



Impostazione delle relazioni di protezione in Unified Manager

Active IQ Unified Manager 9.7

NetApp
April 17, 2024

Sommario

- Impostazione delle relazioni di protezione in Unified Manager 1
 - Prima di iniziare 1
 - Fasi 1
 - Configurazione di una connessione tra Workflow Automation e Unified Manager 1
 - Verifica del caching dell'origine dati di Unified Manager in Workflow Automation 2
 - Cosa succede quando OnCommand Workflow Automation viene reinstallato o aggiornato 3
 - Rimozione dell'installazione di OnCommand Workflow Automation da Unified Manager 3
 - Creazione di una relazione di protezione SnapMirror dalla pagina dei dettagli relativi a volume/stato 3
 - Creazione di una relazione di protezione SnapVault dalla pagina dei dettagli relativi a volume/salute 5
 - Creazione di una policy SnapVault per massimizzare l'efficienza del trasferimento 6
 - Creazione di una policy SnapMirror per massimizzare l'efficienza del trasferimento 7
 - Creazione di pianificazioni SnapMirror e SnapVault 7

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.

Prima di iniziare

- 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.

Prima di iniziare

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



Il "pacchetto WFA per la gestione di Clustered Data ONTAP" è incluso in WFA 5.1, pertanto non è necessario scaricare questo pacchetto dal NetAppStorage Automation Store 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.

Prima di iniziare

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.

Prima di iniziare

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).

Creazione di una relazione di protezione SnapMirror dalla pagina dei dettagli relativi a volume/stato

È possibile utilizzare la pagina Dettagli volume/stato per creare una relazione SnapMirror in modo che la replica dei dati sia attivata per scopi di protezione. La replica di SnapMirror consente di ripristinare i dati dal volume di destinazione in caso di perdita di dati sull'origine.

Prima di iniziare

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

A proposito di questa attività

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

È possibile eseguire fino a 10 lavori di protezione contemporaneamente senza alcun impatto sulle performance. Si potrebbe riscontrare un certo impatto sulle performance quando si eseguono contemporaneamente da 11 a 30 job. Si sconsiglia di eseguire più di 30 lavori contemporaneamente.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse nella vista topologia per visualizzare il nome di un volume che si desidera proteggere.
2. Selezionare **Protect > SnapMirror** dal menu.

Viene visualizzata la finestra di dialogo Configura protezione.

3. Fare clic su **SnapMirror** per visualizzare la scheda **SnapMirror** e configurare le informazioni di destinazione.
4. Fare clic su **Advanced** (Avanzate) per impostare la garanzia di spazio, secondo necessità, quindi fare clic su **Apply** (Applica).
5. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).
6. Fare clic su **Apply** (Applica).

Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

Le attività e i dettagli del lavoro vengono visualizzati nella pagina Dettagli lavoro.

8. Nella pagina dei dettagli **lavoro**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
9. Una volta completate le attività di lavoro, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Health**.

La nuova relazione viene visualizzata nella vista topologia della pagina dei dettagli volume/salute.

Risultati

A seconda della SVM di destinazione specificata durante la configurazione o delle opzioni attivate nelle impostazioni avanzate, la relazione SnapMirror risultante potrebbe essere una delle diverse possibili variazioni:

- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP rispetto a quella del volume di origine, il risultato predefinito è una relazione SnapMirror basata sulla replica a blocchi.
- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP (versione 8.3 o superiore) rispetto a quella del volume di origine, ma è stata attivata la replica flessibile della versione nelle impostazioni avanzate, si ottiene una relazione di SnapMirror con la replica flessibile della versione.
- Se è stata specificata una SVM di destinazione che viene eseguita con una versione precedente di ONTAP 8.3 o una versione superiore a quella del volume di origine e la versione precedente supporta la replica flessibile dalla versione, il risultato è automatico una relazione di SnapMirror con la replica flessibile dalla versione.

Creazione di una relazione di protezione SnapVault dalla pagina dei dettagli relativi a volume/salute

È possibile creare una relazione SnapVault utilizzando la pagina dei dettagli relativi a volume/stato di salute in modo che i backup dei dati siano abilitati per scopi di protezione sui volumi.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Per eseguire questa attività, è necessario aver impostato l'automazione del flusso di lavoro.

A proposito di questa attività

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse su un volume nella vista della topologia che si desidera proteggere.
2. Selezionare **Protect > SnapVault** dal menu.

Viene visualizzata la finestra di dialogo Configura protezione.

3. Fare clic su **SnapVault** per visualizzare la scheda **SnapVault** e configurare le informazioni sulle risorse secondarie.
4. Fare clic su **Advanced** (Avanzate) per impostare deduplica, compressione, crescita automatica e garanzia

di spazio secondo necessità, quindi fare clic su **Apply** (Applica).

5. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).
6. Fare clic su **Apply** (Applica).

Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

Viene visualizzata la pagina Dettagli lavoro.

8. Fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al processo di configurazione della protezione e per determinare quando il processo è completo.

Una volta completate le attività di lavoro, le nuove relazioni vengono visualizzate nella vista topologia della pagina dei dettagli volume/salute.

Creazione di una policy SnapVault per massimizzare l'efficienza del trasferimento

È possibile creare un nuovo criterio SnapVault per impostare la priorità per un trasferimento SnapVault. Le policy vengono utilizzate per massimizzare l'efficienza dei trasferimenti dal primario al secondario in una relazione di protezione.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- È necessario aver già completato l'area Destination Information (informazioni destinazione) nella finestra di dialogo Configure Protection (Configura protezione).

Fasi

1. Dalla scheda **SnapVault** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea policy** nell'area **Impostazioni relazione**.

Viene visualizzata la scheda SnapVault.

2. Nel campo **Policy Name**, digitare il nome che si desidera assegnare al criterio.
3. Nel campo **priorità trasferimento**, selezionare la priorità di trasferimento che si desidera assegnare al criterio.
4. Nel campo **Commento**, inserire un commento per la policy.
5. Nell'area **Replication Label**, aggiungere o modificare un'etichetta di replica, se necessario.
6. Fare clic su **Create** (Crea).

Il nuovo criterio viene visualizzato nell'elenco a discesa Crea criterio.

Creazione di una policy SnapMirror per massimizzare l'efficienza del trasferimento

È possibile creare un criterio SnapMirror per specificare la priorità di trasferimento di SnapMirror per le relazioni di protezione. Le policy di SnapMirror consentono di massimizzare l'efficienza del trasferimento dall'origine alla destinazione assegnando priorità in modo che i trasferimenti a priorità inferiore vengano pianificati per essere eseguiti dopo i trasferimenti a priorità normale.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- Questa attività presuppone che l'area Destination Information (informazioni destinazione) sia già stata completata nella finestra di dialogo Configure Protection (Configura protezione).

Fasi

1. Dalla scheda **SnapMirror** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea policy** nell'area **Impostazioni relazione**.

Viene visualizzata la finestra di dialogo Create SnapMirror Policy (Crea policy SnapMirror).

2. Nel campo **Policy Name** (Nome policy), digitare il nome che si desidera assegnare al criterio.
3. Nel campo **priorità trasferimento**, selezionare la priorità di trasferimento che si desidera assegnare al criterio.
4. Nel campo **Commento**, immettere un commento facoltativo per la policy.
5. Fare clic su **Create** (Crea).

Il nuovo criterio viene visualizzato nell'elenco a discesa SnapMirror Policy (criterio SnapMirror).

Creazione di pianificazioni SnapMirror e SnapVault

È possibile creare pianificazioni SnapMirror e SnapVault di base o avanzate per consentire trasferimenti automatici della protezione dei dati su un volume di origine o primario in modo che i trasferimenti vengano effettuati con maggiore frequenza o meno frequenza, a seconda della frequenza con cui i dati cambiano sui volumi.

Prima di iniziare

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver già completato l'area Destination Information (informazioni destinazione) nella finestra di dialogo Configure Protection (Configura protezione).
- Per eseguire questa attività, è necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Dalla scheda **SnapMirror** o **SnapVault** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea pianificazione** nell'area **Impostazioni relazione**.

Viene visualizzata la finestra di dialogo Create Schedule (Crea pianificazione).

2. Nel campo **Nome pianificazione**, digitare il nome che si desidera assegnare alla pianificazione.
3. Selezionare una delle seguenti opzioni:

- **Di base**

Selezionare questa opzione se si desidera creare una pianificazione di base in stile intervallo.

- **Avanzate**

Selezionare se si desidera creare un programma in stile cron.

4. Fare clic su **Create** (Crea).

La nuova pianificazione viene visualizzata nell'elenco a discesa Pianificazione SnapMirror o Pianificazione SnapVault.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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