



管理 NFSv4 ACL ONTAP 9

NetApp
September 12, 2024

目录

- 管理 NFSv4 ACL 1
 - 启用 NFSv4 ACL 的优势 1
 - NFSv4 ACL 的工作原理 1
 - 启用或禁用修改 NFSv4 ACL 1
 - ONTAP 如何使用 NFSv4 ACL 来确定是否可以删除文件 2
 - 启用或禁用 NFSv4 ACL 2
 - 修改 NFSv4 ACL 的最大 ACE 限制 3

管理 NFSv4 ACL

启用 NFSv4 ACL 的优势

启用 NFSv4 ACL 具有许多优势。

启用 NFSv4 ACL 的优势包括：

- 更精细地控制用户对文件和目录的访问
- 提高 NFS 安全性
- 改进了与 CIFS 的互操作性
- 取消了每个用户 16 个组的 NFS 限制

NFSv4 ACL 的工作原理

使用 NFSv4 ACL 的客户端可以对系统上的文件和目录设置和查看 ACL。在具有 ACL 的目录中创建新文件或子目录时，新文件或子目录会继承 ACL 中已标记有相应继承标志的所有 ACL 条目（ACE）。

在根据 NFSv4 请求创建文件或目录时，生成的文件或目录上的 ACL 取决于文件创建请求是包含 ACL 还是仅包含标准 UNIX 文件访问权限，以及父目录是否具有 ACL：

- 如果请求包含 ACL，则会使用该 ACL。
- 如果此请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL，则只要父目录的 ACL 中的 ACE 已使用适当的继承标志进行标记，新文件或目录就会继承这些 ACE。



即使如此，也会继承父 ACL -v4.0-acl 设置为 off。

- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL，则会使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录具有不可继承的 ACL，则只会使用模式位创建新对象。



如果 -chown-mode 参数已设置为 restricted 中的命令 vserver nfs 或 vserver export-policy rule 系列、文件所有权只能由超级用户更改、即使使用 NFSv4 ACL 设置的磁盘权限允许非 root 用户更改文件所有权也是如此。有关详细信息，请参见相关手册页。

启用或禁用修改 NFSv4 ACL

当 ONTAP 接收到 chmod 命令时、默认情况下、系统会保留并修改 ACL、以反映模式位更改。您可以禁用 -v4-acl-preserve 参数以更改要丢弃 ACL 时的行为。

关于此任务

使用统一安全模式时，此参数还指定客户端为文件或目录发送 chmod，chgroup 或 chown 命令时是保留还是

删除 NTFS 文件权限。

此参数的默认值为 enabled 。

步骤

- 1. 将权限级别设置为高级：

```
set -privilege advanced
```

- 2. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用保留和修改现有 NFSv4 ACL （默认）	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
更改模式位时禁用保留并丢弃 NFSv4 ACL	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

- 3. 返回到管理权限级别：

```
set -privilege admin
```

ONTAP 如何使用 NFSv4 ACL 来确定是否可以删除文件

为了确定是否可以删除某个文件，ONTAP 将结合使用该文件的删除位和所在目录的 delete_child 位。有关详细信息，请参见 NFS 4.1 RFC 5661 。

启用或禁用 NFSv4 ACL

要启用或禁用NFSv4 ACL、您可以修改 -v4.0-acl 和 -v4.1-acl 选项默认情况下，这些选项处于禁用状态。

关于此任务

。 -v4.0-acl 或 -v4.1-acl 选项用于控制NFSv4 ACL的设置和查看、而不用于控制在访问检查中强制实施这些ACL。

步骤

- 1. 执行以下操作之一：

如果您要 ...	那么 ...
启用 NFSv4.0 ACL	输入以下命令： <code>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</code>

禁用 NFSv4.0 ACL	输入以下命令： <pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre>
启用NFSv4.1 ACL	输入以下命令： <pre>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</pre>
禁用NFSv4.1 ACL	输入以下命令： <pre>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</pre>

修改 NFSv4 ACL 的最大 ACE 限制

您可以通过修改参数来修改每个NFSv4 ACL允许的最大ACL数 `-v4-acl-max-aces`。默认情况下，每个 ACL 的限制设置为 400 个 ACE。增加此限制有助于确保使用包含 400 个以上 ACE 的 ACL 将数据成功迁移到运行 ONTAP 的存储系统。

关于此任务

增加此限制可能会影响使用 NFSv4 ACL 访问文件的客户端的性能。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 修改 NFSv4 ACL 的最大 ACE 限制：

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

的有效范围

`max_ace_limit` 为 192 to 1024.

3. 返回到管理权限级别：

```
set -privilege admin
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。