# Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-48/concept/concept_types_of_role_based_access_control_in_snapcenter.html on September 26, 2025. Always check docs.netapp.com for the latest.

# Inhalt


Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter . . . 1
- RBAC-Typen . . . 1
  - RBAC von SnapCenter . . . 1
  - RBAC auf Applikationsebene . . . 2
  - SnapCenter Plug-in für VMware vSphere RBAC . . . 2
  - ONTAP-Berechtigungen . . . 2
- RBAC-Berechtigungen und -Rollen . . . 2
  - SnapCenter Rollen . . . 3
  - SnapCenter Plug-in für VMware vSphere Rollen . . . 3
  - SnapCenter-Berechtigungen . . . 3
- Vordefinierte SnapCenter-Rollen und -Berechtigungen . . . 4
  - SnapCenter Administratorrolle . . . 4
  - Administratorrolle für App Backup und Klonen . . . 4
  - Backup und Clone Viewer-Rolle . . . 6
  - Rolle für den Infrastrukturadministrator . . . 7

# Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter

## RBAC-Typen

Mit der rollenbasierten Zugriffssteuerung (RBAC) und den ONTAP Berechtigungen von SnapCenter können SnapCenter Administratoren die Kontrolle über SnapCenter Ressourcen an verschiedene Benutzer oder Benutzergruppen delegieren. Dank dieses zentral gemanagten Zugriffs können Applikationsadministratoren innerhalb delegierter Umgebungen sicher arbeiten.

Sie können Rollen erstellen und ändern und Benutzern jederzeit Ressourcenzugriff hinzufügen. Wenn Sie jedoch zum ersten Mal SnapCenter einrichten, sollten Sie mindestens Active Directory-Benutzer oder -Gruppen zu Rollen hinzufügen und diesen Benutzern oder Gruppen dann Ressourcenzugriff hinzufügen.

Sie können SnapCenter nicht zum Erstellen von Benutzer- oder Gruppenkonten verwenden. Sie sollten Benutzer- oder Gruppenkonten in Active Directory des Betriebssystems oder der Datenbank erstellen.

SnapCenter verwendet folgende Arten der rollenbasierten Zugriffssteuerung:

- RBAC von SnapCenter
- SnapCenter Plug-in RBAC (für einige Plug-ins)
- RBAC auf Applikationsebene
- ONTAP-Berechtigungen

### RBAC von SnapCenter

#### Rollen und Berechtigungen

SnapCenter wird mit vordefinierten Rollen ausgeliefert, deren Berechtigungen bereits zugewiesen sind. Sie können diesen Rollen Benutzer oder Benutzergruppen zuweisen. Sie können auch neue Rollen erstellen und Berechtigungen und Benutzer verwalten.

#### Zuweisen von Berechtigungen für Benutzer oder Gruppen

Sie können Benutzern oder Gruppen Berechtigungen zuweisen, um auf SnapCenter-Objekte wie Hosts, Speicherverbindungen und Ressourcengruppen zuzugreifen. Sie können die Berechtigungen der SnapCenterAdmin-Rolle nicht ändern.

Sie können Benutzern und Gruppen innerhalb derselben Gesamtstruktur und Benutzern, die zu verschiedenen Wäldern gehören, RBAC-Berechtigungen zuweisen. Sie können Benutzern, die zu verschachtelten Gruppen gehören, keine RBAC-Berechtigungen zuweisen.

Wenn Sie eine benutzerdefinierte Rolle erstellen, muss sie alle Berechtigungen der SnapCenter-Administratorrolle enthalten. Wenn Sie nur einige der Berechtigungen kopieren, z. B. Host add oder Host remove, können Sie diese Vorgänge nicht ausführen.

**Authentifizierung**

Benutzer müssen bei der Anmeldung über die grafische Benutzeroberfläche (GUI) oder PowerShell Commandlets über die Authentifizierung sorgen. Wenn Benutzer Mitglieder mehrerer Rollen sind, werden sie nach der Eingabe von Anmeldedaten aufgefordert, die gewünschte Rolle anzugeben. Benutzer müssen außerdem eine Authentifizierung zur Ausführung der APIs bereitstellen.

### RBAC auf Applikationsebene

SnapCenter verwendet die Zugangsdaten, um sicherzustellen, dass autorisierte SnapCenter Benutzer auch über Berechtigungen auf Applikationsebene verfügen.

Wenn Sie beispielsweise Snapshot Kopien und Datensicherungsvorgänge in einer SQL Server-Umgebung ausführen möchten, müssen Sie die Anmeldedaten mit den richtigen Windows- oder SQL-Anmeldedaten festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die auf beiden Methoden festgelegt sind. Wenn Sie Snapshot Kopien und Datensicherungsvorgänge in einer Windows File-System-Umgebung auf ONTAP Storage durchführen möchten, muss die SnapCenter Administratorrolle über Administratorrechte auf dem Windows Host verfügen.

Wenn Sie Datensicherungsvorgänge in einer Oracle-Datenbank durchführen möchten und wenn die Betriebssystemauthentifizierung im Datenbank-Host deaktiviert ist, müssen Sie die Anmeldedaten mit der Oracle-Datenbank oder den Oracle-ASM-Anmeldeinformationen festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die mit einer dieser Methoden festgelegt wurden, je nach Operation.

### SnapCenter Plug-in für VMware vSphere RBAC

Wenn Sie das SnapCenter VMware Plug-in für die VM-konsistente Datensicherung nutzen, bietet der vCenter Server zusätzliche RBAC-Level. Das SnapCenter VMware Plug-in unterstützt sowohl vCenter Server RBAC als auch Data ONTAP RBAC.

Weitere Informationen finden Sie unter "SnapCenter Plug-in für VMware vSphere RBAC"

### ONTAP-Berechtigungen

Sie sollten vsadmin-Konto mit den erforderlichen Berechtigungen für den Zugriff auf das Speichersystem erstellen.

Informationen zum Erstellen des Kontos und Zuweisen von Berechtigungen finden Sie unter "Erstellen einer ONTAP-Cluster-Rolle mit minimalen Berechtigungen"

# RBAC-Berechtigungen und -Rollen

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter können Sie Rollen erstellen und diesen Rollen Berechtigungen zuweisen und dann den Rollen Benutzer oder Benutzergruppen zuweisen. So können SnapCenter Administratoren eine zentral verwaltete Umgebung erstellen, während Applikationsadministratoren die Datensicherung managen können. SnapCenter wird mit vordefinierten Rollen und Berechtigungen ausgeliefert.

## SnapCenter Rollen

SnapCenter wird mit den folgenden vordefinierten Rollen ausgeliefert. Sie können diesen Rollen Benutzer und Gruppen zuweisen oder neue Rollen erstellen.

Wenn Sie einem Benutzer eine Rolle zuweisen, werden auf der Seite „Jobs“ nur Aufträge angezeigt, die für diesen Benutzer relevant sind, es sei denn, Sie haben die Rolle „SnapCenter-Admin“ zugewiesen.

- Administrator für App Backup und Klonen
- Backup und Clone Viewer
- Infrastrukturadministrator
- SnapCenterAdmin

## SnapCenter Plug-in für VMware vSphere Rollen

Für das Management der VM-konsistenten Datensicherung von VMs, VMDKs und Datastores werden in vCenter die folgenden Rollen vom SnapCenter Plug-in für VMware vSphere erstellt:

- SCV-Administrator
- SCV-Ansicht
- SCV-Backup
- SCV-Wiederherstellung
- Wiederherstellung der SCV-Gastdatei

Weitere Informationen finden Sie unter "RBAC-Typen für SnapCenter Plug-in für VMware vSphere Benutzer"

**Best Practice:** NetApp empfiehlt, eine ONTAP-Rolle für das SnapCenter Plug-in für VMware vSphere Operationen zu erstellen und diese alle erforderlichen Berechtigungen zuzuweisen.

## SnapCenter-Berechtigungen

SnapCenter bietet folgende Berechtigungen:

- Ressourcengruppe
- Richtlinie
- Backup
- Host
- Storage-Anbindung
- Klon
- Bereitstellung (nur für Microsoft SQL Datenbank)
- Dashboard
- Berichte An
- Wiederherstellen
  - Vollständige Volume-Wiederherstellung (nur bei benutzerdefinierten Plug-ins)
- Ressource

Für nicht-Administratoren sind vom Administrator Plug-in-Berechtigungen erforderlich, um eine Ressourcenerkennung durchzuführen.

- Plug-in Installieren oder Deinstallieren

  Wenn Sie die Berechtigungen für die Plug-in-Installation aktivieren, müssen Sie auch die Host-Berechtigung ändern, um Lese- und Updates zu aktivieren.

- Migration
- Mount (nur für Oracle Database)
- Unmount (nur für Oracle Database)
- Job-Überwachung

  Mit der Berechtigung Job Monitor können Mitglieder verschiedener Rollen die Vorgänge für alle Objekte anzeigen, denen sie zugewiesen sind.

# Vordefinierte SnapCenter-Rollen und -Berechtigungen

Im Lieferumfang von SnapCenter sind vordefinierte Rollen enthalten, von denen jede bereits aktiviert ist. Beim Einrichten und Verwalten der rollenbasierten Zugriffssteuerung können Sie entweder die vordefinierten Rollen verwenden oder neue erstellen.

SnapCenter umfasst die folgenden vordefinierten Rollen:

- SnapCenter Administratorrolle
- Administratorrolle für App Backup und Klonen
- Backup und Clone Viewer-Rolle
- Rolle für den Infrastrukturadministrator

Wenn Sie einem Benutzer einer Rolle hinzufügen, müssen Sie entweder die Berechtigung StorageConnection zuweisen, um die Kommunikation mit der Storage Virtual Machine (SVM) zu aktivieren, oder dem Benutzer eine SVM zuweisen, damit die Berechtigung zur Verwendung der SVM aktiviert wird. Mit der Berechtigung für Speicherverbindungen können Benutzer SVM-Verbindungen erstellen.

Ein Benutzer mit der Rolle „SnapCenter-Admin“ kann beispielsweise SVM-Verbindungen erstellen und einem Benutzer mit der Rolle „App-Backup“ und „Clone Admin“ zuweisen. Dieser besitzt standardmäßig keine Berechtigung, SVM-Verbindungen zu erstellen oder zu bearbeiten. Ohne SVM-Verbindung können Benutzer Backup-, Klon- oder Restore-Vorgänge nicht abschließen.

## SnapCenter Administratorrolle

In der SnapCenter-Administratorrolle sind alle Berechtigungen aktiviert. Sie können die Berechtigungen für diese Rolle nicht ändern. Sie können der Rolle Benutzer und Gruppen hinzufügen oder sie entfernen.

## Administratorrolle für App Backup und Klonen

Die Rolle „App Backup“ und „Clone Admin“ verfügt über die erforderlichen Berechtigungen zur Durchführung administrativer Aktionen für Applikations-Backups und klonbezogene Aufgaben. Diese Rolle verfügt nicht über Berechtigungen für Host-Management, Bereitstellung, Storage-Verbindungs-Management oder Remote-

Installation.

| Berechtigungen | Aktiviert | Erstellen | Lesen | Aktualisierung | Löschen |
|---|---|---|---|---|---|
| Ressourcengruppe | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Richtlinie | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Backup | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Host | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Storage-Anbindung | Keine Angabe | Nein | Ja. | Nein | Nein |
| Klon | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Bereitstellung | Keine Angabe | Nein | Ja. | Nein | Nein |
| Dashboard | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Berichte An | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Wiederherstellen | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Ressource | Ja. | Ja. | Ja. | Ja. | Ja. |
| Plug-in Installation/Deinstallation | Nein | Keine Angabe | | Keine Angabe | Keine Angabe |
| Migration | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Montieren | Ja. | Ja. | Keine Angabe | Keine Angabe | Keine Angabe |
| Unmounten | Ja. | Ja. | Keine Angabe | Keine Angabe | Keine Angabe |
| Vollständige Volume-Wiederherstellung | Nein | Nein | Keine Angabe | Keine Angabe | Keine Angabe |
| Job-Überwachung | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |

## Backup und Clone Viewer-Rolle

Die Rolle Backup und Clone Viewer verfügt über eine schreibgeschützte Ansicht aller Berechtigungen. In dieser Rolle sind auch Berechtigungen für Erkennung, Berichterstellung und Zugriff auf das Dashboard aktiviert.

| Berechtigungen | Aktiviert | Erstellen | Lesen | Aktualisierung | Löschen |
|---|---|---|---|---|---|
| Ressourcengruppe | Keine Angabe | Nein | Ja. | Nein | Nein |
| Richtlinie | Keine Angabe | Nein | Ja. | Nein | Nein |
| Backup | Keine Angabe | Nein | Ja. | Nein | Nein |
| Host | Keine Angabe | Nein | Ja. | Nein | Nein |
| Storage-Anbindung | Keine Angabe | Nein | Ja. | Nein | Nein |
| Klon | Keine Angabe | Nein | Ja. | Nein | Nein |
| Bereitstellung | Keine Angabe | Nein | Ja. | Nein | Nein |
| Dashboard | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Berichte An | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Wiederherstellen | Nein | Nein | Keine Angabe | Keine Angabe | Keine Angabe |
| Ressource | Nein | Nein | Ja. | Ja. | Nein |
| Plug-in Installation/Deinstallation | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Migration | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Montieren | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Unmounten | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Vollständige Volume-Wiederherstellung | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |

| Berechtigungen | Aktiviert | Erstellen | Lesen | Aktualisierung | Löschen |
|---|---|---|---|---|---|
| Job-Überwachung | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |

## Rolle für den Infrastrukturadministrator

Die Rolle „Infrastrukturadministrator“ hat Berechtigungen für Host-Management, Storage-Management, Bereitstellung, Ressourcengruppen, Remote-Installationsberichte, Zugriff auf das Dashboard.

| Berechtigungen | Aktiviert | Erstellen | Lesen | Aktualisierung | Löschen |
|---|---|---|---|---|---|
| Ressourcengruppe | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Richtlinie | Keine Angabe | Nein | Ja. | Ja. | Ja. |
| Backup | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Host | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Storage-Anbindung | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Klon | Keine Angabe | Nein | Ja. | Nein | Nein |
| Bereitstellung | Keine Angabe | Ja. | Ja. | Ja. | Ja. |
| Dashboard | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Berichte An | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Wiederherstellen | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Ressource | Ja. | Ja. | Ja. | Ja. | Ja. |
| Plug-in Installation/Deinstallation | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Migration | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Montieren | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |
| Unmounten | Nein | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |

| Berechtigungen | Aktiviert | Erstellen | Lesen | Aktualisierung | Löschen |
|---|---|---|---|---|---|
| Vollständige Volume-Wiederherstellung | Nein | Nein | Keine Angabe | Keine Angabe | Keine Angabe |
| Job-Überwachung | Ja. | Keine Angabe | Keine Angabe | Keine Angabe | Keine Angabe |

**Copyright-Informationen**

Copyright © 2025 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 IRGENDEINER 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.