



# **SMB** を使用したファイルアクセスの管理

## ONTAP 9

NetApp  
September 12, 2024

# 目次

SMB を使用したファイルアクセスの管理	1
ローカルユーザおよびローカルグループを使用して認証と許可を行います	1
トラバースチェックのバイパスを設定する	28
ファイルセキュリティと監査ポリシーに関する情報を表示します	31
CLI を使用して、SVM の NTFS ファイルセキュリティ、NTFS 監査ポリシー、ストレージレベルのアクセス保護を管理します	51
SMB 共有のメタデータキャッシュを設定します	77
ファイルロックを管理します	78
SMB のアクティビティを監視する	83

# SMB を使用したファイルアクセスの管理

## ローカルユーザおよびローカルグループを使用して認証と許可を行います

### ONTAP でのローカルユーザとローカルグループの使用方法

#### ローカルユーザとローカルグループの概念

ローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループの定義を理解し、基本的ないくつかの情報を理解しておく必要があります。

#### • \* ローカルユーザー \*

一意の Security Identifier (SID ; セキュリティ識別子) を持つユーザアカウント。そのユーザアカウントを作成した Storage Virtual Machine (SVM) 上でのみ認識されます。ローカルユーザアカウントには、ユーザ名や SID などの一連の属性があります。ローカルユーザアカウントは、NTLM 認証を使用して CIFS サーバ上でローカルに認証します。

ユーザアカウントには次のような用途があります。

- ユーザに `_ ユーザ権限の管理 _` 権限を付与するために使用します。
- SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

#### • \* ローカルグループ \*

一意の SID を持つグループ。そのグループを作成した SVM 上でのみ認識が可能です。グループには一連のメンバーが含まれます。メンバーは、ローカルユーザ、ドメインユーザ、ドメイングループ、およびドメインマシンアカウントです。グループは、作成、変更、または削除できます。

グループにはいくつかの用途があります。

- メンバーに `_User Rights Management_Privileges` を付与するために使用します。
- SVM が所有するファイルリソースおよびフォルダリソースに対する共有レベルとファイルレベルのアクセスを制御する。

#### • \* ローカルドメイン \*

ローカルスコープを持つドメイン。SVM によりバインドされています。ローカルドメインの名前は CIFS サーバの名前です。ローカルユーザとローカルグループはローカルドメインに含まれています。

#### • \* Security Identifier (SID ; セキュリティ識別子) \*

SID は、Windows 形式のセキュリティプリンシパルを識別する可変長の数値です。たとえば、通常の SID の場合は、次のような形式になります。S-1-5-21-3139654847-1303905135-2517279418-123456。

#### • \* NTLM 認証 \*

CIFS サーバ上のユーザの認証で使用される、Microsoft Windows のセキュリティ方式。

- \* 複製されたクラスタデータベース（RDB） \*

クラスタ内の各ノードのインスタンスを持つ複製されたデータベース。ローカルユーザとローカルグループのオブジェクトは、RDB に格納されます。

ローカルユーザおよびローカルグループを作成する理由

Storage Virtual Machine（SVM）でローカルユーザやローカルグループを作成する理由はいくつかあります。たとえば、ドメインコントローラ（DC）を使用できないときでも、ローカルユーザアカウントを使用して SMB サーバにアクセスできます。ローカルグループを使用して権限を割り当てる場合や、SMB サーバがワークグループにある場合もあります。

ローカルユーザアカウントを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメインユーザを使用できない。

ワークグループ設定にはローカルユーザが必要です。

- ドメインコントローラを使用できないときに、SMB サーバで認証してログインできるようにする。

ドメインコントローラがダウンしている場合や、ネットワークの問題によって SMB サーバからドメインコントローラに接続できない場合でも、ローカルユーザであれば、NTLM 認証を使用して SMB サーバに認証できます。

- ローカル・ユーザに `_ ユーザ権限の管理 _` 権限を割り当てる

*User Rights Management* は、ユーザとグループに付与する SVM の権限を SMB サーバ管理者が制御できる機能です。ユーザに権限を割り当てるには、ユーザのアカウントにそれらの権限を割り当てるか、ユーザをそれらの権限が割り当てられたローカルグループのメンバーにします。

ローカルグループを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメイングループを使用できない。

ワークグループにローカルグループを設定する必要はありませんが、設定するとローカルワークグループユーザのアクセス権限を管理するのに役立ちます。

- 共有やファイルアクセスの制御にローカルグループを使用して、ファイルやフォルダのリソースへのアクセスを制御する。
- カスタマイズした `_ ユーザ権限の管理 _` 権限を持つローカルグループを作成する。

権限があらかじめ定義された組み込みのユーザグループがいくつか用意されています。カスタマイズした一連の権限を割り当てるには、ローカルグループを作成し、そのグループに必要な権限を割り当てます。その後、ローカルグループにローカルユーザ、ドメインユーザ、およびドメイングループを追加します。

関連情報

[ローカルユーザ認証の仕組み](#)

## サポートされる権限のリスト

### ローカルユーザ認証の仕組み

CIFS サーバのデータにアクセスする前に、ローカルユーザは認証されたセッションを作成する必要があります。

SMB はセッションベースであるため、ユーザの ID は、最初にセッションがセットアップされたときに一度だけ確認できます。CIFS サーバでは、ローカルユーザの認証時に NTLM ベースの認証が使用されます。NTLMv1 と NTLMv2 の両方がサポートされています。

ONTAP では、3 つの事例でローカル認証が使用されます。各事例は、ユーザ名のドメイン部分（DOMAIN\user 形式）が CIFS サーバのローカルドメイン名（CIFS サーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致します

データへのアクセスを要求するときにローカルユーザクレデンシャルを指定したユーザが、CIFS サーバでローカルに認証されます。

- ドメイン部分が一致しません

ONTAP は、CIFS サーバが属しているドメインのドメインコントローラで NTLM 認証を試行します。認証に成功した場合は、ログインが完了します。成功しなかった場合は、認証が失敗した理由によって次の動作が異なります。

たとえば、ユーザは Active Directory 内に存在するが、パスワードが無効であるか期限切れになっている場合は、ONTAP は CIFS サーバ上の対応するローカルユーザアカウントの使用を試みません。代わりに、認証は失敗します。その他にも、ONTAP が CIFS サーバ上の対応するローカルアカウントを使用している場合、そのアカウントが存在するときは、NetBIOS ドメイン名が一致していなくても認証に使用する場合があります。たとえば、一致するドメインアカウントが存在するが無効になっている場合、ONTAP は、CIFS サーバ上の対応するローカルアカウントを認証に使用します。

- ドメイン部分は指定されません

ONTAP はまず、ローカルユーザとしての認証を試行します。ローカルユーザとしての認証に失敗した場合は、ONTAP が、CIFS サーバが属しているドメインのドメインコントローラでユーザを認証します。

ローカルユーザまたはドメインユーザの認証が完了したら、ONTAP でローカルグループメンバーシップおよび権限が考慮される完全なユーザアクセストークンが構成されます。

ローカルユーザの NTLM 認証の詳細については、Microsoft Windows のマニュアルを参照してください。

### 関連情報

#### ローカルユーザ認証の有効化と無効化

### ユーザアクセストークンの構成方法

ユーザが共有をマッピングすると、認証された SMB セッションが確立され、ユーザアクセストークンが構成されます。このトークンには、ユーザ、ユーザのグループメンバーシップ、累積権限、マッピングされた UNIX ユーザのそれぞれについて、情報が格納

されています。

この機能が無効になっていないかぎり、ローカルユーザとローカルグループの両方の情報がユーザアクセストークンに追加されます。アクセストークンの構成方法は、ローカルユーザのログインと Active Directory ドメインユーザのログインでは、方法が異なります。

- ローカルユーザログイン

ローカルユーザは複数のローカルグループのメンバーになることができますが、ローカルグループを他のローカルグループのメンバーにすることはできません。ローカルユーザアクセストークンは、その特定のローカルユーザが属するグループに割り当てられたすべての権限の組み合わせから構成されます。

- ドメイン・ユーザ・ログイン

ドメインユーザのログインでは、ONTAP は、ユーザの SID と、そのユーザが属するすべてのドメイングループの SID が格納されたユーザアクセストークンを取得します。ONTAP は、ユーザドメイングループのローカルメンバーシップ（存在する場合）が提供するアクセストークンとドメインユーザアクセストークンとの組み合わせを使用します。また、ドメインユーザに割り当てられた直接権限や、ドメイングループメンバーシップの直接権限も使用します。

ローカルユーザとドメインユーザの両方のログインで、プライマリグループ RID もユーザアクセストークン用に設定されています。デフォルトのRIDはです Domain Users（RID 513）。デフォルトは変更できません。

Windows から UNIX へのネームマッピングと、UNIX から Windows へのネームマッピングのプロセスでは、ローカルアカウントとドメインアカウントのどちらについても同じルールが適用されます。



UNIX ユーザがローカルアカウントに自動的にマッピングされることはありません。このマッピングが必要な場合は、既存のネームマッピングコマンドを使用して明示的なマッピングルールを指定する必要があります。

ローカルグループを含む **SVM** での **SnapMirror** の使用に関するガイドラインを次に示します

ローカルグループを含む SVM によって所有されているボリュームで SnapMirror を設定する際は、一定のガイドラインに注意する必要があります。

SnapMirror によって別の SVM にレプリケートされるファイル、ディレクトリ、または共有に適用する ACE ではローカルグループを使用できません。SnapMirror 機能を使用して別の SVM 上のボリュームに対する DR ミラーを作成する場合に、そのボリュームにローカルグループの ACE があるときは、ミラーには ACE は適用されません。データが別の SVM にレプリケートされる場合、実質的に、そのデータは別のローカルドメインに格納されることになります。ローカルユーザとローカルグループに付与されるアクセス権は、そのオブジェクトが最初に作成された SVM のスコープ内でのみ有効です。

#### **CIFS** サーバを削除したときのローカルユーザとローカルグループに対する影響

CIFS サーバを作成すると、デフォルトの一連のローカルユーザとローカルグループが作成され、CIFS サーバをホストする Storage Virtual Machine（SVM）に関連付けられます。SVM 管理者は、ローカルユーザやローカルグループをいつでも作成することができます。CIFS サーバを削除するときは、それを実行した場合のローカルユーザとローカルグループに対する影響について理解しておく必要があります。

ローカルユーザとローカルグループは SVM に関連付けられます。そのため、セキュリティの観点から、CIFS サーバを削除してもそれらが削除されることはありません。CIFS サーバを削除してもローカルユーザとローカルグループは削除されませんが、表示されなくなります。SVM で CIFS サーバを再作成するまで、表示したり管理したりすることはできません。



CIFS サーバの管理ステータスは、ローカルユーザやローカルグループが表示されるかどうかには影響しません。

## Microsoft 管理コンソールでのローカルユーザとローカルグループの情報の表示

Microsoft 管理コンソールを使用して、ローカルユーザとローカルグループのそれぞれの情報を表示できます。ONTAP の今回のリリースでは、Microsoft 管理コンソールで、ローカルユーザとローカルグループに対する上記以外の管理タスクを実行することはできません。

### リポートに関するガイドライン

ローカルユーザとグループを使用してファイルアクセスまたはユーザ権限を管理している場合に、ローカルユーザとグループをサポートしない ONTAP リリースにクラスタをリポートするときは、一定の考慮事項に注意する必要があります。

- セキュリティ上の理由から、ONTAP をローカルユーザとグループの機能をサポートしないバージョンにリポートしても、設定されているローカルユーザ、グループ、および権限に関する情報は削除されません。
- ONTAP の以前のメジャーバージョンにリポートする際、ONTAP では認証とクレデンシャルの作成時にローカルユーザとローカルグループは使用されません。
- ローカルユーザとローカルグループは、ファイルおよびフォルダの ACL からは削除されません。
- ローカルユーザまたはローカルグループに付与された権限に基づいて許可されるアクセスに依存するファイルアクセス要求は拒否されます。

アクセスを許可するには、ローカルユーザとローカルグループオブジェクトではなく、ドメインオブジェクトに基づいてアクセスを許可するようにファイル権限を再設定する必要があります。

## ローカル権限とは

### サポートされる権限のリスト

ONTAP には、一連のサポートされる権限があらかじめ定義されています特定の事前定義されたローカルグループには、これらの権限の一部がデフォルトで追加されています。事前定義グループの権限は追加または削除できます。また、新しいローカルユーザまたはローカルグループを作成して、そのグループや、既存のドメインユーザおよびグループに権限を追加することもできます。

次の表に、Storage Virtual Machine (SVM) でサポートされる権限の一覧と、その権限が割り当てられている BUILTIN グループを示します。

権限の名前	デフォルトのセキュリティ設定	説明
SeTcbPrivilege	なし	オペレーティングシステムの一部として機能します
SeBackupPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ACL を無視してファイルとディレクトリをバックアップします
SeRestorePrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ファイルおよびディレクトリをリストアし、ACL を上書きすべての有効なユーザまたはグループの SID をファイル所有者として設定します
SeTakeOwnershipPrivilege	BUILTIN\Administrators	ファイルまたはその他のオブジェクトの所有権を取得します
SeSecurityPrivilege	BUILTIN\Administrators	監査の管理  これには、セキュリティログの表示、ダンプ、およびクリアが含まれます。
SeChangeNotifyPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators、 BUILTIN\Power Users、 BUILTIN\Users、Everyone	トラバースチェックのバイパス  この権限を持つユーザには、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース (x) 権限は必要ありません。

#### 関連情報

- [ローカル権限を割り当てます](#)
- [トラバースチェックのバイパスの設定](#)

#### 権限を割り当てます

ローカルユーザまたはドメインユーザに権限を直接割り当てることができます。また、ユーザに付与する権限と一致する権限が割り当てられているローカルグループにユーザを割り当てすることもできます。

- 作成したグループに一連の権限を割り当てることができます。

その後、ユーザに付与する権限が割り当てられているグループにユーザを追加します。

- また、ローカルユーザおよびドメインユーザを、デフォルトの権限がユーザに付与する権限と一致している事前定義グループに割り当てすることもできます。



## 関連情報

- ローカルまたはドメインのユーザまたはグループに対する権限の追加
- ローカルまたはドメインのユーザまたはグループの権限を削除しています
- ローカルまたはドメインのユーザまたはグループの権限をリセットしています
- トラバースチェックのバイパスの設定

**BUILTIN** グループとローカル管理者アカウントの使用に関するガイドラインを次に示します

BUILTIN グループとローカル管理者アカウントを使用する場合は、一定のガイドラインに注意する必要があります。たとえば、ローカル管理者アカウントは、名前の変更は可能ですが、削除はできません。

- Administrator アカウントは、名前の変更は可能ですが、削除はできません。
- Administrator アカウントは BUILTIN\Administrators グループから削除できません。
- BUILTIN グループは、名前の変更は可能ですが、削除はできません。

BUILTIN グループの名前を変更したあと、よく知られた名前を使用して別のローカルオブジェクトを作成できますが、そのオブジェクトには新しい RID が割り当てられます。

- ローカルゲストアカウントがありません。

## 関連情報

### 事前定義の BUILTIN グループとそのデフォルトの権限

## ローカルユーザパスワードの要件

デフォルトでは、ローカルユーザのパスワードは複雑さの要件を満たしている必要があります。パスワードの複雑さの要件は、Microsoft Windows\_Local セキュリティポリシー \_ で定義されている要件に似ています。

パスワードは次の基準を満たしている必要があります。

- 6 文字以上にする必要があります
- ユーザアカウント名を含めることはできません
- 次の 4 種類のうちの 3 種類以上の文字を含める必要があります。
  - 大文字のアルファベット (A~Z)
  - 小文字のアルファベット (a~z)
  - 数字 (0~9)
  - 特殊文字：

~@#\$% { キャレット } &\* \_ +=\| () []:"<>、.?!/

## 関連情報

ローカル SMB ユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFS サーバのセキュリティ設定に関する情報を表示する

ローカルユーザのアカウントパスワードを変更しています

## 事前定義の **BUILTIN** グループとそのデフォルトの権限

ローカルユーザまたはドメインユーザのメンバーシップを、ONTAP の事前定義された一連の BUILTIN グループに割り当てることができます。事前定義グループには、事前定義された権限が割り当てられ

次の表に、事前定義グループを示します。

事前定義の <b>BUILTIN</b> グループ	デフォルトの権限
<p>BUILTIN\Administrators544番</p> <p>最初に作成されたとき、ローカル Administrator RIDが500のアカウントは、自動的にこのグループのメンバーになります。Storage Virtual Machine (SVM) がドメインに参加している場合は、domain\Domain Admins グループがグループに追加されます。SVMがドメインから削除された場合は domain\Domain Admins グループがグループから削除されます。</p>	<ul style="list-style-type: none"><li>• SeBackupPrivilege</li><li>• SeRestorePrivilege</li><li>• SeSecurityPrivilege</li><li>• SeTakeOwnershipPrivilege</li><li>• SeChangeNotifyPrivilege</li></ul>
<p>BUILTIN\Power Users547番地</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーには、次のような特徴があります。</p> <ul style="list-style-type: none"><li>• ローカルユーザとローカルグループを作成および管理できます。</li><li>• 自分自身や他のオブジェクトをに追加することはできません BUILTIN\Administrators グループ：</li></ul>	SeChangeNotifyPrivilege
<p>BUILTIN\Backup Operators住所は551</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。</p>	<ul style="list-style-type: none"><li>• SeBackupPrivilege</li><li>• SeRestorePrivilege</li><li>• SeChangeNotifyPrivilege</li></ul>

事前定義の <b>BUILTIN</b> グループ	デフォルトの権限
<b>BUILTIN\Users</b> RID 545  最初に作成された時点では、このグループには（暗黙の以外に）メンバーはありません <b>Authenticated Users</b> 特殊グループ）。SVMがドメインに参加すると、が表示されます <b>domain\Domain Users</b> グループがこのグループに追加されます。SVMがドメインから削除された場合は <b>domain\Domain Users</b> グループがこのグループから削除されます。	SeChangeNotifyPrivilege
<b>Everyone</b> SID S-1-1-0  このグループには、ゲストを含むすべてのユーザが含まれます（ただし匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。	SeChangeNotifyPrivilege

#### 関連情報

[BUILTIN グループとローカル管理者アカウントの使用に関するガイドラインを次に示します](#)

[サポートされる権限のリスト](#)

[トラバースチェックのバイパスの設定](#)

## ローカルユーザとローカルグループ機能を有効または無効にします

ローカルユーザとローカルグループ機能の概要を有効または無効にします

NTFS セキュリティ形式データのアクセス制御にローカルユーザとローカルグループを使用する前に、ローカルユーザとローカルグループ機能を有効にする必要があります。また、SMB 認証にローカルユーザを使用する場合は、ローカルユーザ認証機能を有効にする必要があります。

ローカルユーザとローカルグループ機能とローカルユーザ認証はデフォルトで有効になっています。有効になっていない場合は、ローカルユーザとローカルグループを設定して使用する前に有効にする必要があります。ローカルユーザとローカルグループ機能はいつでも無効にすることができます。

ローカルユーザとローカルグループ機能の明示的な無効化に加えて、ONTAP では、クラスタ内のノードがローカルユーザとローカルグループ機能をサポートしていないリリースの ONTAP にリバートされた場合にその機能が無効になります。クラスタ内のすべてのノードでその機能をサポートするバージョンの ONTAP が実行されるまで、ローカルユーザとローカルグループ機能は有効になりません。

#### 関連情報

[ローカルユーザアカウントを変更します](#)

[ローカルグループを変更します](#)

## ローカルまたはドメインのユーザまたはグループに権限を追加します

ローカルユーザとローカルグループを有効または無効にします

Storage Virtual Machine（SVM）での SMB アクセスに使用するローカルユーザとローカルグループを有効または無効にすることができます。ローカルユーザとローカルグループ機能はデフォルトで有効になっています。

このタスクについて

SMB 共有および NTFS ファイル権限の設定時にローカルユーザとローカルグループを使用でき、必要に応じて、SMB 接続の作成時の認証のためにローカルユーザを使用できます。認証にローカルユーザを使用するには、ローカルユーザとローカルグループ認証オプションも有効にする必要があります。

手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. 次のいずれかを実行します。

ローカルユーザとローカルグループの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and-groups-enabled false</code>

3. admin 権限レベルに戻ります。set -privilege admin

例

次の例は、SVM vs1 でローカルユーザとローカルグループ機能を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

関連情報

[ローカルユーザ認証を有効または無効にします](#)

[ローカルユーザアカウントを有効または無効にします](#)

ローカルユーザ認証を有効または無効にします

Storage Virtual Machine（SVM）での SMB アクセスに関するローカルユーザ認証を有効または無効にすることができます。デフォルトでは、ローカルユーザ認証は許可されます。これは、SVM がドメインコントローラにアクセスできない場合、またはドメインレベルのアクセス制御を使用しない場合に役立ちます。

作業を開始する前に

CIFS サーバでローカルユーザとローカルグループ機能を有効にする必要があります。

このタスクについて

ローカルユーザ認証はいつでも有効または無効にできます。SMB 接続の作成時の認証のためにローカルユーザを使用する場合は、CIFS サーバのローカルユーザとローカルグループオプションも有効にする必要があります。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 次のいずれかを実行します。

ローカル認証の設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</code>

3. admin 権限レベルに戻ります。 `set -privilege admin`

例

次の例は、SVM vs1 でローカルユーザ認証を有効にします。

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

関連情報

[ローカルユーザ認証の仕組み](#)

## ローカルユーザアカウントを管理します

ローカルユーザアカウントを変更します

既存のユーザのフルネームや概要を変更したり、ユーザアカウントを有効または無効にしたりする場合は、ローカルユーザアカウントを変更します。また、ユーザ名が侵害を受けたり、管理上の目的で名前の変更が必要になった場合にも、ローカルユーザアカウントの名前を変更できます。

状況	入力するコマンド
ローカルユーザのフルネームの変更	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -full-name text</code> フルネームにスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザの概要を変更します	<code>vserver cifs users-and-groups local-user modify -vserver vserver_name -user -name user_name -description text</code> 概要にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルユーザアカウントを有効または無効にします	<code>`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is -account-disabled {true</code>
<code>false}`</code>	ローカルユーザアカウントの名前を変更します

## 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のローカルユーザ「CIFS\_SERVER\sue」の名前を「CIFS\_SERVER\sue\_new」に変更します。

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

ローカルユーザアカウントを有効または無効にします

ユーザが Storage Virtual Machine（SVM）に格納されたデータに SMB 接続経由でアクセスできるようにするには、ローカルユーザアカウントを有効にします。また、そのユーザが SVM のデータに SMB 経由でアクセスできないようにするには、ローカルユーザアカウントを無効にします。

このタスクについて

ユーザアカウントを変更してローカルユーザを有効にします。

#### ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
ユーザアカウントを有効にします	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false</pre>
ユーザアカウントを無効にします	<pre>vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true</pre>

ローカルユーザのアカウントパスワードを変更する

ローカルユーザのアカウントパスワードを変更できます。これは、ユーザのパスワードが侵害された場合やユーザがパスワードを忘れた場合に役立ちます。

#### ステップ

1. 適切な操作を実行してパスワードを変更します。 `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

#### 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 に関連付けられたローカルユーザ「CIFS\_SERVER\sue」のパスワードを設定します。

```
cluster1::> vserver cifs users-and-groups local-user set-password -user -name CIFS_SERVER\sue -vserver vs1
```

```
Enter the new password:
Confirm the new password:
```

#### 関連情報

[ローカル SMB ユーザに対するパスワードの複雑さの要件の有効化と無効化](#)

[CIFS サーバのセキュリティ設定に関する情報を表示する](#)

ローカルユーザに関する情報を表示します

すべてのローカルユーザのリストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認するには、そのユーザの詳細なアカウント情報、および複数のユーザのアカウント情報を表示します。この情報は、ユーザの設定を変更す

必要があるかどうかを判断する場合に加えて、認証やファイルアクセスに関する問題のトラブルシューティングを行う場合にも役立ちます。

このタスクについて

ユーザのパスワードに関する情報は表示されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
Storage Virtual Machine （SVM）のすべてのユーザに関する情報を表示する	<code>vserver cifs users-and-groups local-user show -vserver vserver_name</code>
特定のユーザの詳細なアカウント情報を表示する	<code>vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name</code>

コマンドの実行時に選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例は、SVM vs1 のすべてのローカルユーザに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue    Jones
```

ローカルユーザのグループメンバーシップに関する情報を表示します

ローカルユーザが属しているローカルグループに関する情報を表示できます。この情報を使用して、ユーザに付与する必要があるファイルやフォルダへのアクセスを確認できます。この情報は、ユーザに付与する必要があるファイルやフォルダへのアクセス権や、ファイルアクセスに関する問題のトラブルシューティングを行うタイミングを判断するのに役立ちます。

このタスクについて

コマンドをカスタマイズして、必要な情報のみを表示することができます。

ステップ

1. 次のいずれかを実行します。



状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -user-name user_name</code>
このローカルユーザが属しているローカルグループのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -membership group_name</code>
指定した Storage Virtual Machine（SVM）に関連付けられているローカルユーザのユーザメンバーシップに関する情報を表示する	<code>vserver cifs users-and-groups local-user show-membership -vserver vserver_name</code>
指定した SVM 上のすべてのローカルユーザに関する詳細情報を表示する	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver vserver_name</code>

#### 例

次の例は、SVM vs1 上のすべてのローカルユーザのメンバーシップ情報を表示します。ユーザ「CIFS\_SERVER\Administrator」は「BUILTIN\Administrators」グループのメンバーで、「CIFS\_SERVER\sue」は「CIFS\_SERVER\g1」グループのメンバーです。

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
```

Vserver	User Name	Membership
vs1	CIFS_SERVER\Administrator	BUILTIN\Administrators
	CIFS_SERVER\sue	CIFS_SERVER\g1

#### ローカルユーザアカウントを削除します

CIFS サーバに対するローカル SMB 認証や、SVM に格納されたデータへのアクセス権の定義に使用するローカルユーザアカウントが不要になった場合は、Storage Virtual Machine（SVM）から削除することができます。

#### このタスクについて

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

このユーザを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- ローカルユーザへのすべての参照がメンバーシップおよび権限のデータベースから削除されます。
- Administrator などの標準的な既知のユーザは削除できません。

手順

- 1. 削除するローカルユーザアカウントの名前を確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`
- 2. ローカルユーザを削除します。 `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
- 3. ユーザアカウントが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

例

次の例は、SVM vs1 に関連付けられたローカルユーザ「CIFS\_SERVER\sue」を削除します。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue    Jones

cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

ローカルグループを管理します

ローカルグループを変更します

既存のローカルグループの概要を変更するには、既存のローカルグループの名前を変更するか、グループの名前を変更します。

状況	使用するコマンド
ローカルグループの概要を変更します	<code>vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text</code> 概要 にスペースが含まれている場合は、二重引用符で囲む必要があります。

状況	使用するコマンド
ローカルグループの名前を変更します	<code>vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name</code>

#### 例

次の例では 'ローカル・グループの名前を 'CIFS\_server\engineering' から 'CIFS\_server\engineering\_new' に変更します

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

次の例では 'ローカル・グループの概要を変更します

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

ローカルグループに関する情報を表示します

クラスタまたは指定した Storage Virtual Machine（SVM）で設定されているすべてのローカルグループの一覧を表示できます。この情報は、SVM に格納されているデータに対するファイルアクセスに関する問題や、SVM のユーザ権限に関する問題のトラブルシューティングに役立ちます。

#### ステップ

1. 次のいずれかを実行します。

必要な情報	入力するコマンド
クラスタのすべてのローカルグループ	<code>vserver cifs users-and-groups local-group show</code>
SVM のすべてのローカルグループ	<code>vserver cifs users-and-groups local-group show -vserver vserver_name</code>

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

#### 例

次の例は、SVM vs1 のすべてのローカルグループに関する情報を表示します。

```
cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
```

Vsriver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative privileges
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

## ローカルグループメンバーシップを管理します

ローカルグループメンバーシップの管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

### このタスクについて

ローカルグループへのメンバーの追加に関するガイドラインを次に示します。

- 特殊なグループ `_Everyone` にユーザを追加することはできません。
- ローカルグループにユーザを追加する前に、あらかじめそのグループが存在している必要があります。
- ローカルグループにユーザを追加する前に、あらかじめそのユーザが存在している必要があります。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、Data ONTAP で名前を SID に解決できる必要があります。

ローカルグループからのメンバーの削除に関するガイドラインを次に示します。

- 特殊なグループ `_Everyone` からメンバーを削除することはできません。
- メンバーを削除するグループが存在している必要があります。
- ONTAP は、グループから削除するメンバーの名前を、対応する SID に対して解決できる必要があります。

### ステップ

1. グループのメンバーを追加または削除します。

状況	使用するコマンド
グループにメンバーを追加します	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...] </pre> カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。
グループからメンバーを削除します	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...] </pre> カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

次の例は、SVM vs1 上のローカルグループ「SMB\_server\sue」とドメイングループ「AD\_DOM\dom\_eng」をローカルグループ「SMB\_server\engineering」に追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

次の例は、SVM vs1 上のローカルグループ「SMB\_server\sue」と「SMB\_server\james」からローカルユーザ「SMB\_server\engineering」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## 関連情報

### [ローカルグループのメンバーに関する情報を表示する](#)

ローカルグループのメンバーに関する情報を表示します

クラスタまたは指定した Storage Virtual Machine（SVM）で設定されているローカルグループのすべてのメンバーの一覧を表示できます。この情報は、ファイルアクセスに関する問題やユーザ権限に関する問題のトラブルシューティングに役立ちます。

## ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
クラスタのすべてのローカルグループのメンバー	<code>vserver cifs users-and-groups local-group show-members</code>
SVM のすべてのローカルグループのメンバー	<code>vserver cifs users-and-groups local-group show-members -vserver <i>vserver_name</i></code>

## 例

次の例は、SVM vs1 のすべてのローカルグループのメンバーに関する情報を表示します。

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver      Group Name                Members
-----
vs1          BUILTIN\Administrators    CIFS_SERVER\Administrator
                                     AD_DOMAIN\Domain Admins
                                     AD_DOMAIN\dom_grpl
                                     AD_DOMAIN\Domain Users
                                     AD_DOMAIN\dom_usr1
                                     CIFS_SERVER\engineering
                                     CIFS_SERVER\james
```

## ローカルグループを削除します

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権を決定するのに必要なくなった場合や、SVM ユーザ権限をグループメンバーに割り当てての必要なくなった場合は、SVM からローカルグループを削除できます。

### このタスクについて

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

このグループを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- グループが存在しない場合は、エラーが返されます。
- `special_every_group` は削除できません。
- `BUILTIN\Administrators` `BUILTIN\Users` などの組み込みのグループは削除できません。

## 手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。

```
vserver cifs users-and-groups local-group show -vserver vserver_name
```

2. ローカルグループを削除します。 `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. グループが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

例

次の例は、SVM vs1 に関連付けられたローカルグループ「CIFS\_SERVER\sales」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
	privileges	
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	
vs1	CIFS_SERVER\sales	

```
cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
```

Vserver	Group Name	Description
vs1	BUILTIN\Administrators	Built-in Administrators group
vs1	BUILTIN\Backup Operators	Backup Operators group
vs1	BUILTIN\Power Users	Restricted administrative
	privileges	
vs1	BUILTIN\Users	All users
vs1	CIFS_SERVER\engineering	

ローカルデータベースのドメインユーザおよびグループ名を更新します

CIFS サーバのローカルグループにドメインユーザやドメイングループを追加することができます。これらのドメインオブジェクトは、クラスタのローカルデータベースに登録されます。ドメインオブジェクトの名前を変更した場合は、ローカルデータベースを手動で更新する必要があります。

このタスクについて

ドメイン名を更新する Storage Virtual Machine（SVM）の名前を指定する必要があります。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`

## 2. 適切な操作を実行します。

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループについて、正常に更新されたものと更新できなかったものを表示する	<code>vserver cifs users-and-groups update-names -vserver vserver_name</code>
ドメインユーザとドメイングループについて、正常に更新されたものを表示する	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only false</code>
更新できなかったドメインユーザとドメイングループのみを表示します	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display-failed-only true</code>
更新に関するすべてのステータス情報を非表示にします	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress-all-output true</code>

## 3. admin 権限レベルに戻ります。 `set -privilege admin`

### 例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 に関連付けられているドメインユーザおよびグループの名前を更新します。前回の更新には依存する一連の名前を更新する必要があります。



```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:          EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:          EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:          Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:          EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:          Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

ローカル権限を管理します

ローカルまたはドメインのユーザまたはグループに権限を追加します

ローカルまたはドメインのユーザやグループのユーザ権限を管理できます。追加した権限は、これらのオブジェクトに割り当てられていたデフォルトの権限よりも優先されます。これにより、ユーザまたはグループに付与する権限をカスタマイズして、セキュリティを強化できます。

作業を開始する前に

権限を追加する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

このタスクについて

オブジェクトに権限を追加すると、そのユーザまたはグループのデフォルトの権限は無効になります。権限を追加しても、以前に追加した権限は削除されません。

ローカルまたはドメインのユーザまたはグループに権限を追加する場合は、次の点に注意する必要があります。

- 権限は 1 つ以上追加できます。
- ドメインユーザまたはグループへの権限の追加時、ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上の権限を追加します。 `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 必要な権限がオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上の「CIFS\_SERVER\sueo」ユーザに「`eTcbPrivilege」権限と「`seeOwnershipPrivilege」権限を追加します。

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

ローカルまたはドメインのユーザまたはグループから権限を削除します

ローカルまたはドメインのユーザやグループのユーザ権限を管理するには、権限を削除します。これにより、ユーザとグループに付与される最大権限をカスタマイズして、セキュリティを強化できます。

作業を開始する前に

権限を削除する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

このタスクについて

ローカルまたはドメインのユーザやグループの権限を削除するときは、次の点に注意してください。

- 1 つ以上の権限を削除できます。
- ドメインのユーザまたはグループの権限を削除する場合、ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。

ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループから1つ以上の権限を削除します。 `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 必要な権限がオブジェクトから削除されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のユーザ「CIFS\_SERVER\sueo」から「`s eTcbPrivilege」および「`s eTakeOwnershipPrivilege」権限を削除します。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        -
```

ローカルまたはドメインのユーザとグループの権限をリセットします

ローカルまたはドメインのユーザやグループの権限をリセットできます。これは、ローカルまたはドメインのユーザやグループの権限に対して行った変更が不要になった場合や必要がなくなった場合に役立ちます。

このタスクについて

ローカルまたはドメインのユーザまたはグループの権限をリセットすると、そのオブジェクトの権限のエントリがすべて削除されます。

手順

1. ローカルまたはドメインのユーザまたはグループの権限をリセットします。 `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. オブジェクトの権限がリセットされたことを確認します。 `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 上のユーザ「CIFS\_SERVER\sue」の権限をリセットしています。デフォルトでは、標準ユーザのアカウントには権限は関連付けられません。

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

次の例では 'グループ ""BUILTIN\Administrators ""' の特権をリセットし '実質的に特権エントリを削除します

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

権限の上書きに関する情報を表示します

ドメインまたはローカルのユーザアカウントまたはグループに割り当てられているカスタムの権限に関する情報を表示できます。この情報は、必要なユーザ権限が適用されているかどうかを確認するのに役立ちます。

#### ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
Storage Virtual Machine （SVM）上のすべてのドメインおよびローカルのユーザとグループのカスタム権限	<code>vserver cifs users-and-groups privilege show -vserver vserver_name</code>
SVM 上の特定のドメインまたはローカルのユーザとグループのカスタム権限	<code>vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name</code>

このコマンドを実行するときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

#### 例

次のコマンドを実行すると、SVM vs1 のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべての権限が表示されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	BUILTIN\Administrators	SeTakeOwnershipPrivilege SeRestorePrivilege
vs1	CIFS_SERVER\sue	SeTcbPrivilege SeTakeOwnershipPrivilege

## トラバースチェックのバイパスを設定する

### トラバースチェックのバイパスの設定の概要

トラバースチェックのバイパスは、トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできるかどうかを判断するユーザ権限です。トラバースチェックのバイパスを許可または拒否した場合の動作と、Storage Virtual Machine（SVM）でのユーザに対するトラバースチェックのバイパスの設定方法を理解しておく必要があります。

#### トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとする、中間ディレクトリのトラバース権限が ONTAP でチェックされないで、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、ONTAP はファイルのパスにあるすべてのディレクトリでトラバース（実行）権限をチェックします。

中間ディレクトリのいずれかに「X」（トラバース権限）がない場合、ONTAP はファイルへのアクセスを拒否します。

#### トラバースチェックのバイパスを設定する

ONTAP CLI を使用するか、Active Directory グループポリシーにこのユーザ権限を設定すると、トラバースチェックのバイパスを設定できます。

。SeChangeNotifyPrivilege 権限は、ユーザにトラバースチェックのバイパスを許可するかどうかを制御します。

- この権限を SVM のローカル SMB ユーザまたはグループ、ドメインユーザまたはグループに追加すると、トラバースチェックのバイパスを許可できます。
- この権限を SVM のローカル SMB ユーザまたはグループ、ドメインユーザまたはグループから削除すると、トラバースチェックのバイパスを拒否できます。

SVM の次の BUILTIN グループには、デフォルトでトラバースチェックのバイパス権限が割り当てられています。

- BUILTIN\Administrators
- BUILTIN\Power Users

- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可したくない場合は、グループからこの権限を削除する必要があります。

CLI を使用して SVM のローカル SMB ユーザおよびグループのトラバースチェックのバイパスを設定する場合は、次の点に注意する必要があります。

- カスタムのローカルグループまたはドメイングループのメンバーにトラバースチェックのバイパスを許可する場合は、を追加する必要があります SeChangeNotifyPrivilege そのグループへの特権。
- ローカルユーザまたはドメインユーザにトラバースチェックのバイパスを個別に許可する場合に、そのユーザがその権限を持つグループのメンバーでないときは、を追加できます SeChangeNotifyPrivilege そのユーザアカウントに対する権限。
- ローカルまたはドメインのユーザまたはグループのトラバースチェックのバイパスを無効にするには、を削除します SeChangeNotifyPrivilege いつでも特権。



特定のローカルまたはドメインのユーザまたはグループに対してトラバースチェックのバイパスを無効にするには、も削除する必要があります SeChangeNotifyPrivilege 権限を取得します Everyone グループ：

## 関連情報

[ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する](#)

[ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止します](#)

[ボリュームでの SMB ファイル名の変換のための文字マッピングを設定します](#)

[SMB 共有のアクセス制御リストを作成](#)

[ストレージレベルのアクセス保護を使用してファイルアクセスを保護](#)

[サポートされる権限のリスト](#)

[ローカルまたはドメインのユーザまたはグループに権限を追加します](#)

[ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する](#)

トラバースするディレクトリに対する権限がユーザにない場合でも、ファイルへのパスに含まれるすべてのディレクトリをユーザがトラバースできるようにするには、を追加します SeChangeNotifyPrivilege Storage Virtual Machine (SVM) 上のローカルSMBユーザまたはグループに対する権限。デフォルトでは、ユーザはディレクトリのトラバースチェックをバイパスできます。

作業を開始する前に

- SVM上にSMBサーバが存在している必要があります。

- ローカルユーザとローカルグループのSMBサーバオプションが有効になっている必要があります。
- が格納されているローカルまたはドメインのユーザまたはグループ SeChangeNotifyPrivilege 追加する権限はすでに存在している必要があります。

#### このタスクについて

ドメインユーザまたはグループへの権限の追加時、ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

#### 手順

1. を追加して、トラバースチェックのバイパスを有効にします SeChangeNotifyPrivilege ローカルまたはドメインのユーザまたはグループに対する権限： `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

の値 `-user-or-group-name` パラメータは、ローカルユーザまたはローカルグループ、ドメインユーザまたはグループです。

2. 指定したユーザまたはグループでトラバースチェックのバイパスが有効になっていることを確認します。  
`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

#### 例

次のコマンドは、「example\eng」グループに属するユーザがを追加してディレクトリのトラバースチェックをバイパスできるようにします SeChangeNotifyPrivilege グループに対する権限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng             SeChangeNotifyPrivilege
```

#### 関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスを禁止する](#)

ユーザまたはグループに対してディレクトリのトラバースチェックのバイパスを禁止します

トラバースするディレクトリに対する権限がユーザにないために、ファイルのパスに含まれるすべてのディレクトリをユーザがトラバースできないようにするには、を削除します SeChangeNotifyPrivilege Storage Virtual Machine (SVM) 上のローカルSMBユーザまたはグループからの権限。

作業を開始する前に



権限を削除する対象となるローカルまたはドメインのユーザまたはグループがすでに存在している必要があります。

#### このタスクについて

ドメインのユーザまたはグループの権限を削除する場合、ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

#### 手順

1. トラバースチェックのバイパスを禁止します。vserver cifs users-and-groups privilege remove-privilege -vserver vserver\_name -user-or-group-name name -privileges SeChangeNotifyPrivilege

コマンドは、を削除します SeChangeNotifyPrivilege の値で指定したローカルまたはドメインのユーザまたはグループの権限 -user-or-group-name name パラメータ

2. 指定したユーザまたはグループに対してトラバースチェックのバイパスが無効になっていることを確認します。vserver cifs users-and-groups privilege show -vserver vserver\_name -user-or-group-name name

#### 例

次のコマンドを実行すると、「EXAMPLE\eng」グループに属するユーザに対して、ディレクトリのトラバースチェックのバイパスが禁止されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          EXAMPLE\eng              -
```

#### 関連情報

[ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスを許可する](#)

## ファイルセキュリティと監査ポリシーに関する情報を表示します

ファイルセキュリティと監査ポリシーの概要に関する情報を表示します

Storage Virtual Machine（SVM）上のボリュームに格納されたファイルとディレクトリのファイルセキュリティに関する情報を表示できます。FlexVol の監査ポリシーに関する情報を表示できます。設定されている場合、FlexVol ボリュームのストレージレベルのアクセス保護およびダイナミックアクセス制御セキュリティの設定に関する情報を表示できます。

ファイルセキュリティに関する情報を表示する

次のセキュリティ形式のボリュームと（FlexVol の）qtree に格納されたデータに適用されているファイルセキュリティに関する情報を表示できます。

- NTFS
- 「UNIX」
- 混在

監査ポリシーに関する情報を表示する

次の NAS プロトコルを介した FlexVol ボリューム上のアクセスイベントを監査する監査ポリシーに関する情報を表示できます。

- SMB（すべてのバージョン）
- NFSv4.x に対応している

**Storage-Level Access Guard（SLAG**；ストレージレベルのアクセス保護）セキュリティに関する情報を表示する

ストレージレベルのアクセス保護セキュリティは、次のセキュリティ形式の FlexVol および qtree オブジェクトに適用できます。

- NTFS
- 混在
- UNIX（ボリュームが含まれる SVM で CIFS サーバが設定されている場合）

ダイナミックアクセス制御（**DAC**）セキュリティに関する情報を表示する

ダイナミックアクセス制御セキュリティは、次のセキュリティ形式の FlexVol ボリューム内のオブジェクトに適用できます。

- NTFS
- Mixed（オブジェクトに NTFS 対応のセキュリティが設定されている場合）

関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[ストレージレベルのアクセス保護に関する情報の表示](#)

**NTFS セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示します**

セキュリティ形式と有効なセキュリティ形式、適用されている権限、DOS 属性に関する情報など、NTFS セキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、NTFS ファイルアクセス権と Windows のユーザおよびグループのみを使用してファイルアクセス権を決定するため、UNIX 関連の出力フィールドには表示専用の UNIX ファイルアクセス権情報が格納されます。
- ACL 出力は、NTFS セキュリティが適用されたファイルとフォルダについて表示されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイル ACL とストレージレベルのアクセス保護 ACL の両方が表示されることがあります。
- 指定したファイルまたはディレクトリパスにダイナミックアクセス制御が設定されている場合は、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。

**ステップ**

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vs1 -path /vol1</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vs1 -path /vol1 -expand-mask true</code>

**例**

次の例は、パスに関するセキュリティ情報を表示します /vol1 SVM vs1：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

        Vserver: vs1
        File Path: /vol4
    File Inode Number: 64
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-
```

OI|CI|IO

次の例は、マスクを展開してパスに関するセキュリティ情報を表示します /data/engineering SVM vs1 :

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true
```

```

        Vserver: vs1
        File Path: /data/engineering
    File Inode Number: 5544
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
```

```

    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

```

```

1... .. = Self Relative
.0.. .. = RM Control Valid
..0. .. = SACL Protected
...0 .. = DACL Protected
.... 0... .. = SACL Inherited
.... .0.. .. = DACL Inherited
.... ..0. .... = SACL Inherit Required
.... ...0 .... = DACL Inherit Required
.... .... ..0. .... = SACL Defaulted
.... .... ...0 .... = SACL Present
.... .... .... 0... = DACL Defaulted
.... .... .... .1.. = DACL Present
.... .... .... ..0. = Group Defaulted
.... .... .... ...0 = Owner Defaulted

```

```

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs

```

```

ALLOW-Everyone-0x1f01ff

```

	0... .. =
Generic Read	
	.0.. .. =
Generic Write	
	..0. .... =
Generic Execute	
	...0 .... =
Generic All	
	.... ..0 .... =
System Security	
	.... .... 1 .... =
Synchronize	
	.... .... 1... .. =
Write Owner	
	.... .... 1.. .... =
Write DAC	
	.... .... ..1. .... =
Read Control	
	.... .... ...1 .... =
Delete	

	.....1..... =
Write Attributes	
	.....1.... =
Read Attributes	
	.....1... =
Delete Child	
	.....1. .... =
Execute	
	.....1 .... =
Write EA	
	.....1... =
Read EA	
	.....1... =
Append	
	.....1. .... =
Write	
	.....1 =
Read	
	ALLOW-Everyone-0x10000000-OI CI IO
	0.... .... =
Generic Read	
	.0... .... =
Generic Write	
	..0. .... =
Generic Execute	
	...1 .... =
Generic All	
	.....0 .... =
System Security	
	.....0 .... =
Synchronize	
	.....0 .... =
Write Owner	
	.....0... .... =
Write DAC	
	.....0. .... =
Read Control	
	.....0 .... =
Delete	
	.....0 .... =
Write Attributes	
	.....0... .... =
Read Attributes	
	.....0... .... =
Delete Child	

Execute	.....0..... =
Write EA	.....0..... =
Read EA	.....0..... =
Append	.....0..... =
Write	.....0..... =
Read	.....0..... =

次の例は、パスにあるボリュームの、ストレージレベルのアクセス保護セキュリティ情報を含むセキュリティ情報を表示します /datavol1 SVM vs1：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
        Control:0x8004
        Owner: BUILTIN\Administrators
        Group: BUILTIN\Administrators
        DACL - ACEs
            ALLOW-Everyone-0x1f01ff
            ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

#### 関連情報

[mixed セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

[UNIX セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)



**mixed** セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIX の所有者とグループに関する情報など、mixed セキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはフォルダのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。
- mixed セキュリティ形式のボリュームの最上位には、UNIX 対応のセキュリティまたは NTFS 対応のセキュリティを設定できます。
- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、UNIX ファイル権限とストレージレベルのアクセス保護 ACL の両方が表示されることがあります。
- コマンドで入力したパスが、NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /projects マスクを展開した形式でSVM vs1に格納します。この mixed セキュリティ形式のパスには、UNIX 対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path  
/projects -expand-mask true
```

```
      Vserver: vs1  
      File Path: /projects  
      File Inode Number: 78  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: 0x10  
      ...0 .... = Offline  
      .... ..0. .... = Sparse  
      .... .... 0... .... = Normal  
      .... .... ..0. .... = Archive  
      .... .... ...1 .... = Directory  
      .... .... .... .0.. = System  
      .... .... .... ..0. = Hidden  
      .... .... .... ...0 = Read Only  
      Unix User Id: 0  
      Unix Group Id: 1  
      Unix Mode Bits: 700  
      Unix Mode Bits in Text: rwx-----  
      ACLs: -
```

次の例は、パスに関するセキュリティ情報を表示します /data (SVM vs1)。この mixed セキュリティ形式のパスには、NTFS 対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

次の例は、パスにあるボリュームに関するセキュリティ情報を表示します /datavol5 (SVM vs1)。この mixed セキュリティ形式のボリュームの最上位には、UNIX 対応のセキュリティが設定されています。ボリュームにはストレージレベルのアクセス保護セキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

#### 関連情報

[NTFSセキュリティ形式のボリュームのファイルセキュリティに関する情報の表示](#)

[UNIX セキュリティ形式のボリュームのファイルセキュリティに関する情報を表示する](#)

**UNIX** セキュリティ形式のボリューム上のファイルセキュリティに関する情報を表示します

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIX の所有者と

グループに関する情報など、UNIX セキュリティ形式のボリューム上にあるファイルやディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、ファイルアクセス権の決定時に、UNIX ファイルアクセス権のみが使用されます。モードビットまたは NFSv4 ACL です。
- ACL 出力は、NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NFSv4 セキュリティ記述子には該当しません。

これらのフィールドが意味があるのは、NTFS セキュリティ記述子の場合のみです。

- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、で指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります -path パラメータ

ステップ

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /home SVM vs1：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

Vserver: vs1
File Path: /home
File Inode Number: 9590
Security Style: unix
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 1
    Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
ACLs: -
```

次の例は、パスに関するセキュリティ情報を表示します /home マスクを展開した形式のSVM vs1 :

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

Vserver: vs1
File Path: /home
File Inode Number: 9590
Security Style: unix
Effective Style: unix
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 1
    Unix Mode Bits: 700
Unix Mode Bits in Text: rwx-----
ACLs: -
```

## CLI を使用して、FlexVol の NTFS 監査ポリシーに関する情報を表示する

セキュリティ形式と有効なセキュリティ形式、適用されているアクセス権、システムアクセス制御リストに関する情報など、FlexVol の NTFS 監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはフォルダのパスを指定する必要があります。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、NTFS のシステムアクセス制御リスト（SACL）のみが監査ポリシーに使用されます。
- NTFS 対応のセキュリティが有効な mixed セキュリティ形式のボリューム内のファイルおよびフォルダには、NTFS 監査ポリシーを適用できます。

mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、UNIX または NTFS 対応のセキュリティを有効にすることができ、そこには NTFS SACL が格納されている場合も、格納されていない場合もあります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、通常のファイルおよびフォルダの NFSv4 SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- コマンドで入力したパスが、NTFS 対応のセキュリティを使用するデータへのパスである場合、そのファイルまたはディレクトリパスにダイナミックアクセス制御が設定されていれば、ダイナミックアクセス制御 ACE に関する情報も出力に表示されます。
- NTFS 対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX 関連の出力フィールドには表示専用の UNIX ファイル権限情報が格納されます。

ファイルアクセス権の決定時、NTFS セキュリティ形式のファイルおよびフォルダでは、NTFS ファイルアクセス権と Windows ユーザおよびグループのみが使用されます。

- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されません。

ステップ

1. ファイルおよびディレクトリ監査ポリシー設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細なリストとして	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスの監査ポリシーの情報を表示します /corp (SVM vs1)。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

次の例は、パスの監査ポリシーの情報を表示します /datavol1 (SVM vs1)。このパスには、標準ファイルおよびフォルダの SACL とストレージレベルのアクセス保護の SACL の両方が格納されています。



```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

**CLI を使用して、FlexVol の NFSv4 監査ポリシーに関する情報を表示する**

セキュリティ形式と有効なセキュリティ形式、適用されている権限、システムアクセス制御リスト（SACL）に関する情報など、ONTAP CLI を使用して FlexVol の NFSv4 監

査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

Storage Virtual Machine（SVM）の名前、および監査情報を表示するファイルまたはディレクトリのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、監査ポリシーに NFSv4 SACL のみが使用されます。
- mixed セキュリティ形式のボリュームにある UNIX セキュリティ形式のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

mixed セキュリティ形式のボリュームおよび qtree には、UNIX ファイル権限、モードビットまたは NFSv4 ACL、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、UNIX または NTFS 対応のセキュリティを有効にすることができ、NFSv4 SACL が含まれる場合と含まれない場合があります。
- ACL 出力は、NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

このフィールドは、モードビットのアクセス権のみ（NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、NTFS セキュリティ記述子の場合にのみ適用されます。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたは qtree の有効なセキュリティ形式が UNIX であっても、mixed セキュリティ形式のボリュームまたは qtree で設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたは qtree パスの出力には、標準の NFSv4 ファイルおよびディレクトリの SACL とストレージレベルのアクセス保護の NTFS SACL の両方が表示される場合があります。
- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、で指定したボリュームまたはqtreeに適用されるストレージレベルのアクセス保護セキュリティに関する情報が出力に含まれることがあります -path パラメータ

手順

1. ファイルとディレクトリのセキュリティ設定を必要な詳細レベルで表示します。

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

例

次の例は、パスに関するセキュリティ情報を表示します /lab (SVM vs1)。この UNIX セキュリティ形式のパスには NFSv4 SACL が設定されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

      Vserver: vs1
      File Path: /lab
      File Inode Number: 288
      Security Style: unix
      Effective Style: unix
      DOS Attributes: 11
      DOS Attributes in Text: ----D--R
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 0
      Unix Mode Bits in Text: -----
      ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                  SUCCESSFUL-S-1-520-0-0xf01ff-SA
                  FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                  ALLOW-S-1-520-1-0xf01ff
```

## ファイルセキュリティと監査ポリシーに関する情報を表示する方法

ワイルドカード文字 (\*) を使用すると、特定のパスまたはルートボリュームの下にあるすべてのファイルおよびディレクトリのファイルセキュリティと監査ポリシーに関する情報を表示できます。

ワイルドカード文字 (\*) は、すべてのファイルおよびディレクトリの情報を表示する特定のディレクトリパスの最後のサブコンポーネントとして使用できます。「\*」という名前の特定のファイルまたはディレクトリの情報を表示する場合は、二重引用符 (「`」) で完全なパスを指定する必要があります。

### 例

次のコマンドにワイルドカード文字を指定すると、パスの下にあるすべてのファイルとディレクトリに関する情報が表示されます /1/ SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

次のコマンドは、パスの下に「\*」という名前のファイルの情報を表示します /vol1/a SVM vs1の。パスは二重引用符 ("" ) で囲まれます。

```
cluster::> vservers security file-directory show -vservers vs1 -path  
"/vol1/a/*"
```

```
      Vserver: vs1  
      File Path: "/vol1/a/*"  
      Security Style: mixed  
      Effective Style: unix  
      DOS Attributes: 10  
      DOS Attributes in Text: ----D---  
      Expanded Dos Attributes: -  
          Unix User Id: 1002  
          Unix Group Id: 65533  
          Unix Mode Bits: 755  
      Unix Mode Bits in Text: rwxr-xr-x  
      ACLs: NFSV4 Security Descriptor  
          Control:0x8014  
          SACL - ACEs  
              AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
          DACL - ACEs  
              ALLOW-EVERYONE@-0x1f00a9-FI|DI  
              ALLOW-OWNER@-0x1f01ff-FI|DI  
              ALLOW-GROUP@-0x1200a9-IG
```

## CLI を使用して、SVM の NTFS ファイルセキュリティ、NTFS 監査ポリシー、ストレージレベルのアクセス保護を管理します

CLI の概要を使用して、SVM の NTFS ファイルセキュリティ、NTFS 監査ポリシー、ストレージレベルのアクセス保護を管理します

CLI を使用して、Storage Virtual Machine（SVM）の NTFS ファイルセキュリティ、NTFS 監査ポリシー、ストレージレベルのアクセス保護を管理できます。

NTFS ファイルセキュリティと監査ポリシーは、SMB クライアントから、または CLI を使用して管理できます。ただし、CLI を使用してファイルセキュリティと監査ポリシーを設定する場合、リモートクライアントを使用せずにファイルセキュリティを管理できます。CLI を使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも 1 つのコマンドで実行できるため、所要時間を大幅に短縮できます。

ONTAP から SVM ボリュームに適用されるもう 1 つのセキュリティレイヤであるストレージレベルのアクセス保護を設定できます。ストレージレベルのアクセス保護環境は、すべての NAS プロトコルからストレージレベルのアクセス保護が適用されているストレージオブジェクトへのアクセスを保護します。

ストレージレベルのアクセス保護は ONTAP CLI からのみ設定および管理できます。ストレージレベルのアクセス保護設定を SMB クライアントから管理することはできません。また、NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。システム（Windows または UNIX）管理者であっても、ストレージレベルのア

アクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティレイヤをデータアクセスに追加で提供します。



ストレージレベルのアクセス保護では NTFS のアクセス権のみがサポートされます。ただし、ストレージレベルのアクセス保護が適用されているボリューム上のデータへの NFS 経由のアクセスに対しても、そのボリュームを所有する SVM 上の Windows ユーザに UNIX ユーザがマッピングされている場合は、ONTAP でセキュリティチェックを実行できます。

## NTFS セキュリティ形式のボリューム

NTFS セキュリティ形式のボリュームや qtree に格納されているファイルやフォルダはすべて、NTFS 対応のセキュリティが有効になります。を使用できます `vserver security file-directory` NTFSセキュリティ形式のボリュームに次の種類のセキュリティを実装するためのコマンドファミリー。

- ボリュームに格納されているファイルとフォルダに対するファイル権限と監査ポリシー
- ボリュームに対するストレージレベルのアクセス保護セキュリティ

## mixed セキュリティ形式のボリューム

mixed セキュリティ形式のボリュームおよび qtree には、UNIX 対応のセキュリティを備え、UNIX ファイルアクセス権を使用する一部のファイルおよびフォルダ、モードビットまたは NFSv4.x ACL と NFSv4.x 監査ポリシー、および NTFS 対応のセキュリティを有効にして NTFS ファイルアクセス権と監査ポリシーを使用する一部のファイルおよびフォルダを含めることができます。を使用できます `vserver security file-directory` mixedセキュリティ形式のデータに次の種類のセキュリティを適用するコマンドファミリー。

- mixed 形式のボリュームや qtree での NTFS 対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- ストレージレベルのアクセス保護：NTFS 対応または UNIX 対応のセキュリティ形式のボリューム

## UNIXセキュリティ形式のボリューム

UNIX セキュリティ形式のボリュームと qtree には、UNIX 対応のセキュリティ（モードビットまたは NFSv4.x ACL）を備えたファイルとフォルダが含まれます。を使用する場合は、次の点に注意する必要があります `vserver security file-directory` UNIXセキュリティ形式のボリュームにセキュリティを実装するコマンドファミリー：

- `vserver security file-directory` UNIXセキュリティ形式のボリュームおよびqtreeでは、コマンドファミリーを使用してUNIXファイルセキュリティおよび監査ポリシーを管理することはできません。
- を使用できます `vserver security file-directory` UNIXセキュリティ形式のボリュームを含むSVMにCIFSサーバが含まれている場合に、そのボリュームにストレージレベルのアクセス保護を設定するコマンドファミリー。

## 関連情報

[ファイルセキュリティと監査ポリシーに関する情報を表示します](#)

[CLIを使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

[CLIを使用して、NTFS ファイルおよびフォルダに対して監査ポリシーを設定および適用する](#)

## CLI を使用してファイルおよびフォルダのセキュリティを設定するユースケース

ファイルおよびフォルダのセキュリティは、リモートクライアントを使用せずにローカルで適用および管理できるため、多数のファイルまたはフォルダに対して一括でセキュリティを設定する場合に比べて大幅に時間を短縮できます。

CLI を使用してファイルおよびフォルダのセキュリティを設定すると効果的な状況として、次のようなユースケースがあります。

- ホームディレクトリ内のファイルストレージなど、大規模なエンタープライズ環境のファイルの格納
- データの移行
- Windows ドメインの変更
- NTFS ファイルシステムのファイルセキュリティと監査ポリシーの標準化

## CLI を使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項

ファイルおよびフォルダのセキュリティ設定で CLI を使用する際には、一定の制限事項を知っておく必要があります。

- `vserver security file-directory` コマンドファミリーは NFSv4 ACL の設定をサポートしていません。

NTFS のセキュリティ記述子は NTFS ファイルと NTFS フォルダにのみ適用できます。

## セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

セキュリティ記述子には、ユーザがファイルやフォルダに対して実行できる操作、およびユーザがファイルやフォルダにアクセスするときに監査される内容を決定するアクセス制御リストが含まれます。

### • \* 権限 \*

権限は、オブジェクトの所有者によって許可または拒否され、指定されたファイルまたはフォルダに対してオブジェクト（ユーザ、グループ、またはコンピュータオブジェクト）が実行できる操作を決定します。

### • \* セキュリティ記述子 \*

セキュリティ記述子は、ファイルまたはフォルダに関連付けられた権限を定義するセキュリティ情報を含むデータ構造です。

### • \* アクセス制御リスト (ACL) \*

アクセス制御リストは、セキュリティ記述子内に含まれるリストです。セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の 2 種類の ACL を含めることができます。

- Discretionary Access Control List （ DACL ； 随意アクセス制御リスト）

- システムアクセスセイギョリスト SACL

- \* 随意アクセス制御リスト （ DACL ） \*

DACL には、ファイルまたはフォルダに対して操作を実行するためのアクセスを許可または拒否するユーザ、グループ、およびコンピュータオブジェクトの SID リストが含まれます。DACL には、0 個以上の Access Control Entry （ ACE ； アクセス制御エントリ）が含まれます。

- \* システム・アクセス・コントロール・リスト （ SACL ） \*

SACL には、成功または失敗した監査イベントがログに記録されるユーザ、グループ、およびコンピュータオブジェクトの SID リストが含まれます。SACL には、0 個以上の Access Control Entry （ ACE ； アクセス制御エントリ）が含まれます。

- \* アクセス制御エントリ (ACE) \*

ACE は、DACL または SACL 内の個々のエントリです。

- DACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトに対して許可または拒否されるアクセス権を指定します。

- SACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

- \* 権限の継承 \*

権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトのアクセス権を設定する際に、フォルダ、サブフォルダ、およびファイルがそのアクセス権を継承できるかどうかを「適用先」で決定することができます this-folder、 sub-folders、および`files`」を指定します。

## 関連情報

["SMB および NFS の監査とセキュリティトレース"](#)

[CLI を使用した NTFS ファイルおよびフォルダに対する監査ポリシーの設定および適用](#)

**SVM** ディザスタリカバリデスティネーションでローカルユーザまたはグループを使用するファイルとディレクトリのポリシーを適用する際のガイドライン

ファイルとディレクトリのポリシー設定がセキュリティ記述子、DACL、SACL エントリのいずれかでローカルユーザまたはグループを使用する場合、ID 破棄設定の Storage Virtual Machine （ SVM ） ディザスタリカバリデスティネーションでファイルとディレクトリのポリシーを適用する前に注意すべきいくつかのガイドラインがあります。

ソースクラスタのソース SVM が、ソース SVM からデスティネーションクラスタのデスティネーション SVM にデータと設定をレプリケートする SVM ディザスタリカバリ構成を設定できます。

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます



この設定では、SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

この設定では、SVM と CIFS サーバの ID が維持されません。このシナリオでは、デスティネーション SVM の SVM と CIFS サーバの名前は、ソース SVM の SVM と CIFS サーバの名前と異なります。

## ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「vs1」で CIFS サーバ名が「CIFS1」、デスティネーション SVM 名が「vs1\_dst」で CIFS サーバ名が「CIFS1\_DST」の場合、ローカルユーザ「CIFS1\user1」のローカルドメイン名は「CIFS1\_DST デスティネーション SVM」で自動的に「CIFS1\_DST\user1」に変更されます。

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
	administrator account		
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
	administrator account		
vs1_dst	CIFS1_DST\user1	-	-

ローカルユーザおよびグループデータベースでローカルユーザおよびグループ名が自動的に変更されても、ファイルとディレクトリのポリシー設定（を使用してCLIで設定するポリシー）のローカルユーザまたはグループ名は自動的に変更されません（vserver security file-directory コマンドファミリー）。

たとえば、「vs1」の場合、が配置されているDACLエントリを設定しているとします -account パラメータが「CIFS1\user1」に設定されている場合、デスティネーションSVMでデスティネーションのCIFSサーバ名が反映されて設定が自動的に変更されることはありません。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver  
vs1_dst
```

Vserver: vs1\_dst

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
**CIFS1**\user1	allow	full-control	this-folder

を使用する必要があります `vserver security file-directory modify` CIFSサーバ名を手動でデスティネーションCIFSサーバ名に変更するコマンド

アカウントパラメータを含むファイルとディレクトリのポリシー設定コンポーネント

ローカルユーザまたはグループを含むパラメータ設定を使用できるファイルとディレクトリのポリシー設定コンポーネントは3つあります。

- セキュリティ記述子

必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリグループを指定できます。セキュリティ記述子で所有者とプライマリグループのエントリにローカルユーザまたはグループを使用する場合、デスティネーション SVM にアカウント名を使用するようにセキュリティ記述子を変更する必要があります。を使用できます `vserver security file-directory ntfs modify` コマンドを使用してアカウント名に必要な変更を行います。

- DACL エントリ

各 DACL エントリは、アカウントと関連付ける必要があります。ローカルユーザまたはグループアカウントを使用する DACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存の DACL エントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべての DACL エントリをセキュリティ記述子から削除し、訂正したデスティネーションアカウント名を設定した新しい DACL エントリを作成し、その新しい DACL エントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACL エントリ

各 SACL エントリは、アカウントに関連付ける必要があります。ローカルユーザまたはグループアカウント

トを使用する SACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存の SACL エントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべての SACL エントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しい SACL エントリを作成し、それらの新しい SACL エントリを適切なセキュリティ記述子と関連付ける必要があります。

ポリシーを適用する前に、ファイルとディレクトリのポリシー設定で使用されているローカルユーザまたはグループに必要な変更を行う必要があります。そうしないと、適用ジョブは失敗します。

## CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

### NTFS セキュリティ記述子を作成します

NTFS セキュリティ記述子（ファイルセキュリティポリシー）の作成は、Storage Virtual Machine（SVM）内のファイルやフォルダの NTFS Access Control List（ACL；アクセス制御リスト）を設定および適用するための最初のステップです。セキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けることができます。

#### このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List（DACL；随意アクセス制御リスト）の 4 つの Access Control Entry（ACE；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み管理者	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込みユーザ	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可（Allow）	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者
- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

## NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加

NTFS セキュリティ記述子への随意アクセス制御リスト（DACL）のアクセス制御エントリ（ACE）の追加は、ファイルまたはフォルダに対する NTFS ACL の設定および適用における 2 番目の手順です。各エントリによって、アクセスが許可または拒否されるオブジェクトが識別され、ACE で定義されているファイルまたはフォルダに対してオブジェクトが実行できる操作または実行できない操作が定義されます。

このタスクについて

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれるDACLに既存のACEがある場合は、新しいACEがDACLに追加されます。セキュリティ記述子に DACL が含まれていない場合は、DACL が作成され、その DACL に新しい ACE が追加されます。

必要に応じて、で指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズできます -account パラメータ権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権利
- 詳細な権限
- raw 権限（advanced 権限）



DACLエントリの権限を指定しない場合、権限はデフォルトでに設定されます Full Control。

必要に応じて、継承の適用方法を指定することで、DACL エントリをカスタマイズできます。

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

### 手順

1. セキュリティ記述子にDACLエントリを追加します。

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1 -access-type {allow|deny} -account name_or_SID optional_parameters
```

  

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```
2. DACLエントリが正しいことを確認します。

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type {allow|deny} -account name_or_SID
```

  

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
      Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
    Access Rights: full-control
```

## セキュリティポリシーを作成する

SVM のファイルセキュリティポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

### このタスクについて

セキュリティポリシーに追加するタスクには、NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFS セキュリティ形式または mixed セキュリティ形式のボリュームを含む SVM にそれぞれ関連付ける必要があります。

### 手順

1. セキュリティポリシーを作成します。vserver security file-directory policy create -vserver vserver\_name -policy-name policy\_name

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. セキュリティポリシーを確認します。vserver security file-directory policy show

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

## セキュリティポリシーにタスクを追加します

ACL を設定し、SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

### このタスクについて

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFS または mixed セキュリティが設定され

たファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10、000 個です。
- ポリシーには 1 つ以上のタスクを含めることができます。

ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

セキュリティポリシーにタスクを追加する際には、次の 4 つの必須パラメータを指定する必要があります。

- SVM 名
- ポリシー名
- パス
- パスに関連付けるセキュリティ記述子

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

## 手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` は、のデフォルト値です `-access-control` パラメータファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

Vserver: vs1

Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

## セキュリティポリシーを適用する

SVM へのファイルセキュリティポリシーの適用は、ファイルまたはフォルダに対して NTFS ACL を作成および適用する最後のステップです。

### このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、FlexVol ボリューム（NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。セキュリティポリシーとそれに関連付けられた DACL が適用されると、既存の DACL はすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

## ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver`

```
vserver_name -policy-name policy_name
```

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

セキュリティポリシージョブを監視します

Storage Virtual Machine（SVM）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

このタスクについて

セキュリティポリシージョブに関する詳細情報を表示するには、を使用します `-instance` パラメータ

ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

適用したファイルセキュリティを確認します

Storage Virtual Machine（SVM）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの設定が意図したとおりになっているかを確認するには、ファイルのセキュリティ設定を確認します。

このタスクについて

データが格納されている SVM の名前、およびセキュリティ設定を確認するファイルとフォルダのパスを指定する必要があります。オプションのを使用できます `-expand-mask` セキュリティ設定に関する詳細情報を表示するためのパラメータ。

ステップ

1. ファイルとフォルダのセキュリティ設定を表示します。 `vserver security file-directory show`



```
-vserver vserver_name -path path [-expand-mask true]
```

```
vserver security file-directory show -vserver vs1 -path /data/engineering  
-expand-mask true
```

```
Vserver: vs1  
    File Path: /data/engineering  
File Inode Number: 5544  
    Security Style: ntfs  
    Effective Style: ntfs  
    DOS Attributes: 10  
DOS Attributes in Text: ----D---  
Expanded Dos Attributes: 0x10  
    ...0 .... = Offline  
    .... ..0. .... = Sparse  
    .... .... 0... .... = Normal  
    .... .... ..0. .... = Archive  
    .... .... ...1 .... = Directory  
    .... .... .... .0.. = System  
    .... .... .... ..0. = Hidden  
    .... .... .... ...0 = Read Only  
    Unix User Id: 0  
    Unix Group Id: 0  
    Unix Mode Bits: 777  
Unix Mode Bits in Text: rwxrwxrwx  
    ACLs: NTFS Security Descriptor  
    Control:0x8004  
  
    1... .... = Self Relative  
    .0.. .... = RM Control Valid  
    ..0. .... = SACL Protected  
    ...0 .... = DACL Protected  
    .... 0... .... = SACL Inherited  
    .... .0.. .... = DACL Inherited  
    .... ..0. .... = SACL Inherit Required  
    .... ...0 .... = DACL Inherit Required  
    .... .... ..0. .... = SACL Defaulted  
    .... .... ...0 .... = SACL Present  
    .... .... .... 0... = DACL Defaulted  
    .... .... .... .1.. = DACL Present  
    .... .... .... ..0. = Group Defaulted  
    .... .... .... ...0 = Owner Defaulted  
  
Owner: BUILTIN\Administrators  
Group: BUILTIN\Administrators  
DACL - ACEs
```

	ALLOW-Everyone-0x1f01ff	
	0... .. =	
Generic Read		
	.0... .. =	
Generic Write		
	..0. .... =	
Generic Execute		
	...0 .... =	
Generic All		
	.... ..0 .... =	
System Security		
	.... ....1 .... =	
Synchronize		
	.... ....1... .. =	
Write Owner		
	.... ....1... .. =	
Write DAC		
	.... ....1. .... =	
Read Control		
	.... ....1 .... =	
Delete		
	.... ....1 .... =	
Write Attributes		
	.... ....1... .. =	
Read Attributes		
	.... ....1... .. =	
Delete Child		
	.... ....1... .. =	
Execute		
	.... ....1 .... =	
Write EA		
	.... ....1... .. =	
Read EA		
	.... ....1... .. =	
Append		
	.... ....1. .... =	
Write		
	.... ....1 .... =	
Read		
	ALLOW-Everyone-0x10000000-OI CI IO	
	0... .. =	
Generic Read		
	.0... .. =	
Generic Write		
	..0. .... =	

Generic Execute	...	1	....	....	....	....	....	....	=
Generic All	....	...	0	....	....	....	....	....	=
System Security	....	....	...	0	....	....	....	....	=
Synchronize	....	....	....	...	0	....	....	....	=
Write Owner	....	....	....	...	0	....	....	....	=
Write DAC	....	....	....	...	0	....	....	....	=
Read Control	....	....	....	...	0	....	....	....	=
Delete	....	....	....	...	0	....	....	....	=
Write Attributes	....	....	....	....	...	0	....	....	=
Read Attributes	....	....	....	....	....	...	0	....	=
Delete Child	....	....	....	....	....	...	0	....	=
Execute	....	....	....	....	....	...	0	....	=
Write EA	....	....	....	....	....	...	0	....	=
Read EA	....	....	....	....	....	...	0	....	=
Append	....	....	....	....	....	...	0	....	=
Write	....	....	....	....	....	...	0	....	=
Read	....	....	....	....	....	...	0	....	=

## CLI の概要を使用して、NTFS ファイルおよびフォルダに対して監査ポリシーを設定および適用する

ONTAP CLI を使用して NTFS ファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、NTFS セキュリティ記述子を作成し、SACL をセキュリティ記述子に追加します。次に、セキュリティポリシーを作成してポリシータスクを追加します。その後、Storage Virtual Machine (SVM) にセキュリティポリシーを適用します。

このタスクについて

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視して、適用した監査ポリシーの設定

を確認することができます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

## 関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[CLI を使用してファイルおよびフォルダのセキュリティを設定する場合の制限事項](#)

[セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法](#)

["SMB および NFS の監査とセキュリティトレース"](#)

[CLI を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

## NTFS セキュリティ記述子を作成します

NTFS セキュリティ記述子監査ポリシーの作成は、SVM 内のファイルやフォルダの NTFS Access Control List (ACL ; アクセス制御リスト) を設定および適用するための最初のステップです。このセキュリティ記述子をポリシータスクでファイルパスまたはフォルダパスに関連付けます。

### このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、Discretionary Access Control List (DACL ; 随意アクセス制御リスト) の 4 つの Access Control Entry (ACE ; アクセス制御エントリ) がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

オブジェクト	アクセスタイプ	アクセス権	権限の適用先
組み込み管理者	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
組み込みユーザ	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル
NT AUTHORITY\SYSTEM	許可 (Allow)	フルコントロール	このフォルダ、サブフォルダ、ファイル

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティ記述子の所有者

- 所有者のプライマリグループ
- raw 制御フラグ

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

#### 手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`  
  
`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. advanced権限レベルの場合は、admin権限レベルに戻ります。 `set -privilege admin`

**NTFS** セキュリティ記述子に **NTFS SACL** アクセス制御エントリを追加します

NTFS セキュリティ記述子への SACL（システムアクセス制御リスト）アクセス制御エントリ（ACE）の追加は、SVM 内のファイルやフォルダに対する NTFS 監査ポリシーを作成する 2 番目のステップです。エントリごとに、監査するユーザまたはグループを指定します。SACL エントリは、成功したアクセス試行と失敗したアクセス試行のどちらを監査するかを定義します。

このタスクについて

セキュリティ記述子の SACL には、1 つ以上の ACE を追加できます。

セキュリティ記述子に含まれている SACL に既存の ACE がある場合は、新しい ACE が SACL に追加されます。セキュリティ記述子に SACL が含まれていない場合は、SACL が作成され、その SACL に新しい ACE が追加されます。

SACLエントリを設定するには、で指定したアカウントの成功イベントまたは失敗イベントについて監査する権限を指定します -account パラメータ権限を指定する場合、次の 3 つの相互に排他的な方法があります。

- 権利

- 詳細な権限
- raw 権限（advanced 権限）



SACLエントリの権限を指定しない場合のデフォルト設定はです Full Control。

必要に応じて、で継承を適用する方法を指定して、SACLエントリをカスタマイズできます apply to パラメータこのパラメータを指定しない場合、デフォルトでは、この SACL エントリがこのフォルダ、サブフォルダ、およびファイルに適用されます。

#### 手順

1. SACLエントリをセキュリティ記述子に追加します。 `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
failure -account domain\joe -rights full-control -apply-to this-folder
-vserver vs1
```

2. SACLエントリが正しいことを確認します。 `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

#### セキュリティポリシーを作成する

Storage Virtual Machine（SVM）の監査ポリシーの作成は、ファイルまたはフォルダに対して ACL を設定および適用する 3 番目のステップです。ポリシーは、さまざまなタスクのコンテナとして機能します。各タスクは、ファイルまたはフォルダに適用できる単一のエントリです。あとで、このセキュリティポリシーにタスクを追加できます。

#### このタスクについて

セキュリティポリシーに追加するタスクには、NTFS セキュリティ記述子とファイルパスまたはフォルダパスとの間の関連付けが含まれます。そのため、セキュリティポリシーは、NTFS セキュリティ形式または mixed セキュリティ形式のボリュームを含む各 Storage Virtual Machine（SVM）に関連付ける必要があります。

## 手順

1. セキュリティポリシーを作成します。 `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. セキュリティポリシーを確認します。 `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver          Policy Name
-----
vs1              policy1
```

セキュリティポリシーにタスクを追加します

ACL を設定し、SVM 内のファイルやフォルダへ適用する 4 番目のステップでは、ポリシータスクを作成してセキュリティポリシーに追加します。ポリシータスクを作成するときに、セキュリティポリシーとタスクを関連付けます。セキュリティポリシーには、1 つ以上のタスクエントリを追加できます。

このタスクについて

セキュリティポリシーはタスクのコンテナです。タスクとは、NTFS または mixed セキュリティが設定されたファイルまたはフォルダ（ストレージレベルのアクセス保護を設定する場合はボリュームオブジェクト）へのセキュリティポリシーによって実行できる単一の処理を指します。

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

指定されたファイルやフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

指定されたボリュームにストレージレベルのアクセス保護のセキュリティ記述子を適用するタスクの指定に使用します。ストレージレベルのアクセス保護タスクで適用される ACL は ONTAP CLI からのみ管理できます。

タスクには、ファイル（またはフォルダ）やファイルセット（またはフォルダセット）のセキュリティ構成の定義が含まれています。ポリシー内のすべてのタスクは、一意のパスによって識別されます。1 つのポリシー内の 1 つのパスに含められるのは 1 つのタスクだけです。ポリシーに重複するタスクエントリを含めることはできません。

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10、000 個です。

- ポリシーには 1 つ以上のタスクを含めることができます。

ポリシーには複数のタスクを含めることができますが、ポリシーにファイルとディレクトリのタスクとストレージレベルのアクセス保護タスクの両方を含めることはできません。ポリシーに含めるタスクは、すべてストレージレベルのアクセス保護タスクにするか、すべてファイルとディレクトリのタスクにする必要があります。

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

次のオプションのパラメータを使用して、セキュリティ記述子の設定をカスタマイズできます。

- セキュリティタイプ
- プロパゲーションモード
- インデックス位置
- アクセス制御の種類

オプションのパラメータの値はストレージレベルのアクセス保護では無視されます。詳細については、マニュアルページを参照してください。

#### 手順

1. セキュリティ記述子が関連付けられているタスクをセキュリティポリシーに追加します。 `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` は、のデフォルト値です `-access-control` パラメータファイルとディレクトリのアクセスタスクを設定する場合、アクセス制御の種類の指定は任意です。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dirl1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. ポリシータスクの設定を確認します。 `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```



```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

## セキュリティポリシーを適用する

SVMへの監査ポリシーの適用は、ファイルまたはフォルダに対してNTFS ACLを作成および適用する最後のステップです。

### このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、FlexVol ボリューム（NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。



監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認してください。

### ステップ

1. セキュリティポリシーを適用します。 `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

## セキュリティポリシージョブを監視します

Storage Virtual Machine（SVM）にセキュリティポリシーを適用する場合、セキュリティポリシージョブを監視してその進行状況を監視できます。これは、セキュリティポリシーの適用が成功したかどうかを確認するのに役立ちます。また、多数のファイルやフォルダに一括してセキュリティ設定を適用するような長時間のジョブを実行する場合にも、この方法が便利です。

このタスクについて

セキュリティポリシージョブに関する詳細情報を表示するには、を使用します `-instance` パラメータ

#### ステップ

1. セキュリティポリシージョブを監視します。 `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

適用した監査ポリシーを確認します

Storage Virtual Machine（SVM）のファイルやフォルダにセキュリティポリシーを適用した場合に、それらの監査セキュリティの設定が意図したとおりになっているかを確認するには、監査ポリシーを確認します。

このタスクについて

を使用します `vserver security file-directory show` コマンドを使用して監査ポリシーの情報を表示します。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

#### ステップ

1. 監査ポリシーの設定を表示します。 `vserver security file-directory show -vserver vserver_name -path path`

#### 例

次のコマンドは、SVM vs1 のパス「/corp」に適用されている監査ポリシーの情報を表示します。このパスには、SUCCESS と SUCCESS/FAIL SACL の両方のエントリが適用されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

Vserver: vs1
File Path: /corp
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0x8014
Owner:DOMAIN\Administrator
Group:BUILTIN\Administrators
SACL - ACEs
    ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
    SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
DACL - ACEs
    ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
    ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
    ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
    ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

## セキュリティポリシージョブの管理に関する考慮事項

セキュリティポリシージョブが存在する場合、特定の状況下では、そのセキュリティポリシーやポリシーに割り当てられたタスクを変更できません。セキュリティポリシーの変更が確実に成功するように、ポリシーを変更できる条件やできない条件を理解しておく必要があります。ポリシーの変更には、ポリシーに割り当てられたタスクの追加、削除、変更と、ポリシーの削除または変更が含まれます。

セキュリティポリシーにジョブが存在し、そのジョブが次の状態の場合、そのポリシーまたはポリシーに割り当てられたタスクは変更できません。

- ジョブが実行中または実行中です。
- ジョブが一時停止中の場合
- ジョブが再開され、実行中の状態になります。
- ジョブが別のノードへのフェイルオーバーを待機中の場合。

セキュリティポリシーにジョブが存在する場合、次の状況下では、そのセキュリティポリシーまたはポリシーに割り当てられたタスクを正常に変更できます。

- ポリシージョブが停止されました。
- ポリシージョブが正常に終了しました。

## NTFS セキュリティ記述子を管理するコマンド

ONTAP には、セキュリティ記述子を管理するためのコマンドが用意されています。セキュリティ記述子に関する情報を作成、変更、削除、および表示できます。

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	<code>vserver security file-directory ntfs create</code>
既存の NTFS セキュリティ記述子を変更します	<code>vserver security file-directory ntfs modify</code>
既存の NTFS セキュリティ記述子に関する情報を表示します	<code>vserver security file-directory ntfs show</code>
NTFS セキュリティ記述子を削除します	<code>vserver security file-directory ntfs delete</code>

のマニュアルページを参照してください `vserver security file-directory ntfs` 詳細情報を表示するコマンドです。

## NTFS DACL アクセス制御エントリを管理するコマンド

ONTAP には、DACL のアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、NTFS DACL の ACE に関する情報を変更、削除、表示するなどで、既存の DACL を管理できます。

状況	使用するコマンド
ACE を作成して NTFS DACL に追加します	<code>vserver security file-directory ntfs dacl add</code>
NTFS DACL の既存の ACE の変更	<code>vserver security file-directory ntfs dacl modify</code>
NTFS DACL の既存の ACE に関する情報を表示します	<code>vserver security file-directory ntfs dacl show</code>
NTFS DACL から既存の ACE を削除します	<code>vserver security file-directory ntfs dacl remove</code>

のマニュアルページを参照してください `vserver security file-directory ntfs dacl` 詳細情報を

表示するコマンドです。

## NTFS SACLアクセス制御エントリの管理用コマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、NTFS SACL の ACE に関する情報を変更、削除、表示するなどで、既存の SACL を管理することができます。

状況	使用するコマンド
ACE を作成して NTFS SACL に追加します	<code>vserver security file-directory ntfs sacl add</code>
NTFS SACL の既存の ACE の変更	<code>vserver security file-directory ntfs sacl modify</code>
NTFS SACL の既存の ACE に関する情報を表示します	<code>vserver security file-directory ntfs sacl show</code>
NTFS SACL から既存の ACE を削除します	<code>vserver security file-directory ntfs sacl remove</code>

のマニュアルページを参照してください `vserver security file-directory ntfs sacl` 詳細情報を表示するコマンドです。

## セキュリティポリシーを管理するためのコマンド

ONTAP には、セキュリティポリシーを管理するためのコマンドが用意されています。ポリシーに関する情報を表示したり、ポリシーを削除したりできます。セキュリティポリシーを変更することはできません。

状況	使用するコマンド
セキュリティポリシーを作成する	<code>vserver security file-directory policy create</code>
セキュリティポリシーに関する情報を表示します	<code>vserver security file-directory policy show</code>
セキュリティポリシーを削除する	<code>vserver security file-directory policy delete</code>

のマニュアルページを参照してください `vserver security file-directory policy` 詳細情報を表示するコマンドです。

## セキュリティポリシータスクを管理するコマンド

ONTAP には、セキュリティポリシータスクを追加、変更、削除、および関連する情報表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシータスクを追加する	<code>vserver security file-directory policy task add</code>
セキュリティポリシータスクを変更する	<code>vserver security file-directory policy task modify</code>
セキュリティポリシータスクに関する情報を表示します	<code>vserver security file-directory policy task show</code>
セキュリティポリシータスクを削除する	<code>vserver security file-directory policy task remove</code>

のマニュアルページを参照してください `vserver security file-directory policy task` 詳細情報を表示するコマンドです。

## セキュリティポリシージョブの管理用コマンド

ONTAP には、セキュリティポリシージョブを一時停止、再開、停止、および関連する情報を表示するためのコマンドが用意されています。

状況	使用するコマンド
セキュリティポリシージョブを一時停止します	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
セキュリティポリシージョブを再開します	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>
セキュリティポリシージョブに関する情報を表示します	<code>vserver security file-directory job show -vserver vserver_name</code> このコマンドを使用して、ジョブのジョブIDを確認できます。
セキュリティポリシージョブを停止します	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

のマニュアルページを参照してください `vserver security file-directory job` 詳細情報を表示するコマンドです。

# SMB 共有のメタデータキャッシュを設定します

## SMB メタデータのキャッシングの仕組み

メタデータのキャッシングにより、SMB 1.0 クライアントでファイル属性をキャッシュして、ファイル属性およびフォルダ属性にすばやくアクセスできるようになります。属性のキャッシュは、共有ごとに有効または無効にすることができます。メタデータのキャッシングが有効な場合は、キャッシュされたエントリの TTL を設定することもできます。クライアントが SMB 2.x または SMB 3.0 で共有に接続している場合は、メタデータキャッシュの設定は必要ありません。

SMB メタデータのキャッシングを有効にすると、パスとファイルの属性データが一定期間保存されます。これにより、一般的なワークロードでの SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。

特定のタスクでは、SMB によって大量のトラフィックが作成され、そのトラフィックにはパスとファイルのメタデータに対する複数の同一クエリが含まれることがあります。代わりに、SMB メタデータのキャッシングを使用してキャッシュから情報を読み込むことで、重複するクエリの日数を減らし、SMB 1.0 クライアントのパフォーマンスを向上させることができます。



メタデータのキャッシングを使用すると、ごくまれに、古い情報が SMB 1.0 クライアントに提供されることがあります。ご使用の環境でこのリスクを回避する必要がある場合は、この機能を有効にしないでください。

## SMB メタデータのキャッシングを有効にします

SMB メタデータのキャッシングを有効にすることで、SMB 1.0 クライアントの SMB パフォーマンスを向上させることができます。デフォルトでは、SMB メタデータのキャッシングは無効になっています。

### ステップ

1. 必要な操作を実行します。

状況	入力するコマンド
共有の作成時に SMB メタデータのキャッシングを有効にする	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code>
既存の共有で SMB メタデータのキャッシングを有効にします	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</code>

### 関連情報

[SMB メタデータキャッシュエントリの有効期間の設定](#)

## SMB メタデータキャッシュエントリの有効期間を設定します

SMB メタデータキャッシュエントリの有効期間を設定できます。これにより、環境内での SMB メタデータキャッシュのパフォーマンスを最適化できます。デフォルトは10秒です。

作業を開始する前に

SMB メタデータキャッシュ機能を有効にしている必要があります。SMB メタデータのキャッシングが有効でない場合、SMB キャッシュの TTL 設定は使用されません。

ステップ

1. 必要な操作を実行します。

SMB メタデータキャッシュエントリの有効期間を設定する際の方法	入力するコマンド
共有を作成します	<pre>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</pre>
既存の共有を変更する	<pre>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</pre>

共有を作成または変更するときに、追加の共有設定オプションおよび共有プロパティを指定できます。詳細については、マニュアルページを参照してください。

## ファイルロックを管理します

### プロトコル間のファイルロックについて

ファイルロックは、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、クライアントアプリケーションで使用される方法です。ONTAP でファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントが NFS クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。



- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、`rmdir` および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、NFS の書き込みの処理はエラーになります。
- リンク解除

- NTFSファイルシステムでは、SMBとCIFSの削除処理がサポートされます。

ファイルは最後に閉じた後に削除されます。

- NFSのリンク解除処理はサポートされていません。

NTFSセマンティクスとSMBセマンティクスが必要であり、NFSでは前回の削除時のクローズ処理がサポートされないため、この処理はサポートされません。

- UNIXファイルシステムでは、リンク解除操作がサポートされます。

NFSとUNIXのセマンティクスが必要なため、サポートされています。

- 名前を変更する

- NTFSファイルシステムの場合、デスティネーションファイルがSMBまたはCIFSから開かれていれば、デスティネーションファイルの名前を変更できます。

- NFSの名前変更はサポートされていません。

NTFSセマンティクスとSMBセマンティクスが必要なため、サポートされていません。

UNIX セキュリティ形式のボリュームでは、NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、SMB のロック状態が考慮されます。

## ONTAP による読み取り専用ビットの処理方法

読み取り専用ビットは、ファイルが書き込み可能（無効）なのか読み取り専用（有効）なのかを示すために、ファイルごとに設定されます。

Windows を使用する SMB クライアントは、ファイルごとの読み取り専用ビットを設定できます。NFS クライアントは、ファイルごとの読み取り専用ビットを設定しません。NFS クライアントは、ファイルごとの読み取り専用ビットを使用するプロトコル操作を行わないためです。

ONTAP は、Windows を使用する SMB クライアントによってファイルが作成される際に、そのファイルに読み取り専用ビットを設定できます。ファイルが NFS クライアントと SMB クライアント間で共有されている場合も、ONTAP は読み取り専用ビットを設定できます。一部のソフトウェアは、NFS クライアントおよび SMB クライアントで使用される場合、読み取り専用ビットが有効になっている必要があります。

NFS クライアントと SMB クライアント間で共有されるファイルに対して、適切な読み取りおよび書き込み権限を保持するために、読み取り専用ビットが次の規則に従って処理されます。ONTAP

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファイルとして扱います。
- NFS クライアントがすべての書き込み権限ビットを無効にしたときに、これらのうち少なくとも 1 つが以前有効であったら、ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントがすべての書き込み権限ビットを有効にすると、ONTAP はそのファイルの読み取り専用ビットを無効にします。
- あるファイルの読み取り専用ビットが有効になっているときに、NFS クライアントがそのファイルの権限を調べようとすると、そのファイルの権限ビットは NFS クライアントには送信されず、代わりに書き込み権限ビットがマスクされた権限ビットが ONTAP クライアントに送信されます。
- ファイルの読み取り専用ビットが有効になっているときに、SMB クライアントがこの読み取り専用ビットを無効にすると、ONTAP はそのファイルに対する所有者の書き込み権限ビットを有効にします。
- 読み取り専用ビットが有効になっているファイルに書き込めるのは、root のみです。



ファイル権限の変更は、SMB クライアントではすぐに反映されますが、NFS クライアントが属性のキャッシュを有効にしている場合は NFS クライアントではすぐに反映されないことがあります。

## 共有パスコンポーネントのロックの処理に関する **ONTAP** と **Windows** の違い

Windows とは異なり、ONTAP では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因ではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパスコンポーネントの名前を変更できます。このため、特定のアプリケーションで原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、ユーザまたはアプリケーションが重要なディレクトリの名前を変更できないようにするセキュリティ設定を適用します。

## ロックに関する情報を表示します

有効になっているロックの種類とロックの状態、バイト範囲ロック、共有ロックモード、委譲ロック、および便宜的ロックの詳細、永続性ハンドルを使用してロックが開かれているかどうかなど、現在のファイルロックに関する情報を表示できます。

このタスクについて

NFSv4 または NFSv4.1 を使用して確立されたロックについては、クライアント IP アドレスを表示できません。

デフォルトでは、すべてのロックに関する情報が表示されます。コマンドパラメータを使用すると、特定の Storage Virtual Machine (SVM) のロックに関する情報を表示したり、他の条件によってコマンドの出力をフィルタリングしたりできます。

。 `vserver locks show` コマンドは、次の4種類のロックに関する情報を表示します。

- バイト範囲ロック。ファイルの一部のみをロックします。

- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。SMB を使用してクライアント側キャッシュを制御します。
- 委譲。NFSv4.x を使用してクライアント側キャッシュを制御します

オプションのパラメータを指定すると、各ロックタイプに関する重要な情報を確認できます。詳細については、コマンドのマニュアルページを参照してください。

## ステップ

1. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

## 例

次の例は、パスのファイルに対するNFSv4ロックに関する概要情報を表示します `/vol1/file1`。共有ロックのアクセスモードは `write-deny_none` であり、書き込み委譲でロックが許可されています。

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                    lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation -
                                     Delegation Type: write
```

次の例は、パスのファイルに対するSMBロックに関するoplockおよび共有ロックの詳細情報を表示します `/data2/data2_2/intro.pptx`。IP アドレスが 10.3.1.3 のクライアントに対して、共有ロックのアクセスモードを `write-deny_none` として、永続性ハンドルが許可されています。バッチの oplock レベルで oplock リースが許可されています。

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
```

```

    Bytelock is Superlock: -
        Bytelock is Soft: -
            Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: durable
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: -
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

## ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

## このタスクについて

。 `vserver locks break` コマンドは、advanced権限レベル以上でのみ使用できます。詳細については、コマンドのマニュアルページを参照してください。

## 手順

1. ロックを解除するために必要な情報を確認するには、を使用します `vserver locks show` コマンドを実行します

詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。 `set -privilege advanced`
3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、LIF 名、およびファイルパス	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
ロック ID	<code>vserver locks break -lockid UUID</code>

4. admin 権限レベルに戻ります。 `set -privilege admin`

# SMB のアクティビティを監視する

## SMB セッション情報を表示します

SMB 接続、SMB セッション ID、セッションを使用しているワークステーションの IP アドレスなど、確立された SMB セッションに関する情報を表示できます。セッションの SMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

## このタスクについて

SVM 上のすべてのセッションに関する情報を要約形式で表示できます。ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。

- オプションのを使用できます `-fields` 選択したフィールドに関する出力を表示するためのパラメータ。

入ることができます `-fields` ? 使用できるフィールドを決定します。

- を使用できます `-instance` 確立されたSMBセッションに関する詳細情報を表示するためのパラメータ。
- を使用できます `-fields` パラメータまたは `-instance` パラメータのみ、または他のオプションパラメータと組み合わせて指定します。

## ステップ

1. 次のいずれかを実行します。

表示する <b>SMB</b> セッション情報	入力するコマンド
SVM 上のすべてのセッションを要約形式で表示します	<code>vserver cifs session show -vserver vserver_name</code>
指定した接続 ID のセッション	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
指定したワークステーションの IP アドレスからのセッションです	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
指定した LIF IP アドレスのセッションを表示します	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
指定したノード上のセッションを表示します	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	指定した Windows ユーザからのセッションです
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	を指定します
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
指定したプロトコルバージョンを使用しているセッションです	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1
SMB3	SMB3_1}`
	[NOTE] ==== 継続的可用性を備えた保護と SMB マルチチャネルは、SMB 3.0 以降のセッションでのみ利用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を設定します SMB3 以降が必要です。  ====
指定したレベルの継続的可用性を備えた保護を使用しているセッション	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>

表示する <b>SMB</b> セッション情報	入力するコマンド
Yes	Partial}`  [NOTE] ==== 継続的可用性のステータスがある場合 Partial`つまり、継続的可用性を備えた開いている ファイルがセッションに少なくとも1つ含まれて いますが、継続的可用性を備えた保護を使用して開 かれていないファイルがセッションに含まれていま す。を使用できます `vserver cifs sessions file show コマンドを使用して、確立されたセッ ションのどのファイルが継続的可用性を備えた保護 で開かれていないかを確認します。  ====
指定した SMB 署名セッションステータスのセッ ション	`vserver cifs session show -vserver vs1 -is-session-signed {true

## 例

次のコマンドを実行すると、IP アドレスが 10.1.1.1 のワークステーションから確立された SVM vs1 上のセッションに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver: vs1
Connection Session
ID          ID          Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1          10.1.1.1        DOMAIN\joe        2         23s
```

次のコマンドを実行すると、SVM vs1 上の継続的可用性を備えた保護を使用するセッションに関する詳細なセッション情報が表示されます。この接続はドメインアカウントを使用して確立されています。

```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
Node: node1  
Vserver: vs1  
Session ID: 1  
Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
Windows User: DOMAIN\SERVER1$  
UNIX User: pcuser  
Open Shares: 1  
Open Files: 1  
Open Other: 0  
Connected Time: 10m 43s  
Idle Time: 1m 19s  
Protocol Version: SMB3  
Continuously Available: Yes  
Is Session Signed: false  
User Authenticated as: domain-user  
NetBIOS Name: -  
SMB Encryption Status: Unencrypted
```

次のコマンドは、SVM vs1 上の SMB 3.0 と SMB マルチチャネルを使用しているセッションに関する情報を表示します。この例では、ユーザは LIF IP アドレスを使用して SMB 3.0 対応のクライアントからこの共有に接続しています。そのため、認証メカニズムはデフォルトの NTLMv2 になっています。継続的可用性を備えた保護を使用して接続するためには、Kerberos 認証を使用して接続を確立する必要があります。



```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```
Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

## 関連情報

[開いている SMB ファイルに関する情報を表示する](#)

## 開いている **SMB** ファイルに関する情報を表示します

SMB 接続、SMB セッション ID、ホスティングボリューム、共有名、共有パスなど、開いている SMB ファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

### このタスクについて

確立された SMB セッションで開いているファイルに関する情報を表示できます。これは、SMB セッション内の特定のファイルに関する SMB セッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、開いているファイルの一部が継続的可用性を備えた保護を使用して開いている場合と、残りのファイルが継続的可用性を備えた保護を使用して開かれていない場合（の値 -continuously-available フィールドに入力します vserver cifs session show コマンド出力はです Partial）の場合は、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

を使用して、Storage Virtual Machine (SVM) 上の確立されたSMBセッションのすべての開いているファイル

に関する情報を要約形式で表示できます `vserver cifs session file show` オプションのパラメータを指定しないコマンド。

ただし、多くの場合、大量の出力が返されます。オプションのパラメータを指定すると、出力に表示される情報をカスタマイズできます。これは、開いているファイルの一部のみにに関する情報を表示する場合に便利です。

- オプションのを使用できます `-fields` 選択したフィールドの出力を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

- を使用できます `-instance` 開いているSMBファイルに関する詳細情報を表示するためのパラメータ。

このパラメータは、単独で使用することも、他のオプションのパラメータと組み合わせて使用することもできます。

## ステップ

1. 次のいずれかを実行します。

表示する開いている <b>SMB</b> ファイル	入力するコマンド
をクリックします	<code>vserver cifs session file show -vserver vserver_name</code>
指定したノード上のセッションを表示します	<code>`vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	指定したファイル ID のファイル
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	指定した SMB 接続 ID のファイル
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	指定した SMB セッション ID のファイル
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	指定したホスティングアグリゲートのファイル
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	指定したボリュームのファイルです
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	指定した SMB 共有のファイル

表示する開いている <b>SMB</b> ファイル	入力するコマンド
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	指定した SMB パスのオブジェクト
<code>vserver cifs session file show -vserver vserver_name -path path</code>	指定したレベルの継続的可用性を備えた保護を使用しているファイル
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes}`  [NOTE] ==== 継続的可用性のステータスの場合 `No`つまり、これらの開いているファイルは、テイクオーバーやギブバックからの無停止でのリカバリには対応していません。また、可用性の高い関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。  ====
指定した再接続の状態のファイル	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

ほかにも、出力結果の絞り込みに使用できるオプションのパラメータがあります。詳細については、のマニュアルページを参照してください。

## 例

次の例は、SVM vs1 の開いているファイルに関する情報を表示します。

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:   1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r      data      data      Yes
Path: \mytest.rtf
```

次の例は、SVM vs1 のファイル ID 82 の開いている SMB ファイルに関する詳細情報を表示します。

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

## 関連情報

### SMB セッション情報の表示

## 使用可能な統計オブジェクトと統計カウンタを確認します

CIFS、SMB、監査、および BranchCache ハッシュの統計に関する情報を取得してパフォーマンスを監視する前に、データの取得に使用できるオブジェクトとカウンタを確認しておく必要があります。

## 手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. 次のいずれかを実行します。

確認する項目	入力するコマンド
使用可能なオブジェクト	statistics catalog object show
使用可能な特定のオブジェクト	statistics catalog object show object object_name
使用可能なカウンタ	statistics catalog counter show object object_name

使用可能なオブジェクトとカウンタの詳細については、マニュアルページを参照してください。

3. admin 権限レベルに戻ります。set -privilege admin

例

次のコマンドを実行すると、advanced 権限レベルで表示したときの、クラスタ内の CIFS および SMB アクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only  
when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog object show -object audit  
audit_ng          CM object for exporting audit_ng  
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs  
cifs              The CIFS object reports activity of the  
                  Common Internet File System protocol  
                  ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs  
nblade_cifs       The Common Internet File System (CIFS)  
                  protocol is an implementation of the  
Server  
                  ...
```

```
cluster1::*> statistics catalog object show -object smb1  
smb1              These counters report activity from the  
SMB  
                  revision of the protocol. For information  
                  ...
```

```
cluster1::*> statistics catalog object show -object smb2  
smb2              These counters report activity from the  
                  SMB2/SMB3 revision of the protocol. For  
                  ...
```

```
cluster1::*> statistics catalog object show -object hashd  
hashd             The hashd object provides counters to  
measure  
                  the performance of the BranchCache hash  
daemon.
```

```
cluster1::*> set -privilege admin
```

次のコマンドは、の一部のカウンタに関する情報を表示します `cifs advanced`権限レベルで表示されるオブジェクト。



この例では、で使用可能なカウンタの一部が表示されているわけではありません `cifs` オブジェクト。出力は切り捨てられます。

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

関連情報

[統計情報を表示します](#)

## 統計情報を表示します

CIFS と SMB 、監査、および BranchCache ハッシュに関する統計など、さまざまな統計を表示して、パフォーマンスを監視し、問題を診断することができます。

作業を開始する前に

を使用してデータサンプルを収集しておく必要があります `statistics start` および `statistics stop` オブジェクトに関する情報を表示する前のコマンド。

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。

統計を表示する対象	入力するコマンド
SMB のすべてのバージョン	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x と SMB 3.0	<code>statistics show -object smb2</code>
ノードの CIFS サブシステム	<code>statistics show -object nblade_cifs</code>
マルチプロトコルの監査	<code>statistics show -object audit_ng</code>
BranchCache ハッシュサービス	<code>statistics show -object hashd</code>
動的 DNS	<code>statistics show -object ddns_update</code>

詳細については、各コマンドのマニュアルページを参照してください。

3. `admin` 権限レベルに戻ります。 `set -privilege admin`

関連情報

[使用可能な統計オブジェクトと統計カウンタの確認](#)

[SMB 署名済みセッションの統計の監視](#)

[BranchCache 統計を表示します](#)

[統計を使用した自動ノードリファラルのアクティビティの監視](#)

["Microsoft Hyper-V および SQL Server 向けの SMB の設定"](#)

["パフォーマンス監視のセットアップ"](#)



## 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。