Protezione dei dati e disaster recovery

ONTAP 9

NetApp
April 24, 2024

Sommario

Protezione dei dati e disaster recovery

Protezione dei dati con System Manager

Panoramica sulla protezione dei dati con System Manager

Gli argomenti di questa sezione illustrano come configurare e gestire la protezione dei dati con Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione sistema in ONTAP 9.7 o versioni precedenti, vedere "Documentazione classica di Gestore di sistema ONTAP"

Proteggi i tuoi dati creando e gestendo copie Snapshot, mirror, vault e relazioni mirror-and-vault.

SnapMirror è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o mirror, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

Un *vault* è progettato per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

A partire da ONTAP 9.10.1, è possibile creare relazioni di protezione dei dati tra i bucket S3 utilizzando S3 SnapMirror. I bucket di destinazione possono essere su sistemi ONTAP locali o remoti o su sistemi non ONTAP come StorageGRID e AWS. Per ulteriori informazioni, vedere "Panoramica di S3 SnapMirror".

Creare policy di protezione dei dati personalizzate

È possibile creare policy di protezione dei dati personalizzate con System Manager quando le policy di protezione predefinite esistenti non sono adatte alle proprie esigenze. A partire da ONTAP 9.11.1, è possibile utilizzare Gestore di sistema per creare policy personalizzate di mirroring e vault, per visualizzare e selezionare policy legacy. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.

Creare policy di protezione personalizzate sul cluster di origine e di destinazione.

Fasi

1. Fare clic su **Protection > Local Policy Settings** (protezione > Impostazioni policy locali).
2. Nella sezione **Criteri di protezione**, fare clic su →.
3. Nel riquadro **Criteri di protezione**, fare clic su + Add .
4. Inserire il nuovo nome del criterio e selezionare l'ambito del criterio.
5. Scegliere un tipo di policy. Per aggiungere una policy di solo vault o solo mirror, scegliere **Asynchronous** e fare clic su **Usa un tipo di policy legacy**.
6. Compilare i campi obbligatori.
7. Fare clic su **Save** (Salva).

8. Ripetere questi passaggi sull'altro cluster.

Configurare le copie Snapshot

È possibile creare policy di copia Snapshot per specificare il numero massimo di copie Snapshot create automaticamente e la frequenza di creazione. Il criterio specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome.

Questa procedura crea un criterio di copia Snapshot solo sul cluster locale.

Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali**.
2. In **Snapshot Policies**, fare clic su →, quindi fare clic su + Add .
3. Digitare il nome del criterio, selezionare l'ambito del criterio e in **Pianificazioni**, fare clic su + Add per inserire i dettagli della pianificazione.

Calcola lo spazio recuperabile prima di eliminare le copie Snapshot

A partire da ONTAP 9.10.1, è possibile utilizzare Gestore di sistema per selezionare le copie Snapshot che si desidera eliminare e calcolare lo spazio recuperabile prima di eliminarle.

Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume dal quale si desidera eliminare le copie Snapshot.
3. Fare clic su **copie Snapshot**.
4. Selezionare una o più copie Snapshot.
5. Fare clic su **Calcola spazio recuperabile**.

Attivare o disattivare l'accesso del client alla directory di copia Snapshot

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per attivare o disattivare i sistemi client per accedere a una directory di copia Snapshot su un volume. L'abilitazione dell'accesso rende la directory di copia Snapshot visibile ai client e consente ai client Windows di mappare un disco alla directory Snapshot Copies per visualizzarne e accedervi.

È possibile attivare o disattivare l'accesso alla directory di copia Snapshot di un volume modificando le impostazioni del volume o le impostazioni di condivisione del volume.

Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando un volume

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.

Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.

3. Fare clic su ⋮ E selezionare **Modifica**.
4. Nella sezione **Snapshot Copies (Local) Settings**, selezionare o deselezionare **Show the Snapshot Copies directory to clients** (Mostra la directory Snapshot Copies ai client).
5. Fare clic su **Save** (Salva).

Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando una condivisione

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.

Fasi

1. Fare clic su **Storage > Shares**.
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.
3. Fare clic su ⋮ E selezionare **Modifica**.
4. Nella sezione **Proprietà condivisione**, selezionare o deselezionare **Consenti ai client di accedere alla directory Snapshot Copies**.
5. Fare clic su **Save** (Salva).

Preparazione per il mirroring e il vaulting

È possibile proteggere i dati replicandoli in un cluster remoto per il backup dei dati e il disaster recovery.

Sono disponibili diversi criteri di protezione predefiniti. Se si desidera utilizzare policy personalizzate, è necessario aver creato le policy di protezione.

Fasi

1. Nel cluster locale, fare clic su **protezione > Panoramica**.
2. Espandere **Impostazioni Intercluster**. Fare clic su **Add Network Interfaces** (Aggiungi interfacce di rete) e aggiungere interfacce di rete intercluster per il cluster.

   Ripetere questo passaggio sul cluster remoto.

3. Nel cluster remoto, fare clic su **protezione > Panoramica**. Fare clic su ⋮ Nella sezione Cluster Peers (peer cluster), fare clic su **generate Passphrase** (genera passphrase)
4. Copiare la passphrase generata e incollarla nel cluster locale.
5. Nel cluster locale, in Cluster Peers, fare clic su **Peer Clusters** e eseguire il peer dei cluster locali e remoti.
6. In alternativa, sotto Storage VM Peers, fare clic su ⋮ E poi **Peer Storage VM** per eseguire il peer delle VM di storage.
7. Fare clic su **Protect Volumes** (Proteggi volumi) per proteggere i volumi. Per proteggere i LUN, fare clic su

Storage > LUN, selezionare un LUN da proteggere, quindi fare clic su Protect.

Selezionare la policy di protezione in base al tipo di protezione dei dati desiderata.

8. Per verificare che i volumi e le LUN siano protetti correttamente dal cluster locale, fare clic su **Storage > Volumes** o **Storage > LUN** e espandere la vista volume/LUN.

Altri modi per farlo in ONTAP

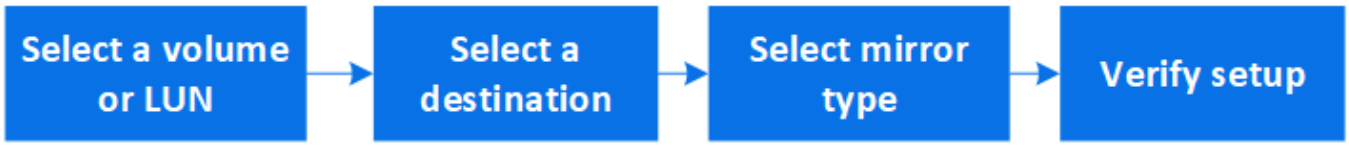
Per eseguire queste attività con…	Guarda questo contenuto…
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica sulla preparazione del disaster recovery dei volumi"
L'interfaccia della riga di comando di ONTAP	"Creare una relazione peer del cluster"

Configurare mirror e vault

Creare un mirror e un vault di un volume per proteggere i dati in caso di disastro e avere più versioni archiviate dei dati su cui eseguire il rollback. A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per selezionare policy di vault e mirror pre-create e personalizzate, per visualizzare e selezionare policy legacy e per ignorare le pianificazioni di trasferimento definite in una policy di protezione quando si proteggono volumi e macchine virtuali di storage. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.

> Se si utilizza ONTAP 9.8P12 o versione successiva della patch per ONTAP 9.8 e si configura SnapMirror utilizzando Gestione di sistema, è necessario utilizzare ONTAP 9.9.1P13 o versione successiva e ONTAP 9.10.1P10 o versioni successive se si intende eseguire l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1.

Questa procedura crea un criterio di protezione dei dati su un cluster remoto. Il cluster di origine e il cluster di destinazione utilizzano interfacce di rete intercluster per lo scambio di dati. La procedura presuppone "vengono create le interfacce di rete tra cluster e i cluster contenenti i volumi vengono peering" (accoppiato). È inoltre possibile eseguire il peer delle macchine virtuali storage per la protezione dei dati; tuttavia, se le macchine virtuali storage non sono in peering, ma le autorizzazioni sono attivate, le macchine virtuali storage vengono automaticamente messe in peering quando viene creata la relazione di protezione.



Fasi

1. Selezionare il volume o il LUN da proteggere: Fare clic su **Storage > Volumes** o **Storage > LUN**, quindi fare clic sul nome del volume o del LUN desiderato.
2. Fare clic su Protect.
3. Selezionare il cluster di destinazione e la VM di storage.
4. Il criterio asincrono viene selezionato per impostazione predefinita. Per selezionare un criterio sincrono, fare clic su **altre opzioni**.

5. Fare clic su **Protect** (protezione).
6. Fare clic sulla scheda **SnapMirror (locale o remoto)** del volume o LUN selezionato per verificare che la protezione sia impostata correttamente.

Informazioni correlate

- "Creazione ed eliminazione di volumi di test del failover SnapMirror".

Altri modi per farlo in ONTAP

Per eseguire queste attività con…	Guarda questo contenuto…
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica del backup del volume con SnapVault"
L'interfaccia della riga di comando di ONTAP	"Creare una relazione di replica"

Risincronizzare una relazione di protezione

Quando il volume di origine è nuovamente disponibile dopo un disastro, è possibile risincronizzare i dati dal volume di destinazione e ristabilire la relazione di protezione.

Questa procedura sostituisce i dati nel volume di origine originale in una relazione asincrona, in modo da poter iniziare nuovamente a servire i dati dal volume di origine e riprendere la relazione di protezione originale.

Fasi

1. Fare clic su **protezione > Relazioni**, quindi sulla relazione interrotta che si desidera risincronizzare.
2. Fare clic su ⋮ Quindi selezionare **Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione controllando lo stato della relazione. Lo stato diventa "mirrored" al termine della risincronizzazione.

Ripristinare un volume da una copia Snapshot precedente

In caso di perdita o danneggiamento dei dati in un volume, è possibile eseguire il rollback dei dati eseguendo il ripristino da una copia Snapshot precedente.

Questa procedura sostituisce i dati correnti sul volume di origine con i dati di una versione di copia Snapshot precedente. Eseguire questa attività sul cluster di destinazione.

Fasi

1. Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume di origine.
2. Fare clic su ⋮ Quindi selezionare **Ripristina**.
3. In **Source** (origine), il volume di origine viene selezionato per impostazione predefinita. Fare clic su **Other Volume** (Altro volume) se si desidera scegliere un volume diverso dall'origine.
4. In **destinazione**, scegliere la copia Snapshot che si desidera ripristinare.
5. Se l'origine e la destinazione si trovano in cluster diversi, sul cluster remoto fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

Altri modi per farlo in ONTAP

Per eseguire queste attività con…	Guarda questo contenuto…
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica del ripristino del volume con SnapVault"
L'interfaccia della riga di comando di ONTAP	"Ripristinare il contenuto di un volume da una destinazione SnapMirror"

Ripristino da copie Snapshot

È possibile ripristinare un volume a un punto precedente eseguendo il ripristino da una copia Snapshot.

Questa procedura ripristina un volume da una copia Snapshot.

Fasi

1. Fare clic su **Storage** e selezionare un volume.
2. In **Snapshot Copies**, fare clic su ⋮ Accanto alla copia Snapshot che si desidera ripristinare e selezionare **Restore** (Ripristina).

Ripristinare su un nuovo volume

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per ripristinare i dati di backup sul volume di destinazione su un volume diverso dall'origine originale.

Quando si esegue il ripristino su un volume diverso, è possibile selezionare un volume esistente o crearne uno nuovo.

Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su ⋮ E fare clic su **Restore**.
3. Nella sezione **origine**, selezionare **Altro volume** e selezionare il cluster e la Storage VM.
4. Selezionare **Existing volume** (volume esistente) o **Create a new volume** (Crea nuovo volume).
5. Se si sta creando un nuovo volume, immettere il nome del volume.
6. Nella sezione **destinazione**, selezionare la copia Snapshot da ripristinare.
7. Fare clic su **Save** (Salva).
8. In **Relazioni**, monitorare l'avanzamento del ripristino visualizzando **Stato trasferimento** per la relazione.

Risincronizzazione inversa di una relazione di protezione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per eseguire un'operazione di risincronizzazione inversa per eliminare una relazione di protezione esistente e invertire le funzioni dei volumi di origine e di destinazione. Quindi si utilizza il volume di destinazione per fornire i dati durante la riparazione o la sostituzione dell'origine, l'aggiornamento dell'origine e il ripristino della configurazione originale dei sistemi.

System Manager non supporta la risincronizzazione inversa con relazioni intracluster. È possibile utilizzare l'interfaccia utente di ONTAP per eseguire operazioni di risincronizzazione inversa con relazioni intracluster.

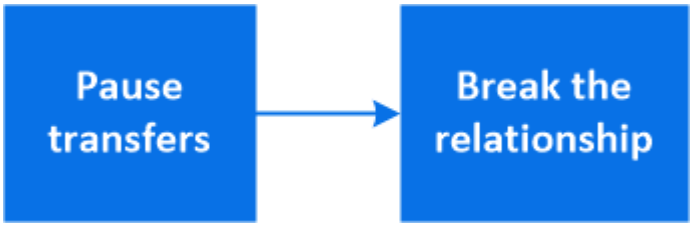
Quando si esegue un'operazione di risincronizzazione inversa, tutti i dati sul volume di origine più recenti dei dati nella copia Snapshot comune vengono cancellati.

Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su ⋮ E fare clic su **Reverse Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione inversa visualizzando **Stato trasferimento** per la relazione.

Fornire i dati da una destinazione SnapMirror

Per fornire dati da una destinazione mirror quando un'origine non è disponibile, interrompere i trasferimenti pianificati verso la destinazione, quindi interrompere la relazione SnapMirror per rendere la destinazione scrivibile.



Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume desiderato.
2. Fare clic su ⋮.
3. Stop scheduled transfer (Interrompi trasferimenti pianificati): Fare clic su **Pause**
4. Rendere scrivibile la destinazione: Fare clic su **Interrompi**.
5. Andare alla pagina principale **Relazioni** per verificare che lo stato della relazione sia visualizzato come "interrotto".

Fasi successive:

Quando il volume di origine disattivato è nuovamente disponibile, è necessario risincronizzare la relazione per copiare i dati correnti nel volume di origine originale. Questo processo sostituisce i dati sul volume di origine originale.

Altri modi per farlo in ONTAP

Per eseguire queste attività con…	Guarda questo contenuto…
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica sul disaster recovery dei volumi"
L'interfaccia della riga di comando di ONTAP	"Attivare il volume di destinazione"

Configurare il disaster recovery delle macchine virtuali dello storage

Con System Manager, è possibile creare una relazione di disaster recovery per le macchine virtuali di storage (DR per le macchine virtuali di storage) per replicare una configurazione delle macchine virtuali di storage in un'altra. In caso di disastro nel sito primario, è possibile attivare rapidamente la VM di storage di destinazione.

Completare questa procedura dalla destinazione. Se è necessario creare un nuovo criterio di protezione, ad esempio, quando la VM dello storage di origine ha SMB configurato, è necessario utilizzare System Manager per creare il criterio e selezionare l'opzione **Identity Preserve** nella finestra **Add Protection Policy**.
Per ulteriori informazioni, vedere "Creare policy di protezione dei dati personalizzate".

Fasi

1. Nel cluster di destinazione, fare clic su **protezione > Relazioni**.
2. In **Relazioni**, fare clic su Proteggi e scegliere **Storage VM (DR)**.
3. Selezionare un criterio di protezione. Se è stato creato un criterio di protezione personalizzato, selezionarlo, quindi scegliere il cluster di origine e la VM di storage che si desidera replicare. È inoltre possibile creare una nuova VM di storage di destinazione immettendo un nuovo nome per la VM di storage.
4. Fare clic su **Save** (Salva).

Fornire i dati da una destinazione DR SVM

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per attivare una VM di storage di destinazione dopo un disastro. L'attivazione della VM di storage di destinazione rende i volumi di destinazione SVM scrivibili e consente di inviare i dati ai client.

Fasi

1. Se il cluster di origine è accessibile, verificare che SVM sia stato arrestato: Selezionare **Storage > Storage VM** e selezionare la colonna **state** per SVM.
2. Se lo stato SVM di origine è "in esecuzione", interromperlo: Selezionare ⋮ E scegliere **Stop**.
3. Sul cluster di destinazione, individuare la relazione di protezione desiderata: Accedere a **protezione > Relazioni**.
4. Fare clic su ⋮ E scegliere **Activate Destination Storage VM**.

Riattivare una VM di storage di origine

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per riattivare una VM di storage di origine dopo un disastro. La riattivazione della VM di storage di origine interrompe la VM di storage di destinazione e riattiva la replica dall'origine alla destinazione.

A proposito di questa attività

Quando si riattiva la VM dello storage di origine, System Manager esegue le seguenti operazioni in background:

- Crea una relazione DR SVM inversa dalla destinazione originale all'origine utilizzando la risincronizzazione

di SnapMirror

- Arresta la SVM di destinazione
- Aggiorna la relazione di SnapMirror
- Interrompe la relazione di SnapMirror
- Riavvia la SVM originale
- Effettua una risincronizzazione di SnapMirror dell'origine originale verso la destinazione originale
- Elimina le relazioni di SnapMirror

Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su ⋮ E fare clic su **Riattiva VM storage di origine**.
3. In **Relazioni**, monitorare l'avanzamento della riattivazione dell'origine visualizzando **Stato trasferimento** per la relazione di protezione.

Risincronizzare una VM di storage di destinazione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per risincronizzare i dati e i dettagli di configurazione dalla VM di storage di origine alla VM di storage di destinazione in una relazione di protezione interrotta e ristabilire la relazione.

ONTAP 9.11.1 introduce un'opzione per evitare la ricostruzione completa del data warehouse quando si esegue una prova di disaster recovery, consentendo di tornare più rapidamente alla produzione.

L'operazione di risincronizzazione viene eseguita solo dalla destinazione della relazione originale. La risincronizzazione elimina tutti i dati nella VM di storage di destinazione più recenti dei dati nella VM di storage di origine.

Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Facoltativamente, selezionare **Perform a quick resync** (Esegui una risincronizzazione rapida) per ignorare la ricostruzione completa del data warehouse durante una prova di disaster recovery.
3. Fare clic su ⋮ E fare clic su **Resync**.
4. In **Relazioni**, monitorare l'avanzamento della risincronizzazione visualizzando **Stato trasferimento** per la relazione.

Eseguire il backup dei dati nel cloud utilizzando SnapMirror

A partire da ONTAP 9.9.1, puoi eseguire il backup dei dati nel cloud e ripristinare i dati dal cloud storage a un volume diverso utilizzando Gestione di sistema. Puoi utilizzare StorageGRID o ONTAP S3 come archivio di oggetti cloud.

Prima di utilizzare la funzione SnapMirror Cloud, è necessario richiedere una chiave di licenza API di SnapMirror Cloud al sito di supporto NetApp: "Richiedere la chiave di licenza API di SnapMirror Cloud". Seguendo le istruzioni, fornisci una semplice descrizione dell'opportunità di business e richiedi la chiave API inviando un'email all'indirizzo email fornito. Entro 24 ore riceverai una risposta via email con ulteriori istruzioni su come acquisire la chiave API.

Aggiungere un archivio di oggetti cloud

Prima di configurare i backup di SnapMirror Cloud, è necessario aggiungere un archivio di oggetti cloud StorageGRID o ONTAP S3.

Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Fare clic su + Add .

Eseguire il backup utilizzando il criterio predefinito

È possibile configurare rapidamente un backup di SnapMirror Cloud per un volume esistente utilizzando la policy di protezione cloud predefinita, DailyBackup.

Fasi

1. Fare clic su **protezione > Panoramica** e selezionare **Backup dei volumi nel cloud**.
2. Se è la prima volta che si esegue il backup nel cloud, inserire la chiave di licenza API di SnapMirror Cloud nel campo della licenza, come indicato.
3. Fare clic su **Authenticate and Continue** (autentica e continua)
4. Selezionare un volume di origine.
5. Selezionare un archivio di oggetti cloud.
6. Fare clic su **Save** (Salva).

Creare una policy di backup cloud personalizzata

Se non si desidera utilizzare la policy cloud predefinita di DailyBackup per i backup di SnapMirror Cloud, è possibile creare una policy personalizzata.

Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali** e selezionare **Criteri di protezione**.
2. Fare clic su **Add** (Aggiungi) e inserire i nuovi dettagli della policy.
3. Nella sezione **Policy Type**, selezionare **Backup to Cloud** per indicare che si sta creando una policy cloud.
4. Fare clic su **Save** (Salva).

Creare un backup dalla pagina volumi

È possibile utilizzare la pagina System Manager **Volumes** per selezionare e creare backup cloud per più volumi contemporaneamente o quando si desidera utilizzare una policy di protezione personalizzata.

Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare i volumi di cui si desidera eseguire il backup nel cloud e fare clic su **Protect**.
3. Nella finestra **Protect Volume** (Proteggi volume), fare clic su **More Options** (altre opzioni).
4. Selezionare un criterio.

   È possibile selezionare il criterio predefinito, DailyBackup o un criterio cloud personalizzato creato.

5. Selezionare un archivio di oggetti cloud.

6. Fare clic su **Save** (Salva).

Eseguire il ripristino dal cloud

È possibile utilizzare System Manager per ripristinare i dati di backup dallo storage cloud a un volume diverso nel cluster di origine.

Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare la scheda **Backup nel cloud**.
3. Fare clic su ⋮ Accanto al volume di origine che si desidera ripristinare e selezionare **Restore** (Ripristina).
4. In **Source** (origine), selezionare una VM di storage e immettere il nome del volume in cui si desidera ripristinare i dati.
5. In **destinazione**, selezionare la copia Snapshot che si desidera ripristinare.
6. Fare clic su **Save** (Salva).

Eliminare una relazione SnapMirror Cloud

È possibile utilizzare System Manager per eliminare una relazione cloud.

Fasi

1. Fare clic su **Storage > Volumes** (archiviazione > volumi) e selezionare il volume che si desidera eliminare.
2. Fare clic su ⋮ Accanto al volume di origine e selezionare **Delete** (Elimina).
3. Selezionare **Delete the cloud object store endpoint (opzionale)** se si desidera eliminare l'endpoint dell'archivio di oggetti cloud.
4. Fare clic su **Delete** (Elimina).

Rimuovere un archivio di oggetti cloud

È possibile utilizzare System Manager per rimuovere un archivio di oggetti cloud se non fa parte di una relazione di backup cloud. Quando un archivio di oggetti cloud fa parte di una relazione di backup cloud, non può essere cancellato.

Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Selezionare l'archivio di oggetti che si desidera eliminare, quindi fare clic su ⋮ E selezionare **Delete** (Elimina).

Eseguire il backup dei dati utilizzando Cloud Backup

A partire da ONTAP 9.9.1, puoi utilizzare Gestione sistema per eseguire il backup dei dati nel cloud utilizzando il backup nel cloud.

> Cloud Backup supporta volumi di lettura/scrittura FlexVol e volumi di protezione dei dati (DP). I volumi FlexGroup e SnapLock non sono supportati.

Prima di iniziare

Per creare un account in BlueXP, attenersi alle seguenti procedure. Per l'account di servizio, è necessario

creare il ruolo di "account Admin". (Gli altri ruoli dell'account di servizio non dispongono dei privilegi necessari per stabilire una connessione da System Manager).

1. "Creare un account in BlueXP".
2. "Creare un connettore in BlueXP" con uno dei seguenti cloud provider:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Piattaforma Google Cloud (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > A partire da ONTAP 9.10.1, è possibile selezionare StorageGRID come provider di backup cloud, ma solo se BlueXP è implementato on-premise. BlueXP Connector deve essere installato on-premise e disponibile tramite l'applicazione Software-as-a-Service (SaaS) BlueXP.

3. "Iscriviti a Cloud Backup Service in BlueXP" (richiede la licenza appropriata).
4. "Generare una chiave di accesso e una chiave segreta utilizzando BlueXP".

Registrare il cluster con BlueXP

È possibile registrare il cluster con BlueXP utilizzando BlueXP o System Manager.

Fasi

1. In System Manager, accedere a **Panoramica sulla protezione**.
2. In **Cloud Backup Service**, fornire i seguenti dettagli:
   - ID client
   - Chiave segreta del client
3. Selezionare **Registra e continua**.

Attiva Cloud Backup

Una volta registrato il cluster con BlueXP, è necessario attivare Cloud Backup e avviare il primo backup nel cloud.

Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.
2. Inserire **ID client** e **Segreto client**.

   > A partire da ONTAP 9.10.1, puoi scoprire il costo dell'utilizzo del cloud facendo clic su **ulteriori informazioni sul costo dell'utilizzo del cloud**.

3. Fare clic su **Connetti e attiva Cloud Backup Service**.
4. Nella pagina **Enable Cloud Backup Service** (attiva protocollo), fornire i seguenti dettagli, a seconda del provider selezionato.

Per questo cloud provider…	Inserire i seguenti dati…

Azure	• ID abbonamento Azure • Regione • Nome del gruppo di risorse (esistente o nuovo)
AWS	• ID account AWS • Tasto di accesso • Chiave segreta • Regione
Google Cloud Project (GCP)	• Nome del progetto Google Cloud • Chiave Google Cloud Access • Chiave segreta di Google Cloud • Regione
StorageGRID (ONTAP 9.10.1 e versioni successive e solo per l'implementazione on-premise di BlueXP)	• Server • Chiave di accesso SG • Chiave segreta SG

5. Selezionare una **policy di protezione**:
   - **Policy esistente**: Scegliere una policy esistente.
   - **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.

     A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.

     Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.

     Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

     - Il numero di giorni trascorsi i quali il volume viene archiviato.
     - Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
     - Per AWS, selezionare la classe di storage di archiviazione.
6. Selezionare i volumi di cui si desidera eseguire il backup.
7. Selezionare **Salva**.

Modificare il criterio di protezione utilizzato per Cloud Backup

È possibile modificare i criteri di protezione utilizzati con Cloud Backup.

Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.

2. Fare clic su ⋮, Quindi **Modifica**.
3. Selezionare una **policy di protezione**:
   - **Policy esistente**: Scegliere una policy esistente.
   - **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.

     A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.

     Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.

     Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

     - Il numero di giorni trascorsi i quali il volume viene archiviato.
     - Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
     - Per AWS, selezionare la classe di storage di archiviazione.
4. Selezionare **Salva**.

Proteggi nuovi volumi o LUN sul cloud

Quando si crea un nuovo volume o LUN, è possibile stabilire una relazione di protezione di SnapMirror che consenta il backup nel cloud per il volume o il LUN.

Prima di iniziare

- È necessario disporre di una licenza SnapMirror.
- È necessario configurare le LIF di intercluster.
- NTP deve essere configurato.
- Il cluster deve eseguire ONTAP 9.9.1.

A proposito di questa attività

Non è possibile proteggere nuovi volumi o LUN sul cloud per le seguenti configurazioni di cluster:

- Il cluster non può trovarsi in un ambiente MetroCluster.
- SVM-DR non supportato.
- Impossibile eseguire il backup di FlexGroups utilizzando Cloud Backup.

Fasi

1. Quando si effettua il provisioning di un volume o di un LUN, nella pagina **Protection** di System Manager, selezionare la casella di controllo **Enable SnapMirror (Local or Remote)** (attiva SnapMirror (locale o remoto)*.
2. Selezionare il tipo di criterio Cloud Backup.
3. Se il backup cloud non è attivato, selezionare **Enable Cloud Backup Service** (attiva backup cloud).

Proteggere i volumi o le LUN esistenti nel cloud

È possibile stabilire una relazione di protezione di SnapMirror per i volumi e le LUN esistenti.

Fasi

1. Selezionare un volume o un LUN esistente e fare clic su **Protect** (protezione).
2. Nella pagina **Protect Volumes**, specificare **Backup using Cloud Backup Service** per il criterio di protezione.
3. Fare clic su **Protect** (protezione).
4. Nella pagina **protezione**, selezionare la casella di controllo **attiva SnapMirror (locale o remoto)**.
5. Selezionare **Enable Cloud Backup Service** (attiva protocollo).

Ripristinare i dati dai file di backup

È possibile eseguire operazioni di gestione del backup, come il ripristino dei dati, l'aggiornamento delle relazioni e l'eliminazione delle relazioni, solo quando si utilizza l'interfaccia BlueXP. Fare riferimento a. "Ripristino dei dati dai file di backup" per ulteriori informazioni.

Peering di cluster e SVM con CLI

Panoramica del peering di cluster e SVM con CLI

È possibile creare relazioni peer tra cluster di origine e di destinazione e tra macchine virtuali storage di origine e di destinazione (SVM). È necessario creare relazioni peer tra queste entità prima di poter replicare le copie Snapshot utilizzando SnapMirror.

ONTAP 9.3 offre miglioramenti che semplificano il modo in cui si configurano le relazioni peer tra cluster e SVM. Le procedure di peering del cluster e delle SVM sono disponibili per tutte le versioni di ONTAP 9. Utilizzare la procedura appropriata per la versione di ONTAP in uso.

Le procedure vengono eseguite utilizzando l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Preparatevi per il peering di cluster e SVM

Nozioni di base sul peering

È necessario creare *relazioni peer* tra cluster di origine e di destinazione e tra SVM di origine e di destinazione prima di poter replicare le copie Snapshot utilizzando SnapMirror. Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro.

I cluster e le SVM nelle relazioni tra pari comunicano sulla rete intercluster utilizzando *LIF (Intercluster Logical Interface)*. Una LIF intercluster è una LIF che supporta il servizio di interfaccia di rete "intercluster-core" e viene generalmente creata utilizzando la policy del servizio di interfaccia di rete "intercluster predefinito". È necessario creare LIF intercluster su ogni nodo dei cluster sottoposti a peering.

Le LIF di intercluster utilizzano i percorsi che appartengono alla SVM di sistema a cui sono assegnate. ONTAP crea automaticamente una SVM di sistema per le comunicazioni a livello di cluster all'interno di un IPSpace.

Sono supportate entrambe le topologie fan-out e cascata. In una topologia a cascata, è necessario creare solo reti di intercluster tra i cluster primario e secondario e tra i cluster secondario e terziario. Non è necessario creare una rete di intercluster tra il cluster primario e il cluster terzo.

> È possibile (ma non consigliabile) che un amministratore rimuova il servizio intercluster-core dalla policy di servizio intercluster predefinita. In questo caso, i LIF creati utilizzando "intercluster predefinito" non saranno effettivamente LIF intercluster. Per confermare che la policy di servizio dell'intercluster predefinito contiene il servizio intercluster-core, utilizzare il seguente comando:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```

Prerequisiti per il peering del cluster

Prima di configurare il peering del cluster, verificare che la connettività, la porta, l'indirizzo IP, la subnet, il firewall, e i requisiti di naming dei cluster sono soddisfatti.

> A partire da ONTAP 9.6, la crittografia peer del cluster fornisce il supporto per la crittografia GCM TLS 1.2 AES-256 per la replica dei dati per impostazione predefinita. I cifrari di sicurezza predefiniti ("PSK-AES256-GCM-SHA384") sono necessari per il funzionamento del peering del cluster anche se la crittografia è disattivata.
>
> A partire da ONTAP 9.11.1, le crittografia di sicurezza DHE-PSK sono disponibili per impostazione predefinita.

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 appartenere al dominio di trasmissione che contiene le porte utilizzate per la comunicazione tra cluster.
- 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 quattro nodi, la subnet utilizzata per la comunicazione tra cluster deve avere quattro 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 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

> A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "Configurare le policy firewall per le LIF".

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

- Traffico ICMP bidirezionale
- Traffico TCP avviato in modo bidirezionale verso gli indirizzi IP di tutti i LIF intercluster sulle porte 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

  Sebbene HTTPS non sia richiesto quando si imposta il peering del cluster utilizzando la CLI, HTTPS è richiesto in seguito se si utilizza System Manager 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.

Requisito del cluster

I cluster devono soddisfare i seguenti requisiti:

- Un cluster non può trovarsi in una relazione peer con più di 255 cluster.

Utilizzare porte condivise o dedicate

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Per decidere se condividere le porte, è necessario considerare la larghezza di banda della rete, l'intervallo di replica e la disponibilità delle porte.

> È possibile condividere le porte su un cluster peered utilizzando le porte dedicate sull'altro.

Larghezza di banda della rete

Se si dispone di una rete ad alta velocità, ad esempio 10 GbE, potrebbe essere disponibile una larghezza di banda LAN locale sufficiente per eseguire la replica utilizzando le stesse porte 10 GbE utilizzate per l'accesso ai dati.

Anche in questo caso, è necessario confrontare la larghezza di banda WAN disponibile con la larghezza di banda della LAN. Se la larghezza di banda WAN disponibile è significativamente inferiore a 10 GbE, potrebbe essere necessario utilizzare porte dedicate.

> L'unica eccezione a questa regola potrebbe essere rappresentata dal fatto che tutti o molti nodi del cluster replicano i dati, nel qual caso l'utilizzo della larghezza di banda è in genere distribuito tra i nodi.

Se non si utilizzano porte dedicate, le dimensioni massime dell'unità di trasmissione (MTU) della rete di replica dovrebbero essere le stesse della dimensione MTU della rete dati.

Intervallo di replica

Se la replica avviene in ore non di punta, dovresti essere in grado di utilizzare le porte dati per la replica anche senza una connessione LAN a 10 GbE.

Se la replica avviene durante il normale orario di lavoro, è necessario considerare la quantità di dati che verranno replicati e se richiede una larghezza di banda così elevata da causare conflitti con i protocolli dati. Se l'utilizzo della rete da parte dei protocolli di dati (SMB, NFS, iSCSI) è superiore al 50%, è necessario utilizzare porte dedicate per la comunicazione tra cluster, per consentire prestazioni non degradate in caso di failover del nodo.

Disponibilità delle porte

Se si determina che il traffico di replica interferisce con il traffico dati, è possibile migrare le LIF di intercluster su qualsiasi altra porta condivisa compatibile con intercluster sullo stesso nodo.

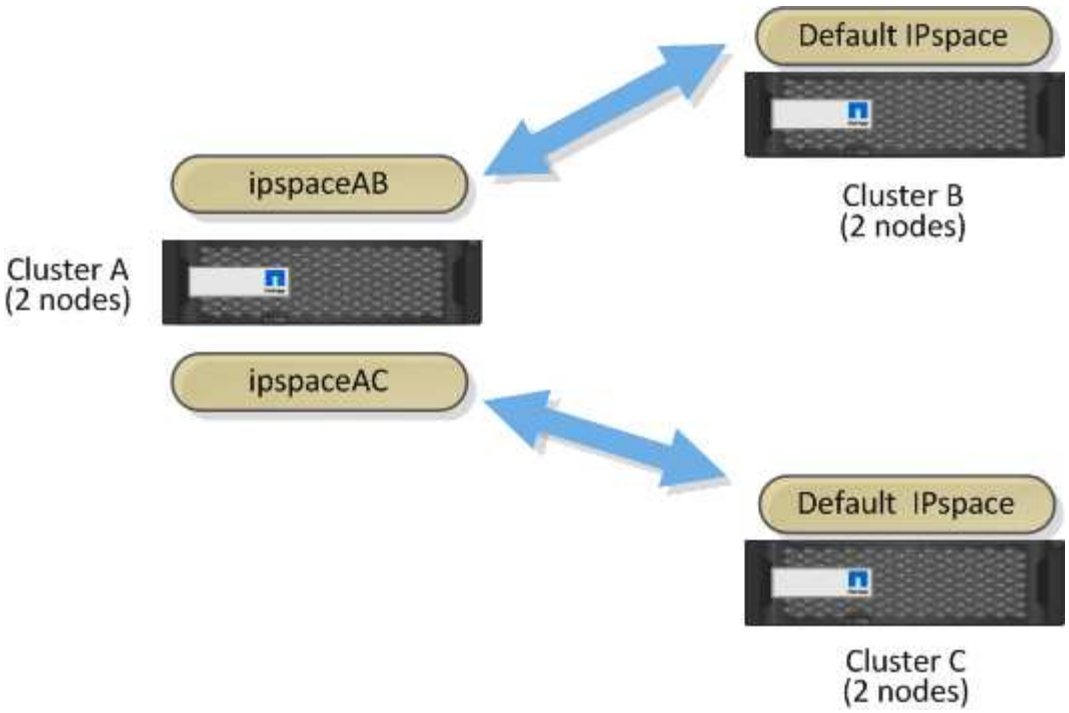
È inoltre possibile dedicare le porte VLAN per la replica. La larghezza di banda della porta è condivisa tra tutte le VLAN e la porta base.

Utilizzare IPspaces personalizzati per isolare il traffico di replica

È possibile utilizzare IPspaces personalizzati per separare le interazioni di un cluster con i peer. Detta *connettività intercluster designata*, questa configurazione consente ai service provider di isolare il traffico di replica in ambienti multi-tenant.

Si supponga, ad esempio, di voler separare il traffico di replica tra il cluster A e il cluster B dal traffico di replica tra il cluster A e il cluster C. A tale scopo, è possibile creare due IPspaces sul cluster A.

Un IPSpace contiene le LIF intercluster utilizzate per comunicare con il cluster B. L'altro contiene le LIF di intercluster utilizzate per comunicare con il cluster C, come mostrato nell'illustrazione seguente.



Per una configurazione IPSpace personalizzata, consultare la *Guida alla gestione di rete*.

Configurare le LIF tra cluster

Configurare le LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Fasi

1. Elencare le porte nel cluster:

   ```
   network port show
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Creazione di LIF intercluster da una SVM di amministrazione (IPSpace predefinito) o da una SVM di sistema (IPSpace personalizzato):

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 e versioni precedenti:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e. `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e. `cluster01_icl02` su `e0c` viene eseguito il failover della porta su `e0d` porta.

```
cluster01::> network interface show -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configurare le LIF di intercluster su porte dedicate

È possibile configurare le LIF tra cluster su porte dedicate. In genere, aumenta la larghezza di banda disponibile per il traffico di replica.

Fasi

1. Elencare le porte nel cluster:

   `network port show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

   `network interface show -fields home-port,curr-port`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte `e0e` e. `e0f` Non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Creare un gruppo di failover per le porte dedicate:

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

Nell'esempio seguente vengono assegnati i port `e0e` e. `e0f` al gruppo di failover `intercluster01` Sul sistema SVM `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verificare che il gruppo di failover sia stato creato:

   `network interface failover-groups show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`

Opzione	Descrizione
In ONTAP 9.5 e versioni precedenti:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover-group` *`failover_group`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e. `cluster01_icl02` nel gruppo di failover `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e. `cluster01_icl02` Su SVM`e0e` viene eseguito il failover della porta su `e0f` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurare le LIF di intercluster in spazi IPpersonalizzati

È possibile configurare le LIF di intercluster in spazi IPpersonalizzati. In questo modo è possibile isolare il traffico di replica in ambienti multitenant.

Quando si crea un IPSpace personalizzato, il sistema crea una SVM (System Storage Virtual Machine) che funge da contenitore per gli oggetti di sistema in tale IPSpace. È possibile utilizzare la nuova SVM come container per qualsiasi LIF di intercluster nel nuovo IPSpace. Il nuovo SVM ha lo stesso nome dell'IPSpace personalizzato.

Fasi

1. Elencare le porte nel cluster:

   `network port show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte di rete in `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Creare spazi IP personalizzati sul cluster:

   `network ipspace create -ipspace` *`ipspace`*

   Nell'esempio seguente viene creato l'IPSpace personalizzato `ipspace-IC1`:

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

3. Determinare quali porte sono disponibili per la comunicazione tra cluster:

   `network interface show -fields home-port,curr-port`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte `e0e` e. `e0f` Non sono stati assegnati LIF:

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01_clus1   e0a       e0a
   Cluster cluster01_clus2   e0b       e0b
   Cluster cluster02_clus1   e0a       e0a
   Cluster cluster02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

4. Rimuovere le porte disponibili dal dominio di trasmissione predefinito:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Una porta non può trovarsi in più di un dominio di trasmissione alla volta. Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono rimosse le porte `e0e` e. `e0f` dal dominio di trasmissione predefinito:

   ```
   cluster01::> network port broadcast-domain remove-ports -broadcast
   -domain Default -ports
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

5. Verificare che le porte siano state rimosse dal dominio di trasmissione predefinito:

   `network port show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le porte `e0e` e. `e0f` sono stati rimossi dal dominio di trasmissione predefinito:

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Creare un dominio di broadcast nell'IPSpace personalizzato:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   Nell'esempio seguente viene creato il dominio di trasmissione `ipspace-IC1-bd` In IPSpace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Verificare che il dominio di trasmissione sia stato creato:

   `network port broadcast-domain show`

   Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name    MTU  Port List                     Status Details
------- ----------- ------  ------------------------------ --------------
Cluster Cluster       9000
                            cluster01-01:e0a              complete
                            cluster01-01:e0b              complete
                            cluster01-02:e0a              complete
                            cluster01-02:e0b              complete
Default Default       1500
                            cluster01-01:e0c              complete
                            cluster01-01:e0d              complete
                            cluster01-01:e0f              complete
                            cluster01-01:e0g              complete
                            cluster01-02:e0c              complete
                            cluster01-02:e0d              complete
                            cluster01-02:e0f              complete
                            cluster01-02:e0g              complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e              complete
                            cluster01-01:e0f              complete
                            cluster01-02:e0e              complete
                            cluster01-02:e0f              complete
```

8. Creare LIF di intercluster sulla SVM di sistema e assegnarle al dominio di trasmissione:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 e versioni precedenti:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

La LIF viene creata nel dominio di trasmissione a cui è assegnata la porta home. Il dominio di broadcast dispone di un gruppo di failover predefinito con lo stesso nome del dominio di broadcast. Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e. `cluster01_icl02` nel dominio di broadcast `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verificare che le LIF dell'intercluster siano state create:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster`

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Verificare che le LIF dell'intercluster siano ridondanti:

Opzione	Descrizione
In ONTAP 9.6 e versioni successive:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 e versioni precedenti:	`network interface show -role intercluster -failover`

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e. `cluster01_icl02` Su SVM `e0e` failover della porta alla porta`e0f`:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurare le relazioni peer

Creare una relazione peer del cluster

È possibile utilizzare `cluster peer create` per creare una relazione peer tra un cluster locale e remoto. Una volta creata la relazione peer, è possibile eseguire `cluster peer create` sul cluster remoto per autenticarlo nel cluster locale.

Prima di iniziare

- È necessario aver creato le LIF di intercluster su ogni nodo dei cluster che vengono sottoposti a peering.
- I cluster devono eseguire ONTAP 9.3 o versione successiva. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in "documento archiviato".)

Fasi

Eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

System Manager

1. Nel cluster locale, fare clic su **Cluster > Impostazioni**.
2. Nella sezione **Impostazioni intercluster**, fare clic su **Aggiungi interfacce di rete** e aggiungere interfacce di rete intercluster per il cluster.

   Ripetere questo passaggio sul cluster remoto.

3. Nel cluster remoto, fare clic su **Cluster > Impostazioni**.
4. Fare clic su ⋮ Nella sezione **Cluster Peers** e selezionare **generate Passphrase**.
5. Selezionare la versione del cluster ONTAP remoto.
6. Copiare la passphrase generata.
7. Nel cluster locale, in **Cluster Peers**, fare clic su ⋮ E selezionare **cluster peer**.
8. Nella finestra **Peer cluster**, incollare la passphrase e fare clic su **Initiate cluster peering**.

CLI

1. Sul cluster di destinazione, creare una relazione peer con il cluster di origine:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS>|1...7days|1...168hours -peer-addrs
   <peer_LIF_IPs > -initial-allowed-vserver-peers <svm_name>|* -ipspace
   <ipspace>
   ```

   Se si specificano entrambi `-generate-passphrase` e. `-peer-addrs`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addrs` può utilizzare la password generata.

   È possibile ignorare `-ipspace` Se non si utilizza un IPSpace personalizzato. Per la sintassi completa dei comandi, vedere la pagina man.

   Se si crea la relazione di peering in ONTAP 9.6 o versione successiva e non si desidera crittografare le comunicazioni di peering tra cluster, è necessario utilizzare `-encryption-protocol-proposed none` opzione per disattivare la crittografia.

   Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM `vs1` e. `vs2` sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Nell'esempio riportato di seguito viene creata una relazione peer del cluster con il cluster remoto agli indirizzi IP LIF 192.140.112.103 e 192.140.112.104 dell'intercluster e viene pre-autorizzata una relazione peer con qualsiasi SVM sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM`vs1` e. `vs2` sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Nel cluster di origine, autenticare il cluster di origine nel cluster di destinazione:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene autenticato il cluster locale nel cluster remoto agli indirizzi IP LIF 192.140.112.101 e 192.140.112.102 dell'intercluster:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Inserire la passphrase per la relazione peer quando richiesto.

3. Verificare che la relazione peer del cluster sia stata creata:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                              Peer Cluster Name: cluster02
                   Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                            Remote Cluster Name: cluster2
                            Active IP Addresses: 192.140.112.101,
192.140.112.102
                          Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Verificare la connettività e lo stato dei nodi nella relazione peer:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

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)	"Preparazione per il mirroring e il vaulting"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica sulla preparazione del disaster recovery dei volumi"

Creare una relazione peer SVM tra cluster

È possibile utilizzare `vserver peer create` Per creare una relazione peer tra SVM su cluster locali e remoti.

Prima di iniziare

- I cluster di origine e di destinazione devono essere peering.
- I cluster devono eseguire ONTAP 9.3. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in "documento archiviato".)
- È necessario disporre di relazioni peer "pre-autorizzate" per le SVM sul cluster remoto.

  Per ulteriori informazioni, vedere "Creazione di una relazione peer del cluster".

A proposito di questa attività

In ONTAP 9,2 e versioni precedenti, puoi autorizzare una relazione di peer per una sola SVM alla volta. Ciò significa che è necessario eseguire `vserver peer accept` Comando ogni volta che autorizzi una relazione peer SVM in sospeso.

A partire da ONTAP 9.3, è possibile "pre-autorizzare" le relazioni peer per più SVM elencando le SVM in `-initial-allowed-vserver` quando si crea una relazione peer del cluster. Per ulteriori informazioni, vedere "Creazione di una relazione peer del cluster".

Fasi

1. Nel cluster di destinazione per la protezione dei dati, visualizzare le SVM pre-autorizzate per il peering:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. Sul cluster di origine per la protezione dei dati, creare una relazione peer con una SVM pre-autorizzata sul cluster di destinazione per la protezione dei dati:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creata una relazione peer tra la SVM locale `pvs1` E la SVM remota pre-autorizzata `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Verificare la relazione peer SVM:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Aggiungere una relazione peer SVM tra cluster

Se si crea una SVM dopo aver configurato una relazione peer del cluster, sarà necessario aggiungere manualmente una relazione peer per la SVM. È possibile utilizzare `vserver peer create` Per creare una relazione peer tra le SVM. Una volta creata la relazione peer, è possibile eseguire `vserver peer accept` sul cluster remoto per autorizzare la relazione peer.

Prima di iniziare

I cluster di origine e di destinazione devono essere peering.

A proposito di questa attività

È possibile creare relazioni peer tra le SVM nello stesso cluster per il backup dei dati locale. Per ulteriori informazioni, consultare `vserver peer create` pagina man.

Gli amministratori utilizzano occasionalmente `vserver peer reject` Comando per rifiutare una relazione peer SVM proposta. Se la relazione tra le SVM si trova in `rejected` state (stato), è necessario eliminare la relazione prima di crearne una nuova. Per ulteriori informazioni, consultare `vserver peer delete` pagina man.

Fasi

1. Nel cluster di origine per la protezione dei dati, creare una relazione peer con una SVM nel cluster di destinazione per la protezione dei dati:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   Nell'esempio seguente viene creata una relazione peer tra la SVM locale`pvs1` E SVM remoto`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Se le SVM locali e remote hanno gli stessi nomi, è necessario utilizzare un *nome locale* per creare la relazione peer SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. Nel cluster di origine per la protezione dei dati, verificare che la relazione peer sia stata avviata:

   `vserver peer show-all`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra che la relazione peer tra SVM`pvs1` E SVM`vs1` è stato avviato:

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster   Applications
--------    --------    ---------  -------------  ------------
pvs1        vs1         initiated   Cluster02       snapmirror
```

3. Sul cluster di destinazione per la protezione dei dati, visualizzare la relazione peer SVM in sospeso:

   `vserver peer show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito sono elencate le relazioni peer in sospeso per `cluster02`:

```
cluster02::> vserver peer show

                   Peer               Peer
Vserver            Vserver            State
-----------        -----------        ------------
vs1                pvs1               pending
```

4. Nel cluster di destinazione per la protezione dei dati, autorizzare la relazione peer in sospeso:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene autorizzata la relazione peer tra la SVM locale `vs1` E SVM remoto `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Verificare la relazione peer SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Abilitare la crittografia del peering del cluster su una relazione peer esistente

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 dei cluster utilizza una chiave precondivisa (PSK) e TLS (Transport Security Layer) per proteggere le comunicazioni di peering tra cluster. Questo aggiunge un ulteriore livello di sicurezza tra i cluster peered.

A proposito di questa attività

Se si aggiornano i cluster peering a ONTAP 9.6 o versione successiva e la relazione di peering è stata creata in ONTAP 9.5 o versione precedente, la crittografia di peering dei cluster deve essere attivata manualmente dopo l'aggiornamento. Entrambi i cluster della relazione di peering devono eseguire ONTAP 9.6 o versione successiva per abilitare la crittografia di peering dei cluster.

Fasi

1. Sul cluster di destinazione, attivare la crittografia per le comunicazioni con il cluster di origine:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Quando richiesto, inserire una passphrase.
3. Nel cluster di origine per la protezione dei dati, abilitare la crittografia per la comunicazione con il cluster di destinazione per la protezione dei dati:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Quando richiesto, inserire la stessa passphrase inserita nel cluster di destinazione.

Rimuovere la crittografia di peering del cluster da una relazione peer esistente

Per impostazione predefinita, la crittografia del peering del cluster è attivata su tutte le relazioni peer create in ONTAP 9.6 o versioni successive. Se non si desidera utilizzare la crittografia per le comunicazioni di peering tra cluster, è possibile disattivarla.

Fasi

1. Nel cluster di destinazione, modificare le comunicazioni con il cluster di origine per interrompere l'utilizzo della crittografia di peering del cluster:
   - Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

     ```
     cluster peer modify _source_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Per rimuovere la crittografia e l'autenticazione, immettere:

     ```
     cluster peer modify _source_cluster_ -auth-status no-authentication
     ```

2. Quando richiesto, inserire una passphrase.
3. Sul cluster di origine, disattivare la crittografia per la comunicazione con il cluster di destinazione:
   - Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

     ```
     cluster peer modify _destination_cluster_ -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Per rimuovere la crittografia e l'autenticazione, immettere:

     ```
     cluster peer modify _destination_cluster_ -auth-status no-
     authentication
     ```

4. Quando richiesto, inserire la stessa passphrase inserita nel cluster di destinazione.

Gestire le copie Snapshot locali

Panoramica sulla gestione delle copie Snapshot locali

Una *copia Snapshot* è un'immagine point-in-time di sola lettura di un volume. L'immagine consuma uno spazio di storage minimo e comporta un overhead delle performance trascurabile, in quanto registra solo le modifiche apportate ai file dall'ultima copia Snapshot.

È possibile utilizzare una copia Snapshot per ripristinare l'intero contenuto di un volume o per ripristinare singoli file o LUN. Le copie Snapshot vengono memorizzate nella directory `.snapshot` sul volume.

In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume FlexVol può contenere fino a 1023 copie Snapshot.

> A partire da ONTAP 9.8, i volumi FlexGroup possono contenere 1023 copie Snapshot. Per ulteriori informazioni, vedere "Proteggere i volumi FlexGroup utilizzando le copie Snapshot".

Configurare policy Snapshot personalizzate

Panoramica sulla configurazione dei criteri Snapshot personalizzati

Una *policy Snapshot* definisce il modo in cui il sistema crea le copie Snapshot. Il criterio specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti e nominare le copie "daily.`timestamp`"

Il criterio predefinito per un volume crea automaticamente le copie Snapshot secondo la seguente pianificazione, con le copie Snapshot meno recenti eliminate per fare spazio alle copie più recenti:

- Un massimo di sei copie Snapshot orarie effettuate cinque minuti dopo l'ora.
- Un massimo di due copie Snapshot giornaliere eseguite da lunedì a sabato a 10 minuti dalla mezzanotte.
- Un massimo di due copie Snapshot settimanali eseguite ogni domenica a 15 minuti dalla mezzanotte.

A meno che non si specifichi un criterio Snapshot quando si crea un volume, il volume eredita il criterio Snapshot associato alla relativa SVM (Storage Virtual Machine).

Quando configurare un criterio Snapshot personalizzato

Se il criterio Snapshot predefinito non è appropriato per un volume, è possibile configurare un criterio personalizzato che modifica la frequenza, la conservazione e il nome delle copie Snapshot. La pianificazione sarà dettata principalmente dalla velocità di cambiamento del file system attivo.

È possibile eseguire il backup di un file system molto utilizzato come un database ogni ora, mentre si eseguono backup di file raramente utilizzati una volta al giorno. Anche per un database, in genere viene eseguito un backup completo una o due volte al giorno, eseguendo il backup dei registri delle transazioni ogni ora.

Altri fattori sono l'importanza dei file per la tua organizzazione, il tuo Service Level Agreement (SLA), il tuo Recovery Point Objective (RPO) e il tuo Recovery Time Objective (RTO). In generale, è necessario conservare solo il numero di copie Snapshot necessario.

Creare una pianificazione del lavoro Snapshot

Una policy Snapshot richiede almeno una pianificazione del lavoro di copia Snapshot. È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo.

A proposito di questa attività

Per impostazione predefinita, ONTAP crea i nomi delle copie Snapshot aggiungendo un indicatore data e ora al nome della pianificazione del processo.

Se si specificano valori per il giorno del mese e il giorno della settimana, i valori vengono considerati indipendentemente. Ad esempio, un programma cron con la specifica del giorno `Friday` e il giorno del mese specificato `13` Viene eseguito ogni venerdì e il 13° giorno di ogni mese, non solo ogni venerdì 13.

Fase

1. Creare una pianificazione del processo:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

   A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

   `job schedule cron create -name job_name -vserver Vserver_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Nell'esempio seguente viene creata una pianificazione del processo denominata `myweekly` Il sabato alle 3:00:

   ```
   cluster1::> job schedule cron create -name myweekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

   Nell'esempio seguente viene creata una pianificazione denominata `myweeklymulti` che specifica più giorni, ore e minuti:

   ```
   job schedule cron create -name myweeklymulti -dayofweek
   "Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
   ```

Creare una policy Snapshot

Un criterio Snapshot specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti e chiamarle "daily. *`timestamp`*" Una policy Snapshot può contenere fino a cinque pianificazioni di lavori.

A proposito di questa attività

Per impostazione predefinita, ONTAP crea i nomi delle copie Snapshot aggiungendo un indicatore data e ora al nome della pianificazione del processo:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Se si preferisce, è possibile sostituire un prefisso con il nome della pianificazione del lavoro.

Il `snapmirror-label` Opzione per la replica di SnapMirror. Per ulteriori informazioni, vedere "Definizione di una regola per un criterio".

Fase

1. Creare una policy Snapshot:

   `volume snapshot policy create -vserver` *`SVM`* `-policy` *`policy_name`* `-enabled true|false -schedule1` *`schedule1_name`* `-count1` *`copies_to_retain`* `-prefix1` *`snapshot_prefix`* `-snapmirror-label1` *`snapshot_label`* … `-schedule5` *`schedule5_name`* `-count5` *`copies_to_retain`*`-prefix5` *`snapshot_prefix`* `-snapmirror-label5` *`snapshot_label`*

   Nell'esempio seguente viene creata una policy Snapshot denominata `snap_policy_daily` che funziona su `daily` pianificazione. Il criterio dispone di un massimo di cinque copie Snapshot, ciascuna con il nome `daily.`*`timestamp`* E l'etichetta SnapMirror `daily`:

   ```
   cluster1::> volume snapshot policy create -vserver vs0 -policy
   snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1 daily
   ```

Gestione manuale delle copie Snapshot

Crea ed elimina copie Snapshot manualmente

Puoi creare copie Snapshot manualmente quando non puoi aspettare la creazione di una copia Snapshot pianificata e puoi eliminare le copie Snapshot quando non sono più necessarie.

Creazione manuale di una copia Snapshot

Puoi creare manualmente una copia Snapshot usando System Manager o l'interfaccia a riga di comando di ONTAP.

System Manager

Fasi

1. Accedere a **archiviazione > volumi** e selezionare la scheda **Snapshot Copies**.
2. Fare clic su + Add .
3. Nella finestra **Aggiungi copia istantanea**, accettare il nome predefinito della copia istantanea o modificarlo, se necessario.
4. **Facoltativo**: Aggiungere un'etichetta SnapMirror.
5. Fare clic su **Aggiungi**.

CLI

1. Creare una copia Snapshot:

   ```
   volume snapshot create -vserver <SVM> -volume <volume> -snapshot
   <snapshot_name>
   ```

Eliminazione manuale di una copia Snapshot

Puoi eliminare manualmente una copia Snapshot usando System Manager o l'interfaccia a riga di comando di ONTAP.

System Manager

Fasi

1. Accedere a **archiviazione > volumi** e selezionare la scheda **Snapshot Copies**.
2. Individuare la copia Snapshot che si desidera eliminare e fare clic su ⋮ E selezionare **Elimina**.
3. Nella finestra **Elimina copia istantanea**, selezionare **Elimina copia istantanea**.
4. Fare clic su **Delete** (Elimina).

CLI

1. Eliminazione di una copia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Gestire la riserva di copie Snapshot

Gestire la panoramica della riserva di copia Snapshot

La *riserva di copia Snapshot* consente di riservare una percentuale di spazio su disco per le copie Snapshot, pari al 5% per impostazione predefinita. Poiché le copie Snapshot utilizzano lo spazio nel file system attivo quando la riserva di copia Snapshot viene esaurita, è possibile aumentare la riserva di copia Snapshot in base alle necessità. In alternativa, è possibile eliminare automaticamente le copie Snapshot quando la riserva è piena.

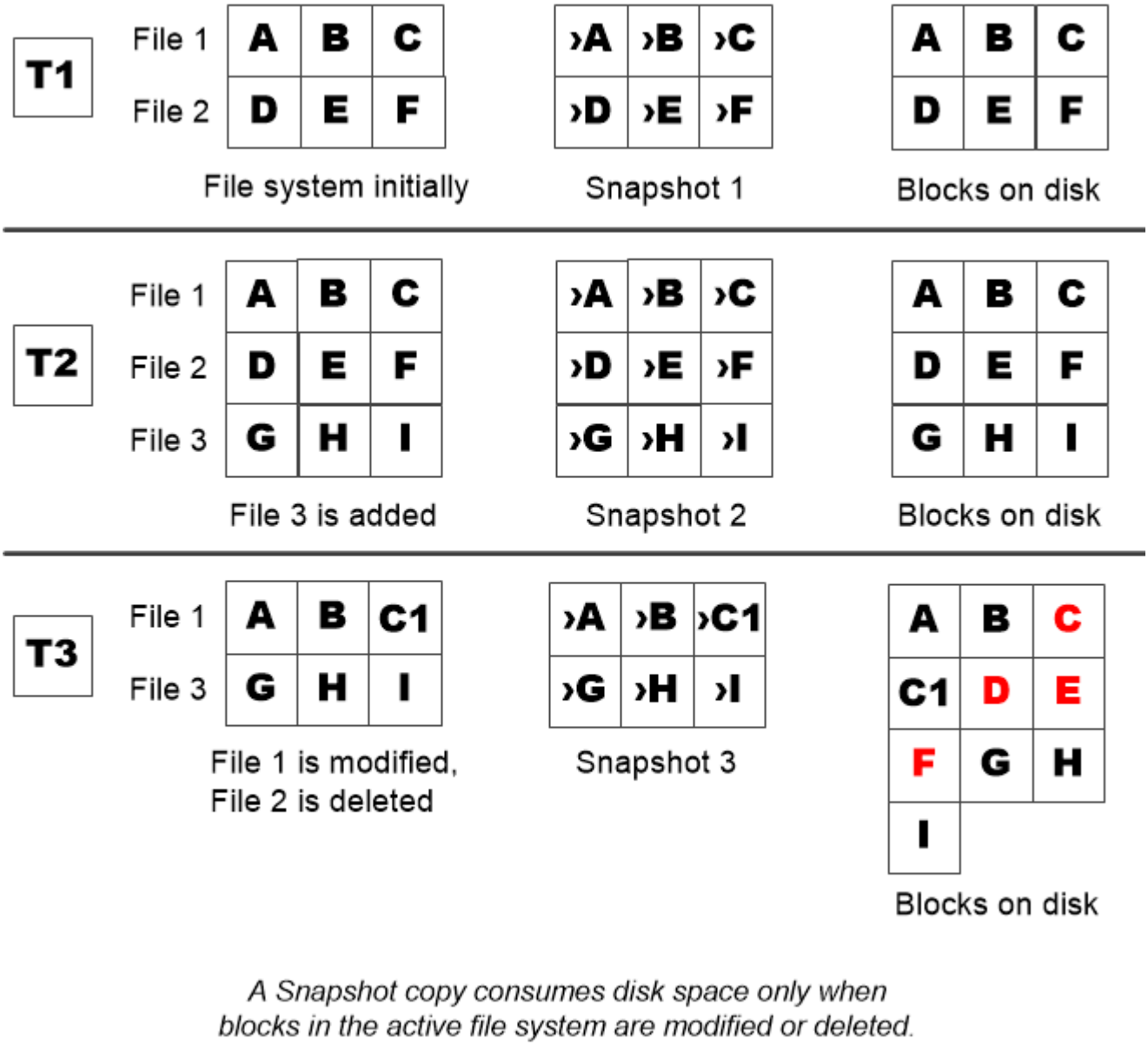
Quando aumentare la riserva di copia Snapshot

Nel decidere se aumentare la riserva Snapshot, è importante ricordare che una copia Snapshot registra solo le modifiche apportate ai file dall'ultima copia Snapshot. Consuma spazio su disco solo quando i blocchi nel file system attivo vengono modificati o cancellati.

Ciò significa che il tasso di cambiamento del file system è il fattore chiave per determinare la quantità di spazio su disco utilizzata dalle copie Snapshot. Indipendentemente dal numero di copie Snapshot create, non consumeranno spazio su disco se il file system attivo non è stato modificato.

Ad esempio, un volume FlexVol contenente registri delle transazioni del database potrebbe avere una riserva di copia Snapshot pari al 20% per tenere conto della maggiore velocità di modifica. Oltre a creare più copie Snapshot per acquisire gli aggiornamenti più frequenti del database, è necessario disporre di una riserva di copie Snapshot più ampia per gestire lo spazio su disco aggiuntivo consumato dalle copie Snapshot.

Una copia Snapshot è costituita da puntatori a blocchi anziché a copie di blocchi. Si può pensare a un puntatore come a “claim” su un blocco: ONTAP “mantiene” il blocco fino a quando la copia Snapshot non viene eliminata.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

In che modo l’eliminazione dei file protetti può ridurre lo spazio dei file rispetto al previsto

Una copia Snapshot punta a un blocco anche dopo aver eliminato il file che ha utilizzato il blocco. Questo spiega perché una riserva di copia Snapshot esaurita potrebbe portare a un risultato controintuitivo in cui l’eliminazione di un intero file system comporta una quantità di spazio disponibile inferiore a quella occupata dal file system.

Si consideri il seguente esempio. Prima di eliminare qualsiasi file, il `df` l’output del comando è il seguente:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Dopo aver eliminato l'intero file system ed eseguito una copia Snapshot del volume, il `df` il comando genera il seguente output:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Come mostra l'output, l'intero 3 GB utilizzato in precedenza dal file system attivo viene ora utilizzato dalle copie Snapshot, oltre ai 0.5 GB utilizzati prima dell'eliminazione.

Poiché lo spazio su disco utilizzato dalle copie Snapshot ora supera la riserva di copia Snapshot, l'overflow di 2.5 GB di "spills" nello spazio riservato ai file attivi, lasciando 0.5 GB di spazio libero per i file in cui si potrebbero ragionevolmente prevedere 3 GB.

Monitorare il consumo dei dischi di copia Snapshot

È possibile monitorare il consumo dei dischi di copia Snapshot utilizzando `df` comando. Il comando visualizza la quantità di spazio libero nel file system attivo e la riserva di copia Snapshot.

Fase

1. Visualizza consumo di dischi di copia Snapshot: `df`

   Il seguente esempio mostra il consumo di dischi di copia Snapshot:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Verificare la riserva di copia Snapshot disponibile su un volume

È possibile verificare la quantità di riserva di copia Snapshot disponibile su un volume utilizzando `snapshot-reserve-available` con il `volume show` comando.

Fase

1. Verificare la riserva di copia Snapshot disponibile su un volume:

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene visualizzata la riserva di copia Snapshot disponibile per `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ -------------------------
vs0     vol1   4.84GB
```

Modificare la riserva di copia Snapshot

È possibile configurare una riserva di copia Snapshot più ampia per impedire alle copie Snapshot di utilizzare lo spazio riservato al file system attivo. È possibile ridurre la riserva di copia Snapshot quando non è più necessario tanto spazio per le copie Snapshot.

Fase

1. Modificare la riserva di copia Snapshot:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-percent-snapshot-space` *`snap_reserve`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene impostata la riserva di copia Snapshot per `vol1` al 10%:

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

Eliminazione automatica delle copie Snapshot

È possibile utilizzare `volume snapshot autodelete modify` Comando per attivare l'eliminazione automatica delle copie Snapshot quando viene superata la riserva Snapshot. Per impostazione predefinita, le copie Snapshot meno recenti vengono eliminate per prime.

A proposito di questa attività

I LUN e i cloni di file vengono cancellati quando non sono più presenti copie Snapshot da eliminare.

Fase

1. Eliminazione automatica delle copie Snapshot:

   `volume snapshot autodelete modify -vserver` *`SVM`* `-volume` *`volume`* `-enabled true|false -trigger volume|snap_reserve`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono eliminate automaticamente le copie Snapshot per `vol1` Quando la riserva

di copia Snapshot è esaurita:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Ripristinare i file dalle copie Snapshot

Ripristinare un file da una copia Snapshot su un client NFS o SMB

Un utente su un client NFS o SMB può ripristinare un file direttamente da una copia Snapshot senza l'intervento di un amministratore del sistema di storage.

Ogni directory del file system contiene una sottodirectory denominata `.snapshot` Accessibile agli utenti NFS e SMB. Il `.snapshot` La sottodirectory contiene le sottodirectory corrispondenti alle copie Snapshot del volume:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Ogni sottodirectory contiene i file a cui fa riferimento la copia Snapshot. Se gli utenti eliminano o sovrascrivono accidentalmente un file, possono ripristinarlo nella directory padre di lettura/scrittura copiandolo dalla sottodirectory Snapshot alla directory di lettura/scrittura:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Abilitare e disabilitare l'accesso dei client NFS e SMB alla directory di copia Snapshot

Per determinare se la directory di copia Snapshot è visibile ai client NFS e SMB per ripristinare un file o un LUN da una copia Snapshot, è possibile attivare e disattivare l'accesso alla directory di copia Snapshot utilizzando `-snapdir-access` opzione di `volume modify` comando.

Fasi

1. Controllare lo stato di accesso alla directory Snapshot:

   `volume show -vserver SVM_name -volume vol_name -fields snapdir-access`

   Esempio:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

2. Attivare o disattivare l'accesso alla directory di copia Snapshot:

   `volume modify -vserver SVM_name -volume vol_name -snapdir-access true|false`

   Il seguente esempio consente l'accesso alla directory di copia Snapshot su vol1:

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

Ripristinare un singolo file da una copia Snapshot

È possibile utilizzare `volume snapshot restore-file` Comando per ripristinare un singolo file o LUN da una copia Snapshot. Se non si desidera sostituire un file esistente, è possibile ripristinare il file in una posizione diversa nel volume di lettura/scrittura padre.

A proposito di questa attività

Se si sta ripristinando un LUN esistente, viene creato un clone del LUN e ne viene eseguito il backup sotto forma di copia Snapshot. Durante l'operazione di ripristino, è possibile leggere e scrivere sul LUN.

I file con flussi vengono ripristinati per impostazione predefinita.

Fasi

1. Elencare le copie Snapshot in un volume:

   `volume snapshot show -vserver SVM -volume volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Ripristinare un file da una copia Snapshot:

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-restore-path` *`destination_path`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene ripristinato il file `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Ripristinare parte di un file da una copia Snapshot

È possibile utilizzare `volume snapshot partial-restore-file` Comando per ripristinare un intervallo di dati da una copia Snapshot a un LUN o a un file container NFS o SMB, presupponendo di conoscere l'offset di byte iniziale dei dati e il numero di byte. È possibile utilizzare questo comando per ripristinare uno dei database su un host che memorizza più database nello stesso LUN.

A partire da ONTAP 9.12.1, il ripristino parziale è disponibile per i volumi in una relazione SM-BC.

Fasi

1. Elencare le copie Snapshot in un volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                 State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Ripristinare parte di un file da una copia Snapshot:

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   L'offset di byte iniziale e il conteggio di byte devono essere multipli di 4,096.

   Nell'esempio seguente vengono ripristinati i primi 4,096 byte del file `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Ripristinare il contenuto di un volume da una copia Snapshot

È possibile utilizzare `volume snapshot restore` Comando per ripristinare il contenuto di un volume da una copia Snapshot.

A proposito di questa attività

Se il volume presenta relazioni SnapMirror, replicare manualmente tutte le copie mirror del volume immediatamente dopo il ripristino da una copia Snapshot. In caso contrario, le copie mirror non possono essere utilizzabili e devono essere eliminate e ricreate.

1. Elencare le copie Snapshot in un volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1  vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Ripristinare il contenuto di un volume da una copia Snapshot:

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   Nell'esempio riportato di seguito viene ripristinato il contenuto di `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1 -snapshot
daily.2013-01-25_0010
```

Replica del volume SnapMirror

Nozioni di base sul disaster recovery asincrono di SnapMirror

SnapMirror è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o *mirror*, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

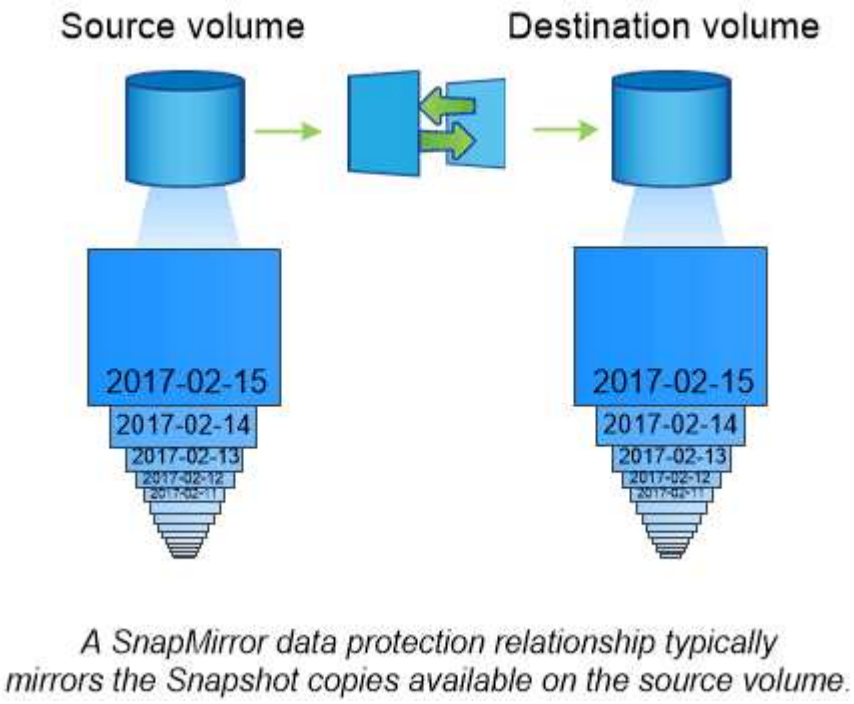
Se il sito primario è ancora disponibile per la fornitura dei dati, è possibile semplicemente trasferire di nuovo i dati necessari e non servire i client dal mirror. Come implica il caso di utilizzo del failover, i controller sul sistema secondario devono essere equivalenti o quasi equivalenti ai controller sul sistema primario per fornire i dati in modo efficiente dallo storage mirrorato.

Relazioni di data Protection

I dati vengono mirrorati a livello di volume. La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene chiamata *relazione di protezione dei dati.* i cluster in cui risiedono i volumi e le SVM che servono i dati dei volumi devono essere *peering.* Una relazione peer consente lo scambio di cluster e SVM dati in modo sicuro.

"Peering di cluster e SVM"

La figura seguente illustra le relazioni di protezione dei dati di SnapMirror.



Ambito delle relazioni di protezione dei dati

È possibile creare una relazione di protezione dei dati direttamente tra i volumi o tra le SVM che possiedono i volumi. In una relazione di protezione dei dati *SVM*, la configurazione SVM completa o parziale, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, viene replicata, così come i dati nei volumi di proprietà di SVM.

È inoltre possibile utilizzare SnapMirror per applicazioni speciali di protezione dei dati:

- Una copia *mirror per la condivisione del carico* del volume root SVM garantisce che i dati rimangano accessibili in caso di interruzione o failover di un nodo.
- Una relazione di protezione dei dati tra *volumi SnapLock* consente di replicare i file WORM sullo storage secondario.

  "Archiviazione e conformità con la tecnologia SnapLock"

- A partire da ONTAP 9.13.1, è possibile utilizzare SnapMirror asincrono per la protezione gruppi di coerenza. A partire da ONTAP 9.14.1, puoi utilizzare SnapMirror asincrono per replicare le snapshot granulari del volume nel cluster di destinazione usando la relazione del gruppo di coerenza. Per ulteriori informazioni, vedere Configurare la protezione asincrona di SnapMirror.

Come vengono inizializzate le relazioni di protezione dei dati di SnapMirror

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. La *policy SnapMirror* per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Trasferimento di riferimento con il criterio predefinito di SnapMirror `MirrorAllSnapshots` prevede i seguenti passaggi:

- Creare una copia Snapshot del volume di origine.

- Trasferire la copia Snapshot e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.
- Trasferire le copie Snapshot rimanenti, meno recenti, sul volume di origine al volume di destinazione per l'utilizzo in caso di danneggiamento del mirror "Active".

Come vengono aggiornate le relazioni di protezione dei dati di SnapMirror

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. La conservazione rispecchia la policy Snapshot sull'origine.

Ad ogni aggiornamento in `MirrorAllSnapshots` SnapMirror crea una copia Snapshot del volume di origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento. Nel seguente output da `snapmirror policy show` comando per `MirrorAllSnapshots` policy, tenere presente quanto segue:

- `Create Snapshot` è "true", a indicare che `MirrorAllSnapshots` Crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- `MirrorAllSnapshots` Dispone delle regole "sm_created" e "all_source_snapshot", che indicano che sia la copia Snapshot creata da SnapMirror che le copie Snapshot eseguite dall'ultimo aggiornamento vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: Asynchronous SnapMirror policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

Policy MirrorLatest

Preconfigurato `MirrorLatest` la policy funziona esattamente come `MirrorAllSnapshots`, Ad eccezione del fatto che solo la copia Snapshot creata da SnapMirror viene trasferita all'inizializzazione e all'aggiornamento.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
```

Nozioni di base sul disaster recovery sincrono di SnapMirror

A partire da ONTAP 9.5, la tecnologia SnapMirror Synchronous (SM-S) è supportata su tutte le piattaforme FAS e AFF con almeno 16 GB di memoria e su tutte le piattaforme ONTAP Select. La tecnologia SnapMirror Synchronous è una funzionalità concessa in licenza per nodo che fornisce la replica sincrona dei dati a livello di volume.

Questa funzionalità soddisfa i requisiti normativi e nazionali per la replica sincrona in settori finanziari, sanitari e altri settori regolamentati in cui non è richiesta alcuna perdita di dati.

Operazioni di SnapMirror Synchronous consentite

Il limite del numero di operazioni di replica sincrona di SnapMirror per coppia ha dipende dal modello di controller.

La tabella seguente elenca il numero di operazioni sincroni di SnapMirror consentite per coppia ha in base al tipo di piattaforma e alla release di ONTAP.

Piattaforma	Versioni precedenti a ONTAP 9.9.1	ONTAP 9.9.1	ONTAP 9.10.1	Da ONTAP 9.11.1 a ONTAP 9.14.1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Funzionalità supportate

La tabella seguente indica le funzionalità supportate con SnapMirror Synchronous e le release ONTAP in cui è disponibile il supporto.

Funzione	Release supportata per la prima volta	Ulteriori informazioni
Antivirus sul volume primario della relazione sincrona di SnapMirror	ONTAP 9.6	
Replica delle copie Snapshot creata dall'applicazione	ONTAP 9.7	Se una copia Snapshot viene contrassegnata con l'etichetta appropriata al momento della `snapshot create` Operazione, utilizzando l'interfaccia CLI o l'API ONTAP, SnapMirror Synchronous replica le copie Snapshot, create dall'utente o con script esterni, dopo aver terminato le applicazioni. Le copie Snapshot pianificate create utilizzando una policy Snapshot non vengono replicate. Per ulteriori informazioni sulla replica delle copie Snapshot create dall'applicazione, consultare l'articolo della Knowledge base: "Come replicare gli snapshot creati dall'applicazione con SnapMirror Synchronous".
Clona eliminazione automatica	ONTAP 9.6	
Gli aggregati FabricPool con policy di tiering Nessuno, Snapshot o Auto sono supportati con origine e destinazione sincrone di SnapMirror.	ONTAP 9.5	Il volume di destinazione in un aggregato FabricPool non può essere impostato su tutti i criteri di tiering.
FC	ONTAP 9.5	Su tutte le reti per le quali la latenza non supera i 10ms ms.
FC-NVMe	ONTAP 9.7	
Cloni dei file	ONTAP 9.7	
FPolicy sul volume primario della relazione sincrona di SnapMirror	ONTAP 9.6	
Quote hard e soft sul volume primario della relazione di SnapMirror Synchronous	ONTAP 9.6	Le regole di quota non vengono replicate nella destinazione, pertanto il database di quota non viene replicato nella destinazione.
Relazioni sincrone all'interno del cluster	ONTAP 9.14.1	L'high Availability viene fornita quando i volumi di origine e destinazione vengono posizionati su diverse coppie ha. In caso di guasto dell'intero cluster, l'accesso ai volumi non sarà possibile fino al ripristino del cluster. Le relazioni sincrone intra-cluster di SnapMirror contribuiranno al limite complessivo della simultaneità Relazioni per coppia ha.
ISCSI	ONTAP 9.5	
Cloni LUN e cloni namespace NVMe	ONTAP 9.7	
Cloni LUN supportati dalle copie Snapshot create dalle applicazioni	ONTAP 9.7	

Accesso al protocollo misto (NFS v3 e SMB)	ONTAP 9.6	
Ripristino NDMP/NDMP	ONTAP 9.13.1	Sia il cluster di origine che quello di destinazione devono eseguire ONTAP 9.13.1 o versione successiva per utilizzare NDMP con SnapMirror Synchronous. Per ulteriori informazioni, vedere Trasferire i dati utilizzando la copia ndmp.
Operazioni sincrone SnapMirror senza interruzioni (NDO) solo su piattaforme AFF/ASA.	ONTAP 9.12.1	Il supporto per operazioni senza interruzioni consente di eseguire molte attività di manutenzione comuni senza pianificare i tempi di inattività. Le operazioni supportate includono takeover e giveback e spostamento del volume, a condizione che un singolo nodo sopravviva tra ciascuno dei due cluster.
NFS v4,2	ONTAP 9.10.1	
NFS v4,3	ONTAP 9.5	
NFS v4.0	ONTAP 9.6	
NFS v4,1	ONTAP 9.6	
NVMe/TCP	9.10.1	
Rimozione della limitazione di frequenza delle operazioni con metadati elevati	ONTAP 9.6	
Sicurezza per i dati sensibili in transito con crittografia TLS 1.2	ONTAP 9.6	
Ripristino di file singoli e file parziale	ONTAP 9.13.1	
SMB 2.0 o versione successiva	ONTAP 9.6	
Cascata del mirror sincrono di SnapMirror	ONTAP 9.6	Il rapporto dal volume di destinazione della relazione di SnapMirror Synchronous deve essere una relazione di SnapMirror asincrono.

Disaster recovery SVM	ONTAP 9.6	* Una fonte di SnapMirror Synchronous può anche essere un'origine di disaster recovery SVM, ad esempio una configurazione fan-out con SnapMirror Synchronous come una tappa e il disaster recovery SVM come l'altra. * Un'origine SnapMirror Synchronous non può essere una destinazione di disaster recovery SVM perché SnapMirror Synchronous non supporta la catena di un'origine di data Protection. È necessario rilasciare la relazione sincrona prima di eseguire la risincronizzazione in caso di disaster recovery delle SVM nel cluster di destinazione. * Una destinazione SnapMirror Synchronous non può essere un'origine di disaster recovery SVM perché il disaster recovery SVM non supporta la replica dei volumi DP. Una risincronizzazione in flip dell'origine sincrona causerebbe il disaster recovery della SVM, escludendo il volume DP nel cluster di destinazione.
Ripristino basato su nastro sul volume di origine	ONTAP 9.13.1	
Parità di timestamp tra volumi di origine e destinazione per NAS	ONTAP 9.6	Se è stato eseguito l'aggiornamento da ONTAP 9,5 a ONTAP 9,6, l'indicatore data e ora viene replicato solo per i file nuovi e modificati nel volume di origine. L'indicatore orario dei file esistenti nel volume di origine non viene sincronizzato.

Funzionalità non supportate

Le seguenti funzionalità non sono supportate con le relazioni di SnapMirror sincrono:

- Gruppi di coerenza
- Sistemi DP_Optimized (DPO)
- Volumi FlexGroup
- Volumi FlexCache
- Rallentamento globale
- In una configurazione fan-out, una sola relazione può essere una relazione sincrona di SnapMirror; tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror.
- Spostamento delle LUN
- Configurazioni MetroCluster
- I LUN di accesso MISTI SAN e NVMe e gli spazi dei nomi NVMe non sono supportati sullo stesso volume o SVM.
- SnapCenter
- Volumi SnapLock
- Copie Snapshot a prova di manomissione

- Backup o ripristino su nastro utilizzando dump e SMTape sul volume di destinazione
- Throughput floor (QoS min) per volumi di origine
- SnapRestore volume
- Vol

Modalità operative

SnapMirror Synchronous dispone di due modalità operative in base al tipo di policy SnapMirror utilizzata:

- **Sync mode** in modalità Sync, le operazioni di i/o dell'applicazione vengono inviate in parallelo ai sistemi di storage primario e secondario. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'applicazione può continuare a scrivere sullo storage primario. Quando la condizione di errore viene corretta, la tecnologia SnapMirror Synchronous risincronizza automaticamente con lo storage secondario e riprende la replica dallo storage primario allo storage secondario in modalità sincrona. In modalità Sync, RPO=0 e RTO sono molto bassi fino a quando non si verifica un errore di replica secondario, in cui RPO e RTO diventano indeterminati, ma pari al tempo necessario per riparare il problema che ha causato il fallimento della replica secondaria e il completamento della risincronizzazione.
- **Modalità StrictSync** SnapMirror Synchronous può funzionare in modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo che lo storage primario e secondario siano identici. L'i/o dell'applicazione verso il primario riprende solo dopo che la relazione SnapMirror ritorna a `InSync` stato. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario, dopo il failover, senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero e l'RTO è molto basso.

Stato della relazione

Lo stato di una relazione sincrona di SnapMirror è sempre in `InSync` stato durante il normale funzionamento. Se il trasferimento di SnapMirror non riesce per qualsiasi motivo, la destinazione non è sincronizzata con l'origine e può andare al `OutofSync` stato.

Per le relazioni sincroni di SnapMirror, il sistema verifica automaticamente lo stato della relazione `InSync` oppure `OutofSync`) a intervalli fissi. Se lo stato della relazione è `OutofSync`, ONTAP attiva automaticamente il processo di risincronizzazione automatica per riportare la relazione a `InSync` stato. La risincronizzazione automatica viene attivata solo se il trasferimento non riesce a causa di un'operazione, ad esempio un failover dello storage non pianificato all'origine o alla destinazione o un'interruzione della rete. Operazioni avviate dall'utente come `snapmirror quiesce` e. `snapmirror break` non attivare la risincronizzazione automatica.

Se lo stato della relazione diventa `OutofSync` Per una relazione sincrona di SnapMirror in modalità StrictSync, tutte le operazioni di i/o sul volume primario vengono interrotte. Il `OutofSync` lo stato per la relazione sincrona di SnapMirror in modalità Sync non è disgregante per il principale e le operazioni di i/o sono consentite sul volume primario.

Informazioni correlate

"Report tecnico NetApp 4733: Configurazione sincrona e Best practice di SnapMirror"

Informazioni sui carichi di lavoro supportati dalle policy di StrictSync e Sync

Le policy StrictSync e Sync supportano tutte le applicazioni basate su LUN con protocolli FC, iSCSI e FC-NVMe, nonché i protocolli NFSv3 e NFSv4 per applicazioni aziendali come database, VMware, quota, SMB e così via. A partire da ONTAP 9.6, SnapMirror

Synchronous può essere utilizzato per i file service aziendali come EDA (Electronic Design Automation), home directory e carichi di lavoro di build del software.

In ONTAP 9.5, per una policy di sincronizzazione, è necessario considerare alcuni aspetti importanti durante la selezione dei carichi di lavoro NFSv3 o NFSv4. La quantità di operazioni di lettura o scrittura dei dati da parte dei carichi di lavoro non è una considerazione, in quanto la policy Sync può gestire elevati carichi di lavoro io in lettura o scrittura. In ONTAP 9.5, i carichi di lavoro che presentano una creazione di file, una creazione di directory, modifiche ai permessi dei file o modifiche ai permessi delle directory eccessive potrebbero non essere adatti (tali carichi di lavoro vengono definiti carichi di lavoro con metadati elevati). Un tipico esempio di workload con metadati elevati è un workload DevOps in cui è possibile creare più file di test, eseguire l'automazione ed eliminare i file. Un altro esempio è rappresentato dal carico di lavoro di creazione parallela che genera più file temporanei durante la compilazione. L'impatto di un elevato tasso di attività di scrittura dei metadati è che può causare la temporanea interruzione della sincronizzazione tra i mirror, che blocca gli iOS di lettura e scrittura dal client.

A partire da ONTAP 9.6, queste limitazioni vengono rimosse e SnapMirror Synchronous può essere utilizzato per i carichi di lavoro dei file service aziendali che includono ambienti multiutente, come home directory e carichi di lavoro di build del software.

Informazioni correlate

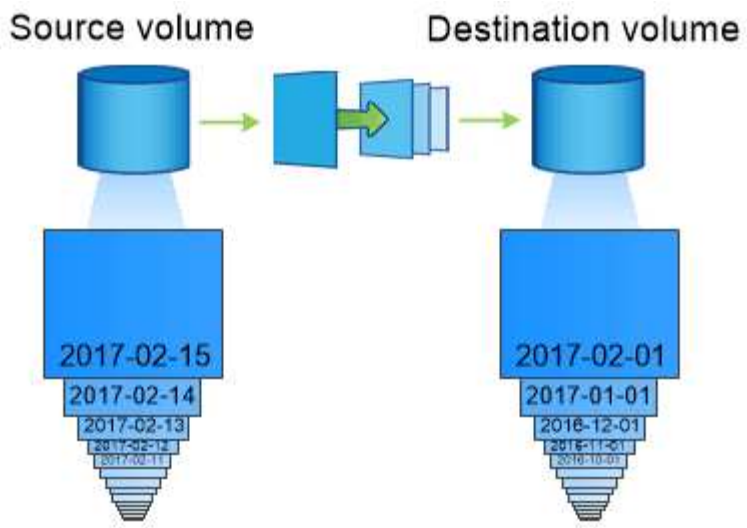
"Procedure consigliate e configurazione sincrona di SnapMirror"

Archiviazione del vault con la tecnologia SnapMirror

I criteri di vault di SnapMirror sostituiscono la tecnologia SnapVault in ONTAP 9.3 e versioni successive. Si utilizza un criterio di vault SnapMirror per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

È possibile conservare copie Snapshot mensili dei dati per un periodo di 20 anni, ad esempio per rispettare le normative contabili governative per la propria azienda. Poiché non è necessario fornire dati dallo storage del vault, è possibile utilizzare dischi più lenti e meno costosi sul sistema di destinazione.

La figura seguente illustra le relazioni di protezione dei dati del vault SnapMirror.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Come vengono inizializzate le relazioni di protezione dei dati del vault

Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento con la policy di default del vault `XDPDefault` Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. A differenza delle relazioni SnapMirror, un backup del vault non include copie Snapshot precedenti nella linea di base.

Come vengono aggiornate le relazioni di protezione dei dati del vault

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. Le regole definite nella policy per la relazione identificano quali nuove copie Snapshot includere negli aggiornamenti e quante copie conservare. Le etichette definite nella policy (“monhly,” ad esempio) devono corrispondere a una o più etichette definite nella policy Snapshot sull’origine. In caso contrario, la replica non riesce.

Ad ogni aggiornamento in `XDPDefault` SnapMirror trasferisce le copie Snapshot eseguite dall’ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri. Nel seguente output da `snapmirror policy show` comando per `XDPDefault` policy, tenere presente quanto segue:

- `Create Snapshot` è “false”, a indicare che `XDPDefault` Non crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- `XDPDefault` Dispone di regole “daily” e “settimanale”, che indicano che tutte le copie Snapshot con etichette corrispondenti sull’origine vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                     Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Nozioni di base sulla replica unificata di SnapMirror

SnapMirror *replica unificata* consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Quando la replica unificata è appropriata, offre vantaggi in termini di riduzione della quantità di storage secondario necessaria, limitazione del numero di trasferimenti di riferimento e riduzione del traffico di rete.

Come vengono inizializzate le relazioni unificate di protezione dei dati

Come con SnapMirror, la protezione unificata dei dati esegue un trasferimento di riferimento la prima volta che lo si richiama. Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento in base alla policy di protezione dei dati unificata predefinita `MirrorAndVault` Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. Come l'archiviazione del vault, la protezione unificata dei dati non include copie Snapshot precedenti nella linea di base.

Come vengono aggiornate le relazioni unificate di protezione dei dati

Ad ogni aggiornamento in `MirrorAndVault` Policy, SnapMirror crea una copia Snapshot del volume di

origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri di Snapshot. Nel seguente output da `snapmirror policy show` comando per `MirrorAndVault` policy, tenere presente quanto segue:

- `Create Snapshot` è "true", a indicare che `MirrorAndVault` Crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- `MirrorAndVault` Dispone delle regole "sm_created", "daily" e "settimanale", che indicano che sia la copia Snapshot creata da SnapMirror che le copie Snapshot con le etichette corrispondenti sull'origine vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified Synchronous SnapMirror and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Politica Unified7year

Preconfigurato `Unified7year` la policy funziona esattamente come `MirrorAndVault`, Ad eccezione del fatto che una quarta regola trasferisce le copie Snapshot mensili e le conserva per sette anni.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
                               daily                   7  false       0 -
-
                               weekly                 52  false       0 -
-
                               monthly                84  false       0 -
-
```

Proteggersi da possibili danneggiamenti dei dati

La replica unificata limita il contenuto del trasferimento di riferimento alla copia Snapshot creata da SnapMirror all'inizializzazione. A ogni aggiornamento, SnapMirror crea un'altra copia Snapshot dell'origine e trasferisce tale copia Snapshot e le nuove copie Snapshot che presentano etichette corrispondenti alle etichette definite nelle regole dei criteri Snapshot.

È possibile proteggersi dalla possibilità che una copia Snapshot aggiornata venga danneggiata creando una copia dell'ultima copia Snapshot trasferita sulla destinazione. Questa "copia locale" viene conservata indipendentemente dalle regole di conservazione sull'origine, in modo che anche se l'istantanea originariamente trasferita da SnapMirror non è più disponibile sull'origine, una copia di essa sarà disponibile sulla destinazione.

Quando utilizzare la replica unificata dei dati

È necessario valutare i vantaggi derivanti dal mantenimento di un mirror completo rispetto ai vantaggi offerti dalla replica unificata nella riduzione della quantità di storage secondario, nella limitazione del numero di trasferimenti di riferimento e nella riduzione del traffico di rete.

Il fattore chiave per determinare l'adeguatezza della replica unificata è il tasso di cambiamento del file system attivo. Un mirror tradizionale potrebbe essere più adatto a un volume che contiene copie Snapshot orarie dei log delle transazioni del database, ad esempio.

XDP sostituisce DP come impostazione predefinita di SnapMirror

A partire da ONTAP 9.3, la modalità XDP (Extended Data Protection) di SnapMirror sostituisce la modalità DP (Data Protection) di SnapMirror come impostazione predefinita.

Prima di eseguire l'aggiornamento a ONTAP 9.12.1, è necessario convertire le relazioni di tipo DP esistenti in XDP prima di poter eseguire l'aggiornamento a ONTAP 9.12.1 e versioni successive. Per ulteriori informazioni, vedere "Convertire una relazione di tipo DP esistente in XDP".

Fino a ONTAP 9.3, SnapMirror invocato in modalità DP e SnapMirror richiamato in modalità XDP utilizzavano diversi motori di replica, con diversi approcci alla dipendenza dalla versione:

- SnapMirror invocato in modalità DP utilizzava un motore di replica *dipendente dalla versione* in cui la

versione di ONTAP doveva essere la stessa sullo storage primario e secondario:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror invocato in modalità XDP utilizzava un motore di replica *version-Flexible* che supportava diverse versioni di ONTAP sullo storage primario e secondario:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Con i miglioramenti delle performance, i benefici significativi di SnapMirror flessibile per la versione superano il leggero vantaggio nel throughput di replica ottenuto con la modalità dipendente dalla versione. Per questo motivo, a partire da ONTAP 9.3, la modalità XDP è stata impostata come nuova impostazione predefinita e tutte le invocazioni della modalità DP sulla riga di comando o in script nuovi o esistenti vengono automaticamente convertite in modalità XDP.

Le relazioni esistenti non vengono influenzate. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. A partire da ONTAP 9.5, MirrorAndVault è il nuovo criterio predefinito quando non viene specificata alcuna modalità di protezione dei dati o quando viene specificata la modalità XDP come tipo di relazione. La tabella seguente mostra il comportamento che ci si può aspettare.

Se si specifica…	Il tipo è…	Il criterio predefinito (se non si specifica un criterio) è…
DP	XDP	MirrorAllSnapshot (DR SnapMirror)
Niente	XDP	MirrorAndVault (replica unificata)
XDP	XDP	MirrorAndVault (replica unificata)

Come mostrato nella tabella, i criteri predefiniti assegnati a XDP in diverse circostanze garantiscono che la conversione mantenga l'equivalenza funzionale dei tipi precedenti. Naturalmente, è possibile utilizzare policy diverse in base alle esigenze, incluse le policy per la replica unificata:

Se si specifica…	E la policy è…	Il risultato è…
DP	MirrorAllSnapshot	Dr. SnapMirror
XDPDefault	SnapVault	MirrorAndVault
Replica unificata	XDP	MirrorAllSnapshot
Dr. SnapMirror	XDPDefault	SnapVault

Le uniche eccezioni alla conversione sono le seguenti:

- Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.3 e versioni precedenti.

  A partire da ONTAP 9.4, le relazioni di protezione dei dati SVM passano per impostazione predefinita alla modalità XDP.

- Le relazioni di protezione dei dati per la condivisione del carico del volume root continuano a essere predefinite in modalità DP.
- Le relazioni di protezione dei dati di SnapLock continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.4 e versioni precedenti.

  A partire da ONTAP 9.5, le relazioni di protezione dei dati di SnapLock passano per impostazione predefinita alla modalità XDP.

- Le invocazioni esplicite di DP continuano a essere predefinite in modalità DP se si imposta la seguente opzione a livello di cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Questa opzione viene ignorata se non si richiama esplicitamente DP.

Quando un volume di destinazione cresce automaticamente

Durante il trasferimento di un mirror per la protezione dei dati, le dimensioni del volume di destinazione aumentano automaticamente se il volume di origine è cresciuto, a condizione che nell'aggregato sia presente spazio disponibile che contiene il volume.

Questo comportamento si verifica indipendentemente da qualsiasi impostazione di crescita automatica sulla destinazione. Non puoi limitare la crescita del volume o impedire a ONTAP di crescere.

Per impostazione predefinita, i volumi di protezione dei dati sono impostati su `grow_shrink` modalità di dimensionamento automatico, che consente al volume di crescere o ridursi in risposta alla quantità di spazio utilizzato. La dimensione automatica massima per i volumi di protezione dei dati è uguale alla dimensione massima FlexVol e dipende dalla piattaforma. Ad esempio:

- FAS6220, volume DP predefinito max-autodize = 70 TB
- FAS8200, volume DP predefinito max-autodize = 100 TB

Per ulteriori informazioni, vedere "NetApp Hardware Universe".

Implementazioni di protezione dei dati fan-out e cascata

È possibile utilizzare un'implementazione *fan-out* per estendere la protezione dei dati a più sistemi secondari. È possibile utilizzare un'implementazione *Cascade* per estendere la protezione dei dati ai sistemi terziari.

Le implementazioni fan-out e cascata supportano qualsiasi combinazione di DR SnapMirror, SnapVault o replica unificata; tuttavia, le relazioni sincrone SnapMirror (supportate a partire da ONTAP 9.5) supportano solo implementazioni fan-out con una o più relazioni SnapMirror asincrone e non supportano implementazioni a cascata. Solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror,

mentre tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror. Continuità aziendale di SnapMirror (Supportato a partire da ONTAP 9.8) supporta anche le configurazioni fan-out.

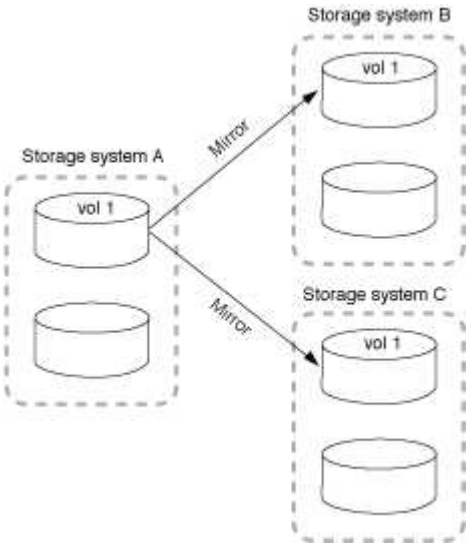
> È possibile utilizzare un'implementazione *fan-in* per creare relazioni di protezione dei dati tra più sistemi primari e un singolo sistema secondario. Ogni relazione deve utilizzare un volume diverso sul sistema secondario.

> Tenere presente che la risincronizzazione dei volumi che fanno parte di una configurazione fan-out o a cascata può richiedere più tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

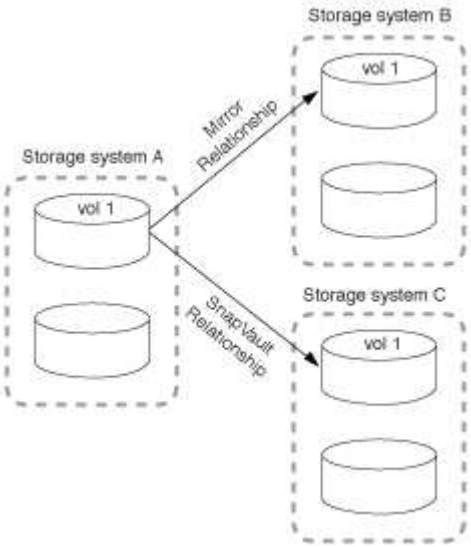
Come funzionano le implementazioni fan-out

SnapMirror supporta le implementazioni fan-out di *mirror multipli* e *mirror-vault*.

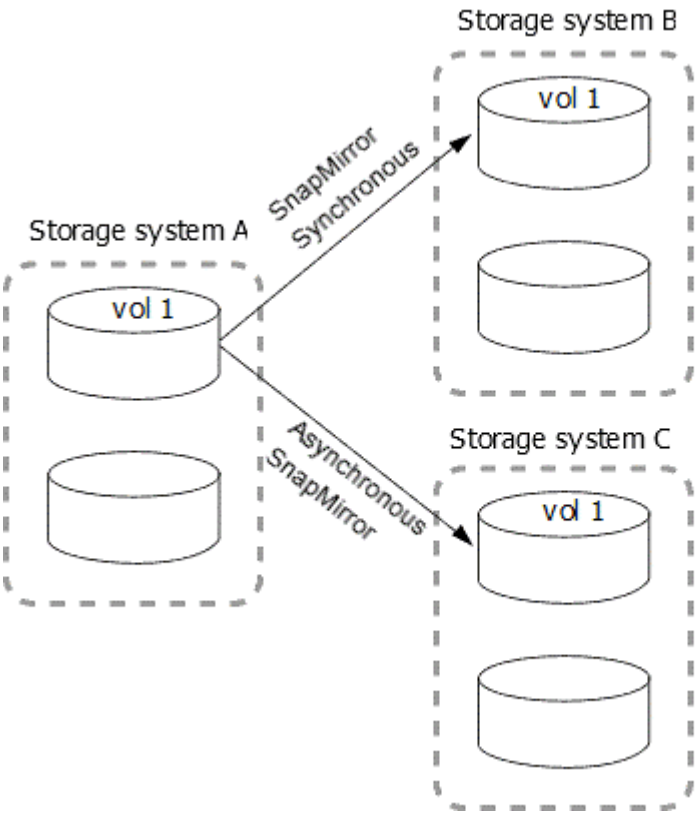
Un'implementazione fan-out con mirror multipli consiste in un volume di origine che ha una relazione di mirroring con più volumi secondari.



Un'implementazione fan-out del vault mirror è costituita da un volume di origine che ha una relazione di mirroring con un volume secondario e una relazione SnapVault con un volume secondario diverso.



A partire da ONTAP 9.5, è possibile avere implementazioni fan-out con relazioni sincrone di SnapMirror; tuttavia, solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror, tutte le altre relazioni dal volume di origine devono essere relazioni asincrone di SnapMirror.

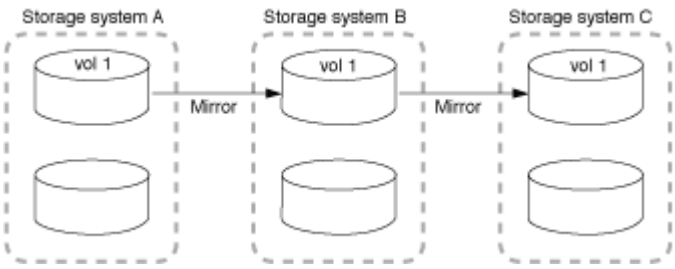


Come funzionano le implementazioni a cascata

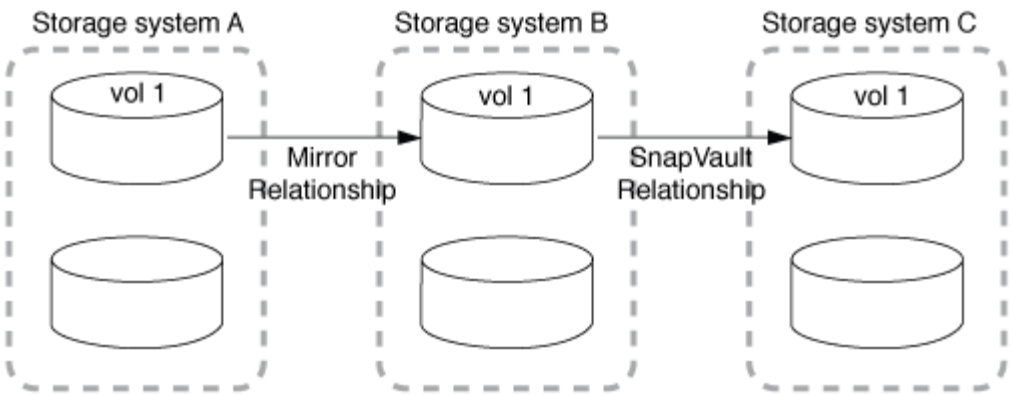
SnapMirror supporta le implementazioni a cascata di *mirror-mirror*, *mirror-vault*, *vault-mirror* e *vault-vault*.

Un'implementazione a cascata di mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene mirrorato su un volume terzo. Se il volume secondario non è più disponibile, è possibile sincronizzare la relazione tra il volume primario e il volume terzo senza eseguire un nuovo trasferimento di riferimento.

A partire da ONTAP 9.6, le relazioni sincroni di SnapMirror sono supportate in una distribuzione a cascata con mirror. Solo i volumi primari e secondari possono trovarsi in una relazione sincrona di SnapMirror. La relazione tra i volumi secondari e i volumi terziari deve essere asincrona.



Un'implementazione a cascata del vault mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene vault su un volume terzo.



Sono supportate anche le implementazioni Vault-Mirror e, a partire da ONTAP 9.2, Vault-Vault Cascade:

- Un'implementazione a cascata del vault-mirror consiste in una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene mirrorato su un volume terzo.
- (A partire da ONTAP 9.2) Una distribuzione a cascata di vault è costituita da una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene vault su un volume terzo.

Ulteriori letture

- Ripristino della protezione in una configurazione fan-out con SM-BC

Licenze SnapMirror

Panoramica sulle licenze di SnapMirror

A partire da ONTAP 9.3, le licenze sono state semplificate per la replica tra istanze di ONTAP. Nelle versioni di ONTAP 9, la licenza SnapMirror supporta le relazioni di vault e mirror. Puoi utilizzare una licenza SnapMirror per supportare la replica ONTAP per casi d'utilizzo di backup e disaster recovery.

Prima della release di ONTAP 9,3, era necessaria una licenza SnapVault separata per configurare le relazioni *vault* tra le istanze di ONTAP, in cui l'istanza DP poteva mantenere un numero più elevato di copie Snapshot per supportare i casi d'utilizzo del backup con tempi di conservazione più lunghi, inoltre, era necessaria una licenza SnapMirror per configurare relazioni *mirror* tra istanze di ONTAP, in cui ciascuna istanza di ONTAP conservava lo stesso numero di copie Snapshot (ovvero un'immagine *mirror*) per supportare i casi d'utilizzo di disaster recovery al fine di rendere possibili i failover dei cluster. Le licenze SnapMirror e SnapVault continuano a essere utilizzate e supportate per le release di ONTAP 8.x e 9.x.

Mentre le licenze SnapVault continuano a funzionare e sono supportate per entrambe le release di ONTAP 8.x e 9.x, la licenza SnapMirror può essere utilizzata al posto di una licenza SnapVault e può essere utilizzata sia per le configurazioni mirror che per quelle del vault.

Per la replica asincrona di ONTAP, a partire da ONTAP 9.3 viene utilizzato un singolo motore di replica unificato per configurare i criteri XDP (Extended Data Protection Mode), in cui la licenza SnapMirror può essere configurata per un criterio mirror, un criterio di vault o un criterio di vault mirror. È necessaria una licenza SnapMirror sia per i cluster di origine che per quelli di destinazione. Se è già installata una licenza SnapVault, non è necessaria alcuna licenza SnapMirror. La licenza perpetua asincrona SnapMirror è inclusa nella suite software ONTAP One installata sui nuovi sistemi AFF e FAS.

I limiti di configurazione per la protezione dei dati vengono determinati in base a diversi fattori, tra cui la

versione di ONTAP, la piattaforma hardware e le licenze installate. Per ulteriori informazioni, vedere "Hardware Universe".

Licenza SnapMirror Synchronous

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. Per creare una relazione sincrona con SnapMirror sono necessarie le seguenti licenze:

- La licenza SnapMirror Synchronous è richiesta sia sul cluster di origine che sul cluster di destinazione.

  La licenza SnapMirror Synchronous è parte di "Suite di licenze ONTAP One".

  Se il sistema è stato acquistato prima di giugno 2019 con un pacchetto Premium o Flash, è possibile scaricare una chiave master NetApp per ottenere la licenza SnapMirror Synchronous richiesta dal sito di supporto NetApp: "Chiavi di licenza master".

- La licenza SnapMirror è richiesta sia sul cluster di origine che sul cluster di destinazione.

Licenza SnapMirror Cloud

A partire da ONTAP 9.8, la licenza di SnapMirror Cloud offre la replica asincrona delle copie Snapshot dalle istanze di ONTAP agli endpoint dello storage a oggetti. Le destinazioni di replica possono essere configurate utilizzando archivi di oggetti on-premise e servizi di storage a oggetti cloud pubblico compatibili con S3 e S3. Le relazioni cloud di SnapMirror sono supportate dai sistemi ONTAP alle destinazioni di storage a oggetti pre-qualificate.

SnapMirror Cloud non è disponibile come licenza standalone. È necessaria una sola licenza per cluster ONTAP. Oltre a una licenza SnapMirror Cloud, è necessaria anche la licenza SnapMirror asincrona.

Per creare una relazione SnapMirror Cloud sono necessarie le seguenti licenze:

- Sia una licenza SnapMirror che una licenza SnapMirror Cloud per la replica direttamente nell'endpoint dell'archivio di oggetti.
- Quando si configura un flusso di lavoro di replica multi-policy (ad esempio, da disco a disco a cloud), è necessaria una licenza SnapMirror su tutte le istanze di ONTAP, mentre la licenza SnapMirror Cloud è richiesta solo per il cluster di origine che esegue la replica direttamente sull'endpoint dello storage a oggetti.

A partire da ONTAP 9,9.1, è possibile "Utilizza System Manager per la replica SnapMirror Cloud".

Un elenco delle applicazioni di terze parti autorizzate di SnapMirror Cloud è pubblicato sul sito Web di NetApp.

Licenza ottimizzata per la protezione dei dati

Le licenze DPO (Data Protection Optimized) non vengono più vendute e il DPO non è supportato sulle piattaforme correnti; tuttavia, se si dispone di una licenza DPO installata su una piattaforma supportata, NetApp continua a fornire supporto fino alla fine della disponibilità di tale piattaforma.

DPO non è incluso nel pacchetto di licenze di ONTAP One e non è possibile eseguire l'aggiornamento al pacchetto di licenze di ONTAP One se la licenza DPO è installata su un sistema.

Per informazioni sulle piattaforme supportate, vedere "Hardware Universe".

Installare le licenze di SnapMirror Cloud

È possibile orchestrare le relazioni con SnapMirror Cloud utilizzando applicazioni di backup di terze parti prequalificate. A partire da ONTAP 9,9.1, puoi anche utilizzare System Manager per orchestrare la replica cloud di SnapMirror. Le licenze di capacità di SnapMirror e SnapMirror Cloud sono necessarie quando si utilizza System Manager per orchestrare ONTAP on-premise ai backup di storage a oggetti. Devi anche richiedere e installare la licenza SnapMirror Cloud API.

A proposito di questa attività

Le licenze di SnapMirror Cloud e S3 SnapMirror sono licenze cluster, non di nodi, quindi *non* vengono fornite con il bundle della licenza di ONTAP One. Queste licenze sono incluse nel pacchetto di compatibilità ONTAP One separato. Per abilitare SnapMirror Cloud, devi richiedere questo bundle.

Inoltre, l'orchestrazione di System Manager dei backup SnapMirror Cloud nello storage a oggetti richiede una chiave SnapMirror Cloud API. Si tratta di una licenza API a singola istanza estesa a tutto il cluster, che non richiede l'installazione su ogni nodo del cluster.

Fasi

Devi richiedere e scaricare il bundle di compatibilità di ONTAP ONE e la licenza API di SnapMirror Cloud, quindi installarli utilizzando System Manager.

1. Individuare e registrare l'UUID del cluster per il cluster che si desidera concedere in licenza.

   L'UUID del cluster è necessario quando invii la richiesta di ordinare il bundle di compatibilità di ONTAP One per il tuo cluster.

2. Contatta il tuo team di vendita NetApp e richiedi il pacchetto compatibilità ONTAP One.
3. Richiedere la licenza SnapMirror Cloud API seguendo le istruzioni fornite sul sito di supporto NetApp.

   "Richiedere la chiave di licenza API di SnapMirror Cloud"

4. Una volta ricevuti e scaricati i file di licenza, utilizzare Gestione sistema per caricare nel cluster la compatibilità cloud NLF di ONTAP e l'API cloud di SnapMirror NLF:
   a. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
   b. Nella finestra **Impostazioni**, fare clic su **licenze**.
   c. Nella finestra **licenze**, fare clic su + Add .
   d. Nella finestra di dialogo **Aggiungi licenza**, fare clic su **Sfoglia** per selezionare l'NLF scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

Informazioni correlate

"Eseguire il backup dei dati nel cloud utilizzando SnapMirror"

"Ricerca licenze software NetApp"

Miglioramenti delle funzionalità dei sistemi DPO

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati aumenta quando viene installata la licenza DP_Optimized (DPO). A partire da ONTAP 9.4, i sistemi con licenza DPO supportano il backoff di SnapMirror, la deduplica in background tra volumi,

l'utilizzo di blocchi Snapshot come donatori e la compattazione.

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati sui sistemi secondari o di protezione dei dati è aumentato, consentendo di scalare fino a 2,500 volumi FlexVol per nodo o fino a 5,000 in modalità di failover. L'aumento dei volumi FlexVol viene abilitato con "Licenza DP_Optimized (DPO)". R "Licenza SnapMirror" è comunque necessario sia sui nodi di origine che su quelli di destinazione.

A partire da ONTAP 9.4, ai sistemi DPO sono stati apportati i seguenti miglioramenti:

- Backoff di SnapMirror: Nei sistemi DPO, al traffico di replica viene assegnata la stessa priorità dei carichi di lavoro client.

  Il backoff di SnapMirror è disattivato per impostazione predefinita nei sistemi DPO.

- Deduplica del volume in background e deduplica del cross-volume in background: La deduplica del volume in background e la deduplica del cross-volume in background sono abilitate nei sistemi DPO.

  È possibile eseguire `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` per deduplicare i dati esistenti. La Best practice consiste nell'eseguire il comando durante le ore di lavoro fuori dalle ore di punta per ridurre l'impatto sulle performance.

- Maggiori risparmi utilizzando i blocchi Snapshot come donatori: I blocchi di dati che non sono disponibili nel file system attivo ma sono intrappolati nelle copie Snapshot vengono utilizzati come donatori per la deduplica dei volumi.

  I nuovi dati possono essere deduplicati con i dati intrappolati nelle copie Snapshot, condividendo efficacemente anche i blocchi Snapshot. L'aumento dello spazio dei donatori offre maggiori risparmi, soprattutto quando il volume dispone di un elevato numero di copie Snapshot.

- Compaction (compattazione): La compattazione dei dati è attivata per impostazione predefinita sui volumi DPO.

Gestire la replica del volume SnapMirror

Workflow di replica di SnapMirror

SnapMirror offre tre tipi di relazione di protezione dei dati: Disaster recovery SnapMirror, archivio (precedentemente noto come SnapVault) e replica unificata. È possibile seguire lo stesso flusso di lavoro di base per configurare ogni tipo di relazione.

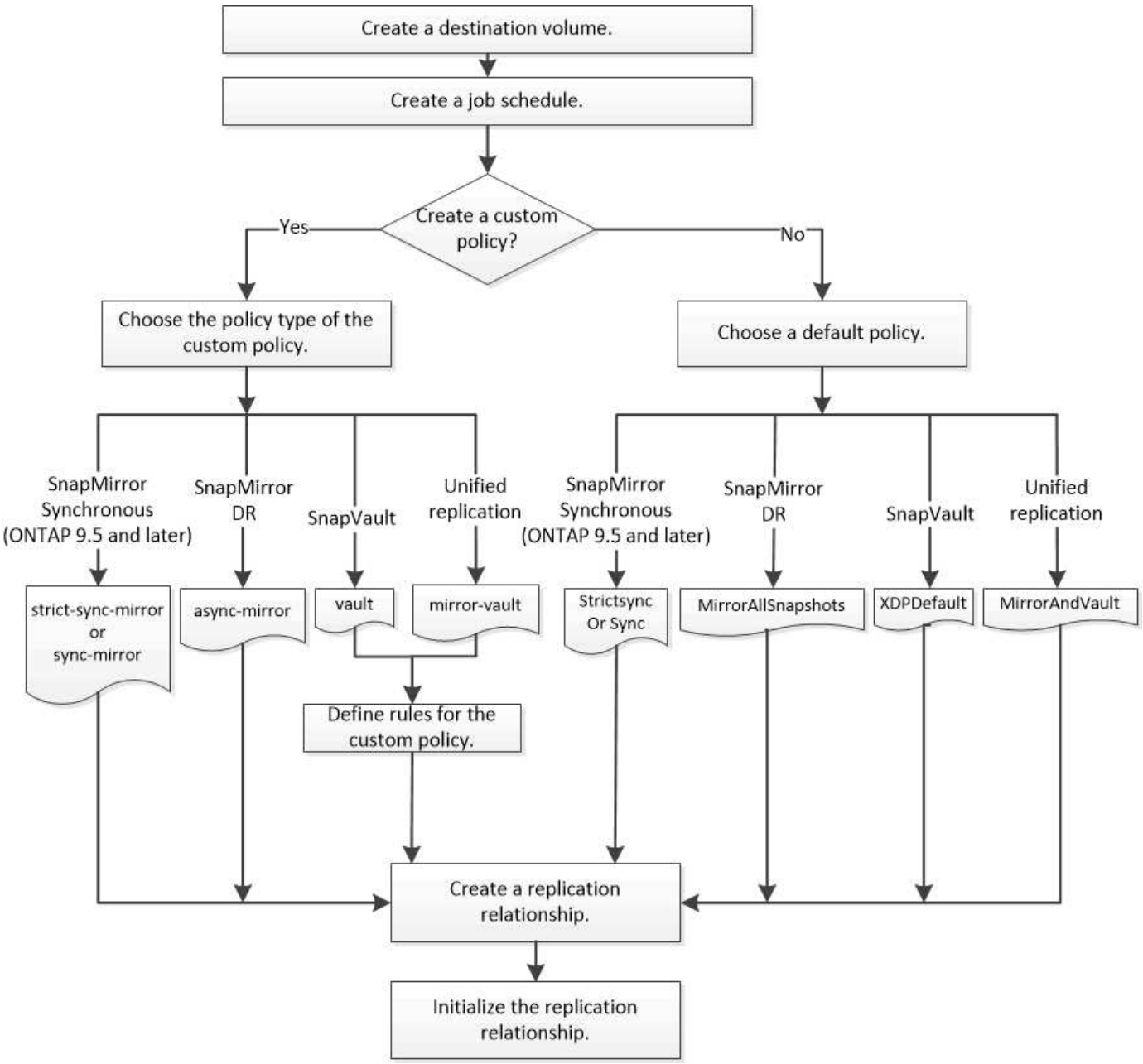
A partire dalla disponibilità generale in ONTAP 9.9.1, la business continuity di SnapMirror (SM-BC) offre un obiettivo di tempo di ripristino zero (RTO zero) o un failover delle applicazioni trasparente (TAF) per consentire il failover automatico delle applicazioni business-critical negli ambienti SAN. SM-BC è supportato in configurazioni con due cluster AFF o due cluster ASA (All-Flash SAN Array).

"Documentazione NetApp: SnapMirror Business Continuity"

Per ogni tipo di relazione di protezione dei dati di SnapMirror, il flusso di lavoro è lo stesso: Creare un volume di destinazione, creare una pianificazione dei processi, specificare una policy, creare e inizializzare la relazione.

A partire da ONTAP 9.3, è possibile utilizzare `snapmirror protect` comando per configurare una relazione

di protezione dei dati in un singolo passaggio. Anche se si utilizza `snapmirror protect`, è necessario comprendere ogni fase del flusso di lavoro.



Configurare una relazione di replica in un'unica fase

A partire da ONTAP 9.3, è possibile utilizzare `snapmirror protect` comando per configurare una relazione di protezione dei dati in un singolo passaggio. Specificare un elenco di volumi da replicare, una SVM sul cluster di destinazione, una pianificazione dei processi e un criterio SnapMirror. `snapmirror protect` fa il resto.

Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

  "Peering di cluster e SVM"

- La lingua del volume di destinazione deve essere la stessa del volume di origine.

A proposito di questa attività

Il `snapmirror protect` Il comando sceglie un aggregato associato alla SVM specificata. Se nessun aggregato è associato alla SVM, sceglie tra tutti gli aggregati del cluster. La scelta dell'aggregato si basa sulla quantità di spazio libero e sul numero di volumi sull'aggregato.

Il `snapmirror protect` il comando esegue quindi le seguenti operazioni:

- Crea un volume di destinazione con un tipo e una quantità di spazio riservato appropriati per ciascun volume nell'elenco di volumi da replicare.
- Configura una relazione di replica appropriata per il criterio specificato.
- Inizializza la relazione.

Il nome del volume di destinazione è del modulo *`source_volume_name_dst`*. In caso di conflitto con un nome esistente, il comando aggiunge un numero al nome del volume. È possibile specificare un prefisso e/o un suffisso nelle opzioni dei comandi. Il suffisso sostituisce quello fornito dal sistema `dst` suffisso.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.

> L'inizializzazione può richiedere molto tempo. `snapmirror protect` non attende il completamento dell'inizializzazione prima del completamento del lavoro. Per questo motivo, è necessario utilizzare `snapmirror show` invece di `job show` comando per determinare quando l'inizializzazione è completa.

A partire da ONTAP 9.5, è possibile creare relazioni sincroni SnapMirror utilizzando `snapmirror protect` comando.

Fase

1. Creare e inizializzare una relazione di replica in un'unica fase:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il `-auto-initialize` l'opzione predefinita è "true".

   Nell'esempio seguente viene creata e inizializzata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

Se preferisci, puoi utilizzare una policy personalizzata. Per ulteriori informazioni, vedere "Creazione di un criterio di replica personalizzato".

Nell'esempio seguente viene creata e inizializzata una relazione SnapVault utilizzando l'impostazione predefinita `XDPDefault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

Nell'esempio seguente viene creata e inizializzata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

Nell'esempio seguente viene creata e inizializzata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `Sync` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

Per SnapVault e le policy di replica unificate, potrebbe essere utile definire una pianificazione per la creazione di una copia dell'ultima copia Snapshot trasferita sulla destinazione. Per ulteriori informazioni, vedere "Definizione di una pianificazione per la creazione di una copia locale sulla destinazione".

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Configurare una relazione di replica un passaggio alla volta

Creare un volume di destinazione

È possibile utilizzare `volume create` sulla destinazione per creare un volume di destinazione. Le dimensioni del volume di destinazione devono essere uguali o superiori a quelle del volume di origine.

Fase

1. Creare un volume di destinazione:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creato un volume di destinazione da 2 GB denominato `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Creare una pianificazione del processo di replica

È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo di replica. La pianificazione del processo determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui viene assegnata la pianificazione.

A proposito di questa attività

Quando si crea una relazione di protezione dei dati, viene assegnata una pianificazione dei processi. Se non si assegna una pianificazione del lavoro, è necessario aggiornare la relazione manualmente.

Fase

1. Creare una pianificazione del processo:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

   A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

   `job schedule cron create -name` *`job_name`* `-vserver` *`Vserver_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   > La pianificazione minima supportata (RPO) per i volumi FlexVol in un volume SnapMirror è di 5 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in un volume SnapMirror è di 30 minuti.

   Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

Personalizzare un criterio di replica

Creare un criterio di replica personalizzato

È possibile creare un criterio di replica personalizzato se il criterio predefinito per una relazione non è adatto. È possibile, ad esempio, comprimere i dati in un trasferimento di rete o modificare il numero di tentativi eseguiti da SnapMirror per trasferire le copie Snapshot.

È possibile utilizzare un criterio predefinito o personalizzato quando si crea una relazione di replica. Per un archivio personalizzato (in precedenza SnapVault) o una policy di replica unificata, è necessario definire una o più *regole* che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento. È inoltre possibile definire una pianificazione per la creazione di copie Snapshot locali sulla destinazione.

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

Tipo di policy	Tipo di relazione
mirror asincrono	Dr. SnapMirror
vault	SnapVault
vault mirror	Replica unificata
mirror di sincronizzazione rigoroso	SnapMirror Synchronous in modalità StrictSync (supportato a partire da ONTAP 9.5)
sync-mirror	SnapMirror Synchronous in modalità Sync (supportato a partire da ONTAP 9.5)

Quando si crea un criterio di replica personalizzato, è consigliabile modellare il criterio dopo un criterio predefinito.

Fase

1. Creare un criterio di replica personalizzato:

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment
   -tries transfer_tries -transfer-priority low|normal -is-network-compression
   -enabled true|false
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia Snapshot comune per le relazioni sincroni di SnapMirror utilizzando `-common-snapshot -schedule` parametro. Per impostazione predefinita, il programma di copia Snapshot comune per le relazioni sincrone di SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia Snapshot per le relazioni sincroni di SnapMirror.

Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che consente la compressione di rete per i trasferimenti di dati:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

Nell'esempio seguente viene creato un criterio di replica personalizzato per SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Nell'esempio seguente viene creato un criterio di replica personalizzato per la relazione sincrona di SnapMirror in modalità StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Al termine

Per i tipi di policy "vault" e "mirror-vault", è necessario definire le regole che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

Utilizzare `snapmirror policy show` Per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina man.

Definire una regola per un criterio

Per le policy personalizzate con il tipo di policy "vault" o "mirror-vault", è necessario definire almeno una regola che determina quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento. È inoltre possibile definire le regole per i criteri di default con il tipo di policy "vault" o "mirror-vault".

A proposito di questa attività

Ogni policy con il tipo di policy "vault" o "mirror-vault" deve avere una regola che specifica quali copie Snapshot replicare. La regola "bimestrale", ad esempio, indica che devono essere replicate solo le copie Snapshot assegnate all'etichetta SnapMirror "bimestrale". Specificare l'etichetta SnapMirror quando si configura il criterio Snapshot sull'origine.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate

automaticamente a un criterio quando si specifica il relativo tipo di criterio. La tabella seguente mostra le regole definite dal sistema.

Regola definita dal sistema	Utilizzato nei tipi di policy	Risultato
sm_created	async-mirror, mirror-vault, Sync, StrictSync	Una copia Snapshot creata da SnapMirror viene trasferita all'inizializzazione e all'aggiornamento.
all_source_snapshot	mirror asincrono	Le nuove copie Snapshot sull'origine vengono trasferite all'inizializzazione e all'aggiornamento.
ogni giorno	vault, vault mirror	Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "daily" vengono trasferite all'inizializzazione e all'aggiornamento.
settimanale	vault, vault mirror	Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "settimanale" vengono trasferite all'inizializzazione e all'aggiornamento.
mensile	vault mirror	Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "mOnhly" vengono trasferite all'inizializzazione e all'aggiornamento.
coerente con l'applicazione	Sync, StrictSync	Le copie Snapshot con l'etichetta SnapMirror "app_coerente" sull'origine vengono replicate in modo sincrono sulla destinazione. Supportato a partire da ONTAP 9.7.

Ad eccezione del tipo di policy "async-mirror", è possibile specificare regole aggiuntive in base alle esigenze, per i criteri predefiniti o personalizzati. Ad esempio:

- Per impostazione predefinita `MirrorAndVault` Policy, è possibile creare una regola chiamata "bimestrale" per associare le copie Snapshot sull'origine con l'etichetta "bimestrale" SnapMirror.
- Per una policy personalizzata con il tipo di policy "mirror-vault", è possibile creare una regola chiamata "bisettimanale" per far corrispondere le copie Snapshot sull'origine con l'etichetta "bisettimanale" SnapMirror.

Fase

1. Definire una regola per un criterio:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-monthly` al valore predefinito `MirrorAndVault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-weekly` al personalizzato `my_snapvault` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `app_consistent` al personalizzato `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

È quindi possibile replicare le copie Snapshot dal cluster di origine che corrispondono a questa etichetta SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Definire una pianificazione per la creazione di una copia locale sulla destinazione

Per le relazioni di replica unificate e SnapVault, è possibile proteggersi dalla possibilità che una copia Snapshot aggiornata venga danneggiata creando una copia dell'ultima copia Snapshot trasferita sulla destinazione. Questa "copia locale" viene conservata indipendentemente dalle regole di conservazione sull'origine, in modo che anche se l'istantanea originariamente trasferita da SnapMirror non è più disponibile sull'origine, una copia di essa sarà disponibile sulla destinazione.

A proposito di questa attività

Specificare la pianificazione per la creazione di una copia locale in `-schedule` opzione di `snapmirror policy add-rule` comando.

Fase

1. Definire una pianificazione per la creazione di una copia locale sulla destinazione:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   Per la sintassi completa dei comandi, vedere la pagina man. Per un esempio su come creare una pianificazione del lavoro, vedere "Creazione di una pianificazione del processo di replica".

   Nell'esempio seguente viene aggiunto un programma per la creazione di una copia locale al valore predefinito `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   Nell'esempio riportato di seguito viene aggiunto un programma per la creazione di una copia locale nel personalizzato `my_unified` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

Creare una relazione di replica

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita *relazione di protezione dei dati.* è possibile utilizzare `snapmirror create` Per creare relazioni di protezione dei dati di replica unificata, SnapVault o DR SnapMirror.

Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

  "Peering di cluster e SVM"

- La lingua del volume di destinazione deve essere la stessa del volume di origine.

A proposito di questa attività

Fino a ONTAP 9.3, SnapMirror invocato in modalità DP e SnapMirror richiamato in modalità XDP utilizzavano diversi motori di replica, con diversi approcci alla dipendenza dalla versione:

- SnapMirror invocato in modalità DP utilizzava un motore di replica *dipendente dalla versione* in cui la versione di ONTAP doveva essere la stessa sullo storage primario e secondario:

  ```
  cluster_dst::>  snapmirror create -type DP -source-path ... -destination
  -path ...
  ```

- SnapMirror invocato in modalità XDP utilizzava un motore di replica *version-Flexible* che supportava diverse versioni di ONTAP sullo storage primario e secondario:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Con i miglioramenti delle performance, i benefici significativi di SnapMirror flessibile per la versione superano il leggero vantaggio nel throughput di replica ottenuto con la modalità dipendente dalla versione. Per questo motivo, a partire da ONTAP 9.3, la modalità XDP è stata impostata come nuova impostazione predefinita e tutte le invocazioni della modalità DP sulla riga di comando o in script nuovi o esistenti vengono automaticamente convertite in modalità XDP.

Le relazioni esistenti non vengono influenzate. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. La tabella seguente mostra il comportamento che ci si può aspettare.

Se si specifica…	Il tipo è…	Il criterio predefinito (se non si specifica un criterio) è…
DP	XDP	MirrorAllSnapshot (DR SnapMirror)
Niente	XDP	MirrorAllSnapshot (DR SnapMirror)
XDP	XDP	XDPDefault (SnapVault)

Vedere anche gli esempi della procedura riportata di seguito.

Le uniche eccezioni alla conversione sono le seguenti:

- Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP.

  Specificare XDP esplicitamente per ottenere la modalità XDP predefinita `MirrorAllSnapshots` policy.

- Le relazioni di protezione dei dati con condivisione del carico continuano a essere impostate per impostazione predefinita sulla modalità DP.
- Le relazioni di protezione dei dati di SnapLock continuano a essere impostate per impostazione predefinita sulla modalità DP.
- Le invocazioni esplicite di DP continuano a essere predefinite in modalità DP se si imposta la seguente opzione a livello di cluster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Questa opzione viene ignorata se non si richiama esplicitamente DP.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror.

Fase

1. Dal cluster di destinazione, creare una relazione di replica:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Il `schedule` Il parametro non è applicabile quando si creano relazioni sincroni di SnapMirror.

   Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorLatest` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   Nell'esempio seguente viene creata una relazione SnapVault utilizzando l'impostazione predefinita `XDPDefault` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination-path
   svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
   ```

   Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando il metodo personalizzato `my_unified` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   my_unified
   ```

   Nell'esempio seguente viene creata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `Sync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

Nell'esempio seguente viene creata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `StrictSync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Con il tipo di DP convertito automaticamente in XDP e senza alcun criterio specificato, il criterio viene automaticamente impostato su `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Se non viene specificato alcun tipo o criterio, il criterio viene impostato automaticamente su `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Se non è stato specificato alcun criterio, il criterio viene impostato automaticamente su `XDPDefault` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

Nell'esempio seguente viene creata una relazione SnapMirror Synchronous con il criterio predefinito `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

> Il criterio predefinito `SnapCenterSync` è di tipo `Sync`. Questo criterio replica qualsiasi copia Snapshot creata con `snapmirror-label` di "app_coerente".

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Informazioni correlate

- "Creazione ed eliminazione di volumi di test del failover SnapMirror".

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"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica del backup del volume con SnapVault"

Inizializzare una relazione di replica

Per tutti i tipi di relazione, l'inizializzazione esegue un *trasferimento baseline*: Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. In caso contrario, il contenuto del trasferimento dipende dalla policy.

Di cosa hai bisogno

I cluster di origine e di destinazione e le SVM devono essere peering.

"Peering di cluster e SVM"

A proposito di questa attività

L'inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror.

Fase

1. Inizializzare una relazione di replica:

   ```
   snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

   Nell'esempio riportato di seguito viene inizializzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Esempio: Configurare una cascata di vault

Un esempio mostra in termini concreti come è possibile configurare le relazioni di replica una fase alla volta. È possibile utilizzare la distribuzione a cascata del vault configurata nell'esempio per conservare più di 251 copie Snapshot etichettate "my-weekly".

Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.
- È necessario eseguire ONTAP 9.2 o versione successiva. Le Cascade del vault non sono supportate nelle versioni precedenti di ONTAP.

A proposito di questa attività

L'esempio presuppone quanto segue:

- Le copie Snapshot sono state configurate sul cluster di origine con le etichette SnapMirror "my-daily", "my-weekly" e "my-monthly".
- Sono stati configurati volumi di destinazione denominati "Vola" nei cluster di destinazione secondari e terziari.
- Sono state configurate le pianificazioni dei processi di replica denominate "my_snapvault" sui cluster di destinazione secondari e terziari.

L'esempio mostra come creare relazioni di replica in base a due criteri personalizzati:

- Il criterio "snapvault_secondary" conserva 7 copie Snapshot giornaliere, 52 settimanali e 180 mensili sul cluster di destinazione secondario.
- La "snapvault_terzo policy" conserva 250 copie Snapshot settimanali sul cluster di destinazione terzo.

Fasi

1. Sul cluster di destinazione secondario, creare il criterio "snapvault_secondary":

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment "Policy on secondary for vault to vault cascade" -vserver
   svm_secondary
   ```

2. Nel cluster di destinazione secondario, definire la regola "y-daily `m`" per la policy:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. Nel cluster di destinazione secondario, definire la regola "my-weekly" per il criterio:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. Nel cluster di destinazione secondario, definire la regola "my-monthly" per il criterio:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. Sul cluster di destinazione secondario, verificare la policy:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                     Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. Sul cluster di destinazione secondario, creare la relazione con il cluster di origine:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. Nel cluster di destinazione secondario, inizializzare la relazione con il cluster di origine:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. Nel cluster di destinazione terzo, creare il criterio “snapvault_terzo”:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment “Policy on tertiary for vault to vault cascade” -vserver
svm_tertiary
```

9. Nel cluster di destinazione terzo, definire la regola “my-weekly” per la policy:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. Nel cluster di destinazione terzo, verificare la policy:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                      Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. Nel cluster di destinazione terzo, creare la relazione con il cluster secondario:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. Nel cluster di destinazione terzo, inizializzare la relazione con il cluster secondario:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Convertire una relazione di tipo DP esistente in XDP

Se si esegue l'aggiornamento a ONTAP 9.12.1 o versioni successive, è necessario convertire le relazioni di tipo DP in XDP prima di eseguire l'aggiornamento. ONTAP 9.12.1 e versioni successive non supportano le relazioni di tipo DP. È possibile convertire facilmente una relazione di tipo DP esistente in XDP per sfruttare SnapMirror flessibile in versione.

A proposito di questa attività

- SnapMirror non converte automaticamente le relazioni di tipo DP esistenti in XDP. Per convertire la relazione, è necessario interrompere ed eliminare la relazione esistente, creare una nuova relazione XDP

e risincronizzare la relazione. Per informazioni generali, vedere "XDP sostituisce DP come impostazione predefinita di SnapMirror".

- Durante la pianificazione della conversione, è necessario tenere presente che la preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

> Dopo aver convertito un tipo di relazione SnapMirror da DP a XDP, le impostazioni relative allo spazio, come la dimensione automatica e la garanzia dello spazio, non vengono più replicate nella destinazione.

Fasi

1. Dal cluster di destinazione, assicurarsi che la relazione SnapMirror sia di tipo DP, che lo stato del mirror sia SnapMirrored, che lo stato della relazione sia inattivo e che la relazione sia integra:

```
snapmirror show -destination-path <SVM:volume>
```

L'esempio seguente mostra l'output di `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

> Potrebbe essere utile conservare una copia di `snapmirror show` output dei comandi per tenere traccia delle impostazioni delle relazioni esistenti.

2. Dai volumi di origine e di destinazione, assicurarsi che entrambi i volumi dispongano di una copia Snapshot comune:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Nell’esempio riportato di seguito viene illustrato il `volume snapshot show` output per i volumi di origine e di destinazione:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Per garantire che gli aggiornamenti pianificati non vengano eseguiti durante la conversione, interrompere la relazione DP-type esistente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Per la sintassi completa dei comandi, vedere "pagina man".

> È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene meno la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

4. Interrompere la relazione di tipo DP esistente:

```
snapmirror break -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere "pagina man".

> È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

5. Se l'eliminazione automatica delle copie Snapshot è attivata sul volume di destinazione, disattivarla:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

Nell'esempio seguente viene disattivata l'eliminazione automatica della copia Snapshot sul volume di destinazione `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Eliminare la relazione DP-type esistente:

```
snapmirror delete -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere "pagina man".

> È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Rilasciare la relazione di disaster recovery della SVM di origine sull'origine:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

L'esempio seguente rilascia la relazione di disaster recovery della SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

8. È possibile utilizzare l'output conservato da `snapmirror show` Comando per creare la nuova relazione XDP-type:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

La nuova relazione deve utilizzare lo stesso volume di origine e di destinazione. Per la sintassi completa dei comandi, vedere la pagina man.

> È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

L'esempio seguente crea una relazione di disaster recovery SnapMirror tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup` utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Per migliorare il tempo di risincronizzazione, è possibile utilizzare `-quick-resync` tuttavia, è importante tenere presente che i risparmi in termini di efficienza dello storage possono andare persi. Per la sintassi completa dei comandi, vedere la pagina man: "Comando di risync di SnapMirror".

> È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

10. Se l'eliminazione automatica delle copie Snapshot è stata disattivata, riattivarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Al termine

1. Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror.
2. Quando il volume di destinazione SnapMirror XDP inizia ad aggiornare le copie Snapshot come definito dalla policy SnapMirror, utilizzare l'output di `snapmirror list-destinations` Dal cluster di origine per visualizzare la nuova relazione SnapMirror XDP.

Convertire il tipo di relazione SnapMirror

A partire da ONTAP 9.5, SnapMirror Synchronous è supportato. È possibile convertire una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous o viceversa senza eseguire un trasferimento di riferimento.

A proposito di questa attività

Non è possibile convertire una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous o viceversa modificando il criterio SnapMirror

Fasi

- **Conversione di una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous**

  a. Dal cluster di destinazione, eliminare la relazione SnapMirror asincrona:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

b. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. Dal cluster di destinazione, creare una relazione sincrona SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
dest_SVM:dest_volume -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. Risincronizzare la relazione sincrona di SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Conversione di una relazione SnapMirror Synchronous in una relazione SnapMirror asincrona**

a. Dal cluster di destinazione, interrompere la relazione sincrona di SnapMirror esistente:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. Dal cluster di destinazione, eliminare la relazione SnapMirror asincrona:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path
```

dest_SVM:dest_volume

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. Dal cluster di destinazione, creare una relazione SnapMirror asincrona:

   `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path` *`dest_SVM:dest_volume`* `-policy MirrorAllSnapshots`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Risincronizzare la relazione sincrona di SnapMirror:

   `snapmirror resync -destination-path` *`dest_SVM:dest_volume`*

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Convertire la modalità di una relazione sincrona SnapMirror

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. È possibile convertire la modalità di una relazione sincrona SnapMirror da StrictSync a Sync o viceversa.

A proposito di questa attività

Non è possibile modificare il criterio di una relazione sincrona di SnapMirror per convertirne la modalità.

Fasi

1. Dal cluster di destinazione, interrompere la relazione sincrona di SnapMirror esistente:

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. Dal cluster di destinazione, eliminare la relazione sincrona SnapMirror esistente:

   `snapmirror delete -destination-path dest_SVM:dest_volume`

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. Dal cluster di destinazione, creare una relazione sincrona di SnapMirror specificando la modalità in cui si desidera convertire la relazione sincrona di SnapMirror:

```
snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume
-policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. Dal cluster di destinazione, risincronizzare la relazione SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

Creazione ed eliminazione di volumi di test del failover SnapMirror

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per creare un clone del volume per verificare il failover e il disaster recovery di SnapMirror, senza interrompere la relazione di SnapMirror attiva. Al termine del test, è possibile cancellare i dati associati ed eliminare il volume del test.

Creazione di un volume di test del failover SnapMirror

A proposito di questa attività

- È possibile eseguire test di failover su relazioni SnapMirror sincrone e asincrone.
- Viene creato un clone del volume per eseguire il test di disaster recovery.
- Il volume clone viene creato sulla stessa macchina virtuale di storage della destinazione SnapMirror.
- Puoi utilizzare relazioni di SnapMirror di FlexVol e FlexGroup.
- Se esiste già un clone di test per la relazione selezionata, non è possibile creare un altro clone per tale relazione.
- Le relazioni del vault di SnapLock non sono supportate.

Prima di iniziare

- Devi essere un amministratore del cluster.
- La licenza SnapMirror deve essere installata sul cluster di origine e destinazione.

Fasi

1. Nel cluster di destinazione, selezionare **protezione > Relazioni**.
2. Selezionare ⋮ Accanto all'origine della relazione e scegliere **Test failover**.
3. Nella finestra **Test failover**, selezionare **Test failover**.
4. Selezionare **Storage > Volumes** (archiviazione > volumi*) e verificare che il volume di failover di prova sia elencato.
5. Selezionare **Storage > Share** (archiviazione > Condividi).
6. Fare clic su + Add E scegliere **Condividi**.
7. Nella finestra **Aggiungi condivisione**, digitare un nome per la condivisione nel campo **Nome condivisione**.
8. Nel campo **cartella**, selezionare **Sfoglia**, selezionare il volume del clone di test e **Salva**.
9. Nella parte inferiore della finestra **Aggiungi condivisione**, scegliere **Salva**.
10. Aprire la condivisione sul client e verificare che il volume di prova disponga di capacità di lettura e scrittura.

Pulire i dati di failover ed eliminare il volume di test

Una volta completato il test di failover, è possibile cancellare tutti i dati associati al volume di test ed eliminarlo.

Fasi

1. Nel cluster di destinazione, selezionare **protezione > Relazioni**.
2. Selezionare ⋮ Accanto all'origine della relazione e scegliere **Clean Up Test failover**.
3. Nella finestra **Clean Up Test failover**, selezionare **Clean Up**.
4. Selezionare **archiviazione > volumi** e verificare che il volume di prova sia stato eliminato.

Fornire i dati da un volume di destinazione DR SnapMirror

Rendere il volume di destinazione scrivibile

È necessario rendere il volume di destinazione scrivibile prima di poter inviare i dati dal volume ai client. È possibile utilizzare `snapmirror quiesce` per arrestare i trasferimenti pianificati verso la destinazione, il `snapmirror abort` per interrompere i trasferimenti in corso e il `snapmirror break` per rendere la destinazione scrivibile.

A proposito di questa attività

È necessario eseguire questa attività dalla SVM di destinazione o dal cluster di destinazione.

Fasi

1. Interrompere i trasferimenti pianificati verso la destinazione:

   ```
   snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

2. Interrompere i trasferimenti in corso verso la destinazione:

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Questo passaggio non è necessario per le relazioni sincroni di SnapMirror (supportate a partire da ONTAP 9.5).

   Nell'esempio seguente vengono interrompiti i trasferimenti in corso tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

3. Interrompere la relazione di disaster recovery di SnapMirror:

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene spezzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
svm_backup:volA_dst
```

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"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica sul disaster recovery dei volumi"

Configurare il volume di destinazione per l'accesso ai dati

Una volta reso scrivibile il volume di destinazione, è necessario configurare il volume per l'accesso ai dati. I client NAS, il sottosistema NVMe e gli host SAN possono accedere ai dati dal volume di destinazione fino alla riattivazione del volume di origine.

Ambiente NAS:

1. Montare il volume NAS nello spazio dei nomi utilizzando lo stesso percorso di giunzione in cui è stato montato il volume di origine nella SVM di origine.
2. Applicare gli ACL appropriati alle condivisioni SMB del volume di destinazione.
3. Assegnare i criteri di esportazione NFS al volume di destinazione.
4. Applicare le regole di quota al volume di destinazione.
5. Reindirizzare i client al volume di destinazione.
6. Rimontare le condivisioni NFS e SMB sui client.

Ambiente SAN:

1. Mappare le LUN nel volume al gruppo iniziatore appropriato.
2. Per iSCSI, creare sessioni iSCSI dagli iniziatori host SAN alle LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dello storage per rilevare i LUN connessi.

Per informazioni sull'ambiente NVMe, vedere "Amministrazione SAN".

Riattivare il volume di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

A proposito di questa attività

- La procedura riportata di seguito presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.
- La preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

Fasi

1. Invertire la relazione di protezione dei dati originale:

   ```
   snapmirror resync -source-path SVM:volume -destination-path SVM:volume
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta. Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

   Nell'esempio seguente viene invertita la relazione tra il volume di origine originale, `volA` acceso `svm1`e il volume da cui vengono forniti i dati, `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

2. Quando si è pronti a ristabilire l'accesso ai dati all'origine originale, interrompere l'accesso al volume di destinazione originale. Un modo per farlo è arrestare la SVM di destinazione originale:

   `vserver stop -vserver SVM`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di destinazione originale o dal cluster di destinazione originale. Questo comando interrompe l'accesso dell'utente all'intera SVM di destinazione originale. È possibile interrompere l'accesso al volume di destinazione originale utilizzando altri metodi.

   Nell'esempio seguente viene interrotta la SVM di destinazione originale:

```
cluster_dst::> vserver stop svm_backup
```

3. Aggiornare la relazione inversa:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

   Nell'esempio riportato di seguito viene aggiornata la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst` acceso `svm_backup`e il volume di origine originale, `volA` acceso `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

4. Dalla SVM di origine originale o dal cluster di origine originale, interrompere i trasferimenti pianificati per la relazione invertita:

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra il volume di destinazione originale, `volA_dst` acceso `svm_backup`e il volume di origine originale, `volA` acceso `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

5. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Eseguire questo comando dalla SVM di origine o dal cluster di origine.

   L'esempio seguente interrompe la relazione tra il volume di destinazione originale, `volA_dst` acceso `svm_backup`e il volume di origine originale, `volA` acceso `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

6. Dalla SVM di origine originale o dal cluster di origine originale, eliminare la relazione di protezione dei dati invertita:

   `snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

   Nell'esempio seguente viene eliminata la relazione inversa tra il volume di origine originale, `volA` acceso `svm1`e il volume da cui vengono forniti i dati, `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

7. Rilasciare la relazione invertita dalla SVM di destinazione originale o dal cluster di destinazione originale.

   `snapmirror release -source-path SVM:volume -destination-path SVM:volume`

   > È necessario eseguire questo comando dalla SVM di destinazione originale o dal cluster di destinazione originale.

   Nell'esempio seguente viene rilasciata la relazione inversa tra il volume di destinazione originale, `volA_dst` acceso `svm_backup`e il volume di origine originale, `volA` acceso `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

8. Ristabilire la relazione di protezione dei dati originale dalla destinazione originale:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene ristabilita la relazione tra il volume di origine originale, `volA` acceso `svm1`e il volume di destinazione originale, `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

9. Se necessario, avviare la SVM di destinazione originale:

   `vserver start -vserver` *`SVM`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene avviata la SVM di destinazione originale:

```
cluster_dst::> vserver start svm_backup
```

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Ripristinare i file da un volume di destinazione SnapMirror

Ripristinare un singolo file, LUN o spazio dei nomi NVMe da una destinazione SnapMirror

È possibile ripristinare un singolo file, LUN, un set di file o LUN da una copia Snapshot o uno spazio dei nomi NVMe da un volume di destinazione SnapMirror. A partire da ONTAP 9.7, è anche possibile ripristinare gli spazi dei nomi NVMe da una destinazione sincrona SnapMirror. È possibile ripristinare i file nel volume di origine originale o in un volume diverso.

Di cosa hai bisogno

Per ripristinare un file o un LUN da una destinazione sincrona SnapMirror (supportata a partire da ONTAP 9.5), è necessario prima eliminare e rilasciare la relazione.

A proposito di questa attività

Il volume su cui si ripristinano file o LUN (il volume di destinazione) deve essere un volume di lettura/scrittura:

- SnapMirror esegue un *ripristino incrementale* se i volumi di origine e di destinazione dispongono di una copia Snapshot comune (come in genere avviene quando si esegue il ripristino nel volume di origine originale).
- In caso contrario, SnapMirror esegue un *ripristino baseline*, in cui la copia Snapshot specificata e tutti i blocchi di dati a cui fa riferimento vengono trasferiti al volume di destinazione.

Fasi

1. Elencare le copie Snapshot nel volume di destinazione:

   `volume snapshot show -vserver SVM -volume volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito vengono illustrate le copie Snapshot di `vserverB:secondary1` destinazione:

   ```
   cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

   Vserver     Volume      Snapshot                State    Size  Total%
   Used%
   -------     ------      ---------- ----------- ------   -----  ------
   -----
   vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
   0%
                           daily.2013-01-25_0010   valid   92KB      0%
   0%
                           hourly.2013-01-25_0105  valid   228KB     0%
   0%
                           hourly.2013-01-25_0205  valid   236KB     0%
   0%
                           hourly.2013-01-25_0305  valid   244KB     0%
   0%
                           hourly.2013-01-25_0405  valid   244KB     0%
   0%
                           hourly.2013-01-25_0505  valid   244KB     0%
   0%

   7 entries were displayed.
   ```

2. Ripristinare un singolo file o LUN o un set di file o LUN da una copia Snapshot in un volume di destinazione SnapMirror:

   `snapmirror restore -source-path SVM:volume|cluster://SVM/volume, … -destination-path SVM:volume|cluster://SVM/volume, … -source-snapshot snapshot -file-list source_file_path,@destination_file_path`

   Per la sintassi completa dei comandi, vedere la pagina man.

È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Il seguente comando ripristina i file `file1` e. `file2` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, nella stessa posizione nel file system attivo del volume di origine originale `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Il seguente comando ripristina i file `file1` e. `file2` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, in una posizione diversa nel file system attivo del volume di origine originale `primary1`.

Il percorso del file di destinazione inizia con il simbolo @ seguito dal percorso del file dalla directory principale del volume di origine originale. In questo esempio, `file1` viene ripristinato a. `/dir1/file1.new` e il file2 viene ripristinato a. `/dir2.new/file2` acceso `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Il seguente comando ripristina i file `file1` e. `file3` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, in posizioni diverse nel file system attivo del volume di origine originale `primary1`e ripristini `file2` da `snap1` nella stessa posizione nel file system attivo di `primary1`.

In questo esempio, il file `file1` viene ripristinato a. `/dir1/file1.new` e. `file3` viene ripristinato a. `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Ripristinare il contenuto di un volume da una destinazione SnapMirror

È possibile ripristinare il contenuto di un intero volume da una copia Snapshot in un volume di destinazione SnapMirror. È possibile ripristinare il contenuto del volume nel volume di origine originale o in un volume diverso.

A proposito di questa attività

Il volume di destinazione per l'operazione di ripristino deve essere uno dei seguenti:

- Un volume di lettura/scrittura, nel qual caso SnapMirror esegue un *ripristino incrementale*, a condizione che i volumi di origine e di destinazione dispongano di una copia Snapshot comune (come accade generalmente quando si esegue il ripristino nel volume di origine originale).

  > Il comando non riesce se non esiste una copia Snapshot comune. Non è possibile ripristinare il contenuto di un volume su un volume vuoto in lettura/scrittura.

- Un volume di protezione dei dati vuoto, nel qual caso SnapMirror esegue un *ripristino baseline*, in cui la copia Snapshot specificata e tutti i blocchi di dati a cui fa riferimento vengono trasferiti al volume di origine.

Il ripristino del contenuto di un volume è un'operazione che comporta interruzioni. Il traffico SMB non deve essere in esecuzione sul volume primario SnapVault quando è in esecuzione un'operazione di ripristino.

Se la compressione del volume di destinazione per l'operazione di ripristino è attivata e la compressione del volume di origine non è attivata, disattivare la compressione sul volume di destinazione. Al termine dell'operazione di ripristino, è necessario riattivare la compressione.

Tutte le regole di quota definite per il volume di destinazione vengono disattivate prima di eseguire il ripristino. È possibile utilizzare `volume quota modify` comando per riattivare le regole di quota al termine dell'operazione di ripristino.

Fasi

1. Elencare le copie Snapshot nel volume di destinazione:

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito vengono illustrate le copie Snapshot di `vserverB:secondary1` destinazione:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Ripristinare il contenuto di un volume da una copia Snapshot in un volume di destinazione SnapMirror:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   <snapshot>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

   Il seguente comando ripristina il contenuto del volume di origine originale `primary1` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than Snapshot copy daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Rimontare il volume ripristinato e riavviare tutte le applicazioni che utilizzano il volume.

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"
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	"Panoramica del ripristino del volume con SnapVault"

Aggiornare manualmente una relazione di replica

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa dello spostamento del volume di origine.

A proposito di questa attività

SnapMirror interrompe i trasferimenti da un volume di origine spostato fino a quando non si aggiorna manualmente la relazione di replica.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. Sebbene i volumi di origine e di destinazione siano sempre sincronizzati in queste relazioni, la vista dal cluster secondario viene sincronizzata con il principale solo su base oraria. Se si desidera visualizzare i dati point-in-time nella destinazione, eseguire un aggiornamento manuale eseguendo il `snapmirror update` comando.

Fase

1. Aggiornare manualmente una relazione di replica:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene aggiornata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Risincronizzare una relazione di replica

È necessario risincronizzare una relazione di replica dopo che si rende scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione o se si desidera modificare il criterio di replica per la relazione.

A proposito di questa attività

- Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.
- La risincronizzazione dei volumi che fanno parte di una configurazione fan-out o a cascata può richiedere più tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

Fase

1. Risincronizzare i volumi di origine e di destinazione:

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -type DP|XDP -policy` *`policy`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

   Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Eliminare una relazione di replica di un volume

È possibile utilizzare `snapmirror delete` e. `snapmirror release` comandi per eliminare una relazione di replica di un volume. È quindi possibile eliminare manualmente i volumi di destinazione non necessari.

A proposito di questa attività

Il `snapmirror release` Il comando elimina tutte le copie Snapshot create da SnapMirror dall'origine. È

possibile utilizzare `-relationship-info-only` Opzione per conservare le copie Snapshot.

Fasi

1. Interrompere la relazione di replica:

   `snapmirror quiesce -destination-path` *`SVM:volume|cluster://SVM/volume`*

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

2. (Facoltativo) interrompere la relazione di replica se si desidera che il volume di destinazione sia un volume di lettura/scrittura. È possibile saltare questo passaggio se si intende eliminare il volume di destinazione o se non è necessario che il volume sia in lettura/scrittura:

   `snapmirror break -source-path SVM:volume|cluster://SVM/volume, … -destination -path SVM:volume|cluster://SVM/volume, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

3. Eliminare la relazione di replica:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Eseguire questo comando dal cluster di destinazione o dalla SVM di destinazione.

   Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

4. Rilasciare le informazioni sulle relazioni di replica dalla SVM di origine:

   `snapmirror release -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination-path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Eseguire questo comando dal cluster di origine o dalla SVM di origine.

   Nell'esempio riportato di seguito vengono rilasciate informazioni per la relazione di replica specificata dalla SVM di origine `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Gestire l'efficienza dello storage

SnapMirror preserva l'efficienza dello storage sui volumi di origine e di destinazione, con un'eccezione, quando la compressione dei dati post-elaborazione è attivata sulla destinazione. In tal caso, tutta l'efficienza dello storage viene persa sulla destinazione. Per risolvere questo problema, è necessario disattivare la compressione post-elaborazione sulla destinazione, aggiornare manualmente la relazione e riattivare l'efficienza dello storage.

Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

  "Peering di cluster e SVM"

- È necessario disattivare la compressione post-elaborazione sulla destinazione.

A proposito di questa attività

È possibile utilizzare `volume efficiency show` comando per determinare se l'efficienza è attivata su un volume. Per ulteriori informazioni, consulta le pagine man.

È possibile verificare se SnapMirror mantiene l'efficienza dello storage visualizzando i registri di controllo di SnapMirror e individuando la descrizione del trasferimento. Se viene visualizzata la descrizione del trasferimento `transfer_desc=Logical Transfer`, SnapMirror non mantiene l'efficienza dello storage. Se viene visualizzata la descrizione del trasferimento `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror sta mantenendo l'efficienza dello storage. Ad esempio:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Trasferimento logico con storage

A partire da ONTAP 9.3, l'aggiornamento manuale non è più necessario per riattivare l'efficienza dello storage. Se SnapMirror rileva che la compressione post-processo è stata disattivata, riattiva automaticamente l'efficienza dello storage al successivo aggiornamento pianificato. Sia l'origine che la destinazione devono eseguire ONTAP 9.3.

A partire da ONTAP 9.3, i sistemi AFF gestiscono le impostazioni di efficienza dello storage in modo diverso dai sistemi FAS dopo che un volume di destinazione è reso scrivibile:

- Dopo aver impostato un volume di destinazione scrivibile utilizzando `snapmirror break` il criterio di

caching sul volume viene automaticamente impostato su “auto” (impostazione predefinita).

> Questo comportamento è applicabile solo ai volumi FlexVol e non ai volumi FlexGroup.

- Alla risincronizzazione, il criterio di caching viene automaticamente impostato su “none” e deduplica e compressione inline vengono automaticamente disabilitate, indipendentemente dalle impostazioni originali. È necessario modificare le impostazioni manualmente in base alle necessità.

> Gli aggiornamenti manuali con l’efficienza dello storage abilitata possono richiedere molto tempo. Potrebbe essere necessario eseguire l’operazione in ore non di punta.

Fase

1. Aggiornare una relazione di replica e riattivare l’efficienza dello storage:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -enable-storage-efficiency true`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il comando non riesce se non esiste una copia Snapshot comune sull’origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

   Nell’esempio seguente viene aggiornata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`e riattiva l’efficienza dello storage:

   ```
   cluster_dst::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst -enable-storage-efficiency true
   ```

Utilizzare la funzione di limitazione globale di SnapMirror

La funzione di limitazione globale della rete è disponibile per tutti i trasferimenti SnapMirror e SnapVault a livello di nodo.

A proposito di questa attività

La limitazione globale di SnapMirror limita la larghezza di banda utilizzata dai trasferimenti SnapMirror e SnapVault in entrata e/o in uscita. La restrizione viene applicata a livello di cluster su tutti i nodi del cluster.

Ad esempio, se l’acceleratore in uscita è impostato su 100 Mbps, per ogni nodo del cluster la larghezza di banda in uscita sarà impostata su 100 Mbps. Se la funzione di limitazione globale è disattivata, viene disattivata su tutti i nodi.

Sebbene le velocità di trasferimento dei dati siano spesso espresse in bit per secondo (bps), i valori di accelerazione devono essere immessi in kilobyte per secondo (kbps).

> In ONTAP 9.9.1 e versioni precedenti, l'acceleratore non ha alcun effetto su `volume move` trasferimenti o trasferimenti mirror di condivisione del carico. A partire da ONTAP 9.10.0, è possibile specificare un'opzione per limitare le operazioni di spostamento di un volume. Per ulteriori informazioni, vedere "Come ridurre lo spostamento del volume in ONTAP 9.10 e versioni successive."

La funzione Global Throttling funziona con la funzione di accelerazione per relazione per i trasferimenti SnapMirror e SnapVault. La regolazione per relazione viene applicata fino a quando la larghezza di banda combinata dei trasferimenti per relazione non supera il valore della valvola a farfalla globale, dopodiché viene applicata la valvola a farfalla globale. Un valore di accelerazione `0` implica che la limitazione globale è disattivata.

> La limitazione globale di SnapMirror non ha alcun effetto sulle relazioni sincrone di SnapMirror quando sono in-Sync. Tuttavia, l'accelerazione influisce sulle relazioni sincrone di SnapMirror quando eseguono una fase di trasferimento asincrona, ad esempio un'operazione di inizializzazione o dopo un evento out of Sync. Per questo motivo, si sconsiglia di attivare la limitazione globale con le relazioni sincroni di SnapMirror.

Fasi

1. Attivare la limitazione globale:

   `options -option-name replication.throttle.enable on|off`

   Nell'esempio seguente viene illustrato come attivare la funzione di limitazione globale di SnapMirror `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Specificare la larghezza di banda totale massima utilizzata dai trasferimenti in entrata sul cluster di destinazione:

   `options -option-name replication.throttle.incoming.max_kbs` *KBps*

   La larghezza di banda dell'acceleratore minima consigliata è di 4 kbps e la massima è di 2 Tbps. Il valore predefinito per questa opzione è `unlimited`, il che significa che non esiste alcun limite alla larghezza di banda totale utilizzata.

   L'esempio seguente mostra come impostare la larghezza di banda massima totale utilizzata dai trasferimenti in entrata su 100 Mbps:

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Mbps = 12500 kbps

3. Specificare la larghezza di banda totale massima utilizzata dai trasferimenti in uscita sul cluster di origine:

   `options -option-name replication.throttle.outgoing.max_kbs` *KBps*

La larghezza di banda dell'acceleratore minima consigliata è di 4 kbps e la massima è di 2 Tbps. Il valore predefinito per questa opzione è `unlimited`, il che significa che non esiste alcun limite alla larghezza di banda totale utilizzata. I valori dei parametri sono espressi in kbps.

L'esempio seguente mostra come impostare la larghezza di banda massima totale utilizzata dai trasferimenti in uscita su 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Gestire la replica di SnapMirror SVM

Informazioni sulla replica di SnapMirror SVM

È possibile utilizzare SnapMirror per creare una relazione di protezione dei dati tra le SVM. In questo tipo di relazione di protezione dei dati, viene replicata tutta o parte della configurazione di SVM, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, nonché i dati nei volumi di proprietà di SVM.

Tipi di relazione supportati

È possibile replicare solo le SVM che servono i dati. Sono supportati i seguenti tipi di relazione per la protezione dei dati:

- *SnapMirror DR,* in cui la destinazione contiene in genere solo le copie Snapshot attualmente presenti nell'origine.

  A partire da ONTAP 9.9.1, questo comportamento cambia quando si utilizza il criterio del vault mirror. A partire da ONTAP 9.9.1, è possibile creare diverse policy Snapshot sull'origine e sulla destinazione e le copie Snapshot sulla destinazione non vengono sovrascritte dalle copie Snapshot sull'origine:

  - Non vengono sovrascritti dall'origine alla destinazione durante le normali operazioni pianificate, gli aggiornamenti e la risincronizzazione
  - Non vengono cancellati durante le operazioni di interruzione.
  - Non vengono cancellati durante le operazioni flip-resync.
    Quando si configura una relazione di emergenza SVM utilizzando il criterio mirror-vault utilizzando ONTAP 9.9.1 e versioni successive, il criterio si comporta come segue:
  - I criteri di copia Snapshot definiti dall'utente all'origine non vengono copiati nella destinazione.
  - I criteri di copia Snapshot definiti dal sistema non vengono copiati nella destinazione.
  - L'associazione dei volumi con le policy Snapshot definite dall'utente e dal sistema non viene copiata nella destinazione. + SVM.
- A partire da ONTAP 9.2, *SnapMirror Unified Replication*, in cui la destinazione è configurata sia per il DR che per la conservazione a lungo termine.

I dettagli su questi tipi di relazione sono disponibili qui: "Informazioni sulla replica dei volumi SnapMirror".

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

Tipo di policy	Tipo di relazione
mirror asincrono	Dr. SnapMirror
vault mirror	Replica unificata

XDP sostituisce DP come replica SVM predefinita in ONTAP 9.4

A partire da ONTAP 9.4, le relazioni di protezione dei dati SVM passano per impostazione predefinita alla modalità XDP. Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.3 e versioni precedenti.

Le relazioni esistenti non vengono influenzate dal nuovo valore predefinito. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. La tabella seguente mostra il comportamento che ci si può aspettare.

Se si specifica…	Il tipo è…	Il criterio predefinito (se non si specifica un criterio) è…
DP	XDP	MirrorAllSnapshot (DR SnapMirror)
Niente	XDP	MirrorAllSnapshot (DR SnapMirror)
XDP	XDP	MirrorAndVault (replica unificata)

I dettagli sulle modifiche di default sono disponibili qui: "XDP sostituisce DP come impostazione predefinita di SnapMirror".

> L'indipendenza dalla versione non è supportata per la replica SVM. In una configurazione di disaster recovery delle SVM, la SVM di destinazione deve trovarsi su un cluster dotato della stessa versione di ONTAP del cluster SVM di origine per supportare le operazioni di failover e failback.

"Versioni ONTAP compatibili per le relazioni SnapMirror"

Come vengono replicate le configurazioni SVM

Il contenuto di una relazione di replica SVM è determinato dall'interazione dei seguenti campi:

- Il `-identity-preserve true` opzione di `snapmirror create` Il comando replica l'intera configurazione SVM.

  Il `-identity-preserve false` L'opzione replica solo i volumi e le configurazioni di autenticazione e autorizzazione della SVM, nonché le impostazioni del protocollo e del servizio nomi elencate nella "Configurazioni replicate nelle relazioni di disaster recovery delle SVM".

- Il `-discard-configs network` opzione di `snapmirror policy create` Il comando esclude le LIF e le relative impostazioni di rete dalla replica SVM, da utilizzare nei casi in cui le SVM di origine e di destinazione si trovano in sottoreti diverse.
- Il `-vserver-dr-protection unprotected` opzione di `volume modify` Il comando esclude il volume specificato dalla replica SVM.

In caso contrario, la replica SVM è quasi identica alla replica del volume. È possibile utilizzare virtualmente lo stesso flusso di lavoro per la replica SVM utilizzato per la replica dei volumi.

Dettagli del supporto

La seguente tabella mostra i dettagli del supporto per la replica SVM di SnapMirror.

Risorsa o funzione	Dettagli del supporto
Tipi di implementazione	• Da origine singola a destinazione singola • A partire da ONTAP 9.4, fan-out. È possibile eseguire la fan-out solo su due destinazioni. Per impostazione predefinita, è consentita una sola relazione effettiva -Identity-Preserve per SVM di origine.
Tipi di relazione	• Disaster recovery SnapMirror • A partire da ONTAP 9.2, la replica unificata di SnapMirror
Ambito della replica	Solo intercluster. Non è possibile replicare le SVM nello stesso cluster.
Protezione ransomware autonoma	• Supportato a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere "Protezione ransomware autonoma"
Supporto asincrono gruppi di coerenza	A partire da ONTAP 9.14.1, sono supportate massimo 32 relazioni di disaster recovery SVM in presenza di gruppi di coerenza. Vedere "Proteggere un gruppo di coerenza" e. "Limiti del gruppo di coerenza" per ulteriori informazioni.
FabricPool	A partire da ONTAP 9.6, la replica SVM di SnapMirror è supportata con FabricPools.

MetroCluster	A partire da ONTAP 9.11.1, entrambi i lati di una relazione di disaster recovery SVM all'interno di una configurazione MetroCluster possono fungere da origine per ulteriori configurazioni di disaster recovery SVM. A partire da ONTAP 9.5, la replica SVM di SnapMirror è supportata nelle configurazioni MetroCluster. • Nelle release precedenti a ONTAP 9,10.X, una configurazione MetroCluster non può essere la destinazione di una relazione di disaster recovery della SVM. • In ONTAP 9.10.1 e versioni successive, una configurazione MetroCluster può essere la destinazione di una relazione di disaster recovery della SVM solo ai fini della migrazione e deve soddisfare tutti i requisiti necessari descritti in "TR-4966: Migrazione di una SVM in una soluzione MetroCluster". • Solo una SVM attiva all'interno di una configurazione MetroCluster può essere l'origine di una relazione di disaster recovery SVM. Un'origine può essere una SVM di origine della sincronizzazione prima dello switchover o una SVM di destinazione della sincronizzazione dopo lo switchover. • Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online. • Quando la SVM sync-source è l'origine di una relazione di disaster recovery della SVM, le informazioni della relazione di disaster recovery della SVM di origine vengono replicate al partner MetroCluster. • Durante i processi di switchover e switchback, è possibile che si verifichi un errore nella replica alla destinazione di disaster recovery della SVM. Tuttavia, al termine del processo di switchover o switchback, gli aggiornamenti pianificati del disaster recovery della SVM successivo avranno esito positivo.
Gruppo di coerenza	Supportato a partire da ONTAP 9.14.1. Per ulteriori informazioni, vedere Proteggere un gruppo di coerenza.

ONTAP S3	Non supportato con disaster recovery SVM.
SnapMirror sincrono	Non supportato con disaster recovery SVM.
Indipendenza dalla versione	Non supportato.
Crittografia dei volumi	• I volumi crittografati sull'origine vengono crittografati sulla destinazione. • I server Onboard Key Manager o KMIP devono essere configurati sulla destinazione. • Le nuove chiavi di crittografia vengono generate alla destinazione. • Se la destinazione non contiene un nodo che supporta la crittografia .volume, la replica ha esito positivo, ma i volumi di destinazione non vengono crittografati.

Configurazioni replicate nelle relazioni di disaster recovery delle SVM

La seguente tabella mostra l'interazione di `snapmirror create -identity-preserve` e il `snapmirror policy create -discard-configs network` opzione:

Configurazione replicata		**`-identity-preserve true`**		**`-identity-preserve false`**
		Policy senza `-discard-configs network` impostato	**Policy con `-discard-configs network` impostato**	
Rete	LIF NAS	Sì	No	No
Configurazione Kerberos LIF	Sì	No	No	LIF SAN
No	No	No	Policy firewall	Sì
Sì	No	Politiche di servizio	Sì	Sì
No	Percorsi	Sì	No	No
Dominio di broadcast	No	No	No	Subnet
No	No	No	IPSpace	No
No	No	PMI	Server SMB	Sì

Sì	No	Gruppi locali e utenti locali	Sì	Sì
Sì	Privilegio	Sì	Sì	Sì
Copia shadow	Sì	Sì	Sì	BranchCache
Sì	Sì	Sì	Opzioni del server	Sì
Sì	Sì	Sicurezza del server	Sì	Sì
No	Home directory, condividere	Sì	Sì	Sì
Link simbolico	Sì	Sì	Sì	Policy Fpolicy, policy FSecurity e FSecurity NTFS
Sì	Sì	Sì	Mappatura dei nomi e mappatura dei gruppi	Sì
Sì	Sì	Informazioni di audit	Sì	Sì
Sì	NFS	Policy di esportazione	Sì	Sì
No	Regole dei criteri di esportazione	Sì	Sì	No
Server NFS	Sì	Sì	No	RBAC
Certificati di sicurezza	Sì	Sì	No	Configurazione dell’utente, della chiave pubblica, del ruolo e del ruolo
Sì	Sì	Sì	SSL	Sì
Sì	No	Servizi di nome	Host DNS e DNS	Sì
Sì	No	Utente UNIX e gruppo UNIX	Sì	Sì

Sì	Aree di autenticazione Kerberos e blocchi di chiavi Kerberos	Sì	Sì	No
Client LDAP e LDAP	Sì	Sì	No	Netgroup
Sì	Sì	No	NIS	Sì
Sì	No	Accesso web e web	Sì	Sì
No	Volume	Oggetto	Sì	Sì
Sì	Copie Snapshot, policy Snapshot e policy di eliminazione automatica	Sì	Sì	Sì
Policy di efficienza	Sì	Sì	Sì	Policy di quota e regola dei criteri di quota
Sì	Sì	Sì	Coda di recovery	Sì
Sì	Sì	Volume root	Namespace	Sì
Sì	Sì	Dati dell'utente	No	No
No	Qtree	No	No	No
Quote	No	No	No	QoS a livello di file
No	No	No	Attributi: stato del volume root, garanzia di spazio, dimensione, dimensionamento automatico e numero totale di file	No
No	No	QoS dello storage	Gruppo di criteri QoS	Sì
Sì	Sì	Fibre Channel (FC)	No	No
No	ISCSI	No	No	No

LUN	Oggetto	Sì	Sì	Sì
igroups	No	No	No	portset
No	No	No	Numeri di serie	No
No	No	SNMP	utenti v3	Sì

Limiti storage per il disaster recovery delle SVM

Nella tabella seguente viene indicato il numero massimo consigliato di volumi e relazioni di disaster recovery delle SVM supportate per ogni oggetto storage. Devi essere consapevole che i limiti sono spesso dipendenti dalla piattaforma. Fare riferimento a. "Hardware Universe" per conoscere i limiti della configurazione specifica.

Oggetto di storage	Limite
SVM	300 volumi flessibili
Coppia HA	1,000 volumi flessibili
Cluster	128 relazioni di disastro delle SVM

Replicare le configurazioni SVM

Workflow di replica di SnapMirror SVM

La replica di SnapMirror SVM implica la creazione della SVM di destinazione, la creazione di una pianificazione dei processi di replica e la creazione e l'inizializzazione di una relazione SnapMirror.

È necessario determinare il flusso di lavoro di replica più adatto alle proprie esigenze:

- "Replica di un'intera configurazione SVM"
- "Escludere le LIF e le relative impostazioni di rete dalla replica SVM"
- "Escludi rete, name service e altre impostazioni dalla configurazione della SVM"

Criteri per l'inserimento dei volumi nelle SVM di destinazione

Durante la replica dei volumi dalla SVM di origine alla SVM di destinazione, è importante conoscere i criteri per la selezione degli aggregati.

Gli aggregati vengono selezionati in base ai seguenti criteri:

- I volumi vengono sempre posizionati su aggregati non root.
- Gli aggregati non root vengono selezionati in base allo spazio libero disponibile e al numero di volumi già ospitati nell'aggregato.

Gli aggregati con più spazio libero e meno volumi hanno la priorità. Viene selezionato l'aggregato con la priorità più alta.

- I volumi di origine sugli aggregati FabricPool vengono collocati su aggregati FabricPool sulla destinazione con la stessa policy di tiering.
- Se un volume sulla SVM di origine si trova su un aggregato di Flash Pool, il volume viene collocato su un aggregato di Flash Pool sulla SVM di destinazione, se tale aggregato esiste e dispone di spazio libero sufficiente.
- Se il `-space-guarantee` l'opzione del volume replicato è impostata su `volume`, vengono presi in considerazione solo gli aggregati con spazio libero maggiore della dimensione del volume.
- Le dimensioni del volume aumentano automaticamente sulla SVM di destinazione durante la replica, in base alle dimensioni del volume di origine.

  Se si desidera riservare in anticipo le dimensioni sulla SVM di destinazione, è necessario ridimensionare il volume. Le dimensioni del volume non si riducono automaticamente sulla SVM di destinazione in base alla SVM di origine.

Se si desidera spostare un volume da un aggregato all'altro, è possibile utilizzare `volume move` Sulla SVM di destinazione.

Replica di un'intera configurazione SVM

È possibile utilizzare `-identity-preserve true` opzione di `snapmirror create` Per replicare un'intera configurazione SVM.

Prima di iniziare

I cluster di origine e di destinazione e le SVM devono essere peering. Per ulteriori informazioni, vedere "Creare una relazione peer del cluster" e. "Creare una relazione peer tra cluster SVM".

Per la sintassi completa dei comandi, vedere la pagina man.

A proposito di questa attività

Questo flusso di lavoro presuppone che si stia già utilizzando un criterio predefinito o un criterio di replica personalizzato.

A partire da ONTAP 9.9.1, quando si utilizza la policy del vault mirror, è possibile creare policy Snapshot diverse sulla SVM di origine e di destinazione e le copie Snapshot sulla destinazione non vengono sovrascritte dalle copie Snapshot sull'origine. Per ulteriori informazioni, vedere "Informazioni sulla replica di SnapMirror SVM".

Fasi

1. Creare una SVM di destinazione:

   `vserver create -vserver` *`SVM_name`* `-subtype dp-destination`

   Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

   Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

   Per ulteriori informazioni, vedere "Creare una relazione peer tra cluster SVM".

3. Creare una pianificazione del processo di replica:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

   > La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

   Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   saturday -hour 3 -minute 0
   ```

4. Dalla SVM di destinazione o dal cluster di destinazione, creare una relazione di replica:

   `snapmirror create -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`: -type DP|XDP -schedule` *`schedule`* `-policy` *`policy`* `-identity-preserve true`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni.

   Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve true
   ```

   Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

   ```
   cluster_dst:> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
   -identity-preserve true
   ```

   Supponendo di aver creato un criterio personalizzato con il tipo di criterio `async-mirror`, Nell'esempio seguente viene creata una relazione di DR di SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `mirror-vault`, nell'esempio seguente viene creata una relazione di replica unificata:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

5. Arrestare la SVM di destinazione:

   `vserver stop`

   `SVM name`

   Nell'esempio seguente viene interrotta una SVM di destinazione denominata dvs1:

   ```
   cluster_dst::> vserver stop -vserver dvs1
   ```

6. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare la relazione di replica SVM: +

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   Nell'esempio seguente viene inizializzata la relazione tra la SVM di origine, `svm1`E la SVM di destinazione, `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1: -destination
   -path svm_backup:
   ```

Escludere le LIF e le relative impostazioni di rete dalla replica SVM

Se le SVM di origine e di destinazione si trovano in sottoreti diverse, è possibile utilizzare `-discard-configs network` opzione di `snapmirror policy create` Comando per escludere le LIF e le relative impostazioni di rete dalla replica SVM.

Di cosa hai bisogno

I cluster di origine e di destinazione e le SVM devono essere peering.

Per ulteriori informazioni, vedere "Creare una relazione peer del cluster" e. "Creare una relazione peer tra cluster SVM".

A proposito di questa attività

Il `-identity-preserve` opzione di `snapmirror create` il comando deve essere impostato su `true` Quando si crea la relazione di replica SVM.

Per la sintassi completa dei comandi, vedere la pagina man.

Fasi

1. Creare una SVM di destinazione:

   `vserver create -vserver SVM -subtype dp-destination`

   Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

   Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

   Per ulteriori informazioni, vedere "Creare una relazione peer tra cluster SVM".

3. Creare una pianificazione del processo:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

   > La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

   Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Creare un criterio di replica personalizzato:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che esclude le LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata che esclude le LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

5. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per creare una relazione di replica:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve true|false`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere gli esempi riportati di seguito.

   Nell'esempio seguente viene creata una relazione di DR di SnapMirror che esclude i LIF:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
   -identity-preserve true
   ```

   Nell'esempio seguente viene creata una relazione di replica unificata di SnapMirror che esclude le LIF:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
   -identity-preserve true
   ```

6. Arrestare la SVM di destinazione:

   `vserver stop`

   SVM name

   Nell'esempio seguente viene interrotta una SVM di destinazione denominata dvs1:

   ```
   cluster_dst::> vserver stop -vserver dvs1
   ```

7. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare una relazione di replica:

   `snapmirror initialize -source-path SVM: -destination-path SVM:`

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene inizializzata la relazione tra l'origine, `svm1` e la destinazione, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Al termine

È necessario configurare la rete e i protocolli sulla SVM di destinazione per l'accesso ai dati in caso di disastro.

Escludere la rete, il servizio nomi e altre impostazioni dalla replica SVM

È possibile utilizzare `-identity-preserve false` opzione di `snapmirror create` Per replicare solo i volumi e le configurazioni di sicurezza di una SVM. Vengono mantenute anche alcune impostazioni del protocollo e del servizio nomi.

A proposito di questa attività

Per un elenco delle impostazioni preservate del protocollo e del servizio nomi, vedere "Configurazioni replicate nelle relazioni di DR SVM".

Per la sintassi completa dei comandi, vedere la pagina man.

Prima di iniziare

I cluster di origine e di destinazione e le SVM devono essere peering.

Per ulteriori informazioni, vedere "Creare una relazione peer del cluster" e. "Creare una relazione peer tra cluster SVM".

Fasi

1. Creare una SVM di destinazione:

   `vserver create -vserver SVM -subtype dp-destination`

   Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

   Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

   Per ulteriori informazioni, vedere "Creare una relazione peer tra cluster SVM".

3. Creare una pianificazione del processo di replica:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

> La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Creare una relazione di replica che escluda le impostazioni di rete, name service e altre impostazioni di configurazione:

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere gli esempi riportati di seguito. È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

   Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve false
   ```

   Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy. La relazione esclude le impostazioni di rete, name service e altre impostazioni di configurazione:

   ```
   cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
   -type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
   false
   ```

   Supponendo di aver creato un criterio personalizzato con il tipo di criterio `async-mirror`, Nell'esempio seguente viene creata una relazione di DR di SnapMirror. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `mirror-vault`, nell'esempio seguente viene creata una relazione di replica unificata. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

5. Arrestare la SVM di destinazione:

   `vserver stop`

   `SVM name`

   Nell'esempio seguente viene interrotta una SVM di destinazione denominata dvs1:

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. Se si utilizza SMB, è necessario configurare anche un server SMB.

   Vedere "Solo SMB: Creazione di un server SMB".

7. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare la relazione di replica SVM:

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

Al termine

È necessario configurare la rete e i protocolli sulla SVM di destinazione per l'accesso ai dati in caso di disastro.

Specificare gli aggregati da utilizzare per le relazioni di DR SVM

Dopo aver creato una SVM per il disaster recovery, è possibile utilizzare `aggr-list` opzione con `vserver modify` Comando per limitare gli aggregati utilizzati per ospitare i volumi di destinazione DR SVM.

Fase

1. Creare una SVM di destinazione:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. Modificare l'elenco di server SVM per il disaster recovery per limitare gli aggregati utilizzati per ospitare il volume SVM per il disaster recovery:

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

Solo SMB: Creare un server SMB

Se la SVM di origine dispone di una configurazione SMB e si è scelto di impostarla `identity-preserve` a. `false`, È necessario creare un server SMB per la SVM di destinazione. Il server SMB è necessario per alcune configurazioni SMB, come ad esempio le condivisioni durante l'inizializzazione della relazione SnapMirror.

Fasi

1. Avviare la SVM di destinazione utilizzando `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Verificare che la SVM di destinazione si trovi in `running` lo stato e il sottotipo sono `dp-destination` utilizzando `vserver show` comando.

```
destination_cluster::> vserver show
                                   Admin      Operational Root
Vserver  Type    Subtype           State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Creare una LIF utilizzando `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

4. Creare un percorso utilizzando `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gestione della rete"

5. Configurare il DNS utilizzando `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Aggiungere il domain controller preferito utilizzando `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Creare il server SMB utilizzando `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Arrestare la SVM di destinazione utilizzando `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Escludere i volumi dalla replica SVM

Per impostazione predefinita, tutti i volumi di dati RW della SVM di origine vengono replicati. Se non si desidera proteggere tutti i volumi sulla SVM di origine, è possibile utilizzare `-vserver-dr-protection unprotected` opzione di `volume modify` Comando per escludere i volumi dalla replica SVM.

Fasi

1. Escludere un volume dalla replica SVM:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Il seguente esempio esclude il volume `volA_src` Dalla replica SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

   Se in seguito si desidera includere un volume nella replica SVM precedentemente esclusa, eseguire il

seguente comando:

`volume modify -vserver SVM -volume volume -vserver-dr-protection protected`

Il seguente esempio include il volume `volA_src` Nella replica SVM:

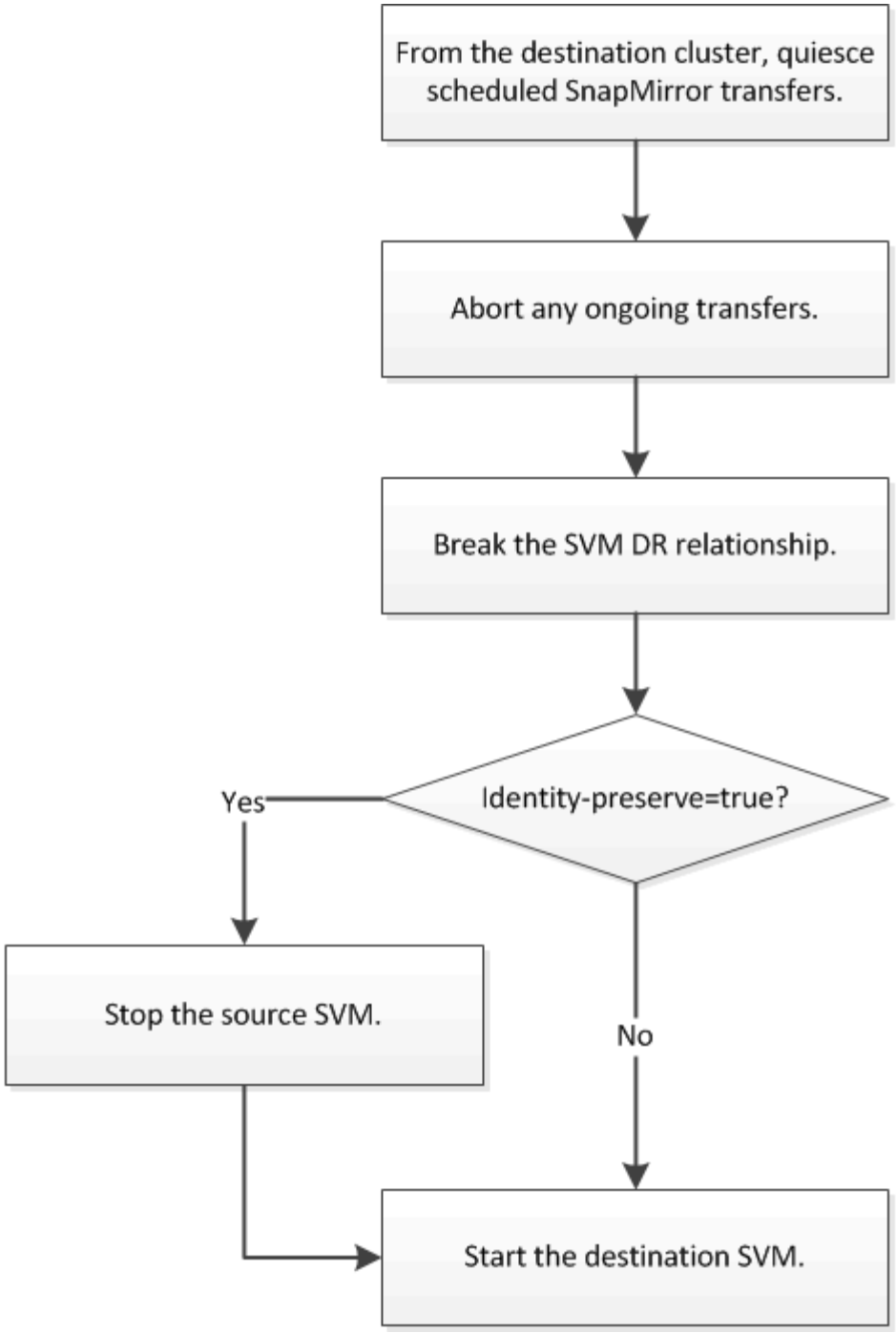
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Creare e inizializzare la relazione di replica SVM come descritto in "Replica di un'intera configurazione SVM".

Fornire i dati da una destinazione DR SVM

Workflow di disaster recovery SVM

Per eseguire il ripristino da un disastro e fornire i dati dalla SVM di destinazione, è necessario attivare la SVM di destinazione. L'attivazione della SVM di destinazione comporta l'interruzione dei trasferimenti pianificati di SnapMirror, l'interruzione dei trasferimenti in corso di SnapMirror, l'interruzione della relazione di replica, l'interruzione della SVM di origine e l'avvio della SVM di destinazione.



Rendere scrivibili i volumi di destinazione SVM

È necessario rendere scrivibili i volumi di destinazione SVM prima di poter fornire i dati ai client. La procedura è in gran parte identica alla procedura per la replica del volume, con un'eccezione. Se si imposta `-identity-preserve true` Una volta creata la relazione di replica SVM, è necessario arrestare la SVM di origine prima di attivare la SVM di destinazione.

A proposito di questa attività

Per la sintassi completa dei comandi, vedere la pagina man.

In uno scenario di disaster recovery, non è possibile eseguire un aggiornamento di SnapMirror dalla SVM di origine alla SVM di destinazione del disaster recovery perché la SVM di origine e i relativi dati non saranno accessibili e poiché gli aggiornamenti dall'ultima risincronizzazione potrebbero essere danneggiati o danneggiati.

Fasi

1. Dalla SVM di destinazione o dal cluster di destinazione, interrompere i trasferimenti pianificati verso la destinazione:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path
   svm_backup:
   ```

2. Dalla SVM di destinazione o dal cluster di destinazione, interrompere i trasferimenti in corso alla destinazione:

   `snapmirror abort -source-path SVM: -destination-path SVM:`

   Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   L'esempio seguente interrompe i trasferimenti in corso tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1: -destination-path
   svm_backup:
   ```

3. Dalla SVM di destinazione o dal cluster di destinazione, interrompere la relazione di replica:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene spezzata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

4. Se si imposta `-identity-preserve true` Una volta creata la relazione di replica SVM, interrompere la SVM di origine:

   `vserver stop -vserver` *SVM*

   Nell'esempio seguente viene interrotta la SVM di origine `svm1`:

   ```
   cluster_src::> vserver stop svm1
   ```

5. Avviare la SVM di destinazione:

   `vserver start -vserver` *SVM*

   Nell'esempio seguente viene avviata la SVM di destinazione `svm_backup`:

   ```
   cluster_dst::> vserver start svm_backup
   ```

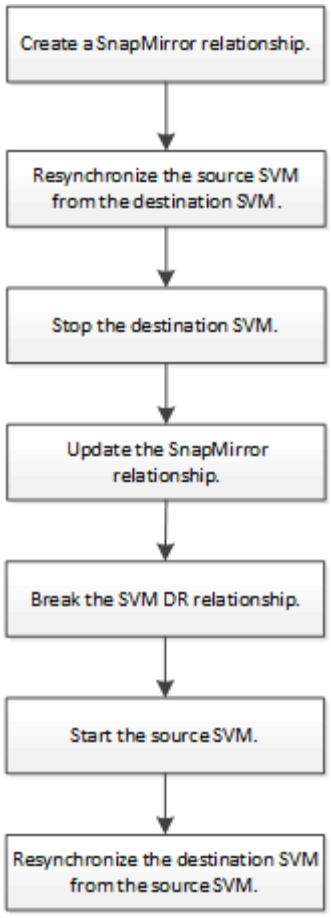
Al termine

Configurare i volumi di destinazione SVM per l'accesso ai dati, come descritto in "Configurazione del volume di destinazione per l'accesso ai dati".

Riattivare l'SVM di origine

Workflow di riattivazione SVM di origine

Se la SVM di origine esiste dopo un disastro, è possibile riattivarla e proteggerla ricreando la relazione di disaster recovery di SVM.



Riattivare l'SVM di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra la SVM di origine e di destinazione quando non è più necessario fornire dati dalla destinazione. La procedura è in gran parte identica alla procedura per la replica del volume, con un'eccezione. È necessario arrestare la SVM di destinazione prima di riattivare la SVM di origine.

Prima di iniziare

Se si sono aumentate le dimensioni del volume di destinazione durante la distribuzione dei dati da esso, prima di riattivare il volume di origine, è necessario aumentare manualmente la dimensione massima automatica sul volume di origine per garantire che possa crescere in modo sufficiente.

"Quando un volume di destinazione cresce automaticamente"

A proposito di questa attività

A partire da ONTAP 9.11.1, è possibile ridurre il tempo di risincronizzazione durante una prova di disaster recovery utilizzando `-quick-resync true` opzione di `snapmirror resync` Durante l'esecuzione di una risincronizzazione inversa di una relazione DR SVM. Una rapida risincronizzazione può ridurre il tempo necessario per tornare alla produzione ignorando le operazioni di ricostruzione e ripristino del data warehouse.

> La risincronizzazione rapida non preserva l'efficienza dello storage dei volumi di destinazione. L'attivazione della risincronizzazione rapida potrebbe aumentare lo spazio del volume utilizzato dai volumi di destinazione.

Questa procedura presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di

base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

Per la sintassi completa dei comandi, vedere la pagina man.

Fasi

1. Dalla SVM di origine originale o dal cluster di origine, creare una relazione DR SVM inversa utilizzando la stessa configurazione, policy e impostazioni di conservazione delle identità della relazione DR SVM originale:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene creata una relazione tra la SVM da cui vengono forniti i dati, `svm_backup`E la SVM di origine originale, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

2. Dalla SVM di origine originale o dal cluster di origine, eseguire il seguente comando per invertire la relazione di protezione dei dati:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

   > Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

   Nell'esempio seguente viene invertita la relazione tra la SVM di origine originale, `svm1`E la SVM da cui vengono forniti i dati, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

   Esempio di utilizzo dell'opzione -quick-resync:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1: -quick-resync true
   ```

3. Quando si è pronti a ristabilire l'accesso ai dati alla SVM di origine, arrestare la SVM di destinazione originale per disconnettere tutti i client attualmente connessi alla SVM di destinazione originale.

   `vserver stop -vserver SVM`

   Nell'esempio riportato di seguito viene interrotta la SVM di destinazione originale che attualmente fornisce i dati:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. Verificare che la SVM di destinazione originale si trovi nello stato arrestato utilizzando `vserver show` comando.

   ```
   cluster_dst::> vserver show
                                    Admin      Operational Root
   Vserver        Type    Subtype    State      State       Volume
   Aggregate
   --------       ------- ---------- ---------- ----------- ----------
   ----------
   svm_backup     data    default    stopped    stopped     rv
   aggr1
   ```

5. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eseguire l'aggiornamento finale della relazione inversa e trasferire tutte le modifiche dalla SVM di destinazione originale alla SVM di origine:

   `snapmirror update -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio riportato di seguito viene aggiornata la relazione tra la SVM di destinazione originale da cui vengono forniti i dati,`svm_backup`E la SVM di origine originale, `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup: -destination
   -path svm1:
   ```

6. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per interrompere i trasferimenti pianificati per la relazione inversa:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra la SVM da cui si stanno fornendo i

dati, `svm_backup`E la SVM originale, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

7. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene spezzata la relazione tra la SVM di destinazione originale da cui si stavano servendo i dati, `svm_backup`E la SVM di origine originale, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

8. Se la SVM di origine originale è stata precedentemente arrestata, dal cluster di origine, avviare la SVM di origine originale:

   `vserver start -vserver SVM`

   Nell'esempio seguente viene avviata la SVM di origine originale:

```
cluster_src::> vserver start svm1
```

9. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ristabilire la relazione di protezione dei dati originale:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene ristabilita la relazione tra la SVM di origine originale, `svm1`E la SVM di destinazione originale, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

10. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eliminare la relazione di protezione dei dati invertita:

`snapmirror delete -source-path SVM: -destination-path SVM:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione inversa tra la SVM di destinazione originale, `svm_backup`E la SVM di origine originale, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

11. Dalla SVM di destinazione originale o dal cluster di destinazione originale, rilasciare la relazione di protezione dei dati invertita:

    `snapmirror release -source-path SVM: -destination-path SVM:`

    > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

    Nell'esempio seguente viene rilasciata la relazione inversa tra SVM di destinazione originale, svm_backup e SVM di origine, `svm1`

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1:
    ```

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Riattivare la SVM di origine originale (solo volumi FlexGroup)

È possibile ristabilire la relazione di protezione dei dati originale tra la SVM di origine e di destinazione quando non è più necessario fornire dati dalla destinazione. Per riattivare la SVM di origine originale quando si utilizzano volumi FlexGroup, è necessario eseguire alcuni passaggi aggiuntivi, tra cui l'eliminazione della relazione DR SVM originale e il rilascio della relazione originale prima di annullare la relazione. È inoltre necessario rilasciare la relazione invertita e ricreare la relazione originale prima di interrompere i trasferimenti pianificati.

Fasi

1. Dalla SVM di destinazione originale o dal cluster di destinazione originale, eliminare la relazione DR SVM originale:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione originale tra SVM di origine, svm1 e SVM di destinazione originale, `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. Dalla SVM di origine originale o dal cluster di origine originale, rilasciare la relazione originale mantenendo intatte le copie Snapshot:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene rilasciata la relazione originale tra SVM di origine, svm1 e SVM di destinazione originale, `svm_backup`.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. Dalla SVM di origine originale o dal cluster di origine, creare una relazione DR SVM inversa utilizzando la stessa configurazione, policy e impostazioni di conservazione delle identità della relazione DR SVM originale:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene creata una relazione tra la SVM da cui vengono forniti i dati, `svm_backup`E la SVM di origine originale, `svm1:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. Dalla SVM di origine originale o dal cluster di origine, eseguire il seguente comando per invertire la relazione di protezione dei dati:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

> Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene invertita la relazione tra la SVM di origine originale, `svm1`E la SVM da cui vengono forniti i dati, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. Quando si è pronti a ristabilire l'accesso ai dati alla SVM di origine, arrestare la SVM di destinazione originale per disconnettere tutti i client attualmente connessi alla SVM di destinazione originale.

   `vserver stop -vserver` *`SVM`*

   Nell'esempio riportato di seguito viene interrotta la SVM di destinazione originale che attualmente fornisce i dati:

```
cluster_dst::> vserver stop svm_backup
```

6. Verificare che la SVM di destinazione originale si trovi nello stato arrestato utilizzando `vserver show` comando.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver        Type    Subtype    State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

7. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eseguire l'aggiornamento finale della relazione inversa e trasferire tutte le modifiche dalla SVM di destinazione originale alla SVM di origine:

   `snapmirror update -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio riportato di seguito viene aggiornata la relazione tra la SVM di destinazione originale da cui vengono forniti i dati,`svm_backup`E la SVM di origine originale, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

8. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per interrompere i trasferimenti pianificati per la relazione inversa:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra la SVM da cui si stanno fornendo i dati, `svm_backup`E la SVM originale, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

9. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene spezzata la relazione tra la SVM di destinazione originale da cui si stavano servendo i dati, `svm_backup`E la SVM di origine originale, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

10. Se la SVM di origine originale è stata precedentemente arrestata, dal cluster di origine, avviare la SVM di origine originale:

    `vserver start -vserver SVM`

    Nell'esempio seguente viene avviata la SVM di origine originale:

```
cluster_src::> vserver start svm1
```

11. Dalla SVM di origine originale o dal cluster di origine, eliminare la relazione DR SVM inversa:

`snapmirror delete -source-path SVM: -destination-path SVM:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione inversa tra SVM di destinazione originale, svm_backup e SVM di origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Dalla SVM di destinazione originale o dal cluster di destinazione originale, rilasciare la relazione invertita mantenendo intatte le copie Snapshot:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

    Nell'esempio seguente viene rilasciata la relazione inversa tra SVM di destinazione originale, svm_backup e SVM di origine, svm1:

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ricreare la relazione originale. Utilizzare le stesse impostazioni di configurazione, policy e conservazione delle identità della relazione DR SVM originale:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

    Nell'esempio seguente viene creata una relazione tra la SVM di origine originale, `svm1`E la SVM di destinazione originale, `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ristabilire la relazione di protezione dei dati originale:

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

> Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene ristabilita la relazione tra la SVM di origine originale, `svm1`E la SVM di destinazione originale, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Convertire le relazioni di replica dei volumi in una relazione di replica SVM

È possibile convertire le relazioni di replica tra i volumi in una relazione di replica tra le macchine virtuali di storage (SVM) che possiedono i volumi, a condizione che ciascun volume sull'origine (eccetto il volume root) venga replicato, inoltre, ciascun volume di origine (incluso il volume root) ha lo stesso nome del volume di destinazione.

A proposito di questa attività

Utilizzare `volume rename` Quando la relazione SnapMirror è inattiva per rinominare i volumi di destinazione, se necessario.

Fasi

1. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per risincronizzare i volumi di origine e di destinazione:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`* `-type DP|XDP -policy` *`policy`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

   Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Creare una relazione di replica SVM tra le SVM di origine e di destinazione, come descritto in "Replica delle configurazioni SVM".

   È necessario utilizzare `-identity-preserve true` opzione di `snapmirror create` quando si crea la relazione di replica.

3. Arrestare la SVM di destinazione:

   `vserver stop -vserver` *`SVM`*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene interrotta la SVM di destinazione `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per risincronizzare le SVM di origine e di destinazione:

   `snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP -policy policy`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.
   >
   > Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

   Nell'esempio seguente viene risincronizzata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Eliminare una relazione di replica SVM

È possibile utilizzare `snapmirror delete` e. `snapmirror release` Comandi per eliminare una relazione di replica SVM. È quindi possibile eliminare manualmente i volumi di destinazione non necessari.

A proposito di questa attività

Il `snapmirror release` Il comando elimina tutte le copie Snapshot create da SnapMirror dall'origine. È possibile utilizzare `-relationship-info-only` Opzione per conservare le copie Snapshot.

Per la sintassi completa dei comandi, vedere la pagina man.

Fasi

1. Eseguire il seguente comando dalla SVM di destinazione o dal cluster di destinazione per interrompere la relazione di replica:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene spezzata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

2. Eseguire il seguente comando dalla SVM di destinazione o dal cluster di destinazione per eliminare la relazione di replica:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio seguente viene eliminata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

3. Eseguire il seguente comando dal cluster di origine o dalla SVM di origine per rilasciare le informazioni sulle relazioni di replica dalla SVM di origine:

   `snapmirror release -source-path SVM: -destination-path SVM:`

   > Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

   Nell'esempio riportato di seguito vengono rilasciate informazioni per la relazione di replica specificata dalla SVM di origine `svm1`:

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

Gestire la replica del volume root di SnapMirror

Panoramica sulla gestione della replica del volume root di SnapMirror

Ogni SVM in un ambiente NAS ha uno spazio dei nomi unico. Il *volume root di SVM,* contenente il sistema operativo e le relative informazioni, è il punto di ingresso della gerarchia dello spazio dei nomi. Per garantire che i dati rimangano accessibili ai client in caso di interruzione o failover di un nodo, è necessario creare una copia mirror di condivisione del carico del volume root SVM.

Lo scopo principale dei mirror di condivisione del carico per i volumi root SVM non è più la condivisione del carico, ma il loro scopo è il disaster recovery.

- Se il volume root non è temporaneamente disponibile, il mirror di load-sharing fornisce automaticamente l'accesso in sola lettura ai dati del volume root.
- Se il volume root non è disponibile in modo permanente, è possibile promuovere uno dei volumi di load sharing per fornire l'accesso in scrittura ai dati del volume root.

Creare e inizializzare relazioni mirror di condivisione del carico

È necessario creare un mirror di condivisione del carico (LSM) per ogni volume root SVM che serve i dati NAS nel cluster. Per i cluster che consistono di due o più coppie ha, è consigliabile considerare mirror di condivisione del carico dei root volumi SVM per garantire l'accessibilità del namespace ai client in caso affermativo
Si guastano entrambi i nodi di una coppia ha. I mirror per la condivisione del carico non sono adatti per i cluster costituiti da una singola coppia ha.

A proposito di questa attività

Se si crea un LSM sullo stesso nodo e il nodo non è disponibile, si dispone di un singolo punto di errore e non si dispone di una seconda copia per garantire che i dati rimangano accessibili ai client. Tuttavia, quando si crea il LSM su un nodo diverso da quello contenente il volume root o su una coppia ha diversa, i dati rimangono accessibili in caso di interruzione.

Ad esempio, in un cluster a quattro nodi con un volume root su tre nodi:

- Per il volume root sul nodo ha 1 1, creare il LSM sul nodo ha 2 1 o il nodo ha 2 2.
- Per il volume root sul nodo ha 1 2, creare il LSM sul nodo ha 2 1 o il nodo ha 2 2.
- Per il volume root sul nodo ha 2 1, creare il LSM sul nodo ha 1 1 o il nodo ha 1 2.

Fasi

1. Creare un volume di destinazione per LSM:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
   -type DP -size <size>
   ```

   Le dimensioni del volume di destinazione devono essere uguali o superiori a quelle del volume root.

   Si consiglia di assegnare un nome al volume root e a quello di destinazione con suffissi, ad esempio `_root` e. `_m1`.

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creato un volume mirror per la condivisione del carico per il volume root `svm1_root` poll `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Creare una pianificazione dei processi di replica".
3. Creare una relazione mirror di condivisione del carico tra il volume root SVM e il volume di destinazione per LSM:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type LS -schedule <schedule>
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creata una relazione mirror di condivisione del carico tra il volume root `svm1_root` e il volume mirror per la condivisione del carico `svm1_m1`:

   ```
   cluster_src::> snapmirror create -source-path svm1:svm1_root
   -destination-path svm1:svm1_m1 -type LS -schedule hourly
   ```

   L'attributo type del mirror di condivisione del carico cambia da `DP` a. `LS`.

4. Inizializzare il mirror di condivisione del carico:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror initialize-ls-set -source-path <SVM:volume>
   ```

   L'inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene inizializzato il mirror di load sharing per il volume root `svm1_root`:

   ```
   cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
   ```

Aggiornare una relazione mirror di condivisione del carico

Le relazioni del mirror di condivisione del carico (LSM) vengono aggiornate automaticamente per i volumi root SVM dopo che un volume nella SVM è stato montato o

dismontato e durante `volume create` operazioni che includono l'opzione `junction-path`. È possibile aggiornare manualmente una relazione LSM se si desidera che venga aggiornata prima del successivo aggiornamento pianificato.

Le relazioni mirror per la condivisione del carico si aggiornano automaticamente nei seguenti casi:

- È il momento di un aggiornamento pianificato
- Viene eseguita un'operazione di montaggio o disinstallazione su un volume nel volume root SVM
- R `volume create` viene emesso un comando che include `juntion-path` opzione

Fase

1. Aggiornare manualmente una relazione mirror di condivisione del carico:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   Nell'esempio riportato di seguito viene aggiornata la relazione del mirror di condivisione del carico per il volume root `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Promuovere un mirror per la condivisione del carico

Se un volume root non è disponibile in modo permanente, è possibile promuovere il volume LOAD-sharing mirror (LSM) per fornire l'accesso in scrittura ai dati del volume root.

Di cosa hai bisogno

Per questa attività, è necessario utilizzare i comandi avanzati del livello di privilegio.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Promuovere un volume LSM:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente promuove il volume `svm1_m2` Come nuovo volume root SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Invio `y`. ONTAP trasforma il volume LSM in un volume di lettura/scrittura ed elimina il volume root originale, se accessibile.

> Il volume root promosso potrebbe non disporre di tutti i dati presenti nel volume root originale se l'ultimo aggiornamento non si è verificato di recente.

3. Torna al livello di privilegio admin:

```
set -privilege admin
```

4. Rinominare il volume promosso seguendo la convenzione di denominazione utilizzata per il volume root:

   È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   Nell'esempio riportato di seguito viene rinomina il volume promosso `svm1_m2` con il nome `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteggere il volume root rinominato, come descritto nei passaggi da 3 a 4 in "Creazione e inizializzazione delle relazioni mirror di load sharing".

Dettagli tecnici di SnapMirror

USA la corrispondenza del modello del nome del percorso

È possibile utilizzare la corrispondenza dei modelli per specificare i percorsi di origine e destinazione in `snapmirror` comandi.

```
`snapmirror` i comandi utilizzano nomi di percorso completi nel seguente
formato: `vserver:volume`. È possibile abbreviare il nome del percorso
senza inserire il nome SVM. In questo caso, il `snapmirror` Il comando
presuppone il contesto SVM locale dell'utente.
```

Supponendo che SVM sia chiamato “vserver1” e che il volume sia chiamato “vol1”, il nome del percorso completo è `vserver1:vol1`.

È possibile utilizzare l’asterisco (*) nei percorsi come carattere jolly per selezionare i nomi dei percorsi completi corrispondenti. Nella tabella seguente sono riportati alcuni esempi di utilizzo del carattere jolly per selezionare un intervallo di volumi.

`*`	Corrisponde a tutti i percorsi.
`vs*`	Consente di confrontare tutti gli SVM e i volumi con i nomi SVM che iniziano con `vs`.
`:*src`	Consente di confrontare tutti gli SVM con i nomi dei volumi che contengono `src` testo.
`:vol`	Consente di confrontare tutti gli SVM con i nomi dei volumi che iniziano con `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                Snapmirrored  Idle           -
true    -
```

Utilizza query estese per agire su molte relazioni SnapMirror

È possibile utilizzare *query estese* per eseguire contemporaneamente operazioni SnapMirror su molte relazioni SnapMirror. Ad esempio, potrebbero essere presenti più relazioni SnapMirror non inizializzate che si desidera inizializzare utilizzando un solo comando.

A proposito di questa attività

È possibile applicare query estese alle seguenti operazioni SnapMirror:

- Inizializzazione delle relazioni non inizializzate
- Ripresa delle relazioni in quiescenza
- Risincronizzazione delle relazioni interrotte
- Aggiornamento delle relazioni inattive
- Interruzione dei trasferimenti di dati di relazione

Fase

1. Eseguire un'operazione SnapMirror su molte relazioni:

   `snapmirror command {-state state } *`

   Il comando seguente inizializza le relazioni SnapMirror che si trovano in un `Uninitialized` stato:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

Garantire una copia Snapshot comune in un'implementazione del vault mirror

È possibile utilizzare `snapmirror snapshot-owner create` Per conservare una copia Snapshot etichettata sul secondario in una distribuzione con vault mirror. In questo modo si garantisce l'esistenza di una copia Snapshot comune per l'aggiornamento della relazione del vault.

A proposito di questa attività

Se si utilizza una combinazione di fan-out del vault mirror o distribuzione a cascata, tenere presente che gli aggiornamenti non avranno esito positivo se non esiste una copia Snapshot comune sui volumi di origine e di destinazione.

Questo non è mai un problema per la relazione del mirror in una distribuzione fan-out o cascata del vault mirror, poiché SnapMirror crea sempre una copia Snapshot del volume di origine prima di eseguire l'aggiornamento.

Tuttavia, potrebbe trattarsi di un problema per la relazione del vault, poiché SnapMirror non crea una copia Snapshot del volume di origine quando aggiorna una relazione del vault. È necessario utilizzare `snapmirror snapshot-owner create` Per garantire la presenza di almeno una copia Snapshot comune sia sull'origine che sulla destinazione della relazione del vault.

Fasi

1. Sul volume di origine, assegnare un proprietario alla copia Snapshot etichettata che si desidera conservare:

   `snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot snapshot -owner owner`

   L'esempio seguente assegna `ApplicationA` in qualità di proprietario di `snap1` Copia Snapshot:

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

2. Aggiornare la relazione mirror, come descritto in "Aggiornamento manuale di una relazione di replica".

   In alternativa, è possibile attendere l'aggiornamento pianificato della relazione mirror.

3. Trasferire la copia Snapshot etichettata nella destinazione del vault:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, … -source-snapshot snapshot`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene trasferito il `snap1` Copia Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   La copia Snapshot etichettata viene mantenuta quando la relazione del vault viene aggiornata.

4. Sul volume di origine, rimuovere il proprietario dalla copia Snapshot etichettata:

   `snapmirror snapshot-owner delete -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-owner` *`owner`*

   I seguenti esempi vengono rimossi `ApplicationA` in qualità di proprietario di `snap1` Copia Snapshot:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

Versioni ONTAP compatibili per le relazioni SnapMirror

Prima di creare una relazione di data Protection SnapMirror, i volumi di origine e destinazione devono eseguire versioni di ONTAP compatibili. Prima di eseguire l'aggiornamento di ONTAP, devi verificare che la tua versione attuale di ONTAP sia compatibile con la tua versione di ONTAP di destinazione per le relazioni SnapMirror.

Relazioni di replica unificate

Per le relazioni SnapMirror di tipo "XDP", utilizzando release on-premise o Cloud Volumes ONTAP:

A partire da ONTAP 9.9.0:

- Le release ONTAP 9.x,0 sono release solo per cloud e supportano i sistemi Cloud Volumes ONTAP. L'asterisco (*) dopo la versione della release indica una release solo cloud.
- Le release ONTAP 9.x,1 sono release generali e supportano sistemi Cloud Volumes ONTAP e on-premise.

L'interoperabilità è bidirezionale.

Interoperabilità per ONTAP versione 9.3 e successive

Versione di ONTAP…	Interagisce con queste versioni precedenti di ONTAP…																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3
9.14.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No	No	No	No
9.14.0*	**Sì**	**Sì**	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	No	No	No	No
9.13.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No	No	No
9.13.0*	**Sì**	No	**Sì**	**Sì**	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	No	No	No	No
9.12.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No	No
9.12.0*	**Sì**	No	**Sì**	No	**Sì**	**Sì**	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	**Sì**	No	No	No	No
9.11.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No
9.11.0*	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	**Sì**	**Sì**	No	**Sì**	No	**Sì**	**Sì**	**Sì**	No	No	No
9.10.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.10.0*	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	**Sì**	**Sì**	No	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.9.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.9.0*	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.8	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	**Sì**

9.7	No	No	No	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	**Sì**
9.6	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	**Sì**
9.5	No	No	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**
9.3	No	No	No	No	No	No	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**

Relazioni sincroni di SnapMirror

SnapMirror Synchronous non è supportato per le istanze cloud di ONTAP.

Versione di ONTAP …	Interagisce con queste versioni precedenti di ONTAP…									
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No
9.13.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.12.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.11.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No	No
9.10.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No	No
9.9.1	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No	No
9.8	**Sì**	**Sì**	**Sì**	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**	No
9.7	No	**Sì**	**Sì**	No	No	**Sì**	**Sì**	**Sì**	**Sì**	**Sì**
9.6	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**	**Sì**
9.5	No	No	No	No	No	No	No	**Sì**	**Sì**	**Sì**

Relazioni di disaster recovery di SnapMirror SVM

- Per i dati di disaster recovery SVM e la protezione SVM:

  Il disaster recovery delle SVM è supportato solo tra cluster che eseguono la stessa versione di ONTAP. **L'indipendenza dalla versione non è supportata per la replica SVM**.

- Per il disaster recovery SVM per la migrazione SVM:
  - La replica è supportata in una singola direzione da una versione precedente di ONTAP sull'origine alla stessa o versione successiva di ONTAP sulla destinazione.
- La versione di ONTAP nel cluster di destinazione non deve essere più recente di due versioni principali on-premise o due versioni principali di cloud più recenti, come mostrato nella tabella seguente.
  - La replica non è supportata per i casi di utilizzo a lungo termine della protezione dei dati.

L'asterisco (*) dopo la versione della release indica una release solo cloud.

Per determinare il supporto, individuare la versione di origine nella colonna della tabella a sinistra, quindi

individuare la versione di destinazione nella riga superiore (DR/migrazione per le versioni simili e migrazione solo per le versioni più recenti).

Origine	Destinazione																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9.3	Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione													
9.4		Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione												
9.5			Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione											
9.6				Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione										
9.7					Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione									
9.8						Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione								
9.9.0*							Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione							
9.9.1								Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione						
9.10.0*									Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione					
9.10.1										Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione				

9.11.0*											Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione			
9.11.1												Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione		
9.12.0*													Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione	
9.12.1														Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione
9.13.0*															Dr/migrazione	Migrazione	Migrazione	Migrazione
9.13.1																Dr/migrazione	Migrazione	Migrazione
9.14.0*																	Dr/migrazione	Migrazione
9.14.1																		Dr/migrazione

Relazioni di disaster recovery di SnapMirror

Per le relazioni SnapMirror di tipo “DP” e di tipo di policy “async-mirror”:

> I mirror di tipo DP non possono essere inizializzati a partire da ONTAP 9.11.1 e sono completamente deprecati in ONTAP 9.12.1. Per ulteriori informazioni, vedere "Deprecazione delle relazioni SnapMirror per la protezione dei dati".

> Nella tabella seguente, la colonna a sinistra indica la versione di ONTAP sul volume di origine, mentre la riga superiore indica le versioni di ONTAP disponibili sul volume di destinazione.

Origine	Destinazione											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9
9.11.1	Sì	No	No	No	No	No	No	No	No	No	No	No

9.10.1	Sì	Sì	No	No	No	No	No	No	No	No	No	No
9.9.1	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No
9.8	No	Sì	Sì	Sì	No	No	No	No	No	No	No	No
9.7	No	No	Sì	Sì	Sì	No	No	No	No	No	No	No
9.6	No	No	No	Sì	Sì	Sì	No	No	No	No	No	No
9.5	No	No	No	No	Sì	Sì	Sì	No	No	No	No	No
9.4	No	No	No	No	No	Sì	Sì	Sì	No	No	No	No
9.3	No	No	No	No	No	No	Sì	Sì	Sì	No	No	No
9.2	No	No	No	No	No	No	No	Sì	Sì	Sì	No	No
9.1	No	No	No	No	No	No	No	No	Sì	Sì	Sì	No
9	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì

L'interoperabilità non è bidirezionale.

Limitazioni di SnapMirror

Prima di creare una relazione di protezione dei dati, è necessario conoscere le limitazioni di base di SnapMirror.

- Un volume di destinazione può avere un solo volume di origine.

  Un volume di origine può avere più volumi di destinazione. Il volume di destinazione può essere il volume di origine per qualsiasi tipo di relazione di replica di SnapMirror.

- A seconda del modello di array, è possibile utilizzare un massimo di otto o sedici volumi di destinazione da un singolo volume di origine. Vedere "Hardware Universe" per ulteriori informazioni sulla configurazione specifica.
- Non è possibile ripristinare i file sulla destinazione di una relazione di DR di SnapMirror.
- I volumi SnapVault di origine o di destinazione non possono essere a 32 bit.
- Il volume di origine per una relazione SnapVault non deve essere un volume FlexClone.

  La relazione funzionerà, ma l'efficienza offerta dai volumi FlexClone non verrà preservata.

Archiviazione e conformità con la tecnologia SnapLock

Che cos'è SnapLock

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage WORM per conservare i file in forma non modificata a scopo normativo e di governance.

SnapLock aiuta a prevenire l'eliminazione, la modifica o la ridenominazione dei dati per soddisfare normative

come SEC 17a-4, HIPAA, FINRA, CFTC e GDPR. Con SnapLock, è possibile creare volumi speciali in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non scrivibile per un determinato periodo di conservazione o a tempo indeterminato. SnapLock consente di eseguire questa conservazione a livello di file attraverso protocolli di file aperti standard come CIFS e NFS. I protocolli di file aperti supportati per SnapLock sono NFS (versioni 2, 3 e 4) e CIFS (SMB 1.0, 2.0 e 3.0).

Utilizzando SnapLock, è possibile assegnare file e copie Snapshot allo storage WORM e impostare periodi di conservazione per i dati protetti DA WORM. Lo storage WORM di SnapLock utilizza la tecnologia Snapshot di NetApp e può sfruttare la replica SnapMirror e i backup SnapVault come tecnologia di base per fornire la protezione del backup recovery per i dati. Scopri di più sullo storage WORM: "Storage WORM conforme con NetApp SnapLock - TR-4526".

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare la funzione di autocommit di SnapLock per il commit automatico dei file IN WORM. È possibile utilizzare un *file .WORM_appendibile* per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log. Per ulteriori informazioni, vedere "Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili".

SnapLock supporta metodi di protezione dei dati che devono soddisfare la maggior parte dei requisiti di conformità:

- È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Vedere "Assegnare le copie Snapshot a WORM".
- È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery. Vedere "Mirrorare i file WORM".

SnapLock è una funzionalità basata su licenza di NetApp ONTAP. Una singola licenza consente di utilizzare SnapLock in modalità di conformità rigorosa, per soddisfare mandati esterni come la norma SEC 17a-4 e una modalità aziendale più allentata, per soddisfare le normative interne per la protezione delle risorse digitali. Le licenze SnapLock fanno parte di "ONTAP uno" suite software.

SnapLock è supportato su tutti i sistemi AFF e FAS e su ONTAP Select. SnapLock non è una soluzione solo software, ma è una soluzione hardware e software integrata. Questa distinzione è importante per le rigide normative WORM come SEC 17a-4, che richiede una soluzione hardware e software integrata. Per ulteriori informazioni, fare riferimento a. "SEC interpretation: Archiviazione elettronica dei record dei broker-dealer".

Cosa puoi fare con SnapLock

Dopo aver configurato SnapLock, è possibile completare le seguenti attività:

- "Esegui il commit dei file su WORM"
- "Assegnare copie Snapshot a WORM per lo storage secondario"
- "Mirroring dei file WORM per il disaster recovery"
- "Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali"
- "Eliminare i file WORM utilizzando la funzione di eliminazione con privilegi"
- "Impostare il periodo di conservazione del file"
- "Spostare un volume SnapLock"
- "Bloccare una copia Snapshot per la protezione dagli attacchi ransomware"
- "Esaminare l'utilizzo di SnapLock con il registro di controllo"
- "Utilizzare le API di SnapLock"

Conformità SnapLock e modalità aziendali

La conformità SnapLock e le modalità aziendali differiscono principalmente per il livello di protezione dei file WORM in ciascuna modalità:

Modalità SnapLock	Livello di protezione	Eliminazione del file WORM durante la conservazione
Modalità compliance	A livello di file	Impossibile eliminare
Modalità Enterprise	A livello di disco	Può essere eliminato dall'amministratore della compliance utilizzando una procedura controllata di "eliminazione con privilegi"

Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari. Una volta che un file è stato salvato in WORM, sia in modalità Compliance che Enterprise, non può essere modificato, anche dopo che il periodo di conservazione è scaduto.

Non è possibile spostare un file WORM durante o dopo il periodo di conservazione. È possibile copiare un file WORM, ma la copia non conserverà le sue caratteristiche WORM.

La seguente tabella mostra le differenze nelle funzionalità supportate dalle modalità di conformità SnapLock e Enterprise:

Funzionalità	Conformità SnapLock	Azienda SnapLock
Abilitare ed eliminare i file utilizzando l'opzione di eliminazione con privilegi	No	Sì
Reinizializzare i dischi	No	Sì
Distruggere gli aggregati e i volumi SnapLock durante il periodo di conservazione	No	Sì, ad eccezione del volume del registro di controllo di SnapLock
Rinominare aggregati o volumi	No	Sì
Utilizzare dischi non NetApp	No	Sì (con "Virtualizzazione FlexArray")
Utilizzare il volume SnapLock per la registrazione dell'audit	Sì	Sì, a partire da ONTAP 9.5

Funzioni supportate e non supportate con SnapLock

La seguente tabella mostra le funzionalità supportate dalla modalità di conformità SnapLock, dalla modalità aziendale SnapLock o da entrambe:

Funzione	Supportato con conformità SnapLock	Supportato con SnapLock Enterprise
Gruppi di coerenza	No	No
Volumi crittografati	Sì, a partire da ONTAP 9.2. Scopri di più Encryption e SnapLock.	Sì, a partire da ONTAP 9.2. Scopri di più Encryption e SnapLock.
FabricPools su aggregati SnapLock	No	Sì, a partire da ONTAP 9.8. Scopri di più FabricPool su aggregati aziendali SnapLock.
Aggregati di Flash Pool	Sì, a partire da ONTAP 9.1.	Sì, a partire da ONTAP 9.1.
FlexClone	È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.	È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.
Volumi FlexGroup	Sì, a partire da ONTAP 9.11.1. Scopri di più [flexgroup].	Sì, a partire da ONTAP 9.11.1. Scopri di più [flexgroup].
LUN	No Scopri di più Supporto del LUN Con SnapLock.	No Scopri di più Supporto del LUN Con SnapLock.
Configurazioni MetroCluster	Sì, a partire da ONTAP 9.3. Scopri di più Supporto MetroCluster.	Sì, a partire da ONTAP 9.3. Scopri di più Supporto MetroCluster.
Verifica multi-admin (MAV)	Sì, a partire da ONTAP 9.13.1. Scopri di più Supporto MAV.	Sì, a partire da ONTAP 9.13.1. Scopri di più Supporto MAV.
SAN	No	No
SnapRestore a file singolo	No	Sì
Continuità aziendale di SnapMirror	No	No
SnapRestore	No	Sì
SMTape	No	No
SnapMirror sincrono	No	No
SSD	Sì, a partire da ONTAP 9.1.	Sì, a partire da ONTAP 9.1.
Funzionalità per l'efficienza dello storage	Sì, a partire da ONTAP 9.9.1. Scopri di più supporto per l'efficienza dello storage.	Sì, a partire da ONTAP 9.9.1. Scopri di più supporto per l'efficienza dello storage.

FabricPool su aggregati aziendali SnapLock

FabricPool sono supportati negli aggregati aziendali di SnapLock a partire da ONTAP 9.8. Tuttavia, il tuo account team deve aprire una richiesta di variazione del prodotto che documenta che sei consapevole del fatto che i dati FabricPool su più livelli di un cloud pubblico o privato non sono più protetti da SnapLock perché un amministratore del cloud può eliminare tali dati.

> Tutti i dati che FabricPool esegue il Tier in un cloud pubblico o privato non sono più protetti da SnapLock perché tali dati possono essere cancellati da un amministratore del cloud.

Volumi FlexGroup

SnapLock supporta i volumi FlexGroup a partire da ONTAP 9.11.1; tuttavia, le seguenti funzionalità non sono supportate:

- Conservazione a fini giudiziari
- Conservazione basata sugli eventi
- SnapLock per SnapVault (supportato a partire da ONTAP 9.12.1)

È inoltre necessario conoscere i seguenti comportamenti:

- Il clock di compliance del volume (VCC) di un volume FlexGroup è determinato dal VCC del costituente root. Tutti i componenti non root avranno il proprio VCC strettamente sincronizzato con il VCC root.
- Le proprietà di configurazione di SnapLock sono impostate solo su FlexGroup nel suo complesso. I singoli componenti non possono avere proprietà di configurazione diverse, come il tempo di conservazione predefinito e il periodo di autocommit.

Supporto del LUN

Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

Supporto MetroCluster

Il supporto SnapLock nelle configurazioni MetroCluster varia tra la modalità di conformità SnapLock e la modalità aziendale SnapLock.

Conformità SnapLock

- A partire da ONTAP 9.3, la conformità SnapLock è supportata su aggregati MetroCluster senza mirror.
- A partire da ONTAP 9.3, la conformità SnapLock è supportata sugli aggregati mirrorati, ma solo se l’aggregato viene utilizzato per ospitare i volumi del registro di controllo SnapLock.
- Le configurazioni SnapLock specifiche di SVM possono essere replicate su siti primari e secondari utilizzando MetroCluster.

Azienda SnapLock

- A partire da ONTAP 9, sono supportati gli aggregati aziendali di SnapLock.
- A partire da ONTAP 9.3, sono supportati gli aggregati aziendali SnapLock con eliminazione con privilegi.

- Le configurazioni SnapLock specifiche di SVM possono essere replicate in entrambi i siti utilizzando MetroCluster.

Configurazioni MetroCluster e orologi per la compliance

Le configurazioni MetroCluster utilizzano due meccanismi di clock di compliance, il clock di compliance del volume (VCC) e il clock di compliance del sistema (SCC). VCC e SCC sono disponibili per tutte le configurazioni SnapLock. Quando si crea un nuovo volume su un nodo, il relativo VCC viene inizializzato con il valore corrente di SCC su quel nodo. Una volta creato il volume, il tempo di conservazione del volume e del file viene sempre monitorato con il VCC.

Quando un volume viene replicato in un altro sito, viene replicato anche il relativo VCC. Quando si verifica uno switchover del volume, ad esempio dal sito A al sito B, il VCC continua ad essere aggiornato sul sito B mentre il SCC sul sito A si arresta quando il sito A passa alla modalità offline.

Quando il sito A viene riportato in linea e viene eseguito il switchback del volume, il clock SCC del sito A viene riavviato mentre il VCC del volume continua ad essere aggiornato. Poiché il VCC viene costantemente aggiornato, indipendentemente dalle operazioni di switchover e switchback, i tempi di conservazione dei file non dipendono dai clock SCC e non si allungano.

Supporto MAV (Multi-admin Ververifica)

A partire da ONTAP 9.13.1, un amministratore del cluster può abilitare esplicitamente la verifica multi-admin su un cluster per richiedere l'approvazione del quorum prima che vengano eseguite alcune operazioni SnapLock. Quando MAV è attivato, le proprietà del volume SnapLock come default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period e Privileged-delete richiedono l'approvazione del quorum. Scopri di più "MAV".

Efficienza dello storage

A partire da ONTAP 9.9.1, SnapLock supporta funzionalità di efficienza dello storage, come la compattazione dei dati, la deduplica tra volumi e la compressione adattiva per volumi e aggregati SnapLock. Per ulteriori informazioni sull'efficienza dello storage, vedere "Panoramica sulla gestione dello storage logico con la CLI".

Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

Disclaimer: NetApp non può garantire che i file WORM protetti da SnapLock su dischi o volumi con crittografia automatica possano essere recuperati se la chiave di autenticazione viene persa o se il numero di tentativi di autenticazione non riusciti supera il limite specificato e il disco viene bloccato in modo permanente. È responsabilità dell'utente garantire la protezione dagli errori di autenticazione.

> A partire da ONTAP 9.2, i volumi crittografati sono supportati negli aggregati SnapLock.

Transizione 7-Mode

È possibile migrare i volumi SnapLock da 7-Mode a ONTAP utilizzando la funzione CBT (Copy-Based Transition) dello strumento di transizione 7-Mode. La modalità SnapLock del volume di destinazione, Compliance o Enterprise, deve corrispondere alla modalità SnapLock del volume di origine. Non è possibile utilizzare la transizione senza copia (CFT) per migrare i volumi SnapLock.

Configurare SnapLock

Configurare SnapLock

Prima di utilizzare SnapLock, è necessario configurare SnapLock completando varie attività, ad esempio "Installare la licenza SnapLock" Per ogni nodo che ospita un aggregato con un volume SnapLock, inizializzare l' "Orologio di conformità", Creare un aggregato SnapLock per i cluster che eseguono release ONTAP precedenti a ONTAP 9.10.1, "Creare e montare un volume SnapLock"e molto altro ancora.

Inizializzare il Compliance Clock

SnapLock utilizza *Volume Compliance Clock* per evitare manomissioni che potrebbero alterare il periodo di conservazione dei file WORM. È necessario prima inizializzare il *system ComplianceClock* su ogni nodo che ospita un aggregato SnapLock.

A partire da ONTAP 9.14.1, è possibile inizializzare o reinizializzare il clock di conformità del sistema quando non ci sono volumi SnapLock o nessun volume con il blocco delle copie Snapshot attivato. La possibilità di reinizializzare consente agli amministratori di sistema di reimpostare l'orologio di conformità del sistema nei casi in cui potrebbe essere stato inizializzato in modo errato o di correggere la deriva dell'orologio sul sistema. In ONTAP 9.13.1 e nelle versioni precedenti, una volta inizializzato il Compliance Clock su un nodo, non è possibile inizializzarlo nuovamente.

Prima di iniziare

Per reinizializzare il Compliance Clock:

- Tutti i nodi nel cluster devono essere in stato integro.
- Tutti i volumi devono essere online.
- La coda di ripristino non può contenere volumi.
- Non può essere presente alcun volume SnapLock.
- Non può essere presente alcun volume con il blocco della copia Snapshot abilitato.

Requisiti generali per l'inizializzazione dell'orologio di conformità:

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- "La licenza SnapLock deve essere installata sul nodo".

A proposito di questa attività

L'ora del Compliance Clock del sistema viene ereditata dal *Volume Compliance Clock*, quest'ultimo dei quali controlla il periodo di conservazione dei file WORM sul volume. Il clock di conformità del volume viene inizializzato automaticamente quando si crea un nuovo volume SnapLock.

> L'impostazione iniziale dell'orologio di conformità del sistema si basa sull'orologio di sistema hardware corrente. Per questo motivo, è necessario verificare che l'ora e il fuso orario del sistema siano corretti prima di inizializzare l'orologio di conformità del sistema su ciascun nodo. Una volta inizializzato il clock di conformità del sistema su un nodo, non è possibile inizializzarlo nuovamente quando sono presenti volumi SnapLock o volumi con blocco abilitato.

Fasi

È possibile utilizzare la CLI di ONTAP per inizializzare l'orologio di conformità oppure, a partire da ONTAP 9.12.1, utilizzare Gestione sistema per inizializzare l'orologio di conformità.

System Manager

1. Accedere a **Cluster > Panoramica**.
2. Nella sezione **nodi**, fare clic su **Inizializza clock di conformità SnapLock**.
3. Per visualizzare la colonna **Orologio conformità** e verificare che l'Orologio conformità sia inizializzato, nella sezione **Cluster > Panoramica > nodi**, fare clic su **Mostra/Nascondi** e selezionare **Orologio conformità SnapLock**.

CLI

1. Inizializzare l'orologio di conformità del sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   Il seguente comando inizializza il Compliance Clock del sistema su `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. Quando richiesto, confermare che l'orologio di sistema è corretto e che si desidera inizializzare l'orologio di conformità:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Ripetere questa procedura per ogni nodo che ospita un aggregato SnapLock.

Abilitare la risincronizzazione del clock di conformità per un sistema configurato con NTP

È possibile attivare la funzione di sincronizzazione dell'ora dell'orologio di conformità SnapLock quando è configurato un server NTP.

Di cosa hai bisogno

- Questa funzione è disponibile solo al livello di privilegio avanzato.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- "La licenza SnapLock deve essere installata sul nodo".
- Questa funzione è disponibile solo per le piattaforme Cloud Volumes ONTAP, ONTAP Select e VSIM.

A proposito di questa attività

Quando il daemon di clock sicuro SnapLock rileva un'inclinazione oltre la soglia, ONTAP utilizza l'ora di sistema per reimpostare sia il sistema che i blocchi di conformità del volume. Come soglia di disallineamento viene impostato un periodo di 24 ore. Ciò significa che l'orologio di conformità del sistema è sincronizzato con l'orologio di sistema solo se l'inclinazione è più vecchia di un giorno.

Il daemon dell'orologio sicuro SnapLock rileva un'inclinazione e modifica l'orologio di conformità all'ora del sistema. Qualsiasi tentativo di modifica dell'ora di sistema per forzare la sincronizzazione dell'orologio di conformità con l'ora di sistema non riesce, poiché l'orologio di conformità si sincronizza con l'ora di sistema solo se l'ora di sistema è sincronizzata con l'ora NTP.

Fasi

1. Attivare la funzione sincronizzazione orologio conformità SnapLock quando è configurato un server NTP:

   `snaplock compliance-clock ntp`

   Il seguente comando abilita la funzione di sincronizzazione dell'ora dell'orologio di conformità del sistema:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. Quando richiesto, verificare che i server NTP configurati siano attendibili e che il canale di comunicazione sia sicuro per abilitare la funzione:
3. Verificare che la funzione sia attivata:

   `snaplock compliance-clock ntp show`

   Il seguente comando verifica che la funzione di sincronizzazione dell'ora del clock di conformità del sistema sia attivata:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Creare un aggregato SnapLock

Il volume viene utilizzato `-snaplock-type` Opzione per specificare un tipo di volume Compliance o Enterprise SnapLock. Per le release precedenti a ONTAP 9.10.1, è necessario creare un aggregato SnapLock separato. A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Il SnapLock "la licenza deve essere installata" sul nodo. Questa licenza è inclusa in "ONTAP uno".
- "È necessario inizializzare il Compliance Clock sul nodo".
- Se i dischi sono stati partizionati come "root", "data1" e "data2", è necessario assicurarsi che siano

disponibili dischi di riserva.

Considerazioni sull'upgrade

Quando si esegue l'aggiornamento a ONTAP 9.10.1, gli aggregati SnapLock e non SnapLock esistenti vengono aggiornati per supportare l'esistenza di volumi SnapLock e non SnapLock; tuttavia, gli attributi dei volumi SnapLock esistenti non vengono aggiornati automaticamente. Ad esempio, i campi di compaction dei dati, deduplica di volumi incrociati e deduplica di background di volumi incrociati rimangono invariati. I nuovi volumi SnapLock creati sugli aggregati esistenti hanno gli stessi valori predefiniti dei volumi non SnapLock e i valori predefiniti per i nuovi volumi e aggregati dipendono dalla piattaforma.

Considerazioni sul revert

Se è necessario ripristinare una versione di ONTAP precedente alla 9.10.1, è necessario spostare tutti i volumi SnapLock Compliance, SnapLock Enterprise e SnapLock nei propri aggregati SnapLock.

A proposito di questa attività

- Non è possibile creare aggregati di conformità per le LUN FlexArray, ma gli aggregati di conformità SnapLock sono supportati con le LUN FlexArray.
- Non è possibile creare aggregati di conformità con l'opzione SyncMirror.
- È possibile creare aggregati di conformità mirrorati in una configurazione MetroCluster solo se l'aggregato viene utilizzato per ospitare volumi di log di audit SnapLock.

> In una configurazione MetroCluster, SnapLock Enterprise è supportato su aggregati mirrorati e senza mirror. La conformità SnapLock è supportata solo su aggregati senza mirror.

Fasi

1. Creare un aggregato SnapLock:

   ```
   storage aggregate create -aggregate <aggregate_name> -node <node_name>
   -diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
   ```

   La pagina man del comando contiene un elenco completo di opzioni.

   Il seguente comando crea un SnapLock `Compliance` aggregato con nome `aggr1` con tre dischi su `node1`:

   ```
   cluster1::> storage aggregate create -aggregate aggr1 -node node1
   -diskcount 3 -snaplock-type compliance
   ```

Creare e montare volumi SnapLock

È necessario creare un volume SnapLock per i file o le copie Snapshot che si desidera assegnare allo stato WORM. A partire da ONTAP 9.10.1, qualsiasi volume creato, indipendentemente dal tipo di aggregato, viene creato per impostazione predefinita come volume non SnapLock. È necessario utilizzare `-snaplock-type` Opzione per creare esplicitamente un volume SnapLock specificando Compliance o Enterprise come tipo SnapLock. Per impostazione predefinita, il tipo di SnapLock è impostato su `non-`

`snaplock`.

Prima di iniziare

- L'aggregato SnapLock deve essere online.
- Dovresti "Verificare che sia installata una licenza SnapLock". Se una licenza SnapLock non è installata sul nodo, è necessario "installare" it. Questa licenza è inclusa con "ONTAP uno". Prima di ONTAP One, la licenza SnapLock era inclusa nel pacchetto sicurezza e conformità. Il bundle Security and Compliance non è più offerto, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo "Eseguire l'aggiornamento a ONTAP One".
- "È necessario inizializzare il Compliance Clock sul nodo".

A proposito di questa attività

Con le autorizzazioni SnapLock appropriate, è possibile distruggere o rinominare un volume Enterprise in qualsiasi momento. Non è possibile distruggere un volume Compliance fino allo scadere del periodo di conservazione. Non è mai possibile rinominare un volume Compliance.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock. Il volume clone sarà dello stesso tipo di SnapLock del volume padre.

> I LUN non sono supportati nei volumi SnapLock. Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

Eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per creare un volume SnapLock.

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi) e fare clic su **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), fare clic su **More Options** (altre opzioni).
3. Inserire le informazioni sul nuovo volume, inclusi il nome e le dimensioni del volume.
4. Selezionare **Enable SnapLock** (attiva conformità) e scegliere il tipo di SnapLock, Compliance (conformità) o Enterprise (Azienda).
5. Nella sezione **Auto-commit Files**, selezionare **Modified** e inserire il tempo in cui un file deve rimanere invariato prima che venga automaticamente salvato. Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.
6. Nella sezione **conservazione dei dati**, selezionare il periodo di conservazione minimo e massimo.
7. Selezionare il periodo di conservazione predefinito.
8. Fare clic su **Save** (Salva).
9. Selezionare il nuovo volume nella pagina **Volumes** per verificare le impostazioni SnapLock.

CLI

1. Creare un volume SnapLock:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise>
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando. Le seguenti opzioni non sono disponibili per i volumi SnapLock: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, e. `vmalign`.

   Il seguente comando crea un SnapLock `Compliance` volume denominato `vol1` acceso `aggr1` acceso `vs1`:

   ```
   cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
   -snaplock-type compliance
   ```

Montare un volume SnapLock

È possibile montare un volume SnapLock su un percorso di giunzione nello spazio dei nomi SVM per l'accesso al client NAS.

Di cosa hai bisogno

Il volume SnapLock deve essere online.

A proposito di questa attività

- È possibile montare un volume SnapLock solo sotto la directory principale della SVM.

- Non è possibile montare un volume normale sotto un volume SnapLock.

Fasi

1. Montare un volume SnapLock:

   volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando consente di montare un volume SnapLock denominato `vol1` al percorso di giunzione `/sales` in `vs1` spazio dei nomi:

   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Impostare il tempo di conservazione

È possibile impostare il tempo di conservazione per un file in modo esplicito oppure utilizzare il periodo di conservazione predefinito per il volume per derivare il tempo di conservazione. A meno che non si definisca esplicitamente il tempo di conservazione, SnapLock utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione. È inoltre possibile impostare la conservazione dei file dopo un evento.

Informazioni sul periodo di conservazione e sul tempo di conservazione

Il *periodo di conservazione* per un file WORM specifica il periodo di tempo in cui il file deve essere conservato dopo il commit allo stato WORM. Il *tempo di conservazione* per un file WORM è il tempo dopo il quale il file non deve più essere conservato. Un periodo di conservazione di 20 anni per un file impegnato nello stato WORM il 10 novembre 2020 alle 6:00, ad esempio, avrebbe un tempo di conservazione del 10 novembre 2040 alle 6:00

> A partire da ONTAP 9.10.1, è possibile impostare un periodo di conservazione fino al 26 ottobre 3058 e un periodo di conservazione fino a 100 anni. Quando estendi le date di conservazione, le policy precedenti vengono convertite automaticamente. In ONTAP 9.9.1 e versioni precedenti, a meno che il periodo di conservazione predefinito non sia impostato su infinito, il tempo di conservazione massimo supportato è gennaio 19 2071 (GMT).

Considerazioni importanti sulla replica

Quando si stabilisce una relazione di SnapMirror con un volume di origine SnapLock utilizzando una data di conservazione successiva al 19 gennaio 2071 (GMT), il cluster di destinazione deve eseguire ONTAP 9.10.1 o versione successiva, altrimenti il trasferimento di SnapMirror avrà esito negativo.

Considerazioni importanti sul revert

ONTAP impedisce di ripristinare un cluster da ONTAP 9.10.1 a una versione precedente di ONTAP quando sono presenti file con un periodo di conservazione successivo a "19 gennaio 2071 8:44:07".

Comprensione dei periodi di conservazione

Un volume aziendale o di conformità SnapLock prevede quattro periodi di conservazione:

- Periodo minimo di conservazione (`min`), con un valore predefinito pari a 0
- Periodo di conservazione massimo (`max`), con un valore predefinito di 30 anni
- Periodo di conservazione predefinito, con un valore predefinito pari a. `min` Sia per la modalità Compliance che per la modalità Enterprise a partire da ONTAP 9.10.1. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, il periodo di conservazione predefinito dipende dalla modalità:
  - Per la modalità Compliance, l'impostazione predefinita è uguale a. `max`.
  - Per la modalità Enterprise, il valore predefinito è uguale a. `min`.
- Periodo di conservazione non specificato.

  A partire da ONTAP 9.8, è possibile impostare il periodo di conservazione dei file in un volume su `unspecified`, per consentire la conservazione del file fino a quando non si imposta un tempo di conservazione assoluto. È possibile impostare un file con tempo di conservazione assoluto su conservazione non specificata e su conservazione assoluta, a condizione che il nuovo tempo di conservazione assoluto sia successivo al tempo assoluto impostato in precedenza.

  A partire da ONTAP 9.12.1, i file WORM con il periodo di conservazione impostato su `unspecified` È garantito che un periodo di conservazione sia impostato sul periodo di conservazione minimo configurato per il volume SnapLock. Quando si modifica il periodo di conservazione del file da `unspecified` per un tempo di conservazione assoluto, il nuovo tempo di conservazione specificato deve essere maggiore del tempo di conservazione minimo già impostato nel file.

Pertanto, se non si imposta esplicitamente il tempo di conservazione prima di impostare un file in modalità Compliance allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 30 anni. Allo stesso modo, se non si imposta esplicitamente il tempo di conservazione prima di eseguire il commit di un file in modalità Enterprise allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 0 anni o, effettivamente, per niente.

Impostare il periodo di conservazione predefinito

È possibile utilizzare `volume snaplock modify` Per impostare il periodo di conservazione predefinito per i file su un volume SnapLock.

Di cosa hai bisogno

Il volume SnapLock deve essere online.

A proposito di questa attività

La tabella seguente mostra i valori possibili per l'opzione periodo di conservazione predefinito:

> Il periodo di conservazione predefinito deve essere maggiore o uguale al (>=) periodo di conservazione minimo e minore o uguale al (⇐) periodo di conservazione massimo.

Valore	Unità	Note
0 - 65535	secondi	

Valore	Unità	Note
0 - 24	ore	
0 - 365	giorni	
0 - 12	mesi	
0 - 100	anni	A partire da ONTAP 9.10.1. Per le release precedenti di ONTAP, il valore è 0 - 70.
max	-	Utilizzare il periodo di conservazione massimo.
min	-	Utilizzare il periodo di conservazione minimo.
infinito	-	Conserva i file per sempre.
non specificato	-	Conservare i file fino a quando non viene impostato un periodo di conservazione assoluto.

I valori e gli intervalli dei periodi di conservazione massimo e minimo sono identici, ad eccezione di `max` e. `min`, che non sono applicabili. Per ulteriori informazioni su questa attività, vedere "Imposta la panoramica del tempo di conservazione".

È possibile utilizzare `volume snaplock show` per visualizzare le impostazioni del periodo di conservazione per il volume. Per ulteriori informazioni, vedere la pagina man del comando.

> Una volta che un file è stato impegnato nello stato WORM, è possibile estendere ma non ridurre il periodo di conservazione.

Fasi

1. Impostare il periodo di conservazione predefinito per i file su un volume SnapLock:

   ```
   volume snaplock modify -vserver SVM_name -volume volume_name -default
   -retention-period default_retention_period -minimum-retention-period
   min_retention_period -maximum-retention-period max_retention_period
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   > Gli esempi seguenti presuppongono che i periodi di conservazione minimo e massimo non siano stati modificati in precedenza.

   Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance o Enterprise su 20 giorni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

Il seguente comando imposta il periodo di conservazione predefinito per un volume Compliance su 70 anni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

Il seguente comando imposta il periodo di conservazione predefinito per un volume Enterprise su 10 anni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

I seguenti comandi impostano il periodo di conservazione predefinito per un volume Enterprise su 10 giorni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance su infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Impostare il tempo di conservazione per un file in modo esplicito

È possibile impostare il tempo di conservazione di un file in modo esplicito modificando l'ultimo tempo di accesso. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'ultimo tempo di accesso.

A proposito di questa attività

Dopo che un file è stato eseguito il commit su WORM, è possibile estendere ma non ridurre il tempo di conservazione. Il tempo di conservazione viene memorizzato in `atime` per il file.

> Non è possibile impostare esplicitamente il tempo di conservazione di un file su `infinite`. Tale valore è disponibile solo quando si utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione.

Fasi

1. Utilizzare un comando o un programma adatto per modificare l'ultimo orario di accesso al file di cui si

desidera impostare il tempo di conservazione.

In una shell UNIX, utilizzare il seguente comando per impostare un tempo di conservazione del 21 novembre 2020 alle 6:00 su un file denominato `document.txt`:

```
touch -a -t 202011210600 document.txt
```

È possibile utilizzare qualsiasi comando o programma adatto per modificare l'ultimo orario di accesso in Windows.

Impostare il periodo di conservazione del file dopo un evento

A partire da ONTAP 9.3, è possibile definire per quanto tempo un file viene conservato dopo un evento utilizzando la funzione di conservazione basata su eventi (EBR)_ di SnapLock.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.

  "Creare un account amministratore di SnapLock"

- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

A proposito di questa attività

Il *criterio di conservazione degli eventi* definisce il periodo di conservazione del file dopo il verificarsi dell'evento. Il criterio può essere applicato a un singolo file o a tutti i file di una directory.

- Se un file non è UN file WORM, viene impegnato nello stato WORM per il periodo di conservazione definito nella policy.
- Se un file è UN file WORM o un file WORM appendibile, il suo periodo di conservazione verrà esteso dal periodo di conservazione definito nella policy.

È possibile utilizzare un volume Compliance-mode o Enterprise-mode.

I criteri EBR non possono essere applicati ai file in stato di conservazione a scopo legale.

Per informazioni sull'utilizzo avanzato, vedere "Storage WORM conforme con NetApp SnapLock".

utilizzo di EBR per estendere il periodo di conservazione dei file WORM già esistenti
EBR è utile quando si desidera estendere il periodo di conservazione dei file WORM già esistenti. Ad esempio, la politica della tua azienda potrebbe essere quella di conservare i record W-4 del dipendente in forma non modificata per tre anni dopo che il dipendente ha modificato un'elezione di ritenuta. Un'altra policy aziendale potrebbe richiedere la conservazione dei record W-4 per cinque anni dopo la cessazione del dipendente. In questa situazione, è possibile creare una policy EBR con un periodo di conservazione di cinque anni. Una volta terminato il dipendente (il "evento"), applicherai la policy EBR al record W-4 del dipendente, prolungandone il periodo di conservazione. In genere, questo sarà più semplice dell'estensione manuale del periodo di conservazione, in particolare quando si tratta di un numero elevato di file.

Fasi

1. Creare un criterio EBR:

   snaplock event-retention policy create -vserver *SVM_name* -name *policy_name* -retention-period *retention_period*

   Il seguente comando crea il criterio EBR `employee_exit` acceso `vs1` con un periodo di conservazione di dieci anni:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Applicare un criterio EBR:

   snaplock event-retention apply -vserver *SVM_name* -name *policy_name* -volume *volume_name* -path *path_name*

   Il seguente comando applica il criterio EBR `employee_exit` acceso `vs1` a tutti i file nella directory `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Creare un registro di controllo

Se utilizzi ONTAP 9.9.1 o versioni precedenti, devi prima creare un aggregato SnapLock e quindi un audit log protetto da SnapLock prima di eseguire un'eliminazione con privilegi o lo spostamento di un volume SnapLock. Il registro di controllo registra la creazione e l'eliminazione degli account amministratore di SnapLock, le modifiche al volume di log, l'eventuale attivazione dell'eliminazione con privilegi, le operazioni di eliminazione con privilegi e le operazioni di spostamento del volume SnapLock.

A partire da ONTAP 9.10.1, non sarà più possibile creare un aggregato SnapLock. Devi utilizzare l'opzione -snaplock-type per "Creare esplicitamente un volume SnapLock" Specificando conformità o impresa come tipo di SnapLock.

Prima di iniziare

Se utilizzi ONTAP 9.9.1 o versioni precedenti, per creare un aggregato SnapLock devi essere un amministratore del cluster.

A proposito di questa attività

Non è possibile eliminare un registro di controllo fino a quando non è trascorso il periodo di conservazione del file di registro. Non è possibile modificare un registro di controllo anche dopo che è trascorso il periodo di conservazione. Ciò vale sia per la conformità SnapLock che per le modalità aziendali.

> In ONTAP 9.4 e versioni precedenti, non è possibile utilizzare un volume aziendale SnapLock per la registrazione dell'audit. È necessario utilizzare un volume di conformità SnapLock. In ONTAP 9.5 e versioni successive, è possibile utilizzare un volume aziendale SnapLock o un volume di conformità SnapLock per la registrazione dell'audit. In tutti i casi, il volume del log di audit deve essere montato sul percorso di giunzione `/snaplock_audit_log`. Nessun altro volume può utilizzare questo percorso di giunzione.

I registri di controllo di SnapLock sono disponibili in `/snaplock_log` directory sotto la directory principale del volume del registro di controllo, in sottodirectory denominate `privdel_log` (operazioni di eliminazione con privilegi) e. `system_log` (tutto il resto). I nomi dei file di log di audit contengono l'indicazione dell'ora della prima operazione registrata, semplificando la ricerca dei record in base all'ora approssimativa in cui sono state eseguite le operazioni.

- È possibile utilizzare `snaplock log file show` per visualizzare i file di log sul volume del registro di controllo.
- È possibile utilizzare `snaplock log file archive` comando per archiviare il file di log corrente e crearne uno nuovo, utile nei casi in cui è necessario registrare le informazioni del log di audit in un file separato.

Per ulteriori informazioni, consulta le pagine man dei comandi.

> Un volume di protezione dei dati non può essere utilizzato come volume del registro di controllo di SnapLock.

Fasi

1. Creare un aggregato SnapLock.

   Creare un aggregato SnapLock

2. Sulla SVM che si desidera configurare per la registrazione dell'audit, creare un volume SnapLock.

   Creare un volume SnapLock

3. Configurare la SVM per la registrazione dell'audit:

   `snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log -size size -retention-period default_retention_period`

   > Il periodo minimo di conservazione predefinito per i file di log di controllo è di sei mesi. Se il periodo di conservazione di un file interessato supera il periodo di conservazione del log di controllo, il periodo di conservazione del log eredita il periodo di conservazione del file. Pertanto, se il periodo di conservazione di un file cancellato mediante eliminazione con privilegi è di 10 mesi e il periodo di conservazione del registro di controllo è di 8 mesi, il periodo di conservazione del registro viene esteso a 10 mesi. Per ulteriori informazioni sul tempo di conservazione e sul periodo di conservazione predefinito, vedere "Impostare il tempo di conservazione".

   Il seguente comando viene configurato `SVM1` Per la registrazione dell'audit utilizzando il volume SnapLock `logVol`. Il registro di controllo ha una dimensione massima di 20 GB e viene conservato per otto mesi.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. Sulla SVM configurata per la registrazione dell'audit, montare il volume SnapLock nel percorso di giunzione `/snaplock_audit_log`.

   Montare un volume SnapLock

Verificare le impostazioni SnapLock

È possibile utilizzare `volume file fingerprint start` e. `volume file fingerprint dump` Comandi per visualizzare informazioni chiave su file e volumi, tra cui il tipo di file (normale, WORM o appendice WORM), la data di scadenza del volume e così via.

Fasi

1. Generare un'impronta digitale del file:

   `volume file fingerprint start -vserver` *`SVM_name`* `-file` *`file_path`*

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   Il comando genera un ID sessione che è possibile utilizzare come input per `volume file fingerprint dump` comando.

   > È possibile utilizzare `volume file fingerprint show` Comando con l'ID di sessione per monitorare l'avanzamento dell'operazione di impronte digitali. Assicurarsi che l'operazione sia stata completata prima di provare a visualizzare l'impronta digitale.

2. Visualizzare l'impronta digitale per il file:

   `volume file fingerprint dump -session-id` *`session_ID`*

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
           Volume:slc_vol
           Path:/vol/slc_vol/f1
           Data
   Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

   Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
   ```

```
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gestire i file WORM

Gestire i file WORM

È possibile gestire i file WORM nei seguenti modi:

- "Esegui il commit dei file su WORM"
- "Assegnare le copie Snapshot a WORM su una destinazione del vault"
- "Mirroring dei file WORM per il disaster recovery"
- "Conservare i file WORM durante i contenziosi"
- "Eliminare i file WORM"

Esegui il commit dei file su WORM

È possibile eseguire il commit dei file in WORM (write once, Read many) manualmente o automaticamente. È inoltre possibile creare file .WORM appendibili.

Esegui il commit dei file in WORM manualmente

Il commit di un file in WORM viene eseguito manualmente rendendo il file di sola lettura. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'attributo Read-write di un file in sola lettura. È possibile scegliere di eseguire il commit manuale dei file se si desidera garantire che un'applicazione abbia terminato la scrittura su un file in modo che il commit del file non venga eseguito in modo prematuro o che si siano riscontrati problemi di scalabilità per lo scanner di autocommit a causa di un elevato numero di volumi.

Di cosa hai bisogno

- Il file che si desidera assegnare deve risiedere in un volume SnapLock.
- Il file deve essere scrivibile.

A proposito di questa attività

Il volume ComplianceClock Time viene scritto su `ctime` del file quando viene eseguito il comando o il programma. Il tempo di ComplianceClock determina quando è stato raggiunto il tempo di conservazione del file.

Fasi

1. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write di un file in sola lettura.

   In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

   ```
   chmod -w document.txt
   ```

   In una shell Windows, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

   ```
   attrib +r document.txt
   ```

Esegui il commit dei file automaticamente SU WORM

La funzione di autocommit di SnapLock consente di assegnare automaticamente i file A WORM. La funzionalità di autocommit commit commette un file allo stato WORM su un volume SnapLock se il file non è stato modificato per la durata del periodo di autocommit. La funzione di invio automatico è disattivata per impostazione predefinita.

Di cosa hai bisogno

- I file che si desidera assegnare automaticamente devono risiedere in un volume SnapLock.
- Il volume SnapLock deve essere online.
- Il volume SnapLock deve essere un volume di lettura/scrittura.

> La funzione di autocommit di SnapLock esegue la scansione di tutti i file nel volume e commit un file se soddisfa i requisiti di autocommit. Potrebbe esserci un intervallo di tempo tra il momento in cui il file è pronto per l'autocommit e il momento in cui viene effettivamente salvato dallo scanner di autocommit SnapLock. Tuttavia, il file è ancora protetto dalle modifiche e dall'eliminazione da parte del file system non appena è idoneo per l'autocommit.

A proposito di questa attività

Il *periodo di autocommit* specifica il periodo di tempo in cui i file devono rimanere invariati prima di eseguire l'autocommit. La modifica di un file prima che sia trascorso il periodo di autocommit riavvia il periodo di autocommit per il file.

La seguente tabella mostra i valori possibili per il periodo di autocommit:

Valore	Unità	Note
nessuno	-	L'impostazione predefinita.
5 - 5256000	minuti	-
1 - 87600	ore	-
1 - 3650	giorni	-
1 - 120	mesi	-
1 - 10	anni	-

> Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.

Fasi

1. Commit automatico dei file su un volume SnapLock in WORM:

   ```
   volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
   -period autocommit_period
   ```

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando esegue il commit automatico dei file sul volume `vol1` Di SVM vs1, a condizione che i file rimangano invariati per 5 ore:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

Creare un file .WORM appendibile

Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. È possibile utilizzare qualsiasi comando o programma adatto per creare un file .WORM appendibile oppure utilizzare la funzione *volume append mode* di SnapLock per creare file .WORM appendibili per impostazione predefinita.

Utilizzare un comando o un programma per creare un file .WORM appendibile

È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per creare un file .WORM appendibile. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

Di cosa hai bisogno

Il file .WORM appendibile deve risiedere su un volume SnapLock.

A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte n×256KB+1 del file, il segmento precedente da 256 KB diventa protetto DA WORM.

Fasi

1. Utilizzare un comando o un programma adatto per creare un file di lunghezza zero con il tempo di conservazione desiderato.

   In una shell UNIX, utilizzare il seguente comando per impostare un tempo di conservazione del 21 novembre 2020 alle 6:00 su un file di lunghezza zero denominato `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write del file in sola lettura.

   In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

   ```
   chmod 444 document.txt
   ```

3. Utilizzare un comando o un programma adatto per modificare nuovamente l'attributo Read-write del file in Writable (scrivibile).

   > Questo passaggio non è considerato un rischio di conformità perché non sono presenti dati nel file.

In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` scrivibile:

```
chmod 777 document.txt
```

4. Utilizzare un comando o un programma adatto per iniziare a scrivere i dati nel file.

   In una shell UNIX, utilizzare il seguente comando per scrivere i dati `document.txt`:

```
echo test data >> document.txt
```

> Quando non è più necessario aggiungere dati al file, riportare i permessi del file in sola lettura.

Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili

A partire da ONTAP 9.3, è possibile utilizzare la funzione SnapLock *volume append mode* (VAM) per creare file .WORM appendibili per impostazione predefinita. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

Di cosa hai bisogno

- Il file .WORM appendibile deve risiedere su un volume SnapLock.
- Il volume SnapLock deve essere smontato e vuoto di copie Snapshot e file creati dall'utente.

A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte n×256KB+1 del file, il segmento precedente da 256 KB diventa protetto DA WORM.

Se si specifica un periodo di autocommit per il volume, i file .WORM che non vengono modificati per un periodo superiore al periodo di autocommit vengono impegnati in WORM.

> VAM non è supportato sui volumi del registro di controllo di SnapLock.

Fasi

1. Attiva VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Per un elenco completo delle opzioni, vedere la pagina man del comando.

   Il seguente comando attiva la funzione VAM sul volume `vol1` Di SVM`vs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. Utilizzare un comando o un programma adatto per creare file con permessi di scrittura.

   Per impostazione predefinita, i file sono associati A WORM.

Assegnare le copie Snapshot a WORM su una destinazione del vault

È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Tutte le attività di base di SnapLock vengono eseguite sulla destinazione del vault. Il volume di destinazione viene montato automaticamente in sola lettura, pertanto non è necessario assegnare esplicitamente le copie Snapshot a WORM; pertanto, la creazione di copie Snapshot pianificate sul volume di destinazione utilizzando i criteri SnapMirror non è supportata.

Prima di iniziare

- Il cluster di origine deve eseguire ONTAP 8.2.2 o versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- Il volume di origine non può essere un volume SnapLock.
- I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered.

  Per ulteriori informazioni, vedere "Peering dei cluster".

- Se la funzione di crescita automatica del volume è disattivata, lo spazio libero sul volume di destinazione deve essere superiore di almeno il cinque percento allo spazio utilizzato sul volume di origine.

A proposito di questa attività

Il volume di origine può utilizzare storage NetApp o non NetApp. Per lo storage non NetApp, è necessario utilizzare la virtualizzazione FlexArray.

> Non è possibile rinominare una copia Snapshot che è stata impegnata nello stato WORM.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.

> I LUN non sono supportati nei volumi SnapLock. Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

A partire da ONTAP 9.14.1, è possibile specificare i periodi di conservazione per etichette SnapMirror specifiche nella policy di SnapMirror della relazione di SnapMirror, in modo che le copie Snapshot replicate dall'origine al volume di destinazione vengano conservate per il periodo di conservazione specificato nella regola. Se non viene specificato alcun periodo di conservazione, viene utilizzato il periodo di conservazione predefinito del volume di destinazione.

A partire da ONTAP 9.13.1, è possibile ripristinare istantaneamente una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione del vault di SnapLock creando un FlexClone con l' `snaplock-type` Opzione impostata su "non snaplock" e specifica la copia Snapshot come "snapshot principale" quando si esegue l'operazione di creazione del clone del volume. Scopri di più "Creazione di un volume FlexClone con un tipo di SnapLock".

Per le configurazioni MetroCluster, è necessario conoscere quanto segue:

- È possibile creare una relazione SnapVault solo tra le SVM di origine della sincronizzazione, non tra una SVM di origine della sincronizzazione e una SVM di destinazione della sincronizzazione.
- È possibile creare una relazione SnapVault da un volume su una SVM di origine della sincronizzazione a una SVM di servizio dati.
- È possibile creare una relazione SnapVault da un volume su una SVM di servizio dati a un volume DP su una SVM di origine sincronizzazione.

L'illustrazione seguente mostra la procedura per l'inizializzazione di una relazione del vault di SnapLock:

Fasi

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, "Installare la licenza SnapLock", "Inizializzare l'orologio di conformità", E, se si utilizza una versione di ONTAP precedente alla 9.10.1, "Creazione di un aggregato SnapLock".
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo `DP` di dimensioni uguali o superiori a quelle del volume di origine:

   `volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-snaplock-type compliance|enterprise -type DP -size` *`size`*

   > A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock, Compliance o Enterprise, viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

   Il seguente comando crea un SnapLock da 2 GB `Compliance` volume denominato `dstvolB` poll `SVM2` sull'aggregato `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

4. Nel cluster di destinazione, impostare il periodo di conservazione predefinito, come descritto in Impostare il periodo di conservazione predefinito.

   > A un volume SnapLock che è una destinazione del vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo viene inizialmente impostato su un minimo di 0 anni per i volumi aziendali SnapLock e su un massimo di 30 anni per i volumi di conformità SnapLock. Ogni copia Snapshot di NetApp viene inizialmente impegnata con questo periodo di conservazione predefinito. Il periodo di conservazione può essere esteso in un secondo momento, se necessario. Per ulteriori informazioni, vedere Imposta la panoramica del tempo di conservazione.

5. Creare una nuova relazione di replica Tra l'origine non SnapLock e la nuova destinazione SnapLock creata

nel passaggio 3.

In questo esempio viene creata una nuova relazione di SnapMirror con il volume SnapLock di destinazione `dstvolB` utilizzando una policy di `XDPDefault` Per eseguire il vault delle copie Snapshot etichettate giornalmente e settimanalmente in base a una pianificazione oraria:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

> Creare un criterio di replica personalizzato oppure un programma personalizzato se le impostazioni predefinite disponibili non sono adatte.

6. Sulla SVM di destinazione, inizializzare la relazione SnapVault creata nella fase 5:

   `snapmirror initialize -destination-path` *`destination_path`*

   Il seguente comando inizializza la relazione tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`:

   ```
   cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

7. Una volta inizializzata la relazione e inattiva, utilizzare `snapshot show` Sulla destinazione per verificare il tempo di scadenza SnapLock applicato alle copie Snapshot replicate.

   Questo esempio elenca le copie Snapshot sul volume `dstvolB` Che hanno l'etichetta SnapMirror e la data di scadenza SnapLock:

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
   snapmirror-label, snaplock-expiry-time
   ```

Informazioni correlate

"Peering di cluster e SVM"

"Backup del volume con SnapVault"

Mirroring dei file WORM per il disaster recovery

È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi. Sia il volume di origine che il volume di destinazione devono essere configurati per SnapLock e entrambi i volumi devono avere la stessa modalità SnapLock, Compliance o Enterprise. Vengono replicate tutte le principali proprietà SnapLock del volume e dei file.

Prerequisiti

I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered. Per ulteriori informazioni, vedere "Peering di cluster e SVM".

A proposito di questa attività

- A partire da ONTAP 9.5, è possibile replicare i file WORM con la relazione SnapMirror di tipo XDP (Extended Data Protection) piuttosto che con la relazione di tipo DP (Data Protection). La modalità XDP è indipendente dalla versione di ONTAP ed è in grado di differenziare i file memorizzati nello stesso blocco, semplificando notevolmente la risincronizzazione dei volumi replicati in modalità Compliance. Per informazioni su come convertire una relazione di tipo DP esistente in una relazione di tipo XDP, vedere "Protezione dei dati".
- Un'operazione di risincronizzazione su una relazione SnapMirror di tipo DP non riesce per un volume in modalità di conformità se SnapLock determina che causerà una perdita di dati. Se un'operazione di risincronizzazione non riesce, è possibile utilizzare `volume clone create` per creare un clone del volume di destinazione. È quindi possibile risincronizzare il volume di origine con il clone.
- Una relazione SnapMirror di tipo XDP tra volumi compatibili con SnapLock supporta una risincronizzazione dopo un'interruzione anche se i dati sulla destinazione sono stati diversi dall'origine dopo l'interruzione.

  In una risincronizzazione, quando viene rilevata una divergenza di dati tra l'origine e la destinazione oltre lo snapshot comune, viene tagliata una nuova istantanea sulla destinazione per acquisire questa divergenza. Il nuovo snapshot e lo snapshot comune sono entrambi bloccati con un tempo di conservazione come segue:

  - Il tempo di scadenza del volume della destinazione
  - Se il tempo di scadenza del volume è passato o non è stato impostato, lo snapshot viene bloccato per un periodo di 30 giorni
  - Se la destinazione dispone di conservazione a fini giudiziari, il periodo di scadenza del volume effettivo viene mascherato e visualizzato come 'indefinito', tuttavia lo snapshot viene bloccato per la durata del periodo di scadenza del volume effettivo.

Se il volume di destinazione ha un periodo di scadenza successivo a quello di origine, il periodo di scadenza di destinazione viene mantenuto e non viene sovrascritto dal periodo di scadenza del volume di origine successivo alla risincronizzazione.

Se sulla destinazione sono presenti legal-stive che differiscono dall'origine, non è consentita una risincronizzazione. L'origine e la destinazione devono avere le stesse disposizioni legali o tutte le disposizioni legali sulla destinazione devono essere rilasciate prima di tentare una risincronizzazione.

Una copia Snapshot bloccata sul volume di destinazione creato per acquisire i dati divergenti può essere copiata nell'origine utilizzando la CLI eseguendo `snapmirror update -s snapshot` comando. Una volta copiata, l'istantanea continuerà a essere bloccata anche all'origine.

- Le relazioni di protezione dei dati SVM non sono supportate.
- Le relazioni di protezione dei dati di condivisione del carico non sono supportate.

La seguente illustrazione mostra la procedura per inizializzare una relazione SnapMirror:

System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione di sistema per impostare la replica di SnapMirror dei file WORM.

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Fare clic su **Mostra/Nascondi** e selezionare **tipo SnapLock** per visualizzare la colonna nella finestra **volumi**.
3. Individuare un volume SnapLock.
4. Fare clic su ⋮ E selezionare **Protect**.
5. Scegliere il cluster di destinazione e la VM di storage di destinazione.
6. Fare clic su **altre opzioni**.
7. Selezionare **Mostra policy legacy** e selezionare **DPDefault (legacy)**.
8. Nella sezione **Destination Configuration details** (Dettagli configurazione destinazione), selezionare **Override transfer schedule** (Ignora pianificazione trasferimento) e selezionare **Hourly** (orario).
9. Fare clic su **Save** (Salva).
10. A sinistra del nome del volume di origine, fare clic sulla freccia per espandere i dettagli del volume, quindi a destra della pagina, esaminare i dettagli della protezione di SnapMirror remoto.
11. Sul cluster remoto, accedere a **Relazioni di protezione**.
12. Individuare la relazione e fare clic sul nome del volume di destinazione per visualizzare i dettagli della relazione.
13. Verificare che il tipo SnapLock del volume di destinazione e altre informazioni SnapLock siano disponibili.

CLI

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, "Installare la licenza SnapLock", "Inizializzare l'orologio di conformità", E, se si utilizza una versione di ONTAP precedente alla 9.10.1, "Creazione di un aggregato SnapLock".
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo `DP` di dimensioni uguali o superiori al volume di origine:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock (Compliance o Enterprise) viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

   Il seguente comando crea un SnapLock da 2 GB `Compliance` volume denominato `dstvolB` poll `SVM2` sull'aggregato `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sulla SVM di destinazione, creare un criterio SnapMirror:

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*

   Il seguente comando crea il criterio a livello di SVM `SVM1-mirror`:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. Sulla SVM di destinazione, creare una pianificazione SnapMirror:

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*

   Il comando seguente crea una pianificazione SnapMirror denominata `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. Sulla SVM di destinazione, creare una relazione SnapMirror:

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

   Il comando seguente crea una relazione SnapMirror tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`e assegna il criterio `SVM1-mirror` e il calendario `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   Il tipo di XDP è disponibile in ONTAP 9.5 e versioni successive. È necessario utilizzare il tipo di DP in ONTAP 9.4 e versioni precedenti.

7. Sulla SVM di destinazione, inizializzare la relazione SnapMirror:

   snapmirror initialize -destination-path *destination_path*

   Il processo di inizializzazione esegue un *trasferimento baseline* al volume di destinazione. SnapMirror crea una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. Inoltre, trasferisce al volume di destinazione tutte le altre copie Snapshot presenti nel volume di origine.

Il seguente comando inizializza la relazione tra il volume di origine `srcvolA` acceso `SVM1` e il volume di destinazione `dstvolB` acceso `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Informazioni correlate

"Peering di cluster e SVM"

"Preparazione al disaster recovery dei volumi"

"Protezione dei dati"

Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali

A partire da ONTAP 9.3, puoi conservare i file WORM in modalità di conformità per tutta la durata di un contenzioso utilizzando la funzione *conservazione legale*.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.

  "Creare un account amministratore di SnapLock"

- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

A proposito di questa attività

Un file in stato di conservazione legale si comporta come un file WORM con un periodo di conservazione indefinito. È responsabilità dell'utente specificare quando scade il periodo di conservazione legale.

Il numero di file che è possibile inserire in un blocco legale dipende dallo spazio disponibile sul volume.

Fasi

1. Avvio di un blocco legale:

   `snaplock legal-hold begin -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   Il seguente comando avvia un blocco legale per tutti i file in `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Fine di un periodo di conservazione legale:

   `snaplock legal-hold end -litigation-name` *`litigation_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   Il seguente comando termina un blocco legale per tutti i file in `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Panoramica sull'eliminazione dei file WORM

È possibile eliminare i file WORM in modalità Enterprise durante il periodo di conservazione utilizzando la funzione di eliminazione con privilegi. Prima di poter utilizzare questa funzione, è necessario creare un account amministratore di SnapLock e, utilizzando l'account, attivare la funzione.

Creare un account amministratore di SnapLock

Per eseguire un'eliminazione con privilegi, è necessario disporre dei privilegi di amministratore di SnapLock. Questi privilegi sono definiti nel ruolo vsadmin-snaplock. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un account amministratore SVM con il ruolo di amministratore di SnapLock.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

Fasi

1. Creare un account amministratore SVM con il ruolo di amministratore di SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   Il seguente comando attiva l'account amministratore SVM `SnapLockAdmin` con il predefinito `vsadmin-snaplock` ruolo di accesso `SVM1` utilizzo di una password:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

Attivare la funzione di eliminazione con privilegi

È necessario attivare esplicitamente la funzionalità di eliminazione con privilegi sul volume Enterprise che contiene i file WORM che si desidera eliminare.

A proposito di questa attività

Il valore di `-privileged-delete` l'opzione determina se l'eliminazione con privilegi è attivata. I valori possibili sono `enabled`, `disabled`, e. `permanently-disabled`.

> `permanently-disabled` è lo stato del terminale. Non è possibile attivare l'eliminazione con privilegi sul volume dopo aver impostato lo stato su `permanently-disabled`.

Fasi

1. Abilitare l'eliminazione con privilegi per un volume aziendale SnapLock:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-privileged -delete disabled|enabled|permanently-disabled`

   Il comando seguente attiva la funzione di eliminazione con privilegi per il volume Enterprise `dataVol` acceso `SVM1`:

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Eliminare i file WORM in modalità Enterprise

È possibile utilizzare la funzione di eliminazione con privilegi per eliminare i file WORM in modalità Enterprise durante il periodo di conservazione.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.
- È necessario aver creato un registro di controllo di SnapLock e attivato la funzione di eliminazione con privilegi sul volume aziendale.

A proposito di questa attività

Non è possibile utilizzare un'operazione di eliminazione con privilegi per eliminare un file WORM scaduto. È possibile utilizzare `volume file retention show` Per visualizzare il tempo di conservazione del file WORM che si desidera eliminare. Per ulteriori informazioni, vedere la pagina man del comando.

Fase

1. Eliminare un file WORM su un volume Enterprise:

   `volume file privileged-delete -vserver` *`SVM_name`* `-file` *`file_path`*

   Il seguente comando elimina il file `/vol/dataVol/f1` Su SVM`SVM1`:

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

Spostare un volume SnapLock

A partire da ONTAP 9.8, è possibile spostare un volume SnapLock in un aggregato di destinazione dello stesso tipo, da Enterprise a Enterprise o Compliance a Compliance.

Per spostare un volume SnapLock, è necessario assegnare il ruolo di protezione SnapLock.

Creare un account amministratore di sicurezza SnapLock

Per eseguire lo spostamento di un volume SnapLock, è necessario disporre dei privilegi di amministratore della sicurezza di SnapLock. Questo privilegio viene concesso con il ruolo *SnapLock*, introdotto in ONTAP 9.8. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un utente di protezione SnapLock con questo ruolo di protezione SnapLock.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

A proposito di questa attività

Il ruolo SnapLock è associato alla SVM amministrativa, a differenza del ruolo vsadmin-snaplock, associato alla SVM dei dati.

Fase

1. Creare un account amministratore SVM con il ruolo di amministratore di SnapLock:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   Il seguente comando attiva l'account amministratore SVM `SnapLockAdmin` con il predefinito `snaplock` Ruolo per accedere a SVM di amministrazione `cluster1` utilizzo di una password:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

Spostare un volume SnapLock

È possibile utilizzare `volume move` Comando per spostare un volume SnapLock in un aggregato di destinazione.

Di cosa hai bisogno

- È necessario aver creato un registro di controllo protetto da SnapLock prima di eseguire lo spostamento del volume SnapLock.

  "Creare un registro di controllo".

- Se si utilizza una versione di ONTAP precedente a ONTAP 9.10.1, l'aggregato di destinazione deve essere dello stesso tipo di SnapLock del volume SnapLock che si desidera spostare, ovvero Compliance to Compliance o Enterprise to Enterprise. A partire da ONTAP 9.10.1, questa restrizione viene rimossa e un aggregato può includere volumi Compliance e Enterprise SnapLock, oltre a volumi non SnapLock.
- Devi essere un utente con il ruolo di sicurezza SnapLock.

Fasi

1. Utilizzando una connessione sicura, accedere alla LIF di gestione del cluster di ONTAP:

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. Spostamento di un volume SnapLock:

   ```
   volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
   -aggregate destination_aggregate_name
   ```

3. Controllare lo stato dell'operazione di spostamento del volume:

   ```
   volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
   volume,phase,vserver
   ```

Bloccare una copia Snapshot per la protezione dagli attacchi ransomware

A partire da ONTAP 9.12.1, è possibile bloccare una copia Snapshot su un volume non SnapLock per fornire protezione dagli attacchi ransomware. Il blocco delle copie Snapshot garantisce che non possano essere eliminate accidentalmente o in modo illecito.

La funzione clock di conformità SnapLock consente di bloccare le copie Snapshot per un periodo specificato in modo che non possano essere eliminate fino al raggiungimento dell'ora di scadenza. Il blocco delle copie Snapshot le rende a prova di manomissione, proteggendole dalle minacce ransomware. È possibile utilizzare le copie Snapshot bloccate per ripristinare i dati se un volume viene compromesso da un attacco ransomware.

A partire da ONTAP 9.14.1, il blocco delle copie Snapshot supporta la conservazione a lungo termine delle copie Snapshot sulle destinazioni del vault SnapLock e su volumi di destinazione SnapMirror non SnapLock. Il blocco della copia Snapshot viene attivato impostando il periodo di conservazione utilizzando le regole dei criteri di SnapMirror associate a un etichetta criterio esistente. La regola ha la priorità sul periodo di conservazione predefinito impostato sul volume. Se non esiste un periodo di conservazione associato all'etichetta SnapMirror, viene utilizzato il periodo di conservazione predefinito del volume.

Requisiti e considerazioni sulle copie Snapshot a prova di manomissione

- Se si utilizza l'interfaccia utente di ONTAP, tutti i nodi del cluster devono eseguire ONTAP 9.12.1 o versione successiva. Se si utilizza Gestore di sistema, tutti i nodi devono eseguire ONTAP 9.13.1 o versione successiva.
- "La licenza SnapLock deve essere installata sul cluster". Questa licenza è inclusa in "ONTAP uno".
- "È necessario inizializzare il clock di conformità sul cluster".
- Quando il blocco Snapshot è attivato su un volume, è possibile aggiornare i cluster a una versione di ONTAP successiva a ONTAP 9.12.1; Tuttavia, non è possibile ripristinare una versione precedente di ONTAP fino a quando tutte le copie Snapshot bloccate non hanno raggiunto la data di scadenza e non vengono eliminate e il blocco delle copie Snapshot non viene disattivato.
- Quando un'istantanea è bloccata, il tempo di scadenza del volume viene impostato sul tempo di scadenza della copia Snapshot. Se più di una copia Snapshot è bloccata, il tempo di scadenza del volume riflette il tempo di scadenza maggiore tra tutte le copie Snapshot.
- Il periodo di conservazione per le copie Snapshot bloccate ha la precedenza sul conteggio copie Snapshot, il che significa che il limite di conservazione non viene rispettato se il periodo di conservazione delle copie Snapshot bloccate non è scaduto.

- In una relazione SnapMirror, è possibile impostare un periodo di conservazione su una regola dei criteri del vault mirror e il periodo di conservazione viene applicato alle copie Snapshot replicate sulla destinazione se il volume di destinazione ha attivato il blocco delle copie Snapshot. Il periodo di conservazione ha la precedenza sul numero di conservazione; ad esempio, le copie Snapshot che non hanno superato la scadenza verranno conservate anche se il numero di conservazione viene superato.
- È possibile rinominare una copia Snapshot su un volume non SnapLock. Le operazioni di ridenominazione di Snapshot sul volume primario di una relazione SnapMirror si riflettono sul volume secondario solo se il criterio è MirrorAllSnapshots. Per gli altri tipi di policy, la copia Snapshot rinominata non viene propagata durante gli aggiornamenti.
- Se si utilizza l'interfaccia utente di ONTAP, è possibile ripristinare una copia Snapshot bloccata con `volume snapshot restore` Solo se la copia Snapshot bloccata è la più recente. Se sono presenti copie Snapshot non scadute dopo quella da ripristinare, l'operazione di ripristino della copia Snapshot non riesce.

Funzionalità supportate con copie Snapshot antimanomissione

- Volumi FlexGroup

  Il blocco delle copie Snapshot è supportato sui volumi FlexGroup. Il blocco di Snapshot si verifica solo sulla copia Snapshot del componente principale. L'eliminazione del volume FlexGroup è consentita solo se è trascorso il tempo di scadenza del costituente root.

- Conversione da FlexVol a FlexGroup

  È possibile convertire un volume FlexVol con copie Snapshot bloccate in un volume FlexGroup. Le copie Snapshot rimangono bloccate dopo la conversione.

- Clone del volume e clone del file

  È possibile creare cloni di volume e file da una copia Snapshot bloccata.

Funzionalità non supportate

Le seguenti funzioni attualmente non sono supportate con le copie Snapshot antimanomissione:

- Cloud Volumes ONTAP
- Gruppi di coerenza
- FabricPool
- Volumi FlexCache
- SMtape
- Continuità aziendale SnapMirror (SM-BC)
- Regole di policy di SnapMirror che utilizzano `-schedule` parametro
- SnapMirror sincrono
- Mobilità dei dati delle SVM (utilizzata per la migrazione o il trasferimento di una SVM da un cluster di origine a un cluster di destinazione)

Attiva il blocco delle copie Snapshot durante la creazione di un volume

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot quando si crea un nuovo volume o quando si modifica un volume esistente utilizzando `-snapshot-locking-enabled` con `volume create` e. `volume modify` Comandi nella CLI. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per

attivare il blocco delle copie Snapshot.

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), selezionare **More Options** (altre opzioni).
3. Immettere il nome del volume, le dimensioni, la policy di esportazione e il nome della condivisione.
4. Selezionare **Enable Snapshot Locking** (attiva blocco snapshot). Questa selezione non viene visualizzata se la licenza SnapLock non è installata.
5. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
6. Salvare le modifiche.
7. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
8. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

CLI

1. Per creare un nuovo volume e attivare il blocco delle copie Snapshot, immettere il seguente comando:

   `volume create -vserver vserver_name -volume volume_name -snapshot-locking -enabled true`

   Il comando seguente attiva il blocco delle copie Snapshot su un nuovo volume denominato vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Attiva il blocco delle copie Snapshot su un volume esistente

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot su un volume esistente utilizzando l’interfaccia utente di ONTAP. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare il blocco delle copie Snapshot su un volume esistente.

System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare ⋮ E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), individuare la sezione Snapshot Copies (Local) Settings (Impostazioni snapshot Copies (locali)) e selezionare **Enable Snapshot Locking** (attiva blocco snapshot).

   Questa selezione non viene visualizzata se la licenza SnapLock non è installata.

4. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
5. Salvare le modifiche.
6. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
7. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

CLI

1. Per modificare un volume esistente per attivare il blocco delle copie Snapshot, immettere il seguente comando:

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Creare una policy di copia Snapshot bloccata e applicare la conservazione

A partire da ONTAP 9.12.1, è possibile creare criteri di copia Snapshot per applicare un periodo di conservazione delle copie Snapshot e applicare il criterio a un volume per bloccare le copie Snapshot per il periodo specificato. È inoltre possibile bloccare una copia Snapshot impostando manualmente un periodo di conservazione. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per creare policy di blocco delle copie Snapshot e applicarle a un volume.

Creare un criterio di blocco delle copie Snapshot

System Manager

1. Accedere a **Storage > Storage VM** e selezionare una storage VM.
2. Selezionare **Impostazioni**.
3. Individuare **Snapshot Policies** e selezionare →.
4. Nella finestra **Add Snapshot Policy**, inserire il nome del criterio.
5. Selezionare + Add .
6. Fornire i dettagli della pianificazione della copia Snapshot, inclusi il nome della pianificazione, il numero massimo di copie Snapshot da conservare e il periodo di conservazione SnapLock.
7. Nella colonna **SnapLock Retention Period**, immettere il numero di ore, giorni, mesi o anni per conservare le copie Snapshot. Ad esempio, un criterio di copia Snapshot con un periodo di conservazione di 5 giorni blocca una copia Snapshot per 5 giorni dal momento della creazione e non può essere eliminata durante tale periodo. Sono supportati i seguenti intervalli di periodi di conservazione:
   - Anni: 0 - 100
   - Mesi: 0 - 1200
   - Giorni: 0 - 36500
   - Orario: 0 - 24
8. Salvare le modifiche.

CLI

1. Per creare un criterio di copia Snapshot, immettere il seguente comando:

   `volume snapshot policy create -policy policy_name -enabled true -schedule1` *`schedule1_name`* `-count1` *`maximum_Snapshot_copies -retention-period1 _retention_period`*

   Il seguente comando crea un criterio di blocco delle copie Snapshot:

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Una copia Snapshot non viene sostituita se è in stato di conservazione attivo; in altri termini, il conteggio delle trattenute non viene rispettato se sono presenti copie Snapshot bloccate che non sono ancora scadute.

Applicare un criterio di blocco a un volume

System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare ⋮ E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), selezionare **Schedule Snapshot Copies** (Pianifica copie Snapshot).
4. Selezionare il criterio di copia Snapshot di blocco dall'elenco.
5. Se il blocco della copia Snapshot non è già attivato, selezionare **Enable Snapshot Locking** (attiva blocco Snapshot).
6. Salvare le modifiche.

CLI

1. Per applicare un criterio di blocco delle copie Snapshot a un volume esistente, immettere il seguente comando:

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Applica il periodo di conservazione durante la creazione manuale della copia Snapshot

È possibile applicare un periodo di conservazione delle copie Snapshot quando si crea manualmente una copia Snapshot. Il blocco della copia Snapshot deve essere attivato sul volume, altrimenti l'impostazione del periodo di conservazione viene ignorata.

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare + Add .
4. Inserire il nome della copia Snapshot e la data di scadenza del SnapLock. È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
5. Salvare le modifiche.
6. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

CLI

1. Per creare manualmente una copia Snapshot e applicare un periodo di conservazione a blocchi, immettere il seguente comando:

   `volume snapshot create -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-snaplock-expiry-time` *`expiration_date_time`*

   Il seguente comando crea una nuova copia Snapshot e imposta il periodo di conservazione:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Applicare il periodo di conservazione a una copia Snapshot esistente

System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare la copia Snapshot, quindi ⋮ E scegliere **Modify SnapLock Expiration Time** (Modifica ora di scadenza protocollo). È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
4. Salvare le modifiche.
5. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

CLI

1. Per applicare manualmente un periodo di conservazione a una copia Snapshot esistente, immettere il seguente comando:

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   Nell'esempio seguente viene applicato un periodo di conservazione a una copia Snapshot esistente:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Modifica di un criterio esistente per applicare la conservazione a lungo termine

A partire da ONTAP 9.14.1, è possibile modificare una policy SnapMirror esistente aggiungendo una regola per impostare la conservazione a lungo termine delle copie Snapshot. La regola viene utilizzata per ignorare il periodo di conservazione dei volumi predefinito sulle destinazioni del vault SnapLock e sui volumi di destinazione non SnapLock SnapMirror.

1. Aggiunta di una regola a una policy SnapMirror esistente:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of Snapshot copies> -retention
   -period [<integer> days|months|years]
   ```

   Nell'esempio seguente viene creata una regola che applica un periodo di conservazione di 6 mesi al criterio esistente denominato "lockvault":

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

API SnapLock

È possibile utilizzare le API Zephyr per l'integrazione con la funzionalità SnapLock negli

script o nell'automazione del workflow. Le API utilizzano la messaggistica XML su HTTP, HTTPS e Windows DCE/RPC. Per ulteriori informazioni, vedere "Documentazione sull'automazione ONTAP".

file-fingerprint-abortire

Interrompere un'operazione di impronta digitale del file.

file-fingerprint-dump

Visualizzare le informazioni sull'impronta digitale del file.

file-fingerprint-get-iter

Visualizza lo stato delle operazioni di impronte digitali del file.

file-fingerprint-start

Generare un'impronta digitale del file.

snaplock-archive-vserver-log

Archiviare il file di log di audit attivo.

snaplock-create-vserver-log

Creare una configurazione del registro di controllo per una SVM.

snaplock-delete-vserver-log

Eliminare una configurazione del registro di controllo per una SVM.

snaplock-file-privileged-delete

Eseguire un'operazione di eliminazione con privilegi.

snaplock-get-file-retention

Ottenere il periodo di conservazione di un file.

snaplock-get-node-compliance-clock

Ottenere la data e l'ora del nodo ComplianceClock.

snaplock-get-vserver-active-log-files-iter

Visualizza lo stato dei file di log attivi.

snaplock-get-vserver-log-iter

Visualizzare la configurazione del registro di controllo.

snaplock-modify-vserver-log

Modificare la configurazione del registro di controllo per una SVM.

snaplock-set-file-retention

Impostare il tempo di conservazione di un file.

snaplock-set-node-compliance-clock

Impostare la data e l'ora del nodo ComplianceClock.

snaplock-volume-set-privilegiate-delete

Impostare l'opzione Privileged-delete su un volume aziendale SnapLock.

volume-get-snaplock-attrs

Ottenere gli attributi di un volume SnapLock.

volume-set-snaplock-attrs

Impostare gli attributi di un volume SnapLock.

Gruppi di coerenza

Panoramica dei gruppi di coerenza

Un gruppo di coerenza è un insieme di volumi gestiti come singola unità. In ONTAP, i gruppi di coerenza offrono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che copre più volumi.

È possibile utilizzare gruppi di coerenza per semplificare la gestione dello storage. Immaginate di disporre di un database importante che comprende venti LUN. È possibile gestire le LUN su base individuale o trattare le LUN come un dataset solitario, organizzandole in un singolo gruppo di coerenza.

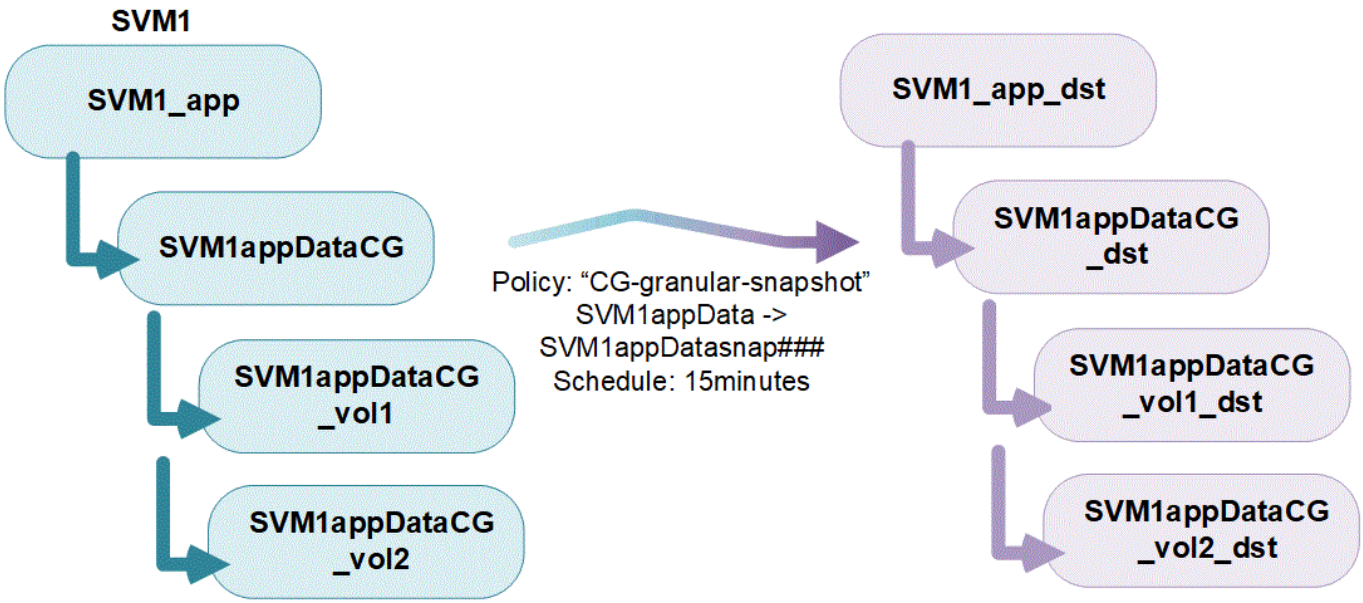
I gruppi di coerenza facilitano la gestione del carico di lavoro dell'applicazione, fornendo policy di protezione locali e remote facilmente configurabili e copie Snapshot simultanee coerenti con il crash o coerenti con l'applicazione di una raccolta di volumi in un momento specifico. Le copie Snapshot di un gruppo di coerenza permettono il ripristino di un intero workload dell'applicazione.

Informazioni sui gruppi di coerenza

I gruppi di coerenza supportano qualsiasi volume FlexVol indipendentemente dal protocollo (NAS, SAN o NVMe) e possono essere gestiti tramite l'API REST di ONTAP o in Gestione sistema nella voce di menu **Storage > Consistency Groups**. A partire da ONTAP 9.14.1, è possibile gestire i gruppi di coerenza con l'interfaccia a riga di comando di ONTAP.

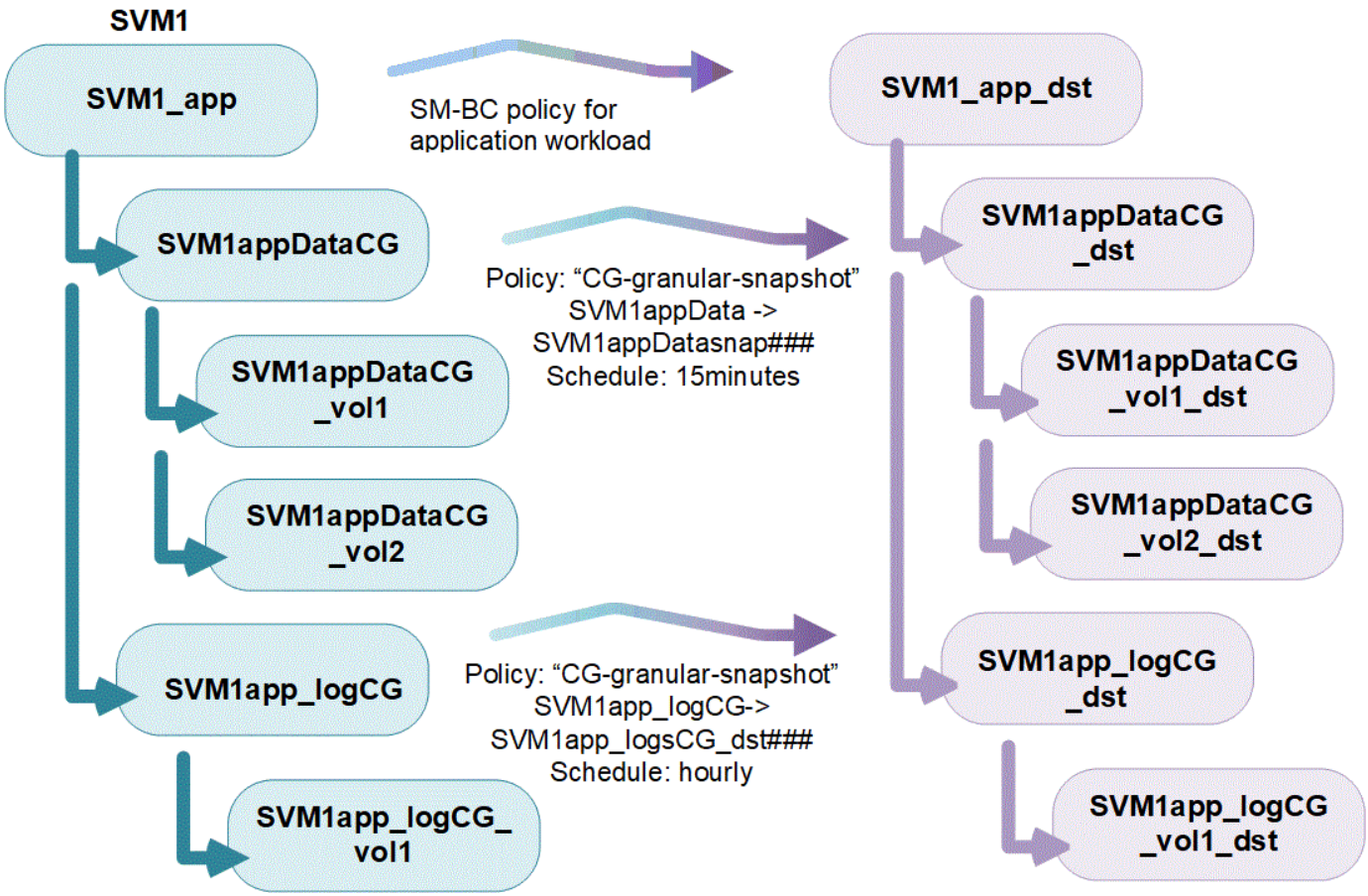
I gruppi di coerenza possono esistere come singole entità, come un insieme di volumi, o in una relazione gerarchica, che consiste di altri gruppi di coerenza. I singoli volumi possono avere una propria policy Snapshot granulare a livello di volume. Inoltre, è possibile utilizzare una policy di Snapshot a livello di gruppo di coerenza. Il gruppo di coerenza può avere solo una relazione di continuità aziendale SnapMirror (SM-BC) e una policy condivisa SM-BC, che possono essere utilizzate per ripristinare l'intero gruppo di coerenza.

Il seguente diagramma illustra come utilizzare un singolo gruppo di coerenza. I dati di un'applicazione ospitata su `SVM1` si estende su due volumi: `vol1` e. `vol2`. Una policy Snapshot nel gruppo di coerenza acquisisce le copie Snapshot dei dati ogni 15 minuti.



I carichi di lavoro delle applicazioni più grandi potrebbero richiedere più gruppi di coerenza. In queste situazioni, è possibile creare gruppi di coerenza gerarchici, in cui un singolo gruppo di coerenza diventa i componenti secondari di un gruppo di coerenza padre. Il gruppo di coerenza padre può includere fino a cinque gruppi di coerenza figlio. Come nei singoli gruppi di coerenza, è possibile applicare una policy di protezione remota SM-BC all'intera configurazione dei gruppi di coerenza (padre e figlio) per ripristinare il carico di lavoro dell'applicazione.

Nell'esempio seguente, un'applicazione è ospitata su `SVM1`. L'amministratore ha creato un gruppo di coerenza principale, `SVM1_app`, che include due gruppi di coerenza figlio: `SVM1appDataCG` per i dati e. `SVM1app_logCG` per i log. Ogni gruppo di coerenza figlio dispone della propria policy Snapshot. Copie Snapshot dei volumi in `SVM1appDataCG` ogni 15 minuti. Snapshot di `SVM1app_logCG` vengono presi ogni ora. Il gruppo di coerenza padre `SVM1_app` Dispone di una policy SM-BC che replica i dati per garantire un servizio continuo in caso di disastro.



A partire da ONTAP 9.12.1, il supporto dei gruppi di coerenza cloning e modificando i membri della coerenza con aggiunta o rimozione di volumi In Gestione di sistema e nell’API REST di ONTAP. A partire da ONTAP 9.12.1, l’API REST ONTAP supporta anche:

- Creazione di gruppi di coerenza con nuovi volumi NFS o SMB o spazi dei nomi NVMe.
- Aggiunta di volumi NFS o SMB nuovi o esistenti o spazi dei nomi NVMe a gruppi di coerenza esistenti.

Per ulteriori informazioni sull’API REST di ONTAP, fare riferimento a. "Documentazione di riferimento API REST di ONTAP".

Monitorare i gruppi di coerenza

A partire da ONTAP 9.13.1, i gruppi di coerenza offrono il monitoraggio della capacità e delle prestazioni in tempo reale e cronologico, offrendo informazioni dettagliate sulle prestazioni delle applicazioni e dei singoli gruppi di coerenza.

I dati di monitoring vengono aggiornati ogni cinque minuti e vengono conservati per un massimo di un anno. Puoi tenere traccia delle metriche per:

- Performance: IOPS, latenza e throughput
- Capacità: Dimensioni, logica utilizzata, disponibile

È possibile visualizzare i dati di monitoraggio nella scheda **Panoramica** del menu del gruppo di coerenza in System Manager o richiederli nell’API REST. A partire da ONTAP 9.14.1, è possibile visualizzare le metriche del gruppo di coerenza con l’interfaccia CLI utilizzando l' `consistency-group metrics show` comando.

In ONTAP 9.13.1, è possibile recuperare solo le metriche storiche utilizzando l'API REST. A partire da ONTAP 9.14.1, sono disponibili anche le metriche cronologiche in System Manager.

Proteggere i gruppi di coerenza

I gruppi di coerenza offrono protezione attraverso:

- Policy di Snapshot
- Continuità aziendale SnapMirror (SM-BC)
- [mcc] (A partire da ONTAP 9.11.1)
- SnapMirror asincrono (A partire da ONTAP 9.13.1)
- "Disaster recovery SVM" (A partire da ONTAP 9.14.1)

La creazione di un gruppo di coerenza non attiva automaticamente la protezione. È possibile impostare policy di protezione locali e remote durante la creazione o dopo la creazione di un gruppo di coerenza.

Per configurare la protezione su un gruppo di coerenza, vedere "Proteggere un gruppo di coerenza".

Per utilizzare la protezione remota, è necessario soddisfare i requisiti di Implementazioni di Business Continuity SnapMirror.

Non è possibile stabilire relazioni SM-BC sui volumi montati per l'accesso NAS.

Gruppi di coerenza nelle configurazioni MetroCluster

A partire da ONTAP 9.11.1, è possibile eseguire il provisioning di gruppi di coerenza con nuovi volumi in un cluster all'interno di una configurazione MetroCluster. Il provisioning di questi volumi viene eseguito su aggregati mirrorati.

Una volta eseguito il provisioning, è possibile spostare i volumi associati ai gruppi di coerenza tra aggregati mirrorati e senza mirror. Pertanto, i volumi associati ai gruppi di coerenza possono essere posizionati su aggregati mirrorati, aggregati senza mirror o entrambi. È possibile modificare gli aggregati mirrorati contenenti volumi associati ai gruppi di coerenza in modo che diventino senza mirror. Allo stesso modo, è possibile modificare aggregati senza mirror contenenti volumi associati a gruppi di coerenza per abilitare il mirroring.

I volumi e le copie Snapshot associati ai gruppi di coerenza posizionati sugli aggregati con mirroring vengono replicati nel sito remoto (sito B). Il contenuto dei volumi sul sito B fornisce una garanzia di ordine di scrittura per il gruppo di coerenza, consentendo il ripristino dal sito B in caso di disastro. Puoi accedere alle copie Snapshot del gruppo di coerenza utilizzando il gruppo di coerenza con l'API REST e System Manager sui cluster che eseguono ONTAP 9.11.1 o versioni successive. A partire da ONTAP 9.14.1, è possibile accedere anche alle copie Snapshot con l'interfaccia a riga di comando di ONTAP.

Se alcuni o tutti i volumi associati a un gruppo di coerenza si trovano su aggregati senza mirror che non sono attualmente accessibili, LE operazioni GET o DELETE sul gruppo di coerenza si comportano come se i volumi locali o gli aggregati di hosting non fossero in linea.

Configurazioni di gruppi di coerenza per la replica

Se il sito B esegue ONTAP 9.10.1 o versioni precedenti, solo i volumi associati ai gruppi di coerenza situati negli aggregati mirrorati vengono replicati nel sito B. Le configurazioni dei gruppi di coerenza vengono replicate solo nel sito B, se entrambi i siti eseguono ONTAP 9.11.1 o versione successiva. Dopo l'aggiornamento del sito B a ONTAP 9.11.1, i dati per i gruppi di coerenza sul sito A che hanno tutti i volumi

associati posizionati su aggregati mirrorati vengono replicati nel sito B.

> Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

Considerazioni sull'upgrade

I gruppi di coerenza creati con SM-BC in ONTAP 9.8 e 9.9.1 verranno automaticamente aggiornati e gestiti in **Storage > Consistency Groups** in System Manager o nell'API REST di ONTAP quando si esegue l'aggiornamento a ONTAP 9.10.1 o versioni successive. Per ulteriori informazioni sull'aggiornamento da ONTAP 9.8 o 9.9.1, vedere "Considerazioni sull'upgrade e il revert di SM-BC".

Le copie Snapshot del gruppo di coerenza create nell'API REST possono essere gestite tramite l'interfaccia del Gruppo di coerenza di System Manager e tramite gli endpoint delle API REST del gruppo di coerenza. A partire da ONTAP 9.14.1, è possibile gestire anche gli Snapshot del gruppo di coerenza con l'interfaccia a riga di comando di ONTAP.

> Copie Snapshot create con i comandi ONTAPI `cg-start` e. `cg-commit` Sono riconosciuti come Snapshot del gruppo di coerenza e pertanto non possono essere gestiti tramite l'interfaccia del gruppo di coerenza di System Manager o gli endpoint del gruppo di coerenza nell'API REST di ONTAP. A partire da ONTAP 9.14.1, queste copie Snapshot possono essere mirrorati sul volume di destinazione, se si sta utilizzando una policy SnapMirror asincrona. Per ulteriori informazioni, vedere Configurare la protezione asincrona di SnapMirror.

Funzionalità supportate dalla release

	ONTAP 9.14.1	**ONTAP 9.13.1**	**ONTAP 9.12.1**	**ONTAP 9.11.1**	**ONTAP 9.10.1**
Gruppi di coerenza gerarchica	✓	✓	✓	✓	✓
Protezione locale con copie Snapshot	✓	✓	✓	✓	✓
Continuità aziendale di SnapMirror	✓	✓	✓	✓	✓
Supporto MetroCluster	✓	✓	✓	✓	
Commit bifase (solo API REST)	✓	✓	✓	✓	
Tag di applicazioni e componenti	✓	✓	✓		
Clonare i gruppi di coerenza	✓	✓	✓		
Aggiungere e rimuovere volumi	✓	✓	✓		
Crea CGS con nuovi volumi NAS	✓	✓	Solo API REST		
Crea CGS con i nuovi NVMe Namespace	✓	✓	Solo API REST		

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Spostare i volumi tra i gruppi di coerenza figlio	✓	✓			
Modificare la geometria del gruppo di coerenza	✓	✓			
Monitoraggio	✓	✓			
SnapMirror asincrono (solo singoli gruppi di coerenza)	✓	✓			
Disaster recovery SVM (solo gruppi di coerenza singoli)	✓				
Supporto CLI	✓				

Scopri di più sui gruppi di coerenza

Ulteriori informazioni

- "Documentazione sull'automazione ONTAP"
- Continuità aziendale di SnapMirror
- Nozioni di base sul disaster recovery asincrono di SnapMirror
- "Documentazione MetroCluster"

Limiti del gruppo di coerenza

Durante la pianificazione e la gestione dei gruppi di coerenza, tenere conto dei limiti degli oggetti nell'ambito del cluster e del gruppo di coerenza padre o figlio.

Limiti imposti

Nella tabella seguente vengono acquisiti i limiti per i gruppi di coerenza. Sono previsti limiti separati per i gruppi di coerenza che utilizzano SnapMirror Business Continuity (SM-BC). Per ulteriori informazioni, vedere "SM-BC restrizioni e limitazioni per i limiti".

Limite	Scopo	Minimo	Massimo
Numero di gruppi di coerenza	Cluster	0	Uguale al numero massimo di volumi nel cluster
Numero di gruppi di coerenza padre	Cluster	0	Uguale al numero massimo di volumi nel cluster
Numero di gruppi di coerenza individuali e principali	Cluster	0	Uguale al numero massimo di volumi nel cluster
Numero di volumi in un gruppo di coerenza	Singolo gruppo di coerenza	1 volume	80 volumi
Numero di volumi nel figlio di un gruppo di coerenza padre	Gruppo di coerenza padre	1 volume	80 volumi
Numero di volumi in un gruppo di coerenza figlio	Gruppo di coerenza figlio	1 volume	80 volumi
Numero di gruppi di coerenza figlio in un gruppo di coerenza padre	Gruppo di coerenza padre	1 gruppo di coerenza	5 gruppi di coerenza
Numero di relazioni di disaster recovery delle SVM in cui è presente un gruppo di coerenza (disponibile a partire dal ONTAP 9.14.1)	Cluster	0	32

Limiti non applicati

La pianificazione minima supportata delle copie Snapshot per i gruppi di coerenza è di 30 minuti. Basata su "Test per i gruppi flessibili", Che condividono la stessa infrastruttura Snapshot dei gruppi di coerenza.

Configurare un singolo gruppo di coerenza

È possibile creare gruppi di coerenza con volumi esistenti o nuove LUN o volumi (a seconda della versione di ONTAP). È possibile associare un volume o un LUN a un solo gruppo di coerenza alla volta.

A proposito di questa attività

- In ONTAP dalla versione 9.10.1 alla 9.11.1, la modifica dei volumi membro di un gruppo di coerenza dopo la sua creazione non è supportata.

A partire da ONTAP 9.12.1, è possibile modificare i volumi membri di un gruppo di coerenza. Per ulteriori informazioni su questo processo, fare riferimento a. Modificare un gruppo di coerenza.

Creare un gruppo di coerenza con nuove LUN o volumi

In ONTAP dalla versione 9.10.1 alla versione 9.12.1, è possibile creare un gruppo di coerenza utilizzando nuove LUN. A partire da ONTAP 9.13.1, System Manager supporta anche la creazione di un gruppo di coerenza con nuovi namespace NVMe o nuovi volumi NAS. (Questo è supportato anche nell'API REST di ONTAP a partire da ONTAP 9.12.1).

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi selezionare il protocollo per l'oggetto di storage.

   In ONTAP dalla versione 9.10.1 alla 9.12.1, l'unica opzione per un nuovo oggetto di storage è **l'utilizzo di nuove LUN**. A partire da ONTAP 9.13.1, System Manager supporta la creazione di gruppi di coerenza con nuovi namespace NVMe e nuovi volumi NAS.

3. Assegnare un nome al gruppo di coerenza. Indicare il numero di volumi o LUN e la capacità per volume o LUN.
   a. **Tipo di applicazione**: Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in Tag di applicazioni e componenti. Se si intende creare un gruppo di coerenza con un criterio di protezione remota, è necessario utilizzare **Altro**.
   b. Per **nuovi LUN**: Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
   c. Per **nuovi volumi NAS**: Scegliere l'opzione di esportazione appropriata (NFS o SMB/CIFS) in base alla configurazione NAS della SVM.
   d. Per **nuovi spazi dei nomi NVMe**: Selezionare il sistema operativo host e il sottosistema NVMe.
4. Per configurare i criteri di protezione, aggiungere un gruppo di coerenza figlio o i permessi di accesso, selezionare **altre opzioni**.
5. Selezionare **Salva**.
6. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro. Se si imposta una policy di protezione, si potrà sapere che è stata applicata quando viene visualizzato uno shield verde sotto la policy appropriata, remota o locale.

CLI

A partire da ONTAP 9.14.1, puoi creare un nuovo gruppo di coerenza con nuovi volumi utilizzando l'interfaccia a riga di comando di ONTAP. Parametri specifici dipendono se i volumi sono SAN, NVMe o NFS.

Crea un gruppo di coerenza con i volumi NFS

1. Creare il gruppo di coerenza:

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-
   group-name -volume volume-prefix -volume-count number -size size -export
   -policy policy_name
   ```

Crea un gruppo di coerenza con i volumi SAN

1. Creare il gruppo di coerenza:

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-
   group-name -lun lun_name -size size -lun-count number -igroup igroup_name
   ```

Crea un gruppo di coerenza con i namespace NVMe

1. Creare il gruppo di coerenza:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group_name -namespace namespace_name -volume-count number
   -namespace-count number -size size -subsystem subsystem_name
   ```

Al termine

1. Verificare che il gruppo di coerenza sia stato creato utilizzando `consistency-group show` comando.

Creare un gruppo di coerenza con i volumi esistenti

È possibile utilizzare i volumi esistenti per creare un gruppo di coerenza.

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi **utilizzando volumi esistenti**.
3. Assegnare un nome al gruppo di coerenza e selezionare la VM di storage.
   a. **Tipo di applicazione**: Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in Tag di applicazioni e componenti. Se il gruppo di coerenza ha una relazione SM-BC, è necessario utilizzare **Altro**.
4. Selezionare i volumi esistenti da includere. Saranno disponibili per la selezione solo i volumi che non fanno già parte di un gruppo di coerenza.

   > Se si crea un gruppo di coerenza con i volumi esistenti, il gruppo di coerenza supporta i volumi FlexVol. I volumi con relazioni SnapMirror sincrone o asincrone possono essere aggiunti ai gruppi di coerenza, ma non sono compatibili con i gruppi di coerenza. I gruppi di coerenza non supportano i bucket S3 o le VM di storage con relazioni SVMDR.

5. Selezionare **Salva**.
6. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se è stata scelta una policy di protezione, confermarla selezionando il gruppo di coerenza dal menu. Se si imposta una policy di protezione, si potrà sapere che è stata applicata quando viene visualizzato uno shield verde sotto la policy appropriata, remota o locale.

CLI

A partire da ONTAP 9.14.1, puoi creare un gruppo di coerenza con i volumi esistenti utilizzando l'interfaccia a riga di comando di ONTAP.

Fasi

1. Eseguire il `consistency-group create` comando. Il `-volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
   ```

2. Visualizzare il gruppo di coerenza utilizzando `consistency-group show` comando.

Passi successivi

- Proteggere un gruppo di coerenza
- Modificare un gruppo di coerenza
- Clonare un gruppo di coerenza

Configurare un gruppo di coerenza gerarchico

I gruppi di coerenza gerarchica consentono di gestire grandi carichi di lavoro su più volumi, creando un gruppo di coerenza padre che funge da ombrello per i gruppi di

coerenza figlio.

I gruppi di coerenza gerarchica hanno un padre che può includere fino a cinque singoli gruppi di coerenza. I gruppi di coerenza gerarchica possono supportare diverse policy Snapshot locali tra gruppi di coerenza o singoli volumi. Se si utilizza un criterio di protezione remota, questo verrà applicato all'intero gruppo di coerenza gerarchico (principale e figlio).

A partire da ONTAP 9.13.1, è possibile modificare la geometria dei gruppi di coerenza e. spostare i volumi tra i gruppi di coerenza figlio.

Per i limiti degli oggetti sui gruppi di coerenza, vedere Limiti degli oggetti per i gruppi di coerenza.

Creare un gruppo di coerenza gerarchica con nuove LUN o volumi

Quando si crea un gruppo di coerenza gerarchica, è possibile compilarlo con nuove LUN. A partire da ONTAP 9.13.1, puoi anche utilizzare nuovi namespace NVMe e volumi NAS.

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi selezionare il protocollo per l'oggetto di storage.

   In ONTAP dalla versione 9.10.1 alla 9.12.1, l'unica opzione per un nuovo oggetto di storage è **l'utilizzo di nuove LUN**. A partire da ONTAP 9.13.1, System Manager supporta la creazione di gruppi di coerenza con nuovi namespace NVMe e nuovi volumi NAS.

3. Assegnare un nome al gruppo di coerenza. Indicare il numero di volumi o LUN e la capacità per volume o LUN.
   a. **Tipo di applicazione**: Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in Tag di applicazioni e componenti. Se si prevede di utilizzare una policy di protezione remota, è necessario scegliere **Altro**.
4. Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
   a. Per **nuovi LUN**: Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
   b. Per **nuovi volumi NAS**: Scegliere l'opzione di esportazione appropriata (NFS o SMB/CIFS) in base alla configurazione NAS della SVM.
   c. Per **nuovi spazi dei nomi NVMe**: Selezionare il sistema operativo host e il sottosistema NVMe.
5. Per aggiungere un gruppo di coerenza figlio, selezionare **altre opzioni**, quindi **+Aggiungi gruppo di coerenza figlio**.
6. Selezionare il livello di performance, il numero di LUN o volumi e la capacità per LUN o volume. Indicare le configurazioni di esportazione appropriate o le informazioni del sistema operativo in base al protocollo in uso.
7. Facoltativamente, selezionare un criterio di snapshot locale e impostare le autorizzazioni di accesso.
8. Ripetere la procedura per un massimo di cinque gruppi di coerenza figlio.
9. Selezionare **Salva**.
10. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se si imposta un criterio di protezione, controllare il criterio appropriato, remoto o locale, che dovrebbe visualizzare uno schermo verde con un segno di spunta.

CLI

A partire da ONTAP 9.14.1, è possibile creare un nuovo gruppo di coerenza gerarchica utilizzando la CLI.

Fase

1. Creare il nuovo gruppo di coerenza utilizzando `consistency-group create` comando.

   Il `volume-count` parametro imposta il numero di volumi in ogni gruppo di coerenza figlio. È possibile creare un gruppo di coerenza di origine con un massimo di cinque gruppi di coerenza child.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -cg-count number_of_child_consistency_groups
   ```

```
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

Creare un gruppo di coerenza gerarchica con i volumi esistenti

È possibile organizzare i volumi esistenti in un gruppo di coerenza gerarchico.

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi **utilizzando volumi esistenti**.
3. Selezionare la VM di storage.
4. Selezionare i volumi esistenti da includere. Saranno disponibili per la selezione solo i volumi che non fanno già parte di un gruppo di coerenza.
5. Per aggiungere un gruppo di coerenza figlio, selezionare **+Aggiungi gruppo di coerenza figlio**. Creare i gruppi di coerenza necessari, che verranno nominati automaticamente.
   a. **Tipo di componente**: Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di componente "dati", "registri" o "Altro". Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in Tag di applicazioni e componenti. Se si intende utilizzare una policy di protezione remota, è necessario utilizzare **Altro**.
6. Assegnare i volumi esistenti a ciascun gruppo di coerenza.
7. Facoltativamente, selezionare un criterio Snapshot locale.
8. Ripetere la procedura per un massimo di cinque gruppi di coerenza figlio.
9. Selezionare **Salva**.
10. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se è stata scelta una policy di protezione, confermarla selezionando il gruppo di coerenza dal menu; sotto il tipo di policy appropriato, viene visualizzato uno shield verde con un segno di spunta all'interno di essa.

CLI

A partire da ONTAP 9.14.1, è possibile creare un gruppo di coerenza gerarchica utilizzando la CLI.

Fasi

1. Provisioning di un nuovo gruppo di coerenza di origine e assegnazione dei volumi a un nuovo gruppo di coerenza child:

   ```
   consistency-group create -vserver svm_name -consistency-group
   child_consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volumes volume_names
   ```

2. Invio `y` per confermare la creazione di un nuovo gruppo di coerenza principale e secondario.

Passi successivi

- Modificare la geometria di un gruppo di coerenza

- Modificare un gruppo di coerenza
- Proteggere un gruppo di coerenza

Proteggere i gruppi di coerenza

I gruppi di coerenza offrono una protezione locale e remota facilmente gestibile per LE applicazioni SAN, NAS e NVMe che si estendono su più volumi.

La creazione di un gruppo di coerenza non attiva automaticamente la protezione. Le policy di protezione possono essere impostate al momento della creazione o dopo la creazione del gruppo di coerenza. È possibile proteggere i gruppi di coerenza utilizzando:

- Copie snapshot locali
- Continuità aziendale SnapMirror (SM-BC)
- MetroCluster (inizio 9.11.1)
- SnapMirror asincrono (inizio 9.13.1)
- Disaster recovery SVM asincrono (inizio 9.14.1)

Se si utilizzano gruppi di coerenza nidificati, è possibile impostare criteri di protezione diversi per i gruppi di coerenza padre e figlio.

A partire da ONTAP 9.11.1, i gruppi di coerenza offrono Creazione Snapshot di un gruppo di coerenza in due fasi. L'operazione Snapshot a due fasi esegue un controllo preliminare, accertandosi che la copia Snapshot venga acquisita correttamente.

Il ripristino può avvenire per un intero gruppo di coerenza, per un singolo gruppo di coerenza in una configurazione gerarchica o per singoli volumi all'interno del gruppo di coerenza. Il ripristino può essere ottenuto selezionando il gruppo di coerenza da cui si desidera eseguire il ripristino, selezionando il tipo di copia Snapshot e identificando la copia Snapshot su cui basare il ripristino. Per ulteriori informazioni su questo processo, vedere "Ripristinare un volume da una copia Snapshot precedente".

Configurare un criterio Snapshot locale

L'impostazione di un criterio di protezione snapshot locale consente di creare un criterio che copre tutti i volumi in un gruppo di coerenza.

A proposito di questa attività

La pianificazione minima supportata delle copie Snapshot per i gruppi di coerenza è di 30 minuti. Basata su "Test per i gruppi flessibili", Che condividono la stessa infrastruttura Snapshot dei gruppi di coerenza.

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
3. Nella parte superiore destra della pagina di panoramica per il gruppo di coerenza, selezionare **Modifica**.
4. Selezionare la casella di controllo accanto a **Schedule Snapshot Copies (local)**.
5. Selezionare una policy Snapshot. Per configurare un nuovo criterio personalizzato, fare riferimento a. "Creare una policy di protezione dei dati personalizzata".
6. Selezionare **Salva**.
7. Tornare al menu della panoramica del gruppo di coerenza. Nella colonna di sinistra sotto **Snapshot Copies (Local)**, lo stato sarà Protected (protetto) accanto a. .

CLI

A partire da ONTAP 9.14.1, è possibile modificare il criterio di protezione di un gruppo di coerenza utilizzando l'interfaccia CLI.

Fase

1. Immettere il seguente comando per impostare o modificare il criterio di protezione:

   Se si modifica il criterio di protezione di una coerenza figlio, è necessario identificare il gruppo di coerenza padre utilizzando `-parent-consistency-group` *`parent_consistency_group_name`* parametro.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Crea una copia Snapshot on-demand

Se devi creare una copia Snapshot del tuo gruppo di coerenza al di fuori di una policy normalmente pianificata, puoi crearne una on-demand.

System Manager

Fasi

1. Accedere a **archiviazione** > **gruppi di coerenza**.
2. Seleziona il gruppo di coerenza per cui desideri creare una copia Snapshot on-demand.
3. Passare alla scheda **Snapshot Copies** e selezionare **+Add**.
4. Fornire un **Name** e una **SnapMirror Label**. Nel menu a discesa per **coerenza**, selezionare **applicazione coerente** o **Crash coerente**.
5. Selezionare **Salva**.

CLI

A partire da ONTAP 9.14.1, puoi creare una copia Snapshot on-demand di un gruppo di coerenza utilizzando la CLI.

Fase

1. Creare la copia Snapshot:

   Per impostazione predefinita, il tipo di Snapshot è coerente con il crash. È possibile modificare il tipo di istantanea con l'opzione `-type` parametro.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Creare Snapshot del gruppo di coerenza in due fasi

A partire da ONTAP 9.11.1, i gruppi di coerenza supportano commit a due fasi per la creazione di snapshot nel CG (Consistency group), che eseguono un controllo preliminare prima di salvare la copia Snapshot. Questa funzione è disponibile solo con l'API REST di ONTAP.

La creazione di snapshot CG in due fasi è disponibile solo per la creazione di Snapshot, non per il provisioning di gruppi di coerenza o il ripristino di gruppi di coerenza.

Un'istantanea CG in due fasi suddivide il processo di creazione delle snapshot in due fasi:

1. Nella prima fase, l'API esegue i controlli preliminari e attiva la creazione di snapshot. La prima fase include un parametro di timeout che indica il tempo necessario per il commit della copia Snapshot.
2. Se la richiesta nella fase uno viene completata correttamente, è possibile richiamare la seconda fase all'interno dell'intervallo designato dalla prima fase, assegnando la copia Snapshot all'endpoint appropriato.

Prima di iniziare

- Per utilizzare la creazione di snapshot CG in due fasi, tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- Solo una chiamata attiva di un'operazione Snapshot del gruppo di coerenza è supportata su un'istanza di un gruppo di coerenza alla volta, sia che si tratti di una fase singola che di due fasi. Se si tenta di richiamare un'operazione snapshot mentre è in corso un'altra operazione, si verifica un errore.
- Quando si richiama la creazione snapshot, è possibile impostare un valore di timeout opzionale compreso tra 5 e 120 secondi. Se non viene fornito alcun valore di timeout, l'operazione scade per impostazione predefinita di 7 secondi. Nell'API, impostare il valore di timeout con `action_timeout` parametro.

Nell'interfaccia CLI, utilizzare il `-timeout` allarme.

Fasi

Puoi completare una snapshot in due fasi con l'API REST o, a cominciare da ONTAP 9.14.1, l'interfaccia a riga di comando di ONTAP. Questa operazione non è supportata in System Manager.

> Se si richiama la creazione di Snapshot con l'API, è necessario assegnare la copia Snapshot all'API. Se si richiama la creazione di Snapshot con la CLI, è necessario assegnare la copia Snapshot con la CLI. I metodi di miscelazione non sono supportati.

CLI

A partire da ONTAP 9.14.1, è possibile creare una copia Snapshot in due fasi utilizzando l'interfaccia a riga di comando.

Fasi

1. Avviare l'istantanea:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Verificare che l'istantanea sia stata acquisita:

   ```
   consistency-group snapshot show
   ```

3. Inserimento dello snapshot:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Richiamare la creazione di Snapshot. Inviare una richiesta POST all'endpoint del gruppo di coerenza utilizzando `action=start` parametro.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Se la richiesta POST ha esito positivo, l'output include un uuid snapshot. Utilizzando tale uuid, inviare una richiesta di PATCH per salvare la copia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Impostare la protezione remota per un gruppo di coerenza

I gruppi di coerenza offrono protezione remota tramite SM-BC e, a partire da ONTAP 9.13.1, SnapMirror asincrono.

Configurare la protezione con SM-BC

È possibile utilizzare SM-BC per garantire che le copie Snapshot dei gruppi di coerenza creati nel proprio gruppo di coerenza vengano copiate nella destinazione. Per ulteriori informazioni su SM-BC o su come configurare SM-BC utilizzando la CLI, vedere Configurare la protezione per la business continuity.

Prima di iniziare

- Non è possibile stabilire relazioni SM-BC sui volumi montati per l'accesso NAS.
- Le etichette dei criteri nel cluster di origine e di destinazione devono corrispondere.
- SM-BC non replica le copie Snapshot per impostazione predefinita, a meno che non venga aggiunta una regola con un'etichetta SnapMirror al predefinito `AutomatedFailOver` Le copie di policy e Snapshot vengono create con tale etichetta.

  Per ulteriori informazioni su questo processo, fare riferimento a. "Proteggere con SM-BC".

- Implementazioni a cascata Non sono supportati con SM-BC.
- A partire da ONTAP 9.13.1, è possibile eseguire operazioni senza interruzioni aggiungere volumi a un gruppo di coerenza Con una relazione SM-BC attiva. Qualsiasi altra modifica apportata a un gruppo di coerenza richiede di interrompere la relazione SM-BC, modificare il gruppo di coerenza, quindi ristabilire e risincronizzare la relazione.

Per configurare SM-BC con la CLI, vedere Proteggere con SM-BC.

Procedura per System Manager

1. Assicurarsi di aver soddisfatto il "Prerequisiti per l'utilizzo di SM-BC".
2. Selezionare **Storage > Consistency groups**.
3. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
4. Nella parte superiore destra della pagina panoramica, selezionare **More** (Altro), quindi **Protect** (protezione).
5. System Manager compila automaticamente le informazioni sul lato di origine. Selezionare il cluster e la VM di storage appropriati per la destinazione. Selezionare un criterio di protezione. Assicurarsi che l'opzione

Inizializza relazione sia selezionata.

6. Selezionare **Salva**.
7. Il gruppo di coerenza deve essere inizializzato e sincronizzato. Verificare che la sincronizzazione sia stata completata correttamente tornando al menu **Consistency group**. Viene visualizzato lo stato **SnapMirror (Remote)** `Protected` accanto a. .

Configurare la protezione asincrona di SnapMirror

A partire da ONTAP 9.13.1, è possibile configurare la protezione SnapMirror asincrona per un singolo gruppo di coerenza. A partire da ONTAP 9.14.1, puoi utilizzare SnapMirror asincrono per replicare le copie Snapshot granulari del volume nel cluster di destinazione usando la relazione del gruppo di coerenza.

A proposito di questa attività

Per replicare le copie Snapshot granulari per volume, devi eseguire ONTAP 9.14.1 o versioni successive. Per le policy MirrorAndVault e Vault, l'etichetta SnapMirror della policy di Snapshot granulare per il volume deve corrispondere alla regola dei criteri di SnapMirror del gruppo di coerenza. Gli Snapshot granulari del volume si basano sul valore di mantenimento della policy SnapMirror del gruppo di coerenza, che viene calcolata indipendentemente dagli Snapshot del gruppo di coerenza. Ad esempio, se disponi di una policy per mantenere due copie Snapshot sulla destinazione, puoi disporre di due copie Snapshot granulari del volume e due copie Snapshot del gruppo di coerenza.

Durante la risincronizzazione del rapporto di SnapMirror con le copie Snapshot granulari del volume, puoi conservare le copie Snapshot granulari del volume con il `-preserve` allarme. Le copie Snapshot granulari del volume più recenti delle copie Snapshot del gruppo di coerenza vengono conservate. Se non è presente una copia Snapshot del gruppo di coerenza, non è possibile trasferire copie Snapshot granulari del volume nell'operazione di risincronizzazione.

Prima di iniziare

- La protezione asincrona di SnapMirror è disponibile solo per singoli gruppi di coerenza. Non è supportato per i gruppi di coerenza gerarchica. Per convertire un gruppo di coerenza gerarchica in un singolo gruppo di coerenza, vedere modificare l'architettura del gruppo di coerenza.
- Le etichette dei criteri nel cluster di origine e di destinazione devono corrispondere.
- È possibile senza interruzioni aggiungere volumi a un gruppo di coerenza Con una relazione SnapMirror asincrona attiva. Qualsiasi altra modifica apportata a un gruppo di coerenza richiede di interrompere la relazione SnapMirror, modificare il gruppo di coerenza, quindi ristabilire e risincronizzare la relazione.
- Se è stato configurato un rapporto di protezione SnapMirror asincrono per più singoli volumi, è possibile convertire tali volumi in un gruppo di coerenza mantenendo al contempo le copie Snapshot esistenti. Per convertire correttamente i volumi:
  - Deve essere presente una copia Snapshot comune dei volumi.
  - È necessario interrompere la relazione SnapMirror esistente, aggiungere i volumi a un singolo gruppo di coerenza, quindi risincronizzare la relazione utilizzando il seguente flusso di lavoro.

Fasi

1. Dal cluster di destinazione, selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
3. Nella parte superiore destra della pagina panoramica, selezionare **More** (Altro), quindi **Protect** (protezione).
4. System Manager compila automaticamente le informazioni sul lato di origine. Selezionare il cluster e la VM di storage appropriati per la destinazione. Selezionare un criterio di protezione. Assicurarsi che l'opzione

Inizializza relazione sia selezionata.

Quando si seleziona un criterio asincrono, è possibile scegliere **Ignora pianificazione trasferimento**.

> La pianificazione minima supportata (Recovery Point Objective, o RPO) per i gruppi di coerenza con SnapMirror asincrono è di 30 minuti.

5. Selezionare **Salva**.
6. Il gruppo di coerenza deve essere inizializzato e sincronizzato. Verificare che la sincronizzazione sia stata completata correttamente tornando al menu **Consistency group**. Viene visualizzato lo stato **SnapMirror (Remote)** `Protected` accanto a. .

Configurare il disaster recovery delle SVM

A partire da ONTAP 9.14.1, Disaster recovery SVM supporta i gruppi di coerenza per eseguire il mirroring delle informazioni del gruppo di coerenza dall'origine al cluster di destinazione.

Se stai abilitando il disaster recovery delle SVM in una SVM che contiene già un gruppo di coerenza, segui i workflow di configurazione delle SVM per System Manager o il CLI ONTAP.

Se stai aggiungendo un gruppo di coerenza a una SVM che si trova in una relazione di disaster recovery SVM attiva e funzionante, devi aggiornare la relazione di disaster recovery della SVM dal cluster di destinazione. Per ulteriori informazioni, vedere Aggiornare manualmente una relazione di replica. È necessario aggiornare la relazione ogni volta che si espande il gruppo di coerenza.

Limitazioni

- Il disaster recovery delle SVM non supporta i gruppi di coerenza gerarchici.
- Il disaster recovery delle SVM non supporta gruppi di coerenza protetti con SnapMirror asincrono. È necessario interrompere il rapporto SnapMirror prima di configurare il disaster recovery delle SVM.
- Entrambi i cluster devono eseguire ONTAP 9.14.1 o versione successiva.
- Le relazioni di fan-out non sono supportate per le configurazioni di disaster recovery delle SVM che contengono gruppi di coerenza.
- Per altri limiti, vedere limiti del gruppo di coerenza.

Visualizzare le relazioni

System Manager visualizza le mappe LUN nel menu **protezione > Relazioni**. Quando si seleziona una relazione di origine, System Manager visualizza una visualizzazione delle relazioni di origine. Selezionando un volume, è possibile approfondire queste relazioni per visualizzare un elenco delle LUN contenute e delle relazioni del gruppo iniziatore. Queste informazioni possono essere scaricate come cartella di lavoro Excel dalla vista del singolo volume; l'operazione di download viene eseguita in background.

Informazioni correlate

- "Clonare un gruppo di coerenza"
- "Configurare le copie Snapshot"
- "Creare policy di protezione dei dati personalizzate"
- "Ripristino da copie Snapshot"
- "Ripristinare un volume da una copia Snapshot precedente"
- "Panoramica di SM-BC"

- "Documentazione sull'automazione ONTAP"
- Nozioni di base sul disaster recovery asincrono di SnapMirror

Modificare i volumi membri in un gruppo di coerenza

A partire da ONTAP 9.12.1, è possibile modificare un gruppo di coerenza rimuovendo volumi o aggiungendo volumi (espandendo il gruppo di coerenza). A partire da ONTAP 9.13.1, è possibile spostare i volumi tra i gruppi di coerenza child se condividono un'origine comune.

Aggiungere volumi a un gruppo di coerenza

A partire da ONTAP 9.12.1, puoi aggiungere volumi senza interruzioni a un gruppo di coerenza.

A proposito di questa attività

- Non è possibile aggiungere volumi associati a un altro gruppo di coerenza.
- I gruppi di coerenza supportano i protocolli NAS, SAN e NVMe.
- È possibile aggiungere fino a 16 volumi alla volta a un gruppo di coerenza se le regolazioni sono all'interno del complessivo limiti del gruppo di coerenza.
- A partire da ONTAP 9.13.1, puoi aggiungere volumi senza interruzioni a un gruppo di coerenza con una policy di protezione SnapMirror Business Continuity (SM-BC) o asincrona.
- Quando si aggiungono volumi a un gruppo di coerenza protetto da SM-BC, lo stato della relazione SM-BC cambia in "Expanding" (in espansione) fino a quando il mirroring e la protezione non vengono configurati per il nuovo volume. Se si verifica un disastro sul cluster primario prima del completamento di questo processo, il gruppo di coerenza torna alla sua composizione originale come parte dell'operazione di failover.
- In ONTAP 9.12.1 e versioni precedenti, *non è possibile* aggiungere volumi a un gruppo di coerenza in una relazione SM-BC. È necessario prima interrompere la relazione SM-BC, modificare il gruppo di coerenza, quindi ripristinare la protezione con SM-BC.
- A partire da ONTAP 9.12.1, l'API REST ONTAP supporta l'aggiunta di volumi *nuovi* o esistenti a un gruppo di coerenza. Per ulteriori informazioni sull'API REST di ONTAP, fare riferimento a. "Documentazione di riferimento API REST di ONTAP".

  A partire da ONTAP 9.13.1, questa funzionalità è supportata in Gestione sistema.

- Quando si espande un gruppo di coerenza, le copie Snapshot del gruppo di coerenza acquisite prima della modifica saranno considerate parziali. Qualsiasi operazione di ripristino basata su tale copia Snapshot rifletterà il gruppo di coerenza nel momento in cui lo snapshot viene creato.
- Se si utilizza ONTAP da 9.10.1 a 9.11.1, non è possibile modificare un gruppo di coerenza. Per modificare la configurazione di un gruppo di coerenza in ONTAP 9.10.1 o 9.11.1, è necessario eliminare il gruppo di coerenza, quindi creare un nuovo gruppo di coerenza con i volumi che si desidera includere.
- A partire da ONTAP 9.14.1, puoi replicare gli Snapshot granulari del volume nel cluster di destinazione utilizzando SnapMirror asincrono. Quando si espande un gruppo di coerenza utilizzando SnapMirror asincrono, gli Snapshot granulari dei volumi vengono replicati solo dopo aver espanso il gruppo di coerenza quando la policy SnapMirror è MirrorAll o MirrorAndVault. Vengono replicati solo gli Snapshot granulari del volume più recenti rispetto allo Snapshot del gruppo di coerenza di base.
- Se Aggiungi volumi a un gruppo di coerenza in una relazione di disaster recovery della SVM (supportato a partire da ONTAP 9.14.1), devi aggiornare la relazione di disaster recovery della SVM dal cluster di

destinazione dopo aver espanso il gruppo di coerenza. Per ulteriori informazioni, vedere Aggiornare manualmente una relazione di replica.

Esempio 1. Fasi

System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera modificare.
3. Se si sta modificando un singolo gruppo di coerenza, nella parte superiore del menu **Volumes** (volumi), selezionare **More** (Altro), quindi **Expand** (Espandi) per aggiungere un volume.

   Se si modifica un gruppo di coerenza figlio, identificare il gruppo di coerenza padre che si desidera modificare. Selezionare il pulsante **>** per visualizzare i gruppi di coerenza secondari, quindi selezionare ⋮ accanto al nome del gruppo di coerenza figlio che si desidera modificare. Da questo menu, selezionare **Espandi**.
4. Selezionare fino a 16 volumi da aggiungere al gruppo di coerenza.
5. Selezionare **Salva**. Al termine dell'operazione, visualizzare i volumi aggiunti di recente nel menu **Volumes** del gruppo di coerenza.

CLI

A partire da ONTAP 9.14.1, è possibile aggiungere volumi a un gruppo di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

Aggiungere volumi esistenti

1. Inserire il seguente comando. Il `-volumes` parameter accetta un elenco di volumi separati da virgole.

   > Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Aggiungere nuovi volumi

La procedura per aggiungere nuovi volumi dipende dal protocollo utilizzato.

> Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

- Per aggiungere nuovi volumi senza esportarli:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- Per aggiungere nuovi volumi NFS:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency-group-name -volume volume-prefix -volume-count number -size
  size -export-policy policy_name
  ```

- Per aggiungere nuovi volumi SAN:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency-group-name -lun lun_name -size size -lun-count number -igroup
  igroup_name
  ```

- Per aggiungere nuovi namespace NVMe:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  consistency_group_name -namespace namespace_name -volume-count number
  -namespace-count number -size size -subsystem subsystem_name
  ```

Rimuovere i volumi da un gruppo di coerenza

I volumi rimossi da un gruppo di coerenza non vengono eliminati. Rimangono attivi nel cluster.

A proposito di questa attività

- Non puoi rimuovere volumi da un gruppo di coerenza in una relazione di disaster recovery SM-BC o SVM. È necessario interrompere prima la relazione SM-BC per modificare il gruppo di coerenza e quindi ristabilire la relazione.
- Se un gruppo di coerenza non contiene volumi dopo l'operazione di rimozione, il gruppo di coerenza viene eliminato.
- Quando un volume viene rimosso da un gruppo di coerenza, le istantanee esistenti del gruppo di coerenza rimangono ma vengono considerate non valide. Le istantanee esistenti non possono essere utilizzate per ripristinare il contenuto del gruppo di coerenza. Le snapshot granulari dei volumi rimangono valide.
- Se si elimina un volume dal cluster, questo viene automaticamente rimosso dal gruppo di coerenza.
- Per modificare la configurazione di un gruppo di coerenza in ONTAP 9.10.1 o 9.11.1, è necessario eliminare il gruppo di coerenza e creare un nuovo gruppo di coerenza con i volumi membro desiderati.
- L'eliminazione di un volume dal cluster comporta la rimozione automatica del gruppo di coerenza.

System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza singolo o secondario che si desidera modificare.
3. Nel menu **Volumes**, selezionare le caselle di controllo accanto ai singoli volumi che si desidera rimuovere dal gruppo di coerenza.
4. Selezionare **Rimuovi volumi dal gruppo di coerenza**.
5. Confermare che la rimozione dei volumi causerà l'invalidità di tutte le copie Snapshot del gruppo di coerenza e selezionare **Rimuovi**.

CLI

A partire da ONTAP 9.14.1, puoi rimuovere i volumi da un gruppo di coerenza utilizzando la CLI.

Fase

1. Rimuovere i volumi. Il `-volumes` parameter accetta un elenco di volumi separati da virgole.

   Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Spostare i volumi tra i gruppi di coerenza

A partire da ONTAP 9.13.1, è possibile spostare i volumi tra gruppi di coerenza child che condividono un'immagine di origine.

A proposito di questa attività

- È possibile spostare i volumi solo tra gruppi di coerenza nidificati nello stesso gruppo di coerenza padre.
- Le istantanee del gruppo di coerenza esistente diventano invalide e non più accessibili come snapshot del gruppo di coerenza. Le snapshot dei singoli volumi rimangono valide.
- Le copie Snapshot del gruppo di coerenza padre rimangono valide.
- Se si spostano tutti i volumi da un gruppo di coerenza figlio, tale gruppo di coerenza verrà eliminato.
- Le modifiche apportate a un gruppo di coerenza devono essere rispettate limiti del gruppo di coerenza.

System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che contiene i volumi che si desidera spostare. Individuare il gruppo di coerenza figlio, quindi espandere il menu **volumi**. Selezionare i volumi che si desidera spostare.
3. Selezionare **Sposta**.
4. Scegliere se spostare i volumi in un nuovo gruppo di coerenza o in un gruppo esistente.
   a. Per passare a un gruppo di coerenza esistente, selezionare **gruppo di coerenza figlio esistente**, quindi scegliere il nome del gruppo di coerenza dal menu a discesa.
   b. Per passare a un nuovo gruppo di coerenza, selezionare **nuovo gruppo di coerenza figlio**. Immettere un nome per il nuovo gruppo di coerenza figlio e selezionare un tipo di componente.
5. Selezionare **Sposta**.

CLI

A partire da ONTAP 9.14.1, puoi spostare i volumi tra gruppi di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

Spostamento dei volumi in un nuovo gruppo di coerenza figlio

1. Il seguente comando crea un nuovo gruppo di coerenza figlio che contiene i volumi designati.

   Quando crei il nuovo gruppo di coerenza, puoi designare nuove policy di Snapshot, QoS e tiering.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Spostamento dei volumi in un gruppo di coerenza figlio esistente

1. Riassegnare i volumi. Il `-volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Informazioni correlate

- Limiti del gruppo di coerenza
- Clonare un gruppo di coerenza

Modificare la geometria del gruppo di coerenza

A partire da ONTAP 9.13.1, è possibile modificare la geometria di un gruppo di coerenza. La modifica della geometria di un gruppo di coerenza consente di modificare la configurazione dei gruppi di coerenza figlio o padre senza interrompere le operazioni io in corso.

La modifica della geometria del gruppo di coerenza avrà un impatto sulle copie Snapshot esistenti.

> Non è possibile modificare la geometria di un gruppo di coerenza configurato con un criterio di protezione remota. È necessario prima interrompere la relazione di protezione, modificare la geometria, quindi ripristinare la protezione remota.

Aggiungere un nuovo gruppo di coerenza figlio

A partire da ONTAP 9.13.1, è possibile aggiungere un nuovo gruppo di coerenza figlio a un gruppo di coerenza padre esistente.

Prima di iniziare

- Un gruppo di coerenza padre può contenere un massimo di cinque gruppi di coerenza figlio. Vedere limiti del gruppo di coerenza per altri limiti.
- Non è possibile aggiungere un gruppo di coerenza figlio a un singolo gruppo di coerenza. Devi prima [promuovi] il gruppo di coerenza, quindi è possibile aggiungere un gruppo di coerenza figlio.
- Le copie Snapshot esistenti del gruppo di coerenza acquisite prima dell'operazione di espansione verranno considerate parziali. Qualsiasi operazione di ripristino basata su tale copia snapshot rifletterà il gruppo di coerenza nel momento in cui la copia Snapshot viene eseguita.

Esempio 2. Fasi

System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre a cui si desidera aggiungere un gruppo di coerenza figlio.
3. Accanto al nome del gruppo di coerenza padre, selezionare **Altro**, quindi **Aggiungi nuovo gruppo di coerenza figlio**.
4. Immettere un nome per il gruppo di coerenza.
5. Scegliere se si desidera aggiungere volumi nuovi o esistenti.
   a. Se si stanno aggiungendo volumi esistenti, selezionare **volumi esistenti**, quindi scegliere i volumi dal menu a discesa.
   b. Se si stanno aggiungendo nuovi volumi, selezionare **nuovi volumi**, quindi specificare il numero di volumi e le relative dimensioni.
6. Selezionare **Aggiungi**.

CLI

A partire da ONTAP 9.14.1, è possibile aggiungere un gruppo di coerenza figlio utilizzando la CLI di ONTAP.

Aggiungere un gruppo di coerenza figlio con nuovi volumi

1. Creare il nuovo gruppo di coerenza. Fornire i valori per il nome del gruppo di coerenza, il prefisso del volume, il numero di volumi, le dimensioni del volume, il servizio di archiviazione, e nome della policy di esportazione:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Aggiungere un gruppo di coerenza figlio con i volumi esistenti

1. Creare il nuovo gruppo di coerenza. Il `volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Scollegare un gruppo di coerenza figlio

A partire da ONTAP 9.13.1, è possibile rimuovere un gruppo di coerenza figlio dal relativo gruppo padre, convertendolo in un singolo gruppo di coerenza.

Prima di iniziare

- La rimozione di un gruppo di coerenza figlio causa l'invalidità e l'inaccessibilità degli snapshot del gruppo di coerenza padre. Gli snapshot granulari del volume rimangono validi.

- Le copie Snapshot esistenti del singolo gruppo di coerenza rimangono valide.
- Questa operazione non riesce se esiste un singolo gruppo di coerenza esistente con lo stesso nome del gruppo di coerenza figlio che si intende scollegare. Se si verifica questo scenario, è necessario rinominare il gruppo di coerenza quando lo si scollega.

Esempio 3. Fasi

System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che contiene il figlio che si desidera scollegare.
3. Accanto al gruppo di coerenza figlio che si desidera scollegare, selezionare **Altro**, quindi **Scollega dall'origine**.
4. Facoltativamente, rinominare il gruppo di coerenza e selezionare un tipo di applicazione.
5. Selezionare **stacca**.

CLI

A partire da ONTAP 9.14.1, è possibile scollegare un gruppo di coerenza figlio utilizzando l'interfaccia a riga di comando di ONTAP.

1. Staccare il gruppo di coerenza. Facoltativamente, rinominare il gruppo di coerenza autonomo con `-new-name` parametro.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Sposta un singolo gruppo di coerenza esistente in un gruppo di coerenza di origine

A partire da ONTAP 9.13.1, è possibile convertire un singolo gruppo di coerenza esistente in un gruppo di coerenza figlio. È possibile spostare il gruppo di coerenza in un gruppo di coerenza padre esistente o creare un nuovo gruppo di coerenza padre durante l'operazione di spostamento.

Prima di iniziare

- Il gruppo di coerenza padre deve avere un massimo di quattro figli. Un gruppo di coerenza padre può contenere un massimo di cinque gruppi di coerenza figlio. Vedere limiti del gruppo di coerenza per altri limiti.
- Le copie Snapshot esistenti del gruppo di coerenza *padre* catturate prima di questa operazione saranno considerate parziali. Qualsiasi operazione di ripristino basata su una di queste copie Snapshot rifletterà il gruppo di coerenza nel momento in cui la copia Snapshot viene eseguita.
- Le snapshot dei gruppi di coerenza esistenti del singolo gruppo di coerenza rimangono valide.

Esempio 4. Fasi

System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera convertire.
3. Selezionare **Altro**, quindi **spostarsi in un gruppo di coerenza diverso**.
4. Facoltativamente, immettere un nuovo nome per il gruppo di coerenza e selezionare un tipo di componente. Per impostazione predefinita, il tipo di componente sarà altro.
5. Scegliere se si desidera migrare a un gruppo di coerenza padre esistente o creare un nuovo gruppo di coerenza padre:
   a. Per migrare a un gruppo di coerenza padre esistente, selezionare **gruppo di coerenza esistente**, quindi scegliere il gruppo di coerenza dal menu a discesa.
   b. Per creare un nuovo gruppo di coerenza padre, selezionare **nuovo gruppo di coerenza**, quindi specificare un nome per il nuovo gruppo di coerenza.
6. Selezionare **Sposta**.

CLI

A partire da ONTAP 9.14.1, puoi spostare un singolo gruppo di coerenza sotto un gruppo di coerenza di origine utilizzando l'interfaccia a riga di comando di ONTAP.

Spostare un gruppo di coerenza in un nuovo gruppo di coerenza di origine

1. Creare il nuovo gruppo di coerenza di origine. Il `-consistency-groups` il parametro migrerà tutti i gruppi di coerenza esistenti al nuovo padre.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

Spostare un gruppo di coerenza in un gruppo di coerenza esistente

1. Spostare il gruppo di coerenza:

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

Promuovere un gruppo di coerenza figlio

A partire da ONTAP 9.13.1, puoi promuovere un singolo gruppo di coerenza in un gruppo di coerenza di origine. Quando si promuove un singolo gruppo di coerenza a un gruppo padre, si crea anche un nuovo gruppo di coerenza figlio che eredita tutti i volumi nel singolo gruppo di coerenza originale.

Prima di iniziare

- Se si desidera convertire un gruppo di coerenza figlio in un gruppo di coerenza padre, è necessario innanzitutto [detach] il gruppo di coerenza figlio quindi seguire questa procedura.
- Le copie Snapshot esistenti del gruppo di coerenza rimangono valide dopo la promozione del gruppo di coerenza.

Esempio 5. Fasi

System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera promuovere.
3. Selezionare **Altro**, quindi **Promuovi al gruppo di coerenza padre**.
4. Inserire un **Nome** e selezionare un **tipo di componente** per il gruppo di coerenza figlio.
5. Selezionare **Promuovi**.

CLI

A partire da ONTAP 9.14.1, puoi spostare un singolo gruppo di coerenza sotto un gruppo di coerenza di origine utilizzando l'interfaccia a riga di comando di ONTAP.

1. Promuovere il gruppo di coerenza. Questo comando creerà un gruppo di coerenza principale e un gruppo secondario.

   ```
   consistency-group promote -vserver SVM_name -consistency-group
   existing_consistency_group -new-name new_child_consistency_group
   ```

Consente di declassare un padre in un singolo gruppo di coerenza

A partire da ONTAP 9.13.1, puoi demotare un gruppo di coerenza di origine in un singolo gruppo di coerenza. Il deeming del padre appiattisce la gerarchia del gruppo di coerenza, rimuovendo tutti i gruppi di coerenza figlio associati. Tutti i volumi nel gruppo di coerenza rimarranno nel nuovo gruppo di coerenza singolo.

Prima di iniziare

- Le copie Snapshot esistenti del gruppo di coerenza padre rimangono valide dopo essere state retrocesse a una singola coerenza. Le copie Snapshot esistenti di uno qualsiasi dei gruppi di coerenza figlio associati di quel padre diventeranno non valide, ma le singole snapshot dei volumi al loro interno continuano ad essere accessibili come snapshot granulari dei volumi.

Esempio 6. Fasi

System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che si desidera declassare.
3. Selezionare **Altro**, quindi **Demodi a singolo gruppo di coerenza**.
4. Un avviso informa che tutti i gruppi di coerenza figlio associati verranno eliminati e i relativi volumi verranno spostati nel nuovo gruppo di coerenza singolo. Selezionare **Demote** per confermare di aver compreso l'impatto.

CLI

A partire da ONTAP 9.14.1, puoi demotizzare un gruppo di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

1. Demotare il gruppo di coerenza. Utilizzare l'opzione `-new-name` parametro per rinominare il gruppo di coerenza.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modificare i tag dell'applicazione e del componente

A partire da ONTAP 9.12.1, i gruppi di coerenza supportano l'etichettatura di componenti e applicazioni. I tag di applicazioni e componenti sono uno strumento di gestione che consente di filtrare e identificare diversi carichi di lavoro nei gruppi di coerenza.

A proposito di questa attività

I gruppi di coerenza offrono due tipi di tag:

- **Tag applicazione**: Si applicano ai singoli gruppi di coerenza e ai gruppi di coerenza padre. I tag applicativi forniscono l'etichettatura per carichi di lavoro come MongoDB, Oracle o SQL Server. Il tag di applicazione predefinito per i gruppi di coerenza è Altro.
- **Tag dei componenti**: I figli nei gruppi di coerenza gerarchica hanno tag dei componenti invece di tag delle applicazioni. Le opzioni per i tag dei componenti sono "dati", "registri" o "Altro". Il valore predefinito è Other (Altro).

È possibile applicare tag durante la creazione di gruppi di coerenza o dopo la creazione di gruppi di coerenza.

> Se il gruppo di coerenza ha una relazione SM-BC, è necessario utilizzare **Altro** come tag dell'applicazione o del componente.

Fasi

A partire da ONTAP 9.12.1, è possibile modificare i tag delle applicazioni e dei componenti utilizzando Gestione di sistema. A partire da ONTAP 9.14.1, è possibile modificare i tag delle applicazioni e dei componenti utilizzando l'interfaccia CLI di ONTAP.

System Manager

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza di cui si desidera modificare il tag. Selezionare ⋮ Accanto al nome del gruppo di coerenza, quindi **Modifica**.
3. Nel menu a discesa, scegliere l'applicazione o il tag del componente appropriato.
4. Selezionare **Salva**.

CLI

A partire da ONTAP 9.14.1, è possibile modificare l'applicazione o il tag del componente di un gruppo di coerenza esistente utilizzando l'interfaccia CLI di ONTAP.

Modificare il tag dell'applicazione

1. I tag dell'applicazione accettano un numero limitato di stringhe preimpostate. Per vedere, l'elenco accettato di stringhe, eseguire il comando seguente:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Scegliere la stringa appropriata dall'output, quindi modificare il gruppo di coerenza:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modificare il tag del componente

1. Modificare il tipo di componente. Il tipo di componente può essere dati, registri o altro. Se si utilizza SM-BC, deve essere "Altro".
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Clonare un gruppo di coerenza

A partire da ONTAP 9.12.1, è possibile clonare un gruppo di coerenza per creare una copia di un gruppo di coerenza e del relativo contenuto. La clonazione di un gruppo di coerenza crea una copia della configurazione del gruppo di coerenza, dei relativi metadati come il tipo di applicazione e di tutti i volumi e i relativi contenuti come file, directory, LUN o spazi dei nomi NVMe.

A proposito di questa attività

Durante la clonazione di un gruppo di coerenza, è possibile clonarlo con la configurazione corrente, ma con il contenuto del volume così come sono o in base a un gruppo di coerenza esistente Snapshot.

La clonazione di un gruppo di coerenza è supportata solo per l'intero gruppo di coerenza. Non è possibile clonare un singolo gruppo di coerenza figlio in una relazione gerarchica: È possibile clonare solo la configurazione completa del gruppo di coerenza.

Quando si clonano gruppi di coerenza, i seguenti componenti non vengono clonati:

- IGroups
- Mappe LUN

- Sottosistemi NVMe
- Mappe dei sottosistemi dello spazio dei nomi NVMe

Prima di iniziare

- Quando si clonano gruppi di coerenza, ONTAP non crea condivisioni SMB per i volumi clonati se non viene specificato un nome di condivisione. * I gruppi di coerenza clonati non vengono montati se non viene specificato un percorso di giunzione.
- Se si tenta di clonare un gruppo di coerenza basato su un'istantanea che non riflette i volumi costituenti correnti del gruppo di coerenza, l'operazione non verrà eseguita correttamente.
- Dopo aver clonato un gruppo di coerenza, è necessario eseguire l'operazione di mappatura appropriata.

  Fare riferimento a. Mappare igroups a più LUN oppure Mappare uno spazio dei nomi NVMe in un sottosistema per ulteriori informazioni.

- La clonazione di un gruppo di coerenza non è supportata per un gruppo di coerenza in una relazione di Business Continuity SnapMirror o con qualsiasi volume DP associato.

System Manager

Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera clonare dal menu **Consistency Group**.
3. Nella parte superiore destra della pagina panoramica del gruppo di coerenza, selezionare **Clone**.
4. Immettere un nome per il nuovo gruppo di coerenza clonato o accettare il nome predefinito.
   a. Scegliere se si desidera attivare "**Thin Provisioning**".
   b. Scegliere **Split Clone** se si desidera separare il gruppo di coerenza dall'origine e allocare ulteriore spazio su disco per il gruppo di coerenza clonato.
5. Per clonare il gruppo di coerenza nello stato corrente, scegliere **Aggiungi una nuova copia Snapshot**.

   Per clonare il gruppo di coerenza in base a uno snapshot, scegliere **Usa una copia Snapshot esistente**. Selezionando questa opzione si apre un nuovo sottomenu. Scegliere l'istantanea che si desidera utilizzare come base per l'operazione di clonazione.
6. Selezionare **Clone**.
7. Tornare al menu **Consistency Group** per confermare che il gruppo di coerenza è stato clonato.

CLI

A partire da ONTAP 9.14.1, è possibile clonare un gruppo di coerenza utilizzando la CLI.

Clonare un gruppo di coerenza

1. Il `consistency-group clone create` command clona il gruppo di coerenza al suo stato corrente point-in-time. Per basare l'operazione di cloning su uno Snapshot, includere il `-source-snapshot` parametro.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Passi successivi

- Mappare igroups a più LUN
- Mappare uno spazio dei nomi NVMe in un sottosistema

Eliminare un gruppo di coerenza

Se si decide di non avere più bisogno di un gruppo di coerenza, è possibile eliminarlo.

A proposito di questa attività

- L'eliminazione di un gruppo di coerenza elimina l'istanza del gruppo di coerenza e *non* influisce sui volumi o sui LUN costituenti. L'eliminazione di un gruppo di coerenza non comporta l'eliminazione delle istantanee presenti su ciascun volume, ma non sarà più accessibile come snapshot del gruppo di coerenza. Tuttavia, gli Snapshot possono continuare a essere gestiti come normali snapshot granulari del volume.
- ONTAP elimina automaticamente un gruppo di coerenza se tutti i volumi del gruppo vengono eliminati.

- L'eliminazione di un gruppo di coerenza principale comporta l'eliminazione di tutti i gruppi di coerenza secondari associati.
- Se si utilizza una versione di ONTAP compresa tra 9.10.1 e 9.12.0, i volumi possono essere rimossi da un gruppo di coerenza solo se il volume stesso viene cancellato, nel qual caso il volume viene automaticamente rimosso dal gruppo di coerenza. A partire da ONTAP 9.12.1, è possibile rimuovere i volumi da un gruppo di coerenza senza eliminare tale gruppo. Per ulteriori informazioni su questo processo, fare riferimento a. Modificare un gruppo di coerenza.

Esempio 7. Fasi

System Manager

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera eliminare.
3. Accanto al nome del gruppo di coerenza, selezionare ⋮ Quindi **Elimina**.

CLI

A partire da ONTAP 9.14.1, è possibile eliminare un gruppo di coerenza utilizzando l'interfaccia CLI.

Eliminare un gruppo di coerenza

1. Eliminare il gruppo di coerenza:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

Continuità aziendale di SnapMirror

Panoramica di SnapMirror Business Continuity

SnapMirror Business Continuity (SM-BC), noto anche come SnapMirror Active Sync, permette ai servizi di business di continuare a funzionare anche attraverso un guasto completo del sito, supportando le applicazioni per il failover in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SM-BC non sono richiesti né interventi manuali né script aggiuntivi.

SM-BC è disponibile a partire da ONTAP 9.8. SM-BC è supportato su cluster AFF o cluster ASA (All-Flash SAN Array), in cui i cluster primari e secondari possono essere AFF o ASA. SM-BC protegge le applicazioni con LUN iSCSI o FCP.

Benefici

SM-BC offre i seguenti vantaggi:

- Disponibilità continua per applicazioni business-critical
- Possibilità di ospitare applicazioni critiche in modo alternato dal sito primario e secondario
- Gestione semplificata delle applicazioni mediante gruppi di coerenza per una coerenza dipendente dell'ordine di scrittura
- Possibilità di testare il failover per ciascuna applicazione

- Creazione istantanea di cloni mirror senza impatto sulla disponibilità delle applicazioni
- A partire da ONTAP 9.11.1, SM-BC supporta SnapRestore a file singolo.
- A partire da ONTAP 9.14.1, SM-BC supporta Windows failover Clustering e. "Prenotazioni permanenti SCSI 3", migliorando l'alta disponibilità.

Casi di utilizzo

Implementazione dell'applicazione per RTO (Zero Recovery Time Object)

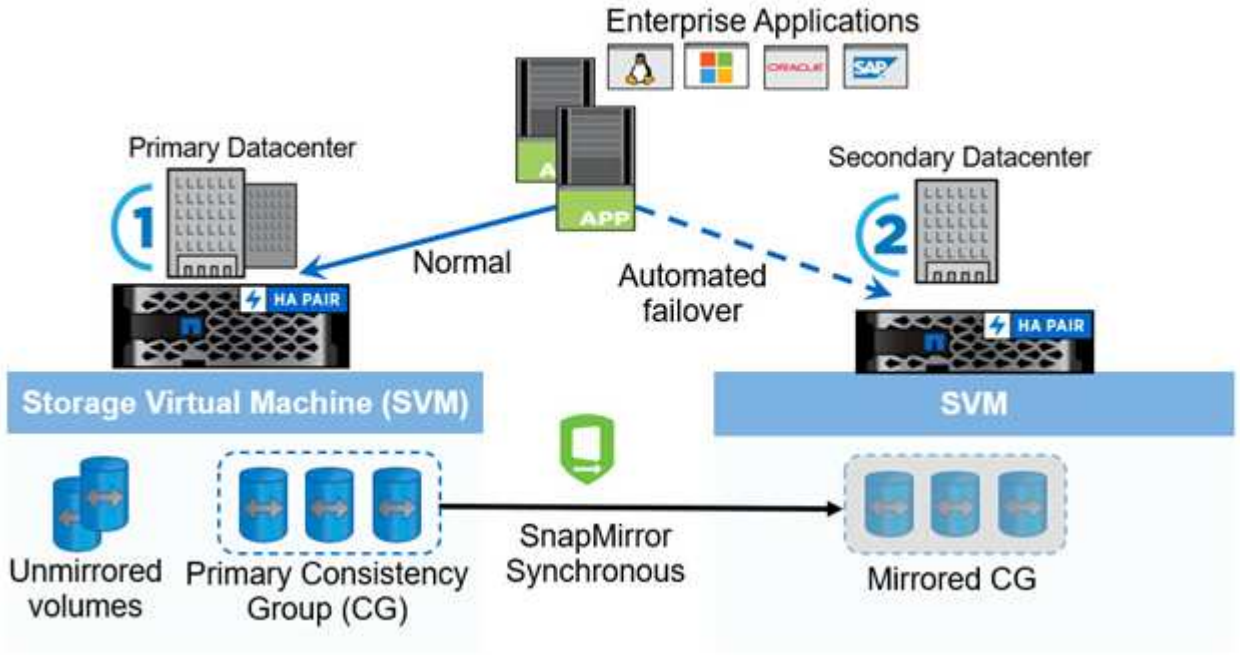
In un'implementazione SM-BC, si disporrà di un cluster primario e secondario. Un LUN nel cluster primario `1LP`) avrà un mirror (`L1s`) Sul secondario; entrambi i LUN condividono lo stesso ID seriale e vengono riportati come LUN di lettura/scrittura sull'host. Tuttavia, le operazioni di lettura e scrittura vengono servite solo al LUN primario, `1LP`. Any scrive nel mirror `L1S` sono serviti dal proxy.

Scenario di disastro

Con SM-BC, è possibile replicare in modo sincrono più volumi per un'applicazione tra siti in ubicazioni geograficamente distribuite. È possibile eseguire automaticamente il failover sulla copia secondaria in caso di interruzione del primario, consentendo così la business continuity per le applicazioni di primo livello.

Architettura

La figura seguente illustra il funzionamento della funzione di continuità aziendale di SnapMirror a un livello elevato.



Nella sezione uno del diagramma, un'applicazione viene implementata su una SVM nel data center primario. I volumi che sono stati aggiunti al gruppo di coerenza primario sono protetti con SM-BC e vengono mirrorati nel gruppo di coerenza secondario di un data center secondario. In caso di interruzione, i volumi nel gruppo di coerenza primario effettueranno il failover nel gruppo di coerenza mirrorato. I volumi non appartenenti a un gruppo di coerenza mirrorato non vengono serviti in caso di failover.

Ulteriori informazioni

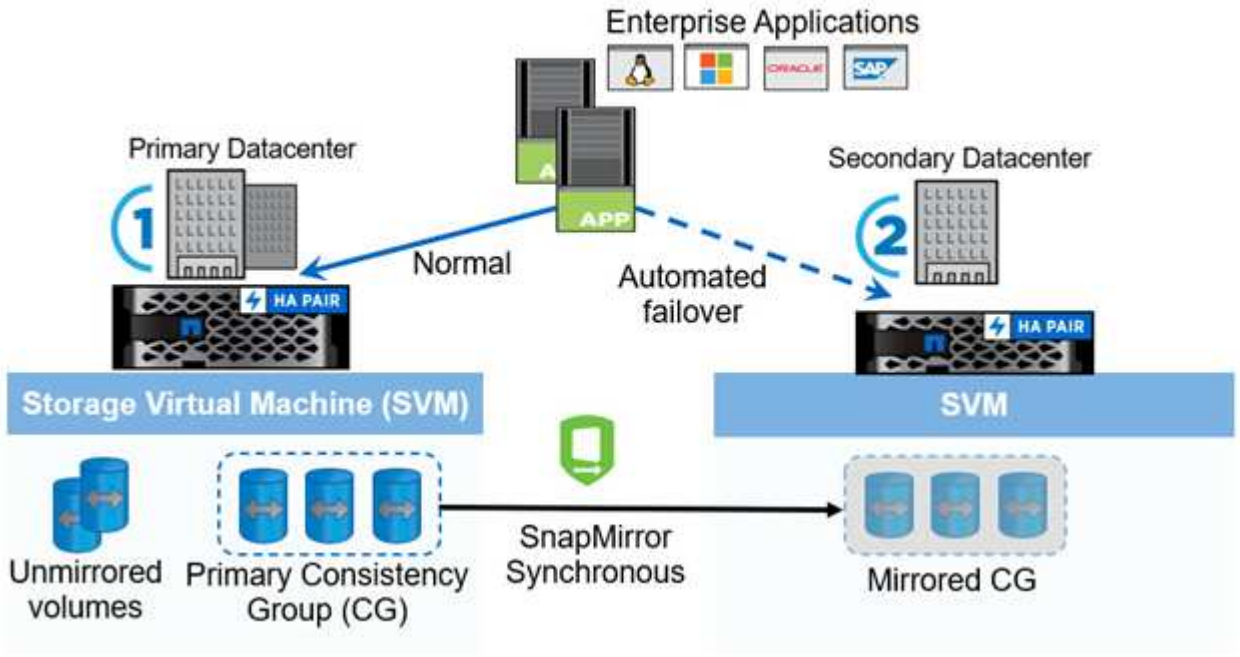
- "TR-4878: Business continuity SnapMirror"

Concetti chiave

La business continuity SnapMirror (SM-BC) utilizza funzionalità come i gruppi di coerenza e il mediatore ONTAP per garantire la replica e il servizio dei dati anche in caso di disastro. Durante la pianificazione dell'implementazione di SM-BC, è importante comprendere i concetti essenziali di SM-BC e della relativa architettura.

Architettura

La figura seguente illustra una panoramica di alto livello di un'implementazione SM-BC.



Il diagramma mostra un'applicazione aziendale ospitata su una VM di storage (SVM) nel data center primario. La SVM contiene cinque volumi, tre dei quali fanno parte di un gruppo di coerenza. I tre volumi nel gruppo di coerenza vengono mirrorati in un data center secondario. In circostanze normali, tutte le operazioni di scrittura vengono eseguite sul data center primario; in effetti, questo data center funge da origine per le operazioni di i/o, mentre il data center secondario funge da destinazione.

In caso di disastro nel data center primario, il mediatore ONTAP indirizzerà il data center secondario a fungere da principale, servendo tutte le operazioni di i/O. Verranno serviti solo i volumi di cui è stato eseguito il mirroring nel gruppo di coerenza. Qualsiasi operazione relativa agli altri due volumi sulla SVM sarà interessata dall'evento di disastro.

Concetti essenziali

La comprensione dei seguenti termini ti aiuterà a implementare SM-BC.

Gruppo di coerenza

Un gruppo di coerenza è un insieme di volumi o LUN che forniscono una garanzia di coerenza dell'ordine di

scrittura per il carico di lavoro dell'applicazione che deve essere protetto per la business continuity. Un gruppo di coerenza garantisce che tutti i volumi di questo set di dati vengano disattivati e quindi sottoposti a snap nello stesso momento, fornendo un punto di ripristino coerente con i dati tra i volumi per quel set di dati.

In SM-BC, creerai un gruppo di coerenza primario e secondario per la replica e la protezione dei dati. Il gruppo di coerenza secondario servirà i dati in caso di interruzione.

Per ulteriori informazioni sui gruppi di coerenza, vedere "Panoramica dei gruppi di coerenza".

Costituente

Un singolo volume o LUN che fa parte di un gruppo di coerenza, protetto dalla relazione SM-BC.

Mediatore ONTAP

I mediatori ONTAP monitorano i due cluster ONTAP e orchestrano il failover in caso di guasto del sistema di storage primario. Con il mediatore ONTAP, l'applicazione si ricollega automaticamente alle risorse del sistema di storage secondario.

Con le informazioni sullo stato di salute del mediatore ONTAP, i cluster possono distinguere tra guasto LIF intercluster e guasto del sito. Quando il sito non funziona, ONTAP Mediator trasmette on-demand le informazioni sullo stato di salute al cluster peer, facilitando il cluster peer al failover.

Scopri di più su "Mediatore ONTAP".

Failover pianificato

Un'operazione manuale per modificare i ruoli delle copie in una relazione SM-BC. I siti primari diventano i secondari, mentre i siti secondari diventano quelli primari.

Failover automatico non pianificato (AUFO)

Un'operazione automatica per eseguire un failover sulla copia mirror. L'operazione richiede l'assistenza di Mediator per rilevare che la copia principale non è disponibile.

Fuori sincronizzazione (OOS)

Quando l'i/o dell'applicazione non viene replicato nel sistema di storage secondario, viene segnalato come **fuori sincronizzazione**. Uno stato fuori sincronizzazione indica che i volumi secondari non sono sincronizzati con il primario (origine) e che la replica di SnapMirror non avviene.

Se lo stato mirror è `Snapmirrored`, indica un errore di trasferimento o un errore dovuto a un'operazione non supportata.

RPO zero

RPO è l'acronimo di Recovery Point Objective, ovvero la quantità di perdita di dati ritenuta accettabile in un determinato periodo di tempo. Zero RPO indica che non è accettabile alcuna perdita di dati.

RTO zero

RTO è l'acronimo di Recovery Time Objective (obiettivo tempo di ripristino), ovvero il tempo ritenuto accettabile per il ritorno di un'applicazione alle normali operazioni in seguito a un'interruzione, un guasto o un altro evento di perdita di dati. Zero RTO significa che non è accettabile alcun downtime.

Pianificare

Prerequisiti

Durante la pianificazione dell'implementazione di SnapMirror Business Continuity,

assicurarsi di aver soddisfatto i diversi requisiti di configurazione hardware, software e di sistema.

Hardware

- Sono supportati solo cluster ha a due nodi
- Entrambi i cluster devono essere AFF (incluso AFF C-Series) o ASA (senza combinazione)

Software

- ONTAP 9.8 o versione successiva
- Mediatore ONTAP 1.2 o versione successiva
- Un server Linux o una macchina virtuale per il mediatore ONTAP che esegue una delle seguenti operazioni:

Versione del mediatore ONTAP	Versioni Linux supportate
1,7	• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1.6	• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2 • Rocky Linux 8 e 9
1.5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Licensing

- La licenza SnapMirror Synchronous (SM-S) deve essere applicata a entrambi i cluster
- La licenza SnapMirror deve essere applicata su entrambi i cluster

> Se i sistemi storage ONTAP sono stati acquistati prima di giugno 2019, vedere "Chiavi di licenza master NetApp ONTAP" Per ottenere la licenza SM-S richiesta.

La licenza SnapMirror sincrona e SnapMirror è inclusa in "ONTAP uno".

Ambiente di rete

- Il tempo di round trip (RTT) di latenza tra cluster deve essere inferiore a 10 millisecondi.
- Le prenotazioni persistenti SCSI-3 sono **non** supportate con SM-BC .

Protocolli supportati

- Sono supportati solo i protocolli SAN (non NFS/SMB).
- Sono supportati solo i protocolli Fibre Channel e iSCSI.
- L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. IPSpace personalizzato non supportato.

Sicurezza NTFS

Lo stile di sicurezza NTFS **non** è supportato sui volumi SM-BC.

Mediatore ONTAP

- Il provisioning del mediatore ONTAP viene eseguito esternamente e collegato a ONTAP per il failover trasparente delle applicazioni.
- Per essere pienamente funzionale e per abilitare il failover automatico non pianificato, il mediatore ONTAP esterno deve essere fornito e configurato con cluster ONTAP.
- Il supporto ONTAP deve essere installato in un terzo dominio di errore, separato dai due cluster ONTAP.
- Quando si installa il mediatore ONTAP, è necessario sostituire il certificato autofirmato con un certificato valido firmato da una CA mainstream affidabile.
- Per ulteriori informazioni sul mediatore ONTAP, vedere "Preparare l'installazione del servizio ONTAP Mediator".

Volumi di destinazione in lettura/scrittura

- Le relazioni SM-BC non sono supportate sui volumi di destinazione in lettura/scrittura. Prima di poter utilizzare un volume di lettura/scrittura, è necessario convertirlo in un volume DP creando una relazione SnapMirror a livello di volume ed eliminando la relazione. Per ulteriori informazioni, vedere "Conversione delle relazioni esistenti in relazioni SM-BC"

Grandi LUN e grandi volumi

Il supporto per LUN di grandi dimensioni e grandi volumi (superiori a 100 TB) dipende dalla versione di ONTAP in uso e dalla piattaforma.

ONTAP 9.12.1P2 e versioni successive

- Per ONTAP 9.12.1 P2 e versioni successive, SMBC supporta LUN di grandi dimensioni e volumi superiori a 100 TB su ASA e AFF (inclusa la serie C).

> Per le versioni ONTAP 9.12.1P2 e successive, è necessario assicurarsi che i cluster primario e secondario siano All-Flash SAN Array o All Flash Array e che abbiano installato ONTAP 9.12.1 P2 o versione successiva. Se il cluster secondario esegue una versione precedente a ONTAP 9.12.1P2 o se il tipo di array non è lo stesso del cluster primario, la relazione sincrona può uscire dalla sincronizzazione se il volume primario supera i 100 TB.

ONTAP 9.8 - 9.12.1P1

- Per le release ONTAP tra ONTAP 9,8 e 9.12.1 P1 (incluse), LUN di grandi dimensioni e volumi maggiori di 100TB TB sono supportati solo sugli array SAN all-flash.

> Per le release ONTAP tra ONTAP 9,8 e 9.12.1 P2, è necessario verificare che i cluster primario e secondario siano array SAN all-flash e che abbiano installato ONTAP 9,8 o versione successiva. Se il cluster secondario esegue una versione precedente a ONTAP 9,8 o se non si tratta di un array All-Flash SAN, la relazione sincrona può disattivarsi se il volume primario cresce oltre 100 TB.

Ulteriori informazioni

- "Hardware Universe"
- "Panoramica del mediatore ONTAP"

Configurazioni e funzionalità supportate

La Business Continuity di SnapMirror è compatibile con numerosi sistemi operativi e altre funzionalità di ONTAP. Scopri i dettagli e le configurazioni consigliate.

Configurazioni supportate

SM-BC è supportato da numerosi sistemi operativi, tra cui:

- AIX (a partire da ONTAP 9.11.1)
- HP-UX (a partire da ONTAP 9.10.1)
- Solaris 11.4 (a partire da ONTAP 9.10.1)

AIX

A partire da ONTAP 9.11.1, AIX è supportato con SM-BC. Con una configurazione AIX, il cluster primario è il cluster "attivo".

In una configurazione AIX, i failover sono disruptive. Con ogni failover, sarà necessario eseguire una nuova scansione sull'host per riprendere le operazioni di i/O.

Per configurare l'host AIX con SM-BC, consultare l'articolo della Knowledge base "Come configurare un host AIX per SnapMirror Business Continuity (SM-BC)".

HP-UX

A partire da ONTAP 9.10.1, è supportato SM-BC per HP-UX.

Limitazioni con HP-UX

Un evento di failover automatico non pianificato (AUFO) sul cluster master isolato può essere causato da un guasto a due eventi quando viene persa la connessione tra il cluster primario e quello secondario e viene persa anche la connessione tra il cluster primario e il mediatore. Questo è considerato un evento raro, a differenza di altri eventi AUFO.

- In questo scenario, potrebbero essere necessari più di 120 secondi per il ripristino dell'i/o sull'host HP-UX. A seconda delle applicazioni in esecuzione, questo potrebbe non causare interruzioni i/o o messaggi di errore.
- Per risolvere il problema, è necessario riavviare le applicazioni sull'host HP-UX che hanno una tolleranza di interruzione inferiore a 120 secondi.

Consigli per l'impostazione degli host Solaris

A partire da ONTAP 9.10.1, SM-BC supporta Solaris 11.4.

Per garantire che le applicazioni client Solaris non siano disgregative quando si verifica uno switchover di failover del sito non pianificato in un ambiente SM-BC, modificare le impostazioni predefinite del sistema operativo Solaris. Per configurare Solaris con le impostazioni consigliate, consultare l'articolo della Knowledge base "Impostazioni consigliate per il supporto degli host Solaris nella configurazione di SnapMirror Business Continuity (SM-BC)".

Clustering di failover Windows

A partire da ONTAP 9.14.1, il clustering di failover Windows è supportato con SM-BC. Per ulteriori informazioni, vedere "TR-4878: Business continuity SnapMirror".

Integrazioni ONTAP

SM-BC offre supporto per altre funzionalità di ONTAP, tra cui:

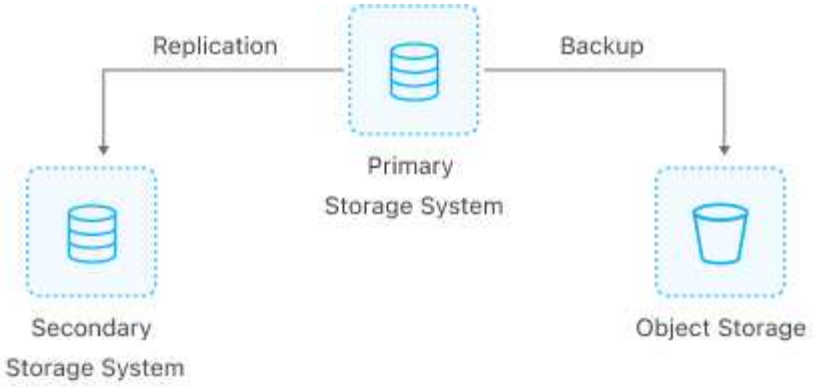
- Configurazioni fan-out
- Copia NDMP (a partire da ONTAP 9.13.1)
- Ripristino parziale dei file (a partire da ONTAP 9.12.1)

FabricPool

SM-BC supporta i volumi di origine e di destinazione sugli aggregati FabricPool con la policy di tiering None (Nessuno), Snapshot (Snapshot) o Auto (automatico). SM-S SM-BC non supporta gli aggregati FabricPool che utilizzano una policy di tiering di tutti.

Configurazioni fan-out

In una configurazioni fan-out, È possibile eseguire il mirroring del volume di origine su un endpoint di destinazione SM-BC e su una o più relazioni SnapMirror asincrone.



SM-BC supporta configurazioni fan-out con `MirrorAllSnapshots` E, a partire da ONTAP 9.11.1, il `MirrorAndVault` policy. Le configurazioni fan-out non sono supportate in SM-BC con `XDPDefault` policy.

Se si verifica un failover sulla destinazione SM-BC in una configurazione fan-out, è necessario manualmente ripristinare la protezione nella configurazione fan-out.

Ripristino NDMP

A partire da ONTAP 9.13.1, è possibile utilizzare NDMP per copiare e ripristinare i dati con SM-BC. L'utilizzo di NDMP consente di spostare i dati nell'origine SM-BC per completare un ripristino senza interrompere la protezione. Questo è particolarmente utile nelle configurazioni fan-out.

Per ulteriori informazioni su questo processo, vedere Trasferire i dati utilizzando la copia ndmp.

Ripristino parziale del file

A partire da ONTAP 9.12.1, il ripristino parziale del LUN è supportato per i volumi SM-BC. Per informazioni su questo processo, fare riferimento a. "Ripristinare parte di un file da una copia Snapshot".

Limiti a oggetti per la business continuity di SnapMirror

Durante la preparazione all'utilizzo e alla gestione di SnapMirror Business Continuity, tenere presenti le seguenti limitazioni.

Gruppi di coerenza in un cluster

I limiti dei gruppi di coerenza per un cluster con SM-BC vengono calcolati in base alle relazioni e dipendono dalla versione di ONTAP utilizzata. I limiti sono indipendenti dalla piattaforma.

Versione di ONTAP	Numero massimo di relazioni
ONTAP 9.8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1 e versioni successive	50

Volumi per gruppo di coerenza

Il numero massimo di volumi per gruppo di coerenza con SM-BC è indipendente dalla piattaforma.

Versione di ONTAP	Numero massimo di volumi supportati in una relazione di gruppo di coerenza
ONTAP 9.8-9.9.1	12
ONTAP 9.10.1 e versioni successive	16

Volumi

I limiti di volume in SM-BC vengono calcolati in base al numero di endpoint, non al numero di relazioni. Un gruppo di coerenza con 12 volumi contribuisce a 12 endpoint sul cluster primario e secondario. Le relazioni sincroni di SM-BC e SnapMirror contribuiscono al numero totale di endpoint.

Nella tabella seguente sono inclusi gli endpoint massimi per piattaforma.

S. No	Piattaforma	Endpoint per ha per SM-BC			Endpoint di sincronizzazione generale e SM-BC per ha		
		ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 e versioni successive	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 e versioni successive
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

Limiti degli oggetti SAN

I limiti degli oggetti SAN sono inclusi nella tabella seguente. I limiti si applicano indipendentemente dalla piattaforma.

Oggetto in una relazione SM-BC	Conta
LUN per volume	256
Mappe LUN per nodo	• 4096 (ONTAP 9,10 e versioni successive) • 2048 (ONTAP 9.9.1 e versioni precedenti)
Mappe LUN per cluster	• 8192 (ONTAP 9,10 e versioni successive) • 4096 (ONTAP 9.9.1 e versioni precedenti)
LIF per SVM (con almeno un volume in relazione SM-BC)	256
LIF tra cluster per nodo	4
LIF tra cluster per cluster	8

Informazioni correlate

- "Hardware Universe"
- "Limiti del gruppo di coerenza"

Installazione e configurazione

Configurare il mediatore ONTAP e i cluster per la business continuity SnapMirror

SnapMirror Business Continuity (SM-BC) utilizza cluster peered per garantire la disponibilità dei dati in caso di failover. Il mediatore ONTAP è una risorsa chiave che garantisce la business continuity, monitorando lo stato di salute di ogni cluster. Per configurare SM-BC, è necessario prima installare il mediatore ONTAP e assicurarsi che i cluster primari e secondari siano configurati correttamente.

Una volta installato il mediatore ONTAP e configurato i cluster, è necessario [initialize-the-ontap-mediator] Il mediatore ONTAP da utilizzare con SM-BC. Devi quindi Creare, inizializzare e mappare il gruppo di coerenza per SM-BC

Mediatore ONTAP

Il mediatore ONTAP stabilisce un quorum per i cluster ONTAP in una relazione SM-BC. Coordina il failover automatico quando viene rilevato un guasto, determinando quale cluster agisce come principale e garantendo che i dati vengano serviti da e verso la destinazione corretta.

Prerequisiti per il mediatore ONTAP

- Il mediatore ONTAP include un proprio set di prerequisiti. È necessario soddisfare questi prerequisiti prima di installare il mediatore.

  Per ulteriori informazioni, vedere "Preparare l'installazione del servizio ONTAP Mediator".

- Per impostazione predefinita, il supporto ONTAP fornisce il servizio tramite la porta TCP 31784. Assicurarsi che la porta 31784 sia aperta e disponibile tra i cluster ONTAP e il mediatore.

Installare il mediatore ONTAP e confermare la configurazione del cluster

Procedere con ciascuna delle seguenti operazioni. Per ogni fase, è necessario confermare che la configurazione specifica è stata eseguita. Utilizza il link incluso dopo ogni passaggio per ottenere ulteriori informazioni in base alle necessità.

Fasi

1. Installare il servizio ONTAP Mediator prima di assicurarsi che i cluster di origine e di destinazione siano configurati correttamente.

   Preparazione all'installazione o all'aggiornamento del servizio ONTAP Mediator

2. Verificare che esista una relazione di peering del cluster tra i cluster.

   > L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. Un IPSpace personalizzato non è supportato.

   Configurare le relazioni peer

3. Verificare che le VM di storage siano create su ciascun cluster.

   Creazione di una SVM

4. Verificare l'esistenza di una relazione peer tra le VM di storage su ciascun cluster.

Creazione di una relazione di peering SVM

5. Verificare che i volumi esistano per le LUN.

   Creazione di un volume

6. Verificare che sia stata creata almeno una LIF SAN su ciascun nodo del cluster.

   "Considerazioni per le LIF in un ambiente SAN cluster"

   "Creazione di una LIF"

7. Verificare che i LUN necessari siano creati e mappati a un igroup, che viene utilizzato per mappare i LUN all'iniziatore sull'host dell'applicazione.

   Creare LUN e mappare igroups

8. Eseguire nuovamente la scansione dell'host dell'applicazione per rilevare eventuali nuove LUN.

Inizializzare il mediatore ONTAP per SM-BC

Una volta installato il mediatore ONTAP e confermata la configurazione del cluster, è necessario inizializzare il mediatore ONTAP per il monitoraggio del cluster. È possibile inizializzare il supporto ONTAP utilizzando Gestione di sistema o l'interfaccia utente di ONTAP.

System Manager

Con Gestione di sistema, è possibile configurare il server ONTAP Mediator per il failover automatico. È inoltre possibile sostituire SSL e CA autofirmati con certificati SSL e CA validati di terze parti, se non è già stato fatto.

Fasi

1. Accedere a **protezione > Panoramica > Mediator > Configura**.
2. Selezionare **Aggiungi** e immettere le seguenti informazioni sul server ONTAP Mediator:
   - Indirizzo IPv4
   - Nome utente
   - Password
   - Certificato

CLI

È possibile inizializzare il mediatore ONTAP dal cluster primario o secondario utilizzando l'interfaccia CLI di ONTAP. Quando si invia il `mediator add` Su un cluster, il mediatore ONTAP viene aggiunto automaticamente sull'altro cluster.

Fasi

1. Inizializzare Mediator su uno dei cluster:

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   Esempio

   ```
   cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
   -peer-cluster cluster2 -username mediatoradmin
   Notice: Enter the mediator password.

   Enter the password: ******
   Enter the password again: ******
   ```

2. Controllare lo stato della configurazione del Mediator:

   ```
   snapmirror mediator show
   ```

   ```
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   192.168.10.1     cluster-2        connected         true
   ```

   `Quorum Status` Indica se le relazioni del gruppo di coerenza SnapMirror sono sincronizzate con il mediatore; uno stato di `true` indica che la sincronizzazione è stata eseguita correttamente.

Proteggere con SnapMirror Business Continuity

La configurazione della protezione mediante la business continuity di SnapMirror implica la selezione delle LUN nel cluster di origine di ONTAP e l'aggiunta di tali LUN a un gruppo di coerenza.

Prima di iniziare

- È necessario disporre di un "Licenza SnapMirror Synchronous".
- È necessario essere un amministratore di cluster o di macchine virtuali per lo storage.
- Tutti i volumi costituenti di un gruppo di coerenza devono trovarsi in una singola VM di storage (SVM).
  - Le LUN possono risiedere su volumi diversi.
- Il cluster di origine e di destinazione non può essere lo stesso.
- Non è possibile stabilire relazioni di gruppo di coerenza SM-BC tra cluster ASA e cluster non ASA.
- L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. IPSpace personalizzato non supportato.
- Il nome del gruppo di coerenza deve essere univoco.
- I volumi sul cluster secondario (di destinazione) devono essere di tipo DP.
- Le SVM primarie e secondarie devono essere in relazione peered.

Fasi

È possibile configurare un gruppo di coerenza utilizzando l'interfaccia utente di ONTAP o Gestione sistema.

A partire da ONTAP 9.10.1, ONTAP offre un endpoint di gruppo coerente e un menu in Gestione sistema, che offre utility di gestione aggiuntive. Se si utilizza ONTAP 9.10.1 o versione successiva, vedere "Configurare un gruppo di coerenza" quindi "configurare la protezione" Per creare una relazione SM-BC.

System Manager

1. Sul cluster primario, accedere a **protezione > Panoramica > Proteggi per la business continuity > Proteggi LUN**.
2. Selezionare i LUN che si desidera proteggere e aggiungerli a un gruppo di protezione.
3. Selezionare il cluster di destinazione e SVM.
4. Per impostazione predefinita, l'opzione **Inizializza relazione** è selezionata. Fare clic su **Save** (Salva) per iniziare la protezione.
5. Accedere a **Dashboard > Performance** per verificare l'attività IOPS per le LUN.
6. Nel cluster di destinazione, utilizzare System Manager per verificare che la protezione per la relazione di business continuity sia sincronizzata: **Protezione > relazioni**.

CLI

1. Creare una relazione di gruppo di coerenza dal cluster di destinazione.
   `destination::> snapmirror create -source-path *source-path* -destination-path *destination-path* -cg-item -mappings *volume-path* -policy *policy-name*

   È possibile mappare fino a 12 volumi costitutivi utilizzando `cg-item-mappings` sul `snapmirror create` comando.

   Nell'esempio seguente vengono creati due gruppi di coerenza: `cg_src_ on the source with` `vol1` e. `vol2` e un gruppo di coerenza di destinazione mirrorato, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. Dal cluster di destinazione, inizializzare il gruppo di coerenza.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Verificare che l'operazione di inizializzazione sia stata completata correttamente. Lo stato deve essere `InSync`.

   ```
   snapmirror show
   ```

4. Su ciascun cluster, creare un igroup in modo da poter mappare le LUN all'iniziatore sull'host dell'applicazione.
   `lun igroup create -igroup *name* -protocol *fcp|iscsi* -ostype *os* -initiator *initiator_name*`
5. Su ciascun cluster, mappare i LUN all'igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Verificare che la mappatura LUN sia stata completata correttamente con `lun map` comando. Quindi, è possibile scoprire i nuovi LUN sull'host dell'applicazione.

Gestire SM-BC e proteggere i dati

Creare una copia Snapshot comune

Oltre alle operazioni di copia Snapshot regolarmente pianificate, è possibile creare manualmente un file comune "Copia Snapshot" Tra i volumi nel gruppo di coerenza SnapMirror primario e i volumi nel gruppo di coerenza SnapMirror secondario.

A proposito di questa attività

- In ONTAP 9.8, l'intervallo di creazione dello snapshot pianificato è di un'ora.

  A partire da ONTAP 9.9.1, l'intervallo è di 12 ore.

Prima di iniziare

- La relazione del gruppo SnapMirror deve essere sincronizzata.

Fasi

1. Creare una copia Snapshot comune:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Monitorare l'avanzamento dell'aggiornamento:

   ```
   destination::>snapmirror show -fields -newest-snapshot
   ```

Eseguire un failover pianificato

In un failover pianificato, è possibile cambiare i ruoli dei cluster primario e secondario, in modo che il cluster secondario prenda il controllo dal cluster primario. Durante un failover, il cluster secondario elabora le richieste di input e output in locale senza interrompere le operazioni del client.

È possibile eseguire un failover pianificato per verificare lo stato della configurazione di disaster recovery o per eseguire la manutenzione sul cluster primario.

A proposito di questa attività

L'amministratore del cluster secondario avvia un failover pianificato. L'operazione richiede la commutazione dei ruoli primario e secondario in modo che il cluster secondario prenda il posto del primario. Il nuovo cluster primario può quindi iniziare a elaborare le richieste di input e output localmente senza interrompere le operazioni del client.

Prima di iniziare

- La relazione SM-BC deve essere sincronizzata.
- Non è possibile avviare un failover pianificato quando è in corso un'operazione senza interruzioni. Le operazioni senza interruzioni includono spostamenti di volumi, trasferimenti di aggregazioni e failover dello storage.
- Il mediatore ONTAP deve essere configurato, connesso e in quorum.

Fasi

È possibile eseguire un failover pianificato utilizzando l'interfaccia utente di ONTAP o Gestione di sistema.

System Manager

1. In System Manager, selezionare **protezione > Panoramica > Relazioni**.
2. Identificare la relazione SM-BC che si desidera eseguire il failover. Accanto al nome, selezionare … Accanto al nome della relazione, quindi selezionare **failover**.
3. Per monitorare lo stato del failover, utilizzare `snapmirror failover show` Nella CLI di ONTAP.

CLI

1. Dal cluster di destinazione, avviare l'operazione di failover:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Monitorare l'avanzamento del failover:

   ```
   destination::>snapmirror failover show
   ```

3. Una volta completata l'operazione di failover, è possibile monitorare lo stato della relazione di protezione di Synchronous SnapMirror dalla destinazione:

   ```
   destination::>snapmirror show
   ```

Ripristino da operazioni di failover automatiche non pianificate

Un'operazione di failover automatico non pianificato (AUFO) si verifica quando il cluster primario è inattivo o isolato. Il mediatore ONTAP rileva quando si verifica un failover ed esegue un failover automatico non pianificato sul cluster secondario. Il cluster secondario viene convertito nel cluster primario e inizia a servire i client. Questa operazione viene eseguita solo con l'assistenza del mediatore ONTAP.

> Dopo il failover automatico non pianificato, è importante eseguire nuovamente la scansione dei percorsi i/o del LUN host in modo che non vi sia alcuna perdita dei percorsi i/O.

Ristabilire la relazione di protezione dopo un failover non pianificato

È possibile ristabilire la relazione di protezione utilizzando Gestione di sistema o l'interfaccia utente di ONTAP.

System Manager

Fasi

1. Accedere a **protezione > Relazioni** e attendere che lo stato della relazione mostri "InSync".
2. Per riprendere le operazioni sul cluster di origine, fare clic su ⋮ E selezionare **failover**.

CLI

È possibile monitorare lo stato del failover automatico non pianificato utilizzando `snapmirror failover show` comando.

Ad esempio:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Fare riferimento a. "Riferimento EMS" per informazioni sui messaggi di evento e sulle azioni correttive.

Riprendere la protezione in una configurazione fan-out dopo il failover

In caso di failover sul cluster secondario nella relazione SM-BC, la destinazione asincrona di SnapMirror diventa malsana. È necessario ripristinare manualmente la protezione eliminando e ricreando la relazione con l'endpoint asincrono di SnapMirror.

Fasi

1. Verificare che il failover sia stato completato correttamente:
   `snapmirror failover show`
2. Nell'endpoint SnapMirror asincrono, eliminare l'endpoint fan-out:
   `snapmirror delete -destination-path` *`destination_path`*
3. Sul terzo sito, creare relazioni SnapMirror asincrone tra il nuovo volume primario SM-BC e il volume di destinazione fan-out asincrono:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Risincronizzare la relazione:
   `snapmirror resync -destination-path` *`destination_path`*
5. Verificare lo stato e la salute della relazione:
   `snapmirror show`

Monitorare le operazioni di Business Continuity di SnapMirror

È possibile monitorare le seguenti operazioni di Business Continuity SnapMirror (SM-BC) per garantire lo stato di salute della configurazione SM-BC:

- Mediatore ONTAP
- Operazioni di failover pianificate
- Operazioni di failover automatiche non pianificate
- Disponibilità SM-BC

Mediatore ONTAP

Durante le normali operazioni, lo stato del mediatore ONTAP deve essere connesso. Se si trova in qualsiasi altro stato, potrebbe essere presente una condizione di errore. È possibile rivedere "Messaggi EMS (Event Management System)" per determinare l'errore e le azioni correttive appropriate.

Operazioni di failover pianificate

È possibile monitorare lo stato e l'avanzamento di un'operazione di failover pianificata utilizzando `snapmirror failover show` comando. Ad esempio:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Una volta completata l'operazione di failover, è possibile monitorare lo stato di protezione di Synchronous SnapMirror dal nuovo cluster di destinazione. Ad esempio:

```
ClusterA::> snapmirror show
```

Fare riferimento a. "Riferimento EMS" per informazioni sui messaggi di evento e sulle azioni correttive.

Operazioni di failover automatiche non pianificate

Durante un failover automatico non pianificato, è possibile monitorare lo stato dell'operazione utilizzando `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Fare riferimento a. "Riferimento EMS" per informazioni sui messaggi di evento e sulle azioni correttive.

Disponibilità SM-BC

È possibile verificare la disponibilità della relazione SM-BC utilizzando una serie di comandi, sul cluster primario, sul cluster secondario o su entrambi.

I comandi utilizzati includono `snapmirror mediator show` sul cluster primario e secondario per controllare lo stato di connessione e quorum, il `snapmirror show` e il `volume show` comando. Ad esempio:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored InSync    -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false           true                      No-consensus
```

Aggiungere o rimuovere volumi a un gruppo di coerenza

Con il variare dei requisiti dei carichi di lavoro delle applicazioni, potrebbe essere necessario aggiungere o rimuovere volumi da un gruppo di coerenza per garantire la continuità del business. Il processo di aggiunta e rimozione di volumi in una relazione SM-BC attiva dipende dalla versione di ONTAP in uso.

Nella maggior parte dei casi, si tratta di un processo di interruzione che richiede di interrompere la relazione SnapMirror, modificare il gruppo di coerenza e riprendere la protezione. A partire da ONTAP 9.13.1, l'aggiunta di volumi a un gruppo di coerenza con una relazione SM-BC attiva è un'operazione senza interruzioni.

A proposito di questa attività

- In ONTAP dalla versione 9.8 alla 9.9.1, è possibile aggiungere o rimuovere volumi a un gruppo di coerenza utilizzando l'interfaccia utente di ONTAP.
- A partire da ONTAP 9.10.1, si consiglia di eseguire la gestione "gruppi di coerenza" Tramite Gestore di sistema o con l'API REST di ONTAP.

  Se si desidera modificare la composizione del gruppo di coerenza aggiungendo o rimuovendo un volume, è necessario prima eliminare la relazione originale e quindi creare nuovamente il gruppo di coerenza con la nuova composizione.

- A partire da ONTAP 9.13.1, è possibile aggiungere senza interruzioni volumi a un gruppo di coerenza con una relazione SM-BC attiva dall'origine o dalla destinazione.

  La rimozione dei volumi è un'operazione di interruzione. Prima di procedere con la rimozione dei volumi, è necessario interrompere la relazione di SnapMirror.

ONTAP 9.8-9.13.0

Prima di iniziare

- Non è possibile iniziare a modificare il gruppo di coerenza mentre si trova in `InSync` stato.
- Il volume di destinazione deve essere di tipo DP.
- Il nuovo volume aggiunto per espandere il gruppo di coerenza deve disporre di una coppia di copie Snapshot comuni tra i volumi di origine e di destinazione.

Fasi

Gli esempi illustrati in due mappature di volumi: `vol_src1` ←→ `vol_dst1` e. `vol_src2` ←→ `vol_dst2`, in una relazione di gruppo di coerenza tra i punti finali `vs1_src:/cg/cg_src` e. `vs1_dst:/cg/cg_dst`.

1. Sui cluster di origine e di destinazione, verificare la presenza di un'istantanea comune tra i cluster di origine e di destinazione con il comando `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Se non esiste una copia Snapshot comune, creare e inizializzare una relazione SnapMirror di FlexVol:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Eliminare la relazione del gruppo di coerenza:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
   ```

4. Rilasciare la relazione SnapMirror di origine e conservare le copie Snapshot comuni:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Annullare la mappatura dei LUN ed eliminare la relazione esistente del gruppo di coerenza:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > I LUN di destinazione non sono mappati, mentre i LUN sulla copia primaria continuano a servire l'i/o host

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Se si utilizza ONTAP da 9.10.1 a 9.13.0,** eliminare e ricreare il gruppo di coerenza sull'origine con la

composizione corretta. Seguire la procedura descritta in Eliminare un gruppo di coerenza e poi Configurare un singolo gruppo di coerenza. In ONTAP 9.10.1 e versioni successive, è necessario eseguire le operazioni di eliminazione e creazione in Gestore di sistema o con l'API REST di ONTAP; non esiste alcuna procedura CLI.

Se si utilizza ONTAP 9.8, 9.0 o 9.9.1, passare alla fase successiva.

7. Creare il nuovo gruppo di coerenza sulla destinazione con la nuova composizione:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Risincronizzare la relazione del gruppo di coerenza RTO zero per assicurarsi che sia sincronizzata:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Rimappare i LUN non mappati nella fase 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

ONTAP 9.13.1 e versioni successive

A partire da ONTAP 9.13.1, è possibile aggiungere volumi senza interruzioni a un gruppo di coerenza con una relazione SM-BC attiva. SM-BC supporta l'aggiunta di volumi sia dall'origine che dalla destinazione.

Per ulteriori informazioni sull'aggiunta di volumi dal gruppo di coerenza di origine, vedere Modificare un gruppo di coerenza.

Aggiungere un volume dal cluster di destinazione

1. Nel cluster di destinazione, selezionare **protezione** > **relazioni**.
2. Individuare la relazione SM-BC a cui si desidera aggiungere volumi. Selezionare ⋮ Quindi **espandere**.
3. Selezionare le relazioni dei volumi i cui volumi devono essere aggiunti al gruppo di coerenza
4. Selezionare **Espandi**.

Convertire le relazioni esistenti in relazioni SM-BC

Se si dispone di una relazione SnapMirror sincrona esistente tra un cluster di origine e di destinazione, è possibile convertirla in una relazione SM-BC. Ciò consente di associare i volumi mirrorati a un gruppo di coerenza, garantendo zero RPO in un carico di lavoro multi-volume. Inoltre, è possibile conservare le snapshot SnapMirror esistenti se è necessario ripristinarle in un momento specifico prima di stabilire la relazione SM-BC.

Prima di iniziare

- Deve esistere una relazione SnapMirror sincrona RPO zero tra il cluster primario e secondario.
- Prima di poter creare la relazione SnapMirror zero RTO, è necessario rimuovere la mappatura di tutti i LUN del volume di destinazione.

- SM-BC supporta solo i protocolli SAN (non NFS/CIFS). Assicurarsi che nessun componente del gruppo di coerenza sia montato per l'accesso NAS.

A proposito di questa attività

- È necessario essere un amministratore di cluster e SVM sui cluster primario e secondario.
- Non è possibile convertire zero RPO in zero RTO Sync modificando il criterio SnapMirror.
- Assicurarsi che i LUN siano dismappati prima di emettere `snapmirror create` comando.

  Se i LUN esistenti sul volume secondario sono mappati e l' `AutomatedFailover` il criterio è configurato, il `snapmirror create` genera un errore.

Fasi

1. Dal cluster secondario, eseguire un aggiornamento di SnapMirror sulla relazione esistente:

   ```
   destination::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verificare che l'aggiornamento di SnapMirror sia stato completato correttamente:

   ```
   destination::>snapmirror show
   ```

3. Interrompere ciascuna delle relazioni sincrone RPO zero:

   ```
   destination::>snapmirror quiesce -destination-path vs1_dst:vol1

   destination::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Eliminare ciascuna delle relazioni sincrone RPO zero:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol1

   destination::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Rilasciare la relazione SnapMirror di origine, conservando le copie Snapshot comuni:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Creare una relazione SnapMirror sincrona RTO zero di gruppo:

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination
   -path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Risincronizzare il gruppo di coerenza:

   ```
   destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

Aggiorna e ripristina ONTAP con SM-BC

A partire da ONTAP 9.8, SnapMirror Business Continuity (SM-BC) è supportato. L'aggiornamento e il ripristino del cluster ONTAP hanno implicazioni sulle relazioni SM-BC a seconda della versione di ONTAP a cui si esegue l'aggiornamento o il ripristino.

Aggiorna ONTAP con SM-BC

Per utilizzare SM-BC, tutti i nodi dei cluster di origine e destinazione devono eseguire ONTAP 9,8 o versioni successive.

Quando si aggiorna ONTAP con relazioni SM-BC attive, è necessario utilizzare Upgrade automatici e senza interruzioni (ANDU). L'utilizzo di ANDU garantisce che le relazioni SM-BC siano sincronizzate e integre durante il processo di aggiornamento.

Non ci sono passaggi di configurazione per preparare le implementazioni di SM-BC per gli aggiornamenti ONTAP. Tuttavia, prima e dopo l'aggiornamento, si consiglia di verificare che:

- Sincronizzazione delle relazioni SM-BC.
- Nel registro eventi non sono presenti errori correlati a SnapMirror.
- Il mediatore è online e sano da entrambi i cluster.
- Tutti gli host sono in grado di visualizzare correttamente tutti i percorsi per proteggere le LUN.

> Quando esegui l'upgrade dei cluster da ONTAP 9,8 o 9.9.1 a ONTAP 9.10.1 e versioni successive, ONTAP crea nuove funzionalità gruppi di coerenza Su cluster sia di origine che di destinazione per relazioni SM-BC che possono essere configurate usando System Manager.

> Il `snapmirror quiesce` e. `snampirror resume` I comandi non sono supportati con SM-BC.

Ripristinare ONTAP 9.9.1 da ONTAP 9.10.1

Per ripristinare le relazioni da 9.10.1 a 9.9.1, è necessario eliminare le relazioni SM-BC, seguite dall'istanza del gruppo di coerenza 9.10.1. I gruppi di coerenza con una relazione SM-BC attiva non possono essere cancellati. Tutti i volumi FlexVol che sono stati aggiornati alla versione 9.10.1 precedentemente associati a un altro smart container o a un'applicazione aziendale nel 9.9.1 o precedente non saranno più associati al revert. L'eliminazione dei gruppi di coerenza non elimina i volumi costituenti o le snapshot granulari del volume. Fare riferimento a. "Eliminare un gruppo di coerenza" Per ulteriori informazioni su questa attività in ONTAP 9.10.1 e versioni successive.

Ripristinare ONTAP 9.7 da ONTAP 9.8

> SM-BC non è supportato con cluster misti ONTAP 9.7 e ONTAP 9.8.

Quando si passa da ONTAP 9.8 a ONTAP 9.7, è necessario tenere presente quanto segue:

- Se il cluster ospita una destinazione SM-BC, il ripristino a ONTAP 9.7 non è consentito fino a quando la relazione non viene interrotta ed eliminata.
- Se il cluster ospita un'origine SM-BC, il ripristino di ONTAP 9.7 non è consentito fino al rilascio della relazione.
- Tutti i criteri di SnapMirror SM-BC personalizzati creati dall'utente devono essere cancellati prima di

tornare a ONTAP 9.7.

Per soddisfare questi requisiti, vedere "Rimuovere una configurazione SM-BC".

Fasi

1. Eseguire un controllo di revert da uno dei cluster nella relazione SM-BC:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   ```

   Esempio:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
      is Quiesced: snapmirror show
       Command to break off a data-protection volume: snapmirror break
       Command to break off a data-protection volume which is the
   destination
      of a SnapMirror relationship with a policy of type "vault":
   ```

```
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.8"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

Per informazioni sul ripristino dei cluster, vedere "Ripristina ONTAP".

Rimuovere una configurazione SM-BC

Se non si richiede più una protezione SnapMirror sincronizzata con RTO pari a zero, è possibile eliminare la relazione SM-BC.

A proposito di questa attività

- Prima di eliminare la relazione SM-BC, tutte le LUN nel cluster di destinazione devono essere dismappate.
- Una volta che i LUN sono stati dismappati e l'host è stato nuovamente scansionato, la destinazione SCSI notifica agli host che l'inventario LUN è stato modificato. Le LUN esistenti sui volumi secondari RTO zero cambiano per riflettere una nuova identità dopo l'eliminazione della relazione RTO zero. Gli host rilevano le LUN del volume secondario come nuove LUN che non hanno alcuna relazione con le LUN del volume di origine.
- I volumi secondari rimangono volumi DP dopo l'eliminazione della relazione. È possibile eseguire il `snapmirror break` comando per convertirli in lettura/scrittura.
- L'eliminazione della relazione non è consentita nello stato di failover quando la relazione non viene invertita.

Fasi

1. Dal cluster secondario, rimuovere la relazione del gruppo di coerenza SM-BC tra l'endpoint di origine e l'endpoint di destinazione:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. Dal cluster primario, rilasciare la relazione del gruppo di coerenza e le copie Snapshot create per la relazione:

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Eseguire una nuova scansione dell'host per aggiornare l'inventario del LUN.
4. A partire da ONTAP 9.10.1, l'eliminazione della relazione SnapMirror non elimina il gruppo di coerenza. Se si desidera eliminare il gruppo di coerenza, è necessario utilizzare Gestione sistema o l'API REST di ONTAP. Vedere Eliminare un gruppo di coerenza per ulteriori informazioni.

Rimuovere il mediatore ONTAP

Se si desidera rimuovere una configurazione di ONTAP Mediator esistente dai cluster ONTAP, è possibile farlo utilizzando `snapmirror mediator remove` comando.

Fasi

1. Rimuovi mediatore ONTAP:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
   cluster_xyz
   ```

Risolvere i problemi

L'operazione di eliminazione di SnapMirror non riesce nello stato di takover

Problema:

Quando ONTAP 9.9.1 viene installato in un cluster, eseguire `snapmirror delete` Il comando non riesce quando una relazione di gruppo di coerenza SM-BC è in stato di Takeover.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Soluzione

Quando i nodi in una relazione SM-BC sono in stato di Takeover, eseguire l'operazione di eliminazione e rilascio di SnapMirror con l'opzione "-force" impostata su true.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Errore durante la creazione di una relazione SnapMirror e l'inizializzazione del gruppo di coerenza

Problema:

La creazione della relazione SnapMirror e l'inizializzazione del gruppo di coerenza non riesce.

Soluzione:

Assicurarsi di non aver superato il limite di gruppi di coerenza per cluster. I limiti del gruppo di coerenza in SM-BC sono indipendenti dalla piattaforma e differiscono in base alla versione di ONTAP. Vedere "Ulteriori restrizioni e limitazioni" Per le limitazioni basate sulla versione di ONTAP.

Errore:

Se l'inizializzazione del gruppo di coerenza è bloccata, controllare lo stato delle inizializzazioni del gruppo di coerenza con l'API REST di ONTAP, Gestore di sistema o il comando `sn show -expand`.

Soluzione:

Se l'inizializzazione dei gruppi di coerenza non riesce, rimuovere la relazione SM-BC, eliminare il gruppo di coerenza, quindi ricreare la relazione e inizializzarla. Questo flusso di lavoro varia a seconda della versione di ONTAP in uso.

Se si utilizza ONTAP 9.8-9.9.1	Se si utilizza ONTAP 9.10.1 o versione successiva
1. "Rimuovere la configurazione SM-BC" 2. "Creare una relazione di gruppo di coerenza" 3. "Inizializzare la relazione del gruppo di coerenza"	1. In **protezione > Relazioni**, individuare la relazione SM-BC nel gruppo di coerenza. Selezionare ⋮, Quindi **Delete** per rimuovere la relazione SM-BC. 2. "Eliminare il gruppo di coerenza" 3. "Configurare il gruppo di coerenza"

Failover pianificato non riuscito

Problema:

Dopo aver eseguito il `snapmirror failover start` il comando, l'output per `snapmirror failover show` command visualizza un messaggio che indica che è in

corso un'operazione senza interruzioni.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                        08:35:04
08:35:04
```

Causa:

Un failover pianificato non può iniziare quando è in corso un'operazione senza interruzioni, tra cui lo spostamento del volume, il trasferimento degli aggregati e il failover dello storage.

Soluzione:

Attendere il completamento dell'operazione senza interruzioni e provare a eseguire nuovamente l'operazione di failover.

Il mediatore ONTAP non è raggiungibile o lo stato del quorum del mediatore è falso

Problema:

Dopo aver eseguito il `snapmirror failover start` il comando, l'output per `snapmirror failover show` Viene visualizzato un messaggio che indica che Mediator non è configurato.

Vedere "Inizializzare il mediatore ONTAP".

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Causa:

Il mediatore non è configurato o si sono riscontrati problemi di connettività di rete.

Soluzione:

Se il mediatore ONTAP non è configurato, è necessario configurare il mediatore ONTAP prima di poter stabilire una relazione SM-BC. Risolvere eventuali problemi di connettività di rete. Assicurarsi che Mediator sia connesso e che lo stato del quorum sia vero sia sul sito di origine che su quello di destinazione utilizzando il comando snapmirror mediator show. Per ulteriori informazioni, vedere Configurare il mediatore ONTAP.

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Failover automatico non pianificato non attivato sul sito B

Problema:

Un guasto nel sito A non attiva un failover non pianificato sul sito B.

Possibile causa n. 1:

Il mediatore ONTAP non è configurato. Per determinare se questa è la causa, eseguire il `snapmirror mediator show` Sul cluster del sito B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Questo esempio indica che il mediatore ONTAP non è configurato sul sito B.

Soluzione:

Assicurarsi che il mediatore ONTAP sia configurato su entrambi i cluster, che lo stato sia connesso e che il quorum sia impostato su vero.

Possibile causa n. 2:

Il gruppo di coerenza SnapMirror non è sincronizzato. Per determinare se questa è la causa, visualizzare il registro eventi per visualizzare se il gruppo di coerenza era sincronizzato durante il momento in cui si è verificato un errore del sito A.

```
cluster::*> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Soluzione:

Completare i seguenti passaggi per eseguire un failover forzato sul sito B.

1. Annullare la mappatura di tutte le LUN appartenenti al gruppo di coerenza dal sito B.
2. Eliminare la relazione del gruppo di coerenza SnapMirror utilizzando `force` opzione.

3. Inserire il `snapmirror break` Sul gruppo di coerenza i volumi costituenti per convertire i volumi da DP a R/W, per abilitare l'i/o dal sito B.
4. Avviare i nodi del sito A per creare una relazione RTO zero dal sito B al sito A.
5. Rilasciare il gruppo di coerenza con `relationship-info-only` On-site A per conservare una copia Snapshot comune e annullare la mappatura delle LUN appartenenti al gruppo di coerenza.
6. Convertire i volumi sul sito A da R/W a DP impostando una relazione a livello di volume utilizzando il criterio Sync o il criterio Async.
7. Eseguire il `snapmirror resync` per sincronizzare le relazioni.
8. Eliminare le relazioni di SnapMirror con il criterio di sincronizzazione sul sito A.
9. Rilasciare le relazioni di SnapMirror con il criterio Sync utilizzando `relationship-info-only true` On-site B.
10. Creare una relazione di gruppo di coerenza tra il sito B e il sito A.
11. Eseguire una risincronizzazione del gruppo di coerenza dal sito A, quindi verificare che il gruppo di coerenza sia sincronizzato.
12. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

Collegamento tra il sito B e il mediatore inattivo e il sito A inattivo

Per verificare la connessione del mediatore ONTAP, utilizzare `snapmirror mediator show` comando. Se lo stato della connessione non è raggiungibile e il sito B non è in grado di raggiungere il sito A, si avrà un'uscita simile a quella riportata di seguito. Per ripristinare la connessione, attenersi alla procedura descritta nella soluzione

```
cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Soluzione

Forzare un failover per abilitare l'i/o dal sito B e quindi stabilire una relazione RTO zero dal sito B al sito A. Completare i seguenti passaggi per eseguire un failover forzato sul sito B.

1. Annullare la mappatura di tutte le LUN appartenenti al gruppo di coerenza dal sito B.
2. Eliminare la relazione del gruppo di coerenza di SnapMirror utilizzando l'opzione force (forza).
3. Inserisci il comando SnapMirror breaker (`snapmirror break -destination_path svm:_volume_`) Sui volumi costituenti del gruppo di coerenza per convertire volumi da DP a RW, per abilitare i/o dal sito B.

   Devi inviare il comando SnapMirror BREAK per ogni relazione nel gruppo di coerenza. Ad esempio, se nel gruppo di coerenza sono presenti tre volumi, verrà inviato il comando per ogni volume.

4. Avviare i nodi del sito A per creare una relazione RTO zero dal sito B al sito A.

5. Rilasciare il gruppo di coerenza con informazioni sulla relazione solo sul sito A per conservare una copia Snapshot comune e annullare la mappatura delle LUN appartenenti al gruppo di coerenza.
6. Convertire i volumi sul sito A da RW a DP impostando una relazione a livello di volume utilizzando il criterio Sync o il criterio Async.
7. Eseguire il `snapmirror resync` per sincronizzare le relazioni.
8. Eliminare le relazioni di SnapMirror con il criterio di sincronizzazione sul sito A.
9. Rilasciare il criterio delle relazioni di SnapMirror con Sync utilizzando solo le informazioni sulla relazione, vero sul sito B.
10. Creare una relazione di gruppo di coerenza tra il sito B e il sito A.
11. Dal cluster di origine, sincronizzare nuovamente il gruppo di coerenza. Verificare che lo stato del gruppo di coerenza sia sincronizzato.
12. Eseguire nuovamente la scansione dei percorsi di i/o delle LUN dell'host per ripristinare tutti i percorsi alle LUN.

Collegamento tra il sito A e il mediatore inattivo e il sito B inattivo

Quando si utilizza SM-BC, è possibile perdere la connettività tra il ONTAP Mediator o i cluster in cui si esegue il peering. È possibile diagnosticare il problema controllando la connessione, la disponibilità e lo stato di consenso delle diverse parti della relazione SM-BC e riprendendo con forza la connessione.

Cosa controllare	Comando CLI	Indicatore
Mediatore dal sito A.	`snapmirror mediator show`	Lo stato della connessione sarà `unreachable`
Connettività del sito B.	`cluster peer show`	La disponibilità sarà `unavailable`
Stato di consenso del volume SM-BC	`volume show` *`volume_name`* `-fields smbc-consensus`	Il `sm-bc consensus` il campo indicherà `Awaiting-consensus`

Per ulteriori informazioni sulla diagnosi e la risoluzione di questo problema, consultare l'articolo della Knowledge base "Collegamento tra il sito A e Mediator Down e il sito B Down quando si utilizza SM-BC".

L'operazione di eliminazione di SM-BC SnapMirror non riesce quando fence è impostato sul volume di destinazione

Problema:

L'operazione di eliminazione di SnapMirror non riesce quando uno dei volumi di destinazione ha una fence di reindirizzamento impostata.

Soluzione

Eseguire le seguenti operazioni per riprovare il reindirizzamento e rimuovere la fence dal volume di destinazione.

- Risincronizzazione di SnapMirror
- Aggiornamento di SnapMirror

Operazione di spostamento del volume bloccata quando il sistema primario è inattivo

Problema:

Un'operazione di spostamento del volume rimane bloccata a tempo indeterminato nello stato di cutover rinviato quando il sito primario è inattivo in una relazione SM-BC. Quando il sito primario è inattivo, il sito secondario esegue un failover automatico non pianificato (AUFO). Quando è in corso un'operazione di spostamento del volume quando viene attivato l'AUFO, lo spostamento del volume si blocca.

Soluzione:

Interrompere l'istanza di spostamento del volume bloccata e riavviare l'operazione di spostamento del volume.

La release di SnapMirror non riesce quando non è possibile eliminare la copia Snapshot

Problema:

L'operazione di rilascio di SnapMirror non riesce quando non è possibile eliminare la copia Snapshot.

Soluzione:

La copia Snapshot contiene un tag transitorio. Utilizzare `snapshot delete` con il `-ignore-owners` Opzione per rimuovere la copia Snapshot transitoria.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Riprovare `snapmirror release` comando.

La copia Snapshot di riferimento per lo spostamento del volume viene visualizzata come la più recente

Problema:

Dopo aver eseguito un'operazione di spostamento del volume su un volume di gruppo di coerenza, la copia Snapshot di riferimento dello spostamento del volume potrebbe essere visualizzata come la più recente per la relazione SnapMirror.

È possibile visualizzare la copia Snapshot più recente con il seguente comando:

```
snapmirror show -fields newest-snapshot status -expand
```

Soluzione:

Eseguire manualmente un `snapmirror resync` oppure attendere la successiva risincronizzazione automatica al termine dell'operazione di spostamento del volume.

Servizio mediatore per MetroCluster e SnapMirror Business Continuity

Panoramica del mediatore ONTAP

Il mediatore ONTAP offre diverse funzioni per le funzioni di ONTAP:

- Fornisce un archivio persistente e recintato per i metadati ha.

- Funge da proxy ping per la vivacità del controller.
- Fornisce una funzionalità di query sincrona sullo stato dei nodi per agevolare la determinazione del quorum.

Il mediatore ONTAP offre due servizi aggiuntivi di systemctl:

- **`ontap_mediator.service`**

  Mantiene il server REST API per la gestione delle relazioni ONAP.

- **`mediator-scst.service`**

  Controlla l'avvio e lo spegnimento del modulo iSCSI (SCST).

Strumenti forniti all'amministratore di sistema

Strumenti forniti all'amministratore di sistema:

- **`/usr/local/bin/mediator_change_password`**

  Imposta una nuova password API quando vengono forniti il nome utente e la password API correnti.

- **`/usr/local/bin/mediator_change_user`**

  Imposta un nuovo nome utente API quando vengono forniti il nome utente e la password API correnti.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Genera un file tgz locale contenente tutte le informazioni di supporto utili necessarie per la comunicazione con il supporto clienti NetApp. Ciò include la configurazione dell'applicazione, i registri e alcune informazioni di sistema. I bundle vengono generati sul disco locale e possono essere trasferiti manualmente, se necessario. Ubicazione dello storage: /Opt/netapp/data/support_bundle/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Rimuove il pacchetto ONTAP Mediator e il modulo kernel SCST. Sono inclusi tutti i dati di configurazione, registri e mailbox.

- **`/usr/local/bin/mediator_unlock_user`**

  Rilascia un blocco sull'account utente API se viene raggiunto il limite di tentativi di autenticazione. Questa funzione viene utilizzata per impedire la derivazione della password con forza bruta. Viene richiesto all'utente di inserire il nome utente e la password corretti.

- **`/usr/local/bin/mediator_add_user`**

  (Solo supporto) utilizzato per aggiungere l'utente API al momento dell'installazione.

Note speciali

ONTAP Mediator si affida a SCST per fornire iSCSI (vedere http://scst.sourceforge.net/index.html). Questo pacchetto è un modulo del kernel che viene compilato durante l'installazione specificamente per il kernel. Qualsiasi aggiornamento del kernel potrebbe richiedere la reinstallazione di SCST. In alternativa, disinstallare

e reinstallare il supporto ONTAP, quindi riconfigurare la relazione ONTAP.

> Qualsiasi aggiornamento del kernel del sistema operativo del server deve essere coordinato con una finestra di manutenzione in ONTAP.

Novità del mediatore ONTAP

Con ogni release vengono forniti nuovi miglioramenti al mediatore ONTAP. Ecco le novità.

Miglioramenti

Versione del mediatore ONTAP	Miglioramenti
1,7	• Supporto per RHEL 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Supporto per Rocky Linux 8 e 9
1.6	• Aggiornamenti di Python 3.9. • Supporto per RHEL 8.4-8.8, 9.0-9.2, Rocky Linux 8 e 9. • Supporto interrotto per tutte le release di RHEL 7.x / CentOS.
1.5	• Ottimizza la velocità per sistemi SMBC su larga scala. • Firma del codice crittografico aggiunta al programma di installazione. • Include avvisi di deprecazione per RHEL 7.x / CentOS 7.x.
1.4	• Supporto per RHEL 8.4 e 8.5. • Include SCST versione 3.6.0. • Aggiunto supporto per Secure Boot (SB) del firmware basato su UFEI.
1.3	• Supporto per RHEL/CentOS 8.2 e 8.3. • Include SCST versione 3.5.0.
1.2	• Supporto per le cassette postali HTTPS. • Per l'utilizzo con ONTAP 9.8+ MCC-IP AUSO e SM-BC ZRTO. • Include SCST versione 3.4.0.
1.1	• Supporto per RHEL/CentOS 7.6, 7.7, 8.0 e 8.1. • Elimina le dipendenze Perl. • Include SCST versione 3.4.0.
1.0	• Supporto per cassette postali iSCSI. • Per l'utilizzo con ONTAP 9.7+ MCC-IP AUSO. • Supporto per RHEL/CentOS 7.6.

Matrice di supporto del sistema operativo

So per mediatore ONTAP	1,7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
7.6	Obsoleto	Obsoleto	Sì	Sì	Sì	Sì	Sì	Sì (solo RHEL)
7.7	Obsoleto	Obsoleto	Sì	Sì	Sì	Sì	No	No
7.8	Obsoleto	Obsoleto	Sì	Sì	Sì	Sì	No	No
7.9	Obsoleto	Obsoleto	Sì	Sì	Sì	Implicito	No	No
RHEL 8.0	Obsoleto	Obsoleto	Sì	Sì	Sì	Sì	Sì	No
RHEL 8.1	Obsoleto	Obsoleto	Sì	Sì	Sì	Sì	No	No
RHEL 8.2	Obsoleto	Obsoleto	Sì	Sì	Sì	No	No	No
RHEL 8.3	Obsoleto	Obsoleto	Sì	Sì	Sì	No	No	No
RHEL 8.4	Obsoleto	Sì	Sì	Sì	No	No	No	No
RHEL 8.5	Sì	Sì	Sì	Sì	No	No	No	No
RHEL 8.6	Sì	Sì	No	No	No	No	No	No
RHEL 8.7	Sì	Sì	No	No	No	No	No	No
RHEL 8.8	Sì	Sì	No	No	No	No	No	No
RHEL 9.0	Sì	Sì	No	No	No	No	No	No
RHEL 9.1	Sì	Sì	No	No	No	No	No	No
RHEL 9.2	Sì	Sì	No	No	No	No	No	No
RHEL 9,3	Sì	No	No	No	No	No	No	No
CentOS 8 e streaming	No	No	No	No	No	N/A.	N/A.	N/A.
Rocky Linux 8	Sì	Sì	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.

Rocky Linux 9	Sì	Sì	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.

- Se non diversamente specificato, OS si riferisce alle release RedHat e CentOS.
- "No" significa che il sistema operativo e il mediatore ONTAP non sono compatibili.
- CentOS 8 è stato rimosso per tutte le release a causa della sua riramificazione. CentOS Stream non è stato considerato un sistema operativo di destinazione adatto per la produzione. Non è previsto alcun supporto.
- ONTAP Mediator 1.5 è stata l'ultima release supportata per i sistemi operativi delle filiali RHEL 7.x.
- ONTAP 1.6 aggiunge il supporto per Rocky Linux 8 e 9.

Problemi risolti

Data della modifica	Modificare l'ID	Descrizione
10 gennaio 2023	6567145	Sono state apportate le seguenti modifiche: • Supporto aggiunto per sistemi operativi aggiuntivi per ONTAP Mediator: RHEL 9.6, 8.7, 9.0 e 9.1. • Aggiunta della nuova versione 3.7.0 di SCST per sbloccare i problemi dei nuovi sistemi operativi supportati. • Supporto aggiunto per Rocky Linux: Rocky 8 e 9.
24 gennaio 2023	6621319	Libreria SCST preinstallata consentita per le installazioni di ONTAP Mediator.
27 febbraio 2023	6623764	Modifiche implementate per caricare sempre il modulo del kernel scst_disk al riavvio del servizio mediator-scst. Queste modifiche garantiscono che il servizio sia sempre pronto a creare nuove destinazioni iSCSI utilizzando la logica standard.
28 febbraio 2023	6625194	Aggiunta di una nuova opzione al programma di installazione del mediatore ONTAP: `--skip-yum-dependencies`
24 marzo 2023	6652840	Aggiornamento del programma di installazione di ONTAP Mediator in modo da poter reinstallare o riparare l'installazione di SCST.
27 marzo 2023	6655179	Risolto un problema di analisi che si verificava quando veniva attivata la raccolta di bundle di supporto con una password complessa.
28 marzo 2023	6656739	La logica di confronto SCST è stata modificata in modo da installare la versione corretta quando viene aggiornato ONTAP Mediator.

Installare o aggiornare

Preparazione all'installazione o all'aggiornamento del servizio ONTAP Mediator

Per installare il servizio ONTAP Mediator, è necessario assicurarsi che tutti i prerequisiti siano soddisfatti, scaricare il pacchetto di installazione ed eseguire il programma di installazione sull'host. Questa procedura viene utilizzata per un'installazione o un aggiornamento di un'installazione esistente.

A proposito di questa attività

- A partire da ONTAP 9.7, è possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una configurazione IP MetroCluster.
- A partire da ONTAP 9.8, è possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una relazione SM-BC.

Prima di iniziare

È necessario soddisfare i seguenti prerequisiti.

Versione del mediatore ONTAP	Versioni Linux supportate
1,7	• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3 • Rocky Linux 8 e 9
1.6	• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2 • Rocky Linux 8 e 9
1.5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

La versione del kernel deve corrispondere alla versione del sistema operativo.

- installazione fisica a 64 bit o macchina virtuale
- 8 GB DI RAM
- 1 GB di spazio su disco (utilizzato per l'installazione delle applicazioni, i log dei server e il database)
- Utente: Accesso root

Tutti i pacchetti di librerie, ad eccezione del kernel, possono essere aggiornati in modo sicuro, ma potrebbero richiedere un riavvio per influire sull'applicazione ONTAP Mediator. Quando è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Se si installa `yum-utils` è possibile utilizzare `needs-restarting` comando.

Il core del kernel può essere aggiornato se viene aggiornato a una versione ancora supportata dalla matrice di versione di ONTAP Mediator. Il riavvio è obbligatorio, pertanto è necessaria una finestra di servizio.

Il modulo kernel SCST deve essere disinstallato prima del riavvio, quindi reinstallato dopo il riavvio.

> L'aggiornamento a un kernel oltre la release del sistema operativo supportata per la release specifica di ONTAP Mediator non è supportato. (Questo probabilmente indica che il modulo SCST testato non viene compilato).

Registrare una chiave di protezione quando UEFI Secure Boot è attivato

Se l'avvio protetto UEFI è attivato, per installare ONTAP Mediator è necessario registrare una chiave di protezione prima che il servizio ONTAP Mediator possa avviarsi. Per determinare se il sistema è abilitato per UEFI e l'avvio protetto è attivato, procedere come segue:

Fasi

1. Se mokutil non è installato, eseguire il seguente comando:

   ```
   yum install mokutil
   ```

2. Per determinare se UEFI Secure Boot è attivato sul sistema, eseguire il comando seguente:

   ```
   mokutil --sb-state
   ```

   I risultati mostrano se l'avvio protetto UEFI è abilitato su questo sistema.

   > ONTAP Mediator 1.2.0 e le versioni precedenti non supportano questa modalità.

Disattivare l'avvio protetto UEFI

È inoltre possibile scegliere di disattivare l'avvio protetto UEFI prima di installare ONTAP Mediator.

Fasi

1. Nelle impostazioni del BIOS della macchina fisica, disattivare l'opzione "UEFI Secure Boot" (Avvio protetto UEFI).
2. Nelle impostazioni VMware per la VM, disattivare l'opzione "Avvio sicuro" per vSphere 6.x o l'opzione "Avvio sicuro" per vSphere 7.x

Aggiornare il sistema operativo host, quindi il mediatore ONTAP

Per aggiornare il sistema operativo host per ONTAP Mediator a una versione successiva, è necessario prima disinstallare ONTAP Mediator.

Prima di iniziare

Le procedure consigliate per l'installazione di Red Hat Enterprise Linux o Rocky Linux e dei repository associati sul vostro sistema sono elencate di seguito. I sistemi installati o configurati in modo diverso

potrebbero richiedere ulteriori passaggi.

- È necessario installare Red Hat Enterprise Linux o Rocky Linux secondo le Best practice di Red Hat. A causa della fine del ciclo di vita del supporto per le versioni di CentOS 8.x, si sconsiglia di utilizzare le versioni compatibili di CentOS 8.x.
- Durante l'installazione del servizio ONTAP Mediator su Red Hat Enterprise Linux o Rocky Linux, il sistema deve avere accesso al repository appropriato in modo che il programma di installazione possa accedere e installare tutte le dipendenze software richieste.
- Affinché il programma di installazione di yum trovi il software dipendente nei repository Red Hat Enterprise Linux, devi aver registrato il sistema durante l'installazione di Red Hat Enterprise Linux o in seguito utilizzando un abbonamento Red Hat valido.

  Per informazioni su Red Hat Subscription Manager, consulta la documentazione di Red Hat.

- Le seguenti porte devono essere inutilizzate e disponibili per Mediator:
  - 31784
  - 3260
- Se si utilizza un firewall di terze parti: Fare riferimento a. "Requisiti del firewall per ONTAP Mediator"
- Se l'host Linux si trova in una posizione senza accesso a Internet, è necessario assicurarsi che i pacchetti richiesti siano disponibili in un repository locale.

  Se si utilizza il protocollo LACP (link Aggregation Control Protocol) in un ambiente Linux, è necessario configurare correttamente il kernel e assicurarsi di `sysctl net.ipv4.conf.all.arp_ignore` è impostato su "2".

Di cosa hai bisogno

I seguenti pacchetti sono richiesti dal servizio di supporto ONTAP:

Tutte le versioni RHEL/CentOS	Pacchetti aggiuntivi per RHEL 8.x / Rocky Linux 8	Pacchetti aggiuntivi per RHEL 9.x / Rocky Linux 9
• openssl • openssl-devel • kernel-devel- (uname -r) • gcc • fare • libselinux-utils • patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeMaker • efibootmgr • mokutil	• python3-pip • elfutils-libelf-devel • policycoreutils-python-utils • redhat-lsb-core • python39 • python39-devel	• python3-pip • elfutils-libelf-devel • policycoreutils-python-utils • python3 • python3-devel

Il pacchetto di installazione di Mediator è un file tar compresso autoestraente che include:

- Un file RPM contenente tutte le dipendenze che non è possibile ottenere dal repository della release supportata.
- Uno script di installazione.

Si consiglia una certificazione SSL valida.

A proposito di questa attività

Quando si aggiorna il sistema operativo host per ONTAP Mediator a una versione successiva (ad esempio, da 7.x a 8.x) utilizzando il tool leapp-upgrade, È necessario disinstallare ONTAP Mediator perché lo strumento cerca di rilevare nuove versioni degli RPM installati nei repository registrati con il sistema.

Poiché un file .rpm è stato installato come parte del programma di installazione di ONTAP Mediator, viene incluso nella ricerca. Tuttavia, poiché il file .rpm è stato decompresso come parte del programma di installazione e non scaricato da un repository registrato, non è possibile trovare un aggiornamento. In questo caso, il tool leapp-upgrade disinstalla il pacchetto.

Per conservare i file di log, che verranno utilizzati per il triage dei casi di supporto, è necessario eseguire il backup dei file prima di eseguire un aggiornamento del sistema operativo e ripristinarli dopo la reinstallazione del pacchetto ONTAP Mediator. Poiché il mediatore ONTAP viene reinstallato, tutti i cluster ONTAP ad esso connessi dovranno essere riconnessi dopo la nuova installazione.

> Le seguenti operazioni devono essere eseguite nell'ordine indicato. Subito dopo aver reinstallato ONTAP Mediator, interrompere il servizio ontap_mediator, sostituire i file di log e riavviare il servizio. In questo modo, i registri non andranno persi.

Fasi

1. Eseguire il backup dei file di log.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Esegui l'upgrade con il tool di aggiornamento leapp.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Reinstallare il mediatore ONTAP.

> Eseguire il resto della procedura immediatamente dopo la reinstallazione di ONTAP Media per evitare la perdita dei file di log.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Arrestare il servizio ontap_mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Sostituire i file di log.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Avviare il servizio ontap_mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Ricollegare tutti i cluster ONTAP al mediatore ONTAP aggiornato

Procedura per MetroCluster over IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procedura per la Business Continuity di SnapMirror

Per SnapMirror Business Continuity, se il certificato TLS è stato installato al di fuori della directory /opt/netapp, non sarà necessario reinstallarlo. Se si utilizza il certificato autofirmato generato per impostazione predefinita o si mette il certificato personalizzato nella directory /opt/netapp, eseguire il backup e il ripristino.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

```
The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true
```

```
peer1::>
```

Abilitare l’accesso ai repository

È necessario abilitare l’accesso ai repository in modo che ONTAP Mediator possa accedere ai pacchetti richiesti durante il processo di installazione

Fasi

1. Determinare quali repository devono essere utilizzati, come mostrato nella tabella seguente:

Se il sistema operativo in uso è…	È necessario fornire l’accesso a questi repository…
RHEL 7.x	• rhel-7-server-optional-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
CentOS 7.x	• C7.6.1810 - repository di base
Rocky Linux 8	• appstream • baseos
Rocky Linux 9	• appstream • baseos

2. Utilizzare una delle seguenti procedure per abilitare l’accesso ai repository elencati in precedenza, in modo che ONTAP Media possa accedere ai pacchetti richiesti durante il processo di installazione.

Procedura per il sistema operativo RHEL 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 7.x** per consentire l'accesso ai repository:

Fasi

1. Iscriviti al repository richiesto:

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-
   server-optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Eseguire `yum repolist` comando.

   Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository "rhel-7-server-optional-rpms" dovrebbe apparire nell'elenco.

   ```
   [root@localhost ~]# yum repolist
   Loaded plugins: product-id, search-disabled-repos, subscription-
   manager
   rhel-7-server-optional-rpms | 3.2 kB  00:00:00
   rhel-7-server-rpms | 3.5 kB  00:00:00
   (1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
   |  26 kB  00:00:00
   (2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
   | 2.5 MB  00:00:00
   (3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
   | 8.3 MB  00:00:01
   repo id                                       repo name
   status
   rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
   Linux 7 Server - Optional (RPMs)   19,447
   rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
   Linux 7 Server (RPMs)              26,758
   repolist: 46,205
   [root@localhost ~]#
   ```

Procedura per il sistema operativo RHEL 8.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 8.x** per abilitare l'accesso ai repository:

Fasi

1. Iscriviti al repository richiesto:

   `subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms`

   Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Eseguire `yum repolist` comando.

   I repository appena sottoscritti dovrebbero apparire nell'elenco.

Procedura per il sistema operativo RHEL 9.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 9.x** per consentire l'accesso ai repository:

Fasi

1. Iscriviti al repository richiesto:

   `subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms`

   Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-baseos-rpms
   Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
   system.
   [root@localhost ~]# subscription-manager repos --enable rhel-9-for-
   x86_64-appstream-rpms
   Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Eseguire `yum repolist` comando.

   I repository appena sottoscritti dovrebbero apparire nell'elenco.

Procedura per il sistema operativo CentOS 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **CentOS 7.x** per consentire l'accesso ai repository:

> I seguenti esempi mostrano un repository per CentOS 7.6 e potrebbero non funzionare per altre versioni di CentOS. Utilizza il repository di base per la tua versione di CentOS.

Fasi

1. Aggiungere il repository di base C7.6.1810. Il repository dei vault di base di C7.6.1810 contiene il pacchetto "kernel-devel" necessario per il mediatore ONTAP.
2. Aggiungere le seguenti righe a /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Eseguire `yum repolist` comando.

   Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository CentOS-7.6.1810 - base dovrebbe apparire nell'elenco.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                  | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz           | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db         | 6.0 MB  00:00:04
repo id                      repo name                 status
C7.6.1810-base/x86_64        CentOS-7.6.1810 - Base    10,019
base/7/x86_64                CentOS-7 - Base           10,097
extras/7/x86_64              CentOS-7 - Extras         307
updates/7/x86_64             CentOS-7 - Updates        1,010
repolist: 21,433
[root@localhost ~]#
```

Procedura per i sistemi operativi Rocky Linux 8 o 9

Utilizzare questa procedura se il sistema operativo in uso è **Rocky Linux 8** o **Rocky Linux 9** per consentire l'accesso ai repository:

Fasi

1. Iscriviti ai repository richiesti:

   ```
   dnf config-manager --set-enabled baseos

   dnf config-manager --set-enabled appstream
   ```

2. Eseguire una `clean` funzionamento:

   ```
   dnf clean all
   ```

3. Verificare l'elenco dei repository:

   ```
   dnf repolist
   ```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Scarica il pacchetto di installazione di Mediator

Scarica il pacchetto di installazione di Mediator come parte del processo di installazione.

Fasi

1. Scarica il pacchetto di installazione di Mediator dalla pagina del mediatore ONTAP.

   "Pagina di download del mediatore ONTAP"

2. Verificare che il pacchetto di installazione di Mediator si trovi nella directory di lavoro corrente:

   `ls`

   ```
   [root@mediator-host ~]#ls
   ontap-mediator-1.7.0.tgz
   ```

   > Per le versioni 1.4 e precedenti di ONTAP Mediator, il programma di installazione è denominato `ontap-mediator`.

   Se ci si trova in una posizione senza accesso a Internet, è necessario assicurarsi che il programma di installazione abbia accesso ai pacchetti richiesti.

3. Se necessario, spostare il pacchetto di installazione di Mediator dalla directory di download alla directory di installazione sull'host Linux Mediator.
4. Decomprimere il pacchetto di installazione:

   `tar xvfz ontap-mediator-1.7.0.tgz`

   ```
   [root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
   ontap-mediator-1.7.0/
   ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
   ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/ontap-mediator-1.7.0
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
   ```

Verificare la firma del codice del mediatore ONTAP

Prima di installare il pacchetto di installazione di ONTAP, verificare la firma del codice del mediatore.

Prima di iniziare

Prima di verificare la firma del codice Mediator, il sistema deve soddisfare i seguenti requisiti.

- openssl versioni da 1.0.2 a 3.0 per la verifica di base
- openssl versione 1.1.0 o successiva per le operazioni TSA (Time Stamping Authority)
- Accesso a Internet pubblico per la verifica OCSP

I seguenti file sono inclusi nel pacchetto di download:

File	Descrizione
`ONTAP-Mediator-development.pub`	Chiave pubblica utilizzata per verificare la firma
`csc-prod-chain-ONTAP-Mediator.pem`	Catena di trust della CA per la certificazione pubblica
`csc-prod-ONTAP-Mediator.pem`	Il certificato utilizzato per generare la chiave
`ontap-mediator-1.7.0`	Il file eseguibile di installazione del prodotto per la versione 1.7.0
`ontap-mediator-1.7.0.sig`	SHA-256 ha eseguito l'hashing, quindi ha firmato RSA utilizzando la chiave csc-PROD, firma per l'installatore
`ontap-mediator-1.7.0.sig.tsr`	La richiesta di revoca per l'utilizzo da parte di OCSCP per la firma dell'installatore
`tsa-prod-ONTAP-Mediator.pem`	Il certificato pubblico per il TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	La catena CA del certificato pubblico per il TSR

Fasi

1. Eseguire il controllo della revoca su `csc-prod-ONTAP-Mediator.pem` Utilizzando il protocollo OCSP (Online Certificate Status Protocol).
   a. Individuare l'URL OCSP utilizzato per registrare il certificato perché i certificati dello sviluppatore potrebbero non fornire un uri.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Generare una richiesta OCSP per il certificato.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Connettersi a OCSP Manager per inviare la richiesta OCSP:

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Verificare la catena di attendibilità del CSC e le date di scadenza rispetto all'host locale:

   `openssl verify`

   > Il `openssl` La versione dal PERCORSO deve avere un valido `cert.pem` (non autofirmato).

   ```
   openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
   Signature-Check certificate has expired or is invalid. Download a newer
   version of the ONTAP Mediator.
   openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
   Stamp certificate has expired or is invalid. Download a newer version of
   the ONTAP Mediator.
   ```

3. Verificare `ontap-mediator-1.6.0.sig.tsr` e. `ontap-mediator-1.7.0.tsr` file che utilizzano i certificati associati:

   `openssl ts -verify`

   > `.tsr` i file contengono la risposta di time stamp associata al programma di installazione e la firma del codice. L'elaborazione conferma che il timestamp ha una firma valida da TSA e che il file di input non è stato modificato. La verifica viene eseguita localmente sul computer. Indipendentemente, non è necessario accedere ai server TSA.

   ```
   openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
   1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
   prod-ONTAP-Mediator.pem
   openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
   1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
   ONTAP-Mediator.pem
   ```

4. Verificare le firme rispetto alla chiave:

   `openssl -dgst -verify`

   ```
   openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
   ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
   ```

Esempio di verifica della firma del codice del mediatore ONTAP (output della console)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#
```

Installare il pacchetto di installazione di ONTAP Mediator

Per installare il servizio di supporto ONTAP, è necessario ottenere il pacchetto di installazione ed eseguire il programma di installazione sull'host.

Fasi

1. Eseguire il programma di installazione e rispondere alle richieste come richiesto:

   `./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
   ```

   Il processo di installazione procede alla creazione degli account richiesti e all'installazione dei pacchetti richiesti. Se sull'host è installata una versione precedente di Mediator, viene richiesto di confermare l'aggiornamento.

2. A partire da ONTAP Mediator 1.4, il meccanismo di avvio sicuro è abilitato sui sistemi UEFI. Quando Secure Boot è attivato, è necessario eseguire ulteriori operazioni per registrare la chiave di sicurezza dopo l'installazione:

   - Seguire le istruzioni nel file README per firmare il modulo del kernel SCST:

     `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

- Individuare le chiavi richieste:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Dopo l’installazione, i file README e la posizione della chiave vengono forniti anche nell’output di sistema.

Esempio di installazione di ONTAP Mediator 1,6 (uscita console)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer


+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall
success
success
success


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

```
Package python3-pip-9.0.3-19.el8.noarch is already installed.
Package policycoreutils-python-utils-2.9-14.el8.noarch is already
installed.
Dependencies resolved.
=========================================================================
=========================================================================
========================================
 Package                                        Architecture
Version                                                   Repository
Size
=========================================================================
=========================================================================
========================================
Installing:
 bzip2                                          x86_64
1.0.6-26.el8                                              rhel-8-for-
x86_64-baseos-rpms                       60 k
 elfutils-libelf-devel                          x86_64
0.186-1.el8                                               rhel-8-for-
x86_64-baseos-rpms                       60 k
 kernel-devel                                   x86_64
4.18.0-348.el8                                            rhel-8-for-
x86_64-baseos-rpms                       20 M
 make                                           x86_64
1:4.2.1-11.el8                                            rhel-8-for-
x86_64-baseos-rpms                      498 k
 openssl-devel                                  x86_64
1:1.1.1k-7.el8_6                                          rhel-8-for-
x86_64-baseos-rpms                      2.3 M
 patch                                          x86_64
2.7.6-11.el8                                              rhel-8-for-
x86_64-baseos-rpms                      138 k
 perl-ExtUtils-MakeMaker                        noarch
1:7.34-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                   301 k
 python36-devel                                 x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                    rhel-8-for-
x86_64-appstream-rpms                    17 k
 redhat-lsb-core                                x86_64
4.1-47.el8                                                rhel-8-for-
x86_64-appstream-rpms                    45 k
Upgrading:
 cpp                                            x86_64
8.5.0-10.1.el8_6                                          rhel-8-for-
x86_64-appstream-rpms                    10 M
 elfutils-libelf                                x86_64
```

```
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      229 k
 elfutils-libs                                  x86_64
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      295 k
 gcc                                            x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-appstream-rpms                    23 M
 libgcc                                         x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                       80 k
 libgomp                                        x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      207 k
 libsemanage                                    x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      168 k
 mokutil                                        x86_64
1:0.3.0-11.el8_6.1                                          rhel-8-for-
x86_64-baseos-rpms                       46 k
 openssl                                        x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      709 k
 openssl-libs                                   x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      1.5 M
 platform-python-pip                            noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-baseos-rpms                      1.6 M
 policycoreutils                                x86_64
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      374 k
 policycoreutils-python-utils                   noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      253 k
 python3-libsemanage                            x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      128 k
 python3-pip                                    noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-appstream-rpms                    20 k
 python3-policycoreutils                        noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      2.2 M
 python36                                       x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                      rhel-8-for-
```

```
x86_64-appstream-rpms                    19 k
Installing dependencies:
 annobin                                         x86_64
10.29-3.el8                                               rhel-8-for-
x86_64-appstream-rpms                   117 k
 at                                              x86_64
3.1.20-11.el8                                             rhel-8-for-
x86_64-baseos-rpms                       81 k
 bc                                              x86_64
1.07.1-5.el8                                              rhel-8-for-
x86_64-baseos-rpms                      129 k
 cups-client                                     x86_64
1:2.2.6-38.el8                                            rhel-8-for-
x86_64-appstream-rpms                   169 k
 dwz                                             x86_64
0.12-10.el8                                               rhel-8-for-
x86_64-appstream-rpms                   109 k
 ed                                              x86_64
1.14.2-4.el8                                              rhel-8-for-
x86_64-baseos-rpms                       82 k
 efi-srpm-macros                                 noarch
3-3.el8                                                   rhel-8-for-
x86_64-appstream-rpms                    22 k
 esmtp                                           x86_64
1.2-15.el8                                                EPEL-8
57 k
 ghc-srpm-macros                                 noarch
1.4.2-7.el8                                               rhel-8-for-
x86_64-appstream-rpms                   9.4 k
 go-srpm-macros                                  noarch
2-17.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    13 k
 keyutils-libs-devel                             x86_64
1.5.10-6.el8                                              rhel-8-for-
x86_64-baseos-rpms                       48 k
 krb5-devel                                      x86_64
1.18.2-14.el8                                             rhel-8-for-
x86_64-baseos-rpms                      560 k
 libcom_err-devel                                x86_64
1.45.6-2.el8                                              rhel-8-for-
x86_64-baseos-rpms                       38 k
 libesmtp                                        x86_64
1.0.6-18.el8                                              EPEL-8
70 k
 libkadm5                                        x86_64
1.18.2-14.el8                                             rhel-8-for-
```

```
x86_64-baseos-rpms                      187 k
 liblockfile                                    x86_64
1.14-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                    32 k
 libselinux-devel                               x86_64
2.9-5.el8                                               rhel-8-for-
x86_64-baseos-rpms                      200 k
 libsepol-devel                                 x86_64
2.9-3.el8                                               rhel-8-for-
x86_64-baseos-rpms                       87 k
 libverto-devel                                 x86_64
0.3.0-5.el8                                             rhel-8-for-
x86_64-baseos-rpms                       18 k
 m4                                             x86_64
1.4.18-7.el8                                            rhel-8-for-
x86_64-baseos-rpms                      223 k
 mailx                                          x86_64
12.5-29.el8                                             rhel-8-for-
x86_64-baseos-rpms                      257 k
 ncurses-compat-libs                            x86_64
6.1-9.20180224.el8                                      rhel-8-for-
x86_64-baseos-rpms                      328 k
 ocaml-srpm-macros                              noarch
5-4.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   9.5 k
 openblas-srpm-macros                           noarch
2-2.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   8.0 k
 pcre2-devel                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      605 k
 pcre2-utf16                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      229 k
 pcre2-utf32                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      220 k
 perl-CPAN-Meta-YAML                            noarch
0.018-397.el8                                           rhel-8-for-
x86_64-appstream-rpms                    34 k
 perl-ExtUtils-Command                          noarch
1:7.34-1.el8                                            rhel-8-for-
x86_64-appstream-rpms                    19 k
 perl-ExtUtils-Install                          noarch
2.14-4.el8                                              rhel-8-for-
x86_64-appstream-rpms                    46 k
```

```
 perl-ExtUtils-Manifest                          noarch
1.70-395.el8                                             rhel-8-for-
x86_64-appstream-rpms                    37 k
 perl-ExtUtils-ParseXS                           noarch
1:3.35-2.el8                                             rhel-8-for-
x86_64-appstream-rpms                    83 k
 perl-JSON-PP                                    noarch
1:2.97.001-3.el8                                         rhel-8-for-
x86_64-appstream-rpms                    68 k
 perl-Math-BigInt                                noarch
1:1.9998.11-7.el8                                        rhel-8-for-
x86_64-baseos-rpms                      196 k
 perl-Math-Complex                               noarch
1.59-421.el8                                             rhel-8-for-
x86_64-baseos-rpms                      109 k
 perl-Test-Harness                               noarch
1:3.42-1.el8                                             rhel-8-for-
x86_64-appstream-rpms                   279 k
 perl-devel                                      x86_64
4:5.26.3-419.el8_4.1                                     rhel-8-for-
x86_64-appstream-rpms                   599 k
 perl-srpm-macros                                noarch
1-25.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    11 k
 perl-version                                    x86_64
6:0.99.24-1.el8                                          rhel-8-for-
x86_64-appstream-rpms                    67 k
 platform-python-devel                           x86_64
3.6.8-41.el8                                             rhel-8-for-
x86_64-appstream-rpms                   249 k
 python-rpm-macros                               noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python-srpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python3-pyparsing                               noarch
2.1.10-7.el8                                             rhel-8-for-
x86_64-baseos-rpms                      142 k
 python3-rpm-generators                          noarch
5-7.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    25 k
 python3-rpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    14 k
 qt5-srpm-macros                                 noarch
```

```
5.15.2-1.el8                                                rhel-8-for-
x86_64-appstream-rpms                   11 k
 redhat-lsb-submod-security                     x86_64
4.1-47.el8                                                  rhel-8-for-
x86_64-appstream-rpms                   22 k
 redhat-rpm-config                              noarch
125-1.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   87 k
 rust-srpm-macros                               noarch
5-2.el8                                                     rhel-8-for-
x86_64-appstream-rpms                  9.3 k
 spax                                           x86_64
1.5.3-13.el8                                                rhel-8-for-
x86_64-baseos-rpms                    217 k
 systemtap-sdt-devel                            x86_64
4.6-4.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   86 k
 time                                           x86_64
1.9-3.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      54 k
 unzip                                          x86_64
6.0-46.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    196 k
 util-linux-user                                x86_64
2.32.1-28.el8                                               rhel-8-for-
x86_64-baseos-rpms                    100 k
 zip                                            x86_64
3.0-23.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    270 k
 zlib-devel                                     x86_64
1.2.11-17.el8                                               rhel-8-for-
x86_64-baseos-rpms                      58 k
Installing weak dependencies:
 perl-CPAN-Meta                                 noarch
2.150010-396.el8                                            rhel-8-for-
x86_64-appstream-rpms                   191 k
 perl-CPAN-Meta-Requirements                    noarch
2.140-396.el8                                               rhel-8-for-
x86_64-appstream-rpms                   37 k
 perl-Encode-Locale                             noarch
1.05-10.module+el8.3.0+6498+9eecfe51                        rhel-8-for-
x86_64-appstream-rpms                   22 k
 perl-Time-HiRes                                x86_64
4:1.9758-2.el8                                              rhel-8-for-
x86_64-appstream-rpms                   61 k
```

```
Transaction Summary
================================================================================
================================================================================
==========================================
Install  69 Packages
Upgrade  17 Packages

Total download size: 72 M
Is this ok [y/N]: y
Downloading Packages:
(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm
735 kB/s |  46 kB     00:00
(2/86): libesmtp-1.0.6-18.el8.x86_64.rpm
1.0 MB/s |  70 kB     00:00
(3/86): esmtp-1.2-15.el8.x86_64.rpm
747 kB/s |  57 kB     00:00
(4/86): rust-srpm-macros-5-2.el8.noarch.rpm
308 kB/s | 9.3 kB     00:00
(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm
781 kB/s |  37 kB     00:00
(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm
2.7 MB/s | 191 kB     00:00
(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm
214 kB/s | 9.5 kB     00:00
(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm
1.2 MB/s |  68 kB     00:00
(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm
5.8 MB/s | 301 kB     00:00
(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm
317 kB/s | 9.4 kB     00:00
(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm
4.5 MB/s | 279 kB     00:00
(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm
520 kB/s |  19 kB     00:00

...

15 MB/s | 1.5 MB     00:00
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------
Total
35 MB/s |  72 MB     00:02
Running transaction check
Transaction check succeeded.
Running transaction test
```

```
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading        : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading        : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading        : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing       : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing       : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading        : libsemanage-2.9-8.el8.x86_64
6/103
  Installing       : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing       : python-srpm-macros-3-41.el8.noarch
8/103
  Installing       : python-rpm-macros-3-41.el8.noarch
9/103
  Installing       : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing       : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing       : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing       : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading        : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading        : policycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: policycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading        : python3-policycoreutils-2.9-19.el8.noarch
16/103
  Installing       : dwz-0.12-10.el8.x86_64
17/103
```

```
  Installing       : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
  Installing       : libesmtp-1.0.6-18.el8.x86_64
19/103
  Installing       : mailx-12.5-29.el8.x86_64
20/103
  Installing       : libkadm5-1.18.2-14.el8.x86_64
21/103
  Upgrading        : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Upgrading        : platform-python-pip-9.0.3-22.el8.noarch
23/103
  Upgrading        : python3-pip-9.0.3-22.el8.noarch
24/103
  Upgrading        : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Upgrading        : cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Upgrading        : gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Installing       : annobin-10.29-3.el8.x86_64
28/103
  Installing       : unzip-6.0-46.el8.x86_64
29/103
  Installing       : zip-3.0-23.el8.x86_64
30/103
  Installing       : perl-Math-Complex-1.59-421.el8.noarch
31/103
  Installing       : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
  Installing       : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
  Installing       : make-1:4.2.1-11.el8.x86_64
34/103
  Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103
```

```
  Installing       : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
  Installing       : util-linux-user-2.32.1-28.el8.x86_64
36/103
  Installing       : libsepol-devel-2.9-3.el8.x86_64
37/103
  Installing       : pcre2-utf32-10.32-2.el8.x86_64
38/103
  Installing       : pcre2-utf16-10.32-2.el8.x86_64
39/103
  Installing       : pcre2-devel-10.32-2.el8.x86_64
40/103
  Installing       : libselinux-devel-2.9-5.el8.x86_64
41/103
  Installing       : patch-2.7.6-11.el8.x86_64
42/103
  Installing       : python3-pyparsing-2.1.10-7.el8.noarch
43/103
  Installing       : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
  Installing       : spax-1.5.3-13.el8.x86_64
45/103
  Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
  Installing       : m4-1.4.18-7.el8.x86_64
46/103
  Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
  Installing       : libverto-devel-0.3.0-5.el8.x86_64
47/103
  Installing       : bc-1.07.1-5.el8.x86_64
48/103
  Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
  Installing       : at-3.1.20-11.el8.x86_64
49/103
  Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
  Installing       : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
  Installing       : krb5-devel-1.18.2-14.el8.x86_64
51/103
  Installing       : time-1.9-3.el8.x86_64
52/103
  Running scriptlet: time-1.9-3.el8.x86_64
52/103
```

```
  Upgrading        : policycoreutils-python-utils-2.9-19.el8.noarch
80/103
  Installing       : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
  Upgrading        : elfutils-libs-0.186-1.el8.x86_64
82/103
  Upgrading        : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
  Upgrading        : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
  Installing       : kernel-devel-4.18.0-348.el8.x86_64
85/103
  Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

  ...

85/103
  Installing       : bzip2-1.0.6-26.el8.x86_64
86/103
  Cleanup          : policycoreutils-python-utils-2.9-14.el8.noarch
87/103
  Cleanup          : python3-policycoreutils-2.9-14.el8.noarch
88/103
  Cleanup          : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Cleanup          : elfutils-libs-0.185-1.el8.x86_64
90/103
  Cleanup          : openssl-1:1.1.1k-4.el8.x86_64
91/103
  Cleanup          : python3-libsemanage-2.9-6.el8.x86_64
92/103
  Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
  Cleanup          : gcc-8.4.1-1.el8.x86_64
93/103
  Running scriptlet: policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : mokutil-1:0.3.0-11.el8.x86_64
95/103
```

```
  Cleanup          : python3-pip-9.0.3-19.el8.noarch
96/103
  Cleanup          : platform-python-pip-9.0.3-19.el8.noarch
97/103
  Cleanup          : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Cleanup          : libsemanage-2.9-6.el8.x86_64
99/103
  Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : libgomp-8.4.1-1.el8.x86_64
102/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : elfutils-libelf-0.185-1.el8.x86_64
103/103
  Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
  Verifying        : esmtp-1.2-15.el8.x86_64
1/103
  Verifying        : libesmtp-1.0.6-18.el8.x86_64

  ...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                              elfutils-
libelf-0.186-1.el8.x86_64     elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                           libgomp-
8.5.0-10.1.el8_6.x86_64        libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                          openssl-
libs-1:1.1.1k-7.el8_6.x86_64   platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch           python3-
libsemanage-2.9-8.el8.x86_64   python3-pip-9.0.3-22.el8.noarch
```

```
python3-policycoreutils-2.9-19.el8.noarch
  python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
  annobin-10.29-3.el8.x86_64                                          at-
3.1.20-11.el8.x86_64                                bc-1.07.1-5.el8.x86_64
  bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64                     dwz-0.12-
10.el8.x86_64
  ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch                        elfutils-libelf-
devel-0.186-1.el8.x86_64
  esmtp-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch                    go-srpm-macros-2-
17.el8.noarch
  kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64               krb5-devel-1.18.2-
14.el8.x86_64
  libcom_err-devel-1.45.6-2.el8.x86_64
libesmtp-1.0.6-18.el8.x86_64                          libkadm5-1.18.2-
14.el8.x86_64
  liblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64                     libsepol-devel-2.9-
3.el8.x86_64
  libverto-devel-0.3.0-5.el8.x86_64                                   m4-
1.4.18-7.el8.x86_64                                 mailx-12.5-
29.el8.x86_64
  make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64         ocaml-srpm-macros-
5-4.el8.noarch
  openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64                 patch-2.7.6-
11.el8.x86_64
  pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64                        pcre2-utf32-10.32-
2.el8.x86_64
  perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch      perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
  perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch             perl-ExtUtils-
Install-2.14-4.el8.noarch
  perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch            perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
  perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch             perl-Math-Complex-
```

```
1.59-421.el8.noarch
  perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64               perl-devel-
4:5.26.3-419.el8_4.1.x86_64
  perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64                 platform-python-
devel-3.6.8-41.el8.x86_64
  python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch                  python3-pyparsing-
2.1.10-7.el8.noarch
  python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch                  python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
  qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64                   redhat-lsb-submod-
security-4.1-47.el8.x86_64
  redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch                     spax-1.5.3-
13.el8.x86_64
  systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64                               unzip-6.0-
46.el8.x86_64
  util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64                               zlib-devel-1.2.11-
17.el8.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /tmp/ontap_mediator.JixKGP/ontap-
mediator-1.6.0/ontap-mediator-1.6.0/install_20221021155929.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20221021155929.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that reboot will be
```

```
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.
+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

Verificare l'installazione

Una volta installato il mediatore ONTAP, verificare che i servizi del mediatore ONTAP siano in esecuzione.

Fasi

1. Visualizza lo stato dei servizi di supporto ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Verificare le porte utilizzate dal servizio di supporto ONTAP:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Configurazione post-installazione

Una volta installato ed eseguito il servizio ONTAP Mediator, è necessario eseguire ulteriori attività di configurazione nel sistema di storage ONTAP per utilizzare le funzioni di Mediator:

- Per utilizzare il servizio ONTAP Mediator in una configurazione IP MetroCluster, vedere "Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster".
- Per utilizzare SnapMirror Business Continuity, vedere "Installare il servizio di supporto ONTAP e confermare la configurazione del cluster ONTAP".

Configurare i criteri di sicurezza di ONTAP Mediator

Il server ONTAP supporta diverse impostazioni di sicurezza configurabili. I valori predefiniti per tutte le impostazioni sono forniti in un file low_space_threshold_mib: 10Read-only:

`/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Tutti i valori inseriti in `ontap_mediator.user_config.yaml` Sovrascrive i valori predefiniti e viene mantenuto in tutti gli aggiornamenti di ONTAP Mediator.

Dopo la modifica `ontap_mediator.user_config.yaml`, Riavviare il servizio di supporto ONTAP:

```
systemctl restart ontap_mediator
```

Modificare gli attributi del mediatore ONTAP

È possibile configurare i seguenti attributi:

> Altri valori predefiniti in `ontap_mediator.config.yaml` non deve essere modificato.

- **Impostazioni utilizzate per installare certificati SSL di terze parti come sostituzioni dei certificati autofirmati predefiniti**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095'                  # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap'            # passphrase for the signed
client cert
```

- **Impostazioni che forniscono protezione contro gli attacchi di indovinare le password a forza bruta**

  Per attivare la funzione, impostare un valore per `window_seconds` e a. `retry_limit`

  Esempi:

  - Fornire una finestra di 5 minuti per le ipotesi, quindi ripristinare il conteggio a zero errori:

    ```
    authentication_lock_window_seconds: 300
    ```

  - Bloccare l'account se si verificano cinque guasti entro il periodo di tempo previsto:

    ```
    authentication_retry_limit: 5
    ```

  - Riduci l'impatto degli attacchi di indovinare le password con la forza bruta impostando un ritardo che si verifica prima di rifiutare ogni tentativo, rallentando gli attacchi.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to
allow before locking API access, null = unlimited
```

- **Campi che controllano le regole di complessità delle password dell'account utente API del mediatore ONTAP**

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

- **Impostazione che controlla lo spazio libero richiesto su `/opt/netapp/lib/ontap_mediator` disco.**

  Se lo spazio è inferiore alla soglia impostata, il servizio emetterà un avviso.

```
low_space_threshold_mib: 10
```

- **Impostazione che controlla RESERVE_LOG_SPACE.**

  L'installazione predefinita del server ONTAP Mediator crea uno spazio su disco separato per i log. Il programma di installazione crea un nuovo file a dimensione fissa con un totale di 700 MB di spazio su disco da utilizzare esplicitamente per la registrazione di Mediator.

  Per disattivare questa funzione e utilizzare lo spazio su disco predefinito, procedere come segue:

  a. Modificare il valore di RESERVE_LOG_SPACE da "`1'" a "`0'" nel seguente file:

     `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

  b. Riavviare Mediator:

i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

ii. `systemctl restart ontap_mediator`

Per riattivare la funzione, modificare il valore da "`0'" a "`1'" e riavviare il Mediator.

> L'alternanza tra gli spazi su disco non elimina i registri esistenti. Viene eseguito il backup di tutti i registri precedenti, quindi viene spostato nello spazio su disco corrente dopo l'attivazione e il riavvio di Mediator.

Gestire il servizio ONTAP mediator

Dopo aver installato il servizio ONTAP Mediator, è possibile modificare il nome utente o la password. È inoltre possibile disinstallare il servizio di supporto ONTAP.

Modificare il nome utente

A proposito di queste attività

Questa operazione viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/mediator_username
```

Procedura

Modificare il nome utente scegliendo una delle seguenti opzioni:

- Eseguire il comando mediator_change_user e rispondere alle richieste come mostrato nell'esempio seguente:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                   Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Eseguire il seguente comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
 [root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Modificare la password

A proposito di questa attività

Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/mediator_change_password
```

Procedura

Modificare la password scegliendo una delle seguenti opzioni:

- Eseguire `mediator_change_password` e rispondere ai prompt come mostrato nell'esempio seguente:

```
 [root@mediator-host ~]# mediator_change_password
 Change the Mediator API password by entering the following values:
    Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
          Confirm Password:
 The password has been updated successfully.
 [root@mediator-host ~]#
```

- Eseguire il seguente comando:

  ```
  MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
  MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
  ```

  L'esempio mostra che la password viene modificata da "mediator1" a "mediator2".

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Arrestare il servizio di supporto ONTAP

Per interrompere il servizio ONTAP Mediator, attenersi alla seguente procedura:

Fasi

1. Arrestare il mediatore ONTAP.

   ```
   systemctl stop ontap_mediator
   ```

2. Arrestare SCST.

   ```
   systemctl stop mediator-scst
   ```

3. Disattivare il mediatore ONTAP e l'SCST.

   ```
   systemctl diable ontap_mediator mediator-scst
   ```

Riattivare il servizio di supporto ONTAP

Per riattivare il servizio ONTAP Mediator, attenersi alla seguente procedura:

Fasi

1. Abilitare il mediatore ONTAP e l'SCST.

   ```
   systemctl enable ontap_mediator mediator-scst
   ```

2. Avviare SCST.

   ```
   systemctl start mediator-scst
   ```

3. Avviare il mediatore ONTAP.

   ```
   systemctl start ontap_mediator
   ```

Verificare che il mediatore ONTAP sia in buone condizioni

Una volta installato il mediatore ONTAP, verificare che i servizi del mediatore ONTAP siano in esecuzione.

Fasi

1. Visualizza lo stato dei servizi di supporto ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Verificare le porte utilizzate dal servizio di supporto ONTAP:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Disinstallare manualmente SCST per eseguire la manutenzione dell'host

Per disinstallare SCST, è necessario il pacchetto tar SCST utilizzato per la versione installata di ONTAP Mediator.

Fasi

1. Scaricare il pacchetto SCST appropriato (come mostrato nella tabella seguente) e scaricarlo.

Per questa versione …	USA questo bundle tar…
ONTAP mediatore 1,7	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.6	scst-3.7.0.tar.bz2
Mediatore ONTAP 1.5	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.4	scst-3.6.0.tar.bz2
Mediatore ONTAP 1.3	scst-3.5.0.tar.bz2
Mediatore ONTAP 1.1	scst-3.4.0.tar.bz2
Mediatore ONTAP 1.0	scst-3.3.0.tar.bz2

2. Eseguire i seguenti comandi nella directory "scst":
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Installare manualmente SCST per eseguire la manutenzione dell'host

Per installare manualmente SCST, è necessario disporre del pacchetto tar SCST utilizzato per la versione installata di ONTAP Mediator (vedere la tabella precedente).

1. Eseguire i seguenti comandi nella directory "scst":
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. (Facoltativo) se l'opzione Secure Boot (Avvio protetto) è attivata, prima di riavviare il sistema, attenersi alla seguente procedura:
   a. Determinare ciascun nome di file per i moduli "scst_vdisk", "scst" e "iscsi_scst".

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. Determinare la release del kernel.

      ```
      [root@localhost ~]# uname -r
      ```

   c. Firmare ogni file con il kernel.

      ```
      [root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
      file \sha256 \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
      le_key.priv \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
      le_key.der \
      _module-filename_
      ```

   d. Installare la chiave corretta con il firmware UEFI.

      Le istruzioni per l'installazione della chiave UEFI sono disponibili all'indirizzo:

      `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing`

La chiave UEFI generata si trova in:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der
```

3. Eseguire un riavvio.

```
reboot
```

Disinstallare il servizio di supporto ONTAP

Prima di iniziare

Se necessario, è possibile rimuovere il servizio di supporto ONTAP. Il mediatore deve essere disconnesso da ONTAP prima di rimuovere il servizio.

A proposito di questa attività

Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/uninstall_ontap_mediator
```

Fase

1. Disinstallare il servizio di supporto ONTAP:

```
uninstall_ontap_mediator
```

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Rigenerare un certificato autofirmato temporaneo

A proposito di questa attività

- Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.
- È possibile eseguire questa attività solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche al nome host o all'indirizzo IP dell'host dopo l'installazione di ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* utilizzare questa attività per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

Fase

Per rigenerare un nuovo certificato autofirmato temporaneo per l'host corrente, attenersi alla seguente procedura:

1. Riavviare ONTAP Mediator:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

   ```
   [root@xyz000123456 ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
   [root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

   Adding Subject Alternative Names to the self-signed server certificate
   #
   # OpenSSL example configuration file.
   Generating self-signed certificates
   Generating RSA private key, 4096 bit long modulus (2 primes)
   ..............................................................................
   ..............................................................................
   ..................++++
   .......................................................++++
   e is 65537 (0x010001)
   Generating a RSA private key
   ...............................................++++
   ..............................................................................
   ...............................................................................+++
   +
   writing new private key to 'ontap_mediator_server.key'
   -----
   Signature ok
   subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
   ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
   support@netapp.com
   Getting CA Private Key
   ```

Gestire l'host del sistema operativo per ONTAP Mediator

Per ottenere performance ottimali, è necessario mantenere regolarmente il sistema operativo host per ONTAP Mediator.

Riavviare l'host

Riavviare l'host quando i cluster sono integri. Mentre il mediatore ONTAP è offline, i cluster rischiano di non essere in grado di reagire correttamente ai guasti. Se è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Il mediatore ONTAP riprende automaticamente durante il riavvio e reinserisce le relazioni precedentemente configurate con i cluster ONTAP.

Aggiornamenti dei pacchetti host

Qualsiasi libreria o pacchetto yum (ad eccezione del kernel) può essere aggiornato in modo sicuro, ma potrebbe richiedere un riavvio per avere effetto. Se è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Se si installa `yum-utils` utilizzare il `needs-restarting` comando per rilevare se qualsiasi modifica del pacchetto richiede un riavvio.

È necessario riavviare il sistema se una delle dipendenze del mediatore ONTAP viene aggiornata perché non avrà effetto immediato sui processi in esecuzione.

Aggiornamenti minori del kernel per il sistema operativo host

SCST deve essere compilato per il kernel in uso. Per aggiornare il sistema operativo, è necessaria una finestra di manutenzione.

Fasi

Per aggiornare il kernel del sistema operativo host, procedere come segue.

1. Arrestare il mediatore ONTAP
2. Disinstallare il pacchetto SCST. (SCST non fornisce un meccanismo di aggiornamento).
3. Aggiornare il sistema operativo e riavviare.
4. Reinstallare il pacchetto SCST.
5. Riattivare i servizi del mediatore ONTAP.

L'host modifica il nome host o l'IP

A proposito di questa attività

- Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.
- È possibile eseguire questa attività solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche al nome host o all'indirizzo IP dell'host dopo l'installazione di ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* utilizzare questa attività per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

Fase

Per rigenerare un nuovo certificato autofirmato temporaneo per l'host corrente, attenersi alla seguente procedura:

1. Riavviare ONTAP Mediator:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.......................................................++++
e is 65537 (0x010001)
Generating a RSA private key
...............................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Gestire i siti MetroCluster con Gestione di sistema

Panoramica sulla gestione del sito MetroCluster con Gestione di sistema

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema come interfaccia semplificata per gestire una configurazione di un'installazione di MetroCluster.

Una configurazione MetroCluster consente a due cluster di eseguire il mirroring dei dati l'uno rispetto all'altro, in modo che, se un cluster non funziona, i dati non vadano persi.

In genere, un'organizzazione imposta i cluster in due ubicazioni geografiche separate. Un amministratore di ogni ubicazione imposta un cluster e lo configura. Quindi, uno degli amministratori può impostare il peering tra i cluster in modo che possano condividere i dati.

L'organizzazione può anche installare un mediatore ONTAP in una terza sede. Il servizio ONTAP Mediator monitora lo stato di ciascun cluster. Quando uno dei cluster rileva che non è in grado di comunicare con il cluster partner, interroga il monitor per determinare se l'errore è un problema con il sistema del cluster o con la

connessione di rete.

Se il problema riguarda la connessione di rete, l'amministratore di sistema esegue i metodi di risoluzione dei problemi per correggere l'errore e riconnettersi. Se il cluster partner non è attivo, l'altro cluster avvia un processo di switchover per controllare l'i/o dei dati per entrambi i cluster.

È inoltre possibile eseguire uno switchover per spegnere uno dei sistemi cluster per la manutenzione pianificata. Il cluster partner gestisce tutte le operazioni di i/o dei dati per entrambi i cluster fino a quando non viene attivato il cluster su cui è stata eseguita la manutenzione ed è stata eseguita un'operazione di switchback.

È possibile gestire le seguenti operazioni:

- "Configurare un sito IP MetroCluster"
- "Impostare il peering di IP MetroCluster"
- "Configurare un sito IP MetroCluster"
- "Eseguire lo switchover e lo switchback di IP MetroCluster"
- "Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster"
- "Upgrade di ONTAP su cluster MetroCluster"

Configurare un sito IP MetroCluster

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per impostare una configurazione IP di un sito MetroCluster.

Un sito MetroCluster è costituito da due cluster. In genere, i cluster si trovano in posizioni geografiche diverse.

Prima di iniziare

- Il sistema deve essere già installato e cablato come indicato nella "Istruzioni per l'installazione e la configurazione" fornito con il sistema.
- Le interfacce di rete del cluster devono essere configurate su ciascun nodo di ciascun cluster per la comunicazione all'interno del cluster.

Assegnare un indirizzo IP di gestione dei nodi

Sistema Windows

Collegare il computer Windows alla stessa subnet dei controller. In questo modo, viene assegnato automaticamente un indirizzo IP di gestione dei nodi al sistema.

Fasi

1. Dal sistema Windows, aprire l'unità **Network** per rilevare i nodi.
2. Fare doppio clic sul nodo per avviare l'installazione guidata del cluster.

Altri sistemi

È necessario configurare l'indirizzo IP di gestione dei nodi per uno dei nodi nel cluster. È possibile utilizzare questo indirizzo IP di gestione dei nodi per avviare la configurazione guidata del cluster.

Vedere "Creazione del cluster sul primo nodo" Per informazioni sull'assegnazione di un indirizzo IP di gestione dei nodi.

Inizializzare e configurare il cluster

Per inizializzare il cluster, impostare una password amministrativa per il cluster e le reti di gestione dei nodi e del cluster. È inoltre possibile configurare servizi come un server DNS per risolvere i nomi host e un server NTP per sincronizzare l'ora.

Fasi

1. In un browser Web, immettere l’indirizzo IP di gestione dei nodi configurato: "https://node-management-IP"

   System Manager rileva automaticamente i nodi rimanenti nel cluster.

2. Nella finestra **Initialize Storage System** (Inizializza sistema di storage), eseguire le seguenti operazioni:
   a. Inserire i dati di configurazione della rete di gestione del cluster.
   b. Inserire gli indirizzi IP di gestione dei nodi per tutti i nodi.
   c. Fornire i dettagli del DNS (Domain Name Server).
   d. Nella sezione **Altro**, selezionare la casella di controllo **Usa servizio ora (NTP)** per aggiungere i server di riferimento orario.

Quando si fa clic su **Submit** (Invia), attendere la creazione e la configurazione del cluster. Quindi, viene eseguito un processo di convalida.

Quali sono le prossime novità?

Una volta configurati, inizializzati e configurati entrambi i cluster, eseguire la seguente procedura:

- "Impostare il peering di IP MetroCluster"

Configurare ONTAP su un nuovo video del cluster

Impostare il peering di IP MetroCluster

A partire da ONTAP 9.8, è possibile gestire una configurazione IP di un'operazione MetroCluster con Gestore di sistema. Dopo aver configurato due cluster, è possibile impostare il peering tra di essi.

Prima di iniziare

Per configurare due cluster, è necessario completare la seguente procedura:

- "Configurare un sito IP MetroCluster"

Alcune fasi di questo processo vengono eseguite da diversi amministratori di sistema situati nei siti geografici di ciascun cluster. Ai fini della spiegazione di questo processo, i cluster sono denominati "cluster del sito A" e "cluster del sito B".

Esecuzione del processo di peering dal sito A.

Questo processo viene eseguito da un amministratore di sistema presso il sito A.

Fasi

1. Accedere al sito Di Un cluster.
2. In System Manager, selezionare **Dashboard** dalla colonna di navigazione a sinistra per visualizzare la panoramica del cluster.

   La dashboard mostra i dettagli del cluster (sito A). Nella sezione **MetroCluster**, a sinistra viene visualizzato un cluster.

3. Fare clic su **Attach Partner Cluster**.
4. Inserire i dettagli delle interfacce di rete che consentono ai nodi del cluster del sito A di comunicare con i nodi del cluster del sito B.
5. Fare clic su **Salva e continua**.
6. Nella finestra **Attach Partner Cluster**, selezionare **i do not have a passphrase**, che consente di generare una passphrase.
7. Copiare la passphrase generata e condividerla con l'amministratore di sistema nel sito B.
8. Selezionare **Chiudi**.

Esecuzione del processo di peering dal sito B.

Questo processo viene eseguito da un amministratore di sistema presso il sito B.

Fasi

1. Accedere al cluster del sito B.
2. In System Manager, selezionare **Dashboard** per visualizzare la panoramica del cluster.

   La dashboard mostra i dettagli del cluster (sito B). Nella sezione MetroCluster, il cluster del sito B viene visualizzato a sinistra.

3. Fare clic su **Attach Partner Cluster** per avviare il processo di peering.
4. Inserire i dettagli delle interfacce di rete che consentono ai nodi del cluster del sito B di comunicare con i nodi del cluster del sito A.

5. Fare clic su **Salva e continua**.
6. Nella finestra **Attach Partner Cluster**, selezionare **ho una passphrase**, che consente di immettere la passphrase ricevuta dall'amministratore di sistema presso il sito A.
7. Selezionare **Peer** per completare il processo di peering.

Quali sono le prossime novità?

Una volta completato correttamente il processo di peering, i cluster vengono configurati. Vedere "Configurare un sito IP MetroCluster".

Configurare un sito IP MetroCluster

A partire da ONTAP 9.8, è possibile gestire una configurazione IP di un'operazione MetroCluster con Gestore di sistema. Dopo aver configurato due cluster e aver eseguito il peering, è possibile configurare ciascun cluster.

Prima di iniziare

Le seguenti procedure dovrebbero essere state completate:

- "Configurare un sito IP MetroCluster"
- "Impostare il peering di IP MetroCluster"

Configurare la connessione tra cluster

Fasi

1. Accedere a System Manager da uno dei siti e selezionare **Dashboard**.

   Nella sezione **MetroCluster**, la figura mostra i due cluster configurati e peered per i siti MetroCluster. Il cluster da cui si sta lavorando (cluster locale) viene visualizzato a sinistra.

2. Fare clic su **Configura MetroCluster**. Da questa finestra è possibile eseguire le seguenti operazioni:
   a. Vengono visualizzati i nodi per ciascun cluster nella configurazione MetroCluster. Utilizzare gli elenchi a discesa per selezionare i nodi del cluster locale che saranno partner di disaster recovery con i nodi del cluster remoto.
   b. Fare clic sulla casella di controllo se si desidera configurare un servizio ONTAP Mediator. Vedere Configurare il servizio ONTAP Mediator.
   c. Se entrambi i cluster dispongono di una licenza per attivare la crittografia, viene visualizzata la sezione **Encryption**.

      Per attivare la crittografia, immettere una passphrase.

   d. Fare clic sulla casella di controllo se si desidera configurare MetroCluster con una rete condivisa Layer 3.

      > I nodi partner ha e gli switch di rete che si connettono ai nodi devono avere una configurazione corrispondente.

3. Fare clic su **Salva** per configurare i siti MetroCluster.

   Nella sezione **MetroCluster** della dashboard, il grafico mostra un segno di spunta sul collegamento tra i due cluster, a indicare che la connessione è in buone condizioni.

Configurare il servizio ONTAP Mediator

Il servizio di supporto ONTAP viene in genere installato in una posizione geografica separata da entrambe le posizioni dei cluster. I cluster comunicano regolarmente con il servizio per indicare che sono attivi e in esecuzione. Se uno dei cluster nella configurazione MetroCluster rileva che la comunicazione con il cluster partner non è attiva, verifica con il mediatore ONTAP se il cluster partner stesso non è attivo.

Prima di iniziare

Entrambi i cluster dei siti MetroCluster devono essere in fase di peering.

Fasi

1. In Gestione sistema in ONTAP 9.8, selezionare **Cluster > Impostazioni**.
2. Nella sezione **Mediator**, fare clic su ⚙.
3. Nella finestra **Configure Mediator** (Configura Mediator), fare clic su **Add+** (Aggiungi+).
4. Inserire i dettagli di configurazione per il mediatore ONTAP.

   È possibile immettere i seguenti dettagli durante la configurazione di un ONTAP Mediator con Gestione di sistema.

   - L'indirizzo IP del mediatore.
   - Il nome utente.
   - La password.

Gestire il Mediator con System Manager

Tramite System Manager, è possibile eseguire attività di gestione del Mediator.

A proposito di queste attività

A partire da ONTAP 9,8, è possibile utilizzare Gestione sistema come interfaccia semplificata per gestire una configurazione IP a quattro nodi di una configurazione MetroCluster, che può includere un ONTAP Mediator installato in una terza posizione.

A partire da ONTAP 9.14.1, è possibile utilizzare System Manager per eseguire queste operazioni anche per una configurazione IP a otto nodi di un sito MetroCluster. Anche se con System Manager non è possibile configurare o espandere un sistema a otto nodi, se è già stato configurato un sistema IP MetroCluster a otto nodi, è possibile eseguire queste operazioni.

Eseguire le seguenti attività per gestire il Mediator.

Per eseguire questa attività…	Intraprendere queste azioni…
Configurare il servizio Mediator	Eseguire le operazioni descritte in "Configurare il servizio ONTAP Mediator".

Attivazione o disattivazione del MAUSO (Mediator-Assisted Automatic Switchover)	1. In System Manager, fare clic su **Dashboard**. 2. Scorrere fino alla sezione MetroCluster. 3. Fare clic su ⋮ Accanto al nome del sito MetroCluster. 4. Selezionare **Abilita** o **Disabilita**. 5. Immettere il nome utente e la password dell'amministratore, quindi fare clic su **Abilita** o **Disabilita**. ⓘ È possibile attivare o disattivare il Mediator quando è possibile raggiungerlo ed entrambi i siti sono in modalità "`normale'". Il mediatore è ancora raggiungibile quando MAUSO è attivato o disattivato se il sistema MetroCluster è in buone condizioni.
Rimuovere il mediatore dalla configurazione MetroCluster	1. In System Manager, fare clic su **Dashboard**. 2. Scorrere fino alla sezione MetroCluster. 3. Fare clic su ⋮ Accanto al nome del sito MetroCluster. 4. Selezionare **Rimuovi mediatore**. 5. Immettere il nome utente e la password dell'amministratore, quindi fare clic su **Rimuovi**.
Controllare lo stato del mediatore	Eseguire le operazioni descritte in "Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster".
Eseguire uno switchover e uno switchback	Eseguire le operazioni descritte in "Eseguire lo switchover e lo switchback di IP MetroCluster".

Eseguire lo switchover e lo switchback di IP MetroCluster

È possibile passare al controllo da un sito IP MetroCluster all'altro per eseguire la manutenzione o il ripristino da un problema.

ⓘ Le procedure di switchover e switchback sono supportate solo per le configurazioni IP MetroCluster.

Panoramica dello switchover e dello switchback

Lo switchover può avvenire in due casi:

- **Uno switchover pianificato**

  Questo switchover viene avviato da un amministratore di sistema che utilizza System Manager. Lo switchover pianificato consente a un amministratore di sistema di un cluster locale di passare al controllo in modo che i servizi dati del cluster remoto vengano gestiti dal cluster locale. Quindi, un amministratore di sistema nella posizione remota del cluster può eseguire la manutenzione sul cluster remoto.

- **Uno switchover non pianificato**

In alcuni casi, quando un cluster MetroCluster non funziona o le connessioni tra i cluster non sono attive, ONTAP avvia automaticamente una procedura di switchover in modo che il cluster ancora in esecuzione gestisca le responsabilità di gestione dei dati del cluster inattivo.

In altri casi, quando ONTAP non è in grado di determinare lo stato di uno dei cluster, l'amministratore di sistema del sito che sta lavorando avvia la procedura di switchover per assumere il controllo delle responsabilità di gestione dei dati dell'altro sito.

Per qualsiasi tipo di procedura di switchover, la funzionalità di servizio dei dati viene restituita al cluster utilizzando un processo *switchback*.

Vengono eseguiti diversi processi di switchover e switchback per ONTAP 9.7 e 9.8:

- Utilizzare Gestione sistema in ONTAP 9.7 per lo switchover e lo switchback
- Utilizzare Gestione sistema in ONTAP 9.8 per lo switchover e lo switchback

Utilizzare Gestione sistema in ONTAP 9.7 per lo switchover e lo switchback

Fasi

1. Accedere a Gestore di sistema in ONTAP 9.7.
2. Fare clic su **(Torna alla versione classica)**.
3. Fare clic su **Configurazione > MetroCluster**.

   System Manager verifica se è possibile uno switchover negoziato.

4. Una volta completato il processo di convalida, eseguire una delle seguenti operazioni secondarie:
   a. Se la convalida non riesce, ma il sito B è attivo, si è verificato un errore. Ad esempio, potrebbe essersi verificato un problema con un sottosistema oppure il mirroring della NVRAM potrebbe non essere sincronizzato.
      i. Risolvere il problema che causa l'errore, fare clic su **Chiudi**, quindi ricominciare dalla fase 2.
      ii. Arrestare i nodi del sito B, fare clic su **Close** (Chiudi), quindi eseguire le operazioni descritte in "Esecuzione di uno switchover non pianificato".
   b. Se la convalida non riesce e il sito B è inattivo, molto probabilmente si è verificato un problema di connessione. Verificare che il sito B sia effettivamente inattivo, quindi eseguire le operazioni descritte in "Esecuzione di uno switchover non pianificato".
5. Fare clic su **Switchover from Site B to Site A** (passa da sito B a sito A) per avviare il processo di switchover.
6. Fare clic su **passa alla nuova esperienza**.

Utilizzare Gestione sistema in ONTAP 9.8 per lo switchover e lo switchback

Eseguire uno switchover pianificato (ONTAP 9.8)

Fasi

1. Accedere a Gestore di sistema in ONTAP 9.8.
2. Selezionare **Dashboard**. Nella sezione **MetroCluster**, i due cluster vengono visualizzati con una connessione.
3. Nel cluster locale (mostrato a sinistra), fare clic su ⋮ E selezionare **Switchover remote data Services to the local site**.

Una volta convalidata la richiesta di switchover, il controllo viene trasferito dal sito remoto al sito locale, che esegue le richieste di servizio dati per entrambi i cluster.

Il cluster remoto viene riavviato, ma i componenti dello storage non sono attivi e il cluster non risponde alle richieste di dati. È ora disponibile per la manutenzione pianificata.

> Il cluster remoto non deve essere utilizzato per la manutenzione dei dati fino a quando non viene eseguito uno switchback.

Eseguire uno switchover non pianificato (ONTAP 9.8)

ONTAP potrebbe avviare automaticamente uno switchover non pianificato. Se ONTAP non è in grado di determinare se è necessario uno switchback, l'amministratore di sistema del sito MetroCluster ancora in esecuzione avvia lo switchover seguendo questa procedura:

Fasi

1. Accedere a Gestore di sistema in ONTAP 9.8.
2. Selezionare **Dashboard**.

   Nella sezione **MetroCluster**, la connessione tra i due cluster viene visualizzata con una "X", il che significa che non è possibile rilevare una connessione. Le connessioni o il cluster non sono attivi.

3. Nel cluster locale (mostrato a sinistra), fare clic su ⋮ E selezionare **Switchover remote data Services to the local site**.

   Se lo switchover non riesce e viene visualizzato un errore, fare clic sul collegamento "View details" (Visualizza dettagli) nel messaggio di errore e confermare lo switchover non pianificato.

   Una volta convalidata la richiesta di switchover, il controllo viene trasferito dal sito remoto al sito locale, che esegue le richieste di servizio dati per entrambi i cluster.

   Il cluster deve essere riparato prima di essere nuovamente messo in linea.

> Una volta che il cluster remoto viene nuovamente messo in linea, non deve essere utilizzato per la manutenzione dei dati fino a quando non viene eseguito uno switchback.

Eseguire uno switchback (ONTAP 9.8)

Prima di iniziare

Che il cluster remoto sia stato inattivo a causa di manutenzione pianificata o a causa di un disastro, ora dovrebbe essere attivo e in attesa dello switchback.

Fasi

1. Nel cluster locale, accedere a Gestione sistema in ONTAP 9.8.
2. Selezionare **Dashboard**.

   Nella sezione **MetroCluster**, vengono visualizzati i due cluster.

3. Nel cluster locale (mostrato a sinistra), fare clic su ⋮ E selezionare **Take back control**.

   I dati vengono prima *guariti*, per garantire la sincronizzazione e il mirroring dei dati tra entrambi i cluster.

4. Una volta completata la riparazione dei dati, fare clic su ⋮ E selezionare **inizia switchback**.

   Una volta completato lo switchback, entrambi i cluster sono attivi e servono le richieste di dati. Inoltre, i dati vengono sottoposti a mirroring e sincronizzati tra i cluster.

Modificare l'indirizzo, la netmask e il gateway in un IP MetroCluster

A partire da ONTAP 9.10.1, è possibile modificare le seguenti proprietà di un'interfaccia IP MetroCluster: Indirizzo IP, maschera e gateway. È possibile utilizzare qualsiasi combinazione di parametri per l'aggiornamento.

Potrebbe essere necessario aggiornare queste proprietà, ad esempio, se viene rilevato un indirizzo IP duplicato o se un gateway deve essere modificato in caso di rete di livello 3 a causa di modifiche alla configurazione del router. È possibile modificare solo un'interfaccia alla volta. L'interfaccia verrà rallentata fino a quando le altre interfacce non saranno aggiornate e le connessioni non verranno ristabilita.

> È necessario apportare le modifiche a ciascuna porta. Analogamente, anche gli switch di rete devono aggiornare la configurazione. Ad esempio, se il gateway viene aggiornato, idealmente viene modificato su entrambi i nodi di una coppia ha, poiché sono identici. Inoltre, anche lo switch connesso a tali nodi deve aggiornare il gateway.

Fase

Aggiornare l'indirizzo IP, la netmask e il gateway per ogni nodo e interfaccia.

Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster

A partire da ONTAP 9.8, Gestione sistema monitora lo stato delle configurazioni di IP MetroCluster e aiuta a identificare e correggere i problemi che potrebbero verificarsi.

Panoramica della verifica dello stato di salute di MetroCluster

System Manager verifica periodicamente lo stato della configurazione di IP MetroCluster. Quando si visualizza la sezione MetroCluster nella dashboard, di solito viene visualizzato il messaggio "i sistemi MetroCluster sono integri".

Tuttavia, quando si verifica un problema, il messaggio mostra il numero di eventi. È possibile fare clic sul messaggio e visualizzare i risultati del controllo dello stato di salute dei seguenti componenti:

- Nodo
- Interfaccia di rete
- Tier (storage)
- Cluster
- Connessione
- Volume
- Replica della configurazione

La colonna **Status** (Stato) identifica i componenti che presentano problemi e la colonna **Details** (Dettagli) suggerisce come risolvere il problema.

Risoluzione dei problemi di MetroCluster

Fasi

1. In System Manager, selezionare **Dashboard**.
2. Nella sezione **MetroCluster**, osservare il messaggio.
   a. Se il messaggio indica che la configurazione di MetroCluster è in buone condizioni e che le connessioni tra i cluster e il mediatore ONTAP sono in buone condizioni (visualizzate con segni di spunta), non si verificano problemi per la correzione.
   b. Se il messaggio elenca il numero di eventi o le connessioni sono scollegate (indicate con una "X"), passare alla fase successiva.
3. Fare clic sul messaggio che mostra il numero di eventi.

   Viene visualizzato il report sullo stato di salute di MetroCluster.

4. Risolvere i problemi visualizzati nel report utilizzando i suggerimenti nella colonna **Dettagli**.
5. Una volta risolti tutti i problemi, fare clic su **Controlla lo stato di salute di MetroCluster**.

   > La verifica dello stato di salute di MetroCluster utilizza una quantità elevata di risorse, pertanto si consiglia di eseguire tutte le attività di risoluzione dei problemi prima di eseguire il controllo.

   Il controllo dello stato di salute di MetroCluster viene eseguito in background. È possibile lavorare su altre attività mentre si attende il completamento.

Protezione dei dati mediante backup su nastro

Panoramica del backup su nastro dei volumi FlexVol

ONTAP supporta il backup e il ripristino su nastro attraverso il protocollo di gestione dei dati di rete (NDMP). NDMP consente di eseguire il backup dei dati nei sistemi storage direttamente su nastro, con un utilizzo efficiente della larghezza di banda della rete. ONTAP supporta motori di dump e SMTape per il backup su nastro.

È possibile eseguire un dump o un backup o ripristino SMTape utilizzando applicazioni di backup conformi a NDMP. È supportata solo la versione 4 di NDMP.

Backup su nastro con dump

Dump è un backup basato su copia Snapshot in cui viene eseguito il backup dei dati del file system su nastro. Il motore di dump ONTAP esegue il backup su nastro di file, directory e le informazioni dell'elenco di controllo di accesso (ACL) applicabili. È possibile eseguire il backup di un intero volume, di un intero qtree o di un sottoalbero che non sia un intero volume o un intero qtree. Dump supporta backup baseline, differenziali e incrementali.

Backup su nastro con SMTape

SMTape è una soluzione di disaster recovery basata su copia Snapshot di ONTAP che esegue il backup di blocchi di dati su nastro. È possibile utilizzare SMTape per eseguire backup dei volumi su nastri. Tuttavia, non è possibile eseguire un backup a livello di qtree o sottostruttura. SMTape supporta backup baseline,

differenziali e incrementali.

A partire da ONTAP 9.13.1, il backup su nastro con SMTape supporta Continuità aziendale di SnapMirror.

Workflow di backup e ripristino su nastro

È possibile eseguire operazioni di backup e ripristino su nastro utilizzando un'applicazione di backup abilitata per NDMP.

A proposito di questa attività

Il flusso di lavoro di backup e ripristino su nastro offre una panoramica delle attività coinvolte nell'esecuzione delle operazioni di backup e ripristino su nastro. Per informazioni dettagliate sull'esecuzione di un'operazione di backup e ripristino, consultare la documentazione dell'applicazione di backup.

Fasi

1. Configurare una libreria di nastri scegliendo una topologia a nastro supportata da NDMP.
2. Abilitare i servizi NDMP sul sistema storage.

   È possibile attivare i servizi NDMP a livello di nodo o di SVM (Storage Virtual Machine). Questo dipende dalla modalità NDMP in cui si sceglie di eseguire l'operazione di backup e ripristino su nastro.

3. Utilizza le opzioni NDMP per gestire NDMP sul tuo sistema storage.

   È possibile utilizzare le opzioni NDMP a livello di nodo o SVM. Questo dipende dalla modalità NDMP in cui si sceglie di eseguire l'operazione di backup e ripristino su nastro.

   È possibile modificare le opzioni NDMP a livello di nodo utilizzando `system services ndmp modify` E a livello di SVM utilizzando `vserver services ndmp modify` comando. Per ulteriori informazioni su questi comandi, consulta le pagine man.

4. Eseguire un'operazione di backup o ripristino su nastro utilizzando un'applicazione di backup abilitata per NDMP.

   ONTAP supporta motori di dump e SMTape per backup e ripristino su nastro.

   Per ulteriori informazioni sull'utilizzo dell'applicazione di backup (denominata anche *applicazioni di gestione dei dati* o *DMA*) per eseguire operazioni di backup o ripristino, consultare la documentazione dell'applicazione di backup.

Informazioni correlate

Topologie comuni di backup su nastro NDMP

Comprendere il motore di dump per i volumi FlexVol

Casi di utilizzo per la scelta di un motore di backup su nastro

ONTAP supporta due motori di backup: SMTape e dump. È necessario conoscere i casi di utilizzo dei motori di backup SMTape e dump per scegliere il motore di backup per eseguire le operazioni di backup e ripristino su nastro.

Il dump può essere utilizzato nei seguenti casi:

- Direct Access Recovery (DAR) di file e directory
- Backup di un sottoinsieme di sottodirectory o file in un percorso specifico
- Esclusione di file e directory specifici durante i backup
- Conservazione del backup per lunghi periodi di tempo

SMTape può essere utilizzato nei seguenti casi:

- Soluzione di disaster recovery
- Preservando i risparmi di deduplica e le impostazioni di deduplica sui dati di cui è stato eseguito il backup durante un'operazione di ripristino
- Backup di grandi volumi

Gestire le unità a nastro

Panoramica sulla gestione delle unità a nastro

Prima di eseguire un'operazione di backup o ripristino su nastro, è possibile verificare le connessioni della libreria di nastri e visualizzare le informazioni sul disco a nastro. È possibile utilizzare un'unità a nastro non qualificata emulando questa unità a nastro in un'unità a nastro qualificata. Oltre a visualizzare gli alias esistenti, è anche possibile assegnare e rimuovere gli alias del nastro.

Quando si esegue il backup dei dati su nastro, i dati vengono memorizzati in file su nastro. I contrassegni dei file separano i file del nastro e non hanno nomi. Specificare un file nastro in base alla posizione sul nastro. Si scrive un file su nastro utilizzando un dispositivo a nastro. Quando si legge il file su nastro, è necessario specificare un dispositivo con lo stesso tipo di compressione utilizzato per scrivere il file su nastro.

Comandi per la gestione delle unità a nastro, dei media changer e delle operazioni del disco a nastro

Sono disponibili comandi per visualizzare le informazioni relative alle unità a nastro e ai media changer in un cluster, portare un'unità a nastro online e portarla fuori linea, modificare la posizione della cartuccia dell'unità a nastro, impostare e cancellare il nome alias dell'unità a nastro e reimpostare un'unità a nastro. È inoltre possibile visualizzare e ripristinare le statistiche del disco a nastro.

Se si desidera…	Utilizzare questo comando…
Portare online un'unità a nastro	`storage tape online`
Cancellare un nome alias per l'unità a nastro o il caricatore di supporti	`storage tape alias clear`
Attivare o disattivare un'operazione di traccia su nastro per un'unità a nastro	`storage tape trace`
Modificare la posizione della cartuccia del disco a nastro	`storage tape position`

Se si desidera…	Utilizzare questo comando…
Ripristinare un'unità a nastro	`storage tape reset` Questo comando è disponibile solo a livello di privilegi avanzati.
Impostare un nome alias per l'unità a nastro o il caricatore di supporti	`storage tape alias set`
Portare un'unità a nastro offline	`storage tape offline`
Visualizza informazioni su tutte le unità a nastro e i media changer	`storage tape show`
Visualizzare le informazioni sulle unità a nastro collegate al cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Consente di visualizzare informazioni sui media changer collegati al cluster	`storage tape show-media-changer`
Visualizzare le informazioni sugli errori relativi alle unità a nastro collegate al cluster	`storage tape show-errors`
Visualizza tutte le unità a nastro qualificate e supportate da ONTAP collegate a ciascun nodo del cluster	`storage tape show-supported-status`
Visualizzare gli alias di tutte le unità a nastro e i media changer collegati a ciascun nodo del cluster	`storage tape alias show`
Azzerare le statistiche di lettura di un'unità a nastro	`storage stats tape zero tape_name` Devi usare questo comando al nodeshell.
Visualizza le unità a nastro supportate da ONTAP	`storage show tape supported [-v]` Devi usare questo comando al nodeshell. È possibile utilizzare `-v` per visualizzare ulteriori dettagli su ciascuna unità a nastro.
Visualizzare le statistiche dei dispositivi a nastro per comprendere le prestazioni dei nastri e verificare il modello di utilizzo	`storage stats tape tape_name` Devi usare questo comando al nodeshell.

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Utilizzare un'unità a nastro non qualificata

È possibile utilizzare un'unità a nastro non qualificata su un sistema storage se è in grado di emulare un'unità a nastro qualificata. Viene quindi trattato come un'unità a nastro qualificata. Per utilizzare un'unità a nastro non qualificata, è necessario prima determinare se emula una delle unità a nastro qualificate.

A proposito di questa attività

Un'unità a nastro non qualificata è collegata al sistema di storage, ma non è supportata o riconosciuta da ONTAP.

Fasi

1. Visualizzare le unità a nastro non qualificate collegate a un sistema di storage utilizzando `storage tape show-supported-status` comando.

   Il seguente comando visualizza le unità a nastro collegate al sistema di storage e lo stato di supporto e qualifica di ciascuna unità a nastro. Vengono inoltre elencate le unità a nastro non qualificate. `tape_drive_vendor_name` È un'unità a nastro non qualificata collegata al sistema di storage, ma non supportata da ONTAP.

   ```
   cluster1::> storage tape show-supported-status -node Node1

             Node: Node1
                                       Is
             Tape Drive                Supported  Support Status
             --------------------      ---------  --------------
             "tape_drive_vendor_name"  false      Nonqualified tape drive
             Hewlett-Packard C1533A    true       Qualified
             Hewlett-Packard C1553A    true       Qualified
             Hewlett-Packard Ultrium 1 true       Qualified
             Sony SDX-300C             true       Qualified
             Sony SDX-500C             true       Qualified
             StorageTek T9840C         true       Dynamically Qualified
             StorageTek T9840D         true       Dynamically Qualified
             Tandberg LTO-2 HH         true       Dynamically Qualified
   ```

2. Emulare l'unità a nastro qualificata.

   "Download NetApp: File di configurazione dei dispositivi su nastro"

Informazioni correlate

Quali sono le unità a nastro qualificate

Assegnare alias nastro

Per una facile identificazione del dispositivo, è possibile assegnare alias del nastro a un'unità a nastro o a un caricatore di supporti. Gli alias forniscono una corrispondenza tra i nomi logici dei dispositivi di backup e un nome assegnato in modo permanente all'unità

a nastro o al caricatore di supporti.

Fasi

1. Assegnare un alias a un'unità a nastro o a un caricatore di supporti utilizzando `storage tape alias set` comando.

   Per ulteriori informazioni su questo comando, vedere le pagine man.

   È possibile visualizzare le informazioni sul numero di serie (SN) delle unità a nastro utilizzando `system node hardware tape drive show` e informazioni sulle librerie di nastri utilizzando `system node hardware tape library show` comandi.

   Il seguente comando imposta un nome alias su un'unità a nastro con numero di serie SN[123456]L4 collegato al nodo, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name st3
   -mapping SN[123456]L4
   ```

   Il seguente comando imposta un nome alias su un media changer con numero di serie SN[65432] collegato al nodo, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name mc1
   -mapping SN[65432]
   ```

Informazioni correlate

Che cos'è l'aliasing su nastro

Rimozione degli alias del nastro

Rimuovere gli alias del nastro

È possibile rimuovere gli alias utilizzando `storage tape alias clear` comando quando gli alias persistenti non sono più necessari per un'unità a nastro o un dispositivo di sostituzione del supporto.

Fasi

1. Rimuovere un alias da un'unità a nastro o da un caricatore di supporti utilizzando `storage tape alias clear` comando.

   Per ulteriori informazioni su questo comando, vedere le pagine man.

   Il seguente comando rimuove gli alias di tutte le unità a nastro specificando l'ambito dell'operazione di cancellazione alias in `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Al termine

Se si esegue un'operazione di backup o ripristino su nastro utilizzando NDMP, dopo aver rimosso un alias da un'unità a nastro o da un caricatore di supporti, è necessario assegnare un nuovo nome alias all'unità a nastro o al caricatore di supporti per continuare l'accesso al dispositivo a nastro.

Informazioni correlate

Che cos'è l'aliasing su nastro

Assegnazione degli alias del nastro

Attivazione o disattivazione delle prenotazioni su nastro

È possibile controllare il modo in cui ONTAP gestisce le prenotazioni dei dispositivi a nastro utilizzando `tape.reservations` opzione. Per impostazione predefinita, la prenotazione su nastro è disattivata.

A proposito di questa attività

L'attivazione dell'opzione di riserva dei nastri può causare problemi se le unità a nastro, i media Changer, i bridge o le librerie non funzionano correttamente. Se i comandi su nastro indicano che il dispositivo è riservato quando nessun altro sistema di storage sta utilizzando il dispositivo, questa opzione deve essere disattivata.

Fasi

1. Per utilizzare il meccanismo SCSI Reserve/Release o SCSI Persistent Reservationsor per disattivare le prenotazioni su nastro, immettere il seguente comandonella shell del clustershell:

   ```
   options -option-name tape.reservations -option-value {scsi | persistent | off}
   ```

   `scsi` Seleziona il meccanismo SCSI Reserve/Release.

   `persistent` Seleziona le prenotazioni persistenti SCSI.

   `off` disattiva le prenotazioni su nastro.

Informazioni correlate

Quali sono le prenotazioni su nastro

Comandi per la verifica delle connessioni della libreria di nastri

È possibile visualizzare informazioni sul percorso di connessione tra un sistema di storage e una configurazione della libreria di nastri collegata al sistema di storage. È possibile utilizzare queste informazioni per verificare il percorso di connessione alla configurazione della libreria di nastri o per la risoluzione dei problemi relativi ai percorsi di connessione.

È possibile visualizzare i seguenti dettagli della libreria di nastri per verificare le connessioni della libreria di nastri dopo l'aggiunta o la creazione di una nuova libreria di nastri o dopo il ripristino di un percorso guasto in un accesso a percorso singolo o multipath a una libreria di nastri. È inoltre possibile utilizzare queste informazioni durante la risoluzione di errori relativi al percorso o in caso di errore nell'accesso a una libreria di nastri.

- Nodo a cui è collegata la libreria di nastri

- ID dispositivo
- Percorso NDMP
- Nome della libreria di nastri
- Porta di destinazione e ID porta iniziatore
- Accesso a percorso singolo o multipath a una libreria di nastri per ogni porta di destinazione o FC Initiator
- Dettagli sull'integrità dei dati relativi al percorso, ad esempio "Path Errors" e "Path Qual"
- Gruppi LUN e conteggi LUN

Se si desidera…	Utilizzare questo comando…
Consente di visualizzare informazioni su una libreria di nastri in un cluster	`system node hardware tape library show`
Visualizzare le informazioni sul percorso di una libreria di nastri	`storage tape library path show`
Visualizzare le informazioni sul percorso di una libreria di nastri per ogni porta di iniziatore	`storage tape library path show-by-initiator`
Visualizzare le informazioni di connettività tra una libreria di nastri di storage e il cluster	`storage tape library config show`

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Informazioni sulle unità a nastro

Panoramica delle unità a nastro qualificate

È necessario utilizzare un'unità a nastro qualificata che sia stata testata e che funzioni correttamente su un sistema di storage. È possibile seguire l'aliasing del nastro e abilitare anche le prenotazioni su nastro per garantire che un solo sistema storage acceda a un'unità a nastro in qualsiasi momento.

Un'unità a nastro qualificata è un'unità a nastro che è stata testata e che funziona correttamente sui sistemi di storage. È possibile qualificare le unità a nastro per le release ONTAP esistenti utilizzando il file di configurazione del nastro.

Formato del file di configurazione del nastro

Il formato del file di configurazione del nastro è costituito da campi quali ID vendor, ID prodotto e dettagli sui tipi di compressione per un'unità a nastro. Questo file è inoltre costituito da campi facoltativi per l'abilitazione della funzione di caricamento automatico di un'unità a nastro e la modifica dei valori di timeout dei comandi di un'unità a nastro.

Nella tabella seguente viene visualizzato il formato del file di configurazione del nastro:

Elemento	Dimensione	Descrizione
`vendor_id` (stringa)	fino a 8 byte	L'ID del vendor come riportato da `SCSI Inquiry` comando.
`product_id`(stringa)	fino a 16 byte	L'ID del prodotto riportato da `SCSI Inquiry` comando.
`id_match_size`(numero)		Il numero di byte dell'ID prodotto da utilizzare per la corrispondenza per rilevare l'unità a nastro da identificare, iniziando dal primo carattere dell'ID prodotto nei dati della richiesta.
`vendor_pretty` (stringa)	fino a 16 byte	Se questo parametro è presente, viene specificato dalla stringa visualizzata dal comando, `storage tape show -device -names`; In caso contrario, viene visualizzato INQ_VENDOR_ID.
`product_pretty`(stringa)	fino a 16 byte	Se questo parametro è presente, viene specificato dalla stringa visualizzata dal comando, `storage tape show -device -names`; In caso contrario, viene visualizzato INQ_PRODUCT_ID.

Il `vendor_pretty` e. `product_pretty` i campi sono facoltativi, ma se uno di questi campi ha un valore, anche l'altro deve avere un valore.

La seguente tabella illustra la descrizione, il codice di densità e l'algoritmo di compressione per i vari tipi di compressione, ad esempio `l`, `m`, `h`, e. `a`:

Elemento	Dimensione	Descrizione
`{l	m	h
a}_description=(string)`	fino a 24 byte	La stringa da stampare per il comando nodeshell, `sysconfig -t`, che descrive le caratteristiche della particolare impostazione di densità.
`{l	m	h

Elemento	Dimensione	Descrizione
a}_density=(hex codes)`		Il codice di densità da impostare nel descrittore di blocco di pagina di modalità SCSI corrispondente al codice di densità desiderato per l, m, h o a.
`{l	m	h
a}_algorithm=(hex codes)`		L'algoritmo di compressione da impostare nella pagina SCSI Compression Mode (modalità di compressione SCSI) corrispondente al codice di densità e alla caratteristica di densità desiderata.

La seguente tabella descrive i campi opzionali disponibili nel file di configurazione del nastro:

Campo	Descrizione
`autoload=(Boolean yes/no)`	Questo campo è impostato su `yes` se l'unità a nastro dispone di una funzione di caricamento automatico, ovvero dopo l'inserimento della cartuccia a nastro, l'unità a nastro diventa pronta senza eseguire un `SCSI load` (unità di avvio/arresto). L'impostazione predefinita per questo campo è `no`.
`cmd_timeout_0x`	Singolo valore di timeout. È necessario utilizzare questo campo solo se si desidera specificare un valore di timeout diverso da quello utilizzato per impostazione predefinita dal driver del nastro. Il file di esempio elenca i valori di timeout dei comandi SCSI predefiniti utilizzati dall'unità a nastro. Il valore di timeout può essere espresso in minuti (m), secondi (s) o millisecondi (ms). Non modificare questo campo.

È possibile scaricare e visualizzare il file di configurazione del nastro dal NetApp Support Site.

Esempio di un formato di file di configurazione del nastro

Il formato del file di configurazione del nastro per l'unità a nastro HP LTO5 ULTRIUM è il seguente:

`vendor_id`="HP"

`product_id`="Ultrium 5-SCSI"

`id_match_size`=9

`vendor_pretty`="Hewlett-Packard"

`product_pretty`="LTO-5"

`l_description`="LTO-3(ro)/4 4/800 GB"

`l_density`=0x00

`l_algorithm`=0x00

`m_description`="lto-3(ro)/4 8/1600 GB cmp"

`m_density`=0x00

`m_algorithm`=0x01

`h_description`="LTO-5 1600 GB"

`h_density`=0x58

`h_algorithm`=0x00

`a_description`="lto-5 3200gb cmp"

`a_density`=0x58

`a_algorithm`=0x01

`autoload`="sì"

Informazioni correlate

"NetApp Tools: File di configurazione dei dispositivi su nastro"

In che modo il sistema storage qualifica dinamicamente una nuova unità a nastro

Il sistema storage qualifica dinamicamente un'unità a nastro associando l'ID del vendor e l'ID del prodotto alle informazioni contenute nella tabella di qualificazione del nastro.

Quando si collega un'unità a nastro al sistema di storage, viene eseguita la ricerca di una corrispondenza tra l'ID del vendor e l'ID del prodotto tra le informazioni ottenute durante il rilevamento del nastro e le informazioni contenute nella tabella di qualificazione del nastro interno. Se il sistema storage rileva una corrispondenza, contrassegna l'unità a nastro come qualificata e può accedere all'unità a nastro. Se il sistema di storage non riesce a trovare una corrispondenza, l'unità a nastro rimane nello stato non qualificato e non viene effettuato l'accesso.

Panoramica dei dispositivi a nastro

Panoramica dei dispositivi a nastro

Un dispositivo a nastro è una rappresentazione di un'unità a nastro. Si tratta di una combinazione specifica di tipo di rewind e funzionalità di compressione di un'unità a nastro.

Viene creato un dispositivo a nastro per ogni combinazione di tipo di rewind e funzionalità di compressione. Pertanto, un'unità a nastro o una libreria a nastro possono essere associati a diversi dispositivi a nastro. È necessario specificare un dispositivo a nastro per spostare, scrivere o leggere i nastri.

Quando si installa un'unità a nastro o una libreria di nastri su un sistema di storage, ONTAP crea dispositivi a nastro associati all'unità a nastro o alla libreria di nastri.

ONTAP rileva le unità a nastro e le librerie a nastro e assegna loro numeri logici e dispositivi a nastro. ONTAP rileva le librerie e le unità a nastro Fibre Channel, SAS e SCSI parallele quando sono collegate alle porte di interfaccia. ONTAP rileva questi dischi quando le interfacce sono attivate.

Formato del nome del dispositivo a nastro

A ciascuna periferica a nastro è associato un nome che viene visualizzato in un formato definito. Il formato include informazioni sul tipo di dispositivo, sul tipo di riavvolgimento, sull'alias e sul tipo di compressione.

Il formato del nome di un dispositivo a nastro è il seguente:

`rewind_type st alias_number compression_type`

`rewind_type` è il tipo di riavvolgimento.

Il seguente elenco descrive i diversi valori del tipo di riavvolgimento:

- **r**

  ONTAP riavvolge il nastro al termine della scrittura del file.

- **nr**

  ONTAP non riavvolge il nastro al termine della scrittura del file. È necessario utilizzare questo tipo di riavvolgimento quando si desidera scrivere più file su nastro sullo stesso nastro.

- **ur**

  Questo è il tipo di riavvolgimento di scaricamento/ricarica. Quando si utilizza questo tipo di riavvolgimento, la libreria di nastri scarica il nastro quando raggiunge la fine di un file di nastro, quindi carica il nastro successivo, se presente.

  È necessario utilizzare questo tipo di riavvolgimento solo nei seguenti casi:

  - L'unità a nastro associata a questo dispositivo si trova in una libreria di nastri o in un caricatore di supporti che si trova in modalità di libreria.
  - L'unità a nastro associata a questo dispositivo è collegata a un sistema di storage.
  - Nella sequenza di nastri della libreria definita per questa unità a nastro sono disponibili nastri sufficienti per l'operazione che si sta eseguendo.

> Se si registra un nastro utilizzando un dispositivo senza riavvolgimento, è necessario riavvolgere il nastro prima di leggerlo.

`st` è la designazione standard per un'unità a nastro.

`alias_number` È l'alias assegnato da ONTAP all'unità a nastro. Quando ONTAP rileva una nuova unità a nastro, ONTAP assegna un alias all'unità a nastro.

`compression_type` è un codice specifico del disco per la densità dei dati sul nastro e il tipo di compressione.

L'elenco seguente descrive i vari valori per `compression_type`:

- **a**

  Compressione massima

- **h**

  Compressione elevata

- **m**

  Compressione media

- **l**

  Compressione bassa

Esempi

`nrst0a` specifica un dispositivo no-rewind sull'unità a nastro 0 utilizzando la compressione più elevata.

Esempio di un elenco di dispositivi a nastro

L'esempio seguente mostra i dispositivi a nastro associati a HP Ultrium 2-SCSI:

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
nrst0a -  no rewind device,     format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

L'elenco seguente descrive le abbreviazioni dell'esempio precedente:

- GB—Gigabyte; questa è la capacità del nastro.
- w/comp—con compressione; indica la capacità del nastro con compressione.

Numero supportato di dispositivi a nastro simultanei

ONTAP supporta un massimo di 64 connessioni simultanee a unità a nastro, 16 media changer e 16 dispositivi bridge o router per ciascun sistema storage (per nodo) in qualsiasi combinazione di collegamenti Fibre Channel, SCSI o SAS.

I dischi a nastro o i media changer possono essere dispositivi in librerie di nastri fisiche o virtuali o dispositivi standalone.

> Sebbene un sistema storage sia in grado di rilevare 64 connessioni a unità a nastro, il numero massimo di sessioni di backup e ripristino che possono essere eseguite contemporaneamente dipende dai limiti di scalabilità del motore di backup.

Informazioni correlate

Limiti di scalabilità per sessioni di dump backup e ripristino

Aliasing del nastro

Panoramica dell'aliasing su nastro

L'aliasing semplifica il processo di identificazione dei dispositivi. L'aliasing associa un nome di percorso fisico (PPN) o un numero di serie (SN) di un nastro o di un media changer a un nome alias persistente ma modificabile.

La seguente tabella descrive in che modo l'aliasing del nastro consente di garantire che un'unità a nastro (o una libreria di nastri o un caricatore di supporti) sia sempre associata a un singolo alias:

Scenario	Riassegnazione dell'alias
Al riavvio del sistema	L'alias precedente viene riassegnato automaticamente all'unità a nastro.
Quando un dispositivo a nastro si sposta su un'altra porta	L'alias può essere regolato in modo da puntare al nuovo indirizzo.
Quando più di un sistema utilizza un particolare dispositivo a nastro	L'utente può impostare lo stesso alias per tutti i sistemi.

> Quando si esegue l'aggiornamento da Data ONTAP 8.1.x a Data ONTAP 8.2.x, la funzione di alias del nastro di Data ONTAP 8.2.x modifica i nomi degli alias del nastro esistenti. In tal caso, potrebbe essere necessario aggiornare i nomi alias del nastro nell'applicazione di backup.

L'assegnazione degli alias del nastro fornisce una corrispondenza tra i nomi logici dei dispositivi di backup (ad esempio, st0 o mc1) e un nome assegnato in modo permanente a una porta, un'unità a nastro o un dispositivo di sostituzione del supporto.

> st0 e st00 sono nomi logici diversi.

> I nomi logici e i numeri di serie vengono utilizzati solo per accedere a una periferica. Una volta effettuato l'accesso alla periferica, vengono visualizzati tutti i messaggi di errore utilizzando il nome del percorso fisico.

Sono disponibili due tipi di nomi per l'aliasing: Nome del percorso fisico e numero di serie.

Quali sono i nomi dei percorsi fisici

I nomi dei percorsi fisici (PPN) sono le sequenze di indirizzi numerici che ONTAP assegna alle unità a nastro e alle librerie a nastro in base all'adattatore o allo switch SCSI-2/3 (posizione specifica) che sono collegati al sistema di storage. Le PPN sono anche note come nomi elettrici.

Le PPN dei dispositivi direct-attached utilizzano il seguente formato: `host_adapter. device_id_lun`

> Il valore del LUN viene visualizzato solo per i dispositivi a nastro e a media unità di sostituzione i cui valori LUN non sono pari a zero, ovvero se il valore del LUN è pari a zero `lun` Parte della PPN non viene visualizzata.

Ad esempio, il codice PPN 8.6 indica che il numero dell'adattatore host è 8, l'ID del dispositivo è 6 e il numero dell'unità logica (LUN) è 0.

I dispositivi a nastro SAS sono anche dispositivi a collegamento diretto. Ad esempio, il codice PPN 5c.4 indica che in un sistema storage l'HBA SAS è collegato nello slot 5, il nastro SAS è collegato alla porta C dell'HBA SAS e l'ID dispositivo è 4.

Le PPN dei dispositivi collegati a switch Fibre Channel utilizzano il seguente formato: `switch:port_id. device_id_lun`

Ad esempio, PPN MY_SWITCH:5.3L2 indica che l'unità a nastro collegata alla porta 5 di uno switch chiamato MY_SWITCH è impostata con l'ID dispositivo 3 e dispone del LUN 2.

Il LUN (Logical Unit Number) è determinato dal disco. Le librerie e le unità a nastro Fibre Channel, SCSI e i dischi dispongono di PPN.

Le PPN delle unità a nastro e delle librerie non cambiano a meno che il nome dello switch non venga modificato, l'unità a nastro o la libreria non venga spostata o l'unità a nastro o la libreria non venga riconfigurata. Le PPN rimangono invariate dopo il riavvio. Ad esempio, se un'unità a nastro denominata MY_SWITCH:5.3L2 viene rimossa e una nuova unità a nastro con lo stesso ID dispositivo e LUN viene collegata alla porta 5 dello switch MY_SWITCH, la nuova unità a nastro sarà accessibile utilizzando MY_SWITCH:5.3L2.

Quali sono i numeri di serie

Un numero di serie (SN) è un identificatore univoco per un'unità a nastro o un dispositivo di sostituzione del supporto. ONTAP genera alias in base al numero di serie anziché al numero di serie.

Poiché SN è un identificatore univoco per un'unità a nastro o un caricatore di supporti, l'alias rimane lo stesso indipendentemente dai percorsi di connessione multipli all'unità a nastro o al caricatore di supporti. Ciò consente ai sistemi storage di tenere traccia dello stesso disco a nastro o del caricatore di supporti in una configurazione di libreria di nastri.

Il numero di serie di un'unità a nastro o di un caricatore di supporti non cambia anche se si rinomina lo switch Fibre Channel a cui è collegato l'unità a nastro o il caricatore di supporti. Tuttavia, in una libreria di nastri se si sostituisce un'unità a nastro esistente con una nuova, ONTAP genera nuovi alias a causa della modifica del numero di serie dell'unità a nastro. Inoltre, se si sposta un'unità a nastro esistente in un nuovo slot di una libreria di nastri o si rimappano le LUN dell'unità a nastro, ONTAP genera un nuovo alias per tale unità a nastro.

È necessario aggiornare le applicazioni di backup con gli alias appena generati.

Il numero di serie di un dispositivo a nastro utilizza il seguente formato: `SN[xxxxxxxxxx]L[X]`

`x` È un carattere alfanumerico e `LX` È il LUN del dispositivo a nastro. Se il LUN è 0, il valore `LX` parte della stringa non viene visualizzata.

Ogni SN è composto da un massimo di 32 caratteri; il formato per il SN non è sensibile al maiuscolo/minuscolo.

Considerazioni per la configurazione dell'accesso su nastro multipath

È possibile configurare due percorsi dal sistema di storage per accedere alle unità a nastro in una libreria di nastri. In caso di guasto di un percorso, il sistema di storage può utilizzare gli altri percorsi per accedere alle unità a nastro senza dover riparare immediatamente il percorso guasto. In questo modo è possibile riavviare le operazioni su nastro.

Quando si configura l'accesso su nastro multipath dal sistema storage, è necessario prendere in considerazione quanto segue:

- Nelle librerie su nastro che supportano la mappatura LUN, per l'accesso multipath a un gruppo LUN, la mappatura LUN deve essere simmetrica su ciascun percorso.

  Le unità a nastro e i media changer vengono assegnati ai gruppi LUN (set di LUN che condividono lo stesso set di percorsi iniziatori) in una libreria di nastri. Tutte le unità a nastro di un gruppo LUN devono essere disponibili per le operazioni di backup e ripristino su tutti i percorsi multipli.

- È possibile configurare un massimo di due percorsi dal sistema di storage per accedere alle unità a nastro in una libreria di nastri.
- L'accesso su nastro multipath supporta il bilanciamento del carico. Il bilanciamento del carico è disattivato per impostazione predefinita.

Nell'esempio seguente, il sistema di storage accede al gruppo LUN 0 attraverso due percorsi iniziatori: 0b e 0d. In entrambi i percorsi, il gruppo LUN ha lo stesso numero LUN, 0, e numero LUN, 5. Il sistema storage accede al gruppo LUN 1 attraverso un solo percorso iniziatore, 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                     LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Per ulteriori informazioni, consulta le pagine man.

Come aggiungere unità nastro e librerie ai sistemi storage

È possibile aggiungere dischi a nastro e librerie al sistema di storage in modo dinamico (senza interrompere la linea del sistema).

Quando si aggiunge un nuovo media changer, il sistema storage rileva la sua presenza e la aggiunge alla configurazione. Se nelle informazioni alias si fa già riferimento al caricatore di supporti, non vengono creati nuovi nomi logici. Se non si fa riferimento alla libreria, il sistema di storage crea un nuovo alias per il dispositivo di modifica del supporto.

Nella configurazione di una libreria di nastri, è necessario configurare un'unità a nastro o un caricatore di supporti sul LUN 0 di una porta di destinazione affinché ONTAP rilevi tutti i caricatori di supporti e le unità a nastro sulla porta di destinazione.

Quali sono le prenotazioni su nastro

Più sistemi storage possono condividere l'accesso a unità nastro, media changer, bridge o librerie di nastri. Le prenotazioni su nastro garantiscono che un solo sistema storage acceda a un dispositivo in qualsiasi momento, attivando il meccanismo SCSI Reserve/Release o SCSI Persistent Reservations per tutte le unità nastro, i media changer, i bridge e le librerie di nastri.

> Tutti i sistemi che condividono i dispositivi in una libreria, indipendentemente dal fatto che gli switch siano coinvolti o meno, devono utilizzare lo stesso metodo di prenotazione.

Il meccanismo SCSI Reserve/Release per riservare i dispositivi funziona bene in condizioni normali. Tuttavia, durante le procedure di ripristino degli errori dell'interfaccia, le riserve possono andare perse. In questo caso, gli iniziatori diversi dal proprietario riservato possono accedere al dispositivo.

Le prenotazioni effettuate con le prenotazioni persistenti SCSI non sono influenzate dai meccanismi di recupero degli errori, come la reimpostazione del loop o la reimpostazione della destinazione; tuttavia, non tutti

i dispositivi implementano correttamente le prenotazioni persistenti SCSI.

Trasferire i dati utilizzando ndmpcopy

Trasferire i dati utilizzando la panoramica di ndmpcopy

Il `ndmpcopy` Il comando nodeshell trasferisce i dati tra sistemi storage che supportano NDMP v4. È possibile eseguire trasferimenti di dati completi e incrementali. È possibile trasferire volumi completi o parziali, qtree, directory o singoli file.

A proposito di questa attività

Utilizzando ONTAP 8.x e le versioni precedenti, i trasferimenti incrementali sono limitati a un massimo di due livelli (uno completo e fino a due backup incrementali).

A partire da ONTAP 9.0 e versioni successive, i trasferimenti incrementali sono limitati a un massimo di nove livelli (un backup completo e fino a nove backup incrementali).

Puoi correre `ndmpcopy` alla riga di comando nodeshell dei sistemi storage di origine e di destinazione, o a un sistema storage che non è né l'origine né la destinazione del trasferimento dei dati. Puoi anche correre `ndmpcopy` su un singolo sistema storage che sia l'origine e la destinazione del trasferimento dei dati.

È possibile utilizzare gli indirizzi IPv4 o IPv6 dei sistemi di storage di origine e di destinazione in `ndmpcopy` comando. Il formato del percorso è `/vserver_name/volume_name \[path\]`.

Fasi

1. Abilitare il servizio NDMP sui sistemi storage di origine e di destinazione:

Se si esegue il trasferimento dei dati all'origine o alla destinazione in…	Utilizzare il seguente comando…
Modalità NDMP con ambito SVM	`vserver services ndmp on` Per l'autenticazione NDMP nella SVM amministrativa, l'account utente è `admin` e il ruolo dell'utente è `admin` oppure `backup`. Nel SVM dei dati, l'account utente è `vsadmin` e il ruolo dell'utente è `vsadmin` oppure `vsadmin-backup` ruolo.
Modalità NDMP con ambito nodo	`system services ndmp on`

2. Trasferire i dati all'interno di un sistema storage o tra sistemi storage utilizzando `ndmpcopy` comando al nodeshell:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

> I nomi DNS non sono supportati in ndmpcopy. Specificare l'indirizzo IP dell'origine e della destinazione. L'indirizzo loopback (127.0.0.1) non è supportato per l'indirizzo IP di origine o di destinazione.

- Il `ndmpcopy` il comando determina la modalità degli indirizzi per le connessioni di controllo come segue:
  - La modalità indirizzo per la connessione di controllo corrisponde all'indirizzo IP fornito.
  - È possibile eseguire l'override di queste regole utilizzando `-mcs` e. `-mcd` opzioni.
- Se l'origine o la destinazione è il sistema ONTAP, a seconda della modalità NDMP (con ambito nodo o SVM), utilizzare un indirizzo IP che consenta l'accesso al volume di destinazione.
- `source_path` e. `destination_path` sono i nomi dei percorsi assoluti fino al livello granulare di volume, qtree, directory o file.
- `-mcs` specifica la modalità di indirizzamento preferita per la connessione di controllo al sistema di storage di origine.

  `inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

- `-mcd` specifica la modalità di indirizzamento preferita per la connessione di controllo al sistema di storage di destinazione.

  `inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

- `-md` specifica la modalità di indirizzamento preferita per i trasferimenti di dati tra i sistemi di storage di origine e di destinazione.

  `inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

  Se non si utilizza `-md` in `ndmpcopy` la modalità di indirizzamento per la connessione dati viene determinata come segue:

  - Se uno degli indirizzi specificati per le connessioni di controllo è un indirizzo IPv6, la modalità di indirizzo per la connessione dati è IPv6.
  - Se entrambi gli indirizzi specificati per le connessioni di controllo sono indirizzi IPv4, il `ndmpcopy` Command prima tenta una modalità di indirizzo IPv6 per la connessione dati.

    In caso di esito negativo, il comando utilizza una modalità di indirizzo IPv4.

    > Un indirizzo IPv6, se specificato, deve essere racchiuso tra parentesi quadre.

    Questo comando di esempio migra i dati da un percorso di origine (`source_path`) su un percorso di destinazione (`destination_path`).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+

Questo comando di esempio imposta esplicitamente le connessioni di controllo e la connessione dati in modo che utilizzino la modalità di indirizzo IPv6:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Opzioni per il comando ndmpcopy

È necessario conoscere le opzioni disponibili per `ndmpcopy` comando nodeshell per trasferire correttamente i dati.

La seguente tabella elenca le opzioni disponibili. Per ulteriori informazioni, consultare `ndmpcopy` pagine man disponibili attraverso il nodeshell.

Opzione	Descrizione
`-sa` `username`:[`password`]	Questa opzione consente di impostare il nome utente e la password per l'autenticazione di origine per la connessione al sistema di storage di origine. Si tratta di un'opzione obbligatoria. Per un utente senza privilegi di amministratore, è necessario specificare la password specifica NDMP generata dal sistema dell'utente. La password generata dal sistema è obbligatoria per gli utenti admin e non admin.
`-da` `username`:[`password`]	Questa opzione consente di impostare il nome utente e la password di autenticazione di destinazione per la connessione al sistema di storage di destinazione. Si tratta di un'opzione obbligatoria.
`-st` {`md5`	`text`}
Questa opzione consente di impostare il tipo di autenticazione di origine da utilizzare durante la connessione al sistema di storage di origine. Si tratta di un'opzione obbligatoria, pertanto l'utente deve fornire `text` oppure `md5` opzione.	`-dt` {`md5`
`text`}	Questa opzione consente di impostare il tipo di autenticazione di destinazione da utilizzare durante la connessione al sistema di storage di destinazione.

Opzione	Descrizione
`-l`	Questa opzione imposta il livello di dump utilizzato per il trasferimento sul valore specificato di level.Valid Values are `0`, `1`, a. `9`, dove `0` indica un trasferimento completo e. `1` a. `9` specifica un trasferimento incrementale. L'impostazione predefinita è `0`.
`-d`	Questa opzione consente la generazione di messaggi di log di debug ndmpcopy. I file di log di debug ndmpcopy si trovano in `/mroot/etc/log` volume root. I nomi dei file di log di debug ndmpcopy si trovano in `ndmpcopy.yyyymmdd` formato.
`-f`	Questa opzione attiva la modalità forzata. Questa modalità consente di sovrascrivere i file di sistema in `/etc` Nella directory principale del volume 7-Mode.
`-h`	Questa opzione consente di stampare il messaggio della guida.
`-p`	Questa opzione richiede di inserire la password per l'autorizzazione di origine e destinazione. Questa password sovrascrive la password specificata per `-sa` e. `-da` opzioni. È possibile utilizzare questa opzione solo quando il comando è in esecuzione in una console interattiva.
`-exclude`	Questa opzione esclude i file o le directory specificati dal percorso specificato per il trasferimento dei dati. Il valore può essere un elenco separato da virgole di nomi di directory o file come **`.pst`** `oppure .txt`.

NDMP per volumi FlexVol

Informazioni su NDMP per FlexVol Volumes

Il protocollo NDMP (Network Data Management Protocol) è un protocollo standardizzato per il controllo di backup, ripristino e altri tipi di trasferimento di dati tra dispositivi di storage primari e secondari, come sistemi storage e librerie su nastro.

Attivando il supporto NDMP su un sistema storage, è possibile consentire a tale sistema di comunicare con applicazioni di backup collegate in rete abilitate NDMP (denominate anche *applicazioni di gestione dati* o *DMA*), server di dati e server a nastro che partecipano alle operazioni di backup o ripristino. Tutte le comunicazioni di rete avvengono tramite rete TCPIP o TCP/IPv6. NDMP offre inoltre un controllo di basso livello di unità nastro e media Changer.

È possibile eseguire operazioni di backup e ripristino su nastro in modalità NDMP con ambito nodo o NDMP con ambito SVM (Storage Virtual Machine).

È necessario conoscere le considerazioni da tenere in considerazione durante l'utilizzo di NDMP, l'elenco delle variabili di ambiente e le topologie di backup su nastro NDMP supportate. È inoltre possibile attivare o disattivare la funzionalità DAR avanzata. I due metodi di autenticazione supportati da ONTAP per l'autenticazione dell'accesso NDMP a un sistema storage sono: Testo normale e sfida.

Informazioni correlate

Variabili di ambiente supportate da ONTAP

Informazioni sulle modalità operative NDMP

Puoi scegliere di eseguire le operazioni di backup e ripristino su nastro a livello di nodo o di Storage Virtual Machine (SVM). Per eseguire queste operazioni con successo a livello di SVM, il servizio NDMP deve essere attivato su SVM.

Se si esegue l'aggiornamento da Data ONTAP 8.2 a Data ONTAP 8.3, la modalità operativa NDMP utilizzata nel 8.2 continuerà a essere mantenuta dopo l'aggiornamento da 8.2 a 8.3.

Se si installa un nuovo cluster con Data ONTAP 8.2 o versione successiva, NDMP si trova nella modalità NDMP con ambito SVM per impostazione predefinita. Per eseguire operazioni di backup e ripristino su nastro in modalità NDMP con ambito nodo, è necessario attivare esplicitamente la modalità NDMP con ambito nodo.

Informazioni correlate

Comandi per la gestione della modalità NDMP con ambito nodo

Gestione della modalità NDMP con ambito nodo per volumi FlexVol

Gestione della modalità NDMP con ambito SVM per volumi FlexVol

Qual è la modalità NDMP con ambito nodo

Nella modalità NDMP con ambito nodo, è possibile eseguire operazioni di backup e ripristino su nastro a livello di nodo. La modalità operativa NDMP utilizzata in Data ONTAP 8.2 continuerà a essere mantenuta dopo l'aggiornamento dalla versione 8.2 alla 8.3.

Nella modalità NDMP con ambito nodo, è possibile eseguire operazioni di backup e ripristino su nastro su un nodo proprietario del volume. Per eseguire queste operazioni, è necessario stabilire connessioni di controllo NDMP su un LIF ospitato sul nodo proprietario dei dispositivi a nastro o volume.

Questa modalità è obsoleta e verrà rimossa in una release futura.

Informazioni correlate

Gestione della modalità NDMP con ambito nodo per volumi FlexVol

Qual è la modalità NDMP con ambito SVM

Se il servizio NDMP è attivato su SVM, è possibile eseguire correttamente operazioni di backup e ripristino su nastro a livello di SVM (Storage Virtual Machine). Se l'applicazione di backup supporta l'estensione CAB, è possibile eseguire il backup e il ripristino di tutti i

volumi ospitati su diversi nodi nella SVM di un cluster.

È possibile stabilire una connessione di controllo NDMP su diversi tipi di LIF. Nella modalità NDMP con ambito SVM, queste LIF appartengono a SVM di dati o SVM di amministrazione. La connessione può essere stabilita su una LIF solo se il servizio NDMP è attivato sulla SVM proprietaria di questa LIF.

Una LIF dei dati appartiene alla SVM dei dati e la LIF di intercluster, la LIF di gestione dei nodi e la LIF di gestione dei cluster appartengono alla SVM amministrativa.

Nella modalità NDMP con ambito SVM, la disponibilità di volumi e dispositivi a nastro per le operazioni di backup e ripristino dipende dal tipo di LIF da cui viene stabilita la connessione di controllo NDMP e dallo stato dell'estensione CAB. Se l'applicazione di backup supporta l'estensione CAB e un volume e il dispositivo a nastro condividono la stessa affinità, l'applicazione di backup può eseguire un'operazione di backup o ripristino locale invece di un'operazione di backup o ripristino a tre vie.

Informazioni correlate

Gestione della modalità NDMP con ambito SVM per volumi FlexVol

Considerazioni sull'utilizzo di NDMP

Quando si avvia il servizio NDMP sul sistema storage, è necessario tenere conto di una serie di considerazioni.

- Ogni nodo supporta un massimo di 16 backup, ripristini o combinazioni simultanei dei due utilizzando le unità a nastro collegate.
- I servizi NDMP possono generare dati di cronologia dei file su richiesta delle applicazioni di backup NDMP.

  La cronologia dei file viene utilizzata dalle applicazioni di backup per consentire il ripristino ottimizzato di set secondari selezionati di dati da un'immagine di backup. La generazione e l'elaborazione della cronologia dei file potrebbero richiedere molto tempo e richiedere un'elevata quantità di CPU sia per il sistema di storage che per l'applicazione di backup.

  SMTape non supporta la cronologia dei file.

  Se la protezione dei dati è configurata per il disaster recovery, dove verrà ripristinata l'intera immagine di backup, è possibile disattivare la generazione della cronologia dei file per ridurre i tempi di backup. Consultare la documentazione dell'applicazione di backup per determinare se è possibile disattivare la generazione della cronologia dei file NDMP.

- Il criterio firewall per NDMP è attivato per impostazione predefinita su tutti i tipi di LIF.
- In modalità NDMP con ambito nodo, il backup di un volume FlexVol richiede l'utilizzo dell'applicazione di backup per avviare un backup su un nodo proprietario del volume.

  Tuttavia, non è possibile eseguire il backup di un volume root del nodo.

- È possibile eseguire il backup NDMP da qualsiasi LIF consentito dalle policy firewall.

  Se si utilizza una LIF dati, è necessario selezionare una LIF non configurata per il failover. Se si verifica un errore di LIF dei dati durante un'operazione NDMP, l'operazione NDMP non riesce e deve essere rieseguita.

- Nella modalità NDMP con ambito nodo e nella modalità NDMP con ambito SVM (Storage Virtual Machine) senza supporto DELL'estensione CAB, la connessione dati NDMP utilizza lo stesso LIF della connessione

di controllo NDMP.

- Durante la migrazione LIF, le operazioni di backup e ripristino in corso vengono interrotte.

  È necessario avviare le operazioni di backup e ripristino dopo la migrazione LIF.

- Il percorso di backup NDMP è del formato `/vserver_name/volume_name/path_name`.

  `path_name` È opzionale e specifica il percorso della directory, del file o della copia Snapshot.

- Quando si esegue il backup su nastro di una destinazione SnapMirror utilizzando il motore di dump, viene eseguito il backup solo dei dati nel volume.

  Tuttavia, se viene eseguito il backup su nastro di una destinazione SnapMirror utilizzando SMTape, viene eseguito anche il backup dei metadati. Il backup delle relazioni SnapMirror e dei metadati associati non viene eseguito su nastro. Pertanto, durante il ripristino, vengono ripristinati solo i dati su quel volume, ma le relazioni SnapMirror associate non vengono ripristinate.

Informazioni correlate

Qual è la funzione di Cluster Aware Backup Extension

"Concetti di ONTAP"

"Amministrazione del sistema"

Variabile di ambiente

Panoramica delle variabili d'ambiente

Le variabili di ambiente vengono utilizzate per comunicare informazioni su un'operazione di backup o ripristino tra un'applicazione di backup abilitata per NDMP e un sistema di storage.

Ad esempio, se un utente specifica che un'applicazione di backup deve eseguire il backup `/vserver1/vol1/dir1`, L'applicazione di backup imposta la variabile di ambiente DEL FILE SYSTEM su `/vserver1/vol1/dir1`. Analogamente, se un utente specifica che un backup deve essere un backup di livello 1, l'applicazione di backup imposta la variabile di ambiente LEVEL su 1 (uno).

> L'impostazione e l'esame delle variabili di ambiente sono in genere trasparenti per gli amministratori del backup, ovvero l'applicazione di backup le imposta automaticamente.

Un amministratore del backup specifica raramente le variabili di ambiente; tuttavia, è possibile modificare il valore di una variabile di ambiente rispetto a quello impostato dall'applicazione di backup per caratterizzare o risolvere un problema funzionale o di performance. Ad esempio, un amministratore potrebbe voler disattivare temporaneamente la generazione della cronologia dei file per determinare se l'elaborazione delle informazioni della cronologia dei file da parte dell'applicazione di backup contribuisce a problemi di performance o di funzionamento.

Molte applicazioni di backup offrono un mezzo per eseguire l'override o modificare le variabili di ambiente o per specificare variabili di ambiente aggiuntive. Per informazioni, consultare la documentazione dell'applicazione di backup.

Variabili di ambiente supportate da ONTAP

Le variabili di ambiente vengono utilizzate per comunicare informazioni su un'operazione di backup o ripristino tra un'applicazione di backup abilitata per NDMP e un sistema di storage. ONTAP supporta le variabili di ambiente, che hanno un valore predefinito associato. Tuttavia, è possibile modificare manualmente questi valori predefiniti.

Se si modificano manualmente i valori impostati dall'applicazione di backup, l'applicazione potrebbe comportarsi in modo imprevedibile. Questo perché le operazioni di backup o ripristino potrebbero non eseguire le operazioni previste dall'applicazione di backup. Tuttavia, in alcuni casi, una modifica prudente potrebbe aiutare a identificare o a risolvere i problemi.

Le tabelle seguenti elencano le variabili di ambiente il cui comportamento è comune a dump e SMTape e quelle che sono supportate solo per dump e SMTape. Queste tabelle contengono anche descrizioni del funzionamento delle variabili di ambiente supportate da ONTAP se utilizzate:

> Nella maggior parte dei casi, le variabili che hanno il valore, `Y` accetta anche `T` e. `N` accetta anche `F`.

Variabili di ambiente supportate per dump e SMTape

Variabile di ambiente	Valori validi	Predefinito	Descrizione
DEBUG	`Y` oppure `N`	`N`	Specifica che le informazioni di debug vengono stampate.
FILESYSTEM	`string`	`none`	Specifica il nome del percorso della directory principale dei dati di cui viene eseguito il backup.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
NDMP_VERSION	`return_only`	`none`	Non modificare la variabile NDMP_VERSION. Creata dall'operazione di backup, la variabile NDMP_VERSION restituisce la versione NDMP. ONTAP imposta la variabile NDMP_VERSION durante un backup per uso interno e per passare a un'applicazione di backup a scopo informativo. La versione NDMP di una sessione NDMP non è impostata con questa variabile.
PATHNAME_SEPARATOR	`return_value`	`none`	Specifica il carattere di separazione del nome del percorso. Questo carattere dipende dal file system di cui viene eseguito il backup. Per ONTAP, il carattere "/" è assegnato a questa variabile. Il server NDMP imposta questa variabile prima di avviare un'operazione di backup su nastro.
TIPO	`dump` oppure `smtape`	`dump`	Specifica il tipo di backup supportato per eseguire operazioni di backup e ripristino su nastro.
DETTAGLIATO	`Y` oppure `N`	`N`	Aumenta i messaggi di log durante l'esecuzione di un'operazione di backup o ripristino su nastro.

Variabili di ambiente supportate per il dump

Variabile di ambiente	Valori validi	Predefinito	Descrizione
ACL_START	`return_only`	`none`	Creata dall'operazione di backup, la variabile ACL_START è un valore di offset utilizzato da un ripristino ad accesso diretto o da un'operazione di backup NDMP ripristinabile. Il valore di offset è l'offset di byte nel file dump in cui iniziano i dati ACL (Pass V) e vengono restituiti alla fine di un backup. Per un'operazione di ripristino ad accesso diretto che ripristini correttamente i dati di cui è stato eseguito il backup, il valore ACL_START deve essere passato all'operazione di ripristino all'inizio. Un'operazione di backup NDMP avviabile utilizza il valore ACL_START per comunicare con l'applicazione di backup in cui inizia la parte non avviabile del flusso di backup.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
BASE_DATE	`0`, `-1`, o. `DUMP_DATE` valore	`-1`	Specifica la data di inizio dei backup incrementali. Quando è impostato su `-1`, L'identificatore incrementale BASE_DATE è disattivato. Quando è impostato su `0` su un backup di livello 0, sono attivati backup incrementali. Dopo il backup iniziale, il valore della variabile DUMP_DATE del backup incrementale precedente viene assegnato alla variabile BASE_DATE. Queste variabili sono un'alternativa ai backup incrementali basati SU LIVELLO/AGGIORNAMENTO.
DIRETTO	`Y` oppure `N`	`N`	Specifica che un ripristino deve avanzare rapidamente direttamente nella posizione sul nastro in cui risiedono i dati del file, invece di eseguire la scansione dell'intero nastro. Affinché il ripristino dell'accesso diretto funzioni, l'applicazione di backup deve fornire informazioni di posizionamento. Se questa variabile è impostata su `Y`, l'applicazione di backup specifica i nomi dei file o delle directory e le informazioni di posizionamento.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
NOME_DMP	`string`	`none`	Specifica il nome di un backup di una sottostruttura multipla. Questa variabile è obbligatoria per i backup di più sottostruttura.
DUMP_DATE	`return_value`	`none`	Questa variabile non viene modificata direttamente. Viene creato dal backup se la variabile BASE_DATE è impostata su un valore diverso da `-1`. La variabile DUMP_DATE viene derivata anteponendo il valore di livello a 32 bit a un valore di tempo a 32 bit calcolato dal software dump. Il livello viene incrementato dall'ultimo valore di livello passato alla variabile BASE_DATE. Il valore risultante viene utilizzato come valore BASE_DATE in un backup incrementale successivo.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
ENHANCED_DAR_ENABLED	`Y` oppure `N`	`N`	Specifica se la funzionalità DAR avanzata è attivata. La funzionalità DAR avanzata supporta directory DAR e DAR di file con flussi NT. Offre miglioramenti delle performance. Il DAR avanzato durante il ripristino è possibile solo se vengono soddisfatte le seguenti condizioni: • ONTAP supporta DAR avanzato. • La cronologia del file viene attivata (HIST=Y) durante il backup. • Il `ndmpd.offset_map.enable` l'opzione è impostata su `on`. • LA variabile ENHANCED_DAR_ENABLED è impostata su `Y` durante il ripristino.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
ESCLUDI	`pattern_string`	`none`	Specifica i file o le directory che vengono esclusi durante il backup dei dati. L'elenco exclude è un elenco separato da virgole di nomi di file o directory. Se il nome di un file o di una directory corrisponde a uno dei nomi nell'elenco, viene escluso dal backup. Le seguenti regole si applicano quando si specificano i nomi nell'elenco di esclusione: • È necessario utilizzare il nome esatto del file o della directory. • L'asterisco (*), un carattere jolly, deve essere il primo o l'ultimo carattere della stringa. Ogni stringa può contenere fino a due asterischi. • Una virgola nel nome di un file o di una directory deve essere preceduta da una barra rovesciata. • L'elenco di esclusione può contenere fino a 32 nomi.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
ESTRARRE	`Y`, `N`, o. `E`	`N`	Specifica che le sottostruttura di un set di dati di cui è stato eseguito il backup devono essere ripristinate. L'applicazione di backup specifica i nomi delle sottostrutture da estrarre. Se un file specificato corrisponde a una directory di cui è stato eseguito il backup, la directory viene estratta in modo ricorrente. Per rinominare un file, una directory o un qtree durante il ripristino senza utilizzare DAR, è necessario impostare la variabile di ambiente DI ESTRAZIONE su `E`.
ESTRAI_ACL	`Y` oppure `N`	`Y`	Specifica che gli ACL del file di cui è stato eseguito il backup vengono ripristinati durante un'operazione di ripristino. L'impostazione predefinita prevede il ripristino degli ACL durante il ripristino dei dati, ad eccezione dei DAR (DIRECT=Y).

Variabile di ambiente	Valori validi	Predefinito	Descrizione
FORZA	`Y` oppure `N`	`N`	Determina se l'operazione di ripristino deve controllare lo spazio del volume e la disponibilità di inode sul volume di destinazione. Impostare questa variabile su `Y` consente all'operazione di ripristino di ignorare i controlli dello spazio del volume e della disponibilità di inode sul percorso di destinazione. Se sul volume di destinazione non è disponibile spazio di volume o inode sufficienti, l'operazione di ripristino ripristina la quantità di dati consentita dallo spazio di volume di destinazione e dalla disponibilità di inode. L'operazione di ripristino si interrompe quando lo spazio del volume o gli inode non sono disponibili.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
HIST	`Y` oppure `N`	`N`	Specifica che le informazioni sulla cronologia del file vengono inviate all'applicazione di backup. La maggior parte delle applicazioni di backup commerciali imposta la variabile HIST su `Y`. Se si desidera aumentare la velocità di un'operazione di backup o risolvere un problema con la raccolta della cronologia dei file, è possibile impostare questa variabile su `N`. Non impostare la variabile HIST su `Y` se l'applicazione di backup non supporta la cronologia dei file.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
IGNORE_CTIME	`Y` oppure `N`	`N`	Specifica che non viene eseguito il backup incrementale di un file se è stato modificato solo il relativo valore ctime rispetto al backup incrementale precedente. Alcune applicazioni, come il software antivirus, modificano il valore ctime di un file all'interno dell'inode, anche se il file o i relativi attributi non sono stati modificati. Di conseguenza, un backup incrementale potrebbe eseguire il backup dei file che non sono stati modificati. Il `IGNORE_CTIME` la variabile deve essere specificata solo se i backup incrementali richiedono una quantità di tempo o spazio inaccettabile a causa della modifica del valore ctime. Il `NDMP dump` set di comandi `IGNORE_CTIME` a. `false` per impostazione predefinita. Impostarlo su `true` può causare la seguente perdita di dati: 1. Se `IGNORE_CTIME` viene impostato su true con un

Variabile di ambiente	Valori validi	Predefinito	Descrizione
IGNORE_QTREE	`Y` oppure `N`	`N`	Specifica che l'operazione di ripristino non ripristina le informazioni qtree dai qtree di cui è stato eseguito il backup.
LIVELLO	`0-31`	`0`	Specifica il livello di backup. Il livello 0 copia l'intero set di dati. I livelli di backup incrementali, specificati da valori superiori a 0, copiano tutti i file (nuovi o modificati) dall'ultimo backup incrementale. Ad esempio, un livello 1 esegue il backup di file nuovi o modificati dal backup di livello 0, un livello 2 esegue il backup di file nuovi o modificati dal backup di livello 1 e così via.
ELENCO	`Y` oppure `N`	`N`	Elenca i nomi dei file di cui è stato eseguito il backup e i numeri di inode senza ripristinare effettivamente i dati.
LIST_QTREE	`Y` oppure `N`	`N`	Elenca i qtree di cui è stato eseguito il backup senza ripristinare effettivamente i dati.

uente elimina zione dei file, che vengon o spostati tra i qtree di origine durante il ripristin o increm entale.

Per evitare

Variabile di ambiente	Valori validi	Predefinito	Descrizione
NOMI_SOTTOSTRUTTURA_MULTIPLI	`string`	`none`	Specifica che il backup è un backup a più sottostruttura. Nella stringa sono specificate più sottostruttura, ovvero un elenco di nomi di sottostruttura separati da una nuova riga e con terminazione nulla. I sottostruttura sono specificati dai nomi dei percorsi relativi alla directory root comune, che deve essere specificata come ultimo elemento dell'elenco. Se si utilizza questa variabile, è necessario utilizzare anche la variabile DMP_NAME.
NDMP_UNICODE_ FH	`Y` oppure `N`	`N`	Specifica che un nome Unicode è incluso in aggiunta al nome NFS del file nelle informazioni sulla cronologia del file. Questa opzione non viene utilizzata dalla maggior parte delle applicazioni di backup e non deve essere impostata a meno che l'applicazione di backup non riceva questi nomi di file aggiuntivi. È necessario impostare anche la variabile HIST.
NO_ACL	`Y` oppure `N`	`N`	Specifica che gli ACL non devono essere copiati durante il backup dei dati.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
STRUTTURA_NON_QUOTA	`Y` oppure `N`	`N`	Specifica che i file e le directory nei qtree devono essere ignorati durante il backup dei dati. Quando è impostato su `Y`, Gli elementi in qtree nel set di dati specificato dalla variabile DI FILESYSTEM non vengono sottoposti a backup. Questa variabile ha un effetto solo se la variabile DI FILESYSTEM specifica un intero volume. La variabile NON_QUOTA_TREE funziona solo su un backup di livello 0 e non funziona se viene specificata la variabile MULTI_SUBTREE_NAMES. ⓘ I file o le directory specificati per essere esclusi per il backup non sono esclusi se si imposta NON_QUOTA_TREE su `Y` simultaneamente.
NOWRITE	`Y` oppure `N`	`N`	Specifica che l'operazione di ripristino non deve scrivere i dati sul disco. Questa variabile viene utilizzata per il debug.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
RICORRENTE	`Y` oppure `N`	`Y`	Specifica che le voci della directory durante un ripristino DAR devono essere espanse. Le variabili di ambiente DIRECT e ENHANCED_DAR_ENABLED devono essere attivate (impostate su `Y`). Se la variabile RICORRENTE è disattivata (impostare su `N`), solo le autorizzazioni e gli ACL per tutte le directory nel percorso di origine originale vengono ripristinati dal nastro, non dal contenuto delle directory. Se la variabile RICORRENTE è impostata su `N` Oppure la variabile RECOVER_FULL_PATHS è impostata su `Y`, il percorso di ripristino deve terminare con il percorso originale. Se la variabile RICORRENTE è disattivata e se sono presenti più percorsi di ripristino, tutti i percorsi di ripristino devono essere contenuti entro il più lungo dei percorsi di ripristino. In caso contrario, viene visualizzato un messaggio di errore.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
RECOVERY_FULL_PATHS	`Y` oppure `N`	`N`	Specifica che il percorso di ripristino completo avrà le relative autorizzazioni e gli ACL ripristinati dopo il DAR. DIRECT e ENHANCED_DAR_ENABLED devono essere attivati (impostare su `Y`). Se RECOVER_FULL_PATHS è impostato su `Y`, il percorso di ripristino deve terminare con il percorso originale. Se nel volume di destinazione sono già presenti directory, le relative autorizzazioni e gli ACL non verranno ripristinati dal nastro.
AGGIORNARE	`Y` oppure `N`	`Y`	Aggiorna le informazioni sui metadati per abilitare il backup incrementale basato SUL LIVELLO.

Variabili di ambiente supportate per SMTape

Variabile di ambiente	Valori validi	Predefinito	Descrizione

BASE_DATE	`DUMP_DATE`	`-1`	Specifica la data di inizio dei backup incrementali.
			
			`` `BASE_DATE` È una rappresentazione stringa degli identificatori Snapshot di riferimento. Utilizzando il `BASE_DATE` Stringa, SMTape individua la copia Snapshot di riferimento. ``
			
			`` `BASE_DATE` non è richiesto per i backup di riferimento. Per un backup incrementale, il valore di `DUMP_DATE` la variabile rispetto alla linea di base precedente o al backup incrementale viene assegnata a `BASE_DATE` variabile. ``
			
			L'applicazione di backup assegna `DUMP_DATE` Valore di una precedente linea di base SMTape o backup incrementale.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
DUMP_DATE	`return_value`	`none`	Al termine di un backup SMTape, DUMP_DATE contiene un identificatore di stringa che identifica la copia Snapshot utilizzata per tale backup. Questa copia Snapshot può essere utilizzata come copia Snapshot di riferimento per un backup incrementale successivo. Il valore risultante di DUMP_DATE viene utilizzato come valore BASE_DATE per i backup incrementali successivi.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifica la sequenza di backup incrementali associata al backup di riferimento. L'ID set di backup è un ID univoco a 128 bit generato durante un backup di base. L'applicazione di backup assegna questo ID come input a `SMTAPE_BACKUP_SET_ID` variabile durante un backup incrementale.
NOME_SNAPSHOT_SMTAPE	Qualsiasi copia Snapshot valida disponibile nel volume	`Invalid`	Quando la variabile SMTAPE_SNAPSHOT_NAME viene impostata su una copia Snapshot, viene eseguito il backup su nastro della copia Snapshot e delle copie Snapshot precedenti. Per il backup incrementale, questa variabile specifica la copia Snapshot incrementale. La variabile BASE_DATE fornisce la copia Snapshot di riferimento.

Variabile di ambiente	Valori validi	Predefinito	Descrizione
SMTAPE_DELETE_SNAPSHOT	`Y` oppure `N`	`N`	Per una copia Snapshot creata automaticamente da SMTape, quando la variabile SMTAPE_DELETE_SNAPSHOT è impostata su `Y`, Quindi, una volta completata l'operazione di backup, SMTape elimina questa copia Snapshot. Tuttavia, una copia Snapshot creata dall'applicazione di backup non verrà eliminata.
SMTAPE_BREAK_MIRROR	`Y` oppure `N`	`N`	Quando la variabile SMTAPE_BREAK_MIRROR è impostata su `Y`, il volume di tipo `DP` viene modificato in a. `RW` dopo un ripristino riuscito.

Topologie comuni di backup su nastro NDMP

NDMP supporta una serie di topologie e configurazioni tra applicazioni di backup e sistemi storage o altri server NDMP che forniscono servizi dati (file system) e su nastro.

Storage system-to-local-tape

Nella configurazione più semplice, un'applicazione di backup esegue il backup dei dati da un sistema storage a un sottosistema a nastro collegato al sistema storage. La connessione di controllo NDMP esiste attraverso il confine di rete. La connessione dati NDMP esistente nel sistema di storage tra i servizi dati e quelli su nastro viene chiamata configurazione locale NDMP.

Storage system-to-tape collegato a un altro sistema storage

Un'applicazione di backup può anche eseguire il backup dei dati da un sistema storage a una libreria di nastri (un dispositivo di sostituzione con una o più unità nastro) collegato a un altro sistema storage. In questo caso, la connessione dati NDMP tra i servizi dati e su nastro viene fornita da una connessione di rete TCP o TCP/IPv6. Questa configurazione è denominata configurazione del sistema di storage a tre vie NDMP.

Libreria di nastri collegata dal sistema di storage alla rete

Le librerie a nastro abilitate per NDMP offrono una variante della configurazione a tre vie. In questo caso, la libreria a nastro si collega direttamente alla rete TCP/IP e comunica con l'applicazione di backup e il sistema di storage attraverso un server NDMP interno.

Storage system-to-data server-to-tape o data server-to-storage system-to-tape

NDMP supporta anche configurazioni a tre vie tra sistema storage e server dati e tra server dati, anche se queste varianti sono meno diffuse. Lo storage system-to-server consente di eseguire il backup dei dati del sistema di storage su una libreria a nastro collegata all'host dell'applicazione di backup o su un altro sistema di server dati. La configurazione da server a sistema storage consente di eseguire il backup dei dati del server in una libreria di nastri collegata al sistema storage.

Metodi di autenticazione NDMP supportati

È possibile specificare un metodo di autenticazione per consentire le richieste di connessione NDMP. ONTAP supporta due metodi per autenticare l'accesso NDMP a un sistema storage: Testo normale e sfida.

Nella modalità NDMP con ambito nodo, sia challenge che plaintext sono attivati per impostazione predefinita. Tuttavia, non è possibile disattivare la sfida. È possibile attivare e disattivare il testo non crittografato. Nel metodo di autenticazione non crittografato, la password di accesso viene trasmessa come testo non crittografato.

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), per impostazione predefinita il metodo di autenticazione è un problema. A differenza della modalità NDMP con ambito di nodo, in questa modalità è possibile attivare e disattivare sia i metodi di autenticazione a testo normale che quelli di verifica.

Informazioni correlate

Autenticazione dell'utente in una modalità NDMP con ambito nodo

Autenticazione dell'utente in modalità NDMP con ambito SVM

Estensioni NDMP supportate da ONTAP

NDMP v4 offre un meccanismo per la creazione di estensioni del protocollo NDMP v4 senza modificare il protocollo NDMP v4 principale. È necessario conoscere le estensioni NDMP v4 supportate da ONTAP.

ONTAP supporta le seguenti estensioni NDMP v4:

- Backup cluster-aware (CAB)

  Questa estensione è supportata solo nella modalità NDMP con ambito SVM.

- Connection Address Extension (CAE) per il supporto IPv6
- Classe di estensione 0x2050

  Questa estensione supporta operazioni di backup avviabili e Snapshot Management Extensions.

Il `NDMP_SNAP_RECOVER` Message, che fa parte delle Snapshot Management Extensions, viene utilizzato per avviare un'operazione di recovery e trasferire i dati ripristinati da una copia Snapshot locale a una posizione del file system locale. In ONTAP, questo messaggio consente il ripristino solo di volumi e file regolari.

Il `NDMP_SNAP_DIR_LIST` Message (messaggio) consente di sfogliare le copie Snapshot di un volume. Se si verifica un'operazione senza interruzioni mentre è in corso un'operazione di esplorazione, l'applicazione di backup deve riavviare l'operazione di esplorazione.

Estensione di backup NDMP reavviabile per un dump supportato da ONTAP

È possibile utilizzare la funzionalità RBE (Restrictable Backup Extension) di NDMP per riavviare un backup da un checkpoint noto nel flusso di dati prima dell'errore.

Qual è la funzionalità DAR migliorata

È possibile utilizzare la funzionalità DAR (Direct Access Recovery) avanzata per le directory DAR e DAR di file e flussi NT. Per impostazione predefinita, la funzionalità DAR avanzata è attivata.

L'attivazione della funzionalità DAR avanzata potrebbe influire sulle prestazioni di backup, poiché è necessario creare e scrivere una mappa di offset su nastro. È possibile attivare o disattivare il DAR avanzato sia nelle modalità NDMP con ambito nodo che in quelle NDMP con ambito SVM (Storage Virtual Machine).

Limiti di scalabilità per le sessioni NDMP

È necessario conoscere il numero massimo di sessioni NDMP che è possibile stabilire simultaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.

I limiti indicati nella seguente tabella si riferiscono al server NDMP. I limiti indicati nella sezione "Slimiti di calabilità per le sessioni di backup e ripristino dump" si riferiscono alla sessione di dump e ripristino.

Limiti di scalabilità per sessioni di dump backup e ripristino

Memoria di sistema di un sistema storage	Numero massimo di sessioni NDMP
Meno di 16 GB	8
Superiore o uguale a 16 GB ma inferiore a 24 GB	20
Maggiore o uguale a 24 GB	36

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il nodeshell). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Informazioni su NDMP per FlexGroup Volumes

A partire da ONTAP 9.7, NDMP è supportato sui volumi FlexGroup.

A partire da ONTAP 9.7, il comando ndmpcopy è supportato per il trasferimento dei dati tra volumi FlexVol e FlexGroup.

Se si ripristina ONTAP 9.7 a una versione precedente, le informazioni di trasferimento incrementale dei trasferimenti precedenti non vengono conservate e, di conseguenza, è necessario eseguire una copia di riferimento dopo il ripristino.

A partire da ONTAP 9.8, le seguenti funzionalità NDMP sono supportate su FlexGroup Volumes:

- Il messaggio NDMP_SNAP_RECOVER nella classe di estensione 0x2050 può essere utilizzato per il ripristino di singoli file in un volume FlexGroup.
- NDMP Restartable Backup Extension (RBE) è supportato per i volumi FlexGroup.
- Le variabili di ambiente EXCLUDE e MULTI_SUBTREE_NAMES sono supportate per i volumi FlexGroup.

Informazioni su NDMP con volumi SnapLock

La creazione di più copie di dati regolamentati offre scenari di recovery ridondanti e, utilizzando il dump e il ripristino NDMP, è possibile preservare le caratteristiche WORM (write once, Read Many) dei file di origine su un volume SnapLock.

Gli attributi WORM sui file di un volume SnapLock vengono conservati durante il backup, il ripristino e la copia dei dati; tuttavia, gli attributi WORM vengono applicati solo quando si esegue il ripristino su un volume SnapLock. Se un backup da un volume SnapLock viene ripristinato in un volume diverso da un volume SnapLock, gli attributi WORM vengono conservati ma ignorati e non applicati da ONTAP.

Gestire la modalità NDMP con ambito nodo per i volumi FlexVol

Gestire la modalità NDMP con ambito nodo per la panoramica dei volumi FlexVol

È possibile gestire NDMP a livello di nodo utilizzando le opzioni e i comandi NDMP. È possibile modificare le opzioni NDMP utilizzando `options` comando. Per accedere a un sistema di storage ed eseguire operazioni di backup e ripristino su nastro, è necessario utilizzare credenziali specifiche di NDMP.

Per ulteriori informazioni su `options` vedere le pagine man.

Informazioni correlate

Comandi per la gestione della modalità NDMP con ambito nodo

Qual è la modalità NDMP con ambito nodo

Comandi per la gestione della modalità NDMP con ambito nodo

È possibile utilizzare `system services ndmp` Comandi per gestire NDMP a livello di nodo. Alcuni di questi comandi sono deprecati e verranno rimossi in una release futura.

È possibile utilizzare i seguenti comandi NDMP solo a livello di privilegi avanzati:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Se si desidera…	Utilizzare questo comando…
Abilitare il servizio NDMP	`system services ndmp on*`
Disattiva servizio NDMP	`system services ndmp off*`
Visualizzare la configurazione NDMP	`system services ndmp show*`
Modificare la configurazione NDMP	`system services ndmp modify*`
Visualizza la versione NDMP predefinita	`system services ndmp version*`
Visualizzare la configurazione del servizio NDMP	`system services ndmp service show`
Modificare la configurazione del servizio NDMP	`system services ndmp service modify`
Visualizza tutte le sessioni NDMP	`system services ndmp status`
Visualizza informazioni dettagliate su tutte le sessioni NDMP	`system services ndmp probe`
Terminare la sessione NDMP specificata	`system services ndmp kill`
Terminare tutte le sessioni NDMP	`system services ndmp kill-all`
Modificare la password NDMP	`system services ndmp password*`
Attiva la modalità NDMP con ambito nodo	`system services ndmp node-scope-mode on*`
Disattiva la modalità NDMP con ambito nodo	`system services ndmp node-scope-mode off*`
Visualizza lo stato della modalità NDMP con ambito nodo	`system services ndmp node-scope-mode status*`
Terminare con forza tutte le sessioni NDMP	`system services ndmp service terminate`

Se si desidera…	Utilizzare questo comando…
Avviare il daemon del servizio NDMP	`system services ndmp service start`
Arrestare il daemon del servizio NDMP	`system services ndmp service stop`
Avviare la registrazione per la sessione NDMP specificata	`system services ndmp log start*`
Interrompere la registrazione per la sessione NDMP specificata	`system services ndmp log stop*`

- Questi comandi sono deprecati e verranno rimossi in una release futura.

Per ulteriori informazioni su questi comandi, consultare le pagine man del `system services ndmp` comandi.

Autenticazione dell'utente in una modalità NDMP con ambito nodo

Nella modalità NDMP con ambito nodo, è necessario utilizzare credenziali specifiche NDMP per accedere a un sistema di storage per eseguire operazioni di backup e ripristino su nastro.

L'ID utente predefinito è "root". Prima di utilizzare NDMP su un nodo, è necessario assicurarsi di modificare la password NDMP predefinita associata all'utente NDMP. È inoltre possibile modificare l'ID utente NDMP predefinito.

Informazioni correlate

Comandi per la gestione della modalità NDMP con ambito nodo

Gestire la modalità NDMP con ambito SVM per i volumi FlexVol

Gestire la modalità NDMP con ambito SVM per la panoramica dei volumi FlexVol

È possibile gestire NDMP per SVM utilizzando le opzioni e i comandi NDMP. È possibile modificare le opzioni NDMP utilizzando `vserver services ndmp modify` comando. Nella modalità NDMP con ambito SVM, l'autenticazione dell'utente è integrata con il meccanismo di controllo degli accessi basato sui ruoli.

È possibile aggiungere NDMP nell'elenco dei protocolli consentiti o non consentiti utilizzando `vserver modify` comando. Per impostazione predefinita, NDMP si trova nell'elenco dei protocolli consentiti. Se NDMP viene aggiunto all'elenco dei protocolli non consentiti, non è possibile stabilire sessioni NDMP.

È possibile controllare il tipo di LIF su cui viene stabilita una connessione dati NDMP utilizzando `-preferred -interface-role` opzione. Durante una connessione dati NDMP, NDMP sceglie un indirizzo IP appartenente al tipo LIF specificato da questa opzione. Se gli indirizzi IP non appartengono a nessuno di questi tipi LIF, non è possibile stabilire la connessione dati NDMP. Per ulteriori informazioni su `-preferred -interface-role` vedere le pagine man.

Per ulteriori informazioni su `vserver services ndmp modify` vedere le pagine man.

Informazioni correlate

Comandi per la gestione della modalità NDMP con ambito SVM

Qual è la funzione di Cluster Aware Backup Extension

"Concetti di ONTAP"

Qual è la modalità NDMP con ambito SVM

"Amministrazione del sistema"

Comandi per la gestione della modalità NDMP con ambito SVM

È possibile utilizzare `vserver services ndmp` Comandi per la gestione di NDMP su ciascuna macchina virtuale di storage (SVM, in precedenza noto come Vserver).

Se si desidera…	Utilizzare questo comando…
Abilitare il servizio NDMP	`vserver services ndmp on` Il servizio NDMP deve essere sempre attivato su tutti i nodi di un cluster. È possibile attivare il servizio NDMP su un nodo utilizzando `system services ndmp on` comando. Per impostazione predefinita, il servizio NDMP è sempre attivato su un nodo.
Disattiva servizio NDMP	`vserver services ndmp off`
Visualizzare la configurazione NDMP	`vserver services ndmp show`
Modificare la configurazione NDMP	`vserver services ndmp modify`
Visualizza la versione NDMP predefinita	`vserver services ndmp version`
Visualizza tutte le sessioni NDMP	`vserver services ndmp status`
Visualizza informazioni dettagliate su tutte le sessioni NDMP	`vserver services ndmp probe`
Terminare una sessione NDMP specificata	`vserver services ndmp kill`
Terminare tutte le sessioni NDMP	`vserver services ndmp kill-all`
Generare la password NDMP	`vserver services ndmp generate-password`

Se si desidera…	Utilizzare questo comando…
Visualizza lo stato dell'interno NDMP	`vserver services ndmp extensions show` Questo comando è disponibile a livello di privilegio avanzato.
Modifica (attiva o disattiva) lo stato dell'interno NDMP	`vserver services ndmp extensions modify` Questo comando è disponibile a livello di privilegio avanzato.
Avviare la registrazione per la sessione NDMP specificata	`vserver services ndmp log start` Questo comando è disponibile a livello di privilegio avanzato.
Interrompere la registrazione per la sessione NDMP specificata	`vserver services ndmp log stop` Questo comando è disponibile a livello di privilegio avanzato.

Per ulteriori informazioni su questi comandi, consultare le pagine man del `vserver services ndmp` comandi.

Qual è la funzione di Cluster Aware Backup Extension

CAB (Cluster Aware Backup) è un'estensione del protocollo NDMP v4. Questa estensione consente al server NDMP di stabilire una connessione dati su un nodo proprietario di un volume. Ciò consente inoltre all'applicazione di backup di determinare se i volumi e i dispositivi a nastro si trovano sullo stesso nodo di un cluster.

Per consentire al server NDMP di identificare il nodo proprietario di un volume e di stabilire una connessione dati su tale nodo, l'applicazione di backup deve supportare l'estensione CAB. CAB Extension richiede che l'applicazione di backup informi il server NDMP del volume di cui eseguire il backup o il ripristino prima di stabilire la connessione dati. Questo consente al server NDMP di determinare il nodo che ospita il volume e di stabilire in modo appropriato la connessione dati.

Con l'estensione CAB supportata dall'applicazione di backup, il server NDMP fornisce informazioni di affinità su volumi e dispositivi a nastro. Utilizzando queste informazioni di affinità, l'applicazione di backup può eseguire un backup locale invece di un backup a tre vie se un volume e un dispositivo a nastro si trovano sullo stesso nodo di un cluster.

Disponibilità di volumi e dispositivi a nastro per il backup e il ripristino su diversi tipi di LIF

È possibile configurare un'applicazione di backup per stabilire una connessione di controllo NDMP su qualsiasi tipo di LIF in un cluster. Nella modalità NDMP con ambito SVM (Storage Virtual Machine), è possibile determinare la disponibilità di volumi e dispositivi a nastro per le operazioni di backup e ripristino in base a questi tipi di LIF e allo stato dell'estensione CAB.

Le seguenti tabelle mostrano la disponibilità di volumi e dispositivi a nastro per i tipi LIF di connessione di controllo NDMP e lo stato dell'estensione CAB:

Disponibilità di volumi e dispositivi a nastro quando L'estensione CAB non è supportata dall'applicazione di backup

Tipo LIF connessione di controllo NDMP	Volumi disponibili per il backup o il ripristino	Dispositivi a nastro disponibili per il backup o il ripristino
LIF di gestione dei nodi	Tutti i volumi ospitati da un nodo	Dispositivi a nastro collegati al nodo che ospita la LIF di gestione dei nodi
LIF dati	Solo i volumi che appartengono alla SVM ospitati da un nodo che ospita la LIF dei dati	Nessuno
LIF gestione cluster	Tutti i volumi ospitati da un nodo che ospita la LIF di gestione del cluster	Nessuno
LIF intercluster	Tutti i volumi ospitati da un nodo che ospita la LIF dell'intercluster	Dispositivi a nastro collegati al nodo che ospita la LIF dell'intercluster

Disponibilità di volumi e dispositivi a nastro quando L'estensione CAB è supportata dall'applicazione di backup

Tipo LIF connessione di controllo NDMP	Volumi disponibili per il backup o il ripristino	Dispositivi a nastro disponibili per il backup o il ripristino
LIF di gestione dei nodi	Tutti i volumi ospitati da un nodo	Dispositivi a nastro collegati al nodo che ospita la LIF di gestione dei nodi
LIF dati	Tutti i volumi che appartengono alla SVM che ospita la LIF dei dati	Nessuno
LIF gestione cluster	Tutti i volumi nel cluster	Tutti i dispositivi a nastro nel cluster
LIF intercluster	Tutti i volumi nel cluster	Tutti i dispositivi a nastro nel cluster

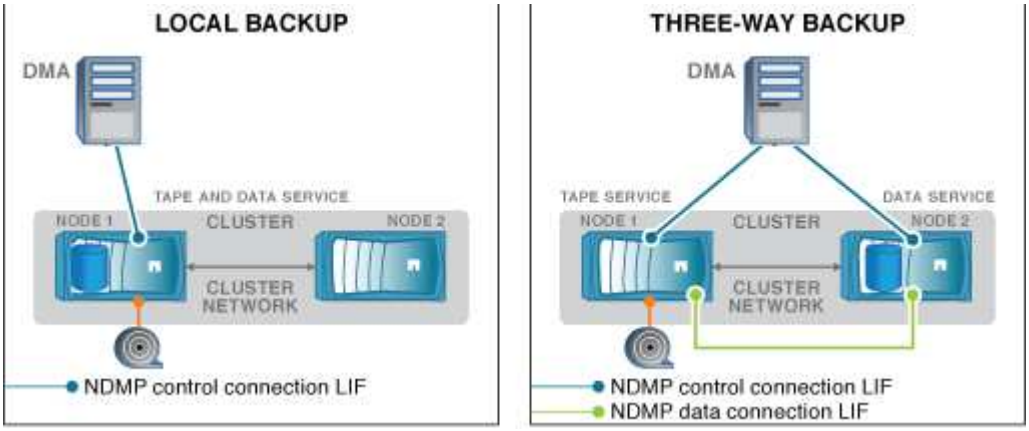
Che cosa sono le informazioni di affinità

Con l'applicazione di backup consapevole DEL CAB, il server NDMP fornisce informazioni univoche sulla posizione dei volumi e dei dispositivi a nastro. Utilizzando queste informazioni di affinità, l'applicazione di backup può eseguire un backup locale invece di un backup a tre vie se un volume e un dispositivo a nastro condividono la stessa affinità.

Se la connessione di controllo NDMP viene stabilita su una LIF di gestione dei nodi, LIF di gestione dei cluster,

O un LIF intercluster, l'applicazione di backup può utilizzare le informazioni di affinità per determinare se un volume e un dispositivo a nastro si trovano sullo stesso nodo ed eseguire quindi un'operazione di backup o ripristino locale o a tre vie. Se la connessione di controllo NDMP viene stabilita su una LIF dati, l'applicazione di backup esegue sempre un backup a tre vie.

Backup NDMP locale e backup NDMP a tre vie



Utilizzando le informazioni di affinità relative a volumi e dispositivi a nastro, DMA (applicazione di backup) esegue un backup NDMP locale sul volume e sul dispositivo a nastro situato nel nodo 1 del cluster. Se il volume si sposta dal nodo 1 al nodo 2, le informazioni di affinità relative al volume e al dispositivo a nastro cambiano. Pertanto, per un backup successivo, il DMA esegue un'operazione di backup NDMP a tre vie. In questo modo si garantisce la continuità del criterio di backup per il volume indipendentemente dal nodo in cui il volume viene spostato.

Informazioni correlate

Qual è la funzione di Cluster Aware Backup Extension

Il server NDMP supporta connessioni di controllo sicure in modalità SVM-scoped

È possibile stabilire una connessione di controllo sicura tra l'applicazione di gestione dei dati (DMA) e il server NDMP utilizzando socket sicuri (SSL/TLS) come meccanismo di comunicazione. Questa comunicazione SSL si basa sui certificati del server. Il server NDMP è in ascolto sulla porta 30000 (assegnata da IANA per il servizio "ndmps").

Dopo aver stabilito la connessione dal client su questa porta, viene eseguita la stretta di mano SSL standard in cui il server presenta il certificato al client. Quando il client accetta il certificato, l'handshake SSL è completo. Al termine di questo processo, tutte le comunicazioni tra il client e il server vengono crittografate. Il flusso di lavoro del protocollo NDMP rimane esattamente come in precedenza. La connessione NDMP sicura richiede solo l'autenticazione del certificato lato server. Un DMA può scegliere di stabilire una connessione connettendosi al servizio NDMP sicuro o al servizio NDMP standard.

Per impostazione predefinita, il servizio NDMP sicuro è disattivato per una macchina virtuale di storage (SVM). È possibile attivare o disattivare il servizio NDMP sicuro su una determinata SVM utilizzando `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` comando.

Tipi di connessione dati NDMP

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), i tipi di connessione dati NDMP supportati dipendono dal tipo di connessione di controllo NDMP LIF e dallo

stato dell'estensione CAB. Questo tipo di connessione dati NDMP indica se è possibile eseguire un'operazione di backup o ripristino NDMP locale o a tre vie.

È possibile eseguire un'operazione di backup o ripristino NDMP a tre vie su una rete TCP o TCP/IPv6. Le seguenti tabelle mostrano i tipi di connessione dati NDMP in base al tipo di connessione di controllo NDMP LIF e allo stato dell'estensione CAB.

Tipo di connessione dati NDMP quando L'estensione CAB è supportata dall'applicazione di backup

Tipo LIF connessione di controllo NDMP	Tipo di connessione dati NDMP
LIF di gestione dei nodi	LOCAL (LOCALE), TCP, TCP/IPV6
LIF dati	TCP, TCP/IPv6
LIF gestione cluster	LOCAL (LOCALE), TCP, TCP/IPV6
LIF intercluster	LOCAL (LOCALE), TCP, TCP/IPV6

Tipo di connessione dati NDMP quando L'estensione CAB non è supportata dall'applicazione di backup

Tipo LIF connessione di controllo NDMP	Tipo di connessione dati NDMP
LIF di gestione dei nodi	LOCAL (LOCALE), TCP, TCP/IPV6
LIF dati	TCP, TCP/IPv6
LIF gestione cluster	TCP, TCP/IPv6
LIF intercluster	LOCAL (LOCALE), TCP, TCP/IPV6

Informazioni correlate

Qual è la funzione di Cluster Aware Backup Extension

"Gestione della rete"

Autenticazione dell'utente in modalità NDMP con ambito SVM

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), l'autenticazione utente NDMP è integrata con il controllo degli accessi basato sui ruoli. Nel contesto SVM, l'utente NDMP deve avere il ruolo "vsadmin" o "vsadmin-backup". In un contesto di cluster, l'utente NDMP deve avere il ruolo "admin" o "backup".

Oltre a questi ruoli predefiniti, un account utente associato a un ruolo personalizzato può essere utilizzato anche per l'autenticazione NDMP, a condizione che il ruolo personalizzato disponga della cartella "vserver Services ndmp" nella directory dei comandi e che il livello di accesso della cartella non sia "none". In questa modalità, è necessario generare una password NDMP per un determinato account utente, che viene creata tramite il controllo dell'accesso basato sul ruolo. Gli utenti del cluster in un ruolo di amministratore o backup possono accedere a una LIF di gestione dei nodi, a una LIF di gestione dei cluster o a una LIF di intercluster.

Gli utenti con ruolo vsadmin-backup o vsadmin possono accedere solo ai dati LIF per tale SVM. Pertanto, a seconda del ruolo di un utente, la disponibilità dei volumi e dei dispositivi a nastro per le operazioni di backup e ripristino varia.

Questa modalità supporta anche l'autenticazione utente per gli utenti NIS e LDAP. Pertanto, gli utenti NIS e LDAP possono accedere a più SVM con un ID utente e una password comuni. Tuttavia, l'autenticazione NDMP non supporta gli utenti di Active Directory.

In questa modalità, un account utente deve essere associato all'applicazione SSH e al metodo di autenticazione "User password".

Informazioni correlate

Comandi per la gestione della modalità NDMP con ambito SVM

"Amministrazione del sistema"

"Concetti di ONTAP"

Generare una password specifica per NDMP per gli utenti NDMP

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), è necessario generare una password per un ID utente specifico. La password generata si basa sulla password di accesso effettiva per l'utente NDMP. Se la password di accesso effettiva viene modificata, è necessario generare nuovamente la password specifica di NDMP.

Fasi

1. Utilizzare `vserver services ndmp generate-password` Per generare una password specifica per NDMP.

   È possibile utilizzare questa password in qualsiasi operazione NDMP corrente o futura che richieda l'immissione della password.

   > Dal contesto della macchina virtuale di storage (SVM, precedentemente noto come Vserver), è possibile generare password NDMP per gli utenti che appartengono solo a tale SVM.

   Nell'esempio seguente viene illustrato come generare una password specifica per NDMP per un ID utente user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Se si modifica la password con il normale account del sistema di storage, ripetere questa procedura per ottenere la nuova password specifica di NDMP.

Impatto delle operazioni di backup e ripristino su nastro durante il disaster recovery nella configurazione MetroCluster

È possibile eseguire contemporaneamente operazioni di backup e ripristino su nastro durante il disaster recovery in una configurazione MetroCluster. È necessario comprendere in che modo queste operazioni vengono influenzate durante il disaster recovery.

Se le operazioni di backup e ripristino su nastro vengono eseguite su un volume di anSVM in una relazione di disaster recovery, è possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali dopo uno switchover e uno switchback.

Informazioni sul motore di dump per i volumi FlexVol

Informazioni sul motore di dump per i volumi FlexVol

Dump è una soluzione di backup e ripristino basata su copia Snapshot di ONTAP che consente di eseguire il backup di file e directory da una copia Snapshot a un dispositivo a nastro e di ripristinare i dati di cui è stato eseguito il backup in un sistema storage.

È possibile eseguire il backup dei dati del file system, ad esempio directory, file e relative impostazioni di sicurezza, su un dispositivo a nastro utilizzando il backup del dump. È possibile eseguire il backup di un intero volume, di un intero qtree o di un sottostruttura che non è né un intero volume né un intero qtree.

È possibile eseguire un backup o un ripristino dump utilizzando applicazioni di backup conformi a NDMP.

Quando si esegue un backup dump, è possibile specificare la copia Snapshot da utilizzare per un backup. Se non si specifica una copia Snapshot per il backup, il motore di dump crea una copia Snapshot per il backup. Una volta completata l'operazione di backup, il motore di dump elimina questa copia Snapshot.

È possibile eseguire backup di livello 0, incrementali o differenziali su nastro utilizzando il motore di dump.

> Dopo il ripristino di una release precedente a Data ONTAP 8.3, è necessario eseguire un'operazione di backup di riferimento prima di eseguire un'operazione di backup incrementale.

Informazioni correlate

"Upgrade, revert o downgrade"

Come funziona un backup dump

Un backup dump scrive i dati del file system da disco a nastro utilizzando un processo predefinito. È possibile eseguire il backup di un volume, di un qtree o di un sottostruttura che non è né un intero volume né un intero qtree.

La seguente tabella descrive il processo utilizzato da ONTAP per eseguire il backup dell'oggetto indicato dal percorso di dump:

Fase	Azione
1	Per un volume inferiore a quello completo o per i backup qtree completi, ONTAP attraversa le directory per identificare i file di cui eseguire il backup. Se si esegue il backup di un intero volume o qtree, ONTAP combina questa fase con la fase 2.
2	Per un backup completo di un volume o di un qtree completo, ONTAP identifica le directory nei volumi o qtree di cui eseguire il backup.
3	ONTAP scrive le directory su nastro.
4	ONTAP scrive i file su nastro.
5	ONTAP scrive le informazioni dell'ACL (se applicabili) su nastro.

Il backup del dump utilizza una copia Snapshot dei dati per il backup. Pertanto, non è necessario portare il volume offline prima di iniziare il backup.

Il backup del dump assegna un nome a ogni copia Snapshot creata `snapshot_for_backup.n`, dove `n` è un numero intero che inizia a 0. Ogni volta che il backup dump crea una copia Snapshot, il numero intero viene incrementato di 1. Il valore intero viene reimpostato su 0 dopo il riavvio del sistema di storage. Una volta completata l'operazione di backup, il motore di dump elimina questa copia Snapshot.

Quando ONTAP esegue più backup di dump contemporaneamente, il motore di dump crea più copie Snapshot. Ad esempio, se ONTAP esegue due backup di dump contemporaneamente, nei volumi da cui viene eseguito il backup dei dati vengono trovate le seguenti copie Snapshot: `snapshot_for_backup.0` e. `snapshot_for_backup.1`.

> Quando si esegue il backup da una copia Snapshot, il motore di dump non crea una copia Snapshot aggiuntiva.

Tipi di dati di cui il motore di dump esegue il backup

Il motore di dump consente di eseguire il backup dei dati su nastro per proteggersi da disastri o interruzioni del controller. Oltre al backup di oggetti dati come file, directory, qtree o interi volumi, il motore di dump può eseguire il backup di molti tipi di informazioni su ciascun file. Conoscere i tipi di dati di cui il motore di dump può eseguire il backup e le restrizioni da prendere in considerazione può aiutarti a pianificare il tuo approccio al disaster recovery.

Oltre a eseguire il backup dei dati nei file, il motore di dump può eseguire il backup delle seguenti informazioni relative a ciascun file, a seconda dei casi:

- UNIX GID, Owner UID e permessi del file
- Tempi di accesso, creazione e modifica UNIX
- Tipo di file
- Dimensione del file
- Nome DOS, attributi DOS e tempo di creazione

- Elenchi di controllo degli accessi (ACL) con 1,024 voci di controllo degli accessi (ACE)
- Informazioni sul qtree
- Percorsi di giunzione

I percorsi di giunzione vengono sottoposti a backup come collegamenti simbolici.

- LUN e LUN

  È possibile eseguire il backup di un intero oggetto LUN; tuttavia, non è possibile eseguire il backup di un singolo file all'interno dell'oggetto LUN. Allo stesso modo, è possibile ripristinare un intero oggetto LUN ma non un singolo file all'interno del LUN.

  Il motore di dump esegue il backup dei cloni LUN come LUN indipendenti.

- File allineati alle macchine virtuali

  Il backup dei file allineati alle macchine virtuali non è supportato nelle versioni precedenti a Data ONTAP 8.1.2.

Quando un clone del LUN con snapshot viene passato da Data ONTAP in 7-Mode a ONTAP, diventa un LUN non coerente. Il motore di dump non esegue il backup di LUN incoerenti.

Quando si ripristinano i dati su un volume, l'i/o client viene limitato alle LUN da ripristinare. La restrizione LUN viene rimossa solo al termine dell'operazione di dump restore. Allo stesso modo, durante un'operazione di ripristino di un singolo file o LUN SnapMirror, l'i/o del client viene limitato sia ai file che ai LUN ripristinati. Questa restrizione viene rimossa solo al termine dell'operazione di ripristino del singolo file o del LUN. Se viene eseguito un backup dump su un volume su cui viene eseguita un'operazione di ripristino dump o un singolo file o LUN di SnapMirror, i file o le LUN con restrizione i/o del client non vengono inclusi nel backup. Questi file o LUN vengono inclusi in una successiva operazione di backup se la restrizione i/o del client viene rimossa.

Un LUN eseguito su Data ONTAP 8.3 di cui è stato eseguito il backup su nastro può essere ripristinato solo alla versione 8.3 e successive e non a una release precedente. Se il LUN viene ripristinato a una release precedente, il LUN viene ripristinato come file.

Quando si esegue il backup di un volume secondario SnapVault o di una destinazione SnapMirror su nastro, viene eseguito il backup solo dei dati sul volume. Non viene eseguito il backup dei metadati associati. Pertanto, quando si tenta di ripristinare il volume, vengono ripristinati solo i dati di tale volume. Le informazioni sulle relazioni di SnapMirror del volume non sono disponibili nel backup e pertanto non vengono ripristinate.

Se si esegue il dump di un file che dispone solo delle autorizzazioni di Windows NT e lo si ripristina in un qtree o volume UNIX, il file ottiene le autorizzazioni UNIX predefinite per quel qtree o volume.

Se si esegue il dump di un file che dispone solo di autorizzazioni UNIX e lo si ripristina in un qtree o volume di stile NTFS, il file ottiene le autorizzazioni Windows predefinite per quel qtree o volume.

Altri dump e ripristini mantengono le autorizzazioni.

È possibile eseguire il backup dei file allineati alle macchine virtuali e di `vm-align-sector` opzione. Per ulteriori informazioni sui file allineati alle macchine virtuali, vedere "Gestione dello storage logico".

Quali sono le catene di incremento

Una catena di incrementi è una serie di backup incrementali dello stesso percorso. Poiché è possibile specificare qualsiasi livello di backup in qualsiasi momento, è necessario comprendere le catene di incremento per poter eseguire backup e ripristini in modo efficace. È possibile eseguire 31 livelli di operazioni di backup incrementali.

Esistono due tipi di catene di incremento:

- Una catena di incrementi consecutiva, una sequenza di backup incrementali che inizia con il livello 0 e viene aumentata di 1 per ogni backup successivo.
- Una catena di incrementi non consecutiva, in cui i backup incrementali ignorano i livelli o hanno livelli fuori sequenza, come 0, 2, 3, 1, 4, o più comunemente 0, 1, 1, 1 o 0, 1, 2, 1, 2.

I backup incrementali si basano sul backup di livello inferiore più recente. Ad esempio, la sequenza dei livelli di backup 0, 2, 3, 1, 4 fornisce due catene di incrementi: 0, 2, 3 e 0, 1, 4. La seguente tabella illustra le basi dei backup incrementali:

Ordine di backup	Livello di incremento	Catena di incremento	Base	File di cui è stato eseguito il backup
1	0	Entrambi	File sul sistema storage	Tutti i file nel percorso di backup
2	2	0, 2, 3	Backup di livello 0	File nel percorso di backup creato dal backup di livello 0
3	3	0, 2, 3	Backup di livello 2	File nel percorso di backup creato a partire dal backup di livello 2
4	1	0, 1, 4	Backup di livello 0, perché si tratta del livello più recente che è inferiore al backup di livello 1	File nel percorso di backup creato dopo il backup di livello 0, inclusi i file che si trovano nei backup di livello 2 e 3
5	4	0, 1, 4	Il backup di livello 1, perché è un livello inferiore ed è più recente dei backup di livello 0, 2 o 3	File creati a partire dal backup di livello 1

Qual è il fattore di blocco

Un blocco di nastri è costituito da 1,024 byte di dati. Durante un backup o ripristino su nastro, è possibile specificare il numero di blocchi di nastro trasferiti in ogni operazione di

lettura/scrittura. Questo numero è chiamato *fattore di blocco*.

È possibile utilizzare un fattore di blocco compreso tra 4 e 256. Se si prevede di ripristinare un backup su un sistema diverso da quello che ha eseguito il backup, il sistema di ripristino deve supportare il fattore di blocco utilizzato per il backup. Ad esempio, se si utilizza un fattore di blocco di 128, il sistema su cui si ripristina il backup deve supportare un fattore di blocco di 128.

Durante un backup NDMP, MOVER_RECORD_SIZE determina il fattore di blocco. ONTAP consente un valore massimo di 256 KB per MOVER_RECORD_SIZE.

Quando riavviare un backup di dump

Un backup dump a volte non termina a causa di errori interni o esterni, come errori di scrittura su nastro, interruzioni di alimentazione, interruzioni accidentali dell'utente o incongruenze interne nel sistema storage. Se il backup non riesce per uno di questi motivi, è possibile riavviarlo.

È possibile scegliere di interrompere e riavviare un backup per evitare periodi di traffico intenso sul sistema di storage o per evitare la concorrenza per altre risorse limitate sul sistema di storage, come un'unità a nastro. È possibile interrompere un backup lungo e riavviarlo in un secondo momento se un ripristino (o backup) più urgente richiede la stessa unità a nastro. I backup riavviabili persistono durante i riavvii. È possibile riavviare un backup su nastro interrotto solo se sono soddisfatte le seguenti condizioni:

- Il backup interrotto si trova nella fase IV
- Sono disponibili tutte le copie Snapshot associate bloccate dal comando dump.
- La cronologia del file deve essere attivata.

Quando un'operazione di dump viene interrotta e lasciata in uno stato di ripristino, le copie Snapshot associate vengono bloccate. Queste copie Snapshot vengono rilasciate dopo l'eliminazione del contesto di backup. È possibile visualizzare l'elenco dei contesti di backup utilizzando `vserver services ndmp restartable backup show` comando.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Come funziona un ripristino dump

Un ripristino dump scrive i dati del file system da nastro a disco utilizzando un processo predefinito.

La procedura riportata nella tabella seguente mostra il funzionamento del ripristino dump:

Fase	Azione
1	ONTAP cataloga i file che devono essere estratti dal nastro.
2	ONTAP crea directory e file vuoti.

Fase	Azione
3	ONTAP legge un file dal nastro, lo scrive su disco e imposta le autorizzazioni (inclusi gli ACL) su di esso.
4	ONTAP ripete le fasi 2 e 3 fino a quando tutti i file specificati non vengono copiati dal nastro.

Tipi di dati ripristinati dal motore di dump

Quando si verifica un'interruzione del controller o di un'emergenza, il motore di dump offre diversi metodi per ripristinare tutti i dati di cui è stato eseguito il backup, dai singoli file agli attributi dei file, alle intere directory. Conoscere i tipi di dati ripristinati dal motore di dump e quando utilizzare il metodo di recovery può contribuire a ridurre al minimo i tempi di inattività.

È possibile ripristinare i dati in una LUN mappata online. Tuttavia, le applicazioni host non possono accedere a questo LUN fino al completamento dell'operazione di ripristino. Una volta completata l'operazione di ripristino, la cache host dei dati LUN deve essere svuotata per garantire la coerenza con i dati ripristinati.

Il motore di dump può recuperare i seguenti dati:

- Contenuto di file e directory
- Permessi di file UNIX
- ACL

  Se si ripristina un file che dispone solo delle autorizzazioni di file UNIX su un qtree o volume NTFS, il file non dispone di ACL Windows NT. Il sistema di storage utilizza solo le autorizzazioni di file UNIX per questo file fino a quando non viene creato un ACL di Windows NT.

  > Se si ripristinano gli ACL di cui è stato eseguito il backup dai sistemi storage che eseguono Data ONTAP 8.2 ai sistemi storage che eseguono Data ONTAP 8.1.x e versioni precedenti con un limite ACE inferiore a 1,024, viene ripristinato un ACL predefinito.

- Informazioni sul qtree

  Le informazioni qtree vengono utilizzate solo se un qtree viene ripristinato nella directory principale di un volume. Le informazioni qtree non vengono utilizzate se un qtree viene ripristinato in una directory inferiore, ad esempio `/vs1/vol1/subdir/lowerdir`e cessa di essere un qtree.

- Tutti gli altri attributi di file e directory
- Flussi Windows NT
- LUN
  - Un LUN deve essere ripristinato a livello di volume o qtree per rimanere come LUN.

    Se viene ripristinato in una directory, viene ripristinato come file perché non contiene metadati validi.

  - Un LUN 7-Mode viene ripristinato come LUN su un volume ONTAP.
- È possibile ripristinare un volume 7-Mode su un volume ONTAP.

- I file allineati alle macchine virtuali ripristinati in un volume di destinazione ereditano le proprietà di allineamento delle macchine virtuali del volume di destinazione.
- Il volume di destinazione per un'operazione di ripristino potrebbe avere file con blocchi obbligatori o di avviso.

  Durante l'esecuzione dell'operazione di ripristino su un volume di destinazione di questo tipo, il motore di dump ignora questi blocchi.

Considerazioni prima del ripristino dei dati

È possibile ripristinare i dati di backup nel percorso originale o in una destinazione diversa. Se si ripristinano i dati di cui si è eseguito il backup in una destinazione diversa, è necessario preparare la destinazione per l'operazione di ripristino.

Prima di ripristinare i dati nel percorso originale o in una destinazione diversa, è necessario disporre delle seguenti informazioni e soddisfare i seguenti requisiti:

- Il livello del ripristino
- Il percorso in cui si stanno ripristinando i dati
- Il fattore di blocco utilizzato durante il backup
- Se si esegue un ripristino incrementale, tutti i nastri devono trovarsi nella catena di backup
- Unità a nastro disponibile e compatibile con il nastro da cui eseguire il ripristino

Prima di ripristinare i dati in una destinazione diversa, è necessario eseguire le seguenti operazioni:

- Se si sta ripristinando un volume, è necessario crearne uno nuovo.
- Se si sta ripristinando un qtree o una directory, è necessario rinominare o spostare i file che hanno probabilmente lo stesso nome dei file che si stanno ripristinando.

> In ONTAP 9, i nomi qtree supportano il formato Unicode. Le versioni precedenti di ONTAP non supportano questo formato. Se un qtree con nomi Unicode in ONTAP 9 viene copiato in una release precedente di ONTAP utilizzando `ndmpcopy` Comando o tramite il ripristino da un'immagine di backup in un nastro, il qtree viene ripristinato come una normale directory e non come un qtree con formato Unicode.

> Se un file ripristinato ha lo stesso nome di un file esistente, il file esistente viene sovrascritto dal file ripristinato. Tuttavia, le directory non vengono sovrascritte.

Per rinominare un file, una directory o un qtree durante il ripristino senza utilizzare DAR, è necessario impostare la variabile di ambiente DI ESTRAZIONE su `E`.

Spazio richiesto sul sistema di storage di destinazione

Sono necessari circa 100 MB di spazio in più sul sistema di storage di destinazione rispetto alla quantità di dati da ripristinare.

L'operazione di ripristino verifica lo spazio del volume e la disponibilità di inode sul volume di destinazione all'avvio dell'operazione di ripristino. Impostazione della variabile di ambiente FORCE su `Y` fa in modo che l'operazione di ripristino salti i controlli dello spazio del volume e della disponibilità di inode sul percorso di destinazione. Se lo spazio del volume o gli inode disponibili sul volume di destinazione non sono sufficienti, l'operazione di ripristino ripristina la quantità di dati consentita dallo spazio del volume di destinazione e dalla disponibilità dell'inode. L'operazione di ripristino si interrompe quando non rimane più spazio o inode del volume.

Limiti di scalabilità per sessioni di dump backup e ripristino

È necessario conoscere il numero massimo di sessioni di backup e ripristino dump che possono essere eseguite simultaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.

I limiti indicati nella seguente tabella si riferiscono al motore di dump o ripristino. I limiti menzionati nei limiti di scalabilità per le sessioni NDMP si riferiscono al server NDMP, che sono superiori ai limiti del motore.

Memoria di sistema di un sistema storage	Numero totale di sessioni di backup e ripristino dump
Meno di 16 GB	4
Superiore o uguale a 16 GB ma inferiore a 24 GB	16
Maggiore o uguale a 24 GB	32

Se si utilizza `ndmpcopy` Comando per copiare i dati all'interno dei sistemi storage, vengono stabilite due sessioni NDMP, una per il backup del dump e l'altra per il ripristino del dump.

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il nodeshell). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Informazioni correlate

Limiti di scalabilità per le sessioni NDMP

Supporto di backup e ripristino su nastro tra Data ONTAP in 7-Mode e ONTAP

È possibile ripristinare i dati di cui è stato eseguito il backup da un sistema storage in 7-Mode o in esecuzione su ONTAP in un sistema storage in 7-Mode o in esecuzione su ONTAP.

Le seguenti operazioni di backup e ripristino su nastro sono supportate tra Data ONTAP in 7-Mode e ONTAP:

- Backup di un volume 7-Mode su un'unità a nastro collegata a un sistema storage che esegue ONTAP
- Backup di un volume ONTAP su un'unità a nastro collegata a un sistema 7-Mode
- Ripristino dei dati di backup di un volume 7-Mode da un'unità a nastro collegata a un sistema storage che esegue ONTAP

- Ripristino dei dati di backup di un volume ONTAP da un'unità a nastro collegata a un sistema 7-Mode
- Ripristino di un volume 7-Mode su un volume ONTAP

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Ripristino di un volume ONTAP su un volume 7-Mode

Un LUN ONTAP viene ripristinato come file normale su un volume 7-Mode.

Elimina i contesti avviabili

Se si desidera avviare un backup invece di riavviare un contesto, è possibile eliminarlo.

A proposito di questa attività

È possibile eliminare un contesto avviabile utilizzando `vserver services ndmp restartable-backup delete` Fornendo il nome SVM e l'ID di contesto.

Fasi

1. Eliminare un contesto avviabile:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Come funziona il dump su un volume secondario SnapVault

È possibile eseguire operazioni di backup su nastro sui dati mirrorati sul volume secondario SnapVault. È possibile eseguire il backup su nastro solo dei dati mirrorati sul volume secondario SnapVault e non dei metadati della relazione SnapVault.

Quando si infrangono le relazioni mirrorate alla protezione dei dati (`snapmirror break`) O quando si verifica una risincronizzazione di SnapMirror, è sempre necessario eseguire un backup di riferimento.

Come funziona il dump con il failover dello storage e le operazioni ARL

Prima di eseguire operazioni di dump backup o ripristino, è necessario comprendere il funzionamento di queste operazioni con operazioni di failover dello storage (takeover e giveback) o di trasferimento aggregato (ARL). Il `-override-vetoes` L'opzione determina il comportamento del motore di dump durante un failover dello storage o un'operazione ARL.

Quando è in esecuzione un'operazione di dump backup o ripristino e il `-override-vetoes` l'opzione è impostata su `false`, Un failover dello storage avviato dall'utente o un'operazione ARL viene interrotta. Tuttavia, se il `-override-vetoes` l'opzione è impostata su `true`, Quindi, il failover dello storage o l'operazione ARL viene proseguita e l'operazione di backup o ripristino del dump viene interrotta. Quando un'operazione ARL o di failover dello storage viene avviata automaticamente dal sistema storage, un'operazione di backup o ripristino dump attivo viene sempre interrotta. Non è possibile riavviare le operazioni di backup e ripristino dump anche dopo il completamento delle operazioni ARL o di failover dello storage.

Operazioni di dump quando è supportata l'estensione DELLA CABINA

Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino incrementali senza riconfigurare le policy di backup dopo un failover dello storage o un'operazione ARL.

Operazioni di dump quando l'estensione DELLA CABINA non è supportata

Se l'applicazione di backup non supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino del dump incrementale se si esegue la migrazione della LIF configurata nel criterio di backup nel nodo che ospita l'aggregato di destinazione. In caso contrario, dopo il failover dello storage e l'operazione ARL, è necessario eseguire un backup di riferimento prima di eseguire l'operazione di backup incrementale.

> Per le operazioni di failover dello storage, la LIF configurata nel criterio di backup deve essere migrata al nodo partner.

Informazioni correlate

"Concetti di ONTAP"

"Alta disponibilità"

Come funziona il dump con lo spostamento del volume

Le operazioni di backup e ripristino su nastro e lo spostamento del volume possono essere eseguite in parallelo fino al tentativo di cutover finale da parte del sistema di storage. Al termine di questa fase, non sono consentite nuove operazioni di backup e ripristino del nastro sul volume che viene spostato. Tuttavia, le operazioni correnti continuano a essere eseguite fino al completamento.

La seguente tabella descrive il comportamento delle operazioni di backup e ripristino su nastro dopo l'operazione di spostamento del volume:

Se si eseguono operazioni di backup e ripristino su nastro in…	Quindi…
Modalità NDMP con ambito SVM (Storage Virtual Machine) quando L'estensione CAB è supportata dall'applicazione di backup	È possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura senza riconfigurare i criteri di backup.
Modalità NDMP SVM-scoped quando l'estensione CAB non è supportata dall'applicazione di backup	È possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura se si esegue la migrazione della LIF configurata nel criterio di backup nel nodo che ospita l'aggregato di destinazione. In caso contrario, dopo lo spostamento del volume, è necessario eseguire un backup di riferimento prima di eseguire l'operazione di backup incrementale.

Quando si verifica uno spostamento del volume, se il volume appartenente a un SVM diverso sul nodo di destinazione ha lo stesso nome del volume spostato, non è possibile eseguire operazioni di backup incrementali del volume spostato.

Informazioni correlate

"Concetti di ONTAP"

Come funziona il dump quando un volume FlexVol è pieno

Prima di eseguire un'operazione di backup incrementale del dump, è necessario assicurarsi che lo spazio libero nel volume FlexVol sia sufficiente.

Se l'operazione non riesce, è necessario aumentare lo spazio libero nel volume Flex Vol aumentandone le dimensioni o eliminando le copie Snapshot. Quindi eseguire nuovamente l'operazione di backup incrementale.

Come funziona il dump quando cambia il tipo di accesso al volume

Quando un volume di destinazione SnapMirror o un volume secondario SnapVault cambia stato da lettura/scrittura a sola lettura o da sola lettura a lettura/scrittura, è necessario eseguire un'operazione di backup o ripristino su nastro di base.

I volumi secondari di destinazione e SnapVault di SnapMirror sono volumi di sola lettura. Se si eseguono operazioni di backup e ripristino su nastro su tali volumi, è necessario eseguire un'operazione di backup o ripristino di base ogni volta che il volume cambia stato da sola lettura a sola lettura/scrittura o da lettura/scrittura a sola lettura.

Informazioni correlate

"Concetti di ONTAP"

Come funziona il dump con il ripristino di un singolo file o LUN SnapMirror

Prima di eseguire operazioni di dump backup o ripristino su un volume su cui viene ripristinato un singolo file o LUN utilizzando la tecnologia SnapMirror, è necessario comprendere il funzionamento delle operazioni di dump con un'operazione di ripristino di un singolo file o LUN.

Durante un'operazione di ripristino di un singolo file o LUN SnapMirror, l'i/o del client viene limitato al file o al LUN da ripristinare. Al termine dell'operazione di ripristino di un singolo file o LUN, la restrizione i/o sul file o sul LUN viene rimossa. Se viene eseguito un backup dump su un volume in cui viene ripristinato un singolo file o LUN, il file o LUN con restrizione i/o del client non viene incluso nel backup dump. In una successiva operazione di backup, il backup di questo file o LUN viene eseguito su nastro dopo la rimozione della restrizione i/O.

Non è possibile eseguire contemporaneamente un ripristino dump e un'operazione di ripristino di un singolo file o LUN SnapMirror sullo stesso volume.

Influenza delle operazioni di backup e ripristino dump nelle configurazioni MetroCluster

Prima di eseguire operazioni di dump backup e ripristino in una configurazione MetroCluster, è necessario comprendere in che modo le operazioni di dump vengono influenzate quando si verifica un'operazione di switchover o switchback.

Eseguire il dump dell'operazione di backup o ripristino e passare al switchover

Prendere in considerazione due cluster: Cluster 1 e cluster 2. Durante un'operazione di dump backup o ripristino sul cluster 1, se viene avviato uno switchover dal cluster 1 al cluster 2, si verifica quanto segue:

- Se il valore di `override-vetoes` l'opzione è `false`, lo switchover viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino del dump viene interrotta e lo switchover continua.

Eseguire un'operazione di dump backup o ripristino seguita da switchback

Viene eseguito uno switchover dal cluster 1 al cluster 2 e viene avviata un'operazione di dump backup o ripristino sul cluster 2. L'operazione di dump esegue il backup o il ripristino di un volume che si trova nel cluster 2. A questo punto, se viene avviato uno switchback dal cluster 2 al cluster 1, si verifica quanto segue:

- Se il valore di `override-vetoes` l'opzione è `false`, quindi lo switchback viene annullato e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino viene interrotta e lo switchback continua.

Operazione di dump backup o ripristino avviata durante uno switchover o uno switchback

Durante lo switchover dal cluster 1 al cluster 2, se viene avviata un'operazione di dump backup o ripristino sul cluster 1, l'operazione di backup o ripristino non riesce e lo switchover continua.

Durante uno switchback dal cluster 2 al cluster 1, se viene avviata un'operazione di dump backup o ripristino dal cluster 2, l'operazione di backup o ripristino non riesce e lo switchback continua.

Informazioni sul motore SMTape per volumi FlexVol

Informazioni sul motore SMTape per volumi FlexVol

SMTape è una soluzione di disaster recovery di ONTAP che esegue il backup di blocchi di dati su nastro. È possibile utilizzare SMTape per eseguire backup dei volumi su nastri. Tuttavia, non è possibile eseguire un backup a livello di qtree o sottostruttura. SMTape supporta backup baseline, differenziali e incrementali. SMTape non richiede una licenza.

È possibile eseguire un'operazione di backup e ripristino SMTape utilizzando un'applicazione di backup compatibile con NDMP. È possibile scegliere SMTape per eseguire operazioni di backup e ripristino solo nella modalità NDMP con ambito SVM (Storage Virtual Machine).

> Il processo di revversion non è supportato quando è in corso una sessione di backup o ripristino SMTape. È necessario attendere il termine della sessione oppure interrompere la sessione NDMP.

Con SMTape, è possibile eseguire il backup di 255 copie Snapshot. Per i backup baseline, incrementali o differenziali successivi, è necessario eliminare le copie Snapshot di backup precedenti.

Prima di eseguire un ripristino baseline, il volume su cui vengono ripristinati i dati deve essere di tipo `DP` e questo volume deve essere nello stato limitato. Una volta eseguito correttamente il ripristino, il volume viene automaticamente online. È possibile eseguire ripristini incrementali o differenziali successivi su questo volume

nell’ordine in cui sono stati eseguiti i backup.

Utilizzare le copie Snapshot durante il backup SMTape

È necessario comprendere come vengono utilizzate le copie Snapshot durante un backup di base SMTape e un backup incrementale. È inoltre necessario tenere presente alcune considerazioni durante l’esecuzione di un backup con SMTape.

Backup di riferimento

Durante l’esecuzione di un backup di riferimento, è possibile specificare il nome della copia Snapshot di cui eseguire il backup su nastro. Se non viene specificata alcuna copia Snapshot, a seconda del tipo di accesso del volume (lettura/scrittura o sola lettura), viene creata automaticamente una copia Snapshot o vengono utilizzate le copie Snapshot esistenti. Quando si specifica una copia Snapshot per il backup, viene eseguito anche il backup su nastro di tutte le copie Snapshot precedenti alla copia Snapshot specificata.

Se non si specifica una copia Snapshot per il backup, si verifica quanto segue:

- Per un volume di lettura/scrittura, viene creata automaticamente una copia Snapshot.

  La copia Snapshot appena creata e tutte le copie Snapshot precedenti vengono sottoposte a backup su nastro.

- Per un volume di sola lettura, viene eseguito il backup su nastro di tutte le copie Snapshot, inclusa l’ultima copia Snapshot.

  Non viene eseguito il backup delle nuove copie Snapshot create dopo l’avvio del backup.

Backup incrementale

Per le operazioni di backup incrementali o differenziali SMTape, le applicazioni di backup conformi a NDMP creano e gestiscono le copie Snapshot.

È necessario specificare sempre una copia Snapshot durante l’esecuzione di un’operazione di backup incrementale. Per un’operazione di backup incrementale riuscita, la copia Snapshot di cui è stato eseguito il backup durante l’operazione di backup precedente (baseline o incrementale) deve trovarsi sul volume da cui viene eseguito il backup. Per assicurarsi di utilizzare questa copia Snapshot di backup, è necessario prendere in considerazione il criterio Snapshot assegnato a questo volume durante la configurazione del criterio di backup.

Considerazioni sui backup SMTape sulle destinazioni SnapMirror

- Una relazione mirror per la protezione dei dati crea copie Snapshot temporanee sul volume di destinazione per la replica.

  Non utilizzare queste copie Snapshot per il backup SMTape.

- Se si verifica un aggiornamento di SnapMirror su un volume di destinazione in una relazione mirror di protezione dei dati durante un’operazione di backup SMTape sullo stesso volume, la copia Snapshot di cui è stato eseguito il backup da SMTape non deve essere eliminata sul volume di origine.

  Durante l’operazione di backup, SMTape blocca la copia Snapshot sul volume di destinazione e, se la copia Snapshot corrispondente viene eliminata sul volume di origine, l’operazione di aggiornamento di SnapMirror successiva non riesce.

- Non utilizzare queste copie Snapshot durante il backup incrementale.

Funzionalità SMTape

Le funzionalità SMTape, come backup di copie Snapshot, backup incrementali e differenziali, conservazione delle funzionalità di deduplica e compressione sui volumi ripristinati e seeding dei nastri, consentono di ottimizzare le operazioni di backup e ripristino dei nastri.

SMTape offre le seguenti funzionalità:

- Offre una soluzione di disaster recovery
- Consente backup incrementali e differenziali
- Esegue il backup delle copie Snapshot
- Consente il backup e il ripristino dei volumi deduplicati e preserva la deduplica sui volumi ripristinati
- Esegue il backup dei volumi compressi e mantiene la compressione sui volumi ripristinati
- Consente il seeding dei nastri

SMTape supporta il fattore di blocco in multipli di 4 KB, nell'intervallo da 4 KB a 256 KB.

> È possibile ripristinare i dati su volumi creati solo in due release principali consecutive di ONTAP.

Funzionalità non supportate in SMTape

SMTape non supporta backup avviabili e verifica dei file di cui è stato eseguito il backup.

Limiti di scalabilità per le sessioni di backup e ripristino SMTape

Durante l'esecuzione delle operazioni di backup e ripristino SMTape tramite NDMP o CLI (seeding su nastro), è necessario conoscere il numero massimo di sessioni di backup e ripristino SMTape che è possibile eseguire contemporaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.

> I limiti di scalabilità delle sessioni di backup e ripristino SMTape sono diversi dai limiti delle sessioni NDMP e dei limiti delle sessioni di dump.

Memoria di sistema del sistema storage	Numero totale di sessioni di backup e ripristino SMTape
Meno di 16 GB	6
Superiore o uguale a 16 GB ma inferiore a 24 GB	16
Maggiore o uguale a 24 GB	32

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il nodeshell). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

Informazioni correlate

Limiti di scalabilità per le sessioni NDMP

Limiti di scalabilità per sessioni di dump backup e ripristino

Che cos'è il seeding del nastro

Il seeding dei nastri è una funzionalità SMTape che consente di inizializzare un volume FlexVol di destinazione in una relazione mirror di protezione dei dati.

Il seeding su nastro consente di stabilire una relazione mirror per la protezione dei dati tra un sistema di origine e un sistema di destinazione su una connessione a bassa larghezza di banda.

Il mirroring incrementale delle copie Snapshot dall'origine alla destinazione è possibile su una connessione a bassa larghezza di banda. Tuttavia, il mirroring iniziale della copia Snapshot di base richiede molto tempo su una connessione a bassa larghezza di banda. In questi casi, è possibile eseguire un backup SMTape del volume di origine su un nastro e utilizzare il nastro per trasferire la copia Snapshot di base iniziale nella destinazione. È quindi possibile impostare gli aggiornamenti incrementali di SnapMirror nel sistema di destinazione utilizzando la connessione a bassa larghezza di banda.

Informazioni correlate

"Concetti di ONTAP"

Funzionamento di SMTape con il failover dello storage e le operazioni ARL

Prima di eseguire operazioni di backup o ripristino SMTape, è necessario comprendere il funzionamento di queste operazioni con operazioni di failover dello storage (takeover e giveback) o di riposizionamento degli aggregati (ARL). Il `-override-vetoes` L'opzione determina il comportamento del motore SMTape durante un'operazione ARL o di failover dello storage.

Quando è in esecuzione un'operazione di backup o ripristino SMTape e il `-override-vetoes` l'opzione è impostata su `false`, Un failover dello storage avviato dall'utente o un'operazione ARL viene interrotta e l'operazione di backup o ripristino viene completata. Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino SMTape incrementali senza riconfigurare i criteri di backup. Tuttavia, se il `-override-vetoes` l'opzione è impostata su `true`, Quindi il failover dello storage o l'operazione ARL viene proseguita e l'operazione di backup o ripristino SMTape viene interrotta.

Informazioni correlate

"Gestione della rete"

"Alta disponibilità"

Funzionamento di SMTape con lo spostamento del volume

Le operazioni di backup SMTape e le operazioni di spostamento del volume possono essere eseguite in parallelo fino a quando il sistema storage non tenta la fase di cutover finale. Dopo questa fase, non è possibile eseguire nuove operazioni di backup SMTape

sul volume che viene spostato. Tuttavia, le operazioni correnti continuano a essere eseguite fino al completamento.

Prima di avviare la fase di cutover di un volume, l'operazione di spostamento del volume verifica la presenza di operazioni di backup SMTape attive sullo stesso volume. Se sono presenti operazioni di backup SMTape attive, l'operazione di spostamento del volume passa a uno stato di cutover rinviato e consente il completamento delle operazioni di backup SMTape. Una volta completate queste operazioni di backup, è necessario riavviare manualmente l'operazione di spostamento del volume.

Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura senza riconfigurare i criteri di backup.

Le operazioni di ripristino di base e di spostamento del volume non possono essere eseguite contemporaneamente; tuttavia, il ripristino incrementale può essere eseguito in parallelo con le operazioni di spostamento del volume, con un comportamento simile a quello delle operazioni di backup SMTape durante le operazioni di spostamento del volume.

Informazioni correlate

"Concetti di ONTAP"

Funzionamento di SMTape con le operazioni di re-hosting dei volumi

Le operazioni SMTape non possono iniziare quando è in corso un'operazione di rehost del volume su un volume. Quando un volume è coinvolto in un'operazione di rehost del volume, le sessioni SMTape non devono essere avviate su quel volume.

Se è in corso un'operazione di rehost del volume, il backup o il ripristino SMTape non riesce. Se è in corso un backup o ripristino SMTape, le operazioni di rehost del volume non riescono e viene visualizzato un messaggio di errore appropriato. Questa condizione si applica alle operazioni di backup o ripristino basate su NDMP e CLI.

In che modo i criteri di backup NDMP vengono influenzati durante ADB

Quando il bilanciamento automatico dei dati (ADB) è attivato, il bilanciamento analizza le statistiche di utilizzo degli aggregati per identificare l'aggregato che ha superato la percentuale di utilizzo ad alta soglia configurata.

Dopo aver identificato l'aggregato che ha superato la soglia, il bilanciamento identifica un volume che può essere spostato in aggregati che risiedono in un altro nodo del cluster e tenta di spostare tale volume. Questa situazione influisce sul criterio di backup configurato per questo volume perché se l'applicazione di gestione dei dati (DMA) non è a conoscenza DEL CAB, l'utente deve riconfigurare il criterio di backup ed eseguire l'operazione di backup di riferimento.

> Se il DMA è in GRADO di riconoscere IL CAB e il criterio di backup è stato configurato utilizzando un'interfaccia specifica, ADB non viene interessato.

Impatto delle operazioni di backup e ripristino SMTape nelle configurazioni MetroCluster

Prima di eseguire operazioni di backup e ripristino SMTape in una configurazione MetroCluster, è necessario comprendere in che modo le operazioni SMTape vengono influenzate quando si verifica un'operazione di switchover o switchback.

Operazione di backup o ripristino SMTape seguita da switchover

Prendere in considerazione due cluster: Cluster 1 e cluster 2. Durante un'operazione di backup o ripristino SMTape sul cluster 1, se viene avviato uno switchover dal cluster 1 al cluster 2, si verifica quanto segue:

- Se il valore di `-override-vetoes` l'opzione è `false`, il processo di switchover viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, L'operazione di backup o ripristino SMTape viene interrotta e il processo di switchover continua.

Operazione di backup o ripristino SMTape seguita da switchback

Viene eseguito uno switchover dal cluster 1 al cluster 2 e viene avviata un'operazione di backup o ripristino SMTape sul cluster 2. L'operazione SMTape esegue il backup o il ripristino di un volume che si trova nel cluster 2. A questo punto, se viene avviato uno switchback dal cluster 2 al cluster 1, si verifica quanto segue:

- Se il valore di `-override-vetoes` l'opzione è `false`, il processo di switchback viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino viene interrotta e il processo di switchback continua.

Operazione di backup o ripristino SMTape avviata durante uno switchover o uno switchback

Durante un processo di switchover dal cluster 1 al cluster 2, se viene avviata un'operazione di backup o ripristino SMTape sul cluster 1, l'operazione di backup o ripristino non riesce e lo switchover continua.

Durante un processo di switchback dal cluster 2 al cluster 1, se viene avviata un'operazione di backup o ripristino SMTape dal cluster 2, l'operazione di backup o ripristino non riesce e lo switchback continua.

Monitorare le operazioni di backup e ripristino dei volumi FlexVol

Monitoraggio delle operazioni di backup e ripristino dei nastri per la panoramica dei volumi FlexVol

È possibile visualizzare i file di registro eventi per monitorare le operazioni di backup e ripristino del nastro. ONTAP registra automaticamente eventi di backup e ripristino significativi e l'ora in cui si verificano in un file di registro denominato `backup` nel controller `/etc/log/` directory. Per impostazione predefinita, la registrazione degli eventi è impostata su `on`.

È possibile visualizzare i file di registro eventi per i seguenti motivi:

- Verifica della riuscita di un backup notturno
- Raccolta di statistiche sulle operazioni di backup
- Per utilizzare le informazioni contenute nei file di log degli eventi precedenti per diagnosticare i problemi relativi alle operazioni di backup e ripristino

Una volta alla settimana, i file di registro degli eventi vengono ruotati. Il `/etc/log/backup` il file viene rinominato in `/etc/log/backup.0`, il `/etc/log/backup.0` il file viene rinominato in `/etc/log/backup.1`e così via. Il sistema salva i file di log per un massimo di sei settimane; pertanto, è possibile disporre di un massimo di sette file di messaggi (/etc/log/backup.[0-5]` e la corrente `/etc/log/backup` file).

Accedere ai file di registro degli eventi

È possibile accedere ai file di registro eventi per le operazioni di backup e ripristino su nastro in `/etc/log/` directory utilizzando `rdfile` comando al nodeshell. È possibile visualizzare questi file di registro eventi per monitorare le operazioni di backup e ripristino su nastro.

A proposito di questa attività

Con configurazioni aggiuntive, ad esempio un ruolo di controllo degli accessi con accesso a `spi` servizio web o account utente configurato con `http` metodo di accesso, è anche possibile utilizzare un browser web per accedere a questi file di log.

Fasi

1. Per accedere al nodeshell, immettere il seguente comando:

   `node run -node node_name`

   `node_name` è il nome del nodo.

2. Per accedere ai file di registro eventi per le operazioni di backup e ripristino su nastro, immettere il seguente comando:

   `rdfile /etc/log/backup`

Informazioni correlate

"Amministrazione del sistema"

"Concetti di ONTAP"

Formato del messaggio di dump e ripristino del registro eventi

Panoramica del formato dei messaggi del registro eventi di dump e ripristino

Per ogni evento di dump e ripristino, viene scritto un messaggio nel file di log di backup.

Il formato del messaggio di dump e ripristino del registro eventi è il seguente:

`type timestamp identifier event (event_info)`

Il seguente elenco descrive i campi nel formato dei messaggi del registro eventi:

- Ogni messaggio di registro inizia con uno degli indicatori di tipo descritti nella tabella seguente:

Tipo	Descrizione
log (registro)	Registrazione dell'evento
dmp	Evento dump
rst	Evento di ripristino

- `timestamp` mostra la data e l'ora dell'evento.
- Il `identifier` Il campo per un evento dump include il percorso dump e l'ID univoco per il dump. Il `identifier` il campo di un evento di ripristino utilizza solo il nome del percorso di destinazione di ripristino come identificatore univoco. I messaggi di evento correlati alla registrazione non includono un `identifier` campo.

Quali sono gli eventi di registrazione

Il campo evento di un messaggio che inizia con un registro specifica l'inizio di una registrazione o la fine di una registrazione.

Contiene uno degli eventi mostrati nella tabella seguente:

Evento	Descrizione
Start_Logging	Indica l'inizio della registrazione o che la registrazione è stata riattivata dopo essere stata disattivata.
Stop_Logging	Indica che la registrazione è stata disattivata.

Quali sono gli eventi di dump

Il campo dell'evento per un evento dump contiene un tipo di evento seguito da informazioni specifiche dell'evento tra parentesi.

La seguente tabella descrive gli eventi, le relative descrizioni e le relative informazioni che potrebbero essere registrate per un'operazione di dump:

Evento	Descrizione	Informazioni sull'evento
Inizio	Viene avviato il dump NDMP	Livello di dump e tipo di dump
Fine	Dump completati correttamente	Quantità di dati elaborati
Interrompere	L'operazione viene annullata	Quantità di dati elaborati
Opzioni	Vengono elencate le opzioni specificate	Tutte le opzioni e i relativi valori, incluse le opzioni NDMP
TAPE_Open	Il nastro è aperto per la lettura/scrittura	Il nome del nuovo dispositivo a nastro
Tape_close	Il nastro è chiuso per la lettura/scrittura	Il nome del dispositivo a nastro
Cambiamento di fase	Un dump sta entrando in una nuova fase di elaborazione	Il nome della nuova fase

Evento	Descrizione	Informazioni sull'evento
Errore	Si è verificato un evento imprevisto in un dump	Messaggio di errore
Snapshot	Viene creata o individuata una copia Snapshot	Il nome e l'ora della copia Snapshot
Base_dump	È stata individuata una voce di dump di base nel metafile interno	Il livello e il tempo del dump di base (solo per i dump incrementali)

Quali sono gli eventi di ripristino

Il campo evento per un evento di ripristino contiene un tipo di evento seguito da informazioni specifiche dell'evento tra parentesi.

La seguente tabella fornisce informazioni sugli eventi, le relative descrizioni e le relative informazioni che è possibile registrare per un'operazione di ripristino:

Evento	Descrizione	Informazioni sull'evento
Inizio	Ripristino NDMP avviato	Livello di ripristino e tipo di ripristino
Fine	Ripristini completati correttamente	Numero di file e quantità di dati elaborati
Interrompere	L'operazione viene annullata	Numero di file e quantità di dati elaborati
Opzioni	Vengono elencate le opzioni specificate	Tutte le opzioni e i relativi valori, incluse le opzioni NDMP
TAPE_Open	Il nastro è aperto per la lettura/scrittura	Il nome del nuovo dispositivo a nastro
Tape_close	Il nastro è chiuso per la lettura/scrittura	Il nome del dispositivo a nastro
Cambiamento di fase	Il ripristino sta entrando in una nuova fase di elaborazione	Il nome della nuova fase
Errore	Il ripristino rileva un evento imprevisto	Messaggio di errore

Attivazione o disattivazione della registrazione degli eventi

È possibile attivare o disattivare la registrazione degli eventi.

Fasi

1. Per attivare o disattivare la registrazione degli eventi, immettere il seguente comando nella shell dei cluster:

   options -*option_name* backup.log.enable -*option-value* {on | off}

   `on` attiva la registrazione degli eventi.

   `off` disattiva la disconnessione degli eventi.

   > La registrazione degli eventi è attivata per impostazione predefinita.

Messaggi di errore per il backup su nastro e il ripristino dei volumi FlexVol

Messaggi di errore relativi al backup e al ripristino

Limitazione delle risorse: Nessun thread disponibile

- **Messaggio**

  `Resource limitation: no available thread`

- **Causa**

  Il numero massimo di thread i/o locali su nastro attivi è attualmente in uso. È possibile disporre di un massimo di 16 unità a nastro locali attive.

- **Azione correttiva**

  Attendere il completamento di alcuni processi su nastro prima di avviare un nuovo processo di backup o ripristino.

Prenotazione del nastro anticipata

- **Messaggio**

  `Tape reservation preempted`

- **Causa**

  L'unità a nastro è in uso da un'altra operazione o il nastro è stato chiuso prematuramente.

- **Azione correttiva**

  Assicurarsi che l'unità a nastro non venga utilizzata da un'altra operazione e che l'applicazione DMA non abbia interrotto il processo, quindi riprovare.

Impossibile inizializzare il supporto

- **Messaggio**

  `Could not initialize media`

- **Causa**

  Questo errore potrebbe verificarsi per uno dei seguenti motivi:

  - L'unità a nastro utilizzata per il backup è danneggiata o danneggiata.
  - Il nastro non contiene il backup completo o è corrotto.
  - Il numero massimo di thread i/o locali su nastro attivi è attualmente in uso.

    È possibile disporre di un massimo di 16 unità a nastro locali attive.

- **Azione correttiva**
  - Se l'unità a nastro è danneggiata o danneggiata, riprovare a eseguire l'operazione con un'unità a nastro valida.
  - Se il nastro non contiene il backup completo o è corrotto, non è possibile eseguire l'operazione di ripristino.
  - Se le risorse su nastro non sono disponibili, attendere il completamento di alcuni processi di backup o ripristino, quindi riprovare l'operazione.

Numero massimo di dump o ripristini consentiti (limite massimo di sessione) in corso

- **Messaggio**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Causa**

  Il numero massimo di processi di backup o ripristino è già in esecuzione.

- **Azione correttiva**

  Riprovare l'operazione al termine di alcuni dei lavori attualmente in esecuzione.

Errore di supporto in scrittura su nastro

- **Messaggio**

  `Media error on tape write`

- **Causa**

  Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

  Sostituire il nastro e riprovare a eseguire il processo di backup.

Scrittura del nastro non riuscita

- **Messaggio**

  `Tape write failed`

- **Causa**

  Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

  Sostituire il nastro e riprovare a eseguire il processo di backup.

Scrittura nastro non riuscita - il nuovo nastro ha rilevato un errore di supporto

- **Messaggio**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Causa**

  Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

  Sostituire il nastro e riprovare a eseguire il backup.

Scrittura nastro non riuscita - il nuovo nastro è rotto o protetto da scrittura

- **Messaggio**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Causa**

  Il nastro utilizzato per il backup è corrotto o protetto da scrittura.

- **Azione correttiva**

  Sostituire il nastro e riprovare a eseguire il backup.

Scrittura nastro non riuscita - il nuovo nastro è già alla fine del supporto

- **Messaggio**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Causa**

  Spazio sul nastro insufficiente per completare il backup.

- **Azione correttiva**

  Sostituire il nastro e riprovare a eseguire il backup.

Errore di scrittura del nastro

- **Messaggio**

```
Tape write error - The previous tape had less than the required minimum
capacity, size MB, for this tape operation, The operation should be restarted
from the beginning
```

- **Causa**

  La capacità del nastro non è sufficiente per contenere i dati di backup.

- **Azione correttiva**

  Utilizzare nastri con capacità maggiore e riprovare a eseguire il processo di backup.

Errore di lettura del supporto su nastro

- **Messaggio**

  ```
  Media error on tape read
  ```

- **Causa**

  Il nastro da cui vengono ripristinati i dati è corrotto e potrebbe non contenere i dati di backup completi.

- **Azione correttiva**

  Se si è certi che il nastro disponga del backup completo, riprovare l'operazione di ripristino. Se il nastro non contiene il backup completo, non è possibile eseguire l'operazione di ripristino.

Errore di lettura del nastro

- **Messaggio**

  ```
  Tape read error
  ```

- **Causa**

  L'unità a nastro è danneggiata o il nastro non contiene il backup completo.

- **Azione correttiva**

  Se l'unità a nastro è danneggiata, utilizzare un'altra unità a nastro. Se il nastro non contiene il backup completo, non è possibile ripristinare i dati.

Già alla fine del nastro

- **Messaggio**

  ```
  Already at the end of tape
  ```

- **Causa**

  Il nastro non contiene dati o deve essere riavvolto.

- **Azione correttiva**

Se il nastro non contiene dati, utilizzare il nastro che contiene il backup e riprovare a eseguire il processo di ripristino. In caso contrario, riavvolgere il nastro e riprovare a eseguire il processo di ripristino.

La dimensione del record del nastro è troppo piccola. Provare a utilizzare un formato più grande.

- **Messaggio**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Causa**

  Il fattore di blocco specificato per l'operazione di ripristino è inferiore al fattore di blocco utilizzato durante il backup.

- **Azione correttiva**

  Utilizzare lo stesso fattore di blocco specificato durante il backup.

La dimensione del record del nastro deve essere block_size1 e non block_size2

- **Messaggio**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Causa**

  Il fattore di blocco specificato per il ripristino locale non è corretto.

- **Azione correttiva**

  Riprovare a eseguire il processo di ripristino con `block_size1` come fattore di blocco.

La dimensione del record del nastro deve essere compresa tra 4 KB e 256 KB

- **Messaggio**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Causa**

  Il fattore di blocco specificato per l'operazione di backup o ripristino non rientra nell'intervallo consentito.

- **Azione correttiva**

  Specificare un fattore di blocco compreso tra 4 KB e 256 KB.

Messaggi di errore NDMP

Errore di comunicazione di rete

- **Messaggio**

  ```
  Network communication error
  ```

- **Causa**

  La comunicazione con un nastro remoto in una connessione NDMP a tre vie non è riuscita.

- **Azione correttiva**

  Verificare la connessione di rete al telecomando.

Messaggio da Read Socket: Error_string

- **Messaggio**

  ```
  Message from Read Socket: error_string
  ```

- **Causa**

  Ripristinare la comunicazione dal nastro remoto nella connessione NDMP a 3 vie con errori.

- **Azione correttiva**

  Verificare la connessione di rete al telecomando.

Messaggio da Write Dirnet: Error_string

- **Messaggio**

  ```
  Message from Write Dirnet: error_string
  ```

- **Causa**

  Si è verificato un errore nella comunicazione di backup con un nastro remoto in una connessione NDMP a tre vie.

- **Azione correttiva**

  Verificare la connessione di rete al telecomando.

Read Socket Received EOF

- **Messaggio**

  ```
  Read Socket received EOF
  ```

- **Causa**

  Il tentativo di comunicare con un nastro remoto in una connessione NDMP a tre vie ha raggiunto la fine del contrassegno file. Potrebbe essere in corso un ripristino a tre direzioni da un’immagine di backup con un blocco di dimensioni maggiori.

- **Azione correttiva**

  Specificare la dimensione del blocco corretta e riprovare l’operazione di ripristino.

ndmpd numero di versione non valido: numero_versione ``

- **Messaggio**

  ```
  ndmpd invalid version number: version_number
  ```

- **Causa**

  La versione NDMP specificata non è supportata dal sistema di storage.

- **Azione correttiva**

  Specificare la versione 4 di NDMP.

ID_sessione ndmpd non attivo

- **Messaggio**

  ```
  ndmpd session session_ID not active
  ```

- **Causa**

  La sessione NDMP potrebbe non esistere.

- **Azione correttiva**

  Utilizzare `ndmpd status` Per visualizzare le sessioni NDMP attive.

Impossibile ottenere vol Ref per Volume volume_name

- **Messaggio**

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- **Causa**

  Impossibile ottenere il riferimento del volume perché il volume potrebbe essere utilizzato da altre operazioni.

- **Azione correttiva**

  Riprovare l'operazione in un secondo momento.

Tipo di connessione dati ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] non supportato per le connessioni di controllo ["IPv6"|"IPv4"]

- **Messaggio**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Causa**

  In modalità NDMP con ambito nodo, la connessione dati NDMP stabilita deve essere dello stesso tipo di

indirizzo di rete (IPv4 o IPv6) della connessione di controllo NDMP.

- **Azione correttiva**

  Contattare il fornitore dell'applicazione di backup.

DATA LISTEN (ASCOLTO DATI): Errore di precondizione di preparazione della connessione dati CAB

- **Messaggio**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Causa**

  L'ascolto dei dati NDMP non riesce quando l'applicazione di backup ha negoziato l'estensione CAB con il server NDMP e c'è una mancata corrispondenza nel tipo di indirizzo di connessione dati NDMP specificato tra i messaggi NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_LISTEN.

- **Azione correttiva**

  Contattare il fornitore dell'applicazione di backup.

DATA CONNECT: Errore di precondizione di preparazione della connessione dati CAB

- **Messaggio**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Causa**

  La connessione dati NDMP non riesce quando l'applicazione di backup ha negoziato l'estensione CAB con il server NDMP e c'è una mancata corrispondenza nel tipo di indirizzo di connessione dati NDMP specificato tra i messaggi NDMP_CAB_DATA_CONN_PREPARE e NDMP_DATA_CONNECT.

- **Azione correttiva**

  Contattare il fornitore dell'applicazione di backup.

Errore:show failed: Impossibile ottenere la password per l'utente '<username>'

- **Messaggio**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Causa**

  Configurazione dell'account utente incompleta per NDMP

- **Azione correttiva**

  Assicurarsi che l'account utente sia associato al metodo di accesso SSH e che il metodo di autenticazione sia la password utente.

Messaggi di errore di dump

Il volume di destinazione è di sola lettura

- **Messaggio**

  `Destination volume is read-only`

- **Causa**

  Il percorso verso il quale si tenta di eseguire l'operazione di ripristino è di sola lettura.

- **Azione correttiva**

  Provare a ripristinare i dati in un'altra posizione.

Il qtree di destinazione è di sola lettura

- **Messaggio**

  `Destination qtree is read-only`

- **Causa**

  Il qtree su cui si tenta di eseguire il ripristino è di sola lettura.

- **Azione correttiva**

  Provare a ripristinare i dati in un'altra posizione.

Dump temporaneamente disattivati sul volume, riprovare

- **Messaggio**

  `Dumps temporarily disabled on volume, try again`

- **Causa**

  Il backup dump NDMP viene tentato su un volume di destinazione SnapMirror che fa parte di uno dei due `snapmirror break` oppure un `snapmirror resync` operazione.

- **Azione correttiva**

  Attendere il `snapmirror break` oppure `snapmirror resync` operazione per terminare e quindi eseguire l'operazione di dump.

  > Ogni volta che lo stato di un volume di destinazione SnapMirror cambia da lettura/scrittura a sola lettura o da sola lettura a lettura/scrittura, è necessario eseguire un backup di riferimento.

Etichette NFS non riconosciute

- **Messaggio**

```
Error: Aborting: dump encountered NFS security labels in the file system
```

- **Causa**

  Le etichette di sicurezza NFS sono supportate a partire da ONTAP 9.9.1 quando NFSv4.2 è attivato. Tuttavia, le etichette di sicurezza NFS non sono attualmente riconosciute dal motore di dump. Se incontra etichette di sicurezza NFS su file, directory o qualsiasi file speciale in qualsiasi formato di dump, il dump non riesce.

- **Azione correttiva**

  Verificare che nessun file o directory abbia etichette di sicurezza NFS.

Nessun file creato

- **Messaggio**

  ```
  No files were created
  ```

- **Causa**

  È stato tentato un DAR di directory senza abilitare la funzionalità DAR avanzata.

- **Azione correttiva**

  Abilitare la funzionalità DAR avanzata e riprovare a eseguire il DAR.

Ripristino del file <file name> non riuscito

- **Messaggio**

  ```
  Restore of the file file name failed
  ```

- **Causa**

  Quando viene eseguito un DAR (Direct Access Recovery) di un file il cui nome file è uguale a quello di un LUN sul volume di destinazione, il DAR non riesce.

- **Azione correttiva**

  Riprovare DAR del file.

Troncamento non riuscito per src inode <inode number>…

- **Messaggio**

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- **Causa**

  L’inode di un file viene cancellato quando il file viene ripristinato.

- **Azione correttiva**

Prima di utilizzare il volume, attendere il completamento dell'operazione di ripristino su un volume.

Impossibile bloccare uno snapshot richiesto dal dump

- **Messaggio**

  `Unable to lock a snapshot needed by dump`

- **Causa**

  La copia Snapshot specificata per il backup non è disponibile.

- **Azione correttiva**

  Riprovare a eseguire il backup con una copia Snapshot diversa.

  Utilizzare `snap list` Per visualizzare l'elenco delle copie Snapshot disponibili.

Impossibile individuare i file bitmap

- **Messaggio**

  `Unable to locate bitmap files`

- **Causa**

  I file bitmap richiesti per l'operazione di backup potrebbero essere stati cancellati. In questo caso, il backup non può essere riavviato.

- **Azione correttiva**

  Eseguire nuovamente il backup.

Il volume si trova temporaneamente in uno stato transitorio

- **Messaggio**

  `Volume is temporarily in a transitional state`

- **Causa**

  Il volume di cui viene eseguito il backup si trova temporaneamente in uno stato non montato.

- **Azione correttiva**

  Attendere qualche istante ed eseguire di nuovo il backup.

Messaggi di errore SMTape

Blocchi fuori servizio

- **Messaggio**

```
Chunks out of order
```

- **Causa**

  I nastri di backup non vengono ripristinati nella sequenza corretta.

- **Azione correttiva**

  Ripetere l'operazione di ripristino e caricare i nastri nella sequenza corretta.

Formato chunk non supportato

- **Messaggio**

```
Chunk format not supported
```

- **Causa**

  L'immagine di backup non è di SMTape.

- **Azione correttiva**

  Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.

Impossibile allocare la memoria

- **Messaggio**

```
Failed to allocate memory
```

- **Causa**

  La memoria del sistema è esaurita.

- **Azione correttiva**

  Riprovare a eseguire il processo in un secondo momento quando il sistema non è troppo occupato.

Impossibile ottenere il buffer dei dati

- **Messaggio**

```
Failed to get data buffer
```

- **Causa**

  Il sistema storage ha esaurito i buffer.

- **Azione correttiva**

  Attendere il completamento di alcune operazioni del sistema di storage, quindi riprovare a eseguire il processo.

Impossibile trovare l'istantanea

- **Messaggio**

  ```
  Failed to find snapshot
  ```

- **Causa**

  La copia Snapshot specificata per il backup non è disponibile.

- **Azione correttiva**

  Controllare se la copia Snapshot specificata è disponibile. In caso contrario, riprovare con la copia Snapshot corretta.

Impossibile creare lo snapshot

- **Messaggio**

  ```
  Failed to create snapshot
  ```

- **Causa**

  Il volume contiene già il numero massimo di copie Snapshot.

- **Azione correttiva**

  Eliminare alcune copie Snapshot, quindi riprovare l'operazione di backup.

Impossibile bloccare snapshot

- **Messaggio**

  ```
  Failed to lock snapshot
  ```

- **Causa**

  La copia Snapshot è in uso o è stata eliminata.

- **Azione correttiva**

  Se la copia Snapshot viene utilizzata da un'altra operazione, attendere il completamento dell'operazione, quindi riprovare a eseguire il backup. Se la copia Snapshot è stata eliminata, non è possibile eseguire il backup.

Impossibile eliminare lo snapshot

- **Messaggio**

  ```
  Failed to delete snapshot
  ```

- **Causa**

  Impossibile eliminare la copia Snapshot automatica perché è in uso da altre operazioni.

- **Azione correttiva**

  Utilizzare `snap` Per determinare lo stato della copia Snapshot. Se la copia Snapshot non è necessaria, eliminarla manualmente.

Impossibile ottenere l'ultimo snapshot

- **Messaggio**

  ```
  Failed to get latest snapshot
  ```

- **Causa**

  La copia Snapshot più recente potrebbe non esistere perché il volume viene inizializzato da SnapMirror.

- **Azione correttiva**

  Riprovare al termine dell'inizializzazione.

Impossibile caricare il nuovo nastro

- **Messaggio**

  ```
  Failed to load new tape
  ```

- **Causa**

  Errore nell'unità a nastro o nel supporto.

- **Azione correttiva**

  Sostituire il nastro e riprovare l'operazione.

Impossibile inizializzare il nastro

- **Messaggio**

  ```
  Failed to initialize tape
  ```

- **Causa**

  Questo messaggio di errore potrebbe essere visualizzato per uno dei seguenti motivi:

  - L'immagine di backup non è di SMTape.
  - Il fattore di blocco del nastro specificato non è corretto.
  - Il nastro è corrotto o danneggiato.
  - Viene caricato il nastro errato per il ripristino.

- **Azione correttiva**
  - Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone di backup SMTape.
  - Se il fattore di blocco non è corretto, specificare il fattore di blocco corretto e riprovare l'operazione.

- Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.
- Se viene caricato il nastro errato, riprovare l'operazione con il nastro corretto.

Impossibile inizializzare il flusso di ripristino

- **Messaggio**

  ```
  Failed to initialize restore stream
  ```

- **Causa**

  Questo messaggio di errore potrebbe essere visualizzato per uno dei seguenti motivi:

  - L'immagine di backup non è di SMTape.
  - Il fattore di blocco del nastro specificato non è corretto.
  - Il nastro è corrotto o danneggiato.
  - Viene caricato il nastro errato per il ripristino.

- **Azione correttiva**
  - Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.
  - Se il fattore di blocco non è corretto, specificare il fattore di blocco corretto e riprovare l'operazione.
  - Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.
  - Se viene caricato il nastro errato, riprovare l'operazione con il nastro corretto.

Impossibile leggere l'immagine di backup

- **Messaggio**

  ```
  Failed to read backup image
  ```

- **Causa**

  Il nastro è corrotto.

- **Azione correttiva**

  Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.

Intestazione immagine mancante o danneggiata

- **Messaggio**

  ```
  Image header missing or corrupted
  ```

- **Causa**

  Il nastro non contiene un backup SMTape valido.

- **Azione correttiva**

  Riprovare con un nastro contenente un backup valido.

Asserzione interna

- **Messaggio**

  ```
  Internal assertion
  ```

- **Causa**

  Si è verificato un errore interno SMTape.

- **Azione correttiva**

  Notificare l'errore e inviare il `etc/log/backup` file al supporto tecnico.

Numero magico dell'immagine di backup non valido

- **Messaggio**

  ```
  Invalid backup image magic number
  ```

- **Causa**

  L'immagine di backup non è di SMTape.

- **Azione correttiva**

  Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.

Checksum immagine di backup non valido

- **Messaggio**

  ```
  Invalid backup image checksum
  ```

- **Causa**

  Il nastro è corrotto.

- **Azione correttiva**

  Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.

Nastro di input non valido

- **Messaggio**

  ```
  Invalid input tape
  ```

- **Causa**

  La firma dell'immagine di backup non è valida nell'intestazione del nastro. Il nastro presenta dati corrotti o non contiene un'immagine di backup valida.

- **Azione correttiva**

  Riprovare a eseguire il processo di ripristino con un'immagine di backup valida.

Percorso del volume non valido

- **Messaggio**

  `Invalid volume path`

- **Causa**

  Il volume specificato per l'operazione di backup o ripristino non viene trovato.

- **Azione correttiva**

  Riprovare a eseguire il processo con un percorso del volume e un nome del volume validi.

Mancata corrispondenza nell'ID set di backup

- **Messaggio**

  `Mismatch in backup set ID`

- **Causa**

  Il nastro caricato durante una sostituzione del nastro non fa parte del set di backup.

- **Azione correttiva**

  Caricare il nastro corretto e riprovare a eseguire il processo.

Mancata corrispondenza nell'indicatore di data e ora del backup

- **Messaggio**

  `Mismatch in backup time stamp`

- **Causa**

  Il nastro caricato durante una sostituzione del nastro non fa parte del set di backup.

- **Azione correttiva**

  Utilizzare `smtape restore -h` comando per verificare le informazioni di intestazione di un nastro.

Processo interrotto a causa dell'arresto

- **Messaggio**

  `Job aborted due to shutdown`

- **Causa**

Riavvio del sistema storage in corso.

- **Azione correttiva**

  Riprovare a eseguire il processo dopo il riavvio del sistema di storage.

Processo interrotto a causa dell'eliminazione automatica di Snapshot

- **Messaggio**

  ```
  Job aborted due to Snapshot autodelete
  ```

- **Causa**

  Il volume non dispone di spazio sufficiente e ha attivato l'eliminazione automatica delle copie Snapshot.

- **Azione correttiva**

  Liberare spazio nel volume e riprovare a eseguire il processo.

Il nastro è attualmente in uso da altre operazioni

- **Messaggio**

  ```
  Tape is currently in use by other operations
  ```

- **Causa**

  L'unità a nastro è in uso da un altro lavoro.

- **Azione correttiva**

  Riprovare a eseguire il backup al termine del processo attualmente attivo.

Nastri fuori servizio

- **Messaggio**

  ```
  Tapes out of order
  ```

- **Causa**

  Il primo nastro della sequenza di nastri per l'operazione di ripristino non ha l'intestazione dell'immagine.

- **Azione correttiva**

  Caricare il nastro con l'intestazione dell'immagine e riprovare a eseguire il processo.

Trasferimento non riuscito (interrotto a causa di un'operazione MetroCluster)

- **Messaggio**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Causa**

  L’operazione SMTape viene interrotta a causa di un’operazione di switchover o switchback.

- **Azione correttiva**

  Eseguire l’operazione SMTape al termine dell’operazione di switchover o switchback.

Trasferimento non riuscito (interruzione avviata da ARL)

- **Messaggio**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Causa**

  Mentre è in corso un’operazione SMTape se viene avviato un trasferimento di aggregato, l’operazione SMTape viene interrotta.

- **Azione correttiva**

  Eseguire l’operazione SMTape al termine dell’operazione di trasferimento degli aggregati.

Trasferimento non riuscito (interruzione avviata da CFO)

- **Messaggio**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Causa**

  L’operazione SMTape viene interrotta a causa di un’operazione di failover dello storage (Takeover e giveback) di un aggregato CFO.

- **Azione correttiva**

  Eseguire l’operazione SMTape al termine del failover dello storage dell’aggregato CFO.

Trasferimento non riuscito (interruzione avviata da SFO)

- **Messaggio**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Causa**

  L’operazione SMTape viene interrotta a causa di un’operazione di failover dello storage (Takeover e giveback).

- **Azione correttiva**

  Eseguire l’operazione SMTape al termine dell’operazione di failover dello storage (Takeover e giveback).

Aggregato sottostante in fase di migrazione

- **Messaggio**

  ```
  Underlying aggregate under migration
  ```

- **Causa**

  Se viene avviata un'operazione SMTape su un aggregato in fase di migrazione (failover dello storage o riposizionamento dell'aggregato), l'operazione SMTape non riesce.

- **Azione correttiva**

  Eseguire l'operazione SMTape al termine della migrazione aggregata.

Il volume è attualmente in fase di migrazione

- **Messaggio**

  ```
  Volume is currently under migration
  ```

- **Causa**

  La migrazione dei volumi e il backup SMTape non possono essere eseguiti contemporaneamente.

- **Azione correttiva**

  Riprovare a eseguire il processo di backup al termine della migrazione del volume.

Volume offline

- **Messaggio**

  ```
  Volume offline
  ```

- **Causa**

  Il volume di cui viene eseguito il backup non è in linea.

- **Azione correttiva**

  Portare il volume online e riprovare il backup.

Volume non limitato

- **Messaggio**

  ```
  Volume not restricted
  ```

- **Causa**

  Il volume di destinazione in cui vengono ripristinati i dati non è limitato.

- **Azione correttiva**

Limitare il volume e riprovare l'operazione di ripristino.

Configurazione NDMP

Panoramica della configurazione NDMP

È possibile configurare rapidamente un cluster ONTAP 9 in modo che utilizzi il protocollo di gestione dei dati di rete (NDMP) per eseguire il backup dei dati direttamente su nastro utilizzando un'applicazione di backup di terze parti.

Se l'applicazione di backup supporta Cluster Aware Backup (CAB), è possibile configurare NDMP come *SVM-scoped* o *node-scoped*:

- SVM-scope a livello di cluster (admin SVM) consente di eseguire il backup di tutti i volumi ospitati su diversi nodi del cluster. Se possibile, si consiglia di utilizzare NDMP con ambito SVM.
- NDMP con ambito nodo consente di eseguire il backup di tutti i volumi ospitati su quel nodo.

Se l'applicazione di backup non supporta CAB, è necessario utilizzare NDMP con ambito nodo.

Gli NDMP con ambito SVM e nodo si escludono a vicenda e non possono essere configurati sullo stesso cluster.

NDMP con ambito del nodo è obsoleto in ONTAP 9.

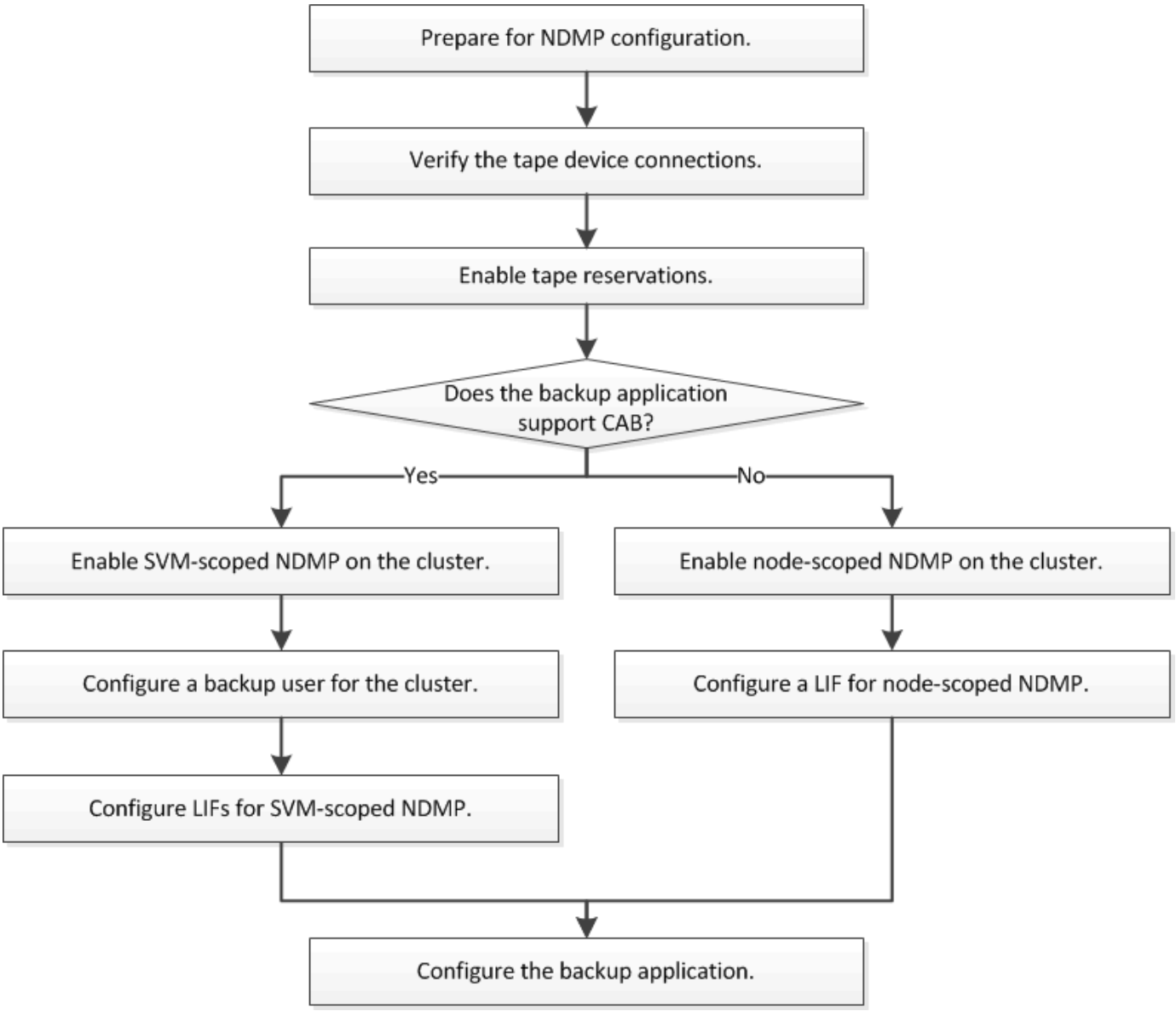
Scopri di più "Backup cluster-aware (CAB)".

Prima di configurare NDMP, verificare quanto segue:

- Si dispone di un'applicazione di backup di terze parti (chiamata anche Data Management Application o DMA).
- Sei un amministratore del cluster.
- Sono installati i dispositivi a nastro e un server multimediale opzionale.
- I dispositivi a nastro sono collegati al cluster tramite uno switch Fibre Channel (FC) e non direttamente.
- Almeno un dispositivo a nastro ha un numero di unità logica (LUN) pari a 0.

Workflow di configurazione NDMP

L'impostazione del backup su nastro su NDMP richiede la preparazione della configurazione NDMP, la verifica delle connessioni dei dispositivi a nastro, l'attivazione delle prenotazioni su nastro, la configurazione di NDMP a livello di SVM o di nodo, l'abilitazione di NDMP sul cluster, la configurazione di un utente di backup, la configurazione di LIF e la configurazione dell'applicazione di backup.



Preparazione per la configurazione NDMP

Prima di configurare l'accesso al backup su nastro tramite NDMP (Network Data Management Protocol), è necessario verificare che la configurazione pianificata sia supportata, verificare che le unità a nastro siano elencate come unità qualificate su ciascun nodo, verificare che tutti i nodi dispongano di LIF intercluster, E identificare se l'applicazione di backup supporta l'estensione CAB (Cluster Aware Backup).

Fasi

1. Fare riferimento alla matrice di compatibilità del provider di applicazioni di backup per il supporto ONTAP (NetApp non qualifica le applicazioni di backup di terze parti con ONTAP o NDMP).

   Verificare che i seguenti componenti NetApp siano compatibili:

   - La versione di ONTAP 9 in esecuzione sul cluster.
   - Il vendor e la versione dell'applicazione di backup: Ad esempio, Veritas NetBackup 8.2 o CommVault.

- I dettagli dei dispositivi a nastro, come il produttore, il modello e l'interfaccia delle unità a nastro, ad esempio IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Le piattaforme dei nodi nel cluster, ad esempio FAS8700 o A400.

> Le matrici di supporto per la compatibilità ONTAP legacy per le applicazioni di backup sono disponibili in "Tool di matrice di interoperabilità NetApp".

2. Verificare che le unità a nastro siano elencate come unità qualificate nel file di configurazione del nastro integrato di ciascun nodo:

   a. Nell'interfaccia della riga di comando, visualizzare il file di configurazione del nastro integrato utilizzando `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
------------------------------   ---------
-------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. Confrontare le unità a nastro con l'elenco delle unità qualificate nell'output.

> I nomi dei dispositivi a nastro nell'output potrebbero variare leggermente rispetto ai nomi sull'etichetta del dispositivo o nella matrice di interoperabilità. Ad esempio, Digital DLT2000 può anche essere noto come DLT2k. È possibile ignorare queste differenze di denominazione minori.

   c. Se un dispositivo non è elencato come qualificato nell'output anche se il dispositivo è qualificato secondo la matrice di interoperabilità, scaricare e installare un file di configurazione aggiornato per il dispositivo utilizzando le istruzioni sul sito del supporto NetApp.

      "Download NetApp: File di configurazione dei dispositivi su nastro"

   Un dispositivo qualificato potrebbe non essere elencato nel file di configurazione del nastro integrato se il dispositivo a nastro è stato qualificato dopo la spedizione del nodo.

3. Verificare che ogni nodo del cluster disponga di una LIF intercluster:

   a. Visualizzare le LIF di intercluster sui nodi utilizzando `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

b. Se non esiste una LIF di intercluster su un nodo, creare una LIF di intercluster utilizzando `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

"Gestione della rete"

4. Identificare se l'applicazione di backup supporta Cluster Aware Backup (CAB) utilizzando la documentazione fornita con l'applicazione di backup.

   Il supporto CAB è un fattore chiave per determinare il tipo di backup che è possibile eseguire.

Verificare le connessioni del dispositivo a nastro

Assicurarsi che tutti i dischi e i media changer siano visibili in ONTAP come dispositivi.

Fasi

1. Visualizzare le informazioni su tutti i dischi e i media changer utilizzando `storage tape show` comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11                tape drive      HP LTO-3
normal
0b.125L1                 media changer   HP MSL G3 Series
normal
0d.4                     tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                   media changer   IBM 3573-TL
normal
...
```

2. Se non viene visualizzata un'unità a nastro, risolvere il problema.
3. Se non viene visualizzato un media changer, visualizzare le informazioni sui media changer utilizzando `storage tape show-media-changer` e risolvere il problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Attivare le prenotazioni su nastro

È necessario assicurarsi che le unità a nastro siano riservate all'utilizzo da parte delle applicazioni di backup per le operazioni di backup NDMP.

A proposito di questa attività

Le impostazioni di prenotazione variano in diverse applicazioni di backup e devono corrispondere all'applicazione di backup e ai nodi o ai server che utilizzano gli stessi dischi. Consultare la documentazione del fornitore dell'applicazione di backup per le impostazioni di prenotazione corrette.

Fasi

1. Attivare le prenotazioni utilizzando `options -option-name tape.reservations -option-value persistent` comando.

   Il seguente comando consente di attivare le prenotazioni con `persistent` valore:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Verificare che le prenotazioni siano attivate su tutti i nodi utilizzando `options tape.reservations` e quindi esaminare l'output.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                 persistent

   cluster1-2
       tape.reservations                 persistent
   2 entries were displayed.
   ```

Configurare NDMP con ambito SVM

Abilitare NDMP con ambito SVM sul cluster

Se il DMA supporta l'estensione CAB (Cluster Aware Backup), è possibile eseguire il backup di tutti i volumi ospitati su diversi nodi di un cluster attivando NDMP con ambito SVM, attivando il servizio NDMP sul cluster (SVM amministrativa) e configurando i LIF per la connessione dati e di controllo.

Di cosa hai bisogno

L'estensione DELLA CABINA deve essere supportata dal DMA.

A proposito di questa attività

La disattivazione della modalità NDMP con ambito nodo attiva la modalità NDMP con ambito SVM sul cluster.

Fasi

1. Abilita la modalità NDMP SVM-scoped:

```
cluster1::> system services ndmp node-scope-mode off
```

   La modalità NDMP SVM-scoped è abilitata.

2. Attivare il servizio NDMP sulla SVM di amministrazione:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

   Il tipo di autenticazione è impostato su `challenge` per impostazione predefinita, l'autenticazione in chiaro è disattivata.

   > Per una comunicazione sicura, è necessario disattivare l'autenticazione in chiaro.

3. Verificare che il servizio NDMP sia abilitato:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Abilitare un utente di backup per l'autenticazione NDMP

Per autenticare NDMP con ambito SVM dall'applicazione di backup, è necessario disporre di un utente amministrativo con privilegi sufficienti e di una password NDMP.

A proposito di questa attività

È necessario generare una password NDMP per gli utenti amministratori del backup. È possibile abilitare gli utenti amministratori di backup a livello di cluster o SVM e, se necessario, creare un nuovo utente. Per impostazione predefinita, gli utenti con i seguenti ruoli possono eseguire l'autenticazione per il backup NDMP:

- A livello di cluster: `admin` oppure `backup`
- SVM individuali: `vsadmin` oppure `vsadmin-backup`

Se si utilizza un utente NIS o LDAP, l'utente deve esistere sul rispettivo server. Non è possibile utilizzare un utente Active Directory.

Fasi

1. Visualizza gli utenti e i permessi di amministrazione correnti:

```
security login show
```

2. Se necessario, creare un nuovo utente di backup NDMP con `security login create` E il ruolo appropriato per i privilegi SVM a livello di cluster o singoli.

   È possibile specificare un nome utente per il backup locale o un nome utente NIS o LDAP per `-user-or-group-name` parametro.

   Il seguente comando crea l'utente di backup `backup_admin1` con `backup` ruolo per l'intero cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   Il seguente comando crea l'utente di backup `vsbackup_admin1` con `vsadmin-backup` Ruolo di una singola SVM:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Inserire una password per il nuovo utente e confermare.

3. Generare una password per la SVM amministrativa utilizzando `vserver services ndmp generate password` comando.

   La password generata deve essere utilizzata per autenticare la connessione NDMP dall'applicazione di backup.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configurare le LIF

È necessario identificare le LIF che verranno utilizzate per stabilire una connessione dati tra le risorse di dati e nastro e per controllare la connessione tra la SVM amministrativa e l'applicazione di backup. Dopo aver identificato i LIF, è necessario verificare che i criteri di firewall e failover siano impostati per i LIF e specificare il ruolo di interfaccia preferito.

A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "LIF e policy di servizio in ONTAP 9.6 e versioni successive".

Fasi

1. Identificare le LIF di gestione di intercluster, cluster e nodi utilizzando `network interface show` con il `-role` parametro.

   Il seguente comando visualizza le LIF dell'intercluster:

```
cluster1::> network interface show -role intercluster

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    IC1               up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2               up/up      192.0.2.68/24      cluster1-2
e0b     true
```

Il seguente comando visualizza la LIF di gestione del cluster:

```
cluster1::> network interface show -role cluster-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------
------------- ------- ----
cluster1    cluster_mgmt      up/up      192.0.2.60/24      cluster1-2
e0M     true
```

Il seguente comando visualizza le LIF di gestione dei nodi:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------        ---------- ------------------ ------------
------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24      cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24      cluster1-2
e0M     true
```

2. Assicurarsi che il criterio firewall sia abilitato per NDMP sulle LIF di intercluster, gestione cluster (gestione cluster) e gestione nodi (gestione nodi):

a. Verificare che il criterio firewall sia abilitato per NDMP utilizzando `system services firewall policy show` comando.

Il seguente comando visualizza il criterio del firewall per la LIF di gestione del cluster:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                        ** ndmp       0.0.0.0/0**
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

Il seguente comando visualizza il criterio firewall per la LIF di gestione dei nodi:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando `system services firewall policy modify` con il `-service` parametro.

   Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Assicurarsi che la policy di failover sia impostata correttamente per tutte le LIF:

   a. Verificare che il criterio di failover per la LIF di gestione del cluster sia impostato su `broadcast-domain-wide`E il criterio per le LIF di gestione di intercluster e nodi è impostato su `local-only` utilizzando `network interface show -failover` comando.

      Il seguente comando visualizza il criterio di failover per le LIF di gestione del cluster, dell'intercluster e dei nodi:

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ----------------- --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover Targets:
                                                     .......

**cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-wide
Default**
                                                     Failover Targets:
                                                     .......
           **IC1                 cluster1-1:e0a    local-only
Default**
                                                     Failover Targets:
           **IC2                 cluster1-1:e0b    local-only
Default**
                                                     Failover Targets:
                                                     .......
**cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
**cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default**
                                                     Failover Targets:
                                                     ......
```

a. Se i criteri di failover non sono impostati correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Specificare le LIF richieste per la connessione dati utilizzando `vserver services ndmp modify` con il `preferred-interface-role` parametro.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verificare che il ruolo di interfaccia preferito sia impostato per il cluster utilizzando `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt, node-
mgmt
```

Configurare NDMP con ambito nodo

Abilitare NDMP con ambito di nodo sul cluster

È possibile eseguire il backup dei volumi ospitati su un singolo nodo attivando NDMP con ambito nodo, attivando il servizio NDMP e configurando una LIF per la connessione dati e di controllo. Questa operazione può essere eseguita per tutti i nodi del cluster.

> NDMP con ambito del nodo è obsoleto in ONTAP 9.

A proposito di questa attività

Quando si utilizza NDMP in modalità Node-Scope, l'autenticazione deve essere configurata per nodo. Per ulteriori informazioni, vedere "L'articolo della Knowledge base "come configurare l'autenticazione NDMP in modalità 'node-scope'"".

Fasi

1. Abilita la modalità NDMP con ambito dei nodi:

```
cluster1::> system services ndmp node-scope-mode on
```

   La modalità ambito-nodo NDMP è abilitata.

2. Abilitare il servizio NDMP su tutti i nodi nel cluster:

   L'utilizzo del carattere jolly "*" attiva il servizio NDMP su tutti i nodi contemporaneamente.

   Specificare una password per l'autenticazione della connessione NDMP da parte dell'applicazione di backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Disattivare `-clear-text` Opzione per la comunicazione sicura della password NDMP:

   Utilizzando il carattere jolly “*” disables the `-clear-text` su tutti i nodi contemporaneamente.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Verificare che il servizio NDMP sia attivato e il `-clear-text` opzione disattivata:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurare una LIF

È necessario identificare una LIF che verrà utilizzata per stabilire una connessione dati e controllare la connessione tra il nodo e l’applicazione di backup. Dopo aver identificato la LIF, è necessario verificare che i criteri di firewall e failover siano impostati per la LIF.

> A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere "Configurare le policy firewall per le LIF".

Fasi

1. Identificare la LIF di intercluster ospitata sui nodi utilizzando `network interface show` con il `-role` parametro.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1    e0a
true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2    e0b
true
```

2. Assicurarsi che il criterio firewall sia abilitato per NDMP sulle LIF dell'intercluster:

   a. Verificare che il criterio firewall sia abilitato per NDMP utilizzando `system services firewall policy show` comando.

      Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         **ndmp       0.0.0.0/0, ::/0**
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando `system services firewall policy modify` con il `-service` parametro.

      Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Assicurarsi che il criterio di failover sia impostato correttamente per le LIF dell'intercluster:

a. Verificare che il criterio di failover per le LIF dell'intercluster sia impostato su `local-only` utilizzando `network interface show -failover` comando.

```
cluster1::> network interface show -failover
            Logical          Home               Failover     Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  ----------------- ------------ --------
cluster1    **IC1               cluster1-1:e0a    local-only
Default**
                                                    Failover Targets:
                                                    .......
            **IC2               cluster1-2:e0b    local-only
Default**
                                                    Failover Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only    Default
                                                    Failover Targets:
                                                    .......
```

b. Se il criterio di failover non è impostato correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Configurare l'applicazione di backup

Una volta configurato il cluster per l'accesso NDMP, è necessario raccogliere informazioni dalla configurazione del cluster e configurare il resto del processo di backup nell'applicazione di backup.

Fasi

1. Raccogliere le seguenti informazioni configurate in precedenza in ONTAP:
   - Nome utente e password richiesti dall'applicazione di backup per creare la connessione NDMP
   - Gli indirizzi IP delle LIF di intercluster richieste dall'applicazione di backup per la connessione al cluster
2. In ONTAP, visualizzare gli alias assegnati da ONTAP a ciascun dispositivo utilizzando `storage tape alias show` comando.

   Gli alias sono spesso utili nella configurazione dell'applicazione di backup.

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                        Alias     Mapping
--------------------------- --------- ------------------------------
stsw-3220-4a-4b-02          st2       SN[HU19497WVR]
...
```

3. Nell'applicazione di backup, configurare il resto del processo di backup utilizzando la documentazione dell'applicazione di backup.

Al termine

Se si verifica un evento di mobilità dei dati, ad esempio uno spostamento del volume o una migrazione LIF, è necessario essere pronti a reinizializzare le operazioni di backup interrotte.

Replica tra il software NetApp Element e ONTAP

Replica tra software NetApp Element e panoramica di ONTAP

È possibile garantire la continuità del business su un sistema di elementi utilizzando SnapMirror per replicare le copie Snapshot di un volume di elementi in una destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il sistema Element al ripristino del servizio.

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un nodo ONTAP in un sistema di elementi. È possibile che sia stata creata una LUN durante un'interruzione del servizio presso il sito Element o che si stia utilizzando una LUN per migrare i dati da ONTAP a Element Software.

Si consiglia di utilizzare il backup Element to ONTAP se si applicano le seguenti condizioni:

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI) di ONTAP, non Gestione di sistema o uno strumento di scripting automatico.
- Si sta utilizzando iSCSI per fornire dati ai client.

Per ulteriori informazioni sulla configurazione o concettuali, consultare la seguente documentazione:

- Configurazione dell'elemento

  "Documentazione del software NetApp Element"

- Concetti e configurazione di SnapMirror

  "Panoramica sulla protezione dei dati"

Sulla replica tra Element e ONTAP

A partire da ONTAP 9.3, è possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in una destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un nodo ONTAP in un sistema di elementi. È possibile che sia stata creata una LUN durante un'interruzione del servizio presso il sito Element o che si stia utilizzando una LUN per migrare i dati da ONTAP a Element Software.

Tipi di relazione di protezione dei dati

SnapMirror offre due tipi di relazione per la protezione dei dati. Per ciascun tipo, SnapMirror crea una copia Snapshot del volume di origine dell'elemento prima di inizializzare o aggiornare la relazione:

- In una relazione di protezione dei dati di *disaster recovery (DR)*, il volume di destinazione contiene solo la copia Snapshot creata da SnapMirror, da cui è possibile continuare a fornire i dati in caso di disastro nel sito primario.
- In una relazione di *conservazione a lungo termine* data Protection, il volume di destinazione contiene copie Snapshot point-in-time create dal software Element, nonché la copia Snapshot creata da SnapMirror. Ad esempio, è possibile conservare le copie Snapshot mensili create nell'arco di 20 anni.

Policy predefinite

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. La *policy SnapMirror* definisce il contenuto della linea di base e gli eventuali aggiornamenti.

È possibile utilizzare una policy predefinita o personalizzata quando si crea una relazione di protezione dei dati. Il *tipo di policy* determina quali copie Snapshot includere e quante copie conservare.

La tabella seguente mostra i criteri predefiniti. Utilizzare `MirrorLatest` Policy per creare una relazione DR tradizionale. Utilizzare `MirrorAndVault` oppure `Unified7year` Policy per creare una relazione di replica unificata, in cui DR e conservazione a lungo termine sono configurati sullo stesso volume di destinazione.

Policy	Tipo di policy	Comportamento degli aggiornamenti
MirrorLatest	mirror asincrono	Trasferire la copia Snapshot creata da SnapMirror.
MirrorAndVault	vault mirror	Trasferire la copia Snapshot creata da SnapMirror e le copie Snapshot meno recenti effettuate dall'ultimo aggiornamento, a condizione che siano dotate di etichette SnapMirror "daily" o "settimanale".
Unified7year	vault mirror	Trasferire la copia Snapshot creata da SnapMirror e le copie Snapshot meno recenti effettuate dall'ultimo aggiornamento, a condizione che siano dotate delle etichette SnapMirror "daily", "settimanale" o "mOnhly".

Per informazioni complete sulle policy di SnapMirror, incluse indicazioni su quali policy utilizzare, vedere "Protezione dei dati".

Informazioni sulle etichette SnapMirror

Ogni policy con il tipo di policy “mirror-vault” deve avere una regola che specifica quali copie Snapshot replicare. La regola “daily”, ad esempio, indica che solo le copie Snapshot assegnate all’etichetta SnapMirror “daily” devono essere replicate. L’etichetta SnapMirror viene assegnata quando si configurano le copie Snapshot degli elementi.

Replica da un cluster di origine elemento a un cluster di destinazione ONTAP

È possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in un sistema di destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

Un volume Element equivale approssimativamente a un LUN ONTAP. SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP. SnapMirror replica i dati su un LUN esistente se il LUN soddisfa i requisiti per la replica Element to ONTAP.

Le regole di replica sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume elemento.
- Non è possibile replicare i dati da un volume ONTAP a più volumi di elementi.

Replica da un cluster di origine ONTAP a un cluster di destinazione elemento

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un sistema ONTAP in un volume Element:

- Se esiste già una relazione SnapMirror tra un’origine elemento e una destinazione ONTAP, un LUN creato durante la fornitura dei dati dalla destinazione viene replicato automaticamente quando l’origine viene riattivata.
- In caso contrario, è necessario creare e inizializzare una relazione SnapMirror tra il cluster di origine ONTAP e il cluster di destinazione degli elementi.

Le regole di replica sono le seguenti:

- La relazione di replica deve avere una policy di tipo “async-mirror”.

  Le policy di tipo “mirror-vault” non sono supportate.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

Prerequisiti

Prima di configurare una relazione di protezione dei dati tra Element e ONTAP, è necessario aver completato le seguenti attività:

- Il cluster di elementi deve eseguire il software NetApp Element versione 10.1 o successiva.
- Il cluster ONTAP deve eseguire ONTAP 9.3 o versione successiva.
- SnapMirror deve essere stato concesso in licenza sul cluster ONTAP.

- È necessario configurare volumi nei cluster Element e ONTAP sufficientemente grandi per gestire i trasferimenti di dati anticipati.
- Se si utilizza il tipo di policy “mirror-vault”, è necessario configurare un’etichetta SnapMirror per la replica delle copie Snapshot degli elementi.

> È possibile eseguire questa attività solo nell’interfaccia utente Web del software Element. Per ulteriori informazioni, consultare "Documentazione del software NetApp Element"

- È necessario assicurarsi che la porta 5010 sia disponibile.
- Se si prevede che potrebbe essere necessario spostare un volume di destinazione, è necessario assicurarsi che la connettività full-mesh esista tra l’origine e la destinazione. Ogni nodo del cluster di origine degli elementi deve essere in grado di comunicare con ogni nodo del cluster di destinazione ONTAP.

Dettagli del supporto

La seguente tabella mostra i dettagli del supporto per il backup Element to ONTAP.

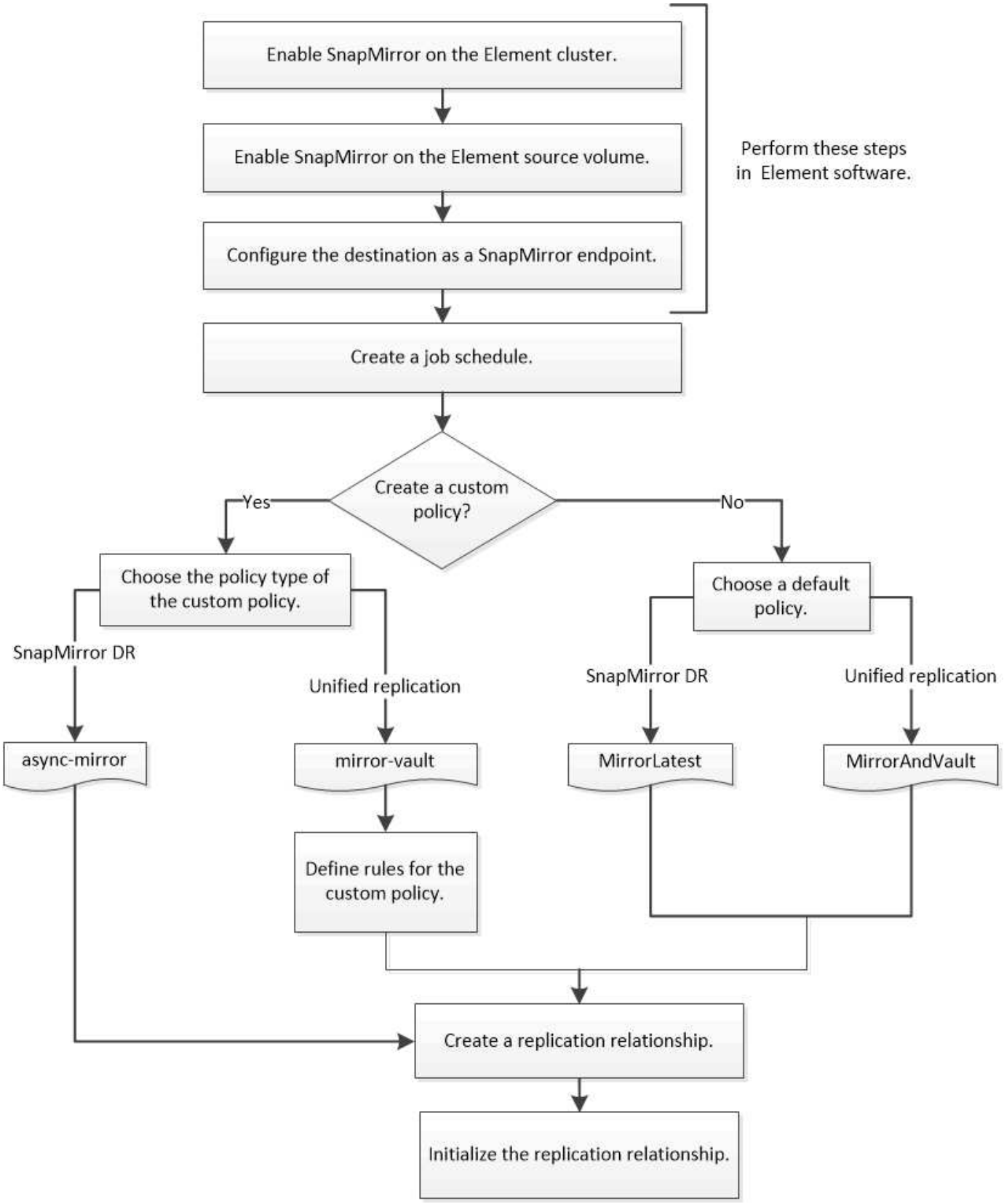
Risorsa o funzione	Dettagli del supporto
SnapMirror	• La funzione di ripristino di SnapMirror non è supportata. • Il `MirrorAllSnapshots` e. `XDPDefault` i criteri non sono supportati. • Il tipo di policy “vault” non è supportato. • La regola definita dal sistema “all_source_snapshot” non è supportata. • Il tipo di policy “mirror-vault” è supportato solo per la replica dal software Element a ONTAP. Utilizzare “async-mirror” per la replica da ONTAP al software Element. • Il `-schedule` e. `-prefix` opzioni per `snapmirror policy add-rule` non sono supportati. • Il `-preserve` e. `-quick-resync` opzioni per `snapmirror resync` non sono supportati. • L’efficienza dello storage non viene preservata. • Le implementazioni di protezione dei dati fan-out e cascata non sono supportate.
ONTAP	• ONTAP Select è supportato a partire da ONTAP 9.4 ed Element 10.3. • Cloud Volumes ONTAP è supportato a partire da ONTAP 9.5 ed Element 11.0.
Elemento	• Il limite delle dimensioni del volume è 8 TIB. • La dimensione del blocco di volume deve essere di 512 byte. Le dimensioni di un blocco di 4K byte non sono supportate. • Le dimensioni del volume devono essere un multiplo di 1 MiB. • Gli attributi del volume non vengono conservati. • Il numero massimo di copie Snapshot da replicare è 30.

Rete	• È consentita una singola connessione TCP per ogni trasferimento. • Il nodo Element deve essere specificato come indirizzo IP. La ricerca del nome host DNS non è supportata. • Gli IPspaces non sono supportati.
SnapLock	I volumi SnapLock non sono supportati.
FlexGroup	I volumi FlexGroup non sono supportati.
DR. SVM	I volumi ONTAP in una configurazione DR SVM non sono supportati.
MetroCluster	I volumi ONTAP in una configurazione MetroCluster non sono supportati.

Workflow per la replica tra Element e ONTAP

Sia che si stiano replicando i dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione del processo, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare un criterio predefinito o personalizzato.

Il flusso di lavoro presuppone che siano state completate le attività preliminari elencate nella Prerequisiti. Per informazioni complete sulle policy di SnapMirror, incluse indicazioni su quali policy utilizzare, vedere "Protezione dei dati".



Attivare SnapMirror nel software Element

Attivare SnapMirror sul cluster di elementi

È necessario attivare SnapMirror sul cluster di elementi prima di poter creare una

relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.

Prima di iniziare

- Il cluster di elementi deve eseguire il software NetApp Element versione 10.1 o successiva.
- SnapMirror può essere abilitato solo per i cluster di elementi utilizzati con i volumi NetApp ONTAP.

A proposito di questa attività

Il sistema Element viene fornito con SnapMirror disattivato per impostazione predefinita. SnapMirror non viene attivato automaticamente come parte di una nuova installazione o di un aggiornamento.

> Una volta attivato, SnapMirror non può essere disattivato. È possibile disattivare la funzione SnapMirror e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster.

Fasi

1. Fare clic su **Clusters** > **Impostazioni**.
2. Individuare le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Enable SnapMirror** (attiva SnapMirror

Attivare SnapMirror sul volume di origine dell'elemento

Prima di creare una relazione di replica, è necessario attivare SnapMirror sul volume di origine dell'elemento. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.

Prima di iniziare

- È necessario aver attivato SnapMirror sul cluster di elementi.
- La dimensione del blocco del volume deve essere di 512 byte.
- Il volume non deve partecipare alla replica remota degli elementi.
- Il tipo di accesso al volume non deve essere "Replication Target".

A proposito di questa attività

La procedura riportata di seguito presuppone che il volume esista già. È inoltre possibile attivare SnapMirror quando si crea o clona un volume.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Selezionare ⚙ per il volume.
3. Nel menu a discesa, selezionare **Modifica**.
4. Nella finestra di dialogo **Edit Volume** (Modifica volume), selezionare **Enable SnapMirror** (attiva SnapMirror).
5. Selezionare **Save Changes** (Salva modifiche).

Creare un endpoint SnapMirror

È necessario creare un endpoint SnapMirror prima di poter creare una relazione di

replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.

Prima di iniziare

È necessario aver attivato SnapMirror sul cluster di elementi.

Fasi

1. Fare clic su **Data Protection** > **SnapMirror Endpoints**.
2. Fare clic su **Create Endpoint** (Crea endpoint).
3. Nella finestra di dialogo **Crea nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster ONTAP.
4. Inserire l'ID utente e la password dell'amministratore del cluster ONTAP.
5. Fare clic su **Create Endpoint** (Crea endpoint).

Configurare una relazione di replica

Creare una pianificazione del processo di replica

Sia che si stiano replicando i dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione del processo, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare un criterio predefinito o personalizzato.

È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo di replica. La pianificazione del processo determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui viene assegnata la pianificazione.

A proposito di questa attività

Quando si crea una relazione di protezione dei dati, viene assegnata una pianificazione dei processi. Se non si assegna una pianificazione del lavoro, è necessario aggiornare la relazione manualmente.

Fase

1. Creare una pianificazione del processo:

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

   A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

   ```
   job schedule cron create -name job_name -vserver Vserver_name -month month
   -dayofweek day_of_week -day day_of_month -hour hour -minute minute
   ```

   Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

Personalizzare un criterio di replica

Creare un criterio di replica personalizzato

È possibile utilizzare un criterio predefinito o personalizzato quando si crea una relazione di replica. Per una policy di replica unificata personalizzata, è necessario definire una o più *regole* che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

È possibile creare un criterio di replica personalizzato se il criterio predefinito per una relazione non è adatto. È possibile, ad esempio, comprimere i dati in un trasferimento di rete o modificare il numero di tentativi eseguiti da SnapMirror per trasferire le copie Snapshot.

A proposito di questa attività

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

Tipo di policy	Tipo di relazione
mirror asincrono	Dr. SnapMirror
vault mirror	Replica unificata

Fase

1. Creare un criterio di replica personalizzato:

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority
   low|normal -is-network-compression-enabled true|false
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia Snapshot comune per le relazioni sincroni di SnapMirror utilizzando `-common-snapshot -schedule` parametro. Per impostazione predefinita, il programma di copia Snapshot comune per le relazioni sincrone di SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia Snapshot per le relazioni sincroni di SnapMirror.

   Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che consente la compressione di rete per i trasferimenti di dati:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_compressed -type async-mirror -comment "DR with network compression
   enabled" -is-network-compression-enabled true
   ```

   Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Al termine

Per i tipi di policy “mirror-vault”, è necessario definire le regole che determinano quali copie Snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento.

Utilizzare `snapmirror policy show` Per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina man.

Definire una regola per un criterio

Per i criteri personalizzati con il tipo di policy “mirror-vault”, è necessario definire almeno una regola che determina quali copie Snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento. È inoltre possibile definire le regole per i criteri di default con il tipo di policy “mirror-vault”.

A proposito di questa attività

Ogni policy con il tipo di policy “mirror-vault” deve avere una regola che specifica quali copie Snapshot replicare. La regola “bimestrale”, ad esempio, indica che devono essere replicate solo le copie Snapshot assegnate all’etichetta SnapMirror “bimestrale”. L’etichetta SnapMirror viene assegnata quando si configurano le copie Snapshot degli elementi.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate automaticamente a un criterio quando si specifica il relativo tipo di criterio. La tabella seguente mostra le regole definite dal sistema.

Regola definita dal sistema	Utilizzato nei tipi di policy	Risultato
sm_created	mirror asincrono, vault mirror	Una copia Snapshot creata da SnapMirror viene trasferita all’inizializzazione e all’aggiornamento.
ogni giorno	vault mirror	Le nuove copie Snapshot sull’origine con l’etichetta SnapMirror “daily” vengono trasferite all’inizializzazione e all’aggiornamento.
settimanale	vault mirror	Le nuove copie Snapshot sull’origine con l’etichetta SnapMirror “settimanale” vengono trasferite all’inizializzazione e all’aggiornamento.

mensile	vault mirror	Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "mOnhly" vengono trasferite all'inizializzazione e all'aggiornamento.

È possibile specificare regole aggiuntive in base alle esigenze, per i criteri predefiniti o personalizzati. Ad esempio:

- Per impostazione predefinita `MirrorAndVault` Policy, è possibile creare una regola chiamata "bimestrale" per associare le copie Snapshot sull'origine con l'etichetta "bimestrale" SnapMirror.
- Per una policy personalizzata con il tipo di policy "mirror-vault", è possibile creare una regola chiamata "bisettimanale" per far corrispondere le copie Snapshot sull'origine con l'etichetta "bisettimanale" SnapMirror.

Fase

1. Definire una regola per un criterio:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-monthly` al valore predefinito `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-weekly` al personalizzato `my_snapvault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `app_consistent` al personalizzato `Sync` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   È quindi possibile replicare le copie Snapshot dal cluster di origine che corrispondono a questa etichetta SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Creare una relazione di replica

Creare una relazione da un'origine elemento a una destinazione ONTAP

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita *relazione di protezione dei dati*. È possibile utilizzare `snapmirror create` Comando per creare una relazione di protezione dei dati da un'origine elemento a una destinazione ONTAP o da un'origine ONTAP a una destinazione elemento.

È possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in un sistema di destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.
- Se si utilizza il tipo di policy "mirror-vault", è necessario configurare un'etichetta SnapMirror per la replica delle copie Snapshot degli elementi.

> È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element. Per ulteriori informazioni, consultare "Documentazione degli elementi".

A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Un volume Element equivale approssimativamente a un LUN ONTAP. SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP. SnapMirror replica i dati su un LUN esistente se il LUN soddisfa i requisiti per la replica dal software Element a ONTAP.

Le regole di replica sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume elemento.
- Non è possibile replicare i dati da un volume ONTAP a più volumi di elementi.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.

Fase

1. Dal cluster di destinazione, creare una relazione di replica da un'origine elemento a una destinazione ONTAP:

   ```
   snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume
   ```

|*cluster://SVM/volume* -type XDP -schedule schedule -policy *policy*

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorLatest` policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando `Unified7year` policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando il metodo personalizzato `my_unified` policy:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Creare una relazione da un'origine ONTAP a una destinazione dell'elemento

A partire da ONTAP 9.4, è possibile utilizzare SnapMirror per replicare le copie Snapshot di un LUN creato su un'origine ONTAP verso una destinazione dell'elemento. È possibile che si stia utilizzando il LUN per migrare i dati da ONTAP a Element Software.

Prima di iniziare

- Il nodo di destinazione dell'elemento deve essere stato reso accessibile a ONTAP.

- Il volume Element deve essere stato abilitato per la replica di SnapMirror.

A proposito di questa attività

Specificare il percorso di destinazione dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Le regole di replica sono le seguenti:

- La relazione di replica deve avere una policy di tipo "async-mirror".

  È possibile utilizzare un criterio predefinito o personalizzato.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

Fase

1. Creare una relazione di replica da un'origine ONTAP a una destinazione dell'elemento:

   `snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -type XDP -schedule schedule -policy policy`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorLatest` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   Nell'esempio riportato di seguito viene creata una relazione di DR SnapMirror utilizzando il metodo personalizzato `my_mirror` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Inizializzare una relazione di replica

Per tutti i tipi di relazione, l'inizializzazione esegue un *trasferimento baseline*: Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.
- Se si utilizza il tipo di policy “mirror-vault”, è necessario configurare un’etichetta SnapMirror per la replica delle copie Snapshot degli elementi.

A proposito di questa attività

Specificare il percorso di origine dell’elemento nel modulo `hostip:/lun/name`, dove “lun” è la stringa effettiva “lun” e. `name` È il nome del volume Element.

L’inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

> Se l’inizializzazione di una relazione da un’origine ONTAP a una destinazione dell’elemento non riesce per qualsiasi motivo, continuerà a fallire anche dopo aver corretto il problema (ad esempio, un nome LUN non valido). La soluzione è la seguente:
>
> 1. Eliminare la relazione.
> 2. Eliminare il volume di destinazione dell’elemento.
> 3. Creare un nuovo volume di destinazione elemento.
> 4. Creare e inizializzare una nuova relazione dall’origine ONTAP al volume di destinazione dell’elemento.

Fase

1. Inizializzare una relazione di replica:

   `snapmirror initialize -source-path hostip:/lun/name -destination-path SVM:volume|cluster://SVM/volume`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell’esempio riportato di seguito viene inizializzata la relazione tra il volume di origine `0005` All’indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Fornire i dati da un volume di destinazione DR SnapMirror

Rendere il volume di destinazione scrivibile

Quando Disaster disattiva il sito primario per una relazione di disaster recovery SnapMirror, è possibile fornire i dati dal volume di destinazione con interruzioni minime. È possibile riattivare il volume di origine quando il servizio viene ripristinato nel sito primario.

È necessario rendere il volume di destinazione scrivibile prima di poter inviare i dati dal volume ai client. È

possibile utilizzare `snapmirror quiesce` per arrestare i trasferimenti pianificati verso la destinazione, il `snapmirror abort` per interrompere i trasferimenti in corso e il `snapmirror break` per rendere la destinazione scrivibile.

A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo *`hostip:`*`/lun/`*`name`*, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Fasi

1. Interrompere i trasferimenti pianificati verso la destinazione:

   `snapmirror quiesce -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra il volume di origine `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Interrompere i trasferimenti in corso verso la destinazione:

   `snapmirror abort -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono interrompiti i trasferimenti in corso tra il volume di origine `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. Interrompere la relazione di disaster recovery di SnapMirror:

   `snapmirror break -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|`*`cluster://SVM/volume`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene spezzata la relazione tra il volume di origine `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Configurare il volume di destinazione per l'accesso ai dati

Una volta reso scrivibile il volume di destinazione, è necessario configurare il volume per l'accesso ai dati. Gli host SAN possono accedere ai dati dal volume di destinazione fino alla riattivazione del volume di origine.

1. Mappare il LUN dell'elemento al gruppo iniziatore appropriato.
2. Creare sessioni iSCSI dagli iniziatori host SAN alle LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dello storage per rilevare il LUN connesso.

Riattivare il volume di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

A proposito di questa attività

La procedura riportata di seguito presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

A partire da ONTAP 9.4, le copie Snapshot di un LUN create durante la distribuzione dei dati dalla destinazione ONTAP vengono replicate automaticamente quando l'origine dell'elemento viene riattivata.

Le regole di replica sono le seguenti:

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

Fasi

1. Eliminare la relazione di protezione dei dati originale:

   `snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -policy policy`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene eliminata la relazione tra il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Invertire la relazione di protezione dei dati originale:

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name -policy policy`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

   Nell'esempio seguente viene invertita la relazione tra il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Aggiornare la relazione inversa:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

   Nell'esempio riportato di seguito viene aggiornata la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst` acceso `svm_backup`e il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Arrestare i trasferimenti pianificati per la relazione invertita:

   `snapmirror quiesce -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente vengono interrompiti i trasferimenti pianificati tra il volume da cui si stanno fornendo i dati, `volA_dst` acceso `svm_backup`e il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Arrestare i trasferimenti in corso per la relazione invertita:

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   L'esempio seguente interrompe i trasferimenti in corso tra il volume da cui si stanno servendo i dati, `volA_dst` acceso `svm_backup`e il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Interrompere la relazione inversa:

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene spezzata la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst` acceso `svm_backup`e il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Eliminare la relazione di protezione dei dati invertita:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip`*`:/lun/`*`name`* `-policy` *`policy`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio seguente viene eliminata la relazione inversa tra il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Ristabilire la relazione di protezione dei dati originale:

   `snapmirror resync -source-path` *`hostip`*`:/lun/`*`name`* `-destination-path`

SVM:volume|cluster://SVM/volume

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene ristabilita la relazione tra il volume di origine originale, `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione originale, `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

Aggiornare manualmente una relazione di replica

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa di un errore di rete.

A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo *hostip:*/lun/*name*, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Fasi

1. Aggiornare manualmente una relazione di replica:

   snapmirror update -source-path *hostip:*/lun/*name* -destination-path *SVM:volume|cluster://SVM/volume*

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

   Nell'esempio seguente viene aggiornata la relazione tra il volume di origine `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

Risincronizzare una relazione di replica

È necessario risincronizzare una relazione di replica dopo che si rende scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione o se si desidera modificare il criterio di replica per la relazione.

A proposito di questa attività

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Fase

1. Risincronizzare i volumi di origine e di destinazione:

   `snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume |cluster://SVM/volume -type XDP -policy policy`

   Per la sintassi completa dei comandi, vedere la pagina man.

   Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `0005` All'indirizzo IP 10.0.0.11 e al volume di destinazione `volA_dst` acceso `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```