テクニカル レポート

NetApp ONTAP でのマルチプロトコルNAS
概要とベストプラクティス

ネットアップ
Justin Parisi
2021年4月| TR-4887

概要

このテクニカルレポートでは、NetApp®ONTAP ®データ管理ソフトウェアにおけるマルチプロトコルNASアクセスの仕組みと、マルチプロトコル環境のベストプラクティスについて説明します。

目次

表一覧

図一覧

ベストプラクティス一覧

概要

このテクニカルレポートでは、ONTAP データ管理ソフトウェアを実行するネットアップストレージシステム上でのマルチプロトコルのNASアクセスについて説明します。マルチプロトコルNASアクセスでは、エンタープライズストレージシステムとスケールアウトストレージシステムから、NFSプロトコルとCIFS / SMBプロトコルを使用して、LinuxベースとWindowsベースの両方のオペレーティングシステムを実行しているクライアントにアクセスを提供できます。マルチプロトコルNAS用語については、このドキュメントの「マルチプロトコルNAS用語」を参照してください

NASとは

マルチプロトコルNASとは、本質的に、複数のNASプロトコルによる統合NASアクセスという名前のことです。ネットアップストレージシステムでマルチプロトコルNASを利用すると、使用するプロトコルの種類に関係なく、すべてのオペレーティングシステムのユーザが同じデータセットにシームレスにアクセスできます。マルチプロトコル環境で必要となるプロトコルは、CIFS / SMBとNFSです。

マルチプロトコルNASは混合モードとも呼ばれますか。

一般的な誤解の1つに、マルチプロトコルNASは混在モードとも呼ばれるという考えがあります。この誤解では、NASを実行するネットアップストレージシステムを導入する際に混乱が生じています。mixedセキュリティ形式の概念も存在するからです。mixedセキュリティ形式については、このドキュメントで後述します（「セキュリティ形式」の項）。

CIFS/SMBとは

CIFS/SMBは、主にMicrosoft Windowsを実行しているオペレーティングシステムを使用して、イーサネットベースのネットワーク間でファイルを共有する方法です。CIFSは、Windows 2000で導入されたネイティブファイル共有プロトコルであり、最新のオペレーティングシステムでクライアントとサーバの間の通信の基盤となるプロトコルとしてSMBを利用します。

CIFS / SMBは、Sambaなどのサードパーティ製の実装を通じて、Apple、Linux、Solarisなどの他のWindows以外のオペレーティングシステムでも使用されます。ネットアップストレージシステム上 のWindows以外のオペレーティングシステムでのCIFS / SMBのサポートは一定ではなく、Interoperability Matrix Tool（IMT）に記載されています。

注： CIFSとSMBはさまざまな点で異なりますが、このマニュアルでは、この2つの用語を同じ意味で使用しています。

NFSとは

NFSは、ユーザがイーサネットベースのネットワークでファイルを共有する方法で、主にLinux、Solaris、UNIX、HPUXなどを実行しているオペレーティングシステム上で使用されます。NFSは、Request for Comments（RFC）と呼ばれるドキュメントを介して、IETFによって定義された一連の標準に従います。これらの標準には、エンタープライズレベルのNFSアクセスを提供することを意図した、すべての主要なNFSクライアントおよびサーバベンダーが従うものとします。NFSは、使用するNFSのバージョンに依存する一連の基本メッセージに依存します。ONTAP のNFSの詳細については、TR-4067：『NFS Best Practices and Implementation Guide』を参照してください。

異機種混在のNAS環境との違い

一部のサイトにはWindowsのみの環境やUNIXのみを使用してすべてのデータにアクセスする環境があります。その場合、次のいずれかを使用します。

- CIFS / SMBとNTFSファイルセキュリティ
- NFSとUNIXのファイルセキュリティ（モードビットまたはNFSv4.xアクセス制御リスト（ACL）

しかし、多くのサイトで、WindowsクライアントとUNIXクライアントの両方からデータセットにアクセスできるようにする必要があります。これらの環境では、ONTAPはマルチプロトコルNASをネイティブでサポートしています。ユーザがネットワークで認証され、適切な共有権限またはエクスポート権限と、必要なファイルレベルの権限の両方が付与されると、NFSを使用するUNIXホストから、またはCIFS / SMBを使用するWindowsホストから、そのユーザがデータにアクセスできるようになります。

マルチプロトコルのNASアクセスを利用 する場合は、オプションとして提供されていても、mixedセキュリティ形式（mixedモードとも呼ばれます）のボリュームやqtreeを使用する必要はありません。

マルチプロトコルNASを使用する理由

マルチプロトコルNASとONTAP データ管理ソフトウェアを使用すると、さまざまなメリットがあります。異なるNASプロトコルを使用するクライアントがデータセットに同時にシームレスにアクセスできるようにすると、次のようなメリットがあります。

- ストレージ管理者の全体的な管理タスクを減らします。
- 複数のクライアントからのNASアクセス用に、データのコピーを1つだけ格納するようにします。
- プロトコルに依存しないNASを使用すると、ストレージ管理者はACLの形式とエンドユーザに提供されるアクセス制御を制御できます。
- NAS環境でアイデンティティ管理操作を一元化します。

ONTAP データ管理ソフトウェアは、25年以上にわたってエンタープライズクラスのマルチプロトコルNASアクセスを提供してきました。スケールアウトONTAP クラスタとNetApp ONTAP FlexGroup ボリュームの登場により、ストレージ管理者はマルチプロトコルNAS環境での柔軟性をさらに高めることができるようになりました。

ユースケース

マルチプロトコルNASの最も一般的な使用方法には、次のようなものがありますが、これらに限定されません。

- ホーム ディレクトリ
- ソースコードリポジトリ
- 研究開発株
- イメージリポジトリ
- オーディオおよびビデオの編集/レンダリング

共通の課題

マルチプロトコルNASアクセスは、多くの組織に柔軟性を求められていますが、マルチプロトコルNASでは、プロトコル間の共有という概念に固有の一連の課題が生じることを、認識することが難しくなっています。この認識は、実際にはアースされていますが、基盤となるインフラストラクチャがマルチプロトコルNASアクセスに対応していない場合に限ります。たとえば、アイデンティティ管理のニーズに対応するLightweight Directory Access Protocol（LDAP）サーバを立ち上げることで、マルチプロトコルのNAS環境を大幅に簡易化できます。

これらの課題には、以下が含まれますが、これらに限定されません。

- 複数のプロトコル、オペレーティングシステム、ストレージシステムに関する知識が必要
- DNS、LDAP、NISなどのネームサービスサーバの実用的な知識。
- 外部要因：
  - 複数の部門やITグループ（Windowsグループ、UNIXグループなど）への対応
  - 企業買収
  - ドメイン統合
  - 組織を再構築します
  - 多くの可動部品

これらの非常に現実的な課題にもかかわらず、マルチプロトコルNASのセットアップ、設定、アクセスは、ベストプラクティスに従っていれば、すべての環境にシンプルかつシームレスに統合できます。このドキュメントでは、マルチプロトコルNASをできるだけ簡単に設定および管理する方法について説明します。

ONTAP におけるマルチプロトコルNASの仕組み：基本事項

ONTAP のマルチプロトコルNASでは、ネームマッピング形式と権限形式を組み合わせて、使用するプロトコルに関係なく一貫したデータアクセスを提供します。つまり、NFSまたはSMBからファイルにアクセスしている場合でも、それらのファイルへのアクセス権を持つユーザーは、ファイルにアクセスでき、これらのファイルにアクセスできないユーザーはファイルにアクセスできないということです。

NASクライアントがONTAP 内のボリュームへのアクセスを要求すると、エンドユーザに最も透過的なエクスペリエンスを提供するために、バックグラウンドでいくつかの処理が行われます。

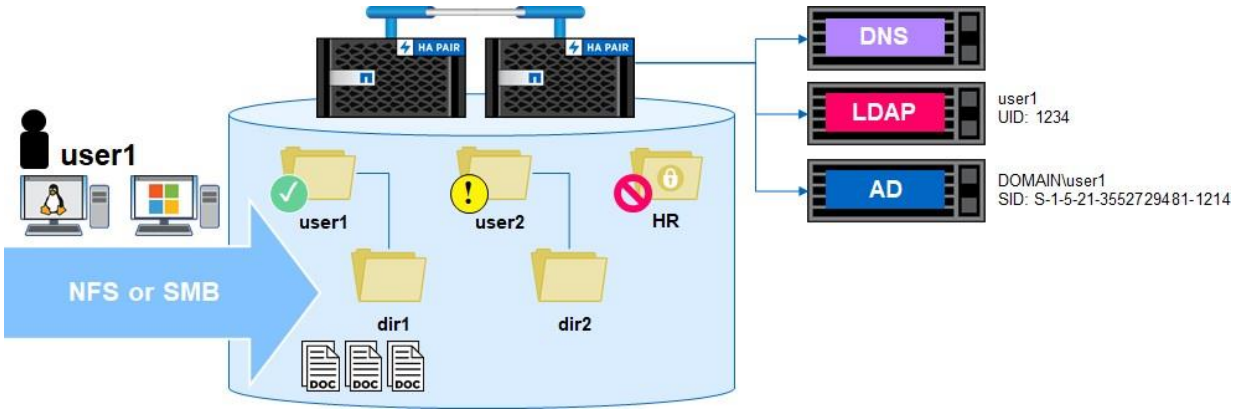
このプロセスはONTAP の設定によって制御されますが、一般的な概念は引き続き適用されます。

1. NASクライアントがONTAP Storage VMにNAS接続しています。
2. NASクライアントは、ユーザーID情報をONTAP に渡します。
3. ONTAPは、NASクライアント/ユーザーがNAS共有にアクセスできることを確認します。
4. ONTAPはそのユーザを取得し、ONTAP がネームサービス内で検索可能な有効なユーザにマッピングします。
5. ONTAPは、そのユーザを使用して、システム内のファイルレベルの権限と比較します。
6. これらの権限によって、ユーザのアクセスレベルが制御されます。

図1 では、user1は、SMBまたはNFSを介してONTAP Storage Virtual Machine（SVM）の共有に認証しています。ONTAPは、LDAPおよびActive Directory内でユーザを検出し、ユーザ1：1をマッピングします。この場合、ユーザはuser1と確認され、user1のアクセス権を取得します。

この場合、ユーザーは自分のフォルダを完全に制御し、user2のフォルダへの読み取りアクセス権を取得します。また、HRフォルダへのアクセス権はありません。これはすべて、ファイルシステムで指定されたACLに基づいています。

図1）マルチプロトコルNASの基本操作



このセクションの残りの部分では、マルチプロトコルNASアクセスに関連するその他の概念について説明します。

ネームスペースとファイルシステムの概念

ONTAP では、SVMを導入してクラスタ内のセキュアなテナントとして機能させ、NASクライアントに独立した固有のファイルシステムを提供できます。SVMには、独自のボリューム、ネットワークインターフェイス、ネームサービス、およびActive Directory構成、権限モデルを設定でき、また、NAS環境の単一のネームスペースとして機能できます。

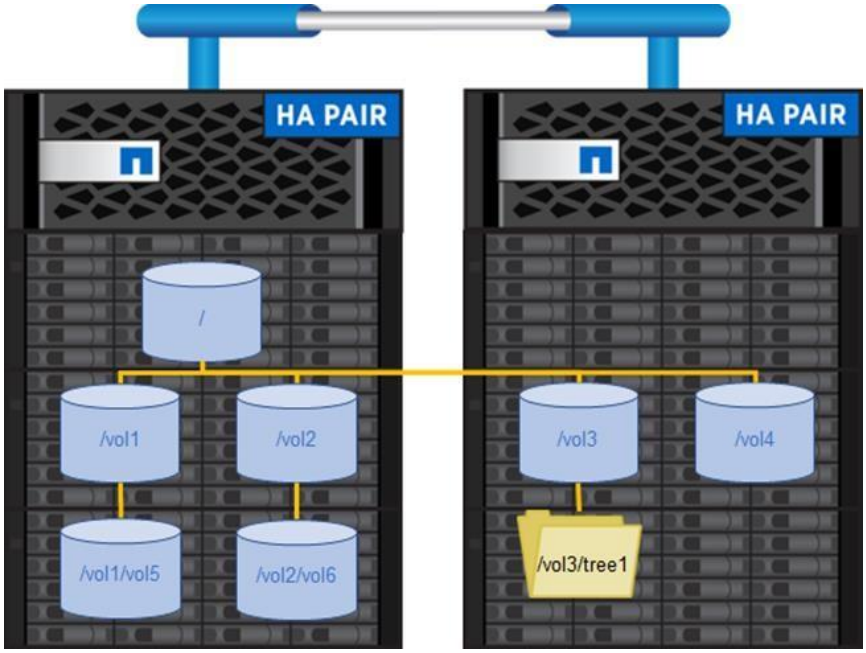
クラスタネームスペース

ONTAP のネームスペースは、クラスタ内の複数のノードにホストされるファイルシステムの集まりで、拡張性に優れたパフォーマンスと容量を提供します。各SVMには、単一のルート ボリュームで構成されるファイル ネームスペースが1つあります。この名前空間は、「/」の場所から始まります。以降 `-junction-path`のボリュームおよび

qtreeはすべて、ボリュームオプションによってエクスポートパスが定義されており、横断的に「/」を行います。SVMネームスペースは1つ以上のボリュームで構成されます。ボリューム同士はジャンクションを使用してリンクされ、あるボリュームの名前付きジャンクションinodeから別のボリュームのルート ディレクトリに接続されます。1つのクラスタには複数のSVMを含めることができますが、各SVMのvsrootと「/」は1つだけで構成され、SVMごとに一意のファイルシステムIDが設定されます。これにより、異なるSVMにある複数のボリュームでファイルシステムIDやファイルハンドルを共有できないようになり、マルチテナント環境でNFSエクスポートをマウントする際の問題を回避できます。

SVMに属するすべてのボリュームは、そのクラスタのグローバル ネームスペースにリンクされます。クラスタ ネームスペースは、クラスタ内の単一ポイントでマウントされます。クラスタ内のクラスタ ネームスペースの最上位ディレクトリは統合型ディレクトリで、クラスタ内の各SVMネームスペースのルート ディレクトリのエントリが含まれています。ネームスペース内 のボリュームには、NetApp FlexVol ®ボリュームまたはFlexGroup ボリュームを使用できます。

図2）クラスタネームスペース



ネームスペースの保護

vsrootボリュームは、複数のノードからSVMにアクセス可能であっても、クラスタ内の1つのノードにしか実装されていません。vsrootはNFSクライアントがネームスペースをトラバースする方法なので、NFSの処理には欠かせません。

```
cluster::> vol offline -vserver NFS -volume vsroot

Warning: Offlining root volume vsroot of Vserver NFS will make all volumes on that Vserver
inaccessible.
Do you want to continue? {y|n}: y
Volume "NFS:vsroot" is now offline.
```

vsrootボリュームが何らかの理由で使用できない場合、vsrootボリュームがファイルシステムをトラバースする必要があるたびにNFSクライアントから問題が発生します。

このプロセスには、次の動作が含まれますが、これらに限定されることはありません。

- マウント要求がハングします。
- “/”がマウントlsされている場合、“/”から別のボリュームへのトラバーサル(cd)は、などの実行中の操作がハングします。

- ボリュームがオンラインに戻ったあともマウントがビジー状態であるため、アンマウント処理が失敗することがあります。
- ボリュームがすでに「/ `/vol1`」の下にマウントされている場合（など）、読み取り/書き込み/リスト表示は成功します。

ONTAP の負荷共有ミラー（LSミラー）は、NetApp ONTAP SnapMirror®機能を利用してvsrootの耐障害性を向上させることができます。

注： LSミラーはvsrootボリュームでのみサポートされます。データボリューム間で負荷を共有するには、代わりに「NetApp FlexCache volumes」を使用することを検討してください。

vsrootボリュームのLSミラーを使用できる場合、NFSv3処理ではLSミラーデスティネーションボリュームを利用してファイルシステムをトラバースできます。LSミラーが使用されている場合、NFSマウント内の.adminフォルダからソースボリュームにアクセスできます。

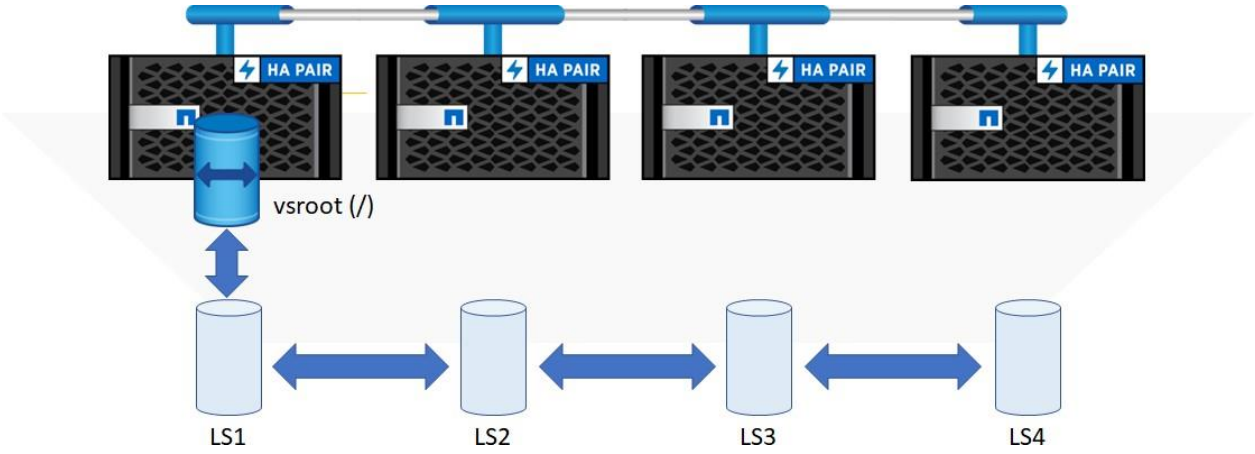
詳細については、「負荷共有ミラー関係の作成と初期化」を参照してください。

NFSv3環境のvsrootボリュームのLSミラー関係を作成することを強く推奨します。

注： NFSv4.xプロトコルの性質上、NFSv4.xクライアントがLSミラーボリュームを使用してファイルシステムをトラバースすることはできません。

図3 は、vsrootが使用できない場合に、負荷共有ミラーから「/」へのアクセスを提供する方法を示しています。

図3）vsrootボリュームの負荷共有ミラー保護



vsrootボリュームの負荷共有ミラーを作成するには、次の手順を実行します。

1. 通常、vsrootボリュームのサイズは1GBです。新しいボリュームを作成する前にvsrootボリュームサイズを確認し、新しいボリュームがすべて同じサイズであることを確認します。
2. クラスタ内の各ノードのvsrootをミラーリングするデスティネーションボリュームを作成します。たとえば、4ノードクラスタで、-type DPを指定して4つの新しいボリュームを作成します。
3. vsrootソースから、新しく作成した各DPボリュームへの新しいSnapMirror関係を作成します。名前空間ルートの変更率に応じて、更新のスケジュールを指定します。たとえば、新しいボリュームを定期的に作成する場合は毎時、作成しない場合は毎日です。
4. `initialize-ls-set` コマンドを使用してSnapMirrorを初期化します。

疑似ファイルシステム

ONTAP アーキテクチャ では、RFC 7530 NFSv4標準に準拠した正しい疑似ファイルシステムを使用できるようになりました。

```
Servers that limit NFS access to "shares" or "exported" file systems should provide a pseudo-file
system into which the exported file systems can be integrated, so that clients can browse the
```

```
server's namespace. The clients' view of a pseudo-file system will be limited to paths that lead
to exported file systems.
```

セクション7.3では、次のようになります

```
NFSv4 servers avoid this namespace inconsistency by presenting all the exports within the
framework of a single-server namespace. An NFSv4 client uses LOOKUP and READDIR operations to
browse seamlessly from one export to another. Portions of the server namespace that are not
exported are bridged via a "pseudo-file system" that provides a view of exported directories
only. A pseudo-file system has a unique fsid and behaves like a normal, read-only file system.
```

ONTAP `/vol` では、ONTAP 7-Modeで表示されるエクスポートされたボリュームの要件が廃止され、疑似ファイルシステムに対してより標準的なアプローチを採用しています。このため、既存のNFSインフラをネットアップストレージとシームレスに統合できるようになりました。7-Modeの場合と同様に、「/」は真の意味で「/」、「/vol/vol0」はリダイレクタではないからです。

clustered Data ONTAPでは、より厳しいアクセス権から緩いアクセス権という順序の場合にのみ疑似ファイルシステムが適用されます。たとえば、vsroot（/にマウント）のアクセス権がデータ ボリュームのアクセス権（/volnameなど）よりも厳しい場合、疑似ファイルシステムが適用されます。

疑似ファイルシステムを使用すると、必要に応じて、ジャンクションパスを使用して他のボリュームにボリュームをマウントすることで、ストレージ管理者が独自のファイルシステムネームスペースを作成できます。この概念を 図2に示します

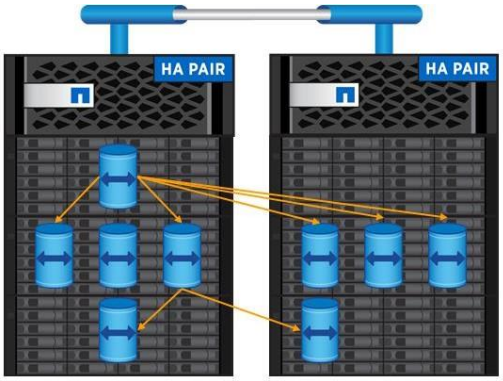
ジャンクション パス

ONTAP では、ジャンクションパスを使用して、ボリュームやqtree、さらにはフォルダを同じクラスタネームスペース内のマウントポイントとして使用することで、NAS環境用の独自のフォルダツリー構造を作成できます。

ジャンクションパスを使用すると、ボリュームを別のボリューム、qtreeへのボリューム、またはサブディレクトリにマウントできます。これにより、ストレージ管理者はネームスペースをきめ細かく制御できるほか、データの保護と管理を柔軟に行うことができます。

図4 は、100TBを超える容量を実現するために結合されたアーキテクチャを使用したFlexVol の設計を示してい

図4）100TB超の容量に対応するFlexVolによるジャンクション アーキテクチャ



注： FlexVol ボリュームとFlexGroup ボリュームは、どちらもジャンクションパスアーキテクチャで使用できます。

FlexVol

フレキシブルボリュームであるNetApp FlexVol ソフトウェアは、ONTAP 7.0（Data ONTAP 7-Mode）リリースの一部として2005年にData ONTAP ソフトウェアに導入されました。FlexVolの目的は、ストレージ ファイルシステムをハードウェア構成全体にわたって仮想化することにより、絶えず変化するデータセンターにおける柔軟なストレージ管理を実現することでした。

FlexVolは、無停止で拡張または縮小でき、シンプロビジョニングされたコンテナとしてストレージ オペレーティング システムに割り当てることで、ストレージ システムのオーバープロビジョニングを可能にしました。ストレージ管理者は、ユーザの要求に応じてスペースを柔軟に割り当てることができます。

qtree

ストレージ管理者は、qtreeを使用してONTAP のGUIまたはCLIからフォルダを作成し、ボリューム内のデータを論理的に分離できます。qtreeでは、独自のエクスポートポリシー、固有のセキュリティ形式、クォータ、および詳細な統計情報を有効化することで、データ管理の柔軟性が向上します。

qtreeには複数のユースケースがあり、ホームディレクトリワークロードに便利です。qtreeには、データにアクセスするユーザのユーザ名を反映した名前を付け、ユーザ名に基づいてアクセスを提供する動的共有を作成できます。

FlexGroup ボリューム内のqtreeに関する詳細情報を次に示します。

- クライアントには、qtreeがディレクトリとして表示されます。
- qtreeはボリュームレベルで作成できます。現在のところ、ディレクトリの下にqtreeを作成してサブディレクトリであるqtreeを作成することはできません。
- qtreeはSnapMirrorではレプリケートできません。現在のSnapMirrorはボリュームレベルでのみ実行されています。ボリュームをさらに細かくレプリケーションする場合は、ジャンクションパスを使用します。
- ボリュームごとに最大4、995個のqtreeがサポートされます。クォータの監視と適用（ONTAP 9.5以降でのFlexGroup ボリュームの適用）は、qtreeレベルまたはユーザレベルで適用できます。

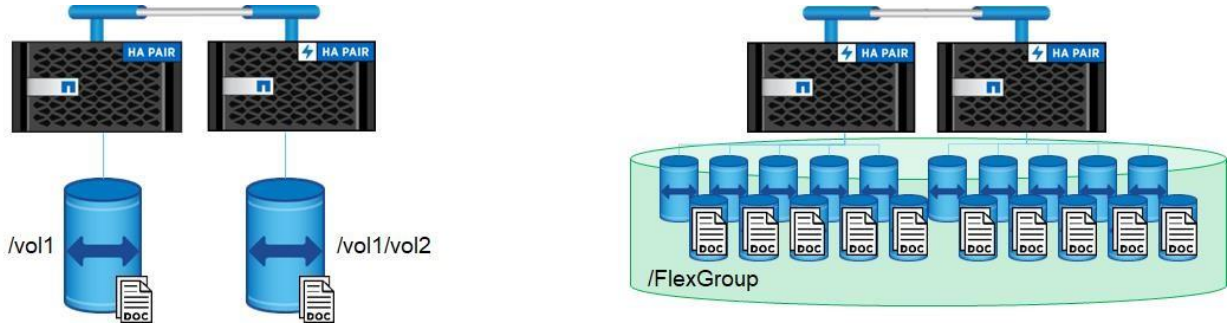
FlexGroupボリューム

FlexGroup では、FlexVol ボリュームの概念を採用し、複数のFlexVol ボリュームをグループ化して1つのコンテナとしてクライアントに提供することで、クラスタ内のノード全体にボリュームを拡張しました。100TB以上20億個のファイルを含むこの拡張された制限に加え、提供されている単一のFlexVol ボリューム上のリソースでボトルネックとなる可能性があるワークロードのパフォーマンス面でのメリットも追加されました。

FlexGroupボリュームを使用した場合、ストレージ管理者は、大規模な単一のネームスペースをほんの数秒で簡単にプロビジョニングできます。FlexVolとは異なり、FlexGroupボリュームには、ハードウェアの物理的制限またはONTAPの合計ボリューム制限を超える容量またはファイル数の制約は、ほとんどありません。制限は、負荷を動的に分散し、すべてのメンバーに均等にスペースを割り当てるためにコラボレーションで機能する、コンスティチュエントメンバーボリュームの全体的な数によって決まります。FlexGroupボリュームではメンテナンスや管理の手間も必要ありません。単にFlexGroupボリュームを作成してNASクライアントと共有するだけで、面倒な処理はONTAPが行います。

図5 は、FlexVol ボリュームとFlexGroup ボリュームのアーキテクチャを比較したものです。

図5）FlexVol とFlexGroup のアーキテクチャの比較



NetApp FlexGroup ：ネットアップのワークロードを強化

ソフトウェア機能の本当のテストの1つは、これです。ソフトウェアの作成者は独自の機能を使用していますか？

この質問の回答は、「はい」と響きます。ネットアップでは、独自の開発環境、NetApp Active IQ データレイク、およびその他多数のワークロードユースケースでFlexGroup ボリュームを活用しています。

ネットアップによるActive IQ でのFlexGroup ボリュームの使用方法の詳細については、次のリソースを参照してください。

- ONTAP FlexGroupテクノロジによって、ネットアップの大規模なActive IQデータ レイクを強化
- Tech OnTap ポッドキャストのエピソード182：ネットアップのポッドキャスト「FlexGroup and Active IQ

ボリューム形式の選択：FlexGroup かFlexVol か？

NFSワークロードで使用するボリュームを導入する際には、次の2つのボリューム形式を選択できます。

- **FlexVol ボリューム**は、ONTAP で使用できる標準的なボリュームタイプで、単一ノードのハードウェアにまたがります。
- **FlexGroup ボリュームは**、クラスタ内の複数のハードウェアドメインにまたがる複数のFlexVol メンバーボリュームで構成されるボリュームで、FlexVol よりも次のような利点があります。
  - 100TBを超えるボリュームサイズ（テストで使用した20PBまで）。
  - ファイル数は20億を超えています（テスト数は4、000億個）。
  - 取り込み負荷の高いワークロードに対して2~6倍のパフォーマンスを提供するマルチスレッドメタデータ処理
  - クラスタ内の複数のノードを使用してワークロードを自動的に分散できる。
  - 使いやすいようにプログラム可能なFlexVol-like。
  - ボリュームの容量が上限に達したときにシステムを停止することなく拡張

ほとんどのNFSワークロードでは、FlexGroup ボリュームはFlexVol よりも多くの利点をもたらします。ここで注意が必要なのは、ボリューム形式間の機能のパリティをチェックして、環境内の必要な機能がサポートされているかどうかを確認することです。導入と意思決定ポイントの詳細については、TR-4571：『NetApp FlexGroup Volumes Best Practices and Implementation』を参照してください。FlexGroup

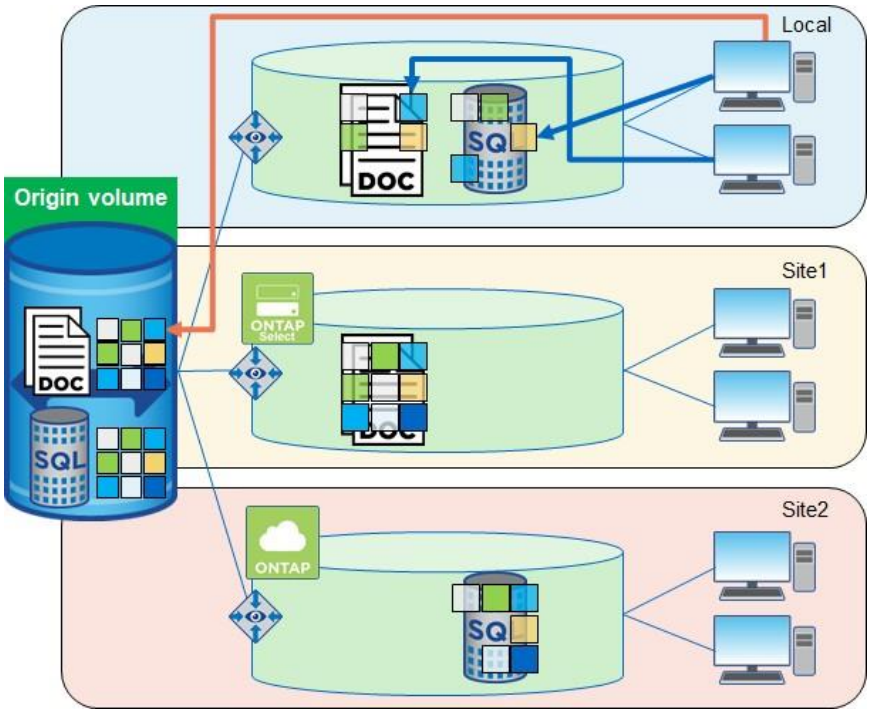
NetApp FlexCacheボリューム

ONTAP のNetApp FlexCache ®テクノロジは、整合性があり、一貫性があり、最新であるボリュームの書き込み可能な永続的キャッシュをリモートサイトに提供します。

キャッシュは、ホストとデータソースの間にある一時的な格納場所です。キャッシュの目的は、ソースデータから頻繁にアクセスされる部分を、ソースデータからデータを取得する場合よりも早く提供できるようにすることです。キャッシュは、データへのアクセスが複数回行われ、複数のホストで共有される、読み取り負荷の高い環境で最も効果的です。

図6 に、NetApp FlexCache ボリュームを示します。

図6）NetApp FlexCacheボリューム



キャッシュは、次の2つの方法のいずれかで高速にデータを提供できます。

- キャッシュシステムは、データソースのあるシステムよりも高速です。具体的には、高速なストレージ（HDDとはソリッドステートドライブ（SSD））、処理能力の向上、キャッシュを提供するプラットフォーム内のメモリの増加（または高速化）などです。
- キャッシュ用のストレージスペースはホストに物理的に近いため、データへのアクセスに時間がかかりません。

キャッシュはさまざまなアーキテクチャ、ポリシー、セマンティクスを使用して実装され、データの整合性はキャッシュに格納されてホストに提供される時点で保護されます。

FlexCache Backupには、次のようなメリットがあります。

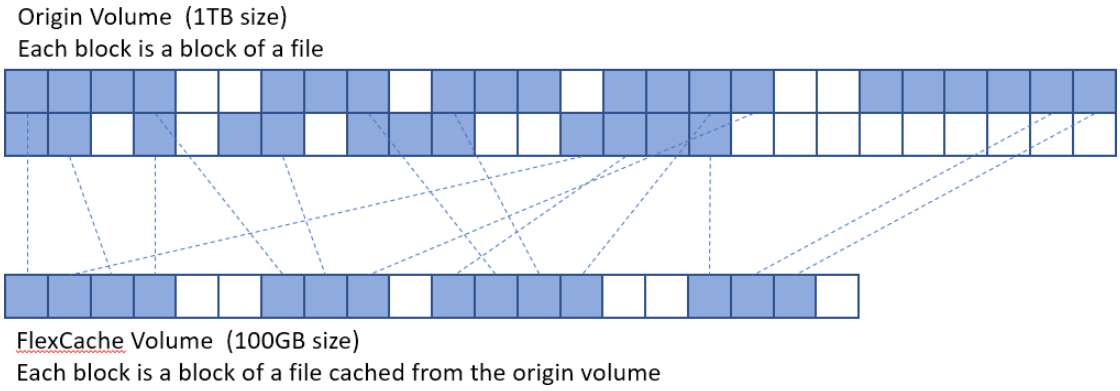
- 負荷分散によりパフォーマンスが向上します
- クライアントアクセスポイントの近くにデータを配置することでレイテンシを低減
- ネットワーク切断時にキャッシュデータを提供することで可用性を向上

FlexCache テクノロジは、キャッシュの一貫性、データの整合性、データの金銭的価値、ストレージの効率的な使用を維持しながら、上記のメリットをすべて実現します。拡張性とパフォーマンスに優れた方法でストレージを使用できます。

FlexCache ボリュームはスパースコンテナであり、送信元データセットのすべてのファイルがキャッシュされるわけではありません。キャッシュされたinodeのすべてのデータブロックがキャッシュに存在するわけではありません。作業データセット（最近使用されたデータ）の保持期間を優先することで、ストレージが効率的に使用されます。図7 はスパースボリュームの詳細を示しています。

FlexCache テクノロジを使用する場合、ディザスタリカバリなどの企業データ戦略の管理は、オリジンにのみ実装する必要があります。データ管理はソースのみが対象であるため、FlexCache テクノロジを使用すると、リソースをより効率的に使用できるようになり、データ管理やディザスタリカバリ戦略がよりシンプルになります。EDAワークロードの場合、SemiWikiでは、FlexCache ボリュームが地理的に分散した設計チームに、Concurrency and Collaborationで作業データセットの現在のキャッシュとの同期をどのように提供するかについて説明します。分散した設計チームをネットアップと同期させます。

図7）スパースボリュームの詳細



ユースケース

FlexCache in ONTAPは、特定のユースケースに最も適した設計となっており、そのユースケースに適したユースケースが記載されています。FlexCache ボリュームは他のユースケースも可能ですが、メリットは完全には検証されていません。ほとんどの場合、ユースケースはサポートされている機能セットを対象としたものです。非理想的なユースケースは推奨されませんが、FlexCache のメリットと非理想的なユースケースに関連するコストを比較する必要があります。

理想的なユースケース

FlexCacheはライトアラウンドモデルに限定されているため、大量の読み取りワークロードに対してはパフォーマンスが向上します。書き込みでレイテンシが発生し、書き込みの数が少ない場合でもレイテンシはデータセットにアクセスするアプリケーションの全体的なパフォーマンスには影響しません。たとえば、次のようなものがありますが、これらに限定されません。

- EDA（電子設計自動化）
- メディアのレンダリング
- 人工知能（AI）、機械学習（ML）、ディープ ラーニング（DL）のワークロード
- ホーム ディレクトリなどの非構造化NASデータ
- ソフトウェアのビルド / テスト環境（GITなど）
- 共通のツール配布
- ホットボリュームによるパフォーマンスの調整
- クラウドバースト、高速化、キャッシング
- NetApp MetroCluster™ 構成全体でのNASボリュームの拡張

ネットワーク アクセス

中央集中型ストレージ解決策 と同様に、ネットワークはエンドユーザに優れたエクスペリエンスを提供するための重要な要素です。このセクションでは、ONTAP におけるネットワークの概念のほか、DNSなどのNAS環境に不可欠なネットワーク隣接の概念について説明します。

データ LIF

ONTAPは、データLIFを通じてクライアントにIPアドレスを提供します。これらは物理ネットワークポートに配置された仮想IPアドレスであり、ノードまたはポートに障害が発生した場合に他のネットワークポートに自動的に移行されます。ノードのメンテナンスを実行し、クラスタからノードを退避する必要がある場合は、手動で移行できます。または、LIFのホームポートを変更するだけです。

データLIFは、基盤となるポートとしてifgrpまたはVLANを使用し、クライアントがネットワークに接続されているポートにのみフェイルオーバーするように設定できます。

ONTAP のデータLIFの詳細については、「LIFの設定」を参照してください。

NAS環境でのデータLIFに関する考慮事項

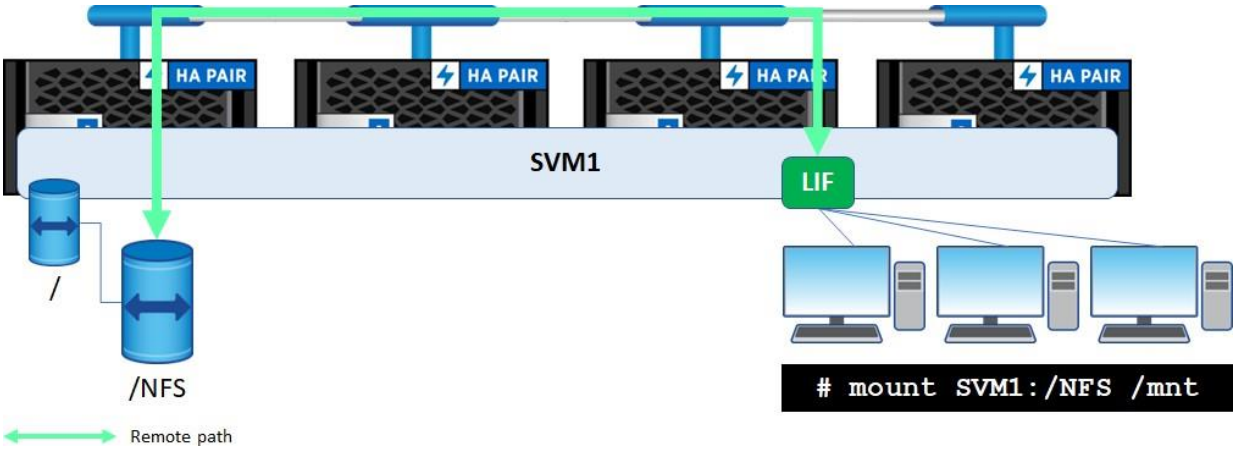
データLIFは、有効なブロードキャスト ドメインに追加された、クラスタ内の任意のポートに配置できます。データLIFはSVM対応のルーティング メカニズムで設定されるため、有効なデータLIFがクラスタ内のどこにあるかにかかわらず、SVM内のイーサネット トラフィックは正しく転送されます。NASインタラクション用のネットワークを設計する場合、2つのアプローチのいずれかを実行できます。

オプション1：簡易性のアプローチ- SVMごとに1つのLIFを使用

基本的に、ONTAP 内のNASデータへのアクセスに必要なのは、ネットワーククライアントにルーティング可能な単一のネットワークIPアドレスです。多くの環境では、NASワークロードには単一のネットワークインターフェイスで十分です。基盤となる物理ネットワークポートに障害が発生した場合や、HAパートナーにストレージノードがテイクオーバーされた場合は、ネットワークIPアドレスがクラスタ内の別の作業ポートに移行します。単一のネットワークインターフェイスを使用すると、必要なIPアドレスの数は減りますが、ワークロードに使用できるネットワーク帯域幅の量も制限されます。クラスタ内の1つのノードにすべてのNASトラフィックを送信すると、使用可能なリソース（CPUやRAMなど）の数も制限されるため、高いスループットが必要なワークロードや、数百から数千のクライアントに接続する必要があると予想される場合は、オプション#2を使用することを推奨します。

図8 は、単一のLIFとNASの連動を示しています。

図8）単一のLIFを使用したNASインターフェイス



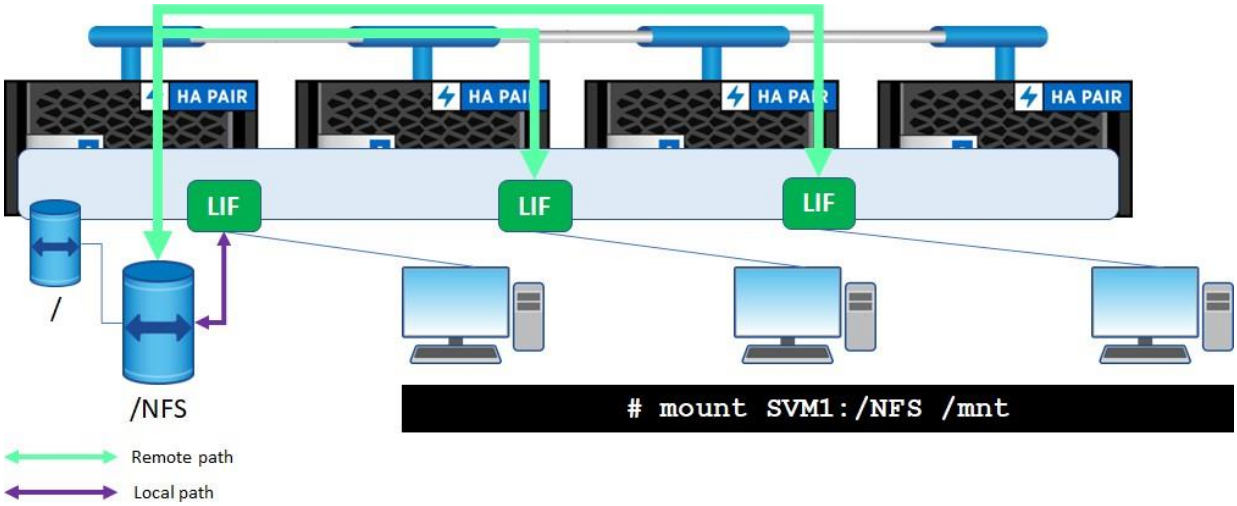
オプション2：パフォーマンスアプローチ- SVMごとに複数のデータLIFを使用する

ONTAP クラスタでは、複数のノードをNAS接続およびストレージで使用できます。NASを使用するONTAP クラスタでは、最大24ノードまでしかスケールアップできないことに注意してください。ノードが複数あると、CPU / RAM /ネットワークインターフェイスなどの物理リソースが複数存在することになります。そのため、SVMに複数のデータLIFがあると、NASワークロードのパフォーマンスが大幅に向上する可能性があります。ノード間でネットワーク接続を分散すると、CPUおよびネットワークポートの競合が軽減されるだけでなく、ノードのTCP接続数が多すぎる場合のシナリオも回避されます。NAS接続、ラウンドロビンDNS、内蔵DNS、または標準のロードバランシングハードウェアのネットワーク負荷分散に利用できます。内蔵DNSとその設定方法 の詳細については、TR-4523『DNS Load Balancing in ONTAP』を参照してください。

最大限のパフォーマンスが必要な場合や、多数のクライアントが同時にNASデバイスにアクセスする場合は、SVMごとに複数のデータLIFを作成するのが効果的です。また、NFSリファーラル、CIFSオートロケーション、pNFSなどのロードバランシングNAS機能を使用するには、データが存在する各ノードにデータLIFが必要です。

図9 は、複数のLIFがNASに通信している状況を示してい

図9）複数のLIFを使用したNASインターフェイス



データLIFの局所性に関する推奨事項

データ局所性機能（NFSリファーラル、CIFSオートロケーション、pNFSなど）を利用して、クラスタ内でのボリュームの場所にかかわらずNFSトラフィックのデータ局所性を実現できます。NFSリファーラルとCIFSオートロケーションの場合、最初のTCP接続は、要求されたボリュームに対してローカルなネットワークインターフェイスに自動的にリダイレクトされます。使用しているボリュームがFlexGroup ボリュームである場合は、NFSリファーラルとCIFSオートロケーションを使用しないでください。

pNFSでは、最初のマウント要求でメタデータパスが提供されますが、読み取りと書き込みはすべてpNFSレイアウト呼び出しによってローカルボリュームに自動的にリダイレクトされます。pNFSは、NFSv4.1プロトコルに対してのみ使用でき、pNFSをサポートするNFSクライアントに対してのみ使用できます。pNFSの詳細については、TR-4067：『NFS Best Practice and Implementation Guide』を参照してください。

オートロケーション機能がない場合、データLIFのローカリティを管理してクラスタネットワークを回避すると、ほとんどのNASワークロードのパフォーマンスへの影響がごくわずかであるため、管理が複雑になり、作業にはそれほど時間をかけないかもしれません。NAS接続はボリュームに対してローカルなデータLIFに接続するのが理想的ですが、FlexGroup ボリューム/スケールアウトNASおよび大規模なクラスタバックエンドネットワークでは、この方法の方が重要性は低くなります。

データローカリティのメリットと考慮事項

このセクションでは、ONTAP におけるデータローカリティのメリットと考慮事項について説明し、これらの概念にシンプルなアプローチを念頭に置いて説明します。

- **ノード間で負荷を分散し、クラスタ内の利用可能なすべてのハードウェアを活用できる。**ボリュームとネットワークインターフェイスを作成する場合は、クラスタ内の複数のノードにワークロードを導入して、パフォーマンスヘッドルームを最大化することを検討してください。使用しないハードウェアはコストの無駄です。

  シンプルなアプローチ： ONTAP では、ONTAP システムマネージャを使用している場合に、ストレージのプロビジョニングを自動化できます。このアプローチでは、使用可能なパフォーマンスヘッドルームが考慮され、利用率が低いノードに新しいボリュームを配置しようとします。さらに、FlexGroup ボリュームは、クラスタ内の複数のノード間でプロビジョニングされ、ワークロードを自動的に1つのネームスペースに分散します。
- **複数のクラスタ ノード間でネットワーク接続を分散できる**クラスタはSVM同様に単一のエンティティです。ただし、その基盤となるハードウェアにはそれぞれ上限があります（接続数など）。

簡易性のアプローチ ：SVMごとに複数のデータLIFを作成し、ONTAP 内蔵DNS機能を使用して、DNSラウンドロビン名またはDNS転送ゾーンの背後にあるインターフェイスをマスクします。さらに、FlexGroup を利用して、複数のノードにワークロードを分散させることもできます。

- **ボリューム移動の際にデータ局所性を実現できる**ボリュームを別のノードに移動する場合に、すべてのノードにSVMのデータLIFがあればデータへのローカル パスを確保できます。ONTAP 内のボリュームを新しいノードに移動しても、NASクライアントに対して既存のTCP接続が維持されます。このため、これらのNAS処理はクラスタネットワークを経由します。

  シンプルなアプローチ：何も行いません。ほとんどの場合、NASクライアントはこれらのNAS共有とのパフォーマンスの違いを認識しません。NFSv4.1では、pNFSの使用を検討します。

NAS導入のためのストレージ ネットワークのベストプラクティス

NAS環境でのネットワークに関する一般的なベストプラクティスを次に示します。

ベストプラクティス1：FlexGroup を使用したネットワーク設計

ONTAP でNAS解決策 を設計する際は、ボリュームの形式に関係なく、次のネットワーク関連のベストプラクティスを考慮してください。

- 各ノードへのパスを確認するために、SVMごとにノードごとに少なくとも1つのデータLIFを作成します。
- 何らかの形のDNSロードバランシングを使用して、単一の完全修飾ドメイン名（FQDN）の背後にあるクライアントに複数のIPアドレスを提供する。DNSロードバランシングの詳細については、TR-4523『ONTAP のDNSロードバランシング』を参照してください。
- 可能な場合は、LACPポートを使用してデータLIFをホストし、スループットとフェイルオーバーを考慮してください。
- クライアントを手動でマウントする場合は、TCP接続をクラスタノード間に均等に分散します。それ以外の場合は、DNSロードバランシングがクライアントTCP接続の分散を処理できるようにします。
- 頻繁にマウントやアンマウントを行うクライアントの場合は、負荷を分散するために内蔵DNSの使用を検討してください。クライアントが頻繁にマウントおよびアンマウントされない場合、内蔵DNSはあまり効果がありません。
- マウントストーム（数百、数千のクライアントが同時にマウントする場合）のようなワークロードでは、外部のDNSロードバランシングを使用するか、NetApp FlexCache ボリュームの使用を検討します。1つのノードへのマウントストームによって、クライアントへのサービス拒否またはパフォーマンスの問題が発生する可能性があります。
- NFSv4.1を使用している場合は、データのローカリゼーションとファイルへの並列接続にpNFSを利用することを検討してください。pNFSは、シーケンシャルI/Oワークロードに最適です。メタデータ比率が高いワークロードは、単一のメタデータサーバ接続時にボトルネックとなる場合があります。
- SMB3ワークロードの場合は、CIFSサーバでマルチチャネルおよび大規模MTU機能を有効にすることを検討してください。
- ネットワークでジャンボフレームを使用している場合は、ネットワークアーキテクチャの各エンドポイントでジャンボフレームが有効になっていることを確認してください。ジャンボフレームの設定が一致していないと、どのボリュームタイプでも診断が難しいパフォーマンスの問題が発生する場合があります。
- NFSクライアントは、複数のネットワークインターフェイスでONTAP 内の同じボリュームに接続された同じクライアントから、複数のマウントポイントを使用することで、パフォーマンスを向上できます。ただし、この設定は複雑になる可能性があります。NFSクライアントでこの機能がサポートされている場合は、TR-4067：『ONTAP』で説明されているnConnectを使用してください。

LACPに関する考慮事項

クライアント側ネットワークでLACPポートを使用すると有効な理由があります。一般的で適切なユースケースは、SMB 1.0プロトコル経由でファイルサーバに接続するクライアントに耐障害性に優れた接続を提供することです。SMB 1.0プロトコルはステートフルであり、OSIスタックの上位レベルでセッション情報を維持するため、LACPはファイルサーバがHA構成の場合に保護を提供します。SMBプロトコルを実装した後は、LACPポートを設定することなく、耐障害性に優れたネットワーク接続を提供できます。詳細については、TR-4100：『Nondisruptive Operations with SMB File Shares』を参照してください。

LACPはスループットと耐障害性にメリットをもたらしますが、LACP環境を維持するという複雑さの検討が必要です。LACPを使用する場合でも、複数のデータLIFを使用する必要があります。

DNSロードバランシングに関する考慮事項

DNSロードバランシング（外部接続とオンボックス接続の両方）を使用して、クラスタ内のノードとポートにネットワーク接続を分散させることができます。最終的に、どのDNSロードバランシング方式を使用するかは、ストレージ管理者とネットワーク管理者の目標によって決定されます。DNSロードバランシング の詳細については、TR-4523：『ONTAP のDNSロードバランシング』を参照してください。

ベストプラクティス2：何らかのDNSロードバランシング形式を使用する

可能な場合は、マルチプロトコルのNAS環境で、何らかの形のDNSロードバランシングを使用してください。

内蔵DNSか外部接続DNSか？

ONTAP には、内蔵DNSサーバを介してDNSクエリにサービスを提供する方法が用意されています。この方法は、ノードのCPUおよびスループットを要因として、NASアクセス要求の処理に最適なデータLIFを判断します。

- 外部DNSは、DNS管理者が複数の「A」ネームレコードを作成する方法で設定します。この名前のレコードは外部DNSサーバ上にあり、データLIFへのラウンドロビンアクセスを提供します。
- マウントストームシナリオを作成するワークロードの場合、ONTAP 内蔵DNSサーバは正常に稼働し、バランスを取ることができないので、オフボックスのDNSを使用することをお勧めします。

ベストプラクティスとして、各SVMのノードごとに少なくとも1つのデータLIFを作成することを推奨します。ただし、データLIFの導入方法を決定するには、「NAS環境でのデータLIFの考慮事項」を参照してください。複数のデータLIFを導入する場合は、DNSロードバランシングを使用して、DNSエイリアスの背後にあるIPアドレスをマスクすることが重要です。DNS名を使用すると、ストレージへのアクセスポイントをわかりやすく覚えやすい名前にできます。複数のデータLIF用のDNSエントリを作成する予定で、Kerberosを利用している場合は、DNS A/AAAAレコードがSVMに割り当てられたKerberos SPNと一致していること、または適切なA/AAAAレコードにリダイレクトする正規名（CNAME）があることを確認してください。そうしないと、Kerberos認証が失敗します。

- 意思決定マトリックスを含む、DNSロードバランシングの詳細については、TR-4523：『ONTAP のDNSロードバランシング』を参照してください。
- NFS Kerberosの詳細およびDNS名がKerberosに与える影響については、TR-4616：『ONTAP におけるNFS Kerberos』を参照してください。

LIFのサービスポリシー

ONTAP 9.6以降 では、ONTAP のネットワークデータインターフェイスのロールの概念に代わる、LIFサービスポリシーが導入されています。LIFポリシーはネットワークインターフェイスに適用または削除できるため、トラフィックを許可または禁止できます。ネットワークインターフェイスを再作成する必要はありません。

インターフェイスに適用されているサービスポリシーを確認するには、次のコマンドを実行します。

```
cluster::*> net int show -vserver DEMO -lif data -fields service-policy
  (network interface show)
vserver lif service-policy
---------- ------ ------------------------
DEMO    data default-data-files
```

LIFサービスポリシーはいくつかのデフォルトポリシーを作成しますが、カスタムポリシーを追加することもできます。これらは、SANトラフィック、NASトラフィック、または管理トラフィックを許可する次のデフォルトポリシーです。1つのデータLIFに一度に割り当てることができるポリシーは1つだけです。

```
cluster::*> network interface service-policy show -vserver DEMO
Vserver   Policy                       Service: Allowed Addresses
--------- ---------------------------- ----------------------------------------------------
DEMO
          default-data-blocks          data-core: 0.0.0.0/0, ::/0
                                       data-iscsi: 0.0.0.0/0, ::/0
                                       data-fpolicy-client: 0.0.0.0/0, ::/0

          default-data-files           data-core: 0.0.0.0/0, ::/0
                                       data-nfs: 0.0.0.0/0, ::/0
                                       data-cifs: 0.0.0.0/0, ::/0
                                       data-flexcache: 0.0.0.0/0, ::/0
                                       data-fpolicy-client: 0.0.0.0/0, ::/0

          default-management           data-core: 0.0.0.0/0, ::/0
                                       management-ssh: 0.0.0.0/0, ::/0
                                       management-https: 0.0.0.0/0, ::/0
                                       data-fpolicy-client: 0.0.0.0/0, ::/0
```

NFSのみまたはCIFS `network interface service-policy createnetwork interface service-policy add-service network interface service-policy remove-service`/ SMBのみを許可するポリシーを作成する場合は、またはを使用してサービスを追加または削除できます。すべて停止なしで実行できます。

マルチプロトコルNASの場合は、default-data-filesポリシーを使用します。

詳細については、ONTAP 9.6以降のLIFとサービスポリシーを参照してください。

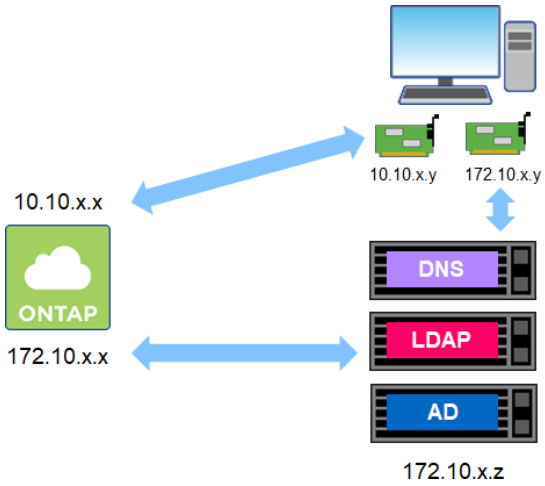
ネームサービスへの接続

マルチプロトコルNASを実装する場合、ネームサービスは解決策 の機能に大きな影響を与えます。そのため、ONTAP SVMのネットワークインターフェイスを使用するには、ネームサービスサーバへのネットワークアクセスが必要です。NASクライアントが、ストレージとネームサービスへの接続を分離した複数のインターフェイスを使用してセグメント化されたネットワークに配置されている場合があります。データLIFまたはネームサービス接続専用の管理LIFを指定できます。

たとえば、クラウドでONTAP ストレージをホストし、NASクライアントとドメインサービスをすべてオンプレミスに配置する場合などです。その場合は、NASクライアントとネームサービスの両方にネットワークアクセスを提供する必要があります。

図10は、セグメント化されたネットワーク内のNASクライアントを示しています。

図10）セグメント化されたネットワーク内のNASクライアント



次の例では、ONTAP へのネームサービスの接続が必要です。

- Active Directory（CIFS / SMB接続とユーザ検索用）
- LDAP（UNIXユーザおよびグループのIDとネットグループ用）
- DNS（ドメインサービスの場合）

注： NFS Kerberosでは、ネームサービスへのアクセスは必要ありません。詳細については、TR-4616：『ONTAP におけるNFS Kerberos』を参照してください。

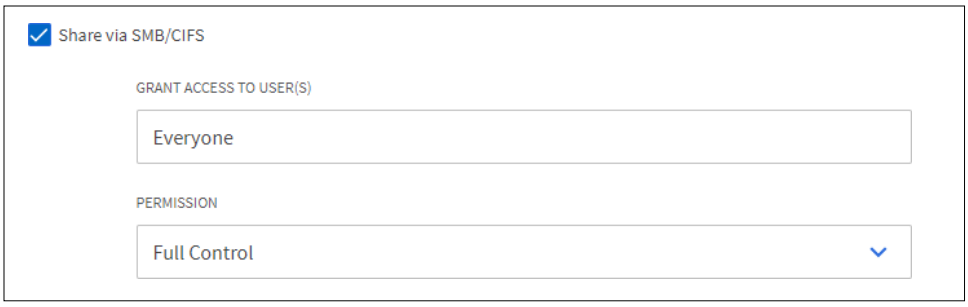
アクセスポイント：ボリューム、共有、エクスポート

ONTAP でボリュームをプロビジョニングすると、使用可能な容量の一部を切り分けることができます。ボリュームがネームスペースにマウントされ、エクスポートポリシーや共有が作成されて、NASクライアントがNFSまたはCIFS / SMB経由でボリュームにアクセスできるようになるまでではありません。このセクションでは、NASクライアントにストレージを提供する際に考慮すべき点をいくつか説明します。

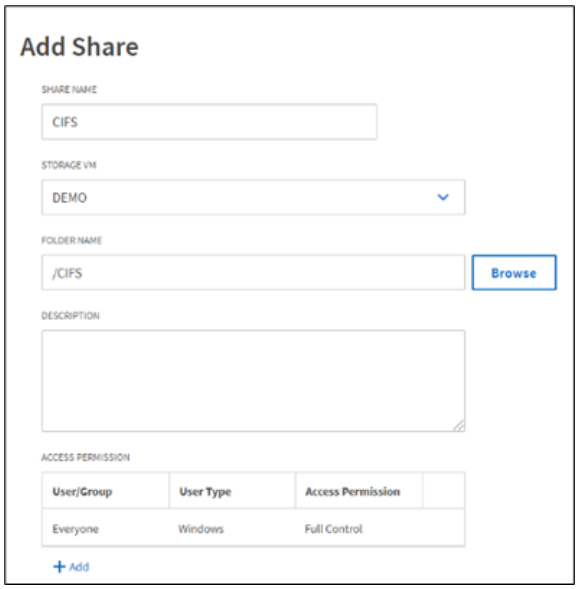
CIFS/SMB共有

CIFSプロトコルを使用してONTAP のボリュームにアクセスするには、そのボリュームの適切なジャンクションパス用にCIFS共有を作成します。この作業は、ONTAP System Managerでのボリュームの初期作成時、またはCLIやSystem Managerでの初期ボリュームの作成時に実行できます。

1. ボリュームの作成中にCIFS共有を作成するには、SMB / CIFSで共有オプションを選択します。



2. ボリュームの作成後にCIFSを作成するには'[ストレージ]→[共有]→[追加]をクリックします



CIFS共有プロパティ

CIFS共有を作成するときに、アプリケーションの要件に応じて、共有に異なるプロパティを割り当てることができます。また、不要になったプロパティを削除することもできます。

共有の作成時に共有プロパティを指定しなかった場合、デフォルトでは次のプロパティが適用されます。

```
oplocks
browsable
changenotify
show-previous-versions
```

注 `Changenotify`：特にFlexGroup ボリュームを使用している場合、ファイル数の多い環境で原因 のパフォーマンスに問題が生じることがあります。詳細については、TR-4571：『NetApp ONTAP FlexGroupボリューム』を参照してください。

その他の使用可能な共有プロパティは次のとおりです。

```
    showsnapshot              attributecache           continuously-available
    branchcache               access-based-enumeration namespace-caching
    encrypt-data
```

これらのプロパティについては、vserver cifs share properties add productドキュメントで説明しています。

CIFS共有ACL

CIFS / SMB共有にアクセスできるユーザとアクセスできないユーザを制御するには、ONTAP で共有権限を割り当てます。この機能では、既存のCIFSサーバを利用してActive Directory内のユーザとグループを検索し、ACLを適切に変換します。共有権限は、共有へのアクセス時にユーザまたはグループに許可するアクセスのレベルを制御しますが、ファイルおよびフォルダの権限によって上書きされます。たとえば、user1がDocumentsという共有に対するフルコントロールを持ち、実際のフォルダ権限に読み取り専用アクセス権限が割り当てられている場合、user1は共有に対する読み取りアクセスのみを持ちます。

ONTAP で共有レベルの権限`cifs share access-control` を割り当てるには、ONTAP システムマネージャ、コマンドライン（）、またはWindowsクライアント（共有プロパティまたはMMC）を使用します。

マルチプロトコルのNAS環境では、Windows共有権限を利用するのはCIFS / SMBクライアントだけです。NFSクライアントは、共有への最初のアクセスにNFSエクスポートを使用します。CIFS / SMBエクスポートポリシーは、ONTAPでも設定できます。詳細については、「CIFS/SMBクライアントおよびエクスポートポリシー」を参照してください。

注： NFSクライアントとCIFS / SMBクライアントでは、ファイルレベルとフォルダレベルの両方の権限がサポートされます。

CIFS / SMBクライアントとエクスポートポリシー

デフォルトでは、ONTAPはCIFS共有を使用してCIFS / SMBクライアントのアクセスを制御します。ただし、ユーザとグループではなくクライアントホスト名/ IPアドレス/サブネットによってアクセスを制御する場合は、CIFS共有に対してエクスポートポリシーの使用を有効にすることができます。

その方法については、を参照してください。SMBアクセスでのエクスポートポリシーの使用方法。

NFS エクスポート

ONTAP 内のボリュームは、クライアントまたはクライアントのセットからアクセスできるパスをエクスポートすることによって、NFSクライアントに共有されます。ボリュームがSVMのネームスペースにマウントされると、ファイルハンドルが作成され、マウントコマンドで要求されたときにNFSクライアントに提供されます。これらのエクスポートに対する権限は、ストレージ管理者が設定可能なエクスポートポリシーとルールによって定義されます。

エクスポート ポリシーとルールの概念

ONTAP では、セキュリティを制御するエクスポートポリシールールのコンテナとしてエクスポートポリシーを提供しています。エクスポート ポリシーはレプリケートされたデータベースに格納されるため、単一のノードに限定されるのではなく、クラスタ内のすべてのノードでエクスポートを利用できます。

これらのボリュームへのNFSアクセスを提供または制限するために、エクスポートポリシールールが作成されます。これらのルールでは、読み取り、書き込み、およびルートアクセスを定義したり、クライアントリストを指定したりできます。1つのポリシーに複数のルールを定義でき、1つのルールに複数のクライアントを含めることができます。

デフォルトのエクスポート ポリシーの保護

新しく作成したSVMには、defaultというエクスポートポリシーが含まれます。このエクスポート ポリシーは、名前変更や修正はできますが、削除はできません。NFSサーバを作成すると、デフォルトのポリシーが自動的に作成され、vsrootボリュームに適用されます。ただし、このデフォルトポリシーにはエクスポートルールがないため、デフォルトのエクスポートポリシーを使用するボリュームへのアクセスは、ルールが追加されるまでマウントできません。新しいボリュームを作成する際、エクスポートポリシーを定義しない場合、vsrootボリュームのエクスポートポリシーが継承されます。

Vsrootとボリュームのトラバーサル

エクスポート ポリシー ルールはデフォルトで継承されるため、ルールを割り当てるときには、SVMのルート ボリューム（vsroot）へのアクセスをすべて許可することを推奨します。vsrootへの読み取りアクセスを制限するデフォルトのエクスポートポリシーにルールを設定すると、そのSVMの下に作成されたボリュームを対象にトラバーサルすることは拒否され、原因 マウントが失敗します。これは、vsrootが「/junction」へのパスの「/」にあたり、マウントおよびトラバースの可否を左右するためです。

qtreeエクスポート

ONTAP では、ボリュームおよび基盤となるqtreeのエクスポートポリシーとルールを設定できます。これにより、ONTAP でストレージ管理ディレクトリへのクライアントアクセスを制限したり許可したりできます。これにより、ストレージ管理者は、ホームディレクトリなどのワークロードをより簡単に管理できます。

デフォルトで、qtreeは親ボリュームのエクスポートポリシーを継承します。ONTAP System Managerでqtreeを作成する際 – `export-policy` には、エクスポートポリシーとエクスポートルールを明示的に選択または作成できます（図11）。CLIオプションを使用することもできます。

図11）qtreeエクスポートの仕様-ONTAP システムマネージャ

vsrootへのアクセス制御

vsrootへの読み取り / 書き込みアクセスを制御するには、ボリュームのUNIX権限、ACL、またはその両方を使用します。ボリュームの所有者でないユーザには、vsrootへの書き込み権限を制限することを推奨します（最高でも0755）。

ボリュームが作成されると、特に指定がないかぎり、次の値がデフォルト値になります。

- 0755は、ボリュームに設定されるデフォルトのUNIXセキュリティです。

- デフォルトの所有者はUID 0、デフォルト グループはGID 1です。

vsrootをトラバースして、「/」をマウントするNFSクライアントへの読み取り/リストアクセスを防止するには、2つの方法があります。

オプション1：vsrootのUNIXモードビットをロックダウンします

vsrootをユーザにロックダウンする最も簡単な方法は、クラスタから所有権と権限を管理することです。

1. SVM固有のローカルUNIXユーザを作成します。たとえば、このUNIXユーザはSVM自体と同じ名前にすることができます。
2. vsrootボリュームを新しいUNIXユーザに設定します。ほとんどのNFSクライアントにはrootユーザが設定されています。つまり、デフォルトでは、vsrootボリュームへのアクセスがrootユーザに過剰に設定されている可能性があります。
3. グループなどをトラバース権限のみに制限するUNIX権限を使用し、ボリューム所有者に必要な権限（0611など）は残します。

オプション2：NFSv4.xまたはNTFS ACLを使用してvsrootをロックダウンします

vsrootをロックダウンするもう1つの方法は、ACLを利用して、一部のユーザまたはグループを除き、すべてのユーザにトラバースする権限を制限することです。そのためには、NFSv4.x ACLを使用するか（NFSv3を使用してマウントする場合も含む）、またはCIFS / SMBプロトコルを提供する環境でNTFS権限を使用します。NFSv3マウントでのNFSv4.x ACL の使用については、TR-4067を参照してください。

エクスポートポリシールール：オプション

エクスポートポリシールールでは、複数の設定オプションを使用できます。エクスポートポリシールールのほとんど `export-policy rule show` のオプションは、コマンドを使用するか、ONTAP System Managerを使用して表示できます。

エクスポートポリシールールのオプションについては、製品ドキュメントを参照してください。ただし、次のエクスポートポリシールールオプションは、マルチプロトコルNAS機能に固有のオプションです。

プロトコル

このポリシーを使用して、アクセスを許可するプロトコルを制御します。指定できるプロトコルは、any、nfs、nfs3、NFS4、およびcifsです。

（-ntfs-unix-security-ops）

このポリシーを使用して、NFSクライアントからの権限の変更をNTFSセキュリティ形式のボリュームでどのように処理するかを制御します。オプションは、Fail（権限の変更がエラーで失敗）またはIgnore（権限の変更がサイレントに失敗する）です。

（-allow-dev）

このポリシーを使用して、デバイスファイルの作成/削除を制御します。ただし、マルチプロトコルのNASでは、デバイスファイルを作成/削除できるのはNFSクライアントのみです。詳細については、バグ337385を参照してください。

エクスポートポリシールール：継承

ONTAP では、エクスポートポリシールールは適用先のボリュームとqtreeにのみ影響します。たとえば、SVMルート ボリュームに、ルート アクセスを特定のクライアントまたはクライアントのサブセットに限定する制限的なエクスポート ポリシー ルールが適用されていたとします。このSVMルート ボリュームの下にあるデータ ボリューム（「/」にマウント）は、そのデータ ボリュームに適用されているエクスポート ポリシーのみに従います。ただし、クライアントへの読み取りアクセスを拒否し、クライアントがそのパス内のボリュームを経由する必要があるエクスポートポリシールールがボリュームに設定されている場合は例外です。現在、ONTAP でのNFSトラバース チェックのバイパスの概念はありません。エクスポートポリシールールの継承の例については、TR-4067を参照してください。

エクスポートポリシールール：インデックス

ONTAP では、ストレージ管理者がエクスポートポリシールールの優先度を設定して、特定の順序でルールが適用されるようにすることができます。ポリシーはアクセスが試みられたときに評価され、ルールは0～999999999の順に読み取られます。

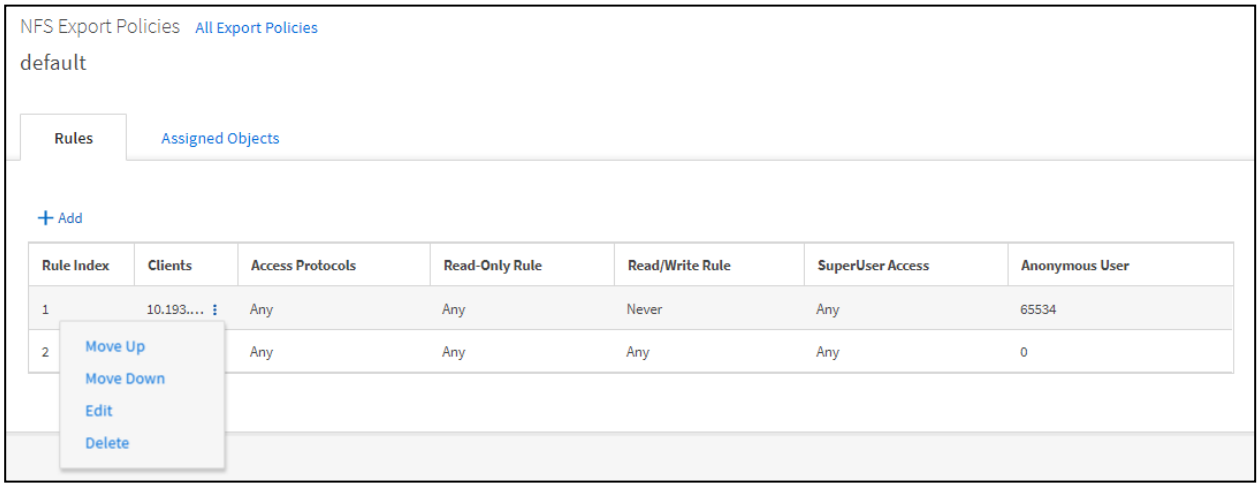
注： ルール インデックスの最大値は999999999ですが、この値の使用は推奨していません。インデックスにはもっと実際的な数値を使用してください。

番号の小さいルール インデックス（1など）が読み取られてあるサブネットにアクセスが許可されたあとに、そのサブネット内のホストが番号の大きなインデックス（99など）のルールによってアクセスを拒否された場合、そのホストはポリシー内で先に読み取られたアクセスを許可するルールに基づいてアクセスを許可されます。

これとは逆に、クライアントがインデックスの番号の小さいエクスポート ポリシー ルールでアクセスを拒否されたあとに、ポリシー内の後続のグローバル エクスポート ポリシー ルール（clientmatch 0.0.0.0/0など）でアクセスを許可された場合、そのクライアントはアクセスを拒否されます。

ポリシールールのルールインデックスの順序をで変更することができます `export-policy rule setindex` コマンドを使用するか、ONTAP System Managerで上へ移動/下へ移動を使用します（図12）。

図12）ONTAP システムマネージャでルールインデックスの再配列



clustered Data ONTAPでクライアントに許可するアクセスと禁止するアクセスを決定する際には、エクスポート ポリシー ルールの順序を検討することが重要です。複数のエクスポート ポリシー ルールを使用する場合は、幅広いクライアントにアクセスを禁止 / 許可するルールによって、同じクライアントにアクセスを禁止 / 許可するルールが上書きされないようにしてください。ルール インデックスはルールが読み取られる順序を決定し、インデックス番号が小さいルールが大きい番号のルールより優先されます。

注： 詳細なルール（管理ホストなどの特定のクライアントなど）を使用する場合は、ルールインデックスの上に配置します。より広範なアクセスルールは、より低く配置する必要があります。たとえば、管理ホストルールはルールインデックス1に、0.0.0.0/0のポリシーはインデックス99になります。

エクスポートポリシールール：Clientmatch

エクスポートポリシールールのclientmatchオプション。ストレージ管理者が、NFSエクスポートをマウントするためのアクセスリストを定義できるほか、クライアントがエクスポートをマウントできる状態になったあとにアクセス権限をハイレベルで制御することもできます。

NFSエクスポートポリシールールClientmatchの有効なエントリは次のとおりです。

- IP アドレス
- ホスト名

- ドメイン
- サブネット
- ネットグループ

注： ONTAP 9.1以降では、1つのルールで複数のIPアドレスまたはホスト名をカンマで区切って定義できます。それぞれに固有のポリシールールを作成する必要はありません。

次の点を考慮する必要があります。

- clientmatchフィールドまたはネットグループでホスト名が使用されている場合、ホスト名をIPアドレスに解決するために、稼働中のDNSサーバまたは手動のホストエントリが必要です。
- ネットグループが使用されている場合は、ホスト名ではなくネットグループを指定していることをONTAP に通知するために、ネットグループの前面に@記号を追加する必要があります。
- 名前解決やネットグループ検索のためにネームサービスに依存している場合は、SVM内に、必要なネームサービスにアクセスできるデータLIFがあることを確認します。

ネームサービス の詳細については、TR-4668：『Name Services Best Practice Guide』を参照してください。

ネットグループ

ネットグループの使用は、多数のホストを一元管理する方法です。エクスポートへのアクセスを制御するには、ホストのリスト全体ではなく、単一のグループ名を追加してください。ホストを追加または削除する必要がある場合は、エクスポートポリシーとルールを管理するのではなく、ネットグループを通じてホストを追加または削除します。

ONTAP では、次の方法で、エクスポートポリシーでのネットグループの使用がサポートされます。

- ローカルファイル
- LDAP
- NIS

NFSでのネットグループの使用については、TR-4067：『NetApp ONTAP』の「Network File System（NFS）」を参照してください。

LDAPを使用 するネットグループの詳細については、TR-4835：『ONTAP でのLDAPの設定方法』を参照してください。

注： マルチプロトコルNASの場合、ネットグループの使用は、エクスポートポリシーおよびルールを使用する場合にのみ適用されます。

セキュリティ形式

CIFS / SMBとNFSでは、ユーザとグループのアクセスに使用する権限モデルが大きく異なります。そのため、ONTAPは、プロトコルアクセスに必要な権限モデルに対応するように設定する必要があります。NFSのみの環境では、UNIXのセキュリティ形式を使用するというシンプルな選択が求められます。

マルチプロトコルNASを使用する場合、作成時にセキュリティ形式を指定しないと、新しく作成したボリュームにSVMルートボリュームのセキュリティ形式が継承されることに注意してください。たとえば、SVMルート（vsroot）ボリュームのセキュリティ形式がNTFSの場合 - `security-style`、オプション（またはONTAP System Managerの同等のフィールド）を使用しないかぎり、新しいボリュームはすべてNTFSセキュリティ形式になります。セキュリティ形式は、ボリュームの作成後にいつでも変更できますが、デフォルトに基づいて誤ったセキュリティ形式を作成すると、アクセスや権限に関する呼び出しを開始するまで問題があることを認識できない場合があります。

NFSとCIFS / SMBが必要な場合は、次の2つの主要な概念に基づいて決定する必要があります。

- ユーザが最も権限を管理するプロトコルはどれですか？
- 目的の権限管理エンドポイントはどれですか？つまり、ユーザにはNFSクライアントまたはWindowsクライアントからアクセス権を管理する機能が必要ですか。それとも両方でしょうか？

ボリュームのセキュリティ形式は本当に権限形式です。

ボリュームとqtreeのセキュリティ形式

ONTAP には、ボリュームとqtreeから選択できる3つのボリュームセキュリティ形式があります。

UNIX

UNIXセキュリティ形式では、基本モードビット（Owner / Group / Everyoneアクセスに標準のRead / Write / Execute権限（0755など）やNFSv4.x ACLなどのUNIX形式の権限が提供されます。POSIXアドレスはサポートされません。

NTFS

NTFSセキュリティ形式では、ACL内のユーザとグループの詳細およびセキュリティ/監査権限が設定された、Windows SMBアクセス権と同じ機能が提供されます。

混在

mixedセキュリティ形式は、UNIXおよびNTFSセキュリティ形式の概念を取得し、最後にACLを変更したプロトコルに基づいて有効な形式として適用します。たとえば、Windows SMBクライアントでmixedセキュリティ形式のボリューム内にあるファイルまたはフォルダの権限を変更すると、そのファイルまたはフォルダはNTFSを有効なセキュリティ形式として使用し、必要なACLを適用します。NFSクライアントがあとで同じファイルまたはフォルダの権限を変更すると、有効なセキュリティ形式はUNIXに変わります。これにより、複数のクライアントが権限を管理でき、この機能を必要とするアプリケーションに最適です。

アプリケーションに直接の要件がないかぎり、セキュリティ形式の混在は推奨されません。

表1に、既存のセキュリティ形式の制限事項を示します。

表1）既存のセキュリティ形式の制限事項

セキュリティ形式	制限事項
UNIX	• Windowsクライアントは、UNIX属性にマッピングするSMB（読み取り/書き込み/実行のみ、特別な権限はなし）を介してのみUNIX権限属性を設定できます。 • NFSv4.x ACLにはGUIやONTAP のCLI管理機能はありません。 • ファイルまたはフォルダにNFSv4.x ACLが設定されている場合、Windows GUIに表示することはできません。
NTFS	• UNIXクライアントは、NFSを使用して属性を設定できません。 • NFSオプション `-ntacl-display-permissive-perms` が無効な場合、ACLを表示するときは概算の権限のみが表示されます（デフォルトは無効）。
混在	• WindowsクライアントとUNIXクライアントの両方が属性を設定できます。 • オブジェクトには一方の形式のACLのみが適用されます。 – UNIX形式のACLを適用すると、NTFS形式のACLが破棄されます。 – NTFS形式のACLを適用すると、UNIX形式のACLが破棄されます。 • ACLの変更に最後に使用されたプロトコルによって、ファイルの有効なセキュリティ形式が決まります。

認証とネームマッピング

NASでの認証とは、ONTAP がユーザが要求するユーザを判別する方法です。この認証により、アクセス権が付与されているかアクセスが拒否されているかに関係なく、ファイルとフォルダへの想定されるアクセス権が確実に提供されます。

ネーム マッピング

ユーザが要求するユーザが決定されると、WindowsとUNIXの権限のセマンティクスが異なるため、ネームマッピングが利用されて、WindowsユーザのIDがUNIXユーザのIDに接続されます。ネームマッピングはユーザレベルでのみ行われ、グループ名はマッピングされません。代わりに、グループメンバーシップは、ネームマッピングの完了後にONTAP によって収集されます。

詳細については、次のリソースを参照してください。

- ネームマッピングの仕組み（NFSガイド）
- ネームマッピングの仕組み（CIFS / SMBガイド）

ネームマッピングは次の順序で行われます。

1. ONTAPは、1：1（対称）のネームマッピングをチェックします。たとえば、UNIXユーザ `netapp` `DOMAIN\netapp`はWindowsユーザにマッピングされます。
2. 1：1のマッピングが存在 `ns-switch database` しない場合は、ネームサービスソースのネームマッピングがネームマッピングの対象となります。デフォルト `vserver name-mapping rule` では、ローカルファイルは（エントリによって）使用されますが、LDAPはネームマップエントリにも使用できます。詳細については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。
3. ユーザにネームマッピングルールが存在しない場合、ONTAPは、CIFS/SMBまたはNFSサーバに設定されたデフォルトユーザ名の使用を試みます。デフォルト `pcuser -default-unix-user`では、CIFS/SMBはデフォルトUNIXユーザとしてを使用します（）。NFSサーバには、デフォルトのWindowsユーザ`-default-win-user`（）が設定されていません。
4. マッピングできるユーザーがない場合、NAS要求は失敗します。

セキュリティ形式に基づくネームマッピング機能

ネームマッピングの方向（WindowsからUNIX、またはUNIXからWindows）は、使用するプロトコル、およびボリュームに適用するセキュリティ形式によって異なります。Windowsクライアントでは、アクセス権の確認にWindowsからUNIXへのネームマッピングが常に必要です。このユーザを適用するかどうかは、セキュリティ形式によって異なります。逆に、NFSクライアントがUNIXからWindowsへのネームマッピングを使用する必要があるのは、NTFSセキュリティ形式が使用されている場合だけです。

表2 は、ネームマッピングの方向とセキュリティ形式をまとめたものです。

表2）ネームマッピングとセキュリティ形式

プロトコル	セキュリティ形式	ネーム マッピングの方向	権限が適用されました
CIFS / SMB	UNIX	Windows から UNIX	UNIX（モードビットまたはNFSv4.x ACL）
CIFS / SMB	NTFS	Windows から UNIX	NTFS ACL（共有へのWindows SIDアクセスに基づく）
CIFS / SMB	混在	Windows から UNIX	有効なセキュリティ形式によって異なります
NFSv3	UNIX	なし	UNIX（モードビットまたはNFSv4.x ACL *）
NFSv4.x	UNIX	UNIXユーザ名の数値ID	UNIX（モードビットまたはNFSv4.x ACL）
NFS	NTFS	UNIX から Windows	NTFS ACL（マッピングされたWindowsユーザSIDに基づく）
NFS	混在	有効なセキュリティ形式によって異なります	有効なセキュリティ形式によって異なります

* NFSv4.x ACLを適用するには、NFSv4.x管理クライアントを使用し、NFSv3クライアントも使用する必要があります。

ローカルファイル

ONTAP SVMには、ローカルファイルを含む独自の一意のネームサービス設定を含めることができます。ONTAP のローカルファイルはファイルではなく、各ノードにコピーがあるレプリケートされたデータベースのエントリです。ノードで障害が発生しても、クラスタ内の他のノードが構成内容を把握しているため、クラスタは通常の運用を継続します。

ONTAP では、ローカルファイルを次の目的に使用できます。

- UNIXユーザおよびグループ
- ネーム マッピング
- ネットグループ
- DNS/hostのエントリ

外部ネームサービスとは異なり、ローカルファイルエントリには許可されるエントリ数に制限があります。ONTAP SVMは、デフォルトではローカルUNIXユーザおよびグループに対して最大64,000エントリをサポートします。

ローカルファイルがプライマリネームサービスであり、64,000を超えるエントリが必要な場合は、拡張/ファイル専用モードを有効にすることをお勧めします。

条件

次のセクション（表3）では、ONTAP でローカルユーザとローカルグループを使用する場合の制限について説明します。これらの制限はクラスタ全体に適用されます。

表3）clustered Data ONTAPでのローカル ユーザとローカル グループの制限

	ローカルUNIXユーザおよびグループ	Scaled-Mode Users/Groups Groups
ローカルユーザとグループの最大エントリ数	65,536	ユーザ数：400K グループ：15k グループメンバーシップ：3000k SVM：{6}
スケールモードのユーザとグループの最大ファイルサイズ	N/A	passwdファイルのサイズ（ユーザ）：10MB * Group file size：25MB * *グループおよびpasswdファイルのサイズはで上書きできます `-skip-file- size-check` が、より大きいファイルサイズはテストされていません

前述したように、ローカルUNIXユーザおよびグループの制限はクラスタ全体に適用され、これにはSVMが複数あるクラスタも該当します。したがって、クラスタに4つのSVMがある場合は、各SVMの最大ユーザ数の合計がクラスタの最大数になる必要があります。

例：

- SVM1のローカルUNIXユーザ数は2,000
- SVM2のローカルUNIXユーザ数は40,000
- SVM3のローカルUNIXユーザ数は20
- この場合、SVM4で作成できるローカルUNIXユーザ数は23,516となります。

上限を超える数のUNIXユーザまたはグループを作成しようとすると、エラー メッセージが表示されます。

例：

```
cluster::> unix-group create -vserver NAS -name test -id 12345

Error: command failed: Failed to add "test" because the system limit of {limit number}
```

```
       "local unix groups and members" has been reached.
```

スケールモード/ファイル専用モード

ONTAP 9.1以降では、ローカルユーザとローカルグループの拡張モード/ファイルのみのモード機能を使用してdiagレベルのネームサービスオプションを有効にし、次にload-from-uri機能を使用してファイルをクラスタにロードして大容量を提供することにより、ローカルユーザとローカルグループの制限を拡張することができます ユーザおよびグループの数。また、ネームサービスサーバやネットワークなどに外部から依存する必要がなくなるため、拡張モード/ファイル専用モードを使用すると、ネームサービス検索のパフォーマンスが向上します。しかし、ファイル管理の負担がストレージ管理の負担となり、人為的ミスの可能性も高くなるため、このパフォーマンスはネームサービスの管理しやすさを犠牲にしています。さらに、ローカルファイル管理をクラスタ単位で行う必要があるため、複雑さが増します。

ユーザとグループに対してこのオプションを有効にするには、`vserver services name-service unix-user file-only vserver services name-service unix-group file-only` コマンドとコマンドを実行します。

モードを有効にしたら、次のコマンドを実行して、URIからユーザとグループのファイルをロードします。

```
cluster::*> vserver services name-service unix-user load-from-uri
```

注： ユーザが10MBを超えるファイル `-skip-file-size- check` や、グループが25MBのファイルをロードするには、オプションを使用します。

ファイルのみのモードを使用する場合、ユーザとグループに対する個別の操作は許可されません。この構成は、現在のところ、MetroCluster またはSVMディザスタリカバリ（SVM DR）のシナリオではサポートされていません。

ファイル専用モードを使用しても外部ネームサービスは使用できますか。

ファイルのみのモードでは、LDAPまたはNISをネームサービスとして使用することはできません。つまり、ローカルユーザとローカルグループの管理は、（レプリケートされたデータベースエントリではなく）ファイルのみで実行されます。ファイルのみのモードが有効になっている場合は、LDAPおよびNISの検索が正常に機能します。

デフォルトのローカル ユーザ

SVMセットアップまたはSystem Managerを使用してSVMを作成すると、デフォルトのローカルUNIXユーザおよびグループ（およびデフォルトのUIDとGID）が作成されます。

これらのユーザとグループを次に示します。

```
cluster::> vserver services unix-user show -vserver vs0
                 User            User   Group  Full
 Vserver         Name             ID     ID     Name
-------------- --------------- ------ ------ --------------------------------
nfs             nobody          65535  65535  -
nfs             pcuser          65534  65534  -
nfs             root            0      0      -

cluster::> vserver services unix-group show -vserver vs0
Vserver         Name                 ID
-------------- -------------------- ----------
nfs             daemon               1
nfs             nobody               65535
nfs             pcuser               65534
nfs             root                 0
```

注： ファイル専用モードを使用する場合は、クラスタの管理に使用されているファイル内に上記のユーザが存在していることを確認してください。ファイルのみモードを有効にすると、アップロードされたファイルに含まれていない場合、デフォルトのユーザが削除されます。

ローカルユーザへの影響

ファイル専用モードが有効になっている場合、ロードするファイルにユーザが設定されていないと、デフォルトのローカルユーザであるroot、pcuser、nobodyが削除されます。ファイルのみモードを使用する場合は、パスワード/グループファイルにローカルユーザとローカルグループを含めるようにしてください。

ネームサービスと外部のアイデンティティプロバイダ

ネットアップでは、LDAP、NIS、DNSなどの外部ネームサービスやIDプロバイダを使用して、ホスト名とユーザ/グループのIDをNASクライアントおよびONTAP に配信することを推奨しています。このベストプラクティスにより、NAS通信に関係するすべてのエンドポイントが、ユーザの名前、数値ID、メンバーであるグループ、どのIPアドレスがホスト名にマッピングされるかについて合意します。さらに、複数のクライアントやストレージシステムにわたって、数百、数千ものローカルファイルを保持する必要はありません。

また、ネームサービスを集中管理することで、グループからユーザを削除する際に、クライアント間で何度も実行するのではなく、1回だけ実行する必要があります。また、このプロセスにより、システム停止や望ましくないアクセス権限の発生につながる人的ミスも削減されます。

UNIX IDおよびネットグループ用のLDAP の設定については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

許可と許可

ユーザが認証されると、ファイルおよびフォルダへのアクセスは許可によって制御されます。ユーザIDは、グループメンバーシップ情報をキャッシュに入力するために使用されます。ファイルおよびフォルダの権限によって、ユーザが取得するアクセスのレベルが決まります。

アクセス制御エントリとアクセス制御リスト

ONTAP の各ファイルおよびフォルダには、ACLが関連付けられています。これらのACLには、ファイルまたはフォルダに対するユーザとグループのアクセスレベルを決定するAccess Control Entry（ACE；アクセス制御エントリ）が含まれます。各ファイルまたはフォルダには最大1,024個のACEを設定できますが、一般的には、パフォーマンスと管理性を向上させるために、ファイルおよびフォルダに使用するACEの数を減らすことをお勧めします。ファイルおよびフォルダのアクセス権を使用する最善の方法は、グループを使用することです。

ONTAP のファイル権限とフォルダ権限は、Windows権限モデルとUNIX権限モデルで同じ標準ルールに従います。ONTAPは、次の3種類の権限構造をサポートしています。

- NTFS ACL
- NFSv4.x ACL
- UNIXモード ビット

マルチプロトコルNASでは、使用するタイプやアクセスプロトコルに関係なく、これらの権限の構造が使用されます。

使用する権限 の種類は、使用しているセキュリティ形式によって異なります。

ACLと各種セキュリティ形式の連携

ボリュームのセキュリティ セマンティクスは、そのセキュリティ形式とACL（NFSv4またはNTFS）で決まります。

UNIXセキュリティ形式のボリュームの場合：

- NFSv4 ACLとモード ビットが有効です。
- NTFS ACLは有効ではありません。
- Windowsクライアントは属性を設定できません。

NTFSセキュリティ形式のボリュームの場合：

- NFSv4 ACLは有効ではありません。
- NTFS ACLとモード ビットが有効です。

- UNIXクライアントは属性を設定できません。

mixedセキュリティ形式のボリュームの場合：

- NFSv4 ACLとモード ビットが有効です。
- NTFS ACLが有効です。
- WindowsクライアントとUNIXクライアントの両方が属性を設定できます。

一般的なベストプラクティス

このセクションでは、最大限の効果を得るために役立つ、マルチプロトコル環境のさまざまなベストプラクティスについて説明します。

マルチプロトコルのベストプラクティス

ONTAP でマルチプロトコルを使用する場合、ベストプラクティスを活用することで、ストレージ管理者の作業が無限に簡単になります。ストレージシステムは、すでにベストプラクティスに従っている場合、CIFSとNFSの両方を利用してNAS環境にシームレスに統合するように設計されています。

セキュリティ、パフォーマンス、および相互運用性を最適化するには、このセクションで説明するベストプラクティスに従う必要があります。

セキュリティ形式を選択します

ONTAP には、NASファイルシステム用のさまざまなボリュームおよびqtreeのセキュリティ形式が用意されています。一般的な前提として、CIFSとNFSの両方を使用する場合は、mixedセキュリティ形式を使用する必要があると考えられます。ただし、ほとんどの場合、NTFSまたはUNIXセキュリティ形式のボリュームとqtreeを使用することをお勧めします。ただし、アプリケーションベンダーが特定のセキュリティ形式を呼び出す場合や、ユーザが権限を変更するときにボリュームの有効なセキュリティ形式を変更する必要がある場合は、mixedモードの使用を除きます。設計上の考慮事項は、次の質問に基づいて作成する必要があります。

- クライアントの大部分が使用しているオペレーティングシステム/ NASプロトコルはどれですか？
- 権限はどの程度細分化する必要がありますか。
- NASクライアントは、最新かつ最大のプロトコル機能とバージョンをサポートしていますか。

表4を参考に、適切なボリュームとqtreeのセキュリティ形式を選択してください。表では、Xは設計上の考慮事項を表し、最後の2つの列に最終的な結果が表示されます。両方の列を選択した場合は、どちらかを選択できます。つまり、セキュリティ形式の各機能が互いにどの程度重要かに基づいて選択する必要があります。

表4）NASボリュームとqtreeのセキュリティ形式の決定マトリックス

セキュリティ形式	そのほとんどがNFSです	ほとんどがCIFS / SMB	きめ細かなセキュリティの必要性	クライアントが任意のプロトコルからアクセス権を変更できるようにする機能
UNIX	X	-	x（NFSv4.x ACLを使用）	-
NTFS	-	X	X	-
混在	-	-	X	X

注： ボリュームのセキュリティ形式 とその長所と短所については、セキュリティ形式で説明しています。

アイデンティティ管理にLDAPを使用します

使用するネームサービススイッチ（ns-switch）を選択する際にはさまざまなオプションがあります。ローカルファイルとNISは有効なオプションですが、次の理由からLDAPを使用することを推奨します。

- **LDAPは将来のニーズにも対応します。**NFSv4.xに対するサポートが追加されるNFSクライアントが増えるに伴い、クライアントとストレージからアクセスできるユーザとグループの最新のリストを含むNFSv4 IDドメインが必要となり、セキュリティを最適化し、アクセスを定義する際のアクセスを保証する必要があります。WindowsユーザとNFSユーザに1対1のネームマッピングを提供するID管理サーバを導入することで、現在だけでなく今後何年にもわたって、ストレージ管理者の業務を大幅に簡易化することができます。また、マルチプロトコル環境がどうしても大きくなると、ストレージ管理者は、次のようなことを意味します。
- **LDAPは拡張性に優れています。**ローカルUNIXユーザおよびグループには、クラスタあたりのソフトデフォルトの制限値32、768が制限されており、65、536まで拡張できます。ただし、複数のSVMを使用するマルチテナント環境や、この数を超える環境では、クラスタの上限に達し、ユーザを追加できなくなります。NISサーバには制限はありませんが、次のような独自の問題があります。
- **LDAPのセキュリティが向上します。**LDAPは、ストレージシステムがLDAPサーバに接続してユーザ情報を要求する方法という形でセキュリティを提供します。LDAPサーバでは、ONTAP とともに次のバインドレベルを使用できます。
  - 匿名
  - パスワード：
  - SASL
  - Kerberos

  NISでは、どのレベルのセキュリティも提供されません。パスワードは弱く暗号化され、クリアな状態でネットワーク経由で送信されます。標準ポートがないため、NISはファイアウォールに対応できません。クライアントは、使用されているNISサーバが実際にNISサーバであることを確認することができません。

  NIS+では'LDAPの機能に合わせてより安全な暗号化を使用していますが'セットアップは難しいため'管理者がNISを置き換える場合は'NIS+上でLDAPを選択することがよくありますその理由は次のとおりです
- **LDAPの堅牢性が向上しています。**NIS、NIS+、およびローカルファイルは、UID、GID、パスワード、ホームディレクトリなどの基本情報を提供します。ただし、LDAPにはこれらの属性とその他多数の属性があります。LDAPで使用される追加の属性によって、NISよりもLDAPにマルチプロトコル管理がはるかに統合されます。実際に…
- **Microsoft Active DirectoryはLDAPを基盤としています。**デフォルトでは、Microsoft Active Directoryはユーザとグループのエントリに LDAPバックエンドを使用します。ただし、このLDAPデータベースにはUNIX形式の属性が含まれていません。LDAPスキーマがIdentity Management for UNIX（Windows 2003R2以降）、Service for UNIX（Windows 2003以前）、またはCentrifyなどのサードパーティ製LDAPツールを使用して拡張される場合に追加されます。Microsoftはバックエンド解決策 としてLDAPを使用するため、ドメインでCIFSを利用する環境にはLDAPが最適です。

Active DirectoryおよびONTAP とLDAP の併用に関する詳細については、TR-4073：『Secure Unified Authentication』を参照してください。

各プロトコル のベストプラクティスについては、TR-4067：『NFS Best Practices and Implementation Guide』およびTR-4191：『Best Practices Guide for Windows File Services』を参照してください。

ローカルファイルをフェイルセーフとして使用します

まれに、設定されているすべてのLDAPサーバへの接続が失われることがあります。このような場合は、LDAP接続が回復するまで管理者がデータにアクセスできるようにするために、安全性を確保することが重要です。このため、次の例に一致するローカルUNIXユーザおよびグループを作成する必要があります。

```
cluster::> unix-user show -vserver SVM
  (vserver services unix-user show)
                 User             User    Group Full
Vserver          Name             ID      ID      Name
---------------- ---------------- ------- ------- --------------------------------------------------------------------------------
SVM              nobody           65535   65535
SVM              pcuser           65534   65534
SVM              root             0       1
```

```
3 entries were displayed.

cluster::> unix-group show -vserver SVM
  (vserver services unix-group show)
Vserver         Name                 ID
--------------- -------------------- --------------------
SVM             daemon               1
SVM             nobody               65535
SVM             pcuser               65534
SVM             root                 0
4 entries were displayed.
```

注： デフォルトでは、これらのユーザとグループはCIFSのセットアップ時に作成されます。

高度なマルチプロトコルの概念

このセクションでは、ONTAP のマルチプロトコルNASの基本について説明します。マルチプロトコルに固有のNFSサーバオプションおよびCIFSサーバオプション、一般的な問題、トラブルシューティング手順、および対処方法など、より高度なトピックについて説明します。マルチプロトコルNASに関連するSMB / CIFSサーバおよびNFSサーバのオプションの一覧については、次のセクションを参照してください。

- 付録B：NFSサーバオプション
- 付録C：CIFS / SMBサーバオプション

マルチプロトコルの**NAS**ファイルロック

ファイルロックとは、アプリケーションが開いているときにファイルの整合性を維持し、現在ロックされているファイルを開こうとすることを他のクライアントに通知することによって使用中のファイルロックです。NFSでは、ファイルロックメカニズムは使用するNFSのバージョンによって異なります。SMBロックは、使用しているSMBのバージョンに関係なく同じです。

NFSv3ロック

NFSv3は、Network Lock Manager（NLM；ネットワークロックマネージャ）やNetwork Status Monitor（NSM；ネットワークステータスモニタ）などの補助プロトコルを使用して、NFSクライアントとサーバ間のファイルロックを調整します。NLMはロックの確立と解除を支援し、NSMはサーバのリブートをピアに通知します。NFSv3ロックでは、クライアントがリブートすると、サーバはロックを解除する必要があります。サーバのリブート時に、クライアントからサーバに保持されていたロックが通知されます。場合によっては、ロックメカニズムが正常に通信しないために、古いロックがサーバ上に残っているため、手動で解除する必要があります。

NFSv4.xロック

NFSv4.xでは、NFSプロトコルに統合されたリースベースのロックモデルが使用されています。つまり、保守や考慮の補助的なサービスは存在しないということです。すべてのロックはNFSv4.x通信にカプセル化されます。

サーバまたはクライアントのリブート時に、指定した猶予期間中にロックを再確立できない場合、ロックは期限切れになります。ONTAP NFSサーバ `-v4-grace- seconds -v4-lease-seconds`は、オプションとを使用してこのロックタイムアウト時間を制御します。

- `-v4-lease-seconds` クライアントがリースを更新するまでにリースが許可される期間です。デフォルトは30秒 `-v4-grace-seconds`で、最小10秒、最大-1秒の値が設定されています。
- `-v4-grace-seconds` ノードのリブート時（フェイルオーバー/ギブバック時など）にクライアントがONTAPからロックを再要求する時間です。デフォルトは45秒で `-v4-lease-seconds`、値の+1秒と最大90秒の範囲で変更できます。

まれに、lease secondsの値と同様にロックがすぐに解放されないことがあり、その結果、2つのリース期間中にロックが解放されることがあります。たとえば、猶予期間が45秒に設定されている場合、ロックを解除するのに90秒かかることがあります。詳細については、バグ957529を参照してください。

SMBロック

SMBでは、便宜的ロックを使用します。これは、ローカルクライアントでファイルをキャッシュすることでパフォーマンスを向上させる方法です。データをローカルにキャッシュすることで、クライアントがファイルを処理している間、ネットワークトラフィックが軽減されます。クライアントがファイルの処理を完了すると、変更はサーバ上のファイルに適用され、他のユーザが編集できるようにファイルがチェックインされます。ファイルの編集中は、他のユーザが変更を行うことはできず、ファイルのデータ一貫性が保たれます。

便宜的ロック（oplock）には次の4種類があります。

- **バッチ**このoplockは、頻繁に開いて閉じられているファイルに対して使用されます。バッチoplockが使用中の場合、クライアントはクローズ要求の送信を遅延させます。クローズ要求が送信される前にそのファイルで別のオープンが発生した場合、クローズ要求はキャンセルされます。これにより、全体的なパフォーマンスが向上します。
- **レベル1 oplock /排他ロック。**oplockレベル1では、クライアントがファイルをローカルにキャッシュしたとき、サーバにコミットする前にローカルコピーの変更を追跡します。このとき、他のクライアントは変更を行わないという前提が適用されます。これは、Microsoft Officeが~filesを作成する方法と似ています。これにより、クライアントとサーバの間で行われるラウンドトリップの数が減少し、パフォーマンスが向上します。
- **レベル2 oplock：**レベル2のoplockは、クライアントがファイルをロックしたが、ロックを放棄して他のクライアントに読み取り/書き込みアクセスを許可する場合に使用します。レベル2 oplockキャッシュは読み取り専用です。一般に、OneDriveとSharePoint問題はロックされます。
- **oplockをフィルタリングします。**フィルタ便宜的ロックは、ファイルをロックして、書き込みまたは削除のどちらのアクセスに対しても開かないようにします。すべてのクライアントがファイルを共有できる必要があります。フィルタoplockは、レベル2のoplockとは異なります。レベル2のoplockでは、読み取りのためのオープン操作が共有違反なしで実行できます。

ONTAP では、oplockを使用しないようにCIFS / SMB共有を設定できます。oplockを無効にすると効果的なユースケースの1つに、クライアントからストレージへの信頼性の低いネットワーク接続（SMB over WANやNAT経由など）が確立されていて、古いバージョンのSMB（SMB 1.0など）が使用されている状況があります。状況によっては、あるプロセスがファイルに対して排他的なoplockを保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスは、キャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントはoplockを放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われることがあります。oplockの詳細 および管理方法については、oplockのONTAP 9ドキュメントセンターのセクションを参照してください。

注： 最新バージョンのSMBプロトコルには、SMB共有および永続的ファイルハンドルなどのロックに対するネットワークの不安定性による影響を軽減する機能があります。

マルチプロトコルNASロックの動作

マルチプロトコルのNAS環境でファイルロックを使用する場合は、使用しているNASプロトコルに応じた動作の違いに注意してください。

- NASクライアントがSMBの場合、ファイルロックは必須ロックです。
- NASクライアントがNFSの場合、ファイルロックはアドバイザリロックです。

これは何を意味するか

NFSファイルとSMBファイルのロックの違いのため、SMBアプリケーションですでに開いているファイルにNFSクライアントからアクセスすると、エラーになる場合があります。

NFSクライアントがSMBアプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のqtreeボリュームでは、rm、rmdir、mvなどのファイル操作を行うと、NFSアプリケーションがエラーになる場合があります。

- NFSの読み取りと書き込みの処理は、SMBの読み取り拒否および書き込み拒否のオープン モードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的なSMBバイトロックでロックされている場合も、NFSの書き込みの処理はエラーになります。UNIXセキュリティ形式のボリュームでは、NFSのリンク解除および名前変更の処理でSMBのロック状態が無視され、ファイルへのアクセスが許可されます。UNIXセキュリティ形式のボリュームでのその他すべてのNFS処理では、SMBのロック状態が考慮されます。

ロックタイプ

NASロックには、次の種類があります。

- **共有ロック：**共有ロックは、複数のプロセスで同時に使用でき、ファイルに排他ロックがない場合にのみ発行できます。これらのロックは読み取り専用ですが、書き込み（データベースの場合など）に使用できます。
- **排他ロック。**これらのロックはCIFS / SMBの排他的ロックと同じように機能しますが、排他的ロックがある場合にファイルを使用できるプロセスは1つだけです。他のプロセスでファイルがロックされている場合は、そのプロセスが分岐されていない限り、排他ロックを発行することはできません。
- **委譲**委譲ロックはNFSv4.xでのみ使用され、NFSサーバオプションが有効になっていてクライアントがNFSv4.x委譲をサポートしている場合に割り当てられます。委譲を使用すると、クライアントで使用されているファイルにソフトロックを作成して、クライアント側で処理をキャッシュできます。このプロセスは、クライアントとサーバの間で行われる呼び出しの数を減らし、SMB便宜的ロックと同様に、処理のパフォーマンスを向上させるために役立ちます。NFS委譲の詳細については、TR-4067：『NetApp ONTAP』の「Network File System（NFS）」を参照してください。
- **バイト範囲ロック。**バイト範囲ロックでは、ファイル全体をロックするのではなく、ファイルの一部のみがロックされます。
- **便宜的ロック**このロックは、SMBがファイルをロックする標準的な方法です。詳細は、SMB 3013742を参照してください。

  注： NFSロックの動作は、ロックのタイプ、クライアントOSのバージョン、および使用するNFSのバージョンによって異なります。想定される動作を測定するために、環境内でのロックをテストしてください。

ONTAP でのファイルロックの詳細については、製品ドキュメントの「ファイルロックの管理」セクションを参照してください。

NFSクライアント上でロックを手動で確立する

NFSロックをテストするには、クライアントがロックを確立するようにNFSサーバに通知する必要があります。ただし、すべてのアプリケーションがロックを使用するわけではありません。たとえば、「vi」などのアプリケーションはファイルをロックしません。その代わりに、非表示のスワップファイルを同じフォルダに作成し、アプリケーションが閉じられたときにそのファイルへの書き込みをコミットします。古いファイルが削除され、スワップファイルの名前がファイル名に変更されます。

ただし、ロックを手動で確立するユーティリティはあります。たとえば、flockはファイルをロックできます。ファイルのロックを確立するには、次の手順を実行します。

1. を実行 `exec` して数値IDを割り当てます。

```
# exec 4<>v4user_file
```

2. ファイルに共有ロックまたは排他ロックを作成するには、flockを使用します。

```
# flock

Usage:
 flock [options] <file|directory> <command> [command args]
 flock [options] <file|directory> -c <command>
 flock [options] <file descriptor number>

Options:
 -s --shared              get a shared lock
 -x --exclusive           get an exclusive lock (default)
 -u --unlock              remove a lock
 -n --nonblock            fail rather than wait
```

```
 -w --timeout <secs>      wait for a limited amount of time
 -E --conflict-exit-code <number> exit code after conflict or timeout
 -o --close               close file descriptor before running command
 -c --command <command> run a single command string through the shell

 -h, --help     display this help and exit
 -V, --version output version information and exit

# flock -n 4
```

3. ONTAP SVMでロックを確認します。

```
cluster::*> vserver locks show -vserver DEMO

Notice: Using this command can impact system performance. It is recommended
that you specify both the vserver and the volume when issuing this command to
minimize the scope of the command's operation. To abort the command, press Ctrl-C.

Vserver:  DEMO
Volume   Object Path                LIF          Protocol Lock Type    Client
-------- --------------------------- ------------ ---------- --------------- -------------
home     /home/v4user_file           data2        nlm        byte-range 10.x.x.x
                Bytelock Offset(Length): 0 (18446744073709551615)
```

4. ファイルのロックを解除します。

```
# flock -u -n 4
```

ファイルを手動でロックすると、ファイルを開いて操作を編集したり、ファイルロックでストレージフェイルオーバーイベントがどのように処理されるかを確認したりできます。

特殊文字に関する考慮事項

Unicodeのほとんどの一般的なテキスト文字（UTF-8形式でエンコードされている場合）は、3バイト以下のエンコードを使用します。この共通テキストには、中国語、日本語、ドイツ語など、最新のすべての言語が含まれます。しかし、絵文字などの特殊文字が人気 を集めているため、UTF-8文字のサイズの中には3バイトを超えるものがあります。たとえば、トロフィー記号は、UTF-8エンコーディングで4バイト必要な文字です。

特殊文字には、次の文字が含まれますが、これらに限定されません。

- 絵文字
- 音楽シンボル
- 数学記号

FlexGroup ボリュームに特殊文字が書き込まれると、次のような動作が発生します。

```
# mkdir /flexgroup4TB/🏆
mkdir: cannot create directory ‘/flexgroup4TB/\360\237\217\206’: Permission denied
```

上の例 `\360\237\217\206 0xF0 0x9F 0x8F 0x86` では、はUTF-8の16進数で、これはトロフィーのシンボルです。

ONTAP ソフトウェアでは、バグ229629に示されているように、NFSで3バイトを超えるUTF-8サイズがネイティブにサポートされていませんでした。3バイトを超える文字サイズを処理 `bagofbits`するために、ONTAP では、余分なバイトをと呼ばれるオペレーティングシステムの領域に配置しました。これらのビットは、クライアントから要求されるまで格納されていました。クライアントは、rawビットの文字を解釈します。FlexVol テクノロジ `bagofbitsbagofbits`はをサポートし、FlexGroup ボリュームはONTAP 9.2でサポートされるようになりました。

ベストプラクティス3：特殊文字の処理-推奨されるONTAP バージョン

特殊文字を適切に処理するには、ONTAP 9.5以降およびutf8mb4ボリューム言語を使用します。

また、ONTAP に bagofbitsは、処理に関する問題を通知するイベント管理システムメッセージがあります。このメッセージには、問題のファイルIDを特定する方法が含まれます。

```
Message Name: wafl.bagofbits.name
Severity: ERROR

Corrective Action: Use the "volume file show-inode" command with the file ID and volume name
information to find the file path. Access the parent directory from an NFSv3 client and rename
the entry using Unicode characters.

Description: This message occurs when a read directory request from an NFSv4 client is made to a
Unicode-based directory in which directory entries with no NFS alternate name contain non-Unicode
characters.
```

utf8mb4ボリューム言語をサポート

前述したように、特殊文字は、標準でサポートされている3バイトのUTF-8エンコーディングを超える可能性があります。ONTAP bagofbits では、この機能を使用してこれらの文字を使用できます。

inode情報を格納するこの方法は理想的ではありません。そのため、ONTAP 9.5以降では、utf8mb4のボリューム言語サポートが追加されました。ボリュームでこの言語 bagofbitsを使用している場合は、サイズが4バイトの特殊文字がではなく適切に格納されます。

ボリューム言語は、NFSv3クライアントから送信される名前をUnicodeに変換し、オンディスクのUnicode名をNFSv3クライアントで想定されるエンコードに変換するために使用されます。NFSホストでUTF-8以外のエンコーディングを使用するように設定されている従来の状況では、対応するボリューム言語を使用する必要があります。UTF-8は最近ほぼユニバーサルになったため、ボリュームの言語もUTF-8である可能性が高くなります。

NFSv4ではUTF-8を使用する必要があるため、NFSv4ホストでUTF-8以外のエンコードを使用する必要はありません。同様に、CIFSでもUnicodeをネイティブで使用するため、任意のボリューム言語でも機能します。ただし、基本面より上にUnicode名を持つファイルはutf8mb4以外のボリュームでは適切に変換されないため、utf8mb4を使用することを推奨します。

ボリュームの言語は -language、ボリュームの作成時にオプションを使用してのみ設定できます。ボリュームの言語を変換することはできません。新しいボリューム言語のファイルを使用するには、ボリュームを作成し、XCP Migration Toolなどのユーティリティを使用してファイルを移行します。

ベストプラクティス4：UTF-8またはutf8mb4？

ONTAP 9.5以降を実行している場合は、クライアントが言語をサポートできないかぎり、utf8mb4ボリューム言語を使用してファイル名の変換に関する問題を回避することをお勧めします。

qtreeに関する考慮事項

qtreeは、ストレージ管理者が、ボリューム内に存在するONTAPで管理されるフォルダをエンドユーザに提示するための手段であり、次の機能を提供します。

- クォータの監視と適用
- エクスポート ポリシーおよびルールを管理します。
- 独自のセキュリティ形式
- アダプティブQuality of Service（QoS）
- qtree statistics

今後、ONTAP ではqtreeが選択されたデータ管理ポイントとみなされ、機能がさらに強化されていく予定です。

このセクションでは、qtreeを使用する際に考慮すべき点をいくつか紹介します。

qtreeおよびファイル移動

qtreeは、ONTAP 内では一意のファイルシステムとみなされます。NASクライアントの観点からはディレクトリのように見えますが、実際のディレクトリとは動作が異なる場合があります。このシナリオの例は、同じボリューム内のqtree間でファイルを移動する場合です。

- ディレクトリ間でボリューム内でファイルを移動すると、ファイル名は単に新しい名前に変更されます。このプロセスは、同じファイルシステム内での移動であるため、数秒以内に実行されます。
- 2つのqtree間でファイルが移動されると、ファイルは名前を変更するのではなく、新しい場所にコピーされます。この処理にはかなりの時間がかかります。このファイル移動は、qtreeがFlexVol ボリュームとFlexGroup ボリュームのどちらにあるかに関係なく動作します。

qtree IDと名前変更の動作

継承されないエクスポートポリシーをqtreeに適用すると、qtree間の操作にはNFSファイルハンドルが若干変更されます。ONTAP では、NFS処理のqtree IDを検証します。これは、ソースフォルダまたはqtreeと同じボリューム内のqtreeに移動する際のファイルの名前変更や移動などに影響します。
これはセキュリティ機能とみなされるため、ホームディレクトリのシナリオなど、qtree間で不要なアクセスを回避できます。ただし、エクスポートポリシールールと権限を適用するだけで同様の目標を達成できます。

たとえば、同じボリューム内のqtreeに対して移動や名前変更を行うと、アクセスが拒否されます。別のボリューム内のqtreeと同じ移動または名前変更を行うと、ファイルはコピーされます。ファイルのサイズが大きい場合、移動処理に異常な時間がかかっているように見えても、ほとんどの移動処理はほぼ瞬時に完了します。これは、同じファイルシステム/ボリューム内の単純なファイル名が変更されるためです。

qtreeでの名前変更の動作は、Advanced Privilegeオプションによって制御 されます。このオプションは、NFSオプション「-validate-qtree-export」が有効な場合にqtree間でファイルを移動する際に、ネットアップの技術情報アーティクルで拒否される権限で説明されています。

この資料では、さまざまな操作の次の動作について説明します。

```
Assuming that file permissions allow and that client is allowed by export policies to access both
source and destination volume/qtree, these are the current permutations with the 'validate-qtree-
export' flag enabled or disabled:

Enabled:
- Rename in same volume and qtree: SUCCESS
- Rename in same volume, different qtrees: EACCESS
- Rename between volumes where qtree IDs differ: EACCESS
- Rename between volumes where qtree IDs match: XDEV

Disabled:
- Rename in same volume and qtree: SUCCESS
- Rename in same volume, different qtrees: SUCCESS
- Rename between volumes where qtree IDs differ: XDEV
- Rename between volumes where qtree IDs match: XDEV
```

注： `NFS3ERR_XDEV NFS3ERR_ACCESS` およびはRFC-1813で定義されています。

qtree間での名前変更や移動の動作を変更 `-validate-qtree-export disabled`するには、をに変更します。詳細については、「qtreeファイル操作のqtree IDの検証」を参照してください。

注 `- validate-qtree-export` ：qtree間で名前変更を許可する以外に、オプションを無効にしても、悪影響はないことがわかっています。

qtreeエクスポートのファイルハンドルへの影響

通常、クライアントに渡されるNFSエクスポートファイルハンドルのサイズは32バイト以下です。ただし、qtreeエクスポートでは、40バイトのファイルハンドルを作成するために追加の数バイトが追加されます。ほとんどのクライアントでは'このバイト・サイズは問題 ではありませんが'1996年に導入されたHPUX 10.20などの古いクライアントでは'これらのエクスポートのマウントで問題が発生する可能性がありますqtreeエクスポートを有効にしたあとにファイルハンドルの動作を変更する方法が現在ないため、qtreeエクスポートを有効にする前に、古いクライアント接続を必ず別のテストSVMでテストしてください。

同じボリューム上の複数のqtreeを同じNFSクライアントにマウントする

qtreeは実質的に独立したファイルシステムとして機能しますが、qtreeが同じボリューム内にある場合は、クライアントとサーバ間のNFSの通信で親ボリュームの同じMSID /ファイルハンドルが使用されます。その結果、NFSクライアントでは、qtreeが同じファイルシステムとして2回マウントされていることが確認され、使用済みスペースは各qtreeで実際に使用されている内容に関係なく同じになります。

たとえば、これらの2つのqtreeは、異なるマウントポイントにある同じクライアントにマウントされます。

```
# mount | grep qtree
10.193.67.214:/testvol/qtree1 on /mnt/qtree1 type nfs
10.193.67.214:/testvol/qtree2 on /mnt/qtree2 type nfs
```

ファイルをコピーする前のスペース使用量はどちらも同じです。

```
# df -h | grep qtree
10.193.67.214:/testvol/qtree1  973G 2.0M 973G     1% /mnt/qtree1
10.193.67.214:/testvol/qtree2  973G 2.0M 973G     1% /mnt/qtree2
```

次に、3.8GBのファイルをqtree1にコピーします。両方のqtreeで使用済みスペースが同じです。

```
# cp debian-8.2.0-amd64-DVD-1.iso /mnt/qtree1/
# df -h | grep qtree
10.193.67.214:/testvol/qtree1  973G 3.8G 970G     1% /mnt/qtree1
10.193.67.214:/testvol/qtree2  973G 3.8G 970G     1% /mnt/qtree2
```

そのためには、qtreeの1つに単純な監視クォータを適用します。これを行うだけで、適切なスペース使用量が表示されます。

```
cluster::*> quota report -vserver NFS
Vserver: NFS

                                     ----Disk---- ----Files-----   Quota
Volume   Tree       Type    ID       Used Limit     Used   Limit   Specifier
-------- ---------- ------- -------- ----------- ------- -------   ---------
testvol qtree1      tree    1
                                    3.73GB       -       2       -   qtree1
testvol qtree2      tree    2           0B       -       1       -   qtree2
testvol             tree    *           0B       -       0       -   *

# df -h | grep qtree
10.193.67.214:/testvol/qtree1  973G 3.8G 970G     1% /mnt/qtree1
10.193.67.214:/testvol/qtree2 970G      0 970G     0% /mnt/qtree2
```

サブディレクトリエクスポート

qtreeはNFS経由でエクスポートできます。単一レベルのサブディレクトリパスが用意されており、クライアントに固有のエクスポートポリシーとルールを定義できます。ただし、個々のディレクトリにエクスポートポリシーとルールを適用することはできません。また、qtreeを作成できるのは、現在ONTAP のボリュームレベルのみです。ディレクトリツリー内のエクスポートが下位必要な環境では、ボリューム、qtree、およびジャンクションパスの組み合わせを使用してサブディレクトリのエクスポートをシミュレートできます。ただし、ジャンクションパスの各レベルでは、クライアントによるトラバーサルを許可するためにエクスポートポリシールールへの読み取りアクセスを許可する必要があるため、この方法ではパス全体が保護されません。

たとえば、次のようなサブディレクトリエクスポートを作成できます。

```
/volume1/qtree1/volume2/qtree2/volume3/qtree3
```

上記のパスにある各オブジェクトを、一意のポリシーとルールを使用してNFSクライアントにエクスポートできます。これらのフォルダのセキュリティレベルを高めるには、NFSでNTFSセキュリティ形式/ ACLまたはKerberosの使用を検討してください。

ユーザおよびグループの所有者

ONTAP 9.8以降 `qtree create qtree modify`では、ONTAP CLIからまたはを使用して、qtreeのユーザおよびグループの所有者を設定できます。以前のリリースでは、これはクライアントからのNASプロトコルを使用して設定されていました。この設定は、現在CLIまたはREST APIでのみ使用できます。ZAPIとONTAP のどちらのSystem Managerもサポートされません。

```
[ -user <user name> ]              User ID
[ -group <group name> ]            Group ID
```

クォータの管理

ONTAP では、NAS処理で使用するユーザ/グループクォータおよびツリークォータをサポートしています。クォータを使用すると、ストレージ管理者は、ストレージシステム内のスペースおよびファイル数の使用状況を監視および制御できます。

FlexGroup ボリュームもクォータをサポートします。これらの見積もりのサポートレベルは、次のカテゴリに分類されます。

- ONTAP 9.3でのクォータレポートのサポート
- FPolicyのサポート。ONTAP 9.4では、DefendX（旧NTP）などのサードパーティベンダーによるクォータ適用を可能にします。
- ONTAP 9.5以降では、クォータの適用（容量とファイル数のハードリミットとソフトリミットの設定）がサポートされています。

ユーザクォータとグループクォータに関する考慮事項

ユーザクォータまたはグループクォータを実装するには、クラスタが指定したユーザ名またはグループを解決できる必要があります。したがって、ユーザまたはグループは、SVM上、またはActive Directory、LDAP、NISなどの解決可能なネームサービスサーバ内にローカルに存在する必要があります。ユーザまたはグループがSVMで見つからない場合は、クォータルールは作成されません。ユーザが無効なためにユーザクォータまたはグループクォータを作成できなかった場合、コマンドラインで次のエラーが発生します。

```
Error: command failed: User name user not found. Reason: SecD Error: object not found.
```

同様のメッセージがONTAP System Managerから送信されます。`event log show` コマンドを使用して問題 をさらに調査します。ONTAP でのID管理用のネームサービスの設定の詳細については、TR-4835：『How to Configure LDAP in ONTAP』およびTR-4668：『Name Services Best Practices Guide』を参照してください。

ユーザクォータまたはグループクォータを作成します

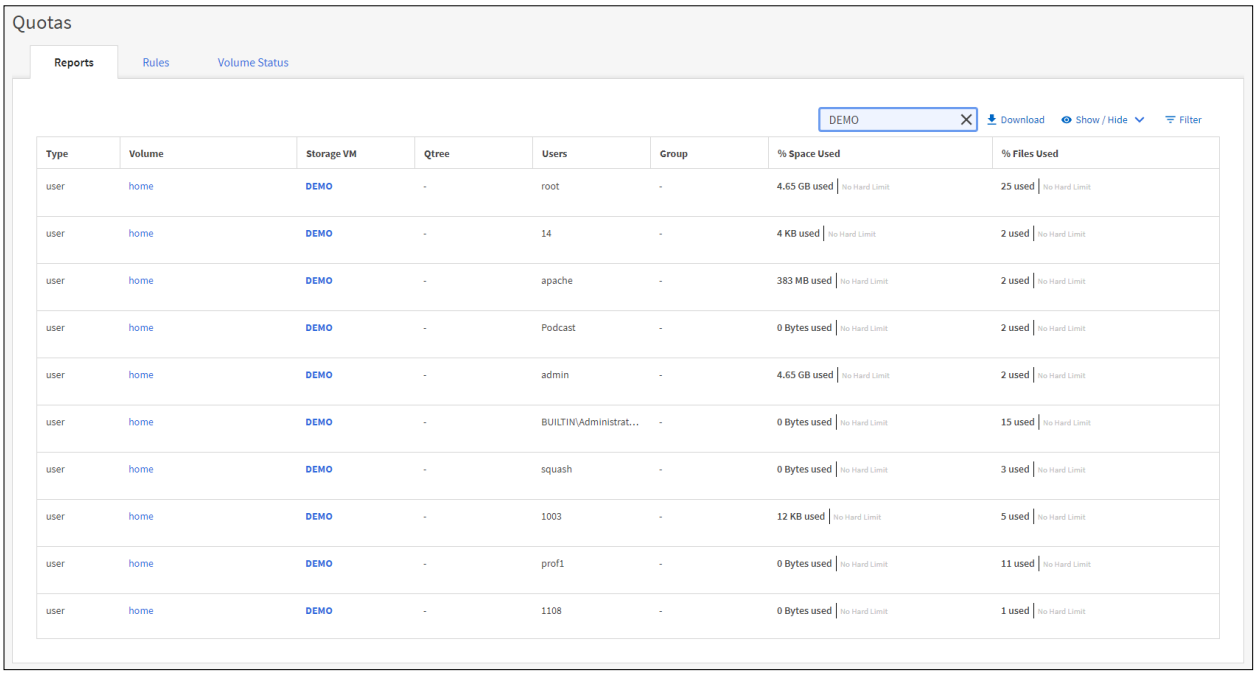
ユーザクォータとグループクォータを作成して、ユーザごとに容量やファイル数の上限をレポートしたり適用したりできます。これらのクォータは、複数のユーザまたはグループが同じネームスペースまたはqtreeを共有するシナリオで使用されます。これらの手順は、FlexVol ボリュームとFlexGroup ボリュームで同じです。

クォータの作成-ONTAP システムマネージャ

ONTAP システムマネージャでユーザクォータまたはグループクォータを作成するには、左側のメニューから[ストレージ]、[クォータ]の順に選択します。レポート、ルール、ボリュームステータスの3つのタブがあるページが表示されます。

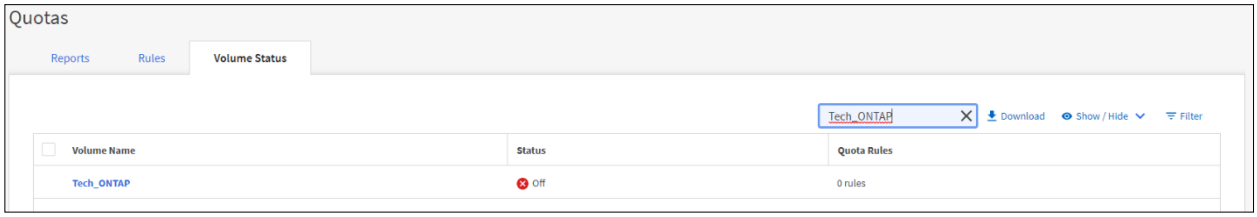
レポートには、ユーザ、グループ、およびqtreeの現在のクォータ追跡が表示されます。

図13）クォータレポート-ONTAP システムマネージャ



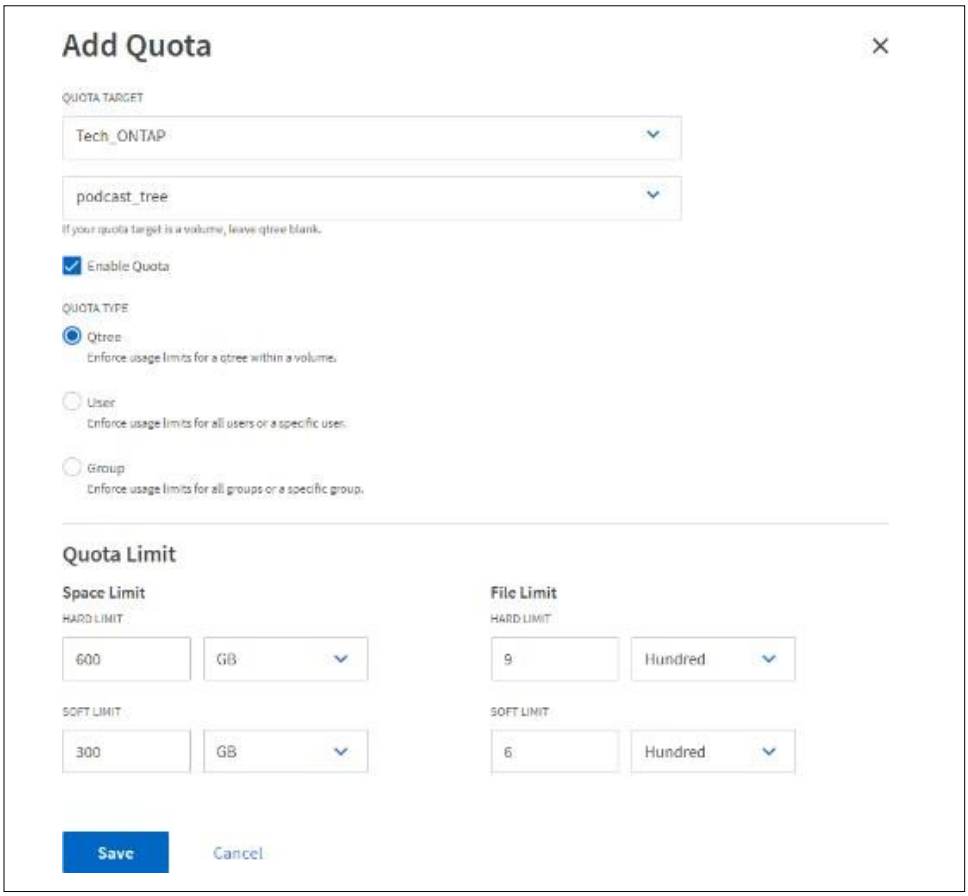
ボリュームのボリュームステータスには、そのボリュームでクォータがオンかオフかが表示されます。

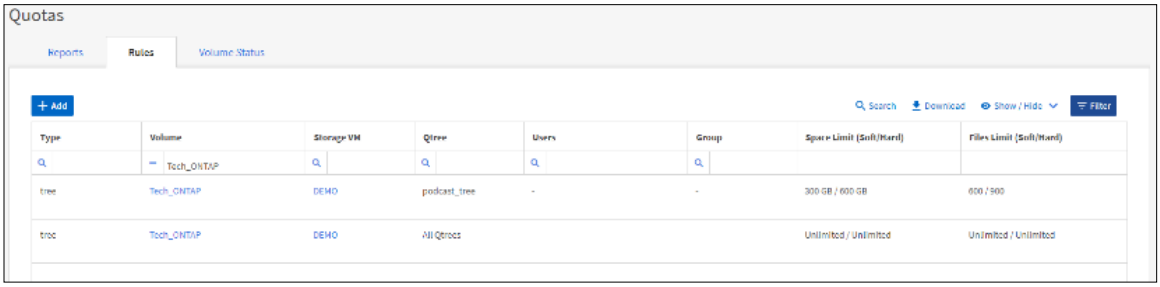
図14）クォータボリュームのステータス- ONTAP システムマネージャ

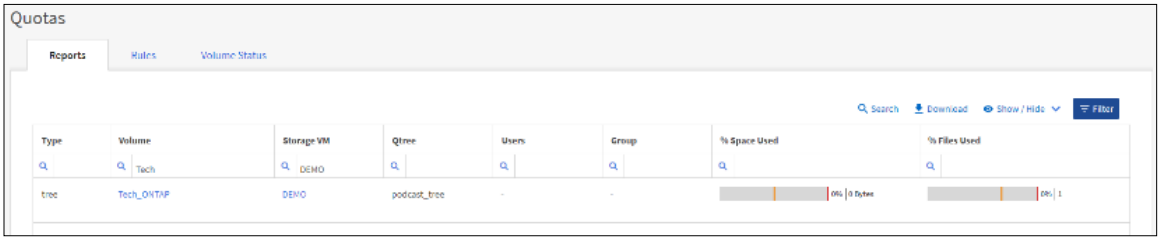


ルールとは、ユーザ、グループ、またはqtreeの新しいクォータを作成する場所です。Addをクリックして、ダイアログボックスにユーザ、グループ、またはqtreeクォータの情報を入力します。ルールの作成後、ONTAP System Managerは必要なすべての手順を実行して、クォータを有効化してアクティブ化します。

図15）クォータルール-ONTAP システムマネージャ







ユーザクォータまたはグループクォータの作成-CLI

CLIを使用して特定のユーザまたはグループのレポートクォータを作成するには、admin権限レベルで次のコマンドを実行します。

```
cluster::> quota policy rule create -vserver SVM1 -policy-name default -volume flexgroup -type
[user|group] -target [username or groupname] -qtree ""
```

CLIを使用してすべてのユーザまたはグループのユーザまたはグループのレポートクォータを作成するには、admin権限レベルで次のコマンドを実行します。ターゲットは、次のようにアスタリスクで示されます `all`。

```
cluster::> quota policy rule create -vserver SVM1 -policy-name default -volume flexgroup -type
[user|group] -target * -qtree ""
```

CLIを使用したツリーレポートクォータの作成

CLIを使用して特定のユーザまたはグループのツリーレポートクォータを作成するには、admin権限レベルで次のコマンドを実行します。

```
cluster::> quota policy rule create -vserver DEMO -policy-name tree -volume flexgroup_local -type
tree -target qtree
```

クォータを有効にするには `quota on`、または `quota resize`を使用します。

```
cluster::> quota on -vserver DEMO -volume flexgroup_local
[Job 9152] Job is queued: "quota on" performed for quota policy "tree" on volume
"flexgroup_local" in Vserver "DEMO".

cluster::> quota resize -vserver DEMO -volume flexgroup_local
[Job 9153] Job is queued: "quota resize" performed for quota policy "tree" on volume
"flexgroup_local" in Vserver "DEMO".

cluster::> quota show -vserver DEMO -volume flexgroup_local

              Vserver Name: DEMO
               Volume Name: flexgroup_local
               Quota State: on
               Scan Status: -
          Logging Messages: -
          Logging Interval: -
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
       User Quota enforced: false
      Group Quota enforced: false
       Tree Quota enforced: true
```

`quota report` 次の例は、ツリークォータが指定されたボリュームに対するコマンドを示しています。

```
cluster::> quota report -vserver DEMO -volume flexgroup_local
Vserver: DEMO

                                     ----Disk---- ----Files-----    Quota
Volume   Tree      Type    ID        Used Limit     Used   Limit   Specifier
---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
flexgroup_local
         qtree     tree    1           0B      -       1       -   qtree
```

使用済みファイルとディスクスペースが監視され、新しいファイルが作成されるたびに増分されます。

```
cluster::> quota report -vserver DEMO -volume flexgroup_local
Vserver: DEMO

                                      ----Disk---- ----Files-----   Quota
Volume   Tree      Type    ID        Used Limit     Used   Limit   Specifier
---------- ---------- ---------- ---------- ---------- ---------- ----------
flexgroup_local
         qtree     tree    1
                                  13.77MB      -       4       -   qtree
```

クォータ適用の例

qtreeまたはユーザ/グループに対してクォータの適用を有効にすると、クォータを超過したあとに、ONTAPは新しいファイルの作成または書き込みを禁止します。これにより、ストレージ管理者は、ボリュームまたはqtreeに書き込まれるデータの量をより細かく制御できます。

また、クォータを超過すると、イベント管理システムメッセージがデバッグ重大度レベルでログに記録され、クォータ違反についてストレージ管理者に通知します。これらのメッセージは、SNMPトラップまたはsyslogメッセージとして転送されるように設定できます。

この例では、1GBおよび10ファイルのハードリミットがクォータに設定されています。

```
cluster::*> quota policy rule show -vserver DEMO

Vserver: DEMO               Policy: tree              Volume: flexgroup_local

                                                 Soft              Soft
                          User          Disk     Disk    Files     Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit     Limit  Threshold
------  --------  ------  -------  ----------  -------  -------  -------  ---------
tree    qtree     ""      -             1GB        -       10        -          -
```

ユーザ `out of space` が1.2GBのファイルをqtreeにコピーしようとすると、ONTAP からエラーが報告されます。

```
[root@centos7 qtree]# cp /SANscreenServer-x64-7.3.1-444.msi /FGlocal/qtree/
cp: failed to close ‘/FGlocal/qtree/SANscreenServer-x64-7.3.1-444.msi’: No space left on device
```

ファイルは部分的に書き込まれていますが、データがないため使用できません。

```
# ls -alh
total 1.1G
drwxr-xr-x 2 root root 4.0K Jul 19 15:44 .
drwxr-xr-x 11 root root 4.0K Jun 28 15:10 ..
-rw-r--r--  1 root root     0 Dec 12  2017 newfile1
-rw-r--r--  1 root root     0 Dec 12  2017 newfile2
-rw-r--r-- 1 root root 1021M Jul 19 2018 SANscreenServer-x64-7.3.1-444.msi
```

その後、ONTAPはクォータを超過と報告します。

```
cluster::*> quota report -vserver DEMO
Vserver: DEMO

                                     ----Disk---- ----Files-----   Quota
Volume   Tree      Type    ID        Used Limit     Used   Limit   Specifier
-------  --------  ------  --------  ---------------------------   ---------
flexgroup_local
         qtree     tree    1
                                   1.01GB    1GB       5      10   qtree
```

ファイル数の上限についても同じ動作が発生します。この例では、ファイル数の上限は10で、qtreeにはすでに5つのファイルがあります。さらに5つのファイルが制限に適合しています。

```
[root@centos7 /]# su student1
sh-4.2$ cd ~
sh-4.2$ pwd
/home/student1
sh-4.2$ touch file1
sh-4.2$ touch file2
sh-4.2$ touch file3
sh-4.2$ touch file4
sh-4.2$ touch file5
touch: cannot touch ‘file5’: Disk quota exceeded

cluster::*> quota report -vserver DEMO
Vserver: DEMO

                                    ----Disk---- ----Files---------Quota
```

```
Volume   Tree       Type    ID        Used Limit     Used   Limit   Specifier
-------- ---------- ------- --------- ------- ------- -------- ------- ----------
flexgroup_local
         qtree      tree    1
                                    1.01GB    1GB       5      10   qtree
home                user    student1, NTAP\student1
                                     4KB    1GB      10      10   student1
2 entries were displayed.
```

イベントログには、クォータ違反が表示されます。

```
cluster::*> event log show -message-name quota.exceeded
Time                 Node              Severity      Event
-------------------------- ---------------------- ----------------- ----------------------------------
7/19/2018 16:27:54 node02
                                       DEBUG         quota.exceeded: ltype="hard", volname="home",
app="", volident="@vserver:7e3cc08e-d9b3-11e6-85e2-00a0986b1210", limit_item="file",
limit_value="10", user="uid=1301", qtree="treeid=1", vfiler=""
7/19/2018 15:45:02 node01
                                       DEBUG         quota.exceeded: ltype="hard",
volname="flexgroup_local", app="", volident="@vserver:7e3cc08e-d9b3-11e6-85e2-00a0986b1210",
limit_item="disk", limit_value="1048576", user="", qtree="treeid=1", vfiler=""
```

クォータスキャンの完了時間

クォータの初期化またはサイズ変更が行われた場合、ONTAPはいくつかのバックグラウンドタスクを実行して、クォータ使用量を正確に反映するために必要な作業を完了する必要があります。これらのタスクには時間がかかりますが、これは以下で説明するいくつかの要因によって異なります。

初期化の完了時間

ボリュームまたはqtreeでクォータが初期化されるまでの時間は、次の要因によって異なります。

- **ボリューム内のファイルとフォルダの数。**ファイル数が多いほど初期化時間は長くなりますが、ファイルサイズは初期化時間に影響しません。
- **ボリュームのタイプ。**FlexVol ボリュームのスキャンは、FlexGroup ボリュームが配置されているノード間でFlexGroup クォータスキャンが並行して実行されるため、FlexGroup ボリュームのスキャンよりも時間がかかることがあります。
- **ハードウェアのタイプとシステムの負荷。**ファイル数の多いシステムでは、スキャンに数時間かかることがあります。

クォータの初期化ステータスを確認するには、次のコマンドを実行します。

```
quota show -volume volname -instance
```

クォータのサイズ変更の完了時間

クォータのサイズ変更は、クォータポリシーを変更するときに使用されます。サイズ変更では、新しい制限値でスキャンが実行されます。このプロセスには、完了までの時間に関する考慮事項もいくつかあります。

- サイズ変更では、新しく追加されたルールのみを使用してスキャンが実行されるため、初期化よりも短時間で完了します。
- サイズ変更は、クォータのオン/オフよりも処理量が少ないため、通常はほんの数秒で完了します。
- サイズ変更が完了するまでの時間が短縮されるため、クォータのオン/オフを切り替えずにresizeを使用してください
- クォータのサイズ変更では、最大100個の同時ジョブを実行できます。100個のジョブのあと、サイズ変更処理はキューで待機する必要があります。
- 同時スキャン数を増やすと、サイズ変更のパフォーマンスに影響し、ジョブが完了するまでの時間が長くなる可能性があります。

クォータに関するユーザマッピングの考慮事項

クォータのマルチプロトコル環境でのユーザマッピング（SMBとNFSの両方からのデータアクセス）は、メンバーボリュームレベルで行われます。最終的に、すべてのメンバーボリュームがユーザマッピングに同意します。ただし、ユーザマッピングに失敗した場合や、別のメンバーのネームマッピングを実行したときにタイムアウトになっ

た場合など、情報が一致しないことがあります。つまり、少なくとも1人のメンバーがユーザーがユーザーマップペアの一部であると見なし、少なくとも1人のメンバーがそれを個別のレコードとみなします。

最悪の場合、問題 が解決されるまでクォータルールの適用が一貫しないことがあります。たとえば、ユーザがクォータ制限を一時的に超過する可能性があります。

ユーザマッピングの結果が調整されると、イベント管理システムメッセージが送信されます。

```
cluster::*> event route show -message-name fg.quota.usermapping.result -instance

                                    Message Name: fg.quota.usermapping.result
                                        Severity: NOTICE
                                Corrective Action: (NONE)
                                     Description: This message occurs when the quota mapper
decides whether to map the Windows quota record and the UNIX quota record of a user into a single
multiuser record.
```

ツリークォータに関する考慮事項

ONTAP のSVMには最大5つのクォータポリシーを設定できますが、同時にアクティブにできるポリシーは1つだけです。SVM内のアクティブポリシーを表示するには、次のコマンドを実行します。

```
cluster::> vserver show -vserver DEMO -fields quota-policy
vserver quota-policy
---------- ----------------
DEMO    default
```

注： 現時点では、この情報をONTAP System Managerで表示することはできません。

デフォルトポリシーはほとんどの場合適切であり、変更する必要はありません。`quota on` を実行すると、ボリュームに割り当てられていたポリシーではなく、アクティブなポリシーが使用されます。そのため、ボリューム `quota on` にクォータとルールを適用したとみなされても、適用に失敗することがあります。

次の例は、クォータポリシーをボリュームに適用します。

```
cluster::*> quota policy show -vserver DEMO -policy-name tree

      Vserver: DEMO
  Policy Name: tree
Last Modified: 10/19/2017 11:25:20
    Policy ID: 42949672962

cluster::*> quota policy rule show -vserver DEMO -policy-name tree -instance

                Vserver: DEMO
            Policy Name: tree
            Volume Name: flexgroup_local
                   Type: tree
                 Target: tree1
             Qtree Name: ""
           User Mapping: -
             Disk Limit: -
            Files Limit: -
Threshold for Disk Limit: -
         Soft Disk Limit: -
        Soft Files Limit: -
```

SVM `default` にクォータが割り当てられていて、ルールが含まれていないため、クォータをオンにするとエラーが発生します。

```
cluster::*> quota on -vserver DEMO -volume flexgroup_local -foreground true

Error: command failed: No valid quota rules found in quota policy default for volume
flexgroup_local in Vserver DEMO.
```

ルール defaultquota on をに追加するとコマンドは機能しますが、SVMは新しいツリーポリシーを使用しません。

```
cluster::*> quota policy rule create -vserver DEMO -policy-name default -volume flexgroup_local -
type tree -target ""

cluster::*> quota on -vserver DEMO -volume flexgroup_local -foreground true
[Job 8063] Job succeeded: Successful

cluster::*> vserver show -vserver DEMO -fields quota-policy
vserver quota-policy
---------- ------------
DEMO    default
```

必要なポリシーを使用するには、SVMを変更してからクォータをオフにしてオンに戻す必要があります。

```
cluster::*> vserver modify -vserver DEMO -quota-policy tree

cluster::*> quota off -vserver DEMO *

cluster::*> quota policy rule delete -vserver DEMO -policy-name default *
1 entry was deleted.

cluster::*> quota on -vserver DEMO -volume flexgroup_local -foreground true
[Job 8084] Job succeeded: Successful
```

クォータが有効な場合にクライアントがスペースを確認する方法

ONTAP であるqtreeに対してクォータが有効になっている場合、クライアントにはそのクォータから報告される使用可能なスペースのみが表示されます。

たとえば、qtree1のクォータは次のようになります。

```
cluster::*> quota report -vserver DEMO -volume flexgroupDS -tree qtree1
Vserver: DEMO

                                  ----Disk---- ----Files-----    Quota
Volume   Tree      Type    ID      Used Limit     Used   Limit   Specifier
---------- --------- ------- ------ ---------- ------- ------- ---------
flexgroupDS
         qtree1    tree    1          0B 500GB       1       -   qtree1
```

ボリュームに実際にあるスペースは次のとおりです。

```
cluster::*> vol show -vserver DEMO -volume flexgroupDS -fields size
vserver volume      size
---------- --------------- ------
DEMO    flexgroupDS 10TB
```

クライアントに表示されるボリュームのスペースは次のとおりです。

```
# df -h /mnt/nas2
Filesystem         Size Used Avail Use% Mounted on
demo:/flexgroupDS  9.5T 4.5G 9.5T     1% /mnt/nas2
```

このqtreeに関して報告される内容は次のとおりです。

```
# df -h /mnt/nas2/qtree1/
Filesystem         Size Used Avail Use% Mounted on
demo:/flexgroupDS 500G      0 500G    0% /mnt/nas2
```

ネームマッピングの高度な概念

ONTAP でのネームマッピングは、WindowsユーザとUNIXユーザが同じユーザ名を使用する場合と同様に簡単に行うことができ、暗黙的な1：1のネームマッピングを実現します。設定を追加する必要はありません。Windowsユーザと UNIXユーザのユーザ名がネームサービスで見つかった場合、それらのユーザ名と一致するとすべてが正常に機能します。ONTAP

ただし、ネームマッピングの方が複雑になります。特に、ユーザ名が一致しない場合や、ONTAP で検索するドメインが複数ある場合は、名前のマッピングが複雑になります。

このセクションでは、これらの複雑さの一部について説明します。

正規表現とワイルドカード

ONTAP のネームマッピングルールでは、正規表現（regex）とワイルドカード値を使用して、非対称ユーザ名のネームマッピングルールを設定できます。ワイルドカードは、UNIX名とWindows名に共通の一般的な違いが複数あるユーザ名に便利です。たとえば、すべてのWindowsユーザ名の最初の名前と最後の名前の間にピリオドがあるものの（Alice .Smithなど）、UNIXユーザ名の名前にアンダースコアがある場合、正規表現を使用してユーザ同士のマッピングを常に維持できます。

ピリオドをアンダースコアに置き換えるWindowsからUNIXへの正規表現ネームマッピングの例を次に示します。

```
vserver name-mapping create -vserver DEMO -direction win-unix -position 1 -pattern
(.+)\\(.+)\.(.+) -replacement \2_\3
```

次に、アンダースコアをピリオドに置き換えるUNIXからWindowsへの正規表現ネームマッピングの例を示します。

```
vserver name-mapping create -vserver DEMO -direction unix-win -position 2 -pattern (.+)_(.+) -
replacement \1\.\2
```

詳細については、ネームマッピングの変換ルールを参照してください。

rootへのWindows管理者ユーザのマッピング

マルチプロトコルのNAS解決策 では、Windows管理者ユーザが、NFS/UNIX環境のrootの場合と同じようにファイルやフォルダにアクセスできるようにすることができます。このようなユースケースの1つに、データ移行があります。管理ユーザは、ACLに追加することなく、ファイルをコピーしてACLをグローバルに変更するためのアクセスを必要とする場合があります。

これを行うには、主に2つの方法があります。

- ルートになるユーザをきめ細かく制御するには、目的のユーザ名をルートユーザにマッピングするwin-unixネームマッピングルールを作成します。この方法を使用すると、SVMのローカルBUILTIN\Administratorsグループに含まれるすべての管理ユーザにグローバルルールを適用することを回避できます。
- SVMのローカルBUILTIN\Administratorsグループ `-is-admin-users-mapped-to-root-enabled`内のすべてのユーザにSVM内のファイルやフォルダへのルートアクセスを許可する場合は、CIFSサーバオプションを使用します。

  注： 単にデータ移行を目的としたユースケースの場合は、代わりにBUILTIN\Backup Operatorsを使用してください。各ローカルグループ上 にある権限の詳細については、「サポートされる権限の一覧」を参照してください。

Windowsクライアントをユーザ名にマッピングする

ユーザ名をユーザ名にマッピングするだけでなく、ネームマッピングルールを使用して個々のクライアントまたはサブネットをユーザ名にマッピングすることもできます。これは、クライアントまたはサブネットのレベルでアクセス権を制限する場合に役立ちます。

たとえば、10.10.10.x/24サブネット内 `DOMAIN\application`のすべてのクライアント（特定のWindows NTFS権限を必要とするアプリケーションを実行している場合）をWindowsユーザにマッピングするには、次のネームマッピングルールを使用します。

```
vserver name-mapping create -vserver SVM -direction unix-win -position 2 -pattern root -
replacement DOMAIN\application -address 10.10.10.0/24
```

ネームマッピングにLDAPを使用

ONTAP ではSVMに対してローカルにネームマッピングルールを明示的に作成できますが、作成できるルールは1、024個までです。ルールが必要になる場合や、LDAPなどの一元管理されたネームマッピングサーバを使用する場合があります。

このような場合は、LDAPを使用してネームマッピングサーバとして機能します。LDAP属性にマッピングするUNIXまたはWindowsユーザ名を入力し、次のLDAPクライアントスキーマのフィールドでその属性を指定します。表5に、これらの属性とその機能を示します。

表5）LDAPクライアントスキーマオプション-ネームマッピング

LDAPスキーマ属性	機能
`-windows-to-unix-object-class`	WindowsからUNIXへのネームマッピングオブジェクトクラスを定義するLDAP属性を提供します。オブジェクトクラスを使用すると、複数のLDAPオブジェクトをグループ化して検索を高速化できます。AD-IDMUのデフォルト値 `User`はです。RFC 2037スキーマの場合、値 `posixAccount`はに設定されます。
`-windows-to-unix-attribute`	UNIXユーザへのWindowsユーザのマッピングに使用される値のLDAP属性を提供します。ONTAP のAD-IDMUスキーマのデフォルト値 `sAMAccountName`はです。 RFC 2307スキーマの場合、値はデフォルト `windowsAccount`でになります。
`-windows-to-unix-no-domain- prefix`	このオプション - `windows-to-unix-attribute`は、の属性値にドメインプレフィックスが追加されているかどうかを制御します。（デフォルトは `false`です）。`sAMAccountName`は単 `DOMAIN\usernamemsDS-PrincipalName` 一のユーザ名で表され、がLDAP検索で使用できる値ではないため、ドメインプレフィックスは機能の非対称ネームマッピングを有効にするために必要な場合があります。この値の必要性は、使用するLDAPスキーマと属性、および複数の一意のWindowsドメインに複数のドメインネームマッピングが存在するかどうかによって異なります。
`-windows-account-attribute`	このオプションは、UNIX名をWindows名にマッピングするときに使用するLDAPスキーマ属性を制御します。この属性のデフォルト値はsAMAccountNameです。このフィールドは、新しいユーザの作成時にWindowsアカウントに使用されます。

LDAPクライアント `namemap ldap,files`がネームマッピング検索用に設定されたら、使用するns-switchデータベースを変更します。WindowsとUNIXのユーザ名が一致しているか対称である場合（たとえば、WindowsのJohnsがUNIXのJohns）、アクションは不要です。非対称ネームマッピングでのLDAP の使用の詳細については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

注： 外部サービスが実際に非対称ネームマッピングに使用されている場合にのみ、ネームマップデータベースに外部サービスを指定します。ネームマッピングルールが設定されていないサーバを指定した場合、ネームマッピングの検索を実行すると要求にレイテンシが生じ、認証に時間がかかったり、失敗したりすることがあります。

NASリダイレクトとグローバル共有

ローカルネットワーク間でファイルを共有するのは一般的に簡単です。ネットワークは信頼性が高く、ロックセマンティクスは、競合するほど複雑ではありません。ただし、NASデータセットをWAN経由で複数のサイトに共有したり、同じネットワーク内の複数のファイルシステム間で共有したりすると、やや複雑になります。このセクションでは、Distributed File System（DFS；分散ファイルシステム）ボリュームとFlexCache ボリュームを使用したシンボリックリンク（symlinks）/widelinkなど、いくつかのシナリオを取り上げます。

シンボリック リンクとワイド リンク

ONTAP では、シンボリックリンクとワイドリンクの両方を使用して、NAS共有内のフォルダやファイルからネットアップ以外のリモートストレージにトラフィックをリダイレクトできます。ストレージ管理者はこの機能を使用して、データがどこにあるかに関係なくクライアントに透過的な単一のネームスペースを作成して提供できます。

シンボリック リンクとは

シンボリックリンクとは、絶対パスまたは相対パスの形式で、別のファイルまたはディレクトリへの参照を含むファイルです。

- **絶対パスは**、現在の作業ディレクトリやシンボリックリンクの場所に関係なく、ファイルシステム内の同じ場所を参照します。このパスは、常にパスの「/」で開始する必要があります。
- **相対パスは**指定された作業ディレクトリから始まります。これはリンクを定義するための短い簡単な方法ですが、誤ったパスが定義されている場合は、パスが見つからないというエラーを作成することもできます。

ONTAP では、NFS経由またはPowerShellを使用してUNIXクライアントからシンボリックリンクを作成できます。この記事は、ONTAP でNFSを使用せずにシンボリックリンクを作成する方法を参照してください。

注： 現時点では、CIFS / SMBクライアントからシンボリックリンクを作成することはできません。詳細については、バグ930915を参照してください。

ワイドリンクとは

widelinkは、NASネームスペースをストレージシステムの外部にある他のNASデバイスに拡張するためのシンボリックリンクです。これには、他のONTAP インスタンスや、Windows DFSを含むネットアップ以外のストレージも含まれます。ONTAP では、適切 `-symlink-properties` なCIFS共有オプションを指定して、シンボリックリンクとワイドリンクを作成できます。

```
cluster::*> cifs share modify -vserver DEMO -share-name share -symlink-properties ?
  enable                    (DEPRECATED)-Enable both local symlinks and wide links for read-write
  hide                      (DEPRECATED)-Hide both symlinks and wide links
  read_only                 (DEPRECATED)-Enable symlinks for read-only
  symlinks                  Enable symlinks only for read-write, DFS is not advertised
  symlinks_and_widelinks    Enable both local symlinks and wide links, DFS is advertised
  disable                   Disable both local symlinks and wide links, DFS is not advertised
  no_strict_security        Allow clients to follow symlinks outside share boundaries
```

ハードリンクとは何ですか？

ハードリンクは、ディレクトリではなくファイルにリンクするために使用できるリンクです。シンボリックリンクとワイドリンクとは異なり、ハードリンクは別のファイルシステムにまたがることができず、ディレクトリをリンクすることもできません。ONTAP では、ハードリンクをスパンできないことを意味します。

- 異なるボリューム
- qtreeが異なります
- Snapshotコピーとアクティブファイルシステム間の移動
- SVMが異なります
- ストレージシステムが異なります

同じボリューム内のフォルダ/ディレクトリは異なるファイルシステムとはみなされませんが、ハードリンクは同じボリューム内の複数レベルのファイルを指すことがあります。

ファイルシステムの境界を越えるハードリンクを作成しようとすると、次のエラーが表示されます。

```
ln: failed to create hard link ‘hard-link’ => ‘/path/to/file: Invalid cross-device link
```

ハードリンクが作成されると、ファイルに複数のinodeアクセスポイントが設定されます。たとえば、ファイルとハードリンクの両方に同じファイル内容が表示されます。

```
# cat /mnt/client1/dir1/dir2/linked-dir/hard-file
this is a linked file

# cat /mnt/client1/hard-link
this is a linked file
```

ハードリンクを持つファイル `ls -i` を検索するには、まずinode番号を検索してから、同じinode番号を持つすべてのファイルを検索します。

例：

```
# ls -i | grep hard-link
1146684405 hard-link

# find /mnt/client1 -inum 1146684405
/mnt/client1/dir1/dir2/linked-dir/hard-file
/mnt/client1/hard-link
```

UNIX/NFSシンボリック リンク

UNIX / NFSシンボリックリンクを作成する場合、特別な設定や考慮事項はありません。リンク先のパスがクライアント上に存在する場合、これらのNFSシンボリックリンクは想定どおりに機能します。

CIFSシンボリックリンクパス

UNIXで作成したシンボリックリンクにCIFS / SMB共有を指定する場合は、リンクが適切に機能するように、シンボリックリンクパスを適切なCIFS共有パスにマッピングしてください。CIFSシンボリックリンクを作成する場合、考慮すべき2つのポイントがあります。

- ストレージシステムでは、UNIX形式のシンボリックリンクとDFSリファーラルがオーバーレイできるため、CIFSクライアントもリダイレクトされます。リンクが相対リンクであり、共有内にとどまる場合、ストレージシステムはこれらのリンクを透過的にマッピングする方法を把握しています。
- シンボリックリンクが絶対パスである場合、または別のエクスポートをポイントしている場合は、リンクがCIFSクライアントを適切な宛先（同じノード上の別のCIFS共有であるか、別のCIFSサーバ上の共有であるか）に解決するように、マッピングルールを作成できます。

ONTAP が適切なファイルまたはディレクトリにリンクをリダイレクトするためには、CIFSシンボリックリンクパスが必要です。これら `cifs symlink create`のパスは、コマンドを実行して作成します。

注　`cifs symlink create` ：コマンドではシンボリックリンクは作成されず、代わりにパスマッピングが作成されます。ただし、シンボリックリンクはNFSクライアントに作成するか、PowerShellを使用して作成する必要があります。

CIFSシンボリックリンクマッピングを作成しています

Data ONTAPシンボリックリンクを正しく機能させるために必要な操作を簡単に説明しています。clusteredのナレッジベースの記事（「7つの重要なポイント」セクション）では、CIFSシンボリックリンクを[CIFSクライアントに対してワイドリンクを機能させる方法]について説明しています。

- `cifs symlink create` コマンドは、シンボリックリンクを作成しません。
- シンボリックリンクは必須であり、NFSクライアントからのみ作成するか、PowerShellツールキットを使用して作成できます。
- CIFSシンボリックリンクマップエントリは、デスティネーションではなく、シンボリックリンクを含む共有があるSVM上に存在する必要があります。
- マッピングするシンボリックリンクがあるSVM上の共有では、シンボリックリンクが有効になっているか、読み取り専用に設定されている必要があります。`cifs share show` コマンドを実行して、この設定を確認します。
- SVMは、リンクの名前やリンク自体のパスではなく、マッピングに使用するシンボリックリンクのコンテンツ（デスティネーションパス）を解析します。リンクが何を指し `ls -l` ているか、つまりマッピングする必要があるかを確認するには、リンクを持つディレクトリでを実行し、リンク先のパスを確認します。

- CIFSリファーラルへのシンボリックリンクのマッピングはディレクトリに対してのみ機能し、ファイルに対しては機能しません。
- シンボリックリンクの唯一の目的がCIFSクライアントのリダイレクトである場合。シンボリックリンクのリンク先のUNIXパスが、実際にはONTAP 内またはNFSクライアント上に存在しない場合は、シンボリックリンクは、CIFSマップのみを目的として存在できます。関連するマッピングが正しく、シンボリックリンクのデスティネーションパスと一致している場合、は、リンク自体がUNIXクライアントまたはLinuxクライアントで機能しない場合でも、CIFSをリダイレクトします。

CIFSシンボリックリンクの例

次のセクションでは、CIFSシンボリックリンクの例を示します。

- 相対パスを使用した、同じボリューム内のCIFSシンボリックリンク。
- 絶対パスを使用して同じボリューム内のCIFSシンボリックリンク。
- 同じSVM /異なるボリューム内のCIFSワイドリンク。
- NetApp以外のCIFS共有にリンクするCIFSワイドリンク。
- ローカルファイルへのCIFSシンボリックリンク。
- リモートファイルへのCIFSシンボリックリンク。

シンボリックリンクを作成しようとすると、CIFS / SMBクライアントとONTAP が、シンボリックリンクパス解決の状態に同意しない場合があります。予期しない動作が発生したり、正常に動作しない場合は、「キャッシュとシンボリックリンクエラー」の項で回避策を参照してください。

MacOSでのDFSの動作とシンボリックリンクの詳細については、「MAC OSクライアントではDFSリンクは機能しない。ONTAP 9.5とシンボリックリンクが有効になっている」を参照してください。

その他 の例については、『clustered Data ONTAP でのシンボリックリンクおよびワイドリンクの作成方法』を参照してください。

CIFSシンボリックリンク：同じボリューム、相対パス

この例は、ボリュームの相対パスを使用して、同じボリューム内の深さが3レベルのフォルダにリダイレクトするリンクをボリュームのルートに作成する方法を示しています。

- 相対フォルダパス `dir1/dir2/linked-dir`はです。
- このリンクは、NFSマウントで次のコマンドを実行することで作成されます。

```
ln -s dir1/dir2/linked-dir rel-link
```

そのリンクが作成されると、NFSから想定される結果が表示されます。symlink ()と`rel-link`フォルダパス `dir1/dir2/linked-dir/`） の両方(同じファイルを表示)

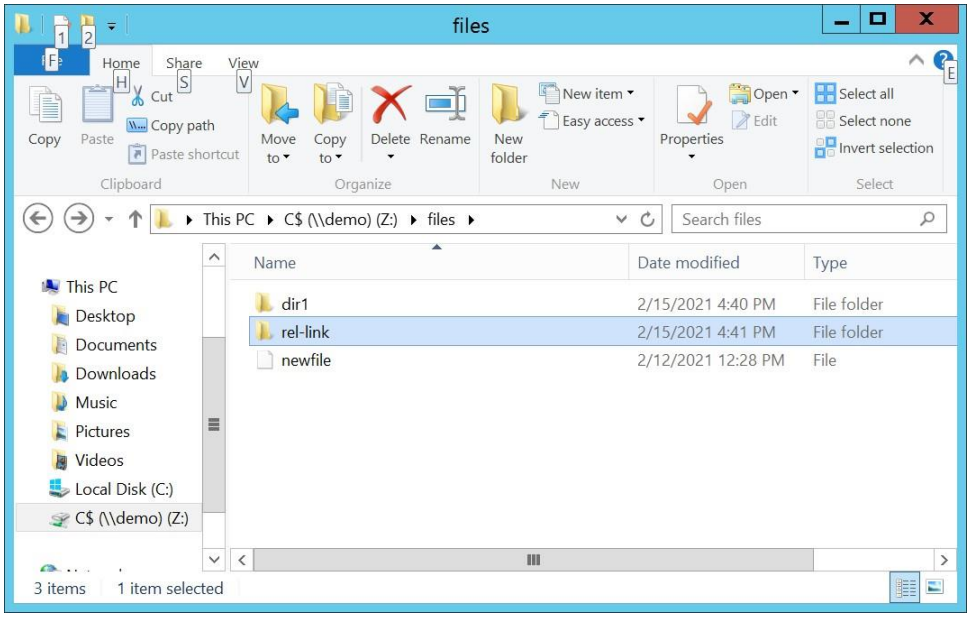
```
# ls -la rel-link/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 16:41 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file

# ls -la dir1/dir2/linked-dir/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 16:41 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file
```

ONTAP では、CIFS共有でsymlinkプロパティが設定されている場合、同じボリューム内の相対パスを使用したシンボリックリンクは、特別なCIFSシンボリックリンクマッピングを作成することなくリダイレクトされます。デフォルトでは、すべてのCIFS共有でこのプロパティがすでに設定されているため、相対CIFSシンボリックリンクは特別な設定を必要とせずにすぐに使用できます。

CIFS / SMB共有では、このリンクはディレクトリまたはショートカットとして表示されます。

注： シンボリックリンクの表示方法（ショートカットまたはファイル/ディレクトリ）は使用中のSMBのバージョンによって異なり、「ジャンクションパスとリパースポイント」で説明したオプションによって制御されます。

図16）CIFSシンボリックリンク、相対パス-同一ボリューム



CIFSシンボリックリンク：同じボリューム、絶対パス

絶対パスでシンボリックリンクを作成すると、リンクが存在するネームスペースの場所に関係なく、使用されるパスは常に使用されるパスであることがリンクに通知されます。

このタイプのリンクが作成されると、ONTAP のデフォルトの動作が異なります。

次の例は、NFSマウントの絶対パスを使用して、ボリュームのルートにリンクを作成し、同じボリューム内の深さが3レベルのフォルダにリダイレクトします。

- 絶対フォルダパス `/mnt/client1/dir1/dir2/linked-dir`はです。
- このリンクは、NFSマウントで次のコマンドを実行することで作成されます。

```
ln -s /mnt/client1/dir1/dir2/linked-dir abs-link
```

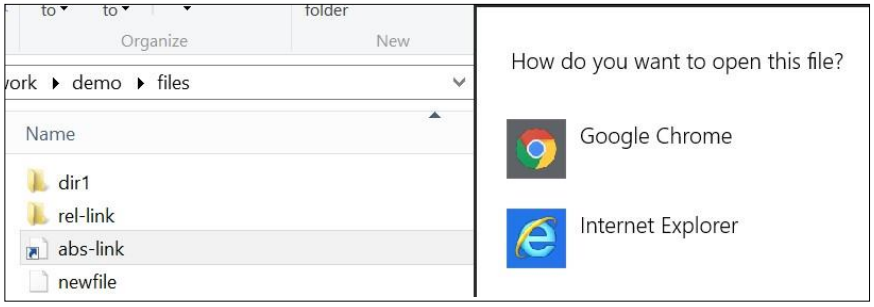
そのリンクが作成されると、NFSから想定される結果が表示されます。絶対パスsymlink ()とabs-linkフォルダパスdir1/dir2/linked-dir/） の両方(同じファイルを表示)

```
# touch abs-link/abs-link-file
# ls -la abs-link/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 17:04 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 17:04 abs-link-file
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file

# ls -la dir1/dir2/linked-dir/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 17:04 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 17:04 abs-link-file
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file
```

ただし、CIFS / SMB共有からは、どこにもリダイレクトされないショートカットファイルがあります。そのファイルを開く方法を尋ねるプロンプトが表示されます。

注： シンボリックリンクの表示方法（ショートカットまたはファイルやディレクトリとして）は、使用しているSMBのバージョンによって異なります。シンボリックリンクは、「ジャンクションパスとリパースポイント」で説明されているオプションによって制御されます。

図17）CIFSシンボリックリンク、絶対パス、同じボリューム-デフォルト動作

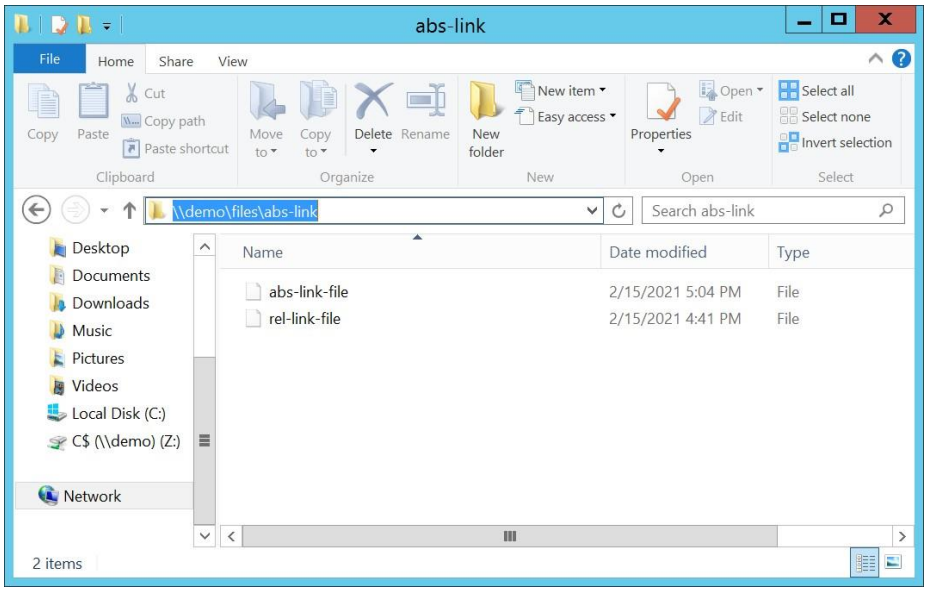


このディレクトリ内のリンクがシンボリックリンクであることをONTAP に通知するには、次のコマンドを実行してCIFSシンボリックリンクパスを定義します。

```
cluster::> cifs symlink create -vserver DEMO -unix-path /mnt/client1/ -cifs-path / -cifs-server
DEMO -locality local -share-name files
```

この例 `-unix-path (/mnt/client1`では、シンボリックリンクを作成したNFSクライアントのマウントパスを使用してが定義されています。ファイル `-locality`は同じボリュームにあるため、値として「local」を使用します。NFSクライアントがアンマウントされていても、ONTAPはCIFS共有内のリンクのリダイレクト方法を認識しています。

図18）CIFSシンボリックリンク、絶対パス-同じボリューム



CIFSシンボリックリンク：別のボリューム/共有（widelink）

次に、同じネームスペース内のボリューム間でリンクする必要があります。各ボリュームは、NASクライアントにとって一意のファイルシステムとみなされるため、これは重要な手順です。これらのボリュームへのリンク方法は、少し異なる方法で扱う必要があります。

この例では、別のNFSマウントの絶対パスを使用して、別のボリュームの深さが3レベルのフォルダにリダイレクトするボリュームのルートにリンクを作成します。ディレクトリツリーで上位のパスを使用しないかぎり、ここでは相対パスを使用しないでください。使用しているディレクトリと同じディレクトリを使用しますが、リンクは別のボリュームに存在します。

- リンクされたボリュームの絶対フォルダパスは /mnt/client1/dir1/dir2/linked-dirです。
- client1 client2 NFSマウントで次のコマンドを実行し、マウントへのリンクを作成します。

```
ln -s /mnt/client1/dir1/dir2/linked-dir remote-link
```

マウントされている2つのボリュームを次に示します。

```
# mount | grep client
DEMO:/files on /mnt/client1 type nfs
DEMO:/flexgroup_16 on /mnt/client2 type nfs
```

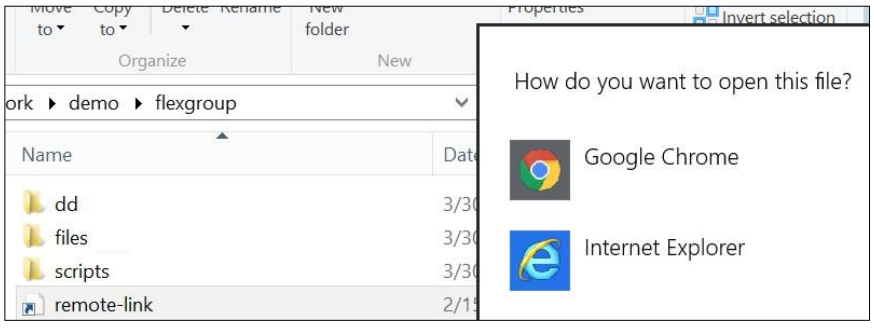
そのリンクが作成されると、NFSから想定される結果が表示されます。リモートシンボリックリンク（remote-link）とフォルダパス（/mnt/client1/dir1/dir2/linked-dir/）シンボリックリンクパスから作成されたファイルと同じファイルを表示します）の両方。

```
# touch /mnt/client2/remote-link/remote-file
# ls -la remote-link/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 17:32 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 17:04 abs-link-file
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file
-rw-r--r-- 1 root root    0 Feb 15 17:32 remote-file

# ls -la /mnt/client1/dir1/dir2/linked-dir/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 17:32 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 17:04 abs-link-file
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file
-rw-r--r-- 1 root root    0 Feb 15 17:32 remote-file
```

デフォルトでは、SMBクライアント上のCIFS共有には、どこにもリダイレクトされないショートカットファイルが表示されます。

注： シンボリックリンクの表示方法（ショートカットまたはファイルやディレクトリとして）は、使用しているSMBのバージョンによって異なります。シンボリックリンクは、「ジャンクションパス とリパースポイント」で説明されているオプションによって制御されます。

図19）CIFSシンボリックリンク、絶対パス、ボリュームごとのデフォルト動作



この場合も、ONTAP にリダイレクト先を通知する必要があります。上記の例 -unix-path /mnt/client1では、と定義したシンボリックリンクパスを作成しています。このシンボリックリンクはを指し /mnt/client1/mnt/client2ていますが、にあるため、ONTAP にパスのリダイレクト先を通知する新しいCIFSシンボリックリンクエントリが必要です。

複数のファイルシステムにまたがっているため、このタイプのリンクはワイドリンクと見なされます。階層化の使用率しきい値を変更するには、次のコマンドを実行します。

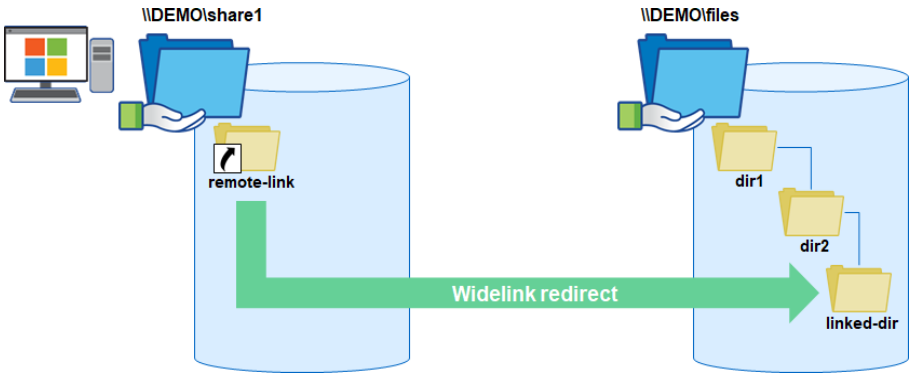
```
cluster::*> cifs symlink modify -vserver DEMO -unix-path /mnt/client1/ -locality widelink
```

また、ソースとデスティネーション symlinks_and_widelinks -symlink-propertiesの両方のCIFS共有でが有効になっている必要があります。シンボリックリンクパス -symlink-properties をワイドリンクとして定義していて、ワイドリンクに変更しない場合は、既存のリンクが解除されます（以前に作成した絶対パスリンクなど）。

このCIFSシンボリックリンクマッピングは、ONTAP のリダイレクト方法です。

```
cluster::*> cifs share modify -vserver DEMO -share-name source -symlink-properties
symlinks_and_widelinks

cluster::*> cifs share modify -vserver DEMO -share-name destination -symlink-properties
symlinks_and_widelinks
```

図20）CIFSワイドリンクリダイレクト-同じSVM



マッピングが完了すると、リンクは、適切なリンク先に正しくリダイレクトされるショートカットフォルダーまたは通常のフォルダー（ショートカットファイルではありません）として表示され、参照しているファイルが表示されます。

注： シンボリックリンクの表示方法（ショートカットまたはファイルやディレクトリとして）は、使用しているSMBのバージョンによって異なります。シンボリックリンクは、「ジャンクションパスとリパースポイント」で説明されているオプションによって制御されます。

図21）CIFSシンボリックリンク-設定前と設定後

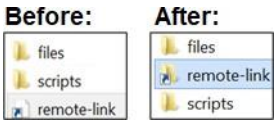
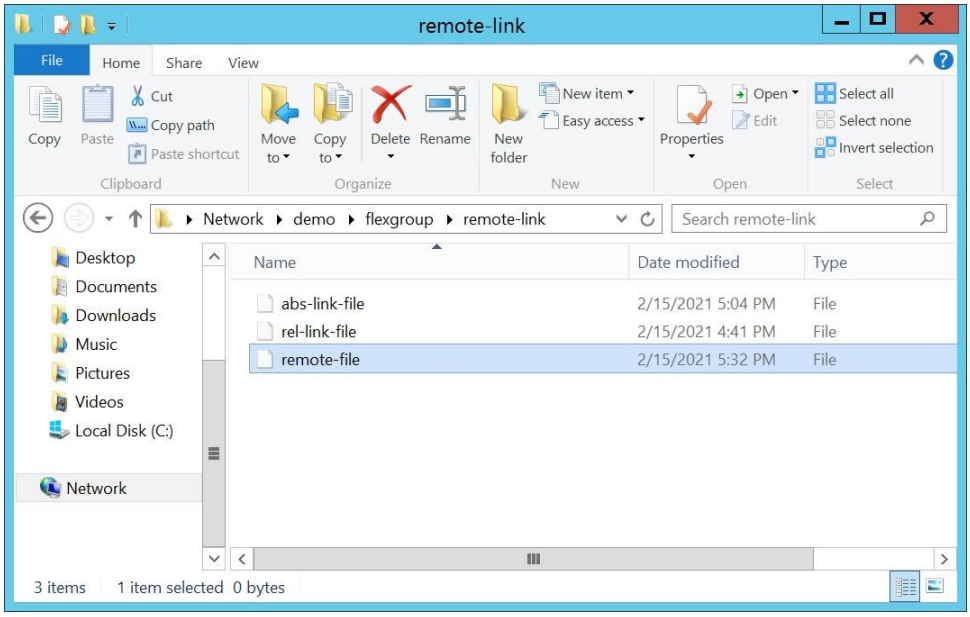


図22）CIFSシンボリックリンク、別のボリューム/同じSVM-ワイドリンク



CIFSシンボリックリンク：ネットアップ以外のCIFS共有（widelink）

ONTAP では、ONTAP ストレージシステムでホストされていないCIFS / SMBサーバにリダイレクトするCIFSシンボリックリンクを設定することもできます。つまり、ONTAPは、Windowsサーバと同様にDFSネームスペースとして機能します。

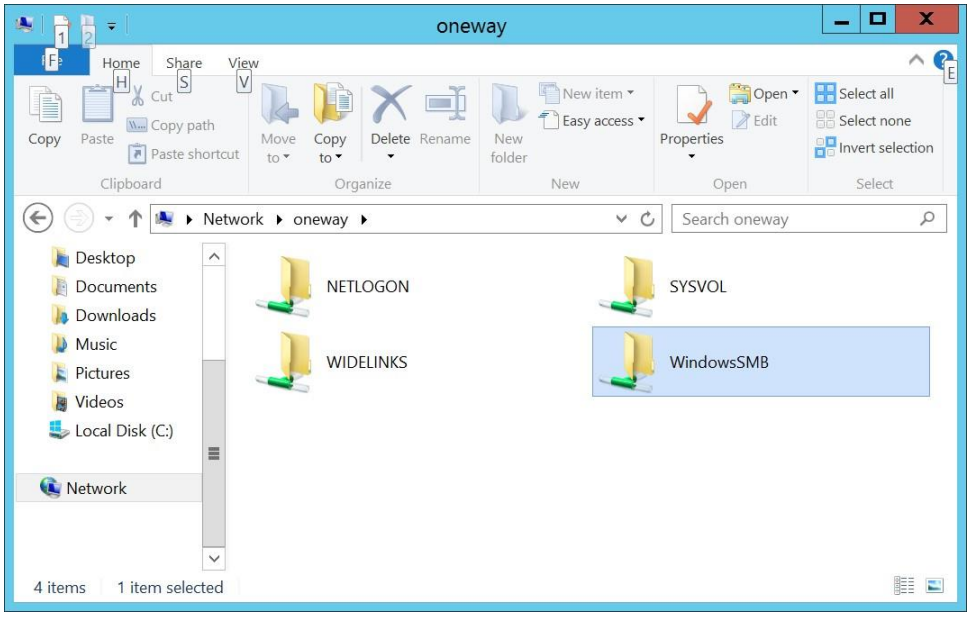
この例では、Windowsサーバでホストされ ているCIFS共有を指すONTAP ボリュームでホストされているCIFSシンボリックリンクを使用します。これはWindowsサーバであるため、NFSクライアントからのシンボリックリンクはテストできませんが、前のセクションで説明したのと同じ概念を利用して、SMBサーバ間に作業用のワイドリンクを作成することができます。

- `-unix-path` リンクされたWindows共有のは `/mnt/winclient/WindowsSMB/` です。
- `client1 client2` NFSマウントで次のコマンドを実行し、マウントへのリンクを作成します。

```
ln -s /mnt/winclient/WindowsSMB/WindowsSMB-link win-widelink
```

Windowsサーバで作成 `ONEWAY.NTAP.LOCALONEWAY` されたWindows共有の名前は、です。つまり、CIFSサーバ名はです。

図23）WindowsサーバのSMB共有



このWindowsサーバのCIFSシンボリックリンクパスを作成するには、次のコマンドを実行します。シンボリックリンク `-symlink-property symlinks_and_widelinks -locality widelink`が配置されているONTAP SVM上のCIFS / SMB共有では、値が設定されていて、に設定されている必要があります。

```
cluster::*> cifs symlink create -vserver DEMO -unix-path /mnt/winclient/WindowsSMB/ -cifs-path /
-cifs-server ONEWAY -locality widelink -share-name WindowsSMB

cluster::*> cifs share show -vserver DEMO -symlink-properties symlinks_and_widelinks -fields
symlink-properties
vserver share-name symlink-properties
------- ---------- ----------------------
DEMO    files      symlinks_and_widelinks
DEMO    flexgroup  symlinks_and_widelinks
```

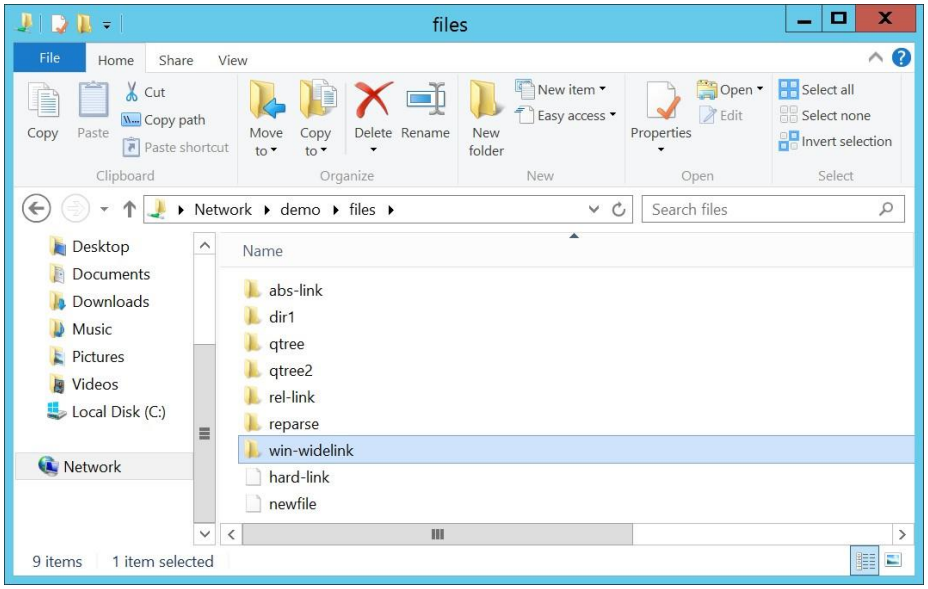
`cifs symlink` このコマンドの構成は次のとおりです。

- `-unix-path` パス（/mnt/winclient/WindowsSMB/はシンボリックリンクの作成に使用されます）。
- `-cifs-path`は/に設定されています。これにより、ナビゲーションが開始されます。
- `-cifs-server`は、デスティネーションCIFS / SMBサーバの名前です。この例では、Windowsサーバ名ONEWAYはです。
- `-locality`は、ファイルシステムを通過するワイドリンクです。
- `-share-name`は、デスティネーションのCIFS / SMB共有の名前です。WindowsSMB

CIFSシンボリックリンクパスを作成したら、新しく作成したシンボリックリンクに移動します。そこから、ショートカットアイコンまたはフォルダーアイコンが表示されます。

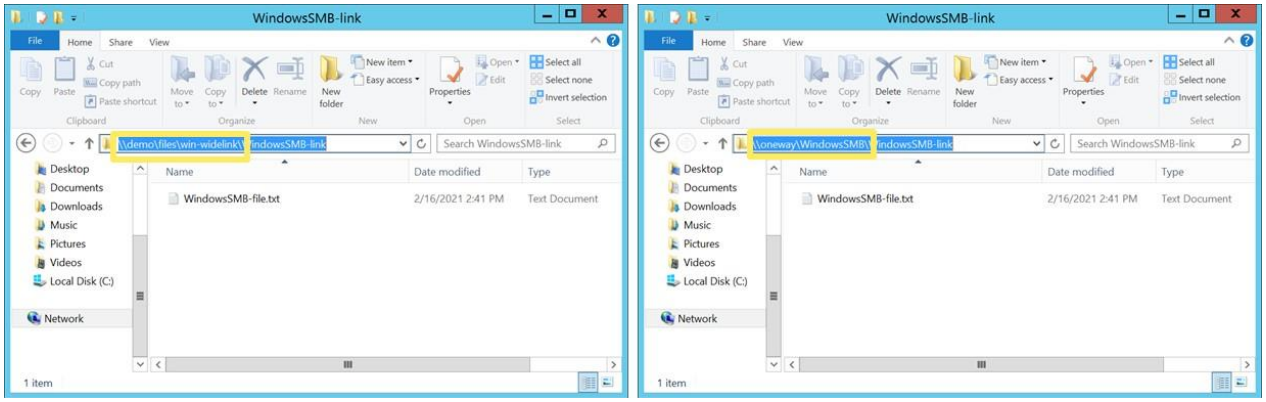
注： シンボリックリンクの表示方法（ショートカットまたはファイルやディレクトリとして）は、使用しているSMBのバージョンによって異なります。シンボリックリンクは、「ジャンクションパス とリパースポイント」で説明されているオプションによって制御されます。

図24）CIFSシンボリックリンク-Windowsサーバへのワイドリンク



widelinkフォルダに移動すると、Windows SMB共有に直接アクセスした場合と同じ内容が表示されます。

図25）CIFSシンボリックリンクとWindows SMB共有への直接接続



Windowsクライアントから `dfsutil diag`は、次のパス解決が表示されます。

```
C:\>dfsutil diag viewdfspath \\demo\files\win-widelink

The DFS Path <\\demo\files\win-widelink> resolves to -> \\ONEWAY\WindowsSMB
```

注： この手順は、DFSリファーラルをサポートするすべてのCIFS / SMBサーバに対して機能します。次のセクションでは、dfsutilの使用方法について詳しく説明します。

CIFSシンボリックリンク：ローカルファイルへのリンク

CIFS / SMBクライアントがファイルとして認識できるファイルを指すシンボリックリンクを作成することもできます。これらのシンボリックリンクを作成するには、次の要件を満たしている必要があります。

- UNIX / NFSでファイルへのシンボリックリンクが作成されました。
- `-locality ローカル`を使用するONTAP のCIFSシンボリックリンクパス。

- が -symlink-properties symlinks のCIFS共有は、または symlinks_and_widelinksに設定されます。
- 設定に応じ -symlink-properties no_strict_security て、オプションは省略可能です。

次の例は、NFS経由で作成されたファイルのシンボリックリンクです。このシンボリックリンクは、リンク先のファイルと同じボリュームに存在します。

```
# ls -la | grep file-symlink
lrwxrwxrwx   1 root root              45 Feb 18 10:12 file-symlink.txt ->
/mnt/client1/dir1/dir2/linked-dir/linked-file
# pwd
/mnt/client1

# cat file-symlink.txt
This is a file symlink.

# cat /mnt/client1/dir1/dir2/linked-dir/linked-file
This is a file symlink.
```

次の例は、ONTAP のCIFSシンボリックリンクパスを示しています。

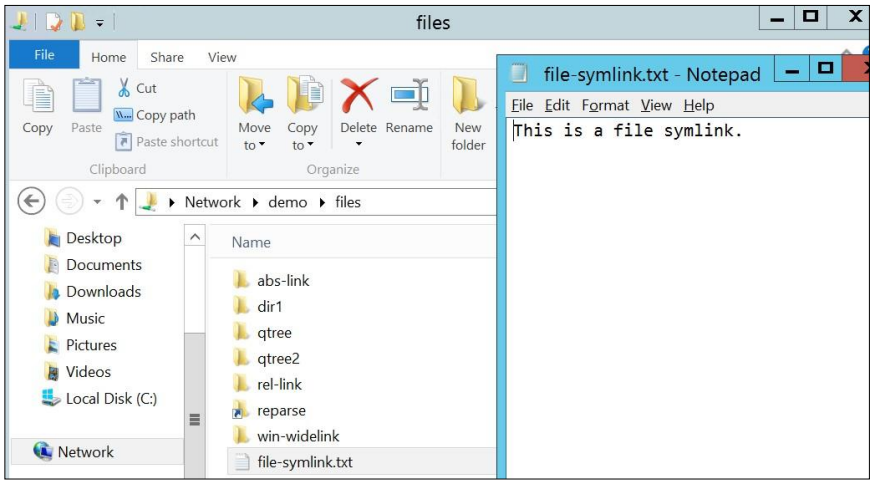
```
cluster::*> cifs symlink show -vserver DEMO -unix-path /mnt/client1/

                  Vserver: DEMO
                UNIX Path: /mnt/client1/
               CIFS Share: files
                CIFS Path: /
Remote NetBIOS Server Name: DEMO
     Local or Wide Symlink: local
            Home Directory: false
```

CIFS共有 -symlink-properties の値：

```
cluster::*> cifs share show -vserver DEMO -share-name files,flexgroup -fields symlink-properties
vserver share-name symlink-properties
---------- ---------- ----------------------------
DEMO     files      symlinks_and_widelinks
```

上記の手順 を使用すると、シンボリックリンクファイルがSMBクライアントに表示されます。

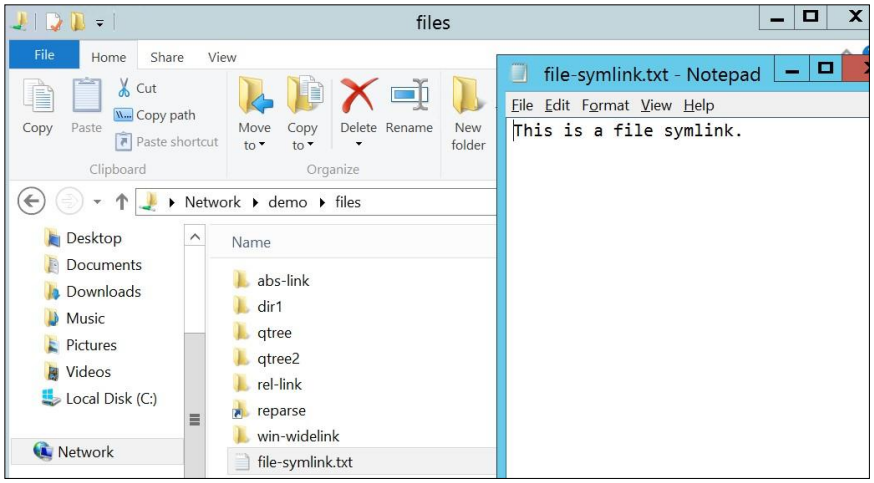
図26）ローカルファイルのシンボリックリンク-ローカルのローカリティ、symlinks_and-widelinks共有プロパティ



CIFS共有 -symlink-properties の値 no_strict_securityをに変更しても、ローカルシンボリックリンクは引き続き機能します。

```
cluster::*> cifs share modify -vserver DEMO -share-name files -symlink-properties
symlinks,no_strict_security
```

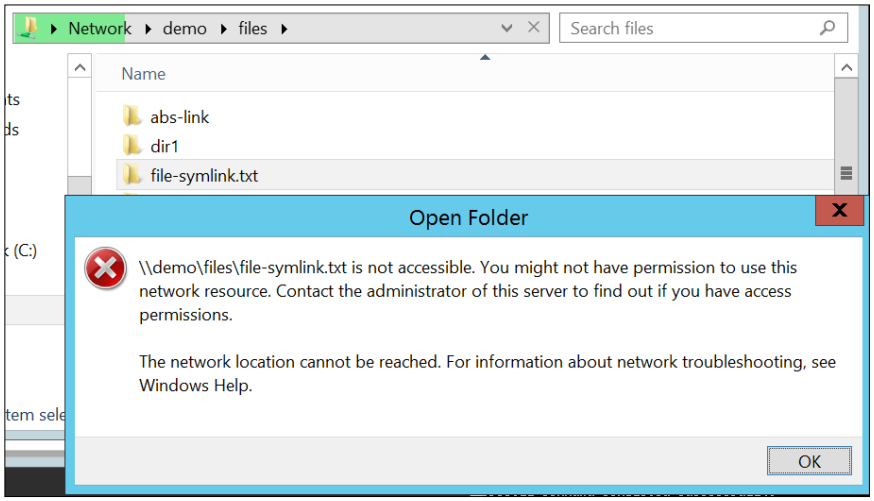
図27）ローカルファイルのシンボリックリンク-ローカルのローカリティ、シンボリックリンク、no_strict_security共有プロパティ



シンボリックリンクのパス `-locality` をwidelinkに変更すると、Windowsではシンボリックリンクがフォルダとして表示され、ファイルが適切に開かれません。

```
cluster::*> cifs symlink modify -vserver DEMO -unix-path /mnt/client1/ -locality widelink
```

図28）ローカルファイルのシンボリックリンク-widelinkのローカリティ、symlinks_and-widelinks共有プロパティ



Widelinkエントリには次の制約があります。

- widelinkのリンク先がファイルであっても、ディレクトリの一覧にはディレクトリとして表示されます。
- ファイルを開くシステムAPIはwidelinkのリンクを正しく参照しますが、一部のアプリケーションでは混乱が発生する場合があります。この問題を回避するには、ファイルではなくディレクトリを参照するwidelinkを作成します。
- widelinkでは、リンク先マシンの非共有領域にクライアントをリダイレクトすることはできません。

CIFS symlink：リモートファイルにリンクします

「CIFS symlink：ローカルファイルへのリンク」に示すように、同じボリューム内のファイルにリンクするファイルシンボリックリンクを作成するのは簡単です。

ただし、ボリュームの範囲から離れたファイルにリンクする場合は、いくつかの課題があります。

- ボリューム境界を残したシンボリックリンクは、一般にワイドリンクとみなされます。
- SMBクライアントではワイドリンクがディレクトリとして表示されます。

では、ファイルとして表示されるファイルのシンボリックリンクを作成し、別の共有にリダイレクトする方法はありますか。

次の2種類の形式がある：

- ジャンクションされたボリュームが含まれるフォルダのルートにCIFSシンボリックリンクマッピングを作成し、./to redirect up the file path to the top level of the directoryを使用します。ユーザが共有から移動することはありません。
- 目的のファイルへの絶対パスを使用する、デスティネーション共有へのCIFSシンボリックリンクマッピングを作成します。ユーザはシンボリックリンクを介して共有をトラバースします。

図29に、これらの各オプションを示します。

図29）ジャンクションされたボリュームおよび./symlinkパスを使用した、共有のルートからのシンボリックリンク

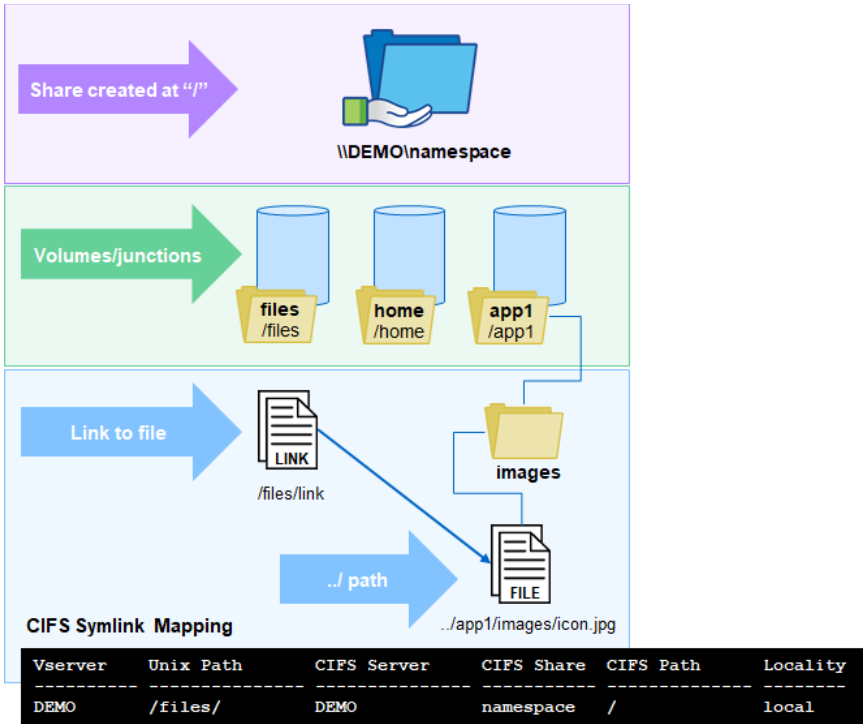
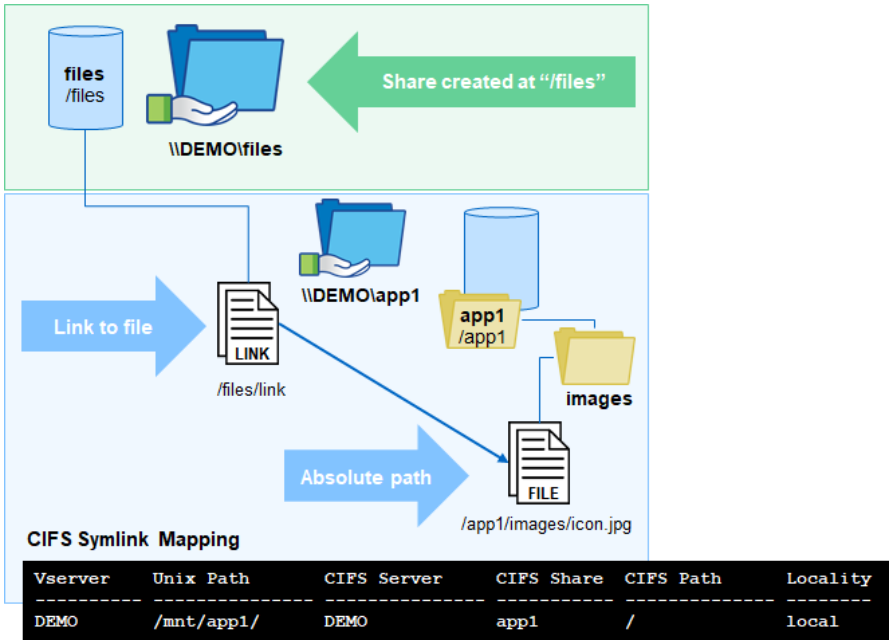


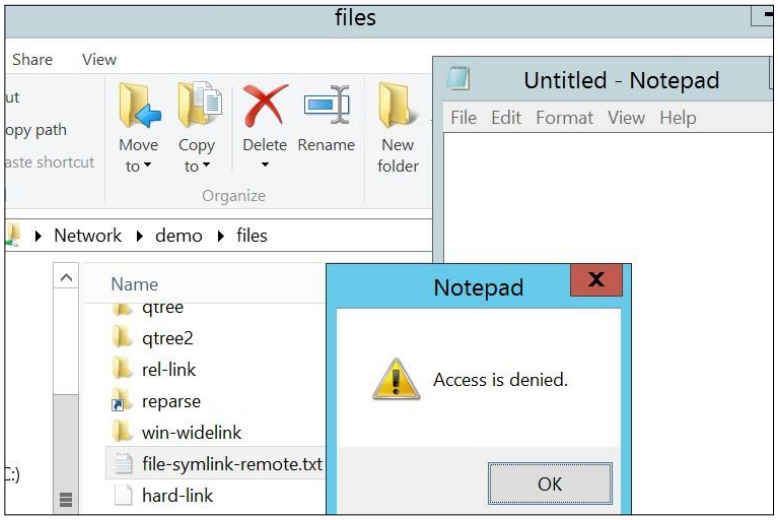
図30）リダイレクトによる共有から別の共有へのシンボリックリンク-絶対パス



ファイルのシンボリックリンクに問題がある可能性があります

場合によっては、ファイルのCIFSシンボリックリンクマッピングを作成したあとに問題が発生することがあります。このセクションでは、発生する可能性のある問題とその潜在的な原因について説明します。

図31）リモートファイルのシンボリックリンク-ローカルのローカリティ、symlinks_and-widelinks共有プロパティ



Access Deniedメッセージ

SMBクライアントからファイルへのシンボリックリンクを開いたときにアクセス拒否が表示される場合は、次の点を確認してください。

- シンボリックリンクのACL
- デスティネーションSVMノACLs LIF
- デスティネーションSVMノACLs LIF

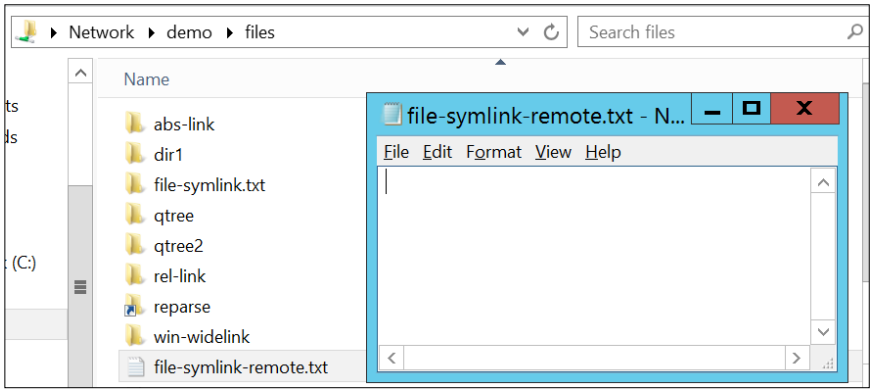
- シンボリックリンクはNFSクライアントから機能していますか。
- CIFSシンボリックリンクマッピングパス設定：
  - 共有名は正しいですか？
  - UNIXエントリが正しいか。
  - 相対パスまたは絶対パスを使用していますか？
  - ローカルをローカリティとして使用していますか？
- cifs share -symlink-properties
  - no_strict_securityは使用されていますか？

注 `no_strict_security` ：一部のSMB適用を削除することで、共有間でシンボリックリンクが機能するようにします。

空のファイルです

場合によっては、CIFSクライアントからシンボリックリンクを開くことはできても、ファイル内に予想されるコンテンツがないことがあります。

図32）リモートファイルのシンボリックリンク-空のファイル、no-strict_security



この問題 が発生した場合は、次の点を確認してください。

- シンボリックリンクはNFSクライアントから機能していますか。
- CIFSシンボリックリンクマッピングパス設定：
  - 共有名は正しいですか？
  - シンボリックリンク内のUNIXパスのパスマッピングが存在するか。
  - UNIXエントリが正しいか。
  - 相対パスまたは絶対パスを使用していますか？
  - ローカルをローカリティとして使用していますか？
- CIFS共有の-symlink-properties：
  - `no_strict_security` 使用済みかどうか

注 `no_strict_security` ：一部のSMB適用を削除することで、共有間でシンボリックリンクが機能するようにします。パスが正しくマッピングされていない場合は、空のファイルが表示されます。

no-strict_security、シンボリックリンク、およびDFS通知

CIFSシンボリックリンクパスを作成する場合、シンボリックリンクが共有の境界を離れるように設定されている場合、または単にDFSをアドバタイズしないで定義されたパスをシンボリックリンクがたどるように、ONTAP がDFSを使用してアドバタイズするかどうかを制御できます。

-symlink-path CIFS共有のnoというオプション_strict_security を使用すると、この動作を制御できます。

このオプション -locality FSCTL_DFS_GET_REFERRALS を無効にする（設定しない）場合、CIFSシンボリックリンクパスがwidelinkに設定されていると、CIFS / SMBクライアントからストレージシステムに送信され、ストレージシステムがDFS経由でパスをアドバタイズしているかどうかが確認されます。

パケットキャプチャでは、DFS通知を使用すると次のパケットが表示されます。Packet from SMB

client：

```
1247    13.520643      x.x.x.x   x.x.x.y      SMB2    230     Ioctl Request
FSCTL_DFS_GET_REFERRALS, File: \demo\files\win-widelink
File Name: \demo\files\win-widelink
```

ONTAP からの応答パケット：

```
1248    13.521286      x.x.x.y   x.x.x.x      SMB2    382     Ioctl Response
FSCTL_DFS_GET_REFERRALS
Path: \demo\files\win-widelink
Alt Path: \demo\files\win-widelink
Node: \ONEWAY\WindowsSMB\WindowsSMB-link
```

一部のアプリケーションではDFS通知を無効にする必要がありますが、シンボリックリンクをトラバースできる必要があります。この例では、共有のDFS通知を無効にします。

DFS経由でアドバタイズされないCIFSシンボリックリンクパスマッピングを作成するには、次の手順を実行します。

1. NFSクライアント上に、通常どおりシンボリックリンクを作成します。
2. -locality ローカル -share 値と[デスティネーション共有名]値を使用するシンボリックリンクパスを作成してください。
3. でシンボリックリンクに使用するパスを使用 -unix-pathします。
4. -symlink-properties no_strict_security ソース共有でsymlinksにを設定します。

次 flexgroup filesの例では、というCIFS共有が、CIFS共有にリダイレクトされる共有のルートにあるシンボリックリンクとなります。

次 /mnt/xyzの例では、シンボリックリンクが参照しています。

```
# ln -s /mnt/xyz nostrict-link
# cd nostrict-link/
# ls -la
total 8
drwxr-xr-x 2 root root 4096 Feb 18 13:15 .
drwxr-xr-x 6 root root 4096 Feb 18 13:15 ..
lrwxrwxrwx 1 root root    8 Feb 18 13:15 xyz -> /mnt/xyz
```

次の例は、CIFSシンボリックリンクパスマッピングを示しています。

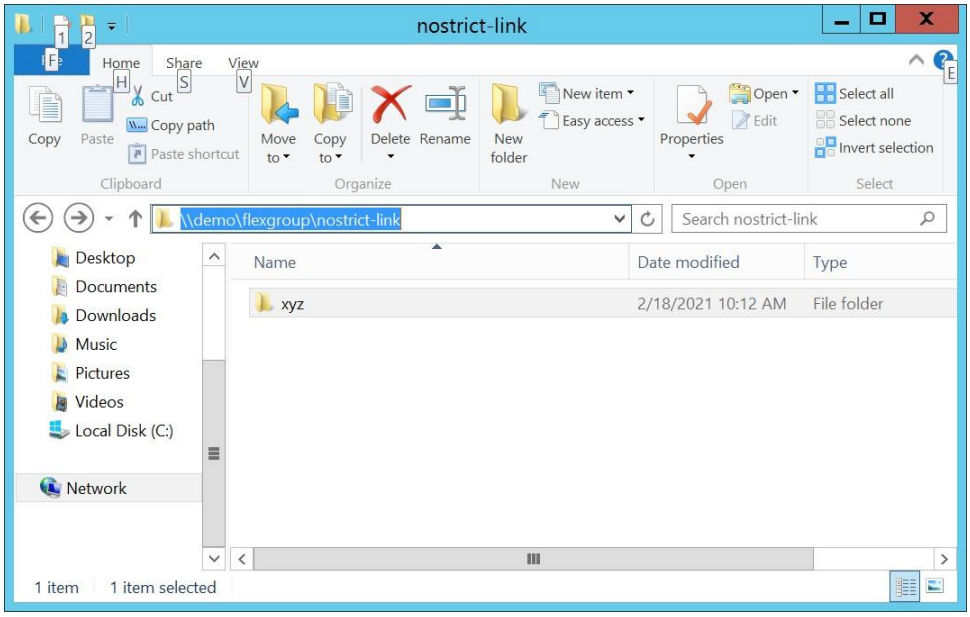
```
cluster::*> cifs symlink create -vserver DEMO -unix-path /mnt/xyz/ -cifs-path / -cifs-server DEMO
-locality local -home-directory false -share-name files
```

次の例は、CIFSのshare-symlink-propertiesを表示します。

```
DEMO     flexgroup symlinks,no_strict_security
```

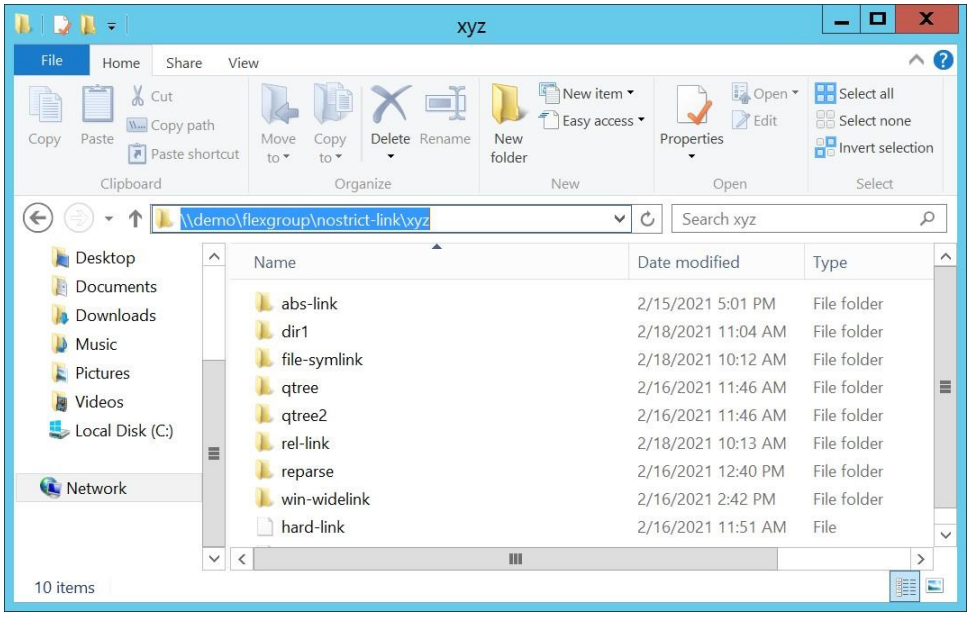
次の例は、CIFSでのシンボリックリンクの表示方法を示しています。

図33）CIFSシンボリックリンク-no_strict_security



このフォルダに移動すると、共有ファイルが表示されます。

図34）CIFSシンボリックリンク-no_strict_securityナビゲーション



クライアントがパスを確認する方法は次のとおりです。

```
C:\>dfsutil diag viewdfspath \\demo\flexgroup

<\\demo\flexgroup> is not a DFS Path
Could not complete the command successfully.
SYSTEM ERROR - The system cannot find the file specified.

C:\>dfsutil diag viewdfspath \\demo\flexgroup\nostrict-link

<\\demo\flexgroup\nostrict-link> is not a DFS Path
```

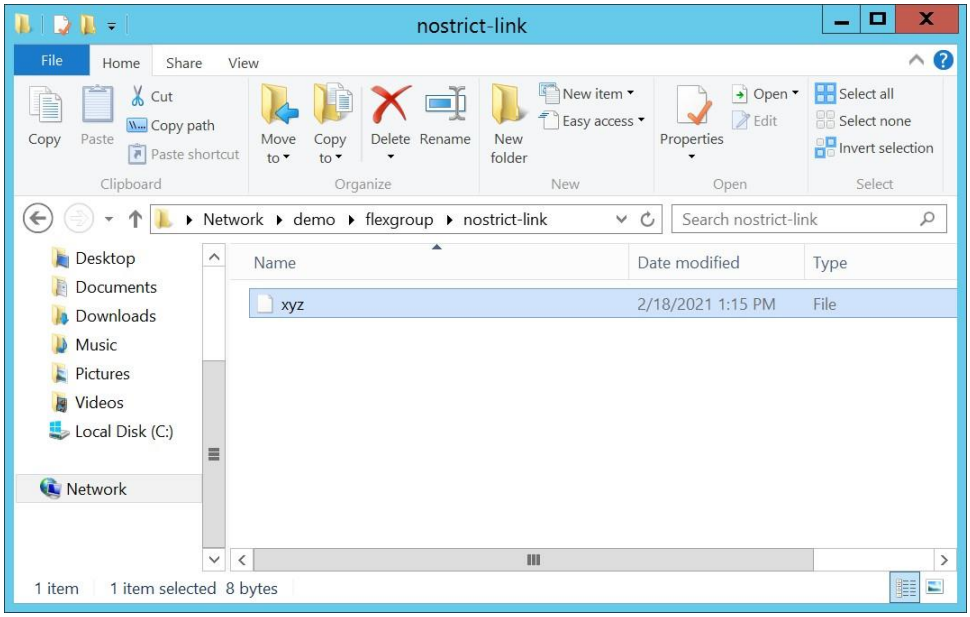
```
Could not complete the command successfully.
SYSTEM ERROR - The system cannot find the file specified.


C:\>dfsutil diag viewdfspath \\demo\flexgroup\nostrict-link\xyz

<\\demo\flexgroup\nostrict-link\xyz> is not a DFS Path
Could not complete the command successfully.
SYSTEM ERROR - The system cannot find the file specified.
```

クライアントがDFSリファーラルを要求 STATUS_NOT_FOUNDすると、ONTAPはと応答します。

```
453     5.681603        x.x.x.x x.x.x.y SMB2    212     Ioctl Request FSCTL_DFS_GET_REFERRALS, File:
\demo\flexgroup
454     5.681805        x.x.x.y x.x.x.x SMB2    131     Ioctl Response, Error: STATUS_NOT_FOUND
```

no_strict_security が設定されていない場合、リンクはファイルとして表示され、トラフィックをリダイレクトしません。このリンクを設定せずに使用 no_strict_security- locality -symlink-properites symlinks_and_widelinksするには、CIFSシンボリックリンクパスマッピングをwidelinkに変更し、CIFS共有をに変更する必要があります。

図35）CIFSシンボリックリンク-no_strict_security no set



CIFSシンボリックリンク、mtime動作、およびno_strict_security

CIFSシンボリックリンクは技術的なシンボリックリンクではなく、ONTAP によって制御されるパスマッピングを使用した、リパースポイント/パスのリダイレクトです。ONTAP におけるCIFSシンボリックリンクの動作が、SMBクライアントによるファイル、フォルダ、およびシンボリックリンクのmtime値の表示に及ぼす影響、およびデフォルトの動作では、ターゲットのmtimeではなく、symlinkのmtimeが表示されます。ONTAP を使用 -symlink-properties したCIFSシンボリックリンクのmtime動作は、DFS通知によって制御されます。共有のオプションにno_strict_securityを使用することによって動作を変更できます。

次に、マウント処理の例を示します。

```
lrwxrwxrwx 1 root root    8 Feb 18 13:15 xyz -> /mnt/xyz
```

/mnt/xyz \\DEMO\files\dir1\dir2 このCIFSシンボリックリンクマッピングを介したwidelinkを使用して、ONTAP パスをCIFSパスにマッピングするように指示されました。

```
cluster::*> cifs symlink show -vserver DEMO
```

```
Vserver     Unix Path        CIFS Server      CIFS Share CIFS Path        Locality
----------- ---------------- ---------------- ---------- ---------------- -----------
DEMO        /mnt/xyz/        DEMO             files      /dir1/dir2/      widelink
```

シンボリックリンクはFlexGroup CIFS共有に存在します。そのため、異なるボリュームターゲット（ファイルCIFS共有）があります。symlinks_and_widelinks その結果、が-として使用symlink-propertiesされました。

```
cluster::*> cifs share show -vserver DEMO -share-name files,flexgroup -fields symlink-properties
vserver share-name symlink-properties
------- ---------- ----------------------------------------------------------------------------
DEMO    files      symlinks_and_widelinks
DEMO    flexgroup  symlinks_and_widelinks
```

クライアントはDFS通知を確認します。これがリダイレクトパスです。

```
C:\>dfsutil diag viewdfspath \\demo\flexgroup\nostrict-link\xyz

The DFS Path <\\demo\flexgroup\nostrict-link\xyz> resolves to -> \\demo\files\dir1\dir2
```

この設定では、シンボリックリンクのmtimeはデスティネーションディレクトリのmtimeとは異なります。これにより、動作のためにmtimeに依存する一部のアプリケーションで原因 の問題が発生する可能性があります。次の例では、ディレクトリmtimeが2021年2月18日の午後12時55分で、symlink mtimeが2021年2月18日の午後1時15分です。

```
C:\>dir /T:W \\demo\files\dir1\  Volume
 in drive \\demo\files is files Volume
 Serial Number is 80F0-4459

 Directory of \\demo\files\dir1

02/18/2021  11:04 AM    <DIR>          .
02/23/2021  11:11 AM    <DIR>          ..
02/18/2021  12:55 PM    <DIR>          dir2 <<< this is the target directory


C:\>dir /T:W \\demo\flexgroup\nostrict-link\ Volume
 in drive \\demo\flexgroup is flexgroup Volume
 Serial Number is 80F0-3768

 Directory of \\demo\flexgroup\nostrict-link

02/18/2021  01:15 PM    <DIR>          .
02/18/2021  01:15 PM    <DIR>          ..
02/18/2021  01:15 PM    <DIR>          xyz <<< this is the name of the symlink
```

リンク no_strict_security とディレクトリの同じmtimeを確認するには、その共有のDFS通知を無効にし、代わりにリンクのリダイレクトオプションを使用します。詳細については、「No_strict_security、symlinksおよびDFS通知」を参照してください。「次の例は、このシンボリックリンクの例が、同一のシンボリックリンクおよびターゲットディレクトリのmtime値を表示するように設定されている方法を示しています。

上記のシナリオを正常に機能させるには、次の手順を実行します。

1. CIFS共有をに変更 -symlink-property symlink,no_strict_securityします。
2. CIFSシンボリックリンクのマッピング -locality 値をに変更 localします。
3. クライアント上でDFSキャッシュをフラッシュして、net useキャッシュを使用します。

dfsutilからパスがアドバタイズされなくなりました。

```
C:\>dfsutil diag viewdfspath \\demo\flexgroup\nostrict-link\xyz

Destination Path <\\demo\flexgroup\nostrict-link\xyz> is inaccessible
Could not complete the command successfully.
SYSTEM ERROR - The network location cannot be reached. For information about network
troubleshooting, see Windows Help.
```

デスティネーションディレクトリの値のみを使用した場合、シンボリックリンクとディレクトリのmtimesが同一になります。

```
C:\>dir /T:W \\demo\flexgroup\nostrict-
 link\ Volume in drive \\demo\flexgroup is
 flexgroup Volume Serial Number is 80F0-3768

 Directory of \\demo\flexgroup\nostrict-link

02/18/2021  01:15 PM    <DIR>          .
02/18/2021  01:15 PM    <DIR>          ..
02/18/2021  12:55 PM    <DIR>          xyz


C:\>dir /T:W \\demo\files\dir1\dir2 Volume
 in drive \\demo\files is files Volume
 Serial Number is 80F0-4459

 Directory of \\demo\files\dir1\dir2

02/18/2021  12:55 PM    <DIR>          .
02/18/2021  11:04 AM    <DIR>          ..
02/18/2021  12:55 PM                12 nostrict-link
```

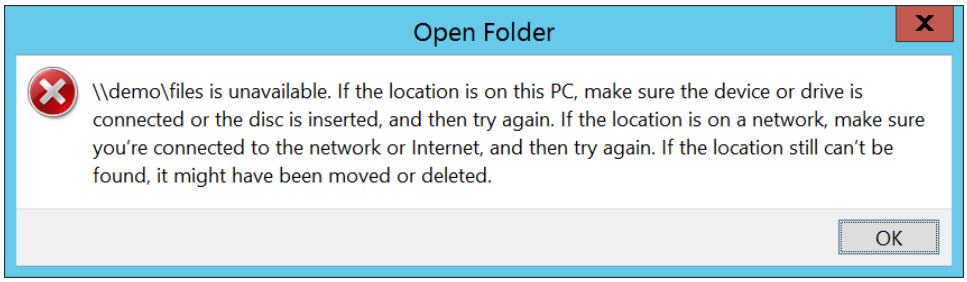
注： シンボリックリンクとターゲットに異なるmtimesを表示するには、widelinkを使用する必要があります。ただし、ファイルを参照している場合、SMBクライアントではワイドリンクが一貫して機能しないため、ディレクトリのみをポイントします。

キャッシュおよびシンボリックリンクのエラー

CIFSシンボリックリンクの設定時に、正しいパスマッピングが見つかったためにリンクの移動やCIFS共有へのアクセスで問題が発生することがあります。この問題 では、有効な問題が混在する検出漏れや誤検出が発生する可能性があるため、正しい設定について原因 で混乱することがあります。

たとえば、正常に動作していたCIFS / SMB共有にアクセスしようとすると、図36に示すエラーメッセージが表示されることがあります。

図36）CIFS共有へのアクセスエラー



これらのエラーの大部分は、SMB共有パスのクライアント側とONTAP側のキャッシュが原因です。その場合は、3つのメインキャッシュについて理解しておく必要があります。

dfsutilキャッシュ

シンボリックリンクでは、Windows SMBクライアントでDFSを使用してリダイレクトを行います。これらのパスをキャッシュすることで、クライアントはパスの解決に必要なネットワークトラフィック量を削減し、パフォーマンスを向上させます。ただし、キャッシュを使用すると、動作しているように見える状況や破損しているように見える状況が実際にはその逆になる場合もあります。

トラブルシューティングの際に、dfsutilコマンドセットを使用してこれらのキャッシュを表示またはフラッシュします。特に注目する必要があるのは、プロバイダキャッシュとリファーラルキャッシュです。

Dfsutil diag には、パスが解決される場所を示すコマンドフラグがあります。この例では、「cifs symlink : different volume/share（widelink）」というタイトルのセクションから、適切に設定されたwidelinkを使用しています。

```
C:\>dfsutil diag viewdfspath \\demo\flexgroup\remote-link

The DFS Path <\\demo\flexgroup\remote-link> resolves to -> <\\demo\files\dir1\dir2\linked-dir>
```

次の例は、プロバイダキャッシュにシンボリックリンクパスが入力されている場合の表示を示しています。

```
C:\>dfsutil cache provider
4 entries

Max size 16384 bytes

Current size 666 bytes

Max TTL is 15m0s

\ONEWAY.NTAP.local\sysvol [TTL 8m40s]

        UNC Provider: \Device\LanmanRedirector [Priority: 1]
        Surrogate Provider: \Device\DfsClient
\demo\IPC$ [TTL 9m55s]

        UNC Provider: \Device\LanmanRedirector [Priority: 1]
        Surrogate Provider: (null)
\demo\files [TTL 9m55s]

        UNC Provider: \Device\LanmanRedirector [Priority: 1]
        Surrogate Provider: \Device\DfsClient
\demo\flexgroup [TTL 12m13s]

        UNC Provider: \Device\LanmanRedirector [Priority: 1]
        Surrogate Provider: \Device\DfsClient
```

上記の例では、プロバイダーキャッシュはTTL情報を提供します。これは、エントリが未使用のままの場合に、そのエントリがキャッシュ内に存続する時間です。

リファーラルキャッシュの例を次に示します。

```
C:\>dfsutil cache referral
Entry: \demo\files\abs-link
ShortEntry: \demo\files\abs-link
Expires in 0 seconds
UseCount: 0 Type:0x1 ( DFS)
   0:[\DEMO\files\dir1\dir2\linked-dir] AccessStatus: 0 ( ACTIVE)

Entry: \demo\flexgroup\remote-link
ShortEntry: \demo\flexgroup\remote-link
Expires in 1651 seconds
UseCount: 0 Type:0x1 ( DFS)
   0:[\DEMO\files\dir1\dir2\linked-dir] AccessStatus: 0 ( ACTIVE)

Entry: \demo\files
ShortEntry: \demo\files
Expires in 1502 seconds
UseCount: 1 Type:0x81 ( REFERRAL_SVC DFS)
   0:[\demo\files] AccessStatus: 0 ( ACTIVE)

Entry: \demo\flexgroup
ShortEntry: \demo\flexgroup
Expires in 1639 seconds
UseCount: 1 Type:0x81 ( REFERRAL_SVC DFS)
   0:[\demo\flexgroup] AccessStatus: 0 ( ACTIVE)
```

このリストには、リンクエントリと、リンクエントリが期限切れになるまでキャッシュに保持される期間が表示されます。は abs-link 0秒後に期限切れになります。これは、が自動的に期限切れにならないことを意味します。エントリを削除するには、キャッシュを手動でクリアする必要があります。

これらのキャッシュをフラッシュするには、次のコマンドを実行します。

```
C:\>dfsutil cache provider flush

C:\>dfsutil cache referral flush
```

ネット使用

SMBクライアントは、DFSキャッシュに加えて、SMB接続とクレデンシャルもキャッシュします。これらのキャッシュは、net useを使用して表示および管理できます。

キャッシュされたCIFS接続とSMB接続を表示するには、次のコマンドを実行します。

```
C:\>net use
```

キャッシュされた接続を個別にクリアする、またはマッピングされたドライブを切断するには、次のコマンドを実行します。

```
C:\>net use /d \\SERVER\share
C:\>net use /d Z:
```

キャッシュされたすべての接続をクリアし、すべてのマッピングされたドライブを切断するには、次のコマンドを実行します。

```
C:\>net use /d *
```

注 `dfsutil dfsutil` ：このコマンドをと組み合わせて実行すると、最初にコマンドを実行してからキャッシュをフラッシュするよりも良い結果が得られます。を実行 `net use /d` すると、CIFS / SMB共有にアクセスできない場合があります（図36を参照）。このようnet use dfsutilな場合は、Windowsエクスプローラウィンドウを閉じ、キャッシュをもう一度フラッシュし（および）、接続を再試行します。

ONTAP パスコンポーネントキャッシュ

ONTAPは、CIFS共有とシンボリックリンクの両方にパスキャッシュを提供します。これらのキャッシュは、Diagnostic Privilegeの次のCIFSサーバオプションによって制御されます。トラブルシューティングの目的でキャッシュを無効にしたり有効にしたりすることはできますが、通常の本番環境のワークロードについては、ネットアップのサポートから特に指示がないかぎり有効にしたままにしてください。

```
[-is-path-component-cache-enabled {true|false}] - Is Path Component Cache Enabled (privilege:
advanced)
This optional parameter specifies whether the path component cache is enabled. The default value
for this parameter is true.

[-is-path-component-cache-symlink-enabled {true|false}] - Is Path Component Cache Symlink
Resolution Enabled (privilege: diagnostic)
This optional parameter specifies whether the symlink resolution for the path component cache is
enabled. The default value of this parameter is true.
```

これらのキャッシュの値を設定できます。ただし、ネットアップサポートから特に指示がないかぎり、デフォルト値のままにしておきます。

```
[-path-component-cache-max-entries <integer>] - Path Component Cache Maximum Entries (privilege:
diagnostic)
This optional parameter specifies the maximum number of entries in an instance of the path
component cache. The default value of this parameter is 5000. The maximum value of this parameter
is 10000.

[-path-component-cache-entry-exp-time <integer>] - Path Component Cache Entry Expiration Time
(privilege: diagnostic)
This optional parameter specifies the maximum expiration time in milliseconds of an entry in the
path component cache. The default value of this parameter is 15000 (15 seconds). The maximum
value of this parameter is 3600000 (1 hour).

[-path-component-cache-symlink-exp-time <integer>] - Path Component Cache Symlink Expiration Time
(privilege: diagnostic)
```

```
This optional parameter specifies the maximum expiration time in milliseconds of an entry that is
a symlink in the path component cache. The default value of this parameter is 15000 (15 seconds).
The maximum value of this parameter is 3600000 (1 hour).

[-path-component-cache-max-session-token-size <integer>] - Path Component Cache Maximum Session
Token Size (privilege: diagnostic)
This optional parameter specifies the maximum session token size for the path component cache.
The default value of this parameter is 1000. The maximum value of this parameter is 10000.
```

これらのキャッシュの統計情報を有効にするには、Diagnostic Privilegeで次のコマンドを実行します。

```
cluster::*> statistics start -counter component_cache -object cifs -vserver DEMO
```

これらの統計を表示するには、次のコマンドを実行します。

```
cluster::*> statistics show -object cifs
Object: cifs
Instance: DEMO
Start-time: 2/16/2021 11:10:00
End-time: 2/16/2021 12:29:01
Elapsed-time: 4740s
Scope: DEMO
    Counter                                                     Value
-------------------------------- --------------------------------
    component_cache                                             -
                  Total Components                            166
                       Total Tests                            140
                        Total Hits                             19
                      Junction Hits                             0
                       Symlink Hits                             9
                      No Cache Miss                            51
                  Not Allowed Miss                              0
                       Expired Miss                            61
               Expired Sym Res Miss                             1
               Unresolved Junc Miss                             0
                Unresolved Sym Miss                             8
                     Total Additions                          142
              Addition Session List                           140
                       Total Purged                             0
                        Total Stale                             0
                     Total Deletions                           99
```

ジャンクションパスとリパースポイント

ONTAP は、SVMネームスペース内のジャンクションパスを使用して、同じネームスペースにマウントされたボリューム間でNASクライアントを転送します。すべてのSVMのネームスペースは、SVMルートボリューム（vsroot）から始まり、パスは「/」です。NFSクライアントは、そのパスをマウントできます。ただし、このパスがエクスポートされている場合に限ります。SMBクライアントは、CIFSの設定時にデフォルトで作成されるC$非表示共有を使用して「/」にアクセスできます。

デフォルト `is-use-junctions-as-reparse-points-enabled`では、ONTAP ジャンクションパスは、高度な権限ONTAP のCIFSオプションを使用して、リパースポイント（基本的にはシンボリックリンクまたはショートカット）として表示されます。CIFSシンボリックリンク`widelink-as-reparse-point-versions`は、SMB 1.0クライアントへのショートカットとして表示されますが、SMB 2.xクライアントおよび3.xクライアントへのディレクトリとしては、このオプションの設定によって表示されます。

ジャンクションパスとリパースポイントのオプションについては、次のデフォルト設定が用意されています。

```
cluster::*> cifs options show -vserver DEMO -fields is-use-junctions-as-reparse-points-
enabled,widelink-as-reparse-point-versions
vserver is-use-junctions-as-reparse-points-enabled widelink-as-reparse-point-versions

DEMO    true                                        SMB1
```

SMB 2.xクライアント `widelink-as-reparse-point-versions` およびSMB 3.xクライアントにシンボリックリンクがショートカットファイルとして表示されるようにするには、オプションを変更して必要なSMBバージョンを含めるようにします。

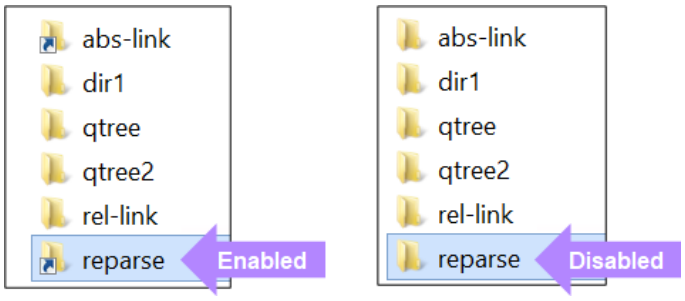
```
cluster::*> cifs options modify -vserver DEMO -widelink-as-reparse-point-versions SMB
```

```
    SMB1    SMB2    SMB2_1 SMB3    SMB3_1
```

ジャンクションパス is-use-junctions-as- reparse-points-enabledをSMBクライアントにディレクトリとして表示する場合は、を無効にします。

```
cluster::*> cifs options modify -vserver DEMO -is-use-junctions-as-reparse-points-enabled false
```

図37）ジャンクションパスのビュー：リパースポイントが有効か無効か



次 cmd の例は、オプションを有効または無効にした状態でボリュームジャンクションパスをプロンプトに表示する方法を示しています。

is-used-junctions as reparse-points-enabled true

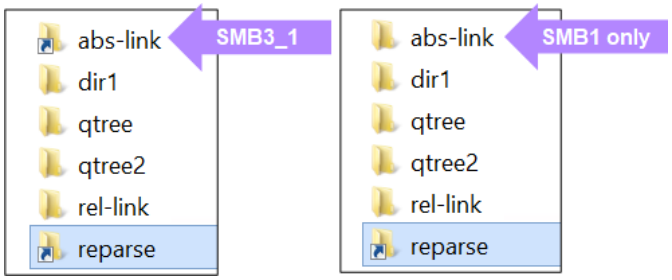
```
C:\>dir \\demo\C$
 Volume in drive \\demo\C$ is c$
 Volume Serial Number is 80F0-3712

 Directory of \\demo\C$

02/02/2021 01:09 PM    <DIR>          .
02/02/2021 01:09 PM    <DIR>          ..
07/18/2017 08:37 AM    <JUNCTION>     home [\??\Volume{80F03713-0000-0000-5879-48F200000040}\]
01/10/2019 09:25 AM    <JUNCTION>     var [\??\Volume{80F03AA7-0000-0000-5C37-55C400000040}\]
03/09/2017 11:24 AM    <JUNCTION>     flexvol [\??\Volume{80F0372F-0000-0000-58C181B200000040}\]
```

is-use-junctions as reparse-points-enabled falseを指定します

```
C:\>dir \\demo\C$
 Volume in drive \\demo\C$ is c$
 Volume Serial Number is 80F0-3712

 Directory of \\demo\C$

02/02/2021 01:09 PM    <DIR>          .
02/02/2021 01:09 PM    <DIR>          ..
07/18/2017 08:37 AM    <DIR>          home
01/10/2019 09:25 AM    <DIR>          var
03/09/2017 11:24 AM    <DIR>          flexvol
```

widelink-as-reparse-point-versions オプションは、シンボリックリンクの表示方法を制御します。図38では、SMB 3.1をアクセスプロトコルとして使用しています。abs-link smb3_1をオプションに追加した場合、シンボリックリンクはSMB 3.1クライアントからのショートカットとして表示され、オプションがデフォルトのSMB1値のままである場合はフォルダとして表示されます。

図38）シンボリックリンクビュー：有効なリパースポイントと無効



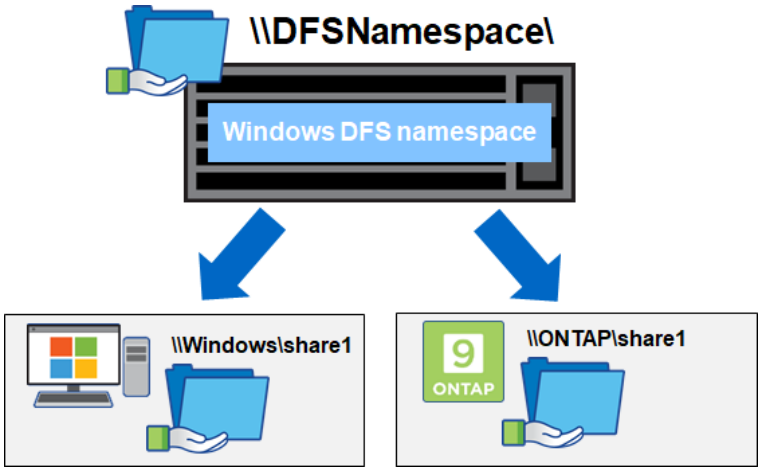
注： シンボリックリンクがリパースポイントとして設定されていないと、一部のクライアントでデスティネーションパスの適切な空きスペースが表示されない可能性があります。詳細については、「スペース不足」エラーによりCIFSシンボリックリンクボリュームに書き込むことができない」という記事を参照してください。

Distributed File Systemsの1つ

Microsoft Windowsでは、DFSと呼ばれる機能をサポートしています。この機能を使用すると、Windowsサーバは、共有の場所に関係なく、SMB共有のエンドポイントのリダイレクタとして機能します。DFSターゲットには、他のWindowsサーバ、ONTAP CIFS共有、または他のストレージ・システムCIFS共有を指定できます。この機能により、管理者は単一のネームスペースをCIFS / SMBクライアントに提示して、エンドユーザがアクセスする複数のIPアドレスやホスト名を把握していなくても移動することができます。その代わり、すべてのユーザが同じサーバに接続し、DFSによって残りの処理が行われます。

図39 に、ONTAP をターゲットとするWindows DFSを示します。

図39）ONTAP をターゲットとするWindows DFS



ONTAPはDFSターゲットとしての機能をサポートしていますが、現在のところDFS -R（レプリケーション）機能はサポートしていません。複数のサイト間でSMB共有を同期する場合は、SMBを使用するFlexCache を選択することを推奨します。

SMBを使用するFlexCache ボリューム

ONTAP 9.8以降では、SMBプロトコルがキャッシュボリュームでサポートされるようになり、FlexCache ボリュームキャビネットを参照するSMB共有を作成できます。エクスポートポリシーと同様に、SMB共有はFlexCache ボリュームの作成とレプリケートされません。また、同じSVM内にFlexCache ボリュームを作成する場合でも、これらのLIFは独立しています。これは、キャッシュに異なる共有権限を実装できることも意味します。キャッシュデータアクセスをきめ細かく制御できるほか、必要に応じてキャッシュを読み取り専用に制限することもできます。

SMB共有を使用してFlexCache データにアクセスする場合は、通常、元のボリュームのセキュリティ形式はNTFSになります。NTFS ACLと共有権限アプリケーションは、ONTAP でのSMBサーバの設定に大きく依存しているため、アクセス権を元の場所とキャッシュで確実に同じにするためにいくつかの要件があります。FlexCache ボリューム、SMB、およびマルチプロトコルNASの詳細とベストプラクティスについては、TR-4743を参照してください。

CIFSとNFSの標準のファイル監査

ONTAPは、CIFS / SMBプロトコルとNFSプロトコルの両方でネイティブのファイルおよびフォルダの監査をサポートしています。ファイルやフォルダの監査を使用すると、ストレージ管理者は、サードパーティの監視ツールを購入することなく、NASファイルシステム内でファイルがアクセス、変更、または削除されるタイミングを追跡できます。

NFSおよびCIFS / SMB監査は、監査するボリュームまたはフォルダに監査ACLを設定することで制御できます。監査ログをXMLファイルまたはEVTファイルとして保存するかどうかを決定し、監査する同じデータボリューム内に格納することができます。

NFSおよびCIFS監査の詳細については、次のリソースを参照してください。

- 『SMB / CIFSおよびNFS監査とセキュリティトレーシングガイド』の対象者
- SVMでのNASイベントの監査
- ONTAP 標準のNAS監査（SMBおよびNFS）

マルチプロトコルNASのトラブルシューティング

ここでは、NASに関する一般的な問題と、ONTAP の問題のトラブルシューティングに使用するコマンドについて説明します。

NFSユーザnfsnobody

場合によっては、NFSクライアントでファイルの所有者またはグループの情報 `nfsnobody`がのファイルリストに表示されることがあります。

```
# ls -la | grep newfile
-rwxrwxrwx   1 nfsnobody nfsnobody          0 May 19 13:30 newfile.txt
```

数値を含むファイルをリスト表示 `owner:group 65534`すると、がになります。

```
# ls -lan | grep newfile
-rwxrwxrwx   1 65534 65534          0 May 19 13:30 newfile.txt
```

ほとんど `65534 nfsnobody`のLinuxクライアントでは、ユーザはです。ONTAP では、ユーザは `pcuser`です。

```
cluster::*> unix-user show -vs rver DEMO -id 65534
                User            User    Group Full
Vserver         Name            ID      ID      Name
--------------- --------------- ------- ------- --------------------
DEMO            pcuser          65534 65534
```

`pcuser anonymous`は、エクスポートポリシールールのデフォルトユーザでもあります。

```
cluster::*> export-policy rule show -vserver DEMO -policyname default -fields anon
vserver policyname ruleindex anon
------- ---------- --------- -----
DEMO    default    1         65534
DEMO    default    2         65534
DEMO    default    3         65534
```

ONTAP クラスタファイル権限については、UNIXの所有者 65534はであるが、Windows ACLと所有者が異なることが表示されることがあります。

```
cluster::*> vserver security file-directory show -vserver DEMO -path /data/newfile.txt

               Vserver: DEMO
             File Path: /data/newfile.txt
     File Inode Number: 7088
        Security Style: ntfs
       Effective Style: ntfs
        DOS Attributes: 20
 DOS Attributes in Text: ---A----
Expanded Dos Attributes: -
           UNIX User Id: 65534
          UNIX Group Id: 65534
         UNIX Mode Bits: 777
 UNIX Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:NTAP\ntfs
                         Group:NTAP\DomainUsers
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff-(Inherited)
```

nfsnobody 65534 NFSのリストにまたはが表示された場合は、次のどちらかの状況が発生している可能性が高くなります。

- NFSクライアントにエクスポートされるボリュームは、Windows SMBクライアントでも使用され、共有に書き込みを行っているWindowsユーザは有効なUNIXユーザやグループにマッピングされません。
- NFSクライアント 65534にエクスポートされているボリュームの匿名ユーザがに設定されているため、NFSユーザが匿名ユーザの権限を引き下げられている。ユーザの引き下げの詳細については、TR-4067：『ONTAP』を参照してください。

WindowsユーザーからUNIXユーザーへのマッピングを表示するには、詳細特権で次のコマンドを実行します。

```
cluster::*> access-check name-mapping show -vserver DEMO -direction win-unix -name ntfs
'ntfs' maps to 'pcuser'

cluster::*> access-check name-mapping show -vserver DEMO -direction win-unix -name prof1
'prof1' maps to 'prof1'
```

NFSクレデンシャルの表示と管理

ONTAP 9.3では、NASクレデンシャルとネームサービスサーバの管理について、パフォーマンス、信頼性、耐障害性、サポート性を向上させるためにネームサービス用のグローバルキャッシュが実装されました。

この変更の1つがNFSクレデンシャルキャッシュの実装でした。NFSエクスポートがアクセスされると、NFSユーザとグループの情報がONTAP に格納されます。

これらのキャッシュを表示および管理 nfs credentials するには、advanced権限でコマンドを実行します。

```
cluster::*> nfs credentials ?
  count                       *Count credentials cached by NFS
  flush                       *Flush credentials cached by NFS
  show                        *Show credentials cached by NFS
```

キャッシュエントリには、NFSマウントのTCP接続が存在するノードが設定されます。この情報を表示するには、クラスタで次のコマンドを実行します。

```
cluster::*> nfs connected-clients show -vserver DEMO -client-ip x.x.x.x -fields data-lif-ip -
volume scripts
node                vserver data-lif-ip   client-ip     volume protocol
------------------------ ---------- ------------------ ------------------ ---------- -----------
Node1               DEMO    x.x.x.y       x.x.x.x       scripts nfs3
```

上記 x.x.x.x のコマンドは、クライアントIPがnode1のデータLIFに接続されていることを示しています。この情報を使用すると、どのノードにキャッシュエントリに焦点を当てるかを絞り込むことができます。

nfs credentials count コマンドを使用すると、NFSクレデンシャルキャッシュに現在格納されているクレデンシャルの数を確認できます。この情報は、キャッシュをクリアした場合の影響を理解するのに役立ちます。

```
cluster::*> nfs credentials count -node node1
Number of credentials cached by NFS on node "node1": 4
```

ユーザがONTAP NFSエクスポートにトラバースすると、ユーザIDやグループIDなどがすべてNFSクレデンシャルキャッシュに追加されます。この例で prof1は、というユーザ名はです。

```
# id prof1
uid=1102(prof1) gid=10002(ProfGroup) groups=10002(ProfGroup),10000(Domain
Users),1202(group2),1101(group1),1220(sharedgroup),1203(group3)
```

このユーザには8つの異なるエントリがあります。1つは数値UIDで、もう1つは7つはグループメンバーシップです。その後、ユーザ prof1はNFSエクスポートにアクセスします。クレデンシャルキャッシュは8つ増えます。

```
cluster::*> nfs credentials count -node node1
Number of credentials cached by NFS on node "node1": 12
```

これはSVM単位ではなく、ノード全体のカウントです。環境に複数のSVMがある場合は、のトラブルシューティングにカウントが役立つとは限りません。

NFSクレデンシャル キャッシュの設定

NFSクレデンシャルキャッシュ内のクレデンシャルの数に加えて、ユーザやグループごとにキャッシュエントリを個別に表示することもできます。環境内のユーザにアクセスの問題がある場合は、そのユーザをキャッシュで検索できます。

注： クレデンシャルキャッシュ全体の内容を表示することはできません。

この例 prof1 では、マウントにアクセスします。このキャッシュエントリと、キャッシュエントリに関する詳細を示すフラグを表示できます。

```
cluster::*> nfs credentials show -node node1 -vserver DEMO -unix-user-name prof1

Credentials
---------------
                     Node: node1
                  Vserver: DEMO
                Client IP: -
                    Flags: unix-extended-creds-present, id-name-mapping-present
  Time since Last Refresh: 52s
   Time since Last Access: 44s
               Hit Count: 4

  UNIX Credentials:
                    Flags: 1
                Domain ID: 0
                      UID: 1102
              Primary GID: 10002
         Additional GIDs: 10002
                          10000
                          1101
                          1202
                          1203
                          1220

  Windows Credentials:
                    Flags: -
                 User SID: -
       Primary Group SID: -
             Domain SIDs: -
```

```
  ID-Name Information:
                     Type: user
                       ID: 1102
                     Name: prof1
```

ユーザのプライマリグループのエントリを表示できます。

```
cluster::*> nfs credentials show -node node1 -vserver DEMO -unix-group-name ProfGroup

Credentials
--------------
                     Node: node1
                  Vserver: DEMO
                Client IP: -
                    Flags: id-name-mapping-present
  Time since Last Refresh: 64s
   Time since Last Access: 6s
                Hit Count: 2

  UNIX Credentials:
                    Flags: -
                Domain ID: -
                      UID: -
              Primary GID: -
          Additional GIDs: -

  Windows Credentials:
                    Flags: -
                 User SID: -
        Primary Group SID: -
              Domain SIDs: -

  ID-Name Information:
                     Type: group
                       ID: 10002
                     Name: ProfGroup
```

アクセスを試行したクライアントIPまでの、ユーザおよびグループのクレデンシャルキャッシュエントリを表示できます。

```
cluster::*> nfs credentials show -node node1 -vserver DEMO -client-ip x.x.x.x -unix-user-id 1102

Credentials
--------------
                         Node: node1
                      Vserver: DEMO
                    Client IP: x.x.x.x
                        Flags: unix-extended-creds-present, id-name-mapping-present
       Time since Last Refresh: 35s
        Time since Last Access: 34s
                    Hit Count: 2
               Reference Count:  4
 Result of Last Update Attempt: no error

  UNIX Credentials:
                     Flags: 1
                 Domain ID: 0
                       UID: 1102
               Primary GID: 10002
           Additional GIDs: 10002
                            10000
                            1101
                            1202
                            1203
                            1220

  Windows Credentials:
                     Flags: -
                  User SID: -
         Primary Group SID: -
```

```
              Domain SIDs: -

  ID-Name Information:
                     Type: user
                       ID: 1102
                     Name: prof1
```

クレデンシャルキャッシュには、負のエントリ（解決できなかったエントリ）もキャッシュに保持されます。ONTAP が数値UIDを有効なユーザに解決できない場合、負のエントリが発生します。この場合、UID 1236はONTAP で解決できませんが、NFSエクスポートへのアクセスは試行されました。

```
# su cifsuser
bash-4.2$ cd /scripts/
bash: cd: /scripts/: Permission denied
bash-4.2$ id
uid=1236(cifsuser) gid=1236(cifsuser) groups=1236(cifsuser)

cluster::*> nfs credentials show -node node1 -vserver DEMO -unix-user-id 1236

Credentials
--------------
                      Node: node1
                   Vserver: DEMO
                 Client IP: -
                     Flags: no-unix-extended-creds, no-id-name-mapping
  Time since Last Refresh: 33s
   Time since Last Access: 7s
                 Hit Count: 15

  UNIX Credentials:
                     Flags: -
                 Domain ID: -
                       UID: -
               Primary GID: -
           Additional GIDs: -

  Windows Credentials:
                     Flags: -
                  User SID: -
         Primary Group SID: -
               Domain SIDs: -

  ID-Name Information:
                     Type: -
                       ID: -
                     Name: -
```

NFSv4.xおよびマルチプロトコルNASを使用するNFSクレデンシャルキャッシュ

NFSクレデンシャルキャッシュエントリには、WindowsクレデンシャルとNFSv4 IDマッピングクレデンシャルも格納されます。

ユーザがNFSv4.xエクスポートを経由してIDドメインに正しくマッピングされている場合は `ID-Name Information`、フィールドに値が入力されます。

```
Credentials
--------------
                         Node: node
                      Vserver: DEMO
                    Client IP: x.x.x.x
                        Flags: unix-extended-creds-present, id-name-mapping-present
      Time since Last Refresh: 12s
       Time since Last Access: 9s
                    Hit Count: 2
                Reference Count:  4
 Result of Last Update Attempt: no error

  UNIX Credentials:
                     Flags: 1
```

```
                Domain ID: 0
                      UID: 1102
              Primary GID: 10002
            Additional GIDs: 10002
                             10000
                             1101
                             1202
                             1203
                             1220

  Windows Credentials:
                    Flags: -
                 User SID: -
        Primary Group SID: -
              Domain SIDs: -

  ID-Name Information:
                     Type: user
                       ID: 1102
                     Name: prof1
```

NTFSの権限やセキュリティ形式のエクスポートにユーザがアクセスすると、フラグと cifs-creds-present ドメインSID情報が Windows Credentials次の場所に表示されます。

```
Credentials
---------------
                          Node: node1
                       Vserver: DEMO
                     Client IP: x.x.x.x
                         Flags: ip-qualifier-configured, unix-extended-creds-present, cifs-creds-
present
        Time since Last Refresh: 19s
         Time since Last Access: 1s
                     Hit Count: 9
                Reference Count:  2
 Result of Last Update Attempt: no error

  UNIX Credentials:
                     Flags: 0
                  Domain ID: 0
                        UID: 1102
                Primary GID: 10002
            Additional GIDs: 10002
                             10000
                             1101
                             1202
                             1203
                             1220

  Windows Credentials:
                     Flags: 8320
                  User SID: S-1-5-21-3552729481-4032800560-2279794651-1214
        Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-513
              Domain SIDs: S-1-5-21-3552729481-4032800560-2279794651
                           S-1-18
                           S-1-1
                           S-1-5
                           S-1-5-32

  ID-Name Information:
                     Type: -
                       ID: -
                     Name: -
```

NFSクレデンシャルキャッシュ設定

NFSクレデンシャルキャッシュのタイムアウト値は、表6に示すNFSサーバオプションで制御されます。

表6）NFSクレデンシャルキャッシュ設定

オプション	機能	デフォルト値（ミリ秒）
-cached-cred-negative-ttl	このパラメータはオプションで、ネガティブ キャッシュされたクレデンシャルがキャッシュからクリアされるまでの時間を指定します。60,000～604,800,000の値を指定する必要があります。	7,200,000ミリ秒
-cached-cred-positive-ttl	このパラメータはオプションで、ポジティブ キャッシュされたクレデンシャルがキャッシュからクリアされるまでの時間を指定します。60,000～604,800,000の値を指定する必要があります。	86、400、000ミリ秒 24時間
-cached-cred-harvest-timeout	このパラメータはオプションで、キャッシュされたクレデンシャルのハーベストタイムアウトを指定します60,000～604,800,000の値を指定する必要があります。	86、400、000ミリ秒 24時間

キャッシュエントリは、前回のアクセス/更新からの経過時間（ show コマンドで確認）を維持します。エントリがアイドル状態のまま一定時間が経過すると、最終的にキャッシュから削除されます。エントリがアクティブな場合は、エントリが更新されてキャッシュに残ります。

これらの値は、目的の影響に応じて、タイムアウト値の増減が可能です。

- **キャッシュタイムアウト値を長くする** と、ネットワークの負荷が軽減され、ユーザの検索時間が短縮されますが、キャッシュエントリがネームサービスと常に同期されているとは限らないため、フォールスポジティブまたはネガティブな結果が生成される可能性があります。
- **キャッシュタイムアウト値** を**短くする**と、ネットワークサーバとネームサーバの負荷が増大し、（ネームサービスソースによっては）名前検索に若干のレイテンシが生じますが、より正確で最新のエントリが得られます。

ネットアップでは、ベストプラクティスとして、この値はそのままにしておくことを推奨します。値を変更する必要がある場合は、必ず結果を監視し、必要に応じて調整してください。

NFSクレデンシャル キャッシュの設定

ユーザがグループに対して追加または削除され、必要なアクセス権がない場合、クレデンシャルキャッシュエントリは、キャッシュエントリのタイムアウトを待たずに手動でフラッシュできます。

次のコマンドは、UNIXユーザ、数値ID、UNIXグループ、または数値IDに対して実行できます。また、このコマンドは、問題 を持つクライアントIPアドレスに応じてきめ細かく実行できます。

```
cluster::*> nfs credentials flush -node node1 -vserver DEMO -client-ip x.x.x.x -unix-user-id 1102

Number of matching credentials flushed: 2
```

注：　フラッシュできるNFSクレデンシャルキャッシュエントリは一度に1つだけです。

NFSクレデンシャルキャッシュは、ネームサービスキャッシュとは別のものです。ネームサービスキャッシュの管理については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

エクスポートポリシールール：キャッシング

クラスタへの要求数を減らすために、エクスポートポリシールール、クライアントホスト名、およびネットグループ情報はすべてONTAP にキャッシュされます。この機能により、要求のパフォーマンスが向上するだけでなく、ネットワークおよびネームサービスサーバの負荷も軽減されます。

clientmatchのキャッシュ

clientmatchエントリをキャッシュすると、SVMのローカルなままになり、キャッシュタイムアウト期間に達したとき、またはエクスポートポリシールールテーブルが変更されたときにフラッシュされます。デフォルトのキャッシュタイムアウト時間 `export-policy access-cache config show`は、ONTAP のバージョンによって異なり、管理者権限でコマンドを実行して確認できます。

これらはデフォルトの設定です。

```
TTL For Positive Entries (Secs): 3600
TTL For Negative Entries (Secs): 3600
Harvest Timeout (Secs): 86400
```

エクスポートポリシーアクセスキャッシュ内の特定のクライアントを表示するには、詳細特権で次のコマンドを実行します。

```
cluster::*> export-policy access-cache show -node node-02 -vserver NFS -policy default -address
x.x.x.x

                                       Node: node-02
                                    Vserver: NFS
                                Policy Name: default
                                 IP Address: x.x.x.x
                    Access Cache Entry Flags: has-usable-data
                                Result Code: 0
                First Unresolved Rule Index: -
                     Unresolved Clientmatch: -
              Number of Matched Policy Rules: 1
         List of Matched Policy Rule Indexes: 2
                               Age of Entry: 11589s
                  Access Cache Entry Polarity: positive
Time Elapsed since Last Use for Access Check: 11298s
      Time Elapsed since Last Update Attempt: 11589s
                Result of Last Update Attempt: 0
                 List of Client Match Strings: 0.0.0.0/0
```

ホスト名/ DNSキャッシュ

clientmatchがホスト名に設定されている場合、その名前はIPアドレスに解決されます。このプロセスは、SVMのネームサービススイッチ（ns-switch）で使用される順序に基づいています。たとえば、ns-switchホストデータベース`files,dns`がに設定されている場合、ONTAPはローカルホストファイルでクライアント一致を検索してからDNSを検索します。

名前の検索後、ONTAPは結果をホストキャッシュにキャッシュします。このキャッシュの設定は構成可能であり、ONTAP CLIから詳細な権限で照会してフラッシュできます。

キャッシュを照会するには、次のコマンドを実行します。

```
cluster::*> name-service cache hosts forward-lookup show -vserver NFS
(vserver services name-service cache hosts forward-lookup show)
                    IP       Address IP                        Create
Vserver   Host      Protocol Family Address          Source Time         TTL(sec)
--------- --------- -------- ------ ---------------- ------ ------------ ----------

NFS       centos7.ntap.local
                    Any      Ipv4    x.x.x.x dns       3/26/2020 3600
                                                            16:31:11
```

ホストのキャッシュ設定を表示するには、次のコマンドを実行します。

```
cluster::*> name-service cache hosts settings show -vserver NFS -instance
  (vserver services name-service cache hosts settings show)

                    Vserver: NFS
          Is Cache Enabled?: true
Is Negative Cache Enabled?: true
               Time to Live: 24h
```

```
     Negative Time to Live: 1m
     Is TTL Taken from DNS: true
```

場合によっては、NFSクライアントのIPアドレスが変更された場合、アクセスの問題を解決するためにホストのエントリをフラッシュする必要があります。

ホストキャッシュエントリをフラッシュするには、次のコマンドを実行します。

```
cluster::*> name-service cache hosts forward-lookup delete -vserver NFS ?
     -host      -protocol -sock-type -flags      -family
```

ネットグループのキャッシュ

clientmatchフィールドのネットグループをエクスポートルールに使用している場合、ONTAPは、ネットグループネームサービスサーバに連絡してネットグループ情報を展開するための追加の作業を行います。ns-switch内のネットグループデータベースは、ONTAP がネットグループを照会する順序を決定します。また、ONTAP がネットグループサポートに使用する方法は、netgroup.byhostサポートが有効か無効かによって異なります。netgroup.byhostの詳細については、TR-4835：ONTAP でのLDAPの設定方法を参照してください。

- netgroup.byhostが無効な場合、ONTAPはネットグループ全体を照会し、すべてのネットグループエントリをキャッシュに読み込みます。ネットグループに数千のクライアントがある場合は、この処理の完了までにさらに時間がかかることがあります。netgroup.byhostはデフォルトで無効になっています。
- netgroup.byhostが有効な場合、ONTAPはホストエントリと関連するネットグループマッピングのみをネームサービスに照会します。このプロセスにより、数千ものクライアントを検索する必要がなくなるため、ネットグループの照会に要する時間が大幅に短縮されます。

これら vserver services name-service cache のエントリはネットグループキャッシュに追加され、コマンドを実行すると確認できます。これらのキャッシュエントリは表示またはフラッシュすることができ、タイムアウト値を設定できます。

ネットグループのキャッシュ設定を表示するには、次のコマンドを実行します。

```
cluster::*> name-service cache netgroups settings show -vserver NFS -instance
  (vserver services name-service cache netgroups settings show)

                    Vserver: NFS
          Is Cache Enabled?: true
Is Negative Cache Enabled?: true
               Time to Live: 24h
      Negative Time to Live: 1m
  TTL for netgroup members: 30m
```

ネットグループ全体がキャッシュされると、メンバーキャッシュに配置されます。

```
cluster::*> name-service cache netgroups members show -vserver DEMO -netgroup netgroup1
  (vserver services name-service cache netgroups members show)

            Vserver: DEMO
           Netgroup: netgroup1
              Hosts: sles15-1,x.x.x.x
        Create Time: 3/26/2020 12:40:56
Source of the Entry: ldap
```

ネットグループエントリが1つだけキャッシュされる場合は ip-to-netgroup hosts reverse-lookup、キャッシュとキャッシュに次のエントリが格納されます。

```
cluster::*> name-service cache netgroups ip-to-netgroup show -vserver DEMO -host x.x.x.y
  (vserver services name-service cache netgroups ip-to-netgroup show)
Vserver    IP Address Netgroup      Source Create Time
---------- ---------- ------------- ---------- ---------------
DEMO       x.x.x.y
                      netgroup1     ldap    3/26/2020 17:13:09

cluster::*> name-service cache hosts reverse-lookup show -vserver DEMO -ip x.x.x.y
```

```
  (vserver services name-service cache hosts reverse-lookup show)
Vserver     IP Address      Host                    Source Create Time     TTL(sec)
----------- --------------- ----------------------- -------- ------------------- -----------
DEMO        x.x.x.y   centos8-ipa.centos-ldap.local
                                                    dns    3/26/2020 17:13:09
                                                                          3600
```

キャッシュタイムアウトの変更に関する考慮事項

キャッシュ設定は、必要に応じて別の値に変更できます。

- タイムアウト値**を増やす**とキャッシュエントリの保持期間は長くなりますが、クライアントがIPアドレスを変更した場合にクライアントアクセスに不整合が発生する可能性があります。たとえば、クライアントIPアドレスにDHCPが使用されていて、DNSが更新されていない場合や、エクスポートルールでIPアドレスが使用されている場合などです。
- タイムアウト値を**小さくする**と、最新情報のキャッシュはより頻繁にフラッシュされますが、ネームサービスサーバへの負荷が増え、クライアントからのマウント要求のレイテンシが長くなる可能性があります。

ほとんどの場合、キャッシュタイムアウト値をそのままにしておくことを推奨します。詳細とガイダンスについては、TR-4668：『Name Services Best Practices』およびTR-4835：『How to Configure LDAP in ONTAP』を参照してください。

exportfsのサポート

ONTAP `exportfs export-policy name-service` では、がキャッシュコマンドとキャッシュコマンドに置き換えられました。を実行すると `exportfs`、次の出力が表示されます。

```
  "exportfs" is not supported: use the "vserver export-policy" command.
```

権限の問題をトラブルシューティングするためのコマンド

ほとんどの場合、NFS権限の問題は単純です。NFSv3は基本的なrwxモードビットを使用します。ただし、NFSv4 ACLやマルチプロトコルのNASアクセスおよびさまざまなセキュリティ形式が関連する場合、複雑さが増します。ここでは、NAS環境で権限の問題をトラブルシューティングする際に役立つコマンドをいくつか紹介します。ネームサービスキャッシュ情報については、「NFSクレデンシャルの表示と管理」を参照してください。詳細については、TR-4835：『LDAP in NetApp ONTAP』を参照してください。

UNIX UIDおよびグループメンバーシップの確認

NFSv3操作では、数値を渡してIDを検証できるため、UNIXユーザ名とグループ名はそれほど重要ではありません。ただし、NFSv4およびNTFSのセキュリティ形式のオブジェクトでは、適切な名前解決のために、数値IDを有効なUNIXユーザおよびグループ名に変換する必要があります。NFSv4 では、ユーザをnobodyに引き下げないようにするために、この数値IDから名前へのマッピング/変換が必要です。NTFSセキュリティ形式では、有効なWindowsユーザ名にマッピングするUNIXユーザ名が必要です。

ONTAP には、UNIXユーザのIDおよびグループメンバーシップを表示するために使用できるいくつかのコマンドがあります。

ローカルUNIXユーザおよびグループの場合は、次のコマンドを実行します。

```
cluster::> unix-user show
cluster::> unix-group show
```

すべてのUNIXユーザ（ローカルおよびネームサービス、Advanced Privilege）のUID / GIDの基本情報については、次のコマンドを実行します。

```
cluster::*> access-check authentication show-ontap-admin-unix-creds
```

または、次のコマンドを実行します。

```
cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username prof1 -show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: LDAP
```

```
pw_name: prof1
pw_passwd:
pw_uid: 1102
pw_gid: 10002
pw_gecos:
pw_dir:
pw_shell:

cluster::*> getxxbyyy getpwbyname -node node1 -vserver DEMO -username host -show-source true
  (vserver services name-service getxxbyyy getpwbyname)
Source used for lookup: Files
pw_name: host
pw_passwd: *
pw_uid: 598
pw_gid: 0
pw_gecos:
pw_dir:
pw_shell:
```

ユーザ情報およびグループメンバーシップ（ローカルおよびネームサービス、Advanced Privilege）を表示するには、次のコマンドを実行します。

```
cluster::*> getxxbyyy getgrlist -node node1 -vserver DEMO -username prof1
  (vserver services name-service getxxbyyy getgrlist)
pw_name: prof1
Groups: 10002 10002 10000 1101 1202 1203 48
```

マルチプロトコルユーザのユーザおよびグループの情報を表示します

ご使用の環境でCIFS / SMBとNFSの両方が設定されている場合は、Advanced Privilegeの1つのコマンドから、ユーザ名、ネームマッピング、ID、グループ名、権限、およびグループメンバーシップの完全なリストを取得できます。このコマンドは、マルチプロトコル環境で使用することを推奨します。SMB / CIFSサーバが設定されていない場合、このコマンドは機能しません。

```
cluster::*> access-check authentication show-creds -node node1 -vserver DEMO -unix-user-name
prof1 -list-name true -list-id true
  (vserver services access-check authentication show-creds)

 UNIX UID: 1102 (prof1) <> Windows User: S-1-5-21-3552729481-4032800560-2279794651-1110
(NTAP\prof1 (Windows Domain User))

 GID: 10002 (ProfGroup)
 Supplementary GIDs:
  10002 (ProfGroup)
  10000 (Domain Users)
  1101 (group1)
  1202 (group2)
  1203 (group3)
  48 (apache-group)

 Primary Group SID: S-1-5-21-3552729481-4032800560-2279794651-1111   NTAP\ProfGroup (Windows
Domain group)

 Windows Membership:
  S-1-5-21-3552729481-4032800560-2279794651-1301   NTAP\apache-group (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1106   NTAP\group2 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-513   NTAP\DomainUsers (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1105   NTAP\group1 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1107   NTAP\group3 (Windows Domain group)
  S-1-5-21-3552729481-4032800560-2279794651-1111 NTAP\ProfGroup (Windows Domain group) S-
  1-5-21-3552729481-4032800560-2279794651-1231 NTAP\local-group.ntap (Windows Alias) S-
  1-18-2 Service asserted identity (Windows Well known group)
  S-1-5-32-551   BUILTIN\Backup Operators (Windows Alias)
  S-1-5-32-544   BUILTIN\Administrators (Windows Alias)
  S-1-5-32-545   BUILTIN\Users (Windows Alias)
 User is also a member of Everyone, Authenticated Users, and Network Users

 Privileges (0x22b7):
```

```
  SeBackupPrivilege
  SeRestorePrivilege
  SeTakeOwnershipPrivilege
  SeSecurityPrivilege
  SeChangeNotifyPrivilege
```

ONTAP で表示されるファイル権限を示します

権限の問題のトラブルシューティング時に、NASクライアントから権限を表示するためのアクセス権がない可能性があります。また、NASクライアントに表示される権限とONTAP の表示内容を確認することもできます。このためには、次のコマンドを実行します。

```
cluster::> file-directory show -vserver DEMO -path /home/prof1
  (vserver security file-directory show)

               Vserver: DEMO
             File Path: /home/prof1
     File Inode Number: 8638
        Security Style: ntfs
       Effective Style: ntfs
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          UNIX User Id: 0
         UNIX Group Id: 0
        UNIX Mode Bits: 777
 UNIX Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8504
                         Owner:NTAP\prof1
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff-OI|CI
                           ALLOW-NTAP\prof1-0x1f01ff-OI|CI
                           ALLOW-NTAP\sharedgroup-0x1200a9-OI|CI
                           ALLOW-NTAP\Administrator-0x1f01ff-OI|CI
```

次のコマンドを実行して、特定のユーザが特定のファイルまたはディレクトリに対して有効な権限を確認することもできます。

```
cluster::> file-directory show-effective-permissions -vserver DEMO -unix-user-name prof1 -path
/home/prof1
  (vserver security file-directory show-effective-permissions)

                       Vserver: DEMO
             Windows User Name: NTAP\prof1
                Unix User Name: prof1
                     File Path: /home/prof1
               CIFS Share Path: -
         Effective Permissions:
                                Effective File or Directory Permission: 0x1f01ff
                                       Read
                                       Write
                                       Append
                                       Read EA
                                       Write EA
                                       Execute
                                       Delete Child
                                       Read Attributes
                                       Write Attributes
                                       Delete
                                       Read Control
                                       Write DAC
                                       Write Owner
                                       Synchronize
```

エクスポートポリシーのアクセスを確認しています

権限の問題はエクスポートポリシーの設定に起因する場合があります。たとえば、ポリシーで読み取りのみを許可するように設定している場合、この設定はマウントに設定されているユーザ権限よりも優先されます。

ONTAP では、次のコマンドを実行して、クライアントのエクスポートポリシーへのアクセスを検証できます。

```
cluster::> export-policy check-access
```

セキュリティトレースの使用

アクセス権の問題を発生時にトレースするには、セキュリティトレースフィルタ機能を使用して、NFS権限とSMB / CIFS権限の両方をトレースします。

トレースフィルタを作成するには、次のコマンドを実行します。

```
cluster::> vserver security trace filter create ?
    -vserver <vserver name>         Vserver
   [-index] <integer>               Filter Index
  [[-protocols] {cifs|nfs}, ...]    Protocols (default: cifs)
  [ -client-ip <IP Address> ]       Client IP Address to Match
  [ -path <TextNoCase> ]            Path
  { [ -windows-name <TextNoCase> ] Windows User Name
  | [ -unix-name <TextNoCase> ] }   UNIX User Name or User ID
  [ -trace-allow {yes|no} ]         Trace Allow Events (default: no)
  [ -enabled {enabled|disabled} ]   Filter Enabled (default: enabled)
  [ -time-enabled {1..720} ]        Minutes Filter is Enabled (default: 60)
```

必要に応じて、トレースを特定のユーザ名またはIPアドレスだけに絞り込むことができます。

```
cluster::*> vserver security trace filter modify -vserver DEMO -index 1 -protocols nfs -client-ip
x.x.x.x -trace-allow yes -enabled enabled
```

トレースが作成されると、結果がリアルタイムで表示されます。結果を表示するときに、成功、失敗、ユーザID、プロトコルなどを基準にフィルタリングできます。

```
cluster::> vserver security trace trace-result show ?
  [ -instance | -fields <fieldname>, ... ]
  [[-node] <nodename>]                  Node
  [ -vserver <vserver name> ]           Vserver
  [[-seqnum] <integer>]                 Sequence Number
  [ -keytime <Date> ]                   Time
  [ -index <integer> ]                  Index of the Filter
  [ -client-ip <IP Address> ]           Client IP Address
  [ -path <TextNoCase> ]                Path of the File Being Accessed
  [ -win-user <TextNoCase> ]            Windows User Name
  [ -security-style <security style> ] Effective Security Style On File
  [ -result <TextNoCase> ]              Result of Security Checks
  [ -unix-user <TextNoCase> ]           UNIX User Name
  [ -session-id <integer> ]             CIFS Session ID
  [ -share-name <TextNoCase> ]          Accessed CIFS Share Name
  [ -protocol {cifs|nfs} ]              Protocol
  [ -volume-name <TextNoCase> ]         Accessed Volume Name
```

次の例は、特定のユーザに対する権限やアクセスの失敗を示しています。

```
cluster::> vserver security trace trace-result show -node * -vserver DEMO -unix-user 1102 -result
*denied*

Vserver: DEMO


Node             Index Filter Details              Reason
---------------- ----- --------------------------- ----------------------------------------------------------
Node2            1     Security Style: UNIX and    Access is denied. The
                       NFSv4 ACL                   requested permissions are not
```

```
                                                granted by the ACE while
                                                setting attributes. Access is
                                                not granted for: "Write DAC"

                    Protocol: nfs
                    Volume: home
                    Share: -
                    Path: /dir
                    Win-User: -
                    UNIX-User: 1102
                    Session-ID: -
```

UNIXセキュリティ形式のオブジェクトでのセキュリティタブビューの制御

ONTAP では、ボリュームまたはqtreeでUNIXセキュリティ形式を使用する場合にセキュリティタブの表示と非表示を切り替えるようにCIFS / SMBサーバを設定できます。これを制御するオプション `is-unix-nt-acl-enabled`はです。

このオプションはデフォルトで有効になっています。つまり、ファイルシステムオブジェクトにUNIXセキュリティ形式が設定されている場合、[セキュリティ]タブが表示されます。タブ内のユーザとグループはSVM固有の製造されたSIDを表示し、UNIX PermUid、UNIX PermGid、およびその他の名前に解決されます。このタブから権限を変更`rwx`できますが、読み取り、書き込み、および実行の各値()についてのみ変更できます。

図40）UNIX SIDが解決される前の権限ビュー

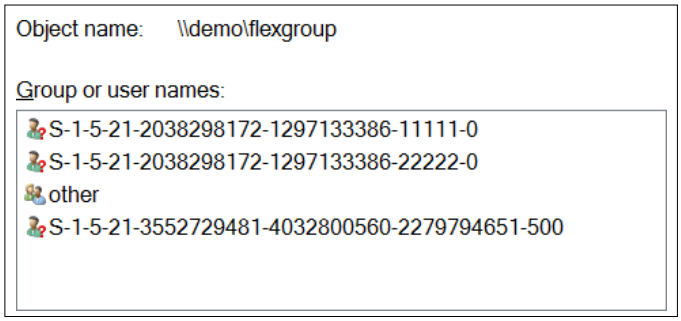
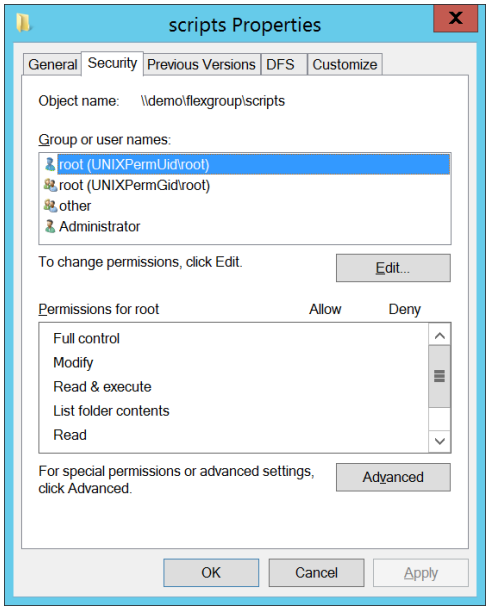


図41では、scriptsフォルダはUNIXセキュリティ形式で、権限は777 `vserver security file-directory show`です（CLIの出力から見たように）。

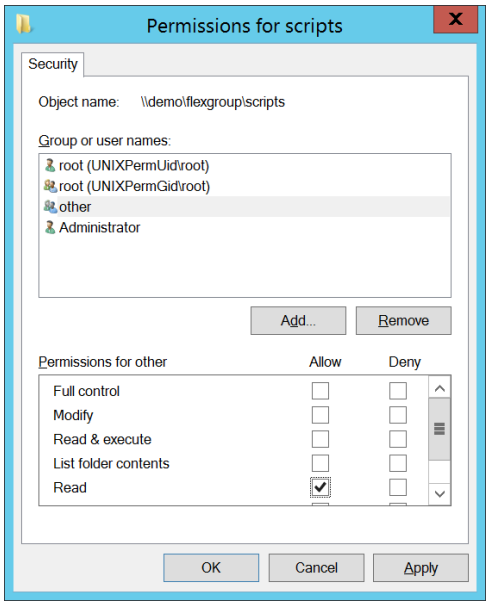
```
cluster::*> vserver security file-directory show -vserver DEMO -path /flexgroup_16/scripts

               Vserver: DEMO
             File Path: /flexgroup_16/scripts
     File Inode Number: 96
        Security Style: unix
       Effective Style: unix
        DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
          UNIX User Id: 0
         UNIX Group Id: 0
        UNIX Mode Bits: 777
 UNIX Mode Bits in Text: rwxrwxrwx
                   ACLs: -
```

図41）UNIXセキュリティ形式の[Security]タブ



このフォルダは権限777に設定されていますが、[セキュリティ]タブを変更して[その他]を読み取りに設定できます。

図42）UNIXセキュリティ形式のSecurityタブ-権限の変更



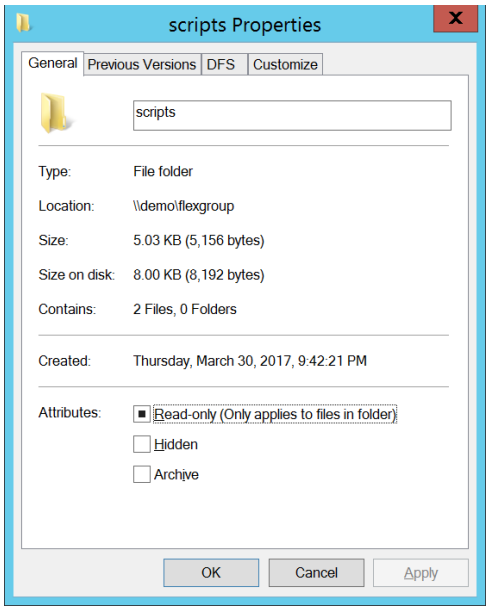
この設定が完了すると、権限が774に変更されます。

```
cluster::*> vserver security file-directory show -vserver DEMO -path /flexgroup_16/scripts

                Vserver: DEMO
              File Path: /flexgroup_16/scripts
      File Inode Number: 96
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
```

```
Expanded Dos Attributes: -
           UNIX User Id: 0
          UNIX Group Id: 0
         UNIX Mode Bits: 774
 UNIX Mode Bits in Text: rwxrwxr--
                   ACLs: -
```

このオプションを無効にすると、UNIXセキュリティ形式のオブジェクトでCIFS / SMBクライアントのセキュリティタブが表示されなくなります。このオプションを無効にするユースケースの1つは、UNIXセキュリティ形式のオブジェクトに対するSMBクライアントからの不要な権限の変更を防止することです。

図43）UNIXセキュリティ形式ではセキュリティタブが非表示



NFSクライアントでのNTFS権限の表示

NTFSセキュリティ形式のボリュームまたはqtreeを使用する場合、NFSクライアントではデフォルトで、オブジェクトに無制限の権限（777）があるようにモード ビットまたはNFSv4 ACLが表示されます。これは、ユーザとストレージ管理者にとって、主に2つの理由で問題となります。

- アプリケーションの機能が、ACLやモード ビットが適切に表示されていることを前提としている場合がある。
- モード ビットが「無制限」と表示されていることでユーザが不安になり、サポート チケットやサポート サイクルをトラブルシューティングに費やす可能性がある。

NTFSセキュリティ形式のボリュームでACLやモード ビットが777を示していても、オブジェクトに誰もがフルアクセスできるわけではありません。clustered Data ONTAPでは、NTFSセキュリティ形式のボリュームへのアクセスが、NTFSのセキュリティとACLに基づいて制御されます。このため、NFSクライアントがこのボリュームにアクセスするには（認証されるためには）、有効なWindowsユーザにマッピングされた有効なUNIXユーザが必要です。初期認証が終わると、マッピングされたユーザを使用して詳細なNTFS ACLに基づいてアクセス権が決定されます。

Data ONTAP 8.3.1では、`ntacl-display-permissive-perms`というオプションが導入されました。このオプションのデフォルト設定は[Disabled]です。このデフォルト値を使用すると、NTFSオブジェクトをマウントするNFSクライアントで解釈されたACLと同等の権限が許可されます。その結果、最小アクセスに基づいて権限が表示され、現在のユーザの実際のNTFS権限に近いUNIXユーザの権限に近い値になります。これにより、問題を軽減し、アプリケーションの互換性に対処できます。

このオプションを指定すると、NTFSセキュリティ形式のボリュームにアクセスするユーザには、共有にアクセスするユーザに基づいて提供される権限と同等の権限が表示されます。このため、このオブジェクトにアクセスするユーザには、NTFSセキュリティ アクセス権に応じて異なる結果が表示される場合があります。

また、NTFS ACLとUNIX形式のACLには大きな違いがあるため、同等の権限が正確でない場合があります。たとえば、NTFSのセキュリティ セマンティクスだけで提供される詳細な権限がユーザに割り当てられている場合、NFSクライアントはその権限を正しく解釈できません。

Windowsのセキュリティタブのビューに対するNFSv4 ACLの影響

ファイル、フォルダ `-is-unix-nt-acl-enabled`、またはボリュームにNFSv4 ACLが設定されている場合、がTrueに設定されていても、SMB 2.0以降のクライアントはSecurityタブを表示または変更できません。これは、新しいバージョンのWindowsクライアントプロトコルでは、SMB 1.0でNFSv4 ACLの解決に使用されているSMB呼び出しと同じSMB呼び出しがサポートされないためです。詳細については、バグ928026を参照してください。

エクスポートポリシールール：アクセスの検証

ONTAP には、`export-policy check-access`エクスポートポリシーのアクセスルールセットをクライアントのアクセスに対してクロスチェックできるコマンド（）が用意されています。これにより、エクスポートポリシールールが導入前に適切に機能しているかどうかの判断や、トラブルシューティングに役立ちます。機能 `exportfs -c`は機能に似ています。このコマンドは、NFSクライアントからの標準マウントで使用される、通常のネームサービス通信とキャッシュ通信をすべて利用します。

export-policy check-accessの例

```
cluster1::*> vserver export-policy check-access -vserver vs1 -client-ip 1.2.3.4 -volume flex_vol
-authentication-method sys -protocol nfs3 -access-type read

                                        Policy    Policy       Rule
Path                          Policy    Owner     Owner Type  Index Access
----------------------------- --------- --------- ---------- ------ ----------
/                             default   vs1_root  volume          1 read
/dir1                         default   vs1_root  volume          1 read
/dir1/dir2                    default   vs1_root  volume          1 read
/dir1/dir2/flex1              data      flex_vol  volume         10 read
```

付録A： マルチプロトコルのNAS用語

表7 に、本ドキュメントで言及されている用語を示します。このセクションでは、用語について詳しく説明します。

表7）マルチプロトコルNASの用語

期間	定義
認証	自分の状態を確認する。ONTAP では、ユーザ名または数値IDを取得し、ONTAP クラスタが認識している有効なWindowsユーザまたはUNIXユーザにマッピングすることを意味します。
許可	認証とネームマッピングのあと、許可はユーザまたはグループがシステム内で持つアクセスのレベルを決定します。ACEやACL、モードビット、共有レベルのアクセス、エクスポート、その他の形式の権限などが含まれます。
ネーム マッピング	WindowsおよびUNIXのアクセス権は必ずしも1:1をマッピングするわけではないため、使用中のNASプロトコルに関係なく適切なアクセスを提供するために、ユーザー名は適切なボリュームセキュリティタイプにマッピングされます。名前がマッピングされるシナリオの詳細については、「ネームマッピング」を参照してください。
論理インターフェイス（LIF）	論理インターフェイス（LIF）はONTAP の仮想IPアドレスで、ストレージシステムに対するデータ、管理、およびその他のネットワークアクセスを提供します。NASプロトコルの 場合は、データLIF、および特定のデータLIFサービスポリシーが必要です。

期間	定義
Storage Virtual Machine（SVM）	ストレージ管理者は、Storage Virtual Machine（SVM）を使用してエンドユーザ用に一意のセキュアなテナントをプロビジョニングできます。SVMには、それぞれ固有のネームスペース、ドメイン、ネームサービスの設定、NASプロトコルの設定などがあります。これにより、サービスプロバイダを使用するなど、複数のエンドユーザにストレージをプロビジョニングする際の柔軟性が向上します。クラスタには1つまたは最大1、024個のSVMを含めることができます。
エクスポート ポリシー	エクスポートポリシーは、NFS（およびSMBも含む）共有のマウントを試みるクライアントのアクセスを決定するために使用される複数のルールのコンテナです。各ボリュームまたはqtreeには一意のエクスポートポリシーを割り当てることができます。
エクスポートポリシールール	エクスポートポリシーはコンテナですが、アクセスレベルはONTAP のエクスポートポリシールールによって決まります。ポリシーには数百個のルールを設定でき、各ルールに複数のclientmatchの値を指定できます。詳細については、「エクスポートポリシーおよびルールの概念」を参照してください。
FlexVol	FlexVol ボリュームは、物理ストレージ上に存在する論理的な境界であり、NASクライアントにはマウントポイントまたは共有パスを提供します。FlexVol ボリュームには、それぞれ一意のファイルシステムIDがあり、クラスタネームスペース内で相互に接続することができます。FlexVol ボリュームは、クラスタ内の個々のノードで動作します。FlexVol ボリュームは最大100TBまで拡張でき、必要に応じて何度でも拡張/縮小できます。
FlexGroupボリューム	FlexGroup ボリュームは、NASクライアントに大規模な単一ネームスペースとして提供されるFlexVol ボリュームのグループです。FlexGroup ボリュームはFlexVol ボリュームよりもはるかに大きく（20PB、2、000億ファイル）、クラスタ内の複数のノードにまたがって拡張でき、並列処理を必要とするワークロードでパフォーマンスを向上できます。詳細については、TR-4571を参照してください。
ネームスペース	ONTAP のネームスペースは、NAS共有のアクセスポイントです。ONTAP SVM内の複数のFlexVol ボリュームは、複数のネームスペースとみなすことができます。また、それらを使用してディレクトリツリーを作成する場合は、1つのネームスペースとみなすことができます。FlexGroup やFlexCache などのONTAPの機能は、単一のネームスペースの概念を強化することを目的としています。詳細については、「ネームスペースとファイルシステムの概念」を参照してください。
FlexCacheボリューム	ONTAP のFlexCacheは、ボリュームの書き込み可能な永続的仮想キャッシュをリモートサイトに提供します。キャッシュは、データへのアクセスが複数回、複数のホストで共有される読み取り負荷の高い環境で効果的です。
CIFS 共有	CIFS（またはSMB）共有は、CIFS / SMBプロトコル経由でNASにアクセスするクライアント用に作成されるアクセスポイントです。一般に、これはWindowsクライアントからのものですが、LinuxまたはMacOSクライアントからのものもあります。
NFS エクスポート	NFSエクスポートは、NFSプロトコルを介してNASデータにアクセスするクライアント用に作成されるアクセスポイントです。一般に、これはLinuxクライアントから実行できますが、WindowsまたはMacOSから実行することもできます。

付録B：NFSサーバオプション

ONTAP のNFSサーバには、ONTAP の構成に対してさまざまなオプションがあります。これらのオプションのほとんどはすべての環境に適用されるわけではありませんが、マルチプロトコル環境に固有の問題を解決するのに役立つ場合もあります。

表8 に、ONTAP 9.8で使用できるNFSオプションと、その用途を示します。これらのオプション `nfs modify` は、コマンドで制御されます。アスタリスクで示されるオプションは、Advanced Privilegeにあります。

表8）マルチプロトコルNASに影響する可能性のあるNFSサーバオプション-ONTAP 9.8以降

オプション	マルチプロトコルのNASに及ぼす影響
`-v4.0/v4.1`	NFSバージョン4.xを有効にするには、UNIXユーザが名前文字列にマッピングされている必要があります。正しく設定されていないと、クライアントの動作が予測できない可能性があります。クライアントでNFSv4.xが望ましくない場合でも、NFSv4.xとネゴシエートできます。これにより、マルチプロトコルNASで、特にWindowsとUNIX間のネームマッピングに関する問題が発生することがあります。
`-default-win-user`	このオプションはデフォルトでは設定されていません。設定すると、NTFS権限を持つボリュームまたはqtreeにアクセスしようとするすべてのUNIXユーザは、既存のWindowsネームマッピングルールまたは1：1のユーザマッピングが存在しない場合、1つのデフォルトWindowsユーザにフォールバックされます。たとえば、UNIXユーザ `jacksprat jacksprat` がNTFSセキュリティ形式のボリュームにアクセスしようとすると、ONTAPは、LDAPまたはローカルファイルで、という名前のWindowsユーザ、または既存のネームマッピングルールを検索しようとします。存在 `jacksprat` しない場合は、デフォルトのWindowsユーザにマッピングされます。デフォルトのWindowsユーザが設定されていないと、ONTAP からNTFSへのセキュリティ形式のボリュームの認証は失敗します。ONTAP では権限を認識できないため、そのユーザが無効と表示されます。
`-ntfs-unix-security-ops*`	このオプションは、NTFSセキュリティ形式のボリュームまたはqtreeで実行するNFS処理の動作を制御します。NFS処理（chmod、chownなど）をNTFSセキュリティ形式のボリュームで実行することはできません。エクスポートポリシールールのデフォルト設定（fail）では、処理の実行時にNFSクライアントにエラーメッセージが送信されます。または、この値をignoreに設定しても、処理の失敗を許可することもできます。 デフォルト `use_export_policy`では、NFSサーバの値はに設定されます。つまり、エクスポートポリシールールは、NTFSセキュリティ形式のオブジェクトに対するNFS処理がクライアントに報告する方法を定義します。NFSサーバで値を明示的に設定すると、すべてのNFSクライアントが同じように動作します。この動作をさらに細かく制御する場合は、このオプションをデフォルトのままにして、個々のエクスポートポリシールールでの動作を制御します。
`-v4-id-domain`	NFSv4.xが有効 `-v4-id-domain` になっている場合に、ONTAPでのユーザ文字列の定義方法がオプションで指定されます。この文字列は、ネーム文字列とドメインのマッピングが適切に行われるように、NFSクライアント上の文字列と一致する必要があります。たとえば `-v4-id-domain`、オプションをdefaultv4iddomain.com文字列に指定 `jacksprat` した場合に、クライアントがjacksprat@domain.comという名前のNFSv4.xユーザを検索しようとしても、ONTAPはdefaultv4iddomain.comドメインに属しているためにその文字列と一致しません。

オプション	マルチプロトコルのNASに及ぼす影響
	jacksprat@domain.com `nobodynobody`は jacksprat@defaultv4iddomain.comと同じではないため、ユーザが権限を引き下げられます。つまり、は有効なUNIXユーザではなく、本来は対象となるUNIXユーザではないため、マルチプロトコルNAS環境でWindowsとUNIXの名前のマッピングが破棄されます。
`-v4-acl-preserve`	このオプション `chmod chown` を有効にすると、NFSv3または操作を実行した場合にNFSv4.x ACLが維持されます。無効 `chown/chmod` にすると、NFSv4.x ACEが消去されます。NFSv4 ACLをNTFSセキュリティ形式に適用することはできないため、このオプションでは環境 UNIXまたはmixedセキュリティ形式のみを使用できます。
`-v4.0-acl/-v4.1-acl`	マルチプロトコル環境でのNFSv4.x ACLの有効化は、UNIXセキュリティ形式またはmixedセキュリティ形式のボリュームにのみ影響します。NTFSセキュリティ形式では、NTFS ACLのみが認識されます。使用しているNFSのバージョンでACLを有効にする必要があります。たとえば、NFSv4.1を使用する場合 `-v4.1-acl`は、を有効にします。2つのNFSバージョンのどちらか1つしか使用していない場合は、両方を有効にする必要はありません。 **注** ：ONTAP 9.8以降では、NFSv4 4.2はサポートされていますが、有効にするNFSオプションはありません。NFSv4.1を有効にすると有効になります。
`-v4-numeric-ids`	`-v4-numeric-ids` オプションは、名前の文字列に一致しない場合にNFSv4.xユーザが数値識別子を利用できるかどうかを決定します。つまり、NFSv4.xではユーザ名を解決するためにNFSv3が使用されるようになり、ドメインIDの文字列をマッピングする必要がなくなります。デフォルトでは、この値は20%です。 マルチプロトコルのNAS環境では、NFSのユーザ名が数値IDとして到着し、（ローカルのfiles/passwdサービスまたはネームサービスを使用して）適切なユーザ名に解決できない場合、UNIXセキュリティ形式のオブジェクトは通常どおり動作します。ただし、NTFSセキュリティ形式では、権限を正確に把握できるように、有効なWindowsユーザにマッピングするための有効なユーザ名が必要になります。 ユーザ名が数字のID 1234で表示 `DOMAIN\1234`され、その数字のIDに対応する有効なUNIXユーザ名がONTAP で見つからない場合、そのユーザのWindowsユーザにマッピングが試行されます。一般に、これらのようなWindowsユーザは存在しないため、NTFSセキュリティ形式のマッピング/認証は失敗します。これは、LDAPなどのマルチプロトコルNAS環境でUNIXユーザ名を適切に解決する手段を持つことの重要性を強調しています。詳細については、TR-4067を参照してください。
`-auth-sys-extended-groups*`	このオプションは'拡張グループを有効にするか無効にするかを制御しますデフォルト `auth_sys auth_gss`では、NFSの処理でサポートされるGIDはユーザあたり最大16個で、GIDは32個です。つまり、あるユーザがNFSでサポート可能な数を超えるグループに属する場合、追加のグループはNFS RPCパケットから破棄され、権限やアクセスの不整合が発生します。

オプション	マルチプロトコルのNASに及ぼす影響
	拡張グループでは、ネームサービスからユーザのグループメンバーシップをプリフェッチし、グループメンバーシップを逆クエリすることで、ユーザごとに最大1、024のグループをサポートできます。マルチプロトコルのNAS環境では、ネームサービスを使用する場合にこのオプションを有効にして、すべてのWindowsユーザ/グループが正しく認識されるようにします。詳細：Support Bulletin TR-4067およびTR-4835
-extended-groups-limit*	このオプションは、拡張グループの最大グループ数を決定します。この値は、32~1、024の範囲で指定できます。ネームサービスサーバへの適切なネットワーク接続と、要求のロードバランシングに必要な数のLDAPサーバがある場合、このオプションのパフォーマンスへの影響は通常最小限です。
-map-unknown-uid-to-default- windows-user*	NTFSセキュリティ形式のボリュームがあり、ユーザーのNFS IDが有効なWindowsユーザー名にマッピングできない場合 -default-win-user、このオプションは、不明なUIDがオプションで定義されたデフォルトのWindowsユーザーにマップされるかどうかを制御します。これは、*すべて*の受信不明なUIDが、指定されたWindowsユーザーにマップされることを意味します。他のユーザーとして動作する予定のユーザーも含まれます。 このオプションのデフォルト値 - default-win-userは[有効]ですが、値は設定されていません。したがって、すべての受信不明ユーザがWindowsユーザにマッピングされないようにデフォルトで動作します。このため、NTFSセキュリティ形式へのアクセスを試みる不明なUIDは認証に失敗します。 通常、デフォルトのWindowsユーザーを設定することはお勧めしませんが、アプリケーションを適切に機能させる必要がある場合があります。その場合は、分離されたSVMを各アプリケーション専用にすることを推奨します。これはグローバルオプションであるためです。
-ntacl-display-permissive-perms*	このオプションは ls -la、などのコマンドを実行する際に、NFSクライアントのエンドユーザにNTFS形式のアクセス権を表示する方法を制御します。NFSはNTFSのセキュリティセマンティクスを理解していないため、クライアントにはデフォルトで777と表示される権限が表示されます。これにより、NTFS ACL /ネームマッピングによって権限が制御されるため、ユーザに不要なアラームが生成されます。また、特定の方法で表示される権限に依存する一部のアプリケーションワークフローを中断することもできます。-ntacl-display-permissive-perms がenabledに設定されている場合、ONTAPはファイルにアクセスするユーザに概算の権限を送信し、共有にアクセスするユーザが実行できる操作とできない操作をより正確に描写します。
-v3-ms-dos-client	このオプションは、SVMでWindows NFSを使用できるかどうかを有効にします。このオプションの詳細については、TR-4067を参照してください。ここでマルチプロトコルNASが及ぼす影響は、Windows NFSの設定（名前とグループのサーバへの提示方法など）によって異なりますが、通常のNFSクライアントの場合と同じ一般的なルールがWindows NFSに適用されます。
-ignore-nt-acl-for-root*	このオプションは、NFSのrootユーザのNTFSセキュリティ形式のボリュームに対する動作を制御します。デフォルトでは、このオプションはDisabledに設定されています。ネゴシエートを支援するためには、rootユーザは他のNFSユーザと同様に有効なWindowsユーザにマッピングする必要があります NTFS 権限有効にすると、rootユーザはすべてのNTFS ACLを無視し、NTFS権限に関係なく、オブジェクトに対する読み取り/書き込みのフルアクセス権を持つUNIX形式のrootユーザと同様の動作をします。このオプションは慎重に使用してください。

オプション	マルチプロトコルのNASに及ぼす影響
-cached-cred-positive-ttl*	このオプションは、NAS環境でキャッシュされているクレデンシャルのタイムアウト時間を制御します。ユーザのクレデンシャルが正常に照会されると、ONTAPはそれらをキャッシュしてネームサービスへの接続回数を減らします。デフォルトのタイムアウト値は86、400、000ミリ秒で、24時間に変換されます。これは、ユーザがグループに追加またはグループから削除された場合にマルチプロトコル環境に影響することがあります。これは、キャッシュが24時間経過するか、または手動でフラッシュされるまでアクセスが更新されないためです。ONTAP でのネームサービス とキャッシュの動作の詳細については、TR-4668を参照してください。これらのオプションがLDAPにどのように関連 するかについては、TR-4835を参照してください。
-cached-cred-negative-ttl*	このオプションは、アクセスが拒否されていると検証されたクレデンシャルのタイムアウト時間を制御します。ユーザがファイルまたはフォルダへのアクセスを拒否された場合、キャッシュにはデフォルトで7、200、000ミリ秒（2時間）が設定されます。これは、ユーザがグループに追加またはグループから削除された場合にマルチプロトコル環境に影響することがあります。これは、キャッシュが24時間経過するか、または手動でフラッシュされるまでアクセスが更新されないためです。ONTAP でのネームサービス とキャッシュの動作の詳細については、TR-4668を参照してください。これらのオプションがLDAPにどのように関連 するかについては、TR-4835を参照してください。
-skip-root-owner-write-perm- check*	このオプションは、ルート/所有者からのNFS書き込み呼び出しに対して権限チェックを省略するかどうかを指定します。継承可能なACLがあるデスティネーション フォルダに読み取り専用ファイルをコピーする場合は、このオプションを有効にする必要があります。 警告：有効にすると、NFSクライアントがNFS ACCESS呼び出しを使用してユーザレベルの権限をチェックせず、その後読み取り専用ファイルへの書き込みを試みた場合に処理が成功します。デフォルト設定はdisabledです。
-v4-inherited-acl-preserve*	NFSv4 ACLを使用している場合、このオプションは、親ディレクトリのモードビットがNFSv4 ACLの継承を無視するかどうかを決定します。デフォルトでは、このオプションは無効になっており、この動作は、作成されたファイルが継承された親ACLのモードビットではなくクライアントモードビットを使用することを目的としています。これはRFC 5661では想定される動作です。ただし、ACLを継承する場合は、このオプションを有効にします。
-cached-cred-harvest-timeout*	このオプションは、アクティブに使用されていないキャッシュ内のエントリがキャッシュに保持される期間を制御します。たとえば、user1がクレデンシャルをキャッシュしたあとで、そのクレデンシャルを使用するようにシステムに戻ってこない場合、ONTAPは、ハーベストタイムアウト値の期限が切れたあとにそのエントリを削除します。古いエントリのキャッシュに不要なメモリを使用することはありません。デフォルトのタイムアウト値は86、400、000（24時間）です。TR-4668は、ONTAP でのネームサービスとキャッシュの動作について説明しています。これらのオプションはLDAPに関するものであるため、TR-4835も取り上げます。

付録C：CIFS / SMBサーバオプション

CIFS / SMBサーバには、マルチプロトコルNAS構成で役立つ、設定可能な一連のオプションもあります。表9 に、ONTAP 9.8で使用可能なCIFS / SMBのオプションと、それらのオプションの用途を示します。これらのオプション `cifs options modify`は、コマンドで制御されます。アスタリスクで示されるオプションは、Advanced Privilegeにあります。

表9）マルチプロトコルNASに影響する可能性のあるCIFSサーバオプション-ONTAP 9.8以降

オプション	マルチプロトコルのNASに及ぼす影響
`default-unix-user` -	このオプションは、有効なUNIXネームマッピングルールがないWindowsユーザのマッピングに使用するUNIXユーザを制御します。デフォルト `pcuser`では、このユーザは数字ID 65534に対応するに設定されています。 Windows / SMBクライアント `pcuser`が共有にファイルを作成し、そのファイルを作成するユーザがデフォルトのUNIXユーザにマッピングする場合、そのファイルには所有者が割り当てられます。詳細については、「認証とネームマッピング」の項を参照してください。 • NFSクライアントでは、通常65534 `nfsnobody` がユーザにマッピングされます。`pcuser`その ため、/65534を指定`nfsnobody`すると、NFSのファイル/所有者が代わりに表示されます。NFSマウントでこの動作が発生する場合、ファイルを作成するWindowsユーザが想定されるユーザ名にマッピングされておらず、デフォルトのUNIXユーザにフォールバックしている可能性があります。 • NTFSセキュリティ形式のボリュームでは、UNIX所有者に関係なくWindowsアクセス権が適用されます。UNIXのセキュリティ形式 `pcuser` では、ファイル所有者に問題がある可能性があります。
`-read-grants-exec`	UNIXセキュリティ形式では、モードビットとNFSv4 ACLを使用して、ファイルまたはフォルダへのアクセスが許可または拒否されます。ファイルが読み取り専用に設定されている場合、実行ビット（x）は設定されません。この設定は、デフォルトでは実行が適切に機能するように設定する必要があるため、CIFS / SMBクライアントからファイルを実行する際に問題が発生する可能性があります。場合によって `read-grants-exec`は、これらのファイルにexecuteを設定できないため、ONTAP にはこの制限を回避するCIFSオプションが用意されています。
`-is-local-auth-enabled`	CIFS / SMBサーバのローカル認証はワークグループモードのONTAP で使用されます。これは、ドメインコントローラやActive Directoryを実装しなくてもCIFS / SMBへのアクセスを可能にする方法です。 マルチプロトコルNASでワークグループモードを使用する場合でも、Windowsユーザを同じ名前のUNIXユーザにマッピングするか、ネームマッピングルールを使用して別のUNIXユーザにマッピングする必要があります。 この機能は、デフォルトで有効に設定されています。
`-is-local-users-and-groups-enabled`	CIFS / SMBサーバのローカル認証はワークグループモードのONTAP で使用されます。これは、ドメインコントローラやActive Directoryを実装しなくてもCIFS / SMBへのアクセスを可能にする方法です。 マルチプロトコルNASでワークグループモードを使用する場合でも、Windowsユーザを同じ名前のUNIXユーザにマッピングするか、ネームマッピングルールを使用して別のUNIXユーザにマッピングする必要があります。

オプション	マルチプロトコルのNASに及ぼす影響
	この機能は、デフォルトで有効に設定されています。
is-exportpolicy-enabled -	このオプションを使用すると、CIFS / SMB共有のエクスポートポリシーとルールを使用できるようになります。エクスポートポリシーとルールを使用する利点は、サブネットまたはホスト名/ IPアドレス経由でアクセスを制御できることです。このオプションはデフォルトで無効になっています。 CIFS / SMB共有 name-mapping create へのアクセスを制限する別の方法として、共有レベルの権限を組み合わせ、コマンドを使用してSMBクライアントをWindowsユーザ名にマッピングする方法があります。詳細については、「Windowsクライアントからユーザー名へのマッピング」を参照してください。」
-is-unix-nt-acl-enabled	このオプションは、CIFS / SMBクライアントおよびセキュリティタブを使用して、UNIXセキュリティ形式のボリュームに対するUNIX権限を表示できるかどうかを制御します。詳細については、「NFSクライアントからのNTFSアクセス権の表示」を参照してください。
-is-trusted-domain-enum-search-enabled	CIFSサーバが双方向の信頼関係を持つドメイン内にあり、UNIXユーザを両方のドメインのWindowsユーザにマッピングする場合は、このオプションを有効にします。デフォルトでは、このオプションは無効です。
-is-read-only-delete-enabled	（オプション）このパラメータは、読み取り専用のファイルとディレクトリの削除を制御します。NTFSの削除セマンティクスでは、読み取り専用属性が設定されたファイルやディレクトリの削除は禁止されます。UNIXの削除セマンティクスでは属性が無視され、代わりに親ディレクトリのアクセス権が尊重されます。一部のアプリケーションにはこの動作が必要です。このオプションを使用して、必要な動作を選択します。デフォルトでは、このオプションは無効になっており、NTFSの動作が優先されます。
-is-unix-extensions-enabled	このオプションを使用すると、UNIXベースのSMBクライアント（MacOSやLinux Sambaなど）がPOSIX/UNIXセキュリティ情報をSMB経由でUNIXベースのSMBクライアントに送信して、変換して適切なPOIX/UNIXセキュリティを表示できるようになります。これは、ONTAP でサポートされていないPOSIX ACLまたは拡張属性(xattr)のサポートとは異なります。
-is-search-short-names-enabled	このオプションは、ONTAP によるCIFS / SMB 8.3の短縮名の処理方法を制御します。詳細については、「ネットワークファイルシステム（NFS）およびSMB / CIFSのファイル名の命名規則と、ファイル名の最大長について」を参照してください。
-guest-unix-user	（オプション）このパラメータは、信頼されていないドメインから接続する認証されていないユーザを、CIFSサーバの指定したUNIXユーザにマッピングする場合に指定します。CIFSサーバがホームドメインまたは信頼できるドメインのドメイン コントローラ、もしくはローカル データベースに対してユーザを認証できず、このオプションが有効である場合、CIFSサーバはユーザをゲスト ユーザとみなし、そのユーザを指定したUNIXユーザにマッピングします。UNIXユーザは有効なユーザである必要があります。
-is-admin-users-mapped-to-root-enabled	このオプションは、SVMのBUILTIN\Administratorsグループに追加されたユーザをrootユーザにマッピングするかどうかを制御します。このユーザ名はrootにマッピングされ、ファイルがrootとして書き込まれ、rootの権限が付与されます。このオプションの詳細については、「Windows管理者ユーザーのrootへのマッピング」を参照してください。

オプション	マルチプロトコルのNASに及ぼす影響
`-is-use-junctions-as-reparse-points-enabled`	このオプションはデフォルトで有効になっており、ONTAP でジャンクションパスとしてマウントされたボリュームをWindows / SMB クライアントが表示する方法を制御します。 有効な場合： • ジャンクションパス `<JUNCTION> dir`は、コマンドをcmdで使用した場合と同様に表示されます。 • Windowsエクスプローラでは、ジャンクションパスがショートカットフォルダとして表示されます。 無効にした場合： • ジャンクションパスは、WindowsエクスプローラおよびcmdでSMBクライアントへの通常のディレクトリとして表示されます。 詳細については、「ジャンクションパスとリパースポイント」を参照してください。
`-grant-unix-group-perms-to-others`	（オプション）このパラメータは、ファイルの所有者ではない接続元のCIFSユーザにグループ権限を付与するかどうかを指定します。接続元のCIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合に、このオプションをtrueに設定すると、ファイルの「グループ」権限が常に付与されます。接続元のCIFSユーザがUNIXセキュリティ形式のファイルの所有者ではない場合に、このオプションをfalseに設定すると、通常のUNIXルールに従って権限が付与されます。このパラメータのデフォルト値はfalseです。
`-widelink-as-reparse-point-versions`	このオプションは、システム内に作成されたワイドリンクをリパースポイントとして表示するSMBバージョンを制御します。デフォルトではSMB1に設定されますが、SMB2とSMB3に対してこの動作を有効にできます。詳細については、「ジャンクションパスとリパースポイント」を参照してください。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- TR-4067: NetApp ONTAP Best Practices and Implementation Guide
  https://www.netapp.com/us/media/tr-4067.pdf
- TR-4569：Security Hardening Guide for NetApp ONTAP 9
  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf
- TR-4571：『NetApp FlexGroup Volumes Best Practices』
  https://www.netapp.com/us/media/tr-4571.pdf
- TR-4616：『NFS Kerberos in NetApp ONTAP』
  https://www.netapp.com/us/media/tr-4647.pdf
- TR-4668：『Name Services Best Practices - NetApp ONTAP』
  https://www.netapp.com/us/media/tr-4647.pdf
- TR-4743：FlexCacheとONTAP
  https://docs.netapp.com/ja-jp/flexpod/security/security-ransomware_what_is_ransomware.html
- TR-4835：『How to Configure LDAP in NetApp ONTAP』
  https://www.netapp.com/media/17115-tr-4810.pdf

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2021年4月	初版リリース

本ドキュメントに記載されている、特定バージョンの製品と機能がお客様の環境でサポートされるかどうかは、ネットアップ サポート サイトにあるInteroperability Matrix Tool（IMT）で確認してください。NetApp IMTには、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4887-0421-JP

NetApp