



NASファイルアクセスについて理解する ONTAP 9

NetApp
December 20, 2024

目次

NASファイルアクセスについて理解する	1
ネームスペースとジャンクションポイント	1
ONTAPによるファイルアクセスの制御方法	6
ONTAPによるNFSクライアント認証の処理	7

NASファイルアクセスについて理解する

ネームスペースとジャンクションポイント

ネームスペースとジャンクションポイントの概要

`nas_namespace_` は、`_junction points_to` によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限があるクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

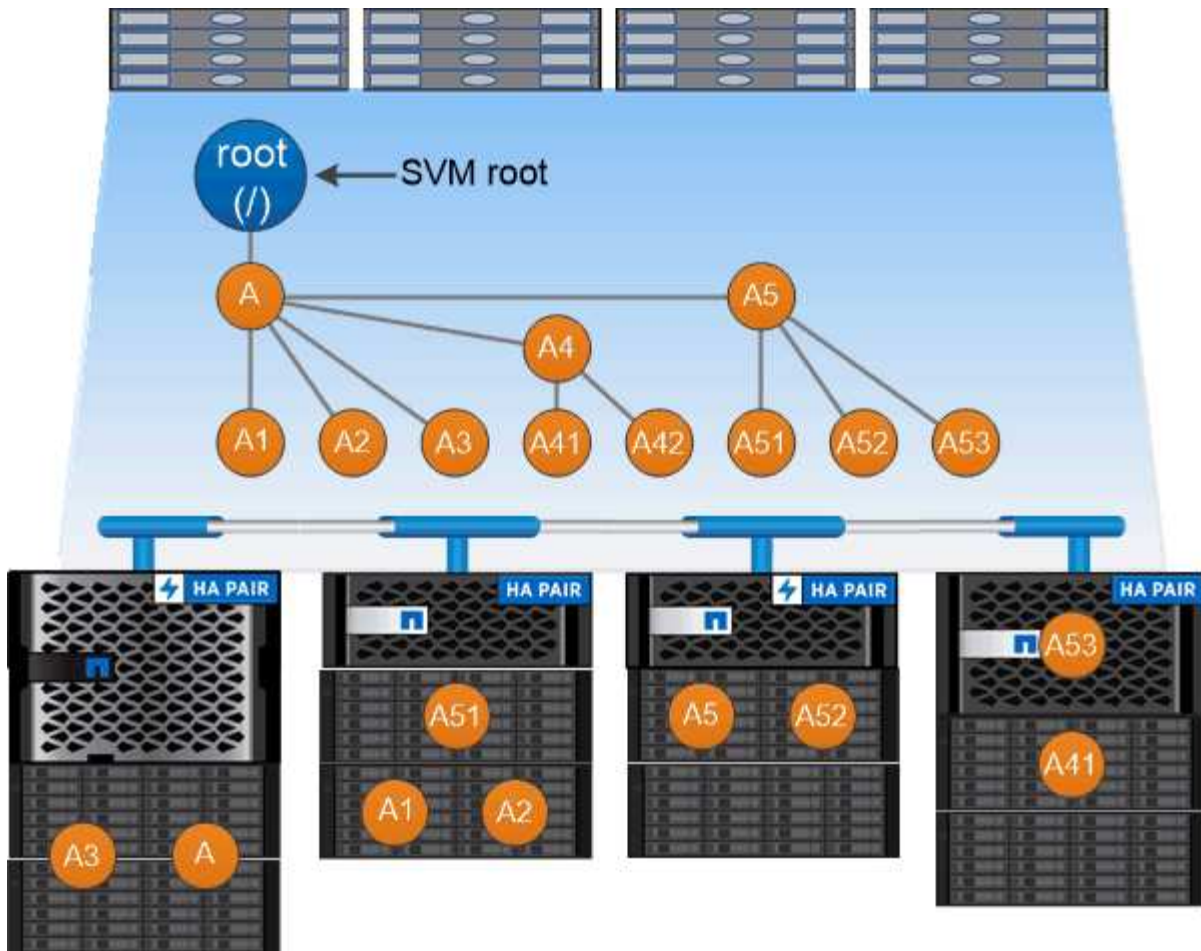
NAS クライアントは、目的のファイルを含むすべてのボリュームをマウントするのではなく、`nfs_export_` をマウントするか、`SMB_share` にアクセスします。`_` エクスポートまたは共有は、ネームスペース全体またはネームスペース内の中間的な場所を表します。クライアントは、アクセスポイントより下にマウントされているボリュームにのみアクセスします。

ネームスペースには必要に応じてボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションのすぐ下に作成することも、ボリューム内のディレクトリに作成することもできます。「vol3」という名前のボリュームのボリュームジャンクションへのパスは、またはの `/vol1/dir2/vol3`` ようになります ``/vol1/vol2/vol3 /dir1/dir2/vol3`。このパスのことを `_junction` パスと呼びます。 `_`

SVM には、それぞれ一意のネームスペースがあります。SVM ルートボリュームは、ネームスペース階層へのエントリポイントです。



ノードに障害やフェイルオーバーが発生したときにデータを引き続き利用できるようにするには、SVM ルートボリュームに `_load-sharing mirror_copy` を作成する必要があります。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

例

次の例は、ジャンクションパスがである「home4」という名前のボリュームをSVM vs1上に作成し`/eng/home`ます。

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

一般的なNAS名前空間アーキテクチャとは

SVM 名前空間を作成するときに使用できる一般的な NAS 名前空間アーキテクチャがいくつかあります。ビジネスやワークフローのニーズに合った名前空間アーキテクチャを選択できます。

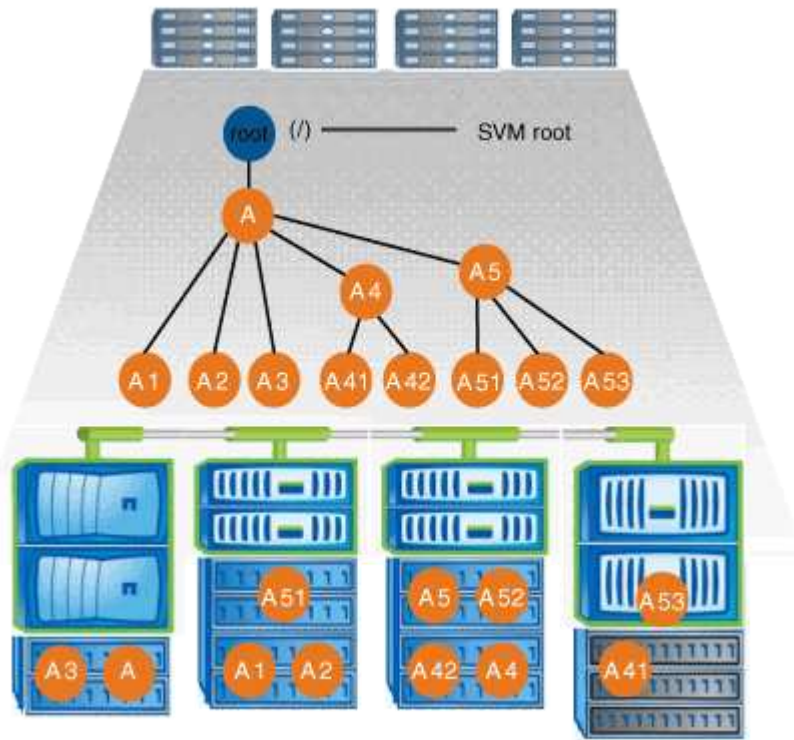
名前空間の最上位は常にルートボリュームで、スラッシュ (/) で表されます。ルートの下の名前空間アーキテクチャは、次の3つの基本カテゴリに分類されます。

- 名前空間のルートへのジャンクションが1つだけの単一分岐ツリー

- ネームスペースのルートへのジャンクションポイントが複数ある複数分岐ツリー
- ネームスペースのルートへの個別のジャンクションポイントを持つ複数のスタンドアロンボリューム

単一分岐ツリーを使用するネームスペース

単一分岐のツリーを使用するアーキテクチャには、SVM ネームスペースのルートへの単一の挿入ポイントがあります。単一の挿入ポイントには、ジャンクションされたボリュームまたはルート直下のディレクトリを指定できます。他のすべてのボリュームは、単一の挿入ポイント（ボリュームまたはディレクトリ）の下のジャンクションポイントでマウントされます。

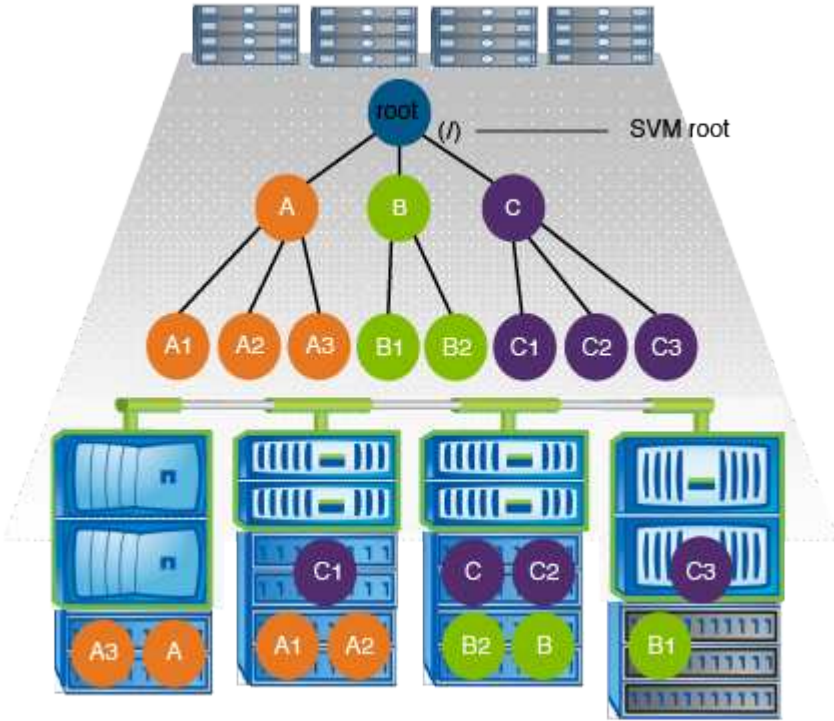


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「d ATA」というディレクトリです。

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

複数分岐ツリーを使用するネームスペース

複数分岐のツリーを使用するネームスペースには、SVM ネームスペースのルートへの複数の挿入ポイントがあります。挿入ポイントは、ルートの下にジャンクションされたボリュームまたはディレクトリのいずれかです。他のすべてのボリュームは、挿入ポイントの下にジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

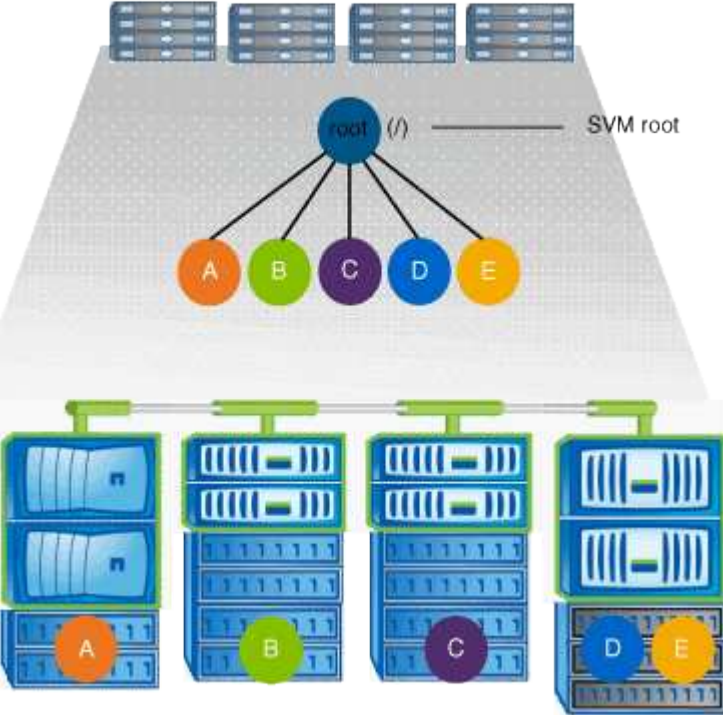


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「data」と「projects」という名前のディレクトリです。挿入ポイントの 1 つは「audit」という名前の結合されたボリュームです。

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

複数のスタンドアロンボリュームを使用するネームスペース

スタンドアロンボリュームを使用するアーキテクチャでは、すべてのボリュームに SVM ネームスペースのルートへの挿入ポイントがありますが、それらのボリュームは別のボリュームの下でジャンクションされません。各ボリュームには一意のパスがあり、ルート直下でジャンクションされるか、ルートより下のディレクトリでジャンクションされます。



たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 5 つの挿入ポイントがあり、それぞれが 1 つのボリュームへのパスを表す以下のような構成になります。

Vserver	Volume	Junction		Junction	
		Active	Junction Path	Path	Source
vs1	eng	true	/eng	RW_volume	
vs1	mktg	true	/vol/mktg	RW_volume	
vs1	project1	true	/project1	RW_volume	
vs1	project2	true	/project2	RW_volume	
vs1	sales	true	/sales	RW_volume	
vs1	vs1_root	-	/	-	

ONTAPによるファイルアクセスの制御方法

ONTAPによるファイルアクセスの制御方法の概要

ONTAP は、指定された認証ベースおよびファイルベースの制限に従って、ファイルアクセスを制御します。

クライアントがファイルにアクセスするためにストレージシステムに接続するとき、ONTAP は 2 つのタスクを実行する必要があります。

- 認証

ONTAP は、信頼できるソースで ID を検証して、クライアントを認証する必要があります。また、クライアントの認証タイプは、エクスポートポリシーの設定時にクライアントがデータにアクセスできるかどうかの判断に使用できる方法の 1 つです（CIFS の場合は省略可能）。

- 許可

ONTAP は、ユーザのクレデンシャルとファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスのタイプ（ある場合）を判別することで、ユーザを許可する必要があります。

ファイルアクセス制御を適切に管理するため、ONTAP は、NIS、LDAP、および Active Directory サーバなどの外部サービスと通信します。CIFS または NFS を使用するストレージシステムのファイルアクセスを設定するには、ONTAP の環境に応じて、サービスを適切に設定する必要があります。

認証ベースの制限

認証ベースの制限を使用すると、Storage Virtual Machine (SVM) に接続できるクライアントマシンおよびユーザを指定できます。

ONTAP は、UNIX サーバおよび Windows サーバの両方からの Kerberos 認証をサポートします。

ファイルベースの制限

ONTAP では、3 つのレベルのセキュリティを評価して、SVM 上にあるファイルおよびディレクトリに対して要求された操作を実行する権限がエンティティにあるかどうかを判

断します。アクセスは、3つのセキュリティレベルの評価後に有効な権限によって判断されます。

どのストレージオブジェクトにも、最大3種類のセキュリティレイヤを含めることができます。

- エクスポート（NFS）および共有（SMB）セキュリティ

エクスポートおよび共有セキュリティは、特定のNFSエクスポートまたはSMB共有へのクライアントアクセスに適用されます。管理Privilegesを持つユーザは、SMBクライアントおよびNFSクライアントからエクスポートおよび共有レベルのセキュリティを管理できます。

- ストレージレベルのアクセス保護のファイルとディレクトリのセキュリティ

ストレージレベルのアクセス保護セキュリティは、SVMボリュームへのSMBおよびNFSクライアントアクセスに適用されます。NTFSのアクセス権限のみがサポートされます。ONTAPがストレージレベルのアクセス保護が適用されているボリューム上のデータにアクセスするUNIXユーザのセキュリティチェックを実行するには、UNIXユーザがボリュームを所有するSVM上のWindowsユーザにマッピングされている必要があります。



NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示した場合、ストレージレベルのアクセス保護セキュリティは表示されません。システム（WindowsまたはUNIX）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。

- NTFS、UNIX、およびNFSv4の標準のファイルレベルセキュリティ

ストレージオブジェクトを表すファイルまたはディレクトリには、ネイティブのファイルレベルのセキュリティが存在します。ファイルレベルのセキュリティはクライアントから設定できます。ファイル権限は、データへのアクセスにSMBとNFSのどちらを使用するかに関係なく有効です。

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、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することで、そのユーザのUNIXクレデンシャルを取得します。ONTAPでは、ローカル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をチェックできます。ONTAPがユーザを正常に認証できるように、これらのうち少なくとも1つを設定する必要があります。複数のネームサービスと、ONTAPによる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を使用する純粋なNFS環境では、この設定だけでNFSクライアントから接続してい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とクライアントに関する情報を取得します。ONTAPは、この情報を使用して、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います。

ストレージシステムを設定する場合は、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）

ネットワーク情報を検索するソースやソースの検索順序をSVMで設定するには、コマンドファミリーを使用し`vserver services name-service ns-switch`ます。これらのコマンドは、UNIXシステムのファイルと同等の機能を提供し`/etc/nsswitch.conf`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でユーザクレデンシャルが適切にマッピングされるようにするには、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"カンリシヤニンシヨウトRBAC"](#)。

ONTAPニヨルNFSクライアントカラノSMBファイルアクセスノキョカホウホウ

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を判別されます。

ONTAPでは、ユーザのUNIXユーザID（UID）をSMBクレデンシャルに変換し、そのクレデンシャルを使用してユーザにファイルへのアクセス権があることを確認します。SMBクレデンシャルは、プライマリのSecurity Identifier（SID；セキュリティ識別子）（通常はユーザのWindowsユーザ名）と、ユーザが属しているWindowsグループに対応する1つ以上のグループSIDで構成されます。

ONTAPがUNIX UIDをSMBクレデンシャルに変換するのにかかる時間は、数十ミリ秒から数百ミリ秒です。これは、この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、クレデンシャルキャッシュにマッピングを入力して変換によって発生する検証時間を短縮します。

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。ONTAPは、後で参照できるように、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することで、パフォーマンスや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。
- ユーザが認証される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機時間をなくすことで、ユーザアクセスを高速化します。

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シャルを受け取っ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、ユーザの初回認証後、ONTAPはそのユーザからのすべての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24時間使用します。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は更新されたクレデンシャルをキャッシュして、次の24時間で使用するようになります。

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、ユーザへのアクセスを最初に拒否したあと、ONTAPはそのユーザからのすべてのアクセス要求を2時間拒否し続けます。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。過去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時間で使用するようになり、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。