# エクスポートポリシーを使用したSMBアクセスの保護

ONTAP 9

NetApp
April 24, 2024

# 目次

# エクスポートポリシーを使用したSMBアクセスの保護

## SMB アクセスでのエクスポートポリシーの使用方法

SMBサーバでSMBアクセスに関するエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御するときにエクスポートポリシーが使用されます。データにアクセスするには、 SMB アクセスを許可するエクスポートポリシーを作成し、 SMB 共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには 1 つ以上のルールが適用されており、このルールで、データへのアクセスを許可されるクライアントと、読み取り専用アクセスと読み取り / 書き込みアクセスでサポートされる認証プロトコルを指定します。エクスポートポリシーを設定して、すべてのクライアント、クライアントのサブネット、または特定のクライアントに SMB 経由のアクセスを許可し、データへの読み取り専用アクセスと読み取り / 書き込みアクセスを決定する際に Kerberos 認証、 NTLM 認証、または Kerberos 認証と NTLM 認証の両方を使用した認証を許可できます。

ONTAP でエクスポートポリシーに適用されたすべてのエクスポートルールを処理したら、クライアントアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windows のユーザとグループではなくクライアントマシンに適用されます。エクスポートルールは、Windows のユーザおよびグループベースの認証と許可に代わるものではありません。共有とファイルのアクセス権限に加えて、エクスポートルールはもう 1 つのアクセスセキュリティレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとにエクスポートポリシーを 1 つ関連付けます。各 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、複数のボリュームを備えた SVM に対して次の操作を実行できます。

- SVM のボリューム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。

各 SVM には、「デフォルト」という名前のエクスポートポリシーが少なくとも 1 つあります。これにはルールは含まれません。このエクスポートポリシーは削除できませんが、名前や内容は変更できます。デフォルトでは、 SVM 上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVM で SMB アクセスのエクスポートポリシーが無効になっている場合、「 default 」エクスポートポリシーは SMB アクセスには影響しません。

NFS ホストと SMB ホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。このポリシーを、 NFS ホストと SMB ホストの両方がアクセスする必要があるデータを含むボリュームに関連付けることができます。または、 SMB クライアントのみがアクセスする必要があるボリュームがある場合は、 SMB プロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証に Kerberos または NTLM のみ（あるいはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーを SMB アクセスのみが必要なボリュームに関連付けます。

SMB に関するエクスポートポリシーが有効になっている場合に、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。クライアントがボリュームの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。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、 SMB 共有を含むボリュームで少なくとも以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアント、またはクライアントの適切なサブセットへのアクセスを許可します
- SMB 経由のアクセスを許可する
- Kerberos 認証または NTLM 認証（あるいはその両方）を使用した適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちら "エクスポートポリシーの設定と管理"。

# 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。

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。

# SMB 経由のアクセスを制限または許可するエクスポートポリシールールの例

以下の例は、 SMB アクセスのエクスポートポリシーが有効になっている SVM で SMB 経由のアクセスを制限または許可するエクスポートポリシールールを作成する方法を示しています。

SMB アクセスに関するエクスポートポリシーは、デフォルトでは無効になっています。SMB 経由のアクセス

を制限または許可するエクスポートポリシールールは、 SMB アクセスのエクスポートポリシーを有効にしている場合にのみ設定する必要があります。

## SMB アクセスのみのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名： cifs1
- インデックス番号： 1
- クライアント一致： 192.168.1.0/24 ネットワーク上のクライアントにのみ一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM 認証または Kerberos 認証を使用するクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証を使用するクライアントに許可します

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

## SMB および NFS アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：cifsnfs1
- インデックス番号： 2.
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスと NFS アクセス
- 読み取り専用アクセス：すべてのクライアントに許可します
- 読み取り / 書き込みアクセス： Kerberos 認証（ NFS および SMB ）または NTLM 認証（ SMB ）を使用するクライアントに許可
- UNIX ユーザ ID 0 （ゼロ）のマッピング：ユーザ ID 65534 （通常ユーザ名 nobody にマッピングされる）にマッピング
- suid と sgid のアクセス：許可しています

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## NTLM のみを使用する SMB アクセスのエクスポートルール

次のコマンドでは、「 vs1 」という名前の SVM に、次の構成のエクスポートルールが作成されます。

- ポリシー名：ntlm1
- インデックス番号： 1
- クライアント一致：すべてのクライアントに一致します
- プロトコル： SMB アクセスのみを有効にします
- 読み取り専用アクセス： NTLM を使用するクライアントにのみ許可されます
- 読み取り / 書き込みアクセス： NTLM を使用するクライアントにのみ許可されます

> NTLM のみを使用するアクセスに読み取り専用オプションまたは読み取り / 書き込みオプションを設定する場合は、クライアント一致オプションで IP アドレスベースのエントリを使用する必要があります。それ以外の場合は、受信します `access denied` エラー。これは、 ONTAP がホスト名を使用してクライアントの権限を確認するときに、 Kerberos Service Principal Name （ SPN ；サービスプリンシパル名）を使用するためです。NTLM 認証では、 SPN 名はサポートされません。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

# SMB アクセスに関するエクスポートポリシーを有効または無効にします

Storage Virtual Machine （ SVM ）での SMB アクセスに関するエクスポートポリシーを有効または無効にすることができます。エクスポートポリシーを使用したリソースへの SMB アクセスの制御はオプションです。

作業を開始する前に

SMB のエクスポートポリシーを有効にするための要件は次のとおりです。

- クライアントのエクスポートルールを作成する前に、そのクライアントの「 PTR 」レコードが DNS に登録されている必要があります。
- SVM が NFS クライアントにアクセスを提供し、 NFS アクセスに使用するホスト名が CIFS サーバ名と異なる場合は、ホスト名に対して「 A 」レコードと「 PTR 」レコードのセットが追加で必要です。

このタスクについて

SVM に新しい CIFS サーバをセットアップするとき、 SMB アクセスに関するエクスポートポリシーの使用はデフォルトで無効になります。認証プロトコル、クライアント IP アドレス、またはホスト名に基づいてアクセスを制御する場合は、 SMB アクセスのエクスポートポリシーを有効にできます。SMB アクセスに関するエクスポートポリシーはいつでも有効または無効にできます。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. エクスポートポリシーを有効または無効にします。
   - エクスポートポリシーを有効にします。 `vserver cifs options modify -vserver`

*vserver_name* -is-exportpolicy-enabled true

- エクスポートポリシーを無効にします。 `vserver cifs options modify -vserver` *vserver_name* `-is-exportpolicy-enabled false`

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

例

次の例は、エクスポートポリシーを使用した SVM vs1 上のリソースへの SMB クライアントアクセスの制御を有効にします。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```