



Proteggi i datastore e le macchine virtuali

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Sommario

- Proteggi i datastore e le macchine virtuali 1
 - Proteggere un cluster host negli ONTAP tools 1
 - Proteggi usando la protezione SRA 2
 - Configurare SRA negli ONTAP tools per proteggere i datastore 2
 - Configurare SRA in ONTAP tools for VMware vSphere per ambienti SAN e NAS 3
 - Configurare SRA in ONTAP tools per ambienti altamente scalabili 4
 - Configurare SRA sull'appliance VMware Live Site Recovery utilizzando ONTAP tools 5
 - Aggiorna le credenziali SRA negli strumenti ONTAP 6
 - Configura i siti protetti e di ripristino negli ONTAP tools 7
 - Configura le risorse del sito protetto e del sito di ripristino 9
 - Verificare i sistemi di archiviazione replicati negli ONTAP tools 12
 - Protezione fan-out negli ONTAP tools 13

Proteggi i datastore e le macchine virtuali

Proteggere un cluster host negli ONTAP tools

ONTAP tools for VMware vSphere gestisce la protezione dei cluster host. Tutti i datastore appartenenti alla SVM selezionata e montati su uno o più host del cluster sono protetti nell'ambito di un cluster host.

Prima di iniziare

Assicurati di soddisfare questi requisiti prima di proteggere un cluster host:

- Il cluster host contiene archivi dati provenienti da una sola SVM.
- I datastore presenti sul cluster non vengono montati su host esterni al cluster.
- I datastore montati sul cluster host sono datastore VMFS con protocollo iSCSI o FC. Non puoi usare vVols, NFS o datastore VMFS con protocolli NVMe/FC e NVMe/TCP.
- I datastore basati su volumi FlexVol/LUN montati su un host non fanno parte di alcun gruppo di coerenza.
- I datastore basati su volumi FlexVol/LUN montati su un host non fanno parte di alcuna relazione SnapMirror.
- Il cluster host contiene almeno un datastore.

Passaggi

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools > Protect Cluster**.
3. Nella finestra di protezione del cluster, il sistema compila automaticamente il tipo di datastore e i dettagli della macchina virtuale (VM) di origine dello storage. Seleziona il collegamento dei datastore per visualizzare i datastore protetti.
4. Seleziona **Aggiungi relazione**.
5. Nella finestra **Aggiungi relazione SnapMirror**, seleziona la **storage VM di destinazione** e il tipo di **policy**.

Il tipo di policy può essere asincrono o AutomatedFailOverDuplex.

Quando si aggiunge la relazione SnapMirror come policy di tipo AutomatedFailOverDuplex, è necessario aggiungere la VM di storage di destinazione come backend di storage allo stesso vCenter in cui ONTAP tools for VMware vSphere è distribuito.

Nel tipo di policy AutomatedFailOverDuplex, sono presenti configurazioni host uniformi e non uniformi. Quando si seleziona il pulsante di attivazione **Configurazione host uniforme**, la configurazione del gruppo initiator host viene replicata implicitamente sul sito di destinazione. Per ulteriori informazioni, consulta ["Concetti e termini chiave"](#).

6. Se scegli di avere una configurazione host non uniforme, seleziona l'accesso host (origine/destinazione) per ciascun host all'interno di quel cluster.
7. Seleziona **Aggiungi**.
8. Puoi modificare la protezione del cluster host usando l'operazione **Modifica protezione cluster host**. Puoi modificare o eliminare le relazioni usando le opzioni del menu con i puntini di sospensione.

9. Seleziona il pulsante **Proteggi**.

Il sistema crea un'attività di vCenter con i dettagli dell'ID del lavoro e ne mostra l'avanzamento nel pannello delle attività recenti. Questa è un'attività asincrona; l'interfaccia utente mostra solo lo stato di invio della richiesta e non attende il completamento dell'attività.

10. Per visualizzare i cluster host protetti, vai su **NetApp ONTAP tools > Protection > Host cluster relationships**. Seleziona un gruppo di coerenza per visualizzarne la capacità, i datastore associati e i gruppi di coerenza figlio.



Se devi rimuovere la protezione entro un'ora dalla creazione, esegui prima la rilevazione dello storage.

Informazioni correlate

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Proteggi usando la protezione SRA

Configurare SRA negli ONTAP tools per proteggere i datastore

ONTAP tools for VMware vSphere offre la possibilità di abilitare la funzionalità SRA per configurare il disaster recovery.

Prima di iniziare

- Dovresti aver già configurato la tua istanza del server vCenter e gli host ESXi.
- Dovresti aver implementato ONTAP tools for VMware vSphere.
- Dovresti aver scaricato il file dell'adattatore SRA `.tar.gz` dal ["Sito di supporto NetApp"](#).
- Dovresti avere le stesse pianificazioni personalizzate di SnapMirror sia sul cluster ONTAP di origine che su quello di destinazione prima di eseguire i flussi di lavoro SRA.
- ["Abilita i servizi di ONTAP tools per VMware vSphere"](#) per abilitare la funzionalità SRA.

Passaggi

1. Accedi all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando l'URL: `https://<srm_ip>:5480`, quindi vai su Storage Replication Adapters nell'interfaccia di gestione dell'appliance VMware Live Site Recovery.
2. Seleziona **Nuovo adattatore**.
3. Carica il file di installazione `.tar.gz` del plug-in SRA su VMware Live Site Recovery.
4. Esegui una nuova scansione degli adattatori per verificare che i dettagli siano aggiornati nella pagina Adattatori di replica dello storage di VMware Live Site Recovery.



Dopo un failover, azioni come espansione, montaggio ed eliminazione potrebbero non essere disponibili per i datastore. Esegui l'individuazione del datastore per aggiornare e visualizzare le azioni appropriate del menu contestuale.



Dopo ogni operazione di riprotezione, devi eseguire la rilevazione dello storage su entrambi i siti.

In una nuova configurazione con protezione SRA, esegui 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 Active Sync di SnapMirror in cui la fonte di SnapMirror passa al sito B per Automated Failover Duplex e Asynchronous SnapMirror, esegui un test failover tra i siti B e C. Saltare questo passaggio può causare un errore nell'operazione di riprotezione.

Informazioni correlate

["Configura il disaster recovery per i datastore NFS usando VMware Site Recovery Manager"](#)

Configurare SRA in ONTAP tools for VMware vSphere per ambienti SAN e NAS

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

Configura SRA per ambienti SAN



I gruppi di coerenza nei flussi di lavoro SRA sono supportati solo con protocolli SAN (iSCSI e Fibre Channel) sia sui sistemi di storage Unified che ASA r2.

Prima di iniziare

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di recovery:

- VMware Live Site Recovery: Il sito VMware fornisce la documentazione per l'installazione di VMware Live Site Recovery.

["Informazioni su VMware Live Site Recovery"](#)

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

Per le configurazioni del protocollo iSCSI, prima di eseguire i flussi di lavoro SRA, tenere presente quanto segue:

- **Sito protetto:** gli adattatori di storage iSCSI e i dettagli LIF dei dati vengono configurati automaticamente durante il provisioning dei datastore. Non è richiesta alcuna configurazione manuale.
- **Sito di ripristino:** gli adattatori di storage iSCSI devono essere configurati manualmente su ciascun host ESXi incluso nella mappatura delle risorse per il ripristino di emergenza. Per evitare di configurare gli adattatori singolarmente su ciascun host, crea un datastore segnaposto di tipo iSCSI sul sito di ripristino utilizzando la SVM su cui sono configurati i workflow SRA. Questo aggiunge automaticamente l'adattatore iSCSI e gli indirizzi IP LIF dei dati necessari a tutti gli host ESXi mappati. Consultare ["Configurare i datastore segnaposto negli ONTAP tools"](#) per maggiori dettagli.

Passaggi

1. Verifica che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario del sito protetto.
2. Verificare che le LUN siano presenti in igroups che hanno l'`ostype` opzione impostata su *VMware* sul sistema di storage primario.
3. Verifica che gli host ESXi del sito di recovery abbiano una connettività iSCSI e Fibre Channel appropriata verso la storage virtual machine (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario, e gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

Puoi farlo verificando che gli host ESXi abbiano LUN locali connessi sull'SVM oppure tramite il comando

iscsi show initiators sugli SVM. Controlla l'accesso ai LUN per i LUN mappati nell'host ESXi per verificare la connettività iSCSI.

Configura SRA per gli ambienti NAS



I gruppi di coerenza non sono supportati per NFS nei flussi di lavoro SRA. Se i volumi di datastore NFS vengono inseriti in un gruppo di coerenza e protetti, l'operazione Discover Devices non andrà a buon fine. Non utilizzare i gruppi di coerenza quando si proteggono i datastore NFS con SRA.

Prima di iniziare

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di recovery:

- VMware Live Site Recovery: Puoi trovare la documentazione di installazione di VMware Live Site Recovery sul sito VMware "[Informazioni su VMware Live Site Recovery](#)".
- SRA: Installa l'adattatore su VMware Live Site Recovery e sul server SRA.

Passaggi

1. Verifica che i datastore 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 storage virtual machine (SVM).
3. Verificare che nel campo **NFS Addresses** siano specificati indirizzi IP validi 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 o il FQDN nel campo **NFS Addresses**.
4. Usa il comando `ping` su ogni host ESXi nel sito di recovery per verificare che l'host abbia una porta VMkernel che può accedere agli indirizzi IP utilizzati per servire le esportazioni NFS dalla SVM.

Configurare SRA in ONTAP tools per ambienti altamente scalabili

Dovresti configurare gli intervalli di timeout di storage secondo le impostazioni consigliate per Storage Replication Adapter (SRA) per ottenere prestazioni ottimali in ambienti altamente scalati.

Impostazioni del provider di archiviazione

Dovresti impostare i seguenti valori di timeout su VMware Live Site Recovery per ambienti scalabili:

Impostazioni avanzate	Valori di timeout
<code>StorageProvider.resignatureTimeout</code>	Aumenta il valore dell'impostazione da 900 secondi a 12000 secondi.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Imposta un valore elevato (per esempio: 99999)

Dovresti anche abilitare l'opzione `StorageProvider.autoResignatureMode`.

Consultare ["Modifica le impostazioni del provider di storage"](#) per ulteriori informazioni sulla modifica delle impostazioni del provider di archiviazione.

Impostazioni di archiviazione

Quando si verifica un timeout, aumenta i valori di `storage.commandTimeout` e `storage.maxConcurrentCommandCnt` a 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.

Consultare ["Modifica le impostazioni di storage"](#) per modificare le impostazioni del provider SAN.

Configurare SRA sull'appliance VMware Live Site Recovery utilizzando ONTAP tools

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

Configurare SRA sull'appliance VMware Live Site Recovery salva le credenziali degli ONTAP tools for VMware vSphere all'interno dell'appliance, abilitando la comunicazione tra VMware Live Site Recovery e SRA.

Prima di iniziare

- Scarica il file `.tar.gz` da ["Sito di supporto NetApp"](#).
- Abilitare i servizi SRA in ONTAP tools Manager. Per ulteriori informazioni, consultare la sezione ["Abilita i servizi"](#).
- Aggiungi i server vCenter all'appliance ONTAP tools for VMware vSphere. Per ulteriori informazioni, consultare la sezione ["Aggiungi vCenter Server"](#).
- Aggiungere backend di storage a ONTAP tools for VMware vSphere. Per ulteriori informazioni, consultare la sezione ["Aggiungi backend di storage"](#).



Se hai applicato la patch del certificato vCenter dagli ONTAP tools, aggiorna la configurazione vCenter nell'appliance VMware Live Site Recovery utilizzando la porta (:5480). Per istruzioni, consulta ["Riconfigura l'appliance di Site Recovery Manager"](#).

Passaggi

1. Nella schermata dell'appliance VMware Live Site Recovery, seleziona **Storage Replication Adapter > New Adapter**.
2. Carica il file `.tar.gz` su VMware Live Site Recovery.
3. Accedi all'appliance VMware Live Site Recovery utilizzando un account amministratore tramite un client SSH come PuTTY.
4. Passa all'utente root utilizzando il comando: `su root`
5. Esegui il comando `cd /var/log/vmware/srm` per accedere alla directory dei log.
6. Nella posizione del log, inserisci il comando per ottenere il Docker ID utilizzato da SRA: `docker ps -l`

7. Per accedere all'ID del container, inserisci il comando: `docker exec -it -u srm <container id> sh`
8. Configura VMware Live Site Recovery con ONTAP tools for VMware vSphere indirizzo IP e password utilizzando il comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Inserisci la password tra virgolette singole in modo che lo script Perl consideri i caratteri speciali come parte della password, non come delimitatori.
 - Puoi impostare il nome utente e la password dell'applicazione (VASA Provider/SRA) in ONTAP tools Manager quando abiliti questi servizi per la prima volta. Usa queste credenziali per registrare SRA con VMware Live Site Recovery.
 - Per individuare il GUID di vCenter, vai alla pagina Server di vCenter in ONTAP tools Manager dopo aver aggiunto la tua istanza vCenter. Fai riferimento alla sezione ["Aggiungi vCenter Server"](#).
9. Esegui una nuova scansione degli adattatori per verificare che i dettagli aggiornati vengano visualizzati nella pagina Adattatori di replica dello storage di VMware Live Site Recovery.

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

Aggiorna le credenziali SRA negli strumenti ONTAP

Affinché VMware Live Site Recovery possa comunicare con SRA, dovresti aggiornare le credenziali di SRA sul server VMware Live Site Recovery se hai modificato le credenziali.

Prima di iniziare

Dovresti aver eseguito i passaggi menzionati nell'argomento ["Configurare SRA sull'appliance VMware Live Site Recovery"](#).

Passaggi

1. Eseguire i seguenti comandi per eliminare le credenziali degli ONTAP tools memorizzate nella cache dalla macchina VMware Live Site Recovery:
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`
 - d. `cd conf/`
 - e. `rm -rf *`
2. Esegui 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>`` Devi mettere una singola virgoletta intorno al valore della password.

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

Riconfigurare vCenter nell'appliance VMware Live Site Recovery dopo una modifica del certificato

Se il certificato vCenter cambia, ad esempio dopo un aggiornamento vCenter, è possibile che si verifichi un errore di mancata corrispondenza dell'impronta digitale nell'estensione Site Recovery. Eseguire i seguenti passaggi per risolverlo.

Passaggi

1. Riconfigurare vCenter nell'appliance VMware Live Site Recovery
 - a. Aprire l'interfaccia di gestione dell'appliance VMware Live Site Recovery in un browser:
`https://<SRM_IP>:5480`
 - b. Seleziona la scheda **Riepilogo**.
 - c. Seleziona **Riconfigura** per la connessione al server vCenter.

Questo recupera e accetta l'impronta digitale del certificato più recente da vCenter.

2. Riconnetti l'associazione del sito (se l'errore persiste)

Se l'errore di mancata corrispondenza dell'impronta digitale persiste dopo la riconfigurazione:

- a. Accedi all'interfaccia utente di vCenter.
- b. Accedere all'estensione **Site Recovery**.
- c. Individua la sezione **Associazione siti**.
- d. Seleziona **Riconnetti** per ristabilire l'associazione del sito con il certificato aggiornato.

Configura i siti protetti e di ripristino negli ONTAP tools

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

Quando aggiungi un nuovo datastore, puoi 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 a un volume protetto, aggiorna SnapMirror ed esegui la discovery dello storage sia sul sito protetto che su quello di recovery. Puoi eseguire la discovery manualmente o secondo una pianificazione per assicurarti che il nuovo datastore venga rilevato e protetto.

Abbina siti protetti e di recovery

Dovresti associare i siti protetti e di recovery creati usando il vSphere Client per permettere allo Storage Replication Adapter (SRA) di rilevare i sistemi storage.



Storage Replication Adapter (SRA) supporta il fan-out con una relazione sincrona di tipo Automated Failover Duplex e una relazione asincrona SnapMirror sul gruppo di coerenza. Tuttavia, il fan-out con due relazioni asincrone SnapMirror sui gruppi di coerenza o relazioni fan-out SnapMirror sui volumi non è supportato. Le relazioni di tipo vault SnapMirror non sono considerate all'interno di queste restrizioni di fan-out. Il supporto dei gruppi di coerenza in SRA è limitato ai protocolli SAN (iSCSI e fibre channel) sui sistemi di storage Unified e ASA r2. I gruppi di coerenza non sono supportati per NFS. Se i volumi del datastore NFS vengono inseriti in un gruppo di coerenza, l'operazione di rilevamento dei dispositivi non andrà a buon fine.

Prima di iniziare

- Dovresti avere VMware Live Site Recovery installato sia sul sito protetto che su quello di recovery.
- Dovresti avere SRA installato sia sul sito protetto che su quello di recovery.

Passaggi

1. Nella pagina iniziale del client vSphere, doppio click sull'icona **Ripristino sito** e quindi seleziona **Siti**.
2. Seleziona **Oggetti > Azioni > Associa siti**.
3. Nella finestra di dialogo **Associa server di Site Recovery Manager**, inserisci l'indirizzo del Platform Services Controller del sito protetto, quindi seleziona **Avanti**.
4. Nella sezione Seleziona vCenter Server, procedi come segue:
 - a. Verifica che il server vCenter del sito protetto appaia come candidato corrispondente per l'accoppiamento.
 - b. Inserisci le credenziali amministrative SSO e poi seleziona **Fine**.
5. Se richiesto, seleziona **Sì** per accettare i certificati di sicurezza.

Risultato

La finestra di dialogo **Oggetti** visualizza sia i siti protetti che quelli di recovery.

Configura i gruppi di protezione

Prima di iniziare

Dovresti assicurarti che sia il sito di origine che quello di destinazione siano configurati come segue:

- Stessa versione di VMware Live Site Recovery installata
- Macchine virtuali
- Siti protetti e di recovery abbinati
- I datastore di origine e di destinazione devono essere montati sui rispettivi siti

Passaggi

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

Tutte le macchine virtuali presenti nel gruppo di replica vengono aggiunte al gruppo di protezione.

6. Puoi selezionare un piano di recovery esistente oppure crearne uno nuovo selezionando **Aggiungi a un nuovo piano di recovery**.
7. Nella scheda Pronto per il completamento, rivedi i dettagli del gruppo di protezione che hai creato e poi seleziona **Fine**.

Configura le risorse del sito protetto e del sito di ripristino

Configurare le mappature di rete negli ONTAP tools

Dovresti configurare le mappature delle risorse, come reti VM, host ESXi e cartelle, su entrambi i siti per permettere la mappatura di ogni risorsa dal sito protetto alla risorsa appropriata nel sito di recovery.

Dovresti completare le seguenti configurazioni delle risorse:

- Mappature di rete
- Mappatura delle cartelle
- Mappature delle risorse
- Datastore segnaposto

Prima di iniziare

Dovresti aver collegato i siti protetto e di recovery.

Passaggi

1. Accedi al vCenter Server e seleziona **Ripristino del sito > Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature di rete > Nuovo** nella scheda Gestisci per creare una nuova mappatura di rete.
4. Nella procedura guidata Crea mappatura di rete, fai quanto segue:
 - a. Seleziona **Prepara automaticamente le mappature per le reti con nomi corrispondenti** e seleziona **Avanti**.
 - b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
 - c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
 - d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

Risultato

La pagina Mappature di rete visualizza le risorse del sito protetto e le risorse del sito di ripristino. Puoi seguire gli stessi passaggi per le altre reti nel tuo ambiente.

Configurare i mapping delle cartelle negli ONTAP tools

Dovresti mappare le cartelle sul sito protetto e sul sito di recovery per abilitare la comunicazione tra di loro.

Prima di iniziare

Dovresti aver collegato i siti protetto e di recovery.

Passaggi

1. Accedi al vCenter Server e seleziona **Ripristino del sito > Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature cartelle > icona Cartella** nella scheda Gestisci per creare una nuova mappatura di cartella.

4. Nella procedura guidata Crea mappatura cartelle, esegui le seguenti operazioni:
 - a. Seleziona **Prepara automaticamente le mappature per le cartelle con nomi corrispondenti** e seleziona **Avanti**.
 - b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
 - c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
 - d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

Risultato

La pagina Mappature cartelle visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire gli stessi passaggi per le altre cartelle presenti nell'ambiente.

Configurare le mappature delle risorse negli ONTAP tools

Dovresti mappare le tue risorse sul sito protetto e sul sito di ripristino in modo che le macchine virtuali siano configurate per eseguire il failover su un gruppo di host o sull'altro.

Prima di iniziare

Dovresti aver collegato i siti protetto e di recovery.



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

Passaggi

1. Accedi al vCenter Server e seleziona **Ripristino del sito > Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature risorse > Nuovo** nella scheda Gestisci per creare una nuova mappatura delle risorse.
4. Nella procedura guidata Crea mappatura risorse, esegui le seguenti operazioni:
 - a. Seleziona **Prepara automaticamente le mappature per le risorse con nomi corrispondenti** e seleziona **Avanti**.
 - b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
 - c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
 - d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

Risultato

La pagina Mappatura risorse visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire gli stessi passaggi per le altre risorse presenti nell'ambiente.

Configurare i datastore segnaposto negli ONTAP tools

Configura un datastore segnaposto per riservare spazio nell'inventario di vCenter nel sito di recovery per le macchine virtuali (VM) protette. I datastore segnaposto richiedono una capacità minima, perché le VM segnaposto sono piccole e di solito usano solo poche

centinaia di kilobyte.

Prima di iniziare

- Assicurati che i siti protetti e di recovery siano collegati.
- Verifica che le mappature delle risorse siano state configurate.

Passaggi

1. Accedi al vCenter Server e seleziona **Ripristino del sito > Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Nella scheda Gestisci, seleziona **Placeholder Datastores > New** per creare un nuovo placeholder datastore.
4. Seleziona l'archivio dati appropriato e seleziona **OK**.



I datastore segnaposto possono risiedere su storage locale o remoto, ma non richiedono la replica.

5. Ripeti i passaggi da 3 a 5 per configurare un datastore segnaposto per il sito di recovery.

Configurare SRA utilizzando il gestore array in ONTAP tools

Puoi configurare Storage Replication Adapter (SRA) usando la procedura guidata Array Manager di VMware Live Site Recovery per abilitare le interazioni tra VMware Live Site Recovery e le macchine virtuali di storage (SVM).

Prima di iniziare

- Dovresti aver associato i siti protetti e i siti di recovery in VMware Live Site Recovery.
- Dovresti aver configurato lo storage integrato prima di configurare l'array manager.
- Dovresti aver configurato e replicato le relazioni di SnapMirror tra i siti protetti e i siti di recovery.
- Dovresti aver abilitato i LIF di gestione SVM per abilitare il multitenancy.

SRA supporta la gestione a livello di cluster e la gestione a livello di SVM. Se aggiungi storage a livello di cluster, puoi individuare ed eseguire operazioni su tutte le SVM presenti nel cluster. Se aggiungi storage a livello di SVM, puoi gestire solo quella specifica SVM.

Passaggi

1. In VMware Live Site Recovery, seleziona **Gestori array > Aggiungi gestore array**.
2. Inserisci le seguenti informazioni per descrivere l'array in VMware Live Site Recovery:
 - a. Inserisci un nome per identificare il gestore dell'array nel campo **Nome visualizzato**.
 - b. Nel campo **Tipo SRA**, seleziona **NetApp Storage Replication Adapter for ONTAP**.
 - c. Inserisci le informazioni per connetterti al cluster o all'SVM:
 - Se ti stai connettendo a un cluster, dovresti inserire la LIF di gestione del cluster.
 - Se ti connetti direttamente a un SVM, devi immettere l'indirizzo IP del LIF di gestione dell'SVM.



Quando configuri l'array manager, dovresti usare la stessa connessione (indirizzo IP) per il sistema storage che hai usato per l'onboarding del sistema storage in ONTAP tools for VMware vSphere. Ad esempio, se la configurazione dell'array manager è a livello SVM, allora lo storage sotto ONTAP tools for VMware vSphere dovrebbe essere aggiunto a livello SVM.

- d. Se ti connetti a un cluster, specifica il nome dell'SVM nel campo **Nome SVM** oppure lascialo vuoto per gestire tutti gli SVM del cluster.
- e. Inserisci i volumi da rilevare nel campo **Volume include list**.

Puoi inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di recovery.

Ad esempio, se vuoi individuare il volume `src_vol1` che è in una relazione di SnapMirror con il volume `dst_vol1`, dovresti specificare `src_vol1` nel campo del sito protetto e `dst_vol1` nel campo del sito di recovery.

- f. **(Facoltativo)** Inserisci i volumi da escludere dalla discovery nel campo **Volume exclude list**.

Puoi inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di recovery.

Ad esempio, se vuoi escludere il volume `src_vol1` che è in una relazione di SnapMirror con il volume `dst_vol1`, dovresti specificare `src_vol1` nel campo del sito protetto e `dst_vol1` nel campo del sito di recovery.

- 3. Seleziona **Avanti**.
- 4. Verifica che l'array venga rilevato e visualizzato nella parte inferiore della finestra Aggiungi gestore array e seleziona **Fine**.

Puoi seguire gli stessi passaggi per il sito di recovery utilizzando gli indirizzi IP di gestione SVM e le credenziali appropriate. Nella schermata Abilita coppie di array della procedura guidata Aggiungi gestore array, dovresti verificare che sia selezionata la coppia di array corretta e che risulti pronta per essere abilitata.

Verificare i sistemi di archiviazione replicati negli ONTAP tools

Dovresti verificare che il sito protetto e il sito di ripristino siano stati associati correttamente dopo aver configurato Storage Replication Adapter (SRA). Il sistema storage replicato deve essere rilevabile sia dal sito protetto che dal sito di ripristino.

Prima di iniziare

- Dovresti aver configurato il tuo sistema storage.
- Dovresti aver associato il sito protetto e il sito di ripristino utilizzando VMware Live Site Recovery array manager.
- Dovresti aver abilitato la licenza FlexClone e la licenza SnapMirror prima di eseguire l'operazione di test failover e l'operazione di failover per SRA.
- Dovresti avere le stesse politiche e pianificazioni SnapMirror sia sul sito di origine che su quello di destinazione.
- Se si utilizzano criteri SnapMirror personalizzati con una pianificazione personalizzata, è necessario configurare la stessa pianificazione e gli stessi criteri sia sul sito protetto che su quello di ripristino.
- Se si utilizzano criteri SnapMirror personalizzati (con pianificazione predefinita o personalizzata), è

necessario eseguire il rilevamento dello storage dagli strumenti ONTAP affinché il nuovo criterio venga riconosciuto. In caso contrario, i flussi di lavoro SRA, inclusi il failover di test e il failover effettivo, non andranno a buon fine. Eseguire il rilevamento dello storage nei seguenti punti:

- Dopo aver creato i criteri personalizzati sul sito di ripristino.
- Dopo un'operazione di riprotezione, che ricrea i criteri sul sito protetto.

Passaggi

1. Accedi al tuo vCenter Server.
2. Vai su **Ripristino del sito > Replica basata su array**.
3. Seleziona la coppia di array richiesta e verifica i dettagli corrispondenti.

I sistemi di archiviazione dovrebbero essere rilevati nel sito protetto e nel sito di ripristino con lo stato **Enabled**.

Protezione fan-out negli ONTAP tools

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



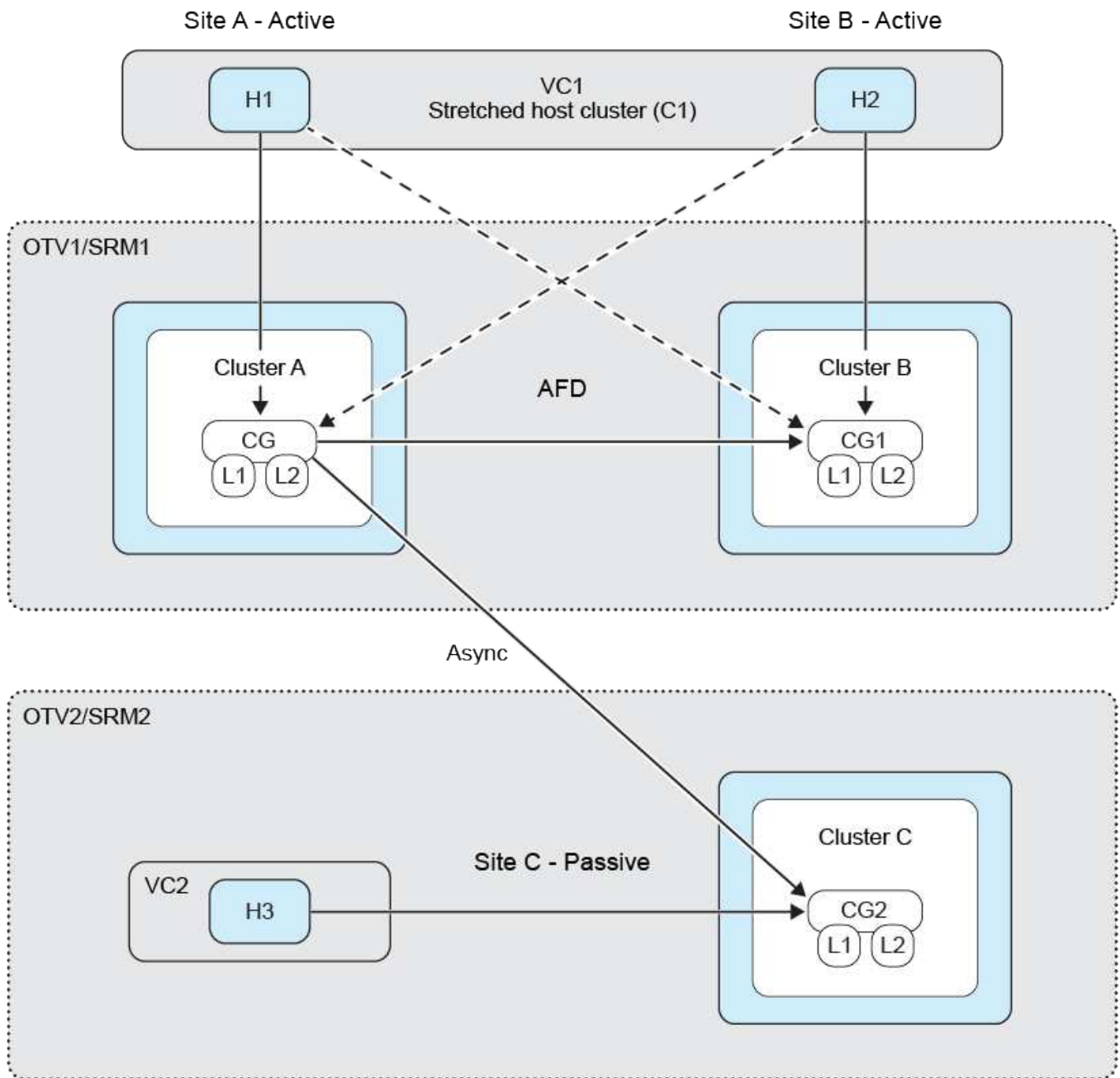
La funzionalità fan-out non è supportata per gli utenti SVM.

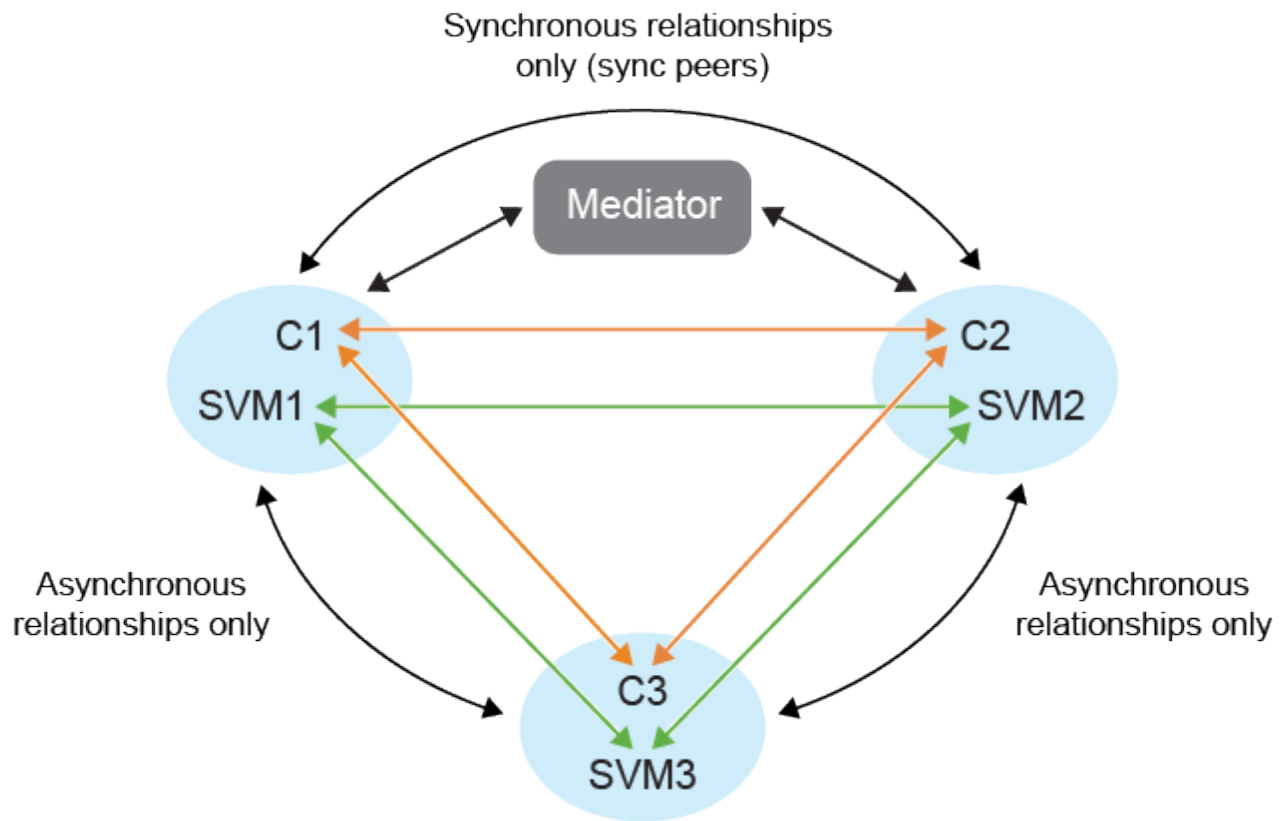
Per configurare la protezione fan-out, effettua il peering tra i tre cluster del sito e gli SVM.

Esempio:

Se	Poi
• Il gruppo di coerenza della fonte si trova sul cluster c1 e sulla SVM svm1 • Il primo gruppo di coerenza di destinazione si trova sul cluster c2 e sull'SVM svm2 e • Il secondo gruppo di coerenza di destinazione si trova sul cluster c3 e sull'SVM svm3	• Il peering del cluster sul cluster ONTAP di origine sarà (C1, C2) e (C1, C3). • Il cluster peering sul primo cluster di destinazione ONTAP sarà (C2, C1) e (C2, C3) e • Il peering del cluster sul secondo cluster di destinazione ONTAP sarà (C3, C1) e (C3, C2). • Il peering SVM sull'SVM sorgente sarà (svm1, svm2) e (svm1, svm3). • Il peering SVM sulla prima SVM di destinazione sarà (svm2, svm1) e (svm2, svm3) e • Il peering SVM sulla seconda SVM di destinazione sarà (svm3, svm1) e (svm3, svm2).

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





Passaggi

1. Selezionare un nuovo archivio dati segnaposto. I criteri di selezione dell'archivio dati segnaposto per la protezione graduale sono:
 - Non posizionare il datastore segnaposto nel cluster 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 della sincronizzazione attiva SnapMirror. Con questa configurazione, è possibile escludere il datastore segnaposto dalla protezione.

Per ulteriori informazioni, fare riferimento a ["Seleziona un datastore segnaposto"](#)

2. Aggiungere i datastore alla protezione del cluster host seguendo ["Modifica cluster protetto"](#). Aggiungere sia i tipi di policy asincroni che sincroni.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.