Dateisperren verwalten

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/smb-admin/file-locking-between-protocols-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Dateisperren verwalten 1
Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen 1
Informationen zu schreibgeschützten Bits in ONTAP SMB 2
Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet 3
Informationen zu ONTAP SMB-Sperren anzeigen 3
ONTAP SMB-Sperren aufheben 5

Dateisperren verwalten

Informationen zur ONTAP SMB-Dateisperrung zwischen Protokollen

Die Dateisperrung ist eine Methode, mit der Clientanwendungen verhindern, dass ein Benutzer auf eine Datei zugreift, die zuvor von einem anderen Benutzer geöffnet wurde. Wie ONTAP Dateien sperrt, hängt vom Protokoll des Clients ab.

Handelt es sich beim Client um einen NFS-Client, sind Sperren empfehlend; handelt es sich beim Client um einen SMB-Client, sind Sperren obligatorisch.

Aufgrund von Unterschieden zwischen den Dateisperren von NFS und SMB kann es vorkommen, dass ein NFS-Client nicht auf eine Datei zugreifen kann, die zuvor von einer SMB-Anwendung geöffnet wurde.

Folgendes geschieht, wenn ein NFS-Client versucht, auf eine von einer SMB-Anwendung gesperrte Datei zuzugreifen:

- In gemischten oder NTFS-Volumes können Dateimanipulationsvorgänge wie `rm`, `rmdir` und `mv` dazu führen, dass die NFS-Anwendung fehlschlägt.
- NFS-Lese- und Schreibvorgänge werden durch die SMB-Öffnungsmodi deny-read und deny-write jeweils für lesen bzw. schreiben verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei mit einer exklusiven SMB-Bytesperre gesperrt ist.
- Link aufheben
  - Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

    Die Datei wird nach dem letzten Schließen gelöscht.
  - NFS unlink-Operationen werden nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und die Operation „Letztes Löschen beim Schließen“ für NFS nicht unterstützt wird.
  - Für UNIX-Dateisysteme wird die Operation "unlink" unterstützt.

    Es wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.
- Umbenennen
  - Für NTFS-Dateisysteme kann die Zieldatei umbenannt werden, wenn sie über SMB oder CIFS geöffnet wird.
  - NFS-Umbenennung wird nicht unterstützt.

    Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind.

In UNIX-Sicherheitsstil-Volumes ignorieren NFS-Unlink- und Rename-Operationen den SMB-Sperrstatus und ermöglichen den Zugriff auf die Datei. Alle anderen NFS-Operationen auf UNIX-Sicherheitsstil-Volumes berücksichtigen den SMB-Sperrstatus.

Informationen zu schreibgeschützten Bits in ONTAP SMB

Das Schreibschutzbit wird für jede Datei einzeln gesetzt, um anzuzeigen, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients unter Windows können ein schreibgeschütztes Bit pro Datei setzen. NFS-Clients setzen kein schreibgeschütztes Bit pro Datei, da NFS-Clients keine Protokolloperationen haben, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann das Schreibschutzbit einer Datei setzen, wenn diese von einem SMB-Client unter Windows erstellt wird. ONTAP kann das Schreibschutzbit auch setzen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Manche Software erfordert, dass das Schreibschutzbit aktiviert ist, wenn sie von NFS-Clients und SMB-Clients verwendet wird.

Damit ONTAP die korrekten Lese- und Schreibberechtigungen für eine zwischen NFS-Client und SMB-Client gemeinsam genutzte Datei beibehält, wird das Schreibschutzbit nach den folgenden Regeln behandelt:

- NFS behandelt jede Datei, bei der das Schreibschutzbit aktiviert ist, so, als ob keine Schreibberechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Schreibberechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert war, aktiviert ONTAP das Schreibschutzbit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungsbit aktiviert, deaktiviert ONTAP das Nur-Lesen-Bit für diese Datei.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein NFS-Client versucht, die Berechtigungen für die Datei zu ermitteln, werden die Berechtigungsbits für die Datei nicht an den NFS-Client gesendet; stattdessen sendet ONTAP die Berechtigungsbits an den NFS-Client, wobei die Schreibberechtigungsbits maskiert sind.
- Wenn das Schreibschutzbit einer Datei aktiviert ist und ein SMB-Client das Schreibschutzbit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien, bei denen das Schreibschutzbit aktiviert ist, sind nur für root beschreibbar.

Das Schreibschutzbit interagiert mit den ACL- und Unix-Modusbits auf folgende Weise:

Wenn das Schreibschutzbit einer Datei gesetzt ist:

- An der ACL für diese Datei werden keine Änderungen vorgenommen. NFS-Clients sehen dieselbe ACL wie vor dem Setzen des Schreibschutzbits.
- Sämtliche Unix-Modusbits, die Schreibzugriff auf die Datei ermöglichen, werden ignoriert.
- Sowohl NFS- als auch SMB-Clients können die Datei lesen, aber sie können sie nicht verändern.
- ACLs und UNIX-Modusbits werden zugunsten des Schreibschutzbits ignoriert. Das bedeutet, dass selbst wenn die ACL Schreibzugriff erlaubt, das Schreibschutzbit Änderungen verhindert.

Wenn das Schreibschutzbit einer Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff anhand der ACL und der UNIX-Modusbits.
  - Wenn entweder die ACL oder die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei nicht ändern.
  - Wenn weder die ACL noch die UNIX-Modusbits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.

Änderungen an Dateiberechtigungen werden auf SMB-Clients sofort wirksam, auf NFS-Clients hingegen möglicherweise nicht sofort, wenn der NFS-Client das Attribut-Caching aktiviert.

Wie ONTAP sich von Windows bei der Handhabung von Sperren auf freigegebenen Pfadkomponenten unterscheidet

Im Gegensatz zu Windows sperrt ONTAP nicht die einzelnen Komponenten des Pfades zu einer geöffneten Datei, solange die Datei geöffnet ist. Dieses Verhalten betrifft auch SMB-Freigabepfade.

Da ONTAP die einzelnen Pfadkomponenten nicht sperrt, ist es möglich, eine Pfadkomponente oberhalb der geöffneten Datei oder Freigabe umzubenennen, was bei bestimmten Anwendungen zu Problemen führen oder den Freigabepfad in der SMB-Konfiguration ungültig machen kann. Dies kann dazu führen, dass die Freigabe nicht zugänglich ist.

Um Probleme zu vermeiden, die durch das Umbenennen von Pfadkomponenten entstehen, lassen sich Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Informationen über die aktuellen Dateisperren können angezeigt werden, einschließlich der Art der gehaltenen Sperren und des Sperrstatus, Details zu Bytebereichssperren, Sharelock-Modi, Delegation Locks und Opportunistic Locks sowie darüber, ob Sperren mit dauerhaften oder persistenten Handles geöffnet sind.

Über diese Aufgabe

Die Client-IP-Adresse kann für Sperren, die über NFSv4 oder NFSv4.1 eingerichtet wurden, nicht angezeigt werden.

Standardmäßig zeigt der Befehl Informationen zu allen Sperren an. Mit Befehlsparametern lässt sich die Anzeige von Informationen zu Sperren für eine bestimmte Storage Virtual Machine (SVM) steuern oder die Ausgabe des Befehls nach anderen Kriterien filtern.

Der `vserver locks show` Befehl zeigt Informationen über vier Arten von Sperren an:

- Byte-Range-Sperren, die nur einen Teil einer Datei sperren.
- Freigabesperren, die geöffnete Dateien sperren.
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Client-seitige Caching über NFSv4.x steuern.

Durch die Angabe optionaler Parameter lassen sich wichtige Informationen zu jedem Sperrtyp ermitteln. Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Informationen zu Sperren werden mit dem `vserver locks show` Befehl angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen zu einer NFSv4-Sperre für eine Datei mit dem Pfad `/vol1/file1`. Der Zugriffsmodus von Sharelock ist write-deny_none, und die Sperre wurde mit Schreibdelegation gewährt:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

Das folgende Beispiel zeigt detaillierte Oplock- und Sharelock-Informationen zur SMB-Sperre einer Datei mit dem Pfad `/data2/data2_2/intro.pptx`. Ein dauerhafter Handle wird für die Datei mit dem Sharelock-Zugriffsmodus write-deny_none an einen Client mit der IP-Adresse 10.3.1.3 gewährt. Ein Lease-Oplock wird mit dem Oplock-Level Batch gewährt:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP SMB-Sperren aufheben

Wenn Dateisperren den Zugriff von Clients auf Dateien verhindern, können Informationen über die aktuell bestehenden Sperren angezeigt und anschließend bestimmte Sperren aufgehoben werden. Beispiele für Szenarien, in denen das Aufheben von Sperren erforderlich sein kann, sind das Debuggen von Anwendungen.

Über diese Aufgabe

Der `vserver locks break`Befehl ist nur auf der erweiterten Berechtigungsstufe und höher verfügbar. Weitere Informationen zu `vserver locks break` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Um die Informationen zu finden, die Sie zum Aufheben einer Sperre benötigen, verwenden Sie den `vserver locks show` Befehl.

   Weitere Informationen zu `vserver locks show` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced`
3. Führen Sie eine der folgenden Aktionen aus:

Wenn ein Schloss durch Angabe von… aufgehoben werden soll	**Geben Sie den Befehl ein…**
Der SVM Name, der Volumenname, der LIF Name und der Dateipfad	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
Die Lock-ID	`vserver locks break -lockid UUID`

4. Zurück zur Administratorrechteebene: `set -privilege admin`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

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.