



# **Sicherer Dateizugriff über SMB-Share-ACLs**

## **ONTAP 9**

NetApp  
April 24, 2024

# Inhalt

Sicherer Dateizugriff über SMB-Share-ACLs .....	1
Richtlinien zum Management von SMB-ACLs auf Share-Ebene .....	1
Erstellen Sie SMB-Zugriffssteuerungslisten .....	1
Befehle zum Managen von SMB-Zugriffssteuerungslisten .....	4

# Sicherer Dateizugriff über SMB-Share-ACLs

## Richtlinien zum Management von SMB-ACLs auf Share-Ebene

Sie können ACLs auf Share-Ebene ändern, um Benutzern mehr oder weniger Zugriffsrechte für die Freigabe zu gewähren. Sie können ACLs auf Share-Ebene entweder mithilfe von Windows-Benutzern und -Gruppen oder UNIX-Benutzern und -Gruppen konfigurieren.

Nachdem Sie eine Freigabe erstellt haben, gewährt die share-Level ACL standardmäßig Lesezugriff auf die Standardgruppe namens Everyone. Lesezugriff in der ACL bedeutet, dass alle Benutzer in der Domäne und alle vertrauenswürdigen Domänen nur Lesezugriff auf die Freigabe haben.

Sie können eine Zugriffssteuerungsliste auf der Share-Ebene ändern, indem Sie die Microsoft Management Console (MMC) in einem Windows-Client oder in der ONTAP-Befehlszeile verwenden.

Die folgenden Richtlinien gelten, wenn Sie die MMC verwenden:

- Der angegebene Benutzer- und Gruppenname muss Windows-Namen sein.
- Sie können nur Windows-Berechtigungen angeben.

Wenn Sie die ONTAP-Befehlszeile verwenden, gelten die folgenden Richtlinien:

- Der angegebene Benutzer- und Gruppenname kann Windows- oder UNIX-Namen sein.

Wenn beim Erstellen oder Ändern von ACLs kein Benutzer- und Gruppentyp angegeben wird, ist der Standardtyp Windows-Benutzer und -Gruppen.

- Sie können nur Windows-Berechtigungen angeben.

## Erstellen Sie SMB-Zugriffssteuerungslisten

Durch die Konfiguration von Freigabeberechtigungen durch die Erstellung von Zugriffssteuerungslisten (ACLs) für SMB-Freigaben können Sie die Zugriffsebene für eine Freigabe für Benutzer und Gruppen steuern.

### Über diese Aufgabe

Sie können ACLs auf Share-Ebene mithilfe lokaler oder Domain-Windows-Benutzer- oder Gruppennamen oder UNIX-Benutzer- oder Gruppennamen konfigurieren.

Bevor Sie eine neue ACL erstellen, sollten Sie die Standard-Freigabe-ACL löschen `Everyone / Full Control`, Die ein Sicherheitsrisiko ist.

Im Arbeitsgruppenmodus ist der Name der lokalen Domäne der Name des SMB-Servers.

### Schritte

1. Löschen Sie die Standard-Freigabe-ACL: ``vserver cifs share Access-control delete -vserver vserver_Name -share share_Name -user-or-Group everyone``

## 2. Konfigurieren Sie die neue ACL:

Wenn Sie ACLs mit... konfigurieren möchten.	Geben Sie den Befehl ein...
Windows-Benutzer	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</pre>
Windows-Gruppe	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\group_name -permission access_right</pre>
UNIX-Benutzer	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</pre>
UNIX-Gruppe	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</pre>

3. Überprüfen Sie, ob die ACL, die auf die Freigabe angewendet wurde, korrekt ist, indem Sie die verwenden `vserver cifs share access-control show` Befehl.

### Beispiel

Der folgende Befehl gibt Change Berechtigungen für die Windows-Gruppe „Sales Team“ für den „sales“-Share auf der „vs1.example.com“ SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\Sales Team	windows	Change

Der folgende Befehl gibt Read Genehmigung der UNIX Gruppe „Engineering“ für den „eng“-Share auf der „vs2.example.com SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

Die folgenden Befehle geben an Change Berechtigung für die lokale Windows-Gruppe namens „Tiger Team“ und Full\_Control Berechtigung für den lokalen Windows-Benutzer namens „Sue Chang“ für die Freigabe „datavol5“ auf der „vs1 SVM:

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change
```

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control
```

```
cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	
-----				
vs1	c\$	BUILTIN\Administrators	windows	
Full_Control				
vs1	datavol5	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

## Befehle zum Managen von SMB-Zugriffssteuerungslisten

Sie müssen die Befehle zum Verwalten von SMB Access Control Lists (ACLs) kennen, die das Erstellen, Anzeigen, Ändern und Löschen von ihnen umfassen.

Ihr Ziel ist	Befehl
Neue ACL erstellen	<code>vsriver cifs share access-control create</code>
ACLs anzeigen	<code>vsriver cifs share access-control show</code>
Ändern Sie eine ACL	<code>vsriver cifs share access-control modify</code>
Löschen einer ACL	<code>vsriver cifs share access-control delete</code>

## 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.