



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

NetApp
June 27, 2024

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
Google Cloud 中 Cloud Volumes ONTAP 的网络连接要求	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 Google Cloud 中为 Cloud Volumes ONTAP 设置许可	21
在 Google Cloud 中启动 Cloud Volumes ONTAP	26
Google Cloud Platform 映像验证	37

开始使用 Google Cloud

在 Google Cloud 中快速启动 Cloud Volumes ONTAP

只需几步即可开始使用适用于Google Cloud的Cloud Volumes ONTAP。

1

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 Google Cloud 中创建 Connector"](#)

请注意、如果要在无法访问Internet的子网中部署Cloud Volumes ONTAP、则需要手动安装此连接器并访问此连接器上运行的BlueXP用户界面。 ["了解如何在无法访问Internet的位置手动安装Connector"](#)

2

规划您的配置

BlueXP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"](#)。

3

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. 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NetApp AutoSupport 的目标VPC启用出站Internet访问。

如果您要在无法访问Internet的位置部署Cloud Volumes ONTAP、则无需执行此步骤。

["详细了解网络要求"](#)。

4

设置服务帐户

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 ["BlueXP备份和恢复"](#) 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"](#)。

5

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BlueXP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

- "[从BlueXP创建连接器](#)"
- "[在 Linux 主机上安装 Connector 软件](#)"
- "[BlueXP对Google Cloud权限的作用](#)"

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Cloud Volumes ONTAP 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](#)"
- "[了解如何设置许可](#)"

选择支持的区域

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BlueXP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、BlueXP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"](#)。

收集网络信息

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	

GCP信息	您的价值
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BlueXP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BlueXP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。

Google Cloud中Cloud Volumes ONTAP 的网络连接要求

设置Google Cloud网络、以便Cloud Volumes ONTAP 系统可以正常运行。

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

Cloud Volumes ONTAP 的要求

必须在Google Cloud中满足以下要求。

单节点系统的特定要求

如果要部署单节点系统、请确保您的网络满足以下要求。

一个VPC

单节点系统需要一个虚拟私有云(Virtual Private Cloud、VPC)。

专用 IP 地址

BlueXP会将3或4个专用IP地址分配给Google Cloud中的单节点系统。

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对的特定要求

如果要部署HA对、请确保您的网络满足以下要求。

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。在创建HA对时、BlueXP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。

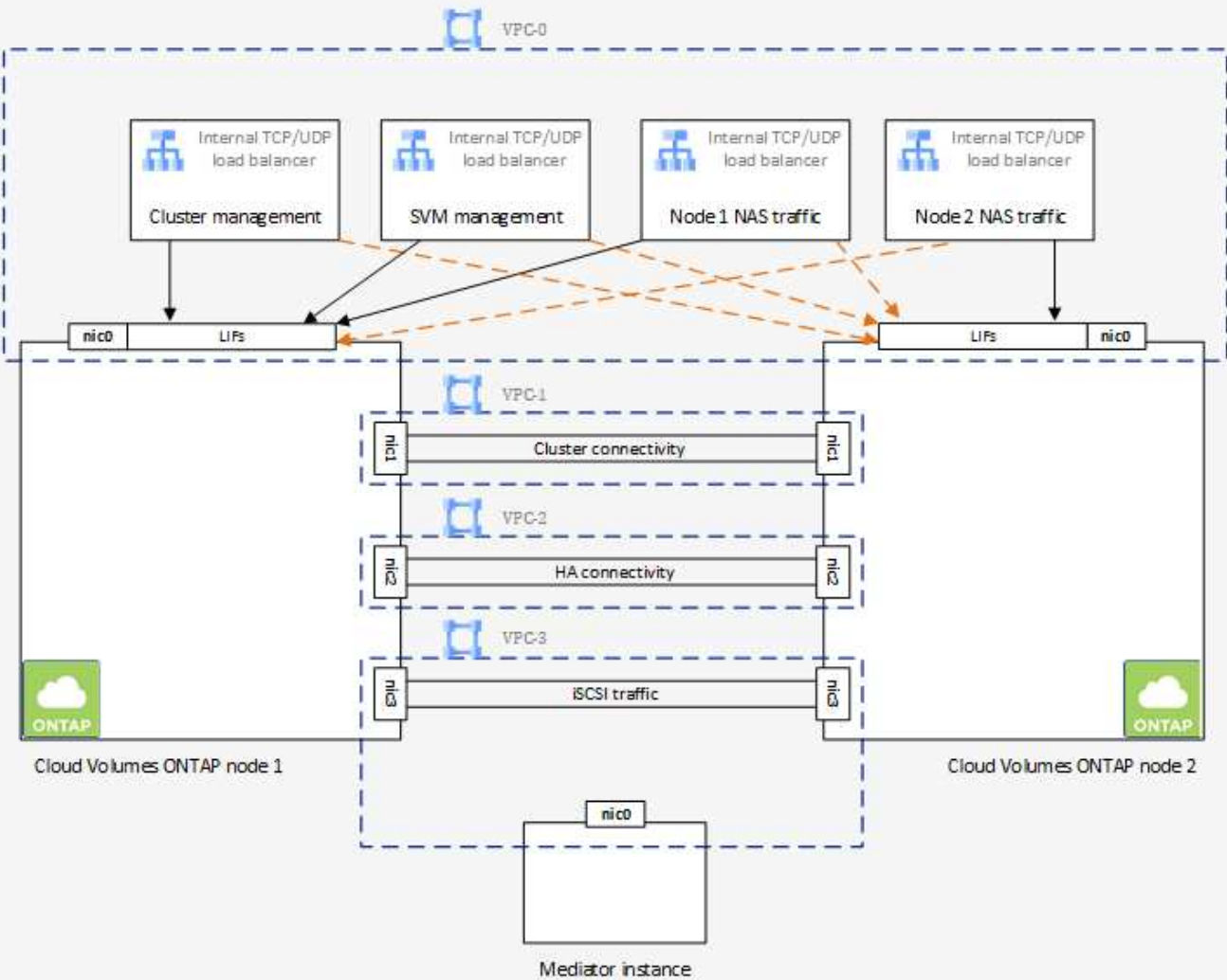
此部署模式确实可以降低成本，因为分区之间没有数据传出费用。

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Google Cloud要求每个网络接口都驻留在一个单独的VPC网络中。

在创建HA对时、BlueXP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



Subnets

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。

专用 IP 地址

BlueXP会自动将所需数量的专用IP地址分配给Google Cloud中的Cloud Volumes ONTAP。您需要确保网络具有足够的可用私有地址。

BlueXP为Cloud Volumes ONTAP 分配的LIF数量取决于您部署的是单节点系统还是HA对。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 。

- * 单节点 *

BlueXP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可通过iSCSI协议提供客户端访问、并由系统用于其他重要的网络工作流。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 Storage VM （SVM）管理 LIF：

```
skipSvmManagementLif: true
```

• * HA对*

BlueXP为HA对分配12-13个IP地址：

- 2个节点管理LIF (e0a)
- 1个集群管理LIF (e0a)
- 2个iSCSI LIF (e0a)



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

- 1个或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 Storage VM （SVM）管理 LIF：

```
skipSvmManagementLif: true
```

内部负载均衡器

BlueXP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。

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。

出站 Internet 访问

Cloud Volumes ONTAP 需要对 NetApp AutoSupport 进行出站 Internet 访问、NetApp 会主动监控系统的运行状况并向 NetApp 技术支持发送消息。

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>

如果无法通过出站 Internet 连接发送 AutoSupport 消息、则 BlueXP 会自动将您的 Cloud Volumes ONTAP 系统配置为使用 Connector 作为代理服务器。唯一的要求是确保 Connector 的防火墙允许通过端口 3128 进行 `_inbound_` 连接。部署 Connector 后、您需要打开此端口。

如果您为 Cloud Volumes ONTAP 定义了严格的出站规则、则还需要确保 Cloud Volumes ONTAP 防火墙允许通过端口 3128 进行 `_outout_` 连接。

确认出站 Internet 访问可用后，您可以测试 AutoSupport 以确保它可以发送消息。有关说明，请参见 "[ONTAP 文档：设置 AutoSupport](#)"。



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

如果BlueXP通知您无法发送AutoSupport 消息、"[对AutoSupport 配置进行故障排除](#)"。

防火墙规则

您无需创建防火墙规则、因为BlueXP可以为您创建防火墙规则。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](#)。

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BlueXP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Google Cloud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](#)"。

防火墙规则

BlueXP会创建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。

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。
- 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](#)。



正在查找有关连接器的信息？ "[查看Connector的防火墙规则](#)"

入站规则

在创建工作环境时、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地址连接Connector并通过HTTPS访问System Manager Web控制台
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	749-74	Kerberos
TCP	2049年	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	63001-630	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
UDP	635	NFS 挂载
UDP	2049年	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	4049-51	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	749-74	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	749-74	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
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)
	TCP	3128	节点管理 LIF	连接器	如果出站Internet连接不可用、则通过Connector上的代理服务器发送AutoSupport 消息
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)
配置备份	HTTP	80	节点管理 LIF	http : //occm/offboxconfig <connector-IP-address>	将配置备份发送到Connector。"了解配置备份文件"。
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

VPC-1、VPC-2和VPC-3的规则

在Google Cloud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、BlueXP为VPC-1、VPC-2和VPC-3中的实例创建的预定义防火墙规则可以通过_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。



要为新的Google Cloud HA对部署启用高写入速度、VPC-1、VPC-2和VPC-3需要至少8、896字节的最大传输单元(MTU)。如果选择将现有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使用这些VPC关闭所有现有HA系统。

连接器的要求

如果尚未创建Connector、则还应查看Connector的网络要求。

- ["查看连接器的网络要求"](#)
- ["Google Cloud中的防火墙规则"](#)

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BlueXP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BlueXP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

BlueXP可直接与Google Cloud API进行通信。这是从Google Cloud外部的的外部IP地址(例如、从api.services.cloud.netapp.com)触发的、或者从分配给BlueXP 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BlueXP都使用由NetApp管理的GCP中某个项目的映像。如果贵组织的策略阻止使用组织中未托管的映像、则这可能会影响BlueXP 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

- BlueXP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BlueXP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 **"BlueXP 备份和恢复"** 将卷备份到低成本对象存储。

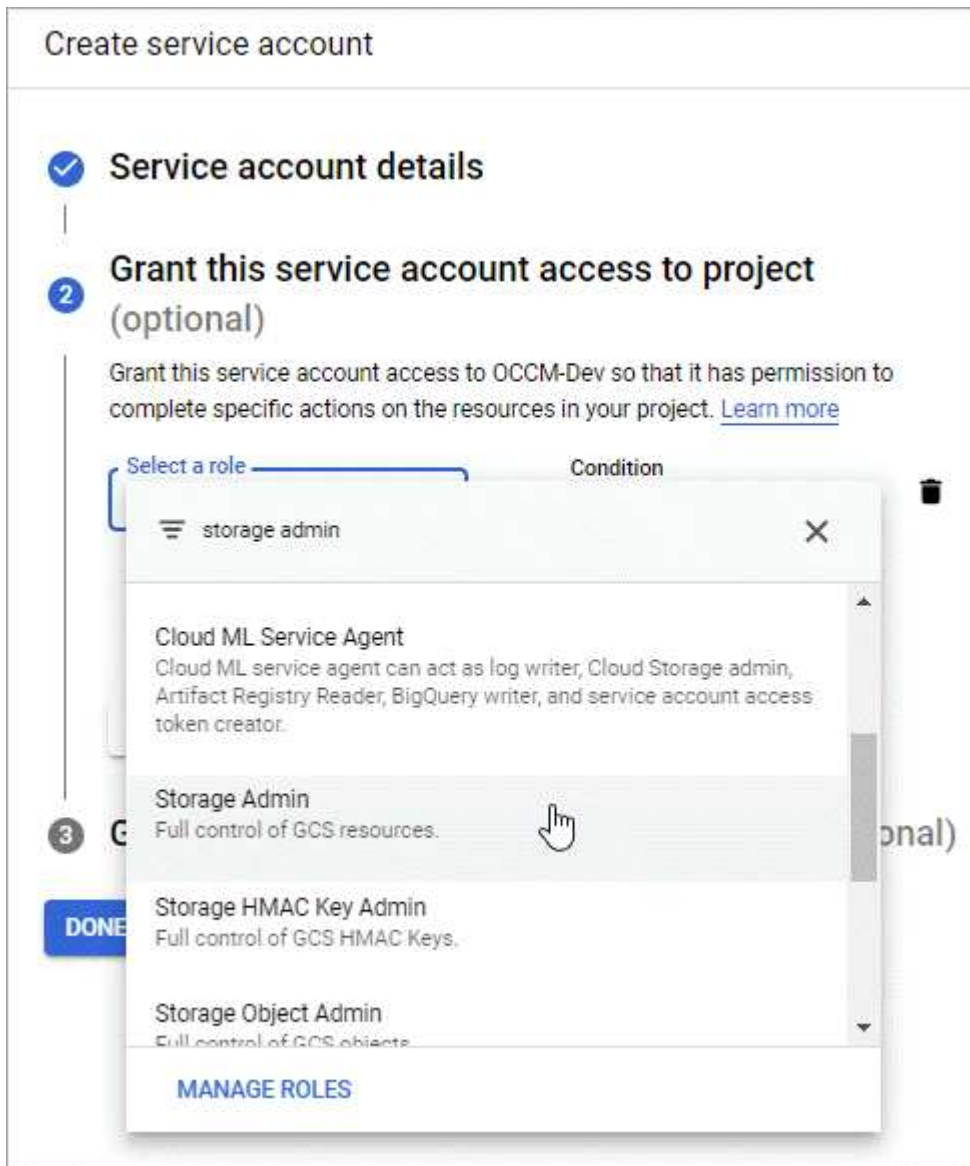
Cloud Volumes ONTAP 使用服务帐户访问和管理一个分层数据存储分段和另一个备份存储分段。

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。BlueXP备份和恢复不需要它。

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

下一步是什么？

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

<p>default-project Google Cloud Project</p>	<p>gcp-sub2 Marketplace Subscription</p>	<div style="border: 1px solid #0070c0; padding: 5px; display: inline-block;">Edit Project</div>
--	---	---

Details

Working Environment Name (Cluster Name)

Service Account

Service Account Name

+ Add Labels Optional Field | Up to four labels

Credentials

User Name

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BlueXP API创建一个使用 `_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. 确保在存储密钥的项目中、BlueXP Connector服务帐户在项目级别具有正确的权限。

权限在中提供 "[默认情况下、Connector服务帐户权限](#)"、但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.useToEncrypt
- 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. 通过调用的get命令获取密钥的"ID" /gcp/vsa/metadata/gcp-encryption-keys API调用、或者在GCP控制台中选择密钥上的"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、则BlueXP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 ["BlueXP自动化文档"](#) 有关使用 GcpEncryption 参数的详细信息，请参见。

在Google Cloud中为Cloud Volumes ONTAP 设置许可

在确定要在Cloud Volumes ONTAP 中使用的许可选项后、需要执行一些步骤、然后才能在创建新的工作环境时选择该许可选项。

免费

选择免费提供的Cloud Volumes ONTAP 、可在配置容量高达500 GiB的情况下免费使用。 ["了解有关免费提供的更多信息"](#)。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP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 中的按需购买服务。

除非您超过500 GiB的已配置容量、否则不会通过Marketplace订阅向您收取费用、此时系统将自动转换为 ["Essentials 软件包"](#)。

- b. 返回到BlueXP后、访问充电方法页面时选择*免费*。

Select Charging Method

<input type="radio"/>	Professional	By capacity	▼
<input type="radio"/>	Essential	By capacity	▼
<input checked="" type="radio"/>	Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/>	Per Node	By node	▼

["查看在Google Cloud中启动Cloud Volumes ONTAP 的分步说明"](#)。

基于容量的许可证

通过基于容量的许可，您可以按每 TiB 容量为 Cloud Volumes ONTAP 付费。基于容量的许可以 `_package_` 的形式提供：Essentials包或Professional包。

Essentials 和 Professional 软件包可用于以下消费模式：

- 从 NetApp 购买的许可证（BYOL）
- 从Google Cloud Marketplace订阅每小时按需购买(PAYGO)
- 年度合同

["了解有关基于容量的许可的更多信息"](#)。

以下各节介绍了如何开始使用上述每种消费模式。

BYOL

通过从NetApp购买许可证(BYOL)预付费用、以便在任何云提供商中部署Cloud Volumes ONTAP 系统。

步骤

1. ["要获取许可证，请联系 NetApp 销售人员"](#)
2. ["将您的NetApp 支持站点 帐户添加到BlueXP"](#)

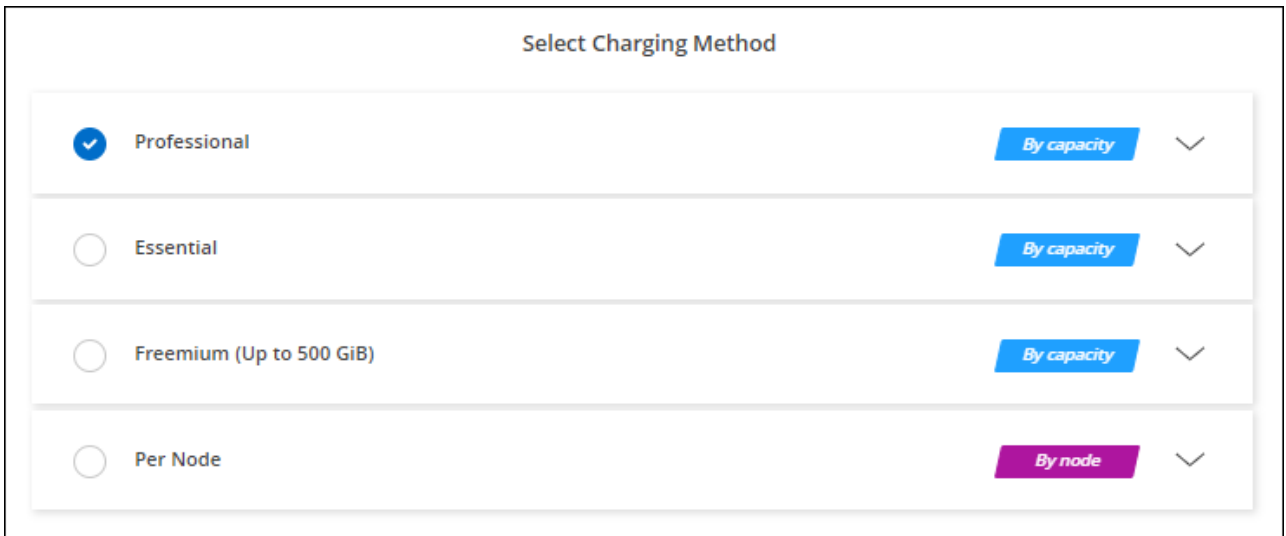
BlueXP会自动查询NetApp的许可服务、以获取与您的NetApp 支持站点 帐户关联的许可证的详细信息。如果没有错误、BlueXP会自动将许可证添加到电子钱包中。

您必须先从BlueXP电子钱包中获取许可证、然后才能在Cloud Volumes ONTAP 中使用它。如果需要，您可以 ["手动将许可证添加到BlueXP电子钱包"](#)。

3. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP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 中的按需购买服务。

您从NetApp购买的许可证始终会先收取费用、但如果超出许可容量或许可证期限到期、您将从市场上的每小时费率中扣除费用。

- b. 返回到BlueXP后、在访问充电方法页面时选择一个基于容量的软件包。



Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

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

PAYGO订阅

通过从云提供商的市场订阅优惠按小时付费。

创建Cloud Volumes ONTAP 工作环境时、BlueXP会提示您订阅Google云市场中提供的协议。然后、该订阅将与工作环境关联以进行收费。您可以对其他工作环境使用相同的订阅。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP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中的按需购买服务。
 - b. 返回到BlueXP后、在访问充电方法页面时选择一个基于容量的软件包。

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

["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Google Cloud凭据和订阅"](#)

年度合同

通过购买年度合同为Cloud Volumes ONTAP 支付年度费用。

步骤

1. 请联系您的NetApp销售代表以购买年度合同。

此合同在Google Cloud Marketplace中以_private_优惠的形式提供。

在NetApp与您共享私人优惠后、您可以在创建工作环境期间从Google Cloud Marketplace订阅年度计划。

2. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP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. 返回到BlueXP后、在访问充电方法页面时选择一个基于容量的软件包。

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity
<input type="radio"/> Essential	By capacity
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity
<input type="radio"/> Per Node	By node

["查看在Google Cloud中启动Cloud Volumes ONTAP 的分步说明"](#)。

Keystone订阅

Keystone订阅是一种基于订阅的按需购买服务。 ["了解有关NetApp Keystone 订阅的更多信息"](#)。

步骤

1. 如果您还没有订阅， ["请联系 NetApp"](#)
2. [mailto: ng-keystone-success@netapp.com](mailto:ng-keystone-success@netapp.com) [联系NetApp]以授权您的BlueXP用户帐户进行一项或多项Keystone订阅。
3. 在 NetApp 授权您的帐户后， ["链接您的订阅以用于 Cloud Volumes ONTAP"](#)。
4. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP中的步骤进行操作。
 - a. 当系统提示您选择充电方式时、选择Keystone订阅充电方式。

Select Charging Method

KeystoneBy capacity^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1▼

ProfessionalBy capacity▼

EssentialBy capacity▼

Freemium (Up to 500 GiB)By capacity▼

Per NodeBy node▼

["查看在Google Cloud中启动Cloud Volumes ONTAP 的分步说明"](#)。

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 ["应具有所需权限"](#)
- 了解要使用的配置。

您应已准备好选择配置并从管理员处获取Google Cloud网络信息。有关详细信息，请参见 ["规划 Cloud Volumes ONTAP 配置"](#)。

- 了解为Cloud Volumes ONTAP 设置许可所需的条件。

"了解如何设置许可"。

- 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Google Cloud中启动单节点系统

在BlueXP中创建工作环境、以便在Google Cloud中启动Cloud Volumes ONTAP。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 【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。
3. * 选择一个位置 *：选择 * Google Cloud* 和 * Cloud Volumes ONTAP *。
4. 如果出现提示，"创建连接器"。
5. 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	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Google Cloud 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 "BlueXP备份和恢复" 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。"了解如何创建服务帐户"。
添加标签	标签是指Google Cloud资源的元数据。BlueXP会将这些标签添加到与该系统关联的Cloud Volumes ONTAP 系统和Google云资源中。 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 。保留默认的 <i>admin</i> 用户名或将其更改为自定义用户名。

字段	Description
编辑项目	<p>选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是BlueXP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BlueXP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BlueXP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> <p> 这是您为BlueXP设置的服务帐户、"如本页所述"。</p> <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Google云市场中选择与Cloud Volumes ONTAP 订阅关联的Google云项目。</p>

以下视频介绍了如何将按需购买的Marketplace订阅与Google Cloud项目关联。或者，也可以按照中的步骤进行订阅 "将Marketplace订阅与Google Cloud凭据关联" 部分。

▶ https://docs.netapp.com/zh-cn/test//media/video_subscribing_gcp.mp4 (video)

6. * 服务 *：选择要在此系统上使用的服务。要选择BlueXP备份和恢复或使用BlueXP分层、您必须已在步骤3中指定服务帐户。



如果要使用WORM和数据分层、则必须禁用BlueXP备份和恢复、并部署9.8或更高版本的Cloud Volumes ONTAP 工作环境。

7. 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 " Google Cloud 文档：配置私有 Google Access "。
已生成防火墙策略	<p>如果您让BlueXP为您生成防火墙策略、则需要选择允许流量的方式：</p> <ul style="list-style-type: none"> • 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。 • 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。
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。链接： https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules [Learn关于Cloud Volumes ONTAP的防火墙规则^。

8. 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 Cloud Volumes ONTAP 的许可选项](#)"。

。"了解如何设置许可"。

9. * 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。

10. 许可：根据需要更改Cloud Volumes ONTAP 版本并选择计算机类型。



如果选定版本具有较新的候选版本、通用可用性或修补程序版本、则在创建工作环境时、BlueXP会将系统更新到该版本。例如、如果选择Cloud Volumes ONTAP 9.10.1和9.10.1 P4可用、则会发生更新。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。

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BlueXP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Google Cloud中估算系统规模](#)"。

12. **Flash Cache**、写入速度和**WORM**：

- a. 如果需要，启用*Flash Cache*。



从Cloud Volumes ONTAP 9.13.1开始、n2-standard-16、n2-standard-32、n2-standard-48和n2-standard-64实例类型均支持Flash Cache。部署后、您无法禁用Flash Cache。

- b. 如果需要、选择*正常*或*高*写入速度。

"了解有关写入速度的更多信息。"



通过*高速*写入速度选项、可以获得较高的写入速度和较高的最大传输单元(MTU)、即8、896字节。此外、较高的MTU 8、896要求在部署时选择VPC-1、VPC-2和VPC-3。有关VPC-1、VPC-2和VPC-3的详细信息、请参见 "[VPC-1、VPC-2和VPC-3的规则](#)"。

- c. 根据需要激活一次写入、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、将阻止还原或降级到Cloud Volumes ONTAP 9.8。

"了解有关 WORM 存储的更多信息。"

- a. 如果激活了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(对于Cloud Volumes ONTAP 9.7或更高版本为必需)、或者选择Google Cloud帐户(对于Cloud Volumes ONTAP 9.6为必需帐户)。

请注意以下事项：

- BlueXP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BlueXP中选择它
- 有关添加Google Cloud帐户的帮助、请参见 ["使用9.6设置和添加用于数据分层的Google Cloud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Google Cloud控制台添加服务帐户。

["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"](#)。

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、BlueXP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）	<p>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。</p> <p>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。</p> <p>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。</p> <p>创建iSCSI卷时、BlueXP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"。</p>

下图显示了已填写 CIFS 协议的卷页面：

Volume Details, Protection & Protocol

Details & Protection	Protocol
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS <input checked="" type="radio"/> CIFS <input type="radio"/> iSCSI </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

15. * 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	<p>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)。</p> <p>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 。</p>
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	<p>AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers 。</p> <p>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* 。</p> <p>"Google Cloud 文档: Google Managed Microsoft AD 中的组织单位"</p>
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	<p>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 "BlueXP 自动化文档" 了解详细信息。</p> <p>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。</p>

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, 并根据需要更改卷分层策略。

有关详细信息，请参见 ["选择卷使用情况配置文件"](#) 和 ["数据分层概述"](#)。

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. 单击*更多信息*可查看有关支持和BlueXP将购买的Google Cloud资源的详细信息。
 - c. 选中 * 我了解 ... * 复选框。
 - d. 单击 * 执行 *。

结果

BlueXP部署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Google Cloud中启动HA对


在BlueXP中创建工作环境、以便在Google Cloud中启动Cloud Volumes ONTAP。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 "画布" 页面上，单击 * 添加工作环境 * 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	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Google Cloud 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 "BlueXP层" 或 "BlueXP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	Description
添加标签	<p>标签是指Google Cloud资源的元数据。BlueXP会将这些标签添加到与该系统关联的Cloud Volumes ONTAP 系统和Google云资源中。</p> <p>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。</p> <p>有关标签的信息，请参见 "Google Cloud 文档：标记资源"。</p>
用户名和密码	<p>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。</p>
编辑项目	<p>选择要 Cloud Volumes ONTAP 驻留的项目。默认项目是BlueXP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BlueXP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BlueXP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> <p> 这是您为BlueXP设置的服务帐户、"如本页所述"。</p> <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Google云市场中选择与Cloud Volumes ONTAP 订阅关联的Google云项目。</p>

以下视频介绍了如何将按需购买的Marketplace订阅与Google Cloud项目关联。或者，也可以按照中的步骤进行订阅 "[将Marketplace订阅与Google Cloud凭据关联](#)" 部分。

► https://docs.netapp.com/zh-cn/test//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BlueXP备份和恢复或使用BlueXP分层、您必须已在步骤3中指定服务帐户。



如果要使用WORM和数据分层、则必须禁用BlueXP备份和恢复、并部署9.8或更高版本的Cloud Volumes ONTAP 工作环境。

6. * 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](#)"。

7. * 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](#)"。

下表介绍了可能需要指导的字段：

字段	Description
已生成策略	如果您让BlueXP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"> • 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。 • 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。
使用现有	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。 "了解Cloud Volumes ONTAP 的防火墙规则" 。

8. 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 Cloud Volumes ONTAP 的许可选项"](#)。
 - ["了解如何设置许可"](#)。
9. * 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。

10. 许可：根据需要更改Cloud Volumes ONTAP 版本并选择计算机类型。



如果选定版本具有较新的候选版本、通用可用性或修补程序版本、则在创建工作环境时、BlueXP会将系统更新到该版本。例如、如果选择Cloud Volumes ONTAP 9.10.1和9.10.1 P4可用、则会发生更新。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。

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BlueXP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Google Cloud中估算系统规模"](#)。

12. **Flash Cache**、写入速度和**WORM**：

- a. 如果需要，启用*Flash Cache*。



从Cloud Volumes ONTAP 9.13.1开始、n2-standard-16、n2-standard-32、n2-standard-48和n2-standard-64实例类型均支持Flash Cache。部署后、您无法禁用Flash Cache。

- b. 如果需要、选择*正常*或*高*写入速度。

["了解有关写入速度的更多信息。"](#)



通过*高*写入速度选项可获得高写入速度和8、896字节的最大传输单元(MTU)、实例类型为n2-standard-16、n2-standard-32、n2-standard-48和n2-standard-64。此外、较高的MTU 8、896要求在部署时选择VPC-1、VPC-2和VPC-3。高写入速度和8、896的MTU与功能相关、不能在已配置的实例中单独禁用。有关VPC-1、VPC-2和VPC-3的详细信息、请参见 "[VPC-1、VPC-2和VPC-3的规则](#)"。

c. 根据需要激活一次写入、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、将阻止还原或降级到Cloud Volumes ONTAP 9.8。

["了解有关 WORM 存储的更多信息。"](#)

a. 如果激活了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的存储管理员角色的服务帐户。

请注意以下事项:

- BlueXP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BlueXP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Google Cloud控制台添加服务帐户。

["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"](#)。

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、BlueXP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。

字段	Description
启动程序组和 IQN（仅适用于 iSCSI）	<p>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。</p> <p>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。</p> <p>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。</p> <p>创建 iSCSI 卷时，BlueXP 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"。</p>

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

15. * 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	<p>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）。</p> <p>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。</p>
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。

字段	Description
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* 。 "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 "BlueXP 自动化文档" 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。

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，并根据需要更改卷分层策略。

有关详细信息，请参见 ["选择卷使用情况配置文件"](#) 和 ["数据分层概述"](#)。

17. * 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*可查看有关支持和BlueXP将购买的Google Cloud资源的详细信息。
 - 选中 * 我了解 ... * 复选框。
 - 单击 * 执行 *。

结果

BlueXP部署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。

Google Cloud Platform映像验证

Google Cloud映像验证概述

Google Cloud映像验证符合增强的NetApp安全要求。我们对生成映像的脚本进行了更改，以便使用为此任务专门生成的私钥在整个过程中对映像进行签名。您可以使用Google Cloud的签名摘要和公共证书来验证GCP映像的完整性、此证书可通过下载 ["NSS"](#) 特定版本。



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

在Google Cloud上将图像转换为原始格式

用于部署新实例、升级或正在现有映像中使用的映像将通过与客户端共享 ["NetApp 支持站点 \(NSS\)"](#)。签名摘要和证书可通过NSS门户下载。确保您下载的是与NetApp支持共享的映像对应的正确版本的摘要和证书。例如，9.13.0映像将具有9.13.0签名的摘要和证书、可在NSS上使用。

为什么需要执行此步骤？

无法直接下载Google Cloud中的映像。要根据签名摘要和证书验证映像、您需要有一种机制来比较这两个文件并下载映像。要执行此操作、您必须将映像导出/转换为disk.raw格式、并将结果保存在Google Cloud的存储分段中。disk.raw文件会在该过程中进行tarred和gzipped。

用户/服务帐户需要具有执行以下操作的权限：

- 访问Google存储分段
- 写入Google Storage bucket
- 创建云构建作业(在导出过程中使用)
- 访问所需映像
- 创建导出映像任务

要验证映像、必须先将其转换为disk.raw格式、然后再下载。

使用Google Cloud命令行导出Google Cloud映像

将映像导出到云存储的首选方法是使用 ["gcloud compute images export命令"](#)。此命令将获取提供的映像、并将其转换为disk.raw文件、该文件会进行tarred和gzipped。生成的文件将保存在目标URL处、然后可下载以进行验证。

要执行此操作、用户/帐户必须具有访问和写入所需存储分段、导出映像以及云构建(供Google用于导出映像)的权限。

使用gcloud导出Google Cloud映像


```
$ 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/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[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
```

提取压缩文件

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



请参见 ["有关导出映像的Google Cloud文档"](#) 有关如何通过Google Cloud导出映像的详细信息。

映像签名验证

验证Google Cloud签名的映像

要验证导出的Google Cloud签名映像、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。

签名映像验证工作流程摘要

下面简要介绍了Google Cloud签名映像验证工作流程。

- 从 **"NSS"**下、下载包含以下文件的Google Cloud归档：
 - 签名摘要(.sig)
 - 包含公共密钥的证书(.pem)
 - 证书链(.pem)

Cloud Volumes ONTAP 9.13.0

Date Posted:

Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

Cloud Volumes ONTAP
Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130_V_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP
Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130_V_NODAR_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

Cloud Volumes ONTAP
Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0_PKG.TAR.GZ \[7.52 KB\]](#)

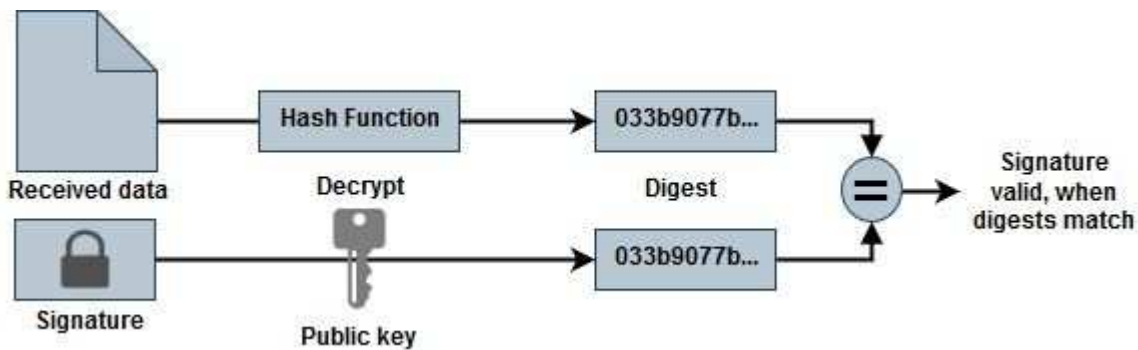
[View and download checksums](#)

Azure Image Digest File

[DOWNLOAD AZURE-9.13.0_PKG.TAR.GZ \[7.55 KB\]](#)

[View and download checksums](#)

- 下载转换后的disk.raw文件
- 使用证书链验证证书
- 使用包含公共密钥的证书验证签名摘要
 - 使用公共密钥对签名摘要进行解密、以提取映像文件的摘要
 - 创建已下载disk.raw文件的摘要
 - 比较两个摘要文件以进行验证



使用OpenSSL验证disk.raw文件和摘要文件内容

您可以根据通过提供的摘要文件内容验证Google Cloud下载的disk.raw文件 "NSS" 使用OpenSSL。



用于验证映像的OpenSSL命令与Linux、Mac OS和Windows计算机兼容。

步骤

1. 使用OpenSSL验证证书。

单击以显示脚本

```
# 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-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.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-20230119-0XXXXXX.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-20230119-0XXXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXXX.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-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.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 ${oscp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocspl -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: CE894F8251AA15A28462CA312361D261F8FE78

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、签名和证书置于目录中。
3. 使用OpenSSL从证书中提取公共密钥。
4. 使用提取的公共密钥对签名进行解密、并验证下载的disk.raw文件的内容。

单击以显示脚本

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