# Sicherer Dateizugriff über SMB-Share-ACLs

ONTAP 9

NetApp
April 24, 2024

# Inhalt

# 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 | `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`* |
| Windows-Gruppe | `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`* |
| UNIX-Benutzer | `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` |
| UNIX-Gruppe | `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` |

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

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
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::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 Share       User/Group               User/Group  Access
Vserver          Name        Name                     Type
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::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
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 | `vserver cifs share access-control create` |
| ACLs anzeigen | `vserver cifs share access-control show` |
| Ändern Sie eine ACL | `vserver cifs share access-control modify` |
| Löschen einer ACL | `vserver cifs share access-control delete` |