NFSv4 ACLの管理

ONTAP 9

NetApp
January 23, 2026

目次

NFSv4 ACLの管理

ONTAP SVMでNFSv4 ACLを有効にすることの利点について学習します。

NFSv4 ACLを有効化するメリットは色々あります。

NFSv4 ACL を有効にすると次のような利点があります：

- ファイルとディレクトリに対するユーザーアクセスのより細かい制御
- NFSセキュリティの向上
- CIFSとの相互運用性の向上
- ユーザーあたり16グループというNFS制限の削除

ONTAP SVM の NFSv4 ACL について学ぶ

NFSv4 ACLを使用しているクライアントは、システム上のファイルとディレクトリにACLを設定し、そのACLを表示することができます。ACLが設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、そのACL内のアクセス制御エントリ（ACE）のうち、該当する継承フラグがタグ付けされたACEがすべて継承されます。

ファイルやディレクトリがNFSv4要求によって作成される場合、作成されるファイルやディレクトリのACLは、ファイル作成要求にACLが含まれているか、標準のUNIXファイル アクセス権限のみが含まれているかによって、また、親ディレクトリにACLがあるかによって異なります。

- 要求にACLが含まれる場合は、そのACLが使用されます。
- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがある場合、親ディレクトリのACLのACEに該当する継承フラグが設定されていれば、それらのACEが新しいファイルやディレクトリに継承されます。

> ℹ `-v4.0-acl`が `off`に設定されている場合でも、親 ACL は継承されます。

- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがない場合は、クライアントのファイル モードを使用して標準のUNIXファイル アクセス権限が設定されます。
- 要求に標準のUNIXファイルアクセス権限のみが含まれ、親ディレクトリに継承不可能なACLがある場合、モード ビットを使用しないと新しいオブジェクトは作成できません。

`-chown-mode`パラメータが `restricted`に `vserver nfs`または `vserver export-policy rule`
ファミリのコマンドで設定されている場合、NFSv4
ACLで設定されたディスク上の権限で非ルートユーザーがファイル所有権を変更できる場合でも、ファイルの所有権を変更できるのはスーパーユーザーのみです。この手順で説明されているコマンドの詳細については、link:https://docs.netapp.com/us-en/ontap-cli/["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP SVMのNFSv4 ACL変更を有効または無効にする

ONTAPがACLを持つファイルまたはディレクトリに対する `chmod`コマンドを受信すると、デフォルトではACLが保持され、モードビットの変更を反映するように変更されます。代わりにACLを削除したい場合は、 `-v4-acl-preserve`パラメータを無効にして動作を変更できます。

タスク概要

unifiedセキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対するchmod、chgroup、またはchownコマンドを送信した際にNTFSファイル アクセス権が保持されるか破棄されるかの指定も行います。

このパラメータのデフォルト設定は有効になっています。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
既存のNFSv4 ACLの保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl-preserve enabled`
保持を無効にして、モード ビットの変更時にNFSv4 ACLを破棄する	`vserver nfs modify -vserver vserver_name -v4-acl-preserve disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAPがNFSv4 ACLを使用してファイルを削除できるかどうかを判断する方法を学びます

ファイルを削除できるかどうかを判断するために、ONTAPはファイルのDELETEビットと、そのファイルを含むディレクトリのDELETE_CHILDビットの組み合わせを使用します。詳細については、NFS 4.1 RFC 5661を参照してください。

ONTAP SVMのNFSv4 ACLを有効または無効にする

NFSv4 ACLを有効または無効にするには、 `-v4.0-acl`および `-v4.1-acl`オプションを変更します。これらのオプションはデフォルトでは無効になっています。

タスク概要

> `-v4.0-acl`または `-v4.1-acl`オプションは、NFSv4 ACLの設定と表示を制御します。アクセス チェックに対するこれらのACLの適用は制御しません。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4.0 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
NFSv4.1 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

ONTAP SVMのNFSv4 ACLの最大ACE制限を変更する

パラメータ `-v4-acl-max-aces`を変更することで、NFSv4 ACLごとに許可されるACEの最大数を変更できます。デフォルトでは、ACLごとに400個のACEに制限されています。この制限を増やすことで、400個を超えるACEを含むACLを持つデータをONTAPで実行されているストレージシステムに正常に移行できるようになります。

タスク概要

この制限を増やすと、NFSv4 ACLを使用してファイルにアクセスするクライアントのパフォーマンスに影響する可能性があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. NFSv4 ACLの最大ACE数を変更します。

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

   有効な

   `max_ace_limit`は `192`1024.`です

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

著作権に関する情報

商標に関する情報