



# 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 ..... 1
  - 管理 SMB 共享级 ACL 的准则 ..... 1
  - 创建 SMB 共享访问控制列表 ..... 1
  - 用于管理 SMB 共享访问控制列表的命令 ..... 4

# 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 <b>ACL</b> ，请使用 ...	输入命令 ...
Windows 用户	<pre>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</pre>
Windows 组	<pre>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</pre>
UNIX 用户	<pre>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</pre>
UNIX 组	<pre>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</pre>

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

cluster1::> vsserver cifs share access-control show -vsserver
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

以下命令提供 Read 对"vs2.example.com" SVM:

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

cluster1::> vsserver cifs share access-control show -vsserver
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

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

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

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

Vserver	Share Name	User/Group Name	User/Group Type	Access 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	<code>vsserver cifs share access-control create</code>
显示 ACL	<code>vsserver cifs share access-control show</code>
修改 ACL	<code>vsserver cifs share access-control modify</code>
删除 ACL	<code>vsserver cifs share access-control delete</code>

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。