エクスポート ポリシーを使用した NFSアクセスの保護

ONTAP 9

NetApp
February 12, 2026

目次

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。

ONTAP NFSエクスポート ルールの仕組み

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。

ONTAP NFSスーパーユーザーアクセス要求の管理について学習します

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。

`-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

キャッシュ名	保存される情報の種類
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`

qtree ID検証を行う場合は…	入力するコマンド
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。