VMware Site Recovery Manager con ONTAP

Enterprise applications

NetApp
May 09, 2024

Sommario

VMware Site Recovery Manager con ONTAP

VMware Site Recovery Manager con ONTAP

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

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

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

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

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

Perché utilizzare ONTAP con SRM?

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

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

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

In che modo SRM sfrutta ONTAP 9

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

- Il plug-in vCenter, precedentemente noto come Virtual Storage Console (VSC), semplifica le funzionalità di gestione ed efficienza dello storage, migliora la disponibilità e riduce i costi di storage e l'overhead

operativo, sia che si utilizzi SAN che NAS. Utilizza le Best practice per il provisioning degli archivi dati e ottimizza le impostazioni degli host ESXi per gli ambienti di storage a blocchi e NFS. Per tutti questi vantaggi, NetApp consiglia questo plug-in quando si utilizza vSphere con sistemi che eseguono il software ONTAP.

- Il provider VASA per ONTAP supporta il framework VMware vStorage API for Storage Awareness (VASA). IL provider VASA connette vCenter Server a ONTAP per facilitare il provisioning e il monitoraggio dello storage delle macchine virtuali. Consente il supporto di VMware Virtual Volumes (vVol) e la gestione dei profili di capacità dello storage (incluse le funzionalità di replica di vVol) e delle performance di VM vVol individuali. Fornisce inoltre allarmi per il monitoraggio della capacità e della conformità con i profili. Se utilizzato in combinazione con SRM, il provider VASA per ONTAP consente il supporto delle macchine virtuali basate su vVol senza richiedere l'installazione di un adattatore SRA sul server SRM.
- SRA viene utilizzato insieme a SRM per gestire la replica dei dati delle macchine virtuali tra siti di produzione e disaster recovery per datastore VMFS e NFS tradizionali e per il test senza interruzioni delle repliche DR. Consente di automatizzare le attività di rilevamento, ripristino e protezione. Include un'appliance server SRA e adattatori SRA per server SRM Windows e appliance SRM.

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

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

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

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

In caso di disastro reale o persino di migrazione pianificata, SRM consente di inviare eventuali modifiche dell'ultimo minuto al dataset tramite un aggiornamento finale di SnapMirror (se si sceglie di farlo). Quindi, interrompe il mirror e monta il datastore sugli host DR. A questo punto, le VM possono essere alimentate automaticamente in qualsiasi ordine in base alla strategia prepianificata.

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

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

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

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

Best practice per l'implementazione

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

Layout e segmentazione SVM per SMT

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

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

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

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

Implementare gli strumenti e le considerazioni di ONTAP per i vVol

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

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

Best practice per la gestione dei sistemi ONTAP 9

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

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

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

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

Best practice operative

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

Datastore e protocolli

- Se possibile, utilizza sempre gli strumenti ONTAP per eseguire il provisioning di datastore e volumi. In questo modo si garantisce che volumi, percorsi di giunzione, LUN, igroups, policy di esportazione, e altre impostazioni sono configurate in modo compatibile.
- SRM supporta iSCSI, Fibre Channel e NFS versione 3 con ONTAP 9 quando si utilizza la replica basata su array tramite SRA. SRM non supporta la replica basata su array per NFS versione 4.1 con datastore tradizionali o vVols.
- Per confermare la connettività, verificare sempre che sia possibile montare e smontare un nuovo datastore di test sul sito DR dal cluster ONTAP di destinazione. Verificare ogni protocollo che si intende utilizzare per la connettività del datastore. Una Best practice consiste nell'utilizzare gli strumenti ONTAP per creare il datastore di test, poiché sta eseguendo tutta l'automazione del datastore come indicato da SRM.
- I protocolli SAN devono essere omogenei per ciascun sito. È possibile combinare NFS e SAN, ma i protocolli SAN non devono essere combinati all'interno di un sito. Ad esempio, è possibile utilizzare FCP nel sito A e iSCSI nel sito B. Non utilizzare sia FCP che iSCSI nel sito A. Il motivo è che l'SRA non crea gruppi igroup misti nel sito di ripristino e l'SRM non filtra l'elenco di iniziatori fornito all'SRA.
- Le guide precedenti hanno consigliato la creazione di una LIF in una località dati. Vale a dire, montare sempre un datastore utilizzando una LIF situata sul nodo che fisicamente possiede il volume. Questo non è più un requisito nelle versioni moderne di ONTAP 9. Quando possibile e se specifiche credenziali di ambito del cluster, i tool ONTAP continueranno a scegliere di bilanciare il carico tra le LIF locali dei dati, ma

non è un requisito di high Availability o performance.

- ONTAP 9 può essere configurato in modo da rimuovere automaticamente le istantanee per preservare l'uptime in caso di esaurimento dello spazio quando il dimensionamento automatico non è in grado di fornire una capacità di emergenza sufficiente. L'impostazione predefinita di questa funzionalità non elimina automaticamente le snapshot create da SnapMirror. Se le snapshot SnapMirror vengono eliminate, il servizio SRA di NetApp non può invertire e risincronizzare la replica per il volume interessato. Per impedire a ONTAP di eliminare snapshot di SnapMirror, configurare la funzionalità di eliminazione automatica Snapshot in modo da provare.

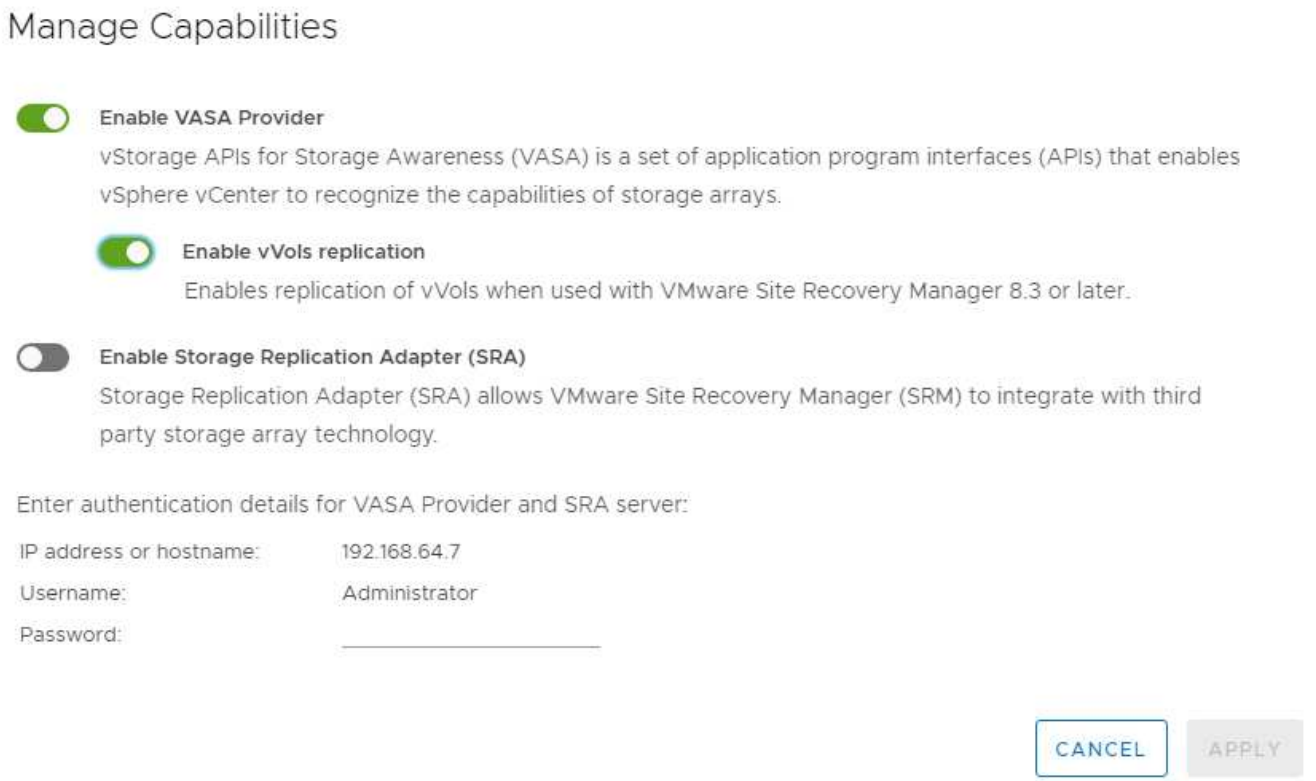
```
snap autodelete modify -volume -commitment try
```

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

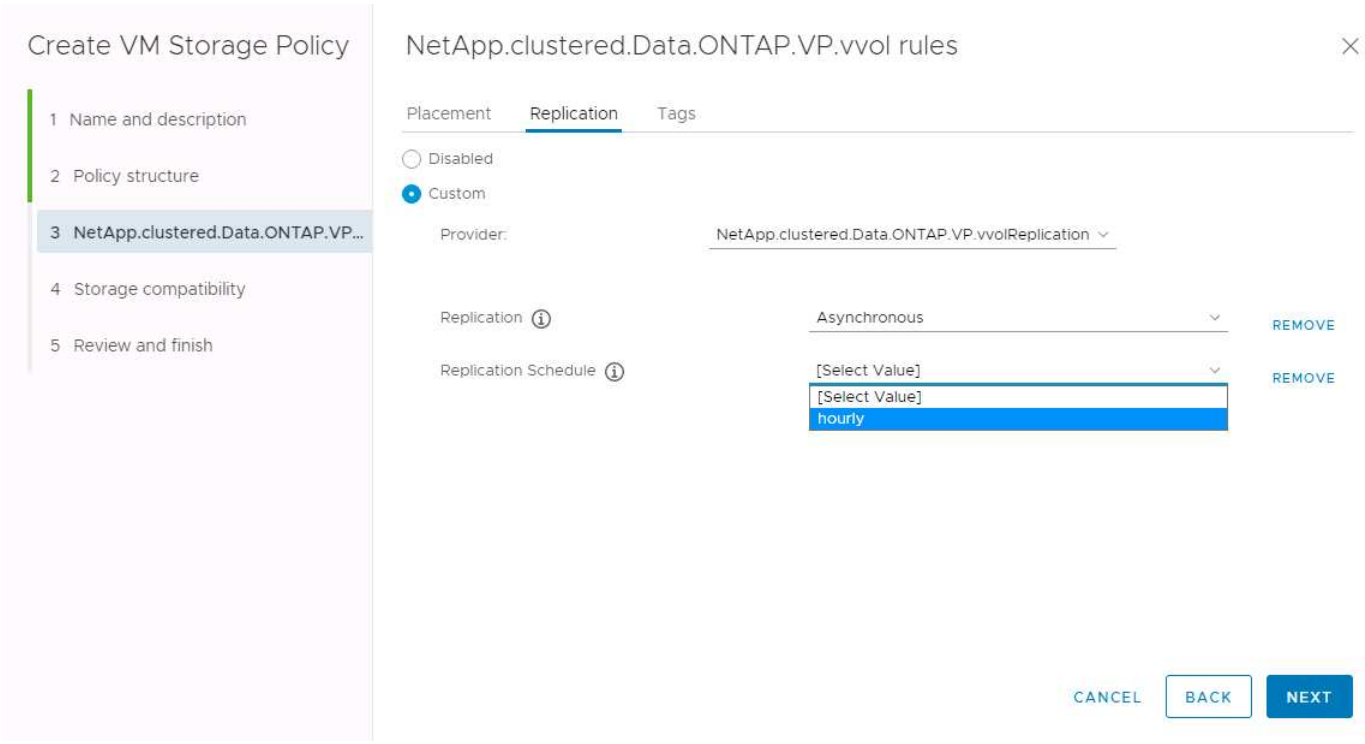
Gestione basata su criteri storage (SPBM, Storage Policy Based Management) e vVol

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

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

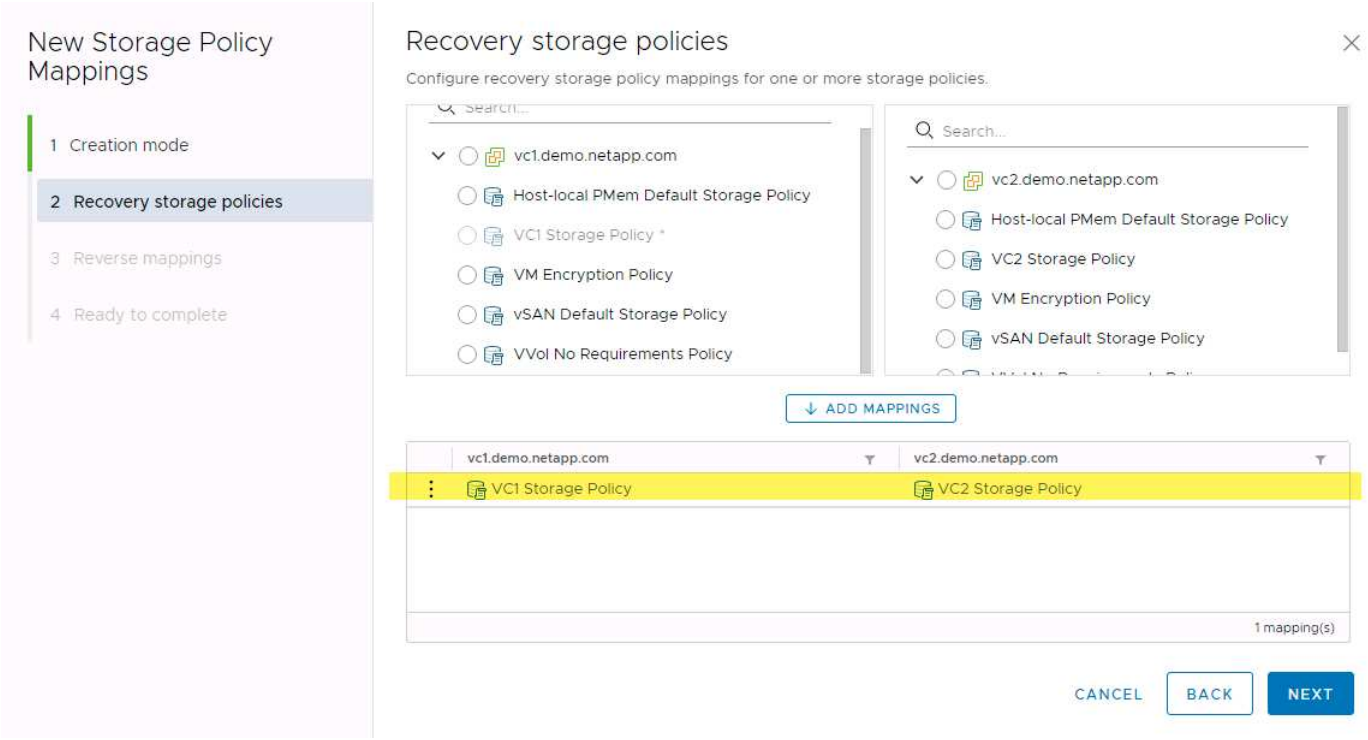


La seguente schermata fornisce un esempio di pianificazioni SnapMirror visualizzate nella procedura guidata Crea policy di storage VM.



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

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



Creare volumi replicati per gli archivi dati vVols

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

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

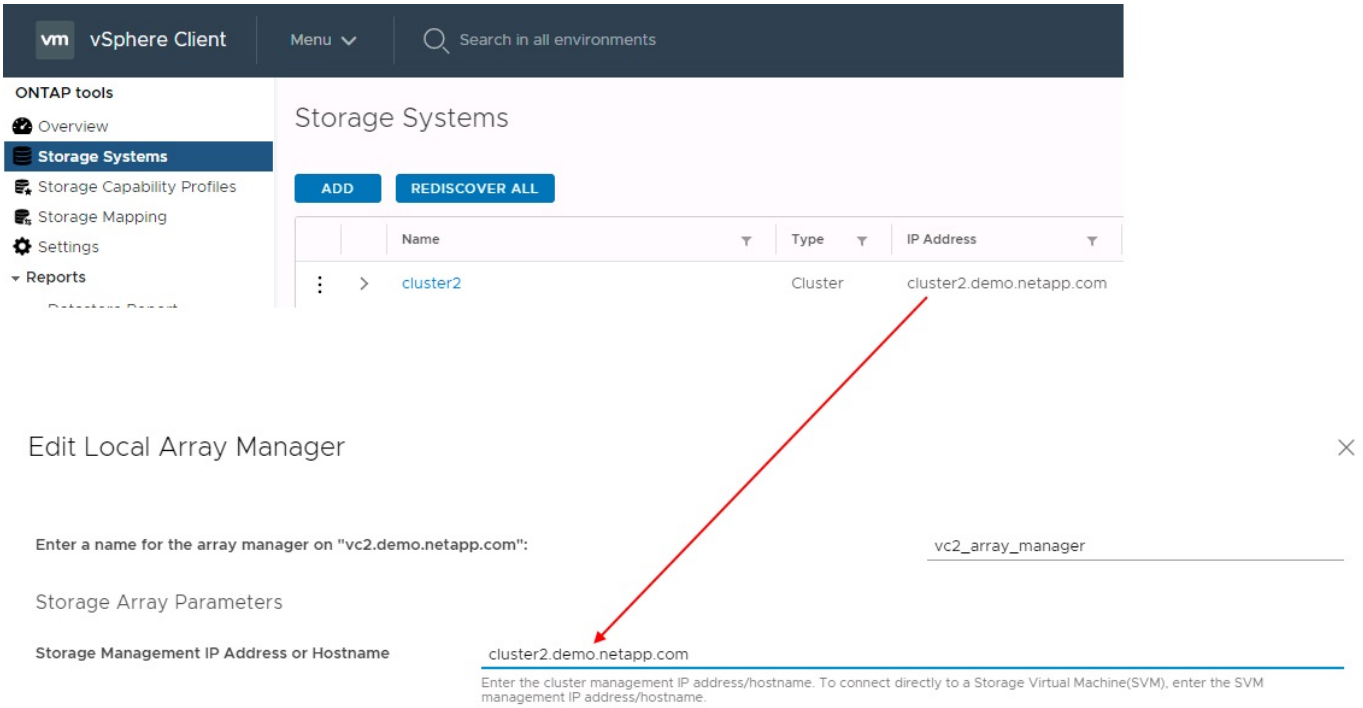
Si consiglia di prestare attenzione quando si tratta di vVol e SRM. Non mischiare mai macchine virtuali protette e non protette nello stesso datastore vVols. Il motivo è che quando si utilizza SRM per eseguire il failover sul sito DR, solo le macchine virtuali che fanno parte del gruppo di protezione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

preziosi.

Informazioni sulle coppie di array

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

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



Informazioni sui gruppi di replica

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

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

non prende in considerazione la deduplica degli aggregati.

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

A proposito dei gruppi di protezione

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

Sui piani di recovery

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

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

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

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

Test del failover

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

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

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

rete di test creata può essere selezionata come rete privata a cui connettere le macchine virtuali durante il test.

Una volta convalidato il test e non più necessario, eseguire un'operazione di pulizia. L'esecuzione della pulizia riporta le macchine virtuali protette al loro stato iniziale e ripristina il piano di ripristino allo stato Pronta.

Considerazioni sul failover

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

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

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

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

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

Proteggere di nuovo

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

Failback

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

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

Protezione del sito originale

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

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

Topologie di replica

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

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

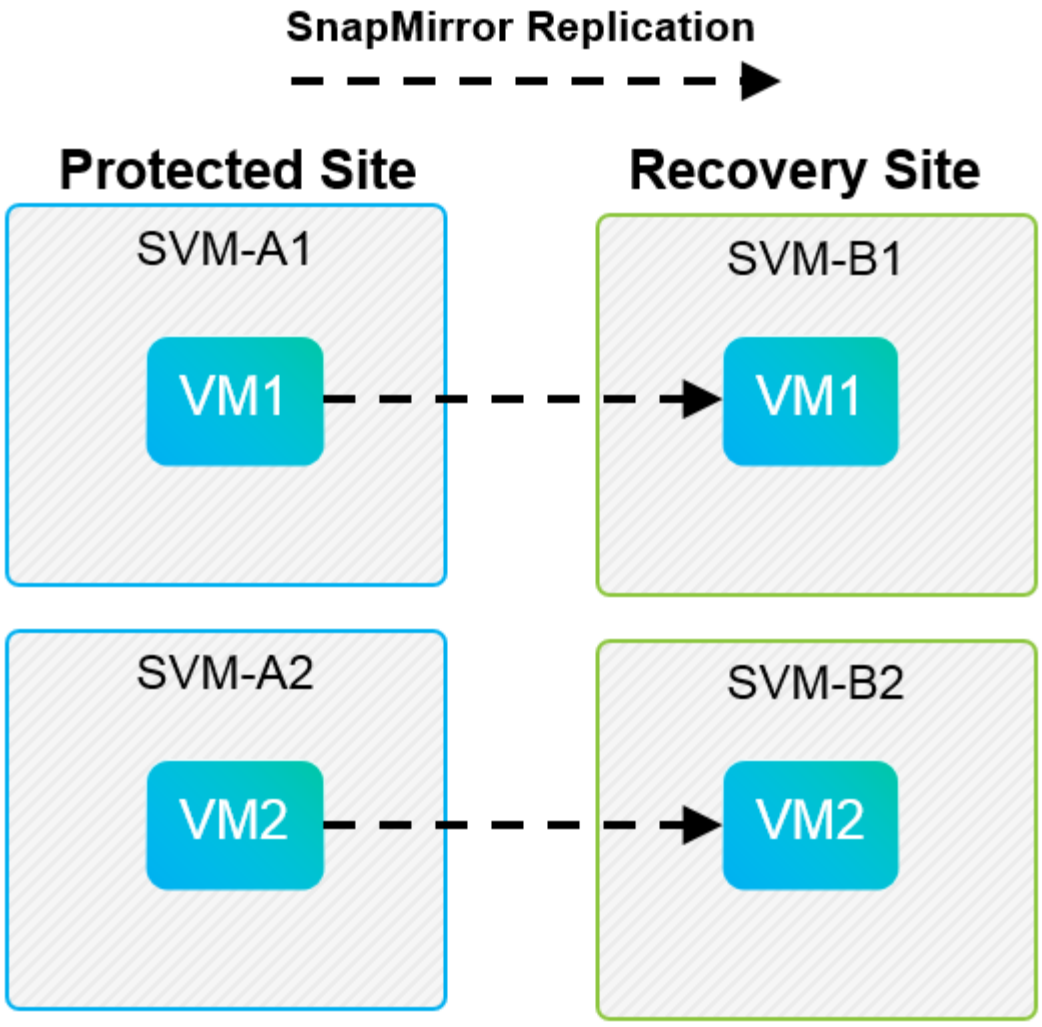
Una singola macchina virtuale non è in grado di gestire i dati (VMDK) o RDM) su più array SRM per i seguenti motivi:

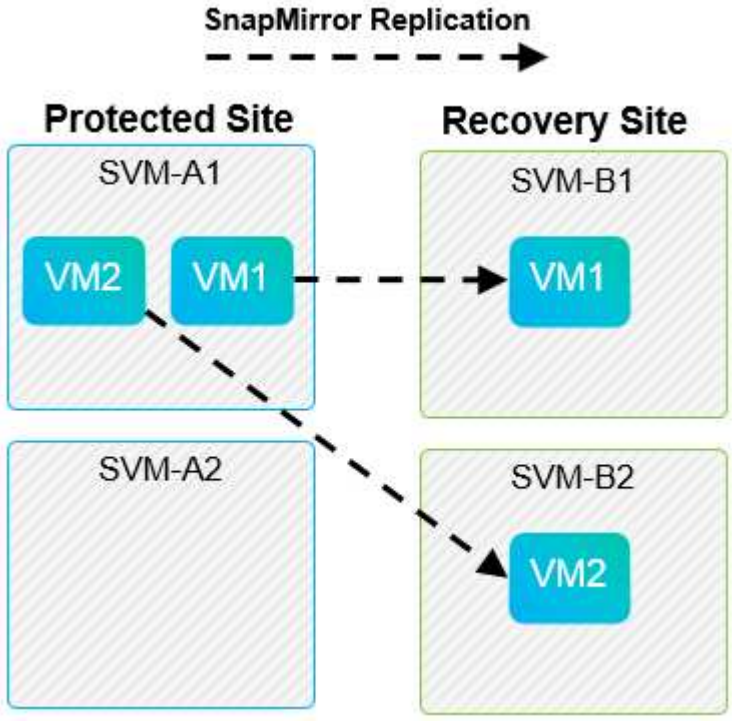
- SRM vede solo la SVM, non un singolo controller fisico.
- Una SVM può controllare LUN e volumi che si estendono su più nodi in un cluster.

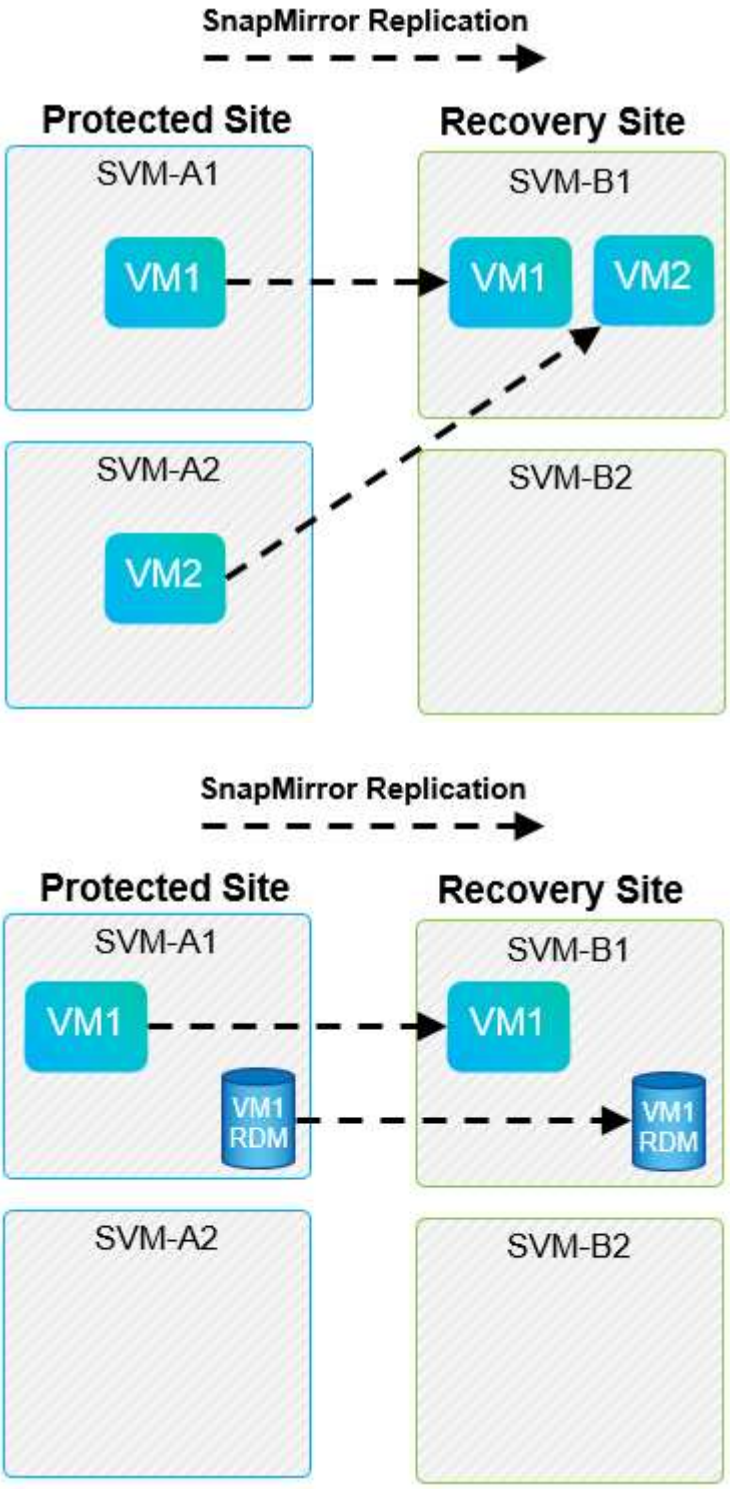
Best practice
Per determinare la supportabilità, tenere presente questa regola: Per proteggere una macchina virtuale utilizzando SRM e NetApp SRA, tutte le parti della macchina virtuale devono esistere su un solo SVM. Questa regola si applica sia al sito protetto che al sito di ripristino.

Layout SnapMirror supportati

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

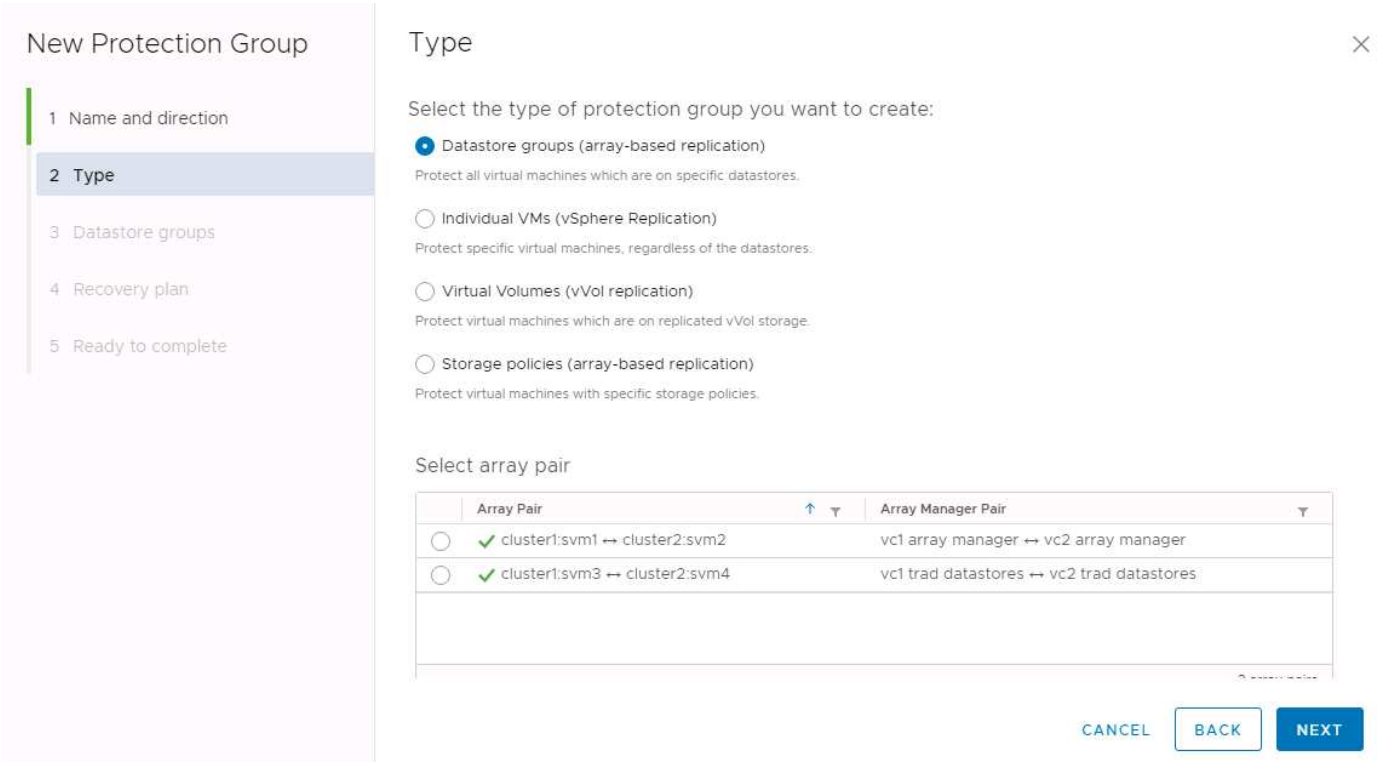

SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2


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



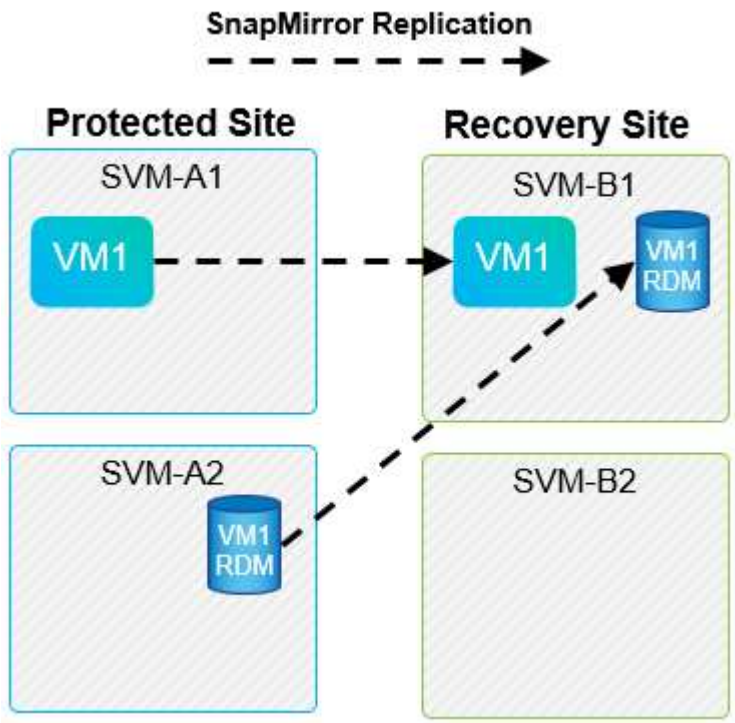
Layout di Array Manager supportati

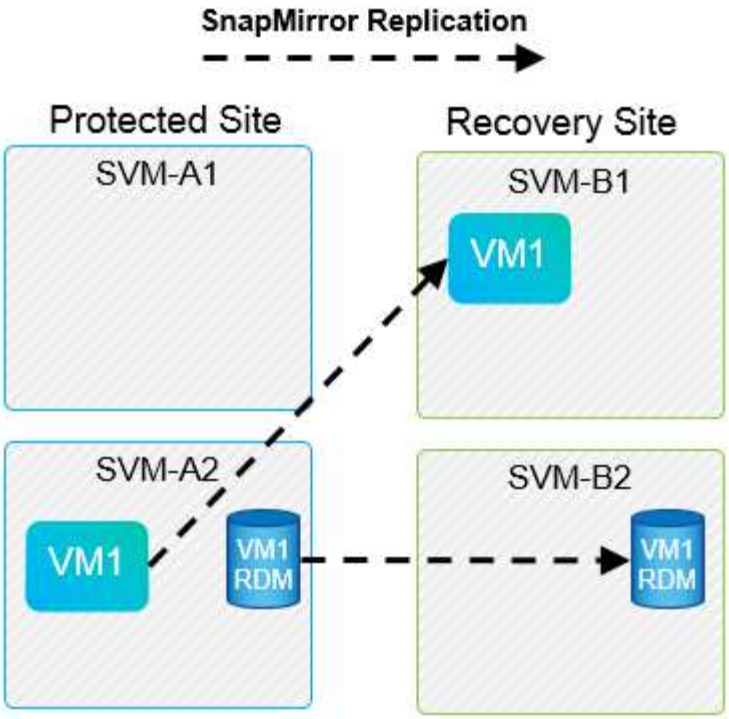
Quando si utilizza la replica basata su array (ABR) in SRM, i gruppi di protezione vengono isolati in una singola coppia di array, come illustrato nella seguente schermata. In questo scenario, `SVM1` e. `SVM2` sono in coppia con `SVM3` e. `SVM4` presso il sito di recovery. Tuttavia, è possibile selezionare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



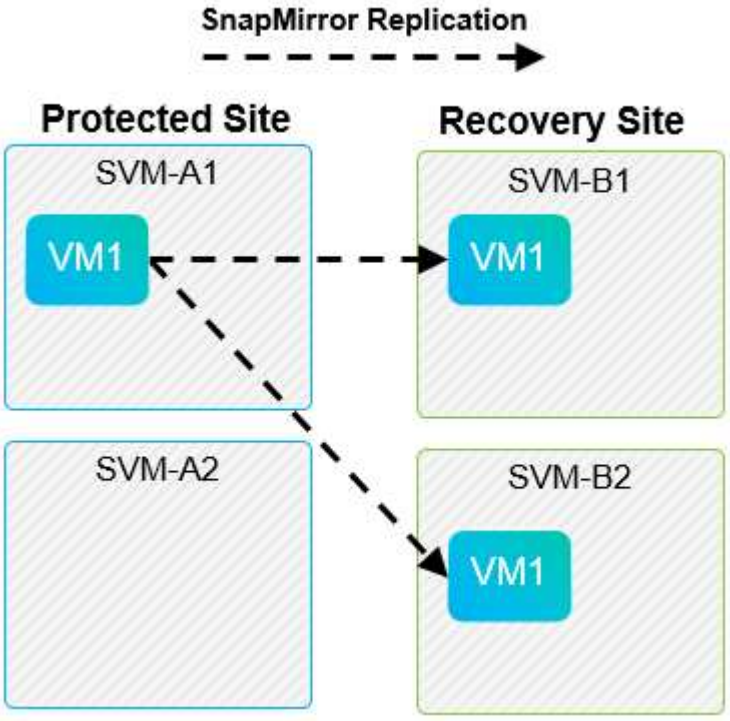
Layout non supportati

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





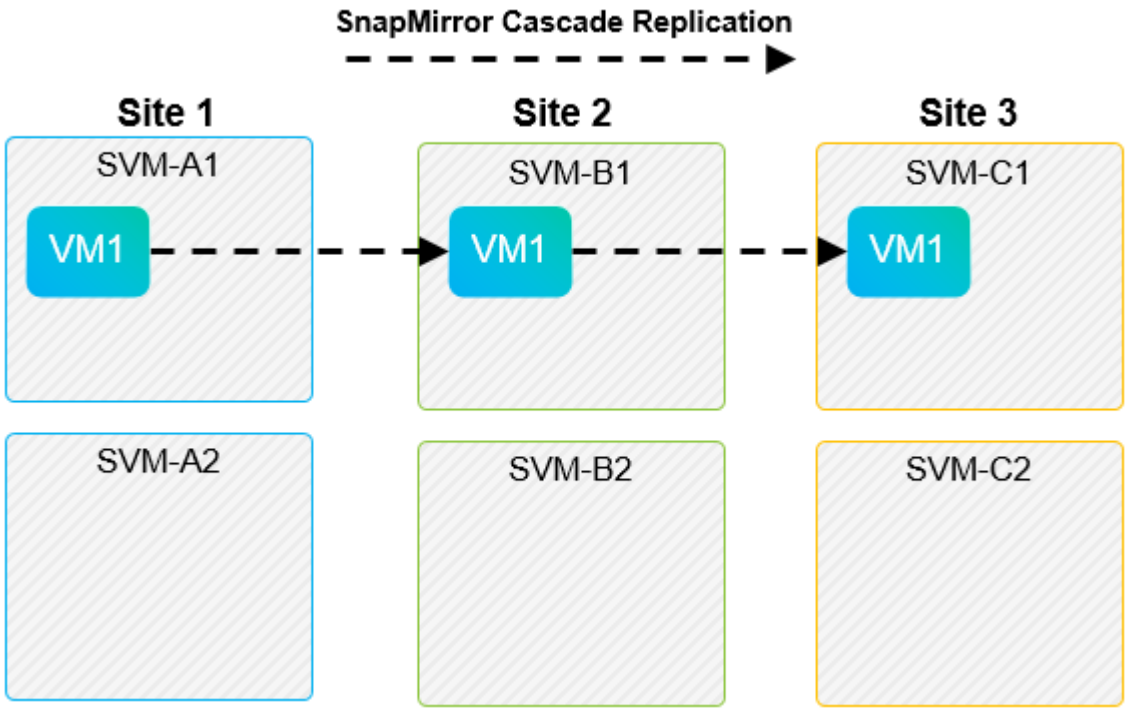
Qualsiasi relazione di replica in cui un singolo volume NetApp viene replicato da una SVM di origine a più destinazioni nella stessa SVM o in SVM differenti viene definita fan-out di SnapMirror. Fan-out non supportato con SRM. Nell'esempio illustrato nella figura seguente, `VM1` Impossibile configurare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



Cascata di SnapMirror

SRM non supporta la sovrapposizione delle relazioni SnapMirror, in cui un volume di origine viene replicato in un volume di destinazione e tale volume di destinazione viene replicato anche con SnapMirror in un altro

volume di destinazione. Nello scenario illustrato nella figura seguente, SRM non può essere utilizzato per il failover tra siti.



SnapMirror e SnapVault

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

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

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

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

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

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

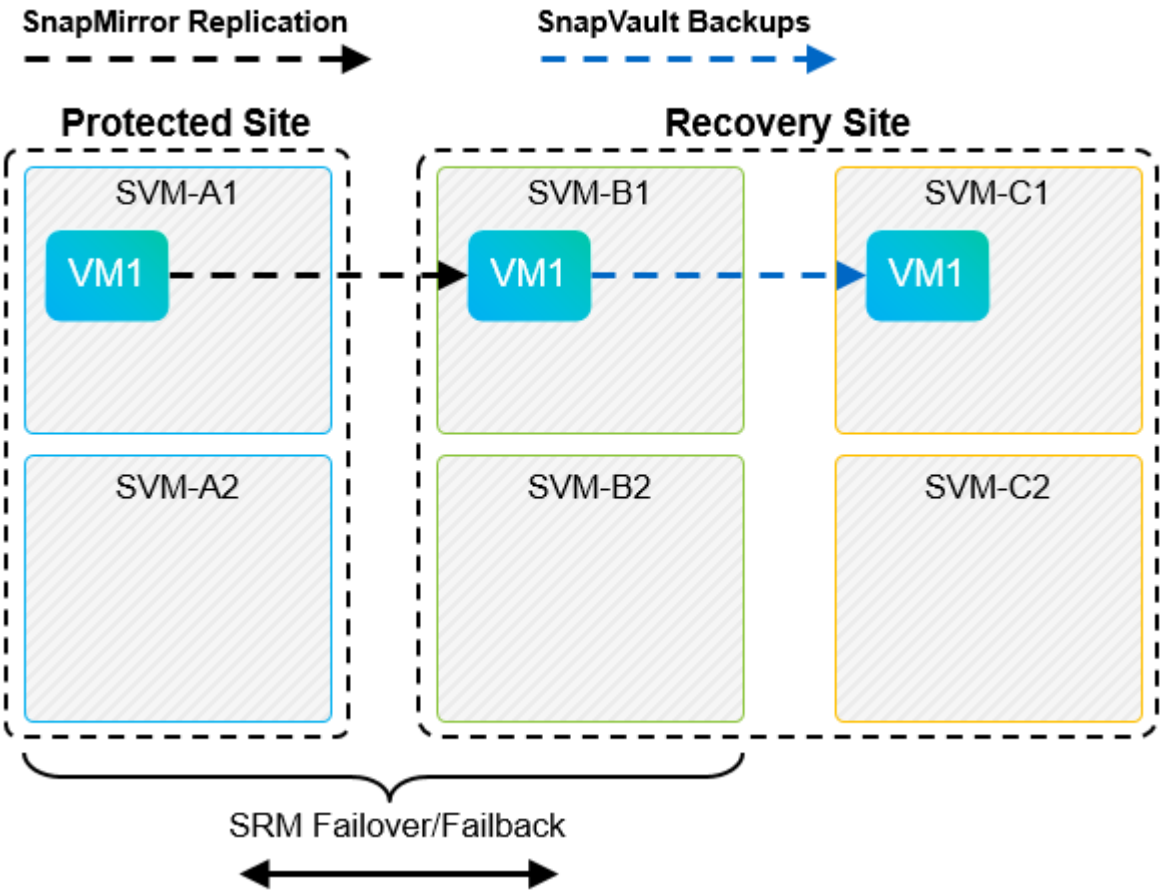
verifica il failover SRM o l'inversione della replica.

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

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

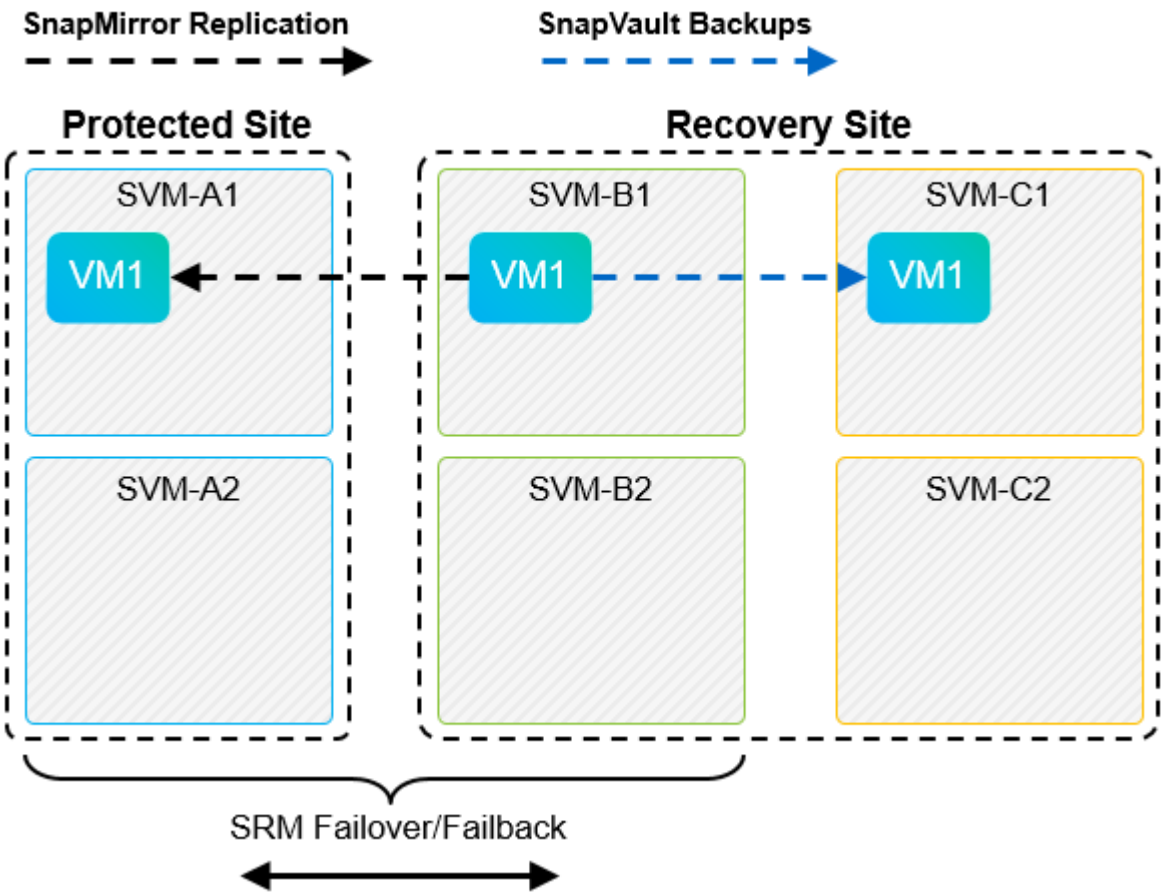
In un ambiente VMware, ogni datastore dispone di un UUID (Universal Unique Identifier) e ogni VM dispone di un MOID (Managed Object ID) univoco. Questi ID non vengono gestiti da SRM durante il failover o il failback. Poiché gli UUID degli archivi di dati e i MOID delle macchine virtuali non vengono mantenuti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

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



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

SnapMirror SnapVault.



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

Utilizzo di Qtree in ambienti Site Recovery Manager

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

Ambienti misti FC e iSCSI

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

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

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

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

Risoluzione dei problemi di SRM quando si utilizza la replica vVol

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

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

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

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

Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i

seguenti documenti e/o siti Web:

- TR-4597: VMware vSphere per ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400: Volumi virtuali VMware vSphere con ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- Guida alle Best practice per la configurazione di SnapMirror TR-4015 per ONTAP 9
  https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P
- Creatore utente RBAC per ONTAP
  "https://mysupport.netapp.com/site/tools/tool-eula/rbac"
- Strumenti ONTAP per le risorse VMware vSphere
  "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- Documentazione di VMware Site Recovery Manager
  "https://docs.vmware.com/en/Site-Recovery-Manager/index.html"

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

Informazioni sul copyright

Informazioni sul marchio commerciale