エクスポートポリシーを使用して NFS アクセスを保護

ONTAP 9

NetApp
April 24, 2024

目次

エクスポートポリシーを使用して NFS アクセスを保護

エクスポートポリシーがボリュームまたは qtree へのクライアントアクセスを制御する仕組み

エクスポートポリシーには、各クライアント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 _ が含まれています。このプロセスの結果、クライアントアクセスを許可するかどうか、およびアクセスのレベルが決まります。クライアントがデータにアクセスするためには、エクスポートルールを含むエクスポートポリシーが Storage Virtual Machine （ SVM ）上に存在する必要があります。

ボリュームまたは qtree へのクライアントアクセスを設定するには、各ボリュームまたは qtree にポリシーを 1 つ関連付けます。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 を含む SVM に対して次の操作を実行できます。

- SVM のボリュームまたは qtree ごとに異なるエクスポートポリシーを割り当て、 SVM の各ボリュームまたは qtree へのクライアントアクセスを個別に制御する。
- 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、同一のクライアントアクセス制御を実行する。ボリュームまたは qtree ごとに新しいエクスポートポリシーを作成する必要はありません。

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うと、権限拒否のメッセージが表示され、その要求は失敗します。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は、すべてのアクセスが暗黙的に拒否されます。

エクスポートポリシーは、 ONTAP を実行しているシステム上で動的に変更できます。

SVM のデフォルトのエクスポートポリシー

各 SVM には、ルールが含まれていないデフォルトのエクスポートポリシーが用意されています。SVM 上のデータにクライアントからアクセスできるようにするには、ルールを備えたエクスポートポリシーを用意する必要があります。SVM 内の各 FlexVol にエクスポートポリシーを関連付ける必要があります。

SVMを作成すると、という名前のデフォルトのエクスポートポリシーがストレージシステムによって自動的に作成されます `default` SVMのルートボリュームに対して実行します。SVM 上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを 1 つ以上作成する必要があります。または、ルールを備えたカスタムの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、変更および名前変更は可能ですが、削除することはできません。

SVM 内に FlexVol ボリュームを作成すると、作成されたボリュームには、 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 に作成し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 内のすべてのボリュームでデフォルトのエクスポートポリシーを使用することも、ボリュームごとに独自のエクスポートポリシーを作成することもできます。複数のボリュームを同じエクスポートポリシーに関連付けることができます。

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では、ボリュームへのクライアントアクセス要求が設定済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

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が少なくとも 1 つ含まれている必要があります。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、そのルールの権限が使用され、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限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。たとえば、 NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

  の最大サイズ `-clientmatch` フィールドは4096文字です。

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

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、すべてのルール違反をエラールールリストに記録することができます。。 `vserver export-policy config-checker` コマンドを実行するとチェッカーが呼び出されて結果が表示され、設定を検証したり、誤ったルールをポリシーから削除したりできます。
>
> 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が一致していても、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別のサブネットに属しています。そのため、クライアントは一致しなくなり、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 アドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。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 で認証されます。

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 で認証されます。

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、認証に使用す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使用するクライアントを管理します

エクスポートルールのアクセスパラメータに指定されていないセキュリティタイプをクライアントが使用している場合は、オプションを使用して、クライアントへのアクセスを拒否するか、クライアントを匿名ユーザIDにマッピングするかを選択できます `none` にアクセスパラメータを指定します。

クライアントは、別のセキュリティタイプで認証されているか、まったく認証されていない（セキュリティタイプ AUTH_NONE ）場合に、アクセスパラメータで指定されていないセキュリティタイプを使用しているとみなされます。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、オプションは追加できます `none` をアクセスパラメータに追加します。リストにないセキュリティ形式を使用

するクライアントは、拒否されずに匿名ユーザ 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るユーザIDを決定します。に指定されたユーザID `-anon` パラメータは、匿名ユーザに適していると思われる権限が設定されている有効なユーザである必要があります。

に有効な値 `-anon` パラメータの範囲はからです `0` 終了： `65535`。

に割り当てられたユーザ**ID** `-anon`	クライアントアクセス要求の処理結果
`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、このユーザに対して設定された権限に応じてアクセスできるようになります。
`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、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。これがデフォルトです。
`65535`	この ID にマッピングされていて、クライアントがセキュリティタイプ AUTH_NONE を使用している場合、クライアントからのアクセス要求は拒否されます。ユーザ ID が 0 のクライアントからのアクセス要求は、この ID にマッピングされ、他のセキュリティタイプをクライアントが使用している場合、拒否されます。

オプションを使用する場合 `none`では、最初に読み取り専用パラメータが処理されることを覚えておくことが重要です。リストにないセキュリティタイプを使用するクライアントのエクスポートルールを設定する際は、次のガイドラインを考慮してください。

読み取り専用にはが含まれます `none`	読み取り/書き込みに含まれます `none`	リストにないセキュリティタイプを使用するクライアントのアクセス結果
いいえ	いいえ	拒否されました
いいえ	はい。	最初に読み取り専用が処理されるため、拒否されました
はい。	いいえ	匿名として読み取り専用です
はい。	はい。	匿名として読み書き可能です

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 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 で認証されます。

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 で認証されます。

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、認証は行われていません（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では、読み取り専用アクセスが、 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許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り専用アクセスが、他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許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスがすべてのセキュリティタイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされている環境クライアントのみが許可されます。

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 / 書き込みアクセス権を取得します。クライアント #2 は、自身のユーザ ID で読み取り / 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 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 で認証されます。

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 で認証されます。

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、認証は行われていません（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では、読み取り専用アクセスが、 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許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り専用アクセスが、他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許可されています。読み取り / 書き込みパラメータでは、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ています。

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 / 書き込みアクセス権を取得します。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権を取得しますが、読み取り / 書き込みアクセスは拒否されます。

セキュリティタイプによるクライアントアクセスレベルの決定方法

クライアントの認証に使用されるセキュリティタイプは、エクスポートルールで特別な役割を果たします。クライアントがボリュームまたは qtree にアクセスする際のレベルがセキュリティタイプによってどのように決定されるかについて理解しておく必要があります。

アクセスレベルには、次の 3 つがあります。

1. 読み取り専用です
2. 読み書き可能です
3. superuser （ユーザ ID が 0 のクライアントの場合）

セキュリティタイプに基づく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。

クライアントに必要なアクセスレベル	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るアクセスパラメータ
標準ユーザの読み取り専用	読み取り専用です (`-rorule`)
標準ユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`)
スーパーユーザの読み取り専用です	読み取り専用です (`-rorule`）および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`）および `-superuser`

次に、これらの 3 つのアクセスパラメータのそれぞれ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、では使用できません `-superuser` パラメータ

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

クライアントのセキュリティタイプを 3 つの各アクセスパラメータと照合したときの結果としては、次の 3 つが考えられます。

クライアントのセキュリティタイプ	クライアント
アクセスパラメータで指定されたタイプと一致する。	独自のユーザ ID を使用して、そのレベルのアクセス権を取得します。
指定したタイプと一致しないが、アクセスパラメータにオプションが指定されている `none`。	で指定されたユーザIDを持つ匿名ユーザとして、そのレベルのアクセス権を取得します `-anon` パラメータ
指定したタイプと一致しないため、アクセスパラメータにオプションが指定されていません `none`。	は、そのレベルのアクセス権を取得しません。これは、には適用されません `-superuser` パラメータには常にが含まれているためです `none` 指定されていない場合でも。

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 で認証されます。

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 で認証されます。

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、認証は行われていません（ 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では、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。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスが、 AUTH_SYS または Kerberos v5 で認証された、自身のユーザ ID を持つクライアントに許可されています。スーパーユーザパラメータでは、スーパーユーザアクセスが、 Kerberos v5 で認証された、ユーザ ID が 0 のクライアントに許可されています。

したがって、クライアント #1 は、 3 つすべてのアクセスパラメータに一致するため、スーパーユーザの読み取り / 書き込みアクセス権を取得します。クライアント #2 は、読み取り / 書き込みアクセス権を取得しますが、スーパーユーザアクセス権は取得できません。クライアント #3 は、読み取り専用アクセス権を取得しますが、スーパーユーザアクセス権は取得できません。

スーパーユーザのアクセス要求を管理します

エクスポートポリシーを設定する際には、ストレージシステムがユーザ ID が 0 のクライアントアクセス要求をスーパーユーザとして受信し、それに応じてエクスポートルールを設定する場合に必要な処理を考慮する必要があります。

UNIX の世界では、ユーザ ID 0 のユーザがスーパーユーザと呼ばれ、通常は root と呼ばれます。このユーザにはシステム上で無制限のアクセス権が与えられています。スーパーユーザ権限の使用は、システムやデータセキュリティの侵害などのいくつかの理由によってリスクを伴う可能性があります。

デフォルトでは、 ONTAP はユーザ ID が 0 のクライアントを匿名ユーザにマッピングします。ただし、は指定できます - `superuser` ユーザIDが0のクライアントの処理方法（セキュリティタイプに応じて）を決定するエクスポートルールのパラメータ。で有効なオプションは次のとおりです `-superuser` パラメータ：

- `any`
- `none`

  これは、を指定しない場合のデフォルト設定です `-superuser` パラメータ

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

ユーザIDが0のクライアントは、に応じて2つの方法で処理されます `-superuser` パラメータ設定：

状況に応じて **-superuser** パラメータおよびクライアントのセキュリティタイプ	クライアント
一致	ユーザ ID 0 でスーパーユーザアクセス権を取得します。
一致しません	で指定されたユーザIDを持つ匿名ユーザとしてアクセスを取得します `-anon` パラメータとその割り当てられた権限。これは、読み取り専用パラメータと読み取り/書き込みパラメータのどちらでオプションが指定されているかに関係ありません `none`。

クライアントがNTFSセキュリティ形式およびのボリュームにアクセスするためにユーザID 0を提示する場合 `-superuser` パラメータはに設定されます `none`ONTAP では、匿名ユーザがネームマッピングを使用して適切なクレデンシャルを取得します。

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で認証されます。

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 で認証されます。

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、認証に使用す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、スーパーユーザアクセス権を取得できません。代わりに、が原因で匿名にマッピングされます `-superuser` パラメータが指定されていません。つまり、デフォルトはです `none` ユーザID 0を匿名に自動的にマッピングします。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権のみを取得します。

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`
- `-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 で認証されます。

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 で認証されます。

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、認証に使用す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。

このエクスポートルールでは、ユーザ ID が 0 のクライアントにスーパーユーザアクセスが許可されています。クライアント#1は、読み取り専用およびのユーザIDおよびセキュリティタイプと一致するため、スーパーユーザアクセスを取得します `-superuser` パラメータクライアント#2の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と一致しないため、読み取り/書き込みアクセス権もスーパーユーザアクセス権も取得されません `-superuser` パラメータ代わりに、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、ユーザ ID は 0 です。

ONTAP でのエクスポートポリシーキャッシュの使用方法

システムパフォーマンスを向上するために、 ONTAP はローカルキャッシュを使用してホスト名やネットグループなどの情報を格納します。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、またキャッシュによって何が行われるのかを理解すると、クライアントアクセスに関する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しているクライアントに対するマッチングを行うパラメータが含まれています。これらのパラメータの一部では、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 サーバのような外部ソースと通信する必要があります。

外部ソースとの通信には少し時間がかかります。パフォーマンスを向上させるために、 ONTAP は、各ノード上の複数のキャッシュに情報をローカルに格納して、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	保存される情報のタイプ
にアクセスします	対応するエクスポートポリシーへのクライアントのマッピング
名前	対応する UNIX ユーザ ID への UNIX ユーザ名のマッピング
ID	対応する UNIX ユーザ ID および拡張された UNIX グループ ID への UNIX ユーザ ID のマッピング
ホスト	対応する IP アドレスへのホスト名のマッピング
ネットグループ	メンバーの対応する IP アドレスへのネットグループのマッピング
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

ONTAP が外部ネームサーバ上の情報を取得してローカルに格納したあとに、環境内の外部ネームサーバ上の情報を変更すると、キャッシュ内の情報が古くなる可能性があります。ONTAP は一定期間の経過後に自動的にキャッシュを更新しますが、有効期限や更新の時期およびアルゴリズムはキャッシュごとに異なります。

キャッシュに古くなった情報が含まれる理由としてもう 1 つ考えられるのは、 ONTAP がキャッシュされた情報の更新を試みたにもかかわらずネームサーバと通信しようとしてエラーが発生した場合です。この場合、 ONTAP は、クライアントの中断を避けるために現在ローカルキャッシュに格納されている情報を引き続き使用します。

その結果、成功することが想定されるクライアントアクセス要求が失敗し、エラーとなることが想定されるクライアントアクセス要求が成功する可能性があります。クライアントアクセスに関するこのような問題のトラブルシューティング時には、エクスポートポリシーキャッシュの一部を表示したり、手動でフラッシュしたり

できます。

アクセスキャッシュの仕組み

ONTAP は、アクセスキャッシュを使用して、ボリュームまたは qtree へのクライアントアクセス処理に対するエクスポートポリシールール評価の結果を格納します。これにより、クライアントから I/O 要求が送信されるたびにエクスポートポリシールール評価の処理を行う場合よりも、アクセスキャッシュから情報をはるかに短時間で取得できるため、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の I/O 要求を送信するたびに、ONTAP はそれぞれの I/O 要求を評価して、その 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、そのボリュームまたは qtree に関連付けられているすべてのエクスポートポリシールールのチェックが伴います。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と交差している場合は、そのパスに付随する複数のエクスポートポリシーに対してこのチェックの実行が必要になる可能性があります。

なお、この評価は、最初のマウント要求についてだけでなく、読み取り、書き込み、リスト、コピーなどの処理を行う NFS クライアントから送信されたすべての I/O 要求について行われます。

ONTAP が適用可能なエクスポートポリシールールを特定して要求を許可するか拒否するかを決定すると、ONTAP はそ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内に作成します。

NFS クライアントが I/O 要求を送信すると、 ONTAP は、そのクライアントの IP アドレス、 SVM の ID 、ターゲットボリュームまたは qtree に関連付けられているエクスポートポリシーを記録したうえで、まずアクセスキャッシュをチェックして一致するエントリがないか確認します。一致するエントリがアクセスキャッシュ内に存在する場合、 ONTAP はそこに格納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 は先ほど述べたすべての適用可能なポリシールールを評価する通常の処理を行います。

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、外部ネームサーバとの無駄な通信が削減されます。

アクセスキャッシュからの情報の取得は、 I/O 要求のたびにエクスポートポリシールールを評価する全体的な処理よりもずっと高速です。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軽減され、パフォーマンスが大幅に向上します。

アクセスキャッシュパラメータの仕組み

アクセスキャッシュ内の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、パフォーマンスと格納される情報の鮮度のバランスを取ることができます。

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。

アクセスキャッシュパラメータは、個々の SVM に対して指定できます。これにより、 SVM のアクセス要件

に応じてパラメータを変更できます。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	説明	更新期間（秒）
正のエントリ	クライアントへのアクセス拒否を発生させなかったアクセスキャッシュエントリです。	最小値： 300 最大値： 86 、 400 デフォルト値は 3,600 です。
負のエントリ	クライアントへのアクセス拒否を発生させたアクセスキャッシュエントリです。	最小：60 最大値： 86 、 400 デフォルト値は 3,600 です。

例

NFS クライアントがクラスタ上のボリュームへのアクセスを試みます。ONTAP は、エクスポートポリシールールに対するクライアントのマッチングを行い、クライアントがエクスポートポリシールール設定に基づいてアクセスを行っていると判断します。ONTAP はエクスポートポリシールールを正のエントリとしてアクセスキャッシュに格納します。デフォルトでは、 ONTAP は、この正のエントリを 1 時間（ 3 、 600 秒）アクセスキャッシュ内に保持したあと、情報を最新の状態にするためにこのエントリを自動的に更新します。

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に、クライアントアクセスの特定の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ための追加のパラメータがあります。これ `-harvest-timeout` パラメータの有効範囲は60~2、592、000秒で、デフォルト設定は86、400秒です。

qtree からエクスポートポリシーを削除する

qtree に割り当てられている特定のエクスポートポリシーが不要になった場合は、代わりに格納先ボリュームのエクスポートポリシーを継承するように qtree を変更することで、エクスポートポリシーを削除できます。これは、を使用して実行できます `volume qtree modify` コマンドにを指定します `-export-policy` パラメータと空の名前文字列（""）。

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 qtree ID を検証します

ONTAP では、オプションで qtree ID の検証を追加で実行できます。この検証により、クライアントのファイル処理要求で有効な qtree ID が使用されるとともに、クライアントによるファイルの移動が同じ qtree 内でのみ行えるようになります。この検証を有効または無効にするには、を変更します `-validate-qtree-export` パラメータこのパラメータはデフォルトで有効になっています。

このタスクについて

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ている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。

検証する **qtree ID** の状態	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
   ```

FlexVol 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でネストされたジャンクションよりも制限が厳しいエクスポートポリシーを設定した場合は、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厳しくないエクスポートポリシーを設定するようにしてください。