



将 **CIFS** 卷添加到启用了 **CIFS** 的 **SVM** System Manager Classic

NetApp
June 22, 2024

目录

将 CIFS 卷添加到启用了 CIFS 的 SVM	1
创建并配置卷	1
创建共享并设置其权限	2
验证 SMB 客户端访问	3
配置并验证 CIFS 客户端访问	3

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。

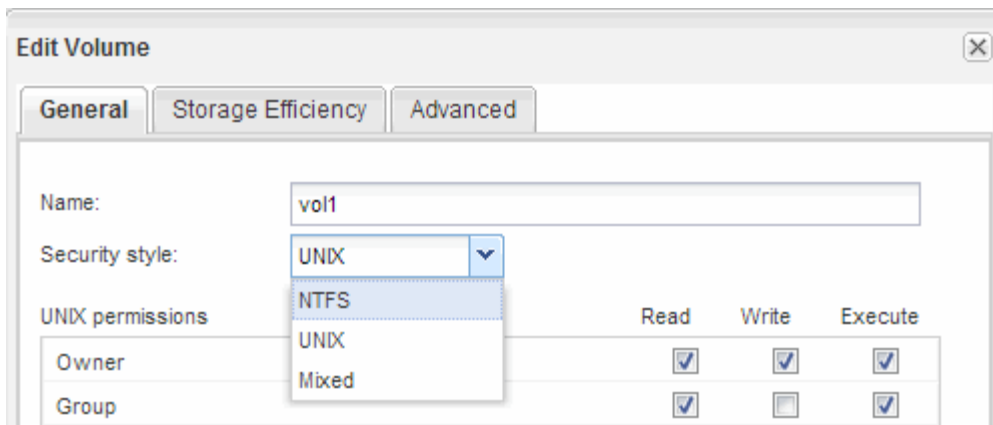
如果要将某些卷组织在名为 data 的主卷下，可以将新卷 "vol1" 从根卷移动到 " data " 卷。

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`、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。

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。