テクニカル レポート

NetApp ONTAPのマルチプロトコルNAS
概要とベストプラクティス

NetApp
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でのマルチプロトコルNASアクセスの仕組みと、マルチプロトコル環境におけるベストプラクティスについて説明します。

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

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しているNetAppストレージシステムでのマルチプロトコルNASアクセスについて説明します。マルチプロトコルNASアクセスにより、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は、それぞれ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す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の用語については、本ドキュメントの「マルチプロトコルNASの用語」セクションを参照してください。

NASとは

基本的には、その名のとおりマルチプロトコルNASです。複数のNASプロトコルを使用した統合NASアクセスです。NetAppストレージシステムでマルチプロトコルNASを活用すると、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使用されるプロトコルは、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。

よくある誤解として、マルチプロトコルNASは混合モードとも呼ばれます。この誤解が原因で、NASを実行するNetAppストレージシステムを実装する際に混乱が生じます。これは、mixedセキュリティ形式の概念も存在するためです。mixedセキュリティ形式については、このドキュメントの後半で説明します（「セキュリティ形式」のセクションで説明します）。

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上の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間の通信の基盤プロトコルとしてSMBを活用します。

CIFS/SMBは、Sambaなどのサードパーティの実装を通じて、Apple、Linux、SolarisなどのWindows以外のオペレーティングシステムでも使用されています。NetApp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のサポートは状況によって異なり、Interoperability Matrix Tool（IMT）を参照してください。

注：CIFSとSMBにはさまざまな意味がありますが、本ドキュメントではこれらの用語を同じ意味で使用しています。

NFSとは

NFSは、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の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。NFSは、Request for Comments（RFC）と呼ばれるドキュメントを通じてInternet Engineering Task Force（IETF；インターネット技術特別調査委員会）によって定義された一連の標準に従います。これらの標準は、エンタープライズレベルのNFSアクセスを提供するすべての主要なNFSクライアント/サーバベンダーに準拠しています。NFSは、使用するNFSのバージョンに応じた一連のメッセージに依存します。ONTAPでの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。

同機種NAS環境と異機種NAS環境

一部のサイトでは、純粋なWindows環境または純粋なUNIX環境を使用して、すべてのデータが次のいずれかを使用してアクセスされます。

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

ただし、多くのサイトでは、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。このような環境では、ONTAPでマルチプロトコルNASが標準でサポートされます。ユーザがネットワーク上で認証され、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割り当てられたら、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、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NASアクセスを活用するには、オプションとして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、明確なメリットがいくつかあります。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なると、次のようなメリットが得られます。

- ストレージ管理者の全体的な管理タスクを軽減
- 複数のクライアントからNASにアクセスするには、データのコピーを1つだけ格納する必要があります。
- 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、エンドユーザに提供するACLの形式とアクセス制御を制御できます。
- アイデンティティ管理オペレーションをNAS環境で一元化

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環境でさらに柔軟性を高めることができます。

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
- 研究とエンジニアリングのシェア
- 画像リポジトリ
- 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アクセスは柔軟性に優れていることから多くの組織に好まれていますが、マルチプロトコルNASには難しさが認識されており、プロトコル間での共有という概念に固有の課題がいくつか存在します。この認識は現実に基づいていますが、基盤となるインフラがマルチプロトコルNASアクセス向けに準備され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合わせてLightweight Directory Access Protocol（LDAP）サーバをセットアップすると、マルチプロトコルNAS環境を大幅に簡易化できます。

次のような課題がありますが、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
- ネームサービスサーバ（DNS、LDAP、NISなど）の実用的な知識。
- 次のような外部要因
  - 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
  - ドメインの統合
  - 再編成
  - 多数の可動部品

このような現実的な課題にもかかわらず、ベストプラクティスに従っていれば、マルチプロトコルNASのセットアップ、設定、アクセスをどのような環境にも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、可能な限り簡単な方法でマルチプロトコルNASを設定および管理する方法について説明します。

ONTAPのマルチプロトコルNASの仕組み：基本

大まかに言うと、ONTAPのマルチプロトコルNASは、ネームマッピングと権限形式を組み合わせて使用することで、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とSMBのどちらからファイルにアクセスしている場合でも、それらのファイルにアクセスできるユーザはアクセスでき、アクセスできないユーザはアクセスできません。

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、一連の処理がバックグラウンドで実行され、エンドユーザに最も透過的なエクスペリエンスが提供されます。

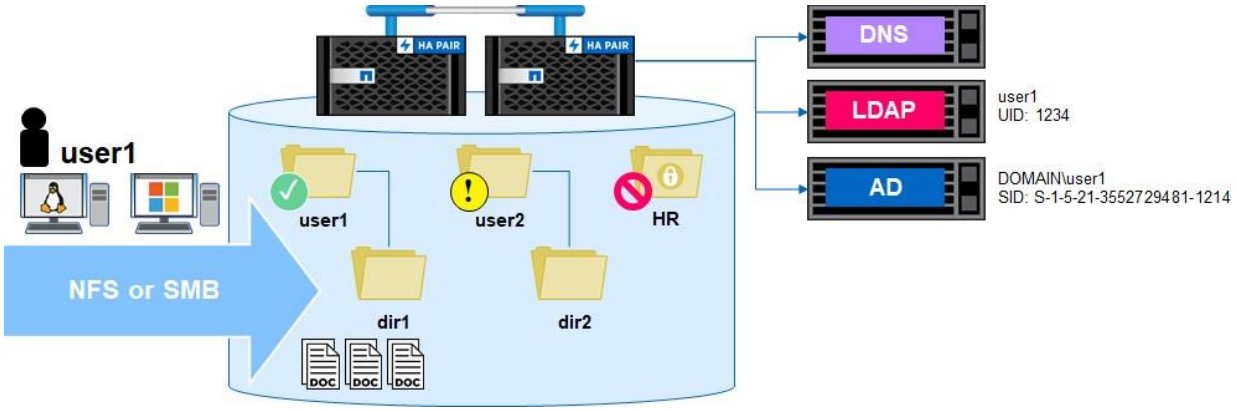
このプロセスは、ONTAPの設定方法によって制御されますが、一般的な概念は引き続き適用されます。

1. NASクライアントがONTAP Storage VMにNAS接続を確立します。
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がネームサービスで検索できる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がSMBまたはNFSを介してONTAP Storage Virtual Machine（SVM）内の共有に対して認証します。ONTAPは、LDAPおよびActive Directoryでユーザを検索し、ユーザ1:1をマッピングします。その後、ユーザはuser1であることが確認され、user1のアクセス権が取得されます。

この場合、ユーザは自分のフォルダに対するフルコントロール、user2のフォルダに対する読み取りアクセス権、HRフォルダへのアクセス権を取得します。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クライアントに分離された一意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、Active Directory設定、権限モデルを設定でき、NAS環境の単一のネームスペースとして機能できます。

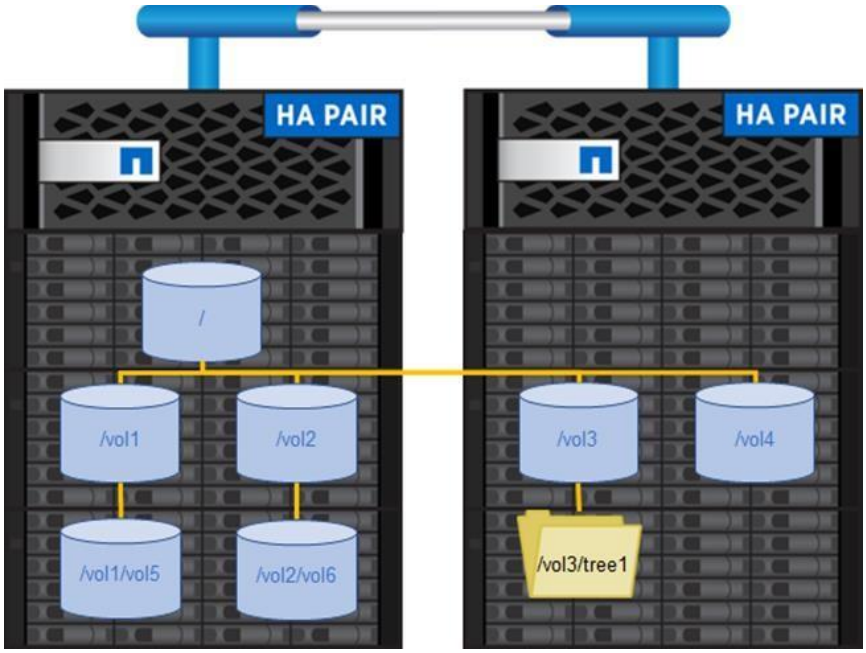
クラスタネームスペース

ONTAPのネームスペースは、拡張性に優れたパフォーマンスと容量を提供するために、クラスタ内の複数のノードでホストされるファイルシステムの集まりです。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。このネームスペースはの場所から始まります。後続のボリュームおよびqtreeはすべてがをトラバースし、ボリュームオプションで定義されたエクスポートパスを持ちます `-junction-path`。SVMネームスペースは1つ以上のボリュームで構成できます。ボリュームはジャンクションでリンクされ、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。クラスタには複数のSVMを含めることができますが、各SVMに割り当てられるvsrootとが1つだけであるため、各SVMには一意のファイルシステムIDのセットが割り当てられます。これにより、複数のSVMにあるボリュームでファイルシステムID /ファイルハンドルが共有されるのを防ぎ、マルチテナント環境でのNFSエクスポートのマウントに関する問題を回避できます。

SVMに属するすべてのボリュームは、エクスポートパスを使用して、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（「/」）は統合されたディレクトリで、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にアクセスできても、クラスタ内の単一のノードにのみ存在します。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であるため、NFSの処理にとって非常に重要です。

```
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形で使用できない場合、ファイルシステムをトラバースするためにvsrootボリュームが必要になるたびにNFSクライアントが問題を解決します。

このプロセスには、次の動作が含まれますが、これらに限定されません。

- マウント要求がハングします。
- 「/」がマウントされている場合、「/」から別のボリュームへのトラバーサル（`cd`） `ls`は停止します。

- ボリュームがオンラインに戻っても、マウントがビジー状態であるために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でマウントされている場合（など） `/vol1`も、読み取り/書き込み/一覧表示は引き続き成功します。

ONTAPの負荷共有ミラー（LSミラー）を使用すると、NetApp ONTAP SnapMirror® 機能を活用してvsrootの耐障害性を高めることができます。

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場合は、代わりに「NetApp FlexCacheボリューム」を使用することを検討してください。

vsrootボリュームで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ミラーを使用している場合は、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。

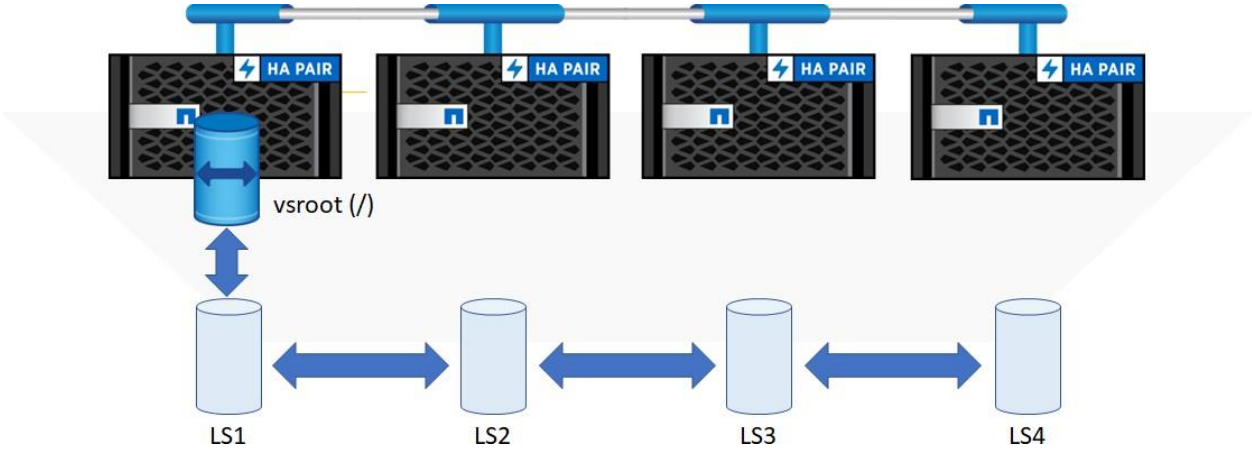
詳細については、負荷共有ミラー関係の作成と初期化を参照してください。

NetApp環境では、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クライアントでは、NFSv4.xプロトコルの性質上、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が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ボリュームのサイズを確認し、新しいボリュームのサイズがすべて同じであることを確認してください。
2. クラスタ内の各ノードで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ノードクラスタでは、タイプがDPの新しいボリュームを4つ作成します。
3. vsrootソースから、作成した新しいDPボリュームごとに新しいSnapMirror関係を作成します。ネームスペース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アーキテクチャにより、RFC 7530 NFSv4標準に準拠した真の疑似ファイルシステムの構築が可能になりました。

```
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：

```
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では /vol、ONTAP 7-Modeでのエクスポートボリュームに関する要件が廃止され、疑似ファイルシステムに対してより標準化されたアプローチが使用されるようになりました。これにより、///vol/vol07-Modeではのリダイレクタではなくが機能するため、既存のNFSインフラをNetApp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。

疑似ファイルシステムが適用されるのはONTAP、権限がより制限の厳しいものからより制限の低いものへと流れている場合だけです。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（など）よりも制限が厳しい場合、 /volname疑似ファイルシステムの概念が適用されます。

疑似ファイルシステムを使用すると、ストレージ管理者は、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、必要に応じて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。

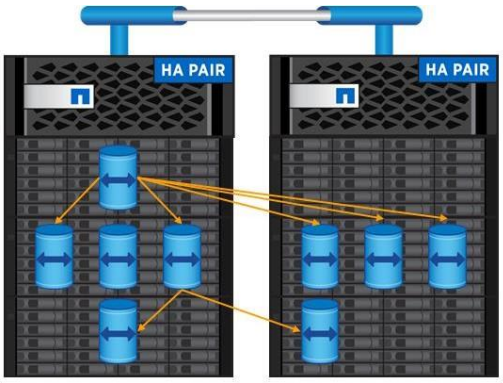
ジャンクション パス

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、ボリュームをqtree、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し、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を超える容量をサポートするジャンクションアーキテクチャを使用したFlexVol設計を示しています。

図4）100TBを超える容量向けのジャンクションアーキテクチャを備えたFlexVol設計



注：ジャンクションパスアーキテクチャでは、FlexVolボリュームとFlexGroupボリュームの両方を使用できます。

FlexVol

フレキシブルボリュームであるNetApp FlexVolソフトウェアは、2005年にData ONTAP 7.0（Data ONTAP 7-Mode）リリースでONTAPソフトウェアに導入されました。その目的は、ストレージファイルシステムをハードウェア構成全体で仮想化し、絶えず変化するデータセンターで柔軟なストレージ管理を実現することでした。

FlexVolボリュームは、システムを停止することなく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て、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す。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

qtreeを使用すると、ストレージ管理者はONTAPのGUIまたはCLIからフォルダを作成して、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、独自のセキュリティ形式、クォータ、および詳細統計を有効にすることで、データ管理を柔軟に行うことができます。

qtreeには複数のユースケースがあり、ホームディレクトリのワークロードに役立ちます。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ることができ、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るためです。

FlexGroupボリューム内のqtreeに関する詳細情報を次に示します。

- qtreeは、クライアントには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。
- SnapMirrorを使用してqtreeをレプリケートすることはできません。SnapMirrorは現在、ボリュームレベルでのみ実行されます。ボリュームを使用したレプリケーションをさらに細かく行う場合は、ジャンクションパスを使用します。
- ボリュームあたり最大4、995個のqtreeがサポートされます。クォータの監視と適用（FlexGroupボリュームのONTAP 9.5以降では適用）は、qtreeレベルまたはユーザレベルで適用できます。

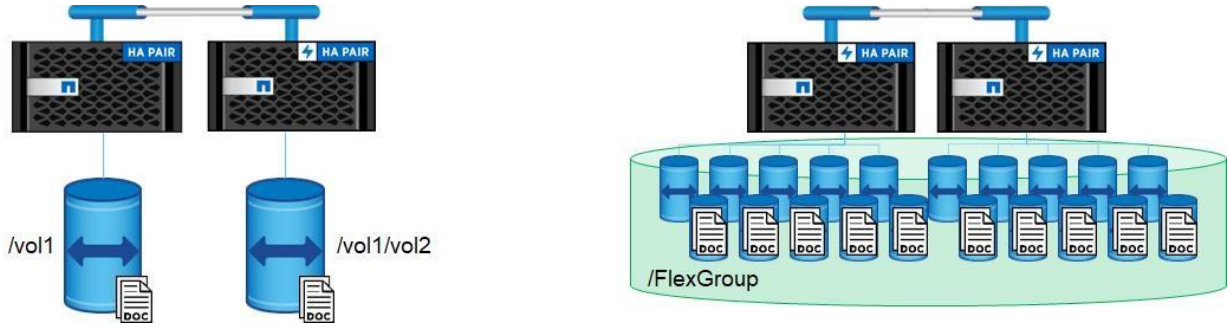
FlexGroupボリューム

FlexGroupボリュームは、FlexVolの概念を取り入れ、複数のFlexVolボリュームをグループ化して単一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拡張しました。この制限は100TBと20億ファイルをはるかに超え、単一のFlexVolボリュームが提供するリソースでボトルネックになる可能性があるワークロードのパフォーマンスがさらに向上しました。

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。FlexGroupボリュームには、ハードウェアの物理的な制限やONTAPの総ボリューム制限以外では、容量やファイル数の制約は事実上ありません。制限は、連携して負荷を動的に分散し、すべてのメンバーにスペースを均等に割り当て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。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す。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の比較です。

図5）FlexVolボリュームとFlexGroupボリュームのアーキテクチャの比較



NetApp FlexGroupボリューム：NetAppワークロードへの電力供給

ソフトウェア機能の最も真のテストの1つは、ソフトウェアの作成者が独自の機能を使用しているかどうかです。

この質問に対する回答は、「はい」という響きがあります。NetAppは、独自の開発環境やNetApp Active IQデータレイク内のFlexGroupボリュームを活用し、他の多数のワークロードユースケースで使用します。

NetAppでの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テクノロジがNetApp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：NetApp on NetApp-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場合は、次の2つのボリューム形式から選択できます。

- **FlexVolボリューム** は、ONTAPで使用できる標準の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るボリュームです。
- **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あり、FlexVolよりも次のような多くの利点があります。
  - ボリュームサイズが100TBを超える（テスト済みの20PB）。
  - ファイル数が20億を超える（テスト済みの4、000億）。
  - 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する機能。
  - 使いやすいFlexVolに似た管理機能。
  - ボリュームの容量が上限に達したときに無停止で拡張できます。

ほとんどのNFSワークロードでは、FlexGroupボリュームはFlexVolボリュームよりも多くのメリットをもたらします。この決定を行う際の主な注意点は、ボリューム形式間の機能のパリティを確認して、ご使用の環境で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。導入や決定ポイントの詳細など、FlexGroupボリュームの詳細については、TR-4571：『NetApp FlexGroup Volume Best Practicesand Implementation』を参照してください。

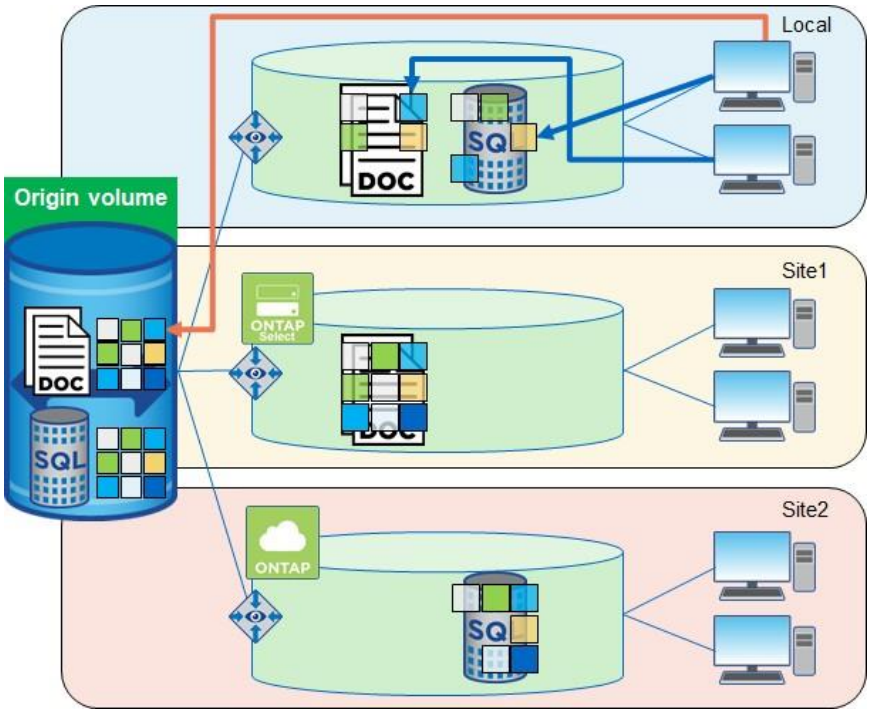
NetApp FlexCacheボリユウム

ONTAPのNetApp FlexCache®テクノロジは、一貫性、一貫性、最新性を備えた、リモートの場所にあるボリュームの書き込み可能な永続的キャッシュを提供します。

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ストレージの場所です。キャッシュの目的は、ソースデータからデータをフェッチするよりも高速にデータを提供できるように、ソースデータの頻繁にアクセスされる部分を格納することです。キャッシュは、データが複数回アクセスされ、複数のホストで共有される読み取り処理の多い環境で最も効果的です。

図6 は、NetApp FlexCacheボリュームを示しています。

図6）NetApp FlexCacheボリューム



キャッシュでは、次の2つの方法のいずれかを使用してデータを迅速に提供できます。

- キャッシュシステムの方が、データソースを使用するシステムよりも高速です。そのためには、ストレージの高速化（HDDよりも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のメモリの高速化（または高速化）が必要です。
- 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、データに到達するまでにそれほど時間はかかりません。

キャッシュは、さまざまなアーキテクチャ、ポリシー、セマンティクスで実装されるため、データがキャッシュに保存されてホストに提供されるときにデータの整合性が保護されます。

FlexCacheテクノロジには、次のようなメリットがあります。

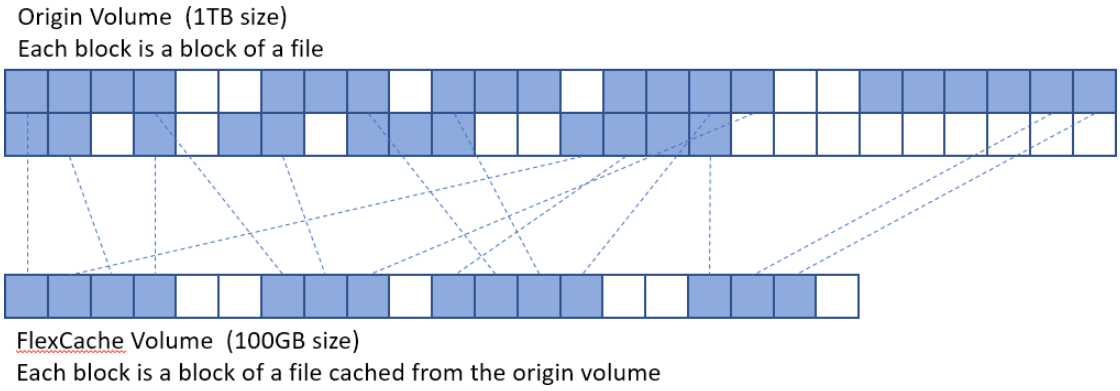
- 負荷分散によるパフォーマンスの向上
- クライアントアクセスポイントの近くにデータを配置することでレイテンシを低減
- ネットワーク切断時にキャッシュされたデータを提供することで可用性を向上

FlexCacheテクノロジは、キャッシュの一貫性、データの整合性、データの通貨性、ストレージの効率的な使用をスケーラブルで高性能な方法で維持しながら、上記のすべてのメリットを提供します。

FlexCacheボリュームはスパースコンテナであり、元の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。また、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できるわけではありません。作業データセット（最近使用したデータ）の保持に優先順位を付け、ストレージを効率的に使用します。図7 に、スパースボリュームの詳細を示します。

FlexCacheテクノロジを使用すると、ディザスタリカバリやその他の企業データ戦略の管理をオリジンに実装するだけで済みます。データ管理はソース上でのみ行われるため、FlexCacheテクノロジを使用すると、リソースをより効果的かつ効率的に使用できるようになり、データ管理とディザスタリカバリの戦略がシンプルになります。EDAワークロードについて、SemiWikiでは、地理的に分散した設計チームが、同時実行およびコラボレーションで作業データセットの現在のキャッシュと同期を維持し、分散した設計チームをNetAppと同期させる方法をFlexCacheボリュームがどのように提供するかについて説明します。

図7）スパースボリュームの詳細



ユースケース

FlexCache in ONTAP設計は、特定のユースケースに最適なメリットを提供します。これらのユースケースには理想的なユースケースが記載されています。FlexCacheボリュームの他のユースケースも可能ですが、そのメリットは十分に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。理想的でないユースケースも推奨されませんが、FlexCacheのメリットと理想的でない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、読み取り負荷の高いワークロードに適しています。書き込みにはレイテンシが発生します。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影響しません。次のような例がありますが、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
- Gitなどのソフトウェアビルド環境
- 共通ツールの配布
- ホットボリュームのパフォーマンス調整
- クラウドバースティング、高速化、キャッシング
- NetApp MetroCluster™ 構成全体でNASボリュームを拡張

ネットワーク アクセス

一元化された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のネットワークの概念と、DNSなどのNAS展開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を介してクライアントにIPアドレスを提供します。物理ネットワークポートに存在する仮想IPアドレスで、ノードまたはポートに障害が発生した場合に自動的に他のネットワークポートに移行されます。ノードのメンテナンスやクラスタからのノードの退避が必要な場合は、手動で移行できます。 または、LIFのホームポートを変更したいだけです。

データLIFでは、ifgrpまたはVLANを基盤となるポートとして使用でき、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

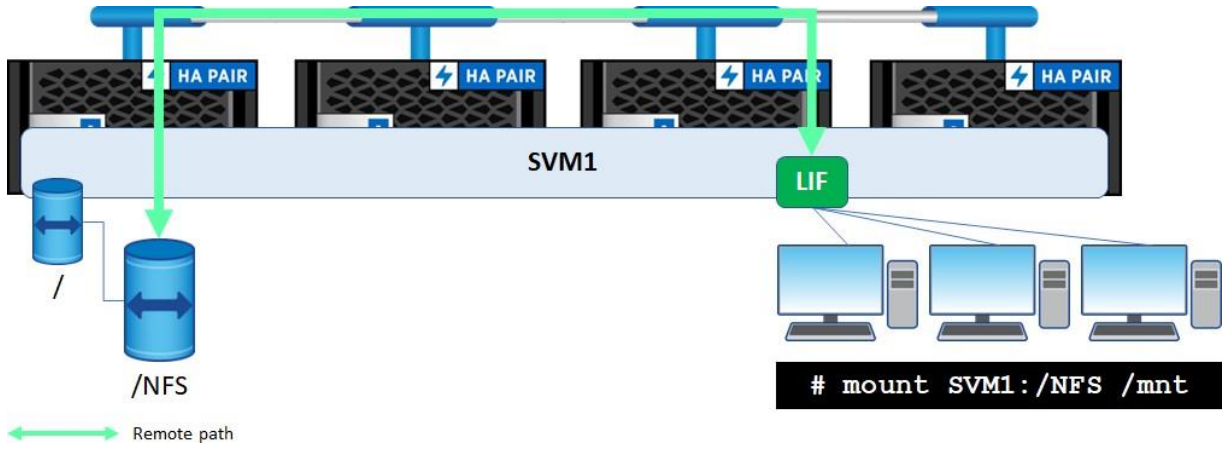
データLIFは、有効なブロードキャスト ドメインに追加された、クラスタ内の任意のポートに配置できます。データLIFはSVM対応のルーティング メカニズムで設定されるため、有効なデータLIFがクラスタ内のどこにあるかにかかわらず、SVM内のイーサネット トラフィックは正しく転送されます。NASインタラクション用のネットワークを設計する場合は、2つのアプローチのいずれかを実行できます。

オプション1：簡易化アプローチ- SVMあたりのLIFは1つ

基本的に、ONTAP内のNASデータにアクセスするために必要なのは、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アドレスだけです。多くの環境では、1つのネットワークインターフェイスでNASワークロードを処理できます。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、またはストレージノードがHAパートナーにテイクオーバーされた場合、ネットワークIPアドレスはクラスタ内の別の動作中ポートに移行されます。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アドレスの数が削減されますが、ワークロードで使用できる可能性のあるネットワーク帯域幅も制限されます。すべてのNASトラフィックをクラスタ内の1つのノードに送信すると、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への接続が予想されるワークロードの場合は、オプション2の方が適しています。

図8 は、単一のLIFのNASの連携を示しています。

図8）単一LIFのNASの連携



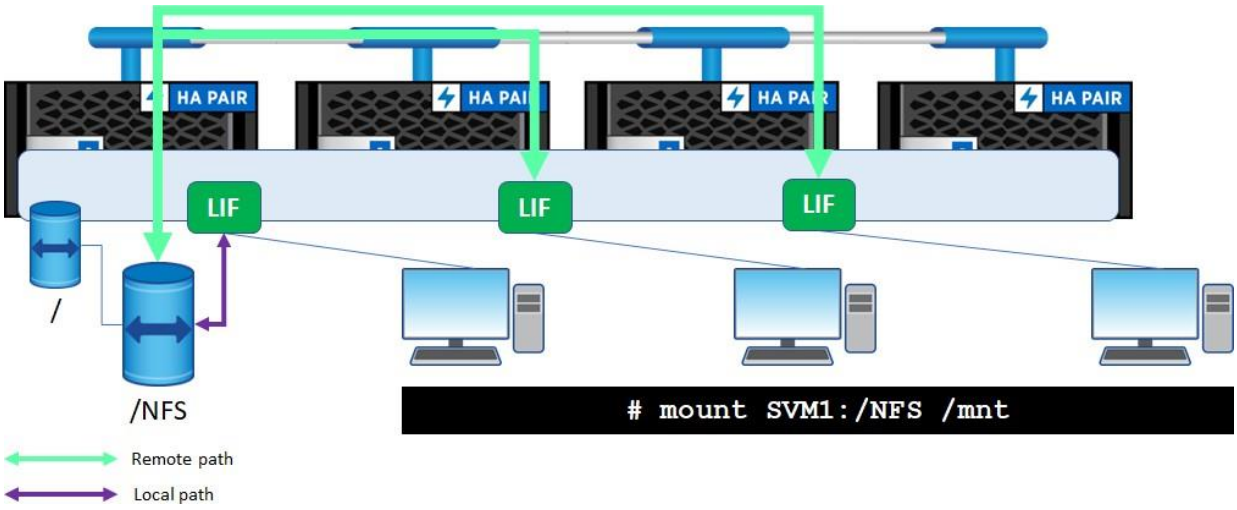
オプション2：パフォーマンスアプローチ- SVMごとに複数のデータLIFを使用

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に使用できます。NASを使用するONTAPクラスタは、最大24ノードまで拡張できます。複数のノードとは、CPU / RAM /ネットワークインターフェイスなど、複数の物理リソースを意味します。そのため、1つの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とネットワークポートの競合が軽減され、ノードのTCP接続数が多すぎるシナリオが回避されます。NAS接続のネットワークロードバランシングには、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を利用できます。内蔵DNSの詳細および設定方法については、TR-4523：『ONTAPにおけるDNSロードバランシング』を参照してください。

可能なかぎり最高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1つのNASデバイスに同時にアクセスする場合は、SVMごとに複数のデータLIFを作成することを推奨します。さらに、NFSリファーラル、CIFSオートロケーション、pNFSなどのNAS機能のロードバランシングを使用すると、データが格納されている各ノードにデータLIFが必要になります。

図9 は、複数LIFのNASの連携を示しています。

図9）複数のLIF NASの連携



データLIFの局所性に関する推奨事項

ONTAPでは、ボリュームがクラスタ内でどこにあるかに関係なく、NFSリファーラル、CIFSオートロケーション、pNFSなどのデータ局所性機能をNASトラフィックに利用できます。NFSリファーラルおよび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ボリュームの場合は、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は最初のマウント要求でメタデータパスを提供しますが、すべての読み取りと書き込みは、pNFSレイアウト呼び出しによって自動的にローカルボリュームにリダイレクトされます。pNFSは、NFSv4.1プロトコルでのみ使用でき、pNFSをサポートするNFSクライアントでのみ使用できます。pNFSの詳細については、TR-4067：『NFS BestPractice and Implementation Guide』を参照してください。

オートロケーション機能を使用しない場合、データLIFの局所性を管理してクラスタネットワークを回避すると、管理が複雑になりますが、ほとんどのNASワークロードのパフォーマンスへの影響はごくわずかであるため、面倒な作業は不要です。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や大規模なクラスタバックエンドネットワークでは、これはそれほど重要ではありません。

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でのデータローカリティのメリットと考慮事項、およびこれらの概念へのシンプルさを念頭に置いたアプローチ方法について説明します。

- **ノード間で負荷を分散し、クラスタ内の使用可能なすべてのハードウェアを活用する機能。**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、パフォーマンスヘッドルームを最大化するために、クラスタ内の複数のノードにワークロードを導入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 System Managerを使用すると、ストレージのプロビジョニングが自動化されます。このアプローチでは、利用可能なパフォーマンスヘッドルームが考慮され、利用率の低いノードに新しいボリュームが配置されます。さらに、FlexGroupボリュームは、クラスタ内の複数のノードにわたってプロビジョニングし、単一のネームスペースにワークロードを自動的に分散します。
- **複数のクラスタノード間でネットワーク接続を分散する機能。**クラスタはSVM同様に単一のエンティティです。ただし、基盤となるハードウェアには独自の最大数（接続数など）があります。

シンプルなアプローチ：SVMごとに複数のデータLIFを作成し、ONTAPの内蔵DNS機能を利用して、それらのインターフェイスをDNSラウンドロビン名またはDNS転送ゾーンの背後にマスクします。さらに、FlexGroupボリュームを活用して、複数のノードにワークロードを分散します。

- **ボリューム移動時にデータの局所性を有効にする機能。**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のボリュームを新しいノードに移動する場合、NASクライアントでは既存のTCP接続が維持されます。その結果、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：何もしない。ほとんどの場合、NASクライアントはこれらのNAS共有に対するパフォーマンスの違いに気付きません。NFSv4.1の場合は、pNFSの使用を検討してください。

NASに関する一般的な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解決策を設計する場合は、ボリュームの形式に関係なく、ネットワークに関する次のベストプラクティスを考慮してください。

- 各SVMのノードごとに少なくとも1つのデータLIFを作成して、各ノードへのパスを確認します。
- 何らかの形式のDNSロードバランシングを使用して、単一のFully Qualified Domain Name（FQDN；完全修飾ドメイン名）の背後にあるクライアントに複数のIPアドレスを提供します。DNSロードバランシングの詳細については、TR-4523：『DNS Load Balancing in ONTAP』を参照してください。
- 可能な場合は、スループットとフェイルオーバーに関する考慮事項として、LACPポートを使用してデータLIFをホストします。
- 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で均等に分散します。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の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、組み込みのDNSを使用して負荷を分散すること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ていない場合、内蔵DNSはあまり役に立ちません。
- マウントストームのワークロード（数百、数千のクライアントが同時にマウントされるなど）の場合は、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てください。1つのノードにマウントストームが発生すると、クライアントへのサービス拒否や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、データローカリゼーションとファイルへの並列接続にpNFSを活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。メタデータの多いワークロードは、単一のメタデータサーバ接続でボトルネックになる可能性があります。
- 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ラージ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。ジャンボフレーム構成が一致していないと、どの種類のボリュームでもパフォーマンスの問題を診断するのが困難になる可能性があります。
- NFSクライアントでは、複数のネットワークインターフェイスを使用して、同じクライアントからONTAPの同じボリュームに複数のマウントポイントを接続することで、パフォーマンスを向上させることができます。ただし、この構成は複雑になる可能性があります。NFSクライアントでサポートされている場合は、nconnectを使用します。nconnectについては、TR-4067『NFS in NetApp ONTAP』を参照してください。

LACPに関する考慮事項

クライアント側ネットワークでLACPポートを使用する理由はいくつかあります。一般的で適切なユースケースは、SMB 1.0プロトコルを使用して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保持するため、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プロトコルをあとから実装することで、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実現できます。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を使用するとスループットと耐障害性にメリットがありますが、LACP環境の保守は複雑であることを考慮して決定する必要があります。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（オフボックスとオンボックスの両方）を使用すると、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できます。結局のところ、どのDNSロードバランシングを使用するかは、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まります。DNSロードバランシングの詳細については、TR-4523：『DNS Load Balancing in ONTAP』を参照してください。

ベストプラクティス2：何らかの形式のDNSロードバランシングを使用する

可能な場合は、マルチプロトコルNAS環境で何らかの形式のDNSロードバランシングを使用します。

オンボックスDNSかオフボックスDNSか？

ONTAPは、内蔵DNSサーバを使用してDNSクエリを処理する方法を提供します。この方法では、ノードのCPUとスループットを考慮して、NASアクセス要求を処理するのに最適なデータLIFが特定されます。

- 外部DNSを設定するには、DNS管理者が、データLIFへのラウンドロビンアクセスを提供する外部DNSサーバ上に、同じ名前の「A」名前レコードを複数作成します。
- マウントストームのシナリオを作成するワークロードの場合、ONTAP内蔵DNSサーバが適切に維持およびバランス調整できないため、外部DNSを使用することを推奨します。

ベストプラクティスとして、NetAppでは、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ています。ただし、データLIFの導入方法については、「NAS環境でのデータLIFに関する考慮事項」セクション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によってDNSエイリアスの背後にIPアドレスをマスクすることを推奨します。DNS名は、ストレージへの使いやすく覚えやすいアクセスポイントを提供します。複数のデータLIF用のDNSエントリを作成する予定でKerberosを使用している場合は、DNS A/AAAAレコードがSVMに割り当てられているKerberos SPNと一致するか、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。

- DNSロードバランシングの詳細（決定マトリックスなど）については、TR-4523：『DNS Load Balancing in ONTAP』を参照してください。
- NFS KerberosおよびDNS名がKerberosに与える影響の詳細については、TR-4616：『NFS Kerberos in ONTAP』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、LIFのサービスポリシーが導入されています。これは、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ものです。LIFポリシーをネットワークインターフェイスに適用または削除すると、ネットワークインターフェイスを再作成しなくてもトラフィックを許可または禁止できます。

次のコマンドを実行すると、インターフェイスに設定されているサービスポリシーを確認できます。

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

LIFのサービスポリシーでは複数のデフォルトポリシーが作成されますが、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、NAS、または管理トラフィックを許可するデフォルトのポリシーです。1つのデータLIFに同時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 / SMBのみを許可するポリシーを作成する場合は、`network interface service-policy createnetwork interface service- policy add-service` またはを使用してサービスを追加または削除 `network interface service-policy remove-service`できます。これらはすべて、システムを停止することなく実行できます。

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。

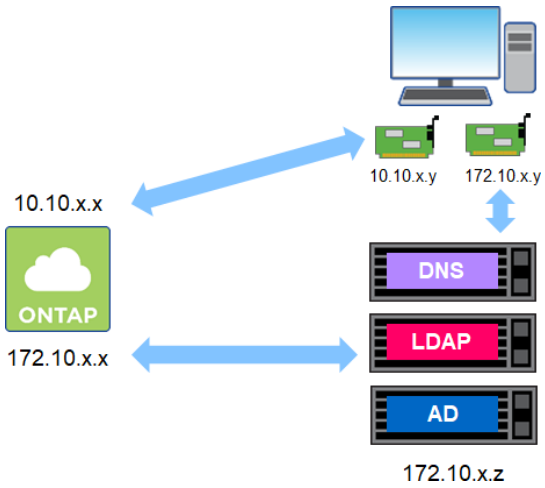
ネームサービスの接続

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役割を果たします。そのため、ONTAP SVMのネットワークインターフェイスには、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になります。NASクライアントが複数のインターフェイスで分割されたネットワークに配置され、ストレージやネームサービスへの接続が分離されている場合もあります。ネームサービス接続専用のデータLIFまたは管理LIFを使用できます。

たとえば、ONTAPストレージをクラウドでホストし、NASクライアントとドメインサービスはすべてオンプレミスで運用している場合などです。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接続が必要です。

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

注： NFS Kerberosでは、ネームサービスにアクセスする必要はありません。詳細については、TR-4616：『NFS Kerberos in ONTAP』を参照してください。

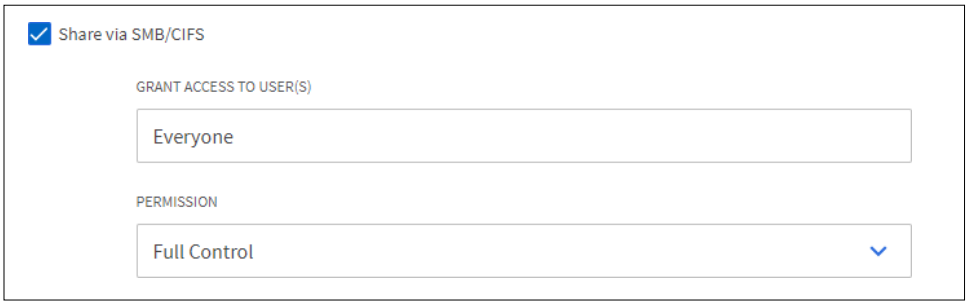
アクセスポイント：ボリューム、共有、エクスポート

ONTAPでボリュームをプロビジョニングする場合は、使用可能な容量の一部を作成するだけです。NASクライアントは、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るまで、NFSまたはCIFS / SMB経由でボリュームにアクセスできません。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の考慮事項について説明します。

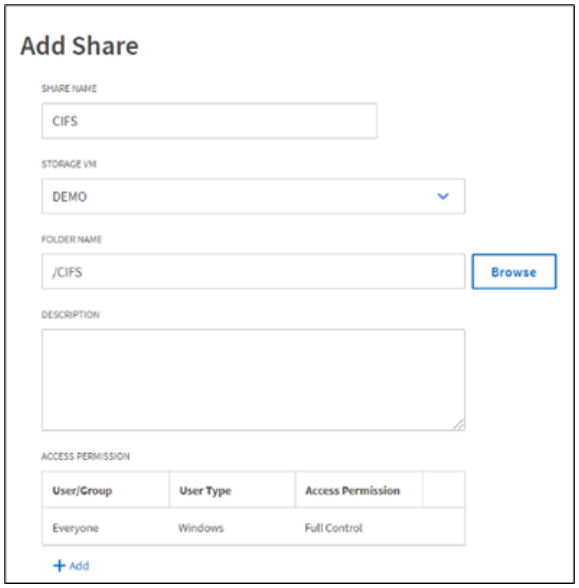
CIFS / SMB共有

ONTAPのボリュームにCIFSプロトコルを使用してアクセスするには、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。この処理は、ONTAP System Managerでのボリューム作成時、またはその後のCLIまたはSystem Managerで実行できます。

1. ボリューム作成時に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キョウユウフロハテイ

CIFS共有を作成するときは、アプリケーションの要件に応じて、共有にさまざまな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。

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

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

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

使用可能なその他の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のドキュメントを参照してください。

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付与できるアクセスレベルを制御しますが、ファイルおよびフォルダの権限で上書きされます。たとえば、user1にDocumentsという名前の共有に対するフルコントロールがあり、実際のフォルダ権限に読み取り専用アクセス権が割り当てられている場合、user1には共有に対する読み取りアクセスのみが許可されます。

ONTAPで共有レベルの権限を割り当てるには、ONTAPシステムマネージャ、コマンドライン（`cifs share access-control`）、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NAS環境では、CIFS / SMBクライアントだけがWindows共有権限を利用します。NFSクライアントは、共有への初期アクセスに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クライアントと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クライアントの両方で、ファイルレベルとフォルダレベルの権限が適用されます。

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、ユーザやグループではなくクライアントのホスト名/ IPアドレス/サブネットで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、「SMBアクセスでのエクスポートポリシーの使用方法」を参照してください。

NFS エクスポート

ONTAP内のボリュームは、あるクライアントまたは一連のクライアントからアクセス可能なパスをエクスポートすることで、NFSクライアントと共有されます。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、mount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。エクスポートに対する権限は、ストレージ管理者が設定できる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ます。これらの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、単一のノードに分離されるのではなく、クラスタ内のすべてのノードでエクスポートを使用できます。

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、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含めることができ、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

新しく作成したSVMには、defaultという名前のエクスポートポリシーが含まれています。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て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してボリュームにアクセスするには、ルールを追加する必要があります。エクスポートポリシーが定義されていない場合は、新しいボリュームの作成時に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はデフォルトで継承されるため、NetAppでは、ルールの割り当て時にSVMのルートボリューム（vsroot）への読み取りアクセスをNFSクライアントに許可することを推奨しています。デフォルトのエクスポートポリシーにvsrootへの読み取りアクセスを制限するルールを設定すると、そのSVMに作成されたボリュームへのトラバーサルが拒否され、原因のマウントは失敗します。これは、vsrootがへのパスに含ま `/junction` れており、マウントおよびトラバースの機能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に対して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内の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または許可し、ストレージ管理者が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るようになります。

デフォルトでは、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を作成する場合（図11）、または `- export-policy` CLIオプションを使用すると、エクスポートポリシーとルールを明示的に選択または作成できます。

図11）qtreeエクスポートの仕様-ONTAP System Manager

vsrootへノアクセスセイキヨ

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 `unix-permissions` やACL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）。

特に指定がないかぎり、ボリュームの作成時のデフォルト値は次のとおりです。

- 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、をマウントする可能性のあるNFSクライアントへの読み取り/リストアクセスも禁止するには、次の2つの方法があります。

オプション1：vsrootでUNIXモードビットをロックダウンする

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に固有のローカルUNIXユーザを作成します。たとえば、SVM自体と同じ名前のUNIXユーザを指定できます。
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、vsrootボリュームにrootユーザからのアクセスがデフォルトで多すぎる可能性があります。
3. グループやその他のユーザをトラバース権限のみに制限するUNIX権限を使用しますが、ボリュームの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をロックダウンする

vsrootをロックダウンするもう1つの方法は、ACLを活用して、一部のユーザまたはグループを除くすべてのユーザに対して権限のトラバースを制限することです。これは、NFSv4.x ACLを使用して（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のNTFS権限を使用して実行できます。NFSv3マウントでNFSv4.x ACLを使用する方法については 、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には、複数の設定オプションがあります。エクスポートポリシールールのほとんどのオプションは、`export-policy rule show` 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、製品の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。protocolオプションには、any、nfs、nfs3、nfs4、およびcifsを指定できます。

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処理する方法を制御します。オプションは、[失敗（Fail）]（権限の変更がエラーで失敗する）または[無視（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NASでは、NFSクライアントからのみデバイスファイルを作成/削除できます。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一部のクライアントに制限する制限的なエクスポートポリシールールがある場合、SVMルートボリューム（にマウント/）の下に存在するデータボリューム 適用されているエクスポートポリシーのみが適用されます。唯一の例外は、クライアントへの読み取りアクセスを拒否す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おり、クライアントがそのパス内のボリュームをトラバースする必要がある場合です。現在、ONTAPでは、NFSのトラバースチェックのバイパスという概念はありません。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を使用すると、ストレージ管理者はエクスポートポリシールールの優先順位を設定して、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999999999は絶対最大値ですが、NetAppで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は、`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]を使用して並べ替えることができます（図12）。

図12）ONTAPシステムマネージャでのルールインデックスの並べ替え

ONTAPでクライアントに許可されるアクセスと許可されない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考慮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へのアクセスを拒否または許可するルールが、それらの同じクライアントへのアクセスを拒否または許可するルールに従わ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ときの順序を決定します。番号が大きいルールは、インデックス内の番号が小さいルールよりも優先されます。

注： より詳細なルール（管理ホストなどの特定のクライアント用など）を使用する場合は、ルールインデックスの上位に配置する必要があります。より広範なアクセスルールを低く設定する必要があります。たとえば、管理ホストのルールはルールインデックス1にあり、0.0.0.0/0のポリシーはインデックス99にあります。

エクスポートポリシールール：clientmatch

ストレージ管理者は、エクスポートポリシールールのclientmatchオプションを使用して、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したり、クライアントがエクスポートをマウントしたあとにアクセス権限を大まかに制御したりできます。

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、複数のIPアドレスまたはホスト名をカンマで区切って1つのルールに定義できます。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は、ホスト名をIPアドレスに解決するために、稼働中のDNSサーバまたは手動ホストエントリが使用可能である必要があります。
- ネットグループを使用する場合は、ネットグループの先頭に@記号を付加して、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に通知する必要があります。
- 名前解決またはネットグループ検索にネームサービスを使用する場合は、必要なネームサービスにアクセスできるデータLIFがSVM内にあることを確認してください。

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

ネットグループを使用すると、多数のホストを一元管理できます。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ます。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、ネットグループを使用して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ネットグループを使用できます。

- ローカルファイル
- LDAP
- NIS

NFSでネットグループを使用する方法については、TR-4067：『Network File Systems（NFS）in NetApp ONTAP』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：『How to Configure LDAP in ONTAP』を参照してください。

注：マルチプロトコルNASでネットグループを使用できるのは、エクスポートポリシーとルールを使用する場合のみです。

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、プロトコルアクセスに必要な権限モデルが適用されるようにONTAPを設定する必要があります。NFSのみの環境では、UNIXセキュリティ形式を使用するかどうかを簡単に判断できます。

マルチプロトコルNASを使用する場合は、作成時にセキュリティ形式を指定しなかった場合、新しく作成したボリュームはSVMルートボリュームのセキュリティ形式を継承す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もいつでも変更できますが、デフォルトに基づいてセキュリティ形式を誤って作成した場合は、アクセス/権限に関する呼び出しを開始するまで問題が認識されないことがあります。

NFSとCIFS / SMBが必要な場合は、主に次の2つの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何ですか。
- 必要な権限管理エンドポイントは何ですか。つまり、ユーザにはNFSクライアントまたはWindowsクライアントの権限を管理する機能が必要なのでしょうか。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、実際には権限形式です。

ONTAPボリューム/ qtreeのセキュリティ形式

ONTAPには、ボリュームおよびqtreeに対して選択できる3つのボリュームセキュリティ形式が用意されています。

UNIX

UNIXセキュリティ形式では、基本モードビット（Owner / Group / Everyoneアクセスと標準の読み取り/書き込み/実行権限（0755など））やNFSv4.x ACLなどのUNIX形式の権限が提供されます。POSIX ACLはサポートされていません。

NTFS

NTFSセキュリティ形式では、Windows SMB権限と同じ機能が提供され、ACLでユーザとグループをきめ細かく設定し、セキュリティと監査の権限を詳細に設定できます。

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り入れ、ACLを最後に変更したプロトコルに基づいて有効な形式として適用されます。たとえば、Windows SMBクライアントがmixedセキュリティ形式のボリューム内のファイルまたはフォルダの権限を変更した場合、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に変更されます。これにより、複数のクライアントが権限を管理できるようになり、この機能を必要とするアプリケーションに最適です。

ベストプラクティスとして、NetAppでは、直接要件がないかぎり、mixedセキュリティ形式は推奨しません。

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属性にマッピングされたSMB経由でのみUNIX権限属性を設定できます（読み取り/書き込み/実行のみ。特別な権限はありません）。 • NFSv4.x ACLでは、GUIまたはONTAP CLIで管理することはできません。 • 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ではそれらのACLを表示できません。
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（デフォルトは無効）の場合にACLを表示すると、NFSクライアントにはおおよその権限のみが表示されます。
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での認証は、ONTAPがユーザが自分であると主張するユーザであることを判断する方法です。この認証により、アクセスが許可されているかアクセスが拒否されているかに関係なく、ファイルやフォルダへの想定されるアクセスが確実に提供されます。

ネーム マッピング

要求されているユーザが特定されると、ネームマッピングを使用してWindowsユーザIDがUNIXユーザIDに接続されます。これは、WindowsとUNIXの権限のセマンティクスが非常に異なるためです。ネームマッピングはユーザレベルでのみ実行され、グループ名はマッピングされません。代わりに、ネームマッピングの完了後にONTAPによってグループメンバーシップが収集されます。

詳細については、次のリソースも参照してください。

- 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実行されます。

1. ONTAPは1対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` はWindowsユーザにマッピングされ `DOMAIN\netapp`ます。
2. 1：1マッピングが存在しない場合は、ネーム `ns-switch database` マッピングでネームサービスソースが参照されます。デフォルトでは、ローカルファイルが（`vserver name-mapping rule` エントリ経由で）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. このユーザのネームマッピングルールが存在しない場合、ONTAPはCIFS / SMBサーバまたはNFSサーバで設定されているデフォルトのユーザ名を使用しようとします。デフォルトでは、CIFS / SMBは `pcuser` デフォルトのUNIXユーザとしてを使用します（`-default-unix-user`）。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、使用されているプロトコルだけでなく、ボリュームに適用されているセキュリティ形式によっても異なります。Windowsクライアントでは、常にWindowsからUNIXへのネームマッピングが必要です。ユーザが権限の確認に適用されているかどうかは、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セキュリティ形式を使用している場合だけです。

表2 に、ネームマッピングの方向とセキュリティ形式を示します。

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	適用される権限
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 （共有にアクセスするWindows SID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る
NFSv3	UNIX	なし	UNIX （モードビットまたはNFSv4.x ACL *）
NFSv4.x	UNIX	数値IDからUNIXユーザ名	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る	有効なセキュリティ形式によって異なる

* NFSv4.x ACLはNFSv4.x管理クライアントを使用して適用でき、NFSv3クライアントでも適用できます。

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ネームサービス設定を指定できます。ONTAPのローカルファイルはファイルではなく、レプリケートされたデータベース内のエントリであり、各ノードにコピーがあります。ノードに障害が発生した場合、クラスタ内の他のノードがその構成を認識するため、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で使用できます。

- 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 /ホストエントリ

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では、ローカルUNIXユーザおよびグループに対してデフォルトで最大64、000個のエントリがサポートされます。

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/ファイルのみ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/グループ	拡張モードのユーザ/グループ
ローカルユーザおよびローカルグループの最大エントリ数	65,536	ユーザ数：40万人 グループ：15k グループメンバーシップ：3000k SVM：6
拡張モードのユーザおよびグループの最大ファイルサイズ	N/A	passwdファイルサイズ（ユーザ）：10MB* グループファイルサイズ：25MB* * groupおよびpasswdファイルのサイズは上書き可能 `-skip-file- size-check` ですが、ファイルサイズが大きい場合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SVMが4つある場合は、各SVMの最大ユーザ数の合計が、クラスタの最大数に達している必要があります。

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.
```

拡張モード/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に対する拡張モード/ファイルのみ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、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容量を拡張することで、ローカルユーザとローカルグループの制限を拡張できます。ユーザとグループの数。拡張モード/ファイル専用モードでは、ネームサービスサーバやネットワークなどに外部の依存関係が不要になるため、ネームサービス検索のパフォーマンスが向上します。ただし、ファイル管理によってストレージ管理のオーバーヘッドが増大し、人為的ミスの可能性が高まるため、このパフォーマンスにはネームサービスの管理が容易になりません。また、ローカルファイル管理はクラスタごとに行う必要があるため、複雑さがさらに増します。

このオプションをユーザとグループに対して有効にするには、`vserver services name-service unix-user file-only` コマンドと `vserver services name-service unix-group file-only` 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
```

メモ： ユーザの場合は10MB、グループの場合は25MBを超えるファイルをロードするには、`-skip-file-size- check` オプションを使用します。

ファイルのみモードを使用している場合、ユーザおよびグループに対する個々の操作は許可されません。この構成は、現在、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いる場合でも、外部ネームサービスを使用できますか。

ファイルのみモードでは、LDAPやNISをネームサービスとして使用できないわけではありません。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）ファイルのみで行われます。ファイル専用モードを有効にしても、LDAPおよびNIS検索は引き続き正常に機能します。

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。

次の例は、これらのユーザとグループを示しています。

```
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するファイル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。ファイル専用モードを有効にすると、アップロードされたファイルにデフォルトユーザが含まれていない場合、デフォルトユーザは削除されます。

ローカルユーザへの影響

ファイル専用モードを有効にすると、ロードされているファイルにユーザがいない場合、root、pcuser、およびnobodyのデフォルトのローカルユーザが削除されます。ファイル専用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IDプロバイダ

NetAppでは、外部のネームサービスとIDプロバイダ（LDAP、NIS、DNSなど）を介してNASクライアントおよびONTAPにホスト名とユーザ/グループのIDを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で、ユーザ、ユーザの数値ID、メンバーであるグループ、ホスト名にマッピングされるIPアドレス、 これにより、複数のクライアントやストレージシステムにまたがる数百、数千のローカルファイルを維持する必要がなくなります。

ネームサービスを一元化することで、一元的な管理が可能になります。グループからのユーザの削除は、クライアント間で何度も実行するのではなく、一度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を引き起こす可能性のある人為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。

許可と権限

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、キャッシュにグループメンバーシップ情報を入力するために使用され、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内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、ユーザとグループがファイルまたはフォルダに対する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）が含まれています。各ファイルまたはフォルダには最大1、024個のACEを含めることができますが、パフォーマンスと管理性を確保するために、ファイルやフォルダで使用するACEの数を減らすことを推奨します。ファイルとフォルダのアクセス権にアプローチする最善の方法は、グループを使用することです。

ONTAPのファイルおよびフォルダ権限は、WindowsおよびUNIX権限モデルと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 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、これらの権限構造が適用されます。

使用する権限のタイプは 、使用しているセキュリティ形式によって異なります。

ACLトコトナルセキュリティケイシキノレンケイ

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、可能な限り最良の結果を得るために役立つ、マルチプロトコル環境における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負担が大幅に軽減されます。ストレージシステムは、すでにベストプラクティスに準拠している場合は、CIFSとNFSの両方を活用してNAS環境にシームレスに統合できるように設計されています。

最適なセキュリティ、パフォーマンス、および相互運用性を実現するには、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

ONTAPは、NASファイルシステムにさまざまなボリュームおよびqtreeのセキュリティ形式を提供します。一般的な概念として、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ります。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を使用することを推奨します。ただし、アプリケーションベンダーがそのセキュリティ形式を特に求めている場合や、ユーザが権限を変更した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モードを使用します。次の質問に基づいて、設計に関する考慮事項を検討する必要があります。

- 大半のクライアントが使用しているオペレーティングシステム/ NASプロトコルは何ですか。
- 権限はどの程度詳細に設定する必要がありますか。
- NASクライアントは、最新かつ優れたプロトコル機能およびバージョンをサポートしていますか。

表4 を使用して、適切なボリュームおよびqtreeのセキュリティ形式を選択してください。表のXは設計上の考慮事項を表し、最終的な結果は最後の2列になります。両方の列を選択した場合はどちらかを選択でき、それぞれのセキュリティ形式機能の重要性に基づいて選択する必要があります。

表4）NASボリュームおよび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	ほとんどNFS	CIFS / SMBが中心	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権限を変更できる機能
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

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が推奨されます。

- **LDAPは将来のニーズに対応しています。**NFSv4.xをサポートするNFSクライアントが増えるにつれ、最適なセキュリティを確保し、アクセスを定義する際のアクセスを保証するために、クライアントやストレージからアクセスできる最新のユーザとグループのリストを含むNFSv4 IDドメインが必要になります。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アイデンティティ管理サーバを使用すると、ストレージ管理者の作業が大幅に簡易化され、現在だけでなく今後何年も作業が簡易化されます。また、マルチプロトコル環境が必然的に拡大しても、ストレージ管理者は次のような問題を解決できます。
- **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は、クラスタあたりのデフォルトのソフトリミットである32、768に制限され、ハードリミットである65、536まで拡張できます。ただし、SVMが複数あるマルチテナント環境やそのユーザ数を超える環境では、クラスタの制限に達し、ユーザを追加できなくなります。NISサーバには上限の下限はありませんが、次のような独自の問題があります。
- **LDAPの方が安全です。**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という形でセキュリティを提供します。LDAPサーバをONTAPで使用すると、次のバインドレベルを許可できます。
  - 匿名
  - 単純なパスワード
  - 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。NISには標準ポートがないため、ファイアウォールを使用するのは困難です。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が使用されますが'設定は困難であり'NISを置き換える場合'管理者はNIS+よりもLDAPを選択することがよくあります
- **LDAPはより堅牢です。**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、これらの属性などが用意されています。LDAPで使用される追加の属性により、マルチプロトコル管理はNISよりもLDAPとはるかに統合されます。実際には…
- **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、ユーザおよび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LDAPツールを使用して拡張された場合に追加されます。MicrosoftではバックエンドとしてLDAPを使用しているため'LDAPはドメインでCIFSを活用することを選択する環境に最適な解決策です

LDAPとActive DirectoryおよびONTAPの連携の詳細については、TR-4073：『Secure Unified Authentication』を参照してください。

個々の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。

フェイルセーフとしてローカルファイルを使用する

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接続が復元されるまで、管理者がデータにアクセスできるように、フェイルセーフが用意されていることを確認することが重要です。そのため、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でのマルチプロトコルNASの基本事項をさらに詳しく説明します。マルチプロトコルに固有のNFSサーバやCIFSサーバオプションなど、より高度なトピック、一般的な問題、トラブルシューティングの手順、対処方法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およびNFSのサーバ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**NAS**ファイルロック

ファイルロックは、ファイルを開いて使用しているときに、そのファイルが現在ロックされていることを他のクライアントに通知することで、ファイルの整合性を維持する方法です。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では、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放に役立ち、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、クライアントのリブート時にサーバでロックを解除する必要があります。サーバがリブートすると、クライアントはサーバに保持されているロックを通知します。場合によっては、ロックメカニズムが適切に通信できず、古いロックがサーバに残っているため、手動でクリア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ます。つまり、維持したり心配したりする補助サービスはなく、すべてのロックはNFSv4.x通信でカプセル化されます。

サーバまたはクライアントをリブートしたときに、指定した猶予期間中にロックを再確立できなかった場合、ロックは期限切れになります。ONTAP NFSサーバは `-v4-grace- seconds` 、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`。

- `-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を示します。デフォルトは30秒です。最小値は10秒で、最大値は次の値の-1秒です。「`-v4-grace-seconds`」
- `-v4-grace-seconds` ノードのリブート時（フェイルオーバーやギブバック時など）にクライアントがONTAPからロックの再要求を試みる時間。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、secondsという値に指定された速度でロックが解放されず、2つのリース期間にわたって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、ロックが解放されるまでに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 便宜的ロックが使用されます 。便宜的ロックは、ローカルクライアントに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削減されます。クライアントがファイルの処理を完了すると、変更がサーバー上のファイルに適用され、他のユーザーが編集できるようにファイルがチェックインされます。ファイルが編集されている間、他のユーザーは変更を行うことができません。これにより、ファイルのデータの一貫性が確保されます。

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、頻繁に開いたり閉じたりするファイルに対して使用されます。バッチoplockが使用されている場合、クライアントはクローズ要求の送信を遅延します。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のoplock /排他ロック** レベル1のoplockは、クライアントがファイルをローカルにキャッシュし、サーバにコミットする前にローカルコピー内の変更を追跡するときに、他のクライアントが変更を加えないことを前提としています。これは、Microsoft Officeが~ファイル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間のラウンドトリップの回数が減り、パフォーマンスが向上します。
- **レベル2のoplock**レベル2のoplockは、クライアントがファイルをロックし、そのロックを解除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します。レベル2のoplockキャッシュは読み取り専用です。これは通常、OneDriveとSharePoint問題のロック方法です。
- **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、書き込みアクセスまたは削除アクセスのために開くことができないようにします。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。oplockのフィルタは、レベル2のoplockとは異なり、読み取りのオープン処理を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を無効にすることが有効なユースケースの1つとして、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（WAN経由のSMBやNAT経由のSMBなど）が確立されていて、古いバージョンのSMB（SMB 1.0など）が使用されている場合があります。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およびoplockの管理方法の詳細については、ONTAP 9ドキュメントセンターのoplockに関するセクションを参照してください。

注： SMBプロトコルの最新バージョンには、永続的ファイルハンドルなど、SMB共有やSMBロックに対するネットワークの不安定さの影響を軽減する機能があります。

マルチプロトコルNASのロックの動作

マルチプロトコルNAS環境でファイルロックを使用する場合は、使用する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。

これが意味すること

NFSファイルとSMBファイルのロックの違いにより、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失敗することがあります。

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ているファイルにアクセスしようとすると、次の処理が実行されます。

- mixed形式またはNTFS形式のボリュームでは `rm`、、などのファイル操作で `rmdirmv` NFSアプリケーションを原因できない場合があります。

- 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上の他のすべてのNFS処理では、SMBロック状態が維持されます。

ロックの種類

NASロックには、次のような種類があります。

- **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の処理を目的としていますが、書き込み（データベースなど）に使用できます。
- **排他ロック。**これらのロックは、CIFS / SMBの排他ロックと同じように動作します。ただし、排他ロックがある場合は、ファイルを使用できるプロセスは1つだけです。他のプロセスがファイルをロックした場合、そのプロセスがフォークされていない限り、排他ロックは発行できません。
- **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で、クライアントがNFSv4.xの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、クライアントが使用す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実行される呼び出しの数を減らすことで、処理のパフォーマンスの一部の側面を向上させるのに役立ちます。SMBの便宜的ロックに似ています。NFS委譲の詳細については、TR-4067：『Network File Systems（NFS）in NetApp ONTAP』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、ファイルの一部だけをロックします。
- **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。詳細については、「SMB ロック」を参照してください。

  注： NFSロックの動作は、ロックの種類、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」を参照してください。

NFSクライアントでのロックの手動確立

NFSロックをテストするには、クライアントがNFSサーバにロックを確立するように指示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。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、アプリケーションを閉じるとそのファイルへの書き込みをコミットします。その後、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、手動でロックを確立するためのユーティリティがあります。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. を実行し `exec` て数値IDを割り当てます。

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

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

```
# 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でロックされていることを確認します。

```
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、ファイルを開いて編集する操作をテストしたり、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で最も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。この一般的なテキストには、中国語、日本語、ドイツ語など、現代のすべての文字言語が含まれています。しかし、絵文字などの特殊文字の普及に伴い、 UTF-8文字の一部のサイズが3バイトを超えています。たとえば、トロフィーシンボルはUTF-8エンコーディングで4バイトを必要とする文字です。

特殊文字には、次のものがあります。

- 絵文字
- 音楽記号
- 数学記号

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

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

上記の例では、 `\360\237\217\206` は `0xF0 0x9F 0x8F 0x86` トロフィーシンボルであるUTF-8の16進数です。

ONTAPソフトウェアでは、バグ229629に示すように、NFSで3バイトを超えるサイズのUTF-8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するために、ONTAPは余分なバイトをオペレーティングシステムのと呼ばれる領域に配置しまし `bagofbits`た。これらのビットは、クライアントが要求するまで保存されていました。次に、クライアントはrawビットから文字を解釈します。FlexVolテクノロジでがサポートされ `bagofbits`、`bagofbits` ONTAP 9.2ではFlexGroupボリュームのサポートが追加されました。

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

特殊文字の処理を最適化するには、ONTAP 9.5以降とutf8mb4ボリューム言語を使用してください。

また、ONTAPには bagofbits、問題のあるファイルIDの特定方法など、処理の問題に関するイベント管理システムメッセージがあります。

```
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.
```

ボリューム言語utf8mb4のサポート

前述したように、特殊文字は、ネイティブ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場合があります。その後、ONTAPはこの bagofbits 機能を使用して、これらの文字を使用できるようにします。

このinode情報の格納方法は理想的ではないため、ONTAP 9.5以降ではボリューム言語utf8mb4がサポートされるようになりました。ボリュームでこの言語を使用すると、サイズが4バイトの特殊文字がにではなく適切に格納され bagofbitsます。

ボリューム言語は、NFSv3クライアントから送信された名前をUnicodeに変換したり、ディスク上のUnicode名をNFSv3クライアントで想定されるエンコーディングに変換したりするために使用されます。UTF-8以外のエンコーディングを使用するようにNFSホストが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の使用は最近ほぼ一般的になっているため、ボリューム言語はUTF-8である可能性が最も高くなります。

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はUnicodeをネイティブに使用するため、任意のボリューム言語で動作します。ただし、Unicode名が基本平面より上にあるファイルはutf8mb4以外のボリュームでは正しく変換されないため、utf8mb4を使用することをお勧めします。

ボリュームの言語は、-language オプションを使用したボリューム作成時にのみ設定できます。ボリュームの言語を隠すことはできません。新しいボリューム言語でファイルを使用するには、XCP Migration Toolなどのユーティリティを使用してボリュームを作成し、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場合を除き、ボリューム言語utf8mb4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推奨します。

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手段で、次の機能を提供します。

- クォータの監視と適用
- 固有のエクスポートポリシーおよびルール
- 固有のセキュリティ形式
- qtreeのサービス品質（QoS）
- qtreeの統計

今後、qtreeはONTAPで選択されるデータ管理ポイントとみなされ、さらに強化された機能が今後も追加される予定です。

ここでは、qtreeを使用する際の考慮事項について説明します。

qtreeとファイル移動

qtreeは、ONTAPでは一意のファイルシステムとみなされます。NASクライアントからはディレクトリのように見えますが、一部の処理は実際のディレクトリとは動作が異なることがあります。このシナリオの例の1つは、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。

- 複数のディレクトリにまたがるボリューム内でファイル移動を実行すると、ファイル名が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間でファイルの移動が発生すると、名前が変更されるのではなく、新しい場所にファイルがコピーされます。このプロセスにより、処理にはるかに時間がかかります。このファイル移動の動作は、qtreeがFlexVolボリュームに配置されているかFlexGroupボリュームに配置されているかに関係なく発生します。

qtreeのIDと名前変更の動作

継承されていないエクスポートポリシーをqtreeに適用すると、qtree間の操作を処理する際にNFSファイルハンドルがわずかに変更されます。ONTAPはNFS処理で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との間で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、ホームディレクトリのシナリオなど、qtree間の不要なアクセスを防止できます。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も同様の目的を達成できます。

たとえば、同じボリューム内のqtreeを移動したりqtree名を変更したりすると、アクセスが拒否されます。別のボリューム内のqtreeとの間で同じ移動または名前変更を行った場合、ファイルがコピーされます。ファイルのサイズが大きい場合、コピー動作により、移動操作に異常に長い時間がかかっているように見えることがあります。ほとんどの移動操作は、同じファイルシステム/ボリューム内での単純なファイル名変更であるため、ほとんどの移動操作がほぼ瞬時に行われます。

qtree内の名前変更の動作は、NetAppナレッジベースの記事「Permission denied while moving files between trees when nfsoption '-validate-qtree-export'」で説明されているアドバンスト権限オプションで制御されます。

この資料では、次の動作がさまざまな操作でどのように行われるか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`：および `NFS3ERR_ACCESS` は RFC-1813で定義されています。

qtree間での名前変更/移動の動作を変更するには `-validate-qtree-export`、次のように変更します。「`disabled`」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： qtree間での名前変更を許可する以外に、 `- validate-qtree-export` オプションを無効にしても悪影響はありません。

qtreeエクスポートに対するファイルハンドルの影響

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、古いクライアント（1996年に導入されたHPUX 10.20など）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

ポートを有効にする前に、古いクライアント接続を別のテストSVMでテストするようにしてください。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は現時点ではないためです。

同じNFSクライアント上の同じボリューム内の複数のqtreeのマウント

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が同じボリュームに配置されている場合、クライアントとサーバ間のNFSのやり取りでは親ボリュームと同じ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、各qtreeで実際に使用されているスペースに関係なく、使用済みスペースは同じになります。

たとえば、これら2つのqtreeは、異なるマウントポイントで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
```

どちらの場合も、ファイルをコピーする前に同じスペース使用量が表示されます。

```
# 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で同じスペースが使用されています。

```
# 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
```

この問題を回避するには、いずれかのqtreeにクォータを監視します。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
```

サブディレクトリのエクスポート

qtreeはNFS経由でエクスポートできます。NFSは、単一レベルのサブディレクトリパスを提供し、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します。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ず、現在ONTAPではqtreeをボリュームレベルでしか作成できません。ディレクトリツリーの下位レベルのエクスポートが必要な環境では、ボリューム、qtree、およびジャンクションパスを組み合わせ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、クライアントが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、パス全体が保護されるわけではありません。

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
```

上記のパス内の各オブジェクトは、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に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以降では `qtree create`、ONTAP CLIでまたはを使用してqtreeのユーザおよびグループの所有者を設定できます `qtree modify`。以前のリリースでは、クライアントから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、現在のところ、CLIまたはREST APIからのみ使用できます。ZAPIまたはONTAP System Managerは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は 、NAS操作で使用するユーザー/グループ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とファイル数の使用量を監視および制御できます。

FlexGroupボリュームではクォータもサポートされます。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できます。

- 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のDefendX（旧NTP）など、サードパーティベンダーからクォータを適用できます。
- 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）は、ONTAP 9.5以降でサポートされています。

ユーザクォータおよび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、クラスタが指定され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。つまり、ユーザまたはグループがSVM上にローカルに存在しているか、解決可能なネームサービスサーバ（Active Directory、LDAP、NISなど）内に存在している必要があります。ユーザまたはグループがSVMで見つからない場合、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の作成に失敗すると、コマンドラインで次のエラーが表示されます。

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

ONTAP System Managerからも同様のメッセージが表示されます。`event log show` コマンドを使用して、問題をさらに調査します。ONTAPでのアイデンティティ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の作成

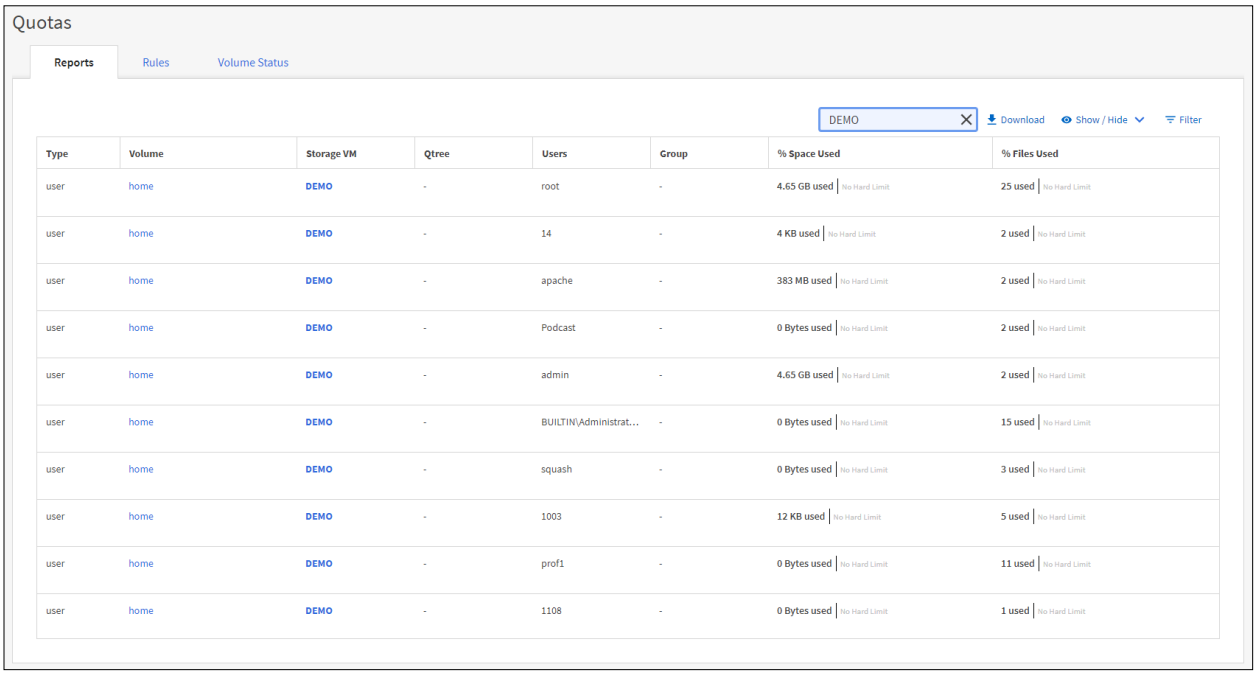
ユーザクォータとグループクォータを作成して、ユーザ単位で容量やファイル数の制限をレポートしたり適用したりできます。これらのクォータは、複数のユーザまたはグループが同じネームスペースまたはqtreeを共有するシナリオで使用されます。これらの手順は、FlexVolボリュームとFlexGroupボリュームで同じです。

クォータの作成-ONTAP System Manager

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]に移動します。ページには[Reports]、[Rules]、[Volume Status]の3つのタブが表示されます。

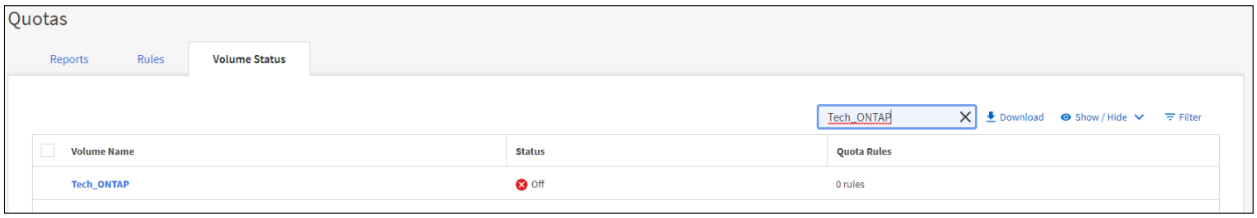
レポートには、ユーザ、グループ、およびqtreeの現在のクォータ追跡情報が表示されます。

図13）クォータレポート-ONTAPシステムマネージャ



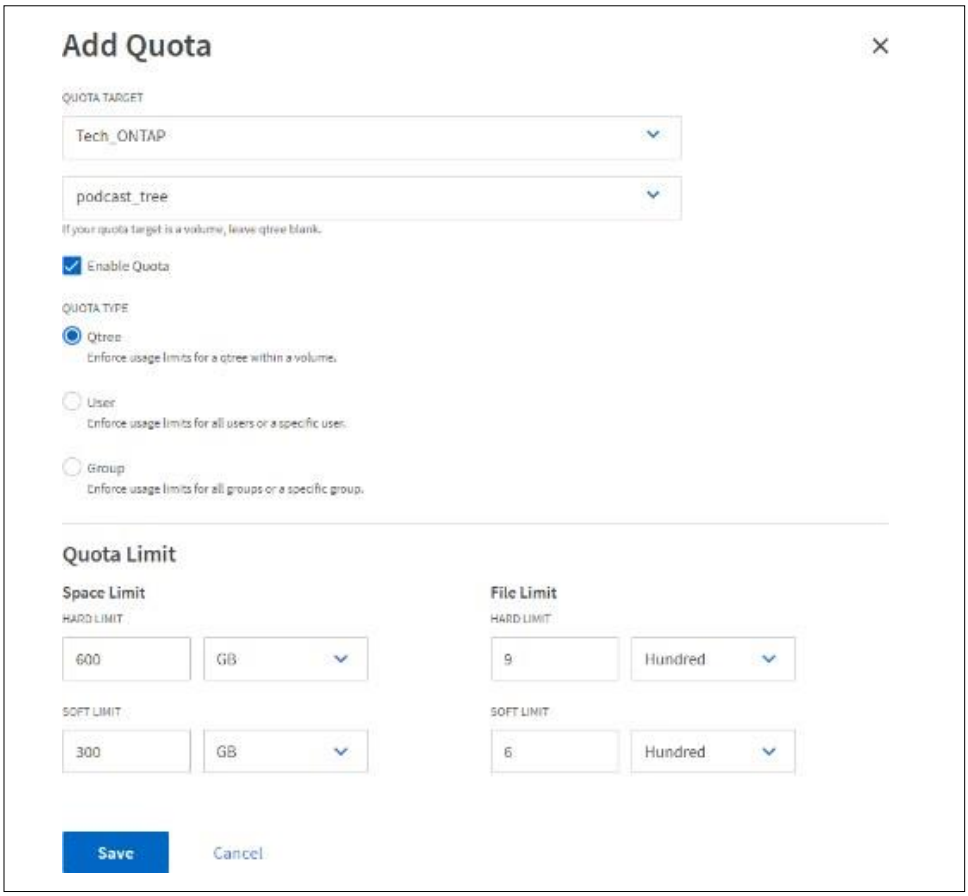
ボリュームステータスには、ボリュームのクォータがオンになっているかオフになっているかが表示されます。

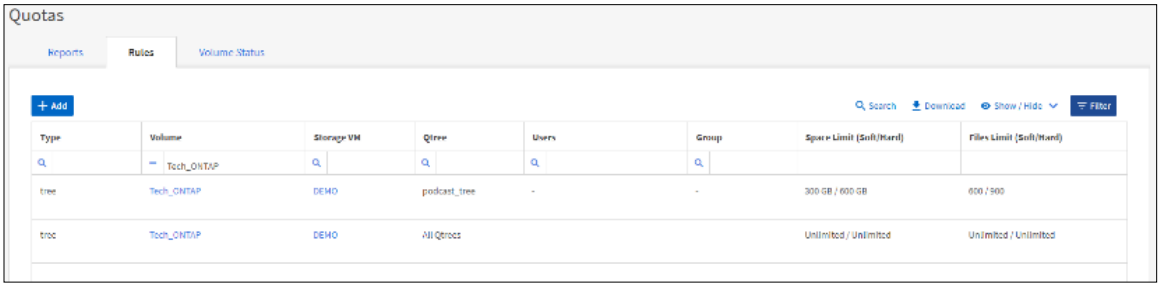
図14）クォータボリュームステータス-ONTAPシステムマネージャ

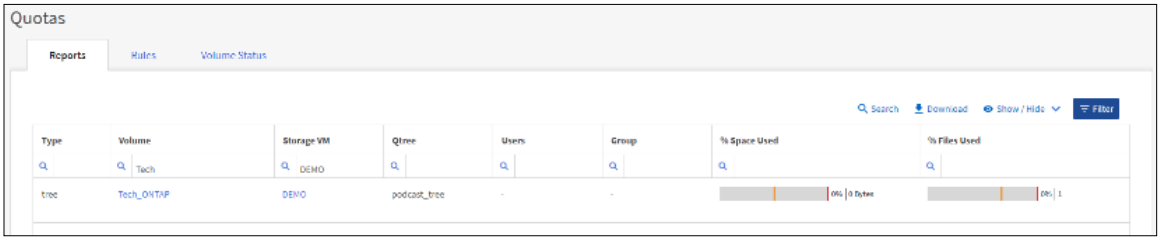


ルールとは、ユーザ、グループ、またはqtreeの新しいクォータを作成することです。[追加]をクリックし、ユーザ、グループ、またはqtreeクォータの情報をダイアログボックスに入力します。ルールが作成されると、ONTAP System Managerがクォータを有効化してアクティブ化するために必要なすべての手順を実行します。

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に対して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 `all`、次のことを示すアスタリスクで示されます。

```
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`、またはを使用し `quota resize`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
```

次の例は `quota report` 、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容量は監視され、新しいファイルが作成されると増加します。

```
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
```

クォータの適用の例

qtreeまたはユーザ/グループに対してクォータの適用が有効になっている場合、ONTAPはクォータ超過後の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DEBUG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されます。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、クォータに1GBのハードリミットと10ファイルのハードリミットが設定されています。

```
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         -          -
```

ユーザが1.2GBのファイルをqtreeにコピーしようとすると、ONTAPから `out of space` 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
```

次に、ONTAPはクォータを超過したと報告します。

```
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
```

ファイル数の制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、このqtreeにはすでに5つのファイルが含まれています。余分な5つのファイルが私たちの制限を満たしています。

```
[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=""
```

クォータスキャン完了時間

クォータの初期化またはサイズ変更が行われると、ONTAPはいくつかのバックグラウンドタスクを実行して、クォータ使用量が正確に反映されるよう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、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 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。**多数のファイルを含むシステムの負荷が高いと、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、クォータポリシーが変更されたときに使用されます。サイズ変更により、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。

- サイズ変更は、新しく追加されたルールを使用してのみスキャンされるため、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/オフよりも少ないため、通常は数秒で完了します。
- サイズ変更の完了までの時間が短縮されるため、クォータのオンとオフを切り替える代わりにresizeを使用します。
- クォータのサイズ変更では、最大100個のジョブを同時に実行できます。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。
- 同時スキャン数が増えると、サイズ変更のパフォーマンスが低下し、ジョブの完了に時間がかかる可能性があります。

クォータでのユーザマッピングに関する考慮事項

マルチプロトコル環境（SMBとNFSの両方からのデータアクセス）でのクォータのユーザマッピングは、メンバーボリュームレベルで実行されます。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で一致

します。ただし、ユーザマッピングに失敗した場合や、別のメンバーで成功したネームマッピングの実行時にタイムアウトになった場合など、不一致が生じることがあります。つまり、少なくとも1人のメンバーがそのユーザーをユーザーマップペアの一部と見なし、もう1人のメンバーがそれを離散レコードと見なします。

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に一貫性がなくなる可能性があります。たとえば、ユーザがクォータ制限を短時間超過できる場合があります。

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内のSVMには最大5つのクォータポリシーを設定できますが、一度にアクティブにできるポリシーは1つだけです。SVM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システムマネージャで表示することはできません。

ほとんどの場合、デフォルトのポリシーで十分であり、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、アクティブポリシーが使用されます。そのため、クォータとルールをボリュームに適用したが `quota on` 失敗したと考えられます。

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に `default` 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、クォータを有効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.
```

にルールを追加する default と quota on コマンドは機能しますが、SVMでは新しいツリーポリシーが使用されません。

```
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、クォータのオンとオフを切り替える必要があります。

```
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
```

クォータが有効になっている場合のクライアントによるスペースの表示方法

ONTAPの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、そのクォータによって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
```

ボリュームの実際のスペース量を示します。

```
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については、次の情報が報告されます。

```
# 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ユーザに同じユーザ名を設定するだけで簡単に実行でき、明示的に1：1のネームマッピングが実行されます。追加の設定は必要ありません。ONTAPがネームサービスでWindowsユーザとUNIXユーザのユーザ名を検出でき、それらが一致していれば、すべて正常に動作します。

ただし、ネームマッピングは複雑で、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には複雑になります。

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、非対称ユーザ名に対する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、複数のユーザ名がUNIX名とWindows名で一般的に異なる場合に役立ちます。たとえば、すべてのWindowsユーザ名の姓名の間にピリオドが含まれていて（alice.smithなど）、UNIXユーザ名にアンダースコアが含まれている場合（alice_smithなど）、regexを使用してそれらのユーザが常に相互にマッピングされるようにすることができます。

次の例では、ピリオドをアンダースコアに置き換えるWindowsからUNIXへの正規表現のネームマッピングを示します。

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

次の例では、UNIXからWindowsへの正規表現のネームマッピングで、アンダースコアをピリオドに置き換えています。

```
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へノWindowsカンリユウサノマツヒンク

マルチプロトコルNAS解決策では、Windows管理者ユーザには、NFS/UNIX環境のrootと同じ方法で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。そのようなユースケースの1つがデータ移行の場合です。管理者ユーザは、ACLに追加することなく、ファイルのコピーやACLの変更をグローバルに行う必要があります。

これを実現するには、主に次の2つの方法があります。

- ユーザをrootにすることを細かく制御するには、必要なユーザ名をroot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。このメソッドを使用すると、SVMのローカルの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しないようにできます。
- SVMのローカルのBUILTIN\Administratorsグループ内のすべてのユーザにSVM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 `-is-admin-users-mapped-to-root-enabled`。

  注: 単にデータ移行のユースケースである場合は、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の権限については、「サポートされる権限の一覧」を参照してください。

Windowsクライアントとユーザ名のマッピング

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、クライアントレベルまたはサブネットレベルでアクセス権を制限する場合に便利です。

たとえば、（実行中のアプリケーションで特定のWindows NTFS権限を必要とする）10.10.x/24サブネット内のすべてのクライアントをWindowsユーザにマッピングする場合 `DOMAIN\application`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
```

LDAPを使用したネームマッピング

ONTAPでは、明示的なネームマッピングルールをローカルでSVM上に作成できますが、許容されるルールの数は1、024個に制限されています。場合によっては、より多くの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、マッピングするUNIXまたはWindowsユーザ名をLDAP属性に入力し、次のLDAPクライアントスキーマフィールドでその属性を指定することで、ネームマッピングサーバとして機能します。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のオプション-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は、複数のLDAPオブジェクトをグループ化して検索を高速化するために使用されます。AD-IDMUのデフォルト値はです `User`。RFC 2037スキーマの場合、値はに設定されます `posixAccount`。
`-windows-to-unix-attribute`	WindowsユーザをUNIXユーザにマッピングするために使用する値のLDAP属性を指定します。ONTAPのAD-IDMUスキーマのデフォルト値はです `sAMAccountName`。 RFC 2307スキーマの場合、この値のデフォルトはです `windowsAccount`。
`-windows-to-unix-no-domain-prefix`	このオプションは、の属性値に - `windows-to-unix-attribute` ドメインプレフィックスを追加するかどうかを制御します。 （デフォルトはです `false`）。 `sAMAccountName` は（ではなく `DOMAIN\username`）単一のユーザ名で表され、 `msDS- PrincipalName` は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、機能的な非対称ネームマッピングを有効にするために必要になる場合があります。 この値の必要性は、使用されている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名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。これは、新しいユーザーが作成されるときにWindowsアカウントで使用される標準フィールドです。

LDAPクライアントでネームマッピング検索を設定したら、`namemap` を使用するようにns-switchデータベースを変更します `ldap,files`。WindowsとUNIXのユーザ名が一致している場合、または対称である場合（たとえば、WindowsのJohnsはUNIXのJohns）、操作は必要ありません。非対称ネームマッピングにLDAPを使用する方法の詳細については、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、ネームマッピング検索によって要求のレイテンシが増大し、認証や失敗に時間がかかることがあります。

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には競合するほどの複雑さはありません。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にまたがって共有したりする場合は、処理が複雑になる可能性があります。ここでは、分散ファイルシステム（DFS）ボリュームやFlexCacheボリュームを使用するシンボリックリンク（シンボリックリンク）/ワイドリンクなど、該当する

いくつかのシナリオについて説明します。

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共有内のフォルダまたはファイルから他の場所（リモートのNetApp以外のストレージも含む）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、データの保存場所に関係なく、クライアントに対して透過的に単一のネームスペースを作成して表示できます。

シンボリックリンクとは

シンボリックリンクは、別のファイルまたはディレクトリへの参照が絶対パスまたは相対パスの形式で含まれているファイルです。

- 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、絶対パスはファイルシステム内の同じ場所を指します。このパスの先頭は必ずに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開始します。これはリンクを定義するためのより短く簡単な方法ですが、間違ったパスが定義されている場合にPath Not Foundエラーが発生することもあります。

ONTAPでは、UNIXクライアントからNFS経由またはPowerShellを使用してシンボリックリンクを作成できます。そのためには、ナレッジベースの記事「How to create a symbolic link in ONTAP without the need for NFS」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

ワイドリンクは、ストレージシステムの外部にあるNASネームスペースを他のNASデバイスに拡張できる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NetApp以外のストレージも含まれます。ONTAPでは、適切なCIFS共有 `-symlink-properties` 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へのリンクに使用できるリンクです。シンボリックリンクやワイドリンクとは異なり、ハードリンクは複数のファイルシステムにまたがることはできず、ディレクトリをリンクすることもできません。ONTAPでは、ハードリンクは次の範囲にまたがることができません。

- 異なるボリューム
- コトナルqtree
- Snapshotコピートアクティブファイルシステムノカン
- コトナルSVM
- コトナルストレージシステム

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見なされません。ただし、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、ファイルには複数のinodeアクセスポイントが含まれます。たとえば、ファイルとハードリンクの両方で同じファイルコンテンツが表示されます。

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

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

ハードリンクがあるファイルを検索するには、まずを使用し `ls -i` てinode番号を検索し、次に同じ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動作します。

CIFSシンボリックリンクパス

CIFS / SMB共有を使用するUNIX作成のシンボリックリンクの場合、リンクが正常に機能するために、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ます。CIFSシンボリックリンクを作成する際には、主に次の2つの点を考慮する必要があります。

- ストレージシステムでは、UNIX形式のシンボリックリンクをDFSリファーラルにオーバーレイできます。そのため、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認識します。
- シンボリックリンクが絶対リンクである場合、または別のエクスポートを参照している場合は、リンクがCIFSクライアントを適切なデスティネーション（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関係なく）に解決するようにマッピングルールを作成できます。

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

注： この `cifs symlink create` コマンドではシンボリックリンクは作成されず、パスマッピングが作成されます。シンボリックリンクは、NFSクライアントまたは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の作成

clusteredの技術情報アーティクル「How to make symbolic links（widelink）work for CIFS clients on clustered Data ONTAP」（「Seven important things to consider」のセクション）で、CIFSシンボリックリンクを正常に動作させるために必要な作業について簡単に説明しています。

- コマンド `cifs symlink create` ではシンボリックリンクは作成されません。
- シンボリックリンクは必須であり、NFSクライアントから、またはPowerShellツールキットを使用してのみ作成できます。
- CIFSシンボリックリンクマップエントリは、シンボリックリンクが含まれている共有を含むSVM上に存在し、デスティネーションではない必要があります。
- マッピングするシンボリックリンクを含むSVM上の共有で、シンボリックリンクを有効にするか、読み取り専用に設定する必要があります。この設定を確認するには、 `cifs share show` コマンドを実行します。
- SVMは、リンク名やリンク自体のパスではなく、シンボリックリンクの内容（デスティネーションパス）を解析してマッピングに使用します。リンクが何を指しているか、つまり何をマッピングする必要があるかを確認するには、 `ls -l` リンクのあるディレクトリでを実行し、宛先パスを確認します。

- シンボリックリンクからCIFSリファーラルへ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目的がCIFSクライアントのリダイレクトのみである場合。シンボリックリンクのリンク先のUNIXパスが、ONTAP内またはNFSクライアント上に実際に存在していない場合は許容されます。シンボリックリンクは、CIFSマップの目的のためだけに存在することができます。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、UNIXクライアントまたはLinuxクライアントでリンク自体が機能していなくても、CIFSに対してリダイレクトは機能します。

CIFSシンボリックリンクの例

ここでは、CIFSシンボリックリンクの例を示します。

- 相対パスを使用して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 /別のボリュームにCIFSワイドリンクがあります。
- NetApp以外のCIFS共有への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の作成時に、CIFS / SMBクライアントとONTAPでシンボリックリンクのパス解決の状態が一致しないことがあります。予期しない動作が発生したり、正常に動作しないように見える場合の対処方法については、「キャッシュとシンボリックリンクのエラー」を参照してください。

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

その他の例については、「clustered Data ONTAPでシンボリックリンクとワイドリンクを作成する方法」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、ボリュームのルートに、ボリュームの相対パスを使用して、同じボリューム内の3階層のフォルダにリダイレクトするリンクを作成する方法を示しています。

- 相対フォルダパスはです `dir1/dir2/linked-dir`。
- リンクを作成するには、NFSマウントで次のコマンドを実行します。

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

このリンクが作成されると、NFSで想定される結果が表示されます。symlink(`rel-link`)とフォルダパス（`dir1/dir2/linked-dir/`）は同じファイルを示しています）の両方が表示されます。

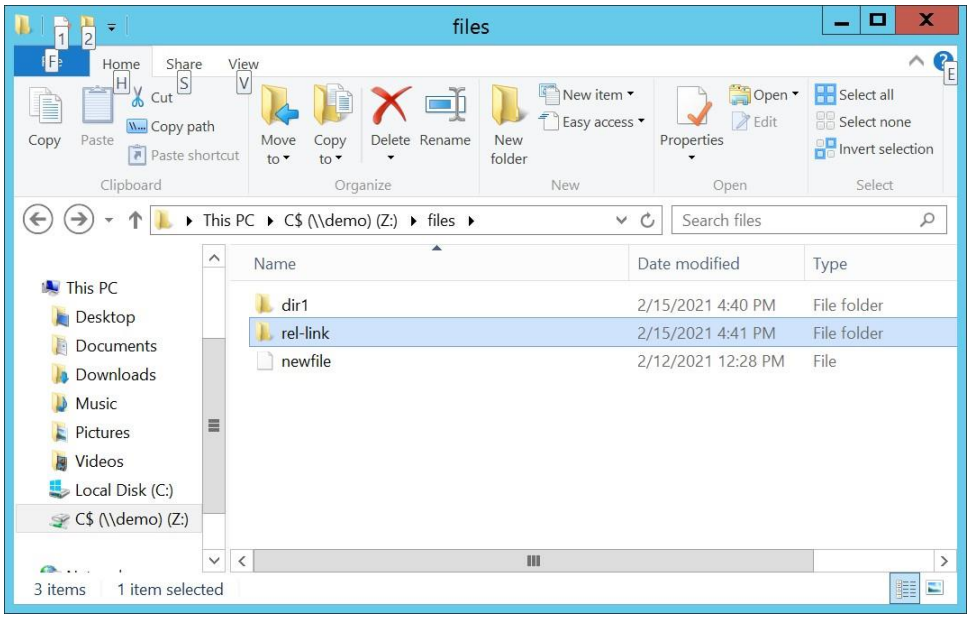
```
# ls -la rel-link/
total 8
drwxr-xr-x 2 root root 4096 Feb 15 16:41 .
drwxr-xr-x 3 root root 4096 Feb 15 16:40 ..
-rw-r--r-- 1 root root    0 Feb 15 16:41 rel-link-file

# 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、シンボリックリンクプロパティがCIFS共有で設定されていれば、同じボリューム内に相対パスを持つシンボリックリンクが、特別なCIFSシンボリックリンクマッピングを作成しなくても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、特別な設定を必要とせずに、相対CIFSシンボリックリンクをすぐに使用できます。

CIFS / SMB共有では、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が（ショートカットまたはファイル/ディレクトリとして）どのように表示されるかは、使用している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」で説明するオプションで制御されます。

図16）CIFSシンボリックリンク、相対パス-同じボリューム



CIFSシンボリックリンク：同じボリューム、絶対パス

絶対パスを指定してシンボリックリンクを作成すると、ネームスペース内のどこにリンクが存在するかに関係なく、使用されるパスが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、ボリュームのルートに、NFSマウントの絶対パスを使用して、同じボリューム内の3階層のフォルダにリダイレクトするリンクを作成します。

- フォルダの絶対パスはです `/mnt/client1/dir1/dir2/linked-dir`。
- リンクを作成するには、NFSマウントで次のコマンドを実行します。

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

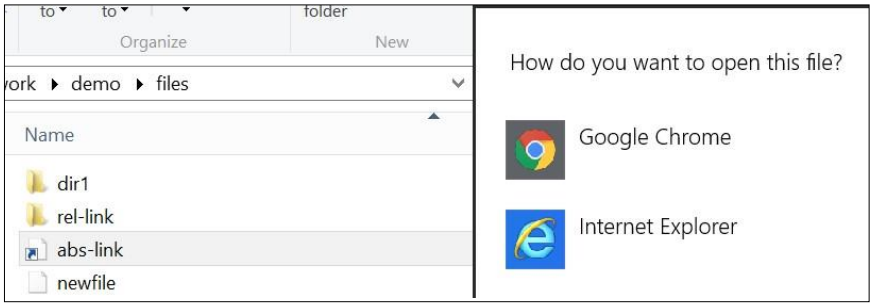
このリンクが作成されると、NFSで想定される結果が表示されます。絶対パスsymlink(`abs-link`)とフォルダパス（`dir1/dir2/linked-dir/`） は同じファイルを示しています）の両方が表示されます。

```
# 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。代わりに、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が（ショートカットまたはファイル/ディレクトリとして）どのように表示されるかは、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」で説明するオプションで制御されます。

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

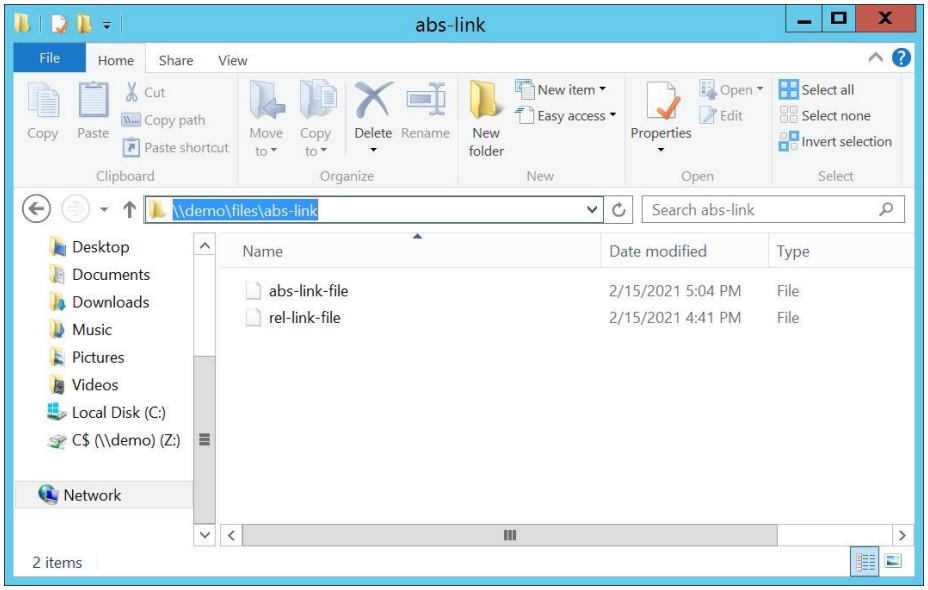


このディレクトリ内のリンクがシンボリックリンクであることをONTAPに通知するには、次のコマンドを実行してCIFSシンボリックリンクパスを定義します。

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

この例では、`-unix-path` 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（`/mnt/client1`います）。ファイルは同じボリューム内にあるため、`-locality` 値に「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（ワイドリンク）

次に、1つのボリュームから同じネームスペース内の別のボリュームに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、これは重要なステップです。これらのボリュームへのリンク方法を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するボリュームのルートにリンクを作成し、別のボリューム内の3階層のフォルダにリダイレクトします。ディレクトリツリーの上位のパスを使用しない限り、ここでは相対パスを使用しないでください。使用していたの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配置されます。

- リンクされたボリュームの絶対フォルダパスはです /mnt/client1/dir1/dir2/linked-dir。
- client1 client2 NFSマウントで次のコマンドを実行して、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つのボリュームは次のとおりです。

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

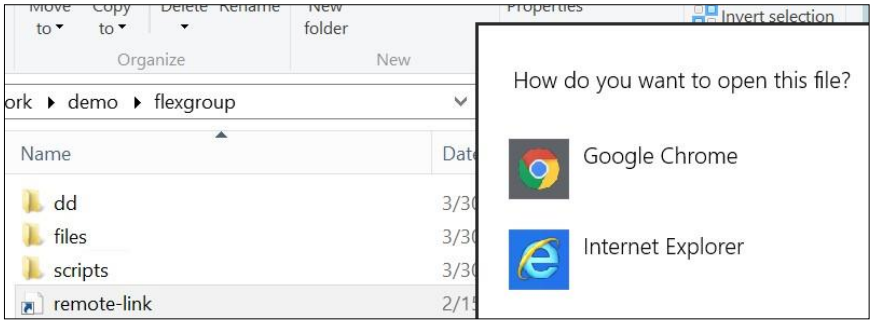
このリンクが作成されると、NFSで想定される結果が表示されます。リモートシンボリックリンク()remote-linkとフォルダパス（/mnt/client1/dir1/dir2/linked-dir/）は、シンボリックリンクパスから作成されたファイルと同じファイルを示しています）の両方が表示されます。

```
# 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が（ショートカットまたはファイル/ディレクトリとして）どのように表示されるかは、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」で説明するオプションで制御されます。

図19）CIFSシンボリックリンク、絶対パス、各種ボリューム-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。前の例では -unix-path、として定義されたシンボリックリンクパスが作成されてい /mnt/client1ます。このシンボリックリンクはを参照して /mnt/client1いますが、に存在する /mnt/client2ため、パスのリダイレクト先をONTAPに通知するための新しいCIFSシンボリックリンクエントリが必要です。

ここでは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みなされます。
- locality オプションを変更するには、次のコマンドを実行します。

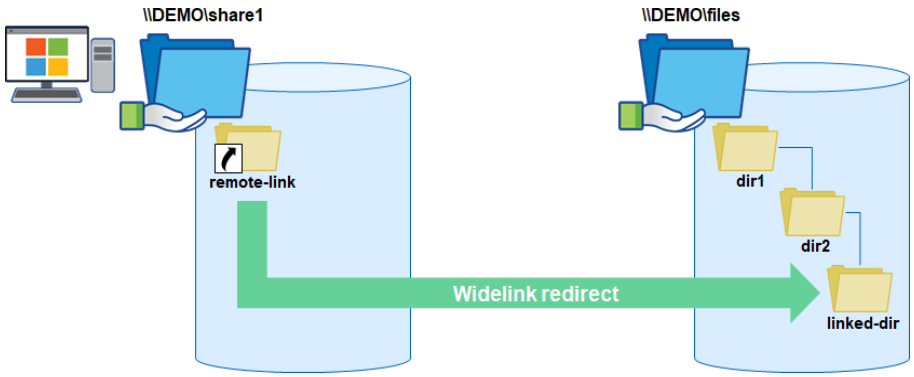
```
cluster::*> cifs symlink modify -vserver DEMO -unix-path /mnt/client1/ -locality widelink
```

さらに、 symlinks_and_widelinks に対して設定する必要があるソースとデスティネーションの両方のCIFS共有を有効にします -symlink-properties。シンボリックリンクパスをワイドリンクとして定義し、を -symlink-properties ワイドリンクに変更しないと、既存のリンク（前の手順で作成した絶対パスリンクなど）が切断されます。

```
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
```

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

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、リンクはショートカットフォルダまたは通常のフォルダ(ショートカットファイルではなく)として表示され、リンクされた適切な場所に正しくリダイレクトされ、表示されるはずのファイルが表示されます。

注： シンボリックリンクが（ショートカットまたはファイル/ディレクトリとして）どのように表示されるかは、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」で説明するオプションで制御されます。

図21）CIFSシンボリックリンク-適切な設定の前後

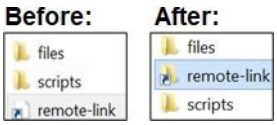
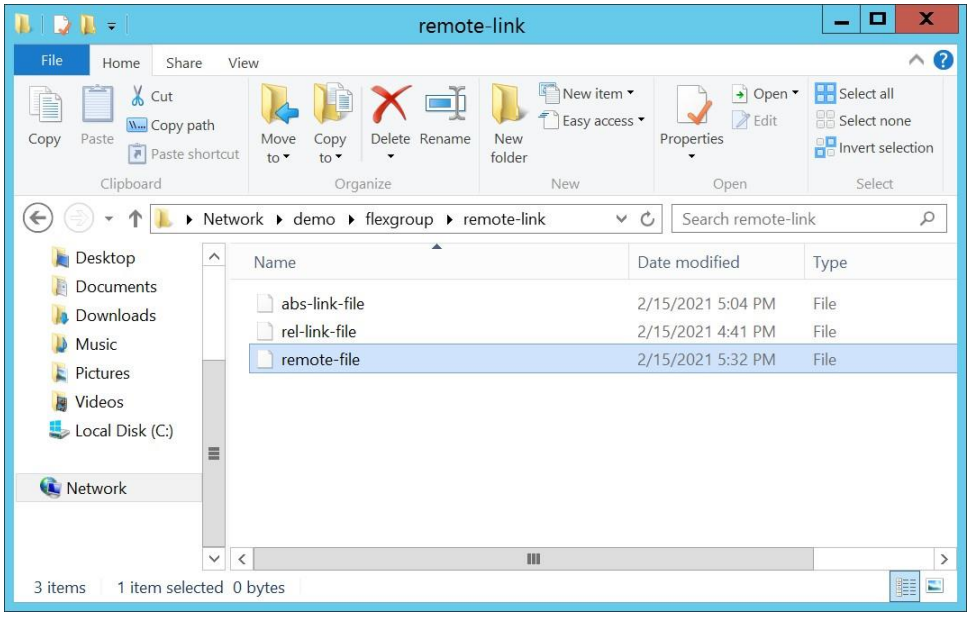


図22）CIFSシンボリックリンク、別のボリューム/同じSVM-widelink



CIFSシンボリックリンク：NetApp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できます。

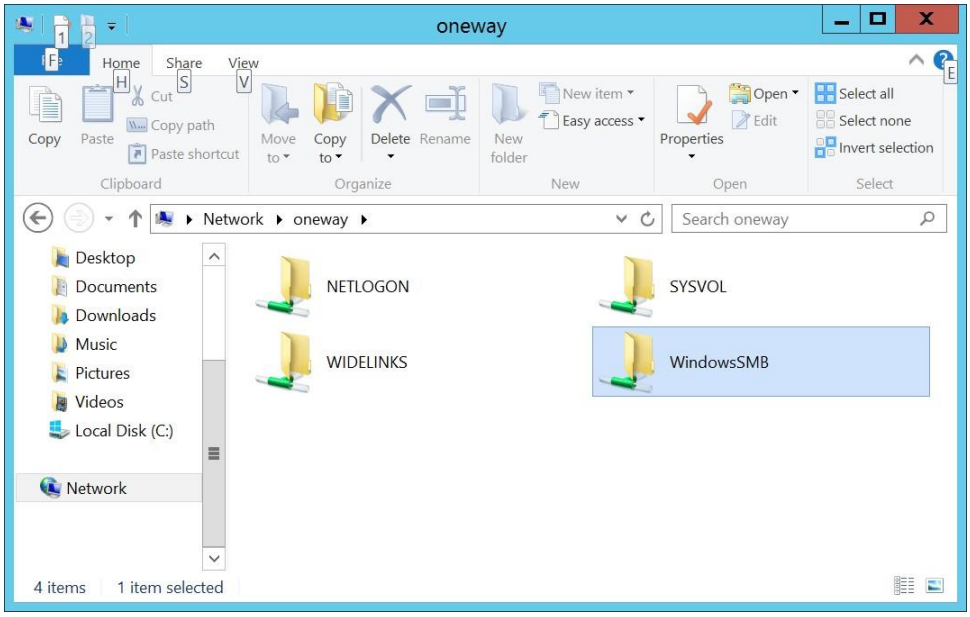
この例では、ONTAPボリュームでホストされているCIFSシンボリックリンクを使用して、Windowsサーバでホストされ ているCIFS共有をポイントします。これはWindowsサーバであるため、NFSクライアントからのシンボリックリンクをテストすることはできませんが、前のセクションで説明した同じ概念を活用して、SMBサーバ間で動作するワイドリンクを作成できます。

- `-unix-path` リンクされたWindows共有のはです `/mnt/winclient/WindowsSMB/`。
- `client1 client2` NFSマウントで次のコマンドを実行して、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サーバ上に作成されたWindows共有の名前はになり `ONEWAY.NTAP.LOCAL`、CIFSサーバ名はになります `ONEWAY`。

図23）WindowsサーバのSMB共有



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が存在するONTAP SVM上のCIFS / SMB共有の `-symlink-property` 値は、`symlinks_and_widelinks -locality` に設定する必要があります `widelink`。

```
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
```

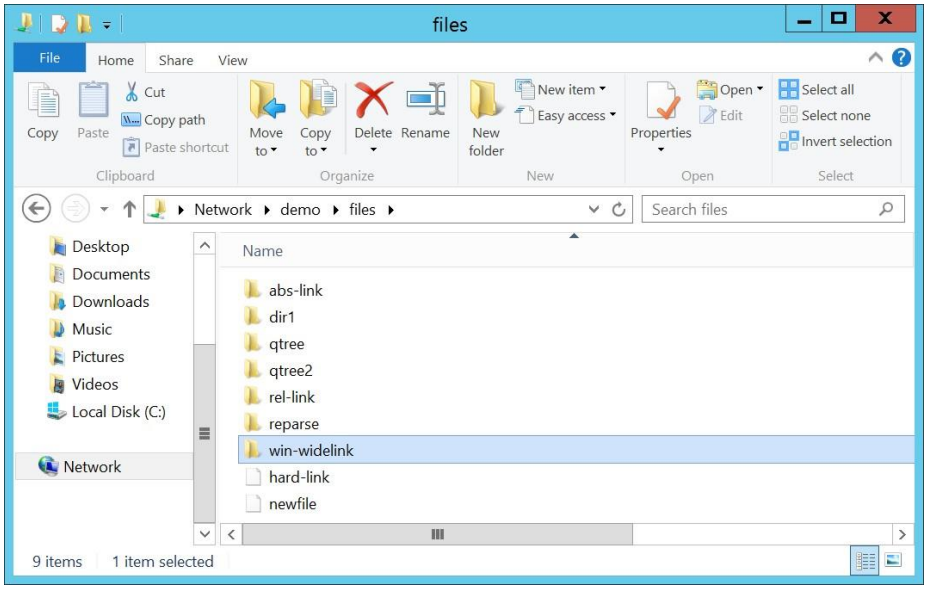
`cifs symlink` このコマンドの構成は次のとおりです。

- `-unix-path` パスはシンボリックリンクの作成に使用され（`/mnt/winclient/WindowsSMB/`ます）。
- `-cifs-path` は`/`に設定されています。ここから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のCIFS / SMBサーバの名前です。この例では、Windowsサーバ名はです `ONEWAY`。
- `-locality` ファイルシステムを横断しているためwidelinkになります。
- `-share-name` は、デスティネーションのCIFS / SMB共有WindowsSMBの名前です。

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アイコンのいずれかが表示されます。

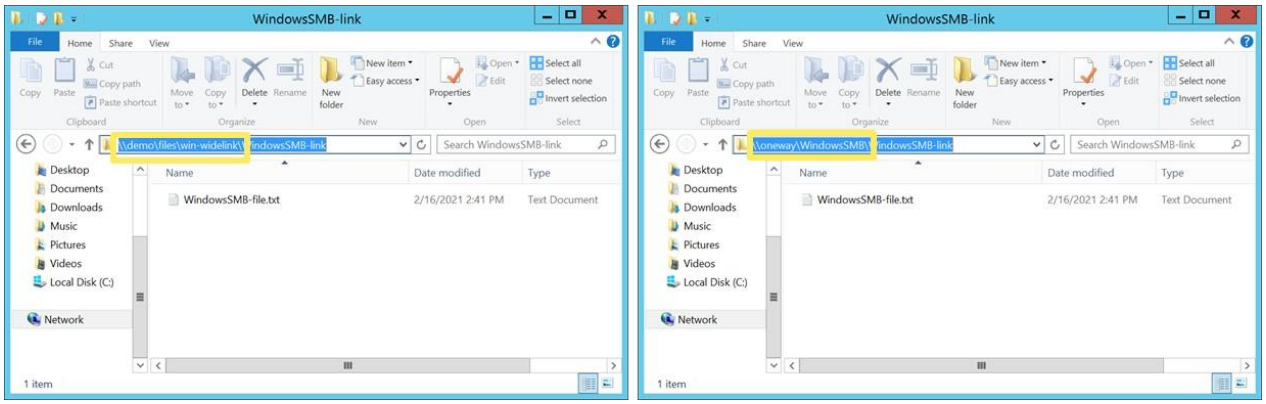
注： シンボリックリンクが（ショートカットまたはファイル/ディレクトリとして）どのように表示されるかは、使用しているSMBのバージョンによって異なります。シンボリックリンクは、「ジャンクションパスとリパースポイント」で説明するオプションで制御されます。

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共有に直接移動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クライアントでは `dfsutil diag` 、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サーバで機能します。

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参照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。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がファイルへのシンボリックリンクを作成しました。
- `-locality` ローカルを使用するONTAPのCIFSシンボリックリンクパス。

- のCIFS共有 `-symlink-properties` が `symlinks` またはに設定されている `symlinks_and_widelinks`。
- 構成に応じて、`-symlink-properties` オプションは `no_strict_security` オプションです。

次の例は、NFSを使用して作成されたファイルのシンボリックリンクを示しています。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配置されます。

```
# 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です。

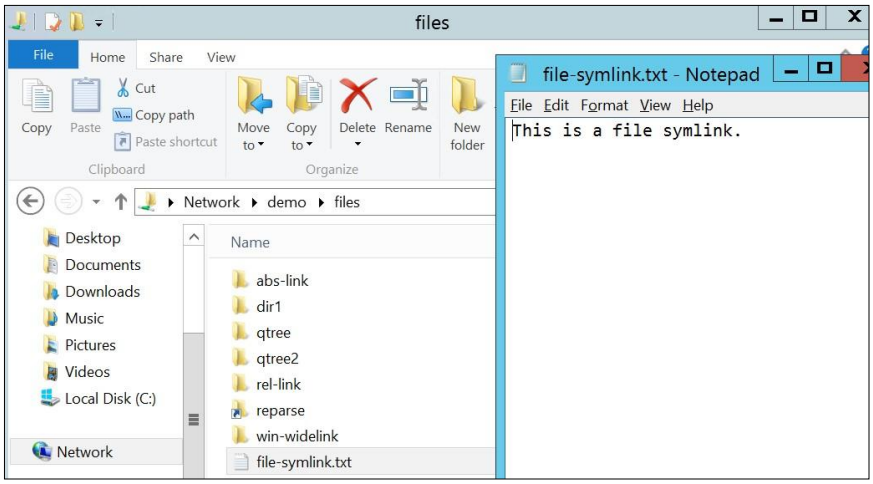
```
cluster::*> cifs symlink show -vserver DEMO -unix-path /mnt/client1/

                  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共有の `-symlink-properties` 値は次のとおりです。

```
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、SMBクライアントにシンボリックリンクファイルが表示されます。

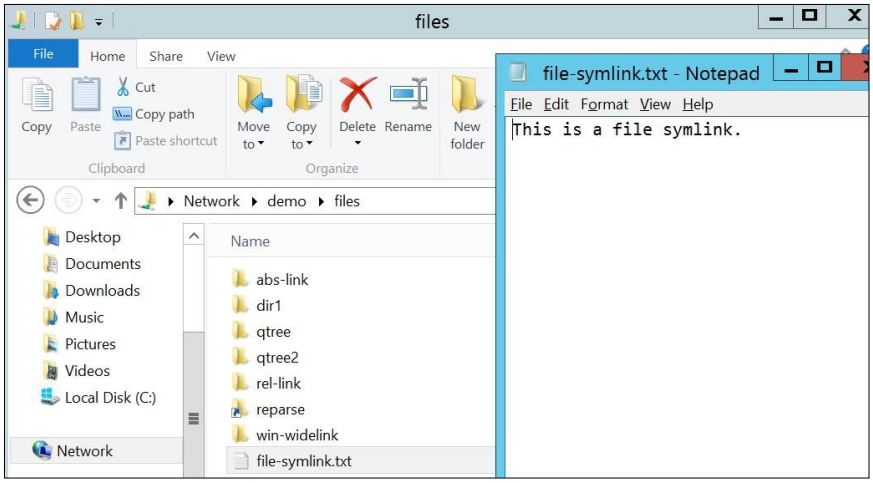
図26）ローカルファイルのシンボリックリンク-ローカルのローカル性、symlinks_and_widelinks共有プロパティ



CIFS共有の `-symlink-properties` 値をに変更し `no_strict_security`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
```

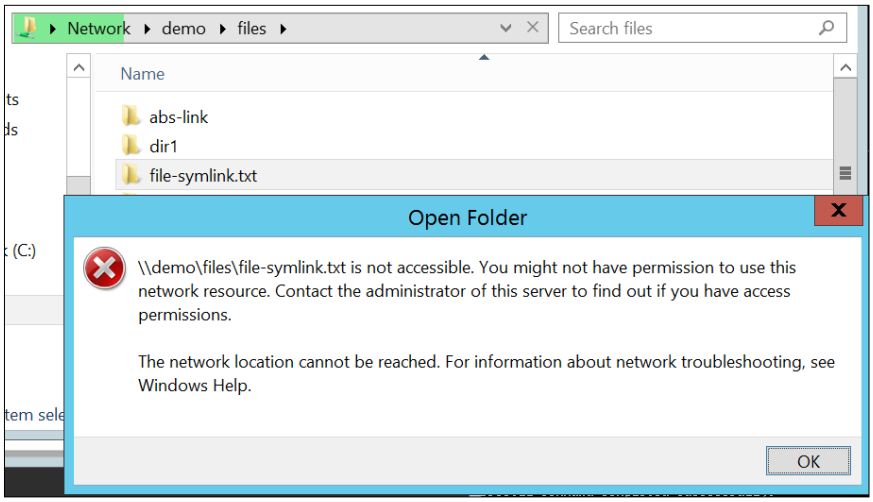
図27）ローカルファイルのシンボリックリンク-ローカルの局所性、シンボリックリンク、no_strict_security共有プロパティ



シンボリックリンクパスを `-locality` 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 locality、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。
- ファイルを開くためのシステムAPIはワイドリンクのあとに正しく表示されますが、このプロセスによって一部のアプリケーションが混乱する可能性があります。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に解決されるワイドリンクを作成します。
- ワイドリンクでは、デスティネーションマシン上の共有されていない領域にクライアントを転送することはできません。

CIFSシンボリックリンク：リモートファイルへのリンク

同じボリューム内のファイルにリンクするファイルのシンボリックリンクを作成するのは簡単です。「CIFSシンボリックリンク：ローカルファイルへのリンク」を参照してください。

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、次のような課題に直面します。

- 一般に、ボリュームの境界を離れるシンボリックリンクはワイドリンクとみなされます。
- ワイドリンクはSMBクライアントではディレクトリとして表示されます。

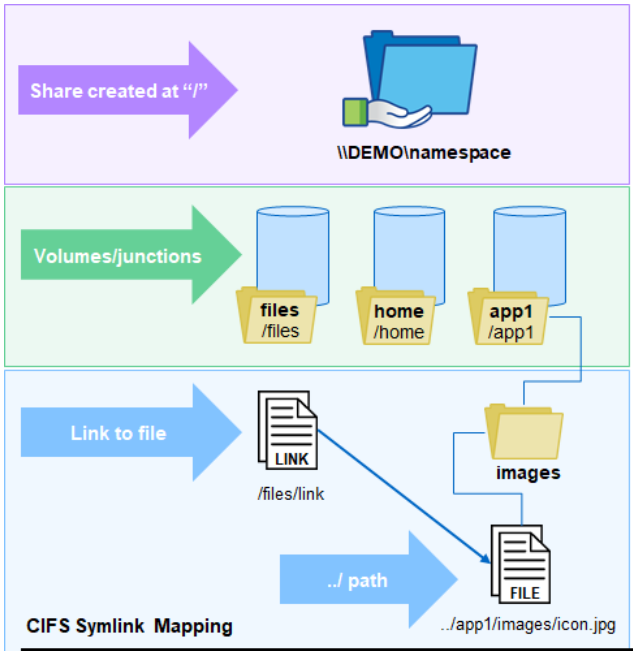
では、ファイルとして表示され、別の共有にリダイレクトされるファイルシンボリックリンクを作成するにはどうすればよいでしょうか。

主に次の2つのオプションがあります。

- ボリュームが結合された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、./を使用してファイルパスをディレクトリの最上位レベルにリダイレクトするシンボリックリンクを使用します。ユーザが共有から離れ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して、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。ユーザーはシンボリックリンクを介して共有します。

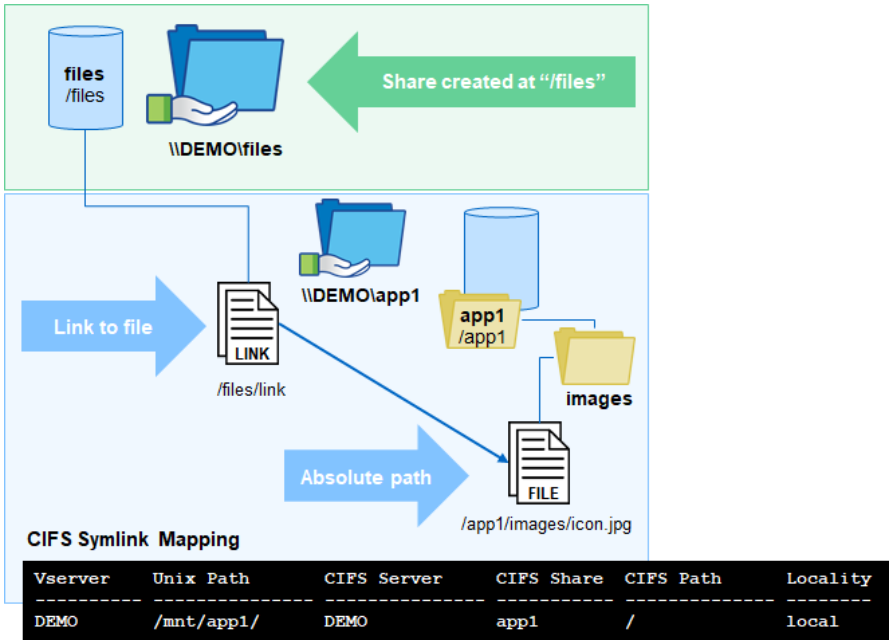
図29 に、これらの各オプションを示します。

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



Vserver	Unix Path	CIFS Server	CIFS Share	CIFS Path	Locality
DEMO	/files/	DEMO	namespace	/	local

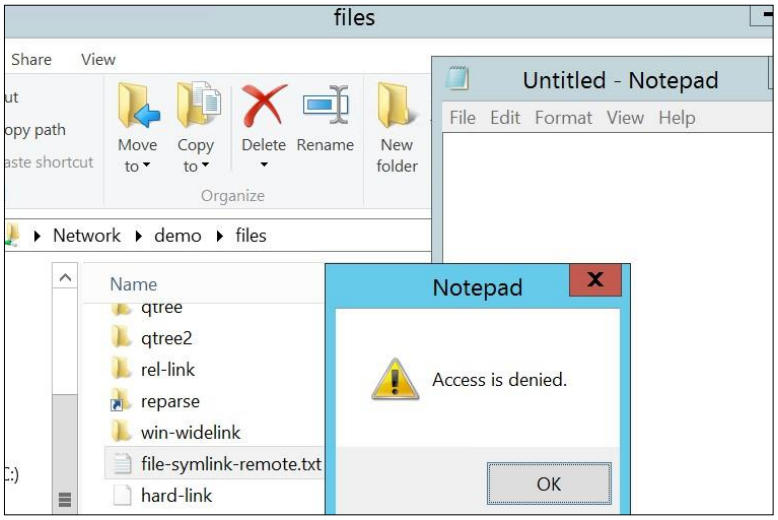
図30）別の共有へのリダイレクトを使用した共有からのシンボリックリンク-絶対パス



ファイルシンボリックリンクに関する潜在的な問題

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-ローカルのローカル性、symlinks_and_widelinks共有プロパティ



アクセス拒否メッセージ

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こうとしたときに[Access Denied]と表示される場合は、次の点を確認してください。

- シンボリックリンクノACL
- デスティネーションファイルノACL
- デスティネーションキョウユウデノACL

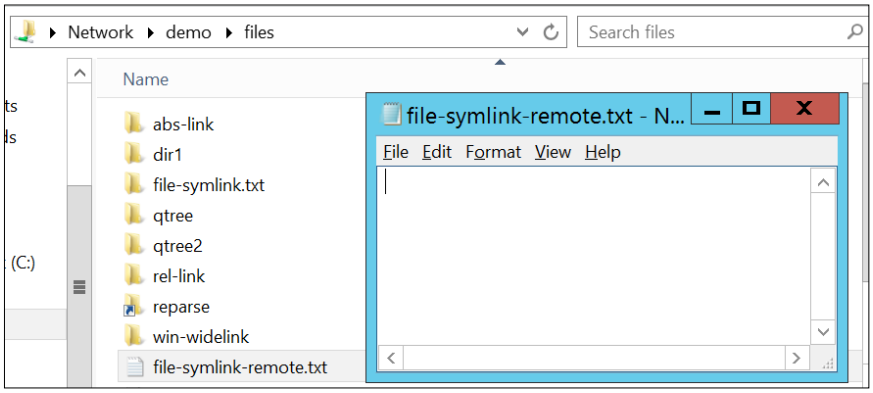
- シンボリックリンクはNFSクライアントで機能しますか。
- CIFSシンボリックリンクマッピングパス設定：
  - 共有名は正しいですか？
  - UNIXパスは正しいか。
  - 相対パスまたは絶対パスを使用していますか。
  - ローカルを地域として使用していますか？
- CIFS共有-symlink-properties
  - no_strict_securityは使用されていますか。

  注： `no_strict_security` SMBの適用を一部削除することで、共有間でのシンボリックリンクの機能を許可します。

空のファイル

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、想定した内容がファイルに含まれていない場合があります。

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クライアントで機能しますか。
- 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しますか。
  - UNIXパスは正しいか。
  - 相対パスまたは絶対パスを使用していますか。
  - ローカルを地域として使用していますか？
- CIFS共有-symlink-properties：
  - `no_strict_security` 使用されているかどうか

  注： `no_strict_security` SMBの適用を一部削除することで、共有間でのシンボリックリンクの機能を許可します。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トDFSツウチ

CIFSシンボリックリンクパスを作成する際に、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や、定義されたパスをたどるだけでDFSをアドバタイズしない場合に、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 _strict_security この動作は、CIFS共有のnoオプションによって制御されます。

このオプションが無効（設定されていない）で、CIFSシンボリックリンクパスが -locality widelinkに設定されている場合、CIFS / SMBクライアントは FSCTL_DFS_GET_REFERRALS ストレージシステムに送信し、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を確認します。

パケットキャプチャでは、DFS通知が使用されると、次のパケットが表示されます。

SMBクライアントからのパケット：

```
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。この場合は、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クライアントで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ます。
3. のシンボリックリンクに使用するパスを使用します -unix-path。
4. -symlink-properties no_strict_security ソース共有で、をsymlinksに設定します。

次の例では、という名前のCIFS共有は、 flexgroup 共有のルートにシンボリックリンクがあり、CIFS共有にリダイレクトされ filesます。

次の例は、シンボリックリンクを示してい /mnt/xyzます。シンボリックリンクのポイントは次のとおりです。

```
# 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。

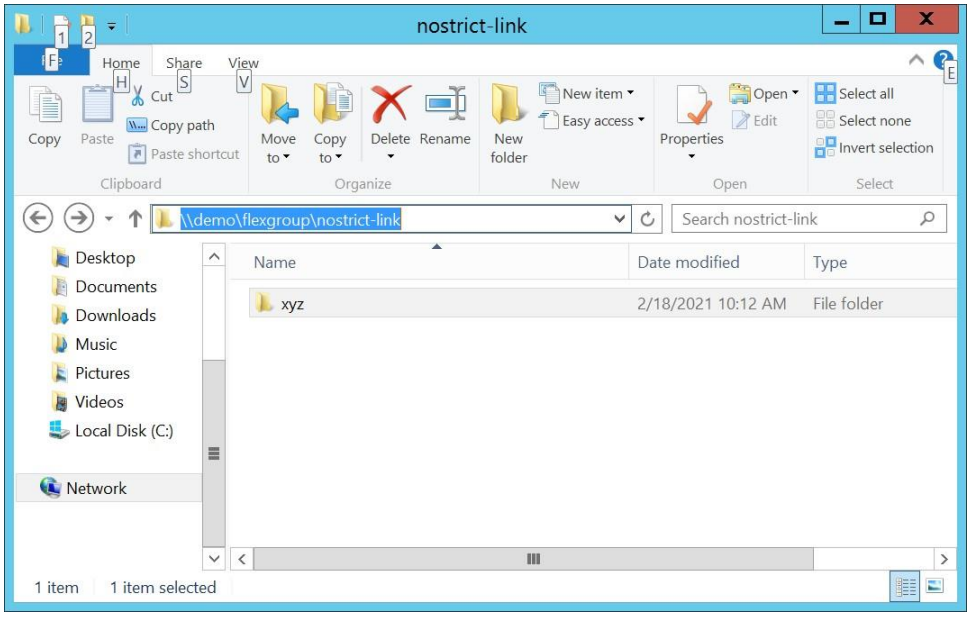
```
cluster::*> cifs symlink create -vserver DEMO -unix-path /mnt/xyz/ -cifs-path / -cifs-server DEMO
-locality local -home-directory false -share-name files
```

次の例は、CIFS共有-symlink-propertiesを表示します。

```
DEMO     flexgroup symlinks,no_strict_security
```

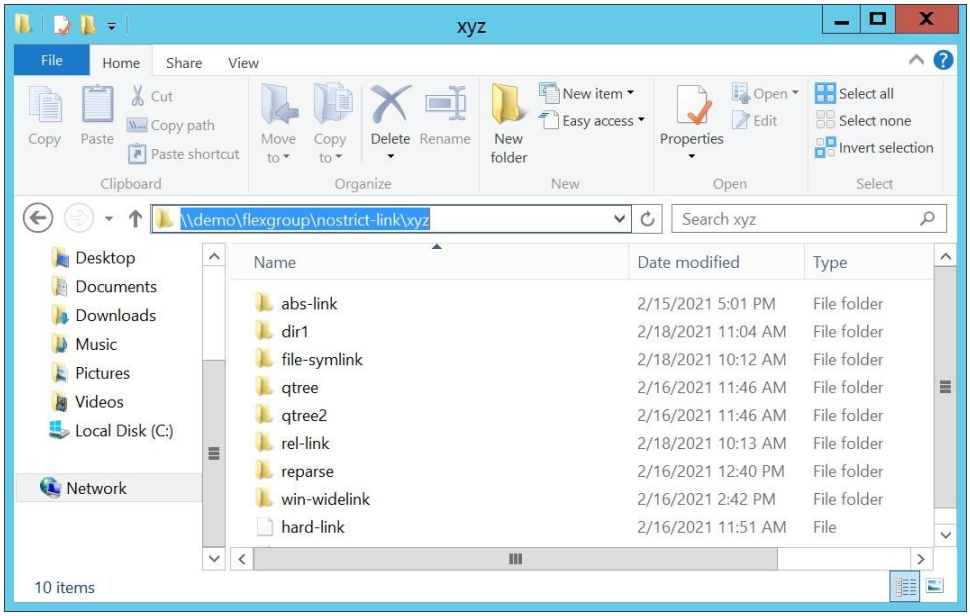
次の例は、CIFSでのシンボリックリンクの表示方法を示しています。

図33）CIFS symlink-no_strict_security



このフォルダに移動すると、共有ファイルに移動します。

図34）CIFS symlink-no_strict_securityのナビゲーション



クライアントがパスを認識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
```

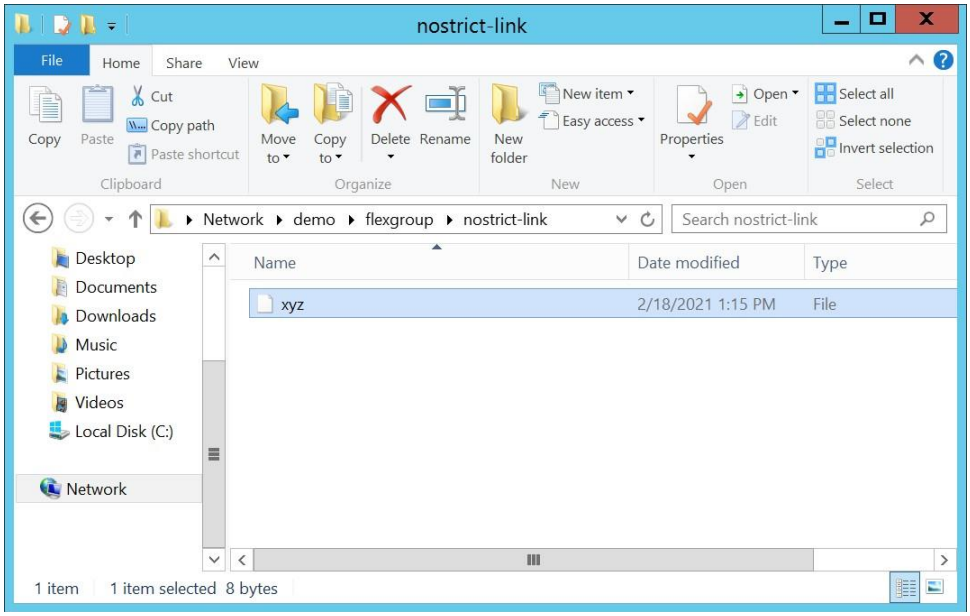
```
Could not complete the command successfully.
SYSTEM ERROR - The system cannot find the file specified.


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すると、ONTAPはと応答します `STATUS_NOT_FOUND`。

```
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、トラフィックはリダイレクトされません。このリンクを設定せずに使用するには、`no_strict_security`CIFSシンボリックリンクパスマッピングで `- locality` ワイドリンクに変更し、CIFS共有を `-symlink-properites` に変更する必要があり `symlinks_and_widelinks`ます。

図35）CIFS symlink-no_strict_security no set



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

CIFSシンボリックリンクは技術的にはシンボリックリンクではなく、ONTAPで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/パスリダイレクトです。ONTAPでのCIFSシンボリックリンクの動作は、SMBクライアントでのファイル、フォルダ、およびシンボリックリンクのmtime値の表示に影響します。デフォルトでは、シンボリックリンクのmtimeはターゲットのmtimeではなくmtimeで表示されます。ONTAPを使用するCIFSシンボリックリンクでのMTIMEの動作は、DFS通知によって制御されます。この動作を変更するには、共有の `-symlink-properties` オプションにno_strict_securityを使用します。

シンボリックリンクの例を次に示します。

```
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使用して、ONTAPからCIFSパスにUNIXパスを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共有に存在するため、別のボリュームターゲット（files CIFS共有）になります。その結果、は symlinks_and_widelinks -として使用されましたsymlink-properties。

```
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
```

クライアントにはDFSアドバタイズメントが表示されます。これはリダイレクションパスです。

```
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がデスティネーションディレクトリのmtimeと異なるため、mtimeに依存して動作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は2021年2月18日12：55PM、シンボリックリンクmtimeは2021年2月18日1：15PM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
```

リンクとディレクトリが同じ時刻になるようにするには、その共有のDFS通知を無効にし、代わりに no_strict_security オプションを使用してリンクをリダイレクトします。詳細については、を参照してくださいno_strict_security、シンボリックリンクおよびDFS通知。次の例は、同一のsymlinkとターゲットディレクトリのmtime値を表示するようにシンボリックリンクの例を示しています。

上記のシナリオを正常に動作させるには、次の手順を実行します。

1. CIFS共有 -symlink-property をに変更します symlink,no_strict_security。
2. CIFSシンボリックリンクマッピング -locality の値をに変更します local。
3. クライアントのDFSキャッシュと正味使用キャッシュをフラッシュします。

dfsutilはパスをアドバタイズしなくなりました。

```
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.
```

宛先ディレクトリの値のみを使用すると、シンボリックリンクとディレクトリのmtimesが同じになります。

```
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
```

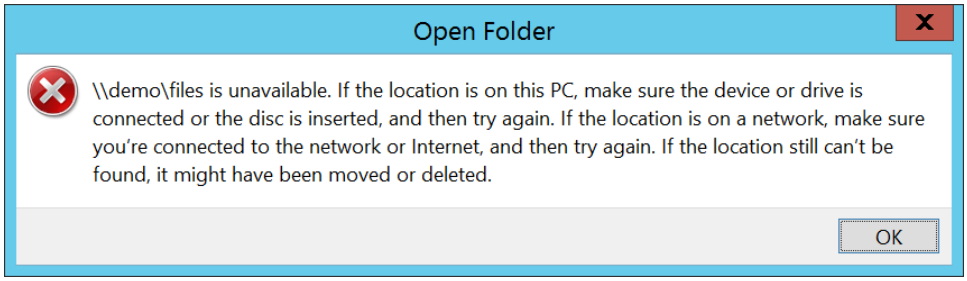
注： シンボリックリンクとターゲットで異なるMタイムを表示するには、ワイドリンクを使用する必要があります。ただし、ファイルを指定した場合、SMBクライアントではワイドリンクが一貫して機能しないため、ディレクトリのみを参照するように指定します。

キャッシュとシンボリックリンクのエラー

CIFSシンボリックリンクを設定する際に、正しいパスマッピングを見つけたときにリンクの移動やCIFS共有へのアクセスで問題が発生することがあります。この問題によって、原因正しい設定が何であるべきかが混乱する可能性があります。これは、有効な問題にfalse negativeやfalse positiveが混在している可能性があるためです。

たとえば、以前は正常に機能していた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キャッシュとONTAP側キャッシュが原因で発生します。このような場合は、3つのメインキャッシュに注意する必要があります。

dfsutilキャッシュ

Windows SMBクライアントでは、シンボリックリンクでDFSを使用してリダイレクトされます。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の量を削減し、パフォーマンスを向上させます。ただし、キャッシュは、動作しているか壊れているように見えるものが実際には反対のシナリオを作成することもできます。

トラブルシューティング時にこれらのキャッシュを表示またはフラッシュするには、dfsutilコマンドセットを使用します。注目すべき主なキャッシュは、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 には、diag パスを解決す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で適切に設定されたワイドリンクを使用しています。

```
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、シンボリックリンクパスが入力された場合のプロバイダキャッシュの状態を示しています。

```
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である場合に、そのエントリがキャッシュ内に存在する期間です。

次に、リファーラルキャッシュの例を示します。

```
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、有効期限が切れるまでキャッシュに保存される期間が表示されます。はabs-link 0秒で期限切れになります。つまり、自動的に期限切れになることはありません。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
```

正味使用量

DFSキャッシュに加えて、SMBクライアントは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。

キャッシュされているCIFSおよび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
```

キャッシュされた個々の接続をクリアするか、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、マッピングされたすべての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： このコマンドをと組み合わせて実行する `dfsutil` と、コマンドを最初に実行してから `dfsutil` キャッシュをフラッシュするよりも結果が良くなります。を実行すると `net use /d`、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）。その場合は、Windowsエクスプローラウィンドウを閉じてキャッシュを再度フラッシュし（`net use` と `dfsutil`）、接続を再試行します。

ONTAPパスの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対してパスキャッシュを提供します。これらのキャッシュは、診断権限の次の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必要に応じて無効または有効にすることができますが、NetAppサポートから特に指示がないかぎり、通常の本番ワークロードでは有効のままにしておく必要があります。

```
[-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、NetApp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ください。

```
[-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イネーブルにするには、診断権限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、パスはになります。NFSクライアントは、そのパスがエクスポートされていればマウントできます。また、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$ hidden共有を使用してにアクセスできます。

デフォルトでは、ONTAPジャンクションパスは、[Advanced Privilege ONTAP CIFS]オプションによっ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 `is-use-junctions-as-reparse-points-enabled`。CIFSシンボリックリンクは、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クライアントではディレクトリとして表示されます（ `widelink-as-reparse-point-versions` オプションの設定によります）。

ジャンクションパスとリパースポイントのオプションのデフォルト設定は次のとおりです。

```
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およびSMB 3.xクライアントで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 `widelink-as-reparse-point-versions` ようにするには、オプションを変更して目的のSMBバージョンを含めます。

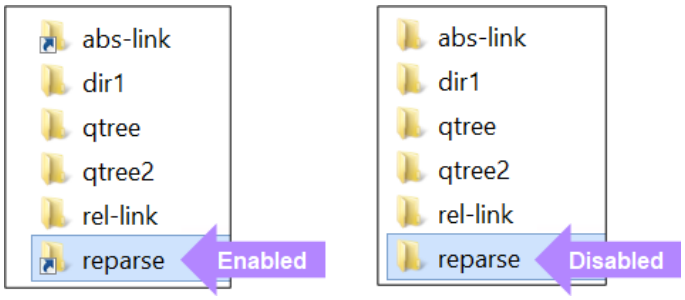
```
cluster::*> cifs options modify -vserver DEMO -widelink-as-reparse-point-versions SMB
```

```
    SMB1    SMB2    SMB2_1 SMB3    SMB3_1
```

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

```
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：リパースポイントの有効化と無効化



次の例は、`cmd` オプションをenabledまたはdisabledに設定してプロンプトにボリュームジャンクションパスを表示する方法を示しています。

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

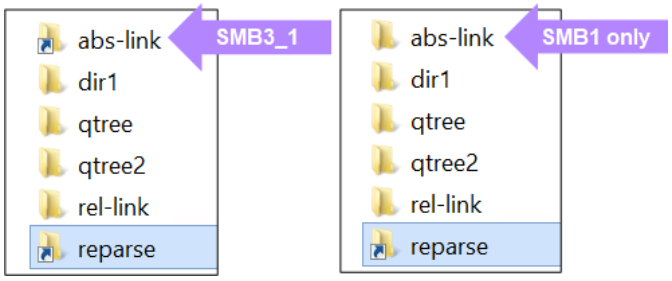
```
C:\>dir \\demo\C$
 Volume in drive \\demo\C$ is
 c$ Volume Serial Number is 80F0-
 3712

 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

```
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、アクセスプロトコルとしてSMB 3.1が使用されています。`abs-link` シンボリックリンクは、smb3_1をオプションに追加するとSMBクライアントからのショートカットとして表示され、オプションをデフォルトのsmb1値のままにすると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：リパースポイントの有効化と無効化



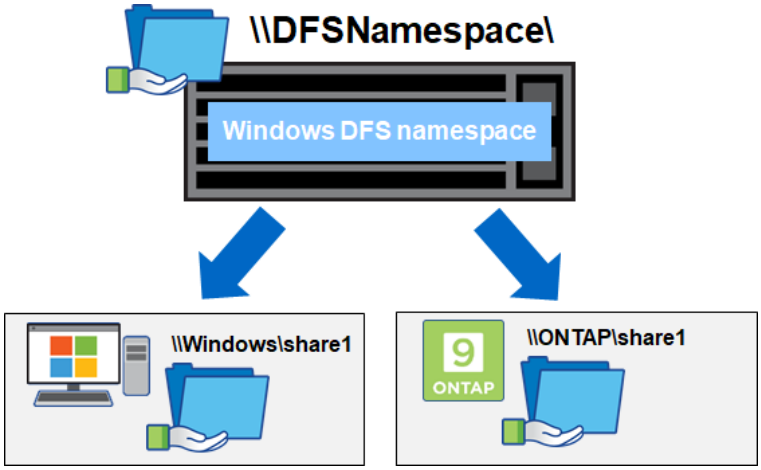
注： シンボリックリンクがリパースポイントとして設定されていない場合、一部のクライアントでデスティネーションパスの適切な量の空きスペースが認識されないことがあります。詳細については、ナレッジベースの記事「Unable to write to a symlink CIFS volume due to "not enough space" error」を参照してください。

分散ファイルシステム

Microsoft Windows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、共有の場所に関係なく、WindowsサーバをSMB共有のエンドポイントのリダイレクタとして機能させることができます。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。この機能を使用すると、CIFS / SMBクライアントに単一のネームスペースを提供し、エンドユーザがアクセスするために複数のIPアドレスやホスト名を知っている必要はありません。代わりに、すべてのユーザが同じサーバに接続し、残りの処理はDFSが行います。

図39 に、ONTAPをターゲットとするWindows DFSを示します。

図39）ONTAPをターゲットとして使用した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、現在はDFS-R（レプリケーション）機能をサポートしていません。複数のサイト間でSMB共有レイアウトを同期する場合は、SMBを使用しているFlexCacheボリュームを使用することを推奨します。

SMBトFlexCacheボリユウム

ONTAP 9.8以降では、FlexCacheボリュームキャブを参照しているSMB共有を作成できるように、SMBプロトコルがキャッシュボリュームでサポートされます。エクスポートポリシーと同様に、FlexCacheボリュームの作成時にSMB共有はレプリケートされません。また、同じSVM内にFlexCacheを作成する場合でも、これらは独立しています。これは、異なる共有権限をキャッシュに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、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と共有権限の適用は、ONTAPでのSMBサーバの設定に大きく依存するため、送信元とキャッシュで同じ権限が適用されるようにするためにはいくつかの要件があります。FlexCacheボリューム、SMB、マルチプロトコルNASに関する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。

ネイティブCIFSおよびNFSファイルの監査

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/フォルダ監査を使用すると、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のファイルがいつアクセス、変更、または削除されたかを追跡できます。

NFSおよびCIFS / SMBの監査は、監査対象の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し、監査と同じデータボリュームに格納するかどうかを決定できます。

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、マルチプロトコルNASの一般的な問題と、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クライアントのファイルリストにファイル所有者/グループ情報がと表示されることがあります `nfsnobody`。

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

ファイルを数値でリストすると、 `owner:group` はになります `65534`。

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

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

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

`pcuser` は、`anonymous` 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クラスタのファイル権限については、UNIXの所有者がであると表示されることがあります 65534 が、WindowsのACLと所有者も異なります。

```
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る場合は、次のいずれか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ているボリュームはWindows SMBクライアントでも使用され、共有に書き込む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クライアントにエクスポートされているボリュームで匿名ユーザがに設定されている 65534ため、NFSユーザが匿名ユーザに引き下げられています。ユーザの引き下げの詳細については、TR-4067：『NFS in NetApp ONTAP』を参照してください。

WindowsユーザとUNIXユーザのマッピングを表示するには、Advanced Privilege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管理のパフォーマンス、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。

その1つが、NFSクレデンシャルキャッシュの実装です。このキャッシュには、NFSエクスポートへのアクセス時にONTAPのユーザとグループの情報が格納されます。

これらのキャッシュを表示および管理するには、nfs credentials Advanced Privilege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は、NFSマウント用のTCP接続が存在するノードに入力されます。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
```

上記のコマンドは `x.x.x.x` 、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、キャッシュエントリに注目するノード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エクスポートに移動すると、ユーザID、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。この例では、というユーザがです `prof1`。

```
# 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つのエントリがあります。1つの数値UIDと7つのグループメンバーシップです。`prof1` その後、ユーザーは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が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数です。環境内に複数のSVMがある場合は、トラブルシューティングの際にこの数を使用しないことがあります。

NFSクレデンシャルキャッシュの表示

NFSクレデンシャルキャッシュにあるクレデンシャルの数だけでなく、ユーザやグループの個々のキャッシュエントリも表示できます。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。

この例では、が `prof1` マウントにアクセスします。そ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、ユーザと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では、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。負のエントリは、ONTAPが数値のUIDを有効なユーザに解決できない場合に発生します。この場合、UID 1236はONTAPで解決できませんが、NFSエクスポートにアクセスしようとしました。

```
# 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での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エクスポートをトラバースして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`、この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
```

ユーザがNTFS権限/セキュリティ形式のエクスポートにアクセスすると、フラグ `cifs-creds-present` とドメインSID情報が表示され `Windows Credentials`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ノセッテイ

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サーバオプションによって制御されます。

表6）NFSクレデンシャルキャッシュの設定

オプション	機能	デフォルト値（ms）
-cached-cred-negative-ttl	（オプション）このパラメータは、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経過時間を指定します。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	（オプション）このパラメータは、受理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経過時間を指定します。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	（オプション）このパラメータは、キャッシュされたクレデンシャルの収集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には、最終アクセス/更新からの時間が保持されます（ show コマンドを参照）。エントリが一定期間アイドル状態のままになると、最終的には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、必要な影響に応じて、タイムアウト値を長くしたり短くしたりできます。

- **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、ユーザの検索が高速になりますが、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、誤検出や誤検出が増加す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）ネーム検索のレイテンシが増加する可能性がありますが、より正確で最新のエントリが提供されます。

NetAppのベストプラクティスでは、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、結果を確認し、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フラッシュ

ユーザがグループに対して追加または削除され、適切なアクセス権がない場合は、キャッシュエントリがタイムアウトするのを待たずに、クレデンシャルキャッシュエントリを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、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アドレスまで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：キャッシュ

クラスタに対する要求数を削減するために、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がすべて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し、ネットワークおよびネームサービスサーバの負荷が軽減されます。

clientmatchキャッシュ

clientmatchエントリがキャッシュされている場合、そのエントリはSVMに対してローカルのままで、キャッシュタイムアウト時間に達した場合やエクスポートポリシールールテーブルが変更された場合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はONTAPのバージョンによって異なり、`export-policy access-cache config show` 管理者権限でコマンドを実行することで確認できます。

デフォルト値は次のとおりです。

```
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の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、アドバンスト権限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にホスト名を設定すると、その名前が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）で使用す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がに設定されている場合 `files,dns`、ONTAPはローカルホストファイルで一致するクライアントを検索し、次にDNSを検索します。

名前検索後、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、詳細権限でONTAP CLIから照会およびフラッシュすることができます。

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ときに、アクセスの問題を解決するためにホストのエントリのフラッシュが必要になることがあります。

ホストの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
```

ネットグループキャッシング

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と通信してネットグループ情報を展開する追加の作業を行います。ns-switch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がネットグループのサポートに使用する方法は、netgroup.byhostの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：『How to Configure LDAP in ONTAP』を参照してください。

- netgroup.byhostが無効になっている場合、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取り込みます。ネットグループに数千のクライアントがある場合は、プロセスが完了する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が有効になっている場合、ONTAPはネームサービスに対して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照会します。このプロセスにより、潜在的に数千のクライアントを検索する必要がないため、ネットグループのクエリに必要な時間が大幅に短縮されます。

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

ネットグループ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、そのネットグループは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
```

キャッシュされているネットグループエントリが1つだけの場合、`ip-to-netgroup` および `hosts reverse-lookup` キャッシュには次のエントリが入力されます。

```
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

必要に応じて、キャッシュ設定を別の値に変更できます。

- タイムアウト値を大きくするとキャッシュエントリが長くなりますが、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の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、キャッシュがフラッシュされる頻度が高くなり、より最新の情報が取得されますが、ネームサービスサーバへの負荷が増大し、クライアントからのマウント要求のレイテンシが増大す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のが最善の方法です。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では、`exportfs` は `export-policy` および `name-service` cacheコマンドに置き換えられています。を実行する `exportfs`と、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コマンド

ほとんどの場合、NFS権限の問題はきわめて簡単です。NFSv3では基本的なrwxモードビットが使用されます。ただし、NFSv4 ACLやマルチプロトコルNASアクセス、およびさまざまなセキュリティ形式が関係する場合は、状況がより複雑になります。このセクションでは、NAS環境での権限の問題のトラブルシューティング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の情報については、「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処理では、IDを確認するために数値を渡すことができるため、UNIXの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ユーザ名およびグループ名に変換する必要があります。NFSv4の場合、ユーザが nobodyに引き下げられるのを防ぐために、この数値IDと名前のマッピング/変換が必要です。NTFSセキュリティ形式では、UNIXユーザ名を有効なWindowsユーザ名にマッピングする必要があります。

ONTAPには、UNIXユーザのIDとグループメンバーシップを表示するためのコマンドがいくつかあります。

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、高度な権限）のUID / GIDの基本情報を表示するには、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:
```

ユーザ情報とグループメンバーシップ（ローカルサービスとネームサービス、高度な権限）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情報の表示

環境でCIFS / SMBとNFSの両方を設定している場合は、Advanced Privilegeの1つのコマンドで、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場合に推奨されるコマンドです。コマンドは、SMB / CIFSサーバが設定されていない場合は機能しません。

```
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テシヨウサレルフアイルケンケンノヒヨウシ

権限の問題をトラブルシューティングする際に、NASクライアントから権限を表示するアクセス権がない場合があります。また、NASクライアントに表示されている権限とONTAPに表示されている権限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
```

また、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になっている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アクセスの確認

場合によっては、権限の問題がエクスポートポリシーの設定に起因することがあります。たとえば、読み取りのみを許可するようにポリシーが設定されている場合、その設定はマウントで設定されているすべての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アクセスを確認できます。

```
cluster::> export-policy check-access
```

セキュリティトレースの使用

権限の問題が発生したとき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、特定のユーザ名またはIPアドレスにトレースを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、プロトコルなどで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/アクセスエラーの状況を示しています。

```
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表示の制御

ONTAPでは、ボリュームまたはqtreeでUNIXのセキュリティ形式が使用されている場合に[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はです `is-unix-nt-acl-enabled`。

このオプションはデフォルトで有効になっており、ファイルシステムオブジェクトのセキュリティ形式がUNIXの場合は[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には、SVM固有の製造済みSIDが表示され、UNIXPermUid、UNIXPermGid、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できますが、読み取り、書き込み、および実行値についてのみ変更できます（`rwx`）。

図40）UNIX SIDを解決する前の[Permissions]ビュー

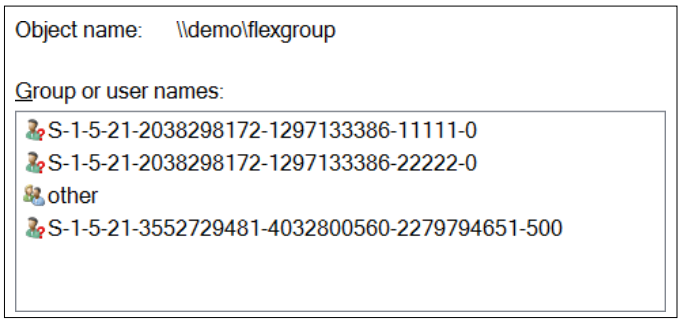
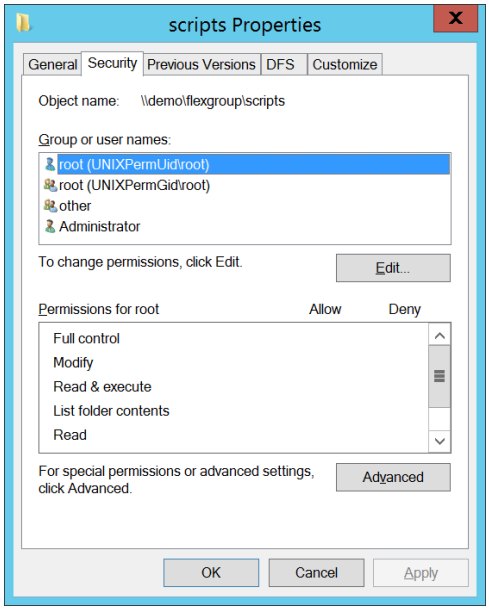


図41 では、scriptsフォルダはUNIXセキュリティ形式で、権限は777です（`vserver security file-directory show` CLI出力から確認）。

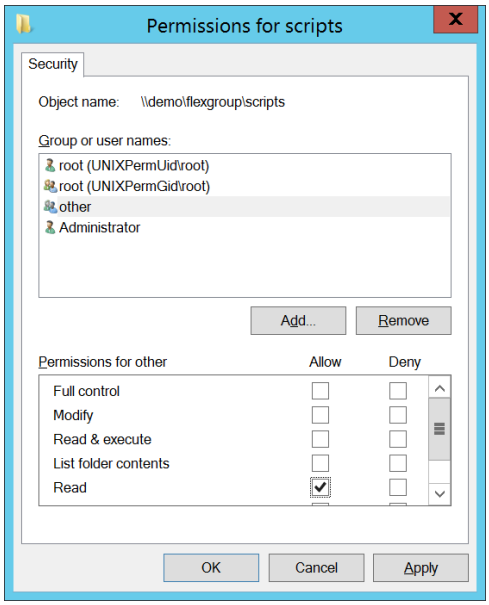
```
cluster::*> vserver security file-directory show -vserver DEMO -path /flexgroup_16/scripts

                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



フォルダの権限は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]に設定することができます。

図42）UNIXセキュリティ形式の[Security]タブ-権限の変更



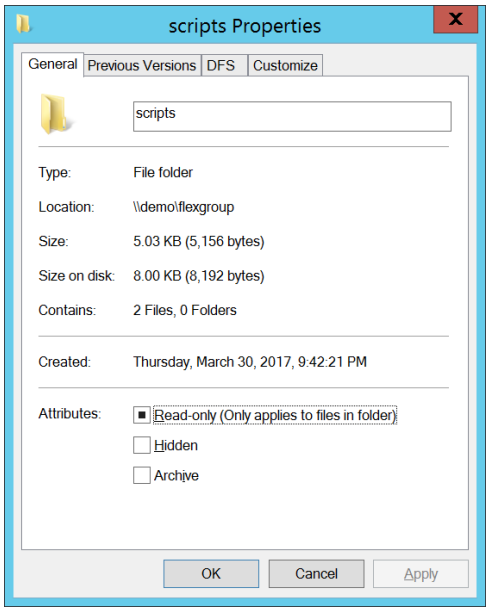
この設定が完了すると、権限は774に変更されます。

```
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セキュリティ形式オブジェクトでCIFS / SMBクライアントに[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、SMBクライアントからUNIXセキュリティ形式オブジェクトに対する権限の不要な変更を防止することです。

図43）UNIXセキュリティ形式で非表示になっている[Security]タブ



NFSクライアントからの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、オブジェクトのモードビットまたはNFSv4 ACLにワイドオープンアクセス権（777）が設定されていると表示されます。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は、ACLまたはモードビットが適切に表示されているかどうかに依存する場合があります。
- モードビットが開いていると表示されたユーザに警告が表示され、サポートチケットやトラブルシューティングに費やされるサイクルが発生す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。ONTAPでは、NTFSセキュリティ形式のボリュームへのアクセスは、NTFSセキュリティとACLに基づいて制御されます。したがって、NFSクライアントがボリュームにまったくアクセス（認証）するためには、有効なWindowsユーザにマッピングされた有効なUNIXユーザが存在している必要があります。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、というオプションが導入されまし `ntacl-display-permissive-perms`た。このオプションのデフォルト値は[Disabled]です。このデフォルト値では、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NTFS ACLと同等の権限が許可されます。その結果、最小アクセス権に基づいて権限が表示され、UNIX用語では現在のユーザの実際のNTFS権限に近いものになります。これは、懸念を軽減し、アプリケーションの互換性に対処するのに役立ちます。

オプションを使用すると、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、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。そのため、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に基づいて異なる結果が表示されることがあります。

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]タブビューに対するNFSv4 ACLの影響

ファイル、フォルダ、またはボリュームにNFSv4 ACLが `-is-unix-nt-acl-enabled` 設定されている場合、SMB 2.0以降のクライアントでは、がTrueに設定されていても、[セキュリティ]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を解決するために使用されるSMB呼び出しと同じもの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：アクセス検証

ONTAPには、エクスポートポリシーのアクセスルールセットとクライアントのアクセスをクロスチェックできるコマンド（`export-policy check-access`）が用意されています。このコマンドを使用すると、エクスポートポリシールールが導入前およびトラブルシューティングの際に適切に機能しているかどうかを判断できます。その機能は `exportfs -c` 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のやり取り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NASの用語

表7 に、この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	あなたが誰であるかを確認します。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します。
許可	認証とネームマッピングのあと、認証によってユーザまたはグループに付与されるシステム内のアクセスレベルが決まります。これには、ACEと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とUNIXの権限は常に1対1にマッピングされるとは限らないため、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、ユーザ名が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。名前をマッピングす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内の仮想IPアドレスで、データや管理、その他のネットワークアクセスをストレージシステムに提供します。NASプロトコルの場合は、データLIFと特定のデータ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、セキュアな固有のテナントをエンドユーザ向けにプロビジョニングできます。SVMごとに、一意のネームスペース、ドメイン、ネームサービス、NASプロトコルなどが設定されます。これにより、サービスプロバイダなど、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に柔軟性を確保できます。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 共有のマウントを試みるクライアント（選択した場合はSMBも含む）へ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。 各ボリュームや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。ポリシーには数百のルールを含めることができ、各ルールに複数のclientmatch値を設定できます。詳細については、「エクスポートポリシーとルールの概念」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境界であり、NASクライアントにマウントポイントまたは共有パスを提供します。FlexVolには、それぞれ固有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ジャンクション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に配置されます。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、FlexVolボリュームのグループであり、大規模なグローバルネームスペースとしてNASクライアントに提供されます。FlexGroupボリュームは、FlexVolボリューム（20PB、2、000億ファイル）よりもはるかに大きく、クラスタ内の複数のノードにまたがることができるため、並列処理が必要なワークロードでパフォーマンスが向上します。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を複数のネームスペースとみなすことも、単一のネームスペース（ディレクトリツリーの構築に使用する場合）とみなすこともできます。FlexGroupやFlexCacheなどのONTAP機能は、グローバルネームスペースの概念をさらに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、リモートの場所にあるボリュームの書き込み可能な永続的仮想キャッシュを提供します。キャッシュは、データが複数回アクセスされ、複数のホストで共有される読み取り処理の多い環境で役立ちます。
CIFS 共有	CIFS（またはSMB）共有は、CIFS / SMBプロトコルを使用して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。通常、これはWindowsクライアントからのものですが、LinuxクライアントまたはMacOSクライアントからのものでもかまいません。
NFSエクスポート	NFSエクスポートは、NFSプロトコルを使用してNASデータにアクセスするクライアント用に作成されたアクセスポイントです。通常、これはLinuxクライアントから実行されますが、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の解決に役立つものもあります。

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は、`nfs modify` コマンドで制御します。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に影響する可能性があるNFSサーバオプション-ONTAP 9.8以降

オプション	マルチフロトコルNASニヨエルエイキヨウ
`-v4.0/v4.1`	NFSバージョン4.xを有効にするには、UNIXユーザを名前文字列にマッピングする必要があります。適切に設定されていないと、クライアントの動作が予測不能になる可能性があります。クライアントにNFSv4.xが不要な場合でも、クライアントはNFSv4.xとネゴシエートできます（指定しない場合）。これにより、マルチプロトコルNAS、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可能性があります。
`-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、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、NTFS権限を使用するボリュームまたはqtreeにアクセスしようとするすべてのUNIXユーザが、デフォルトのWindowsユーザにフォールバックされます。たとえば、UNIXユーザが `jacksprat` 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、という名前のWindowsユーザ `jacksprat`、または既存のネームマッピングルールをLDAPファイルまたはローカルファイルで検索します。存在しない場合は、`jacksprat` 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場合、権限を識別できないためにONTAPはそのユーザを無効とみなすため、NFSからNTFSセキュリティ形式へのボリュームへのONTAPの認証に失敗します。
`-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に対して実行される場合のNFS処理の動作を制御します。NFS処理（chmod、chownなど）は、NTFSセキュリティ形式のボリュームでは実行できません。エクスポートポリシールール（fail）のデフォルトの設定では、処理が試行されたときに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、ignoreに設定して、処理がサイレントに失敗するようにすることもできます。 デフォルトでは、NFSサーバの値はに設定されます `use_export_policy`。つまり、エクスポートポリシールールによって、NTFSセキュリティ形式のオブジェクトに対するNFS処理のクライアントへのレポート方法が決まります。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。この動作をより細かく制御する必要がある場合は、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からその動作を制御します。
`-v4-id-domain`	NFSv4.xが有効な場合、`-v4-id-domain` オプションによってONTAPのユーザ文字列の作成方法が決まります。名前文字列/ドメインマッピングが適切に行われるように、この文字列はNFSクライアント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文字列に指定したままにした場合、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すると、 ONTAPはその文字列に一致しません。は `jacksprat` defaultv4iddomain.comドメインに属しています。

オプション	マルチフロトコルNASニヨエルエイキヨウ
	jacksprat@domain.comは jacksprat@defaultv4iddomain.comと同一ではないため、ユーザは次の nobody場所に引き下げられます。nobody は有効なUNIXユーザではなく、意図したUNIXユーザではないため、マルチプロトコルNAS環境では基本的にWindowsとUNIXのネームマッピングが解除されます。
-v4-acl-preserve	このオプションを有効にすると、NFSv3 chmod chown 処理または処理が試行されてもNFSv4.x ACLが保持されます。 を実行すると、chown/chmod NFSv4.xのACEが無効になります。NFSv4 ACLをNTFSセキュリティ形式に適用できないため、このオプションは環境UNIXまたはmixedセキュリティ形式のみです。
-v4.0-acl/-v4.1-acl	マルチプロトコル環境でNFSv4.x ACLを有効にすると、セキュリティ形式がUNIXまたはmixed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。使用するNFSバージョンのACLを有効にする必要があります。たとえば、NFSv4.1を使用している場合は、を有効にします -v4.1-acl。どちらか一方のNFSバージョンのみを使用する場合は、両方を有効にする必要はありません。 **注：** ONTAP 9.8以降ではNFSv4.2がサポートされますが、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 オプションでは、名前文字列に一致する文字列がない場合に、NFSv4.xユーザが数値IDを利用できるかどうかを指定します。つまり、NFSv4.xはユーザ名解決にNFSv3のような機能を果たし、ドメインID文字列のマッピングは不要です。デフォルトでは、この値は[有効]に設定されています。 マルチプロトコルNAS環境では、NFSのユーザ名が数値IDとして到着し、（ローカルファイル/ passwd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に動作します。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、有効なユーザ名を有効なWindowsユーザにマッピングする必要があります。 ユーザ名に数値ID 1234が指定されていて、その数値IDに対応する有効なUNIXユーザ名が見つからない場合、ONTAPはのWindowsユーザへのマッピングを試み DOMAIN\1234ます。通常、このような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や認証は失敗します。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。デフォルトでは、NFS処理でサポートされるGID auth_sys は、の場合はユーザあたり最大16、の場合は最大32 auth_gssです。つまり、ユーザがNFSでサポートされているよりも多くのグループに属している場合、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	マルチフロトコルNASニヨエルエイキヨウ
	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のリバースクエリを実行することで、ユーザあたり最大1、024個のグループをサポートできます。マルチプロトコルNAS環境でネームサービスを使用する場合は、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。詳細については、TR-4067およびTR-4835を参照してください。
-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です。ネームサービスサーバへのネットワーク接続が良好で、要求の負荷分散に十分な数の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は最小限です。
-map-unknown-uid-to-default-windows-user*	NTFSセキュリティ形式のボリュームがあるシナリオでは、また、ユーザの数値NFS IDを有効なWindowsユーザ名にマッピングすることはできません。このオプションは、不明なUIDを -default-win-user オプションで定義したデフォルトのWindowsユーザにマッピングするかどうかを制御します。これは、*すべての*着信不明UIDが、指定されたWindowsユーザーにマッピングされることを意味します。これは、他のユーザーとして機能する予定のユーザーであっても同様です。 このオプションのデフォルト値は[Enable]ですが、- default-win-user 値は設定されていません。したがって、デフォルトの動作では、すべての着信不明ユーザがWindowsユーザなしにマッピングされます。そのため、NTFSセキュリティ形式にアクセスしようとする不明なUIDは認証に失敗します。通常、デフォルトのWindowsユーザを設定することは推奨されませんが、アプリケーションが正常に機能するために必要なユースケースがある場合があります。グローバルオプションであるため、分離されたSVMをこれらのアプリケーション専用にすることもできます。
-ntacl-display-permissive-perms*	このオプションは、などのコマンドの実行時に、NFSクライアント上のエンドユーザにNTFS形式の権限を表示する方法を制御します ls -la。 NFSはNTFSのセキュリティセマンティクスを認識しないため、クライアントではデフォルトで権限が777と表示されます。これにより、ユーザに対して不要なアラームが生成されます（NTFS ACL /ネームマッピングが権限を制御するため）。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が中断される可能性もあります。- 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権限の概算を送信し、共有にアクセスするユーザが実行できる処理と実行できない処理をより正確に示します。
-v3-ms-dos-client	このオプションを指定すると、SVMでWindows NFSを使用できるかどうかが有効になります。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。ここでのマルチプロトコルNASへの影響は、Windows NFS構成（サーバへの名前/グループの表示方法など）によって異なりますが、Windows NFSに適用される一般的なルールは、通常のNFSクライアントと同じです。
-ignore-nt-acl-for-root*	このオプションは、NTFSセキュリティ形式のボリュームでのNFS内のrootユーザの動作を制御します。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。つまり、NTFS権限のネゴシエートを行うには、他のNFSユーザと同様に、rootユーザを有効なWindowsユーザにマッピングする必要があります。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フル読み取り/書き込みアクセス権を持つUNIX形式のrootユーザのように機能します。このオプションは注意して使用してください。

オプション	マルチフロトコルNASニヨエルエイキヨウ
-cached-cred-positive-ttl*	このオプションは、NAS環境でキャッシュ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。ユーザのクレデンシャルの照会に成功すると、ONTAPによってクレデンシャルがキャッシュされ、ネームサービスへの接続が必要になる回数が削減されます。デフォルトのタイムアウト値は86、400、000ミリ秒で、24時間になります。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可能性があります。これは、キャッシュが24時間経過するか、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とLDAPの関係の詳細については、TR-4835を参照してください。
-cached-cred-negative-ttl*	このオプションは、拒否アクセスがあることが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の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可能性があります。これは、キャッシュが24時間経過するか、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とLDAPの関係の詳細については、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書き込み呼び出しで権限チェックをスキップ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。 **注** ：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、読み取り専用ファイルへの書き込みを試みた場合、処理は成功します。デフォルト設定はdisabledです。
-v4-inherited-acl-preserve*	NFSv4 ACLを使用する場合、このオプションでは、親ディレクトリモードビットがNFSv4 ACLの継承を無視するかどうかを指定します。デフォルトでは、このオプションは無効になっており、作成されたファイルは継承された親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します。これはRFC 5661で想定されている動作です。ただし、代わりにACLの継承が必要な場合は、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をキャッシュに保持す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が、それらのクレデンシャルを使用するためにシステムに戻らなかった場合、ONTAPは、ハーベストタイムアウト値の期限が切れると、そのエントリを削除します。これは、古いエントリのキャッシュに不要なメモリを使用しないためです。デフォルトのタイムアウト値は86、400、000（24時間）です。ONTAPでのネームサービスとキャッシュの動作については、TR-4668を参照してください。LDAPに関連するこれらのオプションについても、TR-4835で説明しています。

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構成に役立つ一連の設定可能なオプションもあります。表9 に、ONTAP 9.8で使用できるCIFS / SMBオプションとその用途を示します。これらのオプションは、`cifs options modify` コマンドで制御します。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NASニヨエルエイキヨウ
`-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。デフォルトでは `pcuser`、このユーザはに設定され、ID 65534に対応します。 Windows / SMBクライアントが共有にファイルを作成し、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されている場合、ファイルに所有者が割り当てられ `pcuser` ます。詳細については、「認証とネームマッピング」のセクションを参照してください。 • NFSクライアントでは、通常65534が `nfsnobody` ユーザにマッピングされます。 そのため `pcuser`、/65534を所有者としてNFSのファイル/所有者のリストに表示されます。 `nfsnobody` NFSマウントでこの動作が表示される場合は、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の所有者に関係なく、Windowsアクセス権が引き続き適用されます。UNIXセキュリティ形式では、ファイル所有者をに設定する `pcuser` と問題が発生す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を許可または拒否します。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。この設定を使用すると、CIFS / SMBクライアントからファイルを実行するときに、実行がデフォルトで正しく機能するように設定する必要があるため、問題が発生する可能性があります。場合によっては、これらのファイルに対して実行を設定できないため、ONTAPには `read-grants-exec` 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では、ONTAPにワークグループモードを使用します。これは、ドメインコントローラ/Active Directoryを実装せずにCIFS / SMBアクセスを許可する方法です。 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。 このオプションはデフォルトで有効になっています。
`-is-local-users-and-groups-enabled`	CIFS / SMBサーバのローカル認証では、ONTAPにワークグループモードを使用します。これは、ドメインコントローラ/Active Directoryを実装せずにCIFS / SMBアクセスを許可する方法です。 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	マルチフロトコルNASニヨエルエイキヨウ
	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共有に対してエクスポートポリシーとルールを使用できます。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の名前/ IPアドレスを使用して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共有へのアクセスを制限するもう1つの方法は、共有レベルの権限と、name-mapping create 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です。 詳細については、「ユーザ名へのWindowsクライアントのマッピング」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アクセス権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権限の表示」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が確立されたドメインに存在し、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ている場合にファイルやディレクトリの削除が禁止されます。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の動作が適用されます。
-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、変換のために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、適切なPOIX/UNIXセキュリティを表示できます。これは、ONTAPがサポートしていない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、「Network File System（NFS）およびSMB / CIFSのファイル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。これにより、ユーザ名が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、「rootへのWindows管理者ユーザのマッピング」を参照してください。

オプション	マルチフロトコルNASニヨエルエイキヨウ
-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、Windows / SMBクライアントが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表示する方法を制御します。 有効な場合： • <JUNCTION> dir cmd内のコマンドを使用した場合、ジャンクションパスはと表示されます。 • エクスプローラで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。 無効になっている場合： • エクスプローラおよびcmdでは、SMBクライアントへのジャンクションパスが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受信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。着信する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。着信する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、システムで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のバージョンを制御します。デフォルトではSMB1に設定されていますが、SMB2とSMB3に対してこの動作を有効にすることができます。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 NFS Best Practices and Implementation Guide』
  https://www.netapp.com/us/media/tr-4067.pdf
- TR-4569：『Security Hardening Guide for ONTAP 9』
  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf
- TR-4571：『NetApp FlexGroup Volume 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-4616.pdf
- TR-4668：『Name Services Best Practices - NetApp ONTAP』
  https://www.netapp.com/us/media/tr-4668.pdf
- TR-4743：『FlexCache in ONTAP』
  https://www.netapp.com/pdf.html?item=/media/7336-tr4743pdf.pdf
- TR-4835：『How to Configure LDAP in NetApp ONTAP』
  https://www.netapp.com/media/19423-tr-4835.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製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp 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