



配置 **SMB** 客户端对共享存储的访问

ONTAP 9

NetApp
February 12, 2026

目录

配置 SMB 客户端对共享存储的访问	1
配置SMB客户端对共享ONTAP存储的访问	1
创建卷或 qtree 存储容器	1
创建ONTAP SMB卷	1
创建ONTAP SMB qtrees	2
创建ONTAP SMB共享时的要求和注意事项	3
创建ONTAP SMB共享	4
验证ONTAP SMB客户端访问	5
创建ONTAP SMB共享访问控制列表	6
在ONTAP SMB共享中配置NTFS文件权限	7
验证ONTAP SMB用户共享访问	9

配置 SMB 客户端对共享存储的访问

配置SMB客户端对共享ONTAP存储的访问

要使 SMB 客户端能够访问 SVM 上的共享存储，您必须创建一个卷或 `qtree` 来提供存储容器，然后为该容器创建或修改共享。然后，您可以配置共享和文件权限，并测试客户端系统的访问权限。

开始之前

- 必须在SVM上完全设置SMB。
- 必须完成对名称服务配置的所有更新。
- 必须完成对 Active Directory 域或工作组配置的任何添加或修改。

创建卷或 `qtree` 存储容器

创建ONTAP SMB卷

您可以使用创建卷并指定其接合点和其他属性 `volume create` 命令：

关于此任务

卷必须包含 *junction path*，才能使其数据可供客户端使用。您可以在创建新卷时指定接合路径。如果在创建卷时未指定接合路径、则必须使用 `_mount_` 在SVM命名空间中挂载此卷 `volume mount` 命令：

开始之前

- SMB应已设置并正在运行。
- SVM安全模式必须为NTFS。
- 从ONTAP 9.13.1开始、您可以创建启用了容量分析和活动跟踪的卷。要启用容量或活动跟踪，请使用或 `-activity-tracking-state`` 将设置为 ``on`` 发出 ``volume create`` 命令 ``-analytics-state``。

要了解有关容量分析和活动跟踪的更多信息，请参见 ["启用文件系统分析"](#)。有关的详细信息 `volume create`，请参见["ONTAP 命令参考"](#)。

步骤

1. 创建具有接合点的卷：

```
volume create -vserver svm_name -volume volume_name
-aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs
-junction-path junction_path
```

的选项 `-junction-path` 包括：

- 直接位于`root`下、例如、`/new_vol`

您可以创建一个新卷并指定将其直接挂载到 SVM 根卷。

- 在现有目录下、例如、 /existing_dir/new_vol

您可以创建一个新卷并指定将其挂载到现有层次结构中的现有卷，以目录的形式表示。

例如、如果要在新目录(在新卷下的新层次结构中)中创建卷、`/new_dir/new_vol`然后，必须先创建一个与SVM根卷连接的新父卷。然后，您将在新父卷的接合路径（新目录）中创建新的子卷。

2. 验证是否已使用所需的接合点创建卷：`volume show -vserver svm_name -volume volume_name -junction`

示例

以下命令将在 SVM vs1.example.com 和聚合 aggr1 上创建一个名为 users1 的新卷。新卷可通过访问 /users。此卷的大小为 750 GB，其卷保证类型为 volume（默认值）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

以下命令会在 SVM "vs1.example.com" 和聚合 "aggr1" 上创建一个名为 "home4" 的新卷。目录 /eng/ 已位于VS1 SVM的命名空间中、新卷可通过访问 /eng/home，将成为的主目录 /eng/ 命名空间。此卷的大小为750 GB、其卷保证类型为 volume (默认情况下)。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

创建ONTAP SMB qtrees

您可以使用创建一个qtree以包含您的数据、并指定其属性 `volume qtree create` 命令：

开始之前

- 要包含新 qtree 的 SVM 和卷必须已存在。

- SVM安全模式必须为NTFS、并且应设置并运行SMB。

步骤

1. 创建 qtree : `volume qtree create -vserver vs1.example.com { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

您可以将卷和qtree指定为单独的参数、也可以采用格式指定qtree路径参数
/vol/volume_name/_qtree_name。

2. 验证是否已使用所需的接合路径创建 qtree : `volume qtree show -vserver vs1.example.com { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

示例

以下示例将在SVM vs1.example.com上创建一个名为qt01的qtree、此qtree具有接合路径 /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

Vserver Name: vs1.example.com
Volume Name: data1
Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
Security Style: ntfs
Oplock Mode: enable
Unix Permissions: ---rwxr-xr-x
Qtree Id: 2
Qtree Status: normal
Export Policy: default
Is Export Policy Inherited: true
```

创建ONTAP SMB共享时的要求和注意事项

在创建 SMB 共享之前，您必须了解共享路径和共享属性的要求，尤其是主目录的要求。

创建SMB共享需要指定目录路径结构(使用 `-path` 选项 `vserver cifs share create` 命令)。目录路径对应于您在 SVM 命名空间中创建的卷或 qtree 的接合路径。在创建共享之前，必须存在目录路径和相应的接合路径。

共享路径具有以下要求：

- 目录路径名称的长度最多可以包含 255 个字符。
- 如果路径名称中有空格、则必须将整个字符串置于引号中(例如、`"/new volume/mount here"`)。

- 如果为UNC路径 (\\servername\sharename\filepath)的字符数超过256个(不包括UNC路径中的初始"\\"), 则Windows属性框中的*Security*选项卡不可用。

这是 Windows 客户端问题描述, 而不是 ONTAP 问题描述。要避免此问题描述, 请勿使用超过 256 个字符的 UNC 路径创建共享。

可以更改共享属性默认值:

- 所有共享的默认初始属性为 `oplocks`, `browsable`, `changenotify`, 和 `show-previous-versions`。
- 可以选择在创建共享时指定共享属性。

但是, 如果在创建共享时指定了共享属性, 则不会使用默认值。如果您使用 `-share-properties` 参数创建共享时, 必须使用逗号分隔列表指定要应用于共享的所有共享属性。

- 要指定主目录共享, 请使用 `homedirectory` 属性。

通过此功能, 您可以配置一个共享, 该共享可根据连接到它的用户和一组变量映射到不同的目录。您无需为每个用户创建单独的共享, 而是使用一些主目录参数配置一个共享, 以定义用户在入口点 (共享) 与其主目录 (SVM 上的目录) 之间的关系。



创建共享后, 您无法添加或删除此属性。

主目录共享具有以下要求:

- 在创建SMB主目录之前, 必须使用至少添加一个主目录搜索路径 `vserver cifs home-directory search-path add` 命令:
- 由的值指定的主目录共享 `homedirectory` 在上 `-share-properties` 参数必须包含 `%w` (Windows用户名)共享名称中的动态变量。

此外, 共享名称还可以包含 `%d` (域名)动态变量(例如 `%d/%w`)或共享名称中的静态部分(例如, `home1_%w`)。

- 如果管理员或用户使用共享连接到其他用户的主目录(使用的选项) `vserver cifs home-directory modify` 命令, 则动态共享名称模式必须前面带有波形符号 (~)。

有关的详细信息 `vserver cifs share`, 请参见"ONTAP 命令参考"。

相关信息

- "SMB管理"

创建ONTAP SMB共享

您必须先创建 SMB 共享, 然后才能与 SMB 客户端共享 SMB 服务器中的数据。创建共享时, 您可以设置共享属性, 例如将共享指定为主目录。您也可以通过配置可选设置来自定义共享。

开始之前

在创建共享之前，卷或 qtree 的目录路径必须位于 SVM 命名空间中。

关于此任务

创建共享时，默认共享ACL (默认共享权限)为 Everyone / Full Control。测试对共享的访问后，您应删除默认共享 ACL 并将其替换为更安全的替代 ACL。

步骤

1. 如有必要，为共享创建目录路径结构。

。vserver cifs share create 命令会检查中指定的路径 -path 选项。如果指定路径不存在，则命令将失败。

2. 创建与指定SVM关联的SMB共享：`vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`

3. 验证是否已创建共享：`vserver cifs share show -share-name share_name`

示例

以下命令将在SVM上创建名为`SHARE1`的SMB共享 vs1.example.com。其目录路径为 /users，并使用默认属性创建。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

验证ONTAP SMB客户端访问

您应通过访问共享并向共享写入数据来验证是否已正确配置 SMB。您应使用 SMB 服务器名称和任何 NetBIOS 别名来测试访问。

步骤

1. 登录到 Windows 客户端。
2. 使用 SMB 服务器名称测试访问：
 - a. 在Windows资源管理器中，按以下格式将驱动器映射到共享：`\\SMB_Server_Name\Share_Name`

如果映射不成功，则可能 DNS 映射尚未传播到整个网络。您必须稍后使用 SMB 服务器名称测试访问。

如果SMB服务器名为vs1.example.com、而共享名为share1、则应输入以下内容：
`\vs0.example.com\SHARE1`

b. 在新创建的驱动器上，创建一个测试文件，然后删除该文件。

您已使用 SMB 服务器名称验证对共享的写入访问。

3. 对任何 NetBIOS 别名重复步骤 2。

创建ONTAP 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。

开始之前

您必须已确定要为哪些用户或组授予对共享的访问权限。

关于此任务

您可以使用本地或域 Windows 用户名或组名称配置共享级 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	<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_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 对"vs1.example.com"SVM:上"s"共享的"SSales Team" Windows组的权限

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

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

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 Change 对名为"Tiger Team"和的本地Windows组的权限 Full_Control Svs1 SVM上的`datavol5`共享的本地Windows用户" ue Chang"的权限：

```
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	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

在ONTAP SMB共享中配置NTFS文件权限

要为有权访问共享的用户或组启用文件访问，您必须从 Windows 客户端为该共享中的文件和目录配置 NTFS 文件权限。

开始之前

执行此任务的管理员必须具有足够的 NTFS 权限才能更改对选定对象的权限。

关于此任务

"SMB管理" 您的 Windows 文档包含有关如何设置标准和高级 NTFS 权限的信息。

步骤

1. 以管理员身份登录到 Windows 客户端。
2. 从 Windows 资源管理器的 * 工具 * 菜单中, 选择 * 映射网络驱动器 *。
3. 完成 * 映射网络驱动器 * 框:
 - a. 选择一个 * 驱动器 * 字母。
 - b. 在 * 文件夹 * 框中, 键入包含要应用权限的数据的共享所在的 SMB 服务器名称以及共享的名称。

如果SMB服务器名称为SMB_SERVER01、而共享名为"SHARE1"、则应输入
\\SMB_SERVER01\SHARE1。



您可以指定SMB服务器数据接口的IP地址、而不是SMB服务器名称。

- c. 单击 * 完成 *。

您选择的驱动器已挂载并准备就绪, 此时将显示 Windows 资源管理器窗口, 其中显示共享中包含的文件和文件夹。

4. 选择要为其设置 NTFS 文件权限的文件或目录。
5. 右键单击文件或目录, 然后选择 * 属性 *。
6. 选择 * 安全性 * 选项卡。

"安全性" 选项卡将显示为其设置 NTFS 权限的用户和组的列表。 < 对象 > 的权限 框显示了对选定用户或组有效的 "允许" 和 "拒绝" 权限列表。

7. 单击 * 编辑 *。

此时将打开 < 对象 > 的权限框。

8. 执行所需的操作:

如果您要 ...	执行以下操作 ...
为新用户或组设置标准 NTFS 权限	<ol style="list-style-type: none">a. 单击 * 添加 *。 <p>此时将打开选择用户, 计算机, 服务帐户或组窗口。</p> <ol style="list-style-type: none">b. 在 * 输入要选择的对象名称 * 框中, 键入要添加 NTFS 权限的用户或组的名称。c. 单击 * 确定 *。

如果您要 ...	执行以下操作 ...
更改或删除用户或组的标准 NTFS 权限	在 * 组或用户名 * 框中，选择要更改或删除的用户或组。

9. 执行所需的操作：

如果您要 ...	执行以下操作：
为新的或现有的用户或组设置标准 NTFS 权限	在 * 对象权限 * 框中，选择要允许或不允许选定用户或组访问的类型对应的 * 允许 * 或 * 拒绝 * 框。
删除用户或组	单击 * 删除 * 。



如果无法选择部分或全部标准权限框，则是因为权限是从父对象继承的。不能选择 * 特殊权限 * 框。如果选择此选项，则表示已为选定用户或组设置一个或多个精细高级权限。

10. 添加，删除或编辑完该对象的 NTFS 权限后，单击 * 确定 * 。

验证ONTAP SMB用户共享访问

您应测试所配置的用户是否可以访问 SMB 共享及其包含的文件。

步骤

1. 在 Windows 客户端上，以现在有权访问共享的用户之一身份登录。
2. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 * 。
3. 完成 * 映射网络驱动器 * 框：
 - a. 选择一个 * 驱动器 * 字母。
 - b. 在 * 文件夹 * 框中，键入要提供给用户的共享名称。

如果SMB服务器名称为SMB_SERVER01、而共享名为"SHARE1"、则应输入
 \\SMB_SERVER01\share1。

- c. 单击 * 完成 * 。

您选择的驱动器已挂载并准备就绪，此时将显示 Windows 资源管理器窗口，其中显示共享中包含的文件和文件夹。

4. 创建一个测试文件，验证该文件是否存在，向其写入文本，然后删除该测试文件。

版权信息

版权所有 © 2026 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。