Creare e risolvere i problemi delle relazioni di protezione

Active IQ Unified Manager

NetApp
October 15, 2025

Sommario

Creare, monitorare e risolvere i problemi delle relazioni di protezione

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

Tipi di protezione SnapMirror

A seconda dell'implementazione della topologia di archiviazione dati, Unified Manager consente di configurare più tipi di relazioni di protezione SnapMirror . Tutte le varianti di protezione SnapMirror offrono protezione di disaster recovery in caso di failover, ma offrono funzionalità diverse in termini di prestazioni, flessibilità delle versioni e protezione da più copie di backup.

Relazioni di protezione asincrone tradizionali SnapMirror

La protezione asincrona SnapMirror tradizionale fornisce protezione mirror di replicazione a blocchi tra i volumi di origine e di destinazione.

Nelle relazioni SnapMirror tradizionali, le operazioni di mirroring vengono eseguite più velocemente rispetto alle relazioni SnapMirror alternative, perché l'operazione di mirroring si basa sulla replicazione a blocchi. Tuttavia, la protezione SnapMirror tradizionale richiede che il volume di destinazione venga eseguito con la stessa versione secondaria del software ONTAP o con una successiva del volume di origine all'interno della stessa versione 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 SnapMirror con replica flessibile in base alla versione

La protezione asincrona SnapMirror con replica flessibile in base alla versione fornisce una protezione mirror di replica logica tra volumi di origine e di destinazione, anche se tali volumi sono in esecuzione con versioni diverse del software ONTAP 8.3 o successive (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 SnapMirror con replica flessibile in base alla versione, le operazioni di mirroring non vengono eseguite con la stessa rapidità delle relazioni SnapMirror tradizionali.

A causa dell'esecuzione più lenta, SnapMirror con protezione della replica flessibile in base alla versione non è adatto all'implementazione in nessuna delle seguenti circostanze:

- L'oggetto sorgente 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. (Ciò significa che la destinazione deve sempre contenere dati speculari e recuperabili che non siano più vecchi di due ore rispetto ai dati presenti nella sorgente.)

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

Protezione asincrona SnapMirror con replica flessibile in base alla versione e opzione di backup

La protezione asincrona SnapMirror con opzione di replica e backup flessibile in base alla versione fornisce protezione mirror tra volumi di origine e di destinazione e la possibilità di archiviare più copie dei dati mirror nella destinazione.

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

Nelle relazioni SnapMirror con opzione di replica e backup flessibile in base alla versione, le operazioni di mirroring non vengono eseguite con la stessa rapidità delle relazioni SnapMirror tradizionali.

SnapMirror Unified Replication (mirror e vault)

La replica unificata SnapMirror consente di configurare il ripristino di emergenza e l'archiviazione sullo stesso volume di destinazione. Come con SnapMirror, la protezione dati unificata esegue un trasferimento di base la prima volta che la si richiama. Un trasferimento di base in base alla policy di protezione 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 dati unificata non include le copie Snapshot più vecchie nella baseline.

Protezione sincrona SnapMirror con sincronizzazione rigorosa

La protezione sincrona SnapMirror con sincronizzazione "strict" garantisce che i volumi primario e secondario siano sempre una copia fedele l'uno dell'altro. Se si verifica un errore di replica durante il tentativo di scrivere dati sul volume secondario, l'I/O del client sul volume primario viene interrotto.

Protezione sincrona SnapMirror con sincronizzazione regolare

La protezione sincrona SnapMirror con sincronizzazione "regolare" non richiede che il volume primario e quello secondario siano sempre una copia fedele l'uno dell'altro, garantendo così la disponibilità del volume primario. Se si verifica un errore di replica durante il tentativo di scrivere dati sul volume secondario, i volumi primario e secondario perdono la sincronizzazione e l'I/O del client continuerà sul volume primario.

> Il pulsante Ripristina e i pulsanti Operazione relazione non sono disponibili quando si monitorano le relazioni di protezione sincrona dalla vista Integrità: tutti i volumi o dalla pagina Dettagli volume/integrità.

Sincronizzazione attiva SnapMirror

La funzionalità di sincronizzazione attiva SnapMirror è disponibile con ONTAP 9.8 e versioni successive e può essere utilizzata per proteggere le applicazioni con LUN, consentendo alle applicazioni di eseguire il failover in modo trasparente, garantendo la continuità aziendale in caso di disastro.

Consente di scoprire e monitorare le relazioni SnapMirror sincrone per i gruppi di coerenza (CG) disponibili su cluster e macchine virtuali di archiviazione da Unified Manager. SnapMirror ActiveSync è supportato su cluster AFF o cluster All SAN Array (ASA), in cui i cluster primario e secondario possono essere AFF o ASA. SnapMirror ActiveSync protegge le applicazioni con LUN iSCSI o FCP.

Quando si visualizzano i volumi e i LUN protetti dalla relazione di sincronizzazione attiva SnapMirror , è possibile ottenere una vista unificata per le relazioni di protezione, i gruppi di coerenza nell'inventario dei

volumi, visualizzare la topologia di protezione per le relazioni dei gruppi di coerenza e visualizzare i dati storici per le relazioni dei gruppi di coerenza fino a un anno. È anche possibile scaricare il rapporto. È inoltre possibile visualizzare il riepilogo delle relazioni del Consistency Group, cercare supporto per le relazioni del Consistency Group e ottenere informazioni sui volumi protetti dal Consistency Group.

Nella pagina Relazioni è inoltre possibile ordinare, filtrare ed estendere la protezione sugli oggetti di archiviazione di origine e di destinazione e sulle relative relazioni protette dal Gruppo di coerenza.

Per saperne di più sulla sincronizzazione attiva SnapMirror , fare riferimento a"Documentazione ONTAP 9 per Snapmirror ActiveSync (precedentemente SM-BC)" .

Impostare le relazioni di protezione in Unified Manager

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

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver stabilito relazioni peer tra due cluster o due macchine virtuali di archiviazione (SVM).
- OnCommand Workflow Automation deve essere integrato con Unified Manager:
  - "Configurare OnCommand Workflow Automation".
  - "Verifica della memorizzazione nella cache della fonte dati di Unified Manager in Workflow Automation".

Passi

1. A seconda del tipo di rapporto di protezione che si desidera creare, procedere in uno dei seguenti modi:
   - "Crea una relazione di protezione SnapMirror".
   - "Crea una relazione di protezione SnapVault".
2. Se si desidera creare una policy per la relazione, a seconda del tipo di relazione che si sta creando, procedere in uno dei seguenti modi:
   - "Crea una policy SnapVault".
   - "Crea una policy SnapMirror".
3. "Crea una pianificazione SnapMirror o SnapVault".

Configurare una connessione tra Workflow Automation e Unified Manager

È possibile configurare una connessione sicura tra OnCommand Workflow Automation (WFA) e Unified Manager. La connessione a Workflow Automation consente di utilizzare funzionalità di protezione quali i flussi di lavoro di configurazione di SnapMirror e SnapVault , nonché comandi per la gestione delle relazioni SnapMirror .

Prima di iniziare

- La versione installata di Workflow Automation deve essere 5.1.1P6 o successiva.

Il "pacchetto WFA per la gestione di Clustered Data ONTAP" è incluso in WFA 5.1.1P6, quindi non è necessario scaricare questo pacchetto da NetAppStorage Automation Store e installarlo separatamente sul server WFA, come era necessario in passato. "Pacchetto WFA per la gestione 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 di utente Schema di integrazione.

- È necessario che ti venga assegnato il ruolo di Amministratore o di Architetto in Workflow Automation.
- 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 Amministratore dell'archiviazione.

Passi

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

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

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

   Viene visualizzata la pagina Automazione del flusso di lavoro.

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

Informazioni correlate

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

Verificare la memorizzazione nella cache della fonte dati di Unified Manager in Workflow Automation

È possibile determinare se la memorizzazione nella cache dell'origine dati di Unified Manager funziona correttamente verificando se l'acquisizione dell'origine dati è riuscita in Workflow Automation. È possibile farlo quando si integra Workflow Automation con Unified Manager per garantire che la funzionalità Workflow Automation sia disponibile dopo l'integrazione.

Prima di iniziare

Per eseguire questa attività, è necessario disporre del ruolo di Amministratore o di Architetto in Workflow Automation.

Passi

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

   Per garantire la corretta integrazione di Workflow Automation con Unified Manager, è necessario risolvere gli errori di acquisizione.

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 OnCommand Workflow Automation attualmente in esecuzione o pianificati siano arrestati.

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.

Rimuovere la configurazione 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 Workflow Automation.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Automazione del flusso di lavoro** nel menu Impostazioni a sinistra.
2. Nella pagina **Automazione del flusso di lavoro**, fare clic su **Rimuovi configurazione**.

Eseguire un failover e un failback della relazione di protezione

Quando un volume di origine nella relazione di protezione viene disabilitato a causa di un guasto hardware o di un disastro, è possibile utilizzare le funzionalità della relazione di protezione in Unified Manager per rendere la destinazione di protezione accessibile in lettura/scrittura ed eseguire il failover su tale volume finché l'origine non torna online; a quel punto, è possibile eseguire il failover sull'origine originale quando è disponibile per fornire dati.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- Per eseguire questa operazione è necessario aver configurato OnCommand Workflow Automation .

Passi

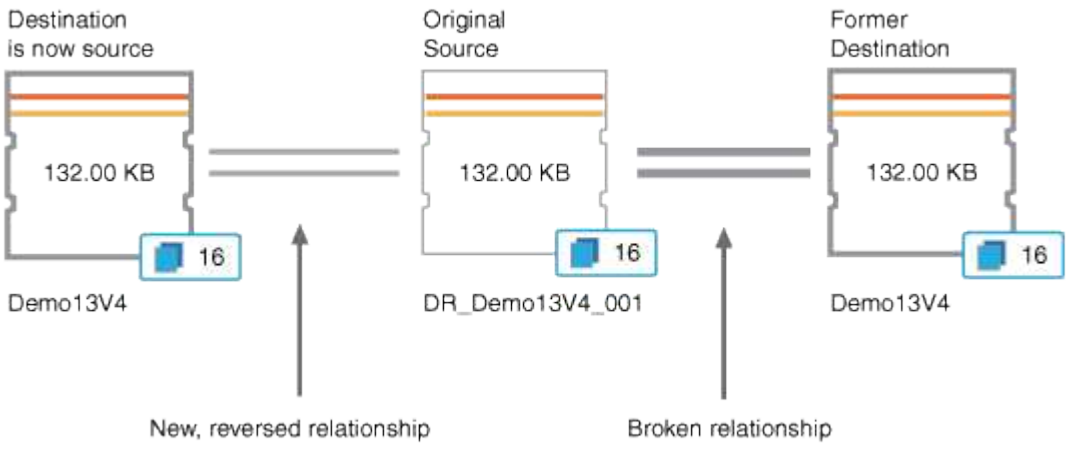
1. "Interrompere la relazione SnapMirror".

   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 poter invertire la relazione.

2. "Invertire il rapporto di protezione".

   Quando il volume sorgente originale sarà nuovamente disponibile, potresti decidere di ristabilire la relazione di protezione originale ripristinando il volume sorgente. Prima di poter ripristinare la sorgente, è necessario sincronizzarla con i dati scritti nella destinazione precedente. Utilizzare l'operazione di risincronizzazione inversa per 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 base per la nuova relazione.

   La relazione invertita è simile a una relazione a cascata:



3. "Interrompere la relazione SnapMirror invertita".

   Quando il volume sorgente originale viene risincronizzato e può nuovamente gestire i dati, utilizzare l'operazione di interruzione per interrompere la relazione invertita.

4. "Rimuovi la relazione".

   Quando la relazione invertita non è più necessaria, è necessario rimuoverla 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.

Interrompere una relazione SnapMirror dalla pagina dei dettagli Volume/Stato

È possibile interrompere una relazione di protezione dalla pagina dei dettagli Volume/Stato e interrompere i trasferimenti di dati tra un volume di origine e uno di

destinazione in una relazione SnapMirror . È possibile interrompere una relazione quando si desidera migrare dati, per il ripristino di emergenza o per testare un'applicazione. Il volume di destinazione viene modificato in un volume di lettura-scrittura. Non è possibile interrompere una relazione SnapVault .

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, seleziona dalla topologia la relazione SnapMirror che desideri 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.

Relazioni di protezione inversa dalla pagina dei dettagli Volume/Salute

Quando un disastro disabilita il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per gestire i dati convertendoli in lettura/scrittura mentre si ripara o si sostituisce l'origine. Quando la sorgente è nuovamente disponibile per ricevere dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sulla sorgente con i dati sulla destinazione di lettura/scrittura.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault .
- Deve già esistere un rapporto di protezione.
- Il rapporto di protezione deve essere interrotto.
- Sia la sorgente che la destinazione devono essere online.
- La sorgente non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando si esegue questa attività, i dati sulla fonte più recenti rispetto ai dati sulla copia Snapshot comune vengono eliminati.
- Le policy e le pianificazioni create sulla relazione di risincronizzazione inversa sono le stesse di quelle sulla relazione di protezione originale.

  Se non esistono policy e pianificazioni, vengono create.

Passi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, individuare nella topologia la relazione SnapMirror su cui si desidera invertire l'origine e la destinazione e fare clic con il pulsante destro

del mouse.

2. Selezionare **Risincronizzazione inversa** dal menu.

   Viene visualizzata la finestra di dialogo Risincronizzazione inversa.

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

   La finestra di dialogo Risincronizzazione inversa viene chiusa e nella parte superiore della pagina Dettagli volume/integrità viene visualizzato un collegamento al processo.

4. **Facoltativo:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume/Stato** per monitorare lo stato di ciascun processo di risincronizzazione inversa.

   Viene visualizzato un elenco filtrato di lavori.

5. **Facoltativo:** fai clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Salute**.

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

Rimuovere una relazione di protezione dalla pagina dei dettagli Volume/Salute

È possibile rimuovere una relazione di protezione per eliminare definitivamente 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.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato l'automazione del flusso di lavoro.

Passi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, seleziona dalla topologia la relazione SnapMirror che desideri rimuovere.
2. Fare clic con il pulsante destro del mouse sul nome della destinazione e selezionare **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 dei dettagli Volume/Salute.

Risincronizzare le relazioni di protezione dalla pagina dei dettagli Volume/Stato

È possibile risincronizzare i dati su una relazione SnapMirror o SnapVault che è stata interrotta e in seguito la destinazione è stata resa di lettura/scrittura in modo che i dati sull'origine corrispondano ai dati sulla destinazione. È anche possibile risincronizzare quando una copia Snapshot comune richiesta sul volume di origine viene eliminata, causando il fallimento degli aggiornamenti di SnapMirror o SnapVault .

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario aver configurato OnCommand Workflow Automation.

Passi

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

   In alternativa, dal menu **Azioni**, seleziona **Relazione** > **Risincronizza** per risincronizzare la relazione di cui stai 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 **Copie snapshot di origine**; quindi, nella colonna **Copia snapshot**, fare clic su **Predefinito**.

   Viene visualizzata la finestra di dialogo Seleziona copia snapshot di origine.

5. Se si desidera specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fare clic su **Copia Snapshot esistente** e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

   Verrà visualizzata nuovamente la finestra di dialogo Risincronizza.

7. Se hai selezionato più di una sorgente da risincronizzare, fai clic su **Predefinito** per la sorgente successiva per la quale desideri specificare una copia Snapshot esistente.
8. Fare clic su **Invia** per avviare il processo di risincronizzazione.

   Il processo di risincronizzazione viene avviato, si torna alla pagina dei dettagli Volume/Stato e nella parte superiore della pagina viene visualizzato un collegamento ai processi.

9. **Facoltativo:** fare clic su **Visualizza processi** nella pagina **Dettagli volume/stato** per monitorare lo stato di ciascun processo di risincronizzazione.

   Viene visualizzato un elenco filtrato di lavori.

10. **Facoltativo:** fai clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Salute**.

    Il processo di risincronizzazione è terminato quando tutte le attività vengono completate correttamente.

Risolvere un errore del processo 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.

Prima di iniziare

Poiché alcune attività in questo flusso di lavoro richiedono l'accesso tramite il ruolo di Amministratore, è necessario avere familiarità con i ruoli richiesti per utilizzare varie funzionalità.

In questo scenario, accedi alla pagina Dashboard per verificare se ci sono problemi con i tuoi processi di protezione. Nell'area Incidente di protezione, si nota la presenza di un incidente Job terminato, che mostra un errore di errore di Job di protezione non riuscito su un volume. Esamina questo errore per determinarne la possibile causa e la possibile soluzione.

Passi

1. Nel pannello Incidenti di protezione dell'area Incidenti e rischi irrisolti della dashboard, fare clic sull'evento **Processo di protezione non riuscito**.

   Il testo collegato all'evento è scritto nella forma `object_name:/object_name - Error Name` , ad esempio `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed` .

   Viene visualizzata la pagina dei dettagli dell'evento per il processo di protezione non riuscito.

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

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

Identificare il problema ed eseguire azioni correttive per un lavoro di protezione non riuscito

Si esamina il messaggio di errore di errore del processo nel campo Causa nella pagina Dettagli evento e si determina che il processo non è riuscito a causa di un errore di copia snapshot. Si passa quindi alla pagina dei dettagli Volume/Salute per raccogliere maggiori informazioni.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Il messaggio di errore fornito nel campo Causa nella 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 lavoro prevedeva una relazione di protezione tra il volume sorgente `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 snapshot non è riuscito per `0426cluster2_src_vol2snap` sul volume sorgente `cluster2_src_svm:/cluster2_src_vol2` .

In questo scenario è possibile identificare la causa e le potenziali azioni correttive dell'errore del processo. Tuttavia, per risolvere l'errore è necessario accedere all'interfaccia utente Web di System Manager o ai comandi ONTAP CLI.

Passi

1. Si esamina il messaggio di errore e si determina che un processo di copia snapshot non è riuscito sul volume di origine, il che indica che probabilmente c'è un problema con il volume di origine.

   Facoltativamente, potresti cliccare sul link **Dettagli lavoro** alla fine del messaggio di errore, ma ai fini di questo scenario, scegli di non farlo.

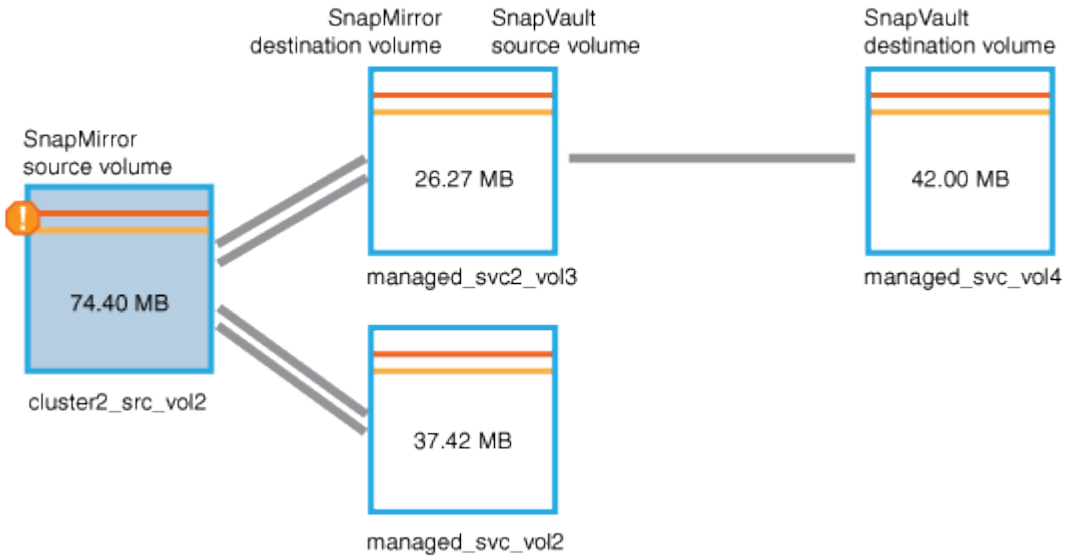
2. Decidi di provare a risolvere l'evento, quindi procedi come segue:
   a. Fare clic sul pulsante **Assegna a** e selezionare **Io** dal menu.
   b. Fare clic sul pulsante **Riconosci** per non continuare a ricevere notifiche di avviso ripetute, se sono stati impostati avvisi per l'evento.
   c. Facoltativamente, puoi anche aggiungere delle note sull'evento.
3. Fare clic sul campo **Origine** nel riquadro **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 processo di copia Snapshot.

   La pagina dei dettagli Volume/Salute viene visualizzata per `cluster2_src_vol2` , che mostra il contenuto della scheda Protezione.

4. Osservando il grafico della topologia di protezione, si nota un'icona di errore associata al primo volume nella topologia, che è il volume di origine per la relazione SnapMirror .

   Sono visibili anche le barre orizzontali nell'icona del volume sorgente, che indicano le soglie di avviso e di errore impostate per quel volume.



5. Posizionando il cursore sull'icona di errore si apre la finestra di dialogo pop-up che mostra le impostazioni della soglia e si nota che il volume ha superato la soglia di errore, il che indica un problema di capacità.
6. Fare clic sulla scheda **Capacità**.

   Informazioni sulla capacità del volume `cluster2_src_vol2` schermi.

7. Nel pannello **Capacità**, puoi vedere 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, puoi vedere che l'aumento automatico del volume è stato disabilitato e che è stata impostata una garanzia di spazio sul volume.

   Potresti decidere di abilitare l'aumento automatico, ma ai fini di questo scenario, decidi di indagare ulteriormente prima di prendere una decisione su come risolvere il problema di capacità.

9. Scorrendo verso il basso fino all'elenco **Eventi** si noterà che sono stati generati gli eventi Protection Job Failed, Volume Days Until Full e Volume Space Full.
10. Nell'elenco **Eventi**, fai clic sull'evento **Spazio volume pieno** per ottenere maggiori informazioni, dopo aver deciso che questo evento sembra il più pertinente al tuo problema di capacità.

    Nella pagina Dettagli evento viene visualizzato l'evento Spazio volume pieno per il volume di origine.

11. Nell'area **Riepilogo** puoi leggere 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 Riepilogo sono presenti le azioni correttive suggerite.

    Le azioni correttive suggerite vengono visualizzate solo per alcuni eventi, pertanto quest'area non è visibile per tutti i tipi di eventi.

    Fai clic sull'elenco delle azioni suggerite che potresti eseguire per risolvere l'evento Spazio volume pieno:

    - Abilita l'aumento automatico su questo volume.
    - Ridimensiona il volume.
    - Abilita ed esegui la deduplicazione su questo volume.
    - Abilita ed esegui la compressione su questo volume.

13. Si decide di abilitare l'aumento automatico sul volume, ma per farlo è necessario determinare lo spazio libero disponibile sull'aggregato padre e l'attuale tasso di crescita del volume:
    a. Guarda l'aggregato genitore, `cluster2_src_aggr1` , nel riquadro **Dispositivi correlati**.

       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 l'aumento automatico del volume.

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

       Si determina che "Giorni per il completamento: Meno di un giorno | Tasso di crescita giornaliero: 5,4%".

14. Vai a System Manager o accedi a ONTAP CLI per abilitare `volume autogrow` opzione.

Prendi nota dei nomi del volume e dell'aggregato in modo da averli a disposizione quando attivi l'aumento automatico.

15. Dopo aver risolto il problema di capacità, torna alla pagina dei dettagli **Evento** di Unified Manager e contrassegna l'evento come risolto.

Risolvere i problemi di ritardo

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

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Nella pagina Dashboard, esaminando l'area Incidenti e rischi irrisolti, si nota un errore SnapMirror Lag nel riquadro Protezione in Rischi di protezione.

Passi

1. Nel riquadro **Protezione** nella pagina **Dashboard**, individua l'errore di ritardo della relazione SnapMirror e fai clic su di esso.

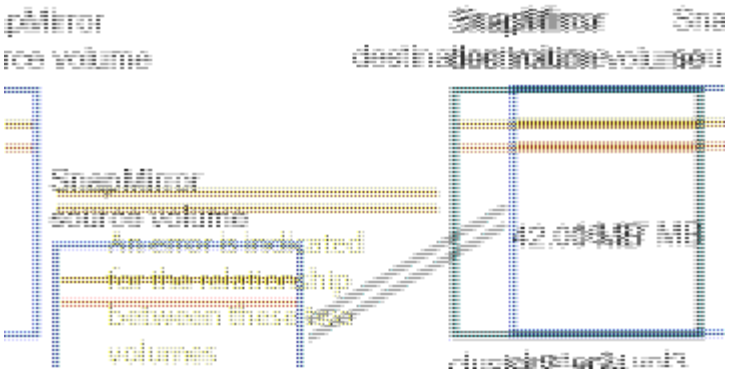
   Viene visualizzata la pagina dei dettagli dell'evento di errore di ritardo.

2. Dalla pagina dei dettagli dell'**Evento** puoi eseguire una o più delle seguenti attività:
   - Esaminare il messaggio di errore nel campo Causa dell'area Riepilogo per determinare se è possibile suggerire un'azione correttiva.
   - Fare clic sul nome dell'oggetto, in questo caso un volume, nel campo Origine dell'area Riepilogo per ottenere dettagli sul volume.
   - Cerca le note che potrebbero essere state aggiunte su questo evento.
   - Aggiungi una nota all'evento.
   - Assegna l'evento a un utente specifico.
   - Riconoscere o risolvere l'evento.
3. In questo scenario, fai clic sul nome dell'oggetto (in questo caso, un volume) nel campo Origine dell'area **Riepilogo** per ottenere dettagli sul volume.

   Viene visualizzata la scheda Protezione della pagina Dettagli volume/integrità.

4. Nella scheda **Protezione**, puoi osservare 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 è evidenziato in grigio scuro e una doppia linea arancione dal volume sorgente indica un errore di relazione SnapMirror .



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

   Selezionando ciascun volume, le informazioni sulla protezione nelle aree Riepilogo, Topologia, Cronologia, Eventi, Dispositivi correlati e Avvisi correlati cambiano per visualizzare i dettagli rilevanti per il volume selezionato.

6. Si guarda l'area **Riepilogo** e si posiziona il cursore sull'icona informativa nel campo **Aggiorna programma** per ciascun volume.

   In questo scenario, si noti che il criterio SnapMirror è DPDefault e che la pianificazione SnapMirror si aggiorna ogni ora, cinque minuti dopo l'ora. Ti rendi conto che tutti i volumi nella relazione stanno tentando di completare un trasferimento SnapMirror contemporaneamente.

7. Per risolvere il problema del ritardo, è necessario modificare le pianificazioni per due dei volumi a cascata in modo che ogni destinazione avvii un trasferimento SnapMirror dopo che la sua origine ha completato un trasferimento.