# NFSを使用したファイルアクセスの設定

ONTAP 9

NetApp
May 09, 2024

# 目次

# NFSを使用したファイルアクセスの設定

## NFS の概要を使用したファイルアクセスのセットアップ

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、さらにいくつかの手順を実行することもできます。

クライアントが NFS を使用して SVM のファイルにアクセスできるようにするには、次の作業を行う必要があります。

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 でエクスポートポリシーを設定します。

   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には、エクスポートポリシーを設定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。 |

| 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 |
|---|---|
| `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 |

| クライアントのセキュリティタイプ | クライアント |
| --- | --- |
| 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<br><br>最大値： 86 、 400<br><br>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<br><br>最大値： 86 、 400<br><br>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。

## **NFS** で **Kerberos** を使用してセキュリティを強化する

### **ONTAP** での **Kerberos** のサポート

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ます。認証により、ユーザおよびプロセスの ID をサーバで検証できます。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確認など）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。これにより、安全性が向上し、負荷も増加します。

- 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、セキュリティを強化するために、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。

## 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、使用しているクライアント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。これらのすべての変数については、本ドキュメントでは説明していません。詳細については、各コンポーネントの該当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。

次の項目を最初に設定する必要があります。

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 MIT Kerberos ）。

  NFSサーバはを使用する必要があります `nfs` マシンプリンシパルの主要コンポーネントとして使用します。

- 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を 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

  各クライアントについて、 Kerberos Realm のユーザアカウントが必要です。NFS サーバでは ' マシン・プリンシパルの主要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です。

    非常にセキュリティ性の高い AES-256 。

  - TGT 通信に対する最も安全な暗号化タイプが有効です。
  - Kerberos Realm とドメインを正しく設定します。
  - GSSはイネーブルです。

    マシンのクレデンシャルを使用する場合：

  - 走らないでください `gssd` を使用 `-n` パラメータ
  - 走らないでください `kinit` をrootユーザとして指定します。

- 各クライアントは、最新かつ更新されたオペレーティングシステムバージョンを使用する必要があります。

  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。

- ホストおよびドメインの情報

  各クライアントの `/etc/hosts` および `/etc/resolv.conf` ファイルには正しいホスト名とDNS情報が格納さ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場合にのみ、Windows クレデンシャルをチェックする必要があります。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 DNS を設定します

  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サアハ

  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。

- 個のボリューム

  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。

| 名前 | 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できます。

- 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** |
|---|---|
| デーモン | 1. |
| ルート | 0 |
| pcuser | 65534 （ SVM を作成すると ONTAP で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 **ID** | プライマリグループ **ID** | コメント（ **Comment** ） |
|---|---|---|---|
| NFS | 500ドル | 0 | GSS INITフェーズで必要<br><br>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。 |

| ユーザ名 | ユーザ **ID** | プライマリグループ **ID** | コメント（ **Comment** ） |
|---|---|---|---|
| pcuser | 65534 | 65534 | NFSトCIFSノマルチフロトコルノシヨウニヒツヨウ<br><br>SVMを作成すると、ONTAPで自動的に作成されてpcuserグループに追加されます。 |
| ルート | 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ルール

  ルートボリュームとデータボリュームおよび qtree に対するエクスポートポリシーと必要なエクスポートルール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へのアクセスにKerberosを使用する場合は、エクスポートルールのオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5` 、 `krb5i`または `krb5p`。

- 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

"ネットアップテクニカルレポート 4073 ：『 Secure Unified Authentication 』"

"NetApp Interoperability Matrix Tool で確認できます"

"システム管理"

"論理ストレージ管理"

## NFSv4 のユーザ 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、を設定します `-v4-id-domain` オプション

このタスクについて

NFSv4 ユーザ ID のマッピングにデフォルトで使用されるドメインは、 NIS ドメインが設定されている場合は NIS ドメインになります。 ONTAPNIS 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。たとえば、複数のユーザ ID ドメインがある場合、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。これは NFSv3 の場合は必要ありません。

ステップ

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

## ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf` UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP 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。ONTAP では、 SVM ごとに個別のネームサービススイッチテーブルが保持されます。

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。

| データベースタイプ | ネームサービスソースの用途 | 有効なソース |
|---|---|---|
| ホスト | ホスト名の IP アドレスへの変換 | ファイル、 DNS |
| グループ | ユーザグループ情報を検索しています | files 、 nis 、 ldap が表示されます |
| パスワード | ユーザ情報を検索しています | files 、 nis 、 ldap が表示されます |
| ネットグループ | ネットグループ情報の検索 | files 、 nis 、 ldap が表示されます |
| namemap | ユーザ名のマッピング | ファイル、 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 | 情報の検索先 | 使用するコマンド |
| --- | --- | --- |
| 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`<br><br>`vserver services name-service netgroup`<br><br>`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管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります `files` また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

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。

| 外部のネームサービスソース | アクセスに使用するプロトコル |
| --- | --- |
| 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 アドレスの検索では、 ONTAP は最初にローカルのソースファイルを参照します。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、 ONTAP はローカルのソースファイルだけを参照します。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、 ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカル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、 ONTAP はデフォルトでローカルのソースファイルだけを参照します。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

## LDAP を使用する

### LDAPの概要

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 LDAP サーバに保存する場合、既存の LDAP データベース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 for ONTAP を設定する前に、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している必要があります。
  - LDAP サーバでサポートされている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされているハッシュ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。

次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 の署名と封印（データの整合性チェックと暗号化を提供）
- START TLS
- LDAPS （ LDAP over TLS または SSL ）

◦ 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。

◦ TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。

- ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
- LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
- 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を設定する必要があります。
  - 双方向
  - 一方向。一次は紹介ドメインを信頼します
  - 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 が設定されていること。
- の認証では、ドメインパスワードが同じである必要があります `--bind-as-cifs-server` trueに設定します。

> 次の設定は LDAP リファーラル追跡でサポートされません。
>
> ◦ 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 以前では（ 9.9.1 以降でサポートされています）：
> ◦ LDAPの署名と封印（ `-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（ `-use-ldaps-for-ad-ldap` オプション）

- ONTAP 9.11.1以降では、を使用できます "nsswitch認証のためのLDAP高速バインド。"
- SVM で LDAP クライアントを設定するときは、 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が適しています。ただし、環境で使用する

LDAP スキーマがこれらと異なる場合は、 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。

追加情報の場合は、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

**LDAP** の署名と封印の概念

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、シークレットキーのテクノロジを使用して、 LDAP ペイロードデータの整合性を確認します。封印は、 LDAP ペイロードデータを暗号化して機密情報がクリアテキストで送信されないようにします。LDAP トラフィックについて、署名が必要か、署名と封印が必要か、どちらも必要ないかは、 *ldap Security Level* オプションで指定します。デフォルトはです `none`。テスト

SMBトラフィックに対するLDAPの署名と封印は、を使用してSVMで有効にします `-session-security -for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

**LDAPS**の概念

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 LDAP サーバ間の認証されたセッションの設定に Start TLS または LDAPS を使用できます。

用語集

ONTAP での LDAP 通信の保護に LDAPS を使用する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 ）情報ディレクトリにアクセスして管理するためのプロトコルです。LDAP は、ユーザ、グループ、ネットグループなどの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。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も提供します。

- **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 ）従来の 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ます。

- * LDAPS （ LDAP over SSL または TLS ） *

  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*」は同じ意味で使用されることがあります。LDAPSはONTAP 9.5以降でサポートされます。

  - ONTAP 9.5-9.8 では、 LDAPS はポート 636 でのみ有効にできます。そのためには、を使用します `-use-ldaps-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します
  - ONTAP 9.9.1以降では、任意のポートでLDAPSを有効にできますが、デフォルトはポート636です。これを行うには、を設定します `-ldaps-enabled` パラメータの値 `true` そして目的のものを指定してください `-port` パラメータ詳細については、を参照してください `vserver services name-service ldap client create` のマニュアルページ

  ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。

- * TLS を開始 *

  （ *START_TLS*,*STARTTLS* 、 *_StartTLS* とも呼ばれます）。 TLS プロトコルを使用してセキュアな通信を提供するメカニズムです。

  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 ID 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 では次の機能がサポートされます

- Active Directory 統合 LDAP サーバと SVM の間の SMB 関連トラフィックに使用する LDAPS
- LDAPS ：ネームマッピングやその他の UNIX 情報で使用する LDAP トラフィックに使用します

  Active Directory 統合 LDAP サーバまたは UNIX ベース LDAP サーバのいずれかを使用して、 LDAP ネームマッピングおよびユーザ、グループ、ネットグループなどのその他の UNIX 情報の格納に使用できます。

- 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 の RFC2307bis サポートを有効にする**

## 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。

必要なもの

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。

このタスクについて

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。この属性には複数の値を含めることができ、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。

このユーザは、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 サポートが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、 ONTAP では RFC2307bis サポートが自動的に有効になります。

追加情報の場合は、を参照してください "ネットアップテクニカルレポート 4835 ：『 How to Configure LDAP in ONTAP 』"。

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
```

**LDAP** ディレクトリ検索の設定オプション

環境にとって最も適切な方法で LDAP サーバに接続するように ONTAP LDAP クライアントを設定することで、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の問題を回避するために、検索をできるだけ効率的に行うことができます。

デフォルトのベースおよびスコープ検索値です

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、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、デフォルトはです `root`。つまり、各クエリでディレクトリ全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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検索スコープです。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、デフォルトはです `subtree`。つまり、各クエリで DN の下にあるサブツリー全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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と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させることができます。

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一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 | カスタム指定要素 |
| --- | --- |

| | |
|---|---|
| `-base-dn` | すべての LDAP 検索のベース DN 複数の値を必要に応じて入力できます（ ONTAP 9.5 以降のリリースで LDAP リファーラル追跡を有効にした場合など）。 |
| `-base-scope` | すべての LDAP 検索のベーススコープ |
| `-user-dn` | すべての LDAP ユーザ検索のベース DN このパラメータは、環境ユーザ名マッピング検索も行います。 |
| `-user-scope` | すべての LDAP ユーザ検索のベーススコープ：このパラメータは、環境ユーザ名マッピング検索も行います。 |
| `-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 グループ検索のベーススコープ |
| `-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ベーススコープ |

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ことがあります。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ている場合は、 DN の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。

scope 環境は、対応するパラメータに指定されている のリスト全体を表します。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。

また、 ONTAP 9.5 以降では、 LDAP_referral_c追いかけ _ を指定することもできます。これにより、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かった場合に、 ONTAP LDAP クライアントがその他の LDAP サーバへのルックアップ要求を参照することができます。クライアントは、このリファーラルデータに記載されたサーバからターゲットオブジェクトを取得します。参照された LDAP サーバにあるオブジェクトを検索するには、参照されたオブジェクトのベース DN を LDAP クライアント設定の一部としてベース DN に追加します。ただし、参照されたオブジェクトは、（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 `-referral-enabled true` オプション）LDAPクライアントの作成時または変更時

**LDAP** ディレクトリのホスト単位ネットグループ検索のパフォーマンスを向上させます

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。

必要なもの

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

DNS サーバには、 NFS クライアントのフォワード（ 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ときは、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。

このタスクについて

NISサーバは、と呼ばれる3つの個別のマップにネットグループ情報を格納します `netgroup`、`netgroup.byuser`および `netgroup.byhost`。の目的 `netgroup.byuser` および `netgroup.byhost` マップはネットグループ検索を高速化するためのものです。ONTAP は、マウントの応答時間を短縮するために NIS サーバ上でホスト単位のネットグループ検索を実行できます。

デフォルトでは、LDAPディレクトリにはそのようなはありません `netgroup.byhost` NISサーバと同様のマッピングただし、サードパーティのツールを使用すると、NISをインポートできます `netgroup.byhost` LDAPディレクトリにマッピングして、ホスト単位の高速ネットグループ検索を有効にします。ホスト単位のネットグループ検索を許可するようにLDAP環境を設定している場合は、を使用してONTAP LDAPクライアントを設定できます `netgroup.byhost` ホスト単位のネットグループ検索を高速化するために、名前、DN、および検索範囲をマッピングします。

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 クライアントがエクスポートへのアクセスを要求した場合、より高速に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遅延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. NISの完全な識別名を取得します `netgroup.byhost` LDAPディレクトリにインポートしたマップ。

   マップ 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ります。最高のパフォーマンスを得るには、正確なマップ DN を指定する必要があります。

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単位の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}` LDAPディレクトリのホスト単位のネットグループ検索を有効または無効にします。デフォルトはです `false`。

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` の識別名を指定します `netgroup.byhost` LDAPディレクトリにマッピングします。これにより、ホスト単位のネットグループ検索のベース DN が無効になります。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、ホスト単位のネットグループ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、デフォルトのが使用されます `subtree`。

LDAPクライアント設定がまだ存在しない場合は、を使用して新しいLDAPクライアント設定を作成するときにこれらのパラメータを指定することで、ホスト単位のネットグループ検索を有効にできます `vserver services name-service ldap client create` コマンドを実行します

> ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、 LDAP サーバのホスト名または IP アドレスを指定できます。

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

例

次のコマンドは、「ldap_corp」という名前の既存のLDAPクライアント設定を変更して、を使用したホスト単位のネットグループ検索を有効にします `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`：

```
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
```

完了後

。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。

関連情報

"IETF RFC 5952 ：『 A Recommendation for IPv6 Address Text Representation 』"

**nsswitch**認証に**LDAP**高速バインドを使用できます

ONTAP 9.11.1以降では、ldap_fast bind_fルキノ ウ（_コンカレントbind_とも呼ばれます）を利用して、クライアント認証要求を迅速かつ簡単に行うことができます。この機能を使用するには、LDAPサーバが高速バインド機能をサポートしている必要があります。

このタスクについて

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サーバで管理ユーザを認証します。この認証方式では、ONTAP がユーザまたはグループの名前をLDAPサーバに送信し、保存されているハッシュパスワードを受信して、サーバのハッシュコードをユーザパスワードからローカルに生成されたハッシュパスコードと比較します。同一の場合、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と、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）のみを送信します。LDAPサーバはこれらのクレデンシャルを検証し、ONTAP にログイン権限を付与するように指示します。

高速バインドの利点の1つは、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。パスワードハッシュはLDAPサーバによって実行されるためです。

"高速バインドの使用方法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、LDAPクライアントがTLSまたはLDAPS用に設定されていることを強く推奨します。設定されていない場合は、パスワードがプレーンテキストでネットワーク経由で送信されます。

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。

- ONTAP 管理者ユーザは、高速バインドをサポートするLDAPサーバで設定する必要があります。
- ネームサービススイッチ（nsswitch）データベースにLDAP用にONTAP SVMが設定されている必要があります。
- 高速バインドを使用してnsswitch認証を行うには、ONTAP 管理者ユーザアカウントとグループアカウントを設定する必要があります。

手順

1. 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LDAP管理者に確認してください。
2. ONTAP 管理者ユーザクレデンシャルがLDAPサーバで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説明します。"

   b. 確認してください `ldap` は、nsswitchに設定されているソースの1つです `passwd` データベースに次のように入力します

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

   "nsswitch設定の詳細は、こちらをご覧ください。"

4. 管理ユーザがnsswitchで認証されていること、およびアカウントで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。

   - 既存のユーザの場合は、と入力します `security login modify` 次のパラメータ設定を確認します。

     ```
     -authentication-method nsswitch
     ```

   `-is-ldap-fastbind true`

   - 新しい管理者ユーザについては、を参照してください "LDAPまたはNISアカウントアクセスを有効にします。"

**LDAP**統計を表示します。

ONTAP 9.2 以降では、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 LDAP 統計を表示することができます。

必要なもの

- SVM で 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。

ステップ

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

次の例は、オブジェクトのパフォーマンスデータを表示します `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                              Value
-------------------------------- --------------------------------
instance_name                        vserverName:LDAP (NIS & Name
                                     Mapping):GetUserInfoFromName:
                                     1.1.1.1
last_modified_time                   1460610787
node_name                            nodeName
num_not_found_responses              1
num_request_failures                 1
num_requests_sent                    1
num_responses_received               1
num_successful_responses             0
num_timeouts                         0
operation                            GetUserInfoFromName
process_name                         secd
request_latency                      52131us
```

# ネームマッピングを設定する

## ネームマッピングの概要を設定する

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クライアントとSMBクライアントのどちらから接続しているかに関係なく、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です。

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 アクセスや 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を使用す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個別に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。

## ネームマッピングの仕組み

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、 ONTAP は小文字の Windows ユーザ名が UNIX ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。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、 ONTAP は SMB ドメインで UNIX 名と一致する Windows アカウントを探します。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。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、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、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。

## UNIX ユーザから Windows ユーザへのネームマッピングのため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、インバウンドまたはアウトバウンドの2種類の単方向の信頼のいずれかにすることもできます。ホームドメインは、 SVM 上の 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、ホームドメインは信頼できるドメインに属するユーザを認証および許可できます。その逆も同様です。

  UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に双方向の信頼関係が確立されたドメインでのみ実行できます。

- アウトバウンドの信頼 _

  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。

  ホームドメインとアウトバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

- インバウンドの信頼 _

  インバウンドの信頼では、もう一方のドメインがSMBサーバのホームドメインを信頼します。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または認可できません。

  ホームドメインとインバウンドの信頼関係にあるドメインは、 UNIX ユーザから Windows ユーザへのネームマッピング検索の実行時に _not_searched になります。

### 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

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（ **Pattern** ） | 交換 | 結果 |
| --- | --- | --- |
| ルート | ｛Asterisk｝ ｛backslash｝ ｛backslash｝ 管理者 | UNIX ユーザ「 root 」は「 administrator 」という名前のユーザにマッピングされます。「 administrator 」という名前の最初の一致するユーザが見つかるまで、すべての信頼できるドメインが順に検索されます。 |
| * | ｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝ | 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。<br>パターン ｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝ は、UNIX から Windows へのネームマッピングでのみ有効で、反対方向では無効です。 |

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に使用する信頼できるドメインのリストを決定する方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

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。

## ネームマッピングの変換ルール

ONTAP システムには、 SVM ごとに一連の変換ルールが保存されています。各ルールは、 a_pattern_ と a_replacement _ の 2 つの要素で構成されます。変換は該当する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実行されます。パターンは UNIX 形式の正規表現です。リプレースメントは、UNIXのように、パターンのサブ式を表すエスケープシーケンスを含む文字列です `sed` プログラム。

## ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

### このタスクについて

ONTAP では、 SVM ごとに、各方向について最大 12 、 500 個のネームマッピングがサポートされます。

### ステップ

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。を使用することもできます `-replacement` null置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント `" "` （スペース文字）。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

   Windows から UNIX へのマッピングを作成した場合、新しいマッピングが作成されたときに ONTAP システムに接続していたすべての SMB クライアントは、新しいマッピングを使用するために、一度ログアウトしてから、再度ログイン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 上にネーム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、優先順位リスト内での位置は 1 番目です。UNIX ユーザ johnd を Windows ユーザ ENG\JohnDoe にマッピングします。

```
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 上に別のネームマッピングを作成します。このマッピングは Windows から UNIX へのマッピングで、優先順位リスト内での位置は 1 番目です。パターンとリプレースメントには正規表現が使用されています。このマッピングにより、ドメイン ENG 内のすべての CIFS ユーザが、 SVM に関連付けられた LDAP ドメイン内のユーザにマッピングされます。

```
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 上に別のネームマッピングを作成します。このパターンには、エスケープする必要がある Windows ユーザ名の要素として「 $` 」が含まれています。Windows ユーザ ENG\john$ops を UNIX ユーザ john_ops にマッピングします。

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

## デフォルトユーザを設定します。

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場合は、デフォルトユーザを設定しないでください。

このタスクについて

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。

ステップ

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 ユーザを設定します | `vserver nfs modify -default-win-user user_name` |

## ネームマッピングの管理用コマンド

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 |
|---|---|
| ネームマッピングを作成します | `vserver name-mapping create` |

| | |
|---|---|
| 特定の位置にネームマッピングを挿入します | `vserver name-mapping insert` |
| ネームマッピングを表示します | `vserver name-mapping show` |
| 2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリが設定されている場合、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します | `vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1` |

詳細については、各コマンドのマニュアルページを参照してください。

# Windows NFS クライアントのアクセスを有効にします

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ています。つまり、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は、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。

このタスクについて

デフォルトでは、 Windows NFSv3 クライアントサポートが無効になっています。

作業を開始する前に

SVM で NFSv3 が有効になっている必要があります。

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、を無効にします `-enable-ejukebox` および `-v3-connection-drop` パラメータ：

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

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

3. 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 `-o mtype=hard` オプション

   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:\
   ```

# NFS クライアントで NFS エクスポートの表示を有効にします

NFSクライアントはを使用できます `showmount -e` コマンドを使用して、ONTAP NFSサーバから使用可能なエクスポートのリストを表示します。これは、ユーザがマウントするファイルシステムを確認するのに役立ちます。

ONTAP 9.2 以降 ONTAP では、 NFS クライアントでのエクスポートリストの表示がデフォルトで許可されます。以前のリリースでは `showmount` のオプション `vserver nfs modify` コマンドは明示的に有効にする必要があります。エクスポートリストを表示するには、 SVM で NFSv3 が有効になっている必要があります。

例

次のコマンドは、 vs1 という SVM に対して showmount を実行します。

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

次のコマンドは、 IP アドレスが 10.63.21.9 の NFS サーバ上のエクスポートのリストを表示します。

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