SMBを使用したファイルアクセスの管理
ONTAP 9

NetApp
December 20, 2024

目次

SMBを使用したファイルアクセスの管理

ローカルユーザとローカルグループを認証と許可に使用する

ONTAPでのローカルユーザとローカルグループの使用方法

ローカルユーザとローカルグループの概念

環境でローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループとは何か、およびそれらに関するいくつかの基本情報を把握しておく必要があります。

- * ローカルユーザー *

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

  ユーザアカウントには次のような用途があります。

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

- * ローカルグループ *

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

  グループにはいくつかの用途があります。

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

- * ローカルドメイン *

  ローカルスコープを持つドメイン。SVMでバインドされています。ローカルドメインの名前はCIFSサーバの名前です。ローカルユーザとローカルグループはローカルドメイン内に格納されます。

- * Security Identifier （ SID ；セキュリティ識別子） *

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

- * NTLM 認証 *

  CIFSサーバでユーザを認証するために使用されるMicrosoft Windowsのセキュリティ方式。

- * 複製されたクラスタデータベース（ RDB ） *

  クラスタ内の各ノード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。ローカルユーザオブジェクトとローカルグループオブジェクトはRDBに格納されます。

ローカルユーザおよびローカルグループを作成する理由

Storage Virtual Machine（SVM）でローカルユーザやローカルグループを作成する理由はいくつかあります。たとえば、ドメインコントローラ（DC）を使用できない場合でも、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。また、ローカルグループを使用してPrivilegesを割り当てたり、SMBサーバがワークグループに含まれている場合もあります。

ローカルユーザアカウントを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメインユーザを使用できません。

  ワークグループを設定するにはローカルユーザが必要です。

- ドメインコントローラを使用できない場合に、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は、ローカルユーザはNTLM認証を使用してSMBサーバに認証できます。

- ローカル・ユーザに _ ユーザ権限の管理 _ 権限を割り当てる

  User Rights Management は、ユーザとグループに付与する SVM の権限を SMB サーバ管理者が制御できる機能です。ユーザにPrivilegesを割り当てるには、ユーザのアカウントにPrivilegesを割り当てるか、ユーザをそのPrivilegesを含む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は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメイングループを使用できません。

  ローカルグループはワークグループ構成では必要ありませんが、ローカルワークグループユーザのアクセスPrivilegesの管理に役立ちます。

- 共有と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、ファイルおよびフォルダリソースへのアクセスを制御する。
- カスタマイズした _ ユーザ権限の管理 _ 権限を持つローカルグループを作成する。

  一部の組み込みユーザグループには、Privilegesが事前に定義されています。カスタマイズしたPrivilegesセットを割り当てるには、ローカルグループを作成し、そのグループに必要なPrivilegesを割り当てます。その後、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そのローカルグループに追加できます。

関連情報

ローカルユーザ認証の仕組み

サポートされるPrivilegesのリスト

ローカルユーザ認証の仕組み

ローカルユーザがCIFSサーバ上のデータにアクセスする前に、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はセッションの最初のセットアップ時に1回だけ確認できます。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は、3つのユースケースでローカル認証を使用します。それぞれのユースケースは、ユーザ名のドメイン部分（domain\user形式）がCIFSサーバのローカルドメイン名（CIFSサーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致する

  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は、CIFSサーバでローカルに認証されます。

- ドメイン部分が一致しません

  ONTAPは、CIFSサーバが属しているドメインのドメインコントローラでNTLM認証を試行します。認証に成功した場合は、ログインが完了します。成功しなかった場合、次に何が起こるかは、認証が成功しなかった理由によって異なります。

  たとえば、ユーザがActive Directoryに存在するにもかかわらず、パスワードが無効であるか期限切れになっている場合、ONTAPはCIFSサーバ上の対応するローカルユーザアカウントの使用を試みません。代わりに、認証は失敗します。NetBIOSドメイン名が一致しなくても、ONTAPが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）を認証に使用するケースは他にもあります。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、ONTAPはCIFSサーバ上の対応するローカルアカウントを認証に使用します。

- ドメイン部分が指定されていません

  ONTAPは最初にローカルユーザとしての認証を試行します。ローカルユーザとしての認証に失敗した場合、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ユーザを認証します。

ローカルユーザまたはドメインユーザの認証が完了すると、ONTAPはローカルグループメンバーシップとPrivilegesを考慮した完全なユーザアクセストークンを構築します。

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

関連情報

ローカルユーザ認証の有効化と無効化

ユーザアクセストークンの構成方法

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

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

- ローカルユーザログイン

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

- ドメイン・ユーザ・ログイン

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

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

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

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

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

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

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

CIFSサーバを削除したときのローカルユーザとローカルグループへの影響

CIFSサーバを作成するとデフォルトの一連のローカルユーザとローカルグループが作成され、CIFSサーバをホストするStorage Virtual Machine（SVM）に関連付けられます。SVM管理者は、ローカルユーザやローカルグループをいつでも作成できます。CIFSサーバを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に関連付けられます。そのため、セキュリティ上の理由から、CIFSサーバを削除してもそれらが削除されることはありません。CIFSサーバを削除してもローカルユー

ザとローカルグループは削除されませんが、表示されません。SVMでCIFSサーバを再作成するまで、表示したり管理したりすることはできません。

> CIFSサーバの管理ステータスは、ローカルユーザやローカルグループの表示には影響しません。

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

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

リバートに関するガイドライン

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

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

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

ローカル権限とは

サポートされる**Privileges**のリスト

ONTAPには、サポートされるPrivilegesのセットがあらかじめ定義されています。一部の事前定義されたローカルグループには、これらのPrivilegesの一部がデフォルトで追加されています。また、事前定義されたグループに対してPrivilegesを追加または削除したり、新しいローカルユーザまたはローカルグループを作成して、作成したグループや既存のドメインユーザおよびグループにPrivilegesを追加したり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Privilegesの一覧と、Privilegesが割り当てられているBUILTINグループの一覧を示します。

権限の名前	デフォルトのセキュリティ設定	説明
SeTcbPrivilege	なし	オペレーティングシステムの一部として機能
SeBackupPrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators	ACLを無視してファイルとディレクトリをバックアップ
SeRestorePrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators	ACLを無視してファイルとディレクトリをリストア有効なユーザまたはグループのSIDをファイル所有者として設定する
SeTakeOwnershipPrivilege	BUILTIN\Administrators	ファイルやその他のオブジェクトの所有権を取得する
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には、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース（x）権限は必要ありません。

関連情報

- ローカルPrivilegesの割り当て
- トラバースチェックのバイパスの設定

Privilegesの割り当て

Privilegesは、ローカルユーザまたはドメインユーザに直接割り当てることができます。また、ユーザに付与する機能と一致するPrivileges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。

  次に、そのユーザに割り当てるPrivilegesを含むグループにユーザを追加します。

- また、デフォルトのPrivilegesがユーザに付与するPrivilegesと一致する事前定義されたグループに、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へのPrivileges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からのPrivilegesの削除
- ロオカルマタハトメインノユウサトクルウフノPrivilegesノリセツト
- トラバースチェックのバイパスの設定

BUILTINグループとローカル管理者アカウントの使用に関するガイドライン

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アカウントの名前は変更できますが、削除することはできません。
- AdministratorアカウントはBUILTIN\Administratorsグループから削除できません。
- 組み込みグループの名前は変更できますが、削除することはできません。

  BUILTINグループの名前を変更すると、既知の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アカウントはありません。

関連情報

事前定義のBUILTINグループとデフォルトのPrivileges

ローカルユーザのパスワードの要件

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

パスワードは次の基準を満たしている必要があります。

- 6文字以上にする必要があります
- ユーザアカウント名を含めることはできません
- 次の4つのカテゴリのうち、少なくとも3つ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）
  - 10進数（0～9）
  - 特殊文字：

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

関連情報

ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFSサーバのセキュリティ設定に関する情報の表示

事前定義の**BUILTIN**グループとデフォルトの**Privileges**

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

事前定義の **BUILTIN** グループ	デフォルトの権限
`BUILTIN\Administrators`RID 544 最初に作成されたときに、RID 500のローカル `Administrator`アカウントが自動的にこのグループのメンバーになります。`Storage Virtual Machine`（`SVM`）がドメインに参加すると、`domain\Domain Admins`グループがグループに追加されます。`SVM`がドメインから削除されると`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および管理できます。 • 自分自身や他のオブジェクトをグループに追加することはできません `BUILTIN\Administrators`。	`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`

事前定義の **BUILTIN** グループ	デフォルトの権限
`BUILTIN\Users`RID 545 最初に作成された時点では、このグループには（暗黙的な特殊グループ以外に）メンバーはありませ`Authenticated Users`ん。SVMがドメインに参加すると、`domain\Domain Users`グループがこのグループに追加されます。SVMがドメインから削除されると、`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（匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。	`SeChangeNotifyPrivilege`

関連情報

BUILTINグループとローカル管理者アカウントの使用に関するガイドライン

サポートされるPrivilegesのリスト

トラバースチェックのバイパスの設定

ローカルユーザとローカルグループ機能の有効化と無効化

ローカルユーザとローカルグループの有効化と無効化の機能の概要

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、クラスタ内のいずれか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ないONTAPリリースにリバートされた場合にローカルユーザとローカルグループ機能が無効になります。クラスタ内のすべてのノードでこの機能をサポートするバージョンのONTAPが実行されるまで、ローカルユーザとローカルグループ機能は有効になりません。

関連情報

ローカルユーザアカウントを変更する

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へのPrivilegesの追加

ローカルユーザとローカルグループの有効化と無効化

Storage Virtual Machine（SVM）で、SMBアクセス用の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。

タスクの内容

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ます。必要に応じて、SMB接続の作成時の認証にローカルユーザを使用することもできます。認証にローカルユーザを使用するには、ローカルユーザとローカルグループ認証オプションも有効にする必要があります。

手順

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

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

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

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

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

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

関連情報

ローカルユーザ認証の有効化または無効化

ローカルユーザアカウントの有効化または無効化

ローカルユーザ認証の有効化または無効化

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接続できない場合や、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する必要があります。

タスクの内容

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にローカルユーザを使用する場合は、CIFSサーバのローカルユーザとローカルグループオプションも有効にする必要があります。

手順

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

ローカル認証の設定	入力するコマンド
有効	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
無効にする	`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

次の例では、SVM vs1でローカルユーザ認証を有効にします。

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

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

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

関連情報

ローカルユーザ認証の仕組み

ローカルユーザアカウントを管理します。

ローカルユーザアカウントを変更する

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

状況	入力するコマンド
ローカルユーザのフルネームの変更	`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。
ローカルユーザの概要を変更します	`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を有効または無効にする	`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を変更する

例

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

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

ローカルユーザアカウントの有効化または無効化

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

タスクの内容

ローカルユーザを有効にするには、ユーザアカウントを変更します。

ステップ

1. 適切な操作を実行します。

状況	入力するコマンド
ユーザアカウントを有効にする	`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`

ローカルユーザアカウントのパスワードの変更

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

ステップ

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

例

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

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

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

関連情報

ローカルSMBユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFSサーバのセキュリティ設定に関する情報の表示

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リストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認する場合は、そのユーザの詳細なアカウント情報だけでなく、複数のユーザのアカウント情報も表示できます。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のに役立ちます。また、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にも役立ちます。

タスクの内容

ユーザのパスワードに関する情報は表示されません。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
Storage Virtual Machine（SVM）上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`

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

例

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

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

ローカルユーザのグループメンバーシップに関する情報を表示する

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するユーザのアクセス権を決定できます。この情報は、ファイルやフォルダに対するユーザのアクセス権を決定する場合や、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役立ちます。

タスクの内容

コマンドをカスタマイズして、必要な情報のみを表示することができます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップ情報を表示する	`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

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

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

ローカルユーザアカウントを削除する

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

タスクの内容

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このユーザー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は調整されません。

- ローカルユーザへの参照は、メンバーシップデータベースとPrivilegesデータベースからすべて削除されます。
- 一般的な標準ユーザ（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アカウントの名前を確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. ローカルユーザを削除します。 `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. ユーザアカウントが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

例

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

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


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

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

ローカルグループを管理します。

ローカルグループの変更

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

状況	使用するコマンド
ローカルグループの概要を変更します	`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します	`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・グループの名前を 'CIFS_server\engineering' から 'CIFS_server\engineering_new' に変更します

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

次の例では ' ローカル・グループの概要を変更します

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

ローカルグループに関する情報を表示する

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。

ステップ

1. 次のいずれかを実行します。

必要な情報	入力するコマンド
クラスタのすべてのローカルグループ	`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ときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次の例では、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
```

ローカルグループメンバーシップを管理します。

ローカルグループメンバーシップの管理では、ローカルユーザまたはドメインユーザの追加と削除、またはドメイングループの追加と削除を行うことができます。これは、グループに設定されたアクセス制御に基づいてデータへのアクセスを制御する場合や、ユーザにそのグループにPrivilegesを関連付ける場合に便利です。

タスクの内容

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は次のとおりです。

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

ローカルグループからのメンバーの削除に関するガイドラインは次のとおりです。

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

ステップ

1. グループのメンバーを追加または削除します。

状況	使用するコマンド
グループ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[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループに追加できます。

状況	使用するコマンド
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[,...]`ローカルユーザ、ドメインユーザ、またはドメイングループをカンマで区切って指定し、指定したローカルグループから削除することができます。

次の例は、 SVM vs1 上のローカルグループ「 S MB_server\sue 」とドメイングループ「 AD_DOM\dom_eng 」をローカルグループ「 S MB_server\engineering 」に追加します。

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

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

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

関連情報

ローカルグループのメンバーに関する情報の表示

ローカルグループのメンバー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、ファイルアクセスの問題やユーザ権限の問題のトラブルシューティングに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
クラスタのすべてのローカルグループのメンバー	`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

次の例では、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
```

ローカルグループを削除します。

Storage Virtual Machine（SVM）に関連付けられたデータへのアクセス権を定義するためのローカルグループが不要になった場合や、グループメンバーへのSVMユーザ権限（Privileges）の割り当てに必要なくなった場合は、SVMからローカルグループを削除できます。

タスクの内容

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およびディレクトリのWindowsセキュリティ記述子は調整されません。

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

手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。 `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. ローカルグループを削除します。 `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. グループが削除されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

例

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

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

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

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

ローカルデータベースでのドメインユーザ名とドメイングループ名の更新

CIFSサーバのローカルグループにドメインユーザやドメイングループを追加できます。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する場合は、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。

タスクの内容

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

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. 適切な操作を実行します。

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループのうち、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`*

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループが正常に更新されたことを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
更新に失敗したドメインユーザとドメイングループのみを表示する	`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

次の例では、Storage Virtual Machine（SVM、旧Vserver）vs1に関連付けられているドメインユーザとドメイングループの名前を更新します。最後の更新では、依存する一連の名前を更新する必要があります。

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

cluster1::*> 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**Privileges**を管理します。

ローカルまたはドメインのユーザまたはグループへの**Privileges**の追加

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

開始する前に

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

タスクの内容

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

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

- 権限は 1 つ以上追加できます。
- Privilegesをドメインユーザまたはグループに追加するときに、ONTAPがドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

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

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上のPrivileges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. 目的のPrivilegesがオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

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

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

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

ローカルまたはドメインのユーザまたはグループから**Privileges**を削除する

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

開始する前に

Privileges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。

タスクの内容

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

- 1 つ以上の権限を削除できます。
- ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続してドメインユーザまたはグループを検証することがあります。

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

手順

1. ローカルまたはドメインのユーザまたはグループから1つ以上のPrivileges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Privilegesがオブジェクトから削除されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

例

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

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

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

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

ローカルまたはドメインのユーザとグループの**Privileges**をリセットします。

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

タスクの内容

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

手順

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

例

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

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

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

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

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

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

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

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

権限の上書きに関する情報を表示する

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Privilegesに関する情報を表示できます。この情報は、必要なユーザー権限が適用されているかどうかを判断するのに役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
Storage Virtual Machine（SVM）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用のカスタムPrivileges	`vserver cifs users-and-groups privilege show -vserver vserver_name`
SVM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Privileges	`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ときに選択できるオプションのパラメータがほかにもあります。詳細については、のマニュアルページを参照してください。

例

次のコマンドは、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Privileges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

トラバースチェックのバイパスの設定の概要

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

トラバースチェックのバイパスを許可または拒否した場合の動作

- 許可した場合、ユーザがファイルにアクセスしようとすると、中間ディレクトリのトラバース権限がONTAPでチェックされず、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

トラバースチェックのバイパスを設定するには、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します。

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

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

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あります。

- `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ない場合は、グループからこの権限を削除する必要があります。

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

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

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

関連情報

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

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

ボリュームでのSMBファイル名の変換のための文字マッピングの設定

SMB共有のアクセス制御リストの作成

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Privilegesのリスト

ローカルまたはドメインのユーザまたはグループへのPrivilegesの追加

ユーザまたはグループにディレクトリのトラバースチェックのバイパスを許可する

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

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

タスクの内容

Privilegesをドメインユーザまたはグループに追加するときに、ONTAPが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ことがあります。

手順

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

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

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

例

次のコマンドは、「example\eng'」グループに権限を追加することで、「example\eng'」グループに属するユーザがディレクトリのトラバースチェックをバイパスできるようにし `SeChangeNotifyPrivilege`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

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

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

開始する前に

Privileges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。

タスクの内容

ドメインユーザまたはグループからPrivilegesを削除する場合、ONTAPはドメインコントローラに接続して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ことがあります。

手順

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

   コマンドは、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またはグループから権限を `-user-or-group-name name`削除します `SeChangeNotifyPrivilege`。

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

例

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

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

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

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

関連情報

ユーザまたはグループに対するディレクトリのトラバースチェックのバイパスの許可

ファイルセキュリティと監査ポリシーに関する情報を表示する

ファイルセキュリティと監査ポリシーに関する情報の概要を表示する

Storage Virtual Machine（SVM）のボリュームに格納されたファイルとディレクトリのファイルセキュリティに関する情報を表示できます。FlexVolの監査ポリシーに関する情

報を表示できます。設定されている場合、FlexVolボリュームのストレージレベルのアクセス保護およびダイナミックアクセス制御セキュリティの設定に関する情報を表示できます。

ファイルセキュリティに関する情報の表示

次のセキュリティ形式のボリュームおよびqtree（FlexVolボリュームの場合）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
- mixed

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ボリューム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ボリュームおよびqtreeオブジェクトに適用できます。

- NTFS
- mixed
- UNIX（ボリュームが格納された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 volume内のオブジェクトに適用できます。

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

関連情報

ストレージレベルのアクセス保護を使用したファイルアクセスの保護

ストレージレベルのアクセス保護に関する情報の表示

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

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。

タスクの内容

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

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

ステップ

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

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

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/vol4`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、マスクを展開して、SVM vs1のパスに関するセキュリティ情報を表示します `/data/engineering`。

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

```
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

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

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。

タスクの内容

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

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

ステップ

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

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

例

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

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

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

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

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

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

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

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

関連情報

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

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

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

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

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

タスクの内容

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指定する必要があります。出力は要約形式で表示することも、詳細なリストとして表示することもできます。

- ファイルアクセス権の決定時に、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の場合は適用されません。

  NTFSセキュリティ記述子でのみ意味があります。

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

ステップ

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

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

例

次の例では、SVM vs1のパスに関するセキュリティ情報を表示し `/home`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、マスクを展開した形式で、SVM vs1のパスに関するセキュリティ情報を表示します `/home`。

```
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

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

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

CLIを使用したFlexVolのNTFS監査ポリシーに関する情報の表示

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

タスクの内容

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

- 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やフォルダには、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には、UNIX対応またはNTFS対応のセキュリティを設定でき、NTFS SACLが格納されている場合と格納されていない場合があります。
- ストレージレベルのアクセス保護セキュリティは、ボリュームのルートまたはqtreeの有効なセキュリティ形式がUNIXであっても、mixedセキュリティ形式のボリュームまたはqtreeで設定できるため、ストレージレベルのアクセス保護が設定されているボリュームまたはqtreeパスの出力には、通常のファイルおよびフォルダのNFSv4 SACLとストレージレベルのアクセス保護NTFS SACL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。
- NTFS対応のセキュリティが有効なファイルおよびフォルダに関するセキュリティ情報を表示する場合、UNIX関連の出力フィールドに表示専用のUNIXファイル権限情報が表示されます。

  ファイルアクセス権の決定時に、NTFSセキュリティ形式のファイルおよびフォルダでは、NTFSファイル権限と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や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。

ステップ

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

表示する情報	入力するコマンド
要約形式	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリスト	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/corp`。パスにはNTFS対応の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およびSUCCESS / FAIL SACLエントリの両方が含まれています。

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

次の例は、SVM vs1のパスの監査ポリシーの情報を表示します `/datavol1`。このパスには、通常のファイルとフォルダのSACLとストレージレベルのアクセス保護のSACLの両方が含まれています。

```
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
```

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

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

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

タスクの内容

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

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

  mixedセキュリティ形式のボリュームおよびqtree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、 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やフォルダでは空になります。

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

手順

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

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

例

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

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

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

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

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

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

例

次のコマンドでワイルドカード文字を使用すると、SVM vs1のパスの下にあるすべてのファイルとディレクトリに関する情報が表示され `/1/` 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のパスの下にある「*」という名前のファイルの情報を表示します `/vol1/a`。パスは二重引用符（ "" ）で囲まれます。

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

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

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

NTFSファイルセキュリティと監査ポリシーは、SMBクライアントから、またはCLIを使用して管理できます。ただし、CLIを使用してファイルセキュリティと監査ポリシーを設定すると、リモートクライアントを使用してファイルセキュリティを管理する必要がなくなります。CLIを使用すると、1つのコマンドで多数のファイルやフォルダにセキュリティを適用する時間を大幅に短縮できます。

ONTAPがSVMボリュームに適用するもう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またはSMBクライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護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個別に設定および管理できる、データアクセスのセキュリティレイヤを強化します。

> ストレージレベルのアクセス保護ではNTFSのアクセス権限のみがサポートされますが、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経由のアクセスについては、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にONTAPでセキュリティチェックを実行できます。

NTFSセキュリティ形式のボリューム

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

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

mixedセキュリティ形式のボリューム

mixedセキュリティ形式のボリュームやqtreeには、UNIX対応のセキュリティが有効で、UNIXファイル権限（モードビットまたはNFSv4.x ACL）とNFSv4.x監査ポリシーを使用するファイルやフォルダ、およびNTFS対応のセキュリティが有効でNTFSファイル権限と監査ポリシーを使用するファイルやフォルダを格納できます。コマンドファミリーを使用すると、mixedセキュリティ形式のデータに次の種類のセキュリティを適用でき `vserver security file-directory`ます。

- mixed形式のボリュームまたはqtreeにおける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およびqtreeには、UNIX対応のセキュリティ（モードビットまたはNFSv4.x ACL）が設定されたファイルおよびフォルダが格納されます。コマンドファミリーを使用して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、次の点に注意する必要があり `vserver security file-directory`ます。

- UNIXセキュリティ形式のボリュームおよびqtreeでは、 `vserver security file-directory`コマンドファミリーを使用してUNIXファイルセキュリティおよび監査ポリシーを管理することはできません。
- ターゲットボリュームを含むSVMにCIFSサーバが含まれている場合は、コマンドファミリーを使用して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保護を設定できます `vserver security file-directory`。

関連情報

ファイルセキュリティと監査ポリシーに関する情報を表示する

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と適用

CLIを使用した監査ポリシーの設定とNTFSファイルおよびフォルダへの適用

ストレージレベルのアクセス保護を使用したファイルアクセスの保護

CLIを使用したファイルおよびフォルダのセキュリティ設定のユースケース

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

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

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

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

CLIを使用してファイルおよびフォルダのセキュリティを設定する場合は、一定の制限事項に注意する必要があります。

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

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

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

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

- * 権限 *

  権限はオブジェクトの所有者によって許可または拒否され、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、セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。セキュリティ記述子には、次の2種類のACLを含めることができます。

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

  ◦ システムアクセスセイギョリスト SACL

- * 随意アクセス制御リスト（ DACL ） *

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

- * システム・アクセス・コントロール・リスト（ SACL ） *

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

- * アクセス制御エントリ (ACE) *

  ACEは、DACLまたはSACLの個 々 のエントリです。

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

- * 権限の継承 *

  権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトにパーミッションを設定する際に、「適用先」、 `sub-folders`「ファイル」でフォルダ、サブフォルダ、およびファイルを継承できるかどうかを指定できます `this-folder`。

関連情報

"SMBおよびNFSの監査とセキュリティトレース"

CLIを使用したNTFSファイルおよびフォルダへの監査ポリシーの設定および適用

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

ファイルとディレクトリのポリシー設定で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る必要がある一定のガイドラインがあります。

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

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

  この設定では、 SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

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

ID 破棄設定に関するガイドライン

ID 破棄設定では、ローカルユーザ、グループ、権限設定を含む SVM ソースを SVM デスティネーションの CIFS サーバ名に一致するようにローカルドメインの名前（ローカル CIFS サーバ名）を変更する必要があります。たとえば、ソース SVM 名が「 vs1 」で CIFS サーバ名が「 CIFS1 」、デスティネーション SVM 名が「 vs1_dst 」で CIFS サーバ名が「 CIFS1_DST` 」の場合、ローカルユーザ「 CIFS1\user1 」のローカルドメイン名は「 CIFS1_DST` デスティネーション SVM 」で自動的に「 CIFS1_DST\user1 」に変更されます。

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

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

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

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

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

たとえば、「vs1」について、パラメータが「`CIFS1\user1`」に設定されたDACLエントリを設定している場合 `-account`、デスティネーションSVMで設定が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ることはありません。

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

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   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
```

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

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

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

- セキュリティ記述子

  必要に応じて、セキュリティ記述子の所有者とセキュリティ記述子の所有者のプライマリグループを指定できます。セキュリティ記述子で所有者とプライマリグループのエントリにローカルユーザまたはグループを使用する場合、デスティネーション SVM にアカウント名を使用するようにセキュリティ記述子を変更する必要があります。アカウント名に必要な変更を加えるには、コマンドを使用し `vserver security file-directory ntfs modify`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、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存のDACLエントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべてのDACLエントリをセキュリティ記述子から削除し、修正したデスティネーションアカウント名を使用して新しいDACLエントリを作成し、それらの新しいDACLエントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACLエントリ

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

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

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

CLIを使用した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と適用

NTFSセキュリティ記述子を作成します。

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

タスクの内容

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

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

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

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

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

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

NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加

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

タスクの内容

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

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

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

- 権限
- 詳細な権限
- raw 権限（ advanced 権限）

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

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

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

手順

1. セキュリティ記述子にDACLエントリを追加します。 `vserver security file-directory ntfs dacl add -vserver 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
```

セキュリティポリシーを作成する

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

タスクの内容

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

手順

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

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

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

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

セキュリティポリシーにタスクを追加する

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

タスクの内容

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

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

タスクには次の2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やフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

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

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

ポリシーへのタスクの追加に関するガイドラインを次に示します。

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

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

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

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

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

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

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

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

手順

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

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

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

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

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

   ```
   Vserver: vs1
   Policy: policy1

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

セキュリティポリシーを適用する

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

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在する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が上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

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

```
vserver_name -policy-name policy_name

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

ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

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

セキュリティポリシージョブを監視する

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

タスクの内容

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、パラメータを使用し `-instance`ます。

ステップ

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

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

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

適用したファイルセキュリティの確認

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

タスクの内容

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

ステップ

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

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

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

```
         Vserver: vs1
               File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

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

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

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

                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
```

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

CLIを使用した監査ポリシーの設定とNTFSファイルおよびフォルダへの適用

CLIの概要を使用したNTFSファイルおよびフォルダへの監査ポリシーの設定と適用

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、そのセキュリティ記述子にSACLを追加します。次に、セキュリティポリシーを作成し、ポリシータスクを追加します。その後、そのセキュリティポリシーをStorage Virtual Machine（SVM）に適用します。

タスクの内容

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、適用した監査ポリシーの設定を確認できます。

監査ポリシーと関連するSACLを適用すると、既存のDACLが上書きされます。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する必要があります。

関連情報

ストレージレベルのアクセス保護を使用したファイルアクセスの保護

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

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

"SMBおよびNFSの監査とセキュリティトレース"

CLIを使用した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と適用

NTFSセキュリティ記述子を作成します。

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

タスクの内容

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

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

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

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

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

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

手順

1. advancedパラメータを使用する場合は、権限レベルをadvancedに設定します。 `set -privilege advanced`
2. セキュリティ記述子を作成します。 `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   ```
   vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
   ```

3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

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

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

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

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

タスクの内容

セキュリティ記述子のSACLには1つ以上のACEを追加できます。

セキュリティ記述子に含まれる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が作成されて新しいACEが追加されます。

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

- 権限

- 詳細な権限
- raw 権限（ advanced 権限）

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

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

手順

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

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

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

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

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

セキュリティポリシーを作成する

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

タスクの内容

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

手順

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

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

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

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

セキュリティポリシーにタスクを追加する

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

タスクの内容

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

タスクには次の2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やフォルダにセキュリティ記述子を適用するタスクの指定に使用します。ファイルとディレクトリのタスクによって適用される ACL は、 SMB クライアントまたは ONTAP CLI で管理できます。

- ストレージレベルのアクセス保護タスク

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

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

ポリシーへのタスクの追加に関するガイドラインを次に示します。

- ポリシーあたりのタスクエントリは最大 10 、 000 個です。

- ポリシーには 1 つ以上のタスクを含めることができます。

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

- ストレージレベルのアクセス保護は、権限の制限に使用します。

  アクセス権限は付与されません。

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

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

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

手順

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

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

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

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

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

```
Vserver: vs1
Policy: policy1

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

セキュリティポリシーを適用する

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

タスクの内容

セキュリティポリシーで定義されたセキュリティ設定を、FlexVolボリューム（NTFSまたはmixedセキュリティ形式）内に存在する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が上書きされます。セキュリティポリシーとそれに関連付けられたDACLが適用されると、既存のDACLはすべて上書きされます。新しいセキュリティポリシーを作成して適用する前に、既存のセキュリティポリシーを確認する必要があります。

ステップ

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

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

   ポリシー適用ジョブがスケジュールされ、ジョブIDが返されます。

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

セキュリティポリシージョブを監視する

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

タスクの内容

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、パラメータを使用し `-instance`ます。

ステップ

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

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

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

適用された監査ポリシーの確認

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

タスクの内容

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

ステップ

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

例

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

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

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

セキュリティポリシージョブを管理する際の考慮事項

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

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

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

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

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

NTFSセキュリティ記述子の管理用コマンド

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

状況	使用するコマンド
NTFS セキュリティ記述子を作成します	`vserver security file-directory ntfs create`
既存の NTFS セキュリティ記述子を変更します	`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します	`vserver security file-directory ntfs show`
NTFS セキュリティ記述子を削除します	`vserver security file-directory ntfs delete`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory ntfs`。

NTFS DACLアクセス制御エントリの管理用コマンド

ONTAPには、DACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS DACL に追加できます。また、DACLのACEを変更、削除、および情報表示することで、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 を作成して NTFS DACL に追加します	`vserver security file-directory ntfs dacl add`
NTFS DACL の既存の ACE の変更	`vserver security file-directory ntfs dacl modify`
NTFS DACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs dacl show`
NTFS DACL から既存の ACE を削除します	`vserver security file-directory ntfs dacl remove`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory`

ntfs dacl。

NTFS SACLアクセス制御エントリの管理用コマンド

ONTAPには、SACLのアクセス制御エントリ（ACE）を管理するためのコマンドが用意されています。ACE はいつでも NTFS SACL に追加できます。また、SACLのACEを変更、削除、および情報表示することで、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 を作成して NTFS SACL に追加します	`vserver security file-directory ntfs sacl add`
NTFS SACL の既存の ACE の変更	`vserver security file-directory ntfs sacl modify`
NTFS SACL の既存の ACE に関する情報を表示します	`vserver security file-directory ntfs sacl show`
NTFS SACL から既存の ACE を削除します	`vserver security file-directory ntfs sacl remove`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory ntfs sacl`。

セキュリティポリシーの管理用コマンド

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

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します	`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`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory policy`。

セキュリティポリシータスクの管理用コマンド

セキュリティポリシータスクに関する情報を追加、変更、削除、および表示するためのONTAP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を変更する	`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します	`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`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory policy task`。

セキュリティポリシージョブの管理用コマンド

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

状況	使用するコマンド
セキュリティポリシージョブを一時停止します	`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します	`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します	`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を確認できます。
セキュリティポリシージョブを停止します	`vserver security file-directory job stop -vserver vserver_name -id integer`

詳細については、コマンドのマニュアルページを参照してください `vserver security file-directory job`。

SMB共有のメタデータキャッシュの設定

SMBメタデータのキャッシングの仕組み

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

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

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

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

SMBメタデータのキャッシュを有効にする

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

ステップ

1. 必要な操作を実行します。

状況	入力するコマンド
共有の作成時にSMBメタデータのキャッシングを有効にする	`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

SMBメタデータキャッシュエントリの有効期間の設定

SMBメタデータキャッシュエントリの有効期間の設定

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

開始する前に

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

ステップ

1. 必要な操作を実行します。

SMB メタデータキャッシュエントリの有効期間を設定する際の方法	入力するコマンド
共有を作成する	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
既存の共有を変更する	`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ときに、追加の共有設定オプションおよび共有プロパティを指定できます。詳細については、マニュアルページを参照してください。

ファイルロックを管理します。

プロトコル間のファイルロックについて

ファイルロックは、別のユーザが以前に開いていたファイルにユーザがアクセスできないようにするためにクライアントアプリケーションで使用される方法です。ONTAPでファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントがNFSクライアントの場合はロックを推奨します。クライアントがSMBクライアントの場合はロックは必須です。

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以前に開いたファイルにNFSクライアントからアクセスすると失敗することがあります。

NFSクライアントがSMBアプリケーションでロックされているファイルにアクセスしようとすると、次の状況が発生します。

- mixed形式またはNTFS形式のボリュームでは、、 `rmdir`などのファイル操作を `rm`mv`行うと、NFSアプリケーションが失敗することがあります。
- NFSの読み取り処理と書き込み処理は、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。
- ファイルの書き込み範囲が排他的なSMBバイトロックでロックされている場合、NFSの書き込み処理が失敗します。
- 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上の他のすべてのNFS処理では、SMBロック状態が維持されます。

ONTAPによる読み取り専用ビットの処理方法

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

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

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

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

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

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

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

Windowsとは異なり、ONTAPはファイルが開いている間、開いているファイルへのパスの各コンポーネントをロックしません。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。その結果、共有にアクセスできなくなる可能性があります。

パスコンポーネントの名前変更による問題を回避するには、セキュリティ設定を適用して、ユーザや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します。

ロックに関する情報を表示する

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

タスクの内容

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

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

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

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。
- 便宜的ロック。 SMB を使用してクライアント側キャッシュを制御します。
- 委譲。 NFSv4.x を使用してクライアント側キャッシュを制御します

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

ステップ

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

例

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

```
cluster1::> vserver locks show

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

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

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

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

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

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

ロックの解除

ファイルロックによってクライアントがファイルにアクセスできない場合は、現在有効なロックに関する情報を表示して、特定のロックを解除できます。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。

タスクの内容

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

手順

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

   詳細については、コマンドのマニュアルページを参照してください。

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

ロックを解除するための指定項目	入力するコマンド
SVM名、ボリューム名、LIF名、およびファイルパス	`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`

SMBアクティビティの監視

SMBセッション情報を表示する

SMB接続、SMB Session 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、確立されている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を確認するのに役立ちます。

タスクの内容

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

- オプションのパラメータを使用すると、選択したフィールドに関する出力を表示できます `-fields`。

  と入力して、使用できるフィールドを指定できます `-fields ?`。

- 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 `-instance`。
- 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、他のオプションのパラメータと組み合わせて使用することもできます `-fields`。

ステップ

1. 次のいずれかを実行します。

表示する **SMB** セッション情報	入力するコマンド
SVM上のすべてのセッション（要約形式）	`vserver cifs session show -vserver vserver_name`
指定した接続IDのファイル	`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	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定したLIF IPアドレスのファイル	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
指定したノードのオブジェクト	`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場合
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
指定したプロトコルバージョンを使用している場合	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 継続的可用性を備えた保護とSMBマルチチャネルは、SMB 3.0以降のセッションでのみ使用できます。該当するすべてのセッションのステータスを表示するには、このパラメータの値を以降に設定します。 `SMB3` ====
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

表示する **SMB** セッション情報	入力するコマンド
Yes	Partial}`  [NOTE] ==== 継続的可用性のステータスがの場合は `Partial`、継続的可用性を備えた開いているファイルがセッションに少なくとも1つ含まれていますが、継続的可用性を備えた保護を使用して開かれていないファイルがセッションに含まれています。コマンドを使用すると、確立されたセッションのファイルのうち、継続的可用性を備えた保護を使用して開かれていないファイルを確認できます `vserver cifs sessions file show`。 ====
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

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

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

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

```
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
```

次のコマンドを実行すると、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セッション情報が表示されます。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**SMB**ファイルに関する情報を表示する

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

タスクの内容

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。表示される情報は、SMBセッション内の特定のファイルに関するSMBセッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、継続的可用性を備えた保護を使用して開いているファイルと継続的可用性を備えた保護を使用して開かれていないファイルがある場合（コマンド出力のフィールド `vserver cifs session show`の値 `-continuously-available`は `Partial`）、このコマンドを使用して、継続的可用性に対応していないファイルを確認できます。

オプションのパラメータを何も指定せずにコマンドを実行することで、Storage Virtual Machine（SVM）上の確立されたSMBセッションのすべての開いているファイルに関する情報を要約形式で表示できます `vserver cifs session file show`。

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。

- オプションのパラメータを使用すると、選択したフィールドの出力を表示できます `-fields`。

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

- 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 `-instance`。

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

ステップ

1. 次のいずれかを実行します。

表示する開いている **SMB** ファイル	入力するコマンド
SVM上のファイル（要約形式）	`vserver cifs session file show -vserver vserver_name`
指定したノードのオブジェクト	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	指定したファイルIDのファイル
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定したSMB接続IDのファイル
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定したSMB Session IDのファイル
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホストアグリゲートのファイル
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	指定したボリュームのファイル
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定したSMB共有のファイル

表示する開いている **SMB** ファイル	入力するコマンド
`vserver cifs session file show -vserver vserver_name -share share_name`	指定したSMBパスのファイル
`vserver cifs session file show -vserver vserver_name -path path`	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
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}` [NOTE] ==== 継続的可用性のステータスがの場合はNo、開いているファイルがテイクオーバーやギブバックからの無停止でのリカバリに対応していません。また、ハイアベイラビリティ関係にあるパートナー間での一般的なアグリゲートの再配置からリカバリすることもできません。 ====
指定した再接続状態のファイル	`vserver cifs session file show -vserver vserver_name -reconnected {No

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

例

次の例では、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
```

次の例では、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

SMBセッション情報の表示

使用可能な統計オブジェクトとカウンタの確認

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

手順

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

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

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

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

例

次のコマンドを実行すると、advanced権限レベルで表示した場合の、クラスタ内のCIFSアクセスとSMBアクセスに関連する選択した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
```

次のコマンドを実行すると、advanced権限レベルで表示したオブジェクトの一部のカウンタに関する情報が

表示され `cifs`ます。

この例で表示されているのはオブジェクトの使用可能なカウンタの一部ではありませ `cifs`ん。出力は省略されています。

```
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

統計を表示する

パフォーマンスの監視と問題の診断を行うために、CIFSとSMB、監査、BranchCacheハッシュに関する統計など、さまざまな統計を表示できます。

開始する前に

オブジェクトに関する情報を表示する前に、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 `statistics start`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。

統計を表示する対象	入力するコマンド
SMBのすべてのバージョン	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.xおよび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`

   詳細については、各コマンドのマニュアルページを参照してください。

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

関連情報

使用可能な統計オブジェクトと統計カウンタの確認

SMB署名済みセッションの統計の監視

BranchCache統計の表示

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オヨヒSQL ServerヨウノSMBノセツテイ"

"パフォーマンス監視のセットアップ"