



Protezione dei dati e disaster recovery

System Manager Classic

NetApp
June 22, 2024

Sommario

- Protezione dei dati e disaster recovery 1
 - Configurazione del peering di cluster e SVM 1
 - Disaster recovery dei volumi 12
 - Preparazione al disaster recovery dei volumi 24
 - Backup del volume con SnapVault 33
 - Gestione del ripristino dei volumi con SnapVault 41

Protezione dei dati e disaster recovery

Configurazione del peering di cluster e SVM

Panoramica del peering di cluster e SVM

Gli amministratori dei cluster possono creare relazioni peer autenticate tra cluster e SVM per consentire ai cluster di comunicare tra loro in modo che i dati siano replicati tra volumi in cluster diversi. È possibile eseguire le procedure utilizzando l'interfaccia *classic* di Gestore di sistema di ONTAP, disponibile con ONTAP 9.7 e versioni precedenti di ONTAP 9.

Utilizzare l'interfaccia *classic* del gestore di sistema di ONTAP per creare relazioni di peer cluster e relazioni di peer SVM se si applicano le seguenti condizioni:

- Si stanno lavorando con cluster che eseguono ONTAP 9.7 o versioni precedenti di ONTAP 9.
- Si desidera che le relazioni di peering dei cluster siano autenticate.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si desidera utilizzare Gestione sistema, non l'interfaccia della riga di comando (CLI) di ONTAP o uno strumento di scripting automatico.

Altri modi per farlo in ONTAP

Gestore di sistema di ONTAP in ONTAP 9.3 semplifica la configurazione delle relazioni peer tra cluster e tra SVM. La procedura di peering del cluster e la procedura di peering SVM possono essere utilizzate per tutte le versioni di ONTAP 9. Utilizzare la procedura appropriata per la versione di ONTAP in uso.

| Per eseguire queste attività con... | Fare riferimento a... |
|---|---|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | <ul style="list-style-type: none">• "Gestione del cluster con System Manager" |
| L'interfaccia della riga di comando (CLI) di ONTAP | <ul style="list-style-type: none">• "Panoramica del peering di cluster e SVM con CLI" <p>Utilizza l'interfaccia della riga di comando per impostare le relazioni di peering dei cluster e le relazioni di peering SVM.</p> <ul style="list-style-type: none">• "Gestione della rete" <p>Utilizzare l'interfaccia della riga di comando per configurare sottoreti, LIF di intercluster, percorsi, policy firewall e altri componenti di rete</p> |

Prerequisiti per il peering del cluster

Prima di impostare il peering del cluster utilizzando l'interfaccia *classic* di Gestione

sistema ONTAP con ONTAP 9.7 o versione precedente, è necessario verificare che la connettività, la porta, l'indirizzo IP, la subnet, il firewall, e i requisiti di naming dei cluster sono soddisfatti.

Requisiti di connettività

Ogni LIF di intercluster sul cluster locale deve essere in grado di comunicare con ogni LIF di intercluster sul cluster remoto.

Sebbene non sia necessario, è in genere più semplice configurare gli indirizzi IP utilizzati per le LIF di intercluster nella stessa subnet. Gli indirizzi IP possono risiedere nella stessa sottorete dei file LIF dei dati o in una sottorete diversa. La subnet utilizzata in ciascun cluster deve soddisfare i seguenti requisiti:

- La subnet deve disporre di un numero sufficiente di indirizzi IP da allocare a un LIF intercluster per nodo.

Ad esempio, in un cluster a sei nodi, la subnet utilizzata per la comunicazione tra cluster deve avere sei indirizzi IP disponibili.

Ciascun nodo deve disporre di una LIF intercluster con un indirizzo IP sulla rete intercluster.

Le LIF di intercluster possono avere un indirizzo IPv4 o IPv6.



ONTAP 9 consente di migrare le reti peering da IPv4 a IPv6, consentendo la presenza simultanea di entrambi i protocolli nelle LIF dell'intercluster. Nelle versioni precedenti, tutte le relazioni tra cluster per un intero cluster erano IPv4 o IPv6. Ciò significava che la modifica dei protocolli era un evento potenzialmente disgregativo.

Requisiti delle porte

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Le porte devono soddisfare i seguenti requisiti:

- Tutte le porte utilizzate per comunicare con un determinato cluster remoto devono trovarsi nello stesso IPspace.

È possibile utilizzare più IPspaces per eseguire il peer con più cluster. La connettività full-mesh a coppie è necessaria solo all'interno di un IPspace.

- Il dominio di broadcast utilizzato per la comunicazione tra cluster deve includere almeno due porte per nodo in modo che la comunicazione tra cluster possa eseguire il failover da una porta a un'altra.

Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).

- Tutte le porte devono essere cablate.
- Tutte le porte devono essere in buono stato.
- Le impostazioni MTU delle porte devono essere coerenti.

Requisiti del firewall

I firewall e i criteri di firewall tra cluster devono consentire i seguenti protocolli:

- Servizio ICMP
- TCP agli indirizzi IP di tutte le LIF dell'intercluster sulle porte 10000, 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

Sebbene HTTPS non sia richiesto quando si imposta il peering del cluster utilizzando l'interfaccia CLI, HTTPS è richiesto in seguito se si utilizza Gestione di sistema di ONTAP per configurare la protezione dei dati.

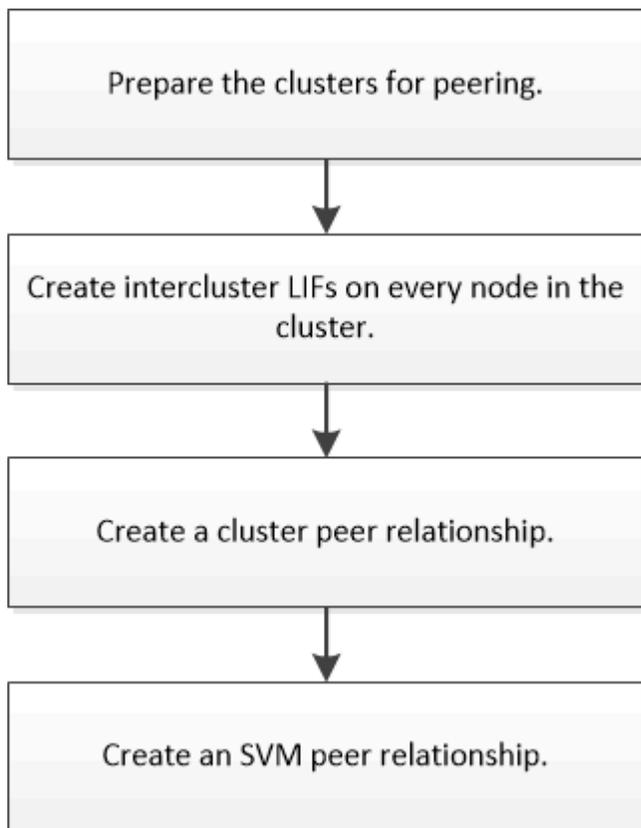
L'impostazione predefinita `intercluster` La policy firewall consente l'accesso tramite il protocollo HTTPS e da tutti gli indirizzi IP (0.0.0.0/0). Se necessario, è possibile modificare o sostituire la policy.

Informazioni correlate

["Protezione dei dati"](#)

Workflow di peering di cluster e SVM

È possibile impostare una relazione di peering utilizzando Gestione di sistema di ONTAP con ONTAP 9.7 o versioni precedenti. L'impostazione di una relazione di peering implica la preparazione di ciascun cluster per il peering, la creazione di interfacce logiche di intercluster (LIF) su ciascun nodo di ciascun cluster, la configurazione di una relazione di peer del cluster e la configurazione di una relazione di peering SVM.



Se si utilizza ONTAP 9.2 o versioni precedenti, si crea una relazione di peering SVM durante la creazione di una relazione di protezione dei dati tra il volume di origine e il volume di destinazione.

Preparatevi per il peering dei cluster

Prima di creare una relazione di peering del cluster utilizzando l'interfaccia *classic* di Gestore di sistema di ONTAP con ONTAP 9.7 o versione precedente, è necessario verificare che l'ora di ciascun cluster sia sincronizzata con un server NTP esterno e determinare le subnet, le porte e le passphrase che si desidera utilizzare.

Fasi

1. Se si utilizza ONTAP 9.2 o versioni precedenti, determinare la passphrase che si desidera utilizzare per ogni relazione peer del cluster.

La passphrase deve contenere almeno otto caratteri.

| Per il rapporto tra... | La passphrase è... |
|--|--------------------|
| Quadro strumenti A e quadro strumenti B. | |

A partire da ONTAP 9.3, è possibile generare la passphrase dal cluster remoto durante la creazione della relazione peer del cluster.

"Creazione di una relazione peer del cluster (a partire da ONTAP 9.3)"

2. Identificare le subnet, gli indirizzi IP e le porte da utilizzare per le LIF di intercluster.

Per impostazione predefinita, l'indirizzo IP viene selezionato automaticamente dalla subnet. Se si desidera specificare manualmente l'indirizzo IP, assicurarsi che l'indirizzo IP sia già disponibile nella subnet o che possa essere aggiunto alla subnet in un secondo momento. Le informazioni sulle subnet sono disponibili nella scheda rete.

Creare una tabella simile alla seguente per registrare le informazioni sui cluster. Nella tabella seguente si presuppone che ciascun cluster abbia quattro nodi. Se un cluster ha più di quattro nodi, aggiungere righe per ottenere ulteriori informazioni.

| | Quadro strumenti A. | Cluster B |
|--|---------------------|-----------|
| Subnet (ONTAP 9.2 o versione precedente) | | |
| Indirizzo IP (a partire da ONTAP 9.3, opzionale per ONTAP 9.2 o versioni precedenti) | | |
| Porta del nodo 1 | | |
| Porta del nodo 2 | | |
| Porta del nodo 3 | | |
| Porta del nodo 4 | | |

Configurare le relazioni peer (a partire da ONTAP 9.3)

Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro. A partire da ONTAP 9.3, fino a ONTAP 9.7, è possibile utilizzare l'interfaccia *classic* del gestore di sistema di ONTAP per eseguire un metodo semplificato per configurare le relazioni peer tra cluster e tra SVM.

Creazione di LIF tra cluster (a partire da ONTAP 9.3)

A partire da ONTAP 9.3, fino a ONTAP 9.7, è possibile utilizzare l'interfaccia *classic* di Gestore di sistema di ONTAP per creare interfacce logiche (LIF) intercluster, che consentono alla rete del cluster di comunicare con un nodo. È necessario creare una LIF intercluster all'interno di ciascun IPspace che verrà utilizzato per il peering, su ciascun nodo di ciascun cluster per il quale si desidera creare una relazione peer.

A proposito di questa attività

Ad esempio, se si dispone di un cluster a quattro nodi che si desidera eseguire il peer con il cluster X su IPspace A e il peer con il cluster Y su IPspace Y, è necessario un totale di otto LIF intercluster; Quattro su IPspace A (uno per nodo) e quattro su IPspace Y (uno per nodo).

È necessario eseguire questa procedura su entrambi i cluster per i quali si desidera creare una relazione peer.

Fasi

1. Fare clic su **Configuration > Advanced Cluster Setup**.
2. Nella finestra **Setup Advanced Cluster Features**, fare clic su **Proceed** (Procedi) accanto all'opzione **Cluster peering**.
3. Selezionare un IPspace dall'elenco **IPspace**.
4. Inserire l'indirizzo IP, la porta, la maschera di rete e i dettagli del gateway di ciascun nodo.

| | IP Address | Port | Netmask | Gateway (Optional) |
|--------------------|------------|------|---------------|--|
| st150-vcim-ucs103a | 10.53.32.1 | e0d | 255.255.240.0 | <input checked="" type="checkbox"/> Use same net...and gateway |
| st150-vcim-ucs103b | 10.53.32.2 | e0d | | |

5. Fare clic su **Invia e continua**.

Cosa fare in seguito

Inserire i dettagli del cluster nella finestra di peering del cluster per continuare con il peering del cluster.

Creazione di una relazione peer del cluster (a partire da ONTAP 9.3)

A partire da ONTAP 9.3, fino a ONTAP 9.7, è possibile utilizzare l'interfaccia *classic* del gestore di sistema di ONTAP per creare una relazione peer del cluster tra due cluster fornendo una passphrase generata dal sistema e gli indirizzi IP delle LIF intercluster del cluster remoto.

A proposito di questa attività

A partire da ONTAP 9.6, la crittografia del peering del cluster è attivata per impostazione predefinita su tutte le relazioni di peering del cluster appena create. La crittografia del peering del cluster deve essere attivata manualmente per la relazione di peering creata prima dell'aggiornamento a ONTAP 9.6. La crittografia del peering dei cluster non è disponibile per i cluster che eseguono ONTAP 9.5 o versioni precedenti. Pertanto, entrambi i cluster nella relazione di peering devono eseguire ONTAP 9.6 per abilitare la crittografia di peering dei cluster.

La crittografia di peering dei cluster utilizza il TLS (Transport Security Layer) per proteggere le comunicazioni di peering tra cluster per le funzionalità di ONTAP come SnapMirror e FlexCache.

Fasi

1. Nel campo **Target Cluster Intercluster LIF IP addresses** (indirizzi IP LIF cluster di destinazione), immettere gli indirizzi IP delle LIF intercluster del cluster remoto.
2. genera una passphrase dal cluster remoto.
 - a. Specificare l'indirizzo di gestione del cluster remoto.
 - b. Fare clic su **URL di gestione** per avviare Gestore di sistema di ONTAP sul cluster remoto.
 - c. Accedere al cluster remoto.
 - d. Nella finestra **Cluster Peers**, fare clic su **generate peering Passphrase**.
 - e. Selezionare le autorizzazioni IPspace, Valid (validità) della passphrase e SVM.

È possibile consentire il peering di tutte le SVM o SVM selezionate. Quando viene generata una richiesta peer SVM, le SVM consentite vengono automaticamente messe in peer con le SVM di origine senza richiedere l'accettazione della relazione peer dalle SVM remote.

- f. Fare clic su **generate** (genera).

Vengono visualizzate le informazioni relative alla passphrase.

Generate Peering Passphrase



Passphrase generated successfully

Use the following information for peering based on the IPspace "Default":

Intercluster LIF IP Address 172.21.91.12

Passphrase QS7k+laFYJzclV9UMPXvHgWd

Passphrase Validity Valid Until Mon Nov... America/New_Y

SVM Permissions All

Email passphrase details

Copy passphrase details

Done

- a. Fare clic su **Copy passphrase details** (Copia dettagli passphrase) o *Email passphrase
- b. Fare clic su **fine**.
3. Nel cluster di origine, immettere la passphrase generata in [Passaggio 2](#).
4. Fare clic su **Initiate Cluster peering** (Avvia peering cluster)
La relazione peer del cluster è stata creata correttamente.
5. Fare clic su **continua**.

Cosa fare in seguito

Specificare i dettagli SVM nella finestra di peering SVM per continuare con il processo di peering.

Creare relazioni peer SVM

A partire da ONTAP 9.3, fino a ONTAP 9.7, è possibile utilizzare l'interfaccia *classic* di Gestore di sistema di ONTAP per creare relazioni peer SVM. Il peering delle macchine virtuali di storage (SVM) consente di stabilire una relazione peer tra due SVM per la protezione dei dati.

Fasi

1. Selezionare l'SVM iniziatore.

2. Selezionare la SVM di destinazione dall'elenco delle SVM consentite.
3. Fare clic su **Initiate SVM peering**.
4. Fare clic su **continua**.

Cosa fare in seguito

Nella finestra Summary (Riepilogo) è possibile visualizzare le LIF dell'intercluster, la relazione peer del cluster e la relazione peer SVM.

Configurare le relazioni peer (ONTAP 9.2 e versioni precedenti)

Utilizzando l'interfaccia *classic* di Gestore di sistema di ONTAP con ONTAP 9.2 o una versione precedente di ONTAP 9, è possibile creare relazioni peer SVM.

Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro. È necessario creare una relazione peer del cluster prima di creare una relazione peer SVM.

Creazione di interfacce di intercluster su tutti i nodi (ONTAP 9.2 o versioni precedenti)

Utilizzando l'interfaccia *classic* di Gestore di sistema di ONTAP con ONTAP 9.2 o una versione precedente di ONTAP 9, è possibile creare LIF intercluster da utilizzare per il peering.

I cluster comunicano tra loro attraverso interfacce logiche (LIF) dedicate alla comunicazione tra cluster. È necessario creare una LIF intercluster all'interno di ogni IPspace che verrà utilizzato per il peering. Le LIF devono essere create su ciascun nodo di ciascun cluster per il quale si desidera creare una relazione peer.

Prima di iniziare

È necessario aver identificato la subnet, le porte e, facoltativamente, gli indirizzi IP che si intende utilizzare per le LIF dell'intercluster.

A proposito di questa attività

È necessario eseguire questa procedura su entrambi i cluster per i quali si desidera creare una relazione peer. Ad esempio, se si dispone di un cluster a quattro nodi che si desidera eseguire il peer con il cluster X su IPspace A e il peer con il cluster Y su IPspace Y, è necessario un totale di otto LIF intercluster; Quattro su IPspace A (uno per nodo) e quattro su IPspace Y (uno per nodo).

Fasi

1. creare una LIF di intercluster su un nodo del cluster di origine:
 - a. Accedere alla finestra **Network Interfaces** (interfacce di rete).
 - b. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create Network Interface (Crea interfaccia di rete).

- c. Immettere un nome per la LIF dell'intercluster.

È possibile utilizzare "icl01" per la LIF dell'intercluster sul primo nodo e "icl02" per la LIF dell'intercluster sul secondo nodo.

- d. Selezionare **Intercluster Connectivity** come ruolo dell'interfaccia.

e. Selezionare IPSpace.

f. Nella finestra di dialogo **Aggiungi dettagli**, selezionare **utilizzando una subnet** dall'elenco a discesa **Assegna indirizzo IP**, quindi selezionare la subnet che si desidera utilizzare per la comunicazione tra cluster.

Per impostazione predefinita, l'indirizzo IP viene selezionato automaticamente dalla subnet dopo aver fatto clic su **Create** (Crea). Se non si desidera utilizzare l'indirizzo IP selezionato automaticamente, è necessario specificare manualmente l'indirizzo IP utilizzato dal nodo per la comunicazione tra cluster.

g. Se si desidera specificare manualmente l'indirizzo IP utilizzato dal nodo per la comunicazione tra cluster, selezionare **Usa questo indirizzo IP** e digitare l'indirizzo IP.

Assicurarsi che l'indirizzo IP che si desidera utilizzare sia già disponibile nella subnet o che possa essere aggiunto alla subnet in un secondo momento.

h. Nell'area **Porte**, fare clic sul nodo che si sta configurando e selezionare la porta che si desidera utilizzare per questo nodo.

i. Se si decide di non condividere le porte per la comunicazione tra cluster e la comunicazione dati, verificare che la porta selezionata visualizzi "0" nella colonna **Hosted Interface Count**.

Specify the following details to add a new network interface for data and management access of the chosen SVM.

Name:

Interface Role: Serves Data Intercluster Connectivity

SVM:

Protocol Access: CIFS ISCSI NFS FC/FCoE

Management Access: Enable Management Access

Subnet:

The IP address is selected from this subnet. Use this IP Address:

i This IP address will be added to the chosen subnet if the address is not already present in the subnet available range.

| Ports or Adapters | Hosted Interface Count | Speed |
|-------------------|------------------------|-----------|
| ▲ clusterA-node1 | | |
| e0c | 3 | 1000 Mbps |
| e0d | 0 | 1000 Mbps |
| e0e | 0 | 1000 Mbps |

j. Fare clic su **Create** (Crea).

2. Ripetere [Fase 1](#) per ogni nodo del cluster.

Ciascun nodo del cluster dispone di una LIF intercluster.

3. Prendere nota degli indirizzi IP delle LIF dell'intercluster in modo da poterli utilizzare in un secondo momento quando si creano relazioni peer con altri cluster:

- a. Nella finestra **Network Interfaces**, nella colonna **role**, fare clic su Deselezionare la casella di controllo **tutto**, quindi selezionare **Intercluster**.

La finestra Network Interfaces (interfacce di rete) visualizza solo le LIF dell'intercluster.

- b. Annotare gli indirizzi IP elencati nella colonna **IP Addresses/WWPN** (indirizzi IP/WWPN*) oppure lasciare aperta la finestra **Network Interfaces** (interfacce di rete) per recuperare gli indirizzi IP in un secondo momento.

È possibile fare clic sull'icona di visualizzazione delle colonne () per nascondere le colonne che non si desidera visualizzare.

Risultati

Tutti i nodi di ciascun cluster dispongono di LIF intercluster in grado di comunicare tra loro.

Creazione di una relazione peer del cluster (ONTAP 9.2 o versione precedente)

Utilizzando l'interfaccia *classic* di Gestore di sistema di ONTAP con ONTAP 9.2 o una versione precedente di ONTAP 9, è possibile creare una relazione di peer del cluster tra due cluster immettendo una passphrase predeterminata e gli indirizzi IP delle LIF dell'intercluster del cluster remoto, e quindi verificare che la relazione sia stata creata correttamente.

Prima di iniziare

- È necessario conoscere gli indirizzi IP di tutte le LIF di intercluster dei cluster che si desidera eseguire.
- È necessario conoscere la passphrase da utilizzare per ogni relazione peer.

A proposito di questa attività

È necessario eseguire questa procedura su ciascun cluster.

Fasi

1. Dal cluster di origine, creare una relazione peer del cluster con il cluster di destinazione.

- a. Fare clic sulla scheda **configurazioni**.
- b. Nel riquadro **Cluster Settings**, fare clic su **Cluster Peers**.
- c. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo **Create Cluster Peer** (Crea peer cluster).

- d. nell'area **Details of the remote cluster to be peered** (Dettagli del cluster remoto da peering*), specificare la passphrase che entrambi i peer utilizzeranno per garantire una relazione peer del cluster autenticata.
- e. Inserire gli indirizzi IP di tutte le LIF intercluster del cluster di destinazione (uno per nodo) separati da virgole.

f. Fare clic su **Create** (Crea).

Lo stato di autenticazione è “pending” perché è stato configurato un solo cluster.

2. Passare al cluster di destinazione, quindi creare una relazione peer del cluster con il cluster di origine:

- a. Fare clic sulla scheda **configurazioni**.
- b. Nel riquadro **Cluster Settings**, fare clic su **Cluster Peers**.
- c. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create Cluster Peer (Crea peer cluster).

d. Nell’area **Dettagli del cluster remoto da eseguire il peering**, specificare la stessa passphrase specificata in [Fase 1d](#) E gli indirizzi IP delle LIF di intercluster del cluster di origine, quindi fare clic su **Create** (Crea).

3. Dalla finestra **Cluster Peers** del cluster di destinazione, verificare che il cluster di origine sia “Available” e che lo stato di autenticazione sia “OK”.

Availability and Authentication Status information might be stale for up to several minutes.

Create Modify Passphrase Modify Peer Network Parameters Delete Refresh

| Peer Cluster | Availability | Authentication Status |
|--------------|--------------|-----------------------|
| clusterA | available | ok |

Potrebbe essere necessario fare clic su **Refresh** (Aggiorna) per visualizzare le informazioni aggiornate.

I due cluster sono in una relazione di pari livello.

4. Passare al cluster di origine e verificare che il cluster di destinazione sia "Available" e che lo stato di autenticazione sia "OK".

Potrebbe essere necessario fare clic su **Refresh** (Aggiorna) per visualizzare le informazioni aggiornate.

Cosa fare in seguito

Creare una relazione peer SVM tra le SVM di origine e di destinazione creando una relazione di protezione dei dati tra il volume di origine e il volume di destinazione.

["Backup del volume con SnapVault"](#)

["Preparazione al disaster recovery dei volumi"](#)

Disaster recovery dei volumi

Panoramica sul disaster recovery dei volumi

È possibile attivare rapidamente un volume di destinazione dopo un disastro e quindi riattivare il volume di origine in ONTAP utilizzando l'interfaccia classica di Gestione di sistema di ONTAP (ONTAP 9.7 e versioni precedenti).

Utilizzare questa procedura se si desidera eseguire il disaster recovery a livello di volume nel modo seguente:

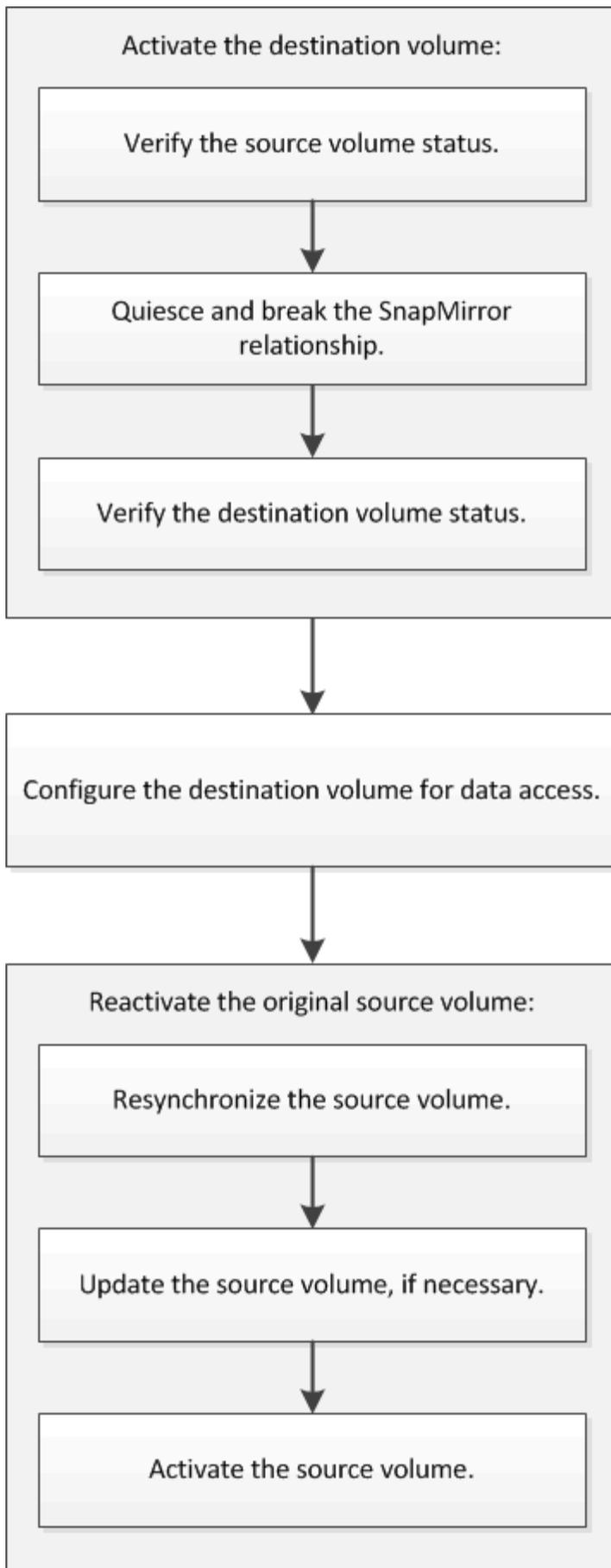
- Stai lavorando con cluster che eseguono ONTAP 9.
- Sei un amministratore del cluster.
- Di seguito è stata configurata la relazione SnapMirror [Preparazione al disaster recovery dei volumi](#)
- L'amministratore del cluster di origine ha dichiarato che i dati nel volume di origine non sono disponibili a causa di eventi come l'infezione da virus che ha portato alla corruzione dei dati o all'eliminazione accidentale dei dati.
- Si desidera utilizzare Gestione sistema, non l'interfaccia della riga di comando di ONTAP o uno strumento di scripting automatico.
- Si desidera utilizzare l'interfaccia classica di Gestione sistema per ONTAP 9.7 e versioni precedenti, non l'interfaccia utente di Gestione sistema di ONTAP per ONTAP 9.7 e versioni successive.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Non si desidera leggere un sacco di background concettuale.

Altri modi per farlo in ONTAP

| Per eseguire queste attività con... | Guarda questo contenuto... |
|---|---|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | "Fornire i dati da una destinazione SnapMirror" |
| L'interfaccia della riga di comando di ONTAP | "Attivare il volume di destinazione" |

Workflow di disaster recovery dei volumi

Il workflow di disaster recovery del volume include l'attivazione del volume di destinazione, la configurazione del volume di destinazione per l'accesso ai dati e la riattivazione del volume di origine originale.



Sono disponibili ulteriori informazioni per aiutarti a gestire le relazioni di disaster recovery a livello di volume e altri metodi di disaster recovery per proteggere la disponibilità delle tue risorse di dati.

- [Backup del volume con SnapVault](#)

Descrive come configurare rapidamente le relazioni dei vault di backup tra volumi che si trovano in diversi cluster ONTAP.

- [Gestione del ripristino dei volumi con SnapVault](#)

Descrive come ripristinare rapidamente un volume da un vault di backup in ONTAP.

Attivare il volume di destinazione

Quando il volume di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline, è necessario attivare il volume di destinazione per fornire l'accesso ai dati fino a quando non si ripristinino i dati sul volume di origine. L'attivazione comporta l'interruzione dei futuri trasferimenti di dati di SnapMirror e l'interruzione della relazione di SnapMirror.

Verificare lo stato del volume di origine

Quando il volume di origine non è disponibile, è necessario verificare che il volume di origine sia offline e quindi identificare il volume di destinazione che deve essere attivato per fornire l'accesso ai dati.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Accedere alla finestra **Volumes**.
2. Selezionare il volume di origine, quindi verificare che il volume di origine sia offline.
3. Identificare il volume di destinazione nella relazione SnapMirror.
 - A partire da ONTAP 9.3: Fare doppio clic sul volume di origine per visualizzare i dettagli, quindi fare clic su **PROTECTION** per identificare il volume di destinazione nella relazione di SnapMirror e il nome della SVM che contiene il volume.

| Health | Destination SVM | Destination Volume | Destination Clu... | Relationship... | Transfer S... | Type | Lag Time | Policy |
|--------|-----------------|--------------------|--------------------|-----------------|---------------|----------------------|-----------|-------------------|
| ✓ | svm2 | vol_mirror_src_dst | cluster2 | Snapmirrored | Idle | Version-Flexible ... | 45 min(s) | MirrorAllSnaps... |

- ONTAP 9.2 o versione precedente: Fare clic sulla scheda **protezione dati** nella parte inferiore della pagina volumi per identificare il volume di destinazione nella relazione SnapMirror e il nome della SVM che contiene il volume.

| Name | Aggregate | Status | Thin Pro... | % Used | Availabi... | Total Sp... | Storage ... | Is Volu... | Encrypted |
|-------------------|-----------|---------|-------------|--------|-------------|-------------|-------------|------------|-----------|
| svm1_svm1_root... | aggr2 | Online | No | 5 | 970.48 MB | 1 GB | Disabled | No | No |
| svm1_vol123_vault | aggr2 | Online | No | 5 | 121.35 MB | 128.02 MB | Enabled | No | No |
| Vol1 | aggr3 | Offline | -NA- | -NA- | -NA- | -NA- | Disabled | No | No |
| svm2_root | aggr1 | Online | No | 5 | 971.12 MB | 1 GB | Disabled | No | No |

| Destination St... | Destination Vo... | Is Healthy | Relationship St... | Transfer Status | Type | Lag Time | Policy |
|-------------------|-------------------|------------|--------------------|-----------------|--------|----------------------|-----------|
| svm1 | vol1 | Yes | Snapmirrored | Idle | Mirror | 7 day(s) 12 hr(s)... | DPDefault |

Details | Space Allocation | Snapshot Copies | Storage Efficiency | **Data Protection** | Volume Move Det | Performance

Interrompere la relazione di SnapMirror

Per attivare il volume di destinazione, è necessario interrompere e interrompere la relazione di SnapMirror. Dopo la disattivazione, i futuri trasferimenti di dati SnapMirror vengono disattivati.

Prima di iniziare

Il volume di destinazione deve essere montato sullo spazio dei nomi SVM di destinazione.

A proposito di questa attività

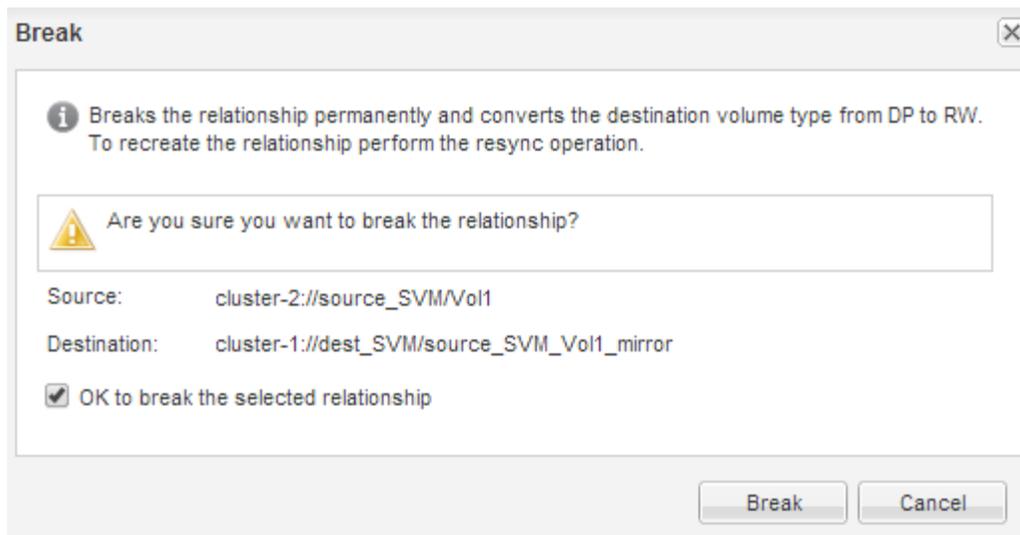
È necessario eseguire questa attività dal cluster **destination**.

Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione di SnapMirror tra i volumi di origine e di destinazione.
3. Fare clic su **Operations > Quiesce** per disattivare i trasferimenti futuri di dati.
4. Selezionare la casella di controllo di conferma, quindi fare clic su **Quiesce**.

L'operazione di quiesce potrebbe richiedere del tempo; non è necessario eseguire altre operazioni sulla relazione SnapMirror fino a quando lo stato del trasferimento non viene visualizzato come *Quiesced*.

5. Fare clic su **operazioni > interruzione**.
6. Selezionare la casella di controllo di conferma, quindi fare clic su **Interrompi**.



La relazione di SnapMirror è stata stabilita **Broken Off** stato.

| Source Sto. | Source Vol. | Destinatio | Destinatio | Is Healthy | Relationship | Transfer St. | Relationship | Lag Time | Policy Name | Policy Type |
|-------------|-------------|----------------|------------|------------|-------------------|--------------|--------------|-----------|-------------|--------------|
| svm1 | svm1_root | svm1_svm1_r... | svm2 | Yes | Snapmirrored | Idle | Mirror | 26 min(s) | DPDefault | Asynchronous |
| svm1 | vol1 | svm1_vol1_m... | svm2 | Yes | Broken Off | Idle | Mirror | None | DPDefault | Asynchronous |

| | | | | | |
|-----------------------|-----------------------|----------------------------|-------------------|----------------------------|--|
| Source Location: | svm1.vol1 | Is Healthy: | Yes | Transfer Status: | Idle |
| Destination Location: | svm2:svm1_vol1_mirror | Relationship State: | Broken Off | Current Transfer Type: | None |
| Source Cluster: | cluster-1 | Network Compression Ratio: | Not Applicable | Current Transfer Error: | None |
| Destination Cluster: | cluster-1 | | | Last Transfer Error: | None |
| Transfer Schedule: | hourly | | | Last Transfer Type: | Update |
| Data Transfer Rate: | Unlimited | | | Latest Snapshot Timestamp: | 02/22/2017 13:05:00 |
| Lag Time: | None | | | Latest Snapshot Copy: | snapmirror.9b4dae7c-e6d0-11e6-b44a-00a0981a1bda_2149622820_2017- |

Verificare lo stato del volume di destinazione

Una volta terminata la relazione SnapMirror, verificare che il volume di destinazione disponga dell'accesso in lettura/scrittura e che le impostazioni del volume di destinazione corrispondano a quelle del volume di origine.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **destination**.

Fasi

1. Accedere alla finestra **Volumes**.
2. Selezionare il volume di destinazione dall'elenco **Volumes**, quindi verificare che il tipo di volume di destinazione sia **rw**, che indica l'accesso in lettura/scrittura.
3. Verificare che le impostazioni del volume, ad esempio thin provisioning, deduplica, compressione e crescita automatica sul volume di destinazione corrispondano alle impostazioni del volume di origine.

È possibile utilizzare le informazioni sulle impostazioni del volume annotate dopo la creazione della relazione SnapMirror per verificare le impostazioni del volume di destinazione.

4. Se le impostazioni del volume non corrispondono, modificare le impostazioni del volume di destinazione come richiesto:

- a. Fare clic su **Edit** (Modifica).
- b. Modificare le impostazioni generali, le impostazioni di efficienza dello storage e le impostazioni avanzate per l'ambiente in uso, in base alle esigenze.
- c. Fare clic su **Save and Close** (Salva e chiudi).

Edit Volume

General | Storage Efficiency | Advanced

Name:

Security style:

Configure UNIX permissions (Optional)

| | Read | Write | Execute |
|--------|-------------------------------------|-------------------------------------|-------------------------------------|
| Owner | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Group | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Others | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Thin Provisioned

When a volume is thin provisioned, space for the volume is not allocated in advance. Instead, space is allocated as data is written to the volume. The unused aggregate space is available to other thin provisioned volumes and LUNs.

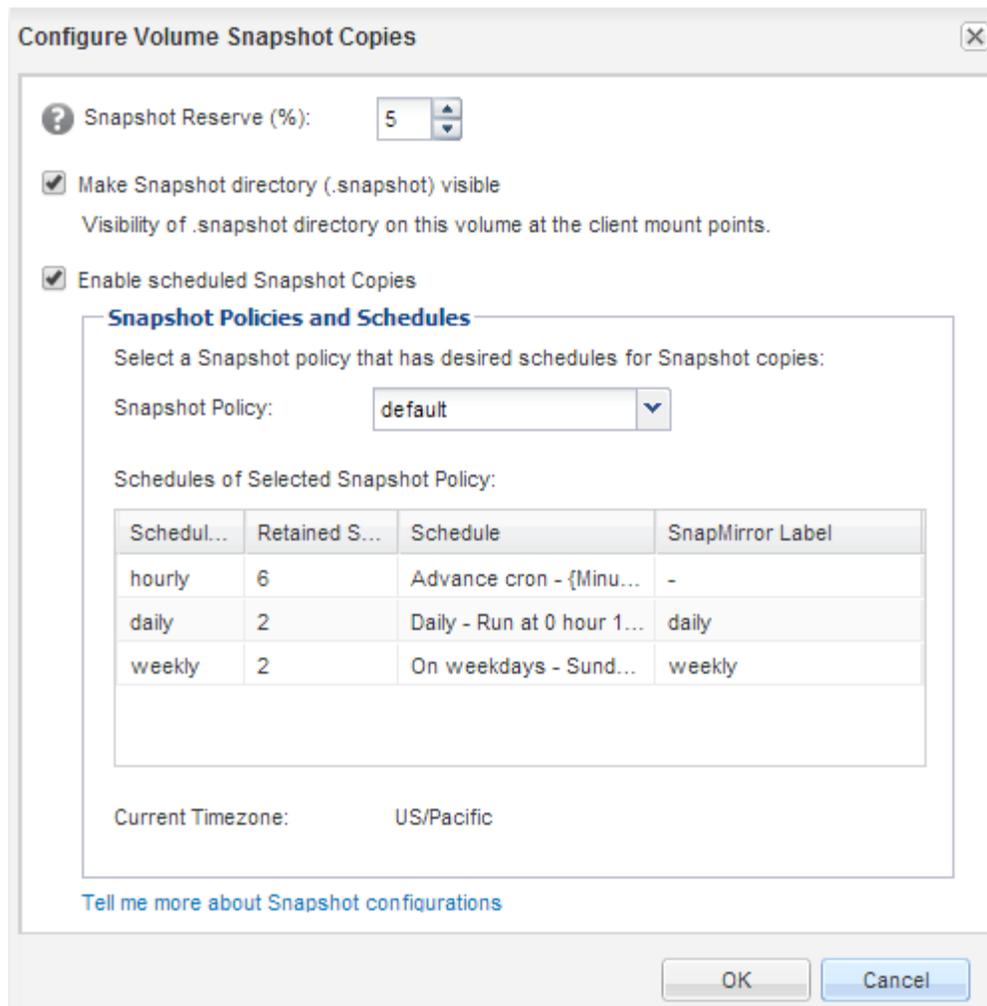
[Tell me more about Thin Provisioning](#)

Save Save and Close Cancel

- d. Verificare che le colonne nell'elenco **volumi** siano aggiornate con i valori appropriati.
5. Attivare la creazione di una copia Snapshot per il volume di destinazione.
- a. A seconda della versione di ONTAP in uso, accedere alla pagina **Configura copie snapshot del volume** in uno dei seguenti modi:

A partire da ONTAP 9.3: Selezionare il volume di destinazione, quindi fare clic su **azioni > Gestisci snapshot > Configura**.

ONTAP 9.2 o versione precedente: Selezionare il volume di destinazione, quindi fare clic su **copie Snapshot > Configura**.
 - b. Selezionare la casella di controllo **Enable scheduled Snapshot copies** (Abilita copie Snapshot pianificate), quindi fare clic su **OK**.



Configurare il volume di destinazione per l'accesso ai dati

Dopo aver attivato il volume di destinazione, è necessario configurare il volume per l'accesso ai dati. I client NAS e GLI host SAN possono accedere ai dati dal volume di destinazione fino alla riattivazione del volume di origine.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **destination**.

Procedura

- Ambiente NAS:
 - a. Montare i volumi NAS nello spazio dei nomi utilizzando lo stesso percorso di giunzione in cui è stato montato il volume di origine nella SVM di origine.
 - b. Applicare gli ACL appropriati alle condivisioni CIFS nel volume di destinazione.
 - c. Assegnare i criteri di esportazione NFS al volume di destinazione.
 - d. Applicare le regole di quota al volume di destinazione.
 - e. Reindirizzare i client al volume di destinazione eseguendo le operazioni necessarie, ad esempio la modifica della risoluzione del nome DNS.
 - f. Rimontare le condivisioni NFS e CIFS sui client.

- Ambiente SAN:
 - a. Mappare le LUN al gruppo iniziatore appropriato per rendere le LUN nel volume disponibili per i client SAN.
 - b. Per iSCSI, creare sessioni iSCSI dagli iniziatori host SAN alle LIF SAN.
 - c. Sul client SAN, eseguire una nuova scansione dello storage per rilevare i LUN connessi.

Cosa fare in seguito

È necessario risolvere il problema che ha causato l'indisponibilità del volume di origine. Quando possibile, è necessario riportare il volume di origine in linea, quindi risincronizzare e riattivare il volume di origine.

Informazioni correlate

["Centro documentazione di ONTAP 9"](#)

Riattivare il volume di origine

Quando il volume di origine diventa disponibile, è necessario risincronizzare i dati dal volume di destinazione al volume di origine, aggiornare le eventuali modifiche dopo l'operazione di risincronizzazione e attivare il volume di origine.

Risincronizzare il volume di origine

Quando il volume di origine è in linea, è necessario risincronizzare i dati tra il volume di destinazione e il volume di origine per replicare i dati più recenti dal volume di destinazione.

Prima di iniziare

Il volume di origine deve essere online.

A proposito di questa attività

È necessario eseguire l'attività dal cluster **destination**.

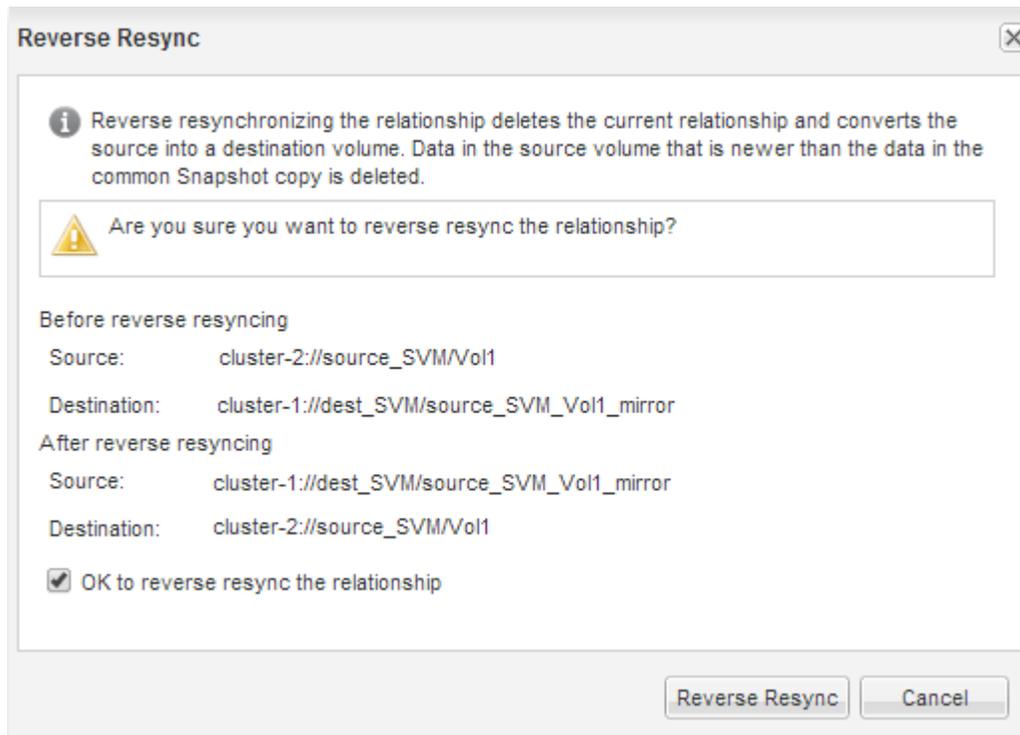
L'immagine seguente mostra che i dati vengono replicati dal volume di destinazione attivo al volume di origine di sola lettura:



Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione di SnapMirror tra i volumi di origine e di destinazione.
3. Prendere nota della pianificazione del trasferimento e del criterio configurato per la relazione SnapMirror.

4. Fare clic su **operazioni > risincronizzazione inversa**.
5. Selezionare la casella di controllo di conferma, quindi fare clic su **Reverse Resync** (risincronizzazione inversa).



A partire da ONTAP 9.3, il criterio SnapMirror della relazione è impostato su `MirrorAllSnapshots` e la pianificazione mirror è impostata su `None`.

Se si utilizza ONTAP 9.2 o versioni precedenti, il criterio SnapMirror della relazione viene impostato su `DPDefault` e la pianificazione mirror è impostata su `None`.

6. Nel cluster di origine, specificare un criterio e una pianificazione SnapMirror che corrispondano alla configurazione di protezione della relazione SnapMirror originale:
 - a. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
 - b. Selezionare la relazione di SnapMirror tra il volume di origine risincronizzato e il volume di destinazione, quindi fare clic su **Edit** (Modifica).
 - c. Selezionare il criterio e la pianificazione di SnapMirror, quindi fare clic su **OK**.

Aggiornare il volume di origine

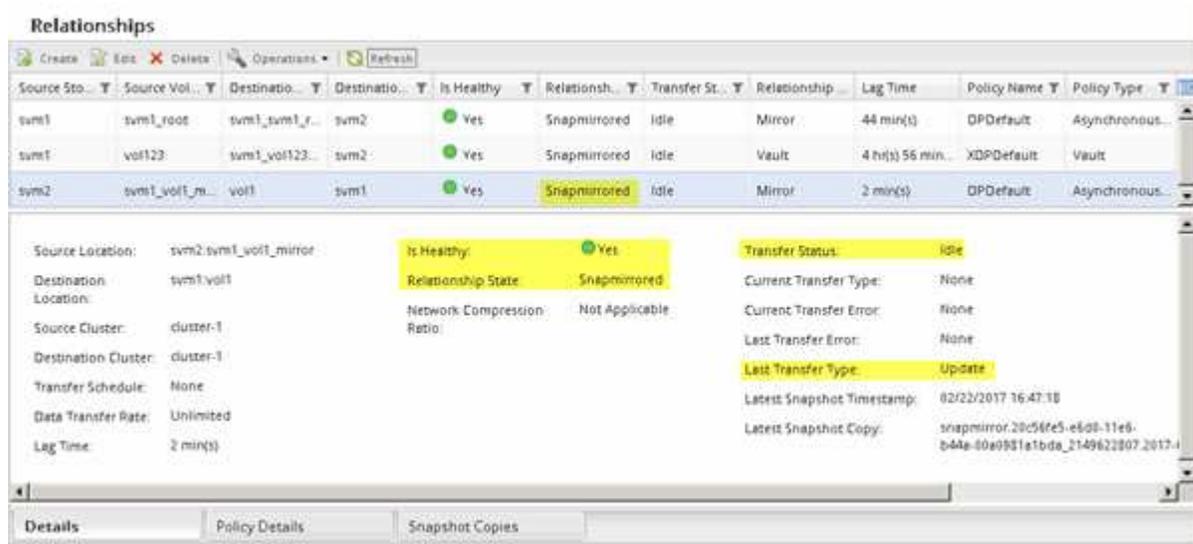
Dopo aver risincronizzato il volume di origine, è possibile assicurarsi che tutte le modifiche più recenti siano aggiornate sul volume di origine prima di attivare il volume di origine.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione di SnapMirror tra i volumi di origine e di destinazione, quindi fare clic su **Operations > Update**.
3. Eseguire un trasferimento incrementale dalla copia Snapshot comune recente tra i volumi di origine e di destinazione.
 - A partire da ONTAP 9.3: Selezionare l'opzione **come da policy**.
 - ONTAP 9.2 o versioni precedenti: Selezionare l'opzione **on demand**.
4. **Opzionale:** selezionare **limita larghezza di banda di trasferimento a** per limitare la larghezza di banda di rete utilizzata per i trasferimenti, quindi specificare la velocità massima di trasferimento.
5. Fare clic su **Aggiorna**.
6. Verificare che lo stato del trasferimento sia `Idle` e l'ultimo tipo di trasferimento è `Update` Nella scheda **Dettagli**.



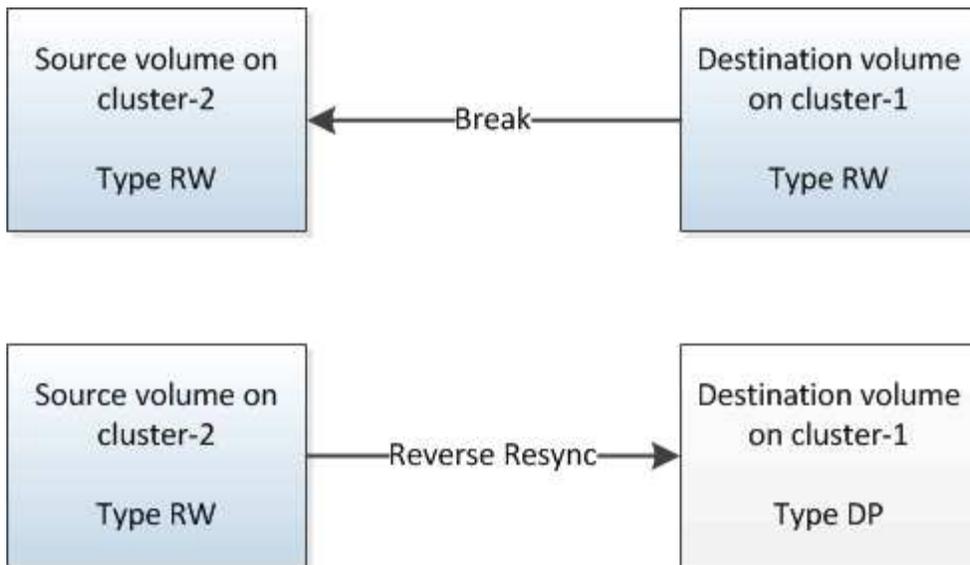
Riattivare il volume di origine

Dopo aver risincronizzato i dati dal volume di destinazione al volume di origine, è necessario attivare il volume di origine interrompendo la relazione SnapMirror. Quindi, risincronizzare il volume di destinazione per proteggere il volume di origine riattivato.

A proposito di questa attività

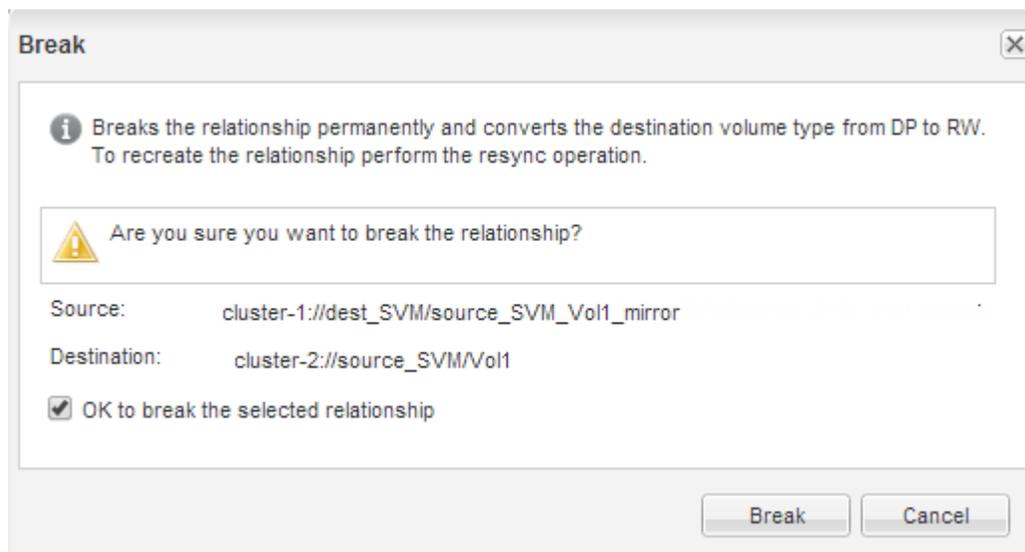
Sia le operazioni di interruzione che di risincronizzazione inversa vengono eseguite dal cluster **source**.

L'immagine seguente mostra che i volumi di origine e di destinazione vengono letti/scritti quando si rompe la relazione SnapMirror. Dopo l'operazione di risincronizzazione inversa, i dati vengono replicati dal volume di origine attivo al volume di destinazione di sola lettura.

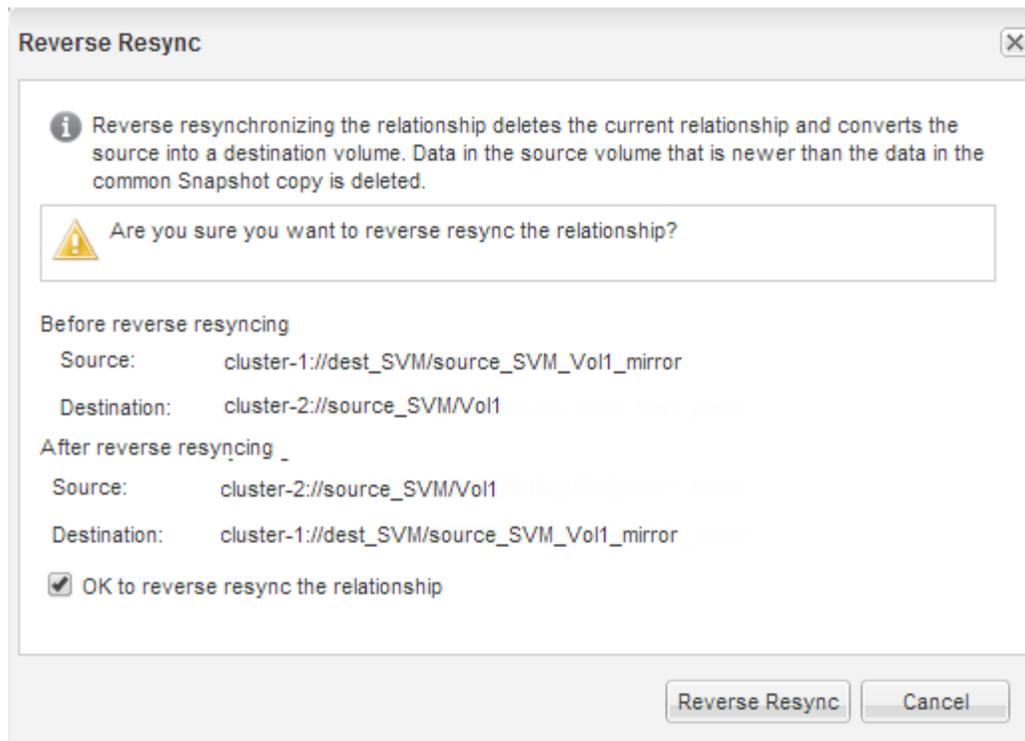


Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione di SnapMirror tra i volumi di origine e di destinazione.
3. Fare clic su **operazioni > Quiesce**.
4. Selezionare la casella di controllo di conferma, quindi fare clic su **Quiesce**.
5. Fare clic su **operazioni > interruzione**.
6. Selezionare la casella di controllo di conferma, quindi fare clic su **Interrompi**.



7. Fare clic su **operazioni > risincronizzazione inversa**.
8. Selezionare la casella di controllo di conferma, quindi fare clic su **Reverse Resync** (risincronizzazione inversa).



A partire da ONTAP 9.3, il criterio SnapMirror della relazione è impostato su MirrorAllSnapshots La pianificazione di SnapMirror è impostata su None.

Se si utilizza ONTAP 9.2 o versioni precedenti, il criterio SnapMirror della relazione viene impostato su DPDefault La pianificazione di SnapMirror è impostata su None.

9. Accedere al volume di origine nella pagina Volumes (volumi) e verificare che la relazione SnapMirror creata sia elencata e che lo stato della relazione sia Snapmirrored.
10. Nel cluster di destinazione, specificare un criterio e una pianificazione SnapMirror che corrispondano alla configurazione di protezione della relazione SnapMirror originale per la nuova relazione SnapMirror:
 - a. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
 - b. Selezionare la relazione di SnapMirror tra i volumi di origine riattivati e quelli di destinazione, quindi fare clic su **Edit** (Modifica).
 - c. Selezionare il criterio e la pianificazione di SnapMirror, quindi fare clic su **OK**.

Risultati

Il volume di origine dispone di accesso in lettura/scrittura ed è protetto dal volume di destinazione.

Preparazione al disaster recovery dei volumi

Panoramica sulla preparazione del disaster recovery dei volumi

È possibile proteggere rapidamente un volume di origine su un cluster Peered ONTAP in preparazione al disaster recovery. È consigliabile utilizzare questa procedura se si desidera configurare e monitorare le relazioni di SnapMirror tra i cluster peered per il

disaster recovery dei volumi e non è necessario un background concettuale elevato per le attività.

SnapMirror offre una protezione dei dati a livello di blocco e asincrona pianificata. SnapMirror replica le copie Snapshot e può replicare i volumi NAS o SAN su cui vengono eseguite la deduplica, la compressione dei dati o entrambi, inclusi i volumi contenenti qtree e LUN. Le informazioni di configurazione di SnapMirror sono memorizzate in un database che ONTAP replica in tutti i nodi del cluster.

Utilizzare questa procedura se si desidera creare relazioni SnapMirror per il disaster recovery a livello di volume nel modo seguente:

- Stai lavorando con cluster che eseguono ONTAP 9.
- Sei un amministratore del cluster.
- Sono state configurate la relazione peer del cluster e la relazione peer SVM.

["Configurazione del peering di cluster e SVM"](#)

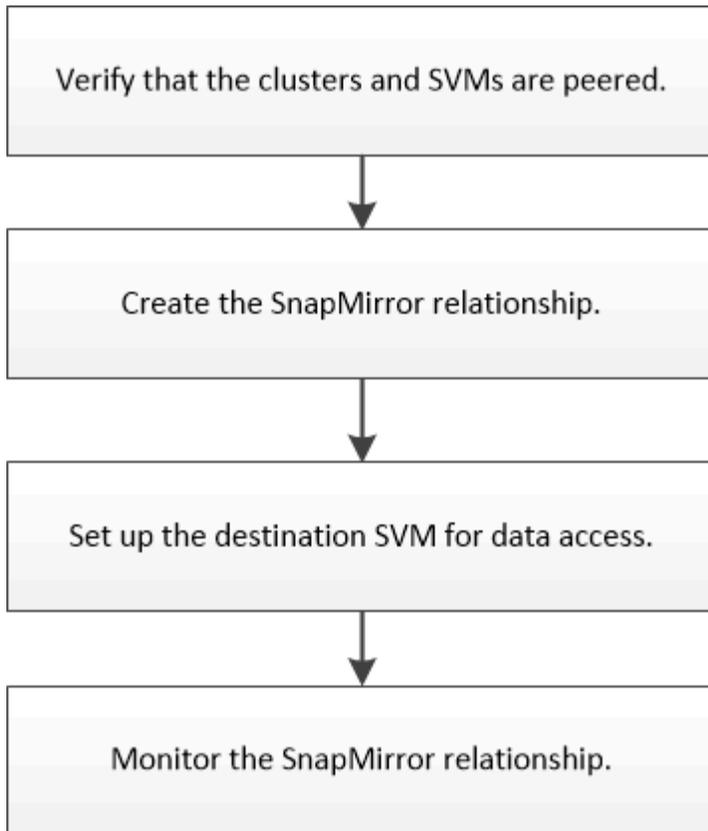
- La licenza SnapMirror è stata attivata sia sul cluster di origine che su quello di destinazione.
- Si desidera utilizzare le policy e le pianificazioni predefinite e non creare policy personalizzate.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili (ONTAP 9.7 e versioni precedenti).

Altri modi per farlo in ONTAP

| Per eseguire queste attività con... | Fare riferimento a... |
|---|---|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | "Preparazione per il mirroring e il vaulting" |
| L'interfaccia della riga di comando di ONTAP | "Creazione di una relazione peer del cluster (ONTAP 9.3 e versioni successive)" |

Workflow di preparazione del disaster recovery dei volumi

La preparazione dei volumi per il disaster recovery implica la verifica della relazione peer del cluster, la creazione della relazione SnapMirror tra i volumi residenti sui cluster peered, la configurazione della SVM di destinazione per l'accesso ai dati e il monitoraggio periodico della relazione SnapMirror.



È disponibile ulteriore documentazione per consentire l'attivazione del volume di destinazione per testare la configurazione del disaster recovery o in caso di disastro. È inoltre possibile ottenere ulteriori informazioni su come riattivare il volume di origine dopo il disastro.

Disaster recovery dei volumi

+ Descrive come attivare rapidamente un volume di destinazione dopo un disastro e riattivare il volume di origine in ONTAP.

Verificare la relazione peer del cluster e la relazione peer SVM

Prima di configurare un volume per il disaster recovery, è necessario verificare che i cluster di origine e di destinazione siano peering e che stiano comunicando tra loro attraverso la relazione peer.

Procedura

- Se si utilizza ONTAP 9.3 o versione successiva, attenersi alla seguente procedura per verificare la relazione peer del cluster e la relazione peer SVM:
 - a. Fare clic su **Configuration > Cluster Peers**.
 - b. Verificare che il cluster peered sia autenticato e disponibile.

| <input type="checkbox"/> Create <input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Refresh <input type="checkbox"/> Manage SVM Permissions | | | | | |
|--|--------------|-----------------------|-----------------------|--|-----------------------|
| <input checked="" type="checkbox"/> Peer Cluster | Availability | Authentication Status | Local Cluster IPspace | Peer Cluster Intercluster IP Addresses | Last Updated Time |
| <input checked="" type="checkbox"/> cluster2 | Available | OK | Default | 10.237.213.119, 10.237.213.127 | Nov 27, 2017, 2:13 PM |

- c. Fare clic su **Configuration > SVM Peers**.

- d. Verificare che la SVM di destinazione sia in peering con la SVM di origine.
- Se si utilizza ONTAP 9.2 o versioni precedenti, attenersi alla seguente procedura per verificare la relazione peer del cluster e la relazione peer SVM:
 - a. Fare clic sulla scheda **configurazioni**.
 - b. Nel riquadro **Cluster Details**, fare clic su **Cluster Peers**.
 - c. Verificare che il cluster peered sia autenticato e disponibile.

| Peer Cluster | Availability | Authentication Status |
|--------------|--------------|-----------------------|
| cluster-1 | available | ok |

- d. Fare clic sulla scheda **SVM** e selezionare la SVM di origine.
- e. Nell'area **Peer Storage Virtual Machines** (macchine virtuali di storage peer), verificare che la SVM di destinazione sia peer con la SVM di origine.

Se in quest'area non viene visualizzata alcuna SVM peered, è possibile creare la relazione peer SVM durante la creazione della relazione SnapMirror.

[Creazione della relazione SnapMirror \(ONTAP 9.2 o versione precedente\)](#)

Creazione della relazione SnapMirror (a partire da ONTAP 9.3)

È necessario creare una relazione SnapMirror tra il volume di origine su un cluster e il volume di destinazione sul cluster peered per la replica dei dati per il disaster recovery.

Prima di iniziare

- L'aggregato di destinazione deve disporre di spazio disponibile.
- Entrambi i cluster devono essere configurati e configurati in modo appropriato per soddisfare i requisiti del proprio ambiente in termini di accesso utente, autenticazione e accesso client.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Fare clic su **Storage > Volumes**.
2. Selezionare il volume per il quale si desidera creare una relazione mirror, quindi fare clic su **azioni > Protect**.
3. Nella sezione **tipo di relazione**, selezionare **Mirror** dall'elenco a discesa **tipo di relazione**.
4. Nella pagina **Volumes: Protect Volumes**, fornire le seguenti informazioni:
 - a. Selezionare **Mirror** come tipo di relazione.
 - b. Selezionare il cluster di destinazione, la SVM di destinazione e il suffisso per il nome del volume di destinazione.

Solo le SVM in peering e le SVM consentite sono elencate nelle SVM di destinazione.

- c. Fare clic su .
- d. Nella finestra di dialogo **Opzioni avanzate**, verificare che `MirrorAllSnapshots` è impostato come criterio di protezione.

`DPDefault` e `MirrorLatest` Sono gli altri criteri di protezione predefiniti disponibili per le relazioni `SnapMirror`.

- e. Selezionare un programma di protezione.

Per impostazione predefinita, il `hourly` pianificazione selezionata.

- f. Verificare che sia selezionato **Sì** per inizializzare la relazione `SnapVault`.

Tutte le relazioni di protezione dei dati vengono inizializzate per impostazione predefinita. L'inizializzazione della relazione `SnapMirror` garantisce che il volume di destinazione disponga di una linea di base per iniziare a proteggere il volume di origine.

- g. Fare clic su **Apply** (Applica) per salvare le modifiche.

Advanced Options ✕

Protection Policy MirrorAllSnapshots ▼

| SnapMirror Labels | Retention Count |
|----------------------|-----------------|
| sm_created | 1 |
| all_source_snapshots | 1 |

Protection Schedule hourly ▼

Every hour at 05 minute(s)

i Initialize Protection Yes No

i SnapLock for SnapVault SnapVault SnapLock for SnapVault is not supported for the selected destination or the selected relationship type.

i FabricPool There is no FabricPool assigned to the destination SVM.

Apply

5. Fare clic su **Save** (Salva) per creare la relazione `SnapMirror`.
6. Verificare che lo stato della relazione di `SnapMirror` sia in `Snapmirrored` stato.
- a. Accedere alla finestra **Volumes**, quindi selezionare il volume per il quale è stata creata la relazione `SnapMirror`.
- b. Fare doppio clic sul volume per visualizzare i dettagli del volume, quindi fare clic su **PROTECTION** per

visualizzare lo stato di protezione dei dati del volume.

Volume: vol_mirror_src

Overview Snapshots Copies Data Protection Storage Efficiency Performance

| Health | Destination SVM | Destination Volume | Destination Clu... | Relationship... | Transfer S... | Type | Lag Time | Policy |
|--------|-----------------|--------------------|--------------------|-----------------|---------------|---------------------|----------|------------------|
| | svm2 | vol_mirror_src_dst | cluster2 | SnapMirrored | Idle | Version-Flexibil... | None | MirrorAllSnap... |

Cosa fare in seguito

È necessario prendere nota delle impostazioni del volume di origine, ad esempio thin provisioning, deduplica, compressione e crescita automatica. È possibile utilizzare queste informazioni per verificare le impostazioni del volume di destinazione quando si rompe la relazione SnapMirror.

Creazione della relazione SnapMirror (ONTAP 9.2 o versione precedente)

È necessario creare una relazione SnapMirror tra il volume di origine su un cluster e il volume di destinazione sul cluster peered per la replica dei dati per il disaster recovery.

Prima di iniziare

- È necessario disporre del nome utente e della password dell'amministratore del cluster per il cluster di destinazione.
- L'aggregato di destinazione deve disporre di spazio disponibile.
- Entrambi i cluster devono essere configurati e configurati in modo appropriato per soddisfare i requisiti del proprio ambiente in termini di accesso utente, autenticazione e accesso client.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Fare clic su **Storage > SVM**.
2. Selezionare la SVM, quindi fare clic su **SVM Settings** (Impostazioni SVM).
3. Fare clic sulla scheda **Volumes** (volumi).
4. Selezionare il volume per il quale si desidera creare una relazione mirror, quindi fare clic su **Protect**.

Viene visualizzata la finestra Create Protection Relationship (Crea relazione di protezione).

5. Nella sezione **tipo di relazione**, selezionare **Mirror** dall'elenco a discesa **tipo di relazione**.
6. Nella sezione **Destination Volume** (Volume di destinazione), selezionare il cluster peered.
7. Specificare la SVM per il volume di destinazione:

| Se SVM è... | Quindi... |
|-------------|---|
| Con peering | Selezionare la SVM in peered dall'elenco. |

| Se SVM è... | Quindi... |
|-------------|---|
| Non peered | a. Selezionare la SVM. b. Fare clic su Authenticate . c. Immettere le credenziali dell'amministratore del cluster in peered, quindi fare clic su Create (Crea). |

8. Creare un nuovo volume di destinazione:

- Selezionare l'opzione **New Volume** (nuovo volume).
- Utilizzare il nome del volume predefinito o specificare un nuovo nome di volume.
- Selezionare l'aggregato di destinazione.

Destination Volume

Cluster:

Storage Virtual Machine:

Volume: New Volume Select Volume

Volume name:

Aggregate:
387.19 GB available (of 390.21 GB)

Space Reserve (optional):

9. Nella sezione **Dettagli configurazione**, selezionare **MirrorAllSnapshots** come policy mirror.

DPDefault e MirrorLatest Sono gli altri criteri mirror predefiniti disponibili per le relazioni SnapMirror.

10. Selezionare un programma di protezione dall'elenco dei programmi.

11. Assicurarsi che la casella di controllo **Inizializza relazione** sia selezionata, quindi fare clic su **Crea**.

L'inizializzazione della relazione SnapMirror garantisce che il volume di destinazione disponga di una linea di base per iniziare a proteggere il volume di origine.

Configuration Details

Mirror Policy: [Create Policy](#)
SnapMirror labels: sm_created

Schedule: hourly [Create Schedule](#)
Every hour at 05 minute(s)
 None

Initialize Relationship

La relazione viene inizializzata avviando un trasferimento di base dei dati dal volume di origine al volume di destinazione.

L'operazione di inizializzazione potrebbe richiedere del tempo. La sezione Status (Stato) mostra lo stato di ciascun lavoro.

Create Protection Relationship

Source Volume

Cluster: cluster-1
Storage Virtual Machine: svm1
Volume: svm1_root { Used space 844 KB }

Destination Volume

Cluster: cluster-1
Storage Virtual Machine: svm2
Volume: svm1_svm1_root_mirror

Configuration Details

Mirror Policy: DPDefault
Schedule: hourly

Status

| | |
|-------------------------|--------------------------|
| Create volume | ✔ Completed successfully |
| Create relationship | ✔ Completed successfully |
| Initialize relationship | ✔ Started successfully |

12. Verificare lo stato di relazione della relazione SnapMirror:

- Selezionare il volume per il quale è stata creata la relazione SnapMirror dall'elenco **Volumes**, quindi fare clic su **Data Protection**.
- Nella scheda **Data Protection**, verificare che sia elencata la relazione SnapMirror creata e che lo stato della relazione sia `SnapshotMirrored`.

| Destination Storage Virtual Mach. | Destination Volume | Is Healthy | Relationship State | Transfer Status | Type | Lag Time | Policy |
|-----------------------------------|-----------------------|------------|--------------------|-----------------|--------|-----------|-----------|
| svm2 | svm1_svm1_root_mirror | ✔ Yes | SnapshotMirrored | Idle | Mirror | 13 min(s) | DPDefault |

Cosa fare in seguito

È necessario prendere nota delle impostazioni del volume di origine, ad esempio thin provisioning, deduplica, compressione e crescita automatica. È possibile utilizzare queste informazioni per verificare le impostazioni del volume di destinazione quando si rompe la relazione SnapMirror.

Impostare la SVM di destinazione per l'accesso ai dati

È possibile ridurre al minimo l'interruzione dell'accesso ai dati durante l'attivazione del volume di destinazione impostando le configurazioni richieste, ad esempio LIF, condivisioni CIFS e policy di esportazione per l'ambiente NAS, LIF e gruppi di iniziatori per l'ambiente SAN sulla SVM contenente il volume di destinazione.

A proposito di questa attività

Questa attività deve essere eseguita sul cluster **destination** per la SVM contenente il volume di destinazione.

Procedura

- Ambiente NAS:
 - a. Creare LIF NAS.
 - b. Creare condivisioni CIFS con gli stessi nomi di condivisione utilizzati nell'origine.
 - c. Creare policy di esportazione NFS appropriate.
 - d. Creare le regole di quota appropriate.
- Ambiente SAN:
 - a. Creazione di LIF SAN.
 - b. **Opzionale:** configurare i portset.
 - c. Configurare i gruppi di iniziatori.
 - d. Per FC, eseguire l'area degli switch FC per consentire ai client SAN di accedere alle LIF.

Cosa fare in seguito

Se sono state apportate modifiche alla SVM contenente il volume di origine, è necessario replicarle manualmente sulla SVM contenente il volume di destinazione.

Informazioni correlate

["Centro documentazione di ONTAP 9"](#)

Monitorare lo stato dei trasferimenti di dati SnapMirror

È necessario monitorare periodicamente lo stato delle relazioni di SnapMirror per garantire che i trasferimenti di dati di SnapMirror si verifichino secondo la pianificazione specificata.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **destination**.

Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione di SnapMirror tra i volumi di origine e di destinazione, quindi verificare lo stato nella scheda **Dettagli** inferiore.

La scheda Dettagli visualizza lo stato di salute della relazione SnapMirror e mostra gli errori di trasferimento e il ritardo.

- Deve essere visualizzato il campo `is healthy` `Yes`.

Per la maggior parte degli errori di trasferimento dei dati SnapMirror, viene visualizzato il campo `No`. In alcuni casi di guasto, tuttavia, il campo continua a essere visualizzato `Yes`. Controllare gli errori di trasferimento nella sezione Dettagli per assicurarsi che non si siano verificati errori di trasferimento dei dati.

- Deve essere visualizzato il campo Relationship state (Stato relazione) Snapmirrored.
- Il tempo di ritardo non deve superare l'intervallo di pianificazione del trasferimento.

Ad esempio, se la pianificazione del trasferimento è oraria, il ritardo non deve superare un'ora.

È necessario risolvere eventuali problemi nelle relazioni di SnapMirror.

["Report tecnico di NetApp 4015: Configurazione e Best practice di SnapMirror per ONTAP 9.1, 9.2"](#)

| | | | | | |
|-----------------------|----------------------------|----------------------------|----------------|----------------------------|--|
| Source Location: | source_SVM/Vol1 | Is Healthy: | Yes | Transfer Status: | Idle |
| Destination Location: | dest_SVM/source_SVM_Vol... | Relationship State: | Snapmirrored | Current Transfer Type: | None |
| Source Cluster: | cluster-2 | Network Compression Ratio: | Not Applicable | Current Transfer Error: | None |
| Destination Cluster: | cluster-1 | | | Last Transfer Error: | None |
| Transfer Schedule: | hourly | | | Last Transfer Type: | Initialize |
| Data Transfer Rate: | Unlimited | | | Latest Snapshot Timestamp: | 09/18/2014 23:42:24 |
| Lag Time: | None | | | Latest Snapshot Copy: | snapmirror.3e51ed5f-31a3-11e4-98c7-005056974d2d_2147484888.2014-09-18_233529 |

Backup del volume con SnapVault

Panoramica del backup del volume con SnapVault

È possibile configurare rapidamente le relazioni di backup di SnapVault tra volumi che si trovano in cluster diversi. Il backup di SnapVault contiene una serie di copie di backup di sola lettura, che si trovano su un volume di destinazione che è possibile utilizzare per il ripristino dei dati in caso di danneggiamento o perdita dei dati.

Utilizzare questa procedura se si desidera creare relazioni di backup SnapVault per i volumi nel modo seguente:

- Stai lavorando con cluster che eseguono ONTAP 9.
- Sei un amministratore del cluster.
- Sono state configurate la relazione peer del cluster e la relazione peer SVM.

["Configurazione del peering di cluster e SVM"](#)

- Dopo aver aggiornato tutti i nodi del cluster alla stessa versione di ONTAP 9, è necessario attivare la licenza SnapMirror o SnapVault.
- Si desidera utilizzare i criteri e le pianificazioni di protezione predefiniti e non creare policy personalizzate.
- Non si desidera eseguire il backup dei dati per un singolo file o ripristino del LUN.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Non si desidera leggere un sacco di background concettuale.
- Si desidera utilizzare Gestione sistema, non l'interfaccia della riga di comando di ONTAP o uno strumento di scripting automatico.
- Si desidera utilizzare l'interfaccia classica di Gestione sistema per ONTAP 9.7 e versioni precedenti, non l'interfaccia utente di Gestione sistema di ONTAP per ONTAP 9.7 e versioni successive.

Se questi presupposti non sono corretti per la situazione o se si desidera ottenere informazioni di base più concettuali, si dovrebbe visualizzare la seguente risorsa:

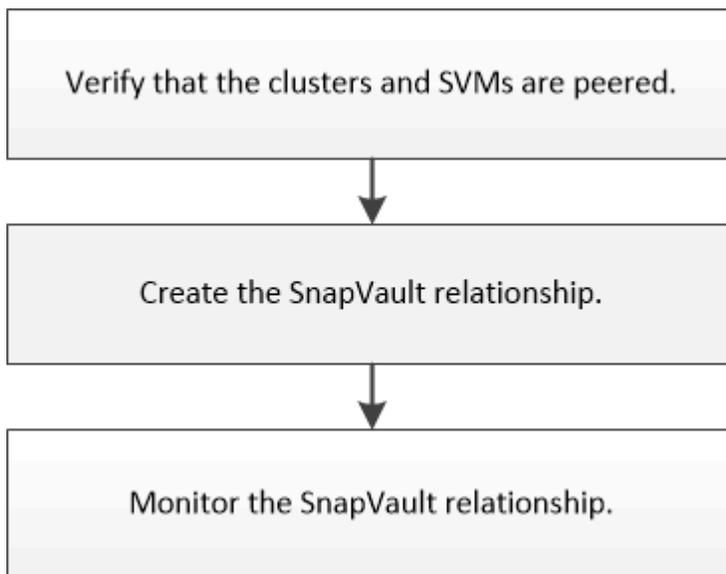
["Report tecnico di NetApp 4183: Best Practice SnapVault"](#)

Altri modi per farlo in ONTAP

| Per eseguire queste attività con... | Guarda questo contenuto... |
|---|---|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | "Configurare mirror e vault" |
| L'interfaccia della riga di comando di ONTAP | "Creare una relazione di replica" |

Workflow di configurazione del backup di SnapVault

La configurazione di una relazione di backup SnapVault include la verifica della relazione peer del cluster, la creazione della relazione SnapVault tra i volumi di origine e di destinazione e il monitoraggio della relazione SnapVault.



È disponibile ulteriore documentazione per il ripristino dei dati da un volume di destinazione per verificare i dati di cui è stato eseguito il backup o in caso di perdita del volume di origine.

- [Gestione del ripristino dei volumi con SnapVault](#)

Descrive come ripristinare rapidamente un volume da un backup SnapVault in ONTAP

Verificare la relazione peer del cluster e la relazione peer SVM

Prima di configurare un volume per la protezione dei dati utilizzando la tecnologia SnapVault, è necessario verificare che il cluster di origine e il cluster di destinazione siano peering e che comunichi tra loro attraverso la relazione peer. È inoltre necessario verificare che la SVM di origine e la SVM di destinazione siano collegate in peering e che comunichi tra loro attraverso la relazione peer.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

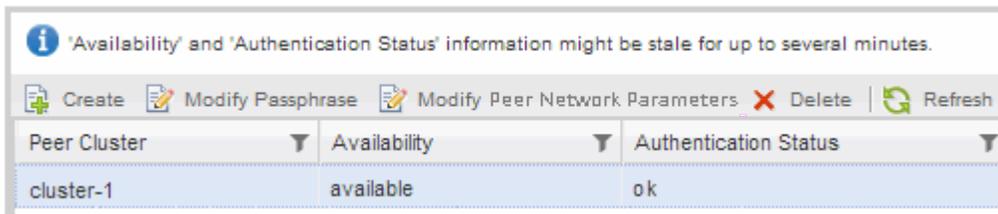
Procedura

- Se si utilizza ONTAP 9.3 o versione successiva, attenersi alla seguente procedura per verificare la relazione peer del cluster e la relazione peer SVM:
 - a. Fare clic su **Configuration > Cluster Peers**.
 - b. Verificare che il cluster peered sia autenticato e disponibile.



| Peer Cluster | Availability | Authentication Status | Local Cluster IPspace | Peer Cluster Intercluster IP Addresses | Last Updated Time |
|--|--------------|-----------------------|-----------------------|--|-----------------------|
| <input checked="" type="checkbox"/> cluster2 | Available | Ok | Default | 10.237.213.119, 10.237.213.127 | Nov 27, 2017, 2:13 PM |

- c. Fare clic su **Configuration > SVM Peers**.
 - d. Verificare che la SVM di destinazione sia in peering con la SVM di origine.
- Se si utilizza ONTAP 9.2 o versioni precedenti, attenersi alla seguente procedura per verificare la relazione peer del cluster e la relazione peer SVM:
 - a. Fare clic sulla scheda **configurazioni**.
 - b. Nel riquadro **Cluster Details**, fare clic su **Cluster Peers**.
 - c. Verificare che il cluster peered sia autenticato e disponibile.



'Availability' and 'Authentication Status' information might be stale for up to several minutes.

| Peer Cluster | Availability | Authentication Status |
|--------------|--------------|-----------------------|
| cluster-1 | available | ok |

- d. Fare clic sulla scheda **SVM** e selezionare la SVM di origine.
- e. Nell'area **Peer Storage Virtual Machines** (macchine virtuali di storage peer), verificare che la SVM di destinazione sia peer con la SVM di origine.

Se in quest'area non viene visualizzata alcuna SVM con peering, è possibile creare la relazione peer SVM durante la creazione della relazione SnapVault.

[Creazione della relazione SnapVault \(ONTAP 9.2 o versione precedente\)](#)

Creare una relazione SnapVault (a partire da ONTAP 9.3)

Per creare un backup SnapVault, è necessario creare una relazione SnapVault tra il volume di origine su un cluster e il volume di destinazione sul cluster peered.

Prima di iniziare

- È necessario disporre del nome utente e della password dell'amministratore del cluster per il cluster di destinazione.
- L'aggregato di destinazione deve disporre di spazio disponibile.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Fare clic su **Storage > Volumes**.
2. Selezionare il volume di cui si desidera eseguire il backup, quindi fare clic su **azioni > Protect**.

È inoltre possibile selezionare più volumi di origine e creare relazioni SnapVault con un singolo volume di destinazione.

3. Nella pagina **Volumes: Protect Volumes**, fornire le seguenti informazioni:
 - a. Selezionare **Vault** dall'elenco a discesa **tipo di relazione**.
 - b. Selezionare il cluster di destinazione, la SVM di destinazione e il suffisso per il volume di destinazione.

Solo le SVM in peering e le SVM consentite sono elencate nelle SVM di destinazione.

Il volume di destinazione viene creato automaticamente. Il nome del volume di destinazione è il nome del volume di origine aggiunto al suffisso.

- a. Fare clic su .
- b. Nella finestra di dialogo **Opzioni avanzate**, verificare che l'opzione **criterio di protezione** sia impostata su `XDPDefault`.
- c. Selezionare il programma di protezione*.

Per impostazione predefinita, il `daily` pianificazione selezionata.

- d. Verificare che sia selezionato **Sì** per inizializzare la relazione SnapVault.

Tutte le relazioni di protezione dei dati vengono inizializzate per impostazione predefinita.

- e. Fare clic su **Apply** (Applica) per salvare le modifiche.

Advanced Options



Protection Policy XDPDefault

| SnapMirror Labels | Retention Count |
|-------------------|-----------------|
| daily | 7 |
| weekly | 52 |

Protection Schedule daily

Every Night at 0:10 AM

i Initialize Protection Yes
 No

i SnapLock for SnapVault There are no SnapLock aggregates assigned to the destination SVM.

i FabricPool There is no FabricPool assigned to the destination SVM.

Apply

4. Nella pagina **Volumes: Protect Volumes** (volumi: Protezione volumi), fare clic su **Validate** (convalida) per verificare se i volumi hanno etichette SnapMirror corrispondenti.
5. Fare clic su **Salva** per creare la relazione SnapVault.
6. Verificare che lo stato della relazione SnapVault sia in `Snapmirrored` stato.
 - a. Accedere alla finestra **Volumes**, quindi selezionare il volume di cui è stato eseguito il backup.
 - b. Espandere il volume e fare clic su **PROTECTION** per visualizzare lo stato di protezione dei dati del volume.

Volumes on SVM All SVMs

Volume: vol_src [Back to All volumes](#) [Edit](#) [Cancel](#) [Actions](#) [Refresh](#)

Overview Snapshots Copies **Data Protection** Storage Efficiency Performance

[Refresh](#)

| Health | Destination SVM | Destination Volume | Destination Clu... | Relationsh... | Transfer S... | Type | Lag Time | Policy |
|--------|-----------------|--------------------|--------------------|---------------|---------------|-------|----------|------------|
| | vst | vst_src_dst | cluster1 | Snapmirrored | SBF | Vault | 29 min() | XDPDefault |

Creazione della relazione SnapVault (ONTAP 9.2 o versione precedente)

Per creare un backup SnapVault, è necessario creare una relazione SnapVault tra il volume di origine su un cluster e il volume di destinazione sul cluster peered.

Prima di iniziare

- È necessario disporre del nome utente e della password dell'amministratore del cluster per il cluster di destinazione.

- L'aggregato di destinazione deve disporre di spazio disponibile.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Fare clic su **Storage > SVM**.
2. Selezionare la SVM, quindi fare clic su **SVM Settings** (Impostazioni SVM).
3. Fare clic sulla scheda **Volumes** (volumi).
4. Selezionare il volume di cui si desidera eseguire il backup, quindi fare clic su **Protect** (protezione).
5. Nella finestra di dialogo **Crea relazione di protezione**, selezionare **Vault** dall'elenco a discesa **tipo di relazione**.
6. Nella sezione **Destination Volume** (Volume di destinazione), selezionare il cluster peered.
7. Specificare la SVM per il volume di destinazione:

| Se SVM è... | Quindi... |
|-------------|--|
| Con peering | Selezionare la SVM in peered dall'elenco. |
| Non peered | <ol style="list-style-type: none"> a. Selezionare la SVM. b. Fare clic su Authenticate. c. Immettere le credenziali dell'amministratore del cluster in peered, quindi fare clic su Create (Crea). |

8. Creare un nuovo volume di destinazione:
 - a. Selezionare l'opzione **New Volume** (nuovo volume).
 - b. Utilizzare il nome del volume predefinito o immettere un nuovo nome per il volume.
 - c. Selezionare l'aggregato di destinazione.
 - d. Assicurarsi che la casella di controllo **Enable dedupe** (attiva deduplica) sia selezionata.

Destination Volume

Cluster:

Storage Virtual Machine:

Volume: New Volume Select Volume

Volume name: Aggregate:

Enable dedupe 70.13 GB available (of 70.14 GB)

9. Nella sezione **Dettagli configurazione**, selezionare **XDPDefault** come policy di protezione.
10. Selezionare un programma di protezione dall'elenco dei programmi.
11. Assicurarsi che la casella di controllo **Inizializza relazione** sia selezionata per trasferire la copia Snapshot di base, quindi fare clic su **Crea**

Configuration Details

Vault Policy:
 Snapshot with labels matching: daily, weekly

Schedule: weekly
 Every Sun at 0:15 am
 None

Initialize Relationship

La procedura guidata crea la relazione con la pianificazione e la policy del vault specificate. La relazione viene inizializzata avviando un trasferimento di base dei dati dal volume di origine al volume di destinazione.

La sezione Status (Stato) mostra lo stato di ciascun lavoro.

Create Protection Relationship

Source Volume

Cluster: cluster-1
 Storage Virtual Machine: svm1
 Volume: vol_2 { Used space 292 KB }

Destination Volume

Cluster: cluster-1
 Storage Virtual Machine: vs0
 Volume: svm1_vol_2_vault

Configuration Details

Vault Policy: XDPDefault
 Schedule: weekly

Status

| | |
|-------------------------|--------------------------|
| Create volume | ✓ Completed successfully |
| Enable dedupe | ✓ Completed successfully |
| Create relationship | ✓ Completed successfully |
| Initialize relationship | ✓ Started successfully |

12. Verificare che lo stato di relazione della relazione SnapVault sia in Snapmirrored stato.
 - a. Selezionare il volume dall'elenco Volumes (volumi), quindi fare clic su **Data Protection** (protezione dati).

- b. Nella scheda in basso **Data Protection**, verificare che la relazione SnapMirror creata sia elencata e che lo stato della relazione sia `Snapshotmirrored` e il tipo è `Vault`.

| Name | Aggregate | Status | Thin Provi... | % Used | Available ... | Total Space | Storage Et... | Is Volume ... | Encrypted |
|---------------|-----------|--------|---------------|--------|---------------|-------------|---------------|---------------|-----------|
| svm1_root | aggr1 | Online | No | 5 | 879.56 MB | 1 GB | Disabled | No | No |
| svm2_svm1_... | aggr2 | Online | No | 5 | 121.36 MB | 128.92 MB | Enabled | No | No |
| vol1 | aggr2 | Online | No | 0 | 1017.7 MB | 1 GB | Disabled | No | No |
| vol123 | aggr1 | Online | Yes | 5 | 1.9 GB | 2 GB | Disabled | Yes | No |

| Destination Store... | Destination Volu... | Is Healthy | Relationship State | Transfer Status | Type | Lag Time | Policy |
|----------------------|---------------------|------------|--------------------|-----------------|-------|-------------------|------------|
| svm2 | svm1_vol123_vault | Yes | Snapshotmirrored | Idle | Vault | 4 hr(s) 21 min(s) | XDPDefault |

Details Space Allocation Snapshot Copies Storage Efficiency **Data Protection** Volume Move Deta Performance

Monitorare la relazione SnapVault

È necessario monitorare periodicamente lo stato delle relazioni SnapVault per assicurarsi che venga eseguito il backup dei dati sul volume di destinazione in base alla pianificazione specificata.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **destination**.

Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la relazione SnapVault tra i volumi di origine e di destinazione, quindi verificare lo stato nella scheda **Dettagli** inferiore.

Vengono visualizzati lo stato di salute della relazione SnapVault, gli eventuali errori di trasferimento e il ritardo:

- Deve essere visualizzato il campo `is healthy` `Yes`.

Per la maggior parte degli errori di trasferimento dei dati, viene visualizzato il campo `No`. In alcuni casi di guasto, tuttavia, il campo continua a essere visualizzato `Yes`. Controllare gli errori di trasferimento nella sezione **Dettagli** per assicurarsi che non si siano verificati errori di trasferimento dei dati.

- Deve essere visualizzato il campo `Relationship state` (Stato relazione) `Snapshotmirrored`.
- Il tempo di ritardo non deve superare l'intervallo di pianificazione del trasferimento.

Ad esempio, se la pianificazione del trasferimento è giornaliera, il tempo di ritardo non deve essere superiore a un giorno.

È necessario risolvere eventuali problemi nelle relazioni SnapVault. Le procedure di troubleshooting per le relazioni di SnapMirror sono applicabili anche alle relazioni di SnapVault.

| Source St. | Source V. | Destinati. | Destinati. | Is Healthy | Relations... | Transfer... | Relationshi... | Lag Time | Policy Na... | Policy Type |
|------------|-----------|---------------|------------|------------|---------------|-------------|----------------|-----------------|--------------|----------------------|
| svm1 | svm1_root | svm1_svm1... | svm2 | Yes | Snapmirror... | Idle | Mirror | 33 min(s) | DPDefault | Asynchronous Mirr... |
| svm1 | vol123 | svm1_vol12... | svm2 | Yes | Snapmirror... | Idle | Vault | 4 hr(s) 28 m... | XDPDefault | Vault |

| | | | | | |
|-----------------------|------------------------|----------------------------|----------------|----------------------------|-----------------------|
| Source Location: | svm1:vol123 | Is Healthy: | Yes | Transfer Status: | Idle |
| Destination Location: | svm2:svm1_vol123_vault | Relationship State: | Snapmirrored | Current Transfer Type: | None |
| Source Cluster: | cluster-1 | Network Compression Ratio: | Not Applicable | Current Transfer Error: | None |
| Destination Cluster: | cluster-1 | | | Last Transfer Error: | None |
| Transfer Schedule: | daily | | | Last Transfer Type: | Update |
| Data Transfer Rate: | Unlimited | | | Latest Snapshot Timestamp: | 02/28/2017 00:10:00 |
| Lag Time: | 4 hr(s) 28 min(s) | | | Latest Snapshot Copy: | daily.2017-02-28_0010 |

Gestione del ripristino dei volumi con SnapVault

Panoramica del ripristino del volume con SnapVault

In caso di perdita di dati, è possibile ripristinare rapidamente un volume da un backup SnapVault in ONTAP.

Utilizzare questa procedura se si desidera eseguire il ripristino dal backup del vault nel modo seguente:

- Stai lavorando con cluster che eseguono ONTAP 9.
- Sei un amministratore del cluster.
- La relazione del vault è stata configurata seguendo la procedura descritta in [Backup del volume con SnapVault](#)
- Non si desidera eseguire un ripristino di un singolo file o LUN.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Non si desidera leggere un sacco di background concettuale.
- Si desidera utilizzare l'interfaccia classica di Gestione sistema per ONTAP 9.7 e versioni precedenti, non l'interfaccia utente di Gestione sistema di ONTAP per ONTAP 9.7 e versioni successive.

Se questi presupposti non sono corretti per la situazione o se si desidera ottenere informazioni di base più concettuali, si dovrebbe visualizzare la seguente risorsa:

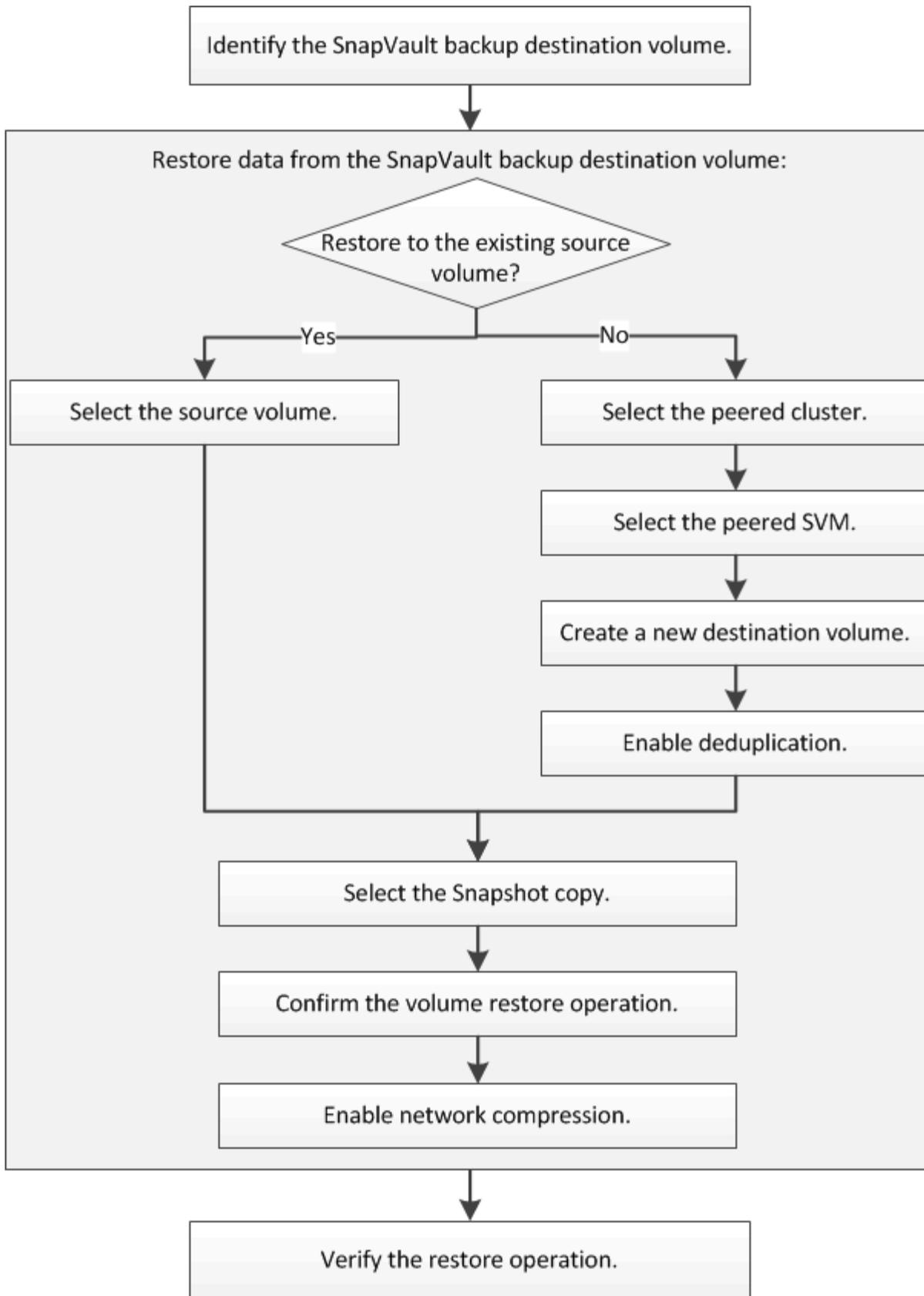
["Report tecnico di NetApp 4183: Best Practice SnapVault"](#)

Altri modi per farlo in ONTAP

| Per eseguire queste attività con... | Guarda questo contenuto... |
|---|---|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | "Ripristinare un volume da una copia Snapshot precedente" |
| L'interfaccia della riga di comando di ONTAP | "Ripristinare il contenuto di un volume da una destinazione SnapMirror" |

Workflow di ripristino del volume

Quando il volume di origine non è disponibile o i dati sono corrotti, è possibile eseguire un ripristino da un backup SnapVault. Il ripristino di un volume da un backup SnapVault comporta la selezione del volume di destinazione SnapVault, il ripristino su un nuovo volume o su un volume esistente e la verifica dell'operazione di ripristino.



Sono disponibili ulteriori informazioni per gestire le relazioni di backup di SnapVault e utilizzare altri metodi di protezione dei dati per proteggere la disponibilità delle risorse dati.

- [Preparazione al disaster recovery dei volumi](#)

Viene descritto come configurare rapidamente un volume di destinazione su un cluster ONTAP diverso in preparazione del disaster recovery.

- [Disaster recovery dei volumi](#)

Descrive come attivare rapidamente un volume di destinazione da un cluster ONTAP diverso dopo un disastro, nonché come ripristinare la relazione SnapMirror al suo stato originale riattivando il volume di origine dopo il ripristino.

Identificare il volume di destinazione del backup di SnapVault

È necessario identificare il volume di destinazione del backup SnapVault da cui si desidera ripristinare i dati quando i dati nel volume di origine vengono danneggiati o persi.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Inserire l'URL `https://IP-address-of-cluster-management-LIF` in un browser Web e accedere a System Manager utilizzando la credenziale dell'amministratore del cluster.
2. Accedere alla finestra **Volumes**.
3. Identificare il volume di destinazione nella relazione SnapVault e il nome della SVM che contiene il volume:
 - ONTAP 9.3 o versione successiva: Fare doppio clic sul volume per visualizzare i dettagli, quindi fare clic su **PROTECTION**.
 - ONTAP 9.2 o versioni precedenti: Fare clic sulla scheda **protezione dati** nella parte inferiore della finestra volumi.

Ripristinare i dati da un backup SnapVault

Dopo aver selezionato il volume di destinazione del backup di SnapVault, è necessario eseguire l'operazione di ripristino su un nuovo volume per verificare i dati di cui è stato eseguito il backup o su un volume esistente per ripristinare i dati persi o danneggiati.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **destination**.

Fasi

1. A seconda della versione di System Manager in esecuzione, eseguire una delle seguenti operazioni:
 - ONTAP 9.4 o versione precedente: Fare clic su **protezione > relazioni**.
 - A partire da ONTAP 9.5: Fare clic su **protezione > Relazioni volume**.
2. Selezionare la SVM che contiene il volume di destinazione del backup di SnapVault, quindi fare clic su **operazioni > Ripristina**.
3. Nella finestra di dialogo **Restore**, ripristinare i dati nel volume di origine originale o in un nuovo volume:

| Se si desidera ripristinare a... | Quindi... |
|----------------------------------|---|
| Il volume di origine originale | Selezionare Volume di origine . |
| Un nuovo volume | <p>a. Selezionare altro volume.</p> <p>b. Selezionare il cluster peered e la SVM peered per il volume.</p> <p>c. Selezionare una SVM in peering dall'elenco.</p> <p>d. Se la SVM non è in peering, creare la relazione peer SVM:</p> <ol style="list-style-type: none"> Selezionare la SVM. Fare clic su Authenticate. Immettere le credenziali dell'amministratore del cluster in peered, quindi fare clic su Create (Crea). <p>e. Selezionare New Volume (nuovo volume).</p> <p>f. Se si desidera modificare il nome predefinito, visualizzato nel formato <code>destination_SVM_name_destination_volume_name_restore</code>, specificare un nuovo nome e selezionare l'aggregato contenente per il volume.</p> <p>g. Selezionare la casella di controllo Enable dedupe (attiva deduplica).</p> |

Restore to _____

Source volume
 Other volume

? Cluster:

Storage Virtual Machine:

Volume: New Volume Select Volume

Volume name:

Aggregate:

Enable dedupe 517.22 GB available (of 520.28 GB)

- Selezionare l'ultima copia Snapshot o selezionare una copia Snapshot specifica che si desidera ripristinare.
- Selezionare la casella di controllo **OK per ripristinare il volume dalla copia Snapshot**.
- Selezionare la casella di controllo **Enable Network Compression** (Abilita compressione di rete) per comprimere i dati trasferiti durante l'operazione di ripristino.
- Fare clic su **Restore** (Ripristina).

Durante il processo di ripristino, il volume da ripristinare viene modificato in sola lettura. Al termine dell'operazione di ripristino, la relazione temporanea viene rimossa e il volume ripristinato viene modificato in lettura/scrittura.



8. Fare clic su **OK** nella finestra del messaggio.

Verificare l'operazione di ripristino

Dopo aver eseguito l'operazione di ripristino dal volume di destinazione del backup di SnapVault, è necessario verificare lo stato dell'operazione di ripristino sul cluster di origine.

A proposito di questa attività

È necessario eseguire questa attività dal cluster **source**.

Fasi

1. Accedere alla finestra **Volumes**.
2. Selezionare il volume di origine nell'elenco Volumes (volumi) ed eseguire una delle seguenti operazioni, a seconda della versione di ONTAP in uso:
 - A partire da ONTAP 9.3: Fare doppio clic sul volume di origine per visualizzare i dettagli, quindi fare clic su **PROTECTION** per identificare il volume di destinazione nella relazione di SnapMirror e il nome della SVM che contiene il volume.
 - ONTAP 9.2 o versioni precedenti: Fare clic sulla scheda inferiore **protezione dati** per identificare il volume di destinazione nella relazione SnapMirror e il nome della SVM che contiene il volume. Viene visualizzato il campo Type (tipo) `Restore` temporaneamente. Al termine dell'operazione di ripristino, viene visualizzato il campo `Vault`.

È necessario risolvere eventuali problemi nelle relazioni SnapVault. Le procedure di troubleshooting per le relazioni di SnapMirror sono applicabili anche alle relazioni di SnapVault.

["Report tecnico di NetApp 4015: Configurazione e Best practice di SnapMirror per ONTAP 9.1, 9.2"](#)

Informazioni sul copyright

Copyright © 2024 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.