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
February 12, 2026

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

ONTAP SMBアクセスでエクスポート ポリシーを使用する方法について学習します

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や、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 ポリシーは、SMB経由のアクセスをすべてのクライアントに許可するか、特定のサブネットのクライアントに許可するか、特定のクライアントに許可するように設定できます。また、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ときに、Kerberos認証を許可するか、NTLM認証を許可するか、KerberosとNTLMの両方の認証を許可するように設定できます。

ONTAPは、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 ルールを処理したあと、クライアントに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します。エクスポート ルールは、Windowsのユーザおよび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。

各ボリュームに1つのエクスポート ポリシーを関連付けることで、ボリュームへのクライアント アクセスを設定できます。各SVMには複数のエクスポート ポリシーを設定できます。これにより、複数のボリュームを持つSVMで以下の操作が可能になります：

- SVM 内の各ボリューム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。
- 各ボリュームに新しいエクスポート ポリシーを作成する必要なく、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ることで、同一のクライアント アクセス制御を実現します。

各SVMには、ルールが含まれていない「`default`」というエクスポート ポリシーが少なくとも1つあります。このエクスポート ポリシーは削除できませんが、名前の変更や変更は可能です。SVM上の各ボリュームは、デフォルトで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にアクセスを許可する
- 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

"エクスポート ポリシーの設定と管理"について学びましょう。

ONTAP SMBエクスポート ルールについて学ぶ

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。

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。

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

例では、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 上で、SMB 経由のアクセスを制限または許可するエクスポート ルールを作成する方法を示します。

SMBアクセスのエクスポート ポリシーはデフォルトで無効になっています。SMBアクセスのエクスポート ポリシーを有効にした場合にのみ、SMB経由のアクセスを制限または許可するエクスポート ルールを構成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

次のコマンドは、「vs1」という名前のSVMに次の構成を持つエクスポート ルールを作成します：

- ポリシー名：cifs1
- インデックス番号：1
- クライアント マッチ：192.168.1.0/24 ネットワーク上のクライアントのみに一致します
- プロトコル：SMBアクセスのみ有効
- 読み取り専用アクセス：NTLM または Kerberos 認証を使用するクライアント
- 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

```
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

次のコマンドは、「` vs1`」という名前の SVM に次の構成を持つエクスポート ルールを作成します：

- 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
- プロトコル：SMBおよび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
- 読み取り/書き込みアクセス：Kerberos（NFS および SMB）または NTLM 認証（SMB）を使用するクライアント
- UNIX ユーザー ID 0（ゼロ）のマッピング：ユーザー ID 65534 にマッピングされます（通常はユーザー名 nobody にマッピングされます）
- suidおよびsgidアクセス：許可

```
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 のみを使用した SMB アクセスのエクスポート ルール

次のコマンドは、「vs1」という名前のSVMに次の構成を持つエクスポート ルールを作成します：

- 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
- プロトコル：SMBアクセスのみ有効
- 読み取り専用アクセス：NTLM を使用するクライアントのみ
- 読み取り/書き込みアクセス：NTLM を使用するクライアントのみ

NTLMのみのアクセスに対して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、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。そうしないと、 `access denied`エラーが発生します。これは、ONTAPがホスト名を使用してクライアントのアクセス権を確認する際に、Kerberosサービスプリンシパル名（SPN）を使用するためです。NTLM認証ではSPN名はサポートされていません。

```
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 アクセスの ONTAP エクスポート ポリシーを有効または無効にする

ストレージ仮想マシン（SVM）上の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 ポリシーを使用してリソースへのSMBアクセスを制御するかどうかは任意です。

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、クライアントの DNS に「PTR」レコードが存在している必要があります。
- SVM が NFS クライアントへのアクセスを提供し、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、ホスト名の「A」レコードと「PTR」レコードの追加セットが必要です。

タスク概要

SVMに新しいCIFSサーバをセットアップする際、SMBアクセス用のエクスポート ポリシーの使用はデフォルトで無効になっています。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アクセス用のエクスポート ポリシーを有効にできます。SMBアクセス用のエクスポート ポリシーはいつでも有効または無効にできます。

NFS 対応 SVM で CIFS/SMB のエクスポート ポリシーを有効にすると、Linux クライアントは SVM 上で `showmount -e`コマンドを使用して、関連付けられているエクスポート ポリシー ルールを持つすべての SMB ボリュームのジャンクション パスを表示できるようになります。

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 ポリシーを有効にする： `vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled true`
   - エクスポート ポリシーを無効にする： `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

商標に関する情報