Konfiguration und Aktivierung richtlinienbasierter Datensicherung

SnapManager for SAP

NetApp
April 19, 2024

Inhalt

Konfiguration und Aktivierung richtlinienbasierter Datensicherung

Sie müssen SnapDrive und den DataFabric Manager-Server konfigurieren, um die Datensicherung im Profil zu ermöglichen, um Backups auf sekundären Storage-Systemen zu sichern. Sie können die Schutzrichtlinien in der Protection Manager-Konsole auswählen, um anzugeben, wie Datenbank-Backups geschützt werden sollen.

> Sie müssen sicherstellen, dass OnCommand Unified Manager auf einem separaten Server installiert ist, um die Datensicherung zu ermöglichen.

Konfigurieren Sie DataFabric Manager Server und SnapDrive, wenn die RBAC aktiviert ist

Wenn die rollenbasierte Zugriffssteuerung aktiviert ist, müssen Sie den DataFabric Manager Server so konfigurieren, dass die RBAC-Funktionen enthalten sind. Sie müssen auch den im DataFabric Manager Server erstellten SnapDrive-Benutzer und den Root-Benutzer des Storage-Systems in SnapDrive registrieren.

Schritte

1. Konfigurieren Sie den DataFabric Manager Server.

   a. Geben Sie den folgenden Befehl ein, um den DataFabric Manager-Server zu aktualisieren, um die Änderungen direkt auf dem Storage-System durch die Zieldatenbank zu aktualisieren:

      dfm host discover *storage_system*

   b. Erstellen Sie einen neuen Benutzer im DataFabric Manager-Server, und legen Sie das Passwort fest.

   c. Geben Sie den folgenden Befehl ein, um den Betriebssystembenutzer zur DataFabric Manager Server-Administratorliste hinzuzufügen:

      dfm user add *sd-admin*

   d. Geben Sie den folgenden Befehl ein, um eine neue Rolle im DataFabric Manager-Server zu erstellen:

      dfm role create *sd-admin-role*

   e. Geben Sie den folgenden Befehl ein, um die Funktion DFM.Core.AccessCheck Global zur Rolle hinzuzufügen:

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

   f. Hinzufügen `sd-admin-role` Geben Sie zum Benutzer des Betriebssystems den folgenden Befehl ein:

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

   g. Geben Sie den folgenden Befehl ein, um eine weitere Rolle im DataFabric Manager-Server für den

SnapDrive-Root-Benutzer zu erstellen:

dfm role create *sd-protect*

h. Um der für den SnapDrive-Root-Benutzer oder den Administrator erstellten Rolle RBAC-Funktionen hinzuzufügen, geben Sie die folgenden Befehle ein:

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. Geben Sie den folgenden Befehl ein, um den oracle-Zieldatenbank zur Liste der Administratoren im DataFabric Manager Server hinzuzufügen und die sd-Protect-Rolle zu zuweisen:

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

b. Geben Sie den folgenden Befehl ein, um das Storage-System hinzuzufügen, das von der Zieldatenbank im DataFabric Manager Server verwendet wird:

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

c. Geben Sie den folgenden Befehl ein, um eine neue Rolle in dem Storage-System zu erstellen, das von der Zieldatenbank auf dem DataFabric Manager-Server verwendet wird:

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

d. Geben Sie den folgenden Befehl ein, um eine neue Gruppe im Storage-System zu erstellen und die neue Rolle zuzuweisen, die im DataFabric Manager-Server erstellt wurde:

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

e. Geben Sie den folgenden Befehl ein, um einen neuen Benutzer im Storage-System zu erstellen und die neue Rolle und die im DataFabric Manager-Server erstellte Gruppe zuzuweisen:

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

2. Konfigurieren Sie SnapDrive.

a. So registrieren Sie die Anmeldeinformationen des `sd-admin` Benutzer mit SnapDrive, geben Sie den folgenden Befehl ein:

snapdrive config set -dfm *sd-admindfm_host*

b. Geben Sie den folgenden Befehl ein, um den Root-Benutzer oder den Administrator des

Speichersystems mit SnapDrive zu registrieren:

```
snapdrive config set tardb_host1storage_system
```

Konfigurieren Sie SnapDrive, wenn die rollenbasierte Zugriffssteuerung nicht aktiviert ist

Sie müssen den Root-Benutzer oder den Administrator des DataFabric Manager Servers und den Root-Benutzer des Storage-Systems mit SnapDrive registrieren, um die Datensicherung zu ermöglichen.

Schritte

1. Geben Sie den folgenden Befehl ein, um den DataFabric Manager-Server zu aktualisieren, um die Änderungen direkt auf dem Storage-System durch die Zieldatenbank zu aktualisieren:

   Beispiel

   ```
   dfm host discover storage_system
   ```

2. Geben Sie den folgenden Befehl ein, um den Root-Benutzer oder den Administrator des DataFabric Manager Servers mit SnapDrive zu registrieren:

   Beispiel

   ```
   snapdrive config set -dfm Administratordfm_host
   ```

3. Geben Sie den folgenden Befehl ein, um den Root-Benutzer oder den Administrator des Speichersystems mit SnapDrive zu registrieren:

   Beispiel

   ```
   snapdrive config set root storage_system
   ```

Allgemeines zum Aktivieren oder Deaktivieren von Datenschutz in Profil

Sie können den Datenschutz beim Erstellen oder Aktualisieren eines Datenbankprofils aktivieren oder deaktivieren.

Um ein geschütztes Backup einer Datenbank auf den sekundären Speicherressourcen zu erstellen, führen Datenbank- und Storage-Administratoren folgende Aktionen durch.

Ihr Ziel ist	Dann…
Erstellen oder bearbeiten Sie ein Profil	So erstellen oder bearbeiten Sie ein Profil: • Backup-Sicherung für den sekundären Storage • Wenn Sie Data ONTAP 7-Mode verwenden und Protection Manager installiert haben, können Sie die Richtlinien auswählen, die vom Storage- oder Backup-Administrator in Protection Manager erstellt wurden. Wenn Sie Data ONTAP in 7-Mode verwenden und der Schutz aktiviert ist, erstellt SnapManager einen Datensatz für die Datenbank. Ein Datenset besteht aus einer Sammlung von Storage Sets und Konfigurationsinformationen, die ihren Daten zugeordnet sind. Zu den mit einem Datensatz verknüpften Speichersätzen zählen ein primärer Speichersatz für den Export von Daten auf Clients sowie der Satz an Replikaten und Archiven, die sich auf anderen Speichergruppen befinden. Datensätze stellen exportierbare Anwenderdaten dar. Wenn der Administrator den Schutz für eine Datenbank deaktiviert, löscht SnapManager den Datensatz. • Wenn Sie ONTAP verwenden, müssen Sie je nach erstellten SnapMirror oder SnapVault Beziehung entweder die Richtlinie *SnapManager_cDOT_Mirror* oder *SnapManager_cDOT_Vault* auswählen. Wenn Sie den Sicherungsschutz deaktivieren, wird eine Warnmeldung angezeigt, die angibt, dass der Datensatz gelöscht wird und die Wiederherstellung oder das Klonen von Backups für dieses Profil nicht möglich ist.
Profil anzeigen	Da der Storage-Administrator noch keine Storage-Ressourcen zur Implementierung der Sicherungsrichtlinie zugewiesen hat, wird das Profil sowohl in der grafischen Benutzeroberfläche von SnapManager als auch im nicht formant angezeigt `profile show` Befehlsausgabe.
Weisen Sie Storage-Ressourcen in der Protection Manager Management Console zu	In der Protection Manager Management-Konsole zeigt der Storage-Administrator den ungeschützten Datensatz an und weist jedem Node des Datensatzes, der dem Profil zugeordnet ist, einen Ressourcen-Pool zu. Der Storage-Administrator stellt dann sicher, dass sekundäre Volumes bereitgestellt und Sicherungsbeziehungen initialisiert werden.
Sehen Sie sich das entsprechende Profil in SnapManager an	In SnapManager erkennt der Datenbankadministrator, dass sich das Profil sowohl in der grafischen Benutzeroberfläche als auch in der in den Status „formant“ geändert hat `profile show` Befehlsausgabe zeigt an, dass Ressourcen zugewiesen wurden.

Ihr Ziel ist	Dann…
Erstellen Sie das Backup	• Wählen Sie das vollständige Backup aus. • Wählen Sie außerdem aus, ob das Backup geschützt werden soll, und wählen Sie die primäre Aufbewahrungsklasse (z. B. stündlich oder täglich) aus. • Wenn Sie Data ONTAP in 7-Mode verwenden und das Backup unmittelbar auf dem sekundären Storage schützen möchten, und den Protection Manager-Schutzzeitplan überschreiben, geben Sie den an `-protectnow` Option. • Wenn Sie ONTAP verwenden und das Backup sofort auf dem sekundären Storage sichern möchten, geben Sie den an `protect` Option. Der `protectnow` Eine Option ist in Clustered Data ONTAP nicht verfügbar.
Backup anzeigen	Das neue Backup wird als geplant für die Sicherung angezeigt, aber noch nicht geschützt (in der SnapManager Schnittstelle und in `backup show` Befehlsausgabe). Der Schutzstatus wird als „`not protected`“ angezeigt.
Zeigen Sie die Sicherungsliste an	Nachdem der Storage-Administrator überprüft hat, ob das Backup in den sekundären Speicher kopiert wurde, ändert SnapManager den Sicherungsstatus von „`not protected`“ in „`protected`“.