Manage NFSv4 ACLs

ONTAP 9

NetApp
August 09, 2022

This PDF was generated from https://docs.netapp.com/us-en/ontap/nfs-admin/benefits-enable-nfsv4-acls-concept.html on August 09, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Manage NFSv4 ACLs . . . 1
- Benefits of enabling NFSv4 ACLs . . . 1
- How NFSv4 ACLs work . . . 1
- Enable or disable modification of NFSv4 ACLs . . . 1
- How ONTAP uses NFSv4 ACLs to determine whether it can delete a file . . . 2
- Enable or disable NFSv4 ACLs . . . 2
- Modify the maximum ACE limit for NFSv4 ACLs . . . 3

Manage NFSv4 ACLs

Benefits of enabling NFSv4 ACLs

There are many benefits to enabling NFSv4 ACLs.

The benefits of enabling NFSv4 ACLs include the following:

- Finer-grained control of user access for files and directories
- Better NFS security
- Improved interoperability with CIFS
- Removal of the NFS limitation of 16 groups per user

How NFSv4 ACLs work

A client using NFSv4 ACLs can set and view ACLs on files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, the new file or subdirectory inherits all ACL Entries (ACEs) in the ACL that have been tagged with the appropriate inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions, and whether the parent directory has an ACL:

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

  A parent ACL is inherited even if `-v4.0-acl` is set to `off`.

- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a non-inheritable ACL, the new object is created only with mode bits.

If the `-chown-mode` parameter has been set to `restricted` with commands in the `vserver nfs` or `vserver export-policy rule` families, file ownership can be changed by the superuser only, even if the on-disk permissions set with NFSv4 ACLs allow a non-root user to change the file ownership. For more information, see the relevant man pages.

Enable or disable modification of NFSv4 ACLs

When ONTAP receives a `chmod` command for a file or directory with an ACL, by default the ACL is retained and modified to reflect the mode bit change. You can disable the `-v4-acl-preserve` parameter to change the behavior if you want the ACL to be dropped

instead.

About this task

When using unified security style, this parameter also specifies whether NTFS file permissions are preserved or dropped when a client sends a chmod, chgroup, or chown command for a file or directory.

The default for this parameter is enabled.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the following command…
Enable retention and modification of existing NFSv4 ACLs (default)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Disable retention and drop NFSv4 ACLs when changing mode bits	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

How ONTAP uses NFSv4 ACLs to determine whether it can delete a file

To determine whether it can delete a file, ONTAP uses a combination of the file's DELETE bit, and the containing directory's DELETE_CHILD bit. For more information, see the NFS 4.1 RFC 5661.

Enable or disable NFSv4 ACLs

To enable or disable NFSv4 ACLs, you can modify the `-v4.0-acl` and `-v4.1-acl` options. These options are disabled by default.

About this task

The `-v4.0-acl` or `-v4.1-acl` option controls the setting and viewing of NFSv4 ACLs; it does not control enforcement of these ACLs for access checking.

Step

1. Perform one of the following actions:

If you want to…	Then…

Enable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Disable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Enable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Disable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modify the maximum ACE limit for NFSv4 ACLs

You can modify the maximum number of allowed ACEs for each NFSv4 ACL by modifying the parameter `-v4-acl-max-aces`. By default, the limit is set to 400 ACEs for each ACL. Increasing this limit can help ensure successful migration of data with ACLs containing over 400 ACEs to storage systems running ONTAP.

About this task

Increasing this limit might impact performance for clients accessing files with NFSv4 ACLs.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Modify the maximum ACE limit for NFSv4 ACLs:

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

   The valid range of

   `max_ace_limit` is `192` to `1024`.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.