Rollenbasierte Zugriffssteuerung in SnapDrive für UNIX

Snapdrive for Unix

NetApp
June 20, 2025

Inhalt

Rollenbasierte Zugriffssteuerung in SnapDrive für UNIX . . . 1
- Welche rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) bietet SnapDrive für UNIX . . . 1
- Interaktion von SnapDrive für UNIX und der Operations Manager Konsole . . . 2
- Konfiguration der rollenbasierten Zugriffssteuerung in SnapDrive für UNIX . . . 3
  - konfigurieren von sd-Admin in der Operations Manager-Konsole . . . 3
  - hinzufügen von sd-Hostname zum Speichersystem . . . 4
  - Konfigurieren von Benutzeranmeldeinformationen auf SnapDrive für UNIX . . . 6
  - Formate für Benutzernamen zur Durchführung von Zugriffsprüfungen mithilfe der Operations Manager Konsole . . . 7
  - Konfigurationsvariablen für die rollenbasierte Zugriffssteuerung . . . 7
- SnapDrive-Befehle und -Funktionen . . . 8
- Vorkonfigurierte Rollen zur einfachen Konfiguration von Benutzerrollen . . . 12
- Automatische Aktualisierung des Storage-Systems auf der Operations Manager Konsole . . . 12
- Mehrere Operations Manager Konsolen-Server . . . 13
- Operations Manager-Konsole nicht verfügbar . . . 14
- Beispiele für RBAC und Storage-Vorgänge . . . 14
  - Vorgang mit einem einzigen Dateisystem auf einem einzigen Storage-Objekt . . . 14
  - Betrieb mit einem einzigen Dateisystem auf mehreren Speicherobjekten . . . 15
  - Betrieb mit mehreren Dateiepec- und Speicherobjekten . . . 15
  - Betrieb mit mehreren Storage-Objekten . . . 16
  - Betrieb mit mehreren Operations Manager Konsolen-Servern, die Storage-Systeme managen . . . 17

Rollenbasierte Zugriffssteuerung in SnapDrive für UNIX

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) wird für die Anmeldung bei Benutzern und für Rollenberechtigungen verwendet. RBAC bietet Administratoren die Möglichkeit, Benutzergruppen zu managen, indem sie Rollen definieren. Wenn Sie den Zugriff auf die Datenbank auf bestimmte Administratoren beschränken müssen, müssen Sie Administratorkonten für sie einrichten. Außerdem müssen Sie Rollen auf die von Ihnen erstellten Administratorkonten anwenden, wenn Sie die Informationen einschränken möchten, können diese Administratoren anzeigen und die Vorgänge, die sie ausführen können, anzeigen.

RBAC wird in SnapDrive für UNIX mithilfe der Operations Manager Konsole verwendet. Operations Manager Konsole ermöglicht den granularen Zugriff auf Storage-Objekte, beispielsweise LUNs, qtrees, Volumes, Aggregate und vFiler Einheiten.

Verwandte Informationen

Obligatorische Überprüfungen für Volume-basierte SnapRestore

Wiederherstellen von Snapshot Kopien auf einem Ziel-Storage-System

Vorgehensweise zum Abtrennen von Schnappverbindungen

Welche rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) bietet SnapDrive für UNIX

RBAC ermöglicht SnapDrive Administratoren den Zugriff auf verschiedene SnapDrive Vorgänge auf ein Storage-System zu beschränken. Dieser begrenzte oder vollständige Zugriff auf Storage-Vorgänge hängt von der Rolle ab, die dem Benutzer zugewiesen ist.

SnapDrive 4.0 für UNIX und höher erfordert eine RBAC-Zugriffsprüfung für alle Vorgänge von SnapDrive für UNIX. So können Storage-Administratoren Abläufe einschränken, die SnapDrive Benutzer je nach zugewiesenen Rollen ausführen können. RBAC wird über die Operations Manager Infrastruktur implementiert. In älteren Versionen als SnapDrive 4.0 für UNIX gab es eine begrenzte Zugriffskontrolle und nur der Root-Benutzer konnte SnapDrive für UNIX-Vorgänge ausführen. SnapDrive 4.0 für UNIX und höher unterstützt Benutzer von lokalen Benutzern ohne Root-Benutzer und NIS (Network Information System) mithilfe der RBAC-Infrastruktur der Operations Manager Konsole. SnapDrive für UNIX erfordert kein Root-Passwort des Storage-Systems. Es kommuniziert mit dem Speichersystem über sd-<hostname> user.

Standardmäßig wird die RBAC-Funktion der Operations Manager Konsole nicht verwendet. Sie müssen die RBAC-Funktionen aktivieren, indem Sie die Variable einstellen *`rbac-method=dfm`* Im `snapdrive.conf` Datei und starten Sie den SnapDrive for UNIX Daemon neu.

Die folgenden Anforderungen müssen erfüllt sein, bevor Sie diese Funktion nutzen können:

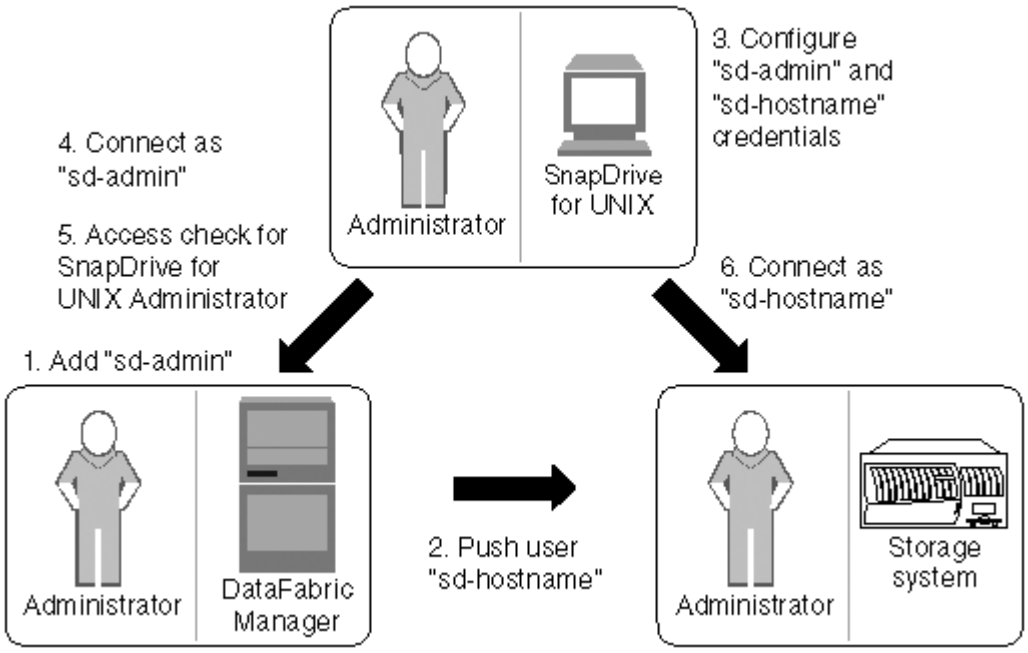
- Operations Manager Konsole 3.7 oder höher.
- Der Operations Manager Konsolen-Server muss im IP-Netzwerk, das die SnapDrive Hosts und Storage-Systeme enthält, vorhanden und konfiguriert sein.

- Die Kommunikationseinstellungen der Operations Manager-Konsole müssen während der SnapDrive-Installation konfiguriert sein.
- SnapDrive for UNIX Daemon sollte ausgeführt werden.

Interaktion von SnapDrive für UNIX und der Operations Manager Konsole

Die Nutzung rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) hängt von der Operations Manager Konsoleninfrastruktur ab. Der Administrator der Operations Manager-Konsole muss Benutzernamen für SnapDrive für die Verwendung von UNIX erstellen. Alle Storage-Betriebsanfragen werden zuerst an die Operations Manager Konsole gesendet, um eine Zugriffsprüfung zu ermöglichen. Nachdem die Operations Manager Konsole einen Storage-Vorgang von einem bestimmten SnapDrive Benutzer überprüft hat, wird der Vorgang abgeschlossen.

Im folgenden Diagramm sind die gesamten RBAC-Funktionen für Storage-Vorgänge dargestellt.



1. Operations Manager-Konsolenadministrator fügt sd-Admin-Benutzer auf der Operations Manager-Konsole hinzu.
2. Operations Manager Console Administrator erstellt sd-Hostname-Benutzer auf dem Speichersystem.
3. Der Administrator der Operations Manager-Konsole sendet Anmeldeinformationen für sd-Admin und sd-Hostname an SnapDrive für UNIX-Administratoren.
4. Der SnapDrive-Administrator konfiguriert SnapDrive mit den erhaltenen Benutzeranmeldeinformationen.
5. Die Operations Manager-Konsole führt eine Zugriffsprüfung für SnapDrive für UNIX mithilfe der vom SnapDrive-Administrator hinzugefügten Benutzeranmeldeinformationen durch.
6. Nach der Authentifizierung des SnapDrive-Benutzers kann der Benutzer eine Verbindung zum Speichersystem herstellen.

Wenn ein SnapDrive-Benutzer einige Speicheroperationen durchführen möchte, gibt der Benutzer den entsprechenden Befehl an der Kommandozeile aus. Die Anforderung wird an die Operations Manager Konsole gesendet, um eine Zugriffsprüfung zu ermöglichen. Die Operations Manager-Konsole überprüft, ob der angeforderte Benutzer über die entsprechenden Berechtigungen zum Durchführen des SnapDrive-Vorgangs verfügt. Das Ergebnis der Zugriffsüberprüfung wird an SnapDrive zurückgegeben. Je nach Ergebnis darf der Benutzer die Speichervorgänge auf dem Storage-System ausführen.

Wenn der Benutzer nach der Zugriffsprüfung verifiziert wird, stellt der Benutzer eine Verbindung zum Speichersystem als sd-Hostname her.

sd-Hostname und sd-Admin sind die empfohlenen Benutzernamen. Sie können SnapDrive für UNIX mit anderen Benutzernamen konfigurieren.

Konfiguration der rollenbasierten Zugriffssteuerung in SnapDrive für UNIX

Zum Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) für SnapDrive für UNIX müssen Sie verschiedene Aufgaben ausführen. Für die Ausführung der Aufgaben können Sie entweder die Operations Manager-Konsole oder die Befehlszeilenschnittstelle verwenden.

konfigurieren von sd-Admin in der Operations Manager-Konsole

Der Administrator der Operations Manager-Konsole kann den sd-Admin-Benutzer erstellen.

Der Administrator der Operations Manager-Konsole erstellt einen Benutzer namens sd-admin, der in der Lage ist, eine zentrale Zugriffsüberprüfung der globalen Gruppe (global) durchzuführen `DFM.Core.AccessCheck`). Nachdem der Administrator der Operations Manager-Konsole den sd-Admin-Benutzer konfiguriert hat, müssen Sie die Anmeldeinformationen manuell an den SnapDrive für UNIX-Administrator senden. Weitere Informationen über die Verwendung der Operations Manager-Konsole zum Konfigurieren von Benutzern und Rollen finden Sie im Administrationshandbuch *Operations Manager Console* und in der Online-Hilfe.

Sie können einen beliebigen Namen anstelle von sd-admin verwenden; es ist jedoch am besten sd-Admin zu verwenden.

Um eine Rolle in der Operations Manager-Konsole zu erstellen, wählen Sie **Setup** > **Rollen**. Auf der seite sd-Admin-Konfiguration muss der Operations Manager-Konsolenadministrator zugewiesen werden `DFM.Database.Write` Funktion auf der globalen Gruppe zur sd-Admin-Rolle, sodass SnapDrive für UNIX Storage-Einheiten in der Operations Manager-Konsole aktualisieren kann.

konfigurieren von sd-Admin über Befehlszeilenschnittstelle

Der Administrator des Speichersystems kann den sd-Admin-Benutzer über die Befehlszeilenschnittstelle konfigurieren.

Schritte

1. Fügen Sie einen Benutzer namens sd-admin hinzu.

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. Fügen Sie einen Administrator namens sd-admin hinzu.

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. Erstellen Sie eine Rolle namens sd-admin-Rolle.

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. Fügen Sie der in Schritt 3 erstellten Rolle eine Funktion hinzu.

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. Der Operations Manager-Administrator kann ebenfalls erteilen `DFM.Database.Write` Fähigkeit auf der globalen Gruppe zu `<sd-admin>` So aktivieren Sie SnapDrive für UNIX, um die Speichersystemeinheiten im Operations Manager zu aktualisieren.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. Fügen Sie dem sd-Admin-Benutzer eine sd-Admin-Rolle hinzu.

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

hinzufügen von sd-Hostname zum Speichersystem

Der Operations Manager-Konsolenadministrator kann den sd-Hostname-Benutzer auf dem Speichersystem mithilfe der Operations Manager-Konsole erstellen. Nach Abschluss

der Schritte muss der Operations Manager-Konsolenadministrator die Anmeldeinformationen manuell an den SnapDrive für UNIX-Administrator senden. Sie können jeden Namen anstelle von sd-Hostname verwenden; jedoch ist es am besten, sd-Hostname zu verwenden.

Schritte

1. Ermitteln Sie das Root-Passwort des Speichersystems und speichern Sie das Passwort.

   Um das Passwort für das Speichersystem hinzuzufügen, wählen Sie **Management** > **Speichersystem**.

2. Erstellen Sie einen sd-Hostname-Benutzer für jedes UNIX-System.
3. Zuweisen von Funktionen `api- Und login-` Auf eine Rolle, z. B. sd-Rolle.
4. Diese Rolle (sd-Rolle) in eine neue Benutzergruppe, z. B. sd-Benutzergruppe, aufnehmen.
5. Verknüpfen Sie diese Benutzergruppe (sd-usergroup) mit dem sd-Hostname-Benutzer auf dem Speichersystem.

hinzufügen von sd- Hostname zum Speichersystem mithilfe von CLI

Der Administrator des Speichersystems kann den sd-Hostname-Benutzer mit dem Benutzer-Admin-Befehl erstellen und konfigurieren.

Schritte

1. Erweitern Sie Ihren Storage.

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

2. Legen Sie das Passwort für den Host fest.

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

3. Erstellen Sie eine Rolle auf dem Host.

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

4. Erstellen Sie eine Benutzergruppe.

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

5. Erstellen Sie einen lokalen Benutzer.

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

Konfigurieren von Benutzeranmeldeinformationen auf SnapDrive für UNIX

Der SnapDrive für UNIX Administrator erhält vom Operations Manager Console Administrator Benutzeranmeldeinformationen. Diese Benutzerkennungen müssen auf SnapDrive für UNIX konfiguriert werden, damit sie ordnungsgemäß durchgeführt werden können.

Schritte

1. konfigurieren sie sd-Admin auf dem Speichersystem.

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

2. konfigurieren sie den sd-Hostnamen auf dem Speichersystem.

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. Überprüfen Sie Schritt 1 und Schritt 2 mit dem `snapdrive config list` Befehl.

```
user name       appliance name          appliance type
----------------------------------------------------
sd-admin        ops_mngr_server         DFM
sd-unix_host    storage_array1          StorageSystem
```

4. Konfiguration von SnapDrive für UNIX zur Nutzung der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) der Operations Manager Konsole durch Festlegen der Konfigurationsvariable `rbac-method="dfm"` Im `snapdrive.conf` Datei:

Die Benutzeranmeldeinformationen werden verschlüsselt und in der vorhandenen gespeichert `.sdupw` Datei: Der Standardspeicherort der früheren Datei ist `/opt/NetApp/snapdrive/.sdupw`.

Formate für Benutzernamen zur Durchführung von Zugriffsprüfungen mithilfe der Operations Manager Konsole

SnapDrive für UNIX verwendet die Benutzernamenformate zur Durchführung von Zugriffsprüfungen über die Operations Manager Konsole. Diese Formate hängen davon ab, ob Sie ein Network Information System (NIS) oder ein lokaler Benutzer sind.

SnapDrive für UNIX verwendet die folgenden Formate, um zu prüfen, ob ein Benutzer zur Ausführung bestimmter Aufgaben berechtigt ist:

- Wenn Sie ein NIS-Benutzer sind, der das ausführt `snapdrive` Befehl, SnapDrive für UNIX verwendet das Format `<nisdomain>\<username>` (Beispiel: `netapp.com\marc`)
- Wenn Sie ein lokaler Benutzer eines UNIX-Hosts wie lnx197-141 sind, verwendet SnapDrive für UNIX das Format `<hostname>\<username>` Format (z. B. `lnx197-141\john`)
- Wenn Sie ein Administrator (Root) eines UNIX Hosts sind, behandelt SnapDrive für UNIX den Administrator immer als lokalen Benutzer und verwendet das Format `lnx197-141\root`.

Konfigurationsvariablen für die rollenbasierte Zugriffssteuerung

Sie müssen die verschiedenen Konfigurationsvariablen für die rollenbasierte Zugriffssteuerung im festlegen `snapdrive.conf` Datei:

Variabel	Beschreibung
contact-http-dfm-port = 8088	Gibt den HTTP-Port an, der für die Kommunikation mit einem Operations Manager-Konsolen-Server verwendet werden soll. Der Standardwert ist 8088.
contact-ssl-dfm-port = 8488	Gibt den SSL-Port an, der für die Kommunikation mit einem Operations Manager-Konsolen-Server verwendet werden soll. Der Standardwert ist 8488.
rbac-method=dfm	Gibt die Methoden der Zugriffskontrolle an. Die möglichen Werte sind `native` Und `dfm`. Wenn der Wert ist `native`, Die in gespeicherte Zugriffskontrolldatei `/vol/vol0/sdprbac/sdhost-name.prbac` Wird für Zugriffskontrollen verwendet. Wenn der Wert auf festgelegt ist `dfm`, Operations Manager Konsole ist eine Voraussetzung. In diesem Fall sendet SnapDrive für UNIX Zugriffsprüfungen an die Operations Manager Konsole.

Variabel	Beschreibung
rbac-cache=on	SnapDrive für UNIX verwaltet eine Cache-Kopie von Zugriffsüberprüfung-Abfragen und den entsprechenden Ergebnissen. SnapDrive für UNIX verwendet diesen Cache nur, wenn alle konfigurierten Operations Manager-Konsolenserver ausgefallen sind. Sie können diesen Wert entweder auf einstellen `on` Um den Cache zu aktivieren, oder auf `off` Um sie zu deaktivieren. Der Standardwert ist aus, sodass Sie SnapDrive für UNIX so konfigurieren können, dass die Operations Manager Konsole verwendet und die festgelegt wird `rbac-method` Konfigurationsvariable auf `dfm`.
rbac-cache-timeout	Gibt den sperrzeitraum für den rbac-Cache an. Er gilt nur, wenn der *`rbac-cache`* Ist aktiviert. Der Standardwert ist `24` Std. SnapDrive für UNIX verwendet diesen Cache nur, wenn alle konfigurierten Operations Manager-Konsolenserver ausgefallen sind.
use-https-to-dfm=on	Mit dieser Variable können Sie festlegen, dass SnapDrive für UNIX bei der Kommunikation mit der Operations Manager-Konsole die SSL-Verschlüsselung (HTTPS) verwendet. Der Standardwert ist `on`.

SnapDrive-Befehle und -Funktionen

Bei der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) muss jeder Vorgang erfolgreich sein. Ein Benutzer muss über die korrekten Funktionen verfügen, die zur Durchführung von Storage-Vorgängen zugewiesen sind.

In der folgenden Tabelle sind die Befehle und die entsprechenden erforderlichen Funktionen aufgeführt:

Befehl	Dar
`storage show`	SD.Storage.Lesen auf Volume
`storage list`	SD.Storage.Lesen auf Volume

Befehl	Dar
`storage create`	• Für LUNs in Volumes: `SD.Storage.Write` Auf Lautstärke • Für LUNs in qtrees: `SD.Storage.Write` Auf qtree
`storage resize`	`SD.Storage.Write` Auf LUN
`storage delete`	`SD.Storage.Delete` Auf LUN
`snap show`	`SD.SnapShot.Read` Auf Lautstärke
`snap list`	`SD.SnapShot.Read` Auf Lautstärke
`snap delete`	`SD.Storage.Delete` Auf Lautstärke
`snap rename`	`SD.Storage.Write` Auf Lautstärke
`snap connect`	• Für LUN-Klone im Volume: `SD.SnapShot.Clone` Auf Lautstärke • Für LUN-Klone in qtree: `SD.SnapShot.Clone` Auf qtree • Für herkömmliches Volume-Klonen: `SD.SnapShot.Clone` Auf dem Storage-System • Für FlexClone Volume: `SD.SnapShot.Clone` Auf dem übergeordneten Volume • Für uneingeschränkte FlexClone Volumes: `SD.SnapShot.UnrestrictedClone` Auf dem übergeordneten Volume
`snap connect-split`	• Für LUN Clones (LUN geklont und im Volume aufgeteilt): `SD.SnapShot.Clone` Auf Volume und `SD.Storage.Write` Auf Lautstärke • Für LUN Clones (LUN geklont und aufgeteilt in qtree): `SD.SnapShot.Clone` Auf qtree und `SD.Storage.Write` Auf qtree • Für herkömmliche geteilte Volume-Klone: `SD.SnapShot.Clone` Auf dem Storage-System und `SD.Storage.Write` Auf dem Storage-System • Für geteilte Flex Volume-Klone: `SD.SnapShot.Clone` Auf dem übergeordneten Volume.

Befehl	Dar
`clone split start`	• Bei LUN-Klonen, auf denen sich das LUN im Volume oder qtree befindet: `SD.SnapShot.Clone` Mit Volume oder qtree • Bei Volume-Klonen: `SD.SnapShot.Clone` Auf dem übergeordneten Volume
`snap disconnect`	• Bei LUN-Klonen, auf denen sich das LUN im Volume oder qtree befindet: `SD.SnapShot.Clone` Mit Volume oder qtree • Bei Volume-Klonen: `SD.SnapShot.Clone` Auf dem übergeordneten Volume • Zum Löschen von unbeschränkten Volume-Klonen: `SD.SnapShot.DestroyUnrestrictedClone` Auf dem Volume
`snap disconnect-split`	• Bei LUN-Klonen, auf denen sich das LUN im Volume oder qtree befindet: `SD.SnapShot.Clone` Auf dem enthaltenden Volume oder qtree • Bei Volume-Klonen: `SD.Storage.Delete` Auf dem übergeordneten Volume • Zum Löschen von unbeschränkten Volume-Klonen: `SD.SnapShot.DestroyUnrestrictedClone` Auf dem Volume

Befehl	Dar
`snap restore`	• Für LUNs, die in einem Volume vorhanden sind: `SD.SnapShot.Restore` Auf Volume und `SD.Storage.Write` Auf LUN • Für LUNs, die in einem qtree vorhanden sind: `SD.SnapShot.Restore` Auf qtree und `SD.Storage.Write` Auf LUN • Für LUNs, die nicht in den Volumes sind: `SD.SnapShot.Restore` Auf Volume und `SD.Storage.Write` Auf Lautstärke • Für LUNs, die nicht im qtree sind: `SD.SnapShot.Restore` Auf qtree und `SD.Storage.Write` Auf qtree • Für Volumes: `SD.SnapShot.Restore` Auf einem Storage-System für herkömmliche Volumes oder `SD.SnapShot.Restore` Auf Aggregat für flexible Volumes • Für Snap Restore in Volumes mit einer Datei: `SD.SnapShot.Restore` Auf dem Volume • Für Snap Restore mit einer Datei in qtree: `SD.SnapShot.Restore` Qtree • Für die Überschreiben von Snapshot Kopien: `SD.SnapShot.DisruptBaseline` Auf dem Volume
`host connect`, `host disconnect`	`SD.Config.Write` Auf der LUN
`config access`	`SD.Config.Read` Auf dem Storage-System
`config prepare`	`SD.Config.Write` Auf mindestens einem Storage-System
`config check`	`SD.Config.Read` Auf mindestens einem Storage-System
`config show`	`SD.Config.Read` Auf mindestens einem Storage-System
`config set`	`SD.Config.Write` Auf dem Storage-System
`config set -dfm`, `config set -mgmtpath`,	`SD.Config.Write` Auf mindestens einem Storage-System
`config delete`	`SD.Config.Delete` Auf dem Storage-System

Befehl	Dar
`config delete dfm_appliance, config delete -mgmtpath`	`SD.Config.Delete` Auf mindestens einem Storage-System
`config list`	`SD.Config.Read` Auf mindestens einem Storage-System
`config migrate set`	`SD.Config.Write` Auf mindestens einem Storage-System
`config migrate delete`	`SD.Config.Delete` Auf mindestens einem Storage-System
`config migrate list`	`SD.Config.Read` Auf mindestens einem Storage-System

SnapDrive für UNIX prüft keine Funktionen für Administrator (Root).

Vorkonfigurierte Rollen zur einfachen Konfiguration von Benutzerrollen

Vorkonfigurierte Rollen vereinfachen die Zuweisung von Rollen zu Benutzern.

In der folgenden Tabelle werden die vordefinierten Rollen aufgeführt:

Rollenname	Beschreibung
GlobalSDStorage	Storage-Management mit SnapDrive für UNIX
GlobalSDConfig	Managen Sie Konfigurationen mit SnapDrive für UNIX
GlobalSDSnapshot	Managen Sie Snapshot Kopien mit SnapDrive für UNIX
GlobalSDFullControl	Vollständige Verwendung von SnapDrive für UNIX

In der vorstehenden Tabelle bezieht sich Global auf alle Storage-Systeme, die von einer Operations Manager-Konsole gemanagt werden.

Automatische Aktualisierung des Storage-Systems auf der Operations Manager Konsole

Operations Manager erkennt die von Ihrem Netzwerk unterstützten Storage-Systeme. Er überwacht regelmäßig die Daten, die von den erkannten Storage-Systemen erfasst werden. Die Daten werden in einem festgelegten Intervall aktualisiert. Der Administrator

der Operations Manager-Konsole kann das Aktualisierungsintervall konfigurieren.

Das LUN-Monitoring-Intervall, das qtree Monitoring-Intervall und das vFiler Monitoring-Intervall sind wichtige Felder, die die Häufigkeit von LUN-, qtree- und vFiler-Updates bestimmen. Wenn beispielsweise eine neue LUN auf einem Storage-System erstellt wird, wird die neue LUN nicht unmittelbar auf der Konsole von Operations Manager aktualisiert. Aus diesem Grund schlägt die Operations Manager Konsole fehl und die Zugriffsprüfung, die für diese LUN zur Operations Manager-Konsole ausgestellt wurde. Um diese Situation zu vermeiden, können Sie das LUN-Überwachungsintervall nach Ihren Anforderungen ändern.

1. Wählen Sie in der Operations Manager-Konsole **Setup** > **Optionen**, um das Überwachungsintervall zu ändern.
2. Der Operations Manager Console Administrator kann die Operations Manager Konsole auch mit der Ausführung kräftig aktualisieren `dfm host discovery filername` In der Befehlszeilenschnittstelle.
3. Der Administrator der Operations Manager-Konsole kann ebenfalls erteilen `DFM.Database.Write` Funktion auf der globalen Gruppe zu sd-admin, um SnapDrive für UNIX zu aktivieren, um die Speichersystemeinheiten auf der Operations Manager-Konsole zu aktualisieren.

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

Mehrere Operations Manager Konsolen-Server

SnapDrive für UNIX unterstützt mehrere Operations Manager Konsolenserver. Diese Funktion ist erforderlich, wenn mehrere Speichersysteme von mehr als einem Operations Manager-Konsolenserver verwaltet werden. SnapDrive für UNIX kontaktiert die Operations Manager Konsolenserver in derselben Reihenfolge, in der die Operations Manager Konsolenserver in SnapDrive für UNIX konfiguriert sind. Sie können die ausführen `snapdrive config list` Befehl zum Abrufen der Konfigurationsreihenfolge.

Das folgende Beispiel zeigt die Ausgabe für mehrere Operations Manager Konsolenserver:

```
# snapdrive config list
username    appliance name     appliance type
--------------------------------------------
root        storage_array1     StorageSystem
root        storage_array2     StorageSystem
sd-admin    ops_mngr_server1   DFM
sd-admin    ops_mngr_server2   DFM
```

Im vorhergehenden Beispiel wird Storage_array1 über OPS_mngr_server1 verwaltet und Storage_array2 wird über OPS_mngr_server2 verwaltet. In diesem Beispiel wurde zuerst der SnapDrive für UNIX-Kontakt OPS_mngr_server1 verwendet. Wenn OPS_mngr_server1 den Zugriff nicht bestimmen kann, verwendet SnapDrive für UNIX-Kontakte OPS_mngr_server2.

SnapDrive für UNIX kontaktiert nur unter den folgenden Bedingungen die zweite Operations Manager-Konsole:

- Wenn die erste Operations Manager-Konsole den Zugriff nicht bestimmen kann. Dieser Fall kann eintreten, weil die erste Operations Manager Konsole das Storage-System nicht verwaltet.
- Wenn die erste Operations Manager-Konsole ausfällt.

Operations Manager-Konsole nicht verfügbar

SnapDrive für UNIX benötigt die Operations Manager Konsole zur Überprüfung der Zugriffsrechte. Der Operations Manager-Konsolen-Server ist manchmal aus verschiedenen Gründen nicht verfügbar.

Wenn die RBAC-Methode verwendet wird *rbac-method = dfm* Ist festgelegt, und Operations Manager-Konsole ist nicht verfügbar. SnapDrive für UNIX zeigt die folgende Fehlermeldung an:

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive für UNIX kann auch einen Cache der Ergebnisse der Benutzerzugriffsüberprüfung aufrechterhalten, die von der Operations Manager Konsole zurückgegeben werden. Dieser Cache ist 24 Stunden lang gültig und kann nicht konfiguriert werden. Wenn Operations Manager Konsole nicht verfügbar ist, verwendet SnapDrive für UNIX den Cache zur ZugriffsBestimmung. Dieser Cache wird nur verwendet, wenn alle konfigurierten Operations Manager-Konsolenserver nicht antworten.

Damit SnapDrive für UNIX den Cache für eine Zugriffsprüfung verwenden kann, müssen Sie den einschalten *rbac-cache* Die Konfigurationsvariable muss aktiviert sein, um den Cache der Zugriffsergebnisse zu erhalten. Der *rbac-cache* Die Konfigurationsvariable ist standardmäßig deaktiviert.

Um SnapDrive für UNIX zu verwenden, auch wenn Operations Manager-Konsole nicht verfügbar ist, muss der Server-Administrator die Methode der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) auf zurücksetzen *rbac-method = native* Im `snapdrive.conf` Datei: Nachdem Sie den geändert haben `snapdrive.conf` Datei. Sie müssen den SnapDrive for UNIX Daemon neu starten. Wenn *rbac-method = native* Ist festgelegt, kann nur der Root-Benutzer SnapDrive für UNIX verwenden.

Beispiele für RBAC und Storage-Vorgänge

Dank der rollenbasierten Zugriffssteuerung können Storage-Vorgänge abhängig von den Ihnen zugewiesenen Funktionen durchgeführt werden. Sie erhalten eine Fehlermeldung, wenn Sie nicht über die richtigen Funktionen für den Speichervorgang verfügen.

Vorgang mit einem einzigen Dateisystem auf einem einzigen Storage-Objekt

SnapDrive für UNIX zeigt eine Fehlermeldung an, wenn Sie kein autorisierter Benutzer sind, um einen Dateiepec auf einem bestimmten Volume zu erstellen.

Filepec: File-pec kann ein Dateisystem, ein Host-Volume, eine Datenträgergruppe oder ein LUN sein.

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

In diesem Beispiel ist John kein Root-Benutzer und ist nicht berechtigt, einen Dateisystem auf dem angegebenen Volume zu erstellen. John muss den Operations Manager-Konsolenadministrator bitten, zu gewähren `SD.Storage.Write` Zugriff auf das Volume `storage_array1:/vol/vol1`.

Betrieb mit einem einzigen Dateisystem auf mehreren Speicherobjekten

SnapDrive für UNIX zeigt eine Fehlermeldung an, wenn der Administrator nicht über die erforderliche Berechtigung für mehrere Speicherobjekte verfügt, um die Speichervorgänge auszuführen.

Filepec: FileSystem, Host Volume, Disk Group oder LUN kann beliebige andere sein

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2  -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mngr_server
```

In diesem Beispiel spannt die Dateiepec auf zwei Storage-System-Volumes auf: Vol1 und vol2. Der Administrator (root) von unix_Host hat nicht `SD.Storage.Write` Zugriff auf beide Volumes: Daher zeigt SnapDrive für UNIX eine Fehlermeldung für jedes Volume. Um mit fortzufahren `storage create`, Der Administrator (root) muss den Operations Manager-Konsolenadministrator bitten, zu gewähren `SD.Storage.Write` Zugriff auf beide Volumes.

Betrieb mit mehreren Dateiepec- und Speicherobjekten

Das folgende Beispiel zeigt die Fehlermeldung, die Sie erhalten würden, wenn Sie kein autorisierter Benutzer sind, um die bestimmte Operation auszuführen.

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

In diesem Beispiel befinden sich drei LUNs auf zwei Storage-System-Volumes: Vol1 und vol2. Benutzer Marc gehört zu nis_Domain und ist nicht berechtigt, filepec auf vol1 und vol2 zu erstellen. SnapDrive für UNIX zeigt die beiden Fehlermeldungen im vorhergehenden Beispiel an. Die Fehlermeldungen zeigen an, dass der Benutzer über eine Eingabe verfügen muss `SD.Storage.Write` Zugriff auf vol1 und vol2.

Betrieb mit mehreren Storage-Objekten

Das folgende Beispiel zeigt die Fehlermeldung, die Sie erhalten würden, wenn Sie kein autorisierter Benutzer sind, um die bestimmte Operation auszuführen.

```
[john]$ snapdrive storage show -all

Connected LUNs and devices:

device filename   adapter  path  size  proto  state  clone  lun path
backing Snapshot
---------------  -------  ----  ----  -----  -----  -----  --------
---------------
/dev/sdao            -     -     200m  iscsi  online  No
storage_array1:/vol/vol2/passlun1           -
/dev/sda1            -     -     200m  fcp    online  No
storage_array1:/vol/vol2/passlun2           -

Host devices and file systems:

dg: testfs1_SdDg                dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv       mount point: /mnt/testfs1
(persistent) fstype jfs2

device filename   adapter  path  size  proto  state   clone  lun path
backing Snapshot
---------------  -------  ----  ----  -----  -----   -----  --------
---------
/dev/sdn             -      P    108m  iscsi  online   No
storage_array1:/vol/vol2/testfs1_SdLun         -
/dev/sdn1             -      P    108m  fcp  online   No
storage_array1:/vol/vol2/testfs1_SdLun1         -

0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mngr_server
```

John ist berechtigt, Storage-Einheiten auf vol2, aber nicht auf vol1 aufzulisten. SnapDrive für UNIX zeigt Einheiten von vol1 an und zeigt eine Warnmeldung für vol2 an.

Für `storage list`, `storage show`, `snap list`, und `snap show` „Commands SnapDrive für UNIX“ zeigt eine Warnung anstelle von Fehlern an.

Betrieb mit mehreren Operations Manager Konsolen-Servern, die Storage-Systeme managen

Die folgende Ausgabe zeigt die Fehlermeldung, die Sie erhalten, wenn Storage-Systeme von mehreren Operations Manager-Konsole gemanagt werden.

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mngr_server1
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user
unix_host\root on Operations Manager server ops_mngr_server2
```

Storage_array1 wird über OPS_mngr_server1 verwaltet und Storage_array2 wird über OPS_mngr_Server2 verwaltet. Administrator von unix_Host ist nicht berechtigt, DatePecs auf Storage_array1 und Storage_array2 zu erstellen. Im vorhergehenden Beispiel zeigt SnapDrive für UNIX die Operations Manager-Konsole an, die zur Ermittlung des Zugriffs verwendet wird.