



# 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 .....	1
SMB アクセスでのエクスポートポリシーの使用方法 .....	1
エクスポートルール of の仕組み .....	2
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 .....	3
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 .....	5

# 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：cifs nfs1
- 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  
cifs nfs1 -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::> vservers export-policy rule create -vservers 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が必要です。

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。 `vservers cifs options modify -vservers`

```
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
```



## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。