



# Erstellen Sie Rollen

## ONTAP Automation

NetApp  
April 21, 2024

This PDF was generated from [https://docs.netapp.com/de-de/ontap-automation/workflows/wf\\_rbac\\_role\\_limit\\_svm.html](https://docs.netapp.com/de-de/ontap-automation/workflows/wf_rbac_role_limit_svm.html) on April 21, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Erstellen Sie Rollen ..... 1
  - Beschränkung des Zugriffs auf SVM-Volume-Vorgänge ..... 1
  - Administration der Datensicherung ..... 3
  - Erstellung von ONTAP-Berichten zulassen ..... 4

# Erstellen Sie Rollen

## Beschränkung des Zugriffs auf SVM-Volume-Vorgänge

Sie können eine Rolle definieren, um die Storage-Volume-Administration innerhalb einer SVM zu beschränken.

### Informationen zu diesem Workflow

Eine herkömmliche Rolle wird zuerst erstellt, um zunächst den Zugriff auf alle wichtigen Volume-Administrationsfunktionen außer dem Klonen zu ermöglichen. Die Rolle wird mit folgenden Merkmalen definiert:

- Alle CRUD Volume-Vorgänge einschließlich get, create, modify und delete
- Volume-Klon kann nicht erstellt werden

Sie können dann optional die Rolle nach Bedarf aktualisieren. In diesem Workflow wird die Rolle im zweiten Schritt geändert, damit der Benutzer einen Volume-Klon erstellen kann.

### Schritt 1: Erstellen Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die RBAC-Rolle zu erstellen.

#### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

| HTTP-Methode | Pfad                       |
|--------------|----------------------------|
| POST         | /API/Sicherheit/Funktionen |

#### Beispiel für die Wellung

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

## JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    { "path": "volume create", "access": "all" },
    { "path": "volume delete", "access": "all" }
  ]
}
```

## Schritt 2: Aktualisieren Sie die Rolle

Sie können einen API-Aufruf ausgeben, um die vorhandene Rolle zu aktualisieren.

### HTTP-Methode und -Endpoint

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpoint.

| HTTP-Methode | Pfad                       |
|--------------|----------------------------|
| POST         | /API/Sicherheit/Funktionen |

### Zusätzliche Eingabeparameter für Curl-Beispiele

Neben den bei allen REST API-Aufrufen üblichen Parametern werden in diesem Schritt auch die folgenden Parameter im Curl-Beispiel verwendet.

| Parameter                | Typ  | Erforderlich | Beschreibung   |
|--------------------------|------|--------------|--|
| SVM_ID USD               | Pfad | Ja.          | Dies ist die UUID der SVM, die die Rollendefinition enthält.       |
| „ROLE_NAME“ IN US-DOLLAR | Pfad | Ja.          | Dies ist der Name der Rolle innerhalb der zu aktualisierenden SVM. |

### Beispiel für die Wellung

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## JSON-Eingabebeispiel

```
{
  "path": "volume clone",
  "access": "all"
}
```

# Administration der Datensicherung

Sie können einem Benutzer begrenzte Datensicherungsfunktionen zur Verfügung stellen.

## Informationen zu diesem Workflow

Die traditionelle erstellte Rolle wird mit den folgenden Merkmalen definiert:

- Es sind möglich, Snapshots zu erstellen und zu löschen und auch SnapMirror Beziehungen zu aktualisieren
- Objekte höherer Ebene wie Volumes oder SVMs können nicht erstellt oder geändert werden

## HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

| HTTP-Methode | Pfad                       |
|--------------|----------------------------|
| POST         | /API/Sicherheit/Funktionen |

## Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## JSON-Eingabebeispiel

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "volume snapshot create", "access": "all"},
    {"path": "volume snapshot delete", "access": "all"},
    {"path": "volume show", "access": "readonly"},
    {"path": "vserver show", "access": "readonly"},
    {"path": "snapmirror show", "access": "readonly"},
    {"path": "snapmirror update", "access": "all"}
  ]
}
```

## Erstellung von ONTAP-Berichten zulassen

Sie können EINE REST-Rolle erstellen, um Benutzern die Möglichkeit zu geben, ONTAP-Berichte zu generieren.

### Informationen zu diesem Workflow

Die erstellte Rolle wird mit folgenden Merkmalen definiert:

- Abrufen aller Kapazitäts- und Performance-Objektinformationen (u. a. Volume, qtree, LUN, Aggregate, Node, Und SnapMirror Beziehungen)
- Objekte höherer Ebene (wie Volumes oder SVMs) können nicht erstellt oder geändert werden.

### HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

| HTTP-Methode | Pfad                       |
|--------------|----------------------------|
| POST         | /API/Sicherheit/Funktionen |

### Beispiel für die Wellung

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

## JSON-Eingabebeispiel

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api/storage/volumes", "access": "readonly"},
    {"path": "/api/storage/qtrees", "access": "readonly"},
    {"path": "/api/storage/luns", "access": "readonly"},
    {"path": "/api/storage/aggregates", "access": "readonly"},
    {"path": "/api/cluster/nodes", "access": "readonly"},
    {"path": "/api/snapmirror/relationships", "access": "readonly"},
    {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

## 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, BEISPIELHAFTE 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.