在 GCP 中入门

Cloud Manager 3.8

NetApp
March 25, 2024

目录

在 GCP 中入门 . . . 1
- Cloud Volumes ONTAP for Google Cloud 入门 . . . 1
- 在 Google Cloud 中规划 Cloud Volumes ONTAP 配置 . . . 2
- 在 GCP 中部署和管理 Cloud Volumes ONTAP 的网络要求 . . . 5
- 将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用 . . . 13
- 在 GCP 中启动 Cloud Volumes ONTAP . . . 14

在 GCP 中入门

Cloud Volumes ONTAP for Google Cloud 入门

通过几个步骤开始使用适用于 GCP 的 Cloud Volumes ONTAP 。

创建连接器

如果您没有 "连接器" 但是，客户管理员需要创建一个。 "了解如何在 GCP 中创建连接器"。

在创建首个 Cloud Volumes ONTAP 工作环境时，如果尚未部署 Connector ，则 Cloud Manager 会提示您部署一个。

规划您的配置

Cloud Manager 可提供符合您的工作负载要求的预配置软件包，您也可以创建自己的配置。如果您选择自己的配置、则应了解可用的选项。 "了解更多信息。"。

设置网络

1. 确保您的 VPC 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
2. 从目标 VPC 启用出站 Internet 访问，以便连接器和 Cloud Volumes ONTAP 可以联系多个端点。

   此步骤非常重要，因为没有出站 Internet 访问， Connector 无法管理 Cloud Volumes ONTAP 。如果需要限制出站连接，请参阅的端点列表 "连接器和 Cloud Volumes ONTAP"。

"详细了解网络要求"。

设置用于数据分层的 **GCP**

要将冷数据从 Cloud Volumes ONTAP 分层到低成本对象存储（ Google 云存储分段），必须满足两项要求。

1. "为专用 Google 访问配置 Cloud Volumes ONTAP 子网"。
2. "设置用于数据分层的服务帐户"：
   - 将预定义的 *Storage Admin* 角色分配给分层服务帐户。
   - 将 Connector 服务帐户作为 *Service Account User* 添加到分层服务帐户。

     您可以提供用户角色 "在创建分层服务帐户时，请执行向导的第 3 步"或 "创建服务帐户后授予角色"。

     稍后在创建 Cloud Volumes ONTAP 工作环境时，您需要选择分层服务帐户。

如果在创建 Cloud Volumes ONTAP 系统时未启用数据分层并选择服务帐户，则需要关闭系统并从 GCP 控制台将服务帐户添加到 Cloud Volumes ONTAP 。

启用 **Google Cloud API**

"在项目中启用以下 Google Cloud API"。部署连接器和 Cloud Volumes ONTAP 需要使用这些 API 。

- Cloud Deployment Manager V2 API
- 云日志记录 API
- Cloud Resource Manager API
- 计算引擎 API
- 身份和访问管理（ IAM ） API

使用 **Cloud Manager** 启动 **Cloud Volumes ONTAP**

单击 * 添加工作环境 * ，选择要部署的系统类型，然后完成向导中的步骤。 "阅读分步说明"。

相关链接

- "评估"
- "使用 Cloud Manager 创建连接器"
- "在 Linux 主机上安装 Connector 软件"
- "Cloud Manager 如何使用 GCP 权限"

在 Google Cloud 中规划 Cloud Volumes ONTAP 配置

在 Google Cloud 中部署 Cloud Volumes ONTAP 时，您可以选择符合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、则应了解可用的选项。

选择许可证类型

Cloud Volumes ONTAP 有两种定价选项：按需购买和自带许可证（ BYOL ）。对于按需购买、可从三种许可证中进行选择： Explore 、 Standard 或 Premium 。每个许可证提供不同的容量和计算选项。

"GCP 中的 Cloud Volumes ONTAP 9.7 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。附加限制会影响聚合和卷的大小。在规划配置时，您应该了解这些限制。

"GCP 中 Cloud Volumes ONTAP 9.7 的存储限制"

在 GCP 中估算系统规模

对 Cloud Volumes ONTAP 系统进行规模估算有助于满足性能和容量要求。在选择计算机类型，磁盘类型和磁盘大小时，您应注意几个要点：

计算机类型

在中查看支持的计算机类型 "《 Cloud Volumes ONTAP 发行说明》" 然后查看 Google 提供的有关每个受支持计算机类型的详细信息。将工作负载要求与此计算机类型的 vCPU 和内存数量相匹配。请注意，每个 CPU 核心都会提高网络连接性能。

有关更多详细信息，请参见以下内容：

- "Google Cloud 文档： N1 标准计算机类型"
- "Google Cloud 文档：性能"

GCP 磁盘类型

在为 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 *zonal SSD persistent disks_or _zonal standard persistent disks*。

SSD 持久磁盘最适合需要高随机 IOPS 速率的工作负载，而标准持久磁盘经济实惠，可处理顺序读 / 写操作。有关详细信息，请参见 "Google Cloud 文档：区域持久性磁盘（标准和 SSD ）"。

GCP 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 Cloud Manager 为您管理系统的容量，但如果您要自行构建聚合，请注意以下事项：

- 聚合中的所有磁盘大小必须相同。
- 确定所需空间，同时考虑性能。
- 永久性磁盘的性能会随磁盘大小和系统可用的 vCPU 数量自动扩展。

  有关更多详细信息，请参见以下内容：

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

GCP 网络信息工作表

在 GCP 中部署 Cloud Volumes ONTAP 时，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收集信息。

GCP 信息	您的价值
Region	
分区	
VPC 网络	
Subnet	

GCP 信息	您的价值
防火墙策略（如果使用自己的策略）	

选择写入速度

利用 Cloud Manager ，您可以为单节点 Cloud Volumes ONTAP 系统选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和建议。

正常写入速度和高速写入速度之间的差异

选择正常写入速度后、数据将直接写入磁盘、从而减少发生计划外系统中断时数据丢失的可能性。

如果选择高速写入速度、则在将数据写入磁盘之前将数据缓冲在内存中、从而提供更快的写入性能。由于这种缓存，如果发生计划外系统中断，则可能会导致数据丢失。

在发生计划外系统中断时可能丢失的数据量是最后两个一致性点的范围。一致性点是将缓冲数据写入磁盘的操作。写入日志已满或 10 秒后（以先到者为准）会出现一致性点。但是， AWS EBS 卷性能可能会影响一致性点处理时间。

何时使用高速写入

如果您的工作负载需要快速写入性能、并且您可以在发生计划外系统中断时承受数据丢失的风险、则可以选择高速写入速度。

使用高速写入时的建议

如果启用高速写入速度、则应确保应用程序层的写保护。

选择卷使用情况配置文件

ONTAP 包含多种存储效率功能、可以减少您所需的存储总量。在 Cloud Manager 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、以帮助您确定要使用的配置文件。

NetApp 存储效率功能具有以下优势：

精简配置
: 为主机或用户提供的逻辑存储比实际在物理存储池中提供的存储多。在写入数据时，存储空间将动态分配给每个卷而不是预先分配存储空间。

重复数据删除
: 通过定位相同的数据块并将其替换为单个共享块的引用来提高效率。此技术通过消除驻留在同一卷中的冗余数据块来降低存储容量需求。

压缩
: 通过在主存储、二级存储和归档存储上的卷中压缩数据来减少存储数据所需的物理容量。

在 GCP 中部署和管理 Cloud Volumes ONTAP 的网络要求

设置您的 Google 云平台网络，以便 Cloud Volumes ONTAP 系统可以正常运行。其中包括连接器和 Cloud Volumes ONTAP 的网络连接。

Cloud Volumes ONTAP 的要求

以下要求必须在 GCP 中满足。

虚拟私有云

Cloud Volumes ONTAP 和 Connector 在 Google Cloud 共享 VPC 以及非共享 VPC 中均受支持。

通过共享 VPC ，您可以跨多个项目配置和集中管理虚拟网络。您可以在 *host project* 中设置共享 VPC 网络，并在 *service project* 中部署 Connector 和 Cloud Volumes ONTAP 虚拟机实例。 "Google Cloud 文档：共享 VPC 概述"。

使用共享 VPC 时的唯一要求是提供 "计算网络用户角色" 连接到 Connector 服务帐户。Cloud Manager 需要这些权限才能查询主机项目中的防火墙， VPC 和子网。

Cloud Volumes ONTAP 的出站 **Internet** 访问

Cloud Volumes ONTAP 要求出站 Internet 访问向 NetApp AutoSupport 发送消息、 NetApp AutoSupport 主动监控存储的运行状况。

路由和防火墙策略必须允许通过 HTTP/HTTPS 流量访问以下端点，以便 Cloud Volumes ONTAP 可以发送 AutoSupport 消息：

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"了解如何配置 AutoSupport"。

IP 地址数

Cloud Manager 会在 GCP 中为 Cloud Volumes ONTAP 分配 5 个 IP 地址。

请注意， Cloud Manager 不会在 GCP 中为 Cloud Volumes ONTAP 创建 SVM 管理 LIF 。

LIF 是与物理端口关联的 IP 地址。SnapCenter 等管理工具需要 SVM 管理 LIF 。

防火墙规则

您无需创建防火墙规则，因为 Cloud Manager 可以为您创建。如果您需要使用自己的防火墙规则，请参见下面列出的防火墙规则。

从 **Cloud Volumes ONTAP** 连接到 **Google** 云存储以进行数据分层

如果要将冷数据分层到 Google 云存储分段，则必须为 Cloud Volumes ONTAP 所在的子网配置私有 Google 访问。有关说明，请参见 "Google Cloud 文档：配置私有 Google Access"。

有关在 Cloud Manager 中设置数据分层所需的其他步骤，请参见 "将冷数据分层到低成本对象存储"。

连接到其他网络中的 **ONTAP** 系统

要在 GCP 中的 Cloud Volumes ONTAP 系统与其他网络中的 ONTAP 系统之间复制数据，您必须在 VPC 与其他网络（例如公司网络）之间建立 VPN 连接。

有关说明，请参见 "Google Cloud 文档： Cloud VPN 概述"。

连接器的要求

设置您的网络，以便 Connector 能够管理公有云环境中的资源和流程。最重要的步骤是确保对各种端点的出站 Internet 访问。

如果您的网络使用代理服务器与 Internet 进行所有通信，则可以从设置页面指定代理服务器。请参见 "将 Connector 配置为使用代理服务器"。

连接到目标网络

连接器要求与要部署 Cloud Volumes ONTAP 的 VPC 和 VN 集建立网络连接。

例如，如果您在公司网络中安装了连接器，则必须设置与启动 Cloud Volumes ONTAP 的 VPC 或 vNet 的 VPN 连接。

出站 **Internet** 访问

连接器需要通过出站 Internet 访问来管理公有云环境中的资源和流程。在 GCP 中管理资源时， Connector 会联系以下端点：

端点	目的
https://www.googleapis.com	使 Connector 能够联系 Google API 以在 GCP 中部署和管理 Cloud Volumes ONTAP 。
https://api.services.cloud.netapp.com:443	对 NetApp Cloud Central 的 API 请求。
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	提供对软件映像、清单和模板的访问。
https://repo.cloud.support.netapp.com	用于下载 Cloud Manager 依赖关系。
http://repo.mysql.com/	用于下载 MySQL 。
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	使 Connector 能够访问和下载清单，模板和 Cloud Volumes ONTAP 升级映像。
https://cloudmanagerinfraprod.azurecr.io	访问运行 Docker 的基础架构中容器组件的软件映像，并提供解决方案以实现与 Cloud Manager 的服务集成。
https://kinesis.us-east-1.amazonaws.com	使 NetApp 能够从审计记录流化数据。
https://cloudmanager.cloud.netapp.com	与 Cloud Manager 服务进行通信，其中包括 Cloud Central 帐户。

端点	目的
https://netapp-cloud-account.auth0.com	与 NetApp Cloud Central 进行通信以实现集中式用户身份验证。
https://mysupport.netapp.com	与 NetApp AutoSupport 通信。
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	与 NetApp 沟通以获得系统许可和支持注册。
https://ipa-signer.cloudmanager.netapp.com	允许 Cloud Manager 生成许可证（例如，适用于 Cloud Volumes ONTAP 的 FlexCache 许可证）
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	要将 Cloud Volumes ONTAP 系统连接到 Kubernetes 集群，需要此许可证。这些端点支持安装 NetApp Trident 。
各种第三方位置，例如： • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repository • https://repo.typesafe.org 第三方位置可能会发生变化。	在升级过程中、 Cloud Manager 会下载最新的软件包以满足第三方依赖性。

虽然您应该从 SaaS 用户界面执行几乎所有任务，但连接器上仍提供本地用户界面。运行 Web 浏览器的计算机必须连接到以下端点：

端点	目的
Connector 主机	要加载 Cloud Manager 控制台，必须从 Web 浏览器输入主机的 IP 地址。 根据您与云提供商的连接，您可以使用分配给主机的专用 IP 或公有 IP ： • 如果您对虚拟网络具有 VPN 和直接连接访问权限，则专用 IP 可以正常工作 • 公有 IP 可用于任何网络连接情形 在任何情况下，您都应确保安全组规则仅允许从授权的 IP 或子网进行访问，从而确保网络访问的安全。
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	您的 Web 浏览器连接到这些端点、以便通过 NetApp Cloud Central 进行集中式用户身份验证。
https://widget.intercom.io	用于与 NetApp 云专家交流的产品内聊天。

Cloud Volumes ONTAP 的防火墙规则

Cloud Manager 可创建包含 Cloud Manager 和 Cloud Volumes ONTAP 成功运行所需的入站和出站规则的 GCP 防火墙规则。您可能希望参考这些端口进行测试或使用自己的安全组。

Cloud Volumes ONTAP 的防火墙规则需要入站和出站规则。

入站规则

预定义安全组中入站规则的源代码为 0.0.0.0/0 。

协议	**Port**	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
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 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
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 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

出站规则

为 Cloud Volumes ONTAP 预定义的安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

为 Cloud Volumes ONTAP 预定义的安全组包括以下出站规则。

协议	**Port**	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

如果您需要严格的出站流量规则、则可以使用以下信息仅打开 Cloud Volumes ONTAP 出站通信所需的端口。

源是 Cloud Volumes ONTAP 系统上的接口（ IP 地址）。

服务	协议	Port	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	节点管理 LIF	Active Directory 目录林	LDAP
	TCP	445	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	UDP	464.	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）
	TCP	88	数据 LIF （ NFS ， CIFS ， iSCSI ）	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	LDAP
	TCP	445	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	UDP	464.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）

服务	协议	Port	源	目标	目的
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信（仅限 Cloud Volumes ONTAP HA ）
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用（仅适用于 Cloud Volumes ONTAP HA ）
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态（仅限 Cloud Volumes ONTAP HA ）
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	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 副本
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	管理 SnapMirror 的集群间通信会话
	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	系统日志转发消息

Connector 的防火墙规则

Connector 的防火墙规则需要入站和出站规则。

入站规则

预定义的防火墙规则中的入站规则源为 0.0.0.0/0 。

协议	Port	目的
SSH	22.	提供对 Connector 主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

出站规则

连接器的预定义防火墙规则会打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

Connector 的预定义防火墙规则包括以下出站规则。

协议	**Port**	目的
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设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。

源 IP 地址是 Connector 主机。

服务	协议	**Port**	目标	目的
Active Directory	TCP	88	Active Directory 目录林	Kerberos V 身份验证
	TCP	139.	Active Directory 目录林	NetBIOS 服务会话
	TCP	389.	Active Directory 目录林	LDAP
	TCP	445	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	TCP	749	Active Directory 目录林	Active Directory Kerberos V 更改和设置密码（ RPCSEC_GSS ）
	UDP	137.	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	Active Directory 目录林	NetBIOS 数据报服务
	UDP	464.	Active Directory 目录林	Kerberos 密钥管理

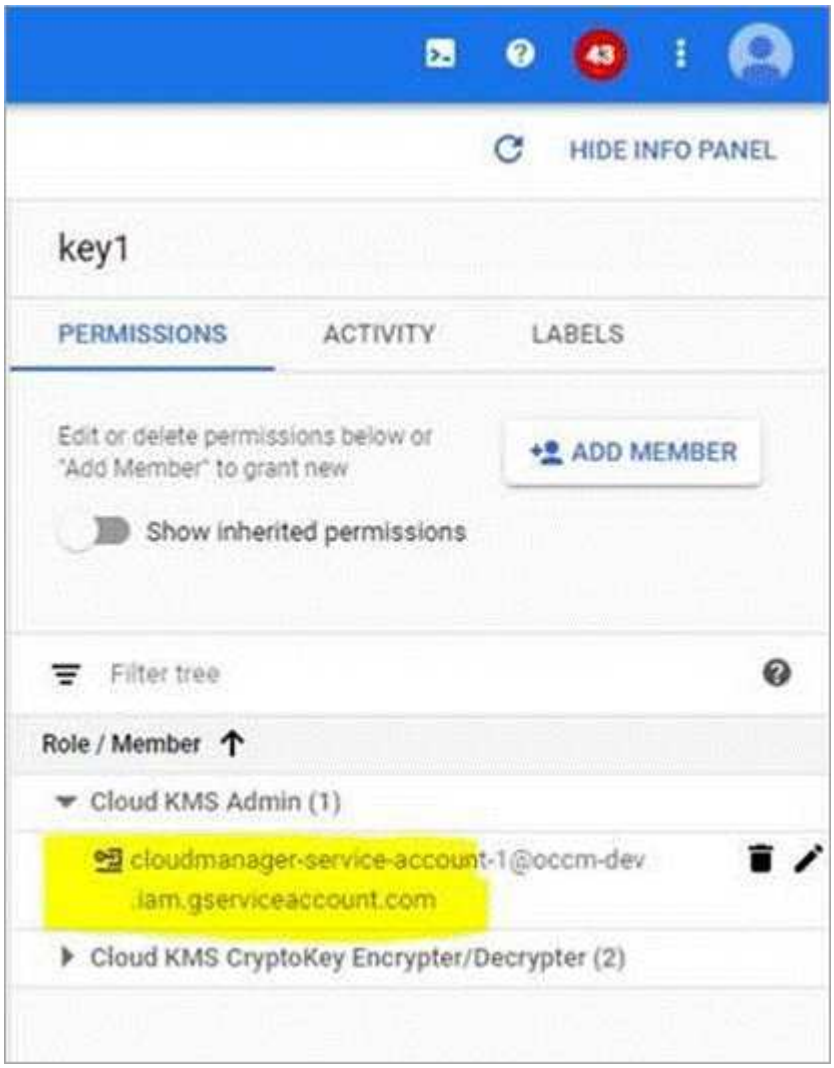
服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 GCP 和 ONTAP 、并将 AutoSupport 消息发送到 NetApp
API 调用	TCP	3000	ONTAP 集群管理 LIF	API 调用 ONTAP
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用

虽然 Google Cloud Storage 始终会在数据写入磁盘之前对数据进行加密，但您可以使用 Cloud Manager API 创建使用 *customer-managed encryption keys* 的 Cloud Volumes ONTAP 系统。这些密钥可通过云密钥管理服务在 GCP 中生成和管理。

步骤

1. 为 Connector 服务帐户授予使用加密密钥的权限。



2. 通过调用 /GCP/vsa/metadata/GCP-encryption-keys API 的 get 命令来获取密钥的 "id" 。
3. 创建工作环境时，请在 API 请求中使用 "GcpEncryption" 参数。

    ◦ 示例 *

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

请参见 "API 开发人员指南" 有关使用 GcpEncryption 参数的详细信息，请参见。

在 GCP 中启动 Cloud Volumes ONTAP

您可以通过创建工作环境在 GCP 中启动单节点 Cloud Volumes ONTAP 系统。

您需要的内容

- 您应具有 "与工作空间关联的连接器"。

    您必须是帐户管理员才能创建 Connector 。在创建首个 Cloud Volumes ONTAP 工作环境时，如果您还没有连接器，则 Cloud Manager 会提示您创建一个连接器。

- "您应做好准备，使 Connector 始终保持运行"。
- 您应已选择配置并从管理员处获取 GCP 网络信息。有关详细信息，请参见 "规划 Cloud Volumes ONTAP 配置"。
- 要部署 BYOL 系统，您需要每个节点的 20 位序列号（许可证密钥）。
- 以下 Google Cloud API 应为 "已在项目中启用"：
    - Cloud Deployment Manager V2 API
    - 云日志记录 API
    - Cloud Resource Manager API
    - 计算引擎 API
    - 身份和访问管理（ IAM ） API

步骤

1. 在工作环境页面上，单击 * 添加工作环境 * 并按照提示进行操作。
2. * 选择一个位置 * ： 选择 * Google Cloud* 和 * Cloud Volumes ONTAP * 。
3. * 详细信息和凭据 * ： 选择项目，指定集群名称，可选择添加标签，然后指定凭据。

    下表介绍了可能需要指导的字段：

字段	Description
工作环境名称	Cloud Manager 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 GCP VM 实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标签	标签是 GCP 资源的元数据。Cloud Manager 会将标签添加到与该系统关联的 Cloud Volumes ONTAP 系统和 GCP 资源中。在创建工作环境时，您最多可以从用户界面添加四个标签，然后可以在创建后添加更多标签。请注意，在创建工作环境时， API 不会将您限制为四个标签。有关标签的信息，请参见 "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 System Manager 或其命令行界面连接到 Cloud Volumes ONTAP 。
编辑项目	选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是 Cloud Manager 所在的项目。 如果您在下拉列表中未看到任何其他项目，则表示您尚未将 Cloud Manager 服务帐户与其他项目关联。转到 Google Cloud 控制台，打开 IAM 服务，然后选择项目。将具有 Cloud Manager 角色的服务帐户添加到该项目中。您需要对每个项目重复此步骤。 这是您为 Cloud Manager 设置的服务帐户， "如本页的步骤 2b 中所述"。 单击 * 添加订阅 * 将选定凭据与订阅关联。 要创建按需购买的 Cloud Volumes ONTAP 系统，您需要从 GCP 市场中选择与 Cloud Volumes ONTAP 订阅关联的 GCP 项目。

以下视频介绍了如何将按需购买的 Marketplace 订阅与您的 GCP 项目相关联：

► https://docs.netapp.com/zh-cn/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. * 位置和连接 * ：选择一个位置，选择防火墙策略，然后选中复选框以确认与 Google Cloud 存储的网络连接以进行数据分层。

   如果要将冷数据分层到 Google 云存储分段，则必须为 Cloud Volumes ONTAP 所在的子网配置私有 Google 访问。有关说明，请参见 "Google Cloud 文档：配置私有 Google Access"。

5. * 许可证和支持站点帐户 * ：指定是要使用按需购买还是 BYOL ，然后指定 NetApp 支持站点帐户。

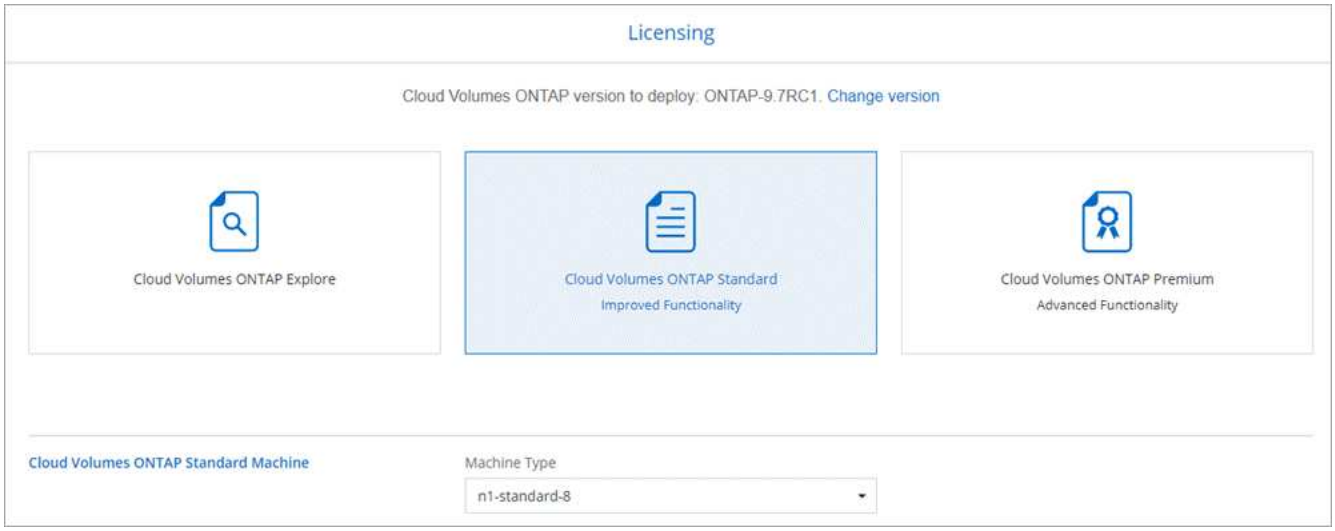
   要了解许可证的工作原理，请参见 "许可"。

   对于按需购买， NetApp 支持站点帐户是可选的，但对于 BYOL 系统则是必需的。 "了解如何添加 NetApp 支持站点帐户"。

6. * 预配置软件包 * ：选择一个软件包以快速部署 Cloud Volumes ONTAP 系统，或者单击 * 创建自己的配置 * 。

   如果选择其中一个包、则只需指定卷、然后检查并批准配置。

7. * 许可 * ：根据需要更改 Cloud Volumes ONTAP 版本，选择许可证并选择虚拟机类型。



如果在启动系统后需要更改、您可以稍后修改许可证或虚拟机类型。

> 如果选定版本有较新的候选版本、一般可用性或修补程序版本可用、则在创建工作环境时，Cloud Manager 会将系统更新为该版本。例如，如果您选择 Cloud Volumes ONTAP 9.6 RC1 和 9.6 GA 可用，则会发生此更新。更新不会从一个版本更新到另一个版本，例如从 9.6 到 9.7 。

8. * 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 Simple Provisioning （简单配置）选项时 Cloud Manager 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，请参见 "在 GCP 中估算系统规模"。

9. * 写入速度和 WORM* ： 选择 * 正常 * 或 * 高 * 写入速度，并根据需要激活一次写入，多次读取（ WORM ）存储。

   仅单节点系统支持选择写入速度。

   "了解有关写入速度的更多信息。"。

   如果启用了数据分层，则无法启用 WORM 。

   "了解有关 WORM 存储的更多信息。"。

10. * Google Cloud Platform 中的数据分层 * ： 选择是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（对于 Cloud Volumes ONTAP 9.7 为必需），还是选择 GCP 帐户（对于 Cloud Volumes ONTAP 9.6 为必需）。

    请注意以下事项：

    - Cloud Manager 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 存储分段的权限。请务必以分层服务帐户的用户身份添加 Cloud Manager 服务帐户，否则无法从 Cloud Manager 中选择它。

- 有关添加 GCP 帐户的帮助，请参见 "使用 9.6 设置和添加用于数据分层的 GCP 帐户"。
- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果禁用数据分层，则可以在后续聚合上启用该功能，但您需要关闭系统并从 GCP 控制台添加服务帐户。

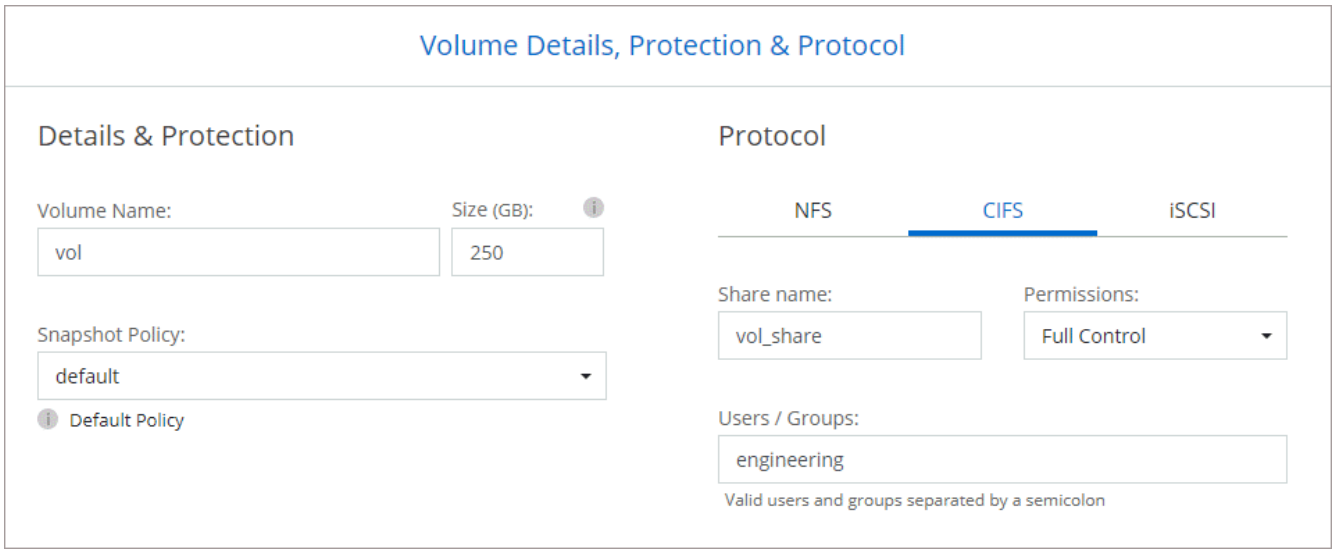
  "了解有关数据分层的更多信息。"。

11. * 创建卷 * ： 输入新卷的详细信息或单击 * 跳过 * 。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	Description
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS ）	导出策略定义子网中可以访问卷的客户端。默认情况下， Cloud Manager 会输入一个值、用于访问子网中的所有实例。
权限和用户 / 组（仅限 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、 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如， Microsoft SQL Server 的 tempdb 。
高级选项（仅适用于 NFS ）	为卷选择 NFS 版本： NFSv3 或 NFSv4 。
启动程序组和 IQN （仅适用于 iSCSI ）	iSCSI 存储目标称为 LUN （逻辑单元），并作为标准块设备提供给主机。启动程序组是包含 iSCSI 主机节点名称的表，用于控制哪些启动程序可以访问哪些 LUN 。iSCSI 目标通过标准以太网网络适配器（ NIC ），带软件启动程序的 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。创建 iSCSI 卷时， Cloud Manager 会自动为您创建 LUN 。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后， "使用 IQN 从主机连接到 LUN"。

下图显示了已填写 CIFS 协议的卷页面：



12. * CIFS 设置 * ：如果选择 CIFS 协议，请设置 CIFS 服务器。

字段	Description
DNS 主 IP 地址和次 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 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
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 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers 。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）的 DNS 域。在大多数情况下，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。如果需要使用其他地址配置 NTP 服务器，则应使用 API 。请参见 "Cloud Manager API 开发人员指南" 了解详细信息。

13. * 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，并根据需要更改卷分层策略。

    有关详细信息，请参见 "了解卷使用情况配置文件" 和 "数据分层概述"。

14. * 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. 单击 * 更多信息 * 可查看有关 Cloud Manager 将购买的支持和 GCP 资源的详细信息。
    c. 选中 * 我了解 …* 复选框。
    d. 单击 * 执行 * 。

结果

Cloud Manager 部署了 Cloud Volumes ONTAP 系统。您可以跟踪时间链中的进度。

如果您在部署 Cloud Volumes ONTAP 系统时遇到任何问题、请查看故障消息。您也可以选择工作环境并单击 * 重新创建环境 * 。

要获得更多帮助，请转至 "NetApp Cloud Volumes ONTAP 支持"。

完成后

- 如果配置了 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该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI 。

  配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。