SMB/CIFS 和 NFS 多协议配置

System Manager Classic

NetApp
June 22, 2024

目录

SMB/CIFS 和 NFS 多协议配置

SMB 和 NFS 多协议配置概述

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 和 NFS 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：

- NFS 访问将通过 NFSv3 进行，而不是通过 NFSv4 或 NFSv4.1 进行。
- 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，应参见 "网络管理" 有关如何配置 LIF 路径故障转移的信息。

- LDAP （如果使用）由 Active Directory 提供。

如果您需要有关 ONTAP NFS 和 SMB 协议功能范围的详细信息，请参见以下文档：

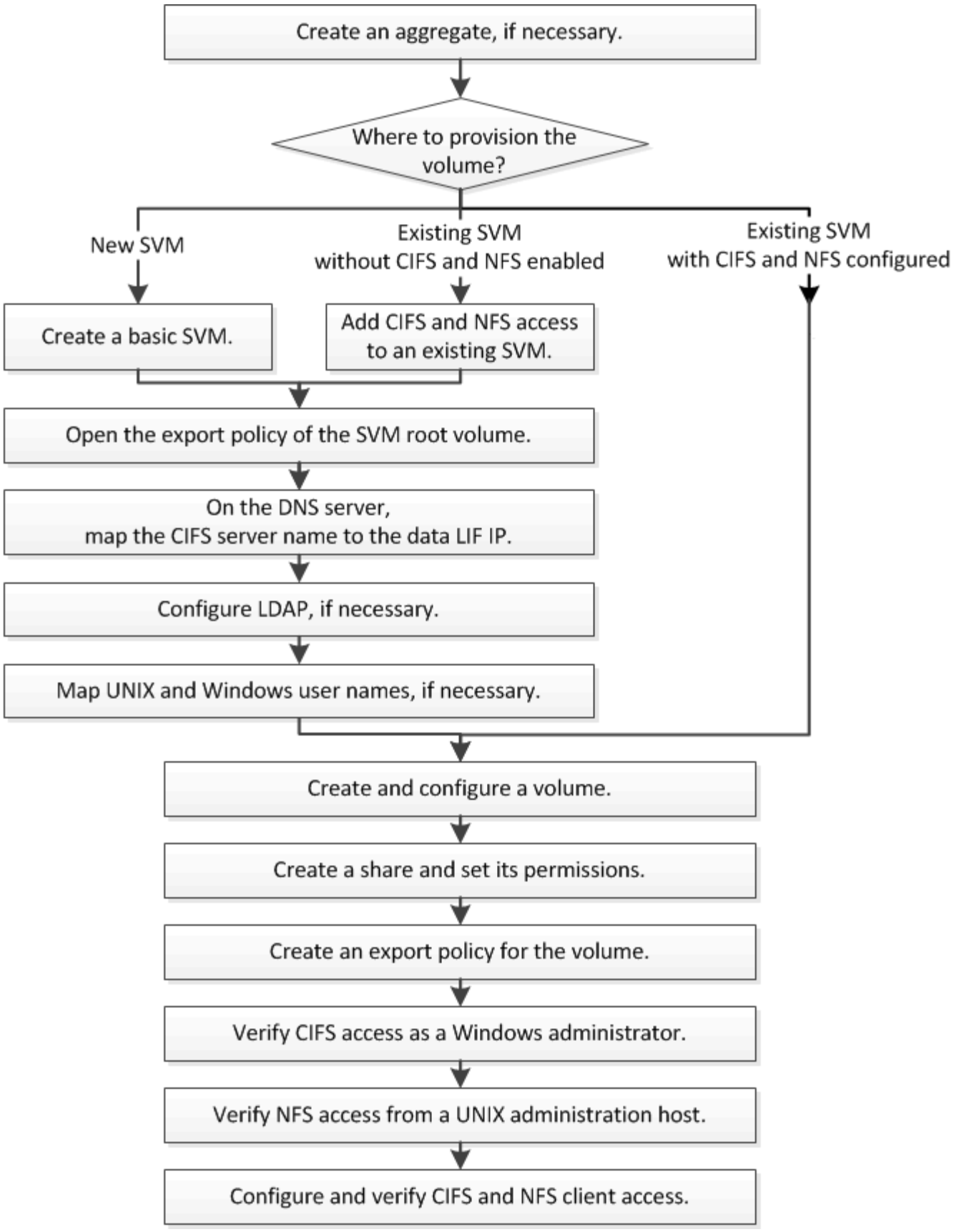
- "NFS 管理"
- "SMB管理"

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 NFS 和 SMB 为 Windows 和 Linux 配置 NAS 存储"
ONTAP 命令行界面	"使用命令行界面概述SMB配置" "使用命令行界面概述 NFS 配置" "安全模式及其影响是什么" "在多协议环境中，文件和目录名称区分大小写"

多协议配置工作流

配置 SMB/CIFS 和 NFS 时，需要选择创建聚合；也可以选择创建新的 SVM 或配置现有 SVM ；创建卷，共享和导出；以及验证从 UNIX 和 Windows 管理主机进行的访问。然后，您可以打开对 SMB/CIFS 和 NFS 客户端的访问。



创建聚合

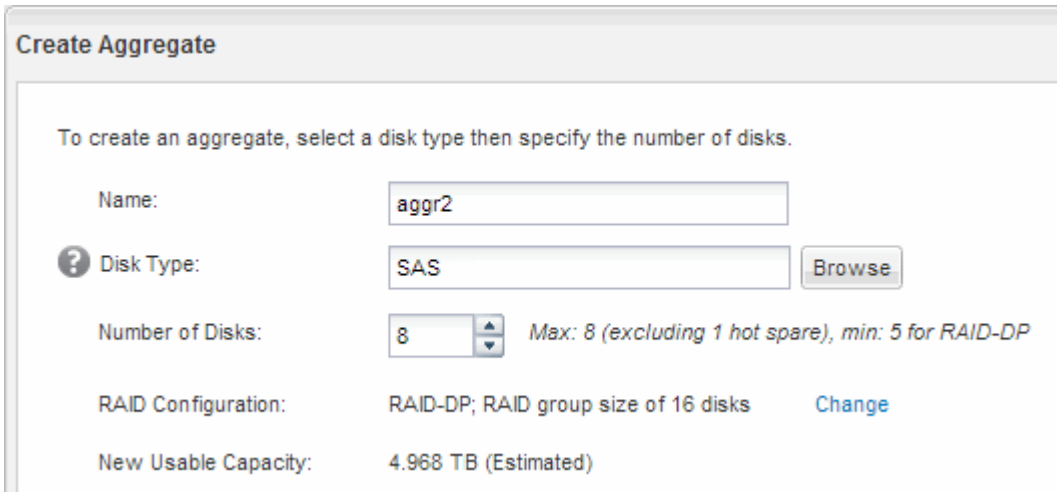
如果不想使用现有聚合，可以创建一个新聚合，以便为要配置的卷提供物理存储。

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. 输入URL `https://IP-address-of-cluster-management-LIF` 并使用您的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

在创建新的多协议卷之前，您必须确定是否将该卷放置在现有 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 SVM 上配置卷，请创建一个基本 SVM 。

  "创建基本 SVM"

  如果现有 SVM 上尚未启用 CIFS 和 NFS ，则必须选择此选项。

- 如果要在已启用 CIFS 和 NFS 但尚未对其进行配置的现有 SVM 上配置卷，请在现有 SVM 上添加 CIFS 和 NFS 访问。

  "在现有 SVM 上添加 CIFS 和 NFS 访问"

- 如果要在已完全配置为可进行 CIFS 和 NFS 多协议访问的现有 SVM 上配置卷，则可以直接创建和配置卷。

  "创建和配置卷"

您可以使用一个向导来指导您完成以下过程：创建新的 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，启用 NFS 以及配置 NIS （可选）。

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
  - NIS 信息，如果您的站点使用 NIS 进行名称服务或名称映射
- 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。

关于此任务

在创建用于多协议访问的 SVM 时，不应使用 Storage Virtual Machine （ SVM ）设置窗口的配置部分，该窗口会创建两个卷，而不是一个具有多协议访问的卷。您可以稍后在工作流中配置卷。

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。
   c. 保留默认语言设置 C.UTF-8 。

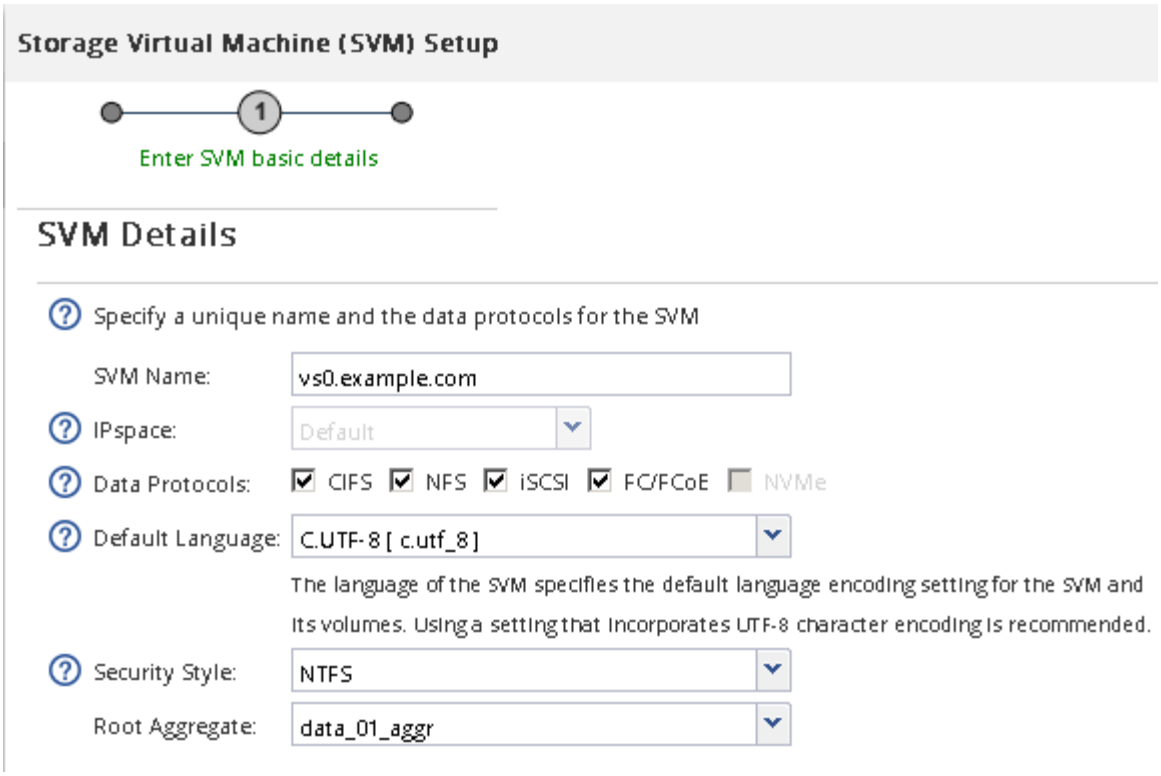
      如果您支持在 NFS 和 SMB/CIFS 客户端中显示国际字符，请考虑使用 * UTF8MB4* 语言代码，该代码从 ONTAP 9.5 开始提供。

   d. 可选：确保将安全模式设置为您的首选项。

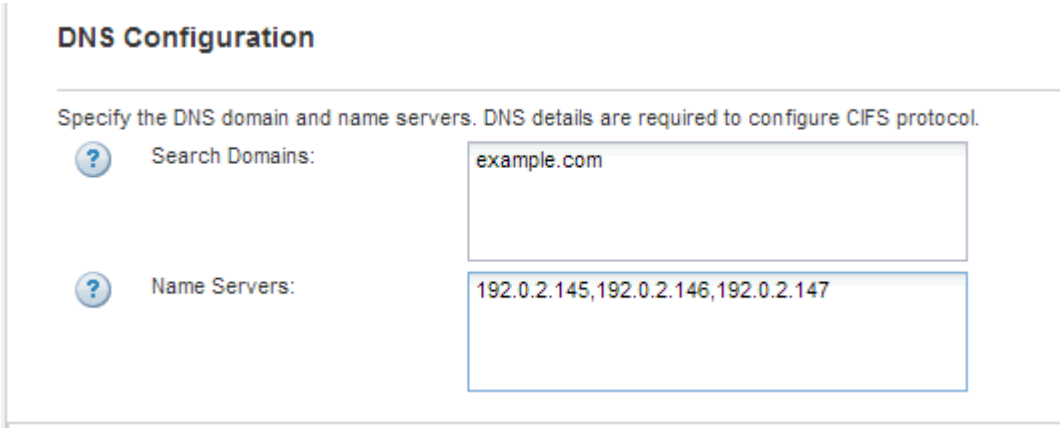
      默认情况下，选择 CIFS 协议会将安全模式设置为 NTFS 。

   e. 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。数据卷的聚合将在后续步骤中单独选择。



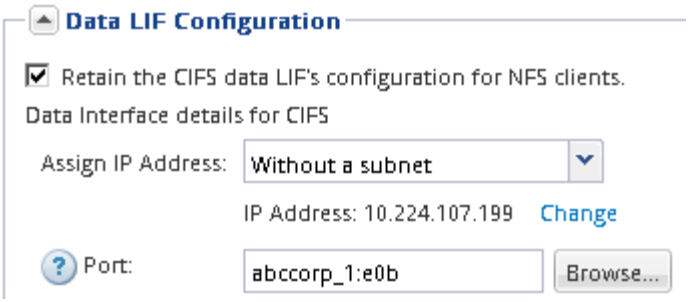
f. 可选：在* DNS配置*区域中、确保默认DNS搜索域和名称服务器是要用于此SVM的域和名称服务器。



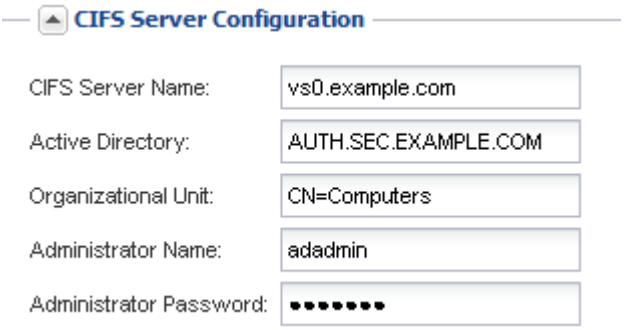
g. 单击 * 提交并继续 * 。

此时将创建 SVM ，但尚未配置协议。

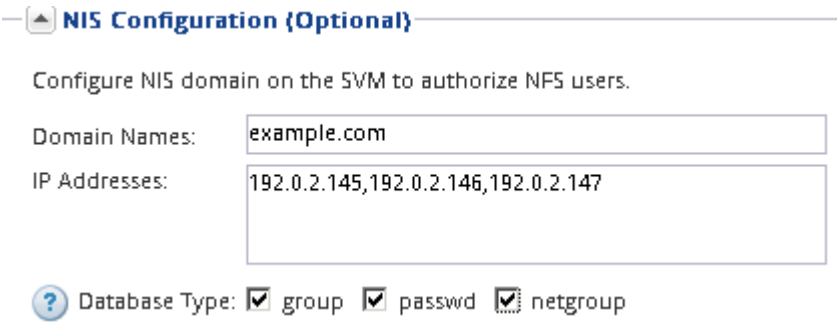
4. 在 * 配置 CIFS/NFS 协议 * 页面的 * 数据 LIF 配置 * 部分中，指定客户端用于访问数据的 LIF 的详细信息：
   a. 从您指定的子网自动为 LIF 分配 IP 地址，或者手动输入地址。
   b. 单击 * 浏览 * 并选择要与 LIF 关联的节点和端口。



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. 跳过 * 为 CIFS 存储配置卷 * 区域，因为它仅为 CIFS 访问配置卷，而不是为多协议访问配置卷。
7. 如果折叠了 * NIS 配置 * 区域，请将其展开。
8. 如果您的站点使用 NIS 进行名称服务或名称映射，请指定 NIS 服务器的域和 IP 地址。



9. 跳过 * 为 NFS 存储配置卷 * 区域，因为它仅为 NFS 访问配置卷，而不是为多协议访问配置卷。
10. 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_nfs_lif1` "
    ◦ 属于 AD 域的 CIFS 服务器

- NFS 服务器

11. 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。
12. 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 * 。
13. 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 服务器的名称。NFS 客户端需要知道数据 LIF 的 IP 地址。

结果

此时将创建一个新的 SVM ，其中包含一个 CIFS 服务器和一个可通过相同数据 LIF 访问的 NFS 服务器。

下一步操作

现在，您必须打开 SVM 根卷的导出策略。

- 相关信息 *

打开 SVM 根卷的导出策略（创建启用了 NFS 的新 SVM ）

添加对现有 **SVM** 的 **CIFS** 和 **NFS** 访问

为现有 SVM 添加 CIFS/SMB 和 NFS 访问权限涉及创建数据 LIF ，配置 CIFS 服务器，启用 NFS 以及配置 NIS （可选）。

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
  - NIS 信息（如果您的站点使用 NIS 进行名称服务或名称映射）
- 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。
- SVM 上必须允许使用 CIFS 和 NFS 协议。

  如果在配置其他协议时未按照此操作步骤创建 SVM ，则会出现这种情况。

关于此任务

配置 CIFS 和 NFS 的顺序会影响显示的对话框。在此操作步骤中，必须先配置 CIFS ，然后再配置 NFS 。

步骤

1. 导航到可配置 SVM 协议的区域：

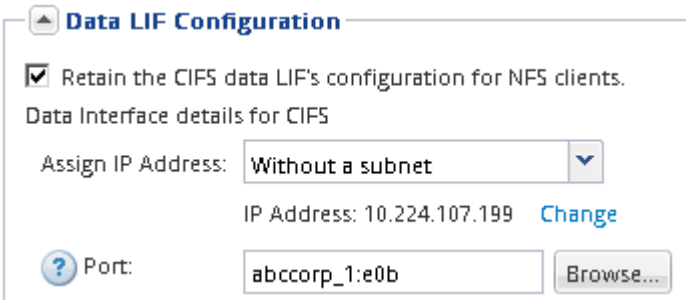
a. 选择要配置的 SVM 。

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：

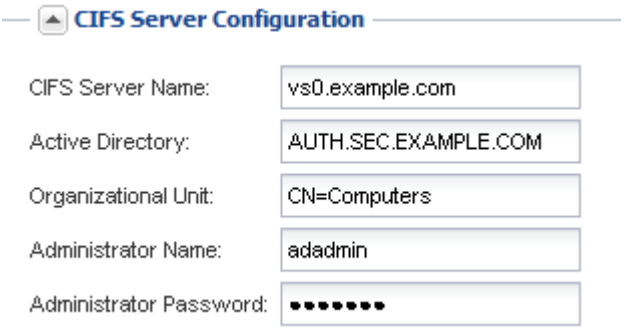
a. 为 CIFS 服务器指定在 AD 域中唯一的名称。

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。

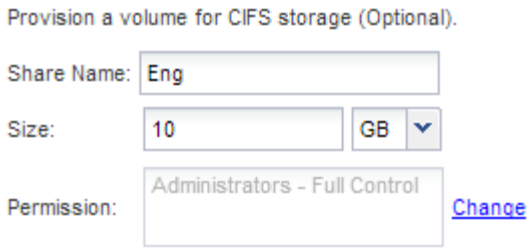


4. 创建用于 CIFS/SMB 访问的卷并在其上配置共享：

a. 命名 CIFS/SMB 客户端将用于访问卷的共享。

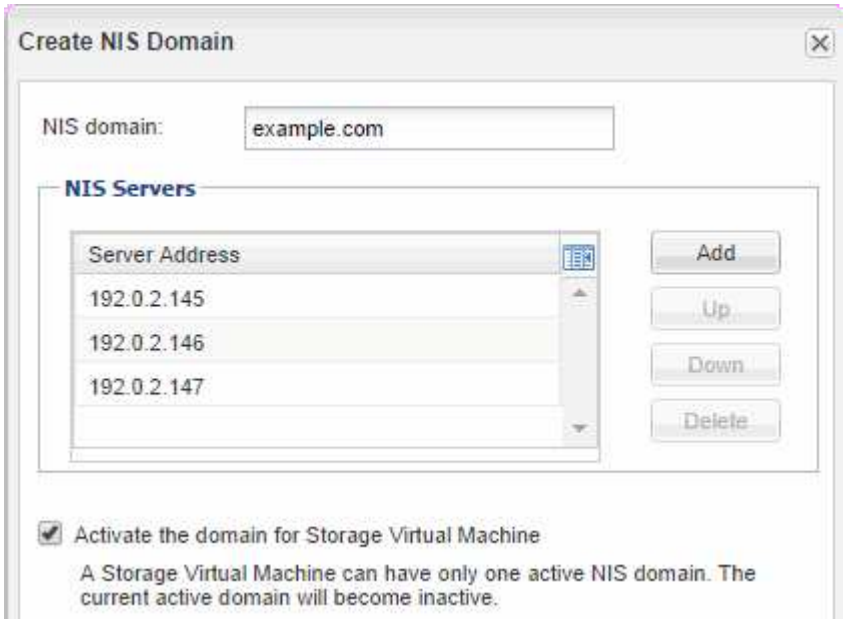
您为共享输入的名称也将用作卷名称。

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. 跳过 * 为 CIFS 存储配置卷 * 区域，因为它仅为 CIFS 访问配置卷，而不是为多协议访问配置卷。
6. 单击 * 提交并关闭 * ，然后单击 * 确定 * 。
7. 启用NFS：
   a. 从 SVM 选项卡中，选择要为其启用 NFS 的 SVM ，然后单击 * 管理 * 。
   b. 在 * 协议 * 窗格中，单击 * NFS * ，然后单击 * 启用 * 。
8. 如果您的站点使用 NIS 进行名称服务或名称映射，请配置 NIS ：
   a. 在 * 服务 * 窗口中，单击 * NIS * 。
   b. 在 * NIS * 窗口中，单击 * 创建 * 。
   c. 指定 NIS 服务器的域。
   d. 添加 NIS 服务器的 IP 地址。
   e. 选择 * 激活 Storage Virtual Machine* 的域，然后单击 * 创建 * 。



下一步操作

打开 SVM 根卷的导出策略。

打开 **SVM** 根卷的导出策略（创建启用了 **NFS** 的新 **SVM** ）

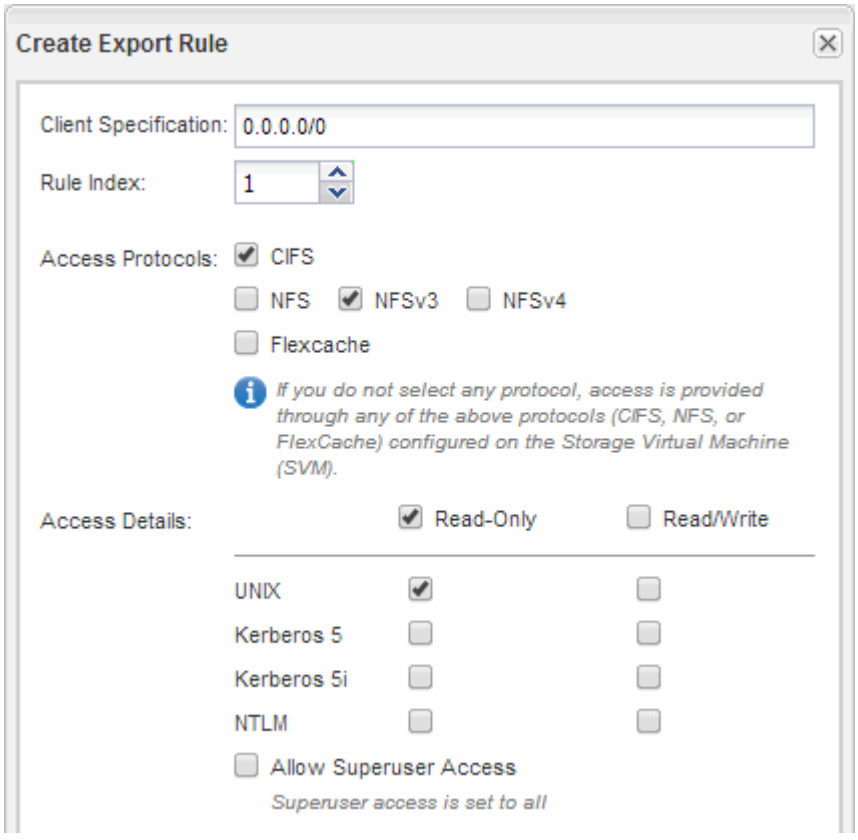
您必须向默认导出策略添加一条规则，以允许所有客户端通过 NFSv3 进行访问。如果没有此规则，则会拒绝所有 NFS 客户端访问 Storage Virtual Machine （ SVM ）及其卷。

关于此任务

您应将所有 NFS 访问指定为默认导出策略，稍后应通过为单个卷创建自定义导出策略来限制对单个卷的访问。

步骤

1. 导航到 * SVM* 窗口。
2. 单击 * SVM 设置 * 选项卡。
3. 在 * 策略 * 窗格中，单击 * 导出策略 * 。
4. 选择名为 * 默认 * 的导出策略，该策略将应用于 SVM 根卷。
5. 在下部窗格中，单击 * 添加 * 。
6. 在 * 创建导出规则 * 对话框中，创建一个规则，以便为 NFS 客户端打开对所有客户端的访问：
   a. 在“客户端规范”字段中，输入 `0.0.0.0/0` 以便规则适用场景所有客户端。
   b. 规则索引的默认值保留为 * 1 * 。
   c. 选择*NFSv3*。
   d. 清除 * 只读 * 下除 * unix* 复选框以外的所有复选框。
   e. 单击 * 确定 * 。



结果

现在， NFSv3 客户端可以访问在 SVM 上创建的任何卷。

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。

配置 **LDAP** （创建启用了 **NFS** 的新 **SVM** ）

如果您希望 Storage Virtual Machine （ SVM ）从基于 Active Directory 的轻型目录访问协议（ LDAP ）中获取用户信息，则必须创建 LDAP 客户端，为 SVM 启用此客户端，并使 LDAP 优先于其他用户信息源。

开始之前

- LDAP 配置必须使用 Active Directory （ AD ）。

  如果您使用其他类型的 LDAP ，则必须使用命令行界面（ CLI ）和其他文档来配置 LDAP 。

  "NetApp 技术报告 4067 ：《 NetApp ONTAP 中的 NFS 》"

  "NetApp 技术报告 4616 ：《采用 Microsoft Active Directory 的 ONTAP 中的 NFS Kerberos 》"

  "NetApp 技术报告 4835 ：《如何在 ONTAP 中配置 LDAP 》"

- 您必须了解 AD 域和服务器以及以下绑定信息：身份验证级别，绑定用户和密码，基础 DN 和 LDAP 端口。

步骤

1. 导航到 * SVM* 窗口。
2. 选择所需的 SVM
3. 单击 * SVM 设置 * 选项卡。

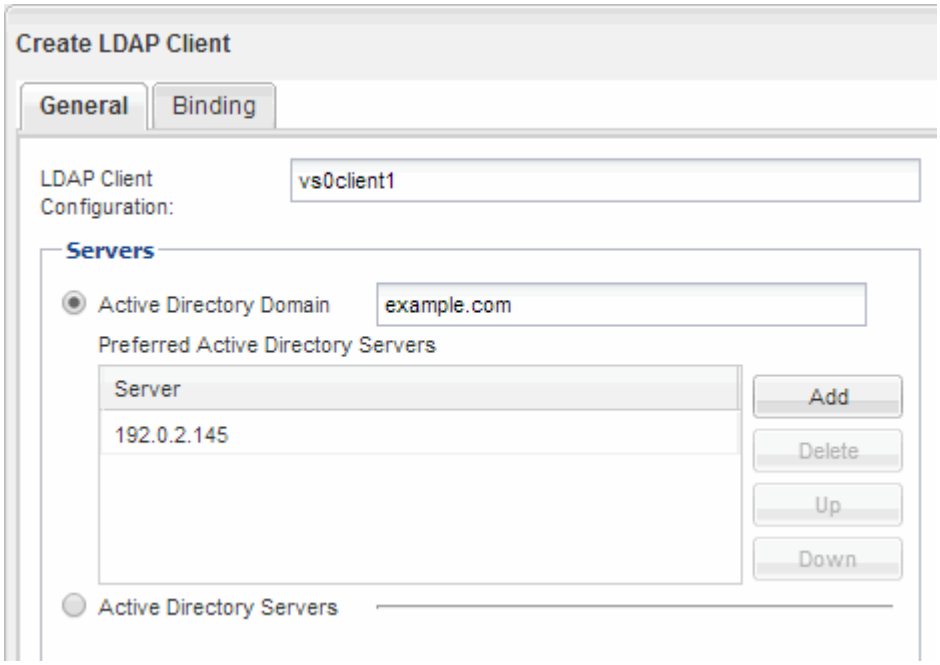
4. 设置 LDAP 客户端以供 SVM 使用：

   a. 在 * 服务 * 窗格中，单击 * LDAP 客户端 * 。

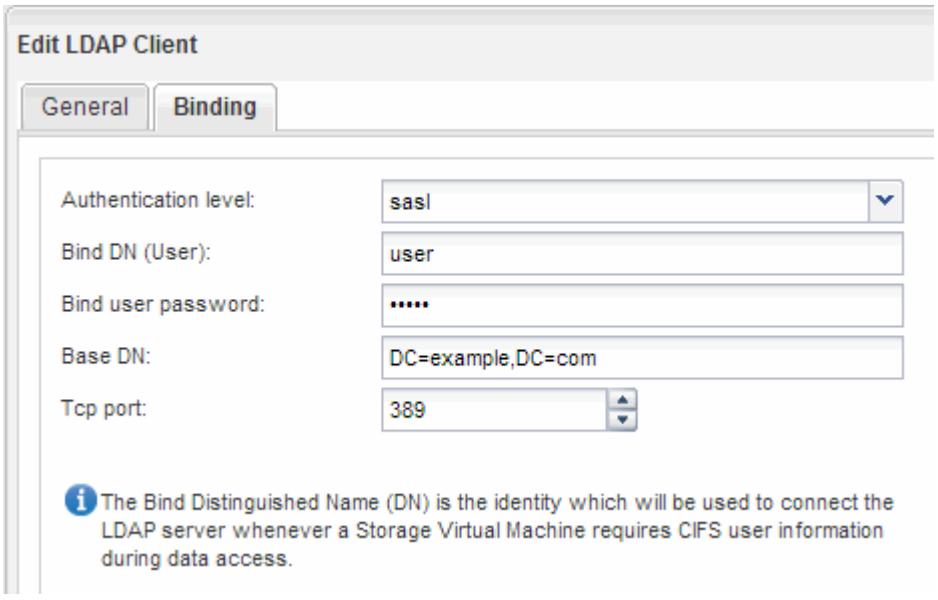
   b. 在 * LDAP 客户端配置 * 窗口中，单击 * 添加 * 。

   c. 在*Create LDAP Client*窗口的*General选项卡中，键入LDAP客户端配置的名称，例如 `vs0client1`。

   d. 添加 AD 域或 AD 服务器。



   e. 单击 * 绑定 * ，然后指定身份验证级别，绑定用户和密码，基本 DN 和端口。

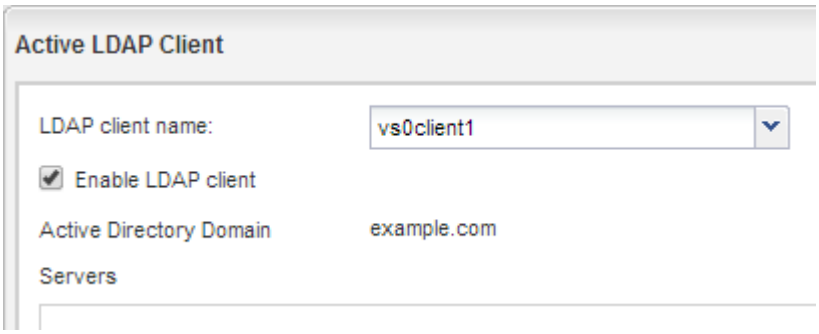


   f. 单击 * 保存并关闭 * 。

此时将创建一个新客户端，并可供 SVM 使用。

5. 为 SVM 启用新的 LDAP 客户端：

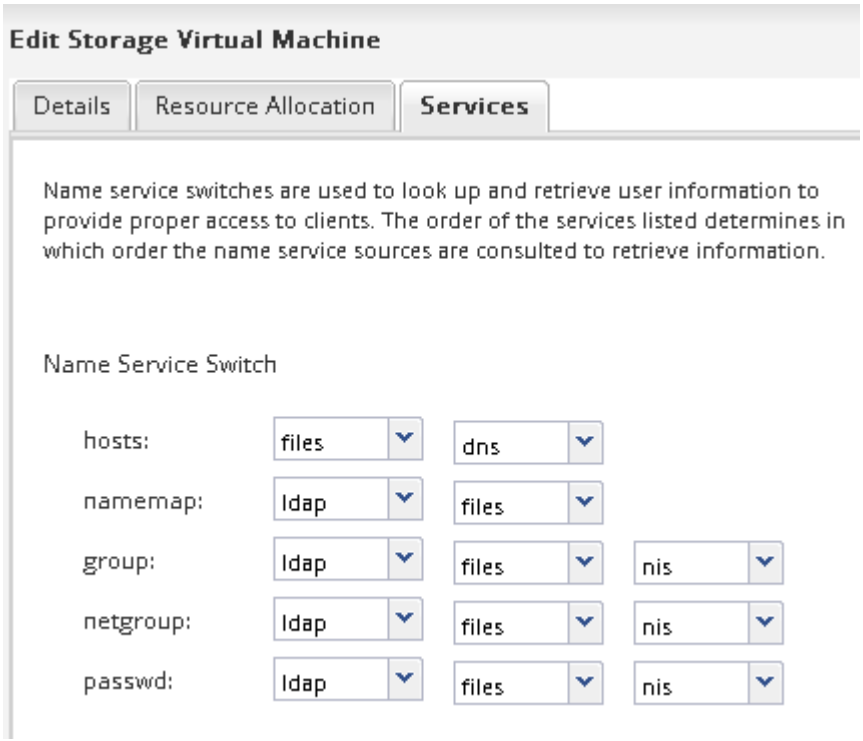
a. 在导航窗格中，单击 * LDAP 配置 * 。
b. 单击 * 编辑 * 。
c. 确保在 * LDAP 客户端名称 * 中选择了刚刚创建的客户端。
d. 选择 * 启用 LDAP 客户端 * ，然后单击 * 确定 * 。



SVM 使用新的 LDAP 客户端。

6. 使 LDAP 优先于其他用户信息源，例如网络信息服务（ NIS ）以及本地用户和组：

a. 导航到 * SVM* 窗口。
b. 选择 SVM 并单击 * 编辑 * 。
c. 单击 * 服务 * 选项卡。
d. 在 * 名称服务开关 * 下，指定 * LDAP * 作为数据库类型的首选名称服务开关源。
e. 单击 * 保存并关闭 * 。



LDAP 是此 SVM 上名称服务和名称映射的主要用户信息来源。

映射 **UNIX** 和 **Windows** 用户名

如果您的站点同时具有 Windows 和 UNIX 用户帐户，则应使用名称映射来确保 Windows 用户可以访问具有 UNIX 文件权限的文件，并确保 UNIX 用户可以访问具有 NTFS 文件权限的文件。名称映射可能涉及隐式映射，转换规则和默认用户的任意组合。

关于此任务

只有当您的站点具有不隐式映射的 Windows 和 UNIX 用户帐户时，即每个 Windows 用户名的小写版本与 UNIX 用户名匹配时，才应使用此操作步骤。可以使用 NIS ， LDAP 或本地用户来执行此操作。如果两组用户不匹配，则应配置名称映射。

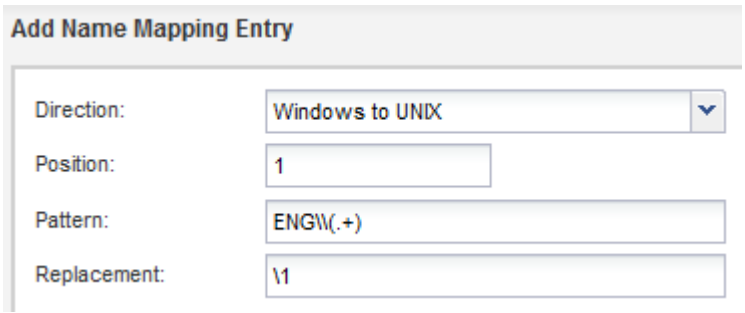
步骤

1. 考虑以下因素，确定名称映射的方法—名称映射转换规则，默认用户映射或两者：
   - 转换规则使用正则表达式将一个用户名转换为另一个用户名，如果要在单个级别控制或跟踪访问，这一点非常有用。

     例如，您可以将 UNIX 用户映射到域中的 Windows 用户，反之亦然。
   - 使用默认用户可以为未通过隐式映射或名称映射转换规则映射的所有用户分配用户名。

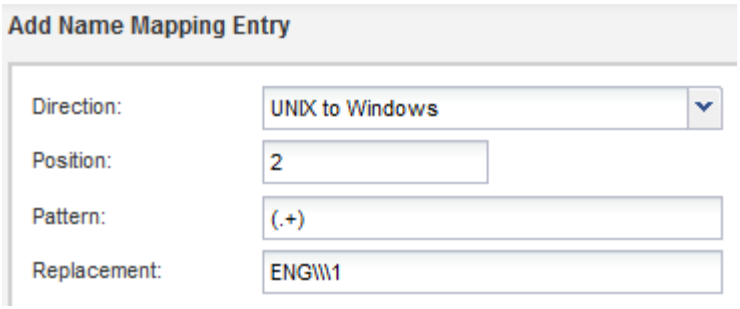
     每个 SVM 都有一个名为 "`pcuser` " 的默认 UNIX 用户，但没有默认 Windows 用户。
2. 导航到 * SVM* 窗口。
3. 选择要配置的 SVM 。
4. 单击 * SVM 设置 * 选项卡。
5. 可选：创建将UNIX用户帐户转换为Windows用户帐户的名称映射、反之亦然：
   a. 在 * 主机用户和组 * 窗格中，单击 * 名称映射 * 。
   b. 单击 * 添加 * ，保留默认的 * 从 Windows 到 UNIX* 方向，然后创建一个正则表达式，以便在 Windows 用户尝试访问使用 UNIX 文件权限的文件时生成 UNIX 凭据。

      使用以下条目将 ENG 域中的任何 Windows 用户转换为同名的 UNIX 用户。模式 `ENG\\(.+)` 查找具有前缀的任何Windows用户名 `ENG\\`和替换项 `\1` 通过删除用户名以外的所有内容来创建UNIX版本。

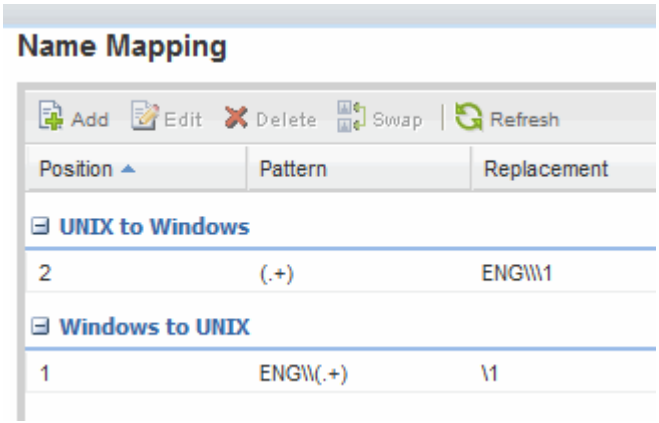
      

   c. 单击 "* 添加 " ，选择 "UNIX 到 Windows* " 方向，然后创建相应的映射，以便在 UNIX 用户尝试访问具有 NTFS 文件权限的文件时生成 Windows 凭据。

      使用以下条目将每个 UNIX 用户转换为 ENG 域中同名的 Windows 用户。模式 `(.+)` 查找任何UNIX名称和替换项 `ENG\\\1` 通过插入创建Windows版本 `ENG\\` 在用户名之前。



a. 由于每个规则的位置决定了应用规则的顺序，因此您应查看结果并确认该顺序符合您的预期。



b. 重复步骤5b到5d以映射SVM上的所有域和名称。

6. 可选：创建默认Windows用户：

a. 在 SVM 的 LDAP ， NIS 或本地用户中创建 Windows 用户帐户。

如果使用本地用户，则可以在 " 主机用户和组 " 窗格的 * Windows * 下创建帐户。

b. 通过在 * 协议 * 窗格中选择 * nfs* > * 编辑 * 并输入用户名来设置默认 Windows 用户。

您可以创建一个名为 "`unixusers` " 的本地 Windows 用户并将其设置为默认 Windows 用户。

7. 可选：如果您希望用户与默认值(即"`pcuser`"用户)不同、请配置默认UNIX用户。

a. 在 SVM 的 LDAP ， NIS 或本地用户中创建 UNIX 用户帐户。

如果使用本地用户，则可以在 " 主机用户和组 " 窗格的 "**UNIX** " 下创建帐户。

b. 通过在 * 协议 * 窗格中选择 * CIFS* > * 选项 * 并输入用户名来设置默认 UNIX 用户。

您可以创建一个名为 "`winusers` " 的本地 UNIX 用户并将其设置为默认 UNIX 用户。

下一步操作

如果您配置了默认用户，则在稍后在工作流中配置文件权限时，应设置默认 Windows 用户和默认 UNIX 用户的权限。

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，而 NFS 客户端则在挂载卷时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。

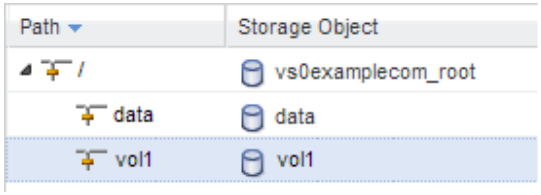
   b. 从下拉菜单中选择 * SVM* 。

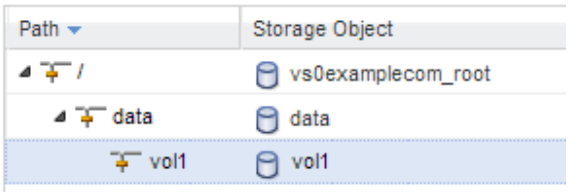
   c. 单击 * 挂载 * 。

   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。



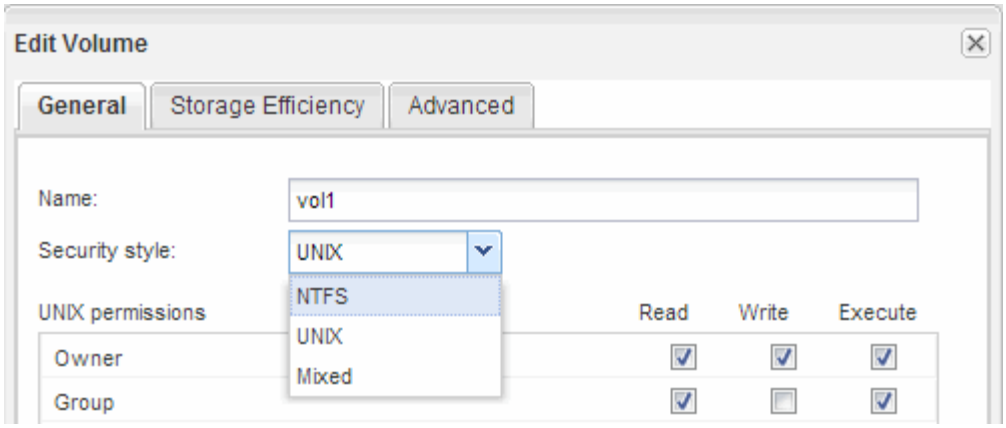


8. 查看卷的安全模式，并根据需要进行更改：

   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. 选择您喜欢的安全模式，然后单击 * 保存并关闭 * 。



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. 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. 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 * 。

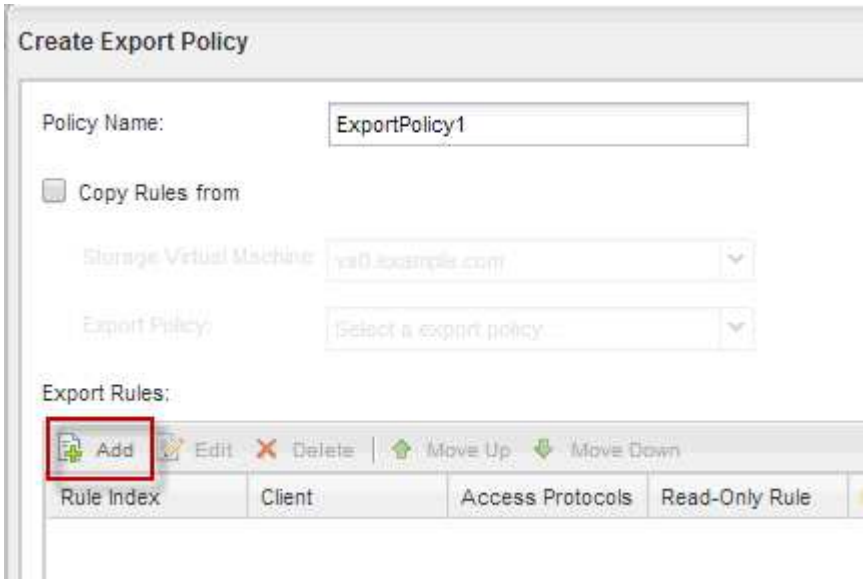
   更新后的共享访问权限将列在 " 共享访问控制 " 窗格中。

为卷创建导出策略

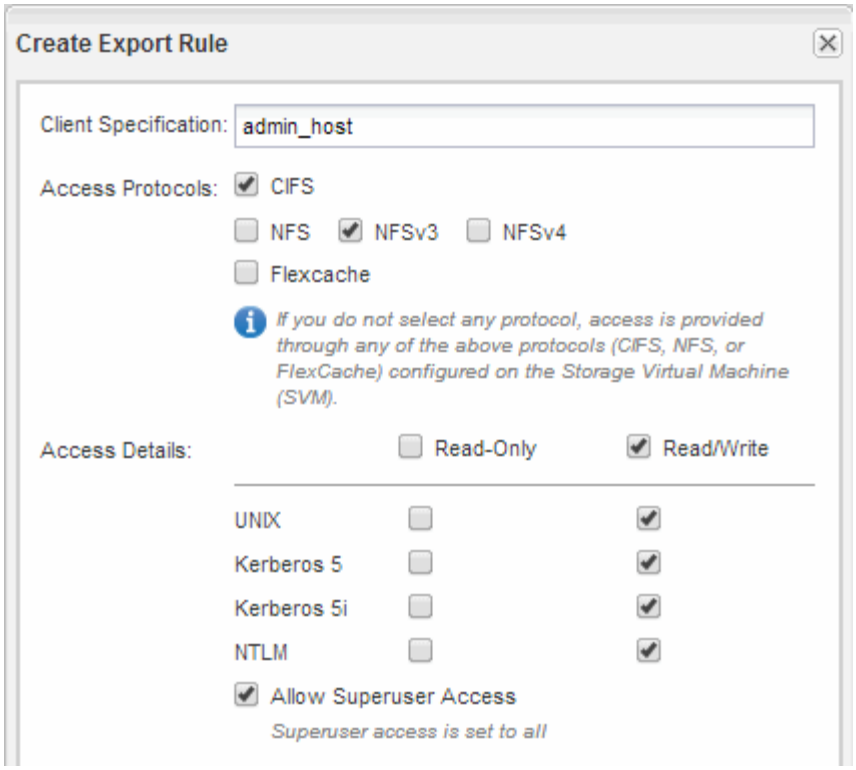
在任何 NFS 客户端能够访问卷之前，您必须为卷创建导出策略，添加允许管理主机访问的规则，并将新导出策略应用于卷。

步骤

1. 导航到 * SVM* 窗口。
2. 单击 * SVM 设置 * 选项卡。
3. 创建新导出策略：
   a. 在 * 策略 * 窗格中，单击 * 导出策略 * ，然后单击 * 创建 * 。
   b. 在 * 创建导出策略 * 窗口中，指定策略名称。
   c. 在 * 导出规则 * 下，单击 * 添加 * 向新策略添加规则。



4. 在 * 创建导出规则 * 对话框中，创建一个允许管理员通过所有协议对导出进行完全访问的规则：
   a. 指定要从中管理导出卷的 IP 地址或客户端名称，例如 admin_host 。
   b. 选择 * CIFS* 和 * NFSv3* 。
   c. 确保已选择所有 * 读 / 写 * 访问详细信息以及 * 允许超级用户访问 * 。



d. 单击 * 确定 * ，然后单击 * 创建 * 。

此时将创建新导出策略及其新规则。

5. 将新导出策略应用于新卷，以便管理员主机可以访问此卷：
   a. 导航到 * 命名空间 * 窗口。
   b. 选择卷并单击 * 更改导出策略 * 。
   c. 选择新策略并单击 * 更改 * 。

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 。

从 **UNIX** 管理主机验证 **NFS** 访问

在配置对 Storage Virtual Machine （ SVM ）的 NFS 访问后，您应登录到 NFS 管理主机并从 SVM 读取数据并向 SVM 写入数据来验证配置。

开始之前

- 客户端系统必须具有先前指定的导出规则允许的 IP 地址。
- 您必须具有 root 用户的登录信息。

步骤

1. 以 root 用户身份登录到客户端系统。
2. 输入 … `cd /mnt/` 将目录更改为挂载文件夹。
3. 使用 SVM 的 IP 地址创建并挂载新文件夹：
   a. 输入 … `mkdir /mnt/folder` 以创建新文件夹。
   b. 输入 … `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` 将卷挂载到此新目录。
   c. 输入 … `cd folder` 可将目录更改为新文件夹。

      以下命令将创建一个名为 test1 的文件夹，并在 test1 挂载文件夹的 192.0.2.130 IP 地址处挂载 vol1 卷，然后更改为新的 test1 目录：

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. 创建一个新文件，验证该文件是否存在并向其写入文本：
   a. 输入 … `touch filename` 以创建测试文件。
   b. 输入 … `ls -l filename` 以验证文件是否存在。
   c. 输入 … `cat >filename`下，键入一些文本，然后按Ctrl+D将文本写入测试文件。
   d. 输入 … `cat filename` 以显示测试文件的内容。
   e. 输入 … `rm filename` 以删除测试文件。
   f. 输入 … `cd ..` 返回父目录。

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

结果

您已确认已启用对 SVM 的 NFS 访问。

配置并验证 **CIFS** 和 **NFS** 客户端访问

准备好后，您可以通过设置 UNIX 或 NTFS 文件权限，修改共享 ACL 以及添加导出规则来配置客户端访问。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. 使用与卷的安全模式对应的方法设置文件权限：

如果卷的安全模式为 ...	执行此操作 ...
NTFS	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。
"unix"	在 UNIX 管理主机上，使用 root 用户在卷上设置 UNIX 所有权和权限。

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 System Manager 中，向导出策略添加允许 NFS 客户端访问共享的规则。
   a. 选择 Storage Virtual Machine （ SVM ），然后单击 * SVM 设置 * 。
   b. 在 * 策略 * 窗格中，单击 * 导出策略 * 。

c. 选择应用于卷的导出策略。

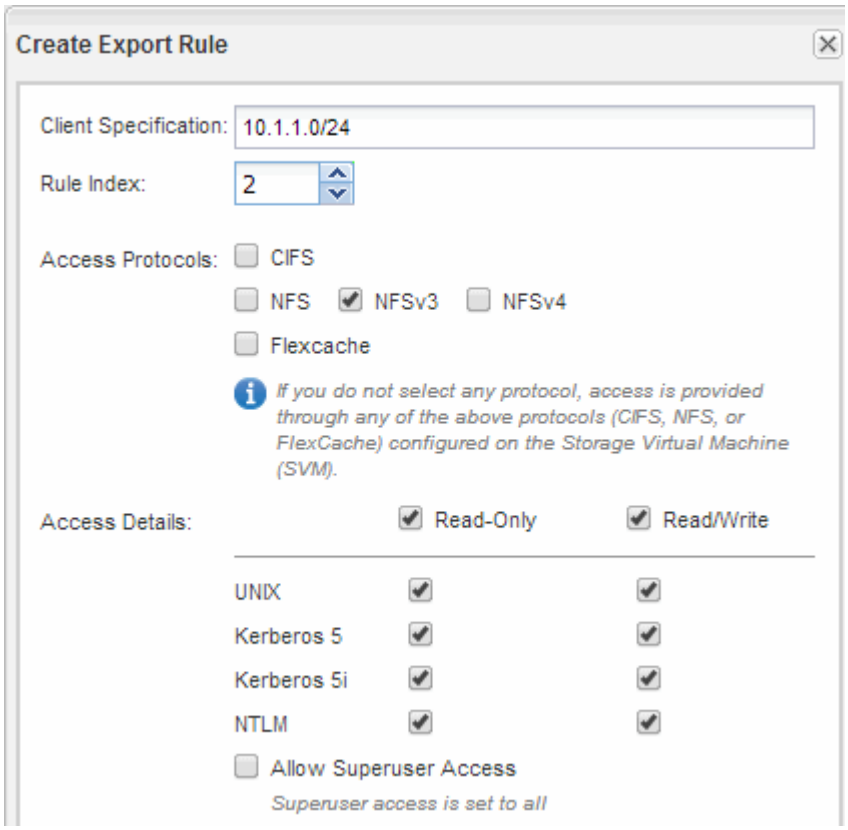
d. 在 * 导出规则 * 选项卡中，单击 * 添加 * 并指定一组客户端。

e. 为 * 规则索引 * 选择 * 。 2 以使此规则在允许访问管理主机的规则之后执行。

f. 选择 * CIFS* 和 * NFSv3* 。

g. 指定所需的访问详细信息，然后单击 * 确定。 *

您可以通过键入子网为客户端授予完全读/写访问权限 `10.1.1.0/24` 作为*Client Specific*，并选中除*Allow Superuser Access*外的所有访问复选框。



5. 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。

6. 在 UNIX 客户端上，以现在有权访问卷的用户之一身份登录，并验证您是否可以挂载卷并创建文件。