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

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 `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	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Windowsグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIXユーザ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIXグループ	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

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
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
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
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
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::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

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

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
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	`vserver cifs share access-control create`
ACL を表示します	`vserver cifs share access-control show`
ACL を変更します	`vserver cifs share access-control modify`
ACL を削除します	`vserver cifs share access-control delete`

著作権に関する情報

商標に関する情報