ONTAPでのローカル ユーザとローカル グループの使用方法

ONTAP 9

NetApp
February 12, 2026

目次

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ONTAP SMBユーザとグループについて学ぶ

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、その定義およびいくつかの基本的な情報を理解しておく必要があります。

- ローカル ユーザ

  一意のセキュリティ識別子（SID）が割り当てられたユーザ アカウント。アカウントが作成されたStorage Virtual Machine（SVM）上でのみ認識されます。ローカル ユーザ アカウントには、ユーザ名やSIDなどの一連の属性があります。ローカル ユーザ アカウントは、NTLM認証を使用してCIFSサーバ上でローカルに認証されます。

  ユーザ アカウントには次の用途があります。

  - ユーザに *User Rights Management* 権限を付与するために使用されます。
  - SVM が所有するファイルおよびフォルダ リソースへの共有レベルおよびファイルレベル アクセスを制御するために使用されます。

- ローカル グループ

  一意のSIDが割り当てられたグループ。グループが作成されたSVM上でのみ認識されます。グループに複数のメンバーが含まれます。メンバーとして指定できるのは、ローカル ユーザ、ドメイン ユーザ、ドメイン グループ、ドメイン マシンの各アカウントです。グループは作成、変更、削除できます。

  グループには次の用途があります。

  - メンバーに *User Rights Management* 権限を付与するために使用されます。
  - SVM が所有するファイルおよびフォルダ リソースへの共有レベルおよびファイルレベル アクセスを制御するために使用されます。

- ローカル ドメイン

  ローカル スコープが割り当てられたドメイン。スコープはSVMによって制限されます。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。

- セキュリティ識別子（**SID**）

  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。例えば、一般的なSIDは次の形式になります：S-1-5-21-3139654847-1303905135-2517279418-123456。

- **NTLM**認証

  CIFSサーバでユーザの認証に使用される、Microsoft Windowsのセキュリティ方式。

- クラスター複製データベース（**RDB**）

クラスタ内の各ノードにインスタンスがある、レプリケートされたデータベース。ローカル ユーザとローカル グループのオブジェクトはRDBに格納されます。

ローカルONTAP SMBユーザーと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。

  ワークグループにローカル ユーザを設定する必要があります。

- 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 ユーザーに *User Rights Management* 権限を割り当てる必要があります。

  User Rights Management は、SMBサーバ管理者がSVM上のユーザとグループの権限を制御する機能です。ユーザに権限を割り当てるには、ユーザのアカウントに権限を割り当てるか、その権限を持つ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管理に役立ちます。

- 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。
- カスタマイズされた_User Rights Management_権限を持つローカルグループを作成します。

  組み込みのユーザ グループの一部には権限があらかじめ定義されています。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。そのあとで、作成したローカル 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 ユーザ認証について

- サポートされる権限の一覧

ローカルONTAP SMBユーザ認証について

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る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ります。

- ドメイン部分が一致する

  データへのアクセスを要求するときにローカル ユーザ クレデンシャルを指定したユーザが、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ない

  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。失敗した場合は、認証の失敗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、CIFSサーバ上の対応するローカル ユーザ アカウントの使用は試行されません。代わりに、認証は失敗します。NetBIOSドメイン名が一致しなくてもCIFSサーバ上の対応するローカル アカウント（存在する場合）が認証に使用されるケースはほかにもあります。たとえば、一致するドメイン アカウントが存在するが無効になっている場合は、CIFSサーバ上の対応するローカル アカウントが認証に使用されます。

- ドメイン部分が指定されていない

  まず、ローカル ユーザとしての認証が試行されます。ローカル ユーザとしての認証に失敗した場合は、CIFSサーバが属しているドメインのドメイン コントローラでユーザが認証されます。

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、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

サーバ上のローカルユーザ認証を有効または無効にする

ONTAP SMB ユーザーアクセストークンについて学ぶ

ユーザーが共有をマップすると、認証されたSMBセッションが確立され、ユーザー、ユーザーのグループメンバーシップと累積権限、およびマップされたUNIXユーザーに関す

る情報を含むユーザーアクセストークンが構築されます。

この機能が無効になっていない限り、ローカルユーザーとグループの情報もユーザーアクセストークンに追加されます。アクセストークンの作成方法は、ログインがローカルユーザー用かActive Directoryドメインユーザー用かによって異なります：

- ローカルユーザーログイン

  ローカルユーザーは異なるローカルグループのメンバーになることができますが、ローカルグループは他のローカルグループのメンバーになることはできません。ローカルユーザーアクセストークンは、特定のローカルユーザーが所属するグループに割り当てられたすべての権限の集合で構成されます。

- ドメインユーザーログイン

  ドメインユーザがログインすると、ONTAPはユーザSIDと、そのユーザが所属するすべてのドメイングループのSIDを含むユーザアクセストークンを取得します。ONTAPは、ドメインユーザアクセストークンと、ユーザの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）によって提供されるアクセストークン、およびドメインユーザまたはそのドメイングループメンバーシップに割り当てられた直接権限を結合したものを使用します。

ローカルユーザーとドメインユーザーのログインの両方において、ユーザーアクセストークンにはプライマリグループRIDも設定されます。デフォルトのRIDは `Domain Users`（RID 513）です。このデフォルトを変更することはできません。

Windows から UNIX へ、および UNIX から Windows への名前マッピングプロセスは、ローカルアカウントとドメインアカウントの両方に対して同じ規則に従います。

> UNIXユーザーからローカルアカウントへの暗黙的な自動マッピングは存在しません。これが必要な場合は、既存の名前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 **ONTAP SMB SVM** で **SnapMirror** を使用する方法について学習します

ローカル グループを含む SVM が所有するボリュームで SnapMirror を設定する場合は、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、または共有に適用されるACEでは、ローカル グループは使用できません。SnapMirror機能を使用して別のSVM上のボリュームにDRミラーを作成する場合、そのボリュームにローカル グループのACEが設定されていても、そのACEはミラー上では無効です。データが別のSVMにレプリケートされると、データは実質的に別のローカル ドメインに渡されることになります。ローカル ユーザーとグループに付与された権限は、それらが元々作成されたSVMのスコープ内でのみ有効です。

ONTAP SMBサーバの削除がユーザとグループに与える影響について学習します

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 ユーザとローカル 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、削除した場合のローカル ユーザとローカル グループへの影響について理解しておく必要があります。

ローカル ユーザとローカル グループはSVMに関連付けられているため、セキュリティの観点から、CIFSサーバを削除しても削除されることはありません。ただし、削除はされませんが非表示になります。SVM上にCIFSサーバを再作成するまで、ローカル ユーザとローカル グループを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。

ローカルの**ONTAP SMB**ユーザーとグループで**Microsoft**管理コンソールを使用する方法を学びます

Microsoft Management Consoleからローカルユーザーおよびグループに関する情報を表示できます。このリリースのONTAPでは、Microsoft Management Consoleからローカルユーザーおよびグループの他の管理タスクを実行することはできません。

ONTAP SMB クラスタのリバートについて

ローカル ユーザとグループをサポートしていない ONTAP リリースにクラスタを戻す予定であり、ファイル アクセスまたはユーザ権限の管理にローカル ユーザとグループが使用されている場合は、特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により、ONTAPがローカル ユーザとグループの機能をサポートしていないバージョンに戻された場合でも、設定されたローカル 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 バージョンに戻すと、ONTAPは認証およびクレデンシャルの作成時にローカル ユーザとグループを使用しません。
- ローカル ユーザーとグループは、ファイルとフォルダーの ACL から削除されません。
- ローカル ユーザーまたはグループに付与された権限によって付与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 ユーザおよびグループ 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。

著作権に関する情報

商標に関する情報