オプションを使用したSMBサーバのカスタマイズ

ONTAP 9

NetApp
February 12, 2026

目次

オプションを使用したSMBサーバのカスタマイズ

利用可能な ONTAP SMB サーバ オプション

SMBサーバーのカスタマイズ方法を検討する際には、利用可能なオプションを知っておくと便利です。一部のオプションはSMBサーバーで一般的に使用されますが、いくつかのオプションは特定のSMB機能を有効化および設定するために使用されます。SMBサーバーのオプションは、 `vserver cifs options modify`オプションで制御されます。

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** セッションのタイムアウト値の設定

  このオプションでは、SMBセッションがアイドルになってから切断されるまでの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**ユーザーの設定

  このオプションを設定すると、SMBサーバが使用するデフォルトのUNIXユーザを指定できます。ONTAPは、「`pcuser`」（UID 65534）というデフォルトユーザと、「`pcuser`」（GID 65534）というグループを自動的に作成し、その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「`pcuser`」をデフォルトのUNIXユーザとして自動的に設定します。

- ゲスト **UNIX** ユーザーの設定

  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 ビットの読み取り許可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無効になっています。

- **NFS**クライアントから読み取り専用ファイルを削除する機能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することで、NFSクライアントが読み取り専用属性が設定されているファイルまたはフォルダを削除できるかどうかを決定します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されているファイルまたはフォルダの削除は許可されません。UNIXの削除セマンティクスでは、読み取り専用ビットは無視され、代わりに親ディレクトリの権限を使用してファイルまたはフォルダの削除可否が判断されます。デフォルト設定は `disabled`で、NTFSの削除セマンティクスが適用されます。

- **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**ユーザーに**UNIX**グループ権限を付与する

  このオプションを設定すると、ファイルの所有者ではない受信 CIFS ユーザーにグループ権限を付与できるかどうかが決定されます。CIFS ユーザーが UNIX セキュリティ スタイルのファイルの所有者ではなく、このパラメータが `true`に設定されている場合、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 スタイルのファイルの所有者ではなく、このパラメータが `false`に設定されている場合、ファイル権限を付与するために通常の UNIX ルールが適用されます。このパラメータは、権限が `mode bits`に設定されている UNIX セキュリティ スタイルのファイルに適用され、NTFS または NFSv4 セキュリティ モードのファイルには適用されません。デフォルト設定は `false`です。

- **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、NetApp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、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** の有効化または無効化

  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 copy offload**の有効化または無効化

  ODX コピー オフロードは、それをサポートする Windows クライアントによって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 copy offload**のダイレクト 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 リファーラルの有効化または無効化

  自動ノード リファーラルでは、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無効になっています。

- ジャンクション ポイントを再解析ポイントとして使用することを有効化または無効化

  このオプションを有効にすると、SMBサーバーはジャンクションポイントを再解析ポイントとしてSMBクライアントに公開します。このオプションはSMB 2.xまたはSMB 3.0接続でのみ有効です。このオプションはデフォルトで有効です。

  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** 接続あたり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 **Windows** ユーザーとグループの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 shadow copy**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ソリューション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。

- **shadow copy** ディレクトリの深さの設定

  このオプションを設定すると、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。

- 名前マッピングのマルチドメイン検索機能の有効化または無効化

  有効にすると、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**UNIX**ユーザが**Windows**ドメインユーザにマッピングされた場合（例：\joe）、ONTAPはホームドメインとの双方向の信頼関係を持つすべてのドメインで指定され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、信頼できるドメインのリストを設定すると、マルチドメイン ネーム マッピングの検索はそのリストを使用して実行されます。

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 システムのセクター サイズの設定

  このオプションを設定すると、ONTAPがSMBクライアントに報告するファイルシステムのセクターサイズ（バイト単位）を設定できます。このオプションには、 `4096`と `512`の2つの有効な値があります。デフォルト値は `4096`です。Windowsアプリケーションが512バイトのセクターサイズしかサポートしていない場合は、この値を `512`に設定する必要があるかもしれません。

- **Dynamic Access Control** 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（匿名を制限）

  このオプションでは、認証されていないセッションに適用される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** 有効セキュリティのボリューム（**UNIX** セキュリティ形式のボリュームまたは **UNIX** 有効セキュリティの混合セキュリティ形式のボリューム）での **NTFS ACL** の表示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、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** フェイク 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** 拡張機能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 OS X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。

- 短縮名検索のサポートを有効または無効にする

  このオプションを有効にすると、SMBサーバーは短いファイル名で検索を実行できるようになります。このオプションを有効にした検索クエリは、長いファイル名だけでなく、8.3形式のファイル名も照合します。このパラメータのデフォルト値は `false`です。

- **DFS** 機能の自動アドバタイズのサポート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、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リファーラルが使用されます。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、 `-max-credits`オプションを設定することで、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接続で付与され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

  ONTAP 9.4以降のリリースで `-is-multichannel-enabled`オプションを有効にすると、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、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`です。

  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。
  - マルチチャネル セッションごとにアドバタイズ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。

ONTAP SMBサーバ オプションを設定する

SMBサーバ オプションは、Storage Virtual Machine（SVM）でのSMBサーバの作成後に随時設定できます。

手順

1. 次のうち必要な操作を実行します。

SMB サーバ オプションを設定する場合...	コマンドを入力してください...
admin権限レベルで設定	`vserver cifs options modify -vserver` *`vserver_name options`*

SMB サーバ オプションを設定する場合...	コマンドを入力してください...
advanced権限レベルで設定	a. `set -privilege advanced` b. `vserver cifs options modify -vserver vserver_name options` c. `set -privilege admin`

`vserver cifs options modify`および SMB サーバー オプションの設定の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-cifs-options-modify.html["ONTAPコマンド リファレンス "^]を参照してください。

ONTAP SMBユーザーにUNIXグループ権限を付与する設定

このオプションを使用して、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できるグループ権限を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目的に応じて設定します。

次の操作を行う場合：	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	`vserver cifs options modify –grant-unix-group-perms-to-others true`
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	`vserver cifs options modify –grant-unix-group-perms-to-others 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 –fields grant-unix-group-perms-to-others`
4. admin権限レベルに戻ります： `set -privilege admin`

匿名ユーザーに対する ONTAP SMB アクセス制限を構成する

デフォルトでは、認証されていない匿名ユーザー（_nullユーザー_とも呼ばれます）はネットワーク上の特定の情報にアクセスできます。SMBサーバーオプションを使用して、匿名ユーザーへのアクセス制限を設定できます。

タスク概要

`-restrict-anonymous`SMB サーバー オプションは、Windows の `RestrictAnonymous`レジストリ エントリに対応します。

匿名ユーザは、ネットワークのWindowsホストから、ユーザ名、ユーザの詳細、アカウント ポリシー、共有名など、特定の種類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。

Value	概要
no-restriction（デフォルト）	匿名ユーザに対して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. 匿名制限設定を構成します： `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

利用可能なサーバー 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の管理

UNIXセキュリティ形式のデータに対して、**SMB**クライアントに**ONTAP**ファイルセキュリティを提供する方法について説明します。

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。それぞれの設定の利点を理解して、ビジネス要件に適した方を選ぶようにしてください。

デフォルトでは、UNIXセキュリティ形式のボリュームに対するUNIXアクセス権がNTFS ACLとしてSMBクライアントに提供されます。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 権限を表示および編集します。

処理がUNIXシステムで許可されていなければ、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システムではこうした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。

- UNIXセキュリティ形式のボリュームに格納されたファイルの編集や保存に特定のWindowsアプリケーション（Microsoft Officeなど）を使用しており、ONTAPでの保存時にUNIXアクセス権を維持する必要がある場合。
- 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。

状況に応じて、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、UNIXセキュリティ形式のボリュームがFATボリュームとしてSMBクライアントに提供されます。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は、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クライアントでしか行わない場合。

  UNIXセキュリティ形式のボリュームがSMBクライアントでマッピングされている場合、[セキュリティ]タブで操作することはできません。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ではボリュームがFATとして報告され、アプリケーションでACLの変更は試行されません。

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用にONTAP SMBクライアントへのNTFS ACLのプレゼンテーションを設定する

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およびUNIX有効セキュリティを使用する混在セキュリティ形式のボリューム）に対して、SMBクライアントへのNTFS ACLの表示を有効または無効にできます。

タスク概要

このオプションを有効にすると、ONTAPは、有効なUNIXセキュリティ形式のボリューム上のファイルとフォルダを、NTFS ACLを持つものとしてSMBクライアントに提示します。このオプションを無効にすると、ボリュームはSMBクライアントに対してFATボリュームとして提示されます。デフォルトでは、SMBクライアントに対してNTFS ACLが提示されます。

手順

1. 権限レベルをadvancedに設定します： `set -privilege advanced`
2. UNIX NTFS ACLオプション設定を構成します。 `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 SMB FlexVolボリュームのUNIX権限の保持について学習します

現在 UNIX 権限を持つ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ると、ONTAP は UNIX 権限を保持できます。

Windows クライアント上のアプリケーションがファイルを編集して保存する場合、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、一時ファイルに元のファイル名を付けます。

Windowsクライアントがセキュリティプロパティのクエリを実行すると、UNIX権限を正確に表す構築済みACLが返されます。この構築済みACLの唯一の目的は、Windowsアプリケーションによってファイルが更新されてもファイルのUNIX権限を保持し、更新後のファイルに同じUNIX権限が付与されるようにすることです。ONTAPは、構築済みACLを使用してNTFS ACLを設定することはありません。

ONTAP SMBサーバのWindowsセキュリティタブを使用してUNIX権限を管理する方法について学習します。

SVM上の混合セキュリティ形式のボリュームまたはqtree内のファイルまたはフォルダのUNIX権限を操作する場合は、Windowsクライアントの[セキュリティ]タブを使用できます。または、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権限の変更

  Windowsの「セキュリティ」タブを使用して、混合セキュリティ形式のボリュームまたはqtreeのUNIX権限を表示および変更できます。Windowsのメインの「セキュリティ」タブを使用してUNIX権限を変更する場合は、変更を加える前に、編集する既存のACEを削除する必要があります（これにより、モードビットが0に設定されます）。または、詳細エディタを使用して権限を変更することもできます。

  モード権限を使用する場合、リストされているUID、GID、その他（コンピューターにアカウントを持つ他のすべてのユーザー）のモード権限を直接変更できます。例えば、表示されているUIDにr-x権限がある場合、UID権限をrwxに変更できます。

- UNIX 権限から NTFS 権限への変更

  Windows セキュリティ タブを使用すると、ファイルとフォルダに UNIX 対応のセキュリティ スタイルが設定されている、混合セキュリティ スタイル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。

  必要なWindowsユーザおよびグループオブジェクトに置き換える前に、まずリストされているすべてのUNIX権限エントリを削除する必要があります。その後、WindowsユーザおよびグループオブジェクトにNTFSベースのACLを設定できます。すべてのUNIXセキュリティオブジェクトを削除し、混合セキュリティ形式のボリュームまたはqtreeのファイルまたはフォルダにWindowsユーザおよびグループのみを追加することで、ファイルまたはフォルダの有効なセキュリティ形式がUNIXからNTFSに変更されます。

  フォルダの権限を変更すると、Windowsのデフォルトの動作では、これらの変更がすべてのサブフォルダ

とファイルに反映されます。したがって、セキュリティスタイル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させたくない場合は、反映方法を適切な設定に変更する必要があります。

著作権に関する情報

商標に関する情報