安全概述—Google Cloud中的NetApp Cloud Volumes Service (CVS)

NetApp Solutions

NetApp
April 12, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/netapp-solutions/ehc/ncvs-gc-overview.html on April 12, 2024. Always check docs.netapp.com for the latest.

目录

安全概述—Google Cloud中的NetApp Cloud Volumes Service (CVS) 1
TR-4918：安全概述—Google Cloud中的NetApp Cloud Volumes Service 1
Google Cloud中的Cloud Volumes Service 如何保护您的数据安全 1
安全注意事项和攻击面 3
架构 7
NAS协议 16
服务操作 55
追加信息和联系信息 56

安全概述—Google Cloud中的NetApp Cloud Volumes Service (CVS)

TR-4918：安全概述—Google Cloud中的NetApp Cloud Volumes Service

NetApp公司Justin Parisi的Oliver Krause

文档范围

安全性、尤其是在基础架构不受存储管理员控制的云环境中、对于将数据信任到云提供商提供的服务产品至关重要。本文档概述了NetApp提供的安全产品 "Cloud Volumes Service 在Google Cloud中提供"。

目标受众

本文档的目标受众包括但不限于以下角色：

- 云提供商
- 存储管理员
- 存储架构师
- 现场资源
- 业务决策者

如果您对本技术报告的内容有任何疑问、请参见一节 ""联系我们。""

缩写	定义
CVS-SW	Cloud Volumes Service 、服务类型CVS
CVS 性能	Cloud Volume Service、服务类型CVS-Performance
PSA	

Google Cloud中的Cloud Volumes Service 如何保护您的数据安全

Google Cloud中的Cloud Volumes Service 提供了多种本机保护数据安全的方法。

安全架构和租户模式

Cloud Volumes Service 通过在不同端点之间分段服务管理(控制平面)和数据访问(数据平面)、在Google Cloud中提供一个安全的架构、这样两者都不会影响另一端(请参见一节) "Cloud Volumes Service 架构"）。它使用Google "私有服务访问" (PSA)提供服务的框架。此框架区分由NetApp提供和运营的服务生产者和客户项目中托管要访问Cloud Volumes Service 文件共享的客户端的虚拟私有云(Virtual Private Cloud、VPC)服务使用者。

在此架构中、租户(请参见第节 ""租户模式"")定义为除非用户明确连接、否则彼此完全隔离的Google Cloud项

目。通过租户、可以使用Cloud Volumes Service 卷平台将数据卷、外部名称服务以及解决方案 的其他基本部分与其他租户完全隔离。由于Cloud Volumes Service 平台是通过VPC对等连接的、因此这种隔离也会对其进行适用场景。您可以使用共享VPC在多个项目之间共享Cloud Volumes Service 卷(请参见一节) ""共享VPC""）。您可以对SMB共享和NFS导出应用访问控制、以限制可以查看或修改数据集的用户或对象。

为控制平台提供强大的身份管理功能

在进行Cloud Volumes Service 配置的控制平面中、身份管理通过进行管理 "身份访问管理(IAM)"。IAM是一项标准服务、可用于控制对Google Cloud项目实例的身份验证(登录)和授权(权限)。所有配置都使用Cloud Volumes Service API通过使用TLS 1.2加密的安全HTTPS传输执行、而身份验证则使用JWT令牌执行、以提高安全性。适用于Cloud Volumes Service 的Google控制台UI可将用户输入转换为Cloud Volumes Service API调用。

安全强化—限制攻击面

有效安全性的一部分是限制服务中可用的攻击面数。攻击面可能包括各种内容、包括空闲数据、正在传输的数据、登录信息以及数据集本身。

托管服务可从其设计中消除某些固有的攻击面。基础架构管理、如一节所述 ""服务操作"、" 由专门的团队处理、并可自动执行、以减少人员实际接触配置的次数、从而有助于减少有意和无意的错误数量。网络隔离、以便只有必要的服务才能彼此访问。加密会插入到数据存储中、只有数据平面需要Cloud Volumes Service 管理员的安全注意。通过隐藏API接口背后的大部分管理内容、可通过限制攻击面来实现安全性。

零信任模式

过去、IT安全理念一直是信任、但要进行验证、这种理念表现为仅依靠外部机制(例如防火墙和入侵检测系统)来缓解威胁。但是、攻击和违规行为演变成通过网络钓鱼、社交工程、内部威胁以及其他验证方法绕过环境中的验证、从而进入网络并造成严重破坏。

Zero Trust已成为一种全新的安全方法、目前的口号是"不信任任何内容、但仍需验证一切"。 因此、默认情况下不允许访问任何内容。此命令可通过多种方式实施、包括标准防火墙和入侵检测系统(IDS)以及以下方法：

- 强大的身份验证方法(例如AES加密的Kerberos或JWT令牌)
- 单一强身份源(例如Windows Active Directory、轻型目录访问协议(LDAP)和Google IAM)
- 网络分段和安全多租户(默认情况下仅允许租户访问)
- 采用最低特权访问策略的粒度访问控制
- 拥有数字审核和纸质跟踪的一小部分专属管理员

在Google Cloud中运行的Cloud Volumes Service 通过实施"不信任、不验证一切"的立场、遵循零信任模式。

加密

对空闲数据进行加密(请参见一节 ""空闲数据加密"") ""SMB加密"" 或NFS Kerberos 5p支持。您可以轻松了解跨区域复制传输是否受TLS 1.2加密保护(请参见一节 ""跨区域复制""）。此外、Google网络还提供加密通信(请参见一节 ""传输中的数据加密""）、以添加抵御攻击的保护层。有关传输加密的详细信息、请参见一节 ""Google Cloud network""。

数据保护和备份

安全性不仅仅是为了防止攻击。此外、还需要了解我们如何从发生的攻击中恢复。此策略包括数据保护和备

份。Cloud Volumes Service 提供了在发生中断时复制到其他区域的方法(请参见一节 ""跨区域复制"")或数据集受勒索软件攻击影响时。此外、它还可以使用将数据异步备份到Cloud Volumes Service 实例以外的位置 "Cloud Volumes Service 备份"。通过定期备份、减少安全事件所需的时间、为管理员节省资金并提高效率。

利用行业领先的**Snapshot**副本快速减少勒索软件

除了数据保护和备份之外、Cloud Volumes Service 还支持不可变的Snapshot副本(请参见一节) ""不可变的Snapshot副本"")允许从勒索软件攻击中恢复的卷(请参见一节 ""服务操作"")在发现问题描述 后数秒内完成、中断最少。恢复时间和影响取决于Snapshot计划、但您可以创建Snapshot副本、在勒索软件攻击中只能提供一小时的增量。Snapshot副本对性能和容量使用的影响微乎其微、是一种低风险、高回报的数据集保护方法。

安全注意事项和攻击面

了解如何保护数据安全的第一步是识别风险和潜在的攻击面。

其中包括(但不限于)以下内容：

- 管理和登录
- 空闲数据
- 数据正在传输
- 网络和防火墙
- 勒索软件、恶意软件和病毒

了解攻击面可以帮助您更好地保护环境。Google Cloud中的Cloud Volumes Service 已经考虑了其中许多主题、并在默认情况下实施了安全功能、而无需任何管理交互。

确保安全登录

在保护关键基础架构组件安全时、必须确保只有经过批准的用户才能登录和管理您的环境。如果不良行为者违反您的管理凭据、则他们将拥有存储区的密钥、并可以执行所需的任何操作—更改配置、删除卷和备份、创建后台或禁用Snapshot计划。

Cloud Volumes Service for Google Cloud可通过将存储即服务(StaaS)混淆来防止未经授权的管理登录。Cloud Volumes Service 由云提供商完全维护、无法从外部登录。所有设置和配置操作都是完全自动化的、因此、除了极少数情况之外、人工管理员不必与系统进行交互。

如果需要登录、Google Cloud中的Cloud Volumes Service 会保留一个非常短的可访问登录到系统的可信管理员列表、从而确保登录安全。这种关守有助于减少具有访问权限的潜在不良行为者的数量。此外、Google Cloud网络还会将系统隐藏在网络层安全的基础之上、并仅向外部环境公开所需的内容。有关Google Cloud、Cloud Volumes Service 架构的信息、请参见一节 "Cloud Volumes Service 架构。"

集群管理和升级

存在潜在安全风险的两个方面包括集群管理(如果不良者拥有管理员访问权限会发生什么情况)和升级(如果软件映像受到影响会发生什么情况)。

存储管理保护

以服务形式提供的存储可通过删除云数据中心以外的最终用户的访问权限、消除管理员面临的额外风险。而是只

为客户的数据访问平面进行配置。每个租户都管理自己的卷、任何租户都无法访问其他Cloud Volumes Service 实例。此服务通过自动化进行管理、只需一小部分受信任管理员即可通过本节所述的流程访问系统 ""服务操作"。"

CVS-Performance服务类型提供跨区域复制选项、以便在发生区域故障时为其他区域提供数据保护。在这种情况下、可以将Cloud Volumes Service 故障转移到不受影响的区域以保持数据访问。

服务升级

更新有助于保护容易受到攻击的系统。每个更新都提供了安全增强功能和错误修复、可最大限度地减少攻击面。软件更新会从中央存储库下载并进行验证、然后才允许更新、以验证是否使用了官方映像、以及升级是否不会受到不良行为者的影响。

借助Cloud Volumes Service 、更新由云提供商团队处理、通过提供精通配置和升级的专家来消除管理员团队面临的风险、这些专家已经对流程进行了自动化和全面测试。升级不会造成中断、Cloud Volumes Service 会维护最新的更新、以获得最佳的整体效果。

有关执行这些服务升级的管理员团队的信息、请参见一节 ""服务操作"。"

保护空闲数据的安全

空闲数据加密对于在磁盘被盗、退回或重新利用时保护敏感数据非常重要。Cloud Volumes Service 中的数据通过基于软件的加密在空闲时受到保护。

- Google生成的密钥用于CVS-SW。
- 对于CVS-Performance、每个卷的密钥存储在Cloud Volumes Service 内置的密钥管理器中、该管理器使用NetApp ONTAP CryptoMod生成AES-256加密密钥。CryptoMod列在CMVP FIPS 140-2验证模块列表中。请参见 "FIPS 140-2证书#4144"。

自2021年11月起、CVS-Performance提供了客户管理的预览加密(CMEK)功能。通过此功能、您可以使用Google密钥管理服务(KMS)中托管的每个项目、每个区域的主密钥对每个卷的密钥进行加密。您可以通过Kms连接外部密钥管理器。

有关如何为KMS配置CVS-Performance的详细信息、 "请参见Cloud Volumes Service 文档"。

有关架构的详细信息、请参见一节 "Cloud Volumes Service 架构。"

保护传输中的数据安全

除了保护空闲数据之外、当数据在Cloud Volumes Service 实例与客户端或复制目标之间传输时、您还必须能够保护数据的安全。Cloud Volumes Service 通过使用加密方法(例如使用Kerberos进行SMB加密、对数据包进行签名/密封以及对数据传输进行端到端加密的NFS Kerberos 5p)为通过NAS协议传输的数据提供加密。

Cloud Volumes Service 卷的复制使用TLS 1.2、它会利用AES-GCM加密方法。

默认情况下、大多数不安全的传输中协议(例如telnet、NDMP等)都处于禁用状态。但是、Cloud Volumes Service 不会对DNS进行加密(不支持DNS安全)、应尽可能使用外部网络加密进行加密。请参见一节 ""传输中的数据加密"" 有关保护传输中数据的详细信息、请参见。

有关NAS协议加密的信息、请参见一节 ""NAS协议"。"

NAS权限的用户和组

在云中保护数据的一部分工作涉及到正确的用户和组身份验证、其中、访问数据的用户会作为环境中的实际用户进行验证、而组包含有效用户。这些用户和组可为存储系统中的文件和文件夹提供初始共享和导出访问权限以及权限验证。

Cloud Volumes Service 对SMB共享和Windows模式权限使用基于Active Directory的标准Windows用户和组身份验证。该服务还可以利用UNIX身份提供程序、例如用于UNIX用户的LDAP以及用于NFS导出的组、NFSv4 ID验证、Kerberos身份验证和NFSv4 ACL。

> 目前、Cloud Volumes Service 仅支持Active Directory LDAP功能。

检测、防止和缓解勒索软件、恶意软件和病毒

勒索软件、恶意软件和病毒是管理员面临的持久威胁、企业组织始终将检测、预防和缓解这些威胁作为头等大事。关键数据集上的一个勒索软件事件可能会导致数百万美元的损失、因此您可以尽最大可能降低风险。

尽管Cloud Volumes Service 目前不包括防病毒保护或等原生 检测或预防措施 "自动检测勒索软件"、通过启用定期Snapshot计划、可以快速从勒索软件事件中恢复。Snapshot副本是指向文件系统中已更改块的不可变和只读指针、它们接近瞬时、对性能的影响最小、并且仅在更改或删除数据时才会占用空间。您可以为Snapshot副本设置计划、使其与所需的可接受恢复点目标(RPO)/恢复时间目标(RTO)相匹配、并且每个卷最多可保留1、024个Snapshot副本。

Snapshot支持包括在Cloud Volumes Service 中、无需额外费用(对于Snapshot副本所保留的更改块/数据收取的数据存储费用除外)、如果发生勒索软件攻击、可以在攻击发生之前使用它回滚到Snapshot副本。快照还原只需几秒钟即可完成、然后您可以恢复正常提供数据。有关详细信息，请参见 "适用于勒索软件的NetApp解决方案"。

要防止勒索软件影响您的业务、需要采用多层方法、其中包括以下一项或多项：

- 端点保护
- 通过网络防火墙防止外部威胁
- 检测数据异常
- 对关键数据集进行多个备份(现场和异地)
- 定期对备份进行还原测试
- 不可变的只读NetApp Snapshot副本
- 关键基础架构的多因素身份验证
- 系统登录的安全审核

此列表远非详尽无遗、但在应对潜在的勒索软件攻击时、是一个理想的蓝图。Google Cloud中的Cloud Volumes Service 提供了多种方法来防止勒索软件事件并减少其影响。

不可变的Snapshot副本

Cloud Volumes Service 本机提供不可变的只读Snapshot副本、这些副本会按照可自定义的计划创建、以便在数据删除或整个卷受到勒索软件攻击时快速进行时间点恢复。根据Snapshot计划和RTO /RO的保留期限、将Snapshot还原到先前的正常Snapshot副本速度非常快、并可最大程度地减少数据丢失。Snapshot技术对性能的影响可以忽略不计。

由于Cloud Volumes Service 中的Snapshot副本为只读副本、因此、除非勒索软件在未经注意的情况下激增到数据集中、并且已为受勒索软件感染的数据创建Snapshot副本、否则它们不会受到勒索软件的感染。因此、您还必须考虑根据数据异常检测勒索软件。Cloud Volumes Service 目前不提供本机检测功能、但您可以使用外部监控软件。

备份和还原

Cloud Volumes Service 提供标准NAS客户端备份功能(例如通过NFS或SMB进行备份)。

- CVS-Performance可跨区域卷复制到其他CVS-Performance卷。有关详细信息，请参见 "卷复制" 在Cloud Volumes Service 文档中。
- CVS-SW提供服务本机卷备份/还原功能。有关详细信息，请参见 "云备份" 在Cloud Volumes Service 文档中。

卷复制可提供源卷的精确副本、以便在发生灾难(包括勒索软件事件)时快速进行故障转移。

跨区域复制

通过CVS-Performance、您可以在NetApp控制的后端服务网络上使用用于在Google网络上运行复制的特定接口使用TLS1.2 AES 256 GCM加密功能、在Google Cloud区域之间安全地复制卷、以实现数据保护和归档使用情形。主(源)卷包含活动生产数据、并复制到二级(目标)卷、以提供主数据集的精确副本。

初始复制会传输所有块、但更新仅传输主卷中发生更改的块。例如、如果将主卷上的1 TB数据库复制到二级卷、则在初始复制时会传输1 TB的空间。如果该数据库中有几百行(假设有几MB)在初始化和下次更新之间发生变化、则只有包含更改行的块才会复制到二级(几MB)。这有助于确保传输时间保持较短、并降低复制成本。

文件和文件夹上的所有权限都会复制到二级卷、但共享访问权限(例如导出策略和规则或SMB共享和共享ACL)必须单独处理。在发生站点故障转移时、目标站点应利用相同的名称服务和Active Directory域连接、以便一致地处理用户和组身份和权限。如果发生灾难、您可以使用二级卷作为故障转移目标、方法是中断复制关系、从而将二级卷转换为读写卷。

卷副本为只读副本、可为异地数据提供不可变的副本、以便在病毒已感染数据或勒索软件已对主数据集进行加密的情况下快速恢复数据。只读数据不会加密、但如果主卷受到影响并发生复制、则受感染的块也会进行复制。您可以使用不受影响的旧Snapshot副本进行恢复、但SLA可能会超出承诺的RTO /RRPO范围、具体取决于检测到攻击的速度。

此外、您还可以通过在Google Cloud中进行跨区域复制(CRR)管理来防止恶意管理操作、例如卷删除、Snapshot删除或Snapshot计划更改。这是通过创建自定义角色来实现的、这些角色会将卷管理员分隔开、这些管理员可以删除源卷、但不会中断镜像、因此无法从无法执行任何卷操作的CRR管理员中删除目标卷。请参见 "安全注意事项" 在Cloud Volumes Service 文档中、了解每个管理员组允许的权限。

Cloud Volumes Service 备份

虽然Cloud Volumes Service 可提供较高的数据持久性、但外部事件可能会导致发生原因 数据丢失。在发生病毒或勒索软件等安全事件时、备份和恢复对于及时恢复数据访问至关重要。管理员可能会意外删除Cloud Volumes Service 卷。或者、用户只希望将数据的备份版本保留数月、而在卷中保留额外的Snapshot副本空间将成为一项成本难题。虽然Snapshot副本应该是在过去几周内保留备份版本以恢复其丢失的数据的首选方式、但它们位于卷中、如果卷消失、它们将丢失。

出于所有这些原因、NetApp Cloud Volumes Service 均通过提供备份服务 "Cloud Volumes Service 备份"。

Cloud Volumes Service 备份会在Google云存储(GCS)上生成卷的副本。它只会备份存储在卷中的实际数据、而不会备份可用空间。它始终以增量形式运行、也就是说、它会一次性传输卷内容、并在上继续备份更改的数据。

与具有多个完整备份的传统备份概念相比、它可以节省大量备份存储、从而降低成本。由于与卷相比、备份空间的每月价格更低、因此、它是延长备份版本的理想之选。

用户可以使用Cloud Volumes Service 备份将任何备份版本还原到同一区域内的相同或不同卷。如果删除了源卷、则备份数据会保留下来、需要单独管理(例如删除)。

Cloud Volumes Service 备份内置在Cloud Volumes Service 中作为选项。用户可以通过激活每个卷的Cloud Volumes Service 备份来确定要保护的卷。请参见 "Cloud Volumes Service 备份文档" 有关备份的信息、请参见 "支持的最大备份版本数"、计划和 "定价"。

项目的所有备份数据都存储在GCS存储分段中、此存储分段由服务管理、用户无法看到。每个项目使用不同的存储分段。目前、存储分段与Cloud Volumes Service 卷位于同一区域、但正在讨论更多选项。有关最新状态、请参见文档。

从Cloud Volumes Service 存储分段到GCS的数据传输使用具有HTTPS和TLS1.2的服务内部Google网络。数据会使用Google管理的密钥在空闲时进行加密。

要管理Cloud Volumes Service 备份(创建、删除和还原备份)、用户必须具有 "角色/netappcloudvolumes.admin" 角色。

架构

概述

信任云解决方案 的一部分是了解架构及其安全保护方式。本节将介绍Google中Cloud Volumes Service 架构的不同方面、以帮助缓解对数据安全保护的潜在担忧、并指出可能需要执行其他配置步骤才能实现最安全的部署。

Cloud Volumes Service 的通用架构可细分为两个主要组件：控制平面和数据平面。

控制面板

Cloud Volumes Service 中的控制平台是由Cloud Volumes Service 管理员和NetApp原生 自动化软件管理的后端基础架构。此平台对最终用户完全透明、并包括网络、存储硬件、软件更新等、可帮助为Cloud Volumes Service 等驻留在云中的解决方案 提供价值。

数据平面

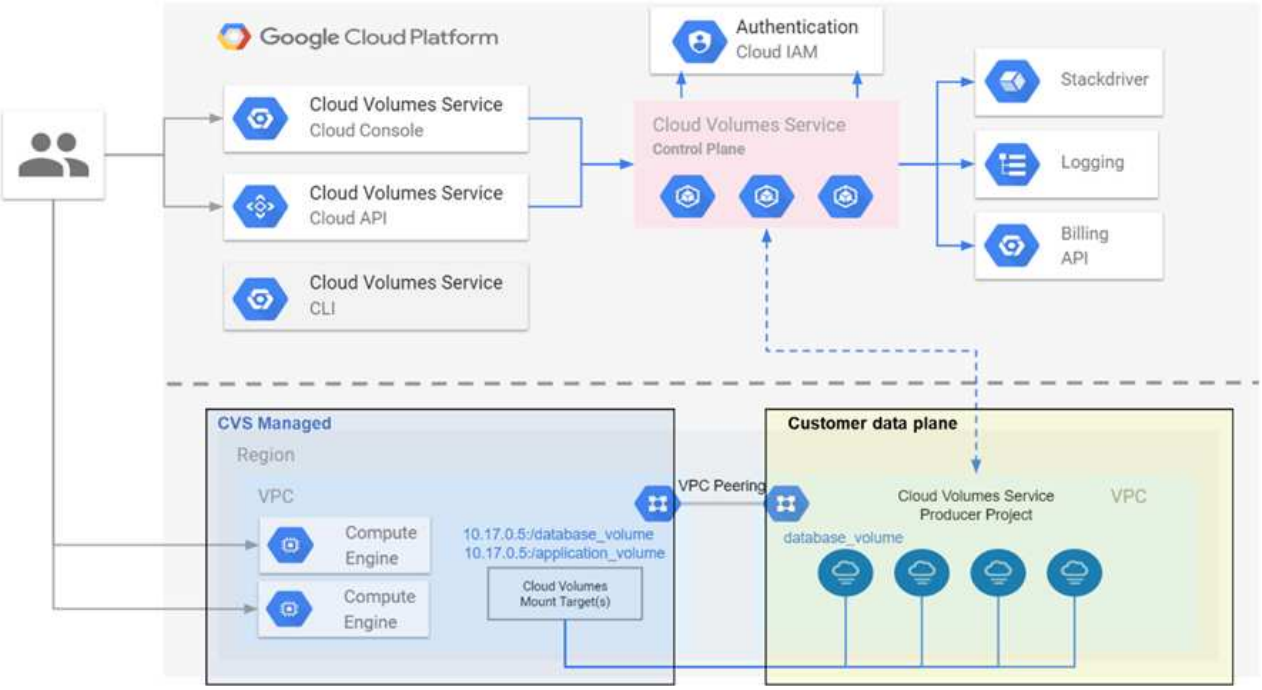
Cloud Volumes Service 中的数据平面包括实际数据卷和整体Cloud Volumes Service 配置(例如访问控制、Kerberos身份验证等)。数据平面完全由Cloud Volumes Service 平台的最终用户和使用者控制。

每个平面的安全保护和管理方式各不相同。以下各节将从Cloud Volumes Service 架构概述开始介绍这些差异。

Cloud Volumes Service 架构

Cloud Volumes Service 采用与其他Google Cloud原生 服务类似的方式、例如CloudSQL、Google Cloud VMware引擎(GCVE)和文件存储库 "Google PSA" 交付服务。在PSA中、服务构建在服务生产者项目中、该项目使用 "VPC网络对等" 以连接到服务使用者。服务生产者由NetApp提供和运营、服务使用者是客户项目中的VPC、负责托管要访问Cloud Volumes Service 文件共享的客户端。

下图、引用自 "架构部分" 显示了Cloud Volumes Service 文档的概要视图。



虚线上方的部分显示服务的控制平面、控制卷生命周期。虚线下方的部分显示数据平面。左侧蓝色框表示用户VPC (服务使用者)、右侧蓝色框表示NetApp提供的服务生产者。两者均通过VPC对等连接。

租户模式

在Cloud Volumes Service 中、各个项目被视为唯一租户。这意味着、卷、Snapshot副本等操作是按项目执行的。换言之、所有卷均归在中创建它们的项目所有、默认情况下、只有该项目才能管理和访问其中的数据。这被视为服务的控制面板视图。

共享 vPC

在数据平面视图中、Cloud Volumes Service 可以连接到共享VPC。您可以在托管项目中或连接到共享VPC的某个服务项目中创建卷。连接到此共享VPC的所有项目(主机或服务)均可访问网络层(TCP/IP)上的卷。由于共享VPC上具有网络连接的所有客户端都可能通过NAS协议访问数据、因此必须使用单个卷上的访问控制(例如、NFS导出的用户/组访问控制列表(ACL)和主机名/IP地址)来控制谁可以访问数据。

每个客户项目最多可以将Cloud Volumes Service 连接到五个vPC。在控制平面上、您可以通过该项目管理所有已创建的卷、无论这些卷连接到哪个VPC。在数据平面上、VPC彼此隔离、每个卷只能连接到一个VPC。

对各个卷的访问由特定协议(NFS/SMB)访问控制机制控制。

换言之、在网络层、连接到共享VPC的所有项目都能够看到卷、而在管理端、控制平面仅允许所有者项目查看卷。

VPC服务控制

VPC服务控制功能可围绕连接到互联网且可在全球访问的Google Cloud服务建立访问控制边界。这些服务可通过用户身份提供访问控制、但不能限制发出哪些网络位置请求。VPC服务控制通过引入限制对定义的网络的访问的功能来缩小这一差距。

Cloud Volumes Service 数据平面不会连接到外部Internet、而是连接到具有明确定义的网络边界(边界)的私有VPC。在该网络中、每个卷都使用特定于协议的访问控制。任何外部网络连接均由Google Cloud项目管理员明确创建。但是、控制平面不提供与数据平面相同的保护、任何人都可以使用有效凭据("JWT令牌"）。

简而言之、Cloud Volumes Service 数据平面可提供网络访问控制功能、无需支持VPC服务控制、也不明确使用VPC服务控制。

数据包嗅探/跟踪注意事项

数据包捕获对于解决网络问题或其他问题(例如NAS权限、LDAP连接等)非常有用、但也可以恶意使用数据包捕获来获取有关网络IP地址、MAC地址、用户和组名称以及端点上使用的安全级别的信息。由于配置Google Cloud网络、VPC和防火墙规则的方式、如果没有用户登录凭据或、则很难获取对网络数据包的不必要访问 "JWT令牌" 迁移到云实例。只有端点(如虚拟机(VM))才可以捕获数据包、只有VPC内部的端点才可以捕获数据包、除非使用共享VPC和/或外部网络通道/IP转发明确允许外部流量传输到端点。无法嗅探客户端外部的流量。

使用共享VPC时、使用NFS Kerberos和/或进行动态加密 "SMB加密" 可以屏蔽从跟踪中获取的大部分信息。但是、某些流量仍以纯文本形式发送、例如 "DNS" 和 "LDAP查询"。下图显示了从Cloud Volumes Service 发起的纯文本LDAP查询中捕获的数据包以及公开的潜在标识信息。Cloud Volumes Service 中的LDAP查询当前不支持加密或基于SSL的LDAP。如果Active Directory请求、CVS-Performance支持LDAP签名。CVS-SW不支持LDAP签名。

> unixUserPassword由LDAP查询、不会以纯文本形式发送、而是以盐哈希形式发送。默认情况下、Windows LDAP不会填充unixUserPassword字段。只有在需要利用Windows LDAP通过LDAP交互式登录到客户端时、才需要此字段。Cloud Volumes Service 不支持对实例进行交互式LDAP登录。

下图显示了通过AUTH_SYS捕获NFS旁边的NFS Kerberos对话中的数据包捕获。请注意、跟踪中提供的信息在这两者之间有何不同、以及启用动态加密如何为NAS流量提供更高的整体安全性。

IP addresses of the NFS client and CVS instance

Genericized NFS call/reply

No.	Time	Source	Destination	Protocol	Length	Info
380	9.218014	10.193.67.225	10.193.67.219	NFS	346	V4 Call (Reply In 381)
381	9.218480	10.193.67.219	10.193.67.225	NFS	426	V4 Reply (Call In 380)
382	9.218641	10.193.67.225	10.193.67.219	NFS	370	V4 Call (Reply In 397)
397	9.369035	10.193.67.219	10.193.67.225	NFS	458	V4 Reply (Call In 382)

```
> Frame 381: 426 bytes on wire (3408 bits), 426 bytes captured (3408 bits)
> Ethernet II, Src: IntelCor_7f:da:bc (90:e2:ba:7f:da:bc), Dst: VMware_a0:2c:2d (00:50:56:a0:2c:2d)
> Internet Protocol Version 4, Src: 10.193.67.219, Dst: 10.193.67.225
> Transmission Control Protocol, Src Port: 2049, Dst Port: 738, Seq: 6305, Ack: 6569, Len: 360
> Remote Procedure Call, Type:Reply XID:0xef5e998d
v GSS-Wrap
    Length: 300
    GSS Data: 050407ff0000000000000000025913451ee1d43d298cf3031…
  > krb5_blob: 050407ff0000000000000000025913451ee1d43d298cf3031…
v Network File System
    [Program Version: 4]
    [V4 Procedure: COMPOUND (1)]
```

GSS wrapped NFS calls/replies with no other identifying information

IP addresses of the NFS client and CVS instance

Detailed NFS call types and file handle information

No.	Time	Source	Destination	Protocol	Length	Info
33	0.958480	10.193.67.201	10.193.67.204	NFS	458	V4 Reply (Call In 32) OPEN StateID: 0x0481
34	0.958784	10.193.67.204	10.193.67.201	NFS	306	V4 Call (Reply In 35) SETATTR FH: 0x6c07918a
35	0.959284	10.193.67.201	10.193.67.204	NFS	358	V4 Reply (Call In 34) SETATTR

```
> Opcode: PUTFH (22)
> Opcode: SETATTR (34)
v Opcode: GETATTR (9)
    Status: NFS4_OK (0)
  v Attr mask[0]: 0x0010011a (Type, Change, Size, FSID, FileId)
    > reqd_attr: Type (1)
    > reqd_attr: Change (3)
    > reqd_attr: Size (4)
    > reqd_attr: FSID (8)
    v reco_attr: FileId (20)
        fileid: 9232254136597092620
  v Attr mask[1]: 0x00b0a03a (Mode, NumLinks, Owner, Owner_Group, Space_Used, Time_Access, Time_Metadata, Time_Modify, Mounted_on_FileId)
    v reco_attr: Mode (33)
      > mode: 0644, Name: Unknown, Read permission for owner, Write permission for owner, Read permission for group, Read permission for others
    > reco_attr: NumLinks (35)
    v reco_attr: Owner (36)
      > fattr4_owner: root@NTAP.LOCAL
    v reco_attr: Owner_Group (37)
      > fattr4_owner_group: root@NTAP.LOCAL
    > reco_attr: Space_Used (45)
    > reco_attr: Time_Access (47)
    > reco_attr: Time_Metadata (52)
    > reco_attr: Time_Modify (53)
    > reco_attr: Mounted_on_FileId (55)
```

File ID

Permission information

Owner and group ID strings

VM网络接口

攻击者可能会尝试的一个技巧是、在中向虚拟机添加新的网络接口卡(Network Interface Card、NIC) "混杂模式"(端口镜像)或在现有NIC上启用混杂模式以嗅探所有流量。在Google Cloud中、添加新的NIC需要完全关闭虚拟机、这样会创建警报、因此攻击者无法在无人察觉的情况下执行此操作。

此外、NIC根本无法设置为混杂模式、并会在Google Cloud中触发警报。

控制平面架构

对Cloud Volumes Service 执行的所有管理操作均通过API完成。集成到GCP云控制台的Cloud Volumes Service 管理也使用Cloud Volumes Service API。

身份和访问管理

身份和访问管理 ("IAM")是一项标准服务、可用于控制对Google Cloud项目实例的身份验证(登录)和授权(权限)。Google IAM可提供权限授权和删除的完整审核跟踪。目前、Cloud Volumes Service 不提供控制平面审核。

授权/权限概述

IAM为Cloud Volumes Service 提供内置的粒度权限。您可以找到 "在此填写粒度权限列表"。

IAM还提供了两个预定义角色、称为`netappcloudvolumes.admin`和`netappcloudvolumes.viewer`。可以将这些角色分配给特定用户或服务帐户。

分配适当的角色和权限以允许IAM用户管理Cloud Volumes Service。

使用粒度权限的示例包括：

- 仅使用获取/列表/创建/更新权限构建自定义角色、以使用户无法删除卷。
- 使用仅具有`snapshot.*`权限的自定义角色创建用于构建应用程序一致的Snapshot集成的服务帐户。
- 构建自定义角色、将`volumereplication *`委派给特定用户。

服务帐户

通过脚本或进行Cloud Volumes Service API调用 "Terraform"、您必须创建一个具有`角色/netappcloudvolumes.admin`角色的服务帐户。您可以使用此服务帐户通过两种不同的方式生成对Cloud Volumes Service API请求进行身份验证所需的JWT令牌：

- 生成JSON密钥并使用Google API从该密钥派生JWT令牌。这是最简单的方法、但涉及手动密钥(JSON密钥)管理。
- 使用 … "服务帐户模拟" 使用`Roles/iam.serviceAccountTokenCreator`。代码(脚本、Terraform等)运行 "应用程序默认凭据" 并模拟服务帐户以获取其权限。此方法反映了Google的安全最佳实践。

请参见 "正在创建服务帐户和私钥" 有关详细信息、请参见Google云文档。

Cloud Volumes Service API

Cloud Volumes Service API使用基于REST的API、并使用HTTPS (TLSv1.2)作为底层网络传输。您可以找到最新的API定义 "此处" 以及有关如何使用API的信息、请参见 "Google云文档中的Cloud Volumes API"。

API端点由NetApp使用标准HTTPS (TLSv1.2)功能进行操作和保护。

JWT令牌

使用JWT承载令牌对API进行身份验证 ("RFC-7519"）。必须使用Google Cloud IAM身份验证获取有效的JWT令牌。必须通过提供服务帐户JSON密钥从IAM提取令牌来完成此操作。

审核日志记录

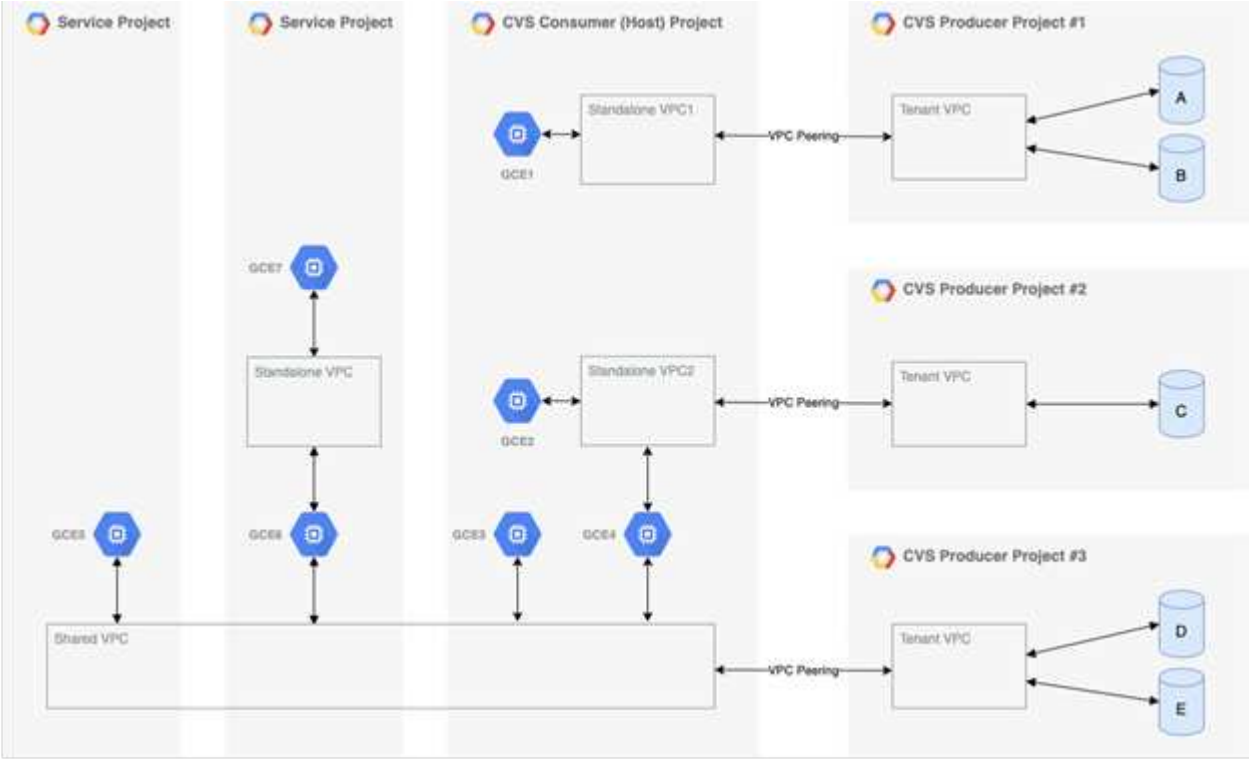
目前、没有用户可访问的控制平面审核日志。

数据平台架构

适用于Google Cloud的Cloud Volumes Service 利用了Google Cloud "私有服务访问" 框架。在此框架中、用户可以连接到Cloud Volumes Service。此框架像使用其他Google Cloud服务一样使用服务网络和VPC对等结构、确保租户之间完全隔离。

有关适用于Google Cloud的Cloud Volumes Service 架构概述、请参见 "适用于Cloud Volumes Service 的架构"。

用户vPC (独立或共享)与托管卷的Cloud Volumes Service 托管租户项目中的vPC建立对等关系。



上图显示了一个项目(中间为CVS使用者项目)、其中三个VPC网络连接到Cloud Volumes Service 、多个计算引擎VM (GCE1-7)共享卷：

- VC1允许GCE1访问卷A和B
- VPC2允许GCE2和GCE4访问卷C
- 第三个VPC网络是一个共享VPC、与两个服务项目共享。它允许GCE3、GCE4、GCE5和GCE6访问卷D和E只有CVS-Performance服务类型的卷才支持共享VPC网络。

> GCE7无法访问任何卷。

可以在Cloud Volumes Service 中对传输中(使用Kerberos和/或SMB加密)和空闲数据进行加密。

传输中的数据加密

传输中的数据可以在NAS协议层进行加密、Google Cloud网络本身也会进行加密、如以下各节所述。

Google Cloud网络

Google Cloud按中所述在网络级别对流量进行加密 "传输中加密" 在Google文档中。如"云卷服务架构"一节所述、Cloud Volumes Service 是通过NetApp控制的PSA生产商项目交付的。

对于CVS-SW、生产者租户运行Google VM来提供服务。Google会自动对用户VM和Cloud Volumes Service VM之间的流量进行加密。

虽然在网络层上、CVS-Performance的数据路径未完全加密、但NetApp和Google会结合使用 "IEEE 802.1AE加密(MAC秒)"， "封装" (数据加密)和受物理限制的网络、用于保护Cloud Volumes Service CVS-Performance服务类型与Google Cloud之间传输的数据。

NAS协议

NFS和SMB NAS协议可在协议层提供可选的传输加密。

SMB加密

"SMB加密" 为SMB数据提供端到端加密、并防止数据在不可信的网络上被窃听。您可以同时为客户端/服务器数据连接(仅适用于具有SMB3.x功能的客户端)和服务器/域控制器身份验证启用加密。

启用SMB加密后、不支持加密的客户端将无法访问共享。

Cloud Volumes Service 支持使用RC4 HMAC、AES-128-CTS-HMAC-SHA1和AES-256-CTS-HMAC-SHA1安全密码进行SMB加密。SMB协商到服务器支持的最高加密类型。

NFSv4.1 Kerberos

对于NFSv4.1、CVS-Performance可提供Kerberos身份验证、如中所述 "RFC7530"。您可以按卷启用Kerberos。

当前最强的Kerberos加密类型为AES-256-CTS-HMAC-SHA1。NetApp Cloud Volumes Service 支持适用于NFS的AES-256-CTS-HMAC-SHA1、AES-128-CTS-HMAC-SHA1、DES3和DES。它还支持对CIFS/SMB流量使用ARCFOUR-HMAC (RC4)、但不支持对NFS使用。

Kerberos为NFS挂载提供了三种不同的安全级别、这些安全级别可以选择Kerberos安全性的强程度。

根据RedHat的要求 "通用挂载选项" 文档：

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

一般来说、Kerberos安全级别必须执行的操作越多、性能就越差、因为客户端和服务器会花费时间对发送的每个数据包的NFS操作进行加密和解密。许多客户端和NFS服务器都支持将AES-NI负载分流到CPU、以获得更好的整体体验、但Kerberos 5p (完全端到端加密)的性能影响远远大于Kerberos 5 (用户身份验证)的影响。

下表显示了每个级别在安全性和性能方面的差异。

安全级别	安全性	性能
NFSv3—系统	• 安全性最低；纯文本、包含数字用户ID/组ID • 能够查看UID、GID、客户端IP地址、导出路径、文件名、 数据包捕获中的权限	• 最适合大多数情况
NFSv4.x—系统	• 比NFSv3 (客户端ID、名称字符串/域字符串匹配)更安全、但仍为纯文本 • 能够查看UID、GID、客户端IP地址、名称字符串、域ID、 数据包捕获中的导出路径、文件名和权限	• 适用于顺序工作负载(如VM、数据库、大型文件) • 错误、文件数量较多/元数据较高(较差30-50%)
NFS—krb5	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/组的UID/GID • 请求访问挂载的用户需要有效的Kerberos票证(通过用户名/密码或手动密钥选项卡交换)；票证将在指定时间段后过期、用户必须重新进行身份验证才能进行访问 • 对于NFS操作或挂载/端口映射程序/NLM等辅助协议、不进行加密(可以查看导出路径、IP地址、文件句柄、权限、文件名、数据包捕获中的atime/mtime)	• 大多数情况下最适合使用Kerberos；比AUTH_SYS更差

安全级别	安全性	性能
NFS—krb5i	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/组的UID/GID • 请求访问挂载的用户需要有效的Kerberos票证(通过用户名/密码或手动密钥选项卡交换)；票证将在指定时间段后过期、用户必须重新进行身份验证才能访问 • 对于NFS操作或挂载/端口映射程序/NLM等辅助协议、不进行加密(可以查看导出路径、IP地址、文件句柄、权限、文件名、数据包捕获中的atime/mtime) • 每个数据包都会添加Kerberos GSS校验和、以确保不会截获任何数据包。如果校验和匹配、则允许对话。	• 优于krb5p、因为NFS有效负载未加密；与krb5相比、唯一增加的开销是完整性校验和。krb5i的性能不会比krb5差得多、但会有所下降。
NFS—krb5p	• 对每个NFS数据包中的凭据进行Kerberos加密—在GSS包装程序中的RPC调用中封装用户/组的UID/GID • 请求访问挂载的用户需要有效的Kerberos票证(通过用户名/密码或手动密钥表交换)；票证将在指定时间段后过期、用户必须重新进行身份验证才能进行访问 • 所有NFS数据包有效负载都使用GSS包装程序进行加密(在数据包捕获中看不到文件句柄、权限、文件名、atime/mtime)。 • 包括完整性检查。 • NFS操作类型是可见的(fsINFO、access、getattr等)。 • 辅助协议(挂载、端口映射、NLM等)未加密-(可以查看导出路径、IP地址)	• 安全级别的性能最差；krb5p必须对更多内容进行加密/解密。 • 对于文件数量较多的工作负载、性能优于使用NFSv4.x时的krb5p。

在Cloud Volumes Service 中、配置的Active Directory服务器用作Kerberos服务器和LDAP服务器(从RFC2307兼容模式查找用户身份)。不支持其他Kerberos或LDAP服务器。NetApp强烈建议您在Cloud Volumes Service 中使用LDAP进行身份管理。有关NFS Kerberos在数据包捕获中的显示方式的信息、请参见一节 "《数据包嗅探/跟踪注意事项》。"

空闲数据加密

Cloud Volumes Service 中的所有卷都使用AES-256加密进行空闲加密、这意味着写入介质的所有用户数据都将进行加密、并且只能使用每个卷的密钥进行解密。

- 对于CVS-SW、使用Google生成的密钥。
- 对于CVS-Performance、每个卷的密钥存储在Cloud Volumes Service 中内置的密钥管理器中。

自2021年11月起、提供了预览客户管理的加密密钥(CMEK)功能。这样、您就可以使用中托管的每个项目的每个区域主密钥对每个卷的密钥进行加密 "Google密钥管理服务(KMS)。" 您可以通过Kms连接外部密钥管理器。

有关为KMS配置CVS-Performance的信息、请参见 "设置客户管理的加密密钥"。

防火墙：

Cloud Volumes Service 公开多个TCP端口以提供NFS和SMB共享：

- "NFS访问所需的端口"
- "SMB访问所需的端口"

此外、SMB、包含Kerberos的LDAP NFS以及双协议配置都需要访问Windows Active Directory域。Active Directory连接必须为 "已配置" 按区域计算。Active Directory域控制器(DC)通过使用进行标识 "基于DNS的DC发现" 使用指定的DNS服务器。将使用返回的任何DC。可以通过指定Active Directory站点来限制符合条件的域控制器列表。

Cloud Volumes Service 会通过分配给的CIDR范围内的IP地址进行访问 `gcloud compute address` 命令 "加入Cloud Volumes Service"。您可以使用此CIDR作为源地址来为Active Directory域控制器配置入站防火墙。

Active Directory域控制器必须 "将端口公开到此处所述的Cloud Volumes Service CIDR中"。

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：

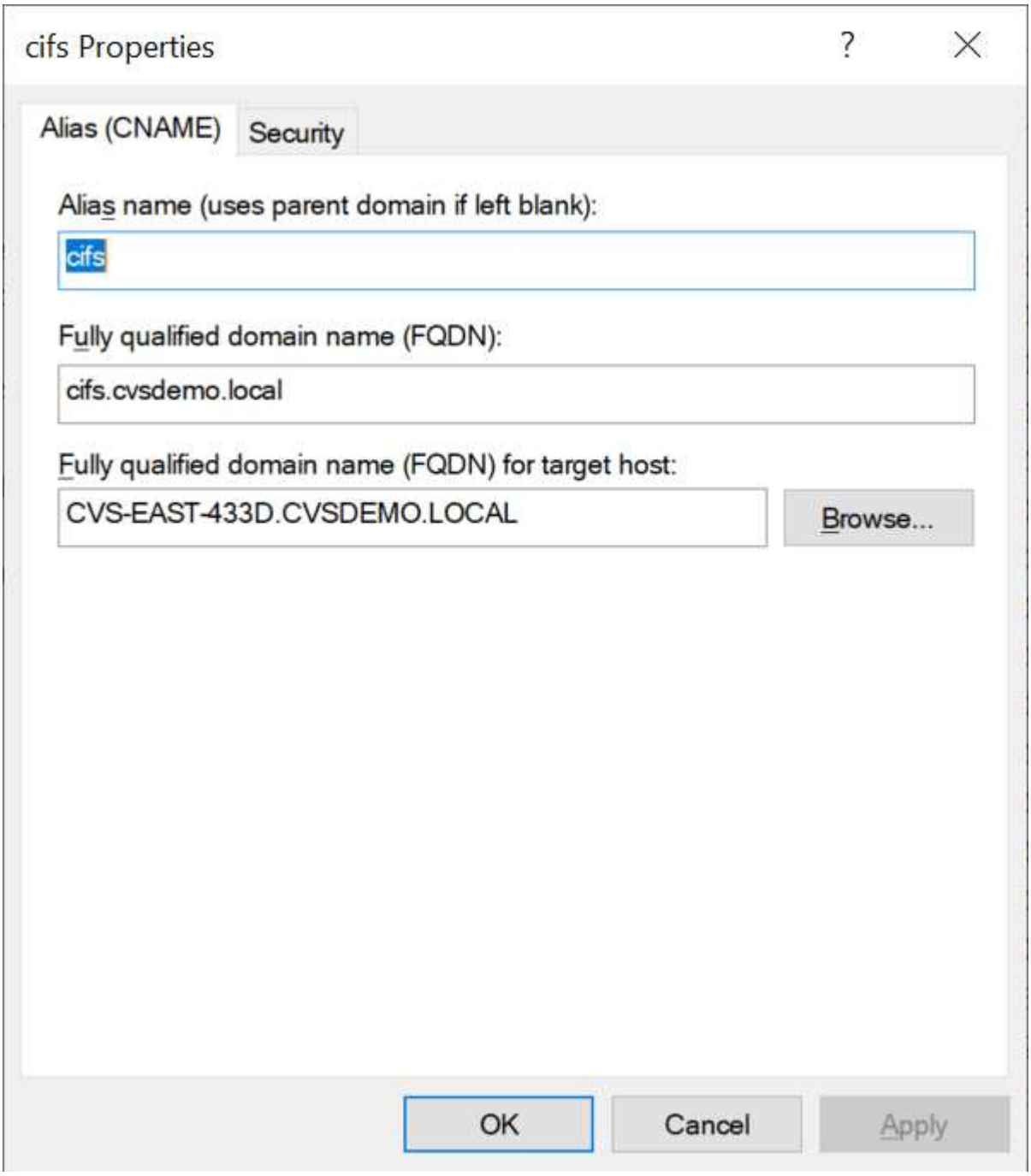
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address: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

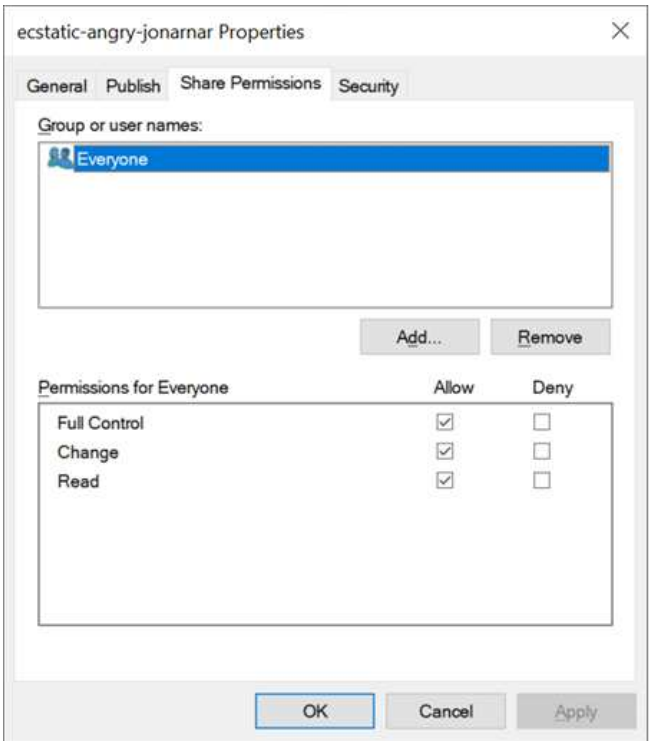
共享权限

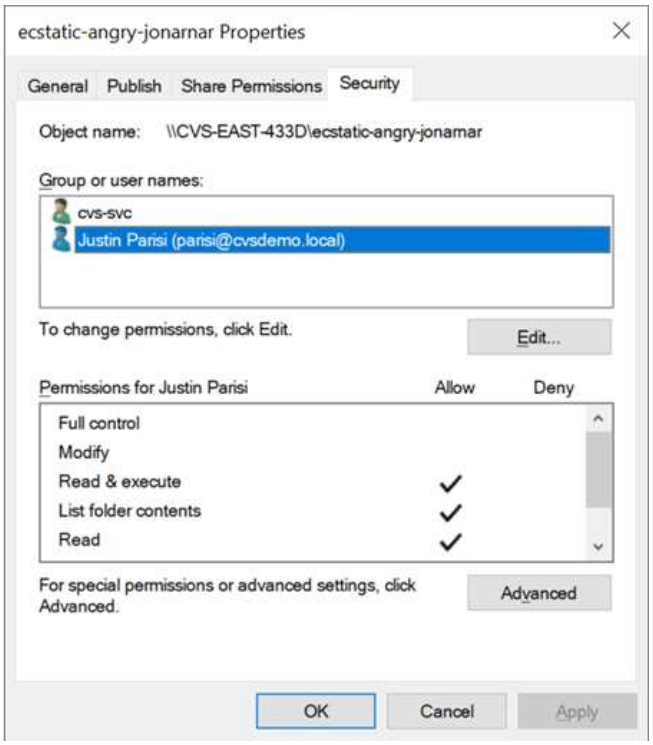
共享权限比NTFS权限更常规(仅限读取/更改/完全控制)、并可控制SMB共享的初始条目、类似于NFS导出策略规则的工作方式。

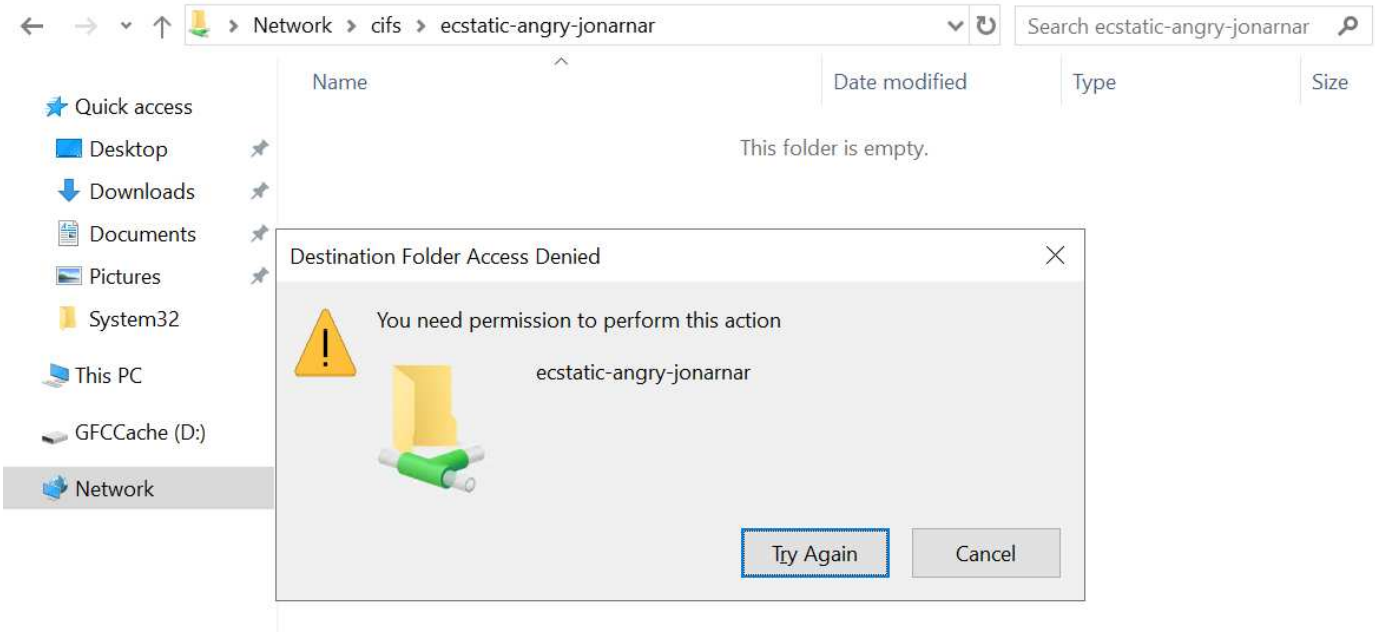
虽然NFS导出策略规则通过IP地址或主机名等基于主机的信息来控制访问、但SMB共享权限可以通过使用共享ACL中的用户和组ACE来控制访问。您可以从Windows客户端或Cloud Volumes Service 管理UI设置共享ACL。

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。

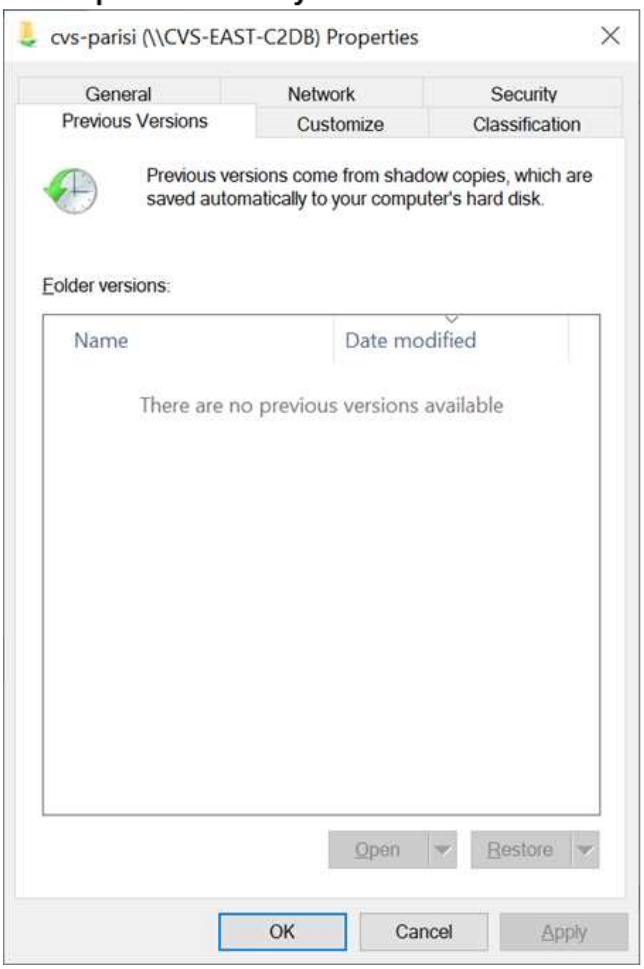
SMB共享安全功能

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。

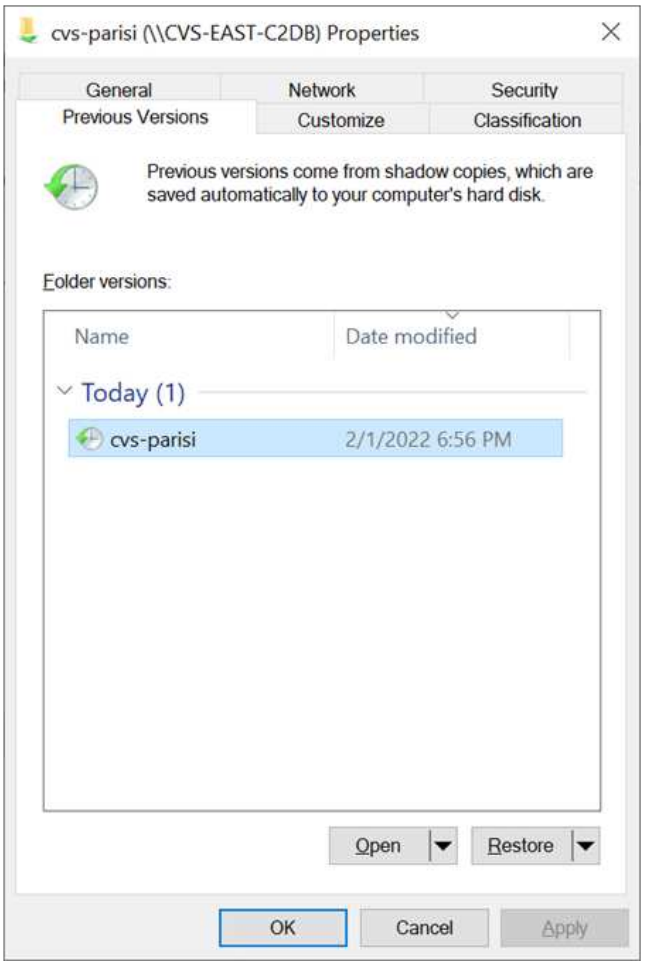
其中一些选项取决于Cloud Volumes Service 级别(性能或软件)、选项包括：

- *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

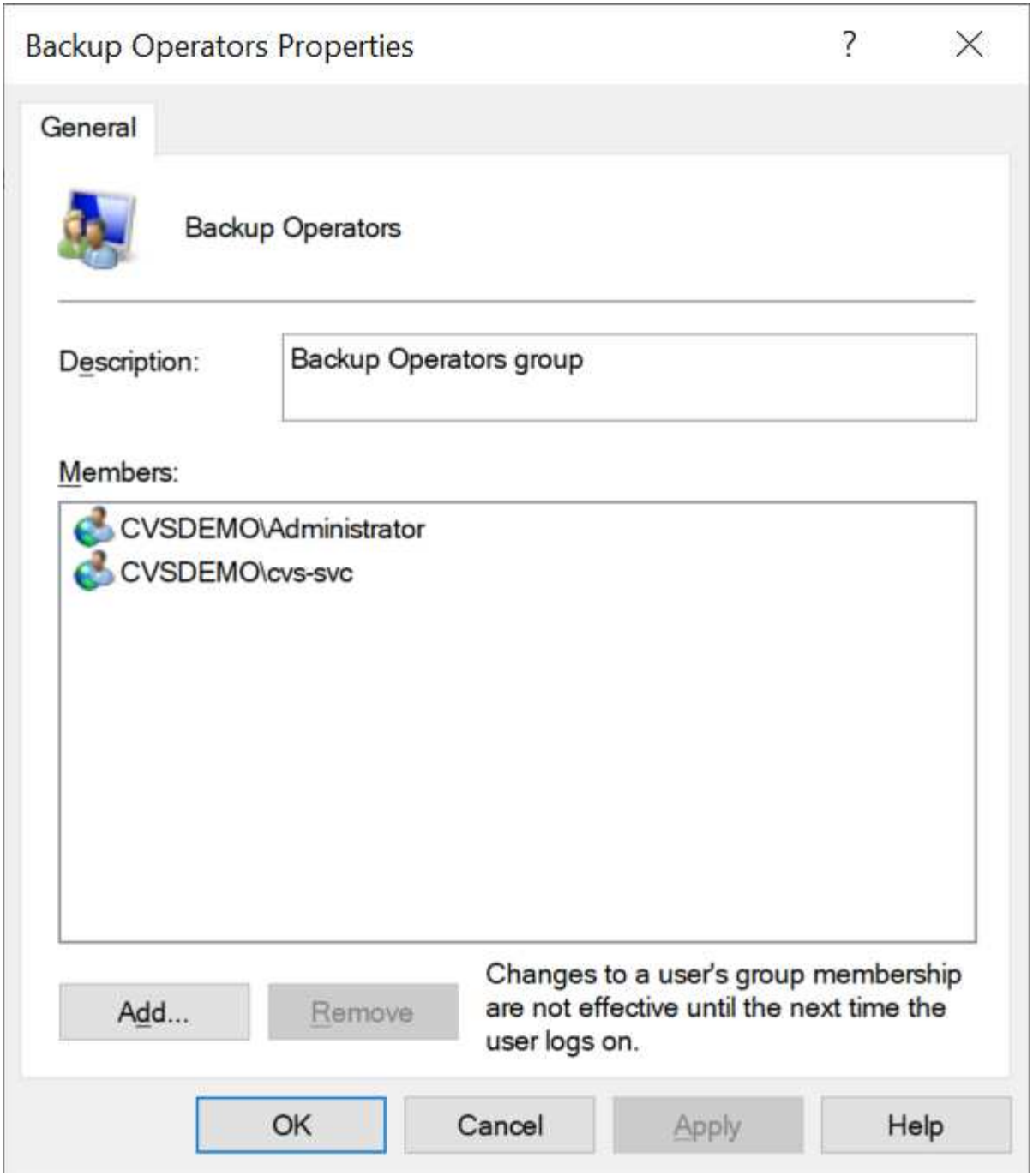
Security Privilege Users

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。

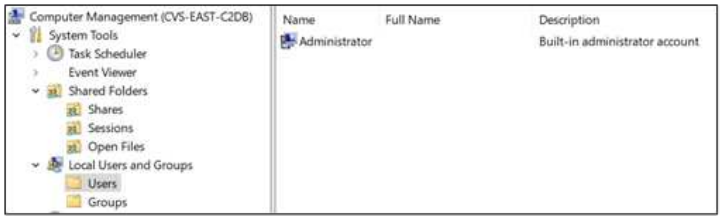


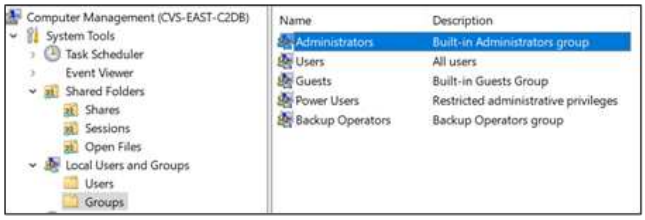
下表显示了默认BUILTIN组的列表以及默认添加的用户/组。

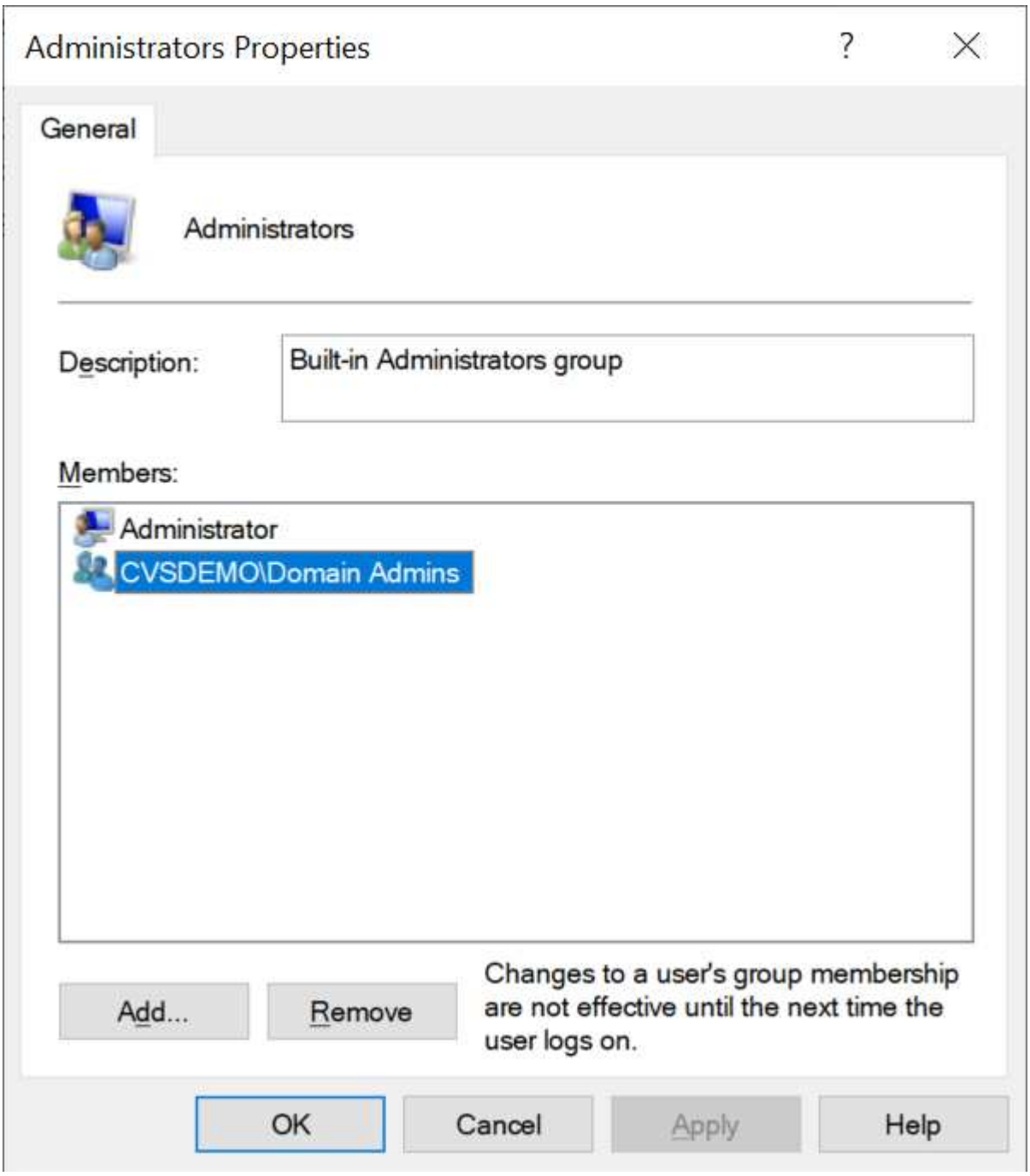
本地/**BUILTIN**组	默认成员
BUILTIN\Administrators *	域\域管理员
BUILTIN\Backup Operators*	无
BUILTIN\guests	域\域子系统
BUILTIN\Power Users	无
BUILTIN\Domain用户	域\域用户

*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

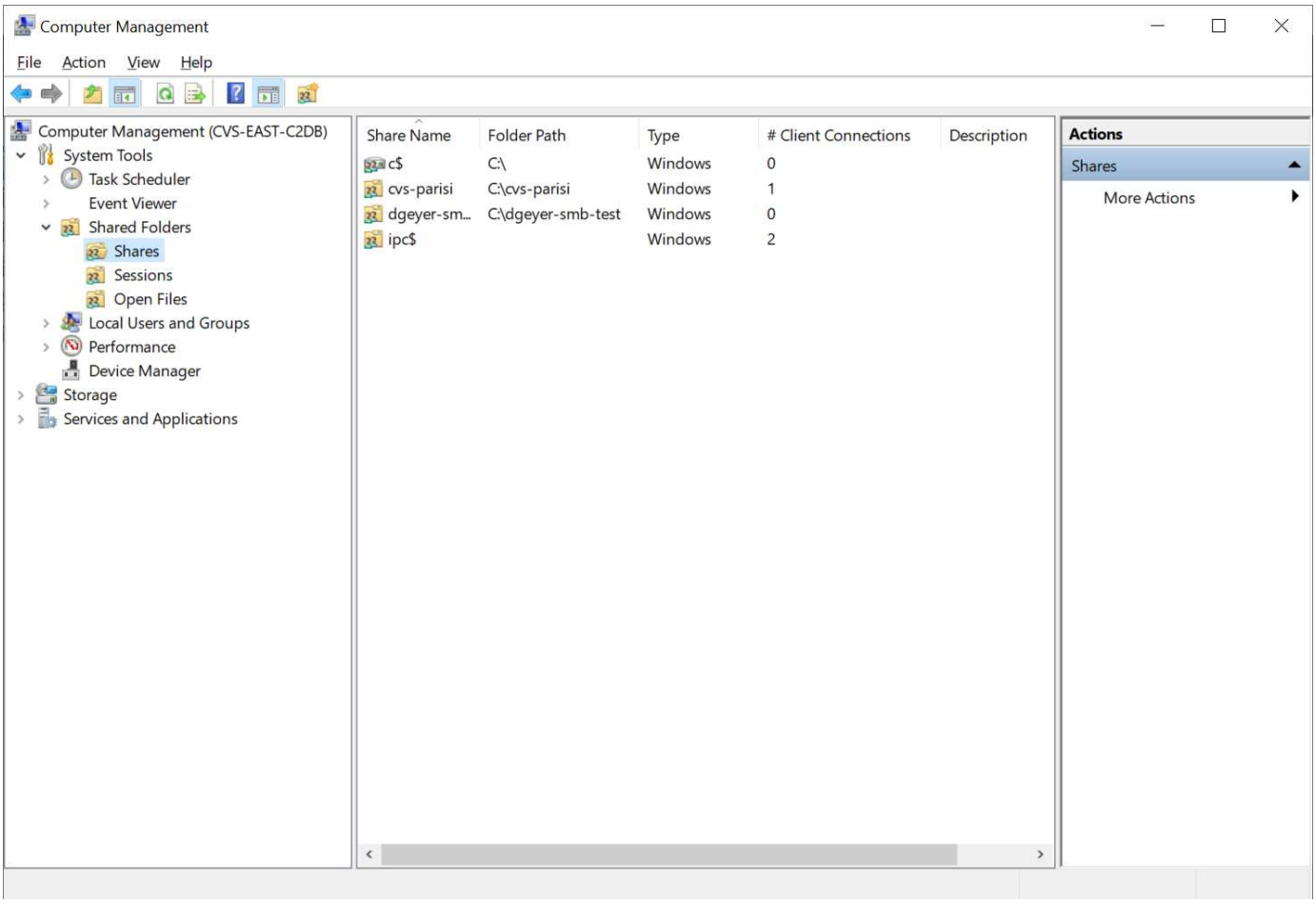
通过Cloud Volumes Service 中的SMB访问、您可以连接到计算机管理MMC、从而可以查看共享、管理共享ACL、以及查看/管理SMB会话和打开的文件。

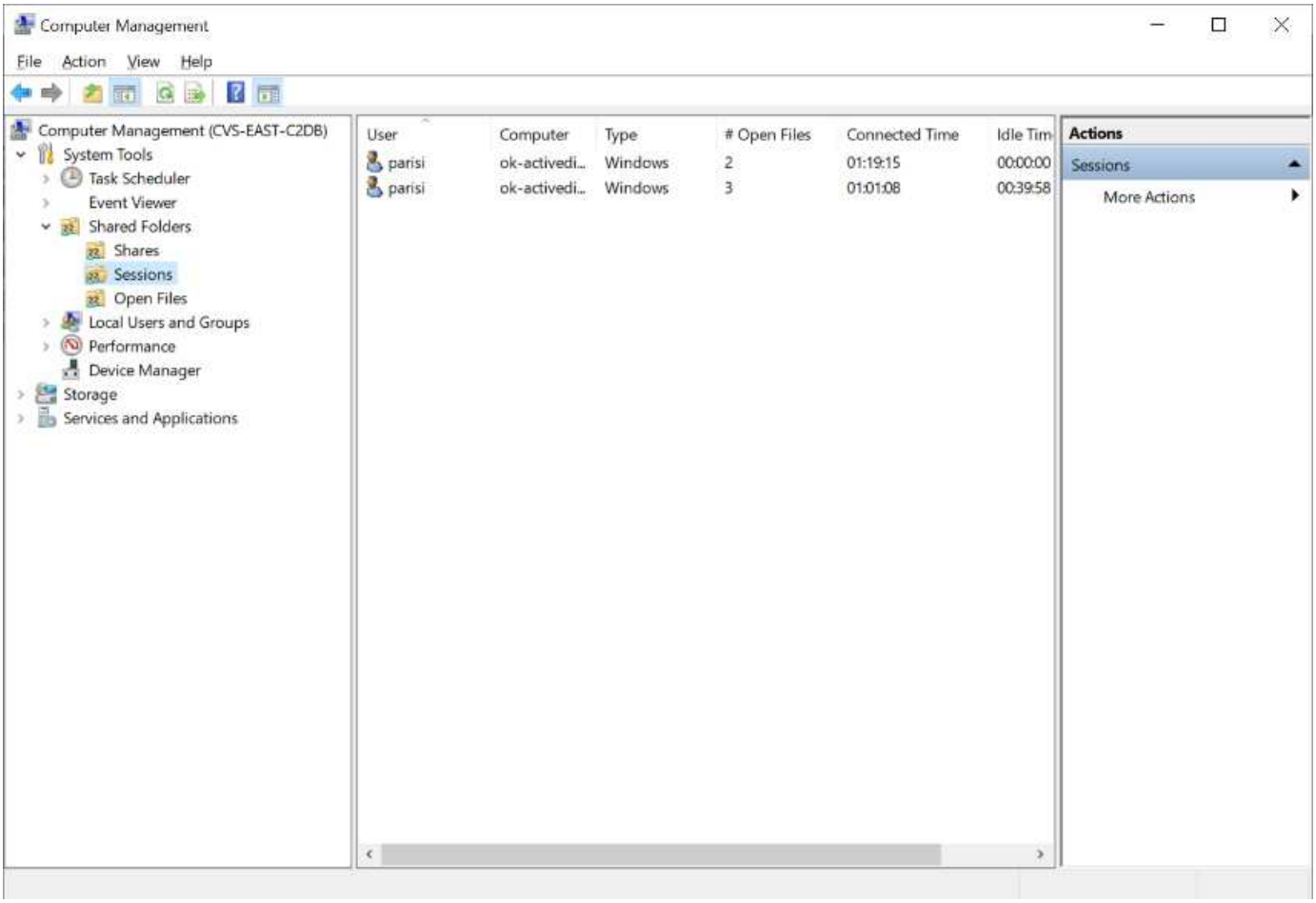
要使用MMC在Cloud Volumes Service 中查看SMB共享和会话、登录的用户当前必须是域管理员。其他用户可以通过MMC查看或管理SMB服务器、并在尝试查看Cloud Volumes Service SMB实例上的共享或会话时收到"您没有权限"对话框。

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。

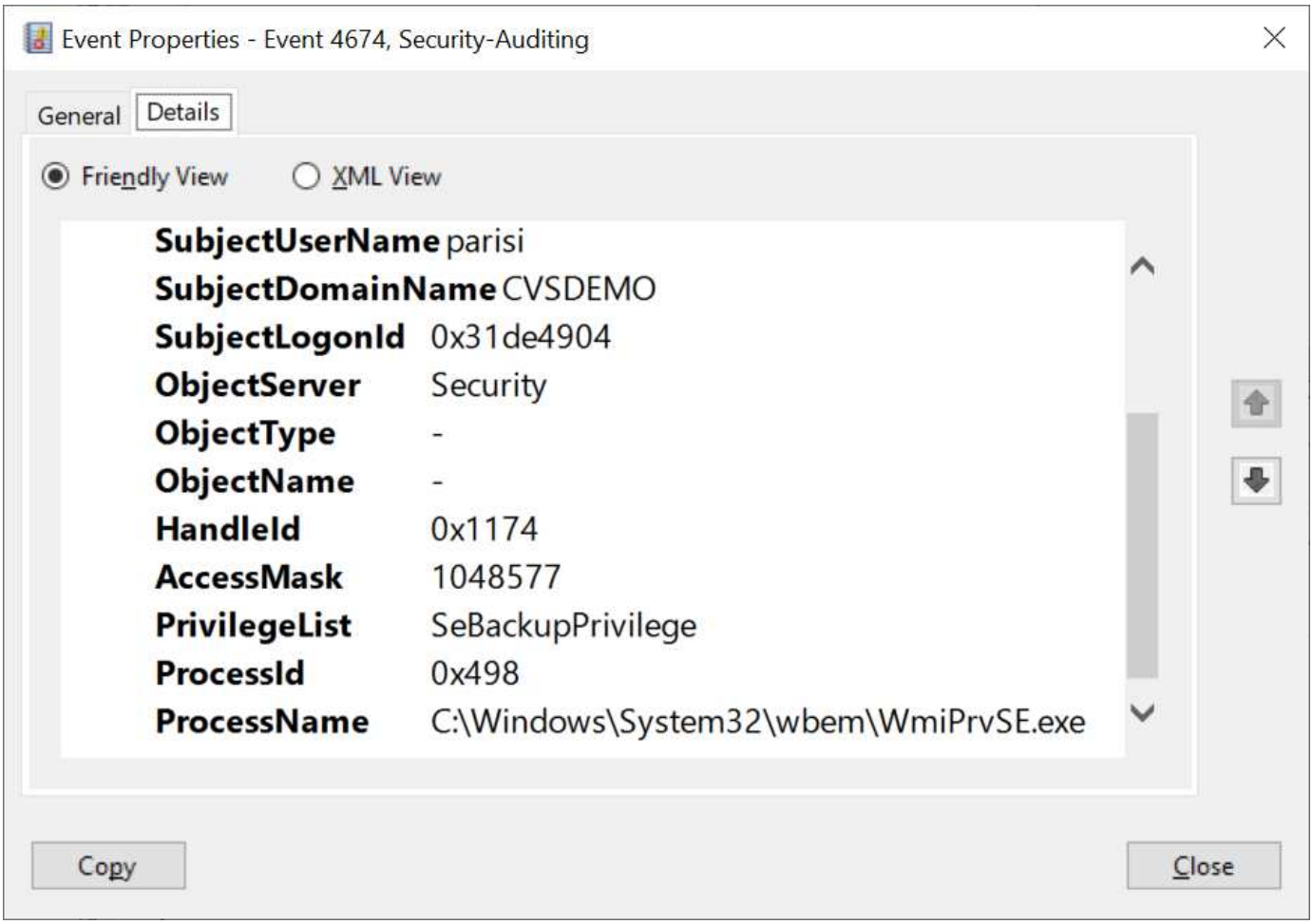
Region

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
仅限NFSv3 Kerberos	Windows Active Directory：* KDC * DNS * LDAP

Configuration	需要依赖关系
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
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)。

属性	功能
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
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

LDAP客户端选项	功能	默认值	是否可以更改?
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。

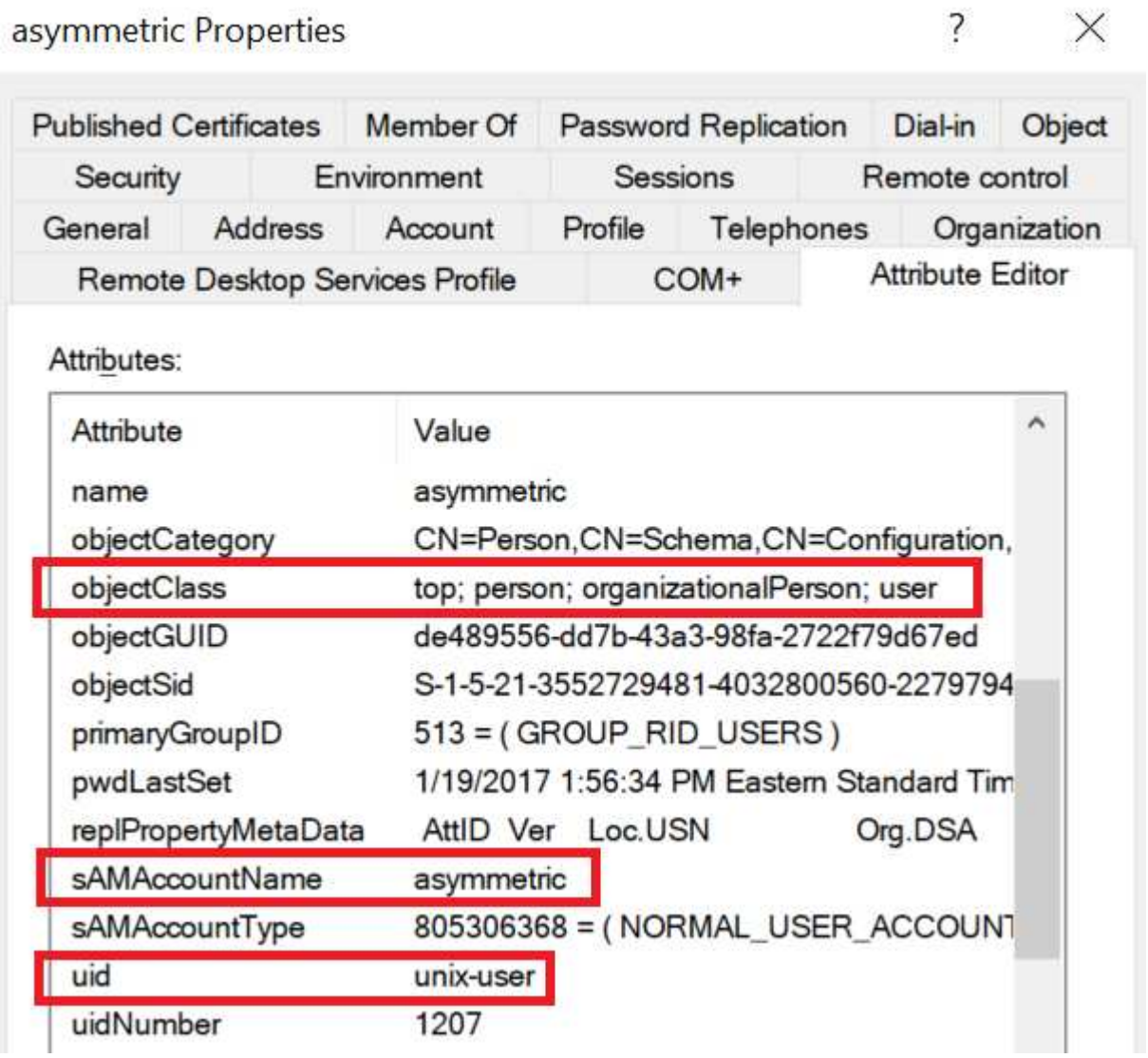
Cloud Volumes Service 属性	功能	**Cloud Volumes Service** 用于名称映射的值
Windows到UNIX对象类	指定要使用的对象类型。(即用户、组、posixAccount等)	必须包括用户(如果需要、可以包含多个其他值。)
Windows到UNIX属性	用于在创建时定义Windows用户名。Cloud Volumes Service 将此功能用于Windows到UNIX查找。	此处无需更改；sAMAccountName与Windows登录名相同。

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。

服务操作

Cloud Volumes Service 团队负责管理Google Cloud中的后端服务、并使用多种策略来保护平台安全并防止不必要的访问。

每个客户都获得自己的唯一子网、默认情况下、该子网的访问会与其他客户隔离、而Cloud Volumes Service 中的每个租户都获得自己的命名空间和VLAN以实现整体数据隔离。用户通过身份验证后、服务交付引擎(SDE)只能读取特定于该租户的配置数据。

物理安全性

经过适当的预先批准后、只有现场工程师和具有NetApp徽标的现场支持工程师(Field Support Engineer、FSE)才能访问固定框架和机架进行物理工作。不允许进行存储和网络管理。只有这些现场资源才能执行硬件维护任务。

对于现场工程师、将为工作说明书(SOW)提交一个服务单、其中包括机架ID和设备位置(RU)、所有其他详细信息均包含在服务单中。对于NetApp现场服务工程师、必须向Colo提交现场访问服务单、此服务单应包含访客的详细信息、日期和时间、以供审核。FSE的SOW会在内部传达给NetApp。

运营团队

Cloud Volumes Service 运营团队由生产工程和云卷服务站点可靠性工程师(SRE)以及NetApp现场支持工程师和硬件合作伙伴组成。所有运营团队成员都获得了在Google Cloud中工作的认证、并为提交的每个服务单维护详细的工作记录。此外、我们还制定了严格的变更控制和批准流程、以确保对每项决策进行适当审查。

SRE团队负责管理控制平台以及如何将数据从UI请求路由到Cloud Volumes Service 中的后端硬件和软件。SRE团队还负责管理系统资源、例如卷和索引节点最大值。不允许SRES与客户数据进行交互或访问客户数据。此外、SRES还可以与退回材料授权(Return Material Authorizations、RMA)进行协调、例如为后端硬件请求新磁盘

或内存更换请求。

客户责任

Cloud Volumes Service 的客户负责管理其组织的Active Directory和用户角色管理以及卷和数据操作。客户可以具有管理角色、并可以使用NetApp和Google Cloud提供的两个预定义角色(管理员和查看器)将权限委派给同一Google Cloud项目中的其他最终用户。

管理员可以将客户项目中的任何VPC与客户确定合适的Cloud Volumes Service 建立对等关系。客户有责任管理对其Google Cloud Marketplace订阅的访问权限、并管理有权访问数据平面的VPC。

恶意SRE保护

可能会出现的一个问题是、Cloud Volumes Service 如何防止出现恶意SRE或SRE凭据受到损坏的情况?

只能由有限数量的SRE人员访问生产环境。管理权限进一步限制为少数经验丰富的管理员。我们的安全信息和事件管理(Cloud Volumes Service)威胁情报平台会记录任何人在生产环境中执行的所有操作、并检测到基线异常或可疑活动。因此、在对Cloud Volumes Service 后端造成过多损坏之前、可以跟踪和缓解恶意操作。

卷生命周期

Cloud Volumes Service 仅管理服务中的对象、而不管理卷中的数据。只有访问卷的客户端才能管理数据、ACL、文件所有者等。这些卷中的数据会在空闲时进行加密、并且只能由Cloud Volumes Service 实例的租户访问。

Cloud Volumes Service 的卷生命周期为create-update-delete。卷会保留卷的Snapshot副本、直到删除卷为止、只有经过验证的Cloud Volumes Service 管理员才能删除Cloud Volumes Service 中的卷。当管理员请求删除卷时、还需要输入卷名称来验证删除操作。删除卷后、该卷将消失、无法恢复。

如果Cloud Volumes Service 合同终止、NetApp会在特定时间段后标记要删除的卷。在该时间段到期之前、您可以根据客户的请求恢复卷。

认证

适用于Google Cloud的Cloud Volumes Services目前已通过ISO/IEC 27001：2013和ISO/IEC 27018：2019标准的认证。该服务最近还收到了其SOC2 I类证明报告。有关NetApp对数据安全和隐私的承诺的信息、请参见 "合规性：数据安全和数据隐私"。

GDPR

我们的许多公司都承诺遵守GDPR并遵守隐私规定 "客户合同"、例如我们的 "客户数据处理附录"、其中包括 "标准合同条款" 由欧盟委员会提供。我们还会在隐私政策中做出这些承诺、并以我们公司行为准则中规定的核心价值为后盾。

追加信息和联系信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 适用于Cloud Volumes Service 的Google Cloud文档

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google私有服务访问

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp 产品文档

  "https://www.netapp.com/support-and-training/documentation/"

- 加密验证模块计划—NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- 适用于勒索软件的NetApp解决方案

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616： ONTAP 中的 NFS Kerberos

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

请联系我们

请告诉我们如何改进本技术报告。

联系我们、电子邮件地址为：mailto：doccomments@netapp.com^ doccomments@netapp.com。在主题行中包含技术报告4918。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本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。