■ NetApp

ONTAPによるNFSクライアント認証の処理 ONTAP 9

NetApp April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/nfs-admin/nfs-client-authentication-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目次

ONTAPによるNFSクライアント認証の処理 · · · · · · · · · · · · · · · · · · ·	 	 	 1
ONTAP による NFS クライアント認証の処理の概要 · · · · · · · · · · · · · · · · · · ·	 	 	 1
ONTAP でのネームサービスの使用方法 · · · · · · · · · · · · · · · · · · ·	 	 	 1
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・・・・・	 	 	 2
NFS クレデンシャル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

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。

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権を有し、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権については、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。