



# Management von Zugriffssteuerungsrollen

ONTAP 9

NetApp  
March 22, 2023

# Inhaltsverzeichnis

- Management von Zugriffssteuerungsrollen ..... 1
  - Übersicht über Zugriffssteuerungsrollen verwalten ..... 1
  - Ändern Sie die einem Administrator zugewiesene Rolle ..... 1
  - Definieren benutzerdefinierter Rollen ..... 1
  - Vordefinierte Rollen für Cluster-Administratoren ..... 3
  - Vordefinierte Rollen für SVM-Administratoren ..... 5

# Management von Zugriffssteuerungsrollen

## Übersicht über Zugriffssteuerungsrollen verwalten

Die einem Administrator zugewiesene Rolle legt die Befehle fest, auf die der Administrator zugreifen kann. Sie weisen die Rolle beim Erstellen des Kontos für den Administrator zu. Sie können je nach Bedarf eine andere Rolle zuweisen oder benutzerdefinierte Rollen definieren.

## Ändern Sie die einem Administrator zugewiesene Rolle

Sie können das verwenden `security login modify` Befehl zum Ändern der Rolle eines Cluster- oder SVM-Administratorkontos. Sie können eine vordefinierte oder benutzerdefinierte Rolle zuweisen.

### Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

### Schritt

1. Ändern Sie die Rolle eines Clusters oder SVM-Administrators:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Eine vollständige Befehlsyntax finden Sie im ["Arbeitsblatt"](#).

### ["Erstellen oder Ändern von Anmeldekonten"](#)

Mit dem folgenden Befehl wird die Rolle des AD-Cluster-Administratorkontos geändert `DOMAIN1\guest1`  
Für den vordefinierten `readonly` Rolle:

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

Mit dem folgenden Befehl wird die Rolle der SVM-Administratorkonten im AD-Gruppenkonto geändert  
`DOMAIN1\adgroup` Auf den Benutzer `vol_role` Rolle:

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

## Definieren benutzerdefinierter Rollen

Sie können das verwenden `security login role create` Befehl zum Definieren

einer benutzerdefinierten Rolle. Sie können den Befehl so oft wie nötig ausführen, um die genaue Kombination der Funktionen zu erreichen, die Sie mit der Rolle verknüpfen möchten.

### Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

### Über diese Aufgabe

- Eine Rolle, ob vordefiniert oder benutzerdefiniert, gewährt oder verweigert den Zugriff auf ONTAP-Befehle oder Befehlsverzeichnisse.

Ein Befehlsverzeichnis (`volume`, Zum Beispiel) ist eine Gruppe verwandter Befehle und Unterverzeichnisse. Sofern nicht wie in diesem Verfahren beschrieben, gewährt oder verweigert das Zulassen des Zugriffs auf ein Befehlsverzeichnis jedem Befehl im Verzeichnis und seinen Unterverzeichnissen den Zugriff.

- Bestimmter Befehlszugriff oder Unterverzeichnis-Zugriff überschreibt den Zugriff auf das übergeordnete Verzeichnis.

Wenn eine Rolle mit einem Befehlsverzeichnis definiert ist und dann erneut mit einer anderen Zugriffsebene für einen bestimmten Befehl oder ein Unterverzeichnis des übergeordneten Verzeichnisses definiert wird, überschreibt die Zugriffsebene, die für den Befehl oder das Unterverzeichnis festgelegt ist, die des übergeordneten Verzeichnisses.



Einem SVM-Administrator kann keine Rolle zugewiesen werden, die einem Befehl oder Befehlsverzeichnis Zugriff gibt, das nur dem zur Verfügung steht `admin` Cluster-Administrator – zum Beispiel der `security` Befehlsverzeichnis.

### Schritt

1. Definieren einer benutzerdefinierten Rolle:

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

Eine vollständige Befehlsyntax finden Sie im ["Arbeitsblatt"](#).

Die folgenden Befehle erteilen das `vol_role` Rollen vollständigen Zugriff auf die Befehle im `volume` Befehlsverzeichnis und schreibgeschützter Zugriff auf die Befehle im `volume snapshot` Unterverzeichnis.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all  
  
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

Die folgenden Befehle erteilen das `SVM_storage` Rolle nur-Lese-Zugriff auf die Befehle in der `storage` Befehlsverzeichnis, kein Zugriff auf die Befehle im `storage encryption` Unterverzeichnis und vollständigen Zugriff auf das `storage aggregate plex offline` Nicht-intrinsischer Befehl.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly
```

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none
```

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

## Vordefinierte Rollen für Cluster-Administratoren

Die vordefinierten Rollen für Cluster-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem Cluster-Administrator das vordefinierte zugewiesene `admin` Rolle:

In der folgenden Tabelle werden die vordefinierten Rollen für Cluster-Administratoren aufgeführt:

Diese Rolle...	Verfügt über diese Zugriffsebene...	Zu den folgenden Befehlen oder Befehlsverzeichnissen
Admin	Alle	Alle Befehlsverzeichnisse (DEFAULT)
Admin-no-fsa (ab ONTAP 9.12.1 verfügbar)	Lese-/Schreibzugriff	<ul style="list-style-type: none"><li>• Alle Befehlsverzeichnisse (DEFAULT)</li><li>• <code>security login rest-role</code></li><li>• <code>security login role</code></li></ul>

Schreibgeschützt	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>	Keine
volume file show-disk-usage	AutoSupport	Alle
<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	Keine	Alle anderen Befehlsverzeichnisse (DEFAULT)
Backup	Alle	vserver services ndmp
readonly	volume	Keine
Alle anderen Befehlsverzeichnisse (DEFAULT)	readonly	Alle

<ul style="list-style-type: none"> <li>• security login password</li> </ul> <p>Nur zur Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</p> <ul style="list-style-type: none"> <li>• set</li> </ul>	Keine	security
readonly	Alle anderen Befehlsverzeichnisse (DEFAULT)	Keine



Der `autosupport` Rolle ist dem vordefinierten zugewiesen `autosupport` Konto, das von AutoSupport OnDemand verwendet wird. ONTAP verhindert, dass Sie den ändern oder löschen können `autosupport` Konto. ONTAP verhindert darüber hinaus, dass Sie das zuweisen `autosupport` Rolle für andere Benutzerkonten.

## Vordefinierte Rollen für SVM-Administratoren

Die vordefinierten Rollen für SVM-Administratoren sollten die meisten Ihrer Anforderungen erfüllen. Sie können bei Bedarf benutzerdefinierte Rollen erstellen. Standardmäßig wird einem SVM-Administrator das vordefinierte zugewiesen `vsadmin` Rolle:

In der folgenden Tabelle sind die vordefinierten Rollen für SVM-Administratoren aufgeführt:

Rollenname	Sorgen
Vsadmin	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Verwalten von Volumes, außer Verschieben von Volumes</li> <li>• Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien</li> <li>• Verwalten von LUNs</li> <li>• Durchführung von SnapLock-Vorgängen mit Ausnahme von privilegierten Löschen</li> <li>• Konfiguration der Protokolle NFS, SMB, iSCSI und FC Einschließlich FCoE</li> <li>• Dienste konfigurieren: DNS, LDAP und NIS</li> <li>• Überwachen von Jobs</li> <li>• Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>

Vsadmin-Volume	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Managen von Volumes, einschließlich Volume-Verschiebungen</li> <li>• Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien</li> <li>• Verwalten von LUNs</li> <li>• Konfiguration von Protokollen NFS, SMB, iSCSI und FC, einschließlich FCoE</li> <li>• Dienste konfigurieren: DNS, LDAP und NIS</li> <li>• Monitoring der Netzwerkschnittstelle</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>
Vsadmin-Protokoll	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Konfiguration von Protokollen NFS, SMB, iSCSI und FC, einschließlich FCoE</li> <li>• Dienste konfigurieren: DNS, LDAP und NIS</li> <li>• Verwalten von LUNs</li> <li>• Monitoring der Netzwerkschnittstelle</li> <li>• Monitoring des Systemzustands der SVM</li> </ul>
Vsadmin-Backup	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Verwalten des NDMP-Betriebs</li> <li>• Erstellung eines wiederhergestellten Lese-/Schreibvorgangs eines Volumes</li> <li>• Verwalten von SnapMirror Beziehungen und Snapshot Kopien</li> <li>• Anzeigen von Volumes und Netzwerkinformationen</li> </ul>



Vsadmin-snaplock	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Verwalten von Volumes, außer Verschieben von Volumes</li> <li>• Verwalten von Quotas, qtrees, Snapshot Kopien und Dateien</li> <li>• Durchführung von SnapLock-Vorgängen einschließlich privilegierter Löschung</li> <li>• Konfiguration von Protokollen: NFS und SMB</li> <li>• Dienste konfigurieren: DNS, LDAP und NIS</li> <li>• Überwachen von Jobs</li> <li>• Monitoring von Netzwerkverbindungen und Netzwerkschnittstelle</li> </ul>
Vsadmin-ReadOnly	<ul style="list-style-type: none"> <li>• Verwaltung des eigenen Benutzerkontos mit lokalem Passwort und Schlüsselinformationen</li> <li>• Monitoring des Systemzustands der SVM</li> <li>• Monitoring der Netzwerkschnittstelle</li> <li>• Anzeigen von Volumes und LUNs</li> <li>• Anzeigen von Services und Protokollen</li> </ul>

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.