Creare e risolvere i problemi delle relazioni di protezione

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-918/data-protection/concept_types_of_snapmirror_protection.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Creare e risolvere i problemi delle relazioni di protezione . . . 1
Tipi di protezione SnapMirror in Active IQ Unified Manager . . . 1
Relazioni tradizionali di protezione asincrona SnapMirror . . . 1
SnapMirror Protezione asincrona con replica flessibile in base alla versione . . . 1
SnapMirror Protezione asincrona con replica flessibile in base alla versione e opzione di backup . . . 1
SnapMirror replica unificata (mirror e vault) . . . 2
SnapMirror Protezione sincrona con sincronizzazione rigorosa . . . 2
SnapMirror protezione sincrona con sincronizzazione regolare . . . 2
SnapMirror active sync . . . 2
Configura le relazioni di protezione in Unified Manager . . . 3
Configura le relazioni di protezione in Active IQ Unified Manager . . . 3
Configura una connessione tra Workflow Automation e Active IQ Unified Manager . . . 3
Verifica la memorizzazione nella cache dell'origine dati di Active IQ Unified Manager in Workflow Automation . . . 4
In che modo la reinstallazione o l'aggiornamento di OnCommand Workflow Automation influisce su Active IQ Unified Manager . . . 5
Rimuovi la configurazione di OnCommand Workflow Automation da Active IQ Unified Manager . . . 5
Esegui il failover e il failback della relazione di protezione . . . 5
Esegui un failover e un failback della relazione di protezione in Active IQ Unified Manager . . . 5
Interrompi una relazione di protezione SnapMirror dalla pagina Volume/Salute di Active IQ Unified Manager . . . 6
Inverti le relazioni di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager . . . 7
Rimuovi una relazione di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager . . . 8
Risincronizza le relazioni di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager . . . 8
Risolvere un errore del processo di protezione . . . 9
Risolvi un errore relativo a un processo di protezione in Active IQ Unified Manager . . . 9
Identifica il problema ed esegui le azioni correttive per un job di protezione non riuscito in Active IQ Unified Manager . . . 10
Risolvi i problemi di latenza in Active IQ Unified Manager . . . 13

Creare e risolvere i problemi delle relazioni di protezione

Tipi di protezione SnapMirror in Active IQ Unified Manager

A seconda della topologia di storage dei dati implementata, Unified Manager ti consente di configurare diversi tipi di relazioni di protezione SnapMirror. Tutte le varianti della protezione SnapMirror offrono protezione dal disaster recovery in caso di failover, ma presentano capacità diverse in termini di prestazioni, flessibilità della versione e protezione di più copie di backup.

Relazioni tradizionali di protezione asincrona SnapMirror

La protezione asincrona tradizionale di SnapMirror offre una protezione mirror della replica 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 replica a blocchi. Tuttavia, la protezione SnapMirror tradizionale richiede che il volume di destinazione esegua la stessa versione secondaria o una versione secondaria successiva del software ONTAP rispetto al 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 una fonte 9.1 a una destinazione 9.0 non è supportata perché la destinazione esegue una versione principale precedente.

SnapMirror Protezione asincrona con replica flessibile in base alla versione

SnapMirror La protezione asincrona con replica flessibile in base alla versione offre una protezione mirror della replica logica tra i volumi di origine e di destinazione, anche se tali volumi vengono eseguiti 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 con cui verrebbero eseguite nelle relazioni SnapMirror tradizionali.

A causa della minore velocità di esecuzione, SnapMirror con protezione della replica flessibile in base alla versione non è adatto da implementare 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. (Ovvero, la destinazione deve sempre contenere dati mirrorati e ripristinabili che non siano più vecchi di due ore rispetto ai dati presenti nell'origine.)

In entrambi i casi elencati, è necessaria l'esecuzione più rapida della protezione predefinita di SnapMirror basata sulla replica a blocchi.

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

SnapMirror La protezione asincrona con replica flessibile in base alla versione e opzione di backup offre una protezione mirror tra i volumi di origine e di destinazione e la possibilità di archiviare più copie dei dati mirrorati

nella destinazione.

L'amministratore dello storage 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 nell'origine.

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

SnapMirror replica unificata (mirror e vault)

SnapMirror La replica unificata ti consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Come con SnapMirror, la protezione dei dati unificata esegue un trasferimento baseline la prima volta che la richiami. Un trasferimento baseline 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 dei dati unificata non include le copie Snapshot meno recenti nella baseline.

SnapMirror Protezione sincrona con sincronizzazione rigorosa

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

SnapMirror protezione sincrona con sincronizzazione regolare

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



Il pulsante Ripristina e i pulsanti delle operazioni di relazione non sono disponibili quando monitori le relazioni di protezione sincrona dalla vista Health: All Volumes o dalla pagina dei dettagli Volume / Health.

SnapMirror active sync

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

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

Quando visualizzi i volumi e le LUN protetti dalla relazione SnapMirror active sync, puoi ottenere una vista unificata delle relazioni di protezione, dei gruppi di coerenza nell'inventario dei volumi, visualizzare la topologia di protezione per le relazioni dei gruppi di coerenza e visualizzare i dati storici delle relazioni dei gruppi di coerenza fino a un anno. Puoi anche scaricare il report. Puoi anche visualizzare il riepilogo delle relazioni dei gruppi di coerenza, cercare le relazioni dei gruppi di coerenza supportate e ottenere informazioni sui volumi protetti dal gruppo di coerenza.

Nella pagina Relazioni, puoi anche ordinare, filtrare ed estendere la protezione degli oggetti di storage di origine e destinazione e della relativa relazione protetti dal Consistency Group.

Per saperne di più su SnapMirror active sync, consulta "Documentazione di ONTAP 9 per Snapmirror active sync (precedentemente SM-BC)".

Configura le relazioni di protezione in Unified Manager

Configura le relazioni di protezione in Active IQ Unified Manager

Per utilizzare Unified Manager e OnCommand Workflow Automation per configurare relazioni di SnapMirror e SnapVault per proteggere i tuoi dati, devi eseguire diversi passaggi.

Prima di iniziare

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

Passaggi

1. A seconda del tipo di relazione di protezione che vuoi creare, procedi in uno dei seguenti modi:
   - "Crea una relazione di protezione di SnapMirror".
   - "Crea una relazione di protezione di SnapVault".
2. Se vuoi creare una policy per la relazione, a seconda del tipo di relazione che stai creando, procedi in uno dei seguenti modi:
   - "Crea un criterio SnapVault".
   - "Crea una policy SnapMirror".
3. "Crea una pianificazione di SnapMirror o SnapVault".

Configura una connessione tra Workflow Automation e Active IQ Unified Manager

Puoi configurare una connessione sicura tra OnCommand Workflow Automation (WFA) e Unified Manager. La connessione a Workflow Automation ti consente di utilizzare funzionalità di protezione come i flussi di lavoro di configurazione di SnapMirror e SnapVault, nonché i comandi per gestire le relazioni di 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 dallo NetAppStorage Automation Store e installarlo separatamente sul server WFA come richiesto in passato. "Download WFA"

- Devi disporre del nome dell'utente del database che hai creato in Unified Manager per supportare le connessioni tra WFA e Unified Manager.

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

- Devi avere il ruolo di Administrator o di Architect in Workflow Automation.
- Devi disporre dell'indirizzo host, del numero di porta 443, del nome utente e della password per la configurazione di Workflow Automation.
- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Workflow Automation**.
2. Nell'area **Database User** della pagina **Workflow Automation**, seleziona il nome e inserisci la password dell'utente del database che hai creato per supportare le connessioni di Unified Manager e Workflow Automation.
3. Nell'area **Workflow Automation Credentials** della pagina, immetti l'host name o l'indirizzo IP (IPv4 o IPv6), il nome utente e la password per la configurazione di Workflow Automation.

   Devi utilizzare la porta del server Unified Manager (porta 443).

4. Fare clic su **Save**.
5. Se utilizzi un certificato autofirmato, fai clic su **Sì** per autorizzare il certificato di sicurezza.

   Viene visualizzata la pagina Workflow Automation.

6. Fai clic su **Sì** per ricaricare l'interfaccia utente web e aggiungere le funzionalità di Workflow Automation.

Informazioni correlate

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

Verifica la memorizzazione nella cache dell'origine dati di Active IQ Unified Manager in Workflow Automation

Puoi determinare se la cache delle origini dati di Unified Manager funziona correttamente controllando se l'acquisizione delle origini dati ha esito positivo in Workflow Automation. Potresti farlo quando integri Workflow Automation con Unified Manager per assicurarti che la funzionalità di Workflow Automation sia disponibile dopo l'integrazione.

Prima di iniziare

Per eseguire questa attività, devi avere assegnato il ruolo Administrator o il ruolo Architect in Workflow Automation.

Passaggi

1. Dall'interfaccia utente di Workflow Automation, seleziona **Esecuzione** > **Origini dati**.
2. Fai clic con il pulsante destro del mouse sul nome dell'origine dati di Unified Manager e seleziona **Acquire Now**.
3. Verifica che l'acquisizione vada a buon fine senza errori.

   Per garantire il successo dell'integrazione di Workflow Automation con Unified Manager, devi risolvere gli

errori di acquisizione.

In che modo la reinstallazione o l'aggiornamento di OnCommand Workflow Automation influisce su Active IQ Unified Manager

Prima di reinstallare o aggiornare OnCommand Workflow Automation, devi prima rimuovere la connessione tra OnCommand Workflow Automation e Unified Manager e assicurarti che tutti i processi di OnCommand Workflow Automation attualmente in esecuzione o pianificati siano arrestati.

Devi anche eliminare manualmente Unified Manager da OnCommand Workflow Automation.

Dopo aver reinstallato o aggiornato OnCommand Workflow Automation, devi configurare di nuovo la connessione con Unified Manager.

Rimuovi la configurazione di OnCommand Workflow Automation da Active IQ Unified Manager

Puoi rimuovere la configurazione di OnCommand Workflow Automation da Unified Manager quando non vuoi più usare Workflow Automation.

Prima di iniziare

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Passaggi

1. Nel riquadro di navigazione a sinistra, nel menu Setup a sinistra, fai clic su **Generale** > **Workflow Automation**.
2. Nella pagina **Workflow Automation**, fai clic su **Remove Setup**.

Esegui il failover e il failback della relazione di protezione

Esegui un failover e un failback della relazione di protezione in Active IQ Unified Manager

Quando un volume di origine nella relazione di protezione viene disabilitato a causa di un guasto hardware o di un evento catastrofico, puoi usare le funzionalità della relazione di protezione in Unified Manager per rendere la destinazione della protezione accessibile in lettura/scrittura ed eseguire il failover su quel volume finché l'origine non torna di nuovo online; quindi, puoi eseguire il failback all'origine originale quando è di nuovo disponibile per fornire i dati.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Per eseguire questa operazione, devi aver configurato OnCommand Workflow Automation.

Passaggi

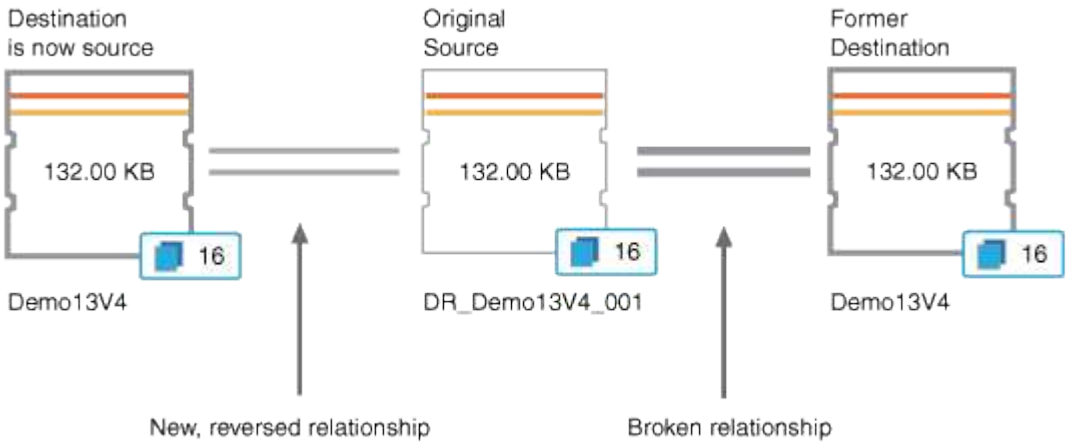
1. "Interrompi la relazione di SnapMirror".

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

2. "Inverti la relazione di protezione".

   Quando il volume di origine originale sarà di nuovo disponibile, potresti decidere di ristabilire la relazione di protezione originale ripristinando il volume di origine. Prima di poter ripristinare il volume di origine, devi sincronizzarlo con i dati scritti nella precedente destinazione. Usi 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 precedente destinazione. Per la nuova relazione viene creata una nuova copia Snapshot di riferimento.

   La relazione inversa è simile a una relazione a cascata:



3. "Interrompi la relazione di SnapMirror invertita".

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

4. "Elimina la relazione".

   Quando la relazione inversa non è più necessaria, dovresti rimuoverla prima di ristabilire la relazione originale.

5. "Risincronizza la relazione".

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

Interrompi una relazione di protezione SnapMirror dalla pagina Volume/Salute di Active IQ Unified Manager

Puoi interrompere una relazione di protezione dalla pagina Dettagli volume/integrità e bloccare i trasferimenti di dati tra un volume di origine e un volume di destinazione in una relazione di SnapMirror. Potresti interrompere una relazione quando vuoi migrare i dati, per il disaster recovery o per testare le applicazioni. Il volume di destinazione viene modificato in un volume di lettura-scrittura. Non puoi interrompere una relazione di SnapVault.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Devi aver configurato Workflow Automation.

Passaggi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume / Integrità**, seleziona dalla topologia la relazione di SnapMirror che desideri interrompere.
2. Fai clic con il pulsante destro del mouse sulla destinazione e seleziona **Break** dal menu.

   Compare la finestra di dialogo Break Relationship.
3. Fai clic su **Continue** per interrompere la relazione.
4. Nella topologia, verifica che la relazione sia interrotta.

Inverti le relazioni di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager

Quando un evento disastroso disabilita il volume di origine nella relazione di protezione, puoi usare il volume di destinazione per fornire dati convertendolo in lettura/scrittura mentre ripari o sostituisci l'origine. Quando l'origine è di nuovo disponibile per ricevere dati, puoi usare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sull'origine con i dati sulla destinazione in lettura/scrittura.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Devi aver configurato Workflow Automation.
- La relazione non deve essere una relazione di SnapVault.
- Deve già esistere una relazione di protezione.
- La relazione di protezione deve essere interrotta.
- Sia l'origine che la destinazione devono essere online.
- L'origine non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando esegui questa operazione, i dati sull'origine più recenti dei dati nella copia Snapshot comune vengono eliminati.
- Le politiche e le pianificazioni create sulla relazione di risincronizzazione inversa sono le stesse di quelle sulla relazione di protezione originale.

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

Passaggi

1. Dalla scheda **Protezione** della pagina dei dettagli **Volume / Health**, individua nella topologia la relazione di SnapMirror su cui vuoi invertire origine e destinazione e fai clic con il pulsante destro del mouse su di essa.
2. Seleziona **Reverse Resync** dal menu.

   Si apre la finestra di dialogo Reverse Resync.

3. Verifica che la relazione visualizzata nella finestra di dialogo **Risincronizzazione inversa** sia quella per cui vuoi eseguire l'operazione di risincronizzazione inversa, quindi fai clic su **Invia**.

   La finestra di dialogo Risincronizzazione inversa si chiude e nella parte superiore della pagina dei dettagli Volume / Health compare un collegamento al processo.

4. **Facoltativo:** Fai clic su **View Jobs** nella pagina dei dettagli **Volume / Health** per monitorare lo stato di ciascun processo di risincronizzazione inversa.

   Viene visualizzato un elenco filtrato di processi.

5. **Facoltativo:** Fai clic sulla freccia **Back** del browser per tornare alla pagina dei dettagli **Volume / Health**.

   L'operazione di risincronizzazione inversa termina quando tutte le attività del processo sono completate correttamente.

Rimuovi una relazione di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager

Puoi rimuovere una relazione di protezione per eliminare definitivamente una relazione esistente tra l'origine e la destinazione: ad esempio, quando vuoi creare una relazione utilizzando una destinazione diversa. Questa operazione rimuove tutti i metadati e non può essere annullata.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Devi aver configurato Workflow Automation.

Passaggi

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

   Viene visualizzata la finestra di dialogo Remove Relationship.

3. Fai clic su **Continua** per rimuovere la relazione.

   La relazione viene rimossa dalla pagina dei dettagli Volume / Health.

Risincronizza le relazioni di protezione dalla pagina Dettagli Volume/Salute in Active IQ Unified Manager

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

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

- Devi aver configurato OnCommand Workflow Automation.

Passaggi

1. Nella scheda **Protezione** della pagina dei dettagli **Volume/Integrità**, individua nella topologia la relazione di protezione che desideri risincronizzare e fai clic con il pulsante destro del mouse su di essa.
2. Seleziona **Risincronizza** dal menu.

   In alternativa, dal menu **Azioni**, seleziona **Relazione** > **Risincronizza** per risincronizzare la relazione di cui stai visualizzando i dettagli.

   Si apre la finestra di dialogo Risincronizza.

3. Nella scheda **Opzioni di risincronizzazione**, seleziona una priorità di trasferimento e la velocità di trasferimento massima.
4. Fai clic su **Copie Snapshot di origine**; quindi, nella colonna **Copia Snapshot**, fai clic su **Default**.

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

5. Se vuoi specificare una copia Snapshot esistente anziché trasferire la copia Snapshot predefinita, fai clic su **Existing Snapshot Copy** e seleziona una copia Snapshot dall'elenco.
6. Fai clic su **Submit**.

   Verrai reindirizzato alla finestra di dialogo Resynchronize.

7. Se hai selezionato più di un'origine da risincronizzare, fai clic su **Predefinito** per l'origine successiva per la quale vuoi specificare una copia Snapshot esistente.
8. Fai clic su **Submit** per avviare il processo di risincronizzazione.

   Il processo di risincronizzazione viene avviato, vieni reindirizzato alla pagina dei dettagli di Volume / Health e nella parte superiore della pagina viene visualizzato un link ai processi.

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

   Viene visualizzato un elenco filtrato di processi.

10. **Facoltativo:** Fai clic sulla freccia **Back** del browser per tornare alla pagina dei dettagli **Volume / Health**.

    Il processo di risincronizzazione termina quando tutte le attività del processo vengono completate correttamente.

Risolvere un errore del processo di protezione

Risolvi un errore relativo a un processo di protezione in Active IQ Unified Manager

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

Prima di iniziare

Poiché alcune attività di questo flusso di lavoro richiedono che tu acceda usando il ruolo di Administrator, devi conoscere bene i ruoli necessari per utilizzare le diverse funzionalità.

In questo scenario, accedi alla pagina Dashboard per verificare se ci sono problemi con i tuoi job di protezione. Nell'area Incidenti di protezione, noti un incidente "Job Terminated" che mostra un errore "Protection Job Failed" su un volume. Indaghi su questo errore per determinarne la possibile causa e la potenziale soluzione.

Passaggi

1. Nel pannello Incidenti di protezione dell'area Incidenti e rischi irrisolti del dashboard, fai 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`.

   Si apre la pagina dei dettagli dell'evento per il processo di protezione non riuscito.

2. Esamina il messaggio di errore nel campo Cause dell'area **Summary** per individuare il problema e valutare le possibili azioni correttive.

   Vedi "Identificare il problema ed eseguire azioni correttive per un job di protezione non riuscito".

Identifica il problema ed esegui le azioni correttive per un job di protezione non riuscito in Active IQ Unified Manager

Esamini il messaggio di errore relativo all'errore del processo nel campo Cause nella pagina Event details e stabilisci che il processo non è riuscito a causa di un errore della copia Snapshot. Passi quindi alla pagina Volume / Health details per raccogliere ulteriori informazioni.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Il messaggio di errore visualizzato nel campo Causa nella pagina Dettagli evento contiene il seguente testo relativo al job 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:

- L'operazione di backup o mirroring non è stata completata correttamente.

  Il processo 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'operazione di copia Snapshot non è riuscita per `0426cluster2_src_vol2snap` sul volume di origine `cluster2_src_svm:/cluster2_src_vol2`.

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

Passaggi

1. Esamina il messaggio di errore e stabilisci che un'operazione di copia Snapshot non è riuscita sul volume di origine, il che indica probabilmente un problema con il volume di origine.

   Facoltativamente, puoi fare clic sul collegamento **Job Details** alla fine del messaggio di errore, ma ai fini di questo scenario scegli di non farlo.

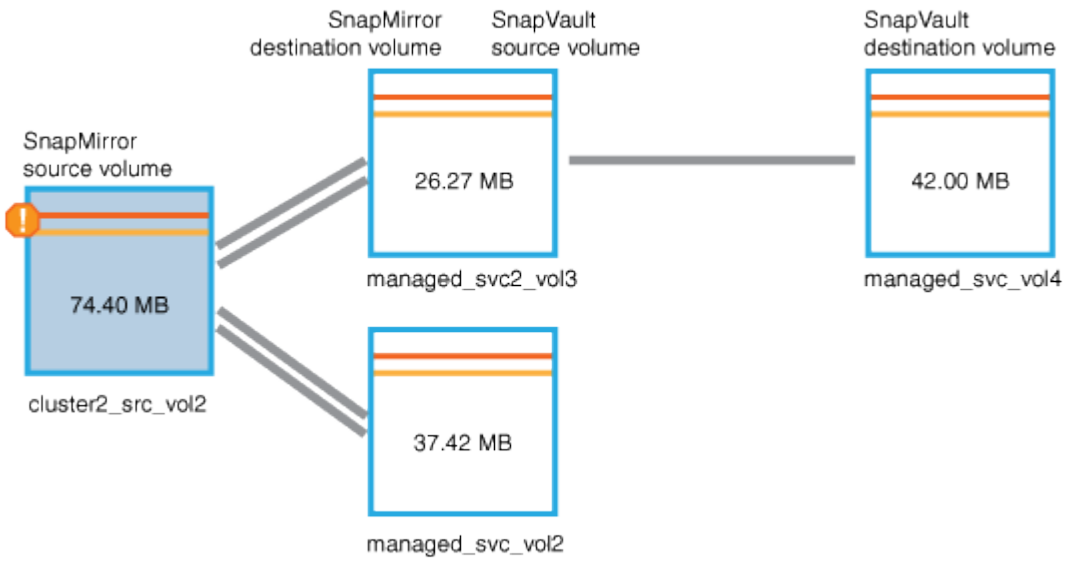
2. Decidi di provare a risolvere l'evento, quindi procedi come segue:
   a. Fai clic sul pulsante **Assign To** e seleziona **Me** dal menu.
   b. Fai clic sul pulsante **Acknowledge** per non continuare a ricevere notifiche di avviso ripetute, se per l'evento erano stati impostati avvisi.
   c. Facoltativamente, puoi anche aggiungere note sull'evento.
3. Fai clic sul campo **Origine** nel riquadro **Riepilogo** per visualizzare i dettagli relativi al 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.

   Compare la pagina dei dettagli Volume / Integrità per `cluster2_src_vol2`, che mostra il contenuto della scheda Protezione.

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

   Nell'icona del volume sorgente sono inoltre visibili delle barre orizzontali che indicano le soglie di avviso e di errore impostate per quel volume.



5. Posiziona il cursore sull'icona di errore per visualizzare la finestra di dialogo a comparsa con le impostazioni della soglia e vedere che il volume ha superato la soglia di errore, indicando un problema di capacità.

6. Fai clic sulla scheda **Capacity**.

   Informazioni sulla capacità dei display del volume `cluster2_src_vol2`.

7. Nel pannello **Capacità**, vedi un'icona di errore nel grafico a barre, che indica nuovamente che la capacità del volume ha superato il livello di soglia impostato per il volume.
8. Sotto il grafico della capacità, vedi che l'espansione automatica del volume è disattivata e che sul volume è impostata una garanzia di spazio.

   Potresti decidere di abilitare l'espansione automatica, ma ai fini di questo scenario decidi di approfondire la questione prima di decidere come risolvere il problema di capacità.

9. Scorri verso il basso fino all'elenco **Events** e vedi che sono comparsi gli eventi Protection Job Failed, Volume Days Until Full e Volume Space Full.
10. Nell'elenco **Events**, fai clic sull'evento **Volume Space Full** per ottenere maggiori informazioni, dopo aver stabilito che questo evento sembra essere il più rilevante per il tuo problema di capacità.

    La pagina dei dettagli dell'evento visualizza l'evento Spazio del volume pieno per il volume di origine.

11. Nell'area **Riepilogo**, leggi 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, vedi le Azioni correttive suggerite.

    Le azioni correttive suggerite vengono visualizzate solo per alcuni eventi, quindi questa sezione non è presente per tutti i tipi di eventi.

    Fai clic sull'elenco delle azioni suggerite che puoi eseguire per risolvere l'evento Spazio del volume esaurito:

    - Abilita la crescita automatica su questo volume.
    - Ridimensiona il volume.
    - Abilita ed esegui la deduplicazione su questo volume.
    - Abilita ed esegui la compressione su questo volume.

13. Decidi di abilitare l'espansione automatica sul volume, ma per farlo devi determinare lo spazio libero sull'aggregate principale e il tasso di crescita corrente del volume:
    a. Osserva l'aggregato principale, `cluster2_src_aggr1` nel riquadro **Dispositivi correlati**.

       Puoi cliccare sul nome dell'aggregato per ottenere maggiori dettagli sull'aggregato.

       Determini che l'aggregato dispone di spazio sufficiente per abilitare l'espansione automatica del volume.

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

       Hai stabilito che "Giorni al riempimento: meno di un giorno | Tasso di crescita giornaliero: 5,4%".

14. Vai in System Manager o accedi alla CLI di ONTAP per abilitare l' `volume autogrow`opzione.

    Prendi nota dei nomi del volume e dell'aggregato in modo da averli a disposizione quando

abiliti l’espansione automatica.

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

Risolvi i problemi di latenza in Active IQ Unified Manager

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

Prima di iniziare

Devi disporre del ruolo di Amministratore dell’applicazione o di Amministratore dello storage.

Nella pagina Dashboard, osservi l’area Incidenti e rischi irrisolti e vedi un errore di ritardo di SnapMirror nel riquadro Protezione in Rischi di protezione.

Passaggi

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

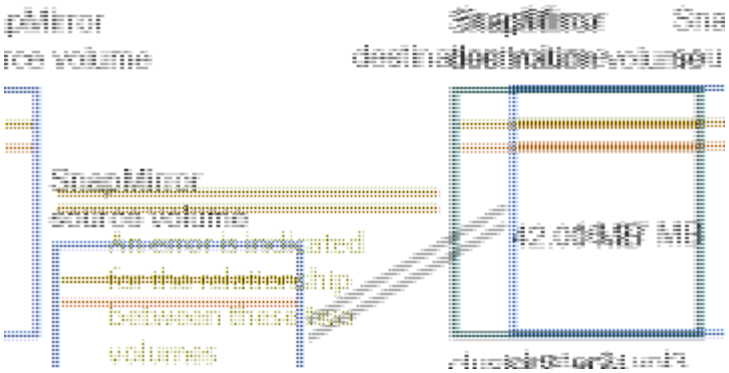
   Viene visualizzata la pagina dei dettagli dell’evento relativo all’errore di ritardo.

2. Dalla pagina dei dettagli di **Event** puoi eseguire una o più delle seguenti operazioni:
   - Esamina il messaggio di errore nel campo Causa dell’area Riepilogo per verificare se è suggerita un’azione correttiva.
   - Fai clic sul nome dell’oggetto, in questo caso un volume, nel campo Origine dell’area Riepilogo per visualizzare i dettagli relativi al volume.
   - Cerca eventuali note aggiunte in merito a questo evento.
   - Aggiungi una nota all’evento.
   - Assegna l’evento a un utente specifico.
   - Riconosci o risolvi l’evento.
3. In questo scenario, fai clic sul nome dell’oggetto (in questo caso, un volume) nel campo Source dell’area **Summary** per ottenere i dettagli sul volume.

   Viene visualizzata la scheda Protezione della pagina dei dettagli Volume/Stato di integrità.

4. Nella scheda **Protezione**, visualizzi il diagramma topologico.

   Noti che il volume con l’errore di ritardo è l’ultimo volume in una cascata di tre volumi di SnapMirror. Il volume che hai selezionato è delineato in grigio scuro e una doppia linea arancione dal volume di origine indica un errore di relazione di SnapMirror.



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

   Quando selezioni ciascun volume, le informazioni di protezione nelle aree Riepilogo, Topologia, Cronologia, Eventi, Dispositivi correlati e Avvisi correlati cambiano per mostrare i dettagli pertinenti al volume selezionato.

6. Guarda l'area **Riepilogo** e posiziona il cursore sull'icona delle informazioni nel campo **Pianificazione aggiornamenti** per ciascun volume.

   In questo scenario, noti che il criterio di SnapMirror è DPDefault e che la pianificazione di 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 di SnapMirror contemporaneamente.

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.