



NFSv4 ACLの管理

ONTAP 9

NetApp
January 23, 2026

目次

NFSv4 ACLの管理	1
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。	1
ONTAP SVM の NFSv4 ACL について学ぶ	1
ONTAP SVMのNFSv4 ACL変更を有効または無効にする	2
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	3
ONTAP SVMのNFSv4 ACLを有効または無効にする	3
ONTAP SVMのNFSv4 ACLの最大ACE制限を変更する	4

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。



`-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）	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</code>
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	<code>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</code>

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

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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。