



# **SMB共有のACLを使用したファイルアクセス の保護**

## ONTAP 9

NetApp  
December 20, 2024

# 目次

|                                 |   |
|---------------------------------|---|
| SMB共有のACLを使用したファイルアクセスの保護 ..... | 1 |
| SMB共有レベルACLの管理に関するガイドライン .....  | 1 |
| SMB共有のアクセス制御リストの作成 .....        | 1 |
| SMB共有アクセス制御リストの管理用コマンド .....    | 4 |

# SMB共有のACLを使用したファイルアクセスの保護

## SMB共有レベルACLの管理に関するガイドライン

共有レベルのACLを変更すると、共有に設定するアクセス権を強化したり、軽減したりできます。WindowsのユーザとグループまたはUNIXのユーザとグループのいずれかを使用して共有レベルのACLを設定できます。

デフォルトでは、共有レベルのACLによって、Everyoneという名前の標準グループにフルコントロールが付与されます。ACLにフルコントロールを指定すると、ドメインおよびすべての信頼できるドメインのすべてのユーザに共有へのフルアクセスが許可されます。共有レベルACLのアクセスレベルは、を使用して制御できます"[WindowsクライアントまたはONTAPコマンドライン上のMicrosoft管理コンソール \(MMC\)](#)"。

MMCを使用する際には、次の点に留意してください。

- 指定するユーザ名およびグループ名はWindows名である必要があります。
- Windowsの権限だけを指定できます。

ONTAPコマンドラインを使用する際には、次の点に留意してください。

- ユーザ名およびグループ名には、Windows名またはUNIX名を使用できます。

ACLの作成時または変更時に指定されない場合、デフォルトのタイプはWindowsのユーザとグループです。

- Windowsの権限だけを指定できます。

## SMB共有のアクセス制御リストの作成

SMB共有のAccess Control List (ACL; アクセス制御リスト) を作成して共有権限を設定すると、ユーザとグループの共有へのアクセスレベルを制御できます。

タスクの内容

ローカルまたはドメインのWindowsユーザまたはグループの名前、またはUNIXユーザまたはグループの名前を使用して、共有レベルのACLを設定できます。

新しいACLを作成する前に、デフォルトの共有ACLを削除する必要があります `Everyone / Full Control` ます。これにより、セキュリティリスクが発生します。

ワークグループモードでは、ローカルドメイン名はSMBサーバ名です。

手順

1. デフォルトの共有ACLを削除します。'vserver cifs share access-control delete -vserver <vserver\_name>-share <share\_name>-user-or-group everyone'
2. 新しいACLを設定します。

| 設定する ACL に使用するアカウント | 入力するコマンド  |
|---------------------|---|
| Windowsユーザ          | <pre>vserver cifs share access-control create -vserver &lt;vserver_name&gt; -share &lt;share_name&gt; -user-group-type windows -user-or-group &lt;Windows_domain_name\user_name&gt; -permission &lt;access_right&gt;</pre>  |
| Windowsグループ         | <pre>vserver cifs share access-control create -vserver &lt;vserver_name&gt; -share &lt;share_name&gt; -user-group-type windows -user-or-group &lt;Windows_domain_name\group_name&gt; -permission &lt;access_right&gt;</pre> |
| UNIXユーザ             | <pre>vserver cifs share access-control create -vserver &lt;vserver_name&gt; -share &lt;share_name&gt; -user-group-type &lt;unix- user&gt; -user-or-group &lt;UNIX_user_name&gt; -permission &lt;access_right&gt;</pre>      |
| UNIXグループ            | <pre>vserver cifs share access-control create -vserver &lt;vserver_name&gt; -share &lt;share_name&gt; -user-group-type &lt;unix- group&gt; -user-or-group &lt;UNIX_group_name&gt; -permission &lt;access_right&gt;</pre>    |

3. コマンドを使用して、共有に適用されたACLが正しいことを確認します `vserver cifs share access-control show`。

例

次のコマンドは、「vs1.example.com」 SVM上の「sales」共有に対するWindowsグループ「sales Team」に権限を付与します `Change`。

```

cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com

```

| Vserver         | Share Name | User/Group Name        | User/Group Type | Access Permission |
|-----------------|------------|------------------------|-----------------|-------------------|
| vs1.example.com | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs1.example.com | sales      | DOMAIN\Sales Team      | windows         | Change            |

次のコマンドは Read、「vs2.example.com」 SVM上の「eng」共有に対して「engineering」UNIXグループに権限を付与します。

```

cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com

```

| Vserver         | Share Name | User/Group Name        | User/Group Type | Access Permission |
|-----------------|------------|------------------------|-----------------|-------------------|
| vs2.example.com | c\$        | BUILTIN\Administrators | windows         | Full_Control      |
| vs2.example.com | eng        | engineering            | unix-group      | Read              |

次のコマンドは Change Full\_Control、SVM「vs1」上の「datavol5」共有に対して「Tiger Team」という名前のローカルWindowsグループに権限と「Sue Chang」という名前のローカルWindowsユーザに権限を付与します。

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change
```

```
cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control
```

```
cluster1::> vsriver cifs share access-control show -vsriver vs1
```

| Vsriver      | Share    | User/Group             | User/Group | Access       |
|--------------|----------|------------------------|------------|--------------|
| Permission   | Name     | Name                   | Type       |              |
| -----        | -----    | -----                  | -----      | -----        |
| vs1          | c\$      | BUILTIN\Administrators | windows    |              |
| Full_Control |          |                        |            |              |
| vs1          | datavol5 | Tiger Team             | windows    | Change       |
| vs1          | datavol5 | Sue Chang              | windows    | Full_Control |

## SMB共有アクセス制御リストの管理用コマンド

Access Control List (ACL ; アクセス制御リスト) の作成、表示、変更、削除など、SMBのAccess Control List (ACL ; アクセス制御リスト) を管理するためのコマンドについて説明します。

| 状況          | 使用するコマンド  |
|-------------|---|
| 新しいACLを作成する | <code>vsriver cifs share access-control create</code> |
| ACLを表示します   | <code>vsriver cifs share access-control show</code>   |
| ACLを変更します   | <code>vsriver cifs share access-control modify</code> |
| ACLを削除します   | <code>vsriver cifs share access-control delete</code> |

## 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。