



Manage file locks

ONTAP 9

NetApp
February 20, 2026

Table of Contents

- Manage file locks 1
 - Learn about ONTAP SMB file locking between protocols 1
 - Learn about ONTAP SMB read-only bits 1
 - How ONTAP differs from Windows in handling locks on share path components 2
 - Display information about ONTAP SMB locks 3
 - Break ONTAP SMB locks 5

Manage file locks

Learn about ONTAP SMB file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

- Unlink

- For NTFS filesystems, SMB and CIFS delete operations are supported.

The file will be removed after the last close.

- NFS unlink operations are not supported.

It is not supported because NTFS and SMB semantics are required, and the Last Delete-On-Close operation is not supported for NFS.

- For UNIX filesystems, unlink operation is supported.

It is supported because NFS and UNIX semantics are required.

- Rename

- For NTFS filesystems, if the destination file is opened from SMB or CIFS, the destination file can be renamed.

- NFS rename is not supported.

It is not supported because NTFS and SMB semantics are required.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

Learn about ONTAP SMB read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit

because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner's write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

The read-only bit interacts with the ACL and Unix mode bits in the following ways:

When the read-only bit is set on a file:

- No changes are made to the ACL for that file. NFS clients will see the same ACL as before the read-only bit was set.
- Any Unix mode bits that allow write access for the file are ignored.
- Both NFS and SMB clients can read the file, but they cannot modify it.
- ACLs and UNIX mode bits are ignored in favor of the read-only bit. This means that even if the ACL allows write access, the read-only bit prevents modifications.

When the read-only bit is not set on a file:

- ONTAP determines access based on the ACL and UNIX mode bits.
 - If either the ACL or the UNIX mode bits deny write access, then NFS and SMB clients cannot modify the file.
 - If neither the ACL nor UNIX mode bits deny write access, then NFS and SMB clients can modify the file.



Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How ONTAP differs from Windows in handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

Display information about ONTAP SMB locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. Learn more about `vserver locks show` in the [ONTAP command reference](#).

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is `write-deny_none`, and the lock was granted with write delegation:

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
-----	-----	-----	-----	-----	-----

voll1	/voll1/file1	lif1	nfsv4	share-level	-
	Sharelock Mode: write-deny_none				
				delegation	-
	Delegation Type: write				

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path /data2/data2_2/intro.pptx. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
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
```

Break ONTAP SMB locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. Learn more about `vserver locks break` in the [ONTAP command reference](#).

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

Learn more about `vserver locks show` in the [ONTAP command reference](#).

2. Set the privilege level to advanced: `set -privilege advanced`
3. Perform one of the following actions:

If you want to break a lock by specifying...	Enter the command...
The SVM name, volume name, LIF name, and file path	<pre>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</pre>
The lock ID	<pre>vserver locks break -lockid UUID</pre>

4. Return to the admin privilege level: `set -privilege admin`

Learn more about the commands described in this procedure in the [ONTAP command reference](#).

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.