SMB/CIFS 配置

System Manager Classic

NetApp
April 09, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-sm-classic/smb-config/index.html on April 09, 2024. Always check docs.netapp.com for the latest.

目录

SMB/CIFS 配置 1
SMB/CIFS 配置概述 1
SMB/CIFS 配置工作流 1
创建启用了 CIFS 的新 SVM 3
配置对现有 SVM 的 SMB/CIFS 访问 9
将 CIFS 卷添加到启用了 CIFS 的 SVM 12

SMB/CIFS 配置

SMB/CIFS 配置概述

使用 ONTAP System Manager 经典界面（ONTAP 9.7 及更早版本），您可以在新的或现有的 Storage Virtual Machine （SVM）上快速设置对新卷的 SMB/CIFS 访问。

如果要按以下方式配置对卷的访问，请使用此操作步骤：

- 您希望使用最佳实践，而不是浏览每个可用选项。
- 您的数据网络使用默认 IP 空间，默认广播域和默认故障转移组。

  如果您的数据网络正常运行，则使用这些默认对象可确保在链路出现故障时 LIF 能够正确地进行故障转移。如果您不使用默认对象，则应参考 "网络管理文档" 有关如何配置 LIF 路径故障转移的信息。

- NTFS 文件权限将用于保护新卷的安全。

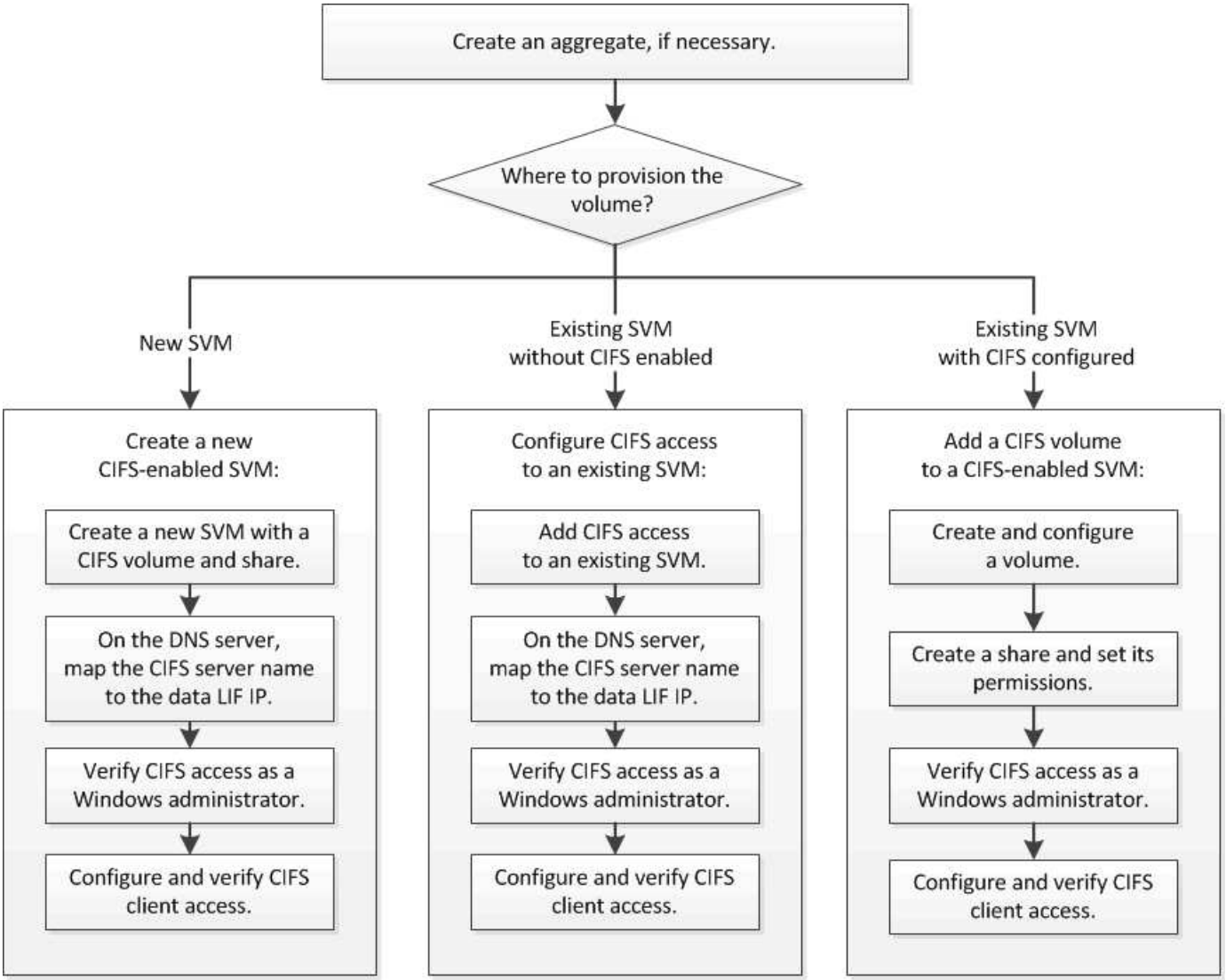
如果您需要有关 ONTAP SMB 协议功能范围的详细信息，请参见 "SMB 参考概述"。

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）	"使用 SMB 为 Windows 服务器配置 NAS 存储"
ONTAP 命令行界面	"使用命令行界面概述 SMB 配置"

SMB/CIFS 配置工作流

配置 SMB/CIFS 需要选择创建聚合，然后选择特定于您的目标的工作流—创建启用了 CIFS 的新 SVM ，配置对现有 SVM 的 CIFS 访问，或者只需将 CIFS 卷添加到已完全配置为可进行 CIFS 访问的现有 SVM 。



创建聚合

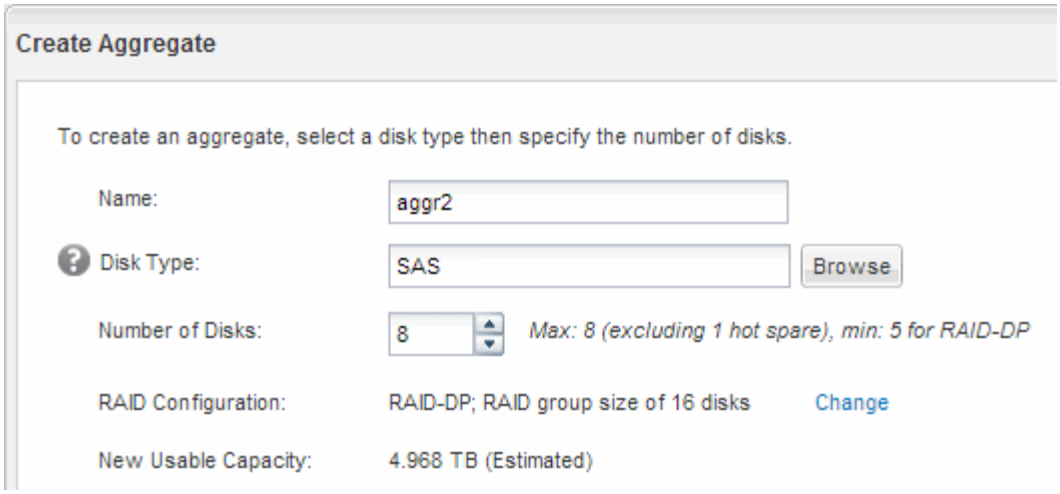
如果不想使用现有聚合，可以创建一个新聚合，以便为要配置的卷提供物理存储。

关于此任务

如果您有要用于新卷的现有聚合，则可以跳过此操作步骤。

步骤

1. 在 Web 浏览器中输入 URL ` https://IP-address-of-cluster-management-LIF` ，然后使用集群管理员凭据登录到 System Manager 。
2. 导航到 * 聚合 * 窗口。
3. 单击 * 创建。 *
4. 按照屏幕上的说明使用默认 RAID-DP 配置创建聚合，然后单击 * 创建 * 。



结果

此时将使用指定的配置创建聚合，并将其添加到聚合窗口的聚合列表中。

确定在何处配置新卷

在创建新的 CIFS 卷之前，您必须确定是否将其放置在现有 Storage Virtual Machine （SVM）中，如果是，还必须确定 SVM 所需的配置。此决定将决定您的工作流。

操作步骤

- 如果要在新的 SVM 上配置卷，请创建一个启用了 CIFS 的新 SVM 。

  "创建启用了 CIFS 的新 SVM"

  如果现有 SVM 未启用 CIFS ，则必须选择此选项。

- 如果要在已启用但未配置 CIFS 的现有 SVM 上配置卷，请在现有 SVM 上配置 CIFS/SMB 访问。

  "在现有 SVM 上配置 CIFS/SMB 访问"

  如果您使用操作步骤创建 SVM 以进行 SAN 访问，则应选择此选项。

- 如果要在已完全配置为可进行 CIFS 访问的现有 SVM 上配置卷，请将 CIFS 卷添加到已启用 CIFS 的 SVM 中。

  "将 CIFS 卷添加到启用了 CIFS 的 SVM"

创建启用了 CIFS 的新 SVM

设置启用了 CIFS 的新 SVM 涉及使用 CIFS 卷和共享创建新 SVM ，在 DNS 服务器上添加映射以及从 Windows 管理主机验证 CIFS 访问。然后，您可以配置 CIFS 客户端访问。

使用 **CIFS** 卷和共享创建新的 **SVM**

您可以使用向导来指导您完成创建新 Storage Virtual Machine （ SVM ），配置域名系统（ DNS ），创建数据逻辑接口（ LIF ），配置 CIFS 服务器以及创建和共享卷的过程。

开始之前

- 您必须配置网络，并且必须将相关物理端口连接到网络。
- 您必须了解 SVM 将使用以下哪些网络组件：
  - 要创建数据逻辑接口（ LIF ）的节点以及该节点上的特定端口
  - 要从中配置数据 LIF IP 地址的子网，或者您也可以选择要分配给数据 LIF 的特定 IP 地址
  - 此 SVM 将加入的 Active Directory （ AD ）域，以及向其中添加 SVM 所需的凭据
- 子网必须可路由到网络信息服务（ NIS ），轻型目录访问协议（ LDAP ）， Active Directory （ AD ）和 DNS 等服务所需的所有外部服务器。
- 必须正确配置任何外部防火墙，才能访问网络服务。
- AD 域控制器，客户端和 SVM 上的时间必须在五分钟内彼此同步。

步骤

1. 导航到 * SVM* 窗口。
2. 单击 * 创建。 *
3. 在 * Storage Virtual Machine （ SVM） Setup* 对话框中，创建 SVM：

   a. 指定 SVM 的唯一名称。

      此名称必须是完全限定域名（ FQDN ），或者遵循其他约定，以确保名称在集群中是唯一的。

   b. 选择您拥有许可证且最终将在 SVM 上使用的所有协议，即使您不想立即配置所有协议也是如此。

      如果最终需要 NFS 访问，则必须立即选择 * NFS *，以便 CIFS 和 NFS 客户端可以共享相同的数据 LIF 。

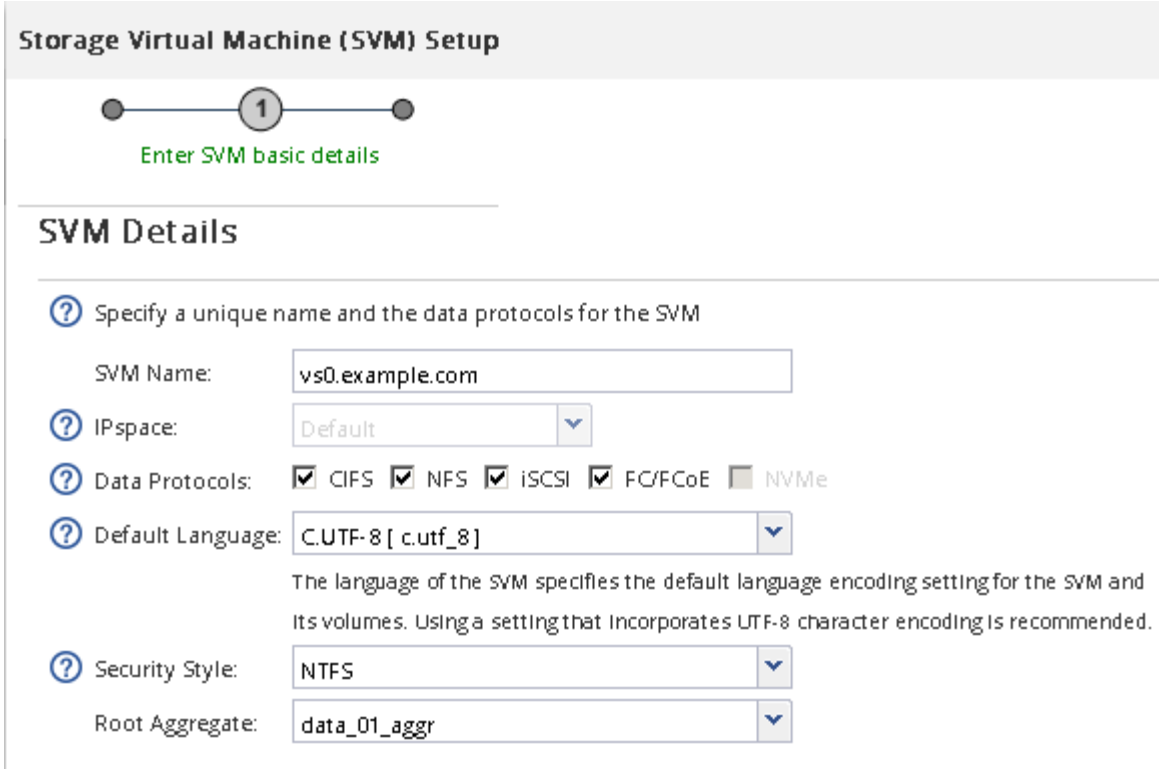
   c. 保留默认语言设置 C.UTF-8 。

      > 如果您支持在 NFS 和 SMB/CIFS 客户端中显示国际字符，请考虑使用 * UTF8MB4* 语言代码，该代码从 ONTAP 9.5 开始提供。

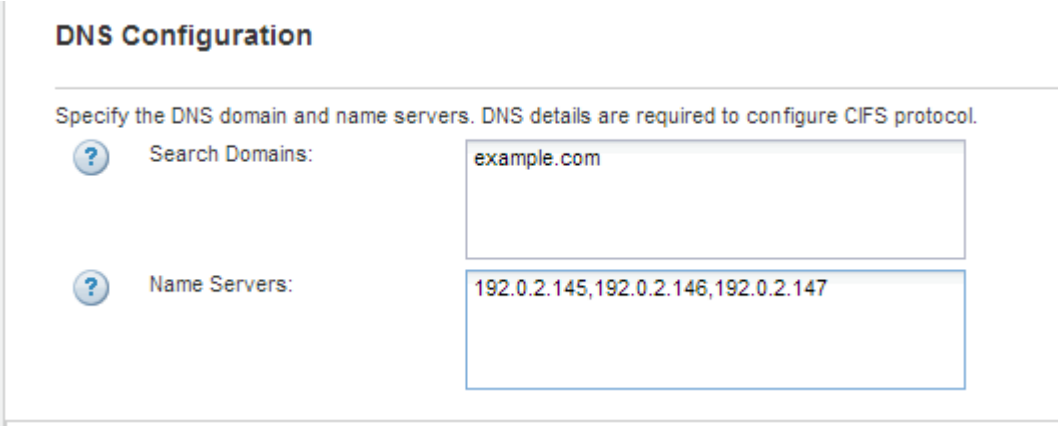
      此语言将由您稍后创建的卷继承，并且无法更改卷的语言。

   d. 可选：选择要包含SVM根卷的根聚合。

      为根卷选择的聚合不会确定数据卷的位置。在稍后配置存储时，系统会自动选择数据卷的聚合。



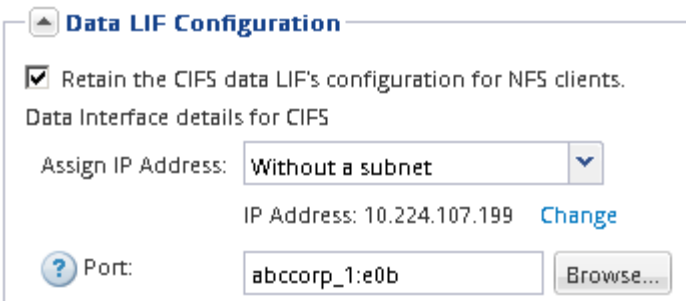
e. 可选：在* DNS配置*区域中、确保默认DNS搜索域和名称服务器是要用于此SVM的域和名称服务器。



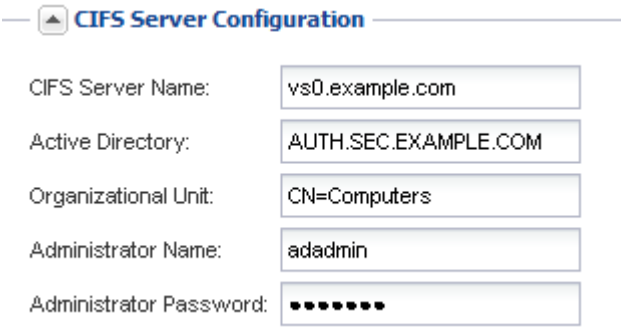
f. 单击 * 提交并继续 * 。

此时将创建 SVM ，但尚未配置协议。

4. 在 * 配置 CIFS/NFS 协议 * 页面的 * 数据 LIF 配置 * 部分中，指定客户端用于访问数据的 LIF 的详细信息：
   a. 从您指定的子网自动为 LIF 分配 IP 地址，或者手动输入地址。
   b. 单击 * 浏览 * 并选择要与 LIF 关联的节点和端口。



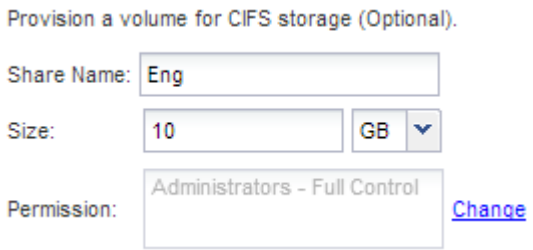
5. 在 * CIFS 服务器配置 * 部分中，定义 CIFS 服务器并将其配置为访问 AD 域：
   a. 为 CIFS 服务器指定在 AD 域中唯一的名称。
   b. 指定 CIFS 服务器可以加入的 AD 域的 FQDN 。
   c. 如果要关联 AD 域中的组织单位（ OU ），而不是 CN=Computers ，请输入 OU 。
   d. 指定具有足够权限将 CIFS 服务器添加到 OU 的管理帐户的名称和密码。
   e. 如果要避免对此 SVM 上的所有共享进行未经授权的访问，请选择使用 SMB 3.0 加密数据的选项。



6. 创建用于 CIFS/SMB 访问的卷并在其上配置共享：
   a. 命名 CIFS/SMB 客户端将用于访问卷的共享。

      您为共享输入的名称也将用作卷名称。

   b. 指定卷的大小。



   您无需为卷指定聚合，因为它会自动位于可用空间最多的聚合上。

7. 可选：通过修改共享ACL限制对共享的访问：
   a. 在 * 权限 * 字段中，单击 * 更改 * 。
   b. 选择 Everyone 组，然后单击 * 删除 * 。

c. 可选：单击*添加*、然后输入包含SVM的Windows Active Directory域中定义的管理员组的名称。
d. 选择新的管理员组，然后选择 * 完全控制 * 。
e. 单击 * 保存并关闭 * 。

8. 单击 * 提交并继续 * 。

   此时将创建以下对象：

   - 以 SVM 命名的数据 LIF ，后缀为 "` cifs_lif1` "
   - 属于 AD 域的 CIFS 服务器
   - 位于可用空间最多的聚合上的卷，其名称与共享名称匹配，并以后缀 "` cifs_volume` " 结尾
   - 卷上的共享

9. 对于显示的所有其他协议配置页面，请单击 * 跳过 * 并稍后配置协议。
10. 显示 * SVM 管理 * 页面时，配置或推迟为此 SVM 配置单独的管理员：
    - 单击 * 跳过 * ，然后根据需要稍后配置管理员。
    - 输入请求的信息，然后单击 * 提交并继续 * 。
11. 查看 * 摘要 * 页面，记下稍后可能需要的任何信息，然后单击 * 确定 * 。

    DNS 管理员需要知道 CIFS 服务器名称和数据 LIF 的 IP 地址。Windows 客户端需要知道 CIFS 服务器和共享的名称。

结果

此时将创建一个新的 SVM ，其中 CIFS 服务器包含一个共享的新卷。

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。

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 且共享名为 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 。

配置并验证 **CIFS** 客户端访问

准备好后，您可以通过在 Windows 资源管理器中设置 NTFS 文件权限并在 System Manager 中修改共享 ACL ，为选定客户端授予对共享的访问权限。然后，您应测试受影响的用户或组是否可以访问此卷。

步骤

1. 确定要为哪些客户端和用户或组授予对共享的访问权限。
2. 在 Windows 客户端上，使用管理员角色为用户或组授予对文件和文件夹的权限。
   a. 以具有足够管理权限的管理员身份登录到 Windows 客户端，以管理 NTFS 权限。
   b. 在 Windows 资源管理器中，右键单击驱动器，然后选择 * 属性 * 。
   c. 选择 * 安全性 * 选项卡，然后根据需要调整组和用户的安全设置。
3. 在 System Manager 中，修改共享 ACL 以授予 Windows 用户或组对共享的访问权限。
   a. 导航到 * 共享 * 窗口。
   b. 选择共享，然后单击 * 编辑 * 。
   c. 选择 * 权限 * 选项卡，并为用户或组授予对共享的访问权限。
4. 在 Windows 客户端上，以现在有权访问共享和文件的用户之一身份登录，并验证您是否可以访问共享并创建文件。

配置对现有 SVM 的 SMB/CIFS 访问

为 SMB/CIFS 客户端添加对现有 SVM 的访问权限涉及到向 SVM 添加 CIFS 配置，在 DNS 服务器上添加映射以及从 Windows 管理主机验证 CIFS 访问。然后，您可以配置 CIFS 客户端访问。

添加对现有 SVM 的 CIFS 访问

为现有 SVM 添加 CIFS/SMB 访问权限涉及创建数据 LIF ，配置 CIFS 服务器，配置卷，共享卷以及配置共享权限。

开始之前

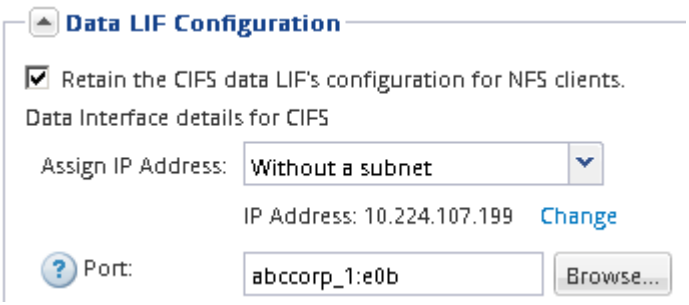
- 您必须了解 SVM 将使用以下哪些网络组件：
  - 要创建数据逻辑接口（ LIF ）的节点以及该节点上的特定端口
  - 要从中配置数据 LIF IP 地址的子网，或者您也可以选择要分配给数据 LIF 的特定 IP 地址
  - 此 SVM 要加入的 Active Directory （ AD ）域，以及向其中添加 SVM 所需的凭据
- 必须正确配置任何外部防火墙，才能访问网络服务。
- SVM 上必须允许使用 CIFS 协议。

  如果您未按照操作步骤创建 SVM 来配置 SAN 协议，则会出现这种情况。

步骤

1. 导航到可配置 SVM 协议的区域：
   a. 选择要配置的 SVM 。
   b. 在 * 详细信息 * 窗格中，单击 * 协议 * 旁边的 * CIFS* 。

2. 在 * 配置 CIFS 协议 * 对话框的 * 数据 LIF 配置 * 部分中，为 SVM 创建数据 LIF ：
   a. 从您指定的子网自动为 LIF 分配 IP 地址，或者手动输入地址。
   b. 单击 * 浏览 * 并选择要与 LIF 关联的节点和端口。

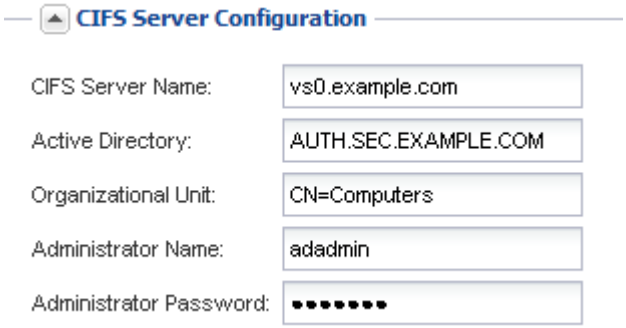
3. 在 * CIFS 服务器配置 * 部分中，定义 CIFS 服务器并将其配置为访问 AD 域：
   a. 为 CIFS 服务器指定在 AD 域中唯一的名称。

b. 指定 CIFS 服务器可以加入的 AD 域的 FQDN 。

c. 如果要关联 AD 域中的组织单位（ OU ），而不是 CN=Computers ，请输入 OU 。

d. 指定具有足够权限将 CIFS 服务器添加到 OU 的管理帐户的名称和密码。

e. 如果要避免对此 SVM 上的所有共享进行未经授权的访问，请选择使用 SMB 3.0 加密数据的选项。

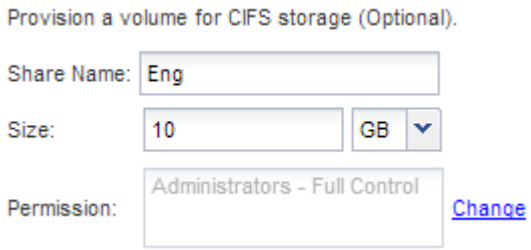


4. 创建用于 CIFS/SMB 访问的卷并在其上配置共享：

   a. 命名 CIFS/SMB 客户端将用于访问卷的共享。

      您为共享输入的名称也将用作卷名称。

   b. 指定卷的大小。



   您无需为卷指定聚合，因为它会自动位于可用空间最多的聚合上。

5. 可选：通过修改共享ACL限制对共享的访问：

   a. 在 * 权限 * 字段中，单击 * 更改 * 。

   b. 选择 Everyone 组，然后单击 * 删除 * 。

   c. 可选：单击*添加*、然后输入包含SVM的Windows Active Directory域中定义的管理员组的名称。

   d. 选择新的管理员组，然后选择 * 完全控制 * 。

   e. 单击 * 保存并关闭 * 。

6. 单击 * 提交并关闭 * ，然后单击 * 确定 * 。

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。

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 且共享名为 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 。

配置并验证 CIFS 客户端访问

准备好后，您可以通过在 Windows 资源管理器中设置 NTFS 文件权限并在 System Manager 中修改共享 ACL ，为选定客户端授予对共享的访问权限。然后，您应测试受影响的用户或组是否可以访问此卷。

步骤

1. 确定要为哪些客户端和用户或组授予对共享的访问权限。

2. 在 Windows 客户端上，使用管理员角色为用户或组授予对文件和文件夹的权限。
   a. 以具有足够管理权限的管理员身份登录到 Windows 客户端，以管理 NTFS 权限。
   b. 在 Windows 资源管理器中，右键单击驱动器，然后选择 * 属性 * 。
   c. 选择 * 安全性 * 选项卡，然后根据需要调整组和用户的安全设置。
3. 在 System Manager 中，修改共享 ACL 以授予 Windows 用户或组对共享的访问权限。
   a. 导航到 * 共享 * 窗口。
   b. 选择共享，然后单击 * 编辑 * 。
   c. 选择 * 权限 * 选项卡，并为用户或组授予对共享的访问权限。
4. 在 Windows 客户端上，以现在有权访问共享和文件的用户之一身份登录，并验证您是否可以访问共享并创建文件。

将 CIFS 卷添加到启用了 CIFS 的 SVM

将 CIFS 卷添加到启用了 CIFS 的 SVM 涉及创建和配置卷，创建共享并设置其权限以及从 Windows 管理主机验证访问。然后，您可以配置 CIFS 客户端访问。

开始之前

必须在 SVM 上完全设置 CIFS 。

创建并配置卷

您必须创建一个 FlexVol 卷以包含数据。您可以选择更改卷的默认安全模式，此模式是从根卷的安全模式继承的。您也可以选择更改卷在命名空间中的默认位置，即 Storage Virtual Machine （ SVM ）的根卷。

步骤

1. 导航到 * 卷 * 窗口。
2. 单击 * 创建 * > * 创建 FlexVol * 。

   此时将显示创建卷对话框。

3. 如果要更改以日期和时间戳结尾的默认名称，请指定一个新名称，例如 `vol1` 。
4. 为卷选择一个聚合。
5. 指定卷的大小。
6. 单击 * 创建 * 。

   默认情况下，在 System Manager 中创建的任何新卷都会使用卷名称作为接合名称挂载到根卷上。在配置 CIFS 共享时，您可以使用接合路径和接合名称。

7. 可选：如果不希望卷位于SVM的根目录、请修改新卷在现有命名空间中的位置：
   a. 导航到 * 命名空间 * 窗口。

b. 从下拉菜单中选择 * SVM* 。

c. 单击 * 挂载 * 。

d. 在 * 挂载卷 * 对话框中，指定卷，其接合路径的名称以及要挂载卷的接合路径。

e. 在 * 命名空间 * 窗口中验证新的接合路径。

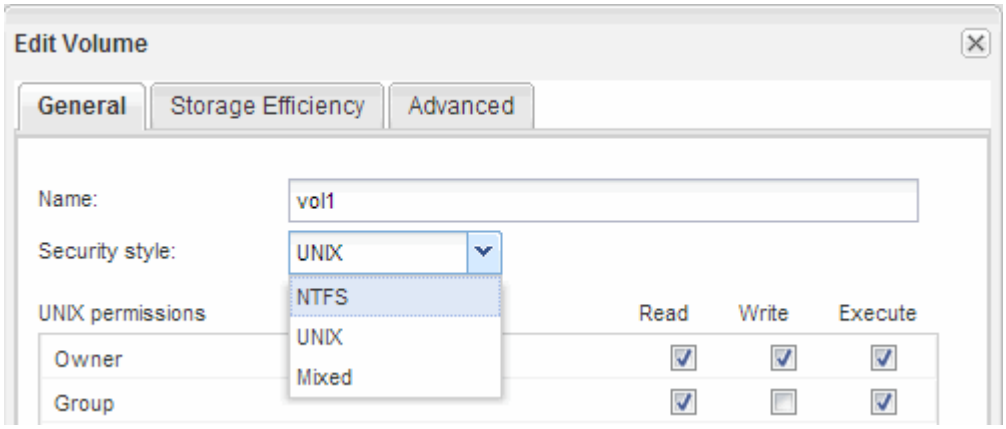
如果要将某些卷组织在名为 `data` 的主卷下，可以将新卷 "`vol1` " 从根卷移动到 " `data` " 卷。

8. 查看卷的安全模式，并根据需要进行更改：

a. 在 * 卷 * 窗口中，选择刚刚创建的卷，然后单击 * 编辑 * 。

此时将显示编辑卷对话框，其中显示了卷的当前安全模式，此安全模式是从 SVM 根卷的安全模式继承的。

b. 确保安全模式为 NTFS 。



创建共享并设置其权限

在 Windows 用户访问卷之前，您必须在卷上创建 CIFS 共享，并通过修改共享的访问控制列表（ACL ）来限制对共享的访问。

关于此任务

出于测试目的，您应仅允许管理员访问。稍后，在确认卷可访问之后，您可以允许访问更多客户端。

步骤

1. 导航到 * 共享 * 窗口。

2. 创建共享，以便 SMB 客户端可以访问此卷：

a. 单击 * 创建共享 * 。

b. 在 * 创建共享 * 对话框中，单击 * 浏览 * ，展开命名空间层次结构，然后选择先前创建的卷。

c. 可选：如果希望共享名称与卷名称不同、请更改共享名称。

d. 单击 * 创建 * 。

创建共享时， Everyone 组的默认 ACL 设置为 Full Control 。

3. 可选：通过修改共享ACL限制对共享的访问：

a. 选择共享，然后单击 * 编辑 * 。
b. 在 * 权限 * 选项卡中，选择 * 任何人 * 组，然后单击 * 删除 * 。
c. 单击 * 添加 * ，然后输入在包含 SVM 的 Windows Active Directory 域中定义的管理员组的名称。
d. 选择新管理员组后，为其选择所有权限。
e. 单击 * 保存并关闭 * 。

更新后的共享访问权限将列在 " 共享访问控制 " 窗格中。

下一步操作

您应以 Windows 管理员身份验证访问权限。

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 且共享名为 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 。

配置并验证 CIFS 客户端访问

准备好后，您可以通过在 Windows 资源管理器中设置 NTFS 文件权限并在 System Manager 中修改共享 ACL ，为选定客户端授予对共享的访问权限。然后，您应测试受影响的用户或组是否可以访问此卷。

步骤

1. 确定要为哪些客户端和用户或组授予对共享的访问权限。
2. 在 Windows 客户端上，使用管理员角色为用户或组授予对文件和文件夹的权限。

   a. 以具有足够管理权限的管理员身份登录到 Windows 客户端，以管理 NTFS 权限。
   b. 在 Windows 资源管理器中，右键单击驱动器，然后选择 * 属性 * 。

   c. 选择 * 安全性 * 选项卡，然后根据需要调整组和用户的安全设置。

3. 在 System Manager 中，修改共享 ACL 以授予 Windows 用户或组对共享的访问权限。
   a. 导航到 * 共享 * 窗口。
   b. 选择共享，然后单击 * 编辑 * 。
   c. 选择 * 权限 * 选项卡，并为用户或组授予对共享的访问权限。
4. 在 Windows 客户端上，以现在有权访问共享和文件的用户之一身份登录，并验证您是否可以访问共享并创建文件。

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。