



# **Supported NFS versions and clients**

## **ONTAP 9**

NetApp  
February 20, 2023

# Table of Contents

- Supported NFS versions and clients . . . . . 1
  - Overview of supported NFS versions and clients . . . . . 1
  - NFSv4.0 functionality supported by ONTAP . . . . . 1
  - Limitations of ONTAP support for NFSv4. . . . . 2
  - ONTAP support for NFSv4.1 . . . . . 2
  - ONTAP support for NFSv4.2 . . . . . 3
  - ONTAP support for parallel NFS . . . . . 4
  - Use of hard mounts . . . . . 4

# Supported NFS versions and clients

## Overview of supported NFS versions and clients

Before you can use NFS in your network, you need to know which NFS versions and clients ONTAP supports.

This table notes when major and minor NFS protocol versions are supported by default in ONTAP. Support by default does not indicate that this is the earliest version of ONTAP supporting that NFS protocol.

| Version | Enabled by default              |
|---------|---------------------------------|
| NFSv3   | Yes                             |
| NFSv4.0 | Yes, beginning with ONTAP 9.9.1 |
| NFSv4.1 | Yes, beginning with ONTAP 9.9.1 |
| NFSv4.2 | Yes, beginning with ONTAP 9.9.1 |
| pNFS    | No                              |

For the latest information about which NFS clients ONTAP supports, see the Interoperability Matrix.

[NetApp Interoperability Matrix Tool](#)

## NFSv4.0 functionality supported by ONTAP

ONTAP supports all the mandatory functionality in NFSv4.0 except the SPKM3 and LIPKEY security mechanisms.

The following NFSV4 functionality is supported:

- **COMPOUND**

Allows a client to request multiple file operations in a single remote procedure call (RPC) request.

- **File delegation**

Allows the server to delegate file control to some types of clients for read and write access.

- **Pseudo-fs**

Used by NFSv4 servers to determine mount points on the storage system. There is no mount protocol in NFSv4.

- **Locking**

Lease-based. There are no separate Network Lock Manager (NLM) or Network Status Monitor (NSM) protocols in NFSv4.

For more information about the NFSv4.0 protocol, see RFC 3530.

## Limitations of ONTAP support for NFSv4

You should be aware of several limitations of ONTAP support for NFSv4.

- The delegation feature is not supported by every client type.
- In ONTAP 9.4 and earlier releases, names with non-ASCII characters on volumes other than UTF8 volumes are rejected by the storage system.

In ONTAP 9.5 and later releases, volumes created with the utf8mb4 language setting and mounted using NFS v4 are no longer subject to this restriction.

- All file handles are persistent; the server does not give volatile file handles.
- Migration and replication are not supported.
- NFSv4 clients are not supported with read-only load-sharing mirrors.

ONTAP routes NFSv4 clients to the source of the load-sharing mirror for direct read and write access.

- Named attributes are not supported.
- All recommended attributes are supported, except for the following:

- archive
- hidden
- homogeneous
- mimetype
- quota\_avail\_hard
- quota\_avail\_soft
- quota\_used
- system
- time\_backup



Although it does not support the `quota*` attributes, ONTAP does support user and group quotas through the RQUOTA side band protocol.

## ONTAP support for NFSv4.1

Beginning with ONTAP 9.8, nconnect functionality is available by default when NFSv4.1 is enabled.

Earlier NFS client implementations use only a single TCP connection with a mount. In ONTAP, a single TCP connection can become a bottleneck with increasing IOPS. However, an nconnect-enabled client can have multiple TCP connections (up to 16) associated with a single NFS mount. Such an NFS client multiplexes file operations onto multiple TCP connections in a round-robin fashion and thus obtains higher throughput from the available network bandwidth. Nconnect is recommended for NFSv3 and NFSv4.1 mounts only.

See your NFS client documentation to confirm whether nconnect is supported in your client version.

NFSv4.1 is enabled by default in ONTAP 9.9.1 and later. In earlier releases, you can enable it by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM).

ONTAP does not support NFSv4.1 directory and file level delegations.

## ONTAP support for NFSv4.2

Beginning with ONTAP 9.8, the NFSv4.2 protocol is supported to allow access for NFSv4.2-enabled clients.

NFSv4.2 is enabled by default in ONTAP 9.9.1 and later. In ONTAP 9.8, you can enable v4.2 by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM). Enabling NFSv4.1 also enables clients to use the NFSv4.1 features while mounted as v4.2.

The following NFSv4.2 optional features are supported:

| Feature                                     | Supported beginning with ... |
|---|------------------------------|
| Mandatory Access Control (MAC) labelled NFS | ONTAP 9.9.1                  |
| NFS extended attributes                     | ONTAP 9.12.1                 |

Additional NFSv4.2 optional features will be added in a later ONTAP release.

### Enable NFS v4.2 security labels

Beginning with ONTAP 9.9.1, NFS security labels can be enabled. They are disabled by default.

With NFS v4.2 security labels, ONTAP NFS servers are Mandatory Access Control (MAC) aware, storing and retrieving `sec_label` attributes sent by clients.

For more information, see [RFC 7240](#)

Beginning with ONTAP 9.12.1, NFS v4.2 security labels are supported for NDMP dump operations. If security labels are encountered on files or directories in earlier releases, the dump fails.

#### Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Enable security labels:

```
vserver nfs modify -vserver svm_name -v4.2-seclabel enabled
```

### Enable NFS extended attributes

Beginning with ONTAP 9.12.1, NFS extended attributes (xattrs) are enabled by default.

Extended attributes are standard NFS attributes defined by [RFC 8276](#) and enabled in modern NFS clients. They can be used to attach user-defined metadata to file system objects, and are of interest in advanced security deployments.

NFS extended attributes are not currently supported for NDMP dump operations. If extended attributes are encountered on files or directories, the dump proceeds but does not back up the extended attributes on those files or directories.

If you need to disable extended attributes, use the `vserver nfs modify -v4.2-xattrs disabled` command.

## ONTAP support for parallel NFS

ONTAP supports parallel NFS (pNFS). The pNFS protocol offers performance improvements by giving clients direct access to the data of a set of files distributed across multiple nodes of a cluster. It helps clients locate the optimal path to a volume.

## Use of hard mounts

When troubleshooting mounting problems, you need to be sure that you are using the correct mount type. NFS supports two mount types: soft mounts and hard mounts. You should use only hard mounts for reliability reasons.

You should not use soft mounts, especially when there is a possibility of frequent NFS timeouts. Race conditions can occur as a result of these timeouts, which can lead to data corruption.

## Copyright information

Copyright © 2023 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.