



CLIを使用したSMBの管理

ONTAP 9

NetApp
April 24, 2024

目次

CLIを使用したSMBの管理	1
SMB リファレンスの概要	1
SMB サーバのサポート	1
SMB サーバを管理します	9
SMB を使用したファイルアクセスをセットアップする	109
SMB を使用したファイルアクセスの管理	178
SMB クライアントベースのサービスを導入する	272
SMB サーバベースのサービスを導入	287
NFS と SMB のファイルとディレクトリの命名規則	355

CLIを使用したSMBの管理

SMB リファレンスの概要

SMB プロトコルで ONTAP ファイルアクセス機能を使用できます。CIFS サーバを有効にしたり、共有を作成したり、Microsoft サービスを有効にしたりできます。



SMB(Server Message Block) は、Common Internet File System (CIFS) プロトコルの最新のダイアレクトです。ONTAP コマンドラインインターフェイス（CLI）および OnCommand 管理ツールでは、_cifs_というメッセージが引き続き表示されます。

これらの手順は、次のような状況で使用する必要があります。

- ONTAP の SMB プロトコル機能の範囲について理解する必要がある。
- SMBの基本的な設定ではなく、あまり一般的でない設定タスクとメンテナンスタスクを実行する。
- System Manager や自動スクリプトツールではなく、コマンドラインインターフェイス（CLI）を使用する必要がある。

SMB サーバのサポート

SMB サーバのサポートの概要

Storage Virtual Machine（SVM）上で SMB サーバを有効にして設定し、SMB クライアントがクラスタ上のファイルにアクセスできるようにすることができます。

- クラスタ内のデータ SVM は、それぞれ 1 つの Active Directory ドメインにバインドできます。
- データ SVM は、必ずしも同じドメインにバインドする必要はありません。
- 複数の SVM を同じドメインにバインドできます。

SMB サーバを作成する前に、データの提供に使用する SVM と LIF を設定しておく必要があります。データネットワークがフラットでない場合は、IPspace、ブロードキャストドメイン、およびサブネットの設定も必要になることがあります。詳細については、『ネットワーク管理ガイド』を参照してください。

関連情報

["Network Management の略"](#)

[SMB サーバを変更](#)

["システム管理"](#)

サポートされる SMB のバージョンと機能

Server Message Block（SMB；サーバメッセージブロック）は、Microsoft Windows クライアントおよびサーバで使用されるリモートファイル共有プロトコルです。ONTAP 9 ではすべての SMB のバージョンがサポートされますが、デフォルトである SMB 1.0

がサポートされるかどうかは ONTAP のバージョンによって異なります。ONTAP SMB サーバが、ご使用の環境で必要なクライアントと機能をサポートしていることを確認する必要があります。

ONTAP がサポートする SMB クライアントおよびドメインコントローラの最新情報については、Interoperability Matrix Tool を参照してください。

SMB 2.0 以降のバージョンは ONTAP 9 の SMB サーバではデフォルトで有効になっており、必要に応じて有効または無効を切り替えることができます。次の表に、SMB 1.0 のサポートとデフォルト設定を示します。

SMB 1.0 の機能：	ONTAP 9 のリリース：			
	9.0	9.1	9.2.	9.3以降
はデフォルトで有効になっています	はい。	はい。	はい。	いいえ
有効または無効にすることができます	いいえ	はい * 9.1 P8 以降が必要です。	はい。	はい。



SMB 1.0 および 2.0 のドメインコントローラへの接続に関するデフォルト設定も ONTAP のバージョンによって異なります。詳細については、[vserver cifs security modify](#) のマニュアルページ。既存の CIFS サーバで SMB 1.0 を実行している環境では、できるだけ早く最新の SMB バージョンに移行して、セキュリティとコンプライアンスを強化する必要があります。詳細については、ネットアップの担当者にお問い合わせください。

次の表に、SMB でサポートされる機能と対応するバージョンを示します。SMB の機能には、デフォルトで有効になるものと追加の設定が必要なものがあります。

* この機能：	* 有効化が必要： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
		1.0	"2.0"	2.1	3.0	3.1.1
従来の SMB 1.0 の機能		X	X	X	X	X
永続性ハンド ル			X	X	X	X
複合操作			X	X	X	X
非同期操作			X	X	X	X

* この機能： *	* 有効化が必要 ： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
読み取り / 書き込みバッファのサイズが増加します			X	X	X	X
拡張性の向上			X	X	X	X
SMB 署名	X	X	X	X	X	X
代替データストリーム (ADS) ファイル形式	X	X	X	X	X	X
Large MTU (ONTAP 9.7 以降ではデフォルトで有効)	X			X	X	X
oplock リース				X	X	X
共有の継続的な可用性	X				X	X
永続的ハンドル					X	X
監視					X	X
SMB 暗号化： AES-128-CCM	X				X	X
スケールアウト (CA 共有で必要)					X	X
透過的なフェイルオーバー					X	X

* この機能： *	* 有効化が必要 ： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
SMB マルチチャネル（ ONTAP 9.4 以降）	X				X	X
事前認証の整合性						X
クラスタ・クライアント・フェイルオーバー v.2（ CCFv2）						X
SMB 暗号化： AES-128-GCM（ ONTAP 9.1 以降）	X					X

関連情報

[SMB 署名を使用したネットワークセキュリティの強化](#)

[SMBサーバの最小認証セキュリティレベルの設定](#)

[SMB を介したデータ転送での SMB サーバの SMB 暗号化要求の設定](#)

"[ネットアップテクニカルレポート 4543：『SMB Protocol Best Practices』](#)"

"[ネットアップの相互運用性](#)"

サポートされない **Windows** の機能

ネットワークで CIFS を使用する場合は、一部の Windows の機能が ONTAP ではサポートされないことに注意する必要があります。

ONTAP では、次の Windows 機能はサポートされません。

- Encrypted File System（EFS；暗号化ファイルシステム）
- 変更ジャーナルでの NT File System（NTFS）イベントのロギング
- Microsoft File Replication Service（FRS；ファイルレプリケーションサービス）
- Microsoft Windows インデックスサービス
- Hierarchical Storage Management（HSM；階層型ストレージ管理）経由のリモートストレージ

- Windows クライアントからのクォータ管理
- Windows のクォータのセマンティクス
- LMHOSTS ファイル
- NTFS のネイティブ圧縮機能です

SVM に NIS または LDAP ネームサービスを設定します

SMB アクセスでは、NTFS セキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIX ユーザへのユーザマッピングが常に行われます。NIS または LDAP ディレクトリストアにその情報が格納されている UNIX ユーザに Windows ユーザをマッピングする場合や、ネームマッピングに LDAP を使用する場合は、SMB のセットアップ時にこのネームサービスを設定する必要があります。

作業を開始する前に

ネームサービスデータベース設定をネームサービスインフラに合わせてカスタマイズしておく必要があります。

このタスクについて

SVM は、ネームサービス ns-switch データベースを使用して、指定されたネームサービスデータベースを検索するソースの順番を決定します。ns-switch ソースには、「files」、「nis」、または「ldap」を任意に組み合わせて使用できます。グループデータベースの場合、ONTAP は設定されたすべてのソースからグループメンバーシップを取得し、統合されたグループメンバーシップ情報をアクセスチェックに使用します。UNIX グループ情報の取得時にこれらのいずれかのソースを使用できないと、ONTAP は完全な UNIX クレデンシャルを取得できず、アクセスチェックが失敗することがあります。そのため、ns-switch 設定にグループデータベースのすべての ns-switch ソースが設定されていることを必ず確認する必要があります。

デフォルトでは、SMBサーバは、すべてのWindowsユーザをローカルに格納されているデフォルトのUNIXユーザにマッピングします passwd データベース：デフォルトの設定を使用する場合、SMB アクセスに対する、NIS または LDAP UNIX ユーザおよびグループのネームサービスまたは LDAP ユーザマッピングの設定は省略可能です。

手順

1. UNIX ユーザ、グループ、ネットグループ情報が NIS ネームサービスによって管理されている場合、NIS ネームサービスを次のように設定します。

- a. を使用して、ネームサービスの現在の順序を確認します `vserver services name-service ns-switch show` コマンドを実行します

この例では、3つのデータベースを示します (group、passwd、および netgroup) を使用できます `nis` ネームサービスソースがのみを使用している files 情報源として

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

を追加する必要があります `nis` を参照してください `group` および `passwd` データベース、およびオプションでにアクセスできます `netgroup` データベース：

- b. を使用して、ネームサービス `ns-switch` データベースを必要な順序で調整します `vserver services name-service ns-switch modify` コマンドを実行します

パフォーマンスを最大にするためには、SVM に設定する予定のないネームサービスデータベースにはネームサービスを追加しないでください。

複数のネームサービスデータベースの設定を変更する場合、変更するそれぞれのネームサービスデータベースに対して別々にコマンドを実行する必要があります。

この例では、`nis` および `files` は、のソースとして設定されています `group` および `passwd` この順番でデータベースを作成します。その他のネームサービスデータベースは変更されません。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. を使用して、ネームサービスの順序が正しいことを確認します `vserver services name-service ns-switch show` コマンドを実行します

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. NISネームサービス設定を作成します。+ vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+

```
vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60 -active true
```



ONTAP 9.2以降では、フィールドが表示されます -nis-servers フィールドを置き換えます -servers。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

- e. NISネームサービスが適切に設定され、アクティブになっていることを確認します。 vserver services name-service nis-domain show vserver vserver_name

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

2. UNIX ユーザ、グループ、ネットグループ情報またはネームマッピングが LDAP ネームサービスによって管理されている場合は、格納されている情報を使用して LDAP ネームサービスを設定します ["NFS の管理"](#)。

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます /etc/nsswitch.conf UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP ネームサービススイッチテーブルは、ONTAP が特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順番で参照するかを決定します。ONTAP では、SVM ごとに個別のネームサービススイッチテーブルが保持されます。

データベースタイプ

テーブルには、次の各データベースタイプについてネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます

データベースタイプ	ネームサービスソースの用途	有効なソース
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、 LDAP

ソースタイプ

ソースタイプによって、該当する情報を取得するために使用するネームサービスソースが決まります。

ソースタイプ	情報の検索先	使用するコマンド
ファイル	ローカルのソースファイル	<pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre>
NIS	SVM の NIS ドメイン設定で指定された外部の NIS サーバ	<pre>vserver services name- service nis-domain</pre>
LDAP	SVM の LDAP クライアント設定で指定された外部の LDAP サーバ	<pre>vserver services name- service ldap</pre>
DNS	SVM の DNS 設定で指定された外部の DNS サーバ	<pre>vserver services name- service dns</pre>

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります
files また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

ONTAP では、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例は、SVMのネームサービススイッチ設定を表示します `svm_1` :

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

ユーザまたはグループ情報の検索では、ONTAP はローカルのソースファイルだけを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカルネットグループファイルが照会されます。

SVM `svm_1` のテーブルには、ネームマッピング用のネームサービスエントリは含まれていません。そのため、ONTAP はデフォルトでローカルのソースファイルだけを参照します。

SMB サーバを管理します

SMB サーバを変更

を使用して、ワークグループからActive Directoryドメイン、ワークグループから別のワークグループ、またはActive DirectoryドメインからワークグループにSMBサーバを移動できます `vserver cifs modify` コマンドを実行します

このタスクについて

SMB サーバ名や管理ステータスなど、SMB サーバのその他の属性を変更することもできます。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。

選択肢

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。
 - SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- ワークグループから Active Directory ドメインに SMB サーバを移動するには、次の手順を実行します。 `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限があるWindowsアカウントの名前とパスワードを指定する必要があります `ou=example ou` 内のコンテナ `example.com` ドメイン。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、`keytab` ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

- ワークグループから別のワークグループに SMB サーバを移動します。

- a. SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. SMBサーバのワークグループを変更します。 `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Active Directory ドメインからワークグループに SMB サーバを移動するには、次の手順を実行します。

- a. SMBサーバの管理ステータスをに設定します `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Active DirectoryドメインからワークグループにSMBサーバを移動します。 `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



ワークグループモードに切り替えるには、継続的可用性を備えた共有、シャドウコピー、AES など、ドメインベースの機能をすべて無効にし、該当する設定がシステムによって自動的に削除されるようにする必要があります。ただし、「`EXAMPLE.COM\userName`」などのドメインで設定された共有 ACL は正しく機能しませんが、ONTAP で削除することはできません。このような共有 ACL は、コマンドの完了後できるだけ早く外部ツールを使用して削除してください。AES が有効になっている場合は、「`example.com`」ドメインで AES を無効にするための十分な権限を持つ Windows アカウントの名前とパスワードの入力を求められることがあります。

- の該当するパラメータを使用して、他の属性を変更します `vserver cifs modify` コマンドを実行します

オプションを使用した**SMB**サーバのカスタマイズ

使用できる **SMB** サーバオプション

SMB サーバのカスタマイズ方法について検討する場合は、使用できるオプションを把握しておくと便利です。一部のオプションは汎用的なものですが、SMB の特定の機能を有効にして設定するためのオプションも複数あります。SMBサーバオプションは、で制御します `vserver cifs options modify` オプション

以下に、admin 権限レベルで使用できる SMB サーバオプションについて説明します。

- * SMB セッションタイムアウト値の設定 *

このオプションでは、SMB セッションが切断されるまでのアイドル時間を秒数で指定できます。アイドルセッションとは、ユーザがクライアントでファイルもディレクトリも開いていないセッションのことです。デフォルト値は900秒です。

- * デフォルトの UNIX ユーザーの構成 *

このオプションでは、SMB サーバで使用されるデフォルトの UNIX ユーザを指定できます。ONTAP はデフォルトユーザ「pcuser」（UID は 65534）を自動的に作成し、グループ「pcuser」（GID は 65534）を作成して、デフォルトユーザを「pcuser」グループに追加します。SMB サーバを作成すると、ONTAP は自動的に「pcuser」をデフォルトの UNIX ユーザとして設定します。

- * ゲスト UNIX ユーザの設定 *

このオプションでは、信頼されていないドメインからログインしたユーザをマッピングする UNIX ユーザの名前を指定できます。これにより、信頼されていないドメインのユーザが SMB サーバに接続できるようになります。デフォルトでは、このオプションは設定されていません（デフォルト値はありません）。このため、信頼されていないドメインのユーザは SMB サーバへの接続を許可されません。

- * モードビットの読み取り権限付与の実行の有効化または無効化 *

このオプションを有効または無効にすると、UNIX 実行可能ビットが設定されていない場合でも、UNIX モードビットが設定された実行可能ファイルの実行を、ファイルへの読み取り権限を持つ SMB クライアントに許可するかどうかを指定できます。このオプションは、デフォルトでは無効になっています。

- * NFS クライアントからの読み取り専用ファイルの削除機能の有効化または無効化 *

このオプションを有効または無効にすると、読み取り専用属性が設定されたファイルやフォルダの削除を NFS クライアントに許可するかどうかを指定できます。NTFS の削除では、読み取り専用属性が設定されたファイルやフォルダの削除は許可されません。UNIX の削除では読み取り専用ビットが無視され、ファイルやフォルダを削除できるかどうかは親ディレクトリの権限によって判断されます。デフォルト設定はです `disabled` これにより、NTFS の削除セマンティクスが発生します。

- * Windows Internet Name Service サーバーアドレスの設定 *

このオプションでは、複数の Windows Internet Name Service（WINS）サーバアドレスをカンマで区切って指定できます。IPv4 アドレスを指定する必要があります。IPv6 アドレスはサポートされません。デフォルト値はありません。

以下に、advanced 権限レベルで使用できる SMB サーバオプションについて説明します。

- * CIFS ユーザーへの UNIX グループ権限の付与 *

このオプションは、ファイルの所有者ではない CIFS ユーザーにグループ権限を付与するかどうかを指定します。CIFSユーザーがUNIXセキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `true` をクリックすると、ファイルに対するグループ権限が付与されます。CIFSユーザーがUNIXセキュリティ形式のファイルの所有者ではない場合に、このパラメータがに設定されます `false` を指定すると、通常のUNIXルールを適用してファイル権限が付与されます。このパラメータは、権限がに設定されているUNIXセキュリティ形式のファイルに適用されます `mode bits` セキュリティモードがNTFSまたはNFSv4のファイルには適用されません。デフォルト設定は `false`。

- * SMB 1.0 の有効化または無効化 *

ONTAP 9.3 で SMB サーバが作成された SVM では、SMB 1.0 がデフォルトで無効になります。



ONTAP 9.3 以降では、ONTAP 9.3 で新しく作成された SMB サーバについては SMB 1.0 がデフォルトで無効になります。できるだけ早く最新の SMB バージョンに移行して、セキュリティとコンプライアンスを強化してください。詳細については、ネットアップの担当者にお問い合わせください。

- * SMB 2.x の有効化または無効化 *

SMB 2.0 は、LIF フェイルオーバーをサポートする SMB の最小バージョンです。SMB 2.x を無効にした場合、ONTAP では SMB 3.x も自動的に無効になります

SMB 2.0 は SVM でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * SMB 3.0の有効化または無効化*

SMB 3.0 は、継続的可用性を備えた共有をサポートする SMB の最小バージョンです。Windows Server 2012 および Windows 8 は、SMB 3.0 をサポートする Windows の最小バージョンです。

SMB 3.0はSVMでのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * SMB 3.1 を有効または無効にします

Windows 10 は、SMB 3.1 をサポートする Windows の唯一のバージョンです。

SMB 3.1はSVMでのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * ODX コピーオフロードの有効化または無効化 *

ODX コピーオフロードは、対応する Windows クライアントで自動的に使用されます。このオプションはデフォルトで有効になっています。

- * ODX コピーオフロードの直接コピーメカニズムの有効化または無効化 *

直接コピーメカニズムは、コピー中のファイル変更を禁止するモードで Windows クライアントがコピー元のファイルを開こうとした場合に、コピーオフロード処理のパフォーマンスを向上させます。デフォルトでは、直接コピーメカニズムは有効になっています。

- * 自動ノードリファラルの有効化または無効化 *

自動ノードリファールでは、SMB サーバはクライアントに対して、要求した共有を介してアクセスするデータのホストノードに対してローカルなデータ LIF を自動的に参照することになります。

- * SMB * のエクスポート・ポリシーの有効化または無効化

このオプションは、デフォルトでは無効になっています。

- * ジャンクションポイントのリパースポイントとしての使用の有効化または無効化 *

このオプションを有効にすると、SMB サーバはジャンクションポイントをリパースポイントとして SMB クライアントに公開します。このオプションは、SMB 2.x 接続または SMB 3.0 接続のみで有効です。このオプションはデフォルトで有効になっています。

このオプションは SVM でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * TCP 接続ごとの最大同時操作数の設定 *

デフォルト値は255です。

- * ローカルの Windows ユーザーとグループ機能の有効化または無効化 *

このオプションはデフォルトで有効になっています。

- * ローカル Windows ユーザー認証の有効化または無効化 *

このオプションはデフォルトで有効になっています。

- * VSS シャドウ・コピー機能の有効化または無効化 *

ONTAP では、シャドウコピー機能によって、Hyper-V over SMB 解決策を使用して格納されたデータのリモートバックアップを実行します。

このオプションは、SVM、および Hyper-V over SMB 構成でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * シャドウ・コピーのディレクトリ階層の設定 *

このオプションでは、シャドウコピー機能を使用するときに、シャドウコピーを作成するディレクトリの最大階層を定義できます。

このオプションは、SVM、および Hyper-V over SMB 構成でのみサポートされます。このオプションは、SVM ではデフォルトで有効になります

- * マルチドメインネームマッピングの検索機能の有効化または無効化 *

有効にすると、UNIX ユーザが Windows ユーザ名のドメイン部分にワイルドカード (*) を使用して Windows ドメインユーザにマッピングされている場合に (* \joe など)、ONTAP 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、指定したユーザを検索します。ホームドメインとは、SMB サーバのコンピュータアカウントが含まれるドメインです。

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。このオプションを有効にして、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ために優先リストが使用されます。

デフォルトでは、マルチドメインネームマッピングの検索は有効になります。

- * ファイルシステムセクターサイズの設定 *

このオプションでは、ONTAP から SMB クライアントに報告されるファイルシステムセクターサイズをバイト単位で設定できます。このオプションには2つの有効な値があります。4096 および 512。デフォルト値はです 4096。この値をに設定する必要がある場合があります 512 Windowsアプリケーションが512バイトのセクターサイズのみをサポートしている場合。

- * ダイナミックアクセス制御の有効化または無効化 *

このオプションを有効にすると、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や、グループポリシーオブジェクトを使用した集約型アクセスポリシーの実装を含めて、ダイナミックアクセス制御を使用して SMB サーバのオブジェクトを保護できます。このオプションは、デフォルトでは無効になっています。

このオプションは SVM でのみサポートされます。

- * 認証されていないセッションのアクセス制限の設定 (restrict anonymous) *

このオプションでは、認証されていないセッションのアクセス制限を指定します。制限は匿名ユーザに適用されます。デフォルトでは、匿名ユーザに対するアクセス制限はありません。

- * UNIX 対応のセキュリティを使用するボリューム (UNIX セキュリティ形式のボリューム、または UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム) での NTFS ACL の提供を有効または無効にする *

このオプションを有効または無効にして、UNIX セキュリティ形式のファイルやフォルダのファイルセキュリティが SMB クライアントに表示される方法を指定します。有効 ONTAP にすると、UNIX 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は、NTFS ACL を使用する NTFS ファイルセキュリティが設定されたファイルやフォルダとして SMB クライアントに表示されます。無効 ONTAP にすると、UNIX セキュリティ形式のボリュームは、ファイルセキュリティのない FAT ボリュームとして表示されます。デフォルトでは、ボリュームは NTFS ACL を使用する NTFS ファイルセキュリティが設定されたボリュームとして表示されます。

- * SMB 擬似オープン機能の有効化または無効化 *

この機能を有効にすると、ONTAP がファイルやディレクトリの属性情報を照会する際のオープン要求とクローズ要求の方法が最適化されて、SMB 2.x および SMB 3.0 のパフォーマンスが向上します。デフォルトでは、SMB 擬似オープン機能は有効になっています。このオプションは、SMB 2.x 以降を使用する接続にのみ有効です。

- * UNIX 拡張の有効化または無効化 *

このオプションを有効にすると、SMB サーバで UNIX 拡張が有効になります。UNIX 拡張を使用すると、SMB プロトコルを介して POSIX/UNIX 形式のセキュリティを表示できます。デフォルトでは、このオプションは無効になっています。

Mac OSX クライアントなど、UNIX ベースの SMB クライアントが環境内にある場合は、UNIX 拡張を有効にしてください。UNIX 拡張を有効にすると、SMB サーバは POSIX/UNIX セキュリティ情報を SMB 経由で UNIX ベースのクライアントに送信できるようになります。クライアントは、受け取ったセキュリティ情報を POSIX/UNIX セキュリティに変換します。

• * 略称を使用した検索のサポートの有効化または無効化 *

このオプションを有効にすると、SMB サーバは短縮名に対して検索を実行できます。このオプションを有効にした場合の検索では、長いファイル名に加えて 8.3 形式のファイル名も照合されます。このパラメータのデフォルト値は `false`。

• * DFS 対応の自動通知のサポートの有効化または無効化 *

このオプションを有効または無効にして、共有に接続する SMB 2.x および SMB 3.0 クライアントに SMB サーバから DFS 対応を自動的に通知するかどうかを指定します。ONTAP では、SMB アクセス用のシンボリックリンクの実装で DFS リファールが使用されます。有効にすると、シンボリックリンクアクセスが有効かどうかに関係なく、SMB サーバは常に DFS 対応を通知します。無効にすると、シンボリックリンクアクセスが有効になっている共有にクライアントが接続する場合にのみ、SMB サーバは DFS 対応を通知します。

• * SMB クレジットの最大数の設定 *

ONTAP 9.4以降ではを設定します `-max-credits` オプションを使用すると、クライアントとサーバがSMBバージョン2以降を実行している場合に、SMB接続に付与するクレジットの数を制限できます。デフォルト値は128です。

• * SMB マルチチャネルのサポートの有効化または無効化 *

を有効にします `-is-multichannel-enabled` ONTAP 9.4以降のリリースのオプションを使用すると、クラスタとそのクライアントに適切なNICが導入されている場合に、SMBサーバは単一のSMBセッションに対して複数の接続を確立できます。これにより、スループットとフォールトトレランスが向上します。このパラメータのデフォルト値は `false`。

SMB マルチチャネルが有効な場合、次のパラメータも指定できます。

- 各マルチチャネルセッションに許可される最大接続数。このパラメータのデフォルト値は 32 です。
- 各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。このパラメータのデフォルト値は256です。

SMBサーバオプションの設定

SMBサーバオプションは、Storage Virtual Machine (SVM) でのSMBサーバの作成後にいつでも設定できます。

ステップ

1. 必要な操作を実行します。

SMBサーバオプションの設定	入力するコマンド
admin 権限レベルで設定します	<pre>vserver cifs options modify -vserver vserver_name options</pre>

SMBサーバオプションの設定	入力するコマンド
advanced 権限レベルで設定します	a. <code>set -privilege advanced</code> b. <code>vserver cifs options modify -vserver vserver_name options</code> c. <code>set -privilege admin</code>

SMBサーバオプションの設定の詳細については、のマニュアルページを参照してください `vserver cifs options modify` コマンドを実行します

SMBユーザへのUNIXグループ権限付与の設定

このオプションを使用すると、ファイルの所有者でない SMB ユーザもファイルやディレクトリにアクセスする権限をグループに付与することができます。

手順

1. 権限レベルを `advanced` に設定します。 `set -privilege advanced`
2. UNIX グループ権限付与を必要に応じて設定します。

状況	入力するコマンド
ユーザがファイルの所有者でない場合にもファイルやディレクトリにアクセスするためのグループ権限を付与する	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
ユーザがファイルの所有者でない場合はファイルやディレクトリにアクセスするためのグループ権限を付与しないようにします	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. `admin` 権限レベルに戻ります。 `set -privilege admin`

匿名ユーザのアクセス制限を設定します

デフォルトでは、認証されていない匿名ユーザ（`_null` ユーザ）はネットワーク上の特定の情報にアクセスできます。SMBサーバオプションを使用して、匿名ユーザに対するアクセス制限を設定できます。

このタスクについて

。 `-restrict-anonymous` SMBサーバオプションはに対応します `RestrictAnonymous` Windowsのレジストリエントリ。

匿名ユーザは、ユーザ名、詳細、アカウントポリシー、共有名など、ネットワーク上の Windows ホストから特定のタイプのシステム情報をリストまたは列挙できます。次の 3 つのうち、いずれかのアクセス制限設定を指定して、匿名ユーザのアクセスを制御することができます。

価値	説明
no-restriction (デフォルト)	匿名ユーザにアクセス制限を設定しません。
no-enumeration	匿名ユーザに対して列挙だけを制限します。
no-access	匿名ユーザに対してアクセスを制限します。

手順

1. 権限レベルを `advanced` に設定します。 `set -privilege advanced`
2. `restrict anonymous`を設定します。 `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
4. `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

UNIX セキュリティ形式のデータに対するファイルセキュリティの **SMB** クライアントへの提供方法を管理します

UNIX セキュリティ形式のデータの概要で、ファイルセキュリティが **SMB** クライアントにどのように提供されるかを管理します

SMB クライアントへの NTFS ACL の提供を有効または無効にすることによって、UNIX セキュリティ形式のデータに対するファイルセキュリティの SMB クライアントへの提供方法を選択できます。それぞれの設定には利点があり、ビジネス要件に最適な設定を選択するために理解しておく必要があります。

デフォルトでは、ONTAP は、UNIX セキュリティ形式のボリュームに対する UNIX アクセス権を NTFS ACL として SMB クライアントに提供します。これは次のような場合に適しています。

- Windows の [プロパティ] ボックスの [セキュリティ *] タブを使用して、UNIX アクセス権を表示および編集する。

処理が UNIX システムで許可されていない場合、Windows クライアントからアクセス権を変更することはできません。たとえば、所有していないファイルの所有権を変更することはできません。これは、UNIX システムではこの処理が許可されていないためです。この制限により、SMB クライアントは、ファイルやフォルダに対して設定された UNIX アクセス権をバイパスできないようになっています。

- ユーザは、Microsoft Office などの特定の Windows アプリケーションを使用して UNIX セキュリティ形式のボリューム上でファイルを編集および保存します。ONTAP では、保存処理中に UNIX アクセス権を保持する必要があります。
- 使用するファイルの NTFS ACL を読み取ることを想定した特定の Windows アプリケーションが環境にある場合。

状況によっては、NTFS ACL としての UNIX アクセス権の提供を無効にすることもできます。この機能を無効にすると、ONTAP は UNIX セキュリティ形式のボリュームを FAT ボリュームとして SMB クライアントに提供します。UNIX セキュリティ形式のボリュームを FAT ボリュームとして SMB クライアントに提供するの、次のような場合です。

- UNIX アクセス権の変更は、マウントを使用して UNIX クライアントでのみ行うことができます。

SMB クライアントで UNIX セキュリティ形式のボリュームがマッピングされている場合は、Security タブを使用できません。マッピングされたドライブは、ファイル権限がない FAT ファイルシステムでフォーマットされたドライブとして表示されます。

- SMB を使用するアプリケーションでアクセスするファイルやフォルダに NTFS ACL を設定しており、データが UNIX セキュリティ形式のボリュームにあると失敗する可能性がある場合。

ONTAP がボリュームを FAT として報告する場合、アプリケーションは ACL の変更を試みません。

関連情報

FlexVol でのセキュリティ形式の設定

qtree でのセキュリティ形式の設定

UNIX セキュリティ形式のデータに対する **NTFS ACL** の提供を有効または無効にします

UNIX セキュリティ形式のデータ（UNIX セキュリティ形式のボリュームと UNIX 対応のセキュリティを使用する mixed セキュリティ形式のボリューム）に対する NTFS ACL の SMB クライアントへの提供を有効または無効にできます。

このタスクについて

このオプションを有効にすると、ONTAP は、UNIX 対応のセキュリティ形式を使用するボリュームのファイルおよびフォルダを NTFS ACL を使用するように SMB クライアントに提供します。このオプションを無効にした場合は、ボリュームが SMB クライアントに FAT ボリュームとして提供されます。デフォルトでは、NTFS ACL が SMB クライアントに提供されます。

手順

1. 権限レベルを advanced に設定します。set -privilege advanced
2. UNIX NTFS ACL オプションを設定します。vserver cifs options modify -vserver `vserver_name` -is-unix-nt-acl-enabled {true|false}
3. オプションが目的の値に設定されていることを確認します。vserver cifs options show -vserver `vserver_name`
4. admin 権限レベルに戻ります。set -privilege admin

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

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て **UNIX** アクセス権を管理します

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。

SMB サーバのセキュリティ設定を管理します

ONTAP による **SMB** クライアント認証の処理

SMB接続を確立してSVMに格納されているデータにアクセスする前に、ユーザはSMBサーバが属しているドメインで認証される必要があります。SMBサーバでは、Kerberos とNTLM（NTLMv1またはNTLMv2）の2つの認証方式がサポートされます。ドメインユーザの認証に使用されるデフォルトの方法は Kerberos です。

Kerberos 認証

ONTAP は、許可された SMB セッションの作成時に Kerberos 認証をサポートします。

Kerberos は Active Directory のプライマリ認証サービスです。Kerberos サーバの Kerberos Key Distribution Center（KDC；キー配布センター）サービスは、Active Directory に対してセキュリティプリンシパルに関する情報の格納や取得を行います。NTLM モデルとは異なり、SMB サーバなどの別のコンピュータとのセッションを確立する Active Directory クライアントは、直接 KDC にアクセスしてセッションのクレデンシャルを取得します。

NTLM認証

NTLM クライアント認証は、パスワードに基づくユーザ固有のシークレットを共有し、チャレンジ - 応答プロトコルを使用して行われます。

ユーザがローカルの Windows ユーザアカウントを使用して SMB 接続を作成した場合、認証は SMB サーバによって NTLMv2 を使用してローカルに行われます。

SVM ディザスタリカバリ構成での SMB サーバセキュリティ設定に関するガイドライン

ID が保持されないディザスタリカバリデスティネーションとして設定された SVM を作成する前に（を参照）`-identity-preserve` オプションはに設定されています `false`（SnapMirror 構成の場合）デスティネーション SVM での SMB サーバセキュリティ設定の管理方法について理解しておく必要があります。

- デフォルト以外の SMB サーバセキュリティ設定はデスティネーションにレプリケートされません。

デスティネーション SVM 上に SMB サーバを作成した場合、すべての SMB サーバセキュリティ設定はデフォルト値に設定されます。SVM のディザスタリカバリ先を初期化、更新、再同期した場合、ソース上の SMB サーバのセキュリティ設定はデスティネーションにレプリケートされません。

- デフォルト以外の SMB サーバセキュリティ設定は手動で設定する必要があります。

ソース SVM 上で SMB サーバセキュリティ設定をデフォルト以外にしている場合、デスティネーションが読み書き可能になったあと（SnapMirror 関係が解除されたあと）にデスティネーション SVM 上で手動で同じ設定を行う必要があります。

SMB サーバのセキュリティ設定に関する情報を表示する

Storage Virtual Machine（SVM）上の SMB サーバセキュリティ設定に関する情報を表示できます。この情報は、セキュリティ設定が正しいかどうかを確認する際に役立ちます。

このタスクについて

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値か、ONTAP CLI または Active Directory グループポリシーオブジェクト（GPO）を使用して設定されたデフォルト以外の値です。

を使用しないでください `vserver cifs security show` 一部のオプションが無効なため、ワークグループモードの SMB サーバに対してコマンドを実行します。

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
指定した SVM のすべてのセキュリティ設定	<code>vserver cifs security show -vserver vserver_name</code>
SVM の特定のセキュリティ設定	<code>vserver cifs security show -vserver vserver_name -fields [fieldname,...]</code> 入ることができます -fields ? 使用できるフィールドを決定します。

例

次の例は、SVM vs1 のすべてのセキュリティ設定を表示します。

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 5 minutes
Kerberos Ticket Age: 10 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
Client Session Security: none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

表示される設定は、実行中の ONTAP のバージョンによって異なります。

次の例は、SVM vs1 の Kerberos のクロックスキューを表示します。

```
cluster1::> vsriver cifs security show -vsriver vs1 -fields kerberos-  
clock-skew
```

```
vsriver kerberos-clock-skew  
-----  
vs1      5
```

関連情報

GPO 設定に関する情報を表示します

ローカル **SMB** ユーザに対するパスワードの複雑さの要件を有効または無効にします

パスワードの複雑さの要件を有効にすると、Storage Virtual Machine（SVM）上のローカル SMB ユーザに対するセキュリティを強化できます。パスワードの複雑さの要件はデフォルトでは有効になっています。この機能は、いつでも無効にして再度有効にすることができます。

作業を開始する前に

CIFS サーバでローカルユーザ、ローカルグループ、およびローカルユーザ認証が有効になっている必要があります。



このタスクについて

を使用しないでください vsriver cifs security modify 一部のオプションが無効なため、ワークグループモードのCIFSサーバに対してコマンドを実行します。

手順

1. 次のいずれかを実行します。

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設定	入力するコマンド
有効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-password-complexity -required true</pre>
無効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-password-complexity -required false</pre>

2. パスワードの複雑さの要件に関するセキュリティ設定を確認します。 vsriver cifs security show -vsriver vsriver_name

例

次の例は、SVM vs1 のローカル SMB ユーザに対してパスワードの複雑さの要件を有効にします。


```
cluster1::> vsriver cifs security modify -vsriver vs1 -is-password
-complexity-required true

cluster1::> vsriver cifs security show -vsriver vs1 -fields is-password-
complexity-required
vsriver is-password-complexity-required
-----
vs1      true
```

関連情報

[CIFS サーバのセキュリティ設定に関する情報を表示する](#)

[ローカルユーザおよびローカルグループを使用した認証と許可](#)

[ローカルユーザパスワードの要件](#)

[ローカルユーザのアカウントパスワードを変更しています](#)

CIFS サーバの **Kerberos** セキュリティ設定を変更します

Kerberos クロックスキュー時間の許容最大値、Kerberos チケットの有効期間、チケットの更新日の最大数など、CIFS サーバの Kerberos セキュリティ設定の一部を変更できます。

このタスクについて

を使用したCIFSサーバのKerberos設定の変更 vsriver cifs security modify コマンドでは、で指定した単一のStorage Virtual Machine (SVM) の設定のみを変更できます -vsriver パラメータActive Directory の Group Policy Object (GPO ; グループポリシーオブジェクト) を使用すると、同一の Active Directory ドメインに属するクラスタ上の SVM すべてについて、Kerberos セキュリティ設定を集中管理できます。

手順

1. 次の操作を 1 つ以上実行します。

状況	入力するコマンド
Kerberosクロックスキューの許容最大時間を分（9.13.1以降）または秒（9.12.1以前）で指定します。	<pre>vsriver cifs security modify -vsriver vsriver_name -kerberos-clock-skew integer_in_minutes</pre> <p>デフォルトの設定は 5 分です。</p>
Kerberos チケットの有効期間を時間で指定します。	<pre>vsriver cifs security modify -vsriver vsriver_name -kerberos-ticket-age integer_in_hours</pre> <p>デフォルトの設定は 10 時間です。</p>

チケットの更新日の最大数を指定します。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>デフォルトの設定は 7 日です。</p>
KDC のソケットのタイムアウトを指定します。この時間を過ぎるとすべての KDC が到達不能とマークされます。	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>デフォルトの設定は 3 秒です。</p>

2. Kerberos セキュリティ設定を確認します。

```
vserver cifs security show -vserver vserver_name
```

例

次の例では、SVM vs1 の Kerberos セキュリティ設定を「Kerberos Clock Skew」に 3 分、「Kerberos Ticket Age」に 8 時間に変更しています。

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew: 3 minutes
Kerberos Ticket Age: 8 hours
Kerberos Renewal Age: 7 days
Kerberos KDC Timeout: 3 seconds
Is Signing Required: false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled: false
LM Compatibility Level: lm-ntlm-ntlmv2-krb
Is SMB Encryption Required: false
```

関連情報

["CIFS サーバのセキュリティ設定に関する情報を表示する"](#)

["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"](#)

SMBサーバの最小認証セキュリティレベルを設定する

SMB サーバの *LMCompatibilityLevel* と呼ばれる SMB サーバの最小セキュリティレベルを設定することで、SMB クライアントアクセスのビジネスセキュリティ要件を満たすことができます。最小セキュリティレベルは、SMBサーバによって許可されるSMBクライアントからのセキュリティトークンの最小レベルです。



このタスクについて

- ワークグループモードのSMBサーバでは、NTLM認証のみがサポートされます。Kerberos 認証はサポートされません。
- LMCompatibilityLevel は SMB クライアント認証にのみ適用され、admin 認証には適用されません。

最低限の認証セキュリティレベルは、サポートされている 4 つのセキュリティレベルのうちの 1 つに設定することができます。

価値	説明
lm-ntlm-ntlmv2-krb (デフォルト)	Storage Virtual Machine (SVM) は、LM、NTLM、NTLMv2、Kerberos 認証セキュリティを許可します。
ntlm-ntlmv2-krb	SVM は、NTLM、NTLMv2、Kerberos 認証セキュリティを許可します。SVM は LM 認証を拒否します。
ntlmv2-krb	SVM は、NTLMv2 と Kerberos 認証セキュリティを許可します。SVM は LM と NTLM 認証を拒否します。
krb	SVM は、Kerberos 認証セキュリティのみを許可します。SVM は LM、NTLM、NTLMv2 認証を拒否します。

手順

1. 最小認証セキュリティレベルを設定します。vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}
2. 認証セキュリティレベルが目的のレベルに設定されていることを確認します。vserver cifs security show -vserver vserver_name

関連情報

[Kerberos ベースの通信用の AES 暗号化を有効または無効にします](#)

AES 暗号化を使用して **Kerberos** ベースの通信のセキュリティを強化できます

Kerberos ベースの通信による最も強固なセキュリティを実現するために、AES-256 暗

号化と AES-128 暗号化を SMB サーバで有効にすることができます。デフォルトでは、SMBでのSMBサーバの作成時にAdvanced Encryption Standard (AES) 暗号化は無効になっています。AES暗号化が提供する強固なセキュリティを活用するには、AES暗号化を有効にする必要があります。

SMB の Kerberos 関連の通信は、SVM で SMB サーバを作成する際や、SMB セッションの設定フェーズで使用されます。SMB サーバでは、Kerberos 通信で次の暗号化タイプがサポートされます。

- AES 256
- AES 128
- DES (デス
- RC4-HMAC

Kerberos 通信で最高のセキュリティを持つ暗号化タイプを使用する場合は、SVM の Kerberos 通信で AES 暗号化を有効にする必要があります。

SMB サーバを作成すると、ドメインコントローラによって Active Directory にコンピュータマシンアカウントが作成されます。この時点で、KDC は特定のマシンアカウントの暗号化機能を認識するようになります。その後、認証時にクライアントがサーバに提示するサービスチケットを暗号化するために、特定の暗号化タイプが選択されます。

ONTAP 9.12.1以降では、Active Directory (AD) KDCにアドバタイズする暗号化タイプを指定できます。を使用できます `-advertised-enc-types` 推奨される暗号化タイプを有効にするオプション。また、弱い暗号化タイプを無効にする場合にも使用できます。方法をご確認ください["Kerberosベースの通信の暗号化タイプを有効または無効にします"](#)。



SMB 3.0 で利用可能な Intel AES New Instructions (Intel AES NI) は AES アルゴリズムの改良版で、サポート対象のプロセッサファミリーでのデータ暗号化処理を高速化します。SMB 3.1.1 以降では、SMB 暗号化で使用されるハッシュアルゴリズムとして AES-128-CCM に代わって AES-128-GCM が使用されます。

関連情報

[CIFS サーバの Kerberos セキュリティ設定の変更](#)

Kerberos ベースの通信用の **AES** 暗号化を有効または無効にします

Kerberosベースの通信で最も強力なセキュリティを活用するには、SMBサーバでAES-256暗号化とAES-128暗号化を使用する必要があります。ONTAP 9.13.1以降では、AES暗号化がデフォルトで有効になります。Active Directory (AD) KDC との Kerberos ベースの通信に AES 暗号化タイプを SMB サーバで選択したくない場合は、AES 暗号化を無効にすることができます。

AES暗号化がデフォルトで有効になっているかどうか、および暗号化タイプを指定できるかどうかは、ONTAPのバージョンによって異なります。

ONTAPバージョン	AES暗号化が有効になっている...	暗号化タイプを指定できますか。
9.13.1以降	デフォルトでは	はい。

ONTAPバージョン	AES暗号化が有効になっている...	暗号化タイプを指定できますか。
9.12.1:	手動で実行する	はい。
9.11.1以前	手動で実行する	いいえ

ONTAP 9.12.1以降では、を使用してAES暗号化を有効または無効にします `-advertised-enc-types` オプション。AD KDCにアドバタイズする暗号化タイプを指定できます。デフォルト設定は `rc4` および `des`、ただし、AESタイプを指定すると、AES暗号化が有効になります。オプションを使用して、弱いRC4暗号化タイプとDES暗号化タイプを明示的に無効にすることもできます。ONTAP 9.11.1以前では、`-is-aes-encryption-enabled` AES暗号化を有効または無効にするオプションを指定できません。また、暗号化タイプは指定できません。

セキュリティを強化するため、Storage Virtual Machine（SVM）はAESセキュリティオプションが変更されるたびに、AD内のマシンアカウントのパスワードを変更します。パスワードの変更には、マシンアカウントが含まれる組織単位（OU）の管理ADクレデンシャルが必要になることがあります。

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（`-identity-preserve` オプションはに設定されています `false` SnapMirrorの設定では、デフォルト以外のSMBサーバセキュリティ設定はデスティネーションにレプリケートされません。ソースSVMでAES暗号化を有効にした場合は、AES暗号化を手動で有効にする必要があります。

例 1. 手順

ONTAP 9.12.1以降

1. 次のいずれかを実行します。

Kerberos 通信の AES 暗号化タイプの設定	入力するコマンド
有効	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
無効	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

注： `-is-aes-encryption-enabled` オプションはONTAP 9.12.1では廃止され、以降のリリースでは削除される可能性があります。

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver   advertised-enc-types
-----
vs1       aes-128,aes-256
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMB サーバを含む OU の管理 AD クレデンシャルを入力するように求められます。

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

ONTAP 9.11.1以前

1. 次のいずれかを実行します。

Kerberos 通信の AES 暗号化タイプの設定	入力するコマンド
有効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
無効	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vsriver cifs security show -vsriver vsriver_name -fields is-aes-encryption-enabled`

。 `is-aes-encryption-enabled` フィールドが表示されます `true` AES暗号化が有効になっている場合と `false` 無効になっている場合。

例

次の例は、SVM vs1のSMBサーバでAES暗号化タイプを有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs1      true
```

次の例は、SVM vs2のSMBサーバでAES暗号化タイプを有効にします。管理者は、SMB サーバを含む OU の管理 AD クレデンシャルを入力するように求められます。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs2      true
```

SMB 署名を使用してネットワークのセキュリティを強化します

SMB 署名を使用してネットワークセキュリティの概要を強化します

SMB 署名は、リプレイアタックを防止することで、SMB サーバとクライアント間のネットワークトラフィックが危険にさらされることのないようにします。デフォルト ONTAP では、クライアントから要求されたときに SMB 署名がサポートされます。ストレージ管理者は、必要に応じて、SMB 署名を必須にするように SMB サーバを設定できます。

CIFS サーバの SMB 署名セキュリティ設定に加えて、クライアントと CIFS サーバ間の通信のデジタル署名を制御する Windows クライアント上の SMB 署名ポリシーが 2 つあります。ビジネス要件に合わせて設定を行うことができます。

クライアント SMB ポリシーは、Microsoft 管理コンソール（MMC）または Active Directory の GPO を使用して設定した Windows ローカルセキュリティポリシー設定で制御されます。クライアントの SMB 署名とセキュリティ問題の詳細については、Microsoft Windows のマニュアルを参照してください。

ここでは、Microsoft クライアントの 2 つの SMB 署名ポリシーについて説明します。

- Microsoft network client: Digitally sign communications (if server agrees)

この設定は、クライアントの SMB 署名機能を有効にするかどうかを制御します。デフォルトでは有効になっています。この設定をクライアントで無効にすると、クライアントの CIFS サーバとの通信は、CIFS サーバ上の SMB 署名の設定によって異なります。

- Microsoft network client: Digitally sign communications (always)

この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。デフォルトでは無効になっています。この設定がクライアントで無効になっている場合、SMB署名の動作はのポリシー設定に基づきます Microsoft network client: Digitally sign communications (if server agrees) およびCIFSサーバの設定。



ご使用の環境に、SMB 署名を必要とするように設定された Windows クライアントが含まれる場合、CIFS サーバ上の SMB 署名を有効にする必要があります。有効にしないと、CIFS サーバはこれらのシステムにデータを提供できません。

クライアントと CIFS サーバの SMB 署名設定の有効な結果は、SMB セッションで SMB 1.0 が使用されるか SMB 2.x 以降が使用されるかによって異なります。

次の表に、セッションで SMB 1.0 が使用される場合の有効な SMB 署名の動作を示します。

クライアント	ONTAP — 署名は不要	ONTAP — 署名が必要
署名は無効になっており、不要です	署名されません	署名
署名が有効になっており、不要である	署名されません	署名
署名が無効になっており、必要です	署名	署名
署名が有効になっており、必要です	署名	署名



古いバージョンの Windows の SMB 1 クライアントや一部の Windows 以外の SMB 1 クライアントでは、署名がクライアントでは無効になっていて CIFS サーバでは必要な場合、接続に失敗することがあります。

次の表に、セッションで SMB 2.x または SMB 3.0 が使用される場合の有効な SMB 署名の動作を示します。



SMB 2.x クライアントと SMB 3.0 クライアントでは、SMB 署名は常に有効になります。無効にすることはできません。

クライアント	ONTAP — 署名は不要	ONTAP — 署名が必要
署名は不要です	署名されません	署名
署名が必要です	署名	署名

次の表に、Microsoft クライアントおよびサーバの SMB 署名のデフォルト動作を示します。

プロトコル	ハッシュアルゴリズム	有効 / 無効を切り替えられます	必須 / 不要	クライアントのデフォルト	サーバのデフォルト	DC のデフォルト
SMB 1.0	MD5	はい。	はい。	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい。	必要ありません	必要ありません	必須
SMB 3.0	AES-CMAC :	いいえ	はい。	必要ありません	必要ありません	必須



Microsoftではの使用を推奨していません Digitally sign communications (if client agrees) または Digitally sign communications (if server agrees) グループポリシーの設定。Microsoftでは、の使用も推奨していません EnableSecuritySignature レジストリ設定。これらのオプションはSMB 1の動作にのみ影響し、で置き換えることができます Digitally sign communications (always) グループポリシー設定または RequireSecuritySignature レジストリ設定。詳細については、Microsoftのブログを参照してください。 <http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The SMB署名の基礎（SMB1とSMB2の両方をカバー）]

SMB 署名のパフォーマンスへの影響

SMB セッションで SMB 署名を使用すると、Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、署名済み SMB トラフィックのパフォーマンスが向上します。SMB 署名オフロードは、SMB 署名が有効になっている場合にデフォルトで有効になります。

SMB 署名のパフォーマンスを向上させるには、AES-NI オフロード機能が必要です。お使いのプラットフォームで AES-NI オフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9 のバージョン、SMB のバージョン、および SVM の実装方法に応じて SMB 署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

ほとんどの Windows クライアントは、サーバで SMB 署名が有効になっている場合は、SMB 署名をデフォルトでネゴシエートします。一部の Windows クライアントで SMB 保護が必要で、SMB 署名がパフォーマンスの問題を引き起こしている場合は、リプレイアタックからの保護を必要としない Windows クライアントに対して SMB 署名を無効にすることができます。Windows クライアントでの SMB 署名の無効化については、Microsoft Windows のマニュアルを参照してください。

SMB 署名の設定に関する推奨事項

SMB クライアントと CIFS サーバの間の SMB 署名の動作は、セキュリティ要件に応じて設定することができます。CIFS サーバでの SMB 署名の設定は、セキュリティ要件の内容によって異なります。

SMB 署名は、クライアントと CIFS サーバのどちらでも設定できます。SMB 署名を設定する際の推奨事項を次に示します。

状況	推奨事項
クライアントとサーバの間の通信のセキュリティを強化する必要がある	を有効にして、クライアントでSMB署名を必須にします Require Option (Sign always) クライアントのセキュリティ設定。
特定の Storage Virtual Machine（SVM）へのすべての SMB トラフィックに署名する	セキュリティ設定で SMB 署名を必須にするように設定して、CIFS サーバで SMB 署名を必須にします。

Windows クライアントのセキュリティ設定の詳細については、Microsoft のマニュアルを参照してください。

複数のデータ LIF が設定されている場合の SMB 署名に関するガイドライン

SMB サーバで SMB 署名要求を有効または無効にするときは、SVM に複数のデータ LIF が設定されている場合のガイドラインに注意する必要があります。

SMB サーバを設定する際に、複数のデータ LIF が設定されていることがあります。その場合、DNSサーバに複数のが含まれています A CIFSサーバのエントリを記録します。SMBサーバホスト名はすべて同じですが、IPアドレスはそれぞれ一意です。たとえば、2つのデータLIFが設定されているSMBサーバのDNSは次のようになります A レコードエントリ：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

通常の動作では、SMB 署名要求の設定を変更すると、クライアントからの新しい接続だけが SMB 署名の設定変更の影響を受けます。ただし、この動作には例外があります。クライアントに共有への既存の接続がある場合、設定の変更後、クライアントは元の接続を維持しながら同じ共有への新しい接続を作成します。この場合、新規と既存の SMB 接続の両方で新しい SMB 署名の要件が適用されます。

次の例を考えてみましょう。

1. client1は、パスを使用してSMB署名を必要とせずに共有に接続します o:\。
2. ストレージ管理者が、SMB 署名を要求するように SMB サーバの設定を変更したとします。
3. client1は、パスを使用してSMB署名要求で同じ共有に接続します s:\ （パスを使用して接続を維持します o:\）。
4. その結果、両方でデータにアクセスするときにSMB署名が使用されます o:\ および s:\ ドライブ。

受信 **SMB** トラフィックの **SMB** 署名要求を有効または無効にします

SMB メッセージへのクライアントによる署名を強制するには、SMB 署名要求を有効にします。有効にすると、ONTAP は有効な署名のある SMB メッセージのみを受け入れます。SMB 署名を許可するが要求しない場合は、SMB 署名要求を無効にできます。

このタスクについて

デフォルトでは、SMB 署名要求は無効になっています。SMB 署名要求はいつでも有効または無効にできます。

次の状況では、SMB 署名はデフォルトで無効になりません。



1. SMB 署名要求が有効になっており、クラスタが SMB 署名をサポートしていないバージョンの ONTAP にリバートされた。
2. その後、クラスタが SMB 署名をサポートするバージョンの ONTAP にアップグレードされた。

このような場合は、サポートされているバージョンの ONTAP で最初に行われた SMB 署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine (SVM) ディザスタリカバリ関係を設定する際にで選択した値 `-identity` `-preserve` のオプション `snapmirror create` コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` (ID保持)。SMB署名のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は `-identity-preserve` オプションをに設定します `false` (ID保持なし)。SMB署名のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションの CIFS サーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 署名要求を有効にしている場合は、デスティネーション SVM で SMB 署名要求を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

SMB 署名要求の設定	入力するコマンド
有効	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
無効	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

2. での値を確認して、SMB署名要求が有効か無効かを確認します Is Signing Required 次のコマンドの出力のフィールドは、目的の値に設定されます。 `vserver cifs security show -vserver vserver_name -fields is-signing-required`

例

次の例は、SVM vs1 で SMB 署名要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----
vs1      true
```



暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

SMB セッションが署名されているかどうかを確認します

CIFS サーバで接続中の SMB セッションに関する情報を表示できます。この情報を使用して、SMB セッションが署名されているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

手順

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
指定した Storage Virtual Machine (SVM) 上の署名されたすべてのセッション	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>

表示する情報	入力するコマンド
SVM 上の指定したセッション ID を持つ署名されたセッションの詳細です	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id integer -instance</code>

例

次のコマンドを実行すると、SVM vs1 上の署名されたセッションに関するセッション情報が表示されます。デフォルトのサマリー出力には 'Is Session Signed' 出力フィールドは表示されません

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

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、セッションが署名されているかどうかを含む詳細なセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
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: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

関連情報

SMB 署名済みセッションの統計の監視

SMB 署名済みセッションの統計を監視します

SMB セッションの統計を監視し、確立されたセッションのうち、署名されたセッションと署名されていないセッションを区別できます。

このタスクについて

。 `statistics advanced` 権限レベルでコマンドを実行すると、が表示されます `signed_sessions` 署名済みSMBセッションの数を監視するために使用できるカウンタ。。 `signed_sessions` カウンタには、次の統計オブジェクトがあります。

- `cifs` すべてのSMBセッションについてSMB署名を監視できます。
- `smb1` SMB 1.0セッションのSMB署名を監視できます。
- `smb2` SMB 2.xセッションとSMB 3.0セッションのSMB署名を監視できます。

SMB 3.0の統計はの出力に表示されます `smb2` オブジェクト。

署名されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `signed_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

手順

1. 権限レベルをadvancedに設定+ `set -privilege advanced`
2. データ収集を開始します：`+statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスター内のすべてのノードについて統計情報を収集します。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 署名統計情報を表示します。

表示する情報	入力するコマンド
署名されたセッション	<code>`show -sample-id sample_ID -counter signed_sessions`</code>
<code>node_name [-node node_name]</code>	署名されたセッションと確立されたセッション

表示する情報	入力するコマンド
`show -sample-id <i>sample_ID</i> -counter signed_sessions	established_sessions

単一のノードの情報のみを表示する場合は、オプションのを指定します `-node` パラメータ

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

次の例では、「vs1」という Storage Virtual Machine（SVM）について、SMB 2.x と SMB 3.0 のそれぞれの署名統計情報を監視する方法を示します。

次のコマンドは、advanced 権限レベルへの変更を行います。

```
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
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1  
Statistics collection is being started for Sample-id: smbsigning_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbsigning_sample  
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

次のコマンドは、ノードが署名した SMB セッションと確立されたセッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

次のコマンドでは、ノード 2 が署名した SMB セッションをサンプルから表示します。

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

次のコマンドは、admin 権限レベルに戻ります。

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

SMB を介したデータ転送に必要な **SMB** 暗号化を **SMB** サーバで設定します

SMB暗号化の概要

SMB を介したデータ転送での SMB 暗号化は、SMB サーバで有効化または無効化できるセキュリティ強化です。共有プロパティ設定を使用して共有ごとに必要な SMB 暗号化を設定することもできます。

デフォルトでは、Storage Virtual Machine (SVM) でのSMBサーバの作成時にSMB暗号化は無効になっています。SMB 暗号化が提供する高度なセキュリティを活用するには、SMB 暗号化を有効にする必要があります。

暗号化された SMB セッションを作成するには、SMB クライアントが SMB 暗号化をサポートしている必要があります。Windows Server 2012 および Windows 8 以降の Windows クライアントでは、SMB 暗号化がサポートされます。

SVM での SMB 暗号化は、次の 2 つの設定によって制御されます。

- SVMの機能を有効にするSMBサーバセキュリティオプション
- 共有ごとにSMB暗号化を設定するSMB共有プロパティ

SVM 上のすべてのデータへのアクセスに暗号化を要求するか、選択した共有のデータにアクセスする場合のみに SMB 暗号化を要求するかを決定できます。SVM レベルの設定は、共有レベルの設定よりも優先されます。

次の表に示す 2 つの設定の組み合わせを使用すると、効果的な SMB 暗号化設定を行うことができます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
正しいです	いいえ	SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、SMB セッション全体で暗号化が行われます。
正しいです	正しいです	共有レベルの暗号化には関係なく SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、SMB セッション全体で暗号化が行われます。
いいえ	正しいです	特定の共有で共有レベルの暗号化が有効です。この設定では、ツリー接続から暗号化が行われます。

SMB サーバ SMB 暗号化が有効	共有暗号化データ設定が有効です	サーバ側の暗号化の動作
いいえ	いいえ	暗号化は有効になっていません。

暗号化をサポートしていないSMBクライアントは、暗号化が必要なSMBサーバや共有には接続できません。

暗号化設定への変更は、新しい接続に対して有効になります。既存の接続は影響を受けません。

SMB 暗号化のパフォーマンスへの影響

SMB セッションで SMB 暗号化を使用すると、Windows クライアントとのすべての SMB 通信でパフォーマンスが低下し、クライアントとサーバ（SMB サーバを含む SVM を実行しているクラスタ上のノード）の両方に影響します。

パフォーマンスへの影響は、CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

パフォーマンスへの影響の程度は、実行している ONTAP 9 のバージョンによって異なります。ONTAP 9.7 以降では、新しい暗号化のオフロードアルゴリズムによって、暗号化された SMB トラフィックのパフォーマンスが向上します。SMB 暗号化オフロードは、SMB 暗号化が有効になっている場合にデフォルトで有効になります。

SMB 暗号化のパフォーマンスを高めるには、AES-NI オフロード機能が必要です。お使いのプラットフォームで AES-NI オフロードがサポートされていることを確認するには、Hardware Universe（HWU）を参照してください。

はるかに高速なGCMアルゴリズムをサポートするSMBバージョン3.11を使用できる場合は、さらにパフォーマンスが向上します。

ネットワーク、ONTAP 9 のバージョン、SMB のバージョン、および SVM の実装方法に応じて SMB 暗号化のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

SMB 暗号化は、SMB サーバではデフォルトで無効になっています。SMB 暗号化は、暗号化を必要とする SMB 共有または SMB サーバでのみ有効にしてください。SMB 暗号化を有効にすると、ONTAP はすべての要求に対して要求を復号化して応答を暗号化する必要があります。そのため、SMB 暗号化は必要な場合にのみ有効にしてください。

受信 SMB トラフィックの SMB 暗号化要求を有効または無効にします

受信 SMB トラフィックに SMB 暗号化を必須にする場合は、CIFS サーバ上または共有レベルで有効にすることができます。デフォルトでは、SMB 暗号化は必須ではありません。

このタスクについて

CIFS サーバ上で SMB 暗号化を有効にすることができます。この場合、CIFS サーバ上のすべての共有が環境によって暗号化されます。CIFS サーバ上のすべての共有で SMB 暗号化要求を有効にしない場合、または受信 SMB トラフィックの SMB 暗号化要求を共有ごとに有効にする場合は、CIFS サーバ上で SMB 暗号化要求を無効にすることができます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係をセットアップするときには選択した値

-identity-preserve のオプション snapmirror create コマンドは、デスティネーションSVMにレプリケートされる設定の詳細を決定します。

を設定した場合は -identity-preserve オプションをに設定します true (ID保持) では、SMB暗号化のセキュリティ設定がデスティネーションにレプリケートされます。

を設定した場合は -identity-preserve オプションをに設定します false (ID保持なし)。SMB暗号化のセキュリティ設定はデスティネーションにレプリケートされません。この場合、デスティネーションの CIFS サーバセキュリティ設定はデフォルト値に設定されます。ソース SVM で SMB 暗号化を有効にしている場合は、デスティネーションで CIFS サーバの SMB 暗号化を手動で有効にする必要があります。

手順

1. 次のいずれかを実行します。

CIFS サーバでの受信 SMB トラフィックの SMB 暗号化要求の設定	入力するコマンド
有効	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</pre>
無効	<pre>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</pre>

2. CIFSサーバでのSMB暗号化要求が必要に応じて有効または無効になっていることを確認します。

```
vserver cifs security show -vserver vserver_name -fields is-smb-encryption-  
required
```

。 is-smb-encryption-required フィールドが表示されます true CIFSサーバおよびでSMB暗号化要求が有効になっている場合 false 無効になっている場合。

例

次の例は、SVM vs1 で CIFS サーバの受信 SMB トラフィックの SMB 暗号化要求を有効にします。

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption  
-required true  
  
cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-  
encryption-required  
vserver  is-smb-encryption-required  
-----  
vs1      true
```

クライアントが暗号化 SMB セッションを使用して接続しているかどうかを確認します

接続中の SMB セッションに関する情報を表示して、クライアントが暗号化された SMB

接続を使用しているかどうかを確認できます。これは、必要なセキュリティ設定を使用して SMB クライアントセッションが接続されているかどうかを確認する場合に役立ちます。

このタスクについて

SMB クライアントセッションには、次の 3 つのいずれかの暗号化レベルを設定できます。

- unencrypted

SMB セッションは暗号化されません。Storage Virtual Machine （ SVM ） レベルの暗号化も共有レベルの暗号化も設定されません。

- partially-encrypted

ツリー接続が行われると、暗号化が開始されます。共有レベルの暗号化が設定されています。SVM レベルの暗号化は有効になりません。

- encrypted

SMB セッションは完全に暗号化されます。SVM レベルの暗号化が有効です。共有レベルの暗号化は、有効になる場合とならない場合があります。SVM レベルの暗号化設定は、共有レベルの暗号化設定よりも優先されます。

手順

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
指定した SVM のセッションで、指定した暗号化設定を使用するセッション	<code>`vserver cifs session show -vserver vserver_name {unencrypted</code>
partially-encrypted	<code>encrypted} -instance`</code>
指定した SVM の特定のセッション ID の暗号化設定	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>

例

次のコマンドを実行すると、セッション ID 2 の SMB セッションに関する、暗号化設定を含む詳細なセッション情報が表示されます。

```

cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
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: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted

```

SMB 暗号化統計情報を監視する

SMB 暗号化の統計を監視し、確立されたセッションおよび共有接続のうち、暗号化されたものと暗号化されていないものを区別できます。

このタスクについて

。statistics advanced権限レベルでコマンドを実行すると次のカウンタが表示され、暗号化されたSMBセッションおよび共有接続の数を監視できます。

カウンタ名	説明
encrypted_sessions	暗号化された SMB 3.0 セッションの数
encrypted_share_connections	ツリー接続が行われた暗号化された共有の数
rejected_unencrypted_sessions	クライアントに暗号化機能がないために拒否されたセッションセットアップ数を示します
rejected_unencrypted_shares	クライアントに暗号化機能がないために拒否された共有マッピング数

これらのカウンタでは、次の統計オブジェクトを使用できます。

- `cifs` すべてのSMB 3.0セッションについてSMB暗号化を監視できます。

SMB 3.0の統計はの出力に表示されます `cifs` オブジェクト。暗号化されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `encrypted_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

暗号化された共有接続数を共有接続の合計数と比較する場合は、の出力を比較します `encrypted_share_connections` の出力でカウンタに設定します `connected_shares` カウンタ。

- `rejected_unencrypted_sessions` SMB暗号化をサポートしていないクライアントから暗号化を必要とするSMBセッションの確立が試行された回数を示します。
- `rejected_unencrypted_shares` SMB暗号化をサポートしていないクライアントから暗号化が必要なSMB共有への接続が試行された回数を示します。

データを取得して表示するには、統計サンプルの収集を開始する必要があります。データ収集を停止しなければ、サンプルからデータを表示できます。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のクエリとの比較に使用できる更新されたデータを取得できます。この比較は、傾向を確認するのに役立ちます。

手順

1. 権限レベルをadvancedに設定+ `set -privilege advanced`
2. データ収集を開始します：`+statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、前のデフォルトサンプルが上書きされます。

必要に応じて、統計を収集するノードを指定できます。ノードを指定しない場合、サンプルは、クラスタ内のすべてのノードについて統計情報を収集します。

3. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 暗号化統計情報を表示します。

表示する情報	入力するコマンド
暗号化されたセッション	<code>`show -sample-id sample_ID -counter encrypted_sessions</code>
<code>node_name [-node node_name]</code>	暗号化されたセッションと確立されたセッション
<code>`show -sample-id sample_ID -counter encrypted_sessions</code>	<code>established_sessions</code>
<code>node_name [-node node_name]</code>	暗号化された共有接続

表示する情報	入力するコマンド
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>
暗号化された共有接続と接続された共有	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections</code>
connected_shares	<code><i>node_name</i> [-node <i>node_name</i>]</code>
暗号化されていないセッションは	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions</code>
<code><i>node_name</i> [-node <i>node_name</i>]</code>	拒否された暗号化されていない
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share</code>	<code><i>node_name</i> [-node <i>node_name</i>]</code>

単一のノードの情報のみを表示する場合は、オプションのを指定します `-node` パラメータ

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

次の例は、「vs1」という Storage Virtual Machine（SVM）について、SMB 3.0 の暗号化統計情報を監視する方法を示します。

次のコマンドは、advanced 権限レベルへの変更を行います。

```
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
```

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

次のコマンドは、サンプルのデータ収集を停止します。

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

次のコマンドは、指定したノードについて、暗号化された SMB セッション数と確立されたセッション数をサンプルから表示します。

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

次のコマンドは、指定したノードについて、拒否された暗号化されていない SMB セッション数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

次のコマンドは、指定したノードについて、接続された SMB 共有数と暗号化された SMB 共有数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

次のコマンドは、指定したノードについて、拒否された暗号化されていない SMB 共有接続数をサンプルから表示します。

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

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](#)

["パフォーマンスの監視と管理の概要"](#)

セキュアな **LDAP** セッション通信

LDAP の署名と封印の概念

ONTAP 9 以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会

に対する LDAP セッションセキュリティを有効にすることができます。Storage Virtual Machine (SVM) の CIFS サーバセキュリティ設定を LDAP サーバの設定に対応するように設定する必要があります。

署名は、シークレットキーのテクノロジーを使用して、LDAP ペイロードデータの整合性を確認します。封印は、LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、*ldap Security Level* オプションで指定します。デフォルトは `none`。

SVMでCIFSトラフィックに対するLDAPの署名と封印が `-session-security-for-ad-ldap` オプションに設定します `vserver cifs security modify` コマンドを実行します

CIFS サーバで LDAP の署名と封印を有効にする

CIFS サーバで Active Directory LDAP サーバとのセキュアな通信に署名と封印を使用するためには、CIFS サーバのセキュリティ設定を変更して LDAP の署名と封印を有効にする必要があります。

作業を開始する前に

AD サーバ管理者に問い合わせ、適切なセキュリティ設定値を決定する必要があります。

手順

1. Active Directory LDAPサーバとのトラフィックの署名と封印を有効にするCIFSサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver vserver_name -session-security-for-ad-ldap {none|sign|seal}`

署名を有効にできます (`sign`、データ整合性)、署名と封印 (`seal`、データ整合性と暗号化)、またはどちらもない `none`、署名または封印なし)。デフォルト値は `none`。

2. LDAPの署名と封印のセキュリティ設定が正しく設定されていることを確認します。 `vserver cifs security show -vserver vserver_name`



SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、で対応する設定を有効にする必要があります `-session-security` のオプション `vserver services name-service ldap client modify` コマンドを実行します

LDAP over TLS を設定する

自己署名ルート CA 証明書のコピーをエクスポートします

Active Directory 通信の保護に LDAP over SSL/TLS を使用するには、まず Active Directory 証明書サービスの自己署名ルート CA 証明書のコピーを証明書ファイルにエクスポートし、それを ASCII テキストファイルに変換する必要があります。ONTAP は、このテキストファイルを使用して証明書を Storage Virtual Machine (SVM) にインストールします。

作業を開始する前に

Active Directory 証明書サービスがすでにインストールされ、CIFS サーバが属しているドメイン用に設定されている必要があります。Active Directory 証明書サービスのインストールと設定の詳細については、Microsoft TechNet ライブラリを参照してください。

"Microsoft TechNet ライブラリ : technet.microsoft.com"

ステップ

1. 内のドメインコントローラのルートCA証明書を取得します .pem テキスト形式。

"Microsoft TechNet ライブラリ : technet.microsoft.com"

完了後

SVM に証明書をインストールします。

関連情報

"Microsoft TechNet ライブラリ"

自己署名ルート **CA** 証明書を **SVM** にインストールします

LDAP サーバにバインドするときに TLS を使用した LDAP 認証が必要な場合は、まず自己署名ルート CA 証明書を SVM にインストールする必要があります。

このタスクについて

LDAP over TLS が有効な場合、SVM 上の ONTAP LDAP クライアントでは、ONTAP 9.0 および 9.1 の破棄された証明書はサポートされません。

ONTAP 9.2 以降では、TLS 通信を使用する ONTAP 内のすべてのアプリケーションで、Online Certificate Status Protocol (OCSP) を使用してデジタル証明書のステータスを確認できます。OCSP が LDAP over TLS に対して有効になっている場合、失効した証明書は拒否され、接続は失敗します。

手順

1. 自己署名ルート CA 証明書をインストールします。
 - a. 証明書のインストールを開始します。 `security certificate install -vserver vserver_name -type server-ca`

コンソール出力に次のメッセージが表示されます。 Please enter Certificate: Press <Enter> when done
 - b. 証明書を開きます .pem ファイルテキストエディタを使用して、で始まる行を含めて証明書をコピーします -----BEGIN CERTIFICATE----- で終わる `-----END CERTIFICATE-----` をクリックし、コマンドプロンプトのあとに証明書を貼り付けます。
 - c. 証明書が正しく表示されることを確認します。
 - d. Enter キーを押してインストールを完了します。
2. 証明書がインストールされていることを確認します。 `security certificate show -vserver vserver_name`

サーバで **LDAP over TLS** を有効にします

SMBサーバでActive Directory LDAPサーバとのセキュアな通信にTLSを使用するには、SMBサーバのセキュリティ設定を変更してLDAP over TLSを有効にする必要があります。

ONTAP 9.10.1 以降では、Active Directory（AD）とネームサービスの両方の LDAP 接続で、LDAP チャネルバインドがデフォルトでサポートされます。ONTAP は、Start-TLS または LDAPS が有効で、セッションセキュリティが署名または封印に設定されている場合にのみ、LDAP 接続でチャネルバインドを試行します。ADサーバとのLDAPチャネルバインディングを無効または再度有効にするには、を使用します `-try -channel-binding-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します

詳細については、以下を参照してください。

- ["LDAPの概要"](#)
- ["2020 年の Windows 向け LDAP チャネルバインドおよび LDAP 署名の要件"](#)。

手順

1. Active Directory LDAPサーバとのセキュアなLDAP通信を許可するSMBサーバのセキュリティ設定を行います。 `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. LDAP over TLSのセキュリティ設定がに設定されていることを確認します `true` : `vserver cifs security show -vserver vserver_name`



SVMがネームマッピングやその他のUNIX情報（ユーザ、グループ、ネットグループなど）の照会に同じLDAPサーバを使用する場合は、も変更する必要があります `-use-start-tls` オプションを使用します `vserver services name-service ldap client modify` コマンドを実行します

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

ONTAP 9.4 以降では、SMB マルチチャネルを設定して、1 つの SMB セッションで ONTAP とクライアントの間に複数の接続を確立することができます。これにより、スループットとフォールトトレランスが向上します。

作業を開始する前に

SMB マルチチャネル機能は、クライアントが SMB 3.0 以降のバージョンでネゴシエートする場合にのみ使用できます。ONTAP SMB サーバでは、SMB 3.0 以降がデフォルトで有効になっています。

このタスクについて

SMB クライアントは、ONTAP クラスタで適切な設定が見つかり、複数のネットワーク接続を自動的に検出して使用します。

SMB セッションでの同時接続数は、導入している NIC によって異なります。

- * クライアントおよび ONTAP クラスタに 1G NIC を搭載 *

クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされます。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の NIC で接続を確立できます。

また、次のパラメータを変更することもできます（advanced 権限）。

- **-max-connections-per-session**

各マルチチャネルセッションに許可される最大接続数。デフォルトの接続数は 32 です。

デフォルトよりも多くの接続を有効にする場合は、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

- **-max-lifs-per-session**

各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 です。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. SMB サーバで SMB マルチチャネルを有効にします。 `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. ONTAP が SMB マルチチャネルセッションを報告していることを確認します。 `vserver cifs session show options`
4. admin 権限レベルに戻ります。 `set -privilege admin`

例

次の例は、すべての SMB セッションに関する情報を表示します。1 つのセッションに対して複数の接続が表示されています。


```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s                                     Administrator
0
```

次の例は、セッション ID 1 が割り当てられた SMB セッションに関する詳細情報を表示します。

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

SMB サーバでのデフォルト **Windows** ユーザから **UNIX** ユーザへのマッピングを設定する

デフォルトの UNIX ユーザを設定する

ユーザに対する他のマッピングの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の UNIX ユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする必要がある場合は、デフォルト UNIX ユーザを設定しないでください。

このタスクについて

デフォルトでは、デフォルト UNIX ユーザの名前は「pcuser」です。これは、デフォルトで、デフォルト UNIX ユーザへのユーザマッピングが有効になっていることを意味します。デフォルトの UNIX ユーザとして使用する別の名前を指定することもできます。指定する名前は、Storage Virtual Machine（SVM）用に設定されているネームサービスデータベース内に存在する必要があります。このオプションを null 文字列に設定すると、どのユーザも UNIX デフォルトユーザとして CIFS サーバにアクセスできません。つまり、CIFS サーバにアクセスするためには、各ユーザがパスワードデータベースにアカウントを持つ必要があります。

ユーザがデフォルトの UNIX ユーザアカウントを使用して CIFS サーバに接続するには、次の前提条件を満たす必要があります。

- ユーザが認証されていること。
- ユーザが、CIFS サーバのローカル Windows ユーザデータベース、CIFS サーバのホームドメイン、信頼できるドメイン（CIFS サーバでマルチドメインネームマッピング検索が有効な場合）のいずれかにあること
- ユーザ名が明示的に null 文字列にマッピングされることはありません。

手順

1. デフォルトの UNIX ユーザを設定します。

状況	入力するコマンド
デフォルトの UNIX ユーザ「pcuser」を使用する	<pre>vserver cifs options modify -default -unix-user pcuser</pre>
別の UNIX ユーザアカウントをデフォルトユーザとして使用します	<pre>vserver cifs options modify -default -unix-user user_name</pre>
デフォルトの UNIX ユーザを無効にします	<pre>vserver cifs options modify -default -unix-user ""</pre>

```
vserver cifs options modify -default-unix-user pcuser
```

2. デフォルトの UNIX ユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vs1`

次の例では、SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「pcuser」を使用するように設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

ゲスト UNIX ユーザを設定します

ゲスト UNIX ユーザを設定すると、信頼されていないドメインからログインしたユーザがゲスト UNIX ユーザにマッピングされ、CIFS サーバに接続できるようになります。ただし、信頼されていないドメインのユーザの認証を失敗にする場合は、ゲスト UNIX ユーザを設定しないでください。デフォルトでは、信頼されていないドメインのユーザによる CIFS サーバへの接続は許可されません（ゲスト UNIX アカウントは設定されません）。

このタスクについて

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- CIFS サーバがホームドメインまたは信頼できるドメインのドメインコントローラ、ローカルデータベースのどちらかに対してユーザを認証できず、このオプションが有効である場合、CIFS サーバはユーザをゲストユーザとみなし、そのユーザを指定した UNIX ユーザにマッピングします。
- このオプションを null 文字列に設定すると、ゲスト UNIX ユーザは無効になります。
- いずれかの Storage Virtual Machine（SVM）ネームサービスデータベースで、ゲスト UNIX ユーザとして使用する UNIX ユーザを作成する必要があります。
- ゲストユーザとしてログインしたユーザは、自動的に CIFS サーバの BUILTIN\guests グループのメンバーになります。
- 「homedirs-public」オプションは、認証されたユーザにのみ適用されます。ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。

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
ゲスト UNIX ユーザを設定します	<pre>vserver cifs options modify -guest -unix-user <i>unix_name</i></pre>
ゲスト UNIX ユーザを無効にします	<pre>vserver cifs options modify -guest -unix-user ""</pre>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. ゲストUNIXユーザが正しく設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`

次の例では、SVM vs1 のデフォルト UNIX ユーザとゲスト UNIX ユーザの両方が UNIX ユーザ「pcuser」を使用するように設定されています。

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

Administrators グループをルートにマッピングします

環境内のクライアントがすべて CIFS クライアントで、Storage Virtual Machine（SVM）がマルチプロトコルストレージシステムとしてセットアップされている場合は、SVM上のファイルにアクセスするための root 権限を持つ Windows アカウントが少なくとも 1 つ必要です。十分なユーザ権限がないため、この SVM を管理できません。

このタスクについて

ただし、ストレージシステムがNTFS専用としてセットアップされている場合は /etc ディレクトリには、AdministratorsグループがONTAP 構成ファイルにアクセスできるようにするファイルレベルのACLが設定されています。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 必要に応じて、Administrators グループをルートにマッピングする CIFS サーバオプションを設定します。

状況	作業
管理者グループメンバーをルートにマッピングします	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> がなくても、Administratorsグループ内のすべてのアカウントはrootとみなされます <code>/etc/usermap.cfg</code> アカウントをrootにマッピングするエントリ。Administrators グループに属するアカウントを使用してファイルを作成する場合、UNIX クライアントからファイルを表示するときに、ファイルはルートによって所有されます。
Administrators グループメンバーのルートへのマッピングを無効にします	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Administratorsグループ内のアカウントがrootにマッピングされなくなります。ルートへのマッピングは、単一のユーザに対して明示的にのみ実行できます。

- オプションが目的の値に設定されていることを確認します。 `vserver cifs options show -vserver vserver_name`
- admin 権限レベルに戻ります。 `set -privilege admin`

SMB セッションを介して接続しているユーザのタイプに関する情報を表示します

SMB セッションを介して接続しているユーザのタイプに関する情報を表示できます。これは、適切なタイプのユーザのみが Storage Virtual Machine（SVM）上の SMB セッションを介して接続していることを確認するのに役立ちます。

このタスクについて

SMB セッションを介して接続できるユーザのタイプは次のとおりです。

- local-user

ローカル CIFS ユーザとして認証されている

- domain-user

ドメインユーザとして（CIFS サーバのホームドメインまたは信頼できるドメインから）認証されている

- guest-user

ゲストユーザとして認証されています

- anonymous-user

匿名ユーザまたは null ユーザとして認証されています

手順

1. SMBセッションを介して接続しているユーザのタイプを確認します。 `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

確立されたセッションのユーザタイプ情報を表示する対象	入力するコマンド
指定したユーザタイプのすべてのセッション	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
domain-user	guest-user
anonymous-user}`	特定のユーザの場合

例

次のコマンドを実行すると、ユーザ「iepubs\user1」によって確立された SVM vs1 上のセッションのユーザタイプに関するセッション情報が表示されます。

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user      user-type
-----
-----
pub1node1 pub1      1          3439441860      10.0.0.1      10.1.1.1
IEPUBS\user1      domain-user
```

Windows クライアントの過剰なリソース消費を制限するコマンドオプション

をクリックします `vserver cifs options modify` コマンドを使用すると、Windowsクライアントのリソース消費を制御できます。ファイルオープン、セッションオープン、変更通知要求が異常に多い場合など、正常な範囲を超えてリソースを消費しているクライアントがある場合に便利です。

には次のオプションがあります `vserver cifs options modify` Windowsクライアントのリソース消費を制御するコマンドが追加されました。これらのオプションの最大値を超えると、要求は拒否され、EMS メッセージが送信されます。これらのオプションで設定された上限の 80% に達したときにも EMS 警告メッセージが送信されます。

- `-max-opens-same-file-per-tree`
CIFS ツリーあたりの同じファイルの最大オープン数
- `-max-same-user-sessions-per-connection`
同じユーザが接続ごとに開いたセッションの最大数

- `-max-same-tree-connect-per-session`

同じ共有に対するセッションあたりの最大ツリー接続数

- `-max-watches-set-per-tree`

ツリーごとに確立されるウォッチの最大数（別名 *change notifier*）

デフォルトの制限および現在の設定を表示する方法については、マニュアルページを参照してください。

ONTAP 9.4 以降では、SMB バージョン 2 以降を実行しているサーバで、クライアントからサーバに SMB 接続で送信できる未処理要求（`_SMB クレジット`）の数を制限することができます。SMB クレジットの管理はクライアント側で開始され、サーバ側で制御されます。

SMB接続で許可できる未処理要求の最大数は、で制御されます `-max-credits` オプションこのオプションのデフォルト値は 128 です。

従来の **oplock** および **oplock** リースでクライアントのパフォーマンスを向上

従来の **oplock** および **oplock** リースの概要でクライアントのパフォーマンスを向上

便宜的 **oplock** と **oplock** リースでは、先読み、あと書き、ロックの各情報を SMB クライアント側でキャッシングできるように、特定のファイル共有シナリオでそのクライアントを有効にします。これにより、クライアントは、目的のファイルへのアクセス要求をサーバに定期的に通知しなくても、ファイルの読み書きを実行できます。これにより、ネットワークトラフィックが軽減され、パフォーマンスが向上します。

oplock リースは **oplock** を強化したもので、SMB 2.1 以降のプロトコルで使用できます。**oplock** リースでは、クライアントが、自身による複数の SMB オープンにおいてキャッシュ状態を取得し、保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティで、を使用します `vserver cifs share create` 共有の作成時にコマンドを実行するか、またはを実行します `vserver share properties` 作成後のコマンド。
- **qtree**プロパティ。を使用します `volume qtree create` コマンドを使用して**qtree**を作成するか、コマンドを使用します `volume qtree oplock` 作成後のコマンド。

oplock を使用するときの書き込みキャッシュデータ消失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的な **oplock** を保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスはキャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントは **oplock** を放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われる可能性があります。

- データ損失の可能性

データの書き込みがキャッシュされるアプリケーションでは、次の場合にそのデータを失う可能性があります

ます。

- 接続は SMB 1.0 を使用して確立されます。
 - ファイルに対して排他的な oplock を使用している場合
 - oplock を解除するか、ファイルを閉じるように指示された場合
 - 書き込みキャッシュをフラッシュするプロセスで、ネットワークまたはターゲットシステムにエラーが発生した場合
- エラー処理および書き込みの完了

キャッシュ自体にはエラー処理がありません。アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行うと、書き込みは常に完了します。キャッシュがネットワーク経由でターゲットシステムに書き込みを行う場合、書き込みは完了していると仮定する必要があります。これは、完了していない場合、データが失われるためです。

SMB 共有の作成時に oplock を有効または無効にします

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。Storage Virtual Machine（SVM）上にある SMB 共有では、oplock が有効になっています。場合によっては、oplock の無効化が必要になることがあります。oplock は共有ごとに有効または無効にできます。

このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームの oplock の設定よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。

oplock 共有プロパティに加えて、その他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する操作を実行します。

状況	作業
共有の作成時に共有で oplock を有効にします	<p>次のコマンドを入力します。vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</p> <div>  <p>共有にデフォルトの共有プロパティのみを設定する場合は、です oplocks、browsable および `changenotify` 有効にすると、を指定する必要はありません -share -properties SMB共有を作成するときのパラメータ。デフォルト以外の共有プロパティを組み合わせる使用の場合は、を指定する必要があります -share-properties パラメータに指定し、その共有に使用する共有プロパティのリストを指定します。</p> </div>
共有の作成時に共有で oplock を無効にします	<p>次のコマンドを入力します。vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</p> <div>  <p>oplockを無効にする場合は、共有の作成時に共有プロパティのリストを指定する必要がありますが、を指定することはできません oplocks プロパティ。</p> </div>

関連情報

[既存の SMB 共有で oplock を有効または無効にします](#)

[oplock ステータスを監視しています](#)

ボリュームおよび **qtree** で **oplock** を有効または無効にするためのコマンド

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。ボリュームや qtree の oplock を有効または無効にするためのコマンドを理解しておく必要があります。また、いつボリュームおよび qtree で oplock を有効または無効にできるかについても理解しておく必要があります。

- ボリュームではデフォルトで oplock が有効になっています。

- ボリュームの作成時に oplock を無効にすることはできません。
- 既存の SVM のボリュームでは、oplock をいつでも有効または無効にできます。
- SVM の qtree では oplock を有効にできます。

oplock モードの設定は、すべてのボリュームのデフォルトの qtree である qtree ID 0 のプロパティです。qtree の作成時に oplock 設定を指定しない場合、qtree は親ボリュームの oplock 設定を継承します。この設定はデフォルトで有効になっています。ただし、新しい qtree に oplock 設定を指定すると、ボリュームの oplock 設定よりも優先されます。

状況	使用するコマンド
ボリュームまたは qtree の oplock を有効にします	volume qtree oplocks を使用 -oplock-mode パラメータをに設定します enable
ボリュームまたは qtree の oplock を無効にします	volume qtree oplocks を使用 -oplock-mode パラメータをに設定します disable

関連情報

[oplock ステータスを監視しています](#)

既存の **SMB** 共有で **oplock** を有効または無効にします

Storage Virtual Machine（SVM）上の SMB 共有では、oplock がデフォルトで有効になっています。場合によっては、oplock の無効化が必要になることがあります。または、以前に共有で oplock を無効にした場合に、oplock を再度有効にすることもできます。

このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームでの oplock の有効化よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。既存の共有での oplock の有効化と無効化はいつでも実行できます。

ステップ

1. 該当する操作を実行します。

状況	作業
既存の共有を変更して、共有で oplock を有効にします	<p>次のコマンドを入力します。vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</p> <div>  <p>追加する共有プロパティをカンマで区切って追加指定できます。</p> </div> <p>新しく追加したプロパティは、共有プロパティの既存のリストに追加されます。以前に指定した共有プロパティは有効なままです。</p>
既存の共有を変更して共有で oplock を無効にします	<p>次のコマンドを入力します。vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</p> <div>  <p>削除する共有プロパティをカンマで区切って追加指定できます。</p> </div> <p>削除した共有プロパティは既存の共有プロパティリストから削除されますが、削除しなかった設定済みの共有プロパティは有効なままです。</p>

例

次のコマンドは、Storage Virtual Machine（SVM、旧 Vserver）vs1 上の「Engineering」という名前の共有の oplock を有効にします。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

次のコマンドは、SVM vs1 上の「Engineering」という名前の共有の oplock を無効にします。

```
cluster1::> vservers cifs share properties remove -vservers vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vservers cifs share properties show
Vserver      Share      Properties
-----
vs1          Engineering browsable
              changenotify
              showsnapshot
```

関連情報

[SMB 共有の作成時における oplock の有効化と無効化](#)

[oplock ステータスを監視しています](#)

[既存の SMB 共有に対する共有プロパティの追加または削除](#)

oplock ステータスを監視します

oplock ステータスについて、情報を監視、表示できます。この情報を使用して、oplock が設定されたファイル、oplock のレベルや oplock の状態レベル、oplock リースの使用の有無を確認できます。また、手動での解除が必要となる可能性のあるロックについて、情報を確認することもできます。

このタスクについて

すべての oplock についての情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、クライアントの IP アドレスやパスを指定して、該当するロックのみを返すように指定できます。

従来の oplock および oplock リースについて、次の情報を表示できます。

- oplock が有効な SVM、ノード、ボリューム、LIF
- ロック UUID
- oplock が有効なクライアントの IP アドレス
- oplock が有効なパス
- ロックのプロトコル（SMB）およびロックのタイプ（oplock）
- ロックの状態
- oplock レベル
- 接続の状態および SMB の有効期限
- oplock リースが許可されている場合は、Open Group ID

を参照してください `vservers oplocks show` 各パラメータの詳細な概要 のマニュアルページ

手順

1. を使用してoplockステータスを表示します `vserver locks show` コマンドを実行します

例

次のコマンドは、すべてのロックに関するデフォルトの情報を表示します。表示されたファイルのoplockは、
で許可されています `read-batch oplock`レベル：

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

次の例は、パスのファイルに対するロックに関する詳細情報を表示します

`/data2/data2_2/intro.pptx`。を使用してファイルにoplockリースが許可されています batch IPアドレス
のクライアントに対するoplockレベル 10.3.1.3：



詳細情報を表示する場合に、このコマンドを使用すると、oplock の情報と共有ロックの情報を別々に表示できます。この例では、oplock の情報のみが表示されています。

```
cluster1::> vserver lock 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: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    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
```

関連情報

[SMB 共有の作成時における oplock の有効化と無効化](#)

[既存の SMB 共有で oplock を有効または無効にします](#)

[ボリュームおよび qtree で oplock を有効または無効にするためのコマンド](#)

SMB サーバへのグループポリシーオブジェクトの適用

SMB サーバへのグループポリシーオブジェクトの適用の概要の説明を参照してください

SMBサーバは、グループポリシーオブジェクト（GPO）をサポートしています。GPO は、Active Directory環境のコンピュータに適用される_グループポリシー属性_と呼ばれる一連のルールです。GPO を使用して、同じ Active Directory ドメインに属するクラスター上のすべての Storage Virtual Machine （SVM）の設定を一元管理できます。

SMBサーバでGPOが有効になっている場合、ONTAPはActive DirectoryサーバにLDAPクエリを送信してGPO情報を要求します。SMBサーバに適用可能なGPO定義がある場合、Active Directoryサーバは次のGPO情報を

返します。

- GPO 名
- 現在の GPO バージョン
- GPO 定義の場所
- GPO ポリシーセットの Universally Unique Identifier (UUID) 一覧

関連情報

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

["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 GPO

すべてのグループポリシーオブジェクト（GPO）を CIFS 対応の Storage Virtual Machine（SVM）に適用できるわけではありませんが、SVM では関連する GPO を認識して処理することができます。

SVM で現在サポートされている GPO は次のとおりです。

- 高度な監査ポリシー設定：

オブジェクトへのアクセス：集約型アクセスポリシーのステージング

次の設定を含む集約型アクセスポリシー（CAP）のステージングで監査対象となるイベントのタイプを指定します。

- 監査しないでください
- 成功イベントのみ監査
- 失敗イベントのみ監査
- 成功イベントと失敗イベントの両方を監査します



3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAP は成功イベントと失敗イベントの両方を監査します。

を使用して設定します Audit Central Access Policy Staging を設定します Advanced Audit Policy Configuration/Audit Policies/Object Access GPO：



高度な監査ポリシー構成 GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で監査を構成する必要があります。SVM で監査が構成されていない場合、GPO 設定は適用されず、破棄されます。

- レジストリ設定：
 - CIFS 対応の SVM のグループポリシーの更新間隔

を使用して設定します Registry GPO :

- グループポリシーの更新間隔のランダムオフセット

を使用して設定します Registry GPO :

- BranchCache のハッシュの発行

BranchCache のハッシュの発行 GPO は、BranchCache の動作モードに対応します。次の 3 つの動作モードがサポートされています。

- 共有ごと
- all-shares
- 無効 を使用して設定します Registry GPO :

- BranchCache のハッシュバージョンサポート

次の 3 つのハッシュバージョン設定がサポートされています。

- BranchCache バージョン 1.7
- BranchCache バージョン 1.7
- BranchCacheバージョン1および2 を使用して設定します Registry GPO :



BranchCache GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で BranchCache を構成する必要があります。SVM で BranchCache が構成されていない場合、GPO 設定は適用されず、破棄されます。

• セキュリティ設定

- 監査ポリシーとイベントログ

- ログオンイベントを監査します

次の設定を含む監査対象となるログオンイベントの種類を指定します。

- 監査しないでください
- 成功イベントのみ監査
- 障害イベントの監査
- 成功イベントと失敗イベントの両方を監査します を使用して設定します Audit logon events を設定します Local Policies/Audit Policy GPO :



3 つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAP は成功イベントと失敗イベントの両方を監査します。

- オブジェクトへのアクセスを監査する

次の設定を含む監査対象となるオブジェクトアクセスの種類を指定します。

- 監査しないでください
- 成功イベントのみ監査
- 障害イベントの監査
- 成功イベントと失敗イベントの両方を監査します を使用して設定します Audit object access を設定します Local Policies/Audit Policy GPO :



3つの監査オプション（成功イベントのみ監査、失敗イベントのみ監査、成功イベントと失敗イベントの両方を監査）のいずれかが設定されている場合、ONTAPは成功イベントと失敗イベントの両方を監査します。

- ログの保持方法

次の設定を含む監査ログの保持方法を指定します。

- ログファイルのサイズが最大ログサイズを超えたら、イベントログを上書きします
- イベントログを上書きしない（手動でログを消去） を使用して設定します Retention method for security log を設定します Event Log GPO :

- 最大ログサイズ

監査ログの最大サイズを指定します。

を使用して設定します Maximum security log size を設定します Event Log GPO :



監査ポリシーとイベントログ GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で監査を構成する必要があります。SVM で監査が構成されていない場合、GPO 設定は適用されず、破棄されます。

- ファイルシステムのセキュリティ

GPO を通してファイルセキュリティを適用するファイルまたはディレクトリのリストを指定します。

を使用して設定します File System GPO :



SVM 内にファイルシステムセキュリティ GPO を構成するボリュームパスが存在している必要があります。

- Kerberos ポリシー

- 最大クロックスキュー

コンピュータクロック同期の最大許容誤差を分単位で指定します。

を使用して設定します Maximum tolerance for computer clock synchronization を設定します Account Policies/Kerberos Policy GPO :

- チケットの有効期間

ユーザチケットの最大有効期間を時間単位で指定します。

を使用して設定します Maximum lifetime for user ticket を設定します Account Policies/Kerberos Policy GPO :

- チケットの更新の有効期間

ユーザチケットの更新の最大有効期間を日単位で指定します。

を使用して設定します Maximum lifetime for user ticket renewal を設定します Account Policies/Kerberos Policy GPO :

- ユーザ権限の割り当て（権限）

- 所有権を取得します

セキュリティ保護が可能なオブジェクトの所有権を持つユーザとグループのリストを指定します。

を使用して設定します Take ownership of files or other objects を設定します Local Policies/User Rights Assignment GPO :

- セキュリティ権限

ファイル、フォルダ、Active Directory オブジェクトなどの個々のリソースへのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。

を使用して設定します Manage auditing and security log を設定します Local Policies/User Rights Assignment GPO :

- 通知権限の変更（トラバースチェックのバイパス）

ユーザとグループがトラバースするディレクトリに対する権限を持っていなくても、ディレクトリツリーをトラバースできるユーザとグループのリストを指定します。

ファイルやディレクトリの変更通知を受け取るユーザにも同じ権限が必要です。を使用して設定します Bypass traverse checking を設定します Local Policies/User Rights Assignment GPO :

- レジストリ値

- 署名要求設定

SMB 署名要求が有効になっているか無効になっているかを示します。

を使用して設定します Microsoft network server: Digitally sign communications (always) を設定します Security Options GPO :

- restrict anonymous（匿名の制限

匿名ユーザの制限内容に次の 3 つの GPO 設定を指定します。

- Security Account Manager（SAM）アカウントを列挙しない：

このセキュリティ設定は、コンピュータへの匿名接続に付与される追加の権限を決定します。こ

のオプションはと表示されます no-enumeration ONTAP（有効になっている場合）。

を使用して設定します Network access: Do not allow anonymous enumeration of SAM accounts を設定します Local Policies/Security Options GPO:

- SAM アカウントと共有は列挙しません

このセキュリティ設定で、匿名による SAM アカウントと共有の列挙を許可するかどうかを決定します。このオプションはと表示されます no-enumeration ONTAP（有効になっている場合）。

を使用して設定します Network access: Do not allow anonymous enumeration of SAM accounts and shares を設定します Local Policies/Security Options GPO:

- 共有と名前付きパイプへの匿名アクセスを制限します

共有とパイプへの匿名アクセスを制限します。このオプションはと表示されます no-access ONTAP（有効になっている場合）。

を使用して設定します Network access: Restrict anonymous access to Named Pipes and Shares を設定します Local Policies/Security Options GPO:

定義済みおよび適用済みのグループポリシーに関する情報を表示する場合は、Resultant restriction for anonymous user Output フィールドには、3つの restrict anonymous GPO 設定による制限に関する情報が表示されます。表示される可能性がある制限結果は、次のとおりです。

- no-access

匿名ユーザは、指定された共有と名前付きパイプへのアクセスを拒否され、SAM アカウントと共有を列挙できません。この制限結果は、の場合に表示されます Network access: Restrict anonymous access to Named Pipes and Shares GPO が有効になっている。

- no-enumeration

匿名ユーザは、指定された共有と名前付きパイプにアクセスできますが、SAM アカウントと共有は列挙できません。この制限は、次の両方の条件に該当する場合に適用されます。

- 。 Network access: Restrict anonymous access to Named Pipes and Shares GPO が無効になっています。
- またはをクリックします Network access: Do not allow anonymous enumeration of SAM accounts または Network access: Do not allow anonymous enumeration of SAM accounts and shares GPO が有効になっている。

- no-restriction

匿名ユーザにはフルアクセスが付与され、列挙できます。この制限は、次の両方の条件に該当する場合に適用されます。

- 。 Network access: Restrict anonymous access to Named Pipes and Shares GPO が無効になっています。
- 両方とも Network access: Do not allow anonymous enumeration of SAM accounts および Network access: Do not allow anonymous enumeration of SAM accounts

and shares GPOが無効になっている。

- 制限されたグループ

制限されたグループを設定して、組み込みまたはユーザ定義のグループのメンバーシップを一元管理することができます。グループポリシーを通して制限されたグループを適用する場合、CIFS サーバローカルグループのメンバーシップは、適用されるグループポリシーで定義されているメンバーリスト設定に一致するように自動的に設定されます。

を使用して設定します **Restricted Groups GPO** :

- 集約型アクセスポリシーの設定

集約型アクセスポリシーのリストを指定します。集約型アクセスポリシーと関連付けられた集約型アクセスポリシールールによって、SVM 上の複数のファイルに対するアクセス権限が決定されます。

関連情報

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

["SMB および NFS の監査とセキュリティトレース"](#)

[CIFS サーバの Kerberos セキュリティ設定の変更](#)

[BranchCache を使用したブランチオフィスでの SMB 共有のコンテンツのキャッシュ](#)

[SMB 署名を使用したネットワークセキュリティの強化](#)

[トラバースチェックのバイパスの設定](#)

[匿名ユーザのアクセス制限を設定します](#)

SMB サーバで **GPO** を使用するための要件

SMB サーバでグループポリシーオブジェクト（GPO）を使用するには、いくつかの要件を満たしている必要があります。

- クラスタで SMB のライセンスが有効になっている必要があります。SMBライセンスはに含まれていません。"ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- SMB サーバが設定され、Windows Active Directory ドメインに参加している必要があります。
- SMB サーバ管理ステータスがオンになっている必要があります。
- GPO が設定され、SMB サーバコンピュータオブジェクトを含む Windows Active Directory の組織単位（OU）に適用されている必要があります。
- SMB サーバで GPO のサポートが有効になっている必要があります。

CIFS サーバ上で GPO のサポートを有効または無効にします

CIFS サーバでグループポリシーオブジェクト（GPO）のサポートを有効または無効にできます。CIFS サーバ上で GPO のサポートを有効にすると、グループポリシー（CIFS サーバコンピュータオブジェクトを含む組織単位に適用されるポリシー）に定義されている該当する GPO が CIFS サーバに適用されます。



このタスクについて
GPO はワークグループモードの CIFS サーバでは有効にできません。

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
GPOs を有効にします。	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
GPOs を無効にする	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. GPOサポートが目的の状態になっていることを確認します。 `vserver cifs group-policy show -vserver +vserver_name_`

ワークグループモードの CIFS サーバのグループポリシーステータスは「disabled」と表示されます。

例

次の例は、Storage Virtual Machine（SVM）vs1 で GPO サポートを有効にします。

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

関連情報

[サポートされる GPO](#)

[CIFSサーバでGPOを使用するための要件](#)

[CIFS サーバでの GPO の更新方法](#)

[CIFS サーバ上の GPO 設定を手動で更新します](#)

[GPO 設定に関する情報を表示します](#)

CIFS サーバでの GPO の更新方法の概要

デフォルトでは、ONTAP はグループポリシーオブジェクト（GPO）の変更を 90 分に 1 回取得して適用します。セキュリティ設定は 16 時間ごとに更新されます。ONTAP で自動的に更新される前に GPO を更新し、新しい GPO ポリシー設定を適用するには、ONTAP コマンドを使用して CIFS サーバで手動更新をトリガーします。

- デフォルトでは、すべての GPO を 90 分に 1 回確認し、必要に応じて更新。

この間隔は設定可能で、を使用して設定できます Refresh interval および Random offset GPO 設定。

ONTAP は、GPO の変更がないかどうかを Active Directory に照会します。Active Directory に記録されている GPO のバージョン番号が CIFS サーバ上の GPO のバージョン番号より大きい場合、ONTAP は新しい GPO を取得して適用します。バージョン番号が同じ場合、CIFS サーバ上の GPO は更新されません。

- セキュリティ設定の GPO を 16 時間に 1 回更新。

ONTAP は、変更の有無にかかわらず、16 時間に 1 回セキュリティ設定の GPO を取得して適用します。



デフォルト値の 16 時間は、現在の ONTAP バージョンでは変更できません。これは Windows クライアントのデフォルト設定です。

- ONTAP コマンドを使用して手動ですべての GPO を更新。

このコマンドは、ウィンドウをシミュレートします gpupdate.exe /force コマンド。

関連情報

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバの Group Policy Object（GPO；グループポリシーオブジェクト）設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

ステップ

1. 適切な操作を実行します。

更新する項目	入力するコマンド
GPO 設定が変更されました	<pre>vserver cifs group-policy update -vserver vserver_name</pre>

更新する項目	入力するコマンド
すべての GPO 設定	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

関連情報

CIFS サーバでの GPO の更新方法

GPO 設定に関する情報を表示します

Active Directory で定義されているグループポリシーオブジェクト（GPO）設定および CIFS サーバに適用されている GPO 設定に関する情報を表示できます。

このタスクについて

CIFS サーバが属しているドメインの Active Directory で定義されているすべての GPO 設定に関する情報を表示するか、または CIFS サーバに適用されている GPO 設定に関する情報のみを表示することができます。

手順

1. 次のいずれかの操作を実行し、GPO 設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
CIFS 対応の Storage Virtual Machine（SVM）に適用されている	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

例

次の例は、vs1 という CIFS 対応の SVM が属する Active Directory で定義されている GPO 設定を表示します。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
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 : version1
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
  Status: enabled
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication for Mode BranchCache: per-share
  Hash Version Support for BranchCache: version1
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

```

次の例は、CIFS 対応の SVM vs1 に適用されている GPO 設定を表示します。

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

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
```

関連情報

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

制限されたグループの **GPO** に関する詳細情報を表示します

Active Directory でグループポリシーオブジェクト（GPO）として定義されている制限されたグループ、および CIFS サーバに適用されている制限されたグループに関する詳細情報を表示できます。

このタスクについて

デフォルトでは、次の情報が表示されます。

- グループポリシー名
- グループポリシーのバージョン
- リンク

グループポリシーを設定するレベルを指定します。出力される値は次のとおりです。

- Local グループポリシーがONTAP で設定されている場合

- Site グループポリシーがドメインコントローラのサイトレベルで設定されている場合
- Domain グループポリシーがドメインコントローラのドメインレベルで設定されている場合
- OrganizationalUnit グループポリシーがドメインコントローラの組織単位（OU）レベルで設定されている場合
- RSOP さまざまなレベルで定義されたすべてのグループポリシーから派生した一連のポリシー

- 制限されたグループ名です
- 制限されたグループに属するユーザとグループ、および属さないユーザとグループ
- 制限されたグループが追加されているグループのリスト

グループは、ここに記載されているグループ以外のグループのメンバーになることもできます。

ステップ

1. 次のいずれかの操作を実行し、制限されたグループのすべての GPO に関する情報を表示します。

情報を表示する制限されたグループのすべての GPO	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

例

次の例は、CIFS 対応の vs1 という名前の SVM が属する Active Directory ドメインで定義されている、制限されたグループの GPO に関する情報を表示します。

```
cluster1::> vsriver cifs group-policy restricted-group show-defined
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

次の例は、CIFS 対応の SVM vs1 に適用されている、制限されたグループの GPO に関する情報を表示します。

```
cluster1::> vsriver cifs group-policy restricted-group show-applied
-vsriver vs1
```

```
Vsriver: vs1
```

```
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

Active Directory で定義されている集約型アクセスポリシーに関する詳細情報を表示できます。また、グループポリシーオブジェクト（GPO）を介して CIFS サーバに適用されている集約型アクセスポリシーに関する情報も表示できます。

このタスクについて

デフォルトでは、次の情報が表示されます。

- SVM 名
- 集約型アクセスポリシーの名前
- SID
- 説明
- 作成時間
- 修正日時
- メンバールール



ワークグループモードの CIFS サーバについては、GPO をサポートしていないため情報は表示されません。

ステップ

1. 次のいずれかの操作を実行し、集約型アクセスポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

例

次の例は、Active Directory で定義されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-defined
```

```
Vserver   Name                               SID
-----
-----
vs1        p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1        p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

次の例は、クラスタ上の Storage Virtual Machine（SVM）に適用されているすべての集約型アクセスポリシーの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

```
Vserver   Name                               SID
-----
-----
vs1        p1                               S-1-17-3386172923-1132988875-3044489393-
3993546205
    Description: policy #1
    Creation Time: Tue Oct 22 09:34:13 2013
    Modification Time: Wed Oct 23 08:59:15 2013
    Member Rules: r1

vs1        p2                               S-1-17-1885229282-1100162114-134354072-
822349040
    Description: policy #2
    Creation Time: Tue Oct 22 10:28:20 2013
    Modification Time: Thu Oct 31 10:25:32 2013
    Member Rules: r1
                r2
```

DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

Active Directory で定義されている集約型アクセスポリシーに関連付けられた集約型アクセスポリシールールに関する詳細情報を表示できます。また、集約型アクセスポリシーの GPO（グループポリシーオブジェクト）を介して CIFS サーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

このタスクについて

定義および適用されている集約型アクセスポリシールールに関する詳細情報を表示できます。デフォルトでは、次の情報が表示されます。

- SVM 名です
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 修正日時
- 現在の権限
- 推奨される権限
- ターゲットリソース

集約型アクセスポリシーに関連付けられた、情報を表示するすべての集約型アクセスポリシールール	入力するコマンド
Active Directory で定義されています	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
CIFS サーバに適用されます	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

例

次の例は、Active Directory で定義されている集約型アクセスポリシーに関連付けられたすべての集約型アクセスポリシールールの情報を表示します。


```
cluster1::> vservers cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

次の例は、クラスタ上で Storage Virtual Machine（SVM）に適用されている集約型アクセスポリシーに関連付けられたすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vservers cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

関連情報

[DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護](#)

[GPO 設定に関する情報を表示します](#)

[集約型アクセスポリシーに関する情報を表示します](#)

SMBサーバコンピュータアカウントパスワードの管理用コマンド

パスワードの変更、リセット、無効化、および自動更新スケジュールの設定に使用するコマンドについて説明します。SMBサーバでスケジュールを設定して自動的に更新することもできます。

状況	使用するコマンド
ドメインアカウントのパスワードを変更またはリセットします。パスワードがわかっている場合	<code>vserver cifs domain password change</code>
ドメインアカウントパスワードをリセットします。パスワードがわからない場合	<code>vserver cifs domain password reset</code>
コンピュータアカウントパスワードの自動変更を行うために SMB サーバを設定する	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>
SMBサーバでのコンピュータアカウントパスワードの自動変更の無効化	<code>vserver cifs domain password schedule modify -vserver vs1 -is-schedule-enabled false</code>

詳細については、各コマンドのマニュアルページを参照してください。

ドメインコントローラ接続を管理します

検出されたサーバに関する情報を表示します

CIFS サーバで検出された LDAP サーバおよびドメインコントローラに関する情報を表示できます。

ステップ

1. 検出されたサーバに関する情報を表示するには、次のコマンドを入力します。 `vserver cifs domain discovered-servers show`

例

次の例は、SVM vs1 で検出されたサーバを表示します。

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

関連情報

サーバのリセットおよび再検出

CIFS サーバを停止または起動しています

サーバをリセットおよび再検出します

CIFS サーバでサーバのリセットと再検出を行うと、LDAP サーバおよびドメインコントローラに格納されている情報が CIFS サーバに破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver vserver_name`

例

次の例は、Storage Virtual Machine（SVM、旧 Vserver）vs1 のサーバをリセットして再検出します。

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

```
Node: node1  
Vserver: vs1
```

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

関連情報

[検出されたサーバに関する情報を表示する](#)

[CIFS サーバを停止または起動しています](#)

ドメインコントローラの検出を管理します

ONTAP 9.3 以降では、ドメインコントローラ（DC）の検出に使用するデフォルトプロセスを変更できます。サイトまたは優先 DC のプールに検出を制限できるため、環境によってはパフォーマンスの向上につながります。

このタスクについて

デフォルトでは、任意の優先 DC、ローカルサイト内のすべての DC、およびすべてのリモート DC を含めて、使用可能なすべての DC が検出されます。そのため、一部の環境では、認証時および共有へのアクセス時にレイテンシが発生する可能性があります。使用する DC のプールが決まっている場合、またはリモート DC が不適切またはアクセスできない場合は、検出方法を変更できます。

ONTAP 9.3以降のリリースでは、`discovery-mode` のパラメータ `cifs domain discovered-servers` コマンドでは、次のいずれかの検出オプションを選択できます。

- ドメイン内のすべての DC が検出されます。
- ローカルサイト内の DC だけが検出されます。
 - `default-site` SMBサーバのパラメータは、`sites-and-services`でサイトに割り当てられていないLIFでこのモードを使用するように定義できます。
- サーバの検出は実行せず、優先 DC のみを使用するように SMB サーバを設定します。

このモードを使用するには、最初に SMB サーバに対して優先 DC を定義する必要があります。

ステップ

1. 目的の検出オプションを指定します。 `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

のオプション mode パラメータ：

- ° all

使用可能なすべての DC を検出します（デフォルト）。

- ° site

DC の検出対象をサイトに制限します。

- ° none

優先 DC のみを使用し、検出は実行しません。

優先ドメインコントローラを追加する

ONTAP は DNS を介してドメインコントローラを自動的に検出します。必要に応じて、特定のドメインに対する優先ドメインコントローラのリストにドメインコントローラを追加することができます。

このタスクについて

指定したドメインに優先ドメインコントローラリストがすでに存在する場合、新しいリストが既存のリストに統合されます。

ステップ

1. 優先ドメインコントローラのリストに追加するには、次のコマンドを入力します。`+vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred -dc IP_address, ...+`

`-vserver vserver_name` Storage Virtual Machine (SVM) 名を示します。

`-domain domain_name` 指定したドメインコントローラが属するドメインの完全修飾Active Directory名を指定します。

``-preferred-dc IP_address``はい。優先ドメインコントローラの1つ以上のIPアドレスを優先順にカンマで区切って指定します。

例

次のコマンドでは、SVM vs1上のSMBサーバがcifs.lab.example.comドメインへの外部アクセスを管理するために使用する優先ドメインコントローラのリストに、ドメインコントローラ172.17.102.25と172.17.102.24を追加します。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain  
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

関連情報

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの管理用コマンド

優先ドメインコントローラの追加、表示、削除を行うコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	<code>vserver cifs domain preferred-dc add</code>
優先ドメインコントローラを表示する	<code>vserver cifs domain preferred-dc show</code>
優先ドメインコントローラを削除する	<code>vserver cifs domain preferred-dc remove</code>

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

優先ドメインコントローラの追加

ドメインコントローラへの **SMB2** 接続を有効にします

ONTAP 9.1 以降では、SMB バージョン 2.0 からドメインコントローラへの接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、SMB2 がデフォルトで有効になります。

このタスクについて

。 `smb2-enabled-for-dc-connections` コマンドオプションを使用すると、使用しているONTAP のリリースに応じたシステムデフォルトが有効になります。ONTAP 9.1 のシステムデフォルトでは、SMB 1.0 が有効、SMB 2.0 が無効になります。ONTAP 9.2 のシステムデフォルトでは、SMB 1.0 が有効になり、SMB 2.0 が有効になります。ドメインコントローラは、最初に SMB 2.0 をネゴシエートし、失敗した場合は SMB 1.0 を使用します。

SMB 1.0 は、ONTAP からドメインコントローラに対して無効にすることができます。ONTAP 9.1 では、SMB 1.0 を無効にした場合、ドメインコントローラと通信するために SMB 2.0 を有効にする必要があります。

詳細情報：

- "有効なSMBのバージョンの確認"。
- "サポートされる SMB のバージョンと機能"。



状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true` ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、サーバとしてのSMB 1.0のインバウンド接続は引き続き受け入れます。

手順

1. SMBセキュリティ設定を変更する前に、有効になっているSMBのバージョンを確認します。 `vserver`

```
cifs security show
```

2. リストを下にスクロールして SMB のバージョンを確認します。
3. を使用して、該当するコマンドを実行します smb2-enabled-for-dc-connections オプション

SMB2 の設定	入力するコマンド
有効	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections true</pre>
無効	<pre>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc -connections false</pre>

ドメインコントローラへの暗号化接続を有効にします

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。

このタスクについて

ONTAP では、ドメインコントローラ（DC）通信の暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`; デフォルトは `false`。このオプションを設定すると、SMB3 でのみ暗号化がサポートされるため、SMB3 プロトコルのみが使用されます。

暗号化されたDC通信が必要な場合は、を参照してください `-smb2-enabled-for-dc-connections` ONTAP はSMB3接続のみをネゴシエートするため、このオプションは無視されます。DC が SMB3 と暗号化をサポートしていない場合、ONTAP は接続しません。

ステップ

1. DCとの暗号化通信を有効にします。

```
vserver cifs security modify -vserver svm_name  
-encryption-required-for-dc-connection true
```

非 **Kerberos** 環境のストレージにアクセスするには、**null** セッションを使用します

非 **Kerberos** 環境でストレージにアクセスする場合は、**null** セッションを使用します

null セッションアクセスは、ローカルシステムで稼働しているクライアントベースのサービスにストレージシステムデータなどのネットワークリソースへのアクセスを提供します。null セッションは、クライアントプロセスが「システム」アカウントを使用してネットワークリソースにアクセスするときに発生します。null セッション設定は非 Kerberos 認証に固有です。

ストレージシステムによる **null** セッションアクセスの実現方法

null セッション共有には認証が必要ないため、null セッションアクセスが必要なクライアントは、その IP アドレスがストレージシステムにマッピングされている必要があります

す。

デフォルトでは、マッピングされていない null セッションクライアントは、共有の列挙など一部の ONTAP システムサービスにはアクセスできますが、ストレージシステムデータへのアクセスは制限されます。



ONTAP は、で Windows RestrictAnonymous レジストリ設定値をサポートしています
-restrict-anonymous オプションにより、マッピングされていない null ユーザが表示
またはアクセスできるシステムリソースの範囲を制御できます。たとえば、共有の一覧や IPC\$
共有（非表示の名前付きパイプ共有）へのアクセスを無効にできます。。 vserver cifs
options modify および vserver cifs options show の詳細については、のマニュアル
ページを参照してください -restrict-anonymous オプション

特に設定がないかぎり、null セッションでストレージシステムアクセスを要求するローカルプロセスを実行しているクライアントは、「everyone」などの制限のないグループのみのメンバーとなります。null セッションアクセスを選択したストレージシステムリソースに制限するには、すべての null セッションクライアントが属するグループを作成します。このグループを作成すると、ストレージシステムアクセスを制限したり、null セッションクライアントのみに適用されるストレージシステムリソース権限を設定したりできます。

ONTAP には、マッピング構文が用意されています vserver name-mapping null ユーザセッションを使用したストレージシステムリソースへのアクセスを許可するクライアントの IP アドレスを指定するコマンドセット。null ユーザ用のグループを作成したら、null セッションのみに適用されるストレージシステムリソースのアクセス制限およびリソース権限を指定できます。null ユーザは匿名ログオンとみなされます。null ユーザは、ホームディレクトリにアクセスできません。

マッピングされた IP アドレスからストレージシステムにアクセスするすべての null ユーザには、マッピングされたユーザ権限が付与されます。null ユーザにマッピングされたストレージシステムへの不正なアクセスを防止するため、適切な予防措置を検討してください。最大限の保護を実現するには、ストレージシステムと null ユーザによるストレージシステムアクセスが必要なすべてのクライアントを別のネットワークに配置し、IP アドレス「SVM」の問題を解消します。

関連情報

[匿名ユーザのアクセス制限を設定します](#)

null ユーザにファイルシステム共有へのアクセスを許可します

null セッションクライアントによるストレージシステムリソースへのアクセスを許可するには、null セッションクライアントに使用するグループを割り当てて null セッションクライアントの IP アドレスを記録し、ストレージシステム上の、null セッションを使用したデータアクセスを許可するクライアントリストにその IP アドレスを追加します。

手順

1. 使用します vserver name-mapping create IP 修飾子を使用して、null ユーザを任意の有効な Windows ユーザにマッピングするコマンド。

次のコマンドは、有効なホスト名 google.com で user1 に null ユーザをマッピングします。

```
vserver name-mapping create -direction win-unix -position 1 -pattern  
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```


次のコマンドは、有効な IP アドレス 10.238.2.54/32 で user1 に null ユーザをマッピングします。

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. を使用します vserver name-mapping show コマンドを入力してネームマッピングを確認します。

```
vserver name-mapping show

Vserver:    vs1
Direction:  win-unix
Position Hostname      IP Address/Mask
-----
1          -           10.72.40.83/32      Pattern: anonymous logon
                                   Replacement: user1
```

3. を使用します vserver cifs options modify -win-name-for-null-user nullユーザにWindows メンバーシップを割り当てるコマンド。

このオプションは、null ユーザに有効なネームマッピングが設定されている場合にのみ使用できます。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. を使用します vserver cifs options show コマンドを使用して、nullユーザのWindowsユーザまたはグループへのマッピングを確認します。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

SMB サーバの NetBIOS エイリアスを管理します

SMB サーバ用の NetBIOS エイリアスの概要を管理します

NetBIOS エイリアスは、SMB クライアントが SMB サーバに接続するときに使用できる SMB サーバの別名です。SMB サーバの NetBIOS エイリアスを設定すると、他のファイルサーバのデータを SMB サーバに統合して、SMB サーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

SMB サーバの作成時または SMB サーバ作成後の任意の時点で、NetBIOS エイリアスのリストを指定できます。リストへの NetBIOS エイリアスの追加や削除は、いつでも行うことができます。SMB サーバには

NetBIOS エイリアスリスト内のどの名前を使用しても接続できます。

関連情報

[NetBIOS over TCP 接続に関する情報を表示する](#)

SMBサーバにNetBIOSエイリアスのリストを追加する

エイリアスを使用してSMBサーバに接続できるようにするには、NetBIOSエイリアスのリストを作成するか、既存のNetBIOSエイリアスのリストにNetBIOSエイリアスを追加します。

このタスクについて

- NetBIOS エイリアス名は 15 文字以内にする必要があります。
- SMBサーバには最大200個のNetBIOSエイリアスを設定できます。
- 次の文字は使用できません。

@#* () =+[] ; : "、 <> \ ?

手順

1. NetBIOSエイリアスを追加します。+ vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,...

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- 1 つ以上の NetBIOS エイリアスをカンマで区切って指定します。
- 指定した NetBIOS エイリアスが既存のリストに追加されます。
- 現在のリストが空である場合、NetBIOS エイリアスの新しいリストが作成されます。

2. NetBIOSエイリアスが正しく追加されたことを確認します。vserver cifs show -vserver vserver_name -display-netbios-aliases

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

関連情報

[NetBIOS エイリアスリストからの NetBIOS エイリアスの削除](#)

[CIFS サーバの NetBIOS エイリアスのリストを表示する](#)

NetBIOS エイリアスリストから NetBIOS エイリアスを削除します

CIFS サーバで特定の NetBIOS エイリアスが不要な場合、その NetBIOS エイリアスをリストから削除できます。リストからすべての NetBIOS エイリアスを削除することもできます。

このタスクについて

複数の NetBIOS エイリアスを削除するには、カンマで区切って指定します。を指定すると、CIFSサーバ上のすべてのNetBIOSエイリアスを削除できます - をの値として指定します -netbios-aliases パラメータ

手順

- 1. 次のいずれかを実行します。

削除する項目	入力するコマンド
リスト内の特定の NetBIOS エイリアス	<code>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios-aliases _NetBIOS_alias_,...</code>
リスト内のすべての NetBIOS エイリアス	<code>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</code>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

- 2. 指定したNetBIOSエイリアスが削除されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

Vserver: vs1

Server Name: CIFS_SERVER

NetBIOS Aliases: ALIAS_2, ALIAS_3

CIFS サーバの NetBIOS エイリアスのリストを表示します

NetBIOS エイリアスのリストを表示できます。これは、SMB クライアントが CIFS サーバへの接続に使用できる名前を確認する場合に役立ちます。

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
CIFS サーバの NetBIOS エイリアス	<code>vserver cifs show -display-netbios-aliases</code>
NetBIOS エイリアスのリストを含む詳細な CIFS サーバ情報	<code>vserver cifs show -instance</code>

次の例は、CIFS サーバの NetBIOS エイリアスに関する情報を表示します。

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

      Server Name: CIFS_SERVER
      NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

次の例は、NetBIOS エイリアスのリストを CIFS サーバの詳細情報の一部として表示します。

```
vserver cifs show -instance
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_SERVER
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

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。

関連情報

[CIFS サーバへの NetBIOS エイリアスのリストの追加](#)

[CIFS サーバの管理用コマンド](#)

SMB クライアントが **NetBIOS** エイリアスを使用して接続しているかどうかを確認します

SMB クライアントが NetBIOS エイリアスを使用して接続しているかどうか、および使用している場合はその NetBIOS エイリアスを確認できます。これは、接続の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。

このタスクについて

を使用する必要があります `-instance` SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するためのパラメータ。CIFSサーバの名前またはIPアドレスを使用してSMB接続を確立している場合は、の出力が表示されます `NetBIOS Name` フィールドはです - （ハイフン）。

ステップ

1. 必要な操作を実行します。

表示する NetBIOS 情報	入力するコマンド
SMBセツソク	<code>vserver cifs session show -instance</code>
指定した NetBIOS エイリアスを使用する接続：	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

次の例は、セッション ID 1 の SMB 接続に使用されている NetBIOS エイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

その他の **SMB** サーバタスクを管理します

CIFS サーバを停止または起動します

ユーザが SMB 共有を介してデータにアクセスしていない間に作業を行う場合は、SVM 上の CIFS サーバを停止すると便利です。SMB アクセスを再開するには、CIFS サーバを起動します。CIFS サーバを停止することによって、Storage Virtual Machine（SVM）で許可されているプロトコルを変更できます。

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
CIFS サーバを停止します	<code>`vserver cifs stop -vserver vserver_name [-foreground {true</code>
<code>false}]`</code>	CIFS サーバを起動します
<code>`vserver cifs start -vserver vserver_name [-foreground {true</code>	<code>false}]`</code>

-foreground コマンドをフォアグラウンドとバックグラウンドのどちらで実行するかを指定します。省略した場合、このパラメータはに設定されます `true` コマンドはフォアグラウンドで実行されます。

- 2. を使用して、CIFSサーバの管理ステータスが正しいことを確認します `vserver cifs show` コマンドを実行します

例

次のコマンドは、SVM vs1 の CIFS サーバを起動します。

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                NetBIOS Domain/Workgroup Name: DOMAIN
                Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                CIFS Server Administrative Status: up
```

関連情報

[検出されたサーバに関する情報を表示する](#)

[サーバのリセットおよび再検出](#)

CIFS サーバを別の OU に移動します

CIFS サーバの create プロセスでは、別の OU を指定しないかぎり、セットアップ時にデフォルトの Organizational Unit （OU；組織単位）CN=Computers が使用されます。CIFS サーバはセットアップ後でも別の OU に移動できます。

手順

1. Windows サーバーで、* Active Directory ユーザーとコンピューター * ツリーを開きます。
2. Storage Virtual Machine （SVM）の Active Directory オブジェクトを見つけます。
3. オブジェクトを右クリックし、* 移動 * （* Move *）を選択します。
4. SVM に関連付ける OU を選択します

結果

選択した OU に、SVM オブジェクトが移動します。

SMB サーバを移動する前に、SVM 上の動的 DNS ドメインを変更します

SMB サーバを別のドメインに移動する際に、SMB サーバの DNS レコードが Active Directory に統合された DNS サーバによって DNS に動的に登録されるようにするには、SMB サーバを移動する前に Storage Virtual Machine （SVM）上の動的 DNS （DDNS）を変更する必要があります。

作業を開始する前に

SMB サーバコンピュータアカウントを含む新しいドメインのサービスロケーションレコードを含む DNS ドメインを使用するには、SVM で DNS ネームサービスを変更する必要があります。セキュア DDNS を使用している場合は、Active Directory に統合された DNS ネームサーバを使用する必要があります。

このタスクについて

DDNS （SVM 上で設定されている場合）はデータ LIF の DNS レコードを新しいドメインに自動的に追加しますが、元のドメインの DNS レコードは元の DNS サーバから自動的に削除されません。手動で削除する必要があります。

SMB サーバを移動する前に DDNS の変更を完了するには、次のトピックを参照してください。

["動的 DNS サービスを設定する"](#)

SVM を Active Directory ドメインに追加します

を使用してドメインを変更すると、既存のSMBサーバを削除することなくStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify` コマンドを実行します現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

作業を開始する前に

- SVM の DNS 設定が完了している必要があります。
- SVM の DNS 設定がターゲットドメインを提供できる必要があります。

DNS サーバには、ドメイン LDAP およびドメインコントローラサーバのサービスロケーションレコード（SRV）が含まれている必要があります。

このタスクについて

- Active Directory ドメインの変更を続行するには、CIFS サーバの管理ステータスを「所有」に設定する必要があります。
- コマンドが正常に完了すると、管理ステータスは自動的に「up」に設定されます。
- ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

手順

1. SVMをCIFSサーバドメインに追加します。 `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

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 `vserver cifs modify` コマンドを実行します新しいドメイン用にDNSを再設定する必要がある場合は、のマニュアルページを参照してください `vserver dns modify` コマンドを実行します

SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限があるWindowsアカウントの名前とパスワードを指定する必要があります `ou= example ou` 内のコンテンツ `example.com` ドメイン。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 `keytab` ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

2. CIFSサーバが目的のActive Directoryドメイン内にあることを確認します。 `vserver cifs show`

例

次の例では、SVM `vs1` 上にある SMB サーバ「`CIFSSERVER1`」を `keytab` 認証を使用して `example.com` ドメインに追加します。

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab
```

```
cluster1::> vserver cifs show
```

	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

NetBIOS over TCP 接続に関する情報を表示します

NetBIOS over TCP（NBT）接続に関する情報を表示できます。これは、NetBIOSに関連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。

ステップ

1. を使用します `vserver cifs nbtstat` NetBIOS over TCP接続に関する情報を表示するコマンド。



IPv6 経由の NetBIOS ネームサービス（NBNS）はサポートされていません。

例

次の例は、「cluster1」について表示される NetBIOS ネームサービスの情報を示しています。

```
cluster1::> vserver cifs nbtstat

Vserver: vs1
Node:    cluster1-01
Interfaces:
    10.10.10.32
    10.10.10.33
Servers:
    17.17.1.2  (active )
NBT Scope:
    [ ]
NBT Mode:
    [h]
NBT Name      NetBIOS Suffix  State   Time Left   Type
-----
CLUSTER_1    00                wins    57
CLUSTER_1    20                wins    57

Vserver: vs1
Node:    cluster1-02
Interfaces:
    10.10.10.35
Servers:
    17.17.1.2  (active )
CLUSTER_1    00                wins    58
CLUSTER_1    20                wins    58
4 entries were displayed.
```

SMBサーバの管理用コマンド

作成、表示、変更、停止、開始、およびSMBサーバを削除しています。また、サーバのリセットと再検出、マシンアカウントパスワードの変更またはリセット、マシンアカウントパスワードのスケジュール変更、NetBIOS エイリアスの追加または削除を行うコマンドもあります。

状況	使用するコマンド
----	----------

SMB サーバを作成	<code>vserver cifs create</code>
SMB サーバに関する情報を表示する	<code>vserver cifs show</code>
SMBサーバを変更する	<code>vserver cifs modify</code>
SMB サーバを別のドメインに移動する	<code>vserver cifs modify</code>
SMB サーバを停止	<code>vserver cifs stop</code>
SMB サーバを起動	<code>vserver cifs start</code>
SMBサーバを削除する	<code>vserver cifs delete</code>
SMBサーバ用のサーバのリセットと再検出	<code>vserver cifs domain discovered-servers reset-servers</code>
SMBサーバのマシンアカウントパスワードを変更する	<code>vserver cifs domain password change</code>
SMBサーバのマシンアカウントパスワードをリセットする	<code>vserver cifs domain password change</code>
SMBサーバのマシンアカウントの自動パスワード変更のスケジュールを設定する	<code>vserver cifs domain password schedule modify</code>
SMBサーバ用のNetBIOSエイリアスを追加する	<code>vserver cifs add-netbios-aliases</code>
SMBサーバのNetBIOSエイリアスを削除する	<code>vserver cifs remove-netbios-aliases</code>

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

["SMB サーバを削除したときにローカルユーザとローカルグループが受ける影響"](#)

NetBIOS ネームサービスを有効にします

ONTAP 9 以降では、NetBIOS ネームサービス（NBNS、Windows Internet Name Service または WINS と呼ばれることもあります）はデフォルトで無効になっています。以前は、WINS がネットワークで有効かどうかに関係なく、CIFS 対応 Storage Virtual Machine（SVM）が名前登録のブロードキャストを送信していました。NBNS が必須の構成でのみこのブロードキャストが送信されるようにするには、新しい CIFS サーバに対して NBNS を明示的に有効にする必要があります。

作業を開始する前に

- すでに NBNS を使用しているシステムを ONTAP 9 にアップグレードした場合、このタスクを実行する必要はありません。NBNS はそれまでと同様に機能します。
- NBNS は UDP（ポート 137）経由で有効になります。
- IPv6 経由の NBNS はサポートされていません。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. CIFS サーバで NBNS を有効にします。

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled  
true
```

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

SMB アクセスと SMB サービスに IPv6 を使用します

IPv6 を使用するための要件

SMB サーバで IPv6 を使用する前に、この機能をサポートする ONTAP および SMB のバージョンとライセンスの要件について確認しておく必要があります。

ONTAP ライセンスの要件：

SMB のライセンスがあれば、IPv6 を使用するために特別なライセンスは必要ありません。SMB ライセンスには含まれています。"ONTAP One"。ONTAP One をお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB プロトコルのバージョン

- SVM について ONTAP は、すべてのバージョンの SMB プロトコルで IPv6 がサポートされます。



IPv6 経由の NetBIOS ネームサービス（NBNS）はサポートされていません。

SMB アクセスと CIFS サービスでの IPv6 のサポート

CIFS サーバで IPv6 を使用する場合は、ONTAP による SMB アクセスや CIFS サービスとのネットワーク通信での IPv6 のサポートについて確認しておく必要があります。

Windows クライアントおよびサーバのサポート

ONTAP では、IPv6 をサポートする Windows サーバおよびクライアントをサポートしています。次に、Microsoft Windows クライアントおよびサーバによる IPv6 のサポートについて説明します。

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012 以降では、SMB ファイル共有と、DNS、LDAP、CLDAP、Kerberos サービスなどの Active Directory サービスの両方で IPv6 がサポートされます。

IPv6 アドレスが設定されている場合、Windows 7 および Windows Server 2008 以降のリリースでは、Active Directory サービスに対してデフォルトで IPv6 が使用されます。IPv6 接続による NTLM 認証と Kerberos 認証の両方がサポートされます。

ONTAP でサポートされる Windows クライアントでは、いずれも IPv6 アドレスを使用して SMB 共有に接続できます。

ONTAPがサポートするWindowsクライアントに関する最新情報については、を参照してください。 ["互換性マトリックス"](#)。



NT ドメインは IPv6 ではサポートされません。

その他の **CIFS** サービスもサポートされます

ONTAP では、SMB ファイル共有と Active Directory サービスに加え、以下に対しても IPv6 をサポートしています。

- クライアント側のサービス：オフラインフォルダ、移動プロファイル、フォルダリダイレクト、以前のバージョン機能など
- サーバ側のサービス：動的ホームディレクトリの有効化（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、BranchCache、ODX コピーオフロード、自動ノードリファール、および以前のバージョン
- ファイルアクセス管理用のサービス：Windows のローカルユーザやローカルグループを使用したアクセス制御と権限の管理、CLI を使用したファイル権限や監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、SMB アクティビティの監視などが可能です
- NAS のマルチプロトコルの監査
- FPolicy の
- 共有の継続的な可用性、監視プロトコル、およびリモート VSS（Hyper-V over SMB 構成で使用）

ネームサービスおよび認証サービスのサポート

次のネームサービスとの通信が IPv6 でサポートされます。

- ドメインコントローラ
- DNS サーバ
- LDAPサーバ
- KDCサーバ
- NISサーバ

要件に対応した設定を作成するには、CIFS サーバが外部サーバへの接続を確立するときに IPv6 がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択

外部サーバへの接続を試行する場合、選択する送信元アドレスは宛先アドレスと同じタイプでなければなりません。たとえば、IPv6 アドレスに接続する場合、CIFS サーバをホストする Storage Virtual Machine (SVM) には、送信元アドレスとして使用する IPv6 アドレスを持つデータ LIF または管理 LIF が必要です。同様に、IPv4 アドレスに接続する場合、SVM には、送信元アドレスとして使用する IPv4 アドレスを持つデータ LIF または管理 LIF が必要です。

- DNS を使用して動的に検出されるサーバの場合、サーバ検出は次のように実行されます。

- クラスタで IPv6 が無効になっている場合は、IPv4 サーバアドレスのみが検出されます。
- クラスタで IPv6 が有効になっている場合は、IPv4 と IPv6 の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうかと、IPv6 または IPv4 のデータ LIF または管理 LIF が使用可能かどうかに応じて、いずれかのタイプが使用されます。動的サーバ検出は、ドメインコントローラとその関連サービス (LSA、NETLOGON、Kerberos、LDAP など) の検出に使用されます。

- DNS サーバへの接続

SVM が DNS サーバに接続するときに IPv6 を使用するかどうかは、DNS ネームサービスの設定によって決まります。IPv6 アドレスを使用するように DNS サービスが設定されている場合は、IPv6 を使用して接続が確立されます。必要に応じて、DNS サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、DNS ネームサービスの設定で IPv4 アドレスを使用できます。DNS ネームサービスの設定時に、IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。

- LDAPサーバへの接続

SVM が LDAP サーバに接続するときに IPv6 を使用するかどうかは、LDAP クライアントの設定によって決まります。IPv6 アドレスを使用するように LDAP クライアントが設定されている場合は、IPv6 を使用して接続が確立されます。必要に応じて、LDAP サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、LDAP クライアントの設定で IPv4 アドレスを使用できます。LDAP クライアントの設定時に、IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。



LDAP クライアントの設定は、UNIX ユーザ、グループ、およびネットグループのネームサービス用に LDAP を設定するときに使用されます。

- NISサーバへの接続

SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネームサービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続で引き続きIPv4アドレスを使用できるように、NISネームサービスの設定でIPv4アドレスを使用できます。NISネームサービスの設定時に、IPv4アドレスとIPv6アドレスを組み合わせて指定できます。



NIS ネームサービスは、UNIX ユーザ、グループ、ネットグループ、およびホスト名オブジェクトを格納および管理するために使用されます。

SMB での IPv6 の有効化（クラスタ管理者のみ）

IPv6 SMB セッション情報の監視および表示

SMB での IPv6 の有効化（クラスタ管理者のみ）

IPv6 ネットワークはクラスタのセットアップ時には有効になりません。SMB で IPv6 を使用するには、クラスタのセットアップ後にクラスタ管理者が IPv6 を有効にする必要があります。クラスタ管理者が IPv6 を有効にすると、IPv6 はクラスタ全体で有効になります。

ステップ

1. IPv6 を有効にします。 `network options ipv6 modify -enabled true`

クラスタでの IPv6 の有効化と IPv6 LIF の設定の詳細については、[_ ネットワーク管理ガイド _](#) を参照してください。

IPv6 が有効になっている。SMB アクセス用の IPv6 データ LIF を設定できます。

関連情報

IPv6 SMB セッション情報の監視および表示

"Network Management の略"

SMB で IPv6 を無効にします

クラスタで IPv6 を有効にするにはネットワークオプションを使用しますが、同じコマンドを使用して SMB での IPv6 を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後に IPv6 を有効にしたインターフェイスを無効にすると、ONTAP は IPv6 を無効にします。IPv6 を有効にしたインターフェイスの管理については、クラスタ管理者と連絡を取る必要があります。

クラスタでの IPv6 の無効化の詳細については、[_ ネットワーク管理ガイド _](#) を参照してください。

関連情報

"Network Management の略"

IPv6 SMB セッション情報を監視および表示します

IPv6 ネットワークで接続されている SMB セッション情報を監視および表示できます。この情報は、IPv6 SMB セッションに関する他の有用な情報と同様、IPv6 を使用して接続するクライアントを決定する上で役に立ちます。

ステップ

1. 必要な操作を実行します。

確認する項目	入力するコマンド
Storage Virtual Machine（SVM）への SMB セッションは、IPv6 を使用して接続されます	<code>vserver cifs session show -vserver vserver_name -instance</code>
特定の LIF アドレスにより、SMB セッションに IPv6 を使用します	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance</code> <i>LIF_IP_address</i> は、データLIFのIPv6アドレスです。

SMB を使用したファイルアクセスをセットアップする

セキュリティ形式を設定する

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とは

セキュリティ形式には、UNIX、NTFS、mixed、および unified の 4 種類があり、セキュリティ形式ごとに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	「UNIX」	NTFS	SMB	NTFS ACL
NTFS	混在	NFS または SMB	NFSv3 モードビット	「UNIX」
NFSv4.x ACL	「UNIX」	NTFS ACL	NTFS	統合：

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
NFS または SMB	NFSv3 モードビット	「UNIX」	NFSv4.1 ACL	「UNIX」
NTFS ACL	NTFS	統合：（ONTAP 9.4 以前のリリースでは、Infinite Volume のみ）。	NFS または SMB	NFSv3 モードビット
「UNIX」	NFSv4.1 ACL			NTFS ACL

FlexVol ボリュームでは、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 の場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。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"](#)。

ONTAP 9.2以降では、show-effective-permissions パラメータをに設定します vserver security file-directory コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindows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も指定します -share-name 有効な共有権限を表示できます。



ONTAP で、最初にデフォルトのファイル権限がいくつか設定されます。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ついては、セキュリティ形式は UNIX、権限の種類は UNIX モードビット（特に指定しないかぎり 0755）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。NTFS セキュリティ形式のボリュームにあるデータについては、デフォルトで NTFS セキュリティ形式が有効になり、すべてのユーザにフルコントロール権限を許可する 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します

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。第1の要素は、ファイルシステムを管理する管理者のタイプです。第2の要素は、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。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して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。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「UNIX」	<ul style="list-style-type: none"> ファイルシステムが UNIX 管理者によって管理される。 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、サービスアカウントとして UNIX ユーザが使用される。
NTFS	<ul style="list-style-type: none"> 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、サービスアカウントとして Windows ユーザが使用される。
混在	ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

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。

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 ルートボリュームのセキュリティ形式を設定する

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. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

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、です `unix`、`ntfs` または `mixed`。

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 ボリュームのセキュリティ形式を設定する

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 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。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	<code>volume create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

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

FlexVol ボリューム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。

詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください ["論理ストレージ管理"](#)。

2. 作成した FlexVol ボリューム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 にセキュリティ形式を設定する

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 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
はまだ存在しません	<code>volume qtree create</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。
はすでに存在します	<code>volume qtree modify</code> を含めます <code>-security-style</code> セキュリティ形式を指定するパラメータ。

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

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`。

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

- 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 ネームスペース内でデータボリュームを作成および管理します

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および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します

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。

作業を開始する前に

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

- ジャンクションポイントを指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、ディレクトリおよび結合されたボリュームを含むことができます。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に適用されている形式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は適切でないセキュリティ形式である場合もあります。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、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。/ENG はと同じです /eng。CIFS 共有を作成する場合、Windows では、ジャンクションパスがあたかも大文字と小文字の区別があるかのように扱わ

れます。たとえば、ジャンクションがの場合などです /ENG、CIFS共有のパスは次の文字で始まる必要があります。 /ENG`ではありません ` /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。これらの機能の詳細については、のマニュアルページを参照してください volume create コマンドを実行します

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 vs1 -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上に作成します /eng/home :

```
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
```

Vserver	Volume	Active	Junction Path	Junction 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

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マウントされず、NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

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 vs1 -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に適用されている形式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は適切でないセキュリティ形式である場合もあります。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、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。これら

の機能の詳細については、のマニュアルページを参照してください volume create コマンドを実行します

2. 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が作成されたことを確認します。 volume show -vserver vs1 -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
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

NAS ネームスペース内の既存のボリュームをマウントまたはアンマウントします

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。ボリュームはアンマウントすることもできます。

このタスクについて

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。



NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純に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、次の技術情報アート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およびボリュームまたはディレクトリ上に作成された 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れば、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内のデータにアクセスできるようになります。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	<code>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</code>
ボリュームをアンマウントします	<code>volume unmount -vserver svm_name -volume volume_name</code> <code>volume offline -vserver svm_name -volume volume_name</code>

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に関する情報を表示します

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。また、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	<code>volume show -vserver vs1 -junction</code>
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	<code>volume show -vserver vs1 -volume volume_name -instance</code>
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	<p>a. 必要に応じて、の有効なフィールドを表示できます <code>-fields</code> パラメータを指定するには、次のコマンドを使用します。 <code>volume show -fields ?</code></p> <p>b. を使用して、必要な情報を表示します <code>-fields</code> パラメータ：<code>volume show -vserver vs1 -fields fieldname、.....</code></p>

例

次の例は、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
```

Vserver	Volume	Active	Junction Path	Junction 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								

ネームマッピングを設定する

ネームマッピングの概要を設定する

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 クライアントからの接続か CIFS クライアントからの接続かに関係なく、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 環境を構成した場合、ボリュームに対して CIFS アクセスまたは NTFS セキュリティ形式を使用する予定はありません。
- 代わりにデフォルトユーザを使用するように設定している場合。

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ません。

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 という単語が先頭または末尾に付くすべての 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 が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、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。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 ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。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。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。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、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、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。

マシンアカウントに定義されているネームマッピングがあっても無視されます。

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 に与える影響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、インバウンドとアウトバウンドの 2 つのタイプがある単方向の信頼のどちら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しています。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、このホームドメインは信頼できるドメインに属しているユーザを認証および認可でき、その反対に、この信頼できるドメインはホームドメインに属しているユーザを認証および認可することができます。

UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に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、ホームドメインが他方のドメインを信頼しています。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しているユーザを認証および認可できます。

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、CIFS サーバのホームドメインが他方のドメインによって信頼されています。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しているユーザを認証または認可できません。

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のためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、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容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（ Pattern ）	交換	結果
ルート	<ul style="list-style-type: none"> • \\ 管理者 	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。
*	**	<p>有効な UNIX ユーザは、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。</p> <div>  <p>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。</p> </div>

マルチドメインの名前検索の実行方法

マルチドメインの名前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方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

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、マッピング先の Windows ユーザはこの検索リスト内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にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、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は、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 プログラム。

ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。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。

このタスクについて

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`



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

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、優先順位リスト内での位置は 1 番目です。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::> vsriver name-mapping create -direction win-unix -position 1
-pattern ENG\\john$ops
-replacement john_ops
```

デフォルトユーザを設定します。

ユーザに対する他のマッピングの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。ただし、マッピングされていないユーザの認証を失敗にする場合は、デフォルトユーザを設定しないでください。

このタスクについて

CIFS 認証で、各 Windows ユーザを個別の UNIX ユーザにマッピングしないようにする場合は、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 ユーザを個別の Windows ユーザにマッピングしないようにする場合は、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	<code>vsriver cifs options modify -default -unix-user user_name</code>
デフォルトの Windows ユーザを設定します	<code>vsriver nfs modify -default-win-user user_name</code>

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します	<code>vsriver name-mapping create</code>
特定の位置にネームマッピングを挿入します	<code>vsriver name-mapping insert</code>
ネームマッピングを表示します	<code>vsriver name-mapping show</code>

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入れ替えます  ネームマッピングが IP 修飾子エントリで設定されている場合は交換できません。	<code>vserver name-mapping swap</code>
ネームマッピングを変更する	<code>vserver name-mapping modify</code>
ネームマッピングを削除する	<code>vserver name-mapping delete</code>
ネームマッピングが正しいことを確認します	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win</code> <code>-user-name user1 -path / -share-name sh1</code>

詳細については、各コマンドのマニュアルページを参照してください。

マルチドメインネームマッピング検索を設定する

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します

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。

このタスクについて

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	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-trusted-domain-enum -search-enabled true</code>
無効	<code>vserver cifs options modify -vserver <i>vserver_name</i> -is-trusted-domain-enum -search-enabled false</code>

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をリセットして再検出します

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。CIFS サーバのコンピュータアカウントを含むドメインであるホームドメインと双方向の信頼が確立されたドメインのみが検出されます。

ステップ

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

```
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を表示する](#)

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

CIFS サーバのホーム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。ホームドメインとは、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です。これは、検出される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把握する場合に役立ちます。

このタスクについて

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 が決めた順序で返すため、リスト内のドメインの順序は予測できません。信頼できるドメインのリストを表示すると、マルチドメインネームマッピングの検索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. 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` コマンドを実行します

```
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に含まれる信頼できるドメインを追加、削除、または置換します

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関係にあるドメインの代わりにこのリストが使用されます。

このタスクについて

- 信頼できるドメインを既存のリストに追加すると、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、双方向の信頼関係にあるドメインのみ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せんが、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にある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します	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...</code>
信頼できるドメインをリストから削除します	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]</code>
既存のリストを変更します	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...</code>

例

次のコマンドは、SVM vs1 が使用す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
```

次のコマンドを実行すると、SVM vs1 で使用されるリストから信頼できるドメインが 2 つ削除されます。

```
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 で使用されてい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を表示する](#)

信頼できるドメインの優先リストに関する情報を表示します

信頼できるドメインの優先リストに含まれ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）ごと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	<code>vserver cifs domain name-mapping-search show</code>
指定した SVM のすべての信頼できる優先ドメインを指定します	<code>vserver cifs domain name-mapping-search show -vserver vserver_name</code>

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に含まれる信頼できるドメインの追加、削除、または置換](#)

SMB 共有を作成および設定

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 共有とは、ボリューム内に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 および SQL Server 向けの SMB の設定"](#)

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

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は作成されなくなりました。

- IPC \$
- admin\$ (ONTAP 9.7以前のみ)
- c\$

末尾が \$ 文字であ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することはできます。

ipc\$ および **admin\$** デフォルト管理共有の用途

ipc\$ および admin\$ 共有は ONTAP が使用するものであり、Windows 管理者が SVM 上にある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、プログラム間通信に必要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や、コンピュータの共有リソースを表示する際に使用されます。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\$ 共有の名前の変更や削除もできません。

- 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は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\$ 共有の名前の変更や削除もできません。

c\$ デフォルト共有の用途

c\$ 共有は、クラスタまたは SVM の管理者が SVM のルートボリュームへのアクセスおよび管理に使用できる管理共有です。

c\$ 共有には、次のような特徴があります。

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

このユーザは、BUILTIN\administrator です。デフォルトで、BUILTIN\administrator を共有にマッピングでき、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の表示、作成、変更、削除が可能です。このディレクトリ内のファイルおよび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\$ 共有の設定や共有プロパティは変更できます。
- 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によって、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 ノセキュリティタブラシヨウシタショウサイナ NTFS ファイルアクセスケンノセツテイ](#)

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 の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あり、次の要件が含まれています。

- 共有名は SMB サーバでそれぞれ一意にする必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大長は 80 文字です。
- 共有名では Unicode がサポートされます。
- \$ 記号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\$、c\$ 管理共有は、すべての CIFS サーバ上に自動的に作成され、共有名が予約されます。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 ONTAP_ADMIN\$ という共有名は使用できません。
- 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の使用がサポートされます。

! @ # \$ % & ' _ . ~ () { }

- SMB 共有の名前では次の特殊文字の使用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す /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 共有プロパティの概要を使用する

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を使用することを指定します。これはクライアント側キャッシュとも呼ばれます。
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。
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。

共有プロパティ	説明
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	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。各ユーザのアクセス権に基づいて ABE フィルタを適用した共有フォルダがユーザに表示され、そのユーザがアクセス権を持たないフォルダやその他の共有リソースは表示されないようにします。
namespace-caching	このプロパティは、この共有に接続する SMB クライアントが、CIFS サーバから返された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 暗号化の使用を義務付けます。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。

既存の **SMB** 共有に対する共有プロパティを追加または削除します

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。この方法は、環境内での要件の変化に合わせて共有の設定を変更する場合に便利です。

作業を開始する前に
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。

このタスクについて
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。

- ・カンマで区切って指定することで、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、共有プロパティの既存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。
- ・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` コマンドを実行します

を使用できます `vserver cifs share properties remove` 共有プロパティを削除するコマンド。

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。

- ・カンマで区切って指定することで、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. 適切な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します	<code>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>
共有プロパティを削除します	<code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>

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

次のコマンドは、を追加します `showsnapshot SVM vs1`上の「share1」という名前の共有に共有プロパティを設定します。


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

```
cluster1::> vservers cifs share show -vservers vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	share1	/share1	oplocks	-	Everyone / Full
Control			browsable changenotify showsnapshot		

次のコマンドでは、が削除されます browsable SVM vs1上の「share2」という名前の共有から共有プロパティを指定します。

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

```
cluster1::> vservers cifs share show -vservers 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 共有設定を使用して、**SMB** ユーザアクセスを最適化します

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確実にアクセスできるようになります。

force-group の指定は、共有が UNIX または mixed qtree 内にある場合にのみ有効です。NTFS セキュリティ形式のボリュームまたは qtree にある共有内のファイルへのアクセスは、UNIX の GID ではなく Windows の権限によって判断されるため、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、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、通常はプライマリ GID または UID を使用してアクセスできないファイルにこの共有内のファイルにアクセスできるようになります。

- 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、同じフォースグループに属します。

SMB ユーザが、NFS ユーザによって作成されたファイルにアクセスしようとする、SMB ユーザのプライマリ GID によって、権限があるかどうか判断されます。

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を与えません。NFS ユーザが作成したファイルは、ファイル所有者から GID を取得します。アクセス権限の決定は、ファイルにアクセスしようとしている NFS ユーザの UID およびプライマリ GID に基づきます。

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確実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。そのため、Engineering グループと Marketing グループのユーザの権限を管理しなくても、すべてのユーザがこの共有に書き込むことができます。

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** 共有を作成します

UNIX ファイルセキュリティ形式のボリュームや qtree にあるデータにアクセスする SMB ユーザが、同じ UNIX グループに属していると ONTAP で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

UNCパスの場合 (\\servername\sharename\filepath) が256文字を超えています (先頭の「\\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 問題ではなく Windows クライアント問題です。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、共有をいつでも変更し、の値として空の文字列(″)を指定できます -force-group-for-create パラメータ共有を変更して 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

次のコマンドを実行すると、Webからアクセスできる「webpages」共有が作成されます
/corp/companyinfo 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ているディレクトリ：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
```

```
/corp/companyinfo -force-group-for-create webgroup1
```

関連情報

[force-group 共有設定を使用して、SMB ユーザアクセスを最適化します](#)

MMC を使用して **SMB** 共有情報を表示します

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。

このタスクについて

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

この処理がサポートされていない場合は、が表示されることがあります remote procedure call failed エラー。

"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

を使用します `vserver cifs share` および `vserver cifs share properties` SMB共有を管理するコマンド。

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

詳細については、各コマンドのマニュアルページを参照してください。

SMB 共有の ACL を使用してファイルアクセスを保護

SMB 共有レベル ACL の管理に関するガイドラインを次に示します

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。

共有を作成すると、共有レベルの ACL のデフォルトでは、Everyone という名前の標準グループに読み取りアクセス権が与えられます。ACL に読み取りアクセス権が設定されているため、ドメイン内およびすべての信頼できるドメイン内のすべてのユーザに共有への読み取り専用アクセス権が与えられます。

共有レベルの ACL を変更するには、Windows クライアントの Microsoft 管理コンソール（MMC）または ONTAP コマンドラインを使用します。

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を作成

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。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名、あるいは UNIX ユーザまたはグループ名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ます。`Everyone / Full Control`は、セキュリティリスクをもたらします。

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	<pre>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</pre>
Windows グループ	<pre>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</pre>
UNIX ユーザ	<pre>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</pre>
UNIX グループ	<pre>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</pre>

3. 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` コマンドを実行します

例

次のコマンドは、を示しています Change SVM 「vs1.example.com」 上の「sales」共有に対する「Sales Team」 Windowsグループへの権限：

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

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access 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、を示しています Read SVM 「vs2.example.com」 上の 「eng」 共有の 「engineering」 UNIX グループへの権限：

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

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

以下のコマンドで説明します Change 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 Full_Control SVM 「vs1」 の 「datavol5」 共有に対する 「Sue Chang」という名前のWindowsローカルユーザの権限：

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

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

```
cluster1::> vsriver cifs share access-control show -vsriver vs1
```

Vsriver	Share	User/Group	User/Group	Access
Permission	Name	Name	Type	
-----	-----	-----	-----	
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

アクセス制御リスト（ACL）の作成、表示、変更、削除など、SMB の ACL 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	<code>vsriver cifs share access-control create</code>
ACL を表示します	<code>vsriver cifs share access-control show</code>
ACL を変更します	<code>vsriver cifs share access-control modify</code>
ACL を削除します	<code>vsriver cifs share access-control delete</code>

ファイル権限を使用してファイルアクセスを保護

Windows のセキュリティタブを使用して、詳細な **NTFS** ファイル権限を設定します

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。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

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を NTFS ファイルおよびディレクトリに適用します。これらのタスクは Windows GUI によって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. [* フォルダー *] ボックスに、許可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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

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、ユーザーおよびグループに割り当てられている既存のファイルアクセス権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。

[アクセス権] 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	実行する処理
新しいユーザまたはグループの詳細な NTFS 権限を設定します	a. [追加 (Add)] 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 アクセス権を変更します	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。次の詳細な権限に関する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を選択できない場合、その権限は親オブジェクトから継承されます。

- 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。
- [OK] をクリックします。
- 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、1つのファイルに NTFS ファイルアクセス権を設定する場合は、[アクセス権] ボックスには表示されません。



この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの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。削除する必要がなかった権限が誤って削除され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 でアクセス権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、このような子オブジェクトに NTFS 権限を適用すると、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 権限が NTFS 権限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。

- OK** をクリックして、*Permissions* ボックスを閉じます。
- 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 を使用して、NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します](#)

[NTFSセキュリティ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](#)

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

ONTAP CLI を使用して **NTFS** ファイル権限を設定します

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を NTFS ファイルおよびディレクトリに適用します。

コマンドラインで設定できるのは NTFS ファイルアクセス権だけです。CLI で 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/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** ファイルアクセス権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。

DAC（ダイナミックアクセス制御）を使用したファイルアクセスの保護

Dynamic Access Control（DAC）；ダイナミックアクセス制御）の概要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、デバイス ID、デバイスの信頼性、ユーザの信頼性という 3 種類の情報がクレデンシャルに追加されます。

- デバイス ID

ユーザ ID 情報に似ていますが、ユーザがログインに使用しているデバイスの ID とグループメンバーシップは例外です。

- デバイスの信頼性

デバイスのセキュリティプリンシパルに関するアサーションです。たとえば、デバイスの信頼性として特定の OU のメンバーであることなどがあります。

- ユーザの信頼性

ユーザのセキュリティプリンシパルに関するアサーションです。たとえば、ユーザの信頼性として AD アカウントが特定の OU のメンバーであることなどがあります。

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、ユーザの信頼性、デバイスの信頼性、およびリソースの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して管理できます。

たとえば、ビジネスへの影響が大きいデータにアクセスする場合、ユーザー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。

高度な監査機能を備え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。ポリシーが適用されていた場合の結果と、現在の設定との違いが、監査イベントとして記録されます。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確認できます。アクセスポリシーの変更による影響を評価したあと、ポリシーを目的の SVM に GPO 経由で導入できます。

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 サーバ上で GPO サポートを有効または無効にします](#)

[GPO 設定に関する情報を表示します](#)

[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ルールに関する情報を表示します](#)

[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を表示する](#)

["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 サーバ上で DAC（ダイナミックアクセス制御）を使用する場合、Active Directory 環境での ONTAP によるダイナミックアクセス制御機能のサポートについて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されます](#)

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。

機能性	コメント
ファイルシステムへの請求	請求とは、ユーザに関する何らかの真実を表す単純な名前と値のペアです。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集中管理	集約型アクセスポリシーは、ファイルへのタグ付けが可能な Active Directory 内に格納される一種の ACL です。ファイルへのアクセスは、ディスク上のセキュリティ記述子とタグ付きの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、管理者はディスク上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	を拡張します <code>vserver security file-directory show</code> 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するコマンド。
集約型アクセスポリシーを含むセキュリティトレース	を拡張します <code>vserver security trace</code> 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するコマンドファミリー。

ダイナミックアクセス制御ではサポートされません

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。

機能性	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。

機能性	コメント
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概要を有効または無効にします

Dynamic Access Control （DAC；ダイナミックアクセス制御）を使用して CIFS サーバ上のオブジェクトを保護するオプションは、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する必要がなくなった場合は、このオプションを無効にすることができます。

このタスクについて

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使用する 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	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

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 が割り当てら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 を削除するまではそのリソースの非ダイナミックアクセス制御 ACE を管理できません。

このタスクについて

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します

集約型アクセスポリシーを使用した CIFS サーバ上のデータへのアクセスを保護するためには、CIFS サーバでの Dynamic Access Control （ DAC ；ダイナミックアクセス制御）の有効化、Active Directory での集約型アクセスポリシーの設定、GPO を使用した 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 GPO を有効にします。

作業を開始する前に

- 集約型アクセスポリシーを使用するには、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 の作成と適用を行うには、Active Directory ドメインコントローラに対して十分なアクセスが必要です。
- 必要なコマンドを実行するためには、Storage Virtual Machine （SVM）で十分な管理アクセスが必要です。

このタスクについて

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）に対して定義および適用されます。集約型アクセスポリシーと GPO の設定については、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. 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、有効にします `vserver cifs options modify` コマンドを実行します

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

2. 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、有効にします `vserver cifs group-policy modify` コマンドを実行します

```
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 サーバコンピュータアカウントが存在するコンテナに GPO を適用します。
6. 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` コマンドを実行します

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

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

次の例は、デフォルトのドメインポリシーに、CIFS サーバに適用される 2 つの集約型アクセスポリシーがあ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:

/voll/home
/voll/dirl

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 設定に関する情報を表示します](#)

[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ルールに関する情報を表示します](#)

[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します](#)

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について、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、および集約

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。

このタスクについて

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

ステップ

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

表示する情報	入力するコマンド
要約形式で表示されます	<code>vserver security file-directory show -vserver vserver_name -path path</code>
詳細が表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>
出力は、グループ SID とユーザ SID とともに表示されます	<code>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</code>
16 進数のビットマスクをテキスト形式に変換するファイルとディレクトリのセキュリティについて	<code>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</code>

例

次の例は、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 SVM vs1：

```

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 設定に関する情報を表示します](#)

[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ルールに関する情報を表示します](#)

[ダイナミックアクセス制御のリポ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 にリポートする場合に発生する状況と、リポ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。

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。
- を含むクラスタで監査の設定を変更する必要があります cap-staging のみを使用するイベントタイプ file-op イベントタイプ。

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方法および使用方法に関する追加情報の参照先

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際には、参考資料を利用することができます。

Active Directory の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の情報は、Microsoft TechNet ライブラリにあります。

["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およびサポートするように SMB サーバを設定するには、次の参考資料を使用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アクセスに関する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とき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1つ以上のルールが適用されており、このルールで、データへのアクセスを許可されるクライアントと、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します。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 認証と NTLM 認証の両方を使用した認証を許可できます。

ONTAP で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ら、クライアント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 のユーザと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と許可に代わるものではありません。共有とファイルのアクセス権限に加えて、エクスポートルールはもう1つのアクセスセキュリティ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、名前や内容は変更できます。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。このポリシーを、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を含む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する必要があ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（あるいはその両方）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 に関する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、その要求は失敗します。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は、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、またはクライアントの適切なサブセットへのアクセスを許可します
- SMB 経由のアクセスを許可する
- Kerberos 認証または NTLM 認証（あるいはその両方）を使用した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 ["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済みの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、クライアントに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に処理されます。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すると、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、クライアントの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。たとえば、NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

の最大サイズ `-clientmatch` フィールドは4096文字です。

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

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、次のパラメータが指定された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アドレスとは別のサブネットに属しています。そのため、クライアントは一致なくなり、このルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定された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内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。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、次のパラメータが指定された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 アドレスは一致しています。読み取り専用パラメータでは、認証に使用するセキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。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、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

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：cifs nfs1
- 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  
cifs nfs1 -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。それ以外の場合は、受信します access denied エラー。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::> vservers export-policy rule create -vservers 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を有効または無効にします

Storage Virtual Machine (SVM) での SMB アクセスに関する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。

作業を開始する前に

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が必要です。

このタスクについて

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。vservers cifs options modify -vservers vservers_name -is-exportpolicy-enabled true
 - エクスポートポリシーを無効にします。vservers cifs options modify -vservers vservers_name -is-exportpolicy-enabled false
3. admin 権限レベルに戻ります。set -privilege admin

例

次の例は、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てファイルアクセスを保護

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

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 のアクセス権のみがサポートされています。ONTAP で、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行うには、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。

このセキュリティは、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、メタデータ内に格納されます。

- 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せん。
- 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 のファイルやフォルダの Access Control List（ACL；アクセス制御リスト）、NFSv4 ACL、または UNIX モードのビット

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を設定するためのワークフロー

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 ファイル権限や監査ポリシーを設定する際に使用する 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を設定する

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ためには、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を提供します。環境がすべての NAS プロトコルからその適用先のストレージオブジェクトにアクセスするセキュリティを提供します。

手順

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

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

Vserver: vs1

NTFS Security Descriptor Name	Owner Name
sd1	-

セキュリティ記述子は、次の 4 つのデフォルト DACL アクセス制御エントリ（ACE）を持つように作成されます。

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
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を設定するとき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に設定したくないデフォルトの DACL ACE を削除します。

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

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. 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` コマンドを実行します

この例では、コマンドからの出力により、セキュリティ記述子から3つのデフォルト DACL ACE が削除され、`NT AUTHORITY\SYSTEM` のデフォルト DACL ACE エントリのみが残されていることを確認できます。

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

Vserver: vs1

NTFS Security Descriptor Name: sd1

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

3. 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` コマンドを実行します

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. 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` コマンドを実行します

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 sac1 add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. を使用して、DACLおよびSACLのACEが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 および vserver security file-directory ntfs sac1 show コマンドを指定します。

この例では、次のコマンドはセキュリティ記述子「`d1`」の DACL エントリに関する情報を表示します。

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

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
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 sac1 show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

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

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

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. 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` コマンドを実行します

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

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

8. を使用して、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` コマンドにを指定します `-access -control` パラメータをに設定します `slag`。

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これはに割り当てられます `/datavol1` アクセス制御タイプが「slag」に設定されているパス。

```
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. 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` コマンドを実行します

```
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. 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ます vsserver security file-directory apply コマンドを実行します

```
vsserver 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. 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ます vsserver security file-directory show コマンドを実行します

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 Full Control を許可するデフォルト 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によって、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にアクセスが制限（および監査）されます。

```
vsserver 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](#)

[ストレージレベルのアクセス保護を設定するためのワークフロー](#)

[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 の適用に関する一覧表

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します

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。

ます。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

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
要約形式で表示されます	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
詳細が表示されます	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

例

次の例は、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 SVM vs1：


```
cluster::> vsriver security file-directory show -vsriver 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
```

次の例は、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 (SVM vs1)。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::> vsriver security file-directory show -vsriver 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を削除します

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. 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 vsriver security file-directory show コマンドを実行します

```
vsriver security file-directory show -vsriver 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. 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 コマンドを実行します

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

3. 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 コマンドを実行します

```
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
```

SMB を使用したファイルアクセスの管理

ローカルユーザおよびローカルグループを使用して認証と許可を行います

ONTAP でのローカルユーザとローカルグループの使用方法

ローカルユーザとローカルグループの概念

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

• * ローカルユーザー *

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

ユーザアカウントには次のような用途があります。

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

クセスを制御する。

- * ローカルグループ *

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

グループにはいくつかの用途があります。

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

- * ローカルドメイン *

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

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

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

- * NTLM 認証 *

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

- * 複製されたクラスタデータベース (RDB) *

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

ローカルユーザおよびローカルグループを作成する理由

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

ローカルユーザアカウントを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメインユーザを使用できない。

ワークグループ設定にはローカルユーザが必要です。

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

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

- ローカル・ユーザに `_ ユーザ権限の管理 _` 権限を割り当てる

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

ローカルグループを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメイングループを使用できない。

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

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

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

関連情報

[ローカルユーザ認証の仕組み](#)

[サポートされる権限のリスト](#)

ローカルユーザ認証の仕組み

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

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

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

- ドメイン部分が一致します

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

- ドメイン部分が一致しません

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

たとえば、ユーザは Active Directory 内に存在するが、パスワードが無効であるか期限切れになっている

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

- ドメイン部分は指定されません

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

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

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

関連情報

ローカルユーザ認証の有効化と無効化

ユーザアクセストークンの構成方法

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

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

- ローカルユーザログイン

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

- ドメイン・ユーザ・ログイン

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

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

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



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

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

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

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

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

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

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



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

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

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

リポートに関するガイドライン

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

- セキュリティ上の理由から、ONTAP をローカルユーザとグループの機能をサポートしないバージョンにリポートしても、設定されているローカルユーザ、グループ、および権限に関する情報は削除されません。

- ONTAP の以前のメジャーバージョンにリバートする際、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 から削除されません。
- ローカルユーザまたはローカルグループに付与された権限に基づいて許可されるアクセスに依存するファイルアクセス要求は拒否されます。

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

ローカル権限とは

サポートされる権限のリスト

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

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

権限の名前	デフォルトのセキュリティ設定	説明
SeTcbPrivilege	なし	オペレーティングシステムの一部として機能します
SeBackupPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ACL を無視してファイルとディレクトリをバックアップします
SeRestorePrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators	ファイルおよびディレクトリをリストアし、ACL を上書きすべての有効なユーザまたはグループの SID をファイル所有者として設定します
SeTakeOwnershipPrivilege	BUILTIN\Administrators	ファイルまたはその他のオブジェクトの所有権を取得します
SeSecurityPrivilege	BUILTIN\Administrators	監査の管理 これには、セキュリティログの表示、ダンプ、およびクリアが含まれます。

権限の名前	デフォルトのセキュリティ設定	説明
SeChangeNotifyPrivilege	BUILTIN\Administrators、 BUILTIN\Backup Operators、 BUILTIN\Power Users、 BUILTIN\Users、 Everyone	トラバースチェックのバイパス この権限を持つユーザには、フォルダ、シンボリックリンク、ジャンクションをトラバースするためのトラバース (x) 権限は必要ありません。

関連情報

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

権限を割り当てます

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

- 作成したグループに一連の権限を割り当てることができます。

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

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

関連情報

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

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

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

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

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

- ローカルゲストアカウントがありません。

関連情報

事前定義の BUILTIN グループとそのデフォルトの権限

ローカルユーザパスワードの要件

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

パスワードは次の基準を満たしている必要があります。

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

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

関連情報

ローカル SMB ユーザに対するパスワードの複雑さの要件の有効化と無効化

CIFS サーバのセキュリティ設定に関する情報を表示する

ローカルユーザのアカウントパスワードを変更しています

事前定義の BUILTIN グループとそのデフォルトの権限

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

次の表に、事前定義グループを示します。

事前定義の BUILTIN グループ	デフォルトの権限
<p>BUILTIN\Administrators544番</p> <p>最初に作成されたとき、ローカル Administrator RIDが500のアカウントは、自動的にこのグループのメンバーになります。Storage Virtual Machine (SVM) がドメインに参加している場合は、domain\Domain Admins グループがグループに追加されます。SVMがドメインから削除された場合は domain\Domain Admins グループがグループから削除されます。</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeSecurityPrivilege • SeTakeOwnershipPrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\Power Users547番地</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーには、次のような特徴があります。</p> <ul style="list-style-type: none"> • 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に追加することはできません BUILTIN\Administrators グループ： 	<p>SeChangeNotifyPrivilege</p>
<p>BUILTIN\Backup Operators住所は551</p> <p>このグループには、最初に作成された時点ではメンバーはありません。このグループのメンバーは、バックアップ目的で開いたファイルやフォルダの読み取りおよび書き込み権限を上書きできます。</p>	<ul style="list-style-type: none"> • SeBackupPrivilege • SeRestorePrivilege • SeChangeNotifyPrivilege
<p>BUILTIN\UsersRID 545</p> <p>最初に作成された時点では、このグループには（暗黙の以外に）メンバーはありません（Authenticated Users 特殊グループ）。SVMがドメインに参加すると、が表示されます 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た場合は domain\Domain Users グループがこのグループから削除されます。</p>	<p>SeChangeNotifyPrivilege</p>
<p>EveryoneSID S-1-1-0</p> <p>このグループには、ゲストを含むすべてのユーザが含まれます（ただし匿名ユーザは含まれません）。このグループは、暗黙のメンバーシップを持つ暗黙のグループです。</p>	<p>SeChangeNotifyPrivilege</p>

関連情報

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

[サポートされる権限のリスト](#)

[トラバースチェックのバイパスの設定](#)

ローカルユーザとローカルグループ機能を有効または無効にします

ローカルユーザとローカルグループ機能の概要を有効または無効にします

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

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

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

関連情報

[ローカルユーザアカウントを変更します](#)

[ローカルグループを変更します](#)

[ローカルまたはドメインのユーザまたはグループに権限を追加します](#)

ローカルユーザとローカルグループを有効または無効にします

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

このタスクについて

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

手順

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

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

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

例

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

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

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

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

関連情報

[ローカルユーザ認証を有効または無効にします](#)

[ローカルユーザアカウントを有効または無効にします](#)

[ローカルユーザ認証を有効または無効にします](#)

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

作業を開始する前に

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

このタスクについて

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

手順

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

2. 次のいずれかを実行します。

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

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

例

次の例は、SVM vs1 でローカルユーザ認証を有効にします。

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

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

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

関連情報

[ローカルユーザ認証の仕組み](#)

[ローカルユーザとローカルグループの有効化と無効化](#)

[ローカルユーザアカウントを管理します](#)

[ローカルユーザアカウントを変更します](#)

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

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

例

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

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

ローカルユーザアカウントを有効または無効にします

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

このタスクについて

ユーザアカウントを変更してローカルユーザを有効にします。

ステップ

1. 適切な操作を実行します。

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

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

ローカルユーザのアカウントパスワードを変更する

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

ステップ

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

例

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

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

Enter the new password:

Confirm the new password:

関連情報

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

[CIFS サーバのセキュリティ設定に関する情報を表示する](#)

ローカルユーザに関する情報を表示します

すべてのローカルユーザのリストを要約形式で表示できます。特定のユーザに対して設定されているアカウント設定を確認するには、そのユーザの詳細なアカウント情報、および複数のユーザのアカウント情報を表示します。この情報は、ユーザの設定を変更する必要があるかどうかを判断する場合に加えて、認証やファイルアクセスに関する問題のトラブルシューティングを行う場合にも役立ちます。

このタスクについて

ユーザのパスワードに関する情報は表示されません。

ステップ

- 次のいずれかを実行します。

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

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

例

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

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

ローカルユーザのグループメンバーシップに関する情報を表示します

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

このタスクについて

コマンドをカスタマイズして、必要な情報のみを表示することができます。

ステップ

1. 次のいずれかを実行します。

状況	入力するコマンド
指定したローカルユーザのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
このローカルユーザが属しているローカルグループのローカルユーザメンバーシップに関する情報を表示します	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>

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

例

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

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

ローカルユーザアカウントを削除します

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

このタスクについて

ローカルユーザを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

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

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

手順

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

```
show -vserver vs1
```

例

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

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

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

ローカルグループを管理します

ローカルグループを変更します

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

状況	使用するコマンド
ローカルグループの概要を変更します	<pre>vs1 cifs users-and-groups local-group modify -vserver vs1 -group-name group_name -description text</pre> 概要 にスペースが含まれている場合は、二重引用符で囲む必要があります。
ローカルグループの名前を変更します	<pre>vs1 cifs users-and-groups local-group rename -vserver vs1 -group-name group_name -new-group-name new_group_name</pre>

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

ローカルグループに関する情報を表示します

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

ステップ

1. 次のいずれかを実行します。

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

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

例

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

```
cluster1::> vsserver cifs users-and-groups local-group show -vsserver 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の管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

このタスクについて

ローカルグループへのメンバーの追加に関するガイドラインを次に示します。

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

ローカルグループからのメンバーの削除に関するガイドラインを次に示します。

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

ステップ

1. グループのメンバーを追加または削除します。

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

次の例は、SVM vs1 上のローカルグループ「`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::> vsriver cifs users-and-groups local-group add-members
-vsriver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

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

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

関連情報

ローカルグループのメンバーに関する情報を表示する

ローカルグループのメンバーに関する情報を表示します

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

ステップ

1. 次のいずれかを実行します。

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

例

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

```
cluster1::> vsriver cifs users-and-groups local-group show-members
-vsvriver vs1
Vsvriver   Group Name                               Members
-----
vs1        BUILTIN\Administrators                 CIFS_SERVER\Administrator
                                                AD_DOMAIN\Domain Admins
                                                AD_DOMAIN\dom_grp1
                                                AD_DOMAIN\Domain Users
                                                AD_DOMAIN\dom_usr1
                                                CIFS_SERVER\james
        BUILTIN\Users
        CIFS_SERVER\engineering
```

ローカルグループを削除します

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

このタスクについて

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

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

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

手順

1. SVM上のローカルグループのリストを表示して、削除するローカルグループの名前を確認します。
vsriver cifs users-and-groups local-group show -vsriver vsriver_name
2. ローカルグループを削除します。vsriver cifs users-and-groups local-group delete -vsriver vsriver_name -group-name group_name
3. グループが削除されたことを確認します。vsriver cifs users-and-groups local-user show -vsriver vsriver_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::> vsriver cifs users-and-groups local-group show -vsriver 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::> vsriver cifs users-and-groups local-group delete -vsriver vs1
-group-name CIFS_SERVER\sales

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

```

ローカルデータベースのドメインユーザおよびグループ名を更新します

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

このタスクについて

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

手順

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

ドメインユーザおよびドメイングループの更新後の処理	使用するコマンド
ドメインユーザとドメイングループについて、正常に更新されたものと更新できなかったものを表示する	<code>vsriver cifs users-and-groups update-names -vsriver vsriver_name</code>

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

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

例

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

```

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

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

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

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

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

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

cluster1::*> set -privilege admin

```

ローカル権限を管理します

ローカルまたはドメインのユーザまたはグループに権限を追加します

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

作業を開始する前に

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

このタスクについて

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

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

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

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

手順

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

例

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

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

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

ローカルまたはドメインのユーザまたはグループから権限を削除します

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

作業を開始する前に

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

このタスクについて

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

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

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

手順

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

例

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

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

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

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

ローカルまたはドメインのユーザとグループの権限をリセットします

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

このタスクについて

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

手順

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

例

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

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

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

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

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

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

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

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

権限の上書きに関する情報を表示します

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

ステップ

1. 次のいずれかを実行します。

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

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

例

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

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

トラバースチェックのバイパスを設定する

トラバースチェックのバイパスの設定の概要

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

トラバースチェックのバイパスを許可または拒否した場合の動作

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

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

トラバースチェックのバイパスを設定する

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

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

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

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

- BUILTIN\Administrators
- BUILTIN\Power Users

- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

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

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

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



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

関連情報

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

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

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

[SMB 共有のアクセス制御リストを作成](#)

[ストレージレベルのアクセス保護を使用してファイルアクセスを保護](#)

[サポートされる権限のリスト](#)

[ローカルまたはドメインのユーザまたはグループに権限を追加します](#)

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

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

作業を開始する前に

- SVM上にSMBサーバが存在している必要があります。

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

このタスクについて

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

手順

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

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

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

例

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

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

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

関連情報

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

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

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

作業を開始する前に

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

このタスクについて

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

手順

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

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

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

例

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

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

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

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

関連情報

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

ファイルセキュリティと監査ポリシーに関する情報を表示します

ファイルセキュリティと監査ポリシーの概要に関する情報を表示します

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

できます。

ファイルセキュリティに関する情報を表示する

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

- NTFS
- 「UNIX」
- 混在

監査ポリシーに関する情報を表示する

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

- SMB（すべてのバージョン）
- NFSv4.x に対応している

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

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

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

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

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

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

関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

[ストレージレベルのアクセス保護に関する情報の表示](#)

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

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

このタスクについて

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

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

ステップ

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

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

例

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

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

```

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

OI|CI|IO

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

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

```

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

```

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

```

```

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

```

```

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

```

```

    ALLOW-Everyone-0x1f01ff

```

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

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

Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

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

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

```

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

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

関連情報

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

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

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

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

このタスクについて

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

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

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

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

ステップ

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

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

例

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

します。この mixed セキュリティ形式のパスには、UNIX 対応のセキュリティが設定されています。

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

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

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

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

```

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

OI|CI|IO

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

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

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

関連情報

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

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

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

セキュリティ形式と有効なセキュリティ形式、適用されている権限、UNIX の所有者とグループに関する情報など、UNIX セキュリティ形式のボリューム上にあるファイルや

ディレクトリのセキュリティに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

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

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

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

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

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

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

ステップ

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

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

例

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

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

```

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

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

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

```

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


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を表示する

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

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

このタスクについて

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

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

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

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

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

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

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

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

ステップ

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

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

例

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

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

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

```

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

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

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

```

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

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

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

このタスクについて

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

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

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

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

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

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

手順

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

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

例

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

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

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

ファイルセキュリティと監査ポリシーに関する情報を表示する方法

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

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

例

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

```

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

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

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

```

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

```
cluster::> 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場合、リモートクライアントを使用せずにファイルセキュリティを管理できます。CLI を使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも 1 つのコマンドで実行できるため、所要時間を大幅に短縮できます。

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

ストレージレベルのアクセス保護は ONTAP CLI からのみ設定および管理できます。ストレージレベルのアクセス保護設定を SMB クライアントから管理することはできません。また、NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護のセキュリティは表示されません。システム（Windows または UNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティレイヤをデータアクセスに追加

で提供します。



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

NTFS セキュリティ形式のボリューム

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

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

mixed セキュリティ形式のボリューム

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

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

UNIXセキュリティ形式のボリューム

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

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

関連情報

[ファイルセキュリティと監査ポリシーに関する情報を表示します](#)

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

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

[ストレージレベルのアクセス保護を使用してファイルアクセスを保護](#)

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

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

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

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

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

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

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

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

セキュリティ記述子を使用したファイルおよびフォルダのセキュリティの適用方法

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

• * 権限 *

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

• * セキュリティ記述子 *

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

• * アクセス制御リスト (ACL) *

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

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

- システムアクセスセイギョリスト SACL

- * 随意アクセス制御リスト (DACL) *

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

- * システム・アクセス・コントロール・リスト (SACL) *

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

- * アクセス制御エントリ (ACE) *

ACE は、DACL または SACL 内の個々のエントリです。

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

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

- * 権限の継承 *

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

関連情報

["SMB および NFS の監査とセキュリティトレース"](#)

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

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

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

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

SVM ディザスタリカバリの 2 つのタイプのうち 1 つを設定できます。

- ID が保持されます

この設定では、SVM と CIFS サーバの ID が維持されます。

- ID が破棄されました

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

ID 破棄設定に関するガイドライン

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

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

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

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

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

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

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

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

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

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

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

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

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

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

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

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

- セキュリティ記述子

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

- DACL エントリ

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

- SACL エントリ

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

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

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

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

NTFS セキュリティ記述子を作成します

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

このタスクについて

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

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

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

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

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

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

アルページを参照してください。

NTFSセキュリティ記述子へのNTFS DACLアクセス制御エントリの追加

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

このタスクについて

セキュリティ記述子のDACLには1つ以上のACEを追加できます。

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

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

- 権利
- 詳細な権限
- raw 権限（advanced 権限）



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

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

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

手順

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

このタスクについて

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

手順

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

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

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

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

セキュリティポリシーにタスクを追加します

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

このタスクについて

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

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

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

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

- ストレージレベルのアクセス保護タスク

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

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

ポリシーへのタスクの追加に関するガイドラインを次に示します。

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

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

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

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

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

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

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

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

手順

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

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

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

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

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

Vserver: vs1

Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor	Name				
-----	-----	-----	-----	-----	

1	/home/dir1	file-directory	ntfs	propagate	sd2

セキュリティポリシーを適用する

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

このタスクについて

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



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

ステップ

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

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

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

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

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

セキュリティポリシージョブを監視します

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

このタスクについて

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

ステップ

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

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

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

適用したファイルセキュリティを確認します

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

このタスクについて

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

ステップ

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

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

```

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

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

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
  ALLOW-Everyone-0x1f01ff
  0... .... =
```

Generic Read	.0..	=
Generic Write	..0.	=
Generic Execute	...0	=
Generic All0	=
System Security1	=
Synchronize1...	=
Write Owner1..	=
Write DAC1.	=
Read Control1	=
Delete1	=
Write Attributes1	=
Read Attributes1...	=
Delete Child1	=
Execute1	=
Write EA1...	=
Read EA1..	=
Append1.	=
Write1	=
Read		
	ALLOW-Everyone-0x10000000-OI CI IO	
Generic Read	0...	=
Generic Write	.0..	=
Generic Execute	..0.	=
	...1	=

Generic All0..... =
System Security0..... =
Synchronize0..... =
Write Owner0..... =
Write DAC0..... =
Read Control0..... =
Delete0..... =
Write Attributes0..... =
Read Attributes0..... =
Delete Child0..... =
Execute0..... =
Write EA0..... =
Read EA0..... =
Append0..... =
Write0..... =
Read0..... =

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

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

このタスクについて

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視して、適用した監査ポリシーの設定を確認することができます。



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

関連情報

[ストレージレベルのアクセス保護を使用したファイルアクセスの保護](#)

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

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

["SMB および NFS の監査とセキュリティトレース"](#)

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

NTFS セキュリティ記述子を作成します

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

このタスクについて

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

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

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

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

- セキュリティ記述子の所有者
- 所有者のプライマリグループ

- raw 制御フラグ

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

手順

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

`vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`
3. セキュリティ記述子の設定が正しいことを確認します。 `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

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

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

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

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

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

このタスクについて

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

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

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

- 権利
- 詳細な権限

- raw 権限（advanced 権限）



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

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

手順

1. SACLエントリをセキュリティ記述子に追加します。vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1 -access-type {failure|success} -account name_or_SID optional_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 vs1 -ntfs-sd sd1 -access-type {failure|success} -account name_or_SID

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

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

セキュリティポリシーを作成する

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

このタスクについて

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

手順

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

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

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

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

セキュリティポリシーにタスクを追加します

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

このタスクについて

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

タスクには次の 2 つのタイプがあります。

- ファイルとディレクトリのタスク

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

- ストレージレベルのアクセス保護タスク

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

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

ポリシーへのタスクの追加に関するガイドラインを次に示します。

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

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

- ストレージレベルのアクセス保護は、権限の制限に使用します。

アクセス権限は付与されません。

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

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

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

手順

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

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

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/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

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

このタスクについて

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



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

ステップ

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

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

ポリシーを適用するジョブがスケジュールされ、ジョブ ID が返されます。

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

セキュリティポリシージョブを監視します

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

このタスクについて

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

ステップ

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

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

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

適用した監査ポリシーを確認します

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

このタスクについて

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

ステップ

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

例

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

```

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

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

```

セキュリティポリシージョブの管理に関する考慮事項

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

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

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

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

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

NTFS セキュリティ記述子を管理するコマンド

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

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

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

NTFS DACL アクセス制御エントリを管理するコマンド

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

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

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

表示するコマンドです。

NTFS SACL アクセス制御エントリの管理用コマンド

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

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

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

セキュリティポリシーを管理するためのコマンド

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

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

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

セキュリティポリシータスクを管理するコマンド

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

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

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

セキュリティポリシージョブの管理用コマンド

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

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

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

SMB 共有のメタデータキャッシュを設定します

SMB メタデータのキャッシングの仕組み

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

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

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



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

SMB メタデータのキャッシングを有効にします

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

ステップ

1. 必要な操作を実行します。

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

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](#)

既存の SMB 共有に対する共有プロパティの追加または削除

SMB メタデータキャッシュエントリの有効期間を設定します

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

作業を開始する前に

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

ステップ

1. 必要な操作を実行します。

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

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

ファイルロックを管理します

プロトコル間のファイルロックについて

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

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

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

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

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

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

ファイルは最後に閉じた後に削除されます。

- NFSのリンク解除処理はサポートされていません。

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

- UNIXファイルシステムでは、リンク解除操作がサポートされます。

NFSとUNIXのセマンティクスが必要なため、サポートされています。

- 名前を変更する

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

- NFSの名前変更はサポートされていません。

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

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

ONTAP による読み取り専用ビットの処理方法

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

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

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

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

- NFS は、読み取り専用ビットが有効になっているファイルを書き込み権限ビットが無効になっているファ

イルとして扱います。

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



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

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

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

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

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

ロックに関する情報を表示します

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

このタスクについて

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

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

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

- バイト範囲ロック。ファイルの一部のみをロックします。
- 共有ロック。開いているファイルをロックします。

- 便宜的ロック。SMB を使用してクライアント側キャッシュを制御します。
- 委譲。NFSv4.x を使用してクライアント側キャッシュを制御します

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

ステップ

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

例

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

```
cluster1::> vserver locks show

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

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

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

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

```

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

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

```

ロックを解除します

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

このタスクについて

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

手順

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

詳細については、コマンドのマニュアルページを参照してください。

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

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

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

SMB のアクティビティを監視する

SMB セッション情報を表示します

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

このタスクについて

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

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

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

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

ステップ

1. 次のいずれかを実行します。

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

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

例

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

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

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

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

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

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

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

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

関連情報

[開いている SMB ファイルに関する情報を表示する](#)

開いている **SMB** ファイルに関する情報を表示します

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

このタスクについて

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

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

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

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

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

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

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

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

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

ステップ

1. 次のいずれかを実行します。

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

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

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

例

次の例は、SVM vs1 の開いているファイルに関する情報を表示します。

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

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

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

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

関連情報

SMB セッション情報の表示

使用可能な統計オブジェクトと統計カウンタを確認します

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

手順

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

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

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

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

例

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

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

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

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

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

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

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

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

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



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

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

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

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

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

Object: cifs

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

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

Object: client

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

[...]

関連情報

[統計情報を表示します](#)

統計情報を表示します

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

作業を開始する前に

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

手順

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

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

詳細については、各コマンドのマニュアルページを参照してください。

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

関連情報

[使用可能な統計オブジェクトと統計カウンタの確認](#)

[SMB 署名済みセッションの統計の監視](#)

[BranchCache 統計を表示します](#)

[統計を使用した自動ノードリファラルのアクティビティの監視](#)

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

SMB クライアントベースのサービスを導入する

オフラインファイルを使用して、オフラインで使用するファイルをキャッシュできます

オフラインファイルを使用して、オフラインで使用するためのファイルのキャッシュの概要を確認します

ONTAP では、Microsoft のオフラインファイル機能（_ クライアント側キャッシュ _）をサポートしています。これにより、オフラインで使用するファイルをローカルホストにキャッシュできます。オフラインファイル機能を使用すると、ネットワークから切断されているファイルでも作業を継続できます。

Windows のユーザドキュメントやプログラムを共有に自動的にキャッシュするかどうか、またはキャッシュするファイルを手動で選択するかどうかを指定できます。新しい共有では、手動キャッシュがデフォルトで有効になります。オフラインで利用可能となったファイルは、Windows クライアントのローカルディスクと同期されます。同期は、特定のストレージシステム共有へのネットワーク接続がリストアされたときに実行されます。

オフラインのファイルおよびフォルダに対するアクセス権限は CIFS サーバに保存されているファイルおよびフォルダと同じであるため、オフラインのファイルおよびフォルダに対して処理を実行するには、CIFS サーバに保存されているファイルおよびフォルダに対する十分な権限が必要です。

ユーザとネットワーク上の他のユーザが同じファイルに変更を加えた場合、ユーザはネットワークにローカルバージョンのファイルを保存するか、別のバージョンを保持するか、または両方を保存できます。両方のバージョンを残す場合は、ローカルユーザが変更した新しいファイルがローカルに保存され、キャッシュされたファイルは CIFS サーバに保存されたバージョンの変更が反映されて上書きされます。

オフラインファイルは、共有ごとに共有の設定を行うことができます。共有を作成または変更するときに、次の 4 つのオフラインフォルダ設定のいずれかを選択できます。

- キャッシュなし

共有のクライアント側キャッシュを無効にします。クライアントのローカルにファイルやフォルダが自動的にキャッシュされず、ユーザがファイルやフォルダをローカルにキャッシュすることもできません。

- 手動キャッシュ

共有にキャッシュするファイルを手動で選択できるようにします。これがデフォルト設定です。デフォルトでは、ファイルやフォルダはローカルクライアントにキャッシュされません。オフラインで使用するためにローカルにキャッシュするファイルやフォルダをユーザが選択できます。

- ドキュメントの自動キャッシュ

ユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイルとフォルダだけです。

- プログラムの自動キャッシュ

プログラムとユーザのドキュメントが共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。また、この設定を有効

にすると、ネットワークに接続されている場合でも、クライアントはローカルにキャッシュされた実行ファイルを実行できます。

Windows サーバおよびクライアントでのオフラインファイルの設定の詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

[移動プロファイルを使用した SVM に関連付けられた CIFS サーバへのユーザプロファイルの一元的な格納](#)

[フォルダリダイレクトを使用した CIFS サーバへのデータの格納](#)

[BranchCache を使用したブランチオフィスでの SMB 共有のコンテンツのキャッシュ](#)

"Microsoft TechNet ライブラリ : technet.microsoft.com/en-us/library/"

オフラインファイルを使用するための要件

CIFS サーバで Microsoft のオフラインファイル機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAP のバージョンの要件

ONTAP の各リリースでオフラインファイルがサポートされます。

SMB プロトコルのバージョン

Storage Virtual Machine (SVM ONTAP) については、すべてのバージョンの SMB でオフラインファイルがサポートされます。

Windows クライアントの要件

Windows クライアントでオフラインファイルがサポートされている必要があります。

オフラインファイル機能をサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

"mysupport.netapp.com/matrix"

オフラインファイルの導入に関するガイドラインを参照してください

が搭載されたホームディレクトリ共有にオフラインファイルを導入する場合は、いくつかの重要なガイドラインについて理解しておく必要があります。showsnapshot ホームディレクトリに設定された共有プロパティ。

状況に応じて showsnapshot オフラインファイルが設定されているホームディレクトリ共有で共有プロパティが設定されている場合、Windows クライアントはすべての Snapshot コピーをの下にキャッシュします ~snapshot ユーザのホームディレクトリ内のフォルダ。

次のいずれかに該当する場合、Windows クライアントでは、すべての Snapshot コピーがホームディレクトリの下にキャッシュされます。

- ユーザが、ホームディレクトリをクライアントからオフラインで利用できるようにしている。

の内容 `~snapshot` ホームディレクトリ内のフォルダが含まれ、オフラインで利用できるようになります。

- ユーザは、などのフォルダをリダイレクトするようにフォルダリダイレクトを設定します `My Documents` CIFSサーバ共有上のホームディレクトリのルートに移動します。

Windows クライアントによっては、リダイレクトされたフォルダが自動的にオフラインで利用できるようになる場合があります。フォルダがホームディレクトリのルートにリダイレクトされる場合は `~snapshot` フォルダは、キャッシュされたオフラインコンテンツに含まれます。



ファイル導入をオフラインにします `~snapshot` フォルダはオフラインファイルに含まれないようにしてください。内のSnapshotコピー `~snapshot` フォルダには、ONTAP がSnapshotコピーを作成した時点のボリューム上のすべてのデータが格納されます。そのため、のオフラインコピーを作成します `~snapshot` フォルダは、クライアント上のローカルストレージを大量に消費し、オフラインファイルの同期中にネットワーク帯域幅を消費します。また、オフラインファイルの同期にかかる時間も長くなります。

CLI を使用して **SMB** 共有でオフラインファイルサポートを設定します

SMB 共有の作成時に、または既存の SMB 共有の変更時にいつでも、ONTAP CLI を使用して、4 つのオフラインファイル設定のいずれかを指定することによって、オフラインファイルのサポートを設定できます。手動オフラインファイルのサポートがデフォルト設定です。

このタスクについて

オフラインファイルのサポートを設定する場合は、次の 4 つのオフラインファイル設定のいずれかを選択できます。

設定	説明
<code>none</code>	Windows クライアントがこの共有のファイルをキャッシュすることを禁止します。
<code>manual</code>	Windows クライアントのユーザが、キャッシュするファイルを手動で選択できるようにします。
<code>documents</code>	Windows クライアントがオフラインアクセスのために使用するユーザのドキュメントをキャッシュすることを許可します。
<code>programs</code>	Windows クライアントがオフラインアクセスのために使用するプログラムをキャッシュすることを許可します。クライアントは、共有が使用可能な場合でも、キャッシュしたプログラムファイルをオフラインモードで使用できます。

選択できるオフラインファイル設定は 1 つだけです。既存の SMB 共有でオフラインファイル設定を変更する

と、元の設定が新しいオフラインファイル設定に置き換えられます。その他の既存の SMB 共有設定および共有プロパティは、削除も置換もされません。明示的に削除または変更しないかぎり、有効なままです。

手順

- 1. 適切な操作を実行します。

オフラインファイルを設定する対象	入力するコマンド
新しい SMB 共有	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	既存の SMB 共有
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	manual
documents	programs}`

- 2. SMB共有の設定が正しいことを確認します。`vserver cifs share show -vserver vserver_name -share-name share_name -instance`

例

次のコマンドでは、オフラインファイルをに設定して「data1」という名前のSMB共有を作成します documents :

```
cluster1::> vsserver cifs share create -vsserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance

                Vserver: vs1
                Share: data1
CIFS Server NetBIOS Name: VS1
                Path: /data1
                Share Properties: oplocks
                                browsable
                                changenotify
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: documents
                Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
                UNIX Group for File Create: -
```

次のコマンドは、オフラインファイルの設定をに変更することで、「data1」という名前の既存のSMB共有を変更します manual ファイルモードとディレクトリモードの作成マスクの値を追加します。

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
        CIFS Server NetBIOS Name: VS1
                Path: /data1
        Share Properties: oplocks
                        browsable
                        changenotify
        Symlink Properties: enable
        File Mode Creation Mask: 644
        Directory Mode Creation Mask: 777
                Share Comment: Offline files
                Share ACL: Everyone / Full Control
        File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
        Vscan File-Operations Profile: standard
        Maximum Tree Connections on Share: 4294967295
        UNIX Group for File Create: -
```

関連情報

既存の SMB 共有に対する共有プロパティの追加または削除

コンピュータの管理 MMC を使用して、**SMB** 共有でオフラインファイルサポートを設定します

オフラインで使用するためにファイルをローカルにキャッシュすることをユーザに許可する場合は、コンピュータの管理 MMC（Microsoft 管理コンソール）を使用してオフラインファイルのサポートを設定できます。

手順

1. Windows サーバー上の MMC を開くには、Windows エクスプローラで、ローカルコンピューターのアイコンを右クリックし、* 管理 * を選択します。
2. 左側のパネルで、「* コンピュータの管理 *」を選択します。
3. 「* 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。

4. CIFS サーバの名前を入力するか、* Browse * をクリックして CIFS サーバを指定します。

CIFS サーバの名前が Storage Virtual Machine（SVM）ホスト名と同じである場合は、SVM 名を入力し

ます。CIFS サーバの名前が SVM ホスト名と異なる場合は、CIFS サーバの名前を入力します。

5. [OK] をクリックします。
6. コンソールツリーで、* システムツール * > * 共有フォルダー * をクリックします。
7. [* 共有] をクリックします。
8. 結果ペインで、共有を右クリックします。
9. * プロパティ * をクリックします。

選択した共有のプロパティが表示されます。

10. [一般*] タブで、[* オフライン設定*] をクリックします。

[オフライン設定] ダイアログボックスが表示されます。

11. 必要に応じて、オフラインの可用性オプションを設定します。
12. [OK] をクリックします。

移動プロファイルを使用すると、**SVM** に関連付けられた **SMB** サーバにユーザプロファイルを一元的に格納できます

移動プロファイルを使用すると、**SVM** の概要に関連付けられた **SMB** サーバにユーザプロファイルを一元的に格納できます

ONTAP では、Windows の移動プロファイルの格納をサポートしており、それらを Storage Virtual Machine (SVM) に関連付けられた CIFS サーバに格納することができます。ユーザ移動プロファイルを設定すると、ユーザはログイン先に関係なく自動でリソースを利用できるようになります。また、移動プロファイルを使用すると、ユーザプロファイルの管理と管理が簡単になります。

移動ユーザプロファイルには、次のような利点があります。

- 自動でリソースを利用できる

Windows 8、Windows 7、Windows 2000、または Windows XP を実行しているコンピュータであれば、ネットワーク上のどのコンピュータにログインしても、各ユーザの一意のプロファイルを自動的に利用できます。ネットワーク上で使用するコンピュータごとにプロファイルを作成する必要はありません。

- コンピュータの交換が簡単

ユーザのプロファイル情報はすべてネットワークに別途保存されるため、交換後の新しいコンピュータにユーザのプロファイルを簡単にダウンロードできます。ユーザが新しいコンピュータに初めてログインしたときに、サーバに保存されているユーザのプロファイルが新しいコンピュータにコピーされます。

関連情報

[オフラインファイルを使用したオフラインで使用するファイルのキャッシュ](#)

[フォルダリダイレクトを使用した CIFS サーバへのデータの格納](#)

移動プロファイルを使用するための要件

CIFS サーバで Microsoft の移動プロファイルを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAP のバージョンの要件

ONTAP では移動プロファイルをサポートしています

SMB プロトコルのバージョン

Storage Virtual Machine（SVM ONTAP）については、すべてのバージョンの SMB で移動プロファイルがサポートされます。

Windows クライアントの要件

移動プロファイルを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

移動プロファイルをサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

移動プロファイルを設定する

ネットワーク上の任意のコンピュータにユーザがログオンするときに、そのユーザのプロファイルを自動的に使用できるようにするには、Active Directory ユーザとコンピュータ MMC スナップインを使用して移動プロファイルを設定します。Windows Serverで移動プロファイルを設定する場合は、Active Directory管理センターを使用できます。

手順

1. Windowsサーバーで、Active DirectoryユーザーとコンピュータMMC（またはWindowsサーバーのActive Directory管理センター）を開きます。
2. 移動プロファイルを設定するユーザを見つけます。
3. ユーザーを右クリックし、* プロパティ * をクリックします。
4. [プロファイル]*タブで、ユーザの移動プロファイルを保存する共有のプロファイルパスを入力し、続けてを入力します %username%。

たとえば、プロファイルパスは次のようになります。

\\vs1.example.com\profiles\%username%。ユーザが初めてログインしたとき、%username% がユーザの名前に置き換えられます。



パス内 \\vs1.example.com\profiles\%username%、profiles は、すべてのメンバーにフルコントロール権限があるStorage Virtual Machine（SVM）vs1上の共有の共有名です。

5. [OK] をクリックします。

フォルダリダイレクトを使用して、**SMB** サーバにデータを格納します

フォルダリダイレクトを使用して、**SMB** サーバの概要にデータを格納します

ONTAP では、Microsoft のフォルダリダイレクトをサポートしています。ユーザや管理者は、この機能を使用して、ローカルフォルダのパスを CIFS サーバの場所にリダイレクトできます。リダイレクトされたフォルダは、データが SMB 共有に格納されていても、ローカルの Windows クライアントに格納されたフォルダのように扱うことができます。

フォルダリダイレクトは、主に、ホームディレクトリをすでに導入しており、既存のホームディレクトリ環境との互換性を維持したい組織を対象としています。

- Documents、Desktop、および Start Menu は、リダイレクト可能なフォルダの例です。
- ユーザは、各自の Windows クライアントからフォルダをリダイレクトできます。
- 管理者は、Active Directory で GPO を設定することで、フォルダリダイレクトを一元的に設定および管理できます。
- 移動プロファイルを設定している場合は、管理者がユーザデータとプロファイルデータを分けることができます。
- 管理者は、フォルダリダイレクトとオフラインファイルを使用して、ローカルフォルダのデータストレージを CIFS サーバにリダイレクトし、ユーザはコンテンツをローカルにキャッシュできます。

関連情報

[オフラインファイルを使用したオフラインで使用するファイルのキャッシュ](#)

[移動プロファイルを使用した SVM に関連付けられた CIFS サーバへのユーザプロファイルの一元的な格納](#)

フォルダリダイレクトを使用するための要件

CIFS サーバで Microsoft のフォルダリダイレクトを使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。

ONTAP のバージョンの要件

ONTAP は、Microsoft のフォルダリダイレクトをサポートしています

SMB プロトコルのバージョン

Storage Virtual Machine（SVM）については、ONTAP のすべてのバージョンの SMB で Microsoft のフォルダリダイレクトがサポートされます。

Windows クライアントの要件

Microsoft のフォルダリダイレクトを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

フォルダリダイレクトをサポートする Windows クライアントに関する最新情報については、Interoperability

Matrix を参照してください。

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)

フォルダリダイレクトを設定します

Windows の [プロパティ] ウィンドウを使用して、フォルダリダイレクトを設定できます。この方法を使用する利点は、Windows ユーザが SVM 管理者のサポートがなくてもフォルダリダイレクトを設定できることです。

手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。
2. * プロパティ * をクリックします。

選択した共有のプロパティが表示されます。

3. [* ショートカット *] タブで、[* ターゲット *] をクリックし、選択したフォルダーをリダイレクトするネットワーク上の場所へのパスを指定します。

たとえば、フォルダをにリダイレクトする場合などです data にマッピングされているホームディレクトリ内のフォルダ Q:\、を指定します Q:\data ターゲットとして。

4. [OK] をクリックします。

オフラインフォルダの設定の詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

["Microsoft TechNet ライブラリ : technet.microsoft.com/en-us/library/"](https://technet.microsoft.com/en-us/library/)

SMB 2.x を使用する Windows クライアントから ~snapshot ディレクトリにアクセスします

へのアクセスに使用する方法 ~snapshot SMB 2.xを使用するWindowsクライアントのディレクトリは、SMB 1.0の場合とは異なります。にアクセスする方法を理解しておく必要があります ~snapshot SMB 2.x接続を使用してSnapshotコピーに格納されたデータに正常にアクセスする場合のディレクトリ。

SVM管理者は、Windowsクライアントのユーザがに表示およびアクセスできるかどうかを制御します ~snapshot 共有上のディレクトリを有効または無効にします showsnapshot vserver cifs share properties familiesコマンドを使用した共有プロパティ。

をクリックします showsnapshot 共有プロパティが無効になっているため、SMB 2.xを使用するWindowsクライアントのユーザはを表示できません ~snapshot ディレクトリにあり、内のSnapshotコピーにはアクセスできません ~snapshot ディレクトリ（へのパスを手動で入力した場合も含む） ~snapshot またはディレクトリ内の特定のSnapshotコピーにコピーします。

をクリックします showsnapshot 共有プロパティが有効になっています。SMB 2.xを使用するWindowsクライアントのユーザは引き続きを表示できません ~snapshot 共有のルート、または共有のルートより下のジャンクションまたはディレクトリ内のディレクトリ。ただし、共有に接続したユーザは非表示のにアクセスでき

まず ~snapshot ディレクトリを手動で追加します \~snapshot 共有パスの末尾に移動します。隠れた者だ ~snapshot ディレクトリには、次の2つのエントリポイントからアクセスできます。

- を共有のルートに追加します
- を共有スペースのすべてのジャンクションポイントでクリックします

隠れた者だ ~snapshot 共有内のジャンクション以外のサブディレクトリからディレクトリにアクセスすることはできません。

例

次の例に示す設定では、「eng」共有へのSMB 2.x接続を使用するWindowsクライアントのユーザがにアクセスできます ~snapshot ディレクトリを手動で追加します \~snapshot を共有パス（共有のルート、およびパス内のすべてのジャンクションポイント）に設定します。隠れた者だ ~snapshot ディレクトリには、次の3つのパスからアクセスできます。

- \\vs1\eng\~snapshot
- \\vs1\eng\projects1\~snapshot
- \\vs1\eng\projects2\~snapshot

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

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

以前のバージョン機能を使用してファイルとフォルダをリカバリする

以前のバージョン機能の概要を使用したファイルとフォルダのリカバリ

Microsoft の以前のバージョン機能は、Snapshot コピーを何らかの形でサポートしているファイルシステムで、それらが有効になっている場合に使用できます。Snapshot テクノロジは ONTAP に不可欠なテクノロジの 1 つです。ユーザは、Windows クライアントで Microsoft の以前のバージョン機能を使用して、Snapshot コピーからファイルとフォルダをリカバリできます。

以前のバージョン機能を使用すると、ストレージ管理者の手を借りなくても、一連の Snapshot コピーを参照

したり、Snapshot コピーからデータをリストアしたりできます。以前のバージョン機能は設定できません。常に有効になります。ストレージ管理者が Snapshot コピーを共有でできるようにした場合、ユーザは以前のバージョン機能を使用して次の作業を実行できます。

- 誤って削除したファイルをリカバリする。
- 誤って上書きしたファイルをリカバリする。
- 作業中にファイルのバージョンを比較します。

Snapshot コピーに格納されているデータは読み取り専用です。ファイルに変更を加えるには、ファイルのコピーを別の場所に保存する必要があります。Snapshot コピーは定期的に削除されるため、以前のバージョンのファイルを残しておく場合は、以前のバージョン機能で格納されたファイルのコピーを作成しておく必要があります。

Microsoft の以前のバージョン機能を使用するための要件

CIFS サーバで Microsoft の以前のバージョン機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。また、Snapshot コピーの設定の要件についても確認しておく必要があります。

ONTAP のバージョンの要件

は、以前のバージョンをサポートします

SMB プロトコルのバージョン

Storage Virtual Machine （SVM ONTAP）については、すべてのバージョンの SMB で以前のバージョン機能がサポートされます。

Windows クライアントの要件

ユーザが以前のバージョン機能を使用して Snapshot コピー内のデータにアクセスするには、Windows クライアントでこの機能がサポートされている必要があります。

以前のバージョンをサポートする Windows クライアントに関する最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

Snapshot コピーの設定の要件

以前のバージョン機能を使用して Snapshot コピー内のデータにアクセスするには、有効な Snapshot ポリシーがデータを含むボリュームに関連付けられ、クライアントが Snapshot データにアクセスできるようになっていて、Snapshot コピーが存在している必要があります。

Snapshot コピーのデータを表示および管理するには、イゼンノバージョンタブを使用します

Windows クライアントマシンのユーザは、Windows のプロパティウィンドウの以前のバージョンタブを使用して、Storage Virtual Machine （SVM）管理者を介さずに Snapshot コピーに格納されたデータをリストアできます。

このタスクについて

管理者が共有を含むボリュームで Snapshot コピーを有効にしている場合、および管理者が Snapshot コピーを表示するように共有を設定している場合は、以前のバージョンタブで SVM に格納されているデータの Snapshot コピーのデータを表示および管理することしかできません。

手順

1. エクスプローラで、CIFS サーバに格納されたデータのマッピングされたドライブの内容を表示します。
2. Snapshot コピーを表示または管理するマッピングされたネットワークドライブのファイルまたはフォルダを右クリックします。
3. * プロパティ * をクリックします。

選択したファイルまたはフォルダのプロパティが表示されます。

4. [以前のバージョン] タブをクリックします。

選択したファイルまたはフォルダの使用可能な Snapshot コピーのリストが [フォルダバージョン:] ボックスに表示されます。表示された Snapshot コピーは、Snapshot コピー名のプレフィックスと作成時のタイムスタンプで識別できます。

5. [* フォルダーバージョン:] ボックスで、管理するファイルまたはフォルダのコピーを右クリックします。
6. 適切な操作を実行します。

状況	実行する処理
Snapshot コピーのデータを表示します	• 開く * をクリックします。
Snapshot コピーからデータのコピーを作成します	[* コピー (Copy)] をクリックします

Snapshot コピーのデータは読み取り専用です。[以前のバージョン] タブにリストされているファイルやフォルダを変更する場合は、変更するファイルやフォルダのコピーを書き込み可能な場所に保存し、コピーを変更する必要があります。

7. スナップショット・データの管理が終了したら **OK** をクリックして * プロパティ * ダイアログ・ボックスを閉じます

以前のバージョンタブを使用して Snapshot データを表示および管理する方法の詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

"Microsoft TechNet ライブラリ: technet.microsoft.com/en-us/library/"

Snapshot コピーが以前のバージョン機能で利用できるかどうかを確認します

有効な Snapshot ポリシーが共有を含むボリュームに適用されていて、ボリューム設定で Snapshot コピーへのアクセスが許可されている場合にのみ、以前のバージョンタブで Snapshot コピーを表示できます。Snapshot コピーの使用可否を確認すると、以前のバージョン機能を使用してアクセス可能かどうか確認できます。

手順

1. 共有データが存在するボリュームで自動Snapshotコピーが有効になっているかどうか、およびクライアントがSnapshotディレクトリにアクセスできるかどうかを確認します。`volume show -vserver vservice-name -volume volume-name -fields vservice, volume, snapdir-access, snapshot-policy, snapshot-count`

出力には、ボリュームに関連付けられている Snapshot ポリシー、クライアントの Snapshot ディレクトリアクセスが有効かどうか、および使用可能な Snapshot コピーの数が表示されます。

2. 関連付けられているSnapshotポリシーが有効になっているかどうかを確認します。`volume snapshot policy show -policy policy-name`
3. 使用可能なSnapshotコピーの一覧を表示します。`volume snapshot show -volume volume_name`

Snapshot ポリシーおよび Snapshot スケジュールの設定と管理の詳細については、を参照してください "[データ保護](#)"。

例

次の例は、「data」上の共有データと使用可能な Snapshot コピーを含む「data」という名前のボリュームに関連付けられている Snapshot ポリシーに関する情報を表示します。


```

cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1

                Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
    Schedule      Count      Prefix      SnapMirror Label
    -----
    hourly        6      hourly      -
    daily          2      daily       daily
    weekly         2      weekly      weekly

cluster1::> volume snapshot show -volume data1

                ---Blocks---
Vserver  Volume  Snapshot      State      Size Total% Used%
-----
vs1      data1
        weekly.2012-12-16_0015  valid      408KB    0%    1%
        daily.2012-12-22_0010  valid      420KB    0%    1%
        daily.2012-12-23_0010  valid      192KB    0%    0%
        weekly.2012-12-23_0015  valid      360KB    0%    1%
        hourly.2012-12-23_1405  valid      196KB    0%    0%
        hourly.2012-12-23_1505  valid      196KB    0%    0%
        hourly.2012-12-23_1605  valid      212KB    0%    0%
        hourly.2012-12-23_1705  valid      136KB    0%    0%
        hourly.2012-12-23_1805  valid      200KB    0%    0%
        hourly.2012-12-23_1905  valid      184KB    0%    0%

```

関連情報

[以前のバージョン機能のアクセスを有効にする Snapshot 設定の作成](#)

"データ保護"

以前のバージョン機能のアクセスを有効にする **Snapshot** 設定を作成します

Snapshot コピーへのクライアントアクセスが有効で、Snapshot コピーが存在する場合は、常に以前のバージョン機能を使用できます。Snapshot コピーの設定がこれらの要件を満たしていない場合は、要件を満たすように Snapshot コピーの設定を作成できます

す。

手順

1. [以前のバージョン機能]からのアクセスを許可する共有が含まれているボリュームにSnapshotポリシーが関連付けられていない場合は、を使用してSnapshotポリシーをボリュームに関連付けて有効にします
`volume modify` コマンドを実行します

を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

2. を使用して、Snapshotコピーへのアクセスを有効にします `volume modify` コマンドを使用してを設定します `-snap-dir` オプションをに設定します `true`。

を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

3. を使用して、Snapshotポリシーが有効になっていること、およびSnapshotディレクトリへのアクセスが有効になっていることを確認します `volume show` および `volume snapshot policy show` コマンド

を使用する方法の詳細については、を参照してください `volume show` および `volume snapshot policy show` コマンドについては、マニュアルページを参照してください。

Snapshot ポリシーおよび Snapshot スケジュールの設定と管理の詳細については、を参照してください "[データ保護](#)"。

関連情報

["データ保護"](#)

ジャンクションを含むディレクトリのリストアに関するガイドライン

以前のバージョンを使用してジャンクションポイントを含むフォルダをリストアする場合は、一定のガイドラインに注意する必要があります。

以前のバージョンを使用して、ジャンクションポイントである子フォルダを含むフォルダをリストアすると、が表示されてリストアに失敗することがあります `Access Denied` エラー。

リストアしようとしているフォルダにジャンクションが含まれているかどうかは、を使用して確認できます `vol show` コマンドにを指定します `-parent` オプションを使用することもできます `vserver security trace` ファイルおよびフォルダのアクセス問題に関する詳細なログを作成するコマンド。

関連情報

[NAS ネームスペース内でのデータボリュームの作成と管理](#)

SMB サーバベースのサービスを導入

ホームディレクトリを管理します

ONTAP で動的ホームディレクトリを有効にする方法

ONTAP ホームディレクトリを使用すると、SMB 共有を設定し、ユーザと一連の変数に基づいてさまざまなディレクトリにマッピングすることができます。ユーザごとに別個の共有を作成するのではなく、1つの共有を設定し、いくつかのホームディレクトリパラメータを指定して、エントリポイント（共有）とホームディレクトリ（SVM上のディレクトリ）間の関係をユーザ単位で定義します。

ゲストユーザとしてログインしたユーザは、ホームディレクトリを持ちません。また、他のユーザのホームディレクトリにアクセスすることはできません。ユーザとディレクトリのマッピング方法を決定する4つの変数があります。

• * 共有名 *

ユーザの接続先として作成する共有の名前です。この共有にはホームディレクトリのプロパティを設定する必要があります。

共有名には、次の動的な名前を使用できます。

- %w（ユーザのWindowsユーザ名）
- %d（ユーザのWindowsドメイン名）
- %u（ユーザのマッピングされたUNIXユーザ名）すべてのホームディレクトリ間で共有名を一意にするには、共有名に/%w または %u 変数（Variable）：共有名には両方を使用できます %d および /%w 変数（例： %d/%w または、共有名に静的な部分と変数の部分（home_ など）を含めることができます /%w`）。

• * 共有パス *

共有によって定義される、つまり、共有名の1つに関連付けられる相対パスです。各検索パスに付加されて、SVMのルートからのユーザのホームディレクトリの完全パスを生成します。静的（例：home）、動的（例：%w）、または2つの組み合わせ（例：eng/%w）。

• * 検索パス *

SVMのルートからの絶対パスのセットで、ONTAPではこのパスに基づいてホームディレクトリが検索されます。を使用して、1つ以上の検索パスを指定できます `vserver cifs home-directory search-path add` コマンドを実行します複数 ONTAP の検索パスを指定すると、有効なパスが見つかるまで、指定された順に各検索パスが試行されます。

• * ディレクトリ *

ユーザに対して作成する、そのユーザのホームディレクトリです。通常、ディレクトリ名はユーザの名前です。ホームディレクトリは、検索パスで定義されるいずれかのディレクトリに作成する必要があります。

たとえば、次のように設定します。

- ユーザ： John Smith
- ユーザのドメイン： acme
- ユーザ名： jsmith

- SVM 名： vs1
- ホームディレクトリ共有名#1： home_ %w -共有パス： %w
- ホームディレクトリ共有名#2： %w -共有パス： %d/%w
- 検索パス#1： /vol0home/home
- 検索パス#2： /vol1home/home
- 検索パス#3： /vol2home/home
- ホームディレクトリ： /vol1home/home/jsmith

シナリオ1：ユーザーがに接続します \\vs1\home_jsmith。これは最初のホームディレクトリ共有名に一致し、相対パスが生成されます jsmith。ONTAP がというディレクトリを検索するようになりました jsmith 各検索パスを順にチェックするには、次の手順に従います。

- /vol0home/home/jsmith は存在しません。検索パス#2に進みます。
- /vol1home/home/jsmith は存在します。したがって、検索パス#3はチェックされません。これで、ユーザは自分のホームディレクトリに接続されました。

シナリオ2：ユーザーがに接続する \\vs1\jsmith。これは2番目のホームディレクトリ共有名に一致し、相対パスが生成されます acme/jsmith。ONTAP がというディレクトリを検索するようになりました acme/jsmith 各検索パスを順にチェックするには、次の手順に従います。

- /vol0home/home/acme/jsmith は存在しません。検索パス#2に進みます。
- /vol1home/home/acme/jsmith は存在しません。検索パス#3に進みます。
- /vol2home/home/acme/jsmith は存在しません。ホームディレクトリが存在しないため、接続は失敗します。

ホームディレクトリ共有

ホームディレクトリ共有を追加します

SMB ホームディレクトリ機能を使用する場合、共有プロパティにホームディレクトリプロパティを含む共有を少なくとも 1 つ追加する必要があります。

このタスクについて

ホームディレクトリ共有は、共有の作成時にを使用して作成できます vserver cifs share create コマンドを入力するか、を使用して、既存の共有をいつでもホームディレクトリ共有に変更できます vserver cifs share modify コマンドを実行します

ホームディレクトリ共有を作成するには、を含める必要があります homedirectory の値 -share -properties オプションは、共有を作成または変更するときに使用します。共有名と共有パスは変数を使用して指定できます。変数はユーザがそれぞれのホームディレクトリに接続するときに動的に変換されます。パスで使用できる変数はです %w、`%d`および `%u` Windows ユーザ名、ドメイン、マッピングされたUNIX ユーザ名にそれぞれ対応します。

手順

1. ホームディレクトリ共有を追加：+ vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties homedirectory[,...]

`-vserver vs1` 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。

`-share-name share-name` ホームディレクトリ共有名を指定します。

共有名にリテラル文字列が含まれている場合は、必須の変数の1つに加えて、必要な変数も含まれています `%w`、`%u` または `%d`ONTAP`` がリテラル文字列を変数として処理しないようにするには、リテラル文字列の前に`%`（パーセント）文字を付ける必要があります（例： ``%%w``）。

- 共有名にはどちらかを使用する必要があります `%w` または `%u` 変数 (Variable) ；
 - 共有名にはさらにを含めることができます `%d` 変数（例： `%d/%w`）または共有名の静的な部分（例： `home1_/%w`）。
 - 管理者が、他のユーザのホームディレクトリに接続するために、またはユーザが他のユーザのホームディレクトリに接続するのを許可するために共有を使用する場合は、動的な共有名のパターンの先頭にチルダ（`~`）を付ける必要があります。
- `vserver cifs home-directory modify` は、を設定してこのアクセスを有効にする場合に使用します `-is-home-dirs-access-for-admin-enabled` オプションをに設定します `true`) または `advanced` オプションを設定します `-is-home-dirs-access-for-public-enabled` 終了：
`true`。

`-path path` ホームディレクトリの相対パスを指定します。

`-share-properties homedirectory[,...]` その共有の共有プロパティを指定します。を指定する必要があります `homedirectory` 価値。追加の共有プロパティをカンマで区切って指定できます。

1. を使用して、ホームディレクトリ共有が追加されたことを確認します `vserver cifs share show` コマンドを実行します

例

次のコマンドは、という名前のホームディレクトリ共有を作成します `%w`。 `oplocks`、`browsable` および `changenotify` 共有プロパティは、に加えて設定します `homedirectory` 共有プロパティ。



この例で表示されているのは、SVM の共有の出力の一部です。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vserver cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable		
			changenotify		
			homedirectory		

ホームディレクトリ検索パスを追加しています

自動ノードリファラルの使用に関する要件とガイドライン

ユーザのホームディレクトリへのアクセスの管理

ホームディレクトリ共有には、一意なユーザ名が必要です

を使用してホームディレクトリ共有を作成する場合は、一意のユーザ名を割り当てるように注意してください `%w` (Windows ユーザ名) または `%u` (UNIX ユーザ名) 変数。共有を動的に生成します。共有名はユーザ名にマッピングされます。

静的共有の名前とユーザの名前が同じ場合、次の 2 つの問題が発生する可能性があります。

- ユーザがを使用してクラスタ上の共有のリストを表示したとき `net view` コマンドを実行すると、同じユーザ名を持つ 2 つの共有が表示されます。
- ユーザがその共有名に接続すると、常に静的共有に接続され、同じ名前のホームディレクトリ共有にはアクセスできません。

たとえば、「`administrator`」という名前の共有があり、「`administrator`」という名前の Windows ユーザ名が割り当てられているとします。ホーム・ディレクトリ共有を作成し、その共有に接続すると、「管理者」のホーム・ディレクトリ共有ではなく、「管理者」の静的共有に接続されます。

共有名が重複している問題を解決するには、次のいずれかの手順を実行します。

- 静的共有の名前を変更し、ユーザのホームディレクトリ共有と競合しないようにします。
- ユーザに新しいユーザ名を割り当てて、静的共有名と競合しないようにします。
- を使用する代わりに、「`home`」などの静的な名前を使用して CIFS ホームディレクトリ共有を作成します `%w` 共有名との競合を回避するためのパラメータ。

アップグレード後に静的ホームディレクトリ共有名が受ける影響

ホームディレクトリ共有名にはのどちらかが含まれている必要があります `%w` または `%u` 動変数。新しい要件がある ONTAP のバージョンにアップグレードしたあとに、既存の静的ホームディレクトリ共有名が受ける影響について理解しておく必要があります。

ホームディレクトリの設定に静的共有名が含まれている場合に ONTAP にアップグレードしても、静的ホームディレクトリ共有名は変更されず、共有も有効なままです。ただし、どちらも含まない新しいホームディレクトリ共有を作成することはできません `%w` または `%u` 変数 (Variable) :

ユーザのホームディレクトリ共有名にどちらかの変数を含めるという必須条件によって、すべての共有名がホームディレクトリ設定全体で一貫であることが保証されます。必要に応じて、静的ホームディレクトリ共有名を、どちらかを含む名前に変更できます `%w` または `%u` 変数 (Variable) :

ホームディレクトリ検索パスを追加します

ONTAP の SMB ホームディレクトリを使用する場合は、ホームディレクトリ検索パスを少なくとも 1 つ追加する必要があります。

このタスクについて

を使用して、ホームディレクトリ検索パスを追加できます `vserver cifs home-directory search-path add` コマンドを実行します

。 `vserver cifs home-directory search-path add` コマンドはで指定されたパスをチェックします `-path` オプション（コマンド実行時）。指定したパスが存在しない場合は、続行するかどうかを確認するメッセージが表示されます。お前が選べ `y` または `n`。をクリックします `y` 続行するには、ONTAP が検索パスを作成します。ただし、ホームディレクトリ設定で検索パスを使用するには、あらかじめディレクトリ構造を作成しておく必要があります。続行しない場合、コマンドは失敗し、検索パスは作成されません。その後、パスディレクトリ構造を作成し、を再実行できます `vserver cifs home-directory search-path add` コマンドを実行します

手順

1. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vs1 -path /home1`
2. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory search-path show` コマンドを実行します

例

次の例は、パスを追加します `/home1` SVM `vs1`のホームディレクトリ設定に移動します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

次の例は、パスの追加を試みます `/home2` SVM `vs1`のホームディレクトリ設定に移動します。パスが存在しません。続行しないように選択します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

関連情報

ホームディレクトリ共有の追加

`%w` 変数と `%d` 変数を使用して、ホームディレクトリの設定を作成します

を使用して、ホームディレクトリ設定を作成できます `%w` および `%d` 変数。ユーザは、動的に作成された共有を使用してホームディレクトリ共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vs1 -vserver_name %w -qtree-path %d/%w`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vs1 -share-name %w -path %d/%w -share-properties homedirectory[,...]`

-vserver vs1 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。

-share-name %w ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ONTAP によって共有名が動的に作成されます。共有名の形式は `_windows_user_name` です。

-path %d/%w ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに `_domain/windows_user_name` の形式で相対パスが動的に作成されます。

-share-properties homedirectory[,...]+ その共有の共有プロパティを指定します。を指定する必要があります homedirectory 価値。追加の共有プロパティをカンマで区切って指定できます。
5. を使用して、共有が目的の設定になっていることを確認します `vserver cifs share show` コマンドを実行します
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vs1 -path %d/%w`

-vserver vs1 検索パスを追加するCIFS対応のSVMを指定します。

-path %d/%w 検索パスの絶対ディレクトリパスを指定します。
7. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory search-path show` コマンドを実行します
8. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。

たとえば、パスがのqtreeを作成したとします `/vol/vol1/users` ディレクトリを作成するユーザ名は `mydomain\user1` で、次のパスでディレクトリを作成します。
`/vol/vol1/users/mydomain/user1`

にマウントされた「home1」という名前のボリュームを作成した場合 `/home1` では、次のパスでディレクトリを作成します。 `/home1/mydomain/user1`
9. ドライブをマッピングするか、UNC パスを使用して、ユーザがホームディレクトリ共有に正常に接続できることを確認します。

たとえば、ユーザ `mydomain\user1` が、SVM vs1 上にあるディレクトリ（手順8で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

例

次の例のコマンドでは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は %w です
- 相対ホームディレクトリパスは %d/%w です
- ホームディレクトリを含むために使用される検索パス /home1、は、NTFSセキュリティ形式で設定されているボリュームです。
- 設定は SVM vs1 上に作成されます。

ユーザが Windows ホストからホームディレクトリにアクセスする場合には、このようなホームディレクトリ設定を使用できます。また、ユーザが Windows ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が Windows ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changesotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
        CIFS Server NetBIOS Name: VS1
                Path: %d/%w
                Share Properties: oplocks
                                browsable
                                changesotify
                                homedirectory
                Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
        File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
        Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

関連情報

%u 変数を使用してホームディレクトリを設定します

追加のホームディレクトリの設定

SMB ユーザのホームディレクトリパスに関する情報を表示する

%u 変数を使用してホームディレクトリを設定します

を使用して、ホームディレクトリを設定を作成し、共有名を指定できます %w 変数ですが、を使用します %u ホームディレクトリ共有の相対パスを指定する変数。これにより、ユーザは、ホームディレクトリの実際の名前やパスを意識することなく、Windows ユーザ名を使用して動的に作成された共有を使用してホームディレクトリ共有に接続できます。

手順

1. ユーザのホームディレクトリを含むqtreeを作成します。 `volume qtree create -vserver vsserver_name -qtree-path qtree_path`
2. qtreeで正しいセキュリティ形式が使用されていることを確認します。 `volume qtree show`
3. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
4. ホームディレクトリ共有を追加します。 `vserver cifs share create -vserver vsserver -share-name %w -path %u -share-properties homedirectory ,...]`

-vserver vsserver 検索パスを追加するCIFS対応のStorage Virtual Machine (SVM) を指定します。

-share-name %w ホームディレクトリ共有名を指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _windows_user_name の形式で共有名が動的に作成されます。



を使用することもできます %u の変数 -share-name オプションこれにより、マッピング先の UNIX ユーザ名を使用して相対共有パスが作成されます。

-path %u ホームディレクトリの相対パスを指定します。ユーザがホームディレクトリに接続すると、ユーザごとに _mapped_UNIX_user_name の形式で共有名が動的に作成されます。



このオプションの値には静的な要素も含めることができます。例： eng/%u。

-share-properties homedirectory\[,...\] その共有の共有プロパティを指定します。を指定する必要があります homedirectory 価値。追加の共有プロパティをカンマで区切って指定できます。

5. を使用して、共有が目的の設定になっていることを確認します `vserver cifs share show` コマンドを実行します
6. ホームディレクトリ検索パスを追加します。 `vserver cifs home-directory search-path add -vserver vsserver -path path`

-vserver vsserver 検索パスを追加するCIFS対応のSVMを指定します。

-path path 検索パスの絶対ディレクトリパスを指定します。

7. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory search-path show` コマンドを実行します
8. UNIXユーザが存在しない場合は、を使用してUNIXユーザを作成します `vserver services unix-user create` コマンドを実行します



ユーザをマッピングするには、Windows ユーザ名のマッピング先となる UNIX ユーザ名があらかじめ存在している必要があります。

9. 次のコマンドを使用して、UNIXユーザへのWindowsユーザのネームマッピングを作成します。 `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`



Windows ユーザを UNIX ユーザにマッピングするネームマッピングがすでに存在する場合は、このマッピング手順を実行する必要はありません。

Windows ユーザ名は対応する UNIX ユーザ名にマッピングされます。Windows ユーザは、ホームディレクトリ共有に接続すると、Windows ユーザ名に対応する共有名を使用して動的に作成されたホームディレクトリに接続することになります。その際、ディレクトリ名が UNIX ユーザ名に対応していることはユーザにはわかりません。

10. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。

たとえば、パスがのqtreeを作成したとします `/vol/vol1/users` ディレクトリを作成するユーザのマッピングされたUNIXユーザ名が「unixuser1」である場合は、次のパスでディレクトリを作成します。
`/vol/vol1/users/unixuser1。`

にマウントされた「home1」という名前のボリュームを作成した場合 `/home1`` では、次のパスでディレクトリを作成します。 ``/home1/unixuser1。`

11. ドライブをマッピングするか、UNC パスを使用して、ユーザがホームディレクトリ共有に正常に接続できることを確認します。

たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順10で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1。`

例

次の例のコマンドでは、次の設定を使用してホームディレクトリの設定を作成します。

- 共有名は %w です
- 相対ホームディレクトリパスは %u です
- ホームディレクトリを含むために使用される検索パス `/home1、` は、UNIXセキュリティ形式で設定されたボリュームです。
- 設定は SVM vs1 上に作成されます。

ユーザが Windows ホストから、または Windows ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が UNIX ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合には、このようなホームディレクトリ設定を使用できます。

```
cluster::> vservice cifs share create -vservice vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vservice cifs share show -vservice vs1 -share-name %u
```

```

                Vservice: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
        Share Properties: oplocks
                        browsable
                        changenotify
                        homedirectory
        Symlink Properties: enable
        File Mode Creation Mask: -
        Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vservice cifs home-directory search-path add -vservice vs1 -path
/home1
```

```
cluster::> vservice cifs home-directory search-path show -vservice vs1
```

Vservice	Position	Path
vs1	1	/home1

```
cluster::> vservice name-mapping create -vservice vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vservice name-mapping show -pattern user1
```

Vservice	Direction	Position
vs1	win-unix	5

Pattern: user1
Replacement: unixuser1

関連情報

[%w 変数と %d 変数を使用したホームディレクトリ設定の作成](#)

[追加のホームディレクトリの設定](#)

SMB ユーザのホームディレクトリパスに関する情報を表示する

追加のホームディレクトリの設定

を使用して、追加のホームディレクトリ設定を作成できます %w、 %d`および ` %u 変数。必要に応じてホームディレクトリの設定をカスタマイズできます。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホームディレクトリの設定を作成できます。次の表に、さまざまなホームディレクトリ設定を作成する例を示します。

で作成されるパス /vol1/user ホームディレクトリを含む...	share コマンド
をクリックして共有パスを作成します \\vs1\~win_username これにより、ユーザがに誘導されます /vol1/user/win_username	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\win_username これにより、ユーザがに誘導されます /vol1/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\win_username これにより、ユーザがに誘導されます /vol1/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
をクリックして共有パスを作成します \\vs1\unix_username これにより、ユーザがに誘導されます /vol1/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

検索パスを管理するコマンド

ONTAPには、SMBホームディレクトリ設定の検索パスを管理するためのコマンドが用意されています。たとえば、検索パスに関する情報を追加、削除、表示するためのコマンドがあります。また、検索パスの順序を変更するためのコマンドもあります。

状況	使用するコマンド
検索パスを追加します	<code>vserver cifs home-directory search-path add</code>
検索パスを表示します	<code>vserver cifs home-directory search-path show</code>

状況	使用するコマンド
検索パスの順序を変更します	<code>vserver cifs home-directory search-path reorder</code>
検索パスを削除します	<code>vserver cifs home-directory search-path remove</code>

詳細については、各コマンドのマニュアルページを参照してください。

SMB ユーザのホームディレクトリパスに関する情報を表示します

Storage Virtual Machine（SVM）上の SMB ユーザのホームディレクトリパスを表示できます。これは、複数の CIFS ホームディレクトリパスが設定されている場合に、ユーザのホームディレクトリが含まれるパスを確認するときに役立ちます。

ステップ

1. を使用して、ホームディレクトリパスを表示します `vserver cifs home-directory show-user` コマンドを実行します

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
-----	-----	-----
vs1	user1	/home/user1

関連情報

[ユーザのホームディレクトリへのアクセスの管理](#)

ユーザのホームディレクトリへのアクセスを管理します

デフォルトでは、ユーザのホームディレクトリにはそのユーザしかアクセスできません。動的な共有名の前にチルダ（ { チルダ } ）が付いている共有の場合、Windows 管理者や他のユーザ（パブリックアクセス）によるユーザのホームディレクトリへのアクセスを有効または無効にできます。

作業を開始する前に

Storage Virtual Machine（SVM）のホームディレクトリ共有に、動的な共有名の前にチルダ（ { チルダ } ）を追加した共有名を設定する必要があります。共有の命名要件は次のとおりです。

ホームディレクトリの共有名	共有に接続するコマンドの例
{ チルダ } %d { チルダ } %w	<code>net use * \\IPAddress\~domain~user/u:credentials</code>

ホームディレクトリの共有名	共有に接続するコマンドの例
{ チルダ } %w	net use * \\IPAddress\~user/u:credentials
{ チルダ } abc { チルダ } %w	net use * \\IPAddress\abc~user/u:credentials

ステップ

1. 適切な操作を実行します。

ユーザのホームディレクトリへのアクセスを有効または無効にする対象	入力するコマンド
Windows 管理者	vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false} デフォルトはです true。
任意のユーザ（パブリックアクセス）	a. 権限レベルをadvancedに設定+ set -privilege advanced b. アクセスを有効または無効にします。`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public -enabled {true

次の例は、ユーザのホームディレクトリへのパブリックアクセスを有効にします。+ set -privilege advanced [] `vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public-enabled true` []
set -privilege admin

関連情報

[SMB ユーザのホームディレクトリパスに関する情報を表示する](#)

UNIX シンボリックリンクへの SMB クライアントアクセスを設定する

ONTAP を使用して **UNIX** シンボリックリンクへの **SMB** クライアントアクセスを提供する方法

シンボリックリンクは UNIX 環境で作成されるファイルで、別のファイルまたはディレクトリへの参照が含まれます。シンボリックリンクにアクセスしたクライアントは、シンボリックリンクが参照するターゲットファイルまたはディレクトリにリダイレクトされます。ONTAP は、ワイドリンク（ローカルファイルシステムの外部にあるターゲットとの絶対リンク）を含む、相対および絶対シンボリックリンクをサポートしています。

ONTAP には、SMB クライアントが SVM で設定されている UNIX のシンボリックリンクをたどるための機能が用意されています。この機能はオプションであり、を使用して共有ごとに設定できます -symlink -properties のオプション vserver cifs share create 次のいずれかの設定を指定してコマンドを実行します。

- 読み取り / 書き込みアクセスで有効化
- 読み取り専用アクセスで有効化
- SMB クライアントに対してシンボリックリンクを非表示にして無効にしました
- SMB クライアントからシンボリックリンクへのアクセス権なしで無効になりました

共有でシンボリックリンクを有効にした場合、相対シンボリックリンクは追加の設定なしで機能します。

共有でシンボリックリンクを有効にただけでは、絶対シンボリックリンクは機能しません。最初に、シンボリックリンクの UNIX パスからデスティネーション SMB パスへのマッピングを作成する必要があります。絶対シンボリックリンクのマッピングを作成する場合、ローカルリンクが `a_widelink` ; ワイドリンクを他のストレージデバイス上のファイルシステムにリンクするか、同じ ONTAP システム上の別々の SVM でホストされているファイルシステムにリンクするかを指定できます。widelink を作成するときは、そのクライアントが参照するための情報を含める必要があります。つまり、クライアントがディレクトリのリパースジャンクションポイントを検出するためのポイントを作成します。ローカル共有外のファイルまたはディレクトリへの絶対シンボリックリンクを作成しても、局所性をローカルに設定すると、ONTAP はターゲットへのアクセスを許可しません。



クライアントがローカルシンボリックリンク（絶対または相対）を削除しようとした場合、シンボリックリンクのみが削除され、ターゲットファイルまたはターゲットディレクトリは削除されません。それに対して、クライアントがワイドリンクを削除しようとした場合には、ワイドリンクが参照する実際のターゲットファイルやターゲットディレクトリが削除されることがあります。クライアントは SVM 外のターゲットファイルまたはディレクトリを明示的に開いて削除できるため、ONTAP ではこの操作を制御できません。

• * リパースポイントと ONTAP ファイルシステムサービス *

`a_reparse point_` は、オプションでファイルとともにボリュームに格納できる NTFS ファイルシステムオブジェクトです。リパースポイントは、SMB クライアントが NTFS 形式のボリュームで作業する際に、拡張ファイルシステムサービスを受け取る機能を提供します。リパースポイントは、リパースポイントのタイプを識別する標準のタグと、クライアントがさらに処理するために SMB クライアントが取得できるリパースポイントのコンテンツで構成されます。ファイルシステムの拡張機能で利用できるオブジェクトタイプの中で、ONTAP は、リパースポイントタグを使用した NTFS シンボリックリンクとディレクトリジャンクションポイントのサポートを実装しています。リパースポイントの内容を認識できない SMB クライアントは、単に無視し、リパースポイントで有効になる可能性がある拡張ファイルシステムサービスを提供しません。

• * ディレクトリジャンクションポイントおよびシンボリックリンクの ONTAP サポート *

ディレクトリジャンクションポイントは、ファイルが格納されている別の場所（別のパス（シンボリックリンク）または別のストレージデバイス（ワイドリンク）を参照できる、ファイルシステムディレクトリ構造内の場所です。ONTAP SMB サーバでは、ディレクトリのジャンクションポイントをリパースポイントとして Windows クライアントに公開し、ディレクトリのジャンクションポイントがトラバースされたときに対応したクライアントが ONTAP からリパースポイントのコンテンツを取得できるようにします。その結果、異なるパスやストレージデバイスを、同じファイルシステムに属しているかのように移動して接続することができます。

• * リパースポイントオプションを使用したワイドリンクサポートの有効化 *

。 `-is-use-junctions-as-reparse-points-enabled` ONTAP 9では、オプションはデフォルトで有効になっています。すべての SMB クライアントがワイドリンクをサポートしているわけではないため、情報を有効にするオプションはプロトコルバージョンごとに設定可能であり、サポート対象とサポー

ト対象外の両方の SMB クライアントに対応できるようにします。ONTAP 9.2以降のリリースでは、オプションを有効にする必要があります `-widelink-as-reparse-point-versions` ワイドリンクを使用して共有にアクセスする各クライアントプロトコル（デフォルトはSMB1）。以前のリリースでは、デフォルトの SMB1 を使用してアクセスされるワイドリンクのみがレポートされ、SMB2 または SMB3 を使用するシステムはワイドリンクにアクセスできませんでした。

詳細については、Microsoft NTFS のマニュアルを参照してください。

["Microsoft のドキュメント：「Reparse Points」](#)

SMB アクセス用に UNIX シンボリックリンクを設定する場合の制限

SMB アクセス用に UNIX シンボリックリンクを設定する際には、一定の制限事項を理解しておく必要があります。

制限（Limit）	説明
4時45分	CIFS サーバ名の FQDN を使用して指定できる CIFS サーバ名の最大文字数。 <div> 代わりに、CIFS サーバ名を NetBIOS 名として指定できますが、その場合は 15 文字に制限されます。</div>
80	共有名の最大文字数。
256	シンボリックリンクを作成するとき、または既存のシンボリックリンクのUNIXパスを変更するときに指定できるUNIXパスの最大長。UNIXパスはで始まる必要があります/ (slash) and end with a /。先頭と末尾のスラッシュは、256 文字の制限に含まれます。
256	シンボリックリンクの作成時または既存のシンボリックリンクのCIFSパスの変更時に指定できるCIFSパスの最大長。CIFSパスはで始まる必要があります/ (slash) and end with a /。先頭と末尾のスラッシュは、256 文字の制限に含まれます。

関連情報

[SMB 共有のシンボリックリンクマッピングの作成](#)

CIFS サーバオプションを使用して、ONTAP で DFS の自動通知を制御する

共有に接続する SMB クライアントに DFS 対応を通知する方法は、CIFS サーバオプションで制御されます。ONTAP では、クライアントが SMB 経由でシンボリックリンクにアクセスするときに DFS リファールを使用するため、このオプションを無効または有効にしたときの影響を理解しておく必要があります。

DFS に対応していることを CIFS サーバが SMB クライアントに自動的に通知するかどうかは、CIFS サーバオプションで指定します。デフォルトでは、このオプションは有効になっており、CIFS サーバは DFS に対応していることを常に SMB クライアントに（たとえシンボリックリンクへのアクセスが無効になっている共有に接続する場合でも）通知します。シンボリックリンクへのアクセスが有効になっている共有にクライアントが接続する場合にのみ、DFS に対応していることを CIFS サーバがクライアントに通知するようにするには、このオプションを無効にします。

このオプションを無効にすると次のような影響があることに注意してください。

- シンボリックリンクの共有設定は変更されません。
- シンボリックリンクアクセス（読み取り / 書き込みアクセスまたは読み取り専用アクセス）を許可するように共有パラメータが設定されている場合、CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知します。

シンボリックリンクへのクライアントの接続とアクセスは中断されることなく続行されます。

- シンボリックリンクアクセスを許可しないように共有パラメータが設定されている場合（アクセスを無効にしているか共有パラメータの値が null の場合）、CIFS サーバは、その共有に接続するクライアントに DFS 対応を通知しません。

クライアントは、CIFS サーバが DFS に対応しているというキャッシュされた情報を保持しており、CIFS サーバはそのことを通知しなくなるので、シンボリックリンクアクセスが無効になっている共有に接続されたクライアントは、CIFS サーバオプションが無効になったあとでそれらの共有にアクセスできなくなることがあります。オプションが無効になったあとで、それらの共有に接続されたクライアントをリポートし、キャッシュされた情報を消去する必要があります。

これらの変更は SMB 1.0 の接続には適用されません。

SMB 共有で UNIX シンボリックリンクサポートを設定する

SMB 共有の作成時に、または既存の SMB 共有の変更によっていつでも、シンボリックリンクの共有プロパティ設定を指定することによって、SMB 共有で UNIX シンボリックリンクのサポートを設定できます。UNIX シンボリックリンクのサポートはデフォルトで有効になっています。UNIX シンボリックリンクのサポートを共有で無効にすることもできます。

このタスクについて

SMB 共有で UNIX シンボリックリンクのサポートを設定する場合は、次の設定のいずれかを選択できます。

設定	説明
enable（廃止予定*）	読み取り / 書き込みアクセスに対してシンボリックリンクを有効にします。
read_only（廃止予定*）	読み取り専用アクセスに対してシンボリックリンクを有効にします。この設定はワイドリンクには適用されません。ワイドリンクアクセスは常に読み取り / 書き込みです。

設定	説明
hide（廃止予定*）	SMB クライアントにシンボリックリンクが表示されないようにします。
no-strict-security	クライアントに共有の範囲を越えるシンボリックリンクの参照を許可します。
symlinks	読み取り / 書き込みアクセスに対してローカルシンボリックリンクを有効にします。CIFSオプションが設定されていても、DFS通知は生成されません is-advertise-dfs-enabled がに設定されます true。これがデフォルト設定です。
symlinks-and-widelinks	読み取り / 書き込みアクセスに対してローカルシンボリックリンクとワイドリンクの両方を有効にします。DFS通知は、CIFSオプションが指定されている場合でも、ローカルシンボリックリンクとワイドリンクの両方に対して生成されます is-advertise-dfs-enabled がに設定されます false。
disable	シンボリックリンクとワイドリンクを無効にします。CIFSオプションが設定されていても、DFS通知は生成されません is-advertise-dfs-enabled がに設定されます true。
""（null、未設定）	シンボリックリンクを共有で無効にします。
-（未設定）	シンボリックリンクを共有で無効にします。



- ONTAP の今後のリリースでは、`enable`, `hide`, `_read-only` パラメータは廃止されており、削除される可能性があります。

手順

1. シンボリックリンクのサポートを設定または無効化します。

条件	入力するコマンド
新しい SMB 共有	<code>`+vserver cifs share create -vserver vservice_name -share-name share_name -path path -symlink -properties {enable</code>
hide	<code>read-only</code>
""	<code>-</code>
symlinks	<code>symlinks-and-widelinks</code>

条件	入力するコマンド
disable},...]+`	既存の SMB 共有
`+vserver cifs share modify -vserver vs1 -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. SMB共有の設定が正しいことを確認します。vserver cifs share show -vserver vs1 -share-name share_name -instance

例

次のコマンドでは、UNIXシンボリックリンク設定をに設定して、「data1」という名前のSMB共有を作成します enable：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path /data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1 -instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
                  browsable
                  changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

関連情報

SMB 共有のシンボリックリンクマッピングの作成

SMB 共有のシンボリックリンクマッピングを作成します

SMB 共有に対する UNIX シンボリックリンクのマッピングを作成できます。親フォルダに対して相対的なファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

このタスクについて

SMB 2.x を使用している場合、Mac OS X クライアントからワイドリンクにアクセスすることはできません。Mac OS X クライアントからワイドリンクを使用して共有に接続しようとすると、接続に失敗します。ただし、SMB 1 を使用している場合は、Mac OS X クライアントでワイドリンクを使用できます。

手順

1. SMB共有のシンボリックリンクマッピングを作成するには：`vserver cifs symlink create`
`-vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

`-vserver virtual_server_name` Storage Virtual Machine (SVM) 名を示します。

`-unix-path path` UNIXパスを指定します。UNIXパスはスラッシュで始まる必要があります (/) とスラッシュで終わる必要があります (/)。

`-share-name share_name` マッピングするSMB共有の名前を指定します。

`-cifs-path path` CIFSパスを指定します。CIFSパスはスラッシュで始まる必要があります (/) とスラッシュで終わる必要があります (/)。

`-cifs-server server_name` CIFSサーバ名を指定します。CIFS サーバ名は、DNS 名 (`mynetwork.cifs.server.com` など)、IP アドレス、または NetBIOS 名として指定できます。NetBIOS名は、を使用して確認できます `vserver cifs show` コマンドを実行しますこのオプションパラメータを指定しない場合、デフォルト値のローカル CIFS サーバの NetBIOS 名が使用されます。

`-locality local|free|widelink}`は、ローカルリンク、フリーリンク、ワイドシンボリックリンクのいずれを作成するかを指定します。ローカルシンボリックリンクはローカル SMB 共有にマッピングされます。フリーシンボリックリンクはローカル SMB サーバ上の任意の場所にマッピングできます。ワイドシンボリックリンクはネットワーク上の任意の SMB 共有にマッピングされます。このオプションパラメータを指定しない場合、デフォルト値は `local` です。

`-home-directory true false}` ターゲットの共有がホームディレクトリかどうかを指定します。このパラメータはオプションですが、このパラメータをに設定する必要があります `true` ターゲットの共有がホームディレクトリとして設定されている場合。デフォルトは `false` です。

例

次のコマンドは、`vs1` という名前の SVM 上にシンボリックリンクマッピングを作成します。UNIXパスが設定されている `/src/`、SMB共有名「ソース」、CIFSパス `/mycompany/source/` およびCIFSサーバのIPアドレス123.123.123.123。ワイドリンクです。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/  
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server  
123.123.123.123 -locality widelink
```

関連情報

[SMB 共有での UNIX シンボリックリンクサポートの設定](#)

シンボリックリンクのマッピングを管理するコマンド

ONTAP には、シンボリックリンクの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
シンボリックリンクのマッピングを作成します	<code>vserver cifs symlink create</code>
シンボリックリンクのマッピングに関する情報を表示する	<code>vserver cifs symlink show</code>
シンボリックリンクのマッピングを変更する	<code>vserver cifs symlink modify</code>
シンボリックリンクのマッピングを削除する	<code>vserver cifs symlink delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

BranchCache を使用してブランチオフィスで SMB 共有のコンテンツをキャッシュする

BranchCache を使用してブランチオフィスの概要で SMB 共有のコンテンツをキャッシュする

BranchCache は、要求元のクライアントのローカルコンピュータにコンテンツをキャッシュできるようにするために Microsoft が開発した機能です。ONTAP に BranchCache を実装すると、Storage Virtual Machine（SVM）に格納されたコンテンツに SMB を使用してブランチオフィスのユーザがアクセスする際に、広域ネットワーク（WAN）の使用量を抑え、アクセス応答時間を短縮することができます。

BranchCache を設定すると、Windows BranchCache クライアントはまず SVM のコンテンツを取得し、次に取得したコンテンツをブランチオフィスのコンピュータにキャッシュします。ブランチオフィスの別の BranchCache 対応クライアントが同じコンテンツを要求すると、SVM は最初に要求元ユーザの認証と許可を実行します。次に SVM は、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

関連情報

[オフラインファイルを使用したオフラインで使用するファイルのキャッシュ](#)

要件とガイドライン

BranchCache バージョンのサポート

ONTAP でサポートされる BranchCache のバージョンを確認しておく必要があります。

ONTAP では、BranchCache 1 と強化された BranchCache 2 がサポートされています。

- Storage Virtual Machine (SVM) の SMB サーバで BranchCache を設定するときに、BranchCache 1、BranchCache 2、またはすべてのバージョンを有効にすることができます。

デフォルトでは、すべてのバージョンが有効になっています。

- BranchCache 2 のみを有効にする場合は、リモートオフィスの Windows クライアントマシンで BranchCache 2 がサポートされている必要があります。

BranchCache 2 をサポートするのは SMB 3.0 以降のクライアントだけです。

BranchCache のバージョンの詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

"Microsoft TechNet ライブラリ: technet.microsoft.com/en-us/library/"

ネットワークプロトコルのサポート要件

ONTAP BranchCache を実装するときは、ネットワークプロトコルの要件を考慮する必要があります。

ONTAP BranchCache 機能は、SMB 2.1 以降を使用して、IPv4 および IPv6 のネットワークに実装できます。

BranchCache の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、SMB 2.1 以降のプロトコルを有効にする必要があります。SMB 2.1 では、プロトコルの機能拡張により、クライアントを BranchCache 環境に含めることができます。SMB プロトコルとして BranchCache をサポートするために必要な最小バージョンを指定してください。SMB 2.1 は、BranchCache バージョン 1 をサポートします。

BranchCache バージョン 2 を使用する場合は、サポートする SMB の最小バージョンは SMB 3.0 になります。BranchCache 2 の実装に含まれるすべての CIFS サーバとブランチオフィスのマシンで、SMB 3.0 以降を有効にする必要があります。

リモートオフィスで SMB 2.1 のみサポートするクライアント、SMB 3.0 をサポートするクライアントが混在する場合は、BranchCache 1 と BranchCache 2 の両方のキャッシングをサポートする CIFS サーバに BranchCache 構成を実装することができます。



Microsoft BranchCache 機能ではファイルアクセスプロトコルとして HTTP / HTTPS と SMB プロトコルの両方がサポートされますが、ONTAP BranchCache でサポートされるのは SMB のみです。

ONTAP および Windows ホストのバージョン要件

BranchCache を設定するには、ONTAP やブランチオフィスの Windows ホストが特定

のバージョン要件を満たしている必要があります。

BranchCache を設定するには、クラスタの ONTAP のバージョンや対象となるブランチオフィスのクライアントで、SMB 2.1 以降と BranchCache の機能をサポートしている必要があります。また、ホスト型キャッシュモードを設定する場合は、サポートされているホストをキャッシュサーバに使用する必要があります。

BranchCache 1 は、次の ONTAP バージョンと Windows ホストでサポートされています。

- コンテンツサーバ：ONTAP を備えた Storage Virtual Machine (SVM)
- キャッシュサーバ：Windows Server 2008 R2 または Windows Server 2012 以降
- ピアまたはクライアント：Windows 7 Enterprise、Windows 7 Ultimate、Windows 8、Windows Server 2008 R2、または Windows Server 2012 以降

BranchCache 2は、次のONTAPバージョンおよびWindowsホストでサポートされています。

- コンテンツサーバ：ONTAP を備えた SVM
- キャッシュサーバ：Windows Server 2012 以降
- ピアまたはクライアント：Windows 8 または Windows Server 2012 以降

ONTAP で BranchCache ハッシュが無効になる理由

ONTAP でどのような場合にハッシュが無効になるかを理解すると、BranchCache の設定を計画するときに役立ちます。この情報に基づいて、設定する必要がある動作モードの決定と、BranchCache を有効にする共有を選択するかどうかの検討の助けになります。

ONTAP は、BranchCache ハッシュが有効なものであるかを管理しています。ハッシュが無効な場合、ONTAP は次にコンテンツが要求されたときにハッシュを無効にして新しいハッシュを計算します。これは、BranchCache が有効なままであることを前提としています。

ONTAP は、以下の場合にハッシュを無効にします。

- サーバキーが変更された場合。

サーバキーが変更された場合は、ONTAP によってハッシュストア内のすべてのハッシュが無効になります。

- BranchCache のハッシュストアの最大サイズに達したために、ハッシュがキャッシュからフラッシュされた場合。

このパラメータは調整可能で、ビジネス要件に合わせて変更することができます。

- SMB または NFS 経由のアクセスでファイルが変更された場合。
- 有効なハッシュが適用されたファイルがを使用してリストアされた場合 `snap restore` コマンドを実行します
- BranchCache対応のSMB共有を含むボリュームがを使用してリストアされた場合 `snap restore` コマンドを実行します

BranchCache を設定する場合は、ハッシュを格納する場所とハッシュストアのサイズを選択します。ハッシュストアの場所とサイズの選択に関するガイドラインについて理解しておく、CIFS 対応の SVM で BranchCache の設定を計画するのに役立ちます。

- ハッシュストアは、atime アップデートが許可されるボリューム上に配置する必要があります。

ハッシュストアでは、ハッシュファイルへのアクセス時間を使用して、アクセス頻度の高いファイルを管理します。atime アップデートが無効になっている場合、作成時間がこの目的に使用されます。使用頻度の高いファイルを追跡するために atime を使用することを推奨します。

- SnapMirror デスティネーションや SnapLock ボリュームなどの読み取り専用のファイルシステムにはハッシュを格納できません。
- ハッシュストアが最大サイズに達すると、新しいハッシュを格納するスペースを確保するために古いハッシュがフラッシュされます。

ハッシュストアの最大サイズを増やすと、キャッシュからフラッシュされるハッシュの量を減らすことができます。

- ハッシュを格納するボリュームが使用できないか、いっぱいである場合、またはクラスタ内通信に BranchCache サービスがハッシュ情報を取得できない問題がある場合、BranchCache サービスは使用できません。

ボリュームは、オフラインであるため、またはストレージ管理者がハッシュストアの新しい場所を指定したために、使用できないことがあります。

これは、ファイルアクセスに関する原因の問題ではありません。ハッシュストアに正常にアクセスできない場合は、ONTAP からクライアントに Microsoft 定義のエラーが返され、クライアントは通常の SMB 読み取り要求を使用してファイルを要求します。

関連情報

[SMBサーバでのBranchCacheの設定](#)

[BranchCache の設定を変更します](#)

BranchCache の推奨事項

BranchCache を設定する前に、BranchCache キャッシュを有効にする SMB 共有の決定時に考慮する必要がある推奨事項がいくつかあります。

使用する動作モードと BranchCache を有効にする SMB 共有の決定時には、次の推奨事項を考慮してください。

- リモートからキャッシュするデータが頻繁に変更されると、BranchCache の利点が十分には生かされません。
- BranchCache サービスは、複数のリモートオフスクライアントによって再利用されるファイルコンテンツ、または単一のリモートユーザが繰り返しアクセスするファイルコンテンツを含む共有の場合に役立ちます。
- Snapshot コピーのデータや SnapMirror デスティネーションのデータなどの読み取り専用コンテンツのキ

キャッシュを有効にすることを検討してください。

BranchCache を設定します

BranchCache の概要を設定

SMB サーバで BranchCache を設定するには、ONTAP コマンドを使用します。BranchCache を実装するには、クライアント、および必要に応じてコンテンツをキャッシュするブランチオフィスにホストされるキャッシュサーバも設定する必要があります。

共有ごとにキャッシュを有効にするように BranchCache を設定する場合は、BranchCache キャッシュサービスの対象となる SMB 共有で BranchCache を有効にする必要があります。

BranchCache を設定するための要件

BranchCache のセットアップを開始する前に、いくつかの前提条件を満たす必要があります。

SVM の CIFS サーバで BranchCache を設定するには、次の要件を満たしている必要があります。

- クラスタ内のすべてのノードに ONTAP がインストールされている必要があります。
- CIFS のライセンスが有効になっていて、SMB サーバが設定されている必要があります。SMB ライセンスには含まれています。"ONTAP One"。ONTAP One をお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。
- IPv4 または IPv6 のネットワーク接続が設定されている必要があります。
- BranchCache 1 の場合、SMB 2.1 以降が有効になっている必要があります。
- BranchCache 2 の場合、SMB 3.0 が有効になっていて、リモートの Windows クライアントで BranchCache 2 がサポートされている必要があります。

SMB サーバでの BranchCache の設定

BranchCache サービスを共有ごとに提供するように BranchCache を設定できます。また、すべての SMB 共有でキャッシュを自動的に有効にするように BranchCache を設定することもできます。

このタスクについて

BranchCache は SVM で設定できます。

- CIFS サーバ上のすべての SMB 共有に格納されたすべてのコンテンツに対してキャッシュサービスを提供する場合は、すべての共有の BranchCache 設定を作成できます。
- CIFS サーバ上の選択した SMB 共有に格納されたコンテンツに対してキャッシュサービスを提供する場合は、共有ごとの BranchCache 設定を作成できます。

BranchCache の設定時には、次のパラメータを指定する必要があります。

必須パラメータ	説明
SVM 名 _	BranchCache は SVM ごとに設定します。BranchCache サービスを設定する CIFS 対応の SVM を指定する必要があります。
ハッシュストアへのパス _	<p>BranchCache ハッシュは SVM ボリューム上の通常のファイルに格納されます。ONTAP にハッシュデータを格納する既存のディレクトリのパスを指定する必要があります。BranchCache ハッシュパスは読み取り / 書き込み可能である必要があります。Snapshot ディレクトリなどの読み取り専用パスは指定できません。他のデータが格納されているボリュームにハッシュデータを格納するか、ハッシュデータを格納するための別のボリュームを作成することができます。</p> <p>SVM が SVM ディザスタリカバリソースである場合、ハッシュパスをルートボリューム上にすることはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。</p> <p>ハッシュパスには、ファイル名に使用できる文字と空白を含めることができます。</p>

必要に応じて、次のパラメータを指定できます。

オプションのパラメータ	説明
サポートされているバージョン _	ONTAP では BranchCache 1 および 2 がサポートされています。バージョン 1、バージョン 2、または両方のバージョンを有効にできます。デフォルトでは、両方のバージョンが有効になります。
_ ハッシュストアの最大サイズ _	ハッシュデータストアに使用するサイズを指定できます。ハッシュデータがこの値を超えると、ONTAP は古いハッシュを削除し、新しいハッシュを格納するスペースを確保します。ハッシュストアのデフォルトサイズは 1GB です。ハッシュが過剰に破棄されない方が、BranchCache のパフォーマンスは向上します。ハッシュストアがいっぱいになるのが原因でハッシュが頻繁に破棄されていると判断した場合は、BranchCache の設定を変更して、ハッシュストアのサイズを大きくすることができます。

オプションのパラメータ	説明
_ サーバキー _	クライアントが BranchCache サーバを偽装できないようにするために BranchCache サービスによって使用されるサーバキーを指定できます。指定しない場合、サーバキーは BranchCache の設定の作成時にランダムに生成されます。サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。サーバキーにスペースを含める場合は、サーバキーを引用符で囲む必要があります。
オペレーティングモード _	<p>デフォルトでは、BranchCache は共有ごとに有効になります。</p> <ul style="list-style-type: none"> • BranchCacheを共有ごとに有効にするBranchCacheの設定を作成するには、このオプションパラメータを指定しないか、を指定します per-share。 • すべての共有でBranchCacheを自動的に有効にするには、動作モードをに設定する必要があります all-shares。

手順

1. 必要に応じて SMB 2.1 および 3.0 を有効にします。
 - a. 権限レベルを advanced に設定します。 `set -privilege advanced`
 - b. SVMのSMB設定を確認して、必要なすべてのバージョンのSMBが有効になっているかどうかを確認します。 `vserver cifs options show -vserver vserver_name`
 - c. 必要に応じて、SMB 2.1を有効にします。 `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

このコマンドを実行すると、SMB 2.0 と SMB 2.1 の両方が有効になります。

- d. 必要に応じて、SMB 3.0を有効にします。 `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
 - e. admin 権限レベルに戻ります。 `set -privilege admin`
2. BranchCacheを設定します。 `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

指定したハッシュストレージのパスが存在し、SVMによって管理されているボリューム上にある必要があります。また、パスは読み取り / 書き込み可能なボリュームにある必要があります。パスが読み取り専用であるか、または存在しない場合、コマンドは失敗します。

SVM BranchCache の追加設定で同じサーバキーを使用する場合は、サーバキーとして入力した値を記録

しておきます。BranchCache の設定に関する情報を表示するときに、サーバキーは表示されません。

3. BranchCache の設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドを実行すると、SMB 2.1 と 3.0 の両方が有効になっていることが確認され、SVM vs1 上のすべての SMB 共有でキャッシュを自動的に有効にするように BranchCache が設定されます。

```
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 show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

次のコマンドを実行すると、SMB 2.1 と 3.0 の両方が有効になっていることが確認され、SVM vs1 上の共有ごとにキャッシュを有効にするように BranchCache が設定されて、BranchCache の設定が確認されます。

```

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

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

関連情報

[要件とガイドライン：BranchCache バージョンのサポート](#)

[リモートオフィスでの BranchCache の設定に関する情報の参照先を指定します](#)

[BranchCache が有効な SMB 共有を作成](#)

[既存の SMB 共有で BranchCache を有効にします](#)

[BranchCache の設定を変更します](#)

[SMB 共有で BranchCache を無効にする手順の概要](#)

[SVM の BranchCache 設定を削除します](#)

リモートオフィスでの **BranchCache** の設定に関する情報の参照先を指定します

SMB サーバで BranchCache を設定したら、クライアントコンピュータに BranchCache をインストールして設定する必要があります。また、必要に応じて、リモートオフィスのキャッシュサーバにも BranchCache をインストールして設定する必要があります。リモートオフィスで BranchCache を設定する手順については、Microsoft から説明が提供

されています。

ブランチオフィスのクライアントを設定する手順、および必要に応じて BranchCache を使用するキャッシュサーバを Microsoft BranchCache の Web サイトで設定する手順について説明します。

["Microsoft BranchCache のドキュメント：「What's New」](#)

BranchCache が有効な SMB 共有を設定

BranchCache が有効な SMB 共有の概要を設定

SMB サーバとブランチオフィスで BranchCache を設定したら、ブランチオフィスのクライアントによるコンテンツのキャッシュを許可する SMB 共有で BranchCache を有効にすることができます。

BranchCache キャッシュは、SMB サーバ上のすべての SMB 共有で有効にするか、共有ごとに有効にすることができます。

- BranchCache を共有ごとに有効にする場合、BranchCache は共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。

既存の SMB 共有でキャッシュを有効にすると、その共有で BranchCache を有効にした時点で、ONTAP によるハッシュの計算と要求元クライアントへのメタデータの送信が開始されます。

- 共有への SMB 接続をすでに確立しているクライアントは、それ以降にその共有で BranchCache が有効になった場合、BranchCache のサポートを得ることができません。

ONTAP は、SMB セッションがセットアップされたときに共有の BranchCache のサポートを通知します。BranchCache が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容をこの共有で使用するために、いったん切断してから再接続する必要があります。



その後 SMB 共有に対する BranchCache を無効にすると、ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ（SMB サーバ）から直接データを取得します。

BranchCache が有効な SMB 共有を作成

SMB 共有の作成時にを設定して、共有で BranchCache を有効にすることができます
branchcache 共有プロパティ。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

これは、共有を作成するときのデフォルト設定です。

- BranchCache が有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。
- を設定できます branchcache Storage Virtual Machine (SVM) で BranchCache が設定されておらず有効になっていない場合も含む共有のプロパティ。

ただし、共有でキャッシュされたコンテンツを提供するには、SVM で BranchCache を設定して有効にする必要があります。

- を使用するときには共有に適用されるデフォルトの共有プロパティはないためです -share-properties パラメータを指定する場合は、に加えて共有に適用する他のすべての共有プロパティを指定する必要があります branchcache プロパティを共有するには、カンマで区切って指定します。
- 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 vservers cifs share create コマンドを実行します

ステップ

1. BranchCacheが有効なSMB共有を作成します。`+vservers cifs share create -vservers vservers_name -share-name share_name -path path -share-properties branchcache[,...]`
2. を使用して、SMB共有に対してBranchCache共有プロパティが設定されていることを確認します `vservers cifs share show` コマンドを実行します

例

次のコマンドでは、「data」という名前のBranchCacheが有効なSMB共有をパスに作成します /data SVM vs1上。デフォルトでは、オフラインファイルの設定はに設定されています manual :

```
cluster1::> vservers cifs share create -vservers vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vservers cifs share show -vservers vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
  Share Properties: branchcache
                   oplocks
                   browsable
                   changenotify
  Symlink Properties: enable
  File Mode Creation Mask: -
  Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
  File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
  Vscan File-Operations Profile: standard
```

関連情報

[単一の SMB 共有での BranchCache の無効化](#)

既存の SMB 共有で **BranchCache** を有効にします

既存のSMB共有でBranchCacheを有効にするには、を追加します `branchcache` 共有プロパティを既存の共有プロパティリストに追加します。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。

- を設定できます `branchcache Storage Virtual Machine (SVM)` でBranchCacheが設定されておらず有効になっていない場合も含む共有のプロパティ。

ただし、共有でキャッシュされたコンテンツを提供するには、SVM で BranchCache を設定して有効にする必要があります。

- を追加したとき `branchcache` 共有プロパティ共有に対する既存の共有設定と共有プロパティは維持されます。

BranchCache 共有プロパティは既存の共有プロパティリストに追加されます。を使用する方法の詳細については、を参照してください `vserver cifs share properties add` コマンドについては、マニュアルページを参照してください。

手順

1. 必要に応じて、オフラインファイルの共有設定を手動キャッシュに設定します。
 - a. を使用して、オフラインファイルの共有設定を確認します `vserver cifs share show` コマンドを実行します
 - b. オフラインファイルの共有設定が `manual` に設定されていない場合は、必要な値に変更します。

```
vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual
```
2. 既存のSMB共有でBranchCacheを有効にします。 `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. SMB共有でBranchCache共有プロパティが設定されていることを確認します。 `vserver cifs share show -vserver vserver_name -share-name share_name`

例

次のコマンドは、「data2」という名前の既存のSMB共有（パス）でBranchCacheを有効にします `/data2 SVM vs1` :


```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share properties add -vsserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

BranchCache の設定を管理および監視する

BranchCache 設定を変更

SVM 上の BranchCache サービスの設定では、ハッシュストアディレクトリのパス、最大サイズ、動作モード、サポートする BranchCachet のバージョンなどの設定を変更できます。ハッシュストアを含めるボリュームのサイズを拡張することもできます。

手順

- 1. 適切な操作を実行します。

状況	入力するコマンド
ハッシュストアディレクトリのサイズを変更する	<code>`vserver cifs branchcache modify -vserver vservice_name -hash-store-max-size {integer}[KB</code>
MB	GB
TB	PB]}`
ハッシュストアを含めるボリュームのサイズを増やします	<code>`volume size -vserver vservice_name -volume volume_name -new-size new_size[k</code>
m	g
t]` ハッシュストアを含むボリュームがいっぱいになった場合は、ボリュームのサイズを拡張できます。新しいボリュームサイズは、数字と単位で指定できます。 の詳細を確認してください " FlexVol ボリュームの管理 "	ハッシュストアディレクトリのパスを変更します

状況	入力するコマンド
<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</code>	<p><code>false}`</code> SVM が SVM ディザスタリカバリソースである場合、ハッシュパスをルートボリューム上にはできません。これは、ルートボリュームがディザスタリカバリデスティネーションにレプリケートされないためです。</p> <p>BranchCache ハッシュパスには、ファイル名に使用できる文字と空白を含めることができます。</p> <p>ハッシュパスを変更する場合は、<code>-flush-hashes</code> は、ONTAP で元のハッシュストアの場所からハッシュをフラッシュするかどうかを指定する必須パラメータです。には次の値を設定できます <code>-flush -hashes</code> パラメータ：</p> <p>を指定する場合 `true` ONTAP では、元の場所にあるハッシュが削除され、BranchCache対応クライアントから新しい要求が行われると、新しい場所に新しいハッシュが作成されます。を指定する場合 `false` を指定すると、ハッシュはフラッシュされません。+ この場合、後でハッシュストアパスを元の場所に戻して、既存のハッシュを再利用することができます。</p>
動作モードを変更します	<code>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</code>
<code>all-shares</code>	<p><code>disable}`</code></p> <p>動作モードを変更するときは、次の点に注意してください。</p> <p>SMBセッションのセットアップ時に、ONTAP によって、BranchCacheの共有のサポートが通知されます。BranchCache が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容をこの共有で使用するために、いったん切断してから再接続する必要があります。</p>
サポートする BranchCache バージョンを変更します	<code>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</code>
<code>v2-enable</code>	<code>enable-all}`</code>

2. を使用して、設定の変更を確認します `vserver cifs branchcache show` コマンドを実行します

BranchCache 設定に関する情報を表示します

Storage Virtual Machine （SVM）の BranchCache 設定に関する情報を表示できます。この情報は、設定を検証する場合や、設定を変更する前に現在の設定を確認する場合に役立ちます。

ステップ

1. 次のいずれかを実行します。

表示する項目	入力するコマンド
すべての SVM の BranchCache 設定に関する概要情報	<code>vserver cifs branchcache show</code>
特定の SVM の設定に関する詳細情報	<code>vserver cifs branchcache show -vserver vserver_name</code>

例

次の例は、SVM vs1 の BranchCache 設定に関する情報を表示します。

```
cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

BranchCache サーバキーを変更します

BranchCache サーバキーを変更するには、Storage Virtual Machine（SVM）で BranchCache の設定を変更し、別のサーバキーを指定します。

このタスクについて

サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュキャッシュをフラッシュすることにも必要になります。ハッシュのフラッシュ後、BranchCache 対応クライアントによって新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

手順

1. 次のコマンドを使用して、サーバキーを変更します。`vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

新しいサーバキーを設定する場合は、も指定する必要があります `-flush-hashes` に設定します `true`。

2. を使用して、BranchCache の設定が正しいことを確認します `vserver cifs branchcache show` コマンドを実行します

例

次の例は、SVM vs1 でスペースを含む新しいサーバキーを設定し、ハッシュキャッシュをフラッシュします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
                CIFS BranchCache Operating Modes: per_share
```

関連情報

ONTAP で BranchCache ハッシュが無効になる理由

指定したパスの **BranchCache** ハッシュを事前に計算します

単一のファイル、ディレクトリ、またはディレクトリ構造内のすべてのファイルのハッシュを事前に計算するように BranchCache サービスを設定できます。これは、BranchCache 対応の共有にあるデータのハッシュをピーク以外の時間帯に計算するのに役立ちます。

このタスクについて

ハッシュの統計を表示する前にデータサンプルを収集する場合は、を使用する必要があります statistics start およびオプションです statistics stop コマンド

- ハッシュを事前に計算する対象の Storage Virtual Machine （SVM）とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかも指定する必要があります。
- ハッシュを再帰的に計算する場合、BranchCache サービスでは、指定されたパスの下のディレクトリツリー全体を参照し、対象となる各オブジェクトのハッシュを計算します。

手順

1. 必要に応じてハッシュを事前に計算します。

ハッシュを事前に計算する対象	入力するコマンド
単一のファイルまたはディレクトリ	vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false
ディレクトリ構造内のすべてのファイルを再帰的に処理します	vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true

2. を使用して、ハッシュが計算されていることを確認します `statistics` コマンドを実行します
 - a. の統計を表示します `hashd` 目的のSVMインスタンスのオブジェクト。 `statistics show -object hashd -instance vserver_name`
 - b. コマンドを繰り返し実行して、作成済みのハッシュの数が増加していることを確認します。

例

次の例は、パスにハッシュを作成します `/data SVM vs1`に格納されているすべてのファイルとサブディレクトリで、次のコマンドを実行します。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

関連情報

"パフォーマンス監視のセットアップ"

SVM BranchCache ハッシュストアからハッシュをフラッシュします

Storage Virtual Machine（SVM）上の BranchCache ハッシュストアから、キャッシュされたハッシュをすべてフラッシュできます。これは、ブランチオフィスの BranchCache の設定を変更した場合に役立ちます。たとえば、最近キャッシュモードを分散キャッシュからホスト型キャッシュモードに再設定した場合は、ハッシュストアをフラッシュする必要があります。

このタスクについて

ハッシュのフラッシュ後、BranchCache 対応クライアントによって新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

ステップ

1. BranchCacheハッシュストアからハッシュをフラッシュします。 `vserver cifs branchcache hash-flush -vserver vserver_name`

```
vserver cifs branchcache hash-flush -vserver vs1
```

BranchCache 統計を表示します

BranchCache 統計を表示すると、さまざまな目的の中でも、キャッシュが適切に機能しているかどうかの確認、キャッシュコンテンツをクライアントに提供しているかどうかの確認、新しいハッシュデータのスペースを確保するためにハッシュファイルが削除されたかどうかの確認に特に役立ちます。

このタスクについて

。 `hashd statistic` オブジェクトには、BranchCacheハッシュに関する統計情報を提供するカウンタが含まれます。。 `cifs statistic` オブジェクトには、BranchCache関連のアクティビティに関する統計情報を提供するカウンタが含まれます。これらのオブジェクトに関する情報は、advanced 権限レベルで収集して表示できます。

手順

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

```
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
```

2. を使用して、BranchCache関連のカウンタを表示します `statistics catalog counter show` コマンドを実行します

統計カウンタの詳細については、このコマンドのマニュアルページを参照してください。

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


Object: hashd

Counter	Description

branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

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
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch

```

hash
data failed. These are failures when
attempting to read existing hash data.
It
does not include attempts to fetch hash
data
that has not yet been generated.
branchcache_hash_fetch_ok Total number of times a request to fetch
hash
data succeeded.
branchcache_hash_sent_bytes Total number of bytes sent to clients
requesting hashes.
branchcache_missing_hash_bytes
Total number of bytes of data that had
to be
read by the client because the hash for
that
content was not available on the server.
....Output truncated....

```

3. を使用して、BranchCache関連の統計を収集します `statistics start` および `statistics stop` コマンド

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. を使用して、収集したBranchCache統計を表示します `statistics show` コマンドを実行します

```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

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

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

関連情報

[統計情報を表示します](#)

["パフォーマンス監視のセットアップ"](#)

BranchCache グループポリシーオブジェクトがサポートされます

ONTAP BranchCache では、BranchCache のグループポリシーオブジェクト（GPO）

をサポートしており、特定の BranchCache の設定パラメータを一元的に管理できます。BranchCache の GPO には、BranchCache のハッシュの発行 GPO と BranchCache のハッシュバージョンサポート GPO の 2 つがあります。

- * BranchCache のハッシュの発行 GPO *

BranchCacheのハッシュの発行GPOはに対応します `-operating-mode` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位（OU）に含まれる Storage Virtual Machine（SVM）オブジェクトにこの値が適用されます。

- * BranchCache のハッシュバージョンサポート *

BranchCacheのハッシュバージョンサポートGPOはに対応します `-versions` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位に含まれる SVM オブジェクトにこの値が適用されます。

関連情報

CIFS サーバへのグループポリシーオブジェクトの適用

BranchCache グループポリシーオブジェクトに関する情報を表示します

CIFS サーバの Group Policy Object（GPO；グループポリシーオブジェクト）設定に関する情報を表示して、CIFS サーバが属しているドメインで BranchCache GPO が定義されているかどうか、定義されている場合は許可されている設定を確認できます。また、BranchCache GPO 設定が CIFS サーバに適用されているかどうかも確認できます。

このタスクについて

CIFS サーバが属しているドメイン内で GPO 設定が定義されていても、CIFS 対応の Storage Virtual Machine（SVM）が含まれる Organizational Unit（OU；組織単位）に適用されているとは限りません。適用される GPO 設定は、CIFS 対応の SVM に適用されているすべての定義済み GPO の一部です。GPO を介して適用された BranchCache 設定は、CLI を介して適用された設定よりも優先さ

手順

1. を使用して、Active Directoryドメインに対して定義されているBranchCache GPO設定を表示します
`vserver cifs group-policy show-defined` コマンドを実行します



この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
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: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. を使用して、CIFSサーバに適用されているBranchCache GPO設定を表示します vserver cifs group-policy show-applied コマンドを実行します`



この例で表示されているのは、コマンドで出力されるフィールドの一部です。出力は省略されています。

```
cluster1::> vsriver cifs group-policy show-applied -vsriver vs1
```

```
Vsriver: 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: version1
```

```
[...]
```

```
    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: version1
```

```
[...]
```

関連情報

[CIFS サーバ上で GPO サポートを有効または無効にします](#)

SMB 共有で BranchCache を無効にします

SMB 共有で BranchCache を無効にする手順の概要

特定の SMB 共有で BranchCache キャッシュサービスを提供する必要がなくなったが、あとでそれらの共有でキャッシュサービスが必要になる可能性がある場合は、共有ごとに BranchCache を無効にすることができます。すべての共有でキャッシュを提供するように BranchCache を設定しているが、一時的にすべてのキャッシュサービスを無効にする必要がある場合は、BranchCache 設定を変更してすべての共有で自動キャッシュを停止することができます。

SMB 共有で有効になっていた BranchCache をあとから無効にすると、ONTAP による要求元クライアントへのメタデータの送信が中止されます。データが必要なクライアントは、コンテンツサーバ (Storage Virtual

Machine（SVM）上の CIFS サーバ）から直接データを取得します。

関連情報

[BranchCache が有効な SMB 共有の設定](#)

単一の SMB 共有で **BranchCache** を無効にします

キャッシュコンテンツを使用できるようにしていた特定の共有でキャッシュサービスを提供する必要がなくなった場合は、既存の SMB 共有で BranchCache を無効にすることができます。

ステップ

1. 次のコマンドを入力します。`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

BranchCache 共有プロパティが削除されます。適用されているその他の共有プロパティは有効なままです。

例

次のコマンドは、「data2」という名前の既存の SMB 共有で BranchCache を無効にします。

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties remove -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

    Vservice: vs1
    Share: data2
CIFS Server NetBIOS Name: VS1
    Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
    Share Comment: -
    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
    Volume Name: -
    Offline Files: manual
Vscan File-Operations Profile: standard
```


すべての **SMB** 共有での自動キャッシュを停止します

Storage Virtual Machine（SVM）のすべての SMB 共有に対して BranchCache キャッシュを自動的に有効にするように設定している場合、BranchCache の設定を変更することで、すべての SMB 共有に対するコンテンツの自動キャッシュを停止することができます。

このタスクについて

すべての SMB 共有に対する自動キャッシュを停止するには、BranchCache の動作モードを共有ごとのキャッシュに変更します。

手順

1. すべてのSMB共有で自動キャッシュを停止するようにBranchCacheを設定します。 `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドは、Storage Virtual Machine（SVM、旧 Vserver）vs1 の BranchCache 設定を変更して、すべての SMB 共有に対する自動キャッシュを停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode per-share

cluster1::> vserver cifs branchcache show -vserver vs1

Vserver: vs1
Supported BranchCache Versions: enable_all
Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: per_share
```

SVM で BranchCache を有効または無効にします

CIFS サーバで **BranchCache** を無効または再度有効にしたときの動作

BranchCache を設定したあとに、ブランチオフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、CIFS サーバでキャッシュを無効にします。BranchCache を無効にするときは、それを実行した場合の動作について理解しておく必要があります

BranchCache を無効にすると、ONTAP によるハッシュの計算や要求元クライアントへのメタデータの送信が行われなくなります。ただし、ファイルアクセスは中断されません。以降に、BranchCache 対応クライアント ONTAP からアクセスするコンテンツのメタデータ情報を要求すると、Microsoft のエラーが返されます。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFS サーバから Storage Virtual Machine（SVM）に格納されている実際のコンテンツが送信さ


れます。

CIFS サーバで BranchCache を無効にしたあとは、SMB 共有で BranchCache の機能がアドバタイズされなくなります。新しい SMB 接続でデータにアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache は、CIFS サーバでいつでも再度有効にすることができます。

- BranchCache ONTAP を無効にしてもハッシュストアは削除されないため、要求されたハッシュがまだ有効であれば、BranchCache を再度有効にしたあとに、格納されたハッシュを使用してハッシュの要求に応答することができます。
- BranchCache 対応の共有に対する SMB 接続を確立したクライアントで接続を確立したときに BranchCache が無効になっていたクライアントの場合には、以降に BranchCache を再度有効にしても、BranchCache のサポートは有効になりません。

これは、SMB セッションのセットアップ時に共有に対する BranchCache のサポートが通知されるから ONTAP です。BranchCache を無効にしたときに BranchCache 対応の共有に対するセッションを確立していた場合、その共有のキャッシュされたコンテンツを使用するには、いったん切断してから再接続する必要があります。



CIFS サーバで BranchCache を無効にしたあとにハッシュストアを保存しておく必要がない場合は、手動で削除することができます。BranchCache を再度有効にするときは、ハッシュストアのディレクトリが存在することを確認する必要があります。BranchCache を再度有効にすると、BranchCache 対応の共有で BranchCache の機能がアドバタイズされるようになります。BranchCache 対応クライアントから新しい要求が行われると、ONTAP によって新しいハッシュが作成されます。

BranchCache を有効または無効にします

Storage Virtual Machine (SVM) で BranchCache を無効にするには、BranchCache の動作モードをに変更します disabled。BranchCache サービスを共有単位で提供するか、すべての共有で自動的に提供するように動作モードを変更すると、いつでも BranchCache を有効にすることができます。

手順

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache を無効にする	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</code>
共有ごとに BranchCache を有効にします	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</code>
すべての共有で BranchCache を有効にします	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code>

2. BranchCacheの動作モードが目的の設定になっていることを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次の例は、SVM vs1 で BranchCache を無効にします。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
                Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

SVM の BranchCache 設定を削除します

BranchCache 設定を削除した場合の動作

BranchCache を設定したあとに、Storage Virtual Machine（SVM）からのキャッシュされたコンテンツの提供を中止する場合は、CIFS サーバで BranchCache 設定を削除します。設定を削除するときは、それを実行した場合の動作について理解しておく必要があります。

設定を削除すると、ONTAP によってその SVM の設定情報がクラスタから削除され、BranchCache サービスが停止します。SVM のハッシュストアについては、ONTAP で削除するかどうかを選択することができます。

BranchCache 設定を削除しても、BranchCache 対応クライアントによるアクセスは中断されません。以降に、BranchCache 対応クライアントから既存の SMB 接続でキャッシュ済みのコンテンツのメタデータ情報を要求すると、ONTAP は Microsoft のエラーを返します。この場合は、クライアントでもう一度要求を送信して、実際のコンテンツを要求します。これに対する応答として、CIFS サーバから SVM に格納されている実際のコンテンツが送信されます。

BranchCache 設定を削除すると、SMB 共有で BranchCache の機能がアドバタイズされなくなります。キャッシュされていないコンテンツに新しい SMB 接続でアクセスするには、通常の SMB 読み取り要求を行います。

BranchCache 設定を削除します

Storage Virtual Machine（SVM）で BranchCache サービスの削除に使用するコマンドは、既存のハッシュを削除するか、保持するかによって異なります。

ステップ

1. 該当するコマンドを実行します。

状況	入力するコマンド
BranchCache 設定を削除し、既存のハッシュを削除します	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code>
BranchCache 設定を削除するが、既存のハッシュは保持する	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code>

例

次の例は、SVM vs1 で BranchCache 設定を削除し、既存のハッシュをすべて削除します。

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

リバートした場合の **BranchCache** の動作

ONTAP を BranchCache がサポートされないリリースにリバートするときは、それを実行した場合の動作について理解しておくことが重要です。

- ONTAP を BranchCache がサポートされないバージョンにリバートすると、BranchCache 対応クライアントに対して SMB 共有で BranchCache の機能がアドバタイズされなくなります。そのため、クライアントからハッシュ情報が要求されることはありません。

代わりに、通常の SMB 読み取り要求を使用して実際のコンテンツを要求します。これに対する応答として、SMBサーバからStorage Virtual Machine (SVM) に格納されている実際のコンテンツが送信されます。

- ハッシュストアをホストするノードを BranchCache がサポートされないリリースにリバートする場合、リバート時に出力されるコマンドを使用して、ストレージ管理者が手動で BranchCache の設定をリバートする必要があります。

このコマンドは、BranchCache の設定とハッシュを削除します。

リバートの完了後、必要に応じて、ハッシュストアが格納されていたディレクトリを手動で削除できます。

関連情報

[SVM の BranchCache 設定を削除します](#)

Microsoft リモートコピーのパフォーマンスを向上

Microsoft リモートコピーのパフォーマンスの概要を改善します

Microsoft Offloaded Data Transfer (ODX ; オフロードデータ転送) は、_コピーオフロード_とも呼ばれ、この機能を使用すると、互換性があるストレージデバイス内やスト

レイジデバイス間で、ホストコンピュータを介さずにデータを直接転送できます。

ONTAPでは、SMBプロトコルとSANプロトコルの両方でODXがサポートされます。ソースとデスティネーションのどちらについても、CIFS サーバと LUN の両方に対応しています。

ODX 以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。つまり、クライアントコンピュータはソースからデータを読み取り、デスティネーションに書き込みます。ODX ファイル転送では、データはソースからデスティネーションに直接コピーされます。

ODX オフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量（CPU、メモリ）の削減、ネットワーク I/O 帯域幅の使用量の削減などが挙げられます。

SMB 環境では、この機能は、クライアントとストレージサーバの両方で SMB 3.0 および ODX 機能がサポートされている場合にのみ使用できます。SAN 環境では、この機能は、クライアントとストレージサーバの両方で ODX 機能がサポートされている場合にのみ使用できます。ODX がサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロードファイル転送が自動的に透過的に使用されます。ODX は、ファイルをエクスプローラでドラッグアンドドロップしたか、コマンドラインのファイルコピーコマンドを使用したか、クライアントアプリケーションによってファイルコピー要求が開始されたかに関係なく使用されます。

関連情報

[Auto Location で SMB 自動ノードリファールを提供することで、クライアントの応答時間を改善します](#)

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

ODX の仕組み

ODX コピーオフロードでは、トークンベースのメカニズムを使用して、ODX 対応の CIFS サーバ内または CIFS サーバ間でデータの読み取りおよび書き込みを行います。CIFS サーバは、ホストを介してデータをルーティングするのではなく、データを表す小さなトークンをクライアントに送信します。ODX クライアントがそのトークンをデスティネーションサーバに提示すると、サーバはそのトークンで表されるデータをソースからデスティネーションに転送できます。

ODX クライアントは、CIFS サーバが ODX 対応であると認識すると、ソースファイルを開いて CIFS サーバのトークンを要求します。デスティネーションファイルを開いたあと、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

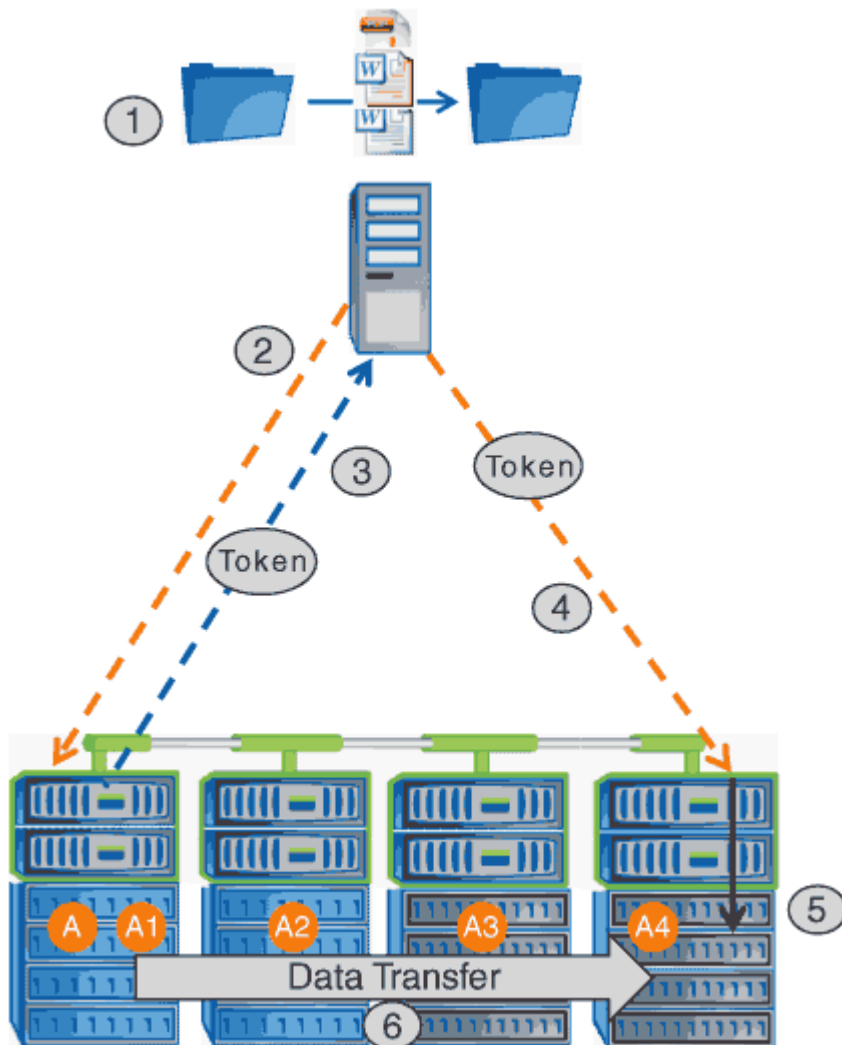


ソースとデスティネーションは、コピー処理の範囲に応じて、同じ Storage Virtual Machine（SVM）上に存在する場合も異なる SVM 上に存在する場合もあります。

トークンは、データのポイントインタイム表現として機能します。たとえば、ストレージ間でデータをコピーする場合、データセグメントを表すトークンが要求元クライアントに返され、そのトークンをクライアントがデスティネーションにコピーするため、クライアントを介して基盤となるデータをコピーする必要があります。

ONTAP では、8MB のデータを表すトークンがサポートされます。8MB を超える ODX コピーは、8MB のデータを表すトークンを複数使用して実行されます。

次の図で、ODX コピー処理に関連する手順について説明します。



1. エクスプローラを使用するか、コマンドラインインターフェイスを使用するか、仮想マシンの移行の一環として、ユーザがファイルをコピーまたは移動します。または、アプリケーションによってファイルのコピーまたは移動が開始されます。

2. ODX 対応のクライアントが、この転送要求を ODX 要求に自動的に変換します。

CIFS サーバに送信される ODX 要求には、トークン要求が含まれています。

3. CIFS サーバで ODX が有効になっていて、接続が SMB 3.0 経由の場合は、ソースのデータを論理的に表したものであるトークンが CIFS サーバによって生成されます。

4. クライアントは、データを表すトークンを受信し、書き込み要求を使用してそのトークンをデスティネーション CIFS サーバに送信します。

ネットワーク経由でソースからクライアントにコピーされ、クライアントからデスティネーションにコピーされるのは、このデータだけです。

5. トークンがストレージサブシステムに送信されます。

6. コピーまたは移動が SVM によって内部的に実行されます。

コピーまたは移動されるファイルが 8MB より大きい場合、コピーを実行するには複数のトークンが必要

になります。コピーが完了するまで、必要に応じて手順 2~6 を実行します。



ODX オフロードコピーで障害が発生した場合、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。同様に、デスティネーション CIFS サーバで ODX がサポートされていない場合、または ODX が無効になっている場合は、コピーまたは移動処理は、その処理の従来の読み取りおよび書き込みにフォールバックされます。

ODX を使用するための要件

Storage Virtual Machine (SVM) で ODX によるコピーオフロードを使用する前に、一定の要件について確認しておく必要があります。

ONTAP のバージョンの要件

ONTAP の各リリースで ODX によるコピーオフロードがサポートされます。

SMB のバージョンの要件

- ONTAP では、SMB 3.0 以降で ODX がサポートされます。
- ODX を有効にする前に、CIFS サーバで SMB 3.0 を有効にしておく必要があります。
 - ODX を有効にすると、SMB 3.0 も有効になります（まだ有効になっていない場合）。
 - SMB 3.0 を無効にすると ODX も無効になります。

Windows サーバとクライアントの要件

ODX によるコピーオフロードを使用するには、Windows クライアントでこの機能がサポートされている必要があります。

。"[NetApp Interoperability Matrix を参照してください](#)"サポートされているWindowsクライアントに関する最新情報が含まれています。

ボリューム要件：

- ソースボリュームは 1.25GB 以上でなければなりません。
- 圧縮されたボリュームを使用する場合は、圧縮形式をアダプティブにする必要があります。サポートされる圧縮グループサイズは 8K のみです。

二次圧縮形式はサポートされません

ODX の使用に関するガイドライン

コピーオフロードに ODX を使用する場合は、一定のガイドラインについて理解しておく必要があります。たとえば、ODX を使用できるボリュームのタイプや、クラスタ内およびクラスタ間の ODX に関する考慮事項を把握しておく必要があります。

ボリュームガイドライン

- 次のようなボリューム設定では、コピーオフロードに ODX を使用できません。

- ソースボリュームサイズが 1.25GB 未満である必要があります

ODX を使用するには、ボリュームサイズが 1.25GB 以上である必要があります。

- 読み取り専用ボリューム

負荷共有ミラー、SnapMirror デスティネーションボリューム、または SnapVault デスティネーションボリュームに存在するファイルやフォルダには ODX を使用できません。

- ソースボリュームが重複排除されていない場合

- ODX コピーはクラスタ内のコピーにのみ対応しています。

ODX を使用して、ファイルまたはフォルダを別のクラスタ内のボリュームにコピーすることはできません。

その他のガイドライン

- SMB 環境では、コピーオフロードに ODX を使用するには、256KB 以上のファイルである必要があります。

サイズの小さいファイルは、従来のコピー処理を使用して転送されます。

- ODX コピーオフロードでは、コピープロセスの一環として重複排除が実行されます。

データのコピーまたは移動時に SVM のボリュームで重複排除が発生しないようにする場合は、その SVM で ODX コピーオフロードを無効にする必要があります。

- データ転送を実行するアプリケーションは、ODX をサポートするように記述する必要があります。

ODX がサポートされるアプリケーション処理は次のとおりです。

- Virtual Hard Disk (VHD ; 仮想ハードディスク) の作成および変換、Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、Hyper-V の管理処理
- エクスプローラでの操作
- Windows PowerShell の copy コマンド
- Windows コマンドプロンプトの copy コマンド

Windows コマンドプロンプトの Robocopy は ODX をサポートしています。



ODX をサポートする Windows サーバまたはクライアント上でアプリケーションを実行する必要があります。

+ Windows サーバおよびクライアントでサポートされる ODX アプリケーションの詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

"Microsoft TechNet ライブラリ : technet.microsoft.com/en-us/library/"

ODX のユースケース

SVM で ODX を使用する前に、どのような場合にパフォーマンスを向上できるかを判断できるようにユースケースについて確認しておく必要があります。

ODX をサポートする Windows サーバおよびクライアントでは、リモートサーバ間でデータをコピーする際に、デフォルトでコピーオフロードが使用されます。Windows サーバまたはクライアントで ODX がサポートされていない場合や、ODX コピーオフロードが任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内

ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- ボリュームとノードが異なり、SVM は同じです

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは同じ SVM に所有されます。

- SVM が異なり、ノードは同じです

ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- クラスタ間

ソース LUN とデスティネーション LUN は、異なるクラスタの異なるノード上の異なるボリュームにあります。これは SAN でのみサポートされ、CIFS では機能しません。

その他にも、いくつかの特殊なユースケースがあります。

- ONTAP の ODX の実装で ODX を使用すると、SMB 共有と FC / iSCSI で接続された仮想ドライブとの間でファイルをコピーできます。


SMB 共有と LUN が同じクラスタにある場合は、Windows エクスプローラ、Windows CLI または PowerShell、Hyper-V、または ODX をサポートするその他のアプリケーションを使用して、SMB 共有と接続された LUN 間の ODX コピーオフロードを使用してファイルをシームレスにコピーまたは移動できます。

- Hyper-V では、さらに次のようなユースケースでも ODX コピーオフロードが使用されます。

- Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（VHD）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。

これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定 VHD を作成する際に、ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。



Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、ODX をサポートするストレージ（SMB または SAN）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、ODX のパススルーはサポートされません。

ODXの有効化または無効化

Storage Virtual Machine（SVM）で ODX 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、SMB 3.0 が有効になっている場合は ODX コピーオフロードのサポートも有効になります。

作業を開始する前に

SMB 3.0 が有効になっている必要があります。

このタスクについて

SMB 3.0 を無効にすると、ONTAP でも SMB ODX が無効になります。SMB 3.0 を再度有効にする場合は、SMB ODX を手動で再度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。

ODX コピーオフロードの設定	入力するコマンド
有効	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
無効	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

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

例

次の例は、SVM vs1 で ODX コピーオフロードを有効にします。

```
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 -copy-offload
-enabled true

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

関連情報

[使用できる SMB サーバオプション](#)

Auto Location で **SMB 自動ノードリファール**を提供することで、クライアントの応答時間を短縮します

Auto Location の概要を示す **SMB 自動ノードリファール**を提供することで、クライアントの応答時間を改善します

Auto Location は、SMB 自動ノードリファールを使用して Storage Virtual Machine (SVM) での SMB クライアントのパフォーマンスを向上します。自動ノードリファールは、要求しているクライアントを、データが存在するボリュームをホストしているノード SVM 上の LIF に自動的にリダイレクトします。これにより、クライアントの応答時間を改善できます。

SMB クライアントが SVM 上でホストされている SMB 共有に接続するときに、要求されたデータを所有していないノード上の LIF を使用して接続することがあります。クライアントが接続しているノードは、クラスタネットワークを使用して別のノードが所有しているデータにアクセスします。SMB 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

- ONTAP では、Microsoft の DFS リファールを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることを SMB クライアントに通知することで、この機能を実現します。

ノードがリファールを作成するのは、データを含むノード上に SVM の LIF が 1 つあることを特定した場合です。

- 自動ノードリファールでは、IPv4 と IPv6 の LIF の IP アドレスがサポートされます。
- リファールは、クライアントの接続に使用されている共有のルートの場所に基づいて作成されます。
- リファールは SMB ネゴシエーション中に発生します。

リファールは、接続が確立される前に作成されます。ONTAP がターゲットノードに参照先の SMB クライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先 LIF パスを介してデータにアクセスします。これにより、クライアントにはより高速なデータアクセスが提供され、クラスタの余分な通信も回避されます。



共有が複数のジャンクションポイントにまたがっていて、ジャンクションの一部が他のノードに格納されているボリュームを参照する場合、共有内のデータは複数のノードに分散されます。ONTAP は共有のルートに対してローカルなリファールを提供するため、ONTAP では、これらのローカルでないボリュームに含まれるデータを取得する際にクラスタネットワークを使用する必要があります。このタイプのネームスペースアーキテクチャでは、自動ノードリファールによる大幅なパフォーマンス向上は望めない場合があります。

データをホストするノードに使用可能な LIF がない場合、ONTAP は、クライアントが選択した LIF を使用して接続を確立します。ファイルが SMB クライアントによって開かれると、クライアントは参照された同じ接続を介してファイルへのアクセスを継続します。

何らかの理由で CIFS サーバがリファールを作成できない場合でも、SMB サービスが中断されることはありません。自動ノードリファールが有効でない場合と同様に SMB 接続が確立されます。

関連情報

[Microsoft リモートコピーのパフォーマンスの向上](#)

自動ノードリファールの使用に関する要件とガイドライン

SMB 自動ノードリファール（別名 `_autolocation_`）を使用する前に、この機能をサポートする ONTAP のバージョンなど、一定の要件について理解しておく必要があります。サポートされる SMB プロトコルのバージョンやその他の特別なガイドラインについても確認しておく必要があります。

ONTAP のバージョンとライセンスの要件

- ・ クラスタ内のすべてのノードで、自動ノードリファールがサポートされているバージョンの ONTAP が実行されている必要があります。
- ・ オートロケーションを使用する SMB 共有でワイドリンクが有効になっている必要があります。
- ・ CIFS のライセンスが有効になっていて、SVM に SMB サーバが配置されている必要があります。SMB ライセンスは含まれています。"ONTAP One"。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB プロトコルのバージョン

- ・ SVM について ONTAP は、すべてのバージョンの SMB で自動ノードリファールがサポートされます。

SMB クライアントの要件

SMB 自動ノードリファールは、ONTAP でサポートされるすべての Microsoft クライアントでサポートされます。

ONTAP でサポートされる Windows クライアントの最新情報については、Interoperability Matrix を参照してください。

["NetApp Interoperability Matrix Tool で確認できます"](#)

データ LIF の要件

データ LIF を SMB クライアントのリファールとして使用する可能性がある場合は、NFS と CIFS の両方を有効にしたデータ LIF を作成する必要があります。

自動ノードリファールは、ターゲットノードのデータ LIF で NFS プロトコルまたは SMB プロトコルのどちらかが有効になっていない場合は機能しないことがあります。

この要件が満たされない場合でも、データアクセスには影響しません。SMB クライアントは、SVM への接続に使用した元の LIF を使用して共有をマッピングします。

参照された SMB 接続を確立する際の NTLM 認証の要件

CIFS サーバを含むドメインと自動ノードリファールを使用するクライアントを含むドメインで、NTLM 認証が許可されている必要があります。

リファールを作成する際には、SMB サーバから Windows クライアントに参照先の IP アドレスが渡されます。IP アドレスを使用した接続には NTLM 認証が使用されるため、参照された接続に対しては Kerberos 認証は実行されません。

これは、Windows クライアントが Kerberos で使用されるサービスプリンシパル名（の形式）を作成できないためです（service/NetBIOS name および service/FQDN）。これは、クライアントがサービスに Kerberos チケットを要求できないことを意味します。

自動ノードリファールでホームディレクトリ機能を使用する場合のガイドラインを次に示します

ホームディレクトリ共有プロパティを有効にして共有を設定した場合、ホームディレクトリの設定で 1 つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、SVM のボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファールを受け取り、使用できるアクティブなローカルデータ LIF があれば、ホームユーザのホームディレクトリに対してローカルな、参照された LIF を介して接続します。

SMB 1.0 クライアントで自動ノードリファールを有効にして動的ホームディレクトリにアクセスする場合は注意が必要です。SMB 1.0 クライアントでは、認証を行う前、つまり SMB サーバに対してユーザの名前が指定されていない段階で自動ノードリファールが必要になるからです。SMB 1.0 クライアントで SMB ホームディレクトリへのアクセスが正常に機能するのは、次の条件に該当する場合です。

- SMB ホームディレクトリは、「%w」（Windows ユーザ名）または「%u」（マッピングされた UNIX ユーザ名）のような単純な名前を使用するように設定されており、「%d\%w」（ドメイン名\ユーザ名）のようなドメイン名形式の名前では使用されません。
- ホーム・ディレクトリ共有を作成するときに、CIFS ホーム・ディレクトリ共有名は変数（「%w」または「%u」）で設定され、「home」などの静的な名前では設定されません。

SMB 2.x クライアントと SMB 3.0 クライアントの場合は、自動ノードリファールを使用してホームディレクトリにアクセスする際に特別なガイドラインはありません。

参照接続が確立されている CIFS サーバで自動ノードリファールを無効にする場合のガイドラインを次に示します

オプションを有効にしたあとに自動ノードリファールを無効にした場合、参照 LIF に現在接続されているクライアントでは参照接続が維持されます。ONTAP では SMB 自動ノードリファールのメカニズムとして DFS リファールを使用しているため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされている DFS リファールがタイムアウトするまでは参照 LIF に再接続できます。これは、自動ノードリファールがサポートされないバージョンの ONTAP にリポートした場合も同様です。クライアント

は、クライアントのキャッシュから DFS リファールがタイムアウトするまで、引き続きリファールを使用します。

オートロケーションは、SMB 自動ノードリファールを使用してクライアントに SVM のデータボリュームを所有しているノード上の LIF を参照させることで、SMB クライアントのパフォーマンスを向上させます。SMB クライアントが SVM 上でホストされている SMB 共有に接続するときに、要求されたデータを所有しておらず、クラスターインターコネクトネットワークを使用してデータを取得しているノード上の LIF を使用して接続することがあります。SMB 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

ONTAP では、Microsoft の分散ファイルシステム（DFS）リファールを使用して、要求されたファイルやフォルダがネームスペース内の別の場所でホストされていることを SMB クライアントに通知することで、この機能を実現します。ノードがリファールを作成するのは、データを含むノード上に SVM の LIF があることを特定した場合です。リファールは、クライアントの接続に使用されている共有のルートの場所に基づいて作成されます。

リファールは SMB ネゴシエーション中に発生します。リファールは、接続が確立される前に作成されます。ONTAP がターゲットノードに参照先の SMB クライアントを通知したあと、接続が確立され、それ以降、クライアントはその参照先 LIF パスを介してデータにアクセスします。これにより、クライアントにはより高速なデータアクセスが提供され、クラスターの余分な通信も回避されます。

Mac OS クライアントで自動ノードリファールを使用する際のガイドラインを次に示します

Mac OS では Microsoft の Distributed File System（DFS；分散ファイルシステム）がサポートされていますが、Mac OS X クライアントは SMB 自動ノードリファールをサポートしていません。Windows クライアントは、SMB 共有に接続する前に DFS リファール要求を行います。ONTAP は、要求されたデータをホストしているノード上で見つかったデータ LIF へのリファールを提供します。これにより、クライアントの応答時間が短縮されます。Mac OS でも DFS はサポートされますが、Mac OS クライアントの動作は Windows クライアントとまったく同じではありません。

関連情報

[ONTAP で動的ホームディレクトリを有効にする方法](#)

["Network Management の略"](#)

["NetApp Interoperability Matrix Tool で確認できます"](#)

SMB 自動ノードリファールのサポート

SMB 自動ノードリファールを有効にする際に、ONTAP の一部の機能ではリファールがサポートされない点に注意してください。

- SMB 自動ノードリファールは、次の種類のボリュームではサポートされません。
 - 負荷共有ミラーの読み取り専用のメンバー
 - データ保護ミラーのデスティネーションボリューム
- LIF が移動してもノードリファールは移動しません。

クライアントが SMB 2.x または SMB 3.0 接続を介した参照接続を使用している場合、データ LIF が無停止で移動してもクライアントは引き続き同じ参照接続を使用します。LIF がデータに対してローカルでなくなった場合も同様です。

- ・ ボリュームが移動してもノードリファールは移動しません。

クライアントがいずれかの SMB 接続による参照接続を使用している場合、ボリュームが移動してもクライアントは引き続き同じ参照接続を使用します。ボリュームがデータ LIF と異なるノードに移動した場合も同様です。

SMB 自動ノードリファールを有効または無効にします

SMB 自動ノードリファールを有効にして、SMB クライアントアクセスのパフォーマンスを向上させることができます。ONTAP で SMB クライアントを参照しないようにするには、自動ノードリファールを無効にします。

作業を開始する前に

Storage Virtual Machine (SVM) で CIFS サーバが設定されて実行されている必要があります。

このタスクについて

SMB 自動ノードリファール機能は、デフォルトでは無効になっています。必要に応じて、各 SVM で有効または無効にすることができます。

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. SMB 自動ノードリファールを必要に応じて有効または無効にします。

SMB 自動ノードリファールの設定	入力するコマンド
有効	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</pre>
無効	<pre>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</pre>

このオプション設定は、新しい SMB セッションで有効になります。既存の接続を使用しているクライアントは、その既存のキャッシュがタイムアウトになった場合にのみノードリファールを利用できます

3. admin権限レベルに切り替えます。set -privilege admin

関連情報

[使用できる SMB サーバオプション](#)

統計を使用して、自動ノードリファールのアクティビティを監視します

参照されるSMB接続の数を確認するには、を使用して自動ノードリファールのアクティビティを監視します statistics コマンドを実行しますリファールを監視することで、自動リファールによって共有をホストするノードに対して接続が割り当てられて

いる範囲を把握し、データ LIF を再配分して CIFS サーバの共有へのローカルアクセスを向上させるべきかどうかを判断することができます。

このタスクについて

。cifs オブジェクトには、SMB自動ノードリファールルの監視に役立つadvanced権限レベルのカウンタがいくつか用意されています。

- `node_referral_issued`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントのうち、共有のルート
のノードへのリファールルが発行されたクライアントの数。

- `node_referral_local`

共有のルートと同じノードでホストされる LIF を使用して接続したクライアントの数。一般に、ローカル
アクセスを使用するとパフォーマンスが最適化され

- `node_referral_not_possible`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントのうち、共有のルート
をホストするノードへのリファールルが発行されていないクライアントの数。これは、共有のルートのノ
ードに対するアクティブなデータ LIF が見つからないためです。

- `node_referral_remote`

共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントの数。リモートアクセ
スを使用するとパフォーマンスが低下する可能性があります。

一定期間内のデータ（サンプル）を収集して表示することにより、Storage Virtual Machine（SVM）の自動
ノードリファールル統計を監視できます。データ収集を停止しなければ、サンプルからデータを表示できま
す。データ収集を停止すると、サンプルが固定された状態になります。データ収集を停止しないと、以前のク
エリとの比較に使用できる更新されたデータを取得できます。この比較は、パフォーマンスの傾向を確認する
のに役立ちます。



から収集した情報を評価および使用するため `statistics` コマンドを使用する場合は、環境内
でのクライアントの分散状況について理解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. を使用して、自動ノードリファールルの統計を表示します `statistics` コマンドを実行します

次に、一定のサンプリング時間におけるデータを収集して表示することにより、自動ノードリファール
ルの統計を表示する例を示します。

- a. 収集を開始します。 `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```


- b. 目的の収集時間が経過するまで待ちます。
- c. 収集を停止します。 `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. 自動ノードリファーラルの統計を表示します。 `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

Counter                                     Value
-----
node_name                                   node1
node_referral_issued                       0
node_referral_local                        1
node_referral_not_possible                 2
node_referral_remote                       2
...

node_name                                   node2
node_referral_issued                       2
node_referral_local                        1
node_referral_not_possible                 0
node_referral_remote                       2
...
```

出力には、SVM vs1 に含まれるすべてのノードのカウンタが表示されます。この例では、わかりやすいように、自動ノードリファーラルの統計に関連する出力フィールドだけを示しています。

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

関連情報

[統計情報を表示します](#)

["パフォーマンス監視のセットアップ"](#)

Windows クライアントを使用して、クライアント側の **SMB** 自動ノードリファーラル情報を監視します

クライアント側から発行されているリファーラルを確認するには、Windowsを使用します `dfsutil.exe` ユーティリティ。

Windows 7以降のクライアントで使用できるRemote Server Administration Tools (RSAT) キットには、が含まれています `dfsutil.exe` ユーティリティ。このユーティリティを使用すると、リファールキャッシュの内容に関する情報を表示できるほか、クライアントで現在使用されている各リファールに関する情報を表示できます。また、このユーティリティを使用して、クライアントのリファールキャッシュをクリアすることもできます。詳細については、Microsoft TechNet ライブラリを参照してください。

関連情報

"Microsoft TechNet ライブラリ: technet.microsoft.com/en-us/library/"

アクセスベースの列挙を使用して共有のフォルダのセキュリティを確保します

アクセスベースの列挙の概要を使用して、共有のフォルダのセキュリティを提供します

Access-Based Enumeration が SMB 共有で有効になっていると、共有内のフォルダまたはファイルに（個人またはグループの権限制限により）アクセスする権限がないユーザーの環境には、その共有リソースは表示されませんが、共有自体は表示されたままです。

従来の共有プロパティでは、共有内のファイルやフォルダの表示や変更権限を持つユーザー（個人またはグループ）を指定できます。ただし、権限のないユーザーに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABE では、共有プロパティが強化され、共有内のファイルやフォルダの列挙表示も対象になりました。このため、ABE を使用して、ユーザーのアクセス権に基づいて共有内のファイルとフォルダの表示をフィルタリングすることができます。つまり、共有自体はすべてのユーザーに表示されますが、共有内のファイルやフォルダは、指定したユーザーに対して表示したり非表示にしたりすることができます。職場の機密情報を保護するだけでなく、ABE を使用すると大きなディレクトリ構造の表示を簡略化できるため、あらゆるコンテンツにアクセスする必要がないユーザーにメリットがあります。たとえば、共有自体はすべてのユーザーに表示されますが、共有内のファイルやフォルダは表示または非表示にすることができます。

詳細はこちら "[SMB / CIFSアクセスベースの列挙を使用する際のパフォーマンスへの影響](#)"。

SMB 共有でのアクセスベースの列挙を有効または無効にします

SMB 共有で Access-Based Enumeration を有効または無効にすると、ユーザーがアクセス権のない共有リソースを表示することを許可または禁止できます。

このタスクについて

デフォルトでは、ABEは無効になっています。

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
新しい共有で ABE を有効にします	<pre>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access- based-enumeration</pre> <p>SMB共有の作成時に、追加のオプションの共有設定および追加の共有プロパティを指定できます。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 <code>vserver cifs share create</code> コマンドを実行します</p>
既存の共有で ABE を有効にします	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>既存の共有プロパティは維持されます。ABE 共有プロパティは既存の共有プロパティリストに追加されます。</p>
既存の共有で ABE を無効にします	<pre>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access- based-enumeration</pre> <p>その他の共有プロパティは維持されます。ABE 共有プロパティのみが共有プロパティリストから削除されます。</p>

2. を使用して、共有設定が正しいことを確認します `vserver cifs share show` コマンドを実行します

例

次の例は、「sales」という名前のABE SMB共有をパスに作成します `/sales SVM vs1`上。共有はを使用して作成されます `access-based-enumeration` 共有プロパティとして：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

          Vserver: vs1
          Share: sales
CIFS Server NetBIOS Name: VS1
          Path: /sales
    Share Properties: access-based-enumeration
                     oplocks
                     browsable
                     changenotify
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard
```

次の例は、を追加します access-based-enumeration 「data2」という名前のSMB共有への共有プロパティ:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

関連情報

[既存の SMB 共有に対する共有プロパティの追加または削除](#)

Windows クライアントからのアクセスベースの列挙を有効または無効にします

SMB 共有での Access-Based Enumeration の有効化と無効化は Windows クライアントから実行できるため、この共有設定は CIFS サーバに接続することなく編集できます。



。 abecmd ユーティリティは、Windows ServerおよびWindowsクライアントの新しいバージョンでは使用できません。Windows Server 2008の一部としてリリースされました。Windows Server 2008のサポートは2020年1月14日をもって終了しました。

手順

1. ABEをサポートするWindowsクライアントで、次のコマンドを入力します。 `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

詳細については、を参照してください abecmd コマンドについては、Windowsクライアントのマニュアルを参照してください。

NFS と SMB のファイルとディレクトリの命名規則

NFS と SMB のファイルとディレクトリの命名規則について概要を示します

ファイルとディレクトリの命名規則は、ONTAP クラスタおよびクライアントの言語設定に加え、ネットワーククライアントのオペレーティングシステムとファイル共有プロトコルによって異なります。

オペレーティングシステムとファイル共有のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、ONTAP のリリースに応じて、ファイル、ディレクトリ、qtree の名前でマルチバイト文字がサポートされます。

ファイル名またはディレクトリ名に使用できる文字

異なるオペレーティングシステムのクライアントからファイルやディレクトリにアクセスする場合は、どちらのオペレーティングシステムでも有効な文字を使用します。

たとえば、UNIX を使用してファイルやディレクトリを作成する場合は、ファイル名やディレクトリ名にコロン (:) を使用しないでください。コロンは、MS-DOS ファイル名やディレクトリ名では使用できないためです。有効な文字の制限はオペレーティングシステムごとに異なります。使用できない文字の詳細については、クライアントのオペレーティングシステムのマニュアルを参照してください。

マルチプロトコル環境でのファイル名とディレクトリ名の大文字と小文字の区別

ファイル名とディレクトリ名では、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されません。この違いがマルチプロトコル環境に及ぼす影響と、SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにはどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `testdir`SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます `testdir`。ただし、SMBユーザがあとでディレクトリ名を

作成しようとした場合 `TESTDIR` を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のディレクトリを作成する場合 `TESTDIR` では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および `TESTDIR` ディレクトリ名では大文字と小文字が区別されるためです。
- SMB クライアントでは、2つのディレクトリを区別するために 8.3 形式の名前が使用されます。1つのディレクトリにはベースファイル名が付けられます。追加のディレクトリには 8.3 形式のファイル名が割り当てられます。
 - SMBクライアントでは、が表示されます `testdir` および `TESTDI~1`。
 - ONTAP によってが作成されます `TESTDI~1` 2つのディレクトリを区別するディレクトリ名。

この場合、Storage Virtual Machine（SVM）での共有の作成時または変更時に共有パスを指定するときは、8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `test.txt` `SMBクライアントとNFSクライアントのどちらでも、ファイル名はと表示されます` `test.txt`。ただし、SMBユーザがあとでを作成しようとした場合 `Test.txt` を指定することはできません。SMBクライアントでは、その名前がすでに存在しているとみなされます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt` では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、 `test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMB クライアントでは、2つのファイルを区別するために 8.3 形式の名前が使用されます。1つのファイルにはベースファイル名が付けられます。追加のファイルには 8.3 形式のファイル名が割り当てられます。
 - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
 - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。



SVM `cifs character-mapping` コマンドを使用して文字マッピングを有効または変更した場合、通常、大文字と小文字は区別されない Windows ルックアップは大文字と小文字が区別されません。

ONTAP によるファイル名とディレクトリ名の作成方法

ONTAP は、SMB クライアントからアクセスされるすべてのディレクトリ内にあるファイルまたはディレクトリに対して 2つの名前が作成され、保持されます。元の長い名前と 8.3 形式の名前です。

名前が 8 文字を超える、または拡張子が 3 文字を超える（ファイルの場合）ファイル名やディレクトリ名について、ONTAP は次のように 8.3 形式の名前を生成します。

- 名前が 6 文字を超える場合は、元のファイル名またはディレクトリ名が 6 文字に切り捨てられます。
- 切り捨て後に一意でなくなったファイル名またはディレクトリ名には、チルダ（~）と 1~5 の数字が追加されます。

同様の名前が 6 つ以上存在するため数字が足りなくなった場合には、元の名前とは無関係な一意の名前が作成されます。

- ファイルの場合は、ファイル名の拡張子が 3 文字に切り捨てられます。

たとえば、NFSクライアントがという名前のファイルを作成するとします `specifications.html`ONTAP` で作成される 8.3 形式のファイル名はです ``specif~1.htm`。この名前がすでに存在する場合、ONTAP はファイル名の最後に別の番号を使用します。たとえば、NFSクライアントがという名前の別のファイルを作成したとします `specifications_new.html`、8.3 形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、ディレクトリ名、**qtree** 名の ONTAP での処理

ONTAP 9.5 以降では、4 バイトの UTF-8 エンコード形式の名前がサポートされるようになり、Basic Multilingual Plane（BMP；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4 バイトの UTF-8 エンコード名のサポートを有効にするには、`new_utf8mb4_` 言語コードを使用できます `vserver` および `volume` コマンド・ファミリー。

次のいずれかの方法で新しいボリュームを作成する必要があります。

- ボリュームを設定しています `-language` 明示的なオプション：`volume create -language utf8mb4 {...}`
- ボリュームを継承しています `-language` オプションを指定して作成または変更した SVM から、次のオプションを選択します。`vserver [create|modify] -language utf8mb4 {...}``volume create {...}`
- ONTAP 9.6 以前では、`utf8mb4` をサポートするために既存のボリュームを変更することはできません。`utf8mb4` 対応の新しいボリュームを作成し、クライアントベースのコピーツールを使用してデータを移行する必要があります。

SVM は `utf8mb4` をサポートするように更新できますが、既存のボリュームの言語コードは元の設定のままです。

ONTAP 9.7P1 以降を使用している場合は、`utf8mb4` の既存ボリュームをサポートリクエストで変更できます。詳細については、を参照してください ["ONTAP での作成後にボリュームの言語を変更できますか。"](#)。

- ONTAP 9.8 以降では、`[-language <Language code>]` ボリュームの言語を*。`utf-8` から `utf8mb4` に変更するためのパラメータ。ボリュームの言語を変更するには、["ネットアップサポート"](#)。



現在のところ、4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、Unicode 文字データは、Windows ファイルシステムアプリケーションでは 16-bit Unicode Transformation Format（UTF-16）、NFS ファイルシステムでは 8-bit Unicode Transformation Format（UTF-8）を使用して表現されます。

ONTAP 9.5 よりも前のリリースでは、Windows クライアントで作成された UTF-16 の補助文字を含む名前は、他の Windows クライアントには正しく表示されましたが、NFS クライアントでは UTF-8 に正しく変換されませんでした。同様に、NFS クライアントで作成された UTF-8 の補助文字を含む名前は、Windows クライアントで UTF-16 に正しく変換されませんでした。

- ONTAP 9.4 以前を実行しているシステムで作成したファイル名に有効な追加文字が含まれている場合や無効な追加文字が含まれている場合、ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は使用しないようにするか、ONTAP 9.5 以降にアップグレードしてください。

ONTAP 9 以降では、Unicode 文字を qtree 名に使用できます。

- どちらかを使用できます volume qtree qtree名を設定または変更するには、コマンドファミリーまたは System Manager を使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。



ONTAP 9.5 よりも前のリリースでは、qtree の親ボリュームのジャンクションパスに、Unicode 文字を使用した qtree 名やディレクトリ名を含めることができます。 volume show 親ボリュームの言語設定が UTF-8 の場合は、コマンドでこれらの名前が正しく表示されます。ただし、親ボリュームの言語設定が UTF-8 のいずれかでない場合は、ジャンクションパスの一部が数値の NFS 名に置き換えられて表示されます。

- 9.5 以降のリリースでは、qtree が utf8mb4 に対応したボリュームに含まれていれば、qtree 名で 4 バイト文字がサポートされます。

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

NFS クライアントは、SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

SMB クライアントが NFS クライアントによって作成されたファイルにアクセスすると、ONTAP はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロンが含まれている場合）、ONTAP は各ファイルに対して保持されている 8.3 形式のファイル名を返します。ただし、これにより、長いファイル名に重要な情報をエンコードするアプリケーションで問題が発生します。

したがって、異なるオペレーティングシステムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に注意する必要があります。

- 文字マッピングは、ジャンクションポイントをまたいで適用されません。

文字マッピングは、各ジャンクションボリュームに対して明示的に設定する必要があります。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

たとえば ' コロン (:) をハイフン (-) にマップしようとした場合 ' ファイル名にハイフン (-) が正しく使用されていれば 'Windows クライアントが "a-b" という名前のファイルにアクセスしようすると ' その要求は NFS 名 "a:b" にマップされます (望ましい結果ではありません)

- 文字マッピングを適用してもまだマッピングに無効な Windows 文字が含まれている場合、ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。つまり、マッピングされた共有にアクセスするアプリケーションは、Windows の大文字と小文字を区別しない動作に依存しません。ただし、8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙 (「dir」) を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ無効な文字が含まれている場合、または Windows で無効な文字が含まれている場合 (「.」または空白で終わる場合など) は、無効な名前の代わりに 8.3 形式の名前が返されます。

ステップ

1. 文字マッピング「+」を設定します

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name
-mapping mapping_text, ... [ + ]
```

マッピングは、「:」で区切られたソース文字とターゲット文字のペアのリストで構成されます。文字は、16 進数値で入力された Unicode 文字です。例：3C : E03C[+]

それぞれの最初の値 mapping_text コロンで区切られたペアは、変換する NFS 文字の 16 進値です。2 番目の値は、SMB で使用される Unicode 値です。マッピングのペアは一意である必要があります (1 対 1 のマッピングが存在する必要があります)。

- ソースマッピング

次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

[+]

Unicode 文字	印刷された文字	説明
0x01-0x19	該当なし	印刷されない制御文字

Unicode 文字	印刷された文字	説明
0x5C		バックスラッシュ
0x3a	:	コロン
0x2A	*	アスタリスク
0x3f	?	疑問符
0x22	"	引用符
0x3C	<	より小さい
0x3E	>	が次の値より大きい
0x7C		
縦線	0xb1	±

- ターゲットマッピング

ターゲット文字には、U+E0000...U+F8FF の範囲の Unicode の「私用領域」を指定できます。

例

次のコマンドは、Storage Virtual Machine （SVM） vs1 上の「data」という名前のボリュームに文字マッピングを作成します。

```
cluster1::> vsserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vsserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

関連情報

[NAS ネームスペース内でのデータボリュームの作成と管理](#)

SMB ファイル名の変換のための文字マッピングを管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	<code>vserver cifs character-mapping create</code>
ファイル文字マッピングに関する情報を表示する	<code>vserver cifs character-mapping show</code>
既存のファイル文字マッピングを変更します	<code>vserver cifs character-mapping modify</code>
ファイル文字マッピングを削除します	<code>vserver cifs character-mapping delete</code>

詳細については、各コマンドのマニュアルページを参照してください。

関連情報

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

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。