



ネーム マッピングの設定

ONTAP 9

NetApp
February 12, 2026

目次

ネーム マッピングの設定	1
ONTAP NAS SVMの名前マッピング構成について学習します	1
ONTAP NAS SVMの名前マッピングについて学ぶ	1
ONTAP NAS SVM上のUNIXからWindowsへのユーザ名マッピングのマルチドメイン検索	2
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	2
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方法	3
マルチドメインの名前検索の実行方法	3
ONTAP NAS SVMの名前マッピング変換ルール	4
ONTAP NAS SVMの名前マッピングを作成する	4
ONTAP NAS SVMのデフォルトユーザを設定する	5
NFSネーム マッピングを管理するためのONTAPコマンド	6

ネーム マッピングの設定

ONTAP NAS SVMの名前マッピング構成について学習します

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クライアントからの接続かSMBクライアントからの接続かに関係なく、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環境を構成しており、ボリュームに対してSMB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 ユーザが使用され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 クレデンシャルをそれぞれ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。

ONTAP NAS SVMの名前マッピングについて学ぶ

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、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確認します。無効だった場合、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、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、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。

ONTAP NAS SVM上のUNIXからWindowsへのユーザ名マッピング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、インバウンドとアウトバウンドの2つのタイプがある単方向の信頼のどちらかにすることもできます。ホーム ドメインは、SVM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合っています。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、このホーム ドメインは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、その反対に、この信頼できるドメインはホーム ドメインに属しているユーザを認証および認可することができます。

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 ドメインおよび他方のドメインとの間に双方向の信頼関係にあるドメインでのみ実行できます。

• アウトバウンド信頼

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。

UNIX ユーザから Windows ユーザ名へのマッピング検索を実行する場合、ホームドメインとのアウトバウンド信頼を持つドメインは検索_されません_。

• インバウンドトラスト

インバウンドの信頼では、SMBサーバのホーム ドメインが他方のドメインによって信頼されています。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することも認可することもできません。

UNIX ユーザから Windows ユーザ名へのマッピング検索を実行する場合、ホームドメインとのインバウン

ド信頼を持つドメインは検索_されません_。

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方法

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	リプレースメント	結果
root	*\\管理者	UNIXユーザ「root」は「administrator」というユーザにマッピングされます。「administrator」という最初の一致するユーザが見つかるまで、すべての信頼されたドメインが順番に検索されます。
*	**	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。  パターン**は、UNIXからWindowsへ名前マッピングにのみ有効で、その逆には有効ではありません。

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で使用する信頼できるドメインのリストを決定するために、次の2つの方法のどちらかを選択できます。

- ONTAPが作成した自動検出による双方向の信頼リストを使用する
- 自分で作成した信頼できる優先ドメイン 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。

ONTAP NAS SVMの名前マッピング変換ルール

ONTAPシステムは、各SVMに対して一連の変換ルールを保持します。各ルールは、`_パターン_`と`_置換_`の2つの要素で構成されます。変換は適切な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置換が実行されます。パターンはUNIX形式の正規表現です。置換は、UNIX `'sed'` プログラムと同様に、パターンの部分式を表すエスケープシーケンスを含む文字列です。

ONTAP NAS SVMの名前マッピングを作成する

```
`vserver name-mapping
```

`create`` コマンドを使用してネームマッピングを作成できます。ネームマッピングを使用すると、WindowsユーザーがUNIXセキュリティ形式のボリュームにアクセスしたり、その逆を行ったりできるようになります。

タスク概要

各SVMについて、ONTAPは方向ごとに最大12,500の名前マッピングをサポートします。

手順

1. ネーム マッピングを作成します。

```
vserver name-mapping create -vserver vs1 -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。また、``-replacement`` ステートメントを使用して、ヌル置換文字列 `` `` (スペース文字) を使用することで、ユーザーへのマッピングを明示的に拒否することもできます。link:<https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html> ["ONTAP コマンド リファレンス"] の ``vserver name-mapping create`` の詳細をご覧ください。

WindowsからUNIXへのマッピングが作成されると、新しいマッピングの作成時にONTAPシステムへの接続を開いているすべてのSMBクライアントは、新しいマッピングを確認するためにログアウトして再度ログインする必要があります。

例

次のコマンドは、SVM vs1 に名前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

ッピングであり、優先度リストの1番目に配置されます。このマッピングにより、UNIX ユーザー johnd が Windows ユーザー ENG\JohnDoe にマッピングされます。

```
vs1::> vsriver name-mapping create -vsriver 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に別の名前マッピングを作成します。このマッピングは、優先順位リストの1番目の位置にあるWindowsからUNIXへのマッピングです。ここでは、パターンと置換に正規表現が含まれています。このマッピングは、ドメインENG内のすべてのCIFSユーザーを、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します。

```
vs1::> vsriver name-mapping create -vsriver 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に別の名前マッピングを作成します。ここでのパターンには、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。このマッピングにより、Windows ユーザーENG\john\$opsがUNIX ユーザーjohn_opsにマッピングされます。

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

ONTAP NAS SVMのデフォルトユーザを設定する

ユーザ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の認証を失敗にする必要がある場合は、デフォルト ユーザを設定しないでください。

タスク概要

CIFS認証で、各Windowsユーザを個別のUNIXユーザ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ユーザを指定できます。

NFS認証で、各UNIXユーザを個別のWindowsユーザ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	<code>vserver cifs options modify -default-unix-user user_name</code>
デフォルトのWindowsユーザを設定する	<code>vserver nfs modify -default-win-user user_name</code>

NFSネーム マッピングを管理するためのONTAP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
名前マッピングを作成する	<code>vserver name-mapping create</code>
特定の位置にネーム マッピングを挿入する	<code>vserver name-mapping insert</code>
ネーム マッピングを表示する	<code>vserver name-mapping show</code>
2つの名前マッピングの位置を交換します。注：名前マッピングが ip-qualifier エントリで構成されている場合、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する	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

`vserver name-mapping`の詳細については、[link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+name-mapping](https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+name-mapping)["ONTAPコマンド リファレンス"]を参照してください。

著作権に関する情報

Copyright © 2026 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。