



Die rollenbasierte Zugriffssteuerung

SnapManager for SAP

NetApp
April 19, 2024

Inhalt

Die rollenbasierte Zugriffssteuerung	1
Rollenbasierte Zugriffssteuerung	2
Legen Sie Funktionen und Rollen für die rollenbasierte Zugriffssteuerung fest	2

Die rollenbasierte Zugriffssteuerung

Dank der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) können Sie kontrollieren, wer Zugriff auf den SnapManager Betrieb hat. Über die rollenbasierte Zugriffssteuerung können Administratoren Benutzergruppen managen, indem sie Rollen festlegen und Benutzern diese Rollen zuweisen. Nutzen Sie die SnapManager RBAC-Funktionen auch in Umgebungen, in denen die RBAC bereits vorhanden ist.

RBAC bietet die folgenden Komponenten:

- Ressourcen: Volumes und LUNs, die die Datendateien enthalten, die Ihre Datenbank ausmachen.
- Fähigkeiten: Arten von Operationen, die an einer Ressource durchgeführt werden können.
- Benutzer: Personen, denen Sie Fähigkeiten gewähren.
- Rollen: Eine Reihe von Ressourcen und Funktionen, die für Ressourcen zulässig sind. Sie weisen einem Benutzer eine bestimmte Rolle zu, der diese Funktionen ausführen soll.

Sie aktivieren die RBAC in SnapDrive. Anschließend können Sie in der grafischen Benutzeroberfläche des Operations Manager Web oder der Befehlszeilenschnittstelle bestimmte Funktionen pro Rolle konfigurieren. RBAC-Überprüfungen erfolgen auf dem DataFabric Manager Server.

In der folgenden Tabelle werden einige Rollen und ihre typischen Aufgaben aufgeführt, die in Operations Manager festgelegt sind.

Rolle	Typische Aufgaben
SAP-Basis Administrator	<ul style="list-style-type: none">• Erstellen, Warten und Überwachen einer Oracle-Datenbank, die sich auf einem Host befindet• Datenbank-Backups planen und erstellen• Sicherstellen, dass Backups gültig sind und wiederhergestellt werden können• Datenbanken klonen
Server-Administrator	<ul style="list-style-type: none">• Einrichtung von Storage-Systemen und Aggregaten• Monitoring von Volumes für freien Speicherplatz• Bereitstellung von Storage auf Anfragen von Benutzern• Konfiguration und Monitoring von Disaster Recovery Mirroring
Storage-Architekt	<ul style="list-style-type: none">• Treffen von Architekturentscheidungen beim Storage• Planung des Wachstums der Storage-Kapazität• Planung von Disaster-Recovery-Strategien• Delegieren von Fähigkeiten an Teammitglieder

Wenn RBAC verwendet wird (d. h., Operations Manager wird installiert und RBAC in SnapDrive aktiviert ist), muss der Storage-Administrator RBAC-Berechtigungen für alle Volumes und Storage-Systeme für die Datenbankdateien zuweisen.

Rollenbasierte Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapManager wird mithilfe von SnapDrive aktiviert. Bei der Installation von SnapDrive ist die RBAC standardmäßig deaktiviert. Nachdem Sie die RBAC in SnapDrive aktiviert haben, führt SnapManager dann alle Vorgänge mit aktivierter rollenbasierter Zugriffssteuerung durch.

Über diese Aufgabe

Der `snapdrive.config` File in SnapDrive bietet viele Optionen, von denen eine die RBAC unterstützt.

Die SnapDrive-Dokumentation enthält Details zum SnapDrive.

Schritte

1. Öffnen Sie das `snapdrive.conf` Datei in einem Editor.
2. RBAC wird im Wert der Cloud ermöglicht `rbac-method` Parameter von **native** Bis **dfm**.

Der Standardwert für diesen Parameter ist **native**, Die RBAC deaktiviert.

["Dokumentation auf der NetApp Support Site"](#)

Legen Sie Funktionen und Rollen für die rollenbasierte Zugriffssteuerung fest

Nachdem Sie die rollenbasierte Zugriffssteuerung (RBAC) für SnapManager über SnapDrive aktiviert haben, können Sie Funktionen für rollenbasierte Zugriffssteuerung und Benutzer zu Rollen hinzufügen, um SnapManager Vorgänge durchzuführen.

Was Sie brauchen

Sie müssen eine Gruppe im Data Fabric Manager Server erstellen und die Gruppe sowohl dem primären als auch dem sekundären Storage hinzufügen. Führen Sie folgende Befehle aus:

- `dfm group create smsap_grp`
- `dfm group add smsap_grpprimary_storage_system`
- `dfm group add smsap_grpsecondary_storage_system`

Über diese Aufgabe

Damit können RBAC-Funktionen und -Rollen entweder über die Operations Manager Webschnittstelle oder die Befehlszeilenschnittstelle (CLI) des Data Fabric Manager Servers geändert werden.

In der Tabelle sind die RBAC-Funktionen aufgeführt, die für die Durchführung des SnapManager Betriebs erforderlich sind:

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Profilerstellen oder Profilaktualisierung	SD.Storage.Read (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz)
Profilschutz	DFM.Database.Write (smsap_grp) SD.Storage.Read (smsap_grp) SD.Config.Lesen (smsap_grp) SD.Config.Write (smsap_grp) SD.Config.Delete (smsap_grp) GlobalDataProtection	Keine
Backup erstellen	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Delete (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Write (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Delete (SMSAP_profile Datensatz)
Backup-Erstellung (mit DBVerify)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Write (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Delete (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz)
Backup-Erstellung (mit RMAN)	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Write (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Delete (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz)

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC- Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Backup Restore	SD.Storage.Read (smsap_grp) SD.Snapshot.Write (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Delete (smsap_grp) SD.Snapshot.Clone (smsap_grp) SD.Snapshot.Restore (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Write (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Delete (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz) SD.Snapshot.Restore (SMSAP_profile Datensatz)
Backup löschen	SD.Snapshot.Delete (smsap_grp)	SD.Snapshot.Delete (SMSAP_profile Datensatz)
Backup verifizieren	SD.Storage.Read (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz)
Backup-Montage	SD.Storage.Read (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz)
Backup nicht verfügbar	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile Datensatz)
Klon erstellen	SD.Storage.Read (smsap_grp) SD.Snapshot.Lesen (smsap_grp) SD.Snapshot.Clone (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz) SD.Snapshot.Read (SMSAP_profile Datensatz) SD.Snapshot.Clone (SMSAP_profile Datensatz)
Klon löschen	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile Datensatz)

SnapManager Betrieb	Wenn Datensicherung nicht aktiviert ist, sind RBAC-Funktionen erforderlich	RBAC-Funktionen sind bei aktivierter Datensicherung erforderlich
Aufteilung klonen	SD.Storage.Read (smsap_grp)	SD.Storage.Read (SMSAP_profile Datensatz)
	SD.Snapshot.Lesen (smsap_grp)	SD.Snapshot.Read (SMSAP_profile Datensatz)
	SD.Snapshot.Clone (smsap_grp)	SD.Snapshot.Clone (SMSAP_profile Datensatz)
	SD.Snapshot.Delete (smsap_grp)	SD.Snapshot.Delete (SMSAP_profile Datensatz)
	SD.Storage.Write (smsap_grp)	SD.Storage.Write (SMSAP_profile Datensatz)

Details zum Definieren der RBAC-Funktionen finden Sie im *OnCommand Unified Manager Operations Manager Administration Guide*.

Schritte

1. Zugriff auf die Operations Manager Konsole.
2. Wählen Sie im Menü Setup die Option **Rollen** aus.
3. Wählen Sie eine vorhandene Rolle aus, oder erstellen Sie eine neue Rolle.
4. Um den Datenbank-Speicherressourcen Vorgänge zuzuweisen, klicken Sie auf **Funktionen hinzufügen**.
5. Klicken Sie auf der Seite Rolleneinstellungen bearbeiten, um Ihre Änderungen an der Rolle zu speichern, auf **Aktualisieren**.

Verwandte Informationen

["OnCommand Unified Manager Operations Manager – Administratorhandbuch"](#)

Copyright-Informationen

Copyright © 2024 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.