SMB-Zugriff mithilfe von Exportrichtlinien absichern

ONTAP 9

NetApp
October 29, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/export-policies-access-concept.html on October 29, 2026. Always check docs.netapp.com for the latest.

Inhalt

SMB-Zugriff mithilfe von Exportrichtlinien absichern . . . 1
Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff . . . 1
Informationen zu ONTAP SMB Exportregeln . . . 2
Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen . . . 3
Exportregel nur für SMB-Zugriff . . . 4
Exportregel für SMB- und NFS-Zugriff . . . 4
Exportregel für SMB-Zugriff ausschließlich über NTLM . . . 4
ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren . . . 5
Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen . . . 6

SMB-Zugriff mithilfe von Exportrichtlinien absichern

Informationen zur Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn auf dem SMB-Server Exportregeln für den SMB-Zugriff aktiviert sind, werden Exportregeln verwendet, um den Zugriff von SMB-Clients auf SVM-Volumes zu steuern. Für den Datenzugriff kann eine Exportregel erstellt werden, die den SMB-Zugriff erlaubt, und anschließend der Richtlinie die Volumes zugeordnet werden, die SMB-Freigaben enthalten.

Für eine Exportregel gilt eine oder mehrere Regeln, die festlegen, welche Clients Zugriff auf die Daten erhalten und welche Authentifizierungsprotokolle für Lese- und Schreibzugriff unterstützt werden. Exportregeln können so konfiguriert werden, dass der Zugriff über SMB für alle Clients, ein Subnetz von Clients oder einen bestimmten Client erlaubt ist und dass die Authentifizierung mittels Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung bei der Bestimmung des Lese- und Schreibzugriffs auf Daten zulässig ist.

Nach der Verarbeitung aller auf die Exportregel angewendeten Exportregeln kann ONTAP feststellen, ob dem Client Zugriff gewährt wird und welche Zugriffsebene gewährt wird. Exportregeln gelten für Client-Rechner, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen nicht die Windows-Benutzer- und -gruppenbasierte Authentifizierung und Autorisierung. Exportregeln bieten eine zusätzliche Sicherheitsebene zum Schutz des Zugriffs, zusätzlich zu den Berechtigungen für Freigaben und Dateizugriff.

Jedem Volume wird genau eine Exportregel zugeordnet, um den Clientzugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportregeln enthalten. Dadurch ergeben sich für SVMs mit mehreren Volumes folgende Möglichkeiten:

- Weisen Sie jedem Volume der SVM unterschiedliche Exportrichtlinien zu, um die Zugriffskontrolle für jeden einzelnen Client auf jedes Volume in der SVM zu ermöglichen.
- Dieselbe Exportregel kann mehreren Volumes der SVM zugewiesen werden, sodass eine identische Clientzugriffskontrolle möglich ist, ohne für jedes Volume eine neue Exportregel erstellen zu müssen.

Jede SVM verfügt über mindestens eine Export-Richtlinie namens „`default`“, die keine Regeln enthält. Sie können diese Export-Richtlinie nicht löschen, aber Sie können sie umbenennen oder ändern. Jedes Volume auf der SVM ist standardmäßig der Standard-Export-Richtlinie zugeordnet. Wenn Export-Richtlinien für den SMB-Zugriff auf der SVM deaktiviert sind, hat die Export-Richtlinie „`default`“ keine Auswirkungen auf den SMB-Zugriff.

Es ist möglich, Regeln zu konfigurieren, die sowohl NFS- als auch SMB-Hosts Zugriff gewähren, und diese Regel mit einer Exportregel zu verknüpfen, die anschließend dem Volume zugeordnet werden kann, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Alternativ kann für einige Volumes, auf die nur SMB-Clients zugreifen müssen, eine Exportregel mit Regeln konfiguriert werden, die ausschließlich den Zugriff über das SMB-Protokoll erlauben und für die Authentifizierung bei Lese- und Schreibzugriffen ausschließlich Kerberos oder NTLM (oder beides) verwenden. Die Exportregel wird dann den Volumes zugeordnet, bei denen ausschließlich SMB-Zugriff erforderlich ist.

Wenn Exportregeln für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportregel nicht zugelassen wird, schlägt die Anfrage mit einer „Zugriff verweigert“-Meldung fehl. Wenn ein

Client keiner Regel in der Exportregel des Volumes entspricht, wird der Zugriff verweigert. Ist eine Exportregel leer, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen den Zugriff ansonsten erlauben würden. Das bedeutet, dass die Exportregel auf Volumes mit SMB-Freigaben mindestens Folgendes zulassen muss:

- Zugriff für alle Clients oder die entsprechende Teilmenge der Clients zulassen
- Zugriff über SMB zulassen
- Angemessener Lese- und Schreibzugriff durch Kerberos- oder NTLM-Authentifizierung (oder beides) möglich

Informationen dazu "Konfiguration und Verwaltung von Exportrichtlinien".

Informationen zu ONTAP SMB Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportregel. Exportregeln gleichen Clientzugriffsanfragen an ein Volume mit spezifischen, von Ihnen konfigurierten Parametern ab, um festzulegen, wie die Clientzugriffsanfragen behandelt werden.

Eine Exportregel muss mindestens in einer Exportregel enthalten sein, damit Clients Zugriff erhalten. Wenn eine Exportregel mehr als eine Regel enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportregel erscheinen. Die Reihenfolge der Regeln wird durch die Regelindexnummer bestimmt. Wenn eine Regel auf einen Client zutrifft, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Wenn keine Regel zutrifft, wird dem Client der Zugriff verweigert.

Exportregeln können so konfiguriert werden, dass die Clientzugriffsberechtigungen anhand der folgenden Kriterien bestimmt werden:

- Das vom Client, der die Anfrage sendet, verwendete Protokoll für den Dateizugriff, beispielsweise NFSv4 oder SMB.
- Eine Client-Kennung, zum Beispiel Hostname oder IP-Adresse.

  Die maximale Größe des `-clientmatch` Feldes beträgt 4096 Zeichen.

- Der vom Client zur Authentifizierung verwendete Sicherheitstyp, beispielsweise Kerberos v5, NTLM oder AUTH_SYS.

Wenn eine Regel mehrere Kriterien festlegt, muss der Client alle erfüllen, damit die Regel Anwendung findet.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv3-Protokoll gesendet und der Client hat die IP-Adresse 10.1.17.37.

Obwohl das Client-Zugriffsprotokoll übereinstimmt, befindet sich die IP-Adresse des Clients in einem anderen Subnetz als dem in der Exportregel angegebenen. Daher schlägt die Clientzuordnung fehl und diese Regel gilt

für diesen Client nicht.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

Die Clientzugriffsanfrage wird mit dem NFSv4-Protokoll gesendet und der Client hat die IP-Adresse 10.1.16.54.

Das Protokoll für den Dateizugriff stimmt überein und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientübereinstimmung erfolgreich und diese Regel gilt für diesen Client. Der Client erhält unabhängig von seinem Sicherheitstyp lesen/schreiben-Zugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit folgenden Parametern:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Client #1 hat die IP-Adresse 10.1.16.207, sendet eine Zugriffsanfrage über das NFSv3-Protokoll und hat sich mit Kerberos v5 authentifiziert.

Client #2 hat die IP-Adresse 10.1.16.211, sendet eine Zugriffsanfrage mit dem NFSv3-Protokoll und hat sich mit AUTH_SYS authentifiziert.

Das Clientzugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der Parameter „Schreibgeschützt“ ermöglicht allen Clients Lesezugriff, unabhängig vom Sicherheitstyp, mit dem sie sich authentifiziert haben. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese- und Schreibzugriff, da er sich mit dem genehmigten Sicherheitstyp Kerberos v5 authentifiziert hat. Client #2 erhält keinen Lese- und Schreibzugriff.

Beispiele für ONTAP Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen

Die Beispiele zeigen, wie Exportrichtlinienregeln erstellt werden, die den Zugriff über SMB auf einer SVM einschränken oder zulassen, auf der Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für den SMB-Zugriff sind standardmäßig deaktiviert. Exportrichtlinienregeln, die den Zugriff über SMB einschränken oder zulassen, sind nur zu konfigurieren, wenn Exportrichtlinien für den SMB-Zugriff aktiviert wurden.

Exportregel nur für SMB-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: cifs1
- Indexnummer: 1
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Für Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese- und Schreibzugriff: Für Clients mit Kerberos-Authentifizierung

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Exportregel für SMB- und NFS-Zugriff

Der folgende Befehl erstellt eine Exportregel auf der SVM namens "vs1", die die folgende Konfiguration aufweist:

- Richtlinienname: cifsnfs1
- Indexnummer: 2
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: SMB und NFS-Zugriff
- Nur-Lese-Zugriff: Für alle Clients
- Lese- und Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zuordnung zur Benutzer-ID 65534 (die typischerweise dem Benutzernamen nobody zugeordnet ist)
- SUID- und SGID-Zugriff: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch
192.168.1.0/255.255.255.0 -rorule any -rwrule krb5,ntlm -anon 65534 -allow
-suid true
```

Exportregel für SMB-Zugriff ausschließlich über NTLM

Der folgende Befehl erstellt eine Exportregel auf der SVM mit dem Namen “vs1”, die die folgende Konfiguration aufweist:

- Richtlinienname: ntlm1

- Indexnummer: 1
- Client-Übereinstimmung: Es werden nur Clients im Netzwerk 192.168.1.0/24 abgeglichen.
- Protokoll: Ermöglicht nur SMB-Zugriff
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese- und Schreibzugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die Option „Nur lesen“ oder „Lesen/Schreiben“ für den NTLM-only-Zugriff konfigurieren, müssen Sie IP-adressbasierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies ist darauf zurückzuführen, dass ONTAP bei Verwendung eines Hostnamens zur Überprüfung der Zugriffsrechte des Clients Kerberos Service Principal Names (SPN) verwendet. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule ntlm -rwrule ntlm
```

ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren

Sie können Exportrichtlinien für den SMB-Zugriff auf Storage Virtual Machines (SVMs) aktivieren oder deaktivieren. Die Verwendung von Exportrichtlinien zur Steuerung des SMB-Zugriffs auf Ressourcen ist optional.

Bevor Sie beginnen

Die folgenden Voraussetzungen gelten für die Aktivierung von Exportrichtlinien für SMB:

- Der Client muss über einen "PTR"-Eintrag im DNS verfügen, bevor die Exportregeln für diesen Client erstellt werden.
- Ein zusätzlicher Satz von „A“- und „PTR“-Einträgen für Hostnamen ist erforderlich, wenn die SVM Zugriff auf NFS-Clients bereitstellt und der Hostname, der für den NFS-Zugriff verwendet werden soll, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für den SMB-Zugriff standardmäßig deaktiviert. Exportrichtlinien für den SMB-Zugriff können aktiviert werden, wenn der Zugriff basierend auf Authentifizierungsprotokoll, Client-IP-Adressen oder Hostnamen gesteuert werden soll. Exportrichtlinien für den SMB-Zugriff können jederzeit aktiviert oder deaktiviert werden.

> Durch die Aktivierung von Exportrichtlinien für CIFS/SMB in einer NFS-fähigen SVM kann ein Linux-Client den `showmount -e` Befehl auf der SVM verwenden, um die Verbindungspfade aller SMB-Volumes mit zugehörigen Exportrichtlinienregeln anzuzeigen.

Schritte

1. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`

2. Exportrichtlinien aktivieren oder deaktivieren:
   - Exportrichtlinien aktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - Exportrichtlinien deaktivieren: `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. Zurück zur Administratorrechteebene: `set -privilege admin`

Beispiel

Das folgende Beispiel ermöglicht die Verwendung von Exportrichtlinien zur Steuerung des SMB-Clientzugriffs auf Ressourcen auf SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Die SMB-Exportregel des ONTAP SVM-Root-Volumes öffnen

Wenn Sie SMB-Exportrichtlinienregeln aktiviert haben, muss die Standardexportrichtlinie des SVM-Root-Volumes eine Regel enthalten, die allen Clients offenen Zugriff über SMB erlaubt. Ohne eine solche Regel wird allen SMB-Clients der Zugriff auf die SVM und ihre Volumes verweigert. Exportrichtlinienregeln sind standardmäßig deaktiviert.

Über diese Aufgabe

Wenn eine neue SVM erstellt wird, wird automatisch eine Standard-Exportregel (genannt default) für das Root-Volume der SVM erstellt. Es müssen eine oder mehrere Regeln für die Standard-Exportregel erstellt werden, bevor Clients auf Daten auf der SVM zugreifen können.

Es empfiehlt sich zu überprüfen, ob der gesamte SMB-Zugriff in der Standard-Exportregel offen ist, und den Zugriff auf einzelne Volumes später durch das Erstellen benutzerdefinierter Exportregeln für einzelne Volumes oder qtrees einzuschränken.

Schritte

1. Wenn Sie eine vorhandene SVM verwenden, überprüfen Sie die Standard-Exportregel für das Root-Volume: `vserver export-policy rule show`

   Die Ausgabe des Befehls sollte in etwa wie folgt aussehen:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance
   ```

```
                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Existiert eine solche Regel, die offenen Zugang erlaubt, ist diese Aufgabe abgeschlossen. Falls nicht, folgt der nächste Schritt.

2. Eine Exportregel für das SVM-Root-Volume erstellen: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Die Regelerstellung kann mithilfe des `vserver export-policy rule show` Befehls überprüft werden.

Ergebnisse

Jeder SMB-Client kann nun auf jedes Volume oder jeden Qtree zugreifen, der auf der SVM erstellt wurde.

Verwandte Informationen

"Erfahren Sie, wie Sie ONTAP Exportrichtlinien für den SMB-Zugriff aktivieren oder deaktivieren".

Copyright-Informationen

Copyright © 2026 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.