



Configurazione e abilitazione della protezione dei dati basata su policy SnapManager for SAP

NetApp
April 19, 2024

Sommario

- Configurazione e abilitazione della protezione dei dati basata su policy 1
 - Configurare il server DataFabric Manager e SnapDrive quando RBAC è attivato 1
 - Configurare SnapDrive quando RBAC non è attivato 3
 - Informazioni sull'attivazione o la disattivazione della protezione dei dati nel profilo 3

Configurazione e abilitazione della protezione dei dati basata su policy

È necessario configurare SnapDrive e il server DataFabric Manager per abilitare la protezione dei dati sul profilo per proteggere i backup sui sistemi di storage secondari. È possibile selezionare i criteri di protezione nella console di Protection Manager per specificare la modalità di protezione dei backup del database.



Per abilitare la protezione dei dati, è necessario assicurarsi che OnCommand sia installato su un server separato.

Configurare il server DataFabric Manager e SnapDrive quando RBAC è attivato

Quando RBAC (role-based access control) è attivato, è necessario configurare il server DataFabric Manager in modo che includa le funzionalità RBAC. È inoltre necessario registrare l'utente SnapDrive creato nel server DataFabric Manager e l'utente root del sistema di storage in SnapDrive.

Fasi

1. Configurare il server DataFabric Manager.

- a. Per aggiornare il server DataFabric Manager e le modifiche apportate direttamente sul sistema di storage dal database di destinazione, immettere il seguente comando:

```
dfm host discover storage_system
```

- b. Creare un nuovo utente nel server DataFabric Manager e impostare la password.
- c. Per aggiungere l'utente del sistema operativo all'elenco di amministrazione del server DataFabric Manager, immettere il seguente comando:

```
dfm user add sd-admin
```

- d. Per creare un nuovo ruolo nel server DataFabric Manager, immettere il seguente comando:

```
dfm role create sd-admin-role
```

- e. Per aggiungere la funzionalità globale DFM.Core.AccessCheck al ruolo, immettere il seguente comando:

```
dfm role add sd-admin-role DFM.Core.AccessCheck Global
```

- f. Da aggiungere `sd-admin-role` per l'utente del sistema operativo, immettere il seguente comando:

```
dfm user role set sd-adminsd-admin-role
```

- g. Per creare un altro ruolo nel server DataFabric Manager per l'utente root di SnapDrive, immettere il seguente comando:

```
dfm role create sd-protect
```

- h. Per aggiungere funzionalità RBAC al ruolo creato per l'utente root SnapDrive o l'amministratore, immettere i seguenti comandi:

```
dfm role add sd-protect SD.Config.Read Global
```

```
dfm role add sd-protect SD.Config.Write Global
```

```
dfm role add sd-protect SD.Config.Delete Global
```

```
dfm role add sd-protect SD.Storage.Read Global
```

```
dfm role add sd-protect DFM.Database.Write Global
```

```
dfm role add sd-protect GlobalDataProtection
```

- a. Per aggiungere l'utente oracle del database di destinazione all'elenco degli amministratori nel server DataFabric Manager e assegnare il ruolo sd-Protect, immettere il seguente comando:

```
dfm user add -r sd-protecttardb_host1\oracle
```

- b. Per aggiungere il sistema storage utilizzato dal database di destinazione nel server DataFabric Manager, immettere il seguente comando:

```
dfm host set storage_system hostLogin=oracle hostPassword=password
```

- c. Per creare un nuovo ruolo nel sistema di storage utilizzato dal database di destinazione nel server DataFabric Manager, immettere il seguente comando:

```
dfm host role create -h storage_system-c "api-,login-" storage-rbac-role
```

- d. Per creare un nuovo gruppo nel sistema di storage e assegnare il nuovo ruolo creato nel server DataFabric Manager, immettere il seguente comando:

```
dfm host usergroup create -h storage_system-r storage-rbac-rolestorage-rbac-group
```

- e. Per creare un nuovo utente nel sistema di storage e assegnare il nuovo ruolo e il gruppo creato nel server DataFabric Manager, immettere il seguente comando:

```
dfm host user create -h storage_system-r storage-rbac-role -p password -g storage-rbac-grouptardb_host1
```

2. Configurare SnapDrive.

- a. Per registrare le credenziali di *sd-admin* Utente con SnapDrive, immettere il seguente comando:

```
snapdrive config set -dfm sd-admindfm_host
```

- b. Per registrare l'utente root o l'amministratore del sistema storage con SnapDrive, immettere il seguente comando:

```
snapdrive config set tardb_host1storage_system
```

Configurare SnapDrive quando RBAC non è attivato

Per abilitare la protezione dei dati, è necessario registrare l'utente root o l'amministratore del server DataFabric Manager e l'utente root del sistema storage con SnapDrive.

Fasi

1. Per aggiornare il server DataFabric Manager e le modifiche apportate direttamente sul sistema di storage dal database di destinazione, immettere il seguente comando:

Esempio

```
dfm host discover storage_system
```

2. Per registrare l'utente root o l'amministratore del server DataFabric Manager con SnapDrive, immettere il seguente comando:

Esempio

```
snapdrive config set -dfm Administrator dfm_host
```

3. Per registrare l'utente root o l'amministratore del sistema storage con SnapDrive, immettere il seguente comando:

Esempio


```
snapdrive config set root storage_system
```

Informazioni sull'attivazione o la disattivazione della protezione dei dati nel profilo

È possibile attivare o disattivare la protezione dei dati durante la creazione o l'aggiornamento di un profilo di database.

Per creare un backup protetto di un database sulle risorse di storage secondarie, gli amministratori del database e gli amministratori dello storage eseguono le seguenti operazioni.

Se si desidera...	Quindi...
Creare o modificare un profilo	<p>Per creare o modificare un profilo, attenersi alla seguente procedura:</p> <ul style="list-style-type: none"> • Abilitare la protezione del backup sullo storage secondario. • Se si utilizza Data ONTAP in 7-Mode e si è installato Protection Manager, è possibile selezionare i criteri creati dall'amministratore dello storage o del backup in Protection Manager. <p>Se si utilizza Data ONTAP in 7-Mode e la protezione è attivata, SnapManager crea un dataset per il database. Un set di dati è costituito da un insieme di set di storage insieme alle informazioni di configurazione associate ai dati. I set di storage associati a un set di dati includono un set di storage primario utilizzato per esportare i dati nei client e l'insieme di repliche e archivi presenti in altri set di storage. I set di dati rappresentano dati esportabili dell'utente. Se l'amministratore disattiva la protezione per un database, SnapManager elimina il dataset.</p> <ul style="list-style-type: none"> • Se si utilizza ONTAP, selezionare il criterio <i>SnapManager_cDOT_Mirror</i> o <i>SnapManager_cDOT_Vault</i> a seconda della relazione SnapMirror o SnapVault creata. <p>Quando si disattiva la protezione di backup, viene visualizzato un messaggio di avviso che indica che il set di dati verrà eliminato e che non sarà possibile ripristinare o clonare i backup per questo profilo.</p>
Visualizzare il profilo	Poiché l'amministratore dello storage non ha ancora assegnato risorse di storage per implementare il criterio di protezione, il profilo viene visualizzato come non conforme sia nell'interfaccia grafica utente di SnapManager che in <code>profile show</code> output del comando.
Assegnare le risorse di storage nella console di gestione di Protection Manager	Nella console di gestione di Protection Manager, l'amministratore dello storage visualizza il dataset non protetto e assegna un pool di risorse per ogni nodo del dataset associato al profilo. L'amministratore dello storage verifica quindi che i volumi secondari siano sottoposti a provisioning e che le relazioni di protezione siano inizializzate.
Visualizza il profilo conforme in SnapManager	In SnapManager, l'amministratore del database rileva che il profilo è stato modificato in stato conforme sia nell'interfaccia utente grafica che in <code>profile show</code> output del comando, che indica che le risorse sono state assegnate.

Se si desidera...	Quindi...
Creare il backup	<ul style="list-style-type: none"> • Selezionare backup completo. • Inoltre, selezionare se il backup deve essere protetto e selezionare la classe di conservazione primaria (ad esempio, oraria o giornaliera). • Se si utilizza Data ONTAP in 7-Mode e si desidera proteggere immediatamente il backup sullo storage secondario sovrascrivendo il programma di protezione di Protection Manager, specificare <code>-protectnow</code> opzione. • Se si utilizza ONTAP e si desidera proteggere immediatamente il backup sullo storage secondario, specificare <code>protect</code> opzione. <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Il <code>protectnow</code> L'opzione non è applicabile in Clustered Data ONTAP.</p> </div>
Visualizzare il backup	<p>Il nuovo backup viene visualizzato come pianificato per la protezione, ma non ancora protetto (nell'interfaccia SnapManager e in <code>backup show</code> output del comando). Lo stato di protezione viene visualizzato come "Not Protected" (non protetto).</p>
Visualizzare l'elenco di backup	<p>Dopo che l'amministratore dello storage ha verificato che il backup è stato copiato nello storage secondario, SnapManager modifica lo stato di protezione del backup da "non protetto" a "protetto".</p>

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.