SMBを使用したファイル アクセスの管理

ONTAP 9

NetApp

February 12, 2026

目次

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 グループを使用した認証と許可

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ONTAP SMBユーザとグループについて学ぶ

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、その定義およびいくつかの基本的な情報を理解しておく必要があります。

- ローカル ユーザ

  一意のセキュリティ識別子（SID）が割り当てられたユーザ アカウント。アカウントが作成された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されます。

  ユーザ アカウントには次の用途があります。

  - ユーザに *User Rights Management* 権限を付与するために使用されます。
  - SVM が所有するファイルおよびフォルダ リソースへの共有レベルおよびファイルレベル アクセスを制御するために使用されます。

- ローカル グループ

  一意のSIDが割り当てられたグループ。グループが作成されたSVM上でのみ認識されます。グループに複数のメンバーが含まれます。メンバーとして指定できるのは、ローカル ユーザ、ドメイン ユーザ、ドメイン グループ、ドメイン マシンの各アカウントです。グループは作成、変更、削除できます。

  グループには次の用途があります。

  - メンバーに *User Rights Management* 権限を付与するために使用されます。
  - SVM が所有するファイルおよびフォルダ リソースへの共有レベルおよびファイルレベル アクセスを制御するために使用されます。

- ローカル ドメイン

  ローカル スコープが割り当てられたドメイン。スコープはSVMによって制限されます。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。

- セキュリティ識別子（**SID**）

  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。例えば、一般的なSIDは次の形式になります：S-1-5-21-3139654847-1303905135-2517279418-123456。

- **NTLM**認証

  CIFSサーバでユーザの認証に使用される、Microsoft Windowsのセキュリティ方式。

- クラスター複製データベース（**RDB**）

  クラスタ内の各ノードにインスタンスがある、レプリケート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**ONTAP SMB**ユーザーと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。

  ワークグループにローカル ユーザを設定する必要があります。

- 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 ユーザーに *User Rights Management* 権限を割り当てる必要があります。

  User Rights Management は、SMBサーバ管理者がSVM上のユーザとグループの権限を制御する機能です。ユーザに権限を割り当てるには、ユーザのアカウントに権限を割り当てるか、その権限を持つ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管理に役立ちます。

- 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。
- カスタマイズされた_User Rights Management_権限を持つローカルグループを作成します。

  組み込みのユーザ グループの一部には権限があらかじめ定義されています。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。そのあとで、作成したローカル 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 ユーザ認証について

- サポートされる権限の一覧

ローカル**ONTAP SMB**ユーザ認証について

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る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ります。

- ドメイン部分が一致する

  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ない

  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。失敗した場合は、認証の失敗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、CIFSサーバ上の対応するローカル ユーザ アカウントの使用は試行されません。代わりに、認証は失敗します。NetBIOSドメイン名が一致しなくてもCIFSサーバ上の対応するローカル アカウント（存在する場合）が認証に使用されるケースはほかにもあります。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は、CIFSサーバ上の対応するローカル アカウントが認証に使用されます。

- ドメイン部分が指定されていない

  まず、ローカル ユーザとしての認証が試行されます。ローカル ユーザとしての認証に失敗した場合は、CIFSサーバが属しているドメインのドメイン コントローラでユーザが認証されます。

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、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

サーバ上のローカルユーザ認証を有効または無効にする

ONTAP SMB ユーザーアクセストークンについて学ぶ

ユーザーが共有をマップすると、認証されたSMBセッションが確立され、ユーザー、ユーザーのグループメンバーシップと累積権限、およびマップされたUNIXユーザーに関する情報を含むユーザーアクセストークンが構築されます。

この機能が無効になっていない限り、ローカルユーザーとグループの情報もユーザーアクセストークンに追加されます。アクセストークンの作成方法は、ログインがローカルユーザー用かActive Directoryドメインユーザー用かによって異なります：

- ローカルユーザーログイン

  ローカルユーザーは異なるローカルグループのメンバーになることができますが、ローカルグループは他のローカルグループのメンバーになることはできません。ローカルユーザーアクセストークンは、特定のローカルユーザーが所属するグループに割り当てられたすべての権限の集合で構成されます。

- ドメインユーザーログイン

  ドメインユーザがログインすると、ONTAPはユーザSIDと、そのユーザが所属するすべてのドメイングループのSIDを含むユーザアクセストークンを取得します。ONTAPは、ドメインユーザアクセストークンと、ユーザの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）によって提供されるアクセストークン、およびドメインユーザまたはそのドメイングループメンバーシップに割り当てられた直接権限を結合したものを使用します。

ローカルユーザーとドメインユーザーのログインの両方において、ユーザーアクセストークンにはプライマリグループRIDも設定されます。デフォルトのRIDは `Domain Users`（RID 513）です。このデフォルトを変更することはできません。

Windows から UNIX へ、および UNIX から Windows への名前マッピングプロセスは、ローカルアカウントとドメインアカウントの両方に対して同じ規則に従います。

> UNIXユーザーからローカルアカウントへの暗黙的な自動マッピングは存在しません。これが必要な場合は、既存の名前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 **ONTAP SMB SVM** で **SnapMirror** を使用する方法について学習します

ローカル グループを含む SVM が所有するボリュームで SnapMirror を設定する場合は、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、または共有に適用されるACEでは、ローカル グループは使用できません。SnapMirror機能を使用して別のSVM上のボリュームにDRミラーを作成する場合、そのボリュームにローカル グループのACEが設定されていても、そのACEはミラー上では無効です。データが別のSVMにレプリケートされると、データは実質的に別のローカル ドメインに渡されることになります。ローカル ユーザーとグループに付与された権限は、それらが元々作成されたSVMのスコープ内でのみ有効です。

ONTAP SMBサーバの削除がユーザとグループに与える影響について学習します

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 ユーザとローカル 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、削除した場合のローカル ユーザとローカル グループへの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に関連付けられているため、セキュリティの観点から、CIFSサー

バを削除しても削除されることはありません。ただし、削除はされませんが非表示になります。SVM上にCIFSサーバを再作成するまで、ローカル ユーザとローカル グループを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。

ローカルの**ONTAP SMB**ユーザーとグループで**Microsoft**管理コンソールを使用する方法を学びます

Microsoft Management Consoleからローカルユーザーおよびグループに関する情報を表示できます。このリリースのONTAPでは、Microsoft Management Consoleからローカルユーザーおよびグループの他の管理タスクを実行することはできません。

ONTAP SMB クラスタのリバートについて

ローカル ユーザとグループをサポートしていない ONTAP リリースにクラスタを戻す予定であり、ファイル アクセスまたはユーザ権限の管理にローカル ユーザとグループが使用されている場合は、特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により、ONTAPがローカル ユーザとグループの機能をサポートしていないバージョンに戻された場合でも、設定されたローカル 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 バージョンに戻すと、ONTAPは認証およびクレデンシャルの作成時にローカル ユーザとグループを使用しません。
- ローカル ユーザーとグループは、ファイルとフォルダーの ACL から削除されません。
- ローカル ユーザーまたはグループに付与された権限によって付与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 ユーザおよびグループ 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

サポートされている**ONTAP SMB**権限のリスト

ONTAPには、一連のサポートされる権限が事前に定義されています。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設定されています。事前定義グループの権限は追加、削除できます。また、新規のローカル 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事前定義グループを示します。

権限名	デフォルトのセキュリティ設定	概要
SeTcbPrivilege	なし	オペレーティング システムの一部として動作する
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	ACL を上書きしてファイルとディレクトリをバックアップする
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	ACLを無視してファイルおよびディレクトリをリストアします。ファイル所有者として、有効なユーザまたはグループのSIDを設定します。
SeTakeOwnershipPrivilege	BUILTIN\Administrators	ファイルなど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 セキュリティ ログの表示、ダンプ、消去など。
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は、フォルダ、シンボリックリンク、ジャンクションを経由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

- 権限の割り当てについて
- バイパス トラバース チェックの設定について学ぶ

ONTAP SMB権限の割り当てについて学ぶ

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。または、ユーザに付与したい権限と同じ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、ユーザに付与したい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。

- ユーザに付与したい権限と同じデフォルトの権限が割り当てられている事前定義のグループに、ローカル ユーザとドメイン ユーザを割り当てることもできます。

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の削除
- ローカルまたはドメインのユーザとグループの権限のリセット
- バイパス トラバース チェックの設定について学ぶ

ONTAP SMBサーバのBUILTINグループとローカル管理者アカウントについて学習します

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Guestアカウントは存在しません。

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ONTAP SMBユーザーパスワードの要件

デフォルトでは、ローカルユーザーのパスワードは複雑さの要件を満たす必要があります。パスワードの複雑さの要件は、Microsoft Windows _Local security policy_で定義されている要件と同様です。

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文字以上である必要があります。
- 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：

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

関連情報

- ローカル ユーザーのパスワードの複雑さを設定する
- サーバー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 パスワードの変更

定義済みの**BUILTIN**グループとデフォルトの**ONTAP SMB**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。BUILTINグループには、事前定義された権限が割り当てられています。

次の表に、事前定義グループを示します。

定義済みの**BUILTIN**グループ	デフォルトの権限
`BUILTIN\Administrators`RID 544 ローカル `Administrator`アカウント（RID 500）は、最初に作成されると自動的にこのグループのメンバーになります。ストレージ仮想マシン（SVM）がドメインに参加すると、 `domain\Domain Admins`グループがグループに追加されます。SVMがドメインから離脱すると、 `domain\Domain Admins`グループはグループから削除されます。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 このグループには、最初に作成された時点ではメンバーがありません。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。 • ローカル ユーザとローカル グループを作成、管理できます。 • 自分自身や他のオブジェクトを`BUILTIN\Administrators`グループに追加することはできません。	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 このグループには、最初に作成された時点ではメンバーがありません。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。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`

定義済みの**BUILTIN**グループ	デフォルトの権限
`BUILTIN\Users`RID 545 このグループが最初に作成された時点では、メンバーは存在しません（暗黙の `Authenticated Users`特殊グループを除く）。SVMがドメインに参加すると、`domain\Domain Users`グループはこのグループに追加されます。SVMがドメインから離脱すると、`domain\Domain Users`グループはこのグループから削除されます。	`SeChangeNotifyPrivilege`
`Everyone`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除く）。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

- サーバーのBUILTINグループとローカル管理者アカウントについて学習します
- サポートされる権限の一覧
- バイパス トラバース チェックの設定について学ぶ

ローカル ユーザとローカル グループ機能の有効化と無効化

ローカル**ONTAP SMB**ユーザとグループの機能について学習します

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 アカウントの変更
- ローカル グループの変更
- 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

ONTAP SMBサーバ上のローカル ユーザとグループを有効または無効にする

Storage Virtual Machine（SVM）で、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。

タスク概要

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。認証のためにローカル 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 ユーザとグループを... にしたい場合	コマンドを入力してください...
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
無効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

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

- サーバ上のローカルユーザ認証を有効または無効にする
- ローカル ユーザ アカウントの有効化と無効化

ONTAPのSMBサーバでローカルユーザ認証を有効または無効にする

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。

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しておく必要があります。

タスク概要

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。

ローカル認証を行う場合は...	コマンドを入力してください...
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
無効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

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 ユーザ認証について
- サーバ上のローカル ユーザとグループを有効または無効にする

ローカル ユーザ アカウントの管理

ローカルONTAP SMBユーザーアカウントを変更する

既存のユーザーのフルネームや説明を変更したい場合、またはユーザーアカウントを有効または無効にしたい場合は、ローカルユーザーアカウントを変更できます。また、ユーザー名が漏洩した場合や管理上の理由で名前を変更する必要がある場合は、ローカルユーザーアカウントの名前を変更することもできます。

状況	コマンドを入力してください...
ローカルユーザーのフルネームを変更する	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -full-name text` 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。
ローカルユーザーの説明を変更する	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -description text` 説明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 アカウントの有効化または無効化	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account-disabled {true
false}`	ローカル ユーザ アカウントの名前の変更

例

次の例では、ストレージ仮想マシン（SVM、旧称Vserver）vs1上のローカル ユーザー「`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ONTAP SMBユーザ アカウントを有効または無効にする

Storage Virtual Machine（SVM）に格納されたデータにユーザが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、SVMのデータにそのユーザが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。

タスク概要

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。

手順

1. 適切な処理を実行します。

状況	コマンドを入力してください...
ユーザ アカウントを有効にする	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false`
ユーザ アカウントを無効にする	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

ローカル**ONTAP SMB**ユーザー アカウントの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、またはユーザがパスワードを忘れた場合に役立ちます。

手順

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

次の例では、Storage Virtual Machine（SVM、旧称 Vserver）vs1 に関連付けられたローカル ユーザー「`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 ユーザーのパスワードの複雑さを設定する

サーバーのセキュリティ設定に関する情報を表示する

ONTAP SMBローカル ユーザに関する情報を表示する

すべてのローカル ユーザの一覧を概要形式で表示できます。特定のユーザに対するアカウント設定を確認する必要がある場合は、個別および複数のユーザのアカウント情報を

表示できます。この情報は、ユーザの設定を変更する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。

タスク概要

ユーザのパスワードに関する情報は表示されません。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
Storage Virtual Machine（SVM）のすべてのユーザに関する情報を表示する	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
特定のユーザの詳細なアカウント情報を表示する	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

コマンド実行時に選択できるオプションパラメータが他にもあります。"ONTAPコマンド リファレンス"の`vserver cifs`の詳細をご覧ください。

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**ONTAP SMB**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、ファイルやフォルダに対してユーザにどのレベルのアクセスを付与するかを決定できます。この情報は、ファイルやフォルダに対してユーザに付与すべきアクセス権を決定する際や、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際に役立ちます。

タスク概要

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。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
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する	`vserver cifs users-and-groups local-user show-membership -user-name` *user_name*
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する	`vserver cifs users-and-groups local-user show-membership -membership` *group_name*
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	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
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	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

例

次の例では、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あり、「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**ONTAP SMB**ユーザーアカウントを削除する

CIFSサーバに対するローカルSMB認証や、Storage Virtual Machine（SVM）に格納されたデータへのアクセス権の判断に必要なくなった場合、SVMからローカル ユーザ アカウントを削除できます。

タスク概要

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。

  そのユーザを参照するファイルおよびディレクトリのWindowsセキュリティ記述子には反映されません。

- メンバーシップおよび権限のデータベースからローカル ユーザへの参照がすべて削除されます。
- 一般に使用される標準のユーザ（Administratorなど）は削除できません。

手順

1. 削除するローカル ユーザー アカウントの名前を決定します `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. ローカルユーザーを削除します： `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. ユーザー 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

次の例では、SVM vs1に関連付けられたローカルユーザー「`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 グループの管理

ローカル**ONTAP SMB**グループを変更する

既存のローカル グループの説明を変更するか、グループの名前を変更することで、既存のローカル グループを変更できます。

状況	使用するコマンド
ローカルグループの説明を変更する	`vserver cifs users-and-groups local-group modify -vserver vserver_name -group-name group_name -description text` 説明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する	`vserver cifs users-and-groups local-group rename -vserver vserver_name -group-name group_name -new-group-name new_group_name`

例

次の例では、ローカル グループ “CIFS_SERVER\engineering” の名前を “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 “CIFS_SERVER\engineering” の説明を変更します：

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

ONTAP SMB ローカル グループに関する情報を表示する

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へのファイル 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。

手順

1. 次のいずれかを実行します。

...についての情報が必要な場合	コマンドを入力してください...
クラスタのすべてのローカル グループ	`vserver cifs users-and-groups local-group show`
SVMのすべてのローカル グループ	`vserver cifs users-and-groups local-group show -vserver vserver_name`

このコマンドを実行する際に選択できるオプション パラメータが他にもあります。"ONTAPコマンド リファレンス"の `vserver cifs`の詳細をご覧ください。

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::> 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
```

ローカル**ONTAP SMB**グループメンバーシップを管理する

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うえで役に立ちます。

タスク概要

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。

- 特別な *Everyone* グループにユーザー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SIDを名前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。

- 特別な *Everyone* グループ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。
- 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、ONTAPで解決できる必要があります。

手順

1. グループのメンバーを追加または削除します。

状況	次に、コマンドを使用します…
グループへのメンバーの追加	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`指定したローカルグループに追加するローカルユーザー、ドメインユーザー、またはドメイングループのコンマ区切りリストを指定できます。

状況	次に、コマンドを使用します...
グループからのメンバーの削除	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]`指定したローカル グループから削除するローカル ユーザー、ドメイン ユーザー、またはドメイン グループのコンマ区切りリストを指定できます。

次の例では、SVM vs1上のローカルグループ「SMB_SERVER\engineering」に、ローカルユーザー「SMB_SERVER\sue」とドメイングループ「AD_DOM\dom_eng」を追加します：

```
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
```

次の例では、SVM vs1上のローカルグループ"`SMB_SERVER\engineering`"からローカルユーザー"`SMB_SERVER\sue`"と"`SMB_SERVER\james`"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の表示

ローカル グループのメンバーに関する **ONTAP SMB** 情報を表示する

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。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合は	コマンドを入力してください...
クラスタのすべてのローカル グループのメンバー	`vserver cifs users-and-groups local-group show-members`
SVMのすべてのローカル グループのメンバー	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

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_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

ローカル**ONTAP SMB**グループを削除する

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権の判断や、グループ メンバーへのSVMユーザ権限の割り当てに必要なくなった場合、SVMからローカル グループを削除できます。

タスク概要

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には反映されません。

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

次の例では、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内の**ONTAP SMB**ドメインユーザー名とグループ名を更新する

CIFSサーバのローカル グループにドメイン ユーザとドメイン グループを追加できます。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。

タスク概要

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. 適切な処理を実行します。

ドメインユーザーとグループを更新する場合は...	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	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

ドメインユーザーとグループを更新する場合は...	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を表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
ドメイン ユーザとドメイン グループについて、更新できなかったものを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
更新に関するすべてのステータス情報を非表示にする	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

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に関連付けられたドメイン ユーザおよびグループの名前を更新します。前回の更新に基づいて、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::*> vserver cifs users-and-groups update-names -vserver 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
```

ローカル権限の管理

ONTAP SMB のローカルまたはドメイン ユーザーまたはグループに権限を追加する

権限を追加することで、ローカルまたはドメインのユーザーやグループのユーザー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たデフォルトの権限をオーバーライドします。これにより、ユーザーまたはグループの権限をカスタマイズできるため、セキュリティが強化されます。

開始する前に

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

タスク概要

オブジェクトに権限を追加すると、そのユーザーまたはグループのデフォルトの権限が上書きされます。権限を追加しても、以前に追加され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ーまたはグループに権限を追加するときは、次の点に留意する必要があります：

- 1 つ以上の権限を追加できます。
- 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がドメイン コントローラに接続できない場合、コマンドが失敗する可能性があります。

手順

1. ローカルまたはドメインのユーザーまたはグループに 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

次の例では、ストレージ仮想マシン（SVM、旧称Vserver）vs1上のユーザー「`CIFS_SERVER\sue`」に権限「`SeTcbPrivilege`」および「`SeTakeOwnershipPrivilege`」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
```

ONTAP SMBのローカルまたはドメインユーザーまたはグループから権限を削除します

権限を削除することで、ローカルまたはドメインのユーザーまたはグループのユーザー権限を管理できます。これにより、ユーザーとグループが持つ権限の上限をカスタマイズできるため、セキュリティが強化されます。

開始する前に

権限を削除す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。

タスク概要

ローカルまたはドメインのユーザーまたはグループから権限を削除するときは、次の点に留意する必要があります：

- 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がドメイン コントローラに接続できない場合、コマンドが失敗する可能性があります。

手順

1. ローカルまたはドメインのユーザー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. 目的の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

次の例では、ストレージ仮想マシン（SVM、旧称Vserver）vs1上のユーザー「`CIFS_SERVER\sue`」から権限「`SeTcbPrivilege`」および「`SeTakeOwnershipPrivilege`」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ーと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ーまたはグループの権限を変更した後、その変更が不要になった場合に役立ちます。

タスク概要

ローカルまたはドメインのユーザー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ー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上のユーザー「`CIFS_SERVER\sue`」の権限をリセットします。デフォルトでは、通常のユーザーにはアカウントに関連付けられた権限がありません：

```
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” の権限をリセットし、権限エントリを実質的に削除します：

```
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.
```

ONTAP SMB権限オーバーライドに関する情報を表示する

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、適切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。

手順

1. 次のいずれかを実行します。

...に関する情報を表示する場合は	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	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
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	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

このコマンドを実行する際に選択できるオプション パラメータが他にもあります。"ONTAPコマンド リファレンス"の `vserver cifs users-and-groups privilege show`の詳細をご覧ください。

例

次のコマンドは、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を表示します。

```
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の設定

ONTAP SMBバイパストラバースチェックの設定について学習します

トラバースチェックのバイパスは、ユーザーがトラバースされたディレクトリに対する権限を持っていない場合でも、ファイルへのパス内のすべてのディレクトリをトラバースできるかどうかを決定するユーザー権限（_権限_とも呼ばれます）です。トラバースチェックのバイパスを許可または禁止すると何が起こるか、また、Storage Virtual Machine（SVM）上のユーザーに対してトラバースチェックのバイパスを設定する方法について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と、中間ディレクトリのトラバース権限が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の設定

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、ユーザーがトラバース
チェックをバイパスでき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 ローカル グループまたはドメイン グループのメンバーが走査チェックをバイパスできるようにするには、 `SeChangeNotifyPrivilege`権限をそのグループに追加する必要があります。
- 個々のローカル ユーザーまたはドメイン ユーザーが走査チェックをバイパスできるようにしたいが、そのユーザーがその権限を持つグループのメンバーではない場合は、そのユーザー アカウントに `SeChangeNotifyPrivilege`権限を追加できます。
- いつでも `SeChangeNotifyPrivilege`権限を削除することで、ローカルまたはドメインのユーザーまたはグループに対する走査チェックのバイパスを無効にすることができます。

> 指定されたローカルまたはドメインのユーザーまたはグループのバイパス トラバーズ チェックを無効にするには、 `Everyone`グループから `SeChangeNotifyPrivilege`権限も削除する必要があります。

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の許可
- 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の禁止
- ボリューム上のファイル名変換の文字マッピングを設定する
- 共有アクセス制御リストを作成する
- 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
- サポートされる権限の一覧
- 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

ユーザーまたはグループが **ONTAP SMB** ディレクトリ トラバース チェックをバイパスできるようにする

ユーザーがファイルパス内のすべてのディレクトリをトラバースできるようにしたい場合、たとえトラバース先のディレクトリに対する権限がユーザーになくても、Storage Virtual Machine（SVM）上のローカルSMBユーザーまたはグループに `SeChangeNotifyPrivilege`権限を追加できます。デフォルトでは、ユーザーはディレクトリトラバースチェックをバイパスできます。

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。
- `SeChangeNotifyPrivilege`権限を追加するローカルまたはドメインのユーザーまたはグループが既に存在している必要があります。

タスク概要

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がドメイン コントローラに照会できない場合、コマンドが失敗することがあります。

手順

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

   > `-user-or-group-name`パラメータの値は、ローカル ユーザーまたはグループ、あるいはドメイン ユーザーまたはグループです。

2. 指定されたユーザーまたはグループでバイパス走査チェック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ーが、 `SeChangeNotifyPrivilege`権限をグループに追加することで、ディレクトリトラバースチェックをバイパスできるようにします：

```
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の禁止

ユーザーまたはグループが**ONTAP SMB**ディレクトリトラバースチェックをバイパスすることを禁止します

ユーザーがトラバースするディレクトリに対する権限を持っていないため、ファイルへのパス内のすべてのディレクトリをトラバースできないようにしたい場合は、ストレージ仮想マシン（SVM）上のローカルSMBユーザーまたはグループから`SeChangeNotifyPrivilege`権限を削除できます。

開始する前に

権限を削除す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。

タスク概要

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がドメイン コントローラに照会できない場合、コマンドが失敗することがあります。

手順

1. バイパストラバースチェックを禁止する： `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

   このコマンドは、 `-user-or-group-name *name*`パラメータの値で指定したローカルまたはドメインのユーザーまたはグループから `SeChangeNotifyPrivilege`権限を削除します。

2. 指定されたユーザーまたはグループで走査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

次のコマンドは、「EXAMPLE\eng」グループに属するユーザーがディレクトリトラバースチェックをバイパスすることを禁止します：

```
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の許可

ファイル セキュリティと監査ポリシーに関する情報の表示

ONTAP SMBファイルセキュリティと監査ポリシーの表示について学習します

Storage Virtual Machine（SVM）のボリューム内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の表示

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
- 混合

監査ポリシーに関する情報の表示

次のNASプロトコルを介したFlexVol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

ストレージレベルのアクセス保護（**SLAG**）セキュリティに関する情報の表示

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
- 混合
- 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の表示

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

- Storage-Level Access Guard を使用した安全なファイルアクセスについて学習します
- サーバ上の Storage-Level Access Guard に関する情報を表示する

ONTAP SMBファイルセキュリティに関する情報を**NTFS**セキュリティ形式のボリューム上に表示します

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。

タスク概要

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。出力には要約または詳細な一覧を表示できます。

- NTFSセキュリティ形式のボリュームとqtreeでは、NTFSファイル権限およびWindowsのユーザとグループのみを使用してファイルのアクセス権を判断するため、UNIX関連の出力フィールドのUNIXファイル権限情報は表示のみです。
- 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で設定できるので、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。
- 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。

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。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1 内のパス `/vol4`に関するセキュリティ情報を表示します：

```
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
```

次の例では、SVM vs1 内のパス `/data/engineering`に関する拡張マスク付きのセキュリティ情報を表示します：

```
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
```

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

次の例では、SVM vs1 内のパス `/datavol1`を持つボリュームのセキュリティ情報（ストレージレベルのアクセス ガードのセキュリティ情報を含む）を表示します：

```
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: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の表示

混合セキュリティ形式のボリューム上のONTAP SMB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。

タスク概要

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。出力には要約または詳細な一覧を表示できます。

- mixedセキュリティ形式のボリュームおよびqtreeは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびフォルダと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。
- 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 ビットの権限のみ（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、たとえ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で設定できるので、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。

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。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/projects`に関するセキュリティ情報を拡張マスク形式で表示します。この混合セキュリティ形式のパスは、UNIX 対応のセキュリティを備えています。

```
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、SVM vs1 内のパス `/data`のセキュリティ情報を表示します。この混合セキュリティ形式のパスには、NTFS 対応のセキュリティが適用されます。

```
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、SVM vs1のパス `/datavol5`にあるボリュームのセキュリティ情報を表示します。この混合セキュリティ形式のボリュームの最上位レベルには、UNIX対応のセキュリティが設定されています。このボリュームには、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の表示

UNIXセキュリティ形式のボリューム上のONTAP SMB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。

タスク概要

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。出力には要約または詳細な一覧を表示できます。

- ファイル権限の決定時、UNIXセキュリティ形式のボリュームおよびqtreeでは、UNIXファイル権限（モード ビットまたはNFSv4 ACL）のみが使用されます。
- 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 ビットの権限のみ（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。

- SVM に CIFS サーバが設定されている場合、UNIX ボリュームまたは qtree でストレージ レベルのアクセス ガード セキュリティがサポートされるため、出力には、 `-path`パラメータで指定されたボリュームまたは qtree に適用されたストレージ レベルのアクセス ガード セキュリティに関する情報が含まれることがあります。

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。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例では、SVM vs1 内のパス `/home`に関するセキュリティ情報を表示します：

```
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: -
```

次の例では、SVM vs1 内のパス `/home`に関するセキュリティ情報を拡張マスク形式で表示します：

```
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: -
```

関連情報

- 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
- 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の表示

SMB FlexVol ボリューム上の NTFS 監査ポリシーに関する情報を表示する ONTAP コマンド

FlexVolボリューム上のNTFS監査ポリシーに関する情報（セキュリティ スタイルと有効なセキュリティ スタイル、適用されている権限、システム アクセス制御リストに関する情報など）を表示できます。この結果を使用して、セキュリティ構成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。

タスク概要

Storage Virtual Machine（SVM）の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力には要約または詳細な一覧を表示できます。

- 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は、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- 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。
- mixedセキュリティ形式のボリュームまたはqtreeでは、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、ストレージレベルのアクセス保護セキュリティを設定できるため、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の出力には、標準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の表示時には、UNIX関連の出力フィールドに表示専用のUNIXファイル アクセス権情報が格納されます。

  ファイル アクセス権の決定時には、NTFSセキュリティ形式のファイルおよびフォルダで、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 ビットの権限のみ（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。

手順

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

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細な一覧	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/corp`の監査ポリシー情報を表示します。パスには NTFS 有効セキュリティが設定されています。NTFS セキュリティ記述子には、SUCCESS と SUCCESS/FAIL の両方の SACL エントリが含まれています。

```
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、SVM vs1 内のパス `/datavol1`の監査ポリシー情報を表示します。パスには、通常の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ガード SACL の両方が含まれています。

```
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
```

SMB FlexVol ボリューム上の NFSv4 監査ポリシーに関する情報を表示する ONTAP コマンド

ONTAP CLIを使用して、FlexVolボリューム上のNFSv4監査ポリシーに関する情報（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）を表示できます。これらの結果を使用して、セキュリティ設定の検証や監査の問題のトラブルシューティングを行うことができます。

タスク概要

ストレージ仮想マシン（SVM）の名前と、監査情報を表示するファイルまたはディレクトリへのパスを指定する必要があります。出力は、概要形式または詳細リスト形式で表示できます。

- UNIX セキュリティ形式のボリュームと qtree は、監査ポリシーに NFSv4 SACL のみを使用します。
- UNIX セキュリティ スタイルの混合セキュリティ スタイル ボリューム内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は、UNIXファイル権限（モード ビットまたはNFSv4 ACL）を使用するファイルおよびディレクトリと、NTFSファイル権限を使用するファイルおよびディレクトリを格納できます。

- 混合セキュリティ形式のボリュームの最上位レベルには、UNIX または NTFS の有効なセキュリティを設定でき、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 ビットの権限のみ（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 ガード セキュリティは、ボリューム ルートまたは qtree の有効なセキュリティ スタイルが UNIX であっても、混合セキュリティ スタイルのボリュームまたは qtree に設定できるため、ストレージ レベルのアクセス ガード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 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 ガードの NTFS SACL の両方が表示される場合があります。
- SVM に CIFS サーバが設定されている場合、UNIX ボリュームまたは qtree でストレージ レベルのアクセス ガード セキュリティがサポートされるため、出力には、 `-path`パラメータで指定されたボリュームまたは qtree に適用されたストレージ レベルのアクセス ガード セキュリティに関する情報が含まれることがあります。

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。

情報を表示する場合...	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1 内のパス `/lab`に関するセキュリティ情報を表示します。この UNIX セキュリティ形式のパスには、NFSv4 SACL があります。

```
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
```

ONTAP SMBファイルのセキュリティと監査ポリシー情報を表示する方法を学びます

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と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、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、そのパス配下のすべてのファイルとディレクトリの情報を表示できます。「」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（"`"）内に完全なパスを指定する必要があります。

例

ワイルドカード文字を使用した次のコマンドは、SVM vs1 のパス `/1/`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を表示します：

```
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、SVM vs1のパス `/vol1/a`下にある「*」という名前のファイルの情報を表示します。パスは二重引用符（" "）で囲まれています。

```
cluster::> vserver security file-directory show -vserver 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を使用した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の管理

SMB NTFSファイルセキュリティ、NTFS監査ポリシー、Storage-Level Access Guardを管理するためのONTAPコマンド

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、作業時間を大幅に短縮できます。

ONTAPがSVMボリュームに提供するもう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るストレージ オブジェクトへのアクセスに適用されます。

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。さらに、NFSや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およびqtreeに含まれるすべてのファイルとフォルダには、NTFS対応のセキュリティが適用されます。 `vserver security file-directory`コマンドファミリを使用して、NTFSセキュリティ形式のボリュームに以下の種類のセキュリティを実装できます：

- ボリュームに含まれるファイルや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

混合セキュリティ形式のボリュームおよびqtreeには、UNIX対応セキュリティが適用され、UNIXファイル権限（モードビットまたはNFSv4.x ACLとNFSv4.x監査ポリシーのいずれか）を使用するファイルとフォルダ、およびNTFS対応セキュリティが適用され、NTFSファイル権限と監査ポリシーを使用するファイルとフォルダが含まれる場合があります。 `vserver security file-directory`コマンドファミリーを使用して、混合セキュリティ形式のデータに以下の種類のセキュリティを適用できます：

- 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
- NTFS対応またはUNIX対応のセキュリティ形式のボリュームに対するストレージレベルのアクセス保護

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対応セキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルとフォルダが含まれます。 `vserver security file-directory`コマンドファミリを使用して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場合は、以下の点に留意してください：

- `vserver security file-directory`コマンド ファミリは、UNIXセキュリティ形式のボリュームおよびqtree上のUNIXファイル セキュリティおよび監査ポリシーの管理には使用できません。
- `vserver security file-directory`コマンド ファミリを使用して、ターゲット ボリュームを持つ SVM に CIFS サーバが含まれている場合、UNIX セキュリティ形式のボリュームにストレージ レベルのアクセス ガードを設定できます。

関連情報

- ファイルのセキュリティと監査ポリシーの表示について学習する
- サーバーに NTFS セキュリティ記述子を作成する
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド
- Storage-Level Access Guard を使用した安全なファイルアクセスについて学習します

SMBファイルとフォルダのセキュリティを設定するためのONTAPコマンド

リモート クライアントを介さずにファイルとフォルダーのセキュリティをローカルで適用および管理できるため、多数のファイルやフォルダーに一括してセキュリティを設定するのにかかる時間を大幅に短縮できます。

次のユースケースでは、CLI を使用してファイルとフォルダーのセキュリティを設定すると便利です：

- 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でのファイルのストレージ
- データの移行
- Windowsドメインの変更
- NTFS ファイルシステム全体にわたるファイルセキュリティと監査ポリシーの標準化

ONTAPコマンドを使用してSMBファイルとフォルダのセキュリティを設定する際の制限について学習します

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て ONTAP SMB ファイルおよびフォルダのセキュリティを適用する

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、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）が指定されたファイルまたはフォルダに対して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。

    - 任意アクセス制御リスト（DACL）

- システム アクセス制御リスト（SACL）

- 任意アクセス制御リスト（**DACL**）

  DACLには、ユーザ、グループ、およびコンピュータ オブジェクトのSIDリストと、ファイルまたはフォルダに対する操作アクセスの許可または拒否設定が含まれています。DACLには、0個以上のアクセス制御エントリ（ACE）が含まれます。

- システム アクセス制御リスト（**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個以上のアクセス制御エントリ（ACE）が含まれます。

- **Access Control Entries**（**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、特定のユーザー、グループ、またはコンピューター 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、特定のユーザー、グループ、またはコンピューター オブジェクトによって実行された指定されたアクションを監査するときにログに記録する成功イベントまたは失敗イベントを指定します。

- 権限の継承

  権限の継承とは、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表します。継承可能な権限のみが子オブジェクトに継承されます。親オブジェクトの権限を設定する際に、「`Apply to `this-folder sub-folders、および files`」を使用して、フォルダ、サブフォルダ、およびファイルに権限を継承するかどうかを指定できます。

関連情報

- "SMBおよびNFS監査とセキュリティトレース"
- ファイルとフォルダに監査ポリシーを設定および適用するためのコマンド

ONTAP SVMディザスタリカバリデスティネーションでローカル**SMB**ユーザまたはグループを使用するファイルディレクトリポリシーの適用について説明します

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 クラスタ上のソース SVM がソース SVM からデスティネーション クラスタ上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 のディザスタ リカバリ設定を構成できます。

次の 2 種類の SVM ディザスタ リカバリのいずれかを設定できます。

- IDの保持

  この構成では、SVM と CIFS サーバのアイデンティティが保持されます。

- ID を破棄しました

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

ID破棄設定のガイドライン

ID破棄設定において、ローカルユーザ、グループ、および権限設定を含むSVMソースの場合、ローカルドメイン名（ローカルCIFSサーバ名）をSVMデスティネーションのCIFSサーバ名と一致するように変更する必要があります。たとえば、ソースSVM名が「`vs1`」、CIFSサーバ名が「`CIFS1`」、デスティネーションSVM名が「`vs1_dst`」、CIFSサーバ名が「`CIFS1_DST`」の場合、「`CIFS1\user1`」というローカルユーザのローカルドメイン名は、デスティネーションSVM上で自動的に「`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 データベースではローカル ユーザ名とグループ名が自動的に変更されますが、ファイル ディレクトリ ポリシー設定（ `vserver security file-directory`コマンド ファミリを使用してCLIで設定されるポリシー）ではローカル ユーザ名またはグループ名は自動的に変更されません。

たとえば、「`vs1`」の場合、 `-account`パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定した場合、デスティネーションSVMの設定はデスティネーションのCIFSサーバ名を反映するように自動的に変更されません。

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

Vserver: vs1
  NTFS Security Descriptor Name: sd1

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

`vserver security file-directory modify`コマンドを使用して、
CIFSサーバ名をデスティネーションCIFSサーバ名に手動で変更する必要があります。

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

ローカル ユーザーまたはグループを含めることができるパラメーター設定を使用できるファイル ディレクトリ ポリシー構成コンポーネントは 3 つあります：

- セキュリティ記述子

  オプションで、セキュリティ記述子の所有者と、そ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およびプライマリ グループのエントリにローカル ユーザまたはグループが使用されている場合は、アカウント名にデスティネーション SVM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。 `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加えることができます。

- DACLエントリ

  各 DACL 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 アカウントを使用する DACL は、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を変更することはできないため、ローカル ユーザまたはグループを含む DACL 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 アカウント名で新しい DACL エントリを作成し、これらの新しい DACL エントリを適切なセキュリティ記述子に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 アカウントを使用する SACL は、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を変更することはできないため、ローカル ユーザまたはグループを含む SACL エントリをセキュリティ記述子から削除し、修正されたデスティネーション アカウント名で新しい SACL エントリを作成し、これらの新しい SACL エントリを適切なセキュリティ記述子に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 ディレクトリ ポリシー構成で使用されるローカル ユーザーまたはグループに必要な変更を加える必要があります。変更を行わないと、適用ジョブは失敗します。

CLIを使用したNTFSファイルおよびフォルダに対するファイル セキュリティの設定および適用

ONTAP SMBサーバにNTFSセキュリティ記述子を作成する

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）内のファイルとフォルダにNTFSアクセス制御リスト（ACL）を設定して適用するための最初のステップです。ポリシー タスクで、セキュリティ記述子をファイルまたはフォルダのパスに関連付けることができます。

タスク概要

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、または混在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が作成されると、そのセキュリティ記述子に4つの随意アクセス制御リスト（DACL）アクセス制御エントリ（ACE）が追加されます。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	権限	権限の適用先
BUILTIN\Administrators	許可	フル コントロール	このフォルダ、サブフォルダ、ファイル
BUILTIN\Users	許可	フル コントロール	このフォルダ、サブフォルダ、ファイル
CREATOR OWNER	許可	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	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 パラメータを使用して、セキュリティ記述子の構成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

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。詳細について

は、"ONTAPコマンド リファレンス"をご覧ください。

ONTAP SMBサーバ上のNTFSセキュリティ記述子にNTFS DACLアクセス制御エントリを追加する

NTFSセキュリティ記述子にDACL（随意アクセス制御リスト）アクセス制御エントリ（ACE）を追加することは、ファイルまたはフォルダにNTFS ACLを設定および適用するための2番目のステップです。各エントリは、アクセスを許可または拒否するオブジェクトを識別し、ACEで定義された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と実行できない操作を定義します。

タスク概要

セキュリティ記述子の DACL に 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。

`_
account`パラメータで指定され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、必要に応じてDACLエントリをカスタマイズできます。権限を指定するには、相互に排他的な3つの方法があります：

- 権限
- 高度な権利
- Raw 権限（advanced-privilege）

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

継承を適用する方法を指定して、必要に応じて DACL エントリをカスタマイズできます。

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"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 vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_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 vserver_name -ntfs-sd SD_name -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
```

`vserver security file-directory ntfs dacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+dacl["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP SMB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ACLを設定および適用するための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、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。セキュリティ ポリシーには後からタスクを追加できます。

タスク概要

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またはフォルダのパスと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を各SVM（NTFSセキュリティ形式のボリュームまたはmixedセキュリティ形式のボリュームを含む）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
```

ONTAP SMB セキュリティ ポリシーにタスクを追加する

ポリシー タスクを作成してセキュリティ ポリシーに追加することは、SVM 内のファイ

ルまたはフォルダに ACL を設定して適用するための 4 番目の手順です。ポリシー タスクを作成すると、そのタスクをセキュリティ ポリシーに関連付けます。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。

タスク概要

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、セキュリティ ポリシーによって NTFS または混合セキュリティのファイルまたはフォルダ（または Storage-Level Access Guard を設定している場合はボリューム オブジェクト）に対して実行できる単一の操作を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルとフォルダにセキュリティ記述子を適用するタスクを指定するために使用されます。ファイルおよびディレクトリタスクを通じて適用されたACLは、SMBクライアントまたはONTAP CLIを使用して管理できます。

- Storage-Level Access Guard 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セキュリティ記述子を適用するタスクを指定するために使用されます。ストレージレベルのアクセス保護タスクを通じて適用されたACLは、ONTAP CLIを通じてのみ管理できます。

タスクには、ファイル（またはフォルダ）またはファイルセット（またはフォルダ）のセキュリティ設定の定義が含まれます。ポリシー内の各タスクは、パスによって一意に識別されます。1つのポリシー内では、パスごとに1つのタスクのみを設定できます。ポリシー内に重複するタスクエントリを設定することはできません。

ポリシーにタスクを追加するためのガイドライン：

- ポリシーごとに最大 10,000 件のタスク エントリが可能です。
- 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、ファイル / ディレクトリ タスクとStorage-Level Access Guardタスクの両方を含むポリシーを設定することはできません。ポリシーには、すべてのStorage-Level Access Guardタスク、またはすべてのファイル / ディレクトリ タスクのいずれかを含める必要があります。

- Storage-Level Access Guard は、アクセス許可を制限するために使用されます。

  追加のアクセス権限を与えることはありません。

セキュリティ ポリシーにタスクを追加するときは、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 パラメータを使用して、セキュリティ記述子の構成をカスタマイズできます：

- セキュリティ タイプ
- 伝播モード
- インデックス位置
- アクセス制御の種類

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 関連付けられたセキュリティ記述子を持つ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 `-access-control`パラメータのデフォルト値です。ファイルおよびディレクトリ アクセス タスクを構成する際にアクセス制御の種類を指定することはオプションです。

   ```
   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 タスクの構成を確認します：`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
   ```

   `vserver security file-directory policy task`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy+task["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP SMB セキュリティ ポリシーを適用する

ファイル セキュリティ ポリシーを SVM に適用することは、NTFS ACL を作成してファイルまたはフォルダに適用する最後の手順です。

タスク概要

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（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 ポリシーと関連するDACL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。

手順

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
   ```

ONTAP SMBセキュリティ ポリシー ジョブを監視する

ストレージ仮想マシン（SVM）にセキュリティ ポリシーを適用する際、セキュリティ ポリシー ジョブを監視することでタスク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場合に役立ちます。また、多数のファイルやフォルダに一括でセキュリティを適用する、実行時間が長いジョブがある場合にも役立ちます。

タスク概要

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、 `-instance` パラメータを使用する必要があります。

手順

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
```

ONTAP SMBファイルのセキュリティを確認する

ファイルセキュリティ設定を検証して、セキュリティポリシーを適用したStorage Virtual Machine（SVM）上のファイルまたはフォルダに必要な設定がされているかどうかを確認できます。

タスク概要

データが格納されているSVMの名前と、セキュリティ設定を確認するファイルおよびフォルダへのパスを指定する必要があります。オプションの `-expand-mask`パラメータを使用すると、セキュリティ設定の詳細情報を表示できます。

手順

1. ファイルとフォルダのセキュリティ設定を表示： `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
```

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

NTFS ファイルとフォルダに SMB 監査ポリシーを設定して適用するための ONTAP コマンド

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。

タスク概要

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

- Storage-Level Access Guard を使用した安全なファイルアクセスについて学習します
- コマンドを使用してSMBファイルとフォルダのセキュリティを設定する際の制限について学習します
- セキュリティ記述子を使用してファイルとフォルダのセキュリティを適用する
- "SMBおよびNFS監査とセキュリティトレース"
- サーバーに NTFS セキュリティ記述子を作成する

ONTAP SMBサーバにNTFSセキュリティ記述子を作成する

NTFSセキュリティ記述子監査ポリシーの作成は、SVM内のファイルとフォルダにNTFSアクセス制御リスト（ACL）を設定および適用するための最初のステップです。ポリシー タスクで、セキュリティ記述子をファイルまたはフォルダのパスに関連付けます。

タスク概要

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、または混在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が作成されると、そのセキュリティ記述子に4つの随意アクセス制御リスト（DACL）アクセス制御エントリ（ACE）が追加されます。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	権限	権限の適用先
BUILTIN\Administrators	許可	フル コントロール	このフォルダ、サブフォルダ、ファイル
BUILTIN\Users	許可	フル コントロール	このフォルダ、サブフォルダ、ファイル
CREATOR OWNER	許可	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	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 パラメータを使用して、セキュリティ記述子の構成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

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 高度な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構成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. 上級権限レベルの場合は、管理者権限レベルに戻ります： `set -privilege admin`

SVM内のファイルまたはフォルダに対するNTFS監査ポリシーを作成するための2番目のステップは、NTFSセキュリティ記述子に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）を追加することです。各エントリは、監査対象となるユーザーまたはグループを識別します。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。

タスク概要

セキュリティ記述子の SACL に 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DACLに新しいACEが追加されます。

`-account`パラメータで指定され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することで、`SACL` エントリを設定できます。権限を指定するには、互いに排他的な `3` つの方法があります：

- 権限
- 高度な権利
- Raw 権限（advanced-privilege）

SACL エントリの権限を指定しない場合、デフォルト設定は `Full Control`になります。

`apply to`パラメータを使用して継承の適用方法を指定することにより、必要に応じて`SACL`エントリをカスタマイズできます。このパラメータを指定しない場合は、デフォルトでこの`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. セキュリティ記述子に SACL エントリを追加します `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
```

ONTAP SMBセキュリティ ポリシーを作成する

ストレージ仮想マシン（SVM）の監査ポリシーの作成は、ファイルまたはフォルダにACLを設定および適用するための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、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。セキュリティ ポリシーには後からタスクを追加できます。

タスク概要

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またはフォルダのパスと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セキュリティ形式のボリュームまたは混在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
```

ONTAP SMB セキュリティ ポリシーにタスクを追加する

ポリシー タスクを作成してセキュリティ ポリシーに追加することは、SVM 内のファイルまたはフォルダに ACL を設定して適用するための 4 番目の手順です。ポリシー タスクを作成すると、そのタスクをセキュリティ ポリシーに関連付けます。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。

タスク概要

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、セキュリティ ポリシーによって NTFS または

混合セキュリティのファイルまたはフォルダ（または Storage-Level Access Guard を設定している場合はボリューム オブジェクト）に対して実行できる単一の操作を指します。

タスクには次の2種類があります。

- ファイルとディレクトリのタスク

  指定されたファイルとフォルダにセキュリティ記述子を適用するタスクを指定するために使用されます。ファイルおよびディレクトリタスクを通じて適用されたACLは、SMBクライアントまたはONTAP CLIを使用して管理できます。

- Storage-Level Access Guard 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セキュリティ記述子を適用するタスクを指定するために使用されます。ストレージレベルのアクセス保護タスクを通じて適用されたACLは、ONTAP CLIを通じてのみ管理できます。

タスクには、ファイル（またはフォルダ）またはファイルセット（またはフォルダ）のセキュリティ設定の定義が含まれます。ポリシー内の各タスクは、パスによって一意に識別されます。1つのポリシー内では、パスごとに1つのタスクのみを設定できます。ポリシー内に重複するタスクエントリを設定することはできません。

ポリシーにタスクを追加するためのガイドライン：

- ポリシーごとに最大 10,000 件のタスク エントリが可能です。
- 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、ファイル / ディレクトリ タスクとStorage-Level Access Guardタスクの両方を含むポリシーを設定することはできません。ポリシーには、すべてのStorage-Level Access Guardタスク、またはすべてのファイル / ディレクトリ タスクのいずれかを含める必要があります。

- Storage-Level Access Guard は、アクセス許可を制限するために使用されます。

  追加のアクセス権限を与えることはありません。

次のオプション パラメータを使用して、セキュリティ記述子の構成をカスタマイズできます：

- セキュリティ タイプ
- 伝播モード
- インデックス位置
- アクセス制御の種類

ストレージレベルのアクセス保護では、オプションパラメータの値は無視されます。この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

手順

1. 関連付けられたセキュリティ記述子を持つ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 `-access-control`パラメータのデフォルト値です。ファイルおよびディレクトリ アクセス タスクを構成する際にアクセス制御の種類を指定することはオプションです。

```
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 タスクの構成を確認します： `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
```

`vserver security file-directory policy task`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy+task["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP SMB セキュリティ ポリシーを適用する

監査ポリシーを SVM に適用することは、NTFS ACL を作成してファイルまたはフォルダに適用する最後の手順です。

タスク概要

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（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 ポリシーと関連するDACL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。

手順

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
```

ONTAP SMBセキュリティ ポリシー ジョブを監視する

ストレージ仮想マシン（SVM）にセキュリティ ポリシーを適用する際、セキュリティ ポリシー ジョブを監視することでタスク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場合に役立ちます。また、多数のファイルやフォルダに一括でセキュリティを適用する、実行時間が長いジョブがある場合にも役立ちます。

タスク概要

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、 `-instance` パラメータを使用する必要があります。

手順

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
```

ONTAP SMB監査ポリシーを確認する

監査ポリシーを検証して、セキュリティポリシーを適用したStorage Virtual Machine（SVM）上のファイルまたはフォルダに必要な監査セキュリティ設定があることを確認できます。

タスク概要

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

手順

1. 監査ポリシー設定を表示： `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情報を表示します。このパスには、SUCCESS と SUCCESS/FAIL の両方の SACL 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
```

ONTAP SMBセキュリティポリシージョブの管理について学習します

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その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成功するように、どのような条件で変更できるか、または変更できないか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、または変更、およびポリシー自体の削除または変更が含まれます。

セキュリティ ポリシーのジョブが存在し、そのジョブが次の状態にある場合は、セキュリティ ポリシーまたはそのポリシーに割り当てられたタスクを変更することはできません：

- ジョブは実行中または進行中です。

- ジョブは一時停止されています。
- ジョブは再開され、実行状態になります。
- ジョブが別のノードへのフェイルオーバーを待機している場合。

次の状況では、セキュリティ ポリシーのジョブが存在する場合、そのセキュリティ ポリシーまたはその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。
- ポリシージョブは正常に終了しました。

SMBサーバー上のNTFSセキュリティ記述子を管理するためのONTAPコマンド

セキュリティ記述子を管理するための専用のONTAPコマンドがあります。セキュリティ記述子に関する情報を作成、変更、削除、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する	`vserver security file-directory ntfs create`
既存のNTFSセキュリティ記述子を変更する	`vserver security file-directory ntfs modify`
既存の NTFS セキュリティ記述子に関する情報を表示する	`vserver security file-directory ntfs show`
NTFSセキュリティ記述子を削除する	`vserver security file-directory ntfs delete`

`vserver security file-directory ntfs`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs["ONTAPコマンドリファレンス"^]をご覧ください。

SMBサーバ上のNTFS DACLアクセス制御エントリを管理するためのONTAPコマンド

DACL アクセス制御エントリ（ACE）を管理するための ONTAP 専用コマンドがあります。NTFS DACL にはいつでも ACE を追加できます。また、DACL 内の ACE に関する情報を変更、削除、表示することで、既存の NTFS DACL を管理することもできます。

状況	使用するコマンド
ACEを作成し、NTFS DACLに追加する	`vserver security file-directory ntfs dacl add`

状況	使用するコマンド
NTFS DACL 内の既存の ACE を変更する	`vserver security file-directory ntfs dacl modify`
NTFS DACL 内の既存の ACE に関する情報を表示する	`vserver security file-directory ntfs dacl show`
NTFS DACLから既存のACEを削除する	`vserver security file-directory ntfs dacl remove`

`vserver security file-directory ntfs dacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+dacl["ONTAPコマンドリファレンス"^]をご覧ください。

SMBサーバ上のNTFS SACLアクセス制御エントリを管理するためのONTAPコマンド

SACL アクセス制御エントリ（ACE）を管理するための ONTAP 専用コマンドがあります。NTFS SACL にはいつでも ACE を追加できます。また、SACL 内の ACE に関する情報を変更、削除、表示することで、既存の NTFS SACL を管理することもできます。

状況	使用するコマンド
ACEを作成し、NTFS SACLに追加する	`vserver security file-directory ntfs sacl add`
NTFS SACLの既存のACEを変更する	`vserver security file-directory ntfs sacl modify`
NTFS SACL内の既存のACEに関する情報を表示する	`vserver security file-directory ntfs sacl show`
NTFS SACLから既存のACEを削除する	`vserver security file-directory ntfs sacl remove`

`vserver security file-directory ntfs sacl`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+ntfs+sacl["ONTAPコマンドリファレンス"^]をご覧ください。

SMBセキュリティポリシーを管理するためのONTAPコマンド

セキュリティポリシーを管理するための特定のONTAPコマンドがあります。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	`vserver security file-directory policy create`
セキュリティポリシーに関する情報を表示する	`vserver security file-directory policy show`
セキュリティポリシーを削除する	`vserver security file-directory policy delete`

`vserver security file-directory policy`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy["ONTAPコマンドリファレンス"^]をご覧ください。

ONTAPのSMBセキュリティポリシータスク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 タスクの追加、変更、削除、および関連する情報の表示を行う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	`vserver security file-directory policy task add`
セキュリティポリシータスクの変更	`vserver security file-directory policy task modify`
セキュリティ ポリシー タスクに関する情報を表示する	`vserver security file-directory policy task show`
セキュリティ ポリシー タスクを削除する	`vserver security file-directory policy task remove`

`vserver security file-directory policy task`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+policy+task["ONTAPコマンドリファレンス"^]をご覧ください。

SMBセキュリティポリシージョブを管理するためのONTAPコマンド

セキュリティ ポリシー ジョブの一時停止、再開、停止、および情報表示を行うための ONTAP コマンドがあります。

状況	使用するコマンド
セキュリティ ポリシー ジョブを一時停止する	`vserver security file-directory job pause -vserver vserver_name -id integer`
セキュリティポリシージョブを再開する	`vserver security file-directory job resume -vserver vserver_name -id integer`
セキュリティ ポリシー ジョブに関する情報を表示する	`vserver security file-directory job show -vserver vserver_name` このコマンドを使用してジョブのジョブ ID を判別できます。
セキュリティポリシージョブを停止する	`vserver security file-directory job stop -vserver vserver_name -id integer`

`vserver security file-directory job`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+security+file-directory+job["ONTAPコマンドリファレンス"^]をご覧ください。

SMB共有のメタデータ キャッシュの設定

ONTAP SMBメタデータキャッシュについて学ぶ

メタデータキャッシュは、SMB 1.0クライアント上のファイル属性キャッシュを有効にし、ファイルおよびフォルダ属性への高速アクセスを実現します。属性キャッシュは共有ごとに有効または無効にできます。メタデータキャッシュが有効な場合は、キャッシュされたエントリの有効期限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経由で共有に接続している場合、メタデータキャッシュの設定は不要です。

有効にすると、SMBメタデータキャッシュはパスとファイル属性データを一定期間保存します。これにより、一般的なワークロードを持つSMB 1.0クライアントのSMBパフォーマンスが向上します。

特定のタスクでは、SMB は大量のトラフィックを発生させ、パスやファイルのメタデータに対する同一のクエリが複数回実行される場合があります。SMB メタデータキャッシュを使用してキャッシュから情報を取得することで、冗長なクエリの数を減らし、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。

可能性は低いですが、メタデータキャッシュがSMB 1.0クライアントに古い情報を提供する可能性があります。このリスクを許容できない環境では、この機能を有効にしないでください。

ONTAP SMBメタデータ キャッシュを有効にする

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パフォーマンスが向上します。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。

手順

1. 次のうち必要な操作を実行します。

状況	コマンドを入力してください...
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	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
既存の共有でSMBメタデータのキャッシングを有効にする	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

関連情報

- メタデータ キャッシュ エントリの有効期間を設定する
- 既存の共有の共有プロパティを追加または削除する

ONTAP 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

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ことで、環境内の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。

開始する前に

SMBメタデータキャッシュ機能を有効にする必要があります。SMBメタデータキャッシュが有効になっていない場合、SMBキャッシュTTL設定は使用されません。

手順

1. 次のうち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場合...	コマンドを入力してください...
共有を作成する	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
既存の共有の変更時	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

共有を作成または変更する際に、追加の共有設定オプションとプロパティを指定できます。"ONTAPコマンド リファレンス"の `vserver cifs share`の詳細をご覧ください。

ファイル ロックの管理

ONTAP プロトコル間の SMB ファイル ロックについて学ぶ

ファイル ロックとは、あるユーザがすでに開いているファイルに別のユーザがアクセスすることを防ぐ機能で、クライアント アプリケーションで使用されます。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。

- 混合ボリュームまたは NTFS ボリュームでは、 `rm`、 `rmdir`、 `mv`などのファイル操作によって NFS アプリケーションが失敗する可能性があります。
- 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ています。

    ファイルは最後に閉じたあとで削除されます。
  - NFSのリンク解除処理は、サポートされていません。

サポートされていない理由は、NTFSとSMBのセマンティクスが必要であり、NFSではLast Delete-On-Close処理がサポートされていないためです。

- 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ています。

  サポートされている理由は、NFSとUNIXのセマンティクスが必要だからです。

- 名前変更
  - NTFSファイルシステムでは、デスティネーション ファイルがSMBかCIFSから開かれている場合には、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。

    サポートされていない理由は、NTFSとSMBのセマンティクスが必要だからです。

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 SMB読み取り専用ビットについて学ぶ

読み取り専用ビットはファイルごとに設定され、ファイルが書き込み可能（無効）か読み取り専用（有効）かを反映します。

Windows を使用する SMB クライアントは、ファイルごとに読み取り専用ビットを設定できます。NFS クライアントでは、ファイルごとに読み取り専用ビットを使用するプロトコル操作がないため、ファイルごとに読み取り専用ビットは設定されません。

ONTAPは、Windowsを使用するSMBクライアントがファイルを作成する際に、そのファイルに読み取り専用ビットを設定できます。ONTAPは、NFSクライアントとSMBクライアント間でファイルを共有する場合にも、読み取り専用ビットを設定できます。NFSクライアントとSMBクライアントで使用される一部のソフトウェアでは、読み取り専用ビットを有効にする必要があります。

ONTAP が 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する適切な読み取りおよび書き込み権限を維持するために、読み取り専用ビットを次のルールに従って処理します：

- 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、書き込み許可ビットが有効になっていないものとして扱います。
- NFS クライアントがすべての書き込み許可ビットを無効にし、それらのビットの少なくとも 1 つが以前に有効になっていた場合、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。
- ファイルの読み取り専用ビットが有効になっていて、NFS クライアントがファイルの権限を検出しようとすると、ファイルの権限ビットは NFS クライアントに送信されません。代わりに、ONTAP は書き込み権限ビットをマスクした状態で権限ビットを NFS クライアントに送信します。
- 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、そのファイルに対する所有者の書き込み権限ビットが有効になります。
- 読み取り専用ビットが有効になっているファイルは、root のみが書き込み可能です。

読み取り専用ビットは、ACL および Unix モード ビットと次のように相互作用します：

ファイルに読み取り専用ビットが設定されている場合：

- そのファイルの ACL は変更されません。NFS クライアントには、読み取り専用ビットが設定される前と同じ ACL が表示されます。
- ファイルへの書き込みアクセスを許可する Unix モード ビットはすべて無視されます。
- NFS クライアントと SMB クライアントはどちらもファイルを読み取ることはできますが、変更することはできません。
- ACLとUNIXモードビットは、読み取り専用ビットが優先されるため無視されます。つまり、ACLが書き込みアクセスを許可していても、読み取り専用ビットによって変更は禁止されます。

ファイルに読み取り専用ビットが設定されていない場合：

- ONTAP は、ACL と UNIX モード ビットに基づいてアクセスを決定します。
  - ACL または UNIX モード ビットのいずれかが書き込みアクセスを拒否した場合、NFS および SMB クライアントはファイルを変更できません。
  - ACL も UNIX モード ビットも書き込みアクセスを拒否しない場合は、NFS および SMB クライアントはファイルを変更できます。

ファイル権限の変更は SMB クライアントでは直ちに有効になりますが、NFS クライアントが属性キャッシュを有効にしている場合は、NFS クライアントでは直ちに有効にならない場合があります。

共有パスコンポーネントのロック処理における **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問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。これにより、共有にアクセスできなくなる場合があります。

パス コンポーネントの名前変更で生じ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。

ONTAP SMB ロックに関する情報を表示する

現在のファイル ロックに関する情報を表示できます。これには、保持され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oplockに関する詳細、およびロックが永続ハンドルまたは永続ハンドルで開かれているかどうかが含まれます。

タスク概要

NFSv4またはNFSv4.1を通じて確立されたロックの場合、クライアントIPアドレスは表示できません。

デフォルトでは、このコマンドはすべてのロックに関する情報を表示します。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、他の基準で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：

- ファイルの一部のみをロックするバイト範囲ロック。
- 開いているファイルをロックする共有ロック。
- SMB 経由のクライアント側キャッシュを制御する便宜的ロック。
- NFSv4.x上のクライアント側キャッシュを制御する委任。

オプションパラメータを指定することで、各ロックの種類に関する重要な情報を確認できます。"ONTAPコマンド リファレンス"の `vserver locks show`の詳細をご覧ください。

手順

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

例

以下の例は、パス `/vol1/file1`のファイルに対するNFSv4ロックの概要情報を表示します。sharelockのアクセス モードはwrite-deny_noneで、ロックは書き込み委譲で付与されました：

```
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
```

以下の例は、パス `/data2/data2_2/intro.pptx`のファイルに対するSMBロックに関するoplockおよびsharelockの詳細情報を表示します。IPアドレス10.3.1.3のクライアントに、共有ロックアクセスモードwrite-deny_noneで永続ハンドルが付与されています。batch oplockレベルでリースoplockが付与されています（

```
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
```

ONTAP SMBロックを解除する

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。

タスク概要

この `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。 `vserver locks break`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

手順

1. ロックを解除するために必要な情報を見つけるには、 `vserver locks show` コマンドを使用します。

   `vserver locks show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

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。

指定してロックを解除する場合...	コマンドを入力してください...
SVM名、ボリューム名、LIF名、およびファイル パス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロックID	`vserver locks break -lockid UUID`

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

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

SMBアクティビティの監視

ONTAP SMB セッション情報を表示する

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。

タスク概要

Storage Virtual Machine（SVM）上のすべてのセッションに関する情報を概要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 `-fields`パラメータを使用して、選択したフィールドに関する出力を表示できます。

  `-fields ?`を入力すると、使用できるフィールドを確認できます。

- `-instance`パラメータを使用すると、確立された SMB セッションに関する詳細情報を表示できます。
- `-fields`パラメータまたは `-instance`パラメータは、単独で使用することも、他のオプション パラメータと組み合わせて使用することもできます。

手順

1. 次のいずれかを実行します。

SMB セッション情報を表示する場合：	入力するコマンド
SVM上のすべてのセッション（概要）	`vserver cifs session show -vserver vserver_name`
指定した接続ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
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	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定したLIF IPアドレス	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
指定したノード	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	指定したWindowsユーザからのセッション
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	指定した認証メカニズムを使用しているセッション
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`

SMB セッション情報を表示する場合：	入力するコマンド
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	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 継続的に利用可能な保護機能およびSMB Multichannelは、SMB 3.0以降のセッションでのみ利用できます。すべての該当セッションでこれらのステータスを表示するには、このパラメータの値を `SMB3`以降に設定する必要があります。 ====
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	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 継続的可用性ステータスが `Partial`の場合、セッションには少なくとも1つの継続的可用性ファイルが開かれていますが、継続的可用性保護が適用されていないファイルもいくつかあります。`vserver cifs sessions file show`コマンドを使用すると、確立されたセッション上のどのファイルで継続的可用性保護が適用されていないかを確認できます。 ====
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 vserver_name -is-session-signed {true

例

次のコマンドは、IPアドレス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情報を表示します。

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

次のコマンドは、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情報を表示します。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の表示

開いている **ONTAP 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も表示できます。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。

タスク概要

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、一部の開いているファイルが継続的に利用可能な保護で開かれており、一部のファイルが継続的に利用可能な保護で開かれていない SMB セッションがある場合（`vserver cifs session show`コマンド出力の `-continuously-available`フィールドの値が `Partial`）、このコマンドを使用して、継続的に利用可能でないファイルを判別できます。

`vserver cifs session file show`コマンドをオプション
パラメータなしで使用すると、ストレージ仮想マシン（SVM）上で確立されたSMBセッションで開いているすべてのファイルの情報を概要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。これは、開いているファイルの一部のみに関する情報を表示する場合に便利です。

- オプションの `-fields`パラメータを使用して、選択したフィールドに出力を表示できます。

  このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。

- `-instance`パラメータを使用すると、開いている SMB ファイルに関する詳細情報を表示できます。

  このパラメータは、単独で、または他のオプションのパラメータと組み合わせて使用できます。

手順

1. 次のいずれかを実行します。

開いている **SMB** ファイルを表示する場合：	入力するコマンド
SVM（概要）	`vserver cifs session file show -vserver vserver_name`
指定したノード	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	指定したファイルID
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定したSMB接続ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定したSMBセッションID
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホスティング アグリゲート
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	指定したボリューム

開いている **SMB** ファイルを表示する場合：	入力するコマンド
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定したSMB共有
`vserver cifs session file show -vserver vserver_name -share share_name`	指定したSMBパス
`vserver cifs session file show -vserver vserver_name -path path`	指定したレベルの継続的可用性の保護
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 継続的可用性ステータスが `No`の場合、これらのオープンファイルはテイクオーバーおよびギブバックから無停止でリカバリできないことを意味します。また、高可用性関係にあるパートナー間の一般的なアグリゲートの再配置からもリカバリできません。 ====
指定した再接続状態	`vserver cifs session file show -vserver vserver_name -reconnected {No

出力結果を絞り込むために使用できる追加のオプションパラメータがあります。 `vserver cifs session file show`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

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::> vserver cifs session file show -vserver 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

セッション情報を表示する

ONTAP SMBサーバで利用可能な統計、オブジェクト、カウンタを特定する

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、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。

決定したい場合は...	入力する内容
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に関する情報	`statistics catalog object show -object object_name`
使用可能なカウンタ	`statistics catalog counter show -object object_name`

`statistics catalog object show`の詳細（使用可能なオブジェクトやカウンターなど）については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-catalog-object-show.html["ONTAPコマンド リファレンス"^]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、高度な権限レベルで表示される `cifs`オブジェクトのいくつかのカウンターに関する情報を表示します。

> この例では、 `cifs`オブジェクトに使用可能なすべてのカウンターが表示されるわけではなく、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

- 統計の表示

- "統計カタログカウンターオブジェクトの表示"
- "statistics start"

ONTAP SMB統計を表示する

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。

開始する前に

オブジェクトに関する情報を表示するには、 `statistics start`コマンドと `statistics stop`コマンドを使用してデータ 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`
> の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=statistics["ONTAPコマンド リファレンス"^]をご覧ください。

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。

...の統計情報を表示する場合	入力する内容
SMBのすべてのバージョン	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.xとSMB 3.0	`statistics show -object smb2`
ノードのCIFSサブシステム	`statistics show -object nblade_cifs`
マルチプロトコルの監査	`statistics show -object audit_ng`
BranchCacheハッシュ サービス	`statistics show -object hashd`
動的DNS	`statistics show -object ddns_update`

> `statistics show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/statistics-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

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

関連情報

- サーバー上で利用可能な統計、オブジェクト、カウンターを決定する
- SMB署名済みセッションの統計の監視
- BranchCache統計の表示
- 統計を使用した自動ノード リファーラル 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"