



# ネームマッピングを設定する

## ONTAP 9

NetApp  
April 24, 2024

# 目次

ネームマッピングを設定する .....	1
ネームマッピングの概要を設定する .....	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します .....	4
デフォルトユーザを設定します。 .....	5
ネームマッピングの管理用コマンド .....	5

# ネームマッピングを設定する

## ネームマッピングの概要を設定する

ONTAPでは、ネームマッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントとSMB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です。

ネームマッピングを使用する必要がある例外が2つあります。

- 純粋な UNIX 環境を構成しており、ボリュームに対して SMB アクセスや 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ている場合。

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ません。

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 という単語が先頭または末尾に付くすべての 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 が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、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。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 ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。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。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。デフォルトの SMB 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、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルト

トの UNIX ユーザを指定しないと、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。

マシンアカウントに定義されているネームマッピングがあっても無視されます。

## 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 に与える影響を理解しておく必要があります。SMB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 上の SMB 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しています。SMB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、ホームドメインと他方のドメインの間に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、ホームドメインが他方のドメインを信頼しています。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しているユーザを認証および認可できます。

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SMB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しているユーザを認証または認可できません。

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のためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、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容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（Pattern）	交換	結果
ルート	{ Asterisk } { backslash } { backslash } 管理者	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。
*	{ Asterisk } { backslash } { backslash } { Asterisk }	<div>有効な UNIX ユーザは、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。</div> <div> パターン { Asterisk } { backslash } { backslash } { Asterisk } は、UNIX から Windows へのネームマッピングでのみ有効で、反対方向では無効です。</div>

## マルチドメインの名前検索の実行方法

マルチドメインの名前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方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

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、マッピング先の Windows ユーザはこの検索リスト内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にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、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は、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 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` プログラム。

## ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。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。

このタスクについて

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
```



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

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、優先順位リスト内での位置は 1 番目です。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 ユーザーが、SVM に関連付けられた LDAP ドメイン内のユーザー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 ユーザー名の要素として「\$」が含まれています。Windows ユーザー ENG\john\$ops を UNIX ユーザー 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
```

## デフォルトユーザを設定します。

ユーザーに対する他のマッピングの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ー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。ただし、マッピングされていないユーザーの認証を失敗にする場合は、デフォルトユーザを設定しないでください。

このタスクについて

CIFS 認証で、各 Windows ユーザーを個別の UNIX ユーザーにマッピングしないようにする場合は、代わりにデフォルトの UNIX ユーザーを指定できます。

NFS 認証で、各 UNIX ユーザーを個別の Windows ユーザーにマッピングしないようにする場合は、代わりにデフォルトの Windows ユーザーを指定できます。

ステップ

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 ユーザーを設定する	<code>vserver cifs options modify -default-unix-user user_name</code>
デフォルトの Windows ユーザーを設定します	<code>vserver nfs modify -default-win-user user_name</code>

## 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します	<code>vserver name-mapping create</code>
特定の位置にネームマッピングを挿入します	<code>vserver name-mapping insert</code>
ネームマッピングを表示します	<code>vserver name-mapping show</code>
2つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、スワップは許可されません。	<code>vserver name-mapping swap</code>
ネームマッピングを変更する	<code>vserver name-mapping modify</code>
ネームマッピングを削除する	<code>vserver name-mapping delete</code>
ネームマッピングが正しいことを確認します	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

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

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权を有し、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权については、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。