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

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。