Creazione e risoluzione dei problemi delle relazioni di protezione

Active IQ Unified Manager 9.14

NetApp
March 13, 2025

Sommario

Creazione, monitoraggio e risoluzione dei problemi delle relazioni di protezione

Unified Manager consente di creare relazioni di protezione, monitorare e risolvere i problemi relativi alla protezione mirror e alla protezione del vault di backup dei dati memorizzati nei cluster gestiti e ripristinare i dati quando vengono sovrascritti o persi.

Tipi di protezione SnapMirror

In base all'implementazione della topologia dello storage dei dati, Unified Manager consente di configurare diversi tipi di relazioni di protezione di SnapMirror. Tutte le varianti della protezione di SnapMirror offrono una protezione di disaster recovery con failover, ma offrono diverse funzionalità in termini di performance, flessibilità della versione e protezione di più copie di backup.

Relazioni di protezione asincrona SnapMirror tradizionali

La protezione asincrona SnapMirror tradizionale offre la protezione del mirror di replica a blocchi tra i volumi di origine e di destinazione.

Nelle relazioni tradizionali di SnapMirror, le operazioni di mirroring vengono eseguite più velocemente rispetto alle relazioni alternative di SnapMirror, in quanto l'operazione di mirroring si basa sulla replica a blocchi. Tuttavia, la protezione SnapMirror tradizionale richiede che il volume di destinazione venga eseguito con la stessa versione minore o successiva del software ONTAP del volume di origine all'interno della stessa release principale (ad esempio, dalla versione 8.x alla 8.x o dalla 9.x alla 9.x). La replica da un'origine 9.1 a una destinazione 9.0 non è supportata perché la destinazione esegue una versione principale precedente.

Protezione asincrona di SnapMirror con replica flessibile della versione

La protezione asincrona di SnapMirror con replica flessibile della versione offre la protezione del mirror della replica logica tra i volumi di origine e di destinazione, anche se tali volumi vengono eseguiti con versioni diverse di ONTAP 8.3 o software successivo (ad esempio, dalla versione 8.3 alla 8.3.1, dalla 8.3 alla 9.1 o dalla 9.2.2 alla 9.2).

Nelle relazioni di SnapMirror con la replica flessibile della versione, le operazioni di mirroring non vengono eseguite con la stessa velocità delle relazioni di SnapMirror tradizionali.

A causa di un'esecuzione più lenta, SnapMirror con protezione della replica flessibile dalla versione non è adatto per l'implementazione in una delle seguenti circostanze:

- L'oggetto di origine contiene più di 10 milioni di file da proteggere.
- L'obiettivo del punto di ripristino per i dati protetti è di due ore o meno. (Ovvero, la destinazione deve sempre contenere dati ripristinabili mirrorati che non siano più di due ore precedenti rispetto ai dati di origine).

In entrambe le circostanze elencate, è richiesta l'esecuzione più rapida basata sulla replica di blocchi della protezione SnapMirror predefinita.

Protezione asincrona di SnapMirror con replica flessibile della versione e opzione di backup

La protezione asincrona di SnapMirror con replica e opzione di backup flessibili in base alla versione offre una protezione mirror tra i volumi di origine e di destinazione e la capacità di memorizzare più copie dei dati mirrorati nella destinazione.

L'amministratore dello storage può specificare quali copie Snapshot vengono duplicate dall'origine alla destinazione e può anche specificare per quanto tempo conservare tali copie nella destinazione, anche se vengono eliminate dall'origine.

Nelle relazioni di SnapMirror con l'opzione di replica e backup flessibile della versione, le operazioni di mirroring non vengono eseguite con la stessa velocità delle relazioni di SnapMirror tradizionali.

Replica unificata di SnapMirror (mirror e vault)

La replica unificata di SnapMirror consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Come con SnapMirror, la protezione unificata dei dati esegue un trasferimento di riferimento la prima volta che lo si richiama. Un trasferimento di riferimento con la policy di protezione dei dati unificata predefinita "MirrorAndVault" crea una copia Snapshot del volume di origine, quindi trasferisce tale copia e i blocchi di dati a cui fa riferimento al volume di destinazione. Come SnapVault, la protezione unificata dei dati non include copie Snapshot precedenti nella linea di base.

SnapMirror protezione sincrona con sincronizzazione rigorosa

La protezione sincrona di SnapMirror con sincronizzazione "strit" garantisce che i volumi primario e secondario siano sempre una copia reale l'uno dell'altro. Se si verifica un errore di replica quando si tenta di scrivere dati nel volume secondario, l'i/o del client nel volume primario viene interrotto.

SnapMirror protezione sincrona con sincronizzazione regolare

La protezione sincrona di SnapMirror con sincronizzazione "regular" non richiede che il volume primario e secondario siano sempre una copia reale l'uno dell'altro, garantendo così la disponibilità del volume primario. Se si verifica un errore di replica quando si tenta di scrivere i dati nel volume secondario, i volumi primario e secondario non sono sincronizzati e l'i/o del client continua sul volume primario.

Il pulsante Restore (Ripristina) e i pulsanti Relationship Operation (operazione relazione) non sono disponibili durante il monitoraggio delle relazioni di protezione sincrone dalla vista Health: All Volumes (Salute: Tutti i volumi) o dalla pagina Volume / Health Details (Dettagli volume/salute).

Sincronizzazione attiva di SnapMirror

La funzionalità di sincronizzazione attiva di SnapMirror è disponibile con ONTAP 9,8 e versioni successive ed è possibile utilizzarla per proteggere le applicazioni con le LUN, consentendo il failover delle applicazioni in modo trasparente, garantendo la business continuity in caso di emergenza.

Consente di rilevare e monitorare le relazioni sincrone SnapMirror per i gruppi di coerenza (CGS) disponibili su cluster e macchine virtuali di storage di Unified Manager. La sincronizzazione attiva di SnapMirror è supportata sui cluster AFF o su cluster ASA (All SAN Array), in cui i cluster primari e secondari possono essere AFF o ASA. La sincronizzazione attiva di SnapMirror protegge le applicazioni con LUN iSCSI o FCP.

Quando visualizzi i volumi e le LUN protetti dalla relazione di sincronizzazione attiva di SnapMirror, puoi

ottenere una vista unificata per le relazioni di protezione, i gruppi di coerenza nell'inventario dei volumi, la topologia di protezione per le relazioni del gruppo di coerenza, la visualizzazione dei dati storici per le relazioni del gruppo di coerenza fino a un anno. È inoltre possibile scaricare il report. È inoltre possibile visualizzare il riepilogo delle relazioni del gruppo di coerenza, cercare il supporto per le relazioni del gruppo di coerenza e ottenere informazioni sui volumi protetti dal gruppo di coerenza.

Nella pagina Relazioni è inoltre possibile ordinare, filtrare ed estendere la protezione degli oggetti di storage di origine e di destinazione e delle relative relazioni protette dal Consistency Group.

Per ulteriori informazioni sulla sincronizzazione attiva di SnapMirror, fare riferimento a "Documentazione di ONTAP 9 per SnapMirror Active Sync (in precedenza SM-BC)".

Impostazione delle relazioni di protezione in Unified Manager

Per utilizzare Unified Manager e OnCommand Workflow Automation per impostare le relazioni SnapMirror e SnapVault per proteggere i dati, è necessario eseguire diversi passaggi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario stabilire relazioni peer tra due cluster o due macchine virtuali di storage (SVM).
- OnCommand Workflow Automation deve essere integrato con Unified Manager:
  - "Configurare OnCommand Workflow Automation".
  - "Verifica del caching dell'origine dati di Unified Manager in Workflow Automation".

Fasi

1. A seconda del tipo di relazione di protezione che si desidera creare, eseguire una delle seguenti operazioni:
   - "Creare una relazione di protezione SnapMirror".
   - "Creare una relazione di protezione SnapVault".
2. Se si desidera creare un criterio per la relazione, a seconda del tipo di relazione che si sta creando, eseguire una delle seguenti operazioni:
   - "Creare un criterio SnapVault".
   - "Creare un criterio SnapMirror".
3. "Creare una pianificazione SnapMirror o SnapVault".

Configurazione di una connessione tra Workflow Automation e Unified Manager

È possibile configurare una connessione sicura tra OnCommand Workflow Automation (Wfa) e Unified Manager. La connessione all'automazione del flusso di lavoro consente di utilizzare funzionalità di protezione come i flussi di lavoro di configurazione di SnapMirror e SnapVault, oltre a comandi per la gestione delle relazioni di SnapMirror.

Cosa ti serve

- La versione installata di Workflow Automation deve essere 5.1 o superiore.

> Il pacchetto ""Wfa pack for Manage Clustered Data ONTAP"" è incluso in Wfa 5,1, pertanto non è necessario scaricare questo pacchetto dall'archivio per l'automazione dello storage NetApp e installarlo separatamente sul server Wfa, come richiesto in passato.
> "PACCHETTO WFA per la gestione di ONTAP"

- Per supportare le connessioni WFA e Unified Manager, è necessario disporre del nome dell'utente del database creato in Unified Manager.

  A questo utente del database deve essere stato assegnato il ruolo utente Integration Schema.

- È necessario assegnare il ruolo di amministratore o di architetto nell'automazione del flusso di lavoro.
- Per la configurazione di Workflow Automation, è necessario disporre dell'indirizzo host, del numero di porta 443, del nome utente e della password.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **automazione del flusso di lavoro**.
2. Nell'area **Database User** della pagina **Workflow Automation**, selezionare il nome e inserire la password dell'utente del database creato per supportare le connessioni di Unified Manager e Workflow Automation.
3. Nell'area **Workflow Automation Credentials** della pagina, immettere il nome host o l'indirizzo IP (IPv4 o IPv6), il nome utente e la password per la configurazione di Workflow Automation.

   È necessario utilizzare la porta del server Unified Manager (porta 443).

4. Fare clic su **Save** (Salva).
5. Se si utilizza un certificato autofirmato, fare clic su **Sì** per autorizzare il certificato di protezione.

   Viene visualizzata la pagina Workflow Automation.

6. Fare clic su **Sì** per ricaricare l'interfaccia utente Web e aggiungere le funzioni di automazione del flusso di lavoro.

Informazioni correlate

"Documentazione NetApp: OnCommand Workflow Automation (release correnti)"

Verifica del caching dell'origine dati di Unified Manager in Workflow Automation

È possibile determinare se il caching dell'origine dati di Unified Manager funziona correttamente controllando se l'acquisizione dell'origine dati ha esito positivo in Workflow Automation. È possibile farlo quando si integra l'automazione del flusso di lavoro con Unified Manager per garantire che la funzionalità di automazione del flusso di lavoro sia disponibile dopo l'integrazione.

Cosa ti serve

Per eseguire questa attività, è necessario assegnare il ruolo di amministratore o di architetto nell'automazione del flusso di lavoro.

Fasi

1. Dall'interfaccia utente di Workflow Automation, selezionare **esecuzione** > **origini dati**.
2. Fare clic con il pulsante destro del mouse sul nome dell'origine dati di Unified Manager, quindi selezionare **Acquire Now** (Acquisisci ora).
3. Verificare che l'acquisizione abbia esito positivo senza errori.

   Gli errori di acquisizione devono essere risolti affinché l'integrazione di Workflow Automation con Unified Manager abbia successo.

Cosa succede quando OnCommand Workflow Automation viene reinstallato o aggiornato

Prima di reinstallare o aggiornare OnCommand Workflow Automation, è necessario rimuovere la connessione tra OnCommand Workflow Automation e Unified Manager e assicurarsi che tutti i processi pianificati o in esecuzione in OnCommand Workflow Automation vengano interrotti.

È inoltre necessario eliminare manualmente Unified Manager da OnCommand Workflow Automation.

Dopo aver reinstallato o aggiornato OnCommand Workflow Automation, è necessario configurare nuovamente la connessione con Unified Manager.

Rimozione dell'installazione di OnCommand Workflow Automation da Unified Manager

È possibile rimuovere la configurazione di OnCommand Workflow Automation da Unified Manager quando non si desidera più utilizzare l'automazione del flusso di lavoro.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **General** > **Workflow Automation** nel menu Setup di sinistra.
2. Nella pagina **Workflow Automation**, fare clic su **Remove Setup** (Rimuovi installazione).

Esecuzione di failover e failback delle relazioni di protezione

Quando un volume di origine nella relazione di protezione viene disattivato a causa di un guasto hardware o di un disastro, è possibile utilizzare le funzionalità delle relazioni di protezione di Unified Manager per rendere la destinazione di protezione accessibile in lettura/scrittura e eseguire il failover su tale volume fino a quando l'origine non è nuovamente online; quindi, è possibile tornare all'origine originale quando è disponibile per la distribuzione dei dati.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Per eseguire questa operazione, è necessario aver configurato OnCommand Workflow Automation.

Fasi

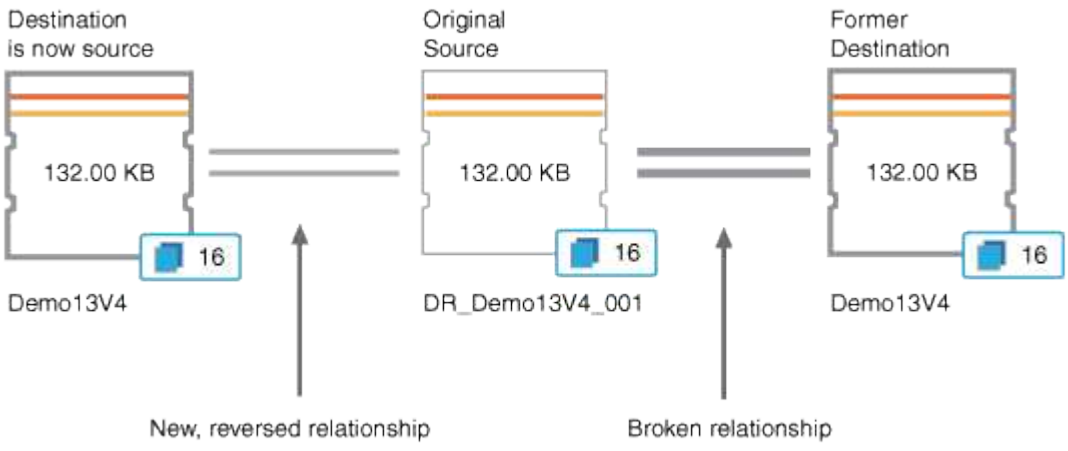
1. "Interrompere la relazione di SnapMirror".

   È necessario interrompere la relazione prima di poter convertire la destinazione da un volume di protezione dati a un volume di lettura/scrittura e prima di invertire la relazione.

2. "Invertire la relazione di protezione".

   Quando il volume di origine originale è nuovamente disponibile, è possibile decidere di ristabilire la relazione di protezione originale ripristinando il volume di origine. Prima di poter ripristinare l'origine, è necessario sincronizzarla con i dati scritti nella destinazione precedente. L'operazione di risincronizzazione inversa consente di creare una nuova relazione di protezione invertendo i ruoli della relazione originale e sincronizzando il volume di origine con la destinazione precedente. Viene creata una nuova copia Snapshot di riferimento per la nuova relazione.

   La relazione invertita appare simile a una relazione a cascata:



3. "Interrompere la relazione SnapMirror inversa".

   Quando il volume di origine originale viene risincronizzato e può nuovamente servire i dati, utilizzare l'operazione di interruzione per interrompere la relazione inversa.

4. "Rimuovere la relazione".

   Quando la relazione invertita non è più necessaria, è necessario rimuovere tale relazione prima di ristabilire la relazione originale.

5. "Risincronizzare la relazione".

   Utilizzare l'operazione di risincronizzazione per sincronizzare i dati dall'origine alla destinazione e ristabilire la relazione originale.

Interruzione di una relazione SnapMirror dalla pagina dei dettagli relativi a volume e salute

È possibile interrompere una relazione di protezione dalla pagina dei dettagli relativi a volume/salute e interrompere i trasferimenti di dati tra un volume di origine e un volume di destinazione in una relazione SnapMirror. È possibile interrompere una relazione quando si desidera migrare i dati, per il disaster recovery o per il test delle applicazioni. Il volume di destinazione viene modificato in un volume di lettura/scrittura. Non è possibile interrompere una relazione SnapVault.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, selezionare dalla topologia la relazione SnapMirror che si desidera interrompere.
2. Fare clic con il pulsante destro del mouse sulla destinazione e selezionare **Interrompi** dal menu.

   Viene visualizzata la finestra di dialogo Interrompi relazione.
3. Fare clic su **continua** per interrompere la relazione.
4. Nella topologia, verificare che la relazione sia interrotta.

Invertire le relazioni di protezione dalla pagina dei dettagli relativi a volume/salute

Quando un disastro disattiva il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per fornire i dati convertendolo in lettura/scrittura durante la riparazione o la sostituzione dell'origine. Quando l'origine è nuovamente disponibile per ricevere i dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sull'origine con i dati sulla destinazione di lettura/scrittura.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault.
- Una relazione di protezione deve già esistere.
- Il rapporto di protezione deve essere interrotto.
- Sia l'origine che la destinazione devono essere in linea.
- L'origine non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando si esegue questa attività, i dati sull'origine più recenti dei dati sulla copia Snapshot comune vengono cancellati.
- Le policy e le pianificazioni create sulla relazione di risincronizzazione inversa sono le stesse della

relazione di protezione originale.

Se le policy e le pianificazioni non esistono, vengono create.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione SnapMirror su cui si desidera invertire l'origine e la destinazione, quindi fare clic con il pulsante destro del mouse.
2. Selezionare **Reverse Resync** (risincronizzazione inversa) dal menu.

   Viene visualizzata la finestra di dialogo Reverse Resync (risincronizzazione inversa).

3. Verificare che la relazione visualizzata nella finestra di dialogo **Reverse Resync** sia quella per cui si desidera eseguire l'operazione di risincronizzazione inversa, quindi fare clic su **Submit** (Invia).

   La finestra di dialogo Reverse Resync (risincronizzazione inversa) viene chiusa e viene visualizzato un collegamento al processo nella parte superiore della pagina dei dettagli relativi a volume/salute.

4. **Opzionale:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume / Health** per tenere traccia dello stato di ciascun processo di risincronizzazione inversa.

   Viene visualizzato un elenco filtrato di lavori.

5. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Health**.

   L'operazione di risincronizzazione inversa è terminata quando tutte le attività del lavoro sono state completate correttamente.

Rimozione di una relazione di protezione dalla pagina Dettagli volume/salute

È possibile rimuovere una relazione di protezione per eliminare in modo permanente una relazione esistente tra l'origine e la destinazione selezionate, ad esempio quando si desidera creare una relazione utilizzando una destinazione diversa. Questa operazione rimuove tutti i metadati e non può essere annullata.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, selezionare dalla topologia la relazione SnapMirror che si desidera rimuovere.
2. Fare clic con il pulsante destro del mouse sul nome della destinazione e selezionare **Remove** (Rimuovi) dal menu.

   Viene visualizzata la finestra di dialogo Rimuovi relazione.

3. Fare clic su **continua** per rimuovere la relazione.

   La relazione viene rimossa dalla pagina Volume / Health Details (Dettagli volume/salute).

Risincronizzazione delle relazioni di protezione dalla pagina dei dettagli relativi a volume/salute

È possibile risincronizzare i dati su una relazione SnapMirror o SnapVault che è stata interrotta e quindi la destinazione è stata fatta in lettura/scrittura in modo che i dati sull'origine corrispondano ai dati sulla destinazione. È inoltre possibile risincronizzare quando viene eliminata una copia Snapshot comune richiesta sul volume di origine, causando il mancato aggiornamento di SnapMirror o SnapVault.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato OnCommand Workflow Automation.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione di protezione che si desidera risincronizzare e fare clic con il pulsante destro del mouse su di essa.
2. Selezionare **Risincronizza** dal menu.

   In alternativa, dal menu **azioni**, selezionare **relazione** > **risincronizza** per risincronizzare la relazione per la quale si stanno visualizzando i dettagli.

   Viene visualizzata la finestra di dialogo risincronizza.
3. Nella scheda **Opzioni di risincronizzazione**, selezionare una priorità di trasferimento e la velocità di trasferimento massima.
4. Fare clic su **Source Snapshot Copies**, quindi nella colonna **Snapshot Copy**, fare clic su **Default**.

   Viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).
5. Se si desidera specificare una copia Snapshot esistente invece di trasferire la copia Snapshot predefinita, fare clic su **Existing Snapshot Copy** (Copia istantanea esistente) e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

   Viene visualizzata nuovamente la finestra di dialogo risincronizza.
7. Se sono state selezionate più origini da risincronizzare, fare clic su **Default** per l'origine successiva per la quale si desidera specificare una copia Snapshot esistente.
8. Fare clic su **Submit** (Invia) per avviare il processo di risincronizzazione.

   Viene avviato il processo di risincronizzazione, viene visualizzata la pagina dei dettagli relativi al volume/salute e viene visualizzato un collegamento ai processi nella parte superiore della pagina.
9. **Opzionale:** fare clic su **Visualizza processi** nella pagina **Dettagli volume/salute** per tenere traccia dello stato di ciascun processo di risincronizzazione.

   Viene visualizzato un elenco filtrato di lavori.
10. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Health**.

Il processo di risincronizzazione è terminato al termine di tutte le attività del processo.

Risoluzione di un errore di un lavoro di protezione

Questo flusso di lavoro fornisce un esempio di come è possibile identificare e risolvere un errore di un processo di protezione dalla dashboard di Unified Manager.

Cosa ti serve

Poiché alcune attività di questo flusso di lavoro richiedono l'accesso mediante il ruolo di amministratore, è necessario conoscere i ruoli richiesti per utilizzare le varie funzionalità.

In questo scenario, puoi accedere alla pagina Dashboard per verificare se ci sono problemi con i tuoi processi di protezione. Nell'area incidente di protezione, si noterà la presenza di un incidente con interruzione del processo, che mostra un errore di errore relativo al processo di protezione non riuscito su un volume. Esaminare questo errore per determinare la possibile causa e la potenziale risoluzione.

Fasi

1. Nel pannello incidenti di protezione dell'area incidenti e rischi non risolti della dashboard, fare clic sull'evento **errore del processo di protezione**.

   Il testo collegato per l'evento è scritto nel modulo `object_name:/object_name - Error Name`, ad esempio `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed.`

   Viene visualizzata la pagina Dettagli evento relativa al processo di protezione non riuscito.

2. Esaminare il messaggio di errore nel campo cause dell'area **Summary** per determinare il problema e valutare le potenziali azioni correttive.

   Vedere "Identificazione del problema ed esecuzione di azioni correttive per un lavoro di protezione non riuscito".

Identificazione del problema ed esecuzione di azioni correttive per un lavoro di protezione non riuscito

Esaminare il messaggio di errore del lavoro nel campo cause della pagina Dettagli evento e determinare che il lavoro non è riuscito a causa di un errore di copia Snapshot. Quindi, accedere alla pagina dei dettagli relativi a volume/salute per ottenere ulteriori informazioni.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Il messaggio di errore fornito nel campo causa della pagina Dettagli evento contiene il seguente testo relativo al processo non riuscito:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Questo messaggio fornisce le seguenti informazioni:

- Un processo di backup o mirroring non è stato completato correttamente.

  Il processo prevedeva una relazione di protezione tra il volume di origine `cluster2_src_vol2` sul server virtuale `cluster2_src_svm` e il volume di destinazione `managed_svc2_vol3` sul server virtuale denominato `cluster3_dst_svm`.

- Un processo di copia istantanea non è riuscito per `0426cluster2_src_vol2snap` sul volume di origine `cluster2_src_svm:/cluster2_src_vol2` .

In questo scenario, è possibile identificare la causa e le potenziali azioni correttive dell'errore del processo. Tuttavia, la risoluzione del problema richiede l'accesso all'interfaccia utente Web di Gestione sistema o ai comandi dell'interfaccia utente di ONTAP.

Fasi

1. Il messaggio di errore viene esaminato e si determina che un lavoro di copia Snapshot non è riuscito sul volume di origine, indicando che probabilmente si è verificato un problema con il volume di origine.

   In alternativa, è possibile fare clic sul collegamento **Dettagli lavoro** alla fine del messaggio di errore, ma per gli scopi di questo scenario si sceglie di non farlo.

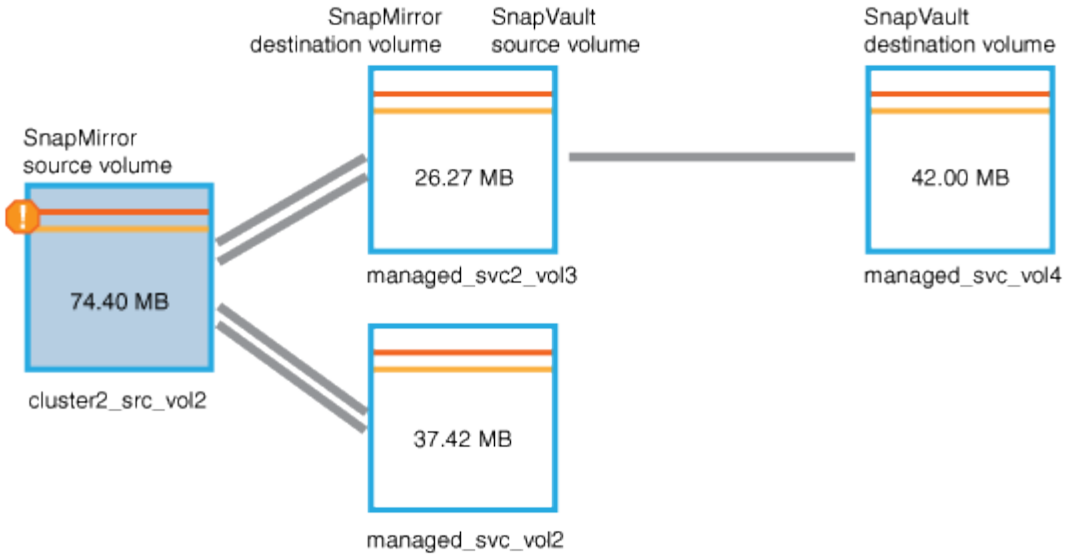
2. Si decide di tentare di risolvere l'evento, quindi eseguire le seguenti operazioni:
   a. Fare clic sul pulsante **Assegna a** e selezionare **Me** dal menu.
   b. Fare clic sul pulsante **Acknowledge** (Conferma) per non continuare a ricevere notifiche di avviso ripetute, se sono stati impostati avvisi per l'evento.
   c. In alternativa, è possibile aggiungere note sull'evento.
3. Fare clic sul campo **Source** (origine) nel riquadro **Summary** (Riepilogo) per visualizzare i dettagli sul volume di origine.

   Il campo **origine** contiene il nome dell'oggetto di origine: In questo caso, il volume su cui è stato pianificato il lavoro di copia Snapshot.

   Viene visualizzata la pagina Dettagli volume / stato per `cluster2_src_vol2`, che mostra il contenuto della scheda protezione.

4. Osservando il grafico della topologia di protezione, viene visualizzata un'icona di errore associata al primo volume della topologia, ovvero il volume di origine per la relazione SnapMirror.

   Vengono inoltre visualizzate le barre orizzontali nell'icona del volume di origine, che indicano le soglie di avviso e di errore impostate per tale volume.



5. Posizionare il cursore sull'icona di errore per visualizzare la finestra di dialogo a comparsa che visualizza le impostazioni di soglia e verificare che il volume abbia superato la soglia di errore, indicando un problema di capacità.
6. Fare clic sulla scheda **Capacity**.

   Vengono visualizzate le informazioni sulla capacità relative al volume `cluster2_src_vol2`.

7. Nel pannello **Capacity**, viene visualizzata un'icona di errore nel grafico a barre, che indica ancora una volta che la capacità del volume ha superato il livello di soglia impostato per il volume.
8. Sotto il grafico della capacità, si vede che la crescita automatica del volume è stata disattivata e che è stata impostata una garanzia di spazio del volume.

   Si potrebbe decidere di attivare la crescita automatica, ma ai fini di questo scenario, si decide di approfondire la ricerca prima di prendere una decisione su come risolvere il problema di capacità.

9. Scorrere verso il basso fino all'elenco **Eventi** e verificare che siano stati generati gli eventi Protection Job Failed (processo di protezione non riuscito), Volume Days until Full (giorni volume fino al pieno) e Volume Space Full (spazio volume pieno).
10. Nell'elenco **Eventi**, fare clic sull'evento **Volume Space Full** per ottenere ulteriori informazioni, avendo deciso che questo evento sembra più rilevante per il problema di capacità.

    La pagina Dettagli evento visualizza l'evento Volume Space Full per il volume di origine.

11. Nell'area **Riepilogo**, si legge il campo causa dell'evento: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Sotto l'area Summary (Riepilogo), vengono visualizzate le azioni correttive suggerite.

    Le azioni correttive suggerite vengono visualizzate solo per alcuni eventi, pertanto questa area non viene visualizzata per tutti i tipi di eventi.

    Fare clic nell'elenco delle azioni consigliate che è possibile eseguire per risolvere l'evento Volume Space Full (spazio volume pieno):

    - Abilitare la crescita automatica su questo volume.

- Ridimensionare il volume.
- Abilitare ed eseguire la deduplica su questo volume.
- Attivare ed eseguire la compressione su questo volume.

13. Si decide di attivare la crescita automatica sul volume, ma per farlo, è necessario determinare lo spazio libero disponibile sull'aggregato di origine e il tasso di crescita del volume corrente:
    a. Esaminare l'aggregato principale, `cluster2_src_aggr1`, nel riquadro **periferiche correlate**.

       È possibile fare clic sul nome dell'aggregato per ottenere ulteriori dettagli sull'aggregato.

       Si determina che l'aggregato dispone di spazio sufficiente per abilitare la crescita automatica del volume.

    b. Nella parte superiore della pagina, osservare l'icona che indica un incidente critico e consultare il testo sotto l'icona.

       Si determina che "giorni a pieno: Meno di un giorno | tasso di crescita giornaliero: 5.4%".

14. Accedere a System Manager o all'interfaccia della riga di comando di ONTAP per abilitare questa `volume autogrow` opzione.

    Prendere nota dei nomi del volume e dell'aggregato in modo che siano disponibili quando si attiva la crescita automatica.

15. Dopo aver risolto il problema di capacità, tornare alla pagina dei dettagli di Unified Manager **Event** e contrassegnare l'evento come risolto.

Risoluzione dei problemi di ritardo

Questo flusso di lavoro fornisce un esempio di come è possibile risolvere un problema di ritardo. In questo scenario, sei un amministratore o un operatore che accede alla pagina Unified ManagerDashboard per vedere se ci sono problemi con le tue relazioni di protezione e, se esistono, per trovare soluzioni.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Nella pagina Dashboard, viene visualizzata l'area Incidents and Risks non risolti e viene visualizzato un errore di SnapMirror Lag nel pannello Protection (protezione) sotto Protection Risks (rischi di protezione).

Fasi

1. Nel riquadro **Protection** della pagina **Dashboard**, individuare l'errore di ritardo della relazione SnapMirror e fare clic su di esso.

   Viene visualizzata la pagina dei dettagli dell'evento relativo all'errore di ritardo.

2. Dalla pagina dei dettagli **evento** è possibile eseguire una o più delle seguenti attività:
   - Esaminare il messaggio di errore nel campo cause dell'area Summary (Riepilogo) per determinare se sono presenti azioni correttive suggerite.

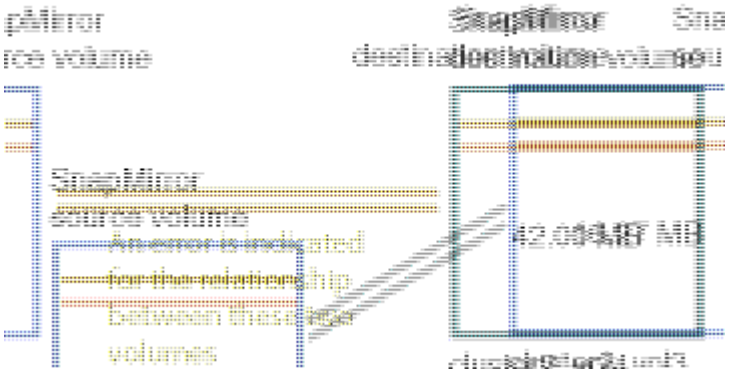
- Fare clic sul nome dell'oggetto, in questo caso un volume, nel campo Source (origine) dell'area Summary (Riepilogo) per visualizzare i dettagli sul volume.
- Cercare le note che potrebbero essere state aggiunte a questo evento.
- Aggiungere una nota all'evento.
- Assegnare l'evento a un utente specifico.
- Riconoscere o risolvere l'evento.

3. In questo scenario, fare clic sul nome dell'oggetto (in questo caso, un volume) nel campo Source (origine) dell'area **Summary** (Riepilogo) per ottenere i dettagli sul volume.

   Viene visualizzata la scheda Protection (protezione) della pagina Volume / Health details (Dettagli volume/salute).

4. Nella scheda **protezione**, viene illustrato il diagramma della topologia.

   Si noti che il volume con l'errore di ritardo è l'ultimo volume in una cascata SnapMirror a tre volumi. Il volume selezionato viene evidenziato in grigio scuro e una doppia linea arancione dal volume di origine indica un errore di relazione di SnapMirror.



5. Fare clic su ciascuno dei volumi nella cascata di SnapMirror.

   Quando si seleziona ciascun volume, le informazioni di protezione in Riepilogo, topologia, Cronologia, Eventi, dispositivi correlati, E le aree degli avvisi correlati vengono modificate per visualizzare i dettagli relativi al volume selezionato.

6. Esaminare l'area **Summary** e posizionare il cursore sull'icona delle informazioni nel campo **Update Schedule** per ciascun volume.

   In questo scenario, si nota che il criterio SnapMirror è DPDefault e la pianificazione di SnapMirror viene aggiornata ogni ora cinque minuti dopo l'ora. Ti renderai conto che tutti i volumi della relazione stanno tentando di completare un trasferimento SnapMirror contemporaneamente.

7. Per risolvere il problema del ritardo, modificare le pianificazioni per due dei volumi a cascata in modo che ciascuna destinazione inizi un trasferimento SnapMirror dopo che l'origine ha completato un trasferimento.