



## 开始使用 **Google Cloud** Cloud Volumes ONTAP

NetApp  
May 09, 2022

This PDF was generated from <https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html> on May 09, 2022. Always check docs.netapp.com for the latest.

# 目录

|   |    |
|---|----|
| 开始使用 Google Cloud .....                         | 1  |
| 在 Google Cloud 中快速启动 Cloud Volumes ONTAP .....  | 1  |
| 在 Google Cloud 中规划 Cloud Volumes ONTAP 配置 ..... | 2  |
| GCP 中的 Cloud Volumes ONTAP 的网络要求 .....          | 5  |
| 在 GCP 中规划 VPC 服务控制 .....                        | 15 |
| 创建用于数据分层和备份的服务帐户 .....                          | 17 |
| 将客户管理的加密密钥与 Cloud Volumes ONTAP 结合使用 .....      | 20 |
| 在 GCP 中启动 Cloud Volumes ONTAP .....             | 21 |

# 开始使用 Google Cloud

## 在 Google Cloud 中快速启动 Cloud Volumes ONTAP

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

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。

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。

["了解有关规划配置的更多信息"](#)。

跨度 `class="image">https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png"</a> Alt-Three "></span><span> 设置您的网络连接`

1. 确保您的 VPC 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
2. 如果您计划启用数据分层， ["为专用 Google 访问配置 Cloud Volumes ONTAP 子网"](#)。
3. 如果要部署 HA 对，请确保您有四个 vPC，每个 vPC 都有自己的子网。
4. 如果您使用的是共享 VPC，请为 Connector 服务帐户提供 *Compute Network User* 角色。
5. 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"](#)。

Cloud Volumes ONTAP 需要一个 Google Cloud 服务帐户，用于两种目的。第一种情况是启用时 ["数据分层"](#) 在 Google Cloud 中将冷数据分层到低成本对象存储。第二种情况是在启用时 ["Cloud Backup Service"](#) 将卷备份到低成本对象存储。

您可以设置一个服务帐户并将其用于这两种目的。服务帐户必须具有 *\* 存储管理员 \** 角色。

["阅读分步说明"](#)。

["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

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

- ["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。

### 查看支持的区域

大多数 Google Cloud 地区均支持 Cloud Volumes ONTAP。 ["查看支持的区域的完整列表"](#)。

### 选择许可证

Cloud Volumes ONTAP 提供了多种许可选项。每个选项都允许您选择一种满足您需求的消费模式。 ["了解 Cloud Volumes ONTAP 的许可选项"](#)。

### 支持的计算机类型

Cloud Volumes ONTAP 支持多种计算机类型，具体取决于您选择的许可证类型。

["GCP 中支持的 Cloud Volumes ONTAP 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 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。磁盘类型可以是以下任一项：

- *Zonal SSD Persistent disks*：SSD 永久性磁盘最适合需要高随机 IOPS 速率的工作负载。
- *Zonal Balanced\_Persistent disks*：这些 SSD 通过提供更低的每 GB IOPS 来平衡性能和成本。
- *Zonal Standard Persistent disks*：标准持久性磁盘经济实惠，可以处理顺序读 / 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"](#)

## 查看默认系统磁盘

除了用户数据存储之外，Cloud Manager 还为 Cloud Volumes ONTAP 系统数据（启动数据，根数据，核心数据和 NVRAM）购买云存储。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。

- ["在 Google Cloud 中查看 Cloud Volumes ONTAP 系统数据的默认磁盘"](#)。
- ["Google Cloud 文档：资源配额"](#)

Google 云计算引擎对资源使用量实施配额，因此在部署 Cloud Volumes ONTAP 之前，您应确保未达到限制。



此连接器还需要一个系统磁盘。 ["查看有关连接器默认配置的详细信息"](#)。

## 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。

- 单节点系统的网络信息 \*

| GCP 信息           | 您的价值 |
|------------------|------|
| Region           |      |
| 分区               |      |
| VPC 网络           |      |
| Subnet           |      |
| 防火墙策略（如果使用自己的策略） |      |

- 多个分区中 HA 对的网络信息 \*

| GCP 信息           | 您的价值 |
|------------------|------|
| Region           |      |
| 节点 1 的分区         |      |
| 节点 2 的分区         |      |
| 调解器的分区           |      |
| 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（如果使用自己的策略） |      |

- 单个分区中 HA 对的网络信息 \*

| GCP 信息           | 您的价值 |
|------------------|------|
| Region           |      |
| 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（如果使用自己的策略） |      |

## 选择写入速度

您可以通过 Cloud Manager 为 Cloud Volumes ONTAP 选择写入速度设置，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](#)。"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。

## GCP 中的 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。

如果要部署 HA 对，则应执行此操作 ["了解 HA 对在 GCP 中的工作原理"](#)。

### Cloud Volumes ONTAP 的要求

以下要求必须在 GCP 中满足。

#### 内部负载均衡器

Cloud Manager 会自动创建四个 Google Cloud 内部负载均衡器（TCP/UDP），用于管理传入到 Cloud Volumes ONTAP HA 对的流量。您无需进行任何设置我们将此列为一项要求，只是为了告知您网络流量并缓解任何安全问题。

一个负载均衡器用于集群管理，一个负载均衡器用于 Storage VM（SVM）管理，一个负载均衡器用于向节点 1 发送 NAS 流量，另一个负载均衡器用于向节点 2 发送 NAS 流量。

每个负载均衡器的设置如下：

- 一个共享专用 IP 地址
- 一次全局运行状况检查

默认情况下，运行状况检查使用的端口为 63001，63002 和 63003。

- 一个区域 TCP 后端服务
- 一个区域 UDP 后端服务
- 一个 TCP 转发规则

- 一个 UDP 转发规则
- 已禁用全局访问

即使默认情况下全局访问处于禁用状态，也支持在部署后启用全局访问。我们禁用了此功能，因为跨区域流量的延迟会显著增加。我们希望确保您不会因意外的跨区域挂载而产生负面体验。启用此选项取决于您的业务需求。

## HA 对的一个或多个分区

您可以通过在多个或单个分区中部署 HA 配置来确保数据的高可用性。创建 HA 对时，Cloud Manager 将提示您选择多个分区或单个分区。

- 多个分区（建议）

在三个分区之间部署 HA 配置可确保在分区发生故障时持续提供数据。请注意，与使用单个分区相比，写入性能略低，但写入性能极低。

- 单个分区

在单个区域中部署时，Cloud Volumes ONTAP HA 配置会使用分布放置策略。此策略可确保 HA 配置免受分区内单点故障的影响，而无需使用单独的分区来实现故障隔离。

此部署模式确实可以降低成本，因为分区之间没有数据传出费用。

## 适用于 HA 对的四个虚拟私有云

一个 HA 配置需要四个虚拟私有云（Virtual Private Cloud，vPC）。需要四个 VPC，因为 GCP 要求每个网络接口驻留在一个单独的 VPC 网络中。

创建 HA 对时，Cloud Manager 将提示您选择四个 vPC：

- vPC-0，用于与数据和节点的入站连接
- VPC-1，VPC-2 和 VPC-3，用于节点与 HA 调解器之间的内部通信





## HA 对的子网

每个 VPC 都需要一个专用子网。

如果将 Connector 置于 VPC-0 中，则需要在子网上启用专用 Google 访问才能访问 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。它们不能具有重叠的 CIDR 范围。

## 一个适用于单节点系统的虚拟私有云

单节点系统需要一个 VPC。

## 共享 vPC

Cloud Volumes ONTAP 和 Connector 在 Google Cloud 共享 VPC 以及独立 VPC 中均受支持。

对于单节点系统，VPC 可以是共享 VPC，也可以是独立 VPC。

对于 HA 对，需要四个 vPC。其中每个 VPC 都可以是共享的，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。

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"](#)。

["查看 Connector 部署中涉及的所需共享 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 VPC 中禁用。如果启用了数据包镜像，则 Cloud Volumes ONTAP 无法正常运行。

## 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>

["了解如何验证 AutoSupport"](#)。



如果您使用的是 HA 对，则 HA 调解器不需要出站 Internet 访问。

## 专用 IP 地址

Cloud Manager 将以下数量的专用 IP 地址分配给 GCP 中的 Cloud Volumes ONTAP：

- \* 单节点 \*：3 或 4 个专用 IP 地址

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 Storage VM（SVM）管理 LIF：

```
skipSvmManagementLif : true
```

LIF 是与物理端口关联的 IP 地址。SnapCenter 等管理工具需要使用 Storage VM（SVM）管理 LIF。

- \* HA 对 \*：14 或 15 个专用 IP 地址
  - VPC-0 的 7 或 8 个专用 IP 地址

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 Storage VM（SVM）管理 LIF：

```
skipSvmManagementLif : true
```

- VPC-1 的两个专用 IP 地址
- VPC-2 的两个专用 IP 地址
- VPC-3 的三个专用 IP 地址

## 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。

请注意，HA 配置需要两组防火墙规则：

- VPC-0 中 HA 组件的一组规则。这些规则允许对 Cloud Volumes ONTAP 进行数据访问。 [了解更多信息。](#)
- VPC-1，VPC-2 和 VPC-3 中 HA 组件的另一组规则。这些规则适用于 HA 组件之间的入站和出站通信。 [了解更多信息。](#)

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

如果您要将冷数据分层到 Google 云存储分段，则必须为 Cloud Volumes ONTAP 所在的子网配置专用 Google 访问（如果您使用的是 HA 对，则此子网位于 VPC-0 中）。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 建立网络连接。如果要部署 HA 对，则 Connector 只需要连接到 VPC-0。

## 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。

| 端点   | 目的                                     |
|--|--|
| <a href="https://support.netapp.com">https://support.netapp.com</a>  | 获取许可信息并向 NetApp 支持部门发送 AutoSupport 消息。 |
| <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>  | 在 Cloud Manager 中提供 SaaS 功能和服务。        |
| <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> | 升级 Connector 及其 Docker 组件。             |

## Cloud Volumes ONTAP 的防火墙规则

Cloud Manager 可创建包含 Cloud Volumes ONTAP 成功运行所需入站和出站规则的 GCP 防火墙规则。您可能需要参考端口进行测试，或者如果您希望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。

如果要部署 HA 配置，这些是 VPC-0 中 Cloud Volumes ONTAP 的防火墙规则。

## 入站规则

对于HA对、预定义的防火墙策略中入站流量的源筛选器为0.0.0.0/0。

对于单节点系统、您可以在部署期间为预定义的防火墙策略选择源筛选器：

- 仅选定**VPC**：入站流量的源筛选器是Cloud Volumes ONTAP 系统VPC的子网范围以及连接器所在VPC的子网范围。这是建议的选项。
- 所有VPC\*：入站流量的源筛选器为0.0.0.0/0 IP范围。

如果您使用自己的防火墙策略、请确保添加需要与Cloud Volumes ONTAP 通信的所有网络、但同时确保同时添加两个地址范围、以使内部Google负载均衡器正常运行。这些地址为 130.11.0.0/22 和 35.191.0.0/16 。有关详细信息，请参见 "[Google Cloud 文档：负载均衡器防火墙规则](#)"。

| 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                          |
| TCP     | 63001-63050 | 负载均衡探测端口，用于确定哪个节点运行状况良好（仅 HA 对需要）                     |
| UDP     | 111.        | 远程过程调用 NFS  |
| UDP     | 161-162.    | 简单网络管理协议  |

| 协议  | Port  | 目的             |
|-----|-------|----------------|
| 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 ）                 |
| AutoSupport      | HTTPS     | 443. | 节点管理 LIF                      | support.netapp.com   | AutoSupport （默认设置为 HTTPS ）                        |
|                  | HTTP      | 80   | 节点管理 LIF                      | support.netapp.com   | AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）            |

| 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） |
| 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  | 系统日志                             |
| TCP | 11105.        | 集群间 LIF                    | ONTAP 集群间 LIF | SnapMirror 数据传输         |                                  |

## VPC-1 ， VPC-2 和 VPC-3 的防火墙规则

在 GCP 中， HA 配置部署在四个 VPC 上。VPC-0 中的 HA 配置所需的防火墙规则为 [上面列出的 Cloud Volumes ONTAP](#)。

同时， Cloud Manager 为 VPC-1 ， VPC-2 和 VPC-3 中的实例创建的预定义防火墙规则可通过 *all* 协议和端口进行传入通信。这些规则允许 HA 节点之间进行通信。

从 HA 节点到 HA 调解器的通信通过端口 3260 （ iSCSI ） 进行。

## 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

| 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   |
|---------------------|-------|------|------------------------------|--|
| API 调用和 AutoSupport | HTTPS | 443. | 出站 Internet 和 ONTAP 集群管理 LIF | API 调用 GCP 和 ONTAP ， 云数据感知， 勒索软件服务以及向 NetApp 发送 AutoSupport 消息 |



| 服务  | 协议  | Port | 目标  | 目的              |
|-----|-----|------|-----|-----------------|
| DNS | UDP | 53.  | DNS | 用于云管理器进行 DNS 解析 |

## 在 GCP 中规划 VPC 服务控制

选择使用 VPC 服务控制锁定 Google 云环境时，您应了解 Cloud Manager 和 Cloud Volumes ONTAP 如何与 Google 云 API 交互，以及如何配置服务边界以部署 Cloud Manager 和 Cloud Volumes ONTAP。

通过 VPC 服务控制，您可以控制对受信任边界以外 Google 管理的服务的访问，阻止来自不受信任位置的数据访问以及降低未经授权的数据传输风险。["了解有关 Google Cloud VPC 服务控制的更多信息"](#)。

### NetApp 服务如何与 VPC 服务控制进行通信

Cloud Central 和 Cloud Manager 等 NetApp 服务可直接与 Google Cloud API 进行通信。这是从 Google Cloud 外部的 IP 地址（例如，从 `api.services.cloud.netapp.com`）触发的，或者从分配给 Cloud Manager Connector 的内部地址在 Google Cloud 内部触发的。

根据连接器的部署模式，可能需要对服务范围进行某些例外处理。

### 映像

Cloud Volumes ONTAP 和 Cloud Manager 都使用由 NetApp 管理的 GCP 中某个项目的映像。如果您的组织的策略阻止使用未托管在组织中的映像，则这可能会影响 Cloud Manager Connector 和 Cloud Volumes ONTAP 的部署。

您可以使用手动安装方法手动部署连接器，但 Cloud Volumes ONTAP 也需要从 NetApp 项目中提取映像。要部署连接器和 Cloud Volumes ONTAP，必须提供允许的列表。

### 部署连接器

部署 Connector 的用户需要能够引用 projectId `netapp-cloudmanager` 中托管的映像，项目编号 `141900 56516`。

### 部署 Cloud Volumes ONTAP

- Cloud Manager 服务帐户需要引用服务项目中 projectId `netapp-cloudmanager` 和项目编号 `1419056516` 中托管的映像。
- 默认 Google API Service Agent 的服务帐户需要引用服务项目中 projectId `netapp-cloudmanager` 和项目编号 `1419056516` 中托管的映像。

下面定义了使用 VPC 服务控制提取这些映像所需的规则示例。

### VPC 服务控制外围策略

策略允许对 VPC 服务控制规则集进行例外处理。有关策略的详细信息，请访问 ["GCP VPC 服务控制策略文档"](#)。

要设置 Cloud Manager 所需的策略，请导航到组织内的 VPC 服务控制外围并添加以下策略。这些字段应与 VPC 服务控制策略页面中提供的选项匹配。另请注意，需要使用 \* 所有 \* 规则，并且规则集中应使用 \* 或 \* 参数。

#### 传入规则

```
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
```

## 外出规则

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



上述项目编号是 NetApp 用于存储 Connector 和 Cloud Volumes ONTAP 映像的 *netapp-cloudmanager* 项目。

## 创建用于数据分层和备份的服务帐户

Cloud Volumes ONTAP 需要一个 Google Cloud 服务帐户，用于两种目的。第一种情况是启用时 **"数据分层"** 在 Google Cloud 中将冷数据分层到低成本对象存储。第二种情况是在启用时 **"Cloud Backup Service"** 将卷备份到低成本对象存储。

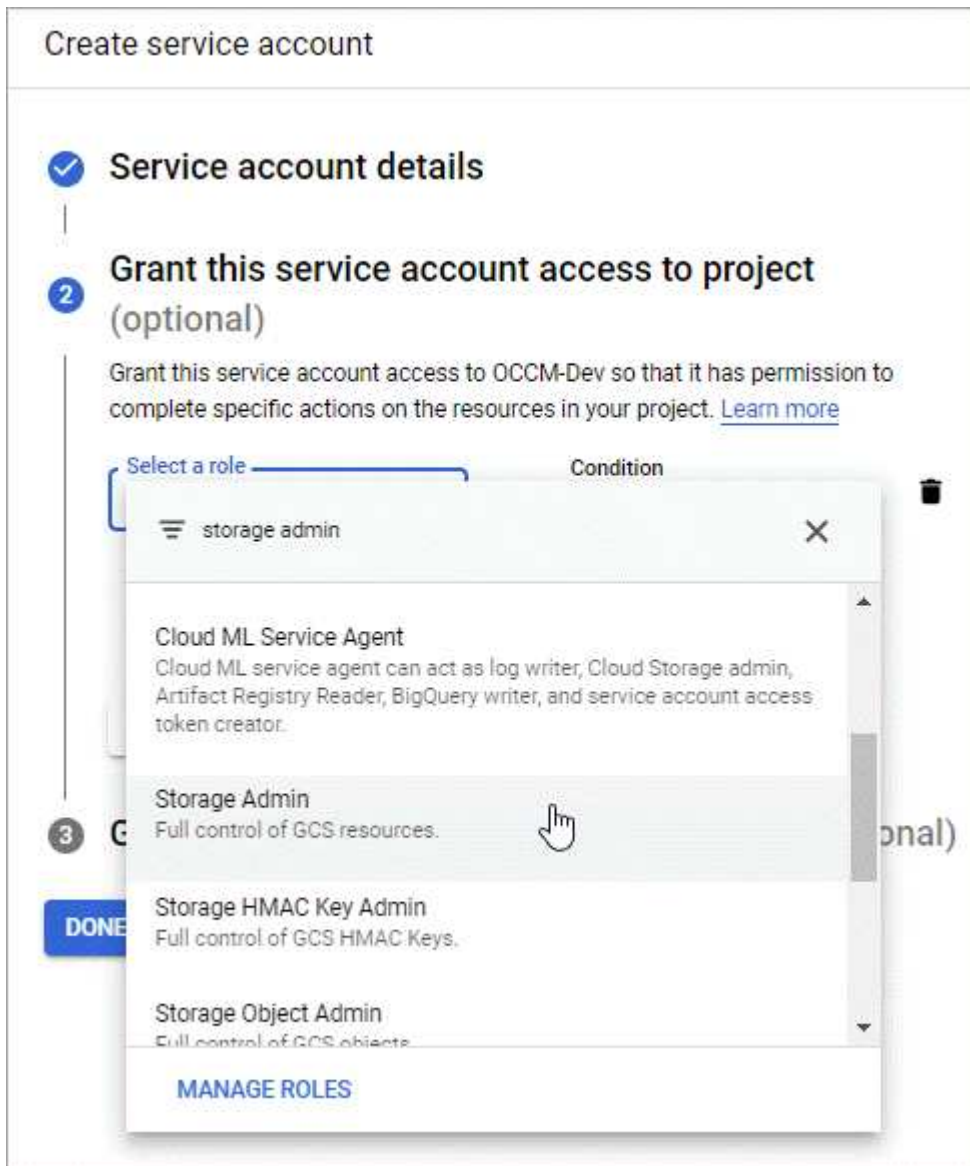
Cloud Volumes ONTAP 使用服务帐户访问和管理一个分层数据存储分段和另一个备份存储分段。

您可以设置一个服务帐户并将其用于这两种目的。服务帐户必须具有 **\* 存储管理员 \*** 角色。

### 步骤

1. 在 Google Cloud 控制台中，**"转到服务帐户页面"**。
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 \***：输入名称和问题描述。

- b. \* 授予此服务帐户对项目的访问权限 \*：选择 \* 存储管理员 \* 角色。



- c. \* 授予用户对此服务帐户的访问权限 \*：将 Connector 服务帐户作为 *Service Account User* 添加到此新服务帐户。

此步骤仅适用于数据分层。Cloud Backup Service 不需要此功能。

Create service account

✓ Service account details

✓ Grant this service account access to project (optional)

3 Grant users access to this service account (optional)  
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

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

Details and Credentials

default-project

Google Cloud Project

gcp-sub2

Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)

cloudvolumesontap

Service Account ⓘ

Service Account Name

account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

## 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. 确保 Cloud Manager Connector 服务帐户在存储密钥的项目中的项目级别具有正确的权限。

权限由提供 ["Cloud Manager YAML 文件"](#) 默认情况下，如果您使用云密钥管理服务的备用项目，则可能不会应用此功能。

权限如下：

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

2. 确保的服务帐户 ["Google 计算引擎服务代理"](#) 对密钥具有 Cloud KMS 加密器 / 解密器权限。

服务帐户的名称采用以下格式：`"service-[service_project_number]@compute-system.iam.gserviceaccount.com"`。

["Google Cloud 文档：将 IAM 与 Cloud KMS 结合使用—为资源授予角色"](#)

3. 通过调用 `GCP/vsa/metadata/gcp-encryption-keys` API 调用的 get 命令或在 GCP 控制台中的密钥上选择 "复制资源名称" 来获取密钥的 "id"。
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，则 Cloud Manager 会尝试使用用于加密永久性磁盘的相同密钥。但是，您首先需要启用 Google Cloud Storage 存储分段才能使用密钥：
  - a. 按照查找 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 加密器 / 解密器权限。有关详细信息，请参见 ["Google Cloud 文档：使用客户管理的加密密钥"](#)
5. 创建工作环境时，请在 API 请求中使用 "GcpEncryption" 参数。

◦ 示例 \*

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

请参见 ["Cloud Manager 自动化文档"](#) 有关使用 GcpEncryption 参数的详细信息，请参见。

## 在 GCP 中启动 Cloud Volumes ONTAP

您可以在单节点配置中启动 Cloud Volumes ONTAP，也可以在 Google 云平台中作为 HA 对启动。

### 开始之前

要创建工作环境，您需要满足以下要求。

- 已启动且正在运行的连接器。
  - 您应具有 ["与工作空间关联的连接器"](#)。
  - ["您应做好准备，使 Connector 始终保持运行"](#)。
  - 与 Connector 关联的服务帐户 ["应具有最新权限"](#)。
- 了解要使用的配置。

您应该已准备好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"](#)。

- 了解在添加工作环境向导中选择特定许可选项所需的条件。 ["了解有关 Cloud Volumes ONTAP 许可的更多信息"](#)。

| 许可选项             | 要求   | 如何满足要求  |
|------------------|--|---|
| 免费               | 需要提供 Marketplace 订阅或 NetApp 支持站点（NSS）帐户。   | 您可以从 * 详细信息和凭据 * 页面订阅云提供商的市场。您可以在 * 充电方法和 NSS 帐户 * 页面上输入 NSS 帐户。  |
| 专业或基本软件包         | 需要 Marketplace 订阅或基于容量的许可证（BYOL）。如果您的帐户没有有效的基于容量的许可证，或者您配置的容量超过许可容量，则建议使用 Marketplace 订阅进行基于容量的收费。 | 您可以从 * 详细信息和凭据 * 页面订阅云提供商的市场。如果要使用从 NetApp 购买的基于容量的许可证（BYOL），必须先将其添加到 * 数字电子钱包 * 中。 <a href="#">"了解如何添加基于容量的 BYOL 许可证"</a> 。  |
| Keystone Flex 订阅 | 您的帐户必须获得授权，并且必须启用订阅才能在 Cloud Volumes ONTAP 中使用。  | <p>a. mailto : <a href="mailto:ng-keystone-success@netapp.com">ng-keystone-success@netapp.com</a>（联系 NetApp）授权您的 Cloud Manager 用户帐户订阅一个或多个 Keystone Flex 订阅。</p> <p>b. 在 NetApp 授权您的帐户后，<a href="#">"链接您的订阅以用于 Cloud Volumes ONTAP"</a>。</p> <p>c. 创建 Cloud Volumes ONTAP HA 对时，请选择 Keystone Flex 订阅收费方法。</p> |
| 按节点许可            | 需要订阅 Marketplace，或者您需要自带许可证（BYOL）。具有现有订阅或现有许可证的客户可以使用此选项。它不适用于新客户。                                 | 如果要使用从 NetApp 购买的基于节点的许可证（BYOL），必须先将其添加到 * 数字电子钱包 * 中。 <a href="#">"了解如何添加基于节点的 BYOL 许可证"</a> 。您可以在 * 充电方法和 NSS 帐户 * 页面上输入 NSS 帐户。  |

- 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

## 在 GCP 中启动单节点系统


在 Cloud Manager 中创建一个工作环境，以便在 GCP 中启动 Cloud Volumes ONTAP。

### 步骤

1. **【订阅】** 在 "画布" 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. 如果出现提示，["创建连接器"](#)。
4. 详细信息和凭据：选择项目、指定集群名称、选择服务帐户、添加标签并指定凭据。



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。   |
| 服务帐户名称 | 如果您计划使用 "数据分层" 或 "云备份" 使用 Cloud Volumes ONTAP 时，您需要启用 * 服务帐户 * 并选择具有预定义的存储管理员角色的服务帐户。 <a href="#">"了解如何创建服务帐户"</a> 。   |
| 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 <a href="#">"Google Cloud 文档：标记资源"</a> 。   |
| 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 。保留默认的 <i>admin</i> 用户名或将其更改为自定义用户名。  |
| 编辑项目   | <p>选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是 Cloud Manager 所在的项目。</p> <p>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。</p> <div> 这是您为 Cloud Manager 设置的服务帐户， <a href="#">"如本页所述"</a>。</div> <p>单击 * 添加订阅 * 将选定凭据与订阅关联。</p> <p>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。</p> |

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：或者，也可以按照中的步骤进行订阅 ["将 Marketplace 订阅与 GCP 凭据关联"](#) 部分。

► [https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

5. \* 服务 \*：选择要在此系统上使用的服务。要选择 Cloud Backup 或使用分层，您必须已在步骤 3 中指定服务帐户。
6. 位置和连接：选择一个位置、选择防火墙策略并确认与 Google Cloud 存储的网络连接以进行数据分层。

下表介绍了可能需要指导的字段：

| 字段        | Description  |
|-----------|--|
| 连接验证      | 要将冷数据分层到Google云存储分段、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 <a href="#">"Google Cloud 文档：配置私有 Google Access"</a> 。   |
| 已生成防火墙策略  | 如果您让Cloud Manager为您生成防火墙策略、则需要选择允许流量的方式： <ul style="list-style-type: none"><li>• 如果选择*仅选定VPC*、则入站流量的源筛选器是选定VPC的子网范围以及Connector所在VPC的子网范围。这是建议的选项。</li><li>• 如果选择*所有VPC*、则入站流量的源筛选器为0.0.0.0/0 IP范围。</li></ul> |
| 使用现有防火墙策略 | 如果您使用现有防火墙策略、请确保该策略包含所需的规则。 <a href="#">"了解Cloud Volumes ONTAP 的防火墙规则"</a> 。   |

7. \* 充电方法和 NSS 帐户 \*：指定要在此系统中使用的充电选项，然后指定 NetApp 支持站点帐户。
  - ["了解这些充电方法"](#)。
  - ["在向导中了解要使用的许可方法的要求"](#)。
8. \* 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。

9. \* 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。

Licensing

Cloud Volumes ONTAP version to deploy: ONTAP-9.7RC1. [Change version](#)

  
Cloud Volumes ONTAP Explore

  
Cloud Volumes ONTAP Standard  
Improved Functionality

  
Cloud Volumes ONTAP Premium  
Advanced Functionality

Cloud Volumes ONTAP Standard Machine

Machine Type  
n1-standard-8

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。

10. \* 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"](#)。

11. \* 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 Cloud Backup 或启用了数据分层，则无法启用 WORM。

["了解有关 WORM 存储的更多信息。"](#)

12. \* 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（对于 Cloud Volumes ONTAP 9.7 或更高版本为必需），或者选择一个 GCP 帐户（对于 Cloud Volumes ONTAP 9.6 为必需帐户）。

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 Connector 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。"](#)

13. \* 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"](#)。

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。 |

| 字段                     | Description  |
|------------------------|--|
| 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， <a href="#">"使用 IQN 从主机连接到 LUN"</a> 。 |

下图显示了已填写 CIFS 协议的卷页面：

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

14. \* 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）。如果要配置 Google Managed 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。   |

| 字段                       | Description   |
|--------------------------|---|
| 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 。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* 。 <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google Cloud 文档： Google Managed Microsoft AD 中的组织单位"^] |
| 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 " <a href="#">Cloud Manager 自动化文档</a> " 了解详细信息。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。   |

15. \* 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](#)"。

16. \* 审核并批准 \*：审核并确认您的选择。

- 查看有关配置的详细信息。
- 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。
- 选中 \* 我了解 ... \* 复选框。
- 单击 \* 执行 \*。

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。

## 在 GCP 中启动 HA 对

在 Cloud Manager 中创建一个工作环境，以便在 GCP 中启动 Cloud Volumes ONTAP 。

## 步骤

1. 在 "画布" 页面上，单击 \* 添加工作环境 \* 并按照提示进行操作。
2. \* 选择位置 \*：选择 \* Google Cloud\* 和 \* Cloud Volumes ONTAP HA\*。
3. \* 详细信息和凭据 \*：选择项目，指定集群名称，选择服务帐户，添加标签并指定凭据。

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。   |
| 服务帐户名称 | 如果您计划使用 "分层" 或 "云备份" 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。   |
| 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 <a href="#">"Google Cloud 文档：标记资源"</a> 。   |
| 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。保留默认的 <i>admin</i> 用户名或将其更改为自定义用户名。   |
| 编辑项目   | <p>选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是 Cloud Manager 所在的项目。</p> <p>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。</p> <div> 这是您为 Cloud Manager 设置的服务帐户， <a href="#">"如本页所述"</a>。</div> <p>单击 * 添加订阅 * 将选定凭据与订阅关联。</p> <p>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。</p> |

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：或者，也可以按照中的步骤进行订阅 ["将 Marketplace 订阅与 GCP 凭据关联"](#) 部分。

► [https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/zh-cn/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)



(video)

4. \* 服务 \*：选择要在此系统上使用的服务。要选择 Cloud Backup 或使用分层，您必须已在步骤 3 中指定服务帐户。
5. \* 高可用性部署模式 \*：为高可用性配置选择多个分区（建议）或一个分区。然后选择一个区域和分区。

["了解有关 HA 部署模式的更多信息"](#)。

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

["详细了解网络要求"](#)。

7. \* 充电方法和 NSS 帐户 \*：指定要在此系统中使用的充电选项，然后指定 NetApp 支持站点帐户。

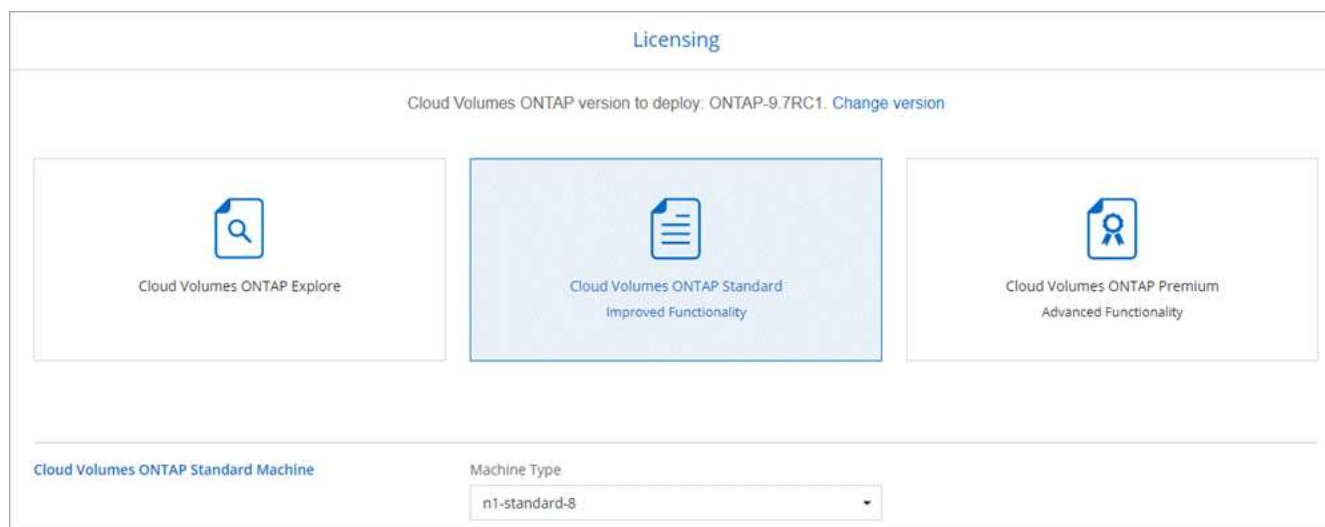
- ["了解这些充电方法"](#)。

- ["在向导中了解要使用的许可方法的要求"](#)。

8. \* 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。

9. \* 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 9.8 RC1 和 9.8 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 9.7 到 9.8。

10. \* 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"](#)。

11. \* WORM\*：根据需要激活一次写入，多次读取（WORM）存储。

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。"](#)

12. \* 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的存储管理员角色的服务帐户。

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 Connector 服务帐户，否则无法从 Cloud Manager 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。"](#)

13. \* 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"](#)。

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， <a href="#">"使用 IQN 从主机连接到 LUN"</a> 。 |



下图显示了已填写 CIFS 协议的卷页面：

Volume Details, Protection & Protocol

Details & Protection

Volume Name:

vol

Size (GB):

250

Snapshot Policy:

default

Default Policy

Protocol

NFS

CIFS

ISCSI

Share name:

vol\_share

Permissions:

Full Control

Users / Groups:

engineering

Valid users and groups separated by a semicolon

14. \* 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）。如果要配置 Google Managed 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。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*。<br>。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 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。如果需要其他地址配置 NTP 服务器，则应使用 API。请参见 <a href="#">"Cloud Manager 自动化文档"</a> 了解详细信息。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。  |

15. \* 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"](#)。

16. \* 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 \* 。

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。

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.