



配置对现有 **SVM** 的 **NFS** 访问

System Manager Classic

NetApp
June 22, 2024

目录

配置对现有 SVM 的 NFS 访问	1
添加对现有 SVM 的 NFS 访问	1
打开 SVM 根卷的导出策略（配置对现有 SVM 的 NFS 访问）	3
配置 LDAP（配置对现有 SVM 的 NFS 访问）	4
从 UNIX 管理主机验证 NFS 访问	7
配置和验证 NFS 客户端访问（配置对现有 SVM 的 NFS 访问）	8

配置对现有 SVM 的 NFS 访问

为 NFS 客户端添加对现有 SVM 的访问权限涉及到向 SVM 添加 NFS 配置，打开 SVM 根卷的导出策略，可选择配置 LDAP 以及从 UNIX 管理主机验证 NFS 访问。然后，您可以配置 NFS 客户端访问。

添加对现有 SVM 的 NFS 访问

为现有 SVM 添加 NFS 访问涉及创建数据 LIF ，可选择配置 NIS ，配置卷，导出卷以及配置导出策略。

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
- 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 NFS 协议。

有关详细信息，请参见 ["网络管理文档"](#)。

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 * NFS * 。

Protocols: NFS FC/FCoE

2. 在 * 配置 NFS 协议 * 对话框中，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。

Data LIF Configuration

Retain the CIFS data LIF's configuration for NFS clients.

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: [Browse...](#)

3. 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，并选择要添加 NIS 名称服务源的数据库类型。

— NIS Configuration {Optional}

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:

IP Addresses:

? Database Type: group passwd netgroup

如果 NIS 服务不可用，请勿尝试对其进行配置。如果 NIS 服务配置不当，则可能会出现发生原因数据存储库访问问题。

4. 创建和导出卷以进行 NFS 访问：

- 对于 * 导出名称 * ，键入一个名称，该名称将同时为导出名称和卷名称的开头。
- 指定要包含文件的卷的大小。

Provision a volume for NFS storage.

Export Name:

Size: GB

Permission: [Change](#)

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。

- 在 * 权限 * 字段中，单击 * 更改 * ，然后指定一个导出规则，此规则可为 NFSv3 授予对 UNIX 管理主机的访问权限，包括超级用户访问权限。

Create Export Rule

Client Specification:
Enter comma-separated values for multiple client specifications

Access Protocols: CIFS
 NFS NFSv3 NFSv4
 Flexcache

i If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access	<small>Superuser access is set to all</small>	

您可以创建一个名为 Eng 的 10 GB 卷，并将其导出为 Eng，然后添加一条规则，为 "admin_host" 客户端授予对导出的完全访问权限，包括超级用户访问权限。

5. 单击 * 提交并关闭 *，然后单击 * 确定 *。

打开 SVM 根卷的导出策略（配置对现有 SVM 的 NFS 访问）

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。

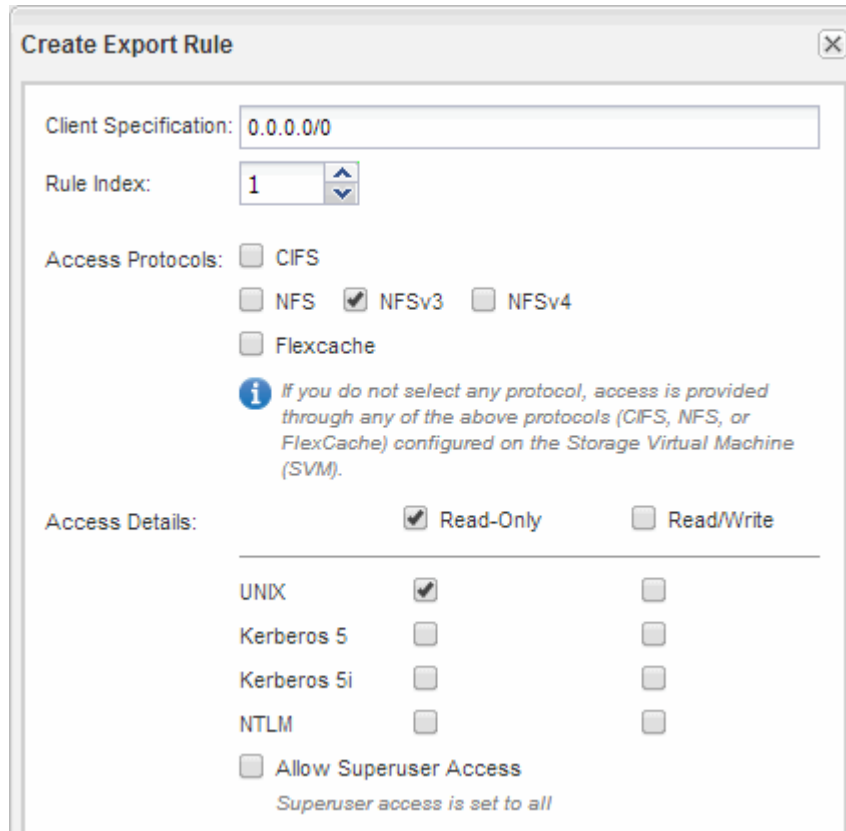
关于此任务

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。

配置 LDAP（配置对现有 SVM 的 NFS 访问）

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。有关详细信息，请参见 ["LDAP 使用概述"](#)。

- 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。

The screenshot shows the 'Create LDAP Client' dialog box with the 'General' tab selected. The 'LDAP Client Configuration' field contains 'vs0client1'. Under the 'Servers' section, the 'Active Directory Domain' radio button is selected with the value 'example.com'. Below it, a table lists 'Preferred Active Directory Servers' with one entry: '192.0.2.145'. To the right of the table are buttons for 'Add', 'Delete', 'Up', and 'Down'. At the bottom, the 'Active Directory Servers' radio button is unselected.

- 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。

The screenshot shows the 'Edit LDAP Client' dialog box with the 'Binding' tab selected. The 'Authentication level' dropdown is set to 'sasl'. The 'Bind DN (User)' field contains 'user'. The 'Bind user password' field contains six dots. The 'Base DN' field contains 'DC=example,DC=com'. The 'Tcp port' spinner is set to '389'. An information icon and text at the bottom state: 'The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.'

- 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 *。

Name Service Switch			
hosts:	files	dns	
namemap:	ldap	files	
group:	ldap	files	nis
netgroup:	ldap	files	nis
passwd:	ldap	files	nis

LDAP 是此 SVM 上名称服务和名称映射的主要用户信息来源。

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。

配置和验证 NFS 客户端访问（配置对现有 SVM 的 NFS 访问）

准备好后，您可以通过在 UNIX 管理主机上设置 UNIX 文件权限并在 System Manager 中添加导出规则来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 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，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. 选择与卷同名的导出策略。
 - 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 *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。

Create Export Rule [X]

Client Specification:

Rule Index: [^] [v]

Access Protocols: CIFS
 NFS NFSv3 NFSv4
 Flexcache

i *If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).*

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

4. 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。

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。