



Konfiguration und Aktivierung richtlinienbasierter Datensicherung

SnapManager Oracle

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/de-de/snapmanager-oracle/unix-administration/task_configuring_snapdrive_when_rbac_is_enabled.html on October 04, 2023. Always check docs.netapp.com for the latest.

Inhalt

- Konfiguration und Aktivierung richtlinienbasierter Datensicherung 1
 - Konfiguration des DataFabric Manager-Servers und des SnapDrive, wenn die RBAC aktiviert ist. 1
 - SnapDrive konfigurieren, wenn die RBAC nicht aktiviert ist. 2
 - Allgemeines zum Aktivieren oder Deaktivieren von Datenschutz in Profil. 2

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.

Konfiguration des DataFabric Manager-Servers und des 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.

1. Konfigurieren Sie den DataFabric Manager Server.
 - a. Um den DataFabric Manager-Server zu aktualisieren, um die Änderungen, die direkt auf dem Storage-System durch die Ziel-Datenbank vorgenommen wurden, zu aktualisieren, geben Sie den folgenden Befehl ein: `dfm Host discover Storage_System`
 - b. Erstellen Sie einen neuen Benutzer im DataFabric Manager-Server, und legen Sie das Passwort fest.
 - c. Geben Sie zum Hinzufügen des Betriebssystembenutzers zur DataFabric Manager Server-Administratorliste den folgenden Befehl ein: `dfm user add sd-admin`
 - d. Geben Sie zum Erstellen einer neuen Rolle im DataFabric Manager-Server den folgenden Befehl ein: `dfm Role create sd-admin-role`
 - e. Um die Funktion `DFM.Core.AccessCheck Global` zur Rolle hinzuzufügen, geben Sie den folgenden Befehl ein: `dfm-Rolle hinzufügen sd-admin-role DFM.Core.AccessCheck Global`
 - f. Geben Sie den folgenden Befehl ein, um dem Benutzer des Betriebssystems eine sd-Admin-Rolle hinzuzufügen: `dfm-Benutzerrolle 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 Rolle, die für den SnapDrive-Root-Benutzer oder den Administrator erstellt wurde, RBAC-Funktionen hinzuzufügen, geben Sie die folgenden Befehle ein: `dfm-Rolle hinzufügen sd-Protect SD.Config.Globaldfm lesen Rolle hinzufügen sd-protect SD.Config hinzufügen Globaldfm Rolle hinzufügen sd-Protect SD.Config.Globaldfm-Rolle löschen SD-Schutz hinzufügen SD.Database.Write Globaldfm-Rolle hinzufügen`
 - i. Um den oracle-Benutzer der Zieldatenbank zur Liste der Administratoren im DataFabric Manager Server hinzuzufügen und die sd-Protect-Rolle zu zuweisen, geben Sie den folgenden Befehl ein: `dfm user add -r sd-protecttardb_host1\oracle`
 - j. Geben Sie zum Hinzufügen des von der Zieldatenbank verwendeten Speichersystems im DataFabric Manager-Server den folgenden Befehl ein: `dfm Host set Storage_System hostLogin=oracle hostPassword=password`

- k. Geben Sie zum Erstellen einer neuen Rolle in dem Storage-System, das von der Zieldatenbank im DataFabric Manager-Server verwendet wird, den folgenden Befehl ein: `dfm Host Role create -h Storage_System-c „API-,Login-“ Storage-rbac-Role`
 - l. Geben Sie zum Erstellen einer neuen Gruppe im Speichersystem und Zuweisen der neuen Rolle, die im DataFabric Manager Server erstellt wurde, den folgenden Befehl ein: `dfm Host usergroup create -h Storage_System-r Storage-rbac-rolestorage-rbac-Group`
 - m. Um einen neuen Benutzer im Storage-System zu erstellen und die neue Rolle und die im DataFabric Manager Server erstellte Gruppe zuzuweisen, geben Sie den folgenden Befehl ein: `dfm Host user create -h Storage_System-r Storage-rbac-Role -p password -g Storage-rbac-grouptardb_host1`
2. Konfigurieren Sie SnapDrive.
- a. Geben Sie den folgenden Befehl ein, um die Anmeldedaten des sd-Admin-Benutzers mit SnapDrive zu registrieren: `snapdrive config set -dfm sd-admin dfm_Host`
 - b. Um den Root-Benutzer oder den Administrator des Speichersystems mit SnapDrive zu registrieren, geben Sie den folgenden Befehl ein: `snapdrive config set tardb_Host 1storage_System`

SnapDrive konfigurieren, wenn die RBAC 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.

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:

`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:

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


`SnapDrive-Konfiguration legt Root Storage_System fest`

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	<p>So erstellen oder bearbeiten Sie ein Profil:</p> <ul style="list-style-type: none"> • 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. <p>Wenn Sie Data ONTAP in 7-Mode verwenden und der Schutz aktiviert ist, erstellt SnapManager einen Datensatz für die Datenbank. Ein Datensatz 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.</p> <ul style="list-style-type: none"> • Wenn Sie ONTAP verwenden, müssen Sie je nach erstellten SnapMirror oder SnapVault Beziehung entweder die Richtlinie <i>SnapManager_cDOT_Mirror</i> oder <i>SnapManager_cDOT_Vault</i> auswählen. <p>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.</p>
Profil anzeigen	<p>Da der Storage-Administrator noch keine Storage-Ressourcen zur Implementierung der Sicherungsrichtlinie zugewiesen hat, wird das Profil sowohl in der grafischen SnapManager Benutzeroberfläche als auch in der Ausgabe des Profils als nicht konform angezeigt.</p>
Weisen Sie Storage-Ressourcen in der Protection Manager Management Console zu	<p>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.</p>

Ihr Ziel ist	Dann...
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 Befehlsausgabe des Profils in den Status „formant“ geändert hat, was bedeutet, dass Ressourcen zugewiesen wurden.
Erstellen Sie das Backup	<ul style="list-style-type: none"> • 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 sofort auf sekundärem Storage schützen möchten, der den Protection Manager-Schutzzeitplan überwählt, geben Sie die Option -protectnow an. • Wenn Sie ONTAP verwenden und das Backup sofort auf dem sekundären Storage schützen möchten, geben Sie die Option „Schutz“ an. <div data-bbox="898 934 951 989">  </div> <div data-bbox="1015 913 1372 1014"> <p>Die Option zum Schutz ist in Clustered Data ONTAP nicht verfügbar.</p> </div>
Backup anzeigen	Das neue Backup wird als geplant für den Schutz angezeigt, aber noch nicht geschützt (in der SnapManager-Schnittstelle und in der Ausgabe des Backup show-Befehls). 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“.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.