



# 使用命令行界面配置**SMB** ONTAP 9

NetApp  
April 24, 2024

# 目录

- 使用命令行界面配置SMB ..... 1
  - 使用命令行界面概述SMB配置 ..... 1
  - SMB配置工作流 ..... 1
  - 准备 ..... 2
  - 配置对SVM的SMB访问 ..... 11
  - 配置 SMB 客户端对共享存储的访问 ..... 31

# 使用命令行界面配置SMB

## 使用命令行界面概述SMB配置

您可以使用 ONTAP 9 命令行界面命令配置 SMB 客户端对新 SVM 或现有 SVM 中新卷或 qtree 中所含文件的访问权限。



SMB（服务器消息块）是指通用 Internet 文件系统（CIFS）协议的现代方言。您仍会在 ONTAP 命令行界面（CLI）和 OnCommand 管理工具中看到 CIFS。

如果要按以下方式配置对卷或 qtree 的 SMB 访问，请使用以下过程：

- 您希望使用 SMB 版本 2 或更高版本。
- 您希望仅为 SMB 客户端提供服务，而不是为 NFS 客户端提供服务（不是多协议配置）。
- 将使用NTFS文件权限来保护新卷的安全。
- 您拥有集群管理员权限，而不是 SVM 管理员权限。

创建 SVM 和 LIF 需要集群管理员权限。SVM 管理员权限足以执行其他 SMB 配置任务。

- 您希望使用命令行界面，而不是 System Manager 或自动脚本编写工具。

要使用 System Manager 配置 NAS 多协议访问，请参见 ["使用 NFS 和 SMB 为 Windows 和 Linux 配置 NAS 存储"](#)。

- 您希望使用最佳实践，而不是浏览每个可用选项。

有关命令语法的详细信息，请参见 CLI 帮助和 ONTAP 手册页。

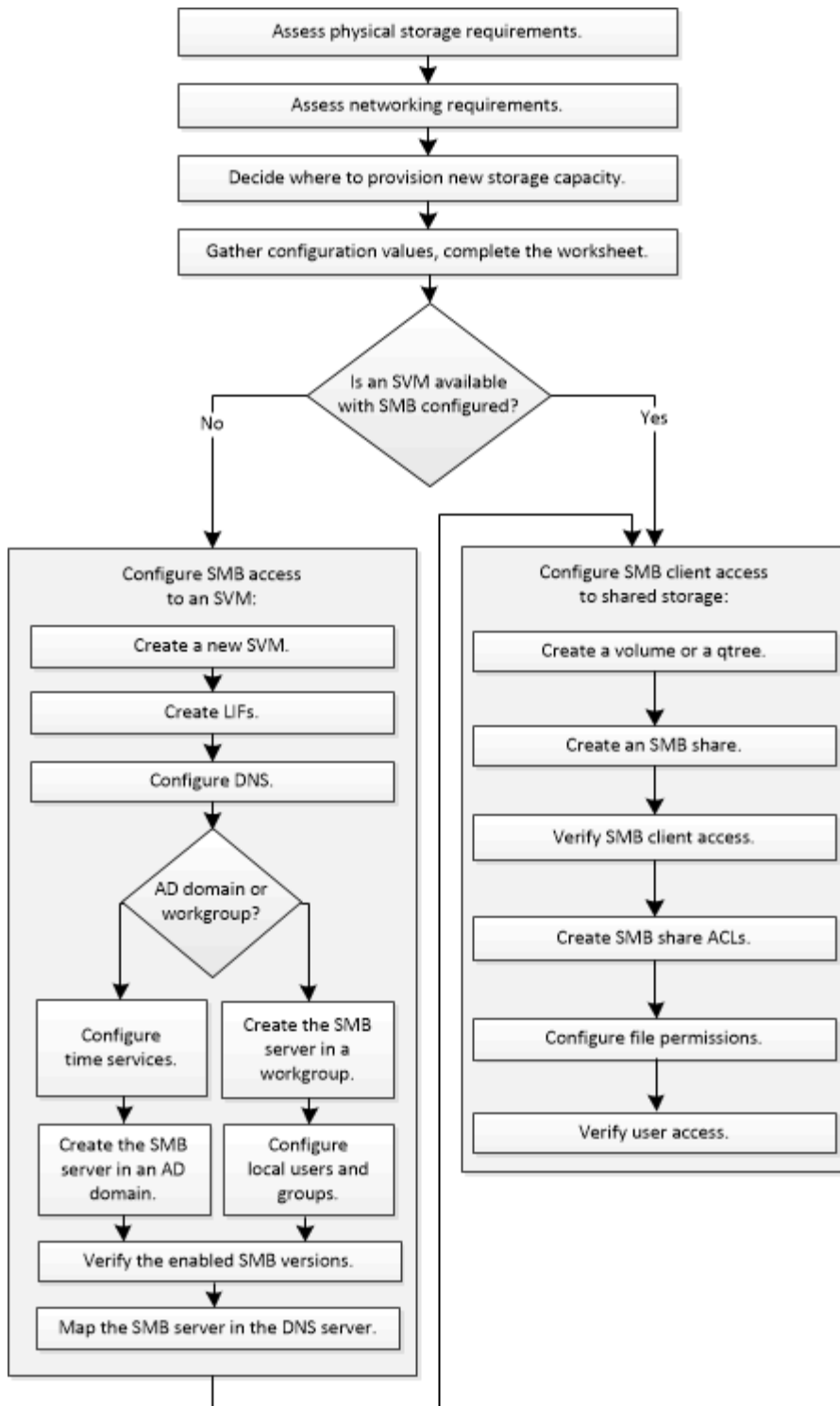
如果您需要有关 ONTAP SMB 协议功能范围的详细信息，请参见 ["SMB 参考概述"](#)。

### 在 ONTAP 中执行此操作的其他方法

要执行以下任务，请执行以下操作 ...	请参见 ...
重新设计的 System Manager（适用于 ONTAP 9.7 及更高版本）	<a href="#">"使用 SMB 为 Windows 服务器配置 NAS 存储"</a>
System Manager 经典版（适用于 ONTAP 9.7 及更早版本）	<a href="#">"SMB配置概述"</a>

## SMB配置 workflow

配置 SMB 涉及评估物理存储和网络要求，然后选择特定于您的目标的工作流；配置 SMB 对新的或现有的 SVM 的访问，或者向已完全配置 SMB 访问的现有 SVM 添加卷或 qtree。



## 准备

### 评估物理存储要求

在为客户端配置SMB存储之前、您必须确保现有聚合中有足够的空间来容纳新卷。如果没有，您可以向现有聚合添加磁盘或创建所需类型的新聚合。

### 步骤

# 1. 显示现有聚合中的可用空间： storage aggregate show

如果聚合具有足够的空间，请在工作表中记录其名称。

```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_4	239.0GB	238.9GB	95%	online	5	node3	raid_dp, normal
aggr_5	239.0GB	239.0GB	95%	online	4	node4	raid_dp, normal

6 entries were displayed.

# 2. 如果没有具有足够空间的聚合、请使用向现有聚合添加磁盘 storage aggregate add-disks 命令、或者使用创建新聚合 storage aggregate create 命令：

## 评估网络连接要求

在向客户端提供SMB存储之前、您必须验证是否已正确配置网络以满足SMB配置要求。

开始之前

必须配置以下集群网络对象：

- 物理和逻辑端口
- 广播域
- 子网（如果需要）
- IP 空间（除默认 IP 空间外，根据需要）
- 故障转移组（根据需要，除每个广播域的默认故障转移组外）
- 外部防火墙

步骤

1. 显示可用的物理和虚拟端口： network port show
  - 如果可能，您应使用数据网络速度最快的端口。
  - 数据网络中的所有组件都必须具有相同的 MTU 设置，才能获得最佳性能。
2. 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，请验证子网是否存在且具有足够的可用地址：

```
network subnet show
```

子网包含属于同一第 3 层子网的 IP 地址池。可使用创建子网 `network subnet create` 命令：

3. 显示可用 IP 空间： `network ipspace show`

您可以使用默认 IP 空间或自定义 IP 空间。

4. 如果要使用 IPv6 地址，请验证是否已在集群上启用 IPv6： `network options ipv6 show`

如果需要、您可以使用启用IPv6 `network options ipv6 modify` 命令：

## 确定在何处配置新的**SMB**存储容量

在创建新的 SMB 卷或 qtree 之前，您必须确定是将其置于新的还是现有的 SVM 中，以及 SVM 需要多少配置。此决定将决定您的工作流。

### 选项

- 如果要在新 SVM 或已启用但未配置 SMB 的现有 SVM 上配置卷或 qtree，请完成 "配置对 SVM 的 SMB 访问" 和 "向启用了 SMB 的 SVM 添加存储容量" 中的步骤。

#### 配置对SVM的SMB访问

#### 配置 SMB 客户端对共享存储的访问

如果满足以下条件之一，您可以选择创建新的 SVM：

- 首次在集群上启用SMB。
- 您不希望在集群中的现有SVM中启用SMB支持。
- 一个集群中有一个或多个启用了 SMB 的 SVM，您需要以下连接之一：
  - 到其他 Active Directory 林或工作组。
  - 连接到隔离命名空间中的 SMB 服务器（多租户情形）。要在已启用但未配置SMB的现有SVM上配置存储、您还应选择此选项。如果您创建了用于 SAN 访问的 SVM，或者在创建 SVM 时未启用任何协议，则可能会出现这种情况。

在SVM上启用SMB后、继续配置卷或qtree。

- 如果要在已完全配置为可进行 SMB 访问的现有 SVM 上配置卷或 qtree，请完成 "将存储容量添加到已启用 SMB 的 SVM" 中的步骤。

#### 配置 SMB 客户端对共享存储的访问

## 用于收集**SMB**配置信息的工作表

通过SMB配置工作表、您可以收集为客户端设置SMB访问所需的信息。

您应完成工作表的一个或两个部分，具体取决于您决定在何处配置存储：

- 如果要配置对 SVM 的 SMB 访问，则应完成这两个部分。

#### 配置对SVM的SMB访问

##### 配置 SMB 客户端对共享存储的访问

- 如果要向启用了SMB的SVM添加存储容量、则只应完成第二部分。

##### 配置 SMB 客户端对共享存储的访问

命令手册页包含有关参数的详细信息。

#### 配置对SVM的SMB访问

- 用于创建 SVM\* 的参数

您可以在中提供这些值 `vserver create` 命令。

字段	Description	您的价值
<code>-vserver</code>	您为新 SVM 提供的名称，可以是完全限定域名（FQDN），也可以遵循在集群中强制实施唯一 SVM 名称的其他约定。	
<code>-aggregate</code>	集群中具有足够空间来容纳新SMB存储容量的聚合的名称。	
<code>-rootvolume</code>	为 SVM 根卷提供的唯一名称。	
<code>-rootvolume-security-style</code>	对SVM使用NTFS安全模式。	<code>ntfs</code>
<code>-language</code>	在此工作流中使用默认语言设置。	<code>C.UTF-8</code>
<code>ipspace</code>	可选：IP 空间是 SVM 所在的不同 IP 地址空间。	

- 用于创建 LIF\* 的参数

您可以在中提供这些值 `network interface create` 命令。

字段	Description	您的价值
<code>-lif</code>	为新 LIF 提供的名称。	
<code>-role</code>	在此工作流中使用数据 LIF 角色。	<code>data</code>

字段	Description	您的价值
-data-protocol	在此工作流中仅使用SMB协议。	cifs
-home-node	LIF返回到的节点 network interface revert 命令将在LIF上运行。	
-home-port	LIF返回到的端口或接口组 network interface revert 命令将在LIF上运行。	
-address	集群上要由新 LIF 用于数据访问的 IPv4 或 IPv6 地址。	
-netmask	LIF 的网络掩码和网关。	
-subnet	IP 地址池。已使用、而不是 -address 和 -netmask 自动分配地址和网络掩码。	
-firewall-policy	在此工作流中使用默认数据防火墙策略。	data
-auto-revert	可选：指定数据 LIF 是在启动时还是在其他情况下自动还原到其主节点。默认设置为 false。	

- 用于 DNS 主机名解析的参数 \*

您可以在中提供这些值 `vserver services name-service dns create` 命令。

字段	Description	您的价值
-domains	最多五个 DNS 域名。	
-name-servers	每个 DNS 名称服务器最多三个 IP 地址。	

## 在 **Active Directory** 域中设置 **SMB** 服务器

- 时间服务配置的参数 \*

您可以在中提供这些值 `cluster time-service ntp server create` 命令。



字段	Description	您的价值
-server	Active Directory 域的 NTP 服务器的主机名或 IP 地址。	

- 用于在 Active Directory 域中创建 SMB 服务器的参数 \*

您可以在中提供这些值 `vserver cifs create` 命令。

字段	Description	您的价值
-vserver	要在其中创建 SMB 服务器的 SVM 的名称。	
-cifs-server	SMB 服务器的名称（最多 15 个字符）。	
-domain	要与 SMB 服务器关联的 Active Directory 域的完全限定域名（FQDN）。	
-ou	可选：Active Directory 域中要与 SMB 服务器关联的组织单位。默认情况下，此参数设置为 CN=Computers。	
-netbios-aliases	可选：NetBIOS 别名列表，这些别名是 SMB 服务器名称的备用名称。	
-comment	可选：服务器的文本注释。在网络上浏览服务器时，Windows 客户端可以看到此 SMB 服务器问题描述。	

## 在工作组中设置 SMB 服务器

- 用于在工作组中创建 SMB 服务器的参数 \*

您可以在中提供这些值 `vserver cifs create` 命令。

字段	Description	您的价值
-vserver	要在其中创建 SMB 服务器的 SVM 的名称。	
-cifs-server	SMB 服务器的名称（最多 15 个字符）。	

字段	Description	您的价值
-workgroup	工作组的名称（最多 15 个字符）。	
-comment	可选：服务器的文本注释。在网络上浏览服务器时，Windows 客户端可以看到此 SMB 服务器问题描述。	

- 用于创建本地用户的参数 \*

您可以在创建本地用户时使用提供以下值 `vserver cifs users-and-groups local-user create` 命令：它们对于工作组中的 SMB 服务器是必需的，在 AD 域中是可选的。

字段	Description	您的价值
-vserver	要在其中创建本地用户的 SVM 的名称。	
-user-name	本地用户的名称（最多 20 个字符）。	
-full-name	可选：用户的全名。如果全名包含空格，请将全名用双引号括起来。	
-description	可选：本地用户的问题描述。如果问题描述包含空格，请将参数用引号括起来。	
-is-account-disabled	可选：指定用户帐户是启用还是禁用。如果未指定此参数，则默认为启用用户帐户。	

- 用于创建本地组的参数 \*

您可以在创建本地组时使用提供以下值 `vserver cifs users-and-groups local-group create` 命令：对于 AD 域和工作组中的 SMB 服务器，它们是可选的。

字段	Description	您的价值
-vserver	要在其中创建本地组的 SVM 的名称。	
-group-name	本地组的名称（最多 256 个字符）。	
-description	可选：本地组的问题描述。如果问题描述包含空格，请将参数用引号括起来。	

向启用了**SMB**的**SVM**添加存储容量

用于创建卷的 \* 参数 \*

您可以在中提供这些值 `volume create` 命令。

字段	Description	您的价值
<code>-vserver</code>	要托管新卷的新 SVM 或现有 SVM 的名称。	
<code>-volume</code>	为新卷提供的唯一描述性名称。	
<code>-aggregate</code>	集群中为新SMB卷提供足够空间的聚合的名称。	
<code>-size</code>	为新卷的大小提供的整数。	
<code>-security-style</code>	对此工作流使用NTFS安全模式。	<code>ntfs</code>
<code>-junction-path</code>	根 (/) 下要挂载新卷的位置。	

用于创建 `qtree`\* 的 \* 参数

您可以在中提供这些值 `volume qtree create` 命令。

字段	Description	您的价值
<code>-vserver</code>	包含 <code>qtree</code> 的卷所在 SVM 的名称。	
<code>-volume</code>	要包含新 <code>qtree</code> 的卷的名称。	
<code>-qtree</code>	为新 <code>qtree</code> 提供的唯一描述性名称，不超过 64 个字符。	
<code>-qtree-path</code>	格式的 <code>qtree</code> 路径参数 <code>/vol/volume_name/qtree_name\&gt;</code> 可以指定、而不是将卷和 <code>qtree</code> 指定为单独的参数。	

- 用于创建 SMB 共享的参数 \*

您可以在中提供这些值 `vserver cifs share create` 命令：

字段	Description	您的价值
-vserver	要在其中创建 SMB 共享的 SVM 的名称。	
-share-name	要创建的 SMB 共享的名称（最多 256 个字符）。	
-path	SMB 共享路径的名称（最多 256 个字符）。在创建共享之前，此路径必须存在于卷中。	
-share-properties	可选：共享属性列表。默认设置为 oplocks, browsable, changenotify, 和 show-previous-versions。	
-comment	可选：服务器的文本注释（最多 256 个字符）。在网络上浏览时，Windows 客户端可以看到此 SMB 共享问题描述。	

- 用于创建 SMB 共享访问控制列表（ACL）的参数 \*

您可以在中提供这些值 vservers cifs share access-control create 命令：

字段	Description	您的价值
-vserver	要在其中创建 SMB ACL 的 SVM 的名称。	
-share	要创建的 SMB 共享的名称。	
-user-group-type	要添加到共享 ACL 的用户或组的类型。默认类型为 windows	windows
-user-or-group	要添加到共享 ACL 的用户或组。如果指定用户名，则必须使用 domain\username 格式包含用户的域。	
-permission	指定用户或组的权限。	`[ No_access
Read	Change	Full_Control ]`

# 配置对SVM的SMB访问

## 配置对SVM的SMB访问

如果尚未为 SMB 客户端访问配置 SVM ，则必须创建并配置新的 SVM 或配置现有 SVM 。配置 SMB 包括打开 SVM 根卷访问，创建 SMB 服务器，创建 LIF ，启用主机名解析，配置名称服务，如果需要， 启用 Kerberos 安全性。

### 创建 SVM：

如果集群中还没有至少一个SVM来为SMB客户端提供数据访问、则必须创建一个SVM。

#### 开始之前

- 从ONTAP 9.13.1开始、您可以为Storage VM设置最大容量。您还可以在SVM接近阈值容量级别时配置警报。有关详细信息，请参见 [管理SVM容量](#)。

#### 步骤

1. 创建 SVM： `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
  - 对使用NTFS设置 `-rootvolume-security-style` 选项
  - 使用默认C.UTF-8 `-language` 选项
  - `ipspace` 设置是可选的。
2. 验证新创建的 SVM 的配置和状态： `vserver show -vserver vserver_name`
  - Allowed Protocols 字段必须包含CIFS。您可以稍后编辑此列表。
  - Vserver Operational State 字段必须显示 running 状态。如果显示 initializing 状态、表示某些中间操作(如创建根卷)失败、您必须删除SVM并重新创建它。

#### 示例

以下命令将在IP空间中创建用于数据访问的SVM ipspaceA：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

以下命令显示已创建根卷为1 GB的SVM、并且此SVM已自动启动并位于中 running 状态。根卷具有一个默认导出策略，该策略不包含任何规则，因此根卷在创建时不会导出。

```
cluster1::> vserver show -vserver vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



从ONTAP 9.13.1开始、您可以设置自适应QoS策略组模板、以便为SVM中的卷应用吞吐量下限和上限限制。只有在创建SVM之后、才能应用此策略。要了解有关此过程的更多信息、请参见 [设置自适应策略组模板](#)。

## 验证是否已在**SVM**上启用**SMB**协议

要在SVM上配置和使用SMB、必须先验证协议是否已启用。

### 关于此任务

此操作通常在SVM设置期间完成、但如果您在设置期间未启用此协议、则可以稍后使用启用它 `vserver add-protocols` 命令：



创建 LIF 后，您不能在该 LIF 中添加或删除协议。

您还可以使用在SVM上禁用协议 `vserver remove-protocols` 命令：

### 步骤

1. 检查 SVM 当前已启用和禁用的协议： `vserver show -vserver vserver_name -protocols`

您也可以使用 `vserver show-protocols` 命令以查看集群中所有SVM上当前已启用的协议。

2. 如有必要，启用或禁用协议：

- 启用SMB协议： `vserver add-protocols -vserver vserver_name -protocols cifs`
- 禁用协议： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. 确认已启用和禁用的协议已正确更新： `vserver show -vserver vserver_name -protocols`

#### 示例

以下命令显示 SVM vs1 上当前已启用和禁用（允许和不允许）的协议：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                        nfs, fcp, iscsi, ndmp
```

以下命令可通过添加来允许通过SMB进行访问 `cifs` 到SVM VS1上已启用的协议列表：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

## 打开 **SVM** 根卷的导出策略

SVM根卷的默认导出策略必须包含一条规则、以允许所有客户端通过SMB进行公开访问。如果没有此规则、则会拒绝所有SMB客户端访问SVM及其卷。

#### 关于此任务

创建新的 SVM 时，系统会自动为 SVM 的根卷创建默认导出策略（称为 `default`）。您必须为默认导出策略创建一个或多个规则，客户端才能访问 SVM 上的数据。

您应验证是否已在默认导出策略中打开所有 SMB 访问，然后通过为单个卷或 `qtree` 创建自定义导出策略来限制对单个卷的访问。

#### 步骤

1. 如果您使用的是现有 SVM，请检查默认根卷导出策略： `vserver export-policy rule show`

命令输出应类似于以下内容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance
```

```

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

如果存在允许开放访问的规则，则此任务将完成。如果没有，请继续执行下一步。

2. 为 SVM 根卷创建导出规则： `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

3. 使用验证规则创建 `vserver export-policy rule show` 命令：

## 结果

现在、任何SMB客户端均可访问在SVM上创建的任何卷或qtree。

## 创建 LIF

LIF 是指与物理或逻辑端口关联的 IP 地址。如果组件出现故障，则 LIF 可以故障转移到或迁移到其他物理端口，从而继续与网络通信。

### 开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 up 状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

子网包含属于同一第 3 层子网的 IP 地址池。它们是使用创建的 `network subnet create` 命令：

- 用于指定 LIF 处理的流量类型的机制已发生更改。对于 ONTAP 9.5 及更早版本，LIF 使用角色指定要处理的流量类型。从 ONTAP 9.6 开始，LIF 使用服务策略指定要处理的流量类型。

### 关于此任务

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF 。
- 如果集群中有大量LIF、则可以使用验证集群上支持的LIF容量 `network interface capacity show` 命令以及每个节点上支持的LIF容量 `network interface capacity details show` 命令(在高级权限级别)。
- 从 ONTAP 9.7 开始，如果同一子网中已存在 SVM 的其他 LIF ，则无需指定 LIF 的主端口。ONTAP 会自动



在与已在同一子网中配置的其他 LIF 位于同一广播域的指定主节点上选择一个随机端口。

## 步骤

### 1. 创建 LIF：

```
network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}
```

#### \* ONTAP 9.5 及更早版本 \*

```
`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

#### \* ONTAP 9.6 及更高版本 \*

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home-node node_name -home-port port_name {-address IP_address -netmask IP_address -subnet-name subnet_name} -firewall-policy data -auto-revert {true false}`
```

- -role 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。
- -data-protocol 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。使用ONTAP 9.5及更早版本时，-data-protocol 必须在创建LIF时指定参数、如果不销毁并重新创建数据LIF、则以后无法修改此参数。
- -home-node 是LIF返回到的节点 network interface revert 命令将在LIF上运行。

您还可以使用指定LIF是否应自动还原到主节点和主端口 -auto-revert 选项

- -home-port 是LIF返回到的物理或逻辑端口 network interface revert 命令将在LIF上运行。
- 您可以使用指定IP地址 -address 和 -netmask 选项、或者使用启用从子网分配 -subnet\_name 选项
- 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
- 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。network route create 手册页包含有关在SVM中创建静态路由的信息。
- -firewall-policy 选项中、使用相同的默认值 data 作为LIF角色。

如果需要，您可以稍后创建和添加自定义防火墙策略。



从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 ["为 LIF 配置防火墙策略"](#)。

- `-auto-revert` 用于指定在启动、更改管理数据库状态或建立网络连接等情况下，数据LIF是否自动还原到其主节点。默认设置为 `false`，但您可以将其设置为 `true` 具体取决于您环境中的网络管理策略。

## 2. 验证是否已成功创建 LIF：

```
network interface show
```

## 3. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	<code>network ping</code>
IPv6地址	<code>network ping6</code>

## 示例

以下命令将使用创建LIF并指定IP地址和网络掩码值 `-address` 和 `-netmask` 参数：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

以下命令将创建一个 LIF，并从指定子网（名为 `client1_sub`）分配 IP 地址和网络掩码值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

以下命令显示 `cluster-1` 中的所有 LIF。数据 LIF `datalif1` 和 `datalif3` 配置了 IPv4 地址，而 `datalif4` 配置了 IPv6 地址：

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	clus1	up/up	192.0.2.12/24	node-1	e0a
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2					
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c
5 entries were displayed.					

以下命令显示如何创建分配给NAS数据LIF default-data-files 服务策略:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

## 启用 DNS 以进行主机名解析

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

开始之前

站点范围的 DNS 服务器必须可用于主机名查找。

您应配置多个 DNS 服务器，以避免单点故障。。 `vserver services name-service dns create` 如果仅输入一个DNS服务器名称、则命令会发出警告。

关于此任务

网络管理指南 \_ 包含有关在 SVM 上配置动态 DNS 的信息。

步骤

1. 在 SVM 上启用 DNS : `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

以下命令将在 SVM vs1 上启用外部 DNS 服务器：

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



从ONTAP 9.2开始、`vserver services name-service dns create` 命令会执行自动配置验证、如果ONTAP无法联系到名称服务器、则会报告错误消息。

2. 使用显示DNS域配置 `vserver services name-service dns show` 命令： ``

以下命令显示集群中所有 SVM 的 DNS 配置：

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

以下命令显示 SVM vs1 的详细 DNS 配置信息：

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

### 3. 使用验证名称服务器的状态 `vserver services name-service dns check` 命令:

- `vserver services name-service dns check` 命令从ONTAP 9.2开始可用。

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## 在 Active Directory 域中设置 SMB 服务器

### 配置时间服务

在 Active Domain 控制器中创建 SMB 服务器之前，您必须确保集群时间和 SMB 服务器所属域的域控制器上的时间在五分钟内匹配。

### 关于此任务

您应将集群 NTP 服务配置为使用与 Active Directory 域相同的 NTP 服务器进行时间同步。

从 ONTAP 9.5 开始，您可以使用对称身份验证设置 NTP 服务器。

### 步骤

#### 1. 使用配置时间服务 `cluster time-service ntp server create` 命令:

- 要配置不采用对称身份验证的时间服务、请输入以下命令: `cluster time-service ntp server create -server server_ip_address`
- 要使用对称身份验证配置时间服务、请输入以下命令: `cluster time-service ntp server create -server server_ip_address -key-id key_id`  
`cluster time-service ntp server create -server 10.10.10.1`  
`cluster time-service ntp server create -server 10.10.10.2`

#### 2. 使用验证是否已正确设置时间服务 `cluster time-service ntp server show` 命令:

```
cluster time-service ntp server show
```

Server	Version
10.10.10.1	auto
10.10.10.2	auto

用于在 **NTP** 服务器上管理对称身份验证的命令

从 ONTAP 9.5 开始，支持网络时间协议（NTP）版本 3。NTPv3 包括使用 SHA-1 密钥的对称身份验证，可提高网络安全性。

要执行此操作 ...	使用此命令 ...
配置不使用对称身份验证的 NTP 服务器	<pre>cluster time-service ntp server create -server server_name</pre>
使用对称身份验证配置 NTP 服务器	<pre>cluster time-service ntp server create -server server_ip_address -key-id key_id</pre>
为现有 NTP 服务器启用对称身份验证可以通过添加所需的密钥 ID 来修改现有 NTP 服务器以启用身份验证。	<pre>cluster time-service ntp server modify -server server_name -key-id key_id</pre>
配置共享 NTP 密钥	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div> 共享密钥由 ID 引用。节点和 NTP 服务器上的 ID，类型和值必须相同</div>
使用未知密钥 ID 配置 NTP 服务器	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre>
使用未在 NTP 服务器上配置的密钥 ID 配置服务器。	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div> 密钥 ID，类型和值必须与 NTP 服务器上配置的密钥 ID，类型和值相同。</div>
禁用对称身份验证	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

## 在 **Active Directory** 域中创建 **SMB** 服务器

您可以使用 `vserver cifs create` 命令以在 SVM 上创建 SMB 服务器并指定其所属的 Active Directory (AD) 域。

### 开始之前

您用于提供数据的 SVM 和 LIF 必须已配置为允许 SMB 协议。LIF 必须能够连接到 SVM 上配置的 DNS 服务器以及要加入 SMB 服务器的域的 AD 域控制器。

任何有权在 SMB 服务器要加入的 AD 域中创建计算机帐户的用户都可以在 SVM 上创建 SMB 服务器。这可能

包括来自其他域的用户。

从 ONTAP 9.7 开始，您的 AD 管理员可以为您提供 keytab 文件的 URI，而不是为您提供特权 Windows 帐户的名称和密码。收到此 URI 后，请将其包含在中 `-keytab-uri` 参数 `vserver cifs` 命令

关于此任务

在 Active Directory 域中创建 SMB 服务器时：

- 指定域时，必须使用完全限定域名（FQDN）。
- 默认设置是将 SMB 服务器计算机帐户添加到 Active Directory CN=Computer 对象。
- 您可以选择使用将 SMB 服务器添加到其他组织单位(OU) `-ou` 选项
- 您也可以选择为 SMB 服务器添加一个或多个 NetBIOS 别名（最多 200 个）的逗号分隔列表。

如果要将其他文件服务器中的数据整合到 SMB 服务器并希望 SMB 服务器响应原始服务器的名称，则为 SMB 服务器配置 NetBIOS 别名非常有用。

。 `vserver cifs` 手册页包含其他可选参数和命名要求。



从 ONTAP 9.1 开始，您可以启用 SMB 版本 2.0 以连接到域控制器（DC）。如果已在域控制器上禁用 SMB 1.0，则必须执行此操作。从 ONTAP 9.2 开始，SMB 2.0 默认处于启用状态。

从 ONTAP 9.8 开始，您可以指定对与域控制器的连接进行加密。当时，ONTAP 需要对域控制器通信进行加密 `-encryption-required-for-dc-connection` 选项设置为 `true`；默认值为 `false`。如果设置了此选项，则只有 SMB3 协议将用于 ONONTAP DC 连接，因为只有 SMB3 才支持加密。。

"SMB 管理" 包含有关 SMB 服务器配置选项的详细信息。

步骤

1. 验证集群上的 SMB 是否已获得许可：`system license show -package cifs`

SMB 许可证包含在中 "ONTAP One"。如果您没有 ONTAP One、并且未安装许可证、请联系您的销售代表。

如果 SMB 服务器仅用于身份验证，则不需要 CIFS 许可证。

2. 在 AD 域中创建 SMB 服务器：`vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

加入域时，此命令可能需要几分钟才能完成。

以下命令会在域 "example.com" 中创建 SMB 服务器 "smb\_server01"

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
smb_server01 -domain example.com
```

以下命令会在域 mydomain.com 中创建 SMB 服务器 smb\_server02，并使用 keytab 文件对

ONTAP 管理员进行身份验证:

```
cluster1::> vsserver cifs create -vsserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. 使用验证SMB服务器配置 `vsserver cifs show` 命令:

在此示例中, 命令输出显示已在 SVM vs1.example.com 上创建名为 SMB\_server01 的 SMB 服务器, 并加入 “example.com” 域。

```
cluster1::> vsserver cifs show -vsserver vs1  
  
Vserver: vs1.example.com  
CIFS Server NetBIOS Name: SMB_SERVER01  
NetBIOS Domain/Workgroup Name: EXAMPLE  
Fully Qualified Domain Name: EXAMPLE.COM  
Default Site Used by LIFs Without Site Membership:  
Authentication Style: domain  
CIFS Server Administrative Status: up  
CIFS Server Description: -  
List of NetBIOS Aliases: -
```

4. 如果需要、请启用与域控制器的加密通信(ONTAP 9.8及更高版本): `vsserver cifs security modify -vsserver svm_name -encryption-required-for-dc-connection true`

示例

以下命令会在 SVM vs2.example.com 上的 “example.com” 域中创建一个名为 smb\_server02 的 SMB 服务器。计算机帐户在 “OU=eng , OU=corp , DC=example , DC=com” 容器中创建。SMB 服务器分配有 NetBIOS 别名。



```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

以下命令允许来自其他域的用户（此处为受信任域的管理员）在 SVM vs3.example.com 上创建名为 smb\_server03 的 SMB 服务器。。 -domain 选项用于指定要在其中创建SMB服务器的主域的名称(在DNS配置中指定)。。 username 选项指定受信任域的管理员。

- 主域： example.com
- 受信任域： trust.lab.com
- 受信任域的用户名： Administrator1.

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

创建用于 **SMB** 身份验证的 **keytab** 文件

从 ONTAP 9.7 开始，ONTAP 支持使用 keytab 文件对 Active Directory（AD）服务器进行 SVM 身份验证。AD管理员生成一个keytab文件、并将其作为统一资源标识符(URI)提供给ONTAP管理员 vserver cifs 命令要求对AD域进行Kerberos身份验证。

AD管理员可以使用标准Windows Server创建keytab文件 ktpass 命令：此命令应在需要进行身份验证的主域上运行。。 ktpass 命令只能用于为主域用户生成keytab文件；不支持使用受信任域用户生成的密钥。

系统会为特定 ONTAP 管理员用户生成 keytab 文件。只要管理员用户的密码不更改，为特定加密类型和域生成的密钥就不会更改。因此，每当更改管理员用户的密码时，都需要一个新的 keytab 文件。

支持以下加密类型：

- ES256-SHA1

- DES-CBC-MD5



ONTAP 不支持 DES-CBC-CRC 加密类型。

- RC4-HMAC

AES256 是最高的加密类型，如果在 ONTAP 系统上启用，则应使用此类型。

可以通过指定管理员密码或使用随机生成的密码来生成 keytab 文件。但是，在任何给定时间，只能使用一个密码选项，因为在 AD 服务器上需要管理员用户专用的专用密钥来解密 keytab 文件中的密钥。对特定管理员的私钥进行任何更改都会使 keytab 文件失效。

## 在工作组中设置 **SMB** 服务器

在工作组概述中设置 **SMB** 服务器

将 SMB 服务器设置为工作组的成员包括创建 SMB 服务器，然后创建本地用户和组。

当 Microsoft Active Directory 域基础架构不可用时，您可以在工作组中配置 SMB 服务器。

工作组模式下的 SMB 服务器仅支持 NTLM 身份验证，不支持 Kerberos 身份验证。

在工作组中创建 **SMB** 服务器

您可以使用 `vserver cifs create` 命令以在 SVM 上创建 SMB 服务器并指定其所属的工作组。

开始之前

您用于提供数据的 SVM 和 LIF 必须已配置为允许 SMB 协议。LIF 必须能够连接到 SVM 上配置的 DNS 服务器。

关于此任务

工作组模式下的 SMB 服务器不支持以下 SMB 功能：

- SMB3 见证协议
- SMB3 CA 共享
- 基于 SMB 的 SQL
- 文件夹重定向
- 漫游配置文件
- 组策略对象（GPO）
- 卷快照服务（VSS）

。 `vserver cifs` 手册页包含其他可选配置参数和命名要求。

步骤

1. 验证集群上的 SMB 是否已获得许可：`system license show -package cifs`

SMB许可证包含在中 **"ONTAP One"**。如果您没有ONTAP One、并且未安装许可证、请联系您的销售代表。

如果 SMB 服务器仅用于身份验证，则不需要 CIFS 许可证。

2. 在工作组中创建SMB服务器: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

以下命令会在工作组 "workgroup01" 中创建 SMB 服务器 "smb\_server01":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. 使用验证SMB服务器配置 `vserver cifs show` 命令:

在以下示例中，命令输出显示已在工作组 "workgroup01" 的 SVM vs1.example.com 上创建名为 smb\_server01 的 SMB 服务器:

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

完成后

对于工作组中的 CIFS 服务器，您必须在 SVM 上创建本地用户以及可选的本地组。

相关信息

["SMB管理"](#)

创建本地用户帐户

您可以创建本地用户帐户，该帐户可用于授权通过 SMB 连接访问 SVM 中包含的数据。创建 SMB 会话时，您还可以使用本地用户帐户进行身份验证。

关于此任务

默认情况下，创建 SVM 时会启用本地用户功能。

创建本地用户帐户时，必须指定用户名，并且必须指定要与该帐户关联的 SVM。

。 `vserver cifs users-and-groups local-user` 手册页包含有关可选参数和命名要求的详细信息。

#### 步骤

1. 创建本地用户： `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

以下可选参数可能有用：

- `-full-name`

用户的全名。

- `-description`

本地用户的问题描述。

- `-is-account-disabled {true|false}`

指定用户帐户是启用还是禁用。如果未指定此参数，则默认为启用用户帐户。

命令将提示输入本地用户的密码。

2. 输入本地用户的密码，然后确认该密码。
3. 验证是否已成功创建此用户： `vserver cifs users-and-groups local-user show -vserver vserver_name`

#### 示例

以下示例将创建一个与 SVM `vs1.example.com` 关联的本地用户 `"SMB_server01\sue"`，其全名为 `"Sue Chang"`：

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                               Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator                   Built-in administrator
account
vs1      SMB_SERVER01\sue                             Sue Chang
```

#### 创建本地组

您可以创建本地组，用于授权通过 SMB 连接访问与 SVM 关联的数据。您还可以分配权限

，以定义组成员的用户权限或功能。

关于此任务

创建 SVM 时，默认情况下会启用本地组功能。

创建本地组时，必须为该组指定一个名称，并且必须指定要与该组关联的 SVM。您可以指定包含或不包含本地域名的组名称，也可以选择为本地组指定问题描述。您不能将本地组添加到其他本地组。

。 `vserver cifs users-and-groups local-group` 手册页包含有关可选参数和命名要求的详细信息。

步骤

- 1. 创建本地组： `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

以下可选参数可能很有用：

- `-description`

本地组的问题描述。

- 2. 验证是否已成功创建此组： `vserver cifs users-and-groups local-group show -vserver vserver_name`

示例

以下示例将创建一个与 SVM vs1 关联的本地组 `SMB_server01\engineering`：

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

完成后

您必须向新组添加成员。

## 管理本地组成员资格

您可以通过添加和删除本地或域用户，或者添加和删除域组来管理本地组成员资格。如果您希望根据对组的访问控制来控制对数据的访问，或者您希望用户拥有与该组关联的权限，则此功能非常有用。

### 关于此任务

如果您不再希望本地用户，域用户或域组具有基于组成员资格的访问权限，则可以从组中删除此成员。

向本地组添加成员时，必须牢记以下几点：

- 您不能将用户添加到特殊的 `_Everyone` 组。
- 您不能将本地组添加到其他本地组。
- 要将域用户或组添加到本地组，ONTAP 必须能够将此名称解析为 SID。

从本地组中删除成员时，必须牢记以下几点：

- 您不能从特殊的 `_Everyone` 组中删除成员。
- 要从本地组中删除成员，ONTAP 必须能够将其名称解析为 SID。

### 步骤

#### 1. 向组添加成员或从组中删除成员。

- 添加成员：`vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

您可以指定要添加到指定本地组的本地用户，域用户或域组的逗号分隔列表。

- 删除成员：`vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

您可以指定要从指定本地组中删除的本地用户，域用户或域组的逗号分隔列表。

### 示例

以下示例将本地用户 `SMB_server01\sue` 添加到 SVM `vs1.example.com` 上的本地组 `SMB_server01\engineering`：

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

以下示例将从 SVM `vs1.example.com` 上的本地组 `Smb_server01\engineering` 中删除本地用户 `Smb_server01\sue` 和 `Smb_server01\james`：

```
cluster1::> vservers cifs users-and-groups local-group remove-members  
-vservers vs1.example.com -group-name SMB_SERVER\engineering -member-names  
SMB_SERVER\sue,SMB_SERVER\james
```

## 验证已启用的 **SMB** 版本

ONTAP 9 版本可确定默认情况下为与客户端和域控制器的连接启用的 SMB 版本。您应验证 SMB 服务器是否支持环境中所需的客户端和功能。

### 关于此任务

对于与客户端和域控制器的连接，应尽可能启用 SMB 2.0 及更高版本。出于安全原因，您应避免使用 SMB 1.0，如果您已确认环境中不需要 SMB 1.0，则应将其禁用。

在 ONTAP 9 中，默认情况下会为客户端连接启用 SMB 2.0 及更高版本，但默认启用的 SMB 1.0 版本取决于您的 ONTAP 版本。

- 从 ONTAP 9.1 P8 开始，可以在 SVM 上禁用 SMB 1.0。
  - `-smb1-enabled` 选项 `vservers cifs options modify` 命令用于启用或禁用 SMB 1.0。
- 从 ONTAP 9.3 开始，默认情况下会在新 SVM 上禁用此功能。

如果 SMB 服务器位于 Active Directory（AD）域中，则可以从 ONTAP 9.1 开始启用 SMB 2.0 以连接到域控制器（DC）。如果在 DC 上禁用了 SMB 1.0，则必须执行此操作。从 ONTAP 9.2 开始，默认情况下会为 DC 连接启用 SMB 2.0。



条件 `-smb1-enabled-for-dc-connections` 设置为 `false` 同时 `-smb1-enabled` 设置为 `true`，ONTAP 拒绝将 SMB 1.0 连接作为客户端，但继续接受入站 SMB 1.0 连接作为服务器。

"SMB 管理" 包含有关支持的 SMB 版本和功能的详细信息。

### 步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 验证启用了哪些 SMB 版本：

```
vservers cifs options show
```

您可以向下滚动列表以查看为客户端连接启用的 SMB 版本，如果要在 AD 域中配置 SMB 服务器，则可以查看为 AD 域连接启用的 SMB 版本。

3. 根据需要为客户端连接启用或禁用 SMB 协议：

- 启用SMB版本：

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- 禁用SMB版本：

```
vserver cifs options modify -vserver vserver_name smb_version false
```

的可能值 smb\_version：

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

以下命令将在SVM vs1.example.com上启用SMB 3.1：

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. 如果 SMB 服务器位于 Active Directory 域中，请根据需要为 DC 连接启用或禁用 SMB 协议：

- 启用SMB版本：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- 禁用SMB版本：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. 返回到管理权限级别：

```
set -privilege admin
```

## 在 DNS 服务器上映射 SMB 服务器

您站点的 DNS 服务器必须具有一个条目，用于将 SMB 服务器名称和任何 NetBIOS 别名



指向数据 LIF 的 IP 地址，以便 Windows 用户可以将驱动器映射到 SMB 服务器名称。

#### 开始之前

您必须对站点的 DNS 服务器具有管理访问权限。如果您没有管理访问权限，则必须要求 DNS 管理员执行此任务。

#### 关于此任务

如果您对 SMB 服务器名称使用 NetBIOS 别名，则最好为每个别名创建 DNS 服务器入口点。

#### 步骤

1. 登录到 DNS 服务器。
2. 创建正向（A - 地址记录）和反向（PTR - 指针记录）查找条目，将 SMB 服务器名称映射到数据 LIF 的 IP 地址。
3. 如果使用 NetBIOS 别名，请创建一个别名规范名称（CNAME 资源记录）查找条目，以便将每个别名映射到 SMB 服务器的数据 LIF 的 IP 地址。

#### 结果

映射在网络中传播之后，Windows 用户可以将驱动器映射到 SMB 服务器名称或其 NetBIOS 别名。

## 配置 SMB 客户端对共享存储的访问

### 配置 SMB 客户端对共享存储的访问

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、请问题描述 `volume create` 命令 `-analytics-state` 或 `-activity-tracking-state` 设置为 `on`。

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](#)。

## 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 qtree

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 vserver_name { -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 vserver_name { -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 **SMB** 共享的要求和注意事项

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 (`~`) 。

"SMB管理" 和 `vserver cifs share` 手册页包含追加信息。

## 创建 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::> vsriver cifs share create -vsriver vs1.example.com -share-name
SHARE1 -path /users

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

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

验证 **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 **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 <b>ACL</b> ， 请使用 ...	输入命令 ...
Windows 用户	<code>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</code>
Windows 组	<code>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</code>

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

cluster1::> vserver 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::> 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 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	<div>a. 单击 * 添加 *。</div> <div>此时将打开选择用户，计算机，服务帐户或组窗口。</div> <div>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。</div> <div>c. 单击 * 确定 *。</div>
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 \*。

## 验证用户访问

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 © 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。