



NFSv4 ACLを管理します。

ONTAP 9

NetApp
December 20, 2024

目次

NFSv4 ACLを管理します。	1
NFSv4 ACLを有効にする利点	1
NFSv4 ACLの仕組み	1
NFSv4 ACLの変更を有効または無効にする	2
ONTAPでのNFSv4 ACLを使用したファイル削除の可否の判別方法	2
NFSv4 ACLを有効または無効にする	2
NFSv4 ACLのACEの最大数を変更する	3

NFSv4 ACLを管理します。

NFSv4 ACLを有効にする利点

NFSv4 ACLを有効にすると、多くのメリットがあります。

NFSv4 ACLを有効にする利点は次のとおりです。

- ファイルやディレクトリへのユーザアクセスのより詳細な制御
- NFSセキュリティの強化
- CIFSとの相互運用性の向上
- NFS のユーザあたりの最大グループ数は 16 ではなくになりました

NFSv4 ACLの仕組み

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が設定されたディレクトリに新しいファイルまたはサブディレクトリを作成すると、新しいファイルまたはサブディレクトリには、該当する継承フラグが設定されたACL内のすべてのAccess Control Entry（ACE；アクセス制御エントリ）が継承されます。

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、または標準の UNIX ファイルアクセス権限のみが含まれているか、および親ディレクトリに ACL が設定されているかどうかによって異なります。

- 要求にACLが含まれている場合は、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に適切な継承フラグが設定されていれば、それらのACEが新しいファイルまたはディレクトリに継承されます。



親ACLは、がに設定されている `off` 場合でも継承され `v4.0-acl` 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 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できない ACL がある場合は、モードビットのみを使用して新しいオブジェクトが作成されます。



または `vserver export-policy rule` ファミリーのコマンドで `vserver nfs` パラメータをに設定した `restricted` 場合 `chown-mode` は、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザにファイル所有権の変更が許可されていても、スーパーユーザのみがファイル所有権を変更できます。詳細については、関連するマニュアルページを参照してください。

NFSv4 ACLの変更を有効または無効にする

ONTAPがACLを含むファイルまたはディレクトリに対するコマンドを受信した場合、`chmod` デフォルトではACLは保持され、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をドロップする場合は、パラメータをディセーブルにして動作を変更できます `-v4-acl-preserve`。

タスクの内容

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ときに、NTFSファイル権限を保持するか破棄するかを指定します。

このパラメータのデフォルトはenabledです。

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でのNFSv4 ACLを使用したファイル削除の可否の判別方法

ファイルを削除できるかどうかを判別するために、ONTAPは、そのファイルのDELETEビットと、ファイルが含まれるディレクトリの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。

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、オプションと`-v4.1-acl`オプションを変更し`-v4.0-acl`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。

タスクの内容

`-v4.0-acl`オプションまたは`-v4.1-acl`オプションは、NFSv4 ACLの設定と表示を制御しますが、アクセスチェックでのNFSv4 ACLの適用は制御しません。

ステップ

1. 次のいずれかを実行します。

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

NFSv4 ACLのACEの最大数を変更する

パラメータを変更すると、各NFSv4 ACLに許可されるACEの最大数を変更できます `-v4 -acl-max-aces`。デフォルトでは、ACLあたりのACEの数は400個に制限されています。この制限値を増やすと、400個を超えるACEを含むACLのデータをONTAPを実行するストレージシステムに移行する際に役立ちます。

タスクの内容

この制限値を増やすと、NFSv4 ACLを含む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が低下することがあります。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. NFSv4 ACLのACEの最大数を変更します。

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

有効な範囲

```
max_ace_limit`で `192`ある `1024.
```

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 © 2024 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随時、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 5252.227-19（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权を有し、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权については、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。