NFSの管理
ONTAP 9

NetApp
January 23, 2026

目次

NFSの管理

NFSプロトコルのONTAPファイルアクセスについて学ぶ

ONTAPには、NFSプロトコルで利用できるファイル アクセス機能があります。NFSサーバを有効にして、ボリュームまたはqtreeをエクスポートできます。

ここで説明する手順は、次の状況で実行します。

- ONTAPのNFSプロトコル機能の範囲について理解する必要がある。
- NFSの基本的な設定ではなく、あまり一般的でない設定およびメンテナンス作業を実施する。
- System Managerや自動スクリプト ツールではなく、コマンドライン インターフェイス（CLI）を使用する必要がある。

NASファイル アクセスについて

ネームスペースとジャンクション ポイント

ONTAP NASのネームスペースとジャンクションポイントについて学ぶ

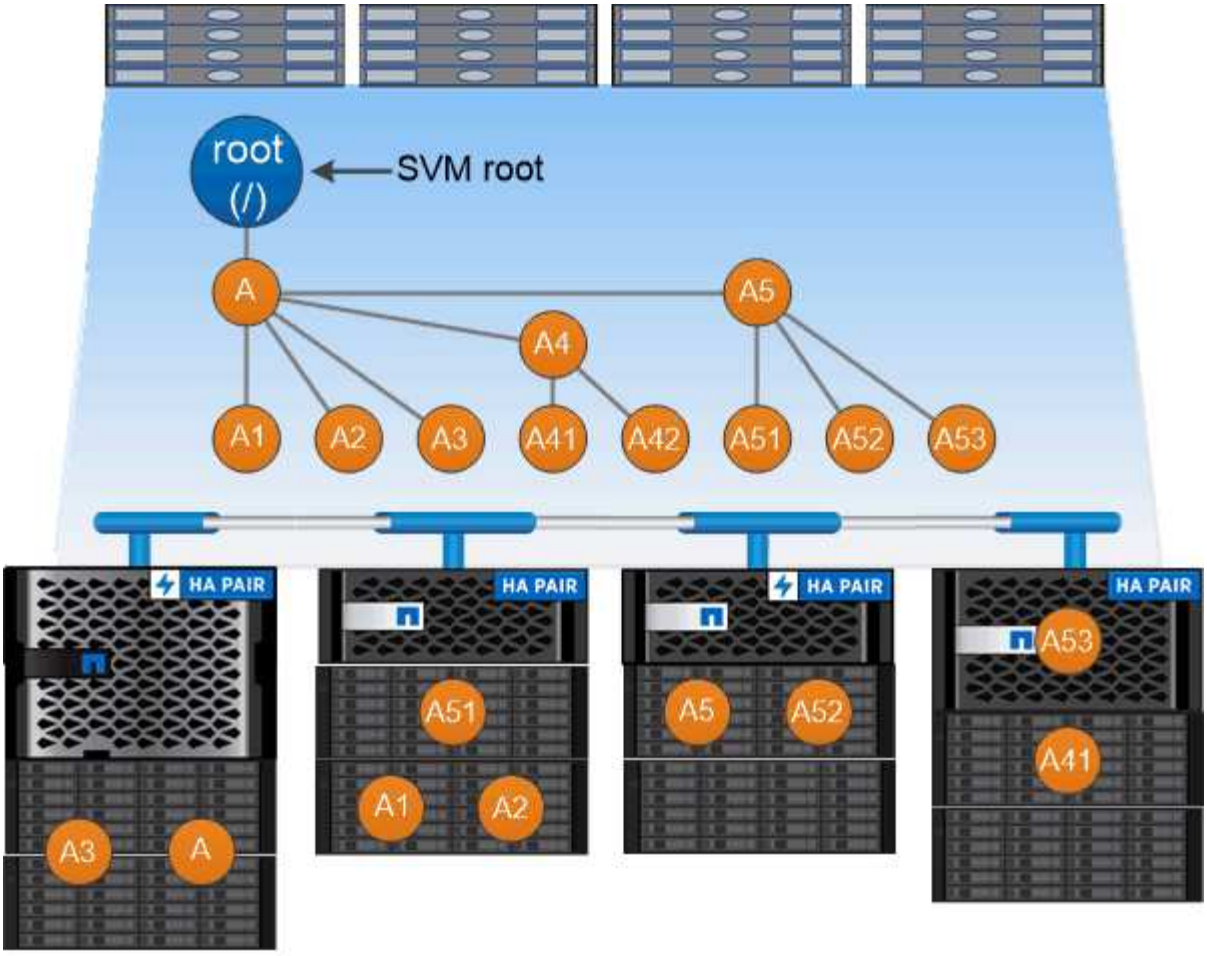
NAS ネームスペース とは、ジャンクション ポイント で結合されたボリュームの論理的なグループであり、単一のファイル システム階層を形成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定することなく、ネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームは、クラスタ内の任意の場所に配置できます。

NASクライアントは、対象となるファイルを含むすべてのボリュームをマウントするのではなく、NFSエクスポートをマウントするか、SMB共有にアクセスします。エクスポートまたは共有は、名前空間全体、または名前空間内の中間位置を表します。クライアントは、アクセス ポイントの下にマウントされたボリュームのみにアクセスします。

必要に応じて、名前空間にボリュームを追加できます。ジャンクションポイントは、親ボリュームジャンクションの直下、またはボリューム内のディレクトリに作成できます。「`vol3`」という名前のボリュームのボリュームジャンクションへのパスは `/vol1/vol2/vol3`、 `/vol1/dir2/vol3`、あるいは `/dir1/dir2/vol3`などです。このパスは_ジャンクションパス_と呼ばれます。

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

ノードの停止やフェイルオーバーが発生した場合でもデータが利用可能であることを保証するには、SVMルート ボリュームの_負荷共有ミラー_コピーを作成する必要があります。



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

例

次の例では、ジャンクション パスを持つ SVM vs1 上に「`home4`」という名前のボリュームを作成します `/eng/home`：

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

ONTAP NASネームスペース アーキテクチャについて学ぶ

SVMネームスペースを作成するときに使用できる一般的なNASネームスペース アーキテクチャがいくつかあります。ビジネス要件やワークフロー要件に合わせて、ネームスペース アーキテクチャを選択できます。

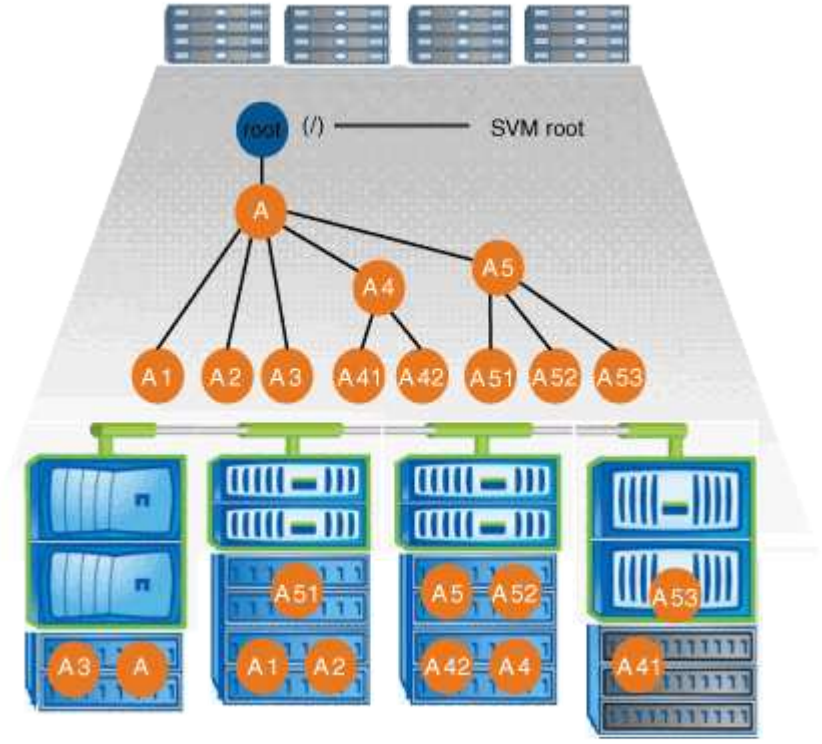
ネームスペースの最上位は常にルート ボリュームであり、スラッシュ（/）で表されます。ルートの下位のネームスペース アーキテクチャは以下の3つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクション ポイントを1つ備えた単一分岐ツリー

- ネームスペースのルートへのジャンクション ポイントを複数備えた複数分岐ツリー
- ボリュームごとにネームスペースのルートへの個別のジャンクション ポイントを備えた複数のスタンドアロン ボリューム

単一分岐ツリーを使用するネームスペース

単一分岐ツリーを使用するアーキテクチャには、SVMネームスペースのルートへの挿入ポイントが1つあります。単一の挿入ポイントは、ジャンクションされたボリュームまたはルートの下のディレクトリのどちらかです。それ以外のすべてのボリュームは、単一の挿入ポイントの下のジャンクション ポイント（ボリュームまたはディレクトリ）でマウントされます。

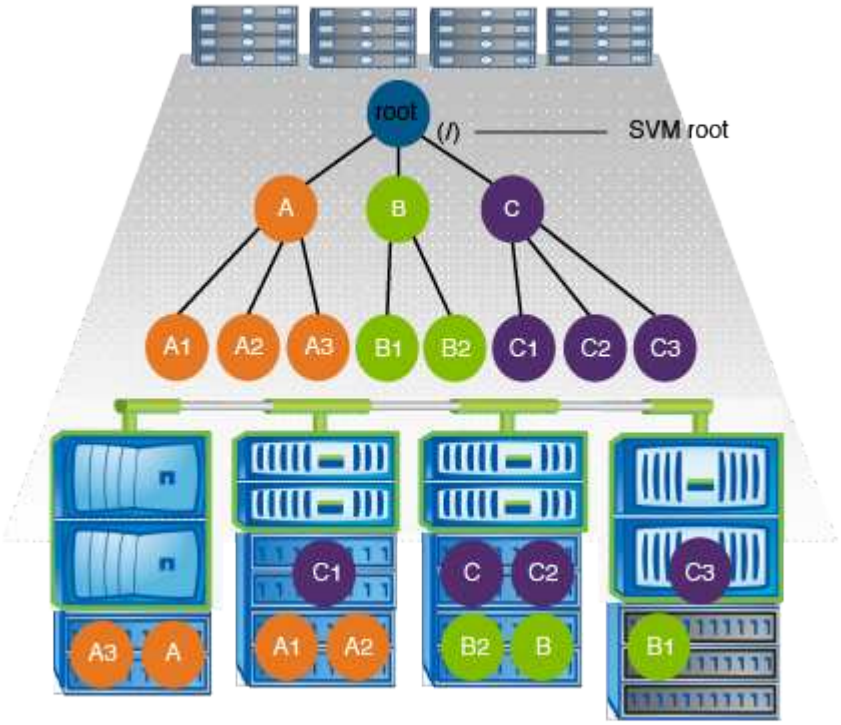


たとえば、上記の名前空間アーキテクチャを使用した一般的なボリューム ジャンクション構成は、次の構成のようになります。この構成では、すべてのボリュームが単一の挿入ポイント（「`data`」という名前のディレクトリ）の下にジャンクションされます：

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

複数分岐ツリーを使用するネームスペース

複数分岐ツリーを使用するアーキテクチャには、SVMネームスペースのルートへの挿入ポイントが複数あります。挿入ポイントは、ルート直下にジャンクションされたボリュームまたはディレクトリのどちらかです。それ以外のすべてのボリュームは、単一の挿入ポイントの下のジャンクション ポイント（ボリュームまたはディレクトリ）でマウントされます。

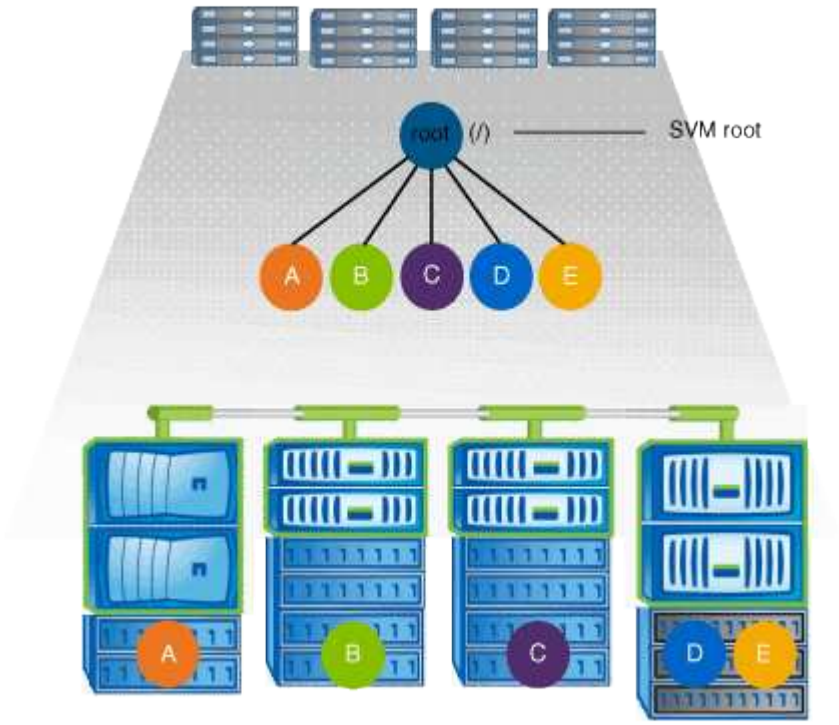


例えば、上記の名前空間アーキテクチャを持つ典型的なボリューム ジャンクション構成は、SVMのルート ボリュームへの挿入ポイントが3つある次の構成のようになります。2つの挿入ポイントは「`data`」と「`projects`」という名前のディレクトリです。1つの挿入ポイントは「`audit`」という名前のジャンクション ボリュームです：

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

複数のスタンドアロン ボリュームを使用するネームスペース

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



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

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

ONTAPによるファイル アクセスの制御方法

ONTAP NAS ファイル アクセス制御について学ぶ

ONTAPは、指定した認証ベースおよびファイルベースの制限に従ってファイルへのアクセスを制御します。

クライアントがストレージ システムに接続してファイルにアクセスする場合、 ONTAP は次の 2 つのタスクを実行する必要があります：

- 認証

  ONTAPは、信頼できるソースでIDを検証することにより、クライアントを認証する必要があります。さらに、クライアントの認証タイプは、エクスポートポリシー（CIFSの場合はオプション）の設定時にクライアントがデータにアクセスできるかどうかを判断する際に使用できる方法の1つです。

- 許可

  ONTAPは、ユーザの認証情報とファイルまたはディレクトリに設定されている権限を比較し、提供するアクセスの種類（ある場合）を決定することで、ユーザを承認する必要があります。

ファイル アクセス制御を適切に管理するには、ONTAP は NIS、LDAP、Active Directory サーバなどの外部サービスと通信する必要があります。CIFS または NFS を使用してファイル アクセス用にストレージ システムを設定するには、ONTAP で環境に応じて適切なサービスをセットアップする必要があります。

ONTAP NAS SVMの認証ベースの制限について学習します

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

ONTAP は、UNIX サーバと Windows サーバの両方からの Kerberos 認証をサポートしています。

ONTAP NAS SVMのファイルベースの制限について学習します

ONTAPは、SVM上のファイルとディレクトリに対して要求されたアクションを実行する権限がエンティティに与えられているかどうかを判断するために、3つのセキュリティレベルを評価します。アクセスは、3つのセキュリティレベルの評価後に有効な権限によっ

て決定されます。

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

- エクスポート（NFS）および共有（SMB）セキュリティ

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

- ストレージレベルのアクセス保護ファイルおよびディレクトリ セキュリティ

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

  > NFS または SMB クライアントからファイルまたはディレクトリのセキュリティ設定を表示すると、Storage-Level Access Guard セキュリティは表示されません。Storage-Level Access Guard セキュリティは、システム管理者（Windows または UNIX）であっても、クライアントから取り消すことはできません。

- NTFS、UNIX、およびNFSv4のネイティブのファイルレベルのセキュリティ

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

ONTAPによるNFSクライアント認証の処理

NASクライアントのONTAP認証について学ぶ

NFSクライアントからSVM上のデータにアクセスするためには、NFSクライアントが正しく認証されている必要があります。ONTAPでは、UNIXクレデンシャルを設定されたネーム サービスに照らしてチェックすることで、そのクライアントを認証します。

NFSクライアントがSVMに接続すると、ONTAPは、SVMのネーム サービス設定に応じて複数のネーム サービスをチェックし、そのユーザのUNIXクレデンシャルを取得します。ONTAPでチェックできるのは、ローカルのUNIXアカウント、NISドメイン、およびLDAPドメインのクレデンシャルです。ONTAPがユーザを認証できるように、このうちの少なくとも1つを設定しておく必要があります。複数のネーム サービスと検索順序を指定できます。

UNIXのボリューム セキュリティ形式のみを使用するNFS環境の場合、この設定だけでNFSクライアントから接続するユーザが認証され、適切なファイル アクセスが提供されます。

ボリュームのセキュリティ形式がmixed、NTFS、またはunifiedの場合、ONTAPがUNIXユーザをWindowsドメイン コントローラで認証するためにはSMBユーザ名を取得する必要があります。そのためには、ローカルのUNIXアカウントまたはLDAPドメインを使用して個々のユーザをマッピングするか、代わりにデフォルトのSMBユーザを使用します。ONTAPが検索するネーム サービスの種類と検索順序を指定するか、またはデフォルトのSMBユーザを指定します。

ONTAPがネーム サービスを使用する方法を学ぶ

ONTAPは、ネーム サービスを使用してユーザやクライアントに関する情報を取得します。ONTAPは、ストレージ システム上でデータにアクセスしたりストレージ システムを管理したりするユーザの認証や、混在環境でのユーザ クレデンシャルのマッピングを行うために、この情報を使用します。

ストレージ システムを設定する際に、ONTAPが認証用のユーザ クレデンシャルを取得するために使用するネーム サービスを指定する必要があります。ONTAPでは、次のネーム サービスをサポートしています。

- ローカル ユーザ（ファイル）
- 外部NISドメイン（NIS）
- 外部LDAPドメイン（LDAP）

> `vserver services name-service ns-switch`コマンドファミリを使用して、SVMにネットワーク情報の検索元と検索順序を設定します。これらのコマンドは、UNIXシステムの `/etc/nsswitch.conf`ファイルと同等の機能を提供します。

NFSクライアントがSVMに接続すると、ONTAPは指定されたネーム サービスをチェックし、ユーザのUNIXクレデンシャルを取得します。ネーム サービスが正しく設定され、ONTAPがUNIXクレデンシャルを取得できる場合、ONTAPはユーザを正常に認証します。

mixedセキュリティ形式の環境では、ONTAPによるユーザ クレデンシャルのマッピングが必要になる場合があります。ONTAPがユーザ クレデンシャルを適切にマッピングできるようにするには、環境のネーム サービスを適切に設定する必要があります。

ONTAPは、SVM管理者アカウントの認証にもネーム サービスを使用します。ネーム サービス スイッチを設定または変更する際は、SVM管理者アカウントの認証を誤って無効にしないように、この点に留意する必要があります。SVM管理ユーザの詳細については、"管理者認証とRBAC"を参照してください。

NFSクライアントからONTAP SMBファイルへのアクセスを許可する

ONTAPは、Windows NT File System（NTFS）セキュリティ セマンティクスを使用して、NFSクライアント上のUNIXユーザがNTFS権限を持つファイルにアクセスできるかどうかを判断します。

ONTAPでは、ユーザのUNIXユーザID（UID）から変換されたSMBクレデンシャルを使用して、ファイルに対するユーザのアクセス権の有無が確認されます。SMBクレデンシャルは、通常はユーザのWindowsユーザ名であるプライマリ セキュリティID（SID）と、ユーザがメンバーとなっているWindowsグループに対応する1つ以上のグループSIDで構成されています。

ONTAPでUNIX UIDをSMBクレデンシャルへ変換するときに要する時間は、数十ミリ秒から数百ミリ秒です。これは、この変換処理にドメイン コントローラへの問い合わせも含まれるためです。ONTAPではUIDがSMBクレデンシャルにマッピングされます。このマッピングはクレデンシャル キャッシュ内に入力されるので、変換によって発生する照合時間が短縮されます。

ONTAP NFS認証情報キャッシュの仕組み

NFSユーザーがストレージシステム上のNFSエクスポートへのアクセスを要求すると、ONTAPはユーザーを認証するために、外部ネームサーバまたはローカルファイルからユーザークレデンシャルを取得する必要があります。その後、ONTAPはこれらのクレデンシャルを内部クレデンシャルキャッシュに保存し、後で参照できるようにします。NFSクレデンシャルキャッシュの仕組みを理解することで、潜在的なパフォーマンスやアクセスの問題に対処できるようになります。

認証情報キャッシュがなければ、 ONTAP は NFS ユーザーがアクセスを要求するたびにネーム サービスにクエリを実行する必要があります。多くのユーザーがアクセスする高負荷のストレージ システムでは、これはすぐに深刻なパフォーマンス問題につながり、不要な遅延や NFS クライアント アクセスの拒否を引き起こす可能性があります。

クレデンシャル キャッシュを使用すると、ONTAPはユーザー クレデンシャルを取得し、NFSクライアントが別の要求を送信した場合に迅速かつ容易にアクセスできるように、所定の時間保存します。この方法には、次のような利点があります：

- 外部ネーム サーバー（NIS や LDAP など）への要求の処理が少なくなるため、ストレージ システムの負荷が軽減されます。
- 外部ネーム サーバーに送信するリクエストの数を減らすことで、外部ネーム サーバーの負荷を軽減します。
- ユーザを認証するために外部ソースからクレデンシャルを取得する待機時間をなくすことで、ユーザ アクセスのスピードが向上します。

ONTAPは、認証情報キャッシュに肯定的認証情報と否定的認証情報の両方を保存します。肯定的認証情報は、ユーザが認証されアクセスが許可されたことを意味します。否定的認証情報は、ユーザが認証されずアクセスが拒否されたことを意味します。

デフォルトでは、ONTAPはポジティブクレデンシャルを24時間保存します。つまり、ユーザを最初に認証した後、ONTAPは24時間、そのユーザによるアクセス要求に対してキャッシュされたクレデンシャルを使用します。ユーザが24時間後にアクセスを要求した場合、このサイクルが最初から開始されます。ONTAPはキャッシュされたクレデンシャルを破棄し、適切なネーム サービス ソースから再度クレデンシャルを取得します。過去24時間以内にネーム サーバ上でクレデンシャルが変更された場合、ONTAPは更新されたクレデンシャルをキャッシュし、次の24時間で使用します。

デフォルトでは、ONTAPはネガティブクレデンシャルを2時間保存します。つまり、最初にユーザのアクセスを拒否した後、ONTAPはそのユーザからのアクセス要求を2時間拒否し続けます。2時間経過後にユーザがアクセスを要求した場合、このサイクルが最初から開始されます。ONTAPは適切なネーム サービス ソースからクレデンシャルを再度取得します。過去2時間以内にネーム サーバ上でクレデンシャルが変更された場合、ONTAPは更新されたクレデンシャルをキャッシュし、次の2時間使用します。

NASネームスペース内でのデータ ボリュームの作成と管理

指定されたジャンクションポイントを持つONTAP NASボリュームを作成する

データ ボリュームを作成するときは、ジャンクション ポイントを指定できます。作成したボリュームは、ジャンクション ポイントに自動的にマウントされ、NASアクセス用の設定にすぐに使用できます。

開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティトラッキングを有効にしたボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、 `-analytics-state`または `-activity-tracking-state`を `on`に設定した `volume create`コマンドを発行します。

  容量分析とアクティビティ追跡の詳細については、 "ファイルシステム分析の有効化"を参照してください。"ONTAPコマンド リファレンス"の `volume create`の詳細を確認してください。

次の文字はジャンクションパスでは使用できません： `* # " > < | ? \`

また、ジャンクション パスの長さは255文字以下にする必要があります。

手順

1. ジャンクション ポイントを設定してボリュームを作成します。

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

   ジャンクション パスはルート（/）で始まる必要があり、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクション パスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は省略可能です。セキュリティ形式を指定しない場合、Storage Virtual Machine（SVM）のルート ボリュームと同じセキュリティ形式を使用してボリュームが作成されます。ただし、ルート ボリュームのセキュリティ形式が、作成するデータ ボリュームには適切でないセキュリティ形式である場合もあります。解決が困難なファイル アクセスの問題ができるだけ発生しないように、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   ジャンクションパスは大文字と小文字が区別されません。 `/ENG`は `/eng`と同じです。CIFS共有を作成すると、Windowsはジャンクションパスを大文字と小文字が区別されるものとして扱います。例えば、ジャンクションが `/ENG`の場合、SMB共有のパスは `/ENG`で始まる必要があり、 `/eng`ではありません。

   データボリュームをカスタマイズするために使用できるオプションパラメータは多数あります。"ONTAPコマンド リファレンス"の `volume create`の詳細をご覧ください。

2. 目的のジャンクション ポイントでボリュームが作成されたことを確認します。

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

例

次の例では、ジャンクション パス `/eng/home`を持つSVM vs1上に `home4`という名前のボリュームを作成します：

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

特定のジャンクションポイントなしで**ONTAP NAS**ボリュームを作成する

ジャンクション ポイントを指定せずにデータ ボリュームを作成できます。作成したボリュームは、自動的にはマウントされず、NASアクセス用の設定に使用することはできません。このボリュームに対してSMB共有またはNFSエクスポートを設定するには、まず、ボリュームをマウントする必要があります。

開始する前に

- ボリュームを作成するアグリゲートがすでに存在している必要があります。
- ONTAP 9.13.1以降では、容量分析とアクティビティトラッキングを有効にしたボリュームを作成できます。容量またはアクティビティトラッキングを有効にするには、 `-analytics-state`または `-activity-tracking-state`を `on`に設定した `volume create`コマンドを発行します。

  容量分析とアクティビティ追跡の詳細については、 "ファイルシステム分析の有効化"を参照してください。"ONTAPコマンド リファレンス"の `volume create`の詳細を確認してください。

手順

1. 次のコマンドを使用して、ジャンクション ポイントが設定されていないボリュームを作成します。

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   ボリュームのセキュリティ形式の指定は省略可能です。セキュリティ形式を指定しない場合、Storage Virtual Machine（SVM）のルート ボリュームと同じセキュリティ形式を使用してボリュームが作成されます。ただし、ルート ボリュームのセキュリティ形式が、データ ボリュームには適切でないセキュリティ形式である場合もあります。解決が困難なファイル アクセスの問題ができるだけ発生しないように、ボリュームの作成時にセキュリティ形式を指定することを推奨します。

   データボリュームをカスタマイズするために使用できるオプションパラメータは多数あります。"ONTAPコマンド リファレンス"の `volume create`の詳細をご覧ください。

2. ジャンクション ポイントが設定されていないボリュームが作成されたことを確認します。

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

例

次の例では、ジャンクション ポイントにマウントされていない SVM vs1 上に「sales」という名前のボリュームを作成します：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

NASネームスペースでONTAP NFSボリュームをマウントまたはアンマウントする

Storage Virtual Machine（SVM）ボリュームに含まれているデータに対するNASクライアントのアクセスを設定するには、ボリュームがNASネームスペースにマウントされている必要があります。現在マウントされていないボリュームであれば、そのボリュームをジャンクション ポイントにマウントできます。また、ボリュームはアンマウントすることもできます。

タスク概要

ボリュームをアンマウントし、オフラインにすると、アンマウントしたボリュームのネームスペース内に含まれたジャンクション ポイントのあるボリューム内のデータも含め、ジャンクション ポイント内のすべてのデータに、NASクライアントからアクセスできなくなります。

> NASクライアントからボリュームへのアクセスを切断するには、ボリュームをアンマウントするだけでは不十分です。ボリュームをオフラインにするか、または他の手順でクライアント側のファイル ハンドル キャッシュを確実に無効にする必要があります。詳細については、次の技術情報アーティクルを参照してください。
>
> "NFSv3クライアントは、ONTAPでネームスペースから削除された後も、ボリュームにアクセスできます"

ボリュームをアンマウントし、オフラインにしても、ボリューム内のデータは失われません。また、既存のボリューム エクスポート ポリシーおよびボリュームまたはディレクトリ上に作成されたSMB共有、およびアンマウントされたボリューム内のジャンクション ポイントは保持されます。アンマウントしたボリュームを再マウントすれば、NASは、既存のエクスポート ポリシーとSMB共有を使用してボリューム内のデータにアクセスできるようになります。

手順

1. 次のうち必要な操作を実行します。

状況	入力するコマンド
ボリュームのマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

ボリュームをアンマウントする	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. ボリュームが目的のマウント状態になっていることを確認します。

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

例

次の例では、SVM「vs1」にある「sales」という名前のボリュームをジャンクションポイント「/sales」にマウントします：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

次の例では、SVM “vs1” にある “data” という名前のボリュームをアンマウントしてオフラインにします：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

ONTAP NASボリュームのマウントとジャンクションポイントの情報を表示します

Storage Virtual Machine（SVM）のマウント ボリューム、およびボリュームがマウントされているジャンクション ポイントに関する情報を表示できます。また、ジャンクション ポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、SVMネームスペースを理解し、管理することができます。

手順

1. 次のうち必要な操作を実行します。

表示したい場合…	コマンドを入力してください…
SVMのマウントされたボリュームとマウントされていないボリュームに関する概要情報	`volume show -vserver vserver_name -junction`
SVMのマウントされたボリュームとマウントされていないボリュームに関する詳細情報	`volume show -vserver vserver_name -volume volume_name -instance`
SVMのマウントされたボリュームとマウントされていないボリュームに関する特定の情報	a. 必要に応じて、 `-fields`パラメータの有効なフィールドを次のコマンドを使用して表示できます： `volume show -fields ?` b. `-fields`パラメータを使用して、必要な情報を表示します： `volume show -vserver vserver_name -fields fieldname,…`

例

次の例は、SVM vs1のマウントされたボリュームとマウントされていないボリュームの概要を表示します。

```
cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

次の例は、SVM vs2上に配置されたボリュームの指定したフィールドに関する情報を表示します。

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

セキュリティ形式の設定

セキュリティ形式がデータ アクセスに与える影響

ONTAP NASのセキュリティ スタイルについて学ぶ

セキュリティ形式には、UNIX、NTFS、mixed、unifiedの4種類があります。各セキュリティ形式は、データに対する権限の処理方法にそれぞれ異なる影響を与えます。目的に応じて適切なセキュリティ形式を選択するには、それぞれの影響を理解する必要があります。

セキュリティ形式はデータにアクセスできるクライアントの種類には影響しないことに注意してください。セキュリティ形式で決まるのは、データ アクセスの制御にONTAPで使用される権限の種類と、それらの権限を変更できるクライアントの種類だけです。

たとえば、ボリュームでUNIXセキュリティ形式を使用している場合でも、ONTAPはマルチプロトコルに対応しているため、SMBクライアントから引き続きデータにアクセスできます（認証と許可が適切な場合）。ただし、ONTAPでは、UNIXクライアントのみが標準のツールを使用して変更できるUNIX権限が使用されます。

セキュリティ形式	権限を変更できるクライアント	クライアントが使用できる権限	結果として得られる実効セキュリティ形式	ファイルにアクセスできるクライアント
UNIX	NFS	NFSv3モード ビット	UNIX	NFSとSMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
混合	NFSまたはSMB	NFSv3モード ビット	UNIX	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
Unified（ONTAP 9.4以前のリリースでは、無限ボリュームのみ）	NFSまたはSMB	NFSv3モード ビット	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVolでは、UNIX、NTFS、およびmixedのセキュリティ形式がサポートされます。セキュリティ形式がmixedまたはunifiedの場合は、ユーザがセキュリティ形式を各自設定するため、権限を最後に変更したクライアントの種類によって有効になる権限が異なります。権限を最後に変更したクライアントがNFSv3クライアントの場合、権限はUNIX NFSv3モード ビットになります。最後のクライアントがNFSv4クライアントの場合、権限はNFSv4 ACLになります。最後のクライアントがSMBクライアントの場合、権限はWindows NTFS ACLになります。

unifiedセキュリティ形式は、ONTAP 9.5以降のリリースではサポートされなくなった無限ボリュームでのみ使用できます。詳細については、FlexGroupボリューム管理の概要を参照してください。

`vserver security file-directory`コマンドの `show-effective-permissions`パラメータを使用すると、指定したファイルまたはフォルダのパスに対してWindowsまたはUNIXユーザーに付与されている有効な権限を表示できます。さらに、オプションのパラメータ `-share-name`
を使用すると、有効な共有権限を表示できます。link:https://docs.netapp.com/us-en/ontap-cli/vserver-security-file-directory-show-effective-permissions.html["ONTAPコマンド リファレンス"^]の `vserver security file-directory show-effective-permissions`の詳細をご覧ください。

ONTAPで、最初にデフォルトのファイル権限がいくつか設定されます。デフォルトでは、UNIX、mixed、およびunifiedのセキュリティ形式のボリュームにあるデータについては、セキュリティ形式はUNIX、権限の種類はUNIXモード ビット（特に指定しないかぎり0755）が有効になります。これは、デフォルトのセキュリティ形式で許可されたクライアントで設定するまで変わりません。同様に、NTFSセキュリティ形式のボリュームにあるデータについては、デフォルトでNTFSセキュリティ形式が有効になり、すべてのユーザにフル コントロール権限を許可するACLが割り当てられます。

関連情報

- "ONTAPコマンド リファレンス"

ONTAP NFS FlexVol ボリュームのセキュリティ スタイルについて学ぶ

セキュリティ形式は、FlexVol volume（ルート ボリュームまたはデータ ボリュームの両方）およびqtreeに設定できます。セキュリティ形式は、作成時に手動で設定したり、自動的に継承したり、後で変更したりできます。

ONTAP NAS SVMで使用するセキュリティスタイルを決定する

ボリュームで使用するセキュリティ形式を決定するには、2つの要素を考慮する必要があります。第1の要素は、ファイルシステムの管理者のタイプで、第2の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定する際は、最適なセキュリティ形式を選択してアクセス権の管理に関する問題を回避するために、環境のニーズを考慮する必要があります。決定時には以下を考慮すると役立ちます。

セキュリティ形式	次の場合に選択…
UNIX	• ファイルシステムがUNIX管理者によって管理される。 • ユーザの大半がNFSクライアントである。 • データにアクセスするアプリケーションで、サービス アカウントとしてUNIXユーザが使用される。
NTFS	• ファイルシステムがWindows管理者によって管理される。 • ユーザの大半がSMBクライアントである。 • データにアクセスするアプリケーションで、サービス アカウントとしてWindowsユーザが使用される。
混合	• ファイルシステムがUNIX管理者とWindows管理者の両方によって管理され、ユーザがNFSクライアントとSMBクライアントの両方で構成される。

ONTAP NFSセキュリティ形式の継承について

新しいFlexVolボリュームまたはqtreeの作成時にセキュリティ スタイルを指定しない場合、そのセキュリティ スタイルがさまざまな方法で継承されます。

セキュリティ スタイルは次のように継承されます：

- FlexVol volumeは、それを含むSVMのルート ボリュームのセキュリティ スタイルを継承します。
- qtreeは、それを含むFlexVol volumeのセキュリティ スタイルを継承します。
- ファイルまたはディレクトリは、それを含むFlexVolボリュームまたはqtreeのセキュリティ形式を継承します。

ONTAP NFS UNIX権限の保持について学ぶ

現在 UNIX 権限を持つFlexVolボリューム内のファイルが Windows アプリケーションに

よって編集および保存されると、ONTAP は UNIX 権限を保持できます。

Windows クライアント上のアプリケーションがファイルを編集して保存する場合、ファイルのセキュリティプロパティを読み取り、新しい一時ファイルを作成し、それらのプロパティを一時ファイルに適用して、一時ファイルに元のファイル名を付けます。

Windowsクライアントがセキュリティプロパティのクエリを実行すると、UNIX権限を正確に表す構築済みACLが返されます。この構築済みACLの唯一の目的は、Windowsアプリケーションによってファイルが更新されてもファイルのUNIX権限を保持し、更新後のファイルに同じUNIX権限が付与されるようにすることです。ONTAPは、構築済みACLを使用してNTFS ACLを設定することはありません。

Windows セキュリティ タブを使用して **ONTAP NFS SVM**の **UNIX** 権限を管理する

SVM上の混合セキュリティ形式のボリュームまたはqtree内のファイルまたはフォルダのUNIX権限を操作する場合は、Windowsクライアントの[セキュリティ]タブを使用できます。または、Windows ACLを照会および設定できるアプリケーションを使用することもできます。

- UNIX権限の変更

  Windowsの「セキュリティ」タブを使用して、混合セキュリティ形式のボリュームまたはqtreeのUNIX権限を表示および変更できます。Windowsのメインの「セキュリティ」タブを使用してUNIX権限を変更する場合は、変更を加える前に、編集する既存のACEを削除する必要があります（これにより、モードビットが0に設定されます）。または、詳細エディタを使用して権限を変更することもできます。

  モード権限を使用する場合、リストされているUID、GID、その他（コンピューターにアカウントを持つ他のすべてのユーザー）のモード権限を直接変更できます。例えば、表示されているUIDにr-x権限がある場合、UID権限をrwxに変更できます。

- UNIX 権限から NTFS 権限への変更

  Windows セキュリティ タブを使用すると、ファイルとフォルダに UNIX 対応のセキュリティ スタイルが設定されている、混合セキュリティ スタイルのボリュームまたは qtree 上で、UNIX セキュリティ オブジェクトを Windows セキュリティ オブジェクトに置き換えることができます。

  必要なWindowsユーザおよびグループオブジェクトに置き換える前に、まずリストされているすべてのUNIX権限エントリを削除する必要があります。その後、WindowsユーザおよびグループオブジェクトにNTFSベースのACLを設定できます。すべてのUNIXセキュリティオブジェクトを削除し、混合セキュリティ形式のボリュームまたはqtreeのファイルまたはフォルダにWindowsユーザおよびグループのみを追加することで、ファイルまたはフォルダの有効なセキュリティ形式がUNIXからNTFSに変更されます。

  フォルダの権限を変更すると、Windowsのデフォルトの動作では、これらの変更がすべてのサブフォルダとファイルに反映されます。したがって、セキュリティスタイルの変更をすべての子フォルダ、サブフォルダ、およびファイルに反映させたくない場合は、反映方法を適切な設定に変更する必要があります。

ONTAP NFS SVMルートボリュームのセキュリティスタイルを設定する

Storage Virtual Machine（SVM）のルート ボリューム上のデータに使用するアクセス権のタイプを決定するには、SVMルート ボリュームのセキュリティ形式を設定します。

手順

1. `vserver create`コマンドに `-rootvolume-security-style`パラメータを指定して、セキュリティ形式を定義します。

   ルート ボリュームのセキュリティ スタイルに使用できるオプションは `unix`、 `ntfs`、または `mixed`です。

2. 作成した SVM のルート ボリューム セキュリティ スタイルを含む設定を表示して確認します：

   ```
   vserver show -vserver vserver_name
   ```

ONTAP NFS FlexVol ボリュームのセキュリティスタイルを設定する

Storage Virtual Machine（SVM）のFlexVol上のデータに使用するアクセス権のタイプを決定するには、FlexVolのセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVolボリュームが…	使用するコマンド
まだ存在しない	`volume create`を実行し、 `-security-style`パラメータを含めてセキュリティ形式を指定します。
すでに存在する	`volume modify`を実行し、 `-security-style`パラメータを含めてセキュリティ形式を指定します。

   FlexVol volumeのセキュリティ形式に使用できるオプションは `unix`、 `ntfs`、または `mixed`です。

   FlexVolの作成時にセキュリティ形式を指定しない場合、ボリュームはルート ボリュームのセキュリティ形式を継承します。

   > `volume create`または `volume modify`
   > コマンドの詳細については、`link:../volumes/index.html["論理ストレージ管理"]`を参照してください。

2. 作成したFlexVolのセキュリティ形式を含む設定を表示するには、次のコマンドを入力します。

   ```
   volume show -volume volume_name -instance
   ```

ONTAP NFS qtreeのセキュリティスタイルを設定する

qtree上のデータに使用するアクセス権のタイプを決定するには、qtreeのセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtreeが…	使用するコマンド
まだ存在しない	`volume qtree create`を実行し、 `-security-style`パラメータを含めてセキュリティ形式を指定します。
すでに存在する	`volume qtree modify`を実行し、 `-security-style`パラメータを含めてセキュリティ形式を指定します。

qtreeセキュリティ形式に使用できるオプションは `unix`、 `ntfs`、または `mixed`です。

qtreeの作成時にセキュリティ形式を指定しない場合、デフォルトのセキュリティ形式は `mixed`になります。

`volume qtree create`または `volume qtree modify`
コマンドの詳細については、`link:../volumes/index.html["論理ストレージ管理"]`を参照してください。

2. 作成した qtree のセキュリティ スタイルを含む設定を表示するには、次のコマンドを入力します。
`volume qtree show -qtree qtree_name -instance`

NFSを使用したファイル アクセスの設定

ONTAP SVMでのNFSファイル アクセスの設定について学習します

クライアントがNFSを使用してStorage Virtual Machine（SVM）上のファイルにアクセスできるようにするには、いくつかの手順を実行する必要があります。環境の現在の設定によっては、さらにいくつかの追加手順があります。

クライアントがNFSを使用してSVM上のファイルにアクセスできるようにするには、次の手順を実行する必要があります。

1. SVMでNFSプロトコルを有効にします。

   クライアントからのNFS経由のデータ アクセスを許可するようにSVMを設定する必要があります。

2. SVMにNFSサーバを作成します。

   NFSサーバは、NFS経由のファイル提供を可能にするSVM上の論理エンティティです、NFSサーバを作成し、許可するNFSプロトコルのバージョンを指定する必要があります。

3. SVMにエクスポート ポリシーを設定します。

   エクスポート ポリシーを設定して、クライアントがボリュームとqtreeを使用できるようにする必要があります。

4. ネットワークおよびストレージの環境に応じて、適切なセキュリティおよびその他の設定を使用してNFSサーバを設定します。

この手順には、Kerberos、LDAP、NIS、ネーム マッピング、ローカル ユーザの設定が含まれます。

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポート ポリシーが **ONTAP NFS** ボリュームまたは **qtree** へのクライアント アクセスを制御する方法

エクスポート ポリシーには、各クライアントのアクセス要求を処理する 1 つ以上の_エクスポート ルール_が含まれます。この処理の結果に基づいて、クライアントのアクセスが拒否されるか許可されるか、またアクセス レベルが決定されます。クライアントがデータにアクセスするには、Storage Virtual Machine（SVM）上にエクスポート ルールを含むエクスポート ポリシーが存在している必要があります。

ボリュームまたはqtreeごとに1つのエクスポート ポリシーを関連付けて、ボリュームまたはqtreeへのクライアント アクセスを設定します。SVMには複数のエクスポート ポリシーを含めることができます。これにより、複数のボリュームまたはqtreeを持つSVMで次の操作が可能になります：

- SVM 内の各ボリュームまたは qtree への個別のクライアント アクセスを制御するために、SVM の各ボリュームまたは qtree に異なるエクスポート ポリシーを割り当てます。
- 各ボリュームまたはqtreeに新しいエクスポート ポリシーを作成することなく、同一のクライアント アクセス制御を行うために、SVMの複数のボリュームまたはqtreeに同じエクスポート ポリシーを割り当てます。

クライアントが適用可能なエクスポート ポリシーで許可されていないアクセス要求を行った場合、その要求は失敗し、権限拒否メッセージが返されます。クライアントがエクスポート ポリシーのどのルールにも一致しない場合、アクセスは拒否されます。エクスポート ポリシーが空の場合、すべてのアクセスは暗黙的に拒否されます。

ONTAP を実行しているシステムでエクスポート ポリシーを動的に変更できます。

ONTAP NFS SVMのデフォルトのエクスポートポリシー

各SVMには、ルールを含まないデフォルトのエクスポートポリシーがあります。クライアントがSVM上のデータにアクセスするには、ルールを含むエクスポートポリシーが存在している必要があります。SVMに含まれる各FlexVolボリュームには、エクスポートポリシーが関連付けられている必要があります。

SVMを作成すると、ストレージシステムは `default`というデフォルトのエクスポートポリシーをSVMのルートボリューム用に自動的に作成します。クライアントがSVM上のデータにアクセスする前に、デフォルトのエクスポートポリシーに1つ以上のルールを作成する必要があります。または、ルールを含むカスタムエクスポートポリシーを作成することもできます。デフォルトのエクスポートポリシーは変更したり名前を変更したりできますが、削除することはできません。

FlexVolボリュームをそのSVMに作成すると、ストレージシステムによってボリュームが作成され、そのSVMのルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。デフォルトでは、SVMに作成された各ボリュームには、ルートボリュームのデフォルトのエクスポートポリシーが関連付けられます。SVMに含まれるすべてのボリュームにデフォルトのエクスポートポリシーを使用することも、ボリュームごとに固有のエクスポートポリシーを作成することもできます。複数のボリュームに同じエクスポートポリシーを関連付けることもできます。

エクスポート ルールは、エクスポート ポリシーの機能要素です。エクスポート ルールは、ボリュームへのクライアント アクセス要求を、ユーザーが設定した特定のパラメータと照合し、クライアント アクセス要求の処理方法を決定します。

エクスポート ポリシーには、クライアントにアクセスを許可するエクスポート ルールを少なくとも1つ含める必要があります。エクスポート ポリシーに複数のルールが含まれている場合、ルールはエクスポート ポリシーに表示される順に処理されます。ルールの順序は、ルール インデックス番号によって決まります。ルールがクライアントに一致すると、そのルールのアクセス権が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

次の条件を使用して、クライアントのアクセス権を決定するようにエクスポート ルールを設定できます。

- クライアントが要求の送信に使用するファイル アクセス プロトコル（NFSv4やSMBなど）
- クライアント識別子（ホスト名やIPアドレスなど）

  `-clientmatch`フィールドの最大サイズは4096文字です。

- クライアントが認証に使用するセキュリティ タイプ（Kerberos v5、NTLM、AUTH_SYSなど）

ルールで複数の条件が指定されている場合、クライアントがそれらのすべてに一致しないとルールは適用されません。

> ONTAP 9.3以降では、エクスポート ポリシーの設定チェックをバックグラウンド ジョブとして有効にし、ルール違反をエラー ルール リストに記録できるようになりました。`vserver export-policy config-checker`コマンドを実行するとチェッカーが起動し、結果が表示されます。この結果を使用して設定を検証し、ポリシーからエラーのあるルールを削除できます。
>
> このコマンドで検証されるのは、エクスポート設定のホスト名、ネットグループ、匿名ユーザのみです。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv3プロトコルを使用して送信され、クライアントのIPアドレスは10.1.17.37です。

クライアント アクセス プロトコルは一致していますが、クライアントのIPアドレスがエクスポート ルールで指定されているアドレスとは異なるサブネット内にあります。したがって、クライアントは一致せず、このルールはこのクライアントに適用されません。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアント アクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアント アクセス プロトコルが一致し、クライアントのIPアドレスが指定されたサブネット内にあります。したがって、クライアントは一致し、このルールはこのクライアントに適用されます。セキュリティ タイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

両方のクライアントで、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータでは、認証に使用されるセキュリティ タイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。したがって、両方のクライアントが読み取り専用アクセス権を取得します。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認されたセキュリティ タイプKerberos v5を使用したためです。クライアント#2は読み取り / 書き込みアクセス権を取得できません。

リストにないセキュリティ タイプを持つ **NFS** クライアントの **ONTAP SVM** アクセスを管理する

クライアントがエクスポート ルールのアクセス パラメータにリストされていないセキュリティ タイプを提示する場合、クライアントへのアクセスを拒否するか、アクセス パラメータの `none`オプションを使用して匿名ユーザー ID にマッピングするかを選択できます。

クライアントは、別のセキュリティタイプで認証されたか、まったく認証されなかった（セキュリティタイプAUTH_NONE）ために、アクセスパラメータにリストされていないセキュリティタイプを提示する場合があります。デフォルトでは、クライアントはそのレベルへのアクセスを自動的に拒否されます。ただし、アクセスパラメータに `none`オプションを追加できます。その結果、リストされていないセキュリティスタイルを持つクライアントは、代わりに匿名ユーザーIDにマッピングされます。 `-anon`パラメータは、これらのクライアントに割り当てられるユーザーIDを決定します。 `-anon`パラメータに指定するユーザーIDは、匿名ユ

ーザーに適切と思われる権限が設定されている有効なユーザーである必要があります。

`-anon`パラメータの有効な値の範囲は `0`～ `65535`です。

割り当てられたユーザー **ID** -anon	クライアント アクセス要求の結果としての処理
0 - 65533	クライアント アクセス要求は匿名ユーザIDにマッピングされ、このユーザに設定されたアクセス権に基づいてアクセスが許可されます。
65534	クライアント アクセス要求はユーザnobodyにマッピングされ、このユーザに設定されたアクセス権に基づいてアクセスが許可されます。これがデフォルトです。
65535	このIDにマッピングされ、セキュリティ タイプがAUTH_NONEのクライアントからのアクセス要求は、すべて拒否されます。このIDにマッピングされ、他のセキュリティ タイプを使用している、ユーザIDが0のクライアントからのアクセス要求は拒否されます。

オプション `none`を使用する場合は、読み取り専用パラメータが最初に処理されることに留意してください。リストにないセキュリティタイプを持つクライアントのエクスポート ルールを設定する場合は、以下のガイドラインを考慮してください：

読み取り専用インクルード none	読み書きには以下が含まれます none	リストにないセキュリティ タイプのクライアントに対するアクセス結果
いいえ	いいえ	拒否されました
いいえ	はい	read-onlyが先に処理されるため、拒否
はい	いいえ	匿名として読み取り専用
はい	はい	匿名として読み取り / 書き込み

例

次の例は、 -rwrule `any`パラメータを含むエクスポート ポリシーを示しています：

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0

- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証されていません（セキュリティ タイプAUTH_NONE）。

3つすべてのクライアントで、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータは、AUTH_SYSで認証された自身のユーザIDを持つクライアントに読み取り専用アクセスを許可します。また、それ以外のセキュリティ タイプを使用して認証されたクライアントには、ユーザIDが70の匿名ユーザとして読み取り専用アクセスを許可します。読み取り / 書き込みパラメータは、すべてのセキュリティ タイプに読み取り / 書き込みアクセスを許可しますが、この例では、読み取り専用ルールですでにフィルタされたクライアントにのみ適用されます。

したがって、クライアント#1とクライアント#3には、ユーザIDが70の匿名ユーザとしてのみ読み取り / 書き込みアクセスが許可されます。クライアント#2には、自身のユーザIDで読み取り / 書き込みアクセスが許可されます。

次の例は、 `-rwrule` `none`パラメータを含むエクスポート ポリシーを示しています：

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

クライアント#1は、IPアドレスが10.1.16.207で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

クライアント#3は、IPアドレスが10.1.16.234で、NFSv3プロトコルを使用してアクセス要求を送信し、認証されていません（セキュリティ タイプAUTH_NONE）。

3つすべてのクライアントで、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータは、AUTH_SYSで認証された自身のユーザIDを持つクライアントに読み取り専用アクセスを許可します。また、それ以外のセキュリティ タイプを使用して認証されたクライアントには、ユーザIDが70の匿名ユーザとして読み取り専用アクセスを許可します。読み取り / 書き込みパラメータは、匿名ユーザとしてのみ読み取り / 書き込みアクセスを許可します。

したがって、クライアント#1とクライアント#3は、ユーザIDが70の匿名ユーザとしてのみ読み取り / 書き込

みアクセスが許可されます。クライアント#2は、自身のユーザIDで読み取り専用アクセスが許可されますが、読み取り / 書き込みアクセスは拒否されます。

ONTAPセキュリティ タイプによる**NFS**クライアント アクセス レベルの決定方法

クライアントが認証に使用したセキュリティ タイプは、エクスポート ルールにおいて特別な役割を果たします。セキュリティ タイプによって、クライアントがボリュームまたはqtreeに対して取得するアクセス レベルがどのように決定されるかを理解する必要があります。

可能な3つのアクセス レベルは次のとおりです：

1. read-only
2. 読み取り / 書き込み
3. スーパーユーザー（ユーザーID 0のクライアントの場合）

セキュリティ タイプ別のアクセス レベルはこの順序で評価されるため、エクスポート ルールでアクセス レベル パラメータを作成するときは、次のルールに従う必要があります。

クライアントがアクセス レベルを取得するには...	これらのアクセス パラメータは、クライアントのセキュリティ タイプと一致する必要があります...
標準ユーザの読み取り専用	読み取り専用(`-rorule`)
標準ユーザの読み取り / 書き込み	読み取り専用(`-rorule`）と読み取り/書き込み(`-rwrule`)
スーパーユーザの読み取り専用	読み取り専用(`-rorule`）、および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用(`-rorule`）と読み取り/書き込み(`-rwrule`）および `-superuser`

次に、3つそれぞれのアクセス パラメータで有効なセキュリティ タイプを示します。

- `any`
- `none`
- `never`

  このセキュリティ タイプは、 `-superuser` パラメータでは使用できません。

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`

- `sys`

クライアントのセキュリティ タイプを3つのアクセス パラメータのそれぞれと照合すると、次の3つの結果が考えられます：

クライアントのセキュリティ タイプが...	するとクライアントは...
アクセス パラメータで指定されたものと一致します。	独自のユーザIDを使用してそのレベルへのアクセスを取得します。
指定されたものと一致しませんが、accessパラメータにオプション `none`が含まれています。	`-anon`パラメータで指定されたユーザーIDを持つ匿名ユーザーとして、そのアクセス レベルを取得します。
指定されたものと一致せず、アクセス パラメータにオプション `none`が含まれていません。	そのレベルではアクセスできません。 `-superuser`パラメータには適用されません。このパラメータには、指定されていない場合でも常に `none`が含まれるためです。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

クライアント#3は、IPアドレスが10.1.16.234、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、認証されませんでした（AUTH_NONE）。

クライアント アクセス プロトコルとIPアドレスは、3つのクライアントすべてに一致しています。読み取り専用パラメータは、セキュリティ タイプに関係なく、すべてのクライアントに読み取り専用アクセスを許可します。読み取り/書き込みパラメータは、AUTH_SYSまたはKerberos v5で認証された、自身のユーザーIDを持つ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。スーパーユーザー パラメータは、Kerberos v5で認証された、ユーザーIDが0のクライアントにスーパーユーザー アクセスを許可します。

したがって、クライアント#1は3つのアクセス パラメータすべてに一致するため、スーパーユーザーの読み取り/書き込みアクセスを取得します。クライアント#2は読み取り/書き込みアクセスを取得しますが、スーパーユーザー アクセスは取得しません。クライアント#3は読み取り専用アクセスを取得しますが、スーパーユーザー アクセスは取得しません。

エクスポート ポリシーを構成するときは、ストレージ システムがユーザー ID 0（つまりスーパーユーザー）のクライアント アクセス要求を受信した場合にどのように処理するかを考慮し、それに応じてエクスポート ルールを設定する必要があります。

UNIXの世界では、ユーザーIDが0のユーザーはスーパーユーザー（通常はroot）と呼ばれ、システムに対して無制限のアクセス権を持ちます。スーパーユーザー権限の使用は、システムやデータのセキュリティ侵害など、いくつかの理由から危険を伴います。

デフォルトでは、ONTAPはユーザID 0を提示するクライアントを匿名ユーザにマッピングします。ただし、エクスポート ルールで `- superuser`パラメータを指定することで、セキュリティタイプに応じてユーザID 0を提示するクライアントの処理方法を決定できます。 `-superuser`パラメータに有効なオプションは次のとおりです：

- `any`
- `none`

  `-superuser`パラメータを指定しない場合、これがデフォルト設定になります。

- `krb5`
- `ntlm`
- `sys`

  `-superuser`パラメータ設定に応じて、ユーザー `ID 0` で提示されるクライアントの処理方法は `2` つあります：

`-superuser` `パラメータとクライアントのセキュリティ タイプが...	するとクライアントは...
一致	ユーザー ID 0 でスーパーユーザー アクセスを取得します。
一致しない	`-anon`パラメータで指定されたユーザー `ID`と割り当てられた権限を持つ匿名ユーザーとしてアクセスを取得します。これは、読み取り専用パラメータまたは読み取り/書き込みパラメータで `none`オプションが指定されているかどうかに関係なく適用されます。

クライアントがNTFSセキュリティ スタイルのボリュームにアクセスするためにユーザーID 0を提示し、 `-

superuser`パラメータが `none`に設定されている場合、ONTAPは匿名ユーザーの名前マッピングを使用して適切な認証情報を取得します。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

両方のクライアントで、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータでは、認証に使用されるセキュリティ タイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント#1だけです。これは、認証に承認されたセキュリティ タイプKerberos v5を使用したためです。

クライアント#2はスーパーユーザーアクセスを取得できません。代わりに、 `-superuser`パラメータが指定されていないため、匿名ユーザーにマッピングされます。つまり、デフォルトは `none`となり、ユーザーID 0が匿名ユーザーに自動的にマッピングされます。また、クライアント#2はセキュリティタイプが読み取り/書き込みパラメータと一致しなかったため、読み取り専用アクセスしか取得できません。

例

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されました。

クライアント#2は、IPアドレスが10.1.16.211、ユーザIDが0で、NFSv3プロトコルを使用してアクセス要求を送信し、AUTH_SYSで認証されました。

両方のクライアントで、クライアント アクセス プロトコルとIPアドレスは一致しています。読み取り専用パラメータでは、認証に使用されるセキュリティ タイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。ただし、読み取り / 書き込みアクセス権を取得するのはクライアント#1だけで

す。これは、認証に承認されたセキュリティ タイプKerberos v5を使用したためです。クライアント#2は読み取り / 書き込みアクセス権を取得できません。

エクスポート ルールは、ユーザID 0のクライアントにスーパーユーザ アクセスを許可します。クライアント#1は、読み取り専用および `-superuser`パラメータのユーザIDとセキュリティ タイプが一致するため、スーパーユーザ アクセスを取得します。クライアント#2は、セキュリティ タイプが読み取り/書き込みパラメータまたは `-superuser`パラメータと一致しないため、読み取り/書き込みアクセスもスーパーユーザ アクセスも取得できません。代わりに、クライアント#2は匿名ユーザにマッピングされます。この場合、匿名ユーザのユーザIDは0です。

ONTAP NFSエクスポート ポリシー キャッシュについて学ぶ

システムパフォーマンスを向上させるため、ONTAPはホスト名やネットグループなどの情報をローカルキャッシュに保存します。これによりONTAPは、外部ソースから情報を取得するよりも迅速にエクスポートポリシールールを処理できます。キャッシュとは何か、そしてその機能を理解することは、クライアントアクセスの問題のトラブルシューティングに役立ちます。

NFSエクスポートへのクライアントアクセスを制御するには、エクスポートポリシーを設定します。各エクスポートポリシーにはルールが含まれており、各ルールには、アクセスを要求するクライアントとルールを一致させるためのパラメータが含まれています。これらのパラメータの中には、ドメイン名、ホスト名、ネットグループなどのオブジェクトを解決するために、ONTAPがDNSサーバやNISサーバなどの外部ソースに接続する必要があるものがあります。

外部ソースとのこれらの通信には多少の時間がかかります。パフォーマンスを向上させるため、ONTAPは各ノードの複数のキャッシュに情報をローカルに保存することで、エクスポート ポリシー ルール オブジェクトの解決にかかる時間を短縮します。

キャッシュ名	保存される情報の種類
アクセス	クライアントと対応するエクスポート ポリシーのマッピング
Name	UNIX ユーザー名と対応する UNIX ユーザー ID のマッピング
ID	UNIX ユーザー ID と対応する UNIX ユーザー ID および拡張 UNIX グループ ID のマッピング
ホスト	ホスト名と対応するIPアドレスのマッピング
Netgroup	ネットグループとメンバーの対応するIPアドレスのマッピング
showmount	SVM ネームスペースからエクスポートされたディレクトリのリスト

環境内の外部ネーム サーバの情報を ONTAP が取得してローカルに保存した後に変更すると、キャッシュに古い情報が含まれる可能性があります。ONTAP は一定期間後にキャッシュを自動的に更新しますが、キャッ

シュごとに有効期限と更新タイミング、およびアルゴリズムが異なります。

キャッシュに古い情報が含まれるもう一つの理由は、ONTAPがキャッシュ情報を更新しようとした際にネーム サーバとの通信に失敗したことが挙げられます。この場合、ONTAPはクライアントの中断を防ぐため、ローカル キャッシュに現在保存されている情報を引き続き使用します。

その結果、成功するはずのクライアントアクセス要求が失敗したり、失敗するはずのクライアントアクセス要求が成功したりすることがあります。このようなクライアントアクセスの問題をトラブルシューティングする際には、エクスポートポリシーキャッシュの一部を確認し、手動でフラッシュすることができます。

ONTAP NFSアクセスキャッシュについて学ぶ

ONTAPは、ボリュームまたはqtreeへのクライアントアクセス操作に対するエクスポートポリシールール評価の結果を保存するために、アクセスキャッシュを使用します。これにより、クライアントがI/O要求を送信するたびにエクスポートポリシールールの評価プロセスを実行するよりも、アクセスキャッシュから情報を取得する方がはるかに高速であるため、パフォーマンスが向上します。

NFSクライアントがボリュームまたはqtree上のデータにアクセスするためにI/O要求を送信すると、ONTAPは各I/O要求を評価し、I/O要求を許可するか拒否するかを決定する必要があります。この評価には、ボリュームまたはqtreeに関連付けられたエクスポートポリシーのすべてのエクスポートポリシールールをチェックすることが含まれます。ボリュームまたはqtreeへのパスが1つ以上のジャンクションポイントを通過する場合、パス上の複数のエクスポートポリシーに対してこのチェックを実行する必要がある場合があります。

この評価は、初期マウント要求だけでなく、読み取り、書き込み、リスト、コピーなどの操作など、NFSクライアントから送信されるすべてのI/O要求に対して実行されることに注意してください。

ONTAPが適用可能なエクスポート ポリシー ルールを識別し、要求を許可するか拒否するかを決定した後、ONTAPはこの情報を格納するためのエントリをアクセス キャッシュに作成します。

NFSクライアントがI/O要求を送信すると、ONTAPはクライアントのIPアドレス、SVMのID、およびターゲットボリュームまたはqtreeに関連付けられたエクスポートポリシーを記録し、まずアクセスキャッシュで一致するエントリをチェックします。アクセスキャッシュに一致するエントリが存在する場合、ONTAPは保存されている情報を使用してI/O要求を許可または拒否します。一致するエントリが存在しない場合、ONTAPは前述のように、適用可能なすべてのポリシールールを評価する通常のプロセスを実行します。

アクティブに使用されていないアクセスキャッシュエントリは更新されません。これにより、外部ネームサーバーとの不要で無駄な通信が削減されます。

アクセスキャッシュから情報を取得する方が、すべてのI/O要求に対してエクスポートポリシールールの評価プロセス全体を実行するよりもはるかに高速です。そのため、アクセスキャッシュを使用すると、クライアントアクセスチェックのオーバーヘッドが削減され、パフォーマンスが大幅に向上します。

ONTAP NFSアクセスキャッシュパラメータについて学ぶ

アクセス キャッシュ内にあるエントリの更新期間を制御するパラメータがいくつかあります。これらのパラメータの仕組みを理解すると、各パラメータを変更して、アクセスキャッシュを調整したり、パフォーマンスと格納される情報の鮮度のバランスをとったりできます。

アクセス キャッシュには、ボリュームまたはqtreeへのアクセスを試みるクライアントに適用される1つ以上

のエクスポート ルールで構成されるエントリが格納されます。これらのエントリは、一定期間格納されたあと、更新されます。更新時間は、アクセス キャッシュ パラメータによって決定され、アクセス キャッシュ エントリのタイプによって異なります。

個々のSVMに対してアクセス キャッシュ パラメータを指定できます。このため、SVMのアクセス要件に応じてパラメータを変えることができます。アクティブに使用されていないアクセス キャッシュ エントリは更新されないため、外部ネーム サーバとの無駄な通信が削減されます。

アクセスキャッシュエントリタイプ	概要	更新間隔（秒）
受理エントリ	クライアントのアクセスが拒否されなかったアクセス キャッシュ エントリです。	最小：300 最大値：86,400 デフォルト：3,600
拒否エントリ	クライアントのアクセスが拒否されたアクセス キャッシュ エントリです。	最小：60 最大値：86,400 デフォルト：3,600

例

NFSクライアントがクラスタ上のボリュームにアクセスしようとします。ONTAPはクライアントをエクスポートポリシールールと照合し、エクスポートポリシールールの設定に基づいてクライアントがアクセスを許可されるかどうかを判断します。ONTAPは、このエクスポートポリシールールをアクセスキャッシュにポジティブエントリとして保存します。デフォルトでは、ONTAPはアクセスキャッシュにポジティブエントリを1時間（3,600秒）保存し、その後自動的にエントリを更新して情報を最新の状態に保ちます。

アクセスキャッシュが不必要にいっぱいになるのを防ぐため、クライアントアクセスの判定に一定期間使用されていない既存のアクセスキャッシュエントリをクリアするパラメータが追加されました。この `-harvest-timeout`パラメータの許容範囲は60秒から2,592,000秒で、デフォルト設定は86,400秒です。

ONTAP NFS qtreeからエクスポート ポリシーを削除します

特定のエクスポート ポリシーをqtreeに割り当てたままにしておく必要がなくなった場合は、qtreeを変更して、含まれているボリュームのエクスポート ポリシーを継承するようにすることで、そのエクスポート ポリシーを削除できます。これを行うには、 `volume qtree modify`コマンドに `-export-policy`パラメータと空の名前文字列（""）を指定します。

手順

1. qtreeからエクスポート ポリシーを削除するには、次のコマンドを入力します。

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. qtreeが適切に変更されたことを確認します。

```
volume qtree show -qtree qtree_name -fields export-policy
```

qtreeファイル操作のONTAP NFS qtree IDを検証する

ONTAPは、オプションでqtree IDの追加検証を実行できます。この検証により、クライアントのファイル操作要求で有効なqtree IDが使用され、クライアントが同じqtree内でのみファイルを移動できるようになります。この検証は、 `-validate-qtree-export`パラメータを変更することで有効または無効にできます。このパラメータはデフォルトで有効になっています。

タスク概要

このパラメータは、Storage Virtual Machine（SVM）上の1つ以上のqtreeにエクスポート ポリシーを直接割り当てた場合にのみ有効です。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

qtree ID検証を行う場合は…	入力するコマンド
有効	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
無効	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP NFS FlexVol ボリュームのエクスポート ポリシーの制限とネストされたジャンクション

上位レベルのジャンクションの制限がネストされたジャンクションよりも厳しいエクスポート ポリシーを設定した場合、下位レベルのジャンクションへのアクセスに失敗する可能性があります。

上位レベルのジャンクションには下位レベルのジャンクションよりも制限が緩いエクスポート ポリシーを設定してください。

NFSでのKerberos使用によるセキュリティ強化

ONTAP の Kerberos に対する NFS サポート

Kerberosは、クライアント / サーバ アプリケーションに対して強力でセキュアな認証を提供し、サーバに対してユーザおよびプロセスのIDの検証機能を提供します。ONTAP環境では、Storage Virtual Machine（SVM）とNFSクライアント間の認証をKerberosで実行できます。

ONTAP 9では、次のKerberos機能がサポートされます。

- 整合性チェック機能を備えたKerberos 5認証（krb5i）

  Krb5iでは、チェックサムを使用して、クライアントとサーバとの間で転送される各NFSメッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの保証など）とデータ整合性に関する理由（信頼性の低いネットワークでNFSを使用する場合のデータ破損の防止など）の両方で有用です。

- プライバシー チェック機能を備えたKerberos 5認証（krb5p）

  krb5pでは、クライアントとサーバ間のすべてのトラフィックがチェックサムで暗号化されます。これによって安全性は高まりますが、負荷も高くなります。

- 128ビットおよび256ビットのAES暗号化

  Advanced Encryption Standard（AES）は電子データを保護するための暗号化アルゴリズムです。ONTAPでは、セキュリティ強化のために、128ビット キーによるAES（AES-128）と256ビット キーによるAES（AES-256）がKerberosでサポートされています。

- SVMレベルのKerberos Realm設定

  SVM管理者は、Kerberos Realm設定をSVMレベルで作成できるようになりました。つまり、SVM管理者は、Kerberos Realm設定に関してクラスタ管理者に頼る必要がなくなり、個別のKerberos Realm設定をマルチテナンシー環境で作成することができます。

ONTAP NFSでKerberosを設定するための要件

NFSでKerberosを使用するための設定をシステムで行う前に、ネットワークおよびストレージの環境のいくつかの項目について、適切に設定されていることを確認する必要があります。

> 環境を設定する手順は、クライアントで使用しているオペレーティング システム、ドメイン コントローラ、Kerberos、DNSなどのバージョンや種類によって異なります。このドキュメントでは、それらのすべてについては説明していません。詳細については、それぞれのコンポーネントの対応するドキュメントを参照してください。
>
> Windows Server 2008 R2のActive DirectoryおよびLinuxホストを使用する環境でのONTAPとKerberos 5およびNFSv3 / NFSv4の設定方法に関する詳しい例については、テクニカル レポート4073を参照してください。

次の項目について事前に設定しておく必要があります。

ネットワーク環境の要件

- Kerberos

  KerberosをKey Distribution Center（KDC;キー配布センター）で設定しておく必要があります（たとえば、Windows Active DirectoryベースのKerberosまたはは MIT Kerberos）。

  NFSサーバは、マシン プリンシパルのプライマリ コンポーネントとして `nfs`を使用する必要があります。

- ディレクトリ サービス

  Active DirectoryやOpenLDAPなどのセキュアなディレクトリ サービスを環境に導入し、SSL / TLS経由のLDAPを使用するように設定する必要があります。

- NTP

  タイム サーバでNTPを実行している必要があります。これは、時刻のずれによるKerberos認証の失敗を回避するために必要です。

- ドメイン名解決（DNS）

  それぞれのUNIXクライアントおよびSVM LIFについて、KDCの前方参照ゾーンと逆引き参照ゾーンに適切なサービス レコード（SRV）が登録されている必要があります。すべてのコンポーネントは、DNSで正しく解決できる必要があります。

- ユーザ アカウント

  各クライアントは Kerberos レルム内にユーザーアカウントを持っている必要があります。NFSサーバーは、マシンプリンシパルのプライマリコンポーネントとして “nfs” を使用する必要があります。

NFSクライアントの要件

- NFS

  NFSv3またはNFSv4を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

  クライアントでRFC1964およびRFC2203がサポートされている必要があります。

- Kerberos

  Kerberos認証を使用するように各クライアントが適切に設定されている必要があります。詳細は次のとおりです。

  - TGS 通信の暗号化が有効になっています。

    非常にセキュリティ性の高いAES-256。

  - TGT 通信に最も安全な暗号化タイプが有効になっています。
  - Kerberos 領域とドメインが正しく設定されています。
  - GSSが有効。

マシンのクレデンシャルを使用する場合：

- `gssd`を `-n`パラメータを付けて実行しないでください。
- `kinit`をrootユーザーとして実行しないでください。

- 各クライアントは、最新かつ更新済みバージョンのオペレーティング システムを使用している必要があります。

  これにより、KerberosでのAES暗号化の互換性と信頼性が最大限確保されます。

- DNS

  DNSを使用して名前が正しく解決されるように各クライアントが適切に設定されている必要があります。

- NTP

  各クライアントがNTPサーバと同期されている必要があります。

- ホストとドメインの情報

  各クライアントの `/etc/hosts`および `/etc/resolv.conf`ファイルには、それぞれ正しいホスト名とDNS情報が含まれている必要があります。

- keytabファイル

  各クライアントについて、KDCのkeytabファイルが必要です。Realmは大文字で指定する必要があります。最高レベルのセキュリティを得るために、暗号化タイプをAES-256にする必要があります。

- オプション：パフォーマンスを最大限に高めるには、ローカル エリア ネットワークとの通信用とストレージ ネットワークとの通信用に、少なくとも2つのネットワーク インターフェイスを設定します。

ストレージ システムの要件

- NFSライセンス

  ストレージ システムに有効なNFSライセンスがインストールされている必要があります。

- CIFSライセンス

  CIFSライセンスはオプションです。マルチプロトコルのネーム マッピングを使用する環境で、Windowsクレデンシャルのチェックを行う場合にのみ必要になります。純粋なUNIXのみの環境では必要ありません。

- SVM

  システムでSVMを少なくとも1つ設定しておく必要があります。

- SVMでのDNS

  各SVMでDNSを設定しておく必要があります。

- NFS サーバ

  SVMでNFSを設定しておく必要があります。

- AES暗号化

  最高レベルのセキュリティを得るために、KerberosでAES-256暗号化のみを許可するようにNFSサーバを設定する必要があります。

- SMB サーバ

  マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMBサーバはマルチプロトコルのネーム マッピングに必要です。

- ボリューム

  SVMで使用するルート ボリュームと少なくとも1つのデータ ボリュームを設定しておく必要があります。

- ルート ボリューム

  SVMのルート ボリュームを次のように設定しておく必要があります。

Name	設定
セキュリティ形式	UNIX
UID	rootまたはID 0
GID	rootまたはID 0
UNIX権限	777

  ルート ボリュームとは異なり、データ ボリュームのセキュリティ形式は任意に設定してかまいません。

- UNIXグループ

  SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループ**ID**
daemon	1
root	0
pcuser	65534（SVMを作成すると自動的に作成されます）

- UNIXユーザ

  SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザーID	プライマリ グループID	コメント
nfs	500	0	GSS INITフェーズで必要 NFSクライアント ユーザのSPNの最初のコンポーネントがユーザとして使用されます。
pcuser	65534	65534	NFSとCIFSのマルチプロトコルで必要 SVMの作成時に、ONTAPによって自動的に作成されてpcuserグループに追加されます。
root	0	0	マウントに必要

NFSクライアント ユーザのSPNに対するKerberos-UNIXネーム マッピングがある場合は、nfsユーザは必要ありません。

- エクスポート ポリシーとエクスポート ルール

  ルートボリューム、データボリューム、およびqtreeに必要なエクスポート ルールを含むエクスポート ポリシーを設定しておく必要があります。SVMのすべてのボリュームがKerberos経由でアクセスされる場合は、ルートボリュームのエクスポート ルール オプション `-rorule`、 `-rwrule`、および `-superuser` を `krb5`、 `krb5i`、または `krb5p`に設定できます。

- Kerberos-UNIXネーム マッピング

  NFSクライアント ユーザのSPNによって識別されたユーザにroot権限を持たせる場合は、rootに対するネーム マッピングを作成する必要があります。

関連情報

"NetAppテクニカル レポート4073: 『Secure Unified Authentication』"

"NetApp Interoperability Matrix Tool"

"システム管理"

"論理ストレージ管理"

NFSv4の**ONTAP**ユーザー**ID**ドメインを指定します

ユーザIDドメインを指定するには、 `-v4-id-domain`オプションを設定します。

タスク概要

デフォルトでは、ONTAPはNISドメインが設定されている場合、NFSv4ユーザIDマッピングにNISドメインを

使用します。NISドメインが設定されていない場合は、DNSドメインが使用されます。例えば、複数のユーザIDドメインがある場合は、ユーザIDドメインの設定が必要になることがあります。ドメイン名はドメイン コントローラのドメイン設定と一致する必要があります。NFSv3では必要ありません。

手順

1. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

ネーム サービスを設定する

ONTAP NFSネーム サービス スイッチ構成について学ぶ

ONTAPは、UNIXシステムの `/etc/nsswitch.conf` ファイルに相当するテーブルにネーム サービス設定情報を保存します。環境に合わせて適切に設定できるように、テーブルの機能とONTAPでの使用方法を理解しておく必要があります。

ネーム サービス スイッチ テーブルは、ONTAPが特定の種類のネーム サービス情報を取得する際にどのネーム サービス ソースをどの順番で参照するかを決定します。ネーム サービス スイッチ テーブルは、SVMごとに作成および保存されます。

データベース タイプ

テーブルには、次の各データベース タイプについてネーム サービスのリストが格納されます。

データベースの種類	... の名前サービス ソースを定義します。	有効なソースは次のとおりです。
ホスト	ホスト名のIPアドレスへの変換	files、dns
グループ	ユーザ グループ情報の検索	files、nis、ldap
passwd	ユーザ情報の検索	files、nis、ldap
netgroup	ネットグループ情報の検索	files、nis、ldap
namemap	ユーザ名のマッピング	files、ldap

ソース タイプ

ソース タイプによって、該当する情報を取得するために使用するネーム サービス ソースが決まります。

ソース タイプを指定...	...の情報を検索するには	コマンド ファミリによって管理されます...

ファイル	ローカルのソース ファイル	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	SVMのNISドメイン設定で指定された外部のNISサーバ	`vserver services name-service nis-domain`
ldap	SVMのLDAPクライアント設定で指定された外部のLDAPサーバ	`vserver services name-service ldap`
dns	SVMのDNS設定で指定された外部のDNSサーバ	`vserver services name-service dns`

データ アクセスと SVM 管理認証の両方に NIS または LDAP を使用する予定の場合でも、 `files`を含め、NIS または LDAP 認証が失敗した場合に備えて、フォールバックとしてローカル ユーザーを設定する必要があります。

外部ソースへのアクセスに使用されるプロトコル

ONTAPでは、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部ネーム サービス ソース	アクセスに使用されるプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例では、SVM svm_1のネーム サービス スイッチ情報を表示しています。

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

ホストのIPアドレス検索では、最初にローカルのソース ファイルが参照され、結果が返されない場合は、次にDNSサーバが照会されます。

ユーザまたはグループ情報の検索では、ローカルのソース ファイルだけが参照され、結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、最初に外部のNISサーバが参照され、結果が返されない場合は、次にローカルのネットグループ ファイルが照会されます。

SVM svm_1のテーブルには、ネーム マッピング用のネーム サービス エントリは含まれていません。そのため、デフォルトの設定に従ってローカルのソース ファイルだけが参照されます。

関連情報

"NetAppテクニカル レポート4668：『Name Services Best Practices Guide』"

LDAPの使用

ONTAP NFS SVMのLDAPについて学ぶ

LDAP（Lightweight Directory Access Protocol）サーバを使用すると、ユーザ情報を一元的に管理できます。ユーザ データベースを環境内のLDAPサーバに格納している場合、既存のLDAPデータベース内のユーザ情報を検索するようにストレージ システムを設定できます。

- LDAPをONTAP用に設定する前に、サイト環境がLDAPサーバおよびクライアント設定のベストプラクティスを満たしていることを確認する必要があります。具体的には、次の条件を満たす必要があります。
  - LDAPサーバのドメイン名がLDAPクライアント上のエントリと一致する必要があります。
  - LDAPサーバでサポートされるLDAPユーザのパスワード ハッシュ タイプに、ONTAPでサポートされる次のタイプが含まれている必要があります。
    - CRYPT（すべてのタイプ）およびSHA-1（SHA、SSHA）
    - ONTAP 9.8以降では、SHA-2ハッシュ（SHA-256、SSH-384、SHA-512、SSHA-256、SSHA-384、およびSSHA-512）もサポートされます。
  - LDAPサーバにセッション セキュリティ対策が必要な場合は、LDAPクライアントで設定する必要があります。

以下のセッション セキュリティ オプションを使用できます。

- LDAP署名（データの整合性チェックを提供）およびLDAP署名と封印（データの整合性チェックと暗号化を提供）
- START TLS
- LDAPS（TLSまたはSSL経由のLDAP）

◦ 署名および封印されたLDAPクエリを有効にするには、次のサービスが設定されている必要があります。

- LDAPサーバでGSSAPI（Kerberos）SASLがサポートされている必要があります。
- LDAPサーバに、DNS A/AAAAレコード、およびDNSサーバで設定されたPTRレコードが必要です。
- Kerberosサーバに、DNSサーバ上に存在するSRVレコードが必要です。

◦ START TLSまたはLDAPSを有効にする場合、次の点を考慮する必要があります。

- NetAppでは、LDAPSではなくStart TLSの使用を推奨しています。
- LDAPSを使用する場合、LDAPサーバでTLSまたはSSL（ONTAP 9.5以降）を有効にする必要があります。SSLはONTAP 9.4～9.0ではサポートされていません。
- 証明書サーバがドメインで設定済みである必要があります。

◦ LDAPリファーラル追跡を有効にするには（ONTAP 9.5以降）、次の条件を満たしている必要があります。

- 両方のドメインで次のいずれかの信頼関係が設定されている必要があります。
  - 双方向
  - 一方向（プライマリ ドメインがリファーラル ドメインを信頼）
  - 親子
- 参照されているすべてのサーバ名を解決するようにDNSが設定されている必要があります。
- `--bind-as-cifs-server`がtrueに設定されている場合、認証にはドメイン パスワードが同じである必要があります。

> 次の設定はLDAPリファーラル追跡でサポートされていません。
>
> ◦ すべてのONTAPバージョン：
>
> ◦ 管理SVM上のLDAPクライアント
>
> ◦ ONTAP 9.8以前の場合（9.9.1以降でサポートされます）：
>
> ◦ LDAP署名とシーリング（ `-session-security`オプション）
>
> ◦ 暗号化されたTLS接続（ `-use-start-tls` オプション）
>
> ◦ LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap` オプション）

- ONTAP 9.11.1以降では、"ONTAP NFS SVMのnsswitch認証にはLDAP高速バインドを使用します。"を使用できます。
- SVMでLDAPクライアントを設定する際は、LDAPスキーマを入力する必要があります。

  ほとんどの場合、デフォルトのONTAPスキーマのいずれかで問題ありません。ただし、環境のLDAPスキ

ーマがデフォルトのスキーマと異なる場合は、LDAPクライアントを作成する前にONTAP用の新しいLDAPクライアント スキーマを作成する必要があります。環境の要件については、LDAP管理者にお問い合わせください。

- LDAPをホスト名解決に使用することはサポートされていません。

詳細については、 "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"を参照してください。

ONTAP NFS SVMのLDAP署名とシーリングについて学習します

ONTAP 9以降では、署名と封印を設定して、Active Directory（AD）サーバへの照会に対するLDAPセッション セキュリティを有効にすることができます。Storage Virtual Machine（SVM）のNFSサーバ セキュリティ設定をLDAPサーバの設定に対応するように設定する必要があります。

署名は、秘密鍵技術を用いてLDAPペイロードデータの整合性を確認します。シールは、LDAPペイロードデータを暗号化することで、機密情報をクリアテキストで送信することを回避します。_LDAPセキュリティレベル_オプションは、LDAPトラフィックに署名が必要か、署名とシールが必要か、あるいはどちらも不要かを指定します。デフォルトは `none`です。test

SMB トラフィック上の LDAP 署名とシーリングは、 `vserver cifs security modify`コマンドの `-session-security-for-ad-ldap`オプションを使用して SVM 上で有効になります。

ONTAP NFS SVMのLDAPSについて学ぶ

ONTAPでのLDAP通信の保護方法に関する用語や概念を理解しておく必要があります。ONTAPは、Active Directory統合LDAPサーバ間またはUNIXベースのLDAPサーバ間の認証されたセッションを設定するために、Start TLSまたはLDAP over TLSを使用できます。

用語

ONTAPでのLDAPSを使用したLDAP通信の保護方法に関して理解しておくべき用語があります。

- **LDAP**

  （Lightweight Directory Access Protocol;ライトウェイト ディレクトリ アクセス プロトコル）情報ディレクトリに対するアクセスおよび管理を行うためのプロトコルです。LDAPは、ユーザ、グループ、ネットグループのようなオブジェクトを格納するための情報ディレクトリとして使用されます。またLDAPは、これらのオブジェクトを管理したりLDAPクライアントからの要求を満たしたりするディレクトリ サービスを提供します。

- **SSL**

  （Secure Sockets Layer）インターネット上で情報を安全に送信するために開発されたプロトコルです。SSLは、ONTAP 9以降でサポートされていますが、TLSの導入に伴い廃止されました。

- **TLS**

  （Transport Layer Security） それまでのSSL仕様に基づいたIETF標準の追跡プロトコルです。SSLの後継にあたります。TLSは、ONTAP 9.5以降でサポートされています。

- **LDAPS**（**SSL** または **TLS** 経由の **LDAP**）

  TLSまたはSSLを使用してLDAPクライアントとLDAPサーバ間の通信を保護するプロトコル。「LDAP over SSL」と「LDAP over TLS」という用語は、同じ意味で使用される場合があります。LDAPSはONTAP 9.5以降でサポートされています。

  - ONTAP 9.8～9.5では、LDAPSはポート636でのみ有効にできます。これを行うには、 `vserver cifs security modify`コマンドで `-use-ldaps-for-ad-ldap`パラメータを使用します。
  - ONTAP 9.9.1以降では、ポート636がデフォルトのままですが、LDAPSは任意のポートで有効にできます。有効にするには、 `-ldaps-enabled`パラメータを `true`に設定し、必要な `-port`パラメータを指定します。"ONTAPコマンド リファレンス"の `vserver services name-service ldap client create`の詳細を確認してください。

  NetAppでは、LDAPSではなくStart TLSの使用を推奨しています。

- **TLS**の開始

  （*start_tls*、*STARTTLS*、*StartTLS* とも呼ばれます）TLSプロトコルを使用して安全な通信を提供するメカニズム。

  ONTAPでは、LDAP通信を保護するためにSTARTTLSを使用し、デフォルトのLDAPポート（389）を使用してLDAPサーバと通信します。LDAPサーバは、LDAPポート389経由の接続を許可するように設定する必要があります。そうしないと、SVMからLDAPサーバへのLDAP TLS接続が失敗します。

ONTAPでの**LDAPS**の使用方法

ONTAPはTLSサーバ認証をサポートしています。この認証により、SVMのLDAPクライアントは、バインド操作時にLDAPサーバの識別情報を確認できます。TLSに対応したLDAPクライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開IDが有効であり、かつクライアントの信頼できるCertificate Authority（CA;認証局）のリストにあるCAによって発行されたものであるかどうかをチェックできます。

LDAPでは、TLSを使用した通信の暗号化方法としてSTARTTLSがサポートされています。STARTTLSは標準のLDAPポート（389）経由でプレーンテキスト接続として開始され、その後TLS接続にアップグレードされます。

ONTAPでは以下をサポートしています。

- Active Directory統合LDAPサーバとSVMとの間のSMB関連トラフィックに対するLDAPSの使用
- ネーム マッピングやその他のUNIX情報のLDAPトラフィックに対するLDAPSの使用

  Active Directory統合LDAPサーバまたはUNIXベースLDAPサーバのどちらかを使用して、LDAPネーム マッピングの情報やその他のUNIX情報（ユーザ、グループ、ネットグループなど）を格納できます。

- 自己署名ルートCA証明書

  Active-Directory統合LDAPを使用している場合は、Windows Server証明書サービスがドメインにインストールされていると自己署名ルート証明書が生成されます。UNIXベースのLDAPサーバをLDAPネーム マッピングに使用している場合は、該当するLDAPアプリケーションに適切な手段を使用して、自己署名ルート証明書の生成と保存が行われます。

デフォルトでは、LDAPSは無効になっています。

LDAPを使用するとともに、ネストされたグループ メンバーシップを使用するための追加機能を必要とする場合は、ONTAPを設定してLDAPのRFC2307bisサポートを有効にすることができます。

開始する前に

デフォルトのLDAPクライアント スキーマのうち、使用するいずれか1つのコピーを作成しておく必要があります。

タスク概要

LDAPクライアント スキーマでは、グループ オブジェクトによってmemberUid属性が使用されます。この属性は、複数の値を格納でき、そのグループに属するユーザの名前を一覧表示できます。RFC2307bis対応のLDAPクライアント スキーマでは、グループ オブジェクトによってuniqueMember属性が使用されます。この属性には、LDAPディレクトリ内の別のオブジェクトの完全なDistinguished Name（DN;識別名）を含めることができます。これにより、グループに他のグループをメンバーとして追加できるため、ネストされたグループを使用できます。

ユーザは、ネストされたグループを含めて256を超えるグループのメンバーになることはできません。ONTAPは、この256グループの上限を超えるグループをすべて無視します。

デフォルトでは、RFC2307bisサポートは無効になっています。

> MS-AD-BISスキーマを使用してLDAPクライアントを作成すると、RFC2307bisサポートは自動的に有効になります。

詳細については、 "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"を参照してください。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. コピーしたRFC2307 LDAPクライアント スキーマを変更して、RFC2307bisのサポートを有効にします。

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. LDAPサーバでサポートされているオブジェクト クラスに一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. LDAPサーバでサポートされている属性名に一致するように、スキーマを変更します。

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

環境にとって最も適した方法でLDAPサーバに接続するようにLDAPクライアントを構成することで、ユーザ、グループ、およびネットグループ情報を含め、LDAPディレクトリ検索を最適化することができます。デフォルトのLDAPベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報のLDAPクライアント検索オプションは、LDAPクエリの失敗、ひいてはストレージ システムへのクライアント アクセスの失敗を回避するのに役立ちます。また、クライアントのパフォーマンスに関する問題を回避するために、検索をできるだけ効率的なものにするのにも役立ちます。

デフォルトのベースおよびスコープ検索値

LDAPベースは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベースDNです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベースDNを使用して行われます。このオプションは、LDAPディレクトリが比較的小さくてすべての関連エントリが同じDN内にある場合に適しています。

カスタムベースDNを指定しない場合、デフォルトは `root`です。つまり、各クエリはディレクトリ全体を検索します。これによりLDAPクエリの成功率は最大化されますが、効率が悪く、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

LDAPベース スコープは、LDAPクライアントがLDAPクエリを実行するために使用するデフォルトのベース スコープです。ユーザ、グループ、ネットグループの検索を含むすべての検索は、ベース スコープを使用して行われます。LDAPクエリによる検索範囲を、名前付きエントリのみ、DNの1レベル下にあるエントリ、またはDNの下にあるサブツリー全体のどれにするかが決定されます。

カスタムベーススコープを指定しない場合、デフォルトは `subtree`です。つまり、各クエリはDN以下のサブツリー全体を検索します。これによりLDAPクエリの成功率は最大化されますが、効率が悪く、大規模なLDAPディレクトリではパフォーマンスが大幅に低下する可能性があります。

カスタム ベースおよびスコープ検索値

必要に応じて、ユーザ、グループ、およびネットグループ検索で、別々のベースおよびスコープ値を指定できます。クエリの検索ベースおよびクエリをこうした形で制限すると、検索対象がLDAPディレクトリのより小さなサブセクションに制限されるため、パフォーマンスを大幅に向上できます。

カスタム ベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索の全般的なデフォルト検索ベースおよびスコープは無視されます。カスタム ベースおよびスコープ値を指定するパラメータは、advanced権限レベルで使用できます。

LDAPクライアントパラメータ…	カスタムを指定します…
`-base-dn`	すべてのLDAP検索のベースDN。必要に応じて複数の値を入力できます（たとえば、ONTAP 9.5以降のリリースでLDAPリファーラル追跡が有効になっている場合など）。
`-base-scope`	すべてのLDAP検索の基本スコープ。

`-user-dn`	すべてのLDAPユーザー検索のベースDN。このパラメータはユーザー名マッピング検索にも適用されます。
`-user-scope`	すべてのLDAPユーザー検索の基本スコープ。このパラメータはユーザー名マッピング検索にも適用されます。
`-group-dn`	すべてのLDAPグループ検索のベースDN。
`-group-scope`	すべてのLDAPグループ検索の基本スコープ。
`-netgroup-dn`	すべてのLDAPネットグループ検索のベースDN。
`-netgroup-scope`	すべてのLDAPネットグループ検索の基本スコープ。

複数のカスタム ベース**DN**値

LDAPディレクトリが複雑な場合は、特定の情報を求めてLDAPディレクトリの複数の部分を検索するために複数のベースDNの指定が必要になる可能性があります。複数のユーザ、グループ、およびネットグループDNパラメータを指定するには、各パラメータをセミコロンで区切り、DN検索リスト全体を二重引用符（"）で囲みます。DNにセミコロンが含まれる場合、DNではセミコロンの直前にエスケープ文字（\）を追加する必要があります。

スコープは、対応するパラメータで指定されているDNのリスト全体に適用されることに注意してください。たとえば、3つの異なるユーザDNのリストとサブツリーをユーザ スコープで指定した場合は、LDAPユーザ検索により、指定された3つのDNのそれぞれでサブツリー全体が検索されます。

ONTAP 9.5以降では、LDAP _referral chasing_も指定できるようになりました。これにより、ONTAPのLDAPクライアントは、プライマリLDAPサーバからLDAPリファーラル応答が返されない場合に、他のLDAPサーバに検索要求を参照できます。クライアントはそのリファーラルデータを使用して、リファーラルデータに記述されているサーバからターゲットオブジェクトを取得します。参照先のLDAPサーバに存在するオブジェクトを検索するには、LDAPクライアント設定の一部として、参照先オブジェクトのbase-dnをbase-dnに追加します。ただし、参照先オブジェクトは、LDAPクライアント作成または変更時に（ `-referral-enabled true`オプションを使用して）リファーラル追跡が有効になっている場合にのみ検索されます。

カスタム**LDAP**検索フィルター

LDAP設定オプションパラメータを使用して、カスタム検索フィルタを作成できます。 `-group-membership-filter`パラメータは、LDAPサーバからグループメンバーシップを検索する際に使用する検索フィルタを指定します。

有効なフィルターの例は次のとおりです：

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

"ONTAPでLDAPを設定する方法"についての詳細をご覧ください。

LDAP環境がホスト単位のネットグループ検索を許可するように設定されている場合は、この機能を利用するようにONTAPを設定し、ホスト単位のネットグループ検索を実行することができます。これにより、ネットグループ検索の処理速度を大幅に引き上げ、ネットグループ検索時のレイテンシによるNFSクライアント アクセスの問題を減らすことができます。

開始する前に

LDAP ディレクトリには `netgroup.byhost` マップが含まれている必要があります。

DNSサーバには、NFSクライアントに対するフォワード（A）およびリバース（PTR）ルックアップ レコードの両方が含まれている必要があります。

ネットグループ内のIPv6アドレスを指定する際には、常にRFC 5952で指定されているとおりに各アドレスを短縮および圧縮する必要があります。

タスク概要

NISサーバは `netgroup`、 `netgroup.byuser`、 `netgroup.byhost`という3つの個別のマップにネットグループ情報を保存します。 `netgroup.byuser`マップと `netgroup.byhost`マップの目的は、ネットグループ検索を高速化することです。ONTAPは、NISサーバ上でホストごとのネットグループ検索を実行し、マウント応答時間を短縮できます。

デフォルトでは、LDAPディレクトリにはNISサーバのような `netgroup.byhost`マップはありません。ただし、サードパーティ製ツールを使用すれば、NIS `netgroup.byhost`マップをLDAPディレクトリにインポートして、ホストごとのネットグループ検索を高速化できます。LDAP環境でホストごとのネットグループ検索を許可するように設定している場合は、ONTAPのLDAPクライアントに `netgroup.byhost`マップ名、DN、検索範囲を指定して設定することで、ホストごとのネットグループ検索を高速化できます。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、ONTAPは、エクスポートへのアクセスをNFSクライアントから要求されたときに、より速くエクスポート ルールを処理できます。これにより、ネットグループ検索によるレイテンシの問題によってアクセスが遅延する可能性が低下します。

手順

1. LDAP ディレクトリにインポートした NIS `netgroup.byhost` マップの正確な完全識別名を取得します。

   マップのDNは、インポートに使用したサードパーティ ツールによって異なる場合があります。最高のパフォーマンスを得るために、正確なマップDNを指定してください。

2. 権限レベルをadvancedに設定します： `set -privilege advanced`
3. Storage Virtual Machine（SVM）のLDAPクライアント設定でホスト別ネットグループ検索を有効にします： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false}` は、LDAPディレクトリのホスト別ネットグループ検索を有効または無効にします。デフォルトは `false`です。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name`LDAPディレクトリ内の

`netgroup.byhost`マップの識別名を指定します。これは、ネットグループとホスト間の検索におけるベースDNを上書きします。このパラメータを指定しない場合、ONTAPは代わりにベースDNを使用します。

`-netgroup-byhost-scope {base|onelevel subtree}` は、ネットグループによるホスト検索の検索範囲を指定します。このパラメータを指定しない場合、デフォルトは `subtree`です。

LDAPクライアント構成がまだ存在しない場合は、 `vserver services name-service ldap client create`コマンドを使用して新しいLDAPクライアント構成を作成するときにこれらのパラメータを指定することにより、ホスト別のネットグループ検索を有効にすることができます。

> ℹ `-ldap-servers`フィールドは `-servers`フィールドを置き換えます。 `-ldap-servers`フィールドを使用して、LDAPサーバのホスト名またはIPアドレスのいずれかを指定できます。

4. admin権限レベルに戻ります： `set -privilege admin`

例

次のコマンドは、既存のLDAPクライアント構成「ldap_corp」を変更し、 netgroup.byhost「nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com」という名前のマップとデフォルトの検索範囲 `subtree`を使用して、ホストごとのネットグループ検索を有効にします：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

終了後の操作

クライアント アクセスの問題を回避するには、ディレクトリ内の `netgroup.byhost`と `netgroup`マップを常に同期しておく必要があります。

関連情報

"IETF RFC 5952：IPv6アドレステキスト表現に関する推奨事項"

ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する

ONTAP 9.11.1以降では、LDAP_ファスト バインド_機能（_コンカレント バインド_とも呼ばれます）を利用して、クライアント認証要求をより高速かつシンプルにすることができます。この機能を使用するには、LDAPサーバがファスト バインド機能をサポートしている必要があります。

タスク概要

高速バインドを使用しない場合、ONTAPはLDAP簡易バインドを使用してLDAPサーバで管理者ユーザを認証します。この認証方式では、ONTAPがLDAPサーバにユーザ名またはグループ名を送信し、サーバに格納されているハッシュ パスワードを受け取って、サーバ ハッシュ コードをユーザ パスワードから生成されたローカル ハッシュ パスコードと比較します。この2つが一致した場合、ONTAPはログイン権限を付与します。

高速バインド機能を使用する場合、ONTAPはセキュアな接続を介してLDAPサーバにユーザ クレデンシャル

（ユーザ名とパスワード）を送信するだけです。LDAPサーバは受け取ったクレデンシャルを検証し、ログイン権限を付与するようにONTAPに指示します。

高速バインドの利点の1つは、パスワードのハッシュ化はLDAPサーバで実行されるため、LDAPサーバでサポートされるすべての新しいハッシュ アルゴリズムをONTAPでサポートする必要がないことです。

"高速バインドの使用について説明します。"

LDAP高速バインドには、既存のLDAPクライアント設定を使用できます。ただし、パスワードがプレーン テキストでネットワークに送信されないように、LDAPクライアントにTLSまたはLDAPSを設定しておくことを強く推奨します。

ONTAP環境でLDAP高速バインドを有効にするには、次の要件を満たす必要があります。

- 高速バインドをサポートするLDAPサーバにONTAP管理者ユーザが設定されている必要があります。
- ONTAP SVMのネーム サービス スイッチ（nsswitch）データベースにLDAPが設定されている必要があります。
- ONTAP管理者ユーザおよびグループのアカウントに高速バインドを使用したnsswitch認証が設定されている必要があります。

手順

1. LDAP管理者に問い合わせて、LDAPサーバでLDAP高速バインドがサポートされていることを確認します。
2. LDAPサーバにONTAP管理者ユーザのクレデンシャルが設定されていることを確認します。
3. 管理SVMまたはデータSVMにLDAP高速バインドが正しく設定されていることを確認します。

   a. LDAP高速バインド サーバがLDAPクライアント設定にリストされていることを確認するには、次のように入力します。

      ```
      vserver services name-service ldap client show
      ```

      "LDAPクライアント設定については、こちらを参照してください。"

   b. `ldap`がnsswitch `passwd`データベースに設定されたソースの1つであることを確認するには、次のように入力します：

      ```
      vserver services name-service ns-switch show
      ```

   "nsswitchの設定については、こちらを参照してください。"

4. 管理者ユーザがnsswitchで認証されていること、および管理者のアカウントでLDAP高速バインド認証が有効になっていることを確認します。

   ◦ 既存のユーザーの場合は、 `security login modify`を入力して次のパラメータ設定を確認します：

      ```
      -authentication-method nsswitch

      -is-ldap-fastbind true
      ```

`security login modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

- 新しい管理者ユーザーの場合は、"LDAPまたはNIS ONTAPアカウントアクセスを有効にする"を参照してください。

ONTAP NFS SVMのLDAP統計を表示する

ストレージ システム上のStorage Virtual Machine（SVM）のLDAP統計を表示して、パフォーマンスを監視し、問題を診断できます。

開始する前に

- SVM に LDAP クライアントを設定しておく必要があります。
- データを表示できるLDAPオブジェクトを特定しておく必要があります。

手順

1. カウンタ オブジェクトのパフォーマンス データを表示します。

```
statistics show
```

例

次の例では、*smpl_1*というサンプルのカウンタ：avg_processor_busyとcpu_busyの統計を表示します。

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

関連情報

- "statistics show"

- "statistics start"
- "statistics stop"

ネーム マッピングの設定

ONTAP NAS SVMの名前マッピング構成について学習します

ONTAPでは、ネーム マッピングを使用して、SMB IDをUNIX IDに、Kerberos IDをUNIX IDに、UNIX IDをSMB IDにマッピングします。この情報は、NFSクライアントからの接続かSMBクライアントからの接続かに関係なく、ユーザ クレデンシャルを取得して適切なファイル アクセスを提供するために必要になります。

ネーム マッピングを使用する必要がない例外が2つあります。

- 純粋なUNIX環境を構成しており、ボリュームに対してSMBアクセスまたはNTFSセキュリティ形式を使用する予定がない場合。
- 代わりにデフォルト ユーザが使用されるように設定している場合。

  このシナリオでは、すべてのクライアント クレデンシャルをそれぞれマッピングするのではなく、すべてのクライアント クレデンシャルが同じデフォルト ユーザにマッピングされるため、ネーム マッピングは必要ありません。

ネーム マッピングはユーザに対してのみ使用でき、グループに対しては使用できません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、SALESという単語が先頭または末尾に付くすべてのADユーザを、特定のUNIXユーザおよびそのユーザのUIDにマッピングできます。

ONTAP NAS SVMの名前マッピングについて学ぶ

ONTAPがユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネーム マッピング データベースおよびLDAPサーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、SVMのネーム サービスの設定で決まります。

- WindowsからUNIXへのマッピングの場合

  マッピングが見つからなかった場合、小文字のWindowsユーザ名がUNIXドメインで有効なユーザ名かどうかを確認します。無効だった場合、デフォルトのUNIXユーザを使用します（設定済みの場合）。デフォルトのUNIXユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

- UNIXからWindowsへのマッピングの場合

  マッピングが見つからなかった場合、SMBドメインでUNIX名と一致するWindowsアカウントを探します。見つからない場合、デフォルトのSMBユーザを使用します（設定済みの場合）。デフォルトのSMBユーザが設定されておらず、この方法でもONTAPがマッピングを取得できない場合、マッピングは失敗し、エラーが返されます。

マシン アカウントは、デフォルトでは、指定されたデフォルトのUNIXユーザにマッピングされます。デフォルトのUNIXユーザが指定されていない場合、マシン アカウントのマッピングは失敗します。

- ONTAP 9.5以降では、マシン アカウントをデフォルトのUNIXユーザ以外のユーザにマッピングできます。
- ONTAP 9.4以前では、マシン アカウントを他のユーザにマッピングすることはできません。

  マシン アカウントに定義されているネーム マッピングがあっても無視されます。

ONTAP NAS SVM上の**UNIX**から**Windows**へのユーザ名マッピングのマルチドメイン検索

ONTAPは、UNIXユーザをWindowsユーザにマッピングする際のマルチドメイン検索をサポートしています。一致する結果が返されるまで、検出されたすべての信頼できるドメインで、変換後のパターンに一致する名前が検索されます。また、信頼できる優先ドメインのリストを設定することもできます。このリストは、検出された信頼できるドメインのリストの代わりに使用され、一致する結果が返されるまで順に検索されます。

ドメインの信頼性が**UNIX**ユーザから**Windows**ユーザへのネーム マッピング検索に与える影響

マルチドメインのユーザ名マッピングの仕組みを理解するには、ドメインの信頼性がONTAPに与える影響を理解しておく必要があります。SMBサーバのホーム ドメインとのActive Directory信頼関係は、双方向の信頼にすることも、インバウンドとアウトバウンドの2つのタイプがある単一方向の信頼のどちらかにすることもできます。ホーム ドメインは、SVMのSMBサーバが属しているドメインです。

- 双方向の信頼

  双方向の信頼では、両方のドメインが相互に信頼し合っています。SMBサーバのホーム ドメインが別のドメインと双方向の信頼関係にある場合、このホーム ドメインは信頼できるドメインに属しているユーザを認証および認可でき、その反対に、この信頼できるドメインはホーム ドメインに属しているユーザを認証および認可することができます。

  UNIXユーザからWindowsユーザへのネーム マッピング検索は、ホーム ドメインおよび他方のドメインとの間に双方向の信頼関係にあるドメインでのみ実行できます。

- アウトバウンド信頼

  アウトバウンドの信頼では、ホーム ドメインが他方のドメインを信頼しています。この場合、ホーム ドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

  UNIX ユーザから Windows ユーザ名へのマッピング検索を実行する場合、ホームドメインとのアウトバウンド信頼を持つドメインは検索_されません_。

- インバウンドトラスト

  インバウンドの信頼では、SMBサーバのホーム ドメインが他方のドメインによって信頼されています。この場合、ホーム ドメインはインバウンドの信頼できるドメインに属しているユーザを認証することも認可することもできません。

  UNIX ユーザから Windows ユーザ名へのマッピング検索を実行する場合、ホームドメインとのインバウンド信頼を持つドメインは検索_されません_。

ワイルドカード（*）を使用したネーム マッピングのためのマルチドメイン検索の設定方法

マルチドメイン ネーム マッピング検索は、Windowsユーザ名のドメイン セクションにワイルドカードを使用することで容易になります。次の表に、マルチドメイン検索を有効にするためにネーム マッピング エントリのドメイン部にワイルドカードを使用する方法を示します。

パターン	リプレースメント	結果
root	*\\管理者	UNIXユーザ「`root`」は「`administrator`」というユーザにマッピングされます。「`administrator`」という最初の一致するユーザが見つかるまで、すべての信頼されたドメインが順番に検索されます。
*	**	有効なUNIXユーザは対応するWindowsユーザにマッピングされます。該当する名前のユーザとの最初の一致が見つかるまで、すべての信頼できるドメインが順に検索されます。 パターン**は、UNIXからWindowsへの名前マッピングにのみ有効で、その逆には有効ではありません。

マルチドメインの名前検索の実行方法

マルチドメインの名前検索で使用する信頼できるドメインのリストを決定するために、次の2つの方法のどちらかを選択できます。

- ONTAPが作成した自動検出による双方向の信頼リストを使用する
- 自分で作成した信頼できる優先ドメイン リストを使用する

ユーザ名のドメイン セクションにワイルドカードを使用してUNIXユーザがWindowsユーザにマッピングされている場合、Windowsユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先のWindowsユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホーム ドメインと双方向の信頼関係にあるすべてのドメインでWindowsユーザの検索が行われます。
- ホーム ドメインと双方向の信頼関係にあるドメインが存在しない場合、ホーム ドメインでユーザの検索が行われます。

UNIXユーザがユーザ名にドメイン セクションのないWindowsユーザにマッピングされている場合は、ホーム ドメインでWindowsユーザの検索が行われます。

ONTAP NAS SVMの名前マッピング変換ルール

ONTAPシステムは、各SVMに対して一連の変換ルールを保持します。各ルールは、_パターン_と_置換_の2つの要素で構成されます。変換は適切なリストの先頭から開始され、最初に一致したルールに基づいて置換が実行されます。パターンはUNIX形式の正規表現です。置換は、UNIX `sed`プログラムと同様に、パターンの部分式を表すエスケープシーケンスを含む文字列です。

ONTAP NAS SVMの名前マッピングを作成する

`vserver name-mapping create`コマンドを使用してネームマッピングを作成できます。ネームマッピングを使用すると、Windowsユーザーが`UNIX`セキュリティ形式のボリュームにアクセスしたり、その逆を行ったりできるようになります。

タスク概要

各SVMについて、ONTAPは方向ごとに最大12,500の名前マッピングをサポートします。

手順

1. ネーム マッピングを作成します。

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```

> `-pattern`および `-replacement`ステートメントは正規表現として記述できます。また、 `-replacement`ステートメントを使用して、ヌル置換文字列 `""`（スペース文字）を使用することで、ユーザーへのマッピングを明示的に拒否することもできます。link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["ONTAPコマンドリファレンス"^]の `vserver name-mapping create`の詳細をご覧ください。

WindowsからUNIXへのマッピングが作成されると、新しいマッピングの作成時にONTAPシステムへの接続を開いているすべてのSMBクライアントは、新しいマッピングを確認するためにログアウトして再度ログインする必要があります。

例

次のコマンドは、SVM vs1 に名前マッピングを作成します。このマッピングは、UNIX から Windows へのマッピングであり、優先度リストの 1 番目に配置されます。このマッピングにより、UNIX ユーザー johnd が Windows ユーザー ENG\JohnDoe にマッピングされます。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

次のコマンドは、vs1という名前のSVMに別の名前マッピングを作成します。このマッピングは、優先順位リストの1番目の位置にあるWindowsからUNIXへのマッピングです。ここでは、パターンと置換に正規表現が含まれています。このマッピングは、ドメインENG内のすべてのCIFSユーザーを、SVMに関連付けられたLDAPドメイン内のユーザーにマッピングします。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

次のコマンドは、vs1という名前のSVMに別の名前マッピングを作成します。ここでのパターンには、エスケープする必要があるWindows ユーザー名の要素として「$」が含まれています。このマッピングにより、Windows ユーザーENG\ john$opsがUNIX ユーザーjohn_opsにマッピングされます。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

ONTAP NAS SVMのデフォルトユーザを設定する

ユーザに対する他のマッピングの試行がすべて失敗した場合や、UNIXとWindowsの間で個々のユーザをマッピングしないようにする場合に使用するデフォルト ユーザを設定できます。ただし、マッピングされていないユーザの認証を失敗にする必要がある場合は、デフォルト ユーザを設定しないでください。

タスク概要

CIFS認証で、各Windowsユーザを個別のUNIXユーザにマッピングしないようにする場合は、代わりにデフォルトのUNIXユーザを指定できます。

NFS認証で、各UNIXユーザを個別のWindowsユーザにマッピングしないようにする場合は、代わりにデフォルトのWindowsユーザを指定できます。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトのUNIXユーザを設定する	`vserver cifs options modify -default-unix-user user_name`

デフォルトのWindowsユーザを設定する	`vserver nfs modify -default-win-user user_name`

NFSネーム マッピングを管理するための**ONTAP**コマンド

ONTAPには、ネーム マッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
名前マッピングを作成する	`vserver name-mapping create`
特定の位置にネーム マッピングを挿入する	`vserver name-mapping insert`
ネーム マッピングを表示する	`vserver name-mapping show`
2 つの名前マッピングの位置を交換します。注：名前マッピングが ip-qualifier エントリで構成されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネーム マッピングを変更する	`vserver name-mapping modify`
ネーム マッピングを削除する	`vserver name-mapping delete`
ネーム マッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

`vserver name-mapping`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+name-mapping["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP SVMのWindows NFSクライアントのアクセスを有効にする

ONTAPはWindows NFSv3クライアントからのファイル アクセスをサポートします。NFSv3をサポートするWindowsオペレーティング システムを実行しているクライアントから、クラスタのNFSv3エクスポートのファイルにアクセスできます。この機能を正しく使用するには、Storage Virtual Machine（SVM）を適切に設定し、一定の要件と制限事項に注意する必要があります。

タスク概要

デフォルトでは、Windows NFSv3クライアントのサポートは無効になっています。

開始する前に

SVMでNFSv3を有効にする必要があります。

手順

1. Windows NFSv3クライアントのサポートを有効にします。

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly
   disabled
   ```

2. Windows NFSv3 クライアントをサポートするすべての SVM で、 `-enable-ejukebox`および `-v3-connection-drop`パラメータを無効にします：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
   -drop disabled
   ```

   これで、Windows NFSv3クライアントはストレージ システム上にエクスポートをマウントできるようになります。

3. `-o mtype=hard`オプションを指定して、各Windows NFSv3クライアントがハードマウントを使用するようにします。

   これは、マウントの信頼性を確保するために必要です。

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

ONTAP SVMのNFSクライアントでのエクスポートの表示を有効にする

NFSクライアントは、 `showmount -e`コマンドを使用して、ONTAPのNFSサーバから利用可能なエクスポートのリストを表示できます。これにより、ユーザーはマウントするファイルシステムを特定しやすくなります。

ONTAPでは、NFSクライアントがデフォルトでエクスポート リストを表示できます。以前のリリースでは、`vserver nfs modify`コマンドの `showmount`オプションを明示的に有効にする必要がありました。エクスポート リストを表示するには、SVMでNFSv3を有効にする必要があります。

例

次のコマンドは、vs1という名前のSVMのshowmount機能を表示します：

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

NFSクライアントで次のコマンドを実行すると、IPアドレス10.63.21.9のNFSサーバ上のエクスポートのリストが表示されます：

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

NFSを使用したファイル アクセスの管理

ONTAP SVMのNFSv3を有効または無効にする

`-v3`オプションを変更することで、NFSv3を有効または無効にできます。これにより、NFSv3プロトコルを使用するクライアントのファイルアクセスが可能になります。デフォルトでは、NFSv3は有効になっています。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
NFSv3の有効化	`vserver nfs modify -vserver vserver_name -v3 enabled`
NFSv3を無効にする	`vserver nfs modify -vserver vserver_name -v3 disabled`

ONTAP SVMのNFSv4.0を有効または無効にする

`-v4.0`オプションを変更することで、NFSv4.0を有効または無効にできます。これにより、NFSv4.0プロトコルを使用するクライアントからのファイルアクセスが可能になります。ONTAP 9.9.1では、NFSv4.0はデフォルトで有効になっていますが、それ以前のリリースではデフォルトで無効になっています。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.0の有効化	`vserver nfs modify -vserver vserver_name -v4.0 enabled`

状況	入力するコマンド
NFSv4.0を無効にする	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

ONTAP SVMのNFSv4.1を有効または無効にする

`-v4.1`オプションを変更することで、NFSv4.1を有効または無効にできます。これにより、NFSv4.1プロトコルを使用するクライアントからのファイルアクセスが可能になります。ONTAP 9.9.1では、NFSv4.1はデフォルトで有効になっていますが、それ以前のリリースではデフォルトで無効になっています。

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
NFSv4.1の有効化	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
NFSv4.1を無効にする	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

ONTAP NFSv4ストアプールの制限を管理する

ONTAP 9.13以降、管理者は、NFSv4サーバがクライアントごとのストアプール リソースの上限に達した場合に、NFSv4クライアントへのリソースの提供を拒否するようにNFSv4サーバを設定できます。クライアントがNFSv4ストアプール リソースを消費しすぎると、NFSv4ストアプール リソースが不足して他のNFSv4クライアントがブロックされる可能性があります。

この機能を有効にすると、ストアプール リソースのアクティブな消費状況をクライアントごとに表示することもできます。これにより、システム リソースを使い果たしているクライアントを特定しやすくなり、クライアントごとにリソース制限を課すことが可能になります。

消費済みストアプール リソース数の表示

この `vserver nfs storepool show`コマンドは、消費されたストアプールリソースの数を表示します。ストアプールは、NFSv4クライアントが使用するリソースのプールです。

手順

1. 管理者として、 `vserver nfs storepool show`コマンドを実行して、NFSv4クライアントのストアプール情報を表示します。

例

以下は、NFSv4クライアントのストアプール情報の例です。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

ストアプールの上限管理の有効化または無効化

管理者は、次のコマンドを使用して、ストアプールの上限管理を有効または無効にできます。

手順

1. 管理者として、次のいずれかの操作を実行します。

状況	入力するコマンド
ストアプールの上限管理を有効にする	`vserver nfs storepool config modify -limit-enforce enabled`
ストアプールの上限管理を無効にする	`vserver nfs storepool config modify -limit-enforce disabled`

ブロックされたクライアントのリストを表示する

ストアプールの上限管理を有効にすると、管理者は、クライアントごとに設定されたリソースしきい値に達してブロックされているクライアントを確認できます。管理者は次のコマンドを使用して、ブロックされているクライアントを確認できます。

手順

1. `vserver nfs storepool blocked-client show`コマンドを使用して、NFSv4のブロックされたクライアント リストを表示します。

ブロック済みクライアント リストからのクライアントの削除

クライアントごとに設定されたしきい値に達したクライアントは切断され、ブロッククライアント キャッシュに追加されます。管理者は次のコマンドを使用して、ブロッククライアント キャッシュからクライアントを削除できます。キャッシュから削除したクライアントは、ONTAP NFSv4サーバに接続できるようになります。

手順

1. `vserver nfs storepool blocked-client flush -client-ip <ip address>`コマンドを使用して、ストアプールのブロックされたクライアント キャッシュをフラッシュします。
2. `vserver nfs storepool blocked-client show`コマンドを使用して、クライアントがブロック クライアント キャッシュから削除されたことを確認します。

例

次の例では、IPアドレスが「10.2.1.1」のブロックされているクライアントを、すべてのノードからフラッシュしています。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

ONTAP SVMのpNFSを有効または無効にする

pNFSは、NFSクライアントがストレージデバイスに対して直接かつ並列に読み取り / 書き込み操作を実行できるようにすることでパフォーマンスを向上させ、潜在的なボトルネックとなるNFSサーバを回避します。pNFS（並列NFS）を有効または無効にするには、`-v4.1-pnfs`オプションを変更します。

ONTAPのリリース	pNFSのデフォルトの状態
9.8以降	無効
9.7以前	有効

開始する前に

pNFSを使用するには、NFSv4.1のサポートが必要です。

pNFSを有効にする場合は、まずNFSリファーラルを無効にする必要があります。両方を同時に有効にすることはできません。

SVMでpNFSとKerberosを併用する場合は、SVM上のすべてのLIFでKerberosを有効にする必要があります。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
pNFSを有効にする	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFSを無効にする	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

関連情報

- NFSトランキングの概要

ONTAP SVMのTCPおよびUDP経由のNFSアクセスを制御する

`-tcp`パラメータおよび `-udp`パラメータを変更することで、TCPおよびUDP経由のStorage Virtual Machine（SVM）へのNFSアクセスを有効または無効にすることができます。これにより、環境内のNFSクライアントがTCP経由またはUDP経由でデータにアクセスできるかどうかを制御できます。

タスク概要

これらのパラメータはNFSのみに適用されます。補助プロトコルには適用されません。たとえば、TCP経由のNFSを無効にしても、TCP経由のマウント処理は引き続き実行できます。TCPまたはUDPトラフィックを完全にブロックするには、エクスポート ポリシー ルールを使用できます。

NFSのTCPを無効にしてコマンド失敗エラーを回避するには、SnapDiff RPCサーバーをオフにする必要があります。TCPを無効にするには、コマンド `vserver snapdiff-rpc-server off -vserver vserver name`を使用します。

手順

1. 次のいずれかを実行します。

NFSアクセスを可能にするには...	コマンドを入力してください...
TCP経由で有効化	`vserver nfs modify -vserver vserver_name -tcp enabled`
TCP経由で無効化	`vserver nfs modify -vserver vserver_name -tcp disabled`
UDP経由で有効化	`vserver nfs modify -vserver vserver_name -udp enabled`

UDP経由で無効化	`vserver nfs modify -vserver vserver_name -udp disabled`

ONTAP SVMの予約されていないポートからのNFS要求を制御する

`-mount-rootonly`オプションを有効にすると、予約されていないポートからのNFSマウント要求を拒否できます。予約されていないポートからのすべてのNFS要求を拒否するには、`-nfs-rootonly`オプションを有効にします。

タスク概要

デフォルトでは、オプション`-mount-rootonly`は`enabled`です。

デフォルトでは、オプション`-nfs-rootonly`は`disabled`です。

これらのオプションは、NULLプロシージャには適用されません。

手順

1. 次のいずれかを実行します。

状況	コマンドを入力してください...
非予約ポートからのNFSマウント要求を許可する	`vserver nfs modify -vserver vserver_name -mount-rootonly disabled`
非予約ポートからのNFSマウント要求を拒否する	`vserver nfs modify -vserver vserver_name -mount-rootonly enabled`
非予約ポートからのすべてのNFS要求を許可する	`vserver nfs modify -vserver vserver_name -nfs-rootonly disabled`
非予約ポートからのすべてのNFS要求を拒否する	`vserver nfs modify -vserver vserver_name -nfs-rootonly enabled`

不明なUNIXユーザーによるONTAP NTFSボリュームまたはqtreeへのNFSアクセスを処理する

ONTAPは、NTFSセキュリティ形式のボリュームまたはqtreeへの接続を試みるUNIXユーザを識別できない場合、そのユーザをWindowsユーザに明示的にマッピングできません。このよう場合、そのユーザのアクセスを拒否してセキュリティを厳しくすることも、デフォルトのWindowsユーザにマッピングしてすべてのユーザに最低レベルのアクセスを保証することもできます。

開始する前に

このオプションを有効にする場合は、デフォルトのWindowsユーザを設定しておく必要があります。

タスク概要

UNIXユーザがNTFSセキュリティ形式のボリュームまたはqtreeへのアクセスを試みた場合、ONTAPがNTFSアクセス権を適切に評価できるように、まずそのUNIXユーザがWindowsユーザにマッピングされる必要があります。ただし、ONTAPが設定されているユーザ情報ネーム サービス ソースでそのUNIXユーザの名前をルックアップできなかった場合、特定のWindowsユーザにそのUNIXユーザを明示的にマッピングすることができません。このような不明なUNIXユーザは、次のいずれかの方法で処理できます。

- 不明なUNIXユーザに対してアクセスを拒否する。

  NTFS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ユーザに明示的なマッピングを要求することで、より厳しいセキュリティを適用します。

- 不明なUNIXユーザをデフォルトのWindowsユーザにマッピングする。

  セキュリティ性は低下しますが、すべてのユーザがデフォルトのWindowsユーザとしてNTFSボリュームまたはqtreeへの最低レベルのアクセスが保証されるため、利便性が向上します。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

不明な UNIX ユーザーにデフォルトの Windows ユーザーを指定したい場合…	コマンドを入力してください…
有効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
無効	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

予約されていないポートに **ONTAP NFS** エクスポートをマウントするクライアントに関する考慮事項

`-mount-rootonly`オプションは、ユーザーが`root`としてログインしている場合でも、予約されていないポートを使用して`NFS`エクスポートをマウントするクライアントをサポートする必要があるストレージシステムでは無効にする必要があります。このようなクライアントには、`Hummingbird`クライアントや`Solaris NFS/IPv6`クライアントが含まれます。

`-mount-rootonly`オプションを有効にすると、
ONTAPでは、予約されていないポート（つまり、1,023より大きい番号のポート）を使用するNFSクライアントがNFSエクスポートをマウントすることを許可しません。

ONTAP NFS SVMのドメインを検証することで、ネットグループに対するより厳格なアクセス チェックを実行します

デフォルトでは、ONTAPはネットグループへのクライアント アクセスを評価する際に追加の検証を実行します。この追加チェックにより、クライアントのドメインがStorage Virtual Machine（SVM）のドメイン設定と一致しているかどうかが確認されます。一致しない場合、ONTAPはクライアント アクセスを拒否します。

タスク概要

ONTAPがクライアント アクセスのエクスポート ポリシー ルールを評価する際、エクスポート ポリシー ルールにネットグループが含まれている場合、ONTAPはクライアントのIPアドレスがそのネットグループに属しているかどうかを判断する必要があります。このため、ONTAPはDNSを使用してクライアントのIPアドレスをホスト名に変換し、完全修飾ドメイン名（FQDN）を取得します。

ネットグループ ファイルにホストの短い名前のみがリストされ、そのホストの短い名前が複数のドメインに存在する場合、異なるドメインのクライアントがこのチェックなしでアクセスを取得できる可能性があります。

これを防ぐため、ONTAPはホストのDNSから返されたドメインを、SVMに設定されているDNSドメイン名のリストと比較します。一致する場合はアクセスが許可されます。一致しない場合はアクセスが拒否されます。

この検証はデフォルトで有効になっています。 `-netgroup-dns-domain-search`パラメータを変更することで管理できます。このパラメータは高度な権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

ネットグループのドメイン検証を行う場合は...	入力する内容
有効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
無効	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 権限レベルをadminに設定します。

   ```
   set -privilege admin
   ```

ONTAP SVMのNFSv3サービスに使用されるポートを変更する

ストレージ システムのNFSサーバは、マウント デーモンやNetwork Lock Manager（NLM;ネットワーク ロック マネージャ）のようなサービスを使用して、特定のデフォルト ネットワーク ポートを介してNFSクライアントと通信します。デフォルト ポートは、ほとんどのNFS環境で正しく機能するので変更する必要はありませんが、別のネットワーク ポートをNFSv3環境で使用したい場合はそうすることができます。

開始する前に

ストレージ システムでNFSポートを変更するには、すべてのNFSクライアントがシステムに再接続する必要があるので、変更に先立ってこの情報をユーザに伝えておく必要があります。

タスク概要

NFSマウント デーモン、Network Lock Manager（NLM;ネットワーク ロック マネージャ）、Network Status Monitor（NSM;ネットワーク ステータス モニタ）、およびNFSクォータ デーモンの各サービスで使用されるポートをStorage Virtual Machine（SVM）ごとに設定できます。ポート番号の変更は、データへのアクセスにTCPとUDPのどちらを使用するNFSクライアントにも影響を与えます。

NFSv4およびNFSv4.1のポートは変更できません。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. NFSへのアクセスを無効にします。

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. 特定のNFSサービスのNFSポートを設定します。

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFSポートパラメータ	概要	デフォルトのポート
-mountd-port	NFSマウント デーモン	635
-nlm-port	ネットワーク ロック マネージャ	4045
-nsm-port	ネットワーク ステータス モニタ	4046
-rquotad-port	NFSクォータ デーモン	4049

   デフォルト ポートに加えて、1,024～65,535の範囲のポート番号を使用できます。各NFSサービスは固有のポートを使用する必要があります。

4. NFSへのアクセスを有効にします。

```
vserver nfs modify -vserver vserver_name -access true
```

5. `network connections listening show`コマンドを使用してポート番号の変更を確認します。

   `network connections listening show`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-connections-listening-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

6. admin権限レベルに戻ります。

```
set -privilege admin
```

例
次のコマンドは、vs1というSVMでNFSマウント デーモンのポートを1113に設定します。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

NFSサーバを管理するためのONTAPコマンド

ONTAPには、NFSサーバを管理するためのコマンドが用意されています。

状況	使用するコマンド
NFSサーバを作成する	`vserver nfs create`
NFSサーバを表示する	`vserver nfs show`
NFSサーバを変更する	`vserver nfs modify`
NFSサーバを削除する	`vserver nfs delete`
NFSv3マウントポイントの下の`.snapshot`ディレクトリリストを非表示にする オプションが有効になっている場合でも、`.snapshot`ディレクトリへの明示的なアクセスは引き続き許可されます。	`vserver nfs `-v3-hide-snapshot`オプションが有効になっているコマンド

`vserver nfs`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+nfs["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP NAS SVMのネーム サービスの問題のトラブルシューティング

名前サービスの問題によりクライアントでアクセス障害が発生した場合、`vserver services name-service getxxbyyy`コマンド ファミリを使用してさまざまな名前サービス検索を手動で実行し、検索の詳細と結果を調べてトラブルシューティングに役立てることができます。

タスク概要

- 各コマンドでは、次の情報を指定できます。
  - 検索を実行するノードまたはStorage Virtual Machine（SVM）の名前。

    特定のノードまたはSVMでネーム サービス ルックアップをテストして、ネーム サービス設定の問題の調査対象を絞り込むことができます。
  - 検索に使用されたソースを表示するかどうか。

    適切なソースが使用されたかどうかをチェックできます。
- ルックアップを実行するサービスは、設定されているネーム サービス スイッチの順序に基づいて選択されます。
- これらのコマンドはadvanced権限レベルで使用できます。

手順

1. 次のいずれかを実行します。

…を取得するには	使用するコマンド
ホスト名のIPアドレス	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname`（IPv4アドレスのみ）
グループのメンバー（グループIDを指定）	`vserver services name-service getxxbyyy getgrbygid`
グループのメンバー（グループ名を指定）	`vserver services name-service getxxbyyy getgrbyname`
ユーザが属しているグループのリスト	`vserver services name-service getxxbyyy getgrlist`
IPアドレスのホスト名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr`（IPv4アドレスのみ）
ユーザ情報（ユーザ名を指定）	`vserver services name-service getxxbyyy getpwbyname` `-use-rbac`パラメータを `true`として指定することで、RBACユーザの名前解決をテストできます。
ユーザ情報（ユーザIDを指定）	`vserver services name-service getxxbyyy getpwbyuid` `-use-rbac`パラメータを `true`として指定することで、RBACユーザの名前解決をテストできます。
クライアントのネットグループ メンバーシップ	`vserver services name-service getxxbyyy netgrp`
クライアントのネットグループ メンバーシップ（ホスト単位のネットグループ検索を使用）	`vserver services name-service getxxbyyy netgrpbyhost`

次の例は、ホストacast1.eng.example.comのIPアドレスを取得することでSVM vs1のDNSルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

次の例は、UIDが501768のユーザのユーザ情報を取得することでSVM vs1のNISルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

次の例は、ldap1というユーザのユーザ情報を取得することでSVM vs1のLDAPルックアップをテストします。

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

次の例は、クライアントdnshost0がネットグループlnetgroup136のメンバーであるかどうかを調べることでSVM vs1のネットグループ検索をテストします。

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 実行したテストの結果を分析し、必要な措置を取ります。

もし...	...を確認してください。
ホスト名またはIPアドレスのルックアップに失敗したか、正しくない結果が返された	DNS設定
正しくないソースでルックアップが実行された	ネーム サービス スイッチの設定
ユーザまたはグループのルックアップに失敗したか、正しくない結果が返された	• ネーム サービス スイッチの設定 • ソースの設定（ローカル ファイル、NISドメイン、LDAPクライアント） • ネットワーク設定（LIF、ルートなど）
ホスト名のルックアップに失敗したかタイムアウトになり、DNSの短縮名（例：host1）がDNSサーバで解決されない	トップレベル ドメイン（TLD）クエリのDNS設定。 `-is-tld-query-enabled false`オプションを`vserver services name-service dns modify`コマンドに使用して、TLDクエリを無効にすることができます。

関連情報

"NetAppテクニカル レポート4668：『Name Services Best Practices Guide』"

ONTAP NAS SVMのネーム サービス接続を確認する

DNSおよびLightweight Directory Access Protocol（LDAP）ネームサーバがONTAPに接続されていることを確認できます。これらのコマンドは管理者権限レベルで使用できます。

タスク概要

DNSまたはLDAPネーム サービスの設定が有効かどうかは、必要時にネーム サービス設定チェックを使用して確認できます。この検証チェックは、コマンドラインまたはSystem Managerで実行できます。

DNS設定の場合、すべてのサーバがテストされ、動作している必要があり、設定が有効とみなされます。LDAP設定の場合、いずれかのサーバが稼働していれば設定は有効です。ネーム サービス コマンドは、`skip-config-validation`フィールドがtrue（デフォルトはfalse）でない限り、設定チェッカーを適用します。

手順

1. 適切なコマンドを使用してネーム サービスの設定を確認します。設定されているサーバのステータスがUIに表示されます。

確認するには...	使用するコマンド
DNSの設定ステータス	`vserver services name-service dns check`

LDAPの設定ステータス	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                 |
| Client Configuration Name: c1                                |
| LDAP Status: up                                              |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                 |
```

設定されているサーバ（name-servers/ldap-servers）の少なくとも1つが到達可能でサービスを提供していれば、設定の検証は成功です。到達不能なサーバがある場合、警告が表示されます。

NASネーム サービス スイッチエントリを管理するためのONTAPコマンド

ネーム サービス スイッチ エントリは、作成、表示、変更、削除の操作によって管理することができます。

状況	使用するコマンド
ネーム サービス スイッチ エントリを作成する	`vserver services name-service ns-switch create`
ネーム サービス スイッチ エントリを表示する	`vserver services name-service ns-switch show`
ネーム サービス スイッチ エントリを変更する	`vserver services name-service ns-switch modify`
ネーム サービス スイッチ エントリを削除する	`vserver services name-service ns-switch delete`

`vserver services name-service ns-switch`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+ns-switch["ONTAPコマンド リファレンス"^]をご覧ください。

関連情報

"NetAppテクニカル レポート4668：『Name Services Best Practices Guide』"

NASネーム サービス キャッシュを管理するためのONTAPコマンド

ネーム サービス キャッシュは、Time-To-Live（TTL）値を変更することで管理できます。TTL値は、ネーム サービス情報がキャッシュに保持される期間です。

TTL値を変更する場合…	使用するコマンド
UNIXユーザ	`vserver services name-service cache unix-user settings`
UNIXグループ	`vserver services name-service cache unix-group settings`
UNIXネットグループ	`vserver services name-service cache netgroups settings`
ホスト	`vserver services name-service cache hosts settings`
グループ メンバーシップ	`vserver services name-service cache group-membership settings`

関連情報

"ONTAPコマンド リファレンス"

NFSネーム マッピングを管理するためのONTAPコマンド

ONTAPには、ネーム マッピングを管理するためのコマンドが用意されています。

状況	使用するコマンド
名前マッピングを作成する	`vserver name-mapping create`
特定の位置にネーム マッピングを挿入する	`vserver name-mapping insert`
ネーム マッピングを表示する	`vserver name-mapping show`

2 つの名前マッピングの位置を交換します。注：名前マッピングが ip-qualifier エントリで構成されている場合、スワップは許可されません。	`vserver name-mapping swap`
ネーム マッピングを変更する	`vserver name-mapping modify`
ネーム マッピングを削除する	`vserver name-mapping delete`
ネーム マッピングが正しいことを確認する	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

`vserver name-mapping`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+name-mapping["ONTAPコマンド リファレンス"^]を参照してください。

NASローカルUNIXユーザーを管理するためのONTAPコマンド

ONTAPには、ローカルUNIXユーザを管理するためのコマンドが用意されています。

状況	使用するコマンド
ローカルUNIXユーザーを作成する	`vserver services name-service unix-user create`
URIからローカルUNIXユーザをロードする	`vserver services name-service unix-user load-from-uri`
ローカルUNIXユーザを表示する	`vserver services name-service unix-user show`
ローカルUNIXユーザーを変更する	`vserver services name-service unix-user modify`
ローカルUNIXユーザを削除する	`vserver services name-service unix-user delete`

`vserver services name-service unix-user`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+unix-user["ONTAPコマンド リファレンス"^]をご覧ください。

NASローカルUNIXグループを管理するためのONTAPコマンド

ONTAPには、ローカルUNIXグループを管理するためのコマンドが用意されています。

状況	使用するコマンド
ローカルUNIXグループを作成する	`vserver services name-service unix-group create`
ローカルUNIXグループにユーザを追加する	`vserver services name-service unix-group adduser`
URIからローカルUNIXグループをロードする	`vserver services name-service unix-group load-from-uri`
ローカルUNIXグループを表示する	`vserver services name-service unix-group show`
ローカルUNIXグループを変更する	`vserver services name-service unix-group modify`
ローカルUNIXグループからユーザを削除する	`vserver services name-service unix-group deluser`
ローカルUNIXグループを削除する	`vserver services name-service unix-group delete`

`vserver services name-service unix-group`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+unix-group["ONTAPコマンドリファレンス"^]をご覧ください。

ONTAP NFS SVMのローカルUNIXユーザ、グループ、グループメンバの制限

ONTAPでは、クラスタ内のUNIXユーザとグループの最大数に制限を設け、これらの制限を管理するためのコマンドを導入しました。これらの制限により、管理者がクラスタ内にローカルUNIXユーザとグループを過剰に作成することを防ぎ、パフォーマンスの問題を回避できます。

ローカルUNIXユーザーグループとグループメンバーの合計数には制限があります。ローカルUNIXユーザーには別の制限があります。これらの制限はクラスタ全体に適用されます。これらの新しい制限はそれぞれデフォルト値に設定されており、事前に割り当てられたハード リミットまで変更できます。

データベース	デフォルトの制限	ハード リミット
ローカルUNIXユーザ	32,768	65,536
ローカルUNIXグループおよびグループ メンバー	32,768	65,536

ONTAP NFS SVMのローカルUNIXユーザとグループの制限を管理する

ローカルUNIXユーザとグループの制限を管理するためのONTAP専用コマンドがあります。クラスタ管理者はこれらのコマンドを使用して、ローカルUNIXユーザとグループの数が多すぎることに起因すると思われるクラスタのパフォーマンス問題をトラブルシューティングできます。

タスク概要

これらのコマンドは、advanced権限レベルのクラスタ管理者が使用できます。

手順

1. 次のいずれかを実行します。

状況	使用するコマンド
ローカルUNIXユーザー制限に関する情報を表示する	`vserver services unix-user max-limit show`
ローカルUNIXグループの制限に関する情報を表示する	`vserver services unix-group max-limit show`
ローカルUNIXユーザ制限の変更	`vserver services unix-user max-limit modify`
ローカルUNIXグループの制限を変更する	`vserver services unix-group max-limit modify`

`vserver services unix`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+unix["ONTAPコマンドリファレンス"^]を参照してください。

NFSローカルネットグループを管理するためのONTAPコマンド

URIからのロード、ノード間でのステータスの確認、表示や削除を行うことで、ローカル ネットグループを管理することができます。

状況	使用するコマンド
URIからネットグループをロードする	`vserver services name-service netgroup load`
ノード間でのネットグループのステータスを確認する	`vserver services name-service netgroup status` advanced権限レベル以上で使用できます。

ローカル ネットグループを表示する	`vserver services name-service netgroup file show`
ローカル ネットグループを削除する	`vserver services name-service netgroup file delete`

`vserver services name-service netgroup file`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+netgroup+file["ONTAPコマンドリファレンス"^]をご覧ください。

NFS NISドメイン構成を管理するためのONTAPコマンド

ONTAPには、NISドメイン設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NISドメイン設定を作成する	`vserver services name-service nis-domain create`
NISドメイン設定を表示する	`vserver services name-service nis-domain show`
NISドメイン設定のバインド ステータスを表示する	`vserver services name-service nis-domain show-bound`
NISの統計を表示する	`vserver services name-service nis-domain show-statistics` 高度な権限レベル以上で利用できます。
NISの統計をクリアする	`vserver services name-service nis-domain clear-statistics` 高度な権限レベル以上で利用できます。
NISドメイン設定を変更する	`vserver services name-service nis-domain modify`
NISドメイン設定を削除する	`vserver services name-service nis-domain delete`
ホスト単位のネットグループ検索でのキャッシュを有効にする	`vserver services name-service nis-domain netgroup-database config modify` 高度な権限レベル以上で利用できます。

`vserver services name-service nis-domain`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+nis-domain["ONTAPコマンドリファレンス"^]をご覧ください。

NFS LDAPクライアント構成を管理するためのONTAPコマンド

ONTAPには、LDAPクライアント設定を管理するためのコマンドが用意されています。

SVM管理者は、クラスタ管理者が作成したLDAPクライアント設定を変更したり削除したりできません。

状況	使用するコマンド
LDAPクライアント構成を作成する	`vserver services name-service ldap client create`
LDAPクライアント設定を表示する	`vserver services name-service ldap client show`
LDAPクライアント設定を変更する	`vserver services name-service ldap client modify`
LDAPクライアントのバインド パスワードを変更する	`vserver services name-service ldap client modify-bind-password`
LDAPクライアント設定を削除する	`vserver services name-service ldap client delete`

`vserver services name-service ldap client`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+ldap+client["ONTAPコマンドリファレンス"^]をご覧ください。

NFS LDAP 構成を管理するための ONTAP コマンド

ONTAPには、LDAP設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LDAP設定を作成する	`vserver services name-service ldap create`
LDAP設定を表示する	`vserver services name-service ldap show`
LDAP設定を変更する	`vserver services name-service ldap modify`
LDAP設定を削除する	`vserver services name-service ldap delete`

`vserver services name-service ldap`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+ldap["ONTAPコマンド リファレンス"^]をご覧ください。

NFS LDAPクライアント スキーマ テンプレートを管理するためのONTAPコマンド

ONTAPには、LDAPクライアント スキーマ テンプレートを管理するためのコマンドが用意されています。

SVM管理者は、クラスタ管理者が作成したLDAPクライアント スキーマを変更したり削除したりできません。

状況	使用するコマンド
既存のLDAPスキーマ テンプレートをコピーする	`vserver services name-service ldap client schema copy` 高度な権限レベル以上で利用できます。
LDAPスキーマ テンプレートを表示する	`vserver services name-service ldap client schema show`
LDAPスキーマ テンプレートを変更する	`vserver services name-service ldap client schema modify` 高度な権限レベル以上で利用できます。
LDAPスキーマ テンプレートを削除する	`vserver services name-service ldap client schema delete` 高度な権限レベル以上で利用できます。

`vserver services name-service ldap client schema`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+services+name-service+ldap+client+schema["ONTAPコマンド リファレンス"^]をご覧ください。

NFS Kerberos インターフェース構成を管理するための ONTAP コマンド

ONTAPには、NFS Kerberosインターフェイスの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
LIFでNFS Kerberosを有効にする	`vserver nfs kerberos interface enable`

NFS Kerberosインターフェイスの設定を表示する	`vserver nfs kerberos interface show`
NFS Kerberosインターフェイスの設定を変更する	`vserver nfs kerberos interface modify`
LIFでNFS Kerberosを無効にする	`vserver nfs kerberos interface disable`

`vserver nfs kerberos interface`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+nfs+kerberos+interface["ONTAPコマンドリファレンス"^]をご覧ください。

NFS Kerberos レルム構成を管理するための ONTAP コマンド

ONTAPには、NFS Kerberos Realmの設定を管理するためのコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realmの設定を作成する	`vserver nfs kerberos realm create`
NFS Kerberos Realmの設定を表示する	`vserver nfs kerberos realm show`
NFS Kerberos Realmの設定を変更する	`vserver nfs kerberos realm modify`
NFS Kerberos Realmの設定を削除する	`vserver nfs kerberos realm delete`

`vserver nfs kerberos realm`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+nfs+kerberos+realm["ONTAPコマンド リファレンス"^]をご覧ください。

エクスポート ポリシーを管理するための**ONTAP**コマンド

ONTAPには、エクスポート ポリシーを管理するためのコマンドが用意されています。

状況	使用するコマンド

エクスポート ポリシーに関する情報を表示する	`vserver export-policy show`
エクスポート ポリシーの名前を変更する	`vserver export-policy rename`
エクスポート ポリシーをコピーする	`vserver export-policy copy`
エクスポート ポリシーを削除する	`vserver export-policy delete`

`vserver export-policy`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+export-policy["ONTAPコマンドリファレンス"^]をご覧ください。

エクスポート ルールを管理するための**ONTAP**コマンド

ONTAPには、エクスポート ルールを管理するためのコマンドが用意されています。

状況	使用するコマンド
エクスポート ルールを作成する	`vserver export-policy rule create`
エクスポート ルールに関する情報を表示する	`vserver export-policy rule show`
エクスポート ルールを変更する	`vserver export-policy rule modify`
エクスポート ルールを削除する	`vserver export-policy rule delete`

異なるクライアントを照合する同一のエクスポート ルールが複数設定されている場合は、エクスポート ルールの管理時にそれらのルールの同期を必ず維持するようにしてください。

`vserver export-policy`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+export-policy["ONTAPコマンドリファレンス"^]をご覧ください。

NFSクレデンシャル キャッシュの設定

ONTAP SVMの**NFS**認証情報キャッシュの有効期限を変更する理由

ONTAPは、NFSエクスポートアクセスのユーザ認証に必要な情報を認証情報キャッシュ

に保存することで、アクセス速度の向上とパフォーマンスの向上を実現します。認証情報キャッシュへの情報の保存期間を設定して、環境に合わせてカスタマイズできます。

NFS 認証情報キャッシュの TTL （Time-To-Live） を変更すると問題解決に役立つシナリオがいくつかあります。これらのシナリオと、変更を行った場合の結果を理解しておく必要があります。

理由

次の状況では、デフォルトの TTL を変更することを検討してください：

問題	是正措置
ご使用の環境内のネームサーバーでは、ONTAPからの大量のリクエストによりパフォーマンスが低下しています。	キャッシュされている受理および拒否されたクレデンシャルのTTLを長くして、ONTAPからネーム サーバへの要求数を減らします。
ネーム サーバ管理者がこれまで拒否されていたNFSユーザのアクセスを許可する変更を行った。	キャッシュされている拒否されたクレデンシャルのTTLを短くして、ONTAPが外部ネーム サーバに新しいクレデンシャルを要求してNFSユーザがアクセスできるようになるまでの時間を短縮します。
ネーム サーバ管理者がこれまで許可されていたNFSユーザのアクセスを拒否する変更を行った。	キャッシュされている受理されたクレデンシャルのTTLを短くして、ONTAPが外部ネーム サーバに新しいクレデンシャルを要求してNFSユーザがアクセスを拒否されるようになるまでの時間を短縮します。

結果

受理されたクレデンシャルと拒否されたクレデンシャルそれぞれについて、キャッシュ期間を変更することができます。ただし、変更によるメリットとデメリットの両方に注意する必要があります。

状況	利点は...	デメリットは...
受理されたクレデンシャルのキャッシュ時間を長くする	ONTAPがクレデンシャルの要求をネーム サーバに送信する回数が減って、ネーム サーバの負荷が軽減されます。	アクセスが許可されなくなったNFSユーザが実際にアクセスを拒否されるまでの時間が長くなります。
受理されたクレデンシャルのキャッシュ時間を短くする	アクセスが許可されなくなったNFSユーザが実際にアクセスを拒否されるまでの時間が短くなります。	ONTAPがクレデンシャルの要求をネーム サーバに送信する回数が増えて、ネーム サーバの負荷が増大します。
ネガティブクレデンシャルのキャッシュ時間を増やす	ONTAPがクレデンシャルの要求をネーム サーバに送信する回数が減って、ネーム サーバの負荷が軽減されます。	アクセスが許可されるようになったNFSユーザが実際にアクセスを許可されるまでの時間が長くなります。

状況	利点は...	デメリットは...
ネガティブクレデンシャルキャッシュ時間を短縮する	アクセスが許可されるようになったNFSユーザが実際にアクセスを許可されるまでの時間が短くなります。	ONTAPがクレデンシャルの要求をネーム サーバに送信する回数が増えて、ネーム サーバの負荷が増大します。

ONTAP SVMのキャッシュされた**NFS**ユーザー認証情報の有効期限を設定する

Storage Virtual Machine（SVM）のNFSサーバを変更することで、ONTAPがNFSユーザのクレデンシャルを内部キャッシュに格納する期間であるTime-To-Live（TTL）を設定できます。これにより、ネーム サーバの高負荷に関する問題や、NFSユーザ アクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

タスク概要

これらのパラメータはadvanced権限レベルで使用できます。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

キャッシュされたデータのTTLを変更したい場合は...	使用するコマンド
受理のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTLはミリ秒単位で測定されます。ONTAP 9.10.1以降では、デフォルトは1時間（3,600,000ミリ秒）です。ONTAP 9.9.1以前では、デフォルトは24時間（86,400,000ミリ秒）です。この値の許容範囲は、1分（60000ミリ秒）から7日間（604,800,000ミリ秒）です。
拒否のクレデンシャル	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTLはミリ秒単位で測定されます。デフォルトは2時間（7,200,000ミリ秒）です。この値の許容範囲は1分（60,000ミリ秒）から7日間（604,800,000ミリ秒）です。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

エクスポート ポリシー キャッシュの管理

ONTAP NAS SVMのエクスポート ポリシー キャッシュをフラッシュする

ONTAPは、エクスポートポリシー関連情報を保存するために複数のエクスポートポリシーキャッシュを使用し、アクセスを高速化します。エクスポートポリシーキャッシュを手動でフラッシュする(`vserver export-policy cache flush`と、古くなった可能性のある情報が削除され、ONTAPが適切な外部リソースから最新の情報を取得するようになります。これにより、NFSエクスポートへのクライアントアクセスに関連するさまざまな問題を解決できます。

タスク概要

エクスポート ポリシー キャッシュ情報は、次の理由により古くなっている可能性があります：

- エクスポート ポリシー ルールが最近変更された
- ネーム サーバでホスト名のレコードが最近変更された
- ネーム サーバでネットグループ エントリが最近変更された
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリが行われた

手順

1. ネーム サービス キャッシュが有効になっていない場合は、アドバンス特権モードで次のいずれかのアクションを実行します：

フラッシュする場合...	コマンドを入力してください...
すべてのエクスポート ポリシー キャッシュ（showmount を除く）	`vserver export-policy cache flush -vserver vserver_name`
エクスポート ポリシー ルール アクセス キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access`オプションの `-node`パラメータを含めて、アクセス キャッシュをフラッシュするノードを指定できます。
ホスト名キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache host`
ネットグループ キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache netgroup`ネットグループの処理はリソースを大量に消費します。古いネットグループが原因で発生したクライアント アクセスの問題を解決する場合にのみ、ネットグループ キャッシュをフラッシュしてください。
showmountキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. 名前サービス キャッシュが有効になっている場合は、次のいずれかのアクションを実行します：

フラッシュする場合...	コマンドを入力してください...
エクスポート ポリシー ルール アクセス キャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache access`オプションの `-node` パラメータを含めて、アクセス キャッシュをフラッシュするノードを指定できます。
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`
ネットグループ キャッシュ	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all`ネットグループの処理はリソースを大量に消費します。古いネットグループが原因で発生したクライアント アクセスの問題を解決する場合にのみ、ネットグループ キャッシュをフラッシュしてください。
showmountキャッシュ	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

ONTAP NFS SVMのエクスポート ポリシー ネットグループ キューとキャッシュを表示します。

ONTAPは、ネットグループのインポートおよび解決時にネットグループキューを使用し、結果情報をネットグループキャッシュに保存します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングする際には、 `vserver export-policy netgroup queue show`コマンドと `vserver export-policy netgroup cache show`コマンドを使用して、ネットグループキューのステータスとネットグループキャッシュの内容を表示できます。

手順

1. 次のいずれかを実行します。

エクスポートポリシーネットグループを表示するには...	コマンドを入力してください...
キュー	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

`vserver export-policy netgroup`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+export-policy+netgroup["ONTAPコマンドリファレンス"^]をご覧ください。

クライアントIPアドレスがONTAP NFSネットグループのメンバーであるかどうかを確認する

ネットグループに関連する NFS クライアント アクセスの問題をトラブルシューティングする場合、 `vserver export-policy netgroup check-membership`コマンドを使用して、クライアント IP が特定のネットグループのメンバーであるかどうかを判断できます。

タスク概要

ネットグループのメンバーシップを確認することで、ONTAPがクライアントがネットグループのメンバーであるかどうかを認識しているかどうかを判断できます。また、ネットグループ情報の更新中にONTAPのネットグループ キャッシュが一時的な状態にあるかどうかも確認できます。この情報は、クライアントが予期せずアクセスを許可または拒否される理由を理解するのに役立ちます。

手順

1. クライアント IP アドレスのネットグループ メンバーシップを確認します： `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   このコマンドは次の結果を返します：

   - クライアントはネットグループのメンバーです。

     これは、逆引きスキャンまたはnetgroup-by-host検索によって確認されました。

   - クライアントはネットグループのメンバーです。

     ONTAPネットグループ キャッシュで見つかりました。

   - クライアントはネットグループのメンバーではありません。
   - ONTAPが現在ネットグループ キャッシュを更新中のため、クライアントのメンバーシップをまだ判別できません。

     これが完了するまでは、メンバーシップを明示的に判定することはできません。 `vserver export-policy netgroup queue show`コマンドを使用してネットグループの読み込み状況を監視し、完了後にチェックを再試行してください。

例

次の例では、IPアドレス172.17.16.72を持つクライアントがSVM vs1上のネットグループmercuryのメンバーであるかどうかを確認します：

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

いくつかのパラメータを構成してアクセス キャッシュを最適化し、パフォーマンスとアクセス キャッシュに保存される情報の最新性との間の適切なバランスを見つけることができます。

タスク概要

アクセス キャッシュの更新期間を構成するときは、次の点に注意してください：

- 値が大きいほど、エントリがアクセス キャッシュ内に長く留まります。

  ONTAPがアクセス キャッシュ エントリの更新に費やすリソースが少なくなるため、パフォーマンスが向上するという利点があります。デメリットは、エクスポート ポリシー ルールが変更され、その結果アクセス キャッシュ エントリが古くなると、更新に時間がかかることです。その結果、アクセスを許可されるべきクライアントが拒否されたり、拒否されるべきクライアントがアクセスを許可されたりする可能性があります。

- 値が小さいほど、ONTAPがアクセス キャッシュ エントリをより頻繁に更新します。

  メリットは、エントリがより最新の状態になり、クライアントへのアクセスが適切に許可または拒否される可能性が高くなることです。デメリットは、ONTAPがアクセス キャッシュ エントリの更新に多くのリソースを費やすため、パフォーマンスが低下することです。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

変更の対象	入力する内容
受理エントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
拒否エントリの更新期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
古いエントリのタイムアウト期間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 新しいパラメータ設定を確認します。

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. admin権限レベルに戻ります。

```
set -privilege admin
```

ファイル ロックの管理

ONTAP NFS SVMのプロトコル間のファイルロックについて学習します

ファイル ロックとは、あるユーザがすでに開いているファイルに別のユーザがアクセスすることを防ぐ機能で、クライアント アプリケーションで使用されます。ONTAPでファイルをロックする方法は、クライアントのプロトコルによって異なります。

クライアントがNFSクライアントである場合、ロックは任意に設定します。クライアントがSMBクライアントである場合、ロックは必須となります。

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

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

- 混合ボリュームまたは NTFS ボリュームでは、 `rm`、 `rmdir`、 `mv`などのファイル操作によって NFS アプリケーションが失敗する可能性があります。
- NFSの読み取りと書き込みの処理は、SMBの読み取り拒否および書き込み拒否のオープン モードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的なSMBバイトロックでロックされている場合も、NFSの書き込みの処理はエラーになります。

UNIXセキュリティ形式のボリュームでは、NFSのリンク解除および名前変更の処理でSMBのロック状態が無視され、ファイルへのアクセスが許可されます。UNIXセキュリティ形式のボリュームでのその他すべてのNFS処理では、SMBのロック状態が考慮されます。

ONTAP NFS SVMの読み取り専用ビットについて学ぶ

読み取り専用ビットはファイルごとに設定され、ファイルが書き込み可能（無効）か読み取り専用（有効）かを反映します。

Windows を使用する SMB クライアントは、ファイルごとに読み取り専用ビットを設定できます。NFS クライアントでは、ファイルごとに読み取り専用ビットを使用するプロトコル操作がないため、ファイルごとに読み取り専用ビットは設定されません。

ONTAPは、Windowsを使用するSMBクライアントがファイルを作成する際に、そのファイルに読み取り専用ビットを設定できます。ONTAPは、NFSクライアントとSMBクライアント間でファイルを共有する場合にも、読み取り専用ビットを設定できます。NFSクライアントとSMBクライアントで使用される一部のソフトウェアでは、読み取り専用ビットを有効にする必要があります。

ONTAP が NFS クライアントと SMB クライアント間で共有されるファイルに対する適切な読み取りおよび書き込み権限を維持するために、読み取り専用ビットを次のルールに従って処理します：

- NFSは、読み取り専用ビットが有効になっているファイルを、書き込み許可ビットが有効になっていないものとして扱います。

- NFS クライアントがすべての書き込み許可ビットを無効にし、それらのビットの少なくとも 1 つが以前に有効になっていた場合、ONTAP はそのファイルの読み取り専用ビットを有効にします。
- NFS クライアントが書き込み権限ビットを有効にすると、ONTAP はそのファイルの読み取り専用ビットを無効にします。
- ファイルの読み取り専用ビットが有効になっていて、NFS クライアントがファイルの権限を検出しようとすると、ファイルの権限ビットは NFS クライアントに送信されません。代わりに、ONTAP は書き込み権限ビットをマスクした状態で権限ビットを NFS クライアントに送信します。
- ファイルの読み取り専用ビットが有効になっているときに、SMBクライアントがこの読み取り専用ビットを無効にすると、そのファイルに対する所有者の書き込み権限ビットが有効になります。
- 読み取り専用ビットが有効になっているファイルは、root のみが書き込み可能です。

読み取り専用ビットは、ACL および Unix モード ビットと次のように相互作用します：

ファイルに読み取り専用ビットが設定されている場合：

- そのファイルの ACL は変更されません。NFS クライアントには、読み取り専用ビットが設定される前と同じ ACL が表示されます。
- ファイルへの書き込みアクセスを許可する Unix モード ビットはすべて無視されます。
- NFS クライアントと SMB クライアントはどちらもファイルを読み取ることはできますが、変更することはできません。
- ACLとUNIXモードビットは、読み取り専用ビットが優先されるため無視されます。つまり、ACLが書き込みアクセスを許可していても、読み取り専用ビットによって変更は禁止されます。

ファイルに読み取り専用ビットが設定されていない場合：

- ONTAP は、ACL と UNIX モード ビットに基づいてアクセスを決定します。
  - ACL または UNIX モード ビットのいずれかが書き込みアクセスを拒否した場合、NFS および SMB クライアントはファイルを変更できません。
  - ACL も UNIX モード ビットも書き込みアクセスを拒否しない場合は、NFS および SMB クライアントはファイルを変更できます。

> ファイル権限の変更は SMB クライアントでは直ちに有効になりますが、NFS クライアントが属性キャッシュを有効にしている場合は、NFS クライアントでは直ちに有効にならない場合があります。

ONTAP NFSと**Windows**の共有パスコンポーネントのロック処理の違いについて学習します。

Windowsとは異なり、ONTAPでは、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作はSMB共有パスにも影響します。

ONTAPではパスの各コンポーネントがロックされないため、開いているファイルまたは共有より上のパス コンポーネントの名前を変更できます。このため、特定のアプリケーションで問題が発生したり、SMB構成の共有パスが無効になったりする可能性があります。これにより、共有にアクセスできなくなる場合があります。

パス コンポーネントの名前変更で生じる問題を回避するには、ユーザまたはアプリケーションが重要なディレクトリの名前を変更できないようにするWindowsのアクセス制御リスト（ACL）セキュリティ設定を適用し

ます。

"クライアントがアクセスしているときにディレクトリの名前が変更されないようにする方法"についての詳細をご覧ください。

ONTAP NFS SVMのロックに関する情報を表示します

現在のファイル ロックに関する情報を表示できます。これには、保持されているロックの種類とロックの状態、バイト範囲ロック、共有ロック モード、委譲ロック、およびoplockに関する詳細、およびロックが永続ハンドルまたは永続ハンドルで開かれているかどうかが含まれます。

タスク概要

NFSv4またはNFSv4.1を通じて確立されたロックの場合、クライアントIPアドレスは表示できません。

デフォルトでは、このコマンドはすべてのロックに関する情報を表示します。コマンドパラメータを使用すると、特定のStorage Virtual Machine（SVM）のロックに関する情報を表示したり、他の基準でコマンドの出力をフィルタリングしたりできます。

`vserver locks show`コマンドは、次の4種類のロックに関する情報を表示します：

- ファイルの一部のみをロックするバイト範囲ロック。
- 開いているファイルをロックする共有ロック。
- SMB 経由のクライアント側キャッシュを制御する便宜的ロック。
- NFSv4.x上のクライアント側キャッシュを制御する委任。

オプションパラメータを指定することで、各ロックの種類に関する重要な情報を確認できます。"ONTAPコマンド リファレンス"の `vserver locks show`の詳細をご覧ください。

手順

1. `vserver locks show`コマンドを使用してロックに関する情報を表示します。

例

以下の例は、パス `/vol1/file1`のファイルに対するNFSv4ロックの概要情報を表示します。sharelockのアクセス モードはwrite-deny_noneで、ロックは書き込み委譲で付与されました：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

以下の例は、パス `/data2/data2_2/intro.pptx`のファイルに対するSMBロックに関するoplockおよびsharelockの詳細情報を表示します。IPアドレス10.3.1.3のクライアントに、共有ロックアクセスモードwrite-deny_noneで永続ハンドルが付与されています。batch oplockレベルでリースoplockが付与されています（

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
```

```
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
    Node Holding Lock State: node3
                 Lock State: granted
   Bytelock Starting Offset: -
     Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
    Shared Lock Access Mode: -
        Shared Lock is Soft: -
            Delegation Type: -
             Client Address: 10.3.1.3
               SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

ONTAP NFS SVMのファイルロックの解除

ファイル ロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

タスク概要

この `vserver locks break`コマンドは、advanced権限レベル以上でのみ使用できます。 `vserver locks break`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

手順

1. ロックを解除するために必要な情報を見つけるには、 `vserver locks show` コマンドを使用します。

   `vserver locks show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-locks-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

3. 次のいずれかを実行します。

指定してロックを解除する場合…	コマンドを入力してください…
SVM名、ボリューム名、LIF名、およびファイル パス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロックID	`vserver locks break -lockid UUID`

4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP FPolicy のファーストリードフィルタとファーストライトフィルタが NFS でどのように機能するかを学びます

外部FPolicyサーバを使用してFPolicyが有効になっており、読み取り / 書き込み処理が監視対象イベントの場合、読み取り / 書き込み要求のトラフィックが多いとNFSクライアント側で応答時間が長くなります。NFSクライアントの場合、FPolicyでfirst-readフィルタとfirst-writeフィルタを使用すると、FPolicy通知の数が減り、パフォーマンスが向上します。

NFSでは、クライアントはファイルのハンドルを取得することでI/Oを実行します。このハンドルは、サーバーとクライアントの再起動後も有効なままになる場合があります。そのため、クライアントはハンドルをキャッシュし、再度ハンドルを取得することなく、そのハンドルに対してリクエストを送信できます。通常のセッションでは、ファイルサーバーに大量の読み取り/書き込みリクエストが送信されます。これらのリクエストすべてに対して通知が生成されると、次のような問題が発生する可能性があります：

- 余計な通知処理のために負荷が増大し、応答時間が長くなる。
- サーバに影響のない通知も含め、多数の通知がFPolicyサーバに送信される。

クライアントから特定のファイルに対する読み取り / 書き込み要求を初めて受信すると、キャッシュ エントリが作成され、読み取り / 書き込みのカウンタが増分されます。この要求は初回読み取り / 書き込み処理とマーキングされ、FPolicyイベントが生成されます。NFSクライアント用のFPolicyフィルタを計画して作成する前に、FPolicyフィルタの基本的な仕組みを理解しておく必要があります。

- first-read：初回読み取りのクライアント要求をフィルタリングします。

  このフィルタを NFS イベントに使用すると、 `-file-session-io-grouping-count`および `-file-session-io-grouping-duration`設定によって、FPolicy が処理される最初の読み取り要求が決定されます。

- first-write：初回書き込みのクライアント要求をフィルタリングします。

  このフィルタを NFS イベントに使用すると、 `-file-session-io-grouping-count`および `-file-session-io-grouping-duration`設定によって、FPolicy が処理する最初の書き込み要求が決定されます。

次のオプションがNFSサーバのデータベースに追加されます。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

ONTAP SVMのNFSv4.1サーバ実装IDを変更する

NFSv4.1プロトコルには、サーバのドメイン、名前、日付を記録するサーバ実装IDが含まれています。サーバ実装IDのデフォルト値は変更できます。デフォルト値の変更は、たとえば使用状況統計の収集や相互運用性に関する問題のトラブルシューティングなどに役立ちます。詳細については、RFC 5661を参照してください。

タスク概要

3 つのオプションのデフォルト値は次のとおりです：

オプション	オプション名	デフォルト値
NFSv4.1実装ID - ドメイン	`-v4.1-implementation -domain`	netapp.com
NFSv4.1実装ID - 名前	`-v4.1-implementation-name`	クラスタバージョン名
NFSv4.1実装ID - 日付	`-v4.1-implementation-date`	クラスタのバージョン日付

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

NFSv4.1 実装 **ID** を変更する場合…	コマンドを入力してください…
ドメイン	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
日付	`vserver nfs modify -v4.1 -implementation-date date`

3. admin権限レベルに戻ります。

```
set -privilege admin
```

NFSv4 ACLの管理

ONTAP SVMで**NFSv4 ACL**を有効にすることの利点について学習します。

NFSv4 ACLを有効化するメリットは色々あります。

NFSv4 ACL を有効にすると次のような利点があります：

- ファイルとディレクトリに対するユーザーアクセスのより細かい制御
- NFSセキュリティの向上
- CIFSとの相互運用性の向上
- ユーザーあたり16グループというNFS制限の削除

ONTAP SVM の **NFSv4 ACL** について学ぶ

NFSv4 ACLを使用しているクライアントは、システム上のファイルとディレクトリにACLを設定し、そのACLを表示することができます。ACLが設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、そのACL内のアクセス制御エントリ（ACE）のうち、該当する継承フラグがタグ付けされたACEがすべて継承されます。

ファイルやディレクトリがNFSv4要求によって作成される場合、作成されるファイルやディレクトリのACLは、ファイル作成要求にACLが含まれているか、標準のUNIXファイル アクセス権限のみが含まれているかによって、また、親ディレクトリにACLがあるかによって異なります。

- 要求にACLが含まれる場合は、そのACLが使用されます。
- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがある場合、親ディレクトリのACLのACEに該当する継承フラグが設定されていれば、それらのACEが新しいファイルやディレクトリに継承されます。

> ℹ `-v4.0-acl`が `off`に設定されている場合でも、親 ACL は継承されます。

- 要求に標準のUNIXファイル アクセス権限のみが含まれ、親ディレクトリにACLがない場合は、クライアントのファイル モードを使用して標準のUNIXファイル アクセス権限が設定されます。
- 要求に標準のUNIXファイルアクセス権限のみが含まれ、親ディレクトリに継承不可能なACLがある場合、モード ビットを使用しないと新しいオブジェクトは作成できません。

`-chown-mode`パラメータが `restricted`に `vserver nfs`または `vserver export-policy rule`
ファミリのコマンドで設定されている場合、NFSv4
ACLで設定されたディスク上の権限で非ルートユーザーがファイル所有権を変更できる場合でも、ファイルの所有権を変更できるのはスーパーユーザーのみです。この手順で説明されているコマンドの詳細については、link:https://docs.netapp.com/us-en/ontap-cli/["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP SVMのNFSv4 ACL変更を有効または無効にする

ONTAPがACLを持つファイルまたはディレクトリに対する `chmod`コマンドを受信すると、デフォルトではACLが保持され、モードビットの変更を反映するように変更されます。代わりにACLを削除したい場合は、 `-v4-acl-preserve`パラメータを無効にして動作を変更できます。

タスク概要

unifiedセキュリティ形式を使用している場合、このパラメータは、クライアントがファイルまたはディレクトリに対するchmod、chgroup、またはchownコマンドを送信した際にNTFSファイル アクセス権が保持されるか破棄されるかの指定も行います。

このパラメータのデフォルト設定は有効になっています。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
既存のNFSv4 ACLの保持と変更を有効にする（デフォルト）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
保持を無効にして、モード ビットの変更時にNFSv4 ACLを破棄する	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAPが**NFSv4 ACL**を使用してファイルを削除できるかどうかを判断する方法を学びます

ファイルを削除できるかどうかを判断するために、ONTAPはファイルのDELETEビットと、そのファイルを含むディレクトリのDELETE_CHILDビットの組み合わせを使用しま

す。詳細については、NFS 4.1 RFC 5661を参照してください。

ONTAP SVMのNFSv4 ACLを有効または無効にする

NFSv4 ACLを有効または無効にするには、 `-v4.0-acl`および `-v4.1-acl`オプションを変更します。これらのオプションはデフォルトでは無効になっています。

タスク概要

`-v4.0-acl`または `-v4.1-acl`オプションは、NFSv4 ACLの設定と表示を制御します。アクセス チェックに対するこれらのACLの適用は制御しません。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4.0 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
NFSv4.0 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
NFSv4.1 ACLを有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
NFSv4.1 ACLを無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

ONTAP SVMのNFSv4 ACLの最大ACE制限を変更する

パラメータ `-v4-acl-max-aces`を変更することで、NFSv4 ACLごとに許可されるACEの最大数を変更できます。デフォルトでは、ACLごとに400個のACEに制限されています。この制限を増やすことで、400個を超えるACEを含むACLを持つデータをONTAPで実行されているストレージシステムに正常に移行できるようになります。

タスク概要

この制限を増やすと、NFSv4 ACLを使用してファイルにアクセスするクライアントのパフォーマンスに影響

する可能性があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. NFSv4 ACLの最大ACE数を変更します。

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   有効な

   `max_ace_limit`は `192`1024.`です

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

NFSv4ファイル委譲の管理

ONTAP SVMのNFSv4読み取りファイル委譲を有効または無効にする

NFSv4読み取りファイル委譲を有効または無効にするには、`-v4.0-read-delegation`またはオプションを変更します。読み取りファイル委譲を有効にすると、ファイルのオープンとクローズに関連するメッセージのオーバーヘッドの大部分を削減できます。

タスク概要

デフォルトでは、読み取りファイル委譲は無効です。

読み取りファイル委譲を有効にした場合の欠点は、サーバのリブートまたはリスタート後、クライアントのリブートまたはリスタート後、あるいはネットワークを分割したあとに、サーバおよびそのクライアントが委譲をリカバリする必要があることです。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4読み取りファイル委譲を有効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
NFSv4.1読み取りファイル委譲を有効にする	次のコマンドを入力します。 + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`

NFSv4読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
NFSv4.1読み取りファイル委譲を無効にする	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

結果

ファイル委譲オプションへの変更はすぐに反映されます。NFSのリブートやリスタートは必要ありません。

ONTAP SVMのNFSv4書き込みファイル委譲を有効または無効にする

書き込みファイル委譲を有効または無効にするには、`-v4.0-write-delegation`またはオプションを変更します。書き込みファイル委譲を有効にすると、ファイルの開閉に加えて、ファイルとレコードのロックに関連するメッセージのオーバーヘッドを大幅に削減できます。

タスク概要

デフォルトでは、書き込みファイル委譲は無効になっています。

書き込みファイル委譲を有効にすることの欠点は、サーバの再起動、クライアントの再起動、またはネットワーク パーティションの発生後に、サーバとそのクライアントが委譲を回復するための追加タスクを実行する必要があることです。

手順

1. 次のいずれかを実行します。

状況	操作
NFSv4書き込みファイル委譲を有効にする	次のコマンドを入力します： `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
NFSv4.1書き込みファイル委譲を有効にする	次のコマンドを入力します： `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
NFSv4書き込みファイル委譲を無効にする	次のコマンドを入力します： `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

状況	操作
NFSv4.1書き込みファイル委譲を無効にする	次のコマンドを入力します： `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

結果

ファイル委譲オプションへの変更はすぐに反映されます。NFSのリブートやリスタートは必要ありません。

NFSv4ファイルおよびレコード ロックの設定

ONTAP SVM の NFSv4 ファイルおよびレコードのロックについて学習します

NFSv4クライアントの場合、ONTAPはNFSv4のファイルロック メカニズムをサポートしているため、すべてのファイルのロック状態がリースベース モデルで保持されます。

"NetAppテクニカル レポート3580：『NFSv4の拡張内容とベスト・プラクティス・ガイド - Data ONTAPでの実装』"

ONTAP SVMのNFSv4ロックリース期間を指定する

NFSv4ロックのリース期間（ONTAPがクライアントに取消不能なロックを許可する期間）を指定するには、 `-v4-lease-seconds`オプションを変更します。リース期間を短くするとサーバのリカバリが高速化されますが、リース期間を長くすると、非常に多くのクライアントを処理するサーバにとってメリットがあります。

タスク概要

デフォルトでは、このオプションは `30`に設定されています。このオプションの最小値は `10`です。このオプションの最大値は、 `locking.lease_seconds`オプションで設定できるロック猶予期間です。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP SVMのNFSv4ロック猶予期間を指定する

NFSv4ロック猶予期間（つまり、サーバ リカバリ中にクライアントがONTAPからロック状態を取り戻そうとする期間）を指定するには、 `-v4-grace-seconds`オプションを変

更します。

タスク概要

デフォルトでは、このオプションは `45`に設定されています。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のコマンドを入力します。

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP SVM の NFSv4 リファーラルについて学ぶ

NFSv4 リファーラルを有効にすると、ONTAP は NFSv4 クライアントに「SVM 内」リファーラルを提供します。SVM 内リファーラルとは、NFSv4 要求を受信したクラスタノードが、NFSv4 クライアントをStorage Virtual Machine（SVM）上の別の論理インターフェイス（LIF）に参照することです。

NFSv4クライアントは、その時点以降、ターゲットLIFでリファーラルを受信したパスにアクセスする必要があります。元のクラスタノードは、データボリュームが存在するクラスタノード上に常駐するSVM内にLIFが存在すると判断した場合、このようなリファーラルを提供します。これにより、クライアントはデータに高速にアクセスでき、余分なクラスタ通信を回避できます。

ONTAP SVMのNFSv4リファーラルを有効または無効にする

ストレージ仮想マシン（SVM）で `-v4-fsid-change`および`-v4.0-referrals`またはオプションを有効にすることで、NFSv4リファーラルを有効にすることができます。NFSv4リファーラルを有効にすると、この機能をサポートするNFSv4クライアントのデータアクセスが高速化されます。

開始する前に

NFSリファーラルを有効にする場合は、まずParallel NFSを無効にする必要があります。両方を同時に有効にすることはできません。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	コマンドを入力してください…
NFSv4リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
NFSv4リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
NFSv4.1リファーラルを有効にする	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
NFSv4.1リファーラルを無効にする	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

ONTAP NFS SVMの統計情報を表示する

パフォーマンスを監視して問題を診断するために、ストレージ システム上のStorage Virtual Machine（SVM）のNFS統計を表示することができます。

手順

1. `statistics catalog object show`コマンドを使用して、データを表示できるNFSオブジェクトを識別します。

   ```
   statistics catalog object show -object nfs*
   ```

2. `statistics start`およびオプションの `statistics stop`コマンドを使用して、1つ以上のオブジェクトからデータ サンプルを収集します。
3. `statistics show`コマンドを使用してサンプルデータを表示します。

例：**NFSv3**パフォーマンスの監視

以下に、NFSv3プロトコルのパフォーマンス データを表示する例を示します。

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

次のコマンドは、正常に行われた読み込み要求および書き込み要求の数と読み込み要求と書き込み要求の総数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    -------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS SVMのDNS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージ システム上のStorage Virtual Machine（SVM）のDNS統計を表示することができます。

手順

1. `statistics catalog object show`コマンドを使用して、データを表示できるDNSオブジェクトを識別します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. `statistics start`および `statistics stop`コマンドを使用して、1つ以上のオブジェクトからデータサンプルを収集します。
3. `statistics show`コマンドを使用してサンプルデータを表示します。

DNS統計の監視

次の例は、DNSクエリのパフォーマンス データを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

次のコマンドは、送信したDNSクエリの数と、受信した / 失敗した / タイムアウトになったDNSクエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

次のコマンドは、特定のサーバのDNSクエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS SVMのNIS統計を表示する

パフォーマンスを監視して問題を診断するために、ストレージ システム上のStorage Virtual Machine（SVM）のNIS統計を表示することができます。

手順

1. `statistics catalog object show`コマンドを使用して、データを表示できるNISオブジェクトを識別します。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. `statistics start`および`statistics stop`コマンドを使用して、1つ以上のオブジェクトからデータサンプルを収集します。
3. `statistics show`コマンドを使用してサンプルデータを表示します。

NIS統計の監視

次の例では、NISクエリのパフォーマンス データを表示します。次のコマンドは、新しいサンプルのデータ収集を開始します。

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

次のコマンドは、送信したNISクエリの数と、受信した / 失敗した / タイムアウトになったNISクエリの数を比較するカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

次のコマンドは、特定のサーバのNISクエリに対して特定のエラーを受信した回数を示すカウンタを指定して、サンプルからデータを表示します。

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                          YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

関連情報

- "パフォーマンス監視のセットアップ"
- "statistics catalog object show"
- "statistics show"
- "statistics start"
- "statistics stop"

ONTAP NFS経由のVMware vStorageのサポートについて学ぶ

ONTAPは、NFS環境で特定のVMware vStorage APIs for Array Integration（VAAI）機能をサポートしています。

サポートされる機能

次の機能がサポートされます。

- コピー オフロード

  ESXiホストで、仮想マシンや仮想マシン ディスク（VMDK）のコピーを、ホストを介さずにソースとデスティネーションのデータ ストア間で直接行うことができます。これにより、ESXiホストのCPUサイクルやネットワーク帯域幅を節約できます。ソース ボリュームがスパース ボリュームの場合、コピー オフロードでスペース効率が保持されます。

- スペース リザベーション

  スペースをリザーブしてVMDKファイル用のストレージ スペースを確保します。

制限事項

NFSでVMware vStorageを使用する際には、次の制限事項があります。

- 次の場合にコピー オフロード処理が失敗することがあります。
  - ソースボリュームまたは宛先ボリュームで wafliron を実行している間（ボリュームが一時的にオフラインになるため）
  - ソースボリュームまたはデスティネーション ボリュームのいずれかを移動中
  - ソースLIFまたは宛先LIFのいずれかを移動している間
  - テイクオーバーまたはギブバック操作の実行中
  - スイッチオーバーまたはスイッチバック処理の実行中
- 次のシナリオでは、ファイル ハンドル形式の違いによってサーバ側のコピーが失敗する可能性があります。

  qtreeのエクスポートを現在行っているか、以前行っていたSVMから、これまでにqtreeをエクスポートしたことがないSVMへのデータのコピーを試みます。上記の制限を回避するために、コピー先SVMで少なくとも1つのqtreeをエクスポートすることができます。

関連情報

"What VAAI offloaded operations are supported by Data ONTAP?"

ONTAP NFS経由でVMware vStorageを有効または無効にする

`vserver nfs modify`コマンドを使用して、ストレージ仮想マシン（SVM）上のVMware vStorage over NFSのサポートを有効または無効にすることができます。

タスク概要

デフォルトでは、VMware vStorage over NFSのサポートは無効になっています。

手順

1. SVMでの現在のvStorageのサポート ステータスを表示します。

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. 次のいずれかを実行します。

状況	入力するコマンド
VMware vStorageのサポートを有効にする	`vserver nfs modify -vserver vserver_name -vstorage enabled`
VMware vStorageのサポートを無効にする	`vserver nfs modify -vserver vserver_name -vstorage disabled`

終了後の操作

この機能を使用するには、VMware VAAI用NFSプラグインをインストールする必要があります。詳細については、_Installing the NetApp NFS Plug-in for VMware VAAI_を参照してください。

関連情報

"NetApp ドキュメント：NetApp NFS Plug-in for VMware VAAI"

ONTAP NFS SVMでrquotaサポートを有効または無効にする

リモート クォータ プロトコル（rquota）を使用すると、NFSクライアントはリモートマシンからユーザのクォータ情報を取得できます。rquotaのバージョンのサポートは、ONTAPのバージョンによって異なります。

- rquota v1 は ONTAP 9 以降でサポートされています。
- rquota v2はONTAP 9.12.1以降でサポートされています。

  rquota v1 から rquota v2 にアップグレードすると、ユーザ クォータ制限に予期せぬ変更が生じる場合があります。この変更は、rquota v1 と rquota v2 のクォータ計算方法の違いによるものです。詳細については、"NetAppナレッジベース：ユーザ クォータ制限が予期せず変更されたのはなぜですか"をご覧ください。

タスク概要

デフォルトでは、rquota は無効になっています。

手順

1. rquota を有効または無効にする：

状況	入力するコマンド
SVM の rquota サポートを有効にする	`vserver nfs modify -vserver vserver_name -rquota enable`
SVM の rquota サポートを無効にする	`vserver nfs modify -vserver vserver_name -rquota disable`

   クォータの詳細については、"論理ストレージ管理"を参照してください。

ONTAP SVM の NFSv3 および NFSv4 のパフォーマンス向上と TCP 転送サイズについて学習します

TCP 最大転送サイズを変更することで、高レイテンシ ネットワーク経由でストレージシステムに接続する NFSv3 および NFSv4 クライアントのパフォーマンスを向上させることができます。

クライアントが、レイテンシが10ミリ秒を超える広域ネットワーク（WAN）やメトロエリアネットワーク（MAN）などの高レイテンシネットワーク経由でストレージシステムにアクセスする場合、TCP最大転送サイズを変更することで接続パフォーマンスを向上できる可能性があります。ローカルエリアネットワーク（LAN）などの低レイテンシネットワーク経由でストレージシステムにアクセスするクライアントの場合、これらのパラメータを変更してもほとんど、あるいは全く効果が得られません。スループットの向上がレイテンシへの影響を上回らない場合は、これらのパラメータを使用しないでください。

これらのパラメータを変更することでストレージ環境が改善されるかどうかを判断するには、まず、パフォーマンスが低いNFSクライアントの包括的なパフォーマンス評価を実施する必要があります。パフォーマンスの低下が、クライアントでの過剰なラウンドトリップ遅延や小さなリクエストによるものかどうかを確認してください。このような状況では、クライアントとサーバーは、接続を介して送信される小さなリクエストとレスポンスの待機にデューティサイクルの大部分を費やすため、利用可能な帯域幅を十分に活用できません。

NFSv3 および NFSv4 の要求サイズを増やすと、クライアントとサーバーは利用可能な帯域幅をより効率的に使用して、単位時間あたりに移動するデータ量を増やすことができるため、接続の全体的な効率が向上します。

ストレージ システムとクライアント間の構成は異なる場合があることにご注意ください。ストレージ システムとクライアントは、転送操作の最大サイズとして 1 MB をサポートしています。ただし、ストレージ システムが最大転送サイズ 1 MB をサポートするように設定しているのに、クライアントが 64 KB しかサポートしていない場合、マウント転送サイズは 64 KB 以下に制限されます。

これらのパラメータを変更する前に、大容量の応答を組み立てて送信するために必要な時間、ストレージ システムで追加のメモリ消費が発生することにご注意ください。ストレージ システムへの高レイテンシ接続が多いほど、追加のメモリ消費量は大きくなります。メモリ容量の大きいストレージ システムでは、この変更による影響はほとんどない可能性があります。メモリ容量の小さいストレージ システムでは、パフォーマンスが著しく低下する可能性があります。

これらのパラメータを効果的に使用するには、クラスタ内の複数のノードからデータを取得できる必要があります。クラスタ ネットワーク固有のレイテンシにより、応答のレイテンシが全体的に増加する可能性があります。これらのパラメータを使用すると、全体的なレイテンシが増加する傾向があります。その結果、レイテンシの影響を受けやすいワークロードでは、悪影響が出る可能性があります。

ONTAP SVMのNFSv3およびNFSv4 TCP最大転送サイズを変更する

`-tcp-max-xfer-size`オプションを変更して、NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続の最大転送サイズを設定できます。

タスク概要

このオプションはStorage Virtual Machine（SVM）ごとに変更できます。

ONTAP 9以降、 `v3-tcp-max-read-size`および `v3-tcp-max-write-size`オプションは廃止されました。代わりに`-tcp-max-xfer-size`オプションを使用する必要があります。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のいずれかを実行します。

状況	コマンドを入力してください...
NFSv3またはNFSv4のTCP最大転送サイズを変更する	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

オプション	範囲	デフォルト
`-tcp-max-xfer-size`	8,192～1,048,576バイト	65,536バイト

ⓘ 最大転送サイズには、4KB（4,096バイト）の倍数を入力する必要があります。要求が要件を満たしていない場合は、パフォーマンスが低下します。

3. `vserver nfs show -fields tcp-max-xfer-size`コマンドを使用して変更を確認します。
4. 静的マウントを使用しているクライアントがある場合、変更したパラメータのサイズを有効にするには、いったんアンマウントしてから再度マウントします。

例

次のコマンドは、vs1というSVMでNFSv3とNFSv4.xのTCP最大転送サイズを1,048,576バイトに設定します。

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

ONTAP SVMのNFSユーザーに許可されるグループIDの数を設定します

デフォルトでは、ONTAPはKerberos（RPCSEC_GSS）認証を使用してNFSユーザクレデンシャルを処理する際に、最大32個のグループIDをサポートします。AUTH_SYS認証を使用する場合、RFC 5531で定義されているように、グループIDのデフォルトの最大数は16です。デフォルト数を超えるグループに所属するユーザがいる場合は、最大数を1,024まで増やすことができます。

タスク概要

デフォルト数を超えるグループIDがクレデンシャルに設定されている場合、残りのグループIDは切り捨てられ、そのユーザがストレージ システムのファイルへのアクセスを試みるとエラーが発生する可能性があります。SVMあたりの最大グループ数は、環境内の最大グループ数と同じ数に設定する必要があります。

ⓘ デフォルトの最大数である16を超えるグループIDを使用する拡張グループ(`-auth-sys-extended-groups`を有効にするためのAUTH_SYS認証の前提条件を理解するには、"NetAppナレッジベース：auth-sys-extended-groups を有効にするための前提条件は何ですか？"を参照してください

次の表は、3つのサンプル構成でグループIDの最大数を決定する `vserver nfs modify`コマンドの2つのパラメータを示しています：

パラメータ	設定	結果のグループIDの制限

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	これらはデフォルト設定です。
		RPCSEC_GSS：32
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS：256
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS：512
		
		AUTH_SYS：512

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

許可される補助グループの最大数を設定する場合…	コマンドを入力してください…
RPCSEC_GSSのみ（AUTH_SYSはデフォルト値16のまま）	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
RPCSEC_GSSとAUTH_SYSの両方	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. `-extended-groups-limit`値を確認し、`AUTH_SYS`が拡張グループを使用しているかどうかを確認します： `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

次の例は、AUTH_SYS認証で拡張されたグループ数を有効にし、AUTH_SYS認証とRPCSEC_GSS認証の両方でグループの最大数を512に設定します。これらの変更は、vs1というSVMにアクセスするクライアントに対してのみ適用されます。

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

関連情報

- "NetAppナレッジベース：ONTAP 9のNFS認証におけるAUTH_SYS拡張グループの変更"

ONTAP SVMのNTFSセキュリティ形式のデータへのrootユーザアクセスの制御

NFSクライアントにNTFSセキュリティ形式のデータへのアクセスを許可し、NTFSクライアントにNFSセキュリティ形式データへのアクセスを許可するようにONTAPを設定することができます。NFSデータ ストアでNTFSセキュリティ形式を使用する際には、rootユーザによるアクセスの処理方法を決定し、それに応じてStorage Virtual Machine（SVM）を設定する必要があります。

タスク概要

rootユーザがNTFSセキュリティ形式のデータにアクセスする際には、次の2つのオプションがあります。

- その他すべてのNFSユーザと同様にrootユーザをWindowsユーザにマッピングし、NTFS ACLに従ってアクセスを管理する。
- NTFS ACLを無視してフル アクセスをrootに対して提供する。

手順

1. 権限レベルをadvancedに設定します。

   ```
   set -privilege advanced
   ```

2. 次のうち必要な操作を実行します。

rootユーザーに次の操作を実行させたい場合…	コマンドを入力してください…

Windowsユーザにマッピングする	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
NT ACLチェックをバイパスする	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

このパラメータはデフォルトで無効になっています。

このパラメータが有効になっていてもrootユーザに対するネーム マッピングが存在しない場合、ONTAPはデフォルトのSMB管理者のクレデンシャルを監査に使用します。

3. admin権限レベルに戻ります。

```
set -privilege admin
```

サポートされるNFSバージョンおよびクライアント

サポートされているONTAP NFSのバージョンとクライアントについて学習します

ネットワークでNFSを使用する前に、ONTAPでサポートされるNFSのバージョンとクライアントを確認しておく必要があります。

次の表は、NFSプロトコルの各メジャー / マイナー バージョンがいつONTAPでデフォルトでサポートされたかを示したものです。デフォルトでサポートされていても、そのNFSプロトコルをサポートする最も古いONTAPのバージョンというわけではありません。

version	サポート	導入
NFSv3	はい	ONTAPのすべてのリリース
NFSv4.0	はい	ONTAP 8
NFSv4.1	はい	ONTAP 8.1
NFSv4.2	はい	ONTAP 9.8
pNFS	はい	ONTAP 8.1

ONTAPでサポートされるNFSクライアントに関する最新情報については、Interoperability Matrixを参照してください。

"NetApp Interoperability Matrix Tool"

ONTAP による NFSv4.0 機能のサポートについて学ぶ

ONTAPは、SPKM3およびLIPKEYセキュリティ メカニズムを除くNFSv4.0のすべての必

須機能をサポートしています。

次の NFSV4 機能がサポートされています：

- **COMPOUND**

  クライアントが単一のリモート プロシージャ コール（RPC）要求で複数のファイル操作を要求できるようにします。

- ファイルの委任

  サーバーが、読み取りおよび書き込みアクセスのために、特定の種類のクライアントにファイル制御を委任できるようにします。

- 疑似**FS**

  NFSv4サーバーがストレージ システム上のマウント ポイントを決定するために使用します。NFSv4にはマウント プロトコルはありません。

- ロック

  リースベース。NFSv4には、個別のNetwork Lock Manager（NLM）またはNetwork Status Monitor（NSM）プロトコルはありません。

NFSv4.0プロトコルの詳細については、RFC 3530を参照してください。

NFSv4 の ONTAP サポートの制限について学習します

ONTAPでのNFSv4のサポートにはいくつかの制限があることに注意してください。

- 委譲機能はすべてのクライアント タイプによってサポートされているわけではありません。
- ONTAP 9.4以前のリリースでは、UTF8以外のボリュームでASCII以外の文字が含まれている名前はストレージ システムで拒否されます。

  ONTAP 9.5以降のリリースでは、utf8mb4言語設定で作成されNFSv4を使用してマウントされたボリュームはこの制限を受けなくなります。

- すべてのファイル ハンドルは永続的です。サーバは揮発性のファイル ハンドルを配布しません。
- 移行およびレプリケーションはサポートされません。
- NFSv4クライアントは、読み取り専用負荷共有ミラーではサポートされていません。

  ONTAPは、NFSv4クライアントを直接読み取りおよび書き込みアクセス用負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされません。
- 次の属性を除くすべての推奨属性がサポートされています。
  - `archive`
  - `hidden`

- homogeneous
- mimetype
- quota_avail_hard
- quota_avail_soft
- quota_used
- system
- time_backup

> `quota*`属性はサポートしていませんが、ONTAPはRQUOTAサイドバンド プロトコルを通じてユーザ クォータとグループ クォータをサポートしています。

ONTAP の NFSv4.1 サポートについて学ぶ

ONTAP 9.8以降、NFSv4.1が有効になっている場合はデフォルトでnconnect機能を使用できます。

以前のNFSクライアント実装は、1つのマウントでTCP接続を1つしか使用しません。ONTAPでは、単一のTCP接続はIOPSの増加時にボトルネックになることがあります。

nconnectは、単一のマウントに対して複数のTCP接続（最大16）を許可することでNFSクライアントのパフォーマンスを向上させ、IOPSの増加に伴って単一のTCP接続で発生する可能性のあるパフォーマンスのボトルネックを克服するのに役立ちます。

ONTAP 9.9.1以降では、NFSv4.1がデフォルトで有効になっています。それ以前のリリースでは、Storage Virtual Machine（SVM）上にNFSサーバを作成する際に `-v4.1`オプションを指定して `enabled`に設定することで有効にできます。

ONTAPは、NFSv4.1ディレクトリおよびファイル レベルの委任をサポートしていません。

関連情報

"NFSパフォーマンスのためのnconnectについて学ぶ"。

ONTAP の NFSv4.2 サポートについて学ぶ

ONTAP 9.8以降では、NFSv4.2プロトコルがサポートされており、NFSv4.2対応クライアントのアクセスが許可されます。

NFSv4.2は、ONTAP 9.9.1以降ではデフォルトで有効になっています。ONTAP 9.8では、Storage Virtual Machine（SVM）上にNFSサーバを作成する際に、 `-v4.2`オプションを指定して `enabled`に設定することで、v4.2を手動で有効にする必要があります。NFSv4.1を有効にすると、クライアントはv4.2としてマウントされている間もNFSv4.1の機能を使用できるようになります。

以降のONTAPリリースでは、NFSv4.2のオプション機能のサポートが拡張されています。

バージョン	含まれる**NFSv4.2**のオプション機能
ONTAP 9.12.1	• NFS拡張属性 • スパース ファイル • スペース リザベーション
ONTAP 9.9.1	強制アクセス制御（MAC）ラベル付きNFS

NFS v4.2セキュリティ ラベル

ONTAP 9.9.1以降では、NFSセキュリティ ラベルを有効にすることができます。デフォルトでは無効になっています。

NFSv4.2セキュリティ ラベルを使用するONTAP NFSサーバは、強制アクセス制御（MAC: Mandatory Access Control）に対応するため、クライアントから送信されたsec_label属性を保存および取得します。

詳細については、"RFC 7240"を参照してください。

ONTAP 9.12.1以降では、NDMPダンプ処理でNFS v4.2セキュリティ ラベルがサポートされます。それよりも前のリリースでファイルまたはディレクトリでセキュリティ ラベルが検出されると、ダンプは失敗します。

手順

1. 権限の設定をadvancedに変更します。

```
set -privilege advanced
```

2. セキュリティ ラベルを有効にします。

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS拡張属性

ONTAP 9.12.1以降では、NFS拡張属性（xattrs）がデフォルトで有効になっています。

拡張属性は "RFC 8276"で定義され、最新のNFSクライアントで有効になっている標準のNFS属性です。ファイル システム オブジェクトにユーザ定義のメタデータを付加するために使用でき、高度なセキュリティ導入において重要です。

現在、NFS拡張属性はNDMPダンプ処理ではサポートされていません。ファイルまたはディレクトリで拡張属性が検出されると、ダンプ処理は続行されますが、それらのファイルまたはディレクトリの拡張属性はバックアップされません。

拡張属性を無効にする必要がある場合は、 `vserver nfs modify -v4.2-xattrs disabled` コマンドを使用します。

NFSパフォーマンスのためのnconnectについて学ぶ

ONTAP 9.8 以降では、NFSv4.1 が有効になっている場合、nconnect 機能がデフォルトで使用できます。nconnect は、単一のマウントに対して複数の TCP 接続を許可することで、NFS クライアントのパフォーマンスを向上させます。

nconnectの仕組み

以前のNFSクライアント実装は、1つのマウントでTCP接続を1つしか使用しません。ONTAPでは、単一のTCP接続はIOPSの増加時にボトルネックになることがあります。

nconnect 対応クライアントは、単一の NFS マウントに複数の TCP 接続（最大 16 個）を関連付けることができます。nconnect は 1 つの IP アドレスのみを使用し、その単一の IP アドレスを介して複数の TCP 接続を確立して NFS エクスポートをマウントします。NFS クライアントは、ファイル操作を複数の TCP 接続にラウンドロビン方式で分散することで、利用可能なネットワーク帯域幅からより高いスループットを実現します。

サポートされるNFSバージョン

- NFSv3、NFSv4.2、および NFSv4.1 マウントには nconnect が推奨されます。
- nconnect は NFSv4.0 マウントには推奨され_ません_。

> 最適なパフォーマンスを得るには、NetAppはNFSv4.0ではなくNFSv4.1とnconnectの使用をお勧めします。NFSv4.0は複数の接続をサポートしますが、NFSv4.1とnconnectは負荷分散とスループットの向上を実現します。

クライアントのサポート

nconnect がクライアントバージョンでサポートされているかどうかを確認するには、NFS クライアントのドキュメントを参照してください。

関連情報

- "ONTAP の NFSv4.1 サポートについて学ぶ"
- "ONTAP の NFSv4.2 サポートについて学ぶ"

ONTAPの並列NFSサポートについて学ぶ

ONTAPはパラレルNFS（pNFS）をサポートしています。pNFSプロトコルは、クラスタ内の複数のノードに分散されたファイルセットのデータにクライアントが直接アクセスできるようにすることで、パフォーマンスを向上させます。クライアントがボリュームへの最適なパスを見つけるのに役立ちます。

ONTAPのNFSハードマウントについて

マウントに関する問題のトラブルシューティングを行う際は、正しいマウントタイプを使用していることを確認する必要があります。NFSはソフトマウントとハードマウント

の2種類のマウントタイプをサポートしています。信頼性の観点から、ハードマウントのみを使用してください。

特にNFSタイムアウトが頻繁に発生する可能性がある場合は、ソフトマウントを使用しないでください。これらのタイムアウトにより競合状態が発生し、データ破損につながる可能性があります。

パラレル**NFS**

はじめに

ONTAPでの並列**NFS**（**pNFS**）について

パラレルNFSは、メタデータとデータパスを分離することで、クライアントがNFSv4.1サーバ上のファイルデータに直接アクセスできるようにするために、2010年1月にRFC-5661でRFC標準として導入されました。この直接アクセスにより、データのローカライゼーション、CPU効率、処理の並列化といったパフォーマンス上のメリットが得られます。その後、2018年にpNFSレイアウトタイプ（RFC-8434）を網羅したRFCが作成され、ファイル、ブロック、およびオブジェクトレイアウトの標準が定義されています。ONTAPはpNFS操作にこのファイルレイアウトタイプを活用します。

> 2024年7月より、これまでPDF形式で公開されていたテクニカルレポートの内容がONTAP製品ドキュメントに統合されました。ONTAP NFSストレージ管理ドキュメントには、_TR-4063：NetApp ONTAPにおけるパラレルネットワークファイルシステム（pNFS）_の内容が含まれるようになりました。

NFSv3は長年にわたり、ほぼすべてのユースケースで使用されてきたNFSプロトコルの標準バージョンでした。しかし、このプロトコルには、ステートフル性の欠如、基本的な権限モデル、基本的なロック機能といった制限がありました。NFSv4.0（RFC 7530）では、NFSv3に対する一連の改良が導入され、その後のNFSv4.1（RFC 5661）およびNFSv4.2（RFC 7862）バージョンでさらに改良が加えられ、パラレルNFS（pNFS）などの機能が追加されました。

NFSv4.xの利点

NFSv4.x は NFSv3 に比べて次のような利点があります：

- ファイアウォールとの親和性。NFSv4では1つのポート（2049）しか使用しません。
- 高度でアグレッシブなキャッシュ管理。NFSv4.xの委譲機能など。
- 強固なRPCセキュリティ種別。暗号化を実装します。
- 文字の国際化
- 複合操作。
- TCPでのみ動作。
- ステートフル プロトコル（NFSv3はステートレス）。
- 効率的な認証メカニズムのための完全なKerberos統合
- NFSリファーラル

- UNIXおよびWindowsと互換性のあるアクセス制御のサポート。
- 文字列ベースのユーザ識別子とグループ識別子。
- pNFS（NFSv4.1）
- 拡張属性（NFSv4.2）
- セキュリティラベル（NFSv4.2）
- スパース ファイル操作（FALLOCATE）（NFSv4.2）

ベスト プラクティスや機能の詳細など、NFSv4.x 全般の詳細については、 "NetAppテクニカル レポート4067：『NFS Best Practice and Implementation Guide』"を参照してください。

関連情報

- "NFS 構成の概要"
- "NFSの管理 - 概要"
- "FlexGroupボリューム管理"
- "NFSトランキングの概要"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf
- "NetApp テクニカルレポート 4616：ONTAP における NFS Kerberos と Microsoft Active Directory"

ONTAPの**pNFS**アーキテクチャについて

pNFSアーキテクチャは、pNFSをサポートするNFSクライアント、メタデータ操作専用のパスを提供するメタデータサーバ、およびファイルへのローカライズされたパスを提供するデータサーバという3つの主要コンポーネントで構成されています。

pNFSへのクライアントアクセスには、NFSサーバで使用可能なデータパスとメタデータパスへのネットワーク接続が必要です。NFSサーバにクライアントがアクセスできないネットワークインターフェイスが含まれている場合、サーバはクライアントにアクセスできないデータパスをアドバタイズし、サービス停止を引き起こす可能性があります。

メタデータサーバ

pNFSのメタデータサーバは、NFSサーバでpNFSが有効になっているときに、クライアントがNFSv4.1以降を使用してマウントを開始すると確立されます。これが完了すると、すべてのメタデータトラフィックはこの接続を介して送信され、インターフェースが別のノードに移行された場合でも、マウント中はこの接続上に維持されます。

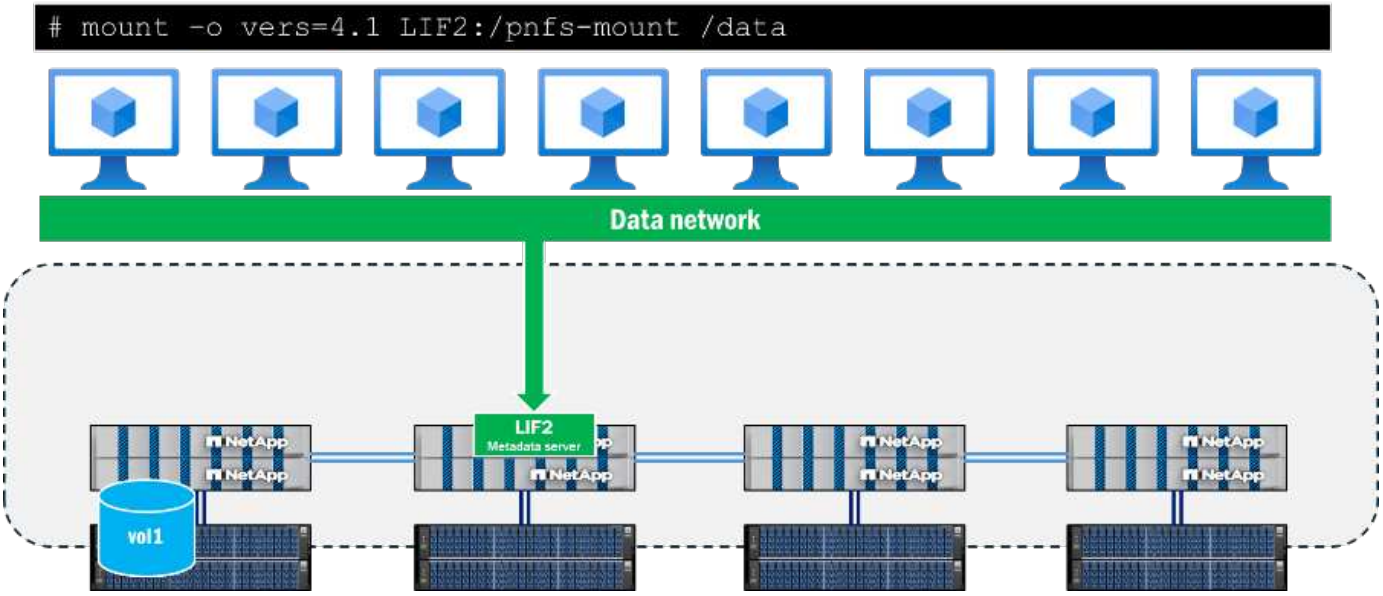


図 1. ONTAPでpNFSのメタデータサーバを確立

pNFSのサポートは、マウント呼び出し、具体的にはEXCHANGE_ID呼び出し時に決定されます。これは、NFS操作の下にあるパケットキャプチャでフラグとして確認できます。pNFSフラグ `EXCHGID4_FLAG_USE_PNFS_DS`と `EXCHGID4_FLAG_USE_PNFS_MDS`が1に設定されている場合、インターフェースはpNFSのデータ操作とメタデータ操作の両方に対応します。

```
Operations (count: 1)
  Opcode: EXCHANGE_ID (42)
    Status: NFS4_OK (0)
    clientid: 0x004050a97100001c
    seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
      0... .... .... .... .... .... .... .... = EXCHGID4_FLAG_CONFIRMED_R: Not set
      .0.. .... .... .... .... .... .... .... = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
      .... .... .... .1.. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_DS: Set
      .... .... .... ..1. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_MDS: Set
      .... .... .... ...0 .... .... .... .... = EXCHGID4_FLAG_USE_NON_PNFS: Not set
      .... .... .... .... .... ...1 .... .... = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
      .... .... .... .... .... .... .... ..0. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
      .... .... .... .... .... .... .... ...0 = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set
```

図 2. pNFSマウントのパケットキャプチャ

NFSのメタデータは通常、ファイルハンドル、権限、アクセス時刻と変更時刻、所有権情報などのファイルとフォルダの属性で構成されます。メタデータには、作成と削除の呼び出し、リンクとリンク解除の呼び出し、名前の変更などが含まれる場合もあります。

pNFSには、pNFS機能に固有のメタデータ呼び出しのサブセットも存在します。これらについては"RFC 5661"で詳しく説明します。これらの呼び出しは、pNFS対応デバイス、デバイスとデータセットのマッピング、その他の必要な情報を決定するのに役立ちます。次の表は、これらのpNFS固有のメタデータ操作の一覧です。

処理	概要
LAYOUTGET	メタデータ サーバからデータ サーバ マップを取得します。
LAYOUTCOMMIT	サーバはレイアウトをコミットし、メタデータ マップを更新します。

処理	概要
LAYOUTRETURN	レイアウト、またはデータが変更された場合は新しいレイアウトを返します。
GETDEVICEINFO	クライアントは、ストレージ クラスタ内のデータ サーバの更新情報を取得します。
デバイスリスト取得	クライアントは、ストレージ クラスタに参加しているすべてのデータ サーバのリストを要求します。
CB_LAYOUTRECALL	競合が検出された場合、サーバはクライアントからデータ レイアウトを再呼び出しします。
CB_RECALL_ANY	すべてのレイアウトをメタデータ サーバに返します。
CB_NOTIFY_DEVICEID	デバイス ID の変更を通知します。

データパス情報

メタデータサーバが確立され、データ操作が開始されると、ONTAPはpNFSの読み取りおよび書き込み操作に有効なデバイスIDと、クラスタ内のボリュームをローカル ネットワーク インターフェースに関連付けるデバイス マッピングの追跡を開始します。このプロセスは、マウント内で読み取りまたは書き込み操作が実行されたときに発生します。 `GETATTR`などのメタデータ呼び出しでは、これらのデバイス マッピングはトリガーされません。そのため、マウント ポイント内で `ls`コマンドを実行しても、マッピングは更新されません。

デバイスとマッピングは、次に示すように、ONTAP CLI の高度な権限を使用して表示できます。

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

これらのコマンドでは、ボリューム名は使用されません。代わりに、ボリュームに関連付けられた数値ID（マスター セット ID（MSID）とデータ セット ID（DSID））が使用されます。マッピングに関連付けられたボリュームを確認するには、ONTAP CLIのadvanced権限で `volume show -dsid [dsid_numeric]`または `volume show -msid [msid_numeric]`を使用します。

クライアントがメタデータ サーバ接続から離れたノードにあるファイルの読み取りまたは書き込みを試みると、pNFSは適切なアクセス パスをネゴシエートし、これらの操作におけるデータの局所性を確保します。クライアントは、ファイルにアクセスするためにクラスタ ネットワークを経由するのではなく、アドバタイズされたpNFSデバイスにリダイレクトします。これにより、CPUオーバーヘッドとネットワークレイテンシが削減されます。

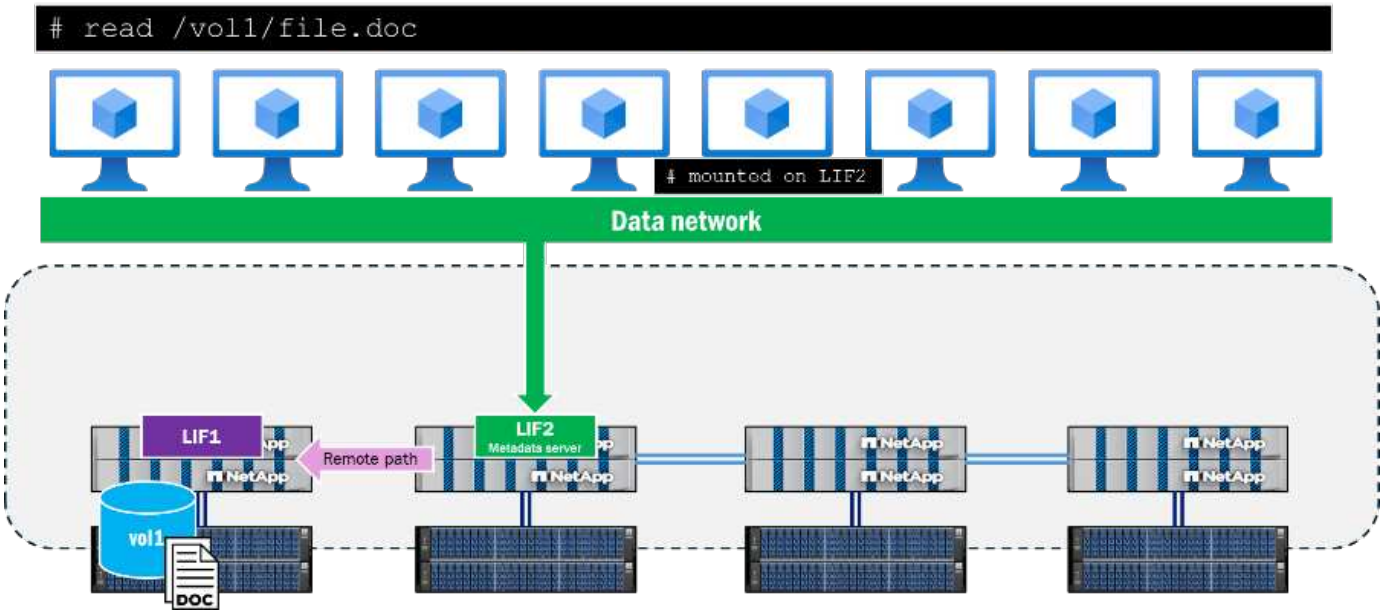


図 **3. pNFS**を使用しない**NFSv4.1**を使用したリモート読み取りパス

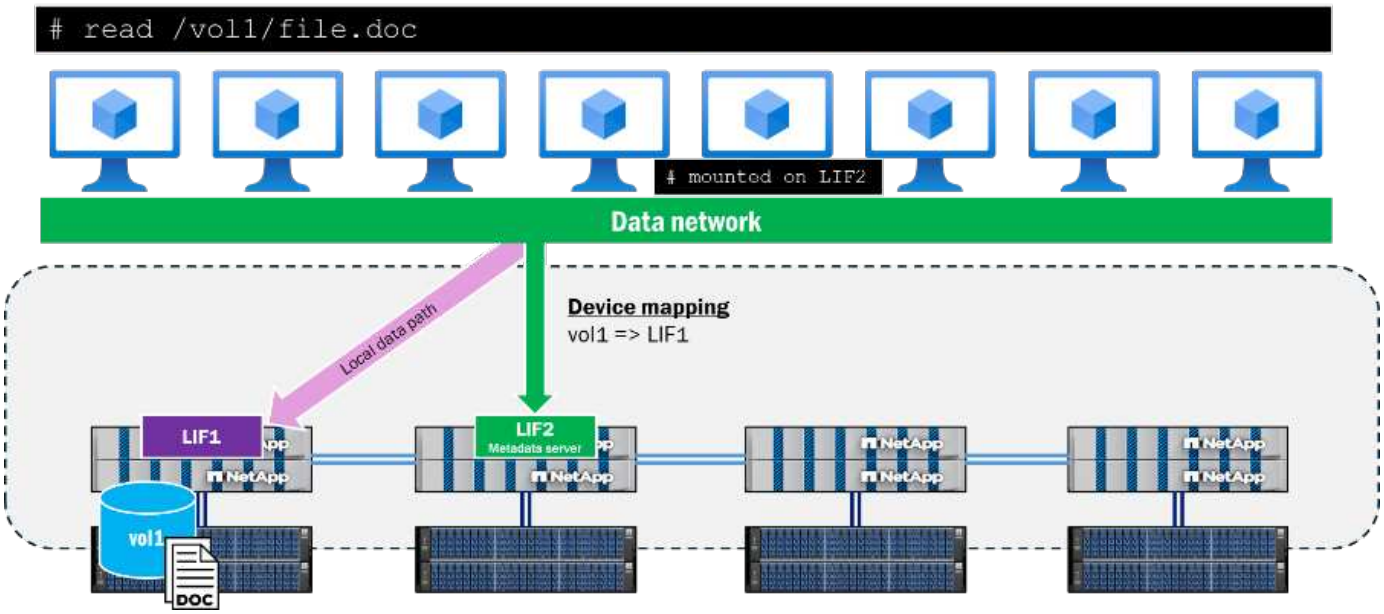


図 **4. pNFS**を使用したローカライズされた読み取りパス

pNFS制御パス

pNFSには、メタデータとデータ部分に加えて、pNFS制御パスも存在します。この制御パスは、NFSサーバがファイルシステム情報を同期するために使用されます。ONTAPクラスタでは、バックエンドクラスタネットワークが定期的にレプリケーションを実行し、すべてのpNFSデバイスとデバイスマッピングが同期されていることを確認します。

pNFSデバイス設定ワークフロー

以下では、クライアントがボリューム内のファイルの読み取りまたは書き込みを要求した後に、pNFSデバイスがONTAPにどのように設定されるかについて説明します。

1. クライアントが読み取りまたは書き込みを要求すると、OPENが実行され、ファイル ハンドルが取得されます。

2. OPENが実行されると、クライアントはメタデータ サーバ接続を介したLAYOUTGET呼び出しでファイル ハンドルをストレージに送信します。
3. LAYOUTGET は、状態 ID、ストライプ サイズ、ファイル セグメント、デバイス ID など、ファイルのレイアウトに関する情報をクライアントに返します。
4. 次に、クライアントはデバイスIDを取得し、GETDEVINFO呼び出しをサーバに送信して、デバイスに関連付けられたIPアドレスを取得します。
5. ストレージは、デバイスへのローカル アクセス用に関連付けられたIPアドレスのリストを含む応答を送信します。
6. クライアントは、ストレージから返されたローカル IP アドレスを介してNFS会話を継続します。

pNFSとFlexGroupボリュームの相互作用

FlexGroupボリュームは、ONTAPでストレージをクラスタ内の複数のノードにまたがるFlexVolボリューム構成要素として提示します。これにより、ワークロードは単一のマウントポイントを維持しながら、複数のハードウェアリソースを活用できます。複数のネットワークインターフェイスを持つ複数のノードがワークロードとやり取りするため、リモートトラフィックがONTAPのバックエンドクラスタネットワークを通過するのは自然な結果です。

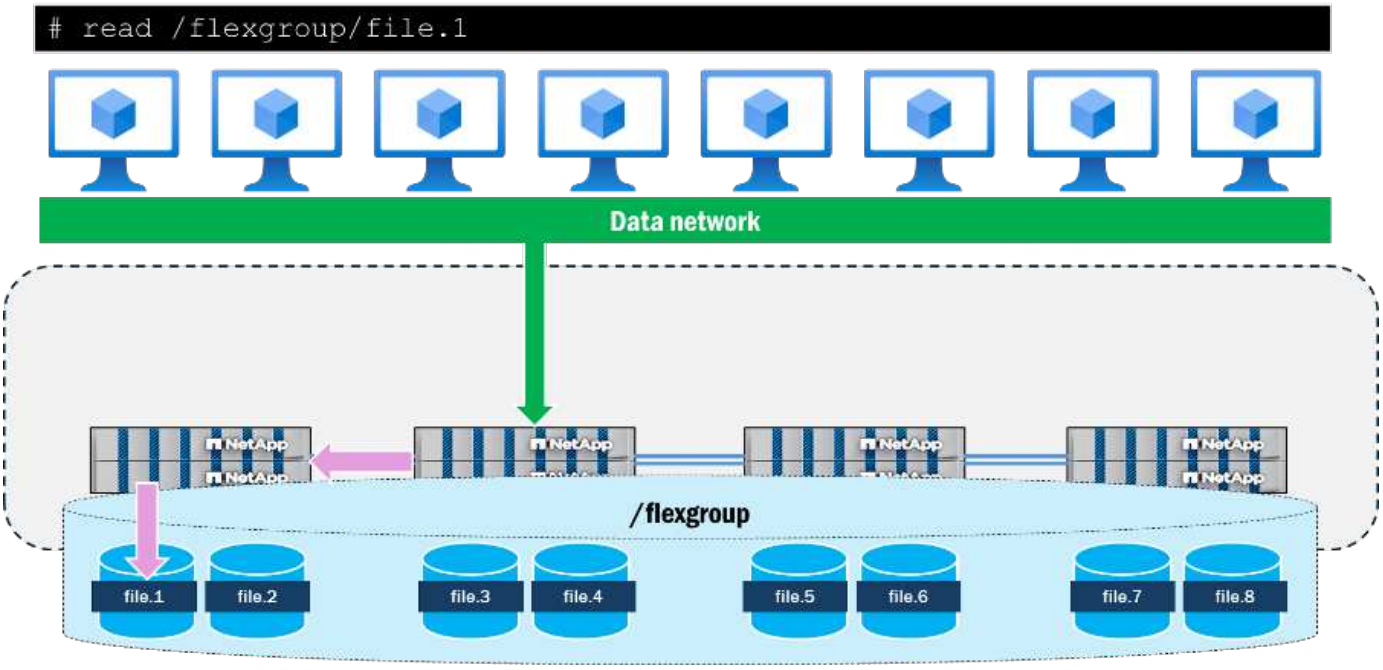


図 **5. pNFS** を使用しない**FlexGroup**ボリューム内の単一ファイル アクセス

pNFSを利用する場合、ONTAPはFlexGroupボリュームのファイルとボリュームのレイアウトを追跡し、それらをクラスタ内のローカル データ インターフェースにマッピングします。例えば、アクセス対象のファイルを含む構成ボリュームがノード1に存在する場合、ONTAPはクライアントにネットワーク トラフィックをノード1のデータ インターフェースにリダイレクトするよう通知します。

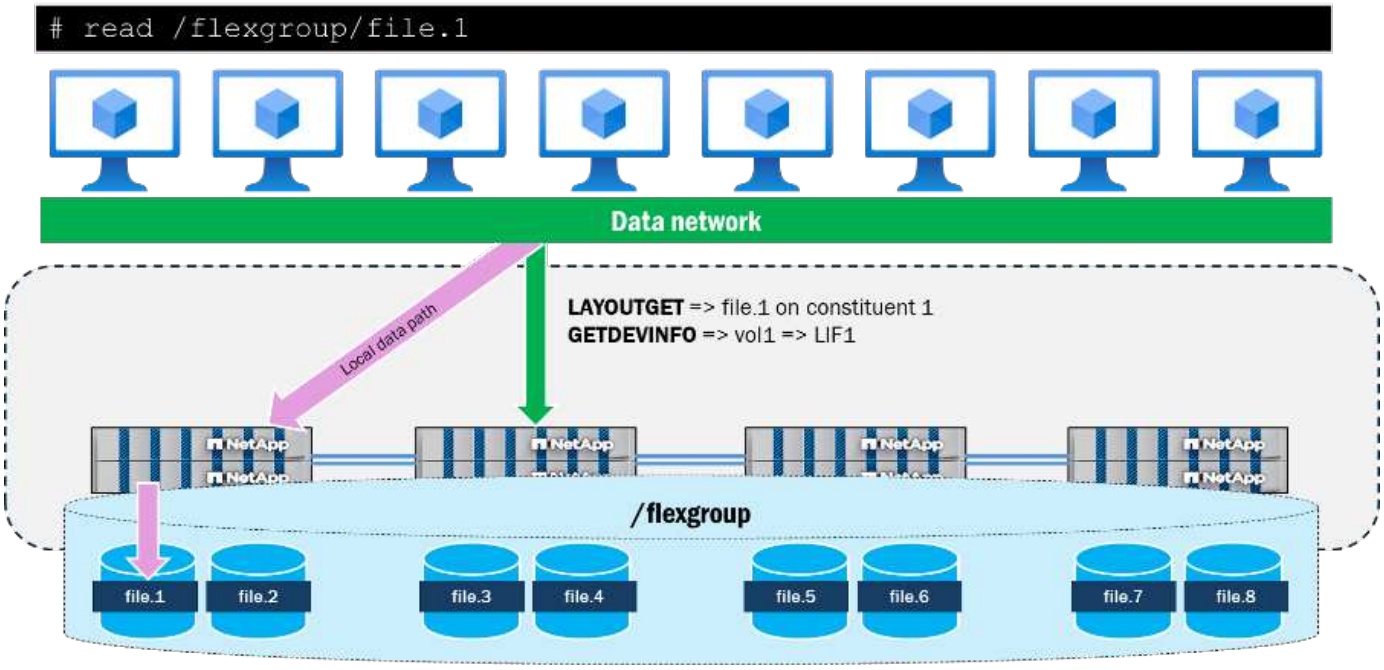


図 **6. pNFS**を使用した**FlexGroup**ボリューム内の単一ファイル アクセス

pNFSは、pNFSのないNFSv4.1では提供されない、単一のクライアントからファイルへの並列ネットワーク パスのプレゼンテーションも提供します。たとえば、クライアントがpNFSのないNFSv4.1を使用して同じマウントから4つのファイルに同時にアクセスする場合、すべてのファイルに同じネットワーク パスが使用され、ONTAPクラスタは代わりにそれらのファイルへのリモート要求を送信します。マウント パスは、すべての操作が単一のパスをたどって単一のノードに到達し、データ操作とともにメタデータ操作も処理するため、操作のボトルネックになる可能性があります。

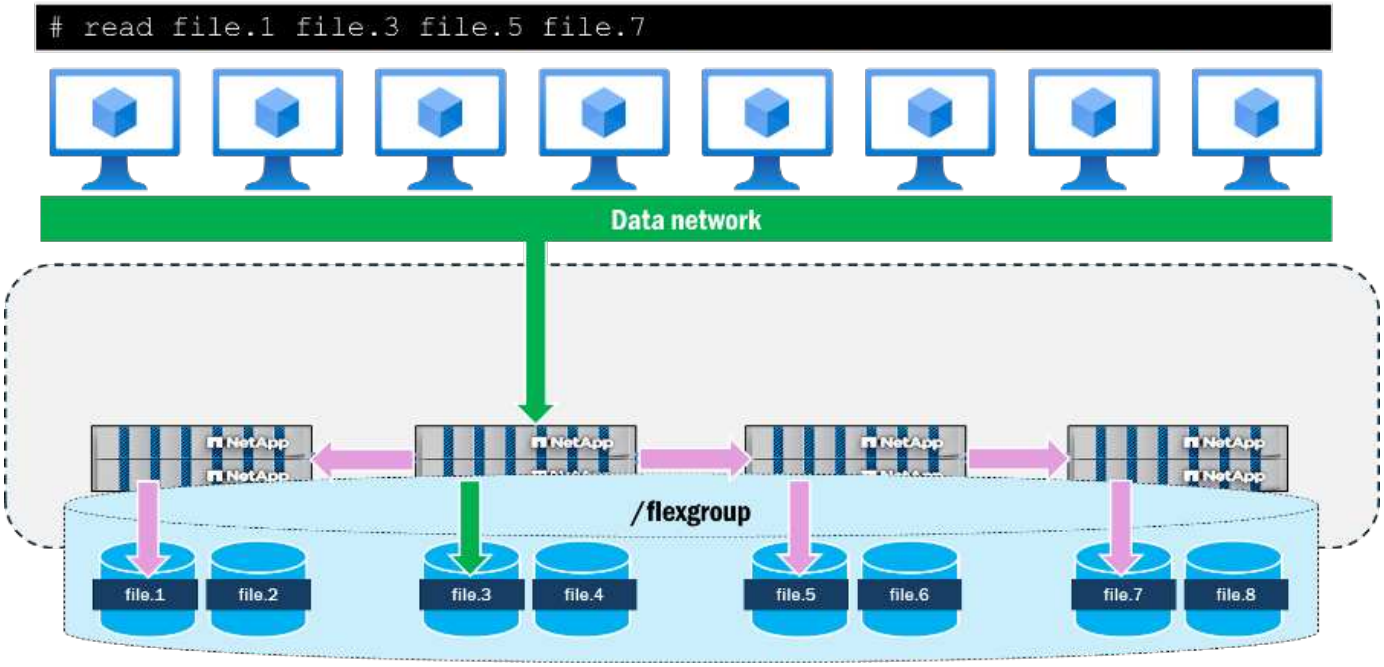


図 **7. pNFS** を使用しない**FlexGroup**ボリュームでの複数の同時ファイル アクセス

pNFSを使用して単一のクライアントから同じ4つのファイルに同時にアクセスする場合、クライアントとサーバはファイルが存在する各ノードへのローカル パスをネゴシエートし、データ操作には複数のTCP接続を使用します。一方、マウント パスはすべてのメタデータ操作の場所として機能します。これにより、ファイルへのローカル パスを使用することでレイテンシが低減されるだけでなく、複数のネットワーク インターフ

ェイスを使用することでスループットも向上します（ただし、クライアントがネットワークを飽和させるのに十分なデータを送信できる場合）。

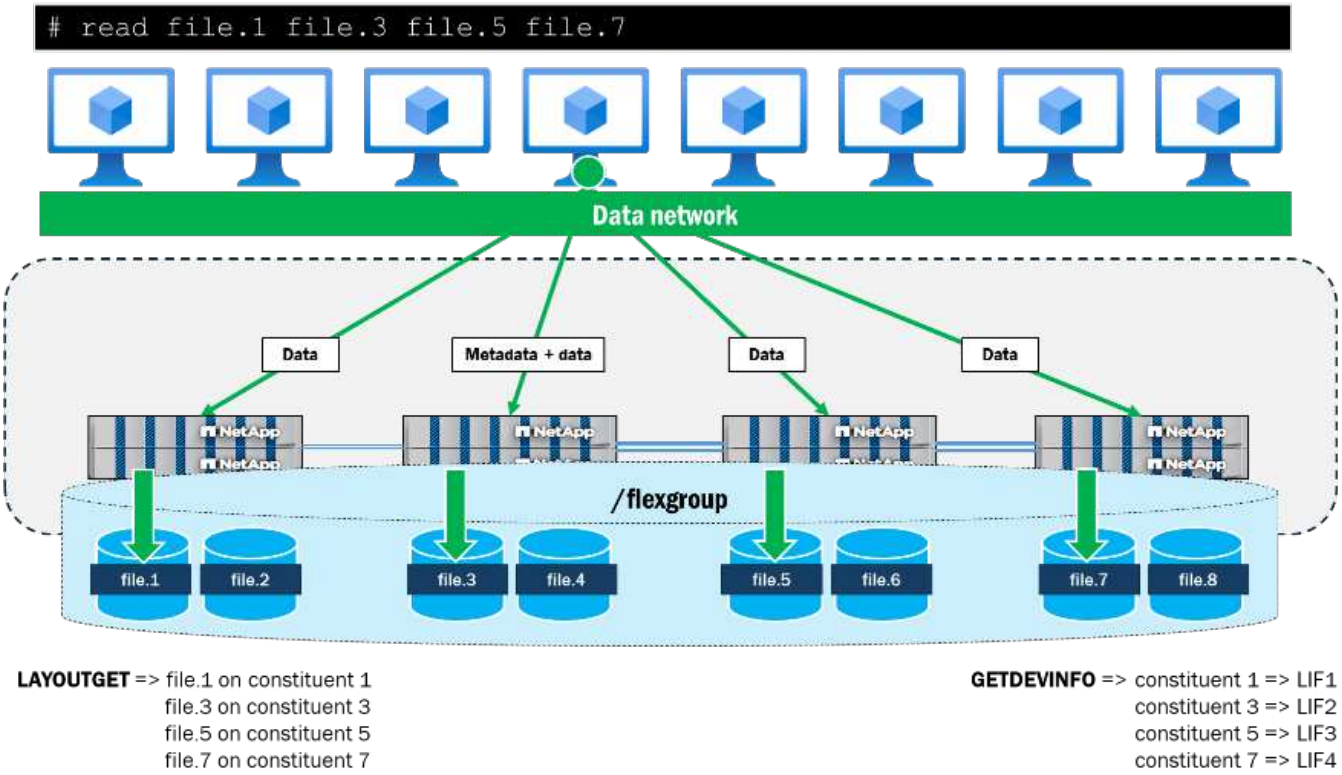


図 **8. pNFS**を使用した**FlexGroup**ボリューム内の複数の同時ファイルアクセス

以下は、単一のRHEL 9.5クライアント上で、2つのONTAPクラスタノードにまたがる異なるコンスティチュエントボリュームにそれぞれ存在する4つの10GBファイルをddを使用して並列に読み取るという簡単なテスト実行の結果です。各ファイルにおいて、pNFSを使用することで全体的なスループットと完了時間が向上しました。pNFSを使用せずにNFSv4.1を使用した場合、マウントポイントに対してローカルなファイルとリモートなファイル間のパフォーマンス差は、pNFSを使用した場合よりも大きくなっていました。

テスト	ファイルあたりのスループット（**MB**/秒）	ファイルあたりの完了時間
NFSv4.1：pNFSなし	• File.1–228（ローカル） • File.2–227（local） • File.3–192（リモート） • File.4–192（リモート）	• File.1–46（ローカル） • File.2–46.1（local） • File.3–54.5（リモート） • File.4–54.5（リモート）
NFSv4.1：pNFS を使用	• File.1–248（ローカル） • File.2–246（ローカル） • File.3–244（pNFS経由のローカル） • File.4–244（pNFS経由のローカル）	• File.1–42.3（local） • File.2–42.6（local） • File.3–43（pNFS経由のローカル） • File.4–43（pNFS経由のlocal）

関連情報

- "FlexGroupボリューム管理"
- "NetAppテクニカルレポート4571：FlexGroupベストプラクティス"

ONTAPにおける**pNFS**のユースケース

pNFSをさまざまなONTAP機能と組み合わせて使用することで、パフォーマンスが向上し、NFSワークロードの柔軟性が向上します。

nconnect を使用した **pNFS**

NFSは、最近のクライアントとサーバーに新しいマウントオプションを導入しました。これにより、単一のIPアドレスをマウントしながら複数のTCP接続を提供することができます。これにより、処理の並列化が向上し、NFSサーバとクライアントの制限を回避できるようになり、特定のワークロードの全体的なパフォーマンスが向上する可能性があります。nconnectは、クライアントがnconnectをサポートしている場合、ONTAP 9.8以降でサポートされます。

pNFSでnconnectを使用する場合、NFSサーバによってアドバタイズされる各pNFSデバイスに対して、nconnectオプションを使用して接続が並列化されます。例えば、nconnectが4に設定され、pNFSに使用できるインターフェースが4つある場合、作成される接続の総数はマウントポイントごとに最大16（nconnect 4個 × IPアドレス4個）になります。

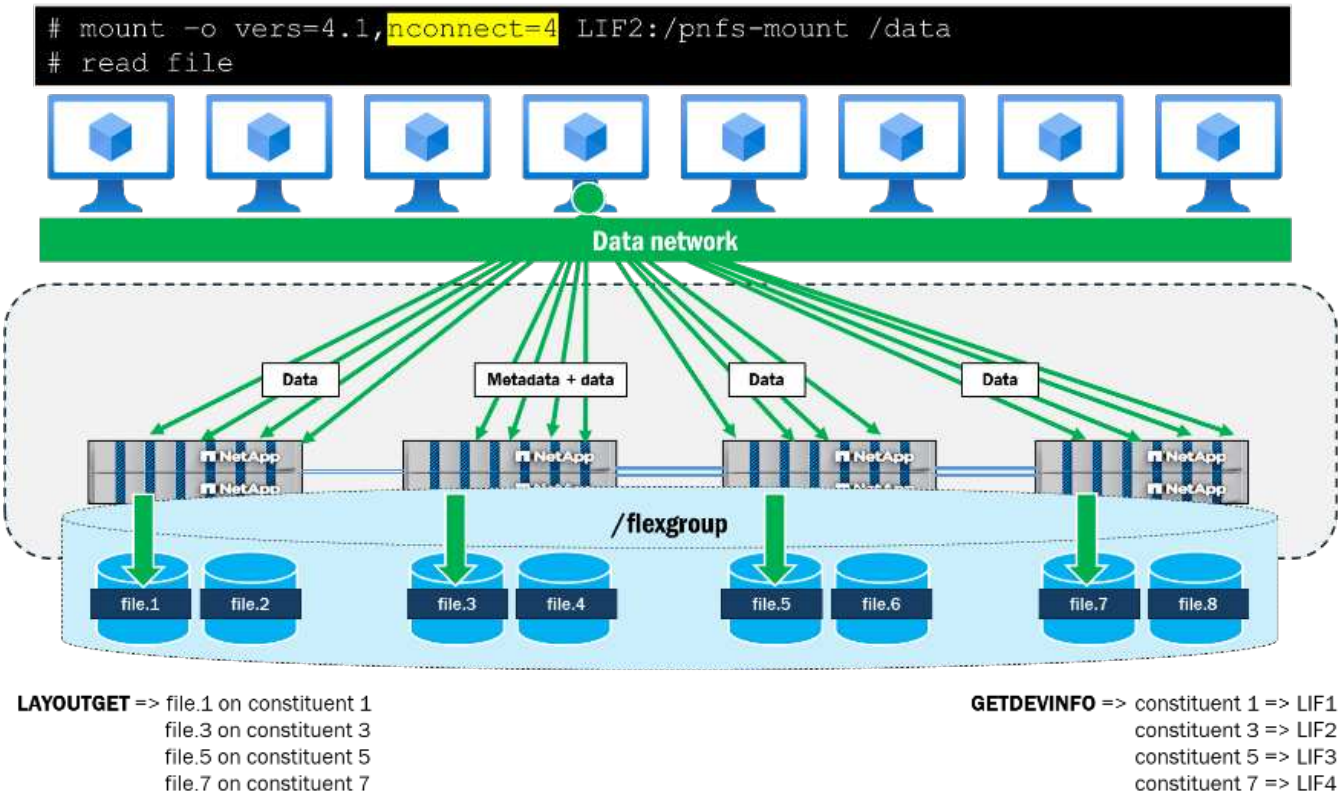


図 **9. nconnect** を **4** に設定した **pNFS**

"ONTAPのNFSv4.1サポートの詳細"

NFSv4.1セッショントランキングを使用したpNFS

NFSv4.1セッション トランキング(["RFC 5661、セクション2.10.5"]）は、クライアントとサーバ間で複数のTCP接続を使用することで、データ転送速度を向上させるものです。NFSv4.1セッション トランキングのサポートはONTAP 9.14.1で追加されており、セッション トランキングをサポートするクライアントと併用する必要があります。

ONTAPでは、クラスタ内の複数のノード間でセッション トランキングを使用することで、接続全体で追加のスループットと冗長性を実現できます。

セッション トランキングは、複数の方法で確立できます：

- *マウント オプションによる自動検出：*最近のほとんどのNFSクライアントでは、マウント オプション（OSベンダーのドキュメントを参照）を介してセッション トランキングを確立できます。マウント オプションはNFSサーバにセッション トランキングに関する情報をクライアントに返すよう指示します。この情報は、NFSパケットを介して `fs_location4`呼び出しとして表示されます。

  使用されるマウント オプションは、クライアントのOSバージョンによって異なります。たとえば、Ubuntu Linuxフレーバーでは通常、 `max_connect=n`を使用してセッション トランクの使用を通知します。RHEL Linuxディストリビューションでは、 `trunkdiscovery`マウント オプションが使用されます。

  Ubuntuの例

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

  RHELの例

  ```
  mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
  ```

  RHEL ディストリビューションで `max_connect`を使用しようとすると、代わりにnconnect として扱われ、セッション トランキングは期待どおりに機能しません。

- *手動で確立：*個々のIPアドレスを同じエクスポート パスとマウント ポイントにマウントすることで、セッション トランキングを手動で確立できます。例えば、エクスポート パスが `/pNFS`である同じノードに2つのIPアドレス（10.10.10.10と10.10.10.11）がある場合、マウント コマンドを2回実行します：

  ```
  mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
  mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
  ```

  トランクに参加させたいすべてのインターフェイスでこのプロセスを繰り返します。

各ノードには独自のセッション トランクがあります。トランクはノードをまたぎません。

pNFSを使用する場合は、セッション トランキング_または_nconnectのいずれかのみを使用してください。両方を使用すると、メタデータ サーバ接続のみがnconnectのメリットを受け、データ サーバは単一の接続を使用するなど、望ましくない動作が発生します。

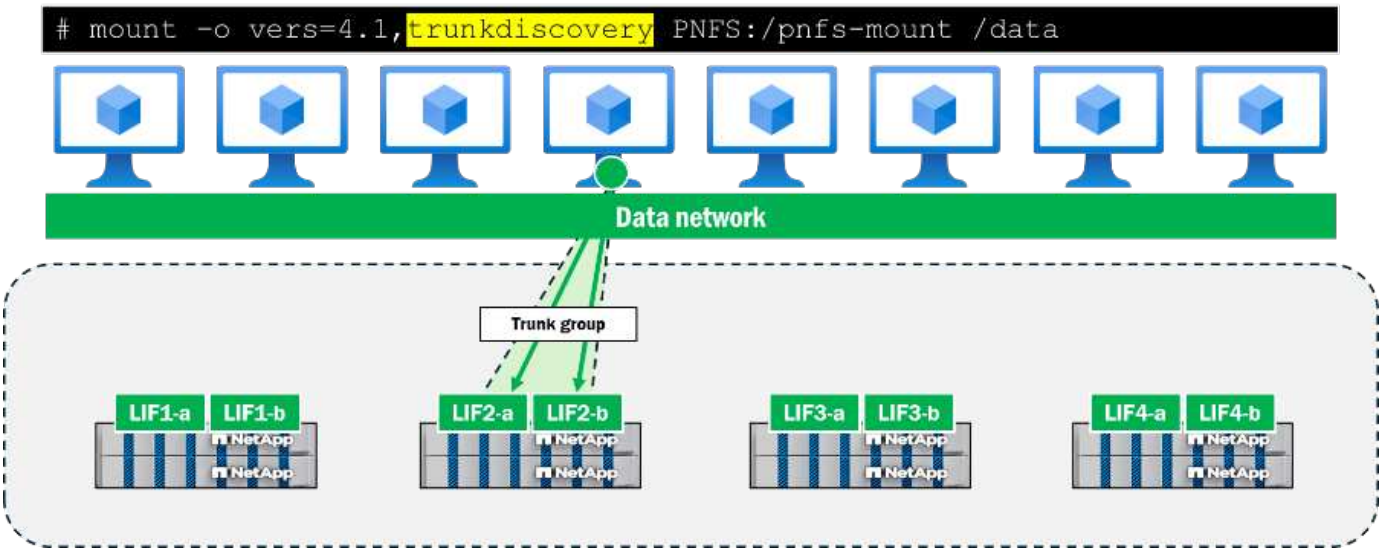
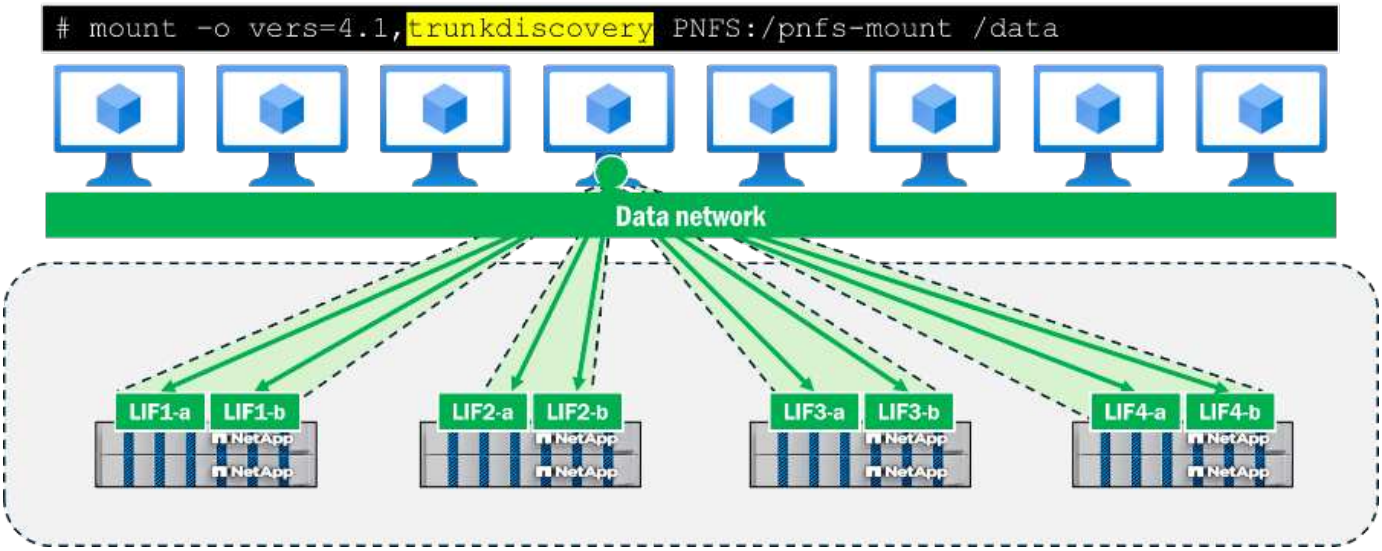


図 **10. ONTAP**での**NFSv4.1**セッション トランキング

pNFSは、クラスタ内の各参加ノードへのローカル パスを提供できます。また、セッション トランキングと併用すると、pNFSはノードごとにセッション トランクを活用して、クラスタ全体のスループットを最大化できます。



`trunkdiscovery`を使用すると、マウントインターフェイスが配置されているNFSサーバ ノード上のリストされたセッション トランク インターフェイスに対して、追加の GETATTR呼び出し（FS_Locations）が利用されます。これらのアドレスが返されると、以降のマウントは返されたアドレスに対して行われます。これは、マウント中のパケット キャプチャで確認できます。

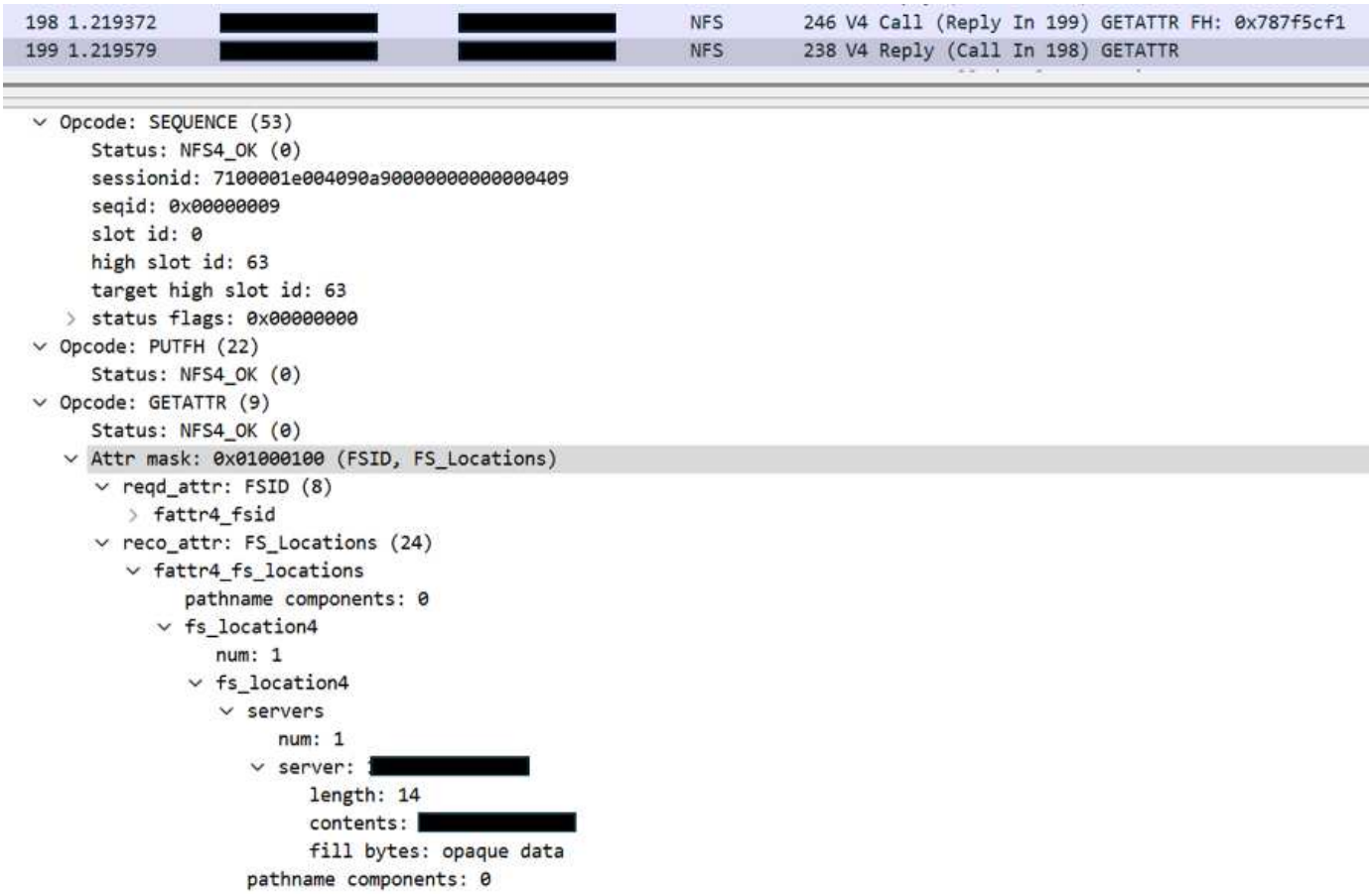


図 **11.** マウント中の**NFS**セッション トランキング検出：パケット キャプチャ

"NFSトランキングの詳細"

pNFS と NFSv4.1 リファラル

NFSv4.1リファーラルは、マウント要求時にクライアントをボリュームの場所に誘導する初期マウント パス リダイレクト モードを提供します。NFSv4.1リファーラルは単一のSVM内で動作します。この機能は、NFS マウントをデータ ボリュームと同じノードにあるネットワーク インターフェースにローカライズしようとします。クライアントにマウントされている間にそのインターフェースまたはボリュームが別のノードに移動した場合、新しいマウントが確立されるまでデータ パスはローカライズされなくなります。

pNFSはマウント パスのローカライズを試みません。代わりに、マウント パスを使用してメタデータ サーバを確立し、必要に応じてデータ パスを動的にローカライズします。

NFSv4.1 リファラルは pNFS でも使用できますが、この機能は不要です。pNFS でリファラルを有効にしても、目立った効果は得られません。

"NFSv4リファーラルの有効化または無効化"

pNFSと高度な容量バランス調整の相互作用

"高度な容量バランシング"ONTAPでは、ファイルデータの一部をFlexGroupボリュームを構成する複数のボリュームに書き込みます（単一FlexVolボリュームではサポートされません）。ファイルのサイズが大きくなると、ONTAPは別の構成ボリューム（同じノードまたは異なるノード）上の新しいマルチパートinodeへのデータの書き込みを開始します。これらのマルチinodeファイルへの書き込み、読み取り、およびメタデータ操作は、クライアントに対して透過的で、中断を伴いません。高度な容量バランス調整により、FlexGroup構成ボリューム間のスペース管理が改善され、より安定したパフォーマンスが実現します。

pNFSは、NFSサーバに格納されているファイル レイアウト情報に応じて、データIOをローカライズされたネットワーク パスにリダイレクトできます。単一の大きなファイルが、クラスタ内の複数のノードにまたがる可能性のある複数の構成ボリュームに分割して作成される場合でも、ONTAPのpNFSは、すべてのファイル パートのファイル レイアウト情報も保持しているため、各ファイル パートにローカライズされたトラフィックを提供できます。ファイルが読み取られると、データ パスのローカル性は必要に応じて変化します。

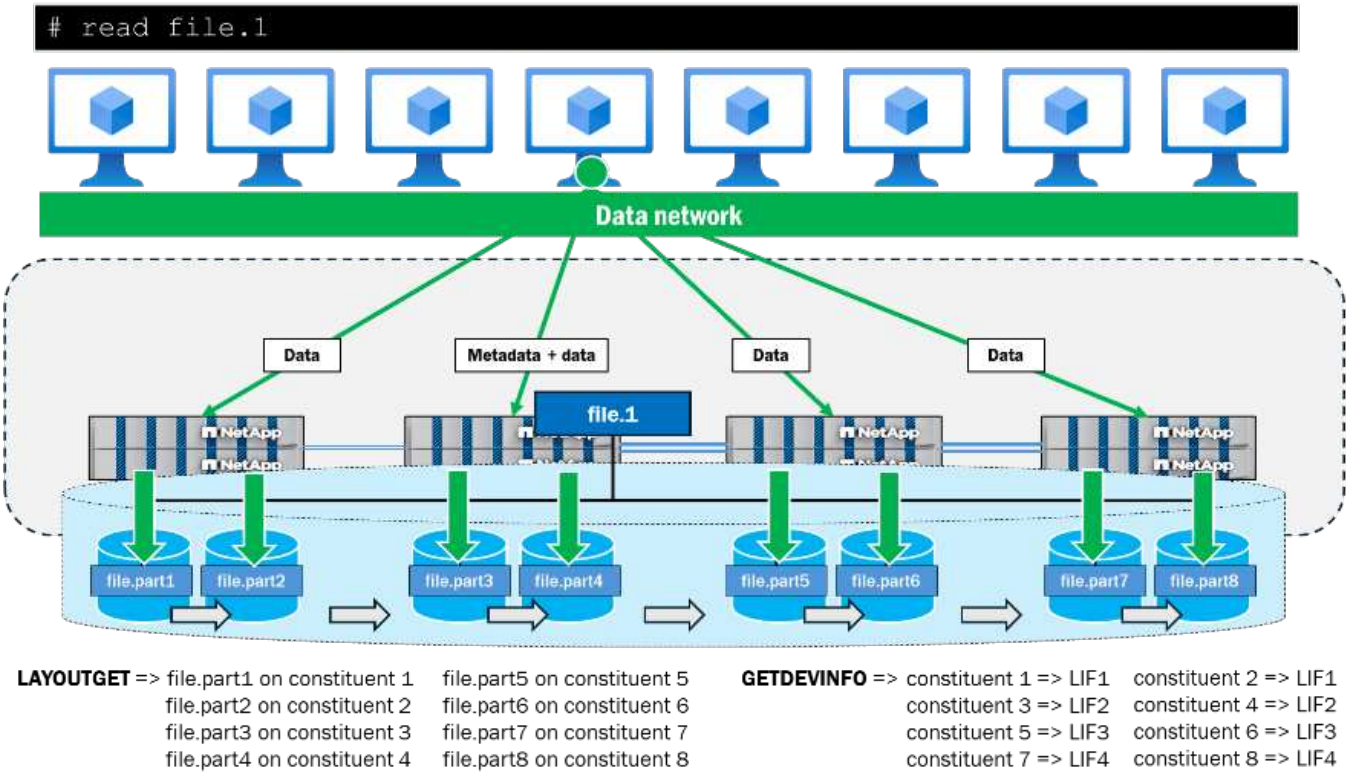


図 **12. pNFS**による高度な容量バランス調整

関連情報

- "FlexGroupボリューム構成"

ONTAPにおける**pNFS**導入戦略

pNFSは、メタデータとデータ パスを分離し、データのローカライズを提供し、並列操作を可能にすることで、従来のNFSを改善するために導入されました。

従来の**NFS**の課題と**pNFS**の利点

次の表は、従来のNFSの課題を示し、ONTAPのpNFSがそれらの課題にどのように対処するかを説明しています。

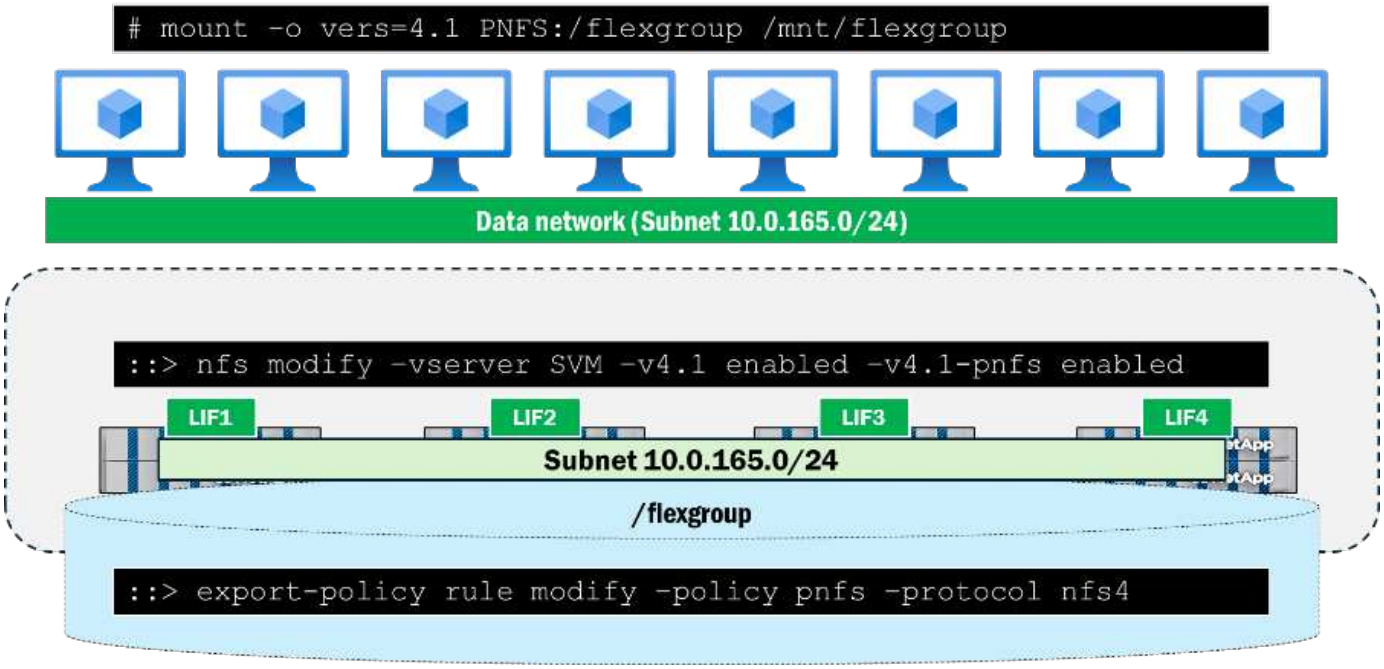
課題	**pNFS**の利点
メタデータとデータの同一パス 従来のNFSでは、メタデータとデータは同じパスを通過します。これにより、単一のパスがクラスタ内の単一のハードウェア ノードに接続されるため、ネットワークとCPUの両方が飽和状態になる可能性があります。多くのユーザーが同じNFSエクスポートにアクセスしようとすると、この問題はさらに悪化します。	メタデータ パスとデータ パスが分離され、データ パスが並列化されます NFS トラフィックのメタデータ パスとデータ パスを分離し、データ パスに複数のネットワーク パスを提供することで、ONTAPクラスタ内のCPUおよびネットワーク リソースが最大化され、ワークロードのスケールが向上します。
ワークロード分散の課題 ONTAP NASクラスタでは最大24ノードまで構成でき、各ノードは独自のデータボリュームとネットワークインターフェイスを持つことができます。各ボリュームは独自のワークロード、またはワークロードのサブセットをホストでき、FlexGroupボリュームでは、単純化のために単一のネームスペースにアクセスする複数のノードにまたがってワークロードを配置できます。クライアントがNFSエクスポートをマウントすると、ネットワーク トラフィックは単一のノードで確立されます。アクセス対象のデータがクラスタ内の別のノードに存在する場合、リモートトラフィックが発生し、ワークロードのレイテンシが増加し、管理が複雑になる可能性があります。	データ構造へのローカルな並列パス pNFSはメタデータからデータパスを分離し、クラスタ内のボリュームのローカル性に応じて複数の並列データパスを提供するため、クラスタ内のネットワーク トラフィックの距離を短縮し、クラスタ内の複数のハードウェアリソースを活用することでレイテンシを削減できます。また、ONTAPのpNFSはデータトラフィックを自動的にリダイレクトするため、管理者は複数のエクスポートパスと場所を管理する必要性が軽減されます。
NFSマウント ポイントの再配置 マウントポイントを確立した後、ボリュームのアンマウントと再マウントを行うと、システム停止が発生します。ONTAPは、ノード間でネットワーク インターフェイスを移行する機能を提供していますが、管理オーバーヘッドが増加し、NFSv4.xを使用したステートフルNFS接続ではシステム停止が発生します。マウント ポイントを再配置する理由の一部は、データの局所性に関する課題に関連しています。	自動パス再配置 pNFSでは、NFSサーバがネットワーク インターフェイスとボリュームの場所を示すテーブルを保持します。pNFSのメタデータ パスを介してクライアントからデータ構造が要求されると、サーバは最適化されたネットワーク パスをクライアントに提供し、クライアントはそのパスをデータ処理に使用します。これにより、ワークロードの管理オーバーヘッドが大幅に削減され、場合によってはパフォーマンスが向上する可能性があります。

構成要件

NetApp ONTAPでpNFSを設定するには、次のものが必要です：

- pNFSをサポートし、NFSv4.1以降でマウントされているNFSクライアント
- ONTAPのNFSサーバでNFSv4.1が有効になっている(`nfs modify -v4.1 enabled`（デフォルトではオフ）
- ONTAPのNFSサーバでpNFSが有効になっている(`nfs modify -v4.1-pnfs enabled`（デフォルトでは無効）
- ノードごとに少なくとも1つのネットワーク インターフェイスがあり、NFSクライアントにルーティング可能

- NFSv4を許可するエクスポート ポリシーとルールを持つSVM内のデータ ボリューム



上記の構成要件が満たされると、pNFS は単独で動作するようになります。

関連情報

- "NFSの設定"
- "ONTAPでのNFSv4.1のサポート"
- "pNFS のネットワーク インターフェイス接続"

Plan

pNFS 展開の計画

環境に pNFS を導入する前に、前提条件を満たしていること、相互運用性の要件と構成の制限を理解していることを確認してください。

前提条件

ONTAPでpNFSを有効にして使用する前に、次の要件が満たされていることを確認してください。

- NFSサーバでNFSv4.1以降が有効になっている
- NFSサーバをホストするSVM用のクラスタ内に少なくとも1つの"ノードごとにデータLIFが存在する"
- すべての"SVM内のデータLIFがルーティング可能である"NFSクライアントへ
- NFSクライアントはpNFSをサポートしています（2014年以降のほとんどの最新のLinuxディストリビューション）
- クライアントとSVM内のすべてのデータLIF間のネットワーク接続が機能している
- DNS解決（ホスト名を使用している場合）がすべてのデータLIFに対して適切に設定されている

- "FlexGroupボリューム"が設定されている（最良の結果を得るには推奨）
- "NFSv4.x IDドメインが一致"クライアントとONTAPの間
- "NFS Kerberos"（使用されている場合）がSVM内のすべてのデータLIFで有効になっている

ベストプラクティスの概要

環境に pNFS を実装する場合は、次のベスト プラクティスに従ってください：

- "FlexGroupボリューム"を使用して、最高のパフォーマンスと容量の拡張を実現
- すべての"SVM内のネットワークインターフェイスがルーティング可能である"をクライアントに確保する
- "NFSv4.0を無効にする"クライアントがNFSv4.1以降を使用するようにします
- マウント ポイントを複数のネットワーク インターフェイスとノードに分散する
- "load balancingメタデータサーバ"にラウンドロビンDNSを使用
- クライアントとサーバーで"NFSv4.x IDドメインが一致"を検証する
- メンテナンス期間中に"ネットワーク インターフェイスの移行"および"ストレージ フェイルオーバー"を実施
- Kerberos セキュリティを使用する場合は、すべてのデータ LIF で "NFS Kerberos" を有効にします。
- pNFSを使用する場合は"NFSv4.1リファーラル"を使用しないでください
- "nconnect設定"TCP接続制限の過大化を避けるため、慎重にテストしてください。
- "セッション トランキング"を"nconnect"の代替として検討してください（両方を併用しないでください）
- 展開前に"クライアントOSベンダーのサポート"pNFSを検証する

相互運用性

ONTAPのpNFSは、RFC準拠のNFSクライアントと連携するように設計されています。以下の点にご注意ください：

- 最新の"2014年以降のLinuxディストリビューション"では pNFS がサポートされています（RHEL 6.4 、Fedora 17 以降）
- クライアントOSベンダーにpNFSがサポートされていることを確認してください
- pNFSは、FlexVolと"FlexGroupボリューム"の両方で動作します。
- pNFSはNFSv4.1および"NFSv4.2"でサポートされています
- pNFSは"NFS Kerberos"（krb5、krb5i、krb5p）で使用できますが、パフォーマンスに影響が出る可能性があります
- pNFSは"nconnect"、または"セッション トランキング"（両方同時には使用できない）と併用できます。
- pNFSは"NFSv4.0"では動作しません

制限

ONTAPのpNFSには次の制限が適用されます。

- "TCP接続制限"ノードあたりの制限はプラットフォームによって異なります（具体的な制限については、NetApp Hardware Universeを確認してください）

- 最大ファイルサイズ：ボリュームタイプとONTAPバージョンによって異なります
- 最大ファイル数：最大2000億ファイル"FlexGroupボリューム"
- 最大容量：最大60PB（"FlexGroupボリューム"使用時）
- "ネットワークインターフェイス数"：ノードごとに少なくとも1つのデータLIFが必要です。ロード バランシングにはさらに多くのLIFが必要になる場合があります

"pNFS を使用した nconnect"を使用する場合、TCP接続数が急速に増加することに注意してください：

- nconnectを使用した各クライアントマウントは、データLIFごとに複数のTCP接続を作成します。
- 多くのクライアントが高いnconnect値を使用すると、"TCP接続制限"を超過する可能性があります
- TCP接続制限を超えると、既存の接続が解放されるまで新しい接続ができなくなります。

関連情報

- "pNFS のネットワーク インターフェイス接続"
- "NFSv4.1の有効化または無効化"
- "ONTAPでのNFSv4.1のサポート"
- "ONTAPでのNFSv4.2のサポート"
- "NetApp Hardware Universe"

pNFS のチューニングとパフォーマンスのベストプラクティス

ONTAPでpNFSを使用する場合は、最良の結果を得るために、次の考慮事項とベスト プラクティスに従ってください。

ボリューム タイプの推奨事項

ONTAPのpNFSはFlexVolボリュームとFlexGroupボリュームの両方で機能しますが、全体的に最良の結果を得るにはFlexGroupボリュームを使用します。

FlexGroupボリュームは以下を提供します：

- pNFSによるデータ トラフィックのローカライズを可能にしながら、クラスタ内の複数のハードウェア リソースにまたがる単一のマウント ポイント
- 大容量の可能性（最大60 PB）と高いファイル数（最大2,000億ファイル）
- 容量のバランシングと潜在的なパフォーマンス上のメリットのためのマルチパート ファイルのサポート
- 単一のワークロードをサポートするボリュームとハードウェアへの並列アクセス

"FlexGroupボリューム管理について学ぶ"

クライアントの推奨事項

すべてのNFSクライアントがpNFSをサポートしているわけではありませんが、最近のクライアントのほとんどはサポートしています。RHEL 6.4とFedora 17は、最初にpNFSをサポートしたクライアントです（2014年頃）。そのため、ここ数年でリリースされたクライアントバージョンは、この機能を完全にサポートしていると想定しても問題ありません。ONTAPのNFSサポートに関するスタンスは、「クライアントが機能をサポートし、RFCに準拠しており、かつONTAPもその機能をサポートしている場合、その組み合わせはサポートさ

れます」というものです。ただし、クライアントOSベンダーがpNFSをサポートしていることを確認することがベストプラクティスです。

ボリューム移動

ONTAPは、同一クラスタ内のノードまたはアグリゲート間でボリュームを無停止で移動できる機能を提供し、容量とパフォーマンスのバランスを柔軟に調整します。ONTAPでボリュームの移動が発生すると、pNFSデバイス マッピングが自動的に更新され、必要に応じてクライアントに新しいボリュームとインターフェイスの関係を使用するように通知されます。

"ボリュームの移動について"

ネットワーク インターフェイスの移行

ONTAPは、パフォーマンスのバランスとメンテナンスの柔軟性を実現するために、同一クラスタ内のノード間でネットワーク インターフェイスを移動する機能を提供します。ボリュームの移動と同様に、ONTAPでネットワーク インターフェイスの移行が行われると、pNFSデバイスのマッピングが自動的に更新され、必要に応じて新しいボリュームとインターフェイスの関係を使用するようにクライアントに通知されます。

ただし、NFSv4.1はステートフル プロトコルであるため、ネットワーク インターフェイスの移行は、NFSマウントをアクティブに使用しているクライアントに混乱をもたらす可能性があります。ネットワーク インターフェイスの移行はメンテナンス ウィンドウ内に実施し、ネットワークの混乱が発生する可能性があることをクライアントに通知することがベスト プラクティスです。

ストレージのフェイルオーバー/ギブバック

pNFSは、NFSv4.1と同じストレージフェイルオーバーの考慮事項に従います。これらの詳細については"NetAppテクニカル レポート4067：『NFS Best Practice and Implementation Guide』"を参照してください。一般に、pNFSに関連するストレージフェイルオーバー/ギブバックは、プロトコルのステートフル性によりストレージの中断が発生する可能性があることを考慮して、メンテナンスウィンドウ内で実行する必要があります。

メタデータのワークロード

メタデータ操作はサイズが小さいですが、ワークロード（大量のファイルを作成しているか、「find」コマンドを実行しているかなど）やファイル総数に応じて、操作回数が大きくなることがあります。そのため、メタデータ呼び出しが多いワークロードは、NFSサーバのCPUに負荷をかけ、単一の接続でボトルネックとなる可能性があります。pNFS（およびNFSv4.x全般）は、ステートフル性、ロックメカニズム、およびプロトコル バージョンのセキュリティ機能がCPU使用率とレイテンシに悪影響を与える可能性があるため、パフォーマンスに依存する高メタデータワークロードには適していません。これらのワークロードタイプ（GETATTRやSETATTRの呼び出しが多いなど）は、一般的にNFSv3の方が適しています。

メタデータサーバ

pNFSのメタデータ サーバは、NFSエクスポートの最初のマウント時に確立されます。マウント ポイントが確立されると、再マウントされるかデータ インターフェイスが移動されるまで、そのマウント ポイントはそのまま維持されます。そのため、同じボリュームにアクセスする複数のクライアントが、SVM全体の異なるノードとデータ インターフェイスにマウントされるようにすることがベスト プラクティスです。このアプローチにより、ノードとCPUリソース間でメタデータ サーバのロード バランシングが実現され、クラスタ内のネットワーク インターフェイスを最大限に活用できます。これを実現する方法の1つとして、ラウンドロビンDNS設定を確立することが挙げられます。これについては"NetAppテクニカルレポート4523：ONTAPにおけるDNSロードバランシング"で説明します。

NFSv4.x IDドメイン

NFSv4.xは様々な方法でセキュリティ機能を提供します（詳細は "NetAppテクニカル レポート4067：『NFS Best Practice and Implementation Guide』"で説明されています）。NFSv4.x IDドメインはその一つで、NFSエクスポートでユーザーとグループを認証する際に、クライアントとサーバーはIDドメインについて合意する必要があります。IDドメインの不一致による副作用の一つとして、不要なアクセスを防ぐために、ユーザーまたはグループが匿名ユーザー（実質的には圧縮されたユーザー）として表示されることがあります。NFSv4.x（およびpNFS）では、クライアントとサーバーのNFSv4.x IDドメインが一致していることを確認することがベストプラクティスです。

nconnect

前述の通り、ONTAPのnconnectは一部のワークロードのパフォーマンス向上に役立ちます。pNFSでは、nconnectはストレージ システムへのTCP接続数を大幅に増加させることでパフォーマンスを向上させる一方で、多くのクライアントがマウント オプションを利用する場合、ストレージへのTCP接続が過負荷になり、問題が発生する可能性があることを理解しておくことが重要です。NetApp Hardware Universeでは、ノードあたりのTCP接続制限について説明しています。

ノードのTCP接続制限を超えると、既存の接続が解放されるまで新しいTCP接続は許可されません。これにより、マウント ストームが発生する可能性のある環境では、問題が発生する可能性があります。

次の表は、nconnect を使用した pNFS が TCP 接続制限を超える可能性があることを示しています：

クライアント数	**nconnect**値	マウントあたり、ノードあたりの潜在的な**TCP**接続の合計数
1	4	4
100	4	400
1000	8	8000
10000	8	80000
10000	16	160000 [1]

[1] ほとんどのONTAPシングルノードTCP接続制限を超えています

NFSv4.1セッション トランキング

ONTAPのセッション トランキングは、NFSv4.xマウントのスループットとパスの復元力を向上させるために使用できます。pNFSと併用すると、クラスタ内の各ノードでセッション トランクを確立できます。ただし、セッション トランクはノードごとに少なくとも2つのインターフェイスを必要とし、pNFSは意図したとおりに動作するためにノードごとに少なくとも1つのインターフェイスを必要とします。さらに、SVM内のすべてのインターフェイスがNFSクライアントにルーティング可能である必要があります。セッション トランキングとpNFSは、nconnectも併用すると正常に動作しません。nconnectとセッション トランキングは相互に排他的な機能であることを考慮してください。

"NFSトランキングについて"

ネットワーク インターフェイスの接続

pNFSが正常に機能するには、クラスタ内の各ノードにルーティング可能なネットワークインターフェースが必要です。pNFSをホストするNFSサーバと同じSVM内に、NFSクライアントにルーティングできないネットワークインターフェースが存在する場合でも、ONTAPはデバイスマッピングでそれらのインターフェースをクライアントにアドバタイズします。NFSクライアントが異なるサブネットのインターフェース経由でデータにアクセスしようとすると、接続できず、システム停止が発生します。pNFSを使用する場合は、SVM内でク

ライアントがアクセスできるネットワークインターフェースのみを許可するのがベストプラクティスです。

> デフォルトでは、pNFSデバイス リストにSVM内のすべてのデータLIFが入力されるため、pNFSではSVM内のすべてのデータLIFがNFSクライアントのインターフェイスにルーティング可能である必要があります。その結果、ルーティング不可能なデータLIFが選択され、停止シナリオが発生する可能性があります。ベスト プラクティスとして、pNFSを使用する場合は、ルーティング可能なデータLIFのみを設定してください。
>
> ONTAP 9.18.1 RC1以降では、サブネットごとにpNFSトラフィックの対象となるインターフェースを指定できるようになりました。これにより、ルーティング可能なインターフェースとルーティング不可能なインターフェースを混在させることができます。コマンドの詳細については、NetAppサポートにお問い合わせください。

NFSv4.0

NFSv4.0は、ONTAP NFSサーバでNFSv4.1と併用できるオプションです。ただし、pNFSはNFSv4.0上では動作しません。NFSサーバでNFSv4.0が有効になっている場合、クライアントが意図せずそのプロトコル バージョンをマウントし、pNFSを利用できなくなる可能性があります。そのため、pNFSを使用する場合は、NFSv4.0を明示的に無効にすることがベストプラクティスです。NFSv4.1は引き続き有効にする必要があり、NFSv4.0とは独立して動作します。

NFSv4.1リファーラル

NFSv4.1 参照は、クライアントからボリュームを所有するノード上のネットワーク インターフェイスへのマウント パスをローカライズします。pNFS はデータ パスをローカライズし、マウント パスはメタデータ サーバになります。

これら2つの機能は併用可能ですが、NFSv4.1のリファーラルをpNFSで使用すると、複数のメタデータ サーバを同一ノード上にスタックし、複数のクラスタ ノードにメタデータ サーバを分散させる能力が低下するという望ましくない影響が生じる可能性があります。pNFSを使用する場合、メタデータ サーバがクラスタ全体に均等に分散されていないと、単一ノードのCPUがメタデータ要求で過負荷になり、パフォーマンスのボトルネックが発生する可能性があります。

そのため、pNFSを使用する場合はNFSv4.1リファラルの使用を避けることがベストプラクティスです。代わりに、マウント ポイントをクラスタ内の複数のネットワーク インターフェイスとノードに分散させてください。

"NFSv4リファーラルの有効化または無効化について学習します"

NFS Kerberos

NFS Kerberos では、krb5 による認証の暗号化に加え、krb5i および krb5p によるデータパケットの暗号化が可能です。これは SVM 内のネットワークインターフェースごとに有効化され、詳細は "NetApp テクニカルレポート 4616：ONTAP における NFS Kerberos と Microsoft Active Directory"で説明されています。

pNFSはSVM内のノードおよびネットワーク インターフェイス間でデータ トラフィックをリダイレクトできるため、SVM内の各ネットワーク インターフェイスでNFS Kerberosが有効になっていて機能している必要があります。SVM内のいずれかのネットワーク インターフェイスでKerberosが有効になっていない場合、pNFSはそれらのインターフェイス上のデータ ボリュームにアクセスしようとしても正常に機能しません。

例えば、2つのネットワーク インターフェイス（Kerberosが有効になっているのは1つだけ）を備えたpNFS対応SVMで並列ddを用いた読み取りテストを実行したところ、Kerberos対応インターフェース上のファイルは正常に動作しましたが、Kerberosが有効になっていないインターフェースを持つノード上のファイルは読み取

りを完了できませんでした。両方のインターフェースでKerberosを有効にすると、すべてのファイルが期待どおりに動作しました。

SVM内のすべてのネットワーク インターフェイスでNFS Kerberosが有効になっている場合、pNFSでNFS Kerberosを使用できます。NFS Kerberosはパケットの暗号化/復号化によってパフォーマンスが低下する可能性があることにご注意ください。そのため、パフォーマンスの低下がワークロードに過度の影響を及ぼさないことを確認するために、ワークロードでpNFSとNFS Kerberosを徹底的にテストすることをお勧めします。

以下は、RHEL 9.5 クライアント上の pNFS で krb5（認証）と krb5p（エンドツーエンド暗号化）を使用した場合の並列読み取りパフォーマンスの例です。このテストでは、krb5p のパフォーマンスが 70% 低下しました。

Kerberosフレーバー	**MB/s**	完了時間
krb5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43.1 • File3-44 • File4-44.1
krb5p	• File1-72.9 • File2-72.8 • File3-71.4 • File4-71.2	• File1-143.9 • File2-144.1 • File3-146.9 • File4-147.3

"強力なセキュリティを実現するNFSでのKerberosについて学ぶ"

NFSv4.2

NFSv4.2はONTAP 9.8に追加され、利用可能な最新のNFSv4.xバージョンです（RFC-7862）。NFSv4.2には、有効化/無効化を明示的に指定するオプションはありません。代わりに、NFSv4.1と同時に有効化/無効化されます(`-4.1 enabled`。クライアントがNFSv4.2をサポートしている場合、 `minorversion=2`マウント オプションで別途指定しない限り、マウント コマンドの実行中にサポートされているNFSの最新バージョンがネゴシエートされます。

ONTAPのNFSv4.2は次の機能をサポートしています：

- セキュリティ ラベル（MACラベル）
- 拡張属性
- スパース ファイル操作（FALLOCATE）

pNFS は NFSv4.1 で導入されましたが、NFSv4.2 でも、付随する機能とともにサポートされています。

"ONTAP の NFSv4.2 サポートについて学ぶ"

pNFSコマンド、統計、イベント ログ

これらのONTAP CLIコマンドはpNFSに特化しており、設定、トラブルシューティン

グ、統計情報の収集に使用できます。

NFSv4.1の有効化

```
nfs modify -vserver SVM -v4.1 enabled
```

pNFSを有効にする

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

pNFSデバイスを表示する（**advanced**権限）

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

pNFSデバイス マッピングを表示する（**advanced**権限）

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

pNFS固有のパフォーマンス カウンターをキャプチャする（高度な権限）

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

pNFS固有のパフォーマンス カウンタを表示する（**advanced**権限）

```
statistics show -object nfsv4_1 -vserver SVM
```

pNFS固有のカウンターのリストを表示する（高度な権限）

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                      Description
---------------------------- ----------------------------------------------
getdeviceinfo_avg_latency    Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error          The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent        Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success        The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total          Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency    Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error          The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent        Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success        The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total          Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency     Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error           The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent         Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success         The number of successful NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_total           Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency        Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error              The number of failed NFSv4.1 LAYOUTGET
```

```
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

NFSのアクティブなネットワーク接続を表示する

`network connections active show`コマンドを使用して、SVMへの複数のTCP接続が確立されているかどうかを確認できます。

たとえば、NFSセッション トランクを表示する場合は、ノードごとに異なるインターフェイスを介して同じクライアントからの接続を探します：

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
               Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

接続されたクライアントの**NFS**バージョン情報を表示する

`nfs connected-clients show`コマンドで
NFS接続を表示することもできます。表示されるクライアント リストは、過去
48時間以内にアクティブなNFSトラフィックがあったクライアントであることに注意してください
。アイドル状態のNFSクライアント（マウントされている場合でも）は、マウントにアクセスするまで表示されない場合があります。 `-idle-
time`機能を指定することで、これらのクライアントをフィルタリングし、最近アクセスしたクライアントのみを表示できます。

たとえば、pNFS SVM の過去 10 分間にアクティビティがあったクライアントを表示するには：

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

関連情報

- "ONTAPでの並列NFS（pNFS）について"

NFS / SMBファイルとディレクトリの命名規則

ONTAP NFSおよびSMBのファイルとディレクトリの命名依存関係について学習します

ファイルとディレクトリの命名規則は、ONTAPクラスタとクライアントの言語設定に加えて、ネットワーク クライアントのオペレーティング システムとファイル共有プロトコルの両方に依存します。

オペレーティング システムとそのファイル共有のプロトコルの種類によって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ファイル、ディレクトリ、qtreeの名前でマルチバイト文字がサポートされるかどうかは、ONTAPのリリースによって異なります。

ONTAP NFS SVMのさまざまなオペレーティングシステムで有効な文字について学習します。

異なるオペレーティング システムを搭載したクライアントからファイルまたはディレク

トリにアクセスする場合は、両方のオペレーティング システムで有効な文字を使用する必要があります。

例えば、UNIXを使用してファイルまたはディレクトリを作成する場合、コロン（：）はMS-DOSのファイル名またはディレクトリ名では使用できないため、名前にコロンを使用しないでください。有効な文字の制限はオペレーティングシステムによって異なるため、使用禁止文字の詳細については、クライアントオペレーティングシステムのドキュメントを参照してください。

ONTAP NFSマルチプロトコル環境におけるファイル名とディレクトリ名の大文字と小文字の区別について学習します

ファイル名とディレクトリ名について、NFSクライアントでは大文字と小文字が区別されますが、SMBクライアントでは大文字と小文字が区別されず、同じ文字として扱われます。この違いがマルチプロトコル環境に及ぼす影響、およびSMB共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにどのように対処すべきかを理解しておく必要があります。

SMBクライアントが `testdir`という名前のディレクトリを作成した場合、SMBクライアントとNFSクライアントの両方でファイル名が `testdir`として表示されます。ただし、SMBユーザーが後から `TESTDIR`という名前のディレクトリを作成しようとした場合、SMBクライアントにとってその名前が既に存在するため、その名前は許可されません。NFSユーザーが後から `TESTDIR`という名前のディレクトリを作成した場合、NFSクライアントとSMBクライアントは、次のように異なるディレクトリ名を表示します：

- NFS クライアントでは、ディレクトリ名は大文字と小文字が区別されるため、 `testdir`と `TESTDIR`のように、作成されたとおりに両方のディレクトリ名が表示されます。
- SMBクライアントでは、2つのディレクトリを区別するために8.3形式の名前が使用されます。1つのディレクトリには基本ファイル名が付けられます。以降のディレクトリには8.3形式の名前が割り当てられます。
  - SMB クライアントでは、 `testdir`および `TESTDI~1`が表示されます。
  - ONTAP は、2 つのディレクトリを区別するために `TESTDI~1`ディレクトリ名を作成します。

    この場合、Storage Virtual Machine（SVM）での共有の作成時または変更時に共有パスを指定するときは、8.3形式の名前を使用する必要があります。

ファイルについても同様に、SMBクライアントが `test.txt`を作成した場合、SMBクライアントとNFSクライアントの両方でファイル名が `text.txt`と表示されます。ただし、SMBユーザーが後から `Test.txt`を作成しようとしても、SMBクライアントにとってその名前が既に存在しているため、その名前は許可されません。NFSユーザーが後から `Test.txt`という名前のファイルを作成した場合、NFSクライアントとSMBクライアントでは、ファイル名が次のように異なって表示されます：

- NFS クライアントでは、ファイル名は大文字と小文字が区別されるため、作成されたときの `test.txt`と `Test.txt`の両方のファイル名が表示されます。
- SMBクライアントでは、2つのファイルを区別するために8.3形式の名前が使用されます。一方のファイルには基本ファイル名が付けられます。追加のファイルには、8.3形式のファイル名が割り当てられます。
  - SMB クライアントでは、 `test.txt`および `TEST~1.TXT`が表示されます。
  - ONTAPは、2つのファイルを区別するために `TEST~1.TXT`ファイル名を作成します。

文字マッピングがvserver cifs character-mappingコマンドを使用して作成されている場合、通常は大文字と小文字が区別されないWindows検索で大文字と小文字が区別されるようになる可能性があります。つまり、文字マッピングが作成されていて、その文字マッピングがファイル名に使用されている場合にのみ、ファイル名検索で大文字と小文字が区別されます。

ONTAP NFSのファイル名とディレクトリ名の作成について学習します

ONTAPは、SMBクライアントからアクセスできるディレクトリ内のファイルまたはディレクトリに対して、元の長い名前と8.3形式の名前の2つの名前を作成して維持します。

8文字の名前または3文字の拡張子の制限（ファイルの場合）を超えるファイル名またはディレクトリ名の場合、ONTAPは次のように8.3形式の名前を生成します：

- 名前が6文字を超える場合、元のファイル名またはディレクトリ名を6文字に切り捨てます。
- 切り捨てられた後に一意ではなくなったファイル名またはディレクトリ名に、チルダ（~）と1から5までの数字を追加します。

  類似した名前が5つ以上あるために数字が足りなくなった場合は、元の名前とは関係のない一意の名前が作成されます。

- ファイルの場合、ファイル名拡張子は3文字に切り捨てられます。

たとえば、NFSクライアントが `specifications.html`という名前のファイルを作成すると、ONTAPによって作成される8.3形式のファイル名は `specif~1.htm`になります。この名前がすでに存在する場合、ONTAPはファイル名の末尾に別の番号を使用します。たとえば、NFSクライアントが `specifications_new.html`という名前の別のファイルを作成すると、 `specifications_new.html`の8.3形式は `specif~2.htm`になります。

ONTAP NFSによるマルチバイトのファイル名、ディレクトリ名、qtree名の処理について学習します。

ONTAP 9.5以降では、4バイトのUTF-8エンコード形式の名前がサポートされるようになり、Basic Multilingual Plane（BMP;基本多言語面）以外のUnicode補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。以前のリリースでは、これらの補助文字はマルチプロトコル環境では正しく表示されませんでした。

4バイトのUTF-8でエンコードされた名前のサポートを有効にするために、 `vserver`および `volume`コマンドファミリで新しい_utf8mb4_言語コードが使用可能です。

- 次のいずれかの方法で新しいボリュームを作成する必要があります。
- volume `-language`オプションを明示的に設定：

  ```
  volume create -language utf8mb4 {…}
  ```

- `-language`オプション付きで作成された、またはオプション用に変更されたSVMからボリュームオプションを継承します：

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- ONTAP 9.6以前を使用している場合、既存のボリュームをutf8mb4をサポートするように変更することはできません。utf8mb4対応の新しいボリュームを作成し、クライアントベースのコピー ツールを使用してデータを移行する必要があります。

  ONTAP 9.7P1以降をご利用の場合は、サポートリクエストを送信することで、既存のボリュームをutf8mb4に変更できます。詳細については、"ONTAPでボリューム言語を作成後に変更できますか？"をご覧ください。

+ SVM を utf8mb4 サポート用に更新できますが、既存のボリュームでは元の言語コードが保持されます。

+

ⓘ 現在のところ、4バイトのUTF-8文字を含むLUN名はサポートされていません。

- 一般に、Unicode文字データは、Windowsファイルシステム アプリケーションでは16-bit Unicode Transformation Format（UTF-16）、NFSファイルシステムでは8-bit Unicode Transformation Format（UTF-8）を使用して表現されます。

  ONTAP 9.5よりも前のリリースでは、Windowsクライアントで作成されたUTF-16の補助文字を含む名前は、他のWindowsクライアントには正しく表示されましたが、NFSクライアントではUTF-8に正しく変換されませんでした。同様に、NFSクライアントで作成されたUTF-8の補助文字を含む名前は、WindowsクライアントでUTF-16に正しく変換されませんでした。

- ONTAP 9.4以前を実行するシステムで補助文字を（有効か無効かにかかわらず）含むファイル名を作成すると、ONTAPはそのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

  この問題を回避するには、ファイル名にBMP文字のみを使用して補助文字は使用しないようにするか、ONTAPを9.5以降にアップグレードしてください。

Unicode文字をqtree名に使用できます。

- `volume qtree`コマンド ファミリまたは System Manager のいずれかを使用して、qtree 名を設定または変更できます。
- 日本語や中国語などのUnicode形式のマルチバイト文字をqtree名に含めることができます。
- ONTAP 9.5よりも前のリリースでは、BMP文字（つまり3バイトで表現可能な文字）のみがサポートされます。

ⓘ ONTAP 9.5より前のリリースでは、qtreeの親ボリュームのジャンクションパスに、Unicode文字を使用したqtree名とディレクトリ名を含めることができます。`volume show`コマンドは、親ボリュームの言語設定がUTF-8の場合、これらの名前を正しく表示します。ただし、親ボリュームの言語がUTF-8言語設定のいずれにも該当しない場合、ジャンクションパスの一部は数値のNFS代替名で表示されます。

- 9.5以降のリリースでは、qtreeがutf8mb4に対応したボリュームに含まれていれば、qtree名で4バイト文字がサポートされます。

ONTAP NFSボリューム上のSMBファイル名変換の文字マッピングを構成する

NFSクライアントは、SMBクライアントと特定のWindowsアプリケーションでは無効な

文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効なNFS名を持つファイルにSMBクライアントからアクセスできます。

タスク概要

NFSクライアントによって作成されたファイルにSMBクライアントがアクセスすると、ONTAPはファイル名を確認します。ファイル名が有効なSMBファイル名でない場合（例えば、コロン「:」が含まれている場合）、ONTAPは各ファイルに保持されている8.3形式のファイル名を返します。ただし、重要な情報を長いファイル名にエンコードするアプリケーションでは、この方法では問題が発生します。

したがって、異なるオペレーティング システムを使用するクライアント間でファイルを共有する場合は、両方のオペレーティング システムで有効な文字をファイル名に使用するようにしてください。

これとは別に、SMBクライアントで有効でない文字を含むNFSクライアントが作成したファイル名がある場合は、無効なNFSの文字を、SMBと特定のWindowsアプリケーションの両方で有効なUnicode文字に変換するマッピングを定義できます。たとえば、この機能はCATIAR MCADおよびMathematicaアプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に留意する必要があります。

- 文字マッピングは、ジャンクション ポイントを越えて適用されることはありません。

  文字マッピングは、各ジャンクション ボリュームに対して明示的に設定する必要があります。

- 無効な文字を表すUnicode文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

  たとえば、コロン（：）をハイフン（-）にマッピングしようとしたが、ファイル名でハイフン（-）が正しく使用されていた場合、Windowsクライアントが “a-b” という名前のファイルにアクセスしようとすると、その要求はNFS名 “a:b” にマッピングされます（望ましい結果ではありません）。

- 文字マッピングを適用してもまだマッピングに無効なWindows文字が含まれている場合、ONTAP はWindows 8.3ファイル名にフォールバックします。
- FPolicy通知、NAS監査ログ、セキュリティ トレース メッセージでは、マッピングされたファイル名が表示されます。
- タイプがDPであるSnapMirror関係が作成されても、ソース ボリュームの文字マッピングはデスティネーションDPボリュームにレプリケーションされません。
- 大文字と小文字の区別：マッピングされたWindows名はNFS名に変わるため、名前の検索もNFSの基準に従います。これには、検索時に大文字と小文字が区別されることも含まれます。そのため、マッピングされた共有にアクセスするアプリケーションは、Windowsの大文字と小文字を区別しない動作に依存できません。ただし8.3形式の名前は（大文字と小文字が区別されませんが）使用可能です。
- 部分マッピングまたは無効なマッピング：名前をマッピングしてクライアントに戻ったあと、「dir」コマンドでディレクトリのファイル一覧を表示すると、生成されたUnicode名がWindowsで有効かどうかチェックされます。この名前に無効な文字が含まれているか、Windowsで無効なファイル名（「.」または空白で終了するなど）の場合は、無効なファイル名の代わりに8.3形式の名前が返されます。

手順

1. 文字マッピングを設定します。

```
vserver cifs character-mapping create -vserver vserver_name -volume
volume_name -mapping mapping_text, ...
```

マッピングは、ソースとターゲットの文字ペアを「:」で区切ったリストで構成されます。文字は16進数で入力されたUnicode文字です。例：3C：E03C。

コロンで区切られた各 `mapping_text`ペアの最初の値は、変換するNFS文字の16進値であり、2番目の値はSMBが使用するUnicode値です。マッピングペアは一意である必要があります（1対1のマッピングが存在する必要があります）。

- ソースマッピング

  次の表に、ソース マッピングで許可されているUnicode文字セットを示します。

Unicode文字	印刷文字	概要
0x01-0x19	該当なし	表示されない制御文字
0x5C	\	バックスラッシュ
0x3A	：	コロン
0x2A	*	アスタリスク
0x3F	?	疑問符
0x22	"	引用符
0x3C	<	小なり
0x3E	>	より大きい
0x7C		
縦線	0xB1	±

- ターゲットマッピング

  対象文字は、Unicodeの「`Private Use Area`」内のU+E0000…U+F8FFの範囲で指定できます。

例

次のコマンドは、ストレージ仮想マシン（SVM）vs1上の「`data`」という名前のボリュームの文字マッピングを作成します：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

SMBファイル名変換の文字マッピングを管理するためのONTAP NFSコマンド

FlexVol上でのSMBファイル名の変換に使用する情報を作成、変更、表示したり、それに使用するファイル文字マッピングを削除することによって文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成する	`vserver cifs character-mapping create`
ファイル文字マッピング情報を表示する	`vserver cifs character-mapping show`
既存のファイル文字マッピングを変更する	`vserver cifs character-mapping modify`
ファイル文字マッピングを削除する	`vserver cifs character-mapping delete`

`vserver cifs character-mapping`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+cifs+character-mapping["ONTAPコマンドリファレンス"^]をご覧ください。