



Verwalten von Dateisperren

ONTAP 9

NetApp
February 12, 2026

Inhalt

- Verwalten von Dateisperren 1
 - Erfahren Sie mehr über die ONTAP SMB-Dateisperre zwischen Protokollen 1
 - Erfahren Sie mehr über ONTAP SMB Read-Only-Bits 2
 - Wie sich ONTAP von Windows unterscheidet, wenn es um Sperren von Komponenten des Freigabepfads geht 3
 - Informationen zu ONTAP SMB-Sperren anzeigen 3
 - ONTAP SMB-Sperren knacken 5

Verwalten von Dateisperren

Erfahren Sie mehr über die ONTAP SMB-Dateisperre zwischen Protokollen

Die Dateisperrung wird von Client-Anwendungen verwendet, um zu 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.

Wenn es sich bei dem Client um einen NFS-Client handelt, sind Locks Advisory. Wenn es sich bei dem Client um einen SMB-Client handelt, sind Locks obligatorisch.

Aufgrund der Unterschiede zwischen den Dateisperren für NFS und SMB kann ein NFS-Client nicht auf eine Datei zugreifen, die zuvor von einer SMB-Applikation geöffnet wurde.

Die folgende Meldung tritt auf, wenn ein NFS-Client versucht, auf eine Datei zuzugreifen, die von einer SMB-Applikation gesperrt wurde:

- In gemischten oder NTFS-Volumes `rm rmdir mv` können Dateimanipulationsvorgänge wie, und dazu führen, dass die NFS-Anwendung fehlschlägt.
- Lese- und Schreibvorgänge für NFS werden vom SMB Deny-read- bzw. Deny-Write-Open-Modus verweigert.
- NFS-Schreibvorgänge schlagen fehl, wenn der geschriebene Bereich der Datei durch einen exklusiven SMB-Bytelock gesperrt ist.
- Link Aufheben

- Für NTFS-Dateisysteme werden SMB- und CIFS-Löschvorgänge unterstützt.

Die Datei wird nach dem letzten Schließen entfernt.

- Vorgänge zum Aufheben der Verknüpfung von NFS werden nicht unterstützt.

Dies wird nicht unterstützt, da NTFS- und SMB-Semantik erforderlich sind und der Vorgang Letztes Löschen bei Schließen für NFS nicht unterstützt wird.

- Für UNIX-Dateisysteme wird der Aufheben der Verknüpfung unterstützt.

Dies wird unterstützt, da NFS- und UNIX-Semantik erforderlich sind.

- Umbenennen

- Bei NTFS-Dateisystemen kann die Zieldatei umbenannt werden, wenn die Zieldatei von SMB oder CIFS geöffnet wird.
- NFS-Umbenennung wird nicht unterstützt.

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

In UNIX-Volumes im Sicherheitsstil ignorieren NFS den SMB-Sperrstatus und erlauben den Zugriff auf die Datei. Alle anderen NFS-Vorgänge auf UNIX Volumes im Sicherheitsstil sorgen für den SMB-Lock-Status.

Erfahren Sie mehr über ONTAP SMB Read-Only-Bits

Das schreibgeschützte Bit wird auf Datei-für-Datei-Basis gesetzt, um zu reflektieren, ob eine Datei beschreibbar (deaktiviert) oder schreibgeschützt (aktiviert) ist.

SMB-Clients, die Windows verwenden, können einen schreibgeschützten Bit pro Datei festlegen. NFS-Clients legen kein Leserbit pro Datei fest, da NFS-Clients über keine Protokollvorgänge verfügen, die ein schreibgeschütztes Bit pro Datei verwenden.

ONTAP kann ein schreibgeschütztes Bit auf einer Datei festlegen, wenn ein SMB-Client, der Windows verwendet, diese Datei erstellt. ONTAP kann auch ein schreibgeschütztes Bit festlegen, wenn eine Datei zwischen NFS-Clients und SMB-Clients gemeinsam genutzt wird. Für einige Software, die von NFS-Clients und SMB-Clients verwendet wird, ist die Aktivierung des Read-Only-Bits erforderlich.

Damit ONTAP die entsprechenden Lese- und Schreibberechtigungen auf eine von NFS Clients und SMB Clients gemeinsam genutzte Datei vorhält, behandelt es das schreibgeschützte Bit gemäß den folgenden Regeln:

- NFS behandelt jede Datei mit aktiviertem Read-Only-Bit, als ob keine Write-Berechtigungsbits aktiviert sind.
- Wenn ein NFS-Client alle Write-Berechtigungsbits deaktiviert und mindestens eines dieser Bits zuvor aktiviert wurde, aktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn ein NFS-Client ein Schreibberechtigungs-Bit aktiviert, deaktiviert ONTAP das schreibgeschützte Bit für diese Datei.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein NFS-Client versucht, 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 mit maskierten Schreibberechtigungs-Bits.
- Wenn das schreibgeschützte Bit für eine Datei aktiviert ist und ein SMB-Client das schreibgeschützte Bit deaktiviert, aktiviert ONTAP das Schreibberechtigungsbit des Eigentümers für die Datei.
- Dateien mit aktiviertem Read-Only-Bit sind nur als Root beschreibbar.

Das Nur-Lese-Bit interagiert mit den ACL- und Unix-Modus-Bits auf folgende Weise:

Wenn das Schreibschutzbit für eine Datei gesetzt ist:

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

Wenn das Schreibschutzbit für eine Datei nicht gesetzt ist:

- ONTAP bestimmt den Zugriff basierend auf den ACL- und 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-Modus-Bits den Schreibzugriff verweigern, können NFS- und SMB-Clients die Datei ändern.



Änderungen an Dateiberechtigungen wirken sich unmittelbar auf SMB-Clients aus, wirken sich jedoch möglicherweise nicht unmittelbar auf NFS-Clients aus, wenn der NFS-Client das Caching von Attributen ermöglicht.

Wie sich ONTAP von Windows unterscheidet, wenn es um Sperren von Komponenten des Freigabepfads geht

Im Gegensatz zu Windows sperrt ONTAP nicht jede Komponente des Pfads zu einer geöffneten Datei, während die Datei geöffnet ist. Dieses Verhalten wirkt sich auch auf die SMB-Freigabungspfade aus.

Da ONTAP nicht jede Komponente des Pfads sperrt, ist es möglich, eine Pfadkomponente über der offenen Datei oder Freigabe umzubenennen, was zu Problemen für bestimmte Anwendungen führen kann oder dass der Freigabepfad in der SMB-Konfiguration ungültig ist. Dies kann dazu führen, dass der Share nicht zugänglich ist.

Um Probleme zu vermeiden, die durch die Umbenennung von Pfadkomponenten verursacht werden, können Sie Sicherheitseinstellungen anwenden, die verhindern, dass Benutzer oder Anwendungen kritische Verzeichnisse umbenennen.

Informationen zu ONTAP SMB-Sperren anzeigen

Sie können Informationen über die aktuellen Dateisperren anzeigen, einschließlich der Arten von Sperren und des Sperrstatus, Informationen über Byte-Range-Sperren, Sharlock-Modi, Delegierter Sicherungen und opportunistische Sperren sowie darüber, ob Sperren mit langlebigen oder dauerhaften Griffen geöffnet werden.

Über diese Aufgabe

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

Standardmäßig werden mit dem Befehl Informationen zu allen Sperren angezeigt. Mit den Befehlsparametern können Informationen über Sperren für eine bestimmte Storage Virtual Machine (SVM) angezeigt oder die Ausgabe des Befehls nach anderen Kriterien gefiltert werden.

Mit dem `vserver locks show` Befehl werden Informationen zu vier Arten von Sperren angezeigt:

- Byte-Bereich-Locks, die nur einen Teil einer Datei sperren.
- Sperren freigeben, die geöffnete Dateien sperren
- Opportunistische Sperren, die das Client-seitige Caching über SMB steuern.
- Delegationen, die das Caching des Clients über NFSv4.x steuern

Durch die Angabe optionaler Parameter können Sie wichtige Informationen zu jedem Sperrtyp ermitteln. Erfahren Sie mehr über `vserver locks show` in der ["ONTAP-Befehlsreferenz"](#).

Schritt

1. Mit dem `vserver locks show` Befehl werden Informationen über Sperren angezeigt.

Beispiele

Das folgende Beispiel zeigt zusammenfassende Informationen für eine NFSv4-Sperre auf einer Datei mit dem Pfad an /vol1/file1. Der Zugriffsmodus für sharlock ist write-Deny_none, und die Sperre wurde mit der 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 über die SMB-Sperre in einer Datei mit dem Pfad /data2/data2_2/intro.pptx. Ein dauerhafter Handle wird auf der Datei mit einem Zugriffsmodus für die Freigabesperre von write-Deny_none einem Client mit einer IP-Adresse von 10.3.1.3 gewährt. Ein Lease Oplock wird mit einem Batch-Oplock-Niveau 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: 553cf484-7030-4998-88d3-1125adbbba0b7
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 knacken

Wenn Dateisperren den Client-Zugriff auf Dateien verhindern, können Sie Informationen zu derzeit gespeicherten Sperren anzeigen und bestimmte Sperren anschließend unterbrechen. Beispiele für Szenarien, in denen Sie Sperren benötigen, sind Debugging-Anwendungen.

Über diese Aufgabe

Der `vserver locks break` Befehl ist nur auf der erweiterten Berechtigungsebene und höher verfügbar. Erfahren Sie mehr über `vserver locks break` in der ["ONTAP-Befehlsreferenz"](#).

Schritte

1. Um die Informationen zu finden, die Sie benötigen, um eine Sperre `vserver locks show` zu brechen, verwenden Sie den Befehl.

Erfahren Sie mehr über `vserver locks show` in der ["ONTAP-Befehlsreferenz"](#).

2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced`

3. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie eine Sperre brechen möchten, indem Sie...	Geben Sie den Befehl ein...
Der Name der SVM, der Name des Volumes, der LIF-Name und der Dateipfad	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
Die Lock-ID	<code>vserver locks break -lockid UUID</code>

4. Kehren Sie zur Administrator-Berechtigungsebene zurück: `set -privilege admin`

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im ["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 IRGEND EINER 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.