NAS 存储管理

ONTAP 9

NetApp
April 24, 2024

目录

NAS 存储管理

使用 System Manager 管理 NAS 协议

使用System Manager进行NAS管理概述

本节中的主题介绍如何在 ONTAP 9.7 及更高版本中使用 System Manager 配置和管理 NAS 环境。

如果您使用的是经典 System Manager （仅适用于 ONTAP 9.7 及更早版本），请参见以下主题：

- "NFS 配置概述"
- "SMB配置概述"

System Manager 支持以下工作流：

- 要用于 NAS 文件服务的集群的初始配置。
- 针对不断变化的存储需求进行额外的卷配置。
- 配置和维护行业标准身份验证和安全设施。

使用 System Manager ，您可以在组件级别管理 NAS 服务：

- 协议— NFS ， SMB 或两者（ NAS 多协议）
- 名称服务— DNS ， LDAP 和 NIS
- 名称服务开关
- Kerberos 安全性
- 导出和共享
- qtree
- 用户和组的名称映射

为VMware数据存储库配置NFS存储

在使用适用于 VMware vSphere 的 Virtual Storage Console （ VSC ）为 ESXi 主机在基于 ONTAP 的存储系统上配置 NFS 卷之前，请使用适用于 ONTAP 9.7 或更高版本的 System Manager 启用 NFS 。

创建后 "启用了 NFS 的 Storage VM" 然后，在 System Manager 中，您可以使用 VSC 配置 NFS 卷并管理数据存储库。

从 VSC 7.0 开始， VSC 属于 "适用于 VMware vSphere 虚拟设备的 ONTAP 工具"，其中包括适用于 VMware vSphere 的 VSC ， vStorage APIs for Storage Awareness （ VASA ） Provider 和 Storage Replication Adapter （ SRA ）功能。

请务必检查 "NetApp 互操作性表" 以确认当前 ONTAP 版本与 VSC 版本之间的兼容性。

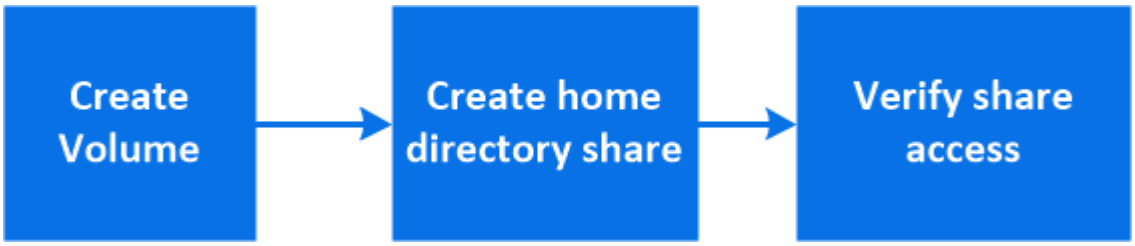
要使用 System Manager 经典版（适用于 ONTAP 9.7 及更早版本）为 ESXi 主机设置对数据存储库的 NFS 访问，请参见 "使用VSC为ESXi配置NFS概述"

有关详细信息，请参见 "TR-4597 ： 适用于 ONTAP 的 VMware vSphere" 以及适用于您的 VSC 版本的文档。

为主目录配置 NAS 存储

创建卷以使用 SMB 协议为主目录提供存储。

此操作步骤会为上的主目录创建新卷 "已启用SMB的现有Storage VM"。您可以在配置卷或指定自定义配置时接受系统默认值。



您可以创建 FlexVol 卷，也可以为具有高性能要求的大型文件系统创建 FlexGroup 卷。 另请参见 "使用 FlexGroup 卷为大型文件系统配置 NAS 存储"。

您也可以将此卷的规格保存到 Ansible 攻略手册中。有关详细信息，请访问 "使用 Ansible 攻略手册添加或编辑卷或 LUN"。

步骤

1. 在启用了 SMB 的 Storage VM 中添加新卷。
   a. 选择*存储>卷*，然后单击*添加*。
   b. 输入名称，选择 Storage VM 并输入大小。

      仅会列出配置了SMB协议的Storage VM。如果只有一个配置了SMB协议的Storage VM可用、则不会显示* Storage VM*字段。

      - 如果此时单击 * 保存 * ，则 System Manager 将使用系统默认值创建和添加 FlexVol 卷。
      - 您可以单击 * 更多选项 * 自定义卷的配置，以启用授权，服务质量和数据保护等服务。 请参见 [自定义卷配置]，然后返回此处完成以下步骤。
2. 【工作流中的第 2 步，第 2 步】单击 * 存储 > 共享 * ，单击 * 添加 * ，然后选择 * 主目录 * 。
3. 在 Windows 客户端上，执行以下操作以验证共享是否可访问。
   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_`

      如果共享名称是使用变量（ %w ， %d 或 %u ）创建的，请务必使用解析后的名称测试访问。

   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。

自定义卷配置

您可以在添加卷时自定义卷配置，而不是接受系统默认值。

操作步骤

单击 * 更多选项 * 后，选择所需功能并输入所需值。

- 远程卷的缓存。
- 性能服务级别（服务质量， QoS ）。

  从ONTAP 9.8开始、除了默认值选择之外、您还可以指定自定义QoS策略或禁用QoS。

  - 要禁用 QoS ，请依次选择 * 自定义 * ， * 现有 * 和 * 无 * 。
  - 如果选择 * 自定义 * 并指定现有服务级别，则会自动选择一个本地层。
  - 从 ONTAP 9.1.1 开始，如果选择创建自定义性能服务级别，则可以使用 System Manager 手动选择要放置所创建卷的本地层（ * 手动放置 * ）。

    如果选择远程缓存或 FlexGroup 卷选项，则此选项不可用。

- FlexGroup 卷（选择 * 在集群中分布卷数据 * ）。

  如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。 否则，默认情况下，您要添加的卷将成为 FlexVol 卷。

- 配置了卷的协议的访问权限。
- 使用 SnapMirror （本地或远程）保护数据，然后从下拉列表中指定目标集群的保护策略和设置。
- 选择*保存*以创建卷并将其添加到集群和Storage VM。

> 保存卷后，返回到 [step2] 完成主目录的配置。

使用 **NFS** 为 **Linux** 服务器配置 **NAS** 存储

使用 NFS 协议和 ONTAP System Manager （ 9.7 及更高版本）创建卷以为 Linux 服务器提供存储。

此操作步骤会在上创建新卷 "已启用 NFS 的现有 Storage VM"。您可以在配置卷或指定自定义配置时接受系统默认值。

您可以创建 FlexVol 卷，也可以为具有高性能要求的大型文件系统创建 FlexGroup 卷。 另请参见 "使用 FlexGroup 卷为大型文件系统配置 NAS 存储"。

您也可以将此卷的规格保存到 Ansible 攻略手册中。有关详细信息，请访问 "使用 Ansible 攻略手册添加或编辑卷或 LUN"。

如果要了解有关ONTAP NFS协议功能范围的详细信息、请参见 "NFS参考概述"。

步骤

1. 在启用了NFS的Storage VM中添加新卷。
   a. 单击 * 存储 > 卷 * ，然后单击 * 添加 * 。
   b. 输入名称，选择 Storage VM 并输入大小。

仅列出配置了 NFS 协议的 Storage VM 。如果只有一个配置了SMB协议的Storage VM可用、则不会显示* Storage VM*字段。

- 如果此时单击 * 保存 * ，则 System Manager 将使用系统默认值创建和添加 FlexVol 卷。

  默认导出策略会为所有用户授予完全访问权限。

- 您可以单击 * 更多选项 * 自定义卷的配置，以启用授权，服务质量和数据保护等服务。 请参见 [自定义卷配置]，然后返回此处完成以下步骤。

2. 在Linux客户端上、执行以下操作以验证访问。

   a. 使用 Storage VM 的网络接口创建并挂载卷。

   b. 在新挂载的卷上，创建一个测试文件，向该文件写入文本，然后删除该文件。

   验证访问后，您可以 "使用卷的导出策略限制客户端访问" 并在挂载的卷上设置所需的任何 UNIX 所有权和权限。

自定义卷配置

您可以在添加卷时自定义卷配置，而不是接受系统默认值。

操作步骤

单击 * 更多选项 * 后，选择所需功能并输入所需值。

- 远程卷的缓存。
- 性能服务级别（服务质量， QoS ）。

  从ONTAP 9.8开始、除了默认值选择之外、您还可以指定自定义QoS策略或禁用QoS。

  - 要禁用 QoS ，请依次选择 * 自定义 * ， * 现有 * 和 * 无 * 。
  - 如果选择 * 自定义 * 并指定现有服务级别，则会自动选择一个本地层。
  - 从 ONTAP 9.1.1 开始，如果选择创建自定义性能服务级别，则可以使用 System Manager 手动选择要放置所创建卷的本地层（ * 手动放置 * ）。

    如果选择远程缓存或 FlexGroup 卷选项，则此选项不可用。

- FlexGroup 卷（选择 * 在集群中分布卷数据 * ）。

  如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。 否则，默认情况下，您要添加的卷将成为 FlexVol 卷。

- 配置了卷的协议的访问权限。
- 使用 SnapMirror （本地或远程）保护数据，然后从下拉列表中指定目标集群的保护策略和设置。
- 选择*保存*以创建卷并将其添加到集群和Storage VM。

保存卷后，返回到 [step2-complete-prov] 使用 NFS 完成 Linux 服务器的配置。

在 **ONTAP** 中执行此操作的其他方法

执行此任务的对象	请参见 …
System Manager 经典版（ONTAP 9.7 及更早版本）	"NFS 配置概述"
ONTAP 命令行界面（CLI）	"使用命令行界面概述 NFS 配置"

使用导出策略管理访问

使用导出策略启用 Linux 客户端对 NFS 服务器的访问。

此操作步骤将为创建或修改导出策略 "已启用 NFS 的现有 Storage VM"。

步骤

1. 在 System Manager 中，单击 * 存储 * > * 卷 * 。
2. 单击启用了 NFS 的卷，然后单击 * 更多 * 。
3. 单击 * 编辑导出策略 * ，然后单击 * 选择现有策略 * 或 * 添加新策略 * 。

使用 **SMB** 为 **Windows** 服务器配置 **NAS** 存储

使用 ONTAP 9.7 及更高版本提供的 System Manager 创建卷以使用 SMB 协议为 Windows 服务器提供存储。

此操作步骤会在上创建新卷 "已启用SMB的现有Storage VM" 并为卷根目录（/）目录创建共享。您可以在配置卷或指定自定义配置时接受系统默认值。在初始 SMB 配置后，您还可以创建其他共享并修改其属性。

您可以创建 FlexVol 卷，也可以为具有高性能要求的大型文件系统创建 FlexGroup 卷。 另请参见 "使用 FlexGroup 卷为大型文件系统配置 NAS 存储"。

您也可以将此卷的规格保存到 Ansible 攻略手册中。有关详细信息，请访问 "使用 Ansible 攻略手册添加或编辑卷或 LUN"。

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"。

开始之前

- 从ONTAP 9.13.1开始、默认情况下、您可以对新卷启用容量分析和活动跟踪。在System Manager中、您可以管理集群或Storage VM级别的默认设置。有关详细信息，请参见 启用文件系统分析。

步骤

1. 在启用了 SMB 的 Storage VM 中添加新卷。
   a. 单击 * 存储 > 卷 * ，然后单击 * 添加 * 。
   b. 输入名称，选择 Storage VM 并输入大小。

      仅会列出配置了SMB协议的Storage VM。如果只有一个配置了SMB协议的Storage VM可用、则不会显示* Storage VM*字段。

      - 如果此时选择*保存*，则System Manager将使用系统默认值创建和添加FlexVol卷。

    - 您可以选择*更多选项*自定义卷配置以启用授权、服务质量和数据保护等服务。 请参见 [自定义卷配置]，然后返回此处完成以下步骤。

2. 【工作流中的步骤2-compl-prov-win、步骤2】切换到Windows客户端以验证共享是否可访问。
    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_`
    b. 在新创建的驱动器上，创建一个测试文件，向该文件写入文本，然后删除该文件。

验证访问后，您可以使用共享 ACL 限制客户端访问，并在映射的驱动器上设置所需的任何安全属性。请参见 "创建 SMB 共享" 有关详细信息 …

添加或修改共享

您可以在初始 SMB 配置后添加其他共享。共享是使用您选择的默认值和属性创建的。这些内容可以稍后修改。

您可以在配置共享时设置以下共享属性：

- 访问权限
- 共享属性
    - 通过 SMB 数据为包含 Hyper-V 和 SQL Server 的共享启用持续可用性（从 ONTAP 9.10.1 开始）。另请参见：
        - "基于 SMB 的 Hyper-V 的持续可用共享要求"
        - "通过 SMB 实现 SQL Server 持续可用的共享要求"
    - 访问此共享时使用 SMB 3.0 加密数据。

初始配置后，您还可以修改以下属性：

- 符号链接
    - 启用或禁用符号链接和 Widelink
- 共享属性
    - 允许客户端访问 Snapshot 副本目录。
    - 启用机会锁，允许客户端在本地锁定文件并缓存内容（默认）。
    - 启用基于访问的枚举（ ABE ）以根据用户的访问权限显示共享资源。

过程

要在启用了 SMB 的卷中添加新共享，请单击 "* 存储 ">" 共享 " ，单击 "* 添加 " ，然后选择 "* 共享 " 。

要修改现有共享、请单击"*存储">"共享"、然后单击 ⋮ 并选择 " 编辑 "* 。

自定义卷配置

您可以在添加卷时自定义卷配置，而不是接受系统默认值。

操作步骤

单击 * 更多选项 * 后，选择所需功能并输入所需值。

- 远程卷的缓存。
- 性能服务级别（服务质量， QoS ）。

  从 ONTAP 9.8 开始，除了默认值选择之外，您还可以指定自定义 QoS 策略或禁用 QoS 。

  - 要禁用 QoS ，请依次选择 * 自定义 * ， * 现有 * 和 * 无 * 。
  - 如果选择 * 自定义 * 并指定现有服务级别，则会自动选择一个本地层。
  - 从 ONTAP 9.1.1 开始，如果选择创建自定义性能服务级别，则可以使用 System Manager 手动选择要放置所创建卷的本地层（ * 手动放置 * ）。

    如果选择远程缓存或 FlexGroup 卷选项，则此选项不可用。

- FlexGroup 卷（选择 * 在集群中分布卷数据 * ）。

  如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。否则，默认情况下，您要添加的卷将成为 FlexVol 卷。

- 如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。否则，默认情况下，您要添加的卷将成为 FlexVol 卷。
- 对配置了卷的协议的访问权限。
- 使用 SnapMirror 进行数据保护（本地或远程），然后从下拉列表中指定目标集群的保护策略和设置。
- 单击 * 保存 * 以创建卷并将其添加到集群和 Storage VM 。

您可以在添加卷时自定义卷配置，而不是接受系统默认值。

操作步骤

单击 * 更多选项 * 后，选择所需功能并输入所需值。

- 远程卷的缓存。
- 性能服务级别（服务质量， QoS ）。

  从ONTAP 9.8开始、除了默认值选择之外、您还可以指定自定义QoS策略或禁用QoS。

  - 要禁用 QoS ，请依次选择 * 自定义 * ， * 现有 * 和 * 无 * 。
  - 如果选择 * 自定义 * 并指定现有服务级别，则会自动选择一个本地层。
  - 从 ONTAP 9.1.1 开始，如果选择创建自定义性能服务级别，则可以使用 System Manager 手动选择要放置所创建卷的本地层（ * 手动放置 * ）。

    如果选择远程缓存或 FlexGroup 卷选项，则此选项不可用。

- FlexGroup 卷（选择 * 在集群中分布卷数据 * ）。

  如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。 否则，默认情况下，您要添加的卷将成为 FlexVol 卷。

- 配置了卷的协议的访问权限。
- 使用 SnapMirror （本地或远程）保护数据，然后从下拉列表中指定目标集群的保护策略和设置。

- 选择*保存*以创建卷并将其添加到集群和Storage VM。

> 保存卷后，返回到 [step2-compl-prov-win] 使用 SMB 完成 Windows 服务器的配置。

在 **ONTAP** 中执行此操作的其他方法

执行此任务的对象	请参见 …
System Manager 经典版（ONTAP 9.7 及更早版本）	"SMB配置概述"
ONTAP 命令行界面	"使用命令行界面概述SMB配置"

使用 **NFS** 和 **SMB** 为 **Windows** 和 **Linux** 配置 **NAS** 存储

创建卷以使用 NFS 或 SMB 协议为客户端提供存储。

此操作步骤会在上创建新卷 "已为 NFS 和 SMB 协议启用现有 Storage VM"。

> NFS协议通常用于Linux环境。 SMB协议通常用于Windows环境。 但是、NFS和SMB均可用于Linux或Windows。

您可以创建 FlexVol 卷，也可以为具有高性能要求的大型文件系统创建 FlexGroup 卷。 请参见 "使用 FlexGroup 卷为大型文件系统配置 NAS 存储"。

您也可以将此卷的规格保存到 Ansible 攻略手册中。有关详细信息，请访问 "使用 Ansible 攻略手册添加或编辑卷或 LUN"。

步骤

1. 在同时为 NFS 和 SMB 启用的 Storage VM 中添加新卷。

   a. 单击 * 存储 > 卷 * ，然后单击 * 添加 * 。

   b. 输入名称，选择 Storage VM 并输入大小。

      仅会列出同时配置了 NFS 和 SMB 协议的 Storage VM 。如果只有一个配置了 NFS 和 SMB 协议的 Storage VM 可用，则不会显示 * Storage VM* 字段。

   c. 单击*更多选项*并选择*通过NFS*导出。

      默认设置会为所有用户授予完全访问权限。您可以稍后向导出策略添加限制性更强的规则。

   d. 选择 * 通过 SMB/CIFS 共享 * 。

      创建共享时， * 任何人 * 组的默认访问控制列表（ACL）设置为 " 完全控制 " 。您可以稍后向 ACL 添加限制。

e. 如果此时单击 * 保存 * ，则 System Manager 将使用系统默认值创建和添加 FlexVol 卷。

或者，您也可以继续启用任何其他所需服务，例如授权，服务质量和数据保护。请参见 [自定义卷配置]，然后返回此处完成以下步骤。

2. 【工作流中的步骤2-compl-prov-nfs-smb、步骤2】在Linux客户端上、验证导出是否可访问。

   a. 使用 Storage VM 的网络接口创建并挂载卷。

   b. 在新挂载的卷上，创建一个测试文件，向该文件写入文本，然后删除该文件。

3. 在 Windows 客户端上，执行以下操作以验证共享是否可访问。

   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_`

   b. 在新创建的驱动器上，创建一个测试文件，向该文件写入文本，然后删除该文件。

   验证访问后，您可以 "使用卷的导出策略限制客户端访问，使用共享 ACL 限制客户端访问"，并在导出的卷和共享卷上设置所需的所有权和权限。

自定义卷配置

您可以在添加卷时自定义卷配置，而不是接受系统默认值。

操作步骤

单击 * 更多选项 * 后，选择所需功能并输入所需值。

- 远程卷的缓存。
- 性能服务级别（服务质量， QoS ）。

  从ONTAP 9.8开始、除了默认值选择之外、您还可以指定自定义QoS策略或禁用QoS。

  - 要禁用 QoS ，请依次选择 * 自定义 * ， * 现有 * 和 * 无 * 。
  - 如果选择 * 自定义 * 并指定现有服务级别，则会自动选择一个本地层。
  - 从 ONTAP 9.1.1 开始，如果选择创建自定义性能服务级别，则可以使用 System Manager 手动选择要放置所创建卷的本地层（ * 手动放置 * ）。

    如果选择远程缓存或 FlexGroup 卷选项，则此选项不可用。

- FlexGroup 卷（选择 * 在集群中分布卷数据 * ）。

  如果先前在 * 性能服务级别 * 下选择了 * 手动放置 * ，则此选项不可用。 否则，默认情况下，您要添加的卷将成为 FlexVol 卷。

- 配置了卷的协议的访问权限。
- 使用 SnapMirror （本地或远程）保护数据，然后从下拉列表中指定目标集群的保护策略和设置。
- 选择*保存*以创建卷并将其添加到集群和Storage VM。

保存卷后，返回到 [step2-compl-prov-nfs-smb] 完成 Windows 和 Linux 服务器的多协议配置。

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 ...	查看此内容 ...
System Manager 经典版（ONTAP 9.7 及更早版本）	"SMB 和 NFS 多协议配置概述"
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"

使用 **Kerberos** 确保客户端访问安全

启用 Kerberos 以保护 NAS 客户端的存储访问。

此操作步骤会在已启用的现有 Storage VM 上配置 Kerberos "NFS" 或 "SMB"。

开始之前，您应已配置 DNS ， NTP 和 "LDAP" 在存储系统上。

步骤

1. 在 ONTAP 命令行中，为 Storage VM 根卷设置 UNIX 权限。

   a. 显示Storage VM根卷上的相关权限： `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

      Storage VM 的根卷必须具有以下配置：

名称	正在设置 ...
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	755

   a. 如果未显示这些值、请使用 `volume modify` 命令进行更新。

2. 设置 Storage VM 根卷的用户权限。

   a. 显示本地 UNIX 用户： `vserver services name-service unix-user show -vserver` *`vserver_name`*

      此 Storage VM 应配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**
NFS	500	0
root	0	0

+

- 注： * 如果 NFS 客户端用户的 SPN 存在 Kerberos - UNIX 名称映射，则不需要 NFS 用户；请参见第 5 步。
  a. 如果未显示这些值、请使用 `vserver services name-service unix-user modify` 命令进行更新。

3. 设置 Storage VM 根卷的组权限。
   a. 显示本地 UNIX 组： `vserver services name-service unix-group show -vserver` *`vserver_name`*

      此 Storage VM 应配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0

   a. 如果未显示这些值、请使用 `vserver services name-service unix-group modify` 命令进行更新。
4. 切换到 System Manager 以配置 Kerberos
5. 在 System Manager 中，单击 * 存储 > Storage VM* 并选择 Storage VM 。
6. 单击 * 设置 * 。
7. 单击 → 在 Kerberos 下。
8. 单击 Kerberos 域下的 * 添加 * ，然后完成以下部分：
   - 添加 Kerberos 域

     根据 KDC 供应商输入配置详细信息。

   - 将网络接口添加到域

     单击 * 添加 * 并选择一个网络接口。

9. 如果需要，可将 Kerberos 主体名称与本地用户名之间的映射添加到其中。
   a. 单击*存储> Storage VM*并选择Storage VM。
   b. 单击 * 设置 * ，然后单击 → 在 * 名称映射 * 下。
   c. 在 * Kerberos 到 UNIX* 下，使用正则表达式添加模式和替换项。

使用名称服务提供客户端访问

使 ONTAP 能够使用 LDAP 或 NIS 查找主机，用户，组或网络组信息以对 NAS 客户端进行身份验证。

此操作步骤会在已启用的现有 Storage VM 上创建或修改 LDAP 或 NIS 配置 "NFS" 或 "SMB"。

对于 LDAP 配置，您应具有环境中所需的 LDAP 配置详细信息，并且应使用默认的 ONTAP LDAP 模式。

步骤

1. 配置所需服务：单击 * 存储 > 存储 VM* 。
2. 选择 Storage VM ，单击 * 设置 * ，然后单击 LDAP 或 NIS 。
3. 在名称服务切换中包括任何更改：单击 在名称服务切换下。

管理目录和文件

展开 System Manager 卷显示以查看和删除目录和文件。

从 ONTAP 9.1.1 开始，目录会通过低延迟快速目录删除功能进行删除。

有关在 ONTAP 9.9.1 及更高版本中查看文件系统的详细信息，请参见 "文件系统分析概述"。

步骤

1. 选择 * 存储 > 卷 * 。展开卷以查看其内容。

使用 **System Manager** 管理主机特定的用户和组

从 ONTAP 9.10.1 开始，您可以使用 System Manager 管理特定于 UNIX 或 Windows 主机的用户和组。

您可以执行以下过程：

Windows	"unix"
• 查看 Windows 用户和组 • [add-edit-delete-Windows] • [manage-windows-users]	• 查看 UNIX 用户和组 • [add-edit-delete-UNIX] • [manage-unix-users]

查看 **Windows** 用户和组

在 System Manager 中，您可以查看 Windows 用户和组的列表。

步骤

1. 在 System Manager 中，单击 * 存储 > 存储 VM* 。
2. 选择 Storage VM ，然后选择 * 设置 * 选项卡。
3. 滚动到 * 主机用户和组 * 区域。

   "**Windows** " 部分显示与选定 Storage VM 关联的每个组中的用户数摘要。

4. 单击 在 * Windows * 部分中。
5. 单击 * 组 * 选项卡，然后单击 在组名称旁边可查看有关该组的详细信息。
6. 要查看组中的用户，请选择该组，然后单击 * 用户 * 选项卡。

添加，编辑或删除 **Windows** 组

在 System Manager 中，您可以通过添加，编辑或删除 Windows 组来对其进行管理。

步骤

1. 在 System Manager 中，查看 Windows 组列表。 请参见 查看 Windows 用户和组。
2. 在 * 组 * 选项卡上，您可以管理具有以下任务的组：

要执行此操作 …	执行以下步骤 …
添加组	1. 单击 + Add 。 2. 输入组信息。 3. 指定权限。 4. 指定组成员（添加本地用户，域用户或域组）。
编辑组	1. 在组名称旁边，单击 ⋮，然后单击 * 编辑 * 。 2. 修改组信息。
删除组	1. 选中要删除的组旁边的框。 2. 单击 Delete 。 *注:*您也可以通过单击来删除单个组 ⋮ 在组名称旁边，然后单击 * 删除 * 。

管理 **Windows** 用户

在 System Manager 中，您可以通过添加，编辑，删除，启用或禁用 Windows 用户来对其进行管理。您还可以更改 Windows 用户的密码。

步骤

1. 在 System Manager 中，查看组的用户列表。 请参见 查看 Windows 用户和组。
2. 在 * 用户 * 选项卡上，您可以使用以下任务管理用户：

要执行此操作 …	执行以下步骤 …
添加用户	1. 单击 + Add 。 2. 输入用户信息。
编辑用户	1. 单击用户名旁边的 ⋮，然后单击 * 编辑 * 。 2. 修改用户信息。

删除用户	1. 选中要删除的用户旁边的框。 2. 单击 Delete 。 ◦ 注意： * 您也可以单击删除单个用户 ⋮ 单击用户名旁边的 * 删除 * 。
更改用户密码	1. 单击用户名旁边的 ⋮，然后单击 * 更改密码 * 。 2. 输入新密码并进行确认。
启用用户	1. 选中要启用的每个已禁用用户旁边的框。 2. 单击 Enable 。
禁用用户	1. 选中要禁用的每个已启用用户旁边的框。 2. 单击 Disable 。

查看 **UNIX** 用户和组

在 System Manager 中，您可以查看 UNIX 用户和组的列表。

步骤

1. 在 System Manager 中，单击 * 存储 > 存储 VM* 。
2. 选择 Storage VM ，然后选择 * 设置 * 选项卡。
3. 滚动到 * 主机用户和组 * 区域。

   "**UNIX** " 部分显示与选定 Storage VM 关联的每个组中的用户数摘要。

4. 单击 → 在 * UNIX * 部分中。
5. 单击 * 组 * 选项卡可查看有关该组的详细信息。
6. 要查看组中的用户，请选择该组，然后单击 * 用户 * 选项卡。

添加，编辑或删除 **UNIX** 组

在 System Manager 中，您可以通过添加，编辑或删除 UNIX 组来对其进行管理。

步骤

1. 在 System Manager 中，查看 UNIX 组的列表。 请参见 查看 UNIX 用户和组。
2. 在 * 组 * 选项卡上，您可以管理具有以下任务的组：

要执行此操作 …	执行以下步骤 …
添加组	1. 单击 + Add 。 2. 输入组信息。 3. （可选）指定关联用户。

编辑组	1. 选择组。 2. 单击 Edit 。 3. 修改组信息。 4. （可选）添加或删除用户。
删除组	1. 选择要删除的一个或多个组。 2. 单击 Delete 。

管理 **UNIX** 用户

在 System Manager 中，您可以通过添加，编辑或删除 Windows 用户来对其进行管理。

步骤

1. 在 System Manager 中，查看组的用户列表。 请参见 查看 UNIX 用户和组。
2. 在 * 用户 * 选项卡上，您可以使用以下任务管理用户：

要执行此操作 …	执行以下步骤 …
添加用户	1. 单击 + Add 。 2. 输入用户信息。
编辑用户	1. 选择要编辑的用户。 2. 单击 Edit 。 3. 修改用户信息。
删除用户	1. 选择要删除的一个或多个用户。 2. 单击 Delete 。

监控 **NFS** 活动客户端

从 ONTAP 9.8 开始， System Manager 将显示在集群上获得 NFS 许可时哪些 NFS 客户端连接处于活动状态。

这样，您可以快速验证哪些 NFS 客户端正在主动连接到 Storage VM ，哪些已连接但处于闲置状态，哪些已断开连接。

对于每个NFS客户端IP地址，*NFS客户端*显示内容将显示：
*上次访问时间
*网络接口IP地址
* NFS连接版本
* Storage VM名称

此外， "* 存储 ">Volumes* " 显示还会显示过去 48 小时内处于活动状态的 NFS 客户端列表，并且 "* 信息板 * "

显示会包含 NFS 客户端的计数。

步骤

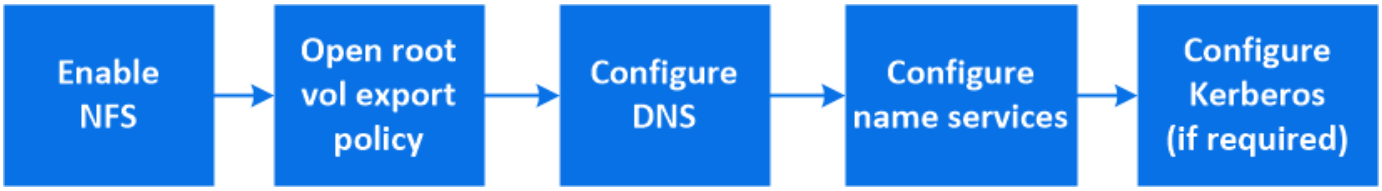
1. 显示 NFS 客户端活动：单击 * 主机 > NFS 客户端 * 。

启用 NAS 存储

使用 NFS 为 Linux 服务器启用 NAS 存储

创建或修改Storage VM、以使NFS服务器能够向Linux客户端提供数据。

此操作步骤可为新的或现有的Storage VM启用NFS协议。假定您的环境中所需的任何网络、身份验证或安全服务均提供了配置详细信息。



步骤

1. 在Storage VM上启用NFS。
   a. 对于新的Storage VM：单击*存储> Storage VM*、单击*添加*、输入Storage VM名称、然后在*SMB/CIFS、NFS、S3*选项卡中选择*启用NFS*。
      - 确认默认语言。
      - 添加网络接口。
      - 更新Storage VM管理员帐户信息(可选)。
   b. 对于现有Storage VM：单击*存储> Storage VM*、选择一个Storage VM、单击*设置*、然后单击 ⚙ 在*NFS *下。
2. 打开 Storage VM 根卷的导出策略：
   a. 单击 * 存储 > 卷 * ，选择 Storage VM 的根卷（默认为 *volume-name* _root ），然后单击 * 导出策略 * 下显示的策略。
   b. 单击 * 添加 * 以添加规则。
      - 客户端规范= `0.0.0.0/0`
      - 访问协议 = NFS
      - 访问详细信息 = UNIX 只读
3. 配置 DNS 以进行主机名解析：单击 * 存储 > 存储 VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ 在 * DNS * 下。
4. 根据需要配置名称服务。
   a. 单击 * 存储 > Storage VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ LDAP 或 NIS 。
   b. 在名称服务切换文件中包含任何更改：单击 ✎ 在名称服务切换图块中。
5. 根据需要配置 Kerberos ：

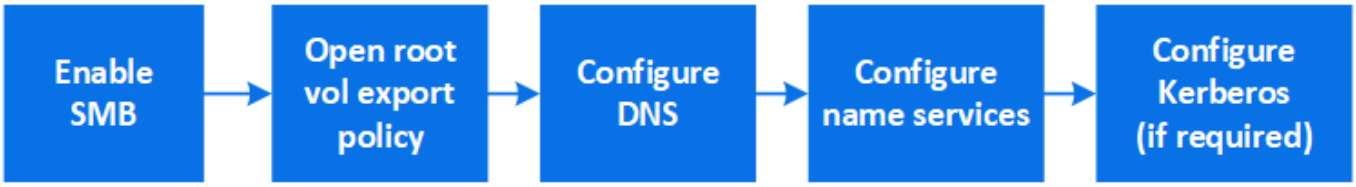
a. 单击 * 存储 > 存储 VM* ，选择此 Storage VM ，然后单击 * 设置 * 。

b. 单击 → 在 Kerberos 磁贴中，然后单击 * 添加 * 。

使用 **SMB** 为 **Windows** 服务器启用 **NAS** 存储

创建或修改Storage VM、以使SMB服务器能够向Windows客户端提供数据。

此操作步骤 可为SMB协议启用新的或现有的Storage VM。假定您的环境中所需的任何网络、身份验证或安全服务均提供了配置详细信息。



步骤

1. 在Storage VM上启用SMB。

   a. 对于新的Storage VM：单击*存储> Storage VM*、单击*添加*、输入Storage VM名称、然后在*SMB/CIFS、NFS、S3*选项卡中选择*启用SMB/CIFS *。

      - 输入以下信息：
        - 管理员名称和密码
        - 服务器名称
        - Active Directory域
      - 确认组织单位。
      - 确认DNS值。
      - 确认默认语言。
      - 添加网络接口。
      - 更新Storage VM管理员帐户信息(可选)。

   b. 对于现有Storage VM：：单击*存储> Storage VM*、选择一个Storage VM、单击*设置*、然后单击 ⚙ 在*SMB*下。

2. 打开 Storage VM 根卷的导出策略：

   a. 单击 * 存储 > 卷 * ，选择 Storage VM 的根卷（默认为 *volume-name_root* ），然后单击 * 导出策略 * 下显示的策略。

   b. 单击 * 添加 * 以添加规则。

      - 客户端规范= `0.0.0.0/0`
      - 访问协议= SMB
      - 访问详细信息= NTFS只读

3. 配置 DNS 以进行主机名解析：

   a. 单击 * 存储 > Storage VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ 在 * DNS * 下。

b. 切换到 DNS 服务器并映射 SMB 服务器。

- 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网络接口的 IP 地址。
- 如果您使用 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 服务器的数据网络接口的 IP 地址。

4. 根据需要配置名称服务

a. 单击 * 存储 > Storage VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ 在 * LDAP * 或 * NIS * 下。

b. 在名称服务切换文件中包含任何更改：单击 ✎ 在 * 名称服务开关 * 下。

5. 根据需要配置 Kerberos ：

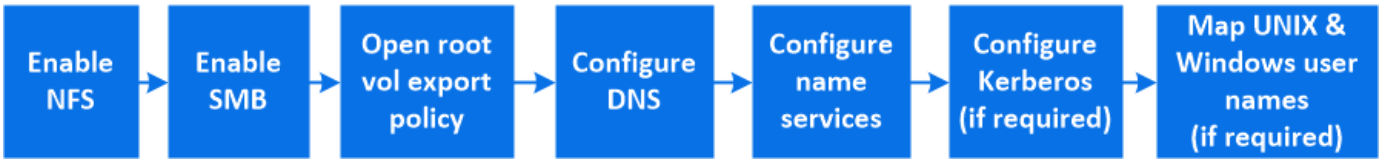
a. 单击 * 存储 > 存储 VM* ，选择此 Storage VM ，然后单击 * 设置 * 。

b. 单击 → 在 * Kerberos * 下，然后单击 * 添加 * 。

使用 **NFS** 和 **SMB** 为 **Windows** 和 **Linux** 启用 **NAS** 存储

创建或修改Storage VM、以使NFS和SMB服务器能够向Linux和Windows客户端提供数据。

通过此操作步骤 、新的或现有的Storage VM可以同时提供NFS和SMB协议。假定您的环境中所需的任何网络、身份验证或安全服务均提供了配置详细信息。



步骤

1. 在Storage VM上启用NFS和SMB。

a. 对于新的Storage VM：单击*存储> Storage VM*、单击*添加*、输入Storage VM名称、然后在*SMB/CIFS、NFS、S3*选项卡中、选择*启用SMB/CIFS 和*启用**NFS**。

- 输入以下信息：
  - 管理员名称和密码
  - 服务器名称
  - Active Directory域
- 确认组织单位。
- 确认DNS值。
- 确认默认语言。
- 添加网络接口。
- 更新Storage VM管理员帐户信息(可选)。

b. 对于现有Storage VM：单击*存储> Storage VM*、选择一个Storage VM、然后单击*设置*。如果尚未启用NFS或SMB、请完成以下子步骤。

- 单击 ⚙ 在* NFS *下。
- 单击 ⚙ 在*SMB*下。

2. 打开 Storage VM 根卷的导出策略：
   a. 单击 * 存储 > 卷 * ，选择 Storage VM 的根卷（默认为 *volume-name_root* ），然后单击 * 导出策略 * 下显示的策略。
   b. 单击 * 添加 * 以添加规则。
      - 客户端规范= `0.0.0.0/0`
      - 访问协议 = NFS
      - 访问详细信息= NFS只读
3. 配置 DNS 以进行主机名解析：
   a. 单击 * 存储 > Storage VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ 在 * DNS * 下。
   b. DNS 配置完成后，切换到 DNS 服务器并映射 SMB 服务器。
      - 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网络接口的 IP 地址。
      - 如果您使用 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 服务器的数据网络接口的 IP 地址。
4. 根据需要配置名称服务：
   a. 单击 * 存储 > Storage VM* ，选择 Storage VM ，单击 * 设置 * ，然后单击 ⚙ LDAP 或 NIS 。
   b. 在名称服务切换文件中包含任何更改：单击 ✎ 在 * 名称服务开关 * 下。
5. 根据需要配置 Kerberos ：单击 → 在 Kerberos 磁贴中，然后单击 * 添加 * 。
6. 根据需要映射 UNIX 和 Windows 用户名：单击 → 在 * 名称映射 * 下，然后单击 * 添加 * 。

   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。此操作步骤可以使用 LDAP ， NIS 或本地用户来完成。如果两组用户不匹配，则应配置名称映射。

使用命令行界面配置 NFS

使用命令行界面概述 NFS 配置

您可以使用 ONTAP 9 命令行界面命令配置 NFS 客户端对新的或现有的 Storage Virtual Machine （SVM）中新卷或 qtree 中所含文件的访问权限。

如果要按以下方式配置对卷或 qtree 的访问，请使用以下过程：

- 您希望使用 ONTAP 当前支持的任何 NFS 版本： NFSv3 ， NFSv4 ， NFSv4.1 ， NFSv4.2 或 NFSv4.1 与 pNFS 。
- 您希望使用命令行界面（CLI），而不是 System Manager 或自动化脚本编写工具。

  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。

- UNIX 文件权限将用于保护新卷的安全。
- 您拥有集群管理员权限，而不是 SVM 管理员权限。

如果要了解有关ONTAP NFS协议功能范围的详细信息、请参见 "NFS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 NFS 为 Linux 服务器配置 NAS 存储"
System Manager 经典版（适用于 ONTAP 9.7 及更早版本	"NFS 配置概述"

NFS 配置工作流

配置 NFS 包括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—配置对新的或现有 SVM 的 NFS 访问，或者向已完全配置 NFS 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 NFS 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：

相关信息

"ONTAP 概念"

评估网络连接要求

在向客户端提供 NFS 存储之前，您必须验证网络配置是否正确，以满足 NFS 配置要求。

您需要的内容

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 **NFS** 存储容量

在创建新的 NFS 卷或 qtree 之前，您必须先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 NFS 的现有 SVM 上配置卷或 qtree ，请完成 " 配置对 SVM 的 NFS 访问 " 和 " 将 NFS 存储添加到启用了 NFS 的 SVM " 中的步骤。

  配置对 SVM 的 NFS 访问

  将NFS存储添加到启用了NFS的SVM

  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 NFS 。
  - 集群中的现有 SVM 不希望启用 NFS 支持。
  - 一个集群中有一个或多个启用了 NFS 的 SVM ，您希望在一个隔离的命名空间中使用另一个 NFS 服务器（多租户情形）。
    您还应选择此选项，以便在已启用但未配置 NFS 的现有 SVM 上配置存储。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 NFS 后，继续配置卷或 qtree 。

- 如果要在已完全配置为可进行 NFS 访问的现有 SVM 上配置卷或 qtree ，请完成 " 将 NFS 存储添加到启用了 NFS 的 SVM" 中的步骤。

  将 NFS 存储添加到启用了 NFS 的 SVM

用于收集 **NFS** 配置信息的工作表

通过 NFS 配置工作表，您可以收集为客户端设置 NFS 访问所需的信息。

您应根据决定在何处配置存储来完成工作表的一个或两个部分：

如果要配置对 SVM 的 NFS 访问，应完成这两个部分。

- 配置对 SVM 的 NFS 访问
- 向启用了 NFS 的 SVM 添加存储容量

如果要向启用了NFS的SVM添加存储容量、则应仅完成以下操作：

- 向启用了 NFS 的 SVM 添加存储容量

有关参数的详细信息，请参见命令手册页。

配置对 **SVM** 的 **NFS** 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
`-vserver`	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。	
`-aggregate`	集群中具有足够空间来容纳新 NFS 存储容量的聚合的名称。	
`-rootvolume`	为 SVM 根卷提供的唯一名称。	
`-rootvolume-security-style`	对 SVM 使用 UNIX 安全模式。	`unix`
`-language`	在此工作流中使用默认语言设置。	`C.UTF-8`
`ipspace`	IP 空间是 Storage Virtual Machine（SVM）所在的不同 IP 地址空间。	

- 用于创建 NFS 服务器的参数 *

您可以在中提供这些值 `vserver nfs create` 命令。

如果要启用 NFSv4 或更高版本，则应使用 LDAP 来提高安全性。

字段	Description	您的价值

`-v3，-v4.0，-v4.1，-v4.1 -pnfs`	根据需要启用 NFS 版本。 ONTAP 9.8及更高版本也支持v4.2 `v4.1` 已启用。	
`-v4-id-domain`	ID 映射域名。	
`-v4-numeric-ids`	支持数字所有者 ID （已启用或已禁用）。	

- 用于创建 LIF* 的参数

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

如果您使用的是 Kerberos ，则应在多个 LIF 上启用 Kerberos 。

字段	Description	您的价值
`-lif`	为新 LIF 提供的名称。	
`-role`	在此工作流中使用数据 LIF 角色。	`data`
`-data-protocol`	在此工作流中仅使用 NFS 协议。	`nfs`
`-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`

- 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。	

名称服务信息

- 用于创建本地用户的参数 *

如果要创建本地用户、请使用提供以下值 `vserver services name-service unix-user create` 命令：如果要通过从统一资源标识符（ Uniform Resource Identifier ， URI ）加载包含 UNIX 用户的文件来配置本地用户，则无需手动指定这些值。

	用户名 (`-user`)	用户 ID (`-id`)	组 ID (`-primary-gid`)	全名 (`-full-name`)
示例	johnm	123.	100	John Miller
1.				
2.				
3.				
…				
不包括				

- 用于创建本地组的参数 *

如果要创建本地组、请使用提供以下值 `vserver services name-service unix-group create` 命令：如果要通过从 URI 加载包含 UNIX 组的文件来配置本地组，则无需手动指定这些值。

	组名称 (`-name`)	组 ID (`-id`)
示例	工程	100
1.		
2.		

3.		
…		
不包括		

- 用于 NIS* 的参数

您可以在中提供这些值 `vserver services name-service nis-domain create` 命令：

> 从ONTAP 9.2开始、此字段为 `-nis-servers` 替换字段 `-servers`。此新字段可以使用NIS服务器的主机名或IP地址。

字段	Description	您的价值
`-domain`	SVM 将用于名称查找的 NIS 域。	
`-active`	活动的 NIS 域服务器。	`true` 或 `false`
`-servers`	ONTAP 9.0 和 9.1： NIS 域配置使用的一个或多个 NIS 服务器 IP 地址。	
`-nis-servers`	ONTAP 9.2： 域配置所使用的 NIS 服务器的 IP 地址和主机名列表，以英文逗号分隔。	

LDAP 的 * 参数 *

您可以在中提供这些值 `vserver services name-service ldap client create` 命令：

您还需要自签名根CA证书 `.pem` 文件

> 从ONTAP 9.2开始、此字段为 `-ldap-servers` 替换字段 `-servers`。此新字段可以使用 LDAP 服务器的主机名或 IP 地址。

字段	**Description**	您的价值
`-vserver`	要为其创建 LDAP 客户端配置的 SVM 的名称。	
`-client-config`	为新 LDAP 客户端配置分配的名称。	

字段	Description	您的价值
`-servers`	ONTAP 9.0 和 9.1 ： 一个或多个 LDAP 服务器，按 IP 地址列出，以逗号分隔。	
`-ldap-servers`	ONTAP 9.2 ： LDAP 服务器的 IP 地址和主机名列表，以英文逗号分隔。	
`-query-timeout`	使用默认值 `3` 秒。	`3`
`-min-bind-level`	最小绑定身份验证级别。默认值为 `anonymous`。必须设置为 `sasl` 如果配置了签名和签章。	
`-preferred-ad-servers`	一个或多个首选 Active Directory 服务器，按 IP 地址列出，以逗号分隔。	
`-ad-domain`	Active Directory 域。	
`-schema`	要使用的模式模板。您可以使用默认模式或自定义模式。	
`-port`	使用默认LDAP服务器端口 `389` 。	`389`
`-bind-dn`	绑定用户可分辨名称。	
`-base-dn`	基本可分辨名称。默认值为 `""` (root)。	
`-base-scope`	使用默认的基本搜索范围 `subnet` 。	`subnet`
`-session-security`	启用 LDAP 签名或签名和签章。默认值为 `none`。	
`-use-start-tls`	启用基于 TLS 的 LDAP 。默认值为 `false`。	

- 用于 Kerberos 身份验证的参数 *

您可以在中提供这些值 `vserver nfs kerberos realm create` 命令：根据您使用 Microsoft Active Directory 作为密钥分发中心（ Key Distribution Center ， KDC ）服务器，还是使用 MIT 或其他 UNIX KDC 服务器，某些值会有所不同。

字段	Description	您的价值
`-vserver`	要与 KDC 通信的 SVM 。	
`-realm`	Kerberos 域。	
`-clock-skew`	客户端和服务器之间允许的时钟偏差。	
`-kdc-ip`	KDC IP 地址。	
`-kdc-port`	KDC 端口号。	
`-adserver-name`	仅限 Microsoft KDC： AD 服务器名称。	
`-adserver-ip`	仅限 Microsoft KDC： AD 服务器 IP 地址。	
`-adminserver-ip`	仅限 UNIX KDC： 管理服务器 IP 地址。	
`-adminserver-port`	仅限 UNIX KDC： 管理服务器端口号。	
`-passwordserver-ip`	仅限 UNIX KDC： 密码服务器 IP 地址。	
`-passwordserver-port`	仅限 UNIX KDC： 密码服务器端口。	
`-kdc-vendor`	KDC 供应商。	{`Microsoft` 我们可以为您提供 `Other`}
`-comment`	任何所需注释。	

您可以在中提供这些值 `vserver nfs kerberos interface enable` 命令：

字段	Description	您的价值
`-vserver`	要为其创建 Kerberos 配置的 SVM 的名称。	
`-lif`	要启用 Kerberos 的数据 LIF 。您可以在多个 LIF 上启用 Kerberos 。	

`-spn`	服务主体名称（SPN）	
`-permitted-enc-types`	基于NFS的Kerberos允许的加密类型； `aes-256` 建议使用、具体取决于客户端功能。	
`-admin-username`	用于直接从 KDC 检索 SPN 机密密钥的 KDC 管理员凭据。密码为必填项	
`-keytab-uri`	如果您没有 KDC 管理员凭据，则为 KDC 中包含 SPN 密钥的 keytab 文件。	
`-ou`	使用域为 Microsoft KDC 启用 Kerberos 时，要在其中创建 Microsoft Active Directory 服务器帐户的组织单位（OU）。	

向启用了 **NFS** 的 **SVM** 添加存储容量

- 用于创建导出策略和规则的参数 *

您可以在中提供这些值 `vserver export-policy create` 命令：

字段	Description	您的价值
`-vserver`	要托管新卷的 SVM 的名称。	
`-policyname`	为新导出策略提供的名称。	

您可以使用为每个规则提供以下值 `vserver export-policy rule create` 命令：

字段	Description	您的价值
`-clientmatch`	客户端匹配规范。	
`-ruleindex`	导出规则在规则列表中的位置。	
`-protocol`	在此工作流中使用 NFS 。	`nfs`
`-rorule`	只读访问的身份验证方法。	
`-rwrule`	读写访问的身份验证方法。	

`-superuser`	用于超级用户访问的身份验证方法。	
`-anon`	匿名用户映射到的用户 ID 。	

您必须为每个导出策略创建一个或多个规则。

-ruleindex	**-clientmatch**	**-rorule**	**-rwrule**	**-superuser**	**-anon**
示例	0.0.0.0/0 ，@rootaccess_netgroup	任意	krb5.	系统	6554
1.					
2.					
3.					
…					
不包括					

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
`-vserver`	要托管新卷的新 SVM 或现有 SVM 的名称。	
`-volume`	为新卷提供的唯一描述性名称。	
`-aggregate`	集群中具有足够空间来容纳新 NFS 卷的聚合的名称。	
`-size`	为新卷的大小提供的整数。	
`-user`	设置为卷根所有者的用户的名称或 ID 。	
`-group`	设置为卷根所有者的组的名称或 ID 。	

`--security-style`	对此工作流使用 UNIX 安全模式。	`unix`
`-junction-path`	根（/）下要挂载新卷的位置。	
`-export-policy`	如果您计划使用现有导出策略，则可以在创建卷时输入其名称。	

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
`-vserver`	包含 qtree 的卷所在 SVM 的名称。	
`-volume`	要包含新 qtree 的卷的名称。	
`-qtree`	为新 qtree 提供的唯一描述性名称，不超过 64 个字符。	
`-qtree-path`	格式的qtree路径参数 `/vol/volume_name/qtree_name\>` 可以指定、而不是将卷和qtree指定为单独的参数。	
`-unix-permissions`	可选： qtree 的 UNIX 权限。	
`-export-policy`	如果您计划使用现有导出策略，则可以在创建 qtree 时输入其名称。	

配置对 **SVM** 的 **NFS** 访问

创建 **SVM**：

如果集群中尚未至少有一个 SVM 来为 NFS 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 vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
```

ipspace_name

- 对使用UNIX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NFS。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 ipspaceA 中创建用于数据访问的 SVM：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -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: unix
                                 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 **NFS** 协议

在 SVM 上配置和使用 NFS 之前，必须验证是否已启用此协议。

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NFS协议：

     ```
     vserver add-protocols -vserver vserver_name -protocols nfs
     ```

   - 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   nfs                       cifs, fcp, iscsi, ndmp
```

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

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

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，允许所有客户端通过 NFS 进行开放访问。如果没有此规则，则会拒绝所有 NFS 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。

您应验证默认导出策略中的所有 NFS 客户端是否均可访问，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:  nfs
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 nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   如果SVM仅包含受Kerberos保护的卷、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5` 或 `krb5i`。例如：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

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

结果

现在，任何 NFS 客户端都可以访问在 SVM 上创建的任何卷或 qtree 。

创建 **NFS** 服务器

在确认NFS在集群上已获得许可后、您可以使用 `vserver nfs create` 命令以在SVM上创建NFS服务器并指定其支持的NFS版本。

关于此任务

可以将 SVM 配置为支持一个或多个 NFS 版本。如果您支持 NFSv4 或更高版本：

- NFSv4 用户 ID 映射域名在 NFSv4 服务器和目标客户端上必须相同。

  只要 NFSv4 服务器和客户端使用相同的名称，它不一定需要与 LDAP 或 NIS 域名相同。

- 目标客户端必须支持 NFSv4 数字 ID 设置。

- 出于安全原因，您应在 NFSv4 部署中使用 LDAP 提供名称服务。

开始之前

必须已将 SVM 配置为允许 NFS 协议。

步骤

1. 验证 NFS 是否已在集群上获得许可：

   ```
   system license show -package nfs
   ```

   如果不是，请联系您的销售代表。

2. 创建 NFS 服务器：

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   您可以选择启用 NFS 版本的任意组合。如果要支持pNFS、则必须同时启用这两者 `-v4.1` 和 `-v4.1-pnfs` 选项

   如果启用 v4 或更高版本，还应确保正确设置以下选项：

   - `-v4-id-domain`

     此可选参数用于指定 NFSv4 协议定义的用户名和组名称字符串形式的域部分。默认情况下，如果设置了 NIS 域，则 ONTAP 将使用 NIS 域；否则，将使用 DNS 域。您必须提供一个与目标客户端使用的域名匹配的值。

   - `-v4-numeric-ids`

     此可选参数用于指定是否在 NFSv4 所有者属性中启用对数字字符串标识符的支持。默认设置为 enabled ，但您应验证目标客户端是否支持该设置。

   您可以稍后使用启用其他NFS功能 `vserver nfs modify` 命令：

3. 验证 NFS 是否正在运行：

   ```
   vserver nfs status -vserver vserver_name
   ```

4. 验证是否已根据需要配置 NFS ：

   ```
   vserver nfs show -vserver vserver_name
   ```

示例

以下命令会在 SVM vs1 上创建一个 NFS 服务器，并启用 NFSv3 和 NFSv4.0 ：

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

以下命令用于验证名为 vs1 的新 NFS 服务器的状态和配置值：

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                  General NFS Access: true
                               NFS v3: enabled
                             NFS v4.0: enabled
                        UDP Protocol: enabled
                        TCP Protocol: enabled
                Default Windows User: -
                 NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

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。

您需要的内容

- 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 。
- 如果您使用的是 Kerberos 身份验证，请在多个 LIF 上启用 Kerberos 。
- 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。

从 ONTAP 9.4 开始，支持 FC-NVMe 。如果要创建 FC-NVMe LIF ，应注意以下事项：

- 创建 LIF 的 FC 适配器必须支持 NVMe 协议。
- FC-NVMe 可以是数据 LIF 上的唯一数据协议。
- 必须为支持 SAN 的每个 Storage Virtual Machine （ SVM ）配置一个 LIF 处理管理流量。
- NVMe LIF 和命名空间必须托管在同一节点上。
- 每个 SVM 只能配置一个处理数据流量的 NVMe LIF 。

步骤

1. 创建 LIF：

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -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}
   ```

选项	Description
• ONTAP 9.5 及更早版本 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -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 *vserver_name* -lif *lif_name* -role data -data-protocol nfs -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` 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。

     。 `-data-protocol` 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。

   - `-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 `false` 具体取决于您环境中的网络管理策略。

2. 使用验证是否已成功创建LIF `network interface show` 命令：
3. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

4. 如果使用的是 Kerberos ，请重复步骤 1 到 3 以创建其他 LIF 。

   必须在每个 LIF 上单独启用 Kerberos 。

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 nfs -home-node node-4 -home-port e1c -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 nfs -home-node node-3 -home-port e1c -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

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            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
true
node-2
            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
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

以下命令显示如何创建分配给的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。

您需要的内容

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
                                                Name
   Vserver           State     Domains             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
```

配置名称服务

配置名称服务概述

根据存储系统的配置， ONTAP 需要能够查找主机，用户，组或网络组信息，以便能够正确访问客户端。您必须配置名称服务，以使 ONTAP 能够访问本地或外部名称服务来获取此信息。

您应使用 NIS 或 LDAP 等名称服务在客户端身份验证期间便于进行名称查找。为了提高安全性，最好尽可能使用 LDAP ，尤其是在部署 NFSv4 或更高版本时。如果外部名称服务器不可用，您还应配置本地用户和组。

名称服务信息必须在所有源上保持同步。

配置名称服务切换表

您必须正确配置名称服务切换表，以使 ONTAP 能够查询本地或外部名称服务以检索主机，用户，组，网络组或名称映射信息。

您需要的内容

您必须已根据环境情况确定要用于主机，用户，组，网络组或名称映射的名称服务。

如果您计划使用网络组，则网络组中指定的所有 IPv6 地址都必须按照 RFC 5952 中的说明进行缩短和压缩。

关于此任务

请勿包含未使用的信息源。例如、如果您的环境未使用NIS、请勿指定 `-sources nis` 选项

步骤

1. 将必要的条目添加到名称服务切换表：

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. 验证名称服务切换表是否包含所需顺序的预期条目：

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   如果要进行任何更正、必须使用 `vserver services name-service ns-switch modify` 或 `vserver services name-service ns-switch delete` 命令

示例

以下示例将在名称服务切换表中为 SVM vs1 创建一个新条目，以便使用本地网络组文件和外部 NIS 服务器按此顺序查找网络组信息：

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完成后

- 您必须配置为 SVM 指定的名称服务以提供数据访问。
- 如果您删除了 SVM 的任何名称服务，则还必须将其从名称服务切换表中删除。

  如果无法从名称服务切换表中删除名称服务，则客户端对存储系统的访问可能无法按预期工作。

配置本地 **UNIX** 用户和组

配置本地 **UNIX** 用户和组概述

您可以在 SVM 上使用本地 UNIX 用户和组进行身份验证和名称映射。您可以手动创建 UNIX 用户和组，也可以通过统一资源标识符（ Uniform Resource Identifier ， URI ）加载包含 UNIX 用户或组的文件。

默认情况下，集群中本地 UNIX 用户组和组成员的组合上限为 32 ， 768 。集群管理员可以修改此限制。

创建本地 **UNIX** 用户

您可以使用 `vserver services name-service unix-user create` 命令以创建本地UNIX用户。本地 UNIX 用户是指您在 SVM 上创建的 UNIX 用户，该用户作为 UNIX 名称服务选项，用于处理名称映射。

步骤

1. 创建本地 UNIX 用户：

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user`

user_name -id *integer* -primary-gid *integer* -full-name *full_name*

-user *user_name* 指定用户名。用户名长度不能超过 64 个字符。

-id *integer* 指定您分配的用户ID。

-primary-gid *integer* 指定主组ID。此操作会将用户添加到主组。创建用户后，您可以手动将该用户添加到任何所需的其他组。

示例

以下命令会在名为 vs1 的 SVM 上创建一个名为 johnm （全名为 "John Miller" ）的本地 UNIX 用户。用户的 ID 为 123 ，主组 ID 为 100 。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

从 **URI** 加载本地 **UNIX** 用户

除了在SVM中手动创建单个本地UNIX用户之外、您还可以通过统一资源标识符(URI)将本地UNIX用户列表加载到SVM中、从而简化此任务。（vserver services name-service unix-user load-from-uri）。

步骤

1. 创建一个包含要加载的本地 UNIX 用户列表的文件。

   文件必须包含UNIX中的用户信息 /etc/passwd 格式：

   user_name: password: user_ID: group_ID: full_name

   命令将丢弃的值 *password* 字段以及后面字段的值 *full_name* 字段 (*home_directory* 和 *shell*）。

   支持的最大文件大小为 2.5 MB 。

2. 验证此列表是否不包含任何重复信息。

   如果此列表包含重复条目，则加载此列表将失败并显示错误消息。

3. 将文件复制到服务器。

   存储系统必须可通过 HTTP ， HTTPS ， FTP 或 FTPS 访问此服务器。

4. 确定文件的 URI 。

   此 URI 是您为存储系统提供的地址，用于指示文件的位置。

5. 从 URI 将包含本地 UNIX 用户列表的文件加载到 SVM 中：

   vserver services name-service unix-user load-from-uri -vserver *vserver_name*

`-uri {ftp|http|ftps|https}://uri -overwrite {true|false}`

`-overwrite {true false}`指定是否覆盖条目。默认值为 `false`。

示例

以下命令将从URI加载本地UNIX用户列表 `ftp://ftp.example.com/passwd` 到名为VS1的SVM中。SVM 上的现有用户不会被 URI 中的信息覆盖。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

创建本地 **UNIX** 组

您可以使用 `vserver services name-service unix-group create` 命令创建SVM的本地UNIX组。本地 UNIX 组用于本地 UNIX 用户。

步骤

1. 创建本地 UNIX 组：

   `vserver services name-service unix-group create -vserver vserver_name -name group_name -id integer`

   `-name group_name` 指定组名称。组名称长度不能超过 64 个字符。

   `-id integer` 指定您分配的组ID。

示例

以下命令会在名为 vs1 的 SVM 上创建一个名为 eng 的本地组。此组的 ID 为 101 。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

将用户添加到本地 **UNIX** 组

您可以使用 `vserver services name-service unix-group adduser` 命令将用户添加到SVM本地的补充UNIX组。

步骤

1. 将用户添加到本地 UNIX 组：

`vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name`

`-name group_name` 指定除用户的主组之外要将用户添加到的UNIX组的名称。

示例

以下命令会将名为 max 的用户添加到名为 vs1 的 SVM 上名为 eng 的本地 UNIX 组：

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

从 **URI** 加载本地 **UNIX** 组

除了手动创建单个本地UNIX组之外、您还可以使用从统一资源标识符(uniual resource ID标识 符、URI)将本地UNIX组列表加载到SVM中 `vserver services name-service unix-group load-from-uri` 命令：

步骤

1. 创建一个包含要加载的本地 UNIX 组列表的文件。

   文件必须包含UNIX中的组信息 `/etc/group` 格式：

   `group_name: password: group_ID: comma_separated_list_of_users`

   命令将丢弃的值 *`password`* 字段。

   支持的最大文件大小为1 MB。

   组文件中每行的最大长度为 32 ， 768 个字符。

2. 验证此列表是否不包含任何重复信息。

   此列表不得包含重复条目，否则加载此列表将失败。如果SVM中已存在条目、则必须设置 `-overwrite` 参数设置为 `true` 使用新文件覆盖所有现有条目、或者确保新文件不包含与现有条目重复的任何条目。

3. 将文件复制到服务器。

   存储系统必须可通过 HTTP ， HTTPS ， FTP 或 FTPS 访问此服务器。

4. 确定文件的 URI 。

   此 URI 是您为存储系统提供的地址，用于指示文件的位置。

5. 从 URI 将包含本地 UNIX 组列表的文件加载到 SVM 中：

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`}指定是否覆盖条目。默认值为 `false`。如果将此参数指定为 `true`，ONTAP将使用您正在加载的文件中的条目替换指定SVM的整个现有本地UNIX组数据库。

示例

以下命令将从URI加载本地UNIX组的列表 `ftp://ftp.example.com/group` 到名为VS1的SVM中。SVM上的现有组不会被 URI 中的信息覆盖。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

使用网络组

使用网络组概述

您可以使用网络组进行用户身份验证，并在导出策略规则中匹配客户端。您可以通过外部名称服务器(LDAP或NIS)提供对网络组的访问权限、也可以使用将网络组从统一资源标识符(URI)加载到SVM中 `vserver services name-service netgroup load` 命令：

您需要的内容

在使用网络组之前，您必须确保满足以下条件：

- 网络组中的所有主机，无论源（ NIS ， LDAP 或本地文件）如何，都必须同时具有正向（ A ）和反向（ PTR ） DNS 记录，才能提供一致的正向和反向 DNS 查找。

  此外，如果客户端的 IP 地址具有多个 PTR 记录，则所有这些主机名都必须是网络组的成员并具有相应的 A 记录。

- 网络组中所有主机的名称，无论其源（ NIS ， LDAP 或本地文件）如何，都必须拼写正确，并使用正确的大小写。网络组中使用的主机名大小写不一致可能导致意外行为，例如导出检查失败。
- 网络组中指定的所有 IPv6 地址都必须按照 RFC 5952 中的说明进行缩短和压缩。

  例如， 2011： hu9： 0： 0： 0： 0： 3： 1 必须缩短为 2011： hu9：： 3： 1 。

关于此任务

使用网络组时，您可以执行以下操作：

- 您可以使用 `vserver export-policy netgroup check-membership` 命令、以帮助确定客户端IP是否为某个网络组的成员。
- 您可以使用 `vserver services name-service getxxbyyy netgrp` 命令以检查客户端是否属于网络组。

  系统将根据配置的名称服务切换顺序选择用于执行查找的底层服务。

将网络组加载到 **SVM** 中

在导出策略规则中匹配客户端的方法之一是使用网络组中列出的主机。除了使用存储在外部名称服务器中的网络组之外、您还可以将网络组从统一资源标识符(URI)加载到SVM中（`vserver services name-service netgroup load`）。

您需要的内容

在加载到 SVM 之前，网络组文件必须满足以下要求：

- 该文件必须使用用于填充 NIS 的正确网络组文本文件格式。

  ONTAP 会在加载网络组文本文件格式之前对其进行检查。如果文件包含错误，则不会加载该文件，并且会显示一条消息，指示您必须在该文件中执行的更正。更正错误后，您可以将网络组文件重新加载到指定的 SVM 中。

- 网络组文件中主机名中的任何字母字符都应小写。
- 支持的最大文件大小为5 MB。
- 支持的嵌套网络组的最大级别为 1000 。
- 在网络组文件中定义主机名时，只能使用主 DNS 主机名。

  为了避免导出访问问题，不应使用 DNS CNAME 或轮循记录定义主机名。

- 网络组文件中三个组的用户和域部分应保留为空，因为 ONTAP 不支持它们。

  仅支持主机 /IP 部分。

关于此任务

ONTAP 支持按主机搜索本地网络组文件。加载网络组文件后， ONTAP 会自动创建 netgroup.byHost 映射以启用按主机搜索网络组。在处理导出策略规则以评估客户端访问时，这可以显著加快本地网络组搜索的速度。

步骤

1. 从 URI 将网络组加载到 SVM：

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   加载网络组文件并构建 netgroup.byHost 映射可能需要几分钟的时间。

   如果要更新网络组，您可以编辑该文件并将更新后的网络组文件加载到 SVM 中。

示例

以下命令会通过HTTP URL将网络组定义加载到名为VS1的SVM中 `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

验证网络组定义的状态

将网络组加载到SVM后、您可以使用 `vserver services name-service netgroup status` 命令以验证网络组定义的状态。这样，您就可以确定支持 SVM 的所有节点上的网络组定义是否一致。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 验证网络组定义的状态：

   ```
   vserver services name-service netgroup status
   ```

   您可以在更详细的视图中显示追加信息。

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

设置权限级别后，以下命令将显示所有 SVM 的网络组状态：

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- --------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

创建 **NIS** 域配置

如果您的环境使用网络信息服务(Network Information Service、NIS)提供名称服务、则必须使用为SVM创建NIS域配置 `vserver services name-service nis-domain create` 命令：

您需要的内容

在 SVM 上配置 NIS 域之前，所有已配置的 NIS 服务器都必须可用且可访问。

如果计划使用 NIS 进行目录搜索，则 NIS 服务器中的映射每个条目不能超过 1 ， 024 个字符。请勿指定不符合此限制的 NIS 服务器。否则，依赖于 NIS 条目的客户端访问可能会失败。

关于此任务

您可以创建多个 NIS 域。但是、您只能使用设置为的 `active`。

如果NIS数据库包含 `netgroup.byhost` 地图、ONTAP可以使用它加快搜索速度。。 `netgroup.byhost` 和 `netgroup` 目录中的映射必须始终保持同步、以避免出现客户端访问问题。从ONTAP 9.7开始、为NIS `netgroup.byhost` 可以使用缓存条目 `vserver services name-service nis-domain netgroup-database` 命令

不支持使用NIS进行主机名解析。

步骤

1. 创建 NIS 域配置：

   `vserver services name-service nis-domain create -vserver vs1 -domain` *`domain_name`* `-active true` *`-servers IP_addresses`*

   最多可以指定 10 个 NIS 服务器。

   > 从ONTAP 9.2开始、此字段为 `-nis-servers` 替换字段 `-servers`。此新字段可以使用NIS服务器的主机名或IP地址。

2. 验证是否已创建域：

   `vserver services name-service nis-domain show`

示例

以下命令将在 SVM vs1 上为 NIS 域 nisdomain 创建 NIS 域配置并使其处于活动状态，并且 NIS 服务器的 IP 地址为 192.0.2.180 ：

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

使用 LDAP

LDAP 使用概述

如果在您的环境中使用 LDAP 提供名称服务，则需要与 LDAP 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 LDAP 客户端启用。

从 ONTAP 9.10.1 开始，默认情况下， Active Directory 和名称服务 LDAP 连接均支持 LDAP 通道绑定。只有在启用了 Start-TLS 或 LDAPS 且会话安全设置为 sign 或 seal 的情况下， ONTAP 才会尝试使用 LDAP 连接进行通道绑定。要禁用或重新启用与名称服务器的LDAP通道绑定、请使用 `-try-channel-binding` 参数 `ldap client modify` 命令：

有关详细信息，请参见
"2020 年 Windows 的 LDAP 通道绑定和 LDAP 签名要求"。

- 在为 ONTAP 配置 LDAP 之前，您应验证站点部署是否符合 LDAP 服务器和客户端配置的最佳实践。具体而言，必须满足以下条件：
  - LDAP 服务器的域名必须与 LDAP 客户端上的条目匹配。
  - LDAP 服务器支持的 LDAP 用户密码哈希类型必须包括 ONTAP 支持的类型：
    - 加密（所有类型）和 SHA-1 （ SHA ， SSHA ）。
    - 从 ONTAP 9.8 开始， SHA-2 哈希（ SHA-256 ， SSH/384 ， SHA-512 ， SSHA-256 ， SSHA-384 和 SSHA-512 ）。
  - 如果 LDAP 服务器需要会话安全措施，则必须在 LDAP 客户端中配置这些措施。

    可以使用以下会话安全选项：

    - LDAP 签名（提供数据完整性检查）和 LDAP 签名和签章（提供数据完整性检查和加密）
    - START TLS
    - LDAPS （基于 TLS 或 SSL 的 LDAP ）
  - 要启用签名和签章的 LDAP 查询，必须配置以下服务：
    - LDAP 服务器必须支持 GSSAPI （ Kerberos ） SASL 机制。
    - LDAP 服务器必须在 DNS 服务器上设置 DNS A/AAAA 记录以及 PTR 记录。
    - Kerberos 服务器必须在 DNS 服务器上存在 SRV 记录。
  - 要启用启动 TLS 或 LDAPS ，应考虑以下几点。
    - NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。
    - 如果使用 LDAPS ，则必须在 ONTAP 9.5 及更高版本中为 TLS 或 SSL 启用 LDAP 服务器。ONTAP 9.09.4 不支持 SSL 。
    - 必须已在域中配置证书服务器。
  - 要启用 LDAP 转介跟踪（在 ONTAP 9.5 及更高版本中），必须满足以下条件：
    - 这两个域都应配置以下信任关系之一：
      - 双向
      - 单向，主站点信任转介域
      - 父 - 子
    - 必须配置 DNS 以解析所有转介的服务器名称。
    - 当 -bind-as-cifs-server 设置为 true 时，域密码应相同以进行身份验证。

LDAP 转介跟踪不支持以下配置。

- 对于所有 ONTAP 版本：
  - 管理 SVM 上的 LDAP 客户端
- 对于 ONTAP 9.8 及更早版本（ 9.9.1 及更高版本支持这些功能）：
  - LDAP签名和签章(`-session-security` 选项)
  - 加密TLS连接(`-use-start-tls` 选项)
  - 通过LAPS端口636 (`-use-ldaps-for-ad-ldap` 选项)

- 在 SVM 上配置 LDAP 客户端时，必须输入 LDAP 模式。

  在大多数情况下，默认 ONTAP 模式之一是合适的。但是，如果环境中的 LDAP 模式与这些模式不同，则必须在创建 LDAP 客户端之前为 ONTAP 创建新的 LDAP 客户端模式。有关您的环境要求，请咨询 LDAP 管理员。

- 不支持使用 LDAP 进行主机名解析。

有关详细信息 ...

- "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"
- "在 SVM 上安装自签名根 CA 证书"

创建新的 **LDAP** 客户端模式

如果环境中的 LDAP 模式与 ONTAP 默认值不同，则必须在创建 LDAP 客户端配置之前为 ONTAP 创建新的 LDAP 客户端模式。

关于此任务

大多数 LDAP 服务器都可以使用 ONTAP 提供的默认模式：

- MS-AD-BIS （大多数 Windows 2012 及更高版本 AD 服务器的首选架构）
- AD-IDMU （ Windows 2008 ， Windows 2012 及更高版本的 AD 服务器）
- AD-SFU （ Windows 2003 及更早版本的 AD 服务器）
- RFC-2307 （ UNIX LDAP 服务器）

如果需要使用非默认 LDAP 模式，则必须在创建 LDAP 客户端配置之前创建该模式。在创建新模式之前，请咨询 LDAP 管理员。

无法修改 ONTAP 提供的默认 LDAP 模式。要创建新模式，请创建一个副本，然后相应地修改该副本。

步骤

1. 显示现有 LDAP 客户端模式模板以确定要复制的模板：

   ```
   vserver services name-service ldap client schema show
   ```

2. 将权限级别设置为高级：

```
set -privilege advanced
```

3. 为现有 LDAP 客户端模式创建副本：

```
vserver services name-service ldap client schema copy -vserver vserver_name
-schema existing_schema_name -new-schema-name new_schema_name
```

4. 修改新架构并根据您的环境对其进行自定义：

```
vserver services name-service ldap client schema modify
```

5. 返回到管理权限级别：

```
set -privilege admin
```

创建 **LDAP** 客户端配置

如果您希望ONTAP访问您环境中的外部LDAP或Active Directory服务、则需要先在存储系统上设置LDAP客户端。

您需要的内容

Active Directory域解析列表中前三个服务器之一必须已启动并提供数据。否则，此任务将失败。

> 有多个服务器、其中在任意时间点有两个以上的服务器停机。

步骤

1. 请咨询LDAP管理员以确定的适当配置值 `vserver services name-service ldap client create` 命令：

   a. 指定与 LDAP 服务器的基于域或基于地址的连接。

      。 `-ad-domain` 和 `-servers` 选项不能同时使用。

      - 使用 `-ad-domain` 选项以在Active Directory域中启用LDAP服务器发现。
        - 您可以使用 `-restrict-discovery-to-site` 用于将LDAP服务器发现限制为指定域的CIFS默认站点的选项。如果使用此选项、则还需要使用指定CIFS默认站点 `-default-site`。
      - 您可以使用 `-preferred-ad-servers` 此选项可按IP地址在逗号分隔列表中指定一个或多个首选Active Directory服务器。创建客户端后、您可以使用修改此列表 `vserver services name-service ldap client modify` 命令：
      - 使用 `-servers` 可选择通过IP地址在逗号分隔列表中指定一个或多个LDAP服务器(Active Directory或UNIX)。

      > 。 `-servers` 选项在ONTAP 9.2中已弃用。从ONTAP 9.2开始、 `-ldap-servers` 字段将取代 `-servers` 字段。此字段可以使用LDAP服务器的主机名或IP地址。

   b. 指定默认或自定义 LDAP 模式。

      大多数 LDAP 服务器都可以使用 ONTAP 提供的默认只读模式。除非另有要求，否则最好使用这些默认

模式。如果是，您可以通过复制默认模式（默认模式为只读）并修改副本来创建自己的模式。

默认模式：

- MS-AD-BIS

  此模式基于 RFC-2307bis ，是大多数标准 Windows 2012 及更高版本 LDAP 部署的首选 LDAP 模式。

- `AD-IDMU`

  此模式基于适用于 UNIX 的 Active Directory 身份管理，适用于大多数 Windows 2008 ， Windows 2012 及更高版本的 AD 服务器。

- `AD-SFU`

  此模式基于适用于 UNIX 的 Active Directory 服务，适用于大多数 Windows 2003 及更早版本的 AD 服务器。

- `RFC-2307`

  根据 RFC-2307 （使用 LDAP 作为网络信息服务的方法 _ ），此模式适用于大多数 UNIX AD 服务器。

c. 选择绑定值。

- `-min-bind-level {anonymous|simple|sasl}` 指定最低绑定身份验证级别。

  默认值为 **anonymous**。

- `-bind-dn` *`LDAP_DN`* 指定绑定用户。

  对于 Active Directory 服务器，您必须在帐户（域 \ 用户）或主体（ user@domain.com ）表单中指定用户。否则，您必须以可分辨名称（ CN=user ， DC=domain ， DC=com ）形式指定用户。

- `-bind-password` *`password`* 指定绑定密码。

d. 如果需要，选择会话安全选项。

如果 LDAP 服务器需要，您可以启用 LDAP 签名和签章或基于 TLS 的 LDAP 。

- `--session-security {none|sign|seal}`

  您可以启用签名 (`sign`、数据完整性)、签名和签章 (`seal``数据完整性和加密)、或者两者都不是`none`，无签名或签章)。默认值为 `none`。

  您还应设置 `-min-bind-level {sasl}`，除非您希望绑定身份验证回退到 **anonymous** 或 **simple** 签名和签章绑定失败时。

- `-use-start-tls {true|false}`

  如果设置为 **true** 如果LDAP服务器支持此功能、则LDAP客户端将使用加密TLS连接连接到该服务器。默认值为 **false**。要使用此选项，您必须安装 LDAP 服务器的自签名根 CA 证书。

> 如果Storage VM已将SMB服务器添加到域中、并且LDAP服务器是SMB服务器主域的域控制器之一、则可以修改 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

e. 选择端口，查询和基本值。

建议使用默认值，但您必须向 LDAP 管理员确认这些值适合您的环境。

- `-port` *`port`* 指定LDAP服务器端口。

  默认值为 `389`。

如果您计划使用 Start TLS 来保护 LDAP 连接，则必须使用默认端口 389 。启动 TLS 以 LDAP 默认端口 389 上的纯文本连接开头，然后该连接升级到 TLS 。如果更改此端口，则启动 TLS 将失败。

- `-query-timeout` *`integer`* 指定查询超时(以秒为单位)。

  允许的范围为 1 到 10 秒。默认值为 `3` 秒。

- `-base-dn` *`LDAP_DN`* 指定基础DN。

  如果需要，可以输入多个值（例如，如果启用了 LDAP 转介跟踪）。默认值为 `""` (root)。

- `-base-scope` {`base`|`onelevel`|`subtree`}指定基本搜索范围。

  默认值为 `subtree`。

- `-referral-enabled` {`true`|`false`}指定是否启用LDAP转介跟踪。

  从 ONTAP 9.5 开始，如果主 LDAP 服务器返回 LDAP 转介响应，指示转介的 LDAP 服务器上存在所需记录，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。默认值为 **`false`**。

要搜索转介 LDAP 服务器中的记录，必须在 LDAP 客户端配置中将转介记录的基础 DN 添加到基础 DN 中。

2. 在Storage VM上创建LDAP客户端配置：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> 创建LDAP客户端配置时、必须提供Storage VM名称。

3. 验证是否已成功创建 LDAP 客户端配置：

```
vserver services name-service ldap client show -client-config
client_config_name
```

示例

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与适用于LDAP的Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要签名和签章的LDAP的Active Directory服务器配合使用、并且LDAP服务器发现仅限于指定域的特定站点：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要LDAP转介跟踪的LDAP Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

以下命令通过指定基础DN来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

以下命令通过启用转介跟踪来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

将 **LDAP** 客户端配置与 **SVM** 关联

要在SVM上启用LDAP、必须使用 `vserver services name-service ldap create` 命令将LDAP客户端配置与SVM关联。

您需要的内容

- LDAP 域必须已存在于网络中，并且必须可供 SVM 所在的集群访问。
- SVM 上必须存在 LDAP 客户端配置。

步骤

1. 在SVM上启用LDAP：

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > 从ONTAP 9.2开始、 `vserver services name-service ldap create` 命令会执行自动配置验证、并在ONTAP无法联系名称服务器时报告错误消息。

   以下命令将在 vs1" SVM 上启用 LDAP ，并将其配置为使用 "ldap1" LDAP 客户端配置：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用 vserver services name-service ldap check 命令验证名称服务器的状态。

   以下命令将验证 SVM vs1. 上的 LDAP 服务器。

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                |
   | Client Configuration Name: c1                               |
   | LDAP Status: up                                             |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                              |
   ```

   从 ONTAP 9.2 开始，可以使用 name service check 命令。

在名称服务切换表中验证 **LDAP** 源

您必须验证 SVM 的名称服务切换表中是否正确列出了名称服务的 LDAP 源。

步骤

1. 显示当前名称服务切换表内容：

   `vserver services name-service ns-switch show -vserver` *`svm_name`*

以下命令显示 SVM My_SVM 的结果：

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

`namemap` 指定要搜索名称映射信息的源及其顺序。在纯 UNIX 环境中，不需要此条目。只有同时使用 UNIX 和 Windows 的混合环境才需要名称映射。

2. 更新 `ns-switch` 根据需要输入：

要更新 **ns-switch** 条目的项	输入命令 ...
用户信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
网络组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

将 **Kerberos** 与 **NFS** 结合使用可增强安全性

将 **Kerberos** 与 **NFS** 结合使用以增强安全性的概述

如果在您的环境中使用 Kerberos 进行强身份验证，则需要与 Kerberos 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 Kerberos 客户端启用。

您的环境应符合以下准则：

- 在为 ONTAP 配置 Kerberos 之前，您的站点部署应遵循 Kerberos 服务器和客户端配置的最佳实践。
- 如果需要 Kerberos 身份验证，请尽可能使用 NFSv4 或更高版本。

  NFSv3 可与 Kerberos 结合使用。但是，只有在 NFSv4 或更高版本的 ONTAP 部署中，才会充分发挥

Kerberos 的全部安全优势。

- 要提高冗余服务器访问能力，应在使用同一 SPN 的集群中多个节点上的多个数据 LIF 上启用 Kerberos 。
- 在 SVM 上启用 Kerberos 时，必须根据 NFS 客户端配置在卷或 qtree 的导出规则中指定以下安全方法之一。
  - `krb5` (Kerberos v5协议)
  - `krb5i` (使用校验和进行完整性检查的Kerberos v5协议)
  - `krb5p` (具有隐私服务的Kerberos v5协议)

除了 Kerberos 服务器和客户端之外，还必须为 ONTAP 配置以下外部服务以支持 Kerberos ：

- 目录服务

  您应在环境中使用安全目录服务，例如 Active Directory 或 OpenLDAP ，该服务配置为使用基于 SSL/TLS 的 LDAP 。请勿使用 NIS ，因为其请求会以明文形式发送，因此不安全。

- NTP

  您必须有一个运行 NTP 的工作时间服务器。为了防止因时间偏差而导致 Kerberos 身份验证失败，必须执行此操作。

- 域名解析（ DNS ）

  每个 UNIX 客户端和每个 SVM LIF 都必须在正向和反向查找区域下向 KDC 注册正确的服务记录（ SRV ）。所有参与者都必须可通过 DNS 正确解析。

验证 **Kerberos** 配置的权限

Kerberos 要求为 SVM 根卷以及本地用户和组设置某些 UNIX 权限。

步骤

1. 显示 SVM 根卷上的相关权限：

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   SVM 的根卷必须具有以下配置：

名称	正在设置 ...
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	755

   如果未显示这些值、请使用 `volume modify` 命令进行更新。

2. 显示本地 UNIX 用户：

`vserver services name-service unix-user show -vserver vserver_name`

SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS 初始化阶段需要此项。 NFS 客户端用户 SPN 的第一个组件用作用户。 如果 NFS 客户端用户的 SPN 存在 Kerberos-UNIX 名称映射，则不需要 NFS 用户。
root	0	0	挂载时需要。

如果未显示这些值、则可以使用 `vserver services name-service unix-user modify` 命令进行更新。

3. 显示本地 UNIX 组：

   `vserver services name-service unix-group show -vserver vserver _name`

   SVM 必须配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0

如果未显示这些值、则可以使用 `vserver services name-service unix-group modify` 命令进行更新。

创建 **NFS Kerberos** 域配置

如果您希望 ONTAP 访问环境中的外部 Kerberos 服务器，则必须先将 SVM 配置为使用现有 Kerberos 域。为此、您需要收集Kerberos KDC服务器的配置值、然后使用 `vserver nfs kerberos realm create` 命令以在SVM上创建Kerberos域配置。

您需要的内容

集群管理员应已在存储系统，客户端和 KDC 服务器上配置 NTP ，以避免出现身份验证问题。客户端和服务器之间的时间差异（时钟偏差）是常见的身份验证失败发生原因。

步骤

1. 请咨询Kerberos管理员以确定要为提供的适当配置值 `vserver nfs kerberos realm create` 命令：

2. 在 SVM 上创建 Kerberos 域配置：

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. 验证是否已成功创建 Kerberos 域配置：

   ```
   vserver nfs kerberos realm show
   ```

示例

以下命令将为 SVM vs1 创建一个 NFS Kerberos 域配置，该配置使用 Microsoft Active Directory 服务器作为 KDC 服务器。Kerberos 域为 AUTH.EXAMPLE.COM 。Active Directory 服务器名为 AD-1 ，其 IP 地址为 10.10.8.14 。允许的时钟偏差为 300 秒（默认值）。KDC 服务器的 IP 地址为 10.10.8.14 ，其端口号为 88 （默认值）。"Microsoft Kerberos config" 是注释。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

以下命令将为使用 MIT KDC 的 SVM vs1 创建 NFS Kerberos 域配置。Kerberos 域为 SECURITY.EXAMPLE.COM 。允许的时钟偏差为 300 秒。KDC 服务器的 IP 地址为 10.10.9.1 ，端口号为 88 。KDC 供应商为 "Other" ，表示 UNIX 供应商。管理服务器的 IP 地址为 10.10.9.1 ，端口号为 749 （默认值）。密码服务器的 IP 地址为 10.10.9.1 ，端口号为 464 （默认值）。"UNIX Kerberos config" 是注释。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

配置 NFS Kerberos 允许的加密类型

默认情况下， ONTAP 支持以下 NFS Kerberos 加密类型： DES ， 3DES ， AES-128 和 AES-256 。您可以使用为每个SVM配置允许的加密类型、以满足特定环境的安全要求 `vserver nfs modify` 命令 `-permitted-enc-types` 参数。

关于此任务

为了最大程度地实现客户端兼容性， ONTAP 默认同时支持弱 DES 和强 AES 加密。例如，这意味着，如果您要提高安全性，并且您的环境支持此安全性，则可以使用此操作步骤禁用 DES 和 3DES ，并要求客户端仅使用 AES 加密。

您应使用可用的最强加密。对于 ONTAP ，即 AES-256 。您应向 KDC 管理员确认您的环境支持此加密级别。

- 在 SVM 上完全启用或禁用 AES （AES-128 和 AES-256 ）会造成中断，因为它会销毁原始 DES 主体 /keytab 文件，从而要求在 SVM 的所有 LIF 上禁用 Kerberos 配置。

  在进行此更改之前，您应验证 NFS 客户端是否不依赖于 SVM 上的 AES 加密。

- 启用或禁用 DES 或 3DES 不需要对 LIF 上的 Kerberos 配置进行任何更改。

步骤

1. 启用或禁用所需的允许加密类型：

要启用或禁用的项	请按照以下步骤操作 ...
DES 或 3DES	a. 配置SVM的NFS Kerberos允许的加密类型： `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 使用逗号分隔多种加密类型。 b. 验证更改是否成功： `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

要启用或禁用的项	请按照以下步骤操作 ...

AES-128或AES-256	a. 确定启用了Kerberos的SVM和LIF：
	
	`vserver nfs kerberos interface show`
	
	b. 在要修改NFS Kerberos允许的加密类型的SVM上的所有SVM上禁用Kerberos：
	
	`vserver nfs kerberos interface disable -lif lif_name`
	
	c. 配置SVM的NFS Kerberos允许的加密类型：
	
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	使用逗号分隔多种加密类型。
	
	d. 验证更改是否成功：
	
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	
	e. 在SVM上的所有SVM上重新启用Kerberos：
	
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	
	f. 验证是否已在所有生命周期管理器上启用Kerberos：
	
	`vserver nfs kerberos interface show`

在数据 **LIF** 上启用 **Kerberos**

您可以使用 `vserver nfs kerberos interface enable` 命令以对数据LIF启用Kerberos。这样， SVM 就可以对 NFS 使用 Kerberos 安全服务。

关于此任务

如果您使用的是 Active Directory KDC ，则所使用的任何 SPN 的前 15 个字符必须在域或域中的 SVM 之间是唯一的。

步骤

1. 创建 NFS Kerberos 配置：

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

ONTAP 需要 KDC 中 SPN 的机密密钥才能启用 Kerberos 接口。

对于 Microsoft KDC ，将联系 KDC ，并在命令行界面上发出用户名和密码提示以获取机密密钥。如果需要在Kerberos域的其他OU中创建SPN、则可以指定可选 `-ou` 参数。

对于非 Microsoft KDC ，可以使用以下两种方法之一获取机密密钥：

如果您 ...	您还必须在命令中包含以下参数 ...
拥有 KDC 管理员凭据，以便直接从 KDC 检索密钥	`-admin-username` *`kdc_admin_username`*
没有 KDC 管理员凭据，但具有包含此密钥的 KDC 中的 keytab 文件	`-keytab-uri` {ftp-http} ： //*`uri`*

2. 验证是否已在 LIF 上启用 Kerberos：

   ```
   vserver nfs kerberos-config show
   ```

3. 重复步骤 1 和 2 ，在多个 LIF 上启用 Kerberos 。

示例

以下命令将在逻辑接口 ves03-d1 上为名为 vs1 的 SVM 创建并验证 NFS Kerberos 配置，并在 OU lab2ou 中使用 SPN NFS/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM：

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

向启用了 **NFS** 的 **SVM** 添加存储容量

将存储容量添加到启用了 **NFS** 的 **SVM** 概述中

要向启用了 NFS 的 SVM 添加存储容量，必须创建一个卷或 qtree 以提供存储容器，并为此容器创建或修改导出策略。然后，您可以从集群验证 NFS 客户端访问，并测试客户端系统的访问。

您需要的内容

- 必须在 SVM 上完全设置 NFS 。
- SVM 根卷的默认导出策略必须包含允许访问所有客户端的规则。
- 必须完成对名称服务配置的所有更新。
- 必须完成对 Kerberos 配置的任何添加或修改。

创建导出策略

在创建导出规则之前，您必须创建一个导出策略来存放这些规则。您可以使用 `vserver export-policy create` 命令以创建导出策略。

步骤

1. 创建导出策略

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

   策略名称最长可为 256 个字符。

2. 验证是否已创建导出策略：

   ```
   vserver export-policy show -policyname policy_name
   ```

示例

以下命令将在名为 vs1 的 SVM 上创建并验证是否已创建名为 exp1 的导出策略：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

向导出策略添加规则

如果没有规则，导出策略将无法提供客户端对数据的访问。要创建新的导出规则，您必须标识客户端并选择客户端匹配格式，选择访问和安全类型，指定匿名用户 ID 映射，选择规则索引编号，然后选择访问协议。然后、您可以使用 `vserver export-policy rule create` 命令将新规则添加到导出策略中。

您需要的内容

- 要添加导出规则的导出策略必须已存在。
- 必须在数据 SVM 上正确配置 DNS ，并且 DNS 服务器必须具有适用于 NFS 客户端的正确条目。

  这是因为 ONTAP 使用数据 SVM 的 DNS 配置对某些客户端匹配格式执行 DNS 查找，如果导出策略规则匹配失败，则可能会阻止客户端数据访问。

- 如果您要使用 Kerberos 进行身份验证，则必须已确定 NFS 客户端使用以下哪种安全方法：
  - `krb5` (Kerberos V5协议)
  - `krb5i` (使用校验和进行完整性检查的Kerberos V5协议)
  - `krb5p` (具有隐私服务的Kerberos V5协议)

关于此任务

如果导出策略中的现有规则满足客户端匹配和访问要求，则无需创建新规则。

如果要使用Kerberos进行身份验证、并且SVM的所有卷都通过Kerberos进行访问、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5`， `krb5i`或 `krb5p`。

步骤

1. 确定新规则的客户端和客户端匹配格式。

   。 `-clientmatch` option用于指定应用此规则的客户端。可以指定一个或多个客户端匹配值；多个值的规范必须用逗号分隔。您可以使用以下任意格式指定匹配项：

客户端匹配格式	示例
域名前面带有 "." 字符	`.example.com` 或 `.example.com,.example.net,...`
主机名	`host1` 或 `host1,host2, ...`
IPv4 地址	`10.1.12.24` 或 `10.1.12.24,10.1.12.25, ...`
IPv4 地址，子网掩码以位数表示	`10.1.12.10/4` 或 `10.1.12.10/4,10.1.12.11/4,...`
带有网络掩码的 IPv4 地址	`10.1.16.0/255.255.255.0` 或 `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
点格式的 IPv6 地址	`::1.2.3.4` 或 `::1.2.3.4,::1.2.3.5,...`
IPv6地址、子网掩码以位数表示	`ff::00/32` 或 `ff::00/32,ff::01/32,...`
一个网络组，其网络组名称前面带有 @ 字符	`@netgroup1` 或 `@netgroup1,@netgroup2,...`

   您还可以组合使用各种类型的客户端定义、例如、 `.example.com,@netgroup1`。

   指定 IP 地址时，请注意以下事项：

   - 不允许输入 IP 地址范围，例如 10.1.12.10-10.1.12.70 。

此格式的条目将被解释为文本字符串，并被视为主机名。

- 在导出规则中指定单个 IP 地址以精细管理客户端访问时，请勿指定动态分配（例如 DHCP ）或临时分配（例如 IPv6 ）的 IP 地址。

  否则，当客户端的 IP 地址发生更改时，客户端将失去访问权限。

- 不允许输入带有网络掩码的 IPv6 地址，例如 ff： 12/ff：： 00 。

2. 为客户端匹配选择访问和安全类型。

   您可以为使用指定安全类型进行身份验证的客户端指定以下一种或多种访问模式：

   - `-rorule` (只读访问)
   - `-rwrule` (读写访问)
   - `-superuser` (root访问权限)

   > 只有当导出规则也允许对特定安全类型进行只读访问时，客户端才能获得该安全类型的读写访问权限。如果只读参数对于安全类型的限制性比读写参数更强，则客户端可能无法获得读写访问权限。超级用户访问也是如此。

   您可以为一个规则指定多种安全类型的逗号分隔列表。将安全类型指定为 `any` 或 `never`，请勿指定任何其他安全类型。从以下有效安全类型中进行选择：

当安全类型设置为 ...	匹配的客户端可以访问导出的数据 ...
`any`	始终，无论传入的安全类型如何。
`none`	如果单独列出，则具有任何安全类型的客户端将被授予匿名访问权限。如果与其他安全类型一起列出，则具有指定安全类型的客户端将被授予访问权限，而具有任何其他安全类型的客户端将被授予匿名访问权限。
`never`	从不，无论传入的安全类型如何。
`krb5`	如果通过 Kerberos 5 进行身份验证。 仅身份验证：每个请求和响应的标头都已签名。
`krb5i`	如果通过 Kerberos 5i 进行身份验证。 身份验证和完整性：每个请求和响应的标头和正文均已签名。
`krb5p`	如果使用Kerberos 5p进行身份验证。 身份验证，完整性和隐私：对每个请求和响应的标题和正文进行签名，并对 NFS 数据有效负载进行加密。
`ntlm`	如果通过 CIFS NTLM 进行身份验证。

当安全类型设置为 ...	匹配的客户端可以访问导出的数据 ...
`sys`	如果通过 NFS AUTH_SYS 进行身份验证。

建议的安全类型为 `sys`或者，如果使用`Kerberos`， `krb5`， `krb5i`或 `krb5p`。

如果要将Kerberos与NFSv3结合使用、则导出策略规则必须允许 `-rorule` 和 `-rwrule` 访问 `sys` 除了 `krb5`。这是因为需要允许 Network Lock Manager （ NLM ）访问导出。

3. 指定匿名用户 ID 映射。

   。 `-anon` option用于指定映射到用户ID为0 (零)的客户端请求的UNIX用户ID或用户名、此用户ID或用户名通常与用户名root相关联。默认值为 `65534`。NFS 客户端通常会将用户 ID 65534 与用户名 nobody 相关联（也称为 *root squash* ）。在 ONTAP 中，此用户 ID 与用户 pcuser 关联。要禁止用户ID为0的任何客户端访问、请指定值 `65535`。

4. 选择规则索引顺序。

   。 `-ruleindex` option用于指定规则的索引编号。规则将根据其在索引编号列表中的顺序进行评估；索引编号较低的规则将首先进行评估。例如，索引编号为 1 的规则会在索引编号为 2 的规则之前进行评估。

如果要添加 ...	那么 ...
导出策略的第一个规则	输入 ... `1`。
导出策略的其他规则	a. 显示策略中的现有规则： `vserver export-policy rule show -instance -policyname` *`your_policy`* b. 根据新规则的评估顺序为其选择索引编号。

5. 选择适用的NFS访问值：｛`nfs`|`nfs3`|`nfs4`｝。

   `nfs` 匹配任何版本、 `nfs3` 和 `nfs4` 仅匹配这些特定版本。

6. 创建导出规则并将其添加到现有导出策略：

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {nfs|nfs3|nfs4} -clientmatch { text |` *`"text,text,…"`* `} -rorule` *`security_type`* `-rwrule` *`security_type`* `-superuser` *`security_type`* `-anon` *`user_ID`*

7. 显示导出策略的规则以验证新规则是否存在：

   `vserver export-policy rule show -policyname` *`policy_name`*

   命令将显示该导出策略的摘要，包括应用于该策略的规则列表。ONTAP 会为每个规则分配一个规则索引编号。知道规则索引编号后，您可以使用它显示有关指定导出规则的详细信息。

8. 验证是否已正确配置应用于导出策略的规则：

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

示例

以下命令将在名为 RS1 的导出策略中的 SVM vs1 上创建导出规则并验证此创建过程。此规则的索引编号为 1 。此规则与域 eng.company.com 和 netgroup @netgroup1 中的任何客户端匹配。此规则将启用所有 NFS 访问。它允许使用 AUTH_SYS 进行身份验证的用户进行只读和读写访问。除非使用 Kerberos 进行身份验证，否则使用 UNIX 用户 ID 0 （零）的客户端将被匿名化。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                   Vserver: vs1
                               Policy Name: exp1
                                Rule Index: 1
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

以下命令将在名为 expol2 的导出策略中的 SVM vs2 上创建导出规则并验证此创建过程。此规则的索引编号为21。此规则会将客户端与网络组 dev_netgroup_main 中的成员匹配。此规则将启用所有 NFS 访问。它允许使用 AUTH_SYS 进行身份验证的用户进行只读访问，并要求对读写和 root 访问进行 Kerberos 身份验证。除非使用 Kerberos 进行身份验证，否则使用 UNIX 用户 ID 0 （零）的客户端将被拒绝进行 root 访问。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual   Policy       Rule    Access    Client              RO
Server    Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2       expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                               Policy Name: expol2
                                Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

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

- 应设置并运行NFS。
- SVM安全模式必须为UNIX。
- 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 unix -user user_name_or_number -group group_name_or_number -junction-path junction_path [-policy export_policy_name]`

   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。

     如果您计划使用现有导出策略、则可以在创建卷时指定此策略。您也可以稍后使用添加导出策略 `volume modify` 命令：

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
                           Junction                 Junction
Vserver           Volume  Active   Junction Path   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
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   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：

您需要的内容

- 要包含新 qtree 的 SVM 和卷必须已存在。
- SVM 安全模式必须为 UNIX ，并且 NFS 应设置并运行。

步骤

1. 创建 qtree：

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   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`*。

   默认情况下， qtree 会继承其父卷的导出策略，但可以将其配置为使用自己的导出策略。如果您计划使用现有导出策略，则可以在创建 qtree 时指定该策略。您也可以稍后使用添加导出策略 `volume qtree modify` 命令：

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 unix
[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: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                           Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

使用导出策略确保 **NFS** 访问安全

使用导出策略确保 **NFS** 访问安全

您可以使用导出策略将对卷或 qtree 的 NFS 访问限制为与特定参数匹配的客户端。配置新存储时，您可以使用现有策略和规则，向现有策略添加规则或创建新策略和规则。您还可以检查导出策略的配置

> 从 ONTAP 9.3 开始，您可以将导出策略配置检查作为后台作业来启用，以便在错误规则列表中记录任何违规。。 `vserver export-policy config-checker` 命令会调用检查程序并显示结果、您可以使用这些结果验证配置并从策略中删除错误的规则。这些命令仅验证主机名、网络组和匿名用户的导出配置。

管理导出规则的处理顺序

您可以使用 `vserver export-policy rule setindex` 命令以手动设置现有导出规则的索引编号。这样，您可以指定 ONTAP 将导出规则应用于客户端请求的优先级。

关于此任务

如果新索引编号已在使用中，则该命令会在指定位置插入规则并相应地对列表重新排序。

步骤

1. 修改指定导出规则的索引编号：

   `vserver export-policy rule setindex -vserver` *`virtual_server_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-newruleindex` *`integer`*

示例

以下命令会将 SVM vs1 上名为 RS1 的导出策略中索引编号为 3 的导出规则的索引编号更改为 2：

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

为卷分配导出策略

SVM 中包含的每个卷都必须与一个导出策略相关联，该导出策略包含导出规则，客户端可以通过这些规则访问卷中的数据。

关于此任务

您可以在创建卷时或创建卷后随时将导出策略与卷关联。您可以将一个导出策略与卷关联，但一个策略可以与多个卷关联。

步骤

1. 如果在创建卷时未指定导出策略，请为此卷分配一个导出策略：

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. 验证是否已将此策略分配给卷：

   ```
   volume show -volume volume_name -fields policy
   ```

示例

以下命令会将导出策略 nfs_policy 分配给 SVM vs1 上的卷 vol1 并验证分配情况：

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

为 **qtree** 分配导出策略

您还可以导出卷上的特定 qtree ，使其可供客户端直接访问，而不是导出整个卷。您可以通过为 qtree 分配导出策略来导出 qtree 。您可以在创建新 qtree 时分配导出策略，也可以通过修改现有 qtree 来分配导出策略。

您需要的内容

导出策略必须存在。

关于此任务

默认情况下，如果在创建时未另行指定， qtree 将继承包含卷的父导出策略。

您可以在创建 qtree 时或在创建 qtree 之后随时将导出策略与 qtree 相关联。您可以将一个导出策略与 qtree 关联，但一个策略可以与多个 qtree 关联。

步骤

1. 如果在创建 qtree 时未指定导出策略，请为此 qtree 分配一个导出策略：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. 验证是否已将此策略分配给 qtree：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

示例

以下命令会将导出策略 nfs_policy 分配给 SVM vs1 上的 qtree qt1 并验证分配情况：

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

从集群验证 **NFS** 客户端访问

您可以通过在 UNIX 管理主机上设置 UNIX 文件权限来为选定客户端授予对共享的访问权限。您可以使用检查客户端访问 `vserver export-policy check-access` 命令、根据需要调整导出规则。

步骤

1. 在集群上、使用检查客户端对导出的访问权限 `vserver export-policy check-access` 命令：

   以下命令将检查 IP 地址为 1.2.3.4 的 NFSv3 客户端对卷 Home2 的读 / 写访问权限。命令输出显示卷使用导出策略 `exp-home-dir` 而且访问被拒绝。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                          Policy    Policy     Rule
Path                     Policy           Owner     Owner Type Index  Access
------------------------ ------------- --------- ---------- ------
----------
/                        default       vs1_root  volume          1 read
/eng                     default       vs1_root  volume          1 read
/eng/home2               exp-home-dir  home2     volume          1 denied

3 entries were displayed.
```

2. 检查输出以确定导出策略是否按预期工作以及客户端访问是否按预期进行。

   具体而言，您应验证卷或 qtree 使用的导出策略以及客户端因此具有的访问类型。

3. 如有必要，请重新配置导出策略规则。

测试客户端系统的 **NFS** 访问

在验证对新存储对象的 NFS 访问之后，您应登录到 NFS 管理主机并从 SVM 读取数据并向 SVM 写入数据来测试配置。然后，您应在客户端系统上以非 root 用户身份重复此过程。

您需要的内容

- 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. 在集群上，验证托管新卷的 LIF 的 IP 地址：

   `network interface show –vserver svm_name`

2. 以 root 用户身份登录到管理主机客户端系统。
3. 将目录更改为挂载文件夹：

   `cd /mnt/`

4. 使用 SVM 的 IP 地址创建并挂载新文件夹：

   a. 创建新文件夹：

      `mkdir /mnt/folder`

   b. 将新卷挂载到此新目录：

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. 将目录更改为新文件夹：

```
cd folder
```

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 hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 创建一个新文件，验证该文件是否存在并向其写入文本：

a. 创建测试文件：

```
touch filename
```

b. 验证文件是否存在：

```
ls -l filename
```

c. 输入 ...

```
cat > filename
```

键入一些文本，然后按 Ctrl+D 将文本写入测试文件。

d. 显示测试文件的内容。

```
cat filename
```

e. 删除测试文件：

```
rm filename
```

f. 返回到父目录：

```
cd ..
```

```
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 ..
```

6. 以 root 用户身份，在挂载的卷上设置所需的任何 UNIX 所有权和权限。
7. 在导出规则中标识的 UNIX 客户端系统上，以现在有权访问新卷的授权用户之一身份登录，然后重复步骤 3 至 5 中的过程，以验证是否可以挂载卷并创建文件。

从何处查找追加信息

成功测试 NFS 客户端访问后，您可以执行其他 NFS 配置或添加 SAN 访问。协议访问完成后，您应保护 Storage Virtual Machine （ SVM ）的根卷。

NFS配置

您可以使用以下信息和技术报告进一步配置 NFS 访问：

- "NFS 管理"

  介绍如何使用 NFS 配置和管理文件访问。

- "NetApp 技术报告 4067 ：《 NFS 最佳实践和实施指南》"

  可作为 NFSv3 和 NFSv4 操作指南，简要介绍 ONTAP 操作系统，重点介绍 NFSv4 。

- "NetApp 技术报告 4073 ：《安全统一身份验证》"

  介绍如何将 ONTAP 配置为与基于 UNIX 的 Kerberos 版本 5 （ krb5 ）服务器结合使用以进行 NFS 存储身份验证，并将 Windows Server Active Directory （ AD ）配置为 KDC 和轻量级目录访问协议（ LDAP ）身份提供程序。

- "NetApp 技术报告 3580 ：《 NFSv4 增强功能和最佳实践指南： Data ONTAP 实施》"

  介绍在连接到运行 ONTAP 的系统的 AIX ， Linux 或 Solaris 客户端上实施 NFSv4 组件时应遵循的最佳实践。

网络配置

您可以使用以下信息和技术报告进一步配置网络功能和名称服务：

- "NFS 管理"

  介绍如何配置和管理 ONTAP 网络。

- "NetApp 技术报告 4182 ：《集群模式 Data ONTAP 配置的以太网存储设计注意事项和最佳实践》"

  介绍 ONTAP 网络配置的实施，并提供常见网络部署场景和最佳实践建议。

- "NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

  介绍如何配置 LDAP ， NIS ， DNS 和本地文件配置以进行身份验证。

SAN 协议配置

如果要提供或修改对新 SVM 的 SAN 访问，可以使用 FC 或 iSCSI 配置信息，此信息可用于多个主机操作系统。

根卷保护

在 SVM 上配置协议后，您应确保其根卷受到保护：

- "数据保护"

  介绍如何创建负载共享镜像以保护 SVM 根卷，这是适用于已启用 NAS 的 SVM 的 NetApp 最佳实践。此外，还介绍如何通过从负载共享镜像提升 SVM 根卷来快速从卷故障或丢失中恢复。

ONTAP 导出与 7- 模式导出有何不同

ONTAP 导出与 **7-** 模式导出有何不同

如果您不熟悉ONTAP如何实施NFS导出、可以比较7-模式和ONTAP导出配置工具以及7-模式示例 `/etc/exports` 具有集群模式策略和规则的文件。

在ONTAP中、没有 `/etc/exports` file和no `exportfs` 命令：而是必须定义导出策略。通过导出策略，您可以像在 7- 模式中一样控制客户端访问，但也可以提供其他功能，例如可以对多个卷重复使用相同的导出策略。

相关信息

"NFS 管理"

"NetApp 技术报告 4067 ：《 NFS 最佳实践和实施指南》"

7- 模式和 **ONTAP** 中的导出比较

ONTAP 中的导出定义和使用方式与 7- 模式环境中不同。

不同之处	7- 模式	ONTAP
如何定义导出	导出在中进行定义 `/etc/exports` 文件	导出可通过在 SVM 中创建导出策略来定义。一个 SVM 可以包含多个导出策略。
导出范围	• 导出将应用于指定的文件路径或 qtree 。 • 您必须在中创建单独的条目 `/etc/exports` 对于每个文件路径或qtree。 • 只有在中定义导出后、这些导出才会持久保留 `/etc/exports` 文件	• 导出策略适用于整个卷，包括卷中包含的所有文件路径和 qtree 。 • 如果需要，可以将导出策略应用于多个卷。 • 所有导出策略都会在系统重新启动后保持不变。

隔离（为特定客户端指定对相同资源的不同访问权限）	要为特定客户端提供对单个导出资源的不同访问权限、必须在中列出每个客户端及其允许的访问权限 `/etc/exports` 文件	导出策略由多个单独的导出规则组成。每个导出规则都定义资源的特定访问权限，并列出具有这些权限的客户端。要为特定客户端指定不同的访问权限，您必须为每组特定访问权限创建一个导出规则，列出具有这些权限的客户端，然后将这些规则添加到导出策略中。
名称别名	定义导出时，您可以选择使导出名称与文件路径名称不同。您应使用 `-actual` 参数 `/etc/exports` 文件	您可以选择使导出卷的名称与实际卷名称不同。为此、您必须在SVM命名空间中使用自定义接合路径名称挂载卷。 默认情况下，卷会使用其卷名称进行挂载。要自定义卷的接合路径名称，您需要将其卸载，重命名并重新挂载。

ONTAP 导出策略示例

您可以查看导出策略示例，以更好地了解导出策略在 ONTAP 中的工作原理。

7- 模式导出的 **ONTAP** 实施示例

以下示例显示了中显示的7-模式导出 `/etc/export` 文件：

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

要将此导出复制为集群模式导出策略，您必须创建一个包含三个导出规则的导出策略，然后将此导出策略分配给卷 vol1 。

规则	**Element**	价值
规则 1.	`-clientmatch` (客户端规范)	`@readonly_netgroup`
`-ruleindex`(导出规则在规则列表中的位置)	`1`	`-protocol`
`nfs`	`-rorule`(允许只读访问)	`sys` (客户端使用AUTH _ SYS进行身份验证)
`-rwrule`(允许读写访问)	`never`	`-superuser`(允许超级用户访问)

规则	Element	价值
none(root用户_squ希_到anon)	第2条	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	第3条
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. 创建名为 exp_vol1 的导出策略：

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. 在基本命令中使用以下参数创建三个规则：
   - 基本命令：

     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```

   - 规则参数：

     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none

     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     -rwrule sys -superuser sys

     -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
     -protocol nfs -rorule sys -rwrule sys -superuser none
     ```

3. 将此策略分配给卷 vol1 ：

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

以下示例显示了7-模式 `/etc/export` 文件、其中每一行对应10个qtrees：

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

在ONTAP中、每个qtree需要两个策略之一：一个策略包含一个规则 `-clientmatch host1519s`，或包含规则的 `-clientmatch host2057s`。

1. 创建两个名为 exp_vol1q1 和 exp_vol1q2 的导出策略：
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 为每个策略创建一个规则：
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. 将策略应用于 qtree：
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [接下来的 4 个 qtree…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [接下来的 4 个 qtree…]

如果稍后需要为这些主机添加其他 qtree ，则可以使用相同的导出策略。

使用命令行界面管理NFS

NFS参考概述

ONTAP 包括可用于 NFS 协议的文件访问功能。您可以启用 NFS 服务器并导出卷或 qtree 。

您可以在以下情况下执行这些操作步骤：

- 您希望了解ONTAP NFS协议功能的范围。
- 您希望执行不太常见的配置和维护任务、而不是基本NFS配置。
- 您希望使用命令行界面（ CLI ），而不是 System Manager 或自动化脚本编写工具。

了解 **NAS** 文件访问

命名空间和接合点

命名空间和接合点概述

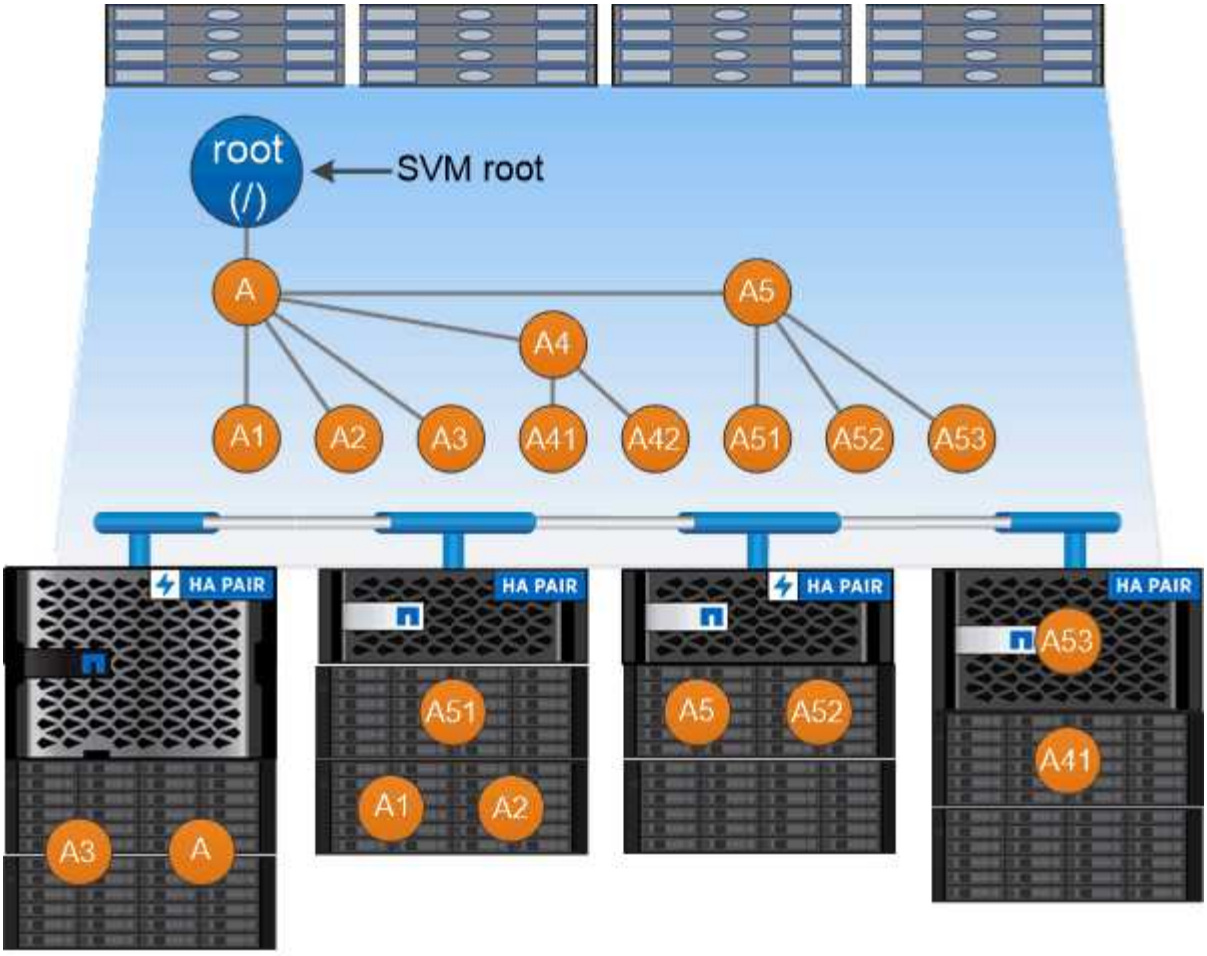
nas_namespaces_ 是指在 *junction points* 处联合在一起的卷的逻辑分组，用于创建单个文件系统层次结构。具有足够权限的客户端可以访问命名空间中的文件，而无需指定文件在存储中的位置。集群中的任何位置都可以驻留未分配的卷。

NAS 客户端不会挂载包含相关文件的每个卷，而是挂载 nfs *export* 或访问 SMB _share 。 _ 导出或共享表示整个命名空间或命名空间中的中间位置。客户端仅访问挂载在其访问点下方的卷。

您可以根据需要向命名空间添加卷。您可以直接在父卷接合下方或卷中的目录上创建接合点。名为"`vol3`"的卷的卷接合路径可能为 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`，甚至 `/dir1/dir2/vol3`。此路径称为 _junction path…

每个 SVM 都有一个唯一的命名空间。SVM 根卷是命名空间层次结构的入口点。

> 要确保在发生节点中断或故障转移时数据仍然可用，您应为 SVM 根卷创建一个 *load-sharing mirror* 副本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

什么是典型的 **NAS** 命名空间架构

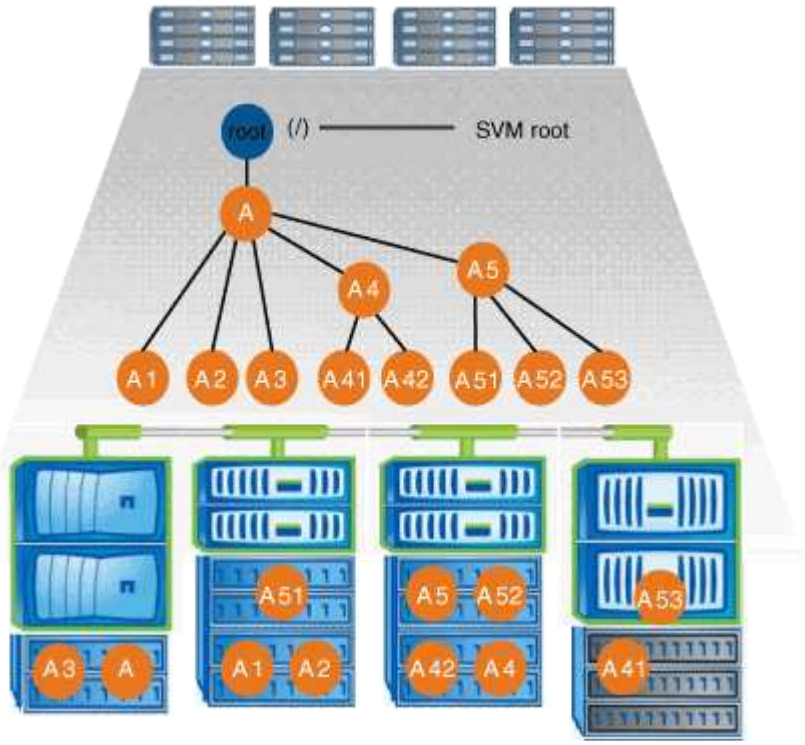
在创建 SVM 名称空间时，您可以使用几种典型的 NAS 命名空间架构。您可以选择符合业务和工作流需求的命名空间架构。

命名空间的顶部始终为根卷，以斜杠（/）表示。根下的命名空间架构分为三个基本类别：

- 一个分支树，与命名空间根只有一个接合点
- 多个分支树，多个接合点指向命名空间的根
- 多个独立卷，每个卷都有一个指向名称空间根的单独接合点

包含单个分支树的命名空间

包含单个分支树的架构在 SVM 命名空间的根上具有一个插入点。单个插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在单个插入点（可以是卷或目录）下的接合点处。

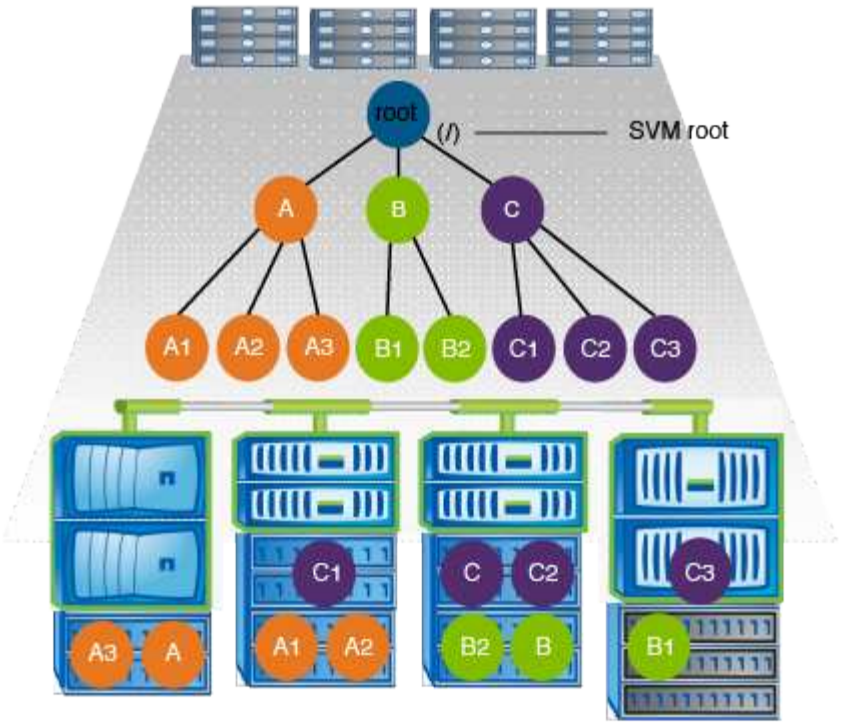


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中所有卷都在单个插入点（即名为 `data` 的目录）下接合：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     corp1        true     /data/dir1/corp1         RW_volume
vs1     corp2        true     /data/dir1/corp2         RW_volume
vs1     data1        true     /data/data1              RW_volume
vs1     eng1         true     /data/data1/eng1         RW_volume
vs1     eng2         true     /data/data1/eng2         RW_volume
vs1     sales        true     /data/data1/sales        RW_volume
vs1     vol1         true     /data/vol1               RW_volume
vs1     vol2         true     /data/vol2               RW_volume
vs1     vol3         true     /data/vol3               RW_volume
vs1     vs1_root     -        /                        -
```

包含多个分支树的命名空间

包含多个分支树的架构在 SVM 命名空间的根目录中具有多个插入点。插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在插入点下方的接合点（可以是卷或目录）。

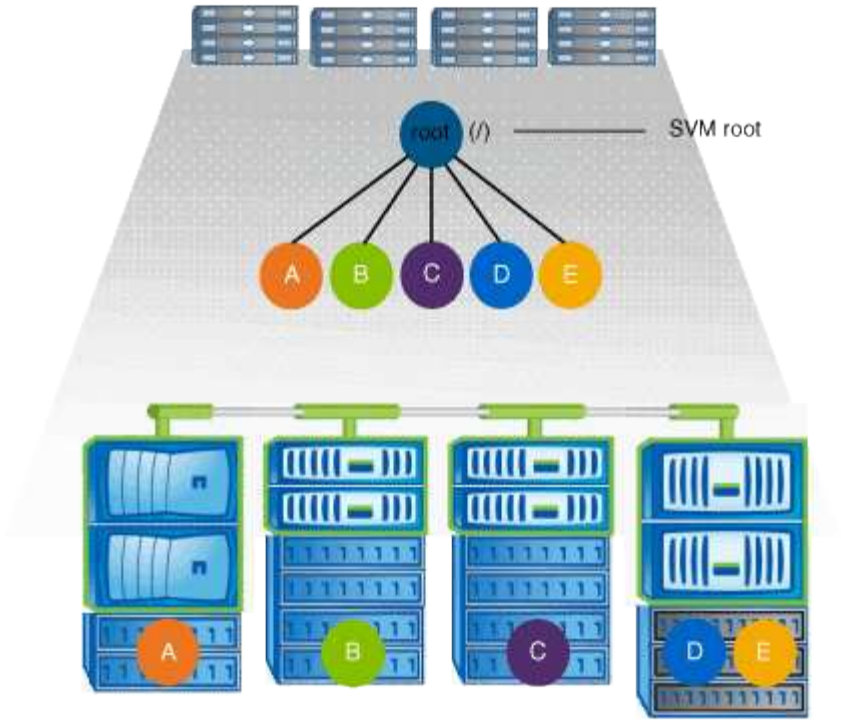


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有三个插入点指向 SVM 的根卷。两个插入点是名为 `data` 和 "`projects` " 的目录。一个插入点是名为 "`audit` " 的接合卷：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     audit        true     /audit                   RW_volume
vs1     audit_logs1  true     /audit/logs1             RW_volume
vs1     audit_logs2  true     /audit/logs2             RW_volume
vs1     audit_logs3  true     /audit/logs3             RW_volume
vs1     eng          true     /data/eng                RW_volume
vs1     mktg1        true     /data/mktg1              RW_volume
vs1     mktg2        true     /data/mktg2              RW_volume
vs1     project1     true     /projects/project1       RW_volume
vs1     project2     true     /projects/project2       RW_volume
vs1     vs1_root     -        /                        -
```

包含多个独立卷的命名空间

在具有独立卷的架构中，每个卷都有一个插入点指向 SVM 命名空间的根；但是，卷不会接合到另一个卷下。每个卷都有一个唯一的路径，可以直接在根下接合，也可以在根下的目录下接合。



例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有五个插入点指向 SVM 的根卷，每个插入点表示一个卷的路径。

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     eng           true     /eng                     RW_volume
vs1     mktg          true     /vol/mktg                RW_volume
vs1     project1      true     /project1                RW_volume
vs1     project2      true     /project2                RW_volume
vs1     sales         true     /sales                   RW_volume
vs1     vs1_root      -        /                        -
```

ONTAP 如何控制对文件的访问

ONTAP 如何控制对文件的访问概述

ONTAP 会根据您指定的基于身份验证和基于文件的限制来控制对文件的访问。

当客户端连接到存储系统以访问文件时， ONTAP 必须执行两项任务：

- 身份验证

  ONTAP 必须通过使用可信源验证身份来对客户端进行身份验证。此外，客户端的身份验证类型是一种可用于确定客户端在配置导出策略时是否可以访问数据的方法（对于 CIFS 为可选）。

- Authorization

ONTAP 必须通过将用户凭据与文件或目录上配置的权限进行比较并确定要提供的访问类型（如果有）来授权用户。

要正确管理文件访问控制， ONTAP 必须与 NIS ， LDAP 和 Active Directory 服务器等外部服务进行通信。要使用 CIFS 或 NFS 配置存储系统以进行文件访问，需要根据您在 ONTAP 中的环境设置相应的服务。

基于身份验证的限制

通过基于身份验证的限制，您可以指定哪些客户端计算机以及哪些用户可以连接到 Storage Virtual Machine （ SVM ）。

ONTAP 支持从 UNIX 和 Windows 服务器进行 Kerberos 身份验证。

基于文件的限制

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估三个安全级别后，访问权限由有效权限决定。

任何存储对象最多可包含三种类型的安全层：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

  > 如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则不会看到存储级别访问防护安全性。即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别访问防护安全性。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

ONTAP如何处理**NFS**客户端身份验证

ONTAP 如何处理 **NFS** 客户端身份验证概述

NFS 客户端必须经过适当的身份验证，才能访问 SVM 上的数据。ONTAP 会根据您配置的名称服务检查客户端的 UNIX 凭据，从而对客户端进行身份验证。

当 NFS 客户端连接到 SVM 时， ONTAP 会根据 SVM 的名称服务配置检查不同的名称服务来获取用户的 UNIX 凭据。ONTAP 可以检查本地 UNIX 帐户， NIS 域和 LDAP 域的凭据。必须至少配置其中一个， ONTAP 才能成功对用户进行身份验证。您可以指定多个名称服务以及 ONTAP 搜索这些服务的顺序。

在采用 UNIX 卷安全模式的纯 NFS 环境中，此配置足以对从 NFS 客户端连接的用户进行身份验证并提供正确的文件访问权限。

如果您使用的是混合、NTFS或统一卷安全模式、则ONTAP必须获取UNIX用户的SMB用户名、以便通过Windows域控制器进行身份验证。这可以通过使用本地UNIX帐户或LDAP域映射单个用户来实现、也可以改用默认SMB用户来实现。您可以指定ONTAP搜索哪些名称服务的顺序、也可以指定默认SMB用户。

ONTAP 如何使用名称服务

ONTAP 使用名称服务获取有关用户和客户端的信息。ONTAP 使用此信息对访问存储系统上的数据或管理存储系统的用户进行身份验证，并在混合环境中映射用户凭据。

配置存储系统时，必须指定希望 ONTAP 用于获取用户凭据进行身份验证的名称服务。ONTAP 支持以下名称服务：

- 本地用户（文件）
- 外部 NIS 域（ NIS ）
- 外部 LDAP 域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列、用于为SVM配置源以搜索网络信息以及搜索顺序。这些命令提供与等效的功能 `/etc/nsswitch.conf` 文件。

当 NFS 客户端连接到 SVM 时， ONTAP 会检查指定的名称服务以获取用户的 UNIX 凭据。如果名称服务配置正确，并且 ONTAP 可以获取 UNIX 凭据，则 ONTAP 将成功对用户进行身份验证。

在具有混合安全模式的环境中， ONTAP 可能必须映射用户凭据。您必须为您的环境正确配置名称服务，以使 ONTAP 能够正确映射用户凭据。

ONTAP 还使用名称服务对 SVM 管理员帐户进行身份验证。在配置或修改名称服务切换时，必须牢记这一点，以免意外禁用 SVM 管理员帐户的身份验证。有关SVM管理用户的详细信息、请参见 "管理员身份验证和RBAC"。

ONTAP 如何从 NFS 客户端授予 SMB 文件访问权限

ONTAP 使用 Windows NT 文件系统（ NTFS ）安全语义来确定 NFS 客户端上的 UNIX 用户是否有权访问具有 NTFS 权限的文件。

为此， ONTAP 会将用户的 UNIX 用户 ID （ UID ）转换为 SMB 凭据，然后使用 SMB 凭据验证用户是否有权访问此文件。SMB 凭据由一个主安全标识符（ SID ）（通常是用户的 Windows 用户名）以及一个或多个与用户所属 Windows 组对应的组 SID 组成。

ONTAP 将 UNIX UID 转换为 SMB 凭据所需的时间可能从数十毫秒到数百毫秒不等，因为此过程涉及到与域控制器联系。ONTAP 会将 UID 映射到 SMB 凭据，并在凭据缓存中输入映射，以缩短转换所导致的验证时间。

NFS 凭据缓存的工作原理

当 NFS 用户请求访问存储系统上的 NFS 导出时， ONTAP 必须从外部名称服务器或本地文件检索用户凭据以对用户进行身份验证。然后， ONTAP 会将这些凭据存储在内部凭据缓存中，以供日后参考。了解 NFS 凭据缓存的工作原理有助于您处理潜在的性能和访问问题。

如果没有凭据缓存， ONTAP 将必须在 NFS 用户每次请求访问时查询名称服务。在许多用户访问的繁忙存储系统上，这可能会快速导致严重的性能问题，从而导致不必要的延迟，甚至拒绝 NFS 客户端访问。

通过凭据缓存， ONTAP 会检索用户凭据，然后将其存储一段预定的时间，以便在 NFS 客户端发送另一个请求时快速轻松地进行访问。此方法具有以下优势：

- 它可以减少对外部名称服务器（例如 NIS 或 LDAP ）的请求，从而减轻存储系统的负载。
- 它可以减少向外部名称服务器发送的请求，从而减轻这些服务器的负载。
- 它可以在用户进行身份验证之前，消除从外部源获取凭据的等待时间，从而加快用户访问速度。

ONTAP 会将肯定和否定凭据存储在凭据缓存中。肯定凭据表示用户已通过身份验证并获得访问权限。否定凭据表示用户未通过身份验证，并被拒绝访问。

默认情况下， ONTAP 会将肯定凭据存储 24 小时；也就是说，在对用户进行初始身份验证后， ONTAP 会对该用户 24 小时内的任何访问请求使用缓存的凭据。如果用户在 24 小时后请求访问，则此周期将重新开始： ONTAP 丢弃缓存的凭据，并从相应的名称服务源再次获取凭据。如果名称服务器上的凭据在过去 24 小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来 24 小时使用。

默认情况下， ONTAP 会将否定凭据存储两个小时；也就是说，在最初拒绝用户访问后， ONTAP 会继续拒绝该用户的任何访问请求两个小时。如果用户在 2 小时后请求访问，则循环将重新开始： ONTAP 再次从相应的名称服务源获取凭据。如果名称服务器上的凭据在过去两小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来两小时使用。

在 **NAS** 命名空间中创建和管理数据卷

创建具有指定接合点的数据卷

您可以在创建数据卷时指定接合点。生成的卷会自动挂载在接合点，并可立即配置用于 NAS 访问。

开始之前

- 要创建卷的聚合必须已存在。
- 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。

> 接合路径中不能使用以下字符： * # " > < | ? \

+
此外，接合路径长度不能超过 255 个字符。

步骤

1. 创建具有接合点的卷：

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path junction_path
```

接合路径必须以根（/）开头，并且可以同时包含目录和接合卷。接合路径不需要包含卷的名称。接合路径与卷名称无关。

指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （SVM）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于您创建的数据卷的安全模式。建议您在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

接合路径不区分大小写； `/ENG` 与相同 `/eng`。如果创建 CIFS 共享， Windows 会将接合路径视为区分大小写。例如、如果接合为 `/ENG`，SMB共享的路径必须以开头 `/ENG`，不是 `/eng`。

您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已使用所需的接合点创建卷：

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                   Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

创建数据卷而不指定接合点

您可以在不指定接合点的情况下创建数据卷。生成的卷不会自动挂载，也不可配置用于 NAS 访问。您必须先挂载卷，然后才能为该卷配置 SMB 共享或 NFS 导出。

开始之前

- 要创建卷的聚合必须已存在。
- 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. 使用以下命令创建不带接合点的卷：

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   ```

`{ntfs|unix|mixed}`

指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （ SVM ）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于数据卷的安全模式。建议您在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已在没有接合点的情况下创建卷：

   `volume show -vserver vserver_name -volume volume_name -junction`

示例

以下示例将在 SVM vs1 上创建一个名为 `sales` 的卷，该卷未挂载在接合点：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data           RW_volume
vs1       home4       true     /eng/home       RW_volume
vs1       vs1_root    -        /               -
vs1       sales       -        -               -
```

挂载或卸载 **NAS** 命名空间中的现有卷

必须先在 NAS 命名空间上挂载卷，然后才能配置 NAS 客户端对 Storage Virtual Machine （ SVM ）卷中所含数据的访问。如果卷当前未挂载，则可以将其挂载到接合点。您也可以卸载卷。

关于此任务

如果卸载某个卷并使其脱机、则NAS客户端将无法访问该接合点中的所有数据、包括接合点位于已卸载卷的命名空间中的卷中的数据。

> 要停止 NAS 客户端对卷的访问，仅仅卸载卷是不够的。您必须使此卷脱机、或者采取其他步骤确保客户端文件句柄缓存失效。有关详细信息，请参见以下知识库文章：
>
> "从 ONTAP 的命名空间中删除卷后， NFSv3 客户端仍可访问该卷"

卸载卷并使其脱机时，卷中的数据不会丢失。此外，在卷上或在已卸载卷内的目录和接合点上创建的现有卷导出策略和 SMB 共享也会保留下来。如果重新挂载卸载的卷， NAS 客户端可以使用现有导出策略和 SMB 共享访问卷中包含的数据。

步骤

1. 执行所需的操作：

如果您要 ...	输入命令 ...
挂载卷	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
卸载卷	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. 验证卷是否处于所需的挂载状态：

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-fields state,junction-path,junction-active`

示例

以下示例将位于SVM"`VS1`"上名为` ales s的卷挂载到接合点"/sales`"：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下示例将卸载位于SVM"`VS1`"上的名为"`data`"的卷并使其脱机：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

显示卷挂载和接合点信息

您可以显示有关 Storage Virtual Machine （SVM）的已挂载卷以及卷挂载到的接合点的信息。您还可以确定哪些卷未挂载到接合点。您可以使用此信息了解和管理 SVM 命名空间。

步骤

1. 执行所需的操作：

要显示的内容	输入命令 …
有关 SVM 上已挂载和已卸载卷的摘要信息	`volume show -vserver` *`vserver_name`* `-junction`
有关 SVM 上已挂载和已卸载卷的详细信息	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`

有关 SVM 上已挂载和已卸载卷的特定信息	a. 如有必要、您可以显示的有效字段 `-fields` 参数：
	`volume show -fields ?`
	b. 使用显示所需信息 `-fields` 参数：
	`volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

示例

以下示例显示了 SVM vs1 上已挂载和已卸载的卷的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

以下示例显示了有关 SVM vs2 上卷的指定字段的信息：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

配置安全模式

安全模式如何影响数据访问

安全模式及其影响是什么

安全模式有四种： UNIX ， NTFS ，混合和统一。每个安全模式对处理数据权限的方式具有不同的影响。您必须了解不同的影响，以确保选择适合您的安全模式。

请务必了解，安全模式并不确定哪些客户端类型可以或不可以访问数据。安全模式仅确定 ONTAP 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

例如，如果某个卷使用 UNIX 安全模式，则由于 ONTAP 的多协议性质， SMB 客户端仍可访问数据（前提是它们正确进行身份验证和授权）。但是， ONTAP 使用的是 UNIX 权限，只有 UNIX 客户端才能使用原生工具进行修改。

安全风格	可以修改权限的客户端	客户端可以使用的权限	生成的有效安全模式	可以访问文件的客户端
"unix"	NFS	NFSv3 模式位	"unix"	NFS 和 SMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
混合	NFS 或 SMB	NFSv3 模式位	"unix"	
		NFSv4.ACL		
		NTFS ACL	NTFS	
统一： (仅限无限卷、 在ONTAP 9.4及更早版本中。)	NFS 或 SMB	NFSv3 模式位	"unix"	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVol卷支持UNIX、NTFS和混合安全模式。混合或统一安全模式时，有效权限取决于上次修改权限的客户端类型，因为用户会逐个设置安全模式。如果修改权限的最后一个客户端是 NFSv3 客户端，则权限为 UNIX NFSv3 模式位。如果最后一个客户端是 NFSv4 客户端，则权限为 NFSv4 ACL 。如果最后一个客户端是 SMB 客户端，则权限为 Windows NTFS ACL 。

统一安全模式仅适用于无限卷，而 ONTAP 9.5 及更高版本不再支持无限卷。有关详细信息，请参见 FlexGroup 卷管理概述。

从ONTAP 9.2开始、 `show-effective-permissions` 参数 `vserver security file-directory` 命令用于显示为Windows或UNIX用户授予的对指定文件或文件夹路径的有效权限。此外、还有可选参数 `-share -name` 用于显示有效共享权限。

> ONTAP 最初会设置一些默认文件权限。默认情况下， UNIX ，混合和统一安全模式卷中所有数据的有效安全模式为 UNIX ，有效权限类型为 UNIX 模式位（ 0755 ，除非另有指定），直到客户端按照默认安全模式进行配置为止。默认情况下， NTFS 安全模式卷中所有数据的有效安全模式为 NTFS ，并且具有一个 ACL ，允许对任何人进行完全控制。

设置安全模式的位置和时间

可以在 FlexVol 卷（根卷或数据卷）和 qtree 上设置安全模式。安全模式可以在创建时手动设置，自动继承或稍后更改。

确定要在 **SVM** 上使用的安全模式

为了帮助您确定要在卷上使用的安全模式，您应考虑两个因素。主要因素是管理文件系统的管理员类型。二级因素是访问卷上数据的用户或服务的类型。

在卷上配置安全模式时，应考虑环境的需求，以确保选择最佳安全模式并避免管理权限时出现问题。以下注意事项有助于您做出决定：

安全风格	选择条件
"unix"	• 文件系统由 UNIX 管理员管理。 • 大多数用户都是 NFS 客户端。 • 访问数据的应用程序使用 UNIX 用户作为服务帐户。
NTFS	• 文件系统由 Windows 管理员管理。 • 大多数用户都是SMB客户端。 • 访问数据的应用程序使用 Windows 用户作为服务帐户。
混合	• 文件系统由 UNIX 和 Windows 管理员管理，用户由 NFS 和 SMB 客户端组成。

安全模式继承的工作原理

如果在创建新的 FlexVol 卷或 qtree 时未指定安全模式，则它会以不同方式继承其安全模式。

安全模式按以下方式继承：

- FlexVol 卷继承其所属 SVM 的根卷的安全模式。
- qtree 继承其所属 FlexVol 卷的安全模式。
- 文件或目录会继承其所在 FlexVol 卷或 qtree 的安全模式。

ONTAP 如何保留 **UNIX** 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 **Windows** 安全性选项卡管理 **UNIX** 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用

Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

  更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。

在 **SVM** 根卷上配置安全模式

您可以配置 Storage Virtual Machine （ SVM ）根卷安全模式，以确定 SVM 根卷上的数据所使用的权限类型。

步骤

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 用于定义安全模式的参数。

   根卷安全模式的可能选项为 `unix`， `ntfs``或 `mixed`。

2. 显示并验证配置，包括您创建的 SVM 的根卷安全模式：

   `vserver show -vserver` *`vserver_name`*

在 **FlexVol** 卷上配置安全模式

您可以配置 FlexVol 卷安全模式，以确定 Storage Virtual Machine （ SVM ）的 FlexVol 卷上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 FlexVol 卷 …	使用命令 …
尚不存在	`volume create` 并包括 `-security-style` 用于指定安全模式的参数。
已存在	`volume modify` 并包括 `-security-style` 用于指定安全模式的参数。

FlexVol卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

如果在创建 FlexVol 卷时未指定安全模式，则此卷将继承根卷的安全模式。

有关的详细信息、请参见 `volume create` 或 `volume modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置，包括您创建的 FlexVol 卷的安全模式，请输入以下命令：

   `volume show -volume volume_name -instance`

在 **qtree** 上配置安全模式

您可以配置 qtree 卷安全模式，以确定 qtree 上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 qtree…	使用命令 …
尚不存在	`volume qtree create` 并包括 `-security-style` 用于指定安全模式的参数。
已存在	`volume qtree modify` 并包括 `-security-style` 用于指定安全模式的参数。

   qtree安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建qtree时未指定安全模式、则默认安全模式为 `mixed`。

   有关的详细信息、请参见 `volume qtree create` 或 `volume qtree modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置(包括所创建的qtree的安全模式)、请输入以下命令： `volume qtree show -qtree` *`qtree_name`* `-instance`

使用**NFS**设置文件访问

使用 **NFS** 概述设置文件访问

要允许客户端使用 NFS 访问 Storage Virtual Machine （ SVM ）上的文件，您必须完成许多步骤。根据环境的当前配置，还有一些可选的附加步骤。

要使客户端能够使用 NFS 访问 SVM 上的文件，您必须完成以下任务：

1. 在 SVM 上启用 NFS 协议。

   您必须将 SVM 配置为允许客户端通过 NFS 访问数据。

2. 在 SVM 上创建 NFS 服务器。

NFS 服务器是 SVM 上的一个逻辑实体，可使 SVM 通过 NFS 提供文件。您必须创建 NFS 服务器并指定要允许的 NFS 协议版本。

3. 在 SVM 上配置导出策略。

   您必须配置导出策略，以使卷和 qtree 可供客户端使用。

4. 根据网络和存储环境，为 NFS 服务器配置适当的安全性和其他设置。

   此步骤可能包括配置 Kerberos ， LDAP ， NIS ，名称映射和本地用户。

使用导出策略确保 **NFS** 访问安全

导出策略如何控制客户端对卷或 **qtree** 的访问

导出策略包含一个或多个 *export rules* ，用于处理每个客户端访问请求。此过程的结果将确定客户端是被拒绝还是被授予访问权限，以及访问级别。Storage Virtual Machine （ SVM ）上必须存在具有导出规则的导出策略，客户端才能访问数据。

您只需将一个导出策略与每个卷或 qtree 相关联，即可配置客户端对卷或 qtree 的访问。SVM 可以包含多个导出策略。这样，您可以对包含多个卷或 qtree 的 SVM 执行以下操作：

- 为 SVM 的每个卷或 qtree 分配不同的导出策略，以控制单个客户端对 SVM 中每个卷或 qtree 的访问。
- 为 SVM 的多个卷或 qtree 分配相同的导出策略，以实现相同的客户端访问控制，而无需为每个卷或 qtree 创建新的导出策略。

如果客户端发出适用导出策略不允许的访问请求，则此请求将失败，并显示权限被拒绝的消息。如果客户端与导出策略中的任何规则不匹配，则会拒绝访问。如果导出策略为空，则会隐式拒绝所有访问。

您可以在运行 ONTAP 的系统上动态修改导出策略。

SVM 的默认导出策略

每个 SVM 都有一个不包含任何规则的默认导出策略。必须存在具有规则的导出策略，客户端才能访问 SVM 上的数据。SVM 中包含的每个 FlexVol 卷都必须与一个导出策略相关联。

创建SVM时、存储系统会自动创建一个名为的默认导出策略 `default` SVM的根卷。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。或者，您也可以使用规则创建自定义导出策略。您可以修改和重命名默认导出策略，但不能删除默认导出策略。

在包含的 SVM 中创建 FlexVol 卷时，存储系统会创建该卷，并将该卷与 SVM 根卷的默认导出策略相关联。默认情况下，在 SVM 中创建的每个卷都会与根卷的默认导出策略相关联。您可以对 SVM 中包含的所有卷使用默认导出策略，也可以为每个卷创建唯一的导出策略。您可以将多个卷与同一导出策略相关联。

导出规则的工作原理

导出规则是导出策略的功能要素。导出规则会根据您配置的特定参数将客户端对卷的访问请求进行匹配，以确定如何处理客户端访问请求。

导出策略必须至少包含一个导出规则，才能访问客户端。如果导出策略包含多个规则，则这些规则将按照它们在导出策略中的显示顺序进行处理。规则顺序由规则索引编号决定。如果某个规则与客户端匹配，则会使用该规则的权限，而不再处理其他规则。如果没有匹配的规则，客户端将被拒绝访问。

您可以使用以下条件配置导出规则以确定客户端访问权限：

- 发送请求的客户端使用的文件访问协议，例如 NFSv4 或 SMB 。
- 客户端标识符，例如主机名或 IP 地址。

  的最大大小 `-clientmatch` 字段为4096个字符。

- 客户端用于进行身份验证的安全类型，例如 Kerberos v5 ， NTLM 或 AUTH_SYS 。

如果某个规则指定了多个条件，则客户端必须与所有条件匹配，才能应用此规则。

> 从 ONTAP 9.3 开始，您可以将导出策略配置检查作为后台作业来启用，以便在错误规则列表中记录任何违规。。 `vserver export-policy config-checker` 命令会调用检查程序并显示结果、您可以使用这些结果来验证配置并从策略中删除错误的规则。
>
> 命令仅验证主机名，网络组和匿名用户的导出配置。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用 NFSv3 协议发送，并且客户端的 IP 地址为 10.1.17.37 。

即使客户端访问协议匹配，客户端的 IP 地址也与导出规则中指定的 IP 地址位于不同的子网中。因此，客户端匹配失败，此规则不适用于此客户端。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用NFSv4协议发送、客户端的IP地址为10.1.16.54。

客户端访问协议匹配，并且客户端的 IP 地址位于指定子网中。因此，客户端匹配成功，此规则将适用场景此客户端。无论安全类型如何，客户端都可以获得读写访问权限。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

客户端 1 的 IP 地址为 10.1.16.207 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

这两个客户端的客户端访问协议和 IP 地址匹配。只读参数允许对所有客户端进行只读访问，而不管客户端使用哪种安全类型进行身份验证。因此，这两个客户端都将获得只读访问权限。但是，只有客户端 1 获得读写访问权限，因为它使用经过批准的安全类型 Kerberos v5 进行身份验证。客户端 2 不会获得读写访问权限。

管理安全类型未列出的客户端

如果客户端的安全类型未列在导出规则的访问参数中、您可以选择拒绝访问该客户端、也可以改用选项将其映射到匿名用户ID `none` 在访问参数中。

客户端可能使用的安全类型未列在访问参数中，因为它是使用其他安全类型进行身份验证的，或者根本未进行身份验证（安全类型为 AUTH_NONE ）。默认情况下，客户端会自动拒绝访问该级别。但是、您可以添加选项 `none` 访问参数。因此，安全模式未列出的客户端会映射到匿名用户 ID 。。 `-anon` 参数用于确定分配给这些客户端的用户ID。为指定的用户ID `-anon` 参数必须是有效用户、并且已配置您认为适合匿名用户的权限。

的有效值 `-anon` 参数范围从 `0` to `65535`。

分配给的用户**ID** `-anon`	处理客户端访问请求的结果
`0 - 65533`	客户端访问请求将映射到匿名用户 ID ，并根据为此用户配置的权限获得访问权限。
`65534`	客户端访问请求将映射到用户 nobody ，并根据为此用户配置的权限获得访问权限。这是默认值。
`65535`	映射到此 ID 后，来自任何客户端的访问请求都会被拒绝，并且客户端会使用安全类型 AUTH_NONE 显示自己。如果客户端的用户 ID 为 0 ，则在映射到此 ID 时，此客户端发出的访问请求将被拒绝，而此客户端将使用任何其他安全类型显示自己。

使用选项时 `none`，请务必记住，只读参数是首先处理的。为安全类型未列出的客户端配置导出规则时，请考虑以下准则：

只读包括 `none`	读写包括 `none`	具有未列出的安全类型的客户端的访问结果
否	否	拒绝

只读包括 none	读写包括 none	具有未列出的安全类型的客户端的访问结果
否	是的。	拒绝，因为首先处理只读
是的。	否	以匿名身份只读
是的。	是的。	以匿名身份读写

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

客户端 1 的 IP 地址为 10.1.16.207 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

客户端 3 的 IP 地址为 10.1.16.234 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（表示安全类型为 AUTH_NONE ）。

所有这三个客户端的客户端访问协议和 IP 地址均匹配。只读参数允许使用自己的用户 ID 并通过 AUTH_SYS 进行身份验证的客户端进行只读访问。只读参数允许使用任何其他安全类型进行身份验证的客户端以用户 ID 为 70 的匿名用户身份进行只读访问。读写参数允许对任何安全类型进行读写访问，但在这种情况下，仅允许已通过只读规则筛选的适用场景客户端。

因此，客户端 1 和 3 只能作为用户 ID 为 70 的匿名用户进行读写访问。客户端 2 使用自己的用户 ID 获得读写访问权限。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

客户端 1 的 IP 地址为 10.1.16.207 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

客户端 3 的 IP 地址为 10.1.16.234 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（表示安全类型为 AUTH_NONE ）。

所有这三个客户端的客户端访问协议和 IP 地址均匹配。只读参数允许使用自己的用户 ID 并通过 AUTH_SYS 进行身份验证的客户端进行只读访问。只读参数允许使用任何其他安全类型进行身份验证的客户端以用户 ID 为 70 的匿名用户身份进行只读访问。读写参数仅允许以匿名用户身份进行读写访问。

因此，客户端 1 和客户端 3 只能作为用户 ID 为 70 的匿名用户进行读写访问。客户端 2 使用自己的用户 ID 获取只读访问，但被拒绝读写访问。

安全类型如何确定客户端访问级别

客户端使用进行身份验证的安全类型在导出规则中起着特殊的作用。您必须了解安全类型如何确定客户端对卷或 qtree 的访问级别。

三种可能的访问级别如下：

1. 只读
2. 读写
3. 超级用户（对于用户 ID 为 0 的客户端）

由于按安全类型评估访问级别的顺序，因此在导出规则中构建访问级别参数时，必须遵循以下规则：

客户端要获取访问级别 ...	这些访问参数必须与客户端的安全类型匹配 ...
普通用户只读	只读 (`-rorule`)
普通用户读写	只读 (`-rorule`)和读写 (`-rwrule`)
超级用户只读	只读 (`-rorule`)和 `-superuser`
超级用户读写	只读 (`-rorule`)和读写 (`-rwrule`)和 `-superuser`

以下是这三个访问参数中每一个参数的有效安全类型：

- `any`
- `none`
- `never`

  此安全类型不适用于 `-superuser` 参数。

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`

- sys

根据三个访问参数中的每个参数匹配客户端的安全类型时，可能会出现以下三种结果：

客户端的安全类型	然后，客户端 ...
与访问参数中指定的值匹配。	使用自己的用户 ID 获取该级别的访问权限。
与指定的不匹配、但访问参数包括选项 none。	获取该级别的访问权限、但作为用户ID由指定的匿名用户 -anon 参数。
与指定的不匹配、并且访问参数不包括选项 none。	不会获取该级别的任何访问权限。这不适用于 -superuser 参数、因为它始终包括 none 即使未指定也是如此。

示例

导出策略包含具有以下参数的导出规则：

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

客户端 3 的 IP 地址为 10.1.16.234 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（ AUTH_NONE ）。

客户端访问协议和 IP 地址与所有三个客户端匹配。只读参数允许对所有客户端进行只读访问，而不考虑安全类型。读写参数允许使用自己的用户 ID 并使用 AUTH_SYS 或 Kerberos v5 进行身份验证的客户端进行读写访问。超级用户参数允许超级用户访问用户 ID 为 0 并使用 Kerberos v5 进行身份验证的客户端。

因此，客户端 1 将获得超级用户读写访问权限，因为它与所有三个访问参数匹配。客户端 2 将获得读写访问权限，但不会获得超级用户访问权限。客户端 3 获得只读访问权限，但无超级用户访问权限。

管理超级用户访问请求

在配置导出策略时，您需要考虑在存储系统收到用户 ID 为 0 （即超级用户）的客户端访问请求并相应地设置导出规则时要发生的情况。

在 UNIX 环境中，用户 ID 为 0 的用户称为超级用户，通常称为 root ，他们对系统拥有无限访问权限。由于多种原因，使用超级用户权限可能会很危险，包括违反系统和数据安全。

默认情况下， ONTAP 会将用户 ID 为 0 的客户端映射到匿名用户。但是、您可以指定 - superuser 用于确定如何根据安全类型处理用户ID为0的客户端的导出规则中的参数。以下是的有效选项 -superuser 参数：

- any
- none

  如果未指定、则此为默认设置 -superuser 参数。

- krb5
- ntlm
- sys

根据、有两种不同的方式处理用户ID为0的客户端 -superuser 参数配置：

如果 **-superuser** 参数和客户端的安全类型	然后，客户端 ...
匹配	获取用户 ID 为 0 的超级用户访问权限。
不匹配	以用户ID由指定的匿名用户身份获取访问 -anon 参数及其分配的权限。这与只读或读写参数指定选项无关 none。

如果客户端使用用户ID 0访问采用NTFS安全模式和的卷 -superuser 参数设置为 none，ONTAP使用匿名用户的名称映射来获取正确的凭据。

示例

导出策略包含具有以下参数的导出规则：

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule krb5,ntlm
- -anon 127

客户端1的IP地址为10.1.16.207、用户ID为746、使用NFSv3协议发送访问请求、并使用Kerberos v5进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

这两个客户端的客户端访问协议和 IP 地址匹配。只读参数允许对所有客户端进行只读访问，而不管客户端使用哪种安全类型进行身份验证。但是，只有客户端 1 获得读写访问权限，因为它使用经过批准的安全类型 Kerberos v5 进行身份验证。

客户端 2 不会获得超级用户访问权限。相反、它会映射到匿名、因为 -superuser 未指定参数。这意味着它默认为 none 并自动将用户ID 0映射到匿名。客户端 2 也仅获取只读访问，因为其安全类型与读写参数不匹配。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

这两个客户端的客户端访问协议和 IP 地址匹配。只读参数允许对所有客户端进行只读访问，而不管客户端使用哪种安全类型进行身份验证。但是，只有客户端 1 获得读写访问权限，因为它使用经过批准的安全类型 Kerberos v5 进行身份验证。客户端 2 不会获得读写访问权限。

导出规则允许用户 ID 为 0 的客户端进行超级用户访问。客户端1将获得超级用户访问、因为它与只读和的用户ID和安全类型匹配 `-superuser` parameters客户端2不会获取读写或超级用户访问权限、因为其安全类型与读写参数或不匹配 `-superuser` 参数。而是将客户端 2 映射到匿名用户，在这种情况下，此用户 ID 为 0 。

ONTAP 如何使用导出策略缓存

为了提高系统性能， ONTAP 使用本地缓存来存储主机名和网络组等信息。这样，与从外部源检索信息相比， ONTAP 可以更快地处理导出策略规则。了解什么是缓存以及缓存的用途可以帮助您解决客户端访问问题。

您可以配置导出策略以控制客户端对 NFS 导出的访问。每个导出策略都包含规则，而每个规则都包含参数，用于将规则与请求访问的客户端匹配。其中一些参数要求 ONTAP 与外部源（例如 DNS 或 NIS 服务器）联系，以解析域名，主机名或网络组等对象。

与外部源的这些通信只需很短的时间。为了提高性能， ONTAP 通过将信息存储在多个缓存中的每个节点本地，减少了解析导出策略规则对象所需的时间。

缓存名称	存储的信息类型
访问	客户端到相应导出策略的映射
Name	UNIX 用户名到相应 UNIX 用户 ID 的映射
ID	UNIX 用户 ID 到相应 UNIX 用户 ID 和扩展 UNIX 组 ID 的映射
主机	主机名到相应 IP 地址的映射

缓存名称	存储的信息类型
网络组	网络组到相应成员 IP 地址的映射
showmount	从 SVM 命名空间导出的目录列表

如果在 ONTAP 检索并将环境中外部名称服务器上的信息存储在本地之后更改了这些信息，则缓存现在可能包含过时的信息。尽管 ONTAP 会在特定时间段后自动刷新缓存，但不同的缓存具有不同的到期时间和刷新时间以及算法。

缓存包含过时信息的另一个可能原因是 ONTAP 尝试刷新缓存的信息，但在尝试与名称服务器通信时遇到故障。如果发生这种情况， ONTAP 将继续使用当前存储在本地缓存中的信息，以防止客户端中断。

因此，应该成功的客户端访问请求可能会失败，而应该失败的客户端访问请求可能会成功。在对此类客户端访问问题进行故障排除时，您可以查看并手动刷新某些导出策略缓存。

访问缓存的工作原理

ONTAP 使用访问缓存来存储导出策略规则评估的结果，以供客户端对卷或 qtree 的访问操作使用。这样可以提高性能，因为与每次客户端发送 I/O 请求时执行导出策略规则评估过程相比，从访问缓存中检索信息的速度要快得多。

每当 NFS 客户端发送 I/O 请求以访问卷或 qtree 上的数据时， ONTAP 都必须评估每个 I/O 请求，以确定是授予还是拒绝 I/O 请求。此评估涉及检查与卷或 qtree 关联的导出策略的每个导出策略规则。如果卷或 qtree 的路径涉及跨越一个或多个接合点，则可能需要对路径上的多个导出策略执行此检查。

请注意，此评估适用于从 NFS 客户端发送的每个 I/O 请求，例如读取，写入，列表，复制和其他操作；而不仅仅适用于初始挂载请求。

在 ONTAP 确定适用的导出策略规则并决定允许还是拒绝请求后， ONTAP 会在访问缓存中创建一个条目来存储此信息。

当 NFS 客户端发送 I/O 请求时， ONTAP 会记下客户端的 IP 地址， SVM 的 ID 以及与目标卷或 qtree 关联的导出策略，并首先检查访问缓存中是否存在匹配条目。如果访问缓存中存在匹配的条目， ONTAP 将使用存储的信息来允许或拒绝 I/O 请求。如果不存在匹配条目， ONTAP 将按照上述说明完成评估所有适用策略规则的正常过程。

当前未使用的访问缓存条目不会刷新。这样可以减少与外部名称服务器之间不必要的浪费通信。

从访问缓存中检索信息比对每个 I/O 请求执行整个导出策略规则评估过程要快得多。因此，使用访问缓存可以降低客户端访问检查的开销，从而显著提高性能。

访问缓存参数的工作原理

多个参数用于控制访问缓存中条目的刷新周期。了解这些参数的工作原理后，您可以对其进行修改，以调整访问缓存并平衡性能与存储信息的最新程度。

访问缓存会存储包含一个或多个导出规则的条目，这些规则适用于尝试访问卷或 qtree 的客户端。这些条目会在刷新之前存储一段时间。刷新时间由访问缓存参数决定，并取决于访问缓存条目的类型。

您可以为单个 SVM 指定访问缓存参数。这样，这些参数就可以根据 SVM 访问要求而有所不同。当前未使用的

访问缓存条目不会刷新，从而减少与外部名称服务之间不必要的浪费性通信。

访问缓存条目类型	Description	刷新周期（以秒为单位）
肯定条目	未导致拒绝客户端访问的访问缓存条目。	最小值： 300 最大值： 86 ， 400 默认值： 3,600 。
否定条目	导致客户端访问被拒绝的访问缓存条目。	最小值：60 最大值： 86 ， 400 默认值： 3,600 。

示例

NFS 客户端尝试访问集群上的卷。ONTAP 会将客户端与导出策略规则匹配，并根据导出策略规则配置确定客户端获取访问权限。ONTAP 会将导出策略规则作为肯定条目存储在访问缓存中。默认情况下， ONTAP 会将肯定条目保留在访问缓存中一小时（ 3 ， 600 秒），然后自动刷新该条目以使信息保持最新。

为了防止访问缓存不必要地填满，还提供了一个参数来清除在特定时间段内未用于确定客户端访问的现有访问缓存条目。这 `-harvest-timeout` 参数的允许范围为60到2、592、000秒、默认设置为86、400秒。

从 qtree 删除导出策略

如果您决定不再需要将特定导出策略分配给 qtree ，则可以通过修改 qtree 以继承包含卷的导出策略来删除导出策略。您可以使用执行此操作 `volume qtree modify` 命令 `-export-policy` 参数和空名称字符串("")。

步骤

1. 要从 qtree 中删除导出策略，请输入以下命令：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. 验证是否已相应修改 qtree：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

验证 qtree 文件操作的 qtree ID

ONTAP 可以对 qtree ID 执行可选的额外验证。此验证可确保客户端文件操作请求使用有效的 qtree ID ，并且客户端只能在同一 qtree 内移动文件。您可以通过修改来启用或禁用此验证 `-validate-qtree-export` 参数。默认情况下，此参数处于启用状态。

关于此任务

只有在已将导出策略直接分配给 Storage Virtual Machine （ SVM ）上的一个或多个 qtree 时，此参数才有效。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

如果您希望 **qtree ID** 验证为 …	输入以下命令 …
enabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
已禁用	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

FlexVol 卷的导出策略限制和嵌套接合

如果您将导出策略配置为在嵌套接合上设置限制性较低的策略，而在更高级别的接合上设置限制性较强的策略，则对较低级别的接合的访问可能会失败。

您应确保较高级别的接合与较低级别的接合相比具有较少限制的导出策略。

将 Kerberos 与 NFS 结合使用以增强安全性

ONTAP 支持 Kerberos

Kerberos 可为客户端 / 服务器应用程序提供强大的安全身份验证。身份验证用于向服务器验证用户和进程身份。在 ONTAP 环境中， Kerberos 在 Storage Virtual Machine （ SVM ）和 NFS 客户端之间提供身份验证。

在 ONTAP 9 中，支持以下 Kerberos 功能：

- Kerberos 5 身份验证与完整性检查（ krb5i ）

  Krb5i 使用校验和验证在客户端和服务器之间传输的每个 NFS 消息的完整性。出于安全原因（例如，确保数据未被篡改）和数据完整性原因（例如，在不可靠的网络上使用 NFS 时，防止数据损坏），这一点非常有用。

- Kerberos 5 身份验证与隐私检查（ krb5p ）

  Krb5p 使用校验和对客户端和服务器之间的所有流量进行加密。这种方法更安全，并且会产生更多负载。

- 128 位和 256 位 AES 加密

高级加密标准（Advanced Encryption Standard， AES）是一种用于保护电子数据安全的加密算法。ONTAP支持使用128位密钥的AES (AES-128)和使用256位密钥的AES (AES-256)对Kerberos进行加密、以增强安全性。

- SVM 级别的 Kerberos 域配置

  现在， SVM 管理员可以在 SVM 级别创建 Kerberos 域配置。这意味着 SVM 管理员无需再依赖集群管理员来配置 Kerberos 域，并且可以在多租户环境中创建单独的 Kerberos 域配置。

使用 **NFS** 配置 **Kerberos** 的要求

在系统上使用 NFS 配置 Kerberos 之前，您必须验证网络和存储环境中的某些项是否已正确配置。

> 配置环境的步骤取决于您使用的客户端操作系统，域控制器， Kerberos， DNS 等的版本和类型。本文档不会介绍如何记录所有这些变量。有关详细信息，请参见每个组件的相应文档。
>
> 有关如何在使用 Windows Server 2008 R2 Active Directory 和 Linux 主机的环境中为 NFSv3 和 NFSv4 设置 ONTAP 和 Kerberos 5 的详细示例，请参见技术报告 4073 。

应首先配置以下项：

网络环境要求

- Kerberos

  您必须使用密钥分发中心（KDC）设置有效的 Kerberos，例如基于 Windows Active Directory 的 Kerberos 或 MIT Kerberos 。

  NFS服务器必须使用 `nfs` 作为其机器主体的主要组件。

- 目录服务

  您必须在环境中使用安全目录服务，例如 Active Directory 或 OpenLDAP，该服务配置为使用基于 SSL/TLS 的 LDAP 。

- NTP

  您必须有一个运行 NTP 的工作时间服务器。为了防止因时间偏差而导致 Kerberos 身份验证失败，必须执行此操作。

- 域名解析（DNS）

  每个 UNIX 客户端和每个 SVM LIF 都必须在正向和反向查找区域下向 KDC 注册正确的服务记录（SRV）。所有参与者都必须可通过 DNS 正确解析。

- 用户帐户

  每个客户端在 Kerberos 域中都必须有一个用户帐户。NFS 服务器必须使用 "`NFS` " 作为其计算机主体的主要组件。

NFS客户端要求

- NFS

  必须正确配置每个客户端，以便使用 NFSv3 或 NFSv4 通过网络进行通信。

  客户端必须支持 RFC1964 和 RFC2203 。

- Kerberos

  必须正确配置每个客户端以使用 Kerberos 身份验证，其中包括以下详细信息：

  - 已启用 TGS 通信加密。

    AES-256 可提供最强大的安全性。

  - 启用 TGT 通信最安全的加密类型。
  - 已正确配置 Kerberos 域。
  - 已启用GSS。

    使用计算机凭据时：

  - 请勿运行 `gssd` 使用 `-n` 参数。
  - 请勿运行 `kinit` 以root用户身份。

- 每个客户端都必须使用最新且更新的操作系统版本。

  这样可以为使用 Kerberos 进行 AES 加密提供最佳兼容性和可靠性。

- DNS

  必须正确配置每个客户端，以使用 DNS 进行正确的名称解析。

- NTP

  每个客户端都必须与 NTP 服务器同步。

- 主机和域信息

  每个客户端的 `/etc/hosts` 和 `/etc/resolv.conf` 文件必须分别包含正确的主机名和DNS信息。

- keytab 文件

  每个客户端都必须具有 KDC 中的 keytab 文件。域必须为大写字母。加密类型必须为 AES-256 ，以获得最高安全性。

- 可选：为了获得最佳性能，客户端至少可以使用两个网络接口：一个用于与局域网通信，一个用于与存储网络通信。

存储系统要求

- NFS 许可证

存储系统必须安装有效的 NFS 许可证。

- CIFS许可证

  CIFS 许可证是可选的。只有在使用多协议名称映射时检查 Windows 凭据才需要此功能。在严格的纯 UNIX 环境中不需要此功能。

- SVM

  您必须在系统上至少配置一个 SVM 。

- SVM 上的 DNS

  您必须已在每个 SVM 上配置 DNS 。

- NFS 服务器

  您必须已在 SVM 上配置 NFS 。

- AES 加密

  为了获得最强的安全性，您必须将 NFS 服务器配置为仅允许对 Kerberos 进行 AES-256 加密。

- SMB服务器

  如果您运行的是多协议环境、则必须事先在SVM上配置SMB。多协议名称映射需要SMB服务器。

- Volumes

  您必须具有一个根卷和至少一个数据卷，以供 SVM 使用。

- 根卷

  SVM 的根卷必须具有以下配置：

Name	正在设置 **...**
安全风格	"unix"
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	777

  与根卷不同，数据卷可以采用任一安全模式。

- UNIX 组

  SVM 必须配置以下 UNIX 组：

组名称	组 ID
守护进程	1.
root	0
pcuser	65534 （在创建 SVM 时由 ONTAP 自动创建）

- UNIX用户

  SVM 必须配置以下 UNIX 用户：

用户名	用户 ID	主组 ID	comment
NFS	500	0	GSS INIT阶段需要此参数 NFS 客户端用户 SPN 的第一个组件用作用户。
pcuser	6554	6554	使用NFS和CIFS多协议时需要此参数 在创建SVM时、ONTAP会自动创建并添加到pcuser组中。
root	0	0	挂载时需要

  如果 NFS 客户端用户的 SPN 存在 Kerberos-UNIX 名称映射，则不需要 NFS 用户。

- 导出策略和规则

  您必须已为导出策略配置根卷和数据卷以及 qtree 所需的导出规则。如果通过Kerberos访问SVM的所有卷、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5` ， `krb5i`或 `krb5p`。

- Kerberos-UNIX 名称映射

  如果您希望 NFS 客户端用户 SPN 标识的用户具有 root 权限，则必须创建一个映射到 root 的名称。

相关信息

"NetApp 技术报告 4073：《安全统一身份验证》"

"NetApp 互操作性表工具"

"系统管理"

"逻辑存储管理"

指定 **NFSv4** 的用户 **ID** 域

要指定用户ID域、您可以设置 `-v4-id-domain` 选项

关于此任务

默认情况下，如果设置了 NIS 域，则 ONTAP 将使用 NIS 域进行 NFSv4 用户 ID 映射。如果未设置 NIS 域，则使用 DNS 域。例如，如果您有多个用户 ID 域，则可能需要设置用户 ID 域。域名必须与域控制器上的域配置匹配。NFSv3 不需要此功能。

步骤

1. 输入以下命令：

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

配置名称服务

ONTAP 名称服务交换机配置的工作原理

ONTAP会将名称服务配置信息存储在一个表中、该表相当于 `/etc/nsswitch.conf` 文件。您必须了解该表的功能以及 ONTAP 如何使用它，以便可以根据您的环境对其进行适当配置。

ONTAP 名称服务切换表可确定 ONTAP 为检索特定类型的名称服务信息而查询的名称服务源。ONTAP 会为每个 SVM 维护一个单独的名称服务切换表。

数据库类型

该表为以下每种数据库类型存储一个单独的名称服务列表：

数据库类型	定义名称服务源 ...	有效源为 ...
主机	将主机名转换为 IP 地址	文件， DNS
组	查找用户组信息	文件， nis ， ldap
密码	查找用户信息	文件， nis ， ldap
网络组	正在查找网络组信息	文件， nis ， ldap
命名映射	正在映射用户名	文件， LDAP

源类型

源用于指定用于检索相应信息的名称服务源。

指定源类型 ...	查找信息的位置	由命令系列管理 ...

文件	本地源文件	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在 SVM 的 NIS 域配置中指定的外部 NIS 服务器	`vserver services name-service nis-domain`
ldap	在 SVM 的 LDAP 客户端配置中指定的外部 LDAP 服务器	`vserver services name-service ldap`
DNS	在 SVM 的 DNS 配置中指定的外部 DNS 服务器	`vserver services name-service dns`

即使您计划使用NIS或LDAP进行数据访问和SVM管理身份验证、也仍应包括 `files` 并将本地用户配置为在NIS或LDAP身份验证失败时的回退。

用于访问外部源的协议

要访问外部源的服务器， ONTAP 使用以下协议：

外部名称服务源	用于访问的协议
NIS	UDP
DNS	UDP
LDAP	TCP

示例

以下示例显示了 SVM SVM_1 的名称服务开关配置：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

要查找主机的 IP 地址， ONTAP 首先会查找本地源文件。如果查询未返回任何结果，则接下来会检查 DNS 服务器。

要查找用户或组信息， ONTAP 仅会查找本地源文件。如果查询未返回任何结果，则查找将失败。

要查找网络组信息， ONTAP 首先会查找外部 NIS 服务器。如果查询未返回任何结果，则接下来会检查本地网络组文件。

SVM SVM_1 的表中没有用于名称映射的名称服务条目。因此，默认情况下， ONTAP 仅会查找本地源文件。

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

使用 LDAP

LDAP 概述

通过 LDAP （轻型目录访问协议）服务器，您可以集中维护用户信息。如果您将用户数据库存储在环境中的 LDAP 服务器上，则可以将存储系统配置为在现有 LDAP 数据库中查找用户信息。

- 在为 ONTAP 配置 LDAP 之前，您应验证站点部署是否符合 LDAP 服务器和客户端配置的最佳实践。具体而言，必须满足以下条件：
  - LDAP 服务器的域名必须与 LDAP 客户端上的条目匹配。
  - LDAP 服务器支持的 LDAP 用户密码哈希类型必须包括 ONTAP 支持的类型：
    - 加密（所有类型）和 SHA-1 （ SHA ， SSHA ）。
    - 从 ONTAP 9.8 开始， SHA-2 哈希（ SHA-256 ， SSH/384 ， SHA-512 ， SSHA-256 ， SSHA-384 和 SSHA-512 ）。
  - 如果 LDAP 服务器需要会话安全措施，则必须在 LDAP 客户端中配置这些措施。

    可以使用以下会话安全选项：

    - LDAP 签名（提供数据完整性检查）和 LDAP 签名和签章（提供数据完整性检查和加密）
    - START TLS

    - LDAPS （基于 TLS 或 SSL 的 LDAP ）
  - 要启用签名和签章的 LDAP 查询，必须配置以下服务：
    - LDAP 服务器必须支持 GSSAPI （ Kerberos ） SASL 机制。
    - LDAP 服务器必须在 DNS 服务器上设置 DNS A/AAAA 记录以及 PTR 记录。
    - Kerberos 服务器必须在 DNS 服务器上存在 SRV 记录。
  - 要启用启动 TLS 或 LDAPS ，应考虑以下几点。
    - NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。
    - 如果使用 LDAPS ，则必须在 ONTAP 9.5 及更高版本中为 TLS 或 SSL 启用 LDAP 服务器。ONTAP 9.09.4 不支持 SSL 。
    - 必须已在域中配置证书服务器。
  - 要启用 LDAP 转介跟踪（在 ONTAP 9.5 及更高版本中），必须满足以下条件：
    - 这两个域都应配置以下信任关系之一：
      - 双向
      - 单向，主站点信任转介域
      - 父 - 子
    - 必须配置 DNS 以解析所有转介的服务器名称。
    - 在进行身份验证时、域密码应相同 `--bind-as-cifs-server` 设置为true。

> LDAP 转介跟踪不支持以下配置。
>
> - 对于所有 ONTAP 版本：
> - 管理 SVM 上的 LDAP 客户端
> - 对于 ONTAP 9.8 及更早版本（ 9.9.1 及更高版本支持这些功能）：
> - LDAP签名和签章(`-session-security` 选项)
> - 加密TLS连接(`-use-start-tls` 选项)
> - 通过LAPS端口636 (`-use-ldaps-for-ad-ldap` 选项)

- 从ONTAP 9.11.1开始、您可以使用 "用于nsswitch身份验证的LDAP快速绑定。"
- 在 SVM 上配置 LDAP 客户端时，必须输入 LDAP 模式。

  在大多数情况下，默认 ONTAP 模式之一是合适的。但是，如果环境中的 LDAP 模式与这些模式不同，则必须在创建 LDAP 客户端之前为 ONTAP 创建新的 LDAP 客户端模式。有关您的环境要求，请咨询 LDAP 管理员。

- 不支持使用 LDAP 进行主机名解析。

对于追加信息，请参见 "NetApp 技术报告 4835： 《如何在 ONTAP 中配置 LDAP 》"。

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （ AD ）服务器的查

询启用 LDAP 会话安全性。您必须将Storage Virtual Machine (SVM)上的NFS服务器安全设置配置为与LDAP服务器上的安全设置相对应。

签名可使用密钥技术确认 LDAP 有效负载数据的完整性。密封功能对 LDAP 有效负载数据进行加密，以避免以明文形式传输敏感信息。"_LDAP 安全级别 _ " 选项指示 LDAP 流量是需要签名，签名和签章，还是两者都不需要。默认值为 `none`。测试

已使用在SVM上启用SMB流量的LDAP签名和签章 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

LDAPS 概念

您必须了解有关 ONTAP 如何确保 LDAP 通信安全的某些术语和概念。ONTAP 可以使用启动 TLS 或 LDAPS 在 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器之间设置经过身份验证的会话。

术语

有关 ONTAP 如何使用 LDAPS 保护 LDAP 通信，您应了解一些特定术语。

- * LDAP *

  （轻型目录访问协议）一种用于访问和管理信息目录的协议。LDAP 用作存储用户，组和网络组等对象的信息目录。LDAP 还提供目录服务，用于管理这些对象并满足 LDAP 客户端的 LDAP 请求。

- * ssl*

  （安全套接字层）一种专为通过 Internet 安全发送信息而开发的协议。ONTAP 9及更高版本支持SSL、但已弃用而改用TLS。

- * TLS *

  （传输层安全性）基于早期 SSL 规范的 IETF 标准跟踪协议。它是 SSL 的后继协议。ONTAP 9.5及更高版本支持TLS。

- * LDAPS （基于 SSL 或 TLS 的 LDAP ） *

  一种使用 TLS 或 SSL 保护 LDAP 客户端与 LDAP 服务器之间通信安全的协议。术语_LDAP over SSL_ 和_LDAP over TLS_有时可以互换使用。ONTAP 9.5及更高版本支持LAPS。

  - 在 ONTAP 9.2-9.8 中，只能在端口 636 上启用 LDAPS 。要执行此操作、请使用 `-use-ldaps-for-ad-ldap` 参数 `vserver cifs security modify` 命令：
  - 从 ONTAP 9.1.1 开始，可以在任何端口上启用 LDAPS ，但端口 636 仍为默认端口。为此、请设置 `-ldaps-enabled` 参数设置为 `true` 并指定所需的 `-port` 参数。有关详细信息，请参见 `vserver services name-service ldap client create` 手册页

  > NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。

- * 启动 TL*

  （也称为 *start_tls* ， *STARTTLS* _ 和 _*Starttls* ）一种使用 TLS 协议提供安全通信的机制。

ONTAP 使用 STARTTLS 保护 LDAP 通信，并使用默认 LDAP 端口（389）与 LDAP 服务器进行通信。必须将 LDAP 服务器配置为允许通过 LDAP 端口 389 进行连接；否则，从 SVM 到 LDAP 服务器的 LDAP TLS 连接将失败。

ONTAP 如何使用 LDAPS

ONTAP 支持 TLS 服务器身份验证，从而使 SVM LDAP 客户端能够在绑定操作期间确认 LDAP 服务器的身份。启用了 TLS 的 LDAP 客户端可以使用公共密钥加密的标准技术来检查服务器的证书和公有 ID 是否有效以及是否由客户端的可信 CA 列表中列出的证书颁发机构（CA）颁发。

LDAP 支持 STARTTLS 使用 TLS 对通信进行加密。StartTLS 以标准 LDAP 端口（389）上的纯文本连接开头，然后该连接升级到 TLS 。

ONTAP 支持以下功能：

- LDAPS 用于 Active Directory 集成的 LDAP 服务器和 SVM 之间的 SMB 相关流量
- LDAP 流量的 LDAPS ，用于名称映射和其他 UNIX 信息

  可以使用 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器来存储 LDAP 名称映射的信息以及其他 UNIX 信息，例如用户，组和网络组。

- 自签名根 CA 证书

  使用 Active Directory 集成的 LDAP 时，在域中安装 Windows Server 证书服务时会生成自签名根证书。使用基于 UNIX 的 LDAP 服务器进行 LDAP 名称映射时，系统会使用适用于该 LDAP 应用程序的方法生成并保存自签名根证书。

默认情况下、LDIPS处于禁用状态。

启用 **LDAP RFC2307bis** 支持

如果您要使用 LDAP 并需要使用嵌套组成员资格的附加功能，则可以将 ONTAP 配置为启用 LDAP RFC2307bis 支持。

您需要的内容

您必须已为要使用的一个默认 LDAP 客户端模式创建一个副本。

关于此任务

在 LDAP 客户端模式中，组对象使用 memberUid 属性。此属性可以包含多个值，并列出属于该组的用户的名称。在启用了 RFC2307bis 的 LDAP 客户端模式中，组对象使用 uniqueMember 属性。此属性可以包含 LDAP 目录中另一个对象的完整可分辨名称（DN）。这样，您就可以使用嵌套组，因为组可以将其他组作为成员。

用户所属的组不应超过 256 个，包括嵌套组。ONTAP 会忽略超过 256 组限制的任何组。

默认情况下， RFC2307bis 支持处于禁用状态。

> 使用 MS-AD-BIS 模式创建 LDAP 客户端时， ONTAP 会自动启用 RFC2307bis 支持。

对于追加信息，请参见 "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 修改复制的 RFC2307 LDAP 客户端模式以启用 RFC2307bis 支持：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改模式以匹配 LDAP 服务器中支持的对象类：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改模式以匹配 LDAP 服务器中支持的属性名称：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

LDAP 目录搜索的配置选项

您可以通过配置 ONTAP LDAP 客户端以最适合您的环境的方式连接到 LDAP 服务器来优化 LDAP 目录搜索，包括用户，组和网络组信息。您需要了解默认 LDAP 基础和范围搜索值何时足够，以及在自定义值更合适时需要指定哪些参数。

LDAP 客户端的用户，组和网络组信息搜索选项有助于避免 LDAP 查询失败，从而避免客户端无法访问存储系统。它们还有助于确保搜索尽可能高效，以避免客户端性能问题。

默认基础和范围搜索值

LDAP 基础是 LDAP 客户端用于执行 LDAP 查询的默认基础 DN 。所有搜索，包括用户，组和网络组搜索，均使用基础 DN 完成。如果 LDAP 目录相对较小且所有相关条目都位于同一 DN 中，则此选项适用。

如果未指定自定义基础DN、则默认值为 `root`。这意味着每个查询都会搜索整个目录。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

LDAP 基础范围是 LDAP 客户端用于执行 LDAP 查询的默认搜索范围。所有搜索，包括用户，组和网络组搜索，均使用基础范围完成。它将确定 LDAP 查询是仅搜索命名条目， DN 下一级的条目还是该 DN 下的整个子树。

如果未指定自定义基础范围、则默认值为 `subtree`。这意味着每个查询都会搜索 DN 下的整个子树。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

自定义基础和范围搜索值

您也可以为用户，组和网络组搜索指定单独的基准值和范围值。通过这种方式限制查询的搜索基础和范围可以显

著提高性能，因为它会将搜索限制为 LDAP 目录的较小部分。

如果指定自定义基础值和范围值，则这些值将覆盖用户，组和网络组搜索的常规默认搜索基础和范围。用于指定自定义基础值和范围值的参数可在高级权限级别使用。

LDAP 客户端参数 …	指定自定义 …
`-base-dn`	所有 LDAP 搜索的基础 DN 如果需要，可以输入多个值（例如，如果在 ONTAP 9.5 及更高版本中启用了 LDAP 转介跟踪）。
`-base-scope`	所有 LDAP 搜索的基本范围
`-user-dn`	所有 LDAP 用户搜索的基础 DNS 此参数也适用于适用场景用户名映射搜索。
`-user-scope`	所有 LDAP 用户搜索的基本范围此参数也适用于适用场景用户名映射搜索。
`-group-dn`	所有 LDAP 组搜索的基础 DNS
`-group-scope`	所有 LDAP 组搜索的基础范围
`-netgroup-dn`	所有 LDAP 网络组搜索的基础 DNS
`-netgroup-scope`	所有 LDAP 网络组搜索的基本范围

多个自定义基础 **DN** 值

如果 LDAP 目录结构更复杂，则可能需要指定多个基础 DNS 来搜索 LDAP 目录的多个部分以查找某些信息。您可以为用户，组和网络组 DN 参数指定多个 DNS ，方法是使用分号（；）将其分隔开，并使用双引号（"）将整个 DN 搜索列表括起来。如果 DN 包含分号，则必须在 DN 中的分号前面添加一个转义字符（\）。

请注意，范围适用场景是为相应参数指定的整个 DNS 列表。例如，如果为用户范围指定了一个包含三个不同用户 DNS 和子树的列表，则 LDAP 用户搜索将在整个子树中搜索三个指定 DNS 中的每个 DNS 。

从 ONTAP 9.5 开始，您还可以指定 ldap_referral Chasing ，这样，如果主 LDAP 服务器未返回 LDAP 转介响应，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。客户端使用该转介数据从转介数据中所述的服务器检索目标对象。要搜索转介 LDAP 服务器中的对象，可以在 LDAP 客户端配置中将转介对象的基础 DN 添加到基础 DN 中。但是、只有在启用转介跟踪(使用)后、才会查找转介对象 `-referral-enabled true` 选项)。

提高 **LDAP** 目录 **netgroup-by-host** 搜索的性能

如果 LDAP 环境配置为允许按主机搜索网络组，则可以将 ONTAP 配置为利用此功能并按主机执行网络组搜索。这样可以显著加快网络组搜索速度，并减少因网络组搜索期间出现延迟而可能导致的 NFS 客户端访问问题。

您需要的内容

LDAP目录必须包含 `netgroup.byhost` 映射。

DNS 服务器应同时包含 NFS 客户端的正向（A）和反向（PTR）查找记录。

在网络组中指定 IPv6 地址时，必须始终按照 RFC 5952 中的说明缩短和压缩每个地址。

关于此任务

NIS服务器将网络组信息存储在三个单独的映射中、这些映射称为 `netgroup`， `netgroup.byuser`，和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 映射用于加快网络组搜索速度。ONTAP 可以在 NIS 服务器上按主机执行网络组搜索，以缩短挂载响应时间。

默认情况下、LDAP目录不具有此类 `netgroup.byhost` 映射为NIS服务器。但是、借助第三方工具、可以导入NIS `netgroup.byhost` 映射到LDAP目录以启用按主机快速网络组搜索。如果您已将LDAP环境配置为允许按主机搜索网络组、则可以使用配置ONTAP LDAP客户端 `netgroup.byhost` 映射名称、DN和搜索范围、以加快按主机搜索网络组的速度。

通过更快地接收按主机搜索网络组的结果， ONTAP 可以在 NFS 客户端请求访问导出时更快地处理导出规则。这样可以减少因网络组搜索延迟问题而导致访问延迟的可能性。

步骤

1. 获取NIS的准确完整可分辨名称 `netgroup.byhost` 映射已导入到LDAP目录。

   映射 DN 可能因用于导入的第三方工具而异。为了获得最佳性能，应指定确切的映射 DN 。

2. 将权限级别设置为高级： `set -privilege advanced`

3. 在Storage Virtual Machine (SVM)的LDAP客户端配置中启用按主机搜索网络组： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`}启用或禁用对LDAP目录的按主机网络组搜索。默认值为 `false`。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` 指定的可分辨名称 `netgroup.byhost` 映射到LDAP目录中。它会覆盖 netgroup-by-host 搜索的基础 DN 。如果不指定此参数，则 ONTAP 将改用基础 DN 。

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`}指定按主机搜索网络组的搜索范围。如果未指定此参数、则默认值为 `subtree`。

   如果LDAP客户端配置尚不存在、则可以在使用创建新的LDAP客户端配置时通过指定这些参数来启用按主机进行网络组搜索 `vserver services name-service ldap client create` 命令：

   > 从ONTAP 9.2开始、此字段为 `-ldap-servers` 替换字段 `-servers`。此新字段可以使用 LDAP 服务器的主机名或 IP 地址。

4. 返回到管理权限级别： `set -privilege admin`

示例

以下命令将修改名为"`ldap_corp`"的现有LDAP客户端配置、以使用启用netgroup-by主机搜索 `netgroup.byhost` 映射名为"`nisMapName="netgroup.byHost"、dc=corp、dc=ex例如、dc=com`"和默认搜索范围 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成后

。 `netgroup.byhost` 和 `netgroup` 目录中的映射必须始终保持同步、以避免出现客户端访问问题。

相关信息

"IETF RFC 5952： IPv6 地址文本表示建议"

使用**LDAP**快速绑定进行**nsswitch**身份验证

从ONTAP 9.11.1开始、您可以利用ldap_fast bind_功能(也称为_concurrent bind_)来更快、更简单地处理客户端身份验证请求。要使用此功能、LDAP服务器必须支持快速绑定功能。

关于此任务

如果没有快速绑定、ONTAP 将使用LDAP简单绑定向LDAP服务器对管理员用户进行身份验证。使用此身份验证方法、ONTAP 会向LDAP服务器发送用户或组名称、接收存储的哈希密码、并将服务器哈希代码与本地通过用户密码生成的哈希密码进行比较。如果它们相同、则ONTAP 会授予登录权限。

借助快速绑定功能、ONTAP 仅通过安全连接向LDAP服务器发送用户凭据(用户名和密码)。然后、LDAP服务器会验证这些凭据并指示ONTAP 授予登录权限。

快速绑定的一个优势是、ONTAP 无需支持LDAP服务器支持的每个新哈希算法、因为密码哈希是由LDAP服务器执行的。

"了解如何使用快速绑定。"

您可以使用现有LDAP客户端配置进行LDAP快速绑定。但是、强烈建议为LDAP客户端配置TLS或LDAPS；否则、密码将通过线缆以纯文本形式发送。

要在ONTAP 环境中启用LDAP快速绑定、您必须满足以下要求：

- 必须在支持快速绑定的LDAP服务器上配置ONTAP 管理员用户。
- 必须在名称服务开关(nsswitch)数据库中为LDAP配置ONTAP SVM。
- 必须使用快速绑定为nsswitch身份验证配置ONTAP 管理员用户和组帐户。

步骤

1. 与LDAP管理员确认LDAP服务器支持LDAP快速绑定。
2. 确保已在LDAP服务器上配置ONTAP 管理员用户凭据。
3. 验证是否已为LDAP快速绑定正确配置管理或数据SVM。

a. 要确认LDAP快速绑定服务器已在LDAP客户端配置中列出、请输入：

```
vserver services name-service ldap client show
```

"了解LDAP客户端配置。"

b. 以确认此情况 `ldap` 是为nsswitch配置的源之一 `passwd` 数据库、输入：

```
vserver services name-service ns-switch show
```

"了解nsswitch配置。"

4. 确保管理员用户正在使用nsswitch进行身份验证、并且已在其帐户中启用LDAP快速绑定身份验证。

   - 对于现有用户、输入 `security login modify` 并验证以下参数设置：

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

   - 对于新的管理员用户、请参见 "启用LDAP或NIS帐户访问。"

显示**LDAP**统计信息

从 ONTAP 9.2 开始，您可以显示存储系统上 Storage Virtual Machine （SVM）的 LDAP 统计信息，以监控性能并诊断问题。

您需要的内容

- 您必须已在 SVM 上配置 LDAP 客户端。
- 您必须已确定可从中查看数据的 LDAP 对象。

步骤

1. 查看计数器对象的性能数据：

```
statistics show
```

示例

以下示例显示了对象的性能数据 `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

配置名称映射

配置名称映射概述

ONTAP 使用名称映射将 SMB 身份映射到 UNIX 身份，将 Kerberos 身份映射到 UNIX 身份以及将 UNIX 身份映射到 SMB 身份。无论用户是从 NFS 客户端还是从 SMB 客户端进行连接， IT 都需要此信息来获取用户凭据并提供正确的文件访问权限。

除了两个例外情况，您无需使用名称映射：

- 您配置的是纯 UNIX 环境，不打算在卷上使用 SMB 访问或 NTFS 安全模式。
- 您可以配置要使用的默认用户。

  在这种情况下，不需要进行名称映射，因为所有客户端凭据都映射到同一默认用户，而不是映射每个客户端凭据。

请注意，您只能对用户使用名称映射，而不能对组使用名称映射。

但是，您可以将一组用户映射到特定用户。例如，您可以将以 SALES 开头或结尾的所有 AD 用户映射到特定

UNIX 用户和用户的 UID 。

名称映射的工作原理

当 ONTAP 必须映射用户的凭据时，它会首先检查本地名称映射数据库和 LDAP 服务器中是否存在现有映射。它是检查一个还是同时检查这两者，以及检查顺序取决于 SVM 的名称服务配置。

- 适用于 Windows 到 UNIX 的映射

  如果未找到映射， ONTAP 将检查小写的 Windows 用户名是否为 UNIX 域中的有效用户名。如果此操作不起作用，则只要配置了默认 UNIX 用户，它就会使用默认 UNIX 用户。如果未配置默认 UNIX 用户，并且 ONTAP 也无法通过这种方式获取映射，则映射将失败并返回错误。

- UNIX 到 Windows 的映射

  如果未找到映射， ONTAP 将尝试查找与 SMB 域中的 UNIX 名称匹配的 Windows 帐户。如果此操作不起作用，则会使用默认 SMB 用户，但前提是已配置此用户。如果未配置默认SMB用户、并且ONTAP也无法通过此方式获取映射、则映射将失败并返回错误。

默认情况下，计算机帐户映射到指定的默认 UNIX 用户。如果未指定默认 UNIX 用户，计算机帐户映射将失败。

- 从 ONTAP 9.5 开始，您可以将计算机帐户映射到默认 UNIX 用户以外的用户。
- 在 ONTAP 9.4 及更早版本中，您无法将计算机帐户映射到其他用户。

  即使为计算机帐户定义了名称映射，也会忽略这些映射。

多域搜索 **UNIX** 用户到 **Windows** 用户名映射

在将 UNIX 用户映射到 Windows 用户时， ONTAP 支持多域搜索。系统将搜索所有已发现的受信任域以查找与替换模式匹配的匹配项，直到返回匹配结果为止。或者，您也可以配置首选受信任域列表，该列表将代替发现的受信任域列表使用，并按顺序进行搜索，直到返回匹配结果为止。

域信任如何影响 **UNIX** 用户到 **Windows** 用户名称映射搜索

要了解多域用户名映射的工作原理，您必须了解域信任如何与 ONTAP 配合使用。与SMB服务器主域的Active Directory信任关系可以是双向信任、也可以是两种类型的单向信任之一、即入站信任或出站信任。主域是SVM上的SMB服务器所属的域。

- _ 双向信任 _

  通过双向信任，两个域相互信任。如果SMB服务器的主域与另一个域具有双向信任、则主域可以对属于受信任域的用户进行身份验证和授权、反之亦然。

  UNIX 用户到 Windows 用户名映射搜索只能在主域和另一个域之间具有双向信任的域上执行。

- 出站信任 _

  对于出站信任，主域信任另一个域。在这种情况下，主域可以对属于出站受信任域的用户进行身份验证和授

权。

执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有出站信任的域。

- *Inbound trust*

  对于入站信任、另一个域信任SMB服务器的主域。在这种情况下，主域无法对属于入站受信任域的用户进行身份验证或授权。

  在执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有入站信任的域。

如何使用通配符（*）配置名称映射的多域搜索

在 Windows 用户名的域部分使用通配符有助于进行多域名称映射搜索。下表说明了如何在名称映射条目的域部分使用通配符来启用多域搜索：

Pattern	更换	结果
root	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ 管理员	UNIX 用户 "`root` " 将映射到名为 "`administrator` " 的用户。系统会按顺序搜索所有受信任域，直到找到第一个名为 "`administrator` " 的匹配用户为止。
*	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ ｛asterisk｝	有效的 UNIX 用户将映射到相应的 Windows 用户。系统将按顺序搜索所有受信任域，直到找到具有该名称的第一个匹配用户为止。 模式 ｛asterisk｝ ｛un斜 杠｝ ｛un斜 杠｝ ｛asterisk｝ 仅适用于从 UNIX 到 Windows 的名称映射，而不是相反。

如何执行多域名搜索

您可以选择以下两种方法之一来确定用于多域名搜索的受信任域列表：

- 使用由 ONTAP 编译的自动发现的双向信任列表
- 使用您编译的首选受信任域列表

如果将 UNIX 用户映射到使用通配符用于用户名的域部分的 Windows 用户，则会在所有受信任域中查找此 Windows 用户，如下所示：

- 如果配置了首选受信任域列表，则只会在此搜索列表中按顺序查找映射的 Windows 用户。
- 如果未配置首选受信任域列表，则会在主域的所有双向受信任域中查找 Windows 用户。
- 如果主域没有双向受信任的域，则会在主域中查找用户。

如果 UNIX 用户映射到用户名中没有域部分的 Windows 用户，则会在主域中查找此 Windows 用户。

名称映射转换规则

ONTAP 系统会为每个 SVM 保留一组转换规则。每个规则都包含两部分： *pattern* 和 *replacement* 。转换从相应列表的开头开始，并根据第一个匹配规则执行替换。模式是 UNIX 模式的正则表达式。替换项是一个字符串、其中包含表示模式中的子表达式的转义序列、与UNIX中的情况一样 `sed` 计划。

创建名称映射

您可以使用 `vserver name-mapping create` 命令以创建名称映射。您可以使用名称映射使 Windows 用户能够访问 UNIX 安全模式卷，反之亦然。

关于此任务

对于每个 SVM ， ONTAP 支持每个方向最多 12 ， 500 个名称映射。

步骤

1. 创建名称映射：

   ```
   vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
   unix|unix-win} -position integer -pattern text -replacement text
   ```

   > 。 `-pattern` 和 `-replacement` 语句可以表达为正则表达式。您也可以使用 `-replacement` 用于使用空替换字符串明确拒绝映射到用户的语句 `" "` (空格字符)。请参见 `vserver name-mapping create` 有关详细信息、请参见手册页。

   创建 Windows 到 UNIX 映射时，在创建新映射时与 ONTAP 系统建立了打开连接的任何 SMB 客户端都必须注销并重新登录才能查看新映射。

示例

以下命令将在名为 vs1 的 SVM 上创建名称映射。此映射是指优先级列表中位置 1 处从 UNIX 到 Windows 的映射。映射会将 UNIX 用户 johnd 映射到 Windows 用户 ENG\JohnDoe 。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此映射是指优先级列表中位置 1 处从 Windows 到 UNIX 的映射。此处的模式和替换项包括正则表达式。此映射会将域 ENG 中的每个 CIFS 用户映射到与 SVM 关联的 LDAP 域中的用户。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此处的模式将 "` $` " 作为必须转义的 Windows 用户名中的一个元素。映射会将 Windows 用户 ENG\ john$ops 映射到 UNIX 用户 john_ops 。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

配置默认用户：

您可以配置一个默认用户，以便在用户的所有其他映射尝试均失败或不希望在 UNIX 和 Windows 之间映射单个用户时使用。或者，如果您希望对未映射用户的身份验证失败，则不应配置默认用户。

关于此任务

对于 CIFS 身份验证，如果不希望将每个 Windows 用户映射到单个 UNIX 用户，则可以改为指定默认 UNIX 用户。

对于 NFS 身份验证，如果不希望将每个 UNIX 用户映射到单个 Windows 用户，则可以改为指定一个默认 Windows 用户。

步骤

1. 执行以下操作之一：

如果您要 …	输入以下命令 …
配置默认 UNIX 用户	`vserver cifs options modify -default-unix-user user_name`
配置默认 Windows 用户	`vserver nfs modify -default-win-user user_name`

用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 …	使用此命令 …
创建名称映射	`vserver name-mapping create`
在特定位置插入名称映射	`vserver name-mapping insert`
显示名称映射	`vserver name-mapping show`
交换两个名称映射的位置 注意：如果为名称映射配置了IP限定符条目、则不允许进行交换。	`vserver name-mapping swap`

修改名称映射	`vserver name-mapping modify`
删除名称映射	`vserver name-mapping delete`
验证名称映射是否正确	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

有关详细信息，请参见每个命令的手册页。

为 **Windows NFS** 客户端启用访问

ONTAP 支持从 Windows NFSv3 客户端访问文件。这意味着、运行支持NFSv3的Windows操作系统的客户端可以访问集群上NFSv3导出上的文件。要成功使用此功能，您必须正确配置 Storage Virtual Machine （ SVM ）并了解某些要求和限制。

关于此任务

默认情况下， Windows NFSv3 客户端支持处于禁用状态。

开始之前

必须在 SVM 上启用 NFSv3 。

步骤

1. 启用 Windows NFSv3 客户端支持：

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. 在支持Windows NFSv3客户端的所有SVM上、禁用 `-enable-ejukebox` 和 `-v3-connection-drop` 参数：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
   ```

   Windows NFSv3 客户端现在可以在存储系统上挂载导出。

3. 通过指定、确保每个Windows NFSv3客户端都使用硬挂载 `-o mtype=hard` 选项

   这是确保可靠挂载所必需的。

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

在 **NFS** 客户端上启用 **NFS** 导出显示

NFS客户端可以使用 `showmount -e` 命令以查看可从ONTAP NFS服务器导出的列表。这有助于用户确定要挂载的文件系统。

从 ONTAP 9.2 开始，默认情况下， ONTAP 允许 NFS 客户端查看导出列表。在早期版本中、 `showmount` 的选项 `vserver nfs modify` 命令必须显式启用。要查看导出列表，应在 SVM 上启用 NFSv3 。

示例

以下命令显示了名为 vs1 的 SVM 上的 showmount 功能：

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

在 NFS 客户端上执行的以下命令显示 IP 地址为 10.63.21.9 的 NFS 服务器上的导出列表：

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

使用NFS管理文件访问

启用或禁用NFSv3

您可以通过修改来启用或禁用NFSv3 `-v3` 选项这样，客户端就可以使用 NFSv3 协议访问文件。默认情况下， NFSv3 处于启用状态。

步骤

1. 执行以下操作之一：

如果您要 …	输入命令 …
启用 NFSv3：	`vserver nfs modify -vserver vserver_name -v3 enabled`
禁用NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

启用或禁用 NFSv4.0

您可以通过修改来启用或禁用NFSv4.0 `-v4.0` 选项这样，使用 NFSv4.0 协议的客户端就可以访问文件。在 ONTAP 9.1.1 中，默认情况下会启用 NFSv4.0 ；在早期版本中，默认情况下会禁用 NFSv4.0 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用 NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
禁用 NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

启用或禁用**NFSv4.1**

您可以通过修改来启用或禁用NFSv4.1 `-v4.1` 选项这样，使用 NFSv4.1 协议的客户端便可访问文件。在 ONTAP 9.1.1 中，默认启用 NFSv4.1 ；在早期版本中，默认禁用 NFSv4.1 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
禁用NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

管理**NFSv4**存储池限制

从ONTAP 9.13开始、管理员可以使NFSv4服务器在达到每个客户端存储池资源限制时拒绝向NFSv4客户端提供资源。如果客户端使用的NFSv4存储池资源过多、则可能会导致其他NFSv4客户端因NFSv4存储池资源不可用而被阻止。

通过启用此功能、客户还可以查看每个客户端的活动存储池资源消耗情况。这样可以更轻松地确定耗尽系统资源的客户端、并可以按客户端设置资源限制。

查看已用存储池资源

。 `vserver nfs storepool show` 命令可显示已使用的存储池资源数量。存储池是NFSv4客户端使用的资源池。

步骤

1. 以管理员身份运行 `vserver nfs storepool show` 命令以显示NFSv4客户端的存储池信息。

示例

此示例显示了NFSv4客户端的存储池信息。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

启用或禁用存储池限制控制

管理员可以使用以下命令启用或禁用存储池限制控制。

步骤

1. 以管理员身份执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用存储池限制控制	`vserver nfs storepool config modify -limit-enforce enabled`
禁用存储池限制控制	`vserver nfs storepool config modify -limit-enforce disabled`

查看被阻止的客户端列表

如果启用了存储池限制、则管理员可以查看在达到每个客户端资源阈值时哪些客户端被阻止。管理员可以使用以下命令查看哪些客户端已标记为被阻止的客户端。

步骤

1. 使用 `vserver nfs storepool blocked-client show` 命令以显示NFSv4阻止的客户端列表。

从阻止的客户端列表中删除客户端

达到每个客户端阈值的客户端将断开连接并添加到块-客户端缓存中。管理员可以使用以下命令从块客户端缓存中删除客户端。这样、客户端便可连接到ONTAP NFSv4服务器。

步骤

1. 使用 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 命令以转储存储池已阻止的客户端缓存。
2. 使用 `vserver nfs storepool blocked-client show` 命令以验证客户端是否已从块客户端缓存中删除。

示例

此示例显示一个被阻止的客户端、其IP地址"10.2.1.1"正在从所有节点转储。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

启用或禁用 **pNFS**

pNFS 允许 NFS 客户端直接并联对存储设备执行读 / 写操作，从而绕过 NFS 服务器作为潜在瓶颈，从而提高性能。要启用或禁用pNFS (并行NFS)、您可以修改 `-v4.1-pnfs` 选项

ONTAP 版本	**pNFS** 默认值为 ...
9.8或更高版本	已禁用
9.7或更早版本	enabled

您需要的内容

要使用 pNFS ，需要 NFSv4.1 支持。

如果要启用 pNFS ，必须先禁用 NFS 转介。它们不能同时启用。

如果在 SVM 上将 pNFS 与 Kerberos 结合使用，则必须在 SVM 上的每个 LIF 上启用 Kerberos 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
启用 pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`

如果您要 ...	输入命令 ...
禁用 pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

相关信息

- NFS中继概述

通过 **TCP** 和 **UDP** 控制 **NFS** 访问

您可以通过修改来启用或禁用通过TCP和UDP对Storage Virtual Machine (SVM)的NFS访问 `-tcp` 和 `-udp` 参数。这样，您可以控制 NFS 客户端是否可以在环境中通过 TCP 或 UDP 访问数据。

关于此任务

这些参数仅适用于 NFS 。它们不会影响辅助协议。例如，如果禁用基于 TCP 的 NFS ，则通过 TCP 的挂载操作仍会成功。要完全阻止 TCP 或 UDP 流量，您可以使用导出策略规则。

> 在为 NFS 禁用 TCP 之前，必须关闭 SnapDiff RPC 服务器，以避免出现命令失败错误。您可以使用命令禁用TCP `vserver snapdiff-rpc-server off -vserver vserver name`。

步骤

1. 执行以下操作之一：

如果您希望 NFS 访问 ...	输入命令 ...
已通过 TCP 启用	`vserver nfs modify -vserver vserver_name -tcp enabled`
已通过 TCP 禁用	`vserver nfs modify -vserver vserver_name -tcp disabled`
通过 UDP 启用	`vserver nfs modify -vserver vserver_name -udp enabled`
已通过UDP禁用	`vserver nfs modify -vserver vserver_name -udp disabled`

控制来自非保留端口的 **NFS** 请求

您可以通过启用来拒绝来自非保留端口的NFS挂载请求 `-mount-rootonly` 选项要拒绝来自非保留端口的所有NFS请求、您可以启用 `-nfs-rootonly` 选项

关于此任务

默认情况下、是选项 `-mount-rootonly` 为 `enabled`。

默认情况下、是选项 `-nfs-rootonly` 为 `disabled`。

这些选项不适用于空操作步骤。

步骤

1. 执行以下操作之一：

如果您要 …	输入命令 …
允许来自非保留端口的 NFS 挂载请求	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
拒绝来自非保留端口的 NFS 挂载请求	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
允许来自非保留端口的所有 NFS 请求	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
拒绝来自非保留端口的所有 NFS 请求	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

处理未知 **UNIX** 用户对 **NTFS** 卷或 **qtree** 的 **NFS** 访问

如果 ONTAP 无法识别尝试使用 NTFS 安全模式连接到卷或 qtree 的 UNIX 用户，则无法将该用户显式映射到 Windows 用户。您可以将 ONTAP 配置为拒绝访问此类用户以提高安全性，或者将其映射到默认 Windows 用户以确保所有用户的最低访问级别。

您需要的内容

如果要启用此选项，必须配置默认 Windows 用户。

关于此任务

如果 UNIX 用户尝试访问采用 NTFS 安全模式的卷或 qtree ，则必须先将 UNIX 用户映射到 Windows 用户，以便 ONTAP 能够正确评估 NTFS 权限。但是，如果 ONTAP 无法在已配置的用户信息名称服务源中查找 UNIX 用户的名称，则无法将 UNIX 用户显式映射到特定的 Windows 用户。您可以通过以下方式决定如何处理此类未知 UNIX 用户：

- 拒绝对未知 UNIX 用户的访问。

  这样就要求所有 UNIX 用户都显式映射才能访问 NTFS 卷或 qtree ，从而实现更严格的安全性。

- 将未知 UNIX 用户映射到默认 Windows 用户。

  这样可以确保所有用户都通过默认 Windows 用户获得对 NTFS 卷或 qtree 的最低访问级别，从而降低安全性，但更方便。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

如果要为未知 UNIX 用户使用默认 Windows 用户 …	输入命令 …
enabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
已禁用	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. 返回到管理权限级别：

```
set -privilege admin
```

使用非预留端口挂载 **NFS** 导出的客户端注意事项

。 `-mount-rootonly` 如果存储系统必须支持使用非保留端口挂载NFS导出的客户端、则即使用户以root身份登录、也必须在该存储系统上禁用此选项。此类客户端包括 Hummingbird 客户端和 Solaris NFS/IPv6 客户端。

如果 `-mount-rootonly` 选项处于启用状态时、ONTAP不允许使用非保留端口(即数量超过1、023的端口)的NFS客户端挂载NFS导出。

通过验证域对网络组执行更严格的访问检查

默认情况下， ONTAP 在评估网络组的客户端访问时会执行额外的验证。此附加检查可确保客户端的域与 Storage Virtual Machine （ SVM ）的域配置匹配。否则， ONTAP 将拒绝客户端访问。

关于此任务

当 ONTAP 评估客户端访问的导出策略规则且导出策略规则包含网络组时， ONTAP 必须确定客户端的 IP 地址是否属于该网络组。为此， ONTAP 会使用 DNS 将客户端的 IP 地址转换为主机名，并获取完全限定域名（ FQDN ）。

如果网络组文件仅列出主机的短名称，而主机的短名称存在于多个域中，则来自不同域的客户端可以在不进行此检查的情况下获得访问权限。

为了防止这种情况发生， ONTAP 会将从主机的 DNS 返回的域与为 SVM 配置的 DNS 域名列表进行比较。如果匹配，则允许访问。如果不匹配，则拒绝访问。

默认情况下，此验证处于启用状态。您可以通过修改对其进行管理 `-netgroup-dns-domain-search` 参数、可在高级权限级别下使用。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 执行所需的操作：

网络组的域验证条件	输入 ...
enabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
已禁用	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 将权限级别设置为 admin：

   ```
   set -privilege admin
   ```

修改用于 **NFSv3** 服务的端口

存储系统上的 NFS 服务器使用挂载守护进程和网络锁定管理器等服务通过特定的默认网络端口与 NFS 客户端进行通信。在大多数 NFS 环境中，默认端口可以正常工作且不需要修改，但如果要在 NFSv3 环境中使用不同的 NFS 网络端口，则可以这样做。

您需要的内容

更改存储系统上的 NFS 端口要求所有 NFS 客户端都重新连接到系统，因此您应在进行更改之前将此信息传达给用户。

关于此任务

您可以为每个 Storage Virtual Machine （ SVM ）设置 NFS 挂载守护进程，网络锁定管理器，网络状态监控器和 NFS 配额守护进程服务使用的端口。端口号更改会影响通过 TCP 和 UDP 访问数据的 NFS 客户端。

无法更改 NFSv4 和 NFSv4.1 的端口。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 禁用对 NFS 的访问：

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. 为特定 NFS 服务设置 NFS 端口：

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

NFS 端口参数	**Description**	默认端口
`-mountd-port`	NFS 挂载守护进程	635
`-nlm-port`	网络锁定管理器	4045

NFS 端口参数	Description	默认端口
`-nsm-port`	网络状态监控器	4046
`-rquotad-port`	NFS 配额守护进程	4049-51

除了默认端口之外，允许的端口号范围为 1024 到 65535 。每个 NFS 服务都必须使用唯一的端口。

4. 启用对 NFS 的访问：

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. 使用 `network connections listening show` 命令以验证端口号是否更改。
6. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

以下命令会将名为 vs1 的 SVM 上的 NFS 挂载守护进程端口设置为 1113：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- --------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

用于管理**NFS**服务器的命令

您可以使用特定的 ONTAP 命令来管理 NFS 服务器。

如果您要 …	使用此命令 …
创建 NFS 服务器	`vserver nfs create`
显示 NFS 服务器	`vserver nfs show`
修改 NFS 服务器	`vserver nfs modify`
删除 NFS 服务器	`vserver nfs delete`
隐藏 `.snapshot` 列出NFSv3挂载点下的目录 显式访问 `.snapshot` 即使启用了该选项、目录仍被允许。	`vserver nfs` 命令 `-v3-hide-snapshot` 选项已启用

有关详细信息，请参见每个命令的手册页。

对名称服务问题进行故障排除

当客户端因名称服务问题而遇到访问失败时、您可以使用 `vserver services name-service getxxbyyy` 命令系列、用于手动执行各种名称服务查找并检查查找的详细信息和结果、以帮助进行故障排除。

关于此任务

- 对于每个命令，您可以指定以下内容：
  - 要执行查找的节点或 Storage Virtual Machine （ SVM ）的名称。

    这样，您可以测试特定节点或 SVM 的名称服务查找，以缩小潜在名称服务配置问题描述的搜索范围。
  - 是否显示用于查找的源。

    这样，您可以检查是否使用了正确的源。
- ONTAP 会根据配置的名称服务切换顺序选择用于执行查找的服务。
- 这些命令可在高级权限级别下使用。

步骤

1. 执行以下操作之一：

检索…	使用命令 …

主机名的IP地址	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (仅限IPv4地址)
按组ID显示组成员	`vserver services name-service getxxbyyy getgrbygid`
按组名称显示组成员	`vserver services name-service getxxbyyy getgrbyname`
用户所属组的列表	`vserver services name-service getxxbyyy getgrlist`
IP地址的主机名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (仅限IPv4地址)
按用户名显示用户信息	`vserver services name-service getxxbyyy getpwbyname` 您可以通过指定来测试RBAC用户的名称解析 `-use-rbac` 参数为 `true`。
按用户ID显示用户信息	`vserver services name-service getxxbyyy getpwbyuid` 您可以通过指定来测试RBAC用户的名称解析 `-use-rbac` 参数为 `true`。
客户端的网络组成员资格	`vserver services name-service getxxbyyy netgrp`
使用netgroup-by-host搜索的客户端的网络组成员资格	`vserver services name-service getxxbyyy netgrpbyhost`

以下示例显示了通过尝试获取主机acast1.eng.example.com的IP地址来对SVM vs1执行的DNS查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

以下示例显示了通过尝试检索UID为501768的用户的用户信息来对SVM vs1执行的NIS查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

以下示例显示了通过尝试检索名为ldap1的用户的用户信息来对SVM vs1执行的LDAP查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

以下示例显示了SVM vs1的网络组查找测试、该测试尝试确定客户端dnshost0是否为网络组lnetgroup136的成员：

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 分析您执行的测试的结果并采取必要的措施。

如果 ...	检查
主机名或 IP 地址查找失败或生成的结果不正确	DNS配置
LOOKUP 查询的源不正确	名称服务开关配置

如果 ...	检查
用户或组查找失败或生成的结果不正确	• 名称服务开关配置 • 源配置(本地文件、NIS域、LDAP客户端) • 网络配置（例如 LIF 和路由）
主机名查找失败或超时，并且 DNS 服务器无法解析 DNS 短名称（例如 host1 ）	用于顶级域(TLD)查询的DNS配置。您可以使用禁用LD查询 `-is-tld-query-enabled false` 选项 `vserver services name-service dns modify` 命令：

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

验证名称服务连接

从 ONTAP 9.2 开始，您可以检查 DNS 和 LDAP 名称服务器以验证它们是否已连接到 ONTAP 。这些命令可在管理员权限级别使用。

关于此任务

您可以根据需要使用名称服务配置检查程序检查是否存在有效的 DNS 或 LDAP 名称服务配置。此验证检查可以在命令行或 System Manager 中启动。

对于 DNS 配置，所有服务器都经过测试，需要正常运行才能将此配置视为有效。对于 LDAP 配置，只要任何服务器已启动，此配置即有效。除非是、否则名称服务命令将应用配置检查程序 `skip-config-validation` 字段为true (默认值为false)。

步骤

1. 使用相应的命令检查名称服务配置。UI 将显示已配置服务器的状态。

要检查的内容	使用此命令 ...
DNS 配置状态	`vserver services name-service dns check`
LDAP配置状态	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

如果至少有一个已配置的服务器（名称服务器 /ldap-servers ）可访问并提供服务，则配置验证将成功。如果某些服务器无法访问，则会显示警告。

用于管理名称服务切换条目的命令

您可以通过创建，显示，修改和删除名称服务切换条目来管理这些条目。

如果您要 ...	使用此命令 ...
创建名称服务切换条目	`vserver services name-service ns-switch create`
显示名称服务切换条目	`vserver services name-service ns-switch show`
修改名称服务切换条目	`vserver services name-service ns-switch modify`
删除名称服务切换条目	`vserver services name-service ns-switch delete`

有关详细信息，请参见每个命令的手册页。

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

用于管理名称服务缓存的命令

您可以通过修改生存时间（ TTL ）值来管理名称服务缓存。TTL 值用于确定名称服务信息在缓存中的持久性。

要修改的 TTL 值	使用此命令 ...
UNIX 用户	`vserver services name-service cache unix-user settings`
UNIX 组	`vserver services name-service cache unix-group settings`
UNIX 网络组	`vserver services name-service cache netgroups settings`
主机	`vserver services name-service cache hosts settings`
组成员资格	`vserver services name-service cache group-membership settings`

相关信息

"ONTAP 9命令"

用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 ...	使用此命令 ...
创建名称映射	`vserver name-mapping create`
在特定位置插入名称映射	`vserver name-mapping insert`
显示名称映射	`vserver name-mapping show`
交换两个名称映射的位置 注意：如果为名称映射配置了IP限定符条目、则不允许进行交换。	`vserver name-mapping swap`
修改名称映射	`vserver name-mapping modify`
删除名称映射	`vserver name-mapping delete`
验证名称映射是否正确	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

有关详细信息，请参见每个命令的手册页。

用于管理本地 **UNIX** 用户的命令

您可以使用特定的 ONTAP 命令来管理本地 UNIX 用户。

如果您要 …	使用此命令 …
创建本地 UNIX 用户	`vserver services name-service unix-user create`
从 URI 加载本地 UNIX 用户	`vserver services name-service unix-user load-from-uri`
显示本地 UNIX 用户	`vserver services name-service unix-user show`
修改本地 UNIX 用户	`vserver services name-service unix-user modify`
删除本地 UNIX 用户	`vserver services name-service unix-user delete`

有关详细信息，请参见每个命令的手册页。

用于管理本地 **UNIX** 组的命令

您可以使用特定的 ONTAP 命令来管理本地 UNIX 组。

如果您要 …	使用此命令 …
创建本地 UNIX 组	`vserver services name-service unix-group create`
将用户添加到本地 UNIX 组	`vserver services name-service unix-group adduser`
从 URI 加载本地 UNIX 组	`vserver services name-service unix-group load-from-uri`
显示本地 UNIX 组	`vserver services name-service unix-group show`
修改本地 UNIX 组	`vserver services name-service unix-group modify`
从本地 UNIX 组中删除用户	`vserver services name-service unix-group deluser`
删除本地 UNIX 组	`vserver services name-service unix-group delete`

有关详细信息，请参见每个命令的手册页。

本地 **UNIX** 用户，组和组成员的限制

ONTAP 对集群中的最大 UNIX 用户和组数以及用于管理这些限制的命令进行了限制。这些

限制可以防止管理员在集群中创建过多的本地 UNIX 用户和组，从而有助于避免性能问题。

本地 UNIX 用户组和组成员的总数存在限制。本地 UNIX 用户有单独的限制。这些限制在集群范围内。每个新限制都设置为默认值，您可以修改该值，但最多不能修改为预先分配的硬限制。

数据库	默认限制	硬限制
本地 UNIX 用户	32、768	这是一项很好的
本地 UNIX 组和组成员	32、768	这是一项很好的

管理本地 **UNIX** 用户和组的限制

您可以使用特定的 ONTAP 命令来管理本地 UNIX 用户和组的限制。集群管理员可以使用这些命令对集群中被认为与本地 UNIX 用户和组数量过多相关的性能问题进行故障排除。

关于此任务

集群管理员可以在高级权限级别使用这些命令。

步骤

1. 执行以下操作之一：

如果您要 ...	使用命令 ...
显示有关本地 UNIX 用户限制的信息	`vserver services unix-user max-limit show`
显示有关本地 UNIX 组限制的信息	`vserver services unix-group max-limit show`
修改本地 UNIX 用户限制	`vserver services unix-user max-limit modify`
修改本地 UNIX 组限制	`vserver services unix-group max-limit modify`

有关详细信息，请参见每个命令的手册页。

用于管理本地网络组的命令

您可以通过以下方式管理本地网络组：从 URI 加载本地网络组，在节点间验证其状态，显示这些网络组并将其删除。

如果您要 …	使用命令 …

从 URI 加载网络组	`vserver services name-service netgroup load`
验证节点间网络组的状态	`vserver services name-service netgroup status` 可在高级权限级别及更高权限级别使用。
显示本地网络组	`vserver services name-service netgroup file show`
删除本地网络组	`vserver services name-service netgroup file delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **NIS** 域配置的命令

您可以使用特定的 ONTAP 命令来管理 NIS 域配置。

如果您要 …	使用此命令 …
创建 NIS 域配置	`vserver services name-service nis-domain create`
显示NIS域配置	`vserver services name-service nis-domain show`
显示 NIS 域配置的绑定状态	`vserver services name-service nis-domain show-bound`
显示NIS统计信息	`vserver services name-service nis-domain show-statistics` 可在高级权限级别及更高权限级别使用。
清除 NIS 统计信息	`vserver services name-service nis-domain clear-statistics` 可在高级权限级别及更高权限级别使用。
修改 NIS 域配置	`vserver services name-service nis-domain modify`
删除 NIS 域配置	`vserver services name-service nis-domain delete`
为按主机搜索网络组启用缓存	`vserver services name-service nis-domain netgroup-database config modify` 可在高级权限级别及更高权限级别使用。

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 客户端配置的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 客户端配置。

SVM 管理员不能修改或删除集群管理员创建的 LDAP 客户端配置。

如果您要 …	使用此命令 …
创建 LDAP 客户端配置	`vserver services name-service ldap client create`
显示 LDAP 客户端配置	`vserver services name-service ldap client show`
修改 LDAP 客户端配置	`vserver services name-service ldap client modify`
更改 LDAP 客户端绑定密码	`vserver services name-service ldap client modify-bind-password`
删除 LDAP 客户端配置	`vserver services name-service ldap client delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 配置的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 配置。

如果您要 …	使用此命令 …
创建 LDAP 配置	`vserver services name-service ldap create`
显示 LDAP 配置	`vserver services name-service ldap show`
修改 LDAP 配置	`vserver services name-service ldap modify`
删除 LDAP 配置	`vserver services name-service ldap delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 客户端模式模板的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 客户端模式模板。

SVM 管理员不能修改或删除集群管理员创建的 LDAP 客户端模式。

如果您要 …	使用此命令 …
复制现有 LDAP 模式模板	`vserver services name-service ldap client schema copy` 可在高级权限级别及更高权限级别使用。

显示 LDAP 模式模板	`vserver services name-service ldap client schema show`
修改 LDAP 模式模板	`vserver services name-service ldap client schema modify` 可在高级权限级别及更高权限级别使用。
删除 LDAP 模式模板	`vserver services name-service ldap client schema delete` 可在高级权限级别及更高权限级别使用。

有关详细信息，请参见每个命令的手册页。

用于管理 **NFS Kerberos** 接口配置的命令

您可以使用特定的 ONTAP 命令来管理 NFS Kerberos 接口配置。

如果您要 …	使用此命令 …
在 LIF 上启用 NFS Kerberos	`vserver nfs kerberos interface enable`
显示 NFS Kerberos 接口配置	`vserver nfs kerberos interface show`
修改 NFS Kerberos 接口配置	`vserver nfs kerberos interface modify`
在 LIF 上禁用 NFS Kerberos	`vserver nfs kerberos interface disable`

有关详细信息，请参见每个命令的手册页。

用于管理 **NFS Kerberos** 域配置的命令

您可以使用特定的 ONTAP 命令来管理 NFS Kerberos 域配置。

如果您要 …	使用此命令 …
创建 NFS Kerberos 域配置	`vserver nfs kerberos realm create`
显示 NFS Kerberos 域配置	`vserver nfs kerberos realm show`
修改 NFS Kerberos 域配置	`vserver nfs kerberos realm modify`
删除 NFS Kerberos 域配置	`vserver nfs kerberos realm delete`

有关详细信息，请参见每个命令的手册页。

用于管理导出策略的命令

您可以使用特定的 ONTAP 命令来管理导出策略。

如果您要 …	使用此命令 …
显示有关导出策略的信息	`vserver export-policy show`
重命名导出策略	`vserver export-policy rename`
复制导出策略	`vserver export-policy copy`
删除导出策略	`vserver export-policy delete`

有关详细信息，请参见每个命令的手册页。

用于管理导出规则的命令

您可以使用特定的 ONTAP 命令来管理导出规则。

如果您要 …	使用此命令 …
创建导出规则	`vserver export-policy rule create`
显示有关导出规则的信息	`vserver export-policy rule show`
修改导出规则	`vserver export-policy rule modify`
删除导出规则	`vserver export-policy rule delete`

> 如果您配置了多个与不同客户端匹配的相同导出规则，请确保在管理导出规则时保持同步。

有关详细信息，请参见每个命令的手册页。

配置 **NFS** 凭据缓存

修改 **NFS** 凭据缓存生存时间的原因

ONTAP 使用凭据缓存存储 NFS 导出访问的用户身份验证所需的信息，以加快访问速度并提高性能。您可以配置凭据缓存中存储信息的时间长度，以便根据您的环境对其进行自定义。

修改 NFS 凭据缓存生存时间（TTL）时，有多种情况可帮助解决问题。您应了解这些情形的含义以及进行这些修改的后果。

reasons

在以下情况下，请考虑更改默认 TTL：

问题描述	补救措施
由于来自 ONTAP 的请求负载较高，您环境中的名称服务器的性能正在下降。	增加缓存的肯定和否定凭据的 TTL ，以减少从 ONTAP 到名称服务器的请求数。
名称服务器管理员进行了更改，以允许访问先前被拒绝的 NFS 用户。	减少缓存的否定凭据的 TTL ，以减少 NFS 用户等待 ONTAP 从外部名称服务器请求新凭据以获得访问权限所需的时间。
名称服务器管理员进行了更改，以拒绝先前允许的 NFS 用户访问。	减少缓存肯定凭据的 TTL ，以缩短 ONTAP 从外部名称服务器请求新凭据的时间，从而使 NFS 用户现在被拒绝访问。

后果

您可以分别修改缓存肯定和否定凭据的时间长度。但是，您应该了解这种做法的优缺点。

如果您 ...	优势是 ...	缺点是 ...
增加肯定凭据缓存时间	ONTAP 向名称服务器发送凭据请求的频率较低，从而减少了名称服务器上的负载。	拒绝访问以前允许访问但不再允许访问的 NFS 用户需要更长时间。
减少肯定凭据缓存时间	拒绝访问先前允许访问但不再允许访问的 NFS 用户所需的时间更短。	ONTAP 会更频繁地向名称服务器发送凭据请求，从而增加名称服务器的负载。
增加否定凭据缓存时间	ONTAP 向名称服务器发送凭据请求的频率较低，从而减少了名称服务器上的负载。	向以前不允许访问但现在允许访问的 NFS 用户授予访问权限需要更长时间。
减少否定凭据缓存时间	为以前不允许访问但现在允许访问的 NFS 用户授予访问权限所需的时间更短。	ONTAP 会更频繁地向名称服务器发送凭据请求，从而增加名称服务器的负载。

为缓存的 **NFS** 用户凭据配置生存时间

您可以通过修改 Storage Virtual Machine （ SVM ）的 NFS 服务器来配置 ONTAP 在其内部缓存中存储 NFS 用户凭据的时间长度（生存时间或 TTL ）。这样，您就可以缓解与名称服务器上的高负载或影响 NFS 用户访问的凭据更改相关的某些问题。

关于此任务

这些参数可在高级权限级别使用。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

要修改缓存的 TTL 的项	使用命令 …
肯定凭据	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTL 以毫秒为单位。从ONTAP 9.10.1及更高版本开始、默认值为1小时(3、600、000毫秒)。 在ONTAP 9.9.1及更早版本中、默认值为24小时(86、400、000毫秒)。 此值的允许范围为 1 分钟（ 60000 毫秒）到 7 天（ 604 ， 800 ， 000 毫秒）。
否定凭据	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL 以毫秒为单位。默认值为 2 小时（ 7 ， 200 ， 000 毫秒）。此值的允许范围为 1 分钟（ 60000 毫秒）到 7 天（ 604 ， 800 ， 000 毫秒）。

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

管理导出策略缓存

刷新导出策略缓存

ONTAP 使用多个导出策略缓存来存储与导出策略相关的信息，以加快访问速度。手动转储导出策略缓存 (`vserver export-policy cache flush`)删除可能过时的信息并强制ONTAP从相应的外部资源检索当前信息。这有助于解决与客户端访问 NFS 导出相关的各种问题。

关于此任务

由于以下原因，导出策略缓存信息可能已过时：

- 最近对导出策略规则进行的更改
- 最近对名称服务器中的主机名记录进行的更改
- 最近对名称服务器中的网络组条目进行的更改
- 从阻止网络组完全加载的网络中断中恢复

步骤

1. 如果未启用名称服务缓存，请在高级权限模式下执行以下操作之一：

要刷新的内容	输入命令 ...
所有导出策略缓存（ showmount 除外）	`vserver export-policy cache flush -vserver vserver_name`
导出策略规则访问缓存	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以包括可选 `-node` 参数以指定要转储访问缓存的节点。
主机名缓存	`vserver export-policy cache flush -vserver vserver_name -cache host`
网络组缓存	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` 处理网络组需要大量资源。只有在尝试解析因网络组陈旧而导致的客户端访问问题描述时，才应刷新网络组缓存。
showmount 缓存	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. 如果启用了名称服务缓存，请执行以下操作之一：

要刷新的内容	输入命令 ...
导出策略规则访问缓存	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以包括可选 `-node` 参数以指定要转储访问缓存的节点。
主机名缓存	`vserver services name-service cache hosts forward-lookup delete-all`
网络组缓存	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` 处理网络组需要大量资源。只有在尝试解析因网络组陈旧而导致的客户端访问问题描述时，才应刷新网络组缓存。
showmount 缓存	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

显示导出策略网络组队列和缓存

ONTAP 在导入和解析网络组时使用网络组队列，并使用网络组缓存存储生成的信息。在对

导出策略网络组相关问题进行故障排除时、您可以使用 `vserver export-policy netgroup queue show` 和 `vserver export-policy netgroup cache show` 用于显示网络组队列状态和网络组缓存内容的命令。

步骤

1. 执行以下操作之一：

要显示导出策略网络组 …	输入命令 …
队列	`vserver export-policy netgroup queue show`
缓存	`vserver export-policy netgroup cache show -vserver vserver_name`

有关详细信息，请参见每个命令的手册页。

检查客户端 IP 地址是否为网络组的成员

在对与网络组相关的NFS客户端访问问题进行故障排除时、您可以使用 `vserver export-policy netgroup check-membership` 命令、以帮助确定客户端IP是否为某个网络组的成员。

关于此任务

通过检查网络组成员资格，您可以确定 ONTAP 是否意识到客户端是或不是网络组的成员。此外，您还可以通过它来了解刷新网络组信息时 ONTAP 网络组缓存是否处于瞬时状态。此信息有助于您了解客户端为何可能会被意外授予或拒绝访问。

步骤

1. 检查客户端IP地址的网络组成员资格： `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   此命令可返回以下结果：

   - 客户端是网络组的成员。

     这已通过反向查找扫描或按主机搜索网络组来确认。

   - 客户端是网络组的成员。

     已在 ONTAP 网络组缓存中找到此文件。

   - 客户端不是网络组的成员。
   - 由于 ONTAP 当前正在刷新网络组缓存，因此无法确定客户端的成员资格。

     除非这样做，否则不能明确排除成员资格。使用 `vserver export-policy netgroup queue show` 命令以监控网络组的加载、并在完成后重试检查。

示例

以下示例检查 IP 地址为 172.17.16.72 的客户端是否为 SVM vs1 上的网络组 mercury 的成员：

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

优化访问缓存性能

您可以配置多个参数来优化访问缓存，并在性能与存储在访问缓存中的信息的最新程度之间找到适当的平衡。

关于此任务

配置访问缓存刷新周期时，请记住以下几点：

- 值越高意味着条目在访问缓存中的保留时间越长。

  其优势在于性能更好，因为 ONTAP 在刷新访问缓存条目上花费的资源更少。缺点是，如果导出策略规则发生更改，而访问缓存条目因此变得陈旧，则更新这些条目需要的时间会较长。因此，应获取访问权限的客户端可能会被拒绝，而应被拒绝的客户端可能会获得访问权限。

- 值越低意味着 ONTAP 更新访问缓存条目的频率越高。

  其优势在于，条目更新，客户端更有可能被正确授予或拒绝访问。缺点是性能下降，因为 ONTAP 会花费更多资源来刷新访问缓存条目。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

要修改的内容	输入 ...
肯定条目的刷新期限	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
否定条目的刷新期限	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
旧条目的超时期限	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 验证新参数设置：

```
vserver export-policy access-cache config show-all-vservers
```

4. 返回到管理权限级别：

```
set -privilege admin
```

管理文件锁定

关于协议之间的文件锁定

文件锁定是客户端应用程序用来防止用户访问先前由另一用户打开的文件的方法。ONTAP 锁定文件的方式取决于客户端的协议。

如果客户端是 NFS 客户端，则建议锁定；如果客户端是 SMB 客户端，则必须锁定。

由于 NFS 和 SMB 文件锁定之间的差异， NFS 客户端可能无法访问先前由 SMB 应用程序打开的文件。

当 NFS 客户端尝试访问 SMB 应用程序锁定的文件时，会发生以下情况：

- 在混合卷或NTFS卷中、文件操作(如) `rm`， `rmdir`，和 `mv` 是否可以对NFS应用程序执行发生原因以使其失败。
- SMB 拒绝读取和拒绝写入打开模式分别拒绝 NFS 读取和写入操作。
- 如果文件的写入范围使用独占 SMB 字节锁锁定，则 NFS 写入操作将失败。

在 UNIX 安全模式卷中， NFS 取消链接和重命名操作会忽略 SMB 锁定状态并允许访问文件。UNIX 安全模式卷上的所有其他 NFS 操作均遵循 SMB 锁定状态。

ONTAP 如何处理只读位

只读位会逐个文件进行设置，以反映文件是可写（已禁用）还是只读（已启用）。

使用 Windows 的 SMB 客户端可以设置每个文件的只读位。NFS 客户端不会设置每个文件只读位，因为 NFS 客户端不会执行任何使用每个文件只读位的协议操作。

当使用 Windows 的 SMB 客户端创建文件时， ONTAP 可以在该文件上设置只读位。在 NFS 客户端和 SMB 客户端之间共享文件时， ONTAP 还可以设置只读位。NFS 客户端和 SMB 客户端使用某些软件时，需要启用只读位。

要使 ONTAP 对 NFS 客户端和 SMB 客户端之间共享的文件保持适当的读写权限，它会根据以下规则处理只读位：

- NFS 会将启用了只读位的任何文件视为未启用写入权限位。
- 如果 NFS 客户端禁用了所有写入权限位，并且先前至少启用了其中一个位，则 ONTAP 会为该文件启用只读位。
- 如果 NFS 客户端启用任何写入权限位，则 ONTAP 会禁用该文件的只读位。
- 如果启用了文件的只读位，而 NFS 客户端尝试发现文件的权限，则不会将文件的权限位发送到 NFS 客户端；而 ONTAP 是将权限位发送到 NFS 客户端，并屏蔽写入权限位。
- 如果启用了文件的只读位，而 SMB 客户端禁用了只读位，则 ONTAP 将为此文件启用所有者的写入权限位。

- 启用了只读位的文件只能由 root 用户写入。

> 对文件权限的更改会立即在 SMB 客户端上生效，但如果 NFS 客户端启用属性缓存，则可能不会立即在 NFS 客户端上生效。

在处理共享路径组件上的锁定时， **ONTAP** 与 **Windows** 有何不同

与 Windows 不同， ONTAP 不会在打开文件时锁定打开文件的路径的每个组件。此行为也会影响 SMB 共享路径。

由于 ONTAP 不会锁定路径的每个组件，因此可以重命名打开的文件或共享上方的路径组件，这可能会导致某些应用程序出现发生原因问题，也可能发生原因会使 SMB 配置中的共享路径无效。这可能发生原因会使此共享无法访问。

为了避免重命名路径组件导致的问题、您可以应用Windows访问控制列表(ACL)安全设置、以防止用户或应用程序重命名关键目录。

了解更多信息 "如何防止在客户端访问目录时重命名这些目录"。

显示有关锁定的信息

您可以显示有关当前文件锁定的信息，包括锁定的锁定类型以及锁定状态，字节范围锁定，共享锁定模式，委派锁定和机会锁定的详细信息，以及锁定是使用持久句柄还是持久句柄打开的。

关于此任务

对于通过 NFSv4 或 NFSv4.1 建立的锁定，无法显示客户端 IP 地址。

默认情况下，命令会显示有关所有锁定的信息。您可以使用命令参数显示有关特定 Storage Virtual Machine （ SVM ）锁定的信息，或者按其他条件筛选命令的输出。

。 `vserver locks show` 命令可显示有关四种类型的锁定的信息：

- 字节范围锁定，仅锁定文件的一部分。
- 共享锁定，用于锁定打开的文件。
- 机会锁，用于控制 SMB 上的客户端缓存。
- 委派，用于通过 NFSv4.x 控制客户端缓存

通过指定可选参数，您可以确定有关每个锁定类型的重要信息。有关详细信息，请参见命令的手册页。

步骤

1. 使用显示有关锁定的信息 `vserver locks show` 命令：

示例

以下示例显示了路径为的文件上的NFSv4锁定的摘要信息 `/vol1/file1`。共享锁定访问模式为 write-deny_none ，而锁定是通过写入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

以下示例显示路径为的文件上SMB锁定的详细操作锁定和共享锁定信息 `/data2/data2_2/intro.pptx`。对于 IP 地址为 10.3.1.3 的客户端，共享锁定访问模式为 write-deny_none 的文件会授予持久句柄。租用机会锁会授予批量机会锁级别：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
```

```
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
    Node Holding Lock State: node3
                 Lock State: granted
   Bytelock Starting Offset: -
     Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
    Shared Lock Access Mode: -
        Shared Lock is Soft: -
            Delegation Type: -
             Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

正在中断锁定

当文件锁定阻止客户端访问文件时，您可以显示有关当前持有的锁定的信息，然后中断特定锁定。可能需要中断锁定的情形示例包括调试应用程序。

关于此任务

。 `vserver locks break` 命令只能在高级权限级别及更高权限级别下使用。命令的手册页包含详细信息。

步骤

1. 要查找解除锁定所需的信息、请使用 `vserver locks show` 命令：

   命令的手册页包含详细信息。

2. 将权限级别设置为高级：

   `set -privilege advanced`

3. 执行以下操作之一：

如果要通过指定 … 来中断锁定	输入命令 …

SVM 名称，卷名称， LIF 名称和文件路径	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
锁定 ID	`vserver locks break -lockid UUID`

4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

FPolicy 首次读取和首次写入筛选器如何与 **NFS** 配合使用

如果使用将读 / 写操作作为受监控事件的外部 FPolicy 服务器启用了 FPolicy ，则 NFS 客户端在读取 / 写入请求的高流量期间会遇到较长的响应时间。对于 NFS 客户端，在 FPolicy 中使用首次读取和首次写入筛选器可减少 FPolicy 通知的数量并提高性能。

在 NFS 中，客户端通过提取文件句柄对文件执行 I/O 。此句柄可能在服务器和客户端重新启动后仍然有效。因此，客户端可以在不重新检索句柄的情况下缓存句柄并在其上发送请求。在常规会话中，会向文件服务器发送大量读 / 写请求。如果为所有这些请求生成通知，可能会导致以下问题：

- 由于额外的通知处理和较长的响应时间，负载会增加。
- 向 FPolicy 服务器发送大量通知，即使该服务器不受所有通知的影响。

从客户端收到特定文件的第一个读 / 写请求后，将创建一个缓存条目，并增加读 / 写计数。此请求将标记为首次读取 / 写入操作，并生成 FPolicy 事件。在为 NFS 客户端规划和创建 FPolicy 筛选器之前，您应了解 FPolicy 筛选器工作原理的基础知识。

- 首次读取：筛选客户端读取请求以进行首次读取。

  如果对NFS事件使用此筛选器、则会显示 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 设置用于确定要处理FPolicy的首次读取请求。

- 首次写入：筛选客户端写入请求以进行首次写入。

  如果对NFS事件使用此筛选器、则会显示 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 设置用于确定要处理FPolicy的首次写入请求。

NFS 服务器数据库中添加了以下选项。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

修改 NFSv4.1 服务器实施 ID

NFSv4.1 协议包含一个服务器实施 ID ，用于记录服务器域，名称和日期。您可以修改服务器实施 ID 的默认值。更改默认值可能会很有用，例如，在收集使用情况统计信息或对互操作性问题进行故障排除时。有关详细信息，请参见 RFC 5661 。

关于此任务

这三个选项的默认值如下：

选项	选项名称	默认值
NFSv4.1 实施 ID 域	`-v4.1-implementation-domain`	NetApp.com
NFSv4.1 实施 ID 名称	`-v4.1-implementation-name`	集群版本名称
NFSv4.1 实施 ID 日期	`-v4.1-implementation-date`	集群版本日期

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

要修改 **NFSv4.1** 实施 **ID** 的项	输入命令 **...**
domain	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

管理 NFSv4 ACL

启用 NFSv4 ACL 的优势

启用 NFSv4 ACL 具有许多优势。

启用 NFSv4 ACL 的优势包括：

- 更精细地控制用户对文件和目录的访问
- 提高 NFS 安全性
- 改进了与 CIFS 的互操作性
- 取消了每个用户 16 个组的 NFS 限制

NFSv4 ACL 的工作原理

使用 NFSv4 ACL 的客户端可以对系统上的文件和目录设置和查看 ACL 。在具有 ACL 的目录中创建新文件或子目录时，新文件或子目录会继承 ACL 中已标记有相应继承标志的所有 ACL 条目（ACE）。

在根据 NFSv4 请求创建文件或目录时，生成的文件或目录上的 ACL 取决于文件创建请求是包含 ACL 还是仅包含标准 UNIX 文件访问权限，以及父目录是否具有 ACL：

- 如果请求包含 ACL ，则会使用该 ACL 。
- 如果此请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL ，则只要父目录的 ACL 中的 ACE 已使用适当的继承标志进行标记，新文件或目录就会继承这些 ACE 。

> 即使如此、也会继承父ACL `-v4.0-acl` 设置为 `off`。

- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL ，则会使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录具有不可继承的 ACL ，则只会使用模式位创建新对象。

> 如果 `-chown-mode` 参数已设置为 `restricted` 中的命令 `vserver nfs` 或 `vserver export-policy rule` 系列、文件所有权只能由超级用户更改、即使使用NFSv4 ACL设置的磁盘权限允许非root用户更改文件所有权也是如此。有关详细信息，请参见相关手册页。

启用或禁用修改 NFSv4 ACL

当ONTAP接收到 `chmod` 命令时、默认情况下、系统会保留并修改ACL、以反映模式位更改。您可以禁用 `-v4-acl-preserve` 参数以更改要丢弃ACL时的行为。

关于此任务

使用统一安全模式时，此参数还指定客户端为文件或目录发送 chmod ， chgroup 或 chown 命令时是保留还是删除 NTFS 文件权限。

此参数的默认值为 enabled 。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

如果您要 …	输入以下命令 …
启用保留和修改现有 NFSv4 ACL （默认）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
更改模式位时禁用保留并丢弃 NFSv4 ACL	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. 返回到管理权限级别：

```
set -privilege admin
```

ONTAP 如何使用 NFSv4 ACL 来确定是否可以删除文件

为了确定是否可以删除某个文件， ONTAP 将结合使用该文件的删除位和所在目录的 delete_child 位。有关详细信息，请参见 NFS 4.1 RFC 5661 。

启用或禁用 NFSv4 ACL

要启用或禁用NFSv4 ACL、您可以修改 `-v4.0-acl` 和 `-v4.1-acl` 选项默认情况下，这些选项处于禁用状态。

关于此任务

。 `-v4.0-acl` 或 `-v4.1-acl` 选项用于控制NFSv4 ACL的设置和查看、而不用于控制在访问检查中强制实施这些ACL。

步骤

1. 执行以下操作之一：

如果您要 …	那么 …
启用 NFSv4.0 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
禁用 NFSv4.0 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
启用NFSv4.1 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

禁用NFSv4.1 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

修改 NFSv4 ACL 的最大 ACE 限制

您可以通过修改参数来修改每个NFSv4 ACL允许的最大ACL数 `-v4-acl-max-aces`。默认情况下，每个 ACL 的限制设置为 400 个 ACE 。增加此限制有助于确保使用包含 400 个以上 ACE 的 ACL 将数据成功迁移到运行 ONTAP 的存储系统。

关于此任务

增加此限制可能会影响使用 NFSv4 ACL 访问文件的客户端的性能。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 修改 NFSv4 ACL 的最大 ACE 限制：

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   的有效范围

   `max_ace_limit` 为 `192` to `1024`.

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

管理 NFSv4 文件委派

启用或禁用 NFSv4 读取文件委派

要启用或禁用NFSv4读取文件委派、您可以修改 `-v4.0-read-delegation`或 选项通过启用读取文件委派，您可以消除与打开和关闭文件相关的大量消息开销。

关于此任务

默认情况下，读取文件委派处于禁用状态。

启用读取文件委派的缺点是，服务器及其客户端必须在服务器重新启动，客户端重新启动或发生网络分区后恢复委派。

步骤

1. 执行以下操作之一：

如果您要 …	那么 …
启用 NFSv4 读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
启用NFSv4.1读取文件委派	输入以下命令： + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
禁用 NFSv4 读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
禁用NFSv4.1读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

结果

文件委派选项一经更改即会生效。无需重新启动或重新启动 NFS 。

启用或禁用 **NFSv4** 写入文件委派

要启用或禁用写入文件委派、您可以修改 `-v4.0-write-delegation`或 选项通过启用写入文件委派，除了打开和关闭文件之外，您还可以消除与文件和记录锁定相关的大量消息开销。

关于此任务

默认情况下，写入文件委派处于禁用状态。

启用写入文件委派的缺点是，在服务器重新启动，客户端重新启动或发生网络分区后，服务器及其客户端必须执行其他任务来恢复委派。

步骤

1. 执行以下操作之一：

如果您要 ...	那么 ...
启用 NFSv4 写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-write -delegation enabled`

如果您要 ...	那么 ...
启用NFSv4.1写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-write -delegation enabled`
禁用 NFSv4 写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-write -delegation disabled`
禁用NFSv4.1写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-write -delegation disabled`

结果

文件委派选项一经更改即会生效。无需重新启动或重新启动 NFS 。

配置 **NFSv4** 文件和记录锁定

关于 **NFSv4** 文件和记录锁定

对于 NFSv4 客户端， ONTAP 支持 NFSv4 文件锁定机制，以便在基于租赁的模式下保持所有文件锁定的状态。

"NetApp 技术报告 3580 ：《 NFSv4 增强功能和最佳实践指南： Data ONTAP 实施》"

指定 **NFSv4** 锁定租赁期限

要指定NFSv4锁定租赁期限(即ONTAP不可撤销地向客户端授予锁定的时间段)、您可以修改 `-v4-lease-seconds` 选项较短的租赁期可加快服务器恢复速度，而较长的租赁期则有利于处理大量客户端的服务器。

关于此任务

默认情况下、此选项设置为 `30`。此选项的最小值为 `10`。此选项的最大值是锁定宽限期、您可以使用设置此宽限期 `locking.lease_seconds` 选项

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 输入以下命令：

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

指定 **NFSv4** 锁定宽限期

要指定NFSv4锁定宽限期(即、客户端在服务器恢复期间尝试从ONTAP回收其锁定状态的时间段)、您可以修改 `-v4-grace-seconds` 选项

关于此任务

默认情况下、此选项设置为 `45`。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 输入以下命令：

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

NFSv4 转介的工作原理

启用 NFSv4 转介时， ONTAP 会为 NFSv4 客户端提供 "`SVM 内` " 转介。SVM 内转介是指收到 NFSv4 请求的集群节点将 NFSv4 客户端转介到 Storage Virtual Machine （ SVM ）上的另一个逻辑接口（ LIF ）。

从那时起， NFSv4 客户端应访问在目标 LIF 上收到转介的路径。如果原始集群节点确定 SVM 中存在驻留在数据卷所在集群节点上的 LIF ，则会提供此类转介，从而使客户端能够更快地访问数据并避免额外的集群通信。

启用或禁用 **NFSv4** 转介

您可以通过启用选项在Storage Virtual Machine (SVM)上启用NFSv4转介 `-v4-fsid-change` 和 `-v4.0-referrals`或。启用 NFSv4 转介可以加快支持此功能的 NFSv4 客户端的数据访问速度。

您需要的内容

如果要启用 NFS 转介，必须先禁用并行 NFS 。您不能同时启用这两者。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

如果您要 …	输入命令 …

启用 NFSv4 转介	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
禁用 NFSv4 转介	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
启用NFSv4.1转介	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
禁用NFSv4.1转介	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

显示**NFS**统计信息

您可以显示存储系统上 Storage Virtual Machine （ SVM ）的 NFS 统计信息，以监控性能并诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的NFS对象。

   ```
   statistics catalog object show -object nfs*
   ```

2. 使用 `statistics start` 和可选 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

示例：监控**NFSv3**性能

以下示例显示了 NFSv3 协议的性能数据。

以下命令将开始收集新样本的数据：

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示成功的读取和写入请求数与读取和写入请求总数：

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                             Value
    --------------------------- ---------------------------
    read_success                                        40042
    read_total                                          40042
    write_success                                     1492052
    write_total                                       1492052
```

相关信息

"性能监控设置"

显示**DNS**统计信息

您可以显示存储系统上Storage Virtual Machine (SVM)的DNS统计信息、以监控性能和诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的DNS对象。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

监控**DNS**统计信息

以下示例显示了 DNS 查询的性能数据。以下命令将开始收集新样本的数据：

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示发送的 DNS 查询数与接收，失败或超时的 DNS 查询数：

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示特定服务器上的 DNS 查询收到特定错误的次数：

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

相关信息

"性能监控设置"

显示**NIS**统计信息

您可以显示存储系统上Storage Virtual Machine (SVM)的NIS统计信息、以监控性能和诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的NIS对象。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

监控 **NIS** 统计信息

以下示例显示了 NIS 查询的性能数据。以下命令将开始收集新样本的数据：

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示发送的 NIS 查询数与接收，失败或超时的 NIS 查询数：

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示在特定服务器上收到 NIS 查询特定错误的次数：

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                        YP_NOTFOUND
    server_ip_address                                 10.227.13.221
3 entries were displayed.
```

相关信息

"性能监控设置"

支持基于 **NFS** 的 **VMware vStorage**

ONTAP 支持 NFS 环境中的某些 VMware vStorage APIs for Array Integration （VAAI）功能。

支持的功能

支持以下功能：

- 副本卸载

  使 ESXi 主机可以直接在源数据存储位置和目标数据存储位置之间复制虚拟机或虚拟机磁盘（VMDK），而无需主机参与。这样可以节省 ESXi 主机的 CPU 周期和网络带宽。如果源卷为稀疏卷，则副本卸载可保留空间效率。

- 空间预留

  通过为 VMDK 文件预留空间来保证其存储空间。

限制

基于 NFS 的 VMware vStorage 具有以下限制：

- 在以下情况下，副本卸载操作可能会失败：

- 在源卷或目标卷上运行 wafliron 时，因为它会暂时使卷脱机
- 移动源卷或目标卷时
- 移动源或目标 LIF 时
- 执行接管或交还操作时
- 执行切换或切回操作时

- 在以下情况下，由于文件句柄格式不同，服务器端复制可能会失败：

  您尝试将当前或先前已导出 qtree 的 SVM 中的数据复制到从未导出 qtree 的 SVM 。要解决此限制，您可以在目标 SVM 上至少导出一个 qtree 。

相关信息

"Data ONTAP 支持哪些 VAAI 卸载操作？"

启用或禁用基于 **NFS** 的 **VMware vStorage**

您可以使用在Storage Virtual Machine (SVM)上启用或禁用对基于NFS的VMware vStorage的支持 `vserver nfs modify` 命令：

关于此任务

默认情况下，不支持基于 NFS 的 VMware vStorage 。

步骤

1. 显示 SVM 的当前 vStorage 支持状态：

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用 VMware vStorage 支持	`vserver nfs modify -vserver vserver_name -vstorage enabled`
禁用 VMware vStorage 支持	`vserver nfs modify -vserver vserver_name -vstorage disabled`

完成后

您必须先安装适用于 VMware VAAI 的 NFS 插件，然后才能使用此功能。有关详细信息，请参见 *Installing the NetApp NFS Plug-in for VMware VAAI* 。

相关信息

"NetApp 文档：适用于 VMware VAAI 的 NetApp NFS 插件"

启用或禁用 **rquota** 支持

ONTAP 支持远程配额协议版本 1 （ rquota v1 ）。使用 rquota 协议， NFS 客户端可以从远程计算机为用户获取配额信息。您可以使用在Storage Virtual Machine (SVM)上启用r配额 `vserver nfs modify` 命令：

关于此任务

默认情况下， rquota 处于禁用状态。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
为 SVM 启用 rquota 支持	`vserver nfs modify -vserver vserver_name -rquota enable`
禁用 SVM 的 rquota 支持	`vserver nfs modify -vserver vserver_name -rquota disable`

有关配额的详细信息，请参见 "逻辑存储管理"。

通过修改 **TCP** 传输大小来提高 **NFSv3** 和 **NFSv4** 的性能

您可以通过修改 TCP 最大传输大小来提高通过高延迟网络连接到存储系统的 NFSv3 和 NFSv4 客户端的性能。

当客户端通过广域网 （ WAN ） 或城域网 （ man ） 等高延迟网络访问存储系统时，如果延迟超过 10 毫秒，则可以通过修改 TCP 最大传输大小来提高连接性能。在低延迟网络（例如局域网 （ LAN ））中访问存储系统的客户端，对这些参数的修改几乎没有好处。如果吞吐量提高不会超过延迟影响，则不应使用这些参数。

要确定您的存储环境是否会因修改这些参数而受益，您应首先对性能较差的 NFS 客户端进行全面的性能评估。查看此低性能是否是由于往返延迟过长以及客户端上的请求较小所致。在这种情况下，客户端和服务器无法充分利用可用带宽，因为它们会花费大部分工作周期来等待通过连接传输的小请求和响应。

通过增加 NFSv3 和 NFSv4 请求大小，客户端和服务器可以更有效地使用可用带宽，以便在每个单元时间移动更多数据，从而提高连接的整体效率。

请注意，存储系统和客户端之间的配置可能会有所不同。存储系统和客户端支持传输操作的最大大小为 1 MB 。但是，如果将存储系统配置为支持 1 MB 最大传输大小，但客户端仅支持 64 KB ，则挂载传输大小将限制为 64 KB 或更少。

在修改这些参数之前，您必须了解，在组装和传输大型响应所需的时间段内，它会导致存储系统占用更多内存。存储系统的高延迟连接越多，额外的内存消耗就越多。具有高内存容量的存储系统可能不会受到此更改的影响。内存容量较低的存储系统的性能可能会明显下降。

要成功使用这些参数，需要能够从集群的多个节点检索数据。集群网络固有的延迟可能会增加响应的整体延迟。使用这些参数时，整体延迟往往会增加。因此，延迟敏感型工作负载可能会产生负面影响。

修改 **NFSv3** 和 **NFSv4 TCP** 最大传输大小

您可以修改 `-tcp-max-xfer-size` 可选择为使用NFSv3和NFSv4.x协议的所有TCP连接配置最大传输大小。

关于此任务

您可以分别为每个 Storage Virtual Machine （ SVM ）修改这些选项。

从ONTAP 9开始、 `v3-tcp-max-read-size` 和 `v3-tcp-max-write-size` 选项已过时。您必须使用 `-tcp-max-xfer-size` 选项。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

如果您要 ...	输入命令 ...
修改 NFSv3 或 NFSv4 TCP 最大传输大小	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

选项	范围	**Default**
`-tcp-max-xfer-size`	8192 到 1048576 字节	6556字节

> 输入的最大传输大小必须是 4 KB （ 4096 字节）的倍数。未正确对齐的请求会对性能产生负面影响。

3. 使用 `vserver nfs show -fields tcp-max-xfer-size` 命令以验证所做的更改。
4. 如果任何客户端使用静态挂载，请卸载并重新挂载，以使新参数大小生效。

示例

以下命令会将名为 vs1 的 SVM 上的 NFSv3 和 NFSv4.x TCP 最大传输大小设置为 1048576 字节：

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

配置 **NFS** 用户允许的组 **ID** 数量

默认情况下，在使用 Kerberos （ RPCSEC_GSS ）身份验证处理 NFS 用户凭据时，ONTAP 最多支持 32 个组 ID 。使用 AUTH_SYS 身份验证时，默认的最大组 ID 数为 16 ，如 RFC 5531 中所定义。如果用户所属的组超过默认组数，则可以将最大值增加到 1 ，024 。

关于此任务

如果用户凭据中的组 ID 超过默认数量，则其余组 ID 将被截断，并且用户在尝试从存储系统访问文件时可能会收到错误。您应将每个 SVM 的最大组数设置为表示环境中最大组数的数字。

下表显示了的两个参数 `vserver nfs modify` 用于确定三个示例配置中组ID最大数量的命令：

Parameters	设置	生成的组 ID 限制

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	这些是默认设置。
		RPCSEC_GSS： 32
		
		AUTH_SYS： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS：256
		
		AUTH_SYS： 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS：512
		
		auth_SYS：512

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

如果要设置允许的最大辅助组数 …	输入命令 …
仅适用于 RPCSEC_GSS ，并保持 AUTH_SYS 设置为默认值 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
适用于 RPCSEC_GSS 和 AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. 验证 `-extended-groups-limit` 值并验证AUTH _SYS是否正在使用扩展组： `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`

4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

以下示例将为 AUTH_SYS 身份验证启用扩展组，并将 AUTH_SYS 和 RPCSEC_GSS 身份验证的最大扩展组数设置为 512 。这些更改仅适用于访问名为 vs1 的 SVM 的客户端：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

控制 **root** 用户对 **NTFS** 安全模式数据的访问

您可以将 ONTAP 配置为允许 NFS 客户端访问 NTFS 安全模式数据，并允许 NTFS 客户端访问 NFS 安全模式数据。在 NFS 数据存储上使用 NTFS 安全模式时，您必须确定如何处理 root 用户的访问并相应地配置 Storage Virtual Machine （ SVM ）。

关于此任务

当 root 用户访问 NTFS 安全模式数据时，您有两种选择：

- 像任何其他 NFS 用户一样将 root 用户映射到 Windows 用户，并根据 NTFS ACL 管理访问。
- 忽略 NTFS ACL 并提供对 root 的完全访问权限。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

如果希望 root 用户 …	输入命令 …
映射到 Windows 用户	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
绕过 NT ACL 检查	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

默认情况下，此参数处于禁用状态。

如果启用了此参数，但 root 用户没有名称映射，则 ONTAP 将使用默认的 SMB 管理员凭据进行审核。

3. 返回到管理权限级别：

```
set -privilege admin
```

支持的NFS版本和客户端

支持的NFS版本和客户端概述

在网络中使用 NFS 之前，您需要了解 ONTAP 支持哪些 NFS 版本和客户端。

下表说明了ONTAP 默认支持主要和次要NFS协议版本的时间。默认情况下、支持并不表示这是支持该NFS协议的ONTAP 的最早版本。

version	默认情况下处于启用状态
NFSv3	是的。
NFSv4.0	是，从 ONTAP 9.9.1 开始
NFSv4.1	是，从 ONTAP 9.9.1 开始
NFSv4.2	是，从 ONTAP 9.9.1 开始
pNFS	否

有关 ONTAP 支持的 NFS 客户端的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

ONTAP 支持的 NFSv4.0 功能

除了 SPKM3 和 LIPKEY 安全机制之外， ONTAP 还支持 NFSv4.0 中的所有必需功能。

支持以下 NFSv4 功能：

- * 复合 *

  允许客户端在一个远程操作步骤调用（ RPC ）请求中请求多个文件操作。

- * 文件委派 *

  允许服务器将文件控制委派给某些类型的客户端以进行读写访问。

- * 伪 FS*

NFSv4 服务器用于确定存储系统上的挂载点。NFSv4 中没有挂载协议。

- * 锁定 *

  基于租赁。NFSv4 中没有单独的网络锁定管理器（ Network Lock Manager ， NLM ）或网络状态监控器（ Network Status Monitor ， NSM ）协议。

有关 NFSv4.0 协议的详细信息，请参见 RFC 3530 。

NFSv4 的 ONTAP 支持限制

您应了解 ONTAP 对 NFSv4 的支持存在一些限制。

- 并非每种客户端类型都支持委派功能。
- 在 ONTAP 9.4 及更早版本中，存储系统会拒绝 UTF8 卷以外的卷上具有非 ASCII 字符的名称。

  在 ONTAP 9.5 及更高版本中，使用 utf8mb4 语言设置创建并使用 NFS v4 挂载的卷不再受此限制。

- 所有文件句柄都是永久性的；服务器不提供易失性文件句柄。
- 不支持迁移和复制。
- 只读负载共享镜像不支持 NFSv4 客户端。

  ONTAP 会将 NFSv4 客户端路由到负载共享镜像的源，以实现直接读写访问。

- 不支持命名属性。
- 支持所有建议属性，但以下属性除外：
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

  ⓘ 但不支持 `quota*` 属性时、ONTAP通过RQUOTA侧带协议支持用户配额和组配额。

ONTAP 支持 NFSv4.1

从 ONTAP 9.8 开始，如果启用了 NFSv4.1 ，则默认情况下可以使用 nconnect 功能。

早期的 NFS 客户端实施仅使用挂载的单个 TCP 连接。在 ONTAP 中，单个 TCP 连接可能会随着 IOPS 的增加

而成为瓶颈。但是，启用了 nconnect 的客户端可以具有多个与单个 NFS 挂载关联的 TCP 连接（最多 16 个）。此类 NFS 客户端会以轮循的方式将文件操作多路由到多个 TCP 连接上，从而从可用网络带宽中获得更高的吞吐量。建议仅对 NFSv3 和 NFSv4.1 挂载使用 nConnect 。

请参见 NFS 客户端文档以确认您的客户端版本是否支持 nconnect 。

默认情况下， ONTAP 9.9.1 及更高版本会启用 NFSv4.1 。在早期版本中、您可以通过指定来启用它 `-v4.1` 选项并将其设置为 `enabled` 在Storage Virtual Machine (SVM)上创建NFS服务器时。

ONTAP 不支持 NFSv4.1 目录和文件级委派。

ONTAP支持NFSv4.2

从ONTAP 9.8开始、ONTAP支持NFSv4.2协议、以允许已启用NFSv4.2的客户端访问。

在ONTAP 9.9.1及更高版本中、默认情况下会启用NFSv4.2。在ONTAP 9.8中、需要通过指定手动启用v4.2 `-v4.1` 选项并将其设置为 `enabled` 在Storage Virtual Machine (SVM)上创建NFS服务器时。启用 NFSv4.1 还可以使客户端在挂载为 v4.2 时使用 NFSv4.1 功能。

连续几个ONTAP版本都扩展了对NFSv4.2可选功能的支持。

开头为 ...	**NFSv4.2**的可选功能包括...
ONTAP 9.12.1	• NFS扩展属性 • 稀疏文件 • 空间预留
ONTAP 9.9.1	标记为NFS的强制访问控制(MAC)

NFS v4.2安全标签

从 ONTAP 9.1.1 开始，可以启用 NFS 安全标签。默认情况下，它们处于禁用状态。

对于 NFS v4.2 安全标签， ONTAP NFS 服务器可识别强制访问控制（ MAC ），存储和检索客户端发送的 sec_label 属性。

有关详细信息，请参见 "RFC 7240"。

从ONTAP 9.12.1开始、NDMP转储操作支持NFS v4.2安全标签。如果在早期版本中的文件或目录上遇到安全标签、则转储将失败。

步骤

1. 将权限设置更改为高级：

```
set -privilege advanced
```

2. 启用安全标签：

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

NFS扩展属性

从ONTAP 9.12.1开始、默认情况下会启用NFS扩展属性(xattrs)。

扩展属性是定义的标准NFS属性 "RFC 8276" 并在现代NFS客户端中启用。它们可用于将用户定义的元数据附加到文件系统对象、并且对高级安全部署很有兴趣。

NDMP转储操作当前不支持NFS扩展属性。如果文件或目录遇到扩展属性、转储将继续进行、但不会备份这些文件或目录上的扩展属性。

如果需要禁用扩展属性、请使用 `vserver nfs modify -v4.2-xattrs disabled` 命令：

支持并行 NFS 的 ONTAP

ONTAP 支持并行 NFS （ pNFS ）。pNFS 协议可使客户端直接访问分布在集群多个节点上的一组文件的数据，从而提高了性能。它可以帮助客户端找到卷的最佳路径。

使用硬挂载

在排除挂载问题时，您需要确保使用的挂载类型正确。NFS 支持两种挂载类型：软挂载和硬挂载。出于可靠性考虑，您应仅使用硬挂载。

您不应使用软挂载，尤其是在可能频繁出现 NFS 超时的情况下。这些超时可能会导致出现争用情况，进而导致数据损坏。

NFS 和 SMB 文件和目录命名依赖关系

NFS和SMB文件及目录命名依赖关系概述

除了 ONTAP 集群和客户端上的语言设置之外，文件和目录命名约定还取决于网络客户端的` 操作系统和文件共享协议。

操作系统和文件共享协议确定以下内容：

- 文件名可以使用的字符
- 文件名区分大小写

ONTAP 支持文件，目录和 qtree 名称中的多字节字符，具体取决于 ONTAP 版本。

文件或目录名称可以使用的字符

如果要从具有不同操作系统的客户端访问文件或目录，则应使用在两个操作系统中均有效的字符。

例如，如果使用 UNIX 创建文件或目录，请勿在名称中使用冒号（：），因为 MS-DOS 文件或目录名称中不允

许使用冒号。由于对有效字符的限制因操作系统而异，请参见客户端操作系统的文档，了解有关禁止字符的详细信息。

在多协议环境中，文件和目录名称区分大小写

对于NFS客户端、文件和目录名称区分大小写；对于SMB客户端、文件和目录名称不区分大小写、但保留大小写。您必须了解多协议环境的含义，以及在创建 SMB 共享时指定路径以及访问共享中的数据时可能需要执行的操作。

SMB客户端创建名为的目录时 `testdir`，SMB和NFS客户端都会将文件名显示为 `testdir`。但是、如果SMB用户稍后尝试创建目录名称 `TESTDIR`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的目录 `TESTDIR`、NFS和SMB客户端显示目录名称的方式不同，如下所示：

- 例如、在NFS客户端上、您可以在创建这两个目录时看到这两个目录名称 `testdir` 和 `TESTDIR`，因为目录名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个目录。一个目录具有基本文件名。为其他目录分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `testdir` 和 `TESTDI~1`。
  - ONTAP将创建 `TESTDI~1` 用于区分这两个目录的目录名称。

    在这种情况下，在 Storage Virtual Machine （ SVM ）上创建或修改共享时，指定共享路径时必须使用 8.3 名称。

同样、对于文件、如果SMB客户端创建 `test.txt`，SMB和NFS客户端都会将文件名显示为 `text.txt`。但是、如果SMB用户稍后尝试创建 `Test.txt`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的文件 `Test.txt`、NFS和SMB客户端显示文件名的方式不同，如下所示：

- 在NFS客户端上、您会在创建时看到这两个文件名、 `test.txt` 和 `Test.txt`，因为文件名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个文件。一个文件具有基本文件名。为其他文件分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP将创建 `TEST~1.TXT` 用于区分这两个文件的文件名。

> 如果已使用vserver cifs character-Mapping命令创建字符映射、则通常不区分大小写的Windows查找可能区分大小写。这意味着、只有在创建了字符映射且文件名正在使用该字符映射的情况下、文件名查找才区分大小写。

ONTAP 如何创建文件和目录名称

ONTAP 会为可从 SMB 客户端访问的任何目录中的文件或目录创建并维护两个名称：原始长名称和 8.3 格式的名称。

对于超过八个字符名称或三个字符扩展名限制的文件或目录名称（对于文件）， ONTAP 将生成 8.3 格式的名称，如下所示：

- 如果原始文件或目录名称超过 6 个字符，则会将其截断为 6 个字符。
- 它会在截断后不再唯一的文件或目录名称后面附加一个颚化符（~ ）和一个数字（ 1 到 5 ）。

如果由于名称相似而导致数字用尽，则会创建一个与原始名称无关的唯一名称。

- 对于文件，它会将文件扩展名截断为三个字符。

例如、如果NFS客户端创建一个名为的文件 `specifications.html`，则ONTAP创建的8.3格式文件名为 `specif~1.htm`。如果此名称已存在，则 ONTAP 会在文件名末尾使用其他数字。例如、如果NFS客户端创建另一个名为的文件 `specifications_new.html`的`8.3`格式 `specifications_new.html` 为 `specif~2.htm`。

ONTAP 如何处理多字节文件，目录和 **qtree** 名称

从 ONTAP 9.5 开始，通过支持 4 字节 UTF-8 编码名称，可以在基本多语言平面（ BMP ）之外创建和显示包含 Unicode 补充字符的文件，目录和树名。在早期版本中，这些补充字符无法在多协议环境中正确显示。

为了支持4字节UTF-8编码名称、为提供了一个新的_utf8mb4_语言代码 `vserver` 和 `volume` 命令系列。

- 您必须通过以下方式之一创建新卷：
- 设置音量 `-language` 显式选项：

  ```
  volume create -language utf8mb4 {…}
  ```

- 继承卷 `-language` 使用选项创建或修改的SVM中的选项：

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- 如果您使用的是ONTAP 9.6及更早版本、则无法修改现有卷以支持utf8mb4；您必须创建一个新的utf8mb4就绪卷、然后使用基于客户端的复制工具迁移数据。

  如果您使用的是ONTAP 9.7P1或更高版本、则可以根据支持请求修改utf8mb4的现有卷。有关详细信息，请参见 "在ONTAP中创建卷后是否可以更改卷语言？"。

  您可以更新 SVM 以获得 utf8mb4 支持，但现有卷会保留其原始语言代码。

  > 当前不支持包含 4 字节 UTF-8 字符的 LUN 名称。

- Unicode 字符数据通常在使用 16 位 Unicode 转换格式（ UTF-16 ）的 Windows 文件系统应用程序和使用 8 位 Unicode 转换格式（ UTF-8 ）的 NFS 文件系统中表示。

  在 ONTAP 9.5 之前的版本中，由 Windows 客户端创建的名称（包括 UTF-16 补充字符）会正确显示给其他 Windows 客户端，但对于 NFS 客户端，这些名称未正确转换为 UTF-8 。同样，对于 Windows 客户端，已创建的 NFS 客户端使用 UTF-8 补充字符的名称也未正确转换为 UTF-16 。

- 在运行 ONTAP 9.4 或更早版本的系统上创建包含有效或无效补充字符的文件名时， ONTAP 将拒绝该文件名并返回无效文件名错误。

  要避免此问题描述，请在文件名中仅使用 BMP 字符并避免使用补充字符，或者升级到 ONTAP 9.5 或更高版本。

qtree 名称中允许使用 Unicode 字符。

- 您可以使用 `volume qtree` 用于设置或修改qtree名称的命令系列或System Manager。
- qtree 名称可以包含 Unicode 格式的多字节字符，例如日语和中文字符。
- 在 ONTAP 9.5 之前的版本中，仅支持 BMP 字符（即，可以用 3 个字节表示的字符）。

> 在 ONTAP 9.5 之前的版本中， qtree 父卷的接合路径可以包含带有 Unicode 字符的 qtree 和目录名称。。 `volume show` 命令可在父卷具有UTF-8语言设置时正确显示这些名称。但是，如果父卷语言不是 UTF-8 语言设置之一，则会使用数字 NFS 备用名称显示接合路径的某些部分。

- 在 9.5 及更高版本中，如果 qtree 位于启用了 utf8mb4 的卷中，则 qtree 名称中支持 4 字节字符。

在卷上配置用于 **SMB** 文件名转换的字符映射

NFS 客户端可以创建包含对 SMB 客户端和某些 Windows 应用程序无效的字符的文件名。您可以为卷上的文件名转换配置字符映射，以使 SMB 客户端能够访问具有 NFS 名称的文件，否则这些名称将无效。

关于此任务

当 SMB 客户端访问 NFS 客户端创建的文件时， ONTAP 将查看该文件的名称。如果此名称不是有效的 SMB 文件名（例如，如果其包含嵌入的冒号 "`：` " 字符），则 ONTAP 将返回为每个文件维护的 8.3 文件名。但是，如果应用程序将重要信息编码为较长的文件名，则会出现此问题。

因此，如果要在不同操作系统上的客户端之间共享文件，则应在文件名中使用在这两个操作系统中均有效的字符。

但是，如果 NFS 客户端创建的文件名包含的字符对于 SMB 客户端无效，则可以定义一个映射，将无效的 NFS 字符转换为 SMB 和某些 Windows 应用程序均可接受的 Unicode 字符。例如，此功能支持 CATIA MCAD 和 Mathematica 应用程序以及具有此要求的其他应用程序。

您可以逐个卷配置字符映射。

在卷上配置字符映射时，必须牢记以下几点：

- 字符映射不会跨接合点应用。

  您必须为每个接合卷显式配置字符映射。

- 您必须确保用于表示无效或非法字符的 Unicode 字符通常不会显示在文件名中；否则，将发生不需要的映射。

  例如，如果您尝试将冒号（：）映射到连字符（ - ），但在文件名中正确使用了连字符（ - ），则尝试访问名为 "`a-b` " 的文件的 Windows 客户端会将其请求映射到 NFS 名称 "`a： b` " （不是所需结果）。

- 应用字符映射后，如果映射仍包含无效的 Windows 字符，则 ONTAP 会回退到 Windows 8.3 文件名。
- 在 FPolicy 通知， NAS 审核日志和安全跟踪消息中，将显示映射的文件名。
- 创建类型为 DP 的 SnapMirror 关系时，源卷的字符映射不会复制到目标 DP 卷上。
- 区分大小写：由于映射的 Windows 名称转换为 NFS 名称，因此，名称的查找遵循 NFS 语义。这包括 NFS 查找区分大小写。这意味着，访问映射共享的应用程序不能依赖 Windows 不区分大小写的行为。但是， 8.3 名称是可用的，不区分大小写。

- 部分映射或无效映射：映射要返回到执行目录枚举（ "dir" ）的客户端的名称后，系统将检查生成的 Unicode 名称是否有效。如果此名称中仍包含无效字符，或者对于 Windows 无效（例如，此名称以 "." 或空白结尾），则会返回 8.3 名称，而不是无效名称。

步骤

1. 配置字符映射：

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   此映射由一个源 - 目标字符对列表组成，并以 "`：`" 分隔。这些字符是使用十六进制数字输入的 Unicode 字符。例如： 3c： E03C 。

   每个的第一个值 `mapping_text` 以冒号分隔的对是要转换的NFS字符的十六进制值、第二个值是SMB使用的Unicode值。映射对必须是唯一的（应存在一对一映射）。

   - 源映射

     下表显示了源映射允许的 Unicode 字符集：

Unicode 字符	打印字符	Description
0x01-0x19	不适用	非打印控制字符
0x5C	\	反斜杠
0x3a	：	冒号
0x2A	*	星号
0x3F	?	问号
0x22	"	引号
0x3C	<	小于
0x3e	>	大于
0x7C	我们可以为您提供	竖线
0xB1	±	加减号

   - 目标映射

     您可以在 Unicode 的 "`私有使用区域`" 中指定以下范围内的目标字符： U+E0000…U+F8FF 。

示例

以下命令会为 Storage Virtual Machine （ SVM ） vs1 上名为 `data` 的卷创建字符映射：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

用于管理用于 **SMB** 文件名转换的字符映射的命令

您可以通过创建，修改，显示有关 FlexVol 卷上用于 SMB 文件名转换的文件字符映射的信息或删除此类映射来管理字符映射。

如果您要 …	使用此命令 …
创建新的文件字符映射	`vserver cifs character-mapping create`
显示有关文件字符映射的信息	`vserver cifs character-mapping show`
修改现有文件字符映射	`vserver cifs character-mapping modify`
删除文件字符映射	`vserver cifs character-mapping delete`

有关详细信息，请参见每个命令的手册页。

管理NFS中继

NFS中继概述

从ONTAP 9.14.1开始、NFSv4.1客户端可以利用会话中继打开与NFS服务器上不同的LUN的多个连接、从而提高数据传输速度并通过多路径提供故障恢复能力。

对于将FlexVol卷导出到具有中继功能的客户端(尤其是VMware和Linux客户端)、或者对于基于RDMA、TCP或pNFS的NFS、中继非常有用。

在ONTAP 9.14.1中、中继仅限于单个节点上的LUN；中继不能跨多个节点的LUN。

中继支持FlexGroup卷。虽然这样可以提高性能、但只能在单个节点上配置对FlexGroup卷的多路径访问。

此版本中的多路径仅支持会话中继。

如何使用中继

要利用中继提供的多路径优势、您需要一组与包含已启用中继的NFS服务器的SVM关联的LF (称为_TRUNKING group_)。中继组中的LUN必须在集群的同一节点上具有主端口、并且它们必须驻留在这些主端口上。最佳实践是、一个中继组中的所有LUN都属于同一个故障转移组。

ONTAP支持从给定客户端为每个节点建立多达16个中继连接。

当客户端挂载启用了中继的服务器中的导出时、它们会为中继组中的LID指定多个IP地址。客户端连接到第一个LIF后、只有在符合中继组要求的情况下、才会向NFSv4.1会话添加其他LIF并将其用于中继。然后、客户端会根据自己的算法(例如轮循)在多个连接上分布NFS操作。

为了获得最佳性能、您应在专用于提供多路径导出的SVM中配置中继、而不是单路径导出。也就是说、您只能在SVM中的NFS服务器上启用中继、而此SVM的导出仅提供给已启用中继的客户端。

支持的客户端

ONTAP NFSv4.1服务器支持与任何支持NFSv4.1会话中继的客户端进行中继。

以下客户端已通过ONTAP 9.14.1的测试：

- VMware—ESXi 7.0U3及更高版本
- Linux—Red Hat Enterprise Linux (RHEL) 8.8和9.3

> 在NFS服务器上启用中继后、在不支持中继的NFS客户端上访问导出共享的用户可能会看到性能下降。这是因为多个SVM数据SVM挂载只使用一个TCP连接。

NFS中继与**nconnect**之间的区别

从 ONTAP 9.8 开始，如果启用了 NFSv4.1 ，则默认情况下可以使用 nconnect 功能。在支持nconnect的客户端上、一个NFS挂载可以通过一个LIF建立多个TCP连接(最多16个)。

相比之下、中继是_multiPathing_功能、可通过多个LIFs提供多个TCP连接。如果您能够在环境中使用其他NIC、则中继可以提供比nconnect更出色的并行处理能力和性能。

了解更多信息 "n连接。"

为中继配置新的**NFS**服务器和导出

创建启用了中继的**NFS**服务器

从ONTAP 9.14.1开始、可以在NFS服务器上启用中继。创建NFS服务器时、默认情况下会启用NFSv4.1。

开始之前

SVM必须：

- 有足够的存储作为后盾、可满足客户端数据要求。
- 已为NFS启用。

- 专用于NFS中继。不应在其上配置任何其他客户端。

步骤

1. 如果不存在合适的SVM、请创建一个：

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. 验证新创建的 SVM 的配置和状态：

   ```
   vserver show -vserver svm_name
   ```

   了解更多信息 "创建SVM。"

3. 创建NFS服务器：

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. 验证 NFS 是否正在运行：

   ```
   vserver nfs status -vserver svm_name
   ```

5. 验证是否已根据需要配置 NFS ：

   ```
   vserver nfs show -vserver svm_name
   ```

   了解更多信息 "NFS服务器配置。"

完成后

根据需要配置以下服务：

- "DNS"
- "LDAP"
- "Kerberos"

准备用于中继的网络

要利用NFSv4.1中继、中继组中的LUN必须位于同一节点上、并且主端口位于同一节点上。应在同一节点上的故障转移组中配置这些LUN。

关于此任务

LIS和NIC的一对一映射可获得最大的性能提升、但不需要启用中继。至少安装两个NIC可以提高性能、但这并不是必需的。

可以有多个故障转移组、但中继的故障转移组应仅包含中继组中的这些LUN。

在故障转移组中添加或删除连接(和底层NIC)时、您应随时调整中继故障转移组。

开始之前

- 如果要创建故障转移组、您应知道与NIC关联的端口名称。
- 这些端口必须都位于同一节点上。

步骤

1. 验证您计划使用的网络端口的名称和状态：

   ```
   network port status
   ```

2. 创建故障转移组：

   ```
   network interface failover-groups create -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   > 虽然不要求具有故障转移组、但强烈建议这样做。

   - *svm_name* 是包含NFS服务器的SVM的名称。
   - *ports_list* 是要添加到故障转移组的端口列表。

     端口以_node_name：port_number_格式添加、例如node1：e0c。

     以下命令将为SVM VS1创建故障转移组fg3并添加三个端口：

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   了解更多信息 "故障转移组。"

3. 如果需要、为中继组的成员创建LUN：

   ```
   network interface create -vserver svm_name -lif lif_name -home-node node_name
   -home-port port_name -address IP_address -netmask IP_address [-service-policy
   policy] [-auto-revert {true|false}]
   ```

   - `-home-node` -在对LIF运行network interface还原命令时、LIF返回到的节点。

     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` 是对LIF运行network interface还原命令时LIF返回到的物理或逻辑端口。
   - 您可以使用指定IP地址 `-address` 和 `-netmask` 选项、而不是使用 `-subnet` 选项
   - 分配IP地址时、如果不同IP子网上有客户端或域控制器、则可能需要配置网关的默认路由。。 `network route create` 手册页包含有关在SVM中创建静态路由的信息。
   - `-service-policy` - LIF的服务策略。如果未指定策略、则会自动分配默认策略。使用 `network interface service-policy show` 命令以查看可用的服务策略。
   - `-auto-revert` 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、但您可以根据环境中的网络管理策略将其设置为true。

     对中继组中的每个LIF重复此步骤。

以下命令将创建 `lif-A` 对于SVM `vs1`，在端口上 `e0c` 节点的 `cluster1_01`：

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

了解更多信息 "创建LIF。"

4. 验证是否已创建这些生命周期：

```
network interface show
```

5. 验证配置的IP地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

导出数据以供客户端访问

要为客户端提供对数据共享的访问权限、您必须创建一个或多个卷、并且此卷的导出策略必须至少具有一个规则。

客户端导出要求：

- Linux客户端必须为每个中继连接(即每个LIF)具有单独的挂载和单独的挂载点。
- VMware客户端只需要为一个已导出的卷创建一个挂载点、并指定多个生命周期。

  VMware客户端需要在导出策略中具有root访问权限。

步骤

1. 创建导出策略

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

策略名称最长可为 256 个字符。

2. 验证是否已创建导出策略：

```
vserver export-policy show -policyname policy_name
```

示例
以下命令将在名为 vs1 的 SVM 上创建并验证是否已创建名为 exp1 的导出策略：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. 创建导出规则并将其添加到现有导出策略：

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
```

```
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

。 `-clientmatch` 参数应标识要挂载导出的具有中继功能的Linux或VMware客户端。

了解更多信息 "正在创建导出规则。"

4. 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 unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

了解相关信息 "正在创建卷。"

5. 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-path
```

创建客户端挂载

支持中继的Linux和VMware客户端可以从启用了中继的ONTAP NFSv4.1服务器挂载卷或数据共享。

在客户端上输入mount命令时、必须为中继组中的每个LIF输入IP地址。

了解相关信息 "支持的客户端"。

Linux客户端要求

中继组中的每个连接都需要一个单独的挂载点。

使用类似以下内容的命令挂载导出的卷：

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

版本 (`vers`)值应为 `4.1` 或更高版本。

。 `max_connect` 值对应于中继组中的连接数。

VMware客户端要求

需要使用mount语句、其中包含中继组中每个连接的IP地址。

使用类似以下内容的命令挂载导出的数据存储库：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值对应于中继组中的连接。

调整现有NFS导出以用于中继

调整单路径导出概述

您可以调整现有单路径(非中继) NFSv4.1导出以使用中继。只要满足服务器和客户端的前提条件、支持中继的客户端就可以在服务器上启用中继后立即利用性能的提高。

通过调整单路径导出以用于中继、您可以在其现有卷和SVM中维护导出的数据集。为此、您必须在NFS服务器上启用中继、更新网络和导出配置、并在客户端上重新挂载导出的共享。

启用中继会重新启动服务器。然后、VMware客户端必须重新挂载导出的数据存储库；Linux客户端必须使用重新挂载导出的卷 `max_connect` 选项

在NFS服务器上启用中继

必须在NFS服务器上显式启用中继。创建NFS服务器时、默认情况下会启用NFSv4.1。

启用中继后、验证是否已根据需要配置以下服务。

- "DNS"
- "LDAP"
- "Kerberos"

步骤

1. 启用中继并确保已启用NFSv4.1：

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. 验证 NFS 是否正在运行：
   `vserver nfs status -vserver svm_name`
3. 验证是否已根据需要配置 NFS：

   ```
   vserver nfs show -vserver svm_name
   ```

   了解更多信息 "NFS服务器配置。"
   …如果要从此SVM为Windows客户端提供服务、请先移动共享、然后再删除服务器。
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

更新网络以进行中继

NFSv4.1中继要求中继组中的LUN位于同一节点上、并且主端口位于同一节点上。所有的LUN都应配置在同一节点上的故障转移组中。

关于此任务

LIS和NIC的一对一映射可获得最大的性能提升、但启用中继并不需要。

可以有多个故障转移组、但中继的故障转移组必须仅包含中继组中的这些LUN。

在故障转移组中添加或删除连接(和底层NIC)时、您应随时调整中继故障转移组。

开始之前

- 要创建故障转移组、您必须知道与NIC关联的端口名称。
- 这些端口必须都位于同一节点上。

步骤

1. 验证您计划使用的网络端口的名称和状态：

   ```
   network port show
   ```

2. 创建中继故障转移组或修改现有中继故障转移组：

   ```
   network interface failover-groups create -vserver svm_name -failover-group
   failover_group_name -targets ports_list

   network interface failover-groups modify -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   > 虽然不要求具有故障转移组、但强烈建议这样做。

   - *svm_name* 是包含NFS服务器的SVM的名称。
   - *ports_list* 是要添加到故障转移组的端口列表。

端口将以格式添加 *node_name:port_number*，例如， `node1:e0c`。

以下命令将创建故障转移组 `fg3` 对于SVM VS1、添加了三个端口：

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

了解更多信息 "故障转移组。"

3. 根据需要为中继组成员创建其他的LUN：

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

   - `-home-node` -在对LIF运行network interface还原命令时、LIF返回到的节点。

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

   - `-home-port` 是对LIF运行network interface还原命令时LIF返回到的物理或逻辑端口。
   - 您可以使用指定IP地址 `-address` 和 `-netmask` 选项
   - 手动分配IP地址(不使用子网)时、如果其他IP子网上有客户端或域控制器、则可能需要配置网关的默认路由。network route create手册页包含有关在SVM中创建静态路由的信息。
   - `-service-policy` - LIF的服务策略。如果未指定策略、则会自动分配默认策略。使用 `network interface service-policy show` 命令以查看可用的服务策略。
   - `-auto-revert` 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**，但您可以根据环境中的网络管理策略将其设置为true。

     对中继组中所需的每个附加LIF重复此步骤。

     以下命令将在节点"cluster-1_01 "的端口e0c上为SVM VS1创建I1-A：

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

了解更多信息 "创建LIF。"

4. 验证是否已创建这些生命周期：

```
network interface show
```

5. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

修改数据导出以供客户端访问

要使客户端能够利用现有数据共享的中继、您可能需要修改导出策略和规则及其所连接的卷。Linux客户端和VMware数据存储库具有不同的导出要求。

客户端导出要求：

- Linux客户端必须为每个中继连接(即每个LIF)具有单独的挂载和单独的挂载点。

  如果要升级到ONTAP 9.14.1、并且已导出卷、则可以继续在中继组中使用该卷。

- VMware客户端只需要为一个已导出的卷创建一个挂载点、并指定多个生命周期。

  VMware客户端需要在导出策略中具有root访问权限。

步骤

1. 验证现有导出策略是否已到位：

   ```
   vserver export-policy show
   ```

2. 验证现有导出策略规则是否适用于中继配置：

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   特别是、请验证 `-clientmatch` 参数可正确标识要挂载导出的具有中继功能的Linux或VMware客户端。

   如果需要进行调整、请使用修改规则 `vserver export-policy rule modify` 命令或创建新规则：

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   了解更多信息 "正在创建导出规则。"

3. 验证现有导出的卷是否联机：

   ```
   volume show -vserver svm_name
   ```

重新建立客户端挂载

要将非中继客户端连接转换为中继连接、必须卸载Linux和VMware客户端上的现有挂载、然后使用LIFs相关信息重新挂载。

在客户端上输入mount命令时、必须为中继组中的每个LIF输入IP地址。

了解相关信息 "支持的客户端"。

卸载VMware客户端会对数据存储库上的任何VM造成中断。另一种方法是、创建一个启用了中继的新数据存储库、然后使用*存储VMVMotion将VM从旧数据存储库移动到新数据存储库。有关详细信息、请参见VMware文档。

Linux客户端要求

中继组中的每个连接都需要一个单独的挂载点。

使用类似以下内容的命令挂载导出的卷：

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

。 `vers` 值应为 `4.1` 或更高版本。

。 `max_connect` 值应与中继组中的连接数相对应。

VMware客户端要求

需要使用mount语句、其中包含中继组中每个连接的IP地址。

使用类似以下内容的命令挂载导出的数据存储库：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值应与中继组中的连接相对应。

通过 RDMA 管理 NFS

基于 RDMA 的 NFS

基于 RDMA 的 NFS 利用 RDMA 适配器，可以在存储系统内存和主机系统内存之间直接复制数据，从而避免 CPU 中断和开销。

基于 RDMA 的 NFS 配置专为具有延迟敏感型或高带宽工作负载（例如机器学习和分析）的客户而设计。NVIDIA 已通过 RDMA 扩展 NFS ，以启用 GPU 直接存储（ GDS ）。GDS可通过完全绕过CPU和主内存、使用RDMA直接在存储系统和GPU内存之间传输数据、进一步加速支持GPU的工作负载。

从ONTAP 9.14.1开始、NFSv4.1协议支持基于RDMA的NFS配置。

从ONTAP 9.10.1开始、如果与使用RoCE协议版本2的RDMA提供支持的迈乐诺克斯CX-5或CX-6适配器结合使用、则NFSv4.0协议支持基于RDMA的NFS配置。只有使用 NVIDIA Tesla 和 Ampere 系列 GPU 以及 Mellanox NIC 卡和 MoFED 软件时，才支持 GDS 。

基于 RDMA 的 NFS 支持仅限于节点 - 本地流量。支持所有成分卷位于同一节点上的标准 FlexVol 或 FlexGroup ，并且必须从同一节点上的 LIF 进行访问。如果 NFS 挂载大小超过 64k ，则会导致 NFS over RDMA 配置的性能不稳定。

要求

- 存储系统必须运行ONTAP 9.10.1或更高版本
  - 从ONTAP 9.12.1开始、您可以使用System Manager配置基于RDMA的NFS。在ONTAP 9.10.1和9.11.1中、您需要使用命令行界面配置基于RDMA的NFS。
- HA对中的两个节点必须为相同版本。
- 存储系统控制器必须支持RDMA

正在**ONTAP**中开始…	以下控制器支持**RDMA**…
9.10.1及更高版本	• A400 • a700 • A800
ONTAP 9.14.1及更高版本	• AFF C系列 • A900

- 配置了RDMA支持的硬件的存储设备(例如 Mellanox CX-5或CX-6)。
- 必须配置数据 LIF 以支持 RDMA 。
- 客户端必须使用支持 Mellanox RDMA 的 NIC 卡和 Mellanox OFED （ MoFED ）网络软件。

基于RDMA的NFS不支持接口组。

下一步行动

- 为基于 RDMA 的 NFS 配置 NIC
- 通过 RDMA 为 NFS 配置 LIF
- 基于 RDMA 的 NFS 的 NFS 设置

相关信息

- "RDMA"
- NFS中继概述
- "RFC 7530： NFS 版本 4 协议"
- "RFC 8166： 适用于远程操作步骤调用版本 1 的远程直接内存访问传输"
- "RFC 8167： 基于 RDMA 的 RPC 传输的双向远程操作步骤调用"
- "RFC 8267： NFS 上层绑定到 RDMA 上的 RPC 版本 1"

为基于 **RDMA** 的 **NFS** 配置 **NIC**

基于 RDMA 的 NFS 需要为客户端系统和存储平台配置 NIC 。

存储平台配置

需要在服务器上安装 X1148 RDMA 适配器。如果您使用的是 HA 配置，则故障转移配对节点上必须具有相应的 X1148 适配器，以便 RDMA 服务可以在故障转移期间继续运行。NIC 必须支持 ROCE 。

从ONTAP 9.10.1开始、您可以使用以下命令查看RDMA卸载协议列表：

```
network port show -rdma-protocols roce
```

客户端系统配置

客户端必须使用支持 Mellanox RDMA 的 NIC 卡（例如 X1148 ）和 Mellanox OFED 网络软件。有关支持的型号和版本，请参见 Mellanox 文档。尽管客户端和服务器可以直接连接，但由于交换机的故障转移性能有所提高，因此建议使用交换机。

客户端，服务器和任何交换机以及交换机上的所有端口都必须使用巨型帧进行配置。此外，还应确保优先级流量控制在任何交换机上有效。

确认此配置后，您可以挂载 NFS 。

System Manager

您必须使用ONTAP 9.12.1或更高版本使用System Manager通过RDMA使用NFS配置网络接口。

步骤

1. 检查是否支持RDMA。导航到*网络>以太网端口*、然后在组视图中选择相应的节点。展开节点时、请查看给定端口的* RDMA protocols*字段：值* RoCE*表示支持RDMA；短划线(-)表示不支持RDMA。
2. 要添加VLAN、请选择*+ VLAN*。选择相应的节点。在*端口*下拉菜单中、如果可用端口支持RDMA、则会显示文本*已启用RoCE *；如果不支持RDMA、则不会显示任何文本。
3. 按照中的工作流进行操作 使用 NFS 为 Linux 服务器启用 NAS 存储 配置新的NFS服务器。

   添加网络接口时、您可以选择*使用RoCE端口*。对于要使用基于RDMA的NFS的任何网络接口、请选择此选项。

命令行界面

1. 使用命令检查 NFS 服务器上是否启用了 RDMA 访问：

   ```
   vserver nfs show-vserver SVM_name
   ```

   默认情况下、 `-rdma` 应启用。如果不是，请在 NFS 服务器上启用 RDMA 访问：

   ```
   vserver nfs modify -vserver SVM_name -rdma enabled
   ```

2. 通过 NFSv4.0 通过 RDMA 挂载客户端：
   a. proto 参数的输入取决于服务器 IP 协议版本。如果为IPv4、请使用 `proto=rdma`。如果使用IPv6、请使用 `proto=rdma6`。
   b. 将NFS目标端口指定为 `port=20049` 而不是标准端口2049：

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address
   :/volume_path mount_point
   ```

3. 可选：如果需要卸载客户端、请运行命令 `unmount mount_path`

更多信息

- 创建 NFS 服务器
- 使用 NFS 为 Linux 服务器启用 NAS 存储

通过 RDMA 为 NFS 配置 LIF

要使用基于RDMA的NFS、必须将LIF (网络接口)配置为与RDMA兼容。LIF及其故障转移对都必须能够支持RDMA。

创建新的 LIF

System Manager

要使用System Manager通过RDMA为NFS创建网络接口、必须运行ONTAP 9.12.1或更高版本。

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … + Add 。
3. 如果选择* NFS、SMB/CIFS、S3*、则可以选择*使用RoCE端口*。选中*使用RoCE端口*复选框。
4. 选择Storage VM和主节点。分配一个名称。输入IP地址和子网掩码。
5. 输入IP地址和子网掩码后、System Manager会将广播域列表筛选为具有支持RoCE的端口的广播域列表。选择广播域。您可以选择添加网关。
6. 选择 * 保存 * 。

命令行界面

步骤

1. 创建 LIF：

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - 服务策略必须为 default-data-files 或包含 data-nfs 网络接口服务的自定义策略。
   - 。 `-rdma-protocols` 参数接受默认为空的列表。时间 `roce` 作为一种价值、只能在支持RoCE卸载的端口上配置LIF、从而影响爬虫程序LIF迁移和故障转移。

修改 LIF

System Manager

要使用System Manager通过RDMA为NFS创建网络接口、必须运行ONTAP 9.12.1或更高版本。

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … ⋮ 要更改的网络接口旁边的*>编辑*。
3. 选中*使用RoCE端口*以启用基于RDMA的NFS、或者取消选中此复选框以将其禁用。如果网络接口位于支持RoCE的端口上、您将看到*使用RoCE端口*旁边的复选框。
4. 根据需要修改其他设置。
5. 选择*保存*以确认所做的更改。

命令行界面

1. 您可以使用检查您的生命周期管理器的状态 `network interface show` 命令：服务策略必须包含 data-nfs 网络接口服务。。 `-rdma-protocols` 列表应包括 `roce`。如果上述任一条件不正确，请修改 LIF 。
2. 要修改 LIF ，请运行：

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

> 如果当前未将 LIF 分配给支持该协议的端口，则修改 LIF 以要求使用特定的卸载协议会产生错误。

迁移 **LIF**

ONTAP 还允许您迁移网络接口(LIF)以利用基于RDMA的NFS。执行此迁移时、必须确保目标端口支持RoCE。从ONTAP 9.12.1开始、您可以在System Manager中完成此操作步骤。在为网络接口选择目标端口时、System Manager将指定端口是否支持RoCE。

只有在以下情况下、才能将LIF迁移到基于RDMA的NFS配置：

- 它是一个NFS RDMA网络接口(LIF)、托管在支持RoCE的端口上。
- 它是一个NFS TCP网络接口(LIF)、托管在支持RoCE的端口上。
- 它是一个NFS TCP网络接口(LIF)、托管在不支持RoCE的端口上。

有关迁移网络接口的详细信息、请参见 迁移 LIF。

更多信息

- 创建 LIF
- 创建 LIF
- 修改 LIF

- 迁移 LIF

修改 NFS 配置

大多数情况下、您不需要修改已启用NFS的Storage VM的配置、以便通过RDMA使用NFS。

但是，如果您要处理与 Mellanox 芯片和 LIF 迁移相关的问题，则应增加 NFSv4 锁定宽限期。默认情况下，宽限期设置为 45 秒。从ONTAP 9.10.1开始、宽限期的最大值为180 (秒)。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 输入以下命令：

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

有关此任务的详细信息，请参见 指定 NFSv4 锁定宽限期。

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。

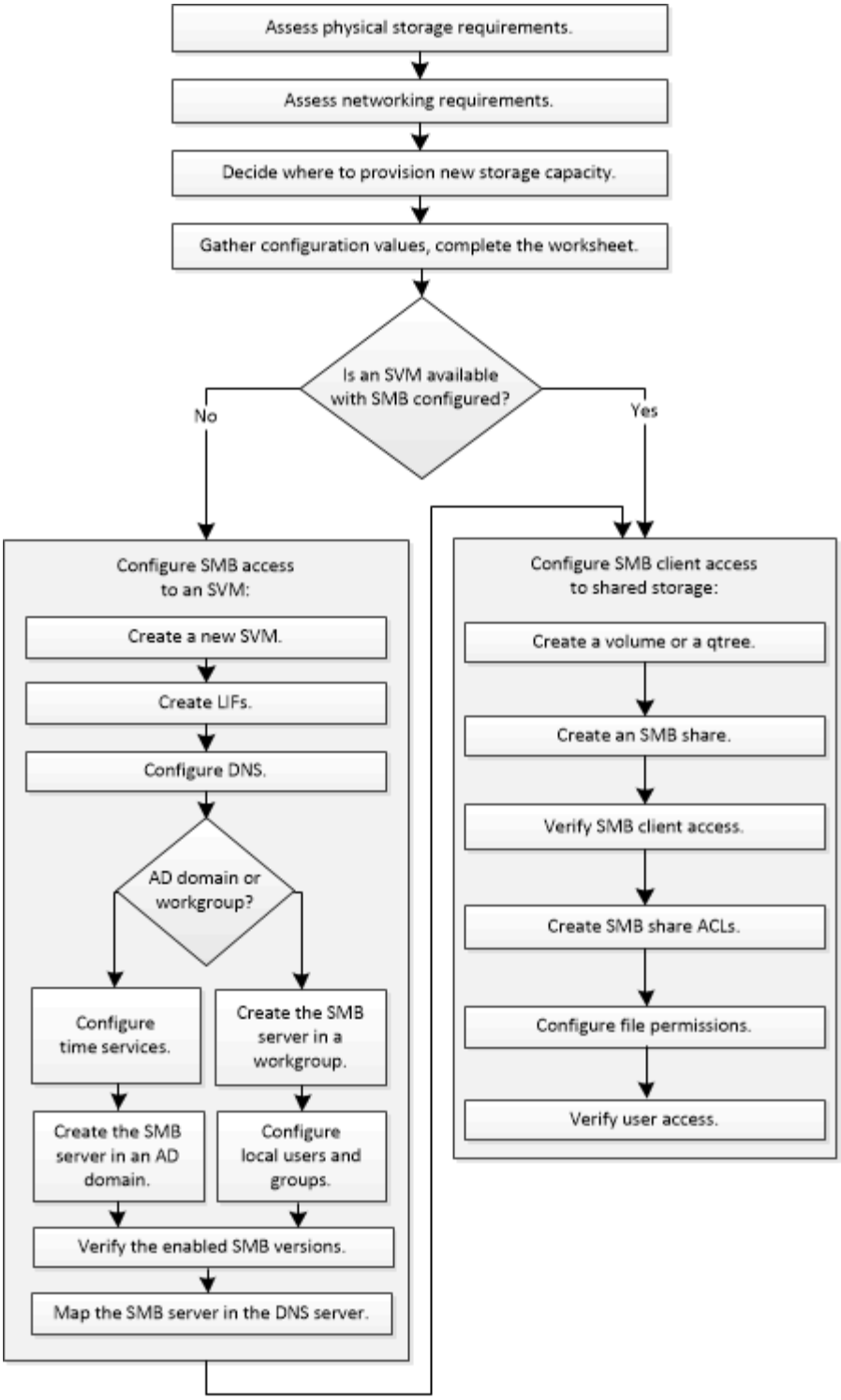
如果您需要有关 ONTAP SMB 协议功能范围的详细信息，请参见 "SMB 参考概述"。

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）	"使用 SMB 为 Windows 服务器配置 NAS 存储"
System Manager 经典版（适用于 ONTAP 9.7 及更早版本）	"SMB配置概述"

SMB配置工作流

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
`-vserver`	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。	
`-aggregate`	集群中具有足够空间来容纳新SMB存储容量的聚合的名称。	
`-rootvolume`	为 SVM 根卷提供的唯一名称。	
`-rootvolume-security-style`	对SVM使用NTFS安全模式。	`ntfs`
`-language`	在此工作流中使用默认语言设置。	`C.UTF-8`
`ipspace`	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
`-lif`	为新 LIF 提供的名称。	
`-role`	在此工作流中使用数据 LIF 角色。	`data`
`-data-protocol`	在此工作流中仅使用SMB协议。	`cifs`

字段	Description	您的价值
-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）。	
`-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
-vserver	要托管新卷的新 SVM 或现有 SVM 的名称。	
-volume	为新卷提供的唯一描述性名称。	
-aggregate	集群中为新SMB卷提供足够空间的聚合的名称。	
-size	为新卷的大小提供的整数。	
-security-style	对此工作流使用NTFS安全模式。	ntfs
-junction-path	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
-vserver	包含 qtree 的卷所在 SVM 的名称。	
-volume	要包含新 qtree 的卷的名称。	
-qtree	为新 qtree 提供的唯一描述性名称，不超过 64 个字符。	
-qtree-path	格式的qtree路径参数 /vol/volume_name/qtree_name\> 可以指定、而不是将卷和qtree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）。	

字段	Description	您的价值
-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 vserver 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 vserver_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 *vserver_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 *vserver_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 `false` 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	`network ping`
IPv6地址	`network ping6`

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 e1c -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 e1c -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

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            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
true
node-2
            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
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

以下命令显示如何创建分配给的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
                                                  Name
   Vserver           State     Domains              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	`cluster time-service ntp server create -server server_name`
使用对称身份验证配置 NTP 服务器	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
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。	`cluster time-service ntp server modify -server server_name -key-id key_id`
配置共享 NTP 密钥	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 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
使用未知密钥 ID 配置 NTP 服务器	`cluster time-service ntp server create -server server_name -key-id key_id`
使用未在 NTP 服务器上配置的密钥 ID 配置服务器。	`cluster time-service ntp server create -server server_name -key-id key_id` 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。
禁用对称身份验证	`cluster time-service ntp server modify -server server_name -authentication disabled`

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::> vserver cifs create -vserver 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 `vserver 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::> vserver cifs show -vserver 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)： `vserver cifs security modify -vserver 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
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
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。

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::> vserver cifs users-and-groups local-group remove-members
-vserver 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 `vserver 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：

   ```
   vserver 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
                           Junction                 Junction
Vserver           Volume  Active   Junction Path   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
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   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::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          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 **ACL** ，请使用 ...	输入命令 ...
Windows 用户	`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`
Windows 组	`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`

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
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
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::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
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	a. 单击 * 添加 * 。 此时将打开选择用户，计算机，服务帐户或组窗口。 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。 c. 单击 * 确定 * 。
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。

使用命令行界面管理SMB

SMB 参考概述

SMB 协议提供了 ONTAP 文件访问功能。您可以启用 CIFS 服务器，创建共享和启用 Microsoft 服务。

> *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* 。

在以下情况下，应使用这些过程：

- 您希望了解 ONTAP SMB 协议功能的范围。
- 您希望执行不太常见的配置和维护任务、而不是基本SMB配置。
- 您希望使用命令行界面（ CLI ），而不是 System Manager 或自动化脚本编写工具。

SMB 服务器支持

SMB 服务器支持概述

您可以在 Storage Virtual Machine （ SVM ）上启用和配置 SMB 服务器，以使 SMB 客户端能够访问集群上的文件。

- 集群中的每个数据 SVM 只能绑定到一个 Active Directory 域。

- 数据 SVM 不需要绑定到同一个域。
- 多个 SVM 可以绑定到同一个域。

在创建 SMB 服务器之前，您必须配置用于提供数据的 SVM 和 LIF 。如果您的数据网络不平整，则可能还需要配置 IP 空间，广播域和子网。网络管理指南 _ 包含详细信息。

相关信息

"网络管理"

修改 SMB 服务器

"系统管理"

支持的 **SMB** 版本和功能

服务器消息块（ SMB ）是 Microsoft Windows 客户端和服务器使用的一种远程文件共享协议。在 ONTAP 9 中，支持所有 SMB 版本；但是，默认 SMB 1.0 支持取决于您的 ONTAP 版本。您应验证 ONTAP SMB 服务器是否支持环境中所需的客户端和功能。

有关 ONTAP 支持的 SMB 客户端和域控制器的最新信息，请参见 *Interoperability Matrix Tool* 。

默认情况下， ONTAP 9 SMB 服务器会启用 SMB 2.0 及更高版本，并且可以根据需要启用或禁用这些版本。下表显示了 SMB 1.0 支持和默认配置。

SMB 1.0 功能：	在以下 **ONTAP 9** 版本中：			
	9.0	9.1.	9.2.	9.3及更高版本
默认情况下处于启用状态	是的。	是的。	是的。	否
可以启用或禁用	否	是 * 需要 9.1 P8 或更高版本。	是的。	是的。

> 与域控制器的 SMB 1.0 和 2.0 连接的默认设置也取决于 ONTAP 版本。有关详细信息、请参见 `vserver cifs security modify` 手册页。对于现有 CIFS 服务器运行 SMB 1.0 的环境，您应尽快迁移到更高的 SMB 版本，以便为增强安全性和合规性做好准备。有关详细信息，请联系您的 NetApp 代表。

下表显示了每个 SMB 版本支持的 SMB 功能。默认情况下，某些 SMB 功能处于启用状态，某些功能需要额外配置。

* 此功能： *	* 需要启用： *	对于以下 **SMB** 版本： * ， **ONTAP 9** 支持 *				
		1.0	2.0	2.1.	3.0	3.1.1
旧版 SMB 1.0 功能		X	X	X	X	X

* 此功能： *	* 需要启用： *	对于以下 **SMB** 版本： * ， **ONTAP 9** 支持 *				
耐用手柄			X	X	X	X
复合操作			X	X	X	X
异步操作			X	X	X	X
读取和写入缓冲区大小增加			X	X	X	X
提高可扩展性			X	X	X	X
SMB 签名	X	X	X	X	X	X
备用数据流（ ADS ）文件格式	X	X	X	X	X	X
大型 MTU （从 ONTAP 9.7 开始，默认情况下处于启用状态）	X			X	X	X
租用机会锁				X	X	X
持续可用的共享	X				X	X
持久句柄					X	X
见证					X	X
SMB 加密：AES-128-CCM	X				X	X
横向扩展（ CA 共享需要）					X	X
透明故障转移					X	X

* 此功能： *	* 需要启用： *	对于以下 **SMB** 版本： * ， **ONTAP 9** 支持 *				
SMB 多通道（从 ONTAP 9.4 开始）	X				X	X
预身份验证完整性						X
集群客户端故障转移 v.2 （CCFv2）						X
SMB 加密：AES-128-GCM （从 ONTAP 9.1 开始）	X					X

相关信息

使用 SMB 签名增强网络安全性

设置 SMB 服务器的最低身份验证安全级别

在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密

"NetApp 技术报告 4543 ：《 SMB 协议最佳实践》"

"NetApp 互操作性"

不支持的 **Windows** 功能

在网络中使用 CIFS 之前，您需要了解 ONTAP 不支持的某些 Windows 功能。

ONTAP 不支持以下 Windows 功能：

- 加密文件系统（ EFS ）
- 在更改日志中记录 NT 文件系统（ NTFS ）事件
- Microsoft 文件复制服务（ FRS ）
- Microsoft Windows 索引服务
- 通过分层存储管理（ HSM ）实现远程存储
- 从 Windows 客户端管理配额
- Windows 配额语义
- LMHOSTS 文件
- NTFS 原生压缩

在 **SVM** 上配置 **NIS** 或 **LDAP** 名称服务

通过 SMB 访问，即使访问 NTFS 安全模式卷中的数据，也始终会执行用户到 UNIX 用户的映射。如果将 Windows 用户映射到信息存储在 NIS 或 LDAP 目录存储中的相应 UNIX 用户，或者使用 LDAP 进行名称映射，则应在 SMB 设置期间配置这些名称服务。

开始之前

您必须已自定义名称服务数据库配置，以匹配名称服务基础架构。

关于此任务

SVM 使用名称服务 ns-switch 数据库确定查找给定名称服务数据库源的顺序。ns-switch 源可以是 "`files` "，"`nis` " 或 "`ldap` " 的任意组合。对于组数据库， ONTAP 会尝试从所有已配置的源获取组成员资格，然后使用整合的组成员资格信息进行访问检查。如果在获取 UNIX 组信息时其中一个源不可用，则 ONTAP 无法获取完整的 UNIX 凭据，后续访问检查可能会失败。因此，您必须始终检查 ns-switch 设置中是否为组数据库配置了所有 ns-switch 源。

默认情况下、SMB服务器会将所有Windows用户映射到本地存储的默认UNIX用户 `passwd` 数据库。如果要使用默认配置，可选择配置 NIS 或 LDAP UNIX 用户和组名称服务或 LDAP 用户映射以进行 SMB 访问。

步骤

1. 如果 UNIX 用户，组和网络组信息由 NIS 名称服务管理，请配置 NIS 名称服务：

   a. 使用确定名称服务的当前顺序 `vserver services name-service ns-switch show` 命令：

      在此示例中、三个数据库 (`group`， `passwd`，和 `netgroup`) `nis` 作为名称服务源、仅使用 `files` 作为源。

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                      Source
      Vserver         Database       Enabled          Order
      --------------- ------------   ---------        ---------
      vs1             hosts          true             dns,
                                                      files
      vs1             group          true             files
      vs1             passwd         true             files
      vs1             netgroup       true             files
      vs1             namemap        true             files
      ```

      您必须添加 `nis` 源到 `group` 和 `passwd` 数据库、并可选择添加到 `netgroup` 数据库。

   b. 使用根据需要调整名称服务ns-switch数据库的顺序 `vserver services name-service ns-switch modify` 命令：

      为了获得最佳性能，您不应向名称服务数据库添加名称服务，除非您计划在 SVM 上配置该名称服务。

      如果修改多个名称服务数据库的配置，则必须为要修改的每个名称服务数据库单独运行此命令。

在此示例中、 `nis` 和 `files` 配置为的源 `group` 和 `passwd` 数据库、按此顺序。其余名称服务数据库保持不变。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. 使用验证名称服务的顺序是否正确 `vserver services name-service ns-switch show` 命令：

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                    Source
Vserver         Database       Enabled              Order
--------------- ------------   ---------            ---------
vs1             hosts          true                 dns,
                                                    files
vs1             group          true                 nis,
                                                    files
vs1             passwd         true                 nis,
                                                    files
vs1             netgroup       true                 files
vs1             namemap        true                 files
```

d. 创建NIS名称服务配置：+
`vserver services name-service nis-domain create -vserver` *`vserver_name`*
`-domain` *`NIS_domain_name`* `-servers` *`NIS_server_IPaddress`*`,… -active true+`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```

> 从ONTAP 9.2开始、此字段为 `-nis-servers` 替换字段 `-servers`。此新字段可以使用NIS服务器的主机名或IP地址。

e. 验证NIS名称服务是否已正确配置且处于活动状态： `vserver services name-service nis-domain show vserver` *`vserver_name`*

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver        Domain               Active Server
-------------- -------------------- ------ ---------------
vs1            example.com          true   10.0.0.60
```

2. 如果 UNIX 用户，组和网络组信息或名称映射由 LDAP 名称服务管理，请使用位于的信息配置 LDAP 名称服务 "NFS 管理"。

ONTAP 名称服务交换机配置的工作原理

ONTAP会将名称服务配置信息存储在一个表中、该表相当于 `/etc/nsswitch.conf` 文件。您必须了解该表的功能以及 ONTAP 如何使用它，以便可以根据您的环境对其进行适当配置。

ONTAP 名称服务切换表可确定 ONTAP 为检索特定类型的名称服务信息而查询的名称服务源。ONTAP 会为每个 SVM 维护一个单独的名称服务切换表。

数据库类型

该表为以下每种数据库类型存储一个单独的名称服务列表：

数据库类型	定义名称服务源 ...	有效源为 ...
主机	将主机名转换为 IP 地址	文件， DNS
组	查找用户组信息	文件， nis ， ldap
密码	查找用户信息	文件， nis ， ldap
网络组	正在查找网络组信息	文件， nis ， ldap
命名映射	正在映射用户名	文件， LDAP

源类型

源用于指定用于检索相应信息的名称服务源。

指定源类型 ...	查找信息的位置	由命令系列管理 ...

文件	本地源文件	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在 SVM 的 NIS 域配置中指定的外部 NIS 服务器	`vserver services name-service nis-domain`
ldap	在 SVM 的 LDAP 客户端配置中指定的外部 LDAP 服务器	`vserver services name-service ldap`

指定源类型 ...	查找信息的位置	由命令系列管理 ...
DNS	在 SVM 的 DNS 配置中指定的外部 DNS 服务器	`vserver services name-service dns`

即使您计划使用NIS或LDAP进行数据访问和SVM管理身份验证、也仍应包括 `files` 并将本地用户配置为在NIS或LDAP身份验证失败时的回退。

用于访问外部源的协议

要访问外部源的服务器， ONTAP 使用以下协议：

外部名称服务源	用于访问的协议
NIS	UDP
DNS	UDP
LDAP	TCP

示例

以下示例显示了SVM的名称服务开关配置 `svm_1`：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

要查找用户或组信息， ONTAP 仅会查找本地源文件。如果查询未返回任何结果，则查找将失败。

要查找网络组信息， ONTAP 首先会查找外部 NIS 服务器。如果查询未返回任何结果，则接下来会检查本地网络组文件。

SVM SVM_1 的表中没有用于名称映射的名称服务条目。因此，默认情况下， ONTAP 仅会查找本地源文件。

管理 **SMB** 服务器

修改 **SMB** 服务器

您可以使用将SMB服务器从工作组移动到Active Directory域、从工作组移动到另一个工作组或从Active Directory域移动到工作组 `vserver cifs modify` 命令：

关于此任务

您还可以修改 SMB 服务器的其他属性，例如 SMB 服务器名称和管理状态。有关详细信息，请参见手册页。

选项

- 将 SMB 服务器从工作组移动到 Active Directory 域：

  a. 将SMB服务器的管理状态设置为 `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. 将SMB服务器从工作组移动到Active Directory域： `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  要为SMB服务器创建Active Directory计算机帐户、您必须提供具有足够权限的Windows帐户的名称和密码、以便向添加计算机 `ou=`*`example`* `ou` 中的容器 *`example`*.com域。

  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

- 将 SMB 服务器从一个工作组移动到另一个工作组：

  a. 将SMB服务器的管理状态设置为 `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. 修改SMB服务器的工作组： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- 将 SMB 服务器从 Active Directory 域移动到工作组：

  a. 将SMB服务器的管理状态设置为 `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. 将SMB服务器从Active Directory域移动到工作组： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

  ```
  cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
  ```

> 要进入工作组模式，系统必须禁用所有基于域的功能并自动删除其配置，包括持续可用的共享，卷影副本和 AES 。但是，域配置的共享 ACL （例如 EXAMPLE.COM\userName" ）将无法正常工作，但 ONTAP 无法删除。命令完成后，使用外部工具尽快删除这些共享 ACL 。如果已启用 AES ，则可能会要求您提供具有足够权限的 Windows 帐户的名称和密码，以便在 example.com 域中禁用它。

- 使用的相应参数修改其他属性 `vserver cifs modify` 命令：

使用选项自定义SMB服务器

可用的 SMB 服务器选项

在考虑如何自定义 SMB 服务器时，了解哪些选项可用非常有用。虽然某些选项在 SMB 服务器上通用，但也有一些选项用于启用和配置特定的 SMB 功能。SMB服务器选项可通过控制 `vserver cifs options modify` 选项

以下列表指定了在管理员权限级别可用的 SMB 服务器选项：

- * 配置 SMB 会话超时值 *

  通过配置此选项，您可以指定断开 SMB 会话之前空闲时间的秒数。空闲会话是指用户未在客户端上打开任何文件或目录的会话。默认值为900秒。

- * 配置默认 UNIX 用户 *

  通过配置此选项，您可以指定 SMB 服务器使用的默认 UNIX 用户。ONTAP 会自动创建一个名为 "`pcuser` " 的默认用户 （ UID 为 65534 ），创建一个名为 "`pcuser` " 的组 （ GID 为 65534 ），并将默认用户添加到 "`pcuser` " 组。创建 SMB 服务器时， ONTAP 会自动将 "`pcuser` " 配置为默认 UNIX 用户。

- * 配置子系统 UNIX 用户 *

  通过配置此选项，您可以指定从不可信域登录的用户映射到的 UNIX 用户的名称，从而允许来自不可信域的用户连接到 SMB 服务器。默认情况下，不会配置此选项（没有默认值）；因此，默认情况下不允许来自不可信域的用户连接到 SMB 服务器。

- * 启用或禁用模式位的读取授予执行 *

  通过启用或禁用此选项，您可以指定是否允许 SMB 客户端使用其具有读取访问权限的 UNIX 模式位运行可执行文件，即使未设置 UNIX 可执行位也是如此。默认情况下，此选项处于禁用状态。

- * 启用或禁用从 NFS 客户端删除只读文件的功能 *

  启用或禁用此选项将确定是否允许 NFS 客户端删除设置了只读属性的文件或文件夹。设置只读属性后，NTFS 删除语义不允许删除文件或文件夹。UNIX 删除语义将忽略只读位，而是使用父目录权限来确定是否可以删除文件或文件夹。默认设置为 `disabled`，这会导致NTFS删除义。

- * 配置 Windows Internet 名称服务服务器地址 *

  通过配置此选项，您可以将 Windows Internet 名称服务 （ WINS ）服务器地址列表指定为逗号分隔列表。您必须指定 IPv4 地址。不支持 IPv6 地址。没有默认值。

以下列表指定了在高级权限级别可用的 SMB 服务器选项：

- * 向 CIFS 用户授予 UNIX 组权限 *

  配置此选项可确定是否可以向不是文件所有者的传入 CIFS 用户授予组权限。如果CIFS用户不是UNIX安全模式文件的所有者、并且此参数设置为 `true`，则为该文件授予组权限。如果CIFS用户不是UNIX安全模式文件的所有者、并且此参数设置为 `false``则可以使用常规`UNIX`规则授予文件权限。此参数适用于权限设置为的`UNIX`安全模式文件 `mode bits` 和不适用于采用NTFS或NFSv4安全模式的文件。默认设置为 `false`。

- * 启用或禁用 SMB 1.0*

  默认情况下，在 ONTAP 9.3 中为其创建 SMB 服务器的 SVM 上禁用 SMB 1.0 。

  > 从 ONTAP 9.3 开始，默认情况下，对于在 ONTAP 9.3 中创建的新 SMB 服务器， SMB 1.0 处于禁用状态。您应尽快迁移到更高版本的 SMB ，以便为增强安全性和合规性做好准备。有关详细信息，请联系您的 NetApp 代表。

- * 启用或禁用 SMB 2.x *

  SMB 2.0 是支持 LIF 故障转移的最低 SMB 版本。如果禁用 SMB 2.x ，则 ONTAP 还会自动禁用 SMB 3.x

  SMB 2.0 仅在 SVM 上受支持。默认情况下，此选项在 SVM 上处于启用状态

- 启用或禁用**SMB 3.0**

  SMB 3.0 是支持持续可用共享的最低 SMB 版本。Windows Server 2012 和 Windows 8 是支持 SMB 3.0 的最低 Windows 版本。

  SMB 3.0仅在SVM上受支持。默认情况下，此选项在 SVM 上处于启用状态

- 启用或禁用**SMB 3.1**

  Windows 10 是唯一支持 SMB 3.1 的 Windows 版本。

  SMB 3.1仅在SVM上受支持。默认情况下，此选项在 SVM 上处于启用状态

- * 启用或禁用 ODX 副本卸载 *

  ODX 副本卸载由支持它的 Windows 客户端自动使用。默认情况下，此选项处于启用状态。

- * 启用或禁用 ODX 副本卸载的直接复制机制 *

  如果 Windows 客户端尝试以防止在复制过程中更改文件的模式打开副本的源文件，则直接复制机制可以提高副本卸载操作的性能。默认情况下，直接复制机制处于启用状态。

- * 启用或禁用自动节点转介 *

  对于自动节点转介， SMB 服务器会自动将客户端转介到托管通过请求的共享访问的数据的节点的本地数据 LIF 。

- * 启用或禁用 SMB 的导出策略 *

默认情况下，此选项处于禁用状态。

- * 启用或禁用使用接合点作为重新解析点 *

  如果启用此选项，则 SMB 服务器会将接合点作为重新解析点公开给 SMB 客户端。此选项仅适用于 SMB 2.x 或 SMB 3.0 连接。默认情况下，此选项处于启用状态。

  此选项仅在 SVM 上受支持。默认情况下，此选项在 SVM 上处于启用状态

- * 配置每个 TCP 连接的最大并发操作数 *

  默认值为255。

- * 启用或禁用本地 Windows 用户和组功能 *

  默认情况下，此选项处于启用状态。

- * 启用或禁用本地 Windows 用户身份验证 *

  默认情况下，此选项处于启用状态。

- * 启用或禁用 VSS 卷影复制功能 *

  ONTAP 使用卷影复制功能对使用 Hyper-V over SMB 解决方案存储的数据执行远程备份。

  此选项仅在 SVM 上受支持，并且仅适用于基于 SMB 的 Hyper-V 配置。默认情况下，此选项在 SVM 上处于启用状态

- * 配置卷影复制目录深度 *

  通过配置此选项，您可以定义在使用卷影复制功能时要创建卷影副本的目录的最大深度。

  此选项仅在 SVM 上受支持，并且仅适用于基于 SMB 的 Hyper-V 配置。默认情况下，此选项在 SVM 上处于启用状态

- * 启用或禁用名称映射的多域搜索功能 *

  如果启用了此选项，则在使用 Windows 用户名的域部分（例如， *\joe ）中的通配符（ * ）将 UNIX 用户映射到 Windows 域用户时， ONTAP 将在对主域具有双向信任的所有域中搜索指定用户。主域是包含 SMB 服务器计算机帐户的域。

  除了搜索所有双向受信任域之外，您还可以配置首选受信任域的列表。如果启用了此选项并配置了首选列表，则会使用首选列表执行多域名称映射搜索。

  默认情况下，启用多域名称映射搜索。

- * 配置文件系统扇区大小 *

  通过配置此选项，您可以配置 ONTAP 向 SMB 客户端报告的文件系统扇区大小（以字节为单位）。此选项有两个有效值： `4096` 和 `512`。默认值为 `4096`。您可能需要将此值设置为 `512` 如果Windows应用程序仅支持512字节的扇区大小。

- * 启用或禁用动态访问控制 *

启用此选项后，您可以使用动态访问控制（ DAC ）来保护 SMB 服务器上的对象，包括使用审核暂存中央访问策略以及使用组策略对象实施中央访问策略。默认情况下，此选项处于禁用状态。

此选项仅在 SVM 上受支持。

- * 设置非身份验证会话的访问限制（限制匿名） *

  设置此选项可确定非身份验证会话的访问限制。这些限制将应用于匿名用户。默认情况下，匿名用户没有访问限制。

- * 启用或禁用在具有 UNIX 有效安全性的卷（ UNIX 安全模式卷或具有 UNIX 有效安全性的混合安全模式卷）上呈现 NTFS ACL *

  启用或禁用此选项可确定如何向 SMB 客户端提供具有 UNIX 安全性的文件和文件夹的文件安全性。如果启用，则 ONTAP 会将具有 UNIX 安全性的卷中的文件和文件夹呈现给 SMB 客户端，并将其视为具有 NTFS ACL 的 NTFS 文件安全性。如果禁用，则 ONTAP 会将具有 UNIX 安全性的卷显示为 FAT 卷，而不会提供文件安全性。默认情况下，卷显示为具有 NTFS ACL 的 NTFS 文件安全性。

- * 启用或禁用 SMB 虚假打开功能 *

  启用此功能可优化 ONTAP 在查询文件和目录上的属性信息时发出打开和关闭请求的方式，从而提高 SMB 2.x 和 SMB 3.0 的性能。默认情况下， SMB fake open 功能处于启用状态。此选项仅适用于使用 SMB 2.x 或更高版本建立的连接。

- * 启用或禁用 UNIX 扩展 *

  启用此选项可在 SMB 服务器上启用 UNIX 扩展。UNIX 扩展允许通过 SMB 协议显示 POSIX/UNIX 模式的安全性。默认情况下，此选项处于禁用状态。

  如果您的环境中有基于 UNIX 的 SMB 客户端，例如 Mac OSX 客户端，则应启用 UNIX 扩展。启用 UNIX 扩展后， SMB 服务器可以通过 SMB 将 POSIX/UNIX 安全信息传输到基于 UNIX 的客户端，然后将安全信息转换为 POSIX/UNIX 安全。

- * 启用或禁用对短名称搜索的支持 *

  启用此选项可使 SMB 服务器对短名称执行搜索。启用了此选项的搜索查询会尝试匹配 8.3 文件名和长文件名。此参数的默认值为 `false`。

- * 启用或禁用对自动公布 DFS 功能的支持 *

  启用或禁用此选项可确定 SMB 服务器是否自动向连接到共享的 SMB 2.x 和 SMB 3.0 客户端公布 DFS 功能。ONTAP 在实施用于 SMB 访问的符号链接时使用 DFS 转介。如果启用，则无论是否启用符号链接访问， SMB 服务器都会始终公布 DFS 功能。如果禁用，则只有当客户端连接到启用了符号链接访问的共享时，SMB 服务器才会公布 DFS 功能。

- * 配置最大 SMB 信用数 *

  从ONTAP 9.4开始、配置 `-max-credits` 选项允许您限制在客户端和服务器运行SMB版本2或更高版本时在SMB连接上授予的信用值数量。默认值为128。

- * 启用或禁用对 SMB 多通道的支持 *

  启用 `-is-multichannel-enabled` 如果在集群及其客户端上部署了适当的NIC、则ONTAP 9.4及更高版

本中的选项允许SMB服务器为单个SMB会话建立多个连接。这样可以提高吞吐量和容错能力。此参数的默认值为 `false`。

启用 SMB 多通道后，您还可以指定以下参数：

- 每个多通道会话允许的最大连接数。此参数的默认值为 32 。
- 每个多通道会话公布的最大网络接口数。此参数的默认值为256。

配置SMB服务器选项

在Storage Virtual Machine (SVM)上创建SMB服务器后、您可以随时配置SMB服务器选项。

步骤

1. 执行所需的操作：

要配置SMB服务器选项的项	输入命令 ...
处于管理权限级别	`vserver cifs options modify -vserver` *`vserver_name options`*
在高级权限级别	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

有关配置SMB服务器选项的详细信息、请参见的手册页 `vserver cifs options modify` 命令：

配置向SMB用户授予UNIX组权限

您可以将此选项配置为授予组访问文件或目录的权限、即使传入的SMB用户不是文件的所有者也是如此。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 根据需要配置授予 UNIX 组权限：

如果您要 ...	输入命令 ...
启用对文件或目录的访问以获取组权限，即使用户不是文件的所有者也是如此	`vserver cifs options modify –grant-unix-group-perms-to-others true`
禁用对文件或目录的访问以获取组权限，即使用户不是文件的所有者也是如此	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. 验证此选项是否设置为所需值： `vserver cifs options show –fields grant-unix-group-`

`perms-to-others`

4. 返回到管理权限级别： `set -privilege admin`

配置匿名用户的访问限制

默认情况下，未经身份验证的匿名用户（也称为 *null user* ）可以访问网络上的某些信息。您可以使用SMB服务器选项为匿名用户配置访问限制。

关于此任务

。 `-restrict-anonymous` SMB服务器选项对应于 `RestrictAnonymous` Windows中的注册表项。

匿名用户可以列出或枚举网络上 Windows 主机中的某些类型的系统信息，包括用户名和详细信息，帐户策略和共享名称。您可以通过指定以下三种访问限制设置之一来控制匿名用户的访问：

价值	**Description**
`no-restriction` (默认)	不指定匿名用户的访问限制。
`no-enumeration`	指定仅限制匿名用户的枚举。
`no-access`	指定对匿名用户的访问进行限制。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置限制匿名设置： `vserver cifs options modify -vserver` *`vserver_name`* `-restrict -anonymous {no-restriction|no-enumeration|no-access}`
3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

相关信息

可用的 SMB 服务器选项

管理如何为 **UNIX** 安全模式数据的 **SMB** 客户端提供文件安全性

管理如何向 **SMB** 客户端提供文件安全性以了解 **UNIX** 安全模式数据概述

您可以通过启用或禁用向 SMB 客户端提供 NTFS ACL 来选择如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性。每个设置都有一些优势，您应了解这些优势，才能选择最适合您业务需求的设置。

默认情况下， ONTAP 会将 UNIX 安全模式卷上的 UNIX 权限作为 NTFS ACL 提供给 SMB 客户端。在某些情况下，这种做法是可取的，其中包括以下情形：

- 要查看和编辑 UNIX 权限，请使用 Windows 属性框中的 * 安全性 * 选项卡。

  如果 UNIX 系统不允许修改 Windows 客户端的权限，则不能修改此操作。例如，您不能更改不拥有的文件

的所有权，因为 UNIX 系统不允许执行此操作。此限制可防止 SMB 客户端绕过对文件和文件夹设置的 UNIX 权限。

- 用户正在使用某些 Windows 应用程序编辑和保存 UNIX 安全模式卷上的文件，例如 Microsoft Office ，在这些应用程序中， ONTAP 必须在保存操作期间保留 UNIX 权限。
- 您的环境中有一些 Windows 应用程序希望对其使用的文件读取 NTFS ACL 。

在某些情况下，您可能需要禁用将 UNIX 权限作为 NTFS ACL 呈现。如果禁用此功能，则 ONTAP 会将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端。您可能希望将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端的具体原因如下：

- 您只能通过在 UNIX 客户端上使用挂载来更改 UNIX 权限。

  在 SMB 客户端上映射 UNIX 安全模式卷时， " 安全 " 选项卡不可用。映射的驱动器似乎已使用 FAT 文件系统进行格式化，该文件系统没有文件权限。

- 您正在通过 SMB 使用应用程序，这些应用程序会对访问的文件和文件夹设置 NTFS ACL ，如果数据驻留在 UNIX 安全模式卷上，则这些应用程序可能会失败。

  如果 ONTAP 将卷报告为 FAT ，则应用程序不会尝试更改 ACL 。

相关信息

在 FlexVol 卷上配置安全模式

在 qtree 上配置安全模式

启用或禁用为 **UNIX** 安全模式数据提供 **NTFS ACL**

您可以为 UNIX 安全模式数据（ UNIX 安全模式卷和具有 UNIX 有效安全性的混合安全模式卷）启用或禁用向 SMB 客户端提供 NTFS ACL 。

关于此任务

如果启用此选项，则 ONTAP 会将具有有效 UNIX 安全模式的卷上的文件和文件夹作为具有 NTFS ACL 提供给 SMB 客户端。如果禁用此选项，这些卷将作为 FAT 卷呈现给 SMB 客户端。默认情况下，将 NTFS ACL 提供给 SMB 客户端。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置UNIX NTFS ACL选项设置： `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

ONTAP 如何保留 **UNIX** 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 **Windows** 安全性选项卡管理 **UNIX** 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用 Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

  如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

  更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。

管理 **SMB** 服务器安全设置

ONTAP 如何处理 **SMB** 客户端身份验证

用户必须先通过SMB服务器所属的域进行身份验证、然后才能创建SMB连接以访问SVM上包含的数据。SMB服务器支持两种身份验证方法：Kerberos和NTLM (NTLMv1或NTLMv2)。Kerberos 是用于对域用户进行身份验证的默认方法。

Kerberos 身份验证

在创建经过身份验证的 SMB 会话时， ONTAP 支持 Kerberos 身份验证。

Kerberos 是 Active Directory 的主身份验证服务。Kerberos 服务器或 Kerberos 密钥分发中心（ KDC ）服务可在 Active Directory 中存储和检索有关安全原则的信息。与 NTLM 模式不同，要与另一台计算机（如 SMB 服务器）建立会话的 Active Directory 客户端会直接联系 KDC 以获取其会话凭据。

NTLM身份验证

NTLM 客户端身份验证可使用质询响应协议来完成，该协议基于密码共享用户特定的机密信息。

如果用户使用本地 Windows 用户帐户创建 SMB 连接，则 SMB 服务器将使用 NTLMv2 在本地完成身份验证。

SVM 灾难恢复配置中的 **SMB** 服务器安全设置准则

在创建配置为不保留身份的灾难恢复目标的SVM之前(`-identity-preserve` 选项设置为 `false` 在SnapMirror配置中)、您应了解如何在目标SVM上管理SMB服务器安全设置。

- 非默认 SMB 服务器安全设置不会复制到目标。

  在目标 SVM 上创建 SMB 服务器时，所有 SMB 服务器安全设置均设置为默认值。初始化，更新或重新同步 SVM 灾难恢复目标时，源上的 SMB 服务器安全设置不会复制到目标。

- 您必须手动配置非默认 SMB 服务器安全设置。

  如果在源 SVM 上配置了非默认 SMB 服务器安全设置，则在目标变为读写（ SnapMirror 关系中断）后，必须在目标 SVM 上手动配置这些相同的设置。

显示有关**SMB**服务器安全设置的信息

您可以显示Storage Virtual Machine (SVM)上的SMB服务器安全设置信息。您可以使用此信息验证安全设置是否正确。

关于此任务

显示的安全设置可以是该对象的默认值，也可以是使用 ONTAP 命令行界面或使用 Active Directory 组策略对象（ GPO ）配置的非默认值。

请勿使用 `vserver cifs security show` 命令、因为某些选项无效。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
指定 SVM 上的所有安全设置	`vserver cifs security show -vserver` *`vserver_name`*
SVM 上的特定安全设置	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 您可以输入 `-fields ?` 以确定您可以使用哪些字段。

示例

以下示例显示了 SVM vs1 的所有安全设置：

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                           Is Signing Required:       false
               Is Password Complexity Required:       true
         Use start_tls For AD LDAP connection:        false
                     Is AES Encryption Enabled:       false
                        LM Compatibility Level:       lm-ntlm-ntlmv2-krb
                    Is SMB Encryption Required:       false
                       Client Session Security:       none
               SMB1 Enabled for DC Connections:       false
               SMB2 Enabled for DC Connections:       system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

请注意，显示的设置取决于正在运行的 ONTAP 版本。

以下示例显示了 SVM vs1 的 Kerberos 时钟偏差：

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

相关信息

显示有关 GPO 配置的信息

为本地 SMB 用户启用或禁用所需的密码复杂度

所需的密码复杂性可增强 Storage Virtual Machine （SVM）上本地 SMB 用户的安全性。默认情况下，所需的密码复杂度功能处于启用状态。您可以随时将其禁用并重新启用。

开始之前

必须在 CIFS 服务器上启用本地用户，本地组和本地用户身份验证。

关于此任务

您不能使用 `vserver cifs security modify` 命令、因为某些选项无效。

步骤

1. 执行以下操作之一：

本地 **SMB** 用户所需的密码复杂度	输入命令 ...
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. 验证所需密码复杂度的安全设置： `vserver cifs security show -vserver` *`vserver_name`*

示例

以下示例显示为 SVM vs1 的本地 SMB 用户启用了所需的密码复杂度：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

相关信息

显示有关 CIFS 服务器安全设置的信息

使用本地用户和组进行身份验证和授权

本地用户密码的要求

更改本地用户帐户密码

修改 **CIFS** 服务器 **Kerberos** 安全设置

您可以修改某些 CIFS 服务器 Kerberos 安全设置，包括允许的最大 Kerberos 时钟偏差时间， Kerberos 票证生命周期以及票证续订天数。

关于此任务

使用修改CIFS服务器Kerberos设置 `vserver cifs security modify` 命令仅会修改您使用指定的单

个Storage Virtual Machine (SVM)上的设置 `-vserver` 参数。您可以使用 Active Directory 组策略对象（ GPO ）集中管理属于同一 Active Directory 域的集群上所有 SVM 的 Kerberos 安全设置。

步骤

1. 执行以下一项或多项操作：

如果您要 …	输入 …
指定允许的最大Kerberos时钟偏差时间(以分钟(9.13.1及更高版本)或秒(9.12.1或更低版本)为单位。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* 默认设置为 5 分钟。
以小时为单位指定 Kerberos 票证的生命周期。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` 默认设置为 10 小时。
指定最大票证续订天数。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* 默认设置为 7 天。
指定 KDC 上的套接字超时，超过此超时后，所有 KDC 都将标记为不可访问。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* 默认设置为 3 秒。

2. 验证 Kerberos 安全设置：

   `vserver cifs security show -vserver` *`vserver_name`*

示例

以下示例对 Kerberos 安全性进行了以下更改：对于 SVM vs1 ， "`Kerberos Clock Skew` " 设置为 3 分钟，"`Kerberos 票证期限` " 设置为 8 小时：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                     Kerberos Clock Skew:                    3 minutes
                     Kerberos Ticket Age:                    8 hours
                    Kerberos Renewal Age:                    7 days
                    Kerberos KDC Timeout:                    3 seconds
                     Is Signing Required:                false
        Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
               Is AES Encryption Enabled:               false
                  LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                false
```

相关信息

"显示有关 CIFS 服务器安全设置的信息"

"支持的 GPO"

"将组策略对象应用于 CIFS 服务器"

设置**SMB**服务器最低身份验证安全级别

您可以在 SMB 服务器上设置 SMB 服务器的最低安全级别，也称为 *LMCompatibilityLevel* ，以满足 SMB 客户端访问的业务安全要求。最低安全级别是SMB服务器从SMB客户端接受的最低安全令牌级别。

关于此任务

- 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。
- LMCompatibilityLevel 仅适用于 SMB 客户端身份验证，而不适用于管理员身份验证。

您可以将最低身份验证安全级别设置为四个受支持的安全级别之一。

价值	**Description**
`lm-ntlm-ntlmv2-krb` (默认)	Storage Virtual Machine （ SVM ）接受 LM ， NTLM ， NTLMv2 和 Kerberos 身份验证安全性。
`ntlm-ntlmv2-krb`	SVM 接受 NTLM ， NTLMv2 和 Kerberos 身份验证安全性。SVM 拒绝 LM 身份验证。

价值	Description
`ntlmv2-krb`	SVM 接受 NTLMv2 和 Kerberos 身份验证安全性。SVM 拒绝 LM 和 NTLM 身份验证。
`krb`	SVM 仅接受 Kerberos 身份验证安全性。SVM 拒绝 LM ， NTLM 和 NTLMv2 身份验证。

步骤

1. 设置最低身份验证安全级别： `vserver cifs security modify -vserver vserver_name -lm -compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 验证身份验证安全级别是否设置为所需级别： `vserver cifs security show -vserver vserver_name`

相关信息

为基于 Kerberos 的通信启用或禁用 AES 加密

使用 AES 加密为基于 Kerberos 的通信配置强大的安全性

为了通过基于 Kerberos 的通信实现最强的安全性，您可以在 SMB 服务器上启用 AES-256 和 AES-128 加密。默认情况下、在SVM上创建SMB服务器时、高级加密标准(Advanced Encryption Standard、AES)加密处于禁用状态。您必须启用它才能利用AES加密提供的强大安全性。

在 SVM 上创建 SMB 服务器期间以及 SMB 会话设置阶段期间，会使用 SMB 的 Kerberos 相关通信。SMB 服务器支持以下 Kerberos 通信加密类型：

- AES 256
- AES 128
- DES
- RC4-HMAC

如果要对 Kerberos 通信使用最高安全加密类型，则应在 SVM 上为 Kerberos 通信启用 AES 加密。

创建 SMB 服务器时，域控制器会在 Active Directory 中创建计算机帐户。此时， KDC 将了解特定计算机帐户的加密功能。随后，系统会选择一种特定的加密类型来加密客户端在身份验证期间向服务器提供的服务单。

从ONTAP 9.12.1开始、您可以指定要向Active Directory (AD) KDC公布的加密类型。您可以使用 `-advertised-enc-types` 选项以启用建议的加密类型、您可以使用此选项禁用较弱的加密类型。了解操作方法 "为基于Kerberos的通信启用和禁用加密类型"。

> SMB 3.0 提供了 Intel AES 新指令（ Intel AES NI ），可改进 AES 算法并加快受支持处理器系列的数据加密速度。从 SMB 3.1.1 开始， AES-128-GCM 将 AES-128-CCM 替换为 SMB 加密使用的哈希算法。

相关信息

修改 CIFS 服务器 Kerberos 安全设置

要利用基于Kerberos的通信的最强安全性、您应在SMB服务器上使用AES-256和AES-128加密。从ONTAP 9.131开始、默认情况下会启用AES加密。 如果不希望SMB服务器为与Active Directory (AD) KDC进行基于Kerberos的通信选择AES加密类型、则可以禁用AES加密。

默认情况下是否启用AES加密以及是否可以指定加密类型取决于您的ONTAP版本。

ONTAP 版本	**AES**加密已启用…	是否可以指定加密类型?
9.13.1及更高版本	默认情况下。	是的。
9.12.1.	手动	是的。
9.11.1及更早版本	手动	否

从ONTAP 9.12.1开始、使用启用和禁用AES加密 `-advertised-enc-types` 选项、用于指定向AD KDC公布的加密类型。默认设置为 `rc4` 和 `des`、但如果指定了AES类型、则会启用AES加密。您还可以使用选项显式禁用较弱的RC4和DES加密类型。在ONTAP 9.11.1及更早版本中、必须使用 `-is-aes-encryption-enabled` 用于启用和禁用AES加密的选项、并且无法指定加密类型。

为了增强安全性， Storage Virtual Machine （ SVM ）会在每次修改 AES 安全选项时更改 AD 中的计算机帐户密码。更改密码可能需要包含计算机帐户的组织单位（ OU ）的管理 AD 凭据。

如果将SVM配置为不保留身份的灾难恢复目标(`-identity-preserve` 选项设置为 `false` 在SnapMirror配置中)、非默认SMB服务器安全设置不会复制到目标。如果已在源SVM上启用AES加密、则必须手动启用它。

示例 **1.** 步骤

ONTAP 9.12.1及更高版本

1. 执行以下操作之一：

Kerberos 通信的 **AES** 加密类型	输入命令 **...**
enabled	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
已禁用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   注意： `-is-aes-encryption-enabled` 选项在ONTAP 9.12.1中已弃用、可能会在更高版本中删除。

2. 验证是否已根据需要启用或禁用AES加密： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

示例

以下示例将为SVM vs1上的SMB服务器启用AES加密类型：

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

以下示例为SVM VS2上的SMB服务器启用AES加密类型。系统会提示管理员输入包含SMB服务器的OU的管理AD凭据。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1及更早版本

1. 执行以下操作之一：

Kerberos 通信的 **AES** 加密类型	输入命令 **...**
enabled	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
已禁用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. 验证是否已根据需要启用或禁用AES加密： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   - `is-aes-encryption-enabled` 字段 `true` 如果启用了AES加密、则为和 `false` 如果已禁用。

示例

以下示例将为SVM vs1上的SMB服务器启用AES加密类型：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- --------------------------
vs1      true
```

以下示例为SVM VS2上的SMB服务器启用AES加密类型。系统会提示管理员输入包含SMB服务器的OU的管理AD凭据。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- --------------------------
vs2      true
```

使用 **SMB** 签名增强网络安全性

使用 **SMB** 签名增强网络安全概述

SMB 签名有助于确保 SMB 服务器和客户端之间的网络流量不会受到影响；它可以通过防止重放攻击来实现这一点。默认情况下，当客户端请求 SMB 签名时， ONTAP 支持 SMB 签名。或者，存储管理员可以将 SMB 服务器配置为需要 SMB 签名。

SMB 签名策略如何影响与 **CIFS** 服务器的通信

除了 CIFS 服务器 SMB 签名安全设置之外， Windows 客户端上的两个 SMB 签名策略还控制客户端与 CIFS 服务器之间通信的数字签名。您可以配置满足业务要求的设置。

客户端 SMB 策略通过 Windows 本地安全策略设置进行控制，这些设置通过使用 Microsoft 管理控制台（MMC）或 Active Directory GPO 进行配置。有关客户端 SMB 签名和安全问题的详细信息，请参见 Microsoft Windows 文档。

下面介绍了 Microsoft 客户端上的两个 SMB 签名策略：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  此设置控制是否启用客户端的 SMB 签名功能。默认情况下，此选项处于启用状态。如果在客户端上禁用此设置，则客户端与 CIFS 服务器的通信取决于 CIFS 服务器上的 SMB 签名设置。

- `Microsoft network client: Digitally sign communications (always)`

  此设置控制客户端是否需要 SMB 签名才能与服务器进行通信。默认情况下，此选项处于禁用状态。如果在客户端上禁用此设置、则SMB签名行为取决于的策略设置 `Microsoft network client: Digitally sign communications (if server agrees)` 和CIFS服务器上的设置。

> 如果您的环境包含配置为需要 SMB 签名的 Windows 客户端，则必须在 CIFS 服务器上启用 SMB 签名。否则， CIFS 服务器将无法为这些系统提供数据。

客户端和 CIFS 服务器 SMB 签名设置的有效结果取决于 SMB 会话是使用 SMB 1.0 还是 SMB 2.x 及更高版本。

下表总结了会话使用 SMB 1.0 时有效的 SMB 签名行为：

客户端	不需要 **ONTAP** 签名	需要 **ONTAP** 签名
已禁用且不需要签名	未签名	已签名
已启用签名，但不需要签名	未签名	已签名
签名已禁用且为必填项	已签名	已签名
已启用且需要签名	已签名	已签名

> 如果在客户端上禁用了签名，但在 CIFS 服务器上需要签名，则较早的 Windows SMB 1 客户端和某些非 Windows SMB 1 客户端可能无法连接。

下表总结了会话使用 SMB 2.x 或 SMB 3.0 时有效的 SMB 签名行为：

> 对于 SMB 2.x 和 SMB 3.0 客户端， SMB 签名始终处于启用状态。不能将其禁用。

客户端	不需要 **ONTAP** 签名	需要 **ONTAP** 签名
不需要签名	未签名	已签名
需要签名	已签名	已签名

下表总结了默认的 Microsoft 客户端和服务器 SMB 签名行为：

协议	哈希算法	可以启用 / 禁用	可能需要 / 不需要	客户端默认值	服务器默认值	**DC** 默认值
SMB 1.0	MD5	是的。	是的。	已启用（不需要）	已禁用（不需要）	Required
SMB 2.x	HMAC SHA-256	否	是的。	不需要	不需要	Required
SMB 3.0	AES-CMAC 。	否	是的。	不需要	不需要	Required

> Microsoft不再建议使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 组策略设置。Microsoft也不再建议使用 `EnableSecuritySignature` 注册表设置。这些选项仅影响SMB 1行为、可以替换为 `Digitally sign communications (always)` 组策略设置或 `RequireSecuritySignature` 注册表设置。您还可以从Microsoft博客中获取更多信息。http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The签名基础知识(涵盖SMB1和SMB2)]

SMB 签名的性能影响

当 SMB 会话使用 SMB 签名时，与 Windows 客户端之间的所有 SMB 通信都会受到性能影响，从而影响客户端和服务器（即运行包含 SMB 服务器的 SVM 的集群上的节点）。

性能影响显示为客户端和服务器上的 CPU 利用率增加，但网络流量不会改变。

性能影响的程度取决于所运行的 ONTAP 9 版本。从 ONTAP 9.7 开始，新的非负载加密算法可以提高签名 SMB 流量的性能。如果启用了 SMB 签名，则默认情况下会启用 SMB 签名卸载。

要提高 SMB 签名性能，需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 AES-NI 卸载。

如果您能够使用SMB版本3.11、该版本支持更快的GCM算法、则性能也可能进一步提高。

根据您的网络， ONTAP 9 版本， SMB 版本和 SVM 实施情况， SMB 签名对性能的影响可能差别很大；您只能通过在网络环境中进行测试来验证它。

如果在服务器上启用了 SMB 签名，则大多数 Windows 客户端默认协商 SMB 签名。如果您需要为某些 Windows 客户端提供 SMB 保护，并且 SMB 签名导致性能问题，则可以在任何不需要防止重放攻击的 Windows 客户端上禁用 SMB 签名。有关在 Windows 客户端上禁用 SMB 签名的信息，请参见 Microsoft Windows 文档。

配置 **SMB** 签名的建议

您可以在 SMB 客户端和 CIFS 服务器之间配置 SMB 签名行为，以满足您的安全要求。在 CIFS 服务器上配置 SMB 签名时选择的设置取决于您的安全要求。

您可以在客户端或 CIFS 服务器上配置 SMB 签名。配置 SMB 签名时，请考虑以下建议：

条件	建议
您希望提高客户端与服务器之间通信的安全性	通过启用、在客户端上设置所需的SMB签名 `Require Option (Sign always)` 客户端上的安全设置。
您希望对特定 Storage Virtual Machine （ SVM ）的所有 SMB 流量进行签名	通过将安全设置配置为需要 SMB 签名，在 CIFS 服务器上设置需要 SMB 签名。

有关配置 Windows 客户端安全设置的详细信息，请参见 Microsoft 文档。

配置多个数据 **LIF** 时的 **SMB** 签名准则

如果在 SMB 服务器上启用或禁用所需的 SMB 签名，则应了解 SVM 的多个数据 LIF 配置的准则。

配置 SMB 服务器时，可能会配置多个数据 LIF 。如果是、则DNS服务器包含多个 `A` 记录CIFS服务器的条目、所有条目都使用相同的SMB服务器主机名、但每个条目都具有唯一的IP地址。例如、配置了两个数据生命周期的SMB服务器可能具有以下DNS `A` 记录条目：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

正常情况下，更改所需的 SMB 签名设置后，只有来自客户端的新连接才会受到 SMB 签名设置更改的影响。但是，此行为存在例外情况。在某些情况下，客户端已与共享建立连接，并且客户端会在更改此设置后创建与同一共享的新连接，同时保持原始连接。在这种情况下，新的和现有的 SMB 连接都采用新的 SMB 签名要求。

请考虑以下示例：

1. 客户端1使用路径连接到共享、而不需要SMB签名 `O:\`。
2. 存储管理员将 SMB 服务器配置修改为需要 SMB 签名。
3. 客户端1使用路径连接到具有所需SMB签名的同一共享 `S:\` (同时使用路径保持连接 `O:\`）。
4. 这样、在通过这两个访问数据时、将使用SMB签名 `O:\` 和 `S:\` 驱动器。

为传入的 **SMB** 流量启用或禁用所需的 **SMB** 签名

您可以通过启用所需的 SMB 签名来强制实施客户端对 SMB 消息签名的要求。如果启用，则 ONTAP 仅在 SMB 消息具有有效签名时才接受这些消息。如果要允许 SMB 签名，但不需要它，可以禁用所需的 SMB 签名。

关于此任务

默认情况下，所需的 SMB 签名处于禁用状态。您可以随时启用或禁用所需的 SMB 签名。

在以下情况下，默认情况下不会禁用 SMB 签名：

1. 已启用所需的 SMB 签名，并且集群将还原到不支持 SMB 签名的 ONTAP 版本。
2. 集群随后升级到支持 SMB 签名的 ONTAP 版本。

   在这些情况下，最初在受支持的 ONTAP 版本上配置的 SMB 签名配置将通过还原和后续升级保留。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、是为选择的值 `-identity-preserve` 的选项 `snapmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则SMB签名安全设置将复制到目标。

如果您设置了 `-identity-preserve` 选项 `false` (非ID保留)、则SMB签名安全设置不会复制到目标。在这种情况下，目标上的 CIFS 服务器安全设置将设置为默认值。如果已在源 SVM 上启用所需的 SMB 签名，则必须在目标 SVM 上手动启用所需的 SMB 签名。

步骤

1. 执行以下操作之一：

所需的 **SMB** 签名状态	输入命令 **...**
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 通过确定中的值来验证是否已启用或禁用所需的SMB签名 `Is Signing Required` 字段设置为所需值：
   `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

示例

以下示例将为 SVM vs1 启用所需的 SMB 签名：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

对加密设置所做的更改将对新连接生效。现有连接不受影响。

确定 **SMB** 会话是否已签名

您可以显示有关 CIFS 服务器上已连接的 SMB 会话的信息。您可以使用此信息确定 SMB 会话是否已签名。这有助于确定 SMB 客户端会话是否使用所需的安全设置进行连接。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
指定 Storage Virtual Machine （ SVM ）上的所有已签名会话	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
SVM 上具有特定会话 ID 的已签名会话的详细信息	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

示例

以下命令显示 SVM vs1 上已签名会话的会话信息。默认摘要输出不会显示 "`Is Session Signed` " 输出字段：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                      Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279  1       10.1.1.1         DOMAIN\joe          2          23s
```

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括会话是否已签名：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                  Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                 Windows User: DOMAIN\joe
                    UNIX User: pcuser
                  Open Shares: 1
                   Open Files: 1
                   Open Other: 0
               Connected Time: 10m 43s
                    Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

相关信息

监控 SMB 签名会话统计信息

监控 **SMB** 签名会话统计信息

您可以监控 SMB 会话统计信息，并确定哪些已建立的会话已签名，哪些未签名。

关于此任务

。 `statistics` 命令可在高级权限级别提供 `signed_sessions` 可用于监控已签名SMB会话数的计数器。。 `signed_sessions` 计数器可用于以下统计信息对象：

- `cifs` 用于监控所有SMB会话的SMB签名。
- `smb1` 用于监控SMB 1.0会话的SMB签名。
- `smb2` 用于监控SMB 2.x和SMB 3.0会话的SMB签名。

  SMB 3.0统计信息包括在的输出中 `smb2` 对象。

如果要将已签名会话数与会话总数进行比较、可以比较的输出 `signed_sessions` 计数器与的输出 `established_sessions` 计数器。

您必须先启动统计信息样本收集，然后才能查看生成的数据。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定趋势。

步骤

1. 将权限级别设置为高级：+
   `set -privilege advanced`
2. 开始数据收集：+
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果未指定 `-sample-id` 参数时、该命令将为您生成示例标识符、并将此示例定义为命令行界面会话的默认示例。的值 `-sample-id` 是文本字符串。如果您在同一命令行界面会话期间运行此命令、但未指定 `-sample-id` 参数、则此命令将覆盖先前的默认样本。

   您也可以指定要收集统计信息的节点。如果未指定节点，则此示例将收集集群中所有节点的统计信息。
3. 使用 `statistics stop` 命令停止收集样本数据。
4. 查看 SMB 签名统计信息：

要查看的信息	输入 ...
已签名的会话	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	已签名的会话和已建立的会话
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   如果要仅显示单个节点的信息、请指定可选 `-node` 参数。
5. 返回到管理权限级别：+
   `set -privilege admin`

示例

以下示例显示了如何监控 Storage Virtual Machine （ SVM ） vs1 上的 SMB 2.x 和 SMB 3.0 签名统计信息。

以下命令将移至高级权限级别：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

以下命令将开始收集新样本的数据：

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

以下命令将停止收集样本的数据：

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

以下命令按示例中的节点显示已签名的 SMB 会话和已建立的 SMB 会话：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

以下命令显示样本中 node2 的已签名 SMB 会话：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- -------------------------
    node_name                                                node2
    signed_sessions                                              1
```

以下命令将移回管理权限级别：

```
cluster1::*> set -privilege admin
```

相关信息

确定 SMB 会话是否已签名

"性能监控和管理概述"

在 **SMB** 服务器上配置通过 **SMB** 传输数据所需的 **SMB** 加密

SMB加密概述

通过 SMB 进行数据传输的 SMB 加密是一种安全增强功能，您可以在 SMB 服务器上启用或禁用此功能。您还可以通过共享属性设置在共享基础上配置所需的 SMB 加密设置。

默认情况下、在Storage Virtual Machine (SVM)上创建SMB服务器时、SMB加密处于禁用状态。您必须启用 SMB 加密才能利用 SMB 加密提供的增强安全性。

要创建加密的 SMB 会话， SMB 客户端必须支持 SMB 加密。从 Windows Server 2012 和 Windows 8 开始的 Windows 客户端支持 SMB 加密。

SVM 上的 SMB 加密通过两种设置控制：

- 在SVM上启用此功能的SMB服务器安全选项
- 一种SMB共享属性、用于基于共享配置SMB加密设置

您可以决定是要求加密才能访问 SVM 上的所有数据，还是要求 SMB 加密才能仅访问选定共享中的数据。SVM 级别的设置将取代共享级别的设置。

有效的 SMB 加密配置取决于这两种设置的组合，下表对此进行了介绍：

已启用 **SMB** 服务器 **SMB** 加密	已启用共享加密数据设置	服务器端加密行为
true	false	已为 SVM 中的所有共享启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
true	true	无论共享级别加密如何， SVM 中的所有共享都会启用服务器级别加密。使用此配置时，整个 SMB 会话都会进行加密。
false	true	已为特定共享启用共享级别加密。使用此配置时，会从树连接进行加密。
false	false	未启用加密。

不支持加密的SMB客户端无法连接到需要加密的SMB服务器或共享。

对加密设置所做的更改将对新连接生效。现有连接不受影响。

SMB 加密对性能的影响

当 SMB 会话使用 SMB 加密时，与 Windows 客户端之间的所有 SMB 通信都会受到性能影响，从而影响客户端和服务器（即运行包含 SMB 服务器的 SVM 的集群上的节点）。

性能影响显示为客户端和服务器上的 CPU 利用率增加，但网络流量不会改变。

性能影响的程度取决于所运行的 ONTAP 9 版本。从 ONTAP 9.7 开始，新的加密负载下算法可以提高加密 SMB 流量的性能。如果启用了 SMB 加密，则默认情况下会启用 SMB 加密卸载。

增强的 SMB 加密性能需要 AES-NI 卸载功能。请参见 Hardware Universe （ HWU ）以验证您的平台是否支持 AES-NI 卸载。

如果您能够使用SMB版本3.11、该版本支持更快的GCM算法、则性能也可能进一步提高。

根据您的网络， ONTAP 9 版本， SMB 版本和 SVM 实施情况， SMB 加密对性能的影响可能差别很大；您只能通过在网络环境中进行测试来验证它。

SMB 服务器默认禁用 SMB 加密。您应仅在需要加密的 SMB 共享或 SMB 服务器上启用 SMB 加密。通过 SMB 加密， ONTAP 可以对请求进行解密，并对每个请求的响应进行加密。因此，只有在必要时才应启用 SMB 加密。

为传入的 **SMB** 流量启用或禁用所需的 **SMB** 加密

如果您希望为传入的 SMB 流量要求 SMB 加密，可以在 CIFS 服务器或共享级别启用它。默认情况下，不需要 SMB 加密。

关于此任务

您可以在 CIFS 服务器上启用 SMB 加密，该服务器会对 CIFS 服务器上的所有共享进行适用场景。如果您不希望 CIFS 服务器上的所有共享都需要 SMB 加密，或者您希望为基于共享的传入 SMB 流量启用所需的 SMB 加密，则可以在 CIFS 服务器上禁用所需的 SMB 加密。

在设置Storage Virtual Machine (SVM)灾难恢复关系时、您为选择的值 `-identity-preserve` 的选项 `snapmirror create` 命令用于确定复制到目标SVM中的配置详细信息。

如果您设置了 `-identity-preserve` 选项 `true` (ID保留)、则SMB加密安全设置将复制到目标。

如果您设置了 `-identity-preserve` 选项 `false` (非ID保留)、则SMB加密安全设置不会复制到目标。在这种情况下，目标上的 CIFS 服务器安全设置将设置为默认值。如果已在源 SVM 上启用 SMB 加密，则必须在目标上手动启用 CIFS 服务器 SMB 加密。

步骤

1. 执行以下操作之一：

CIFS 服务器上传入的 **SMB** 流量所需的 **SMB** 加密	输入命令 **...**
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`

CIFS 服务器上传入的 SMB 流量所需的 SMB 加密	输入命令 ...
已禁用	`vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false`

2. 验证是否已根据需要在CIFS服务器上启用或禁用所需的SMB加密： `vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 字段 `true` 如果需要、可在CIFS服务器和上启用SMB加密 `false` 如果已禁用。

示例

以下示例将为 SVM vs1 上的 CIFS 服务器的传入 SMB 流量启用所需的 SMB 加密：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

确定客户端是否使用加密的 **SMB** 会话进行连接

您可以显示有关已连接 SMB 会话的信息，以确定客户端是否正在使用加密的 SMB 连接。这有助于确定 SMB 客户端会话是否使用所需的安全设置进行连接。

关于此任务

SMB 客户端会话可以具有以下三种加密级别之一：

- `unencrypted`

  SMB 会话未加密。未配置 Storage Virtual Machine （ SVM ）级别或共享级别的加密。

- `partially-encrypted`

  发生树连接时会启动加密。已配置共享级别加密。未启用 SVM 级别的加密。

- `encrypted`

  SMB 会话已完全加密。已启用 SVM 级别的加密。可能已启用，也可能未启用共享级别加密。SVM 级别的加密设置将取代共享级别的加密设置。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
具有指定 SVM 上会话的指定加密设置的会话	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定 SVM 上特定会话 ID 的加密设置	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

示例

以下命令显示会话 ID 为 2 的 SMB 会话的详细会话信息，包括加密设置：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

监控 **SMB** 加密统计信息

您可以监控 SMB 加密统计信息，并确定哪些已建立的会话和共享连接已加密，哪些未加密。

关于此任务

。 `statistics` 高级权限级别的命令提供了以下计数器、您可以使用这些计数器监控加密的SMB会话和共享连接的数量：

计数器名称	说明
encrypted_sessions	提供加密的 SMB 3.0 会话的数量
encrypted_share_connections	提供发生树连接的加密共享的数量
rejected_unencrypted_sessions	提供因缺少客户端加密功能而拒绝的会话设置数量
rejected_unencrypted_shares	提供因缺少客户端加密功能而拒绝的共享映射的数量

这些计数器可用于以下统计信息对象：

- `cifs` 用于监控所有SMB 3.0会话的SMB加密。

  SMB 3.0统计信息包括在的输出中 `cifs` 对象。 如果要将加密会话数与会话总数进行比较、可以比较的输出 `encrypted_sessions` 计数器与的输出 `established_sessions` 计数器。

  如果要将加密共享连接数与共享连接总数进行比较、则可以比较的输出 `encrypted_share_connections` 计数器与的输出 `connected_shares` 计数器。

- `rejected_unencrypted_sessions` 提供尝试建立需要从不支持SMB加密的客户端加密的SMB会话的次数。
- `rejected_unencrypted_shares` 提供尝试连接到需要从不支持SMB加密的客户端加密的SMB共享的次数。

您必须先启动统计信息样本收集，然后才能查看生成的数据。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定趋势。

步骤

1. 将权限级别设置为高级：+
   `set -privilege advanced`
2. 开始数据收集：+
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果未指定 `-sample-id` 参数时、该命令将为您生成示例标识符、并将此示例定义为命令行界面会话的默认示例。的值 `-sample-id` 是文本字符串。如果您在同一命令行界面会话期间运行此命令、但未指定 `-sample-id` 参数、则此命令将覆盖先前的默认样本。

   您也可以指定要收集统计信息的节点。如果未指定节点，则此示例将收集集群中所有节点的统计信息。

3. 使用 `statistics stop` 命令停止收集样本数据。
4. 查看 SMB 加密统计信息：

要查看的信息	输入 ...
加密会话	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	已加密会话和已建立的会话
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共享连接
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共享连接和连接的共享	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒绝的未加密会话	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒绝未加密的共享连接
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

如果要仅显示单个节点的信息、请指定可选 `-node` 参数。

5. 返回到管理权限级别：+
   `set -privilege admin`

示例

以下示例显示了如何监控 Storage Virtual Machine （ SVM ） vs1 上的 SMB 3.0 加密统计信息。

以下命令将移至高级权限级别：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

以下命令将开始收集新样本的数据：

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

以下命令将停止收集该样本的数据：

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

以下命令显示样本中节点的加密 SMB 会话和已建立的 SMB 会话：

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                Value
    ----------------------------  -----------------------
    established_sessions                      1
    encrypted_sessions                        1

2 entries were displayed
```

以下命令显示样本中节点拒绝的未加密 SMB 会话的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

以下命令显示样本中节点的已连接 SMB 共享和加密 SMB 共享的数量：

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                      Value
    ----------------------------    ----------------------
    connected_shares                               2
    encrypted_share_connections                    1

2 entries were displayed.
```

以下命令显示样本中节点拒绝的未加密 SMB 共享连接的数量：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

相关信息

确定可用的统计信息对象和计数器

"性能监控和管理概述"

安全 **LDAP** 会话通信

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （AD）服务器的查询启用 LDAP 会话安全性。您必须在 Storage Virtual Machine （SVM）上配置 CIFS 服务器安全设置，使其与 LDAP 服务器上的设置相对应。

签名可使用密钥技术确认 LDAP 有效负载数据的完整性。密封功能对 LDAP 有效负载数据进行加密，以避免以明文形式传输敏感信息。"_LDAP 安全级别 _" 选项指示 LDAP 流量是需要签名，签名和签章，还是两者都不需要。默认值为 `none`。

已使用在SVM上启用CIFS流量的LDAP签名和签章 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

在 **CIFS** 服务器上启用 **LDAP** 签名和签章

在 CIFS 服务器使用签名和签章与 Active Directory LDAP 服务器进行安全通信之前，您必须修改 CIFS 服务器安全设置以启用 LDAP 签名和签章。

开始之前

您必须咨询 AD 服务器管理员以确定适当的安全配置值。

步骤

1. 配置CIFS服务器安全设置、以启用与Active Directory LDAP服务器之间的已签名和已密封流量： `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap`

`{none|sign|seal}`

您可以启用签名 (`sign`、数据完整性)、签名和签章 (`seal``数据完整性和加密)、或者两者都不是 `none`，无签名或签章)。默认值为 `none`。

2. 验证是否已正确设置LDAP签名和签章安全设置： `vserver cifs security show -vserver` *`vserver_name`*

> 如果SVM使用同一个LDAP服务器查询名称映射或其他UNIX信息(例如用户、组和网络组)、则必须使用启用相应的设置 `-session-security` 的选项 `vserver services name-service ldap client modify` 命令：

配置基于 **TLS** 的 **LDAP**

导出自签名根 **CA** 证书的副本

要使用基于 SSL/TLS 的 LDAP 确保 Active Directory 通信安全，必须先将 Active Directory 证书服务的自签名根 CA 证书副本导出到证书文件，然后将其转换为 ASCII 文本文件。ONTAP 使用此文本文件在 Storage Virtual Machine （ SVM ）上安装证书。

开始之前

必须已为 CIFS 服务器所属的域安装和配置 Active Directory 证书服务。有关安装和配置 Active Director 证书服务的信息，请参见 Microsoft TechNet 库。

"Microsoft TechNet 库： technet.microsoft.com"

步骤

1. 获取中域控制器的根CA证书 `.pem` 文本格式。

   "Microsoft TechNet 库： technet.microsoft.com"

完成后

在 SVM 上安装证书。

相关信息

"Microsoft TechNet 库"

在 **SVM** 上安装自签名根 **CA** 证书

如果在绑定到 LDAP 服务器时需要使用 TLS 进行 LDAP 身份验证，则必须先在 SVM 上安装自签名根 CA 证书。

关于此任务

启用基于 TLS 的 LDAP 后， SVM 上的 ONTAP LDAP 客户端在 ONTAP 9.0 和 9.1 中不支持已撤销的证书。

从 ONTAP 9.2 开始， ONTAP 中使用 TLS 通信的所有应用程序都可以使用联机证书状态协议（ Online Certificate Status Protocol ， OCSP ）检查数字证书状态。如果为基于 TLS 的 LDAP 启用了 OCSP ，则已撤销的证书将被拒绝，并且连接将失败。

步骤

1. 安装自签名根 CA 证书：
   a. 开始安装证书： `security certificate install -vserver vserver_name -type server-ca`

      控制台输出将显示以下消息： `Please enter Certificate: Press <Enter> when done`

   b. 打开证书 `.pem` 文件，使用文本编辑器复制证书，包括以开头的行 `-----BEGIN CERTIFICATE-----` 并以结尾 `-----END CERTIFICATE-----`，然后在命令提示符后粘贴证书。
   c. 验证证书是否显示正确。
   d. 按 Enter 键完成安装。
2. 验证是否已安装此证书： `security certificate show -vserver *vserver_name*`

在服务器上启用基于 **TLS** 的 **LDAP**

在SMB服务器使用TLS与Active Directory LDAP服务器进行安全通信之前、您必须修改SMB服务器安全设置以启用基于TLS的LDAP。

从 ONTAP 9.10.1 开始，默认情况下， Active Directory （AD）和名称服务 LDAP 连接均支持 LDAP 通道绑定。只有在启用了 Start-TLS 或 LDAPS 且会话安全设置为 sign 或 seal 的情况下， ONTAP 才会尝试使用 LDAP 连接进行通道绑定。要禁用或重新启用与AD服务器的LDAP通道绑定、请使用 `-try-channel-binding-for-ad-ldap` 参数 `vserver cifs security modify` 命令：

要了解更多信息、请参见：

- "LDAP概述"
- "2020 年 Windows 的 LDAP 通道绑定和 LDAP 签名要求"。

步骤

1. 配置SMB服务器安全设置、以允许与Active Directory LDAP服务器进行安全LDAP通信： `vserver cifs security modify -vserver *vserver_name* -use-start-tls-for-ad-ldap true`
2. 验证基于TLS的LDAP安全设置是否设置为 `true`： `vserver cifs security show -vserver *vserver_name*`

> 如果SVM使用同一个LDAP服务器来查询名称映射或其他UNIX信息(例如用户、组和网络组)、则还必须修改 `-use-start-tls` 选项 `vserver services name-service ldap client modify` 命令：

为 **SMB** 多通道配置性能和冗余

从 ONTAP 9.4 开始，您可以配置 SMB 多通道，以便在单个 SMB 会话中提供 ONTAP 与客户端之间的多个连接。这样可以提高吞吐量和容错能力。

开始之前

只有在客户端以 SMB 3.0 或更高版本进行协商时，才能使用 SMB 多通道功能。默认情况下， ONTAP SMB 服务器上会启用 SMB 3.0 及更高版本。

关于此任务

如果在 ONTAP 集群上确定了正确的配置，则 SMB 客户端会自动检测并使用多个网络连接。

SMB 会话中同时连接的数量取决于您部署的 NIC：

- 客户端和 ONTAP 集群上的 * 1G NIC *

  客户端为每个 NIC 建立一个连接，并将会话绑定到所有连接。

- 客户端和 ONTAP 集群上的 * 10 G 及更大容量 NIC *

  客户端为每个 NIC 最多建立四个连接，并将会话绑定到所有连接。客户端可以在多个 10G 及更大容量的 NIC 上建立连接。

您还可以修改以下参数（高级权限）：

- **`-max-connections-per-session`**

  每个多通道会话允许的最大连接数。默认值为 32 个连接。

  如果要启用比默认连接更多的连接，则必须对客户端配置进行类似的调整，该配置的默认连接数也为 32 个。

- **`-max-lifs-per-session`**

  每个多通道会话公布的最大网络接口数。默认值为 256 个网络接口。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 在 SMB 服务器上启用 SMB 多通道： `vserver cifs options modify -vserver` *`vserver_name`* `-is-multichannel-enabled true`
3. 验证 ONTAP 是否正在报告 SMB 多通道会话： `vserver cifs session show` *`options`*
4. 返回到管理权限级别： `set -privilege admin`

示例

以下示例显示了有关所有 SMB 会话的信息，其中显示了单个会话的多个连接：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

以下示例显示了有关 session-id 为 1 的 SMB 会话的详细信息：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

在 **SMB** 服务器上配置默认 **Windows** 用户到 **UNIX** 用户映射

您可以配置默认 UNIX 用户，以便在用户的所有其他映射尝试均失败或不希望在 UNIX 和 Windows 之间映射单个用户时使用。或者，如果您希望对未映射用户的身份验证失败，则不应配置默认 UNIX 用户。

关于此任务

默认情况下，默认 UNIX 用户名称为 "`pcuser` "，这意味着默认情况下，系统会启用用户到默认 UNIX 用户的映射。您可以指定另一个名称以用作默认 UNIX 用户。您指定的名称必须存在于为 Storage Virtual Machine （ SVM ）配置的名称服务数据库中。如果此选项设置为空字符串，则任何人都无法以 UNIX 默认用户身份访问 CIFS 服务器。也就是说，每个用户都必须在密码数据库中有一个帐户，然后才能访问 CIFS 服务器。

要使用户使用默认 UNIX 用户帐户连接到 CIFS 服务器，该用户必须满足以下前提条件：

- 用户已通过身份验证。
- 用户位于 CIFS 服务器的本地 Windows 用户数据库， CIFS 服务器的主域或受信任域中（如果在 CIFS 服务器上启用了多域名称映射搜索）。
- 用户名未显式映射到空字符串。

步骤

1. 配置默认 UNIX 用户：

如果您要 ...	输入 ...
使用默认 UNIX 用户 "`pcuser` "	`vserver cifs options modify -default -unix-user pcuser`
使用另一个 UNIX 用户帐户作为默认用户	`vserver cifs options modify -default -unix-user` *`user_name`*
禁用默认 UNIX 用户	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. 验证是否已正确配置默认 UNIX 用户： `vserver cifs options show -vserver` *`vserver_name`*

   在以下示例中， SVM vs1 上的默认 UNIX 用户和子系统 UNIX 用户均配置为使用 UNIX 用户 "`pcuser` "：

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

配置子系统 **UNIX** 用户

配置子系统 UNIX 用户选项意味着，从不可信域登录的用户将映射到子系统 UNIX 用户，并可连接到 CIFS 服务器。或者，如果您希望对来自不可信域的用户进行身份验证失败，则不应配置子系统 UNIX 用户。默认情况下，不允许来自不可信域的用户连接到 CIFS 服务器（未配置来宾 UNIX 帐户）。

关于此任务

配置子系统 UNIX 帐户时，应记住以下几点：

- 如果 CIFS 服务器无法根据主域，受信任域或本地数据库的域控制器对用户进行身份验证，并且启用了此选项，则 CIFS 服务器会将该用户视为来宾用户，并将该用户映射到指定的 UNIX 用户。
- 如果此选项设置为空字符串，则会禁用子系统 UNIX 用户。
- 您必须创建一个 UNIX 用户，以用作其中一个 Storage Virtual Machine （ SVM ）名称服务数据库中的子系统 UNIX 用户。
- 以来宾用户身份登录的用户会自动成为 CIFS 服务器上 BUILTIN\guests 组的成员。
- "homedirs-public" 选项仅适用于经过身份验证的用户。以来宾用户身份登录的用户没有主目录，无法访问其他用户的主目录。

步骤

1. 执行以下操作之一：

如果您要 ...	输入 ...
配置子系统 UNIX 用户	`vserver cifs options modify -guest -unix-user` *`unix_name`*
禁用子系统 UNIX 用户	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. 验证是否已正确配置子系统UNIX用户： `vserver cifs options show -vserver` *`vserver_name`*

在以下示例中， SVM vs1 上的默认 UNIX 用户和子系统 UNIX 用户均配置为使用 UNIX 用户 "`pcuser` "：

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

将管理员组映射到 root

如果您的环境中只有 CIFS 客户端，并且您的 Storage Virtual Machine （ SVM ）设置为多协议存储系统，则必须至少有一个 Windows 帐户具有访问 SVM 上文件的 root 权限；否则，您将无法管理 SVM ，因为您没有足够的用户权限。

关于此任务

如果存储系统设置为仅限NTFS、则为 `/etc` 目录具有一个文件级ACL、可使管理员组访问ONTAP配置文件。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置 CIFS 服务器选项，以便根据需要将管理员组映射到 root ：

如果您要 ...	那么 ...
将管理员组成员映射到 root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` 即使您没有、管理员组中的所有帐户都将视为root用户 `/etc/usermap.cfg` 将帐户映射到root的条目。如果使用属于管理员组的帐户创建文件，则在从 UNIX 客户端查看文件时，该文件属于 root 用户。
禁用将管理员组成员映射到 root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` 管理员组中的帐户不再映射到root。您只能显式将单个用户映射到 root 。

3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

显示有关通过 **SMB** 会话连接的用户类型的信息

您可以显示有关通过 SMB 会话连接的用户类型的信息。这有助于确保只有适当类型的用户通过 Storage Virtual Machine （ SVM ）上的 SMB 会话进行连接。

关于此任务

以下类型的用户可以通过 SMB 会话进行连接：

- `local-user`

  以本地 CIFS 用户身份进行身份验证

- `domain-user`

  以域用户身份进行身份验证（从 CIFS 服务器的主域或受信任域）

- `guest-user`

  以来宾用户身份进行身份验证

- `anonymous-user`

  以匿名或空用户身份进行身份验证

步骤

1. 确定通过SMB会话连接的用户类型： `vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

要显示已建立会话的用户类型信息 ...	输入以下命令 ...
具有指定用户类型的所有会话	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	用于特定用户

示例

以下命令显示由用户 "` iepubs\user1` " 在 SVM vs1 上建立的会话的用户类型的会话信息：

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

用于限制 **Windows** 客户端资源过度消耗的命令选项

选项 `vserver cifs options modify` 命令用于控制Windows客户端的资源消耗。如果任何客户端超出资源消耗的正常范围，例如打开的文件，打开的会话或更改通知请求异常多，则此功能将非常有用。

的以下选项 `vserver cifs options modify` 添加了命令以控制Windows客户端资源消耗。如果超过其中任何一个选项的最大值，则请求将被拒绝并发送 EMS 消息。当达到这些选项的已配置限制的 80% 时，也会发送 EMS 警告消息。

- `-max-opens-same-file-per-tree`

  每个 CIFS 树中同一文件的最大打开数

- `-max-same-user-sessions-per-connection`

  同一用户在每个连接中打开的最大会话数

- `-max-same-tree-connect-per-session`

  每个会话同一共享上的最大树连接数

- `-max-watches-set-per-tree`

  为每个树建立的最大监视数（也称为 *change NOVES* ）

有关默认限制和显示当前配置的信息，请参见手册页。

从 ONTAP 9.4 开始，运行 SMB 版本 2 或更高版本的服务器可以限制客户端可通过 SMB 连接发送到服务器的未处理请求（ _SMB 信用值 _ ）的数量。SMB 信用的管理由客户端启动，并由服务器控制。

可在SMB连接上授予的最大未处理请求数由控制 `-max-credits` 选项此选项的默认值为 128 。

使用传统机会锁和租用机会锁提高客户端性能

通过传统机会锁和租用机会锁概述提高客户端性能

在某些文件共享情形下， SMB 客户端可以通过传统机会锁（机会锁）和租用机会锁对预读，后写和锁定信息执行客户端缓存。然后，客户端可以对文件进行读取或写入，而无需

定期提醒服务器它需要访问相关文件。这样可以通过减少网络流量来提高性能。

租用机会锁是 SMB 2.1 协议及更高版本提供的一种增强型机会锁。租用机会锁允许客户端在来自自身的多个 SMB 打开之间获取和保留客户端缓存状态。

可以通过两种方式控制机会锁：

- 通过共享属性使用 `vserver cifs share create` 命令(创建共享时)、或 `vserver share properties` 命令。
- 通过qtree属性、使用 `volume qtree create` 命令(创建qtree时)、或 `volume qtree oplock` 命令。

使用机会锁时的写入缓存数据丢失注意事项

在某些情况下，如果某个进程对某个文件具有独占机会锁，而另一个进程尝试打开该文件，则第一个进程必须使缓存的数据失效，并刷新写入和锁定。然后，客户端必须放弃机会锁并访问文件。如果在此刷新期间出现网络故障，缓存的写入数据可能会丢失。

- 数据丢失的可能性

  在以下情况下，任何具有写入缓存数据的应用程序都可能丢失该数据：

  - 此连接使用 SMB 1.0 建立。
  - 此文件具有独占机会锁。
  - 系统会指示中断该机会锁或关闭文件。
  - 在刷新写入缓存的过程中，网络或目标系统会生成错误。
- 处理和写入完成时出错

  缓存本身没有任何错误处理—应用程序确实如此。应用程序向缓存写入数据时，写入操作始终完成。如果缓存进而通过网络向目标系统写入数据，则必须假定写入已完成，因为如果不完成写入，则数据将丢失。

创建 **SMB** 共享时启用或禁用机会锁

机会锁允许客户端在本地锁定文件和缓存内容，从而提高文件操作的性能。在 Storage Virtual Machine （ SVM ）上的 SMB 共享上启用机会锁。在某些情况下，您可能需要禁用机会锁。您可以基于共享启用或禁用机会锁。

关于此任务

如果在包含共享的卷上启用了机会锁，但禁用了该共享的机会锁共享属性，则会为该共享禁用机会锁。在共享上禁用机会锁优先于卷机会锁设置。在共享上禁用机会锁会同时禁用机会锁和租用机会锁。

除了使用逗号分隔列表指定 oplock 共享属性之外，您还可以指定其他共享属性。您还可以指定其他共享参数。

步骤

1. 执行适用的操作：

如果您要 ...	那么 ...
在共享创建期间在共享上启用机会锁	输入以下命令：`vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share -properties [oplocks,...]` 如果您希望共享仅具有默认共享属性、即 `oplocks`，`browsable`，和 `changenotify` 启用后、您无需指定 `-share-properties` 参数。如果要使用默认值以外的任何共享属性组合、则必须指定 `-share -properties` 参数以及要用于该共享的共享属性列表。
在共享创建期间禁用共享上的机会锁	输入以下命令：`vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` 禁用操作锁定时、您必须在创建共享时指定共享属性列表、但不应指定 `oplocks` 属性。

相关信息

在现有 SMB 共享上启用或禁用机会锁

监控机会锁状态

用于在卷和 **qtree** 上启用或禁用机会锁的命令

机会锁允许客户端在本地锁定文件和缓存内容，从而提高文件操作的性能。您需要了解用于在卷或 qtree 上启用或禁用机会锁的命令。此外，您还必须了解何时可以在卷和 qtree 上启用或禁用机会锁。

- 默认情况下，卷上已启用机会锁。
- 创建卷时，您不能禁用机会锁。
- 您可以随时在 SVM 的现有卷上启用或禁用机会锁。
- 您可以在 SVM 的 qtree 上启用机会锁。

  机会锁模式设置是 qtree ID 0 的属性，这是所有卷的默认 qtree 。如果在创建 qtree 时未指定机会锁设置，则 qtree 会继承父卷的机会锁设置，该设置默认为启用状态。但是，如果您在新 qtree 上指定了机会锁设置，则该设置优先于卷上的机会锁设置。

如果您要 ...	使用此命令 ...
在卷或 qtree 上启用机会锁	`volume qtree oplocks` 使用 `-oplock-mode` 参数设置为 `enable`
在卷或 qtree 上禁用机会锁	`volume qtree oplocks` 使用 `-oplock-mode` 参数设置为 `disable`

相关信息

监控机会锁状态

在现有 SMB 共享上启用或禁用机会锁

默认情况下， Storage Virtual Machine （SVM）上的 SMB 共享上会启用机会锁。在某些情况下，您可能需要禁用机会锁；或者，如果先前已在共享上禁用机会锁，则可能需要重新启用机会锁。

关于此任务

如果在包含共享的卷上启用了机会锁，但禁用了该共享的机会锁共享属性，则会为该共享禁用机会锁。在共享上禁用机会锁优先于在卷上启用机会锁。在共享上禁用机会锁会同时禁用机会锁和租用机会锁。您可以随时在现有共享上启用或禁用机会锁。

步骤

1. 执行适用的操作：

如果您要 ...	那么 ...
通过修改现有共享在共享上启用机会锁	输入以下命令： `vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties oplocks` 您可以使用逗号分隔列表指定要添加的其他共享属性。 新添加的属性将附加到现有共享属性列表中。先前指定的任何共享属性仍有效。

如果您要 ...	那么 ...
通过修改现有共享禁用共享上的机会锁	输入以下命令： `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks` 您可以使用逗号分隔列表指定要删除的其他共享属性。 您删除的共享属性将从现有共享属性列表中删除；但是，先前配置的未删除的共享属性仍有效。

示例

以下命令为 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上名为 "`Engineering` " 的共享启用机会锁：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

以下命令会对 SVM vs1 上名为 "`Engineering` " 的共享禁用机会锁：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

相关信息

创建 SMB 共享时启用或禁用机会锁

监控机会锁状态

在现有 SMB 共享上添加或删除共享属性

监控机会锁状态

您可以监控和显示有关机会锁状态的信息。您可以使用此信息确定哪些文件具有机会锁，机会锁级别和机会锁状态级别是什么，以及是否使用机会锁租赁。您还可以确定有关可能需要手动中断的锁定的信息。

关于此任务

您可以摘要或详细列表形式显示有关所有机会锁的信息。您还可以使用可选参数显示有关较小一部分现有锁定的信息。例如，您可以指定输出仅返回使用指定客户端 IP 地址或指定路径锁定的。

您可以显示有关传统机会锁和租用机会锁的以下信息：

- 建立机会锁的 SVM ，节点，卷和 LIF
- 锁定 UUID
- 具有机会锁的客户端的 IP 地址
- 建立机会锁的路径
- 锁定协议（ SMB ）和类型（ oplock ）
- 锁定状态
- 机会锁级别
- 连接状态和 SMB 到期时间
- 如果已授予租用机会锁，请打开组 ID

请参见 `vserver oplocks show` 每个参数的详细问题描述的手册页。

步骤

1. 使用显示oplock状态 `vserver locks show` 命令：

示例

以下命令显示有关所有锁定的默认信息。显示的文件上的oplock将授予 `read-batch` oplock级别：

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

以下示例显示了有关路径为的文件锁定的更多详细信息 `/data2/data2_2/intro.pptx`。使用为文件授予租用机会锁 `batch` IP地址为的客户端的机会锁级别 `10.3.1.3`：

> 显示详细信息时，命令会为机会锁和共享锁定信息提供单独的输出。此示例仅显示 oplock 部分的输出。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

相关信息

创建 SMB 共享时启用或禁用机会锁

在现有 SMB 共享上启用或禁用机会锁

用于在卷和 qtree 上启用或禁用机会锁的命令

将组策略对象应用于 SMB 服务器

将组策略对象应用于 SMB 服务器概述

SMB服务器支持组策略对象(GPO)、这是一组称为_group policy attributes的规则、适用

于Active Directory环境中的计算机。您可以使用 GPO 集中管理属于同一 Active Directory 域的集群上所有 Storage Virtual Machine （ SVM ）的设置。

如果SMB服务器上启用了GPO、则ONTAP会将LDAP查询发送到请求GPO信息的Active Directory服务器。如果存在适用于SMB服务器的GPO定义、则Active Directory服务器将返回以下GPO信息：

- GPO名称
- 当前 GPO 版本
- GPO 定义的位置
- GPO 策略集的 UUID 列表（通用唯一标识符）

相关信息

使用动态访问控制（ DAC ）保护文件访问

"SMB 和 NFS 审核和安全跟踪"

支持的 GPO

虽然并非所有组策略对象（ GPO ）都适用于启用了 CIFS 的 Storage Virtual Machine （ SVM ），但 SVM 可以识别和处理相关的 GPO 集。

SVM 当前支持以下 GPO ：

- 高级审核策略配置设置：

  对象访问：中央访问策略暂存

  指定要为中央访问策略（ CAP ）暂存审核的事件类型，包括以下设置：

  - 请勿审核
  - 仅审核成功事件
  - 仅审核失败事件
  - 审核成功和失败事件

  > 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

  使用设置 `Audit Central Access Policy Staging` 中的设置 `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO。

  > 要使用高级审核策略配置 GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置审核。如果未在 SVM 上配置审核，则 GPO 设置将不会应用，并将被丢弃。

- 注册表设置：

  - 已启用 CIFS 的 SVM 的组策略刷新间隔

使用设置 `Registry` GPO。

- 组策略刷新随机偏移

  使用设置 `Registry` GPO。

- BranchCache 的哈希发布

  BranchCache 的哈希发布 GPO 对应于 BranchCache 操作模式。支持以下三种操作模式：

  - 每个共享
  - 所有共享
  - 已禁用
    使用设置 `Registry` GPO。

- BranchCache 的哈希版本支持

  支持以下三种哈希版本设置：

  - BranchCache 1.7 版
  - BranchCache 1.7 版
  - anchCache版本1和2
    使用设置 `Registry` GPO。

> 要使用 BranchCache GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置 BranchCache 。如果未在 SVM 上配置 BranchCache ，则 GPO 设置将不会应用，并将被丢弃。

- 安全设置

  - 审核策略和事件日志

    - 审核登录事件

      指定要审核的登录事件的类型，包括以下设置：

      - 请勿审核
      - 仅审核成功事件
      - 审核失败事件
      - 审核成功和失败事件
        使用设置 `Audit logon events` 中的设置 `Local Policies/Audit Policy` GPO。

        > 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

    - 审核对象访问

      指定要审核的对象访问类型，包括以下设置：

- 请勿审核
- 仅审核成功事件
- 审核失败事件
- 审核成功和失败事件
  使用设置 `Audit object access` 中的设置 `Local Policies/Audit Policy` GPO。

> 如果设置了三个审核选项中的任何一个（仅审核成功事件，仅审核失败事件，审核成功和失败事件），则 ONTAP 将同时审核成功和失败事件。

- 日志保留方法

  指定审核日志保留方法，包括以下设置：

  - 如果日志文件大小超过最大日志大小，则覆盖事件日志
  - 不要覆盖事件日志(手动清除日志)
    使用设置 `Retention method for security log` 中的设置 `Event Log` GPO。

- 最大日志大小

  指定审核日志的最大大小。

  使用设置 `Maximum security log size` 中的设置 `Event Log` GPO。

> 要使用审核策略和事件日志 GPO 设置，必须在已启用 CIFS 且要应用这些设置的 SVM 上配置审核。如果未在 SVM 上配置审核，则 GPO 设置将不会应用，并将被丢弃。

◦ 文件系统安全性

指定通过 GPO 应用文件安全性的文件或目录列表。

使用设置 `File System` GPO。

> 配置文件系统安全 GPO 的卷路径必须位于 SVM 中。

◦ Kerberos 策略

- 最大时钟偏差

  指定计算机时钟同步的最大容错（以分钟为单位）。

  使用设置 `Maximum tolerance for computer clock synchronization` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 最长票证期限

  指定用户服务单的最长生命周期（以小时为单位）。

  使用设置 `Maximum lifetime for user ticket` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 最长票证续订期限

  指定用户票证续订的最长生命周期（以天为单位）。

使用设置 `Maximum lifetime for user ticket renewal` 中的设置 `Account Policies/Kerberos Policy` GPO。

- 用户权限分配（权限）

  - 取得所有权

    指定有权取得任何安全对象所有权的用户和组的列表。

    使用设置 `Take ownership of files or other objects` 中的设置 `Local Policies/User Rights Assignment` GPO。

  - 安全权限

    指定可以为文件，文件夹和 Active Directory 对象等单个资源的对象访问指定审核选项的用户和组列表。

    使用设置 `Manage auditing and security log` 中的设置 `Local Policies/User Rights Assignment` GPO。

  - 更改通知权限（绕过遍历检查）

    指定可以遍历目录树的用户和组列表，即使用户和组可能对遍历的目录没有权限也是如此。

用户接收文件和目录更改通知需要相同的权限。使用设置 `Bypass traverse checking` 中的设置 `Local Policies/User Rights Assignment` GPO。

- 注册表值

  - 需要签名设置

    指定是启用还是禁用所需的 SMB 签名。

使用设置 `Microsoft network server: Digitally sign communications (always)` 中的设置 `Security Options` GPO。

- 限制匿名

指定匿名用户的限制并包括以下三个 GPO 设置：

  - 不枚举安全帐户管理器（ SAM ）帐户：

    此安全设置可确定为匿名连接到计算机授予哪些其他权限。此选项显示为 `no-enumeration` 在ONTAP中(如果已启用)。

    使用设置 `Network access: Do not allow anonymous enumeration of SAM accounts` 中的设置 `Local Policies/Security Options` GPO。

- 不枚举 SAM 帐户和共享

  此安全设置确定是否允许匿名枚举 SAM 帐户和共享。此选项显示为 `no-enumeration` 在ONTAP中(如果已启用)。

  使用设置 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 中的设置 `Local Policies/Security Options` GPO。

- 限制对共享和命名管道的匿名访问

  此安全设置限制对共享和管道的匿名访问。此选项显示为 `no-access` 在ONTAP中(如果已启用)。

  使用设置 `Network access: Restrict anonymous access to Named Pipes and Shares` 中的设置 `Local Policies/Security Options` GPO。

  显示有关已定义和已应用组策略的信息时、 `Resultant restriction for anonymous user` 输出字段提供有关三个限制匿名GPO设置所产生限制的信息。可能产生的限制如下：

° `no-access`

匿名用户被拒绝访问指定的共享和命名管道，并且不能使用 SAM 帐户和共享枚举。如果存在、则会显示此结果限制 `Network access: Restrict anonymous access to Named Pipes and Shares` 已启用GPO。

° `no-enumeration`

匿名用户有权访问指定的共享和命名管道，但不能使用 SAM 帐户和共享枚举。如果同时满足以下两个条件，则会显示由此产生的限制：

- 。 `Network access: Restrict anonymous access to Named Pipes and Shares` 已禁用GPO。
- 或 `Network access: Do not allow anonymous enumeration of SAM accounts` 或 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO已启用。

° `no-restriction`

匿名用户具有完全访问权限，可以使用枚举。如果同时满足以下两个条件，则会显示由此产生的限制：

- 。 `Network access: Restrict anonymous access to Named Pipes and Shares` 已禁用GPO。
- 这两个 `Network access: Do not allow anonymous enumeration of SAM accounts` 和 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 已禁用GPO。
  - 受限组

    您可以配置受限组以集中管理内置或用户定义的组的成员资格。通过组策略应用受限组时，CIFS 服务器本地组的成员资格会自动设置为与应用的组策略中定义的成员资格列表设置匹配。

使用设置 `Restricted Groups` GPO。

- 中央访问策略设置

  指定中央访问策略的列表。中央访问策略和关联的中央访问策略规则可确定 SVM 上多个文件的访问权限。

相关信息

在 CIFS 服务器上启用或禁用 GPO 支持

使用动态访问控制（DAC）保护文件访问

"SMB 和 NFS 审核和安全跟踪"

修改 CIFS 服务器 Kerberos 安全设置

使用 BranchCache 在分支机构缓存 SMB 共享内容

使用 SMB 签名增强网络安全性

配置绕过遍历检查

配置匿名用户的访问限制

对 SMB 服务器使用 GPO 的要求

要对 SMB 服务器使用组策略对象（GPO），您的系统必须满足多项要求。

- SMB 必须在集群上获得许可。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。
- 必须配置 SMB 服务器并将其加入 Windows Active Directory 域。
- SMB 服务器管理员状态必须为 on 。
- 必须配置 GPO 并将其应用于包含 SMB 服务器计算机对象的 Windows Active Directory 组织单位（OU）。
- 必须在 SMB 服务器上启用 GPO 支持。

在 CIFS 服务器上启用或禁用 GPO 支持

您可以在 CIFS 服务器上启用或禁用组策略对象（GPO）支持。如果在 CIFS 服务器上启用 GPO 支持，则在组策略（即应用于包含 CIFS 服务器计算机对象的组织单位（OU）的策略）上定义的适用 GPO 将应用于 CIFS 服务器。

关于此任务

无法在工作组模式下在 CIFS 服务器上启用 GPO 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
启用 GPOs：	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
禁用 GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. 验证GPO支持是否处于所需状态： `vserver cifs group-policy show -vserver +vserver_name_`

   在工作组模式` 下， CIFS 服务器的组策略状态显示为 " 已 `d" 。

示例

以下示例将在 Storage Virtual Machine （ SVM ） vs1 上启用 GPO 支持：

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

相关信息

支持的 GPO

在CIFS服务器中使用GPO的要求

如何在 CIFS 服务器上更新 GPO

手动更新 CIFS 服务器上的 GPO 设置

显示有关 GPO 配置的信息

如何在SMB服务器上更新GPO

如何在 **CIFS** 服务器概述中更新 **GPO**

默认情况下， ONTAP 每 90 分钟检索并应用组策略对象（ GPO ）更改一次。安全设置每 16 小时刷新一次。如果要在 ONTAP 自动更新 GPO 之前更新 GPO 以应用新的 GPO 策略设置，则可以使用 ONTAP 命令在 CIFS 服务器上触发手动更新。

- 默认情况下，所有 GPO 都会根据需要每 90 分钟进行一次验证和更新。

  此间隔可配置、并可使用进行设置 `Refresh interval` 和 `Random offset` GPO设置。

  ONTAP 会查询 Active Directory 以了解对 GPO 的更改。如果 Active Directory 中记录的 GPO 版本号高于

CIFS 服务器上的版本号，则 ONTAP 将检索并应用新的 GPO 。如果版本号相同，则不会更新 CIFS 服务器上的 GPO 。

- 安全设置 GPO 每 16 小时刷新一次。

  ONTAP 每 16 小时检索并应用一次安全设置 GPO ，无论这些 GPO 是否已更改。

  > 在当前 ONTAP 版本中，不能更改 16 小时的默认值。这是 Windows 客户端的默认设置。

- 可以使用 ONTAP 命令手动更新所有 GPO 。

  此命令模拟Windows `gpupdate.exe`/force`命令。

相关信息

手动更新 CIFS 服务器上的 GPO 设置

手动更新 **CIFS** 服务器上的 **GPO** 设置

如果要立即更新 CIFS 服务器上的组策略对象（GPO）设置，可以手动更新这些设置。您只能更新已更改的设置，也可以强制更新所有设置，包括先前应用但尚未更改的设置。

步骤

1. 执行相应的操作：

要更新的内容	输入命令 ...
已更改 GPO 设置	`vserver cifs group-policy update -vserver vserver_name`
所有 GPO 设置	`vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true`

相关信息

如何在 CIFS 服务器上更新 GPO

显示有关 **GPO** 配置的信息

您可以显示有关 Active Directory 中定义的组策略对象（GPO）配置以及应用于 CIFS 服务器的 GPO 配置的信息。

关于此任务

您可以显示 CIFS 服务器所属域的 Active Directory 中定义的所有 GPO 配置的信息，也可以仅显示应用于 CIFS 服务器的 GPO 配置的信息。

步骤

1. 通过执行以下操作之一显示有关 GPO 配置的信息：

要显示有关所有组策略配置的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy show-defined -vserver vserver_name`
应用于启用了 CIFS 的 Storage Virtual Machine （SVM）	`vserver cifs group-policy show-applied -vserver vserver_name`

示例

以下示例显示了在启用了 CIFS 且名为 vs1 的 SVM 所属的 Active Directory 中定义的 GPO 配置：

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
```

```
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2

      GPO Name: Resultant Set of Policy
        Status: enabled
    Advanced Audit Settings:
        Object Access:
            Central Access Policy Staging: failure
    Registry Settings:
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication for Mode BranchCache: per-share
        Hash Version Support for BranchCache: version1
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
```

```
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

以下示例显示了应用于启用了 CIFS 的 SVM vs1 的 GPO 配置：

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
```

```
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
```

```
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

相关信息

在 CIFS 服务器上启用或禁用 GPO 支持

显示有关受限组 **GPO** 的详细信息

您可以显示有关在 Active Directory 中定义为组策略对象（GPO）并应用于 CIFS 服务器的受限组的详细信息。

关于此任务

默认情况下，将显示以下信息：

- 组策略名称
- 组策略版本
- 链接。

  指定配置组策略的级别。可能的输出值包括：

  - `Local` 在ONTAP中配置组策略时
  - `Site` 在域控制器中的站点级别配置组策略时
  - `Domain` 在域控制器的域级别配置组策略时
  - `OrganizationalUnit` 在域控制器的组织单位(OU)级别配置组策略时
  - `RSOP` 根据在不同级别定义的所有组策略生成的一组策略
- 受限组名称
- 属于和不属于受限制组的用户和组
- 添加受限制组的组的列表

  组可以是此处列出的组以外的组的成员。

步骤

1. 通过执行以下操作之一显示有关所有受限组 GPO 的信息：

要显示有关所有受限组 **GPO** 的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`

要显示有关所有受限组 **GPO** 的信息 ...	输入命令 ...
应用于 CIFS 服务器	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

示例

以下示例显示了有关在启用了 CIFS 且名为 vs1 的 SVM 所属的 Active Directory 域中定义的受限组 GPO 的信息：

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

以下示例显示了应用于启用了 CIFS 的 SVM vs1 的受限组 GPO 的信息：

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

您可以显示有关 Active Directory 中定义的中央访问策略的详细信息。您还可以显示有关通过组策略对象（GPO）应用于 CIFS 服务器的中央访问策略的信息。

关于此任务

默认情况下，将显示以下信息：

- SVM name
- 中央访问策略的名称
- SID
- Description
- 创建时间
- 修改时间
- 成员规则

> 工作组模式下的 CIFS 服务器不会显示，因为它们不支持 GPO 。

步骤

1. 通过执行以下操作之一显示有关中央访问策略的信息：

要显示有关所有中央访问策略的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
应用于 CIFS 服务器	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

示例

以下示例显示了 Active Directory 中定义的所有中央访问策略的信息：

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-------------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

以下示例显示了应用于集群上的 Storage Virtual Machine （SVM）的所有中央访问策略的信息：

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

相关信息

使用动态访问控制（DAC）保护文件访问

显示有关 GPO 配置的信息

显示有关中央访问策略规则的信息

显示有关中央访问策略规则的信息

您可以显示与 Active Directory 中定义的中央访问策略关联的中央访问策略规则的详细信息。您还可以显示有关通过中央访问策略 GPO （组策略对象）应用于 CIFS 服务器的中央访问策略规则的信息。

关于此任务

您可以显示有关已定义和应用的中央访问策略规则的详细信息。默认情况下，将显示以下信息：

- Vserver name
- 中央访问规则的名称
- Description
- 创建时间
- 修改时间
- 当前权限
- 建议的权限

- 目标资源

要显示与中央访问策略关联的所有中央访问策略规则的信息 ...	输入命令 ...
在 Active Directory 中定义	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
应用于 CIFS 服务器	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

示例

以下示例显示了与 Active Directory 中定义的中央访问策略关联的所有中央访问策略规则的信息：

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

以下示例显示了与应用于集群上 Storage Virtual Machine （ SVM ）的中央访问策略关联的所有中央访问策略规则的信息：

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

相关信息

使用动态访问控制（DAC）保护文件访问

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

用于管理**SMB**服务器计算机帐户密码的命令

您需要了解用于更改，重置和禁用密码以及配置自动更新计划的命令。您还可以在SMB服务器上配置计划以自动更新它。

如果您要 ...	使用此命令 ...
更改或重置域帐户密码，并且您知道该密码	`vserver cifs domain password change`
重置域帐户密码，但您不知道密码	`vserver cifs domain password reset`
配置SMB服务器以自动更改计算机帐户密码	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
在SMB服务器上禁用计算机帐户密码自动更改	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

有关详细信息，请参见每个命令的手册页。

显示有关已发现服务器的信息

您可以显示与 CIFS 服务器上发现的 LDAP 服务器和域控制器相关的信息。

步骤

1. 要显示与已发现服务器相关的信息、请输入以下命令： `vserver cifs domain discovered-servers show`

示例

以下示例显示了为 SVM vs1 发现的服务器：

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

相关信息

重置和重新发现服务器

停止或启动 CIFS 服务器

重置和重新发现服务器

通过重置和重新发现 CIFS 服务器上的服务器， CIFS 服务器可以丢弃有关 LDAP 服务器和域控制器的存储信息。丢弃服务器信息后， CIFS 服务器将重新获取这些外部服务器的当前信息。如果连接的服务器未正确响应，则此功能非常有用。

步骤

1. 输入以下命令： `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 显示有关新重新发现的服务器的信息： `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

示例

以下示例将重置和重新发现 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 的服务器：

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

相关信息

显示有关已发现服务器的信息

停止或启动 CIFS 服务器

管理域控制器发现

从 ONTAP 9.3 开始，您可以修改发现域控制器（ DC ）的默认过程。这样，您就可以将发现限制为您的站点或首选 DC 池，从而根据环境的不同提高性能。

关于此任务

默认情况下，动态发现过程会发现所有可用的 DC ，包括任何首选 DC ，本地站点中的所有 DC 以及所有远程 DC 。此配置可能会导致在某些环境中进行身份验证和访问共享时出现延迟。如果您已确定要使用的 DC 池，或者远程 DC 不足或无法访问，则可以更改发现方法。

在ONTAP 9.3及更高版本中、 `discovery-mode` 的参数 `cifs domain discovered-servers` 命令用于选择以下发现选项之一：

- 发现域中的所有 DC 。
- 仅发现本地站点中的 DC 。

  。 `default-site` 可以定义SMB服务器的参数、使其对未在site-and-services中分配给站点的CIFS使用此模式。

- 不执行服务器发现， SMB 服务器配置仅取决于首选 DC 。

  要使用此模式，必须先为 SMB 服务器定义首选 DC 。

步骤

1. 指定所需的发现选项： `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

的选项 `mode` 参数：

- `all`

  发现所有可用的 DC （默认）。

- `site`

  仅限您的站点进行 DC 发现。

- `none`

  仅使用首选 DC ，而不执行发现。

添加首选域控制器

ONTAP 会通过 DNS 自动发现域控制器。或者，您也可以将一个或多个域控制器添加到特定域的首选域控制器列表中。

关于此任务

如果指定域已存在首选域控制器列表，则新列表将与现有列表合并。

步骤

1. 要添加到首选域控制器列表、请输入以下命令：+
   `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …`+

   `-vserver` *`vserver_name`* 指定Storage Virtual Machine (SVM)名称。

   `-domain` *`domain_name`* 指定指定域控制器所属域的完全限定Active Directory名称。

   `-preferred-dc` *`IP_address`*、 按首选顺序以逗号分隔列表形式指定首选域控制器的一个或多个IP地址。

示例

以下命令会将域控制器172.17.102.25和172.17.102.24添加到首选域控制器列表中、SVM VS1上的SMB服务器使用该列表来管理对cifs.lab.example.com域的外部访问。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

相关信息

用于管理首选域控制器的命令

用于管理首选域控制器的命令

您需要了解用于添加，显示和删除首选域控制器的命令。

如果您要 ...	使用此命令 ...
添加首选域控制器	`vserver cifs domain preferred-dc add`
显示首选域控制器	`vserver cifs domain preferred-dc show`
删除首选域控制器	`vserver cifs domain preferred-dc remove`

有关详细信息，请参见每个命令的手册页。

相关信息

添加首选域控制器

启用与域控制器的 SMB2 连接

从 ONTAP 9.1 开始，您可以启用 SMB 版本 2.0 以连接到域控制器。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， SMB2 默认处于启用状态。

关于此任务

。 `smb2-enabled-for-dc-connections` 命令选项可为您使用的ONTAP版本启用系统默认设置。对于 SMB 1.0 ， ONTAP 9.1 的系统默认设置为已启用，而对于 SMB 2.0 ，系统默认设置为已禁用。对于 SMB 1.0 ，系统默认启用 ONTAP 9.2 ，对于 SMB 2.0 ，系统默认启用 SMB 9.2 。如果域控制器最初无法协商 SMB 2.0 ，则会使用 SMB 1.0 。

可以从 ONTAP 到域控制器禁用 SMB 1.0 。在 ONTAP 9.1 中，如果已禁用 SMB 1.0 ，则必须启用 SMB 2.0 才能与域控制器进行通信。

详细了解：

- "验证已启用的SMB版本"。
- "支持的 SMB 版本和功能"。

> 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。

步骤

1. 更改SMB安全设置之前、请验证已启用哪些SMB版本： `vserver cifs security show`
2. 向下滚动列表以查看 SMB 版本。
3. 使用执行相应的命令 `smb2-enabled-for-dc-connections` 选项

SMB2 的目标位置	输入命令 ...
enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections true`

SMB2 的目标位置	输入命令 ...
已禁用	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc -connections false`

启用与域控制器的加密连接

从 ONTAP 9.8 开始，您可以指定对与域控制器的连接进行加密。

关于此任务

当时、ONTAP需要对域控制器(DC)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。

当需要加密DC通信时、 `-smb2-enabled-for-dc-connections` 选项将被忽略、因为ONTAP仅协商SMB3连接。如果 DC 不支持 SMB3 和加密， ONTAP 将不会与其连接。

步骤

1. 启用与DC的加密通信： `vserver cifs security modify -vserver` *`svm_name`* `-encryption -required-for-dc-connection true`

使用空会话访问非 **Kerberos** 环境中的存储

使用空会话访问非 **Kerberos** 环境中的存储概述

空会话访问可为存储系统数据等网络资源以及在本地系统下运行的基于客户端的服务提供权限。当客户端进程使用 `ssystem` 帐户访问网络资源时，将发生空会话。空会话配置专用于非 Kerberos 身份验证。

存储系统如何提供空会话访问

由于空会话共享不需要身份验证，因此需要空会话访问的客户端必须在存储系统上映射其 IP 地址。

默认情况下，未映射的空会话客户端可以访问某些 ONTAP 系统服务，例如共享枚举，但会限制它们访问任何存储系统数据。

> ONTAP通过支持Windows注册表设置值 `-restrict-anonymous` 选项这样，您可以控制未映射的空用户查看或访问系统资源的范围。例如，您可以禁用共享枚举和对 IPC$ 共享（隐藏的命名管道共享）的访问。。 `vserver cifs options modify` 和 `vserver cifs options show` 手册页提供了有关的详细信息 `-restrict-anonymous` 选项

除非另有配置，否则运行通过空会话请求存储系统访问的本地进程的客户端仅是非限制性组的成员，例如 "`everyone` " 。要限制对选定存储系统资源的空会话访问，您可能需要创建所有空会话客户端所属的组；通过创建此组，您可以限制存储系统访问并设置专门应用于空会话客户端的存储系统资源权限。

ONTAP在中提供了映射语法 `vserver name-mapping` 用于指定允许使用空用户会话访问存储系统资源的客户端的IP地址的命令集。为空用户创建组后，您可以指定存储系统资源的访问限制以及仅适用于空会话的资源权

限。空用户标识为匿名登录。空用户无权访问任何主目录。

从映射的 IP 地址访问存储系统的任何空用户都将获得映射的用户权限。请考虑适当的预防措施，以防止未经授权访问与空用户映射的存储系统。要获得最大保护，请将存储系统和所有需要空用户存储系统访问的客户端置于单独的网络上，以消除 IP 地址 `spoofing` 的可能性。

相关信息

配置匿名用户的访问限制

授予空用户对文件系统共享的访问权限

您可以通过分配空会话客户端要使用的组并记录空会话客户端的 IP 地址以添加到允许使用空会话访问数据的客户端列表，从而允许空会话客户端访问存储系统资源。

步骤

1. 使用 `vserver name-mapping create` 命令、用于将空用户映射到任何有效的Windows用户、并使用IP限定符。

   以下命令使用有效主机名 google.com 将空用户映射到 user1：

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   “ANONYMOUS LOGON” -replacement user1 - hostname google.com
   ```

   以下命令使用有效 IP 地址 10.238.2.54/32 将空用户映射到 user1：

   ```
   vserver name-mapping create -direction win-unix  -position 2 -pattern
   “ANONYMOUS LOGON” -replacement user1 -address 10.238.2.54/32
   ```

2. 使用 `vserver name-mapping show` 命令以确认名称映射。

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                                Replacement: user1
   ```

3. 使用 `vserver cifs options modify -win-name-for-null-user` 用于将Windows成员资格分配给空用户的命令。

   只有当空用户具有有效的名称映射时，此选项才适用。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. 使用 `vserver cifs options show` 命令以确认将空用户映射到Windows用户或组。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

管理 SMB 服务器的 NetBIOS 别名

管理 SMB 服务器的 NetBIOS 别名概述

NetBIOS 别名是 SMB 服务器的备用名称， SMB 客户端可以在连接到 SMB 服务器时使用这些别名。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 服务器响应原始文件服务器的名称，则为 SMB 服务器配置 NetBIOS 别名非常有用。

您可以在创建 SMB 服务器时或创建 SMB 服务器后的任何时间指定 NetBIOS 别名列表。您可以随时在列表中添加或删除 NetBIOS 别名。您可以使用 NetBIOS 别名列表中的任何名称连接到 SMB 服务器。

相关信息

显示有关基于 TCP 连接的 NetBIOS 的信息

向SMB服务器添加NetBIOS别名列表

如果您希望SMB客户端使用别名连接到SMB服务器、则可以创建NetBIOS别名列表、也可以将NetBIOS别名添加到现有NetBIOS别名列表。

关于此任务

- NetBIOS 别名长度最多可以为 15 个字符。
- 您最多可以在 SMB 服务器上配置 200 个 NetBIOS 别名。
- 不允许使用以下字符：

  @#*()=+[]|；："、<>\/?

步骤

1. 添加NetBIOS别名：+
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

- 您可以使用逗号分隔列表指定一个或多个 NetBIOS 别名。
- 指定的 NetBIOS 别名将添加到现有列表中。
- 如果 NetBIOS 别名列表当前为空，则会创建一个新的 NetBIOS 别名列表。

2. 验证NetBIOS别名是否已正确添加： `vserver cifs show -vserver vserver_name -display -netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

相关信息

从 NetBIOS 别名列表中删除 NetBIOS 别名

显示 CIFS 服务器上的 NetBIOS 别名列表

从 **NetBIOS** 别名列表中删除 **NetBIOS** 别名

如果 CIFS 服务器不需要特定的 NetBIOS 别名，可以从列表中删除这些 NetBIOS 别名。您也可以从列表中删除所有 NetBIOS 别名。

关于此任务

您可以使用逗号分隔列表删除多个 NetBIOS 别名。您可以通过指定来删除CIFS服务器上的所有NetBIOS别名 - 作为的值 `-netbios-aliases` 参数。

步骤

1. 执行以下操作之一：

要删除的内容	输入 ...
列表中的特定 NetBIOS 别名	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
列表中的所有 NetBIOS 别名	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 验证指定的NetBIOS别名是否已删除： `vserver cifs show -vserver vserver_name -display -netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

显示 **CIFS** 服务器上的 **NetBIOS** 别名列表

您可以显示 NetBIOS 别名列表。如果您要确定 SMB 客户端可用来连接到 CIFS 服务器的名称列表，则此功能非常有用。

步骤

1. 执行以下操作之一：

要显示的信息	输入 ...
CIFS 服务器的 NetBIOS 别名	`vserver cifs show -display-netbios -aliases`
NetBIOS 别名列表，作为 CIFS 服务器详细信息的一部分	`vserver cifs show -instance`

以下示例显示了有关 CIFS 服务器的 NetBIOS 别名的信息：

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

以下示例将 NetBIOS 别名列表显示为 CIFS 服务器详细信息的一部分：

```
vserver cifs show -instance
```

```
                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    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: ALIAS_1, ALIAS_2,
ALIAS_3
```

有关详细信息，请参见命令手册页。

相关信息

向 CIFS 服务器添加 NetBIOS 别名列表

用于管理 CIFS 服务器的命令

确定 SMB 客户端是否使用 NetBIOS 别名进行连接

您可以确定 SMB 客户端是否使用 NetBIOS 别名进行连接，如果是，还可以确定使用哪个 NetBIOS 别名进行连接。在对连接问题进行故障排除时，此功能非常有用。

关于此任务

您必须使用 `-instance` 参数以显示与SMB连接关联的NetBIOS别名(如果有)。如果使用CIFS服务器名称或IP地址建立SMB连接、则为的输出 `NetBIOS Name` 字段为 - (连字符)。

步骤

1. 执行所需的操作：

要显示 **NetBIOS** 信息的对象	输入 **...**
SMB连接	`vserver cifs session show -instance`
使用指定 NetBIOS 别名的连接：	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

以下示例显示了用于与会话 ID 1 建立 SMB 连接的 NetBIOS 别名的信息：

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                  Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                 Windows User: EXAMPLE\user1
                    UNIX User: user1
                  Open Shares: 2
                   Open Files: 2
                   Open Other: 0
               Connected Time: 1d 1h 10m 5s
                    Idle Time: 22s
             Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                 NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

管理其他 SMB 服务器任务

停止或启动 CIFS 服务器

您可以停止 SVM 上的 CIFS 服务器，这在用户不通过 SMB 共享访问数据时执行任务时非常有用。您可以通过启动 CIFS 服务器来重新启动 SMB 访问。通过停止 CIFS 服务器，您还可以修改 Storage Virtual Machine （SVM）上允许的协议。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
停止 CIFS 服务器	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	启动 CIFS 服务器
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` 指定命令应在前台还是后台执行。如果不输入此参数、则此参数将设置为 `true`，命令将在前台执行。

2. 使用验证CIFS服务器管理状态是否正确 `vserver cifs show` 命令：

示例

以下命令将在 SVM vs1 上启动 CIFS 服务器：

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                            Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

相关信息

显示有关已发现服务器的信息

重置和重新发现服务器

将 CIFS 服务器移动到不同的 OU

除非指定其他 OU ，否则 CIFS 服务器 create-process 会在设置期间使用默认组织单位（ OU ） CN=Computers 。您可以在设置后将 CIFS 服务器移动到不同的 OU 。

步骤

1. 在 Windows 服务器上，打开 * Active Directory 用户和计算机 * 树。
2. 找到 Storage Virtual Machine （ SVM ）的 Active Directory 对象。
3. 右键单击该对象并选择 * 移动 * 。
4. 选择要与 SVM 关联的 OU

结果

SVM 对象将放置在选定的 OU 中。

移动 SMB 服务器之前，请修改 SVM 上的动态 DNS 域

如果您希望 Active Directory 集成的 DNS 服务器在将 SMB 服务器移动到另一个域时在 DNS 中动态注册 SMB 服务器的 DNS 记录，则必须在移动 SMB 服务器之前修改 Storage Virtual Machine （ SVM ）上的动态 DNS （ DDNS ）。

开始之前

必须在 SVM 上修改 DNS 名称服务，才能使用包含将包含 SMB 服务器计算机帐户的新域的服务位置记录的 DNS 域。如果使用的是安全 DDNS ，则必须使用 Active Directory 集成的 DNS 名称服务器。

关于此任务

尽管 DDNS （如果在 SVM 上配置）会自动将数据 LIF 的 DNS 记录添加到新域中，但原始域的 DNS 记录不会自动从原始 DNS 服务器中删除。您必须手动删除它们。

要在移动 SMB 服务器之前完成 DDNS 修改，请参见以下主题：

"配置动态 DNS 服务"

将 **SVM** 加入 **Active Directory** 域

您可以通过使用修改域来将Storage Virtual Machine (SVM)加入Active Directory域、而无需删除现有SMB服务器 `vserver cifs modify` 命令：您可以重新加入当前域或加入新域。

开始之前

- SVM 必须已具有 DNS 配置。
- SVM 的 DNS 配置必须能够为目标域提供服务。

  DNS 服务器必须包含域 LDAP 和域控制器服务器的服务位置记录（ SRV ）。

关于此任务

- CIFS 服务器的管理状态必须设置为 " d拥有 " 才能继续修改 Active Directory 域。
- 如果命令成功完成，则管理状态会自动设置为 "`up` " 。
- 加入域时，此命令可能需要几分钟才能完成。

步骤

1. 将SVM加入CIFS服务器域： `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   有关详细信息、请参见的手册页 `vserver cifs modify` 命令：如果需要为新域重新配置DNS、请参见的手册页 `vserver dns modify` 命令：

   要为SMB服务器创建Active Directory计算机帐户、您必须提供具有足够权限的Windows帐户的名称和密码、以便向添加计算机 `ou=` *`example`* `ou` 中的容器 *`example`*.com域。

   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

2. 验证CIFS服务器是否位于所需的Active Directory域中： `vserver cifs show`

示例

在以下示例中， SVM vs1 上的 SMB 服务器 "`CIFSSERVER1` " 使用 keytab 身份验证加入 example.com 域：

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name               Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

显示有关基于 **TCP** 连接的 **NetBIOS** 的信息

您可以显示有关基于 TCP （ NBT ）的 NetBIOS 连接的信息。在对 NetBIOS 相关问题进行故障排除时，此功能非常有用。

步骤

1. 使用 `vserver cifs nbtstat` 命令以显示有关基于TCP连接的NetBIOS的信息。

> 不支持基于 IPv6 的 NetBIOS 名称服务（ NBNS ）。

示例

以下示例显示了为 "`cluster1` " 显示的 NetBIOS 名称服务信息：

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

用于管理**SMB**服务器的命令

您需要了解用于创建、显示、修改、停止、启动、 和删除SMB服务器。此外，还可以使用命令重置和重新发现服务器，更改或重置计算机帐户密码，计划更改计算机帐户密码以及添加或删除 NetBIOS 别名。

如果您要 …	使用此命令 …
创建SMB服务器	`vserver cifs create`
显示有关 SMB 服务器的信息	`vserver cifs show`
修改SMB服务器	`vserver cifs modify`
将 SMB 服务器移动到另一个域	`vserver cifs modify`

停止 SMB 服务器	`vserver cifs stop`
启动 SMB 服务器	`vserver cifs start`
删除SMB服务器	`vserver cifs delete`
重置和重新发现 SMB 服务器的服务器	`vserver cifs domain discovered-servers reset-servers`
更改SMB服务器的计算机帐户密码	`vserver cifs domain password change`
重置SMB服务器的计算机帐户密码	`vserver cifs domain password change`
为SMB服务器的计算机帐户计划自动密码更改	`vserver cifs domain password schedule modify`
为SMB服务器添加NetBIOS别名	`vserver cifs add-netbios-aliases`
删除SMB服务器的NetBIOS别名	`vserver cifs remove-netbios-aliases`

有关详细信息，请参见每个命令的手册页。

相关信息

"删除SMB服务器时本地用户和组会发生什么情况"

启用 NetBIOS 名称服务

从 ONTAP 9 开始， NetBIOS 名称服务（ NBNS ，有时称为 Windows Internet 名称服务或 WINS ）默认处于禁用状态。以前，无论网络上是否启用了 WINS ，启用了 CIFS 的 Storage Virtual Machine （ SVM ）都会发送名称注册广播。要将此类广播限制为需要 NBNS 的配置，必须为新的 CIFS 服务器显式启用 NBNS 。

开始之前

- 如果您已在使用 NBNS ，并且已升级到 ONTAP 9 ，则无需完成此任务。NBNS 将继续照常运行。
- NBNS 通过 UDP （端口 137 ）启用。
- 不支持基于 IPv6 的 NBNS 。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 在 CIFS 服务器上启用 NBNS 。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. 返回到管理权限级别：

```
set -privilege admin
```

对 SMB 访问和 SMB 服务使用 IPv6

使用 IPv6 的要求

在 SMB 服务器上使用 IPv6 之前，您需要了解哪些版本的 ONTAP 和 SMB 支持 IPv6 ，以及许可证要求是什么。

ONTAP 许可证要求：

如果 SMB 已获得许可，则 IPv6 不需要任何特殊许可证。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。

SMB 协议版本要求

- 对于 SVM ， ONTAP 在所有版本的 SMB 协议上均支持 IPv6 。

> 不支持基于 IPv6 的 NetBIOS 名称服务（ NBNS ）。

支持使用 SMB 访问和 CIFS 服务的 IPv6

如果要在 CIFS 服务器上使用 IPv6 ，则需要了解 ONTAP 如何支持 IPv6 用于 SMB 访问以及 CIFS 服务的网络通信。

Windows 客户端和服务器支持

ONTAP 支持支持 IPv6 的 Windows 服务器和客户端。下面介绍了 Microsoft Windows 客户端和服务器 IPv6 支持：

- Windows 7 ， Windows 8 ， Windows Server 2008 ， Windows Server 2012 及更高版本支持对 SMB 文件共享和 Active Directory 服务使用 IPv6 ，包括 DNS ， LDAP ， CLDAP 和 Kerberos 服务。

  如果配置了 IPv6 地址，则 Windows 7 和 Windows Server 2008 及更高版本默认对 Active Directory 服务使用 IPv6 。支持通过 IPv6 连接进行 NTLM 和 Kerberos 身份验证。

  ONTAP 支持的所有 Windows 客户端均可使用 IPv6 地址连接到 SMB 共享。

有关ONTAP支持的Windows客户端的最新信息、请参见 "互操作性表"。

> IPv6 不支持 NT 域。

其他 **CIFS** 服务支持

除了对 SMB 文件共享和 Active Directory 服务的 IPv6 支持之外， ONTAP 还为以下各项提供 IPv6 支持：

- 客户端服务，包括脱机文件夹，漫游配置文件，文件夹重定向以及先前版本
- 服务器端服务，包括动态主目录（主目录功能），符号链接和 Widelink ， BranchCache ， ODX 副本卸载，自动节点转介， 和先前版本
- 文件访问管理服务，包括使用 Windows 本地用户和组进行访问控制和权限管理，使用 CLI 设置文件权限和审核策略，安全跟踪，文件锁定管理以及监控 SMB 活动
- NAS 多协议审核
- fpolicy
- 持续可用的共享，见证协议和远程 VSS （与基于 SMB 的 Hyper-V 配置结合使用）

名称服务和身份验证服务支持

IPv6 支持与以下名称服务进行通信：

- 域控制器
- DNS 服务器
- LDAP服务器
- KDC服务器
- NIS服务器

CIFS 服务器如何使用 **IPv6** 连接到外部服务器

要创建符合要求的配置，您必须了解 CIFS 服务器在连接到外部服务器时如何使用 IPv6 。

- 源地址选择

  如果尝试连接到外部服务器，则选定源地址的类型必须与目标地址相同。例如，如果连接到 IPv6 地址，则托管 CIFS 服务器的 Storage Virtual Machine （ SVM ）必须具有一个数据 LIF 或管理 LIF ，该数据 LIF 或管理 LIF 必须使用 IPv6 地址作为源地址。同样，如果要连接到 IPv4 地址， SVM 必须具有一个数据 LIF 或管理 LIF ，并将 IPv4 地址用作源地址。

- 对于使用 DNS 动态发现的服务器，将按如下方式执行服务器发现：
  - 如果在集群上禁用了 IPv6 ，则只会发现 IPv4 服务器地址。
  - 如果在集群上启用了 IPv6 ，则会发现 IPv4 和 IPv6 服务器地址。根据地址所属服务器的适用性以及 IPv6 或 IPv4 数据或管理 LIF 的可用性，可以使用任一类型。
    动态服务器发现用于发现域控制器及其关联服务，例如 LSA ， NETLOGON ， Kerberos 和 LDAP 。
- DNS 服务器连接

  SVM 在连接到 DNS 服务器时是否使用 IPv6 取决于 DNS 名称服务配置。如果 DNS 服务配置为使用 IPv6 地址，则使用 IPv6 进行连接。如果需要， DNS 名称服务配置可以使用 IPv4 地址，以便继续使用 IPv4 地址连接到 DNS 服务器。在配置 DNS 名称服务时，可以指定 IPv4 和 IPv6 地址的组合。

- LDAP服务器连接

SVM 在连接到 LDAP 服务器时是否使用 IPv6 取决于 LDAP 客户端配置。如果 LDAP 客户端配置为使用 IPv6 地址，则使用 IPv6 进行连接。如果需要， LDAP 客户端配置可以使用 IPv4 地址，以便继续使用 IPv4 地址连接到 LDAP 服务器。在配置 LDAP 客户端配置时，可以指定 IPv4 和 IPv6 地址的组合。

> 在为 UNIX 用户，组和网络组名称服务配置 LDAP 时，将使用 LDAP 客户端配置。

- NIS服务器连接

  SVM在连接到NIS服务器时是否使用IPv6取决于NIS名称服务配置。如果NIS服务配置为使用IPv6地址、则使用IPv6进行连接。如果需要、NIS名称服务配置可以使用IPv4地址、以便继续使用IPv4地址连接到NIS服务器。在配置NIS名称服务时、可以指定IPv4和IPv6地址的组合。

> NIS 名称服务用于存储和管理 UNIX 用户，组，网络组和主机名对象。

相关信息

为 SMB 启用 IPv6 （仅限集群管理员）

监控和显示有关 IPv6 SMB 会话的信息

为 SMB 启用 IPv6 （仅限集群管理员）

集群设置期间未启用 IPv6 网络。集群管理员必须在集群设置完成后启用 IPv6 ，才能对 SMB 使用 IPv6 。如果集群管理员启用了 IPv6 ，则会为整个集群启用 IPv6 。

步骤

1. 启用IPv6： `network options ipv6 modify -enabled true`

   有关在集群上启用 IPv6 和配置 IPv6 LIF 的详细信息，请参见 *Network Management Guide* 。

   已启用 IPv6 。可以配置用于 SMB 访问的 IPv6 数据 LIF 。

相关信息

监控和显示有关 IPv6 SMB 会话的信息

"网络管理"

为 SMB 禁用 IPv6

即使使用网络选项在集群上启用了 IPv6 ，您也不能使用同一命令为 SMB 禁用 IPv6 。而是在集群管理员禁用集群上最后一个启用了 IPv6 的接口时， ONTAP 会禁用 IPv6 。您应与集群管理员就启用了 IPv6 的接口的管理事宜进行沟通。

有关在集群上禁用 IPv6 的详细信息，请参见 *Network Management Guide* 。

相关信息

"网络管理"

监控和显示有关 **IPv6 SMB** 会话的信息

您可以监控和显示有关使用 IPv6 网络连接的 SMB 会话的信息。此信息可用于确定使用 IPv6 连接的客户端，以及有关 IPv6 SMB 会话的其他有用信息。

步骤

1. 执行所需的操作：

要确定是否 ...	输入命令 ...
与 Storage Virtual Machine （ SVM ）的 SMB 会话使用 IPv6 进行连接	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 用于通过指定 LIF 地址的 SMB 会话	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* 是数据LIF的IPv6地址。

使用 **SMB** 设置文件访问

配置安全模式

安全模式如何影响数据访问

安全模式及其影响是什么

安全模式有四种： UNIX ， NTFS ，混合和统一。每个安全模式对处理数据权限的方式具有不同的影响。您必须了解不同的影响，以确保选择适合您的安全模式。

请务必了解，安全模式并不确定哪些客户端类型可以或不可以访问数据。安全模式仅确定 ONTAP 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

例如，如果某个卷使用 UNIX 安全模式，则由于 ONTAP 的多协议性质， SMB 客户端仍可访问数据（前提是它们正确进行身份验证和授权）。但是， ONTAP 使用的是 UNIX 权限，只有 UNIX 客户端才能使用原生工具进行修改。

安全风格	可以修改权限的客户端	客户端可以使用的权限	生成的有效安全模式	可以访问文件的客户端
"unix"	NFS	NFSv3 模式位	"unix"	NFS 和 SMB
NFSv4.x ACL	"unix"	NTFS	SMB	NTFS ACL
NTFS	混合	NFS 或 SMB	NFSv3 模式位	"unix"
NFSv4.x ACL	"unix"	NTFS ACL	NTFS	统一：

安全风格	可以修改权限的客户端	客户端可以使用的权限	生成的有效安全模式	可以访问文件的客户端
NFS 或 SMB	NFSv3 模式位	"unix"	NFSv4.1 ACL	"unix"
NTFS ACL	NTFS	统一： (仅限无限卷、在ONTAP 9.4及更早版本中。)	NFS 或 SMB	NFSv3 模式位
"unix"	NFSv4.1 ACL			NTFS ACL

FlexVol卷支持UNIX、NTFS和混合安全模式。混合或统一安全模式时，有效权限取决于上次修改权限的客户端类型，因为用户会逐个设置安全模式。如果修改权限的最后一个客户端是 NFSv3 客户端，则权限为 UNIX NFSv3 模式位。如果最后一个客户端是 NFSv4 客户端，则权限为 NFSv4 ACL 。如果最后一个客户端是 SMB 客户端，则权限为 Windows NTFS ACL 。

统一安全模式仅适用于无限卷，而 ONTAP 9.5 及更高版本不再支持无限卷。有关详细信息，请参见 "FlexGroup 卷管理概述"。

从ONTAP 9.2开始、 `show-effective-permissions` 参数 `vserver security file-directory` 命令用于显示为Windows或UNIX用户授予的对指定文件或文件夹路径的有效权限。此外、还有可选参数 `-share -name` 用于显示有效共享权限。

> ONTAP 最初会设置一些默认文件权限。默认情况下， UNIX ，混合和统一安全模式卷中所有数据的有效安全模式为 UNIX ，有效权限类型为 UNIX 模式位（ 0755 ，除非另有指定），直到客户端按照默认安全模式进行配置为止。默认情况下， NTFS 安全模式卷中所有数据的有效安全模式为 NTFS ，并且具有一个 ACL ，允许对任何人进行完全控制。

设置安全模式的位置和时间

可以在 FlexVol 卷（根卷或数据卷）和 qtree 上设置安全模式。安全模式可以在创建时手动设置，自动继承或稍后更改。

确定要在 **SVM** 上使用的安全模式

为了帮助您确定要在卷上使用的安全模式，您应考虑两个因素。主要因素是管理文件系统的管理员类型。二级因素是访问卷上数据的用户或服务的类型。

在卷上配置安全模式时，应考虑环境的需求，以确保选择最佳安全模式并避免管理权限时出现问题。以下注意事项有助于您做出决定：

安全风格	选择条件
"unix"	• 文件系统由 UNIX 管理员管理。 • 大多数用户都是 NFS 客户端。 • 访问数据的应用程序使用 UNIX 用户作为服务帐户。

安全风格	选择条件
NTFS	• 文件系统由 Windows 管理员管理。 • 大多数用户都是SMB客户端。 • 访问数据的应用程序使用 Windows 用户作为服务帐户。
混合	文件系统由 UNIX 和 Windows 管理员管理，用户由 NFS 和 SMB 客户端组成。

安全模式继承的工作原理

如果在创建新的 FlexVol 卷或 qtree 时未指定安全模式，则它会以不同方式继承其安全模式。

安全模式按以下方式继承：

- FlexVol 卷继承其所属 SVM 的根卷的安全模式。
- qtree 继承其所属 FlexVol 卷的安全模式。
- 文件或目录会继承其所在 FlexVol 卷或 qtree 的安全模式。

ONTAP 如何保留 **UNIX** 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 **Windows** 安全性选项卡管理 **UNIX** 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用 Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

  如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

  更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。

在 **SVM** 根卷上配置安全模式

您可以配置 Storage Virtual Machine （ SVM ）根卷安全模式，以确定 SVM 根卷上的数据所使用的权限类型。

步骤

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 用于定义安全模式的参数。

   根卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

2. 显示并验证配置，包括您创建的 SVM 的根卷安全模式： `vserver show -vserver` *`vserver_name`*

在 **FlexVol** 卷上配置安全模式

您可以配置 FlexVol 卷安全模式，以确定 Storage Virtual Machine （ SVM ）的 FlexVol 卷上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 FlexVol 卷 …	使用命令 …
尚不存在	`volume create` 并包括 `-security-style` 用于指定安全模式的参数。
已存在	`volume modify` 并包括 `-security-style` 用于指定安全模式的参数。

   FlexVol卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建 FlexVol 卷时未指定安全模式，则此卷将继承根卷的安全模式。

   有关的详细信息、请参见 `volume create` 或 `volume modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置，包括您创建的 FlexVol 卷的安全模式，请输入以下命令：

```
volume show -volume volume_name -instance
```

在 qtree 上配置安全模式

您可以配置 qtree 卷安全模式，以确定 qtree 上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 qtree…	使用命令 …
尚不存在	`volume qtree create` 并包括 `-security -style` 用于指定安全模式的参数。
已存在	`volume qtree modify` 并包括 `-security -style` 用于指定安全模式的参数。

   qtree安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建qtree时未指定安全模式、则默认安全模式为 `mixed`。

   有关的详细信息、请参见 `volume qtree create` 或 `volume qtree modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置(包括所创建的qtree的安全模式)、请输入以下命令： `volume qtree show -qtree qtree_name -instance`

在 NAS 命名空间中创建和管理数据卷

在 NAS 命名空间中创建和管理数据卷概述

要在 NAS 环境中管理文件访问，您必须管理 Storage Virtual Machine （ SVM ）上的数据卷和接合点。其中包括规划命名空间架构，创建具有或不具有接合点的卷，挂载或卸载卷以及显示有关数据卷和 NFS 服务器或 CIFS 服务器命名空间的信息。

创建具有指定接合点的数据卷

您可以在创建数据卷时指定接合点。生成的卷会自动挂载在接合点，并可立即配置用于 NAS 访问。

开始之前

要创建卷的聚合必须已存在。

> 接合路径中不能使用以下字符： * # " > < | ? \
>
> 此外，接合路径长度不能超过 255 个字符。

步骤

1. 创建具有接合点的卷： `volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path *junction_path*`

   接合路径必须以根（/）开头，并且可以同时包含目录和接合卷。接合路径不需要包含卷的名称。接合路径与卷名称无关。

   指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （SVM）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于您创建的数据卷的安全模式。建议您在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

   接合路径不区分大小写； `/ENG` 与相同 `/eng`。如果创建 CIFS 共享， Windows 会将接合路径视为区分大小写。例如、如果接合为 `/ENG`，则CIFS共享的路径必须以开头 `/ENG`，不是 `/eng`。

   您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已使用所需的接合点创建卷： `volume show -vserver *vserver_name* -volume *volume_name* -junction`

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                   Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

创建数据卷而不指定接合点

您可以在不指定接合点的情况下创建数据卷。生成的卷不会自动挂载，也不可配置用于 NAS 访问。您必须先挂载卷，然后才能为该卷配置 SMB 共享或 NFS 导出。

开始之前

要创建卷的聚合必须已存在。

步骤

1. 使用以下命令创建不带接合点的卷： `volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （SVM）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于数据卷的安全模式。建议您

在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已在没有接合点的情况下创建卷： `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

示例

以下示例将在 SVM vs1 上创建一个名为 `sales` 的卷，该卷未挂载在接合点：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data           RW_volume
vs1       home4       true     /eng/home       RW_volume
vs1       vs1_root    -        /               -
vs1       sales       -        -               -
```

挂载或卸载 **NAS** 命名空间中的现有卷

必须先在 NAS 命名空间上挂载卷，然后才能配置 NAS 客户端对 Storage Virtual Machine （ SVM ）卷中所含数据的访问。如果卷当前未挂载，则可以将其挂载到接合点。您也可以卸载卷。

关于此任务

如果卸载某个卷并使其脱机、则NAS客户端将无法访问该接合点中的所有数据、包括接合点位于已卸载卷的命名空间中的卷中的数据。

> 要停止 NAS 客户端对卷的访问，仅仅卸载卷是不够的。您必须使此卷脱机、或者采取其他步骤确保客户端文件句柄缓存失效。有关详细信息，请参见以下知识库文章： "从 ONTAP 的命名空间中删除卷后， NFSv3 客户端仍可访问该卷"

卸载卷并使其脱机后、卷中的数据不会丢失。此外，在卷上或在已卸载卷内的目录和接合点上创建的现有卷导出策略和 SMB 共享也会保留下来。如果重新挂载卸载的卷， NAS 客户端可以使用现有导出策略和 SMB 共享访问卷中包含的数据。

步骤

1. 执行所需的操作：

如果您要 ...	输入命令 ...
挂载卷	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
卸载卷	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. 验证卷是否处于所需的挂载状态：

   `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-fields state,junction-path,junction-active`

示例

以下示例将位于SVM"`VS1`"上名为` ales s的卷挂载到接合点"/sales`"：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下示例将卸载位于SVM"`VS1`"上的名为"`data`"的卷并使其脱机：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

您可以显示有关 Storage Virtual Machine （SVM）的已挂载卷以及卷挂载到的接合点的信息。您还可以确定哪些卷未挂载到接合点。您可以使用此信息了解和管理 SVM 命名空间。

步骤

1. 执行所需的操作：

要显示的内容	输入命令 ...
有关 SVM 上已挂载和已卸载卷的摘要信息	`volume show -vserver vserver_name -junction`
有关 SVM 上已挂载和已卸载卷的详细信息	`volume show -vserver vserver_name -volume volume_name -instance`
有关 SVM 上已挂载和已卸载卷的特定信息	a. 如有必要、您可以显示的有效字段 `-fields` 参数： `volume show -fields ?` b. 使用显示所需信息 `-fields` 参数：volume show -vserver vserver-name -fieldname、…

示例

以下示例显示了 SVM vs1 上已挂载和已卸载的卷的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

以下示例显示了有关 SVM vs2 上卷的指定字段的信息：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

配置名称映射

配置名称映射概述

ONTAP 使用名称映射将 CIFS 身份映射到 UNIX 身份，将 Kerberos 身份映射到 UNIX 身份，并将 UNIX 身份映射到 CIFS 身份。无论用户是从 NFS 客户端还是从 CIFS 客户端进行连接，它都需要此信息来获取用户凭据并提供正确的文件访问权限。

除了两个例外情况，您无需使用名称映射：

- 您配置的是纯 UNIX 环境，不打算对卷使用 CIFS 访问或 NTFS 安全模式。
- 您可以配置要使用的默认用户。

  在这种情况下，不需要进行名称映射，因为所有客户端凭据都映射到同一默认用户，而不是映射每个客户端凭据。

请注意，您只能对用户使用名称映射，而不能对组使用名称映射。

但是，您可以将一组用户映射到特定用户。例如，您可以将以 SALES 开头或结尾的所有 AD 用户映射到特定 UNIX 用户和用户的 UID 。

名称映射的工作原理

当 ONTAP 必须映射用户的凭据时，它会首先检查本地名称映射数据库和 LDAP 服务器中是否存在现有映射。它是检查一个还是同时检查这两者，以及检查顺序取决于 SVM 的名称服务配置。

- 适用于 Windows 到 UNIX 的映射

  如果未找到映射， ONTAP 将检查小写的 Windows 用户名是否为 UNIX 域中的有效用户名。如果此操作不起作用，则只要配置了默认 UNIX 用户，它就会使用默认 UNIX 用户。如果未配置默认 UNIX 用户，并且 ONTAP 也无法通过这种方式获取映射，则映射将失败并返回错误。

- UNIX 到 Windows 的映射

  如果未找到映射， ONTAP 将尝试查找与 SMB 域中的 UNIX 名称匹配的 Windows 帐户。如果此操作不起作用，则会使用默认 SMB 用户，但前提是已配置此用户。如果未配置默认 CIFS 用户，并且 ONTAP 也无法通过此方式获取映射，则映射将失败并返回错误。

默认情况下，计算机帐户映射到指定的默认 UNIX 用户。如果未指定默认 UNIX 用户，计算机帐户映射将失败。

- 从 ONTAP 9.5 开始，您可以将计算机帐户映射到默认 UNIX 用户以外的用户。
- 在 ONTAP 9.4 及更早版本中，您无法将计算机帐户映射到其他用户。

  即使为计算机帐户定义了名称映射，也会忽略这些映射。

多域搜索 **UNIX** 用户到 **Windows** 用户名映射

在将 UNIX 用户映射到 Windows 用户时， ONTAP 支持多域搜索。系统将搜索所有已发现的受信任域以查找与替换模式匹配的匹配项，直到返回匹配结果为止。或者，您也可以配置首选受信任域列表，该列表将代替发现的受信任域列表使用，并按顺序进行搜索，直到返回匹配结果为止。

域信任如何影响 **UNIX** 用户到 **Windows** 用户名称映射搜索

要了解多域用户名映射的工作原理，您必须了解域信任如何与 ONTAP 配合使用。与 CIFS 服务器主域的 Active Directory 信任关系可以是双向信任，也可以是两种类型的单向信任之一，即入站信任或出站信任。主域是 SVM 上的 CIFS 服务器所属的域。

- _ 双向信任 _

  通过双向信任，两个域相互信任。如果 CIFS 服务器的主域与另一个域具有双向信任，则主域可以对属于受信任域的用户进行身份验证和授权，反之亦然。

  UNIX 用户到 Windows 用户名映射搜索只能在主域和另一个域之间具有双向信任的域上执行。

- 出站信任 _

  对于出站信任，主域信任另一个域。在这种情况下，主域可以对属于出站受信任域的用户进行身份验证和授权。

执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有出站信任的域。

- *Inbound trust*

  对于入站信任，另一个域信任 CIFS 服务器的主域。在这种情况下，主域无法对属于入站受信任域的用户进行身份验证或授权。

  在执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有入站信任的域。

如何使用通配符（*）配置名称映射的多域搜索

在 Windows 用户名的域部分使用通配符有助于进行多域名称映射搜索。下表说明了如何在名称映射条目的域部分使用通配符来启用多域搜索：

Pattern	更换	结果
root	• 。 \\ 管理员	UNIX 用户 "`root` " 将映射到名为 "`administrator` " 的用户。系统会按顺序搜索所有受信任域，直到找到第一个名为 "`administrator` " 的匹配用户为止。
*	**	有效的 UNIX 用户将映射到相应的 Windows 用户。系统将按顺序搜索所有受信任域，直到找到具有该名称的第一个匹配用户为止。 模式 ** 仅适用于从 UNIX 到 Windows 的名称映射，而不是相反。

如何执行多域名搜索

您可以选择以下两种方法之一来确定用于多域名搜索的受信任域列表：

- 使用由 ONTAP 编译的自动发现的双向信任列表
- 使用您编译的首选受信任域列表

如果将 UNIX 用户映射到使用通配符用于用户名的域部分的 Windows 用户，则会在所有受信任域中查找此 Windows 用户，如下所示：

- 如果配置了首选受信任域列表，则只会在此搜索列表中按顺序查找映射的 Windows 用户。
- 如果未配置首选受信任域列表，则会在主域的所有双向受信任域中查找 Windows 用户。
- 如果主域没有双向受信任的域，则会在主域中查找用户。

如果 UNIX 用户映射到用户名中没有域部分的 Windows 用户，则会在主域中查找此 Windows 用户。

名称映射转换规则

ONTAP 系统会为每个 SVM 保留一组转换规则。每个规则都包含两部分： *pattern* 和 *replacement* 。转换从相应列表的开头开始，并根据第一个匹配规则执行替换。模式是 UNIX 模式的正则表达式。替换项是一个字符串、其中包含表示模式中的子表达式的转义序列、与UNIX中的情况一样 `sed` 计划。

创建名称映射

您可以使用 `vserver name-mapping create` 命令以创建名称映射。您可以使用名称映射使 Windows 用户能够访问 UNIX 安全模式卷，反之亦然。

关于此任务

对于每个 SVM ， ONTAP 支持每个方向最多 12 ， 500 个名称映射。

步骤

1. 创建名称映射： `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > 。 `-pattern` 和 `-replacement` 语句可以表达为正则表达式。您也可以使用 `-replacement` 用于使用空替换字符串明确拒绝映射到用户的语句 `" "` (空格字符)。请参见 `vserver name-mapping create` 有关详细信息、请参见手册页。

   创建 Windows 到 UNIX 映射时，在创建新映射时与 ONTAP 系统建立了打开连接的任何 SMB 客户端都必须注销并重新登录才能查看新映射。

示例

以下命令将在名为 vs1 的 SVM 上创建名称映射。此映射是指优先级列表中位置 1 处从 UNIX 到 Windows 的映射。映射会将 UNIX 用户 johnd 映射到 Windows 用户 ENG\JohnDoe 。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此映射是指优先级列表中位置 1 处从 Windows 到 UNIX 的映射。此处的模式和替换项包括正则表达式。此映射会将域 ENG 中的每个 CIFS 用户映射到与 SVM 关联的 LDAP 域中的用户。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此处的模式将 "` $` " 作为必须转义的 Windows 用户名中的一个元素。映射会将 Windows 用户 ENG\ john$ops 映射到 UNIX 用户 john_ops 。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

配置默认用户：

您可以配置一个默认用户，以便在用户的所有其他映射尝试均失败或不希望在 UNIX 和 Windows 之间映射单个用户时使用。或者，如果您希望对未映射用户的身份验证失败，则不应配置默认用户。

关于此任务

对于 CIFS 身份验证，如果不希望将每个 Windows 用户映射到单个 UNIX 用户，则可以改为指定默认 UNIX 用户。

对于 NFS 身份验证，如果不希望将每个 UNIX 用户映射到单个 Windows 用户，则可以改为指定一个默认 Windows 用户。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
配置默认 UNIX 用户	`vserver cifs options modify -default -unix-user` *`user_name`*
配置默认 Windows 用户	`vserver nfs modify -default-win-user` *`user_name`*

用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 ...	使用此命令 ...
创建名称映射	`vserver name-mapping create`
在特定位置插入名称映射	`vserver name-mapping insert`
显示名称映射	`vserver name-mapping show`
交换两个名称映射的位置 ⓘ 如果使用 IP 限定符条目配置了名称映射，则不允许交换。	`vserver name-mapping swap`

如果您要 ...	使用此命令 ...
修改名称映射	`vserver name-mapping modify`
删除名称映射	`vserver name-mapping delete`
验证名称映射是否正确	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

有关详细信息，请参见每个命令的手册页。

配置多域名称映射搜索

启用或禁用多域名称映射搜索

对于多域名称映射搜索，在配置 UNIX 用户到 Windows 用户名的映射时，您可以在 Windows 名称的域部分使用通配符（*）。通过在名称的域部分中使用通配符（*），ONTAP 可以搜索与包含 CIFS 服务器计算机帐户的域具有双向信任的所有域。

关于此任务

除了搜索所有双向受信任域之外，您还可以配置首选受信任域的列表。配置首选受信任域列表后， ONTAP 将使用首选受信任域列表而不是发现的双向受信任域来执行多域名称映射搜索。

- 默认情况下，多域名称映射搜索处于启用状态。
- 此选项可在高级权限级别下使用。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

多域名称映射搜索的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum-search-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum-search-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

相关信息

可用的 SMB 服务器选项

重置和重新发现受信任域

您可以强制重新发现所有受信任域。当受信任域服务器未正确响应或信任关系发生更改时，此功能非常有用。只会发现与主域具有双向信任的域，即包含 CIFS 服务器计算机帐户的域。

步骤

1. 使用重置和重新发现受信任域 `vserver cifs domain trusts rediscover` 命令：

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

相关信息

显示有关已发现的受信任域的信息

显示有关已发现的受信任域的信息

您可以显示有关 CIFS 服务器主域的已发现受信任域的信息，该域是包含 CIFS 服务器计算机帐户的域。如果您希望了解发现了哪些受信任域以及如何在发现的受信任域列表中对这些域进行排序，则此功能非常有用。

关于此任务

仅发现与主域具有双向信任的域。由于主域的域控制器（ Domain Controller， DC ）按 DC 确定的顺序返回受信任域列表，因此无法预测此列表中域的顺序。通过显示受信任域列表，您可以确定多域名称映射搜索的搜索顺序。

显示的受信任域信息按节点和 Storage Virtual Machine （ SVM ）分组。

步骤

1. 使用显示有关已发现的受信任域的信息 `vserver cifs domain trusts show` 命令：

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

相关信息

重置和重新发现受信任域

在首选受信任域列表中添加，删除或替换受信任域

您可以在SMB服务器的首选受信任域列表中添加或删除受信任域、也可以修改当前列表。如果您配置了首选受信任域列表，则在执行多域名称映射搜索时，系统将使用此列表，而不是发现的双向受信任域。

关于此任务

- 如果要向现有列表添加受信任域，则新列表将与现有列表合并，并在末尾放置新条目系统将按受信任域列表中显示的顺序搜索这些受信任域。
- 如果您要从现有列表中删除受信任域，但未指定列表，则会删除指定 Storage Virtual Machine （ SVM ）的整个受信任域列表。
- 如果修改现有受信任域列表，则新列表将覆盖现有列表。

> 您应在首选受信任域列表中仅输入双向受信任域。即使您可以在首选域列表中输入出站或入站信任域，但在执行多域名称映射搜索时不会使用它们。ONTAP 会跳过单向域的条目，然后转到列表中的下一个双向受信任域。

步骤

1. 执行以下操作之一：

如果要对首选受信任域列表执行以下操作 ...	使用命令 ...
将受信任域添加到列表中	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
从列表中删除受信任域	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
修改现有列表	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

示例

以下命令会将两个受信任域（ cifs1.example.com 和 cifs2.example.com ）添加到 SVM vs1 使用的首选受信任域列表中：

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

以下命令将从 SVM vs1 使用的列表中删除两个受信任域：

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

以下命令将修改 SVM vs1 使用的受信任域列表。新列表将替换原始列表：

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

相关信息

显示有关首选受信任域列表的信息

显示有关首选受信任域列表的信息

如果启用了多域名称映射搜索，则可以显示有关首选受信任域列表中的受信任域以及这些域的搜索顺序的信息。您可以配置首选受信任域列表，以替代使用自动发现的受信任域列表。

步骤

1. 执行以下操作之一：

要显示以下内容的信息 ...	使用命令 ...
按 Storage Virtual Machine （ SVM ）分组的集群中的所有首选受信任域	`vserver cifs domain name-mapping-search show`
指定 SVM 的所有首选受信任域	`vserver cifs domain name-mapping-search show -vserver vserver_name`

以下命令显示集群上所有首选受信任域的信息：

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

相关信息

在首选受信任域列表中添加，删除或替换受信任域

创建和配置 SMB 共享

创建和配置 SMB 共享概述

在用户和应用程序通过 SMB 访问 CIFS 服务器上的数据之前，您必须创建和配置 SMB 共享， SMB 共享是卷中的一个命名访问点。您可以通过指定共享参数和共享属性来自定义共享。您可以随时修改现有共享。

创建 SMB 共享时， ONTAP 会为共享创建一个默认 ACL ，并为 Everyone 创建具有完全控制权限的 ACL 。

SMB 共享与 Storage Virtual Machine （ SVM ）上的 CIFS 服务器绑定。如果删除了 SVM 或从 SVM 中删除了与之关联的 CIFS 服务器，则会删除 SMB 共享。如果在SVM上重新创建CIFS服务器、则必须重新创建SMB共享。

相关信息

使用 SMB 管理文件访问

"Microsoft Hyper-V 和 SQL Server 的 SMB 配置"

在卷上配置用于 SMB 文件名转换的字符映射

什么是默认管理共享

在Storage Virtual Machine (SVM)上创建CIFS服务器时、系统会自动创建默认管理共享。您应了解这些默认共享是什么以及如何使用它们。

在创建 CIFS 服务器时， ONTAP 会创建以下默认管理共享：

> 从ONTAP 9.8开始、默认情况下不再创建admin$共享。

- ipc$
- admin$(仅限ONTAP 9.7及更早版本)
- C$

由于以 $ 字符结尾的共享是隐藏共享，因此默认管理共享在 " 我的电脑 " 中不可见，但您可以使用共享文件夹查看它们。

如何使用 **ipc$** 和 **admin$** 默认共享

ipc$ 和 admin$ 共享由 ONTAP 使用， Windows 管理员无法使用这些共享访问驻留在 SVM 上的数据。

- ipc$ 共享

  ipc$ 共享是一种共享命名管道的资源，这些管道对于程序之间的通信至关重要。ipc$ 共享用于远程管理计算机和查看计算机的共享资源。您不能更改 ipc$ 共享的共享设置，共享属性或 ACL 。您也不能重命名或删除 ipc$ 共享。

- admin$共享(仅限ONTAP 9.7及更早版本)

  > 从ONTAP 9.8开始、默认情况下不再创建admin$共享。

  admin$ 共享用于远程管理 SVM 。此资源的路径始终是 SVM 根的路径。您不能更改 admin$ 共享的共享设置，共享属性或 ACL 。您也不能重命名或删除 admin$ 共享。

如何使用 **c$** 默认共享

c$ 共享是一个管理共享，集群或 SVM 管理员可以使用它来访问和管理 SVM 根卷。

以下是 c$ 共享的特征：

- 此共享的路径始终是 SVM 根卷的路径，无法修改。
- c$ 共享的默认 ACL 为管理员 / 完全控制。

  此用户为 BUILTIN\administrator 。默认情况下， BUILTIN\administrator 可以映射到共享，并查看，创建，修改或删除映射的根目录中的文件和文件夹。管理此目录中的文件和文件夹时，应谨慎。

- 您可以更改 c$ 共享的 ACL 。
- 您可以更改 c$ 共享设置和共享属性。
- 您不能删除 c$ 共享。
- SVM 管理员可以通过跨越命名空间接合从映射的 c$ 共享访问 SVM 命名空间的其余部分。
- 可以使用 Microsoft 管理控制台访问 c$ 共享。

相关信息

使用 Windows 安全性选项卡配置高级 NTFS 文件权限

在 SMB 服务器上创建 ONTAP 共享时，应牢记 SMB 共享命名要求。

ONTAP 的共享命名约定与 Windows 相同，其中包括以下要求：

- 每个共享的名称对于 SMB 服务器必须是唯一的。
- 共享名称不区分大小写。
- 最大共享名称长度为 80 个字符。
- 支持 Unicode 共享名称。
- 以 $ 字符结尾的共享名称是隐藏的共享。
- 对于ONTAP 9.7及更早版本、系统会自动在每个CIFS服务器上创建admin$、ipc$和c$管理共享、这些共享是保留的共享名称。从ONTAP 9.8开始、不再自动创建admin$共享。
- 创建共享时，不能使用共享名称 ontap_admin$ 。
- 支持包含空格的共享名称：
  - 不能使用空格作为共享名称中的第一个字符或最后一个字符。
  - 必须将包含空格的共享名称用引号括起来。

    单引号被视为共享名称的一部分，不能代替引号。

- 命名 SMB 共享时，支持以下特殊字符：

  ！ @ # $ % & ' _ - 。~ （） { }

- 命名 SMB 共享时不支持以下特殊字符：
  - " / \ ： ； _< > ， ? * =

在多协议环境中创建共享时的目录区分大小写要求

如果您在 SVM 中创建共享，并使用 8.3 命名方案来区分名称之间只有大小写差异的目录名称，则必须在共享路径中使用 8.3 名称，以确保客户端连接到所需的目录路径。

在以下示例中，在 Linux 客户端上创建了两个名为 "`testdir` " 和 "`testdir` " 的目录。包含这些目录的卷的接合路径为 `/home`。第一个输出来自 Linux 客户端，第二个输出来自 SMB 客户端。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

在向第二个目录创建共享时，必须在共享路径中使用 8.3 名称。在此示例中、第一个目录的共享路径为 `/home/testdir` 第二个目录的共享路径为 `/home/TESTDI~1`。

使用 SMB 共享属性

使用 SMB 共享属性概述

您可以自定义 SMB 共享的属性。

可用的共享属性如下：

共享属性	Description
`oplocks`	此属性指定共享使用机会锁，也称为客户端缓存。
`browsable`	此属性允许 Windows 客户端浏览共享。
`showsnapshot`	此属性指定客户端可以查看和遍历 Snapshot 副本。
`changenotify`	此属性指定共享支持更改通知请求。对于 SVM 上的共享，这是默认的初始属性。
`attributecache`	通过此属性，可以在 SMB 共享上缓存文件属性，从而加快属性访问速度。默认情况下，禁用属性缓存。只有当有客户端通过 SMB 1.0 连接到共享时，才应启用此属性。如果客户端通过 SMB 2.x 或 SMB 3.0 连接到共享，则此共享属性不适用。
`continuously-available`	此属性允许支持它的 SMB 客户端以持久方式打开文件。以这种方式打开的文件不会受到故障转移和交还等中断事件的影响。
`branchcache`	此属性指定共享允许客户端对此共享中的文件请求 BranchCache 哈希。只有在 CIFS BranchCache 配置中将 "`per-share` " 指定为操作模式时，此选项才有用。

共享属性	Description
`access-based-enumeration`	此属性指定已在此共享上启用 _Access Based 枚举 _（ABE）。用户可以根据用户的访问权限查看 ABE 筛选的共享文件夹，从而防止显示用户无权访问的文件夹或其他共享资源。
`namespace-caching`	此属性指定连接到此共享的 SMB 客户端可以缓存 CIFS 服务器返回的目录枚举结果，从而提高性能。默认情况下， SMB 1 客户端不会缓存目录枚举结果。由于默认情况下 SMB 2 和 SMB 3 客户端会缓存目录枚举结果，因此指定此共享属性仅会为 SMB 1 客户端连接提供性能优势。
`encrypt-data`	此属性指定访问此共享时必须使用 SMB 加密。访问 SMB 数据时不支持加密的 SMB 客户端将无法访问此共享。

在现有 **SMB** 共享上添加或删除共享属性

您可以通过添加或删除共享属性来自定义现有 SMB 共享。如果您要更改共享配置以满足环境中不断变化的要求，此功能将非常有用。

开始之前

要修改其属性的共享必须存在。

关于此任务

添加共享属性的准则：

- 您可以使用逗号分隔列表添加一个或多个共享属性。
- 先前指定的任何共享属性仍有效。

  新添加的属性将附加到现有共享属性列表中。

- 如果为已应用于共享的共享属性指定新值，则新指定的值将替换原始值。
- 您不能使用删除共享属性 `vserver cifs share properties add` 命令：

  您可以使用 `vserver cifs share properties remove` 命令以删除共享属性。

删除共享属性的准则：

- 您可以使用逗号分隔列表删除一个或多个共享属性。
- 先前指定但未删除的任何共享属性仍有效。

步骤

1. 输入相应的命令：

如果您要 ...	输入命令 ...
添加共享属性	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
删除共享属性	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 验证共享属性设置：`vserver cifs share show -vserver vserver_name -share-name share_name`

示例

以下命令将添加 `showsnapshot` 将共享属性分配给SVM VS1上名为`shre1`的共享：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

以下命令将删除 `browsable` SVM VS1上名为`shre2`的共享中的共享属性：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

相关信息

用于管理 SMB 共享的命令

在从 ONTAP 命令行创建共享以存储具有 UNIX 有效安全性的数据时，您可以指定由该共享中的 SMB 用户创建的所有文件属于同一个组，称为 *force-group* ，该组必须是 UNIX 组数据库中的预定义组。使用强制组可以更轻松地确保属于不同组的 SMB 用户可以访问文件。

只有当共享位于 UNIX 或混合 qtree 中时，指定强制组才有意义。无需为 NTFS 卷或 qtree 中的共享设置强制组，因为这些共享中的文件访问由 Windows 权限而不是 UNIX GID 决定。

如果为共享指定了强制组，则共享的以下内容将变为 true：

- 强制组中访问此共享的 SMB 用户将临时更改为强制组的 GID 。

  通过此 GID ，他们可以访问此共享中无法通过其主 GID 或 UID 正常访问的文件。

- 无论文件所有者的主 GID 如何， SMB 用户创建的此共享中的所有文件都属于同一个强制组。

当 SMB 用户尝试访问 NFS 创建的文件时， SMB 用户的主 GID 将确定访问权限。

强制组不会影响 NFS 用户访问此共享中文件的方式。NFS 创建的文件从文件所有者获取 GID 。访问权限的确定取决于尝试访问文件的 NFS 用户的 UID 和主 GID 。

使用强制组可以更轻松地确保属于不同组的 SMB 用户可以访问文件。例如，如果您要创建一个共享来存储公司的网页并为工程和营销部门的用户授予写入访问权限，则可以创建一个共享并为名为 "`webgroup1` " 的强制组授予写入访问权限。由于使用强制组， SMB 用户在此共享中创建的所有文件均归 "`webgroup1` " 组所有。此外，在访问共享时，系统会自动为用户分配 "`webgroup1` " 组的 GID 。因此，所有用户都可以写入此共享，而无需管理工程和营销部门中用户的访问权限。

相关信息

使用 force-group 共享设置创建 SMB 共享

使用 **force-group** 共享设置创建 **SMB** 共享

如果您希望 ONTAP 将访问具有 UNIX 文件安全性的卷或 qtree 上的数据的 SMB 用户视为属于同一 UNIX 组，则可以使用强制组共享设置创建 SMB 共享。

步骤

1. 创建SMB共享： `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   如果为UNC路径 (`\\servername\sharename\filepath`)包含超过256个字符(不包括初始"`\\`")，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。

   如果要在创建共享后删除强制组、则可以随时修改共享并指定空字符串("")作为的值 `-force-group-for-create` 参数。如果通过修改共享来删除 force-group ，则此共享的所有现有连接仍将使用先前设置的 force-group 作为主 GID 。

示例

以下命令将创建一个"`webpages`"共享、此共享可通过中的Web进行访问 `/corp/companyinfo` 将SMB用户创

建的所有文件分配给webgroup1组的目录：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

相关信息

使用强制组共享设置优化 SMB 用户访问

使用 MMC 查看有关 SMB 共享的信息

您可以使用 Microsoft 管理控制台（MMC）查看 SVM 上的 SMB 共享信息并执行某些管理任务。在查看共享之前，您需要将 MMC 连接到 SVM 。

关于此任务

您可以使用 MMC 对 SVM 中包含的共享执行以下任务：

- 查看共享
- 查看活动会话
- 查看打开的文件
- 枚举系统中的会话，文件和树连接列表
- 关闭系统中已打开的文件
- 关闭打开的会话
- 创建 / 管理共享

> 上述功能显示的视图是特定于节点的视图，而不是特定于集群的视图。因此，在使用 MMC 连接到 SMB 服务器主机名（即 cifs01.domain.local ）时，系统会根据 DNS 设置方式将您路由到集群中的单个 LIF 。

适用于 ONTAP 的 MMC 不支持以下功能：

- 创建新的本地用户 / 组
- 管理 / 查看现有本地用户 / 组
- 查看事件或性能日志
- 存储
- 服务和应用程序

在不支持此操作的情况下、您可能会遇到这种情况 `remote procedure call failed` 错误。

"常见问题解答：在 ONTAP 中使用 Windows MMC"

步骤

1. 要在任何 Windows 服务器上打开计算机管理 MMC ，请在 * 控制面板 * 中选择 * 管理工具 * > * 计算机管理 * 。
2. 选择 * 操作 * > * 连接到另一台计算机 * 。

此时将显示选择计算机对话框。

3. 键入存储系统的名称或单击 * 浏览 * 以查找存储系统。
4. 单击 * 确定 * 。

   MMC 连接到 SVM 。

5. 在导航窗格中，单击 * 共享文件夹 * > * 共享 * 。

   SVM 上的共享列表将显示在右侧显示窗格中。

6. 要显示共享的共享属性，请双击该共享以打开 * 属性 * 对话框。
7. 如果无法使用 MMC 连接到存储系统，则可以在存储系统上使用以下命令之一将用户添加到 BUILTIN\Administrators 组或 BUILTIN\Power Users 组：

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

用于管理 **SMB** 共享的命令

您可以使用 `vserver cifs share` 和 `vserver cifs share properties` 用于管理SMB共享的命令。

如果您要 ...	使用此命令 ...
创建 SMB 共享	`vserver cifs share create`
显示 SMB 共享	`vserver cifs share show`
修改 SMB 共享	`vserver cifs share modify`
删除 SMB 共享	`vserver cifs share delete`
向现有共享添加共享属性	`vserver cifs share properties add`
从现有共享中删除共享属性	`vserver cifs share properties remove`
显示有关共享属性的信息	`vserver cifs share properties show`

有关详细信息，请参见每个命令的手册页。

使用 SMB 共享 ACL 确保文件访问安全

管理 SMB 共享级 ACL 的准则

您可以更改共享级 ACL ，为用户授予对共享的或多或少的访问权限。您可以使用 Windows 用户和组或 UNIX 用户和组配置共享级 ACL 。

默认情况下，创建共享后，共享级 ACL 会为名为 Everyone 的标准组授予读取访问权限。ACL 中的读取访问权限意味着域和所有受信任域中的所有用户都对共享具有只读访问权限。

您可以使用 Windows 客户端上的 Microsoft 管理控制台（ MMC ）或 ONTAP 命令行更改共享级别 ACL 。

使用 MMC 时，请遵循以下准则：

- 指定的用户名和组名必须为 Windows 名称。
- 您只能指定 Windows 权限。

使用 ONTAP 命令行时，请遵循以下准则：

- 指定的用户和组名称可以是 Windows 名称或 UNIX 名称。

  如果在创建或修改 ACL 时未指定用户和组类型，则默认类型为 Windows 用户和组。

- 您只能指定 Windows 权限。

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。

关于此任务

您可以使用本地或域 Windows 用户或组名称或 UNIX 用户或组名称来配置共享级 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 **ACL**，请使用 ...	输入命令 ...
Windows 用户	`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`*
Windows 组	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\group_name`* `-permission` *`access_right`*
UNIX 用户	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-user`* `-user-or-group` *`UNIX_user_name`* `-permission access_right`
UNIX 组	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-group`* `-user-or-group` *`UNIX_group_name`* `-permission access_right`

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` 在"`Svs1.example.coms`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
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 `Read` 对"`vs2.example.com`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 Share       User/Group               User/Group  Access
Vserver          Name        Name                     Type
Permission
---------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

以下命令提供 `Change` 对名为"`Tiger Team`"和的本地Windows组的权限 `Full_Control` 对`Svs1d`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

用于管理 **SMB** 共享访问控制列表的命令

您需要了解用于管理 SMB 访问控制列表（ACL）的命令，其中包括创建，显示，修改和删除这些列表。

如果您要 ...	使用此命令 ...
创建新ACL	`vserver cifs share access-control create`
显示 ACL	`vserver cifs share access-control show`
修改 ACL	`vserver cifs share access-control modify`
删除 ACL	`vserver cifs share access-control delete`

使用文件权限确保文件访问安全

使用 **Windows** 安全性选项卡配置高级 **NTFS** 文件权限

您可以使用 Windows 属性窗口中的 * Windows 安全性 * 选项卡配置文件和文件夹的标准 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

通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（DACL）添加条目，可以在 Windows 主机上配置 NTFS 文件权限。然后，安全描述符将应用于 NTFS 文件和目录。这些任务由 Windows 图形用户界面自动处理。

步骤

1. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 * 。
2. 完成 * 映射网络驱动器 * 对话框：
   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的 CIFS 服务器名称以及共享的名称。

      如果CIFS服务器名称为"`CIFS_SERVER`"、而共享名为"`shre1`"、则应键入 `\\CIFS_SERVER\share1`。

      您可以为 CIFS 服务器指定数据接口的 IP 地址，而不是 CIFS 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。
3. 选择要为其设置 NTFS 文件权限的文件或目录。
4. 右键单击文件或目录，然后选择 * 属性 * 。
5. 选择 * 安全性 * 选项卡。
   - 安全性 * 选项卡显示设置了 NTFS 权限的用户和组的列表。* 权限 * 框显示了对选定的每个用户或组有效的允许和拒绝权限列表。
6. 单击 * 高级 * 。

   Windows 属性窗口显示有关分配给用户和组的现有文件权限的信息。
7. 单击 * 更改权限 * 。

   此时将打开权限窗口。
8. 执行所需的操作：

如果您要 ...	执行以下操作 ...
为新用户或组设置高级 NTFS 权限	a. 单击 * 添加 * 。 b. 在 * 输入要选择的对象名称 * 框中，键入要添加的用户或组的名称。 c. 单击 * 确定 * 。

如果您要 ...	执行以下操作 ...
更改用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要更改其高级权限的用户或组。 b. 单击 * 编辑 * 。
删除用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要删除的用户或组。 b. 单击 * 删除 * 。 c. 跳至步骤 13 。

如果要为新用户或组添加高级 NTFS 权限，或者更改现有用户或组的 NTFS 高级权限，则会打开 < 对象 > 的权限条目框。

9. 在 * 应用于 * 框中，选择要如何应用此 NTFS 文件权限条目。

   如果要对单个文件设置 NTFS 文件权限，则 * 应用于 * 框不会处于活动状态。* 应用于 * 设置默认为 * 仅此对象 * 。

10. 在 * 权限 * 框中，为要对此对象设置的高级权限选择 * 允许 * 或 * 拒绝 * 框。

    - 要允许指定的访问，请选中 * 允许 * 框。
    - 要不允许指定的访问，请选中 * 拒绝 * 框。
      您可以对以下高级权限设置权限：
    - * 完全控制 *

      如果选择此高级权限，则会自动选择所有其他高级权限（允许或拒绝权限）。

    - * 遍历文件夹 / 执行文件 *
    - * 列出文件夹 / 读取数据 *
    - * 读取属性 *
    - * 读取扩展属性 *
    - * 创建文件 / 写入数据 *
    - * 创建文件夹 / 附加数据 *
    - * 写入属性 *
    - * 写入扩展属性 *
    - * 删除子文件夹和文件 *
    - * 删除 *
    - * 读取权限 *
    - * 更改权限 *
    - * 取得所有权 *

> 如果任何高级权限框不可选，则是因为权限是从父对象继承的。

11. 如果希望此对象的子文件夹和文件继承这些权限，请选中 * 仅将这些权限应用于此容器中的对象和 / 或容器 * 框。
12. 单击 * 确定 * 。
13. 添加，删除或编辑完 NTFS 权限后，请为此对象指定继承设置：
    - 选中 * 包括此对象父级的可继承权限 * 框。

      这是默认值。
    - 选中 * 将所有子对象权限替换为此对象的可继承权限 * 框。

      如果要对单个文件设置 NTFS 文件权限，则权限框中不存在此设置。

      > 选择此设置时请务必小心。此设置将删除所有子对象的所有现有权限，并将其替换为此对象的权限设置。您可能会无意中删除不希望删除的权限。在混合安全模式卷或 qtree 中设置权限时尤其重要。如果子对象采用 UNIX 有效安全模式，则将 NTFS 权限传播到这些子对象会导致 ONTAP 将这些对象从 UNIX 安全模式更改为 NTFS 安全模式，并且这些子对象上的所有 UNIX 权限将替换为 NTFS 权限。

    - 选择这两个框。
    - 不选择任何一个框。
14. 单击 * 确定 * 关闭 * 权限 * 框。
15. 单击 * 确定 * 以关闭 * 对象 * 的高级安全设置框。

有关如何设置高级 NTFS 权限的详细信息，请参见 Windows 文档。

相关信息

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

显示NTFS安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

使用 **ONTAP** 命令行界面配置 **NTFS** 文件权限

您可以使用 ONTAP 命令行界面为文件和目录配置 NTFS 文件权限。这样，您就可以配置 NTFS 文件权限，而无需使用 Windows 客户端上的 SMB 共享连接到数据。

您可以通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（ DACL ）添加条目来配置 NTFS 文件权限。然后，安全描述符将应用于 NTFS 文件和目录。

您只能使用命令行配置 NTFS 文件权限。您不能使用命令行界面配置 NFSv4 ACL 。

步骤

1. 创建NTFS安全描述符。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. 将DACL添加到NTFS安全描述符。

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. 创建文件/目录安全策略。

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

通过 **SMB** 访问文件时， **UNIX** 文件权限如何提供访问控制

FlexVol 卷可以采用以下三种安全模式之一： NTFS ， UNIX 或混合。无论安全模式如何，您都可以通过 SMB 访问数据；但是，要以 UNIX 有效安全模式访问数据，需要适当的 UNIX 文件权限。

通过 SMB 访问数据时，在确定用户是否有权执行请求的操作时，会使用多种访问控制：

- 导出权限

  配置 SMB 访问的导出权限是可选的。

- 共享权限
- 文件权限

  以下类型的文件权限可能会应用于用户要执行操作的数据：

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX 模式位

对于设置了 NFSv4 ACL 或 UNIX 模式位的数据，将使用 UNIX 模式权限来确定对数据的文件访问权限。SVM 管理员需要设置适当的文件权限，以确保用户有权执行所需的操作。

> 混合安全模式卷中的数据可能采用 NTFS 或 UNIX 有效安全模式。如果数据采用 UNIX 有效安全模式，则在确定数据的文件访问权限时会使用 NFSv4 权限或 UNIX 模式位。

使用动态访问控制（ **DAC** ）确保文件访问安全

您可以使用动态访问控制来保护访问安全，也可以在 Active Directory 中创建中央访问策略，并通过已应用的组策略对象（ GPO ）将这些策略应用于 SVM 上的文件和文件夹。您可以配置审核，以便在应用对中央访问策略所做的更改之前，使用中央访问策略暂存事件查看这些更改的影响。

CIFS 凭据的附加项

在动态访问控制之前， CIFS 凭据包括安全主体（用户）的身份和 Windows 组成员资格。通过动态访问控制，凭据中又添加了三种类型的信息：设备标识，设备声明和用户声明：

- 设备标识

  模拟用户的身份信息，但用户登录设备的身份和组成员资格除外。

- 设备声明

  有关设备安全主体的断言。例如，设备声明可能是它是特定 OU 的成员。

- 用户声明

  有关用户安全主体的断言。例如，用户声明可能是其 AD 帐户是特定 OU 的成员。

中央访问策略

通过文件的中央访问策略，组织可以使用用户组，用户声明，设备声明和资源属性集中部署和管理包括条件表达式在内的授权策略。

例如，要访问对业务影响较高的数据，用户必须是全职员工，并且只能从受管设备访问数据。中央访问策略在 Active Directory 中定义，并通过 GPO 机制分发到文件服务器。

具有高级审核功能的中央访问策略暂存

中央访问策略可以是 " `stated` " ，在这种情况下，在文件访问检查期间会以 "`what - if` " 的方式对其进行评估。如果策略有效，会发生什么情况以及这与当前配置有何不同，则会将结果记录为审核事件。通过这种方式，管理员可以使用审核事件日志来研究访问策略更改的影响，然后再实际应用该策略。在评估访问策略更改的影响后，可以通过 GPO 将此策略部署到所需的 SVM 。

相关信息

支持的 GPO

将组策略对象应用于 CIFS 服务器

在 CIFS 服务器上启用或禁用 GPO 支持

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

显示有关动态访问控制安全性的信息

"SMB 和 NFS 审核和安全跟踪"

支持的动态访问控制功能

如果要在 CIFS 服务器上使用动态访问控制（DAC），则需要了解 ONTAP 如何在 Active Directory 环境中支持动态访问控制功能。

支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 支持以下功能：

功能	注释
声明到文件系统	声明是简单的名称和值对，用于说明有关用户的一些事实。用户凭据包含声明信息、文件上的安全描述符可以执行包括声明检查在内的访问检查。这样，管理员可以更精细地控制谁可以访问文件。
文件访问检查的条件表达式	修改文件的安全参数时、用户可以将任意复杂的条件表达式添加到文件的安全描述符中。条件表达式可以包括对声明的检查。
通过中央访问策略集中控制文件访问	中央访问策略是存储在 Active Directory 中的一种 ACL，可以标记为文件。只有在磁盘上的安全描述符和带标记的中央访问策略的访问检查均允许访问时，才会授予对文件的访问权限。这样，管理员便可以从中央位置（AD）控制对文件的访问，而无需修改磁盘上的安全描述符。
中央访问策略暂存	增加了在不影响实际文件访问的情况下尝试安全更改的功能，方法是 " `staging` " 对中央访问策略的更改，并在审核报告中查看更改的影响。
支持使用 ONTAP 命令行界面显示有关中央访问策略安全性的信息	扩展 `vserver security file-directory show` 命令以显示有关应用的中央访问策略的信息。
包括中央访问策略的安全跟踪	扩展 `vserver security trace` 命令系列、以显示包含应用的中央访问策略相关信息的结果。

不支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 不支持以下功能：

功能	注释
NTFS 文件系统对象的自动分类	这是 ONTAP 不支持的 Windows 文件分类基础架构的扩展。
除中央访问策略暂存之外的高级审核	高级审核仅支持中央访问策略暂存。

对 **CIFS** 服务器使用动态访问控制和中央访问策略时的注意事项

在使用动态访问控制（DAC）和中央访问策略保护 CIFS 服务器上的文件和文件夹时，必须牢记一些注意事项。

如果策略规则为适用场景 **domain\administrator user**，则可以拒绝对 **root** 的 **NFS** 访问

在某些情况下，如果对 root 用户尝试访问的数据应用中央访问策略安全性，则可能会拒绝 NFS 对 root 的访问。如果中央访问策略包含应用于域 \ 管理员且根帐户映射到域 \ 管理员帐户的规则，则会发生问题描述。

您应将规则应用于具有管理权限的组，例如 domain\administrator 组，而不是将规则应用于 domain\administrator 用户。通过这种方式，您可以将 root 映射到域 \ 管理员帐户，而不会使 root 受到此问题描述的影响。

如果在**Active Directory**中找不到应用的中央访问策略、则**CIFS**服务器的**BUILTIN\Administrators**组可以访问资源

CIFS 服务器中包含的资源可能已应用中央访问策略，但当 CIFS 服务器使用中央访问策略的 SID 尝试从 Active Directory 检索信息时， SID 与 Active Directory 中的任何现有中央访问策略 SID 不匹配。在这些情况下， CIFS 服务器会对该资源应用本地默认恢复策略。

本地默认恢复策略允许 CIFS 服务器的 BUILTIN\Administrators 组访问该资源。

启用或禁用动态访问控制概述

默认情况下，用于使用动态访问控制（DAC）保护 CIFS 服务器上的对象的选项处于禁用状态。如果要在 CIFS 服务器上使用动态访问控制，则必须启用此选项。如果您稍后决定不使用动态访问控制来保护存储在 CIFS 服务器上的对象，则可以禁用此选项。

关于此任务

启用动态访问控制后，文件系统可以包含具有与动态访问控制相关的条目的 ACL 。如果禁用了动态访问控制，则会忽略当前的动态访问控制条目，并且不允许输入新条目。

此选项仅在高级权限级别可用。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

动态访问控制的目标位置	输入命令 …

enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 返回到管理员权限级别： `set -privilege admin`

相关信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

禁用动态访问控制时，管理包含动态访问控制 ACE 的 ACL

如果您的资源使用动态访问控制 ACE 应用 ACL ，并且您在 Storage Virtual Machine （ SVM ）上禁用了动态访问控制，则必须先删除动态访问控制 ACE ，然后才能管理该资源上的非动态访问控制 ACE 。

关于此任务

禁用动态访问控制后，在删除现有动态访问控制 ACE 之前，您无法删除现有的非动态访问控制 ACE 或添加新的非动态访问控制 ACE 。

您可以使用通常用于管理 ACL 的任何工具来执行这些步骤。

步骤

1. 确定对资源应用了哪些动态访问控制 ACE 。
2. 从资源中删除动态访问控制 ACE 。
3. 根据需要在资源中添加或删除非动态访问控制 ACE 。

配置中央访问策略以保护 CIFS 服务器上的数据安全

要使用中央访问策略保护对 CIFS 服务器上数据的访问，您必须执行几个步骤，包括在 CIFS 服务器上启用动态访问控制（ DAC ），在 Active Directory 中配置中央访问策略，将中央访问策略应用于具有 GPO 的 Active Directory 容器， 并在 CIFS 服务器上启用 GPO 。

开始之前

- 必须将 Active Directory 配置为使用中央访问策略。
- 您必须对 Active Directory 域控制器具有足够的访问权限，才能创建中央访问策略，并创建 GPO 并将其应用于包含 CIFS 服务器的容器。
- 您必须对 Storage Virtual Machine （ SVM ）具有足够的管理访问权限才能执行必要的命令。

关于此任务

中央访问策略已定义并应用于 Active Directory 上的组策略对象（ GPO ）。有关配置中央访问策略和 GPO 的说明，请参见 Microsoft TechNet 库。

"Microsoft TechNet 库"

步骤

1. 如果尚未使用启用动态访问控制、请在SVM上启用它 `vserver cifs options modify` 命令：

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 如果尚未使用启用组策略对象(GPO)、请在CIFS服务器上启用它们 `vserver cifs group-policy modify` 命令：

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. 在 Active Directory 上创建中央访问规则和中央访问策略。
4. 创建组策略对象（ GPO ）以在 Active Directory 上部署中央访问策略。
5. 将 GPO 应用于 CIFS 服务器计算机帐户所在的容器。
6. 使用手动更新应用于CIFS服务器的GPO `vserver cifs group-policy update` 命令：

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. 使用验证是否已将GPO中央访问策略应用于CIFS服务器上的资源 `vserver cifs group-policy show-applied` 命令：

   以下示例显示默认域策略具有两个应用于 CIFS 服务器的中央访问策略：

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ------------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
         Event Audit and Event Log:
             Audit Logon Events: none
             Audit Object Access: success
             Log Retention Method: overwrite-as-needed
             Max Log Size: 16384
         File Security:
             /vol1/home
   ```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
 2 entries were displayed.
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

启用或禁用动态访问控制

显示有关动态访问控制安全性的信息

您可以显示 NTFS 卷上的动态访问控制（DAC）安全性信息，以及混合安全模式卷上使用 NTFS 有效安全性的数据信息。其中包括有关条件 ACE，资源 ACE 和中央访问策略 ACE 的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （SVM）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`

要显示信息的项	输入以下命令 ...
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
其中输出显示有组和用户 SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
关于十六进制位掩码转换为文本格式的文件和目录的文件和目录安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

示例

以下示例显示了有关路径的动态访问控制安全信息 `/vol1` 在SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

动态访问控制的还原注意事项

您应了解还原到不支持动态访问控制（DAC）的 ONTAP 版本时会发生什么情况，以及还原前后必须执行哪些操作。

如果要将集群还原到不支持动态访问控制的 ONTAP 版本，并且在一个或多个 Storage Virtual Machine （SVM）上启用了动态访问控制，则必须在还原之前执行以下操作：

- 您必须在集群上启用动态访问控制的所有 SVM 上禁用动态访问控制。
- 您必须修改包含的集群上的任何审核配置 `cap-staging` 仅使用的事件类型 `file-op` 事件类型。

对于具有动态访问控制 ACE 的文件和文件夹，您必须了解一些重要的还原注意事项并采取相应措施：

- 如果还原集群，则不会删除现有动态访问控制 ACE ；但是，在文件访问检查中将忽略这些 ACE 。
- 由于还原后将忽略动态访问控制 ACE ，因此使用动态访问控制 ACE 的文件将更改对文件的访问。

  这样，用户就可以访问以前无法访问的文件，或者无法访问以前可以访问的文件。

- 您应将非动态访问控制 ACE 应用于受影响的文件，以还原其先前的安全级别。

  可以在还原之前或还原完成后立即执行此操作。

> 由于还原后会忽略动态访问控制 ACE ，因此在将非动态访问控制 ACE 应用于受影响的文件时，您无需删除它们。但是，如果需要，您可以手动将其删除。

从何处查找有关配置和使用动态访问控制和中央访问策略的追加信息

我们还提供了其他资源来帮助您配置和使用动态访问控制和中央访问策略。

您可以在 Microsoft TechNet 库中找到有关如何在 Active Directory 上配置动态访问控制和中央访问策略的信息。

"Microsoft TechNet ： 动态访问控制场景概述"

"Microsoft TechNet ： 中央访问策略场景"

以下参考资料可帮助您将SMB服务器配置为使用和支持动态访问控制和中央访问策略：

- *在SMB服务器上使用GPO *

  将组策略对象应用于SMB服务器

- 在**SMB**服务器上配置**NAS**审核

  "SMB 和 NFS 审核和安全跟踪"

使用导出策略确保**SMB**访问安全

如何在 **SMB** 访问中使用导出策略

如果在SMB服务器上启用了SMB访问导出策略、则在控制SMB客户端对SVM卷的访问时会使用导出策略。要访问数据，您可以创建一个允许 SMB 访问的导出策略，然后将该策略与包含 SMB 共享的卷相关联。

导出策略应用了一个或多个规则，用于指定允许哪些客户端访问数据以及只读和读写访问支持哪些身份验证协议。您可以配置导出策略，以允许通过 SMB 访问所有客户端，一个子网客户端或特定客户端，并允许在确定对数据的只读和读写访问时使用 Kerberos 身份验证， NTLM 身份验证或 Kerberos 和 NTLM 身份验证进行身份验证。

在处理应用于导出策略的所有导出规则后， ONTAP 可以确定是否授予客户端访问权限以及授予的访问级别。导出规则适用于客户端计算机，而不适用于 Windows 用户和组。导出规则不会取代基于 Windows 用户和组的身份验证和授权。除了共享和文件访问权限之外，导出规则还提供了另一层访问安全性。

您只需将一个导出策略关联到每个卷，即可配置客户端对卷的访问。每个 SVM 可以包含多个导出策略。这样，您可以对包含多个卷的 SVM 执行以下操作：

- 为 SVM 的每个卷分配不同的导出策略，以便对 SVM 中的每个卷进行单个客户端访问控制。
- 为 SVM 的多个卷分配相同的导出策略，以实现相同的客户端访问控制，而无需为每个卷创建新的导出策略。

每个 SVM 至少有一个名为 `default` 的导出策略，该策略不包含任何规则。您不能删除此导出策略，但可以重命名或修改它。默认情况下， SVM 上的每个卷都与默认导出策略相关联。如果在 SVM 上禁用了 `d`访问导出策略，则 `"'` 默认 `''`导出策略对 SMB 访问没有任何影响。

您可以配置规则以提供对 NFS 和 SMB 主机的访问，并将该规则与导出策略关联，然后导出策略可以与包含 NFS 和 SMB 主机都需要访问的数据的卷关联。或者，如果某些卷中只有 SMB 客户端需要访问，则可以为导出策略配置规则，这些规则只允许使用 SMB 协议进行访问，并且仅使用 Kerberos 或 NTLM （或两者）进行只读和写访问身份验证。然后，导出策略将与只需要 SMB 访问的卷相关联。

如果启用了 SMB 的导出策略，并且客户端发出适用导出策略不允许的访问请求，则此请求将失败，并显示权限被拒绝的消息。如果客户端与卷导出策略中的任何规则不匹配，则访问将被拒绝。如果导出策略为空，则会隐式拒绝所有访问。即使共享和文件权限允许访问，也是如此。这意味着，您必须将导出策略配置为在包含 SMB 共享的卷上至少允许以下内容：

- 允许访问所有客户端或相应的部分客户端
- 允许通过 SMB 进行访问
- 允许使用 Kerberos 或 NTLM 身份验证（或这两者）进行适当的只读和写访问

了解相关信息 "配置和管理导出策略"。

导出规则的工作原理

导出规则是导出策略的功能要素。导出规则会根据您配置的特定参数将客户端对卷的访问请求进行匹配，以确定如何处理客户端访问请求。

导出策略必须至少包含一个导出规则，才能访问客户端。如果导出策略包含多个规则，则这些规则将按照它们在导出策略中的显示顺序进行处理。规则顺序由规则索引编号决定。如果某个规则与客户端匹配，则会使用该规则的权限，而不再处理其他规则。如果没有匹配的规则，客户端将被拒绝访问。

您可以使用以下条件配置导出规则以确定客户端访问权限：

- 发送请求的客户端使用的文件访问协议，例如 NFSv4 或 SMB 。
- 客户端标识符，例如主机名或 IP 地址。

  的最大大小 `-clientmatch` 字段为4096个字符。

- 客户端用于进行身份验证的安全类型，例如 Kerberos v5 ， NTLM 或 AUTH_SYS 。

如果某个规则指定了多个条件，则客户端必须与所有条件匹配，才能应用此规则。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用 NFSv3 协议发送，并且客户端的 IP 地址为 10.1.17.37 。

即使客户端访问协议匹配，客户端的 IP 地址也与导出规则中指定的 IP 地址位于不同的子网中。因此，客户端匹配失败，此规则不适用于此客户端。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用NFSv4协议发送、客户端的IP地址为10.1.16.54。

客户端访问协议匹配，并且客户端的 IP 地址位于指定子网中。因此，客户端匹配成功，此规则将适用场景此客户端。无论安全类型如何，客户端都可以获得读写访问权限。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

客户端 1 的 IP 地址为 10.1.16.207 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

这两个客户端的客户端访问协议和 IP 地址匹配。只读参数允许对所有客户端进行只读访问，而不管客户端使用哪种安全类型进行身份验证。因此，这两个客户端都将获得只读访问权限。但是，只有客户端 1 获得读写访问权限，因为它使用经过批准的安全类型 Kerberos v5 进行身份验证。客户端 2 不会获得读写访问权限。

这些示例显示了如何在启用了 SMB 访问导出策略的 SVM 上创建导出策略规则来限制或允许通过 SMB 进行访问。

默认情况下， SMB 访问的导出策略处于禁用状态。只有在为 SMB 访问启用了导出策略时，您才需要配置导出策略规则来限制或允许通过 SMB 进行访问。

仅适用于 **SMB** 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifs1
- 索引号： 1
- 客户端匹配：仅匹配 192.168.1.0/24 网络上的客户端
- 协议：仅启用 SMB 访问
- 只读访问：使用 NTLM 或 Kerberos 身份验证的客户端
- 读写访问：使用 Kerberos 身份验证的客户端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB 和 **NFS** 访问的导出规则

以下命令会在名为 "` vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifsnfs1.
- 索引编号：2
- 客户端匹配：匹配所有客户端
- 协议： SMB 和 NFS 访问
- 只读访问：对所有客户端
- 读写访问：使用 Kerberos （ NFS 和 SMB ）或 NTLM 身份验证（ SMB ）的客户端
- 映射 UNIX 用户 ID 0 （零）：映射到用户 ID 65534 （通常映射到用户名 nobody ）
- SUID 和 sgid 访问：允许

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

仅使用 **NTLM** 进行 **SMB** 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称：ntlm1
- 索引号： 1
- 客户端匹配：匹配所有客户端
- 协议：仅启用 SMB 访问
- 只读访问：仅适用于使用 NTLM 的客户端
- 读写访问：仅适用于使用 NTLM 的客户端

> 如果为仅限 NTLM 的访问配置只读选项或读写选项，则必须在客户端匹配选项中使用基于 IP 地址的条目。否则、您将收到 `access denied` 错误。这是因为 ONTAP 在使用主机名检查客户端的访问权限时使用 Kerberos 服务主体名称（ SPN ）。NTLM 身份验证不支持 SPN 名称。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

启用或禁用 **SMB** 访问导出策略

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用 SMB 访问导出策略。可以选择使用导出策略控制 SMB 对资源的访问。

开始之前

以下是为 SMB 启用导出策略的要求：

- 在为客户端创建导出规则之前，客户端必须在 DNS 中具有 "`PTR` " 记录。
- 如果 SVM 提供对 NFS 客户端的访问权限，并且要用于 NFS 访问的主机名与 CIFS 服务器名称不同，则需要为主机名另外设置一组 "`A` " 和 "`PTR` " 记录。

关于此任务

默认情况下，在 SVM 上设置新的 CIFS 服务器时，不会使用导出策略进行 SMB 访问。如果要根据身份验证协议或客户端 IP 地址或主机名控制访问，则可以为 SMB 访问启用导出策略。您可以随时为 SMB 访问启用或禁用导出策略。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 启用或禁用导出策略：
   - 启用导出策略： `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - 禁用导出策略： `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例支持使用导出策略控制 SMB 客户端对 SVM vs1 上资源的访问：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

使用存储级别访问防护确保文件访问安全

使用存储级别访问防护确保文件访问安全

除了使用原生文件级别以及导出和共享安全性来保护访问之外，您还可以配置存储级别访问防护，这是 ONTAP 在卷级别应用的第三层安全保护。从所有 NAS 协议到应用它的存储对象的存储级别访问防护适用场景访问。

仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

存储级别访问防护行为

- 存储级别访问防护适用场景存储对象中的所有文件或所有目录。

  由于卷中的所有文件或目录都受存储级别访问防护设置的限制，因此不需要通过传播进行继承。

- 您可以将存储级别访问防护配置为仅应用于文件，仅应用于目录或同时应用于卷中的文件和目录。
  - 文件和目录安全性

    适用场景存储对象中的每个目录和文件。这是默认设置。

  - 文件安全性

    适用场景存储对象中的每个文件。应用此安全性不会影响对目录的访问或审核。

  - 目录安全性

    适用场景存储对象中的每个目录。应用此安全性不会影响对文件的访问或审核。

- 存储级别访问防护用于限制权限。

  它不会提供额外的访问权限。

- 如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则看不到存储级别访问防护安全性。

  它会在存储对象级别应用，并存储在用于确定有效权限的元数据中。

- 即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别的安全性。

  它只能由存储管理员进行修改。

- 您可以将存储级别访问防护应用于采用 NTFS 或混合安全模式的卷。
- 只要包含该卷的 SVM 配置了 CIFS 服务器，您就可以对采用 UNIX 安全模式的卷应用存储级别访问防护。
- 如果卷挂载在卷接合路径下，并且该路径上存在存储级别访问防护，则该防护不会传播到挂载在该路径下的卷。
- 存储级别访问防护安全描述符可通过 SnapMirror 数据复制和 SVM 复制进行复制。
- 病毒扫描程序具有特殊例外。

  即使存储级别访问防护拒绝访问对象，也允许对这些服务器进行异常访问以筛选文件和目录。

- 如果由于存储级别访问防护而拒绝访问，则不会发送 FPolicy 通知。

访问检查的顺序

文件或目录的访问取决于导出或共享权限，卷上设置的存储级别访问防护权限以及应用于文件和 / 或目录的原生文件权限的组合效果。系统会评估所有级别的安全性，以确定文件或目录具有哪些有效权限。安全访问检查按以下顺序执行：

1. SMB 共享或 NFS 导出级别权限
2. 存储级别访问防护
3. NTFS 文件 / 文件夹访问控制列表（ ACL ）， NFSv4 ACL 或 UNIX 模式位

使用存储级别访问防护的用例

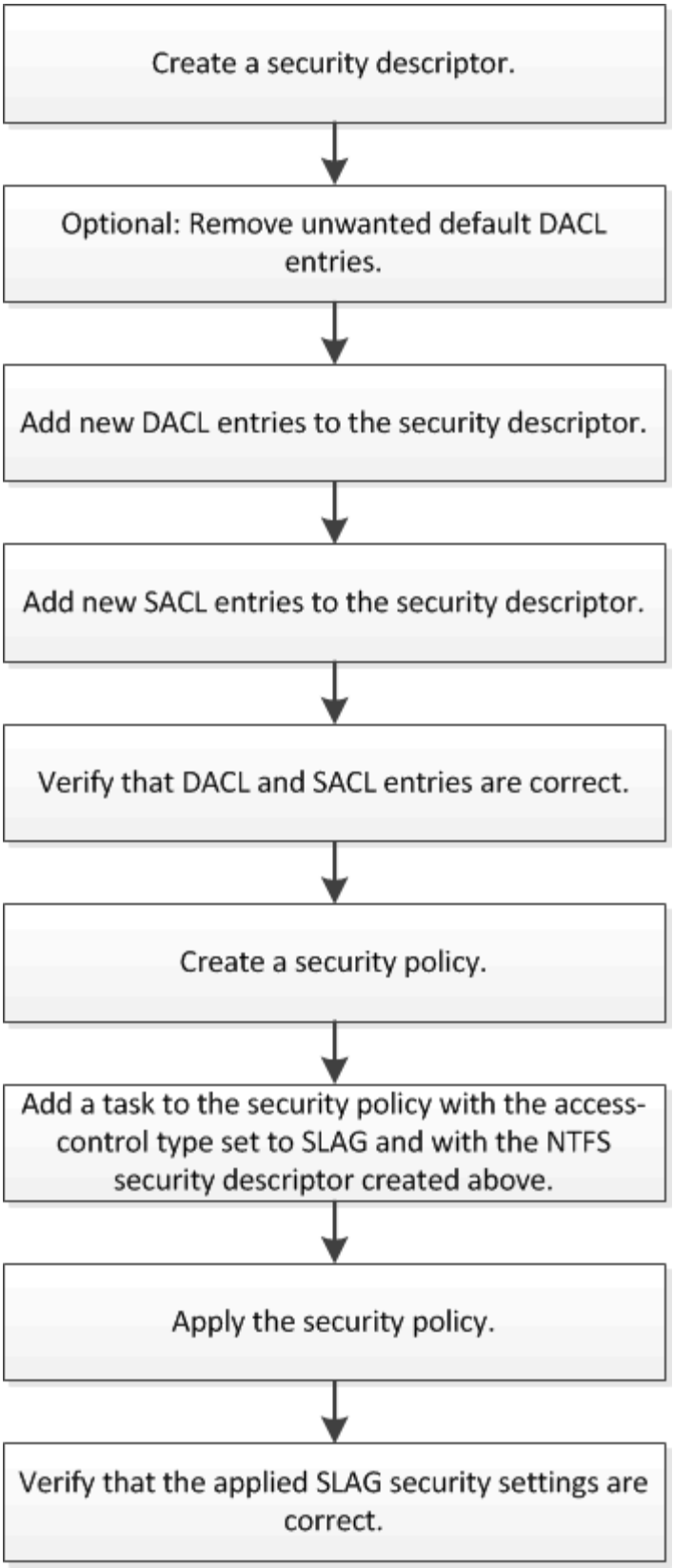
存储级别访问防护可在存储级别提供额外的安全性，这在客户端不可见；因此，任何用户或管理员都无法从其桌面撤消此功能。在某些使用情形下，在存储级别控制访问的功能会很有用。

此功能的典型使用情形包括以下情形：

- 通过审核和控制所有用户在存储级别的` 访问来保护知识产权
- 为金融服务公司提供存储，包括银行和交易团队
- 为各个部门提供单独的文件存储的政府服务
- 保护所有学生档案的大学

用于配置存储级别访问防护的工作流

配置存储级别访问防护（ SLAG ）的工作流使用与配置 NTFS 文件权限和审核策略相同的 ONTAP 命令行界面命令。您无需在指定目标上配置文件和目录访问，而是在指定的 Storage Virtual Machine （ SVM ）卷上配置 SLAG 。



相关信息

配置存储级别访问防护

要在卷或 qtree 上配置存储级别访问防护，需要执行多个步骤。存储级别访问防护可提供在存储级别设置的访问安全性级别。它可以确保从所有 NAS 协议对应用了该协议的存储对象进行的所有访问均通过适用场景进行安全保护。

步骤

1. 使用创建安全描述符 `vserver security file-directory ntfs create` 命令：

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1` `vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   系统将使用以下四个默认 DACL 访问控制条目（ACE ）创建安全描述符：

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   如果您不想在配置存储级别访问防护时使用默认条目，则可以在创建自己的 ACE 并将其添加到安全描述符之前将其删除。

2. 从安全描述符中删除不希望配置存储级别访问防护安全性的任何默认 DACL ACE：

   a. 使用删除任何不需要的DACL ACL ACL `vserver security file-directory ntfs dacl remove` 命令：

在此示例中，将从安全描述符中删除三个默认 DACL ACE： BUILTIN\Administrators， BUILTIN\Users 和 Creator OWNER。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. 使用验证是否已从安全描述符中删除不想用于存储级别访问防护安全性的DACL ACL ACL ACL `vserver security file-directory ntfs dacl show` 命令：

在此示例中，命令的输出将验证是否已从安全描述符中删除三个默认 DACL ACE，而仅保留 NT AUTHORITY\SYSTEM 默认 DACL ACE 条目：

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 使用向安全描述符添加一个或多个DACL条目 `vserver security file-directory ntfs dacl add` 命令：

在此示例中，将两个 DACL ACE 添加到安全描述符中：

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. 使用向安全描述符添加一个或多个SACL条目 `vserver security file-directory ntfs sacl add` 命令：

在此示例中、将两个SACL Aces添加到安全描述符中：

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. 使用验证是否已正确配置DACL和SACL ACL `vserver security file-directory ntfs dacl show`

和 `vserver security file-directory ntfs sacl show` 命令。

在此示例中，以下命令显示有关安全描述符 " `sD1` " 的 DACL 条目的信息：

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

在此示例中、以下命令显示有关安全描述符"`sd1`"的SACL条目的信息：

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. 使用创建安全策略 `vserver security file-directory policy create` 命令：

   以下示例将创建一个名为 "`policy1` " 的策略：

```
vserver security file-directory policy create -vserver vs1 -policy-name
policy1
```

7. 使用验证是否已正确配置此策略 `vserver security file-directory policy show` 命令：

   `vserver security file-directory policy show`

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. 使用将具有关联安全描述符的任务添加到安全策略中 `vserver security file-directory policy task add` 命令 `-access-control` 参数设置为 `slag`。

   即使策略可以包含多个存储级别访问防护任务，您也无法将策略配置为同时包含文件目录和存储级别访问防护任务。策略必须包含所有存储级别访问防护任务或所有文件目录任务。

   在此示例中，将任务添加到名为 "`policy1` " 的策略中，该策略分配给安全描述符 " `sD1` " 。它将分配给 `/datavol1` 访问控制类型设置为`slag`的路径。

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1`

9. 使用验证是否已正确配置此任务 `vserver security file-directory policy task show` 命令：

   `vserver security file-directory policy task show -vserver vs1 -policy-name policy1`

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
      -----  -----------  ---------------  --------  ----------
   ---------------
      1      /datavol1    slag             ntfs      propagate  sd1
   ```

10. 使用应用存储级别访问防护安全策略 `vserver security file-directory apply` 命令：

    `vserver security file-directory apply -vserver vs1 -policy-name policy1`

    已计划应用安全策略的作业。

11. 使用验证应用的存储级别访问防护安全设置是否正确 `vserver security file-directory show` 命令：

    在此示例中、命令的输出显示已对NTFS卷应用存储级别访问防护安全性 `/datavol1`。即使默认 DACL 允

许对所有人进行完全控制，存储级别访问防护安全性也会限制（和审核）对存储级别访问防护设置中定义的组的访问。

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```
                 Vserver: vs1
               File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

相关信息

使用命令行界面管理 SVM 上的 NTFS 文件安全性， NTFS 审核策略和存储级别访问防护

用于配置存储级别访问防护的工作流

显示有关存储级别访问防护的信息

正在删除存储级别访问防护

有效的 **SLAG** 列表

您可以在卷或 qtree 上配置 SLAG ，也可以同时在这两者上配置 SLAG 。SLAG 列表定义了在表中列出的各种情形下适用的 SLAG 配置所在的卷或 qtree 。

	AFS 中的卷 **SLAG**	**Snapshot** 副本中的卷 **SLAG**	**AFS** 中的 **qtree SLAG**	**Snapshot** 副本中的 **qtree SLAG**
访问文件系统（AFS）中的卷访问	是的。	否	不适用	不适用
Snapshot 副本中的卷访问	是的。	否	不适用	不适用
AFS 中的 qtree 访问（当 qtree 中存在 SLAG 时）	否	否	是的。	否
AFS 中的 qtree 访问（当 qtree 中不存在 SLAG 时）	是的。	否	否	否
Snapshot 副本中的 qtree 访问（当 qtree AFS 中存在 SLAG 时）	否	否	是的。	否
Snapshot 副本中的 qtree 访问（当 qtree AFS 中不存在 SLAG 时）	是的。	否	否	否

显示有关存储级别访问防护的信息

存储级别访问防护是应用于卷或 qtree 的第三层安全保护。无法使用 Windows 属性窗口查看存储级别访问防护设置。您必须使用 ONTAP 命令行界面查看有关存储级别访问防护安全性的信息，您可以使用这些信息验证配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （SVM）的名称以及要显示其存储级别访问防护安全信息的卷或 qtree 的路径。您可以摘要形式或详细列表形式显示输出。

步骤

1. 使用所需的详细信息级别显示存储级别访问防护安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示路径为的NTFS安全模式卷的存储级别访问防护安全信息 `/datavol1` 在SVM VS1中：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

以下示例显示路径中混合安全模式卷的存储级别访问防护信息 `/datavol5` 在SVM VS1中。此卷的顶层具有UNIX 有效安全性。此卷具有存储级别访问防护安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

删除存储级别访问防护

如果您不再需要在存储级别设置访问安全性，则可以删除卷或 qtree 上的存储级别访问防护。删除存储级别访问防护不会修改或删除常规 NTFS 文件和目录安全性。

步骤

1. 使用验证卷或qtree是否已配置存储级别访问防护 `vserver security file-directory show` 命令：

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                 Vserver: vs1
               File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. 使用删除存储级别访问防护 `vserver security file-directory remove-slag` 命令：

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. 使用验证是否已从卷或qtree中删除存储级别访问防护 `vserver security file-directory show` 命令：

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                 Vserver: vs1
               File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

使用 SMB 管理文件访问

使用本地用户和组进行身份验证和授权

ONTAP 如何使用本地用户和组

本地用户和组概念

在确定是否在环境中配置和使用本地用户和组之前，您应了解什么是本地用户和组以及有关它们的一些基本信息。

- * 本地用户 *

  具有唯一安全标识符（ SID ）的用户帐户，仅在创建该帐户的 Storage Virtual Machine （ SVM ）上可见。本地用户帐户具有一组属性，包括用户名和 SID 。本地用户帐户使用 NTLM 身份验证在 CIFS 服务器上进行本地身份验证。

  用户帐户有多种用途：

  - 用于向用户授予 *User Rights Management* 权限。
  - 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。
- * 本地组 *

具有唯一 SID 的组只能在其创建所在的 SVM 上显示。组包含一组成员。成员可以是本地用户，域用户，域组和域计算机帐户。可以创建，修改或删除组。

组有多种用途：

- 用于向其成员授予 *User Rights Management* 权限。
- 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。

* 本地域 *

具有本地作用域的域，该域受 SVM 的限制。本地域的名称是 CIFS 服务器名称。本地用户和组包含在本地域中。

* 安全标识符（ SID ） *

SID 是一个可变长度的数值，用于标识 Windows 模式的安全主体。例如，典型的 SID 采用以下形式： S-1-5-21-3139654847-1303905135-2517279418-123456 。

* NTLM 身份验证 *

一种 Microsoft Windows 安全方法，用于对 CIFS 服务器上的用户进行身份验证。

* 集群复制数据库（ RDB ） *

一个复制的数据库，其中集群中的每个节点上都有一个实例。本地用户和组对象存储在 RDB 中。

创建本地用户和本地组的原因

在 Storage Virtual Machine （ SVM ）上创建本地用户和本地组的原因有多种。例如，如果域控制器（ DC ）不可用，您可能希望使用本地组分配权限或 SMB 服务器位于工作组中，则可以使用本地用户帐户访问 SMB 服务器。

您可以出于以下原因创建一个或多个本地用户帐户：

- SMB 服务器位于工作组中，域用户不可用。

  在工作组配置中需要本地用户。

- 您希望在域控制器不可用时能够进行身份验证并登录到 SMB 服务器。

  当域控制器关闭或网络问题导致 SMB 服务器无法联系域控制器时，本地用户可以使用 NTLM 身份验证向 SMB 服务器进行身份验证。

- 您希望将 *User Rights Management* 权限分配给本地用户。

  User Rights Management 是 SMB 服务器管理员控制用户和组对 SVM 拥有的权限的能力。您可以通过为用户的帐户分配权限或使用户成为具有这些权限的本地组的成员来为用户分配权限。

您可以出于以下原因创建一个或多个本地组：

- SMB 服务器位于工作组中，并且域组不可用。

工作组配置不需要本地组，但它们对于管理本地工作组用户的访问权限非常有用。

- 您希望通过使用本地组进行共享和文件访问控制来控制对文件和文件夹资源的访问。
- 您希望使用自定义的 *User Rights Management* 权限创建本地组。

  某些内置用户组具有预定义的权限。要分配一组自定义权限，您可以创建一个本地组并为该组分配必要的权限。然后，您可以将本地用户，域用户和域组添加到本地组。

相关信息

本地用户身份验证的工作原理

支持的权限列表

本地用户身份验证的工作原理

本地用户必须先创建经过身份验证的会话，然后才能访问 CIFS 服务器上的数据。

由于 SMB 基于会话，因此首次设置会话时，只需确定一次用户身份即可。CIFS 服务器在对本地用户进行身份验证时使用基于 NTLM 的身份验证。支持 NTLMv1 和 NTLMv2 。

ONTAP 在三种使用情形下使用本地身份验证。每个用例取决于用户名的域部分（采用 domain\user 格式）是否与 CIFS 服务器的本地域名（ CIFS 服务器名称）匹配：

- 域部分匹配

  请求访问数据时提供本地用户凭据的用户将在 CIFS 服务器上进行本地身份验证。

- 域部分不匹配

  ONTAP 尝试对 CIFS 服务器所属域中的域控制器使用 NTLM 身份验证。如果身份验证成功，则登录完成。如果失败，接下来会发生什么情况取决于身份验证失败的原因。

  例如，如果用户位于 Active Directory 中，但密码无效或已过期，则 ONTAP 不会尝试使用 CIFS 服务器上的相应本地用户帐户。相反，身份验证将失败。在其他情况下， ONTAP 会使用 CIFS 服务器上的相应本地帐户（如果存在）进行身份验证，即使 NetBIOS 域名不匹配也是如此。例如，如果存在匹配的域帐户，但该帐户已禁用，则 ONTAP 会使用 CIFS 服务器上的相应本地帐户进行身份验证。

- 未指定域部分

  ONTAP 首先尝试以本地用户身份进行身份验证。如果以本地用户身份进行身份验证失败，则 ONTAP 会使用 CIFS 服务器所属域中的域控制器对用户进行身份验证。

成功完成本地或域用户身份验证后， ONTAP 将根据本地组成员资格和权限构建完整的用户访问令牌。

有关本地用户的 NTLM 身份验证的详细信息，请参见 Microsoft Windows 文档。

相关信息

启用或禁用本地用户身份验证

如何构建用户访问令牌

当用户映射共享时，将建立经过身份验证的 SMB 会话，并构建用户访问令牌，其中包含有关用户，用户的组成员资格和累积权限以及映射的 UNIX 用户的信息。

除非禁用此功能，否则本地用户和组信息也会添加到用户访问令牌中。构建访问令牌的方式取决于登录用户是本地用户还是 Active Directory 域用户：

- 本地用户登录

  尽管本地用户可以是不同本地组的成员，但本地组不能是其他本地组的成员。本地用户访问令牌由分配给特定本地用户所属组的所有权限组成。

- 域用户登录

  域用户登录时， ONTAP 会获取一个用户访问令牌，该令牌包含用户所属的所有域组的用户 SID 和 SID 。ONTAP 使用域用户访问令牌与用户域组的本地成员资格（如果有）提供的访问令牌以及分配给域用户或其任何域组成员资格的任何直接权限进行联合。

对于本地和域用户登录，还会为用户访问令牌设置主组 RID 。默认RID `Domain Users` (里德513)。您不能更改默认值。

Windows 到 UNIX 和 UNIX 到 Windows 名称映射过程会对本地帐户和域帐户遵循相同的规则。

> 从 UNIX 用户到本地帐户没有隐含的自动映射。如果需要，必须使用现有名称映射命令指定显式映射规则。

在包含本地组的 **SVM** 上使用 **SnapMirror** 的准则

在包含本地组的 SVM 所拥有的卷上配置 SnapMirror 时，应了解相关准则。

您不能在应用于 SnapMirror 复制到另一个 SVM 的文件，目录或共享的 ACE 中使用本地组。如果您使用 SnapMirror 功能为另一个 SVM 上的卷创建 DR 镜像，并且该卷具有本地组的 ACE ，则 ACE 在该镜像上无效。如果将数据复制到其他 SVM ，则数据会有效地跨越到其他本地域。授予本地用户和组的权限仅在最初创建这些用户和组的 SVM 的范围内有效。

删除 **CIFS** 服务器时本地用户和组会发生什么情况

默认的本地用户和组集是在创建 CIFS 服务器时创建的，它们与托管 CIFS 服务器的 Storage Virtual Machine （ SVM ）相关联。SVM 管理员可以随时创建本地用户和组。您需要了解删除 CIFS 服务器时本地用户和组会发生什么情况。

本地用户和组与 SVM 关联；因此，出于安全考虑，删除 CIFS 服务器时不会删除它们。虽然删除 CIFS 服务器时不会删除本地用户和组，但它们是隐藏的。在 SVM 上重新创建 CIFS 服务器之前，您无法查看或管理本地用户和组。

> CIFS 服务器管理状态不会影响本地用户或组的可见性。

如何对本地用户和组使用 **Microsoft** 管理控制台

您可以从 Microsoft 管理控制台查看有关本地用户和组的信息。使用此版本的 ONTAP ，您无法从 Microsoft 管理控制台为本地用户和组执行其他管理任务。

还原准则

如果您计划将集群还原到不支持本地用户和组的 ONTAP 版本，并且正在使用本地用户和组管理文件访问或用户权限，则必须了解某些注意事项。

- 由于安全原因，在将 ONTAP 还原到不支持本地用户和组功能的版本时，不会删除有关已配置的本地用户，组和权限的信息。
- 还原到 ONTAP 的先前主要版本后， ONTAP 在身份验证和凭据创建期间不会使用本地用户和组。
- 不会从文件和文件夹 ACL 中删除本地用户和组。
- 如果文件访问请求取决于因向本地用户或组授予权限而授予的访问权限，则这些请求将被拒绝。

  要允许访问，您必须重新配置文件权限，以允许基于域对象而不是本地用户和组对象进行访问。

什么是本地权限

支持的权限列表

ONTAP 具有一组预定义的受支持权限。默认情况下，某些预定义的本地组已添加其中一些权限。此外，您还可以从预定义组添加或删除权限，或者创建新的本地用户或组，并向您创建的组或现有域用户和组添加权限。

下表列出了 Storage Virtual Machine （ SVM ）上支持的权限，并列出了已分配权限的 BUILTIN 组：

权限名称	默认安全设置	**Description**
`SeTcbPrivilege`	无	作为操作系统的一部分
`SeBackupPrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	备份文件和目录，覆盖所有 ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	还原文件和目录，覆盖任何 ACL 会将任何有效的用户或组 SID 设置为文件所有者
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	获取文件或其他对象的所有权
`SeSecurityPrivilege`	`BUILTIN\Administrators`	管理审核 其中包括查看、转储和清除安全日志。

权限名称	默认安全设置	Description
SeChangeNotifyPrivilege	BUILTIN\Administrators，BUILTIN\Backup Operators，BUILTIN\Power Users，BUILTIN\Users， Everyone	绕过遍历检查 具有此权限的用户无需具有遍历(x)权限即可遍历文件夹、符号链接或接合。

相关信息

- 分配本地权限
- 配置绕过遍历检查

分配权限

您可以直接为本地用户或域用户分配权限。或者，您也可以将用户分配给已分配权限与这些用户所需功能匹配的本地组。

- 您可以为创建的组分配一组权限。

  然后，将用户添加到具有所需权限的组。

- 您还可以将本地用户和域用户分配给默认权限与要授予这些用户的权限匹配的预定义组。

相关信息

- 向本地或域用户或组添加权限
- 从本地或域用户或组中删除权限
- 重置本地或域用户和组的权限
- 配置绕过遍历检查

使用 **BUILTIN** 组和本地管理员帐户的准则

使用 BUILTIN 组和本地管理员帐户时，应牢记一些特定准则。例如，您可以重命名本地管理员帐户，但不能删除此帐户。

- 管理员帐户可以重命名，但无法删除。
- 无法从 BUILTIN\Administrators 组中删除管理员帐户。
- BUILTIN 组可以重命名，但不能删除。

  重命名 BUILTIN 组后，可以使用已知名称创建另一个本地对象；但是，系统会为该对象分配一个新的 RID 。

- 没有本地来宾帐户。

相关信息

预定义的 BUILTIN 组和默认权限

本地用户密码的要求

默认情况下，本地用户密码必须满足复杂性要求。密码复杂度要求与 Microsoft Windows *local security policy* 中定义的要求类似。

密码必须满足以下条件：

- 长度必须至少为六个字符
- 不得包含用户帐户名称
- 必须包含以下四个类别中至少三个类别的字符：
  - 大写英文字符（A 到 Z）
  - 小写英文字符（a 到 z）
  - 基数为 10 位（0 到 9）
  - 特殊字符：

    ~@ # $ % ｛caret｝ & * _ - + = ` \ | （） [ ] ： ； " < > ， .? /

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

更改本地用户帐户密码

预定义的 **BUILTIN** 组和默认权限

您可以将本地用户或域用户的成员资格分配给 ONTAP 提供的一组预定义的 BUILTIN 组。预定义的组已分配预定义的权限。

下表介绍了预定义的组：

预定义的 **BUILTIN** 组	默认权限
`BUILTIN\Administrators`第544次 首次创建时、本地 `Administrator` ID为500的帐户将自动成为此组的成员。Storage Virtual Machine (SVM)加入域后、 `domain\Domain Admins` 将组添加到组中。如果SVM离开域、则 `domain\Domain Admins` 组将从组中删除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

预定义的 **BUILTIN** 组	默认权限
`BUILTIN\Power Users`547 首次创建时，此组没有任何成员。此组的成员具有以下特征： • 可以创建和管理本地用户和组。 • 无法将自身或任何其他对象添加到中 `BUILTIN\Administrators` 组。	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`第551号 首次创建时，此组没有任何成员。如果出于备份目的打开文件或文件夹，则此组的成员可以覆盖对这些文件或文件夹的读写权限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`545 首次创建时、此组没有任何成员(除了隐含的 `Authenticated Users` 特殊组)。当SVM加入域时、 `domain\Domain Users` 已将组添加到此组。如果SVM离开域、则 `domain\Domain Users` 已从此组中删除组。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此组包括所有用户，包括来宾（但不包括匿名用户）。这是具有隐含成员资格的隐含组。	`SeChangeNotifyPrivilege`

相关信息

使用 BUILTIN 组和本地管理员帐户的准则

支持的权限列表

配置绕过遍历检查

启用或禁用本地用户和组功能

启用或禁用本地用户和组功能概述

在使用本地用户和组访问 NTFS 安全模式数据之前，必须启用本地用户和组功能。此外，如果要使用本地用户进行 SMB 身份验证，则必须启用本地用户身份验证功能。

默认情况下，本地用户和组功能以及本地用户身份验证处于启用状态。如果未启用它们，则必须先启用它们，然后才能配置和使用本地用户和组。您可以随时禁用本地用户和组功能。

除了显式禁用本地用户和组功能之外，如果集群中的任何节点还原到不支持本地用户和组功能的 ONTAP 版本，则 ONTAP 还会禁用此功能。只有当集群中的所有节点都运行支持本地用户和组功能的 ONTAP 版本时，才会启

用此功能。

相关信息

修改本地用户帐户

修改本地组

向本地或域用户或组添加权限

启用或禁用本地用户和组

您可以在 Storage Virtual Machine （SVM）上启用或禁用 SMB 访问的本地用户和组。默认情况下，本地用户和组功能处于启用状态。

关于此任务

您可以在配置 SMB 共享和 NTFS 文件权限时使用本地用户和组，也可以选择在创建 SMB 连接时使用本地用户进行身份验证。要使用本地用户进行身份验证，还必须启用本地用户和组身份验证选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

希望本地用户和组 ...	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户和组功能：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

相关信息

启用或禁用本地用户身份验证

启用或禁用本地用户帐户

启用或禁用本地用户身份验证

您可以为 Storage Virtual Machine （SVM）上的 SMB 访问启用或禁用本地用户身份验证。默认设置为允许本地用户身份验证，当 SVM 无法联系域控制器或您选择不使用域级别访问控制时，此功能非常有用。

开始之前

必须在 CIFS 服务器上启用本地用户和组功能。

关于此任务

您可以随时启用或禁用本地用户身份验证。如果要在创建 SMB 连接时使用本地用户进行身份验证，则还必须启用 CIFS 服务器的本地用户和组选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

本地身份验证的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户身份验证：

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

相关信息

本地用户身份验证的工作原理

启用或禁用本地用户和组

管理本地用户帐户

修改本地用户帐户

如果要更改现有用户的全名或问题描述，以及要启用或禁用用户帐户，则可以修改本地用户帐户。如果用户的名称受到影响或出于管理目的需要更改名称，您也可以重命名本地用户帐户。

如果您要 ...	输入命令 ...
修改本地用户的全名	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` 如果全名包含空格、则必须使用双引号将其括起来。
修改本地用户的问题描述	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` 如果问题描述包含空格、则必须使用双引号将其括起来。
启用或禁用本地用户帐户	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	重命名本地用户帐户

示例

以下示例将 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的本地用户 "`CIFS_SERVER\sue` " 重命名为 "`CIFS_SERVER\sue_new` "：

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

启用或禁用本地用户帐户

如果您希望用户能够通过 SMB 连接访问 Storage Virtual Machine （ SVM ）中包含的数据，则可以启用本地用户帐户。如果您不希望本地用户帐户通过 SMB 访问 SVM 数据，也可以禁用该用户帐户。

关于此任务

您可以通过修改用户帐户来启用本地用户。

步骤

1. 执行相应的操作：

如果您要 ...	输入命令 ...
启用用户帐户	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
禁用用户帐户	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

更改本地用户帐户密码

您可以更改本地用户的帐户密码。如果用户的密码受到影响或用户忘记了密码，则此功能非常有用。

步骤

1. 通过执行相应的操作更改密码： `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

示例

以下示例将为与 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 关联的本地用户 "`CIFS_SERVER\sue` " 设置密码：

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

显示有关本地用户的信息

您可以通过摘要形式显示所有本地用户的列表。如果要确定为特定用户配置了哪些帐户设置，则可以显示该用户的详细帐户信息以及多个用户的帐户信息。此信息可帮助您确定是否需要修改用户的设置，以及对身份验证或文件访问问题进行故障排除。

关于此任务

不会显示有关用户密码的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示有关 Storage Virtual Machine （ SVM ）上所有用户的信息	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
显示用户的详细帐户信息	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

运行命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地用户的信息：

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

显示有关本地用户的组成员资格的信息

您可以显示有关本地用户所属的本地组的信息。您可以使用此信息来确定用户对文件和文件夹应具有的访问权限。此信息有助于确定用户应拥有哪些文件和文件夹访问权限，或者解决文件访问问题。

关于此任务

您可以自定义命令，使其仅显示要查看的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示指定本地用户的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
显示此本地用户所属本地组的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
显示与指定 Storage Virtual Machine （ SVM ）关联的本地用户的用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
显示指定 SVM 上所有本地用户的详细信息	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

示例

以下示例显示 SVM vs1 上所有本地用户的成员资格信息；用户 "`CIFS_SERVER\Administrator` " 是 "`BUILTIN\Administrators` " 组的成员， "`CIFS_SERVER\sue` " 是 "`CIFS_SERVER\G1` " 组的成员：

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

删除本地用户帐户

如果不再需要本地用户帐户对 CIFS 服务器进行本地 SMB 身份验证或确定对 SVM 中数据的访问权限，则可以从 Storage Virtual Machine （ SVM ）中删除这些帐户。

关于此任务

删除本地用户时，请记住以下几点：

- 文件系统未更改。

  不会调整引用此用户的文件和目录上的 Windows 安全描述符。

- 所有对本地用户的引用都将从成员资格和权限数据库中删除。
- 无法删除众所周知的标准用户，例如管理员。

步骤

1. 确定要删除的本地用户帐户的名称： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. 删除本地用户： `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. 验证是否已删除此用户帐户： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地用户 "`CIFS_SERVER\sue` "：

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


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

管理本地组

修改本地组

您可以通过更改现有本地组的问题描述或重命名组来修改现有本地组。

如果您要 ...	使用命令 ...
修改本地组问题描述	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` 如果问题描述包含空格、则必须使用双引号将其括起来。
重命名本地组	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

示例

以下示例将本地组 "`CIFS_SERVER\engineering` " 重命名为 "`CIFS_SERVER\engineering_new` "：

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

以下示例修改本地组 "`CIFS_SERVER\engineering` " 的问题描述：

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

显示有关本地组的信息

您可以显示在集群或指定 Storage Virtual Machine （ SVM ）上配置的所有本地组的列表。在对 SVM 上所含数据的文件访问问题或 SVM 上的用户权限（特权）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

所需信息	输入命令 ...
集群上的所有本地组	`vserver cifs users-and-groups local-group show`
SVM 上的所有本地组	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地组的信息：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

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。如果您希望根据放置在组上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

向本地组添加成员的准则：

- 您不能将用户添加到特殊的 _Everyone 组。
- 本地组必须存在，然后才能向其中添加用户。
- 用户必须存在，然后才能将其添加到本地组。
- 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， Data ONTAP 必须能够将此名称解析为 SID 。

从本地组中删除成员的准则：

- 您不能从特殊的 _Everyone _ 组中删除成员。
- 要从中删除成员的组必须存在。
- ONTAP 必须能够将要从组中删除的成员的名称解析为相应的 SID 。

步骤

1. 添加或删除组中的成员。

如果您要 ...	然后使用命令 ...
将成员添加到组	`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。
从组中删除成员	`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。

以下示例将本地用户 `SMB_SERVER\sue` 和域组`AD_DOM\DOM_eng` 添加到 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下示例将从 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中删除本地用户 `SMB_SERVER\sue` 和 `SMB_SERVER\James`：

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

相关信息

显示有关本地组成员的信息

显示有关本地组成员的信息

您可以显示在集群或指定 Storage Virtual Machine （SVM）上配置的本地组的所有成员的列表。在对文件访问问题或用户权限（权限）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
集群上所有本地组的成员	`vserver cifs users-and-groups local-group show-members`

要显示的信息	输入命令 ...
SVM 上所有本地组的成员	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

示例

以下示例显示了有关 SVM vs1 上所有本地组的成员的信息：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

删除本地组

如果不再需要本地组来确定与该 SVM 关联的数据的访问权限，或者不再需要将 SVM 用户权限（特权）分配给组成员，则可以从 Storage Virtual Machine （ SVM ）中删除该本地组。

关于此任务

删除本地组时，请记住以下几点：

- 文件系统未更改。

  不会调整引用此组的文件和目录上的 Windows 安全描述符。

- 如果该组不存在，则会返回错误。
- 不能删除特殊的 _Everyone 组。
- 无法删除 *BUILTIN\Administrators _ _BUILTIN\Users* 等内置组。

步骤

1. 通过显示SVM上的本地组列表来确定要删除的本地组的名称： `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 删除本地组： `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 验证是否已删除此组： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地组 "`CIFS_SERVER\sales` "：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

更新本地数据库中的域用户和组名称

您可以将域用户和组添加到 CIFS 服务器的本地组。这些域对象会注册到集群上的本地数据库中。如果重命名域对象，则必须手动更新本地数据库。

关于此任务

您必须指定要更新域名的 Storage Virtual Machine （ SVM ）的名称。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行相应的操作：

要更新域用户和组以及 ...	使用此命令 ...
显示成功更新和无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

要更新域用户和组以及 ...	使用此命令 ...
显示已成功更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only false`
仅显示无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display -failed-only true`
禁止有关更新的所有状态信息	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress -all-output true`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将更新与 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 关联的域用户和组的名称。对于上次更新，需要更新一组依赖名称：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

管理本地权限

向本地或域用户或组添加权限

您可以通过添加权限来管理本地或域用户或组的用户权限。添加的权限将覆盖分配给其中任何对象的默认权限。这样可以自定义用户或组的权限，从而增强安全性。

开始之前

要添加权限的本地或域用户或组必须已存在。

关于此任务

向对象添加权限将覆盖该用户或组的默认权限。添加权限不会删除先前添加的权限。

在向本地或域用户或组添加权限时，必须牢记以下几点：

- 您可以添加一个或多个权限。
- 在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 向本地或域用户或组添加一个或多个权限： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 验证所需权限是否已应用于对象： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下示例将特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege` 添加到 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的用户 "`CIFS_SERVER\sue` " 中：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

从本地或域用户或组中删除权限

您可以通过删除权限来管理本地或域用户或组的用户权限。这样可以自定义用户和组的最大权限，从而增强安全性。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从本地或域用户或组删除权限时，必须牢记以下几点：

- 您可以删除一个或多个权限。
- 从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 从本地或域用户或组中删除一个或多个权限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 验证是否已从对象中删除所需权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将从 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上的用户 "`cifs_server\sue` " 中删除特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege`：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

重置本地或域用户和组的权限

您可以重置本地或域用户和组的权限。如果您已修改本地或域用户或组的权限，并且不再需要或需要这些修改，则此功能将非常有用。

关于此任务

重置本地或域用户或组的权限会删除该对象的任何权限条目。

步骤

1. 重置本地或域用户或组的权限： `vserver cifs users-and-groups privilege reset-privilege -vserver *vserver_name* -user-or-group-name *name*`

2. 验证是否已对此对象重置权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将重置 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上用户 "`CIFS_SERVER\sue` " 的权限。默认情况下，普通用户没有与其帐户关联的权限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

以下示例将重置组 "`BUILTIN\Administrators` " 的权限，从而有效地删除权限条目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

显示有关权限覆盖的信息

您可以显示有关分配给域或本地用户帐户或组的自定义权限的信息。此信息有助于确定是否应用了所需的用户权限。

步骤

1. 执行以下操作之一：

要显示的信息	输入此命令 ...
Storage Virtual Machine （ SVM ）上所有域和本地用户及组的自定义权限	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
SVM 上特定域或本地用户和组的自定义权限	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下命令显示与 SVM vs1 的本地或域用户和组明确关联的所有权限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

配置绕过遍历检查

配置绕过遍历检查概述

绕过遍历检查是一种用户权限（也称为 _privilege _ ），用于确定用户是否可以遍历路径中的所有目录以访问某个文件，即使用户对遍历的目录没有权限也是如此。您应了解允许或禁止绕过遍历检查时会发生什么情况，以及如何为 Storage Virtual Machine （ SVM ）上的用户配置绕过遍历检查。

允许或禁止绕过遍历检查时会发生什么情况

- 如果允许，当用户尝试访问某个文件时， ONTAP 在确定是授予还是拒绝访问该文件时不会检查中间目录的遍历权限。
- 如果不允许， ONTAP 将检查文件路径中所有目录的遍历（执行）权限。

  如果任何中间目录不具有 "`X` "（遍历权限），则 ONTAP 将拒绝访问此文件。

配置绕过遍历检查

您可以使用 ONTAP 命令行界面或使用此用户权限配置 Active Directory 组策略来配置绕过遍历检查。

。 `SeChangeNotifyPrivilege` 权限控制是否允许用户绕过遍历检查。

- 通过将其添加到 SVM 上的本地 SMB 用户或组或域用户或组，可以绕过遍历检查。
- 从 SVM 上的本地 SMB 用户或组或域用户或组中删除该文件将禁止绕过遍历检查。

默认情况下， SVM 上的以下 BUILTIN 组有权绕过遍历检查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不希望允许其中一个组的成员绕过遍历检查，则必须从该组中删除此权限。

在使用命令行界面为 SVM 上的本地 SMB 用户和组配置绕过遍历检查时，必须牢记以下几点：

- 如果要允许自定义本地或域组的成员绕过遍历检查、则必须添加 `SeChangeNotifyPrivilege` 权限。
- 如果要允许单个本地或域用户绕过遍历检查、而该用户不是具有该权限的组的成员、则可以添加 `SeChangeNotifyPrivilege` 权限。
- 您可以通过删除来禁用本地或域用户或组绕过遍历检查 `SeChangeNotifyPrivilege` 随时享受特权。

> 要为指定的本地或域用户或组禁用绕过访问程序检查、还必须删除 `SeChangeNotifyPrivilege` 特权 `Everyone` 组。

相关信息

允许用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

在卷上配置用于 SMB 文件名转换的字符映射

创建 SMB 共享访问控制列表

使用存储级别访问防护确保文件访问安全

支持的权限列表

向本地或域用户或组添加权限

允许用户或组绕过目录遍历检查

如果您希望用户能够遍历路径中的所有目录以查找某个文件、即使该用户对遍历的目录没有权限、则可以添加 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。默认情况下，用户可以绕过目录遍历检查。

开始之前

- SVM上必须存在SMB服务器。

- 必须启用本地用户和组SMB服务器选项。
- 要使用的本地或域用户或组 `SeChangeNotifyPrivilege` 要添加的权限必须已存在。

关于此任务

在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 通过添加启用绕过遍历检查 `SeChangeNotifyPrivilege` 本地或域用户或组的权限： `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 参数是本地用户或组、或者域用户或组。

2. 验证指定的用户或组是否已启用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下命令可使属于"`explexe\eng`"组的用户通过添加来绕过目录遍历检查 `SeChangeNotifyPrivilege` 组权限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相关信息

禁止用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

如果您不希望用户遍历路径中的所有目录以访问某个文件、因为该用户对遍历的目录没有权限、则可以删除 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 禁止绕过遍历检查： `vserver cifs users-and-groups privilege remove-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   此命令将删除 `SeChangeNotifyPrivilege` 使用的值指定的本地或域用户或组的权限 `-user-or-group-name *name*` 参数。

2. 验证指定的用户或组是否已禁用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下命令禁止属于 "`example\eng` " 组的用户绕过目录遍历检查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           -
```

相关信息

允许用户或组绕过目录遍历检查

显示有关文件安全性和审核策略的信息

显示有关文件安全性和审核策略概述的信息

您可以显示 Storage Virtual Machine （SVM）上卷中包含的文件和目录的文件安全信息。您可以显示有关 FlexVol 卷上审核策略的信息。如果已配置，则可以显示有关 FlexVol 卷上存储级别访问防护和动态访问控制安全设置的信息。

显示有关文件安全性的信息

您可以使用以下安全模式显示应用于卷和 qtree （对于 FlexVol 卷）中数据的文件安全性信息：

- NTFS
- "unix"
- 混合

显示有关审核策略的信息

您可以通过以下 NAS 协议显示有关审核 FlexVol 卷上访问事件的审核策略的信息：

- SMB （所有版本）
- NFSv4.x

显示有关存储级别访问防护（ **SLAG** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷和 qtree 对象应用存储级别访问防护安全性：

- NTFS
- 混合
- UNIX （如果在包含此卷的 SVM 上配置了 CIFS 服务器）

显示有关动态访问控制（ **DAC** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷中的对象应用动态访问控制安全性：

- NTFS
- 混合（如果对象具有 NTFS 有效安全性）

相关信息

使用存储级别访问防护保护文件访问安全

显示有关存储级别访问防护的信息

显示 **NTFS** 安全模式卷上的文件安全性信息

您可以显示 NTFS 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 DOS 属性的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 由于 NTFS 安全模式卷和 qtree 在确定文件访问权限时仅使用 NTFS 文件权限以及 Windows 用户和组，因此与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。
- 对于采用 NTFS 安全模式的文件和文件夹，将显示 ACL 输出。
- 由于可以在卷根或 qtree 上配置存储级别访问防护安全性，因此配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件 ACL 和存储级别访问防护 ACL 。
- 如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示路径的安全信息 `/vol4` 在SVM VS1中：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                 Vserver: vs1
                               File Path: /vol4
                       File Inode Number: 64
                          Security Style: ntfs
                         Effective Style: ntfs
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下示例显示了路径的安全信息以及展开的掩码 `/data/engineering` 在SVM VS1中：

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
```

```
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
```

```
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
```

```
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

以下示例显示路径为的卷的安全信息、包括存储级别访问防护安全信息 `/datavol1` 在SVM VS1中：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

相关信息

显示混合安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

您可以显示混合安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和文件夹，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。
- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性。
- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和目录，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示 UNIX 文件权限和存储级别访问防护 ACL 。
- 如果在命令中输入的路径指向具有 NTFS 有效安全性的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示路径的安全信息 `/projects` 在SVM VS1中、以扩展掩码形式显示。此混合安全模式路径具有 UNIX 有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

以下示例显示路径的安全信息 `/data` 在SVM VS1中。此混合安全模式路径具有 NTFS 有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                 Vserver: vs1
                               File Path: /data
                       File Inode Number: 544
                          Security Style: mixed
                         Effective Style: ntfs
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下示例显示路径上卷的安全信息 `/datavol5` 在SVM VS1中。此混合安全模式卷的顶层具有 UNIX 有效安全性。此卷具有存储级别访问防护安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

显示有关 **UNIX** 安全模式卷上的文件安全性的信息

您可以显示 UNIX 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全配

置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其文件或目录安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 在确定文件访问权限时， UNIX 安全模式卷和 qtree 仅使用 UNIX 文件权限，模式位或 NFSv4 ACL 。
- 只有具有 NFSv4 安全性的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和目录，此字段为空。

- 对于 NFSv4 安全描述符， ACL 输出中的所有者和组输出字段不适用。

  它们仅对 NTFS 安全描述符有意义。

- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
扩展了详细信息	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

示例

以下示例显示路径的安全信息 `/home` 在SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                   Unix Mode Bits in Text: rwx------
                                     ACLs: -
```

以下示例显示路径的安全信息 `/home` 在扩展掩码形式的SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                 Vserver: vs1
                               File Path: /home
                       File Inode Number: 9590
                          Security Style: unix
                         Effective Style: unix
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: 0x10
                      ...0 .... .... .... = Offline
                      .... ..0. .... .... = Sparse
                      .... .... 0... .... = Normal
                      .... .... ..0. .... = Archive
                      .... .... ...1 .... = Directory
                      .... .... .... .0.. = System
                      .... .... .... ..0. = Hidden
                      .... .... .... ...0 = Read Only
                            Unix User Id: 0
                           Unix Group Id: 1
                          Unix Mode Bits: 700
                   Unix Mode Bits in Text: rwx------
                                     ACLs: -
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

使用命令行界面显示有关 **FlexVol** 卷上 **NTFS** 审核策略的信息

您可以显示有关 FlexVol 卷上的 NTFS 审核策略的信息，包括什么是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表的信息。您可以使用结果验证安全配置或对审核问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其审核信息的文件或文件夹的路径。您可以摘要形式或详细列表形式显示输出。

- 对于审核策略， NTFS 安全模式卷和 qtree 仅使用 NTFS 系统访问控制列表（ SACL ）。
- 具有 NTFS 有效安全性的混合安全模式卷中的文件和文件夹可以应用 NTFS 审核策略。

  混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NTFS SACL 。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件和文件夹 NFSv4 SACL 以及存储级别访问防护 NTFS SACL 。
- 如果在命令中输入的路径指向采用 NTFS 有效安全模式的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。
- 显示有关具有 NTFS 有效安全性的文件和文件夹的安全信息时，与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。

  在确定文件访问权限时， NTFS 安全模式文件和文件夹仅使用 NTFS 文件权限以及 Windows 用户和组。

- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。

步骤

1. 显示具有所需详细级别的文件和目录审核策略设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
作为详细列表	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示了路径的审核策略信息 `/corp` 在SVM VS1中。此路径具有 NTFS 有效安全性。NTFS 安全描述符包含成功和成功 / 失败 SACL 条目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

以下示例显示了路径的审核策略信息 `/datavol1` 在SVM VS1中。此路径包含常规文件和文件夹 SACL 以及存储级别访问防护 SACL 。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

使用命令行界面显示有关 **FlexVol** 卷上 **NFSv4** 审核策略的信息

您可以使用 ONTAP 命令行界面显示有关 FlexVol 卷上 NFSv4 审核策略的信息，包括什么是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表（ SACL ）的信

息。您可以使用结果验证安全配置或对审核问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （ SVM ）的名称以及要显示其审核信息的文件或目录的路径。您可以摘要形式或详细列表形式显示输出。

- UNIX 安全模式卷和 qtree 仅对审核策略使用 NFSv4 SACL 。
- 混合安全模式卷中采用 UNIX 安全模式的文件和目录可以应用 NFSv4 审核策略。

  混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL ，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NFSv4 SACL 。
- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

  对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL ）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX ，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性， 配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规 NFSv4 文件和目录 SACL 以及存储级别访问防护 NTFS SACL 。
- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示路径的安全信息 `/lab` 在SVM VS1中。此 UNIX 安全模式路径具有 NFSv4 SACL 。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

显示有关文件安全性和审核策略信息的方式

您可以使用通配符（*）显示有关给定路径或根卷下所有文件和目录的文件安全和审核策略的信息。

通配符（*）可用作给定目录路径的最后一个子组件，在该路径下，您希望显示所有文件和目录的信息。如果要显示名为 "` *` " 的特定文件或目录的信息，则需要在双引号（"`` "）中提供完整路径。

示例

以下带有通配符的命令显示路径下所有文件和目录的信息 `/1/` SVM VS1：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

以下命令显示路径下名为"*"的文件的信息 `/vol1/a` SVM VS1。路径用双引号括起来（""）。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                  Vserver: vs1
                File Path: “/vol1/a/*”
           Security Style: mixed
          Effective Style: unix
           DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
             Unix User Id: 1002
            Unix Group Id: 65533
           Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

使用命令行界面管理 **SVM** 上的 **NTFS** 文件安全性， **NTFS** 审核策略和存储级别访问防护

使用 **CLI** 概述管理 **SVM** 上的 **NTFS** 文件安全性， **NTFS** 审核策略和存储级别访问防护

您可以使用命令行界面管理 Storage Virtual Machine （ SVM ） 上的 NTFS 文件安全性，NTFS 审核策略和存储级别访问防护。

您可以从 SMB 客户端或使用命令行界面管理 NTFS 文件安全性和审核策略。但是，使用命令行界面配置文件安全性和审核策略后，无需使用远程客户端来管理文件安全性。使用 CLI 可以显著缩短使用一个命令对多个文件和文件夹应用安全性所需的时间。

您可以配置存储级别访问防护，这是 ONTAP 应用于 SVM 卷的另一层安全保护。存储级别访问防护适用场景从所有 NAS 协议访问应用了存储级别访问防护的存储对象。

只能通过 ONTAP 命令行界面配置和管理存储级别访问防护。您不能从 SMB 客户端管理存储级别访问防护设置。此外，如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则不会看到存储级别访问防护安全性。即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别访问防护安全性。因此，存储级别访问防护为数据访问提供了额外的安全层，该层由存储管理员独立设置和管理。

> 即使存储级别访问防护仅支持 NTFS 访问权限，但如果 UNIX 用户映射到拥有该卷的 SVM 上的 Windows 用户，则 ONTAP 可以对通过 NFS 访问应用了存储级别访问防护的卷上的数据执行安全检查。

NTFS 安全模式卷

NTFS 安全模式卷和 qtree 中包含的所有文件和文件夹都具有 NTFS 有效安全性。您可以使用 `vserver security file-directory` 命令系列、用于在NTFS安全模式卷上实施以下类型的安全性：

- 卷中包含的文件和文件夹的文件权限和审核策略
- 卷上的存储级别访问防护安全性

混合安全模式卷

混合安全模式卷和 qtree 可以包含一些具有 UNIX 有效安全性并使用 UNIX 文件权限（模式位或 NFSv4.x ACL 和 NFSv4.x 审核策略）的文件和文件夹，以及一些具有 NTFS 有效安全性并使用 NTFS 文件权限和审核策略的文件和文件夹。您可以使用 `vserver security file-directory` 用于将以下类型的安全性应用于混合安全模式数据的命令系列：

- 混合卷或 qtree 中采用 NTFS 有效安全模式的文件和文件夹的文件权限和审核策略
- 对采用 NTFS 和 UNIX 有效安全模式的卷的存储级别访问防护

UNIX安全模式卷

UNIX 安全模式卷和 qtree 包含具有 UNIX 有效安全性（模式位或 NFSv4.x ACL ）的文件和文件夹。如果要使用、必须牢记以下几点 `vserver security file-directory` 用于在UNIX安全模式卷上实施安全性的命令系列：

- 。 `vserver security file-directory` 命令系列不能用于管理UNIX安全模式卷和qtrees上的UNIX文件安全性和审核策略。
- 您可以使用 `vserver security file-directory` 命令系列、用于在UNIX安全模式卷上配置存储级别访问防护、前提是带有目标卷的SVM包含CIFS服务器。

相关信息

显示有关文件安全性和审核策略的信息

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

使用命令行界面配置审核策略并将其应用于 NTFS 文件和文件夹

使用存储级别访问防护确保文件访问安全

使用命令行界面设置文件和文件夹安全性的用例

由于您可以在本地应用和管理文件和文件夹安全性，而无需远程客户端的参与，因此可以显著缩短为大量文件或文件夹设置批量安全性所需的时间。

在以下使用情形中，使用命令行界面设置文件和文件夹安全性会很有用：

- 在大型企业环境中存储文件，例如主目录中的文件存储
- 数据迁移
- 更改 Windows 域
- 跨 NTFS 文件系统实现文件安全和审核策略标准化

使用命令行界面设置文件和文件夹安全性的限制

在使用命令行界面设置文件和文件夹安全性时，您需要了解某些限制。

- 。 `vserver security file-directory` 命令系列不支持设置NFSv4 ACL。

  您只能将 NTFS 安全描述符应用于 NTFS 文件和文件夹。

如何使用安全描述符应用文件和文件夹安全性

安全描述符包含访问控制列表，用于确定用户可以对文件和文件夹执行的操作以及在用户访问文件和文件夹时审核的内容。

- * 权限 *

  权限由对象的所有者允许或拒绝，并确定对象（用户，组或计算机对象）可以对指定文件或文件夹执行的操作。

- * 安全描述符 *

  安全描述符是指包含安全信息的数据结构，用于定义与文件或文件夹关联的权限。

- * 访问控制列表（ ACL ） *

  访问控制列表是安全描述符中包含的列表，其中包含有关用户，组或计算机对象可以对应用了安全描述符的文件或文件夹执行的操作的信息。安全描述符可以包含以下两种类型的 ACL：

  - 随机访问控制列表（ DACL ）
  - 系统访问控制列表（ SACL ）

- * 随机访问控制列表（ DACL ） *

  DACL 包含允许或拒绝对文件或文件夹执行操作的用户，组和计算机对象的 SID 列表。DACL 包含零个或多个访问控制条目（ ACE ）。

- * 系统访问控制列表（ SACL ） *

  SACL 包含记录成功或失败审核事件的用户，组和计算机对象的 SID 列表。SACL 包含零个或多个访问控制条目（ ACE ）。

- * 访问控制条目（ ACE ） *

  ACE 是 DACL 或 SACL 中的各个条目：

  - DACL 访问控制条目指定允许或拒绝特定用户，组或计算机对象的访问权限。
  - SACL 访问控制条目指定审核特定用户，组或计算机对象执行的指定操作时要记录的成功或失败事件。

- * 权限继承 *

  权限继承介绍如何将安全描述符中定义的权限从父对象传播到对象。子对象仅继承可继承的权限。在对父对象设置权限时、您可以通过"`Apply to "(应用到)来确定文件夹、子文件夹和文件是否可以继承它们 `this-folder`， `sub-folders`和`files`”。

相关信息

"SMB 和 NFS 审核和安全跟踪"

使用命令行界面配置审核策略并将其应用于 NTFS 文件和文件夹

在 **SVM** 灾难恢复目标上应用使用本地用户或组的文件目录策略的准则

如果文件目录策略配置在安全描述符或 DACL 或 SACL 条目中使用本地用户或组，则在 ID 丢弃配置中对 Storage Virtual Machine （ SVM ）灾难恢复目标应用文件目录策略之前，必须牢记一些特定准则。

您可以为 SVM 配置灾难恢复配置，以便源集群上的源 SVM 将数据和配置从源 SVM 复制到目标集群上的目标 SVM 。

您可以设置以下两种类型的 SVM 灾难恢复之一：

- 身份保留

  在此配置中， SVM 和 CIFS 服务器的标识将保留下来。

- 已丢弃身份

  在此配置中，不会保留 SVM 和 CIFS 服务器的身份。在这种情况下，目标 SVM 上的 SVM 和 CIFS 服务器名称与源 SVM 上的 SVM 和 CIFS 服务器名称不同。

身份丢弃配置准则

在身份丢弃配置中，对于包含本地用户，组和权限配置的 SVM 源，必须更改本地域的名称（本地 CIFS 服务器名称），使其与 SVM 目标上的 CIFS 服务器名称匹配。例如，如果源 SVM 名称为 “vs1` " ， CIFS 服务器名称为 "`CIFS1` " ，而目标 SVM 名称为 "`vs1_dst` " ， CIFS 服务器名称为 "`CIFS1_dst` " ，则本地用户的本地域名 "`CIFS1\user1` " 会自动更改为` " 目标 SIFS1\DST1”：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

即使本地用户和组名称会在本地用户和组数据库中自动更改、但本地用户或组名称不会在文件目录策略配置(使用在命令行界面上配置的策略)中自动更改 `vserver security file-directory` 命令系列)。

例如、对于"`VS1`"、如果您在中配置了DACL条目 `-account` 参数设置为"`CIFS1\user1`"、则此设置不会在目标SVM上自动更改、以反映目标的CIFS服务器名称。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

您必须使用 `vserver security file-directory modify` 用于手动将CIFS服务器名称更改为目标CIFS服

务器名称的命令。

包含帐户参数的文件目录策略配置组件

有三个文件目录策略配置组件可以使用可包含本地用户或组的参数设置：

- 安全描述符

  您可以选择指定安全描述符的所有者以及安全描述符所有者的主组。如果安全描述符对所有者和主组条目使用本地用户或组，则必须修改安全描述符，以便在帐户名称中使用目标 SVM 。您可以使用 `vserver security file-directory ntfs modify` 命令以对帐户名称进行任何必要的更改。

- DACL 条目

  每个 DACL 条目都必须与一个帐户相关联。您必须修改任何使用本地用户或组帐户的 DACL ，才能使用目标 SVM 名称。由于您无法修改现有 DACL 条目的帐户名称，因此必须从安全描述符中删除任何具有本地用户或组的 DACL 条目，使用更正后的目标帐户名称创建新的 DACL 条目，并将这些新的 DACL 条目与相应的安全描述符关联。

- SACL条目

  每个SACL条目都必须与一个帐户关联。您必须修改任何使用本地用户或组帐户的 SACL ，以使用目标 SVM 名称。由于您无法修改现有 SACL 条目的帐户名称，因此必须从安全描述符中删除任何具有本地用户或组的 SACL 条目，使用更正后的目标帐户名称创建新的 SACL 条目，并将这些新的 SACL 条目与相应的安全描述符相关联。

在应用此策略之前，您必须对文件目录策略配置中使用的本地用户或组进行任何必要的更改；否则，应用作业将失败。

使用命令行界面在 **NTFS** 文件和文件夹上配置和应用文件安全性

创建 **NTFS** 安全描述符

创建 NTFS 安全描述符（文件安全策略）是配置 NTFS 访问控制列表（ ACL ）并将其应用于 Storage Virtual Machine （ SVM ）中的文件和文件夹的第一步。您可以将安全描述符与策略任务中的文件或文件夹路径相关联。

关于此任务

您可以为 NTFS 安全模式卷中的文件和文件夹或混合安全模式卷上的文件和文件夹创建 NTFS 安全描述符。

默认情况下，在创建安全描述符时，会向该安全描述符添加四个随机访问控制列表（ DACL ）访问控制条目（ ACE ）。四个默认 ACE 如下所示：

对象	访问类型	访问权限	应用权限的位置
BUILTIN\Administrators	允许	完全控制	此文件夹，子文件夹，文件
BUILTIN\Users	允许	完全控制	此文件夹，子文件夹，文件

对象	访问类型	访问权限	应用权限的位置
Creator 所有者	允许	完全控制	此文件夹，子文件夹，文件
NT AUTHORITIC\SYSTEM	允许	完全控制	此文件夹，子文件夹，文件

您可以使用以下可选参数自定义安全描述符配置：

- 安全描述符的所有者
- 所有者的主组
- 原始控制标志

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

将**NTFS DACL**访问控制条目添加到**NTFS**安全描述符中

向 NTFS 安全描述符添加 DACL （随机访问控制列表）访问控制条目（ ACE ）是配置 NTFS ACL 并将其应用于文件或文件夹的第二步。每个条目都标识允许或拒绝访问的对象，并定义对象可以或不能对 ACE 中定义的文件或文件夹执行的操作。

关于此任务

您可以将一个或多个ACL添加到安全描述符的DACL中。

如果安全描述符包含具有现有 ACE 的 DACL ，则该命令会将新 ACE 添加到 DACL 中。如果安全描述符不包含 DACL ，则该命令将创建 DACL 并向其中添加新 ACE 。

您可以选择通过指定要为中指定的帐户允许或拒绝的权限来自定义DACL条目 `-account` 参数。指定权限的方法有三种，这三种方法是互斥的：

- 权限
- 高级权限
- 原始权限（高级权限）

> 如果未指定DACL条目的权限、则默认为将权限设置为 `Full Control`。

您可以选择通过指定如何应用继承来自定义 DACL 条目。

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将DACL条目添加到安全描述符： `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   ```

```
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. 验证DACL条目是否正确： `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                        Vserver: vs1
             Security Descriptor Name: sd1
                       Allow or Deny: deny
                 Account Name or SID: DOMAIN\joe
                       Access Rights: full-control
               Advanced Access Rights: -
                            Apply To: this-folder
                       Access Rights: full-control
   ```

创建安全策略

为 SVM 创建文件安全策略是配置 ACL 并将其应用于文件或文件夹的第三步。策略充当各种任务的容器，其中每个任务都是一个条目，可应用于文件或文件夹。您可以稍后将任务添加到安全策略中。

关于此任务

添加到安全策略的任务包含 NTFS 安全描述符与文件或文件夹路径之间的关联。因此，您应将安全策略与每个 SVM （包含 NTFS 安全模式卷或混合安全模式卷）相关联。

步骤

1. 创建安全策略： `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory policy create -policy-name policy1 -vserver
   vs1
   ```

2. 验证安全策略： `vserver security file-directory policy show`

   ```
             vserver security file-directory policy show
                Vserver          Policy Name
             ------------     --------------
                 vs1              policy1
   ```

将任务添加到安全策略中

创建策略任务并将其添加到安全策略是配置 ACL 并将其应用于 SVM 中的文件或文件夹的第四步。创建策略任务时，您需要将此任务与安全策略相关联。您可以将一个或多个任务

条目添加到安全策略中。

关于此任务

安全策略是任务的容器。任务是指可通过安全策略对具有 NTFS 或混合安全模式的文件或文件夹（如果配置存储级别访问防护，则也可以对卷对象）执行的单个操作。

任务类型有两种：

- 文件和目录任务

  用于指定将安全描述符应用于指定文件和文件夹的任务。通过文件和目录任务应用的 ACL 可以通过 SMB 客户端或 ONTAP 命令行界面进行管理。

- 存储级别访问防护任务

  用于指定将存储级别访问防护安全描述符应用于指定卷的任务。通过存储级别访问防护任务应用的 ACL 只能通过 ONTAP 命令行界面进行管理。

任务包含文件（或文件夹）或一组文件（或文件夹）的安全配置定义。策略中的每个任务都由路径唯一标识。一个策略中的每个路径只能有一个任务。策略不能包含重复的任务条目。

将任务添加到策略的准则：

- 每个策略最多可以包含 10 ， 000 个任务条目。
- 一个策略可以包含一个或多个任务。

  即使策略可以包含多个任务，您也无法将策略配置为同时包含文件目录和存储级别访问防护任务。策略必须包含所有存储级别访问防护任务或所有文件目录任务。

- 存储级别访问防护用于限制权限。

  它不会提供额外的访问权限。

向安全策略添加任务时，必须指定以下四个必需参数：

- SVM name
- Policy name
- 路径
- 要与路径关联的安全描述符

您可以使用以下可选参数自定义安全描述符配置：

- 安全类型
- 传播模式
- 索引位置
- 访问控制类型

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将具有关联安全描述符的任务添加到安全策略：`vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 是的默认值 `-access-control` 参数。在配置文件和目录访问任务时指定访问控制类型是可选的。

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. 验证策略任务配置：`vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

应用安全策略

将文件安全策略应用于 SVM 是创建 NTFS ACL 并将其应用于文件或文件夹的最后一步。

关于此任务

您可以将安全策略中定义的安全设置应用于驻留在 FlexVol 卷（ NTFS 或混合安全模式）中的 NTFS 文件和文件夹。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。应用安全策略及其关联的DACL后、任何现有DACL都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

步骤

1. 应用安全策略：`vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   此时将计划策略应用作业，并返回作业 ID 。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

监控安全策略作业

在将安全策略应用于 Storage Virtual Machine （SVM）时，您可以通过监控安全策略作业来监控任务进度。如果您希望确定安全策略的应用成功，这将非常有用。如果您的作业运行时间较长，并且要对大量文件和文件夹应用批量安全性，则此功能也会很有用。

关于此任务

要显示有关安全策略作业的详细信息、应使用 `-instance` 参数。

步骤

1. 监控安全策略作业：`vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

验证应用的文件安全性

您可以验证文件安全设置，以确认应用安全策略的 Storage Virtual Machine （SVM）上的文件或文件夹具有所需设置。

关于此任务

您必须提供包含要验证安全设置的文件和文件夹的数据和路径的 SVM 名称。您可以使用可选 `-expand-mask` 用于显示有关安全设置的详细信息的参数。

步骤

1. 显示文件和文件夹安全设置：`vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
          Vserver: vs1
               File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
```

```
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
```

```
System Security
                            .... .... ...1 .... .... .... .... .... =
Synchronize
                            .... .... .... 1... .... .... .... .... =
Write Owner
                            .... .... .... .1.. .... .... .... .... =
Write DAC
                            .... .... .... ..1. .... .... .... .... =
Read Control
                            .... .... .... ...1 .... .... .... .... =
Delete
                            .... .... .... .... .... ...1 .... .... =
Write Attributes
                            .... .... .... .... .... .... 1... .... =
Read Attributes
                            .... .... .... .... .... .... .1.. .... =
Delete Child
                            .... .... .... .... .... .... ..1. .... =
Execute
                            .... .... .... .... .... .... ...1 .... =
Write EA
                            .... .... .... .... .... .... .... 1... =
Read EA
                            .... .... .... .... .... .... .... .1.. =
Append
                            .... .... .... .... .... .... .... ..1. =
Write
                            .... .... .... .... .... .... .... ...1 =
Read

                          ALLOW-Everyone-0x10000000-OI|CI|IO
                            0... .... .... .... .... .... .... .... =
Generic Read
                            .0.. .... .... .... .... .... .... .... =
Generic Write
                            ..0. .... .... .... .... .... .... .... =
Generic Execute
                            ...1 .... .... .... .... .... .... .... =
Generic All
                            .... ...0 .... .... .... .... .... .... =
System Security
                            .... .... ...0 .... .... .... .... .... =
Synchronize
                            .... .... .... 0... .... .... .... .... =
Write Owner
                            .... .... .... .0.. .... .... .... .... =
```

```
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

使用 **CLI** 概述配置审核策略并将其应用于 **NTFS** 文件和文件夹

使用 ONTAP 命令行界面时，要将审核策略应用于 NTFS 文件和文件夹，必须执行几个步骤。首先，创建 NTFS 安全描述符并将 SACL 添加到安全描述符中。接下来，创建安全策略并添加策略任务。然后，将此安全策略应用于 Storage Virtual Machine （ SVM ）。

关于此任务

应用安全策略后，您可以监控安全策略作业，然后验证应用的审核策略的设置。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

相关信息

使用存储级别访问防护保护文件访问安全

使用命令行界面设置文件和文件夹安全性的限制

如何使用安全描述符应用文件和文件夹安全性

"SMB 和 NFS 审核和安全跟踪"

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

创建 NTFS 安全描述符审核策略是配置 NTFS 访问控制列表（ACL）并将其应用于 SVM 中的文件和文件夹的第一步。您将在策略任务中将安全描述符与文件或文件夹路径相关联。

关于此任务

您可以为 NTFS 安全模式卷中的文件和文件夹或混合安全模式卷上的文件和文件夹创建 NTFS 安全描述符。

默认情况下，在创建安全描述符时，会向该安全描述符添加四个随机访问控制列表（DACL）访问控制条目（ACE）。四个默认 ACE 如下所示：

对象	访问类型	访问权限	应用权限的位置
BUILTIN\Administrators	允许	完全控制	此文件夹，子文件夹，文件
BUILTIN\Users	允许	完全控制	此文件夹，子文件夹，文件
Creator 所有者	允许	完全控制	此文件夹，子文件夹，文件
NT AUTHORITIC\SYSTEM	允许	完全控制	此文件夹，子文件夹，文件

您可以使用以下可选参数自定义安全描述符配置：

- 安全描述符的所有者
- 所有者的主组
- 原始控制标志

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 如果要使用高级参数、请将权限级别设置为高级： `set -privilege advanced`
2. 创建安全描述符： `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. 验证安全描述符配置是否正确： `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

```
                                    Vserver: vs1
                          Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
```

4. 如果您处于高级权限级别、请返回到管理权限级别： `set -privilege admin`

将 **NTFS SACL** 访问控制条目添加到 **NTFS** 安全描述符

向 NTFS 安全描述符添加 SACL （系统访问控制列表）访问控制条目（ ACE ）是为 SVM 中的文件或文件夹创建 NTFS 审核策略的第二步。每个条目都标识要审核的用户或组。SACL 条目用于定义是要审核成功的还是失败的访问尝试。

关于此任务

您可以将一个或多个 ACE 添加到安全描述符的 SACL 中。

如果安全描述符包含具有现有 ACE 的 SACL ，则该命令会将新 ACE 添加到 SACL 。如果安全描述符不包含 SACL ，则该命令将创建 SACL 并将新 ACE 添加到其中。

您可以通过为中指定的帐户指定要审核成功或失败事件的权限来配置SACL条目 `-account` 参数。指定权限的方法有三种，这三种方法是互斥的：

- 权限
- 高级权限
- 原始权限（高级权限）

> 如果未指定SACL条目的权限、则默认设置为 `Full Control`。

您可以选择通过指定如何使用应用继承来自定义SACL条目 `apply to` 参数。如果未指定此参数，则默认情况下会将此 SACL 条目应用于此文件夹，子文件夹和文件。

步骤

1. 将SACL条目添加到安全描述符： `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. 验证SACL条目是否正确： `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                                Vserver: vs1
                   Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                     Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
```

创建安全策略

为 Storage Virtual Machine （ SVM ）创建审核策略是配置 ACL 并将其应用于文件或文件夹的第三步。策略充当各种任务的容器，其中每个任务都是一个条目，可应用于文件或文件夹。您可以稍后将任务添加到安全策略中。

关于此任务

添加到安全策略的任务包含 NTFS 安全描述符与文件或文件夹路径之间的关联。因此，您应将安全策略与每个 Storage Virtual Machine （ SVM ）（包含 NTFS 安全模式卷或混合安全模式卷）相关联。

步骤

1. 创建安全策略：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. 验证安全策略：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

将任务添加到安全策略中

创建策略任务并将其添加到安全策略是配置 ACL 并将其应用于 SVM 中的文件或文件夹的第四步。创建策略任务时，您需要将此任务与安全策略相关联。您可以将一个或多个任务条目添加到安全策略中。

关于此任务

安全策略是任务的容器。任务是指可通过安全策略对具有 NTFS 或混合安全模式的文件或文件夹（如果配置存储级别访问防护，则也可以对卷对象）执行的单个操作。

任务类型有两种：

- 文件和目录任务

  用于指定将安全描述符应用于指定文件和文件夹的任务。通过文件和目录任务应用的 ACL 可以通过 SMB 客户端或 ONTAP 命令行界面进行管理。

- 存储级别访问防护任务

  用于指定将存储级别访问防护安全描述符应用于指定卷的任务。通过存储级别访问防护任务应用的 ACL 只能通过 ONTAP 命令行界面进行管理。

任务包含文件（或文件夹）或一组文件（或文件夹）的安全配置定义。策略中的每个任务都由路径唯一标识。一个策略中的每个路径只能有一个任务。策略不能包含重复的任务条目。

将任务添加到策略的准则：

- 每个策略最多可以包含 10 ， 000 个任务条目。
- 一个策略可以包含一个或多个任务。

  即使策略可以包含多个任务，您也无法将策略配置为同时包含文件目录和存储级别访问防护任务。策略必须包含所有存储级别访问防护任务或所有文件目录任务。

- 存储级别访问防护用于限制权限。

  它不会提供额外的访问权限。

您可以使用以下可选参数自定义安全描述符配置：

- 安全类型
- 传播模式
- 索引位置
- 访问控制类型

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将具有关联安全描述符的任务添加到安全策略： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 是的默认值 `-access-control` 参数。在配置文件和目录访问任务时指定访问控制类型是可选的。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. 验证策略任务配置： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

应用安全策略

将审核策略应用于SVM是创建NTFS ACL并将其应用于文件或文件夹的最后一步。

关于此任务

您可以将安全策略中定义的安全设置应用于驻留在 FlexVol 卷（ NTFS 或混合安全模式）中的 NTFS 文件和文件夹。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。应用安全策略及其关联的DACL后、任何现有DACL都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

步骤

1. 应用安全策略： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   此时将计划策略应用作业，并返回作业 ID 。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

监控安全策略作业

在将安全策略应用于 Storage Virtual Machine （ SVM ）时，您可以通过监控安全策略作业来监控任务进度。如果您希望确定安全策略的应用成功，这将非常有用。如果您的作业运行时间较长，并且要对大量文件和文件夹应用批量安全性，则此功能也会很有用。

关于此任务

要显示有关安全策略作业的详细信息、应使用 `-instance` 参数。

步骤

1. 监控安全策略作业： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

验证应用的审核策略

您可以验证审核策略，以确认应用此安全策略的 Storage Virtual Machine （ SVM ）上的文件或文件夹具有所需的审核安全设置。

关于此任务

您可以使用 `vserver security file-directory show` 命令以显示审核策略信息。您必须提供包含要显示其文件或文件夹审核策略信息的数据所在 SVM 的名称以及该数据的路径。

步骤

1. 显示审核策略设置： `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

示例

以下命令显示应用于 SVM vs1 中路径 "` /corp` " 的审核策略信息。此路径同时应用了成功和成功 / 失败 SACL 条目：

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

管理安全策略作业时的注意事项

如果存在安全策略作业，则在某些情况下，您无法修改该安全策略或分配给该策略的任务。您应了解可以或不能在哪些条件下修改安全策略，以便成功尝试修改此策略。对策略的修改包括添加，删除或修改分配给策略的任务以及删除或修改策略。

如果某个安全策略存在作业且该作业处于以下状态，则无法修改该策略或分配给该策略的任务：

- 作业正在运行或正在进行中。
- 作业已暂停。
- 作业将恢复并处于运行状态。
- 作业正在等待故障转移到其他节点。

在以下情况下，如果某个安全策略存在作业，则可以成功修改该安全策略或分配给该策略的任务：

- 策略作业已停止。
- 策略作业已成功完成。

用于管理 **NTFS** 安全描述符的命令

您可以使用特定的 ONTAP 命令来管理安全描述符。您可以创建，修改，删除和显示有关安全描述符的信息。

如果您要 ...	使用此命令 ...
创建 NTFS 安全描述符	`vserver security file-directory ntfs create`
修改现有 NTFS 安全描述符	`vserver security file-directory ntfs modify`
显示有关现有 NTFS 安全描述符的信息	`vserver security file-directory ntfs show`
删除 NTFS 安全描述符	`vserver security file-directory ntfs delete`

请参见的手册页 `vserver security file-directory ntfs` 有关详细信息、请参见命令。

用于管理 **NTFS DACL** 访问控制条目的命令

您可以使用特定的 ONTAP 命令来管理 DACL 访问控制条目（ACE）。您可以随时将 ACE 添加到 NTFS DACL 中。您还可以通过修改，删除和显示有关 DACL 中 ACE 的信息来管理现有 NTFS DACL 。

如果您要 ...	使用此命令 ...
创建 ACE 并将其添加到 NTFS DACL 中	`vserver security file-directory ntfs dacl add`
修改 NTFS DACL 中的现有 ACE	`vserver security file-directory ntfs dacl modify`
显示有关 NTFS DACL 中现有 ACE 的信息	`vserver security file-directory ntfs dacl show`
从 NTFS DACL 中删除现有 ACE	`vserver security file-directory ntfs dacl remove`

请参见的手册页 `vserver security file-directory ntfs dacl` 有关详细信息、请参见命令。

用于管理**NTFS SACL**访问控制条目的命令

您可以使用特定的ONTAP命令来管理SACL访问控制条目(Access Control entries、ACE)。您可以随时将 ACE 添加到 NTFS SACL 。您还可以通过修改，删除和显示有关

SACL 中 ACE 的信息来管理现有 NTFS SACL 。

如果您要 ...	使用此命令 ...
创建 ACE 并将其添加到 NTFS SACL	`vserver security file-directory ntfs sacl add`
修改 NTFS SACL 中的现有 ACE	`vserver security file-directory ntfs sacl modify`
显示有关 NTFS SACL 中现有 ACE 的信息	`vserver security file-directory ntfs sacl show`
从 NTFS SACL 中删除现有 ACE	`vserver security file-directory ntfs sacl remove`

请参见的手册页 `vserver security file-directory ntfs sacl` 有关详细信息、请参见命令。

用于管理安全策略的命令

您可以使用特定的 ONTAP 命令来管理安全策略。您可以显示有关策略的信息，也可以删除策略。您不能修改安全策略。

如果您要 ...	使用此命令 ...
创建安全策略	`vserver security file-directory policy create`
显示有关安全策略的信息	`vserver security file-directory policy show`
删除安全策略	`vserver security file-directory policy delete`

请参见的手册页 `vserver security file-directory policy` 有关详细信息、请参见命令。

用于管理安全策略任务的命令

您可以使用 ONTAP 命令添加，修改，删除和显示有关安全策略任务的信息。

如果您要 ...	使用此命令 ...
添加安全策略任务	`vserver security file-directory policy task add`

如果您要 ...	使用此命令 ...
修改安全策略任务	`vserver security file-directory policy task modify`
显示有关安全策略任务的信息	`vserver security file-directory policy task show`
删除安全策略任务	`vserver security file-directory policy task remove`

请参见的手册页 `vserver security file-directory policy task` 有关详细信息、请参见命令。

用于管理安全策略作业的命令

您可以使用 ONTAP 命令暂停，恢复，停止和显示有关安全策略作业的信息。

如果您要 ...	使用此命令 ...
暂停安全策略作业	`vserver security file-directory job pause -vserver vserver_name -id integer`
恢复安全策略作业	`vserver security file-directory job resume -vserver vserver_name -id integer`
显示有关安全策略作业的信息	`vserver security file-directory job show -vserver vserver_name` 您可以使用此命令确定作业的作业ID。
停止安全策略作业	`vserver security file-directory job stop -vserver vserver_name -id integer`

请参见的手册页 `vserver security file-directory job` 有关详细信息、请参见命令。

为 **SMB** 共享配置元数据缓存

SMB 元数据缓存的工作原理

通过元数据缓存， SMB 1.0 客户端上的文件属性缓存可以更快地访问文件和文件夹属性。您可以基于每个共享启用或禁用属性缓存。如果启用了元数据缓存，您还可以为缓存条目配置生存时间。如果客户端通过 SMB 2.x 或 SMB 3.0 连接到共享，则无需配置元数据缓存。

启用后， SMB 元数据缓存会将路径和文件属性数据存储一段有限的时间。这样可以提高具有常见工作负载的 SMB 1.0 客户端的 SMB 性能。

对于某些任务， SMB 会创建大量流量，其中可能包括对路径和文件元数据的多个相同查询。您可以改用 SMB

元数据缓存从缓存中提取信息，从而减少冗余查询的数量并提高 SMB 1.0 客户端的性能。

> 元数据缓存虽然不太可能为 SMB 1.0 客户端提供过时的信息。如果您的环境无法承担此风险，则不应启用此功能。

启用 **SMB** 元数据缓存

您可以通过启用 SMB 元数据缓存来提高 SMB 1.0 客户端的 SMB 性能。默认情况下，SMB 元数据缓存处于禁用状态。

步骤

1. 执行所需的操作：

如果您要 ...	输入命令 ...
创建共享时启用 SMB 元数据缓存	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
在现有共享上启用 SMB 元数据缓存	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

相关信息

配置 SMB 元数据缓存条目的生命周期

在现有 SMB 共享上添加或删除共享属性

配置 **SMB** 元数据缓存条目的生命周期

您可以配置 SMB 元数据缓存条目的生命周期，以优化环境中的 SMB 元数据缓存性能。默认值为10秒。

开始之前

您必须已启用 SMB 元数据缓存功能。如果未启用 SMB 元数据缓存，则不会使用 SMB 缓存 TTL 设置。

步骤

1. 执行所需的操作：

如果要在以下情况下配置 **SMB** 元数据缓存条目的生命周期 ...	输入命令 ...
创建共享	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
修改现有共享	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

您可以在创建或修改共享时指定其他共享配置选项和属性。有关详细信息，请参见手册页。

管理文件锁定

关于协议之间的文件锁定

文件锁定是客户端应用程序用来防止用户访问先前由另一用户打开的文件的方法。ONTAP 锁定文件的方式取决于客户端的协议。

如果客户端是 NFS 客户端，则建议锁定；如果客户端是 SMB 客户端，则必须锁定。

由于 NFS 和 SMB 文件锁定之间的差异， NFS 客户端可能无法访问先前由 SMB 应用程序打开的文件。

当 NFS 客户端尝试访问 SMB 应用程序锁定的文件时，会发生以下情况：

- 在混合卷或NTFS卷中、文件操作(如) `rm`， `rmdir`，和 `mv` 是否可以对NFS应用程序执行发生原因以使其失败。
- SMB 拒绝读取和拒绝写入打开模式分别拒绝 NFS 读取和写入操作。
- 如果文件的写入范围使用独占 SMB 字节锁锁定，则 NFS 写入操作将失败。
- 取消链接
  - 对于NTFS文件系统、支持SMB和CIFS删除操作。

    上次关闭后、此文件将被删除。
  - 不支持NFS取消链接操作。

    不支持此功能、因为需要NTFS和SMB义、并且NFS不支持上次关闭时删除操作。
  - 对于UNIX文件系统、支持取消链接操作。

    之所以支持此功能、是因为需要NFS和UNIX义。
- 重命名
  - 对于NTFS文件系统、如果目标文件是从SMB或CIFS打开的、则可以重命名目标文件。

- 不支持NFS重命名。

  不支持此功能、因为需要NTFS和SMB义。

在 UNIX 安全模式卷中， NFS 取消链接和重命名操作会忽略 SMB 锁定状态并允许访问文件。UNIX 安全模式卷上的所有其他 NFS 操作均遵循 SMB 锁定状态。

ONTAP 如何处理只读位

只读位会逐个文件进行设置，以反映文件是可写（已禁用）还是只读（已启用）。

使用 Windows 的 SMB 客户端可以设置每个文件的只读位。NFS 客户端不会设置每个文件只读位，因为 NFS 客户端不会执行任何使用每个文件只读位的协议操作。

当使用 Windows 的 SMB 客户端创建文件时， ONTAP 可以在该文件上设置只读位。在 NFS 客户端和 SMB 客户端之间共享文件时， ONTAP 还可以设置只读位。NFS 客户端和 SMB 客户端使用某些软件时，需要启用只读位。

要使 ONTAP 对 NFS 客户端和 SMB 客户端之间共享的文件保持适当的读写权限，它会根据以下规则处理只读位：

- NFS 会将启用了只读位的任何文件视为未启用写入权限位。
- 如果 NFS 客户端禁用了所有写入权限位，并且先前至少启用了其中一个位，则 ONTAP 会为该文件启用只读位。
- 如果 NFS 客户端启用任何写入权限位，则 ONTAP 会禁用该文件的只读位。
- 如果启用了文件的只读位，而 NFS 客户端尝试发现文件的权限，则不会将文件的权限位发送到 NFS 客户端；而 ONTAP 是将权限位发送到 NFS 客户端，并屏蔽写入权限位。
- 如果启用了文件的只读位，而 SMB 客户端禁用了只读位，则 ONTAP 将为此文件启用所有者的写入权限位。
- 启用了只读位的文件只能由 root 用户写入。

> 对文件权限的更改会立即在 SMB 客户端上生效，但如果 NFS 客户端启用属性缓存，则可能不会立即在 NFS 客户端上生效。

在处理共享路径组件上的锁定时， ONTAP 与 Windows 有何不同

与 Windows 不同， ONTAP 不会在打开文件时锁定打开文件的路径的每个组件。此行为也会影响 SMB 共享路径。

由于 ONTAP 不会锁定路径的每个组件，因此可以重命名打开的文件或共享上方的路径组件，这可能会导致某些应用程序出现发生原因问题，也可能发生原因会使 SMB 配置中的共享路径无效。这可能发生原因会使此共享无法访问。

为了避免重命名路径组件导致的问题，您可以应用安全设置来防止用户或应用程序重命名关键目录。

显示有关锁定的信息

您可以显示有关当前文件锁定的信息，包括锁定的锁定类型以及锁定状态，字节范围锁定

，共享锁定模式，委派锁定和机会锁定的详细信息，以及锁定是使用持久句柄还是持久句柄打开的。

关于此任务

对于通过 NFSv4 或 NFSv4.1 建立的锁定，无法显示客户端 IP 地址。

默认情况下，命令会显示有关所有锁定的信息。您可以使用命令参数显示有关特定 Storage Virtual Machine （SVM）锁定的信息，或者按其他条件筛选命令的输出。

。`vserver locks show` 命令可显示有关四种类型的锁定的信息：

- 字节范围锁定，仅锁定文件的一部分。
- 共享锁定，用于锁定打开的文件。
- 机会锁，用于控制 SMB 上的客户端缓存。
- 委派，用于通过 NFSv4.x 控制客户端缓存

通过指定可选参数，您可以确定有关每个锁定类型的重要信息。有关详细信息，请参见命令的手册页。

步骤

1. 使用显示有关锁定的信息 `vserver locks show` 命令：

示例

以下示例显示了路径为的文件上的NFSv4锁定的摘要信息 `/vol1/file1`。共享锁定访问模式为 write-deny_none ，而锁定是通过写入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

以下示例显示路径为的文件上SMB锁定的详细操作锁定和共享锁定信息 `/data2/data2_2/intro.pptx`。对于 IP 地址为 10.3.1.3 的客户端，共享锁定访问模式为 write-deny_none 的文件会授予持久句柄。租用机会锁会授予批量机会锁级别：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
```

```
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
```

```
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

中断锁定

当文件锁定阻止客户端访问文件时，您可以显示有关当前持有的锁定的信息，然后中断特定锁定。可能需要中断锁定的情形示例包括调试应用程序。

关于此任务

。 `vserver locks break` 命令只能在高级权限级别及更高权限级别下使用。命令的手册页包含详细信息。

步骤

1. 要查找解除锁定所需的信息、请使用 `vserver locks show` 命令：

   命令的手册页包含详细信息。

2. 将权限级别设置为高级： `set -privilege advanced`
3. 执行以下操作之一：

如果要通过指定 ... 来中断锁定	输入命令 ...
SVM 名称，卷名称， LIF 名称和文件路径	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
锁定 ID	`vserver locks break -lockid UUID`

4. 返回到管理权限级别： `set -privilege admin`

监控 **SMB** 活动

显示 **SMB** 会话信息

您可以显示有关已建立的 SMB 会话的信息，包括 SMB 连接和会话 ID 以及使用会话的工作站的 IP 地址。您可以显示有关会话的 SMB 协议版本和持续可用保护级别的信息，这有助于确定会话是否支持无中断操作。

关于此任务

您可以摘要形式显示 SVM 上所有会话的信息。但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息：

- 您可以使用可选 `-fields` 用于显示有关所选字段的输出的参数。

  您可以输入 `-fields ?` 以确定您可以使用哪些字段。

- 您可以使用 `-instance` 用于显示有关已建立SMB会话的详细信息的参数。

- 您可以使用 `-fields` 参数或 `-instance` 参数单独使用或与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

要显示 **SMB** 会话信息的项	输入以下命令 **...**
SVM 上的所有会话的摘要形式	`vserver cifs session show -vserver vserver_name`
指定的连接 ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
指定的工作站 IP 地址	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定的 LIF IP 地址	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
在指定节点上	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	指定的 Windows 用户
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	使用指定的身份验证机制
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
使用指定的协议版本	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1
SMB3	SMB3_1}`  [NOTE] ==== 持续可用的保护和 SMB 多通道仅适用于 SMB 3.0 及更高版本的会话。要查看其在所有符合条件的会话中的状态、应指定此参数并将值设置为 `SMB3` 或更高版本。 ====

要显示 **SMB** 会话信息的项	输入以下命令 **...**
具有指定级别的持续可用保护	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 持续可用状态为 `Partial`，这意味着会话至少包含一个打开的持续可用文件，但会话中的某些文件未使用持续可用保护打开。您可以使用 `vserver cifs sessions file show` 命令、用于确定已建立会话中哪些文件未在持续可用的保护下打开。 ====
具有指定的 SMB 签名会话状态	`vserver cifs session show -vserver vserver_name -is-session-signed {true

示例

以下命令显示 SVM vs1 上从 IP 地址为 10.1.1.1 的工作站建立的会话的会话信息：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

以下命令显示 SVM vs1 上具有持续可用保护的会话的详细会话信息。此连接是使用域帐户建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

以下命令显示 SVM vs1 上使用 SMB 3.0 和 SMB 多通道的会话的会话信息。在此示例中，用户使用 LIF IP 地址从支持 SMB 3.0 的客户端连接到此共享；因此，身份验证机制默认为 NTLMv2 。必须使用 Kerberos 身份验证进行连接，以获得持续可用的保护。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
               Connected Time: 6m 22s
                    Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

相关信息

显示有关打开的 SMB 文件的信息

显示有关打开的 SMB 文件的信息

您可以显示有关打开的 SMB 文件的信息，包括 SMB 连接和会话 ID ，托管卷，共享名称和共享路径。您可以显示有关文件的持续可用保护级别的信息，这有助于确定打开的文件是否处于支持无中断操作的状态。

关于此任务

您可以显示有关已建立的 SMB 会话上打开的文件的信息。如果需要确定 SMB 会话中特定文件的 SMB 会话信息，则显示的信息非常有用。

例如、如果您有一个SMB会话、其中一些打开的文件已打开且具有持续可用的保护、而另一些文件未打开且具有持续可用的保护(的值 `-continuously-available` 字段输入 `vserver cifs session show` 命令输出为 `Partial`)、则可以使用此命令确定哪些文件不持续可用。

您可以使用以摘要形式显示Storage Virtual Machine (SVM)上已建立的SMB会话上的所有打开文件的信息 `vserver cifs session file show` 命令、而不带任何可选参数。

但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息。如果您只想查看一小部分打开文件的信息，这将非常有用。

- 您可以使用可选 `-fields` 用于显示所选字段的输出的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

- 您可以使用 `-instance` 用于显示有关打开的SMB文件的详细信息的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
以摘要形式显示在 SVM 上	`vserver cifs session file show -vserver vserver_name`
在指定节点上	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	指定的文件 ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定的 SMB 连接 ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定的 SMB 会话 ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的托管聚合上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定卷上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定的 SMB 共享上
`vserver cifs session file show -vserver vserver_name -share share_name`	指定的 SMB 路径上
`vserver cifs session file show -vserver vserver_name -path path`	具有指定级别的持续可用保护

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 持续可用状态为 `No`，这意味着这些打开的文件无法从接管和恢复中无系统地恢复。它们也无法从高可用性关系中的合作伙伴之间的常规聚合重新定位中恢复。 ====
具有指定的重新连接状态	`vserver cifs session file show -vserver vserver_name -reconnected {No

您可以使用其他可选参数来细化输出结果。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上打开的文件的信息：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

以下示例显示了有关 SVM vs1 上文件 ID 82 的已打开 SMB 文件的详细信息：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                   Node: node1
                Vserver: vs1
                File ID: 82
          Connection ID: 104617
             Session ID: 1
              File Type: Regular
              Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
             Share Mode: rw
            Range Locks: 1
Continuously Available: Yes
            Reconnected: No
```

相关信息

显示 SMB 会话信息

确定可用的统计信息对象和计数器

在获取有关 CIFS ， SMB ，审核和 BranchCache 哈希统计信息以及监控性能的信息之前，您必须了解哪些对象和计数器可用于获取数据。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

要确定的内容	输入 ...
哪些对象可用	`statistics catalog object show`
可用的特定对象	`statistics catalog object show object object_name`
哪些计数器可用	`statistics catalog counter show object object_name`

有关哪些对象和计数器可用的详细信息，请参见手册页。

3. 返回到管理权限级别： `set -privilege admin`

示例

以下命令显示与集群中的 CIFS 和 SMB 访问相关的选定统计信息对象的说明，如高级权限级别所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

以下命令显示有关的某些计数器的信息 `cifs` 对象、如高级权限级别所示：

> 此示例不会显示的所有可用计数器 `cifs` 对象；输出被截断。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                             vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

相关信息

显示统计信息

您可以显示各种统计信息，包括有关 CIFS 和 SMB ，审核和 BranchCache 哈希的统计信息，以监控性能并诊断问题。

开始之前

您必须已使用收集数据样本 `statistics start` 和 `statistics stop` 命令、然后才能显示有关对象的信息。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

要显示统计信息的对象	输入 ...
SMB 的所有版本	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x 和 SMB 3.0	`statistics show -object smb2`
节点的 CIFS 子系统	`statistics show -object nblade_cifs`
多协议审核	`statistics show -object audit_ng`
BranchCache 哈希服务	`statistics show -object hashd`
动态 DNS	`statistics show -object ddns_update`

有关详细信息，请参见每个命令的手册页。

3. 返回到管理权限级别： `set -privilege admin`

相关信息

确定可用的统计信息对象和计数器

监控 SMB 签名会话统计信息

显示 BranchCache 统计信息

使用统计信息监控自动节点转介活动

"Microsoft Hyper-V 和 SQL Server 的 SMB 配置"

"性能监控设置"

部署基于 SMB 客户端的服务

使用脱机文件可以缓存文件以供脱机使用

使用脱机文件允许缓存文件以供脱机使用概述

ONTAP 支持 Microsoft 脱机文件功能或 *client-side cacheration*、 该功能允许将文件缓存在本地主机上以供脱机使用。即使与网络断开连接，用户也可以使用脱机文件功能继续处理文件。

您可以指定 Windows 用户文档和程序是否自动缓存在共享上，或者是否必须手动选择文件进行缓存。默认情况下，新共享会启用手动缓存。脱机可用的文件将同步到 Windows 客户端的本地磁盘。恢复与特定存储系统共享的网络连接时，将发生同步。

由于脱机文件和文件夹保留的访问权限与保存在 CIFS 服务器上的文件和文件夹版本相同，因此用户必须对保存在 CIFS 服务器上的文件和文件夹拥有足够的权限，才能对脱机文件和文件夹执行操作。

当用户和网络上的其他人更改同一文件时，用户可以将该文件的本地版本保存到网络，保留另一个版本或同时保存这两者。如果用户同时保留这两个版本，则包含本地用户所做更改的新文件将保存在本地，缓存的文件将被保存在 CIFS 服务器上的文件版本所做的更改覆盖。

您可以使用共享配置设置基于共享配置脱机文件。在创建或修改共享时，您可以从四种脱机文件夹配置中选择一种：

- 无缓存

  禁用共享的客户端缓存。文件和文件夹不会自动缓存在客户端本地，用户也无法选择在本地缓存文件或文件夹。

- 手动缓存

  允许手动选择要缓存在共享上的文件。这是默认设置。默认情况下，不会在本地客户端上缓存任何文件或文件夹。用户可以选择要在本地缓存哪些文件和文件夹以供脱机使用。

- 自动文档缓存

  允许用户文档自动缓存在共享上。只有被访问的文件和文件夹才会在本地缓存。

- 自动程序缓存

  允许程序和用户文档自动缓存在共享上。只有被访问的文件，文件夹和程序才会在本地缓存。此外，即使连接到网络，此设置也允许客户端运行本地缓存的可执行文件。

有关在 Windows 服务器和客户端上配置脱机文件的详细信息，请参阅 Microsoft TechNet 库。

相关信息

使用漫游配置文件将用户配置文件集中存储在与 SVM 关联的 CIFS 服务器上

使用文件夹重定向将数据存储在 CIFS 服务器上

使用 BranchCache 在分支机构缓存 SMB 共享内容

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

使用脱机文件的要求

在 CIFS 服务器上使用 Microsoft 脱机文件功能之前，您需要了解哪些版本的 ONTAP 和 SMB 以及哪些 Windows 客户端支持此功能。

ONTAP 版本要求

ONTAP 版本支持脱机文件。

SMB 协议版本要求

对于 Storage Virtual Machine （ SVM ）， ONTAP 在所有 SMB 版本上均支持脱机文件。

Windows 客户端要求

Windows 客户端必须支持脱机文件。

有关哪些 Windows 客户端支持脱机文件功能的最新信息，请参见互操作性表。

"mysupport.netapp.com/matrix"

部署脱机文件的准则

在具有的主目录共享上部署脱机文件时、需要了解一些重要准则 `showsnapshot` 在主目录上设置共享属性。

如果 `showsnapshot` 共享属性在配置了脱机文件的主目录共享上设置、Windows客户端会将所有Snapshot副本缓存在下 `~snapshot` 文件夹。

如果满足以下条件之一，则 Windows 客户端会将所有 Snapshot 副本缓存到主目录下：

- 用户使主目录可从客户端脱机使用。

  的内容 `~snapshot` 主目录中的文件夹将包含在内、并可脱机使用。

- 用户配置文件夹重定向以重定向文件夹、例如 `My Documents` 到驻留在CIFS服务器共享上的主目录的根目录。

  某些 Windows 客户端可能会自动使重定向的文件夹脱机可用。如果文件夹重定向到主目录的根目录、则 `~snapshot` 文件夹包含在缓存的脱机内容中。

> 脱机文件部署、其中 `~snapshot` 应避免脱机文件中包含文件夹。中的Snapshot副本 `~snapshot` 文件夹包含卷上ONTAP创建Snapshot副本时的所有数据。因此、请创建的脱机副本 `~snapshot` 文件夹会占用客户端上的大量本地存储、在脱机文件同步期间占用网络带宽、并增加同步脱机文件所需的时间。

您可以使用 ONTAP 命令行界面配置脱机文件支持，方法是在创建 SMB 共享时指定四个脱机文件设置之一，或者随时修改现有 SMB 共享。默认设置为手动脱机文件支持。

关于此任务

配置脱机文件支持时，您可以选择以下四种脱机文件设置之一：

正在设置 ...	**Description**
`none`	禁止 Windows 客户端缓存此共享上的任何文件。
`manual`	允许 Windows 客户端上的用户手动选择要缓存的文件。
`documents`	允许 Windows 客户端缓存用户用于脱机访问的用户文档。
`programs`	允许 Windows 客户端缓存用户用于脱机访问的程序。即使共享可用，客户端也可以在脱机模式下使用缓存的程序文件。

您只能选择一个脱机文件设置。如果修改现有 SMB 共享上的脱机文件设置，则新的脱机文件设置将替换原始设置。不会删除或替换其他现有 SMB 共享配置设置和共享属性。它们将一直有效，直到被明确删除或更改为止。

步骤

1. 执行相应的操作：

要配置脱机文件的位置	输入命令 ...
新的 SMB 共享	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	现有 SMB 共享
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. 验证SMB共享配置是否正确： `vserver cifs share show -vserver vserver_name -share -name share_name -instance`

示例

以下命令将创建名为`data1`的SMB共享、其中脱机文件设置为 `documents`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

以下命令会通过将脱机文件设置更改为来修改名为`data1`的现有SMB共享 `manual` 并为文件和目录模式创建掩码添加值：

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: 644
     Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相关信息

在现有 SMB 共享上添加或删除共享属性

使用计算机管理 **MMC** 在 **SMB** 共享上配置脱机文件支持

如果要允许用户在本地缓存文件以供脱机使用，您可以使用计算机管理 MMC （Microsoft 管理控制台）配置脱机文件支持。

步骤

1. 要在 Windows 服务器上打开 MMC ，请在 Windows 资源管理器中右键单击本地计算机的图标，然后选择 * 管理 * 。
2. 在左侧面板上，选择 * 计算机管理 * 。
3. 选择 * 操作 * > * 连接到另一台计算机 * 。

   此时将显示选择计算机对话框。

4. 键入 CIFS 服务器的名称或单击 * 浏览 * 以查找 CIFS 服务器。

   如果 CIFS 服务器的名称与 Storage Virtual Machine （SVM）主机名相同，请键入 SVM 名称。如果 CIFS 服务器名称与 SVM 主机名称不同，请键入 CIFS 服务器的名称。

5. 单击 * 确定 * 。
6. 在控制台树中，单击 * 系统工具 * > * 共享文件夹 * 。
7. 单击 * 共享 * 。
8. 在结果窗格中，右键单击共享。
9. 单击 * 属性 * 。

   此时将显示选定共享的属性。

10. 在 * 常规 * 选项卡中，单击 * 脱机设置 * 。

    此时将显示脱机设置对话框。

11. 根据需要配置脱机可用性选项。
12. 单击 * 确定 * 。

使用漫游配置文件将用户配置文件集中存储在与 **SVM** 关联的 **SMB** 服务器上

使用漫游配置文件将用户配置文件集中存储在与 **SVM** 概述关联的 **SMB** 服务器上

ONTAP 支持将 Windows 漫游配置文件存储在与 Storage Virtual Machine （ SVM ）关联的 CIFS 服务器上。配置用户漫游配置文件可为用户带来优势，例如，无论用户登录到何处，均可自动获得资源。漫游配置文件还可以简化用户配置文件的管理。

漫游用户配置文件具有以下优势：

- 自动资源可用性

  当用户登录到网络上运行 Windows 8 ， Windows 7 ， Windows 2000 或 Windows XP 的任何计算机时，该用户的唯一配置文件将自动可用。用户无需在网络上使用的每台计算机上创建配置文件。

- 简化了计算机更换

  由于用户的所有配置文件信息都在网络上单独维护，因此用户的配置文件可以轻松下载到新的替代计算机上。当用户首次登录到新计算机时，用户配置文件的服务器副本将复制到新计算机。

相关信息

使用脱机文件允许缓存文件以供脱机使用

使用文件夹重定向将数据存储在 CIFS 服务器上

使用漫游配置文件的要求

在 CIFS 服务器上使用 Microsoft 的漫游配置文件之前，您需要了解哪些版本的 ONTAP 和 SMB 以及哪些 Windows 客户端支持此功能。

ONTAP 版本要求

ONTAP 支持漫游配置文件。

SMB 协议版本要求

对于 Storage Virtual Machine （ SVM ）， ONTAP 支持在所有 SMB 版本上使用漫游配置文件。

Windows 客户端要求

在用户使用漫游配置文件之前， Windows 客户端必须支持此功能。

有关哪些 Windows 客户端支持漫游配置文件的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

配置漫游配置文件

如果要在用户登录到网络上的任何计算机时自动使其配置文件可用，则可以通过 Active Directory 用户和计算机 MMC 管理单元配置漫游配置文件。如果要在Windows Server上配置漫游配置文件、则可以使用Active Directory管理中心。

步骤

1. 在Windows服务器上、打开Active Directory用户和计算机MMC (或Windows服务器上的Active Directory管理中心)。
2. 找到要为其配置漫游配置文件的用户。
3. 右键单击该用户，然后单击 * 属性 * 。
4. 在*配置文件*选项卡上，输入要存储用户漫游配置文件的共享的配置文件路径，然后输入 `%username%`。

   例如、配置文件路径可能如下所示： `\\vs1.example.com\profiles\%username%`。用户首次登录时、 `%username%` 替换为用户名。

   > 在路径中 `\\vs1.example.com\profiles\%username%`， `profiles` 是Storage Virtual Machine (SVM) VS1上对任何人都具有完全控制权限的共享的共享名称。

5. 单击 * 确定 * 。

使用文件夹重定向将数据存储在 **SMB** 服务器上

使用文件夹重定向将数据存储在 **SMB** 服务器概述中

ONTAP 支持 Microsoft 文件夹重定向，用户或管理员可以通过此功能将本地文件夹的路径重定向到 CIFS 服务器上的某个位置。重定向的文件夹似乎存储在本地 Windows 客户端上，即使数据存储在 SMB 共享上也是如此。

文件夹重定向主要用于已部署主目录并希望与现有主目录环境保持兼容的组织。

- `Documents`， `Desktop`，和 `Start Menu` 是可以重定向的文件夹示例。
- 用户可以从其 Windows 客户端重定向文件夹。
- 管理员可以通过在 Active Directory 中配置 GPO 来集中配置和管理文件夹重定向。
- 如果管理员配置了漫游配置文件，则通过文件夹重定向，管理员可以将用户数据与配置文件数据分开。

- 管理员可以同时使用文件夹重定向和脱机文件将本地文件夹的数据存储重定向到 CIFS 服务器，同时允许用户在本地缓存内容。

相关信息

使用脱机文件允许缓存文件以供脱机使用

使用漫游配置文件将用户配置文件集中存储在与 SVM 关联的 CIFS 服务器上

使用文件夹重定向的要求

在 CIFS 服务器上使用 Microsoft 的文件夹重定向之前，您需要了解哪些版本的 ONTAP 和 SMB 以及哪些 Windows 客户端支持此功能。

ONTAP 版本要求

ONTAP 支持 Microsoft 文件夹重定向。

SMB 协议版本要求

对于 Storage Virtual Machine （ SVM ）， ONTAP 在所有 SMB 版本上均支持 Microsoft 的文件夹重定向。

Windows 客户端要求

在用户使用 Microsoft 的文件夹重定向之前， Windows 客户端必须支持此功能。

有关哪些 Windows 客户端支持文件夹重定向的最新信息，请参见互操作性表。

"mysupport.netapp.com/matrix"

配置文件夹重定向

您可以使用 Windows 属性窗口配置文件夹重定向。使用此方法的优点是， Windows 用户可以在没有 SVM 管理员协助的情况下配置文件夹重定向。

步骤

1. 在 Windows 资源管理器中，右键单击要重定向到网络共享的文件夹。
2. 单击 * 属性 * 。

   此时将显示选定共享的属性。

3. 在 * 快捷方式 * 选项卡中，单击 * 目标 * 并指定要重定向选定文件夹的网络位置的路径。

   例如、如果要将文件夹重定向到 `data` 主目录中映射到的文件夹 `Q:\`、请指定 `Q:\data` 作为目标。

4. 单击 * 确定 * 。

   有关配置脱机文件夹的详细信息，请参阅 Microsoft TechNet 库。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

使用 **SMB 2.x** 从 **Windows** 客户端访问 **~Snapshot** 目录

用于访问的方法 `~snapshot` 使用SMB 2.x的Windows客户端的目录与使用SMB 1.0的方法不同。您需要了解如何访问 `~snapshot` 使用SMB 2.x连接成功访问Snapshot副本中存储的数据时的目录。

SVM管理员控制Windows客户端上的用户是否可以查看和访问 `~snapshot` 通过启用或禁用共享上的目录 `showsnapshot` 使用Vserver CIFS共享属性系列中的命令共享属性。

当 `showsnapshot` 共享属性已禁用、使用SMB 2.x的Windows客户端上的用户无法查看 `~snapshot` 目录中的Snapshot副本 `~snapshot` 目录、即使手动输入的路径也是如此 `~snapshot` 目录或目录中的特定Snapshot副本。

当 `showsnapshot` 已启用共享属性、使用SMB 2.x的Windows客户端上的用户仍无法查看 `~snapshot` 目录位于共享根目录或共享根目录下的任何接合或目录中。但是、在连接到共享后、用户可以访问隐藏的 `~snapshot` 目录 `\~snapshot` 到共享路径的末尾。隐藏的 `~snapshot` 可从两个入口点访问目录：

- 位于共享的根目录
- 共享空间中的每个接合点

隐藏的 `~snapshot` 无法从共享中的非接合子目录访问目录。

示例

对于以下示例中所示的配置、SMB 2.x连接到"`eng`"共享的Windows客户端上的用户可以访问 `~snapshot` 目录 `\~snapshot` 共享路径位于共享的根目录以及路径中的每个接合点。隐藏的 `~snapshot` 可从以下三个路径访问目录：

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

使用先前版本恢复文件和文件夹

使用先前版本概述恢复文件和文件夹

使用 Microsoft 先前版本的功能适用于支持某种形式的 Snapshot 副本并已启用这些副本的文件系统。Snapshot 技术是 ONTAP 不可或缺的一部分。用户可以使用 Microsoft 先前版本功能从 Windows 客户端的 Snapshot 副本恢复文件和文件夹。

通过先前版本的功能，用户可以浏览 Snapshot 副本或从 Snapshot 副本还原数据，而无需存储管理员干预。先前版本不可配置。它始终处于启用状态。如果存储管理员在共享上提供了 Snapshot 副本，则用户可以使用先前版本执行以下任务：

- 恢复意外删除的文件。
- 从意外覆盖文件中恢复。
- 在工作时比较文件版本。

Snapshot 副本中存储的数据为只读数据。用户必须将文件的副本保存到其他位置，才能对文件进行任何更改。Snapshot 副本会定期删除；因此，如果用户要无限期保留某个文件的先前版本，则需要为先前版本中包含的文件创建副本。

使用 **Microsoft** 先前版本的要求

在 CIFS 服务器上使用先前版本之前，您需要了解哪些版本的 ONTAP 和 SMB 以及哪些 Windows 客户端支持它。您还需要了解 Snapshot 副本设置要求。

ONTAP 版本要求

支持先前版本。

SMB 协议版本要求

对于 Storage Virtual Machine （ SVM ）， ONTAP 在所有 SMB 版本上均支持先前版本。

Windows 客户端要求

在用户使用早期版本访问 Snapshot 副本中的数据之前， Windows 客户端必须支持此功能。

有关哪些 Windows 客户端支持先前版本的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

Snapshot 副本设置的要求

要使用先前版本访问 Snapshot 副本中的数据，必须将已启用的 Snapshot 策略与包含数据的卷相关联，客户端必须能够访问 Snapshot 数据，并且 Snapshot 副本必须存在。

使用先前版本选项卡查看和管理 **Snapshot** 副本数据

Windows 客户端计算机上的用户可以使用 Windows 属性窗口中的先前版本选项卡还原 Snapshot 副本中存储的数据，而无需让 Storage Virtual Machine （ SVM ）管理员参与。

关于此任务

只有当管理员已在包含共享的卷上启用 Snapshot 副本，并且管理员将共享配置为显示 Snapshot 副本时，才能使用先前版本选项卡查看和管理 SVM 上存储的数据的 Snapshot 副本中的数据。

步骤

1. 在 Windows 资源管理器中，显示存储在 CIFS 服务器上的数据的映射驱动器内容。
2. 右键单击映射的网络驱动器中要查看或管理其 Snapshot 副本的文件或文件夹。
3. 单击 * 属性 * 。

   此时将显示选定文件或文件夹的属性。

4. 单击 * 先前版本 * 选项卡。

   选定文件或文件夹的可用 Snapshot 副本列表将显示在文件夹版本：框中。列出的 Snapshot 副本由 Snapshot 副本名称前缀和创建时间戳标识。

5. 在 * 文件夹版本： * 框中，右键单击要管理的文件或文件夹的副本。
6. 执行相应的操作：

如果您要 ...	执行以下操作 ...
查看该 Snapshot 副本中的数据	单击 * 打开 * 。
从该 Snapshot 副本创建一份数据副本	单击 * 复制 * 。

   Snapshot 副本中的数据为只读。如果要修改 " 先前版本 " 选项卡中列出的文件和文件夹，必须将要修改的文件和文件夹的副本保存到可写位置，并对这些副本进行修改。

7. 管理完 Snapshot 数据后，单击 * 确定 * 以关闭 * 属性 * 对话框。

   有关使用先前版本选项卡查看和管理 Snapshot 数据的详细信息，请参阅 Microsoft TechNet 库。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

确定先前版本是否可以使用 **Snapshot** 副本

只有当已启用的 Snapshot 策略应用于包含共享的卷，并且卷配置允许访问 Snapshot 副本时，才能从先前版本选项卡查看 Snapshot 副本。在帮助用户访问先前版本时，确定 Snapshot 副本可用性非常有用。

步骤

1. 确定共享数据所在的卷是否已启用自动Snapshot副本、以及客户端是否有权访问Snapshot目录： `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   输出将显示与卷关联的 Snapshot 策略，是否启用了客户端 Snapshot 目录访问以及可用 Snapshot 副本的数量。

2. 确定是否已启用关联的Snapshot策略： `volume snapshot policy show -policy policy-name`
3. 列出可用的Snapshot副本： `volume snapshot show -volume volume_name`

   有关配置和管理 Snapshot 策略和 Snapshot 计划的详细信息，请参见 "数据保护"。

示例

以下示例显示了与名为 `data1` 的卷关联的 Snapshot 策略的信息，该卷包含 " `data1` " 上的共享数据和可用 Snapshot 副本。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ----------------------------------
default                    3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- -------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                            ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

相关信息

创建 Snapshot 配置以启用先前版本的访问

"数据保护"

创建 **Snapshot** 配置以启用先前版本的访问

如果已启用客户端对 Snapshot 副本的访问，并且存在 Snapshot 副本，则先前版本的功能始终可用。如果 Snapshot 副本配置不满足这些要求，则可以创建一个 Snapshot 副本配置。

步骤

1. 如果包含要允许先前版本访问的共享的卷没有关联的Snapshot策略、请将Snapshot策略与该卷关联、然后使用启用它 `volume modify` 命令：

   有关使用的详细信息、请参见 `volume modify` 命令、请参见手册页。

2. 使用启用对Snapshot副本的访问 `volume modify` 命令以设置 `-snap-dir` 选项 `true`。

   有关使用的详细信息、请参见 `volume modify` 命令、请参见手册页。

3. 使用验证是否已启用Snapshot策略以及是否已启用对Snapshot目录的访问 `volume show` 和 `volume snapshot policy show` 命令

   有关使用的详细信息、请参见 `volume show` 和 `volume snapshot policy show` 命令、请参见手册页。

   有关配置和管理 Snapshot 策略和 Snapshot 计划的详细信息，请参见 "数据保护"。

相关信息

"数据保护"

还原包含接合的目录的准则

在使用早期版本还原包含接合点的文件夹时，应牢记一些特定准则。

如果使用先前版本还原包含作为接合点的子文件夹的文件夹、则还原可能会失败、并显示 `Access Denied` 错误。

您可以使用确定要尝试还原的文件夹是否包含接合 `vol show` 命令 `-parent` 选项您也可以使用 `vserver security trace` 用于创建有关文件和文件夹访问问题的详细日志的命令。

相关信息

在 NAS 命名空间中创建和管理数据卷

部署基于 **SMB** 服务器的服务

管理主目录

ONTAP 如何启用动态主目录

通过 ONTAP 主目录，您可以配置一个 SMB 共享，该共享根据连接到它的用户和一组变量映射到不同的目录。您可以使用一些主目录参数配置一个共享，以定义入口点（共享）与主目录（ SVM 上的目录）之间的用户关系，而不是为每个用户创建单独的共享。

以来宾用户身份登录的用户没有主目录，无法访问其他用户的主目录。可通过四个变量确定用户映射到目录的方式：

- * 共享名称 *

  这是您创建的共享的名称，用户将连接到该共享。您必须为此共享设置主目录属性。

共享名称可以使用以下动态名称：

  - `%w` (用户的Windows用户名)
  - `%d` (用户的Windows域名)
  - `%u` (用户的映射UNIX用户名)
    要使共享名称在所有主目录中都是唯一的、共享名称必须包含/`%w` 或 `%u` 变量。共享名称可以同时包含 `%d` 和/`%w` 变量(例如、 `%d/%w`)、或者共享名称可以包含静态部分和可变部分(例如、HOME_/`%w`）。

- * 共享路径 *

  此路径是由共享定义的相对路径，因此与某个共享名称关联，并附加到每个搜索路径中，以便从 SVM 的根目录生成用户的整个主目录路径。它可以是静态的(例如、 `home`)、动态(例如、 `%w`)或两者的组合(例如、`eng/%w`）。

- * 搜索路径 *

  这是从 SVM 根目录开始的一组绝对路径，您可以指定这些绝对路径来指示 ONTAP 搜索主目录。您可以使用指定一个或多个搜索路径 `vserver cifs home-directory search-path add` 命令：如果指定了多个搜索路径，则 ONTAP 将按指定顺序尝试这些路径，直到找到有效路径为止。

- * 目录 *

  这是您为用户创建的用户主目录。目录名称通常是用户的名称。您必须在搜索路径定义的一个目录中创建主目录。

例如，请考虑以下设置：

- 用户： John Smith
- 用户域： acme
- 用户名： jsmith
- SVM 名称： vs1
- 主目录共享名称1：HOME_ `%w` -共享路径： `%w`
- 主目录共享名称2： `%w` -共享路径： `%d/%w`
- 搜索路径1： `/vol0home/home`
- 搜索路径2： `/vol1home/home`
- 搜索路径3： `/vol2home/home`
- 主目录： `/vol1home/home/jsmith`

场景1：用户连接到 `\\vs1\home_jsmith`。这与第一个主目录共享名称匹配并生成相对路径 `jsmith`。现在、ONTAP将搜索名为的目录 `jsmith` 按顺序检查每个搜索路径：

- `/vol0home/home/jsmith` 不存在；继续搜索路径2。
- `/vol1home/home/jsmith` 存在；因此、不会检查搜索路径3；用户现在已连接到其主目录。

场景2：用户连接到 `\\vs1\jsmith`。这与第二个主目录共享名称匹配并生成相对路径 `acme/jsmith`。现

在、ONTAP将搜索名为的目录 `acme/jsmith` 按顺序检查每个搜索路径：

- `/vol0home/home/acme/jsmith` 不存在；继续搜索路径2。
- `/vol1home/home/acme/jsmith` 不存在；继续搜索路径3。
- `/vol2home/home/acme/jsmith` 不存在；主目录不存在；因此连接失败。

主目录共享

添加主目录共享

如果要使用 SMB 主目录功能，则必须至少添加一个共享，并将主目录属性包含在共享属性中。

关于此任务

您可以在创建主目录共享时使用创建此共享 `vserver cifs share create` 命令、或者您可以随时使用将现有共享更改为主目录共享 `vserver cifs share modify` 命令：

要创建主目录共享、必须包含 `homedirectory` 中的值 `-share-properties` 选项。您可以使用变量指定共享名称和共享路径，这些变量在用户连接到其主目录时会动态扩展。可在路径中使用的可用变量为 `%w`， `%d`，和 `%u`，分别对应于Windows用户名、域和映射的UNIX用户名。

步骤

1. 添加主目录共享：+
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` 指定已启用CIFS且要添加搜索路径的Storage Virtual Machine (SVM)。

   `-share-name` *`share-name`* 指定主目录共享名称。

   除了包含一个必需的变量之外、如果共享名称还包含一个文字字符串 `%w`， `%u``或 `%d`，必须在文本字符串前面加上%(百分比)字符，以防止ONTAP将文本字符串视为变量(例如， `%%w`）。

   - 共享名称必须包含 `%w` 或 `%u` 变量。
   - 此外、共享名称还可以包含 `%d` 变量(例如、 `%d/%w`)或共享名称中的静态部分(例如home_1_/`%w`）。
   - 如果管理员使用共享连接到其他用户的主目录或允许用户连接到其他用户的主目录，则动态共享名称模式前面必须有一个颚化符（~ ）。

     。 `vserver cifs home-directory modify` 用于通过设置启用此访问 `-is-home-dirs-access-for-admin-enabled` 选项 `true`)或设置高级选项 `-is-home-dirs-access-for-public-enabled` to `true`。

   `-path path` 指定主目录的相对路径。

`-share-properties homedirectory[,…]` 指定该共享的共享属性。您必须指定 `homedirectory` 价值。您可以使用逗号分隔列表指定其他共享属性。

1. 使用验证是否已成功添加主目录共享 `vserver cifs share show` 命令：

示例

以下命令将创建名为的主目录共享 `%w`。。 `oplocks`， `browsable`，和 `changenotify` 除了设置之外、还会设置共享属性 `homedirectory` 共享属性。

> 此示例不会显示 SVM 上所有共享的输出。输出被截断。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

相关信息

正在添加主目录搜索路径

使用自动节点转介的要求和准则

管理用户主目录的可访问性

主目录共享需要唯一的用户名

使用创建主目录共享时、请注意分配唯一的用户名 `%w` (Windows用户名)或 `%u` (UNIX用户名)用于动态生成共享的变量。共享名称将映射到您的用户名。

如果静态共享的名称和用户的名称相同，则可能会出现两个问题：

- 当用户使用列出集群上的共享时 `net view` 命令、则会显示两个具有相同用户名的共享。
- 当用户连接到该共享名称时，该用户始终连接到静态共享，并且无法访问同名的主目录共享。

例如，有一个名为 "`administrator` " 的共享，您有一个 "`administrator` " 的 Windows 用户名。如果创建主目录共享并连接到该共享，则会连接到 "`administrator` " 静态共享，而不是 "`administrator` " 主目录共享。

您可以按照以下任一步骤使用重复的共享名称解析问题描述：

- 重命名静态共享，使其不再与用户的主目录共享冲突。
- 为用户提供新的用户名，使其不再与静态共享名称冲突。
- 使用静态名称(例如"`home`")创建CIFS主目录共享、而不是使用 `%w` 参数以避免与共享名称冲突。

升级后静态主目录共享名称会发生什么情况

主目录共享名称必须包含 `%w` 或 `%u` 动态变量。您应了解在根据新要求升级到 ONTAP 版本后现有静态主目录共享名称会发生什么情况。

如果主目录配置包含静态共享名称，而您升级到 ONTAP ，则静态主目录共享名称不会更改，并且仍然有效。但是、您不能创建任何不包含的新主目录共享 `%w` 或 `%u` 变量。

要求将其中一个变量包含在用户的主目录共享名称中，可确保每个共享名称在整个主目录配置中都是唯一的。如果需要、您可以将静态主目录共享名称更改为包含任一的名称 `%w` 或 `%u` 变量。

添加主目录搜索路径

如果要使用 ONTAP SMB 主目录，必须至少添加一个主目录搜索路径。

关于此任务

您可以使用添加主目录搜索路径 `vserver cifs home-directory search-path add` 命令：

。 `vserver cifs home-directory search-path add` 命令会检查中指定的路径 `-path` 选项。如果指定的路径不存在，该命令将生成一条消息，提示您是否要继续。任您选择 `y` 或 `n`。如果您选择 `y` 要继续操作、ONTAP将创建搜索路径。但是，必须先创建目录结构，然后才能在主目录配置中使用搜索路径。如果选择不继续，则命令将失败；不会创建搜索路径。然后、您可以创建路径目录结构并重新运行 `vserver cifs home-directory search-path add` 命令：

步骤

1. 添加主目录搜索路径： `vserver cifs home-directory search-path add -vserver vserver -path path`
2. 使用验证是否已成功添加搜索路径 `vserver cifs home-directory search-path show` 命令：

示例

以下示例将添加路径 `/home1` 到SVM VS1上的主目录配置。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

以下示例将尝试添加路径 `/home2` 到SVM VS1上的主目录配置。此路径不存在。选择不继续。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

相关信息

添加主目录共享

使用 %w 和 %d 变量创建主目录配置

您可以使用创建主目录配置 `%w` 和 `%d` 变量。然后，用户可以使用动态创建的共享连接到其主共享。

步骤

1. 创建一个qtree以包含用户的主目录： `volume qtree create -vserver vserver_name -qtree -path qtree_path`
2. 验证qtree是否使用正确的安全模式： `volume qtree show`
3. 如果qtree未使用所需的安全模式、请使用更改安全模式 `volume qtree security` 命令：
4. 添加主目录共享： `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` 指定已启用CIFS且要添加搜索路径的Storage Virtual Machine (SVM)。

   `-share-name %w` 指定主目录共享名称。当每个用户连接到其主目录时， ONTAP 会动态创建共享名称。共享名称的格式为 *windows_user_name* 。

   `-path %d/%w` 指定主目录的相对路径。当每个用户连接到其主目录时，系统会动态创建相对路径，其格式为 *domain/windows_user_name* 。

   `-share-properties homedirectory[,…]+` 指定该共享的共享属性。您必须指定 `homedirectory` 价值。您可以使用逗号分隔列表指定其他共享属性。
5. 使用验证共享是否具有所需的配置 `vserver cifs share show` 命令：
6. 添加主目录搜索路径： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* 指定已启用CIFS且要添加搜索路径的SVM。

   `-path` *`path`* 指定搜索路径的绝对目录路径。
7. 使用验证是否已成功添加搜索路径 `vserver cifs home-directory search-path show` 命令：
8. 对于具有主目录的用户，请在指定用于包含主目录的 qtree 或卷中创建相应的目录。

   例如、如果您创建的qtree的路径为 `/vol/vol1/users` 要创建其目录的用户名是mydomain\user1、则应使用以下路径创建目录： `/vol/vol1/users/mydomain/user1`。

如果您创建了一个名为"`home/"的卷、则挂载于 `/home1`，则应使用以下路径创建目录：`/home1/mydomain/user1`。

9. 通过映射驱动器或使用 UNC 路径进行连接，验证用户是否可以成功连接到主共享。

   例如、如果用户mydomain\user1要连接到在步骤8中创建的位于SVM VS1上的目录、则user1将使用UNC路径进行连接 `\\vs1\user1`。

示例

以下示例中的命令使用以下设置创建主目录配置：

- 共享名称为 %w
- 相对主目录路径为 %d/%w
- 用于包含主目录的搜索路径、 `/home1`是配置了NTFS安全模式的卷。
- 此时将在 SVM vs1 上创建配置。

当用户从 Windows 主机访问其主目录时，您可以使用此类主目录配置。如果用户从 Windows 和 UNIX 主机访问其主目录，而文件系统管理员使用基于 Windows 的用户和组来控制对文件系统的访问，则也可以使用此类配置。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

相关信息

使用 %u 变量配置主目录

其他主目录配置

显示有关 SMB 用户主目录路径的信息

使用 %u 变量配置主目录

您可以创建主目录配置、在该配置中使用指定共享名称 `%w` 变量、但您使用 `%u` 用于指定主目录共享的相对路径的变量。然后，用户可以使用使用其 Windows 用户名动态创建的共享连接到其主目录共享，而无需知道主目录的实际名称或路径。

步骤

1. 创建一个qtree以包含用户的主目录： `volume qtree create -vserver vserver_name -qtree -path qtree_path`
2. 验证qtree是否使用正确的安全模式： `volume qtree show`
3. 如果qtree未使用所需的安全模式、请使用更改安全模式 `volume qtree security` 命令：
4. 添加主目录共享： `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` 指定已启用CIFS且要添加搜索路径的Storage Virtual Machine (SVM)。

   `-share-name %w` 指定主目录共享名称。当每个用户连接到其主目录时，系统会动态创建共享名称，其格式为 *windows_user_name* 。

   > 您也可以使用 `%u` 的变量 `-share-name` 选项这样将创建一个相对共享路径，该路径使用映射的 UNIX 用户名。

   `-path %u` 指定主目录的相对路径。当每个用户连接到其主目录时，系统会动态创建相对路径，其格式为 *mapped_unix_user_name* 。

   > 此选项的值也可以包含静态元素。例如： `eng/%u`。

   `-share-properties homedirectory\[,...\]` 指定该共享的共享属性。您必须指定 `homedirectory` 价值。您可以使用逗号分隔列表指定其他共享属性。

5. 使用验证共享是否具有所需的配置 `vserver cifs share show` 命令：
6. 添加主目录搜索路径： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` 指定已启用CIFS且要添加搜索路径的SVM。

   `-path path` 指定搜索路径的绝对目录路径。

7. 使用验证是否已成功添加搜索路径 `vserver cifs home-directory search-path show` 命令：
8. 如果UNIX用户不存在、请使用创建UNIX用户 `vserver services unix-user create` 命令：

   > 在映射 Windows 用户名之前，必须存在要将其映射到的 UNIX 用户名。

9. 使用以下命令创建Windows用户到UNIX用户的名称映射： `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   > 如果已存在将 Windows 用户映射到 UNIX 用户的名称映射，则无需执行映射步骤。

   Windows 用户名将映射到相应的 UNIX 用户名。当 Windows 用户连接到其主目录共享时，他们会使用与其 Windows 用户名对应的共享名称连接到动态创建的主目录，而无需知道该目录名与 UNIX 用户名对应。

10. 对于具有主目录的用户，请在指定用于包含主目录的 qtree 或卷中创建相应的目录。

例如、如果您创建的qtree的路径为 `/vol/vol1/users` 如果要创建其目录的用户的映射UNIX用户名是"`unixuser1`"、则应使用以下路径创建目录： `/vol/vol1/users/unixuser1`。

如果您创建了一个名为"`home/"的卷、则挂载于 `/home1`，则应使用以下路径创建目录：`/home1/unixuser1`。

11. 通过映射驱动器或使用 UNC 路径进行连接，验证用户是否可以成功连接到主共享。

    例如、如果用户mydomain\user1映射到UNIX用户unixuser1、并希望连接到在步骤10中创建的位于SVM VS1上的目录、则user1将使用UNC路径进行连接 `\\vs1\user1`。

示例

以下示例中的命令使用以下设置创建主目录配置：

- 共享名称为 %w
- 相对主目录路径为 %u
- 用于包含主目录的搜索路径、 `/home1`是配置了UNIX安全模式的卷。
- 此时将在 SVM vs1 上创建配置。

如果用户同时从 Windows 主机或 Windows 和 UNIX 主机访问其主目录，并且文件系统管理员使用基于 UNIX 的用户和组来控制对文件系统的访问，则可以使用此类主目录配置。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                                Replacement: unixuser1
```

相关信息

使用 %w 和 %d 变量创建主目录配置

其他主目录配置

其他主目录配置

您可以使用创建其他主目录配置 %w， %d，和 %u 变量、用于自定义主目录配置以满足您的需求。

您可以在共享名称和搜索路径中组合使用变量和静态字符串来创建多个主目录配置。下表提供了一些示例，用于说明如何创建不同的主目录配置：

路径创建时间 /vol1/user 包含主目录...	共享命令 ...
以创建共享路径 \\vs1\~win_username 将用户定向到 /vol1/user/win_username	vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory
以创建共享路径 \\vs1\win_username 将用户定向到 /vol1/user/domain/win_username	vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory
以创建共享路径 \\vs1\win_username 将用户定向到 /vol1/user/unix_username	vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory
以创建共享路径 \\vs1\unix_username 将用户定向到 /vol1/user/unix_username	vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory

用于管理搜索路径的命令

您可以使用特定的ONTAP命令来管理SMB主目录配置的搜索路径。例如，可以使用命令添加，删除和显示有关搜索路径的信息。此外，还有一个用于更改搜索路径顺序的命令。

如果您要 ...	使用此命令 ...
添加搜索路径	vserver cifs home-directory search-path add
显示搜索路径	vserver cifs home-directory search-path show
更改搜索路径顺序	vserver cifs home-directory search-path reorder

如果您要 ...	使用此命令 ...
删除搜索路径	`vserver cifs home-directory search-path remove`

有关详细信息，请参见每个命令的手册页。

显示有关 **SMB** 用户主目录路径的信息

您可以在 Storage Virtual Machine （SVM）上显示 SMB 用户的主目录路径，如果您配置了多个 CIFS 主目录路径，并且希望查看哪个路径包含用户的主目录，则可以使用此路径。

步骤

1. 使用显示主目录路径 `vserver cifs home-directory show-user` 命令：

   `vserver cifs home-directory show-user -vserver vs1 -username user1`

   ```
   Vserver      User                 Home Dir Path
   -----------  -------------------  -----------------------
   vs1          user1                /home/user1
   ```

相关信息

管理用户主目录的可访问性

管理用户主目录的可访问性

默认情况下，用户的主目录只能由该用户访问。对于共享的动态名称前面带有颚化符（ {tide} ）的共享，您可以启用或禁用 Windows 管理员或任何其他用户对用户主目录的访问（公有访问）。

开始之前

Storage Virtual Machine （SVM）上的主目录共享必须使用前面带有路径（ {tide} ）的动态共享名称进行配置。以下案例说明了共享命名要求：

主目录共享名称	连接到共享的命令示例
{tiLde} %d {tiLde} %w	`net use * \\IPaddress\~domain~user/u:credentials`
{tiLde} %w	`net use * \\IPaddress\~user/u:credentials`
{tide} abc {tide} %w	`net use * \\IPaddress\abc~user/u:credentials`

步骤

1. 执行相应的操作：

如果要启用或禁用对用户主目录的访问 ...	输入以下内容 ...
Windows 管理员	`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true|false}` 默认值为 `true`。
任何用户（公有访问）	a. 将权限级别设置为高级：+ `set -privilege advanced` b. 启用或禁用访问：`vserver cifs home-directory modify -vserver *vserver_name* -is-home-dirs -access-for-public-enabled {true

以下示例将启用对用户主目录的公共访问：+

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

相关信息

显示有关 SMB 用户主目录路径的信息

配置 SMB 客户端对 UNIX 符号链接的访问

如何使用 ONTAP 为 SMB 客户端提供对 UNIX 符号链接的访问权限

符号链接是在 UNIX 环境中创建的文件，其中包含对其他文件或目录的引用。如果客户端访问符号链接，则会将客户端重定向到该符号链接所引用的目标文件或目录。ONTAP 支持相对符号链接和绝对符号链接，包括 Widelink （与本地文件系统外部目标的绝对链接）。

通过 ONTAP ， SMB 客户端可以访问在 SVM 上配置的 UNIX 符号链接。此功能是可选的、您可以使用为每个共享配置此功能 `-symlink-properties` 的选项 `vserver cifs share create` 命令、并使用以下设置之一：

- 已启用，具有读 / 写访问权限
- 启用，具有只读访问权限
- 通过隐藏 SMB 客户端的符号链接来禁用
- 已禁用，但无法从 SMB 客户端访问符号链接

如果在共享上启用符号链接，则相对符号链接无需进一步配置即可正常工作。

如果在共享上启用符号链接，则绝对符号链接不会立即生效。您必须先在符号链接的 UNIX 路径与目标 SMB 路径之间创建映射。创建绝对符号链接映射时，您可以指定它是本地链接还是 *widelink* ； Widelink 可以是指向其他存储设备上的文件系统的链接，也可以是指向同一 ONTAP 系统上不同 SVM 中托管的文件系统的链接。创建 Widelink 时，它必须包含客户端要遵循的信息；也就是说，您可以为客户端创建重新解析点以发现目录接合点。

如果创建指向本地共享以外的文件或目录的绝对符号链接，但将位置设置为本地，则 ONTAP 将禁止访问目标。

> 如果客户端尝试删除本地符号链接（绝对或相对），则只会删除符号链接，而不会删除目标文件或目录。但是，如果客户端尝试删除 Widelink ，则可能会删除 Widelink 所引用的实际目标文件或目录。ONTAP 无法对此进行控制，因为客户端可以明确打开 SVM 外部的目标文件或目录并将其删除。

- * 重新解析点和 ONTAP 文件系统服务 *

  重新解析点 _ 是一个 NTFS 文件系统对象，可以选择将其与文件一起存储在卷上。重新解析点使 SMB 客户端能够在使用 NTFS 模式的卷时接收增强或扩展的文件系统服务。重新解析点由用于标识重新解析点类型的标准标记以及可供 SMB 客户端检索以供客户端进一步处理的重新解析点内容组成。在可用于扩展文件系统功能的对象类型中， ONTAP 使用重新解析点标记实现对 NTFS 符号链接和目录接合点的支持。无法理解重新解析点内容的 SMB 客户端只需忽略它，而不提供重新解析点可能启用的扩展文件系统服务。

- * 对符号链接的目录接合点和 ONTAP 支持 *

  目录接合点是指文件系统目录结构中的位置，可以是指存储文件的备用位置，可以是位于不同路径（符号链接）上，也可以是位于单独的存储设备（ Widelink ）上。ONTAP SMB 服务器将目录接合点作为重新解析点向 Windows 客户端公开，从而使具有功能的客户端能够在遍历目录接合点时从 ONTAP 获取重新解析点内容。因此，它们可以导航并连接到不同的路径或存储设备，就像它们属于同一文件系统一样。

- * 使用重新解析点选项启用 Widelink 支持 *

  。 `-is-use-junctions-as-reparse-points-enabled` 选项在ONTAP 9中默认处于启用状态。并非所有 SMB 客户端都支持 Widelink ，因此，启用信息的选项可按协议版本进行配置，从而允许管理员同时支持受支持和不受支持的 SMB 客户端。在ONTAP 9.2及更高版本中、必须启用选项 `-widelink-as-reparse-point-versions` 对于使用widelink访问共享的每个客户端协议、默认值为smb1。在早期版本中，仅报告使用默认 SMB1 访问的 Widelink ，而使用 SMB2 或 SMB3 的系统无法访问 Widelink 。

有关详细信息，请参见 Microsoft NTFS 文档。

"Microsoft 文档：重新解析点"

为 **SMB** 访问配置 **UNIX** 符号链接时的限制

在为 SMB 访问配置 UNIX 符号链接时，您需要了解某些限制。

limit	Description
45.	使用 FQDN 作为 CIFS 服务器名称时可以指定的 CIFS 服务器名称的最大长度。 您也可以将 CIFS 服务器名称指定为 NetBIOS 名称，此名称不得超过 15 个字符。
80	共享名称的最大长度。

limit	Description
256.	创建符号链接或修改现有符号链接的UNIX路径时、可以指定的UNIX路径的最大长度。UNIX路径必须以"`"开头/`" (slash) and end with a “/”。起始和结束斜线都计入 256 个字符的限制。
256.	创建符号链接或修改现有符号链接的CIFS路径时可以指定的CIFS路径的最大长度。CIFS路径必须以"`"开头/`" (slash) and end with a “/”。起始和结束斜线都计入 256 个字符的限制。

相关信息

为 SMB 共享创建符号链接映射

使用 CIFS 服务器选项在 ONTAP 中控制自动 DFS 公告

CIFS 服务器选项用于控制连接到共享时如何向 SMB 客户端公布 DFS 功能。由于 ONTAP 在客户端通过 SMB 访问符号链接时使用 DFS 转介，因此您应了解禁用或启用此选项会产生什么影响。

CIFS 服务器选项可确定 CIFS 服务器是否自动向 SMB 客户端公布支持 DFS 。默认情况下，此选项处于启用状态， CIFS 服务器始终向 SMB 客户端公布 DFS 功能（即使连接到已禁用符号链接访问的共享也是如此）。如果您希望 CIFS 服务器仅在客户端连接到启用了符号链接访问的共享时才向客户端公布 DFS 功能，则可以禁用此选项。

您应了解禁用此选项时会发生什么情况：

- 符号链接的共享配置保持不变。
- 如果共享参数设置为允许符号链接访问（读写访问或只读访问），则 CIFS 服务器会向连接到该共享的客户端公布 DFS 功能。

  客户端连接和符号链接访问将继续进行，不会中断。

- 如果共享参数设置为不允许符号链接访问（通过禁用访问或共享参数的值为空），则 CIFS 服务器不会向连接到该共享的客户端公布 DFS 功能。

  由于客户端已缓存 CIFS 服务器支持 DFS 的信息，并且不再公布此信息，因此，在禁用 CIFS 服务器选项后，连接到已禁用符号链接访问的共享的客户端可能无法访问这些共享。禁用此选项后，您可能需要重新启动连接到这些共享的客户端，从而清除缓存的信息。

这些更改不适用于 SMB 1.0 连接。

在 SMB 共享上配置 UNIX 符号链接支持

您可以通过在创建 SMB 共享时指定符号链接共享属性设置来配置 SMB 共享上的 UNIX 符号链接支持，也可以随时修改现有 SMB 共享来配置 UNIX 符号链接支持。默认情况下，UNIX 符号链接支持处于启用状态。您还可以在共享上禁用 UNIX 符号链接支持。

关于此任务

在为 SMB 共享配置 UNIX 符号链接支持时，您可以选择以下设置之一：

正在设置 ...	Description
`enable` (已弃用*)	指定为读写访问启用符号链接。
`read_only` (已弃用*)	指定为只读访问启用符号链接。此设置不适用于 Widelink 。Widelink 访问始终为读写访问。
`hide` (已弃用*)	指定阻止 SMB 客户端查看符号链接。
`no-strict-security`	指定客户端遵循共享边界以外的符号链接。
`symlinks`	指定在本地为读写访问启用符号链接。即使使用CIFS选项、也不会生成DFS公告 `is-advertise-dfs-enabled` 设置为 `true`。这是默认设置。
`symlinks-and-widelinks`	指定本地符号链接和 Widelink 进行读写访问。即使使用CIFS选项、也会为本地符号链接和widelink生成DFS公告 `is-advertise-dfs-enabled` 设置为 `false`。
`disable`	指定禁用符号链接和 Widelink 。即使使用CIFS选项、也不会生成DFS公告 `is-advertise-dfs-enabled` 设置为 `true`。
"" (空、未设置)	禁用共享上的符号链接。
- (未设置)	禁用共享上的符号链接。

- *enable* ， *hide* 和 *read-onter* 参数已弃用，可能会在未来版本的 ONTAP 中删除。

步骤

1. 配置或禁用符号链接支持：

如果 ...	输入 ...
新的 SMB 共享	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks

如果 ...	输入 ...
disable},…]+`	现有 SMB 共享
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. 验证SMB共享配置是否正确： `vserver cifs share show -vserver vserver_name -share -name share_name -instance`

示例

以下命令将创建名为`data1`的SMB共享、并将UNIX符号链接配置设置为 `enable`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                  Share Comment: -
                      Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                  Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相关信息

为 SMB 共享创建符号链接映射

您可以为 SMB 共享创建 UNIX 符号链接的映射。您可以创建相对符号链接，该链接引用与其父文件夹相对的文件或文件夹，也可以创建绝对符号链接，该链接使用绝对路径引用文件或文件夹。

关于此任务

如果使用 SMB 2.x ，则无法从 Mac OS X 客户端访问 Widelink当用户尝试从 Mac OS X 客户端使用 Widelink 连接到共享时，尝试将失败。但是，如果使用 SMB 1 ，则可以将 Widelink 与 Mac OS X 客户端结合使用。

步骤

1. 要为SMB共享创建符号链接映射、请执行以下操作： `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` 指定Storage Virtual Machine (SVM)名称。

   `-unix-path path` 指定UNIX路径。UNIX路径必须以斜杠开头 (`/`)、并且必须以斜杠结尾 (`/`）。

   `-share-name share_name` 指定要映射的SMB共享的名称。

   `-cifs-path path` 指定CIFS路径。CIFS路径必须以斜杠开头 (`/`)、并且必须以斜杠结尾 (`/`）。

   `-cifs-server server_name` 指定CIFS服务器名称。CIFS 服务器名称可以指定为 DNS 名称（例如 mynetwork.cifs.server.com ）， IP 地址或 NetBIOS 名称。NetBIOS名称可通过使用来确定 `vserver cifs show` 命令：如果未指定此可选参数，则默认值为本地 CIFS 服务器的 NetBIOS 名称。

   `-locality local|free|widelink}`指定是创建本地链接、自由链接还是宽符号链接。本地符号链接映射到本地 SMB 共享。可用符号链接可以映射到本地 SMB 服务器上的任意位置。宽符号链接映射到网络上的任何 SMB 共享。如果未指定此可选参数、则默认值为 `local`。

   `-home-directory true false}`指定目标共享是否为主目录。即使此参数是可选的、您也必须将此参数设置为 `true` 目标共享配置为主目录时。默认值为 `false`。

示例

以下命令会在名为 vs1 的 SVM 上创建符号链接映射。它具有UNIX路径 `/src/``SMB共享名称`SOURCE`、即CIFS路径 `/mycompany/source/`和CIFS服务器IP地址123.123.123.123.123，并且它是一个widelink。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

相关信息

在 SMB 共享上配置 UNIX 符号链接支持

用于管理符号链接映射的命令

您可以使用特定的 ONTAP 命令来管理符号链接映射。

如果您要 ...	使用此命令 ...
创建符号链接映射	`vserver cifs symlink create`
显示有关符号链接映射的信息	`vserver cifs symlink show`
修改符号链接映射	`vserver cifs symlink modify`
删除符号链接映射	`vserver cifs symlink delete`

有关详细信息，请参见每个命令的手册页。

使用 **BranchCache** 在分支机构缓存 **SMB** 共享内容

使用 **BranchCache** 在分支机构概述中缓存 **SMB** 共享内容

BranchCache 是由 Microsoft 开发的，用于在发出请求的客户端本地计算机上缓存内容。ONTAP 实施 BranchCache 可以降低广域网（Wide Area Network， WAN）的利用率，如果分支机构的用户使用 SMB 访问 Storage Virtual Machine （SVM）上存储的内容，则还可以缩短访问响应时间。

如果您配置 BranchCache，则 Windows BranchCache 客户端首先会从 SVM 中检索内容，然后在分支机构的计算机上缓存该内容。如果分支机构中另一个启用了 BranchCache 的客户端请求相同的内容，则 SVM 会首先对发出请求的用户进行身份验证和授权。然后， SVM 将确定缓存的内容是否仍为最新内容，如果是最新内容，则会发送有关缓存内容的客户端元数据。然后，客户端使用元数据直接从基于本地的缓存中检索内容。

相关信息

使用脱机文件允许缓存文件以供脱机使用

要求和准则

BranchCache 版本支持

您应了解 ONTAP 支持哪些 BranchCache 版本。

ONTAP 支持 BranchCache 1 和增强型 BranchCache 2：

- 在 SMB 服务器上为 Storage Virtual Machine （SVM）配置 BranchCache 时，可以启用 BranchCache 1， BranchCache 2 或所有版本。

  默认情况下，所有版本均处于启用状态。

- 如果仅启用 BranchCache 2，则远程办公室的 Windows 客户端计算机必须支持 BranchCache 2。

  只有 SMB 3.0 或更高版本的客户端支持 BranchCache 2。

有关 BranchCache 版本的详细信息，请参见 Microsoft TechNet 库。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

网络协议支持要求

您必须了解实施 ONTAP BranchCache 的网络协议要求。

您可以使用 SMB 2.1 或更高版本在 IPv4 和 IPv6 网络上实施 ONTAP BranchCache 功能。

所有参与 BranchCache 实施的 CIFS 服务器和分支机构计算机都必须启用 SMB 2.1 或更高版本的协议。SMB 2.1 具有允许客户端参与 BranchCache 环境的协议扩展。这是提供 BranchCache 支持的最低 SMB 协议版本。SMB 2.1 支持 BranchCache 版本 1 。

如果要使用 BranchCache 版本 2 ，则 SMB 3.0 是支持的最低版本。所有参与 BranchCache 2 实施的 CIFS 服务器和分支机构计算机都必须启用 SMB 3.0 或更高版本。

如果您的远程办公室中的某些客户端仅支持 SMB 2.1 ，而某些客户端支持 SMB 3.0 ，则可以在 CIFS 服务器上实施 BranchCache 配置，该配置可通过 BranchCache 1 和 BranchCache 2 提供缓存支持。

> 尽管 Microsoft BranchCache 功能支持使用 HTTP/HTTPS 和 SMB 协议作为文件访问协议，但 ONTAP BranchCache 仅支持使用 SMB 。

ONTAP 和 Windows 主机版本要求

在配置 BranchCache 之前， ONTAP 和分支机构 Windows 主机必须满足特定版本要求。

在配置 BranchCache 之前，您必须确保集群和相关分支机构客户端上的 ONTAP 版本支持 SMB 2.1 或更高版本并支持 BranchCache 功能。如果配置托管缓存模式，则还必须确保为缓存服务器使用受支持的主机。

以下 ONTAP 版本和 Windows 主机支持 BranchCache 1 ：

- 内容服务器：采用 ONTAP 的 Storage Virtual Machine （ SVM ）
- 缓存服务器： Windows Server 2008 R2 或 Windows Server 2012 或更高版本
- 对等或客户端： Windows 7 Enterprise ， Windows 7 Ultimate ， Windows 8 ， Windows Server 2008 R2 或 Windows Server 2012 或更高版本

以下ONTAP版本和Windows主机支持网络缓存2：

- 内容服务器：带有 ONTAP 的 SVM
- 缓存服务器： Windows Server 2012 或更高版本
- 对等方或客户端： Windows 8 或 Windows Server 2012 或更高版本

ONTAP 使 BranchCache 哈希失效的原因

在规划 BranchCache 配置时，了解 ONTAP 使哈希失效的原因可能会很有帮助。它可以帮助您确定应配置的操作模式，并帮助您选择要启用 BranchCache 的共享。

ONTAP 必须管理 BranchCache 哈希，以确保哈希有效。如果哈希无效，则 ONTAP 会使哈希失效，并在下次请求该内容时计算新的哈希，前提是 BranchCache 仍处于启用状态。

ONTAP 会使哈希失效，原因如下：

- 服务器密钥已修改。

  如果修改了服务器密钥， ONTAP 将使哈希存储中的所有哈希失效。

- 由于已达到 BranchCache 哈希存储的最大大小，因此会从缓存中刷新哈希。

  这是一个可调参数，可以根据您的业务需求进行修改。

- 通过 SMB 或 NFS 访问修改文件。
- 使用还原已计算哈希的文件 `snap restore` 命令：
- 包含已启用了anchCache的SMB共享的卷将使用还原 `snap restore` 命令：

选择哈希存储位置的准则

在配置 BranchCache 时，您可以选择哈希的存储位置以及哈希存储的大小。了解选择哈希存储位置和大小的准则有助于您在启用了 CIFS 的 SVM 上规划 BranchCache 配置。

- 您应在允许使用 atime 更新的卷上找到哈希存储。

  哈希文件的访问时间用于将经常访问的文件保留在哈希存储中。如果禁用了 atime 更新，则创建时间将用于此目的。最好使用 atime 来跟踪常用的文件。

- 不能将哈希存储在只读文件系统上，例如 SnapMirror 目标和 SnapLock 卷。
- 如果达到哈希存储的最大大小，则会刷新旧哈希，以便为新哈希留出空间。

  您可以增加哈希存储的最大大小，以减少从缓存中刷新的哈希数量。

- 如果存储哈希的卷不可用或已满，或者存在具有集群内通信的问题描述，而 BranchCache 服务无法检索哈希信息，则 BranchCache 服务不可用。

  此卷可能不可用，因为它已脱机或存储管理员为哈希存储指定了一个新位置。

  这不会影响文件访问的发生原因问题。如果阻止访问哈希存储， ONTAP 会向客户端返回 Microsoft 定义的错误，从而导致客户端使用正常的 SMB 读取请求请求请求文件。

相关信息

在SMB服务器上配置anchCache

修改 BranchCache 配置

BranchCache 建议

在配置 BranchCache 之前，在确定要启用 BranchCache 缓存的 SMB 共享时，您应记住一些建议。

在确定要使用的操作模式以及要在哪些 SMB 共享上启用 BranchCache 时，应牢记以下建议：

- 如果要远程缓存的数据频繁更改， BranchCache 的优势将会降低。
- BranchCache 服务对于包含多个远程办公室客户端重复使用的文件内容或单个远程用户重复访问的文件内容的共享非常有用。
- 请考虑为只读内容启用缓存，例如 Snapshot 副本和 SnapMirror 目标中的数据。

配置 **BranchCache**

配置 **BranchCache** 概述

您可以使用 ONTAP 命令在 SMB 服务器上配置 BranchCache 。要实施 BranchCache ，还必须在要缓存内容的分支机构配置客户端以及托管缓存服务器（可选）。

如果您将 BranchCache 配置为在共享基础上启用缓存，则必须在要提供 BranchCache 缓存服务的 SMB 共享上启用 BranchCache 。

配置 **BranchCache** 的要求

满足某些前提条件后，您可以设置 BranchCache 。

在 SVM 的 CIFS 服务器上配置 BranchCache 之前，必须满足以下要求：

- ONTAP 必须安装在集群中的所有节点上。
- 必须获得CIFS的许可、并且必须配置SMB服务器。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。
- 必须配置 IPv4 或 IPv6 网络连接。
- 对于 BranchCache 1 ，必须启用 SMB 2.1 或更高版本。
- 对于 BranchCache 2 ，必须启用 SMB 3.0 ，并且远程 Windows 客户端必须支持 BranchCache 2 。

在**SMB**服务器上配置**anchCache**

您可以将 BranchCache 配置为按共享提供 BranchCache 服务。或者，您也可以将 BranchCache 配置为在所有 SMB 共享上自动启用缓存。

关于此任务

您可以在 SVM 上配置 BranchCache 。

- 如果要为 CIFS 服务器上所有 SMB 共享中的所有内容提供缓存服务，则可以创建纯共享 BranchCache 配置。
- 如果要为 CIFS 服务器上选定 SMB 共享中的内容提供缓存服务，则可以创建每个共享 BranchCache 配置。

配置 BranchCache 时，必须指定以下参数：

所需参数	Description
_SVM 名称 _	BranchCache 按 SVM 进行配置。您必须指定要在哪个启用了 CIFS 的 SVM 上配置 BranchCache 服务。
哈希存储的路径 _	BranchCache 哈希存储在 SVM 卷上的常规文件中。您必须指定希望 ONTAP 存储哈希数据的现有目录的路径。 BranchCache 哈希路径必须为可读写路径。不允许使用只读路径，例如 Snapshot 目录。您可以将哈希数据存储在包含其他数据的卷中，也可以创建单独的卷来存储哈希数据。 如果 SVM 是 SVM 灾难恢复源，则哈希路径不能位于根卷上。这是因为根卷不会复制到灾难恢复目标。 哈希路径可以包含空格和任何有效的文件名字符。

您也可以指定以下参数：

可选参数	Description
_ 支持的版本 _	ONTAP 支持 BranchCache 1 和 2 。您可以启用版本 1 ，版本 2 或这两个版本。默认情况下会同时启用这两个版本。
哈希存储的最大大小 _	您可以指定用于哈希数据存储的大小。如果哈希数据超过此值， ONTAP 将删除旧哈希，以便为新哈希腾出空间。哈希存储的默认大小为 1 GB 。如果不以过于激进的方式丢弃哈希， BranchCache 的性能将会更高效。如果由于哈希存储已满而确定经常丢弃哈希，则可以通过修改 BranchCache 配置来增加哈希存储大小。
服务器密钥 _	您可以指定 BranchCache 服务用来防止客户端模拟 BranchCache 服务器的服务器密钥。如果未指定服务器密钥，则在创建 BranchCache 配置时会随机生成一个密钥。您可以将服务器密钥设置为特定值，以便在多个服务器为相同文件提供 BranchCache 数据时，客户端可以使用使用使用同一服务器密钥的任何服务器的哈希。如果服务器密钥包含任何空格，则必须将服务器密钥用引号引起来。
操作模式 _	默认情况下，每个共享启用 BranchCache 。 • 要创建在每个共享上启用了anchCache的anchCache配置、您可以不指定此可选参数、也可以指定 `per-share`。 • 要在所有共享上自动启用anchCache、必须将操作模式设置为 `all-shares`。

步骤

1. 根据需要启用 SMB 2.1 和 3.0 ：
   a. 将权限级别设置为高级： `set -privilege advanced`
   b. 检查已配置的SVM SMB设置以确定是否已启用所有所需的SMB版本： `vserver cifs options show -vserver vserver_name`
   c. 如有必要、启用SMB 2.1： `vserver cifs options modify -vserver vserver_name -smb2 -enabled true`

      命令将同时启用 SMB 2.0 和 SMB 2.1 。
   d. 如有必要、启用SMB 3.0： `vserver cifs options modify -vserver vserver_name -smb3 -enabled true`
   e. 返回到管理权限级别： `set -privilege admin`
2. 配置anchCache： `vserver cifs branchcache create -vserver vserver_name -hash-store -path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   指定的哈希存储路径必须存在，并且必须驻留在 SVM 管理的卷上。此路径还必须位于可读写卷上。如果路径为只读或不存在，则此命令将失败。

   如果要对其他 SVM BranchCache 配置使用相同的服务器密钥，请记录为服务器密钥输入的值。显示有关 BranchCache 配置的信息时，不会显示服务器密钥。
3. 验证是否正确配置了anchCache： `vserver cifs branchcache show -vserver vserver_name`

示例

以下命令验证是否已启用 SMB 2.1 和 3.0 ，并将 BranchCache 配置为在 SVM vs1 上的所有 SMB 共享上自动启用缓存：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

以下命令验证是否已启用 SMB 2.1 和 3.0 ，将 BranchCache 配置为在 SVM vs1 上启用每个共享的缓存，并验证 BranchCache 配置：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

相关信息

要求和准则： BranchCache 版本支持

从何处查找有关在远程办公室配置 BranchCache 的信息

创建启用了 BranchCache 的 SMB 共享

在现有 SMB 共享上启用 BranchCache

修改 BranchCache 配置

禁用 SMB 共享上的 BranchCache 概述

删除 SVM 上的 BranchCache 配置

从何处查找有关在远程办公室配置 **BranchCache** 的信息

在SMB服务器上配置了anchCache后、您必须在客户端计算机上安装和配置了anchCache、也可以在远程办公室的缓存服务器上安装和配置它。Microsoft 提供了有关在远程办公室配置 BranchCache 的说明。

有关配置分支机构客户端以及缓存服务器以使用 BranchCache 的说明，请参见 Microsoft BranchCache 网站。

"Microsoft BranchCache 文档：新增功能"

配置已启用 **BranchCache** 的 **SMB** 共享

配置已启用 **BranchCache** 的 **SMB** 共享概述

在 SMB 服务器和分支机构上配置 BranchCache 后，您可以在包含要允许分支机构客户端缓存的内容的 SMB 共享上启用 BranchCache 。

可以在 SMB 服务器上的所有 SMB 共享上启用 BranchCache 缓存，也可以在共享基础上启用 BranchCache 缓存。

- 如果在逐个共享的基础上启用 BranchCache ，则可以在创建共享时或通过修改现有共享来启用 BranchCache 。

  如果在现有 SMB 共享上启用缓存，则一旦在该共享上启用 BranchCache ， ONTAP 就会开始计算哈希并向请求内容的客户端发送元数据。

- 如果随后在某个共享上启用了 BranchCache ，则与某个共享具有现有 SMB 连接的任何客户端都不会获得 BranchCache 支持。

  在设置 SMB 会话时， ONTAP 会公布 BranchCache 对共享的支持。启用 BranchCache 后，已建立会话的客户端需要断开连接并重新连接，才能使用此共享的缓存内容。

> 如果随后禁用 SMB 共享上的 BranchCache ，则 ONTAP 将停止向请求客户端发送元数据。需要数据的客户端直接从内容服务器（ SMB 服务器）检索数据。

创建启用了 **BranchCache** 的 **SMB** 共享

通过设置创建共享时、您可以在SMB共享上启用anchCache `branchcache` 共享属性。

关于此任务

- 如果在 SMB 共享上启用了 BranchCache ，则该共享必须将脱机文件配置设置为手动缓存。

  这是创建共享时的默认设置。

- 您还可以在创建启用了 BranchCache 的共享时指定其他可选共享参数。
- 您可以设置 `branchcache` 属性、即使未在Storage Virtual Machine (SVM)上配置和启用了anchCache也是如此。

  但是，如果您希望共享提供缓存的内容，则必须在 SVM 上配置并启用 BranchCache 。

- 因为使用时不会应用于共享的默认共享属性 `-share-properties` 参数、则除了之外、您还必须指定要应用于共享的所有其他共享属性 `branchcache` 共享属性。
- 有关详细信息、请参见的手册页 `vserver cifs share create` 命令：

步骤

1. 创建启用了anchCache的SMB共享：+
   `vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`
2. 使用验证是否已在SMB共享上设置了anchCache共享属性 `vserver cifs share show` 命令：

示例

以下命令将使用路径创建一个名为`data`的已启用了anchCache的SMB共享 `/data` 在SVM VS1上。默认情况下、脱机文件设置设置为 `manual`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相关信息

在单个 SMB 共享上禁用 BranchCache

在现有 **SMB** 共享上启用 **BranchCache**

您可以通过添加在现有SMB共享上启用anchCache `branchcache` 共享属性到现有共享属性列表。

关于此任务

- 如果在 SMB 共享上启用了 BranchCache ，则该共享必须将脱机文件配置设置为手动缓存。

  如果现有共享的脱机文件设置未设置为手动缓存，则必须通过修改共享对其进行配置。

- 您可以设置 `branchcache` 属性、即使未在Storage Virtual Machine (SVM)上配置和启用了anchCache也是如此。

但是，如果您希望共享提供缓存的内容，则必须在 SVM 上配置并启用 BranchCache 。

- 添加时 `branchcache` 共享属性保留到共享、现有共享设置和共享属性。

  BranchCache 共享属性将添加到现有共享属性列表中。有关使用的详细信息、请参见 `vserver cifs share properties add` 命令、请参见手册页。

步骤

1. 如有必要，请配置脱机文件共享设置以进行手动缓存：
   a. 使用确定脱机文件共享设置 `vserver cifs share show` 命令：
   b. 如果脱机文件共享设置未设置为手动、请将其更改为所需值： `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. 在现有SMB共享上启用anchCache： `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. 验证是否已在SMB共享上设置了anchCache共享属性： `vserver cifs share show -vserver vserver_name -share-name share_name`

示例

以下命令将在名为`data2`的现有SMB共享上使用路径启用anchCache `/data2` 在SVM VS1上：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               showsnapshot
                               changenotify
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相关信息

在现有 SMB 共享上添加或删除共享属性

在单个 SMB 共享上禁用 BranchCache

管理和监控 **BranchCache** 配置

修改 **BranchCache** 配置

您可以修改 SVM 上 BranchCache 服务的配置，包括更改哈希存储目录路径，哈希存储最大目录大小，操作模式以及支持的 BranchCache 版本。您还可以增加包含哈希存储的卷的大小。

步骤

1. 执行相应的操作：

如果您要 ...	输入以下内容 ...
修改哈希存储目录大小	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
增加包含哈希存储的卷的大小	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` 如果包含哈希存储的卷已满、您可以增加卷的大小。您可以将新卷大小指定为一个数字，后跟一个单位名称。 了解更多信息 "管理FlexVol 卷"	修改哈希存储目录路径

如果您要 ...	输入以下内容 ...
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` 如果 SVM 是 SVM 灾难恢复源，则哈希路径不能位于根卷上。这是因为根卷不会复制到灾难恢复目标。  BranchCache 哈希路径可以包含空格和任何有效的文件名字符。  如果修改哈希路径、 `-flush-hashes` 是一个必需参数、用于指定是否希望ONTAP从原始哈希存储位置转储哈希。您可以为设置以下值 `-flush-hashes` 参数：  如果指定 **`true`**，**ONTAP**将删除原始位置的哈希，并在启用了**anchCache**的客户端发出新请求时在新位置创建新哈希。 如果指定 `false`，哈希不会被转储。 + 在这种情况下，您可以选择稍后通过将哈希存储路径更改回原始位置来重复使用现有哈希。
更改运行模式	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` 修改操作模式时、应注意以下事项： 设置**SMB**会话后、**ONTAP** 会公布**BranchCache**对共享的支持。 启用 BranchCache 后，已建立会话的客户端需要断开连接并重新连接，才能使用此共享的缓存内容。
更改 BranchCache 版本支持	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. 使用验证配置更改 `vserver cifs branchcache show` 命令：

显示有关 **BranchCache** 配置的信息

您可以显示 Storage Virtual Machine （SVM）上的 BranchCache 配置信息，这些信息可在验证配置或在修改配置之前确定当前设置时使用。

步骤

1. 执行以下操作之一：

要显示的内容	输入此命令 ...
有关所有 SVM 上 BranchCache 配置的摘要信息	`vserver cifs branchcache show`

要显示的内容	输入此命令 ...
有关特定 SVM 上配置的详细信息	`vserver cifs branchcache show -vserver` *`vserver_name`*

示例

以下示例显示了有关 SVM vs1 上 BranchCache 配置的信息：

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                   Vserver: vs1
            Supported BranchCache Versions: enable_all
                        Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

更改 **BranchCache** 服务器密钥

您可以通过修改 Storage Virtual Machine （SVM）上的 BranchCache 配置并指定其他服务器密钥来更改 BranchCache 服务器密钥。

关于此任务

您可以将服务器密钥设置为特定值，以便在多个服务器为相同文件提供 BranchCache 数据时，客户端可以使用使用使用同一服务器密钥的任何服务器的哈希。

更改服务器密钥时，还必须刷新哈希缓存。刷新哈希后， ONTAP 会在启用了 BranchCache 的客户端发出新请求时创建新哈希。

步骤

1. 使用以下命令更改服务器密钥： `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   配置新服务器密钥时、还必须指定 `-flush-hashes` 并将值设置为 `true`。

2. 使用验证anchCache配置是否正确 `vserver cifs branchcache show` 命令：

示例

以下示例将设置一个包含空格的新服务器密钥，并刷新 SVM vs1 上的哈希缓存：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

相关信息

ONTAP 使 BranchCache 哈希失效的原因

预先计算指定路径上的 **BranchCache** 哈希

您可以将 BranchCache 服务配置为为为单个文件，目录或目录结构中的所有文件预先计算哈希。如果您希望在非高峰时段对启用了 BranchCache 的共享中的数据计算哈希，这将非常有用。

关于此任务

如果要在显示哈希统计信息之前收集数据样本、则必须使用 `statistics start` 和可选 `statistics stop` 命令

- 您必须指定要预先计算哈希的 Storage Virtual Machine （ SVM ）和路径。
- 您还必须指定是否要以递归方式计算哈希。
- 如果要以递归方式计算哈希， BranchCache 服务将遍历指定路径下的整个目录树，并为每个符合条件的对象计算哈希。

步骤

1. 根据需要预计算哈希：

如果要预先计算哈希 ...	输入命令 ...
单个文件或目录	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
在目录结构中的所有文件上以递归方式执行	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. 使用验证是否正在计算哈希 `statistics` 命令：
   a. 显示的统计信息 `hashd` 所需SVM实例上的对象： `statistics show -object hashd -instance`

```
vserver_name
```

b. 重复执行此命令，以验证创建的哈希数量是否正在增加。

示例

以下示例将在路径上创建哈希 `/data` 和SVM VS1上的所有包含文件和子目录：

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

相关信息

"性能监控设置"

从 SVM BranchCache 哈希存储刷新哈希

您可以刷新 Storage Virtual Machine （ SVM ）上 BranchCache 哈希存储中的所有缓存哈希。如果您更改了分支机构 BranchCache 配置，则此功能非常有用。例如，如果您最近将缓存模式从分布式缓存重新配置为托管缓存模式，则需要刷新哈希存储。

关于此任务

刷新哈希后， ONTAP 会在启用了 BranchCache 的客户端发出新请求时创建新哈希。

步骤

1. 从"anchCache哈希存储"转储哈希： `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   `vserver cifs branchcache hash-flush -vserver vs1`

显示 BranchCache 统计信息

您可以显示 BranchCache 统计信息，以便确定缓存的执行情况，确定您的配置是否正在向客户端提供缓存内容，以及确定是否删除了哈希文件，以便为最新的哈希数据腾出空间。

关于此任务

。 `hashd` 统计信息对象包含计数器、这些计数器可提供有关anchCache哈希的统计信息。。 `cifs` 统计信息对象包含计数器、这些计数器提供有关与anchCache相关的活动的统计信息。您可以在高级权限级别收集和显示有关这些对象的信息。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. 使用显示与anchCache相关的计数器 `statistics catalog counter show` 命令：

   有关统计信息计数器的详细信息，请参见此命令的手册页。

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
       Counter                     Description
       ---------------------------
   ----------------------------------------------
       branchcache_hash_created    Number of times a request to generate
                                   BranchCache hash for a file succeeded.
   ```

```
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
---------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
```

```
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
   ....Output truncated....
```

3. 使用收集与anchCache相关的统计信息 `statistics start` 和 `statistics stop` 命令

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. 使用显示收集的anchCache统计信息 `statistics show` 命令：

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. 返回到管理权限级别： `set -privilege admin`

```
cluster1::*> set -privilege admin
```

相关信息

显示统计信息

"性能监控设置"

支持 **BranchCache** 组策略对象

ONTAP BranchCache 支持 BranchCache 组策略对象（GPO），从而可以集中管理某些

BranchCache 配置参数。BranchCache 使用两个 GPO： BranchCache 的哈希发布 GPO 和 BranchCache 的哈希版本支持 GPO 。

- BranchCache GPO 的 * 哈希发布 *

  针对anchCache的哈希发布GPO对应于 `-operating-mode` 参数。发生 GPO 更新时，此值将应用于组策略所适用的组织单位（ OU ）中包含的 Storage Virtual Machine （ SVM ）对象。

- BranchCache GPO 的 * 哈希版本支持 *

  "对anchCache的哈希版本支持" GPO对应于 `-versions` 参数。发生 GPO 更新时，此值将应用于组策略所适用的组织单位中包含的 SVM 对象。

相关信息

将组策略对象应用于 CIFS 服务器

显示有关 **BranchCache** 组策略对象的信息

您可以显示有关 CIFS 服务器的组策略对象（ GPO ）配置的信息，以确定是否为 CIFS 服务器所属的域定义了 BranchCache GPO ，如果是，则确定允许的设置是什么。您还可以确定 BranchCache GPO 设置是否应用于 CIFS 服务器。

关于此任务

即使在 CIFS 服务器所属的域中定义了 GPO 设置，但它不一定会应用于包含启用了 CIFS 的 Storage Virtual Machine （ SVM ）的组织单位（ OU ）。应用的 GPO 设置是应用于启用了 CIFS 的 SVM 的所有已定义 GPO 的子集。通过 GPO 应用的 BranchCache 设置会覆盖通过 CLI 应用的设置。

步骤

1. 使用显示为Active Directory域定义的"anchCache GPO设置" `vserver cifs group-policy show-defined` 命令：

   此示例不会显示命令的所有可用输出字段。输出被截断。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. 使用显示应用于CIFS服务器的anchCache GPO设置 `vserver cifs group-policy show-applied` 命令：``

   此示例不会显示命令的所有可用输出字段。输出被截断。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

相关信息

在 CIFS 服务器上启用或禁用 GPO 支持

在 SMB 共享上禁用 BranchCache

禁用 SMB 共享上的 BranchCache 概述

如果您不希望在某些 SMB 共享上提供 BranchCache 缓存服务，但稍后可能希望在这些共享上提供缓存服务，则可以在共享基础上禁用 BranchCache 。如果已将 BranchCache 配置为在所有共享上提供缓存，但您希望暂时禁用所有缓存服务，则可以修改 BranchCache 配置以停止对所有共享的自动缓存。

如果 SMB 共享上的 BranchCache 在首次启用后随后被禁用，则 ONTAP 将停止向请求客户端发送元数据。需要数据的客户端直接从内容服务器（ Storage Virtual Machine （ SVM ）上的 CIFS 服务器）检索数据。

相关信息

在单个 **SMB** 共享上禁用 **BranchCache**

如果您不希望在先前提供缓存内容的某些共享上提供缓存服务，则可以在现有 SMB 共享上禁用 BranchCache 。

步骤

1. 输入以下命令： `vserver cifs share properties remove -vserver vserver_name -share -name share_name -share-properties branchcache`

   此时将删除 BranchCache 共享属性。其他应用的共享属性仍有效。

示例

以下命令会在名为 `data2` 的现有 SMB 共享上禁用 BranchCache ：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

停止对所有 **SMB** 共享的自动缓存

如果 BranchCache 配置自动对每个 Storage Virtual Machine （ SVM ）上的所有 SMB 共享启用缓存，则可以修改 BranchCache 配置以停止自动缓存所有 SMB 共享的内容。

关于此任务

要停止所有 SMB 共享上的自动缓存，请将 BranchCache 操作模式更改为每共享缓存。

步骤

1. 将anchCache配置为在所有SMB共享上停止自动缓存： `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. 验证是否正确配置了anchCache： `vserver cifs branchcache show -vserver vserver_name`

示例

以下命令将更改 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的 BranchCache 配置，以停止对所有 SMB 共享的自动缓存：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

在 **SVM** 上禁用或启用 **BranchCache**

在 **CIFS** 服务器上禁用或重新启用 **BranchCache** 时会发生什么情况

如果先前已配置 BranchCache ，但不希望分支机构客户端使用缓存的内容，则可以在 CIFS 服务器上禁用缓存。您必须了解禁用 BranchCache 时会发生什么情况。

禁用 BranchCache 后， ONTAP 将不再计算哈希或将元数据发送到发出请求的客户端。但是，文件访问不会中断。此后，当启用了 BranchCache 的客户端请求要访问的内容的元数据信息时， ONTAP 会做出响应，并显示 Microsoft 定义的错误，这会导致客户端发送第二个请求，请求实际内容。在响应内容请求时， CIFS 服务器会发送存储在 Storage Virtual Machine （ SVM ）上的实际内容。

在 CIFS 服务器上禁用 BranchCache 后， SMB 共享不会公布 BranchCache 功能。要访问新 SMB 连接上的数据，客户端会发出正常的读取 SMB 请求。

您可以随时在 CIFS 服务器上重新启用 BranchCache 。

- 由于禁用 BranchCache 时不会删除哈希存储，因此，如果请求的哈希仍然有效，则在重新启用

BranchCache 后， ONTAP 可以使用存储的哈希响应哈希请求。

- 如果随后重新启用了 BranchCache ，则在禁用 BranchCache 期间与已启用 BranchCache 的共享建立 SMB 连接的任何客户端都不会获得 BranchCache 支持。

  这是因为在设置 SMB 会话时， ONTAP 会公布对共享的 BranchCache 支持。在禁用 BranchCache 期间与已启用 BranchCache 的共享建立会话的客户端需要断开连接并重新连接，才能使用此共享的缓存内容。

> 如果在 CIFS 服务器上禁用 BranchCache 后不想保存哈希存储，则可以手动将其删除。如果重新启用 BranchCache ，则必须确保哈希存储目录存在。重新启用 BranchCache 后，启用了 BranchCache 的共享会公布 BranchCache 功能。启用了 BranchCache 的客户端发出新请求时，ONTAP 会创建新哈希。

禁用或启用 **BranchCache**

您可以通过将anchCache操作模式更改为来在Storage Virtual Machine (SVM)上禁用anchCache `disabled`。您可以随时通过将运行模式更改为按共享提供 BranchCache 服务或自动为所有共享启用 BranchCache 。

步骤

1. 运行相应的命令：

如果您要 ...	然后输入以下内容 ...
禁用 BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
为每个共享启用 BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
为所有共享启用 BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. 验证是否已使用所需设置配置了anchCache运行模式： `vserver cifs branchcache show -vserver vserver_name`

示例

以下示例将在 SVM vs1 上禁用 BranchCache ：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

删除 **SVM** 上的 **BranchCache** 配置

删除 **BranchCache** 配置时会发生什么情况

如果先前已配置 BranchCache ，但不希望 Storage Virtual Machine （ SVM ）继续提供缓存的内容，则可以删除 CIFS 服务器上的 BranchCache 配置。您必须了解删除配置时会发生什么情况。

删除配置时， ONTAP 会从集群中删除该 SVM 的配置信息并停止 BranchCache 服务。您可以选择 ONTAP 是否应删除 SVM 上的哈希存储。

删除 BranchCache 配置不会中断已启用 BranchCache 的客户端的访问。此后，当启用了 BranchCache 的客户端请求有关已缓存内容的现有 SMB 连接的元数据信息时， ONTAP 将做出响应并显示 Microsoft 定义的错误，这将导致客户端发送第二个请求，请求实际内容。在响应内容请求时， CIFS 服务器会发送存储在 SVM 上的实际内容

删除 BranchCache 配置后， SMB 共享不会公布 BranchCache 功能。要访问以前未使用新 SMB 连接缓存的内容，客户端会发出正常的读取 SMB 请求。

删除 **BranchCache** 配置

用于删除 Storage Virtual Machine （ SVM ）上的 BranchCache 服务的命令会有所不同，具体取决于您是要删除还是保留现有哈希。

步骤

1. 运行相应的命令：

如果您要 ...	然后输入以下内容 ...
删除 BranchCache 配置并删除现有哈希	`vserver cifs branchcache delete -vserver` *`vserver_name`* `-flush-hashes true`

如果您要 ...	然后输入以下内容 ...
删除 BranchCache 配置，但保留现有哈希	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

示例

以下示例将删除 SVM vs1 上的 BranchCache 配置并删除所有现有哈希：

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

还原时 **BranchCache** 会发生什么情况

请务必了解将 ONTAP 还原到不支持 BranchCache 的版本时会发生什么情况。

- 还原到不支持 BranchCache 的 ONTAP 版本时， SMB 共享不会向已启用 BranchCache 的客户端公布 BranchCache 功能；因此，客户端不会请求哈希信息。

  而是使用正常的 SMB 读取请求来请求实际内容。在对内容请求的响应中、SMB服务器会发送Storage Virtual Machine (SVM)上存储的实际内容。

- 当托管哈希存储的节点还原到不支持 BranchCache 的版本时，存储管理员需要使用在还原期间输出的命令手动还原 BranchCache 配置。

  此命令将删除 BranchCache 配置和哈希。

  还原完成后，存储管理员可以根据需要手动删除包含哈希存储的目录。

相关信息

删除 SVM 上的 BranchCache 配置

提高 **Microsoft** 远程复制性能

改进 **Microsoft** 远程复制性能概述

Microsoft 卸载数据传输（ Offloaded Data Transfer ， ODX ）也称为 *copy ofload* ，可在兼容存储设备内部或之间直接传输数据，而无需通过主机计算机传输数据。

ONTAP支持对SMB和SAN协议使用ODX。源可以是 CIFS 服务器或 LUN ，目标可以是 CIFS 服务器或 LUN 。

在非 ODX 文件传输中，数据将从源读取，并通过网络传输到客户端计算机。客户端计算机通过网络将数据传输回目标。总之，客户端计算机从源读取数据并将其写入目标。使用 ODX 文件传输时，数据会直接从源复制到目标。

由于 ODX 卸载副本是直接在源存储和目标存储之间执行的，因此具有显著的性能优势。实现的性能优势包括：源和目标之间的复制时间更短，客户端上的资源利用率（ CPU ，内存）更低，网络 I/O 带宽利用率更低。

对于 SMB 环境，只有当客户端和存储服务器都支持 SMB 3.0 和 ODX 功能时，此功能才可用。对于 SAN 环境，只有当客户端和存储服务器都支持 ODX 功能时，此功能才可用。支持 ODX 且启用了 ODX 的客户端计算机在移动或复制文件时会自动透明地使用卸载文件传输。无论您是通过 Windows 资源管理器拖放文件还是使用命令行文件复制命令，还是客户端应用程序启动文件复制请求，系统都会使用 ODX 。

相关信息

通过为 SMB 自动节点转介提供自动位置来缩短客户端响应时间

"Microsoft Hyper-V 和 SQL Server 的 SMB 配置"

ODX 的工作原理

ODX 副本卸载使用基于令牌的机制在启用了 ODX 的 CIFS 服务器内部或之间读取和写入数据。CIFS 服务器不会通过主机路由数据，而是会向客户端发送一个表示数据的小令牌。ODX 客户端将该令牌呈现给目标服务器，然后，目标服务器可以将该令牌表示的数据从源传输到目标。

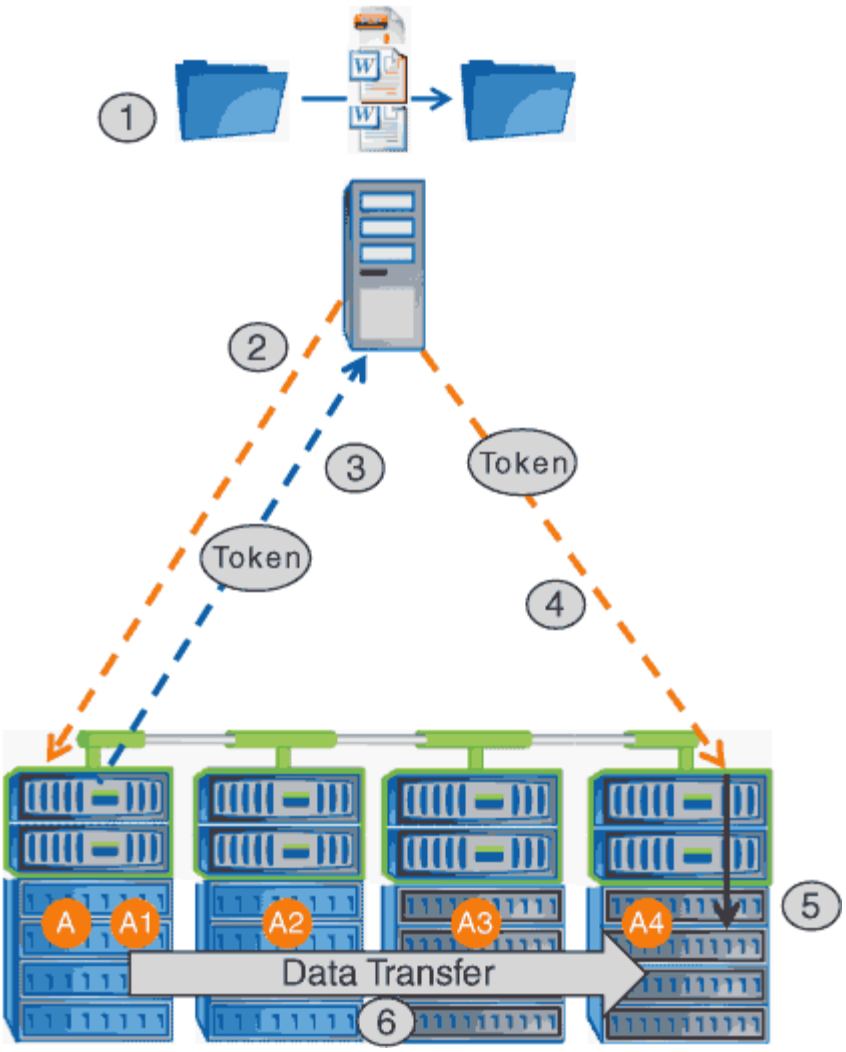
当 ODX 客户端了解到 CIFS 服务器支持 ODX 时，它会打开源文件并从 CIFS 服务器请求令牌。打开目标文件后，客户端将使用令牌指示服务器将数据直接从源复制到目标。

> 源和目标可以位于同一个 Storage Virtual Machine （ SVM ）上，也可以位于不同的 SVM 上，具体取决于复制操作的范围。

令牌可用作数据的时间点表示形式。例如，当您在存储位置之间复制数据时，表示数据段的令牌将返回给发出请求的客户端，客户端会将其复制到目标，从而无需通过客户端复制基础数据。

ONTAP 支持表示 8 MB 数据的令牌。大于 8 MB 的 ODX 副本可使用多个令牌执行，每个令牌表示 8 MB 的数据。

下图说明了 ODX 复制操作所涉及的步骤：



1. 用户使用 Windows 资源管理器，命令行界面或在虚拟机迁移过程中复制或移动文件，或者应用程序启动文件复制或移动。
2. 支持 ODX 的客户端会自动将此传输请求转换为 ODX 请求。

   发送到 CIFS 服务器的 ODX 请求包含令牌请求。

3. 如果在 CIFS 服务器上启用了 ODX ，并且此连接通过 SMB 3.0 建立，则 CIFS 服务器将生成一个令牌，此令牌是源上数据的逻辑表示。
4. 客户端会收到一个表示数据的令牌，并将其与写入请求一起发送到目标 CIFS 服务器。

   这是唯一通过网络从源复制到客户端，然后从客户端复制到目标的数据。

5. 令牌将传递到存储子系统。
6. SVM 在内部执行复制或移动。

   如果复制或移动的文件大于 8 MB ，则需要多个令牌才能执行复制。根据需要执行第 2 步至第 6 步以完成复制。

> 如果 ODX 卸载副本出现故障，则复制或移动操作将回退为传统读写操作来执行复制或移动操作。同样，如果目标 CIFS 服务器不支持 ODX 或 ODX 已禁用，则复制或移动操作将回退为传统的复制或移动操作读写操作。

使用 **ODX** 的要求

在 Storage Virtual Machine （ SVM ）中使用 ODX 进行副本卸载之前，您需要了解某些要求。

ONTAP 版本要求

ONTAP 版本支持使用 ODX 进行副本卸载。

SMB版本要求

- ONTAP 支持使用 SMB 3.0 及更高版本的 ODX 。
- 必须先在 CIFS 服务器上启用 SMB 3.0 ，然后才能启用 ODX ：
  - 启用 ODX 还会启用 SMB 3.0 （如果尚未启用）。
  - 禁用 SMB 3.0 也会禁用 ODX 。

Windows 服务器和客户端要求

在使用 ODX 卸载副本之前， Windows 客户端必须支持此功能。

。 "NetApp 互操作性表"包含有关受支持的Windows客户端的最新信息。

卷要求：

- 源卷必须至少为 1.25 GB 。
- 如果使用压缩卷，则压缩类型必须是自适应的，并且仅支持压缩组大小 8K 。

  不支持二级压缩类型

使用 **ODX** 的准则

在使用 ODX 进行副本卸载之前，您需要了解相关准则。例如，您需要了解可以使用 ODX 的卷类型，并了解集群内和集群间 ODX 的注意事项。

卷准则

- 在以下卷配置中，不能使用 ODX 进行副本卸载：
  - 源卷大小小于 1.25 GB

    要使用 ODX ，卷大小必须大于或等于 1.25 GB 。

  - 只读卷

    ODX 不用于驻留在负载共享镜像或 SnapMirror 或 SnapVault 目标卷中的文件和文件夹。

    - 如果源卷未进行重复数据删除
- 只有集群内副本才支持 ODX 副本。

  您不能使用 ODX 将文件或文件夹复制到另一个集群中的卷。

其他准则

- 在 SMB 环境中，要使用 ODX 进行副本卸载，文件必须大于或等于 256 KB 。

  较小的文件通过传统复制操作进行传输。

- ODX 副本卸载会在复制过程中使用重复数据删除。

  如果您不希望在复制或移动数据时在 SVM 卷上发生重复数据删除，则应在该 SVM 上禁用 ODX 副本卸载。

- 必须写入执行数据传输的应用程序以支持 ODX 。

  支持 ODX 的应用程序操作包括：

    - Hyper-V 管理操作，例如创建和转换虚拟硬盘（ VHD ），管理 Snapshot 副本以及在虚拟机之间复制文件
    - Windows 资源管理器操作
    - Windows PowerShell copy 命令
    - Windows 命令提示符复制命令

      Windows 命令提示符处的 Robocopy 支持 ODX 。

      > 应用程序必须在支持 ODX 的 Windows 服务器或客户端上运行。

  +
  有关 Windows 服务器和客户端上支持的 ODX 应用程序的详细信息，请参阅 Microsoft TechNet 库。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

ODX 的用例

您应了解在 SVM 上使用 ODX 的使用情形，以便确定 ODX 在何种情况下可为您带来性能优势。

支持 ODX 的 Windows 服务器和客户端会使用副本卸载作为在远程服务器之间复制数据的默认方式。如果 Windows 服务器或客户端不支持 ODX ，或者 ODX 副本卸载在任何时刻失败，则复制或移动操作将回退为复制或移动操作的传统读写操作。

以下使用情形支持使用 ODX 副本和移动：

- 卷内

源文件或 LUN 与目标文件或 LUN 位于同一个卷中。

- 卷间，同一节点，同一 SVM

  源文件或 LUN 和目标文件或 LUN 位于同一节点上的不同卷上。数据属于同一个 SVM 。

- 卷间，不同节点，相同 SVM

  源文件或 LUN 和目标文件或 LUN 位于不同节点上的不同卷上。数据属于同一个 SVM 。

- SVM 间，同一节点

  源和目标文件或 LUN 位于同一节点上的不同卷上。数据属于不同的 SVM 。

- SVM 间，不同节点

  源和目标文件或 LUN 位于不同节点上的不同卷上。数据属于不同的 SVM 。

- 集群间

  源 LUN 和目标 LUN 位于集群中不同节点上的不同卷上。此功能仅适用于 SAN ，不适用于 CIFS 。

还有一些其他特殊使用情形：

- 在 ONTAP ODX 实施中，您可以使用 ODX 在 SMB 共享与 FC 或 iSCSI 连接的虚拟驱动器之间复制文件。

  您可以使用 Windows 资源管理器， Windows 命令行界面或 PowerShell ， Hyper-V 或其他支持 ODX 的应用程序，在 SMB 共享和连接的 LUN 之间使用 ODX 副本卸载功能无缝复制或移动文件，但前提是 SMB 共享和 LUN 位于同一集群上。

- Hyper-V 还提供了一些 ODX 副本卸载的其他使用情形：

  - 您可以使用 ODX 副本卸载直通与 Hyper-V 在虚拟硬盘（ VHD ）文件内部或之间复制数据，或者在同一集群中映射的 SMB 共享和连接的 iSCSI LUN 之间复制数据。

    这样，子操作系统中的副本就可以传递到底层存储。

  - 创建固定大小的 VHD 时， ODX 用于使用众所周知的置零令牌以零初始化磁盘。
  - 如果源存储和目标存储位于同一集群上，则使用 ODX 副本卸载进行虚拟机存储迁移。

> 要利用 Hyper-V ODX 副本卸载直通的使用情形，子操作系统必须支持 ODX ，而子操作系统的磁盘必须是 SCSI 磁盘，并由支持 ODX 的存储（ SMB 或 SAN ）提供支持。子操作系统上的 IDE 磁盘不支持 ODX 直通。

启用或禁用**ODX**

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用 ODX 。默认情况下，如果同时启用了 SMB 3.0 ，则会启用对 ODX 副本卸载的支持。

开始之前

必须启用 SMB 3.0 。

关于此任务

如果禁用 SMB 3.0 ，则 ONTAP 还会禁用 SMB ODX 。如果重新启用 SMB 3.0 ，则必须手动重新启用 SMB ODX 。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

ODX 副本卸载的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
已禁用	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用 ODX 副本卸载：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

相关信息

可用的 SMB 服务器选项

通过使用自动位置提供 SMB 自动节点转介来缩短客户端响应时间

通过提供 SMB 自动节点转介和自动位置概述来缩短客户端响应时间

自动定位使用 SMB 自动节点转介来提高 Storage Virtual Machine （ SVM ）上的 SMB 客户端性能。自动节点转介会自动将请求客户端重定向到托管数据所在卷的节点 SVM 上的 LIF ，从而缩短客户端响应时间。

当 SMB 客户端连接到 SVM 上托管的 SMB 共享时，它可能会使用不拥有所请求数据的节点上的 LIF 进行连接。客户端连接到的节点使用集群网络访问另一个节点拥有的数据。如果 SMB 连接使用位于包含请求数据的节

点上的 LIF ，则客户端的响应速度会更快：

- ONTAP 通过使用 Microsoft DFS 转介来提供此功能，以通知 SMB 客户端命名空间中的请求文件或文件夹托管在其他位置。

  当节点确定包含数据的节点上存在 SVM LIF 时，它会进行转介。

- IPv4 和 IPv6 LIF IP 地址支持自动节点转介。
- 转介是根据客户端所连接的共享的根位置进行的。
- 转介发生在 SMB 协商期间。

  在建立连接之前进行转介。在 ONTAP 将 SMB 客户端转介到目标节点后，将建立连接，并且客户端将从该点通过转介的 LIF 路径访问数据。这样，客户端可以更快地访问数据，并避免额外的集群通信。

> 如果共享跨越多个接合点，而某些接合点指向其他节点上包含的卷，则共享中的数据将分布在多个节点上。由于 ONTAP 提供的转介是共享根的本地转介，因此 ONTAP 必须使用集群网络检索这些非本地卷中包含的数据。 使用这种类型的命名空间架构时，自动节点转介可能不会带来显著的性能优势。

如果托管数据的节点没有可用的 LIF ，则 ONTAP 将使用客户端选择的 LIF 建立连接。SMB 客户端打开文件后，它将继续通过相同的转介连接访问该文件。

如果由于任何原因 CIFS 服务器无法进行转介，则 SMB 服务不会中断。此时将建立 SMB 连接，就好像未启用自动节点转介一样。

相关信息

提高 Microsoft 远程复制性能

使用自动节点转介的要求和准则

在使用 SMB 自动节点转介（也称为 *autolocation*） 之前，您需要了解某些要求，包括支持此功能的 ONTAP 版本。您还需要了解支持的 SMB 协议版本以及某些其他特殊准则。

ONTAP 版本和许可证要求

- 集群中的所有节点都必须运行支持自动节点转介的 ONTAP 版本。
- 要使用自动定位，必须在 SMB 共享上启用 Widelink 。
- CIFS 必须获得许可， SVM 上必须存在 SMB 服务器。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。

SMB 协议版本要求

- 对于 SVM ， ONTAP 在所有 SMB 版本上均支持自动节点转介。

SMB 客户端要求

ONTAP 支持的所有 Microsoft 客户端均支持 SMB 自动节点转介。

互操作性表包含有关 ONTAP 支持的 Windows 客户端的最新信息。

"NetApp 互操作性表工具"

数据 LIF 要求

如果要使用数据 LIF 作为 SMB 客户端的潜在转介，则必须创建同时启用了 NFS 和 CIFS 的数据 LIF 。

如果目标节点包含仅为 NFS 协议启用或仅为 SMB 协议启用的数据 LIF ，则自动节点转介可能无法正常工作。

如果不满足此要求，则数据访问不受影响。SMB 客户端使用客户端用于连接到 SVM 的原始 LIF 映射共享。

建立转介 SMB 连接时的 NTLM 身份验证要求

必须允许在包含 CIFS 服务器的域和包含要使用自动节点转介的客户端的域上进行 NTLM 身份验证。

转介时， SMB 服务器会将 IP 地址转介给 Windows 客户端。由于在使用 IP 地址建立连接时使用 NTLM 身份验证，因此不会对转介连接执行 Kerberos 身份验证。

之所以出现这种情况、是因为Windows客户端无法创建Kerberos使用的服务主体名称(格式为 `service/NetBIOS name` 和 `service/FQDN`)、这意味着客户端无法向服务请求Kerberos票证。

将自动节点转介与主目录功能结合使用的准则

如果在配置共享时启用了主目录共享属性，则可以为主目录配置配置一个或多个主目录搜索路径。搜索路径可以指向包含 SVM 卷的每个节点上包含的卷。客户端会收到转介，如果有活动的本地数据 LIF 可用，则通过主用户主目录本地的转介 LIF 进行连接。

SMB 1.0 客户端在启用了自动节点转介的情况下访问动态主目录时，应遵循一些准则。这是因为 SMB 1.0 客户端在进行身份验证之前需要自动节点转介，而 SMB 服务器尚未拥有用户名。但是，如果满足以下条件，则 SMB 1.0 客户端可以正确访问 SMB 主目录：

- SMB 主目录配置为使用简单名称，例如 "` %w` " （ Windows 用户名）或 "` %u` " （映射的 UNIX 用户名），而不是域名模式名称，例如 "` %d\%w ` " （ domain-name\user-name ）。
- 创建主目录共享时， CIFS 主目录共享名称会使用变量（ "` %w` " 或 "` %u` " ）进行配置，而不是使用静态名称进行配置，例如 "`home` " 。

对于 SMB 2.x 和 SMB 3.0 客户端，使用自动节点转介访问主目录时，没有任何特殊准则。

在具有现有转介连接的 CIFS 服务器上禁用自动节点转介的准则

如果在启用此选项后禁用自动节点转介，则当前连接到转介 LIF 的客户端将保留此转介连接。由于 ONTAP 使用 DFS 转介作为 SMB 自动节点转介的机制，因此，在禁用此选项后，客户端甚至可以重新连接到转介的 LIF ，直到客户端缓存的转介转介转介给转介连接超时为止。即使还原到不支持自动节点转介的 ONTAP 版本，也是如此。客户端将继续使用转介，直到客户端缓存中的 DFS 转介超时为止。

自动定位通过 SMB 自动节点转介将客户端转介到拥有 SVM 数据卷的节点上的 LIF 来提高 SMB 客户端性能。当 SMB 客户端连接到 SVM 上托管的 SMB 共享时，它可能会在不拥有所请求数据的节点上使用 LIF 进行连接，并使用集群互连网络来检索数据。如果 SMB 连接使用位于包含所请求数据的节点上的 LIF ，则客户端的响应速度会更快。

ONTAP 通过使用 Microsoft 分布式文件系统（ DFS ）转介来提供此功能，以通知 SMB 客户端命名空间中请求的文件或文件夹托管在其他位置。当节点确定包含数据的节点上存在 SVM LIF 时，它会进行转介。转介是根据客户端所连接的共享的根位置进行的。

转介发生在 SMB 协商期间。在建立连接之前进行转介。在 ONTAP 将 SMB 客户端转介到目标节点后，将建立连接，并且客户端将从该点通过转介的 LIF 路径访问数据。这样，客户端可以更快地访问数据，并避免额外的集群通信。

在 **Mac OS** 客户端中使用自动节点转介的准则

Mac OS X 客户端不支持 SMB 自动节点转介，即使 Mac OS 支持 Microsoft 的分布式文件系统（ DFS ）也是如此。在连接到 SMB 共享之前， Windows 客户端会发出 DFS 转介请求。ONTAP 可转介到托管所请求数据的同一节点上的数据 LIF ，从而缩短客户端响应时间。尽管 Mac OS 支持 DFS ，但 Mac OS 客户端在这方面的行为与 Windows 客户端不完全相同。

相关信息

ONTAP 如何启用动态主目录

"网络管理"

"NetApp 互操作性表工具"

支持 **SMB** 自动节点转介

在启用 SMB 自动节点转介之前，您应了解某些 ONTAP 功能不支持转介。

- 以下类型的卷不支持 SMB 自动节点转介：
  - 负载共享镜像的只读成员
  - 数据保护镜像的目标卷
- 节点转介不会随 LIF 移动而移动。

  如果客户端正在使用通过 SMB 2.x 或 SMB 3.0 连接的转介连接，并且数据 LIF 无中断移动，则即使 LIF 不再是数据的本地连接，客户端也会继续使用相同的转介连接。

- 节点转介不会随卷移动而移动。

  如果客户端正在通过任何 SMB 连接使用转介连接，并且发生卷移动，则即使卷不再与数据 LIF 位于同一节点上，客户端仍会使用相同的转介连接。

启用或禁用 **SMB** 自动节点转介

您可以启用 SMB 自动节点转介以提高 SMB 客户端访问性能。如果不希望 ONTAP 向 SMB 客户端进行转介，则可以禁用自动节点转介。

开始之前

必须在 Storage Virtual Machine （ SVM ）上配置并运行 CIFS 服务器。

关于此任务

默认情况下， SMB 自动节点转介功能处于禁用状态。您可以根据需要在每个 SVM 上启用或禁用此功能。

此选项可在高级权限级别下使用。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 根据需要启用或禁用 SMB 自动节点转介：

SMB 自动节点转介的目标位置	输入以下命令 ...
enabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
已禁用	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

选项设置将对新的 SMB 会话生效。只有当现有缓存超时到期时，具有现有连接的客户端才能使用节点转介。

3. 切换到管理权限级别： `set -privilege admin`

相关信息

可用的 SMB 服务器选项

使用统计信息监控自动节点转介活动

要确定转介的SMB连接数、您可以使用监控自动节点转介活动 `statistics` 命令：通过监控转介，您可以确定自动转介在托管共享的节点上查找连接的范围，以及是否应重新分布数据 LIF 以更好地在本地访问 CIFS 服务器上的共享。

关于此任务

。 `cifs` 对象在高级权限级别提供了多个计数器、这些计数器在监控SMB自动节点转介时很有用：

- `node_referral_issued`

  在客户端使用由共享根节点托管的 LIF 进行连接后，已向共享根节点发出转介的客户端数量。

- `node_referral_local`

  使用由托管共享根的同一节点托管的 LIF 连接的客户端数量。本地访问通常可提供最佳性能。

- `node_referral_not_possible`

  在使用由共享根节点之外的节点托管的 LIF 进行连接后，尚未向托管共享根的节点发出转介的客户端数量。这是因为未找到共享根节点的活动数据 LIF 。

- `node_referral_remote`

  使用由与托管共享根的节点不同的节点托管的 LIF 连接的客户端数量。远程访问可能会导致性能下降。

您可以通过收集和查看特定时间段的数据（样本）来监控 Storage Virtual Machine （ SVM ）上的自动节点转介统计信息。如果不停止数据收集，您可以查看样本中的数据。停止数据收集可提供一个固定样本。如果不停止数据收集，则可以获取更新后的数据，以便与先前的查询进行比较。此比较可帮助您确定性能趋势。

评估和使用从收集的信息 `statistics` 命令中、您应了解客户端在环境中的分布情况。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 使用查看自动节点转介统计信息 `statistics` 命令：

   此示例通过收集和查看采样时间段的数据来查看自动节点转介统计信息：

   a. 开始收集： `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. 等待所需的收集时间过去。

   c. 停止收集： `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   d. 查看自动节点转介统计信息： `statistics show -sample-id sample1 -counter` **`node`**

   ```
   Object: cifs
   Instance: vs1
   Start-time: 2/4/2013 19:27:02
   End-time: 2/4/2013 19:30:11
   Cluster: cluster1

       Counter                                                   Value
       ----------------------------- ---------------------------
       node_name                                               node1
       node_referral_issued                                        0
       node_referral_local                                         1
       node_referral_not_possible                                  2
       node_referral_remote                                        2
       ...

       node_name                                               node2
       node_referral_issued                                        2
       node_referral_local                                         1
       node_referral_not_possible                                  0
       node_referral_remote                                        2
       ...
   ```

   输出将显示参与 SVM vs1 的所有节点的计数器。为清晰起见，此示例仅提供与自动节点转介统计信息相

关的输出字段。

3. 返回到管理权限级别： `set -privilege admin`

相关信息

显示统计信息

"性能监控设置"

使用 **Windows** 客户端监控客户端 **SMB** 自动节点转介信息

要从客户端的角度确定转介的内容、您可以使用Windows `dfsutil.exe` 实用程序。

Windows 7及更高版本的客户端提供的远程服务器管理工具(RRAS)套件包含 `dfsutil.exe` 实用程序。使用此实用程序，您可以显示有关转介缓存内容的信息，并查看有关客户端当前正在使用的每个转介的信息。您也可以使用实用程序清除客户端的转介缓存。有关详细信息，请参阅 Microsoft TechNet 库。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

使用基于访问的枚举为共享提供文件夹安全性

使用基于访问的枚举概述为共享提供文件夹安全性

在 SMB 共享上启用基于访问的枚举（ABE ）后，无权访问共享中包含的文件夹或文件的用户（无论是通过个人权限还是组权限限制）将看不到该共享资源显示在其环境中，尽管共享本身仍然可见。

通过传统的共享属性，您可以指定哪些用户（单个或组）有权查看或修改共享中包含的文件或文件夹。但是，它们不允许您控制共享中的文件夹或文件是否对无权访问它们的用户可见。如果共享中这些文件夹或文件的名称描述敏感信息，例如客户或正在开发的产品的名称，则可能会出现问题。

基于访问的枚举（ABE ）扩展了共享属性，以包括共享中文件和文件夹的枚举。因此， ABE 允许您根据用户访问权限筛选共享中的文件和文件夹的显示。也就是说，共享本身对所有用户可见，但共享中的文件和文件夹可能对指定用户显示或隐藏。除了保护工作场所中的敏感信息之外， ABE 还可以帮助您简化大型目录结构的显示，以使不需要访问您的全部内容的用户受益。例如，共享本身对所有用户可见，但共享中的文件和文件夹可能会显示或隐藏。

了解相关信息 "使用基于SMB/CIFS访问的枚举时对性能的影响"。

在 **SMB** 共享上启用或禁用基于访问的枚举

您可以在 SMB 共享上启用或禁用基于访问的枚举（ABE ），以允许或阻止用户查看其无权访问的共享资源。

关于此任务

默认情况下、ABE处于禁用状态。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
在新共享上启用 ABE	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` 创建SMB共享时、您可以指定其他可选共享设置和其他共享属性。有关详细信息、请参见的手册页 `vserver cifs share create` 命令：
在现有共享上启用 ABE	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 保留现有共享属性。ABE 共享属性将添加到现有共享属性列表中。
在现有共享上禁用 ABE	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 其他共享属性将保留。只会从共享属性列表中删除 ABE 共享属性。

2. 使用验证共享配置是否正确 `vserver cifs share show` 命令：

示例

以下示例将使用路径创建名为`sales`的ABE SMB共享 `/sales` 在SVM VS1上。共享是使用创建的 `access-based-enumeration` 作为共享属性：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

以下示例将添加 `access-based-enumeration` 将共享属性分配给名为`data2`的SMB共享：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

相关信息

在现有 SMB 共享上添加或删除共享属性

从 **Windows** 客户端启用或禁用基于访问的枚举

您可以从 Windows 客户端对 SMB 共享启用或禁用基于访问的枚举（ABE），这样您就可以配置此共享设置，而无需连接到 CIFS 服务器。

。 `abecmd` 实用程序在新版本的Windows Server和Windows客户端中不可用。它是作为Windows Server 2008的一部分发布的。Windows Server 2008的支持已于2020年1月14日结束。

步骤

1. 在支持ABE的Windows客户端中、输入以下命令： `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   有关的详细信息、请参见 `abecmd` 命令、请参见Windows客户端文档。

NFS 和 SMB 文件和目录命名依赖关系

NFS 和 SMB 文件和目录命名依赖关系概述

除了 ONTAP 集群和客户端上的语言设置之外，文件和目录命名约定还取决于网络客户端的` 操作系统和文件共享协议。

操作系统和文件共享协议确定以下内容：

- 文件名可以使用的字符
- 文件名区分大小写

ONTAP 支持文件，目录和 qtree 名称中的多字节字符，具体取决于 ONTAP 版本。

文件或目录名称可以使用的字符

如果要从具有不同操作系统的客户端访问文件或目录，则应使用在两个操作系统中均有效的字符。

例如，如果使用 UNIX 创建文件或目录，请勿在名称中使用冒号（：），因为 MS-DOS 文件或目录名称中不允许使用冒号。由于对有效字符的限制因操作系统而异，请参见客户端操作系统的文档，了解有关禁止字符的详细信息。

在多协议环境中，文件和目录名称区分大小写

对于NFS客户端、文件和目录名称区分大小写；对于SMB客户端、文件和目录名称不区分大小写、但保留大小写。您必须了解多协议环境的含义，以及在创建 SMB 共享时指定路径以及访问共享中的数据时可能需要执行的操作。

SMB客户端创建名为的目录时 `testdir`，SMB和NFS客户端都会将文件名显示为 `testdir`。但是、如果SMB用户稍后尝试创建目录名称 `TESTDIR`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的目录 `TESTDIR`、NFS和SMB客户端显示目录名称的方式不同，如下所示：

- 例如、在NFS客户端上、您可以在创建这两个目录时看到这两个目录名称 `testdir` 和 `TESTDIR`，因为目录名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个目录。一个目录具有基本文件名。为其他目录分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `testdir` 和 `TESTDI~1`。

- ONTAP将创建 `TESTDI~1` 用于区分这两个目录的目录名称。

  在这种情况下，在 Storage Virtual Machine （ SVM ）上创建或修改共享时，指定共享路径时必须使用 8.3 名称。

同样、对于文件、如果SMB客户端创建 `test.txt`，SMB和NFS客户端都会将文件名显示为 `text.txt`。但是、如果SMB用户稍后尝试创建 `Test.txt`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的文件 `Test.txt`、NFS和SMB客户端显示文件名的方式不同，如下所示：

- 在NFS客户端上、您会在创建时看到这两个文件名、 `test.txt` 和 `Test.txt`，因为文件名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个文件。一个文件具有基本文件名。为其他文件分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP将创建 `TEST~1.TXT` 用于区分这两个文件的文件名。

> 如果您已使用 vserver cifs character-mapping 命令启用或修改了字符映射，则通常不区分大小写的 Windows 查找将区分大小写。

ONTAP 如何创建文件和目录名称

ONTAP 会为可从 SMB 客户端访问的任何目录中的文件或目录创建并维护两个名称：原始长名称和 8.3 格式的名称。

对于超过八个字符名称或三个字符扩展名限制的文件或目录名称（对于文件）， ONTAP 将生成 8.3 格式的名称，如下所示：

- 如果原始文件或目录名称超过 6 个字符，则会将其截断为 6 个字符。
- 它会在截断后不再唯一的文件或目录名称后面附加一个颚化符（~ ）和一个数字（ 1 到 5 ）。

  如果由于名称相似而导致数字用尽，则会创建一个与原始名称无关的唯一名称。

- 对于文件，它会将文件扩展名截断为三个字符。

例如、如果NFS客户端创建一个名为的文件 `specifications.html`，则ONTAP创建的8.3格式文件名为 `specif~1.htm`。如果此名称已存在，则 ONTAP 会在文件名末尾使用其他数字。例如、如果NFS客户端创建另一个名为的文件 `specifications_new.html``的8.3格式 `specifications_new.html` 为 `specif~2.htm`。

ONTAP 如何处理多字节文件，目录和 **qtree** 名称

从 ONTAP 9.5 开始，通过支持 4 字节 UTF-8 编码名称，可以在基本多语言平面（ BMP ）之外创建和显示包含 Unicode 补充字符的文件，目录和树名。在早期版本中，这些补充字符无法在多协议环境中正确显示。

为了支持4字节UTF-8编码名称、为提供了一个新的_utf8mb4_语言代码 `vserver` 和 `volume` 命令系列。

您必须通过以下方式之一创建新卷：

- 设置音量 `-language` 显式选项： `volume create -language utf8mb4 {…}`

- 继承卷 `-language` 使用选项创建或修改的SVM中的选项： `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- 在ONTAP 9.6及更早版本中、您不能修改现有卷以支持utf8mb4；您必须创建一个新的utf8mb4就绪卷、然后使用基于客户端的复制工具迁移数据。

  您可以更新 SVM 以获得 utf8mb4 支持，但现有卷会保留其原始语言代码。

  如果您使用的是ONTAP 9.7P1或更高版本、则可以根据支持请求修改utf8mb4的现有卷。有关详细信息，请参见 "在ONTAP中创建卷后是否可以更改卷语言？"。

- 从ONTAP 9.8开始、您可以使用 `[-language <Language code>]` 用于将卷语言从*。UTF-8更改为utf8mb4的参数。要更改卷的语言、请联系 "NetApp 支持"。

  当前不支持包含 4 字节 UTF-8 字符的 LUN 名称。

- Unicode 字符数据通常在使用 16 位 Unicode 转换格式（ UTF-16 ）的 Windows 文件系统应用程序和使用 8 位 Unicode 转换格式（ UTF-8 ）的 NFS 文件系统中表示。

  在 ONTAP 9.5 之前的版本中，由 Windows 客户端创建的名称（包括 UTF-16 补充字符）会正确显示给其他 Windows 客户端，但对于 NFS 客户端，这些名称未正确转换为 UTF-8 。同样，对于 Windows 客户端，已创建的 NFS 客户端使用 UTF-8 补充字符的名称也未正确转换为 UTF-16 。

- 在运行 ONTAP 9.4 或更早版本的系统上创建包含有效或无效补充字符的文件名时， ONTAP 将拒绝该文件名并返回无效文件名错误。

  要避免此问题描述，请在文件名中仅使用 BMP 字符并避免使用补充字符，或者升级到 ONTAP 9.5 或更高版本。

从 ONTAP 9 开始， qtree 名称中允许使用 Unicode 字符。

- 您可以使用 `volume qtree` 用于设置或修改qtree名称的命令系列或System Manager。
- qtree 名称可以包含 Unicode 格式的多字节字符，例如日语和中文字符。
- 在 ONTAP 9.5 之前的版本中，仅支持 BMP 字符（即，可以用 3 个字节表示的字符）。

  在 ONTAP 9.5 之前的版本中， qtree 父卷的接合路径可以包含带有 Unicode 字符的 qtree 和目录名称。。 `volume show` 命令可在父卷具有UTF-8语言设置时正确显示这些名称。但是，如果父卷语言不是 UTF-8 语言设置之一，则会使用数字 NFS 备用名称显示接合路径的某些部分。

- 在 9.5 及更高版本中，如果 qtree 位于启用了 utf8mb4 的卷中，则 qtree 名称中支持 4 字节字符。

在卷上配置用于 **SMB** 文件名转换的字符映射

NFS 客户端可以创建包含对 SMB 客户端和某些 Windows 应用程序无效的字符的文件名。您可以为卷上的文件名转换配置字符映射，以使 SMB 客户端能够访问具有 NFS 名称的文件，否则这些名称将无效。

关于此任务

当 SMB 客户端访问 NFS 客户端创建的文件时， ONTAP 将查看该文件的名称。如果此名称不是有效的 SMB 文

件名（例如，如果其包含嵌入的冒号 "`：`" 字符），则 ONTAP 将返回为每个文件维护的 8.3 文件名。但是，如果应用程序将重要信息编码为较长的文件名，则会出现此问题。

因此，如果要在不同操作系统上的客户端之间共享文件，则应在文件名中使用在这两个操作系统中均有效的字符。

但是，如果 NFS 客户端创建的文件名包含的字符对于 SMB 客户端无效，则可以定义一个映射，将无效的 NFS 字符转换为 SMB 和某些 Windows 应用程序均可接受的 Unicode 字符。例如，此功能支持 CATIA MCAD 和 Mathematica 应用程序以及具有此要求的其他应用程序。

您可以逐个卷配置字符映射。

在卷上配置字符映射时，必须牢记以下几点：

- 字符映射不会跨接合点应用。

  您必须为每个接合卷显式配置字符映射。

- 您必须确保用于表示无效或非法字符的 Unicode 字符通常不会显示在文件名中；否则，将发生不需要的映射。

  例如，如果您尝试将冒号（：）映射到连字符（ - ），但在文件名中正确使用了连字符（ - ），则尝试访问名为 "`a-b`" 的文件的 Windows 客户端会将其请求映射到 NFS 名称 "`a： b`" （不是所需结果）。

- 应用字符映射后，如果映射仍包含无效的 Windows 字符，则 ONTAP 会回退到 Windows 8.3 文件名。
- 在 FPolicy 通知， NAS 审核日志和安全跟踪消息中，将显示映射的文件名。
- 创建类型为 DP 的 SnapMirror 关系时，源卷的字符映射不会复制到目标 DP 卷上。
- 区分大小写：由于映射的 Windows 名称转换为 NFS 名称，因此，名称的查找遵循 NFS 语义。这包括 NFS 查找区分大小写。这意味着，访问映射共享的应用程序不能依赖 Windows 不区分大小写的行为。但是， 8.3 名称是可用的，不区分大小写。
- 部分映射或无效映射：映射要返回到执行目录枚举（ "dir" ）的客户端的名称后，系统将检查生成的 Unicode 名称是否有效。如果此名称中仍包含无效字符，或者对于 Windows 无效（例如，此名称以 "." 或空白结尾），则会返回 8.3 名称，而不是无效名称。

步骤

1. 配置字符映射： +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

此映射由一个源 - 目标字符对列表组成，并以 "`：`" 分隔。这些字符是使用十六进制数字输入的 Unicode 字符。例如： 3c： E03C 。+

每个的第一个值 `mapping_text` 以冒号分隔的对是要转换的NFS字符的十六进制值、第二个值是SMB使用的Unicode值。映射对必须是唯一的（应存在一对一映射）。

- 源映射 +

下表显示了源映射允许的 Unicode 字符集：

+

Unicode 字符	打印字符	Description
0x01-0x19	不适用	非打印控制字符
0x5C		反斜杠
0x3a	:	冒号
0x2A	*	星号
0x3F	?	问号
0x22	"	引号
0x3C	<	小于
0x3e	>	大于
0x7C	我们可以为您提供	竖线
0xB1	±	加减号

- 目标映射

  您可以在 Unicode 的 "`私有使用区域` " 中指定以下范围内的目标字符： U+E0000…U+F8FF 。

示例

以下命令会为 Storage Virtual Machine （ SVM ） vs1 上名为 `data` 的卷创建字符映射：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

相关信息

在 NAS 命名空间中创建和管理数据卷

用于管理用于 **SMB** 文件名转换的字符映射的命令

您可以通过创建，修改，显示有关 FlexVol 卷上用于 SMB 文件名转换的文件字符映射的信息或删除此类映射来管理字符映射。

如果您要 ...	使用此命令 ...
创建新的文件字符映射	`vserver cifs character-mapping create`
显示有关文件字符映射的信息	`vserver cifs character-mapping show`
修改现有文件字符映射	`vserver cifs character-mapping modify`
删除文件字符映射	`vserver cifs character-mapping delete`

有关详细信息，请参见每个命令的手册页。

相关信息

在卷上配置用于 SMB 文件名转换的字符映射

提供对NAS数据的S3客户端访问

S3多协议概述

从ONTAP 9.12.1开始、您可以使运行S3协议的客户端访问为使用NFS和SMB协议的客户端提供的相同数据、而无需重新格式化。通过此功能、可以继续为NAS客户端提供NAS数据、同时向运行S3应用程序(如数据挖掘和人工智能)的S3客户端提供对象数据。

S3多协议功能可解决两种使用情形：

1. 使用S3客户端访问现有NAS数据

   如果您的现有数据是使用传统NAS客户端(NFS或SMB)创建的、并且位于NAS卷(FlexVol 或FlexGroup 卷)上、则现在可以使用S3客户端上的分析工具访问此数据。

2. 为能够使用NAS和S3协议执行I/O的现代客户端提供后端存储

   现在、您可以为Spark和Kafka等应用程序提供集成访问、这些应用程序可以使用NAS和S3协议读写相同的数据。

S3多协议的工作原理

使用ONTAP 多协议、您可以将相同的数据集作为文件层次结构或存储分段中的对象来呈现。为此、ONTAP 会创建"S3 NAS分段"、以使S3客户端能够使用S3对象请求在NAS存储中创建、读取、删除和枚举文件。此映射符合NAS安全配置、可观察文件和目录访问权限、并根据需要写入安全审核记录。

此映射是通过将指定的NAS目录层次结构显示为S3分段来实现的。目录层次结构中的每个文件都表示为S3对象、该对象的名称与映射的目录相对、目录边界由斜杠字符("/")表示。

正常的ONTAP定义的S3用户可以访问此存储、该存储受为映射到NAS目录的存储分段定义的存储分段策略的约束。为此、必须在S3用户和SMB/NFS用户之间定义映射。SMB/NFS用户的凭据将用于NAS权限检查、并包含在这些访问所产生的任何审核记录中。

当文件由SMB或NFS客户端创建时、文件会立即放置在目录中、因此在写入任何数据之前、客户端可以看到该文件。S3客户端希望使用不同的语义、在写入新对象的所有数据之前、新对象不会显示在命名空间中。将S3映射到NAS存储会使用S3语义创建文件、从而使这些文件在外部不可见、直到S3创建命令完成为止。

S3 NAS存储分段的数据保护

S3 NAS的"分段"只是S3客户端的NAS数据映射、而不是标准S3分段。因此、无需使用NetApp S3 SnapMirror功能来保护S3 NAS分段。相反、您可以使用异步SnapMirror卷复制来保护包含S3 NAS分段的卷。不支持SnapMirror同步和SVM灾难恢复。

从ONTAP 9.14.1开始、MetroCluster IP和FC配置的镜像和未镜像聚合支持S3 NAS分段。

了解相关信息 "异步SnapMirror"。

审核S3 NAS存储分段

由于S3 NAS存储分段不是传统的S3存储分段、因此无法配置S3审核来审核其访问权限。了解更多信息 "S3审核"。

但是、可以使用传统的ONTAP 审核过程审核S3 NAS存储分段中映射的NAS文件和目录以查看访问事件。因此、S3操作可能会触发NAS审核事件、但以下情况除外：

- 如果S3策略配置(组或存储分段策略)拒绝S3客户端访问、则不会对此事件启动NAS审核。这是因为在执行SVM审核检查之前会检查S3权限。
- 如果S3 GET请求的目标文件大小为0、则会将0个内容返回到GET请求、并且不会记录读取访问权限。
- 如果S3 GET请求的目标文件位于用户无遍历权限的文件夹中、则访问尝试将失败、并且事件不会记录。

了解相关信息 "审核SVM上的NAS事件"。

S3和NAS互操作性

ONTAP S3 NAS分段支持标准NAS和S3功能、但此处列出的功能除外。

S3 NAS存储分段当前不支持NAS功能

FabricPool 容量层

S3 NAS存储分段不能配置为FabricPool 的容量层。

S3 NAS存储分段当前不支持S3功能

AWS用户元数据

- 在当前版本中、作为S3用户元数据一部分收到的键值对不会与对象数据一起存储在磁盘上。
- 前缀为"x-AMZ-meta"的请求标头将被忽略。

AWS标记

- 在PUT对象和Multipart启动请求上、会忽略前缀为"x-AMZ-Tagging"的标头。
- 更新现有文件上的标记的请求(即使用"标记查询字符串"的PUT、GET和Delete请求)将被拒绝、并显示错误。

版本控制

无法在存储分段映射配置中指定版本控制。

- 包含非空版本规范(versionId=xyz query-string)的请求会收到错误响应。
- 影响存储分段版本控制状态的请求将被拒绝、但出现错误。

多部分操作

不支持以下操作：

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

S3客户端访问的NAS数据要求

请务必了解、在映射NAS文件和目录以进行S3访问时、存在一些固有的不兼容性。在使用S3 NAS分段提供NAS文件层次结构之前、可能需要对其进行调整。

通过使用S3存储分段语法映射NAS目录、S3 NAS分段可提供对该目录的S3访问、并且目录树中的文件将被视为对象。对象名称是相对于S3存储分段配置中指定的目录的文件的斜杠分隔路径名。

如果使用S3 NAS分段提供文件和目录、则此映射会产生一些要求：

- S3名称限制为1024字节、因此使用S3无法访问路径名较长的文件。
- 文件和目录名称不得超过255个字符、因此对象名称的连续非斜杠(‘/’)字符不能超过255个
- 使用反斜杠(‘\’)字符分隔的SMB路径名将在S3中显示为包含正斜杠(‘/’)字符的对象名称。
- 某些合法S3对象名称对不能同时位于映射的NAS目录树中。例如、合法S3对象名称"part1/part2"和"part1/part2/part3"映射到NAS目录树中不能同时存在的文件、因为"part1/part2"是第一个名称中的文件、而另一个名称中的目录。
  - 如果"part1/part2"是现有文件、则在S3上创建"part1/part2/part3"将失败。
  - 如果"part1/part2/part3"是现有文件、则S3创建或删除"part1/part2"将失败。
  - 创建与现有对象名称匹配的S3对象将替换已存在的对象(位于未版本控制的分段中)；该对象保留在NAS中、但需要完全匹配。上述示例不会通过发生原因 删除现有对象、因为名称发生冲突时不匹配。

虽然对象存储可支持大量任意名称、但如果将大量名称放置在一个目录中、则NAS目录结构可能会遇到性能问题。特别是、其中没有斜杠(‘/’)字符的名称将全部放置在NAS映射的根目录中。如果应用程序大量使用不是"不适合NAS的"名称、则最好托管在实际对象存储分段上、而不是NAS映射上。

启用对NAS数据的S3协议访问

启用S3协议访问包括确保启用了NAS的SVM满足与启用了S3的服务器相同的要求、包括添加对象存储服务器以及验证网络连接和身份验证要求。

对于新的ONTAP 安装、建议在将SVM配置为向客户端提供NAS数据后启用对SVM的S3协议访问。要了解有关NAS协议配置的信息、请参见：

- "NFS配置"
- "SMB配置"

开始之前

在启用S3协议之前、必须配置以下内容：

- S3协议和所需的NAS协议(NFS、SMB或两者)均已获得许可。
- 已为所需的NAS协议配置SVM。
- NFS和/或SMB服务器已存在。
- 已配置DNS和任何其他所需服务。
- 正在将NAS数据导出或共享到客户端系统。

关于此任务

要启用从 S3 客户端到启用了 S3 的 SVM 的 HTTPS 流量，需要证书颁发机构（ CA ）证书。可以使用以下三种来源的CA证书：

- SVM上的新ONTAP 自签名证书。
- SVM上的现有ONTAP 自签名证书。
- 第三方证书。

您可以对S3/NAS存储分段使用与提供NAS数据相同的数据LIF。如果需要特定的IP地址、请参见 "创建数据 LIF："。要在LIF上启用S3数据流量、需要使用S3服务数据策略；您可以修改SVM的现有服务策略以包括S3。

创建S3对象服务器时、您应准备好将S3服务器名称输入为完全限定域名(FQDN)、客户端将使用该域名进行S3访问。S3服务器FQDN不能以分段名称开头。

System Manager

1. 在配置了NAS协议的Storage VM上启用S3。
   a. 单击*存储>存储VM*、选择一个已准备好NAS的Storage VM、单击设置、然后单击 ⚙ 在 S3 下。
   b. 选择证书类型。无论选择系统生成的证书还是您自己的证书之一，客户端访问都需要此证书。
   c. 输入网络接口。
2. 如果选择了系统生成的证书，则在确认创建新 Storage VM 后，您将看到证书信息。单击 * 下载 * 并保存以供客户端访问。
   - 不会再显示此机密密钥。
   - 如果您再次需要证书信息：单击 * 存储 > 存储 VM* ，选择 Storage VM ，然后单击 * 设置 * 。

命令行界面

1. 验证SVM：+是否允许使用S3协议
   `vserver show -fields allowed-protocols`
2. 记录此SVM的公有 密钥证书。+
   如果需要新的ONTAP自签名证书、请参见 "在 SVM 上创建并安装 CA 证书"。
3. 更新服务数据策略
   a. 显示SVM +的服务数据策略
      `network interface service-policy show -vserver svm_name`
   b. 添加 `data-core` 和 `data-s3-server services` 如果不存在。+
      `network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. 验证SVM上的数据LIF是否满足您的要求：+
   `network interface show -vserver svm_name`
5. 创建S3服务器：+
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

您可以在创建 S3 服务器时或以后任何时间指定其他选项。

- 默认情况下， HTTPS 在端口 443 上处于启用状态。您可以使用-secure listener-port选项更改端口号。+
  启用 HTTPS 后，要与 SSL/TLS 正确集成，需要 CA 证书。
- 默认情况下， HTTP 处于禁用状态；启用后，服务器将侦听端口 80 。您可以使用-is-http-enabled选项启用此端口、也可以使用-listener-port选项更改端口号。+
  启用 HTTP 后，所有请求和响应都将通过网络以明文形式发送。
  1. 验证是否已根据需要配置S3：+
     `vserver object-store-server show`

示例+
以下命令将验证所有对象存储服务器的配置值：+

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

创建S3 NAS存储分段

S3 NAS存储分段是S3存储分段名称和NAS路径之间的映射。通过S3 NAS分段、您可以为SVM命名空间中具有现有卷和目录结构的任何部分提供S3访问权限。

开始之前

- 在包含NAS数据的SVM中配置了S3对象服务器。
- NAS数据符合 "S3客户端访问的要求"。

关于此任务

您可以配置S3 NAS存储分段以指定SVM根目录中的任何一组文件和目录。

您还可以设置分段策略、以便根据以下参数的任意组合允许或禁止访问NAS数据：

- 文件和目录
- 用户和组权限
- S3操作

例如、您可能希望使用单独的存储分段策略、为一组用户授予只读数据访问权限、并使用另一个存储分段策略、允许受限组对该数据的一部分执行操作。

由于S3 NAS的"分段"是映射而不是S3分段、因此标准S3分段的以下属性不适用于S3 NAS分段。

- **aggr-list \ aggr-list-multi**倍 频**\ storage-service-level \ volume \ size \ exex**懦**-aggr-list \ QoS-policy-group+**
  配置S3 NAS分段时、不会创建任何卷或qtree。
- 角色\受**-protre**｝\受**-proty-on-ONTAP**保护\受**-proty-on-Cloud**保护+
  S3 NAS分段不会使用S3 SnapMirror进行保护或镜像、而是会使用卷粒度级别的常规SnapMirror保护。
- 版本控制状态+
  NAS卷通常采用Snapshot技术来保存不同的版本。但是、S3 NAS存储分段当前不支持版本控制。
- *逻辑使用\ object-count *+
  可通过volume命令为NAS卷提供等效统计信息。

System Manager

在启用了NAS的Storage VM上添加新的S3 NAS存储分段。

1. 单击 * 存储 > 分段 * ，然后单击 * 添加 * 。
2. 输入S3 NAS存储分段的名称并选择Storage VM、不要输入大小、然后单击*更多选项*。
3. 输入有效的路径名称或单击浏览以从有效路径名称列表中进行选择。+
   输入有效的路径名后、与S3 NAS配置无关的选项将被隐藏。
4. 如果已将S3用户映射到NAS用户并创建了组、则可以配置其权限、然后单击*保存*。+
   在此步骤中配置权限之前、您必须已将S3用户映射到NAS用户。

否则、请单击*保存*以完成S3 NAS存储分段配置。

命令行界面

在包含NAS文件系统的SVM中创建S3 NAS存储分段。+

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

示例：+

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

启用S3客户端用户

要使S3客户端用户能够访问NAS数据、您必须将S3用户名映射到相应的NAS用户、然后向其授予使用存储分段服务策略访问NAS数据的权限。

开始之前

客户端访问的用户名—Linux/UNIX、Windows和S3客户端用户—必须已存在。

关于此任务

通过将S3用户名映射到相应的Linux/UNIX或Windows用户、可以在S3客户端访问NAS文件时对这些文件进行授权检查。通过提供S3用户名_Pattern_来指定S3到NAS的映射、该用户名可以表示为单个名称或POSIX正则表达式、并提供Linux/UNIX或Windows用户名_Replacement。

如果不存在名称映射、则会使用默认名称映射、其中S3用户名本身将用作UNIX用户名和Windows用户名。您可以使用修改UNIX和Windows默认用户名映射 `vserver object-store-server modify` 命令：

仅支持本地名称映射配置；不支持LDAP。

将S3用户映射到NAS用户后、您可以为用户授予权限、以指定其有权访问的资源(目录和文件)以及允许或不允许在其中执行的操作。

System Manager

1. 为UNIX或Windows客户端(或两者)创建本地名称映射。
   a. 单击*存储>分段*、然后选择启用了S3/NAS的Storage VM。
   b. 选择*设置*、然后单击 → 在*名称映射*中(在*主机用户和组*下)。
   c. 在* S3到Windows 或 S3到UNIX*图块(或两者)中、单击*添加*、然后输入所需的*模式*(S3)和*替换*(NAS)用户名。
2. 创建存储分段策略以提供客户端访问。
   a. 单击*存储>分段*、然后单击 ⋮ 在所需的S3存储分段旁边、单击*编辑*。
   b. 单击*添加*并提供所需的值。
      - 主体—提供S3用户名或使用默认值(所有用户)。
      - 影响-选择*允许*或*拒绝*。
      - 操作-输入这些用户和资源的操作。对象存储服务器当前为S3 NAS分段支持的一组资源操作包括：GetObject、PutObject、DeleteObject、ListBucketAcl、GetBucketAcl、 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning和ListBucketVersions。此参数可使用通配符。
      - 资源-输入允许或拒绝操作的文件夹或文件路径、或者使用默认值(存储分段的根目录)。

命令行界面

1. 为UNIX或Windows客户端(或两者)创建本地名称映射。+
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` —映射评估的优先级编号；输入1或2。
   - `-pattern` —S3用户名或正则表达式
   - `-replacement` —Windows或UNIX用户名

示例+

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. 创建存储分段策略以提供客户端访问。+
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` -指定在用户请求操作时是允许还是拒绝访问。
   - `-action <Action>, …` -指定允许或拒绝的资源操作。对象存储服务器当前为S3 NAS分段支持的一组资源操作包括：GetObject、PutObject、DeleteObject、ListBucketAcl、GetBucketAcl、GetObjectAcl、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、 GetBucketVersioning、PutBucketVersioning和ListBucketVersions。此参数可使用通配符。
   - `-principal <Objectstore Principal>, …` -根据在此参数中指定的对象存储服务器用户或组验证请求访问的用户。

        - 通过向组名称添加前缀group/来指定对象存储服务器组。
        - `-principal` -(连字符)授予所有用户访问权限。
    - `-resource <text>, …` -指定为其设置了允许/拒绝权限的分段、文件夹或对象。此参数可使用通配符。
    - `[-sid <SID>]` -指定对象存储服务器存储分段策略语句的可选文本注释。

示例+

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Microsoft Hyper-V 和 SQL Server 的 SMB 配置

Microsoft Hyper-V 和 SQL Server 的 SMB 配置概述

通过 ONTAP 功能，您可以通过 SMB 协议为 Microsoft Hyper-V 和 Microsoft SQL Server 这两个 Microsoft 应用程序启用无中断运行。

如果要在以下情况下实施 SMB 无中断操作，应使用以下过程：

- 已配置基本 SMB 协议文件访问。
- 您希望启用 SVM 中的 SMB 3.0 或更高版本文件共享以存储以下对象：
    - Hyper-V 虚拟机文件
    - SQL Server 系统数据库

相关信息

有关ONTAP技术以及与外部服务交互的追加信息、请参见以下技术报告(TRs)：
* "NetApp 技术报告 4172： 《基于 SMB 3.0 的 Microsoft Hyper-V 与 ONTAP 最佳实践》"
* "NetApp 技术报告 4369： 《采用集群模式 Data ONTAP 的 Microsoft SQL Server 和 SnapManager 7.2 for SQL Server 最佳实践》"

配置基于 SMB 的适用于 Microsoft Hyper-V 和 SQL Server 的 ONTAP 解决方案

您可以使用持续可用的 SMB 3.0 及更高版本的文件共享将 Hyper-V 虚拟机文件或 SQL Server 系统数据库和用户数据库存储在 SVM 中的卷上，同时为计划内和计划外事件提供无中断运行（ NDO ）。

基于 SMB 的 Microsoft Hyper-V

要创建基于 SMB 解决方案的 Hyper-V ，必须先配置 ONTAP ，以便为 Microsoft Hyper-V 服务器提供存储服务。此外，您还必须配置 Microsoft 集群（如果使用集群配置）， Hyper-V 服务器，与 CIFS 服务器托管的共享的持续可用 SMB 3.0 连接以及备份服务（可选），以保护存储在 SVM 卷上的虚拟机文件。

> Hyper-V 服务器必须在 Windows 2012 Server 或更高版本上进行配置。独立和集群 Hyper-V 服务器配置均受支持。

- 有关创建 Microsoft 集群和 Hyper-V 服务器的信息，请参见 Microsoft 网站。
- SnapManager for Hyper-V 是一款基于主机的应用程序，可用于提供基于 Snapshot 副本的快速备份服务，旨在与基于 SMB 的 Hyper-V 配置集成。

  有关将 SnapManager 与基于 SMB 的 Hyper-V 配置结合使用的信息，请参见 _Hyper-V SnapManager 安装和管理指南 _ 。

基于 SMB 的 Microsoft SQL Server

要通过 SMB 解决方案创建 SQL Server ，必须先配置 ONTAP ，以便为 Microsoft SQL Server 应用程序提供存储服务。此外，您还必须配置 Microsoft 集群（如果使用的是集群配置）。然后，您可以在 Windows 服务器上安装和配置 SQL Server ，并创建持续可用的 SMB 3.0 连接以连接到 CIFS 服务器托管的共享。您可以选择配置备份服务来保护存储在 SVM 卷上的数据库文件。

> 必须在 Windows 2012 Server 或更高版本上安装和配置 SQL Server 。独立配置和集群配置均受支持。

- 有关创建 Microsoft 集群以及安装和配置 SQL Server 的信息，请参见 Microsoft 网站。
- 适用于Microsoft SQL Server的SnapCenter 插件是一款基于主机的应用程序、它有助于提供基于Snapshot副本的快速备份服务、旨在通过SMB配置与SQL Server集成。

  有关使用适用于Microsoft SQL Server的SnapCenter 插件的信息、请参见 "适用于 Microsoft SQL Server 的 SnapCenter 插件" 文档

通过 SMB 实现 Hyper-V 和 SQL Server 无中断运行

Hyper-V 和基于 SMB 的 SQL Server 无中断运行的含义

Hyper-V 和基于 SMB 的 SQL Server 无中断运行是指通过这些功能的组合，可以使应用程序服务器和包含的虚拟机或数据库保持联机状态，并在执行多项管理任务期间提供持续可用性。这包括存储基础架构的计划内和计划外停机。

支持通过 SMB 对应用程序服务器执行无中断操作的操作包括：

- 计划内接管和交还
- 计划外接管
- 升级
- 计划内聚合重新定位（ARL）

- LIF 迁移和故障转移
- 计划内卷移动

支持通过 **SMB** 实现无中断操作的协议

随着 SMB 3.0 的发布， Microsoft 发布了新协议，以提供必要的功能，支持通过 SMB 对 Hyper-V 和 SQL Server 执行无中断操作。

ONTAP 在通过 SMB 为应用程序服务器提供无中断运行时使用以下协议：

- SMB 3.0
- 见证

有关基于 **SMB** 的 **Hyper-V** 和 **SQL Server** 无中断运行的关键概念

在通过 SMB 解决方案配置 Hyper-V 或 SQL Server 之前，您应了解有关无中断运行（ NDOS ）的某些概念。

- * 持续可用共享 *

  设置了持续可用共享属性的 SMB 3.0 共享。通过持续可用的共享进行连接的客户端可以在接管，交还和聚合重新定位等中断事件发生后继续运行。

- 节点

  作为集群成员的单个控制器。为了区分 SFO 对中的两个节点，一个节点有时称为 *local nodge* ，另一个节点有时称为 *partner nodge* 或 *remote nodge* 。存储的主所有者是本地节点。辅助所有者是配对节点，在主所有者出现故障时控制存储。每个节点都是其存储的主所有者，也是其配对节点存储的二级所有者。

- * 无中断聚合重新定位 *

  能够在集群中 SFO 对内的配对节点之间移动聚合，而不会中断客户端应用程序。

- * 无中断故障转移 *

  请参见 *Takeover* 。

- * 无中断 LIF 迁移 *

  能够执行 LIF 迁移，而不会中断通过 LIF 连接到集群的客户端应用程序。对于 SMB 连接，只有使用 SMB 2.0 或更高版本进行连接的客户端才可以执行此操作。

- * 无中断运行 * 。

  能够执行主要的 ONTAP 管理和升级操作，并在不中断客户端应用程序的情况下承受节点故障。此术语指的是从整体上收集的无中断接管，无中断升级和无中断迁移功能。

- * 无中断升级 *

  能够在不中断应用程序的情况下升级节点硬件或软件。

- * 无中断卷移动 *

  可以在整个集群中自由移动卷，而不会中断正在使用该卷的任何应用程序。对于 SMB 连接，所有版本的 SMB 都支持无中断卷移动。

- * 持久性句柄 *

  SMB 3.0 的一个属性，允许持续可用的连接在断开连接时透明地重新连接到 CIFS 服务器。与持久句柄类似，在与连接客户端的通信丢失后， CIFS 服务器会将永久性句柄保留一段时间。但是，持久句柄比持久句柄更具弹性。在重新连接后，除了让客户端有机会在 60 秒的窗口内回收句柄之外， CIFS 服务器还会在该 60 秒窗口期间拒绝访问请求访问文件的任何其他客户端。

  有关永久性句柄的信息会镜像到 SFO 配对节点的永久性存储上，这样，在 SFO 配对节点接管节点存储所有权的事件发生后，具有已断开永久性句柄的客户端可以回收此持久句柄。除了在发生 LIF 移动时提供无中断操作（持久处理支持）之外，永久性句柄还可为接管，交还和聚合重新定位提供无中断操作。

- * SFO 交还 *

  从接管事件中恢复时，将聚合返回到其主位置。

- * SFO 对 *

  一对节点，其控制器已配置为在其中一个节点停止运行时彼此提供数据。根据系统型号，两个控制器可以位于一个机箱中，也可以位于不同的机箱中。在双节点集群中称为 HA 对。

- * 接管 *

  当存储的主所有者出现故障时，配对节点控制存储的过程。在 SFO 环境下，故障转移和接管是同义词。

SMB 3.0 功能如何支持通过 **SMB** 共享进行无中断操作

SMB 3.0 提供了关键功能，支持通过 SMB 共享对 Hyper-V 和 SQL Server 执行无中断操作。其中包括 `continuously-available` 共享属性和一种称为_PER持 式句柄_的文件句柄类型、该句柄允许SMB客户端回收文件打开状态并透明地重新建立SMB连接。

对于连接到具有持续可用共享属性集的共享的支持 SMB 3.0 的客户端，可以将永久性句柄授予这些客户端。如果 SMB 会话已断开连接，则 CIFS 服务器会保留有关永久性句柄状态的信息。在允许客户端重新连接的 60 秒期间， CIFS 服务器会阻止其他客户端请求，从而允许具有永久性句柄的客户端在网络断开连接后回收句柄。具有永久性句柄的客户端可以使用 Storage Virtual Machine （ SVM ）上的一个数据 LIF 进行重新连接，方法是通过同一个 LIF 或不同的 LIF 进行重新连接。

聚合重新定位，接管和交还都发生在 SFO 对之间。为了无缝管理具有永久性句柄的文件的会话断开连接和重新连接，配对节点会维护一份所有永久性句柄锁定信息的副本。无论是计划内事件还是计划外事件， SFO 配对节点都可以无中断地管理永久性句柄重新连接。利用这一新功能，与 CIFS 服务器的 SMB 3.0 连接可以透明，无中断地故障转移到传统中断事件中分配给 SVM 的另一个数据 LIF 。

尽管使用永久性句柄可以使 CIFS 服务器透明地对 SMB 3.0 连接进行故障转移，但如果故障导致 Hyper-V 应用程序故障转移到 Windows Server 集群中的另一个节点，则客户端无法回收这些已断开的句柄的文件句柄。在这种情况下，如果 Hyper-V 应用程序在其他节点上重新启动，处于 Disconnected 状态的文件句柄可能会阻止其访问。"`故障转移集群` " 是 SMB 3.0 的一部分，可通过提供一种机制来使陈旧的冲突句柄失效来解决此情形。通过这种机制， Hyper-V 集群可以在 Hyper-V 集群节点出现故障时快速恢复。

见证协议如何增强透明故障转移

见证协议为 SMB 3.0 持续可用的共享（ CA 共享）提供增强的客户端故障转移功能。见证有助于加快故障转移速度，因为它会绕过 LIF 故障转移恢复期间。当节点不可用时，它会通知应用程序服务器，而无需等待 SMB 3.0 连接超时。

故障转移是无缝的，客户端上运行的应用程序不会意识到发生了故障转移。如果见证不可用，则故障转移操作仍会成功执行，但无见证的故障转移效率较低。

满足以下要求时，可以执行见证增强型故障转移：

- 它只能用于启用了 SMB 3.0 的支持 SMB 3.0 的 CIFS 服务器。
- 共享必须使用 SMB 3.0 并设置了持续可用性共享属性。
- 应用程序服务器所连接节点的 SFO 配对节点必须至少为托管应用程序服务器数据的 Storage Virtual Machine （ SVM ）分配一个运行数据 LIF 。

> 见证协议在 SFO 对之间运行。由于 LIF 可以迁移到集群中的任何节点，因此任何节点都可能需要成为其 SFO 配对节点的见证。 如果托管应用程序服务器数据的 SVM 在配对节点上没有活动数据 LIF ，则见证协议无法为给定节点上的 SMB 连接提供快速故障转移。因此，对于托管其中一种配置的每个 SVM ，集群中的每个节点必须至少具有一个数据 LIF 。

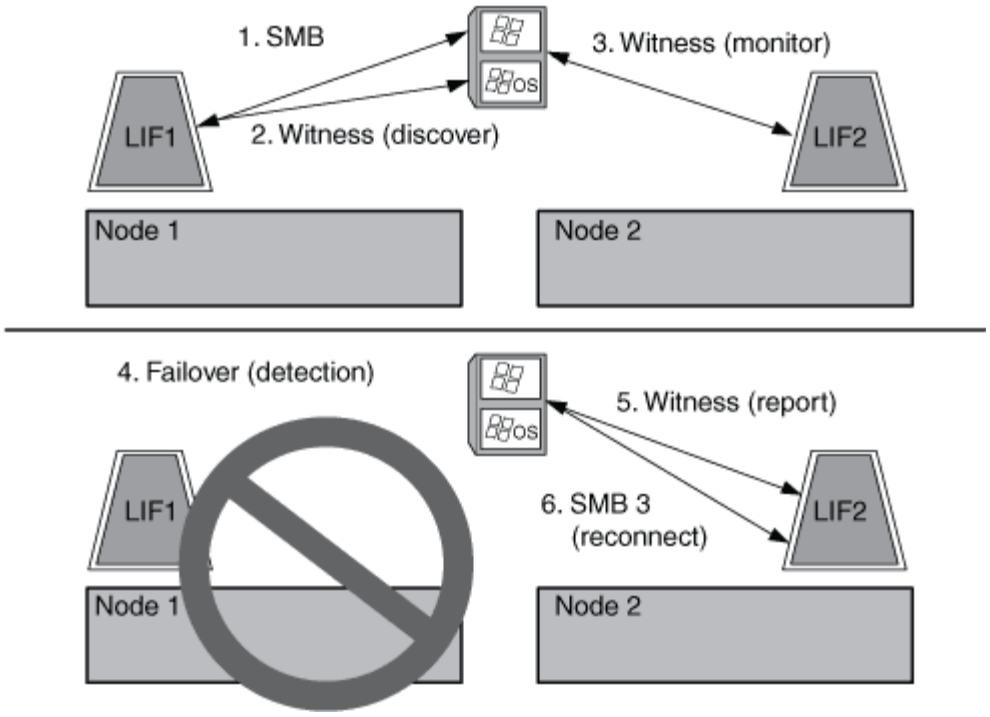
- 应用程序服务器必须使用存储在 DNS 中的 CIFS 服务器名称来连接到 CIFS 服务器，而不是使用单个 LIF IP 地址。

见证协议的工作原理

ONTAP 通过使用节点的 SFO 配对节点作为见证来实施见证协议。如果发生故障，配对节点会快速检测到故障并通知 SMB 客户端。

见证协议可通过以下过程提供增强的故障转移：

1. 当应用程序服务器与 Node1 建立持续可用的 SMB 连接时， CIFS 服务器会通知应用程序服务器见证可用。
2. 应用程序服务器从 Node1 请求见证服务器的 IP 地址，并接收分配给 Storage Virtual Machine （ SVM ）的 Node2 （ SFO 配对节点）数据 LIF IP 地址列表。
3. 应用程序服务器会选择一个 IP 地址，创建与 Node2 的见证连接，并注册以在 Node1 上持续可用的连接必须移动时收到通知。
4. 如果 Node1 上发生故障转移事件，则见证者会协助处理故障转移事件，但不会涉及交还。
5. 见证服务器检测故障转移事件，并通过见证连接通知应用程序服务器， SMB 连接必须移至 Node2 。
6. 应用程序服务器会将 SMB 会话移至 Node2 ，并在不中断客户端访问的情况下恢复连接。



使用远程 **VSS** 进行基于共享的备份

使用远程 **VSS** 进行基于共享的备份概述

您可以使用远程 VSS 对存储在 CIFS 服务器上的 Hyper-V 虚拟机文件执行基于共享的备份。

Microsoft 远程 VSS （卷影复制服务）是现有 Microsoft VSS 基础架构的扩展。借助远程 VSS ， Microsoft 扩展了 VSS 基础架构，以支持 SMB 共享的卷影复制。此外、Hyper-V等服务器应用程序可以将VHD文件存储在SMB文件共享上。通过这些扩展、可以为在共享上存储数据和配置文件的虚拟机创建应用程序一致的卷影副本。

远程 **VSS** 概念

您应了解一些必要的概念，以了解备份服务如何使用基于 SMB 的 Hyper-V 配置的远程 VSS （卷影复制服务）。

- * VSS （卷影复制服务） *

  一种 Microsoft 技术，用于在特定时间点为特定卷上的数据创建备份副本或快照。VSS 可在数据服务器，备份应用程序和存储管理软件之间进行协调，以支持创建和管理一致的备份。

- * 远程 VSS （远程卷影复制服务） *

  一项 Microsoft 技术，用于为在通过 SMB 3.0 共享访问数据的特定时间点处于数据一致状态的数据创建基于共享的备份副本。也称为 *Volume Shadow Copy Service* 。

- * 卷影复制 *

  共享中包含的一组重复数据，在定义明确的即时状态下运行。卷影副本用于为数据创建一致的时间点备份，从而使系统或应用程序能够继续更新原始卷上的数据。

- * 卷影复制集 *

  一个或多个卷影副本的集合，其中每个卷影副本对应于一个共享。卷影副本集中的卷影副本表示必须在同一操作中备份的所有共享。启用了 VSS 的应用程序上的 VSS 客户端可确定要包含在卷影集中的卷影副本。

- * 卷影复制设置自动恢复 *

  启用了 VSS 的远程备份应用程序的备份过程的一部分，其中包含卷影副本的副本目录在时间点上保持一致。备份开始时，应用程序上的 VSS 客户端会触发应用程序对计划备份的数据（ Hyper-V 中的虚拟机文件）进行软件检查。然后， VSS 客户端允许应用程序继续运行。创建卷影副本集后，远程 VSS 会使卷影副本集可写，并将可写副本公开给应用程序。应用程序使用先前的软件检查点执行自动恢复，从而准备卷影副本集以进行备份。自动恢复会撤消自创建检查点以来对文件和目录所做的更改，从而使卷影副本处于一致状态。对于启用了 VSS 的备份，自动恢复是一个可选步骤。

- * 卷影复制 ID*

  用于唯一标识卷影副本的 GUID 。

- * 卷影复制集 ID*

  一个 GUID ，用于唯一标识一组卷影复制 ID 到同一服务器。

- * 适用于 Hyper-V 的 SnapManager *

  一款可自动执行和简化 Microsoft Windows Server 2012 Hyper-V 备份和还原操作的软件SnapManager for Hyper-V 使用具有自动恢复功能的远程 VSS 通过 SMB 共享备份 Hyper-V 文件。

相关信息

有关基于 SMB 的 Hyper-V 和 SQL Server 无中断运行的关键概念

使用远程 VSS 进行基于共享的备份

远程 **VSS** 使用的目录结构示例

远程 VSS 会在创建卷影副本时遍历存储 Hyper-V 虚拟机文件的目录结构。了解什么是合适的目录结构非常重要，这样您才能成功创建虚拟机文件的备份。

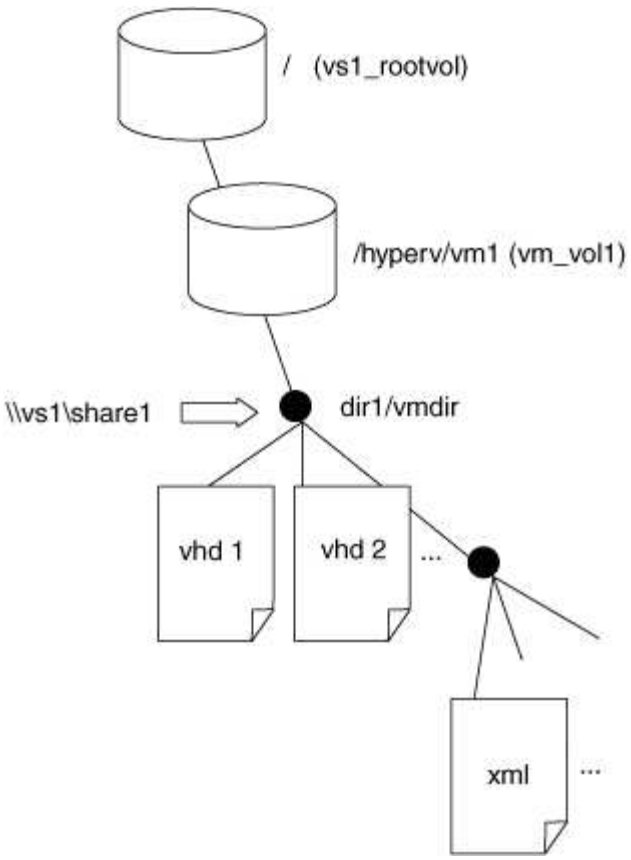
成功创建卷影副本所支持的目录结构符合以下要求：

- 用于存储虚拟机文件的目录结构中仅存在目录和常规文件。

  目录结构不包含接合，链接或非常规文件。

- 虚拟机的所有文件都位于一个共享中。
- 用于存储虚拟机文件的目录结构不会超过卷影副本目录的已配置深度。
- 共享的根目录仅包含虚拟机文件或目录。

在下图中、创建了名为vm_vol1的卷、其中接合点位于 `/hyperv/vm1` 在Storage Virtual Machine (SVM)的VS1上。包含虚拟机文件的子目录会在接合点下创建。Hyper-V服务器的虚拟机文件通过具有路径的共享1进行访问 `/hyperv/vm1/dir1/vmdir`。卷影复制服务会为共享 1 下的目录结构中包含的所有虚拟机文件创建卷影副本（直到卷影复制目录的已配置深度为止）。



SnapManager for Hyper-V 如何通过 **SMB** 管理 **Hyper-V** 基于 **VSS** 的远程备份

您可以使用 SnapManager for Hyper-V 管理基于 VSS 的远程备份服务。使用适用于 Hyper-V 的 SnapManager 托管备份服务创建节省空间的备份集具有一定优势。

Hyper-V 托管备份的 SnapManager 优化包括以下内容：

- SnapDrive 与 ONTAP 的集成可在发现 SMB 共享位置时实现性能优化。

  ONTAP 为 SnapDrive 提供共享所在卷的名称。

- SnapManager for Hyper-V 指定卷影复制服务需要复制的 SMB 共享中的虚拟机文件列表。

  通过提供目标虚拟机文件列表，卷影复制服务无需为共享中的所有文件创建卷影副本。

- Storage Virtual Machine （ SVM ）会保留 SnapManager for Hyper-V 的 Snapshot 副本以用于还原。

  没有备份阶段。备份是节省空间的 Snapshot 副本。

SnapManager for Hyper-V 可通过以下过程为基于 SMB 的 HyperV 提供备份和还原功能：

1. 准备卷影复制操作

   SnapManager for Hyper-V 应用程序的 VSS 客户端会设置卷影副本集。VSS 客户端收集有关卷影副本集中要包含的共享的信息，并将此信息提供给 ONTAP 。一个卷集可能包含一个或多个卷影副本，一个卷影副本对应于一个共享。

2. 创建卷影副本集（如果使用自动恢复）

   对于卷影副本集中包含的每个共享， ONTAP 会创建一个卷影副本并使卷影副本可写。

3. 公开卷影副本集

   在 ONTAP 创建卷影副本后，这些副本会公开到 SnapManager for Hyper-V 中，以便应用程序的 VSS 写入程序可以执行自动恢复。

4. 自动恢复卷影副本集

   在创建卷影副本集期间，会有一段时间对备份集中的文件进行活动更改。应用程序的 VSS 写入程序必须更新卷影副本，以确保它们在备份之前处于完全一致的状态。

   > 自动恢复的执行方式取决于应用程序。此阶段不涉及远程 VSS 。

5. 完成并清理卷影副本集

   VSS 客户端会在完成自动恢复后通知 ONTAP 。卷影副本集将设为只读，然后准备好进行备份。使用 SnapManager for Hyper-V 进行备份时， Snapshot 副本中的文件将成为备份；因此，在备份阶段，系统会为包含备份集中共享的每个卷创建 Snapshot 副本。备份完成后，卷影副本集将从 CIFS 服务器中删除。

如何通过 **SMB** 共享在 **Hyper-V** 和 **SQL Server** 中使用 **ODX** 副本卸载

卸载数据传输（ Offloaded Data Transfer ， ODX ）也称为 *copy ofload* ，可在兼容存储设备内部或之间直接传输数据，而无需通过主机计算机传输数据。通过 SMB 安装在应用程序服务器上执行复制操作时， ONTAP ODX 副本卸载功能可为您带来性能优势。

在非 ODX 文件传输中，将从源 CIFS 服务器读取数据，并通过网络传输到客户端计算机。客户端计算机通过网络将数据传输回目标 CIFS 服务器。总之，客户端计算机从源读取数据并将其写入目标。使用 ODX 文件传输时，数据会直接从源复制到目标。

由于 ODX 卸载副本是直接在源存储和目标存储之间执行的，因此具有显著的性能优势。实现的性能优势包括：源和目标之间的复制时间更短，客户端上的资源利用率（ CPU ，内存）更低，网络 I/O 带宽利用率更低。

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
以下使用情形支持使用 ODX 副本和移动：
```

- 卷内

  源文件或 LUN 与目标文件或 LUN 位于同一个卷中。

- 卷间，同一节点，同一 Storage Virtual Machine （ SVM ）

  源文件或 LUN 和目标文件或 LUN 位于同一节点上的不同卷上。数据属于同一个 SVM 。

- 卷间，不同节点，相同 SVM

源文件或 LUN 和目标文件或 LUN 位于不同节点上的不同卷上。数据属于同一个 SVM 。

- SVM 间，同一节点

  源和目标文件或 LUN 位于同一节点上的不同卷上。数据属于不同的 SVM 。

- SVM 间，不同节点

  源和目标文件或 LUN 位于不同节点上的不同卷上。数据属于不同的 SVM 。

Hyper-V 解决方案中 ODX 副本卸载的具体使用情形包括：

- 您可以使用 ODX 副本卸载直通与 Hyper-V 在虚拟硬盘（ VHD ）文件内部或之间复制数据，或者在同一集群中映射的 SMB 共享和连接的 iSCSI LUN 之间复制数据。

  这样，子操作系统中的副本就可以传递到底层存储。

- 创建固定大小的 VHD 时， ODX 用于使用众所周知的置零令牌以零初始化磁盘。
- 如果源存储和目标存储位于同一集群上，则使用 ODX 副本卸载进行虚拟机存储迁移。

> 要利用 Hyper-V ODX 副本卸载直通的使用情形，子操作系统必须支持 ODX ，而子操作系统的磁盘必须是 SCSI 磁盘，并由支持 ODX 的存储（ SMB 或 SAN ）提供支持。子操作系统上的 IDE 磁盘不支持 ODX 直通。

SQL Server 解决方案中 ODX 副本卸载的具体使用情形包括：

- 您可以使用 ODX 副本卸载在映射的 SMB 共享之间或在同一集群中的 SMB 共享和连接的 iSCSI LUN 之间导出和导入 SQL Server 数据库。
- 如果源存储和目标存储位于同一集群上，则 ODX 副本卸载用于数据库导出和导入。

配置要求和注意事项

ONTAP 和许可要求

在 SVM 上创建 SQL Server 或基于 SMB 的 Hyper-V 解决方案以实现无中断运行时，您需要了解某些 ONTAP 和许可要求。

ONTAP 版本要求

- 基于 SMB 的 Hyper-V

  对于在 Windows 2012 或更高版本上运行的 Hyper-V ， ONTAP 支持通过 SMB 共享进行无中断操作。

- 基于 SMB 的 SQL Server

  对于在 Windows 2012 或更高版本上运行的 SQL Server 2012 或更高版本， ONTAP 支持通过 SMB 共享进行无中断操作。

有关通过 SMB 共享实现无中断操作所支持的 ONTAP ， Windows Server 和 SQL Server 版本的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

许可要求

需要以下许可证：

- CIFS
- FlexClone （仅适用于基于 SMB 的 Hyper-V ）

  如果使用远程 VSS 进行备份，则需要此许可证。卷影复制服务使用 FlexClone 为文件创建时间点副本，然后在创建备份时使用这些副本。

  如果您使用的备份方法不使用远程 VSS ，则 FlexClone 许可证是可选的。

FlexClone许可证包含在中 "ONTAP One"。如果您没有ONTAP One、则应这样做 "验证是否已安装所需的许可证"，如有必要， "安装它们"。

网络和数据 **LIF** 要求

在创建 SQL Server 或基于 SMB 的 Hyper-V 配置以实现无中断运行时，您需要了解特定的网络和数据 LIF 要求。

网络协议要求

- 支持 IPv4 和 IPv6 网络。
- 需要 SMB 3.0 或更高版本。

  SMB 3.0 提供了创建持续可用的 SMB 连接所需的功能，以实现无中断运行。

- DNS 服务器必须包含将 CIFS 服务器名称映射到为 Storage Virtual Machine （ SVM ）上的数据 LIF 分配的 IP 地址的条目。

  在访问虚拟机或数据库文件时， Hyper-V 或 SQL Server 应用程序服务器通常会通过多个数据 LIF 建立多个连接。为了正常运行，应用程序服务器必须使用 CIFS 服务器名称进行多个 SMB 连接，而不是与多个唯一 IP 地址建立多个连接。

  见证还需要使用 CIFS 服务器的 DNS 名称，而不是单个 LIF IP 地址。

  从 ONTAP 9.4 开始，您可以通过启用 SMB 多通道来提高基于 SMB 配置的 Hyper-V 和 SQL 服务器的吞吐量和容错能力。为此，您必须在集群和客户端上部署多个 1G ， 10G 或更大的 NIC 。

数据 **LIF** 要求

- 通过 SMB 解决方案托管应用程序服务器的 SVM 必须在集群中的每个节点上至少具有一个可运行的数据 LIF 。

  SVM 数据 LIF 可以故障转移到集群中的其他数据端口，包括当前未托管应用程序服务器访问的数据的节点。此外，由于见证节点始终是应用程序服务器所连接节点的 SFO 配对节点，因此集群中的每个节点都可能是见证节点。

- 不能将数据 LIF 配置为自动还原。

  发生接管或交还事件后，您应手动将数据 LIF 还原到其主端口。

- 所有数据 LIF IP 地址都必须在 DNS 中有一个条目，并且所有条目都必须解析为 CIFS 服务器名称。

  应用程序服务器必须使用 CIFS 服务器名称连接到 SMB 共享。您不能将应用程序服务器配置为使用 LIF IP 地址进行连接。

- 如果 CIFS 服务器名称与 SVM 名称不同，则 DNS 条目必须解析为 CIFS 服务器名称。

基于 **SMB** 的 **Hyper-V** 的 **SMB** 服务器和卷要求

在创建基于 SMB 的 Hyper-V 配置以实现无中断运行时，您需要了解特定的 SMB 服务器和卷要求。

SMB服务器要求

- 必须启用 SMB 3.0 。

  默认情况下，此选项处于启用状态。

- 必须使用有效的 UNIX 用户帐户配置默认 UNIX 用户 CIFS 服务器选项。

  应用程序服务器在创建 SMB 连接时使用计算机帐户。由于所有 SMB 访问都要求 Windows 用户成功映射到 UNIX 用户帐户或默认 UNIX 用户帐户，因此 ONTAP 必须能够将应用程序服务器的计算机帐户映射到默认 UNIX 用户帐户。

- 必须禁用自动节点转介（默认情况下，此功能处于禁用状态）。

  如果要使用自动节点转介来访问 Hyper-V 计算机文件以外的数据，则必须为该数据创建单独的 SVM 。

- SMB 服务器所属的域必须允许 Kerberos 和 NTLM 身份验证。

  ONTAP 不会为远程 VSS 公布 Kerberos 服务；因此，应将域设置为允许 NTLM 。

- 必须启用卷影复制功能。

  默认情况下，此功能处于启用状态。

- 卷影复制服务在创建卷影副本时使用的 Windows 域帐户必须是 SMB 服务器本地 BUILTIN\Administrators 或 BUILTIN\Backup Operators 组的成员。

卷要求：

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

  要使用持续可用的 SMB 连接为应用程序服务器提供 NDOS ，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能通过 SMB 共享将其直接用于 NDOS 。如果您将混合安全模式卷更改为 NTFS 安全模式卷，并打算通过 SMB 共享将其用于 NDOS ，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到包含的所有文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至

另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 要成功执行卷影复制操作，卷上必须有足够的可用空间。

  可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。此要求仅支持具有自动恢复功能的适用场景卷影副本。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

基于 **SMB** 的 **SQL Server** 的 **SMB** 服务器和卷要求

在创建基于 SMB 的 SQL Server 配置以实现无中断运行时，您需要了解特定的 SMB 服务器和卷要求。

SMB服务器要求

- 必须启用 SMB 3.0 。

  默认情况下，此选项处于启用状态。

- 必须使用有效的 UNIX 用户帐户配置默认 UNIX 用户 CIFS 服务器选项。

  应用程序服务器在创建 SMB 连接时使用计算机帐户。由于所有 SMB 访问都要求 Windows 用户成功映射到 UNIX 用户帐户或默认 UNIX 用户帐户，因此 ONTAP 必须能够将应用程序服务器的计算机帐户映射到默认 UNIX 用户帐户。

  此外， SQL Server 还使用域用户作为 SQL Server 服务帐户。服务帐户还必须映射到默认 UNIX 用户。

- 必须禁用自动节点转介（默认情况下，此功能处于禁用状态）。

  如果要使用自动节点转介来访问 SQL Server 数据库文件以外的数据，则必须为该数据创建一个单独的 SVM 。

- 必须为用于在 ONTAP 上安装 SQL Server 的 Windows 用户帐户分配 SeSecurityPrivilege 权限。

  此权限将分配给 SMB 服务器本地 BUILTIN\Administrators 组。

卷要求：

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

  要使用持续可用的 SMB 连接为应用程序服务器提供 NDOS ，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能通过 SMB 共享将其直接用于 NDOS 。如果您将混合安全模式卷更改为 NTFS 安全模式卷，并打算通过 SMB 共享将其用于 NDOS ，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到包含的所有文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 尽管包含数据库文件的卷可以包含接合，但在创建数据库目录结构时， SQL Server 不会跨越接合。
- 要使适用于Microsoft SQL Server的SnapCenter 插件备份操作成功、卷上必须具有足够的可用空间。

SQL Server 数据库文件所在的卷必须足够大，才能容纳数据库目录结构以及驻留在共享中的所有包含的文件。

相关信息

"Microsoft TechNet 库： technet.microsoft.com/en-us/library/"

基于 **SMB** 的 **Hyper-V** 的持续可用共享要求和注意事项

在为支持无中断运行的基于 SMB 的 Hyper-V 配置配置配置持续可用的共享时，您需要了解某些要求和注意事项。

共享要求

- 应用程序服务器使用的共享必须配置为具有持续可用属性集。

  连接到持续可用共享的应用程序服务器会收到永久性句柄，使其能够无中断地重新连接到 SMB 共享，并在发生接管，交还和聚合重新定位等中断事件后回收文件锁定。

- 如果要使用启用了 VSS 的远程备份服务，则不能将 Hyper-V 文件放入包含接合的共享中。

  在自动恢复情形下，如果在遍历共享时遇到接合，则卷影副本创建将失败。在非自动恢复情况下，卷影副本创建不会失败，但接合不会指向任何内容。

- 如果要将启用了 VSS 的远程备份服务与自动恢复结合使用，则不能将 Hyper-V 文件置于包含以下内容的共享中：
  - 符号链接，硬链接或 Widelink
  - 非常规文件

    如果共享中存在指向卷影副本的任何链接或非常规文件，则卷影副本创建将失败。此要求仅支持具有自动恢复功能的适用场景卷影副本。

  - 要成功执行卷影复制操作，卷上必须有足够的可用空间（仅适用于基于 SMB 的 Hyper-V ）。

    可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。此要求仅支持具有自动恢复功能的适用场景卷影副本。

- 不得在应用程序服务器使用的持续可用共享上设置以下共享属性：
  - 主目录
  - 属性缓存
  - BranchCache

注意事项

- 持续可用的共享支持配额。
- 基于 SMB 的 Hyper-V 配置不支持以下功能：
  - 审核
  - fpolicy

- 不会对使用的SMB共享执行病毒扫描 `continuously-availability` 参数设置为 `Yes`。

基于 **SMB** 的 **SQL Server** 的持续可用共享要求和注意事项

在为支持无中断运行的基于 SMB 的 SQL Server 配置配置配置持续可用的共享时，您需要了解某些要求和注意事项。

共享要求

- 用于存储虚拟机文件的卷必须创建为 NTFS 安全模式卷。

  要使用持续可用的 SMB 连接为应用程序服务器提供无中断运行，包含共享的卷必须为 NTFS 卷。此外，它必须始终是 NTFS 卷。您不能将混合安全模式卷或 UNIX 安全模式卷更改为 NTFS 安全模式卷，也不能直接使用该卷通过 SMB 共享执行无中断操作。如果将混合安全模式卷更改为 NTFS 安全模式卷，并打算使用该卷通过 SMB 共享执行无中断操作，则必须手动将 ACL 放置在卷顶部，并将该 ACL 传播到所有包含的文件和文件夹。否则，如果源卷或目标卷最初创建为混合卷或 UNIX 安全模式卷，然后更改为 NTFS 安全模式，则将文件移至另一个卷的虚拟机迁移或数据库文件导出和导入可能会失败。

- 应用程序服务器使用的共享必须配置为具有持续可用属性集。

  连接到持续可用共享的应用程序服务器会收到永久性句柄，使其能够无中断地重新连接到 SMB 共享，并在发生接管，交还和聚合重新定位等中断事件后回收文件锁定。

- 尽管包含数据库文件的卷可以包含接合，但在创建数据库目录结构时， SQL Server 不会跨越接合。
- 要使适用于Microsoft SQL Server的SnapCenter 插件操作成功、卷上必须具有足够的可用空间。

  SQL Server 数据库文件所在的卷必须足够大，才能容纳数据库目录结构以及驻留在共享中的所有包含的文件。

- 不得在应用程序服务器使用的持续可用共享上设置以下共享属性：
  - 主目录
  - 属性缓存
  - BranchCache

分享注意事项

- 持续可用的共享支持配额。
- 基于 SMB 的 SQL Server 配置不支持以下功能：
  - 审核
  - fpolicy
- 不会对使用的SMB共享执行病毒扫描 `continuously-availability` 共享属性集。

基于 **SMB** 的 **Hyper-V** 配置的远程 **VSS** 注意事项

在对基于 SMB 的 Hyper-V 配置使用支持远程 VSS 的备份解决方案时，您需要了解一些注意事项。

常规远程 **VSS** 注意事项

- 每个 Microsoft 应用程序服务器最多可配置 64 个共享。

  如果卷影副本集中的共享超过 64 个，则卷影复制操作将失败。这是 Microsoft 的要求。

- 每个 CIFS 服务器仅允许设置一个活动卷影副本。

  如果正在同一 CIFS 服务器上执行卷影复制操作，则卷影复制操作将失败。这是 Microsoft 的要求。

- 在远程 VSS 创建卷影副本的目录结构中，不允许使用任何接合。
  - 在自动恢复情形下，如果在遍历共享时遇到接合，则卷影副本创建将失败。
  - 在非自动恢复情形下，卷影副本创建不会失败，但接合不会指向任何内容。

仅适用于具有自动恢复功能的卷影副本的远程 **VSS** 注意事项

某些限制仅适用于具有自动恢复功能的卷影副本。

- 创建卷影副本时，最多允许五个子目录的深度。

  这是卷影复制服务创建卷影副本备份集所使用的目录深度。如果包含虚拟机文件的目录嵌套深度超过五个级别，则卷影副本创建将失败。这样可以限制克隆共享时的目录遍历。可以使用 CIFS 服务器选项更改最大目录深度。

- 卷上的可用空间量必须足够。

  可用空间必须至少与卷影副本备份集中包含的共享中的所有文件，目录和子目录所使用的总空间相同。

- 在远程 VSS 创建卷影副本的目录结构中，不允许使用任何链接或非常规文件。

  如果共享中存在指向卷影副本的任何链接或非常规文件，则卷影副本创建将失败。克隆过程不支持这些设置。

- 目录上不允许使用 NFSv4 ACL 。

  虽然卷影复制创建会保留文件上的 NFSv4 ACL ，但目录上的 NFSv4 ACL 会丢失。

- 创建卷影副本集最多允许 60 秒。

  Microsoft 规范最多允许 60 秒创建卷影副本集。如果 VSS 客户端无法在此时间内创建卷影副本集，则卷影复制操作将失败；因此，这会限制卷影副本集中的文件数。备份集中可包含的文件或虚拟机的实际数量各不相同；该数量取决于多种因素，必须根据每个客户环境来确定。

基于 **SMB** 的 **SQL Server** 和 **Hyper-V** 的 **ODX** 副本卸载要求

如果要迁移虚拟机文件或直接将数据库文件从源导出和导入目标存储位置，而无需通过应用程序服务器发送数据，则必须启用 ODX 副本卸载。对于将 ODX 副本卸载与 SQL Server 和基于 SMB 的 Hyper-V 解决方案结合使用，您必须了解一些特定要求。

使用 ODX 副本卸载可显著提高性能。默认情况下，此 CIFS 服务器选项处于启用状态。

- 要使用 ODX 副本卸载，必须启用 SMB 3.0 。
- 源卷必须至少为 1.25 GB 。
- 必须在使用副本卸载的卷上启用重复数据删除。
- 如果使用压缩卷，则压缩类型必须是自适应的，并且仅支持压缩组大小 8K 。

  不支持二级压缩类型

- 要使用 ODX 副本卸载功能在磁盘内部和磁盘之间迁移 Hyper-V 子系统，必须将 Hyper-V 服务器配置为使用 SCSI 磁盘。

  默认情况下，配置 IDE 磁盘，但如果使用 IDE 磁盘创建磁盘，则迁移子系统时 ODX 副本卸载将不起作用。

针对 **SQL Server** 和基于 **SMB** 的 **Hyper-V** 配置的建议

要确保 SQL Server 和基于 SMB 的 Hyper-V 配置稳健且正常运行，您需要熟悉配置解决方案时建议的最佳实践。

一般建议

- 将应用程序服务器文件与常规用户数据分开。

  如果可能，请将整个 Storage Virtual Machine （ SVM ）及其存储专用于应用程序服务器的数据。

- 为了获得最佳性能，请勿在用于存储应用程序服务器数据的 SVM 上启用 SMB 签名。
- 为了获得最佳性能并提高容错能力，请启用 SMB 多通道，以便在一个 SMB 会话中提供 ONTAP 与客户端之间的多个连接。
- 请勿在 Hyper-V 或基于 SMB 的 SQL Server 配置中使用的共享以外的任何共享上创建持续可用的共享。
- 对用于持续可用性的共享禁用更改通知。
- 请勿与聚合重新定位（ Aggregate Relocation ， ARL ）同时执行卷移动，因为 ARL 具有暂停某些操作的阶段。
- 对于基于 SMB 的 Hyper-V 解决方案，请在创建集群模式虚拟机时使用来宾 iSCSI 驱动器。共享 `.VHDX` 在ONTAP SMB共享中、基于SMB的Hyper-V不支持文件。

规划基于 **SMB** 的 **Hyper-V** 或 **SQL Server** 配置

填写卷配置工作表

通过此工作表，您可以轻松地记录为 SQL Server 和基于 SMB 的 Hyper-V 配置创建卷时所需的值。

对于每个卷，必须指定以下信息：

- Storage Virtual Machine （ SVM ）名称

  所有卷的 SVM 名称都相同。

- Volume name
- Aggregate name

  您可以在集群中任何节点上的聚合上创建卷。

- Size
- Junction path

在创建用于存储应用程序服务器数据的卷时，应牢记以下几点：

- 如果根卷没有 NTFS 安全模式，则必须在创建卷时将安全模式指定为 NTFS 。

  默认情况下，卷会继承 SVM 根卷的安全模式。

- 应使用默认卷空间保证配置卷。
- 您可以选择配置自动调整大小空间管理设置。
- 您应设置用于确定Snapshot副本空间预留的选项 `0`。
- 必须禁用应用于卷的 Snapshot 策略。

  如果禁用了 SVM Snapshot 策略，则无需为卷指定 Snapshot 策略。这些卷将继承 SVM 的 Snapshot 策略。如果 SVM 的 Snapshot 策略未禁用，并且配置为创建 Snapshot 副本，则必须在卷级别指定 Snapshot 策略，并且必须禁用该策略。启用了卷影复制服务的备份和 SQL Server 备份可管理 Snapshot 副本的创建和删除。

- 您不能为卷配置负载共享镜像。

应选择要创建应用程序服务器使用的共享的接合路径，以便在共享入口点下方没有接合卷。

例如，如果要将虚拟机文件存储在名为 "`vol1` "， "`vol2` "， "`vol3` " 和 "`vol4` " 的四个卷上，则可以创建示例中所示的命名空间。然后、您可以通过以下路径为应用程序服务器创建共享： `/data1/vol1`， `/data1/vol2`， `/data2/vol3`，和 `/data2/vol4`。

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     data1         true     /data1                 RW_volume
vs1     vol1          true     /data1/vol1            RW_volume
vs1     vol2          true     /data1/vol2            RW_volume
vs1     data2         true     /data2                 RW_volume
vs1     vol3          true     /data2/vol3            RW_volume
vs1     vol4          true     /data2/vol4            RW_volume
```

信息类型	值
_Volume 1 ： 卷名称，聚合，大小，接合路径 _	

信息类型	值
Volume 2：卷名称、聚合、大小、接合路径	
Volume 3：卷名称、聚合、大小、接合路径	
Volume 4：卷名称、聚合、大小、接合路径	
Volume 5：卷名称、聚合、大小、接合路径	
Volume 6：卷名称、聚合、大小、接合路径	
附加卷：卷名称，聚合，大小，接合路径 _	

填写 **SMB** 共享配置工作表

使用此工作表可记录在为 SQL Server 和基于 SMB 的 Hyper-V 配置创建持续可用的 SMB 共享时所需的值。

有关 **SMB** 共享属性和配置设置的信息

对于每个共享，必须指定以下信息：

- Storage Virtual Machine （ SVM ）名称

  所有共享的 SVM 名称都相同

- Share name
- 路径
- 共享属性

  您必须配置以下两个共享属性：

  - `oplocks`
  - `continuously-available`

不能设置以下共享属性：

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - 必须禁用符号链接(的值 `-symlink-properties` 参数必须为空[""])。

有关共享路径的信息

如果您使用远程 VSS 备份 Hyper-V 文件，则在从 Hyper-V 服务器到存储虚拟机文件的存储位置建立 SMB 连接时，选择要使用的共享路径非常重要。虽然可以在命名空间中的任意位置创建共享，但 Hyper-V 服务器使用的共享路径不应包含接合卷。不能对包含接合点的共享路径执行卷影复制操作。

在创建数据库目录结构时， SQL Server 无法跨越接合。您不应为包含接合点的 SQL Server 创建共享路径。

例如、在显示的命名空间中、如果要将虚拟机文件或数据库文件存储在卷"`vol1`"、“vol2”、"`vol3`"和"`vol4`"上、则应在以下路径为应用程序服务器创建共享： `/data1/vol1`， `/data1/vol2`， `/data2/vol3`，和 `/data2/vol4`。

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- -------------------    -----------
vs1     data1         true     /data1                 RW_volume
vs1     vol1          true     /data1/vol1            RW_volume
vs1     vol2          true     /data1/vol2            RW_volume
vs1     data2         true     /data2                 RW_volume
vs1     vol3          true     /data2/vol3            RW_volume
vs1     vol4          true     /data2/vol4            RW_volume
```

> 但您可以在上创建共享 `/data1` 和 `/data2` 用于管理管理的路径、则不能将应用程序服务器配置为使用这些共享来存储数据。

规划工作表

信息类型	值
_Volume 1： SMB 共享名称和路径 _	
Volume 2：*SMB*共享名称和路径	
Volume 3：*SMB*共享名称和路径	
Volume 4：*SMB*共享名称和路径	
Volume 5：*SMB*共享名称和路径	
Volume 6：*SMB*共享名称和路径	
Volume 7：*SMB*共享名称和路径	
_Additional volumes： SMB 共享名称和路径 _	

创建 ONTAP 配置，以便通过 SMB 使用 Hyper-V 和 SQL Server 实现无中断运行

使用基于 SMB 的 Hyper-V 和 SQL Server 概述创建 ONTAP 配置以实现无中断运行

您必须执行多个 ONTAP 配置步骤来准备通过 SMB 实现无中断操作的 Hyper-V 和 SQL Server 安装。

在通过 SMB 为 Hyper-V 和 SQL Server 创建无中断操作的 ONTAP 配置之前，必须完成以下任务：

- 必须在集群上设置时间服务。
- 必须为 SVM 设置网络连接。
- 必须创建 SVM 。
- 必须在 SVM 上配置数据 LIF 接口。
- 必须在 SVM 上配置 DNS 。
- 必须为 SVM 设置所需的名称服务。
- 必须创建SMB服务器。

相关信息

规划基于 SMB 的 Hyper-V 或 SQL Server 配置

配置要求和注意事项

验证是否允许 Kerberos 和 NTLMv2 身份验证（基于 SMB 共享的 Hyper-V ）

基于 SMB 的 Hyper-V 无中断运行要求数据 SVM 上的 CIFS 服务器和 Hyper-V 服务器同时允许 Kerberos 和 NTLMv2 身份验证。您必须验证 CIFS 服务器和 Hyper-V 服务器上用于控制允许使用的身份验证方法的设置。

关于此任务

建立持续可用的共享连接时，需要进行 Kerberos 身份验证。远程 VSS 进程的一部分使用 NTLMv2 身份验证。因此，基于 SMB 的 Hyper-V 配置必须支持使用这两种身份验证方法的连接。

必须将以下设置配置为允许 Kerberos 和 NTLMv2 身份验证：

- 必须在 Storage Virtual Machine （ SVM ）上禁用 SMB 的导出策略。

SVM 上始终启用 Kerberos 和 NTLMv2 身份验证，但导出策略可用于根据身份验证方法限制访问。

SMB 的导出策略是可选的，默认情况下处于禁用状态。如果禁用了导出策略，则默认情况下， CIFS 服务器上允许使用 Kerberos 和 NTLMv2 身份验证。

- CIFS 服务器和 Hyper-V 服务器所属的域必须同时允许 Kerberos 和 NTLMv2 身份验证。

默认情况下， Active Directory 域启用 Kerberos 身份验证。但是，可以使用安全策略设置或组策略禁止 NTLMv2 身份验证。

步骤

1. 执行以下操作，验证是否已在 SVM 上禁用导出策略：
   a. 将权限级别设置为高级：

      set -privilege advanced

   b. 验证是否已 `-is-exportpolicy-enabled` CIFS服务器选项设置为 `false`：

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. 返回到管理权限级别：

      set -privilege admin

2. 如果 SMB 的导出策略未禁用，请禁用它们：

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. 验证域中是否允许 NTLMv2 和 Kerberos 身份验证。

   有关确定域中允许使用的身份验证方法的信息，请参见 Microsoft TechNet 库。

4. 如果域不允许进行 NTMLv2 身份验证，请使用 Microsoft 文档中所述的方法之一启用 NTLMv2 身份验证。

示例

以下命令验证是否已在 SVM vs1 上禁用 SMB 的导出策略：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

验证域帐户是否映射到默认 **UNIX** 用户

Hyper-V 和 SQL Server 使用域帐户创建与持续可用共享的 SMB 连接。要成功创建连接，计算机帐户必须成功映射到 UNIX 用户。为此，最方便的方法是将计算机帐户映射到默认 UNIX 用户。

关于此任务

Hyper-V 和 SQL Server 使用域计算机帐户创建 SMB 连接。此外， SQL Server 还使用域用户帐户作为服务帐户，该帐户还会建立 SMB 连接。

创建Storage Virtual Machine (SVM)时、ONTAP会自动创建名为"`pcuser`"(UID为 `65534`)和名为"`pcuser`"的组(GID为 `65534`)、并将默认用户添加到"`pcuser`"组。如果要在将集群升级到 Data ONTAP 8.2 之前存在的 SVM 上配置基于 SMB 解决方案的 Hyper-V ，则默认用户和组可能不存在。否则，必须先创建它们，然后再配置 CIFS 服务器的默认 UNIX 用户。

步骤

1. 确定是否存在默认 UNIX 用户：

   vserver cifs options show -vserver *vserver_name*

2. 如果未设置默认用户选项，请确定是否存在可指定为默认 UNIX 用户的 UNIX 用户：

   vserver services unix-user show -vserver *vserver_name*

3. 如果未设置默认用户选项，并且没有可指定为默认 UNIX 用户的 UNIX 用户，请创建默认 UNIX 用户和默认组，然后将默认用户添加到组中。

   通常、系统会为默认用户提供用户名"`pcuser`"、并且必须为其分配UID `65534`。默认组通常被指定为组名称"`pcuser` "。分配给组的GID必须为 `65534`。

   a. 创建默认组：

      vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534

   b. 创建默认用户并将默认用户添加到默认组：

      vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534

   c. 验证是否已正确配置默认用户和默认组：

      vserver services unix-user show -vserver *vserver_name*

      vserver services unix-group show -vserver *vserver_name* -members

4. 如果未配置 CIFS 服务器的默认用户，请执行以下操作：

   a. 配置默认用户：

      vserver cifs options modify -vserver *vserver_name -default-unix-user pcuser*

   b. 验证是否已正确配置默认 UNIX 用户：

      vserver cifs options show -vserver *vserver_name*

5. 要验证应用程序服务器的计算机帐户是否正确映射到默认用户、请将驱动器映射到驻留在SVM上的共享、然

后使用确认Windows用户到UNIX用户的映射 `vserver cifs session show` 命令：

有关使用此命令的详细信息，请参见手册页。

示例

以下命令确定未设置 CIFS 服务器的默认用户，但确定 "`pcuser` " 用户和 "`pcuser` " 组存在。在 SVM vs1 上，将 "`pcuser` " 用户分配为 CIFS 服务器的默认用户。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

验证 **SVM** 根卷的安全模式是否设置为 **NTFS**

要确保通过 SMB 成功执行 Hyper-V 和 SQL Server 无中断操作，必须使用 NTFS 安全模式创建卷。由于根卷的安全模式默认应用于在 Storage Virtual Machine （SVM）上创建的卷，因此根卷的安全模式应设置为 NTFS 。

关于此任务

- 您可以在创建 SVM 时指定根卷的安全模式。
- 如果创建SVM时未将根卷设置为NTFS安全模式、则可以稍后使用更改安全模式 `volume modify` 命令：

步骤

1. 确定 SVM 根卷的当前安全模式：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. 如果根卷不是 NTFS 安全模式卷，请将安全模式更改为 NTFS ：

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. 验证 SVM 根卷是否设置为 NTFS 安全模式：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

示例

以下命令验证 SVM vs1 上的根卷安全模式是否为 NTFS ：

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

验证是否已配置所需的 **CIFS** 服务器选项

您必须验证是否已根据 Hyper-V 和 SQL Server 通过 SMB 无中断运行的要求启用和配置所需的 CIFS 服务器选项。

关于此任务

- 必须启用 SMB 2.x 和 SMB 3.0 。
- 要使用性能增强型副本卸载，必须启用 ODX 副本卸载。
- 如果基于 SMB 的 Hyper-V 解决方案使用启用了 VSS 的远程备份服务（仅限 Hyper-V ），则必须启用 VSS 卷影复制服务。

步骤

1. 验证是否已在 Storage Virtual Machine （ SVM ）上启用所需的 CIFS 服务器选项：
   a. 将权限级别设置为高级：

      `set -privilege advanced`

   b. 输入以下命令：

      `vserver cifs options show -vserver vserver_name`

      以下选项应设置为 `true`：

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (仅限Hyper-V)
2. 如果任何选项未设置为 `true`，执行以下操作：
   a. 将其设置为 `true` 使用 `vserver cifs options modify` 命令：
   b. 验证这些选项是否设置为 `true` 使用 `vserver cifs options show` 命令：

3. 返回到管理权限级别：

   set -privilege admin

示例

以下命令验证是否已在 SVM vs1 上启用基于 SMB 的 Hyper-V 配置所需的选项。在此示例中，必须启用 ODX 副本卸载才能满足选项要求。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

为 **SMB** 多通道配置性能和冗余

从 ONTAP 9.4 开始，您可以配置 SMB 多通道，以便在单个 SMB 会话中提供 ONTAP 与客户端之间的多个连接。这样做可以提高 Hyper-V 和 SQL Server 在 SMB 配置上的吞吐量和容错能力。

您需要的内容

只有在客户端以 SMB 3.0 或更高版本进行协商时，才能使用 SMB 多通道功能。默认情况下， ONTAP SMB 服务器上会启用 SMB 3.0 及更高版本。

关于此任务

如果在 ONTAP 集群上确定了正确的配置，则 SMB 客户端会自动检测并使用多个网络连接。

SMB 会话中同时连接的数量取决于您部署的 NIC：

- 客户端和 ONTAP 集群上的 * 1G NIC *

客户端为每个 NIC 建立一个连接，并将会话绑定到所有连接。

- 客户端和 ONTAP 集群上的 * 10 G 及更大容量 NIC *

  客户端为每个 NIC 最多建立四个连接，并将会话绑定到所有连接。客户端可以在多个 10G 及更大容量的 NIC 上建立连接。

您还可以修改以下参数（高级权限）：

- **`-max-connections-per-session`**

  每个多通道会话允许的最大连接数。默认值为 32 个连接。

  如果要启用比默认连接更多的连接，则必须对客户端配置进行类似的调整，该配置的默认连接数也为 32 个。

- **`-max-lifs-per-session`**

  每个多通道会话公布的最大网络接口数。默认值为 256 个网络接口。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 在 SMB 服务器上启用 SMB 多通道：

   ```
   vserver cifs options modify -vserver vserver_name -is-multichannel-enabled
   true
   ```

3. 验证 ONTAP 是否正在报告 SMB 多通道会话：

   ```
   vserver cifs session options show
   ```

4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

以下示例显示了有关所有 SMB 会话的信息，其中显示了单个会话的多个连接：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

以下示例显示了有关 session-id 为 1 的 SMB 会话的详细信息：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

创建 **NTFS** 数据卷

您必须先在 Storage Virtual Machine （SVM）上创建 NTFS 数据卷，然后才能配置持续可用的共享，以便通过 SMB 应用程序服务器与 Hyper-V 或 SQL Server 结合使用。使用

卷配置工作表创建数据卷。

关于此任务

您可以使用可选参数自定义数据卷。有关自定义卷的详细信息，请参见 xref:./smb-hyper-v-sql/"逻辑存储管理"。

创建数据卷时，不应在包含以下内容的卷中创建接合点：

- ONTAP 为其创建卷影副本的 Hyper-V 文件
- 使用 SQL Server 备份的 SQL Server 数据库文件

> 如果无意中创建了使用混合安全模式或 UNIX 安全模式的卷，则无法将此卷更改为 NTFS 安全模式卷，然后直接使用此卷创建持续可用的共享以实现无中断运行。除非将配置中使用的卷创建为 NTFS 安全模式卷，否则基于 SMB 的 Hyper-V 和 SQL Server 的无中断操作无法正常运行。您必须删除卷并使用 NTFS 安全模式重新创建卷， 或者，您也可以在 Windows 主机上映射卷，并应用卷顶部的 ACL ，然后将 ACL 传播到卷中的所有文件和文件夹。

步骤

1. 输入相应的命令以创建数据卷：

如果要在根卷安全模式为 ... 的 **SVM** 中创建卷	输入命令 ...
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
非 NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]-security-style ntfs -junction-path path**

2. 验证卷配置是否正确：

   volume show -vserver *vserver_name* -volume *volume_name*

创建持续可用的 **SMB** 共享

创建数据卷后，您可以创建持续可用的共享，应用程序服务器可使用这些共享访问 Hyper-V 虚拟机，配置文件和 SQL Server 数据库文件。创建 SMB 共享时，应使用共享配置工作表。

步骤

1. 显示有关现有数据卷及其接合路径的信息：

   volume show -vserver *vserver_name* -junction

2. 创建持续可用的 SMB 共享：

vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

- 您可以选择向共享配置添加注释。
- 默认情况下、脱机文件共享属性在共享上配置、并设置为 `manual`。
- ONTAP会使用的Windows默认共享权限创建共享 `Everyone` / `Full Control`。

3. 对共享配置工作表中的所有共享重复上述步骤。
4. 使用验证您的配置是否正确 `vserver cifs share show` 命令：
5. 通过将驱动器映射到每个共享并使用 * Windows 属性 * 窗口配置文件权限，在持续可用的共享上配置 NTFS 文件权限。

示例

以下命令会在 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上创建名为 `data2` 的持续可用共享。通过设置禁用符号链接 `-symlink` 参数设置为 `""`：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

将 **SeSecurityPrivilege** 权限添加到用户帐户（对于 **SMB** 共享的 **SQL Server**）

必须为用于安装 SQL 服务器的域用户帐户分配 `SeSecurityPrivilege` 特权，才能在 CIFS 服务器上执行某些操作，这些操作需要默认情况下未分配给域用户的权限。

您需要的内容

用于安装 SQL Server 的域帐户必须已存在。

关于此任务

在将权限添加到 SQL Server 安装程序的帐户时， ONTAP 可能会通过联系域控制器来验证此帐户。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 添加 " `SeSecurityPrivilege` " 权限：

vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

的值 `-user-or-group-name` 参数是用于安装SQL Server的域用户帐户的名称。

2. 验证是否已将此权限应用于此帐户：

vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

示例

以下命令会将 " `SeSecurityPrivilege` " 权限添加到 Storage Virtual Machine （ SVM ） vs1 的示例域中的 SQL Server 安装程序帐户：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

配置 **VSS** 卷影复制目录深度（对于基于 **SMB** 共享的 **Hyper-V** ）

您也可以在 SMB 共享中配置用于创建卷影副本的目录的最大深度。如果要手动控制 ONTAP 应在其上创建卷影副本的子目录的最大级别，此参数非常有用。

您需要的内容

必须启用 VSS 卷影复制功能。

关于此任务

默认情况下，最多为五个子目录创建卷影副本。如果此值设置为 `0`，ONTAP将为所有子目录创建卷影副本。

> 尽管您可以指定卷影副本集目录深度包含五个以上的子目录或所有子目录，但 Microsoft 要求必须在 60 秒内完成卷影副本集创建。如果无法在此时间内完成卷影副本集创建，则会失败。您选择的卷影复制目录深度不能使创建时间发生原因超过时间限制。

步骤

1. 将权限级别设置为高级：

set -privilege advanced

2. 将 VSS 卷影复制目录深度设置为所需级别：

vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. 返回到管理权限级别：

```
set -privilege admin
```

通过 SMB 配置管理 Hyper-V 和 SQL Server

配置现有共享以实现持续可用性

您可以修改现有共享，使其成为持续可用的共享， Hyper-V 和 SQL Server 应用程序服务器可使用这些共享无中断地访问 Hyper-V 虚拟机和配置文件以及 SQL Server 数据库文件。

关于此任务

如果现有共享具有以下特征，则不能使用该共享作为持续可用的共享，以便通过 SMB 与应用程序服务器进行无中断操作：

- 如果 `homedirectory` 共享属性已在该共享上设置
- 如果共享包含已启用的符号链接或 Widelink
- 如果共享包含位于共享根目录下的接合卷

您必须验证以下两个共享参数是否设置正确：

- 。 `-offline-files` 参数设置为任一 `manual` (默认值)或 `none`。
- 必须禁用符号链接。

必须配置以下共享属性：

- `continuously-available`
- `oplocks`

不得设置以下共享属性。如果它们位于当前共享属性列表中，则需要从持续可用的共享中删除它们：

- `attributecache`
- `branchcache`

步骤

1. 显示当前共享参数设置和当前已配置共享属性列表：

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. 如有必要、请使用修改共享参数以禁用符号链接、并将脱机文件设置为手动 `vserver cifs share properties modify` 命令：

   您可以通过设置的值来禁用符号链接 `-symlink` 参数设置为 `""`。

- 您可以通过设置的值来禁用符号链接 `-symlink` 参数设置为 `""`。
- 您可以设置 `-offline-files` 参数到正确的设置 `manual`。

3. 添加 `continuously-available` 共享属性、如果需要、还包括 `oplocks` 共享属性：

   vserver cifs share properties add -vserver *vserver_name* -share-name *share_name* -share-properties continuously-available[,oplock]

   如果 `oplocks` 尚未设置共享属性、必须将其与一起添加 `continuously-available` 共享属性。

4. 删除持续可用的共享不支持的任何共享属性：

   vserver cifs share properties remove -vserver *vserver_name* -share-name *share_name* -share-properties properties[,…]

   您可以通过使用逗号分隔列表指定共享属性来删除一个或多个共享属性。

5. 验证是否已 `-symlink` 和 `-offline-files` 参数设置正确：

   vserver cifs share show -vserver *vserver_name* -share-name *share_name* -fields symlink-properties,offline-files

6. 验证已配置的共享属性列表是否正确：

   vserver cifs shares properties show -vserver *vserver_name* -share-name share_name

示例

以下示例说明如何在 Storage Virtual Machine （ SVM ） vs1 上为 NDOS 配置一个名为 `share1` 的现有共享，并使用 SMB 上的应用程序服务器：

- 通过设置在共享上禁用符号链接 `-symlink` 将参数设置为""。
- 。 `-offline-file` 参数已修改并设置为 `manual`。
- 。 `continuously-available` 共享属性将添加到共享中。
- 。 `oplocks` 共享属性已在共享属性列表中、因此无需添加。
- 。 `attributecache` 共享属性将从共享中删除。
- 。 `browsable` 对于在SMB上使用应用程序服务器的NDO中使用的持续可用共享、共享属性是可选的、并保留为共享属性之一。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

为基于 **SMB** 的 **Hyper-V** 备份启用或禁用 **VSS** 卷影副本

如果使用 VSS 感知型备份应用程序备份存储在 SMB 共享上的 Hyper-V 虚拟机文件，则必须启用 VSS 卷影复制。如果您不使用 VSS 感知型备份应用程序，则可以禁用 VSS 卷影复制。默认情况下，启用 VSS 卷影复制。

关于此任务

您可以随时启用或禁用 VSS 卷影副本。

步骤

1. 将权限级别设置为高级：

   `set -privilege advanced`

2. 执行以下操作之一：

VSS 卷影副本的目标位置	输入命令 **...**
enabled	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true`**
已禁用	**`vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false`**

3. 返回到管理权限级别：

   `set -privilege admin`

示例

以下命令可在 SVM vs1 上启用 VSS 卷影副本：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

使用统计信息通过 **SMB** 监控 **Hyper-V** 和 **SQL Server** 活动

确定可用的统计信息对象和计数器

在获取有关 CIFS ， SMB ，审核和 BranchCache 哈希统计信息以及监控性能的信息之前

，您必须了解哪些对象和计数器可用于获取数据。

步骤

1. 将权限级别设置为高级：

   `set -privilege advanced`

2. 执行以下操作之一：

要确定的内容	输入 ...
哪些对象可用	**`statistics catalog object show`**
可用的特定对象	**`statistics catalog object show object`** ***`object_name`***
哪些计数器可用	**`statistics catalog counter show object`** ***`object_name`***

   有关哪些对象和计数器可用的详细信息，请参见手册页。

3. 返回到管理权限级别：

   `set -privilege admin`

示例

以下命令显示与集群中的 CIFS 和 SMB 访问相关的选定统计信息对象的说明，如高级权限级别所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

以下命令显示有关的某些计数器的信息 `cifs` 对象、如高级权限级别所示：

> 此示例不会显示的所有可用计数器 `cifs` 对象；输出被截断。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ---------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                      2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

显示 **SMB** 统计信息

您可以显示各种 SMB 统计信息来监控性能和诊断问题。

步骤

1. 使用 `statistics start` 和可选 `statistics stop` 用于收集数据样本的命令。
2. 执行以下操作之一：

要显示统计信息的对象	输入以下命令 ...
SMB 的所有版本	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x 和 SMB 3.0	**`statistics show -object smb2`**
节点的SMB子系统	**`statistics show -object nblade_cifs`**

详细了解 `statistics` 命令：

- "statistics show"
- "统计信息启动"
- "统计信息停止"

验证此配置是否能够无中断运行

使用运行状况监控来确定无中断运行状态是否正常

运行状况监控可提供有关整个集群中的系统运行状况的信息。运行状况监控器可通过 SMB 监控 Hyper-V 和 SQL Server 配置，以确保应用程序服务器无中断运行（ NDO ）。如果状态为 degraded ，则可以查看有关问题的详细信息，包括可能的发生原因和建议的恢复操作。

有多个运行状况监控器。ONTAP 可监控各个运行状况监控器的整体系统运行状况和运行状况。节点连接运行状况监控器包含 CIFS-NDO 子系统。监控器具有一组运行状况策略，可在某些物理条件可能导致中断时触发警报，如果存在中断情况，则会生成警报并提供有关更正操作的信息。对于基于 SMB 的 NDO 配置，将针对以下两种情况生成警报：

警报 **ID**	**severity**	条件
`HaNotReadyCifsNdo_Alert`	major	节点上聚合中某个卷托管的一个或多个文件已通过持续可用的 SMB 共享打开，并承诺在发生故障时会持久存在；但是，与配对节点的 HA 关系未配置或运行状况不佳。

警报 ID	severity	条件
NoStandbyLifCifsNdo_Alert	次要	Storage Virtual Machine （SVM）正在通过节点主动通过 SMB 提供数据，并且在持续可用的共享上持久打开了 SMB 文件；但是，其配对节点不会公开 SVM 的任何活动数据 LIF 。

使用系统运行状况监控功能显示无中断运行状态

您可以使用 `system health` 用于显示有关集群的整体系统运行状况和CI-NDo子系统运行状况的信息、响应警报、配置未来警报以及显示有关如何配置运行状况监控的信息的命令。

步骤

1. 通过执行相应的操作来监控运行状况：

要显示的内容	输入命令 ...
系统的运行状况，反映单个运行状况监控器的整体状态	**`system health status show`**
有关 CIFS-NDO 子系统运行状况的信息	**`system health subsystem show -subsystem CIFS-NDO -instance`**

2. 显示有关如何通过执行相应操作配置 CIFS-NDO 警报监控的信息：

要显示的信息	输入命令 ...
CIFS-NDO 子系统运行状况监控器的配置和状态，例如受监控节点，初始化状态和状态	**`system health config show -subsystem CIFS-NDO`**
CIFS-NDO 警报，运行状况监控器可能会生成此警报	**`system health alert definition show -subsystem CIFS-NDO`**
CIFS-NDO 运行状况监控策略，用于确定何时发出警报	**`system health policy definition show -monitor node-connect`**

> 使用 `-instance` 用于显示详细信息的参数。

示例

以下输出显示了有关集群和 CIFS-NDO 子系统的整体运行状况的信息：

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

以下输出显示了有关 CIFS-NDO 子系统运行状况监控器的配置和状态的详细信息：

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

验证持续可用的 **SMB** 共享配置

要支持无中断运行，必须将 Hyper-V 和 SQL Server SMB 共享配置为持续可用的共享。此外，您还必须检查某些其他共享设置。如果发生计划内或计划外中断事件，您应验证共享是否已正确配置，以便为应用程序服务器提供无缝无中断运行。

关于此任务

您必须验证以下两个共享参数是否设置正确：

- 。 `-offline-files` 参数设置为任一 `manual` (默认值)或 `none`。
- 必须禁用符号链接。

要实现正确的无中断运行，必须设置以下共享属性：

- `continuously-available`
- `oplocks`

不能设置以下共享属性：

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

步骤

1. 验证脱机文件是否设置为 `manual` 或 `disabled` 并禁用符号链接：

   `vserver cifs shares show -vserver` *`vserver_name`*

2. 验证 SMB 共享是否已配置为持续可用性：

   `vserver cifs shares properties show -vserver` *`vserver_name`*

示例

以下示例显示了 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上名为 `share1` 的共享的共享设置。脱机文件设置为 `manual` 和符号链接已禁用(在中使用连字符指定) `Symlink Properties` 字段输出)：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

以下示例显示了 SVM vs1 上名为 `share1` 的共享的共享属性：

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

验证 **LIF** 状态

即使您将采用 Hyper-V 和基于 SMB 的 SQL Server 配置的 Storage Virtual Machine （SVM）配置为在集群中的每个节点上都具有 LIF ，在日常操作期间，某些 LIF 也可能会移至另一节点上的端口。您必须验证 LIF 状态并采取任何必要的更正操作。

关于此任务

要提供无缝，无中断的操作支持，集群中的每个节点必须至少为 SVM 配置一个 LIF ，并且所有 LIF 都必须与主端口关联。如果某些已配置的 LIF 当前未与其主端口关联，则必须修复任何端口问题，然后将 LIF 还原到其主端口。

步骤

1. 显示有关为 SVM 配置的 LIF 的信息：

   network interface show -vserver *vserver_name*

   在此示例中， "`lif1` " 不位于主端口上。

   network interface show -vserver vs1

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2      e0d
   false
               lif2         up/up    10.0.0.129/24    node2      e0d
   true
   ```

2. 如果某些 LIF 不在其主端口上，请执行以下步骤：

   a. 对于每个 LIF ，确定 LIF 的主端口是什么：

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

      network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. 对于每个 LIF ，确定 LIF 的主端口是否已启动：

network port show -node *node_name* -port *port* -fields port,link

`network port show -node node1 -port e0d -fields port,link`

```
node       port link
---------- ---- ----
node1      e0d  up
```

+
在此示例中、"`if1`"应迁移回其主端口、 `node1:e0d`。

3. 如果应与这些IF关联的任何主端口网络接口不在中 `up` 请解决此问题、使这些接口正常运行。
4. 如果需要，请将 LIF 还原到其主端口：

network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

5. 验证集群中的每个节点是否都具有适用于 SVM 的活动 LIF ：

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

确定 **SMB** 会话是否持续可用

您可以显示有关已建立的 SMB 会话的信息，包括 SMB 连接和会话 ID 以及使用会话的工作站的 IP 地址。您可以显示有关会话的 SMB 协议版本和持续可用保护级别的信息，这有助于确定会话是否支持无中断操作。

关于此任务

您可以摘要形式显示 SVM 上所有会话的信息。但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息：

- 您可以使用可选 `-fields` 用于显示有关所选字段的输出的参数。

  您可以输入 `-fields ?` 以确定您可以使用哪些字段。

- 您可以使用 `-instance` 用于显示有关已建立SMB会话的详细信息的参数。
- 您可以使用 `-fields` 参数或 `-instance` 参数单独使用或与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

要显示 **SMB** 会话信息的项	输入以下命令 **...**
SVM 上的所有会话的摘要形式	**`vserver cifs session show -vserver vserver_name`**
指定的连接 ID	**`vserver cifs session show -vserver vserver_name -connection-id integer`**
指定的工作站 IP 地址	**`vserver cifs session show -vserver vserver_name -address workstation_IP_address`**
指定的 LIF IP 地址	**`vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address`**
在指定节点上	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	指定的 Windows 用户

要显示 **SMB** 会话信息的项	输入以下命令 **...**
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* 的格式 `user_name` 为 `[domain]\user`。	使用指定的身份验证机制
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism 的值 `-auth -mechanism` 可以是以下选项之一： • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	使用指定的协议版本

要显示 **SMB** 会话信息的项	输入以下命令 **...**
`vserver cifs session show -vserver vserver_name -protocol-version protocol_version` 的值 `-protocol -version` 可以是以下选项之一： • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` 持续可用的保护和 SMB 多通道仅适用于 SMB 3.0 及更高版本的会话。要查看其在所有符合条件的会话中的状态、应指定此参数并将值设置为 `SMB3` 或更高版本。	具有指定级别的持续可用保护

要显示 **SMB** 会话信息的项	输入以下命令 **...**
`vserver cifs session show -vserver` *`vserver_name`* `-continuously-available` *`continuously_available_protection_level`* 的值 `-continuously-available` 可以是以下选项之一： • `No` • `Yes` • `Partial` 持续可用状态为 `Partial`，这意味着会话至少包含一个打开的持续可用文件，但会话中的某些文件未使用持续可用保护打开。您可以使用 `vserver cifs sessions file show` 命令、用于确定已建立会话中哪些文件未在持续可用的保护下打开。	具有指定的 SMB 签名会话状态

示例

以下命令显示 SVM vs1 上从 IP 地址为 10.1.1.1 的工作站建立的会话的会话信息：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

以下命令显示 SVM vs1 上具有持续可用保护的会话的详细会话信息。此连接是使用域帐户建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
               Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

以下命令显示 SVM vs1 上使用 SMB 3.0 和 SMB 多通道的会话的会话信息。在此示例中，用户使用 LIF IP 地址从支持 SMB 3.0 的客户端连接到此共享；因此，身份验证机制默认为 NTLMv2 。必须使用 Kerberos 身份验证进行连接，以获得持续可用的保护。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

显示有关打开的 **SMB** 文件的信息

您可以显示有关打开的 SMB 文件的信息，包括 SMB 连接和会话 ID ，托管卷，共享名称和共享路径。您还可以显示有关文件的持续可用保护级别的信息，这有助于确定打开的文件是否处于支持无中断操作的状态。

关于此任务

您可以显示有关已建立的 SMB 会话上打开的文件的信息。如果需要确定 SMB 会话中特定文件的 SMB 会话信息，则显示的信息非常有用。

例如、如果您有一个SMB会话、其中一些打开的文件已打开且具有持续可用的保护、而另一些文件未打开且具有持续可用的保护(的值 `-continuously-available` 字段输入 `vserver cifs session show` 命令输出为 `Partial`)、则可以使用此命令确定哪些文件不持续可用。

您可以使用以摘要形式显示Storage Virtual Machine (SVM)上已建立的SMB会话上的所有打开文件的信息 `vserver cifs session file show` 命令、而不带任何可选参数。

但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息。如果您只想查看一小部分打开文件的信息，这将非常有用。

- 您可以使用可选 `-fields` 用于显示所选字段的输出的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

- 您可以使用 `-instance` 用于显示有关打开的SMB文件的详细信息的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
以摘要形式显示在 SVM 上	**`vserver cifs session file show -vserver vserver_name`**
在指定节点上	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	指定的文件 ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定的 SMB 连接 ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定的 SMB 会话 ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的托管聚合上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定卷上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定的 SMB 共享上
`vserver cifs session file show -vserver vserver_name -share share_name`	指定的 SMB 路径上
`vserver cifs session file show -vserver vserver_name -path path`	具有指定级别的持续可用保护

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
`vserver cifs session file show -vserver vserver_name -continuously -available continuously_available_status` 的值 `-continuously-available` 可以是以下选项之一： • `No` • `Yes` 持续可用状态为 `No`，这意味着这些打开的文件无法从接管和恢复中无系统地恢复。它们也无法从高可用性关系中的合作伙伴之间的常规聚合重新定位中恢复。	具有指定的重新连接状态

您可以使用其他可选参数来细化输出结果。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上打开的文件的信息：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

以下示例显示了有关 SVM vs1 上文件 ID 82 的已打开 SMB 文件的详细信息：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```