NAS协议

NetApp Solutions

NetApp
April 12, 2024

目录

NAS协议

NAS协议概述

NAS协议包括NFS (v3和v4.1)和SMB/CIFS (2.x和3.x)。这些协议是CVS允许在多个NAS客户端之间共享访问数据的方式。此外、Cloud Volumes Service 还可以同时提供对NFS和SMB/CIFS客户端的访问(双协议)、同时遵守NAS共享中文件和文件夹的所有身份和权限设置。为了保持尽可能高的数据传输安全性、Cloud Volumes Service 支持使用SMB加密和NFS Kerberos 5p进行协议加密。

> 双协议仅适用于CVS-Performance。

NAS协议基础知识

NAS协议是一个网络上的多个客户端访问存储系统上相同数据的方法、例如GCP上的Cloud Volumes Service。NFS和SMB是定义的NAS协议、在客户端/服务器基础上运行、Cloud Volumes Service 充当服务器。客户端向服务器发送访问、读取和写入请求、服务器负责协调文件锁定机制、存储权限以及处理身份和身份验证请求。

例如、如果NAS客户端要在文件夹中创建新文件、则遵循以下常规过程。

1. 客户端要求服务器提供有关目录的信息(权限、所有者、组、文件ID、可用空间、 等)；如果发出请求的客户端和用户对父文件夹具有必要的权限、则服务器将使用此信息进行响应。
2. 如果目录上的权限允许访问、则客户端会询问服务器所创建的文件名是否已存在于文件系统中。如果文件名已在使用中、则创建将失败。如果文件名不存在、服务器会让客户端知道它可以继续。
3. 客户端调用服务器以使用目录句柄和文件名创建文件、并设置访问和修改时间。服务器会向文件发出唯一的文件ID、以确保不会使用相同的文件ID创建其他文件。
4. 在执行写入操作之前、客户端会发送一个调用来检查文件属性。如果权限允许、客户端将写入新文件。如果协议/应用程序使用锁定、则客户端会要求服务器提供锁定、以防止其他客户端在锁定期间访问文件、以防止数据损坏。

NFS

NFS是一种分布式文件系统协议、它是在Request for Comments (RFC)中定义的开放式IETF标准、允许任何人实施该协议。

通过导出客户端或一组客户端可访问的路径、可以将Cloud Volumes Service 中的卷共享到NFS客户端。挂载这些导出的权限由导出策略和规则定义、这些策略和规则可由Cloud Volumes Service 管理员配置。

NetApp NFS实施被视为该协议的黄金标准、用于无数企业级NAS环境。以下各节介绍了Cloud Volumes Service 中提供的NFS和特定安全功能及其实施方式。

默认本地UNIX用户和组

Cloud Volumes Service 包含多个用于各种基本功能的默认UNIX用户和组。当前无法修改或删除这些用户和组。当前无法将新的本地用户和组添加到Cloud Volumes Service 中。默认用户和组以外的UNIX用户和组需要由外部LDAP名称服务提供。

下表显示了默认用户和组及其对应的数字ID。NetApp建议不要在LDAP中或在重新使用这些数字ID的本地客户端上创建新用户或组。

默认用户：数字ID	默认组：数值ID
• 根：0 • pcuser：65534 • nobody：65535	• 根：0 • 守护进程：1. • pcuser：65534 • nobody：65535

> 使用NFSv4.1时、root用户在NFS客户端上运行目录列出命令时可能会显示为nobody。这是因为客户端的ID域映射配置。请参见名为的部分 NFSv4.1和nobody用户/组 有关此问题描述 以及如何解决此问题的详细信息、请参见。

root用户

在Linux中、root帐户可以访问基于Linux的文件系统中的所有命令、文件和文件夹。由于此帐户的强大功能、安全最佳实践通常要求以某种方式禁用或限制root用户。在NFS导出中、可以通过导出策略和规则以及称为根强制转换的概念在Cloud Volumes Service 中控制root用户对文件和文件夹的能力。

根强制转换可确保访问NFS挂载的root用户被强制转换为匿名数字用户65534 (请参见第节[匿名用户]")、并且当前仅在使用CVS-Performance时可用、方法是在创建导出策略规则期间选择off作为root访问权限。如果root用户被强制转换为匿名用户、则它将无法再运行chown或 "setuid/setgid命令(粘滞位)" 对于NFS挂载中的文件或文件夹、以及root用户创建的文件或文件夹、将anon UID显示为所有者/组。此外、root用户无法修改NFSv4 ACL。但是、root用户仍可访问其没有显式权限的chmod和已删除的文件。如果要限制对root用户的文件和文件夹权限的访问、请考虑使用具有NTFS ACL的卷、创建名为`root`的Windows用户并将所需权限应用于文件或文件夹。

匿名用户

匿名(anon)用户ID指定映射到未使用有效NFS凭据的客户端请求的UNIX用户ID或用户名。使用root用户强制转换时、这可能包括root用户。Cloud Volumes Service 中的anon用户为65534。

在Linux环境中、此UID通常与用户名`nobody`或`nfsnobody`关联。Cloud Volumes Service 还使用65534作为本地UNIX用户` pcuser`(请参见第节默认本地UNIX用户和组")、当在LDAP中找不到有效匹配的UNIX用户时、它也是Windows到UNIX名称映射的默认回退用户。

由于Linux和Cloud Volumes Service 中UID 65534的用户名不同、因此使用NFSv4.1时映射到65534的用户的名称字符串可能不匹配。因此、在某些文件和文件夹上、您可能会看到`nobody`作为用户。请参见第节"NFSv4.1和nobody用户/组有关此问题描述 以及如何解决此问题的信息、请参见。

访问控制/导出

NFS挂载的初始导出/共享访问通过导出策略中包含的基于主机的导出策略规则进行控制。定义了主机IP、主机

名、子网、网络组或域、以允许访问挂载NFS共享以及主机允许的访问级别。导出策略规则配置选项取决于Cloud Volumes Service 级别。

对于CVS-SW、导出策略配置可使用以下选项：

- 客户端匹配。 IP地址列表以逗号分隔、主机名、子网、网络组和域名列表以逗号分隔。
- * RO/RW访问规则。*选择读/写或只读以控制对导出的访问级别。cvs-Performance提供了以下选项：
- 客户端匹配。 IP地址列表以逗号分隔、主机名、子网、网络组和域名列表以逗号分隔。
- * RO或RW访问规则。*选择读/写或只读以控制导出的访问级别。
- *根访问(开/关)。*配置根强制转换(请参见一节[root用户]"了解详细信息)。
- *协议类型。*此操作会将对NFS挂载的访问限制为特定协议版本。为卷同时指定NFSv3和NFSv4.1时、请将这两个字段留空或同时选中这两个框。
- * Kerberos安全级别(选择启用Kerberos时)。*提供了krb5、krb5i和/或krb5p选项、用于只读或读写访问。

更改所有权(chown)和更改组(chgrp)

Cloud Volumes Service 上的NFS仅允许root用户对文件和文件夹运行chown/chgrp。其他用户会看到`Operation not permitted`错误、即使是在其拥有的文件上也是如此。如果使用root squash (如第节中所述)[root用户]")、根卷将被强制转换为非root用户、并且不允许访问chown和chgrp。目前、Cloud Volumes Service 中没有允许非root用户使用chown和chgrp的解决方法。如果需要更改所有权、请考虑使用双协议卷并将安全模式设置为NTFS、以便从Windows端控制权限。

权限管理

Cloud Volumes Service 同时支持模式位(例如rwx的6444、777等)和NFSv4.1 ACL、以控制使用UNIX安全模式的卷在NFS客户端上的权限。标准权限管理用于这些对象(例如chmod、chown或nfs4_setfacl)、并可用于支持这些对象的任何Linux客户端。

此外、使用设置为NTFS的双协议卷时、NFS客户端可以利用Cloud Volumes Service 名称映射到Windows用户、然后使用该映射来解析NTFS权限。这需要通过LDAP连接到Cloud Volumes Service 来提供数字ID到用户名的转换、因为Cloud Volumes Service 需要有效的UNIX用户名才能正确映射到Windows用户名。

为**NFSv3**提供粒度**ACL**

模式位权限仅涵盖语义中的所有者、组和其他所有人、这意味着基本NFSv3没有粒度用户访问控制。Cloud Volumes Service 既不支持POSIX ACL、也不支持扩展属性(例如chattr)、因此、只有在使用NFSv3的以下情况下、才可以使用粒度ACL：

- 具有有效UNIX到Windows用户映射的NTFS安全模式卷(需要CIFS服务器)。
- 使用挂载NFSv4.1的管理客户端应用NFSv4.1 ACL以应用ACL。

这两种方法都需要使用LDAP连接进行UNIX身份管理、并填充有效的UNIX用户和组信息(请参见一节 ""LDAP"")、并且仅适用于CVS-Performance实例。要对NFS使用NTFS安全模式卷、必须使用双协议(SMB和NFSv3)或双协议(SMB和NFSv4.1)、即使未建立SMB连接也是如此。要对NFSv3挂载使用NFSv4.1 ACL、必须选择`both (NFSv3/NFSv4.1)`作为协议类型。

常规UNIX模式位提供的权限粒度级别与NTFS或NFSv4.x ACL提供的权限级别不同。下表对NFSv3模式位和NFSv4.1 ACL之间的权限粒度进行了比较。有关NFSv4.1 ACL的信息、请参见 "NFS4_ACL—NFSv4访问控制列表"。

NFSv3 模式位	NFSv4.1 ACL
• 执行时设置用户ID • 执行时设置组ID • 保存交换的文本(未在POSIX中定义) • 所有者的读取权限 • 所有者的写入权限 • 对文件执行所有者权限；或者在目录中查找(搜索)所有者权限 • 组的读取权限 • 组的写入权限 • 对文件中的组执行权限；或者在目录中查找(搜索)组权限 • 其他人的读取权限 • 其他人的写入权限 • 对其他人对文件执行权限；或者在目录中查找(搜索)其他人的权限	访问控制条目(ACE)类型(允许/拒绝/审核)*继承标志*目录继承*文件继承*无传播-继承*仅继承 权限*读取数据(文件)/列表目录(目录)*写入数据(文件)/创建文件(目录)*附加数据(文件)/创建子目录(目录)*执行(文件)/更改目录(目录)*删除*删除子目录*读取属性*写入属性*读取命名属性*写入ACL *写入所有者*写入ACL *写入操作

最后、根据RPC数据包限制、对于AUTH_SYS、NFS组成员资格(在NFSv3和NFSv4.x中)限制为默认最大16个。NFS Kerberos最多可提供32个组、NFSv4 ACL可通过粒度用户和组ACL (每个ACE最多1024个条目)来消除此限制。

此外、Cloud Volumes Service 还提供了扩展的组支持、可将支持的最大组数扩展到32个。这需要通过LDAP连接到包含有效UNIX用户和组身份的LDAP服务器。有关配置此的详细信息、请参见 "创建和管理NFS卷" 在Google文档中。

NFSv3用户和组ID

NFSv3用户和组ID以数字ID而非名称的形式通过网线传输。Cloud Volumes Service 使用NFSv3无法解析这些数字ID的用户名、而UNIX安全模式卷仅使用模式位。如果存在NFSv4.1 ACL、则需要进行数字ID查找和/或名称字符串查找才能正确解析此ACL、即使使用NFSv3也是如此。对于NTFS安全模式卷、Cloud Volumes Service 必须将数字ID解析为有效的UNIX用户、然后映射到有效的Windows用户以协商访问权限。

NFSv3用户和组ID的安全限制

使用NFSv3时、客户端和服务器无需确认尝试使用数字ID进行读写的用户是否为有效用户；这只是隐式信任。这样、只需欺骗任何数字ID即可使文件系统不受潜在漏洞的影响。为了防止出现此类安全漏洞、Cloud Volumes Service 提供了一些选项。

- 实施适用于NFS的Kerberos会强制用户使用用户名和密码或keytab文件进行身份验证、以获取Kerberos票证以允许访问挂载。Kerberos可用于CVS-Performance实例、仅适用于NFSv4.1。
- 限制导出策略规则中的主机列表会限制哪些NFSv3客户端可以访问Cloud Volumes Service 卷。
- 使用双协议卷并对卷应用NTFS ACL会强制NFSv3客户端将数字ID解析为有效的UNIX用户名、以便正确进行身份验证以访问挂载。这需要启用LDAP并配置UNIX用户和组身份。

- 将root用户强制转换会限制root用户对NFS挂载可能造成的损害、但不会完全消除风险。有关详细信息、请参见"[root用户]。 "

最终、NFS安全性仅限于您所使用的协议版本。虽然NFSv3的总体性能优于NFSv4.1、但提供的安全性级别不同。

NFSv4.1

与NFSv3相比、NFSv4.1的安全性和可靠性更高、原因如下：

- 通过基于租赁的机制实现集成锁定
- 有状态会话
- 通过单个端口提供所有NFS功能(2049)
- 仅限TCP
- ID域映射
- Kerberos集成(NFSv3可以使用Kerberos、但只能用于NFS、而不能用于辅助协议、例如NLM)

NFSv4.1依赖关系

由于NFSv4.1中的额外安全功能、因此、使用NFSv3时不需要涉及一些外部依赖关系(类似于SMB需要依赖关系的方式、例如Active Directory)。

NFSv4.1 ACL

Cloud Volumes Service 支持NFSv4.x ACL、与正常的POSIX模式权限相比、这些ACL具有明显的优势、例如：

- 精细控制用户对文件和目录的访问
- 提高 NFS 安全性
- 改进了与CIFS/SMB的互操作性
- 取消了使用AUTH_SYS安全性时每个用户16个组的NFS限制
- ACL不需要进行组ID (GID)解析、从而有效地消除了GID限制NFSv4.1 ACL由NFS客户端控制、而不是通过Cloud Volumes Service 控制。要使用NFSv4.1 ACL、请确保您的客户端软件版本支持这些ACL、并安装了正确的NFS实用程序。

NFSv4.1 ACL与SMB客户端之间的兼容性

NFSv4 ACL与Windows文件级ACL (NTFS ACL)不同、但具有类似的功能。但是、在多协议NAS环境中、如果存在NFSv4.1 ACL、而您使用的是双协议访问(同一数据集中的NFS和SMB)、则使用SMB2.0及更高版本的客户端将无法通过Windows安全选项卡查看或管理ACL。

NFSv4.1 ACL的工作原理

定义了以下术语以供参考：

- *访问控制列表(ACL)。*权限条目的列表。
- *访问控制条目(ACE)。*列表中的一个权限条目。

当客户端在SETATTR操作期间为文件设置NFSv4.1 ACL时、Cloud Volumes Service 会在对象上设置此ACL、以替换任何现有ACL。如果文件没有ACL、则文件的模式权限将通过所有者@、组@和所有人@计算得出。如果文件上存在任何现有的SUID/SGID/粘滞位、它们不会受到影响。

如果客户端在getattr操作期间获取文件的NFSv4.1 ACL、则Cloud Volumes Service 将读取与该对象关联的NFSv4.1 ACL、构建ACE列表并将该列表返回给客户端。如果文件具有NT ACL或模式位、则会使用模式位构建ACL并将其返回给客户端。

如果ACL中存在拒绝ACE、则拒绝访问；如果存在允许ACE、则授予访问权限。但是、如果ACL中不存在任何ACE、则访问也会被拒绝。

安全描述符由一个安全ACL (SACL)和一个随机ACL (DACL)组成。如果NFSv4.1与CIFS/SMB互操作、则DACL将与NFSv4和CIFS进行一对一映射。DACL由ALLOW ACE和DENY ACE组成。

如果在设置了NFSv4.1 ACL的文件或文件夹上运行基本的`chmod`、则会保留现有用户和组ACL、但会修改默认所有者@、组@、每个人@ ACL。

使用NFSv4.1 ACL的客户端可以为系统上的文件和目录设置和查看ACL。在具有ACL的目录中创建新文件或子目录时、该对象将继承ACL中已标记为相应的所有ACE "继承标志"。

如果文件或目录具有NFSv4.1 ACL、则无论使用哪个协议访问文件或目录、都可以使用该ACL来控制访问。

只要父目录上的NFSv4 ACL为ACE添加了正确的继承标志、文件和目录就会继承这些ACE (可能需要进行适当修改)。

在根据NFSv4请求创建文件或目录时、生成的文件或目录上的ACL取决于文件创建请求是包含ACL还是仅包含标准UNIX文件访问权限。ACL还取决于父目录是否具有ACL。

- 如果请求包含 ACL ，则会使用该 ACL 。
- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL ，则会使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果此请求仅包含标准UNIX文件访问权限、并且父目录具有不可继承的ACL、则会根据传递给此请求的模式位为新对象设置默认ACL。
- 如果此请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL ，则只要父目录的 ACL 中的 ACE 已使用适当的继承标志进行标记，新文件或目录就会继承这些 ACE 。

ACE权限

NFSv4.1 ACL权限使用一系列大小写字母值(例如`rxtncy`)来控制访问。有关这些字母值的详细信息、请参见 "如何：使用NFSv4 ACL"。

具有**umask**和**ACL**继承的**NFSv4.1 ACL**行为

"NFSv4 ACL可提供ACL继承功能"。ACL继承是指在设置了NFSv4.1 ACL的对象下创建的文件或文件夹可以根据的配置继承ACL "ACL继承标志"。

"umask" 用于控制在目录中创建文件和文件夹而无需管理员干预的权限级别。默认情况下、Cloud Volumes Service 允许umask覆盖继承的ACL、这是预期的行为 "RFC 5661"。

ACL格式化

NFSv4.1 ACL采用特定格式。以下示例是对文件设置的ACE：

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

上述示例遵循以下ACL格式准则：

```
type:flags:principal:permissions
```

类型`a`表示"允许"。 在这种情况下、不会设置继承标志、因为主体不是组、并且不包括继承。此外、由于ACE不是审核条目、因此无需设置审核标志。有关NFSv4.1 ACL的详细信息、请参见"http://linux.die.net/man/5/nfs4_acl"。

如果NFSv4.1 ACL设置不正确(或者客户端和服务器无法解析名称字符串)、则ACL可能无法按预期运行、或者ACL更改可能无法应用并引发错误。

示例错误包括：

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

显式拒绝

NFSv4.1权限可以包括所有者、组和所有人的显式拒绝属性。这是因为NFSv4.1 ACL为default-deny、这意味着如果ACE未明确授予ACL、则会拒绝该ACL。显式拒绝属性会覆盖任何访问ACE、无论显式还是非显式。

deny ACE使用属性标记`D`设置。

在以下示例中、组@允许所有读取和执行权限、但拒绝所有写入访问。

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

应尽可能避免拒绝ACE、因为它们可能会造成混乱和复杂；不明确定义的允许ACL会被隐式拒绝。如果设置了拒绝ACE、则在用户希望获得访问权限时、可能会拒绝其访问。

上述一组ACE相当于模式位中的755、这意味着：

- 所有者拥有完全权限。
- 组具有只读。
- 其他用户只读。

但是、即使权限调整为775等效权限、访问也可能会因为对Everyone设置了显式拒绝而被拒绝。

NFSv4.1 ID域映射依赖关系

NFSv4.1利用ID域映射逻辑作为安全层、帮助验证尝试访问NFSv4.1挂载的用户是否确实是他们所宣称的身份。在这些情况下、NFSv4.1客户端的用户名和组名称会附加一个名称字符串并将其发送到Cloud Volumes Service 实例。如果此用户名/组名称和ID字符串组合不匹配、则此用户和/或组将被强制转换为客户端上的`/etc/idmapd.conf`文件中指定的默认nobody用户。

要确保正确遵守权限、需要使用此ID字符串、尤其是在使用NFSv4.1 ACL和/或Kerberos时。因此、要确保客户端和Cloud Volumes Service 之间的一致性、以正确解析用户和组名称身份、必须具有LDAP服务器等名称服务服务器依赖关系。

Cloud Volumes Service 使用静态默认ID域名值`defaultv4iddomain.com`。NFS客户端的ID域名设置默认为DNS域名、但您可以在`/etc/idmapd.conf`中手动调整ID域名。

如果在Cloud Volumes Service 中启用了LDAP、则Cloud Volumes Service 会自动将NFS ID域更改为DNS中为搜索域配置的内容、并且客户端不需要修改、除非它们使用不同的DNS域搜索名称。

如果Cloud Volumes Service 可以解析本地文件或LDAP中的用户名或组名称、则会使用域字符串、而不匹配的域ID将强制转换为nobody。如果Cloud Volumes Service 在本地文件或LDAP中找不到用户名或组名称、则会使用数字ID值、NFS客户端会正确解析此名称(这类似于NFSv3行为)。

如果不更改客户端的NFSv4.1 ID域以匹配Cloud Volumes Service 卷正在使用的内容、您将看到以下行为：

- 在Cloud Volumes Service 中具有本地条目的UNIX用户和组(如在本地UNIX用户和组中定义的root)将被强制转换为nobody值。
- 如果NFS客户端和Cloud Volumes Service 之间的DNS域不同、则具有LDAP条目的UNIX用户和组(如果Cloud Volumes Service 配置为使用LDAP)将强制转换为nobody。
- 没有本地条目或LDAP条目的UNIX用户和组使用数字ID值并解析为NFS客户端上指定的名称。如果客户端上不存在任何名称、则仅显示数字ID。

下面显示了上述情形的结果：

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

如果客户端ID域和服务器ID域匹配、则相同文件列表的显示方式如下：

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

有关此问题描述 以及如何解决此问题的详细信息、请参见"NFSv4.1和nobody用户/组。 "

Kerberos依赖关系

如果您计划对NFS使用Kerberos、则Cloud Volumes Service 必须具有以下配置：

- Kerberos分发中心服务(KDC)的Active Directory域
- Active Directory域、其中用户和组属性填充了有关LDAP功能的UNIX信息(Cloud Volumes Service 中的NFS Kerberos需要用户SPN到UNIX用户映射才能正常运行。)
- 已在Cloud Volumes Service 实例上启用LDAP
- DNS服务的Active Directory域

NFSv4.1和nobody用户/组

NFSv4.1配置中最常见的问题之一是、如果列表中使用`ls`显示的文件或文件夹属于`user：group` combination of `nobody：nobody`。

例如：

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

数字ID为`99`。

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

在某些情况下、文件可能会显示正确的所有者、但会显示组`nobody`。

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

谁不是谁?

NFSv4.1中的`nobody`用户与`nfsnobody`用户不同。您可以运行`id`命令来查看NFS客户端如何识别每个用户：

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

使用NFSv4.1时、`nobody`用户是由`idmapd.conf`文件定义的默认用户、可定义为要使用的任何用户。

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

为什么会发生这种情况?

由于通过名称字符串映射实现安全性是NFSv4.1操作的关键要素、因此、如果名称字符串不匹配、则默认行为是将该用户强制转换为通常无法访问用户和组所拥有的文件和文件夹的用户。

如果您在文件列表中看到用户和/或组的`nobody`、则这通常意味着NFSv4.1中的某些内容配置不当。区分大小写可以在此处发挥作用。

例如、如果user1@CVSDEMO.LOCAL (uid 1234、gid 1234)正在访问导出、则Cloud Volumes Service 必须能够找到user1@CVSDEMO.LOCAL (uid 1234、gid 1234)。如果Cloud Volumes Service 中的用户为USER1@CVSDEMO.LOCAL、则不匹配(大写用户1与小写用户1)。在许多情况下、您可以在客户端上的消息文件中看到以下内容：

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

客户端和服务器都必须同意用户确实是他们所声称的用户、因此您必须检查以下内容、以确保客户端看到的用户与Cloud Volumes Service 看到的用户具有相同的信息。

- * NFSv4.x ID域。*客户端：`idmapd.conf` file；Cloud Volumes Service 使用`defaultv4iddomain.com`、无法手动更改。如果将LDAP与NFSv4.1结合使用、则Cloud Volumes Service 会将ID域更改为DNS搜索域所使用的域、该域与AD域相同。
- *用户名和数字ID。*这决定了客户端查找用户名的位置、并利用名称服务开关配置—client：`nsswitch.conf`和/或本地passwd和group文件；Cloud Volumes Service 不允许修改此设置、但在启用LDAP后会自动将其添加到配置中。
- *组名称和数字ID。*这决定了客户端查找组名称的位置、并利用名称服务开关配置—client：`nsswitch.conf`和/或本地passwd和group文件；Cloud Volumes Service 不允许修改此设置、但会在启用LDAP后自动将其添加到配置中。

在几乎所有情况下、如果您在客户端的用户和组列表中看到`nobody`、则问题描述 将在Cloud Volumes Service 和NFS客户端之间进行用户或组名称域ID转换。要避免这种情况、请使用LDAP在客户端和Cloud Volumes Service 之间解析用户和组信息。

查看客户端上**NFSv4.1**的名称**ID**字符串

如果您使用的是NFSv4.1、则会在NFS操作期间进行名称-字符串映射、如上所述。

除了使用`/var/log/messages`查找具有NFSv4 ID的问题描述 之外、您还可以使用 "nfsidmap -l" 命令以查看哪些用户名已正确映射到NFSv4域。

例如、这是客户端发现的用户以及Cloud Volumes Service 访问NFSv4.x挂载后命令的输出：

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

如果某个用户未正确映射到NFSv4.1 ID域(在本例中为`netapp-user`)、则会尝试访问同一挂载并触摸某个文件、系统会按预期为其分配`nobody：nobody`。

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

`nfsidmap -l`**输出会在屏幕上显示用户**`pcuser`、但不会显示`netapp-user`；这是我们导出策略规则中的匿名用户(`65534`)。

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" 是Microsoft开发的一种网络文件共享协议、可通过以太网为多个SMB客户端提供集中式用户/组身份验证、权限、锁定和文件共享。文件和文件夹通过共享呈现给客户端、共享可以配置各种共享属性、并通过共享级别权限提供访问控制。SMB可以提供给提供协议支持的任何客户端、包括Windows、Apple和Linux客户端。

Cloud Volumes Service 支持SMB 2.1和3.x版本的协议。

访问控制/SMB共享

- 当Windows用户名请求访问Cloud Volumes Service 卷时、Cloud Volumes Service 会使用Cloud Volumes Service 管理员配置的方法查找UNIX用户名。
- 如果配置了外部UNIX身份提供程序(LDAP)、并且Windows/UNIX用户名相同、则Windows用户名将1：1映射到UNIX用户名、而无需任何其他配置。启用LDAP后、Active Directory用于托管用户和组对象的这些UNIX属性。
- 如果Windows名称和UNIX名称不匹配、则必须将LDAP配置为允许Cloud Volumes Service 使用LDAP名称映射配置(请参见一节) ""使用LDAP进行非对称名称映射""）。
- 如果未使用LDAP、则Windows SMB用户会映射到Cloud Volumes Service 中名为`pcuser`的默认本地UNIX用户。这意味着在多协议NAS环境中、映射到`pcuser`的用户在Windows中写入的文件将UNIX所有权显示为`pcuser`。`pcuser`此处是Linux环境中的`nobody`用户(UID 65534)。

在仅使用SMB的部署中、仍会进行`pcuser`映射、但这无关紧要、因为Windows用户和组所有权会正确显示、并且不允许对仅使用SMB的卷进行NFS访问。此外、仅SMB卷在创建后不支持转换为NFS或双协议卷。

Windows利用Kerberos与Active Directory域控制器进行用户名身份验证、这需要与AD DC进行用户名/密码交换、AD DC位于Cloud Volumes Service 实例外部。如果SMB客户端使用`\\servername` UNC路径且满足以下条件、则会使用Kerberos身份验证：

- 服务器名称存在DNS A/AAAA条目
- 服务器名称存在有效的SMB/CIFS访问SPN

创建Cloud Volumes Service SMB卷时、系统会按照一节中的定义创建计算机帐户名称 "《Cloud Volumes Service 在Active Directory中的显示方式》。" 该计算机帐户名称也会成为SMB共享访问路径、因为Cloud Volumes Service 利用动态DNS (DDNS)在DNS中创建必要的A/AAAA和PTR条目、并在计算机帐户主体上创建必要的SPN条目。

> 要创建PTR条目、DNS服务器上必须存在Cloud Volumes Service 实例IP地址的反向查找区域。

例如、此Cloud Volumes Service 卷使用以下UNC共享路径：`\\cvs-east- 433d.cvsdema.local`。

在Active Directory中、这些是Cloud Volumes Service生成的SPN条目：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

这是DNS正向/反向查找结果：

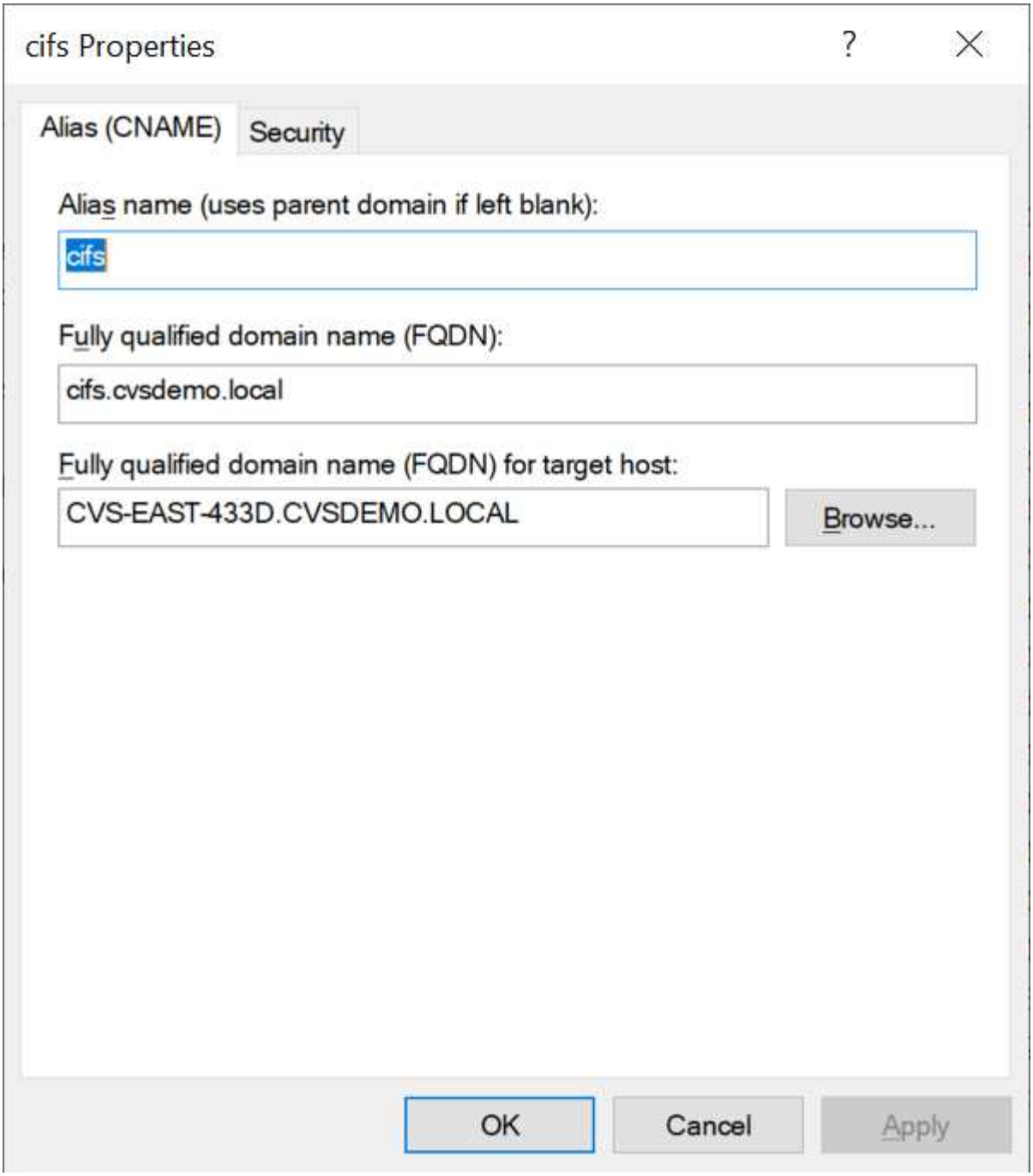
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

或者、可以通过在Cloud Volumes Service 中为SMB共享启用/要求SMB加密来应用更多访问控制。如果其中一个端点不支持SMB加密、则不允许访问。

使用**SMB**名称别名

在某些情况下、如果最终用户知道Cloud Volumes Service 使用的计算机帐户名称、则可能会出于安全考虑。在其他情况下、您可能只想为最终用户提供一个更简单的访问路径。在这种情况下、您可以创建SMB别名。

如果要为SMB共享路径创建别名、可以利用DNS中的CNAME记录。例如、如果您要使用名称`\\cifs`来访问共享、而不是`\\cvs-east- 433d.cvsdema.local`、但您仍要使用Kerberos身份验证、则DNS中指向现有A/AAAA记录的CNAME以及添加到现有计算机帐户的其他SPN可提供Kerberos访问。



这是添加CNAME后生成的DNS正向查找结果：

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

这是添加新SPN后生成的SPN查询：

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

在数据包捕获中、我们可以使用与CNAME绑定的SPN查看会话设置请求。

```
431 4.156722                                    SMB2    308 Negotiate Protocol Response
432 4.156785                                    SMB2    232 Negotiate Protocol Request
434 4.158108                                    SMB2    374 Negotiate Protocol Response
435 4.160977                                    SMB2   1978 Session Setup Request
437 4.166224                                    SMB2    322 Session Setup Response
438 4.166891                                    SMB2    152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2    138 Tree Connect Response

        realm: CVSDEMO.LOCAL
      ⌄ sname
          name-type: kRB5-NT-SRV-INST (2)
        ⌄ sname-string: 2 items
            SNameString: cifs
            SNameString: cifs
      ⌄ enc-part
          etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB身份验证方言

Cloud Volumes Service 支持以下功能 "方言" 对于SMB身份验证：

- LM
- NTLM
- NTLMv2
- Kerberos

用于SMB共享访问的Kerberos身份验证是您可以使用的最安全的身份验证级别。启用AES和SMB加密后、安全级别将进一步提高。

Cloud Volumes Service 还支持LM和NTLM身份验证的向后兼容性。如果Kerberos配置不当(例如创建SMB别名)、则共享访问会回退到身份验证方法较弱的位置(例如NTLMv2)。由于这些机制的安全性较低、因此在某些Active Directory环境中会禁用它们。如果禁用了较弱的身份验证方法、并且未正确配置Kerberos、则共享访问将失败、因为没有可回退的有效身份验证方法。

有关在Active Directory中配置/查看受支持的身份验证级别的信息、请参见 "网络安全：LAN Manager身份验证级别"。

权限模式

NTFS/文件权限

NTFS权限是指应用于符合NTFS逻辑的文件系统中的文件和文件夹的权限。您可以在`基本`或`高级`中应用NTFS权限、并可设置为`允许`或`D允许`来进行访问控制。

基本权限包括：

- 完全控制
- 修改
- 读取和执行
- 读取
- 写入

为用户或组(称为ACE)设置权限时、该用户或组驻留在ACL中。NTFS权限使用与UNIX模式位相同的读/写/执行基础知识、但也可以扩展到更精细的扩展访问控制(也称为"特殊权限")、例如"获取所有权"、"创建文件夹/附加数据"、"写入属性"等。

标准UNIX模式位提供的粒度级别与NTFS权限不同(例如、能够为ACL中的各个用户和组对象设置权限或设置扩展属性)。但是、NFSv4.1 ACL提供的功能与NTFS ACL相同。

NTFS权限比共享权限更具体、可与共享权限结合使用。对于NTFS权限结构、限制性最强。因此、在定义访问权限时、显式拒绝用户或组甚至会覆盖"完全控制"。

NTFS权限由Windows SMB客户端控制。

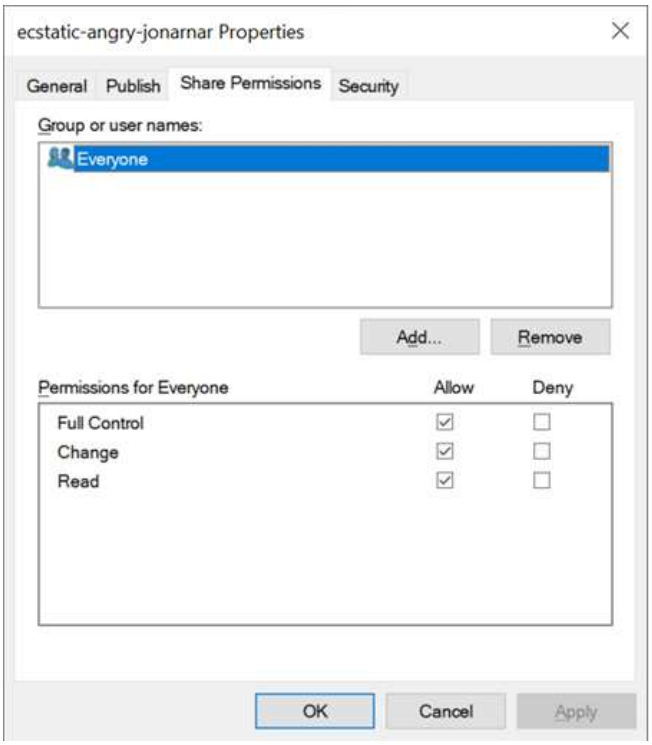
共享权限

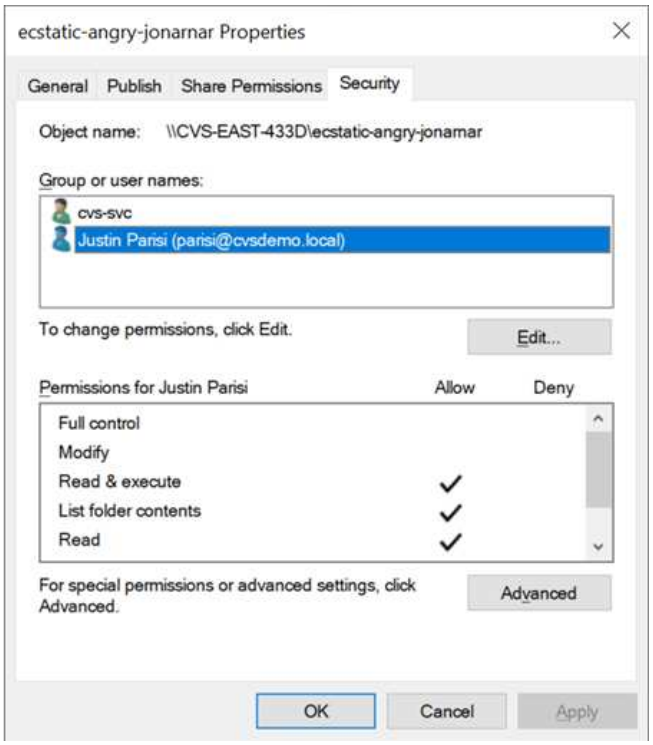
共享权限比NTFS权限更常规(仅限读取/更改/完全控制)、并可控制SMB共享的初始条目、类似于NFS导出策略规则的工作方式。

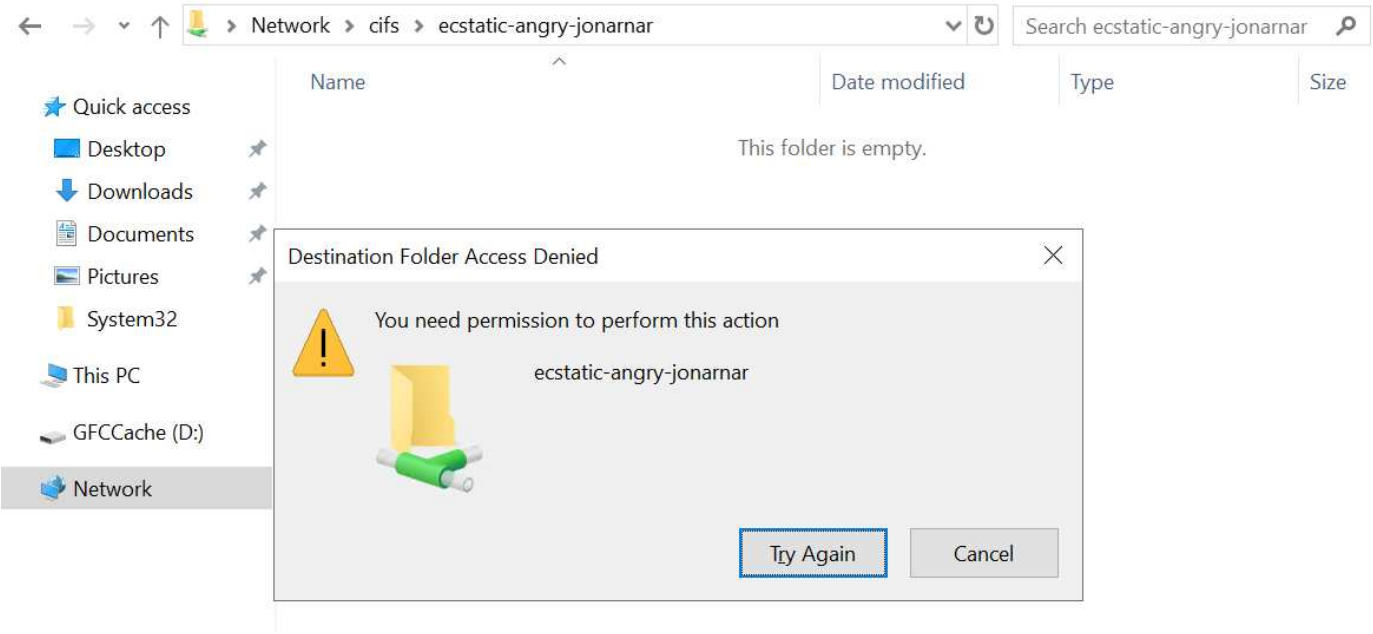
虽然NFS导出策略规则通过IP地址或主机名等基于主机的信息来控制访问、但SMB共享权限可以通过使用共享ACL中的用户和组ACE来控制访问。您可以从Windows客户端或Cloud Volumes Service 管理UI设置共享ACL。

默认情况下、共享ACL和初始卷ACL包括具有完全控制的Everyone。应更改文件ACL、但共享权限会被共享中对象的文件权限所取代。

例如、如果仅允许用户读取Cloud Volumes Service 卷文件ACL、则即使共享ACL设置为"具有完全控制的所有人"、也会拒绝用户访问创建文件和文件夹、如下图所示。







要获得最佳安全性结果、请执行以下操作：

- 从共享和文件ACL中删除Everyone、而是为用户或组设置共享访问权限。
- 使用组进行访问控制、而不是使用单个用户、以便于管理、并加快删除/添加用户的速度、以便通过组管理共享ACL。
- 允许对共享权限上的ACE进行限制性更低的常规共享访问、并锁定对具有文件权限的用户和组的访问、以实现更精细的访问控制。
- 避免常规使用显式拒绝ACL、因为它们会覆盖允许ACL。限制需要限制的用户或组快速访问文件系统时使用显式拒绝ACL。
- 请务必注意 "ACL继承" 修改权限时的设置；在文件数量较多的目录或卷的顶层设置继承标志意味着该目录或

卷下的每个文件都添加了继承权限、 这可能会在调整每个文件时产生不必要的行为、例如意外访问/拒绝以及长时间更改权限。

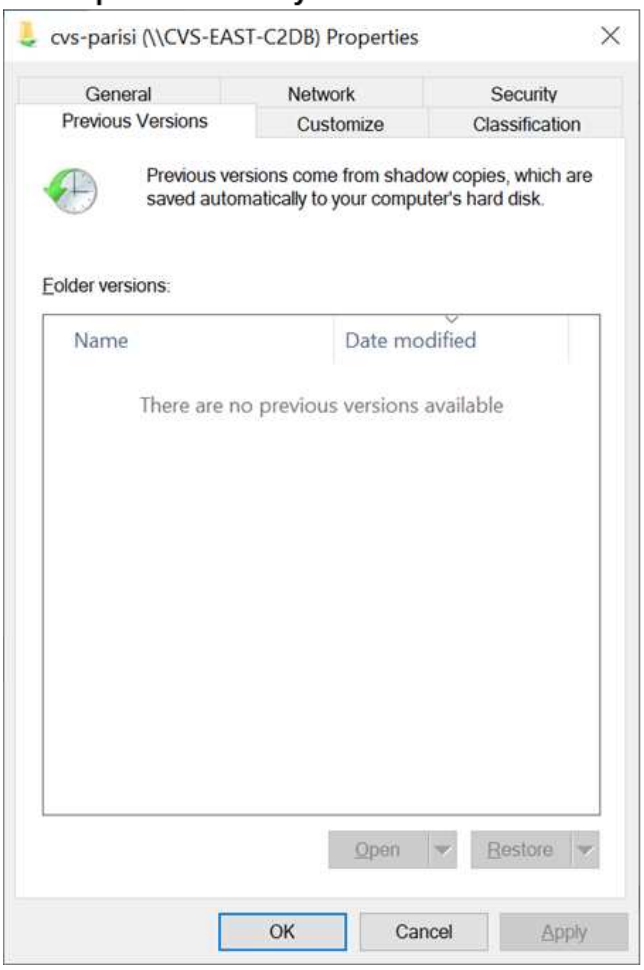
SMB共享安全功能

首次在Cloud Volumes Service 中创建具有SMB访问权限的卷时、系统会为您提供一系列用于保护该卷的选项。

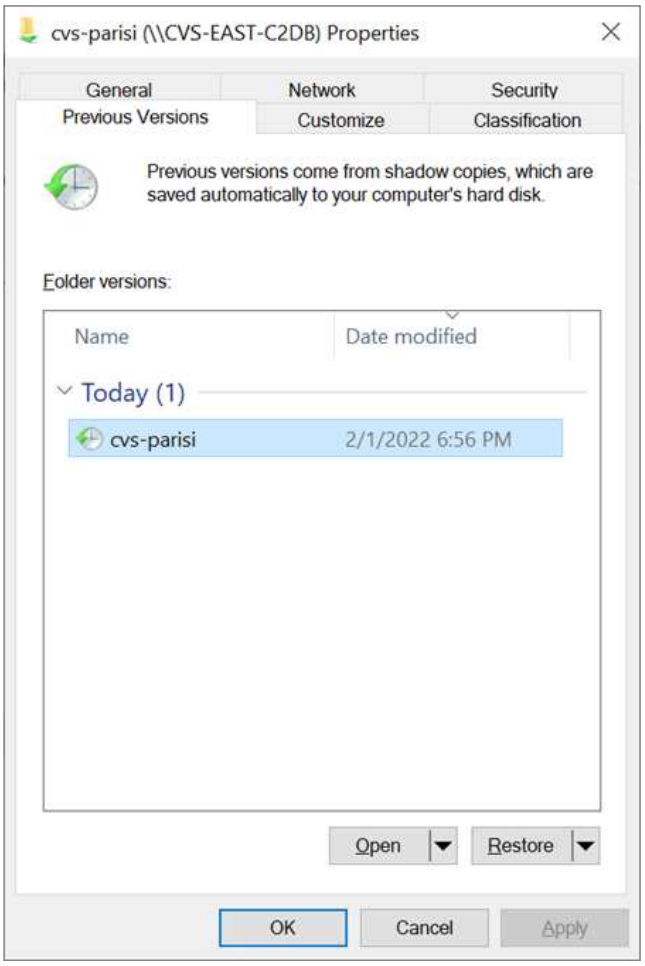
其中一些选项取决于Cloud Volumes Service 级别(性能或软件)、选项包括：

- *使Snapshot目录可见(可用于CVS-Performance和CVS-SW)。*此选项控制SMB客户端是否可以访问SMB共享中的Snapshot目录(`\\server\share~snapshot`和/或先前版本选项卡)。默认设置不会选中、这意味着卷默认隐藏和禁止访问~snapshot`目录、并且卷的"先前版本"选项卡中不会显示任何Snapshot副本。

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



出于安全原因、性能原因(从AV扫描中隐藏这些文件夹)或偏好、可能需要向最终用户隐藏Snapshot副本。Cloud Volumes Service 快照是只读的、因此、即使这些快照可见、最终用户也无法删除或修改Snapshot目录中的文件。创建Snapshot副本时对文件或文件夹的文件权限将适用。如果文件或文件夹在Snapshot副本之间的权限发生变化、则所做的更改也会应用于Snapshot目录中的文件或文件夹。用户和组可以根据权限访问这些文件或文件夹。虽然无法删除或修改Snapshot目录中的文件、但可以从Snapshot目录中复制文件或文件夹。

- *启用SMB加密(可用于CVS-Performance和CVS-SW)。*默认情况下、SMB共享上禁用SMB加密(未选中)。选中此复选框可启用SMB加密、这意味着SMB客户端和服务器之间的流量将使用协商的最高支持加密级别进行动态加密。Cloud Volumes Service 最多支持对SMB进行AES-256加密。启用SMB加密确实会对SMB客户端造成性能降低、这种降低可能会也可能不会对SMB客户端造成明显影响、大致处于10-20%的范围

内。NetApp强烈建议通过测试来确定性能降低是否可接受。

- *隐藏SMB共享(可用于CVS-Performance和CVS-SW)。*设置此选项可在正常浏览时隐藏SMB共享路径。这意味着、不知道共享路径的客户端在访问默认UNC路径(例如`\\CVS-SMB`)时无法看到共享。选中此复选框后、只有明确知道SMB共享路径或具有组策略对象定义的共享路径的客户端才能访问此路径(通过混淆实现安全性)。
- *启用基于访问的枚举(ABE)(仅限CVS-SW)。*这与隐藏SMB共享类似、只是共享或文件仅对无权访问对象的用户或组隐藏。例如、如果至少不允许Windows用户`Joe`通过权限进行读取访问、则Windows用户`Joe`根本看不到SMB共享或文件。默认情况下、此选项处于禁用状态、您可以通过选中此复选框来启用它。有关ABE的详细信息、请参见NetApp知识库文章 "基于访问的枚举(ABE)如何工作？"
- 启用持续可用**(CA)**共享支持**(**仅限**CVS-Performance)**。 "持续可用的SMB共享" 通过在Cloud Volumes Service 后端系统中的节点之间复制锁定状态、提供一种在故障转移事件期间最大限度地减少应用程序中断的方法。这不是一项安全功能、但可以提供更好的整体故障恢复能力。目前、此功能仅支持SQL Server和FSLogix应用程序。

默认隐藏共享

在Cloud Volumes Service 中创建SMB服务器时、会显示 "隐藏的管理共享" (使用$命名约定)。其中包括C$(命名空间访问)和IPC$(共享命名管道以在程序之间进行通信、例如用于Microsoft管理控制台(MMC)访问的远程操作步骤 调用(RPC))。

ipc$共享不包含共享ACL、无法修改—它严格用于RPC调用和 "默认情况下、Windows不允许匿名访问这些共享"。

默认情况下、C$共享允许BUILTIN/Administrators访问、但Cloud Volumes Service 自动化会删除共享ACL、并且不允许任何人访问、因为访问C$共享可以查看Cloud Volumes Service 文件系统中所有已挂载的卷。因此、尝试导航到`\\Server\C$`失败。

具有本地/BUILTIN管理员/备份权限的帐户

Cloud Volumes Service SMB服务器与常规Windows SMB服务器具有类似的功能、因为有本地组(例如BUILTIN\Administrators)会将访问权限应用于选定域用户和组。

指定要添加到备份用户的用户时、该用户将添加到使用该Active Directory连接的Cloud Volumes Service 实例中的BUILTIN\Backup Operators组中、然后该组将获取 "SeBackupPrivilege和SeRestorePrivilege"。

将用户添加到安全权限用户时、系统会为该用户授予SeSecurityPrivilege、这在某些应用程序使用情形下非常有用、例如 "SMB共享上的SQL Server"。

Backup Users

Provide a comma separated list of domain users or a domain group name that require elevated privileges to access volumes created by Cloud Volumes Service.

Accountnames

administrator,cvs-svc

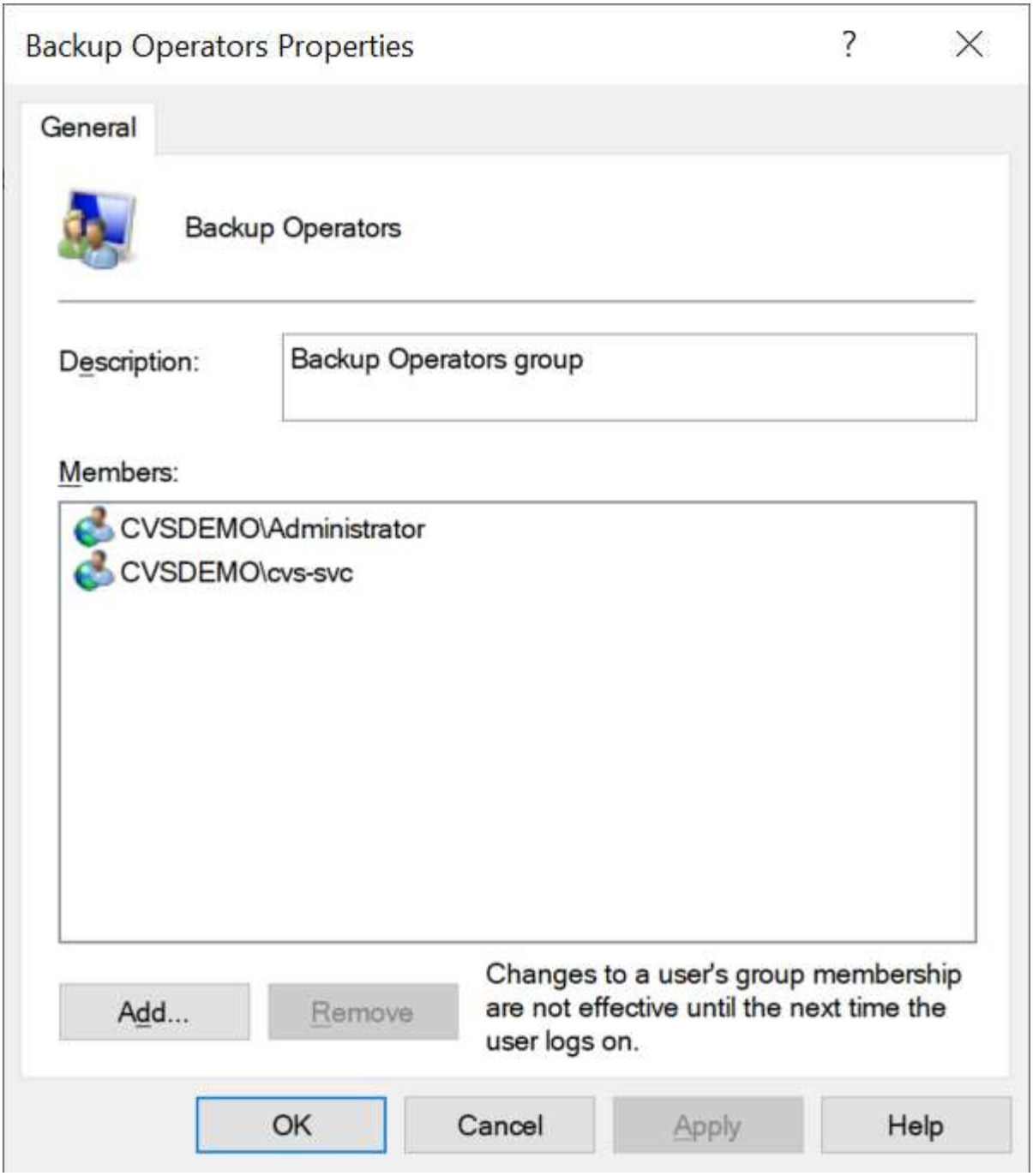
Security Privilege Users

Provide a list of comma separated domain user accounts that require elevated privileges to manage security log for the Active Directory associated with Cloud Volumes Service.

Accountnames

administrator,cvs-svc

您可以使用适当的权限通过MMC查看Cloud Volumes Service 本地组成员资格。下图显示了已使用Cloud Volumes Service 控制台添加的用户。

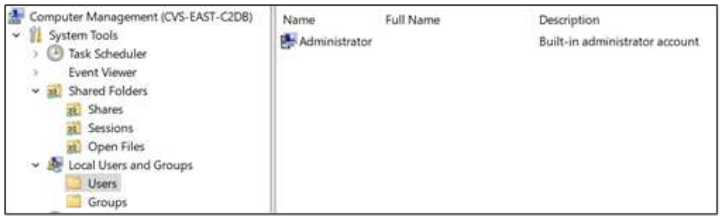


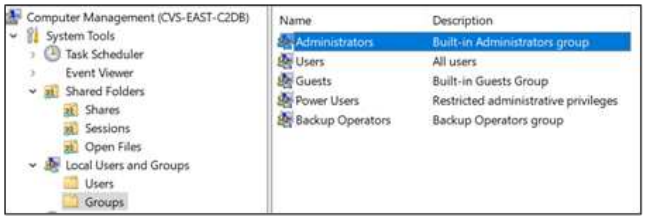
下表显示了默认BUILTIN组的列表以及默认添加的用户/组。

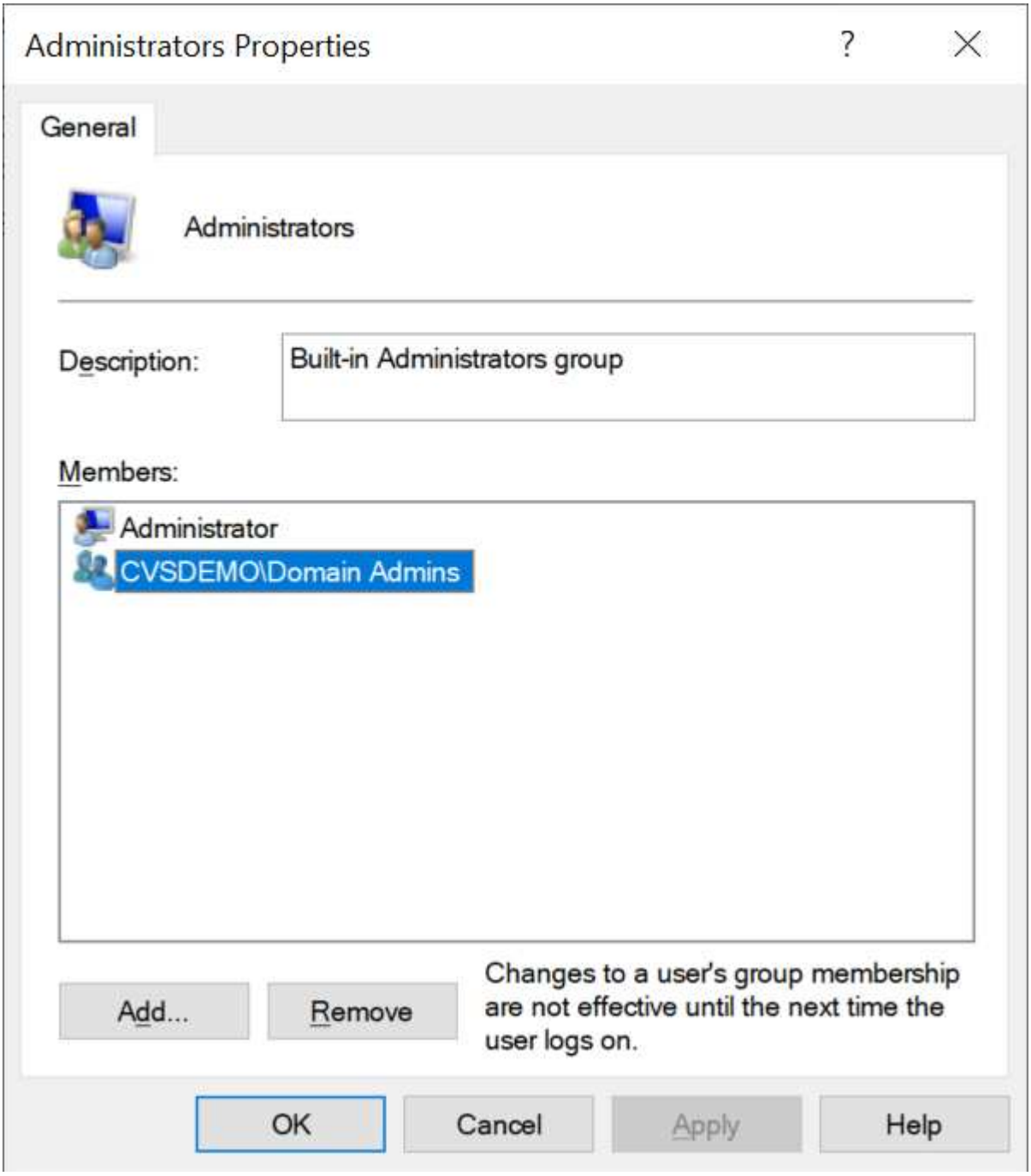
本地/**BUILTIN**组	默认成员
BUILTIN\Administrators *	域\域管理员
BUILTIN\Backup Operators*	无
BUILTIN\guests	域\域子系统
BUILTIN\Power Users	无
BUILTIN\Domain用户	域\域用户

*组成员资格在Cloud Volumes Service Active Directory连接配置中控制。

您可以在MMC窗口中查看本地用户和组(以及组成员)、但不能在此控制台中添加或删除对象或更改组成员资格。默认情况下、只有域管理员组和管理员才会添加到Cloud Volumes Service 中的BUILTIN\Administrators组。目前、您无法修改此设置。







MMC/计算机管理访问

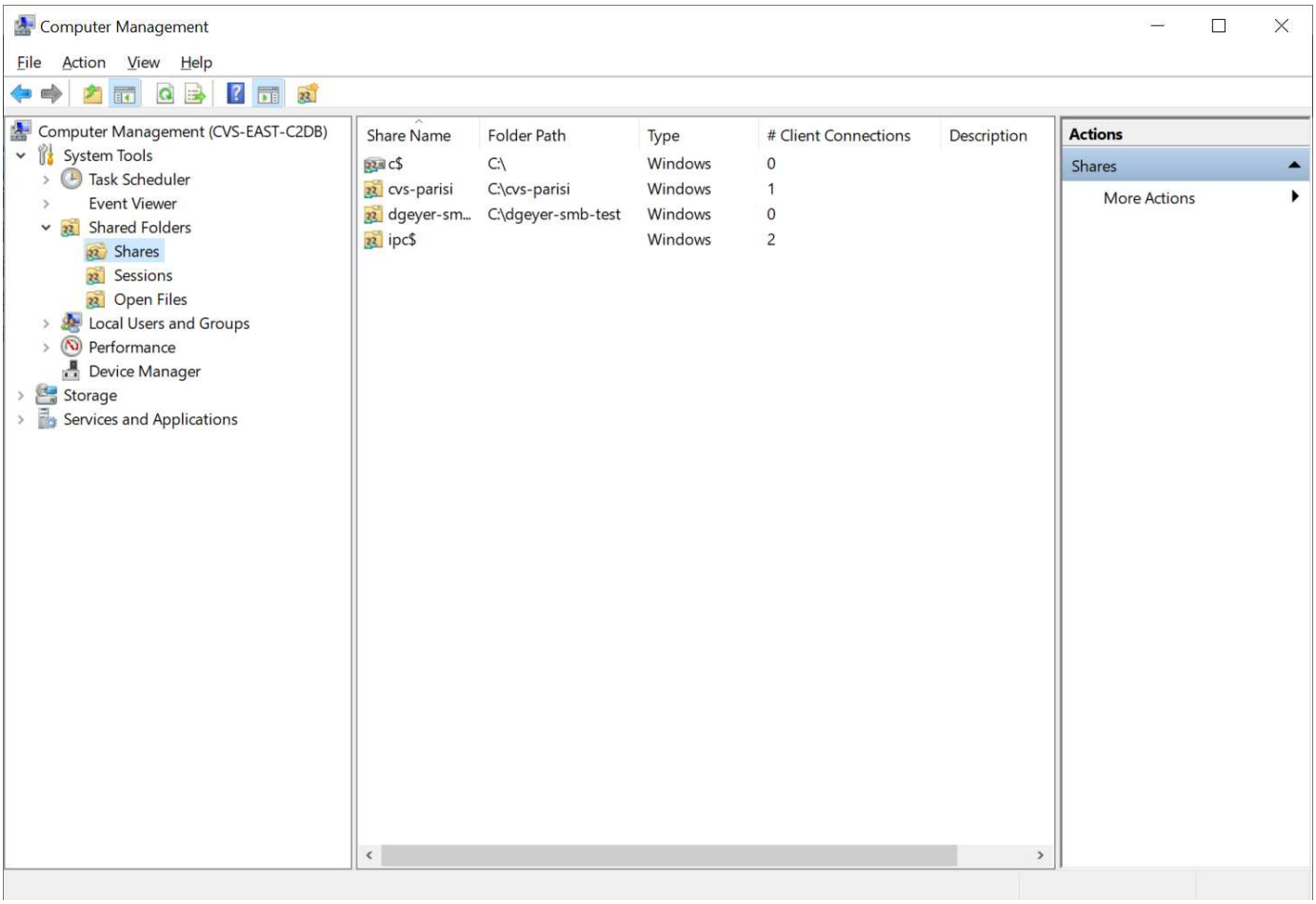
通过Cloud Volumes Service 中的SMB访问、您可以连接到计算机管理MMC、从而可以查看共享、管理共享ACL、以及查看/管理SMB会话和打开的文件。

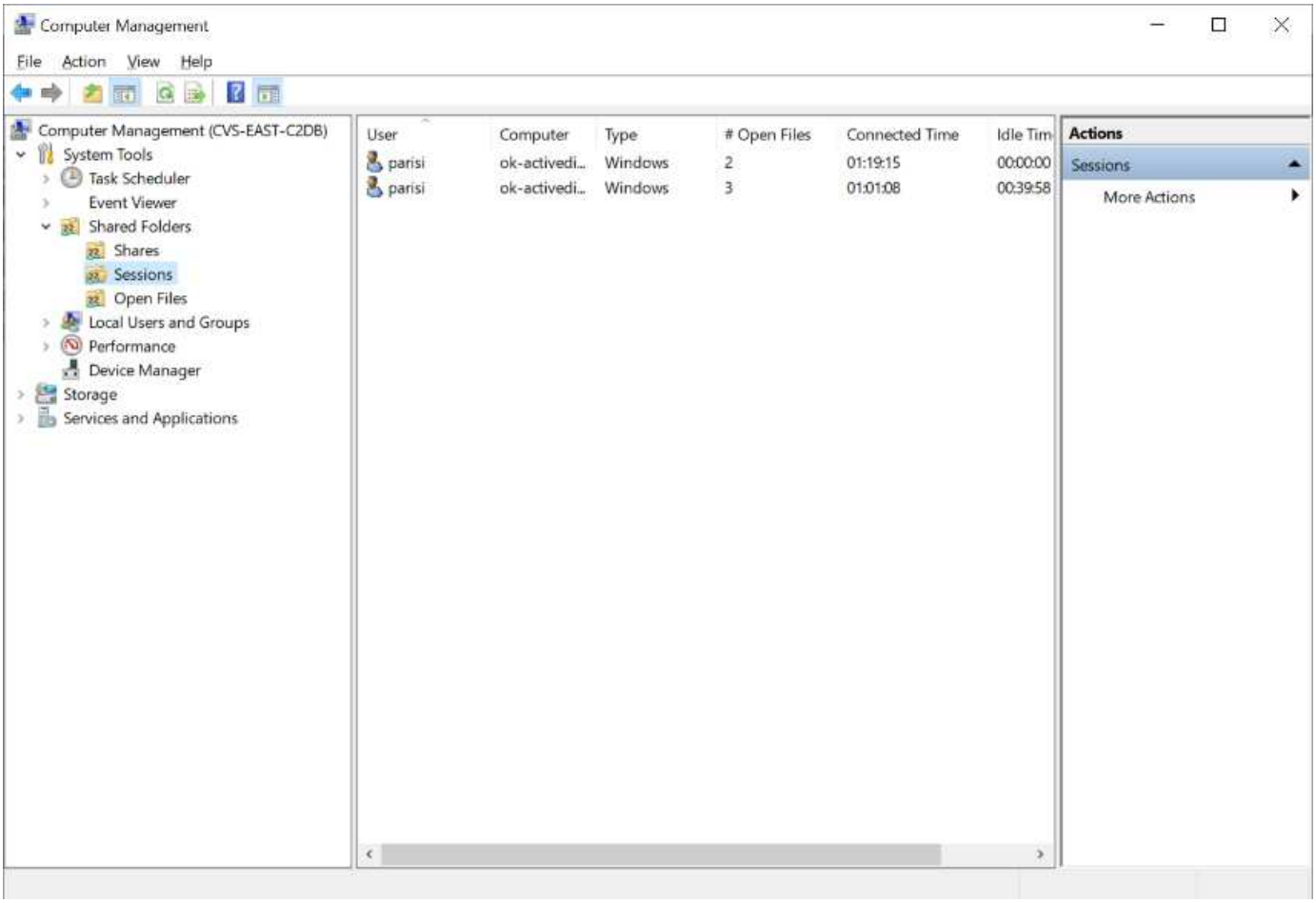
要使用MMC在Cloud Volumes Service 中查看SMB共享和会话、登录的用户当前必须是域管理员。其他用户可以通过MMC查看或管理SMB服务器、并在尝试查看Cloud Volumes Service SMB实例上的共享或会话时收到"您没有权限"对话框。

要连接到SMB服务器、请打开计算机管理、右键单击计算机管理、然后选择连接到另一台计算机。此时将打开选择计算机对话框、在此可以输入SMB服务器名称(可在Cloud Volumes Service 卷信息中找到)。

查看具有适当权限的SMB共享时、您会看到Cloud Volumes Service 实例中共享Active Directory连接的所有可用共享。要控制此行为、请在Cloud Volumes Service 卷实例上设置隐藏SMB共享选项。

请记住、每个区域仅允许一个Active Directory连接。





下表列出了MMC支持/不支持的功能。

支持的功能	不支持的功能
• 查看共享 • 查看活动的SMB会话 • 查看打开的文件 • 查看本地用户和组 • 查看本地组成员资格 • 枚举系统中的会话、文件和树连接列表 • 关闭系统中已打开的文件 • 关闭打开的会话 • 创建 / 管理共享	• 创建新的本地用户 / 组 • 管理/查看现有本地用户/组 • 查看事件或性能日志 • 管理存储 • 管理服务和应用程序

SMB服务器安全信息

Cloud Volumes Service 中的SMB服务器使用一系列选项来定义SMB连接的安全策略、包括Kerberos时钟偏差、票证期限、加密等。

下表列出了这些选项、它们的功能、默认配置以及是否可以使用Cloud Volumes Service 进行修改。某些选项不

适用于Cloud Volumes Service。

安全选项	功能	默认值	是否可以更改?
最大Kerberos时钟间隔(分钟)	Cloud Volumes Service 与域控制器之间的最大时间偏差。如果时间偏差超过5分钟、则Kerberos身份验证将失败。此值设置为Active Directory默认值。	5.	否
Kerberos票证生命周期(小时)	在要求续订之前、Kerberos票证保持有效的最长时间。如果在10小时之前未发生续订、您必须获取新的服务单。Cloud Volumes Service 会自动执行这些续订。Active Directory默认值为10小时。	10	否
Kerberos票证续订上限(天)	在需要新的授权请求之前可以续订Kerberos票证的最长天数。Cloud Volumes Service 会自动续订SMB连接的服务单。Active Directory默认值为七天。	7.	否
Kerberos KDC连接超时(秒)	KDC连接超时前的秒数。	3.	否
传入SMB流量需要签名	设置为SMB流量需要签名。如果设置为true、则不支持签名的客户端连接将失败。	false	
本地用户帐户需要密码复杂度	用于本地SMB用户的密码。Cloud Volumes Service 不支持创建本地用户、因此此选项不适用于Cloud Volumes Service。	true	否
对Active Directory LDAP连接使用start_tls	用于为Active Directory LDAP启用启动TLS连接。Cloud Volumes Service 当前不支持启用此功能。	false	否
已启用适用于Kerberos的AES-128和AES-256加密	此选项用于控制是否对Active Directory连接使用AES加密、并在创建/修改Active Directory连接时使用为Active Directory身份验证启用AES加密选项进行控制。	false	是的。

安全选项	功能	默认值	是否可以更改?
LM兼容性级别	Active Directory连接支持的身份验证方言级别。请参见第节"SMB身份验证方言"了解更多信息。	NTLMv2-KRB	否
传入CIFS流量需要SMB加密	所有共享都需要SMB加密。Cloud Volumes Service 不会使用此功能；而是按卷设置加密(请参见一节SMB共享安全功能")。	false	否
客户端会话安全性	为LDAP通信设置签名和/或密封。目前未在Cloud Volumes Service 中设置此选项、但在未来版本中可能需要执行此操作。本节将介绍由于Windows修补程序而导致的LDAP身份验证问题的修复方法 ""LDAP通道绑定。""。	无	否
SMB2为DC连接启用	使用SMB2进行DC连接。默认情况下处于启用状态。	系统默认值	否
LDAP转介跟踪	使用多个LDAP服务器时、如果在第一个服务器中找不到条目、则转介跟踪功能允许客户端引用列表中的其他LDAP服务器。Cloud Volumes Service 目前不支持此功能。	false	否
使用LDAPS实现安全Active Directory连接	启用基于SSL的LDAP。Cloud Volumes Service 目前不支持。	false	否
DC连接需要加密	要成功建立DC连接、需要加密。默认情况下、在Cloud Volumes Service 中处于禁用状态。	false	否

双协议/多协议

通过Cloud Volumes Service 、可以向SMB和NFS客户端共享相同的数据集、同时保持适当的访问权限 ("双协议") 。这是通过协调协议之间的身份映射以及使用中央后端LDAP服务器向Cloud Volumes Service 提供UNIX身份来实现的。您可以使用Windows Active Directory为Windows和UNIX用户提供方便易用的功能。

访问控制

- *共享访问控制。*确定哪些客户端和/或用户和组可以访问NAS共享。对于NFS、导出策略和规则控制客户端对导出的访问。NFS导出可通过Cloud Volumes Service 实例进行管理。SMB使用CIFS/SMB共享和共享ACL、在用户和组级别提供更精细的控制。您只能使用从SMB客户端配置共享级ACL "MMC/计算机管理" 具有Cloud Volumes Service 实例管理员权限的帐户(请参见一节 ""具有本地/BUILTIN管理员/备份权限的帐户。"")。
- *文件访问控制。*在文件或文件夹级别控制权限、并且始终从NAS客户端进行管理。NFS客户端可以使用传统模式位(rwx)或NFSv4 ACL。SMB客户端利用NTFS权限。

为NFS和SMB提供数据的卷的访问控制取决于所使用的协议。有关双协议权限的信息、请参见"[权限模型]。 "

用户映射

当客户端访问卷时、Cloud Volumes Service 会尝试反向将传入用户映射到有效用户。这一点对于跨协议确定正确的访问权限以及确保请求访问的用户确实是他们所宣称的用户是必不可少的。

例如、如果名为`joe`的Windows用户尝试通过SMB访问具有UNIX权限的卷、则Cloud Volumes Service 将执行搜索以查找名为`joe`的相应UNIX用户。如果存在一个、则以Windows用户`joe`的身份写入SMB共享的文件在NFS客户端中显示为UNIX用户`joe`。

或者、如果名为`Joe`的UNIX用户尝试使用Windows权限访问Cloud Volumes Service 卷、则UNIX用户必须能够映射到有效的Windows用户。否则、将拒绝对卷的访问。

目前、只有Active Directory支持使用LDAP进行外部UNIX身份管理。有关配置对此服务的访问权限的详细信息、请参见 "创建AD连接"。

权限模型

使用双协议设置时、Cloud Volumes Service 会使用卷的安全模式来确定ACL的类型。这些安全模式是根据指定的NAS协议设置的、对于双协议、则是在创建Cloud Volumes Service 卷时选择的。

- 如果您仅使用NFS、则Cloud Volumes Service 卷将使用UNIX权限。
- 如果您仅使用SMB、则Cloud Volumes Service 卷将使用NTFS权限。

如果要创建双协议卷、则可以在创建卷时选择ACL模式。应根据所需的权限管理来做出此决策。如果您的用户从Windows/SMB客户端管理权限、请选择NTFS。如果您的用户希望使用NFS客户端和chmod/chown、请使用UNIX安全模式。

创建Active Directory连接的注意事项

通过Cloud Volumes Service 、可以将Cloud Volumes Service 实例连接到外部Active Directory服务器、以便为SMB和UNIX用户进行身份管理。要在Cloud Volumes Service 中使用SMB、需要创建Active Directory连接。

此配置提供了多个选项、需要在一定程度上考虑安全性。外部Active Directory服务器可以是内部实例或云原生。如果您使用的是内部Active Directory服务器、请勿将域公开到外部网络(例如使用DMZ或外部IP地址)。而是使用安全专用通道或VPN、单向林信任或专用网络连接到内部网络 "私有 Google 访问"。有关的详细信息、请参见Google Cloud文档 "在Google Cloud中使用Active Directory的最佳实践"。

> CVS-SW要求Active Directory服务器位于同一区域。如果尝试在CVS-SW中与另一个区域建立DC连接、则尝试将失败。使用CVS-SW时、请务必创建包含Active Directory DC的Active Directory站点、然后在Cloud Volumes Service 中指定站点、以避免尝试跨区域DC连接。

Active Directory凭据

启用SMB或LDAP for NFS后、Cloud Volumes Service 将与Active Directory控制器进行交互、以创建用于身份验证的计算机帐户对象。这与Windows SMB客户端加入域的方式并要求对Active Directory中的组织单位(OU)具有相同的访问权限没有区别。

在许多情况下、安全组不允许在Cloud Volumes Service 等外部服务器上使用Windows管理员帐户。在某些情况下、作为安全最佳实践、Windows管理员用户将被完全禁用。

创建**SMB**计算机帐户所需的权限

要将Cloud Volumes Service 计算机对象添加到Active Directory、此帐户对域具有管理权限或具有管理权限 "用于创建和修改计算机帐户对象的委派权限" 指定的OU为必填项。您可以使用Active Directory中的"控制委派向导"执行此操作、方法是创建一个自定义任务、使用户能够使用提供的以下访问权限创建/删除计算机对象：

- 读 / 写
- 创建/删除所有子对象
- 读/写所有属性
- 更改/重置密码

这样会自动将定义的用户的安全ACL添加到Active Directory中的OU中、并最大限度地减少对Active Directory环境的访问。委派用户后、可以在此窗口中将此用户名和密码作为Active Directory凭据提供。

> 传递到Active Directory域的用户名和密码会在计算机帐户对象查询和创建期间利用Kerberos加密来提高安全性。

Active Directory连接详细信息

。 "Active Directory连接详细信息" 为管理员提供字段、以便为计算机帐户放置提供特定的Active Directory架构信息、例如：

- * Active Directory连接类型*用于指定某个区域中的Active Directory连接是用于Cloud Volumes Service 服务类型的卷还是CVS-Performance服务类型的卷。如果在现有连接上设置不正确、则在使用或编辑时可能无法正常工作。
- 域。 Active Directory域名。
- *站点*为了保证安全性和性能、将Active Directory服务器限制为特定站点 "注意事项"。如果多个Active Directory服务器跨越多个区域、则必须执行此操作、因为Cloud Volumes Service 目前不支持向Cloud Volumes Service 实例以外的其他区域的Active Directory服务器发出Active Directory身份验证请求。(例如、Active Directory域控制器所在的区域仅支持CVS-Performance、但您希望在CVS-SW实例中使用SMB共享。)
- * DNS服务器。*要在名称查找中使用的DNS服务器。
- * NetBIOS名称(可选)。*如果需要、则为服务器指定NetBIOS名称。这是使用Active Directory连接创建新计算机帐户时使用的。例如、如果NetBIOS名称设置为cvs-East、则计算机帐户名称将为cvs-East-｛1234｝。

请参见一节 "Cloud Volumes Service 在Active Directory中的显示方式" 有关详细信息 …

- *组织单位(OU)。*用于创建计算机帐户的特定OU。如果要将计算机帐户的控制权委派给特定OU的用户、则此功能非常有用。
- * AES加密。*您也可以选中或取消选中为AD身份验证启用AES加密复选框。为Active Directory身份验证启用AES加密可在用户和组查找期间为Cloud Volumes Service 到Active Directory的通信提供额外的安全性。启用此选项之前、请与域管理员联系以确认Active Directory域控制器支持AES身份验证。

> 默认情况下、大多数Windows服务器不会禁用较弱的密码(例如DES或RC4-HMAC)、但如果您选择禁用较弱的密码、请确认已将Cloud Volumes Service Active Directory连接配置为启用AES。否则、身份验证将失败。启用AES加密不会禁用较弱的密码、而是会向Cloud Volumes Service SMB计算机帐户添加对AES密码的支持。

Kerberos域详细信息

此选项不适用于SMB服务器。而是在为Cloud Volumes Service 系统配置NFS Kerberos时使用。填充这些详细信息后、将配置NFS Kerberos域(类似于Linux上的krb5.conf文件)、并在创建Cloud Volumes Service 卷时指定NFS Kerberos时使用此域、因为Active Directory连接充当NFS Kerberos分发中心(KDC)。

> 目前不支持将非Windows KDC与Cloud Volumes Service 结合使用。

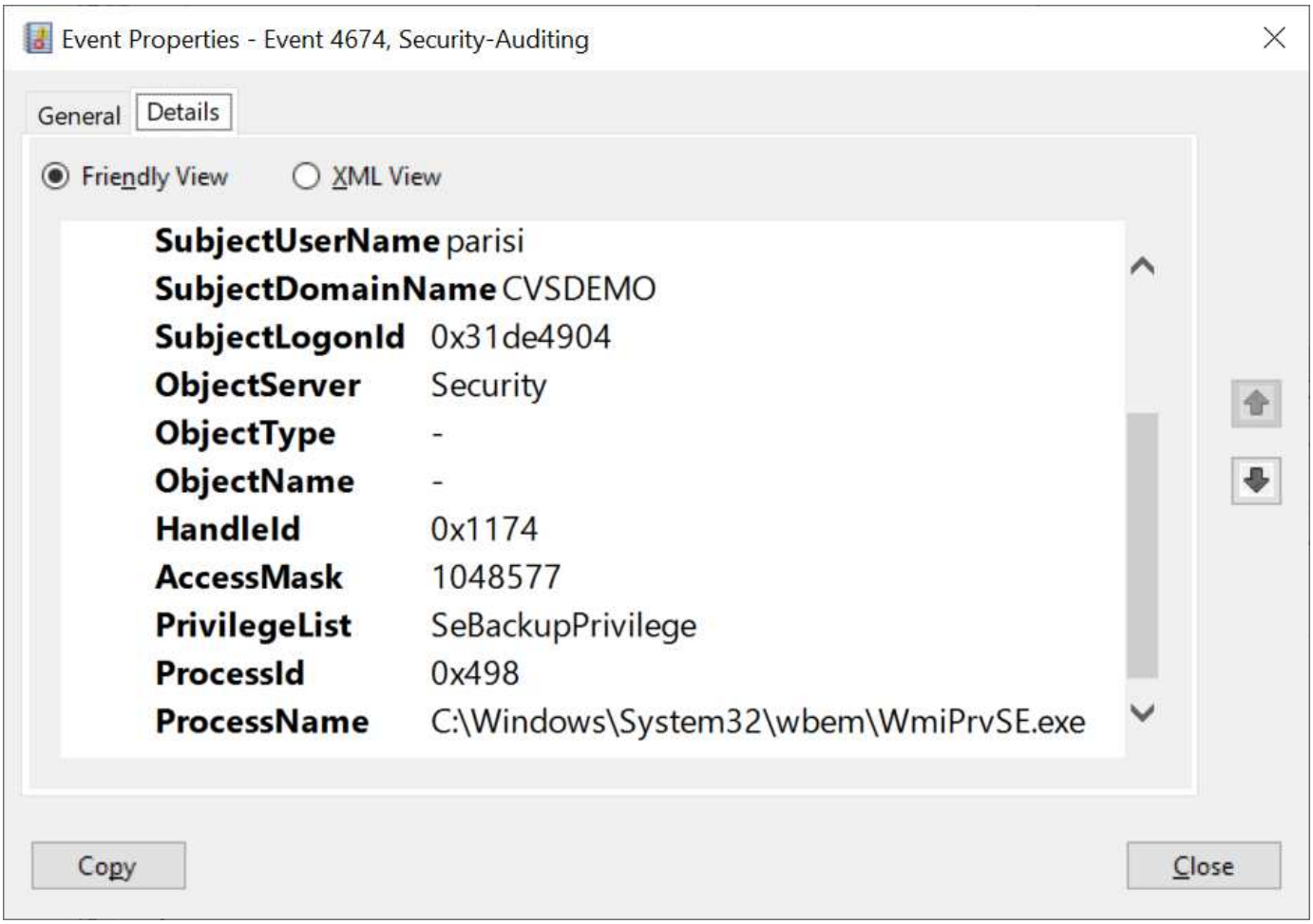
Region

使用区域可以指定Active Directory连接所在的位置。此区域必须与Cloud Volumes Service 卷所在的区域相同。

- *使用LDAP的本地NFS用户。*本节还提供了一个允许使用LDAP的本地NFS用户的选项。如果要将UNIX用户组成员资格支持扩展到NFS (扩展组)的16组限制之外、则必须取消选择此选项。但是、使用扩展组需要为UNIX身份配置LDAP服务器。如果您没有LDAP服务器、请取消选择此选项。如果您有LDAP服务器、并且还希望使用本地UNIX用户(例如root)、请选择此选项。

备份用户

使用此选项可以指定对Cloud Volumes Service 卷具有备份权限的Windows用户。某些应用程序需要使用备份特权(SeBackupPrivilege)来正确备份和还原NAS卷中的数据。此用户对卷中的数据具有较高的访问权限、因此您应考虑这一点 "启用对该用户访问的审核"。启用后、审核事件将显示在事件查看器> Windows日志>安全性中。



安全权限用户

使用此选项可以指定对Cloud Volumes Service 卷具有安全修改权限的Windows用户。某些应用程序需要安全特权(SeSecurityPrivilege) ("例如SQL Server")以在安装期间正确设置权限。管理安全日志需要此权限。虽然此特权的功能不如SeBackupPrivilege强大、但NetApp建议这样做 "审核用户的访问权限" 如果需要、则使用此权限级别。

有关详细信息，请参见 "分配给新登录的特殊权限"。

Cloud Volumes Service 在Active Directory中的显示方式

Cloud Volumes Service 在Active Directory中显示为普通计算机帐户对象。命名约定如下。

- CIFS/SMB和NFS Kerberos会创建单独的计算机帐户对象。
- 启用了LDAP的NFS会在Active Directory中为Kerberos LDAP绑定创建一个计算机帐户。
- 使用LDAP的双协议卷共享LDAP和SMB的CIFS/SMB计算机帐户。
- CIFS/SMB计算机帐户的命名约定为name-1234 (随机四位ID、并在< 10个字符名称后附加连字符)。您可以通过Active Directory连接上的NetBIOS名称设置来定义名称(请参见一节Active Directory连接详细信息")。
- NFS Kerberos使用nfs-name-1234作为命名约定(最多15个字符)。如果使用的字符数超过15个、则名称为nfs-truncated-name-1234。
- 启用了LDAP的仅NFS CVS-Performance实例创建一个SMB计算机帐户、以便使用与CIFS/SMB实例相同的

命名约定绑定到LDAP服务器。

- 创建SMB计算机帐户时、默认隐藏的管理共享(请参见一节 ""默认隐藏共享"")也会创建(c$、admin$、ipc$)、但这些共享没有分配ACL、因此无法访问。
- 默认情况下、计算机帐户对象放置在CN=Computers中、但您可以在必要时指定其他OU。请参见第节"创建SMB计算机帐户所需的权限有关为Cloud Volumes Service 添加/删除计算机帐户对象所需的访问权限的信息。

当Cloud Volumes Service 将SMB计算机帐户添加到Active Directory时、将填充以下字段：

- cn (使用指定的SMB服务器名称)
- dnsHostName (使用SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (如果未启用AES加密、则允许使用DES_CBC_MD5、RC4_HMAC_MD5；如果启用了AES加密、则允许使用计算机Kerberos帐户使用DES_CBC_MD5、RC4_HMAC_MD5、AES128_CTS_HMAC_SHA1_96、AES256_CTS_HMAC_SHA1_96)
- 名称(使用SMB服务器名称)
- sAMAccountName (使用SMBserver$)
- servicePrincipalName (具有用于Kerberos的host/smbserver.domain.com和host/smbserver SPN)

如果要在计算机帐户上禁用较弱的Kerberos加密类型(enctype)、则可以将计算机帐户上的MSDS-SupportedEncryptionTypes值更改为下表中的一个值、以便仅允许AES。

MSDS-SupportedEncryptionTypes值	已启用**EncType**
2.	DES_CBC_MD5
4.	RC4 HMAC
8.	仅限AES128_CTS_HMAC_SHA1_96
16.	仅限AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 和AES256_CTS_HMAC_SHA1_96
30 个	DES_CBC_MD5、RC4_HMAC、AES128_CTS_HMAC_SHA1_96和AES256_CTS_HMAC_SHA1_96

要为SMB计算机帐户启用AES加密、请在创建Active Directory连接时单击为AD身份验证启用AES加密。

为NFS Kerberos启用AES加密、 "请参见Cloud Volumes Service 文档"。

其他NAS基础架构服务依赖关系(KDC、LDAP和DNS)

在对NAS共享使用Cloud Volumes Service 时、可能需要外部依赖关系才能正常运行。这些依赖关系在特定情况下起作用。下表显示了各种配置选项以及需要哪些依赖关系(如果有)。

Configuration	需要依赖关系
仅限NFSv3	无

Configuration	需要依赖关系
仅限NFSv3 Kerberos	Windows Active Directory：* KDC * DNS * LDAP
仅限NFSv4.1	客户端ID映射配置(/etc/idmap.conf)
仅限NFSv4.1 Kerberos	• 客户端ID映射配置(/etc/idmap.conf) • Windows Active Directory：KDC DNS LDAP
仅SMB	Active Directory：* KDC * DNS
多协议NAS (NFS和SMB)	• 客户端ID映射配置(仅限NFSv4.1；/etc/idmap.conf) • Windows Active Directory：KDC DNS LDAP

计算机帐户对象的Kerberos keytab轮换/密码重置

对于SMB计算机帐户、Cloud Volumes Service 会为SMB计算机帐户计划定期密码重置。这些密码重置会使用Kerberos加密进行、并按每第四个星期日的计划在晚上11点到凌晨1点之间随机运行。这些密码重置会更改Kerberos密钥版本、轮换存储在Cloud Volumes Service 系统上的密钥选项卡、并帮助保持在Cloud Volumes Service 中运行的SMB服务器的更高级别安全性。计算机帐户密码是随机设置的、管理员不知道这些密码。

对于NFS Kerberos计算机帐户、只有在与KDC创建/交换新的keytab时、才会发生密码重置。目前、在Cloud Volumes Service 中无法执行此操作。

用于LDAP和Kerberos的网络端口

使用LDAP和Kerberos时、您应确定这些服务正在使用的网络端口。您可以在中找到Cloud Volumes Service 正在使用的端口的完整列表 "有关安全注意事项的Cloud Volumes Service 文档"。

LDAP

Cloud Volumes Service 充当LDAP客户端、并使用标准LDAP搜索查询来查找用户和组的UNIX身份。如果要使用Cloud Volumes Service 提供的标准默认用户之外的用户和组、则需要使用LDAP。如果您计划将NFS Kerberos与用户主体(如user1@domain.com)结合使用、也需要LDAP。目前、仅支持使用Microsoft Active Directory的LDAP。

要使用Active Directory作为UNIX LDAP服务器、您必须在要用于UNIX身份的用户和组上填充必要的UNIX属性。Cloud Volumes Service 使用默认LDAP模式模板、根据查询属性 "RFC-2307-bis"。因此、下表显示了为用户和组填充所需的最小Active Directory属性以及每个属性的用途。

有关在Active Directory中设置LDAP属性的详细信息、请参见 "管理双协议访问。"

属性	功能
UID*	指定UNIX用户名
uidNumber*	指定UNIX用户的数字ID
gidNumber*	指定UNIX用户的主组数字ID

属性	功能
objectclass*	指定正在使用的对象类型；Cloud Volumes Service 要求在对象类列表中包含"用户"(默认情况下、大多数Active Directory部署都包含此用户)。
name	有关帐户的常规信息(真实姓名、电话号码等、也称为gecos)
unixUserPassword	无需设置此参数；不会在用于NAS身份验证的UNIX身份查找中使用。如果设置此选项、则会将配置的unixUserPassword值设置为纯文本。
unixHomeDirectory	定义用户从Linux客户端根据LDAP进行身份验证时UNIX主目录的路径。如果要使用LDAP for UNIX主目录功能、请设置此选项。
loginShell	定义用户根据LDAP进行身份验证时Linux客户端的bash/配置文件Shell的路径。

*表示要在Cloud Volumes Service 中正常运行、必须具有属性。其余属性仅供客户端使用。

属性	功能
CN*	指定UNIX组名称。使用Active Directory进行LDAP时、会在首次创建对象时设置此值、但可以稍后更改。此名称不能与其他对象相同。例如、如果名为user1的UNIX用户属于Linux客户端上名为user1的组、则Windows不允许两个具有相同CN属性的对象。要解决此问题、请将Windows用户重命名为唯一名称(例如user1-unix)；Cloud Volumes Service 中的LDAP将使用UID属性作为UNIX用户名。
gidNumber*	指定UNIX组数字ID。
objectclass*	指定正在使用的对象类型；Cloud Volumes Service 要求组包含在对象类列表中(默认情况下、此属性包含在大多数Active Directory部署中)。
memberUID	指定哪些UNIX用户是UNIX组的成员。对于Cloud Volumes Service 中的Active Directory LDAP、不需要此字段。Cloud Volumes Service LDAP模式使用成员字段作为组成员资格。
成员*	组成员资格/二级UNIX组必需。此字段通过向Windows组添加Windows用户来填充。但是、如果Windows组未填充UNIX属性、则这些属性不会包含在UNIX用户的组成员资格列表中。任何需要在NFS中可用的组都必须填充此表中列出的所需UNIX组属性。

*表示要在Cloud Volumes Service 中正常运行、必须具有属性。其余属性仅供客户端使用。

LDAP绑定信息

要在LDAP中查询用户、Cloud Volumes Service 必须绑定(登录)到LDAP服务。此登录具有只读权限、用于查询LDAP UNIX属性以查找目录。目前、LDAP绑定只能使用SMB计算机帐户。

您只能为`CVS-Performance`实例启用LDAP、并将其用于NFSv3、NFSv4.1或双协议卷。要成功部署已启用LDAP的卷、必须在与Cloud Volumes Service 卷相同的区域建立Active Directory连接。

启用LDAP后、在特定情况下会发生以下情况。

- 如果Cloud Volumes Service 项目仅使用NFSv3或NFSv4.1、则会在Active Directory域控制器中创建一个新的计算机帐户、并且Cloud Volumes Service 中的LDAP客户端会使用计算机帐户凭据绑定到Active Directory。不会为NFS卷和默认隐藏管理共享创建SMB共享(请参见一节 ""默认隐藏共享"")已删除共享ACL。
- 如果Cloud Volumes Service 项目使用双协议卷、则只会使用为SMB访问创建的单个计算机帐户将Cloud Volumes Service 中的LDAP客户端绑定到Active Directory。不会创建其他计算机帐户。
- 如果专用SMB卷是单独创建的(在启用具有LDAP的NFS卷之前或之后)、则用于LDAP绑定的计算机帐户将与SMB计算机帐户共享。
- 如果还启用了NFS Kerberos、则会创建两个计算机帐户—一个用于SMB共享和/或LDAP绑定、一个用于NFS Kerberos身份验证。

LDAP查询

尽管LDAP绑定已加密、但LDAP查询仍会使用通用LDAP端口389以纯文本形式通过网线进行传递。目前无法在Cloud Volumes Service 中更改此众所周知的端口。因此、有权在网络中嗅探数据包的用户可以查看用户和组名称、数字ID以及组成员资格。

但是、Google Cloud VM无法嗅探其他VM的单播流量。只有主动参与LDAP流量(即能够绑定)的VM才能看到LDAP服务器的流量。有关在Cloud Volumes Service 中嗅探数据包的详细信息、请参见一节 "《数据包嗅探/跟踪注意事项》。"

LDAP客户端配置默认值

在Cloud Volumes Service 实例中启用LDAP后、默认情况下会创建一个LDAP客户端配置、其中包含特定的配置详细信息。在某些情况下、选项不适用于Cloud Volumes Service (不受支持)或不可配置。

LDAP客户端选项	功能	默认值	是否可以更改?
LDAP服务器列表	设置要用于查询的LDAP服务器名称或IP地址。这不适用于Cloud Volumes Service。而是使用Active Directory域定义LDAP服务器。	未设置	否
Active Directory域	设置用于LDAP查询的Active Directory域。Cloud Volumes Service 利用DNS中LDAP的SRV记录在域中查找LDAP服务器。	设置为在Active Directory连接中指定的Active Directory域。	否
首选Active Directory服务器	设置用于LDAP的首选Active Directory服务器。Cloud Volumes Service 不支持。而是使用Active Directory站点控制LDAP服务器选择。	未设置。	否

LDAP客户端选项	功能	默认值	是否可以更改?
使用SMB服务器凭据绑定	使用SMB计算机帐户绑定到LDAP。目前、Cloud Volumes Service 中唯一支持的LDAP绑定方法。	true	否
模式模板	用于LDAP查询的模式模板。	MS-AD-BIS	否
LDAP服务器端口	用于LDAP查询的端口号。Cloud Volumes Service 当前仅使用标准LDAP端口389。目前不支持LDAPS/端口636。	389.	否
是否已启用LDAPS	控制是否对查询和绑定使用基于安全套接字层的LDAP (SSL)。Cloud Volumes Service 目前不支持。	false	否
查询超时(秒)	查询超时。如果查询所用时间超过指定值、则查询将失败。	3.	否
最低绑定身份验证级别	支持的最低绑定级别。由于Cloud Volumes Service 使用计算机帐户进行LDAP绑定、并且默认情况下Active Directory不支持匿名绑定、因此出于安全考虑、此选项不起作用。	匿名	否
绑定 DN	使用简单绑定时用于绑定的用户/可分辨名称(DN)。Cloud Volumes Service 使用计算机帐户进行LDAP绑定、目前不支持简单绑定身份验证。	未设置	否
基础DN	用于LDAP搜索的基础DN。	用于Active Directory连接的Windows域、采用DN格式(即DC=domain、DC=local)。	否
基本搜索范围	基础DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 仅支持子树搜索。	子树	否
用户DN	定义LDAP查询的用户搜索开始位置的DN。目前Cloud Volumes Service 不支持、因此所有用户搜索均从基础DN开始。	未设置	否

LDAP客户端选项	功能	默认值	是否可以更改?
用户搜索范围	用户DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 不支持设置用户搜索范围。	子树	否
组DN	定义为LDAP查询开始组搜索的DN。目前Cloud Volumes Service 不支持、因此所有组搜索均从基础DN开始。	未设置	否
组搜索范围	组DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 不支持设置组搜索范围。	子树	否
网络组DN	定义为LDAP查询启动网络组搜索的DN。目前Cloud Volumes Service 不支持、因此所有网络组搜索均从基础DN开始。	未设置	否
网络组搜索范围	网络组DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 不支持设置网络组搜索范围。	子树	否
使用基于LDAP的start_tls	利用Start TLS通过端口389建立基于证书的LDAP连接。Cloud Volumes Service 目前不支持。	false	否
启用netgroup-by-host查找	启用按主机名查找网络组、而不是扩展网络组以列出所有成员。Cloud Volumes Service 目前不支持。	false	否
按主机的网络组DN	定义在LDAP查询中按主机搜索网络组的起始DN。Cloud Volumes Service 当前不支持按主机进行网络组。	未设置	否
netgroup-by-host搜索范围	netgroup-by-host DN搜索的搜索范围。值可以包括base、onelevel或subtree。Cloud Volumes Service 当前不支持按主机进行网络组。	子树	否

LDAP客户端选项	功能	默认值	是否可以更改?
客户端会话安全性	定义LDAP使用的会话安全级别(签名、签章或无)。如果Active Directory请求、CVS-Performance支持LDAP签名。CVS-SW不支持LDAP签名。对于这两种服务类型、目前不支持密封。	无	否
LDAP转介跟踪	使用多个LDAP服务器时、如果在第一个服务器中找不到条目、则转介跟踪功能允许客户端引用列表中的其他LDAP服务器。Cloud Volumes Service 目前不支持此功能。	false	否
组成员资格筛选器	提供了一个自定义LDAP搜索筛选器、用于从LDAP服务器查找组成员资格。Cloud Volumes Service 当前不支持。	未设置	否

使用**LDAP**进行非对称名称映射

默认情况下、Cloud Volumes Service 会双向映射用户名相同的Windows用户和UNIX用户、而无需特殊配置。只要Cloud Volumes Service 可以找到有效的UNIX用户(使用LDAP)、就会进行1：1名称映射。例如、如果使用了Windows用户`johnsmith`、则如果Cloud Volumes Service 在LDAP中找到名为`johnsmith`的UNIX用户、则该用户的名称映射将成功、则由`johnsmith`创建的所有文件/文件夹将显示正确的用户所有权、 而且、无论使用何种NAS协议、影响`johnsmith`的所有ACL都将得到遵守。这称为对称名称映射。

非对称名称映射是指Windows用户和UNIX用户身份不匹配的情况。例如、如果Windows用户`johnsmith`的UNIX身份为`jsmith`、则Cloud Volumes Service 需要了解此变体。由于Cloud Volumes Service 当前不支持创建静态名称映射规则、因此必须使用LDAP查找用户的身份以获取Windows和UNIX身份、以确保文件和文件夹的所有权以及所需权限正确无误。

默认情况下、Cloud Volumes Service 在名称映射数据库的实例的ns-switch中包含`ldap`、因此、要通过对非对称名称使用LDAP来提供名称映射功能、您只需修改某些用户/组属性以反映Cloud Volumes Service 的查找内容即可。

下表显示了为实现非对称名称映射功能、必须在LDAP中填充哪些属性。在大多数情况下、Active Directory已配置为执行此操作。

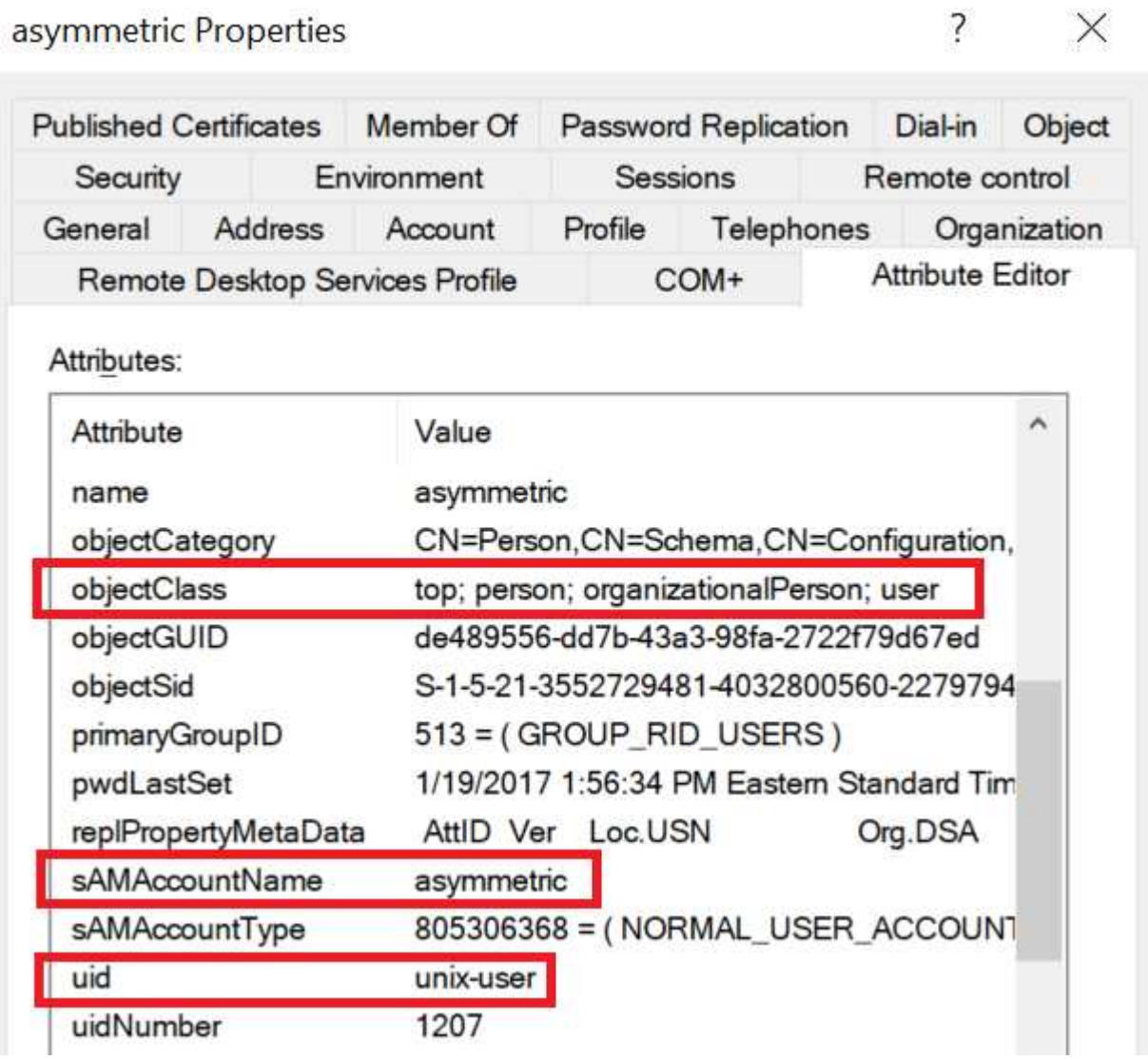
Cloud Volumes Service 属性	功能	**Cloud Volumes Service** 用于名称映射的值
Windows到UNIX对象类	指定要使用的对象类型。(即用户、组、posixAccount等)	必须包括用户(如果需要、可以包含多个其他值。)
Windows到UNIX属性	用于在创建时定义Windows用户名。Cloud Volumes Service 将此功能用于Windows到UNIX查找。	此处无需更改；sAMAccountName与Windows登录名相同。

Cloud Volumes Service 属性	功能	Cloud Volumes Service 用于名称映射的值
UID	定义UNIX用户名。	所需的UNIX用户名。

Cloud Volumes Service 当前不会在LDAP查找中使用域前缀、因此多域LDAP环境无法在LDAP命名映射查找中正常运行。

以下示例显示了一个名为`unymmetric`、UNIX名为`unix-user`的用户、以及从SMB和NFS写入文件时的行为。

下图显示了LDAP属性在Windows服务器中的外观。



在NFS客户端中、您可以查询UNIX名称、但不能查询Windows名称：

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

从NFS写入文件时、如果为`unix-user`、则NFS客户端会生成以下结果：

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

在Windows客户端中、您可以看到文件所有者已设置为正确的Windows用户：

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

相反、Windows用户`非对称`从SMB客户端创建的文件将显示正确的UNIX所有者、如以下文本所示。

SMB：

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS：

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP通道绑定

由于Windows Active Directory域控制器存在一个漏洞、 "Microsoft安全建议ADV190023" 更改DC允许LDAP绑定的方式。

对Cloud Volumes Service 的影响与对任何LDAP客户端的影响相同。Cloud Volumes Service 当前不支持通道绑定。由于Cloud Volumes Service 默认通过协商支持LDAP签名、因此LDAP通道绑定不应是问题描述。如果在启用了通道绑定的情况下绑定到LDAP时确实存在问题、请按照ADV190023中的修复步骤操作、以允许从Cloud Volumes Service 进行LDAP绑定。

DNS

Active Directory和Kerberos都依赖于DNS来进行主机名到IP/IP到主机名解析。DNS要求端口53处于打开状态。Cloud Volumes Service 不会对DNS记录进行任何修改、目前也不支持使用 "动态DNS" 在网络接口上。

您可以配置Active Directory DNS以限制哪些服务器可以更新DNS记录。有关详细信息，请参见 "保护Windows DNS的安全"。

请注意、Google项目中的资源默认使用Google Cloud DNS、而Google Cloud DNS未连接到Active Directory DNS。使用云DNS的客户端无法解析Cloud Volumes Service 返回的UNC路径。加入Active Directory域的Windows客户端已配置为使用Active Directory DNS、并且可以解析此类UNC路径。

要将客户端加入Active Directory、必须将其DNS配置为使用Active Directory DNS。或者、您也可以配置云DNS以将请求转发到Active Directory DNS。请参见 "为什么我的客户端无法解析SMB NetBIOS名称？"有关详细信息…

Cloud Volumes Service 当前不支持DNSSEC、DNS查询以纯文本形式执行。

文件访问审核

目前不支持Cloud Volumes Service。

防病毒保护

您必须在客户端的Cloud Volumes Service 中对NAS共享执行防病毒扫描。目前未将原生 防病毒与Cloud Volumes Service 集成。