ネームマッピングの設定
ONTAP 9

NetApp
December 20, 2024

目次

ネームマッピングの設定 1
ネームマッピングの設定の概要 1
ネームマッピングの仕組み 1
UNIXユーザからWindowsユーザへのネームマッピングのためのマルチドメイン検索 2
ネームマッピングの変換ルール 4
ネームマッピングを作成する 4
デフォルトユーザの設定 5
ネームマッピングの管理用コマンド 5

ネームマッピングの設定

ネームマッピングの設定の概要

ONTAPでは、ネームマッピングを使用して、CIFS IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをCIFS IDにマッピングします。この情報は、NFSクライアントとCIFSクライアントのどちらから接続しているかに関係なく、ユーザクレデンシャルを取得して適切なファイルアクセスを提供するために必要になります。

ネームマッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成し、ボリュームでCIFSアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
- 代わりにデフォルトユーザを使用するように設定します。

  このシナリオでは、すべてのクライアントクレデンシャルを個別にマッピングするのではなく、すべてのクライアントクレデンシャルが同じデフォルトユーザにマッピングされるため、ネームマッピングは必要ありません。

ネームマッピングはユーザに対してのみ使用でき、グループに対しては使用できないことに注意してください。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、salesという語で開始または終了するすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。

ネームマッピングの仕組み

ONTAPでユーザのクレデンシャルをマッピングする必要がある場合は、まずローカルのネームマッピングデータベースとLDAPサーバで既存のマッピングの有無を確認します。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVMのネームサービスの設定で決まります。

- WindowsからUNIXへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPは小文字のWindowsユーザ名がUNIXドメインで有効かどうかを確認します。見つからない場合は、デフォルトのUNIXユーザを使用します（設定済みの場合）。デフォルトのUNIXユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIXからWindowsへのマッピングの場合

  マッピングが見つからなかった場合、ONTAPはSMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合は、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのCIFSユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシンアカウントは、デフォルトで指定されたデフォルトのUNIXユーザにマッピングされます。デフォルト

のUNIXユーザが指定されていない場合、マシンアカウントのマッピングは失敗します。

- ONTAP 9 .5以降では、マシンアカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9 .4以前では、マシンアカウントを他のユーザにマッピングすることはできません。

  マシンアカウントのネームマッピングが定義されていても、それらのマッピングは無視されます。

UNIXユーザからWindowsユーザへのネームマッピングのためのマルチドメイン検索

ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性がUNIXユーザからWindowsユーザへのネームマッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がONTAPとどのように連携するかを理解しておく必要があります。CIFSサーバのホームドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、SVMのCIFSサーバが属しているドメインです。

- _ 双方向の信頼 _

  双方向の信頼では、両方のドメインが相互に信頼されます。CIFSサーバのホームドメインが別のドメインと双方向の信頼関係にある場合、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

  UNIXユーザからWindowsユーザへのネームマッピング検索は、ホームドメインともう一方のドメイン間で双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  アウトバウンドの信頼では、ホームドメインはもう一方のドメインを信頼します。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属するユーザを認証および許可できます。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがCIFSサーバのホームドメインを信頼します。この場合、ホームドメインはインバウンドの信頼できるドメインに属するユーザを認証または許可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

ワイルドカード（*）を使用したネームマッピング用のマルチドメイン検索の設定方法

マルチドメインネームマッピングの検索は、Windowsユーザ名のドメインセクションにワイルドカードを使用することで簡単に実行できます。次の表に、ネームマッピングエントリのドメイン部分でワイルドカードを使用してマルチドメイン検索を有効にする方法を示します。

パターン	交換	結果
root	*\\administrator	UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。
*	\ * \\ *	有効なUNIXユーザが対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 パターン「 \ * \\ * 」は、 UNIX から Windows へのネームマッピングでのみ有効であり、反対方向では無効です。

マルチドメインの名前検索の実行方法

マルチドメイン名の検索に使用する信頼できるドメインのリストを決定するには、次の2つの方法のいずれかを選択します。

- ONTAPによってコンパイルされた自動検出双方向信頼リストを使用する
- コンパイルした信頼できるドメインの優先リストを使用する

ユーザ名のドメインセクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピングされたWindowsユーザはこの検索リストでのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、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Windowsユーザの検索が行われます。
- ホームドメインに双方向の信頼関係が確立されたドメインがない場合は、ホームドメインでユーザの検索が行われます。

UNIXユーザがユーザ名にドメインセクションのないWindowsユーザにマッピングされている場合、ホームドメインでWindowsユーザの検索が行われます。

ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当するリストの先頭から開始され、最初に一致したルールに基づいて実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXプログラムのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed`。

ネームマッピングを作成する

コマンドを使用すると、ネームマッピングを作成できます `vserver name-mapping create`。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

タスクの内容

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

ステップ

1. ネームマッピングを作成します。 `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   および `-replacement`ステートメントは、 `-pattern`正規表現として記述できます。また、ステートメントを使用して、`null`の置換文字列（スペース文字）を使用してユーザへのマッピングを明示的に拒否する `" "`こともできます `-replacement`。詳細については、のマニュアルページを参照して `vserver name-mapping create` ください。

   Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログインする必要があります。

例

次のコマンドは、 vs1 という名前の SVM 上にネームマッピングを作成します。このマッピングは、UNIXからWindowsへのマッピングで、優先順位リストの1番目にあります。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、 vs1 という名前の SVM 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

デフォルトユーザの設定

ユーザに対する他のマッピング試行がすべて失敗した場合や、UNIXとWindowsの間で個々 のユーザをマッピングしないようにする場合に使用するデフォルトユーザを設定できます。または、マッピングされていないユーザの認証を失敗させる場合は、デフォルトユーザを設定しないでください。

タスクの内容

CIFS認証で、各Windowsユーザを個 々 のUNIXユーザにマッピングしない場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個 々 のWindowsユーザにマッピングしない場合は、代わりにデフォルトのWindowsユーザを指定できます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトのUNIXユーザを設定する	`vserver cifs options modify -default -unix-user` *`user_name`*
デフォルトのWindowsユーザを設定する	`vserver nfs modify -default-win-user` *`user_name`*

ネームマッピングの管理用コマンド

ONTAPには、ネームマッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
ネームマッピングを作成する	`vserver name-mapping create`
特定の位置にネームマッピングを挿入する	`vserver name-mapping insert`
ネームマッピングを表示する	`vserver name-mapping show`
2つのネームマッピングの位置を交換する IP修飾子エントリを使用してネームマッピングが設定されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネームマッピングを変更する	`vserver name-mapping modify`
ネームマッピングを削除する	`vserver name-mapping delete`
ネームマッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

詳細については、各コマンドのマニュアルページを参照してください。

著作権に関する情報

商標に関する情報