobili, è possibile esplorare diversi approcci utilizzando Storage vMotion per spostare le VM tra datastore VMFS, NFS o vVols , tutti sullo stesso sistema di storage.

Ecco i fattori chiave che i clienti apprezzano oggi:

- **Archiviazione unificata.** I sistemi che eseguono ONTAP sono unificati in diversi modi significativi. Originariamente, questo approccio si riferiva sia ai protocolli NAS che SAN e ONTAP continua a essere una piattaforma leader per SAN, oltre alla sua forza originaria in NAS. Nel mondo vSphere, questo approccio potrebbe anche significare un sistema unificato per l’infrastruttura desktop virtuale (VDI) insieme all’infrastruttura server virtuale (VSI). I sistemi che eseguono ONTAP sono in genere meno costosi per VSI rispetto ai tradizionali array aziendali e tuttavia dispongono di funzionalità avanzate di efficienza di archiviazione per gestire VDI nello stesso sistema. ONTAP unifica inoltre una varietà di supporti di archiviazione, dagli SSD ai SATA, e può estenderli facilmente al cloud. Non è necessario acquistare un sistema operativo di archiviazione per le prestazioni, un altro per gli archivi e un altro ancora per il cloud. ONTAP li collega tutti insieme.
- **All SAN Array (ASA).** I sistemi ONTAP ASA più recenti (a partire dai modelli A1K, A90, A70, A50, A30 e A20) sono costruiti su una nuova architettura dello storage in grado di eliminare il tradizionale paradigma dello storage ONTAP per la gestione degli aggregati e dei volumi. Poiché non ci sono condivisioni di file system, non c’è bisogno di volumi! Tutto lo storage collegato a una coppia ha viene trattato come una SAZ (Storage Availability zone) comune, all’interno della quale i LUN e i namespace NVMe vengono forniti come "Storage Units" (SUS). I più recenti sistemi ASA sono progettati per essere semplici da gestire e con un’esperienza familiare per gli amministratori dello storage SAN. Questa nuova architettura è ideale per gli ambienti vSphere, poiché consente una facile gestione delle risorse storage e fornisce un’esperienza semplificata per gli amministratori dello storage SAN. L’architettura ASA supporta anche la più recente tecnologia NVMe over Fabrics (NVMe-of), che offre performance e scalabilità ancora superiori per i workload vSphere.
- **Tecnologia Snapshot.** ONTAP è stata la prima azienda a offrire la tecnologia Snapshot per la protezione dei dati, che rimane la più avanzata del settore. Questo approccio efficiente in termini di spazio alla data Protection è stato esteso per supportare le API VMware vSphere per l’integrazione degli array (VAAI). Questa integrazione ti consente di sfruttare le funzionalità snapshot di ONTAP per le operazioni di backup e ripristino, riducendo l’impatto sul tuo ambiente di produzione. Questo approccio consente inoltre di utilizzare le snapshot per un rapido recovery delle macchine virtuali, riducendo tempo e lavoro necessari per il ripristino dei dati. Inoltre, la tecnologia snapshot di ONTAP è integrata con le soluzioni VLSR (Live Site Recovery Manager) di VMware, in precedenza Site Recovery Manager [SRM], per fornire una strategia di protezione dei dati completa per il vostro ambiente virtualizzato.
- **Gestione basata su policy di archiviazione e volumi virtuali.** NetApp è stata uno dei primi partner di progettazione di VMware nello sviluppo di vSphere Virtual Volumes (vVols), fornendo input architettonici e supporto iniziale per vVols e VMware vSphere API for Storage Awareness (VASA). Questo approccio non solo ha introdotto la gestione granulare dello storage delle VM in VMFS, ma ha anche supportato l’automazione del provisioning dello storage tramite una gestione basata su policy di storage. Questo approccio consente agli architetti di storage di progettare pool di storage con diverse funzionalità che possono essere facilmente utilizzate dagli amministratori delle VM. ONTAP è leader nel settore dello storage in termini di scala vVol, supportando centinaia di migliaia di vVols in un singolo cluster, mentre i fornitori di array aziendali e di array flash più piccoli supportano solo alcune migliaia vVols per array. NetApp sta inoltre guidando l’evoluzione della gestione granulare delle VM con le sue funzionalità future.
- **Efficienza di archiviazione.** Sebbene NetApp sia stata la prima a fornire la deduplicazione per i carichi di lavoro di produzione, questa innovazione non è stata né la prima né l’ultima in questo settore. Tutto è iniziato con gli snapshot, un meccanismo di protezione dei dati efficiente in termini di spazio e senza effetti sulle prestazioni, insieme alla tecnologia FlexClone per creare istantaneamente copie di lettura/scrittura delle VM per uso in produzione e backup. NetApp ha continuato a fornire funzionalità inline, tra cui

deduplicazione, compressione e deduplicazione a blocchi zero, per ottenere il massimo spazio di archiviazione dai costosi SSD. ONTAP ha inoltre aggiunto la possibilità di impacchettare operazioni di I/O e file più piccoli in un blocco di disco utilizzando la compattazione. La combinazione di queste funzionalità ha portato i clienti a ottenere risparmi fino a 5:1 per VSI e fino a 30:1 per VDI. La nuova generazione di sistemi ONTAP include anche la compressione e la deduplicazione accelerate dall'hardware, che possono migliorare ulteriormente l'efficienza di archiviazione e ridurre i costi. Questo approccio consente di archiviare più dati in meno spazio, riducendo il costo complessivo di archiviazione e migliorando le prestazioni. NetApp è così sicura delle sue capacità di efficienza di storage che offre un collegamento: https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf [Garanzia di efficienza^].

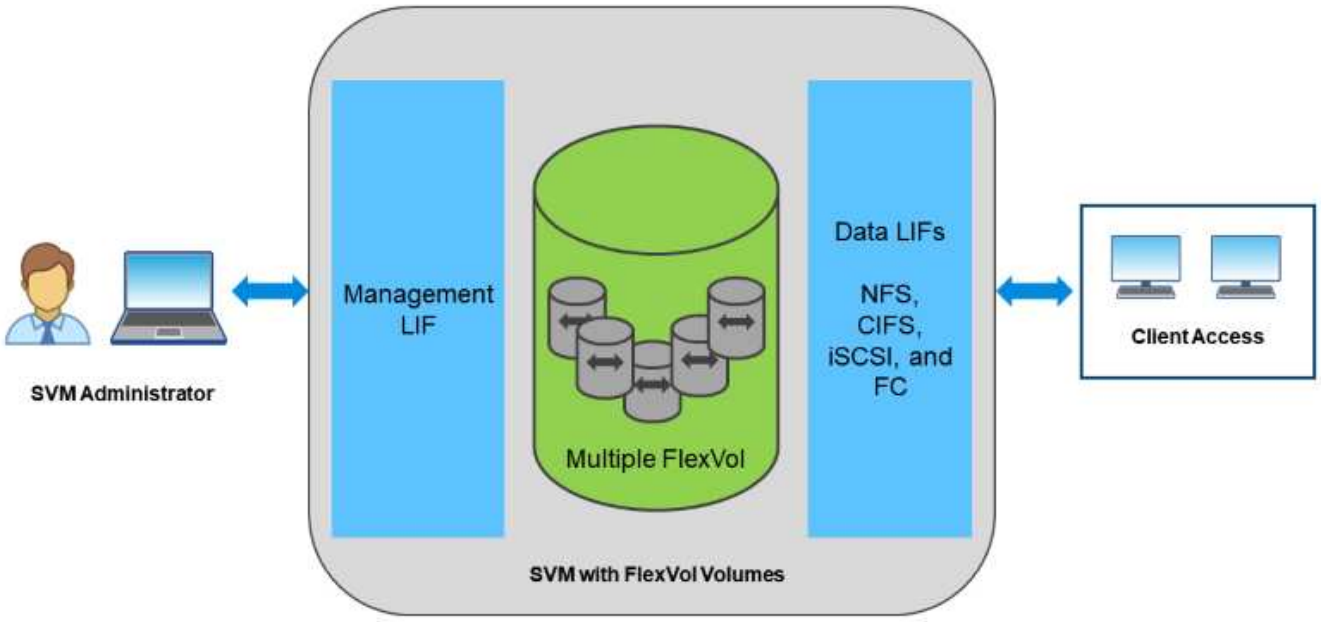
- **Multi-tenancy.** ONTAP è da tempo leader nel multitenancy, consentendo di creare più macchine virtuali di storage (SVM) su un singolo cluster. Questo approccio consente di isolare i carichi di lavoro e di fornire diversi livelli di servizio a diversi tenant, rendendolo ideale per i fornitori di servizi e le grandi aziende. L'ultima generazione di sistemi ONTAP include anche il supporto per la gestione della capacità degli inquilini. Questa funzionalità consente di impostare limiti di capacità per ciascun tenant, assicurando che nessun tenant possa consumare tutte le risorse disponibili. Questo approccio contribuisce a garantire che tutti gli inquilini ricevano il livello di servizio che si aspettano, garantendo al contempo un elevato livello di sicurezza e isolamento tra gli inquilini. Inoltre, le funzionalità multi-tenancy di ONTAP sono integrate con la piattaforma vSphere di VMware, consentendo di gestire e monitorare facilmente l'ambiente virtualizzato tramite "Strumenti ONTAP per VMware vSphere" E "Informazioni sull'infrastruttura dati" .
- **Cloud ibrido.** Che vengano utilizzate per un cloud privato on-premise, un'infrastruttura cloud pubblica o un cloud ibrido che combina il meglio di entrambi, le soluzioni ONTAP ti aiutano a creare il tuo data fabric per semplificare e ottimizzare la gestione dei dati. Inizia con sistemi all-flash ad alte prestazioni, quindi abbinali a sistemi di archiviazione su disco o cloud per la protezione dei dati e il cloud computing. Scegli tra Azure, AWS, IBM o Google Cloud per ottimizzare i costi ed evitare vincoli. Sfrutta il supporto avanzato per OpenStack e le tecnologie container in base alle tue esigenze. NetApp offre inoltre strumenti di backup basati su cloud (SnapMirror Cloud, Cloud Backup Service e Cloud Sync) e di archiviazione e suddivisione in livelli di storage (FabricPool) per ONTAP , per contribuire a 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

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 "Panoramica della configurazione S3". Il termine storage unificato si è evoluto per indicare un approccio unificato alla gestione dello storage, inclusa la capacità di gestire tutte le risorse di storage da una singola interfaccia. Tra cui la possibilità di gestire le risorse di storage sia on-premise che nel cloud, i più recenti sistemi All SAN Array (ASA) e la possibilità di gestire più sistemi storage da una singola interfaccia.

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 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 ONTAP sono di solito meno costosi per VSI rispetto agli array aziendali tradizionali e allo stesso tempo dispongono di funzionalità avanzate per l'efficienza dello storage per gestire l'infrastruttura di desktop virtuale 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 fornisce diversi strumenti software standalone compatibili con i sistemi tradizionali ONTAP e ASA, integrando vSphere per gestire in modo efficace il tuo ambiente virtualizzato.

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

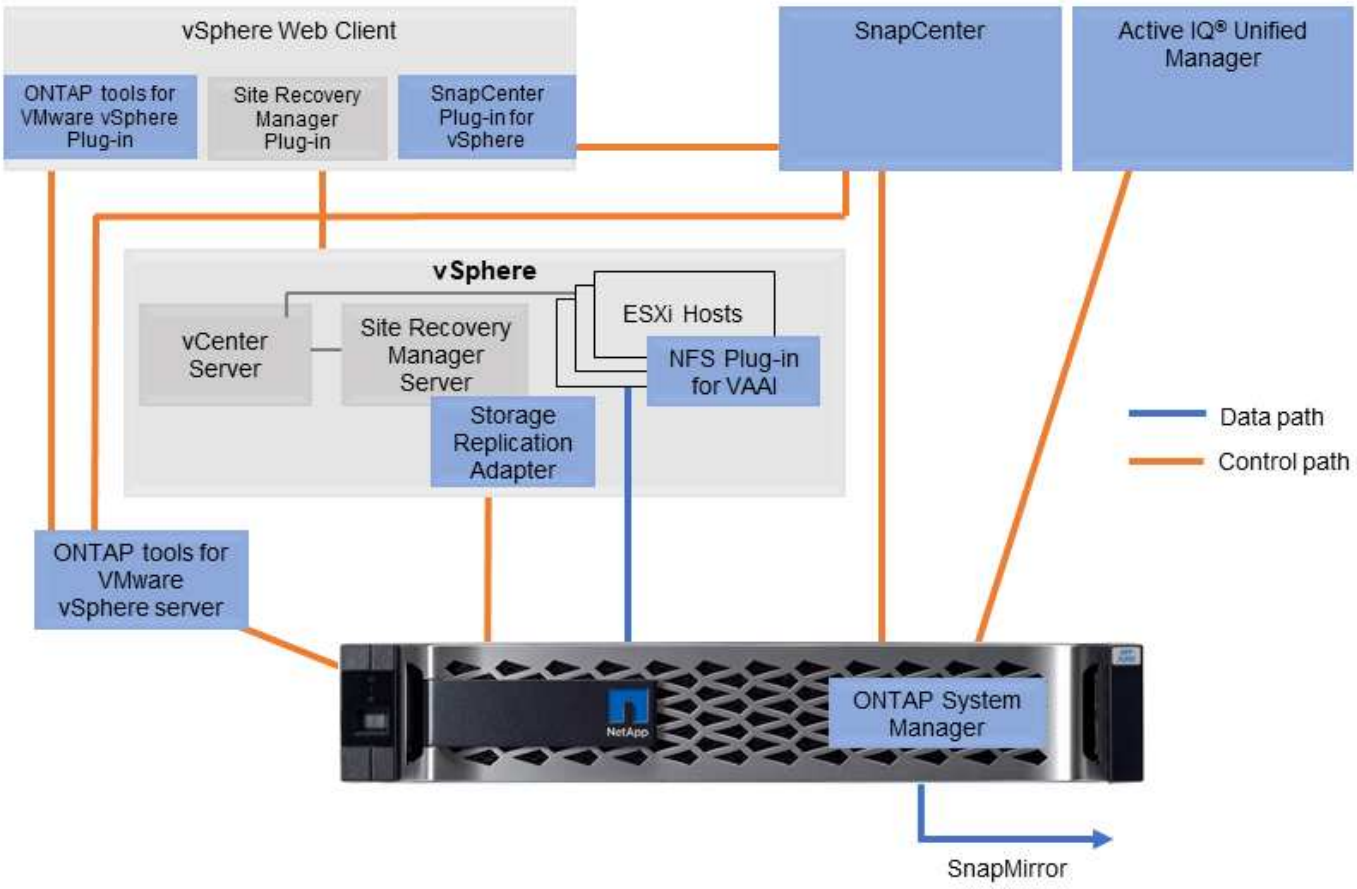
Strumenti ONTAP per VMware vSphere

"Strumenti ONTAP per VMware vSphere" È un set di tool 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 strumenti ONTAP come Best practice quando si utilizza vSphere con sistemi che eseguono 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.

- **Estensioni dell'interfaccia utente vCenter.** Le estensioni dell'interfaccia utente dei tool di ONTAP semplificano il lavoro dei team operativi e degli amministratori vCenter incorporando menu sensibili al contesto e di facile utilizzo per la gestione di host e storage, portlet informativi e funzionalità di alerting native direttamente nell'interfaccia utente di vCenter per workflow ottimizzati.
- **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.
- **Adattatore di replicazione dell'archiviazione.** SRA viene utilizzato insieme a VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) per gestire la replica dei dati tra siti di produzione e di disaster recovery utilizzando SnapMirror per la replica basata su array. Può automatizzare l'attività di failover in caso di disastro e può aiutare a testare le repliche DR in modo non distruttivo per garantire l'affidabilità della soluzione DR.

La figura seguente mostra gli strumenti ONTAP per vSphere.



Plug-in SnapCenter per VMware vSphere

IL "Plug-in SnapCenter per VMware vSphere" è un plug-in per vCenter Server che consente di gestire backup e ripristini di macchine virtuali (VM) e datastore. Fornisce un'unica interfaccia per la gestione di backup, ripristini e cloni di VM e datastore su più sistemi ONTAP . SnapCenter supporta la replica e il ripristino da siti secondari tramite SnapMirror. Le versioni più recenti supportano anche SnapMirror su cloud (S3), snapshot Tamperproof, SnapLock e SnapMirror ActiveSync. Il plug-in SnapCenter per VMware vSphere può essere integrato con i plug-in dell'applicazione SnapCenter per fornire backup coerenti con l'applicazione.

Plug-in NFS per VMware VAAI

```
https://mysupport.netapp.com/site/products/all/details/nfsplugin-vmware-vaai/about-tab["Plug-in NFS NetApp per VMware VAAI"]È un plug-in per gli host ESXi che consente loro di utilizzare le funzionalità VAAI con i datastore 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).
```

Opzioni software premium

NetApp mette a disposizione i seguenti prodotti software premium. Non sono inclusi nella licenza ONTAP One e devono essere acquistati separatamente.

- "NetApp Disaster Recovery"per VMware vSphere. Si tratta di un servizio basato su cloud che fornisce ripristino di emergenza e backup per ambienti VMware. Può essere utilizzato con o senza SnapCenter e supporta il DR on-prem su on-prem tramite SAN o NAS e on-prem da/verso il cloud tramite NFS, ove supportato.
- "Informazioni sull'infrastruttura dati (DII)". Si tratta di un servizio basato su cloud che fornisce monitoraggio e analisi per gli ambienti VMware. Supporta altri fornitori di storage in ambienti di storage eterogenei, nonché più fornitori di switch e altri hypervisor. DII fornisce informazioni complete e complete sulle prestazioni, la capacità e lo stato di salute del tuo ambiente VMware.

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

Annunciato per la prima volta nel 2012, NetApp è stato un primo partner di progettazione di VMware nello sviluppo di VMware vSphere APIs for Storage Awareness (VASA), le fondamenta della gestione basata su criteri storage (SPBM, Storage Policy Based Management) con array storage Enterprise. Questo approccio offriva una gestione granulare dello storage delle macchine virtuali limitata allo storage VMFS e NFS.

In qualità di partner di progettazione tecnologica, NetApp ha fornito un input architetturale e nel 2015 ha annunciato il supporto per vVol. Questa nuova tecnologia ha ora consentito l'automazione del provisioning dello storage granulare delle macchine virtuali e realmente nativo degli array tramite SPBM.

Volumi virtuali (vVol)

I vVol sono una rivoluzionaria architettura di storage che consente la gestione granulare dello storage delle macchine virtuali, consentendo la gestione dello storage non solo in base alle macchine virtuali (compresi i metadati delle macchine virtuali) ma anche in base ai VMDK. I vVol sono un componente chiave della strategia SDDC (Software Defined Data Center) che costituisce la base di VMware Cloud Foundation (VCF), fornendo un'architettura di storage più efficiente e scalabile per gli ambienti virtualizzati.

I vVol consentono alle macchine virtuali di utilizzare lo storage per ogni macchina virtuale, perché ogni oggetto storage delle macchine virtuali è un'entità univoca in NetApp ONTAP. Con i sistemi ASA R2, che non richiedono più la gestione dei volumi, questo significa che ogni oggetto storage delle macchine virtuali è un'unica unità di storage (su) sull'array e può essere controllato in modo indipendente. Ciò consente la creazione di policy di storage che possono essere applicate a singole macchine virtuali o VMDK (e quindi include un SUS duale), fornendo un controllo granulare sui servizi storage quali performance, disponibilità e protezione dei dati.

Gestione basata su criteri storage (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 storage architect di progettare pool di storage con funzionalità differenti. Questi pool possono essere facilmente utilizzati dagli amministratori VM. Gli amministratori possono quindi abbinare i requisiti dei carichi di lavoro delle macchine virtuali ai pool di storage di cui è stato eseguito il provisioning. Questo approccio semplifica la gestione dello storage e permette un utilizzo più efficiente delle risorse di storage.

SPBM è un componente chiave di vVol, che fornisce un framework basato su criteri per la gestione dei servizi storage. Le policy vengono create dagli amministratori di vSphere utilizzando regole e funzionalità esposte dal

provider VASA (VP) del vendor. È possibile creare policy per diversi servizi di storage, quali performance, disponibilità e protezione dei dati. È possibile assegnare le policy a singole macchine virtuali o VMDK per un controllo granulare sui servizi storage.

NetApp ONTAP e vVol

NetApp ONTAP è leader nel settore dello storage nella scalabilità dei vVol, supportando centinaia di migliaia di vVol in un singolo cluster*. Al contrario, gli array Enterprise e i vendor di flash array più piccoli supportano fino a diverse migliaia di vVol per array. ONTAP offre una soluzione storage scalabile ed efficiente per ambienti VMware vSphere, supportando i vVol con un ricco set di servizi storage, tra cui deduplica dei dati, compressione, thin provisioning e protezione dei dati. SPBM consente un'integrazione perfetta con gli ambienti VMware vSphere.

In precedenza abbiamo indicato agli amministratori delle macchine virtuali la possibilità di consumare capacità come pool di storage. Ciò avviene mediante l'utilizzo di container di storage rappresentati in vSphere come datastore logici.

I container storage vengono creati dagli amministratori dello storage e utilizzati per raggruppare le risorse storage che possono essere consumate dagli amministratori delle macchine virtuali. I container storage possono essere creati in maniera differente a seconda del tipo di sistema ONTAP che stai utilizzando. Con i cluster tradizionali di ONTAP 9, ai container viene assegnato uno o più volumi FlexVol di supporto che formano insieme il pool di storage. Con i sistemi ASA R2, l'intero cluster è il pool di storage.

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

*A seconda della piattaforma e del protocollo

Datastore e protocolli

Panoramica delle funzionalità del datastore e del protocollo di vSphere

Per collegare VMware vSphere ai datastore su un sistema che esegue ONTAP sono utilizzati sei protocolli:

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

FCP, NVMe/FC, NVMe/TCP e iSCSI sono protocolli a blocchi che utilizzano il VMFS (vSphere Virtual Machine file System) per memorizzare le VM nei LUN di ONTAP o negli namespace NVMe contenuti in un ONTAP FlexVol volume. 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 il "Strumento

VMware Configuration Maximums" per le release specifiche di vSphere per confermare i limiti specifici.

Funzionalità	FC	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 connessioni NFS per host (interessate da nconnect e trunking di sessione) 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	300 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	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
Software di backup abilitato per VADP (VMware vStorage APIs for Data Protection)	Sì	Sì	Sì	Sì

Capacità/funzionalità	FC	ISCSI	NVMe-of	NFS
Microsoft Cluster Service (MSCS) o clustering di failover all'interno di una macchina virtuale	Sì	Sì [1]	Sì [1]	Non supportato
Tolleranza agli errori	Sì	Sì	Sì	Sì
Gestione ripristino sito live/ripristino sito	Sì	Sì	No [2]	V3 solo [2]
Macchine virtuali con thin provisioning (dischi virtuali)	Sì	Sì	Sì	Sì Si tratta dell'impostazione predefinita per tutte le macchine virtuali su NFS quando non si utilizza VAAI.
Multipathing nativo di VMware	Sì	Sì	Sì	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	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	Sì	Sì
Monitoraggio e configurazione dell'host con gli strumenti ONTAP per VMware vSphere	Sì	Sì	Sì	Sì
Provisioning con gli strumenti ONTAP per VMware vSphere	Sì	Sì	Sì	Sì

La tabella seguente elenca le funzionalità di backup supportate.

Funzionalità	FC	ISCSI	NVMe-of	NFS
Snapshot ONTAP	Sì	Sì	Sì	Sì
SRM supportato da backup replicati	Sì	Sì	No [2]	V3 solo [2]
Volume SnapMirror	Sì	Sì	Sì	Sì
Accesso all'immagine VMDK	Software di backup compatibile con SnapCenter e VADP	Software di backup compatibile con SnapCenter e VADP	Software di backup compatibile con SnapCenter e VADP	Software di backup abilitato per SnapCenter e VADP, client vSphere e browser del datastore del client web vSphere
Accesso a livello di file VMDK	Software di backup compatibile con SnapCenter e VADP, solo Windows	Software di backup compatibile con SnapCenter e VADP, solo Windows	Software di backup compatibile con SnapCenter e VADP, solo Windows	Software di backup SnapCenter e VADP e applicazioni di terze parti
Granularità NDMP	Datastore	Datastore	Datastore	Datastore o macchina virtuale

[1] **NetApp consiglia** l'utilizzo di iSCSI in-guest per i cluster Microsoft piuttosto che VMDK abilitati per il multi-writer in un datastore VMFS. Questo approccio è pienamente supportato da Microsoft e VMware, offre una grande flessibilità con ONTAP (da SnapMirror ai sistemi ONTAP on-premise o nel cloud), è semplice da configurare e automatizzare e può essere protetto con SnapCenter. VSphere 7 aggiunge una nuova opzione VMDK in cluster. Si tratta di una configurazione diversa da VMDK abilitati per multi-writer, che richiede un datastore VMFS 6 con supporto VMDK per cluster abilitato. Sono previste altre restrizioni. Per le linee guida sulla configurazione, consultare la documentazione di VMware"Configurazione per il clustering di failover di Windows Server".

[2] i datastore che utilizzano NVMe-of e NFS v4,1 richiedono la replica vSphere. La replica basata su array per NFS v4,1 non è attualmente supportata da SRM. La replica basata su array con NVMe-of non è attualmente supportata dai tool ONTAP per VMware vSphere Storage Replication Adapter (SRA).

Selezione di un protocollo di storage

I sistemi che eseguono ONTAP supportano tutti i principali protocolli di storage, consentendo ai clienti di scegliere il miglior ambiente per il proprio ambiente, a seconda dell'infrastruttura di rete esistente e pianificata e delle competenze dello staff. In passato, i test di NetApp hanno generalmente mostrato una piccola differenza tra i protocolli in esecuzione a velocità di linea simili e il numero di connessioni. Tuttavia, la tecnologia NVMe-of (NVMe/TCP e NVMe/FC) mostra guadagni notevoli in termini di IOPS, riduzione della latenza e riduzione fino al 50% o più del consumo della CPU host da parte dell'io storage. Dall'altra parte dello spettro, NFS offre la massima flessibilità e facilità di gestione, in particolare per un gran numero di macchine virtuali. Tutti questi protocolli possono essere utilizzati e gestiti con i tool ONTAP per VMware vSphere, che offre una semplice interfaccia per creare e gestire datastore.

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

- **Ambiente operativo corrente.** Sebbene i team IT siano generalmente esperti nella gestione dell'infrastruttura IP Ethernet, non tutti sono esperti nella gestione di un fabric FC SAN. 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, è necessario eseguire diverse operazioni, tra cui la crescita di un LUN, la ripetizione della scansione per rilevare le nuove dimensioni e l'espansione del file system. Sebbene sia possibile espandere un LUN, non lo è la dimensione di un LUN. NFS consente un facile dimensionamento in alto o in basso e questo ridimensionamento può essere automatizzato dal sistema storage. La SAN offre il recupero dello spazio tramite i comandi guest OS UNSPAKE/TRIM/UNMAP, consentendo di restituire all'array spazio dai file eliminati. Questo tipo di recupero di spazio non è possibile 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 utilizzano gli strumenti ONTAP per il provisioning dei datastore per vSphere (elencati nella sezione "Host ESXi consigliato e altre impostazioni ONTAP"), di seguito sono riportate 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 ampio può trarre vantaggio dall'efficienza dello storage e offrire vantaggi operativi, prendi in considerazione l'utilizzo di almeno quattro datastore (volumi FlexVol) per nodo per memorizzare le macchine virtuali su un singolo controller del ONTAP, in modo da ottenere le massime performance 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** l'utilizzo di 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.
- 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 300 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. I tool ONTAP per la procedura guidata di provisioning del datastore di VMware vSphere utilizzano il dimensionamento automatico per impostazione predefinita per i nuovi

datastore. 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, i datastore VMFS possono essere configurati con LUN o namespace NVMe (chiamati anche unità storage nei nuovi sistemi ASA) accessibili tramite FC, iSCSI, NVMe/FC o NVMe/TCP. VMFS consente l'accesso simultaneo ai datastore 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). Le dimensioni massime del LUN del ONTAP sono di 128TB GB su sistemi AFF, ASA e FAS. NetApp consiglia sempre di utilizzare una singola LUN di grandi dimensioni per ciascun datastore, invece di provare a utilizzare estensioni. Come per NFS, prendere in considerazione l'utilizzo di datastore multipli (volumi o unità storage) per massimizzare le performance su un singolo controller del 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 stai utilizzando un vecchio sistema operativo che potrebbe richiedere un allineamento, cerca nella Knowledge base di supporto NetApp gli articoli che utilizzano "allineamento VM" o richiedi una copia del documento TR-3747 a un contatto commerciale o di un partner 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. Considerare i file system guest-owned come NFS, SMB, NVMe/TCP o iSCSI gestiti dal guest. Per indicazioni specifiche sulle applicazioni, consulta i report tecnici NetApp relativi alla tua applicazione. Ad esempio, "Database Oracle su ONTAP" ha 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. Inoltre, una

volta che le VM sono sul cluster NetApp, storage vMotion può sfruttare gli offload VAAI per spostare le VM tra datastore nel cluster, senza richiedere una copia basata su host. Tuttavia, NFS non consente di scaricare lo storage vMotion di macchine virtuali alimentate, ma VMFS.

- 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. Per ulteriori informazioni, vedere "Migrazione dei database Oracle sui sistemi di storage ONTAP" . 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 quando si utilizza vSphere con sistemi che eseguono ONTAP è quella di installare e utilizzare i tool ONTAP per il plug-in VMware vSphere (precedentemente noto come Virtual Storage Console). Questo plug-in vCenter semplifica la gestione dello storage, aumenta la disponibilità e riduce i costi dello storage e l'overhead operativo, sia che si utilizzino SAN o NAS, su ASA, AFF, FAS o persino ONTAP Select (una versione software-defined ONTAP che viene eseguita in una macchina virtuale VMware o KVM). 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.

> Nei cluster vSphere basati su immagini, sarà comunque necessario aggiungere il plug-in NFS all'immagine in modo che non si discostino dalla conformità quando viene installato con gli strumenti ONTAP.

I tool ONTAP sono anche l'interfaccia di gestione per molte funzioni del provider VASA per ONTAP, supportando una gestione basata su policy di storage con vVol.

In generale, **NetApp consiglia** di utilizzare gli strumenti ONTAP per l'interfaccia di VMware vSphere all'interno di vCenter per effettuare il provisioning dei datastore tradizionali e vVol per assicurarsi che vengano seguite le Best practice.

Rete generale

La configurazione delle impostazioni di rete quando si utilizza vSphere con sistemi che eseguono 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 solo il controllo di flusso di rete sulle porte di cluster Interconnect in 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 connessi a reti di storage Ethernet, **NetApp consiglia** di configurare le porte Ethernet a cui questi sistemi si connettono come porte edge Rapid Spanning Tree Protocol (RSTP) o utilizzando la funzione Cisco PortFast. **NetApp consiglia** di abilitare la funzione di trunk PortFast Spanning-Tree in ambienti che utilizzano la funzione PortFast Cisco e che dispongono di trunking VLAN 802,1Q abilitato al server ESXi o agli array di storage ONTAP.
- **NetApp consiglia** le seguenti procedure consigliate 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).

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

In vSphere, esistono quattro modi per utilizzare i dispositivi di storage a blocchi:

- Con datastore VMFS
- Con RDM (raw device mapping)
- Come LUN connessa a iSCSI o namespace connesso a NVMe/TCP, accessibile e controllato da un iniziatore software da un sistema operativo guest di macchine virtuali
- Come datastore vVols

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.

Le estensioni sono un concetto di storage vSphere tramite cui è possibile "unire" diverse LUN per creare un singolo datastore più grande. Non utilizzare mai estensioni per raggiungere le dimensioni desiderate del datastore. Una singola LUN è la Best practice per un datastore VMFS.

VSphere include il supporto integrato per diversi percorsi verso i dispositivi storage. VSphere è in grado di rilevare il tipo di dispositivo storage per i sistemi storage supportati e di configurare automaticamente lo stack multipath per supportare le funzionalità del sistema storage in uso, la sovranità del protocollo utilizzato o se si utilizza ASA, AFF, FAS o Software Defined ONTAP.

Sia vSphere che ONTAP supportano l'Asymmetric Logical Unit Access (ALUA) per stabilire percorsi Active/ottimizzati e Active/non ottimizzati per Fibre Channel e iSCSI e l'Asymmetric Namespace (ANA) per gli spazi dei nomi NVMe utilizzando NVMe/FC e NVMe/TCP. In ONTAP, un percorso ALUA o ANA ottimizzato segue un percorso diretto dei dati, utilizzando una porta di destinazione sul nodo che ospita la LUN o il namespace a cui si accede. ALUA/ANA è attivato per impostazione predefinita sia in vSphere che in ONTAP. Il software multipathing di vSphere riconosce il cluster ONTAP come ALUA o ANA e utilizza il plug-in nativo appropriato con la policy di bilanciamento del carico round robin.

Con i sistemi ASA di NetApp, i LUN e gli spazi dei nomi vengono presentati agli host ESXi con percorso simmetrico. Ciò significa che tutti i percorsi sono attivi e ottimizzati. Il software multipathing di vSphere riconosce il sistema ASA come simmetrico e utilizza il plug-in nativo appropriato con la policy di bilanciamento del carico round robin.

Per le impostazioni di multipathing ottimizzate, consultare la sezione"Host ESXi consigliato e altre impostazioni ONTAP".

ESXi non vede LUN, namespace o percorsi oltre i propri limiti. 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.

Fare riferimento alla "Strumento VMware Configuration Maximums" per i limiti supportati più aggiornati in ESXi.

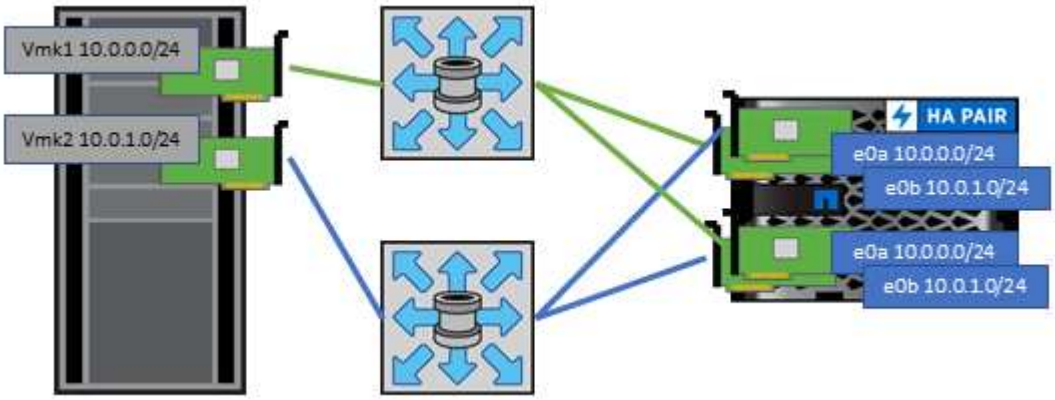
SLM limita i nodi che pubblicizzano i percorsi a una determinata LUN. È consigliabile utilizzare NetApp per almeno due LIF per nodo per SVM e SLM per limitare i percorsi pubblicizzati al nodo che ospita la LUN e il partner ha. Sebbene esistano altri percorsi, essi non vengono pubblicizzati per impostazione 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 le LUN create prima di Data ONTAP 8,3, applicare manualmente SLM eseguendo il comando per rimuovere i nodi di reporting LUN e limitare l'accesso LUN `lun mapping remove-reporting-nodes` al nodo proprietario LUN e al partner ha.

I protocolli a blocchi basati su SCSI (iSCSI, FC e FCoE) accedono ai LUN usando ID LUN, numeri di serie e nomi univoci. FC e FCoE utilizzano nomi mondiali (WWN e WWPN) e iSCSI utilizza nomi qualificati iSCSI (IQN) per stabilire percorsi basati su LUN per le mappature igroup filtrate da portset e SLM. I protocolli a blocchi basati su NVMe vengono gestiti assegnando un namespace con un ID namespace generato automaticamente a un sottosistema NVMe e mappando tale sottosistema al NVMe Qualified Name (NQN) degli host. Indipendentemente da FC o TCP, i namespace NVMe vengono mappati utilizzando l'NQN e non il WWPN o il WWNN. L'host crea quindi un controller definito dal software per il sottosistema mappato per accedere ai propri spazi dei nomi. Il percorso verso LUN e namespace all'interno di ONTAP non ha alcun senso per i protocolli a blocchi e non viene presentato in alcun modo nel 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.

Altre Best practice da prendere in considerazione:

- Verificare "Host ESXi consigliato e altre impostazioni ONTAP"le impostazioni consigliate da NetApp in collaborazione con VMware.
- 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

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 vantaggi in termini di facilità di utilizzo e di visibilità dell'efficienza dello storage, come menzionato nella "datastore"sezione.

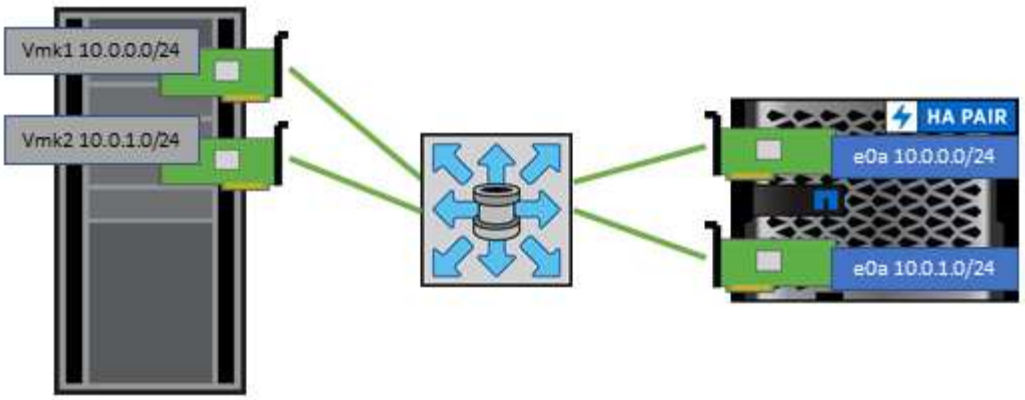
Quando si utilizza ONTAP NFS con vSphere, si consiglia di seguire le seguenti Best practice:

- Utilizza i tool ONTAP per VMware vSphere (la Best practice più importante):
  - Utilizza i tool di ONTAP per VMware vSphere per il provisioning dei datastore in quanto 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.
- 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).
- Se si utilizza fpolicy, assicurarsi di escludere i file .lck poiché vengono utilizzati da vSphere per il blocco ogni volta che una VM viene accesa.
- 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 e all'update 3 per NFS v4,1. 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. È possibile ottenere ulteriori informazioni sulla funzione nconnect e sul modo in cui migliora le prestazioni a "Funzione NFSv3 nconnect con NetApp e VMware".

  - Il valore massimo per nconnect in vSphere 8 è 4 e il valore predefinito è 1. Il limite massimo di valore in vSphere può essere aumentato in base all'host tramite impostazioni avanzate, tuttavia in genere non è necessario.
  - Per gli ambienti che richiedono prestazioni superiori a quelle consentite da una singola connessione TCP, si consiglia di utilizzare il valore 4.
  - Tenere presente che ESXi ha un limite di 256 connessioni NFS e ogni connessione nconnect conta per quel totale. Ad esempio, due datastore con nconnect=4 contano come otto connessioni totali.
  - È importante verificare l'impatto delle prestazioni di nconnect sull'ambiente prima di implementare cambiamenti su larga scala negli ambienti di produzione.
- 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 di matrice di interoperabilità NetApp" per i livelli di patch ESXi specifici richiesti per il supporto.
- Come menzionato in "impostazioni", se non si utilizza vSphere CSI per Kubernetes, è necessario

impostare il nuovo SyncInterval per "VMware KB 386364"

- Regole delle policy di esportazione NFS vengono utilizzate per controllare l'accesso dagli host vSphere. È possibile utilizzare un criterio con più volumi (datastore). Con NFS, 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 delle policy di esportazione con valori diversi per `-anon` e `-allow-suid` possono causare problemi di rilevamento SVM con gli strumenti ONTAP. Gli indirizzi IP devono essere un elenco separato da virgole senza spazi degli indirizzi della porta vmkernel che montano gli archivi dati. Ecco un esempio di regola dei criteri:
  - Access Protocol: nfs (che include sia nfs3 che nfs4)
  - Elenco di nomi host, indirizzi IP, netgroup o domini corrispondenti ai client: 192.168.42.21,192.168.42.22
  - Regola di accesso RO: Any
  - Regola di accesso RW: Qualsiasi
  - ID utente a cui sono mappati gli utenti anonimi: 65534
  - Tipi di protezione superutente: Qualsiasi
  - Honor setuid bits in SETATTR: True
  - Consenti la creazione di dispositivi: True
- Se si utilizza il plug-in NFS NetApp per VMware VAAI, è necessario impostare il protocollo come `nfs` al momento della creazione o della modifica della regola dei criteri di esportazione. Per il funzionamento dell'offload delle copie VAAI è necessario il protocollo NFSv4, specificando che il protocollo `nfs` include automaticamente le versioni NFSv3 e NFSv4. Questa operazione è necessaria anche se il tipo di datastore viene creato come NFS v3.
- 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:
  - Protocollo di accesso: nfs
  - Spec. Corrispondenza client: 192.168.42.21,192.168.42.22
  - 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)
- 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
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)

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 9,8-9,13 e al plug-in SnapCenter per VMware 4,4 e versioni successive, ha aggiunto il supporto per 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.

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 meccanismo di cloning FlexGroup mantenendo costantemente al caldo la cache dei cloni.

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 costituente viene quindi utilizzata per creare rapidamente un'istanza dei cloni delle macchine virtuali on-demand.

Per attivare l'offload delle copie ottimizzato per FlexGroup, fare riferimento alla sezione "Come configurare i volumi 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 Volumes con VAAI, fai 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 delle altre VM dello stesso datastore per quell'host. 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 dell'Interoperability Matrix Tool (IMT) 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 "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 carichi di lavoro di cloning al momento di decidere di utilizzare volumi 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 9,8-9,13 per monitorare le performance delle macchine virtuali FlexGroup utilizzando le metriche ONTAP (dashboard e report VM) e 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 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 a meno che la guida alla soluzione non lo richieda specificamente; utilizzare gli switch per disporre di percorsi ridondanti e consentire a VMware ha di funzionare senza alcun intervento.
- I frame jumbo devono essere utilizzati se supportati dalla rete. 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 solo il controllo di flusso di rete sulle porte di cluster Interconnect in un cluster ONTAP. NetApp non fornisce altre raccomandazioni per le Best practice relative al controllo di flusso 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, NVMe/FC, iSCSI, NVMe/TCP), RDM

ONTAP offre storage a blocchi di livello Enterprise per VMware vSphere utilizzando i tradizionali iSCSI e Fibre Channel Protocol (FCP) oltre al protocollo a blocchi di nuova generazione, NVMe over Fabrics (NVMe-of), ad alta efficienza e performance, con supporto per NVMe/FC e NVMe/TCP.

Per le Best practice dettagliate per l'implementazione dei protocolli a blocchi per lo storage delle macchine virtuali con vSphere e ONTAP, fare riferimento a. "Datastore e protocolli: SAN"

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 menzionato nella "datastore"sezione, quando si utilizza NFS con vSphere, esistono alcuni benefici di facilità d'uso ed efficienza dello storage.

Per le Best practice consigliate fare riferimento a. "Datastore e protocolli: NFS"

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. Tuttavia, ci sono alcune limitazioni e avvertimenti da essere informati di.

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 fino a quando 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.

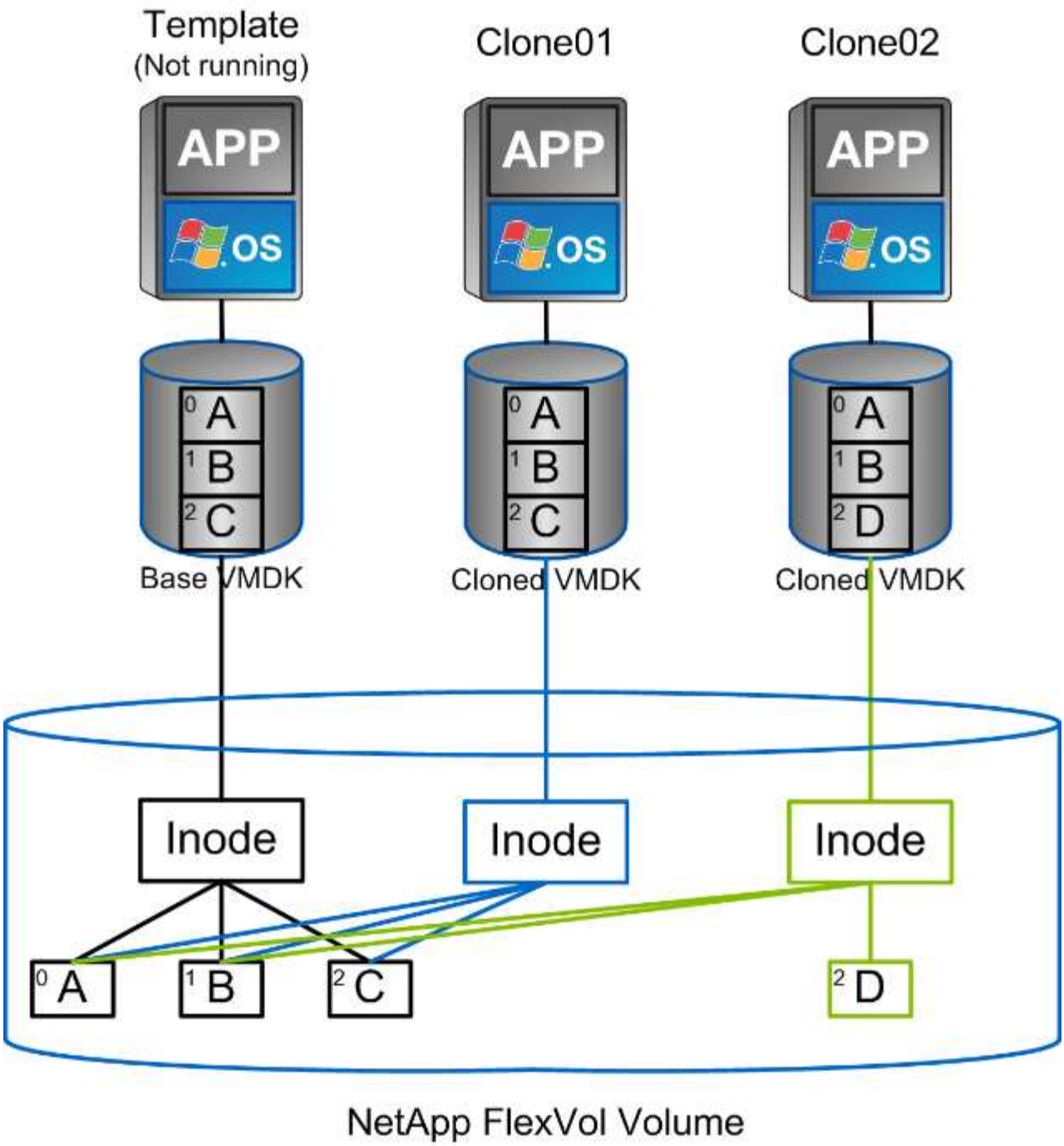
Clonazione di VM e datastore

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.



Il cloning può essere scaricato sui sistemi che eseguono ONTAP attraverso diversi meccanismi, generalmente 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 in ONTAP negli ambienti SAN e NAS (NetApp fornisce un plug-in ESXi per consentire VAAI per NFS), mentre vSphere alleggerisce il carico delle operazioni delle macchine virtuali cold (spente) in un datastore NAS, mentre le operazioni delle macchine virtuali hot (cloning e storage vMotion) vengono anch'esse trasferite nella SAN. ONTAP utilizza l'approccio più

efficiente in base all'origine e alla destinazione. Questa funzionalità viene utilizzata anche da "Omnissa Vista orizzonte".

- SRA (utilizzato con VMware Live Site Recovery/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 di una macchina virtuale in modo che sia possibile ripristinare i singoli file.

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 in un datastore tradizionale mediante un FlexVol volume può essere rapido ed efficiente con la licenza FlexClone (inclusa nella licenza ONTAP One), 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 e il ripristino rapido delle macchine virtuali (VM) sono vantaggi chiave dell'utilizzo di ONTAP per vSphere. Questa funzionalità può essere facilmente gestita all'interno di vCenter tramite il plug-in SnapCenter per VMware vSphere. Molti clienti migliorano le loro soluzioni di backup di terze parti con SnapCenter per sfruttare la tecnologia Snapshot di ONTAP, poiché offre il modo più veloce e semplice di ripristinare una macchina virtuale tramite ONTAP. SnapCenter è disponibile gratuitamente per i clienti che dispongono della licenza ONTAP ONE; potrebbero essere disponibili anche altri bundle di licenze.

Inoltre, il plug-in SnapCenter per VMware può essere integrato con "NetApp Backup and Recovery per macchine virtuali", consentendo soluzioni di backup 3-2-1 efficaci per la maggior parte dei sistemi ONTAP . Si noti che potrebbero essere applicati dei costi se si utilizza Backup e Ripristino per macchine virtuali con servizi premium, come gli archivi di oggetti per ulteriore spazio di archiviazione per il backup. Questa sezione descrive le varie opzioni disponibili per proteggere le VM e gli archivi dati.

Snapshot dei volumi NetApp ONTAP

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.

Le snapshot sono una funzionalità chiave di ONTAP, consentendoti di creare copie point-in-time dei tuoi dati. Sono efficienti in termini di spazio e possono essere create rapidamente, rendendole ideali per proteggere macchine virtuali e datastore. Gli snapshot possono essere utilizzati per vari scopi, incluso backup, recovery e test. Questi Snapshot sono diversi dalle Snapshot VMware (di coerenza) e sono adatti per una protezione a lungo termine. Gli snapshot gestiti da vCenter di VMware sono consigliati solo per un utilizzo a breve termine, a causa delle prestazioni e di altri effetti. Per "Limitazioni delle snapshot"ulteriori dettagli, fare riferimento a.

Vengono create a livello di volume copie Snapshot che possono essere utilizzate per proteggere tutte le macchine virtuali e i datastore all'interno di tale volume. Ciò significa che puoi creare una snapshot di un intero datastore, che include tutte le macchine virtuali all'interno di tale datastore.

Per gli archivi dati NFS, è possibile visualizzare facilmente i file VM nelle istantanee navigando nella directory .istantanee. Ciò consente di accedere e ripristinare rapidamente i file da uno snapshot senza dover utilizzare una soluzione di backup specifica.

Per gli archivi dati VMFS, è possibile creare un FlexClone dell'archivio dati in base allo snapshot desiderato. Ciò consente di creare un nuovo datastore basato sullo snapshot, che può essere utilizzato a scopo di test o sviluppo. La FlexClone occupa spazio solo per le modifiche apportate dopo la creazione della snapshot, creando un modo efficiente in termini di spazio per creare una copia dell'archivio dati. Una volta creato FlexClone, è possibile mappare la LUN o il namespace a un host ESXi come un normale datastore. Ciò consente non solo di ripristinare file VM specifici, ma anche di creare rapidamente ambienti di test o sviluppo in base ai dati di produzione, senza influire sulle performance dell'ambiente di produzione.

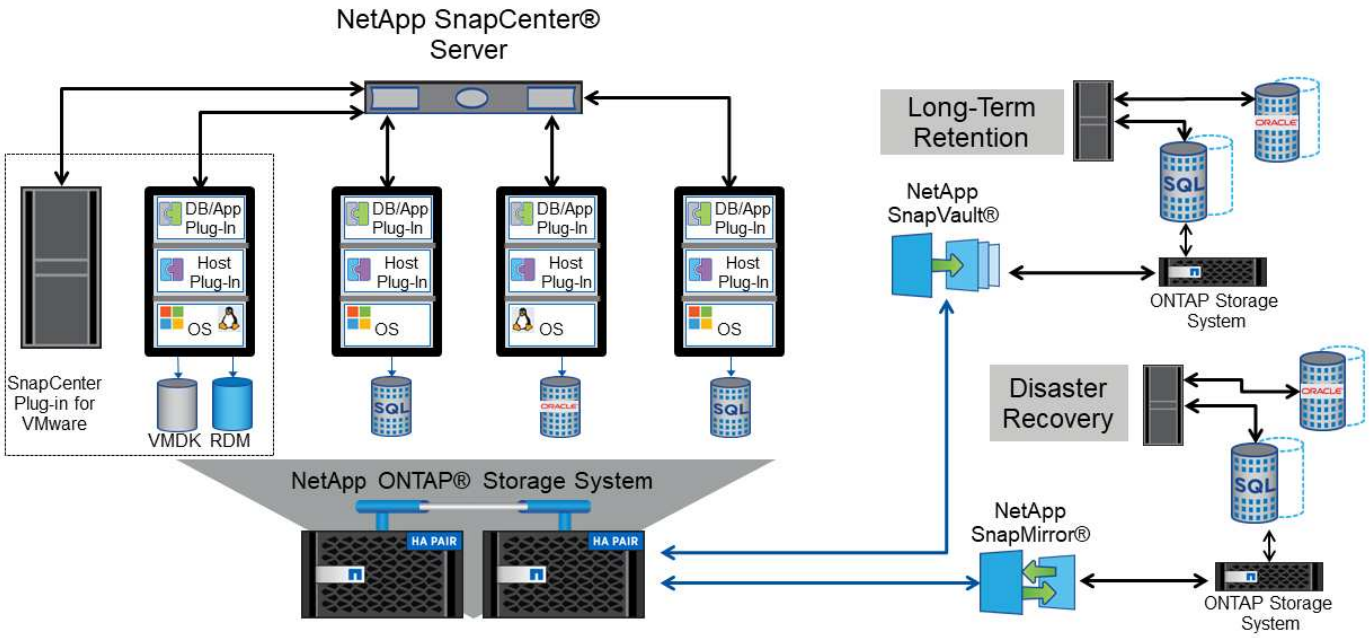
Per ulteriori informazioni sugli snapshot, fare riferimento alla documentazione ONTAP . I seguenti link forniscono ulteriori dettagli: "Copie snapshot locali ONTAP" "Flusso di lavoro di replicazione ONTAP SnapMirror"

Plug-in SnapCenter per VMware vSphere

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 continuano a consentire 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 delle applicazioni SnapCenter per proteggere i dati transazionali come SQL Server o Oracle.

Questi plug-in offrono funzionalità estese per proteggere i database in ambienti fisici e virtuali. Grazie a vSphere, puoi utilizzarli per proteggere i database SQL Server o Oracle, in cui i dati vengono memorizzati su LUN RDM, vVol o namespace NVMe/TCP e LUN iSCSI direttamente connessi al sistema operativo guest, oppure file VMDK su datastore VMFS o NFS. I plug-in consentono di specificare diversi tipi di backup del database, supportando il backup online o offline e proteggendo i file di database insieme ai file di registro. Oltre al backup e alla recovery, 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 informazioni sul dimensionamento, fare riferimento a. "Guida al dimensionamento per il plugin SnapCenter per VMware vSphere"

Tool ONTAP per VMware vSphere con VMware Live Site Recovery

I tool di ONTAP per VMware vSphere (OT4VS) sono un plug-in gratuito che offre una perfetta integrazione tra VMware vSphere e NetApp ONTAP. Consente di gestire lo storage ONTAP direttamente dal client web vSphere, semplificando l'esecuzione di attività come il provisioning dello storage, la gestione della replica e il monitoraggio delle performance.

Per funzionalità di disaster recovery migliorate, considerare l'utilizzo di NetApp SRA for ONTAP, che fa parte degli strumenti ONTAP per VMware vSphere, insieme a VMware Live Site Recovery (precedentemente noto come Site Recovery Manager). Questo tool non solo supporta la replica di datastore in un sito di disaster recovery mediante SnapMirror, ma consente anche di eseguire test senza interruzioni nell'ambiente di disaster recovery mediante il cloning dei datastore replicati. Inoltre, il recovery da un disastro e la reprotezione della produzione dopo la risoluzione di un black-out sono ottimizzati grazie alle funzionalità di automazione integrate.

NetApp Disaster Recovery

Disaster Recovery (DR) è un servizio basato su cloud che fornisce una soluzione completa per la protezione dei dati e delle applicazioni in caso di disastro. Offre una gamma di funzionalità, tra cui failover e failback automatizzati, più punti di ripristino point-in-time, disaster recovery coerente con l'applicazione e supporto per sistemi ONTAP sia on-premise che basati su cloud. NetApp Disaster Recovery è progettato per funzionare in modo ottimale con ONTAP e l'ambiente VMware vSphere, offrendo una soluzione unificata per il disaster recovery.

VSphere Metro Storage Cluster (vMSC) con sincronizzazione attiva NetApp MetroCluster e SnapMirror

Infine, per il massimo livello di protezione dei dati, prendere in considerazione la configurazione di VMware vSphere Metro Storage Cluster (vMSC) che utilizza NetApp MetroCluster. VMSC è una soluzione supportata da NetApp con certificazione VMware che utilizza la replica sincrona, offrendo gli stessi vantaggi di un cluster ad alta disponibilità ma distribuita in siti separati per la protezione contro il disastro del sito. La sincronizzazione attiva NetApp SnapMirror, con ASA e AFF e MetroCluster con AFF, offre configurazioni

convenienti per una replica sincrona con recovery trasparente da qualsiasi guasto di un componente storage singolo, nonché recovery trasparente nel caso di SnapMirror Active Sync o recovery con singolo comando in caso di disastro del sito con MetroCluster. VMSC è descritto in maggior dettaglio in "TR-4128".

Qualità del servizio (QoS)

I limiti di throughput sono utili per controllare i livelli di servizio, gestire carichi di lavoro sconosciuti o testare le applicazioni prima della distribuzione per assicurarsi che non influiscano su altri carichi di lavoro in produzione. Possono anche essere utilizzati per limitare un carico di lavoro ingombrante dopo l'identificazione.

Supporto della policy QoS di ONTAP

I sistemi che eseguono ONTAP possono utilizzare la funzionalità di qualità del servizio di storage 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.

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.

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 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.

Fare riferimento a. "Panoramica sulla gestione e sul monitoraggio delle performance" per ulteriori informazioni.

Datastore NFS non vVol

È possibile applicare una policy di QoS ONTAP all'intero datastore o ai singoli file VMDK al suo interno. Tuttavia, è importante comprendere che tutte le macchine virtuali di un datastore NFS tradizionale (non vVol) condividono una coda i/o comune da un determinato host. Se una macchina virtuale viene rallentata da una policy di QoS ONTAP, in pratica tutto l'i/o del datastore sembrerà rallentato per quell'host.

Esempio:
* È stato configurato un limite QoS su VM1.vmdk per un volume montato come datastore NFS tradizionale dall'host esxi-01.
* Lo stesso host (esxi-01) utilizza VM2.vmdk e si trova sullo stesso volume.
* Se VM1.vmdk viene rallentato, allora anche VM2.vmdk sembrerà essere rallentato poiché condivide la stessa coda io con VM1.vmdk.

Questo non si applica ai vVol.

A partire da vSphere 6,5 è possibile gestire limiti granulari dei file sui datastore non vVol sfruttando la gestione basata su criteri dello storage (SPBM, Storage Policy-Based Management) con Storage i/o Control (SIOC) v2.

Fare riferimento ai link seguenti per ulteriori informazioni sulla gestione delle prestazioni con i criteri SIOC e SPBM.

"Regole basate su host SPBM: SIOC v2"
"Gestisci le risorse i/o di storage con vSphere"

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.

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. Tieni presente che si applicano ancora le limitazioni di qualità del servizio menzionate in precedenza per i datastore NFS tradizionali.

Datastore VMFS

Utilizzando le LUN di ONTAP, le policy di QoS possono essere applicate al volume FlexVol che contiene le LUN o le singole LUN, ma non ai singoli file VMDK perché ONTAP non conosce il file system VMFS.

Datastore vVol

È possibile impostare facilmente una qualità del servizio minima e/o massima su singole macchine virtuali o VMDK senza impatti su altre macchine virtuali o VMDK grazie alla gestione basata su policy di storage e ai vVol.

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.

VVol richiede l'utilizzo dei tool ONTAP per VMware vSphere, che funziona come provider VASA per ONTAP. Fare riferimento a "Volumi virtuali di VMware vSphere (vVol) con ONTAP" per le procedure consigliate per i vVol.

QoS ONTAP e SIOC VMware

ONTAP QoS e VMware vSphere Storage i/o Control (SIOC) sono tecnologie complementari che gli amministratori di vSphere e dello storage possono utilizzare insieme per gestire le performance delle VM vSphere ospitate in sistemi che eseguono 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	Sì (il datastore può essere rallentato)
Impostare QoS sul volume (datastore NFS)?	Sì	Sì (il datastore può essere rallentato)
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.

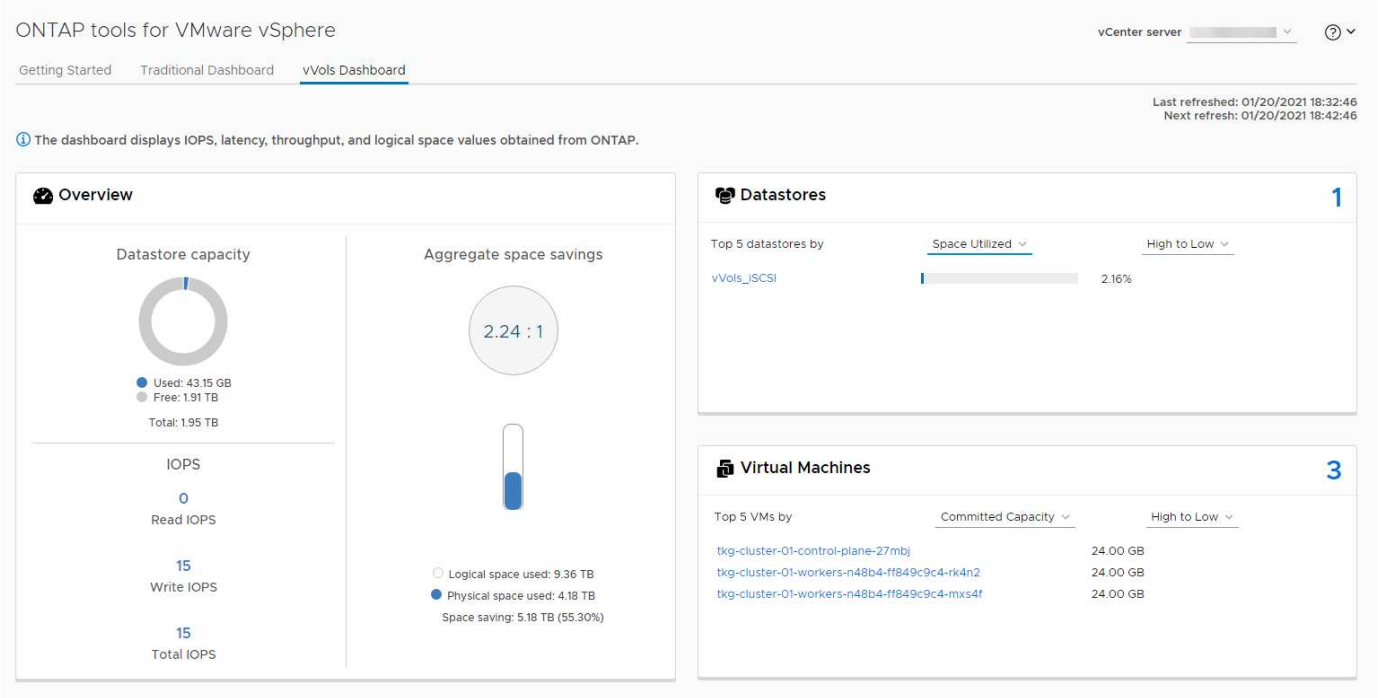
Gestione basata su criteri di archiviazione e vVol

Le API VMware vSphere per Storage Awareness (VASA) consentono a un amministratore dello storage di configurare con facilità i datastore con funzionalità ben definite, consentendo all'amministratore delle macchine virtuali di utilizzare tali dati 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 policy di storage delle macchine virtuali, ma dovevano collaborare con l'amministratore dello storage per identificare i datastore appropriati, spesso utilizzando documentazione o convenzioni di naming. 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.



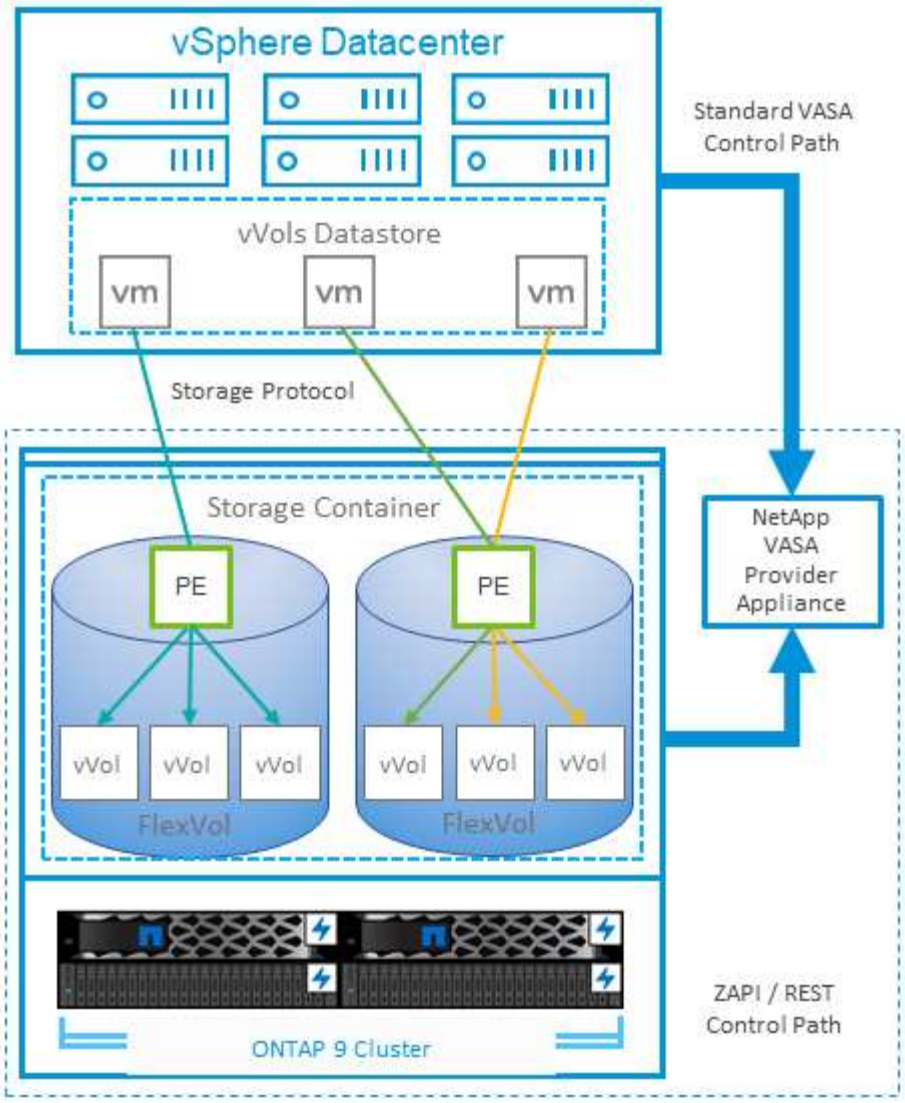
Una volta definito il profilo di capacità dello storage, è possibile utilizzarlo per eseguire il provisioning delle macchine virtuali utilizzando la policy di storage che ne identifica i requisiti. La mappatura tra il criterio di storage delle macchine virtuali e il profilo di capacità dello storage 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:

- **Offerte di prima parte.** Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes e Azure NetApp Files forniscono servizi di archiviazione gestiti multiprotocollo ad alte prestazioni nei principali ambienti cloud pubblici. Possono essere utilizzati direttamente da VMware Cloud on AWS (VMC on AWS), Azure VMware Solution (AVS) e Google Cloud VMware Engine (GCVE) come datastore o storage per sistemi operativi guest (GOS) e istanze di elaborazione.
- **Servizi cloud.** Utilizza NetApp Backup and Recovery o SnapMirror Cloud per proteggere i dati dai sistemi on-premise tramite storage cloud pubblico. NetApp Copy and Sync ti aiuta a migrare e mantenere sincronizzati i tuoi dati su NAS e archivi di oggetti. NetApp Disaster Recovery fornisce una soluzione efficiente e conveniente per sfruttare le tecnologie NetApp come base per una soluzione di disaster recovery solida e capace per DR su cloud, DR su locale e da locale a locale.
- **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 progetti le tue applicazioni basate su VM, considera la futura mobilità nel cloud. Ad esempio, anziché collocare insieme i file di dati e quelli dell'applicazione, utilizzare un'esportazione LUN o NFS separata per i dati. Ciò consente di migrare separatamente la VM e i dati sui servizi cloud.

Per un'analisi approfondita di altri argomenti relativi alla sicurezza, fare riferimento alle seguenti risorse.

- "Documentazione ONTAP Select"
- "Documentazione di backup e ripristino"
- "Documentazione sul ripristino di emergenza"
- "Amazon FSX per NetApp ONTAP"
- "VMware Cloud su AWS"
- "Che cos'è Azure NetApp Files?"
- "Soluzione VMware Azure"
- "Motore VMware Google Cloud"
- "Che cos'è Google Cloud NetApp Volumes?"

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 ONTAP semplificano la protezione di qualsiasi dato grazie alla crittografia a riposo. La crittografia dello storage NetApp (NSE) utilizza dischi con crittografia automatica (SED) con ONTAP per proteggere i dati di 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. Puoi eseguire l'aggiornamento e iniziare a utilizzarlo senza interruzioni per client o applicazioni, validati secondo lo standard FIPS 140-2 livello 1, incluso Onboard Key Manager.

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.

- **Key Manager integrato incluso.** La crittografia software NetApp include un gestore delle chiavi integrato senza costi aggiuntivi, il che semplifica l'avvio senza server di gestione delle chiavi ad alta disponibilità che sono 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 Onboard Key Manager specificando una passphrase e quindi creare un nuovo volume o spostare un volume lato storage per attivare la crittografia. NetApp sta lavorando per aggiungere un supporto più integrato per le funzionalità di crittografia nelle versioni future dei suoi strumenti VMware.

Per un'analisi approfondita di altri argomenti relativi alla sicurezza, fare riferimento alle seguenti risorse.

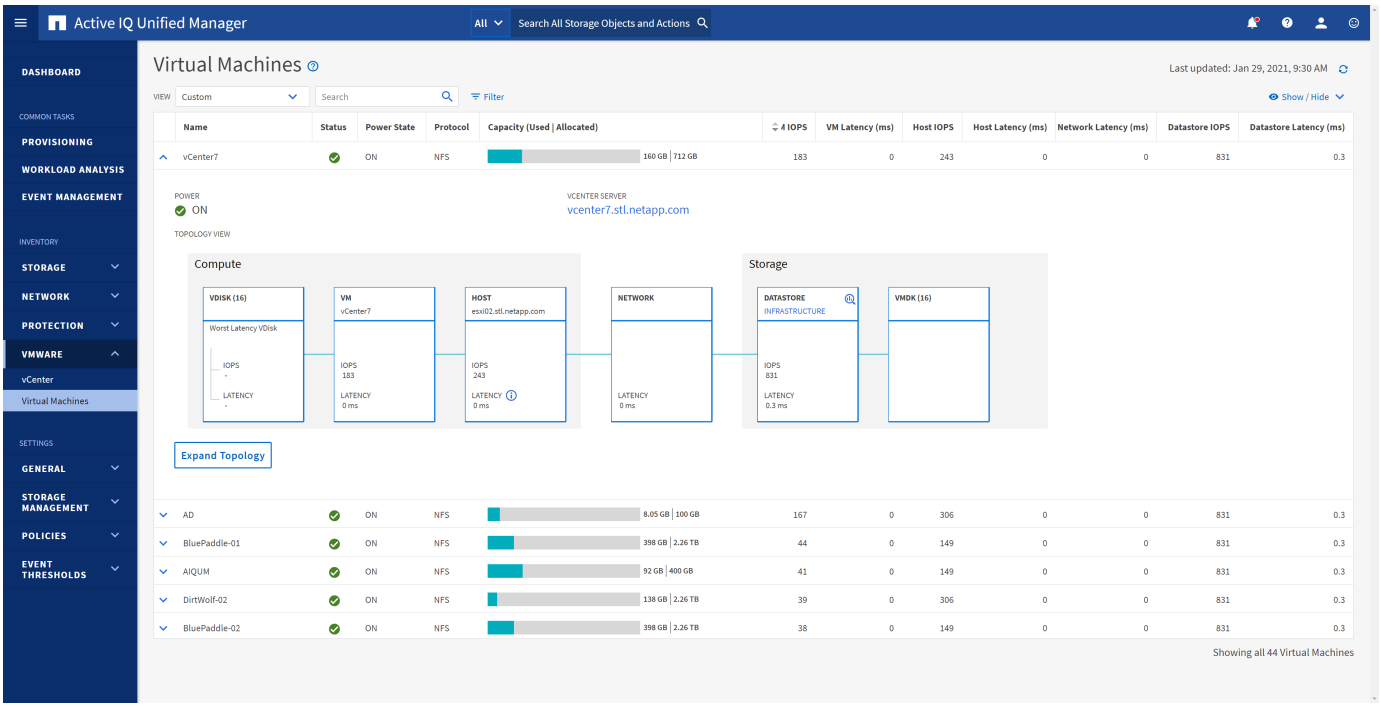
- "Report tecnici sulla sicurezza"
- "Guide per la protezione avanzata"
- "Documentazione del prodotto di sicurezza e crittografia dei dati ONTAP"

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.

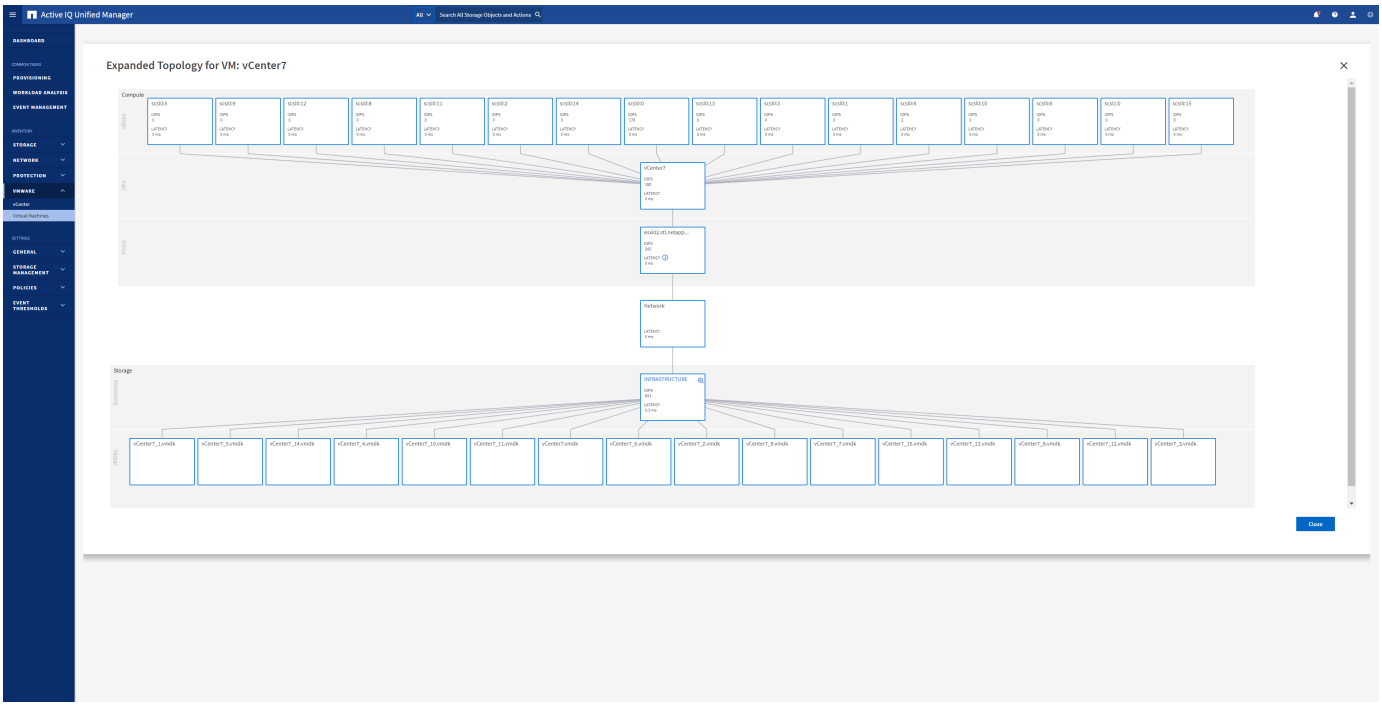
Una tipica implementazione di un'infrastruttura virtuale su ONTAP include diversi componenti distribuiti tra livelli di calcolo, rete e storage. Eventuali ritardi nelle performance in un'applicazione VM potrebbero verificarsi a causa di una combinazione di latenze affrontate dai vari componenti nei rispettivi 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) consentono a un amministratore dello storage di configurare con facilità i datastore con funzionalità ben

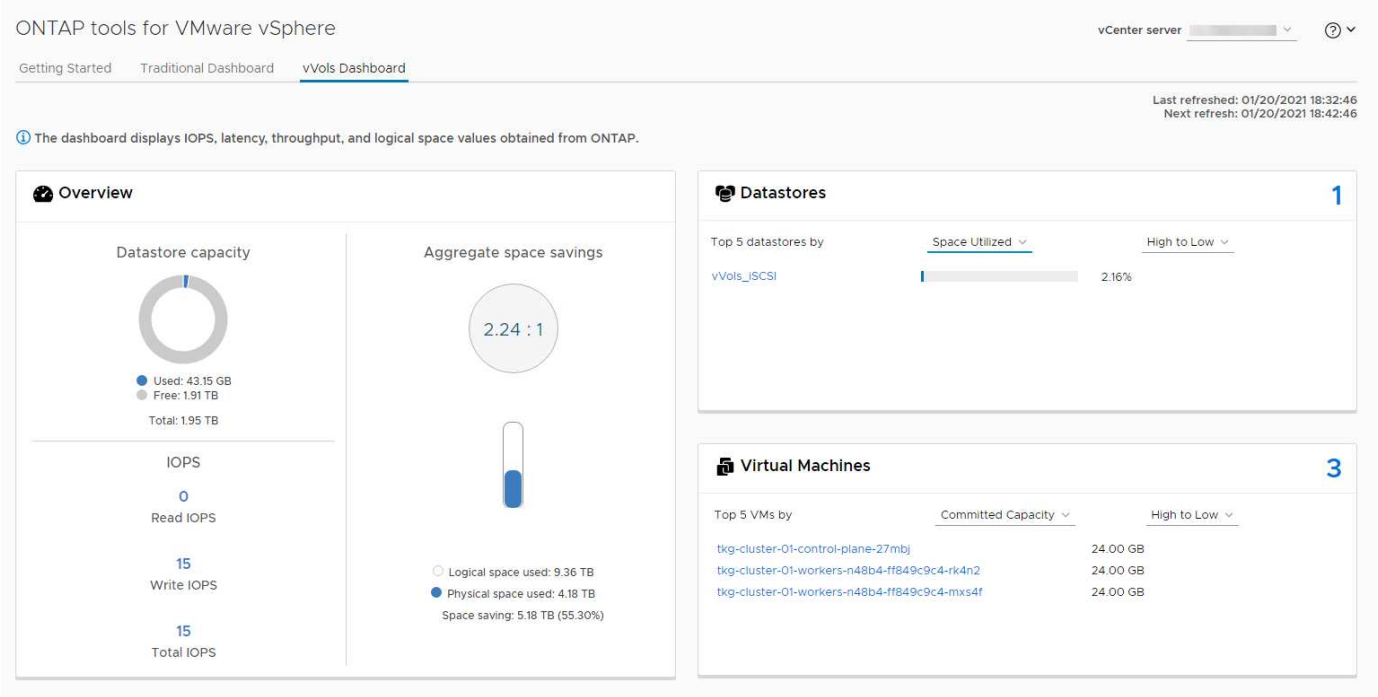
definite, consentendo all'amministratore delle macchine virtuali di utilizzare tali dati quando necessario per eseguire il provisioning delle macchine virtuali senza dover interagire tra loro.

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 policy di storage delle macchine virtuali, ma dovevano collaborare con l'amministratore dello storage per identificare i datastore appropriati, spesso utilizzando documentazione o convenzioni di naming. 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.

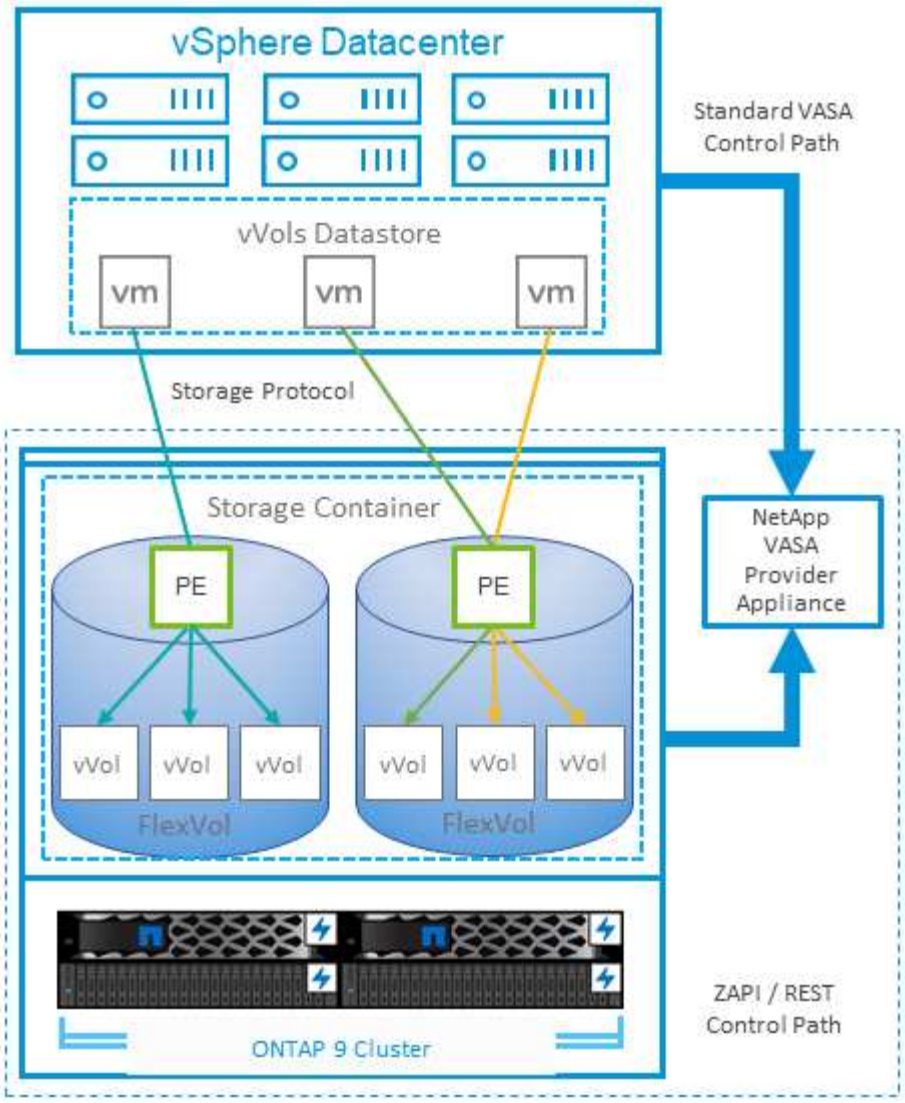
VASA offre la tecnologia per eseguire query sullo storage e restituire un set di funzionalità di storage a vCenter. I vendor provider VASA forniscono la traduzione tra le API e i costrutti del sistema storage e le API VMware comprese da vCenter. Il provider VASA di NetApp per ONTAP viene offerto come 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 funzione vSphere che posiziona automaticamente le macchine virtuali in un cluster di datastore in base alla latenza di 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:

- Non utilizzare i DSP a meno che non si disponga di un requisito specifico per farlo.
  - I DSP non sono necessari quando si utilizza ONTAP. GLI SDR non sono consapevoli delle funzionalità

di efficienza dello storage ONTAP come la deduplica e la compressione, per cui potrebbero prendere decisioni non ottimali per l'ambiente in uso.

- GLI SDR non sono a conoscenza delle policy QoS di ONTAP, pertanto potrebbero prendere decisioni che non sono ottimali per le performance.
- GLI SDR non sono a conoscenza delle copie snapshot ONTAP, pertanto potrebbero prendere decisioni che causano una crescita esponenziale delle snapshot. Ad esempio, spostando una macchina virtuale in un altro datastore vengono creati nuovi file nel nuovo datastore, con una conseguente crescita dello snapshot. Ciò vale in particolare per le macchine virtuali con dischi di grandi dimensioni o molte istantanee. Quindi, se la macchina virtuale dovesse essere spostata di nuovo nel datastore originale, lo snapshot nel datastore originale crescerà ulteriormente.

Se si utilizzano gli SDR, prendere in considerazione le seguenti procedure consigliate:

- 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 LE SDR spostano i VMDK tra datastore, qualsiasi risparmio di spazio derivante dal cloning o dalla deduplica ONTAP può essere ridotto a seconda della qualità di deduplica o compressione della destinazione.
  - 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.

Ulteriori informazioni sugli SDR sono disponibili nella documentazione VMware all'indirizzo "Domande frequenti su Storage DRS".

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 sono facilmente impostabili utilizzando gli strumenti ONTAP per VMware vSphere: Dalla pagina di panoramica degli strumenti ONTAP, scorrere fino alla fine e fare clic su Applica impostazioni consigliate nel portlet conformità host ESXi.

Di seguito sono riportate le impostazioni dell'host consigliate per tutte le versioni di ONTAP attualmente supportate.

Impostazione host	Valore consigliato da NetApp	Riavvio richiesto
Configurazione avanzata ESXi		
VMFS3.HardwareAcceleratedLocking	Mantieni predefinito (1)	No

Impostazione host	Valore consigliato da NetApp	Riavvio richiesto
VMFS3.EnableBlockDelete	Mantenere l'impostazione predefinita (0), ma può essere modificata se necessario. Per ulteriori informazioni, vedere "Recupero di spazio per VMFS5 macchine virtuali"	No
VMFS3.EnableVMFS6Unmap	Mantenere l'impostazione predefinita (1) per ulteriori informazioni, vedere "API VMware vSphere: Integrazione degli array (VAAI)"	No
Impostazioni NFS		
NewSyncInterval	Se non si utilizza vSphere CSI per Kubernetes, impostare come indicato in "VMware KB 386364"	No
NET.TcpipelHeapSize	VSphere 6.0 o versione successiva, impostato su 32. 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. Impostare sul valore predefinito (1024MB) per 6.5U3, 6.7U3 e 7,0 o versioni successive.	Sì
NFS.MaxVolumes	VSphere 6,0 o versioni successive, impostare su 256 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 da 7.0 a 8.0, impostato su 128. Questa impostazione viene ignorata nelle versioni ESXi successive alla 8.0.	No
Impostazioni FC/FCoE		

Impostazione host	Valore consigliato da NetApp	Riavvio richiesto
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. L'impostazione di questo valore su RR consente di fornire il bilanciamento del carico in tutti i percorsi attivi/ottimizzati. 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. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.	No
Disk.QFullThreshold	Impostare su 8 per tutte le configurazioni. 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. 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. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.	No
Disk.QFullThreshold	Impostare su 8 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.	No

L'opzione di configurazione avanzata NFS MaxQueueDepth potrebbe non funzionare come previsto quando si utilizzano VMware vSphere ESXi 7.0.1 e VMware vSphere ESXi 7,0.2. Per ulteriori informazioni, fare riferimento "Tastiera VMware 86331"a.

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:

- Quando si utilizzano sistemi non ASA in ambienti ad alte prestazioni o quando si testano le prestazioni con un singolo datastore LUN, valutare la possibilità di modificare l'impostazione del bilanciamento del carico della policy di selezione del percorso (PSP) round-robin (VMW_PSP_RR) dall'impostazione IOPS predefinita di 1000 a un valore di 1. Vedere"VMware KB 2069356" per maggiori informazioni.
- In vSphere 6.7 Update 1, VMware ha introdotto un nuovo meccanismo di bilanciamento del carico di latenza per il Round Robin PSP. L'opzione di latenza è ora disponibile anche quando si utilizza HPP (High Performance Plugin) con namespace NVMe e con vSphere 8.0u2 e versioni successive, LUN connesse tramite iSCSI e FCP. La nuova opzione considera la larghezza di banda I/O e la latenza del percorso quando seleziona il percorso ottimale per I/O. NetApp consiglia di utilizzare l'opzione di latenza in ambienti con connettività di percorso non equivalente, ad esempio nei casi con più hop di rete su un percorso rispetto a un altro, oppure quando si utilizza un sistema NetApp ASA . Vedere "Modifica dei parametri predefiniti per la latenza Round Robin" per maggiori 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. Per ulteriori dettagli, visitare la pagina "Utilizzo di VMware vSphere 8.x con ONTAP" relativa a NVMe-of con vSphere 7. Per ulteriori dettagli, visitare il sito "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, ulteriori dettagli sono disponibili 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 strumenti ONTAP 10

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 di vVol presenti in vSphere 8,0 update 3, nella versione 10,4 degli strumenti ONTAP e nei nuovi sistemi NetApp ASA.

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 - namespace NVMe (utilizzati con gli strumenti ONTAP 9.13P2). NetApp ha lavorato a stretto contatto con VMware come partner di riferimento per vVol rilasciati con vSphere 6 nel 2015 e ancora come partner di progettazione per vVol che utilizzano NVMe over Fabrics 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.

Punto terminale del protocollo (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.

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.

Per ulteriori informazioni, vedere "NVMe e volumi virtuali" acceso "vmware.com"

Datastore di volumi virtuali

| Il datastore Virtual Volume è una rappresentazione logica del datastore di un contenitore vVols , creato e gestito da un provider VASA. Il contenitore rappresenta un pool di capacità di archiviazione fornita dai sistemi di archiviazione gestiti dal provider VASA. Gli strumenti ONTAP supportano l'allocazione di più volumi FlexVol (denominati volumi di backup) a un singolo datastore vVols ; questi datastore vVols possono estendersi su più nodi in un cluster ONTAP , combinando sistemi flash e ibridi con diverse funzionalità. L'amministratore può creare nuovi volumi FlexVol utilizzando la procedura guidata di provisioning o l'API REST oppure selezionare volumi FlexVol pre-creati per l'archiviazione di backup, se disponibili.

Volumi virtuali (vVol)

I vVols sono i file e i dischi effettivi della macchina virtuale archiviati nel datastore vVols . Utilizzando il termine vVol (singolare) si fa riferimento a un singolo file specifico, LUN o namespace. ONTAP crea namespace, LUN o file NVMe a seconda del protocollo utilizzato dal datastore. Esistono diversi tipi distinti di vVols; i più comuni sono Config (l'unico con VMFS, contiene file di metadati come il file VMX della VM), Data (disco virtuale o VMDK) e Swap (creato all'accensione della VM). I vVols protetti dalla crittografia della VM VMware saranno di tipo Altro. La crittografia delle VM VMware non deve essere confusa con la crittografia dei volumi ONTAP o con quella degli aggregati.

Gestione basata sulle policy

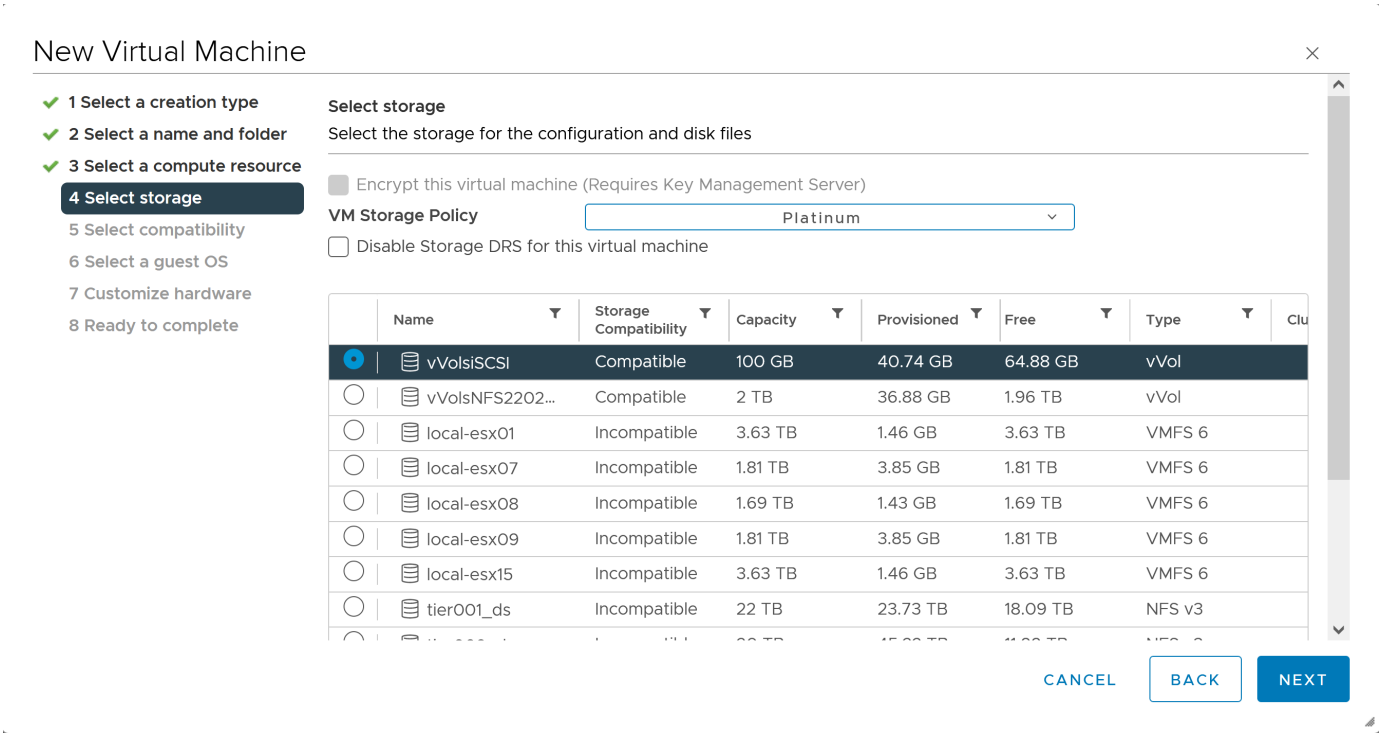
Le API VMware vSphere per Storage Awareness (VASA) consentono agli amministratori di VM di utilizzare facilmente tutte le funzionalità di storage necessarie per il provisioning delle VM, senza dover interagire con il proprio team di storage. Prima di VASA, gli amministratori delle VM potevano definire le policy di archiviazione delle VM, ma dovevano collaborare con i propri amministratori di archiviazione per identificare gli archivi dati appropriati, spesso utilizzando la documentazione o convenzioni di denominazione. Con VASA, gli amministratori di vCenter dotati delle autorizzazioni appropriate possono definire una gamma di funzionalità di archiviazione che gli utenti di vCenter possono poi utilizzare per il provisioning delle VM. La mappatura tra la policy di archiviazione della VM e le funzionalità del datastore consente a vCenter di visualizzare un elenco di datastore compatibili tra cui scegliere, oltre ad abilitare altre tecnologie come VCF (in precedenza noto come Aria e vRealize) Automation o VMware vSphere Kubernetes Service (VKS) per selezionare automaticamente lo storage da una policy assegnata. Questo approccio è noto come gestione basata sulle policy di archiviazione. Sebbene le regole del provider VASA e le policy di archiviazione delle VM possano essere utilizzate anche con i datastore tradizionali, in questo caso ci concentreremo sui datastore vVols .

Policy di storage delle VM

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 ONTAP 10.X ora offrono un approccio più semplice rispetto ai tool ONTAP 9.X, consentendo di specificare direttamente gli attributi di storage nel criterio di storage della VM.

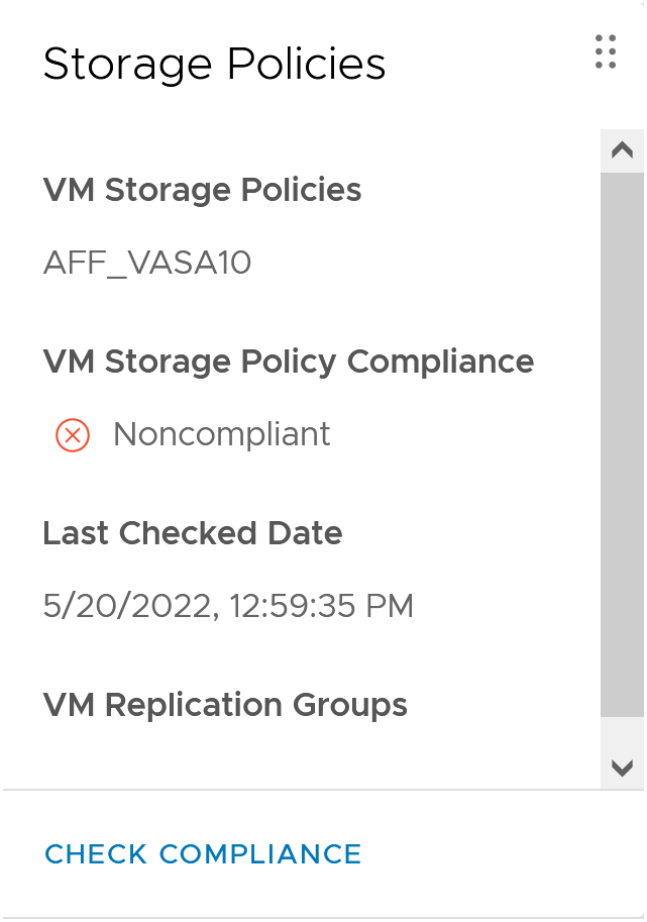
Come menzionato in precedenza, l'utilizzo delle policy può contribuire a semplificare l'attività di provisioning di una macchina virtuale o di un VMDK. Basta selezionare una policy appropriata e il provider VASA mostrerà i datastore vVol che supportano tale policy e posizioneranno il vVol in un singolo FlexVol volume conforme.

Implementare la macchina virtuale utilizzando i criteri di storage



Una volta eseguito il provisioning di una VM, il provider VASA continuerà a verificare la conformità e avviserà l'amministratore della VM con un allarme in vCenter quando il volume di supporto non è più conforme alla policy.

Conformità delle policy di storage delle macchine virtuali



Supporto vVol NetApp

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

ONTAP

Oltre a ONTAP 9 sui sistemi AFF, ASA e FAS , NetApp supporta i carichi di lavoro VMware su ONTAP Select, Amazon FSx per NetApp con VMware Cloud su AWS, Azure NetApp Files con Azure VMware Solution, Google Cloud NetApp Volumes con Google Cloud VMware Engine e NetApp Private Storage in Equinix, ma le funzionalità specifiche possono variare in base al fornitore di servizi e alla connettività di rete disponibile.

Al momento della pubblicazione, gli ambienti hyperscaler sono limitati ai tradizionali datastore NFS v3; pertanto, i vVols sono disponibili solo con sistemi ONTAP on-premise o sistemi connessi al cloud che offrono tutte le funzionalità di un sistema on-premise, come quelli ospitati dai partner NetApp e dai provider di servizi 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 introdusse il supporto vVols con VASA 2.0 nel 2015, lo descrisse come "un framework di integrazione e gestione che fornisce un nuovo modello operativo per l'archiviazione esterna (SAN/NAS)". Questo modello operativo offre numerosi vantaggi insieme allo storage ONTAP .

Gestione basata sulle policy

Come spiegato nella sezione 1.2, la gestione basata su policy consente di eseguire il provisioning delle VM e di gestirle successivamente utilizzando policy predefinite. Ciò può aiutare le operazioni IT in diversi modi:

- **Aumentare la velocità.** Grazie agli strumenti ONTAP , l'amministratore di vCenter non ha più bisogno di aprire ticket con il team di storage per le attività di provisioning dello storage. Tuttavia, i ruoli RBAC degli strumenti ONTAP in vCenter e nel sistema ONTAP consentono comunque team indipendenti (ad esempio team di archiviazione) o attività indipendenti da parte dello stesso team, limitando l'accesso a funzioni specifiche, se desiderato.
- **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.** Gli strumenti VASA e ONTAP consentono di vedere la capacità dello storage fino al singolo livello di aggregato, se necessario, e fornire più livelli di avviso in caso di esaurimento della capacità.

Gestione granulare delle macchine virtuali nella moderna SAN

I primi sistemi di archiviazione SAN che utilizzano Fibre Channel e iSCSI sono stati supportati da VMware per ESX, ma non erano in grado di gestire singoli file e dischi VM dal sistema di archiviazione. Al contrario, vengono predisposti i LUN e VMFS gestisce i singoli file. Ciò rende difficile per il sistema di storage gestire direttamente le prestazioni di storage, la clonazione e la protezione delle singole VM. I vVols offrono la granularità di storage di cui i clienti che utilizzano storage NFS già godono, con le solide e performanti funzionalità SAN di ONTAP.

Ora, con vSphere 8 e gli ONTAP tools for VMware vSphere 9.12 e versioni successive, gli stessi controlli granulari utilizzati da vVols per i protocolli legacy basati su SCSI sono disponibili nella moderna SAN Fibre Channel che utilizza NVMe su Fabric per prestazioni ancora maggiori su larga scala. Con vSphere 8.0 Update 1, è ora possibile distribuire una soluzione NVMe end-to-end completa utilizzando vVols senza alcuna traduzione di I/O nello stack di storage dell'hypervisor.

Maggiori funzionalità di offload dello storage

Sebbene VAAI offra una varietà di operazioni che vengono trasferite allo storage, vi sono alcune lacune che vengono affrontate dal fornitore VASA. SAN VAAI non è in grado di scaricare gli snapshot gestiti da VMware sul sistema di storage. NFS VAAI può scaricare gli snapshot gestiti dalla VM, ma su una VM con snapshot nativi di archiviazione sono presenti delle limitazioni. Poiché i vVols utilizzano LUN, namespace o file individuali per i dischi delle macchine virtuali, ONTAP può clonare in modo rapido ed efficiente i file o le LUN per creare snapshot granulari per VM che non richiedono più file delta. NFS VAAI non supporta inoltre le operazioni di clonazione di offload per le migrazioni Storage vMotion a caldo (attivate). Quando si utilizza VAAI con datastore NFS tradizionali, la VM deve essere spenta per consentire lo scaricamento della migrazione. Il provider VASA negli strumenti ONTAP consente cloni quasi istantanei ed efficienti in termini di archiviazione per migrazioni a caldo e a freddo e supporta anche copie quasi istantanee per migrazioni tra volumi di vVols. Grazie a questi significativi vantaggi in termini di efficienza di archiviazione, potresti essere in grado di sfruttare

appieno i carichi di lavoro vVols con "Garanzia di efficienza" programma. Allo stesso modo, se i cloni cross-volume che utilizzano VAAI non soddisfano i tuoi requisiti, probabilmente riuscirai a risolvere la sfida aziendale grazie ai miglioramenti nell'esperienza di copia con vVols.

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 automazione e orchestrazione tramite la suite aria (in precedenza vRealize), OpenStack e così via.
- **Dischi di prima classe (FCD)**
  - Volumi persistenti VMware vSphere Kubernetes Service (VKS).
  - Fornire servizi simili ad Amazon EBS tramite la 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 , il che rappresenta un vantaggio rispetto ai tradizionali cloni abilitati per VAAI. Sono anche efficienti in termini di stoccaggio. I cloni all'interno di un volume utilizzano il clone di file ONTAP , che è simile ai volumi FlexClone e memorizza solo le modifiche dal file vVol/LUN/namespace di origine. Le VM a lungo termine per scopi di produzione o altre applicazioni vengono create rapidamente, occupano uno spazio minimo e possono trarre vantaggio dalla protezione a livello di VM (utilizzando il plug-in NetApp SnapCenter per VMware vSphere, gli snapshot gestiti da VMware o il backup VADP) e dalla gestione delle prestazioni (con ONTAP QoS). I cloni tra volumi sono molto più rapidi con vVols che con VAAI perché con VASA possiamo creare il clone e consentirne l'accesso alla destinazione prima che la copia sia completata. I blocchi di dati vengono copiati come processo in background per popolare il vVol di destinazione. Questo è simile al funzionamento dello spostamento LUN non-disruptive ONTAP per le LUN tradizionali.
- 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.
- I servizi simili ad Amazon EBS possono essere forniti tramite 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 VM a cui potrebbe essere collegato.

Elenco di controllo

Utilizzare questo elenco di controllo per garantire una distribuzione corretta (aggiornato per 10,3 e versioni successive).

Pianificazione iniziale

- Prima di iniziare l'installazione, è necessario controllare il "Tool di matrice di interoperabilità (IMT)" per assicurarsi che la distribuzione sia stata certificata.
- Determina le dimensioni e il tipo di configurazione degli strumenti ONTAP richiesti dall'ambiente. Per ulteriori informazioni, fare riferimento alla "Limiti di configurazione per l'implementazione dei tool ONTAP per VMware vSphere" .
- Determina se utilizzi SVM multitenant o consenti un accesso completo al cluster. Se utilizzi SVM multitenant, dovrai avere un LIF di gestione SVM su ciascuna SVM da utilizzare. Questa LIF deve essere raggiungibile tramite la porta 443 dagli strumenti ONTAP.
- Determinare se si utilizzerà Fibre Channel (FC) per la connettività dello storage. In tal caso, occorre "configurare lo zoning" utilizzare gli switch FC per abilitare la connettività tra gli host ESXi e le LIF FC della SVM.
- Determinare se si intende utilizzare l'adattatore di replica dello storage (SRA) degli strumenti ONTAP per VMware Site Recovery Manager (SRM) o Live Site Recovery (VLSR). In tal caso, sarà necessario accedere all'interfaccia di gestione del server SRM/VLSR per installare SRA.
- Se si utilizza la replica di SnapMirror gestita dagli strumenti ONTAP (inclusa, ma non solo, la sincronizzazione attiva di SnapMirror), l'amministratore di ONTAP deve "Creare una relazione di peer cluster in ONTAP" e "Creare una relazione di peer intercluster SVM in ONTAP" prima di poter utilizzare gli strumenti ONTAP con SnapMirror.
- "Scarica" ONTAP mette a disposizione OVA e, se necessario, il file SRA tar.gz.

Fornire indirizzi IP e record DNS

- Richiedere le seguenti informazioni IP al proprio team di rete. Sono necessari i primi tre indirizzi IP; il nodo due e il nodo tre sono utilizzati per implementazioni di ha (high Availability) scale-out. I record host DNS sono obbligatori e tutti i nomi dei nodi e tutti gli indirizzi devono trovarsi sulla stessa VLAN e subnet.
- ONTAP tools indirizzo applicazione _____ . _____ . _____ . _____
- Indirizzo servizi interni _____ . _____ . _____ . _____
- Il nome host DNS del nodo uno _____
- L'indirizzo IP del nodo uno _____ . _____ . _____ . _____
- Maschera di sottorete _____ . _____ . _____ . _____
- Gateway predefinito _____ . _ . _ . __
- Server DNS 1 _____ . _____ . _____ . _____
- Server DNS 2 _____ . _____ . _____ . _____
- Dominio di ricerca DNS _____
- Nome host DNS del nodo due (opzionale) _____
- Indirizzo IP del nodo due (opzionale) _____ . _____ . _____ . _____
- Nome host DNS del nodo tre (opzionale) _____
- Indirizzo IP del nodo tre (opzionale) _____ . _____ . _____ . _____
- Creare record DNS per tutti gli indirizzi IP indicati sopra.

Configurazione del firewall di rete

- Aprire le porte richieste per gli indirizzi IP sopra indicati nel firewall di rete. Per l'aggiornamento più recente,

consultare la sezione "Requisiti delle porte".

4 Flash in modo Smart

- È necessario un datastore su un dispositivo storage condiviso. In alternativa, è possibile utilizzare una libreria di contenuti nello stesso datastore del nodo uno per semplificare la clonazione rapida del modello con VAAI.
- Libreria di contenuti (richiesta solo per ha) _____
- Nodo 1 datastore _____
- Datastore nodo due (opzionale, ma consigliato per ha) ___________
- Datastore nodo tre (opzionale, ma consigliato per ha) ____

5 Distribuire l'OVA

- Si noti che questo passaggio può richiedere fino a 45 minuti
- "Distribuire l'OVA" Utilizzando il client vSphere.
- Nel passaggio 3 della distribuzione OVA, selezionare l'opzione "Customize this virtual machine's hardware" (Personalizza l'hardware di questa macchina virtuale) e impostare quanto segue nel passaggio 10:
- "Attiva aggiunta a caldo CPU"
- "Hot plug memoria"

6 Aggiungere vCenter agli strumenti ONTAP

- "Aggiungere istanze di vCenter Server" In ONTAP Tools Manager.

7 Aggiungi i backend di storage ai tool ONTAP

- "Configurare i ruoli e i privilegi degli utenti ONTAP" Utilizzo del file JSON incluso se non si utilizza admin.
- Se si intende assegnare SVM specifiche ai vCenter utilizzando la multitenancy di storage anziché le credenziali del cluster ONTAP in vCenter, attenersi alla seguente procedura:
- "cluster integrati" In ONTAP Tools Manager e associarli a vCenter.
- "SVM integrate" Negli strumenti ONTAP, l'interfaccia utente vCenter.
- Se **non** si utilizzano SVM multitenant in vCenter:
- "cluster integrati" Direttamente nell'interfaccia utente vCenter degli strumenti ONTAP. In alternativa, in questo scenario è possibile aggiungere SVM direttamente quando non si utilizzano i vVol.

8 Configurare i servizi delle appliance (opzionali)

- Per utilizzare vVol, è necessario prima "Modificare le impostazioni dell'appliance e attivare il servizio VASA". Allo stesso tempo, rivedere i due elementi seguenti.
- Se si prevede di utilizzare vVol in produzione, "abilita l'alta disponibilità" con i due indirizzi IP opzionali sopra indicati.
- Se si prevede di utilizzare l'adattatore di replica dello storage (SRA, Storage Replication Adapter) degli

strumenti ONTAP per VMware Site Recovery Manager o Live Site Recovery, "Attivare i servizi SRA".

9 **Certificati (opzionali)**

- Per VMware, i certificati CA firmati sono necessari se si utilizzano vVol con più vCenter.
- Servizi VASA _____
- Servizi amministrativi _____\

10 **Altre attività successive all'implementazione**

- Crea regole di affinità per le macchine virtuali in un'implementazione ha.
- Se si utilizza l'ha, lo storage vMotion si nodi due e tre per separare i datastore (facoltativo, ma consigliato).
- "utilizzare gestisci certificati" In ONTAP Tools Manager per installare tutti i certificati CA firmati richiesti.
- Se SRA è stato abilitato per SRM/VLSR per proteggere i datastore tradizionali, "Configurare SRA sull'appliance VMware Live Site Recovery".
- Configurare backup nativi per "RPO prossimo allo zero".
- Configurare backup regolari su altri supporti di archiviazione.

Utilizzo di vVol con ONTAP

La chiave per l'utilizzo di vVol con NetApp sono i tool ONTAP per VMware vSphere, che funge da interfaccia provider VASA (vSphere API for Storage Awareness) per i sistemi ONTAP 9 di NetApp.

Gli strumenti ONTAP includono inoltre estensioni dell'interfaccia utente vCenter, servizi API REST, adattatori di replica storage per VMware Site Recovery Manager/Live Site Recovery, strumenti di monitoraggio e configurazione host e una serie di report che consentono di gestire al meglio l'ambiente VMware.

Prodotti e documentazione

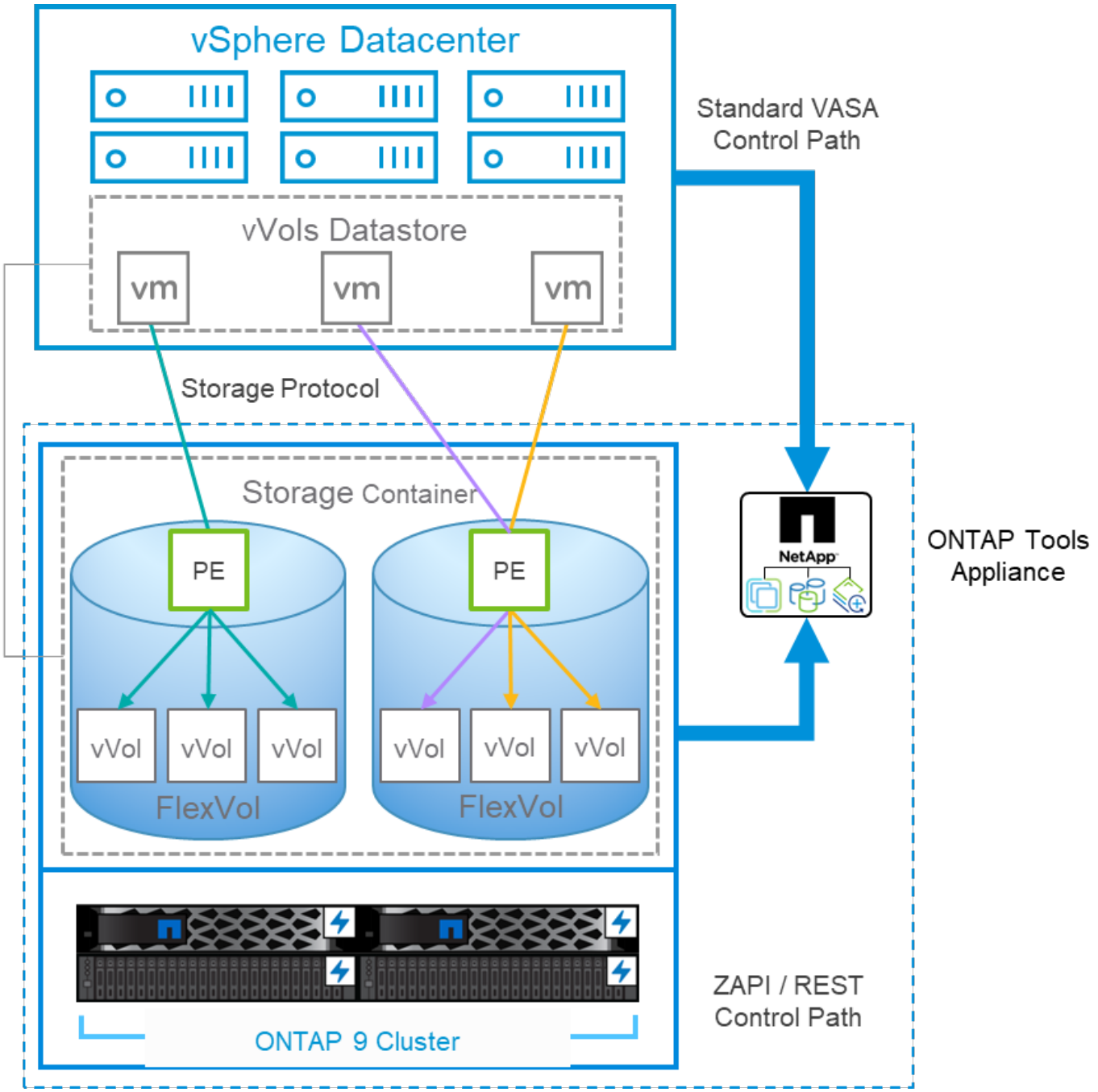
La licenza di ONTAP One include tutte le licenze necessarie per l'utilizzo di vVol con i sistemi ONTAP. L'unico requisito aggiuntivo è il ONTAP gratuito strumenti OVA, che agisce come il fornitore VASA. In un ambiente vVol, il software VASA Provider traduce le funzionalità di array in attributi basati su policy che possono essere sfruttati attraverso le API VASA senza che l'amministratore vSphere debba sapere come le funzionalità vengono gestite dietro le quinte. Ciò consente un consumo dinamico della capacità dello storage allocata in base alle policy, eliminando la necessità di creare manualmente datastore tradizionali e di gestire i rispettivi tassi di consumo dello storage individuale. In breve, i vVol eliminano tutta la complessità della gestione dello storage Enterprise e lo astraggono dall'amministratore vSphere, consentendo loro di concentrarsi sul layer di virtualizzazione.

Per i clienti che utilizzano VMware Cloud Foundation con vSAN, è possibile aggiungere vVol a qualsiasi dominio di gestione o carico di lavoro come storage supplementare. VVol si integra perfettamente con vSAN attraverso un framework di gestione comune basato su criteri di storage.

La famiglia di strumenti ONTAP di nuova generazione release 10 modernizza le funzionalità precedenti con un'architettura scalabile, containerizzata e basata su microservizi, che può essere implementata tramite una semplice appliance in formato OVA su ESXi. Strumenti ONTAP 10 combina tutte le funzionalità di tre precedenti appliance e prodotti in un'unica implementazione. Per la gestione di vVol, userai le estensioni intuitive dell'interfaccia utente di vCenter o le API REST per il provider VASA degli strumenti ONTAP. Tenere

presente che il componente SRA è destinato a datastore tradizionali; VMware Site Recovery Manager non utilizza SRA per vVol.

ONTAP mette a disposizione l'architettura provider VASA quando si utilizza iSCSI o FCP con sistemi unificati



Installazione del prodotto

Per le nuove installazioni, implementa l'appliance virtuale nel tuo ambiente vSphere. Una volta implementato, potrai accedere all'interfaccia utente del manager o utilizzare le API REST per scalare in verticale o in orizzontale l'implementazione, gli vCenter integrati (che registrano il plug-in con vCenter), i sistemi storage integrati e associare i sistemi storage ai vCenter. L'integrazione dei sistemi storage nell'interfaccia utente del gestore dei tool ONTAP e l'associazione dei cluster ai vCenter sono necessari solo se intendi utilizzare la multi-tenancy sicura con SVM dedicate, altrimenti potrai semplicemente integrare i cluster storage desiderati nelle estensioni dell'interfaccia utente di vCenter dei tool ONTAP o utilizzando le API REST.

Fare riferimento a "Implementazione dello storage vVol" nel presente documento, o "Tool ONTAP per la documentazione di VMware vSphere".

È consigliabile archiviare gli strumenti ONTAP e le appliance vCenter sui tradizionali datastore NFS o VMFS, in modo da evitare conflitti di interdipendenza. Poiché sia i tool vCenter che ONTAP devono comunicare tra loro durante le operazioni dei vVol, non installare o spostare le appliance dei tool ONTAP o le appliance vCenter Server (VCSA) nello storage vVol che stanno gestendo. In questo caso, il riavvio delle appliance per gli strumenti vCenter o ONTAP può causare un'interruzione dell'accesso al piano di controllo e l'impossibilità di avviare l'appliance.

Gli aggiornamenti in-place degli strumenti ONTAP sono supportati utilizzando il file ISO di aggiornamento disponibile per il download all'indirizzo "Tool ONTAP per VMware vSphere 10 - Download" sul sito di supporto NetApp (è richiesto l'accesso). Seguire le "Aggiornamento dai tool ONTAP per VMware vSphere 10.x alla 10,3" istruzioni della guida per aggiornare l'apparecchio. È inoltre possibile eseguire un aggiornamento affiancato dagli strumenti ONTAP 9,13 a 10,3. Fare riferimento a "Migrazione dai tool ONTAP per VMware vSphere 9.x a 10,3" per un'analisi più approfondita dell'argomento.

Per il dimensionamento dell'appliance virtuale e la comprensione dei limiti di configurazione, fare riferimento alla sezione "Limiti di configurazione per l'implementazione dei tool ONTAP per VMware vSphere"

Documentazione del prodotto

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

"Tool ONTAP per la documentazione di VMware vSphere"

Inizia subito

- "Note di rilascio"
- "Panoramica sui tool ONTAP per VMware vSphere"
- "Implementare gli strumenti ONTAP"
- "Aggiornare i tool ONTAP"

Utilizzare gli strumenti ONTAP

- "Eseguire il provisioning degli archivi dati"
- "Configurare il controllo degli accessi in base al ruolo"
- "Configurare la disponibilità elevata"
- "Modificare le impostazioni dell'host ESXi"

Proteggere e gestire i datastore

- "Configurare vSphere Metro Storage Cluster (vMSC) utilizzando gli strumenti ONTAP e la sincronizzazione attiva SnapMirror"
- "Proteggere le macchine virtuali" Con SRM
- "Monitorare cluster, datastore e macchine virtuali"

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 e le LUN di vVol, inclusi latenza, IOPS, throughput e altro ancora. È attivata per impostazione predefinita quando si utilizzano tutte le versioni attualmente supportate di ONTAP 9. Si noti che dopo la configurazione iniziale possono essere necessari fino a 30 minuti affinché i dati popolino la dashboard.

Altre 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"). Verificare sempre la "NetApp Hardware Universe" presenza di limiti aggiornati su numero e dimensioni di LUN, namespace 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 gli strumenti ONTAP sarà possibile creare automaticamente gli endpoint di protocollo in base alle necessità e creare volumi FlexVol (non richiesti con ASA R2) utilizzando le Best practice ONTAP. 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 risultare in una "situazione uova e pollo" se è necessario riavviare gli apparecchi perché non sarà in grado di riassociare i loro vVol durante il riavvio. È possibile memorizzarli in un datastore vVol gestito da un diverso tool ONTAP e da una distribuzione vCenter.

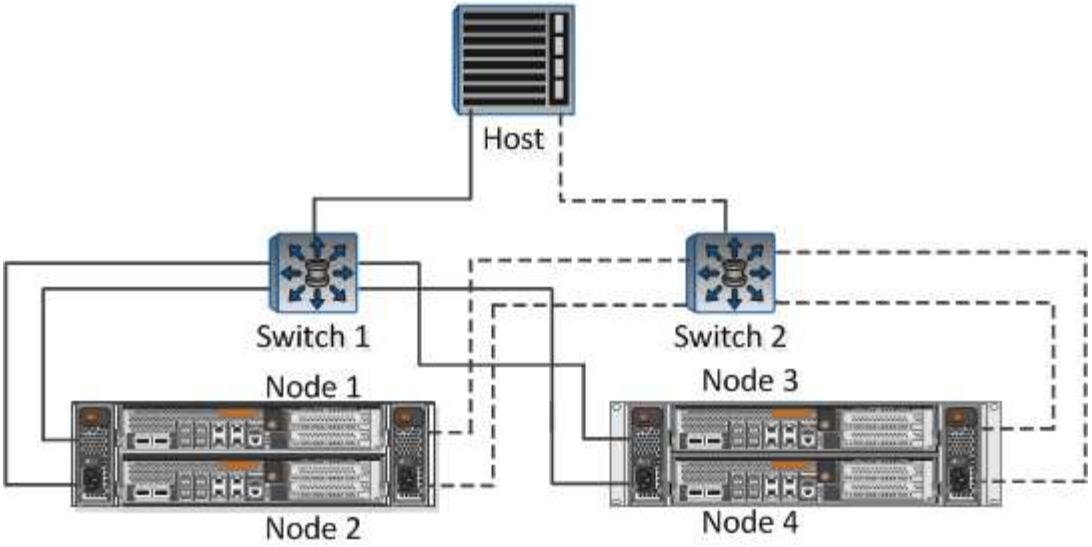
Evitare le operazioni vVol in diverse release di ONTAP.

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.

Zona del fabric Fibre Channel prima di utilizzare FCP per vVol.

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*"

Pianificate i vostri volumi FlexVol di backup in base alle vostre esigenze.

Per i sistemi diversi da ASA R2, può essere conveniente 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.

Con i sistemi ASA R2, questa complessità viene rimossa dal momento che il concetto di un volume o aggregato viene astratto dall'utente. Il posizionamento dinamico viene gestito automaticamente e gli endpoint del protocollo vengono creati in base alle necessità. È possibile creare automaticamente al volo endpoint di protocollo aggiuntivi qualora sia necessaria una maggiore scalabilità.

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

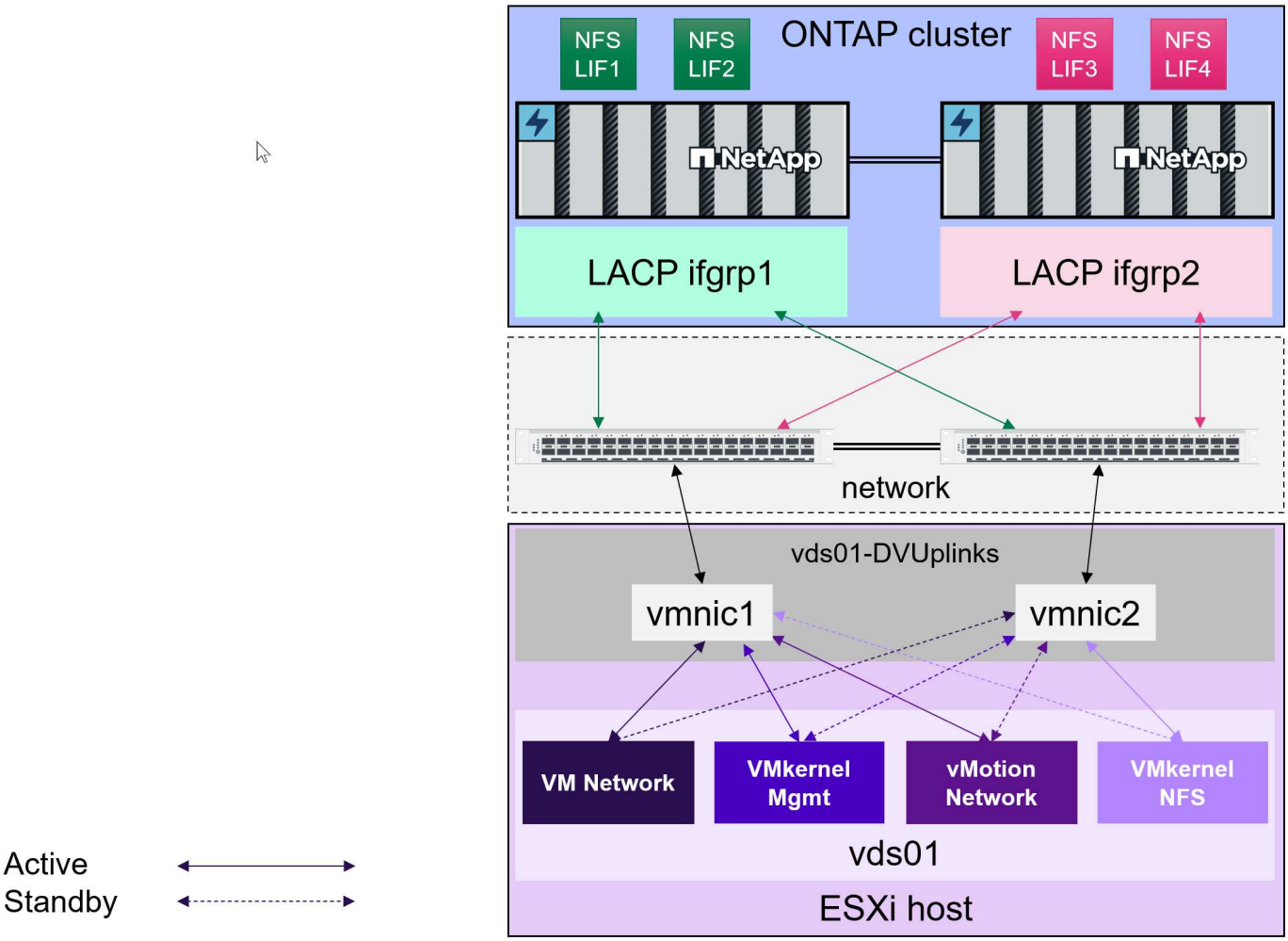
Per la prima volta disponibile nel provider VASA 7.1, è possibile utilizzare il massimo IOPS per limitare gli IOPS a un vVol specifico per un carico di lavoro sconosciuto, in modo da evitare impatti su altri carichi di lavoro più critici. Per ulteriori informazioni sulla gestione delle performance, vedere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

Assicurarsi di disporre di LIF di dati sufficienti. Fare riferimento alla "Implementazione dello storage vVol".

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 di vVol su sistemi AFF, ASA, ASA R2 e FAS

Seguire queste Best practice per la creazione dello storage vVol per le macchine virtuali.

Il provisioning dei datastore vVol implica diversi passaggi. I sistemi ASA R2 di NetApp sono progettati per carichi di lavoro VMware e offrono un'esperienza utente diversa dai sistemi ONTAP tradizionali. Quando si utilizzano i sistemi ASA R2, i tool ONTAP versione 10,3 o successive richiedono pochi passaggi per configurare e includere le estensioni dell'interfaccia utente e il supporto delle API REST ottimizzato per la nuova architettura storage.

Preparazione alla creazione di archivi dati vVol con gli strumenti ONTAP

È possibile saltare le prime due fasi del processo di distribuzione se si utilizzano già strumenti ONTAP per gestire, automatizzare e creare report sui sistemi di storage VMFS o tradizionali basati su NFS. Per la distribuzione e la configurazione degli strumenti ONTAP, è anche possibile fare riferimento a questa sezione completa"elenco di controllo".

1. Creare la Storage Virtual Machine (SVM) e la relativa configurazione del protocollo. Si noti che questo potrebbe non essere necessario per i sistemi ASA r2, poiché in genere dispongono già di un singolo SVM

per i servizi dati. Selezionerai NVMe/FC (solo strumenti ONTAP 9.13), NFSv3, NFSv4.1, iSCSI, FCP o una combinazione di queste opzioni. NVMe/TCP e NVMe/FC possono essere utilizzati anche per i tradizionali datastore VMFS con gli strumenti ONTAP 10.3 e versioni successive. È possibile utilizzare le procedure guidate di ONTAP System Manager o la riga di comando della shell del cluster.

- "Assegnazione dei Tier locali (aggregati) alle SVM" Per tutti i sistemi non ASA R2.
- 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. Un'unica LIF per nodo è sufficiente per i vVol basati su NFS, ma questa LIF deve essere protetta da un ifgroup LACP. Per ulteriori informazioni, fare riferimento alla "Panoramica sulla configurazione delle LIF" e "Combina le porte fisiche per creare gruppi di interfacce" alla.
- Almeno un LIF di gestione per SVM se si intende utilizzare credenziali con ambito SVM per i vCenter tenant.
- Se si prevede di utilizzare SnapMirror, assicurarsi che l'origine e la destinazione "Peering di cluster ONTAP e SVM"siano corrette.
- Per i sistemi non ASA r2, i volumi possono essere creati in questo momento, ma è consigliabile lasciare che la procedura guidata *Provision Datastore* negli strumenti ONTAP li crei. L'unica eccezione a questa regola si verifica se si prevede di utilizzare la replica vVols con VMware Site Recovery Manager e gli strumenti ONTAP 9.13. Questa operazione è più semplice da configurare con volumi FlexVol preesistenti con relazioni SnapMirror esistenti. Prestare attenzione a non abilitare QoS su alcun volume da utilizzare per vVols, poiché questa funzione è destinata a essere gestita dagli strumenti SPBM e ONTAP .

2. "Implementa i tool ONTAP per VMware vSphere" Utilizzando l'OVA scaricato dal sito di assistenza NetApp.
   - ONTAP Tools 10.0 e versioni successive supportano più server vCenter per appliance; non è più necessario distribuire un'appliance ONTAP Tools per vCenter.
     - Se si prevede di connettere più vCenter a una singola istanza degli strumenti ONTAP , è necessario creare e installare certificati firmati da una CA. Fare riferimento a "Gestire i certificati" per i gradini.
   - A partire dalla versione 10.3, gli strumenti ONTAP vengono distribuiti come appliance di piccole dimensioni a nodo singolo, adatte alla maggior parte dei carichi di lavoro non vVol.

- La migliore pratica consigliata è quella di "Tool ONTAP a scalabilità orizzontale" 10.3 e versioni successive alla configurazione ad alta disponibilità (HA) a 3 nodi per tutti i carichi di lavoro di produzione. Per scopi di laboratorio o di test, è possibile utilizzare una distribuzione a nodo singolo.
- La best practice consigliata per l'utilizzo vVols di produzione è quella di eliminare ogni singolo punto di errore. Creare regole anti-affinità per impedire che le VM degli strumenti ONTAP vengano eseguite insieme sullo stesso host. Dopo la distribuzione iniziale, si consiglia inoltre di utilizzare Storage vMotion per posizionare le VM degli strumenti ONTAP in diversi datastore. Per saperne di più "Utilizzo delle regole di affinità senza vSphere DRS" O "Creare una regola di affinità VM-VM". Dovresti anche pianificare backup frequenti e/o "utilizzare l'utilità di backup della configurazione integrata".

1. Configurare gli strumenti ONTAP 10,3 per il proprio ambiente.
   - "Aggiungere istanze di vCenter Server" Nell'interfaccia utente di ONTAP Tools Manager.
   - Gli strumenti ONTAP 10,3 supportano la multi-tenancy sicura. Se non hai bisogno della multi-tenancy sicura, puoi semplicemente "Aggiungi i tuoi cluster ONTAP" accedere al menu degli strumenti di ONTAP in vCenter, fare clic su *backend di archiviazione* e fare clic sul pulsante *add*.
   - In un ambiente multitenant sicuro in cui desideri delegare alcune Storage Virtual Machine (SVM) a

vCenter specifici, devi eseguire le seguenti operazioni.

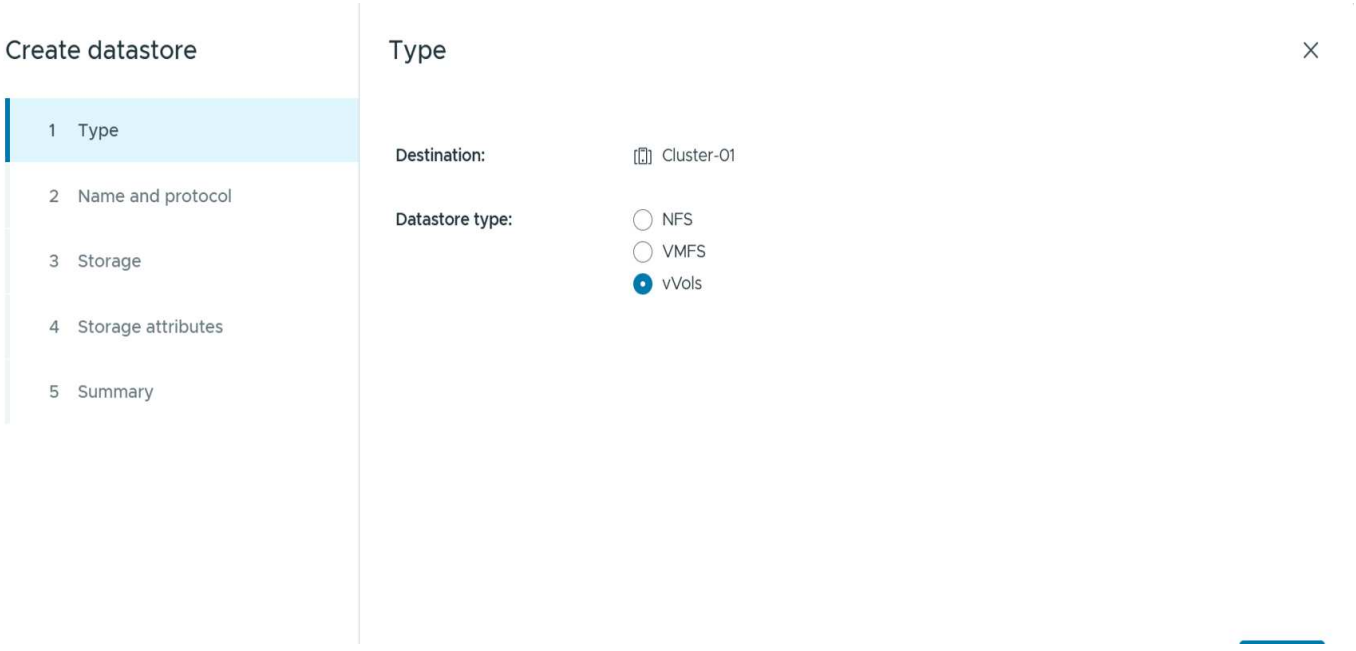
- Accedere all'interfaccia utente di ONTAP Tools Manager
- "Integrare il cluster di storage"
- "Associazione di un backend dello storage a un'istanza di vCenter Server"
- Fornire le credenziali SVM specifiche all'amministratore di vCenter, che aggiungerà quindi l'SVM come backend di archiviazione nel menu backend di archiviazione degli strumenti ONTAP in vCenter.

- È una Best practice creare ruoli RBAC per gli account storage.
- Gli strumenti ONTAP includono un file JSON contenente le autorizzazioni di ruolo necessarie per gli account di archiviazione degli strumenti ONTAP . È possibile caricare il file JSON su ONTAP System Manager per semplificare la creazione di ruoli e utenti RBAC.
- Per ulteriori informazioni sui ruoli RBAC di ONTAP, visitare il sito Web all'indirizzo "Configurare i ruoli e i privilegi degli utenti ONTAP".

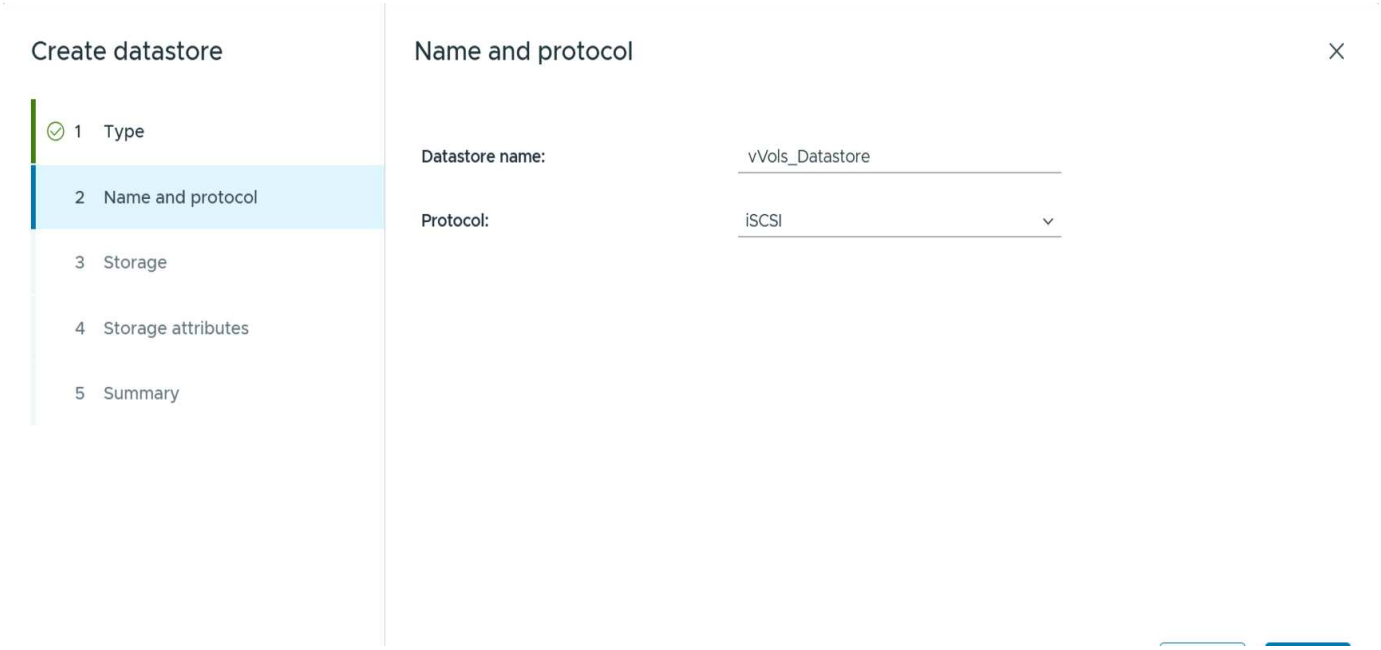
Il motivo per cui l'intero cluster deve essere integrato nell'interfaccia utente del gestore degli strumenti ONTAP è che molte delle API utilizzate per i vVols sono disponibili solo a livello di cluster.

Creazione di archivi dati vVol con gli strumenti ONTAP

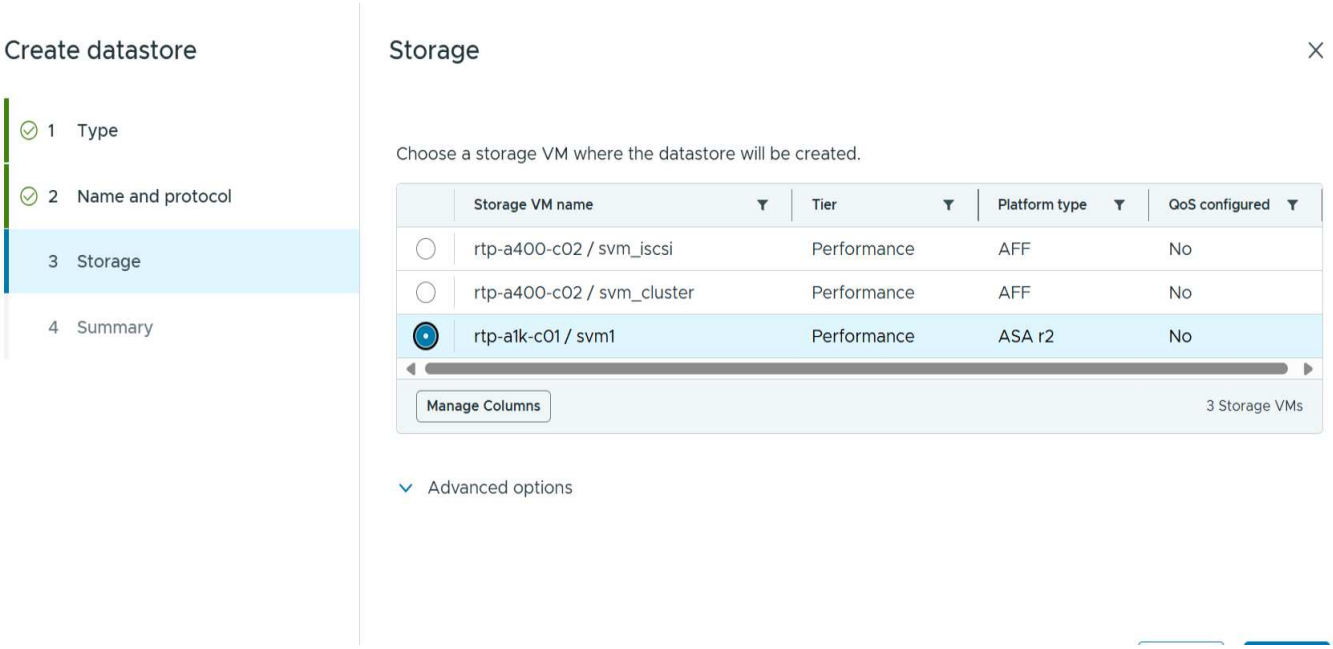
Fare clic con il pulsante destro del mouse sull'host, sul cluster o sul data center su cui si desidera creare il datastore vVols, quindi selezionare *ONTAP Tools* > *Provision Datastore*.



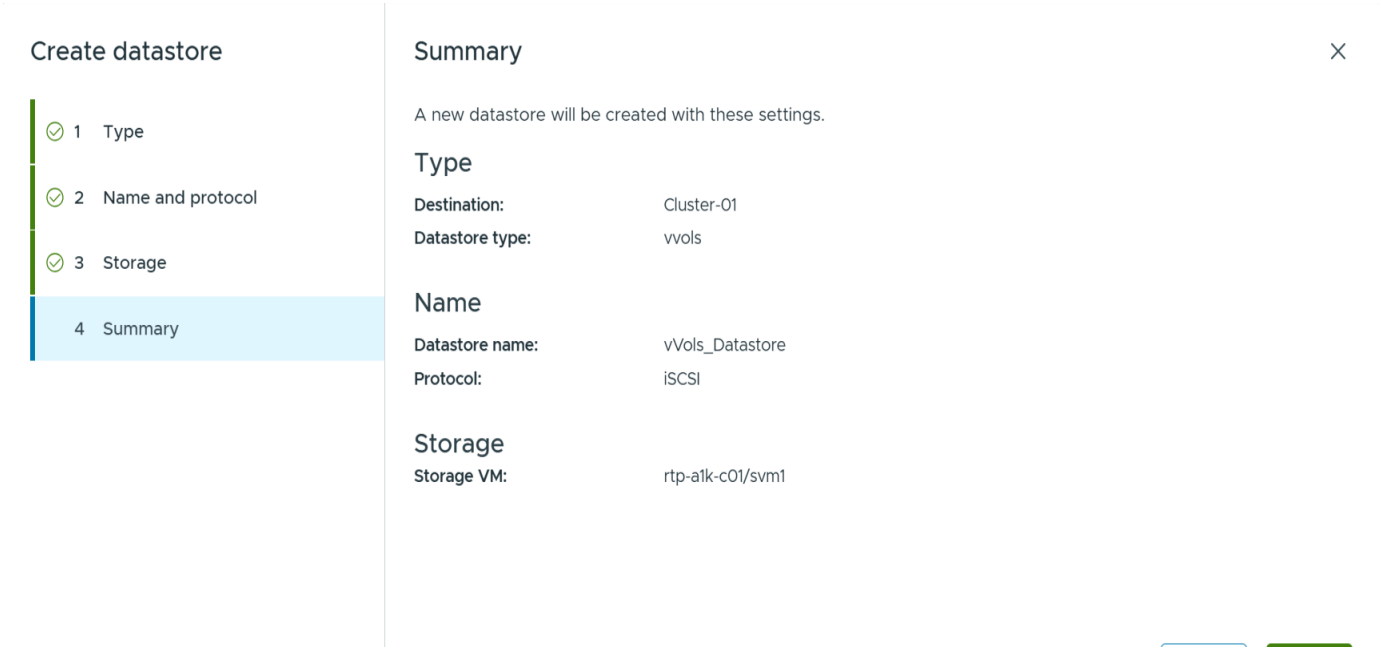
- Scegliere vVol e fornire un nome significativo e selezionare il protocollo desiderato. È anche possibile fornire una descrizione del datastore.
  - Strumenti ONTAP 10,3 con ASA R2.



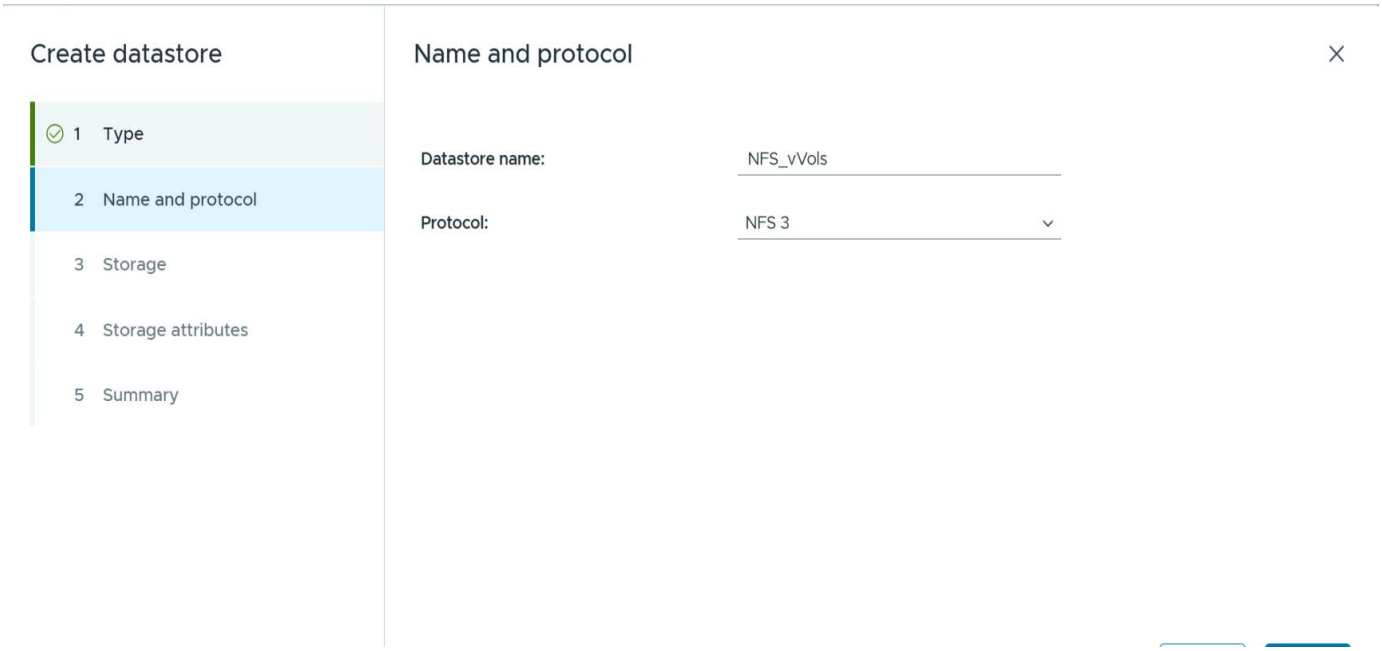
- Seleziona la SVM del sistema ASA R2 e fai clic su *next*.



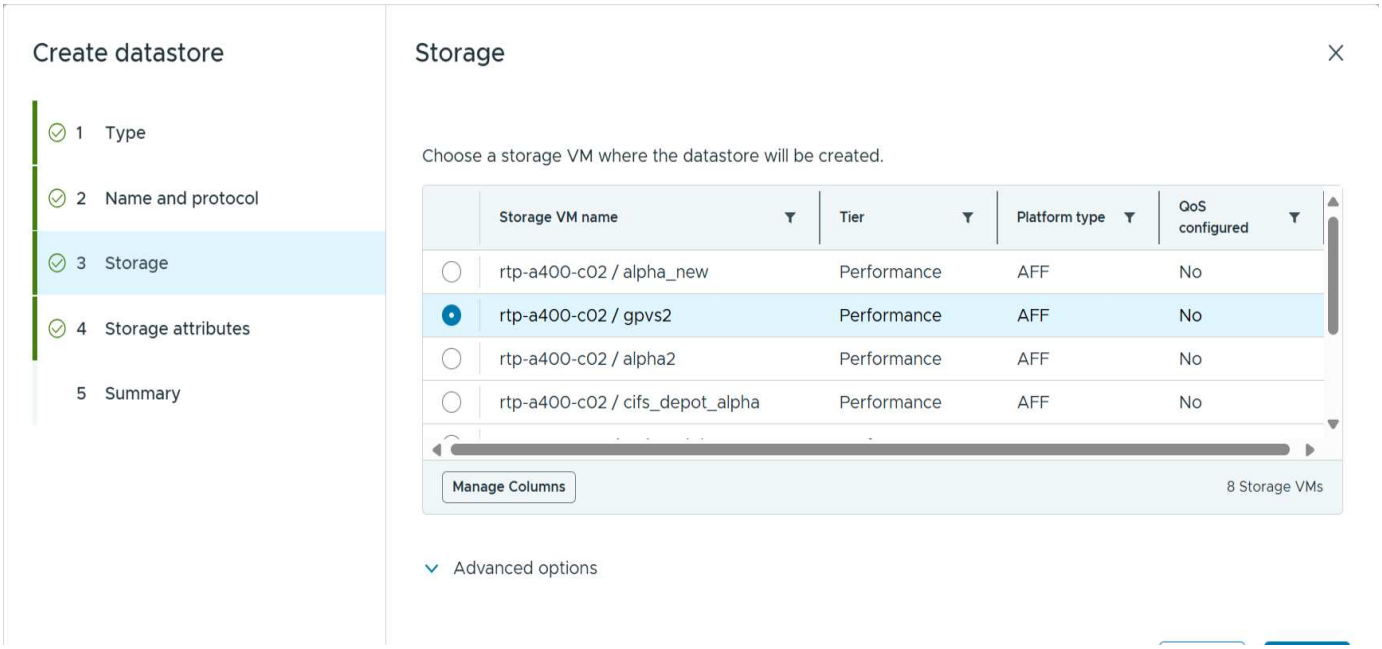
- Fare clic su *fine*



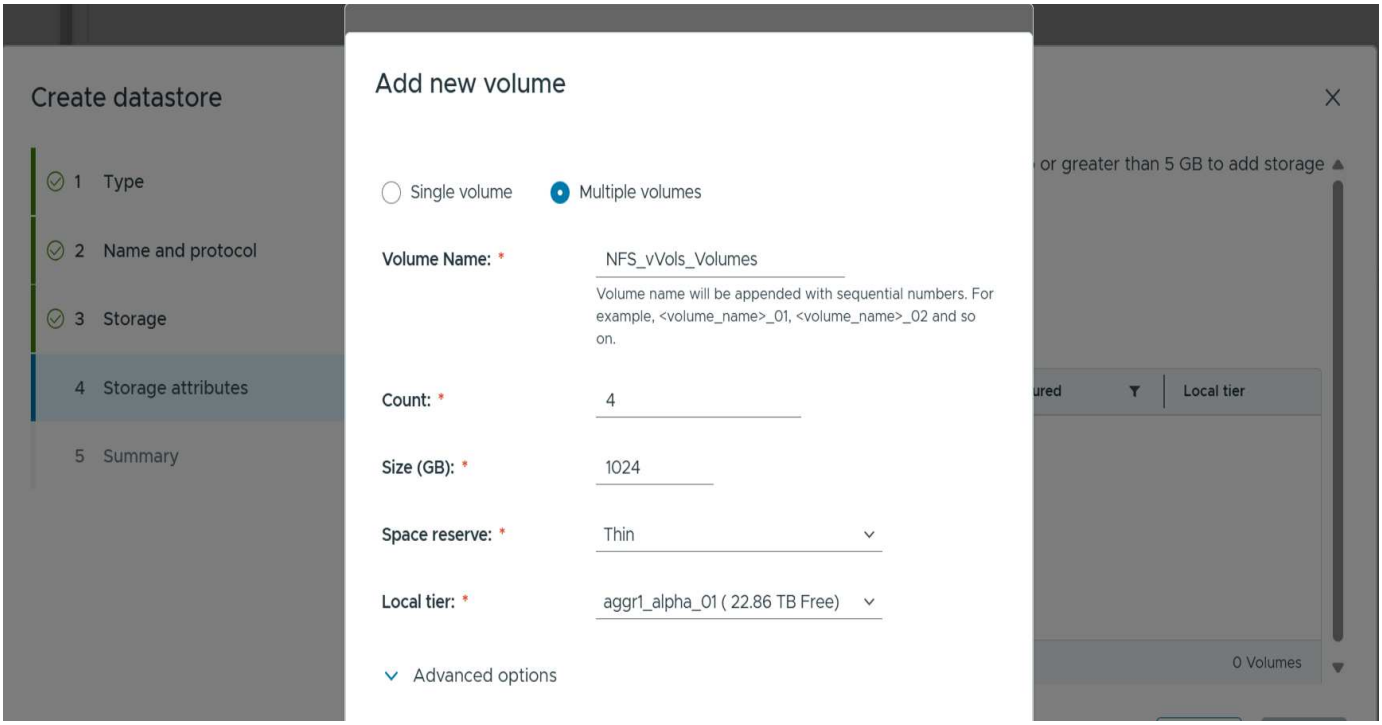
- È facile!
  - Strumenti ONTAP 10.3 con ONTAP FAS, AFF e ASA precedenti ad ASA r2.
- Selezionare il protocollo

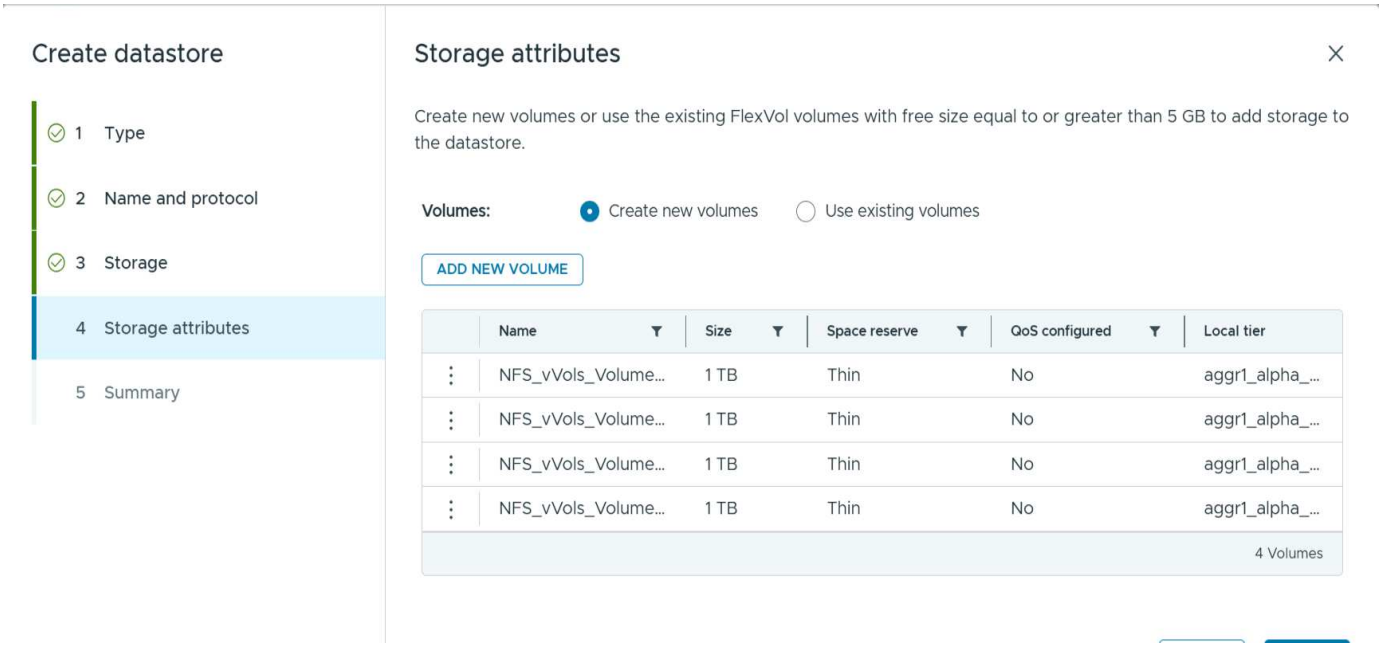


- Seleziona la SVM e fai clic su *next*.

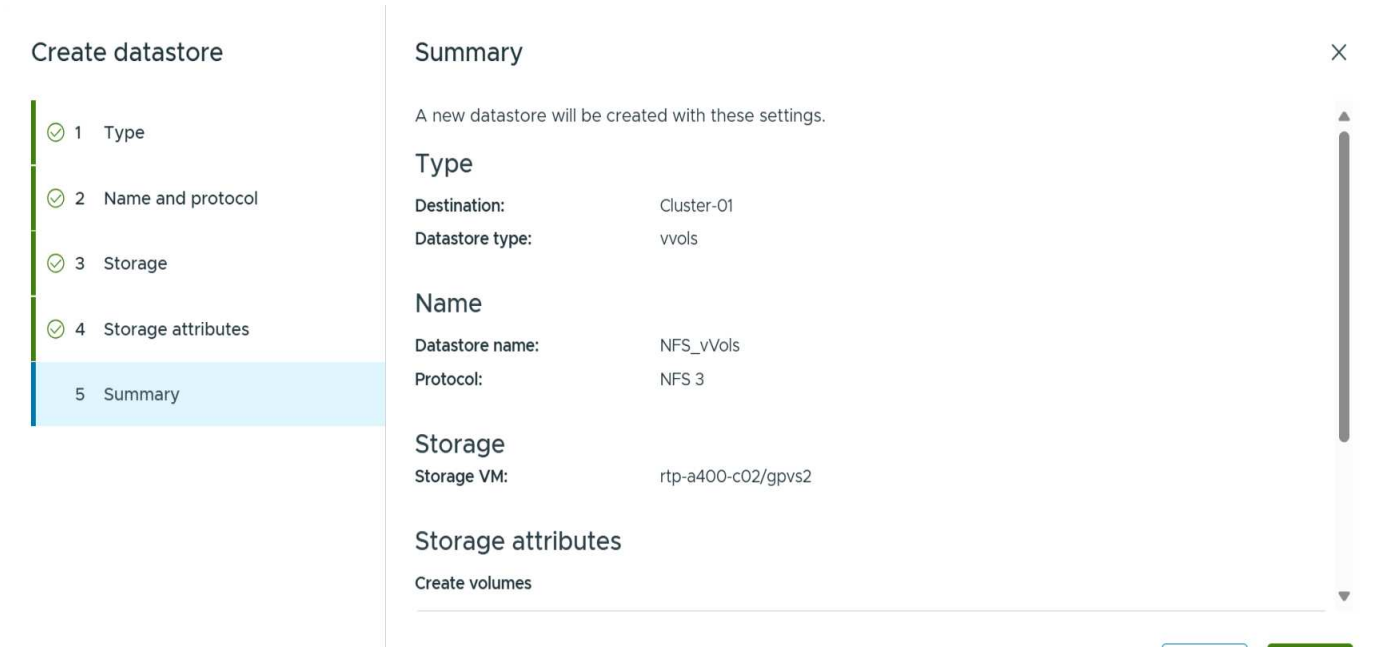


- Fare clic su *aggiungi nuovi volumi* o *usa volume esistente* e specificare gli attributi. Si noti che negli strumenti ONTAP 10.3 è possibile richiedere la creazione di più volumi contemporaneamente. È anche possibile aggiungere manualmente più volumi per bilanciarli nel cluster ONTAP . Clicca su *avanti*

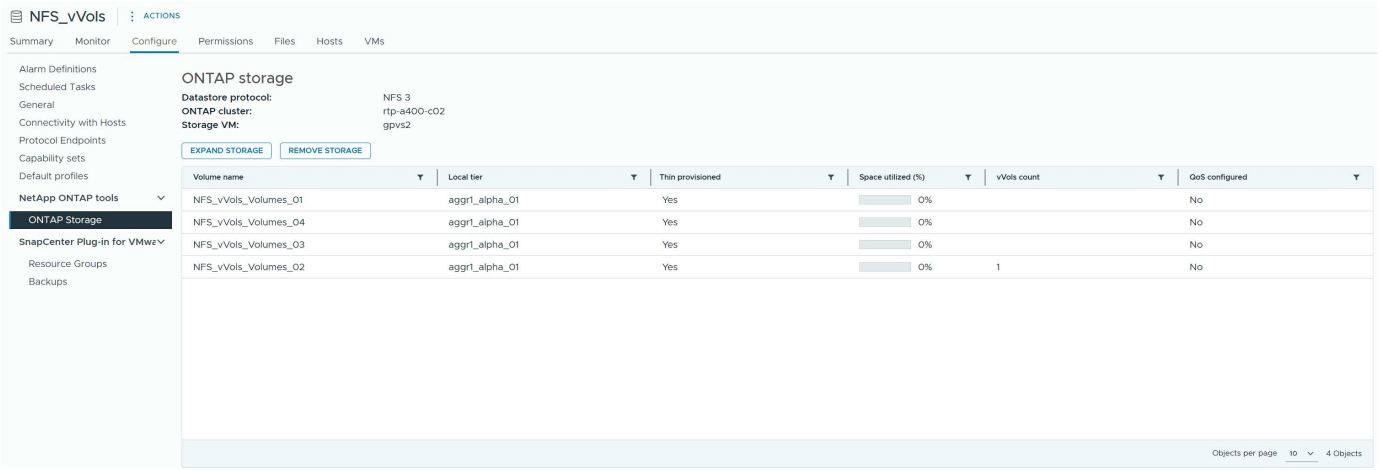




- Fare clic su *fine*



- I volumi assegnati possono essere visualizzati nel menu ONTAP tools della scheda Configure per l'archivio dati.



- Ora puoi creare policy storage delle macchine virtuali dal menu *Policies and Profiles* nell'interfaccia utente di vCenter.

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*. Quando richiesto, seleziona una policy storage della macchina virtuale che corrisponda al datastore vVol. È possibile eseguire l'offload delle operazioni di copia della migrazione con vSphere 6,0 e versioni successive per le migrazioni da VMFS SAN a vVol, ma non da VMDK NAS a vVol.

Gestione delle VM mediante policy

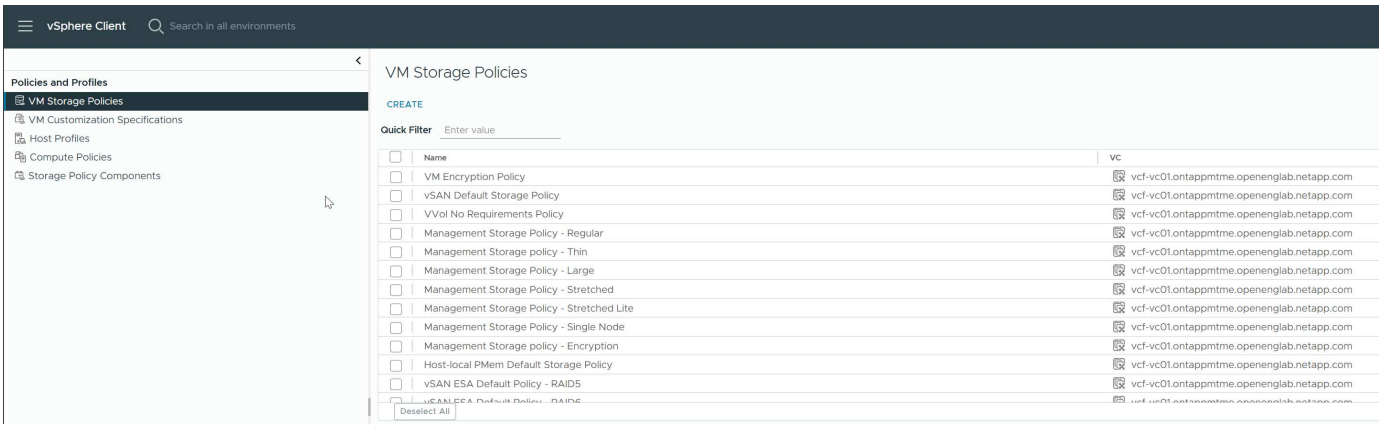
Per automatizzare il provisioning dello storage con la gestione basata su policy, è necessario creare policy di storage per le VM che siano compatibili con le capacità di storage desiderate.

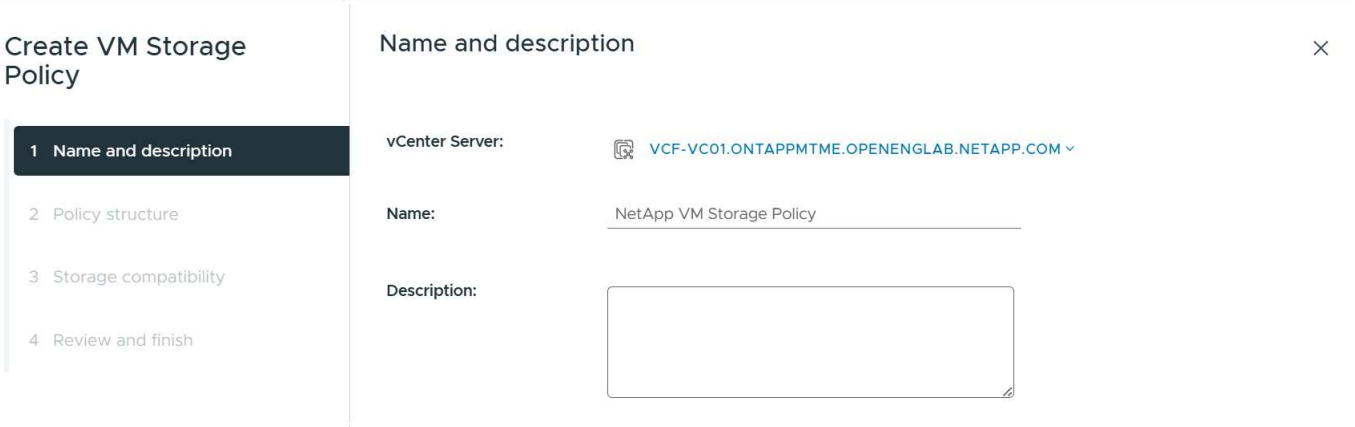
> Gli strumenti ONTAP 10,0 e versioni successive non utilizzano più i profili di funzionalità dello storage come le versioni precedenti. Le funzionalità di storage vengono invece definite direttamente nel criterio di storage delle macchine virtuali.

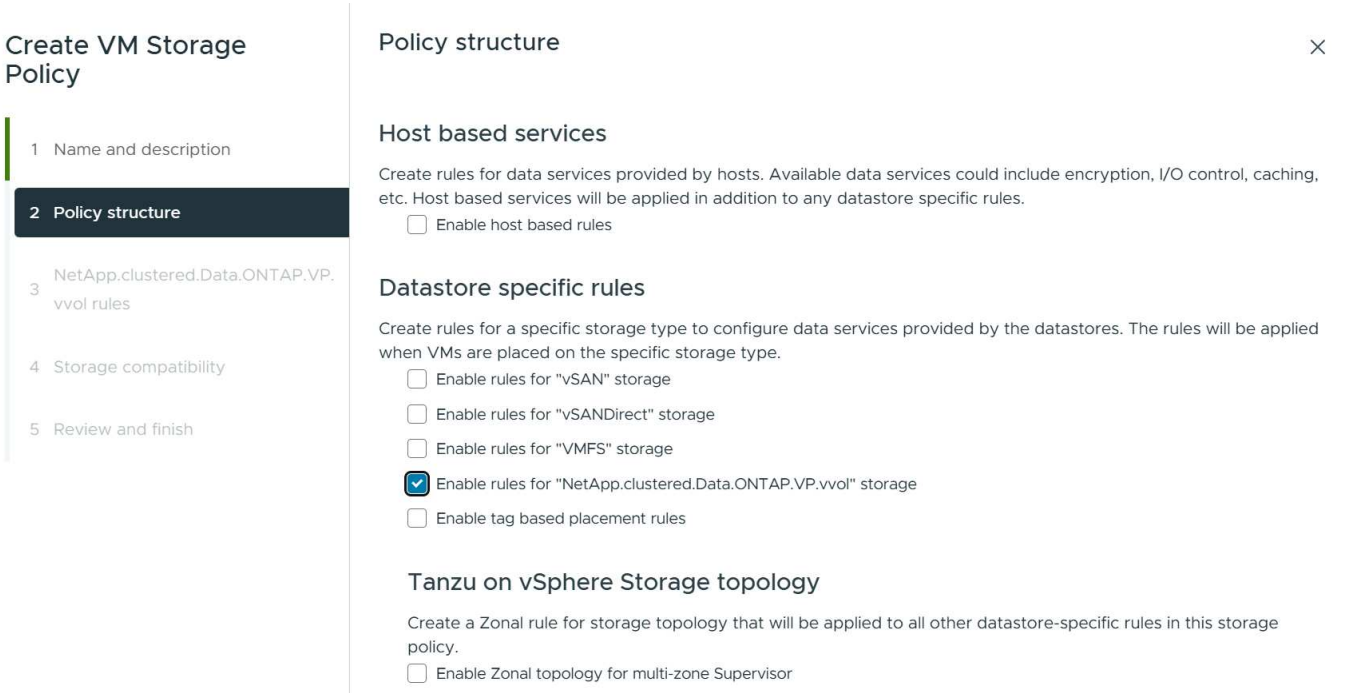
Creazione di policy di storage delle macchine virtuali

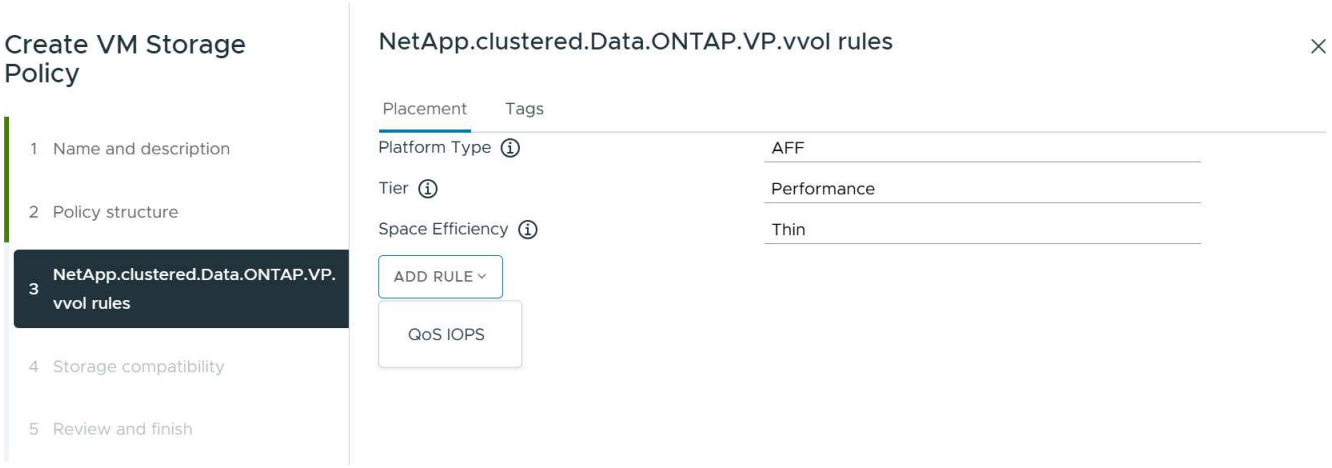
Le policy di archiviazione delle VM vengono utilizzate in vSphere per gestire funzionalità opzionali quali Storage I/O Control o vSphere Encryption. Vengono inoltre utilizzati con vVols per applicare specifiche capacità di archiviazione alla VM. Utilizzare il tipo di archiviazione "NetApp.clustered.Data. ONTAP .VP.vvol". Per un esempio di ciò con gli strumenti ONTAP VASA Provider, vedere il collegamento:vmware-vvols-ontap.html#Best Practices[esempio di configurazione di rete utilizzando vVols su NFS v3]. Le regole per l'archiviazione " NetApp.clustered.Data. ONTAP.VP.VASA10" devono essere utilizzate con datastore non basati su vVols.

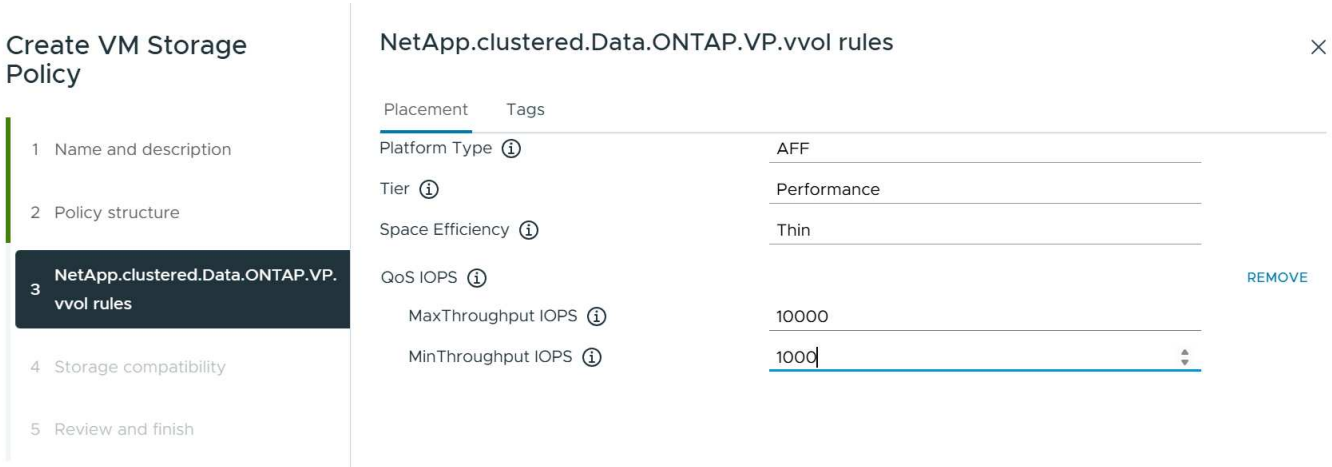
Una volta creato, il criterio storage può essere utilizzato per il provisioning di nuove macchine virtuali.

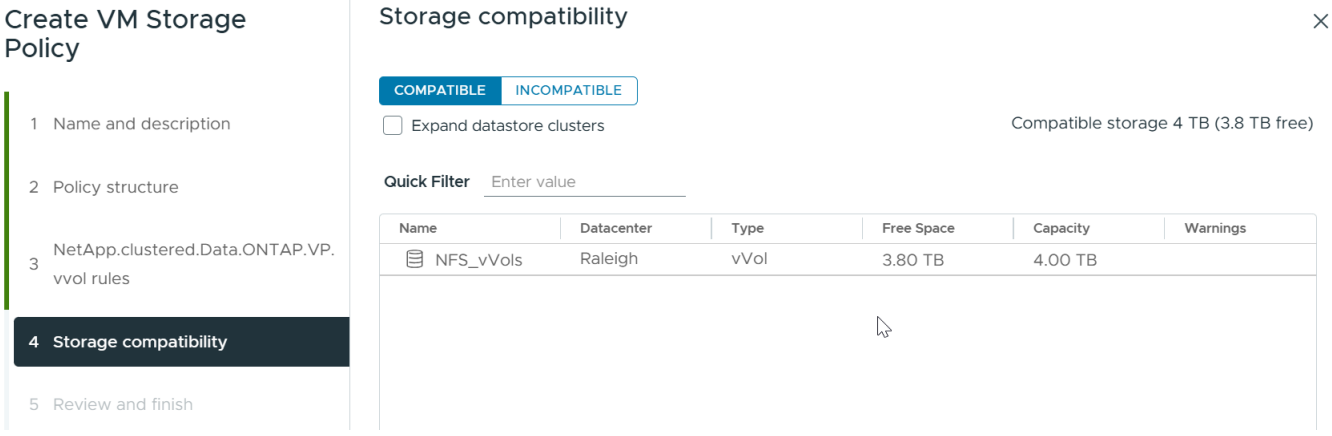

vSphere Client
Search in all environments
Policies and Profiles
VM Storage Policies
VM Customization Specifications
Host Profiles
Compute Policies
Storage Policy Components
VM Storage Policies
CREATE
Quick Filter
Enter value
Name
VC
VM Encryption Policy
vSAN Default Storage Policy
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
Management Storage Policy - Large
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Single Node
Management Storage policy - Encryption
Host-local PMem Default Storage Policy
vSAN ESA Default Policy - RAID5
vcf-vc01.ontappmtme.openenglab.netapp.com
Deselect All

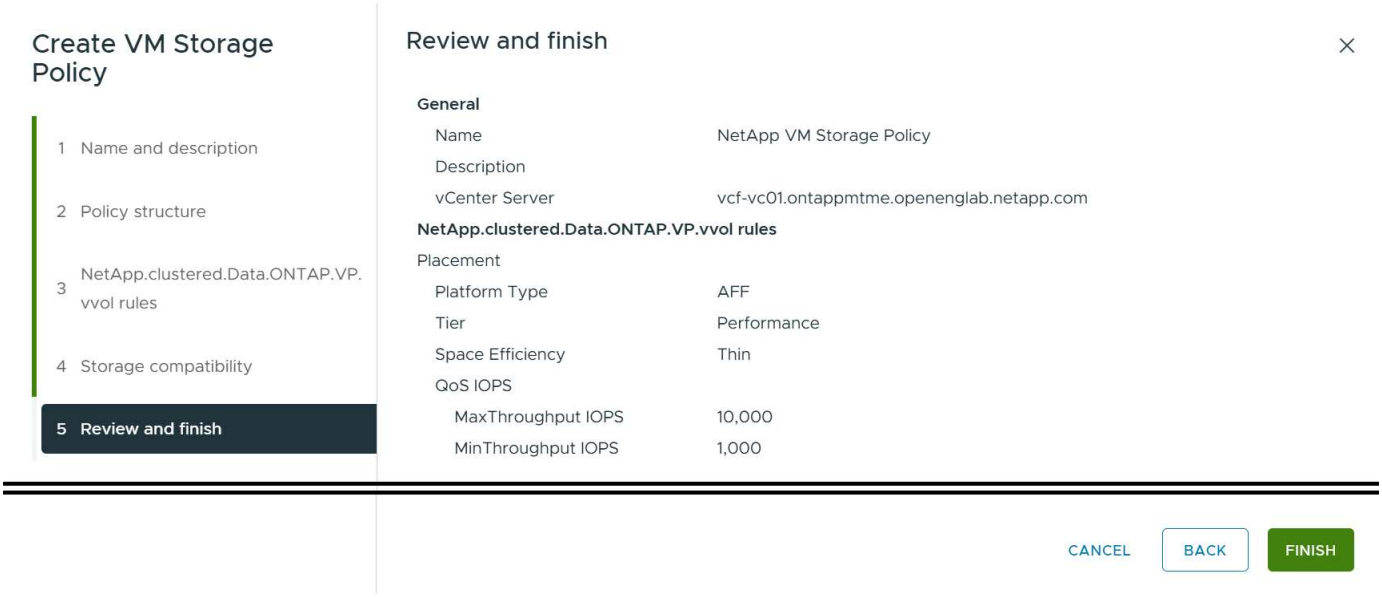

Create VM Storage Policy
1 Name and description
2 Policy structure
3 Storage compatibility
4 Review and finish
Name and description
vCenter Server:
VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM
Name:
NetApp VM Storage Policy
Description:


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP.vvol rules
4 Storage compatibility
5 Review and finish
Storage compatibility
COMPATIBLE
INCOMPATIBLE
Expand datastore clusters
Compatible storage 4 TB (3.8 TB free)
Quick Filter
Enter value
Name
Datacenter
Type
Free Space
Capacity
Warnings
NFS_vVols
Raleigh
vVol
3.80 TB
4.00 TB



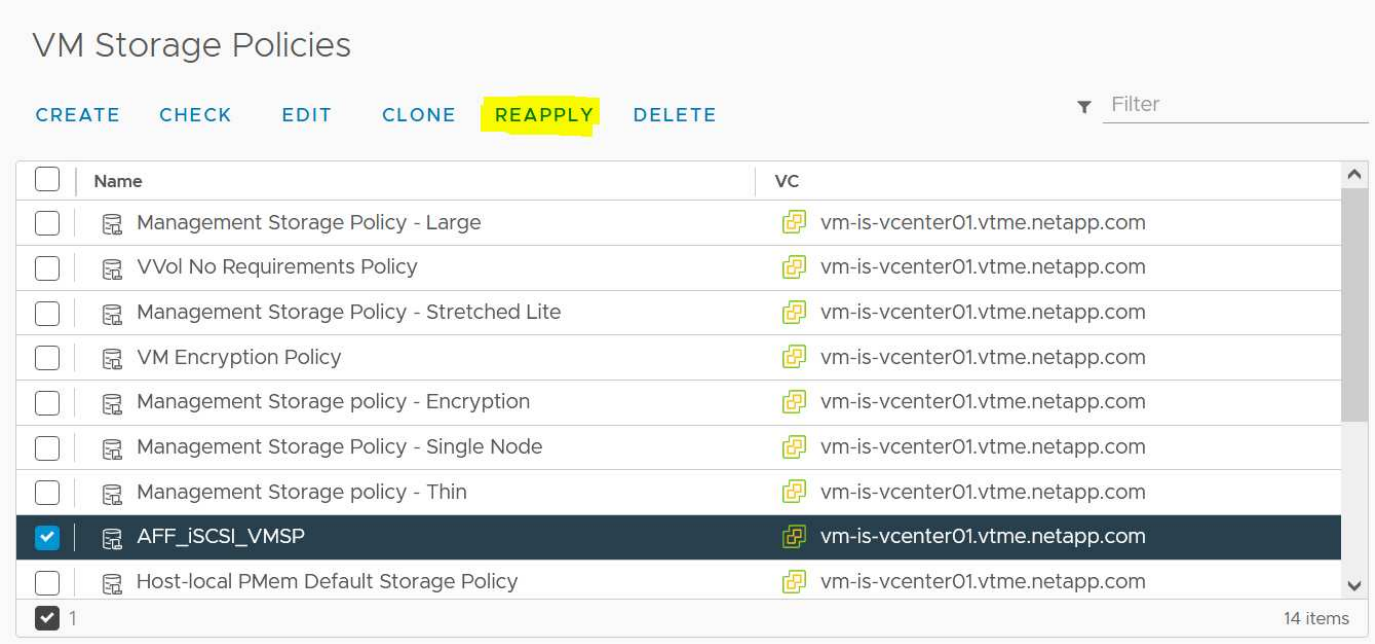
Gestione delle performance con tool ONTAP

I tool ONTAP utilizzano il proprio algoritmo di posizionamento bilanciato per posizionare un nuovo vVol nel BEST FlexVol volume, con sistemi ASA unificati o classici, o Storage Availability zone (SAZ) con sistemi ASA R2, all'interno di un datastore vVol. Il posizionamento si basa sulla corrispondenza tra lo storage di backup e il criterio di archiviazione della VM. In questo modo si garantisce che il datastore e lo storage di backup soddisfino i requisiti di performance specificati.

La modifica delle capacità di prestazione, come IOPS minimi e massimi, richiede una certa attenzione alla configurazione specifica.

- **IOPS minimi e massimi** possono essere specificati in un criterio VM.
  - La modifica degli IOPS nella policy non modificherà la QoS sui vVols finché la policy della VM non verrà riapplicata alle VM che la utilizzano. In alternativa, è possibile creare una nuova policy con gli IOPS desiderati e applicarla alle VM di destinazione. In genere, si consiglia di definire semplicemente criteri di archiviazione VM separati per diversi livelli di servizio e di modificare semplicemente i criteri di archiviazione VM sulla VM.
  - Le personalità ASA, ASA r2, AFF e FAS hanno impostazioni IOP diverse. Sia Min che Max sono disponibili su tutti i sistemi flash; tuttavia, i sistemi non AFF possono utilizzare solo le impostazioni Max IOPs.
- 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).

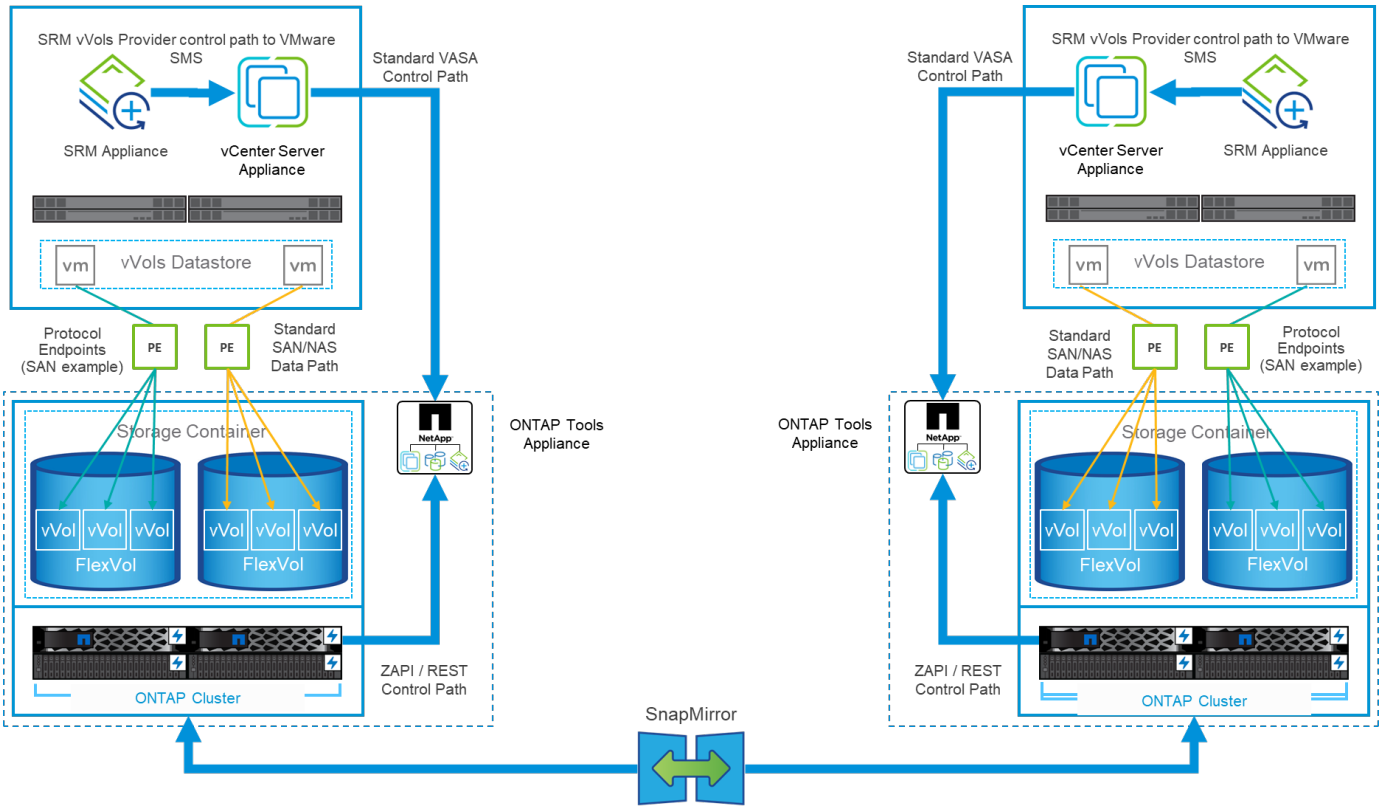
Questo requisito per uno strumento software è ancora più importante per gestire la replica di vVol. Sebbene alcuni aspetti possano essere gestiti da funzionalità native (ad esempio, le snapshot gestite da VMware di vVol vengono trasferite su ONTAP, che utilizza cloni di file o LUN rapidi ed efficienti), 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 release iniziale del supporto SRM con i tool ONTAP 9.7.1 era necessario creare in anticipo i volumi 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.

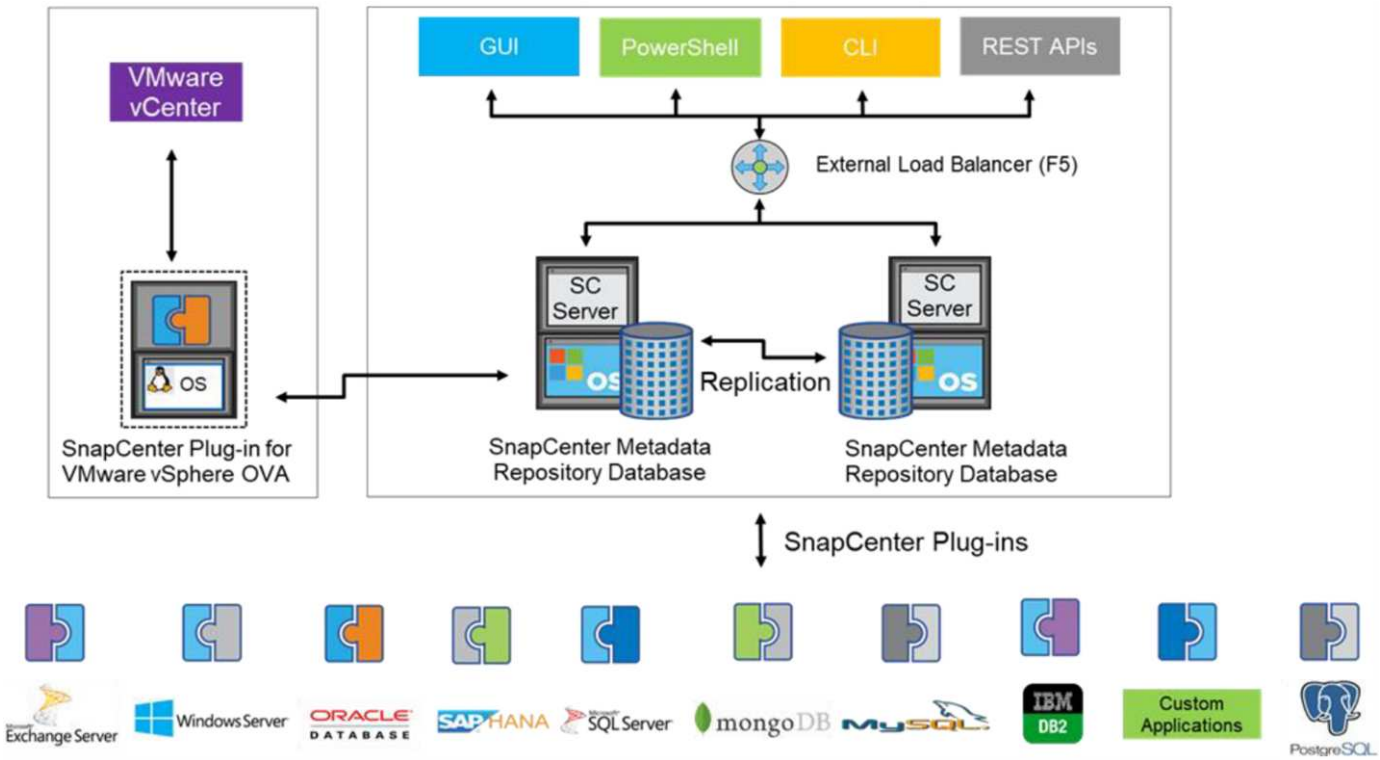
Il supporto di vSphere 8.0 è stato introdotto con SCV 4.7, che utilizzava un'architettura di plug-in locale isolata. Il supporto di vSphere 8.0U1 è stato aggiunto a SCV 4.8, che ha completato la transizione alla nuova architettura di plug-in remoto.

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"

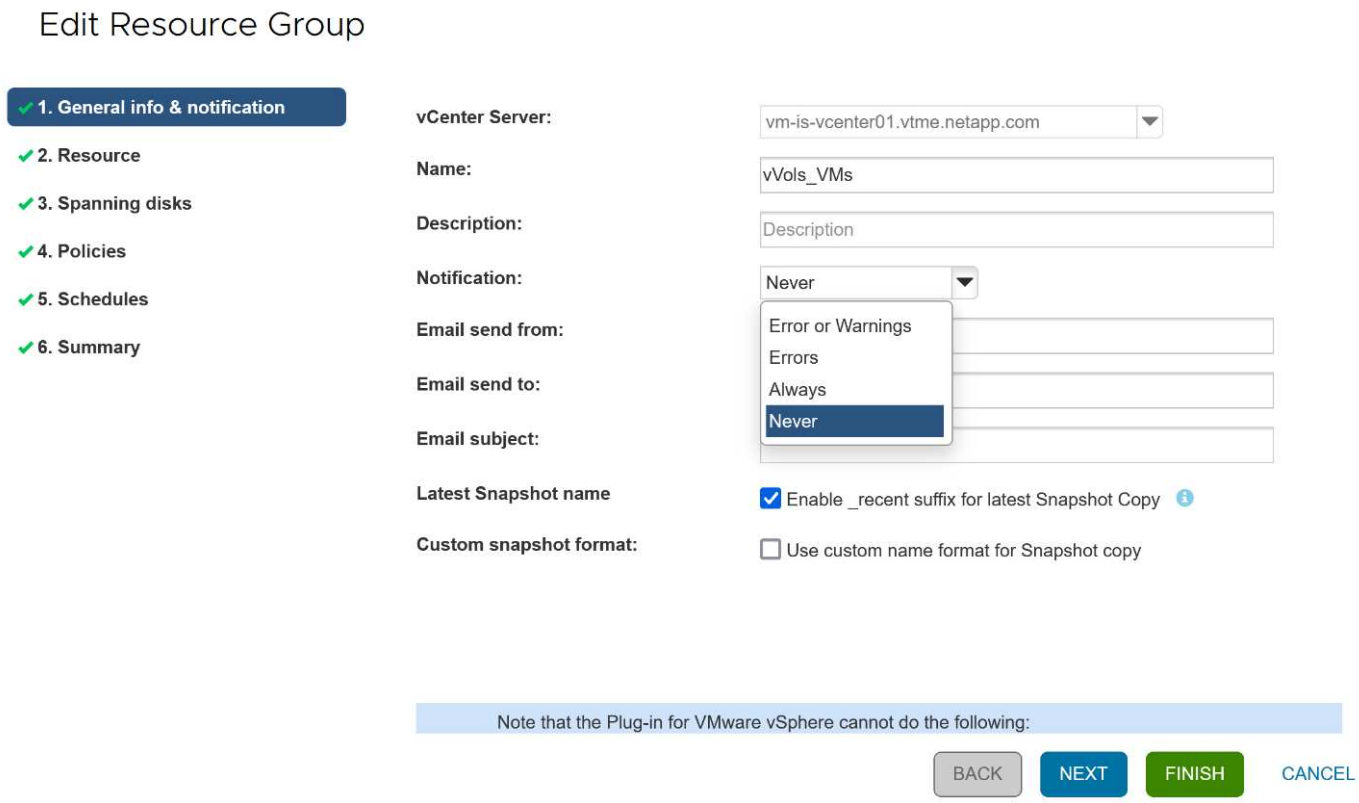
Per informazioni sulle API REST del plug-in SnapCenter per VMware vSphere, vedere "Plug-in SnapCenter per le API REST di VMware vSphere"

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 vasta gamma di articoli della Knowledge base per i prodotti di virtualizzazione NetApp, il sito di supporto NetApp offre anche una comoda landing page per il "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 con VMware di Broadcom*"

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 Live Site Recovery con ONTAP

ONTAP è una soluzione di storage leader per VMware vSphere e, più di recente, per Cloud Foundation, da quando ESX è stato introdotto nei data center moderni più di due decenni fa. NetApp continua a introdurre sistemi innovativi, come l'ultima generazione della serie ASA A, insieme a funzionalità come la sincronizzazione attiva SnapMirror . Questi progressi semplificano la gestione, migliorano la resilienza e riducono il costo totale di proprietà (TCO) della tua infrastruttura IT.

Questo documento presenta la soluzione ONTAP per VMware Live Site Recovery (VLSR), precedentemente nota come Site Recovery Manager (SRM), il software di disaster recovery (DR) leader del settore di VMware, comprese le informazioni più recenti sul prodotto e le best practice per semplificare la distribuzione, ridurre i rischi e semplificare la gestione continua.

> Questa documentazione sostituisce il rapporto 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 si concentra sulle funzionalità delle versioni recenti di ONTAP 9 utilizzate insieme agli strumenti ONTAP per VMware vSphere 10,4 (che include l'adattatore di replica dello storage NetApp [SRA] e il provider VASA [VP]), nonché su VMware Live Site Recovery 9.

Perché utilizzare ONTAP con VLSR o SRM?

Le piattaforme di gestione dati NetApp basate su ONTAP sono tra le soluzioni di storage più ampiamente adottate per VLSR. Le ragioni sono molteplici: una piattaforma di gestione dei dati sicura, ad alte prestazioni e

con protocollo unificato (NAS e SAN insieme) che fornisce efficienza di archiviazione senza pari nel settore, multi-tenancy, controlli della qualità del servizio, protezione dei dati con snapshot efficienti in termini di spazio e replica con SnapMirror. Tutto ciò sfrutta l'integrazione nativa multi-cloud ibrida per la protezione dei carichi di lavoro VMware e una miriade di strumenti di automazione e orchestrazione a portata di mano.

Quando si utilizza SnapMirror per la replica basata su array, si sfrutta una delle tecnologie più collaudate e mature di ONTAP. SnapMirror offre il vantaggio di trasferimenti di dati sicuri e altamente efficienti, copiando solo i blocchi del file system modificati e non intere VM o datastore. Anche questi blocchi sfruttano il risparmio di spazio, tramite deduplicazione, compressione e compattazione. I moderni sistemi ONTAP ora utilizzano SnapMirror indipendente dalla versione, consentendo flessibilità nella selezione dei cluster di origine e di destinazione. SnapMirror è diventato davvero uno degli strumenti più potenti disponibili per il disaster recovery.

Indipendentemente dal fatto che si utilizzino datastore tradizionali collegati a NFS, iSCSI o Fibre Channel (ora con supporto per datastore vVols), VLSR fornisce un'offerta proprietaria affidabile che sfrutta il meglio delle funzionalità ONTAP per il disaster recovery o la pianificazione e l'orchestrazione della migrazione del data center.

In che modo VLSR sfrutta ONTAP 9

VLSR 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 dei tool ONTAP, in precedenza noto come Virtual Storage Console (VSC), semplifica le funzionalità di gestione ed efficienza dello storage, aumenta la disponibilità e riduce i costi dello storage e l'overhead operativo, sia che si stia utilizzando SAN o NAS. Utilizza le Best practice per il provisioning degli archivi dati e ottimizza le impostazioni degli host ESXi per gli ambienti di storage a blocchi e NFS. Per tutti questi vantaggi, NetApp consiglia questo plug-in quando si utilizza vSphere con sistemi che eseguono ONTAP.
- Il ONTAP provider VASA supporta le API vStorage di VMware per il framework VASA (Storage Awareness). IL provider VASA connette vCenter Server a ONTAP per facilitare il provisioning e il monitoraggio dello storage delle macchine virtuali. In questo modo, è stato abilitato il supporto dei volumi virtuali VMware (vVol) e la gestione delle policy storage delle macchine virtuali e delle performance dei singoli vVol delle macchine virtuali. Fornisce inoltre allarmi per il monitoraggio della capacità e della conformità con i profili.
- SRA viene utilizzato insieme a VLSR 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 sia un server appliance SRA che adattatori SRA per il server Windows SRM e l'appliance VLSR.

Dopo aver installato e configurato gli adattatori SRA sul server VLSR per la protezione dei datastore non vVols, è possibile iniziare l'attività di configurazione dell'ambiente vSphere per il disaster recovery.

SRA fornisce un'interfaccia di comando e controllo per il server VLSR per la gestione dei volumi ONTAP FlexVol che contengono le macchine virtuali (VM) VMware, nonché la replica SnapMirror che le protegge.

VLSR può testare il tuo piano DR in modo non invasivo utilizzando la tecnologia proprietaria FlexClone di NetApp per creare cloni quasi istantanei dei tuoi datastore protetti nel tuo sito DR. VLSR crea un sandbox per effettuare test in modo sicuro, in modo che la tua organizzazione e i tuoi clienti siano protetti in caso di un vero disastro, dandoti fiducia nella capacità della tua organizzazione di eseguire un failover durante un disastro.

In caso di disastro reale o persino di migrazione pianificata, VLSR 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.

Mentre i sistemi ONTAP permettono di accoppiare le SVM nello stesso cluster per la replica SnapMirror, questo scenario non viene testato e certificato con VLSR. Pertanto, si consiglia di utilizzare solo SVM di cluster diversi quando si utilizza VLSR.

VLSR con ONTAP e altri casi di utilizzo: Cloud ibrido e migrazione

L'integrazione della distribuzione VLSR con le funzionalità avanzate di gestione dei dati ONTAP consente di ottenere prestazioni e scalabilità notevolmente migliorate rispetto alle opzioni di archiviazione locale. Ma più di questo, offre la flessibilità del cloud ibrido. Il cloud ibrido consente di risparmiare denaro suddividendo i blocchi di dati inutilizzati dal tuo array ad alte prestazioni al tuo hyperscaler preferito tramite FabricPool, che potrebbe essere un archivio S3 locale come NetApp StorageGRID. È inoltre possibile utilizzare SnapMirror per sistemi edge-based con ONTAP Select definito dal software o DR basato su cloud utilizzando "NetApp Storage su Equinix Metal"o altri servizi ONTAP ospitati.

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.

VLSR 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.

Utilizzare la versione più recente di ONTAP Tools 10

Gli strumenti ONTAP 10 forniscono miglioramenti significativi rispetto alle versioni precedenti, tra cui:

- failover dei test 8x volte più veloce*
- pulizia e protezione 2x volte più veloci*
- failover più veloce del 32%*
- Maggiore scalabilità
- Supporto nativo per layout di siti condivisi

*Questi miglioramenti si basano su test interni e possono variare in base all'ambiente in uso.

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.

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, devi creare un nuovo account SVM. "Configurare i ruoli e i privilegi degli utenti ONTAP" Utilizzando il file JSON incluso. Può essere utilizzato per account SVM o con ambito cluster.
- Poiché il plug-in dell'interfaccia utente vCenter, il provider VASA e il server SRA sono tutti microservizi completamente integrati, devi aggiungere storage all'adattatore SRA in SRM nello stesso modo in cui Aggiungi lo storage nell'interfaccia utente di vCenter per i tool 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, a meno che non si abbia la precedenza nel gestore dei tool ONTAP e non le si "cluster integrati" associ ai vCenter. 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.
- 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. Sebbene questa sia ancora la Best practice, non è più un requisito nelle moderne versioni 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 evitare che ONTAP elimini gli snapshot SnapMirror, configurare la funzionalità di eliminazione automatica degli snapshot su 'Try'.

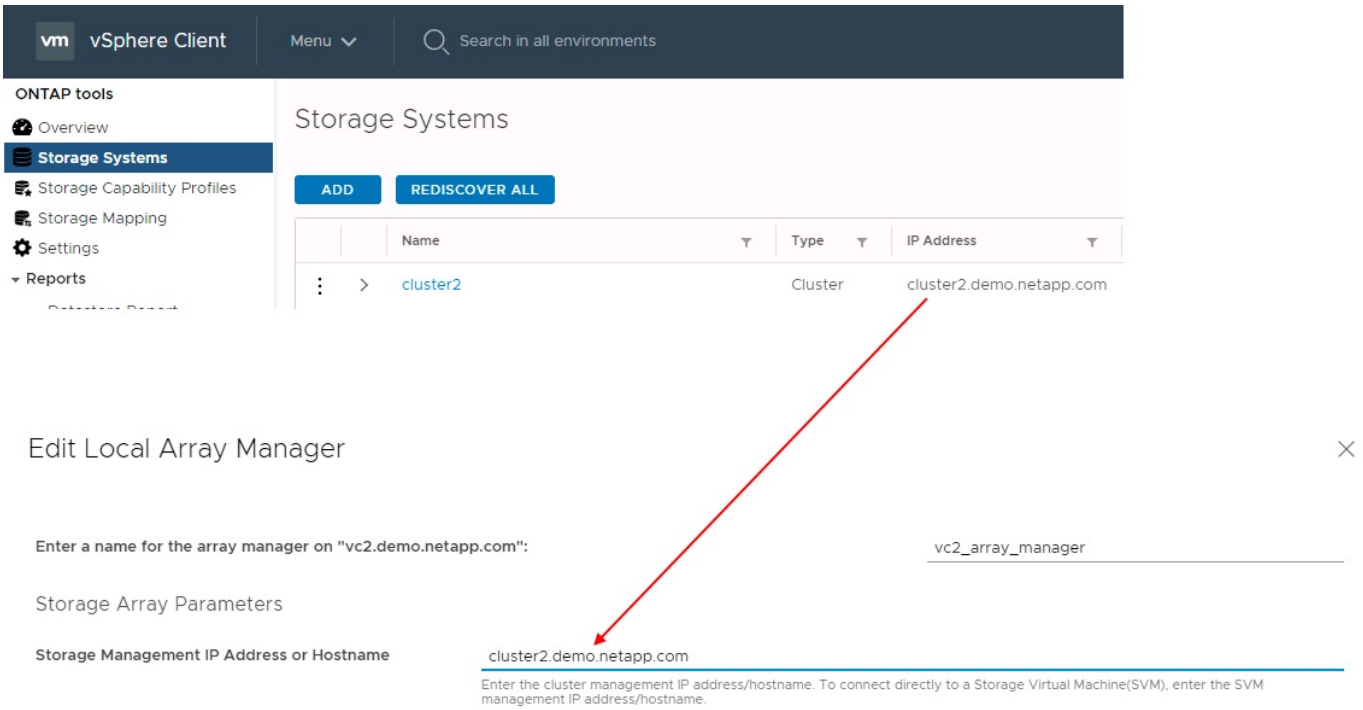
```
snap autodelete modify -volume -commitment try
```

- Il dimensionamento automatico del volume deve essere impostato su `grow` per i volumi che contengono datastore SAN e `grow_shrink` per i datastore NFS. Ulteriori informazioni su questo argomento sono disponibili all'indirizzo "Configurare i volumi per aumentare e ridurre automaticamente le dimensioni".
- 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.

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. 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 non prende in considerazione la deduplica aggregata.

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 si avvii prima del server Microsoft SQL, che deve essere online prima del server di applicazioni 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 failover di test ogni volta che viene apportata una modifica alla configurazione dello storage protetto delle macchine virtuali. 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 NetApp SVM viene trattato come un array univoco in Site Recovery Manager. VLSR supporta determinati layout di replicazione array-to-array (o SVM-to-SVM).

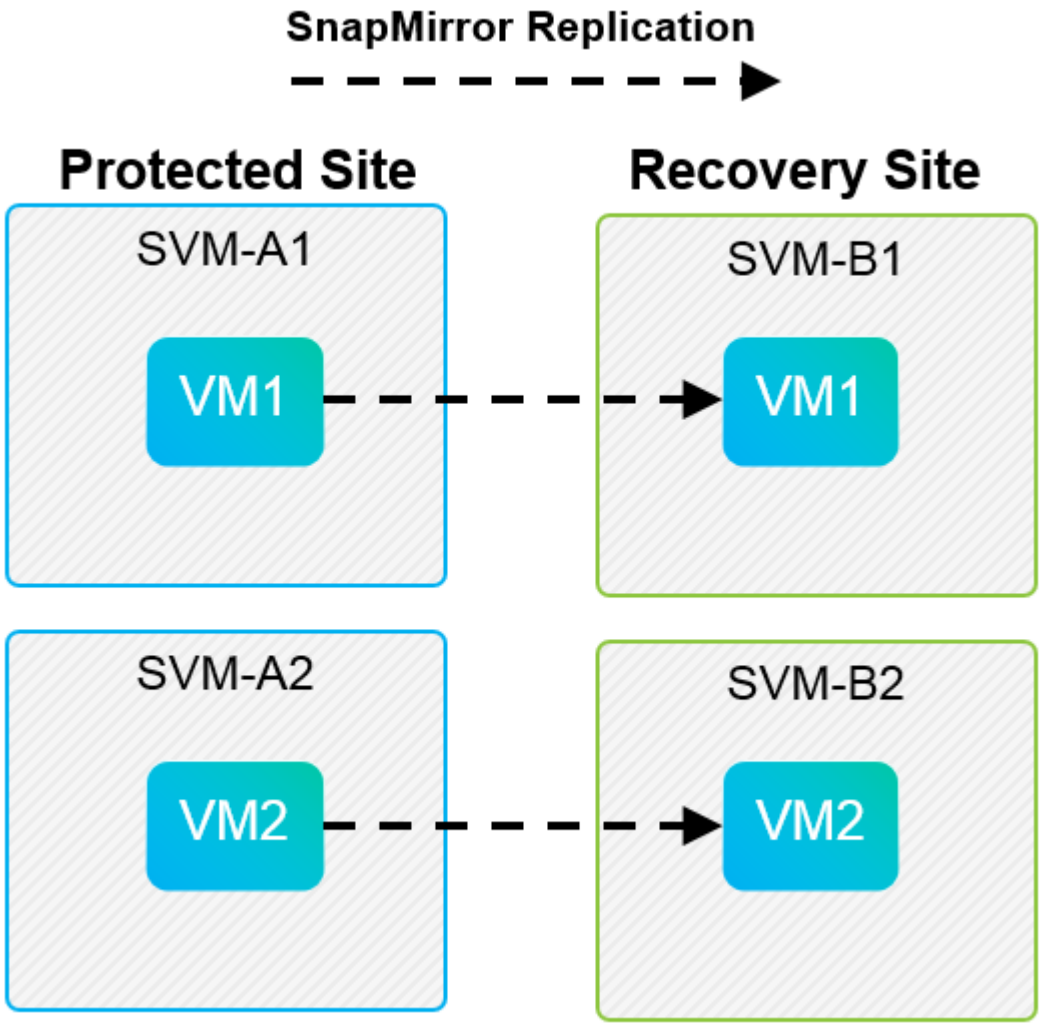
Una singola macchina virtuale non è in grado di gestire i dati (VMDK) o RDM) su più array VLSR per i seguenti motivi:

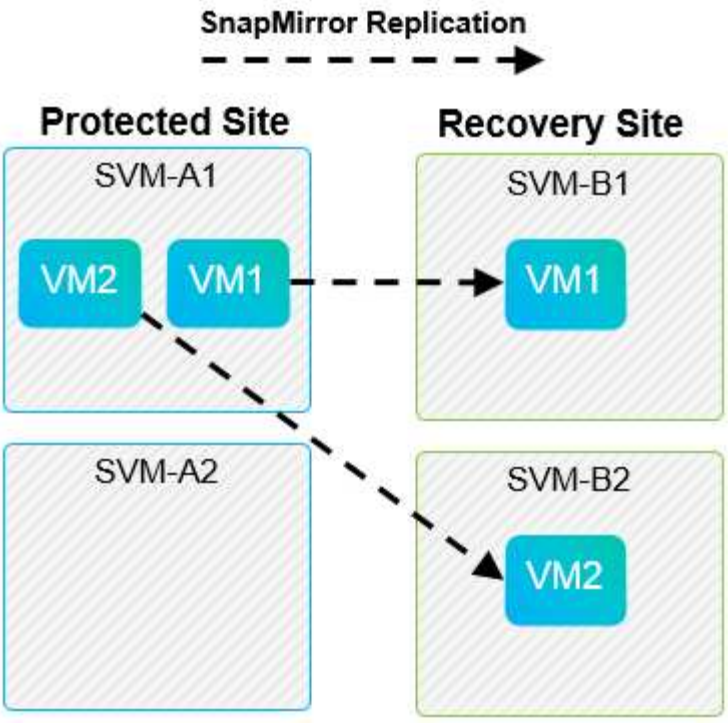
- VLSR vede solo la SVM, non un singolo controller fisico.
- Una SVM può controllare LUN e volumi che si estendono su più nodi in un cluster.

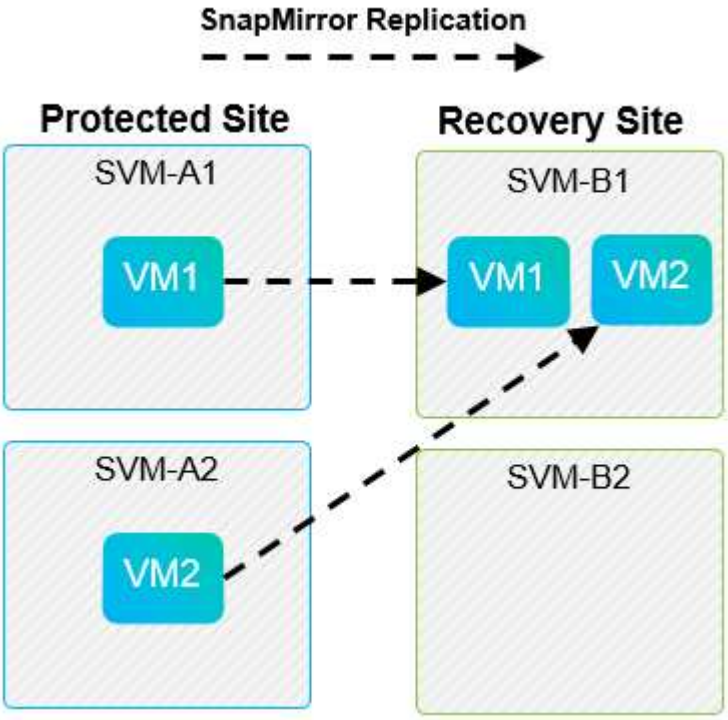
Best practice
Per determinare la supportabilità, tenere presente questa regola: Per proteggere una macchina virtuale utilizzando VLSR e NetApp SRA, tutte le parti della macchina virtuale devono esistere su un solo SVM. Questa regola si applica sia al sito protetto che al sito di ripristino.

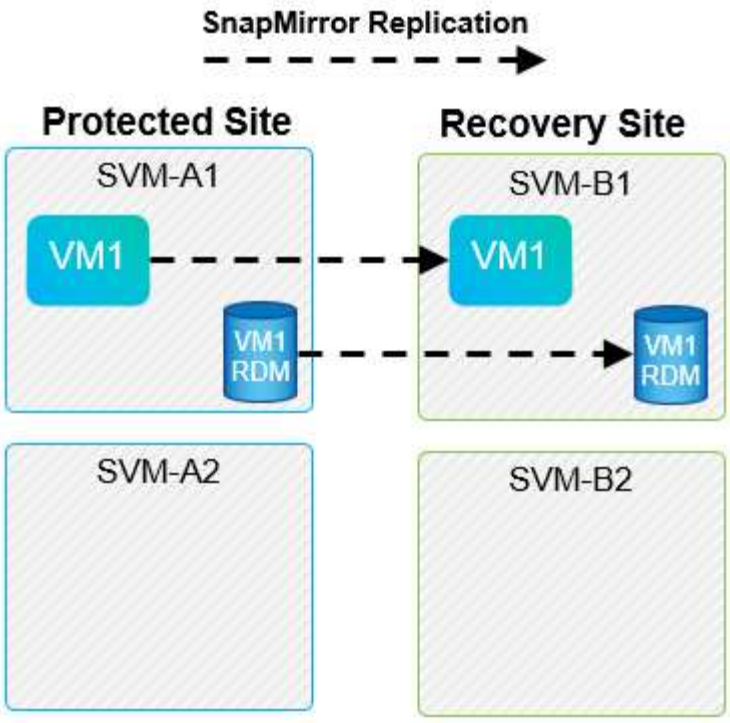
Layout SnapMirror supportati

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




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


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



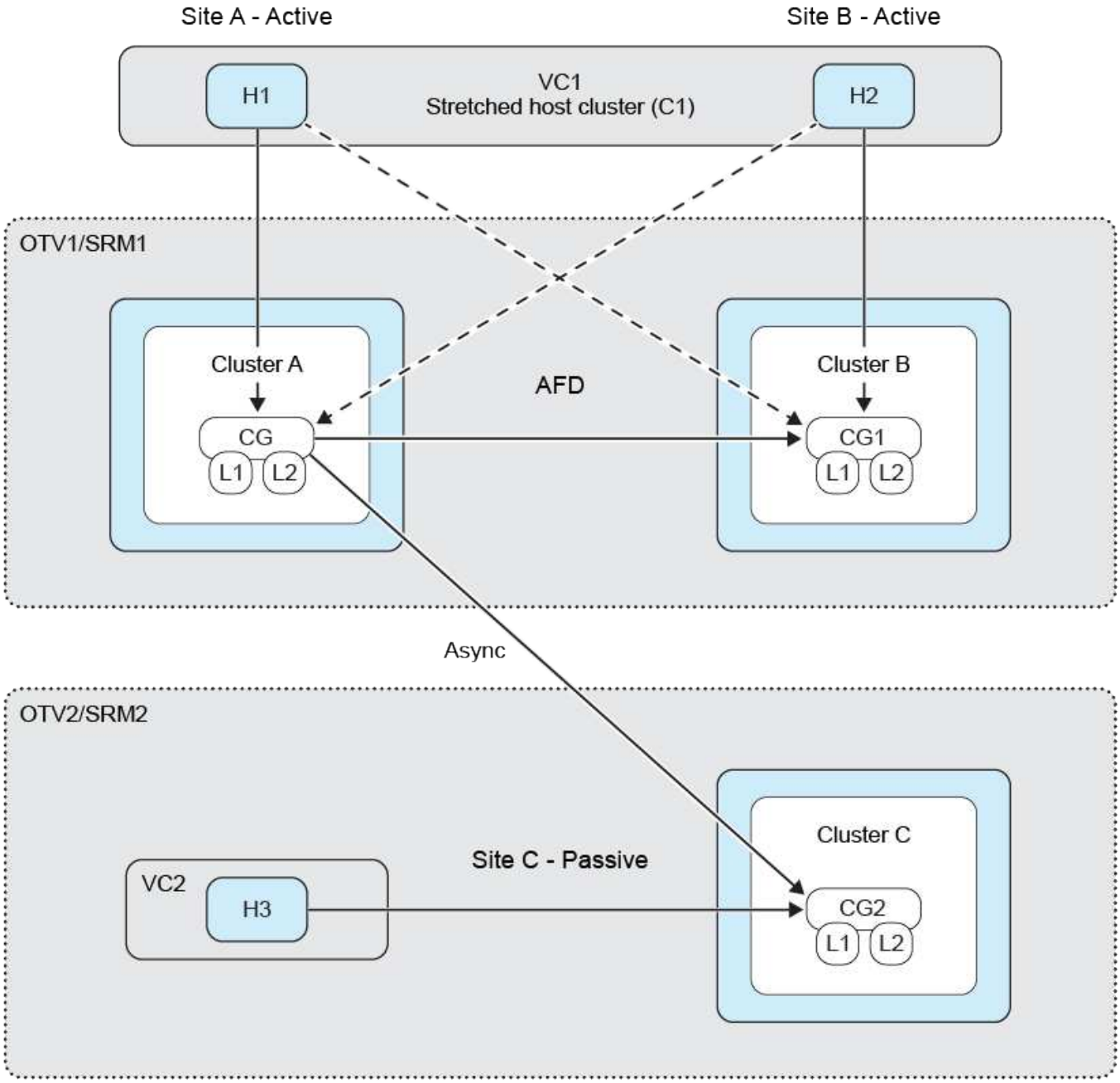
Supporto VMFS con sincronizzazione attiva SnapMirror

Gli strumenti ONTAP 10.3 e versioni successive supportano anche la protezione dei datastore VMFS con SnapMirror Active Sync (SMas). Ciò consente un failover trasparente per la continuità aziendale tra due data center (definiti domini di errore) relativamente vicini tra loro. Il disaster recovery a lunga distanza può quindi essere orchestrato utilizzando SnapMirror in modalità asincrona tramite gli strumenti ONTAP SRA con VLSR.

"Scopri di più sulla sincronizzazione attiva ONTAP SnapMirror"

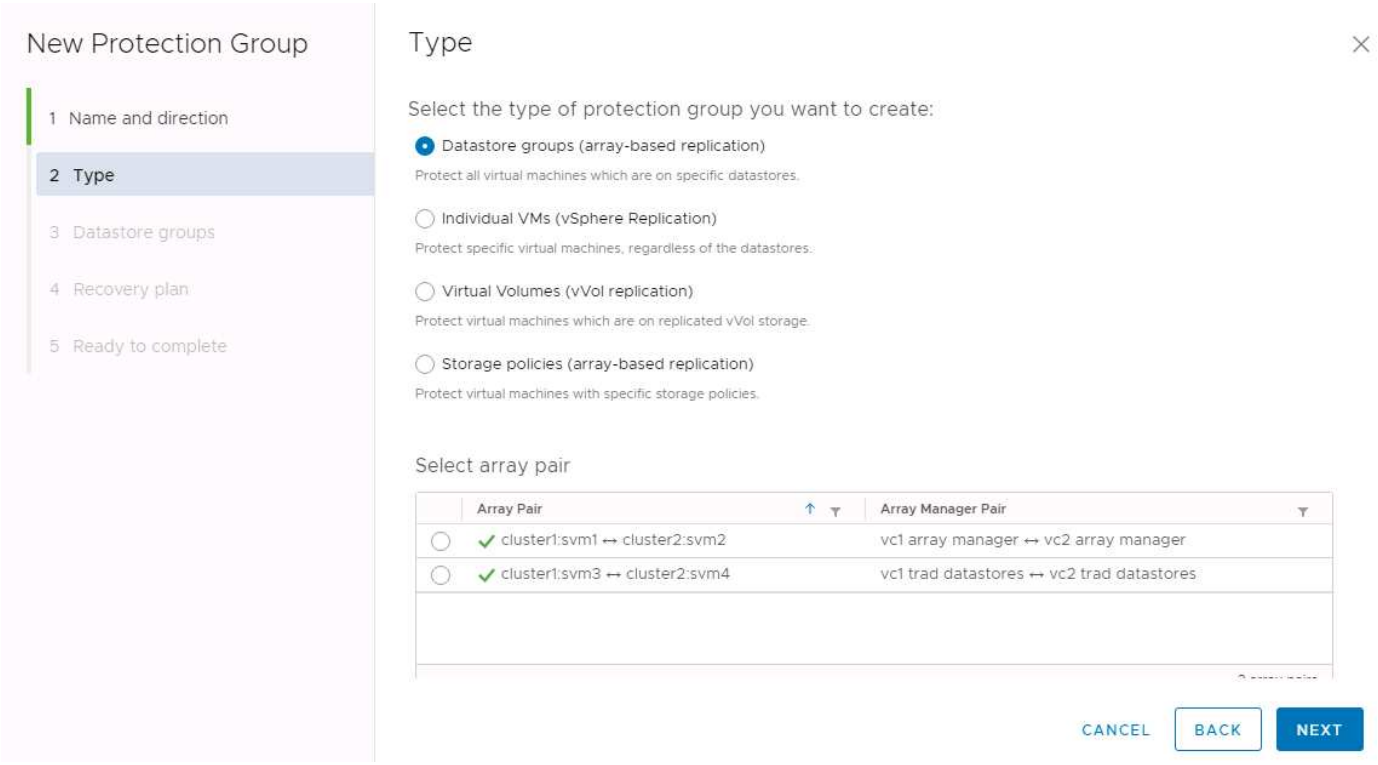
Gli archivi dati vengono raccolti in un gruppo di coerenza (CG) e le VM in tutti gli archivi dati manterranno tutte la coerenza nell'ordine di scrittura in quanto membri dello stesso CG.

Alcuni esempi potrebbero essere la protezione di siti a Berlino e Amburgo tramite SMas e una terza replica del sito tramite SnapMirror asincrono e protetta tramite VLSR. Un altro esempio potrebbe essere quello di proteggere i siti di New York e del New Jersey utilizzando SMas, con un terzo sito a Chicago.



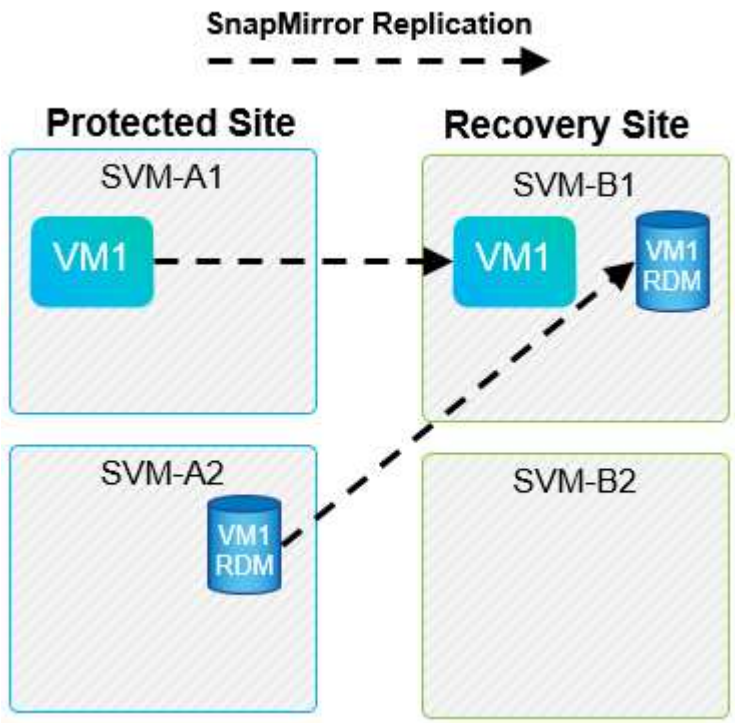
Layout di Array Manager supportati

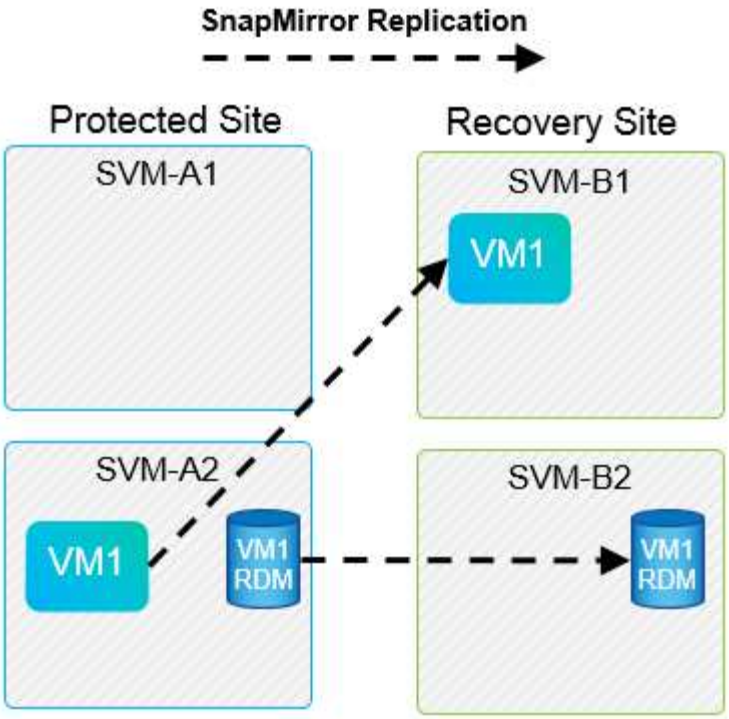
Quando si utilizza la replica basata su array (ABR) in VLSR, i gruppi di protezione vengono isolati in una singola coppia di array, come illustrato nella seguente schermata. In questo scenario, `SVM1` e `SVM2` vengono sottoposti a peed con `SVM3` e `SVM4` nel sito di recovery. Tuttavia, è possibile selezionare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



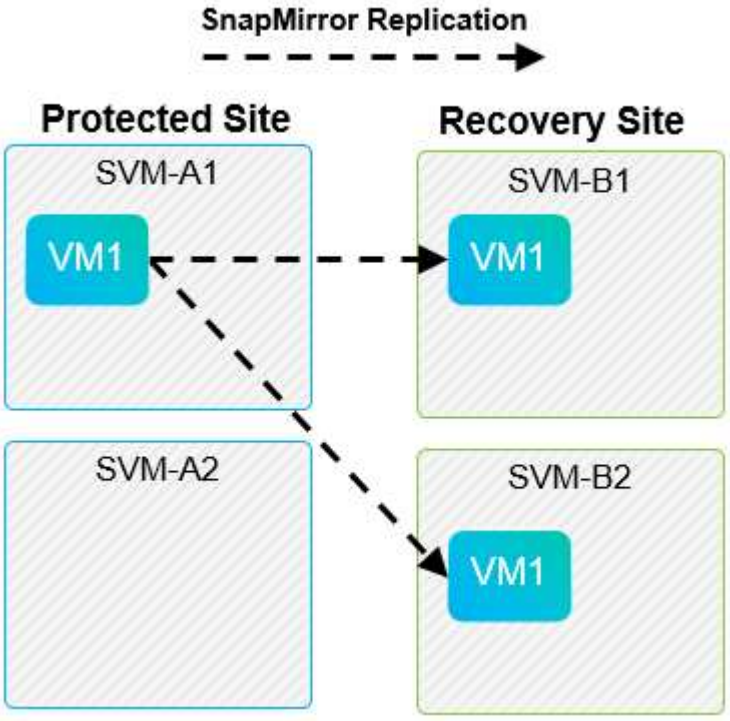
Layout non supportati

Le configurazioni non supportate dispongono di dati (VMDK o RDM) su più SVM di proprietà di una singola macchina virtuale. Negli esempi mostrati nelle seguenti figure, `VM1` non è possibile configurare la protezione con VLSR perché `VM1` dispone di dati su due SVM.





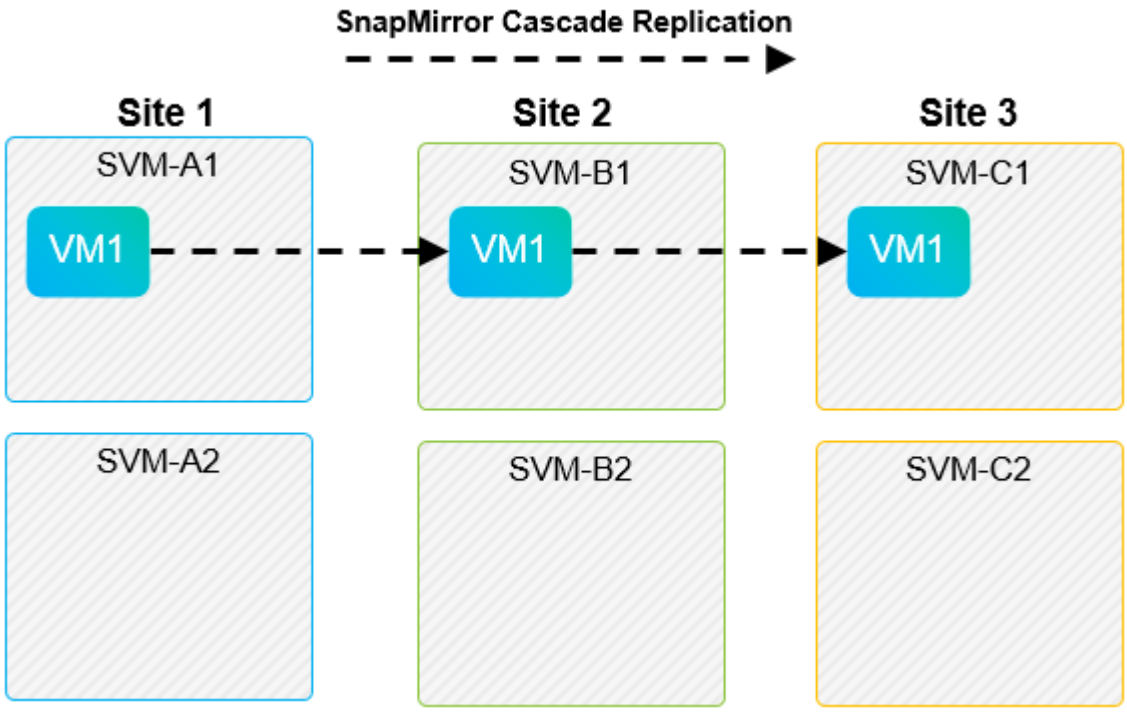
Qualsiasi relazione di replica in cui un singolo volume NetApp viene replicato da una SVM di origine a più destinazioni nella stessa SVM o in SVM differenti viene definita fan-out di SnapMirror. Fan-out non supportato con VLSR. Nell'esempio mostrato nella figura seguente, `VM1` non è possibile configurare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



Cascata di SnapMirror

VLSR 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, VLSR 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, VLSR 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.

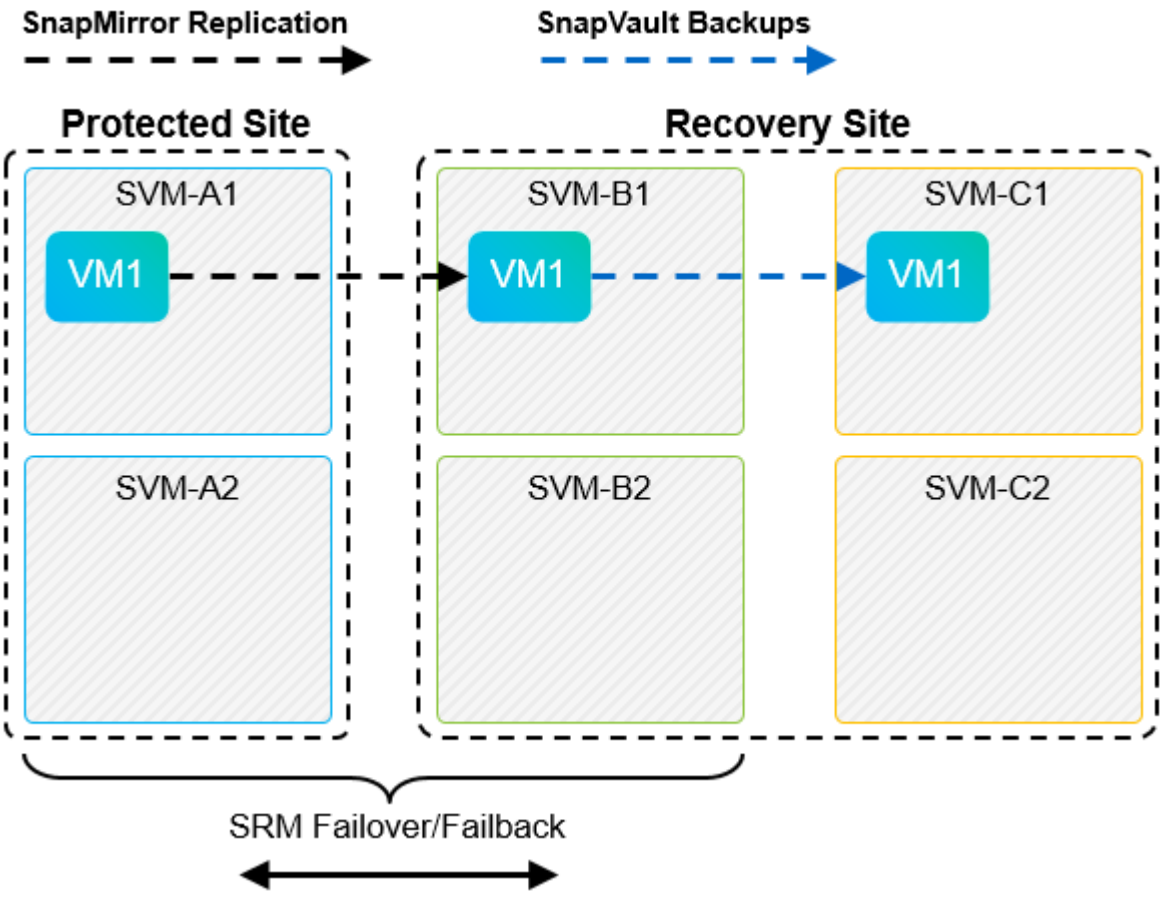
È possibile creare un volume di origine in una configurazione a cascata in cui un volume viene replicato in una destinazione SnapMirror nel sito DR e da qui viene vault in una destinazione SnapVault. È possibile creare un volume di origine anche in una relazione fan-out in cui una destinazione è una 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 VLSR o l'inversione della replica.

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

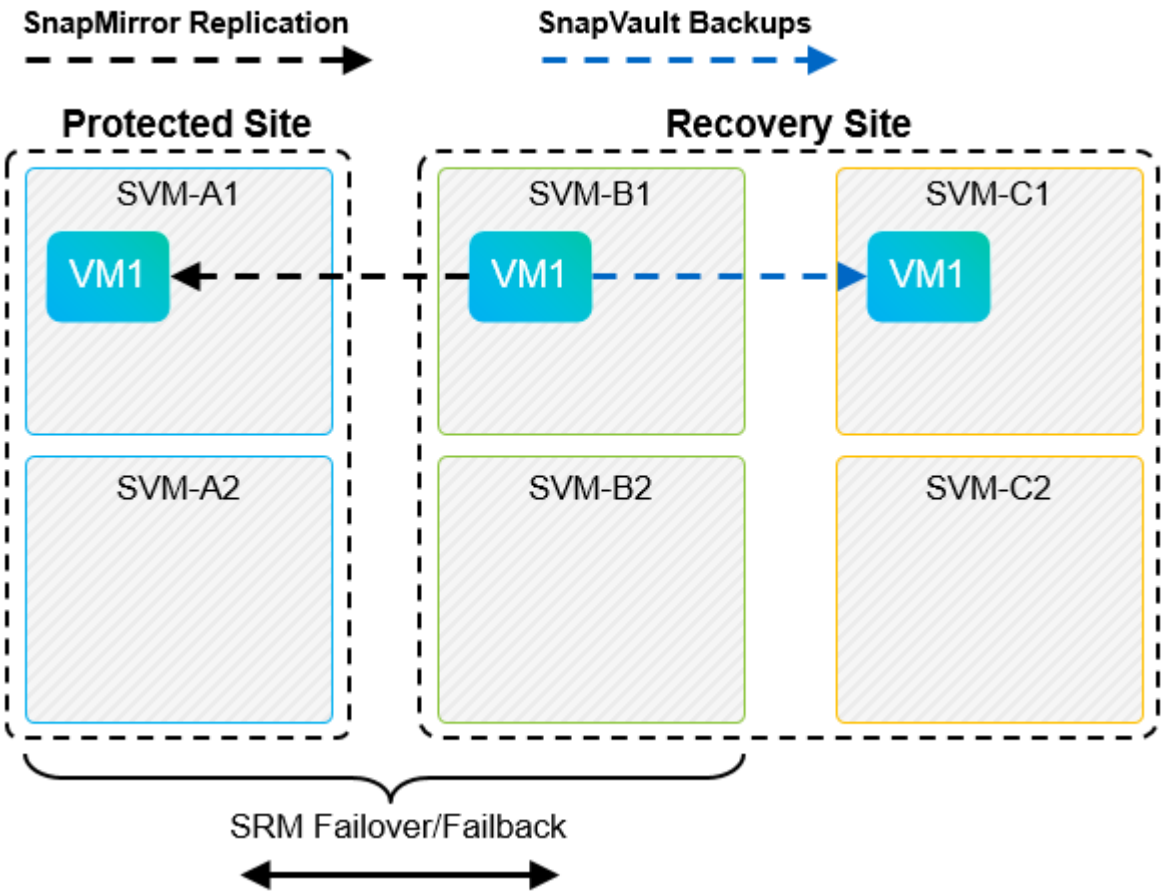
Best practice
Se SnapVault e VLSR vengono utilizzati nello stesso ambiente, NetApp consiglia di utilizzare una configurazione a cascata da SnapMirror a SnapVault in cui i backup di SnapVault vengono normalmente eseguiti dalla destinazione di SnapMirror nel sito di DR. In caso di disastro, questa configurazione 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 VLSR 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 VLSR, tutte le applicazioni che dipendono da questi ID devono essere riconfigurate dopo il failover di VLSR. 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 VLSR 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 vsrm 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 VLSR.

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 VLSR 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 VLSR perché, durante il failover VLSR o il failover di test, VLSR include tutti gli iniziatori FC e iSCSI negli host ESXi nella richiesta.

Best practice
VLSR 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 VLSR in modo che le macchine virtuali siano configurate per il failover in un gruppo di host o nell'altro.

Risoluzione dei problemi relativi a VLSRM/SRM quando si utilizza la replica vVols

Quando si utilizzano gli strumenti ONTAP 9.13P2, il flusso di lavoro all'interno di VLSR e SRM è notevolmente diverso quando si utilizza la replica vVol da ciò che viene utilizzato con SRA e i datastore tradizionali. Ad esempio, non esiste alcun concetto di gestore di array. Come tali, `discoverarrays` e `discoverdevices` i comandi non vengono mai visti.

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:

- Tool ONTAP per le risorse di VMware vSphere 10.x
"https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- Tool ONTAP per le risorse di VMware vSphere 9.x
"https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- 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 migliori pratiche di configurazione SnapMirror TR-4015 per ONTAP 9
https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf
- Documentazione di VMware Live Site Recovery "https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

Per verificare se le versioni delle funzionalità e dei prodotti descritti nel presente documento sono supportate nel proprio ambiente specifico, fare riferimento "Tool di matrice di interoperabilità (IMT)"alla sul sito di supporto NetApp. 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.

Questa documentazione sostituisce i report tecnici precedentemente pubblicati *TR-4128: VSphere on NetApp MetroCluster*

Soluzioni di disponibilità continua per ambienti vSphere

L'architettura ONTAP è una piattaforma di archiviazione flessibile e scalabile che fornisce servizi SAN (FCP, iSCSI e NVMe-oF) e NAS (NFS v3 e v4.1) per gli archivi dati. I sistemi di 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 (Cluster failover on Disaster 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, disponibile su sistemi non MetroCluster e su sistemi ASA R2,

offre una protezione granulare dei datastore con protocolli SAN FCP e iSCSI. Consente di proteggere l'intero vMSC o in modo selettivo 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. A partire da ONTAP 9.15.1, SnapMirror Active Sync supporta una funzionalità Active/Active simmetrica, consentendo operazioni i/o in lettura e scrittura da entrambe le copie di un LUN protetto con replica sincrona bidirezionale, consentendo alle due copie LUN di servire le operazioni i/O. Prima di ONTAP 9.15.1, la sincronizzazione attiva di SnapMirror supporta solo configurazioni Active/Active asimmetriche, in cui i dati sul sito secondario sono sottoposti a proxy alla copia primaria di una LUN.

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 a "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 esteso insieme a cluster di host ESXi, distribuiti su diversi domini di errore, come rack, edifici, campus o persino città. Le tecnologie di storage ActiveSync NetApp MetroCluster e SnapMirror vengono utilizzate per fornire una protezione con obiettivo di punto di ripristino zero (RPO=0) ai cluster host. La configurazione vMSC è progettata per garantire che i dati siano sempre disponibili anche in caso di guasto di un "sito" fisico o logico completo. Un dispositivo di archiviazione che fa parte della configurazione vMSC deve essere certificato dopo aver superato con successo il processo di certificazione vMSC. Tutti i dispositivi di archiviazione supportati possono essere trovati in "Guida alla compatibilità dello storage VMware".

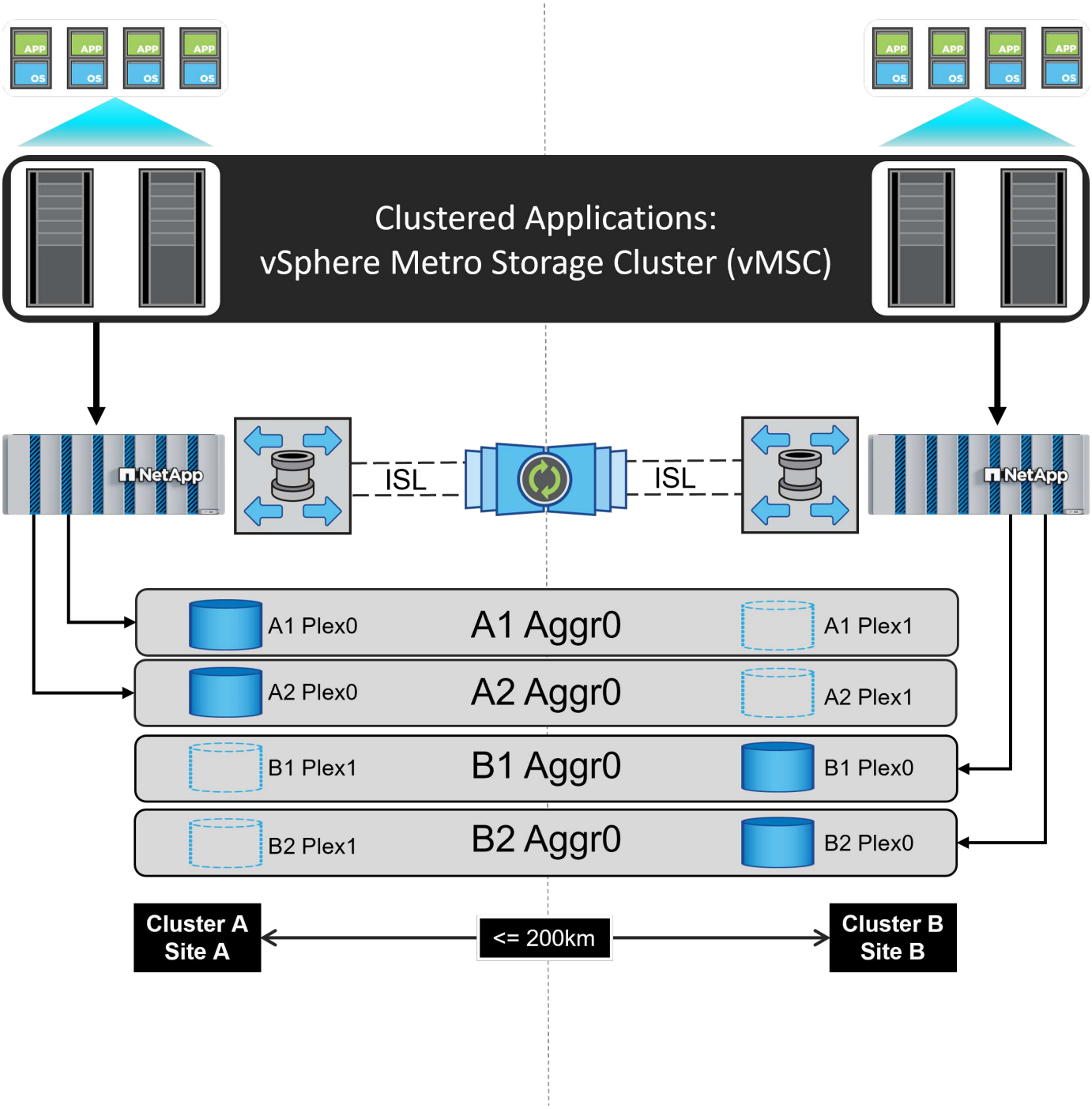
Per ulteriori informazioni sulle linee guida di progettazione per vSphere Metro Storage Cluster, consultare la seguente documentazione:

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

NetApp MetroCluster può essere implementato in due configurazioni diverse per l'utilizzo con vSphere:

- Stretch MetroCluster
- Fabric MetroCluster

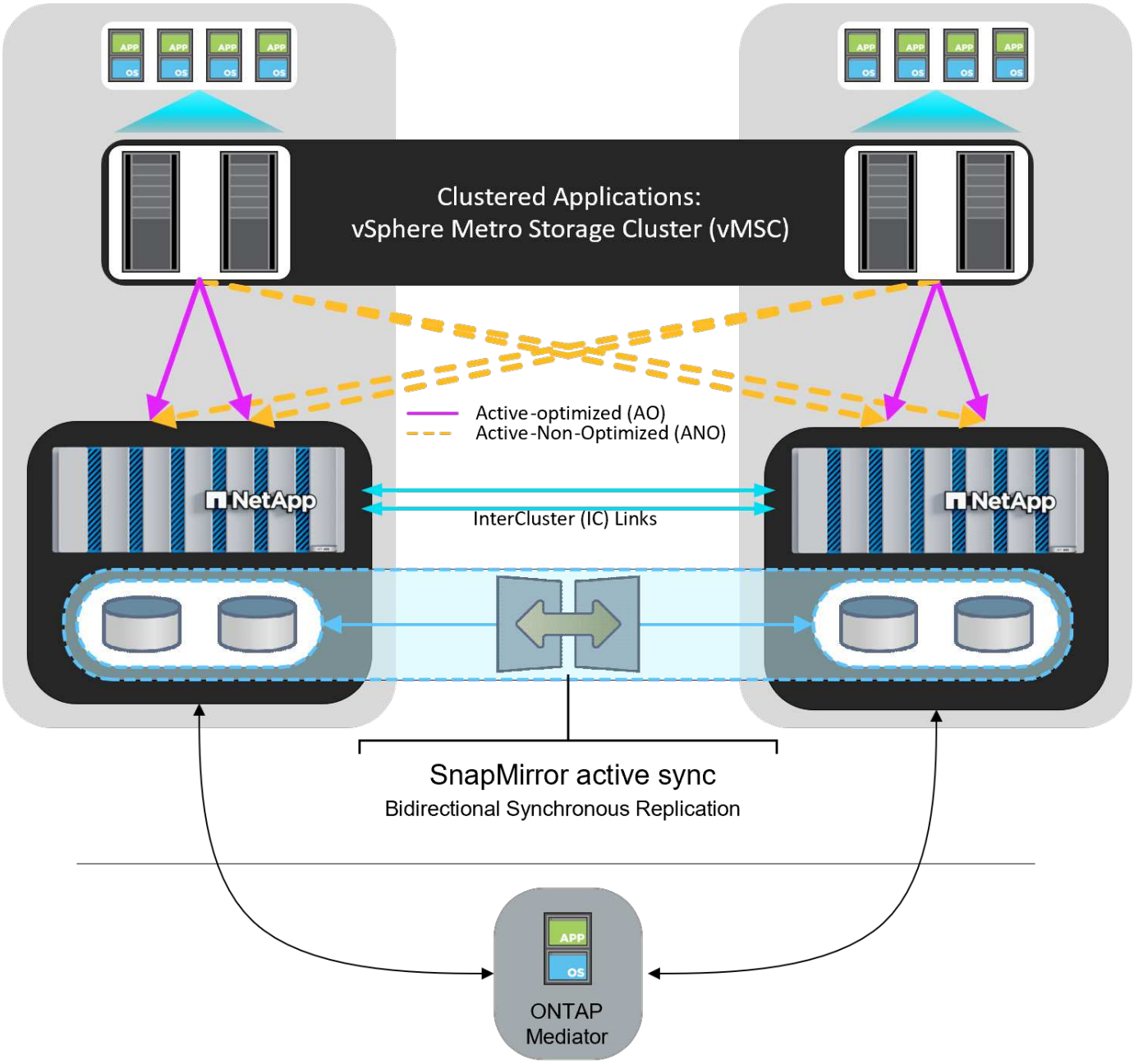
Di seguito viene illustrato uno schema topologico di alto livello di Stretch MetroCluster.



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
- Active Sync simmetrico (ONTAP 9.15.1)



Per informazioni specifiche sulla progettazione e la distribuzione della sincronizzazione attiva di SnapMirror, consultare la sezione "Documenti NetApp".

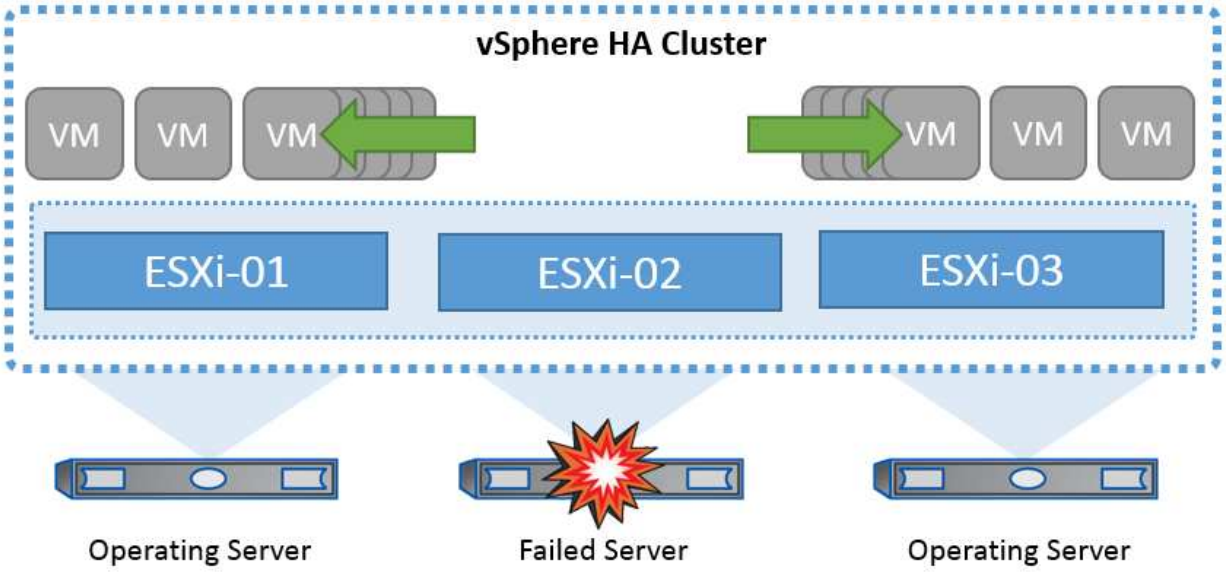
Panoramica della soluzione VMware vSphere

vCenter Server Appliance (VCSA) è un potente sistema di gestione centralizzata e un unico pannello di controllo per vSphere che consente agli amministratori di gestire in modo efficace i cluster ESXi. Facilita funzioni chiave quali il provisioning delle VM, il funzionamento di vMotion, l'alta disponibilità (HA), il Distributed Resource Scheduler (DRS), VMware vSphere Kubernetes Service (VKS) e molto altro. È un componente essenziale negli ambienti cloud VMware e dovrebbe 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 fornisce vSphere High Availability (ha), offrendo un'elevata disponibilità e una semplicità d'uso 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 può riavviare la macchina virtuale interessata sullo stesso server fisico. VSphere ha consente di ridurre i tempi di inattività pianificati, prevenire i tempi di inattività non pianificati e ripristinare rapidamente i dati in caso di interruzioni.

Cluster vSphere HA che ripristina le VM da un server guasto.



È importante comprendere che VMware vSphere non conosce la sincronizzazione attiva di NetApp MetroCluster o SnapMirror 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 host e VM.

Rilevamento errori host

Non appena viene creato il cluster HA, tutti gli host nel cluster partecipano all'elezione e uno degli host diventa master. Ogni slave esegue un heartbeat di rete verso il master, e il master, a sua volta, esegue un heartbeat di rete su tutti gli host slave. L'host master di un cluster vSphere HA è responsabile del rilevamento dei guasti 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.

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

Isolation Response è un'impostazione di vSphere HA che determina l'azione attivata sulle macchine virtuali quando un host in un cluster vSphere HA perde le sue connessioni di rete di gestione ma continua a funzionare. Sono disponibili tre opzioni per questa impostazione: "Disabilitato", "Arresta e riavvia le VM" e "Spegni e riavvia le VM".

"Arresta" è meglio di "Spegni", che non elimina le modifiche più recenti sul disco né 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.

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 archiviazione si guasta in modo permanente o viene rimosso amministrativamente e non si prevede che verrà ripristinato. L'array di archiviazione NetApp invia un codice SCSI Sense a ESXi, dichiarando che il dispositivo è stato perso definitivamente. Nella sezione Condizioni di errore e risposta della VM di vSphere HA, è possibile configurare la risposta da adottare dopo il rilevamento di una condizione PDL.

NetApp consiglia di impostare la "Risposta per Datastore con PDL" su "**Spegni e riavvia le VM**". Quando viene rilevata questa condizione, una VM verrà riavviata immediatamente su un host funzionante 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 verso l'array. ESXi ritiene che si tratti di un problema temporaneo del dispositivo e si aspetta che torni 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).

- NetApp consiglia di configurare "Risposta per datastore con APD" su "**Spegni e riavvia le VM (conservative)**".
- Con "conservativo" si intende la probabilità che HA sia in grado di riavviare le VM. Se impostato su Conservativo, HA riavvierà la VM interessata dall'APD solo se sa che un altro host può riavviarla. Nel caso di Aggressive, HA tenterà di riavviare la VM anche se non conosce lo stato degli altri host. Ciò può comportare il mancato riavvio delle VM se non è presente alcun host con accesso al datastore in cui si trovano.
- Se lo stato APD viene risolto e l'accesso allo storage viene ripristinato prima che sia trascorso il timeout, ha non riavvierà inutilmente la macchina virtuale a meno che non sia stata esplicitamente configurata. 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.
- NetApp consiglia di configurare la risposta per il ripristino APD dopo il timeout APD su Disabilitato.

Implementazione di VMware DRS per NetApp SnapMirror Active Sync

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.

Implementazione VMware DRS per NetApp MetroCluster

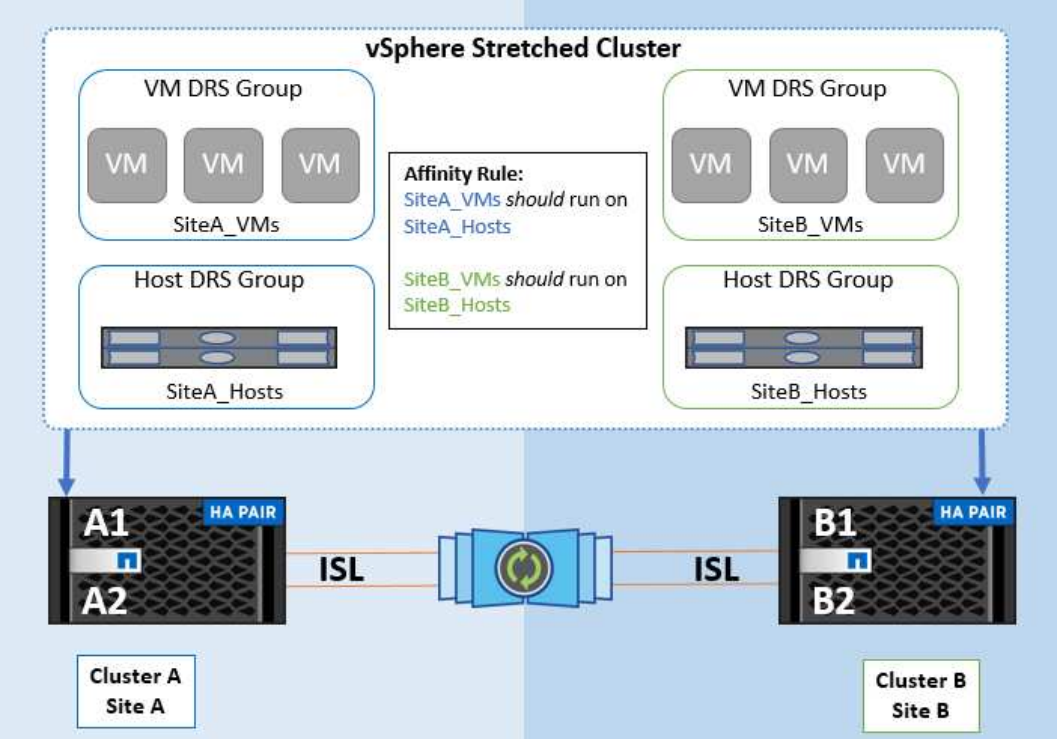
```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that, unless
there is a complete site failure, HA and DRS will only use local hosts.
Se si crea una regola di affinità DRS per il cluster, è possibile
specificare in che modo vSphere applica tale regola durante il failover di
una macchina virtuale.
```

Esistono due tipi di regole che è possibile specificare per il comportamento del 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 regole "should" invece di regole "must", in quanto vengono violate da vSphere ha in caso di errore. L'utilizzo di regole "must" potrebbe potenzialmente causare interruzioni del servizio.

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

Implementazione di VMware Storage DRS con NetApp MetroCluster

La funzionalità 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 (SIOC).

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.

*Quando si utilizza l'archiviazione ONTAP, si consiglia di disattivare l'archiviazione DRS.

- I DRS di archiviazione non sono generalmente necessari o consigliati per l'uso con i sistemi di archiviazione ONTAP.
- ONTAP offre proprie funzionalità di efficienza dello storage, come deduplica, compressione e compaction, che possono essere influenzate dallo Storage DRS.
- Se si utilizzano snapshot ONTAP , Storage vMotion lascerebbe indietro la copia della VM nello snapshot, aumentando potenzialmente l'utilizzo dello storage e potrebbe avere un impatto sulle applicazioni di backup come NetApp SnapCenter, che tiene traccia delle VM e dei relativi snapshot ONTAP .

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 sono disponibili all'indirizzo "Documentazione MetroCluster". Le istruzioni per SnapMirror Active Sync (SMA) sono disponibili anche 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, o se disponi di sistemi ONTAP non supportati per MetroCluster, come ad esempio i sistemi ASA R2, puoi utilizzare SnapMirror Active Sync che fornisce una protezione granulare dei datastore e l'accesso Active-Active su più cluster ONTAP in diversi domini di errore. SMA utilizza gruppi di coerenza (CGS) per garantire la coerenza dell'ordine di scrittura tra uno o più datastore ed è possibile creare più CGS in base ai requisiti dell'applicazione e del datastore. I gruppi di coerenza sono particolarmente utili per le applicazioni che richiedono la sincronizzazione dei dati tra datastore multipli. Ad esempio, LVM guest distribuiti tra datastore. SMA supporta inoltre RDM (Raw Device Mapping) e storage connesso al guest con iniziatori iSCSI in-guest. Per ulteriori informazioni sui gruppi di coerenza, visitare il sitoWeb 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, SMA è una configurazione solo SAN, nessun datastore NFS può essere protetto 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. Terzo, devi creare uno o più gruppi di coerenza per i datastore da proteggere con la sincronizzazione attiva di SnapMirror. Infine, è necessario creare un criterio SnapMirror per i gruppi di coerenza creati. Tutto questo può essere fatto facilmente usando la procedura guidata "Protect cluster" nel plug-in vCenter di ONTAP tools, o usando manualmente la CLI di ONTAP o System Manager.

Utilizzo del plug-in vCenter di ONTAP Tools per SnapMirror Active Sync

Il plug-in vCenter degli strumenti ONTAP fornisce un modo semplice e intuitivo per configurare SnapMirror Active Sync per vMSC. Puoi usare il plug-in vCenter di ONTAP Tools per creare e gestire relazioni di sincronizzazione attive di SnapMirror tra due cluster ONTAP. Questo plugin fornisce un'interfaccia di facile utilizzo per stabilire e gestire queste relazioni in modo efficiente. Per ulteriori informazioni sul plug-in vCenter degli strumenti ONTAP, visitare il sito Web all'indirizzo "Strumenti ONTAP per VMware vSphere", oppure accedere direttamente a "Proteggere utilizzando la protezione del cluster host".

Configurazione di VMware vSphere

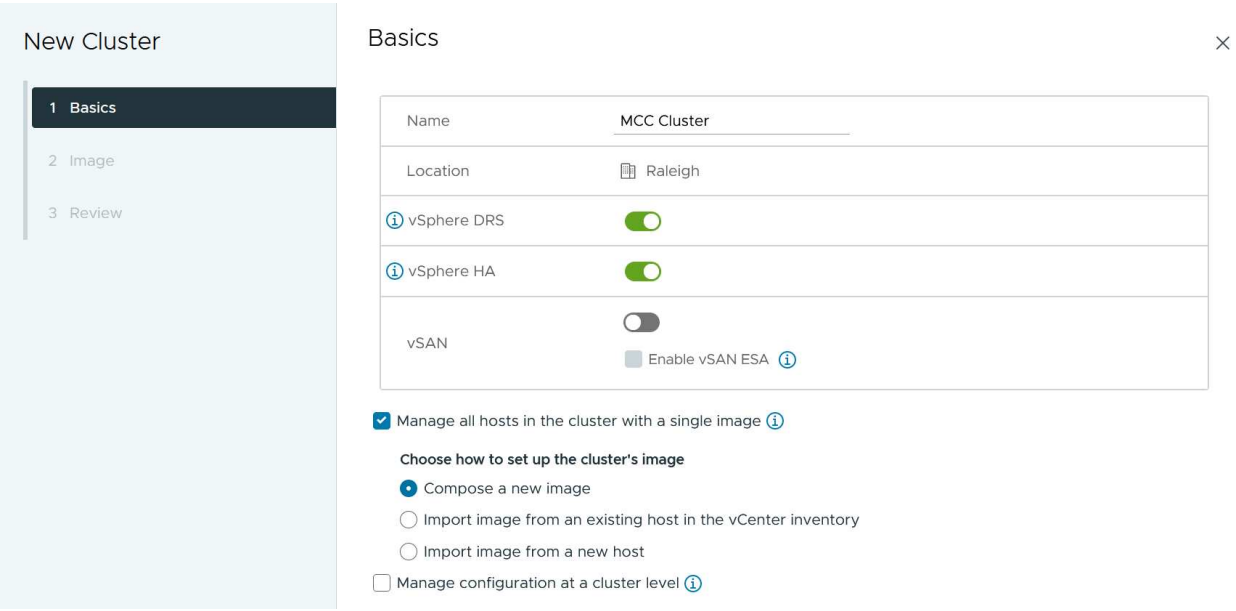
Creare un cluster vSphere ha

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.

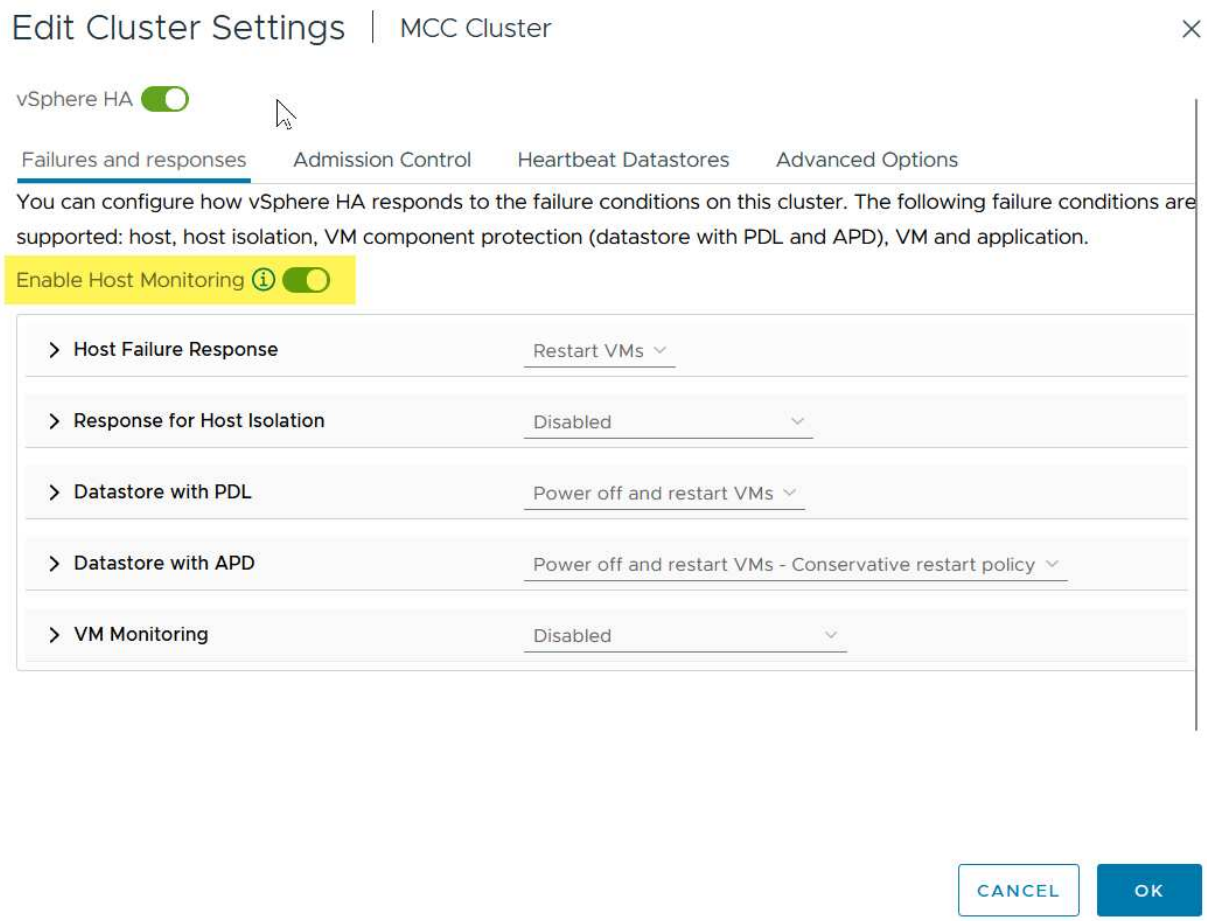
> Nessuna disposizione del presente documento sostituisce "Procedure consigliate per VMware vSphere Metro Storage Cluster". Questo contenuto viene fornito a scopo di riferimento e non sostituisce la documentazione ufficiale VMware.

Per configurare un cluster ha, completare i seguenti passaggi:

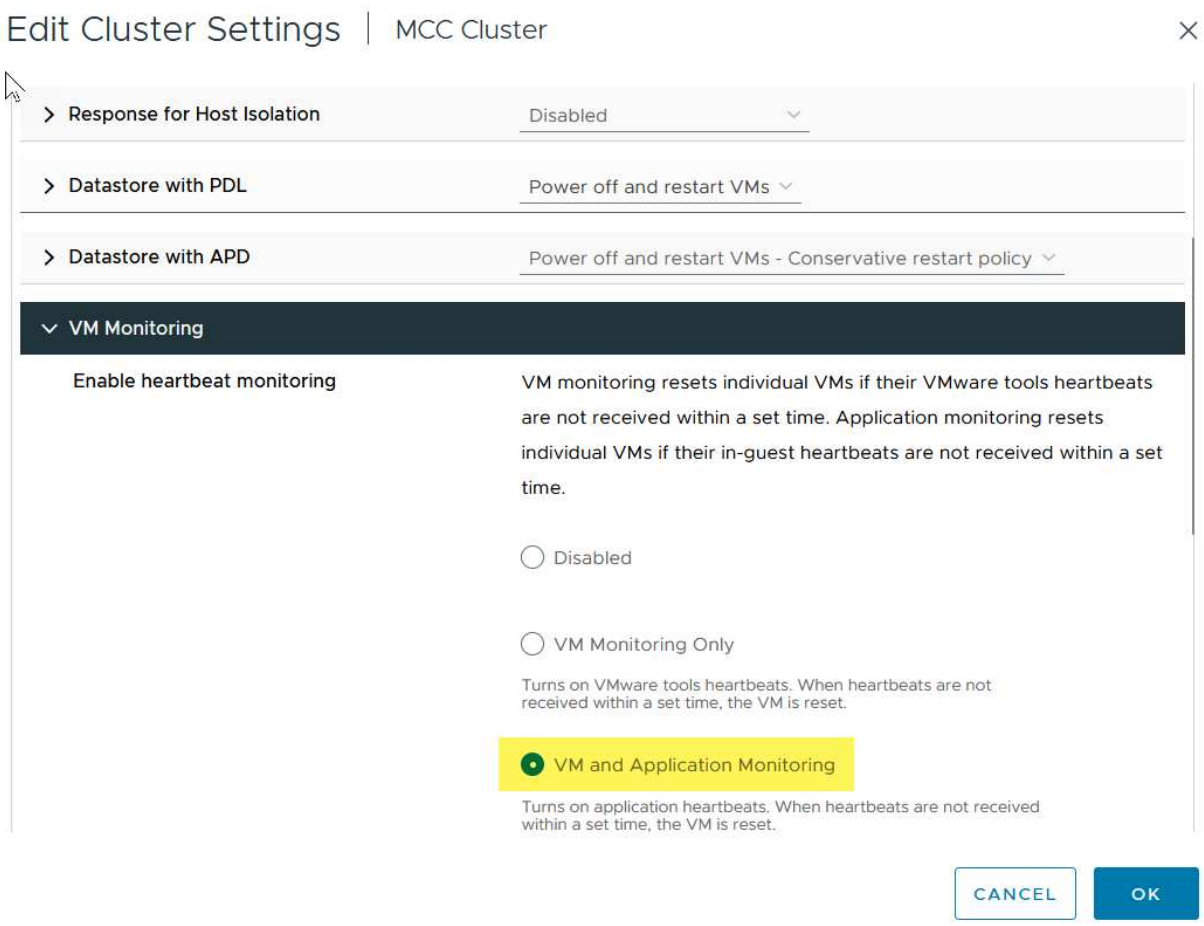
1. Connettersi all'interfaccia utente di vCenter.
2. In host e cluster, individuare il data center in cui si desidera creare il cluster ha.
3. Fare clic con il pulsante destro del mouse sull'oggetto del data center e selezionare nuovo cluster. In base alle nozioni di base, assicurarsi di aver abilitato vSphere DRS e vSphere ha. Completare la procedura guidata.



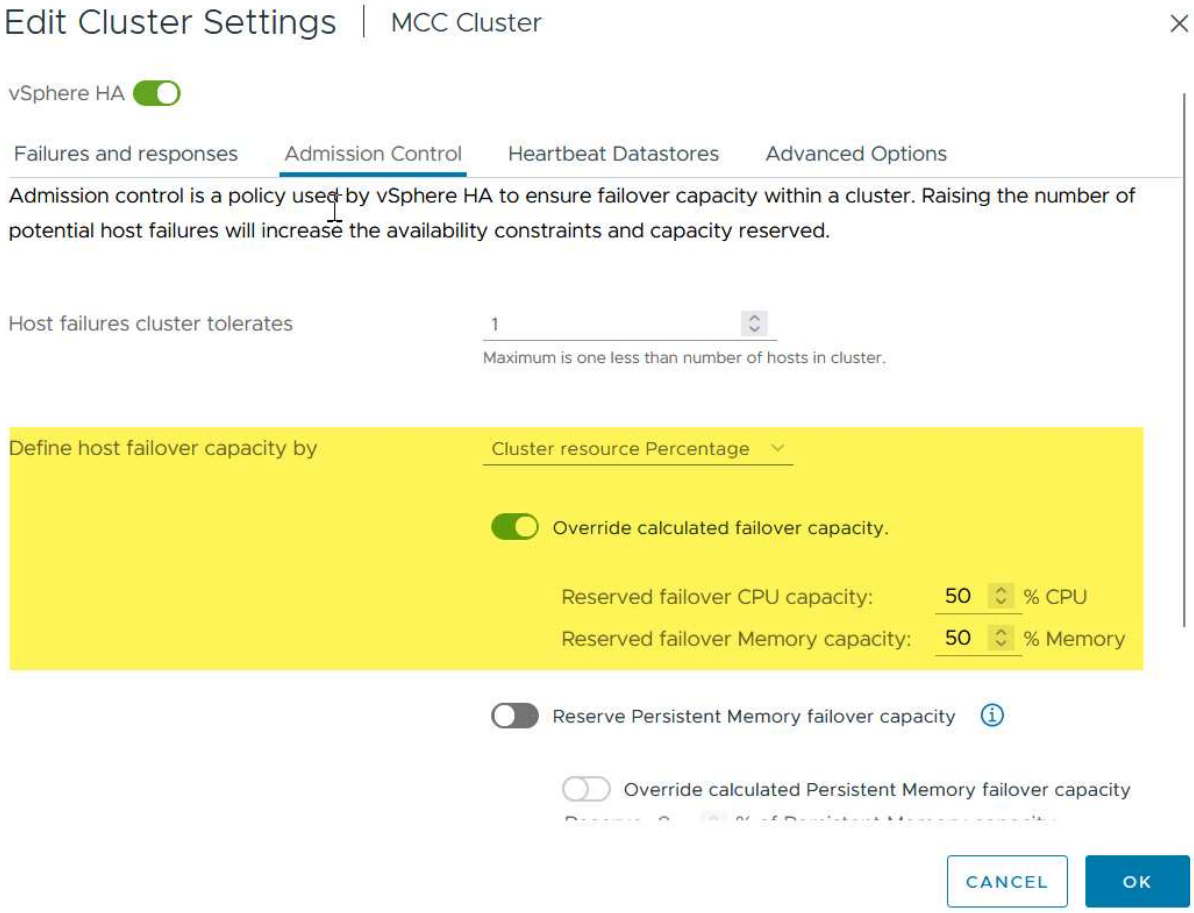
1. Selezionare il cluster e accedere alla scheda di configurazione. Selezionare vSphere ha e fare clic su Modifica.
2. In monitoraggio host, selezionare l'opzione attiva monitoraggio host.



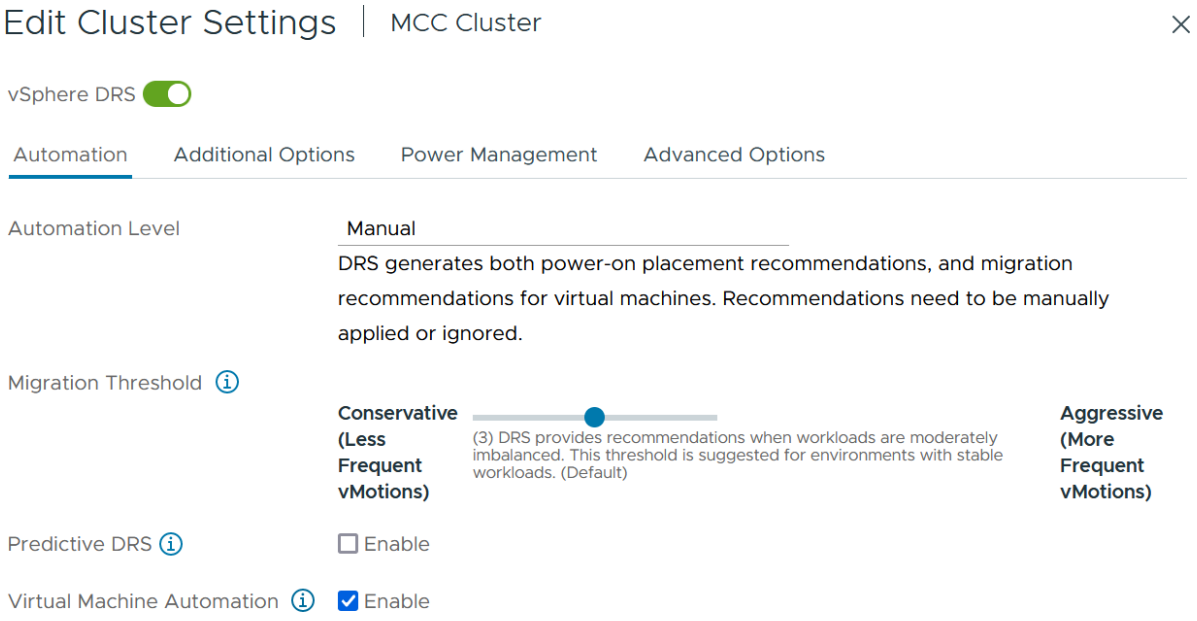
1. Nella scheda guasti e risposte, in monitoraggio VM, selezionare l'opzione solo monitoraggio VM o monitoraggio VM e applicazione.



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.



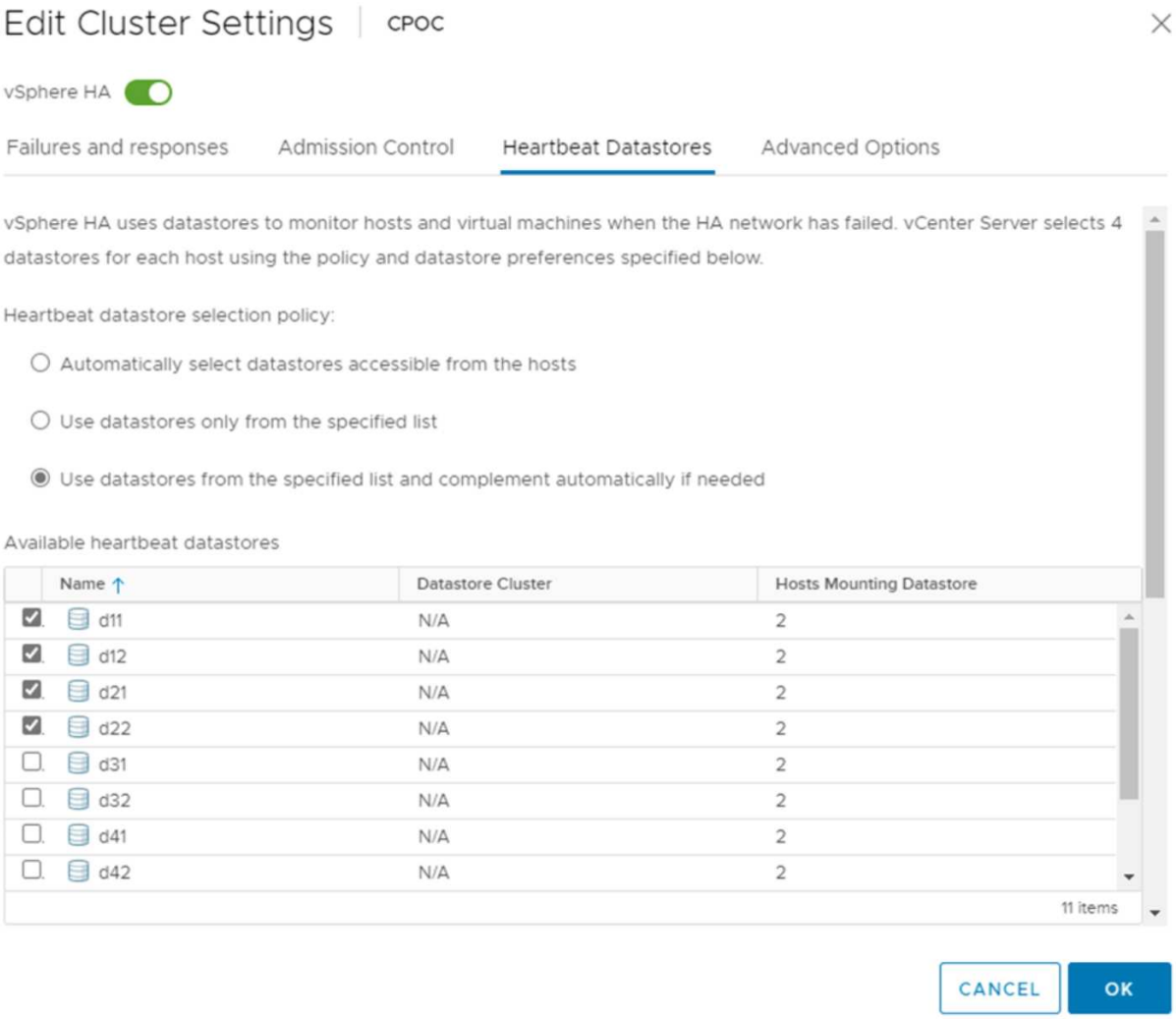
1. Abilitare la protezione dei componenti VM, fare riferimento a. "docs.vmware.com".
2. Le seguenti impostazioni aggiuntive di vSphere ha sono consigliate per vMSC con MetroCluster:

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:

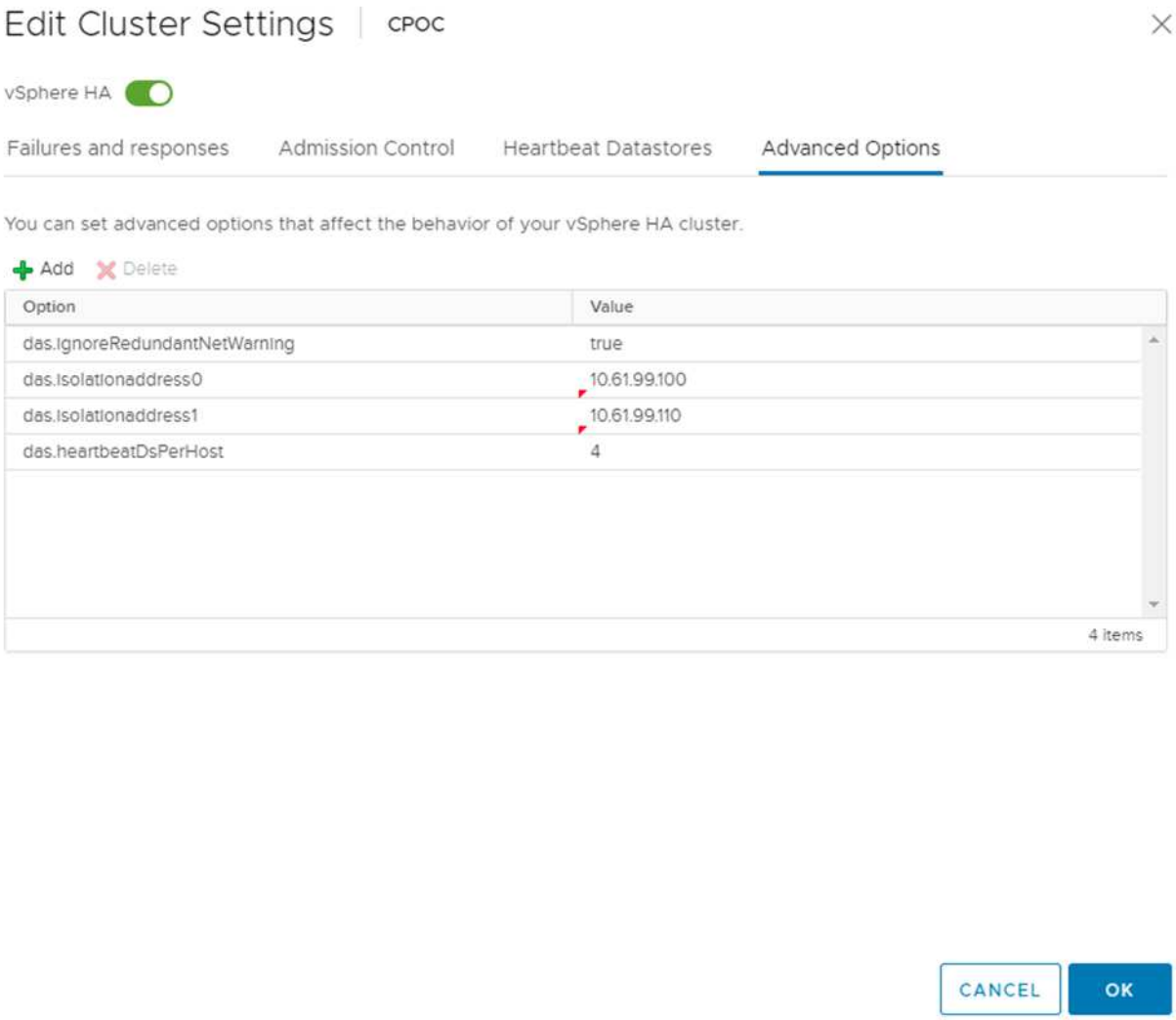
1. Nella sezione Heartbeating del datastore, selezionare Usa archivi dati dall'elenco specificato e completare automaticamente se necessario.
2. Seleziona i datastore che desideri utilizzare vCenter da entrambi i siti e premi OK.



Configurare le opzioni avanzate

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 "Procedure consigliate per VMware vSphere Metro Storage Cluster" 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 "Seleziona dall'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 MetroCluster o SnapMirror.

Fare riferimento a "Procedure consigliate per VMware vSphere Metro Storage Cluster" 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.

- 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.
- 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 is Violating VM-host Affinity Rule" (VM viola la regola di affinità VM-host) come trigger dell'evento. Per ulteriori informazioni sulla creazione e la modifica degli allarmi, consultare "Monitoraggio e performance di vSphere"la 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.

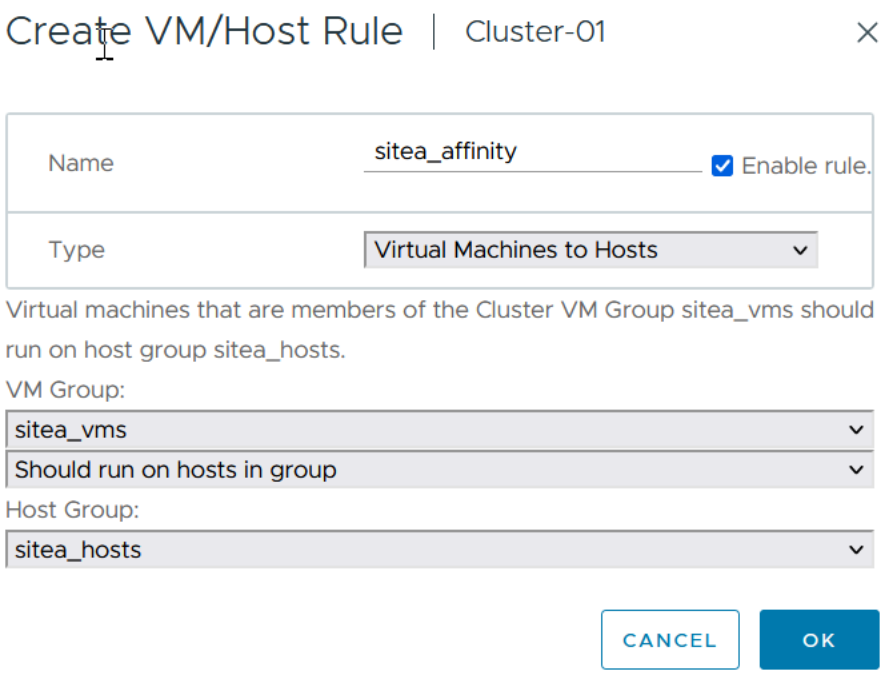
Crea regole host VM

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.



Crea cluster di datastore se necessario

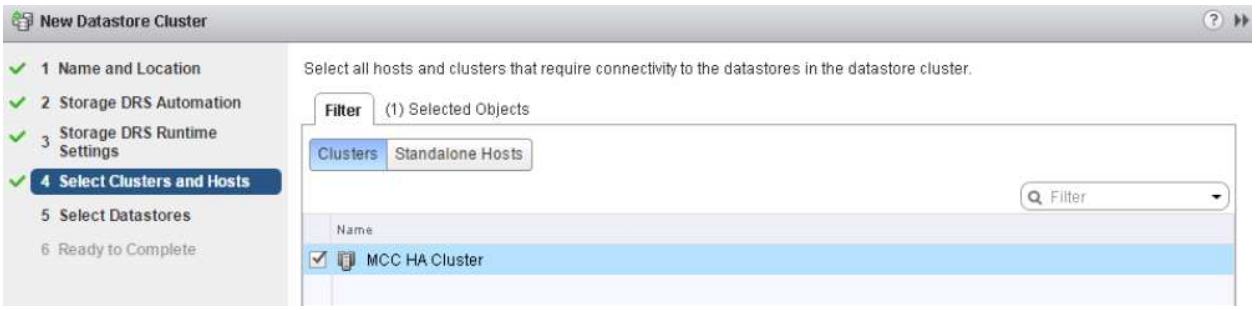
Per configurare un cluster di datastore per ciascun sito, attenersi alla seguente procedura:

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.

*Quando si utilizza l'archiviazione ONTAP, si consiglia di disattivare l'archiviazione DRS.

- I DRS di archiviazione non sono generalmente necessari o consigliati per l'uso con i sistemi di archiviazione ONTAP.
- ONTAP offre proprie funzionalità di efficienza dello storage, come deduplica, compressione e compaction, che possono essere influenzate dallo Storage DRS.
- Se si utilizzano snapshot ONTAP, storage vMotion lascerebbe la copia della macchina virtuale nella snapshot, aumentando potenzialmente l'utilizzo dello storage e potrebbe avere un impatto sulle applicazioni di backup, come NetApp SnapCenter, che tengono traccia delle macchine virtuali e delle relative snapshot ONTAP.

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 stia utilizzando server standalone, cluster di server ad alta disponibilità, container 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 LIF NAS nelle configurazioni MetroCluster eseguono automaticamente il failover. Tuttavia, le LIF SAN non vengono sottoposte a failover e continueranno a utilizzare il percorso diretto dei LUN (Logical Unit Number).

Per ulteriori informazioni sul takeover e sullo sconto ha, consultare 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 ONTAP Mediator è necessario per garantire che il failover del sito avvenga correttamente.

Scenari di errore per vMSC con MetroCluster

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.

In questo scenario non vi sono cambiamenti nel comportamento di MetroCluster e tutti i datastore continuano a 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.

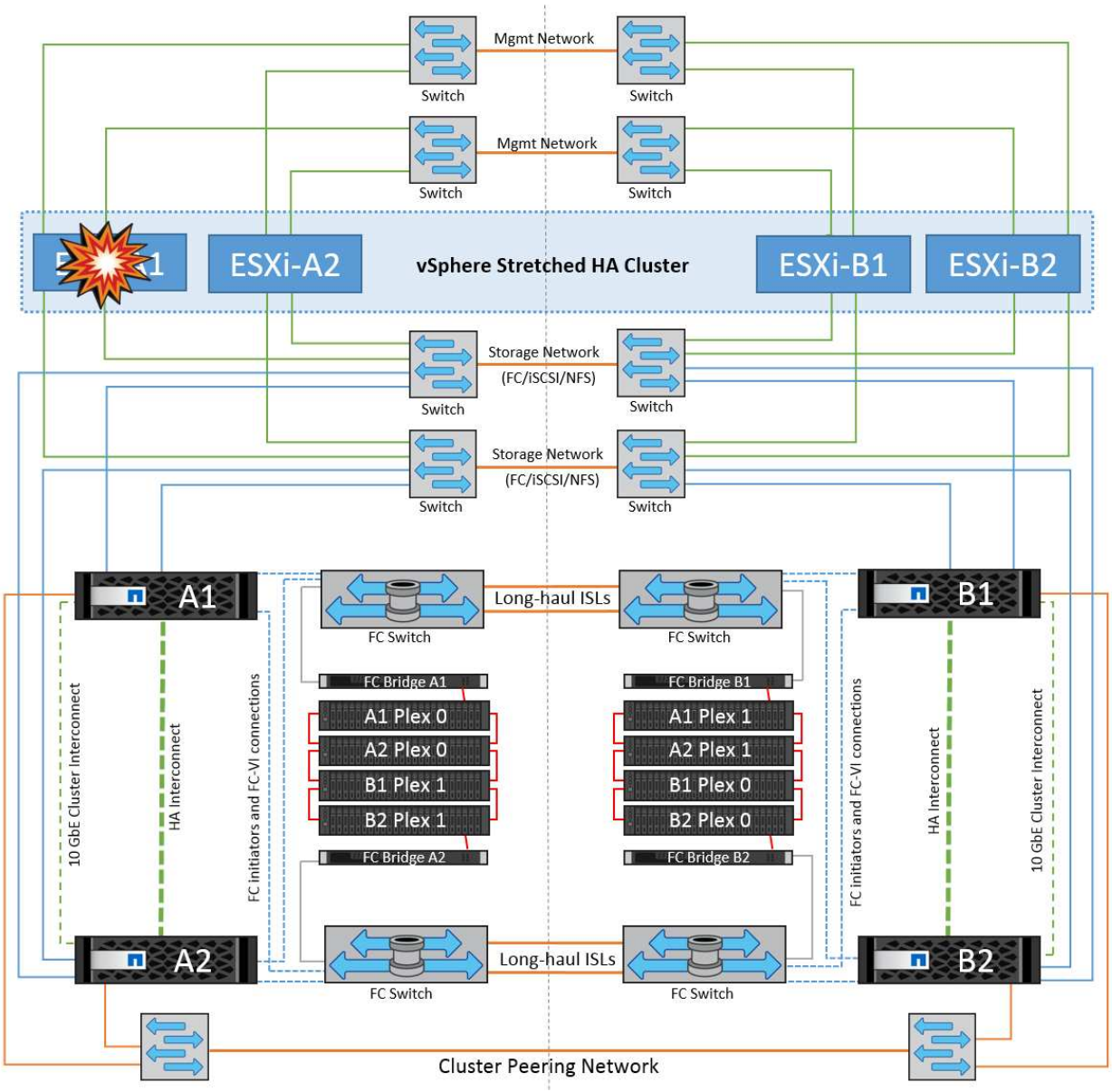
Inoltre, per i LUN iSCSI, il multipathing deve essere configurato legando le interfacce vmkernel agli adattatori di rete iSCSI. Per ulteriori informazioni, fai riferimento alla documentazione dello storage vSphere.

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



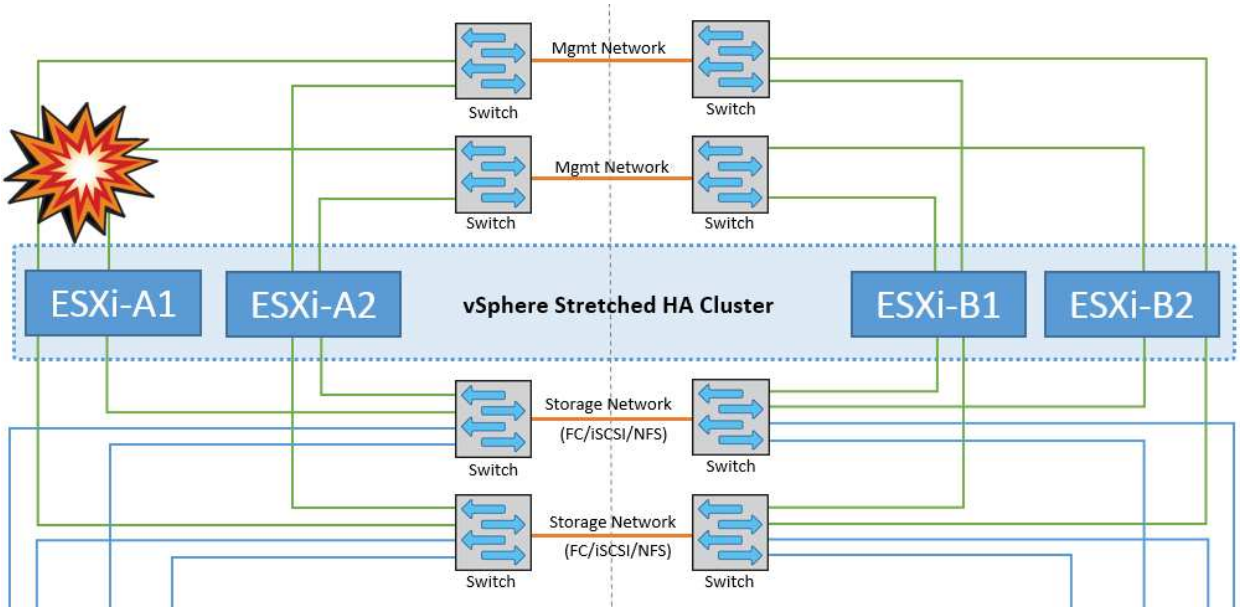
In questo scenario, se si verifica un guasto dell'host ESXi, il nodo master nel cluster VMware ha rileva il guasto dell'host in quanto non riceve più gli heartbeat di rete. Per determinare se l'host è effettivamente inattivo o solo una partizione di rete, il nodo master monitora gli heartbeat del datastore 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

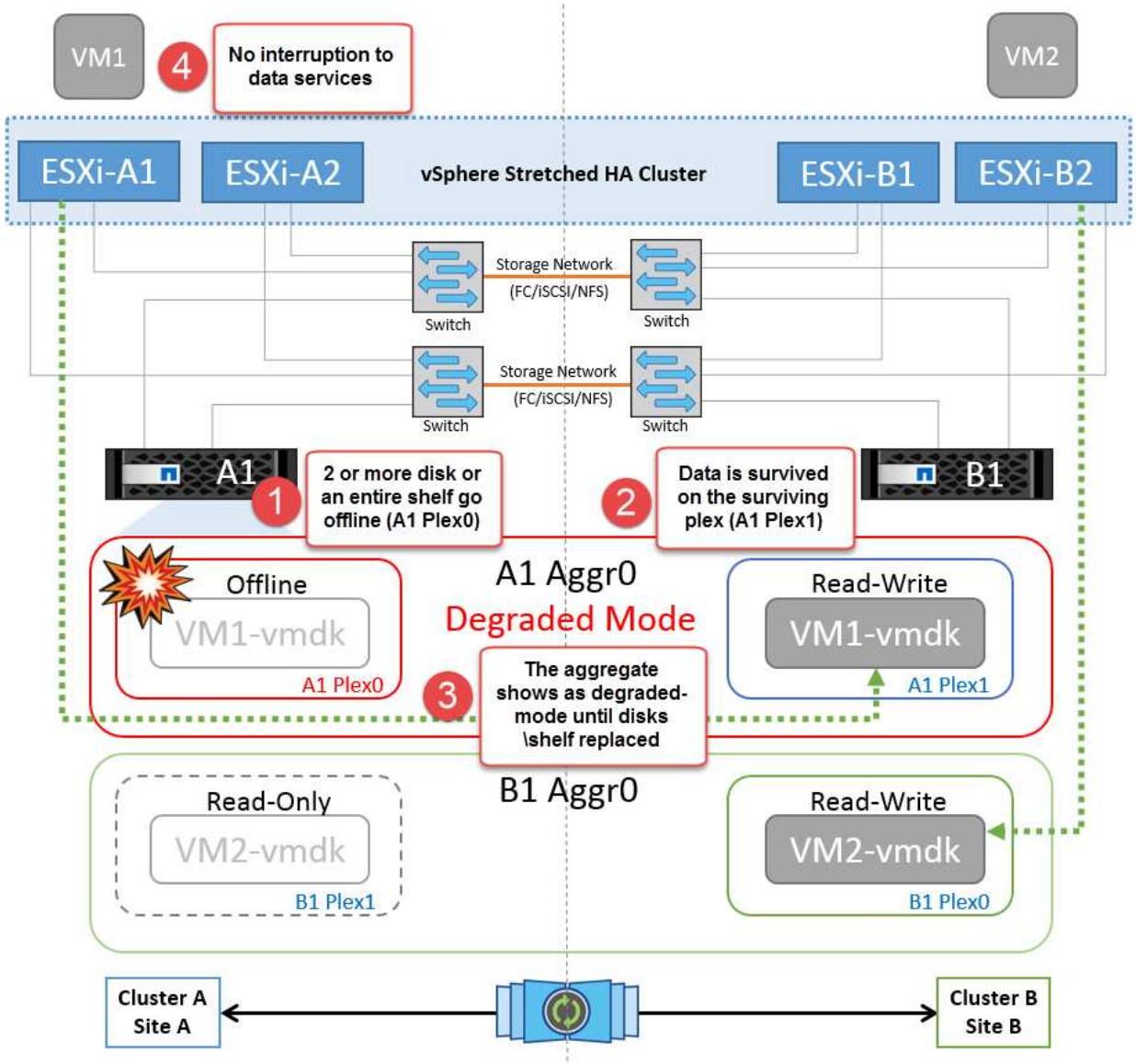


In questo scenario, se la rete di gestione dell'host ESXi non è attiva, il nodo master nel cluster ha non riceverà alcun heartbeat, pertanto l'host viene isolato nella rete. Per determinare se si è verificato un errore o se è solo isolato, il nodo master inizia a monitorare l'heartbeat del datastore. 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.

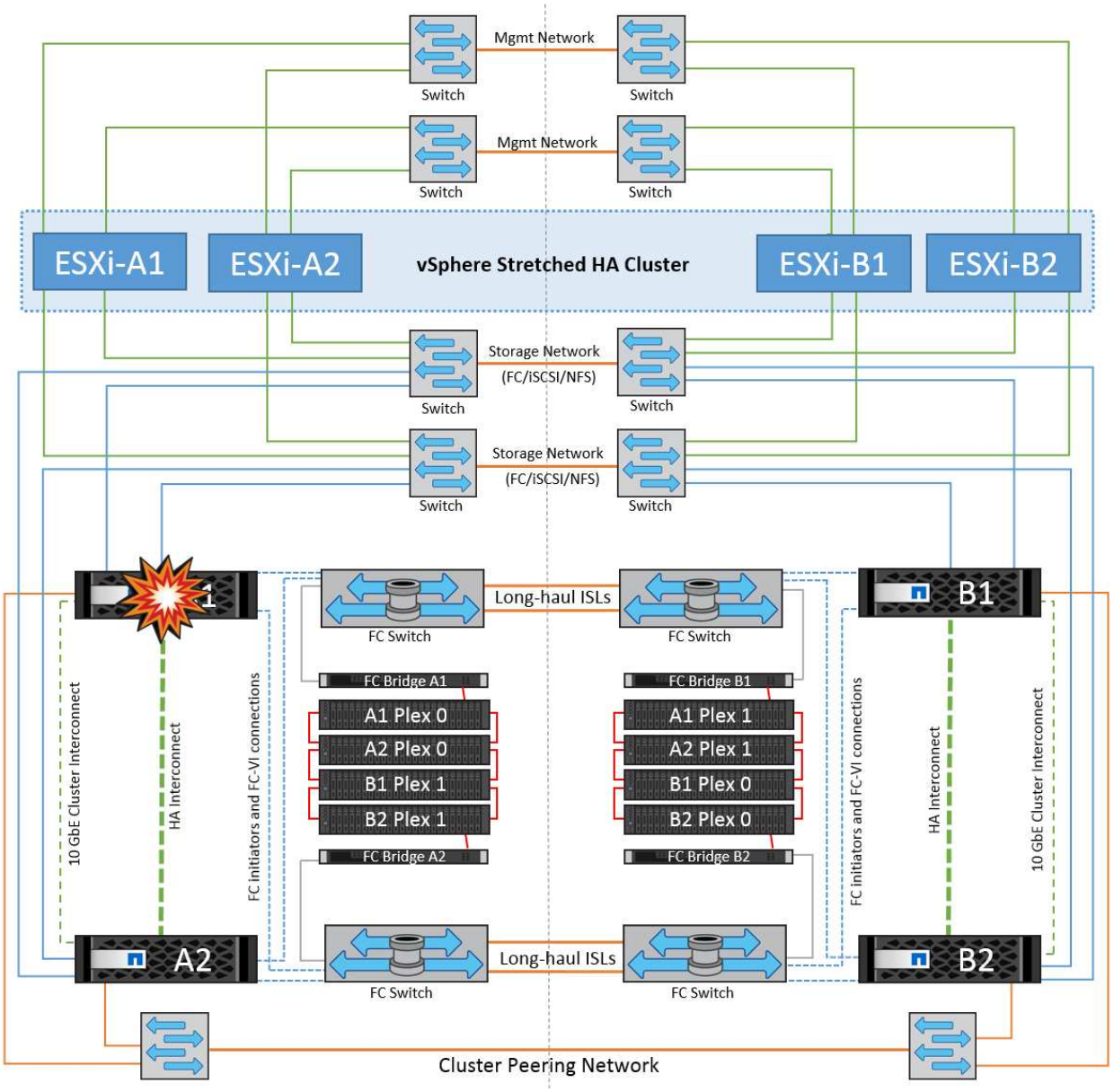


*[NOTA]

- Durante questo periodo, non si verifica alcun impatto sulle operazioni di i/o della macchina virtuale, tuttavia le performance sono peggiorate a causa dell'accesso ai dati dallo shelf di dischi remoto attraverso link ISL.

Guasto a un singolo storage controller

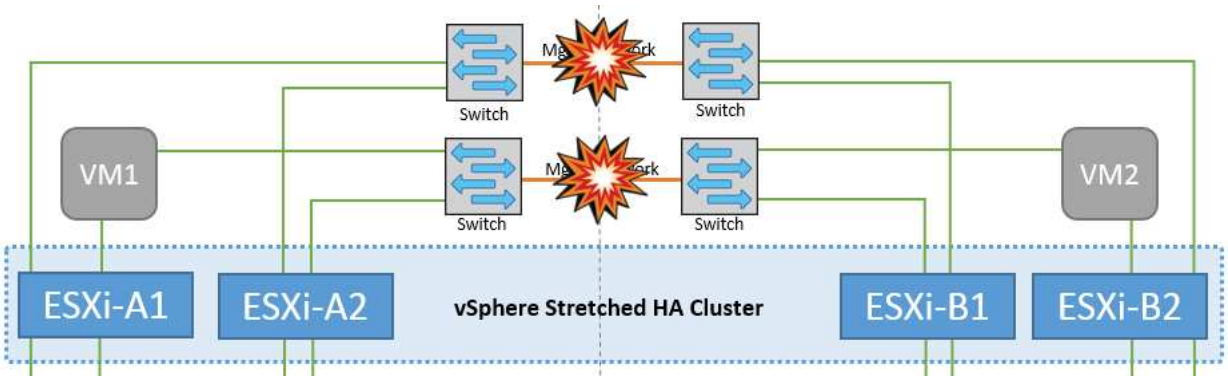
In questo scenario, uno dei due storage controller si guasta in un solo sito. Poiché è presente una coppia ha in ciascun sito, un guasto di un nodo attiva automaticamente il failover sull'altro nodo. Ad esempio, in caso di guasto al nodo A1, il relativo storage e carichi di lavoro vengono trasferiti 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

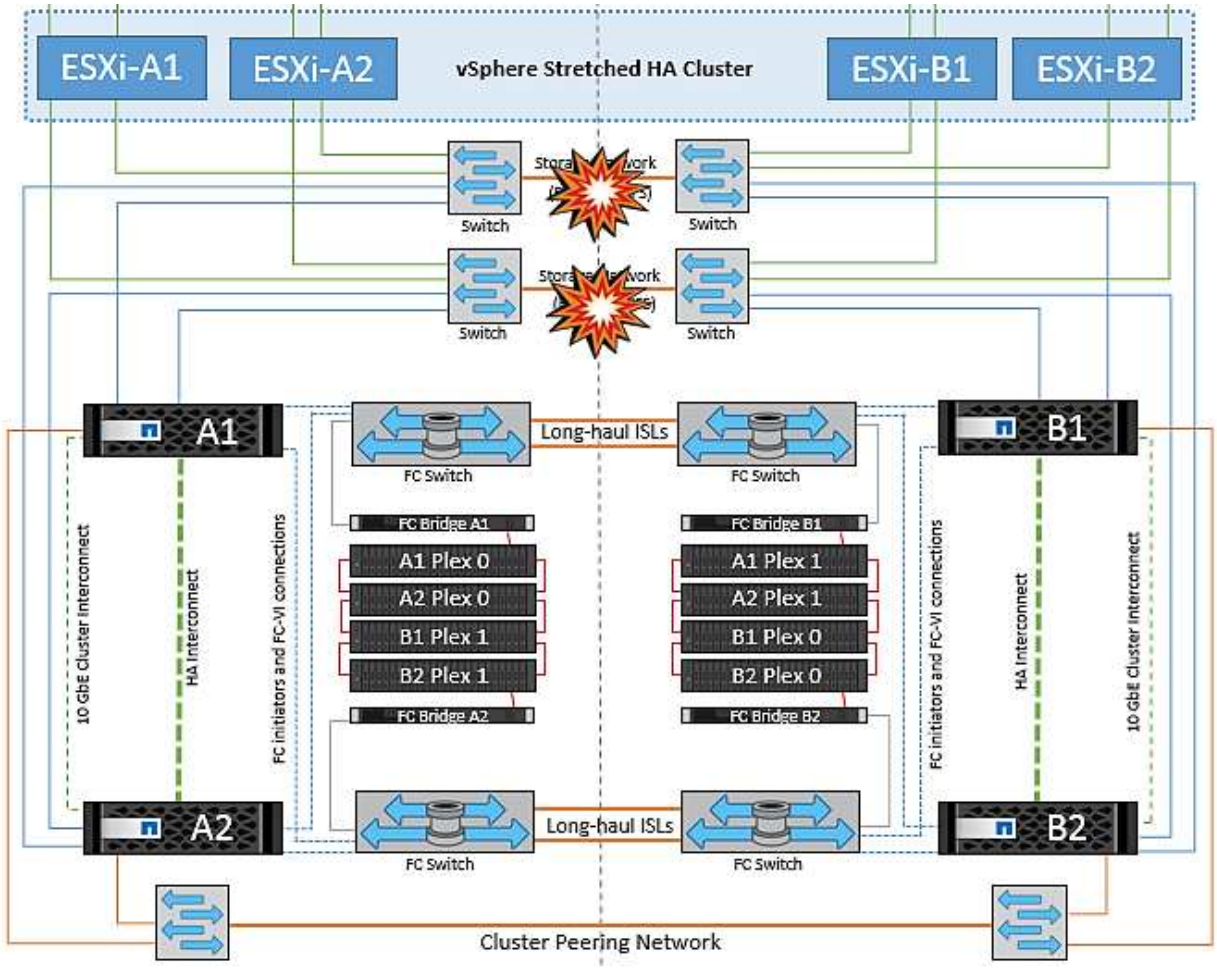
Errore collegamento interswitch sulla rete di gestione



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.

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

Errore collegamento interswitch sulla rete di storage

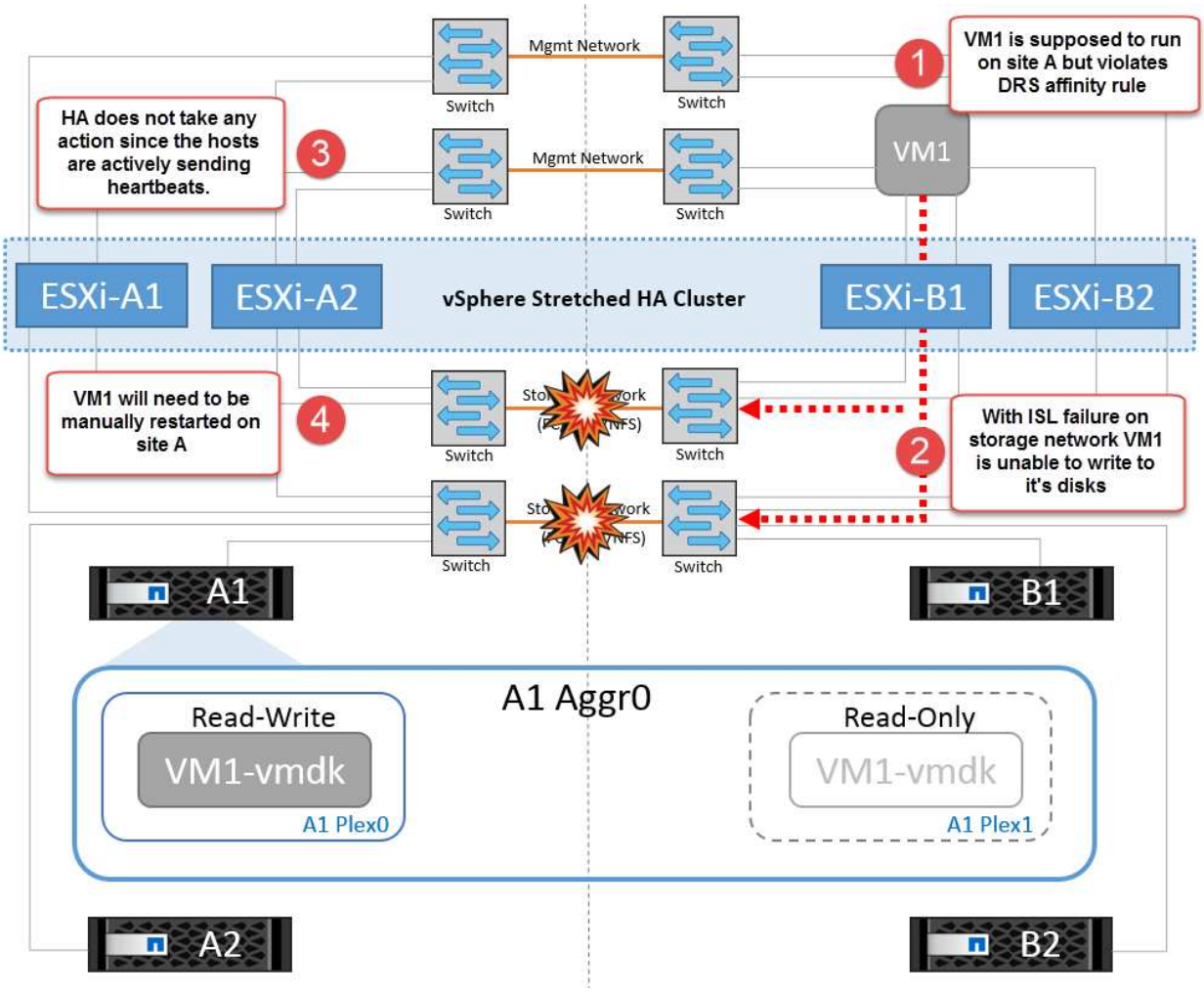


In questo scenario, se si verifica un errore nei collegamenti ISL nella rete di storage backend, gli host sul sito A perderanno l'accesso ai volumi di storage o alle LUN del cluster B nel sito B e viceversa. Le regole VMware DRS sono definite in modo che l'affinità tra il sito host e il sito di storage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

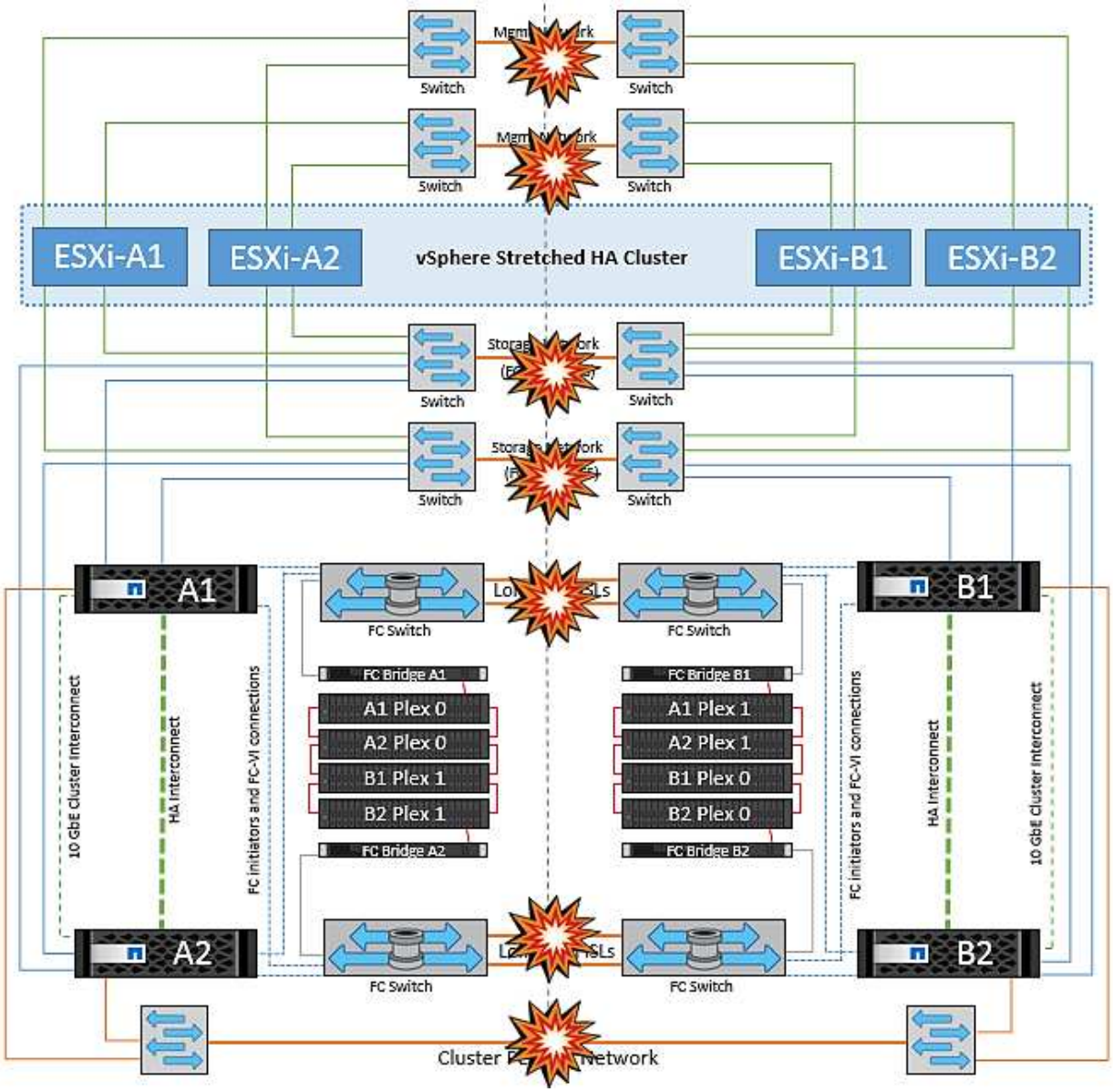
storage non sono attivi e quella particolare macchina virtuale non è attiva. In queste situazioni, VMware ha non intraprende alcuna azione poiché gli host stanno inviando heartbeat. Tali macchine virtuali devono essere spente e attivate manualmente nei rispettivi siti. La figura seguente illustra una VM che viola una regola di affinità DRS.



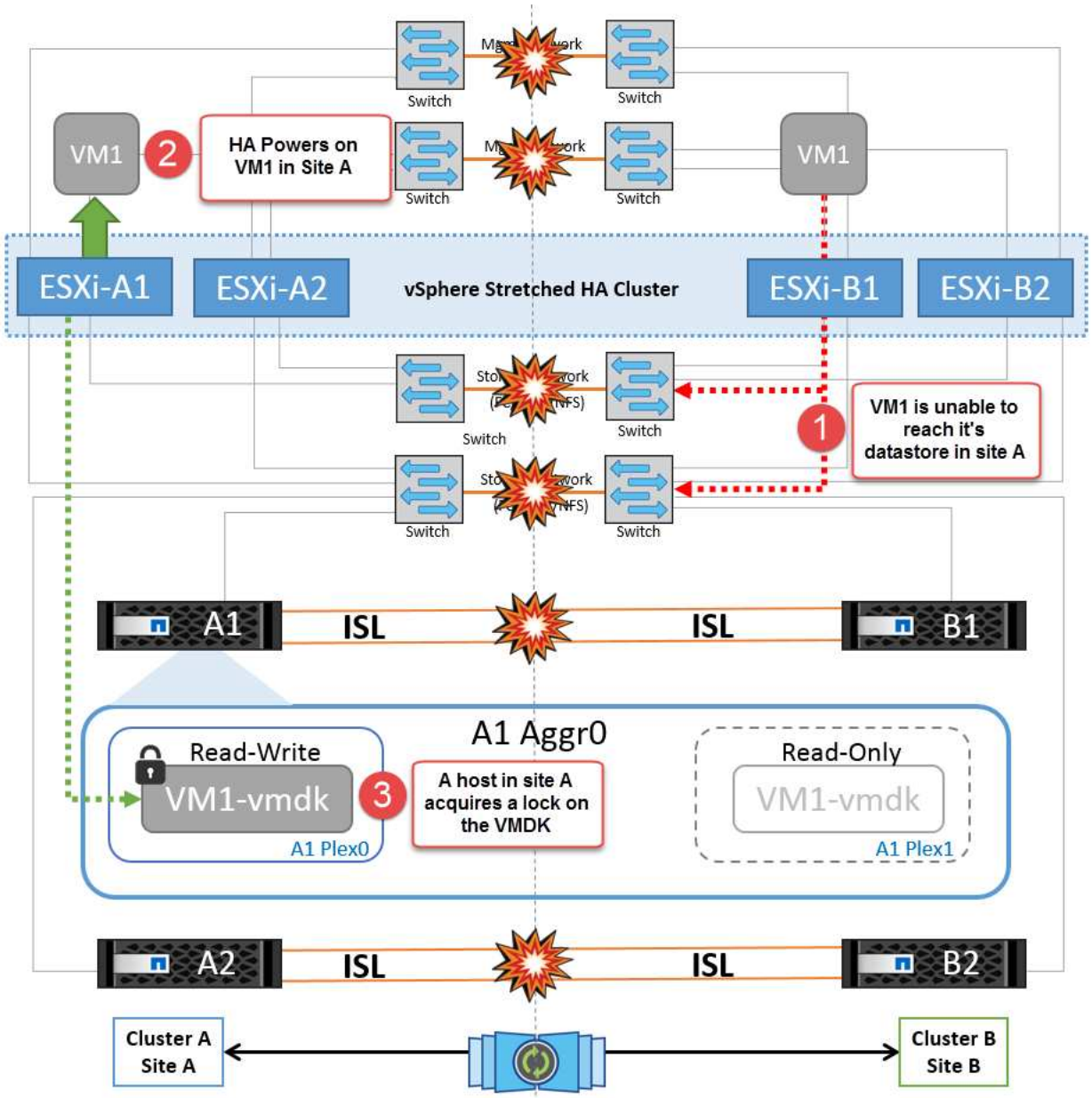
Guasto a tutti gli interswitch o partizione completa del data center

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 supporteranno che gli altri host ESXi presenti nel sito B siano guasti a causa dell'assenza di heartbeat di rete/datastore. VSphere ha nel sito A tenterà di riavviare le macchine virtuali del sito B con un errore infine dovuto al fatto che 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.



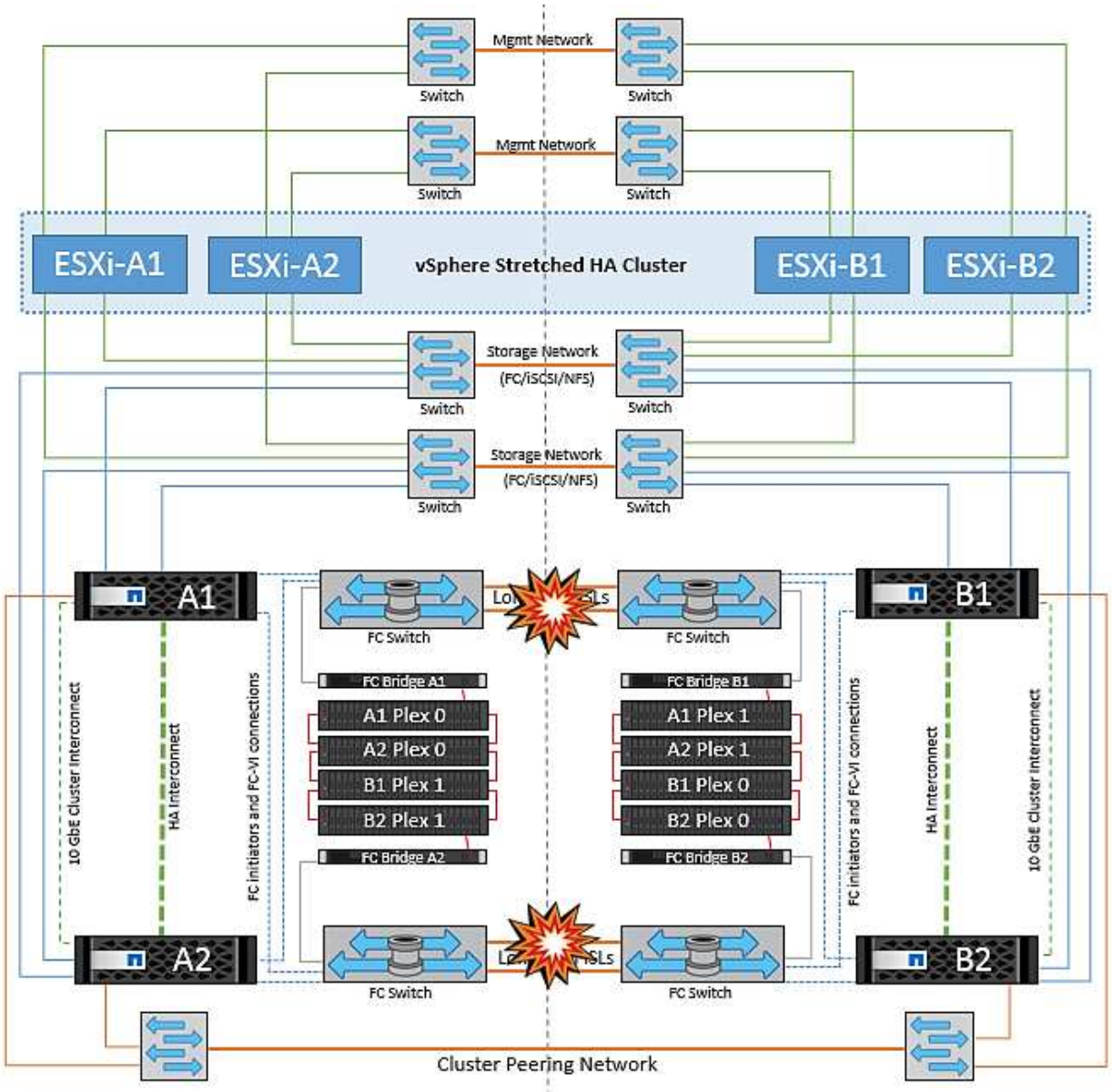
NetApp consiglia di determinare se una macchina virtuale ha violato le regole DRS. Tutte le macchine virtuali in esecuzione da un sito remoto non potranno accedere al datastore, quindi vSphere ha riavvia la macchina virtuale nel sito locale. Una volta che i collegamenti ISL sono tornati in linea, la 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

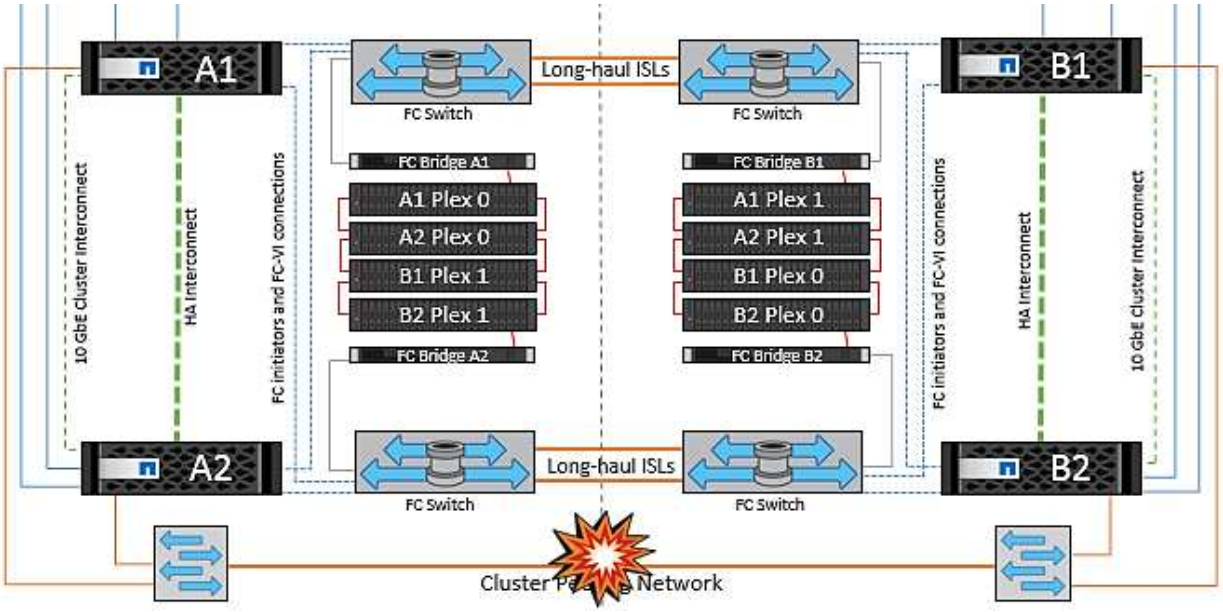
In uno scenario di errore di uno o più ISL, il traffico continua attraverso i collegamenti rimanenti. In caso di errore di tutti gli ISL su entrambi i fabric, in modo da eliminare un collegamento tra i siti per la replica di storage e NVRAM, ciascun controller continuerà a fornire i propri dati locali. Su un minimo di un ISL viene ripristinato, 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 recupero del collegamento al 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.



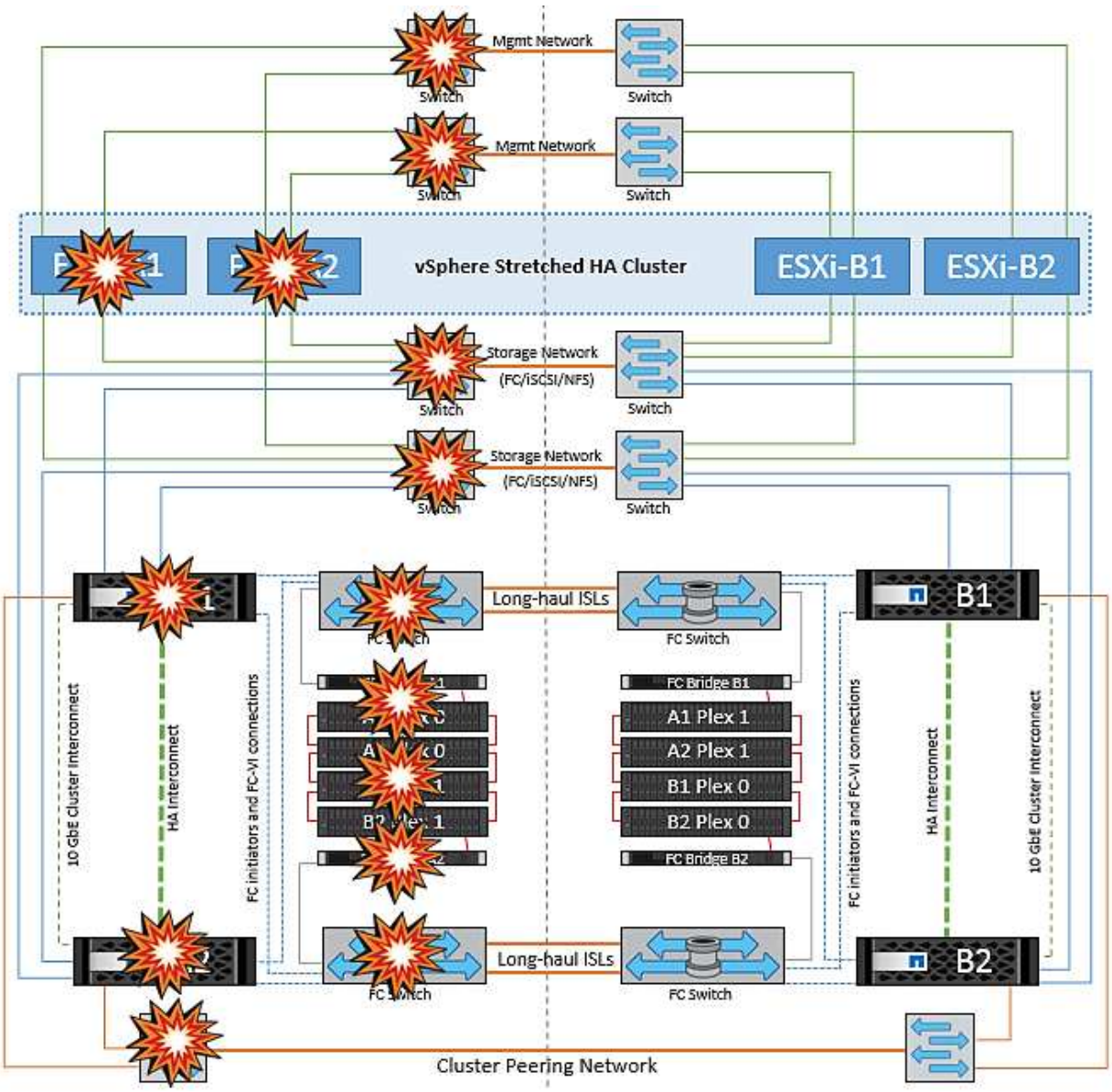
Errore completo del sito

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).

Il master ha non avvia i tentativi di riavvio fino a quando il placement manager non trova lo storage appropriato, quindi in caso di un guasto completo del sito, ciò si verificherebbe 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 Utilizzato per connessioni SOAP su https 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 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 9,13

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 9,13

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

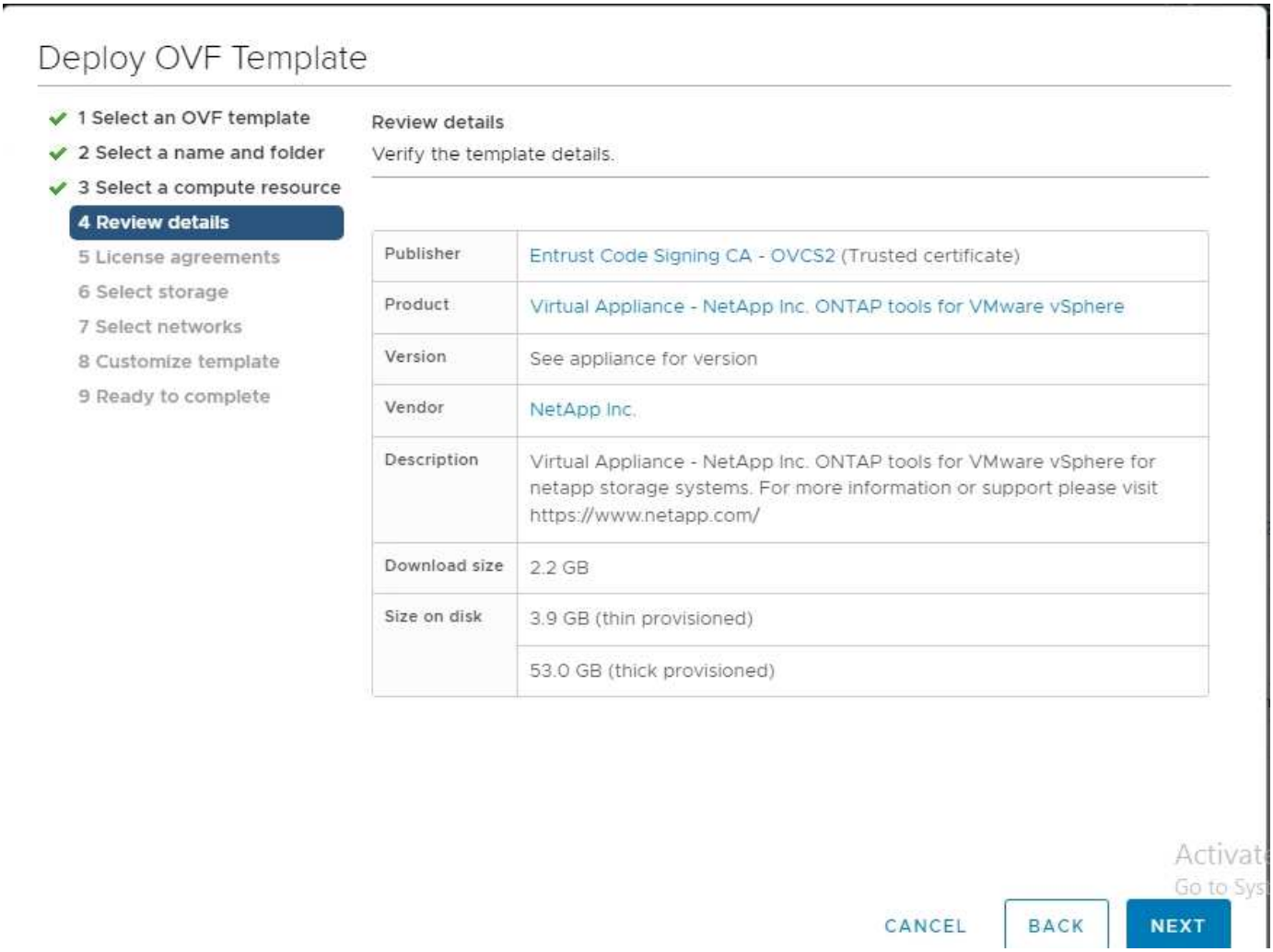
Il pacchetto di installazione vApp viene fornito sotto forma di tarball. Questo tarball contiene certificati intermedi e root per l'appliance virtuale insieme a un file README e un pacchetto OVA. Il file README guida gli utenti su come verificare l'integrità del pacchetto vApp OVA.

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 iniziale, selezionare Amministrazione. b. in 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 per gli strumenti ONTAP 9,13

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

Annotare 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 Utilizzato per connessioni SOAP su HTTPS 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 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 9,13 (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.

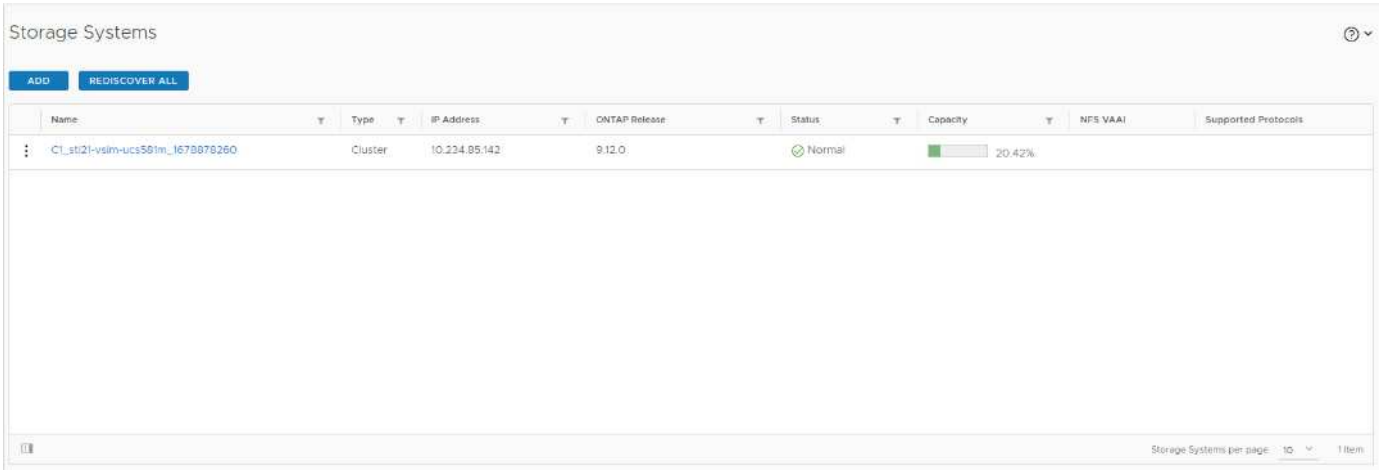
ONTAP tools 9,13 Mutual TLS (autenticazione basata su certificato)

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

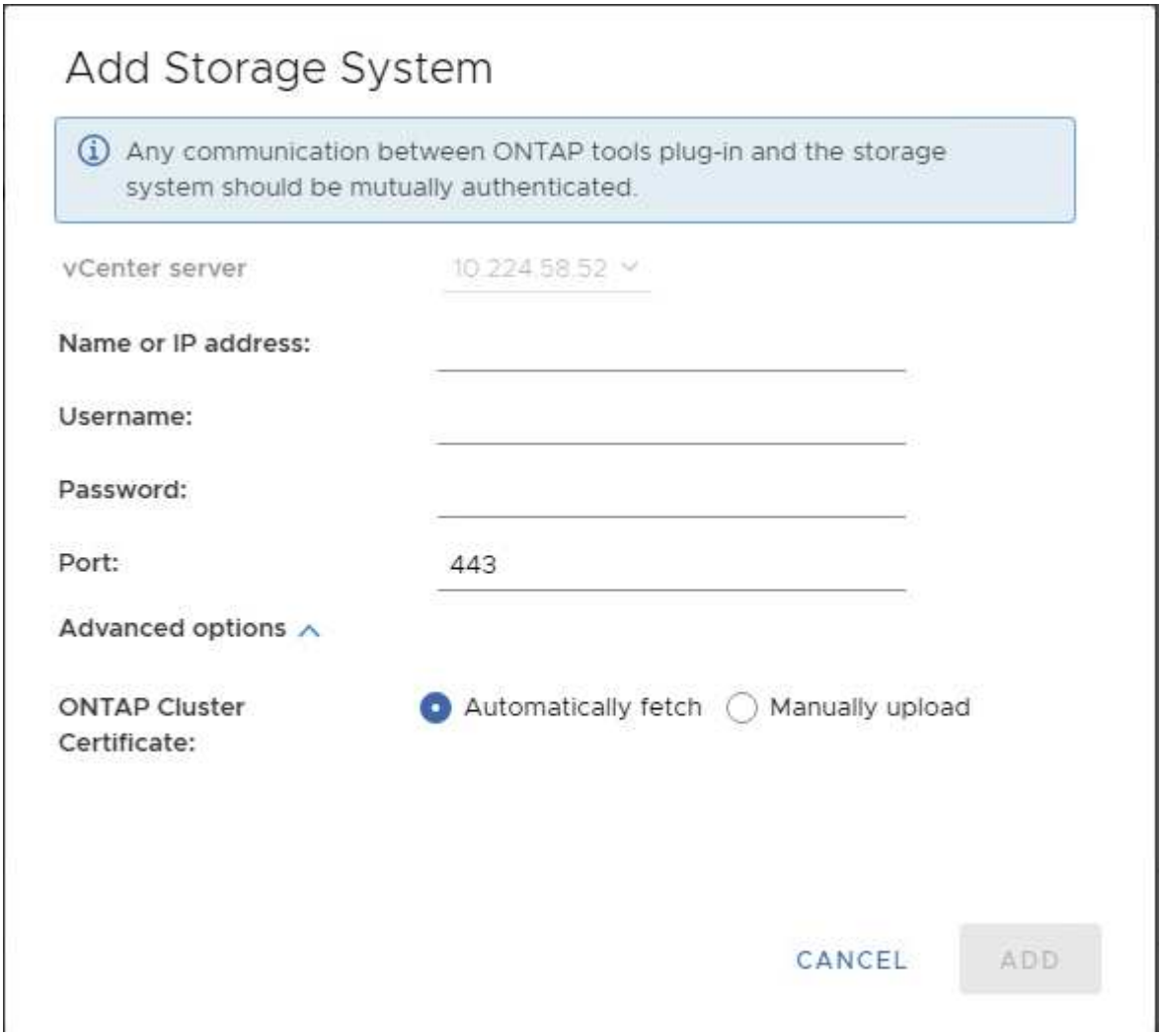
Per tutti i sistemi storage aggiunti in precedenza: Durante un aggiornamento, tutti i sistemi storage aggiunti diventeranno automaticamente attendibili e verranno configurati i meccanismi di autenticazione basati su certificato.

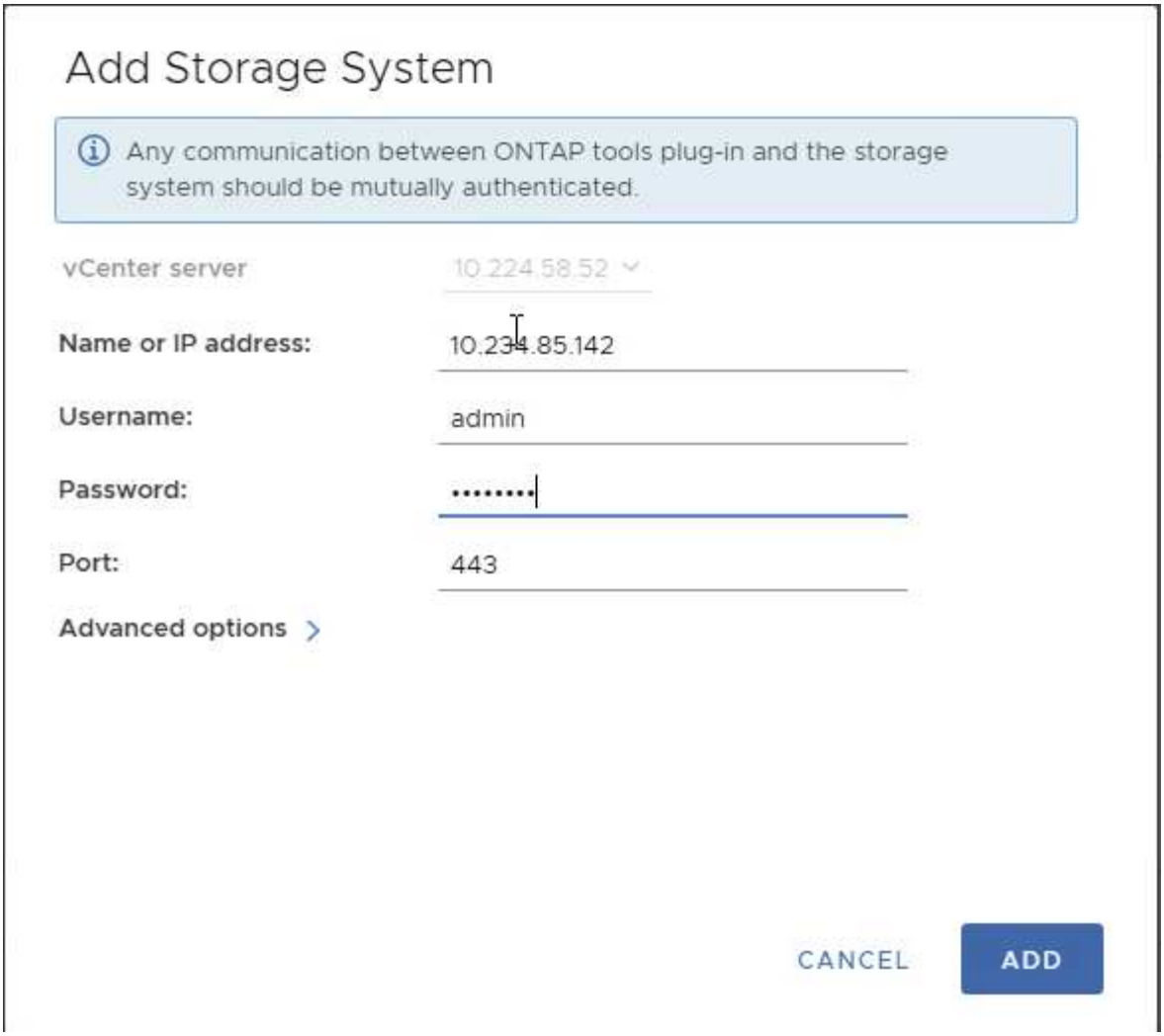
Come nella schermata riportata di seguito, nella pagina di configurazione del cluster viene visualizzato lo stato di Mutual TLS (autenticazione basata su certificato), configurato per ciascun cluster.

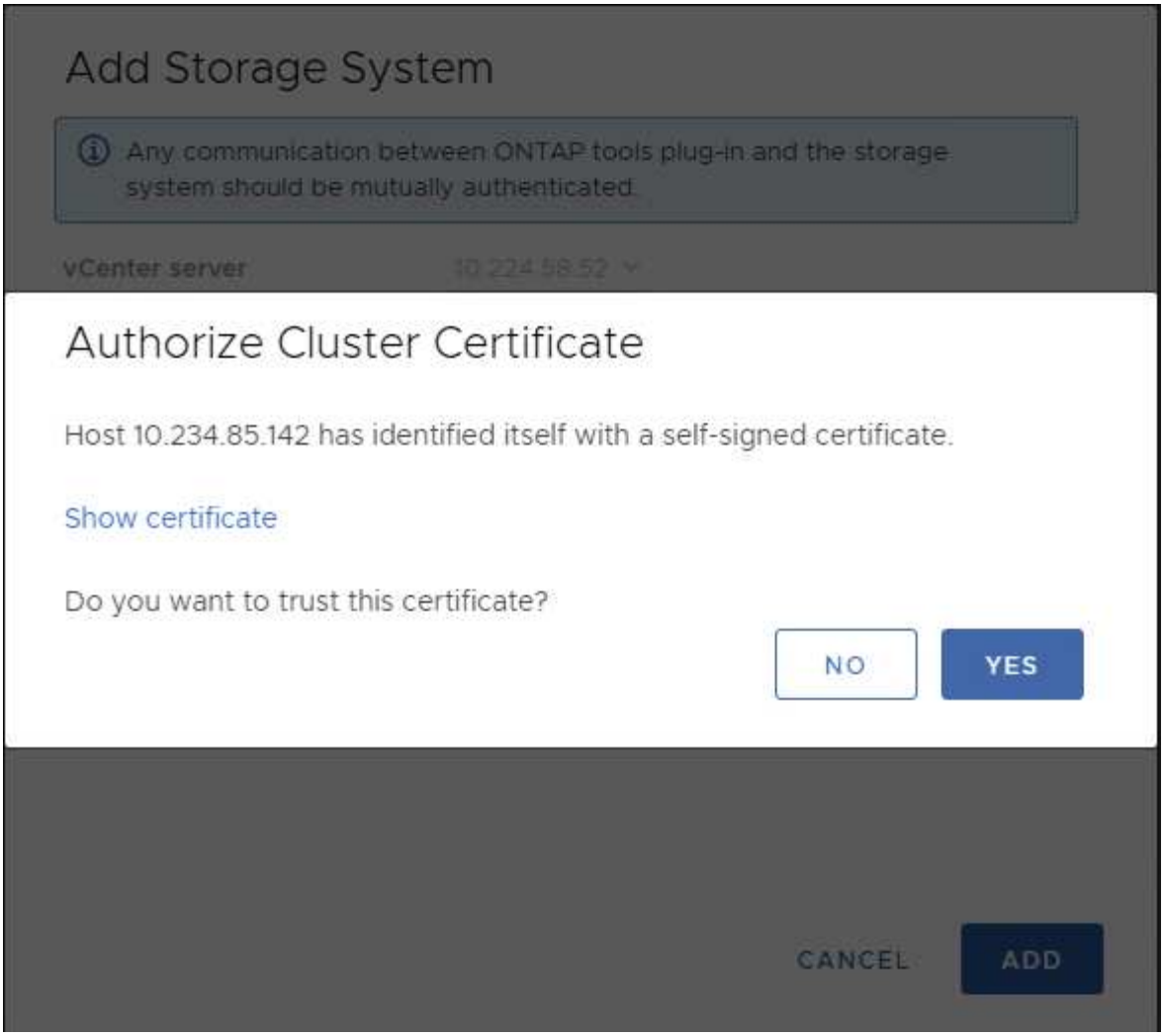


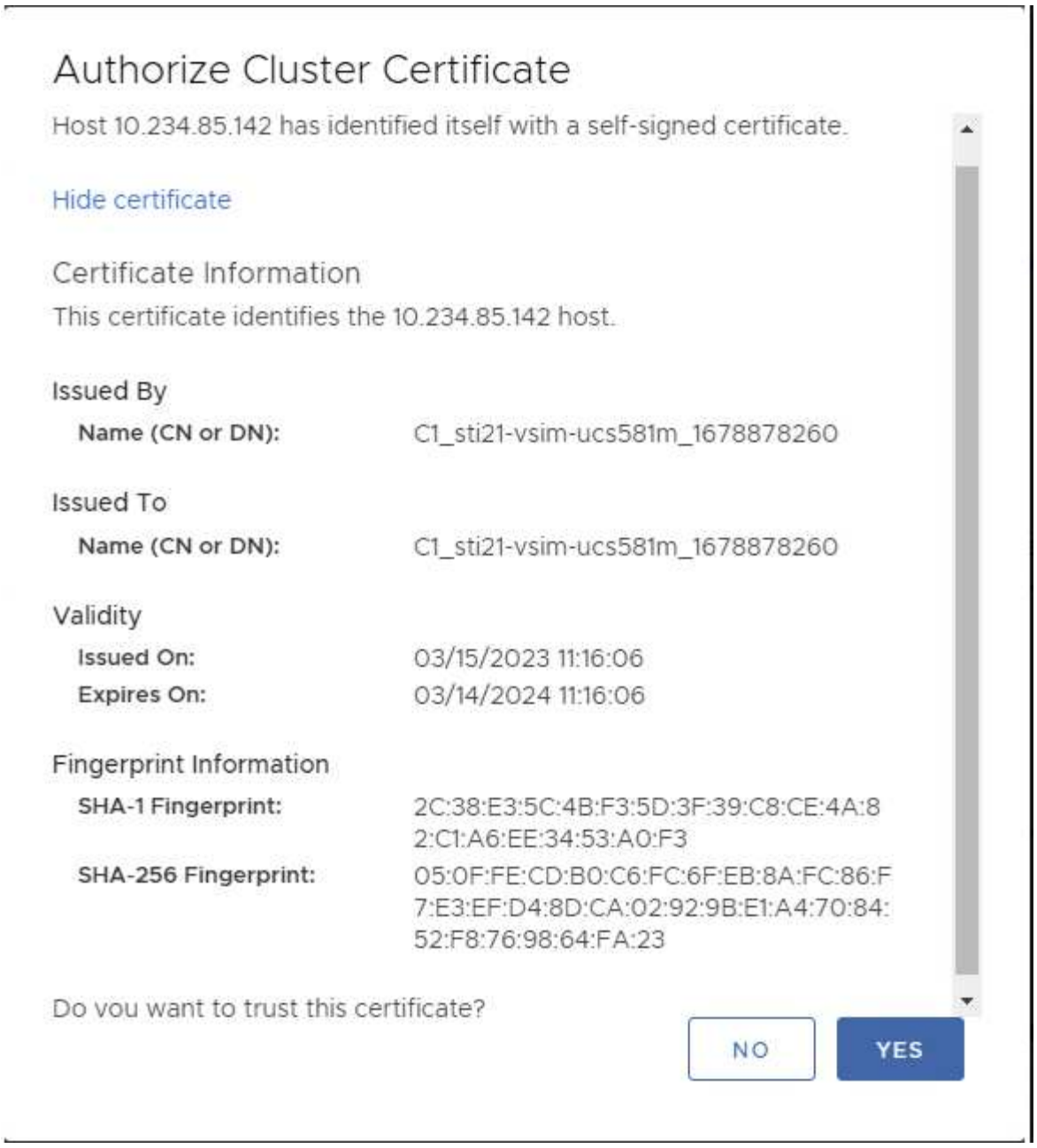
Aggiunta cluster

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

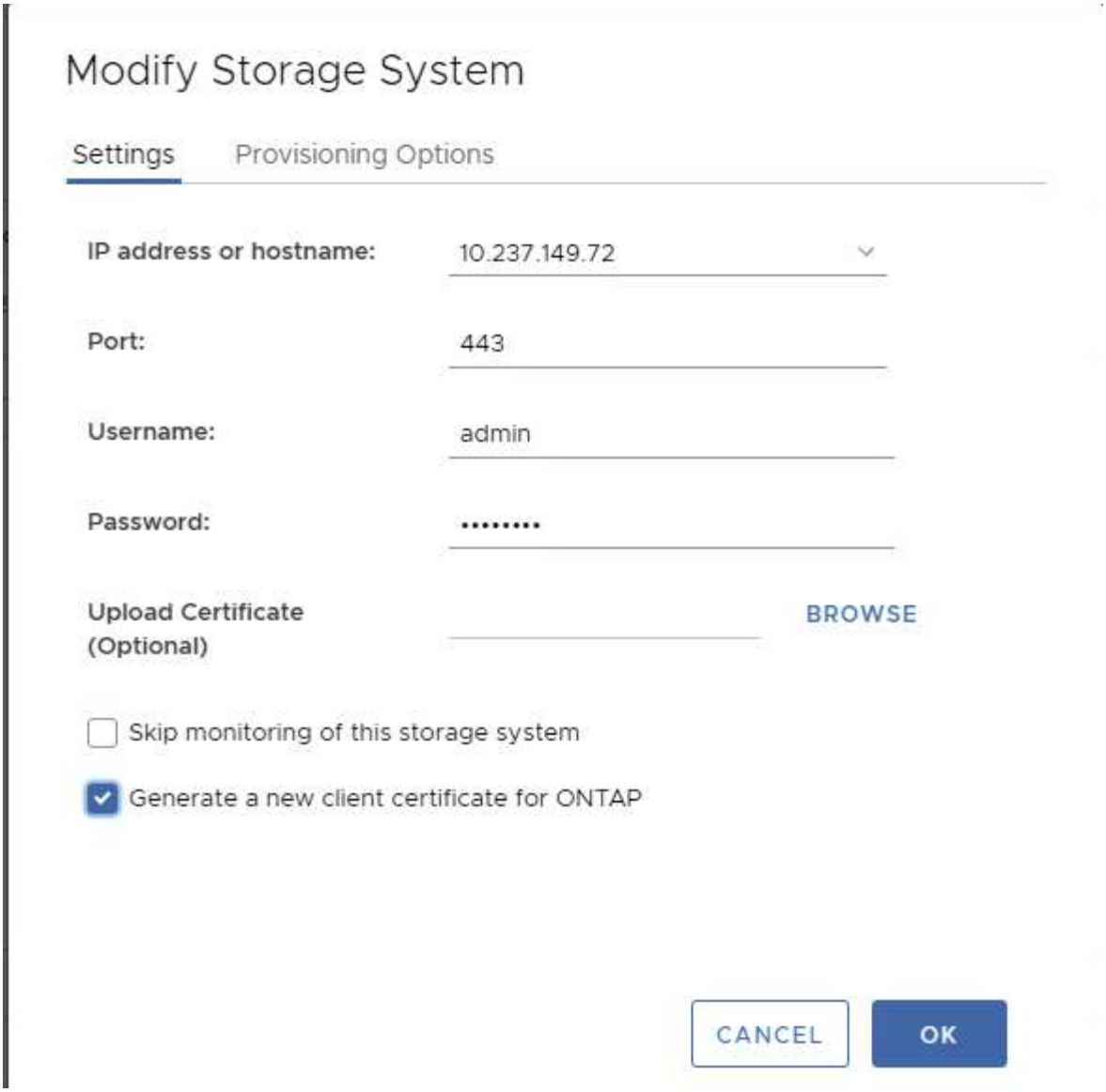

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

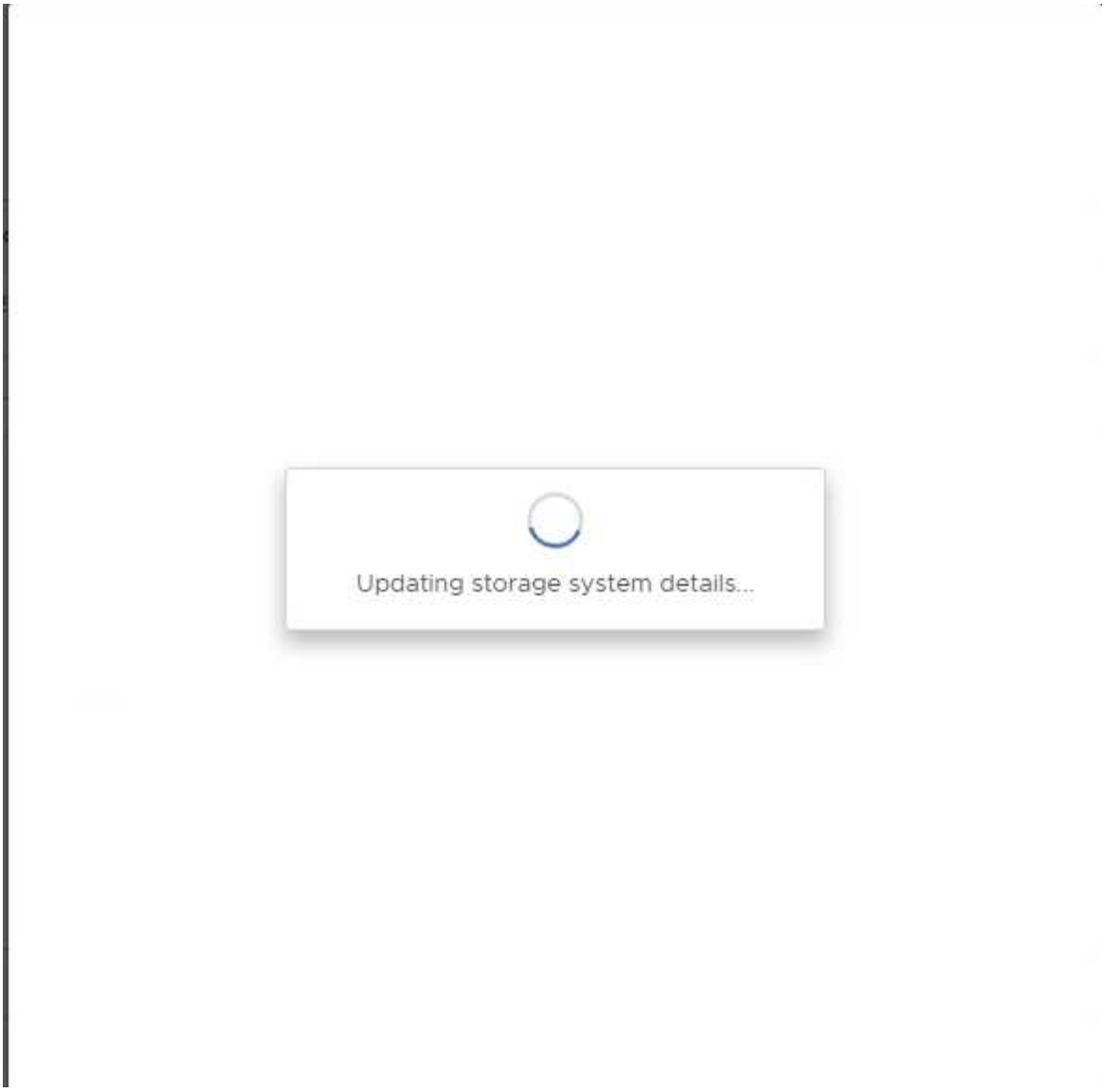


Cluster Edit (Modifica cluster)

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



ONTAP tools 9,13 certificato HTTPS

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 di ONTAP Tools 9,13

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 gli strumenti ONTAP 9,13

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) Strumenti ONTAP per VMware vSphere 9,13

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"}
```

Configurazione del protocollo NTP (Network Time Protocol) per gli strumenti ONTAP 9,13

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.

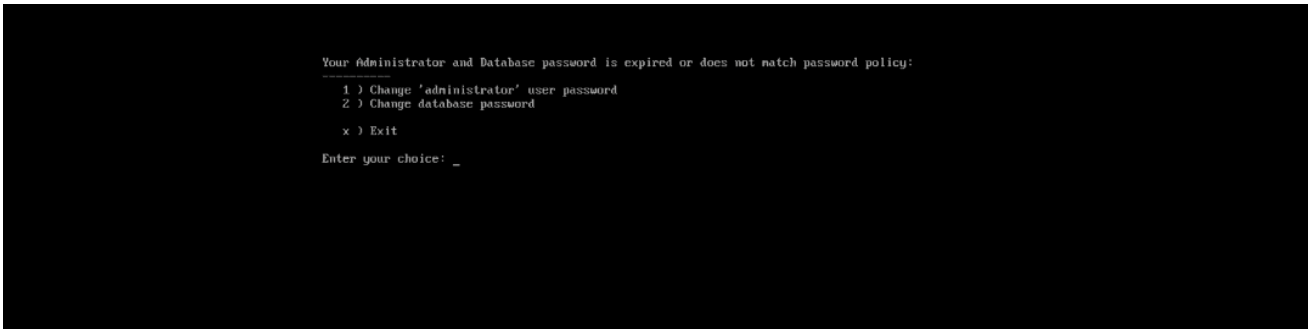
Criteri delle password per gli strumenti ONTAP 9,13

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: