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
December 20, 2024

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

ローカルユーザとローカルグループの概念

環境で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とは何か、およびそれらに関するいくつかの基本情報を把握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されます。

  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を持つグループは、そのグループを作成したSVM上でのみ認識されます。グループには一連のメンバーが含まれます。メンバーには、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を指定できます。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で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内に格納されます。

- * Security Identifier （ SID ；セキュリティ識別子） *

  SIDは可変長の数値で、Windows形式のセキュリティプリンシパルを識別します。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サーバでユーザを認証するために使用される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。ローカルユーザオブジェクトとローカルグループオブジェクトは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）を使用できない場合でも、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。また、ローカルグループを使用してPrivilegesを割り当てたり、SMBサーバがワークグループに含まれている場合もあります。

ローカルユーザアカウントを作成する理由は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメインユーザを使用できません。

  ワークグループを設定する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場合に、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は、ローカルユーザは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Privilegesを割り当てるには、ユーザのアカウントにPrivilegesを割り当てるか、ユーザをそのPrivilegesを含む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は次のとおりです。

- SMBサーバがワークグループに含まれており、ドメイングループを使用できません。

  ローカルグループはワークグループ構成では必要ありませんが、ローカルワークグループユーザのアクセスPrivilegesの管理に役立ちます。

- 共有と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、ファイルおよびフォルダ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。

  一部の組み込みユーザグループには、Privilegesが事前に定義されています。カスタマイズしたPrivilegesセットを割り当てるには、ローカルグループを作成し、そのグループに必要なPrivilegesを割り当てます。その後、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そのローカルグループに追加できます。

関連情報

ローカルユーザ認証の仕組み

サポートされるPrivilegesのリスト

ローカルユーザ認証の仕組み

ローカルユーザがCIFSサーバ上のデータにアクセスする前に、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はセッションの最初のセットアップ時に1回だけ確認できます。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は、3つのユースケースでローカル認証を使用します。それぞれのユースケースは、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は、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、次に何が起こるかは、認証が成功しなかった理由によって異なります。

  たとえば、ユーザがActive Directoryに存在するにもかかわらず、パスワードが無効であるか期限切れになっている場合、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。NetBIOSドメイン名が一致しなくても、ONTAPが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）を認証に使用するケースは他にもあります。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、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。

- ドメイン部分が指定されていません

  ONTAPは最初に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、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すると、ONTAPはローカルグループメンバーシップとPrivilegesを考慮した完全なユーザアクセストークンを構築します。

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（RID 513）です `Domain Users`。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への影響

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できます。CIFS

サーバを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に関連付けられます。そのため、セキュリティ上の理由から、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、表示されません。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の表示には影響しません。

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。

リバ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バートするときは、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バートしても、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 からは削除されません。
- 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。

著作権に関する情報

商標に関する情報