SMBを使用したファイルアクセスのセットアップ

ONTAP 9

NetApp
December 20, 2024

目次

SMBを使用したファイルアクセスのセットアップ . . . 1
セキュリティ形式の設定 . . . 1
NASネームスペースでのデータボリュームの作成と管理 . . . 5
ネームマッピングの設定 . . . 11
マルチドメインネームマッピング検索の設定 . . . 17
SMB共有の作成と設定 . . . 21
SMB共有のACLを使用したファイルアクセスの保護 . . . 31
ファイル権限を使用したファイルアクセスの保護 . . . 34
ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護 . . . 39
エクスポートポリシーを使用したSMBアクセスの保護 . . . 50
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 . . . 55

SMBを使用したファイルアクセスのセットアップ

セキュリティ形式の設定

セキュリティ形式がデータアクセスに与える影響

セキュリティ形式とその影響

セキュリティ形式には、 UNIX 、 NTFS 、 mixed 、および unified の 4 種類があり、セキュリティ形式によって、データに対する権限の処理方法が異なります。目的に応じて適切なセキュリティ形式を選択できるように、それぞれの影響について理解しておく必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データ アクセスの制御にONTAPで使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームでUNIXセキュリティ形式を使用している場合でも、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	有効になるセキュリティ形式	ファイルにアクセスできるクライアント
UNIX	NFS	NFSv3モードビット	UNIX	NFSとSMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
mixed	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
unified （ Infinite Volume のみ、ONTAP 9.4 以前のリリース）	NFSまたはSMB	NFSv3モードビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合、ユーザはセキュリティ形式を個別に設定するため、権限を最後に変更したクライアントのタイプによって有効な権限が異なります。権限を最後に変更したクライアントがNFSv3クライアントの場合、権限はUNIX NFSv3モードビットになります。最後のクライアントがNFSv4クライアントの場合、権限はNFSv4 ACLになります。最後のクライアントがSMBクライアントの場合、権限はWindows NTFS ACLになります。

unifiedセキュリティ形式は、Infinite Volumeでのみ使用できます。Infinite Volumeは、ONTAP 9 .5以降のリリースではサポートされなくなりました。詳細については、を参照してください FlexGroup ボリュームの管理の概要。

Windows.2以降では、コマンドのパラメータを `vserver security file-directory`使用して、指定したファイルまたはフォルダパスでONTAP 9 `show-effective-permissions`ユーザまたはUNIXユーザに付与されている有効な権限を表示できます。また、オプションのパラメータを `-share-name`使用すると、有効な共有権限を表示できます。

ONTAPは、最初に一部のデフォルトのファイル権限を設定します。デフォルトでは、UNIX、mixed、およびunifiedのセキュリティ形式のボリュームにあるデータには、セキュリティ形式はUNIXになり、アクセス権のタイプはUNIXモードビット（特に指定がないかぎり0755）になります。これは、デフォルトのセキュリティ形式で許可されるようにクライアントによって設定されるまでの間です。デフォルトでは、NTFSセキュリティ形式のボリューム内のすべてのデータに対するセキュリティ形式はNTFSになり、すべてのユーザにフルコントロールを許可するACLが割り当てられます。

セキュリティ形式を設定する場所とタイミング

セキュリティ形式は、 FlexVol （ルートボリュームとデータボリュームの両方）および qtree で設定できます。セキュリティ形式は、作成時に手動で設定することも、自動的に継承することも、あとで変更することもできます。

SVMで使用するセキュリティ形式を決定する

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。主な要因は、ファイルシステムを管理する管理者のタイプです。2番目の要因は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームでセキュリティ形式を設定する場合は、最適なセキュリティ形式を選択し、権限の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定には、次の考慮事項が役立ちます。

セキュリティ形式	以下の場合に選択
UNIX	• ファイルシステムはUNIX管理者によって管理されます。 • ユーザの大半がNFSクライアントである。 • データにアクセスするアプリケーションでは、UNIXユーザをサービスアカウントとして使用します。
NTFS	• ファイルシステムはWindows管理者によって管理されます。 • ユーザの大部分がSMBクライアントです。 • データにアクセスするアプリケーションでは、Windowsユーザをサービスアカウントとして使用します。
mixed	ファイルシステムはUNIX管理者とWindows管理者の両方によって管理され、ユーザはNFSクライアントとSMBクライアントの両方で構成されます。

セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式はさまざまな方法で継承されます。

セキュリティ形式は、次のように継承されます。

- FlexVol ボリュームは、そのボリュームを含む SVM のルートボリュームのセキュリティ形式を継承します。
- qtree は、その qtree を含む FlexVol ボリュームのセキュリティ形式を継承します。
- ファイルまたはディレクトリは、そのファイルまたはディレクトリを含む FlexVol ボリュームまたは qtree のセキュリティ形式を継承します。

ONTAPによる**UNIX**アクセス権の維持方法

UNIX アクセス権を現在持っている FlexVol ボリューム内のファイルが Windows アプリケーションによって編集および保存されても、 ONTAP は UNIX アクセス権を維持できます。

Windows クライアントのアプリケーションは、ファイルを編集して保存するときに、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

セキュリティプロパティのクエリを実行すると、 Windows クライアントは、 UNIX アクセス権を正確に表す構築済み ACL を受け取ります。この構築済み ACL は、 Windows アプリケーションによってファイルが更新されるときにファイルの UNIX アクセス権を維持し、生成されたファイルが同じ UNIX アクセス権を持つようにするためだけに使用されます。ONTAP は、構築済み ACL を使用して NTFS ACL を設定しません。

Windowsの**[**セキュリティ**]**タブを使用した**UNIX**アクセス権の管理

SVM 上の mixed セキュリティ形式のボリュームまたは qtree に含まれるファイルまたはフォルダの UNIX アクセス権を操作する場合は、 Windows クライアントのセキュリティタブを使用できます。また、 Windows ACL を照会および設定できるアプリケーションを使用することもできます。

- UNIX アクセス権の変更

  Windows のセキュリティタブを使用して、 mixed セキュリティ形式のボリュームまたは qtree の UNIX アクセス権を表示および変更できます。メインの [Windows Security] タブを使用して UNIX アクセス権を変更する場合は、編集する既存の ACE を削除してから（モードビットを 0 に設定）、変更を行う必要があります。または、高度なエディタを使用して権限を変更することもできます。

  モードのアクセス権を使用している場合は、リストされた UID 、 GID 、およびその他（コンピュータにアカウントを持つその他すべてのユーザ）のモードアクセス権を直接変更できます。たとえば、表示された UID に r-x のアクセス権が設定されている場合、この UID のアクセス権を rwx に変更できます。

- UNIX アクセス権を NTFS アクセス権に変更しています

  Windows のセキュリティタブを使用して、ファイルおよびフォルダのセキュリティ形式が UNIX 対応である mixed 型セキュリティ形式のボリュームまたは qtree 上で、 UNIX セキュリティオブジェクトを

Windows セキュリティオブジェクトに置き換えることができます。

適切な Windows のユーザおよびグループのオブジェクトに置き換える前に、リストされている UNIX アクセス権のエントリをすべて削除しておく必要があります。次に、 Windows のユーザおよびグループのオブジェクトに NTFS ベースの ACL を設定します。すべての UNIX セキュリティオブジェクトを削除し、 Windows のユーザおよびグループのみを mixed セキュリティ形式のボリュームまたは qtree 上のファイルまたはフォルダに追加すると、ファイルまたはフォルダのセキュリティ形式が UNIX から NTFS へ変換されます。

フォルダの権限を変更する場合、 Windows のデフォルトの動作では、すべてのサブフォルダとファイルにこれらの変更が反映されます。したがって、セキュリティ形式の変更をすべての子フォルダ、サブフォルダ、およびファイルに反映したくない場合は、反映する範囲を希望の範囲に変更する必要があります。

SVMルートボリュームでのセキュリティ形式の設定

Storage Virtual Machine（SVM）のルートボリューム上のデータに使用するアクセス権のタイプを決定するには、SVMルートボリュームのセキュリティ形式を設定します。

手順

1. セキュリティ形式を定義するには、コマンドで `-rootvolume-security-style`パラメータを使用し `vserver create`ます。

   ルートボリュームのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

2. 作成したSVMのルートボリュームセキュリティ形式を含む設定を表示して確認します。 `vserver show -vserver` *`vserver_name`*

FlexVolボリュームでのセキュリティ形式の設定

Storage Virtual Machine（SVM）のFlexVol上のデータに使用するアクセス権のタイプを決定するには、FlexVol volumeセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
まだ存在しません	`volume create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

FlexVol volumeセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

FlexVol volumeの作成時にセキュリティ形式を指定しない場合、ボリュームはルートボリュームのセキュリティ形式を継承します。

コマンドまたは `volume modify`コマンドの詳細については `volume create`、を参照してください"

論理ストレージ管理"。

2. 作成したFlexVol volumeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

```
volume show -volume volume_name -instance
```

qtreeでのセキュリティ形式の設定

qtree上のデータに使用するアクセス権のタイプを決定するには、qtreeボリュームのセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
まだ存在しません	`volume qtree create`セキュリティ形式を指定するパラメータを追加します `-security-style`。
すでに存在します	`volume qtree modify`セキュリティ形式を指定するパラメータを追加します `-security-style`。

qtreeのセキュリティ形式に指定できるオプションは `unix`、、 `ntfs`または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式はです `mixed`。

コマンドまたは `volume qtree modify`コマンドの詳細については `volume qtree create`、を参照してください"論理ストレージ管理"。

2. 作成したqtreeのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。 `volume qtree show -qtree qtree_name -instance`

NASネームスペースでのデータボリュームの作成と管理

NASネームスペースでのデータボリュームの作成と管理の概要

NAS環境でファイルアクセスを管理するには、Storage Virtual Machine（SVM）上でデータボリュームとジャンクションポイントを管理する必要があります。これには、ネームスペースアーキテクチャの計画、ジャンクションポイントが設定されたボリュームまたはジャンクションポイントが設定されていないボリュームの作成、ボリュームのマウントまたはアンマウント、およびデータボリュームや NFS サーバまたは CIFS サーバのネームスペースに関する情報の表示が含まれます。

ジャンクションポイントを指定してデータボリュームを作成する

ジャンクションポイントは、データボリュームの作成時に指定できます。作成したボリュームはジャンクションポイントに自動的にマウントされ、NASアクセス用の設定にすぐに使用できます。

開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

ジャンクションパスに次の文字を使用することはできません。 * # <> < | ? \

また、ジャンクションパスの長さは255文字以下にする必要があります。

手順

1. ジャンクションポイントを設定してボリュームを作成します。 `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   ジャンクションパスはルート（/）で始まる必要があり、ディレクトリと結合されたボリュームの両方を含めることができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   ジャンクションパスでは大文字と小文字が区別されません。はと同じ `/eng`です。 `/ENG`CIFS共有を作成する場合、Windowsではジャンクションパスは大文字と小文字が区別されるかのように扱われます。たとえば、ジャンクションがの場合、 `/ENG`CIFS共有のパスははではなくで `/eng`始まる必要があります `/ENG`。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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 `volume create`ください。

2. 目的のジャンクションポイントでボリュームが作成されたことを確認します。 `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成し `/eng/home`ます。

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

ジャンクションポイントを指定せずにデータボリュームを作成する

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、NASアクセス用に設定することもできません。ボリュームに対してSMB共有またはNFSエクスポートを設定するには、ボリュームをマウントする必要があります。

開始する前に

ボリュームを作成するアグリゲートがすでに存在している必要があります。

手順

1. 次のコマンドを使用して、ジャンクションポイントが設定されていないボリュームを作成します。
   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   ボリュームのセキュリティ形式の指定は任意です。セキュリティ形式を指定しない場合、ONTAPはStorage Virtual Machine（SVM）のルートボリュームと同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームに適用するセキュリティ形式と異なる場合があります。トラブルシューティングが困難なファイルアクセスの問題を最小限に抑えるために、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   データボリュームのカスタマイズに使用できるオプションのパラメータが多数用意されています。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 `volume create`ください。

2. ボリュームがジャンクションポイントなしで作成されたことを確認します。 `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NASネームスペースで既存のボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに格納されたデータへのNASクライアントからのアクセスを設定するには、ボリュームがNASネームスペースにマウントされている必要があります。現在マウントされていないボリュームは、ジャンクションポイントにマウントできます。ボリュームをアンマウントすることもできます。

タスクの内容

ボリュームをアンマウントしてオフラインにすると、アンマウントしたボリュームのネームスペース内に含まれていたジャンクションポイントのあるボリューム内のデータも含め、ジャンクションポイント内のすべてのデータにNASクライアントからアクセスできなくなります。

> ボリュームへのNASクライアントアクセスを中止するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、クライアント側のファイルハンドルキャッシュを確実に無効にするためのその他の手順を実行する必要があります。詳細については、次のナレッジベースの記事を参照してください。 "ONTAP のネームスペースから NFSv3 クライアントを削除しても、ボリュームにアクセスできるようになります"

ボリュームをアンマウントしてオフラインにしても、ボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーと、ボリュームまたはディレクトリに作成されたSMB共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすると、NASクライアントは既存のエクスポートポリシーとSMB共有を使用してボリュームに格納されているデータにアクセスできます。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームのマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

状況	入力するコマンド

ボリュームのアンマウント	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例は、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします。

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例は、SVM「vs1」にある「data」という名前のボリュームをアンマウントしてオフラインにします。

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ボリュームマウントポイントとジャンクションポイントの情報を表示します。

Storage Virtual Machine（SVM）のマウントボリューム、およびボリュームがマウント

されているジャンクションポイントに関する情報を表示できます。ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVMネームスペースを理解し、管理することができます。

手順

1. 必要な操作を実行します。

表示する項目	入力するコマンド
SVMのマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver vserver_name -junction`
SVMのマウントされたボリュームとマウントされていないボリュームに関する詳細情報	`volume show -vserver vserver_name -volume volume_name -instance`
SVMのマウントされたボリュームとマウントされていないボリュームに関する特定の情報	a. 必要に応じて、次のコマンドを使用してパラメータの有効なフィールドを表示できます `-fields。 volume show -fields ?` b. パラメータを使用して、必要な情報を表示し `-fields`ます。volume show -vserver vserver_name -fields fieldname、……

例

次の例では、SVM vs1のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

次の例は、SVM vs2上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

ネームマッピングの設定

ネームマッピングの設定の概要

ONTAPでは、ネームマッピングを使用して、CIFS IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをCIFS IDにマッピングします。この情報は、NFSクライアントとCIFSクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要になります。

ネームマッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成し、ボリュームでCIFSアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定します。

  このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できないことに注意してください。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、salesという語で開始または終了するすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。

ネームマッピングの仕組み

ONTAPでユーザのクレデンシャルをマッピングする必要がある場合は、まずローカルのネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVMのネームサービスの設定で決まります。

- WindowsからUNIXへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、デフォルトのUNIXユーザを使用します（設定済みの場合）。デフォルトのUNIXユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIXからWindowsへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのCIFSユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

UNIXユーザから**Windows**ユーザへのネームマッピングのためのマルチドメイン検索

ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性が**UNIX**ユーザから**Windows**ユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がONTAPとどのように連携するかを理解しておく必要があります。CIFSサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVMのCIFSサーバが属しているドメインです。

- _ 双方向の信頼 _

  双方向の信頼では、両方のドメインが相互に信頼されます。CIFSサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

  UNIXユーザからWindowsユーザへのネームマッピング検索は、ホームドメインともう一方のドメイン間で双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  アウトバウンドの信頼では、ホームドメインはもう一方のドメインを信頼します。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属するユーザを認証および許可できます。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがCIFSサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属するユーザを認証または許可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、Windowsユーザ名のドメインセクションにワイルドカードを使用することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	*\\administrator	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。

パターン	交換	結果
*	\ * \\ *	有効なUNIXユーザが対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 パターン「 \ * \\ * 」は、 UNIX から Windows へのネームマッピングでのみ有効であり、反対方向では無効です。

マルチドメインの名前検索の実行方法

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

ユーザ名のドメインセクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係が確立されたすべてのドメインでWindowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

UNIXユーザがユーザ名にドメインセクションのないWindowsユーザにマッピングされている場合、ホームドメインでWindowsユーザの検索が行われます。

ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXプログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

ネームマッピングを作成する

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping`

create。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`

   および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。詳細については、のマニュアルページを参照して `vserver name-mapping create` ください。

   Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、 vs1 という名前の SVM 上にネームマッピングを作成します。このマッピングは、UNIXからWindowsへのマッピングで、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトユーザの設定

ユーザに対する他のマッピング試行がすべて失敗した場合や、UNIXとWindowsの間で個々 のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個 々 のWindowsユーザにマッピングしない場合は、代わりにデフォルトのWindowsユーザを指定できます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトのUNIXユーザを設定する	`vserver cifs options modify -default -unix-user` *`user_name`*
デフォルトのWindowsユーザを設定する	`vserver nfs modify -default-win-user` *`user_name`*

ネームマッピングの管理用コマンド

ONTAPには、ネームマッピングを管理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
ネームマッピングを作成する	`vserver name-mapping create`
特定の位置にネームマッピングを挿入する	`vserver name-mapping insert`
ネームマッピングを表示する	`vserver name-mapping show`

状況	使用するコマンド
2つのネームマッピングの位置を交換する IP修飾子エントリを使用してネームマッピングが設定されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

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。

マルチドメインネームマッピング検索の設定

マルチドメインネームマッピングの検索を有効または無効にする

マルチドメインネームマッピングの検索では、 UNIX ユーザから Windows ユーザへのネームマッピングを設定するときに、 Windows 名のドメイン部分にワイルドカード（ * ）を使用できます。名前のドメイン部分にワイルドカード（ * ）を使用すると、 ONTAP で、 CIFS サーバのコンピュータアカウントが含まれるドメインと双方向の信頼関係が確立されているすべてのドメインを検索できるようになります。

タスクの内容

双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。信頼できるドメインのリストを設定すると、ONTAPは双方向の信頼関係が確立された検出ドメインの代わりに、信頼できるドメインのリストを使用してマルチドメインネームマッピングの検索を実行します。

- マルチドメインネームマッピングの検索は、デフォルトで有効になっています。
- このオプションは、advanced権限レベルで使用できます。

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。

マルチドメインネームマッピングの検索の設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

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

関連情報

使用できるSMBサーバオプション

信頼できるドメインのリセットと再検出

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。ホームドメイン（CIFSサーバのコンピュータアカウントを含むドメイン）と双方向の信頼関係が確立されたドメインのみが検出されます。

ステップ

1. コマンドを使用して、信頼できるドメインをリセットして再検出し `vserver cifs domain trusts rediscover` ます。

```
vserver cifs domain trusts rediscover -vserver vs1
```

関連情報

検出された信頼できるドメインに関する情報の表示

検出された信頼できるドメインに関する情報を表示する

CIFSサーバのホームドメイン（CIFSサーバのコンピュータアカウントが含まれているドメイン）で検出された信頼できるドメインに関する情報を表示できます。この情報は、検出された信頼できるドメインと、検出された信頼できるドメインのリスト内でのそれらの順序を確認する場合に役立ちます。

タスクの内容

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ（DC）は、信頼できるドメインのリストをDCが決定した順序で返すため、リスト内のドメインの順序を予測することはできません。信頼できるドメインのリストを表示することで、マルチドメインネームマッピングの検索での検索順序を確認できます。

表示される信頼できるドメインの情報は、ノードおよびStorage Virtual Machine（SVM）別にグループ化されます。

ステップ

1. コマンドを使用して、検出された信頼できるドメインに関する情報を表示します `vserver cifs domain trusts show`。

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

関連情報

信頼できるドメインのリセットおよび再検出

信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、置換

SMBサーバの信頼できるドメインの優先リストに対して信頼できるドメインを追加または削除したり、現在のリストを変更したりできます。信頼できるドメインの優先リストを設定すると、マルチドメインネームマッピングの検索を実行するときに、検出された双方向の信頼できるドメインの代わりにこのリストが使用されます。

タスクの内容

- 信頼できるドメインを既存のリストに追加する場合は、新しいリストが既存のリストにマージされ、新しいエントリが末尾に追加されます。信頼できるドメインは、リスト内の順序で検索されます。
- 信頼できるドメインを既存のリストから削除する際にリストを指定しないと、指定したStorage Virtual Machine（SVM）の信頼できるドメインのリスト全体が削除されます。
- 信頼できるドメインの既存のリストを変更すると、新しいリストで上書きされます。

信頼できるドメインのリストには、双方向の信頼関係が確立されたドメインだけを入力してください。アウトバウンドまたはインバウンドの信頼ドメインを優先ドメインリストに入力することはできますが、マルチドメインネームマッピングの検索では使用されません。ONTAPは単方向ドメインのエントリをスキップし、リスト内の次の双方向の信頼関係が確立されたドメインに移動します。

ステップ

1. 次のいずれかを実行します。

信頼できるドメインのリストに対して行う操作	使用するコマンド
信頼できるドメインをリストに追加する	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
信頼できるドメインをリストから削除する	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
既存のリストを変更する	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

例

次のコマンドは、SVM vs1で使用される信頼できるドメインの優先リストに2つの信頼できるドメイン（cifs1.example.comおよびcifs2.example.com）を追加します。

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用されるリストから信頼できるドメインを2つ削除します。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、SVM vs1で使用される信頼できるドメインのリストを変更します。元のリストが新しいリストに置き換えられます。

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

関連情報

信頼できるドメインの優先リストに関する情報の表示

信頼できるドメインの優先リストに関する情報を表示する

信頼できるドメインの優先リストに含まれている信頼できるドメインに関する情報、およびマルチドメインネームマッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出された信頼できるドメインの優先リストを使用する代わりに、信頼できるドメインの優先リストを設定することもできます。

手順

1. 次のいずれかを実行します。

表示する情報	使用するコマンド
Storage Virtual Machine（SVM）別にグループ化されたクラスタ内のすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show`
指定したSVMのすべての信頼できる優先ドメイン	`vserver cifs domain name-mapping-search show -vserver vserver_name`

次のコマンドは、クラスタ上のすべての信頼できる優先ドメインに関する情報を表示します。

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
--------------   ----------------------------------
vs1              CIFS1.EXAMPLE.COM
```

関連情報

信頼できるドメインの優先リスト内の信頼できるドメインの追加、削除、または置換

SMB共有の作成と設定

SMB共有の作成と設定の概要

ユーザやアプリケーションがSMB経由でCIFSサーバ上のデータにアクセスできるようにするには、SMB共有を作成して設定する必要があります。SMB共有は、ボリューム内の指定されたアクセスポイントです。共有をカスタマイズするには、共有パラメータと共有プロパティを指定します。既存の共有はいつでも変更できます。

SMB共有を作成すると、すべてのメンバーにフルコントロール権限が設定されたACLがONTAPによってデフォルトで作成されます。

SMB共有は、Storage Virtual Machine（SVM）上のCIFSサーバに関連付けられます。SVMが削除された場合、または関連付けられているCIFSサーバがSVMから削除された場合、SMB共有は削除されます。SVMにCIFSサーバを再作成する場合は、SMB共有を再作成する必要があります。

関連情報

SMBを使用したファイルアクセスの管理

"Microsoft Hyper-VオヨヒSQL ServerヨウノSMBノセツテイ"

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

デフォルトの管理共有とは

Storage Virtual Machine（SVM）上にCIFSサーバを作成すると、デフォルトの管理共有が自動的に作成されます。これらのデフォルトの共有とその用途について理解しておく必要があります。

CIFSサーバを作成すると、ONTAPによって次のデフォルトの管理共有が作成されます。

ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

- IPC$
- admin$（ONTAP 9.7以前のみ）
- c$

$文字で終わる共有は非表示の共有であるため、デフォルトの管理共有は[マイコンピュータ]には表示されませんが、[共有フォルダ]を使用して表示できます。

ipc$**および**admin$デフォルト共有の使用方法

ipc$共有とadmin$共有はONTAPが使用するものであり、Windows管理者がSVM上のデータにアクセスするために使用することはできません。

- ipc$共有

  ipc$共有は、プログラム間の通信に不可欠な名前付きパイプを共有するリソースです。ipc$共有は、コンピュータのリモート管理中およびコンピュータの共有リソースを表示するときに使用されます。ipc$共有の共有設定、共有プロパティ、ACLは変更できません。また、ipc$共有の名前を変更したり削除したりすることもできません。

- admin$共有（ONTAP 9.7以前のみ）

  ONTAP 9 .8以降では、admin$共有はデフォルトで作成されなくなりました。

  admin$共有は、SVMのリモート管理に使用されます。このリソースのパスは、常にSVMルートへのパスです。admin$共有の共有設定、共有プロパティ、ACLは変更できません。また、admin$共有の名前変更や削除もできません。

c$テフオルトキヨウユウノシヨウホウホウ

c$共有は、クラスタ管理者またはSVM管理者がSVMルートボリュームへのアクセスと管理に使用できる管理共有です。

c$共有の特徴は次のとおりです。

- この共有のパスは、常にSVMルートボリュームへのパスであり、変更することはできません。
- c$共有のデフォルトのACLは、Administrator/Full Controlです。

  このユーザはBUILTIN\administratorです。デフォルトでは、BUILTIN\administratorを共有にマッピングし、マッピングされたルートディレクトリ内のファイルやフォルダを表示、作成、変更、削除できます。このディレクトリ内のファイルとフォルダを管理する場合は、注意が必要です。

- c$共有のACLは変更できます。
- c$共有設定と共有プロパティを変更できます。
- c$共有は削除できません。
- SVM管理者は、ネームスペースジャンクションを横断することで、マッピングされたc$共有から残りのSVMネームスペースにアクセスできます。
- c$共有には、Microsoft管理コンソールを使用してアクセスできます。

関連情報

Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の設定

SMB共有の命名要件

SMBサーバでSMB共有を作成するときは、ONTAP共有の命名要件に注意してください。

ONTAPの共有の命名規則はWindowsの命名規則と同じで、次の要件があります。

- 各共有名はSMBサーバで一意である必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大文字数は80文字です。
- 共有名はUnicodeに対応しています。
- $文字で終わる共有名は非表示の共有です。
- ONTAP 9 .7以前の場合、admin$、ipc$、およびc$管理共有はすべてのCIFSサーバで自動的に作成され、共有名が予約されています。ONTAP 9 .8以降では、admin$共有は自動的に作成されなくなりました。
- 共有の作成時に共有名ONTAP _ ADMIN$を使用することはできません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。

    単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB共有の名前では次の特殊文字がサポートされます。

  なんだ? @ #$%&'__ 。~ （） { }

- SMB共有の名前では、次の特殊文字はサポートされません。

◦ "//\\:;|<> 、 ? * =

マルチプロトコル環境で共有を作成する際のディレクトリの大文字と小文字の区別

名前に大文字と小文字の違いしかないディレクトリ名を区別するために 8.3 の命名方法が使用されている SVM に共有を作成する場合は、クライアントが必要なディレクトリパスに接続できるように共有パスに 8.3 の名前を使用する必要があります。

次の例では、 Linux クライアント上に「 testdir 」と「 testdir 」という名前の 2 つのディレクトリが作成されています。ディレクトリを含むボリュームのジャンクションパスは、です `/home`。最初の出力は Linux クライアントで、 2 番目の出力は SMB クライアントで行います。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

2 番目のディレクトリへの共有を作成する場合、共有パスに 8.3 の名前を使用する必要があります。この例では、最初のディレクトリの共有パスはで `/home/testdir`、2番目のディレクトリの共有パスはです `/home/TESTDI~1`。

SMB共有プロパティを使用する

SMB共有プロパティの使用の概要

SMB 共有のプロパティをカスタマイズすることができます。

使用可能な共有プロパティは次のとおりです。

共有プロパティ	説明
`oplocks`	共有で便宜的ロック（クライアント側キャッシュ）を使用することを指定します。
`browsable`	Windowsクライアントが共有を参照することを許可します。
`showsnapshot`	クライアントがSnapshotコピーを表示およびトラバースできることを指定します。

共有プロパティ	説明
changenotify	共有が変更通知要求をサポートすることを指定します。SVM 上の共有では、これはデフォルトの初期プロパティです。
attributecache	属性にすばやくアクセスできるように SMB 共有でのファイル属性のキャッシュを有効にします。デフォルトでは、属性のキャッシュは無効になっています。このプロパティは、 SMB 1.0 経由で共有に接続するクライアントがある場合にのみ有効にしてください。クライアントが SMB 2.x または SMB 3.0 経由で共有に接続している場合、この共有プロパティは適用されません。
continuously-available	このプロパティは、サポートするSMBクライアントが永続的な方法でファイルを開くことを許可します。この方法で開いたファイルは、フェイルオーバーやギブバックなど、システムを停止させるイベントから保護されます。
branchcache	共有内のファイルに対するBranchCacheハッシュの要求をクライアントに許可します。このオプションが役立つのは、 CIFS の BranchCache 設定で動作モードとして「共有ごと」を指定した場合だけです。
access-based-enumeration	このプロパティは、この共有で _ アクセスベースの列挙 _ （ ABE ）を有効にするように指定します。ABEでフィルタリングされた共有フォルダは、個 々 のユーザのアクセス権に基づいてユーザに表示されるため、ユーザがアクセス権を持っていないフォルダやその他の共有リソースは表示されません。
namespace-caching	共有に接続するSMBクライアントが、CIFSサーバから返されるディレクトリの列挙結果をキャッシュできることを指定します。これにより、パフォーマンスが向上します。デフォルトでは、 SMB 1 のクライアントはディレクトリの列挙結果をキャッシュしません。SMB 2 および SMB 3 クライアントはデフォルトでディレクトリ列挙結果をキャッシュするため、この共有プロパティを指定してパフォーマンスが向上するのは SMB 1 クライアント接続のみです。
encrypt-data	この共有へのアクセス時にSMB暗号化を使用する必要があることを指定します。SMB データへのアクセスで暗号化をサポートしていない SMB クライアントは、この共有にアクセスできません。

共有プロパティを追加または削除することで、既存のSMB共有をカスタマイズできます。これは、環境内の要件の変化に合わせて共有設定を変更する場合に便利です。

開始する前に

プロパティを変更する共有が存在している必要があります。

タスクの内容

共有プロパティの追加に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。

  新しく追加したプロパティは、既存の共有プロパティのリストに追加されます。
- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- コマンドを使用して共有プロパティを削除することはできません `vserver cifs share properties add`。

  共有プロパティを削除するには、コマンドを使用し `vserver cifs share properties remove`ます。

共有プロパティの削除に関するガイドラインは次のとおりです。

- カンマで区切って1つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

手順

1. 該当するコマンドを入力します。

状況	入力するコマンド
共有プロパティを追加する	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
共有プロパティを削除する	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 共有プロパティの設定を確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドを実行すると、SVM vs1上の「`share1`」という名前の共有に共有プロパティが追加され

`showsnapshot`ます。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share1   /share1    oplocks      -          Everyone / Full
Control
                               browsable
                               changenotify
                               showsnapshot
```

次のコマンドは、SVM vs1上の「`share2'」という名前の共有から共有プロパティを削除し`browsable`ます。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share    Path       Properties   Comment    ACL
---------  ------   --------   ----------   --------   -----------
vs1        share2   /share2    oplocks      -          Everyone / Full
Control
                               changenotify
```

関連情報

SMB共有の管理用コマンド

force-group共有設定を使用したSMBユーザアクセスの最適化

ONTAP コマンドラインから、 UNIX 対応のセキュリティを使用するデータへの共有を作成するときに、 SMB ユーザがその共有内に作成するすべてのファイルが、 *force-group* と呼ばれる同じグループに属するように指定できます。このグループは、 UNIX グループデータベースで事前に定義されている必要があります。force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。

force-groupの指定が意味を持つのは、共有がUNIXまたはmixed qtree内にある場合のみです。NTFSボリュームまたはqtreeの共有内のファイルへのアクセスはUNIXのGIDではなくWindows権限によって決定されるため、これらの共有にforce-groupを設定する必要はありません。

共有にforce-groupが指定されている場合、共有は次のようになります。

- この共有にアクセスするforce-group内のSMBユーザは、force-groupのGIDに一時的に変更されます。

このGIDを使用すると、プライマリGIDまたはUIDでは通常アクセスできない共有内のファイルにアクセスできます。

- SMBユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリGIDに関係なく、同じforce-groupに属します。

SMBユーザがNFSで作成されたファイルにアクセスしようとすると、SMBユーザのプライマリGIDによってアクセス権が決定されます。

force-groupは、NFSユーザがこの共有内のファイルにアクセスする方法には影響しません。NFSで作成されたファイルは、ファイル所有者からGIDを取得します。アクセス権限は、ファイルにアクセスしようとしているNFSユーザのUIDとプライマリGIDに基づいて決定されます。

force-groupを使用すると、さまざまなグループに属するSMBユーザがファイルにアクセスできるようになります。たとえば、会社の Web ページを保存する共有を作成し、 Engineering グループと Marketing グループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「 webgroup1 」という名前の force-group に書き込み権限を与えます。force-group が指定されているため、 SMB ユーザがこの共有内に作成するすべてのファイルは「 webgroup1 」グループによって所有されます。また、ユーザが共有にアクセスするときは、「 webgroup1 」グループの GID が自動的に割り当てられます。その結果、すべてのユーザがこの共有に書き込むことができます。エンジニアリング部門とマーケティング部門のユーザのアクセス権を管理する必要はありません。

関連情報

force-group共有設定を使用したSMB共有の作成

force-group共有設定を使用してSMB共有を作成する

UNIXファイルセキュリティ形式のボリュームまたはqtree上のデータにアクセスするSMBユーザが、ONTAPで同じUNIXグループに属しているとみなされるようにするには、force-group共有設定を使用してSMB共有を作成します。

ステップ

1. SMB共有を作成します。 `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   (`\\servername\sharename\filepath`共有のUNCパスの文字数が256文字を超えている場合（UNCパスの先頭の""は除く\\）、Windowsの[プロパティ]ボックスの*[セキュリティ]*タブは使用できません。これは、ONTAPの問題ではなく、Windowsクライアントの問題です。この問題を回避するには、UNCパスが256文字を超える共有を作成しないでください。

   共有の作成後にforce-groupを削除する場合は、いつでも共有を変更し、パラメータの値として空の文字列（""）を指定でき`-force-group-for-create`ます。共有を変更してforce-groupを削除した場合、この共有への既存のすべての接続には、引き続き以前に設定されたforce-groupがプライマリGIDとして使用されます。

例

次のコマンドは、SMBユーザが作成するすべてのファイルがwebgroup1グループに割り当てられるディレクトリに、Webからアクセス可能な「webpages」共有を作成し`/corp/companyinfo`ます。

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

関連情報

force-group共有設定を使用したSMBユーザアクセスの最適化

MMCを使用したSMB共有に関する情報の表示

Microsoft 管理コンソール（ MMC ）を使用して SVM の SMB 共有情報を表示し、いくつかの管理タスクを実行できます。共有を表示する前に、 MMC を SVM に接続する必要があります。

タスクの内容

MMC を使用すると、 SVM 内の共有に対して次のタスクを実行できます。

- 共有を表示します
- アクティブなセッションを表示します
- 開いているファイルを表示します
- システムのセッション、ファイル、およびツリー接続のリストを列挙します
- 開いているファイルを閉じます
- 開いているセッションを閉じます
- 共有を作成 / 管理します

上記の機能によって表示されるビューは、クラスタではなくノードに固有のものです。そのため、 MMC を使用して SMB サーバホスト名（ cifs01.domain.local ）に接続すると、 DNS の設定に基づいてクラスタ内の単一の LIF にルーティングされます。

次の機能は、 MMC for ONTAP ではサポートされていません。

- 新しいローカルユーザ / グループを作成しています
- 既存のローカルユーザ / グループの管理 / 表示
- イベントまたはパフォーマンスログを表示する
- ストレージ
- サービスとアプリケーション

サポートされていない処理では、エラーが発生することがあり `remote procedure call failed`ます。

"FAQ ： ONTAP で Windows MMC を使用する"

手順

1. 任意の Windows サーバーでコンピュータの管理 MMC を開くには、 [コントロールパネル] で、 [管理ツール *]>[コンピュータの管理 *] を選択します。
2. 「 * アクション * > * 別のコンピューターに接続 * 」を選択します。

   [コンピュータの選択] ダイアログボックスが表示されます。
3. ストレージ・システムの名前を入力するか、または * Browse * をクリックしてストレージ・システムを検

索します。

4. [OK]*をクリックします。

   MMC が SVM に接続します。

5. ナビゲーションペインで、 * 共有フォルダ * > * 共有 * をクリックします。

   右側の表示ペインに SVM の共有のリストが表示されます。

6. 共有の共有プロパティを表示するには、共有をダブルクリックして * プロパティ * ダイアログボックスを開きます。

7. MMC を使用してストレージシステムに接続できない場合は、ストレージシステムで次のいずれかのコマンドを使用して、 BUILTIN\Administrators グループまたは BUILTIN\Power Users グループにユーザを追加できます。

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

SMB共有の管理用コマンド

SMB共有を管理するには、コマンドと `vserver cifs share properties`コマンドを使用し `vserver cifs share`ます。

状況	使用するコマンド
SMB共有を作成する	`vserver cifs share create`
SMB共有を表示する	`vserver cifs share show`
SMB共有を変更する	`vserver cifs share modify`
SMB共有を削除する	`vserver cifs share delete`
既存の共有に共有プロパティを追加する	`vserver cifs share properties add`
既存の共有から共有プロパティを削除する	`vserver cifs share properties remove`
共有プロパティに関する情報を表示する	`vserver cifs share properties show`

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。

SMB共有のACLを使用したファイルアクセスの保護

SMB共有レベルACLの管理に関するガイドライン

共有レベルの ACL を変更すると、共有に設定するアクセス権を強化したり、軽減したりできます。Windows のユーザとグループまたは UNIX のユーザとグループのいずれかを使用して共有レベルの ACL を設定できます。

デフォルトでは、共有レベルのACLによって、Everyoneという名前の標準グループにフルコントロールが付与されます。ACLにフルコントロールを指定すると、ドメインおよびすべての信頼できるドメインのすべてのユーザに共有へのフルアクセスが許可されます。共有レベルACLのアクセスレベルは、を使用して制御できます"WindowsクライアントまたはONTAPコマンドライン上のMicrosoft管理コンソール（MMC）"。

MMC を使用する際には、次の点に留意してください。

- 指定するユーザ名およびグループ名はWindows名である必要があります。
- Windows の権限だけを指定できます。

ONTAP コマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、 Windows 名または UNIX 名を使用できます。

  ACL の作成時または変更時に指定されない場合、デフォルトのタイプは Windows のユーザとグループです。

- Windows の権限だけを指定できます。

SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List（ACL；アクセス制御リスト）を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前、またはUNIXユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があり `Everyone / Full Control`ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。'vserver cifs share access-control delete -vserver <vserver_name>-share <share_name>-user-or-group everyone'
2. 新しいACLを設定します。

設定する **ACL** に使用するアカウント	入力するコマンド
Windowsユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windowsグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIXユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIXグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com」SVM上の「sales」共有に対するWindowsグループ「sales Team」に権限を付与します `Change`。

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

次のコマンドは `Read`、「vs2.example.com」SVM上の「eng」共有に対して「engineering」UNIXグループに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

次のコマンドは `Change` `Full_Control`、SVM「vs1」上の「datavol5」共有に対して「Tiger Team」という名前のローカルWindowsグループに権限と「Sue Chang」という名前のローカルWindowsユーザに権限を付与します。

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

SMB共有アクセス制御リストの管理用コマンド

Access Control List（ACL；アクセス制御リスト）の作成、表示、変更、削除など、SMBのAccess Control List（ACL；アクセス制御リスト）を管理するためのコマンドについて説明します。

状況	使用するコマンド
新しいACLを作成する	`vserver cifs share access-control create`
ACL を表示します	`vserver cifs share access-control show`
ACL を変更します	`vserver cifs share access-control modify`
ACL を削除します	`vserver cifs share access-control delete`

ファイル権限を使用したファイルアクセスの保護

Windowsの[セキュリティ]タブを使用した詳細なNTFSファイル権限の設定

Windows の [プロパティ] ウィンドウの [Windows セキュリティ *] タブを使用して、ファイルおよびフォルダの標準 NTFS ファイルアクセス権を構成できます。

開始する前に

このタスクを実行する管理者には、選択したオブジェクトの権限を変更するための十分なNTFS権限が必要です。

タスクの内容

NTFSファイル権限を設定するには、Windowsホストで、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。これらのタスクはWindows GUIで自動的に処理されます。

手順

1. Windows Explorer の * ツール * メニューから、 * ネットワークドライブのマップ * を選択します。
2. [* ネットワークドライブの割り当て *] ダイアログボックスに入力します。
   a. ドライブ文字を選択します。
   b. [* フォルダ *] ボックスに、権限を適用するデータと共有名を含む共有を含む CIFS サーバー名を入力します。

      CIFSサーバ名が「CIFS_SERVER」で、共有の名前が「'share1'」の場合は、と入力します。
      `\\CIFS_SERVER\share1`

      CIFSサーバ名の代わりに、CIFSサーバのデータ インターフェイスのIPアドレスを指定することもできます。

   c. [完了] をクリックします。

   選択したドライブがマウントされ、Windowsエクスプローラウィンドウに共有内に格納されているファイルとフォルダが表示されます。
3. NTFSファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * プロパティ * を選択します。
5. [* セキュリティ *] タブを選択します。

   Security タブには、 NTFS アクセス権が設定されているユーザーおよびグループのリストが表示されます。[* アクセス許可の対象 *] ボックスには、選択した各ユーザーまたはグループに対して有効な [許可] と [拒否] のアクセス許可のリストが表示されます。
6. 「 * 詳細設定 * 」をクリックします。

   Windowsの[プロパティ]ウィンドウには、ユーザおよびグループに割り当てられている既存のファイル権限に関する情報が表示されます。
7. [権限の変更 *] をクリックします。

   [権限]ウィンドウが開きます。
8. 次のうち必要な操作を実行します。

状況	操作
新しいユーザまたはグループの詳細なNTFS権限を設定する	a. [追加]*をクリックします。 b. [* 選択するオブジェクト名を入力してください *] ボックスに、追加するユーザーまたはグループの名前を入力します。 c. [OK]*をクリックします。
ユーザまたはグループの詳細なNTFS権限を変更する	a. [* アクセス権エントリ： *] ボックスで、詳細なアクセス権を変更するユーザーまたはグループを選択します。 b. [編集（ Edit ）] をクリックします。
ユーザまたはグループの詳細なNTFS権限を削除する	a. [* アクセス許可エントリ： *] ボックスで、削除するユーザーまたはグループを選択します。 b. [削除（ Remove ）] をクリックします。 c. 手順13に進みます。

新しいユーザまたはグループに詳細な NTFS 権限を追加する場合、または既存のユーザまたはグループの NTFS 詳細権限を変更する場合は、 <Object> の権限エントリボックスが開きます。

9. [* 適用先 *] ボックスで、この NTFS ファイル許可エントリを適用する方法を選択します。

   1 つのファイルに NTFS ファイル権限を設定する場合、 * Apply to * ボックスはアクティブになりません。[* 適用先 * （ Apply to * ）] 設定のデフォルトは、 * このオブジェクトのみ * です。

10. [* アクセス許可 *] ボックスで、このオブジェクトに設定する詳細なアクセス許可の [* 許可 *] または [* 拒否 *] ボックスを選択します。

    - 指定したアクセスを許可するには、 * 許可 * ボックスを選択します。
    - 指定されたアクセスを許可しない場合は、 * Deny * ボックスを選択します。次の詳細な権限に対して権限を設定できます。
    - * フルコントロール *

      この詳細な権限を選択すると、他のすべての詳細な権限が自動的に選択されます（それらの権限が許可または拒否されます）。

    - * フォルダの移動 / ファイルの実行 *
    - * フォルダのリスト / データの読み取り *
    - * 属性の読み取り *
    - * 拡張属性の読み取り *
    - * ファイルの作成 / データの書き込み *
    - * フォルダの作成 / データの追加 *
    - * 属性の書き込み *

- * 拡張属性の書き込み *
- * サブフォルダとファイルの削除 *
- * 削除 *
- * 読み取り許可 *
- * 権限の変更 *
- * 所有権を取りなさい *

> いずれかの詳細な権限ボックスが選択できない場合は、権限が親オブジェクトから継承されるためです。

11. このオブジェクトのサブフォルダとファイルにこれらのアクセス権を継承させる場合は、 [このコンテナ内のオブジェクトまたはコンテナにこれらのアクセス権を適用する *] ボックスをオンにします。
12. [OK]*をクリックします。
13. NTFS権限の追加、削除、または編集が完了したら、このオブジェクトの継承設定を指定します。
    - [このオブジェクトの親から継承可能な権限を含める *] ボックスをオンにします。

      これがデフォルトです。
    - [このオブジェクトから継承可能な権限ですべての子オブジェクトを置換する *] ボックスをオンにします。

      この設定は、単一ファイルに対してNTFSファイル権限を設定する場合は[権限]ボックスに表示されません。

      > この設定を選択する場合は注意が必要です。この設定では、すべての子オブジェクトに対する既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除したくない権限を誤って削除する可能性があります。これは、mixedセキュリティ形式のボリュームまたはqtreeで権限を設定する場合に特に重要です。子オブジェクトがUNIX対応のセキュリティ形式を使用している場合に、これらの子オブジェクトにNTFSアクセス権を適用すると、ONTAPによってこれらのオブジェクトがUNIXセキュリティ形式からNTFSセキュリティ形式に変更され、これらの子オブジェクトのすべてのUNIXアクセス権がNTFSアクセス権に置き換えられます。
    - 両方のボックスを選択します。
    - どちらのボックスも選択しない。
14. **OK** をクリックして、 *Permissions * ボックスを閉じます。
15. OK * をクリックして、 * <Object>* の高度なセキュリティ設定ボックスを閉じます。

詳細なNTFS権限の設定方法の詳細については、Windowsのマニュアルを参照してください。

関連情報

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

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

ONTAP CLIを使用したNTFSファイル権限の設定

ONTAP CLIを使用して、ファイルおよびディレクトリに対してNTFSファイル権限を設定できます。これにより、WindowsクライアントでSMB共有を使用してデータに接続することなくNTFSファイル権限を設定できます。

NTFSファイル権限を設定するには、NTFSセキュリティ記述子に関連付けられているNTFS Discretionary Access Control List（DACL；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子がNTFSファイルおよびディレクトリに適用されます。

コマンドラインを使用して設定できるのはNTFSファイル権限のみです。CLIを使用してNFSv4 ACLを設定することはできません。

手順

1. NTFSセキュリティ記述子を作成します。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. NTFSセキュリティ記述子にDACLを追加します。

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. ファイルやディレクトリのセキュリティポリシーを作成します。

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

SMB経由でファイルにアクセスする際のUNIXファイル権限によるアクセス制御方法

FlexVol ボリュームのセキュリティ形式は、 NTFS 、 UNIX 、 mixed の 3 種類のいずれかにすることができます。セキュリティ形式に関係なく SMB 経由でデータにアクセスできますが、 UNIX 対応のセキュリティを使用するデータにアクセスするには、適切な UNIX ファイル権限が必要になります。

SMB 経由でのデータへのアクセス時には、いくつかのアクセス制御を使用して、要求した操作を実行する権限がユーザにあるかどうかが判断されます。

- エクスポート権限

  SMB アクセスに関するエクスポート権限の設定はオプションです。

- 共有権限
- ファイル権限

  ユーザが操作を実行するデータには、次のタイプのファイル権限を適用できます。

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX モードビット

NFSv4 ACL または UNIX モードビットが設定されたデータの場合は、 UNIX 形式のアクセス権を使用してデータへのファイルアクセス権が決定されます。SVM 管理者は、適切なファイル権限を設定して、ユーザに目的のアクションを実行する権限が付与されるようにする必要があります。

mixed セキュリティ形式のボリューム内のデータでは、 NTFS または UNIX 対応のセキュリティ形式を使用できます。UNIX 対応のセキュリティ形式を使用するデータの場合は、データに対するファイル権限を判断するときに NFSv4 権限または UNIX モードビットが使用されます。

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護

ダイナミックアクセス制御（DAC）を使用したファイルアクセスの保護の概要

ダイナミックアクセス制御を使用してアクセスを保護できます。Active Directoryで集約型アクセスポリシーを作成し、適用されたGPOを使用してSVM上のファイルとフォルダにそのポリシーを適用します。集約型アクセスポリシーのステージングイベントを使用するように監査を設定すると、集約型アクセスポリシーの変更を適用する前にその影響を確認できます。

CIFSクレデンシャルへの追加

ダイナミックアクセス制御が導入される前は、CIFSクレデンシャルにセキュリティプリンシパル（ユーザ）のIDとWindowsグループメンバーシップが含まれていました。ダイナミックアクセス制御では、さらに3種類の情報（デバイスID、デバイス要求、およびユーザ要求）がクレデンシャルに追加されます。

- デバイスID

  ユーザーのID情報と類似していますが、ユーザーがログインしているデバイスのIDとグループメンバーシップが異なります。

- デバイスの信頼性

  デバイスセキュリティプリンシパルに関するアサーション。たとえば、デバイスが特定のOUのメンバーであることが要求される場合があります。

- ユーザの信頼性

  ユーザセキュリティプリンシパルに関するアサーション。たとえば、ADアカウントが特定のOUのメンバーであることをユーザが要求する場合があります。

集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザ要求、デバイス要求、およびリソースプロパティを使用した条件式を含む許可ポリシーを一元的に導入および管理できます。

たとえば、ビジネスに影響の大きいデータにアクセスするには、フルタイムの従業員であり、管理対象デバイスからのみデータにアクセスできる必要があります。集約型アクセスポリシーはActive Directoryで定義され、GPOメカニズムを介してファイルサーバに配布されます。

高度な監査を使用した集約型アクセスポリシーのステージング

集約型アクセスポリシーは「集約型」にすることができます。この場合、ファイルアクセスチェック時に「what if 」方式で評価されます。ポリシーが有効になっていた場合に発生した結果、および現在の設定とどのように異なるかが監査イベントとして記録されます。このようにして、管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセスポリシーの変更による影響を調べることができます。アクセスポリシーの変更による影響を評価したら、GPOを使用して目的のSVMにポリシーを導入できます。

関連情報

サポートされるGPO

CIFSサーバへのグループ ポリシー オブジェクトの適用

CIFSサーバでのGPOサポートの有効化と無効化

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

CIFSサーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御セキュリティに関する情報の表示

"SMBおよびNFSの監査とセキュリティトレース"

サポートされるダイナミックアクセス制御機能

CIFSサーバでダイナミックアクセス制御（DAC）を使用する場合は、ONTAPがActive Directory環境でどのようにダイナミックアクセス制御機能をサポートするかを理解しておく必要があります。

ダイナミックアクセス制御でサポート

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートします。

機能	コメント
ファイルシステムへの要求	クレームは単純な名前と値のペアで、ユーザーについての真実を記述します。ユーザクレデンシャルにはクレーム情報が含まれており、ファイルのセキュリティ記述子はクレームチェックを含むアクセスチェックを実行できます。これにより、管理者は誰がファイルにアクセスできるかをより細かく制御できます。
ファイルアクセスチェック用の条件式	ファイルのセキュリティパラメータを変更する場合、ユーザは任意に複雑な条件式をファイルのセキュリティ記述子に追加できます。条件式には、クレームのチェックを含めることができます。
集約型アクセスポリシーによるファイルアクセスの一元管理	集約型アクセスポリシーは、Active Directoryに格納されるACLの一種で、ファイルへのタグ付けが可能です。ファイルへのアクセスは、ディスクのセキュリティ記述子とタグ付けされた集約型アクセスポリシーの両方のアクセスチェックでアクセスが許可されている場合にのみ許可されます。これにより、管理者は、ディスクのセキュリティ記述子を変更することなく、一元的な場所（AD）からファイルへのアクセスを制御できます。
集約型アクセスポリシーのステージング	集約型アクセスポリシーへの変更を「集約型アクセスポリシー」し、監査レポートで変更の影響を確認することで、実際のファイルアクセスに影響を与えずにセキュリティの変更を試す機能を追加します。
ONTAP CLIを使用した集約型アクセスポリシーセキュリティに関する情報の表示のサポート	コマンドを拡張し `vserver security file-directory show`て、適用されている集約型アクセスポリシーに関する情報を表示します。
集約型アクセスポリシーを含むセキュリティトレース	コマンドファミリーを拡張し、 `vserver security trace`適用されている集約型アクセスポリシーに関する情報を含む結果を表示します。

ダイナミックアクセス制御でサポートされない

CIFSサーバでダイナミックアクセス制御が有効になっている場合、ONTAPは次の機能をサポートしません。

機能	コメント
NTFSファイルシステムオブジェクトの自動分類	これは、ONTAPでサポートされていないWindowsファイル分類インフラストラクチャの拡張機能です。
集約型アクセスポリシーのステージング以外の高度な監査	高度な監査では、集約型アクセスポリシーのステージングのみがサポートされます。

CIFSサーバでダイナミックアクセス制御と集約型アクセスポリシーを使用する際の考慮事項

CIFS サーバ上のファイルとフォルダを保護するために Dynamic Access Control （ DAC ；ダイナミックアクセス制御）と集約型アクセスポリシーを使用する際は、一定の考慮事項に注意する必要があります。

ポリシールール「環境 domain\administrator user 」の場合、 root に対して NFS アクセスが拒否されることがあります

特定の状況では、 root ユーザがアクセスしようとしているデータに集約型アクセスポリシーセキュリティが適用されていると、 root に対して NFS アクセスが拒否されることがあります。問題は、集約型アクセスポリシーに domain\administrator に適用されるルールが含まれており、 root アカウントが domain\administrator アカウントにマッピングされている場合に実行されます。

domain\administrator ユーザにルールを適用する代わりに、 domain\administrators グループなど、管理者権限を持つグループにルールを適用してください。これにより、 root を domain\administrator アカウントにマッピングしても、 root はこの問題の影響を受けなくなります。

適用された集約型アクセスポリシーがActive Directoryに見つからないと、CIFSサーバのBUILTIN\Administratorsグループにリソースへのアクセスが許可されます

CIFS サーバに格納されたリソースに集約型アクセスポリシーが適用されている場合に、 CIFS サーバが集約型アクセスポリシーの SID を使用して Active Directory から情報を取得しようとしても、 SID が Active Directory 内の既存の集約型アクセスポリシーの SID と一致しないことがあります。このような場合、 CIFS サーバはそのリソースにローカルのデフォルトのリカバリポリシーを適用します。

ローカルのデフォルトのリカバリポリシーでは、 CIFS サーバの BUILTIN\Administrators グループにそのリソースへのアクセスが許可されます。

ダイナミックアクセス制御の有効化または無効化の概要

ダイナミックアクセス制御（DAC）を使用してCIFSサーバ上のオブジェクトを保護できるオプションは、デフォルトでは無効になっています。CIFSサーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFSサーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用しない場合は、オプションを無効にすることができます。

タスクの内容

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを含むACLをファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御エントリは無視され、新しいエントリは許可されません。

このオプションは、advanced権限レベルでのみ使用できます。

ステップ

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。

ダイナミックアクセス制御の設定	入力するコマンド
有効	`vserver cifs options modify -vserver vserver_name -is-dac-enabled true`
無効にする	`vserver cifs options modify -vserver vserver_name -is-dac-enabled false`

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

関連情報

CIFSサーバ上のデータを保護する集約型アクセスポリシーの設定

ダイナミックアクセス制御が無効な場合にダイナミックアクセス制御**ACE**を含む**ACL**を管理します。

ダイナミックアクセス制御ACEが適用されたACLが設定されたリソースがある場合にStorage Virtual Machine（SVM）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御ACEを削除してから、そのリソースの非ダイナミックアクセス制御ACEを管理する必要があります。

タスクの内容

ダイナミックアクセス制御を無効にした場合、既存のダイナミックアクセス制御 ACE を削除するまでは、既存の非ダイナミックアクセス制御 ACE の削除や新しい非ダイナミックアクセス制御 ACE の追加はできません。

これらの手順は、通常 ACL の管理に使用している任意のツールを使用して実行できます。

手順

1. リソースに適用されているダイナミックアクセス制御 ACE を確認します。
2. リソースからダイナミックアクセス制御 ACE を削除します。
3. 必要に応じて、リソースに対して非ダイナミックアクセス制御 ACE を追加または削除します。

CIFSサーバ上のデータを保護する集約型アクセスポリシーを設定する

集約型アクセスポリシーを使用してCIFSサーバ上のデータへのアクセスを保護するには、CIFSサーバでのダイナミックアクセス制御（DAC）の有効化、Active Directoryでの集約型アクセスポリシーの設定、GPOを含むActive Directoryコンテナへの集約型アクセスポリシーの適用、CIFSサーバでのGPOの有効化など、いくつかの手順を実行する必要があります。

開始する前に

- 集約型アクセスポリシーを使用するようにActive Directoryを設定する必要があります。
- 集約型アクセスポリシーを作成し、CIFSサーバを含むコンテナにGPOを作成して適用するには、Active Directoryドメインコントローラに対する十分なアクセスが必要です。

- 必要なコマンドを実行するには、Storage Virtual Machine（SVM）に対する十分な管理アクセスが必要です。

タスクの内容

集約型アクセスポリシーは、Active Directoryのグループポリシーオブジェクト（GPO）に定義されて適用されます。集約型アクセスポリシーとGPOの設定手順については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNetライブラリ"

手順

1. コマンドを使用して、SVMのダイナミックアクセス制御を有効にしていない場合は有効にし `vserver cifs options modify`ます。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. コマンドを使用して、CIFSサーバでグループポリシーオブジェクト（GPO）を有効にしていない場合は有効にし `vserver cifs group-policy modify`ます。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Active Directoryで集約型アクセスルールと集約型アクセスポリシーを作成します。
4. グループポリシーオブジェクト（GPO）を作成して、Active Directoryに集約型アクセスポリシーを導入します。
5. CIFSサーバのコンピュータアカウントが配置されているコンテナにGPOを適用します。
6. コマンドを使用して、CIFSサーバに適用されたGPOを手動で更新します `vserver cifs group-policy update`。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. コマンドを使用して、CIFSサーバ上のリソースにGPO集約型アクセスポリシーが適用されていることを確認します `vserver cifs group-policy show-applied`。

   次の例は、デフォルトのドメインポリシーに2つの集約型アクセスポリシーがあり、それらがCIFSサーバに適用されていることを示しています。

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
   ```

```
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
```

```
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

関連情報

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

ダイナミックアクセス制御の有効化と無効化

ダイナミックアクセス制御セキュリティに関する情報を表示する

NTFSボリューム、およびmixedセキュリティ形式のボリューム上のNTFS対応セキュリティを使用するデータのダイナミックアクセス制御（DAC）セキュリティに関する情報を表示できます。これには、条件付きACE、リソースACE、集約型アクセスポリシーACEに関する情報が含まれます。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。

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`
出力にはグループSIDとユーザSIDが表示されます。	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16進数のビットマスクがテキスト形式に変換されるファイルおよびディレクトリのファイルおよびディレクトリのセキュリティについて	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

例

次の例では、SVM vs1のパスに関するダイナミックアクセス制御セキュリティの情報を表示します `/vol1`。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                            Vserver: vs1
                          File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

関連情報

GPO設定に関する情報の表示

集約型アクセスポリシーに関する情報の表示

集約型アクセスポリシールールに関する情報の表示

ダイナミックアクセス制御のリバートに関する考慮事項

ダイナミックアクセス制御（ DAC ）をサポートしないバージョンの ONTAP にリバートする場合に発生する状況と、リバートの前後に必要な処理を把握しておく必要がありま

す。

ダイナミックアクセス制御がサポートされていないバージョンの ONTAP にクラスタをリバートし、 1 つ以上の Storage Virtual Machine （ SVM ）でダイナミックアクセス制御が有効になっている場合、リバート前に次の処理を実行する必要があります。

- クラスタでダイナミックアクセス制御が有効になっているすべての SVM で、ダイナミックアクセス制御を無効にする必要があります。
- イベントタイプを含むクラスタでは、イベントタイプのみを使用するように `file-op`監査の設定を変更する必要があります `cap-staging`。

ダイナミックアクセス制御 ACE が設定されているファイルやフォルダについて、リバートに関する重要な考慮事項を理解し、対応する必要があります。

- クラスタをリバートした場合、既存のダイナミックアクセス制御 ACE は削除されませんが、ファイルアクセスチェックで無視されます。
- リバート後はダイナミックアクセス制御 ACE は無視されるため、ダイナミックアクセス制御 ACE が設定されたファイルへのアクセスには変更が発生します。

  これにより、ユーザは以前にアクセスできなかったファイルにアクセスできるようになり、以前にアクセスできたファイルにアクセスできなくなる可能性があります。

- 以前のセキュリティレベルに戻すには、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する必要があります。

  この処理は、リバート前またはリバート完了直後に実行できます。

> リバート後はダイナミックアクセス制御 ACE は無視されるため、影響を受けるファイルに非ダイナミックアクセス制御 ACE を適用する際にダイナミックアクセス制御 ACE を削除する必要はありません。ただし、必要に応じて手動で削除することもできます。

ダイナミックアクセス制御と集約型アクセスポリシーの設定および使用に関する詳細情報の参照先

ダイナミックアクセス制御と集約型アクセスポリシーを設定および使用する方法については、その他のリソースを参照してください。

Active Directoryに対するダイナミックアクセス制御と集約型アクセスポリシーの設定方法については、Microsoft TechNetライブラリを参照してください。

"Microsoft TechNet ：「ダイナミックアクセス制御のシナリオの概要"

"Microsoft TechNet ：「集約型アクセスポリシーのシナリオ"

ダイナミックアクセス制御と集約型アクセスポリシーを使用してサポートするようにSMBサーバを設定するには、次の資料を参照することができます。

- * SMBサーバーでのGPOの使用*

  SMBサーバへのグループポリシーオブジェクトの適用

- * SMBサーバでのNAS監査の設定*

  "SMBおよびNFSの監査とセキュリティトレース"

エクスポートポリシーを使用したSMBアクセスの保護

SMBアクセスでのエクスポートポリシーの使用方法

SMBサーバでSMBアクセスのエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御する際にエクスポートポリシーが使用されます。データにアクセスするには、SMBアクセスを許可するエクスポートポリシーを作成し、SMB共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには、データへのアクセスを許可するクライアント、および読み取り専用アクセスと読み取り/書き込みアクセスでサポートされる認証プロトコルを指定するルールが1つ以上適用されます。エクスポートポリシーを設定して、すべてのクライアント、クライアントのサブネット、または特定のクライアントにSMB経由のアクセスを許可し、データへの読み取り専用アクセスと読み取り/書き込みアクセスを決定する際にKerberos認証、NTLM認証、またはKerberosとNTLMの両方を使用した認証を許可できます。

ONTAPは、エクスポートポリシーに適用されたすべてのエクスポートルールを処理したあと、クライアントにアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windowsのユーザおよびグループではなく、クライアントマシンに適用されます。エクスポートルールは、Windowsのユーザおよびグループベースの認証および許可に代わるものではありません。エクスポートルールは、共有権限とファイルアクセス権限に加えて、アクセスセキュリティのもう1つのレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとにエクスポートポリシーを1つ関連付けます。各 SVM には複数のエクスポートポリシーを含めることができます。これにより、複数のボリュームを備えた SVM に対して次の操作を実行できます。

- SVM のボリュームごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームへのクライアントアクセスを個別に制御する。
- SVM の複数のボリュームに同じエクスポートポリシーを割り当て、同一のクライアントアクセス制御を実行する。ボリュームごとに新しいエクスポートポリシーを作成する必要はありません。

各 SVM には、「デフォルト」という名前のエクスポートポリシーが少なくとも 1 つあります。これにはルールは含まれません。このエクスポートポリシーは削除できませんが、名前や変更は可能です。デフォルトでは、 SVM 上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVM で SMB アクセスのエクスポートポリシーが無効になっている場合、「 default 」エクスポートポリシーは SMB アクセスには影響しません。

NFSホストとSMBホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。エクスポートポリシーを、NFSホストとSMBホストの両方がアクセスする必要があるデータが格納されたボリュームに関連付けることができます。または、SMBクライアントのみがアクセスを必要とするボリュームがある場合は、SMBプロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証にKerberosまたはNTLMのみ（またはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーをSMBアクセスのみが必要なボリュームに関連付けます。

SMBのエクスポートポリシーが有効になっている場合に、クライアントが適用可能なエクスポートポリシー

で許可されていないアクセス要求を行うと、権限拒否のメッセージが表示されて要求は失敗します。クライアントがボリュームのエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポートポリシーが空の場合、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、SMB共有を含むボリュームで少なくとも以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアントまたは適切なクライアントサブセットへのアクセスを許可する
- SMB経由のアクセスを許可する
- Kerberos認証またはNTLM認証（またはその両方）を使用して、適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちらをご覧ください "エクスポートポリシーの設定と管理"。

エクスポートルールの仕組み

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポートルールでは、ボリュームへのクライアントアクセス要求が設定した特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順序で処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致した場合、そのルールの権限が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用してクライアントアクセス権限を決定するようにエクスポートルールを設定できます。

- クライアントが要求の送信に使用するファイルアクセスプロトコル（NFSv4やSMBなど）。
- クライアント識別子（ホスト名やIPアドレスなど）。

  フィールドの最大サイズ `-clientmatch`は4096文字です。

- クライアントが認証に使用するセキュリティタイプ（Kerberos v5、NTLM、AUTH_SYSなど）。

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

例
エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv3プロトコルを使用して送信され、クライアントのIPアドレスは10.1.17.37です。

クライアントアクセスプロトコルが一致していても、クライアントのIPアドレスがエクスポートルールで指定されているサブネットとは異なるサブネットに属しています。そのため、クライアント一致は失敗し、このルールはこのクライアントには適用されません。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントのIPアドレスが指定したサブネットにあります。したがって、クライアント一致は成功し、このルールはこのクライアントに適用されます。セキュリティタイプに関係なく、クライアントは読み取り/書き込みアクセス権を取得します。

例

エクスポートポリシーには、次のパラメータを持つエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されます。

両方のクライアントでクライアントアクセスプロトコルとIPアドレスが一致している。読み取り専用パラメータでは、認証に使用したセキュリティタイプに関係なく、すべてのクライアントに読み取り専用アクセスが許可されます。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り/書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認済みのセキュリティタイプKerberos v5が使用されているためです。クライアント#2は読み取り/書き込みアクセス権を取得しません。

SMB経由のアクセスを制限または許可するエクスポートポリシールールの例

以下の例は、 SMB アクセスのエクスポートポリシーが有効になっている SVM で SMB 経由のアクセスを制限または許可するエクスポートポリシールールを作成する方法を示しています。

SMB アクセスに関するエクスポートポリシーは、デフォルトでは無効になっています。SMB 経由のアクセスを制限または許可するエクスポートポリシールールは、 SMB アクセスのエクスポートポリシーを有効にしている場合にのみ設定する必要があります。

SMB アクセスのみのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifs1
- インデックス番号： 1.
- クライアント一致： 192.168.1.0/24 ネットワーク上のクライアントにのみ一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM 認証または Kerberos 認証を使用するクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証を使用するクライアントに許可します

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB および **NFS** アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifsnfs1
- インデックス番号： 2.
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスと NFS アクセス
- 読み取り専用アクセス：すべてのクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証（ NFS および SMB ）または NTLM 認証（ SMB ）を使用するクライアントに許可
- UNIX ユーザ ID 0 （ゼロ）のマッピング：ユーザ ID 65534 （通常ユーザ名 nobody にマッピングされる）にマッピング
- suid と sgid のアクセス：許可しています

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

NTLM のみを使用する **SMB** アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：ntlm1
- インデックス番号： 1.
- クライアント一致：すべてのクライアントに一致します

- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM を使用するクライアントにのみ許可されます
- 読み取り / 書き込みアクセス： NTLM を使用するクライアントにのみ許可されます

> NTLM のみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションで IP アドレスベースのエントリを使用する必要があります。そうしないと、エラーが発生し `access denied`ます。これは、 ONTAP がホスト名を使用してクライアントの権限を確認するときに、 Kerberos Service Principal Name （ SPN ；サービスプリンシパル名）を使用するためです。NTLM 認証では、 SPN 名はサポートされません。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

SMBアクセスに関するエクスポートポリシーの有効化または無効化

Storage Virtual Machine （ SVM ）での SMB アクセスに関するエクスポートポリシーを有効または無効にすることができます。エクスポートポリシーを使用したリソースへの SMB アクセスの制御はオプションです。

開始する前に

SMB のエクスポートポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポートルールを作成する前に、そのクライアントの「 PTR 」レコードが DNS に登録されている必要があります。
- SVM が NFS クライアントにアクセスを提供し、 NFS アクセスに使用するホスト名が CIFS サーバ名と異なる場合は、ホスト名に対して「 A 」レコードと「 PTR 」レコードのセットが追加で必要です。

タスクの内容

SVM に新しい CIFS サーバをセットアップするとき、 SMB アクセスに関するエクスポートポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアント IP アドレス、またはホスト名に基づいてアクセスを制御する場合は、 SMB アクセスのエクスポートポリシーを有効にできます。SMB アクセスに関するエクスポートポリシーはいつでも有効または無効にできます。

手順

1. 権限レベルをadvancedに設定します。 `set -privilege advanced`
2. エクスポートポリシーを有効または無効にします。
   - エクスポートポリシーを有効にします。 `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled true`
   - エクスポートポリシーを無効にします。 `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`
3. admin権限レベルに戻ります。 `set -privilege admin`

例

次の例では、エクスポートポリシーを使用したSVM vs1上のリソースへのSMBクライアントアクセスの制御を有効にします。

```
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-exportpolicy
-enabled true

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

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を使用したファイルアクセスの保護

ネイティブファイルレベルのセキュリティとエクスポートおよび共有のセキュリティを使用したアクセスの保護に加えて、ボリュームレベルで ONTAP によって適用される第 3 のセキュリティレイヤとして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：すべての NAS プロトコルから適用されるストレージオブジェクトへの環境アクセスを保護します。

NTFSのアクセス権限のみがサポートされます。ONTAP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にアクセスするUNIXユーザのセキュリティチェックを実行するには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。

ストレージレベルのアクセス保護の動作

- ストレージレベル環境のアクセス保護：ストレージオブジェクト内のすべてのファイルまたはすべてのディレクトリを保護します。

  ボリューム内のすべてのファイルまたはディレクトリがストレージレベルのアクセス保護設定の影響を受けるため、伝播による継承は必要ありません。

- ストレージレベルのアクセス保護は、ボリューム内のファイルのみ、ディレクトリのみ、またはファイルとディレクトリの両方に適用されるように設定できます。
  - ファイルとディレクトリのセキュリティ

    ストレージオブジェクト内のすべてのディレクトリとファイルを環境に格納します。これがデフォルト設定です。

  - ファイルセキュリティ

    ストレージオブジェクト内のすべてのファイルを環境します。このセキュリティを適用しても、ディ

レクトリへのアクセスとディレクトリの監査には影響しません。

- ディレクトリセキュリティ

  ストレージオブジェクト内のすべてのディレクトリを環境します。このセキュリティを適用しても、ファイルへのアクセスとファイルの監査には影響しません。

- 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。

- NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。

  有効な権限を決定するために、ストレージオブジェクトレベルで適用され、メタデータに格納されます。

- 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。

  このセキュリティは、ストレージ管理者のみが変更できるように設計されています。

- ストレージレベルのアクセス保護は、 NTFS または mixed セキュリティ形式のボリュームに適用できます。
- ストレージレベルのアクセス保護を UNIX セキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれている SVM で CIFS サーバが設定されている場合に限られます。
- ボリュームがボリュームジャンクションパス以下にマウントされていて、そのパスにストレージレベルのアクセス保護が存在している場合、その下にマウントされているボリュームには伝播されません。
- 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は、 SnapMirror データレプリケーションおよび SVM レプリケーションによってレプリケートされます。
- ウィルススキャンについては特別な免除があります。

  ファイルやディレクトリのスクリーニングを行うこれらのサーバに対しては、ストレージレベルのアクセス保護によってオブジェクトへのアクセスが拒否されていても、例外的なアクセスが許可されます。

- ストレージレベルのアクセス保護によってアクセスが拒否された場合、 FPolicy 通知は送信されません。

アクセスチェックの順序

ファイルまたはディレクトリへのアクセスは、エクスポートまたは共有の権限、ボリュームで設定されているストレージレベルのアクセス保護権限、ファイルやディレクトリに適用されるネイティブのファイル権限の各影響の組み合わせによって決まります。すべてのレベルのセキュリティが評価されて、ファイルまたはディレクトリの有効な権限が決定されます。セキュリティアクセスチェックは、次の順序で実行されます。

1. SMB 共有または NFS エクスポートレベルの権限
2. ストレージレベルのアクセス保護
3. NTFSのファイル/フォルダのAccess Control List（ACL；アクセス制御リスト）、NFSv4 ACL、またはUNIXモードビット

ストレージレベルのアクセス保護の使用のユースケース

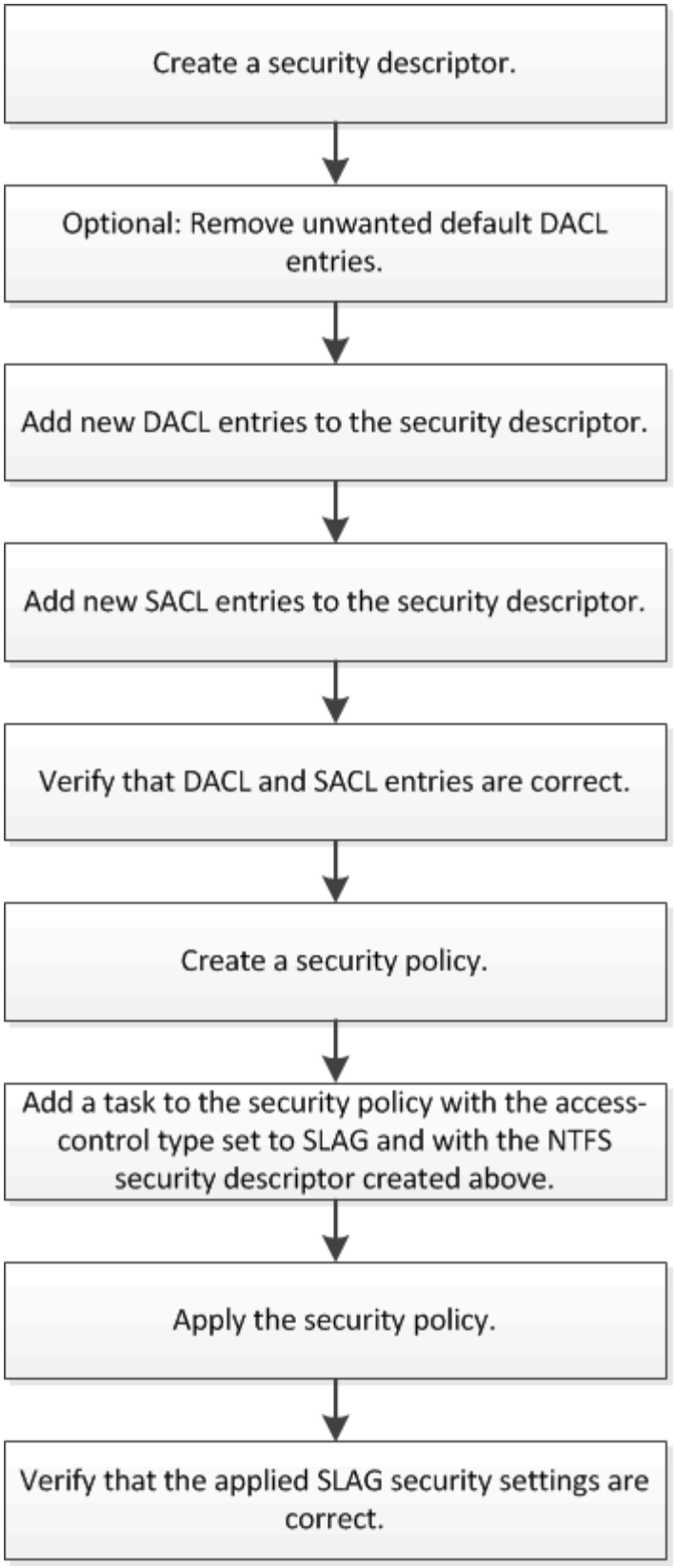
ストレージレベルのアクセス保護は、ストレージレベルでの追加セキュリティを提供します。このセキュリティはクライアント側からは見えないため、ユーザや管理者がデスクトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

この機能の一般的なユースケースとしては、次のようなシナリオがあります。

- すべてのユーザーのアクセスをストレージ・レベルで監査および制御することにより ' 知的財産を保護します
- 銀行や証券会社など、金融サービス企業のストレージの場合
- 部門ごとに個別のファイルストレージを使用する行政サービス
- すべての学生のファイルを保護する大学

ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護（SLAG）を設定するワークフローでは、NTFSファイル権限と監査ポリシーの設定に使用するONTAP CLIコマンドと同じコマンドを使用します。対象のファイルやディレクトリのアクセスを設定する代わりに、対象のStorage Virtual Machine（SVM）ボリュームのSLAGを設定します。



関連情報

ストレージレベルのアクセス保護の設定

ストレージレベルのアクセス保護の設定

ボリュームまたはqtreeにストレージレベルのアクセス保護を設定するには、いくつかの手順に従う必要があります。ストレージレベルのアクセス保護は、ストレージレベルで設定されるアクセスセキュリティのレベルを提供します。すべてのNASプロトコルから適用先のストレージオブジェクトへのすべてのアクセスに適用されるセキュリティを提供します。

手順

1. コマンドを使用して、セキュリティ記述子を作成し `vserver security file-directory ntfs create`ます。

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

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   セキュリティ記述子は、次の4つのデフォルトDACL Access Control Entry（ACE；アクセス制御エントリ）で作成されます。

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   ストレージレベルのアクセス保護の設定時にデフォルトのエントリを使用しない場合は、セキュリティ記述子に独自のACEを作成して追加する前に、デフォルトのエントリを削除できます。

2. セキュリティ記述子から、ストレージレベルのアクセス保護セキュリティで設定したくないデフォルト

のDACL ACEを削除します。

a. コマンドを使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove`。

   この例では、セキュリティ記述子から BUILTIN\Administrators 、 BUILTIN\Users 、 CREATOR OWNER の 3 つのデフォルト DACL ACE を削除しています。

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. コマンドを使用して、ストレージレベルのアクセス保護セキュリティに使用しないDACL ACEがセキュリティ記述子から削除されたことを確認します `vserver security file-directory ntfs dacl show`。

   この例では、コマンドの出力によって、3つのデフォルトDACL ACEがセキュリティ記述子から削除され、NT AUTHORITY\SYSTEMデフォルトDACL ACEエントリのみが残されていることが確認されます。

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access           Apply To
                     Type     Rights
    --------------   -------  -------          -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. コマンドを使用して、セキュリティ記述子に1つ以上のDACLエントリを追加します `vserver security file-directory ntfs dacl add`。

   この例では、セキュリティ記述子に2つのDACL ACEを追加しています。

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. コマンドを使用して、セキュリティ記述子に1つ以上のSACLエントリを追加します `vserver security file-directory ntfs sacl add`。

   この例では、セキュリティ記述子に2つのSACL ACEを追加しています。

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. コマンドと `vserver security file-directory ntfs sacl show`コマンドを使用して、DACL ACEとSACL ACEがそれぞれ正しく設定されていることを確認します `vserver security file-directory ntfs dacl show。

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の DACL エントリに関する情報が表示されます。

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

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   この例では、次のコマンドを実行すると、セキュリティ記述子「`d1"」の SACL エントリに関する情報が表示されます。

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

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. コマンドを使用して、セキュリティポリシーを作成し `vserver security file-directory policy create`ます。

   次に、「 policy1 」という名前のポリシーを作成する例を示します。

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

7. コマンドを使用して、ポリシーが正しく設定されていることを確認します `vserver security file-directory policy show`。

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

   ```
      Vserver          Policy Name
      ------------     --------------
      vs1              policy1
   ```

8. コマンドでパラメータをに設定 `slag`して `-access-control`、セキュリティ記述子が関連付けられた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`。

   ポリシーには複数のストレージレベルのアクセス保護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。

   この例では ' セキュリティー記述子 "`d1" に割り当てられている "policy1 " という名前のポリシーにタスクが追加されますアクセス制御タイプが「`slag」に設定されたパスに割り当てられ `/datavol1`ます。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. コマンドを使用して、タスクが正しく設定されていることを確認します `vserver security file-directory policy task show`。

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. コマンドを使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用し `vserver security file-directory apply`ます。

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

    セキュリティポリシーを適用するジョブがスケジュールされます。

11. コマンドを使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認し `vserver security file-directory show`ます。

    この例では、コマンドの出力から、ストレージレベルのアクセス保護セキュリティがNTFSボリュームに適用されていることがわかります `/datavol1`。Everyoneにフルコントロールを許可するデフォルトのDACLは残っていますが、ストレージレベルのアクセス保護セキュリティは、ストレージレベルのアクセス保護設定で定義されたグループへのアクセスを制限（および監査）します。

    ```
    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

CLIを使用したSVMのNTFSファイルセキュリティ、NTFS監査ポリシー、ストレージレベルのアクセス保護の管理

ストレージレベルのアクセス保護の設定ワークフロー

ストレージレベルのアクセス保護に関する情報の表示

SLAGノテキヨウニカンスルマトリックス

SLAG は、ボリューム、 qtree 、またはその両方に対して設定できます。次の表に、さまざまな状況について、ボリュームまたは qtree に SLAG 構成を適用できるかどうかを示します。

	AFS 内のボリューム **SLAG**	**Snapshot** コピー内のボリューム **SLAG**	**AFS** 内の **qtree SLAG**	**Snapshot** コピー内の **qtree SLAG**
AFS 内のボリュームへのアクセス	はい	いいえ	N/A	N/A
Snapshot コピー内のボリュームへのアクセス	はい	いいえ	N/A	N/A
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されている場合）	いいえ	いいえ	はい	いいえ
AFS 内の qtree へのアクセス（ qtree に SLAG が設定されていない場合）	はい	いいえ	いいえ	いいえ
Snapshot コピー内の qtree へのアクセス（ qtree に SLAG が設定されている場合）	いいえ	いいえ	はい	いいえ
Snapshot コピー内の qtree へのアクセス（ qtree に SLAG が設定されていない場合）	はい	いいえ	いいえ	いいえ

ストレージレベルのアクセス保護に関する情報を表示する

ストレージレベルのアクセス保護は、ボリュームまたは qtree に適用される 3 番目のセキュリティレイヤです。ストレージレベルのアクセス保護設定は、 Windows のプロパティウィンドウでは表示できません。ストレージレベルのアクセス保護セキュリティに関する情報を表示するには、 ONTAP CLI を使用する必要があります。この情報を使用して、構成の検証や、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、およびストレージレベルのアクセス保護セキュリティ情報を表示するボリュームまたは qtree 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。

ステップ

1. ストレージレベルのアクセス保護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のパスにあるNTFSセキュリティ形式の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
```

次の例では、SVM vs1のパスにあるmixedセキュリティ形式のボリュームに関するストレージレベルのアクセス保護の情報を表示します `/datavol5`。こ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
                         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
```

ストレージレベルのアクセス保護の削除

ストレージレベルのアクセスセキュリティの設定が不要になった場合は、ボリュームや qtree からストレージレベルのアクセス保護を削除できます。ストレージレベルのアクセス保護を削除しても、通常の NTFS のファイルやディレクトリのセキュリティは変更されたり削除されたりしません。

手順

1. コマンドを使用して、ボリュームまたはqtreeにストレージレベルのアクセス保護が設定されていることを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. コマンドを使用して、ストレージレベルのアクセス保護を削除します `vserver security file-directory remove-slag`。

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. コマンドを使用して、ボリュームまたはqtreeからストレージレベルのアクセス保護が削除されたことを確認します `vserver security file-directory show`。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```