开始使用 **Google Cloud**

Cloud Volumes ONTAP

NetApp
February 26, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/storage-management-cloud-volumes-ontap/task-getting-started-gcp.html on February 26, 2026. Always check docs.netapp.com for the latest.

目录

开始使用 Google Cloud

Google Cloud 中的Cloud Volumes ONTAP快速入门

只需几个步骤即可在 Google Cloud 中开始使用Cloud Volumes ONTAP 。

1 创建控制台代理

如果你没有 "控制台代理"但是，你需要创建一个。 "了解如何在 Google Cloud 中创建控制台代理"

请注意，如果您想在没有互联网访问的子网中部署Cloud Volumes ONTAP ，则需要手动安装控制台代理并访问在该控制台代理上运行的NetApp Console。 "了解如何在没有互联网访问的地方手动安装控制台代理"

2 规划您的配置

控制台提供符合您的工作负载要求的预配置包，或者您可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

"了解有关规划配置的更多信息" 。

3 设置网络

1. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 如果您计划启用数据分层， "为私有 Google 访问配置Cloud Volumes ONTAP子网" 。
3. 如果您正在部署 HA 对，请确保您有四个 VPC，每个 VPC 都有自己的子网。
4. 如果您使用共享 VPC，请向控制台代理服务帐户提供_计算网络用户_角色。
5. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

   如果您在没有互联网访问的位置部署Cloud Volumes ONTAP，则不需要执行此步骤。

"了解有关网络要求的更多信息" 。

4 设置服务帐户

Cloud Volumes ONTAP需要 Google Cloud 服务帐户来实现两个目的。第一个是当你启用"数据分层"将冷数据分层到 Google Cloud 中的低成本对象存储。第二个是当你启用 "NetApp Backup and Recovery"将卷备份到低成本的对象存储。

您可以设置一个服务帐户并将其用于两种用途。服务帐户必须具有*存储管理员*角色。

"阅读分步说明" 。

5 启用 **Google Cloud API**

"在项目中启用 Google Cloud API"。 "这些 API"，您可能已经在创建 Console 代理时启用了这些功能，这些功能是在 Google Cloud 中部署 Cloud Volumes ONTAP 所必需的。

6 使用控制台启动**Cloud Volumes ONTAP**

单击“添加系统”，选择您想要部署的系统类型，然后完成向导中的步骤。"阅读分步说明" 。

相关链接

- "创建控制台代理"
- "在 Linux 主机上安装控制台代理软件"
- "控制台代理的 Google Cloud 权限"

在 Google Cloud 中规划您的Cloud Volumes ONTAP配置

在 Google Cloud 中部署Cloud Volumes ONTAP时，您可以选择符合您的工作负载要求的预配置系统，也可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

选择**Cloud Volumes ONTAP**许可证

Cloud Volumes ONTAP有多种许可选项。每个选项都可以让您选择符合您需求的消费模式。

- "了解Cloud Volumes ONTAP的许可选项"
- "了解如何设置许可"

选择支持的区域

大多数 Google Cloud 区域都支持Cloud Volumes ONTAP 。 "查看支持区域的完整列表" 。

选择支持的机器类型

Cloud Volumes ONTAP支持多种机器类型，具体取决于您选择的许可证类型。

"Google Cloud 中 Cloud Volumes ONTAP 支持的配置"

了解存储限制

Cloud Volumes ONTAP系统的原始容量限制与许可证相关。额外的限制会影响聚合和卷的大小。在规划配置时您应该注意这些限制。

"Google Cloud 中 Cloud Volumes ONTAP 的存储限制"

在 Google Cloud 中调整系统大小

调整Cloud Volumes ONTAP系统的大小可以帮助您满足性能和容量要求。在选择机器类型、磁盘类型和磁盘大小时，您应该注意几个关键点：

机器类型

请查看支持的机器类型。 "Cloud Volumes ONTAP发行说明"然后查看谷歌提供的关于每种受支持机器类型的详细信息。将您的工作负载要求与机器类型的 vCPU 和内存数量相匹配。请注意，每个 CPU 核心都会提高网络性能。

请参阅以下内容以了解更多详细信息：

- "Google Cloud 文档：N1 标准机器类型"
- "Google Cloud 文档：性能"

磁盘类型

为Cloud Volumes ONTAP创建卷时，您需要选择Cloud Volumes ONTAP用于磁盘的底层云存储。磁盘类型可以是以下任意一种：

- 区域 *SSD* 持久磁盘：SSD 持久磁盘最适合需要高随机 IOPS 率的工作负载。
- 区域平衡持久磁盘：这些 SSD 通过提供每 GB 较低的 IOPS 来平衡性能和成本。
- 区域标准持久磁盘：标准持久磁盘经济实惠，可以处理顺序读/写操作。

  欲了解更多详情，请参阅 "Google Cloud 文档：区域持久磁盘（标准和 SSD）"。

磁盘大小

部署Cloud Volumes ONTAP系统时，您需要选择初始磁盘大小。之后，您可以让NetApp Console为您管理系统的容量，但如果您想自己构建聚合，请注意以下事项：

- 聚合中的所有磁盘必须具有相同的大小。
- 确定所需的空间，同时考虑性能。
- 持久磁盘的性能会随着磁盘大小和系统可用的 vCPU 数量自动扩展。

  请参阅以下内容以了解更多详细信息：

  - "Google Cloud 文档：区域持久磁盘（标准和 SSD）"
  - "Google Cloud 文档：优化持久磁盘和本地 SSD 性能"

查看默认系统磁盘

除了用户数据的存储之外，控制台还购买了Cloud Volumes ONTAP系统数据（启动数据、根数据、核心数据和NVRAM）的云存储。出于规划目的，在部署Cloud Volumes ONTAP之前查看这些详细信息可能会有所帮助。

- "查看 Google Cloud 中Cloud Volumes ONTAP系统数据的默认磁盘" 。
- "Google Cloud 文档：云配额概述"

  Google Cloud Compute Engine 对资源使用实施配额，因此您应确保在部署Cloud Volumes ONTAP之前尚未达到限制。

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

收集网络信息

在 Google Cloud 中部署 Cloud Volumes ONTAP 时，您需要指定有关虚拟网络的详细信息。您可以使用工作表从管理员处收集信息。

单节点系统的网络信息

Google Cloud 信息	你的价值
地区	
分区	
VPC 网络	
子网	
防火墙策略（如果使用您自己的）	

多个区域中 **HA** 对的网络信息

Google Cloud 信息	你的价值
地区	
节点 1 的区域	
节点 2 的区域	
调解员区域	
VPC-0 和子网	
VPC-1 和子网	
VPC-2 和子网	
VPC-3 和子网	
防火墙策略（如果使用您自己的）	

单个区域中 **HA** 对的网络信息

Google Cloud 信息	你的价值
地区	
分区	
VPC-0 和子网	
VPC-1 和子网	
VPC-2 和子网	
VPC-3 和子网	
防火墙策略（如果使用您自己的）	

选择写入速度

控制台可让您选择Cloud Volumes ONTAP的写入速度设置，但 Google Cloud 中的高可用性 (HA) 对除外。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息" 。

选择卷使用情况配置文件

ONTAP包含多种存储效率功能，可以减少您所需的总存储量。在控制台中创建卷时，您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息，以帮助您决定使用哪个配置文件。

NetApp存储效率功能具有以下优势：

精简配置

向主机或用户提供比物理存储池中实际拥有的更多的逻辑存储。不是预先分配存储空间，而是在写入数据时动态地将存储空间分配给每个卷。

重复数据删除

通过定位相同的数据块并将其替换为对单个共享块的引用来提高效率。该技术通过消除驻留在同一卷中的冗余数据块来减少存储容量要求。

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

为Cloud Volumes ONTAP设置 Google Cloud 网络

NetApp Console负责设置Cloud Volumes ONTAP的网络组件，例如 IP 地址、网络掩码和路由。您需要确保可以访问出站互联网、有足够的私有 IP 地址、有正确的连接等等。

如果你想部署 HA 对，你应该"了解 HA 对在 Google Cloud 中的工作原理"。

Cloud Volumes ONTAP的要求

Google Cloud 必须满足以下要求。

特定于单节点系统的要求

如果要部署单节点系统，请确保网络满足以下要求。

一个 VPC

单节点系统需要一个虚拟私有云 (VPC)。

私有 IP 地址

对于 Google Cloud 中的单节点系统，Console 将私有 IP 地址分配给以下内容：

- 节点

- 集群
- Storage VM
- 数据 NAS LIF
- 数据 iSCSI LIF

如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

LIF 是与物理端口关联的 IP 地址。 SnapCenter等管理工具需要存储虚拟机 (SVM) 管理 LIF。

HA 对的特定要求

如果您要部署 HA 对，请确保您的网络满足以下要求。

一个或多个区域

您可以通过在多个区域或单个区域中部署 HA 配置来确保数据的高可用性。创建 HA 对时，控制台会提示您选择多个区域或单个区域。

- 多区域（推荐）

  跨三个区域部署 HA 配置可确保当一个区域内发生故障时数据仍然可用。请注意，与使用单个区域相比，写入性能略低，但差别很小。

- 单区

  在单个区域中部署时， Cloud Volumes ONTAP HA 配置使用分散放置策略。此策略可确保 HA 配置免受区域内单点故障的影响，而无需使用单独的区域来实现故障隔离。

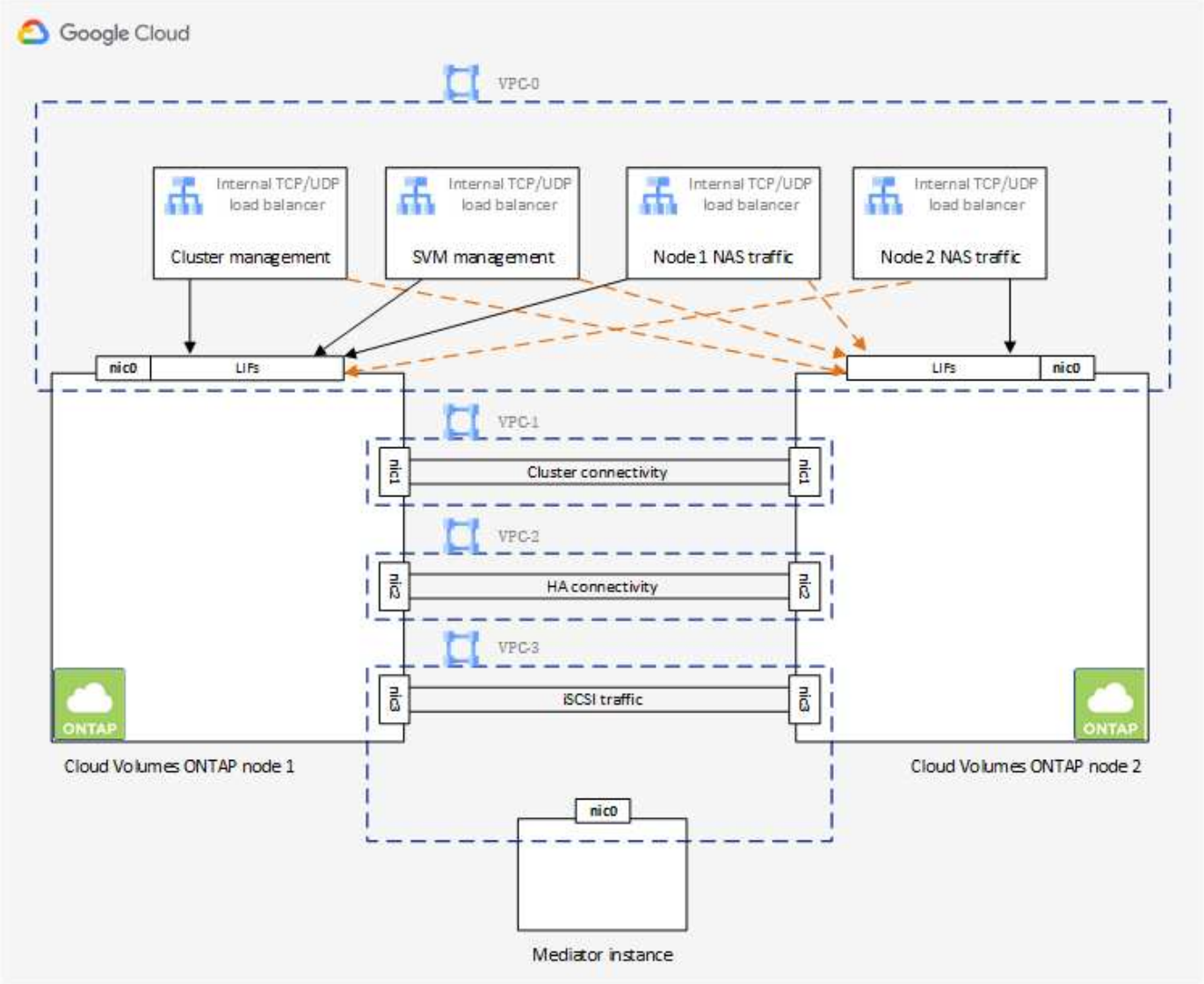
  这种部署模型确实降低了您的成本，因为区域之间没有数据流出费用。

四个虚拟私有云

HA 配置需要四个虚拟私有云 (VPC)。需要四个 VPC，因为 Google Cloud 要求每个网络接口位于单独的 VPC 网络中。

创建 HA 对时，控制台会提示您选择四个 VPC：

- VPC-0 用于数据和节点的入站连接
- VPC-1、VPC-2 和 VPC-3 用于节点和 HA 中介之间的内部通信



子网

每个 VPC 都需要一个私有子网。

如果将控制台代理放置在 VPC-0 中，则需要在子网上启用私有 Google 访问权限以访问 API 并启用数据分层。

这些 VPC 中的子网必须具有不同的 CIDR 范围。它们不能有重叠的 CIDR 范围。

私有 **IP** 地址

控制台会自动为 Google Cloud 中的Cloud Volumes ONTAP分配所需数量的私有 IP 地址。您需要确保您的网络有足够的可用私有地址。

为 Cloud Volumes ONTAP 分配的 LIF 数量取决于您是部署单节点系统还是 HA 对。LIF 是与物理端口关联的 IP 地址。像 SnapCenter 这样的管理工具需要 SVM 管理 LIF。

- 单节点 Console 为单节点系统分配 4 个 IP 地址：
  - 节点管理 LIF

- 集群管理 LIF
- iSCSI 数据 LIF

  iSCSI LIF 通过 iSCSI 协议提供客户端访问，并被系统用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。

- NAS LIF

  如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

- **HA** 对 控制台为 HA 对分配 12-13 个 IP 地址：
  - 2 个节点管理 LIF (e0a)
  - 1 集群管理 LIF (e0a)
  - 2 个 iSCSI LIF (e0a)

    iSCSI LIF 通过 iSCSI 协议提供客户端访问，并被系统用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。

  - 1 或 2 个 NAS LIF (e0a)
  - 2 个集群 LIF (e0b)
  - 2 个 HA 互连 IP 地址 (e0c)
  - 2 个 RSM iSCSI IP 地址（e0d）

    如果您使用 API 部署Cloud Volumes ONTAP并指定以下标志，则可以跳过创建存储虚拟机 (SVM) 管理 LIF：

```
skipSvmManagementLif: true
```

内部负载均衡器

控制台创建四个 Google Cloud 内部负载均衡器（TCP/UDP），用于管理传入Cloud Volumes ONTAP HA 对的流量。您无需进行任何设置。我们将其列为一项要求只是为了告知您网络流量并减轻任何安全问题。

一个负载均衡器用于集群管理，一个用于存储虚拟机 (SVM) 管理，一个用于到节点 1 的 NAS 流量，最后一个用于到节点 2 的 NAS 流量。

每个负载均衡器的设置如下：

- 一个共享的私有 IP 地址
- 一次全球健康检查

  默认情况下，健康检查使用的端口为63001、63002、63003。

- 一个区域 TCP 后端服务
- 一个区域 UDP 后端服务
- 一条 TCP 转发规则
- 一条 UDP 转发规则
- 全局访问已禁用

  尽管默认情况下禁用全局访问，但支持在部署后启用它。我们禁用它是因为跨区域流量会有明显更高的延迟。我们希望确保您不会因为意外的跨区域坐骑而产生负面体验。启用此选项是为了满足您的业务需求。

共享 **VPC**

Google Cloud 共享 VPC 和独立 VPC 均支持Cloud Volumes ONTAP和控制台代理。

对于单节点系统，VPC 可以是共享 VPC 或独立 VPC。

对于 HA 对，需要四个 VPC。每个 VPC 可以是共享的，也可以是独立的。例如，VPC-0 可以是共享 VPC，而 VPC-1、VPC-2 和 VPC-3 可以是独立 VPC。

共享 VPC 使您能够跨多个项目配置和集中管理虚拟网络。您可以在_主机项目_中设置共享 VPC 网络，并在_服务项目_中部署控制台代理和Cloud Volumes ONTAP虚拟机实例。

"Google Cloud 文档：共享 VPC 概览" 。

"查看控制台代理部署中涵盖的所需共享 VPC 权限"

VPC 中的数据包镜像

"数据包镜像"必须在部署Cloud Volumes ONTAP的 Google Cloud 子网中禁用。

出站互联网访问

Cloud Volumes ONTAP系统需要出站互联网访问才能访问外部端点以实现各种功能。如果这些端点在具有严格安全要求的环境中被阻止， Cloud Volumes ONTAP将无法正常运行。

控制台代理还联系多个端点以进行日常操作。有关端点的信息，请参阅 "查看从控制台代理联系的端点"和 "准备使用控制台的网络"。

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	端点不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。

端点	适用于	目的	部署模式	端点不可用时的影响
https://cloudbuild.googleapis.com/v1 （仅适用于私有模式部署） https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud（商业用途）。	与 Google Cloud 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Google Cloud 服务通信以对 Google Cloud 中的控制台执行特定操作。

与其他网络中的**ONTAP**系统的连接

要在 Google Cloud 中的Cloud Volumes ONTAP系统和其他网络中的ONTAP系统之间复制数据，您必须在 VPC 和其他网络（例如您的公司网络）之间建立 VPN 连接。

"Google Cloud 文档：Cloud VPN 概览" 。

防火墙规则

控制台创建 Google Cloud 防火墙规则，其中包括Cloud Volumes ONTAP成功运行所需的入站和出站规则。您可能希望参考端口以进行测试，或者您更喜欢使用自己的防火墙规则。

Cloud Volumes ONTAP的防火墙规则需要入站和出站规则。如果您正在部署 HA 配置，这些是 VPC-0 中Cloud Volumes ONTAP的防火墙规则。

请注意，HA 配置需要两组防火墙规则：

- 针对 VPC-0 中的 HA 组件的一组规则。这些规则允许对Cloud Volumes ONTAP进行数据访问。
- 针对 VPC-1、VPC-2 和 VPC-3 中的 HA 组件的另一组规则。这些规则对于 HA 组件之间的入站和出站通信开放。了解更多 。

正在寻找有关控制台代理的信息？ "查看控制台代理的防火墙规则"

入站规则

添加Cloud Volumes ONTAP系统时，您可以在部署期间选择预定义防火墙策略的源过滤器：

- 仅限选定的 **VPC**：入站流量的源过滤器是Cloud Volumes ONTAP系统的 VPC 子网范围和控制台代理所在的 VPC 子网范围。这是推荐的选项。
- 所有 **VPC**：入站流量的源过滤器是 0.0.0.0/0 IP 范围。

如果您使用自己的防火墙策略，请确保添加所有需要与Cloud Volumes ONTAP通信的网络，同时还要确保添加两个地址范围以允许内部 Google 负载均衡器正常运行。这些地址是 130.211.0.0/22 和 35.191.0.0/16。欲了解更多信息，请参阅 "Google Cloud 文档：负载均衡器防火墙规则"。

协议	端口	目的
所有 ICMP	全部	对实例执行 ping 操作
HTTP	80	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
HTTPS	443	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
SSH	22	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111	NFS 的远程过程调用
TCP	139	CIFS 的 NetBIOS 服务会话
TCP	161-162	简单网络管理协议
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁守护进程
TCP	4046	NFS 网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104	SnapMirror集群间通信会话的管理
TCP	11105	使用集群间 LIF 进行SnapMirror数据传输
TCP	63001-63050	负载平衡探测端口以确定哪个节点是健康的（仅 HA 对需要）

协议	端口	目的
UDP	111	NFS 的远程过程调用
UDP	161-162	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049	NFS 服务器守护进程
UDP	4045	NFS 锁守护进程
UDP	4046	NFS 网络状态监视器
UDP	4049	NFS rquotad 协议

出站规则

Cloud Volumes ONTAP的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

协议	端口	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开Cloud Volumes ONTAP出站通信所需的端口。 Cloud Volumes ONTAP集群使用以下端口来调节节点流量。

源是Cloud Volumes ONTAP系统的接口（IP 地址）。

服务	协议	端口	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 林	Kerberos V 身份验证
	UDP	137	节点管理 LIF	Active Directory 林	NetBIOS 名称服务
	UDP	138	节点管理 LIF	Active Directory 林	NetBIOS 数据报服务
	TCP	139	节点管理 LIF	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	节点管理 LIF	Active Directory 林	LDAP
	TCP	445	节点管理 LIF	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	节点管理 LIF	Active Directory 林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
	TCP	88	数据 LIF（NFS 、CIFS、iSCSI）	Active Directory 林	Kerberos V 身份验证
	UDP	137	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 名称服务
	UDP	138	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 数据报服务
	TCP	139	数据 LIF（NFS 、CIFS）	Active Directory 林	NetBIOS 服务会话
	TCP 和 UDP	389	数据 LIF（NFS 、CIFS）	Active Directory 林	LDAP
	TCP	445	数据 LIF（NFS 、CIFS）	Active Directory 林	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
	TCP	464	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（SET_CHANGE）
	UDP	464	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos 密钥管理
	TCP	749	数据 LIF（NFS 、CIFS）	Active Directory 林	Kerberos V 更改和设置密码（RPCSEC_GSS）
AutoSupport	HTTPS	443	节点管理 LIF	mysupport.netapp.com	AutoSupport （默认为 HTTPS）
	HTTP	80	节点管理 LIF	mysupport.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）
	TCP	3128	节点管理 LIF	控制台代理	如果出站互联网连接不可用，则通过控制台代理上的代理服务器发送AutoSupport消息

服务	协议	端口	源	目标	目的
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP 地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档"
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600-18699	节点管理 LIF	目标服务器	NDMP 拷贝
SMTP	TCP	25	节点管理 LIF	邮件服务器	SMTP 警报，可用于AutoSupport
SNMP	TCP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104	集群间 LIF	ONTAP集群间 LIF	SnapMirror集群间通信会话的管理
	TCP	11105	集群间 LIF	ONTAP集群间 LIF	SnapMirror数据传输
系统日志	UDP	514	节点管理 LIF	系统日志服务器	Syslog 转发消息

VPC-1、**VPC-2** 和 **VPC-3** 的规则

在 Google Cloud 中，HA 配置部署在四个 VPC 中。 VPC-0 中的 HA 配置所需的防火墙规则是上面列出的Cloud Volumes ONTAP。

同时，为 VPC-1、VPC-2 和 VPC-3 中的实例创建的预定义防火墙规则支持通过所有协议和端口进行入站通信。这些规则支持 HA 节点之间的通信。

从 HA 节点到 HA 中介的通信通过端口 3260（iSCSI）进行。

> 为了使新的 Google Cloud HA 对部署实现较高的写入速度，VPC-1、VPC-2 和 VPC-3 需要至少 8,896 字节的最大传输单元 (MTU)。如果您选择将现有的 VPC-1、VPC-2 和 VPC-3 升级到 8,896 字节的 MTU，则必须在配置过程中关闭使用这些 VPC 的所有现有 HA 系统。

适用于专用模式部署的 **Infrastructure Manager** 配置

如果要在私有模式下部署 Cloud Volumes ONTAP 9.16.1 或更高版本，则需要进行一些配置更改，以便 Cloud Volumes ONTAP 可以使用 Google Cloud Infrastructure Manager 作为部署服务，而不是 Google 最终将弃用的 Deployment Manager。

开始之前

- 确保您的 Cloud Volumes ONTAP 系统为 9.16.1 或更高版本。如果不是，请升级您的系统。有关说明，请参阅 "升级Cloud Volumes ONTAP"。
- 请确保已启用 Google Cloud API。请参阅 "启用 Google Cloud API"。
- 确保已启用 Cloud Build API。请参阅 "在此处启用 Cloud Build API"。
- 验证 Console 代理的服务帐户是否具有所有标准权限。此外，请确保服务帐户具有 `cloudbuild.workerpools.get`和 `cloudbuild.workerpools.list`权限。请参阅 "控制台代理的 Google Cloud 权限"。

步骤

1. 在与 Cloud Volumes ONTAP 部署相同的区域中使用此配置创建专用工作者池。有关创建专用工作者池的信息，请参阅 "Google Cloud 文档：创建和管理私有池"和 "Google Cloud Build 定价"。

   工作进程池必须具有以下配置：

   - 机器类型：e2-medium
   - 磁盘大小：100 GB
   - 分配外部 IP：False
   - 网络：Default 或 private。
   - 配置为访问 "Google APIs"的子网。执行以下步骤以确保子网可以访问 Google API：
     i. 确保子网的 "Private Google Access" 已打开。
     ii. 转到 **VPC Network level > Private Service Access Tab > Allocated IP ranges for services**。
     iii. 选择 分配 **IP** 范围 ，并为与 Google Compute Service 的私有连接分配内部 IP 范围。
     iv. 在 **Private connection to services** 上，选择 **Create Connection**。
     v. 选择 **Connected service producer = Google Cloud Platform**。
     vi. 为您在上一步中创建的专用连接 IP 范围分配配额。
2. 部署此工作者池并使其运行以进行 Cloud Volumes ONTAP 管理。Google Cloud 使用此工作者池在隔离环境中运行所有 Terraform 操作。
3. 在私有模式下部署 Cloud Volumes ONTAP 时，请在 **GCP Worker Pool** 字段中选择此工作池的名称。有关说明，请参阅 "在 Google Cloud 中启动Cloud Volumes ONTAP"。

控制台代理的要求

如果您尚未创建控制台代理，则应查看网络要求。

- "查看控制台代理的网络要求"
- "Google Cloud 中的防火墙规则"

支持控制台代理的网络配置

您可以使用为控制台代理配置的代理服务器来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

- 显式代理：来自Cloud Volumes ONTAP 的出站流量使用控制台代理代理配置期间指定的代理服务器的 HTTP 地址。控制台代理管理员可能还配置了用户凭据和根 CA 证书以进行额外的身份验证。Cloud Volumes ONTAP显式代理有可用的根 CA 证书，请确保使用 "ONTAP CLI：安全证书安装"命令。
- 透明代理：网络配置为通过控制台代理代理自动路由来自Cloud Volumes ONTAP 的出站流量。设置透明代理时，控制台代理管理员仅需要提供用于从Cloud Volumes ONTAP进行连接的根 CA 证书，而不是代理服务器的 HTTP 地址。确保使用以下方式获取相同的根 CA 证书并将其上传到您的Cloud Volumes ONTAP系统 "ONTAP CLI：安全证书安装"命令。

有关为控制台代理配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

在 **Google Cloud** 中为**Cloud Volumes ONTAP**配置网络标签

在控制台代理的透明代理配置期间，管理员为 Google Cloud 添加网络标签。您需要获取并手动添加Cloud Volumes ONTAP配置的相同网络标签。此标签对于代理服务器正常运行是必需的。

1. 在 Google Cloud Console 中，找到 Cloud Volumes ONTAP 系统。
2. 转到*详细信息>网络>网络标签*。
3. 添加用于控制台代理的标签并保存配置。

相关主题

- "验证Cloud Volumes ONTAP 的AutoSupport设置"
- "了解ONTAP内部端口" 。

设置 VPC 服务控制以在 Google Cloud 中部署Cloud Volumes ONTAP

当选择使用 VPC 服务控制锁定您的 Google Cloud 环境时，您应该了解NetApp Console和Cloud Volumes ONTAP如何与 Google Cloud API 交互，以及如何配置您的服务边界以部署控制台和Cloud Volumes ONTAP。

VPC 服务控制使您能够控制对受信任边界之外的 Google 管理服务的访问，阻止来自不受信任位置的数据访问，并降低未经授权的数据传输风险。 "详细了解 Google Cloud VPC 服务控制" 。

NetApp服务如何与 VPC 服务控制进行通信

控制台直接与 Google Cloud API 通信。这可以从 Google Cloud 外部的外部 IP 地址触发（例如，来自 api.services.cloud.netapp.com），也可以从 Google Cloud 内部分配给控制台代理的内部地址触发。

根据控制台代理的部署方式，您的服务边界可能需要做出某些例外。

图片

Cloud Volumes ONTAP 和 Console 都使用来自 Google Cloud 中由 NetApp 管理的项目的映像。如果您的组织具有阻止使用未在组织内托管的映像的策略，这可能会影响 Console 代理和 Cloud Volumes ONTAP 的部署。

您可以使用手动安装方法手动部署控制台代理，但Cloud Volumes ONTAP还需要从NetApp项目中提取图像。您必须提供允许列表才能部署控制台代理和Cloud Volumes ONTAP。

部署控制台代理

部署控制台代理的用户需要能够引用 projectId 为 *netapp-cloudmanager* 且项目编号为 *14190056516* 中托管的图像。

部署**Cloud Volumes ONTAP**

- 控制台服务帐户需要引用服务项目中托管在 projectId *netapp-cloudmanager* 中的图像和项目编号 *14190056516*。
- 默认 Google API 服务代理的服务帐户需要引用服务项目中 projectId *netapp-cloudmanager* 和项目编号 *14190056516* 中托管的图像。

下面定义了使用 VPC 服务控制拉取这些图像所需的规则示例。

VPC 服务控制边界策略

策略允许对 VPC Service Controls 规则集进行例外。有关策略的详细信息，请访问 "Google Cloud VPC Service Controls Policy 文档"。

要设置控制台所需的策略，请导航到您组织内的 VPC 服务控制边界并添加以下策略。这些字段应与 VPC 服务控制策略页面中给出的选项相匹配。还要注意，*所有*规则都是必需的，并且规则集中应该使用*OR*参数。

入口规则

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

或

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

或

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出口规则

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上面列出的项目编号是NetApp用于存储控制台代理和Cloud Volumes ONTAP 的图像的项目 *netapp-cloudmanager*。

为Cloud Volumes ONTAP创建 Google Cloud 服务帐号

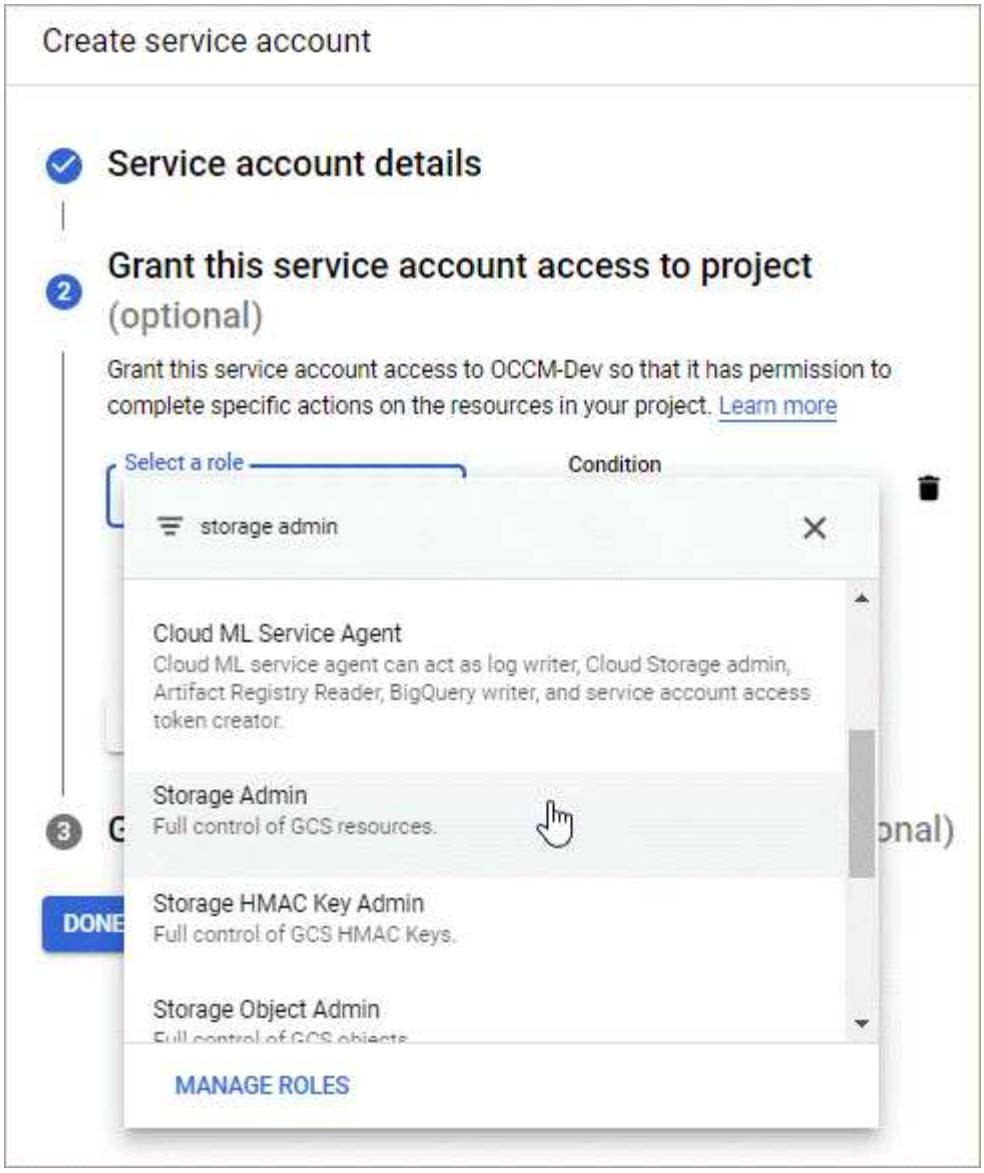
Cloud Volumes ONTAP需要 Google Cloud 服务帐户来实现两个目的。第一个是当你启用"数据分层"将冷数据分层到 Google Cloud 中的低成本对象存储。第二个是当你启用"NetApp Backup and Recovery"将卷备份到低成本的对象存储。

Cloud Volumes ONTAP使用服务帐户来访问和管理一个用于分层数据的存储桶以及另一个用于备份的存储桶。

您可以设置一个服务帐户并将其用于两种用途。服务帐户必须具有*存储管理员*角色。

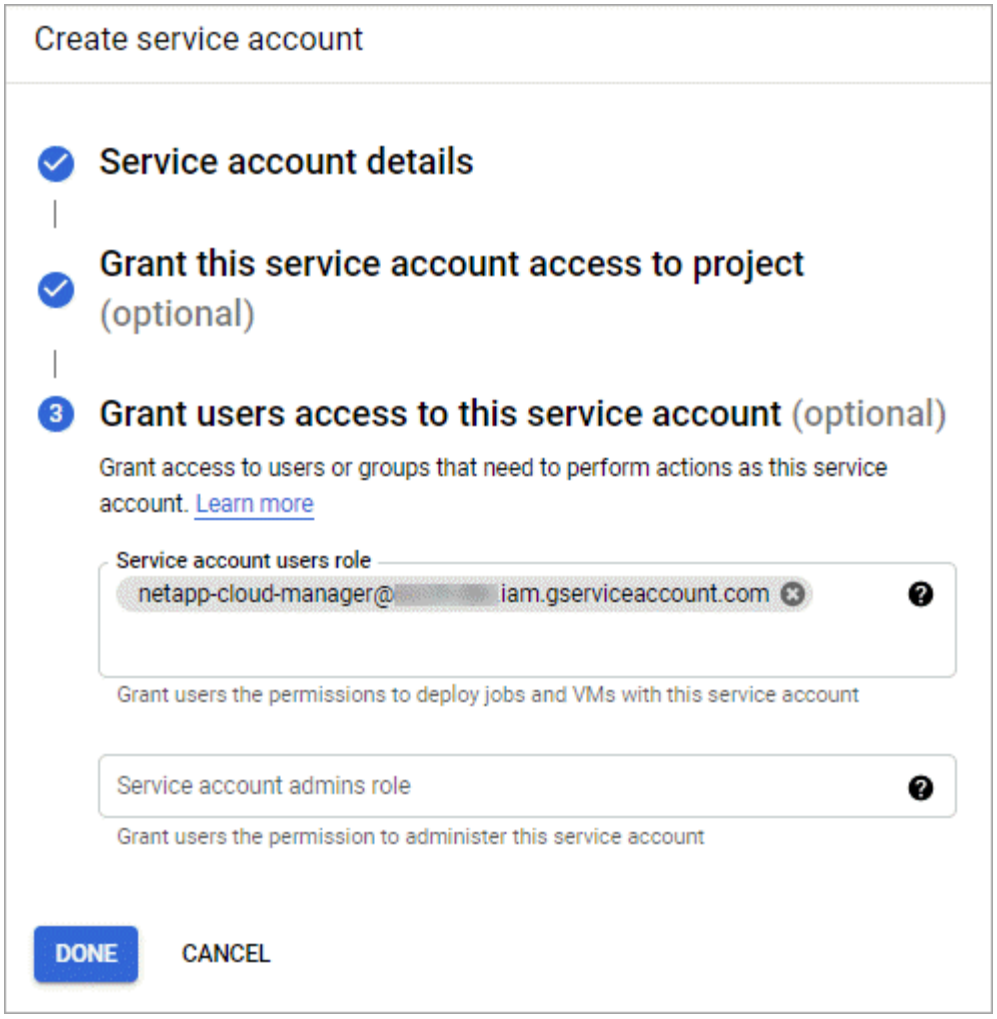
步骤

1. 在 Google Cloud Console 中， "前往服务帐户页面"。
2. 选择您的项目。
3. 单击*创建服务帐户*并提供所需信息。
    a. 服务帐户详细信息：输入名称和描述。
    b. 授予此服务帐户访问项目的权限：选择*存储管理员*角色。



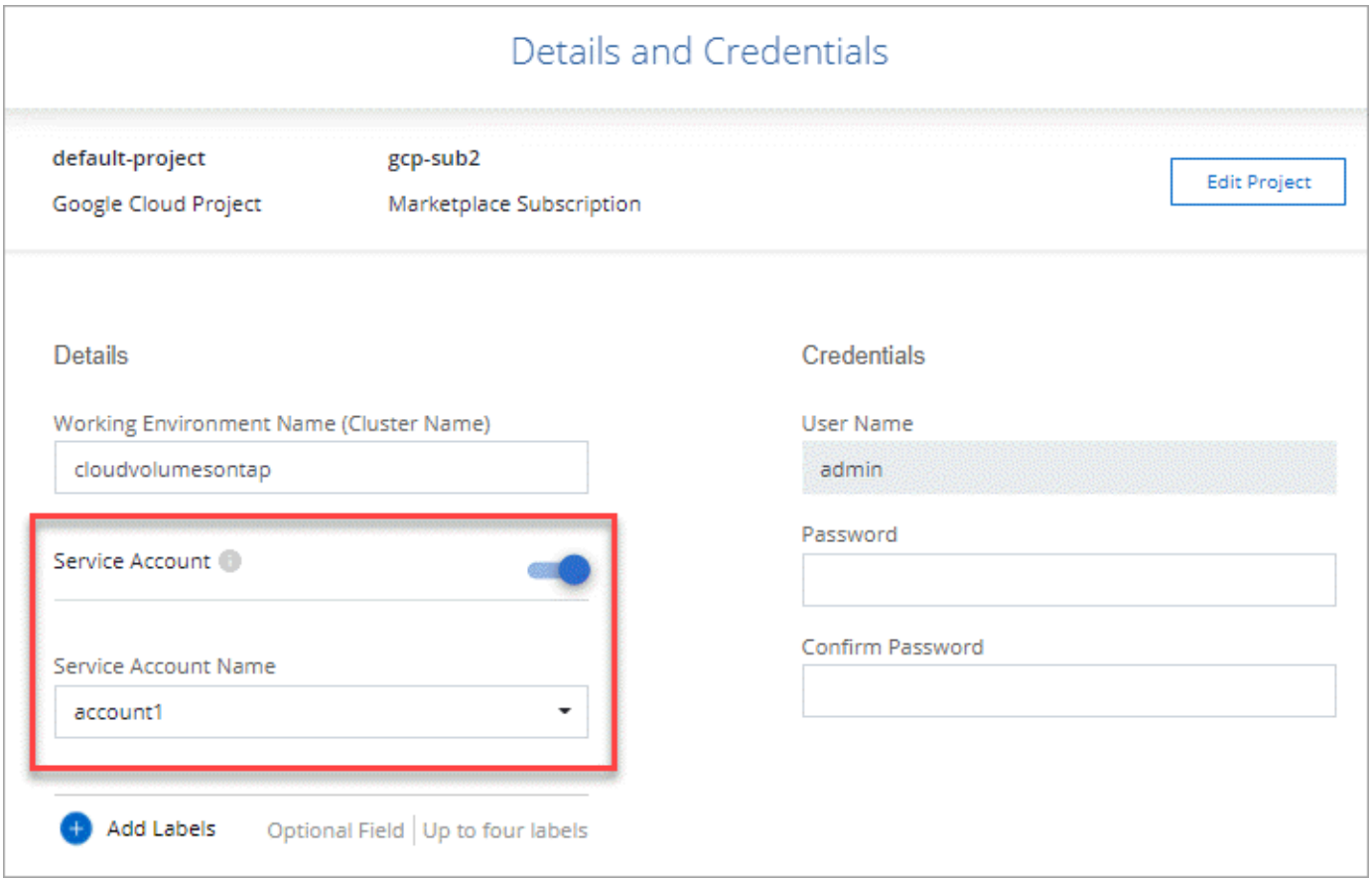
c. 授予用户访问此服务帐户的权限：将控制台代理服务帐户作为_服务帐户用户_添加到此新服务帐户。

此步骤仅对于数据分层是必需的。备份和恢复不需要它。



下一步是什么?

稍后创建Cloud Volumes ONTAP系统时，您需要选择服务帐户。



将客户管理的加密密钥与Cloud Volumes ONTAP结合使用

虽然 Google Cloud Storage 始终会在将数据写入磁盘之前对其进行加密，但您可以使用 API 创建使用_客户管理加密密钥_的Cloud Volumes ONTAP系统。这些是您使用云密钥管理服务在 GCP 中生成和管理的密钥。

步骤

1. 确保控制台代理服务帐户在存储密钥的项目中具有项目级别的正确权限。

   权限已在以下文件中提供： "默认的服务帐户权限"但如果您使用其他项目来管理云密钥服务，则可能无法应用此功能。

   权限如下：

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 确保 "Google Compute Engine 服务代理"对密钥具有 Cloud KMS 加密器/解密器权限。

   服务帐户的名称使用以下格式：“service-[service_project_number]@compute-system.iam.gserviceaccount.com”。

"Google Cloud 文档：将 IAM 与 Cloud KMS 结合使用 - 授予资源角色"

3. 通过调用 get 命令获取密钥的“id” `/gcp/vsa/metadata/gcp-encryption-keys` API 调用或通过在 GCP 控制台中的键上选择“复制资源名称”。
4. 如果使用客户管理的加密密钥并将数据分层到对象存储， NetApp Console会尝试使用用于加密持久磁盘的相同密钥。但您首先需要启用 Google Cloud Storage 存储桶才能使用密钥：

   a. 按照以下步骤查找 Google Cloud Storage 服务代理 "Google Cloud 文档：获取云存储服务代理"。

   b. 导航到加密密钥并为 Google Cloud Storage 服务代理分配 Cloud KMS Encrypter/Decrypter 权限。

   有关详细信息，请参阅 "Google Cloud 文档：使用客户管理的加密密钥"

5. 创建系统时，请将 "gcpEncryption" 参数与 API 请求一起使用。

   例子

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

请参阅 "NetApp Console自动化文档"有关使用“GcpEncryption”参数的更多详细信息。

在 Google Cloud 中设置Cloud Volumes ONTAP许可

在您决定要对Cloud Volumes ONTAP使用哪种许可选项后，需要执行几个步骤才能在创建新系统时选择该许可选项。

免费增值

选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

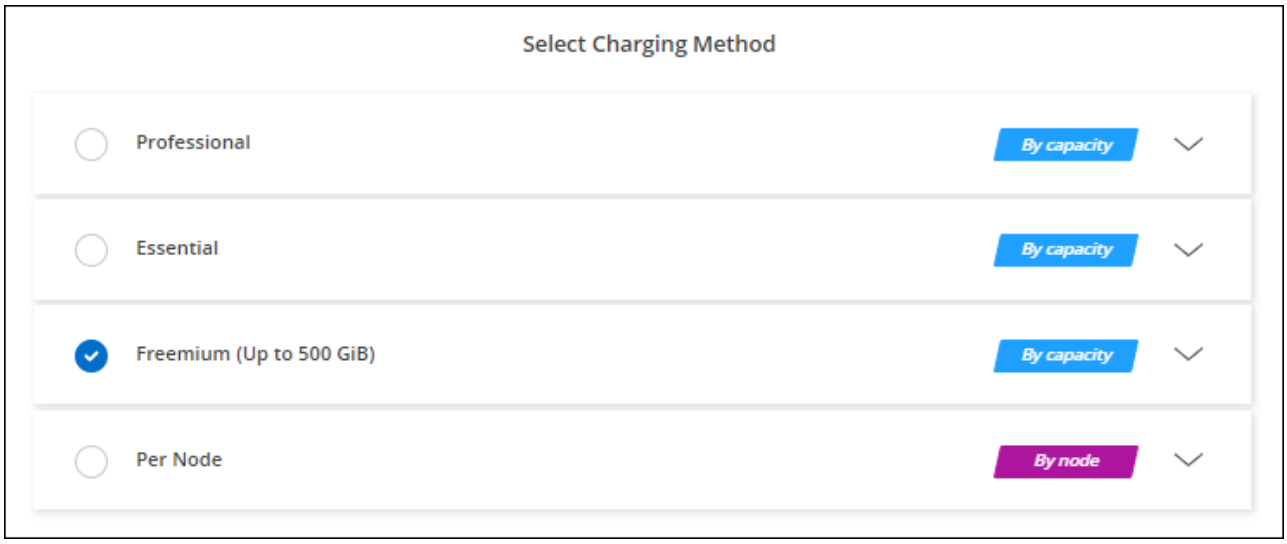
步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在“系统”页面上，单击“添加系统”并按照NetApp Console中的步骤进行操作。

   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。

      除非您超过 500 GiB 的预配置容量，否则您无需通过市场订阅付费，此时系统将自动转换为"基本套餐"。

   b. 返回控制台后，到达收费方式页面时选择“免费增值”。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

基于容量的许可证

基于容量的许可使您能够按 TiB 容量支付Cloud Volumes ONTAP费用。基于容量的许可以_包_的形式提供：Essentials 或 Professional 包。

Essentials 和 Professional 套餐提供以下几种消费模式或购买选项：

- 从NetApp购买的许可证（自带许可证 (BYOL)）
- Google Cloud Marketplace 的按小时付费 (PAYGO) 订阅
- 年度合同

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

通过从NetApp购买许可证 (BYOL) 进行预付款，以便在任何云提供商处部署Cloud Volumes ONTAP系统。

已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。

步骤

1. "联系NetApp销售人员获取许可证"
2. "将您的NetApp支持站点帐户添加到NetApp Console"

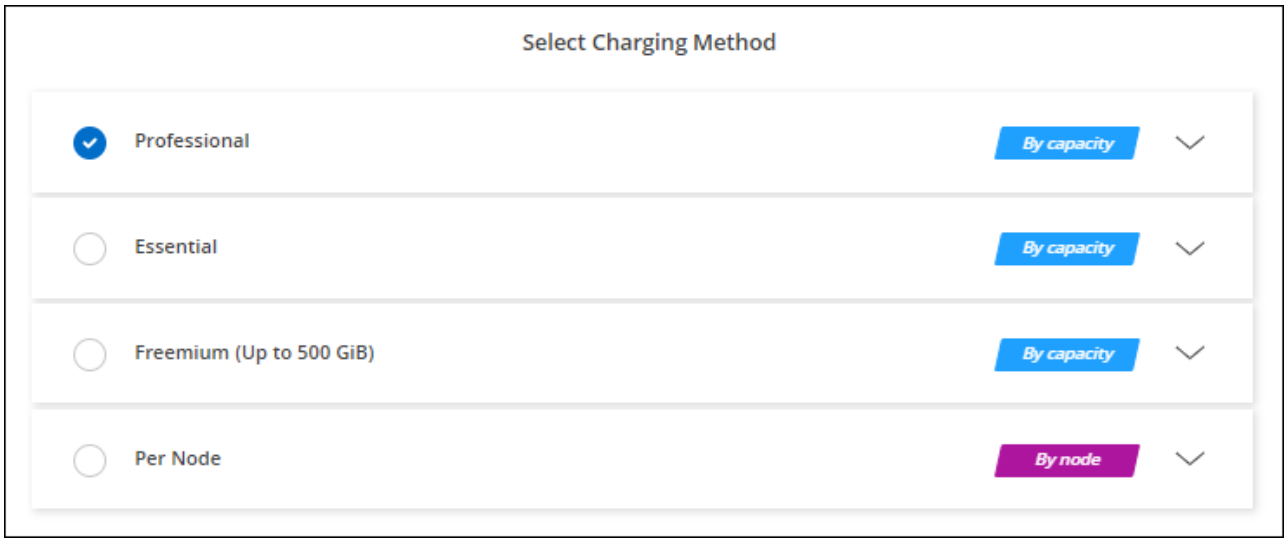
   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台将添加许可证。

   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"手动将许可证添加到控制台"。

3. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。

      始终会先向您从NetApp购买的许可证收费，但如果您超出许可容量或许可证期限到期，则会按照市场上的小时费率向您收费。

   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

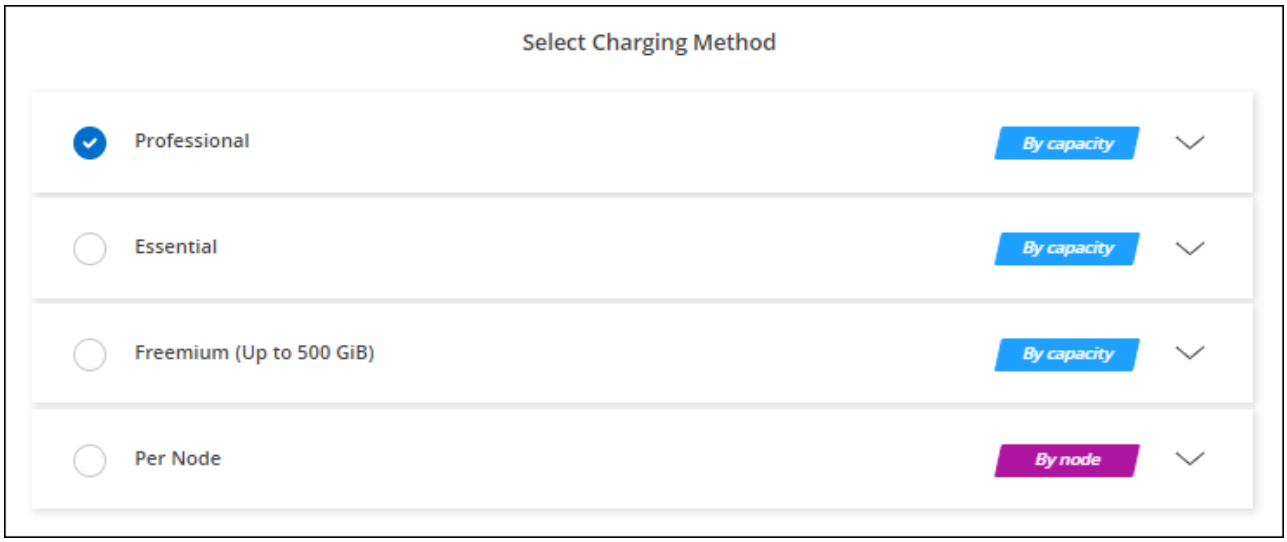
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 Google Cloud Marketplace 中提供的协议。然后将该订阅与系统关联以进行收费。您可以将同一订阅用于其他系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示订阅 Google Cloud Marketplace 中的即用即付产品。
   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

您可以从“设置”>“凭据”页面管理与您的帐户关联的 Google Cloud Marketplace 订阅。 "了解如何管理您的 Google Cloud 凭据和订阅"

年度合同

通过购买年度合同每年支付Cloud Volumes ONTAP 的费用。

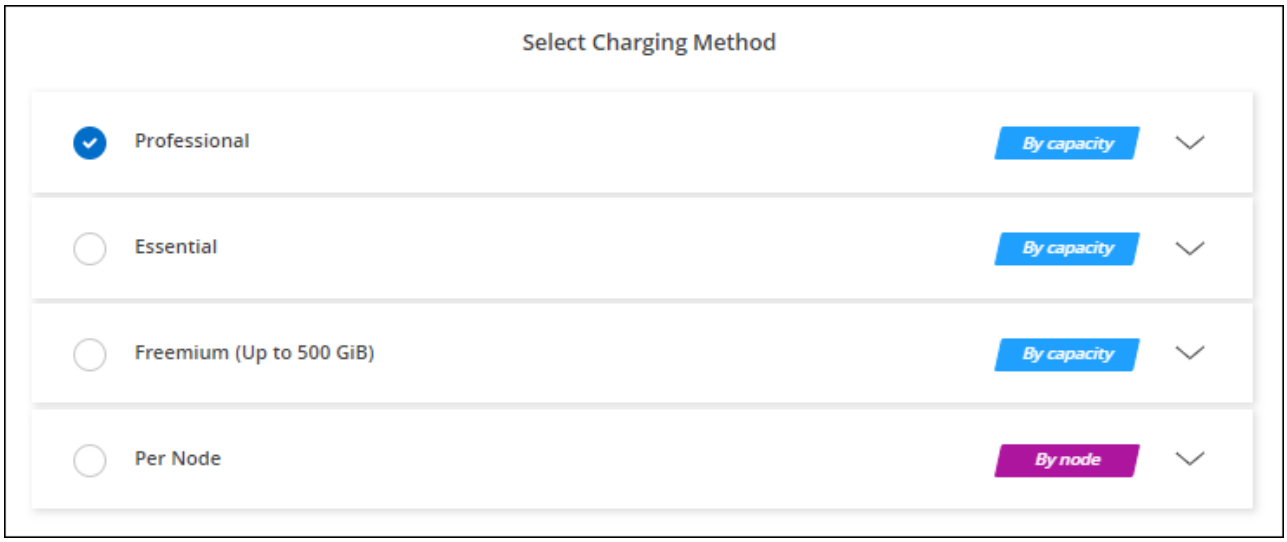
步骤

1. 联系您的NetApp销售代表购买年度合同。

   该合同在 Google Cloud Marketplace 中以私人优惠形式提供。

   NetApp与您分享私人优惠后，您可以在系统创建期间从 Google Cloud Marketplace 订阅时选择年度计划。

2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭据*页面上，单击*编辑凭据>添加订阅*，然后按照提示在 Google Cloud Marketplace 中订阅年度计划。
   b. 在 Google Cloud 中，选择与您的帐户共享的年度计划，然后单击*订阅*。
   c. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



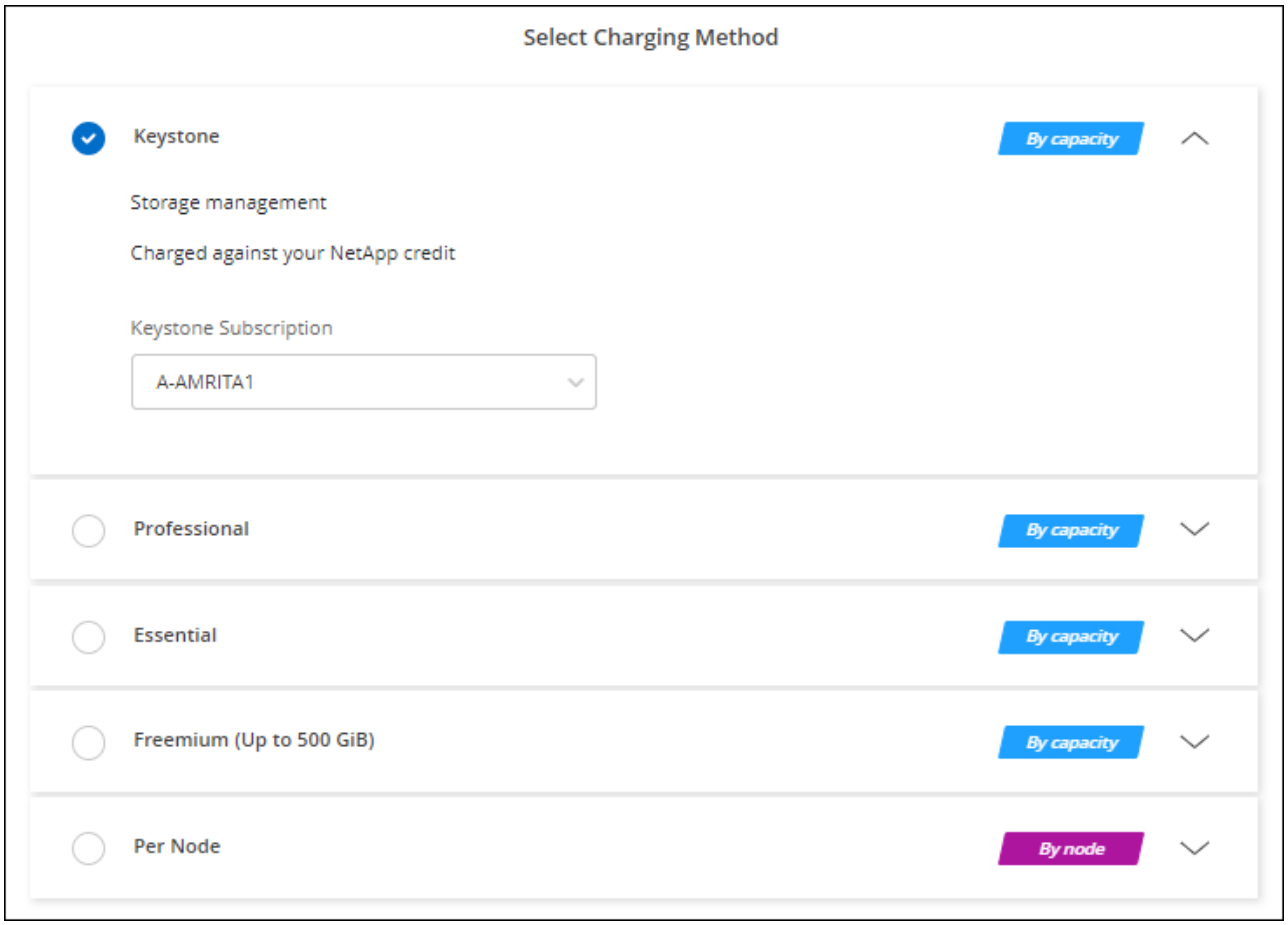
"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

Keystone订阅

Keystone订阅是一种按需付费的订阅式服务。"了解有关NetApp Keystone订阅的更多信息" 。

步骤

1. 如果您尚未订阅， "联系NetApp"
2. 联系NetApp 授权您的控制台用户帐户拥有一个或多个Keystone订阅。
3. NetApp授权您的帐户后，"链接您的订阅以用于Cloud Volumes ONTAP" 。
4. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 当提示选择收费方式时，选择Keystone Subscription 收费方式。



"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

基于节点的许可证

基于节点的许可证是Cloud Volumes ONTAP的上一代许可证。基于节点的许可证可以从NetApp (BYOL) 处购买，并且仅在特定情况下才可以续订许可证。有关信息，请参阅：

- "基于节点的许可证的可用性终止"
- "基于节点的许可证的可用性终止"
- "将基于节点的许可证转换为基于容量的许可证"

在 Google Cloud 中启动Cloud Volumes ONTAP

您可以在单节点配置中启动Cloud Volumes ONTAP ，也可以在 Google Cloud 中以 HA 对的形式启动 Cloud Volumes ONTAP。

开始之前

开始之前您需要以下内容。

- 已启动且正在运行的 NetApp Console 代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。

- "您应该准备好让控制台代理始终处于运行状态" 。
- 与控制台代理关联的服务帐户 "应该具有所需的权限"

- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 Google Cloud 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。

- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。

- Google Cloud API 应该 "在您的项目中启用"：
  - 云部署管理器 V2 API
  - 云日志 API
  - 云资源管理器 API
  - 计算引擎 API
  - 身份和访问管理 (IAM) API

在 Google Cloud 中启动单节点系统

在NetApp Console中创建一个系统以在 Google Cloud 中启动Cloud Volumes ONTAP 。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择位置：选择*Google Cloud*和* Cloud Volumes ONTAP*。
4. 如果出现提示， "创建控制台代理" 。
5. 详细信息和凭证：选择一个项目，指定一个集群名称，可选地选择一个服务帐户，可选地添加标签，然后指定凭证。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Google Cloud VM 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
服务帐户名称	如果你打算使用"数据分层"或者 "NetApp Backup and Recovery"使用Cloud Volumes ONTAP，则需要启用*服务帐户*并选择具有预定义存储管理员角色的服务帐户。"了解如何创建服务帐号" 。
添加标签	标签是您的 Google Cloud 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP系统以及与该系统关联的 Google Cloud 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Google Cloud 文档：标记资源"。

字段	描述
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑项目	选择您希望Cloud Volumes ONTAP驻留的项目。默认项目是控制台所在的项目。 如果您在下拉列表中没有看到任何其他项目，则表示您尚未将服务帐户与其他项目关联。转到 Google Cloud Console，打开 IAM 服务，然后选择项目。将具有用于 Console 的角色的服务帐户添加到该项目。您需要为每个项目重复此步骤。 这是您为控制台设置的服务帐户，"如本页所述" 。 单击“添加订阅”将选定的凭据与订阅关联。 要创建按使用量付费的Cloud Volumes ONTAP系统，您需要从 Google Cloud 市场选择与Cloud Volumes ONTAP订阅相关联的 Google Cloud 项目。参考 "将市场订阅与 Google Cloud 凭据关联"。

6. 服务：选择您想要在此系统上使用的服务。为了选择备份和恢复，或使用NetApp Cloud Tiering，您必须在步骤 3 中指定服务帐户。

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

7. 位置和连接：为您的系统选择 Google Cloud 区域和区域，选择防火墙策略，并确认网络连接到 Google Cloud 存储以进行数据分层。

   下表描述了您可能需要指导的字段：

字段	描述
连接验证	要将冷数据分层到 Google Cloud Storage 存储桶，必须为Cloud Volumes ONTAP所在的子网配置私有 Google Access。有关说明，请参阅 "Google Cloud 文档：配置私有 Google 访问权限"。
生成的防火墙策略	如果您让控制台为您生成防火墙策略，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的源过滤器是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的源过滤器是 0.0.0.0/0 IP 范围。
使用现有的防火墙策略	如果您使用现有的防火墙策略，请确保它包含所需的规则："了解Cloud Volumes ONTAP的防火墙规则"

8. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户：
   - "了解Cloud Volumes ONTAP的许可选项"

- "了解如何设置许可"

9. 预配置的软件包：选择其中一个软件包以快速部署 Cloud Volumes ONTAP 系统，或单击*创建我自己的配置*。预配置的软件包因所选 Cloud Volumes ONTAP 版本而异。例如，对于 Cloud Volumes ONTAP 9.18.1 及更高版本，Console 显示包含 C3 VM 的软件包，包括 Hyperdisk Balanced 磁盘。您可以根据工作负载需求修改配置，例如 IOPS 和吞吐量参数。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

10. 许可：根据需要更改Cloud Volumes ONTAP版本并选择机器类型。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 — 例如，从 9.13 到 9.14。

11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

    磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

    有关选择磁盘类型和大小的帮助，请参阅"在 Google Cloud 中调整系统大小"。

12. 闪存缓存、写入速度和 **WORM**：

    a. 如果需要，启用 **Flash Cache** 或选择*普通*或*高*写入速度。

       详细了解 "Flash Cache" 和 "写入速度"。

       通过*高*写入速度选项可实现高写入速度和更高的 8,896 字节最大传输单元 (MTU)。此外，8,896 的更高 MTU 要求选择 VPC-1、VPC-2 和 VPC-3 进行部署。有关 VPC-1、VPC-2 和 VPC-3 的更多信息，请参阅 "VPC-1、VPC-2 和 VPC-3 的规则"。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

13. **Google Cloud Platform** 中的数据分层：选择是否在初始聚合上启用数据分层，为分层数据选择存储类，然后选择具有预定义存储管理员角色的服务帐户（ Cloud Volumes ONTAP 9.7 或更高版本所需），或选择 Google Cloud 帐户（ Cloud Volumes ONTAP 9.6 所需）。

    请注意以下事项：

    - 控制台在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。请确保将控制台代理服务帐户添加为分层服务帐户的用户，否则，您无法从控制台中选择它。

- 如需添加 Google Cloud 帐户的帮助，请参阅 "使用 9.6 设置和添加 Google Cloud 帐户以进行数据分层"。
- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它，但您需要关闭系统并从 Google Cloud Console 添加服务帐户。

  "了解有关数据分层的更多信息" 。

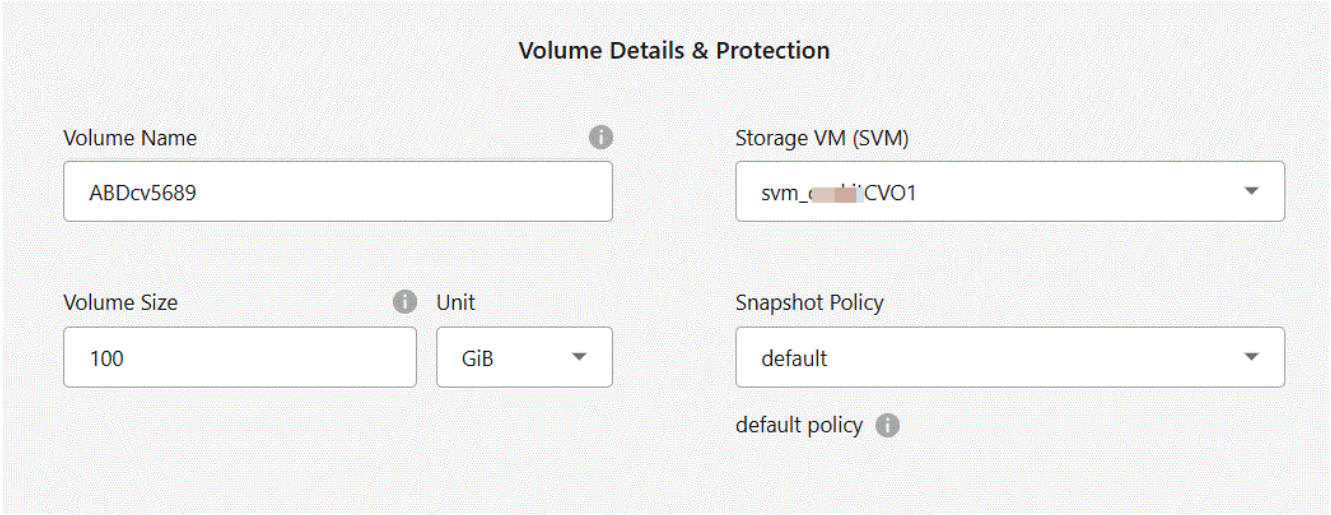
14. 创建卷：输入新卷的详细信息或单击*跳过*。

    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 策略	Snapshot 副本策略指定自动创建的NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 TCP 卸载引擎 (TOE) 卡、融合网络适配器 (CNA) 或专用主机总线适配器 (HBA) 连接到网络，并通过 iSCSI 限定名称 (IQN) 进行标识。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

    下图显示了卷创建向导的第一页：



15. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。如果您正在配置 Google 管理的 Active Directory，则默认情况下可以使用 169.254.169.254 IP 地址访问 AD。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Google Managed Microsoft AD 配置为Cloud Volumes ONTAP的 AD 服务器，请在此字段中输入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。欲了解更多信息，请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

16. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"选择卷使用情况配置文件"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？"

17. 审核并批准：审核并确认您的选择。

    a. 查看有关配置的详细信息。

b. 点击*更多信息*查看有关支持和控制台将购买的 Google Cloud 资源的详细信息。

c. 选中*我明白…*复选框。

d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在*审核*页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 CIFS 共享，请授予用户或组对文件和文件夹的权限，并验证这些用户是否可以访问共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

部署流程完成后，请勿修改 Google Cloud 门户中系统生成的 Cloud Volumes ONTAP 配置，例如系统标签以及 Google Cloud 资源中设置的标签。对这些配置进行的任何更改都可能导致意外行为或数据丢失。

在 Google Cloud 中启动 HA 对

在控制台中创建一个系统以在 Google Cloud 中启动Cloud Volumes ONTAP 。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*存储>系统*并按照提示进行操作。
3. 选择位置：选择*Google Cloud*和* Cloud Volumes ONTAP HA*。
4. 详细信息和凭证：选择一个项目，指定一个集群名称，可选地选择一个服务帐户，可选地添加标签，然后指定凭证。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Google Cloud VM 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
服务帐户名称	如果您打算使用"NetApp Cloud Tiering"或者 "备份和恢复"服务，您需要启用*服务帐户*开关，然后选择具有预定义存储管理员角色的服务帐户。

字段	描述
添加标签	标签是您的 Google Cloud 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP系统以及与该系统关联的 Google Cloud 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Google Cloud 文档：标记资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑项目	选择要让 Cloud Volumes ONTAP 驻留的项目。 如果您在下拉列表中没有看到任何其他项目，则表示您尚未将服务帐户与其他项目关联。转到 Google Cloud Console，打开 IAM 服务，然后选择项目。将具有用于 Console 的角色的服务帐户添加到该项目。您需要为每个项目重复此步骤。 这是您为控制台设置的服务帐户，"如本页所述" 。 单击“添加订阅”将选定的凭据与订阅关联。 要创建按使用量付费的Cloud Volumes ONTAP系统，您需要从 Google Cloud Marketplace 中选择与Cloud Volumes ONTAP订阅相关联的 Google Cloud 项目。参考 "将市场订阅与 Google Cloud 凭据关联"。

5. 服务：选择您想要在此系统上使用的服务。要选择备份和恢复，或使用NetApp Cloud Tiering，您必须在步骤 3 中指定服务帐户。

   如果您想使用 WORM 和数据分层，则必须禁用备份和恢复并部署版本 9.8 或更高版本的Cloud Volumes ONTAP系统。

6. **HA Deployment Models**：为 HA 配置选择多个区域（推荐）或单个区域。然后选择一个区域和可用区。

   "了解有关 HA 部署模型的更多信息" 。

7. 连接性：为 HA 配置选择四个不同的 VPC，每个 VPC 中选择一个子网，然后选择一个防火墙策略。

   "了解有关网络要求的更多信息" 。

   下表描述了您可能需要指导的字段：

字段	描述
生成的策略	如果您让控制台为您生成防火墙策略，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的源过滤器是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的源过滤器是 0.0.0.0/0 IP 范围。

字段	描述
使用现有的	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

8. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
   - "了解Cloud Volumes ONTAP的许可选项" 。
   - "了解如何设置许可" 。
9. 预配置包：选择其中一个包来快速部署Cloud Volumes ONTAP系统，或者单击*创建我自己的配置*。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。
10. 许可：根据需要更改Cloud Volumes ONTAP版本并选择机器类型。

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.13 到 9.14。
11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

    磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

    有关选择磁盘类型和大小的帮助，请参阅"在 Google Cloud 中调整系统大小"。
12. 闪存缓存、写入速度和 **WORM**：
    a. 如果需要，启用 **Flash Cache** 或选择*普通*或*高*写入速度。

       详细了解 "Flash Cache" 和 "写入速度"。

       通过 n2-standard-16、n2-standard-32、n2-standard-48 和 n2-standard-64 实例类型的高 写入速度选项，可以获得高写入速度和更高的 8,896 字节的最大传输单元 (MTU)。此外，8,896 的更高 MTU 要求选择 VPC-1、VPC-2 和 VPC-3 进行部署。高写入速度和 8,896 的 MTU 取决于功能，无法在配置的实例中单独禁用。有关 VPC-1、VPC-2 和 VPC-3 的更多信息，请参阅 "VPC-1、VPC-2 和 VPC-3 的规则"。

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       如果为Cloud Volumes ONTAP 9.7 及更低版本启用了数据分层，则无法启用 WORM。启用 WORM 和分层后，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。
13. **Google Cloud** 中的数据分层：选择是否在初始聚合上启用数据分层，为分层数据选择存储类，然后选择具有预定义存储管理员角色的服务帐户。

请注意以下事项：

- 控制台在Cloud Volumes ONTAP实例上设置服务帐户。此服务帐户提供将数据分层到 Google Cloud Storage 存储桶的权限。请确保将控制台代理服务帐户添加为分层服务帐户的用户，否则，您无法从控制台中选择它。
- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它，但您需要关闭系统并从 Google Cloud Console 添加服务帐户。

  "了解有关数据分层的更多信息" 。

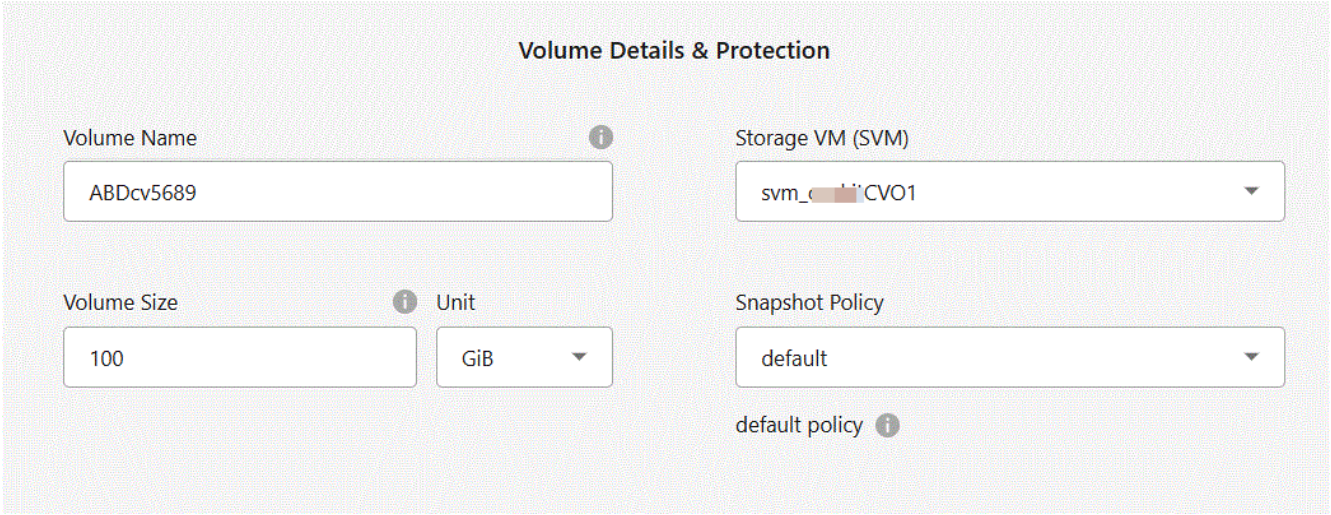
14. 创建卷：输入新卷的详细信息或单击*跳过*。

"了解支持的客户端协议和版本" 。

此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 策略	Snapshot 副本策略指定自动创建的NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 TCP 卸载引擎 (TOE) 卡、融合网络适配器 (CNA) 或专用主机总线适配器 (HBA) 连接到网络，并通过 iSCSI 限定名称 (IQN) 进行标识。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



15. **CIFS** 设置：如果您选择了 CIFS 协议，请设置 CIFS 服务器。

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。如果您正在配置 Google 管理的 Active Directory，则默认情况下可以使用 169.254.169.254 IP 地址访问 AD。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Google Managed Microsoft AD 配置为Cloud Volumes ONTAP的 AD 服务器，请在此字段中输入 **OU=Computers,OU=Cloud** 。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 文档：Google Managed Microsoft AD 中的组织单位"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

16. 使用情况配置文件、磁盘类型和分层策略：选择是否要启用存储效率功能并更改卷分层策略（如果需要）。

    更多信息，请参阅"选择卷使用情况配置文件"，"数据分层概述" ， 和 "KB：CVO 支持哪些内联存储效率功能？"

17. 审核并批准：审核并确认您的选择。

    a. 查看有关配置的详细信息。

b. 点击*更多信息*查看有关支持和控制台将购买的 Google Cloud 资源的详细信息。

c. 选中*我明白…*复选框。

d. 单击“开始”。

结果

控制台部署Cloud Volumes ONTAP系统。您可以在*审核*页面上跟踪进度。

如果您在部署Cloud Volumes ONTAP系统时遇到任何问题，请查看失败消息。您也可以选择系统并单击*重新创建环境*。

如需更多帮助，请访问 "NetApp Cloud Volumes ONTAP支持"。

完成后

- 如果您配置了 CIFS 共享，请授予用户或组对文件和文件夹的权限，并验证这些用户是否可以访问共享并创建文件。
- 如果要将配额应用于卷，请使用ONTAP系统管理器或ONTAP CLI。

  配额使您能够限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

部署流程完成后，请勿修改 Google Cloud 门户中系统生成的 Cloud Volumes ONTAP 配置，例如系统标签以及 Google Cloud 资源中设置的标签。对这些配置进行的任何更改都可能导致意外行为或数据丢失。

相关链接

- "在 Google Cloud 中规划Cloud Volumes ONTAP配置"

Google Cloud Platform 图像验证

了解如何在Cloud Volumes ONTAP中验证 Google Cloud 映像

Google Cloud 映像验证符合增强的NetApp安全要求。已经对生成图像的脚本进行了更改，以便使用专门为此任务生成的私钥对图像进行签名。您可以使用 Google Cloud 的签名摘要和公共证书来验证 Google Cloud 映像的完整性，该证书可通过以下方式下载 "国家安全局"针对特定版本。

Cloud Volumes ONTAP软件版本 9.13.0 或更高版本支持 Google Cloud 映像验证。

将 Google Cloud 映像转换为Cloud Volumes ONTAP 的原始格式

用于部署新实例、升级或在现有映像中使用的映像将通过以下方式与客户端共享 "NetApp 支持站点 (NSS)"。已签名的摘要和证书可通过 NSS 门户下载。确保您下载的摘要和证书与NetApp支持共享的图像对应的正确版本。例如，9.13.0 图像将具有 9.13.0 签名摘要和 NSS 上可用的证书。

为什么需要这一步？

无法直接下载来自 Google Cloud 的图片。为了根据签名的摘要和证书验证图像，您需要有一种机制来比较两个文件并下载图像。为此，您必须将图像导出/转换为 disk.raw 格式，并将结果保存在 Google Cloud 的存储桶中。在此过程中，disk.raw 文件被压缩并压缩。

用户/服务帐户需要权限才能执行以下操作：

- 访问 Google 存储桶
- 写入 Google 存储桶
- 创建云构建作业（在导出过程中使用）
- 访问所需图像
- 创建导出图像任务

要验证图像，必须将其转换为 disk.raw 格式，然后下载。

使用 **Google Cloud** 命令行导出 **Google Cloud** 镜像

将图像导出到云存储的首选方法是使用 "gcloud compute images export 命令"。此命令获取提供的图像并将其转换为 disk.raw 文件，然后对其进行 tar 和 gzip 压缩。生成的文件保存在目标URL，然后可以下载进行验证。

用户/帐户必须具有访问和写入所需存储桶、导出图像和云构建（Google 用于导出图像）的权限才能执行此操作。

使用 **gcloud** 导出 **Google Cloud** 镜像

点击显示

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

解压压缩文件

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

有关如何通过 Google Cloud 导出图像的更多信息，请参阅 "Google Cloud 文档：导出图像"。

图像签名验证

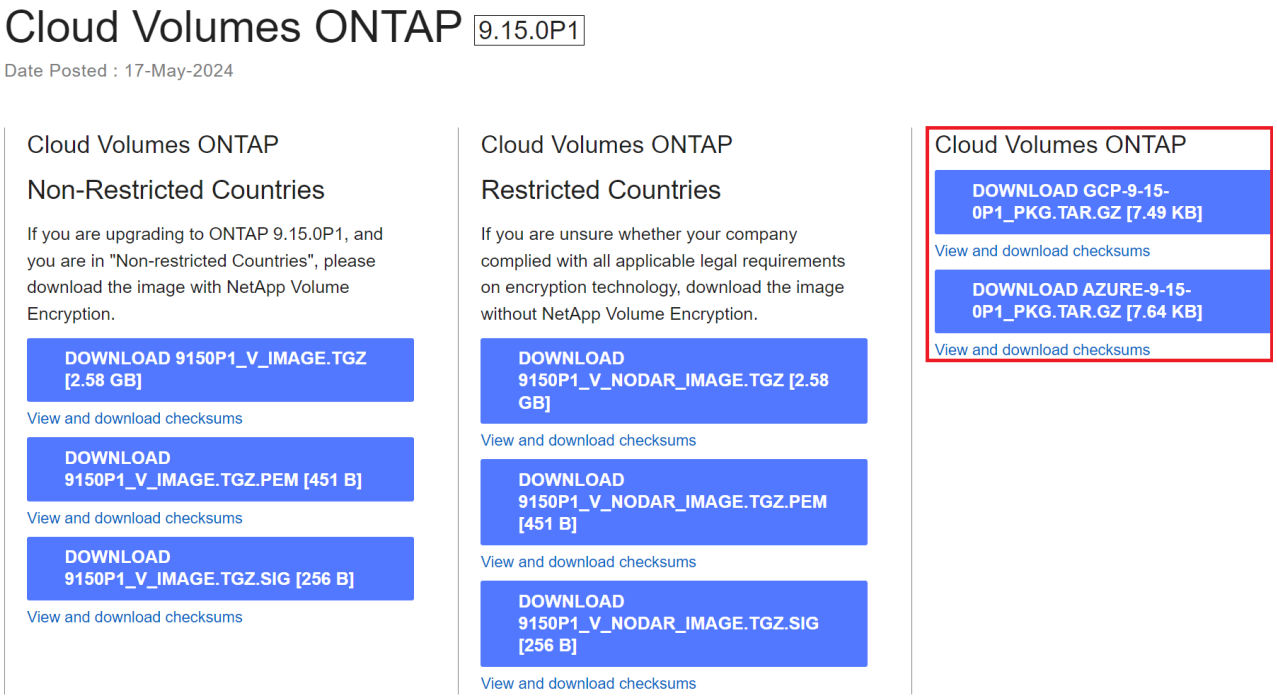
Cloud Volumes ONTAP的 **Google Cloud** 映像签名验证

要验证导出的 Google Cloud 签名映像，您必须从 NSS 下载映像摘要文件以验证 disk.raw 文件和摘要文件内容。

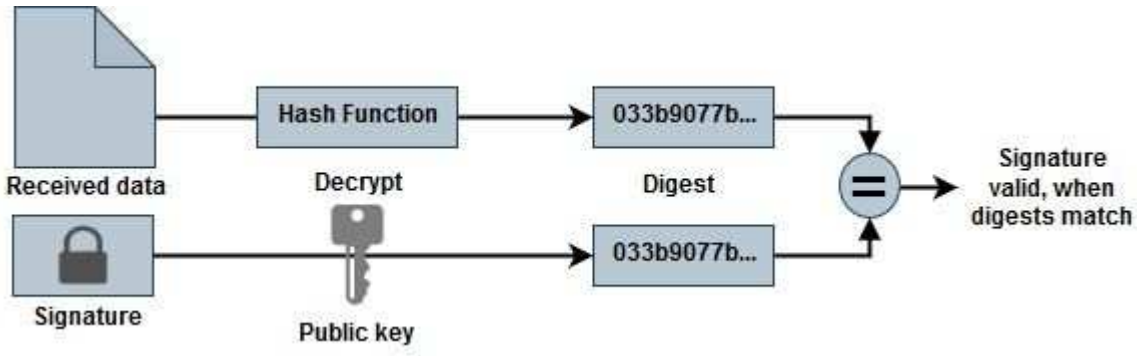
签名图像验证工作流程摘要

以下是 Google Cloud 签名图像验证工作流程的概述。

- 从 "国家安全局"，下载包含以下文件的 Google Cloud 存档：
  - 签名摘要（.sig）
  - 包含公钥的证书（.pem）
  - 证书链（.pem）



- 下载转换后的 disk.raw 文件
- 使用证书链验证证书
- 使用包含公钥的证书验证签名的摘要
  - 使用公钥解密签名的摘要，以提取图像文件的摘要
  - 创建下载的 disk.raw 文件的摘要
  - 比较两个摘要文件进行验证



使用 **OpenSSL** 验证**Cloud Volumes ONTAP**的 **Google Cloud** 映像 **disk.raw** 文件

您可以通过以下方式验证 Google Cloud 下载的 disk.raw 文件与摘要文件内容 "国家安全局"使用 OpenSSL。

用于验证图像的 OpenSSL 命令与 Linux、macOS 和 Windows 机器兼容。

步骤

1. 使用 OpenSSL 验证证书。

点击显示

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 将下载的 disk.raw 文件、签名和证书放在一个目录中。
3. 使用 OpenSSL 从证书中提取公钥。
4. 使用提取的公钥解密签名并验证下载的 disk.raw 文件的内容。

点击显示

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

版权信息

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

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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