



Preparazione al disaster recovery dei volumi

System Manager Classic

NetApp
June 22, 2024

Sommario

- Preparazione al disaster recovery dei volumi 1
- Panoramica sulla preparazione del disaster recovery dei volumi 1
- Workflow di preparazione del disaster recovery dei volumi 1

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"](#)

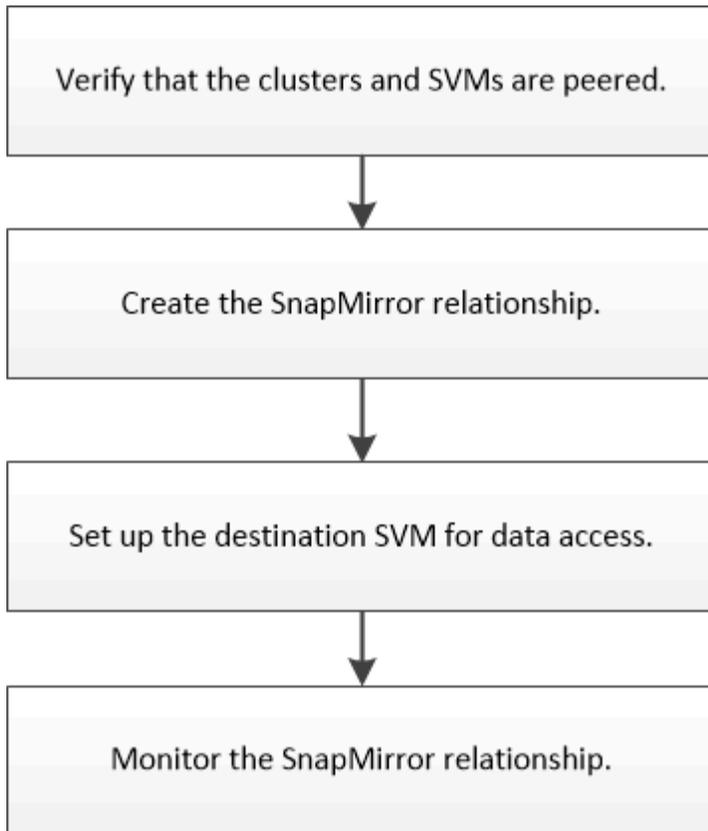
- La licenza SnapMirror è stata attivata sia sul cluster di origine che su quello di destinazione.
- Si desidera utilizzare le policy e le pianificazioni predefinite e non creare policy personalizzate.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili (ONTAP 9.7 e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



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 mins	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_Vol1	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_2147494888.2014-09-18_233529

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.