管理 NFSv4 ACL

ONTAP 9

NetApp
September 12, 2024

目录

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）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
更改模式位时禁用保留并丢弃 NFSv4 ACL	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

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： `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`

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

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
   ```