ONTAPによるNFSクライアント認証の処理

ONTAP 9

NetApp
April 24, 2024

目次

ONTAPによるNFSクライアント認証の処理

ONTAP による NFS クライアント認証の処理の概要

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 ONTAP 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。

mixed、NTFS、またはunifiedのボリュームセキュリティ形式を使用している場合、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。これには、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ことも、デフォルトのSMBユーザを指定することもできます。

ONTAP でのネームサービスの使用方法

ONTAP は、ネームサービスを使用してユーザおよび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ときに、 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）

を使用します `vserver services name-service ns-switch` ネットワーク情報を検索するソースとソースの検索順序をSVMに設定するコマンドファミリー。これらのコマンドは、と同等の機能を提供します `/etc/nsswitch.conf` UNIXシステム上のファイル。

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て、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ていて ONTAP が UNIX クレデンシャルを取得できる場合、 ONTAP はユーザの認証に成功します。

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にはこの点を念頭に置いて、 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する必要があります。SVM管理ユーザの詳細については、を参照してください "管理者認証と RBAC"。

ONTAP による NFS クライアントからの SMB ファイルアクセスの許可方法

ONTAP では、 NTFS （ Windows NT ファイルシステム）のセキュリティセマンティクスを利用して、 NTFS アクセス権によるファイルへのアクセス権が、 NFS クライアント上の UNIX ユーザにあるかどうかが判別されます。

ONTAP では、ユーザの UNIX User ID （ UID ； UNIX ユーザ ID ）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 Security Identifier （ SID ；セキュリティ識別子）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 は UID を SMB クレデンシャルにマッピングします。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検証時間が短縮されます。

NFS クレデンシャルキャッシュの仕組み

NFS ユーザ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、ユーザの認証を行う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クレデンシャルを取得する必要があります。その後、 ONTAP は、以降の参照用にこれらのクレデンシャルを内部のクレデンシャルキャッシュに格納します。NFS クレデンシャルキャッシュの仕組みを理解しておくと、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。

クレデンシャルキャッシュがないと、 ONTAP ユーザは NFS ユーザからアクセスが要求されるたびにネームサービスを照会しなければなりません。多数のユーザがアクセスする使用頻度の高いストレージシステムでは、こうした状況がすぐに深刻なパフォーマンス上の問題につながり、不必要な遅延や、場合によっては NFS クライアントアクセスの拒否さえ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があれば、 ONTAP は取得したユーザクレデンシャルをあらかじめ決められた期間だけ格納しておき、同じ NFS クライアントから再び要求があっても迅速かつ簡単にアクセスすることができます。この方法には、次の利点があります。

- 外部ネームサーバ（ NIS や LDAP など）への要求の処理を減らすことで、ストレージシステムの負荷が軽減されます。
- 外部ネームサーバに送信する要求を減らすことで、外部ネームサーバの負荷が軽減されます。
- ユーザの認証を行う前に外部ソースからクレデンシャルを取得するための待ち時間をなくすことで、ユーザアクセスが高速になります。

ONTAP は、受理されたクレデンシャルと拒否されたクレデンシャルの両方をクレデン受理されたクレデンシャルとは、ユーザが認証されてアクセス権を付与されたこと拒否されたクレデンシャルとは、ユーザが認証されずに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 は受理されたクレデンシャルを 24 時間保存します。つまり、ユーザの最初の認証から 24 時間は、そのユーザからのすべてのアクセス要求で ONTAP はキャッシュされたクレデンシャルを使用します。24 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 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びクレデンシャルを取得します。それまでの 24 時間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、次の 24 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

デフォルトでは、 ONTAP は拒否されたクレデンシャルを 2 時間保存します。つまり、ユーザに対する最初のアクセス拒否から 2 時間は、そのユーザからのすべてのアクセス要求を ONTAP は拒否し続けます。2 時間後にそのユーザからアクセスが要求された場合は、最初からやり直しになります。 ONTAP は適切なネームサービスソースから再びクレデンシャルを取得します。それまでの 2 時間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、次の 2 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。