オプションを使用した**SMB**サーバのカスタマイズ

ONTAP 9

NetApp
April 24, 2024

目次

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。デフォルト設定はです `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です `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です `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	`vserver cifs options modify -vserver` *`vserver_name options`*

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. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

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	`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ようにします	`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ィプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用してから、一時ファイルに元のファイル名を付けます。

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

Windows のセキュリティタブを使用して **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。