



ONTAPによるNFSクライアント認証の処理

ONTAP 9

NetApp
February 12, 2026

目次

ONTAPによるNFSクライアント認証の処理	1
NASクライアントのONTAP認証について学ぶ	1
ONTAPがネーム サービスを使用する方法を学ぶ	1
NFSクライアントからONTAP SMBファイルへのアクセスを許可する	2
ONTAP NFS認証情報キャッシュの仕組み	2

ONTAPによるNFSクライアント認証の処理

NASクライアントのONTAP認証について学ぶ

NFSクライアントからSVM上のデータにアクセスするためには、NFSクライアントが正しく認証されている必要があります。ONTAPでは、UNIXクレデンシャルを設定されたネーム サービスに照らしてチェックすることで、そのクライアントを認証します。

NFSクライアントがSVMに接続すると、ONTAPは、SVMのネーム サービス設定に応じて複数のネーム サービスをチェックし、そのユーザのUNIXクレデンシャルを取得します。ONTAPでチェックできるのは、ローカルのUNIXアカウント、NISドメイン、およびLDAPドメインのクレデンシャルです。ONTAPがユーザを認証できるように、このうちの少なくとも1つを設定しておく必要があります。複数のネーム サービスと検索順序を指定できます。

UNIXのボリューム セキュリティ形式のみを使用するNFS環境の場合、この設定だけでNFSクライアントから接続するユーザが認証され、適切なファイル アクセスが提供されます。

ボリュームのセキュリティ形式がmixed、NTFS、またはunifiedの場合、ONTAPがUNIXユーザをWindowsドメイン コントローラで認証するためにはSMBユーザ名を取得する必要があります。そのためには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個々のユーザをマッピングするか、代わりにデフォルトのSMBユーザを使用します。ONTAPが検索するネーム サービスの種類と検索順序を指定するか、またはデフォルトのSMBユーザを指定します。

ONTAPがネーム サービスを使用する方法を学ぶ

ONTAPは、ネーム サービスを使用してユーザやクライアントに関する情報を取得します。ONTAPは、ストレージ システム上でデータにアクセスしたりストレージ システムを管理したりするユーザの認証や、混在環境でのユーザ クレデンシャルのマッピングを行うために、この情報を使用します。

ストレージ システムを設定する際に、ONTAPが認証用のユーザ クレデンシャルを取得するために使用するネーム サービスを指定する必要があります。ONTAPでは、次のネーム サービスをサポートしています。

- ローカル ユーザ (ファイル)
- 外部NISドメイン (NIS)
- 外部LDAPドメイン (LDAP)

```
`vserver services name-service ns-switch` コマンドファミリーを使用して、SVMにネットワーク情報の検索元と検索順序を設定します。これらのコマンドは、UNIXシステムの ` /etc/nsswitch.conf ` ファイルと同等の機能を提供します。
```

NFSクライアントがSVMに接続すると、ONTAPは指定されたネーム サービスをチェックし、ユーザのUNIXクレデンシャルを取得します。ネーム サービスが正しく設定され、ONTAPがUNIXクレデンシャルを取得できる場合、ONTAPはユーザを正常に認証します。

mixedセキュリティ形式の環境では、ONTAPによるユーザ クレデンシャルのマッピングが必要になる場合があります。ONTAPがユーザ クレデンシャルを適切にマッピングできるようにするには、環境のネーム サービスを適切に設定する必要があります。

ONTAPは、SVM管理者アカウントの認証にもネーム サービスを使用します。ネーム サービス スイッチを設定または変更する際は、SVM管理者アカウントの認証を誤って無効にしないように、この点に留意する必要があります。SVM管理ユーザの詳細については、"[管理者認証とRBAC](#)"を参照してください。

NFSクライアントからONTAP SMBファイルへのアクセスを許可する

ONTAPは、Windows NT File System (NTFS) セキュリティ セマンティクスを使用して、NFSクライアント上のUNIXユーザがNTFS権限を持つファイルにアクセスできるかどうかを判断します。

ONTAPでは、ユーザのUNIXユーザID (UID) から変換されたSMBクレデンシャルを使用して、ファイルに対するユーザのアクセス権の有無が確認されます。SMBクレデンシャルは、通常はユーザのWindowsユーザ名であるプライマリ セキュリティID (SID) と、ユーザがメンバーとなっているWindowsグループに対応する1つ以上のグループSIDで構成されています。

ONTAPでUNIX UIDをSMBクレデンシャルへ変換するときに要する時間は、数十ミリ秒から数百ミリ秒です。これは、この変換処理にドメイン コントローラへの問い合わせも含まれるためです。ONTAPではUIDがSMBクレデンシャルにマッピングされます。このマッピングはクレデンシャル キャッシュ内に入力されるので、変換によって発生する照合時間が短縮されます。

ONTAP NFS認証情報キャッシュの仕組み

NFSユーザーがストレージシステム上のNFSエクスポートへのアクセスを要求すると、ONTAPはユーザーを認証するために、外部ネームサーバまたはローカルファイルからユーザークレデンシャルを取得する必要があります。その後、ONTAPはこれらのクレデンシャルを内部クレデンシャルキャッシュに保存し、後で参照できるようにします。NFSクレデンシャルキャッシュの仕組みを理解することで、潜在的なパフォーマンスやアクセスの問題に対処できるようになります。

認証情報キャッシュがなければ、ONTAPはNFSユーザーがアクセスを要求するたびにネーム サービスにクエリを実行する必要があります。多くのユーザーがアクセスする高負荷のストレージ システムでは、これはすぐに深刻なパフォーマンス問題につながり、不要な遅延やNFSクライアント アクセスの拒否を引き起こす可能性があります。

クレデンシャル キャッシュを使用すると、ONTAPはユーザー クレデンシャルを取得し、NFSクライアントが別の要求を送信した場合に迅速かつ容易にアクセスできるように、所定の時間保存します。この方法には、次のような利点があります：

- 外部ネーム サーバー (NIS や LDAP など) への要求の処理が少なくなるため、ストレージ システムの負荷が軽減されます。
- 外部ネーム サーバーに送信するリクエストの数を減らすことで、外部ネーム サーバーの負荷を軽減します。
- ユーザを認証するために外部ソースからクレデンシャルを取得する待機時間をなくすことで、ユーザ アク

セスのスピードが向上します。

ONTAPは、認証情報キャッシュに肯定的認証情報と否定的認証情報の両方を保存します。肯定的認証情報は、ユーザが認証されアクセスが許可されたことを意味します。否定的認証情報は、ユーザが認証されずアクセスが拒否されたことを意味します。

デフォルトでは、ONTAPはポジティブクレデンシャルを24時間保存します。つまり、ユーザを最初に認証した後、ONTAPは24時間、そのユーザによるアクセス要求に対してキャッシュされたクレデンシャルを使用します。ユーザが24時間後にアクセスを要求した場合、このサイクルが最初から開始されます。ONTAPはキャッシュされたクレデンシャルを破棄し、適切なネーム サービス ソースから再度クレデンシャルを取得します。過去24時間以内にネーム サーバ上でクレデンシャルが変更された場合、ONTAPは更新されたクレデンシャルをキャッシュし、次の24時間で使用します。

デフォルトでは、ONTAPはネガティブクレデンシャルを2時間保存します。つまり、最初にユーザのアクセスを拒否した後、ONTAPはそのユーザからのアクセス要求を2時間拒否し続けます。2時間経過後にユーザがアクセスを要求した場合、このサイクルが最初から開始されます。ONTAPは適切なネーム サービス ソースからクレデンシャルを再度取得します。過去2時間以内にネーム サーバ上でクレデンシャルが変更された場合、ONTAPは更新されたクレデンシャルをキャッシュし、次の2時間使用します。

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。