使用 SMB 共享 ACL 确保文件访问安全

ONTAP 9

NetApp
May 09, 2024

目录

使用 SMB 共享 ACL 确保文件访问安全

管理 SMB 共享级 ACL 的准则

您可以更改共享级 ACL ，为用户授予对共享的或多或少的访问权限。您可以使用 Windows 用户和组或 UNIX 用户和组配置共享级 ACL 。

默认情况下，创建共享后，共享级 ACL 会为名为 Everyone 的标准组授予读取访问权限。ACL 中的读取访问权限意味着域和所有受信任域中的所有用户都对共享具有只读访问权限。

您可以使用 Windows 客户端上的 Microsoft 管理控制台（ MMC ）或 ONTAP 命令行更改共享级别 ACL 。

使用 MMC 时，请遵循以下准则：

- 指定的用户名和组名必须为 Windows 名称。
- 您只能指定 Windows 权限。

使用 ONTAP 命令行时，请遵循以下准则：

- 指定的用户和组名称可以是 Windows 名称或 UNIX 名称。

  如果在创建或修改 ACL 时未指定用户和组类型，则默认类型为 Windows 用户和组。

- 您只能指定 Windows 权限。

创建 SMB 共享访问控制列表

通过为 SMB 共享创建访问控制列表（ ACL ）来配置共享权限，可以控制用户和组对共享的访问级别。

关于此任务

您可以使用本地或域 Windows 用户或组名称或 UNIX 用户或组名称来配置共享级 ACL 。

在创建新ACL之前、应删除默认共享ACL `Everyone / Full Control`，这会带来安全风险。

在工作组模式下，本地域名为 SMB 服务器名称。

步骤

1. 删除默认共享ACL：`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`*`-user-or-group Everyone`
2. 配置新 ACL ：

如果要使用配置 **ACL**，请使用 ...	输入命令 ...
Windows 用户	`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 组	`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 用户	`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 组	`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. 使用验证应用于共享的ACL是否正确 `vserver cifs share access-control show` 命令：

示例

以下命令提供 `Change` 在"`Svs1.example.coms`"SVM：

```
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
```

以下命令提供 `Read` 对"`vs2.example.com`"SVM：

```
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
```

以下命令提供 `Change` 对名为"`Tiger Team`"和的本地Windows组的权限 `Full_Control` 对`Svs1d`"SVM：

```
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
```

用于管理 SMB 共享访问控制列表的命令

您需要了解用于管理 SMB 访问控制列表（ACL）的命令，其中包括创建，显示，修改和删除这些列表。

如果您要 ...	使用此命令 ...
创建新ACL	`vserver cifs share access-control create`
显示 ACL	`vserver cifs share access-control show`
修改 ACL	`vserver cifs share access-control modify`
删除 ACL	`vserver cifs share access-control delete`