Proteggere utilizzando la protezione SRA

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

Sommario

Proteggere utilizzando la protezione SRA

Configurare SRA per proteggere gli archivi dati

I tool ONTAP per VMware vSphere offrono la possibilità di abilitare la funzionalità SRA per la configurazione del disaster recovery.

Prima di iniziare

- È necessario aver configurato l'istanza di vCenter Server e l'host ESXi configurato.
- Devi aver implementato tool ONTAP per VMware vSphere.
- Il `.tar.gz` file dell'adattatore SRA dovrebbe essere stato scaricato dal "Sito di supporto NetApp" .
- Prima di eseguire i flussi di lavoro SRA, è necessario disporre delle stesse pianificazioni SnapMirror personalizzate sui cluster ONTAP di origine e di destinazione.
- "Abilita i tool ONTAP per i servizi VMware vSphere" per abilitare la funzionalità SRA.

Fasi

1. Accedere all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando l'URL: `https://:<srm_ip>:5480`, Quindi accedere a Storage Replication Adapter nell'interfaccia di gestione dell'appliance VMware Live Site Recovery.
2. Selezionare **Nuova scheda**.
3. Caricare il programma di installazione *.tar.gz* per il plug-in SRA in VMware Live Site Recovery.
4. Eseguire nuovamente la scansione delle schede di rete per verificare che i dettagli siano aggiornati nella pagina VMware Live Site Recovery Storage Replication Adapters (schede di replica storage di VMware Live Site Recovery).

> Dopo un failover, azioni quali espansione, montaggio ed eliminazione potrebbero non essere disponibili per i datastore. Eseguire la scoperta del datastore per aggiornare e visualizzare le azioni appropriate del menu contestuale.

> Dopo ogni operazione di riprotezione, è necessario eseguire l'individuazione dello storage su entrambi i siti.

In una nuova configurazione con protezione SRA, eseguire sempre un failover di prova. Saltare il failover di prova potrebbe causare il fallimento dell'operazione di riprotezione.

In una configurazione fan-out, dopo un failover SnapMirror Active Sync in cui la sorgente SnapMirror cambia nel sito B per Automated Failover Duplex e Asynchronous SnapMirror, eseguire un failover di prova tra i siti B e C. Saltare questo passaggio potrebbe comportare il fallimento dell'operazione di riprotezione.

Informazioni correlate

"Configurare il disaster recovery per i datastore NFS utilizzando VMware Site Recovery Manager"

Configurare SRA per gli ambienti SAN e NAS

È necessario configurare i sistemi di storage prima di eseguire Storage Replication Adapter (SRA) per VMware Live Site Recovery.

Configurare SRA per gli ambienti SAN

Prima di iniziare

Nel sito protetto e nel sito di ripristino devono essere installati i seguenti programmi:

- VMware Live Site Recovery: il sito VMware fornisce la documentazione di installazione per VMware Live Site Recovery.

  "Informazioni su VMware Live Site Recovery"

- SRA: installare l'adattatore su VMware Live Site Recovery.

Fasi

1. Verificare che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario sul sito protetto.
2. Verificare che i LUN si trovino in igroups che dispongono di `ostype` Opzione impostata su *VMware* sul sistema di storage primario.
3. Verificare che gli host ESXi nel sito di ripristino dispongano di una connettività iSCSI e Fibre Channel appropriata alla macchina virtuale di archiviazione (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario, mentre gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

   Per farlo, verificare che gli host ESXi abbiano LUN locali connessi alla SVM o al `iscsi show initiators` Sulle SVM. Controllare l'accesso LUN per i LUN mappati nell'host ESXi per verificare la connettività iSCSI.

Configurare SRA per gli ambienti NAS

Prima di iniziare

Nel sito protetto e nel sito di ripristino devono essere installati i seguenti programmi:

- VMware Live Site Recovery: la documentazione sull'installazione di VMware Live Site Recovery è disponibile sul sito VMware - "Informazioni su VMware Live Site Recovery"
- SRA: installare l'adattatore su VMware Live Site Recovery e sul server SRA.

Fasi

1. Verificare che gli archivi dati del sito protetto contengano macchine virtuali registrate con vCenter Server.
2. Verificare che gli host ESXi nel sito protetto abbiano montato i volumi di esportazione NFS dalla macchina virtuale di storage (SVM).
3. Verificare che nel campo **Indirizzi NFS** siano specificati indirizzi validi, come l'indirizzo IP o il nome di dominio completo (FQDN) su cui sono presenti le esportazioni NFS, quando si utilizza la procedura guidata di Array Manager per aggiungere array a VMware Live Site Recovery. Non utilizzare il nome host NFS nel campo **Indirizzi NFS**.
4. Utilizzare `ping` Su ciascun host ESXi nel sito di ripristino per verificare che l'host disponga di una porta VMkernel in grado di accedere agli indirizzi IP utilizzati per le esportazioni NFS dalla SVM.

Configurare SRA per ambienti ad alta scalabilità

È necessario configurare gli intervalli di timeout dello storage in base alle impostazioni

consigliate per Storage Replication Adapter (SRA) in modo da garantire prestazioni ottimali in ambienti altamente scalabili.

Impostazioni del provider di storage

È necessario impostare i seguenti valori di timeout su VMware Live Site Recovery per l'ambiente scalato:

Impostazioni avanzate	Valori di timeout
`StorageProvider.resignatureTimeout`	Aumentare il valore dell'impostazione da 900 secondi a 12000 secondi.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Impostare un valore alto (ad esempio: 99999)

Attivare anche il `StorageProvider.autoResignatureMode` opzione.

Per ulteriori informazioni sulla modifica delle impostazioni del provider di archiviazione, fare riferimento alla "Modificare le impostazioni del provider di storage" .

Impostazioni di storage

Quando si preme un timeout, aumentare i valori di `storage.commandTimeout` e. `storage.maxConcurrentCommandCnt` ad un valore più alto.

> L'intervallo di timeout specificato è il valore massimo. Non è necessario attendere che venga raggiunto il timeout massimo. La maggior parte dei comandi termina entro l'intervallo di timeout massimo impostato.

Per modificare le impostazioni dei provider SAN, consultare la sezione "Modificare le impostazioni di archiviazione".

Configurare SRA sull'appliance VMware Live Site Recovery

Dopo aver distribuito l'appliance VMware Live Site Recovery, configurare Storage Replication Adapter (SRA) per abilitare la gestione del disaster recovery.

La configurazione di SRA sull'appliance VMware Live Site Recovery salva le credenziali ONTAP tools for VMware vSphere all'interno dell'appliance, consentendo la comunicazione tra VMware Live Site Recovery e SRA.

Prima di iniziare

- Scarica il file *.tar.gz* dal "Sito di supporto NetApp" .
- Abilitare i servizi SRA in ONTAP Tools Manager. Per ulteriori informazioni, consulta "Abilita i servizi" sezione.

- Aggiungere vCenter Server agli strumenti ONTATP per l'appliance VMware vSphere. Per ulteriori informazioni, consulta "Aggiungi server vCenter" sezione.
- Aggiungere backend di storage agli ONTAP tools for VMware vSphere. Per ulteriori informazioni, consulta "Aggiungere backend di archiviazione" sezione.

Fasi

1. Nella schermata dell'appliance VMware Live Site Recovery, selezionare **Storage Replication Adapter** > **New Adapter**.
2. Caricare il file *.tar.gz* su VMware Live Site Recovery.
3. Accedere al dispositivo VMware Live Site Recovery utilizzando un account amministratore tramite un client SSH come PuTTY.
4. Passare all'utente root utilizzando il comando: `su root`
5. Esegui il comando `cd /var/log/vmware/srm` per andare alla directory del registro.
6. Nella posizione del registro, immettere il comando per ottenere l'ID Docker utilizzato da SRA: `docker ps -l`
7. Per accedere all'ID contenitore, immettere il comando: `docker exec -it -u srm <container id> sh`
8. Configurare VMware Live Site Recovery con gli ONTAP tools for VMware vSphere utilizzando il comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Fornire la password tra virgolette singole in modo che lo script Perl tratti i caratteri speciali come parte della password e non come delimitatori.
   - È possibile impostare il nome utente e la password dell'applicazione (VASA Provider/SRA) in ONTAP Tools Manager quando si abilitano questi servizi per la prima volta. Utilizzare queste credenziali per registrare SRA con VMware Live Site Recovery.
   - Per individuare il GUID di vCenter, accedere alla pagina vCenter Server in ONTAP Tools Manager dopo aver aggiunto l'istanza di vCenter. Fare riferimento a"Aggiungi server vCenter" sezione.
9. Eseguire nuovamente la scansione degli adattatori per confermare che i dettagli aggiornati siano visualizzati nella pagina Adattatori VMware Live Site Recovery Storage Replication.

Risultati Viene visualizzato un messaggio di conferma che indica che le credenziali di archiviazione sono state salvate. Ora puoi utilizzare SRA per comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali specificati.

Aggiornare le credenziali SRA

Affinché VMware Live Site Recovery comunichi con SRA, è necessario aggiornare le credenziali SRA sul server VMware Live Site Recovery se sono state modificate le credenziali.

Prima di iniziare

È necessario aver eseguito i passaggi descritti nell'argomento "Configurazione di SRA sull'appliance VMware Live Site Recovery".

Fasi

1. Eseguire i seguenti comandi per eliminare la cartella della macchina per il ripristino dei siti live di VMware

memorizzata nella cache degli strumenti ONTAP Password del nome utente:

a. `sudo su <enter root password>`
b. `docker ps`
c. `docker exec -it <container_id> sh`
d. `cd conf/`
e. `rm -rf *`

2. Eseguire il comando Perl per configurare SRA con le nuove credenziali:

a. `cd ..`
b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` È necessario disporre di un'unica citazione relativa al valore della password.

   Viene visualizzato un messaggio di conferma dell'avvenuta memorizzazione delle credenziali di storage. SRA può comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali forniti.

Configurare siti protetti e di ripristino

È necessario creare gruppi di protezione per proteggere un gruppo di macchine virtuali sul sito protetto.

Quando si aggiunge un nuovo datastore, è possibile includerlo nel gruppo di datastore esistente oppure aggiungere un nuovo datastore e creare un nuovo volume o gruppo di coerenza per la protezione. Dopo aver aggiunto un nuovo datastore a un gruppo di coerenza o volume protetto, aggiornare SnapMirror ed eseguire il discovery dello storage sia sul sito protetto che su quello di ripristino. È possibile eseguire il discovery manualmente o in base a una pianificazione per garantire che il nuovo datastore venga rilevato e protetto.

Associare siti protetti e di ripristino

È necessario associare i siti protetti e di ripristino creati utilizzando il client vSphere per consentire l'individuazione dei sistemi di storage mediante Storage Replication Adapter (SRA).

> Storage Replication Adapter (SRA) supporta il fan-out con una relazione di sincronizzazione di tipo Automated Failover Duplex e una relazione asincrona SnapMirror sul gruppo di coerenza. Tuttavia, la fan-out con due SnapMirror asincroni sul gruppo di coerenza o gli SnapMirror fan-out sul volume non sono supportati.

Prima di iniziare

- È necessario che VMware Live Site Recovery sia installato sui siti protetti e di ripristino.
- È necessario che SRA sia installato nei siti protetti e di ripristino.

Fasi

1. Nella home page di vSphere Client, fare doppio clic sull'icona **Site Recovery** e quindi selezionare **Siti**.
2. Selezionare **oggetti** > **azioni** > **abbina siti**.
3. Nella finestra di dialogo **Associa server di Site Recovery Manager**, immettere l'indirizzo del Platform Services Controller del sito protetto, quindi selezionare **Avanti**.

4. Nella sezione Select vCenter Server (Seleziona server vCenter), procedere come segue:
    a. Verificare che vCenter Server del sito protetto venga visualizzato come candidato corrispondente per l'associazione.
    b. Immettere le credenziali amministrative SSO, quindi selezionare **fine**.
5. Se richiesto, selezionare **Sì** per accettare i certificati di protezione.

Risultato

Nella finestra di dialogo **Oggetti** vengono visualizzati sia i siti protetti che quelli di ripristino.

Configurare i gruppi di protezione

Prima di iniziare

Assicurarsi che i siti di origine e di destinazione siano configurati per:

- È installata la stessa versione di VMware Live Site Recovery
- Macchine virtuali
- Siti di ripristino e protezione associati
- Gli archivi dati di origine e di destinazione devono essere montati sui rispettivi siti

Fasi

1. Accedi a vCenter Server e seleziona **Site Recovery** > **Gruppi di protezione**.
2. Nel riquadro **gruppi di protezione**, selezionare **nuovo**.
3. Specificare un nome e una descrizione per il gruppo protezione, direzione e selezionare **Avanti**.
4. Nel campo **Tipo**, seleziona l'opzione **Tipo…** come gruppi di datastore (replica basata su array) per datastore NFS e VMFS. Il dominio di errore è costituito esclusivamente da SVM con replica abilitata. Vengono visualizzate le SVM che hanno implementato solo il peering e non presentano problemi.
5. Nella scheda gruppi di replica, selezionare la coppia di array abilitata o i gruppi di replica che hanno configurato la macchina virtuale, quindi selezionare **Avanti**.

    Tutte le macchine virtuali presenti nel gruppo di replica vengono aggiunte al gruppo di protezione.
6. È possibile selezionare il piano di ripristino esistente oppure crearne uno nuovo selezionando **Aggiungi al nuovo piano di ripristino.**
7. Nella scheda Pronto per il completamento, esaminare i dettagli del gruppo di protezione creato, quindi selezionare **fine**.

Configurare le risorse protette e del sito di ripristino

Configurare le mappature di rete

È necessario configurare i mapping delle risorse, ad esempio reti di macchine virtuali, host ESXi e cartelle su entrambi i siti, in modo da consentire la mappatura di ciascuna risorsa dal sito protetto alla risorsa appropriata nel sito di ripristino.

È necessario completare le seguenti configurazioni delle risorse:

- Mappature di rete

- Mappature delle cartelle
- Mappature delle risorse
- Datastore segnaposto

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **mappature di rete** > **nuovo** nella scheda Gestisci per creare una nuova mappatura di rete.
4. Nella procedura guidata Crea mappatura di rete, effettuare le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per reti con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Network Mappings (Mapping di rete) visualizza le risorse protette del sito e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare le mappature delle cartelle

È necessario mappare le cartelle sul sito protetto e sul sito di ripristino per consentire la comunicazione tra di esse.

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **Mapping cartelle** > **icona cartella** nella scheda Gestisci per creare una nuova mappatura cartelle.
4. Nella procedura guidata Create Folder Mapping (Crea mappatura cartelle), eseguire le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per cartelle con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Folder Mappings (Mapping cartelle) visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare le mappature delle risorse

È necessario mappare le risorse sul sito protetto e sul sito di ripristino in modo che le macchine virtuali siano configurate per eseguire il failover in un gruppo di host o nell'altro.

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.

> In VMware Live Site Recovery, le risorse possono essere pool di risorse, host ESXi o cluster vSphere.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery** > **Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **mappature risorse** > **nuovo** nella scheda Gestisci per creare una nuova mappatura delle risorse.
4. Nella procedura guidata Create Resource Mapping (Crea mappatura risorse), eseguire le seguenti operazioni:
   a. Selezionare **prepara automaticamente mappature per risorsa con nomi corrispondenti** e selezionare **Avanti**.
   b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
   c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
   d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Resource Mappings (Mapping delle risorse) visualizza le risorse protette del sito e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare gli archivi dati segnaposto

Configurare un datastore segnaposto per riservare spazio nell'inventario vCenter nel sito di ripristino per le macchine virtuali (VM) protette. Gli archivi dati segnaposto richiedono una capacità minima, perché le VM segnaposto sono piccole e in genere utilizzano solo poche centinaia di kilobyte.

Prima di iniziare

- Assicurarsi che i siti protetti e di ripristino siano connessi.
- Verificare che le mappature delle risorse siano state configurate.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery** > **Sites**.

2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **segnaposto datastore** > **nuovo** nella scheda Gestisci per creare un nuovo archivio dati segnaposto.
4. Selezionare l'archivio dati appropriato e selezionare **OK**.

> Gli archivi dati segnaposto possono risiedere su storage locali o remoti, ma non richiedono replica.

5. Ripetere i passaggi da 3 a 5 per configurare un archivio dati segnaposto per il sito di ripristino.

Configurare SRA utilizzando Array Manager

È possibile configurare Storage Replication Adapter (SRA) utilizzando la procedura guidata Array Manager di VMware Live Site Recovery per abilitare le interazioni tra VMware Live Site Recovery e le Storage Virtual Machine (SVM).

Prima di iniziare

- È necessario aver abbinato i siti protetti e i siti di ripristino in VMware Live Site Recovery.
- Prima di configurare il gestore array, è necessario aver configurato lo spazio di archiviazione integrato.
- Dovresti aver configurato e replicato le relazioni SnapMirror tra i siti protetti e i siti di recovery.
- Dovresti aver abilitato le LIF di gestione SVM per l'abilitazione della multi-tenancy.

SRA supporta la gestione a livello di cluster e la gestione a livello di SVM. Aggiungendo lo storage a livello di cluster è possibile rilevare ed eseguire operazioni su tutte le SVM del cluster. Se si aggiunge storage a livello di SVM, è possibile gestire solo la SVM specifica.

Fasi

1. In VMware Live Site Recovery, selezionare **Array Managers** > **Add Array Manager**.
2. Immettere le seguenti informazioni per descrivere l'array in VMware Live Site Recovery:
    a. Immettere un nome per identificare il gestore array nel campo **Display Name**.
    b. Nel campo **tipo SRA**, selezionare **scheda di replica storage NetApp per ONTAP**.
    c. Inserire le informazioni per la connessione al cluster o alla SVM:
        - Se ci si connette a un cluster, è necessario immettere il LIF di gestione del cluster.
        - Se ci si connette direttamente a una SVM, è necessario immettere l'indirizzo IP del LIF di gestione della SVM.

> Durante la configurazione dell'array manager occorre utilizzare la stessa connessione (indirizzo IP) per il sistema storage utilizzato per integrare il sistema storage nei tool ONTAP per VMware vSphere. Ad esempio, se la configurazione del gestore degli array ha un ambito SVM, occorre aggiungere lo storage nei tool ONTAP per VMware vSphere a livello di SVM.

    d. Se ci si connette a un cluster, specificare il nome SVM nel campo **Nome SVM** oppure lasciarlo vuoto per gestire tutte le SVM nel cluster.
    e. Inserire i volumi da rilevare nel campo **Volume include list** (elenco di inclusione del volume).

È possibile inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera rilevare il volume src_vol1 che si trova in una relazione SnapMirror con il volume dst_vol1, è necessario specificare src_vol1 nel campo del sito protetto e dst_vol1 nel campo del sito di ripristino.

f. **(opzionale)** inserire i volumi da escludere dal rilevamento nel campo **elenco esclusioni volume**.

È possibile inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera escludere il volume *src_vol1* che si trova in una relazione SnapMirror con il volume *dst_vol1*, è necessario specificare *src_vol1* nel campo del sito protetto e *dst_vol1* nel campo del sito di ripristino.

3. Selezionare **Avanti**.
4. Verificare che l'array sia rilevato e visualizzato nella parte inferiore della finestra Add Array Manager (Aggiungi array) e selezionare **Finish** (fine).

È possibile seguire gli stessi passaggi per il sito di ripristino utilizzando gli indirizzi IP e le credenziali di gestione SVM appropriati. Nella schermata Enable Array Pairs (Abilita coppie di array) della procedura guidata Add Array Manager (Aggiungi gestore array), verificare che sia selezionata la coppia di array corretta e che sia visualizzata come pronta per essere abilitata.

Verificare i sistemi storage replicati

È necessario verificare che il sito protetto e il sito di ripristino siano associati correttamente dopo la configurazione dell'adattatore di replica dello storage (SRA). Il sistema storage replicato deve essere raggiungibile sia dal sito protetto che dal sito di recovery.

Prima di iniziare

- È necessario aver configurato il sistema di archiviazione.
- È necessario abbinare il sito protetto e il sito di ripristino utilizzando il gestore dell'array VMware Live Site Recovery.
- Prima di eseguire l'operazione di test failover e di failover per SRA, è necessario aver attivato la licenza FlexClone e la licenza SnapMirror.
- È necessario disporre degli stessi criteri e pianificazioni SnapMirror sui siti di origine e destinazione.

Fasi

1. Accedere al server vCenter.
2. Vai a **Site Recovery** > **Array Based Replication**.
3. Selezionare la coppia di array richiesta e verificare i dettagli corrispondenti.

I sistemi di archiviazione devono essere rilevati nel sito protetto e nel sito di ripristino con lo stato "`abilitato'".

Protezione fan-out

In uno scenario di protezione fan-out, il gruppo di coerenza è doppiamente protetto con relazione sincrona sul primo cluster ONTAP di destinazione e con relazione asincrona sul secondo cluster ONTAP di destinazione. I flussi di lavoro di creazione, modifica ed eliminazione della protezione ActiveSync SnapMirror mantengono la protezione sincrona. I flussi di lavoro di failover e riprotezione dell'appliance VMware Live Site Recovery mantengono la protezione asincrona.

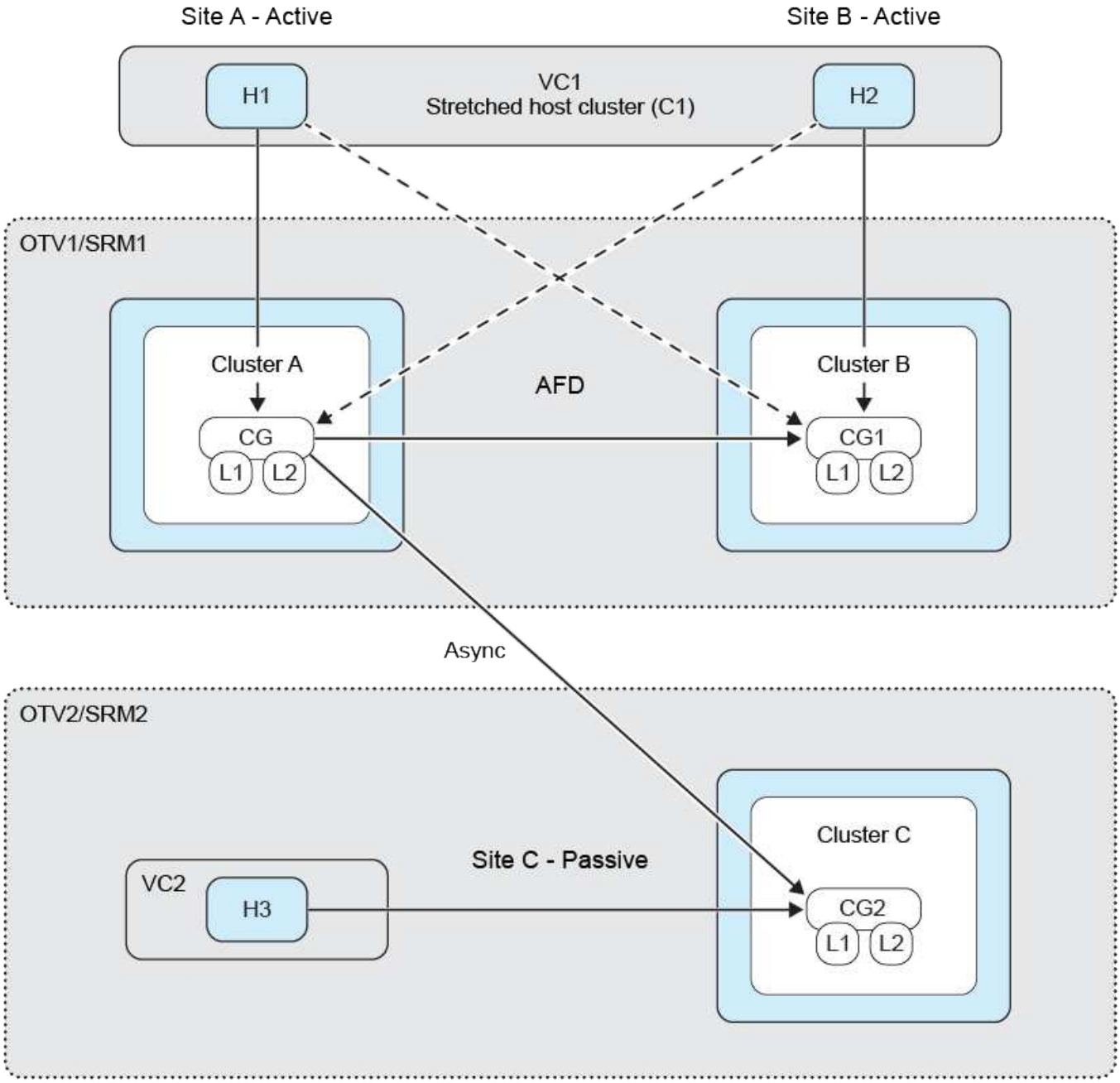
Il fan-out non è supportato per l'utente SVM.

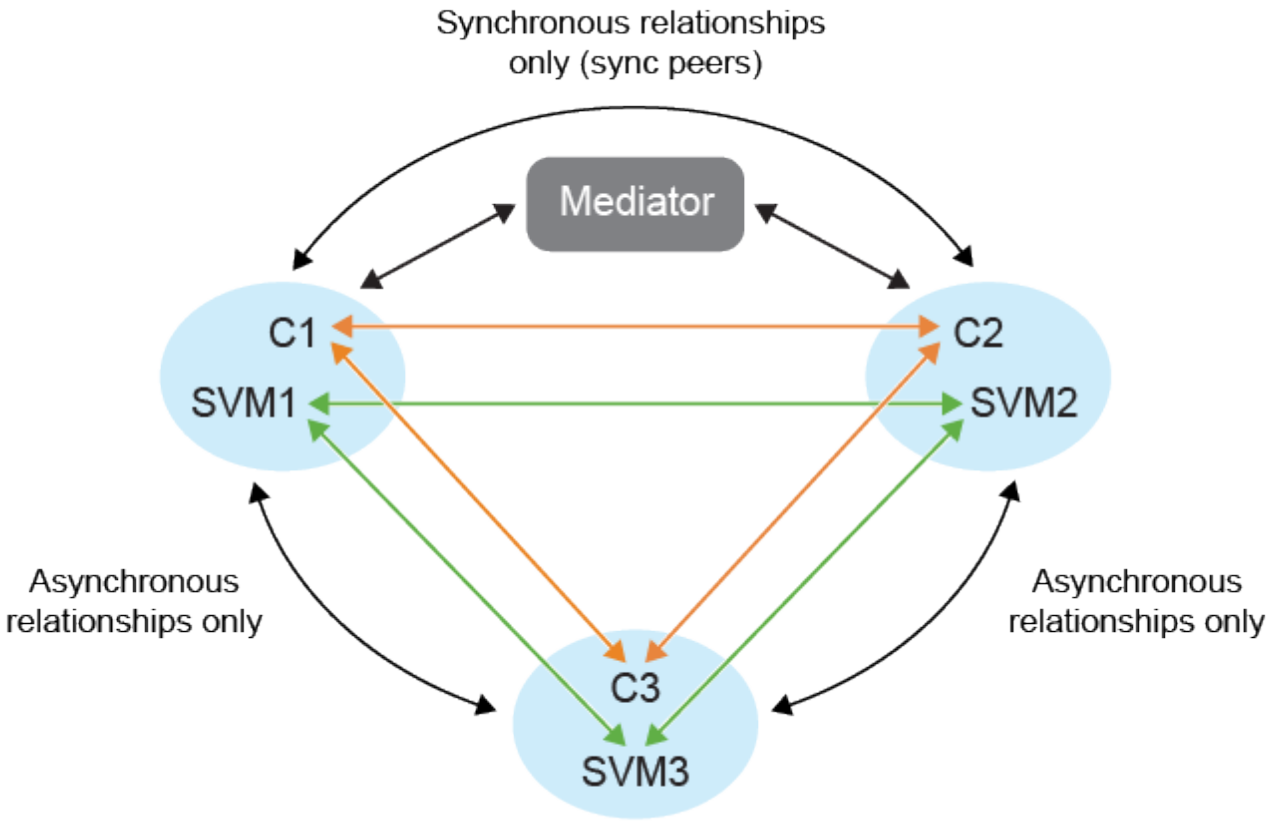
Per impostare la protezione fan-out, collegare in peering i tre cluster di siti e le SVM.

Esempio:

Se	quindi
• Il gruppo di coerenza di origine è nel cluster C1 e SVM svm1 • Il primo gruppo di coerenza di destinazione è sul cluster C2 e SVM svm2 e. • Il secondo gruppo di coerenza di destinazione è sul cluster C3 e SVM svm3	• Il peering dei cluster sul cluster ONTAP di origine sarà (C1, C2) e (C1, C3). • Il peering del cluster sul primo cluster ONTAP di destinazione sarà (C2, C1), (C2, C3) e. • Il peering del cluster sul secondo cluster ONTAP di destinazione sarà (C3, C1) e (C3, C2). • Il peering delle SVM sull'origine SVM sarà (svm1, svm2) e (svm1, svm3). • Il peering delle SVM sulla prima SVM di destinazione sarà (svm2, svm1) e (svm2, svm3) e. • Il peering delle SVM sulla seconda destinazione SVM sarà (svm3, svm1) e (svm3, svm2).

Il diagramma seguente mostra la configurazione della protezione fan-out:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Fasi

1. Selezionare un nuovo datastore segnaposto. I criteri di selezione del datastore segnaposto per la protezione graduale sono:
   - Non posizionare il datastore segnaposto nel cluster host che stai proteggendo.
   - Se è necessario includere il datastore segnaposto nel cluster host, aggiungerlo all'appliance VMware Live Site Recovery prima di configurare la protezione ActiveSync SnapMirror . Con questa configurazione, è possibile lasciare il datastore segnaposto fuori dalla protezione.

     Per maggiori informazioni, fare riferimento a "Selezionare un datastore segnaposto"
2. Aggiungere il datastore alla protezione del cluster host seguendo quanto segue"Modificare il cluster host protetto" . Aggiungere tipi di policy sia asincroni che sincroni.

Informazioni sul copyright

Informazioni sul marchio commerciale