NFSv4-ACLs verwalten

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nfs-admin/benefits-enable-nfsv4-acls-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

NFSv4-ACLs verwalten . . . 1
Informationen zu den Vorteilen der Aktivierung von NFSv4-ACLs für ONTAP SVMs . . . 1
Informationen zu NFSv4-ACLs für ONTAP SVMs . . . 1
Aktivieren oder Deaktivieren der NFSv4-ACL-Änderung für ONTAP SVMs . . . 2
Wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können . . . 2
NFSv4-ACLs für ONTAP SVMs aktivieren oder deaktivieren . . . 2
Ändern des maximalen ACE-Limits für NFSv4-ACLs für ONTAP SVMs . . . 3

NFSv4-ACLs verwalten

Informationen zu den Vorteilen der Aktivierung von NFSv4-ACLs für ONTAP SVMs

Die Aktivierung von NFSv4 ACLs bietet viele Vorteile.

Die Vorteile der Aktivierung von NFSv4-ACLs umfassen Folgendes:

- Feinere Steuerung des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Verbesserte Interoperabilität mit CIFS
- Aufhebung der NFS-Beschränkung von 16 Gruppen pro Benutzer

Informationen zu NFSv4-ACLs für ONTAP SVMs

Ein Client, der NFSv4-ACLs verwendet, kann ACLs für Dateien und Verzeichnisse im System festlegen und anzeigen. Wenn in einem Verzeichnis mit einer ACL eine neue Datei oder ein neues Unterverzeichnis erstellt wird, erbt die neue Datei bzw. das neue Unterverzeichnis alle Zugriffssteuerungseinträge (ACEs) in der ACL, die mit den entsprechenden Vererbungsflags versehen sind.

Wird eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anfrage erstellt, hängt die ACL der resultierenden Datei oder des resultierenden Verzeichnisses davon ab, ob die Dateierstellungsanfrage eine ACL oder nur die standardmäßigen UNIX-Dateizugriffsberechtigungen enthält und ob das übergeordnete Verzeichnis über eine ACL verfügt:

- Wenn die Anfrage eine ACL enthält, wird diese ACL verwendet.
- Enthält die Anfrage lediglich Standard-UNIX-Dateizugriffsberechtigungen, verfügt das übergeordnete Verzeichnis jedoch über eine ACL, werden die ACEs in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis übernommen, sofern die ACEs mit den entsprechenden Vererbungsflags versehen wurden.

  Eine übergeordnete ACL wird auch dann vererbt, wenn `-v4.0-acl` auf `off` gesetzt ist.

- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL hat, wird der Client-Dateimodus verwendet, um die Standard-UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anfrage nur Standard-UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis eine nicht vererbbare ACL hat, wird das neue Objekt nur mit Modusbits erstellt.

Wenn der `-chown-mode` Parameter auf `restricted` mit Befehlen aus den `vserver nfs`- oder `vserver export-policy rule`-Familien gesetzt wurde, kann die Dateibesitzberechtigung nur vom Superuser geändert werden, selbst wenn die mit NFSv4-ACLs festgelegten Berechtigungen auf der Festplatte es einem Nicht-Root-Benutzer erlauben, die Dateibesitzberechtigung zu ändern. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Aktivieren oder Deaktivieren der NFSv4-ACL-Änderung für ONTAP SVMs

Wenn ONTAP einen `chmod` Befehl für eine Datei oder ein Verzeichnis mit einer ACL empfängt, wird die ACL standardmäßig beibehalten und entsprechend der Änderung des Modusbits angepasst. Es besteht die Möglichkeit, den `-v4-acl-preserve` Parameter zu deaktivieren, wodurch das Verhalten geändert wird, sodass die ACL stattdessen entfernt wird.

Über diese Aufgabe

Bei Verwendung des einheitlichen Sicherheitsstils legt dieser Parameter auch fest, ob die NTFS-Dateiberechtigungen erhalten bleiben oder verworfen werden, wenn ein Client einen chmod, chgroup oder chown Befehl für eine Datei oder ein Verzeichnis sendet.

Dieser Parameter ist standardmäßig aktiviert.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Beibehaltung und Änderung bestehender NFSv4-ACLs (Standard) ermöglichen	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Beibehaltung deaktivieren und NFSv4-ACLs beim Ändern der Modusbits entfernen	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

Wie ONTAP NFSv4-ACLs verwendet, um zu bestimmen, ob Dateien gelöscht werden können

Um festzustellen, ob eine Datei gelöscht werden kann, verwendet ONTAP eine Kombination aus dem DELETE-Bit der Datei und dem DELETE_CHILD-Bit des übergeordneten Verzeichnisses. Weitere Informationen enthält die NFS 4.1 RFC 5661.

NFSv4-ACLs für ONTAP SVMs aktivieren oder deaktivieren

Um NFSv4-ACLs zu aktivieren oder zu deaktivieren, können die Optionen `-v4.0-acl` und `-v4.1-acl` geändert werden. Diese Optionen sind standardmäßig deaktiviert.

Über diese Aufgabe

Die `-v4.0-acl` oder `-v4.1-acl` Option steuert das Festlegen und Anzeigen von NFSv4-ACLs; sie steuert nicht die Durchsetzung dieser ACLs für die Zugriffsprüfung.

Schritt

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie möchten…	Dann…
NFSv4.0-ACLs aktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACLs deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1-ACLs aktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
NFSv4.1 ACLs deaktivieren	Führen Sie den folgenden Befehl aus: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Ändern des maximalen ACE-Limits für NFSv4-ACLs für ONTAP SVMs

Sie können die maximale Anzahl zulässiger ACEs für jede NFSv4-ACL durch Ändern des Parameters `-v4-acl-max-aces` anpassen. Standardmäßig ist das Limit auf 400 ACEs pro ACL festgelegt. Eine Erhöhung dieses Limits kann dazu beitragen, die erfolgreiche Migration von Daten mit ACLs, die mehr als 400 ACEs enthalten, auf Speichersysteme mit ONTAP sicherzustellen.

Über diese Aufgabe

Eine Erhöhung dieses Grenzwerts könnte die Leistung von Clients beeinträchtigen, die auf Dateien mit NFSv4-ACLs zugreifen.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Das maximale ACE-Limit für NFSv4-ACLs ändern:

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   Der gültige Bereich von

`max_ace_limit` ist `192` zu `1024`.

3. Zurück zur Administrator-Privilegstufe:

   ```
   set -privilege admin
   ```

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.