管理 SMB 服务器

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/smb-admin/modify-servers-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

目录

管理 SMB 服务器 1
修改ONTAP SMB服务器 1
使用选项自定义SMB服务器 2
可用的ONTAP SMB服务器选项 2
配置ONTAP SMB服务器选项 6
配置向ONTAP SMB用户授予UNIX组权限 6
为匿名用户配置ONTAP SMB访问限制 7
管理如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性 7
管理 SMB 服务器安全设置 9
了解如何处理ONTAP SMB客户端身份验证 10
了解ONTAP SVM灾难恢复配置的SMB服务器安全设置 10
显示有关ONTAP SMB服务器安全设置的信息 10
为本地SMB用户配置ONTAP密码复杂度 12
修改ONTAP SMB服务器Kerberos安全设置 13
设置ONTAP SMB服务器最低身份验证安全级别 15
使用AES加密为基于Kerberos的通信配置强大的ONTAP SMB安全性 15
为基于ONTAP SMB Kerberos的通信配置AES加密 16
使用 SMB 签名增强网络安全性 19
在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密 29
安全 LDAP 会话通信 37
配置ONTAP SMB多通道以实现性能和冗余 39
在 SMB 服务器上配置默认 Windows 用户到 UNIX 用户映射 42
配置默认ONTAP SMB UNIX用户 42
配置子系统ONTAP SMB UNIX用户 43
将管理员组映射到ONTAP SMB根 44
显示有关通过ONTAP SMB会话连接的用户类型的信息 45
用于限制Windows客户端资源过度消耗的ONTAP命令选项 46
使用传统机会锁和租用机会锁提高客户端性能 47
了解如何使用传统机会锁和租用机会锁提高ONTAP SMB客户端性能 47
了解使用oplock时编写ONTAP SMB缓存数据丢失注意事项 47
创建ONTAP SMB共享时启用或禁用操作锁定 47
用于在SMB卷和qtrees上启用或禁用操作锁定的ONTAP命令 48
在现有ONTAP SMB共享上启用或禁用操作锁定 49
监控ONTAP SMB操作锁定状态 51
将组策略对象应用于 SMB 服务器 53
了解如何将组策略对象应用于ONTAP SMB服务器 53
了解支持的ONTAP SMB GPO 54
GPO的ONTAP SMB服务器要求 59
在ONTAP SMB服务器上启用或禁用GPO支持 59

如何在SMB服务器上更新GPO 60
手动更新ONTAP SMB服务器上的GPO设置 61
显示有关ONTAP SMB GPO配置的信息 61
显示有关ONTAP SMB受限组GPO的信息 65
显示有关ONTAP SMB中央访问策略的信息 68
显示有关ONTAP SMB中央访问策略规则的信息 70
用于管理SMB服务器计算机帐户密码的ONTAP命令 72
管理域控制器连接 72
显示有关ONTAP SMB发现的服务器的信息 72
重置并重新发现ONTAP SMB服务器 73
管理ONTAP SMB域控制器发现 74
添加首选ONTAP SMB域控制器 75
用于管理首选SMB域控制器的ONTAP命令 76
启用与ONTAP SMB域控制器的加密连接 76
使用空会话访问非 Kerberos 环境中的存储 76
使用ONTAP SMB空会话访问非Kerberos环境中的存储 76
了解ONTAP SMB存储系统如何提供空会话访问 76
为空用户授予对ONTAP SMB文件系统共享的访问权限 77
管理 SMB 服务器的 NetBIOS 别名 78
了解如何管理ONTAP SMB服务器的NetBIOS别名 78
将NetBIOS别名列表添加到ONTAP SMB服务器 78
从ONTAP SMB服务器的列表中删除NetBIOS别名 79
显示ONTAP SMB服务器的NetBIOS别名列表 80
确定ONTAP SMB客户端是否使用NetBIOS别名进行连接 81
管理其他 SMB 服务器任务 82
停止或启动ONTAP SMB服务器 82
将ONTAP SMB服务器移动到不同的OU 83
在移动ONTAP SMB服务器之前修改动态DNS域 84
将ONTAP SMB SVM加入Active Directory域 84
显示有关基于TCP连接的ONTAP SMB NetBIOS的信息 85
用于管理SMB服务器的ONTAP命令 86
启用ONTAP SMB NetBIOS名称服务 87
对 SMB 访问和 SMB 服务使用 IPv6 88
了解IPv6的ONTAP SMB要求 88
了解ONTAP SMB访问和CIFS服务对IPv6的支持 88
了解ONTAP SMB服务器如何使用IPv6连接到外部服务器 89
为ONTAP SMB服务器启用IPv6 90
了解如何为ONTAP SMB服务器禁用IPv6 90
监控和显示有关IPv6 ONTAP SMB会话的信息 91

管理 SMB 服务器

修改ONTAP 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。有关的详细信息 `vserver cifs modify`，请参见"ONTAP 命令参考"。

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ONTAP 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ONTAP 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`

有关和配置SMB服务器选项的详细信息 `vserver cifs options modify`，请参见"ONTAP 命令参考"。

配置向ONTAP 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`

为匿名用户配置ONTAP SMB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

了解如何为**UNIX**安全模式数据的**SMB**客户端提供**ONTAP**文件安全性

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

配置向**ONTAP SMB**客户端提供**UNIX**安全模式数据的**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`

了解如何为**ONTAP SMB FlexVol**卷保留**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 。

了解如何使用**ONTAP SMB**服务器的**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

了解如何处理**ONTAP 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。

了解**ONTAP SVM**灾难恢复配置的**SMB**服务器安全设置

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**ONTAP 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用户配置ONTAP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

请勿在工作组模式下对CIFS服务器使用 `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

- 显示有关服务器安全设置的信息
- 了解本地用户和群组
- 本地用户密码的要求
- 更改本地用户帐户密码

修改ONTAP SMB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ONTAP 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。
`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 的通信配置 AES 加密

使用AES加密为基于Kerberos的通信配置强大的ONTAP SMB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`选项启用建议的加密类型、也可以使用它禁用较弱的加密类型。了解如何"为基于 Kerberos 的通信配置 AES 加密"。

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

修改服务器安全设置

为基于ONTAP SMB Kerberos的通信配置AES加密

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
```

相关信息

"域用户无法使用域通道登录集群"

使用 **SMB** 签名增强网络安全性

了解如何使用**ONTAP SMB**签名增强网络安全性

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。

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)]

了解**ONTAP 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。

ONTAP SMB签名配置建议

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。

了解适用于多个数据**ONTAP**的**SMB**签名配置

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**ONTAP**流量配置**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。

相关信息

- "SnapMirror 创建"

确定**ONTAP 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**ONTAP 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。

   有关的详细信息 `statistics start`，请参见"ONTAP 命令参考"。

3. 使用 `statistics stop` 命令停止收集样本数据。

   详细了解 `statistics stop`在"ONTAP 命令参考" 。

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。

   有关的详细信息 `statistics show`，请参见"ONTAP 命令参考"。

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

了解**ONTAP SMB**加密

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。

了解**ONTAP 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。

为传入流量启用或禁用**ONTAP 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
```

相关信息

- "SnapMirror 创建"

确定客户端是否使用加密的**ONTAP 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**ONTAP 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。

   有关的详细信息 `statistics start`，请参见"ONTAP 命令参考"。

3. 使用 `statistics stop` 命令停止收集样本数据。

   详细了解 `statistics stop`在"ONTAP 命令参考" 。

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。

有关的详细信息 `statistics show`，请参见"ONTAP 命令参考"。

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

- 确定服务器上可用的统计数据、对象和计数器
- "性能监控和管理概述"

安全 LDAP 会话通信

了解ONTAP SMB LDAP签名和签章

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ONTAP SMB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ONTAP SMB SVM的自签名根CA证书

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ONTAP SMB 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

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`

相关信息

- "安全证书安装"
- "security certificate show"

在**ONTAP SMB**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：

- "了解适用于 ONTAP NFS SVM 的 LDAP"
- "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：

配置ONTAP SMB多通道以实现性能和冗余

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
```

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

配置默认ONTAP SMB UNIX用户

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ONTAP SMB 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**ONTAP SMB**根

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、则目录具有文件级ACL、 `/etc`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ONTAP 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ONTAP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* ）

有关的详细信息 `vserver cifs options modify`，请参见"ONTAP 命令参考"。

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

了解如何使用传统机会锁和租用机会锁提高ONTAP SMB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。

了解使用oplock时编写ONTAP SMB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ONTAP SMB共享时启用或禁用操作锁定

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SMB卷和qtrees上启用或禁用操作锁定的ONTAP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**ONTAP SMB**共享上启用或禁用操作锁定

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。
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
- 添加或删除现有共享的共享属性

监控ONTAP SMB操作锁定状态

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

有关的详细信息 `vserver oplocks show`，请参见"ONTAP 命令参考"。

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 SMB 卷和 qtree 上启用或禁用 oplock 的命令

将组策略对象应用于 SMB 服务器

了解如何将组策略对象应用于ONTAP SMB服务器

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

- 了解服务器的文件访问安全性
- "SMB 和 NFS 审核和安全跟踪"

了解支持的ONTAP SMB 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

- 在服务器上启用或禁用 GPO 支持
- 了解服务器的文件访问安全性

- "SMB 和 NFS 审核和安全跟踪"
- 修改服务器安全设置
- 了解如何使用 BranchCache 在分支机构缓存共享内容
- 了解如何使用 ONTAP 签名来增强网络安全
- 了解如何配置绕过遍历检查
- 配置匿名用户的访问限制

GPO的ONTAP SMB服务器要求

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许可证随一起提供"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ONTAP SMB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

了解受支持的 GPO

GPO 的服务器要求

了解如何在 SMB 服务器上更新 GPO

手动更新 SMB 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

了解如何在**ONTAP SMB**服务器上更新**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 SMB 服务器上的 GPO 设置

手动更新ONTAP SMB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

了解如何在 SMB 服务器上更新 GPO

显示有关ONTAP SMB 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

在服务器上启用或禁用 GPO 支持

显示有关ONTAP SMB受限组GPO的信息

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`
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ONTAP SMB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

- 了解服务器的文件访问安全性

- 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ONTAP SMB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

- 了解服务器的文件访问安全性
- 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ONTAP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 ...
当ONTAP与AD服务同步时、更改域帐户密码	`vserver cifs domain password change`
如果ONTAP未与AD服务同步、请重置域帐户密码	`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`

有关的详细信息 `vserver cifs domain password`，请参见"ONTAP 命令参考"。

管理域控制器连接

显示有关ONTAP SMB发现的服务器的信息

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
- 停止或启动服务器

重置并重新发现ONTAP SMB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
- 停止或启动服务器

管理ONTAP SMB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 。

开始之前

您必须处于高级权限级别。

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ONTAP SMB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SMB域控制器的ONTAP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`

有关的详细信息 `vserver cifs domain preferred-dc`，请参见"ONTAP 命令参考"。

相关信息

添加首选域控制器

启用与ONTAP SMB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ONTAP SMB空会话访问非Kerberos环境中的存储

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。

了解ONTAP SMB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支持带有选项的Windows注册表设置值 `-restrict-anonymous`。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。有关和 `vserver cifs options show`以及 `–restrict-anonymous`选项的详细信息， `vserver cifs options modify`请参见"ONTAP 命令参考"。

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

为空用户授予对ONTAP SMB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

了解如何管理ONTAP SMB服务器的NetBIOS别名

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

将NetBIOS别名列表添加到ONTAP SMB服务器

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 SMB 服务器列表中删除 NetBIOS 别名
- 显示 SMB 服务器的 NetBIOS 别名列表

从ONTAP SMB服务器的列表中删除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ONTAP SMB服务器的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
```

有关的详细信息 `vserver cifs show`，请参见"ONTAP 命令参考"。

相关信息

- 向服务器添加 NetBIOS 别名列表
- 管理服务器的命令

确定ONTAP 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`

要显示 **NetBIOS** 信息的对象	输入 ...
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**ONTAP SMB**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ONTAP SMB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。

在移动ONTAP SMB服务器之前修改动态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ONTAP SMB 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

- 要继续修改Active Directory域、必须将CIFS服务器的管理状态设置为 `down`。
- 如果命令成功完成，管理状态将自动设置为 `up`。有关的详细信息 `up`，请参见"ONTAP 命令参考"。
- 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`

   有关的详细信息 `vserver cifs modify`，请参见"ONTAP 命令参考"。如果需要为新域重新配置DNS，请在中了解有关的更多信息 `vserver dns modify`"ONTAP 命令参考"。

   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**ONTAP SMB 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ONTAP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`

有关的详细信息 `vserver cifs`，请参见"ONTAP 命令参考"。

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ONTAP SMB 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

了解IPv6的ONTAP SMB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许可证随一起提供"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 ）。

了解ONTAP SMB访问和CIFS服务对IPv6的支持

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

了解**ONTAP SMB**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

- 为服务器启用 IPv6
- 监视并显示有关 IPv6 会话的信息

为ONTAP SMB服务器启用IPv6

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`

   已启用 IPv6 。可以配置用于 SMB 访问的 IPv6 数据 LIF 。

相关信息

- 监视并显示有关 IPv6 会话的信息
- "使用System Manager直观地显示网络"
- "在集群上启用 IPv6"
- "网络选项ipv6 modify"

了解如何为ONTAP SMB服务器禁用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。

相关信息

- "使用System Manager直观地显示ONTAP网络"

监控和显示有关IPv6 ONTAP 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。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。