Sicherer SMB-Zugriff über Exportrichtlinien

ONTAP 9

NetApp
February 12, 2026

Inhalt

Sicherer SMB-Zugriff über Exportrichtlinien

Erfahren Sie mehr über die Verwendung von Exportrichtlinien mit ONTAP SMB-Zugriff

Wenn Exportrichtlinien für SMB-Zugriff auf dem SMB-Server aktiviert sind, werden Exportrichtlinien verwendet, um den Zugriff auf SVM-Volumes durch SMB-Clients zu steuern. Um auf Daten zuzugreifen, können Sie eine Exportrichtlinie erstellen, über die SMB-Zugriff möglich ist, und die Richtlinie dann den Volumes mit SMB-Freigaben zuordnen.

Eine Exportrichtlinie hat eine oder mehrere Regeln angewendet, die festlegen, welche Clients Zugriff auf die Daten haben und welche Authentifizierungsprotokolle für schreibgeschützten und schreibgeschützten Zugriff unterstützt werden. Sie können Exportrichtlinien konfigurieren, um allen Clients, einem Subnetz von Clients oder einem bestimmten Client den Zugriff über SMB zu ermöglichen, und um die Authentifizierung über Kerberos-Authentifizierung, NTLM-Authentifizierung oder sowohl Kerberos- als auch NTLM-Authentifizierung zu ermöglichen, wenn der schreibgeschützten und der Lese-/Schreibzugriff auf Daten bestimmt wird.

Nach der Verarbeitung aller auf die Exportrichtlinie angewandten Exportregeln kann ONTAP bestimmen, ob dem Client der Zugriff gewährt wird und welche Zugriffsstufe gewährt wird. Exportregeln gelten für Clientcomputer, nicht für Windows-Benutzer und -Gruppen. Exportregeln ersetzen die Authentifizierung und Autorisierung von Windows-Benutzern und -Gruppen nicht. Exportregeln bieten zusätzlich zu Freigabeberechtigungen und Zugriffsberechtigungen eine weitere Zugriffsebene.

Sie ordnen jedem Volume genau eine Exportrichtlinie zu, um den Client-Zugriff auf das Volume zu konfigurieren. Jede SVM kann mehrere Exportrichtlinien enthalten. Dies ermöglicht Ihnen bei SVMs mit mehreren Volumes folgende Aufgaben:

- Jedem Volume der SVM sollten für jedes Volume in der SVM unterschiedliche Exportrichtlinien zugewiesen werden, um für jedes Volume in der SVM eine individuelle Client-Zugriffskontrolle zu ermöglichen.
- Weisen Sie für eine identische Client-Zugriffskontrolle dieselbe Exportrichtlinie mehreren Volumes der SVM zu, ohne für jedes Volume eine neue Exportrichtlinie erstellen zu müssen.

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

Sie können Regeln konfigurieren, die Zugriff auf NFS- und SMB-Hosts gewähren, und diese Regel einer Exportrichtlinie zuordnen. Diese kann dann dem Volume zugeordnet werden, das Daten enthält, auf die sowohl NFS- als auch SMB-Hosts zugreifen müssen. Falls es einige Volumes gibt, auf denen nur SMB-Clients Zugriff benötigen, können Sie eine Exportrichtlinie mit Regeln konfigurieren, die nur den Zugriff über das SMB-Protokoll gestattet. Darüber hinaus wird nur Kerberos oder NTLM (oder beides) für die Authentifizierung für Read-Only- und Write-Zugriff verwendet. Die Exportrichtlinie wird dann den Volumes zugeordnet, auf denen nur SMB-Zugriff gewünscht wird.

Wenn Exportrichtlinien für SMB aktiviert sind und ein Client eine Zugriffsanfrage stellt, die von der entsprechenden Exportrichtlinie nicht zulässig ist, schlägt die Anforderung mit einer Meldung, die eine Berechtigung verweigert hat, fehl. Wenn ein Client keine Regeln in der Exportrichtlinie des Volumes erfüllt, wird der Zugriff verweigert. Wenn eine Exportrichtlinie leer ist, werden alle Zugriffe implizit verweigert. Dies gilt auch dann, wenn die Freigabe- und Dateiberechtigungen ansonsten den Zugriff erlauben würden. Das bedeutet,

dass Sie Ihre Exportrichtlinie so konfigurieren müssen, dass bei Volumes mit SMB-Freigaben Folgendes minimal zulässig ist:

- Zugriff auf alle Clients oder die entsprechende Untergruppe von Clients zulassen
- Zugriff über SMB zulassen
- Mit Kerberos- oder NTLM-Authentifizierung (oder beides) ist ein angemessener Lese- und Schreibzugriff möglich.

Erfahren Sie mehr über "Konfigurieren und Verwalten von Exportrichtlinien".

Erfahren Sie mehr über die ONTAP SMB-Exportregeln

Exportregeln sind die funktionalen Elemente einer Exportrichtlinie. Exportregeln stimmen die Client-Zugriffsanforderungen auf ein Volume ab. Dabei werden bestimmte Parameter verwendet, die Sie konfigurieren, um zu bestimmen, wie die Clientzugriffsanforderungen verarbeitet werden sollen.

Eine Exportrichtlinie muss mindestens eine Exportregel enthalten, um den Zugriff auf Clients zu ermöglichen. Wenn eine Exportrichtlinie mehrere Regeln enthält, werden die Regeln in der Reihenfolge verarbeitet, in der sie in der Exportrichtlinie angezeigt werden. Die Regelreihenfolge wird durch die Indexnummer der Regel vorgegeben. Stimmt eine Regel mit einem Client überein, werden die Berechtigungen dieser Regel verwendet und keine weiteren Regeln verarbeitet. Stimmen keine Regeln überein, wird dem Client der Zugriff verweigert.

Sie können Exportregeln konfigurieren, um Clientzugriffsberechtigungen anhand der folgenden Kriterien zu ermitteln:

- Das Dateizugriffsprotokoll, das vom Client verwendet wird, der die Anforderung sendet, z. B. NFSv4 oder SMB.
- Eine Client-ID, z. B. Hostname oder IP-Adresse.

  Die maximale Größe für das `-clientmatch` Feld beträgt 4096 Zeichen.

- Der vom Client zum Authentifizieren verwendete Sicherheitstyp, z. B. Kerberos v5, NTLM oder AUTH_SYS.

Wenn in einer Regel mehrere Kriterien angegeben sind, muss der Client alle Kriterien erfüllen, damit die Regel angewendet werden kann.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

Die Client-Zugriffsanforderung 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 Clientabgleich fehl, und diese Regel gilt nicht für diesen Client.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den folgenden Parametern:

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

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

Das Client-Zugriffsprotokoll stimmt überein, und die IP-Adresse des Clients befindet sich im angegebenen Subnetz. Daher ist die Clientabgleich erfolgreich, und diese Regel gilt für diesen Client. Der Client erhält unabhängig vom Sicherheitstyp Lese-/Schreibzugriff.

Beispiel

Die Exportrichtlinie enthält eine Exportregel mit den 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 authentifiziert mit Kerberos v5.

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

Das Client-Zugriffsprotokoll und die IP-Adresse stimmen für beide Clients überein. Der schreibgeschützte Parameter ermöglicht den schreibgeschützten Zugriff auf alle Clients unabhängig vom Sicherheitstyp, mit dem sie authentifiziert wurden. Daher erhalten beide Clients nur Lesezugriff. Allerdings erhält nur Client #1 Lese-Schreib-Zugriff, weil er den genehmigten Sicherheitstyp Kerberos v5 zur Authentifizierung verwendet hat. Client #2 erhält keinen Lese-/Schreibzugriff.

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

Die Beispiele zeigen, wie man Richtlinien für den Export erstellt, die den Zugriff auf SMB für eine SVM einschränken oder zulassen, deren Exportrichtlinien für SMB-Zugriff aktiviert sind.

Exportrichtlinien für SMB-Zugriff sind standardmäßig deaktiviert. Sie müssen Richtlinien für den Export konfigurieren, die den Zugriff über SMB einschränken oder zulassen, nur wenn Sie Exportrichtlinien für SMB-Zugriff aktiviert haben.

Exportregel nur für SMB-Zugriff

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „vs1“ erstellt, die die folgende Konfiguration hat:

- Richtlinienname: Ziff1
- Indexnummer: 1
- Client Match: Entspricht nur Clients im 192.168.1.0/24 Netzwerk
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Auf Clients mit NTLM- oder Kerberos-Authentifizierung
- Lese-Schreib-Zugriff für Clients, die Kerberos-Authentifizierung verwenden

```
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

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „` vs1`“ erstellt, die die folgende Konfiguration hat:

- Policy Name: Cifsnfs1
- Indexnummer: 2
- Client-Match: Entspricht allen Clients
- Protokoll: SMB- und NFS-Zugriff
- Schreibgeschützter Zugriff: Für alle Clients
- Lese-Schreibzugriff: Für Clients, die Kerberos (NFS und SMB) oder NTLM-Authentifizierung (SMB) verwenden
- Zuordnung für UNIX-Benutzer-ID 0 (Null): Zugeordnet zu Benutzer-ID 65534 (die typischerweise dem Benutzernamen niemand zugeordnet ist)
- SUID und sgid Access: Ermöglicht

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Exportregel für SMB-Zugriff nur mit NTLM

Mit dem folgenden Befehl wird eine Exportregel für die SVM mit dem Namen „vs1“ erstellt, die die folgende Konfiguration hat:

- Policy-Name: Ntlm1
- Indexnummer: 1

- Client-Match: Entspricht allen Clients
- Protokoll: Nur SMB-Zugriff möglich
- Schreibgeschützter Zugriff: Nur für Clients, die NTLM verwenden
- Lese-Schreib-Zugriff: Nur für Clients, die NTLM verwenden

> Wenn Sie die schreibgeschützte Option oder die Lese-Schreib-Option für NTLM-Only-Zugriff konfigurieren, müssen Sie IP-address-basierte Einträge in der Client-Match-Option verwenden. Andernfalls erhalten Sie `access denied` Fehler. Dies liegt daran, dass ONTAP Kerberos-Dienst-Principal-Namen (SPN) verwendet, wenn ein Hostname verwendet wird, um die Zugriffsrechte des Clients zu überprüfen. NTLM-Authentifizierung unterstützt keine SPN-Namen.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Aktivieren oder Deaktivieren von ONTAP-Exportrichtlinien für den SMB-Zugriff

Sie können Exportrichtlinien für 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

Nachfolgend sind die Anforderungen für die Aktivierung von Exportrichtlinien für SMB aufgeführt:

- Der Client muss über einen „PTR“-Datensatz in DNS verfügen, bevor Sie die Exportregeln für diesen Client erstellen.
- Ein zusätzlicher Satz von „A“- und „PTR“-Datensätzen für Hostnamen ist erforderlich, wenn die SVM den Zugriff auf NFS-Clients ermöglicht, und der Hostname, den Sie für den NFS-Zugriff verwenden möchten, sich vom CIFS-Servernamen unterscheidet.

Über diese Aufgabe

Beim Einrichten eines neuen CIFS-Servers auf Ihrer SVM ist die Verwendung von Exportrichtlinien für SMB-Zugriff standardmäßig deaktiviert. Sie können Exportrichtlinien für SMB-Zugriffe aktivieren, wenn Sie den Zugriff auf Basis des Authentifizierungsprotokoll oder anhand von Client-IP-Adressen oder Host-Namen steuern möchten. Die Exportrichtlinien für 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 mithilfe des Befehls auf der SVM die Verbindungspfade aller SMB-Volumes mit zugehörigen Regeln für `showmount -e` die Exportrichtlinie anzeigen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest: `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. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Beispiel

Im folgenden Beispiel können Exportrichtlinien verwendet werden, um den Zugriff von SMB-Clients auf Ressourcen von SVM vs1 zu kontrollieren:

```
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
```