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
April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/smb-admin/local-users-groups-concepts-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

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 . . . 1
- ローカルユーザとローカルグループの概念 . . . 1
- 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 . . . 2
- ローカルユーザ認証の仕組み . . . 3
- ユーザアクセストークンの構成方法 . . . 3
- 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 . . . 4
- 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 . . . 4
- 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 . . . 5
- リバートに関するガイドライン . . . 5

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ケースがあります。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

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権を有し、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権については、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。