VMware Site Recovery Manager con ONTAP

Enterprise applications

NetApp
February 10, 2026

Sommario

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

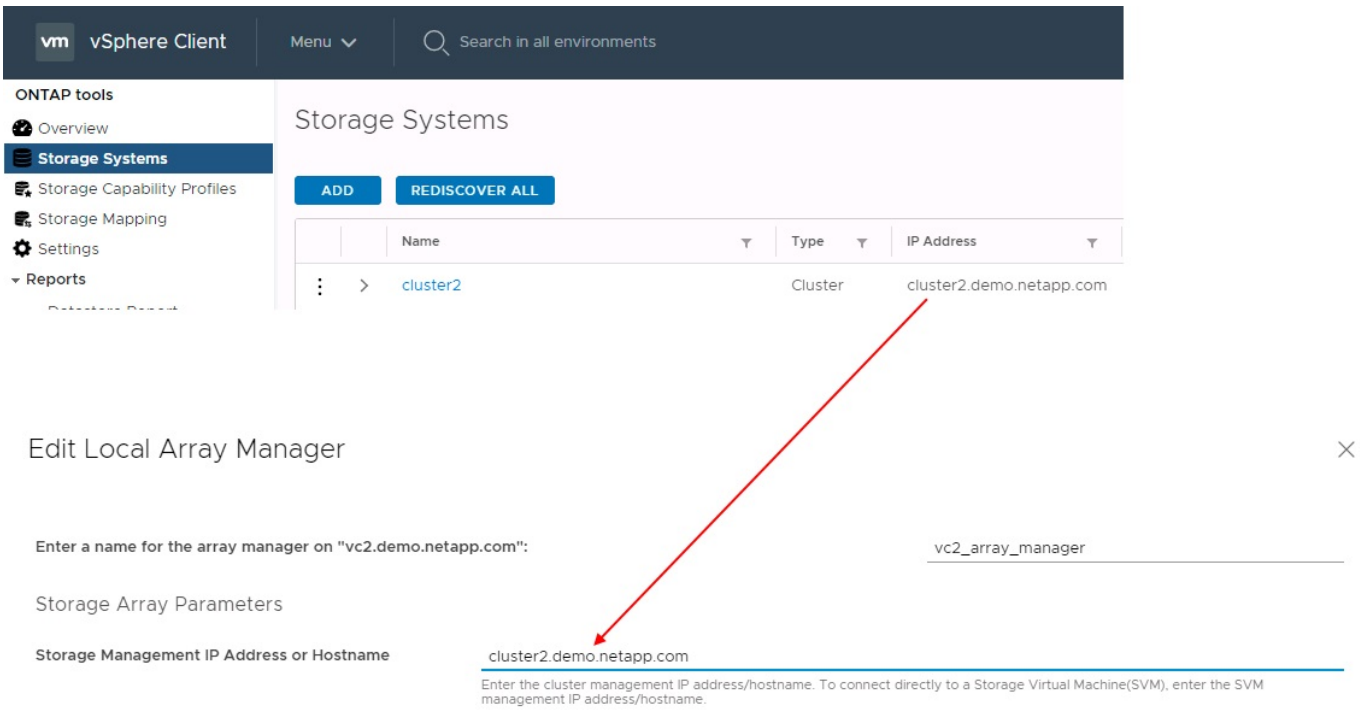
disponibili all'indirizzo "Configurare i volumi per aumentare e ridurre automaticamente le dimensioni".

- 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).

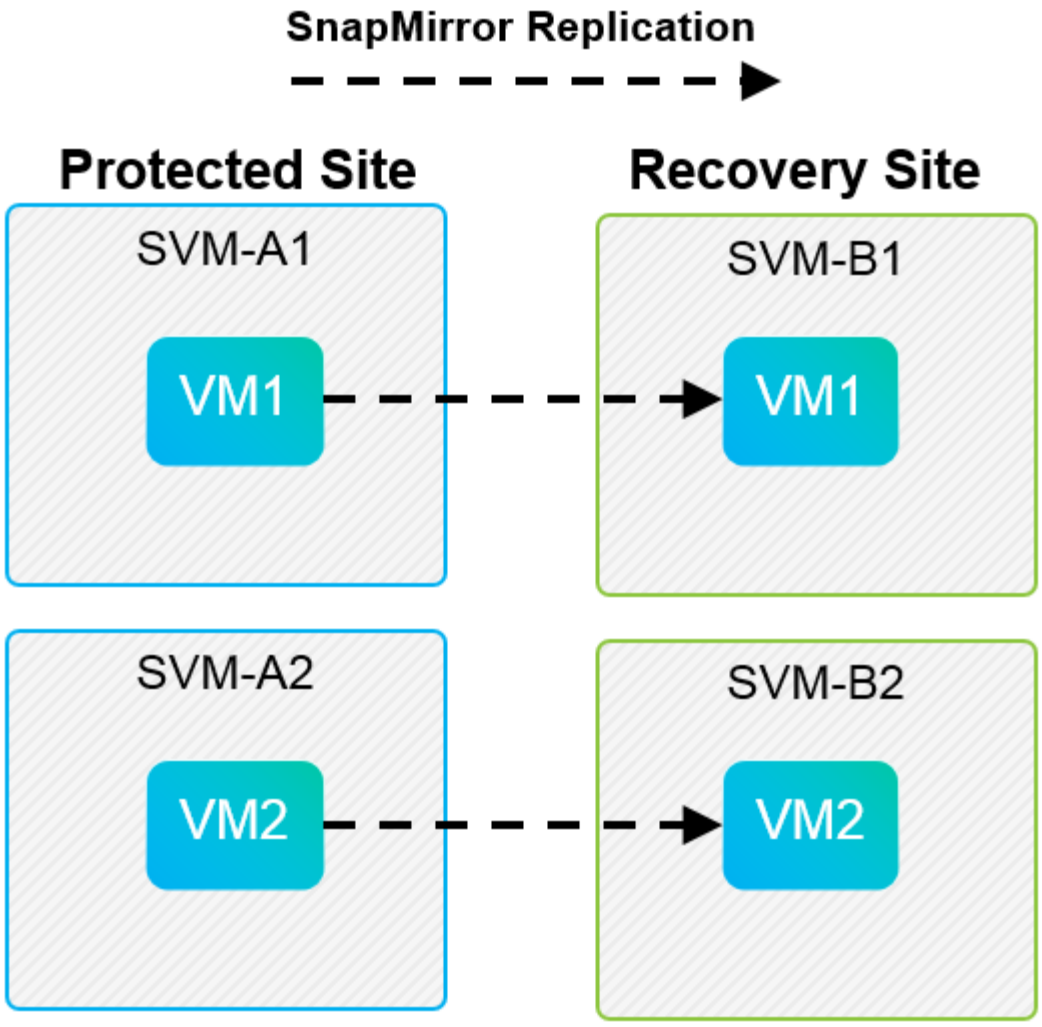
Una singola macchina virtuale non è in grado di gestire i dati (VMDK) o RDM) su più array VLSR per i seguenti motivi:

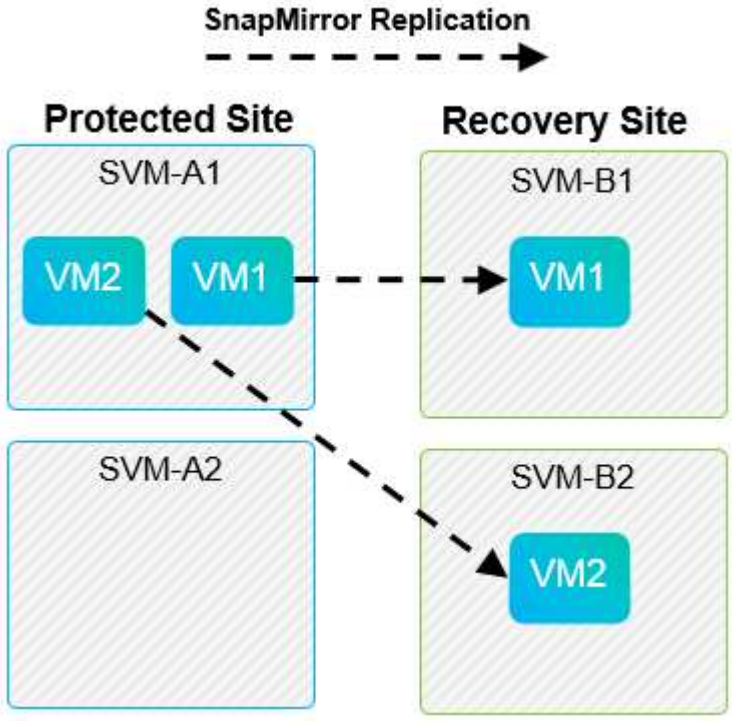
- VLSR vede solo la SVM, non un singolo controller fisico.
- Una SVM può controllare LUN e volumi che si estendono su più nodi in un cluster.

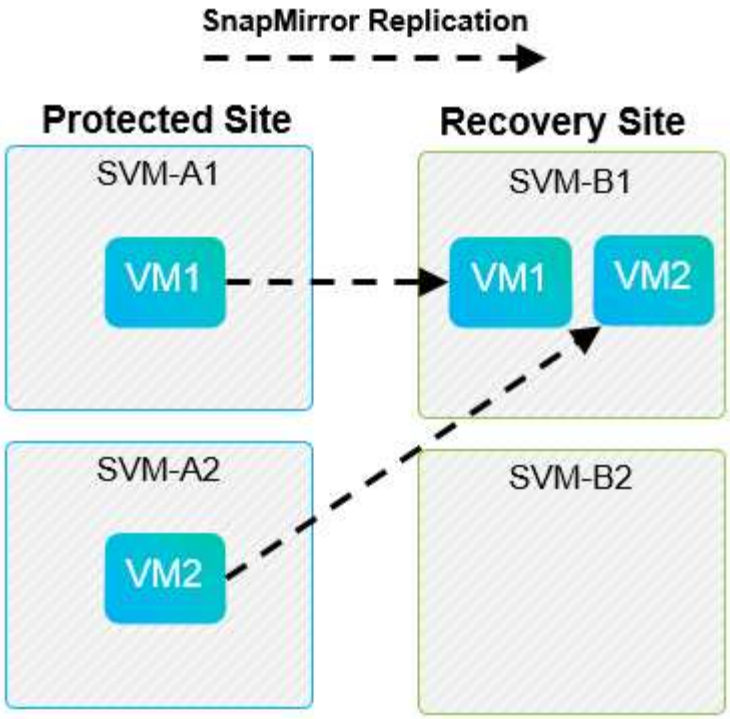
Best practice
Per determinare la supportabilità, tenere presente questa regola: Per proteggere una macchina virtuale utilizzando VLSR e NetApp SRA, tutte le parti della macchina virtuale devono esistere su un solo SVM. Questa regola si applica sia al sito protetto che al sito di ripristino.

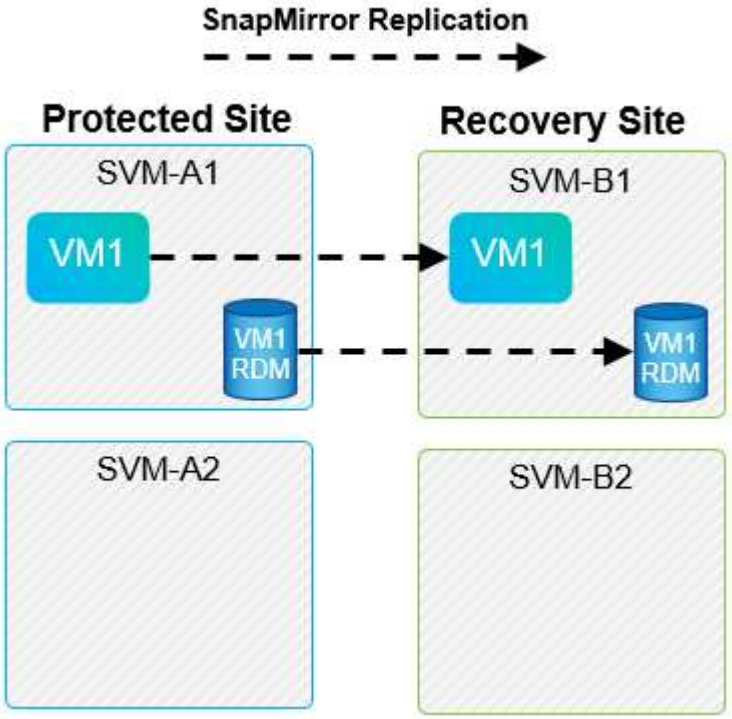
Layout SnapMirror supportati

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
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2


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





Supporto VMFS con sincronizzazione attiva SnapMirror

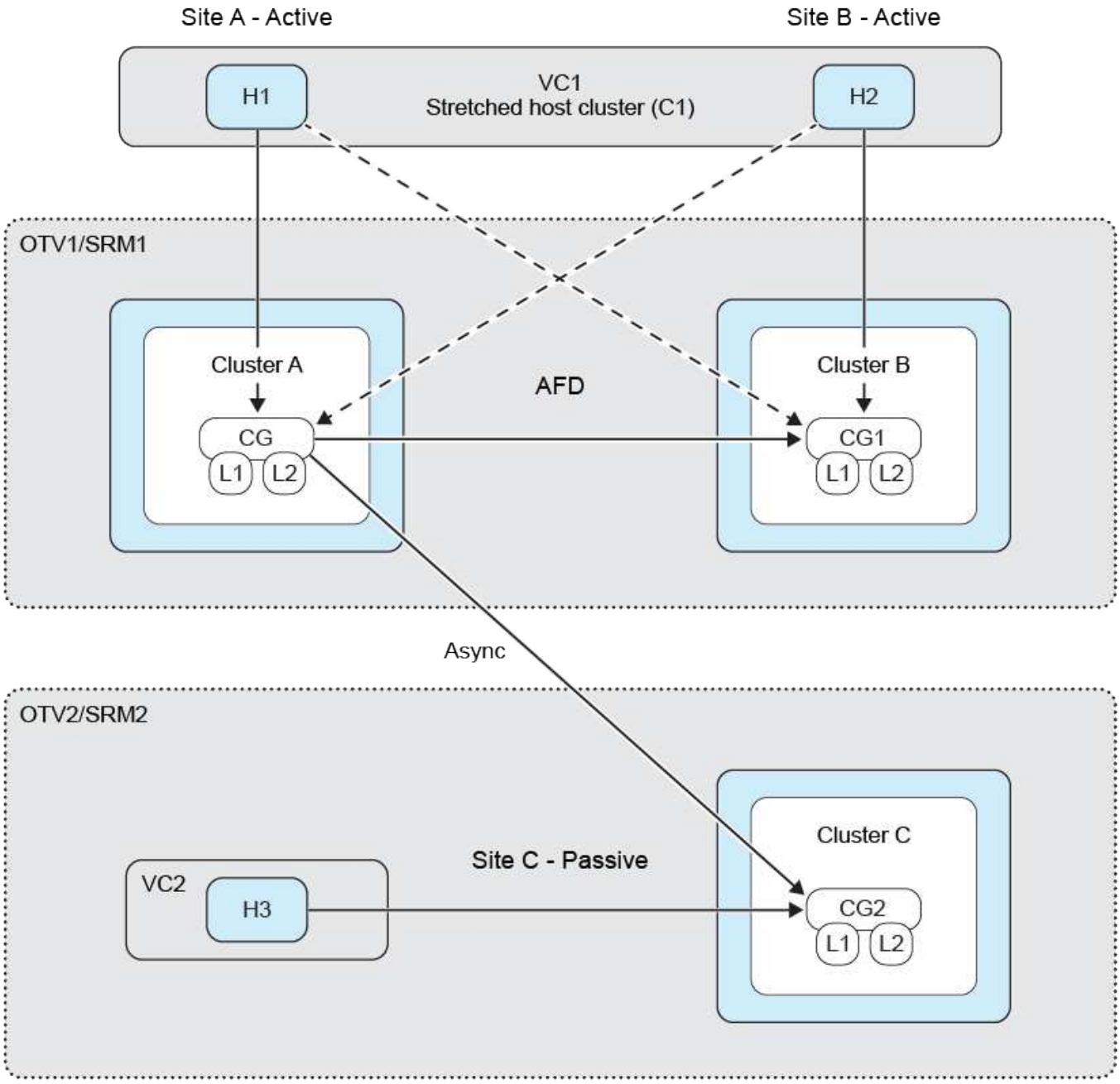
Gli strumenti ONTAP 10.3 e versioni successive supportano anche la protezione dei datastore VMFS con SnapMirror Active Sync (SMas). Ciò consente un failover trasparente per la continuità aziendale tra due data center (definiti domini di errore) relativamente vicini tra loro. Il disaster recovery a lunga 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

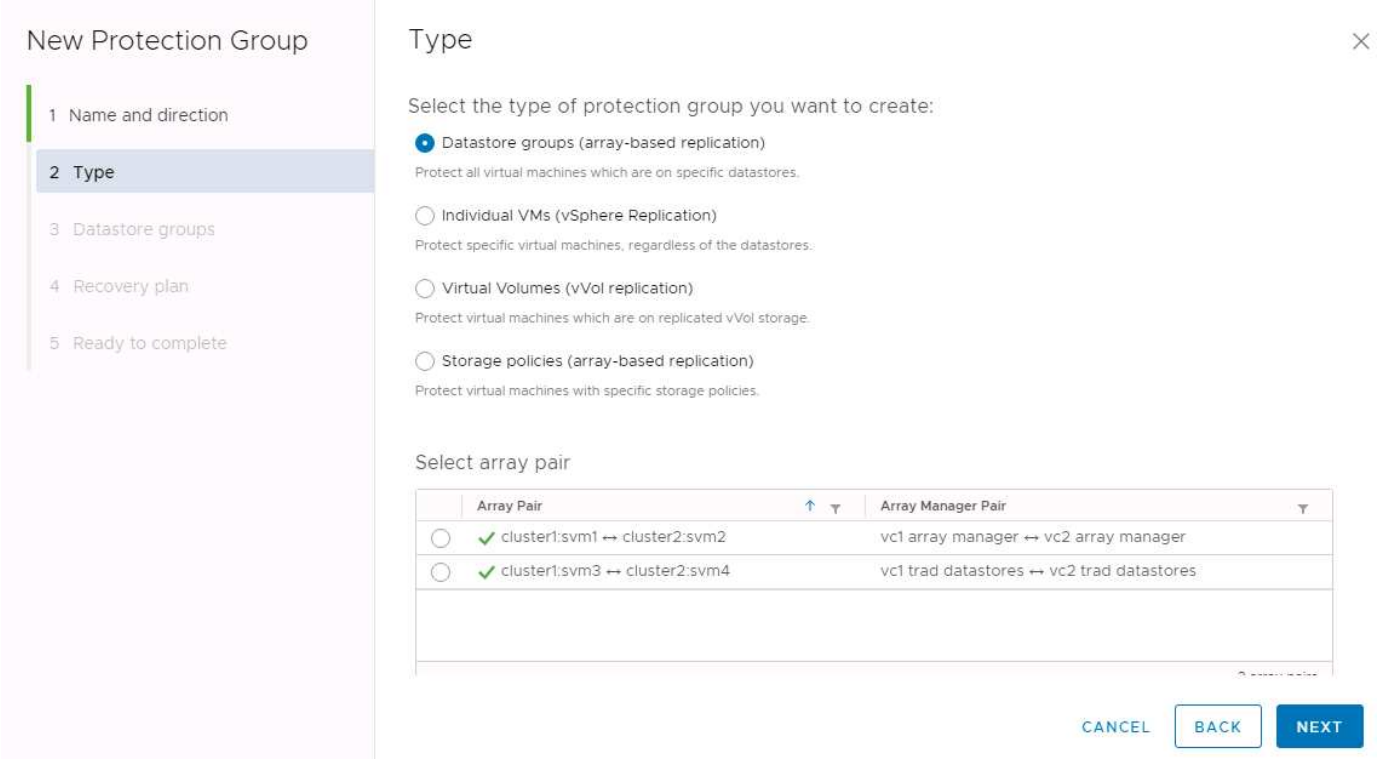
la coerenza nell'ordine di scrittura in quanto membri dello stesso CG.

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.



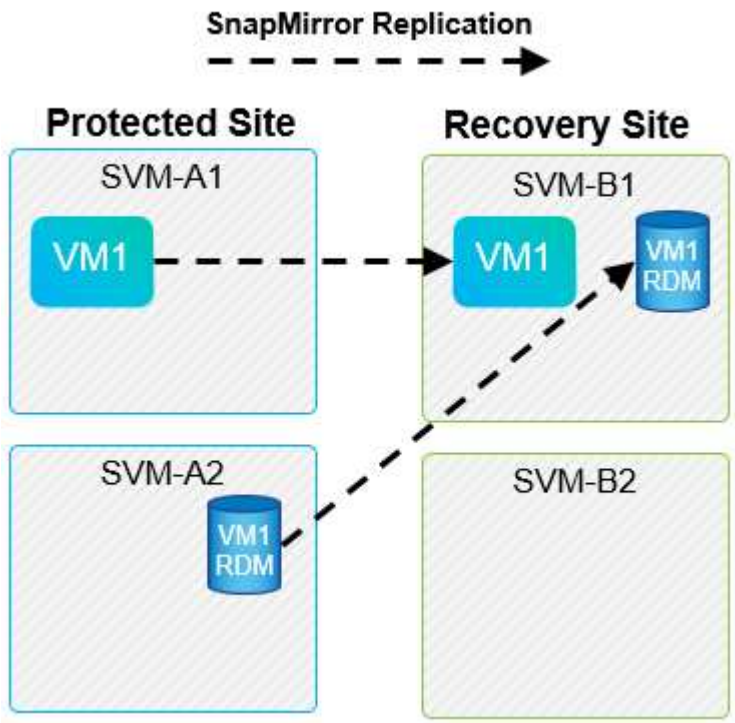
Layout di Array Manager supportati

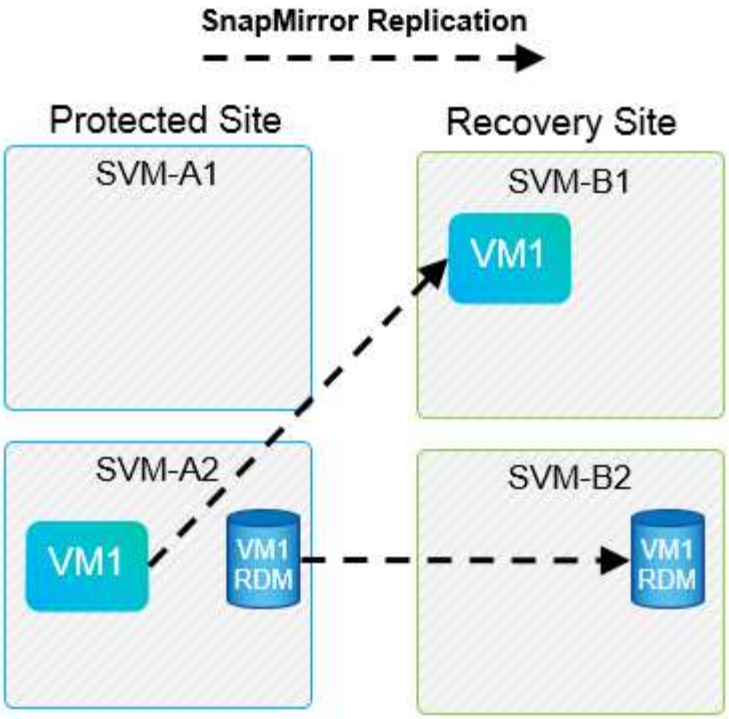
Quando si utilizza la replica basata su array (ABR) in VLSR, i gruppi di protezione vengono isolati in una singola coppia di array, come illustrato nella seguente schermata. In questo scenario, `SVM1` e `SVM2` vengono sottoposti a peed con `SVM3` e `SVM4` nel sito di recovery. Tuttavia, è possibile selezionare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



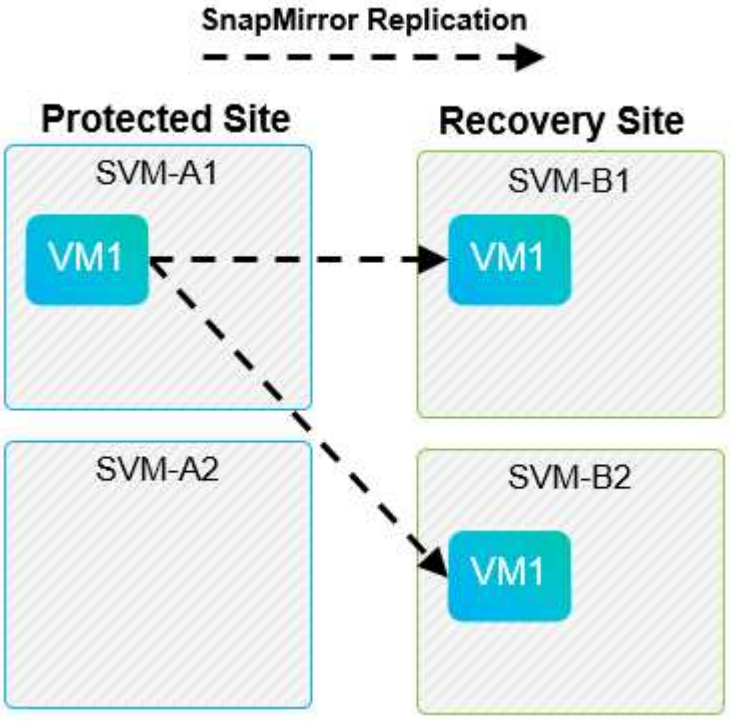
Layout non supportati

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.





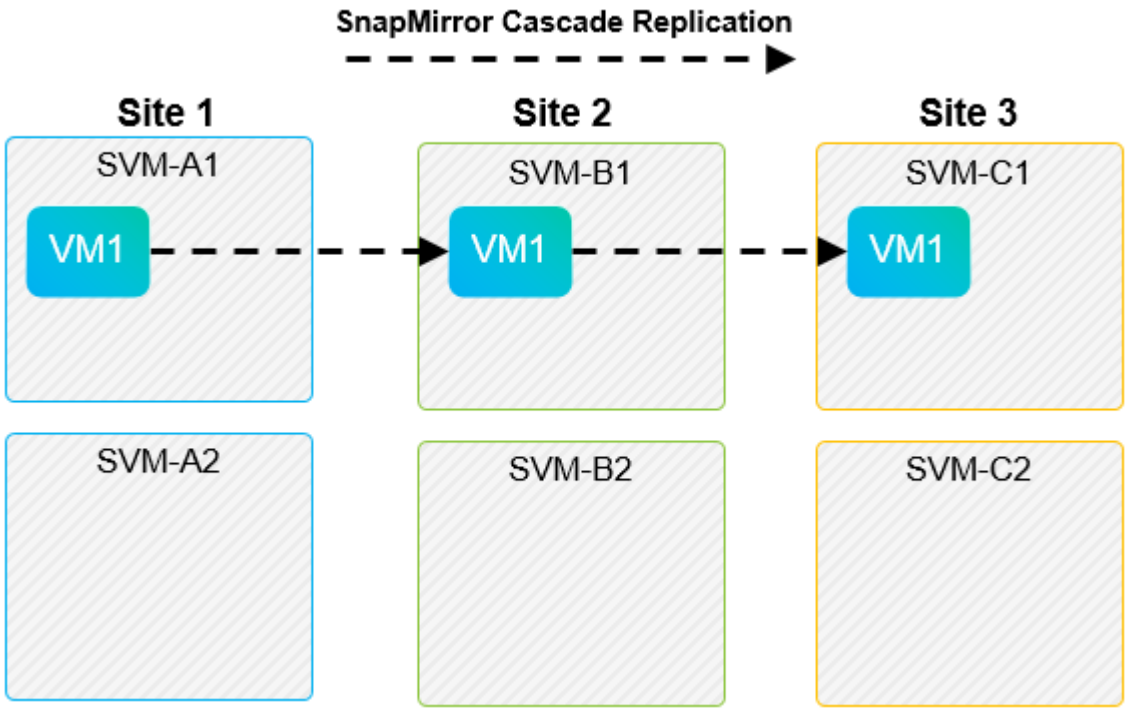
Qualsiasi relazione di replica in cui un singolo volume NetApp viene replicato da una SVM di origine a più destinazioni nella stessa SVM o in SVM differenti viene definita fan-out di SnapMirror. Fan-out non supportato con VLSR. Nell'esempio mostrato nella figura seguente, `VM1` non è possibile configurare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

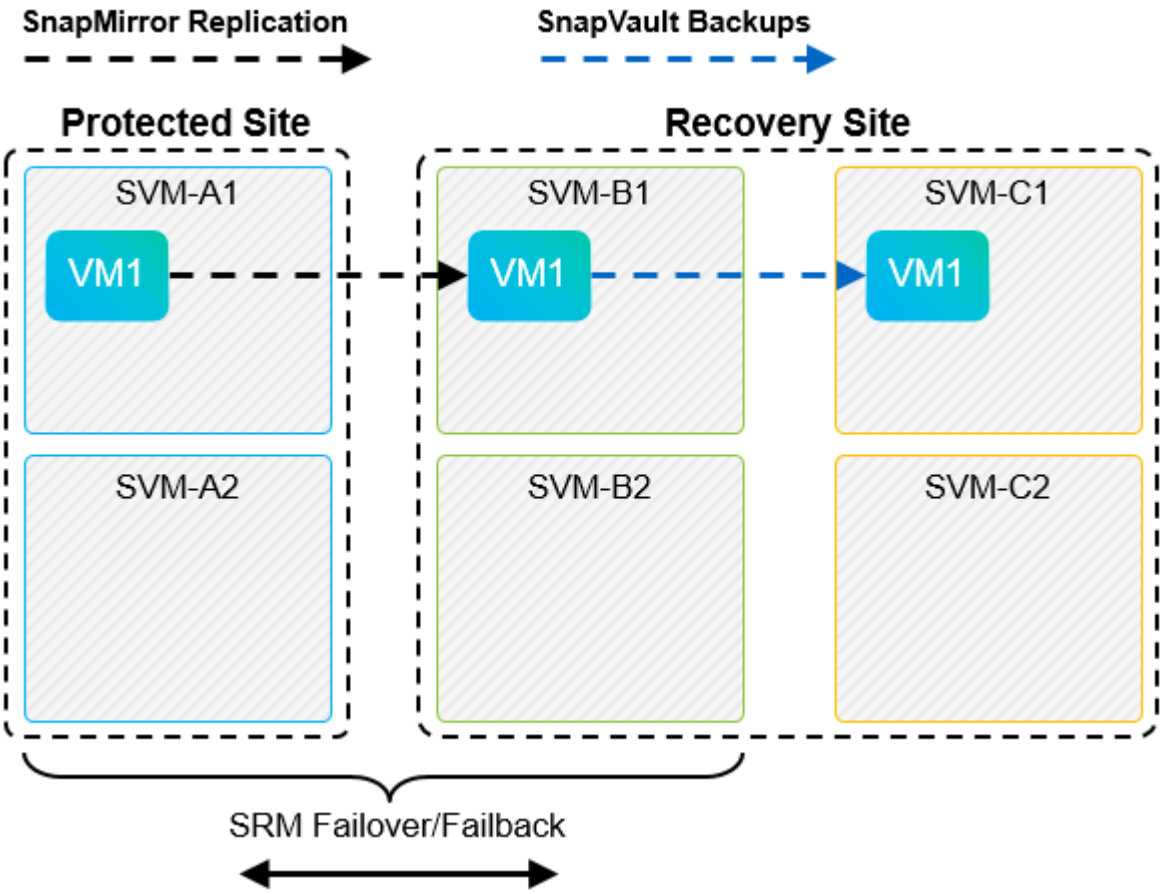
verifica il failover VLSR o l'inversione della replica.

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.

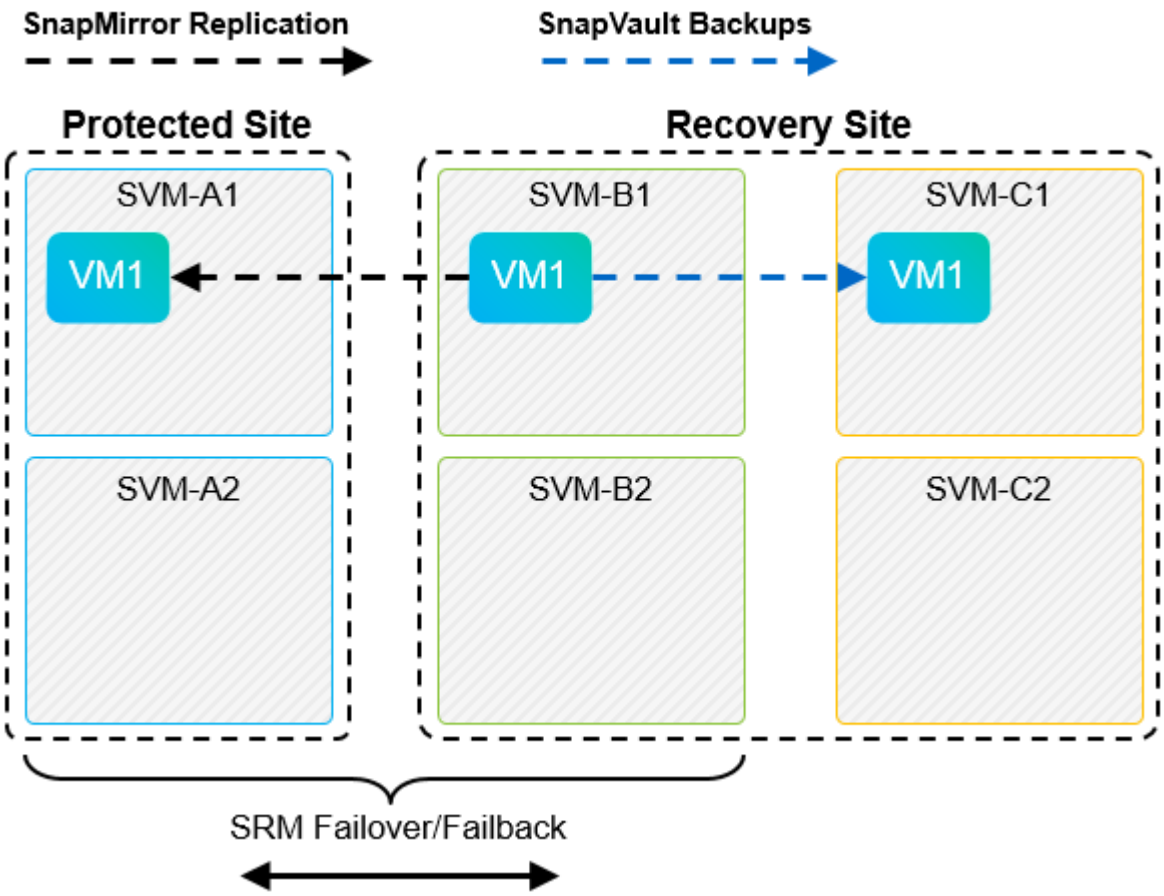
In un ambiente VMware, ogni datastore dispone di un UUID (Universal Unique Identifier) e ogni VM dispone di un MOID (Managed Object ID) univoco. Questi ID non vengono gestiti da VLSR durante il failover o il failback. Poiché gli UUID degli archivi di dati e i MOID delle macchine virtuali non vengono 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.