



# 入门 Cloud Volumes ONTAP

NetApp  
June 27, 2024

# 目录

入门 .....	1
了解 Cloud Volumes ONTAP .....	1
新部署支持的版本 .....	2
开始使用 Amazon Web Services .....	4
开始使用 Microsoft Azure .....	67
开始使用 Google Cloud .....	101

# 入门

## 了解 Cloud Volumes ONTAP

借助 Cloud Volumes ONTAP，您可以优化云存储成本和性能，同时增强数据保护，安全性和合规性。

Cloud Volumes ONTAP 是一款纯软件存储设备，可在云中运行 ONTAP 数据管理软件。它提供具有以下主要功能的企业级存储、供下次测试时使用：

- 存储效率

利用内置的重复数据删除，数据压缩，精简配置和克隆功能最大限度地降低存储成本。

- 高可用性

在云环境发生故障时，确保企业级可靠性和持续运行。

- 数据保护

Cloud Volumes ONTAP 利用 NetApp 行业领先的复制技术 SnapMirror 将内部数据复制到云，以便可以轻松地为多种使用情形提供二级副本。

Cloud Volumes ONTAP 还可与 BlueXP 备份和恢复相集成、提供备份和恢复功能、用于保护和长期归档云数据。

["了解有关 BlueXP 备份和恢复的更多信息"](#)

- 数据分层

按需在高性能和低性能存储池之间切换，而无需使应用程序脱机。

- 应用程序一致性

使用 NetApp SnapCenter 确保 NetApp Snapshot 副本的一致性。

["了解有关 SnapCenter 的更多信息"](#)

- 数据安全性

Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。

- 隐私合规性控制

与 BlueXP 分类的集成有助于您了解数据上下文并识别敏感数据。

["了解有关 BlueXP 分类的更多信息"](#)



Cloud Volumes ONTAP 中包含 ONTAP 功能的许可证。

["查看支持的 Cloud Volumes ONTAP 配置"](#)

["了解有关 Cloud Volumes ONTAP 的更多信息"](#)

## 新部署支持的版本

通过BlueXP、您可以在创建新的ONTAP 工作环境时从多个不同的Cloud Volumes ONTAP 版本中进行选择。

新部署不支持所有其他Cloud Volumes ONTAP 版本。

### **AWS**

#### 单个节点

- 9.13.1 GA
- 9.12.1大会
- 9.12.1 RC1.
- 9.12.0 P1
- 9.11.1 P3.
- 9.10.1.
- 9.9.1 P6.
- 9.8.
- 9.7 P5
- 9.5 P6.

#### **HA对**

- 9.13.1 GA
- 9.12.1大会
- 9.12.1 RC1.
- 9.12.0 P1
- 9.11.1 P3.
- 9.10.1.
- 9.9.1 P6.
- 9.8.
- 9.7 P5
- 9.5 P6.

### **Azure 酒店**

#### 单个节点

- 9.13.1 GA
- 9.12.1大会

- 9.12.1 RC1.
- 9.11.1 P3.
- 9.10.1 P3.
- 9.9.1 P8.
- 9.9.1 P7.
- 9.8 P10.
- 9.7 P6.
- 9.5 P6.

#### HA对

- 9.13.1 GA
- 9.12.1大会
- 9.12.1 RC1.
- 9.11.1 P3.
- 9.10.1 P3.
- 9.9.1 P8.
- 9.9.1 P7.
- 9.8 P10.
- 9.7 P6.

## Google Cloud

#### 单个节点

- 9.13.1 GA
- 9.12.1大会
- 9.12.1 RC1.
- 9.12.0 P1
- 9.11.1 P3.
- 9.10.1.
- 9.9.1 P6.
- 9.8.
- 9.7 P5

#### HA对

- 9.13.1 GA
- 9.12.1大会
- 9.12.1 RC1.
- 9.12.0 P1
- 9.11.1 P3.
- 9.10.1.

- 9.9.1 P6.
- 9.8.

# 开始使用 Amazon Web Services

## 在 AWS 中快速启动 Cloud Volumes ONTAP

在 AWS 中开始使用 Cloud Volumes ONTAP ， 只需几个步骤即可。

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AWS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、则了解可用的选项。 ["了解更多信息。"](#)

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. 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。

3. 将 VPC 端点设置为 S3 服务。

如果要将冷数据从 Cloud Volumes ONTAP 分层到低成本对象存储，则需要 VPC 端点。

["详细了解网络要求"](#)。

4

### 设置 AWS KMS

如果要对 Cloud Volumes ONTAP 使用 Amazon 加密，则需要确保存在有效的客户主密钥（CMK）。此外，您还需要通过添加 IAM 角色来修改每个 CMK 的密钥策略，该角色以 *key user* 的身份为 Connector 提供权限。 ["了解更多信息。"](#)

5

### 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"](#)
- ["从 AWS Marketplace 启动 Connector"](#)
- ["在 Linux 主机上安装 Connector 软件"](#)
- ["BlueXP对AWS权限的作用"](#)

## 在AWS中规划Cloud Volumes ONTAP 配置

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

必须先启用较新的 AWS 区域，然后才能在这些区域中创建和管理资源。 ["了解如何启用区域"](#)。

### 选择受支持的实例

Cloud Volumes ONTAP 支持多种实例类型，具体取决于您选择的许可证类型。

### ["AWS 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。

### ["AWS 中 Cloud Volumes ONTAP 的存储限制"](#)

### 在AWS中调整系统大小

对 Cloud Volumes ONTAP 系统进行规模估算有助于满足性能和容量要求。在选择实例类型，磁盘类型和磁盘大小时，应注意以下要点：

#### Instance type

- 将工作负载要求与每个 EC2 实例类型的最大吞吐量和 IOPS 相匹配。
- 如果多个用户同时向系统写入数据，请选择一种具有足够 CPU 来管理请求的实例类型。
- 如果您的应用程序大部分是读取的，请选择具有足够 RAM 的系统。
  - ["AWS 文档： Amazon EC2 实例类型"](#)
  - ["AWS 文档： Amazon EBS 优化实例"](#)

## EBS 磁盘类型

在较高级别上、EBS 磁盘类型之间的区别如下所示：要了解有关 EBS 磁盘使用情形的更多信息，请参见 ["AWS 文档：EBS 卷类型"](#)。

- 通用 SSD（GP3）\_ 磁盘是成本最低的 SSD，用于平衡各种工作负载的成本和性能。性能是按 IOPS 和吞吐量定义的。Cloud Volumes ONTAP 9.7 及更高版本支持 GP3 磁盘。

选择GP3磁盘时、BlueXP会填充默认IOPS和吞吐量值、这些值可根据选定磁盘大小提供与GP2磁盘等效的性能。您可以通过增加这些值来以更高的成本获得更高的性能，但我们不支持使用较低的值，因为它可能会导致性能下降。简而言之，请坚持使用默认值或增加默认值。请勿降低。"[详细了解 GP3 磁盘及其性能](#)"。

请注意、Cloud Volumes ONTAP 支持使用GP3磁盘的Amazon EBS弹性卷功能。"[了解有关Elastic Volumes支持的更多信息](#)"。

- 通用 SSD（GP2）\_ 磁盘可平衡各种工作负载的成本和性能。性能是根据 IOPS 来定义的。
- \_Provisioned IOPS SSD（IO1）\_ 磁盘适用于需要以较高成本获得最高性能的关键应用程序。

请注意、Cloud Volumes ONTAP 支持使用IO1磁盘的Amazon EBS弹性卷功能。"[了解有关Elastic Volumes支持的更多信息](#)"。

- \_Throughput Optimized HDD（st1）\_ 磁盘适用于需要以更低价格实现快速一致吞吐量的频繁访问的工作负载。



使用吞吐量优化型 HDD（st1）时，不建议将数据分层到对象存储。

## EBS 磁盘大小

如果您选择的配置不支持 ["Amazon EBS弹性卷功能"](#)、然后、您需要在启动Cloud Volumes ONTAP 系统时选择初始磁盘大小。之后，您可以 ["让BlueXP为您管理系统的容量"](#)，但如果需要 ["自行创建聚合"](#)，请注意以下事项：

- 聚合中的所有磁盘大小必须相同。
- EBS 磁盘的性能取决于磁盘大小。该大小决定了 SSD 磁盘的基准 IOPS 和最大突发持续时间以及 HDD 磁盘的基准和突发吞吐量。
- 最后，您应选择磁盘大小，以获得所需的 \_stimed\_perform 性能。
- 即使您选择了更大的磁盘（例如六个 4 TiB 磁盘）、但由于 EC2 实例可以达到其带宽限制，因此您可能无法获得全部 IOPS。

有关 EBS 磁盘性能的详细信息，请参见 ["AWS 文档：EBS 卷类型"](#)。

如上所述、支持Amazon EBS弹性卷功能的Cloud Volumes ONTAP 配置不支持选择磁盘大小。"[了解有关Elastic Volumes支持的更多信息](#)"。

## 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。



"查看 AWS 中 Cloud Volumes ONTAP 系统数据的默认磁盘"。



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"。

## 准备在AWS前台部署Cloud Volumes ONTAP

如果您有 AWS 前台，则可以通过在 "工作环境 " 向导中选择前台 VPC 来在该前台部署 Cloud Volumes ONTAP 。体验与 AWS 中的任何其他 VPC 相同。请注意，您需要先在 AWS 前台部署 Connector 。

需要指出的限制如下：

- 目前仅支持单节点 Cloud Volumes ONTAP 系统
- 您可以与 Cloud Volumes ONTAP 结合使用的 EC2 实例仅限于前台可用的实例
- 目前仅支持通用 SSD （ GP2 ）

## 收集网络信息

在 AWS 中启动 Cloud Volumes ONTAP 时，需要指定有关 VPC 网络的详细信息。您可以使用工作表从管理员收集信息。

单个AZ中的单节点或HA对

AWS 信息	您的价值
Region	
VPC	
Subnet	
安全组（如果使用您自己的）	

HA对位于多个AZs中

AWS 信息	您的价值
Region	
VPC	
安全组（如果使用您自己的）	
节点 1 可用性区域	
节点 1 子网	
节点2可用性区域	
节点2子网	
调解器可用性区域	
调解器子网	
调解器的密钥对	

AWS 信息	您的价值
用于集群管理端口的浮动 IP 地址	
节点 1 上数据的浮动 IP 地址	
节点2上数据的浮动IP地址	
浮动 IP 地址的路由表	

## 选择写入速度

通过BlueXP、您可以为Cloud Volumes ONTAP 选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和[建议](#)。"[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。

## 设置网络

### AWS 中的 Cloud Volumes ONTAP 的网络要求

BlueXP负责为Cloud Volumes ONTAP 设置网络组件、例如IP地址、网络掩码和路由。您需要确保出站 Internet 访问可用，有足够的专用 IP 地址可用，正确的连接到位等。

#### 一般要求

以下要求必须在 AWS 中满足。

#### Cloud Volumes ONTAP 节点的出站 Internet 访问

Cloud Volumes ONTAP 节点需要通过出站Internet访问NetApp AutoSupport、NetApp会主动监控系统运行状况并向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>

如果您有 NAT 实例、则必须定义允许 HTTPS 流量从私有子网传输到 Internet 的入站安全组规则。

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的安全组允许通过端口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 安全组允许通过端口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BlueXP通知您无法发送AutoSupport 消息、"[对AutoSupport 配置进行故障排除](#)"。

## HA 调解器的出站 Internet 访问

HA 调解器实例必须具有与 AWS EC2 服务的出站连接、以便能够帮助进行存储故障转移。要提供连接、可以添加公共 IP 地址、指定代理服务器或使用手动选项。

手动选项可以是 NAT 网关或从目标子网到 AWS EC2 服务的接口 VPC 端点。有关 VPC 端点的详细信息，请参见 "[AWS 文档：接口 VPC 端点（AWS PrivateLink）](#)"。

## 专用 IP 地址

BlueXP会自动为Cloud Volumes ONTAP 分配所需数量的专用IP地址。您需要确保网络具有足够的可用专用 IP 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。

## 单节点系统的 IP 地址

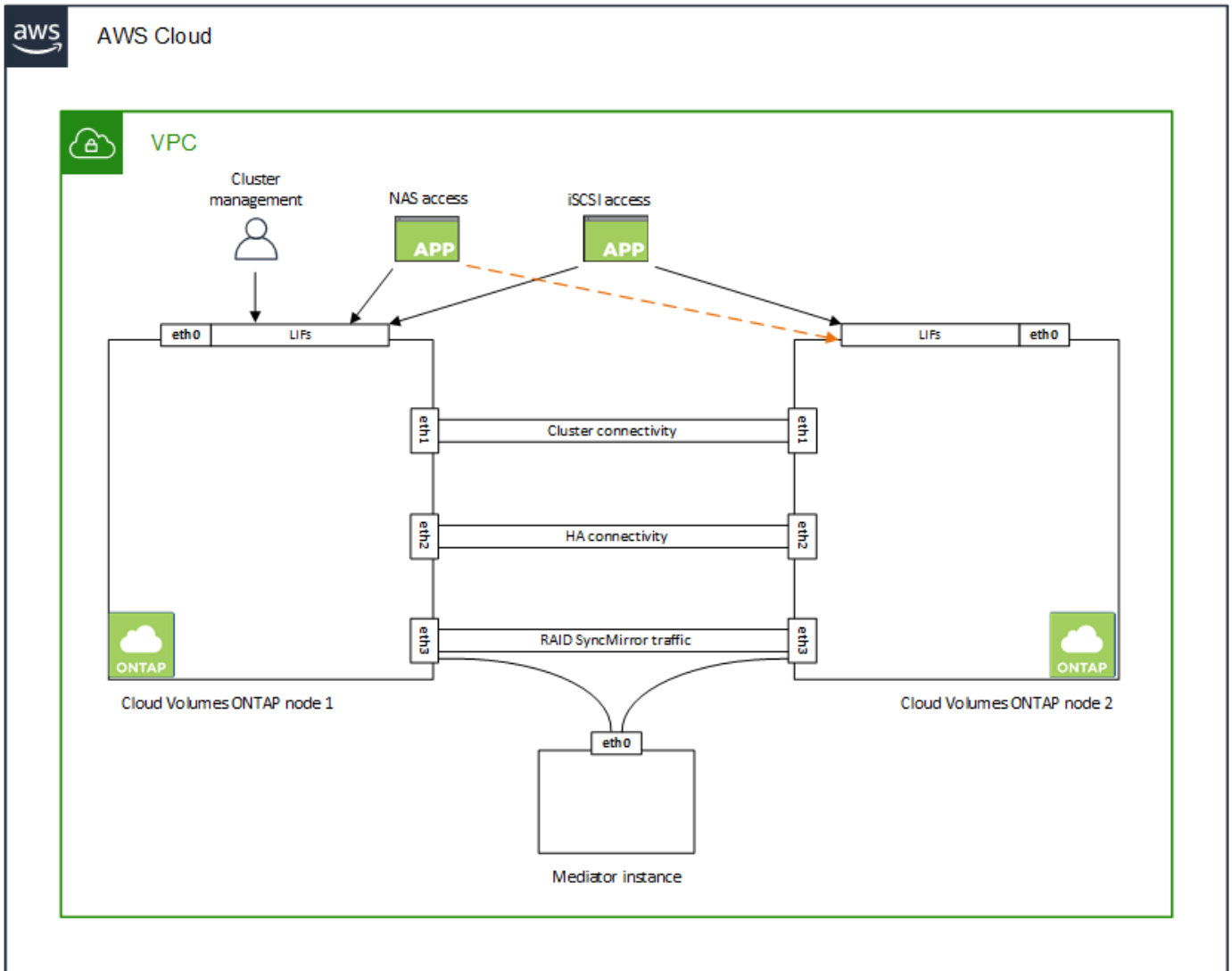
BlueXP会将6个IP地址分配给一个节点系统。

下表提供了有关与每个专用IP地址关联的LIF的详细信息。

LIF	目的
集群管理	对整个集群（HA 对）进行管理管理。
节点管理	节点的管理管理。
集群间	跨集群通信，备份和复制。
NAS 数据	通过 NAS 协议进行客户端访问。
iSCSI 数据	通过 iSCSI 协议进行客户端访问。系统也会将其用于其他重要的网络 workflow。此LIF为必填项、不应删除。
Storage VM管理	Storage VM 管理 LIF 与 SnapCenter 等管理工具结合使用。

## HA 对的 IP 地址

与单节点系统相比，HA 对所需的 IP 地址更多。这些 IP 地址分布在不同的以太网接口上，如下图所示：



HA 对所需的专用 IP 地址数量取决于您选择的部署模式。部署在 `_single` AWS 可用性区域（AZ）中的 HA 对需要 15 个专用 IP 地址，而部署在 `_Multiple _AZs` 中的 HA 对则需要 13 个专用 IP 地址。

下表提供了有关与每个专用 IP 地址关联的 LIF 的详细信息。

### 一个 AZ 中的 HA 对的 LIF

LIF	接口	Node	目的
集群管理	eth0	节点 1	对整个集群（HA 对）进行管理管理。
节点管理	eth0	节点 1 和节点 2	节点的管理管理。
集群间	eth0	节点 1 和节点 2	跨集群通信，备份和复制。
NAS 数据	eth0	节点 1	通过 NAS 协议进行客户端访问。

LIF	接口	Node	目的
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。系统也会将其用于其他重要的网络工作流。这些LIF是必需的、不应删除。
集群连接	Eth1	节点 1 和节点 2	使节点可以彼此通信并在集群中移动数据。
HA 连接	Eth2	节点 1 和节点 2	发生故障转移时两个节点之间的通信。
RSM iSCSI 流量	Eth3.	节点 1 和节点 2	RAID SyncMirror iSCSI 流量以及两个 Cloud Volumes ONTAP 节点与调解器之间的通信。
调解器	eth0	调解器	节点与调解器之间的通信通道，用于协助存储接管和交还过程。

### 多个 AZs 中 HA 对的 LIF

LIF	接口	Node	目的
节点管理	eth0	节点 1 和节点 2	节点的管理管理。
集群间	eth0	节点 1 和节点 2	跨集群通信，备份和复制。
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。这些LIF还可管理节点之间浮动IP地址的迁移。这些LIF是必需的、不应删除。
集群连接	Eth1	节点 1 和节点 2	使节点可以彼此通信并在集群中移动数据。
HA 连接	Eth2	节点 1 和节点 2	发生故障转移时两个节点之间的通信。
RSM iSCSI 流量	Eth3.	节点 1 和节点 2	RAID SyncMirror iSCSI 流量以及两个 Cloud Volumes ONTAP 节点与调解器之间的通信。
调解器	eth0	调解器	节点与调解器之间的通信通道，用于协助存储接管和交还过程。



如果部署在多个可用性区域中，则会与多个 LIF 关联 **"浮动 IP 地址"**，不计入 AWS 专用 IP 限制。

### 安全组

您无需创建安全组、因为BlueXP可以为您创建安全组。如果您需要使用自己的，请参见 **"安全组规则"**。



正在查找有关连接器的信息？ ["查看Connector的安全组规则"](#)

### 数据分层连接

如果要将 EBS 用作性能层、将 AWS S3 用作容量层、则必须确保 Cloud Volumes ONTAP 与 S3 建立连接。提供该连接的最佳方法是创建到 S3 服务的 VPC 端点。有关说明，请参见 **"AWS 文档：创建网关端点"**。

创建 VPC 端点时，请确保选择与 Cloud Volumes ONTAP 实例对应的区域、VPC 和路由表。您还必须修改安全组才能添加出站 HTTPS 规则、该规则允许通信到 S3 端点。否则，Cloud Volumes ONTAP 无法连接到 S3

服务。

如果遇到任何问题，请参见 ["AWS 支持知识中心：为什么我无法使用网关 VPC 端点连接到 S3 存储分段？"](#)

## 连接到 ONTAP 系统

要在 AWS 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 AWS VPC 与其他网络（例如企业网络）之间建立 VPN 连接。有关说明，请参见 ["AWS 文档：设置 AWS VPN 连接"](#)。

## 用于 CIFS 的 DNS 和 Active Directory

如果要配置 CIFS 存储，必须在 AWS 中设置 DNS 和 Active Directory 或将内部设置扩展到 AWS。

DNS 服务器必须为 Active Directory 环境提供名称解析服务。您可以将 DHCP 选项集配置为使用默认的 EC2 DNS 服务器，该服务器不能是 Active Directory 环境使用的 DNS 服务器。

有关说明，请参见 ["AWS 文档：AWS 云上的 Active Directory 域服务：快速入门参考部署"](#)。

## VPC 共享

从 9.11.1 版开始，具有 VPC 共享的 AWS 支持 Cloud Volumes ONTAP HA 对。通过 VPC 共享，您的组织可以与其他 AWS 帐户共享子网。要使用此配置，您必须设置 AWS 环境，然后使用 API 部署 HA 对。

["了解如何在共享子网中部署 HA 对"](#)。

## 多个 AZs 中 HA 对的要求

其他 AWS 网络要求适用于使用多可用性区域（AZs）的 Cloud Volumes ONTAP HA 配置。在启动 HA 对之前，您应查看这些要求，因为在创建工作环境时，您必须在 BlueXP 中输入网络详细信息。

要了解 HA 对的工作原理，请参见 ["高可用性对"](#)。

## 可用性区域

此 HA 部署模型使用多个 AZ 来确保数据的高可用性。您应该为每个 Cloud Volumes ONTAP 实例和调解器实例使用专用的 AZ，该实例在 HA 对之间提供通信通道。

每个可用性区域都应有一个子网。

## 用于 NAS 数据和集群 /SVM 管理的浮动 IP 地址

多个 AZs 中的 HA 配置使用浮动 IP 地址，如果发生故障，这些地址会在节点之间迁移。除非您自己，否则它们不能从 VPC 外部本机访问 ["设置 AWS 传输网关"](#)。

一个浮动 IP 地址用于集群管理、一个用于节点 1 上的 NFS/CIFS 数据、一个用于节点 2 上的 NFS/CIFS 数据。SVM 管理的第四个浮动 IP 地址是可选的。



如果将 SnapDrive for Windows 或 SnapCenter 与 HA 对结合使用，则 SVM 管理 LIF 需要浮动 IP 地址。

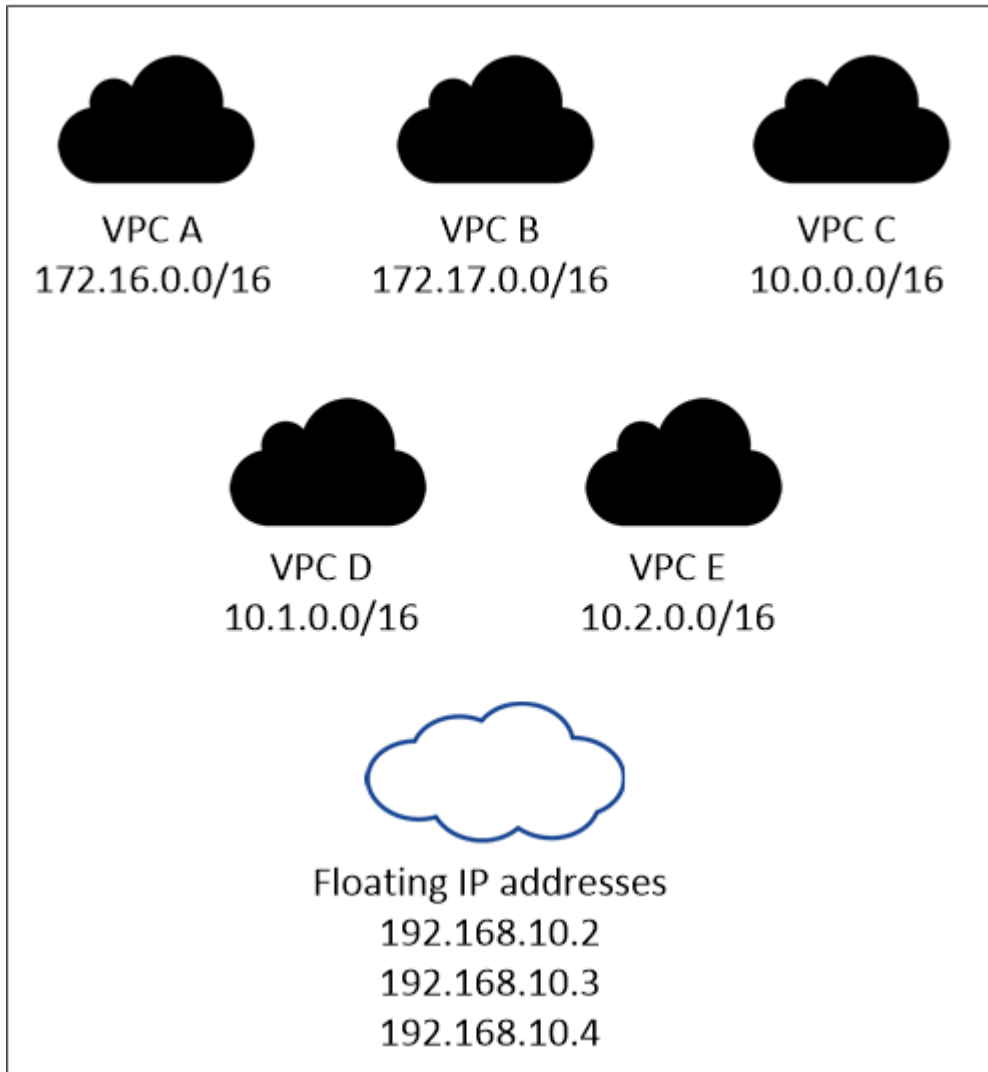
创建 Cloud Volumes ONTAP HA 工作环境时，您需要在 BlueXP 中输入浮动 IP 地址。BlueXP 在启动系统时会分配 IP 地址给 HA 对。

对于部署 HA 配置的 AWS 区域中的所有 vPC，浮动 IP 地址必须不在 CIDR 块的范围内。将浮动 IP 地址视

为您所在地区 VPC 之外的逻辑子网。

以下示例显示了 AWS 区域中浮动 IP 地址与 VPC 之间的关系。虽然浮动 IP 地址不在所有 VPC 的 CIDR 块之外，但它们可以通过路由表路由到子网。

## AWS region



BlueXP会自动创建静态IP地址、用于从VPC外部的客户端进行iSCSI访问和NAS访问。您无需满足这些类型的 IP 地址的任何要求。

传输网关，用于从 **VPC** 外部启用浮动 IP 访问

如果需要，"[设置 AWS 传输网关](#)" 允许从 HA 对所在的 VPC 外部访问 HA 对的浮动 IP 地址。

### 路由表

在BlueXP中指定浮动IP地址后、系统将提示您选择应包含浮动IP地址路由的路由表。这将启用客户端对 HA 对的访问。

如果VPC中的子网只有一个路由表(主路由表)、则BlueXP会自动将浮动IP地址添加到该路由表中。如果您有多个路由表，则在启动 HA 对时选择正确的路由表非常重要。否则，某些客户端可能无法访问 Cloud Volumes ONTAP。

例如，您可能有两个子网与不同的路由表相关联。如果选择路由表 A，而不选择路由表 B，则与路由表 A 关联的子网中的客户端可以访问 HA 对，但与路由表 B 关联的子网中的客户端无法访问。

有关路由表的详细信息，请参见 ["AWS 文档：路由表"](#)。

### 与 NetApp 管理工具的连接

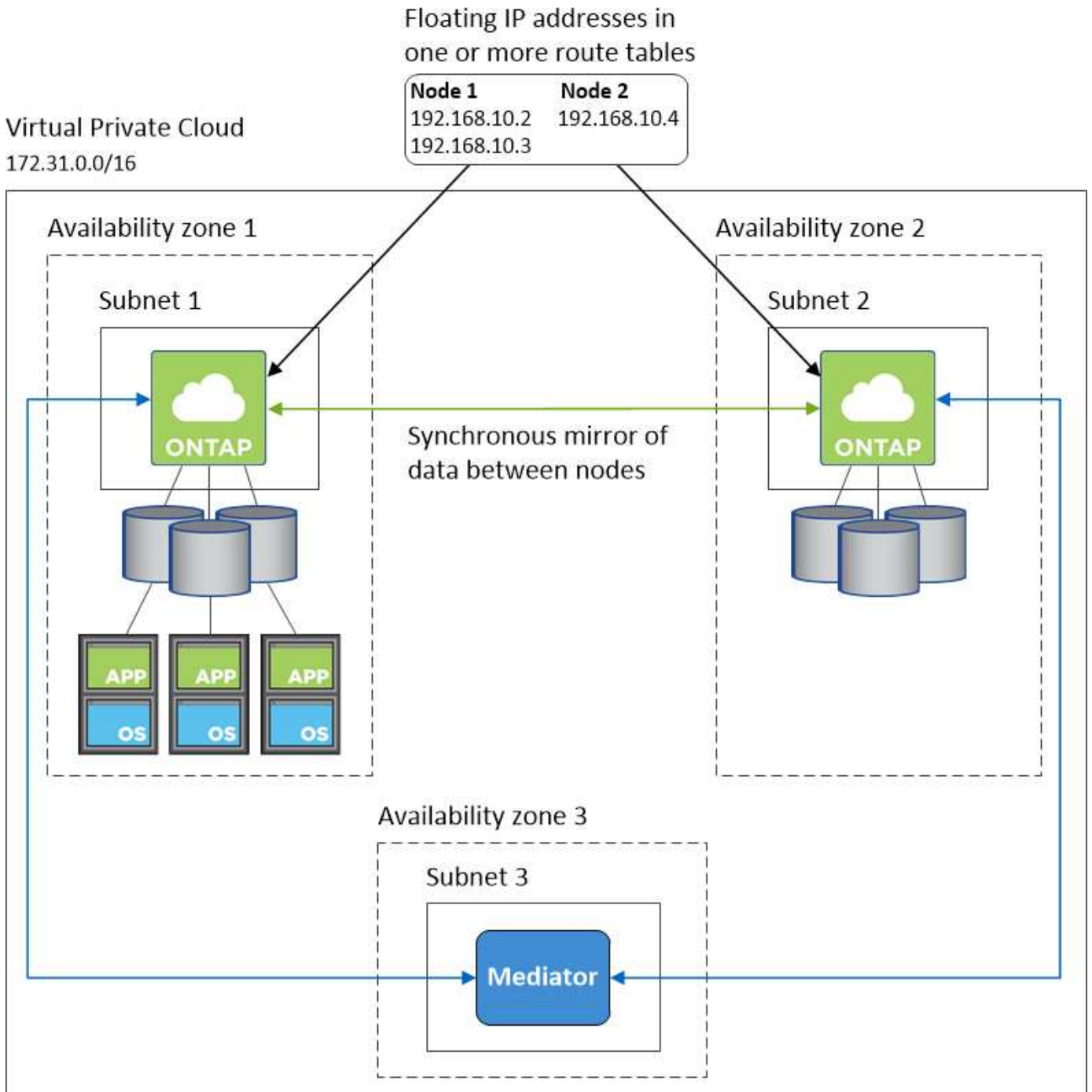
要对多个 AZs 中的 HA 配置使用 NetApp 管理工具，您可以选择两种连接方式：

1. 在其他 VPC 和中部署 NetApp 管理工具 ["设置 AWS 传输网关"](#)。通过网关，可以从 VPC 外部访问集群管理接口的浮动 IP 地址。
2. 在与 NAS 客户端具有类似路由配置的另一 VPC 中部署 NetApp 管理工具。

### HA 配置示例

下图显示了多个 AZs 中特定于 HA 对的网络组件：三个可用性区域，三个子网，浮动 IP 地址和路由表。





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"](#)
- ["AWS中的安全组规则"](#)

为多个 AZs 中的 HA 对设置 AWS 传输网关

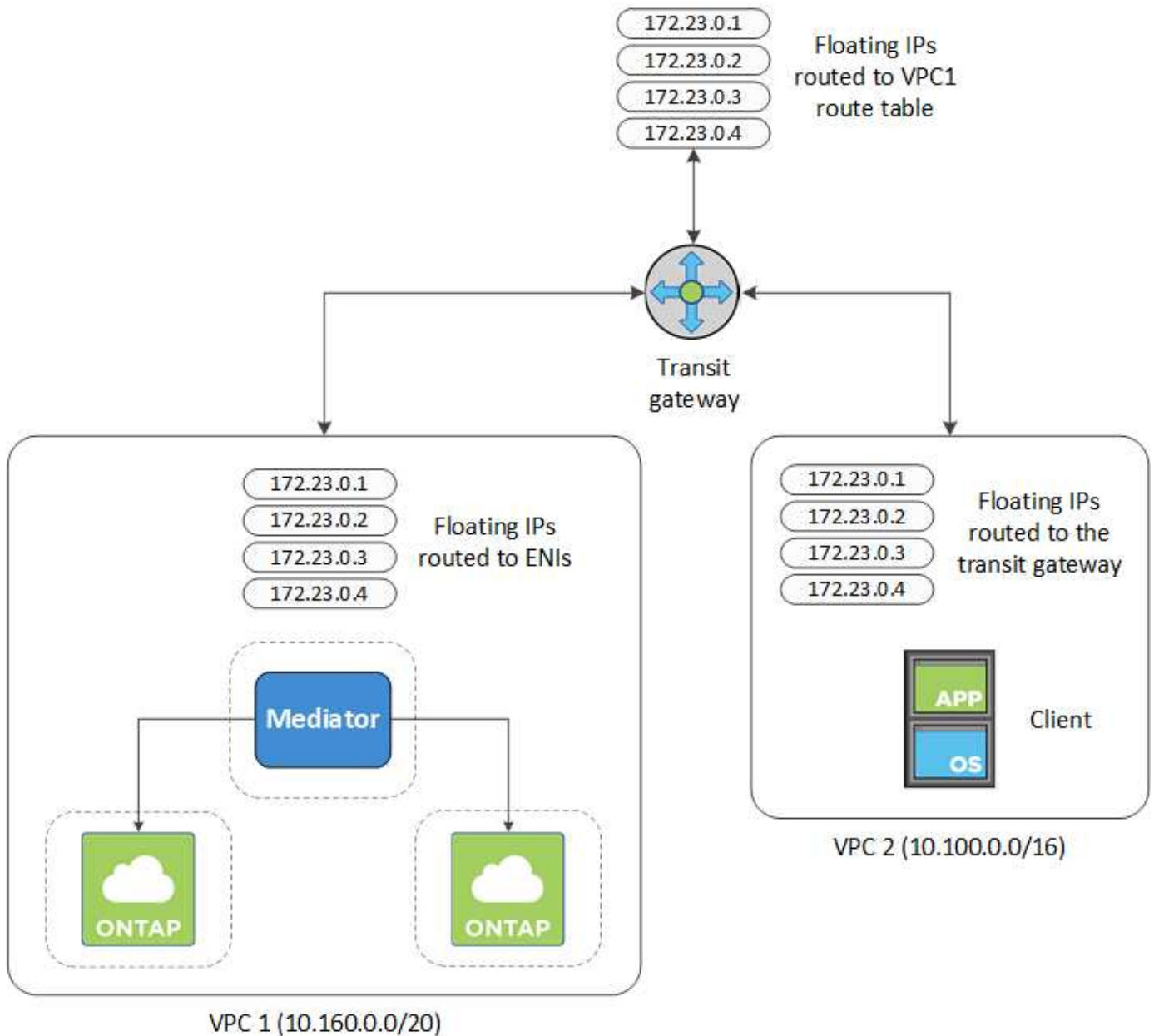
设置 AWS 传输网关以允许访问 HA 对 ["浮动 IP 地址"](#) 从 HA 对所在的 VPC 外部。

如果 Cloud Volumes ONTAP HA 配置分布在多个 AWS 可用性区域中，则从 VPC 内部访问 NAS 数据需要浮动 IP 地址。这些浮动 IP 地址可以在发生故障时在节点之间迁移，但无法从 VPC 外部本机访问。独立的专用 IP 地址可从 VPC 外部提供数据访问，但不提供自动故障转移。

集群管理接口和可选 SVM 管理 LIF 也需要浮动 IP 地址。

如果您设置了 AWS 传输网关，则可以从 HA 对所在的 VPC 外部访问浮动 IP 地址。这意味着 VPC 外部的 NAS 客户端和 NetApp 管理工具可以访问浮动 IP。

以下示例显示了通过传输网关连接的两个 vPC。一个 HA 系统驻留在一个 VPC 中，而一个客户端驻留在另一个 VPC 中。然后，您可以使用浮动 IP 地址在客户端上挂载 NAS 卷。



以下步骤说明了如何设置类似的配置。

步骤

1. "创建传输网关并将 vPC 连接到该网关"。

2. 将 vPC 与传输网关路由表关联。
  - a. 在 \* VPC\* 服务中，单击 \* 传输网关路由表 \* 。
  - b. 选择路由表。
  - c. 单击 \* 关联 \* ，然后选择 \* 创建关联 \* 。
  - d. 选择要关联的附件（ vPC ），然后单击 \* 创建关联 \* 。
3. 通过指定 HA 对的浮动 IP 地址，在传输网关的路由表中创建路由。

您可以在BlueXP的"工作环境信息"页面上找到浮动IP地址。以下是一个示例：

## NFS & CIFS access from within the VPC using Floating IP

### i Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

下图示例显示了传输网关的路由表。它包括到 Cloud Volumes ONTAP 所使用的两个 vPC 的 CIDR 块和四个浮动 IP 地址的路由。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

Floating IP Addresses

4. 修改需要访问浮动 IP 地址的 vPC 的路由表。
  - a. 向浮动 IP 地址添加路由条目。
  - b. 向 HA 对所在 VPC 的 CIDR 块添加路由条目。

下图示例显示了 VPC 2 的路由表，其中包括指向 VPC 1 的路由和浮动 IP 地址。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

5. 通过向需要访问浮动 IP 地址的 VPC 添加路由来修改 HA 对的 VPC 的路由表。

此步骤非常重要，因为它会完成 VPC 之间的路由。

下图示例显示了 VPC 1 的路由表。它包括一条指向浮动 IP 地址和客户端所在 VPC 2 的路由。在部署 HA 对时、BlueXP 会自动将浮动 IP 添加到路由表中。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

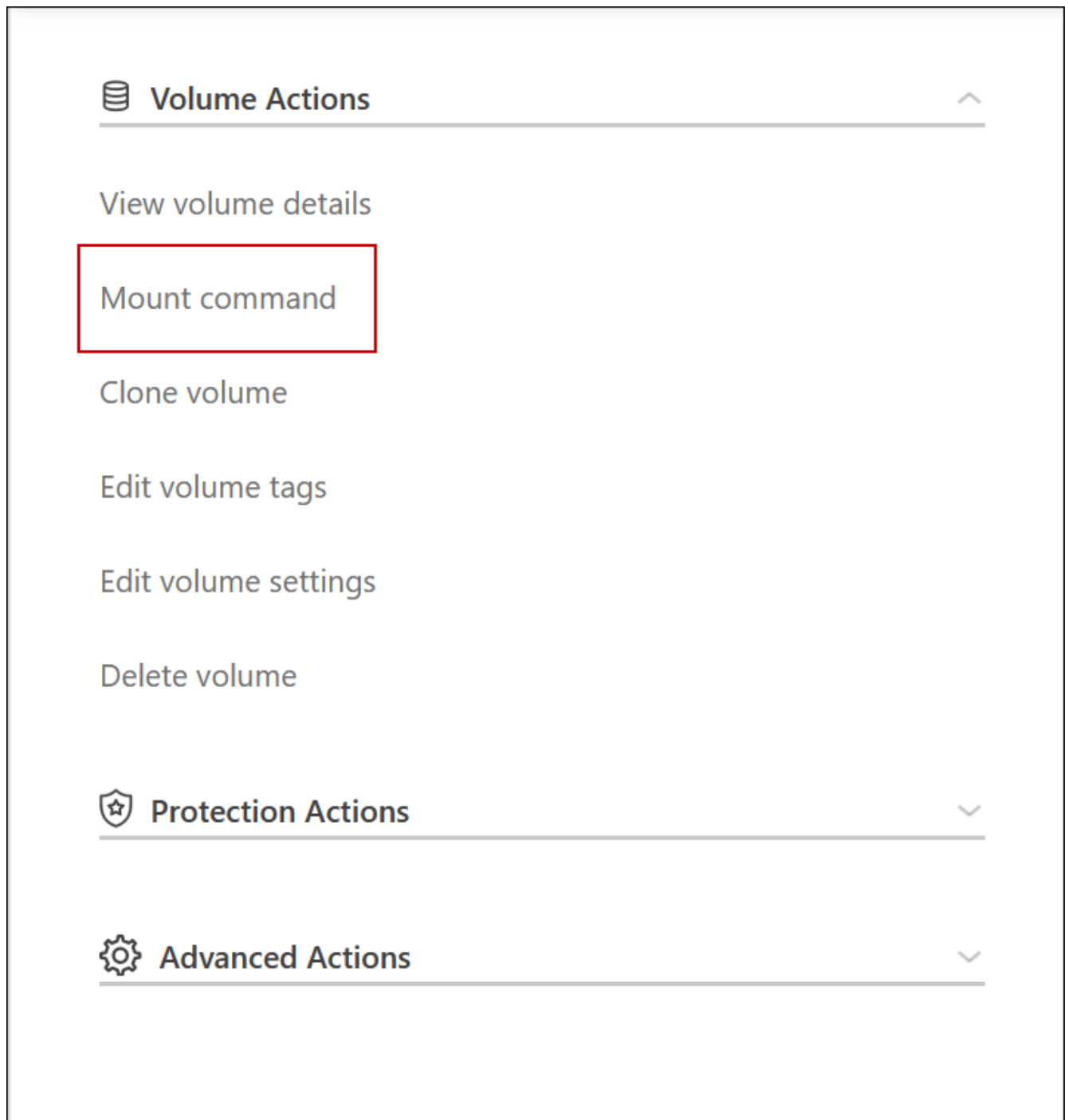
View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2  
Floating act IP Addresses

6. 使用浮动 IP 地址将卷挂载到客户端。

您可以通过 BlueXP 中“管理卷”面板下的\*挂载命令\*选项在 BlueXP 中找到正确的 IP 地址。



7. 如果要挂载 NFS 卷，请将导出策略配置为与客户端 VPC 的子网匹配。

["了解如何编辑卷"](#)。

- [相关链接 \\*](#)
- ["AWS 中的高可用性对"](#)
- ["AWS 中的 Cloud Volumes ONTAP 的网络要求"](#)

在共享子网中部署HA对

从9.11.1版开始、具有VPC共享的AWS支持Cloud Volumes ONTAP HA对。通过VPC共

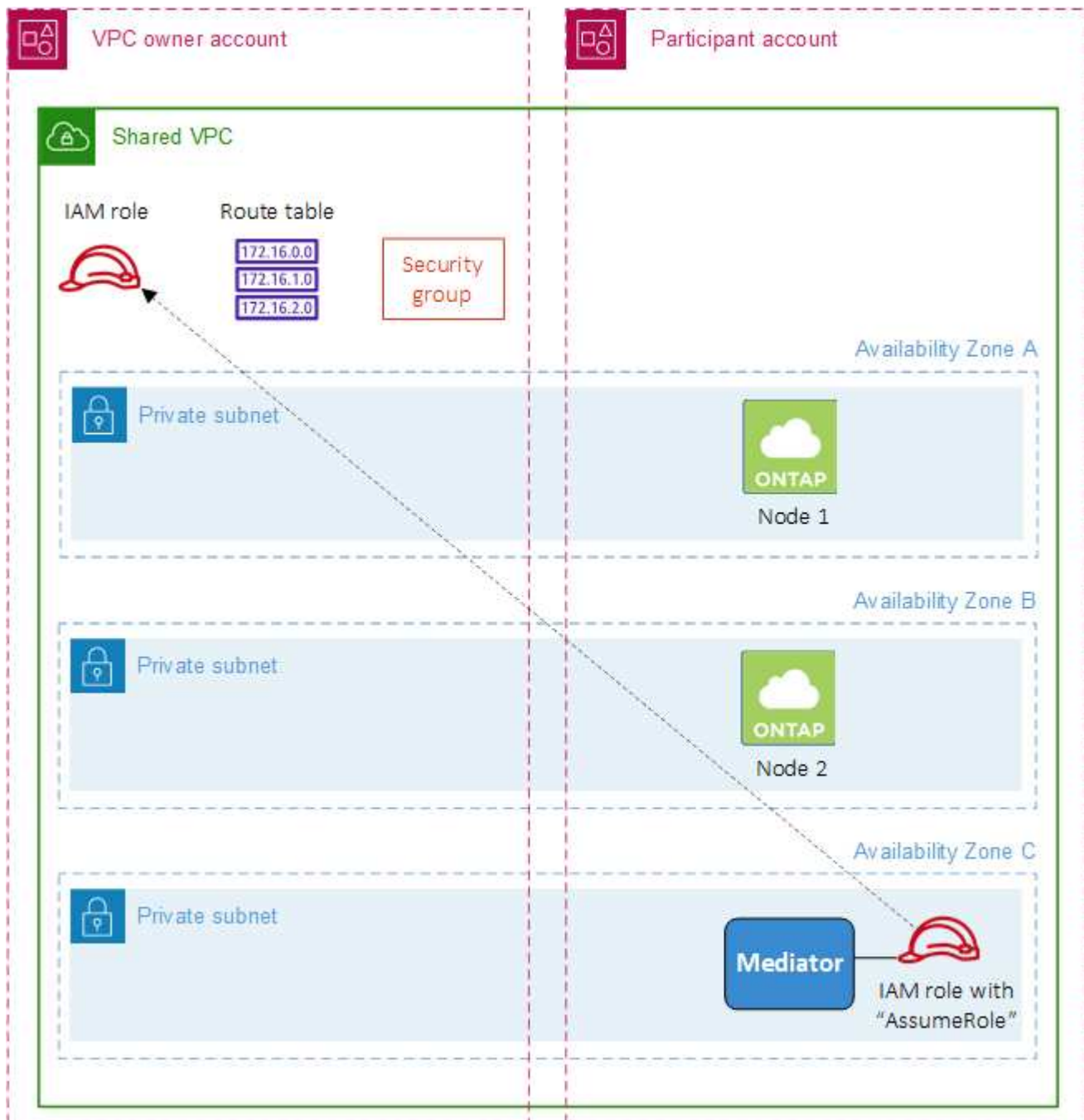
享、您的组织可以与其他AWS帐户共享子网。要使用此配置、您必须设置AWS环境、然后使用API部署HA对。

使用 "VPC共享"、一个Cloud Volumes ONTAP HA配置分布在两个帐户中：

- 拥有网络(VPC、子网、路由表和Cloud Volumes ONTAP 安全组)的VPC所有者帐户
- 参与者帐户、其中EC2实例部署在共享子网中(包括两个HA节点和调解器)

如果Cloud Volumes ONTAP HA配置部署在多个可用性区域中、则HA调解器需要特定的权限来写入VPC所有者帐户中的路由表。您需要通过设置调解器可以承担的IAM角色来提供这些权限。

下图显示了此部署涉及的组件：



如以下步骤所述、您需要与参与者帐户共享子网、然后在VPC所有者帐户中创建IAM角色和安全组。

创建Cloud Volumes ONTAP 工作环境时、BlueXP会自动创建IAM角色并将其附加到调解器。此角色将承担您在VPC所有者帐户中创建的IAM角色、以便更改与HA对关联的路由表。

#### 步骤

1. 与参与者帐户共享VPC所有者帐户中的子网。

要在共享子网中部署HA对、需要执行此步骤。

["AWS文档：共享子网"](#)

2. 在VPC所有者帐户中、为Cloud Volumes ONTAP 创建一个安全组。

["请参见Cloud Volumes ONTAP 的安全组规则"](#)。请注意、您不需要为HA调解器创建安全组。BlueXP可以为您提供这种服务。

3. 在VPC所有者帐户中、创建一个包含以下权限的IAM角色：

```
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ]
```

4. 使用BlueXP API创建新的Cloud Volumes ONTAP 工作环境。

请注意、您必须指定以下字段：

- "securityGroupId"

"securityGroupId"字段应指定您在VPC所有者帐户中创建的安全组(请参见上文第2步)。

- "haParams"对象中的"assumeRoleArn"

"assumeRoleArn"字段应包含您在VPC所有者帐户中创建的IAM角色的ARN (请参见上文第3步)。

例如：

```
    "haParams": {
      "assumeRoleArn":
        "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
    }
```



## AWS 的安全组规则

BlueXP会创建AWS安全组、其中包含Cloud Volumes ONTAP 成功运行所需的入站和出站规则。您可能希望参考这些端口进行测试或使用自己的安全组。

### Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

#### 入站规则

在创建工作环境并选择预定义的安全组时、您可以选择允许以下其中一个范围内的流量：

- 仅选定**VPC**：入站流量的源是Cloud Volumes ONTAP 系统的VPC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IP范围为0.0.0.0/0。

协议	Port	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理LIF的IP地址连接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
UDP	111.	远程过程调用 NFS



协议	Port	目的
UDP	161-162	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049-51	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
备份到 S3	TCP	5010	集群间 LIF	备份端点或还原端点	备份到 S3 功能的备份和还原操作
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信 (仅限 Cloud Volumes ONTAP HA)
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用 (仅适用于 Cloud Volumes ONTAP HA)
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态 (仅限 Cloud Volumes ONTAP HA)
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

## HA 调解器外部安全组的规则

Cloud Volumes ONTAP HA 调解器的预定义外部安全组包括以下入站和出站规则。

### 入站规则

HA调解器的预定义安全组包括以下入站规则。

协议	Port	源	目的
TCP	3000	连接器的CIDR	从 Connector 进行 RESTful API 访问

### 出站规则

HA 调解器的预定义安全组将打开所有出站通信。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

HA 调解器的预定义安全组包括以下出站规则。

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

如果需要严格的出站通信规则、可以使用以下信息仅打开 HA 调解器出站通信所需的端口。

协议	Port	目标	目的
HTTP	80	AWS EC2实例上连接器的IP地址	下载调解器升级
HTTPS	443.	ec2.amazonaws.com	帮助进行存储故障转移
UDP	53.	ec2.amazonaws.com	帮助进行存储故障转移



您可以创建从目标子网到 AWS EC2 服务的接口 VPC 端点，而不是打开端口 443 和 53 。

## HA配置内部安全组的规则

为Cloud Volumes ONTAP HA配置预定义的内部安全组包括以下规则。通过此安全组、可以在HA节点之间以及调解器与节点之间进行通信。

BlueXP始终会创建此安全组。您没有使用自己的选项。

### 入站规则

预定义的安全组包括以下入站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

## 出站规则

预定义的安全组包括以下出站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

## Connector 的规则

["查看Connector的安全组规则"](#)

## 设置 AWS KMS

如果要在 Cloud Volumes ONTAP 中使用 Amazon 加密，则需要设置 AWS 密钥管理服务（KMS）。

### 步骤

1. 确保存在有效的客户主密钥（CMK）。

CMK 可以是 AWS 管理的 CMK 或客户管理的 CMK。它可以与 BlueXP 和 Cloud Volumes ONTAP 位于同一个 AWS 帐户中、也可以位于不同的 AWS 帐户中。

["AWS 文档：客户主密钥（CMK）"](#)

2. 通过添加 IAM 角色来修改每个 CMK 的密钥策略、该角色以 `_key user__` 的身份为 BlueXP 提供权限。

如果将 IAM 角色添加为密钥用户、则 BlueXP 将获得在 Cloud Volumes ONTAP 中使用 CMK 的权限。

["AWS 文档：编辑密钥"](#)

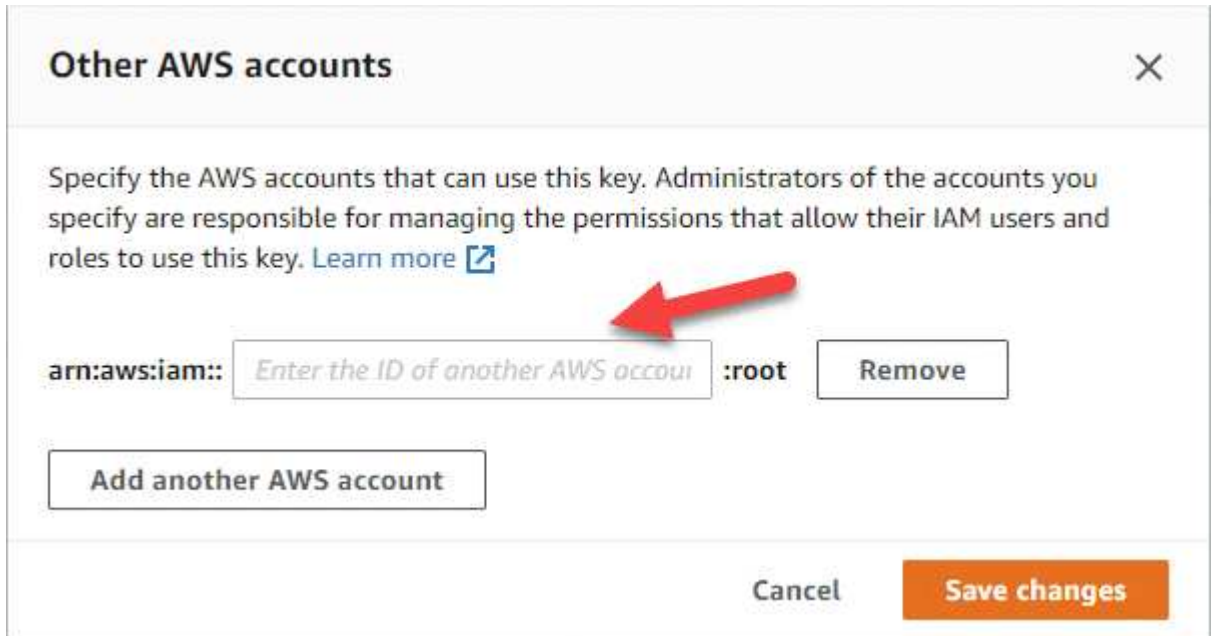
3. 如果 CMK 位于其他 AWS 帐户中，请完成以下步骤：

- a. 从 CMK 所在的帐户转到 KMS 控制台。
- b. 选择密钥。
- c. 在 \* 常规配置 \* 窗格中，复制密钥的 ARN。

创建 Cloud Volumes ONTAP 系统时、您需要为 BlueXP 提供 ARN。

- d. 在 \* 其他 AWS 帐户 \* 窗格中、添加为 BlueXP 提供权限的 AWS 帐户。

在大多数情况下、这是 BlueXP 所在的帐户。如果 BlueXP 未安装在 AWS 中、则您会为其提供对 BlueXP 的 AWS 访问密钥。



- e. 现在、切换到为BlueXP提供权限的AWS帐户、然后打开IAM控制台。
- f. 创建一个包含以下权限的 IAM 策略。
- g. 将策略附加到为BlueXP提供权限的IAM角色或IAM用户。

以下策略提供了BlueXP从外部AWS帐户使用CMK所需的权限。请务必在 "资源" 部分中修改区域和帐户ID。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

有关此过程的其他详细信息，请参见 ["AWS 文档：允许其他帐户中的用户使用 KMS 密钥"](#)。

4. 如果您使用的是客户管理的 Cloud Volumes ONTAP，请通过将 CMK 的 IAM 角色添加为 `_key user_` 来修改 CMK 的密钥策略。

如果您在 Cloud Volumes ONTAP 上启用了数据分层并希望对存储在 S3 存储分段中的数据进行加密，则需

要执行此步骤。

部署 Cloud Volumes ONTAP 后，您需要执行此步骤，因为 IAM 角色是在创建工作环境时创建的。（当然，您可以选择使用现有的 Cloud Volumes ONTAP IAM 角色，因此可以先执行此步骤。）

["AWS 文档：编辑密钥"](#)

## 为 Cloud Volumes ONTAP 设置 IAM 角色

必须将具有所需权限的 IAM 角色附加到每个 Cloud Volumes ONTAP 节点。HA 调解器也是如此。让 BlueXP 为您创建 IAM 角色最简单，但您可以使用自己的角色。

此任务为可选任务。创建 Cloud Volumes ONTAP 工作环境时，默认选项是让 BlueXP 为您创建 IAM 角色。如果贵企业的安全策略要求您自己创建 IAM 角色，请执行以下步骤。



在 AWS 商用云服务环境中，需要提供您自己的 IAM 角色。 ["了解如何在 C2S 中部署 Cloud Volumes ONTAP"](#)。

### 步骤

1. 转到 AWS IAM 控制台。
2. 创建包含以下权限的 IAM 策略：
  - Cloud Volumes ONTAP 节点的基本策略



## 标准区域

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

## GovCloud (美国)地区

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-us-gov:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}
```

**C2S**环境

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}
```

- Cloud Volumes ONTAP 节点的备份策略

如果您计划对Cloud Volumes ONTAP 系统使用BlueXP备份和恢复、则节点的IAM角色必须包括以下第二个策略。

## 标准区域

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

## GovCloud (美国)地区

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

**C2S环境**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

◦ HA 调解器

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses",
      "sts:AssumeRole",
      "ec2:DescribeSubnets"
    ],
    "Resource": "*"
  }
]
}

```

3. 创建IAM角色并将您创建的策略附加到该角色。

#### 结果

现在、您可以在创建新的Cloud Volumes ONTAP 工作环境时选择IAM角色。

#### 更多信息

- ["AWS文档：创建IAM策略"](#)
- ["AWS文档：创建IAM角色"](#)

## 在AWS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AWS 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"。

### Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go  
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

a. 返回到BlueXP后、访问充电方法页面时选择\*免费\*。

### Select Charging Method

Professional **By capacity** ▾

Essential **By capacity** ▾

Freemium (Up to 500 GiB) **By capacity** ▾

Per Node **By node** ▾

"查看在AWS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）
- AWS Marketplace提供的每小时按需购买(PAYGO)订阅
- AWS Marketplace的年度合同

["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AWS 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。

## Edit Credentials & Add Subscription

---

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
 Pay for Cloud Volumes ONTAP at an hourly rate.

---

**The next steps:**

- 1 **AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

---

Continue
Cancel

a. 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	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> <span>∨</span>
<input type="radio"/>	Essential	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> <span>∨</span>
<input type="radio"/>	Freemium (Up to 500 GiB)	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> <span>∨</span>
<input type="radio"/>	Per Node	<span style="background-color: #800080; color: white; padding: 2px 5px;">By node</span> <span>∨</span>

"查看在AWS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AWS Marketplace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AWS Marketplace中的按需购买服务。

**Edit Credentials & Add Subscription**

---

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

---

**The next steps:**

**1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.

**2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

---

**Continue** **Cancel**

- 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AWS中启动Cloud Volumes ONTAP 的分步说明"。



您可以从"设置">"凭据"页面管理与AWS帐户关联的AWS Marketplace订阅。 ["了解如何管理AWS帐户和订阅"](#)

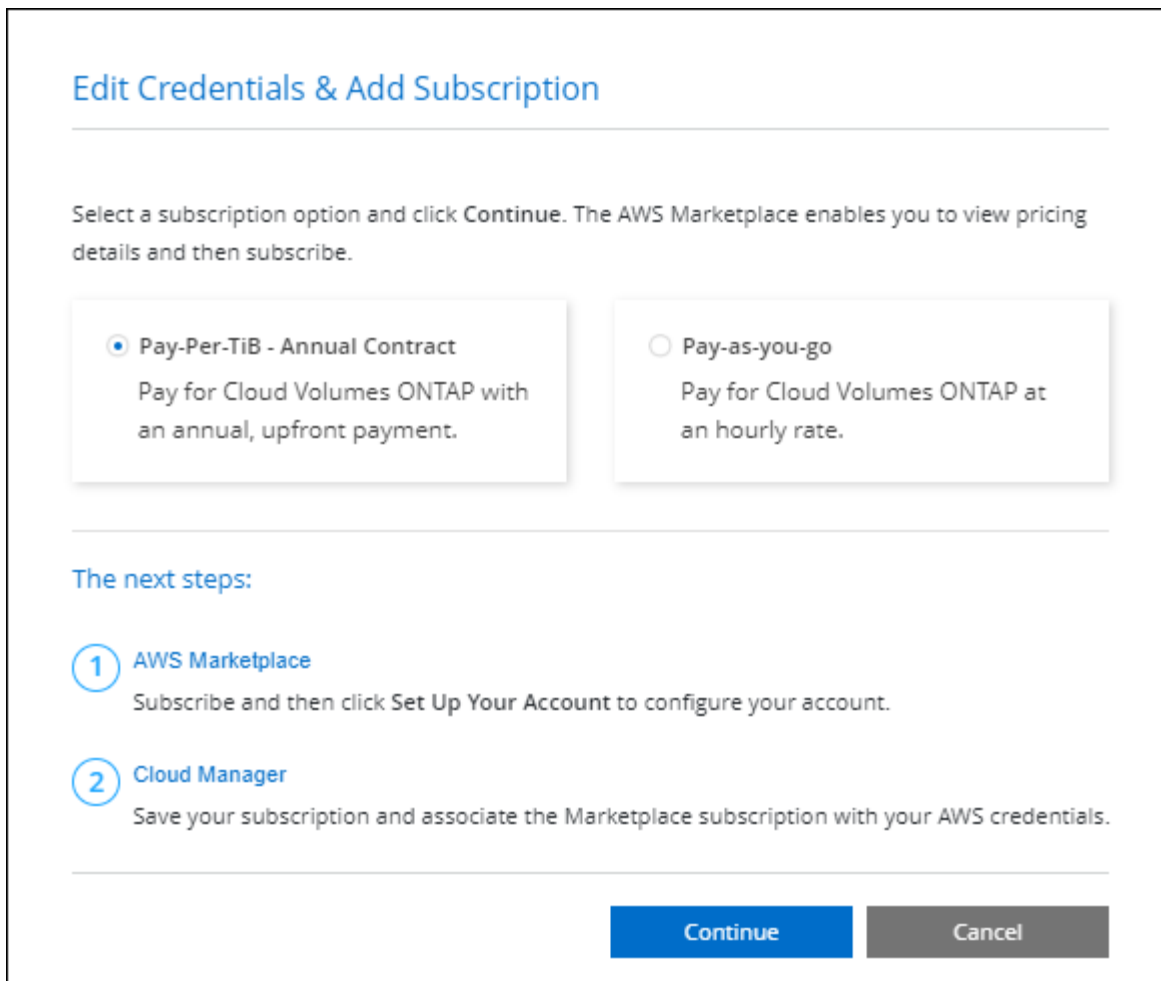
#### 年度合同

通过从云提供商的市场购买年度合同、按年付费。

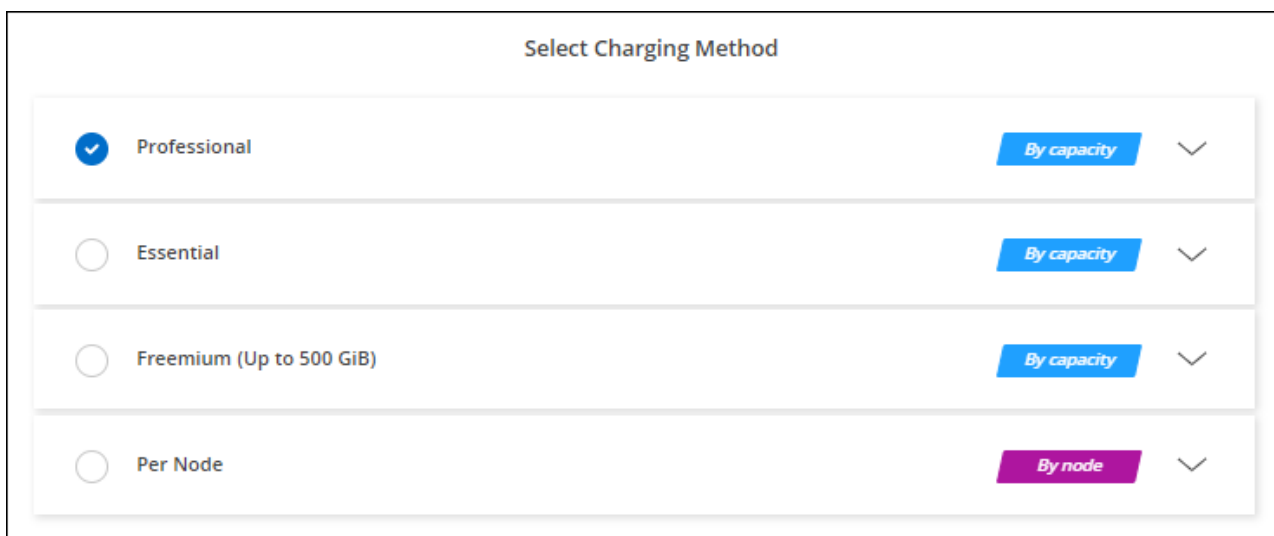
与按小时订阅类似、BlueXP会提示您订阅AWS Marketplace中提供的年度合同。

#### 步骤

1. 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AWS Marketplace中订阅年度合同。



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。



"查看在AWS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。

The screenshot shows a 'Select Charging Method' dialog box. It has a title bar and a list of five options. The 'Keystone' option is selected, indicated by a blue checkmark in a circle. To its right is a blue button labeled 'By capacity' and an upward-pointing chevron. Below the 'Keystone' option, there is text: 'Storage management', 'Charged against your NetApp credit', and 'Keystone Subscription'. Under 'Keystone Subscription', there is a dropdown menu with 'A-AMRITA1' selected. The other four options are 'Professional', 'Essential', 'Freemium (Up to 500 GiB)', and 'Per Node'. Each of these has a radio button to its left and a button to its right labeled 'By capacity' (for the first three) or 'By node' (for 'Per Node').

"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

## 在 AWS 中启动 Cloud Volumes ONTAP

您可以在单系统配置中或在 AWS 中作为 HA 对启动 Cloud Volumes ONTAP 。

### 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"。

- 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 AWS 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"](#)。

- 用于 CIFS 配置的 DNS 和 Active Directory 。

有关详细信息，请参见 ["AWS 中的 Cloud Volumes ONTAP 的网络要求"](#)。

## 在 AWS 中启动单节点 Cloud Volumes ONTAP 系统

如果要在 AWS 中启动 Cloud Volumes ONTAP，则需要在 BlueXP 中创建新的工作环境

### 关于此任务

创建工作环境后，BlueXP 会立即在指定的 VPC 中启动一个测试实例以验证连接。如果成功，BlueXP 将立即终止实例，然后开始部署 Cloud Volumes ONTAP 系统。如果 BlueXP 无法验证连接，则创建工作环境将失败。该测试实例可以是 t2.nano（对于默认 vPC 占用）或 m3.medium（对于专用 vPC 占用）。

### 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 **\*Amazon Web Services\*** 和 **\*Cloud Volumes ONTAP Single Node\***。
4. 如果出现提示，**"创建连接器"**。
5. **\*详细信息和凭据\***：可选择更改 AWS 凭据和订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

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
工作环境名称	BlueXP 使用工作环境名称来命名 Cloud Volumes ONTAP 系统和 Amazon EC2 实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标记	<p>AWS 标记是 AWS 资源的元数据。BlueXP 会将标记添加到 Cloud Volumes ONTAP 实例以及与该实例关联的每个 AWS 资源。</p> <p>在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。</p> <p>有关标记的信息，请参见 <a href="#">"AWS 文档：标记 Amazon EC2 资源"</a>。</p>
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
编辑凭据	<p>选择与要部署此系统的帐户关联的 AWS 凭据。您还可以关联 AWS Marketplace 订阅以用于此 Cloud Volumes ONTAP 系统。</p> <p>单击 * 添加订阅 * 将选定凭据与新的 AWS Marketplace 订阅关联。订阅可以是一份年度合同，也可以是按小时付费的 Cloud Volumes ONTAP。</p> <p>"了解如何向BlueXP添加其他AWS凭据"。</p>

以下视频介绍如何将按需购买的 Marketplace 订阅与您的 AWS 凭据相关联：

► [https://docs.netapp.com/zh-cn/test//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-cn/test//media/video_subscribing_aws.mp4) (video)

如果多个 IAM 用户在同一个 AWS 帐户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS Marketplace 会通知后续用户他们已订阅，如下图所示。虽然已为 AWS account 订阅，但每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到以下消息、请单击\*单击此处\*链接以转到BlueXP网站并完成此过程。



**Cloud Manager (for Cloud Volumes ONTAP)**

---

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

**?** **Having issues signing up for your product?**  
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

**Pricing Details**

Software Fees

6. \* 服务 \*：保持服务处于启用状态或禁用不想在 Cloud Volumes ONTAP 中使用的单个服务。
- "了解有关BlueXP分类的更多信息"
  - "了解有关BlueXP备份和恢复的更多信息"



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 \*：输入您在中记录的网络信息 "AWS 工作表"。

下表介绍了可能需要指导的字段：

字段	Description
VPC	如果您有 AWS 前台，则可以通过选择前台 VPC 在该前台部署单节点 Cloud Volumes ONTAP 系统。体验与 AWS 中的任何其他 VPC 相同。
已生成安全组	<p>如果您让BlueXP为您生成安全组、则需要选择允许流量的方式：</p> <ul style="list-style-type: none"> <li>• 如果选择*仅选定VPC*、则入站流量的源是选定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IP范围为0.0.0.0/0。</li> </ul>



字段	Description
使用现有安全组	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> "。

8. \* 数据加密 \*：不选择数据加密或 AWS 管理的加密。

对于 AWS 管理的加密，您可以从您的帐户或其他 AWS 帐户中选择其他客户主密钥（CMK）。



创建 Cloud Volumes ONTAP 系统后，您无法更改 AWS 数据加密方法。

"[了解如何为 Cloud Volumes ONTAP 设置 AWS KMS](#)"。

"[了解有关支持的加密技术的更多信息](#)"。

9. 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](#)"。

10. \* Cloud Volumes ONTAP 配置 \*（仅限年度 Marketplace 合同）：查看默认配置，然后单击 \* 继续 \* 或单击 \* 更改配置 \* 以选择您自己的配置。

如果保留默认配置，则只需指定一个卷，然后查看并批准该配置。

11. 预配置软件包：选择一个软件包以快速启动 Cloud Volumes ONTAP、或者单击 \* 更改配置 \* 以选择您自己的配置。

如果选择其中一个软件包，则只需指定一个卷，然后查看并批准该配置。

12. \* IAM 角色 \*：最好保留默认选项、让 BlueXP 为您创建角色。

如果您希望使用自己的策略，则必须满足 "[Cloud Volumes ONTAP 节点的策略要求](#)"。

13. 许可：根据需要更改 Cloud Volumes ONTAP 版本、并选择实例类型和实例租户。



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。

14. 底层存储资源：选择磁盘类型、配置底层存储、然后选择是否启用数据分层。

请注意以下事项：

- 磁盘类型适用于初始卷(和聚合)。您可以为后续卷(和聚合)选择不同的磁盘类型。
- 如果您选择 GP3 或 IO1 磁盘、则 BlueXP 会根据需要使用 AWS 中的弹性卷功能自动增加底层存储磁盘容量。您可以根据存储需求选择初始容量、并在部署 Cloud Volumes ONTAP 后进行修改。"[了解有关在 AWS 中支持弹性卷的更多信息](#)"。
- 如果您选择 GP2 或 st1 磁盘、则可以为初始聚合中的所有磁盘以及 BlueXP 在使用简单配置选项时创建的任何其他聚合选择一个磁盘大小。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

- 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它。

["了解数据分层的工作原理"](#)。

#### 15. 写入速度和WORM:

- 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。"](#)。

- 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。"](#)。

- 如果激活了WORM存储、请选择保留期限。

#### 16. \* 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

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

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，则应在此字段中输入 * OU=Computers，OU=corp*。

字段	Description
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。如果需要其他地址配置 NTP 服务器，则应使用 API。请参见 <a href="#">"BlueXP 自动化文档"</a> 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>

18. \* 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编辑卷分层策略。

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"](#)。

19. \* 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AWS资源的详细信息。
- c. 选中 \* 我了解 ... \* 复选框。
- d. 单击 \* 执行 \*。

## 结果

BlueXP将启动Cloud Volumes ONTAP 实例。您可以跟踪时间链中的进度。

如果在启动 Cloud Volumes ONTAP 实例时遇到任何问题，请查看故障消息。您还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 AWS 中启动 Cloud Volumes ONTAP HA 对

如果要在AWS中启动Cloud Volumes ONTAP HA对、则需要在BlueXP中创建HA工作环境。

## 限制

目前，AWS 前向不支持 HA 对。

## 关于此任务

创建工作环境后、BlueXP会立即在指定的VPC中启动一个测试实例以验证连接。如果成功、BlueXP将立即终止实例、然后开始部署Cloud Volumes ONTAP 系统。如果BlueXP无法验证连接、则创建工作环境将失败。该测试实例可以是 t2.nano（对于默认 vPC 占用）或 m3.medium（对于专用 vPC 占用）。

## 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. 选择一个位置：选择\* Amazon Web Services\*和\* Cloud Volumes ONTAP HA\*。
4. \* 详细信息和凭据 \*：可选择更改 AWS 凭据和订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

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
工作环境名称	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Amazon EC2实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标记	<p>AWS 标记是 AWS 资源的元数据。BlueXP会将标记添加到Cloud Volumes ONTAP 实例以及与该实例关联的每个AWS资源。</p> <p>在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。</p> <p>有关标记的信息，请参见 "<a href="#">AWS 文档：标记 Amazon EC2 资源</a>"。</p>
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。
编辑凭据	<p>选择要用于此 Cloud Volumes ONTAP 系统的 AWS 凭据和 Marketplace 订阅。</p> <p>单击 * 添加订阅 * 将选定凭据与新的 AWS Marketplace 订阅关联。订阅可以是一份年度合同，也可以是按小时付费的 Cloud Volumes ONTAP 。</p> <p>如果直接从 NetApp （BYOL）购买许可证，则不需要 AWS 订阅。</p> <p><a href="#">"了解如何向BlueXP添加其他AWS凭据"</a>。</p>

以下视频介绍如何将按需购买的 Marketplace 订阅与您的 AWS 凭据相关联：

► [https://docs.netapp.com/zh-cn/test//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/zh-cn/test//media/video_subscribing_aws.mp4) (video)

如果多个 IAM 用户在同一个 AWS 帐户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS Marketplace 会通知后续用户他们已订阅，如下图所示。虽然已为 AWS *account* 订阅，但每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到以下消息、请单击\*单击此处\*链接以转到BlueXP网站并完成此过程。



### Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.



#### Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

#### Pricing Details

Software Fees

5. \* 服务 \*：保持服务处于启用状态或禁用不想在此 Cloud Volumes ONTAP 系统中使用的单个服务。

- ["了解有关BlueXP分类的更多信息"](#)
- ["了解有关BlueXP备份和恢复的更多信息"](#)



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 \*：选择一个高可用性配置。

有关部署模式的概述，请参见 ["适用于 AWS 的 Cloud Volumes ONTAP HA"](#)。

7. 位置和连接(单个AZ)或\*区域和VPC\*(多个AZs)：输入您在AWS工作表中记录的网络信息。

下表介绍了可能需要指导的字段：

字段	Description
已生成安全组	如果您让BlueXP为您生成安全组、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IP范围为0.0.0.0/0。</li></ul>
使用现有安全组	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> 。

8. \* 连接和 SSH 身份验证 \*：选择 HA 对和调解器的连接方法。

9. \* 浮动 IP\*：如果选择多个 AZs ，请指定浮动 IP 地址。

该区域中所有 VPC 的 IP 地址必须位于 CIDR 块之外。有关其他详细信息，请参见 ["适用于多个 AWS 中的 Cloud Volumes ONTAP HA 的 AWS 网络要求"](#)。

10. \* 路由表 \*：如果选择多个 AZs ，请选择应包含指向浮动 IP 地址的路由的路由表。

如果有多个路由表、则选择正确的路由表非常重要。否则，某些客户端可能无法访问 Cloud Volumes ONTAP HA 对。有关路由表的详细信息，请参见 ["AWS 文档：路由表"](#)。

11. \* 数据加密 \*：不选择数据加密或 AWS 管理的加密。

对于 AWS 管理的加密，您可以从您的帐户或其他 AWS 帐户中选择其他客户主密钥（CMK）。



创建 Cloud Volumes ONTAP 系统后，您无法更改 AWS 数据加密方法。

["了解如何为 Cloud Volumes ONTAP 设置 AWS KMS"](#)。

["了解有关支持的加密技术的更多信息"](#)。

12. 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"](#)。

13. \* Cloud Volumes ONTAP 配置 \* (仅限年度 Marketplace 合同) : 查看默认配置, 然后单击 \* 继续 \* 或单击 \* 更改配置 \* 以选择您自己的配置。

如果保留默认配置, 则只需指定一个卷, 然后查看并批准该配置。

14. \* 预配置软件包 \* (仅限每小时或自带卷) : 选择一个软件包以快速启动 Cloud Volumes ONTAP , 或者单击 \* 更改配置 \* 以选择您自己的配置。

如果选择其中一个软件包, 则只需指定一个卷, 然后查看并批准该配置。

15. \* IAM角色\* : 最好保留默认选项、让BlueXP为您创建角色。

如果您希望使用自己的策略, 则必须满足 ["Cloud Volumes ONTAP 节点和 HA 调解器的策略要求"](#)。

16. 许可: 根据需要更改Cloud Volumes ONTAP 版本、并选择实例类型和实例租户。



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 。

17. 底层存储资源: 选择磁盘类型、配置底层存储、然后选择是否启用数据分层。

请注意以下事项:

- 磁盘类型适用于初始卷(和聚合)。您可以为后续卷(和聚合)选择不同的磁盘类型。
- 如果您选择GP3或IO1磁盘、则BlueXP会根据需要使用AWS中的弹性卷功能自动增加底层存储磁盘容量。您可以根据存储需求选择初始容量、并在部署Cloud Volumes ONTAP 后进行修改。 ["了解有关在AWS中支持弹性卷的更多信息"](#)。
- 如果您选择GP2或st1磁盘、则可以为初始聚合中的所有磁盘以及BlueXP在使用简单配置选项时创建的任何其他聚合选择一个磁盘大小。您可以使用高级分配选项创建使用不同磁盘大小的聚合。
- 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它。

["了解数据分层的工作原理"](#)。

18. 写入速度和WORM:

- a. 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。"](#)

- b. 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。

19. \* 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，"<a href="#">使用 IQN 从主机连接到 LUN</a>"。</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;"> <span style="margin-right: 20px;">NFS</span> <span style="margin-right: 20px; border-bottom: 2px solid #007bff; display: inline-block; width: 100px;"></span> <span>iSCSI</span> </p> <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 style="font-size: small;">Valid users and groups separated by a semicolon</p>

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

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (服务位置记录)。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器, 则应在此字段中输入 * OU=Computers, OU=corp*。
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。如果需要其他地址配置 NTP 服务器, 则应使用 API。请参见 <a href="#">"BlueXP 自动化文档"</a> 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>

21. \* 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编辑卷分层策略。

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"](#)。

22. \* 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AWS资源的详细信息。

c. 选中 \* 我了解 ...\* 复选框。

d. 单击 \* 执行 \* 。

## 结果

BlueXP将启动Cloud Volumes ONTAP HA对。您可以跟踪时间链中的进度。

如果在启动 HA 对时遇到任何问题、请查看故障消息。您还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。

## 开始在 **AWS C2S** 环境中使用 **Cloud Volumes ONTAP**

与标准 AWS 区域类似，您可以在中使用 Cloud Manager "[AWS 商用云服务（C2S）](#)" 部署 Cloud Volumes ONTAP 的环境，为您的云存储提供企业级功能。AWS C2S 是一个特定于美国的封闭区域智能社区；此页面上的说明仅适用于 AWS C2S 区域用户。

### C2S中支持的版本

- 支持Cloud Volumes ONTAP 9.8
- 支持连接器3.9.4版

Connector是在AWS中部署和管理Cloud Volumes ONTAP 所需的软件。您将从安装在 Connector 实例上的软件登录到 Cloud Manager 。C2S环境不支持适用于Cloud Manager的SaaS网站。



Cloud Manager最近已重命名为BlueXP、但我们仍在C2S中将其称为Cloud Manager、因为Connector 3.9.4版附带的用户界面仍称为Cloud Manager。

### C2S 中支持的功能

在 C2S 环境中， Cloud Manager 提供了以下功能：

- Cloud Volumes ONTAP
- 数据复制
- 审核时间表

对于 Cloud Volumes ONTAP ，您可以创建单节点系统或 HA 对。这两种许可选项均可用：按需购买和自带许可证（BYOL）。

C2S 中的 Cloud Volumes ONTAP 也支持将数据分层到 S3 。

## 限制

- Cloud Manager 不提供任何 NetApp 云服务。
- 由于 C2S 环境中无法访问 Internet ，因此以下功能也不可⽤：
  - 从 Cloud Manager 自动升级软件
  - NetApp AutoSupport
  - Cloud Volumes ONTAP 资源的 AWS 成本信息
- C2S环境不支持免费许可证。

## 部署概述

在 C2S 中开始使用 Cloud Volumes ONTAP 包括几个步骤。

### 1. 准备AWS环境

其中包括设置网络，订阅 Cloud Volumes ONTAP ，设置权限以及选择设置 AWS KMS 。

### 2. 安装Connector并设置Cloud Manager

在开始使用 Cloud Manager 部署 Cloud Volumes ONTAP 之前，您需要先创建 *Connector* 。借助此连接器，Cloud Manager 可以管理公有云环境（包括 Cloud Volumes ONTAP ）中的资源和流程。

您将从安装在 Connector 实例上的软件登录到 Cloud Manager 。

### 3. 从Cloud Manager启动Cloud Volumes ONTAP

下面介绍了其中的每个步骤。

## 准备AWS环境

您的 AWS 环境必须满足一些要求。

### 设置网络

设置 AWS 网络，以便 Cloud Volumes ONTAP 可以正常运行。

### 步骤

1. 选择要启动连接器实例和 Cloud Volumes ONTAP 实例的 VPC 和子网。
2. 确保您的 VPC 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
3. 将 VPC 端点设置为 S3 服务。

如果要将冷数据从 Cloud Volumes ONTAP 分层到低成本对象存储，则需要 VPC 端点。

## 订阅 Cloud Volumes ONTAP

要从 Cloud Manager 部署 Cloud Volumes ONTAP ，需要订阅 Marketplace 。

### 步骤

1. 转到 AWS 智能社区市场并搜索 Cloud Volumes ONTAP 。
2. 选择您计划部署的产品。
3. 查看条款并单击 \* 接受 \* 。
4. 如果您计划部署其他产品，请对其重复上述步骤。

您必须使用 Cloud Manager 启动 Cloud Volumes ONTAP 实例。不得从 EC2 控制台启动 Cloud Volumes ONTAP 实例。

#### 设置权限

设置IAM策略和角色、为Connector和Cloud Volumes ONTAP 提供在AWS商用云服务环境中执行操作所需的权限。

您需要为以下每项设置一个 IAM 策略和 IAM 角色：

- Connector 实例
- Cloud Volumes ONTAP 实例
- Cloud Volumes ONTAP HA 调解器实例（如果要部署 HA 对）

#### 步骤

1. 转到 AWS IAM 控制台，然后单击 \* 策略 \* 。
2. 为 Connector 实例创建策略。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
```

```

    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2>DeleteNetworkInterface",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcs",
    "ec2:DescribeDhcpOptions",
    "ec2:CreateSnapshot",
    "ec2>DeleteSnapshot",
    "ec2:DescribeSnapshots",
    "ec2:GetConsoleOutput",
    "ec2:DescribeKeyPairs",
    "ec2:DescribeRegions",
    "ec2>DeleteTags",
    "ec2:DescribeTags",
    "cloudformation:CreateStack",
    "cloudformation>DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:ValidateTemplate",
    "iam:PassRole",
    "iam:CreateRole",
    "iam>DeleteRole",
    "iam:PutRolePolicy",
    "iam:ListInstanceProfiles",
    "iam:CreateInstanceProfile",
    "iam>DeleteRolePolicy",
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam>DeleteInstanceProfile",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:ListAllMyBuckets",
    "kms:List*",
    "kms:Describe*",
    "ec2:AssociateIamInstanceProfile",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DisassociateIamInstanceProfile",
    "ec2:DescribeInstanceAttribute",
    "ec2:CreatePlacementGroup",
    "ec2>DeletePlacementGroup"
],
"Resource": "*"

```

```

    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
      ]
    }
  ]
}

```

### 3. 为 Cloud Volumes ONTAP 创建策略。

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

### 4. 如果您计划部署 Cloud Volumes ONTAP HA 对，请为 HA 调解器创建一个策略。

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }
]
}

```

5. 创建角色类型为 Amazon EC2 的 IAM 角色，并附加您在上述步骤中创建的策略。

与策略类似，您应该为 Connector 设置一个 IAM 角色，为 Cloud Volumes ONTAP 节点设置一个 IAM 角色，并为 HA 调解器设置一个 IAM 角色（如果要部署 HA 对）。

启动 Connector 实例时，必须选择 Connector IAM 角色。

在从 Cloud Manager 创建 Cloud Volumes ONTAP 工作环境时，您可以为 Cloud Volumes ONTAP 和 HA 调解器选择 IAM 角色。

## 设置 AWS KMS

如果要将 Amazon 加密与 Cloud Volumes ONTAP 结合使用，请确保满足 AWS 密钥管理服务的要求。

### 步骤

1. 确保您的帐户或其他 AWS 帐户中存在有效的客户主密钥（CMK）。

CMK 可以是 AWS 管理的 CMK 或客户管理的 CMK。

2. 如果 CMK 位于与您计划部署 Cloud Volumes ONTAP 的帐户不同的 AWS 帐户中，则需要获取该密钥的 ARN。

创建 Cloud Volumes ONTAP 系统时，您需要为 Cloud Manager 提供 ARN。

3. 将 Connector 实例的 IAM 角色添加到 CMK 的关键用户列表中。

这为 Cloud Manager 提供了将 CMK 与 Cloud Volumes ONTAP 配合使用的权限。



## 安装Connector并设置Cloud Manager

在 AWS 中启动 Cloud Volumes ONTAP 系统之前，您必须先从 AWS Marketplace 启动 Connector 实例，然后登录并设置 Cloud Manager。

### 步骤

1. 获取由证书颁发机构（CA）以隐私增强邮件（PEM）Base-64 编码 X.509 格式签名的根证书。有关获取证书的信息，请参见贵组织的策略和流程。

您需要在设置过程中上传证书。Cloud Manager 在通过 HTTPS 向 AWS 发送请求时使用可信证书。

2. 启动 Connector 实例：
  - a. 转到 Cloud Manager 的 AWS 智能社区市场页面。
  - b. 在自定义启动选项卡上，选择用于从 EC2 控制台启动实例的选项。
  - c. 按照提示配置实例。

配置实例时，请注意以下事项：

- 我们建议使用 T3.xlarge。
- 您必须选择在准备 AWS 环境时创建的 IAM 角色。
- 您应保留默认存储选项。
- 连接器所需的连接方法如下：SSH，HTTP 和 HTTPS。

3. 从连接到 Connector 实例的主机设置 Cloud Manager：
  - a. 打开 Web 浏览器并输入 `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>` 其中 `_ipaddress_` 是安装了连接器的 Linux 主机的 IP 地址。
  - b. 指定用于连接到 AWS 服务的代理服务器。
  - c. 上传您在步骤 1 中获得的证书。
  - d. 完成设置向导中的步骤以设置 Cloud Manager。
    - \* 系统详细信息 \*：输入此 Cloud Manager 实例的名称并提供您的公司名称。
    - \* 创建用户 \*：创建用于管理 Cloud Manager 的管理员用户。
    - \* 审核 \*：查看详细信息并批准最终用户许可协议。
  - e. 要完成 CA 签名证书的安装，请从 EC2 控制台重新启动 Connector 实例。
4. Connector 重新启动后，使用您在设置向导中创建的管理员用户帐户登录。

## 从Cloud Manager启动Cloud Volumes ONTAP

您可以通过在 Cloud Manager 中创建新的工作环境在 AWS 商用云服务环境中启动 Cloud Volumes ONTAP 实例。

### 您需要的内容

- 如果您购买了许可证，则必须具有从 NetApp 收到的许可证文件。此许可证文件是一个 .NLF 文件，采用 JSON 格式。
- 要为 HA 调解器启用基于密钥的 SSH 身份验证，需要使用密钥对。

## 步骤

1. 在工作环境页面上，单击 \* 添加工作环境 \*。
2. 在创建下，选择 Cloud Volumes ONTAP 或 Cloud Volumes ONTAP HA。
3. 完成向导中的步骤以启动 Cloud Volumes ONTAP 系统。

完成向导后，请注意以下事项：

- 如果要在多个可用性区域中部署 Cloud Volumes ONTAP HA，请按如下所示部署此配置，因为发布时 AWS 商用云服务环境中只有两个可用的 AZS：
  - 节点 1：可用性区域 A
  - 节点 2：可用性区域 B
  - 调解器：可用性区域 A 或 B
- 您应保留默认选项以使用生成的安全组。

预定义的安全组包含 Cloud Volumes ONTAP 成功运行所需的规则。如果您需要使用自己的，请参阅下面的安全组部分。

- 您必须选择在准备 AWS 环境时创建的 IAM 角色。
- 底层 AWS 磁盘类型适用于初始 Cloud Volumes ONTAP 卷。

您可以为后续卷选择不同的磁盘类型。

- AWS 磁盘的性能与磁盘大小相关。

您应选择可提供所需持续性能的磁盘大小。有关 EBS 性能的更多详细信息，请参见 AWS 文档。

- 磁盘大小是系统上所有磁盘的默认大小。



如果您稍后需要其他大小的磁盘，则可以使用高级分配选项创建使用特定大小磁盘的聚合。

- 存储效率功能可以提高存储利用率并减少所需的总存储量。

## 结果

Cloud Manager 将启动 Cloud Volumes ONTAP 实例。您可以跟踪时间链中的进度。

## 安全组规则

Cloud Manager 创建的安全组包含 Cloud Manager 和 Cloud Volumes ONTAP 在云中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安全组。

## Connector 的安全组

Connector 的安全组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

Connector 的预定义安全组包括以下出站规则。

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

## Cloud Volumes ONTAP 的安全组

Cloud Volumes ONTAP 节点的安全组需要入站和出站规则。

## 入站规则

在创建工作环境并选择预定义的安全组时、您可以选择允许以下其中一个范围内的流量：

- 仅选定**VPC**：入站流量的源是Cloud Volumes ONTAP 系统的VPC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IP范围为0.0.0.0/0。

协议	Port	目的
所有 ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP（通过 TCP）和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749-74	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

协议	Port	目的
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049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

### HA 调解器的外部安全组

Cloud Volumes ONTAP HA 调解器的预定义外部安全组包括以下入站和出站规则。

### 入站规则

入站规则的源是来自连接器所在 VPC 的流量。

协议	Port	目的
SSH	22.	SSH 与 HA 调解器的连接
TCP	3000	从 Connector 进行 RESTful API 访问

### 出站规则

HA 调解器的预定义安全组包括以下出站规则。

协议	Port	目的
所有 TCP	全部	所有出站流量

协议	Port	目的
所有UDP	全部	所有出站流量

#### HA 调解器的内部安全组

为 Cloud Volumes ONTAP HA 调解器预定义的内部安全组包括以下规则。Cloud Manager 始终会创建此安全组。您无法选择使用自己的。

#### 入站规则

预定义的安全组包括以下入站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

#### 出站规则

预定义的安全组包括以下出站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

## 开始使用 Microsoft Azure

### 在 Azure 中快速启动 Cloud Volumes ONTAP

只需几步即可开始使用适用于 Azure 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 Azure 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。"[了解更多信息。](#)"。

3

#### 设置网络

1. 确保您的 vNet 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
2. 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"](#)。



#### 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"](#)
- ["从 Azure Marketplace 创建 Connector"](#)
- ["在 Linux 主机上安装 Connector 软件"](#)
- ["BlueXP对权限执行的操作"](#)

### 在Azure中规划Cloud Volumes ONTAP 配置

在 Azure 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 Microsoft Azure 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VM类型

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

["支持 Azure 中 Cloud Volumes ONTAP 的配置"](#)

了解存储限制

Cloud Volumes ONTAP 系统的原始容量限制与许可证相关。附加限制会影响聚合和卷的大小。在规划配置时，您应该了解这些限制。

["Azure 中 Cloud Volumes ONTAP 的存储限制"](#)

在Azure中调整系统大小

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

## 虚拟机类型

在中查看支持的虚拟机类型 "[《 Cloud Volumes ONTAP 发行说明》](#)" 然后查看有关每个受支持 VM 类型的详细信息。请注意，每种 VM 类型都支持特定数量的数据磁盘。

- "[Azure 文档：通用虚拟机大小](#)"
- "[Azure 文档：内存优化的虚拟机大小](#)"

## 采用单节点系统的Azure磁盘类型

当您为 Cloud Volumes ONTAP 创建卷时、需要选择 Cloud Volumes ONTAP 用作磁盘的底层云存储。

单节点系统可以使用三种类型的 Azure 受管磁盘：

- **\_Premium SSD 受管磁盘\_** 以较高的成本为 I/O 密集型工作负载提供高性能。
- **标准 SSD 受管磁盘\_** 可为需要低 IOPS 的工作负载提供稳定一致的性能。
- 如果您不需要高 IOPS 并希望降低成本， **\_Standard HDD 受管磁盘\_** 是一个不错的选择。

有关这些磁盘的使用情形的其他详细信息，请参见 "[Microsoft Azure 文档： Azure 中提供了哪些磁盘类型?](#)"。

## 具有HA对的Azure磁盘类型

HA系统使用高级SSD共享受管磁盘、这两种磁盘均以较高的成本为I/O密集型工作负载提供高性能。9.12.1版之前创建的HA部署使用高级页面Blobs。

## Azure 磁盘大小

启动 Cloud Volumes ONTAP 实例时，必须为聚合选择默认磁盘大小。BlueXP会将此磁盘大小用于初始聚合、以及在使用简单配置选项时它创建的任何其他聚合。您可以创建使用与默认大小不同的磁盘大小的聚合 "[使用高级分配选项](#)"。



聚合中的所有磁盘大小必须相同。

选择磁盘大小时，应考虑多个因素。磁盘大小会影响您为存储支付的费用、可以在聚合中创建的卷大小、可用于 Cloud Volumes ONTAP 的总容量以及存储性能。

Azure 高级存储的性能取决于磁盘大小。更大的磁盘可提供更高的 IOPS 和吞吐量。例如，选择 1 TiB 磁盘可以提供比 500 GiB 磁盘更好的性能、而且成本更高。

标准存储的磁盘大小之间没有性能差异。应根据需要的容量选择磁盘大小。

有关按磁盘大小显示的 IOPS 和吞吐量，请参见 Azure：

- "[Microsoft Azure：受管磁盘定价](#)"
- "[Microsoft Azure：页面 Blob 定价](#)"

## 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。

"查看 Azure 中 Cloud Volumes ONTAP 系统数据的默认磁盘"。



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 Azure 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。

Azure 信息	您的价值
Region	
虚拟网络 (VNet)	
Subnet	
网络安全组 (如果使用您自己的组)	

## 选择写入速度

通过BlueXP、您可以为Cloud Volumes ONTAP 选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和<sup>建议</sup>。"[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<sup>您</sup>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。

## Azure 中的 Cloud Volumes ONTAP 的网络要求

设置 Azure 网络，以便 Cloud Volumes ONTAP 系统可以正常运行。

### Cloud Volumes ONTAP 的要求

在 Azure 中必须满足以下网络连接要求。



## 出站 Internet 访问

Cloud Volumes ONTAP 节点需要通过出站Internet访问NetApp AutoSupport、NetApp会主动监控系统运行状况并向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的安全组允许通过端口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 安全组允许通过端口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BlueXP通知您无法发送AutoSupport 消息、["对AutoSupport 配置进行故障排除"](#)。

## IP 地址

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



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。

## 单节点系统的 IP 地址

BlueXP会将5或6个IP地址分配给单节点系统：

- 集群管理IP
- 节点管理IP
- SnapMirror的集群间IP
- NFS/CIFS IP
- iSCSI IP



iSCSI IP可通过iSCSI协议提供客户端访问。系统也会将其用于其他重要的网络工作流。此LIF为必填项、不应删除。

- SVM管理(可选—默认情况下未配置)

## HA 对的 IP 地址

在部署期间、BlueXP会将IP地址分配给4个NIC (每个节点)。

请注意、BlueXP会在HA对上创建SVM管理LIF、但不会在Azure中的单节点系统上创建。

### NIC0

- 节点管理IP
- 集群间IP
- iSCSI IP



iSCSI IP可通过iSCSI协议提供客户端访问。系统也会将其用于其他重要的网络工作流。此LIF为必填项、不应删除。

- NIC 1\*
- 集群网络IP

### Ni2

- 集群互连IP (HA IC)
- NIC 3\*
- Pageblob NIC IP (磁盘访问)



NIC3仅适用于使用页面Blob存储的HA部署。

上述IP地址不会在发生故障转移事件时迁移。

此外、还配置了4个前端IP (FIPS)、以便在发生故障转移事件时进行迁移。这些前端IP位于负载均衡器中。

- 集群管理IP
- 节点A数据IP (NFS/CIFS)
- NodeB数据IP (NFS/CIFS)
- SVM管理IP

### 安全连接到 Azure 服务

默认情况下、BlueXP会为Cloud Volumes ONTAP 和Azure页面Blob存储帐户之间的连接启用Azure专用链接。

在大多数情况下、您无需执行任何操作—BlueXP为您管理Azure专用链路。但是，如果您使用 Azure 私有 DNS，则需要编辑配置文件。此外、您还应了解Azure中连接器位置的要求。

如果业务需要、您还可以禁用专用链路连接。如果禁用此链接、则BlueXP会将Cloud Volumes ONTAP 配置为使用服务端点。

["了解有关将Azure专用链路或服务端点与Cloud Volumes ONTAP 结合使用的更多信息"](#)。

连接到其他 ONTAP 系统

要在 Azure 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 Azure vNet 与其他网络(例如您的企业网络)之间建立 VPN 连接。

有关说明, 请参见 ["Microsoft Azure 文档: 在 Azure 门户中创建站点到站点连接"](#)。

用于 HA 互连的端口

Cloud Volumes ONTAP HA 对包括一个 HA 互连, 通过该互连, 每个节点可以持续检查其配对节点是否正常运行, 并镜像另一节点的非易失性内存的日志数据。HA 互连使用 TCP 端口 10006 进行通信。

默认情况下, HA 互连 LIF 之间的通信处于打开状态, 并且此端口没有安全组规则。但是, 如果在 HA 互连 LIF 之间创建防火墙, 则需要确保端口 10006 的 TCP 流量处于打开状态, 以便 HA 对可以正常运行。

一个 Azure 资源组中只有一个 HA 对

您必须为在 Azure 中部署的每个 Cloud Volumes ONTAP HA 对使用 `_dedicated` 资源组。一个资源组仅支持一个 HA 对。

如果您尝试在 Azure 资源组中部署第二个 Cloud Volumes ONTAP HA 对, 则 BlueXP 会遇到连接问题。

安全组规则

BlueXP 会创建包含 Cloud Volumes ONTAP 成功运行所需入站和出站规则的 Azure 安全组。您可能希望参考这些端口进行测试或使用自己的安全组。

Cloud Volumes ONTAP 的安全组需要入站和出站规则。



正在查找有关连接器的信息? ["查看 Connector 的安全组规则"](#)

单节点系统的入站规则

在创建工作环境并选择预定义的安全组时, 您可以选择允许以下其中一个范围内的流量:

- **\*仅选定 vNet\***: 入站流量的源是 Cloud Volumes ONTAP 系统的 vNet 子网范围以及 Connector 所在的 vNet 的子网范围。这是建议的选项。
- **所有 VNets\***: 入站流量的源为 0.0.0.0/0 IP 范围。

优先级和名称	端口和协议	源和目标	Description
1000 inbound_ssh	22. TCP	任意到任意	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
1001. inbound_http	80 TCP	任意到任意	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
第 Inbound_111_tcp	111. TCP	任意到任意	远程过程调用 NFS
1003. 入站_111_UDP	111. UDP	任意到任意	远程过程调用 NFS

优先级和名称	端口和协议	源和目标	Description
1004. Inbound_139	139. TCP	任意到任意	用于 CIFS 的 NetBIOS 服务会话
第以及第 Inbound_161-162_TCP	161-162. TCP	任意到任意	简单网络管理协议
1006. Inbound_161-162_UDP	161-162. UDP	任意到任意	简单网络管理协议
1007. Inbound_443	443 TCP	任意到任意	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
1008. Inbound_445	445 TCP	任意到任意	Microsoft SMB/CIFS over TCP (通过 TCP ) 和 NetBIOS 成帧
1009. Inbound_635_tcp	635 TCP	任意到任意	NFS 挂载
1010. 入站_635_UDP	635 UDP	任意到任意	NFS 挂载
1011. Inbound_749	749-74 TCP	任意到任意	Kerberos
1012. Inbound_2049_tcp	2049年 TCP	任意到任意	NFS 服务器守护进程
1013. 入站_2049_UDP	2049年 UDP	任意到任意	NFS 服务器守护进程
1014. Inbound_3260	3260 TCP	任意到任意	通过 iSCSI 数据 LIF 进行 iSCSI 访问
1015 Inbound_4045-4046_tcp	4045至4046 TCP	任意到任意	NFS 锁定守护进程和网络状态监控器
1016. 入站_4045-4046_UDP	4045至4046 UDP	任意到任意	NFS 锁定守护进程和网络状态监控器
1017. 入站_10000	10000 TCP	任意到任意	使用 NDMP 备份
1018. Inbound_11104-11105	11104-11105 TCP	任意到任意	SnapMirror 数据传输
3000 inbound_deny_all_tcp	任何端口 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001. inbound_deny_all_udp	任何端口 UDP	任意到任意	阻止所有其他UDP入站流量
65000 AllowVnetInBound	任何端口 任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量

优先级和名称	端口和协议	源和目标	Description
65001 AllowAzureLoad BalancerInBound	任何端口 任何协议	AzureLoadBalancer 到任 何	来自 Azure 标准负载均衡 器的数据流量
65500 DenyAllInBound	任何端口 任何协议	任意到任意	阻止所有其他入站流量

## HA 系统的入站规则

在创建工作环境并选择预定义的安全组时、您可以选择允许以下其中一个范围内的流量：

- **\*仅选定vNet\***：入站流量的源是Cloud Volumes ONTAP 系统的vNet子网范围以及Connector所在的vNet的子网范围。这是建议的选项。
- **所有VNets\***：入站流量的源为0.0.0.0/0 IP范围。



与单节点系统相比，HA 系统的入站规则更少，因为入站数据流量通过 Azure 标准负载均衡器。因此，来自负载均衡器的流量应处于打开状态，如 "AllowAzureLoadBalancerInBound" 规则中所示。

优先级和名称	端口和协议	源和目标	Description
100 Inbound_443	443 任何协议	任意到任意	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
101. Inbound_111_tcp	111. 任何协议	任意到任意	远程过程调用 NFS
102. Inbound_2049_tcp	2049年 任何协议	任意到任意	NFS 服务器守护进程
111. inbound_ssh	22. 任何协议	任意到任意	SSH 访问集群管理 LIF 或 节点管理 LIF 的 IP 地址
121. 入站_53	53. 任何协议	任意到任意	DNS 和 CIFS
65000 AllowVnetInBound	任何端口 任何协议	VirtualNetwork 到 VirtualNetwork	vNet 中的入站流量
65001 AllowAzureLoad BalancerInBound	任何端口 任何协议	AzureLoadBalancer 到任 何	来自 Azure 标准负载均衡 器的数据流量
65500 DenyAllInBound	任何端口 任何协议	任意到任意	阻止所有其他入站流量

## 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。

Port	协议	目的
全部	所有 TCP	所有出站流量
全部	所有UDP	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	Port	协议	源	目标	目的
Active Directory	88	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	137.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	138.	UDP	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	139.	TCP	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	389.	TCP 和 UDP	节点管理 LIF	Active Directory 目录林	LDAP
	445	TCP	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	464)	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	464)	UDP	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	749-74	TCP	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)
	88	TCP	数据 LIF (NFS, CIFS, iSCSI)	Active Directory 目录林	Kerberos V 身份验证
	137.	UDP	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 名称服务
	138.	UDP	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 数据报服务
	139.	TCP	数据 LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 服务会话
	389.	TCP 和 UDP	数据 LIF (NFS、CIFS)	Active Directory 目录林	LDAP
	445	TCP	数据 LIF (NFS、CIFS)	Active Directory 目录林	Microsoft SMB/CIFS over TCP (通过 TCP) 和 NetBIOS 成帧
	464)	TCP	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (set_change)
	464)	UDP	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos 密钥管理
	749-74	TCP	数据 LIF (NFS、CIFS)	Active Directory 目录林	Kerberos V 更改和设置密码 (RPCSEC_GSS)

服务	Port	协议	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
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。" <a href="#">了解配置备份文件</a> "。
DHCP	68	UDP	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	67	UDP	节点管理 LIF	DHCP	DHCP服务器
DNS	53.	UDP	节点管理 LIF 和数据 LIF ( NFS、CIFS )	DNS	DNS
NDMP	18600 – 18699	TCP	节点管理 LIF	目标服务器	NDMP 副本
SMTP	25.	TCP	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	161.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	161.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	TCP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	162.	UDP	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	11104.	TCP	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	11105.	TCP	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	514.	UDP	节点管理 LIF	系统日志服务器	系统日志转发消息

## 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](#)"
- "[Azure中的安全组规则](#)"

## 设置 Cloud Volumes ONTAP 以在 Azure 中使用客户管理的密钥

数据会使用在 Azure 中的 Cloud Volumes ONTAP 上自动加密 "[Azure 存储服务加密](#)" 使用 Microsoft 管理的密钥。但是，您可以按照此页面上的步骤使用自己的加密密钥。



## 数据加密概述

Cloud Volumes ONTAP 数据在 Azure 中使用自动加密 **"Azure 存储服务加密"**。默认实施使用 Microsoft 管理的密钥。无需设置。

如果要在 Cloud Volumes ONTAP 中使用客户管理的密钥，则需要完成以下步骤：

1. 从 Azure 创建密钥存储，然后在该存储中生成密钥
2. 在BlueXP中、使用API创建使用密钥的Cloud Volumes ONTAP 工作环境

## 密钥轮换

如果创建新版本的密钥， Cloud Volumes ONTAP 将自动使用最新版本的密钥。

## 如何对数据进行加密

创建配置为使用客户管理的密钥的 Cloud Volumes ONTAP 工作环境后， Cloud Volumes ONTAP 数据将按如下所示进行加密。

### Azure HA多可用性区域

- Cloud Volumes ONTAP 的所有Azure存储帐户均使用客户管理的密钥进行加密。<sup>1</sup>
- 对于根磁盘、启动磁盘、NVRAM磁盘、核心磁盘和数据磁盘、BlueXP使用磁盘加密集、通过该加密集可以管理具有受管磁盘的加密密钥。
- 任何新数据磁盘也会使用相同的磁盘加密集。

### Azure HA单一可用性区域

- Cloud Volumes ONTAP 的所有Azure存储帐户均使用客户管理的密钥进行加密。<sup>1</sup>
- 任何新存储帐户(例如、添加磁盘或聚合时)也会使用相同的密钥。<sup>1</sup>
- 从ONTAP 9.10.1P3开始、对于NVRAM和核心磁盘、BlueXP使用 **"磁盘加密集"**，用于管理具有受管磁盘的加密密钥。较低版本将使用Microsoft管理的密钥、而不是客户管理的密钥。

## 单个节点

- 适用于 Cloud Volumes ONTAP 的所有 Azure 存储帐户均使用客户管理的密钥进行加密。<sup>1</sup>
- 对于根磁盘、启动磁盘和数据磁盘、BlueXP使用 **"磁盘加密集"**，用于管理具有受管磁盘的加密密钥。
- 任何新数据磁盘也会使用相同的磁盘加密集。
- 从ONTAP 9.9.91P7开始、对于NVRAM和核心磁盘、BlueXP使用磁盘加密集、通过该加密集可以管理具有受管磁盘的加密密钥。较低版本将使用Microsoft管理的密钥、而不是客户管理的密钥。

## 脚注

1. 如果要在创建存储帐户期间对其进行加密、则必须在CVO创建请求中创建并提供资源的ID。这适用于所有类型的部署。如果您不提供此密钥、则存储帐户仍将加密、但BlueXP将首先使用Microsoft管理的密钥加密创建存储帐户、然后更新存储帐户以使用客户管理的密钥。

## 创建用户分配的受管身份

您可以选择创建一个称为用户分配的托管标识的资源。这样、您可以在创建Cloud Volumes ONTAP工作环境时对存储帐户进行加密。建议在创建密钥存储和生成密钥之前先创建此资源。

此资源的ID如下： `userassignedidentity`。

#### 步骤

1. 在Azure中、转到Azure服务并选择\*托管身份\*。
2. 单击 \* 创建 \*。
3. 请提供以下详细信息：
  - 订阅：选择订阅。我们建议选择与Connector订阅相同的订阅。
  - 资源组：使用现有资源组或创建新资源组。
  - 区域：(可选)选择与连接器相同的区域。
  - 名称：输入资源的名称。
4. (可选)添加标记。
5. 单击 \* 创建 \*。

#### 创建密钥存储并生成密钥

密钥存储必须位于您计划创建 Cloud Volumes ONTAP 系统的同一 Azure 订阅和区域中。

如果您 [已创建用户分配的受管身份](#)，创建密钥存储时，还应为密钥存储创建访问策略。

#### 步骤

1. ["在 Azure 订阅中创建密钥存储"](#)。

请注意密钥存储的以下要求：

- 密钥存储必须与 Cloud Volumes ONTAP 系统位于同一区域。
  - 应启用以下选项：
    - \* 软删除 \*（默认情况下，此选项处于启用状态，但必须禁用 *not*）
    - \* 清除保护 \*
    - 用于卷加密的**Azure**磁盘加密(适用于多个分区中的单节点系统或HA对)
  - 如果创建了用户分配的受管身份、则应启用以下选项：
    - 存储访问策略
2. 如果选择了存储访问策略、请单击创建为密钥存储创建访问策略。如果没有、请跳至步骤3。
    - a. 选择以下权限：
      - 获取
      - 列表
      - 解密
      - 加密
      - 取消换行键
      - 换行键

- 验证
- 签名

b. 选择用户分配的受管标识(资源)作为主体。

c. 查看并创建访问策略。

### 3. "在密钥存储中生成密钥"。

请注意此密钥的以下要求：

- 密钥类型必须为 \* RSA \*。
- 建议的 RSA 密钥大小为 \* 2048 \*，但支持其他大小。

## 创建一个使用加密密钥的工作环境

创建密钥存储并生成加密密钥后，您可以创建一个配置为使用此密钥的新 Cloud Volumes ONTAP 系统。使用 BlueXP API 可支持这些步骤。

### 所需权限

如果要在单节点 Cloud Volumes ONTAP 系统中使用客户管理的密钥，请确保 BlueXP Connector 具有以下权限：

```
"Microsoft.Compute/diskEncryptionSets/read",  
"Microsoft.Compute/diskEncryptionSets/write",  
"Microsoft.Compute/diskEncryptionSets/delete",  
"Microsoft.KeyVault/vaults/deploy/action",  
"Microsoft.KeyVault/vaults/read",  
"Microsoft.KeyVault/vaults/accessPolicies/write",  
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

### "查看最新的权限列表"

#### 步骤

1. 使用以下 BlueXP API 调用获取 Azure 订阅中的密钥存储列表。

对于 HA 对：GET /azure/ha/metadata/vaults

对于单个节点：GET /azure/vsa/metadata/vaults

记下 \* 名称 \* 和 \* 资源组 \*。您需要在下一步中指定这些值。

["了解有关此 API 调用的更多信息"](#)。

2. 使用以下 BlueXP API 调用获取存储中的密钥列表。

对于 HA 对：GET /azure/ha/metadata/keys-vault

对于单个节点：GET /azure/vsa/metadata/keys-vault

记下 \* 密钥名称 \*。您需要在下一步中指定该值（以及存储名称）。

["了解有关此 API 调用的更多信息"](#)。

### 3. 使用以下BlueXP API调用创建Cloud Volumes ONTAP 系统。

#### a. 对于 HA 对:

```
POST /azure/ha/working-environments
```

请求正文必须包含以下字段:

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```



包括 "userAssignedIdentity": " userAssignedIdentityId" 字段。

["了解有关此 API 调用的更多信息"](#)。

#### b. 对于单节点系统:

```
POST /azure/vsa/working-environments
```

请求正文必须包含以下字段:

```
"azureEncryptionParameters": {  
  "key": "keyName",  
  "vaultName": "vaultName"  
}
```



包括 "userAssignedIdentity": " userAssignedIdentityId" 字段。

["了解有关此 API 调用的更多信息"](#)。

## 结果

您有一个新的 Cloud Volumes ONTAP 系统，该系统配置为使用客户管理的密钥进行数据加密。

## 在Azure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Azure 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"。

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials  
Managed Service Identity

Azure Subscription  
OCCM Dev (Default)

Marketplace Subscription  
ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 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Azure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 Azure 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、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 Azure 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。

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials  
Managed Service Identity

Azure Subscription  
OCCM Dev (Default)

Marketplace Subscription  
ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. 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Azure中启动Cloud Volumes ONTAP 的分步说明"。

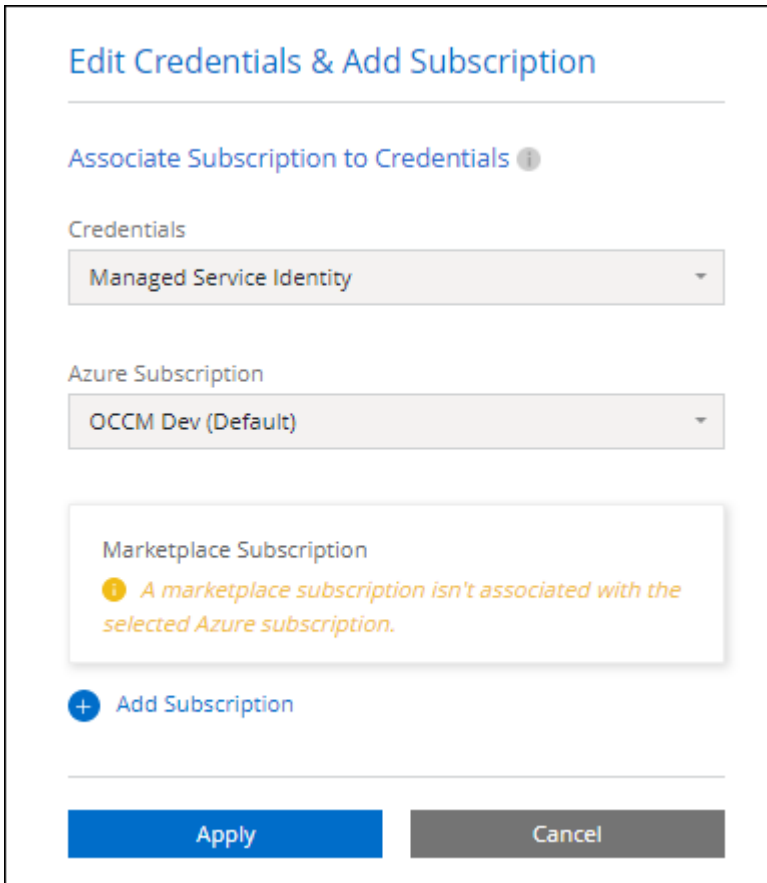
## PAYGO 订阅

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 Azure Marketplace 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 Azure Marketplace 中的按需购买服务。



**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- 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Azure中启动Cloud Volumes ONTAP 的分步说明"。



您可以从"设置">"凭据"页面管理与Azure帐户关联的Azure Marketplace订阅。 "了解如何管理Azure帐户和订阅"

#### 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Azure 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Azure 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>继续\*。
  - b. 在Azure门户中、选择与您的Azure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

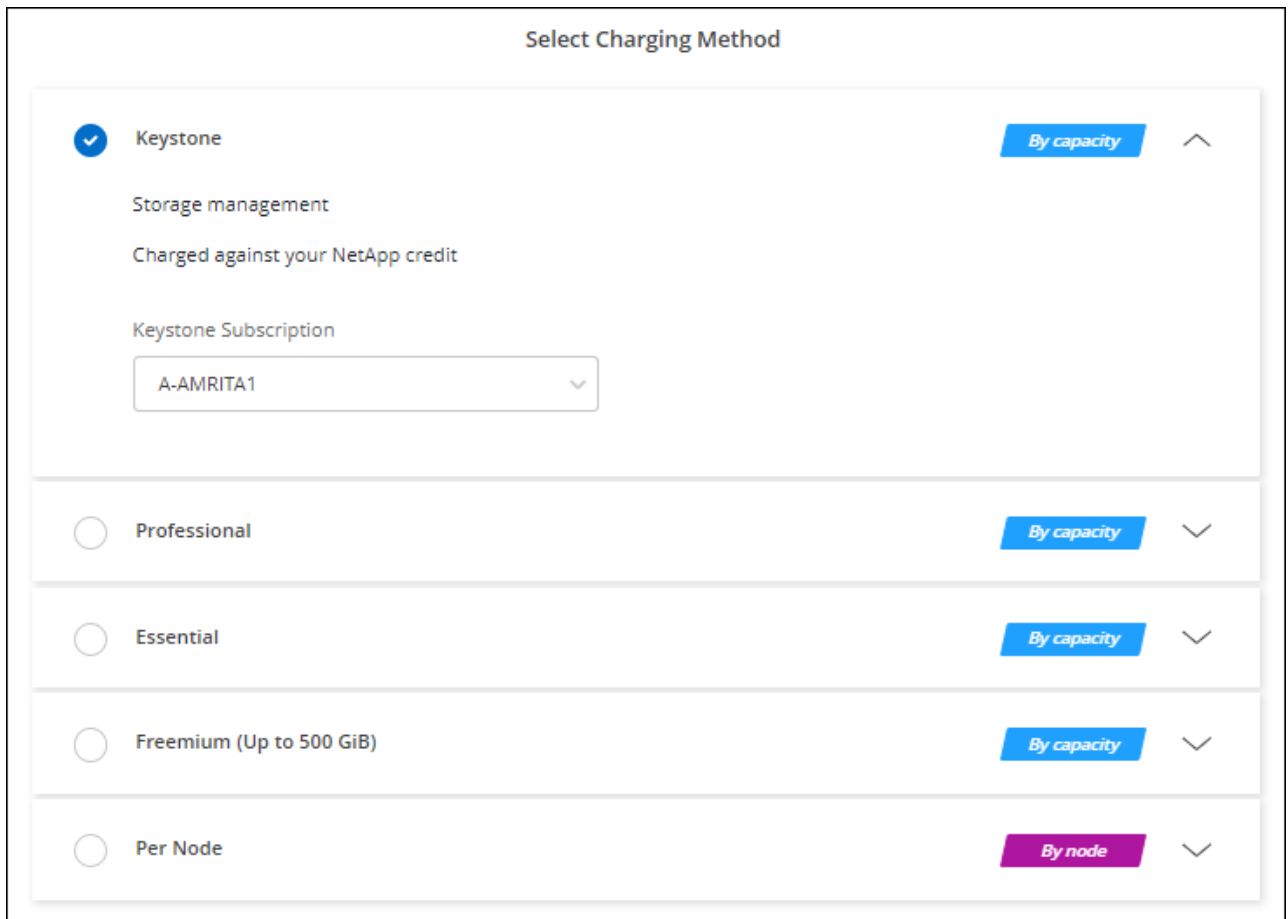
"查看在Azure中启动Cloud Volumes ONTAP 的分步说明"。

### 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。



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

## 在Azure中启用高可用性模式

应启用Microsoft Azure的高可用性模式、以缩短计划外故障转移时间并为Cloud Volumes ONTAP 启用NFSv4支持。

从Cloud Volumes ONTAP 9.10.1版开始、我们缩短了Microsoft Azure中运行的Cloud Volumes ONTAP HA对的计划外故障转移时间、并增加了对NFSv4的支持。要使这些增强功能可供Cloud Volumes ONTAP 使用、您需要在Azure订阅上启用高可用性功能。

如果需要在Azure订阅上启用此功能、BlueXP将在"需要操作"消息中提示您提供这些详细信息。

请注意以下事项：

- Cloud Volumes ONTAP HA 对的高可用性没有问题。此 Azure 功能可与 ONTAP 配合使用，以减少客户端观察到的 NFS 协议因计划外故障转移事件而发生的应用程序中断时间。
- 启用此功能不会对 Cloud Volumes ONTAP HA 对造成中断。
- 在 Azure 订阅上启用此功能不会将问题发生原因给其他 VM 。

拥有"所有者"权限的Azure用户可以从Azure命令行界面启用此功能。

步骤

### 1. "从Azure门户访问Azure Cloud Shell"

### 2. 注册高可用性模式功能:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

### 3. (可选)验证此功能现在是否已注册:

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure命令行界面应返回类似于以下内容的结果:

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

## 在 Azure 中启动 Cloud Volumes ONTAP

您可以通过在BlueXP中创建Cloud Volumes ONTAP 工作环境在Azure中启动单节点系统或HA对。

您需要的内容

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"](#)。
- 了解要使用的配置。

您已选择配置并从管理员处获取 Azure 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"](#)。

#### 关于此任务

当BlueXP在Azure中创建Cloud Volumes ONTAP 系统时、它会创建多个Azure对象、例如资源组、网络接口和存储帐户。您可以在向导结束时查看资源摘要。



可能会丢失数据

最佳做法是，为每个 Cloud Volumes ONTAP 系统使用一个新的专用资源组。

由于存在数据丢失的风险，建议不要在现有共享资源组中部署 Cloud Volumes ONTAP 。虽然在部署失败或删除时、BlueXP可以从共享资源组中删除Cloud Volumes ONTAP 资源、但Azure用户可能会意外从共享资源组中删除Cloud Volumes ONTAP 资源。

#### 在Azure中启动单节点Cloud Volumes ONTAP 系统

如果要在Azure中启动单节点Cloud Volumes ONTAP 系统、则需要在BlueXP中创建单节点工作环境。

#### 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. 选择位置：选择\* Microsoft Azure\*和\* Cloud Volumes ONTAP 单节点\*。
4. 如果出现提示， ["创建连接器"](#)。
5. \* 详细信息和凭据 \*：可选择更改 Azure 凭据和订阅，指定集群名称，根据需要添加标记，然后指定凭据。

下表介绍了可能需要指导的字段：

字段	Description
工作环境名称	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Azure虚拟机。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。
资源组标记	<p>标记是 Azure 资源的元数据。在此字段中输入标记后、BlueXP会将其添加到与Cloud Volumes ONTAP 系统关联的资源组中。</p> <p>在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。</p> <p>有关标记的信息，请参见 <a href="#">"Microsoft Azure 文档：使用标记组织 Azure 资源"</a>。</p>
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。
【视频】 编辑凭据	您可以选择不同的 Azure 凭据和不同的 Azure 订阅以用于此 Cloud Volumes ONTAP 系统。您需要将 Azure Marketplace 订阅与选定 Azure 订阅关联，才能部署按需购买的 Cloud Volumes ONTAP 系统。 <a href="#">"了解如何添加凭据"</a> 。

以下视频显示了如何将 Marketplace 订阅与 Azure 订阅关联：

► [https://docs.netapp.com/zh-cn/test//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/zh-cn/test//media/video_subscribing_azure.mp4) (video)

- \* 服务 \*：保持服务处于启用状态或禁用不想在 Cloud Volumes ONTAP 中使用的单个服务。
  - "了解有关BlueXP分类的更多信息"
  - "了解有关BlueXP备份和恢复的更多信息"



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。

- 位置：选择一个区域、可用性区域、vNet和子网、然后选中此复选框以确认连接器与目标位置之间的网络连接。

对于单节点系统，您可以选择要在其中部署 Cloud Volumes ONTAP 的可用性区域。如果不选择AZ、BlueXP将为您选择一个。

- 连接：选择一个新资源组或现有资源组、然后选择是使用预定义的安全组还是使用您自己的资源组。

下表介绍了可能需要指导的字段：

字段	Description
Resource Group	<p>为 Cloud Volumes ONTAP 创建新资源组或使用现有资源组。最佳实践是为 Cloud Volumes ONTAP 使用新的专用资源组。虽然可以在现有共享资源组中部署 Cloud Volumes ONTAP ，但由于存在数据丢失的风险，建议不要这样做。有关详细信息，请参见上述警告。</p> <p> 如果您正在使用的 Azure 帐户具有 "所需权限"、在部署失败或删除时、BlueXP会从资源组中删除Cloud Volumes ONTAP 资源。</p>
已生成安全组	<p>如果您让BlueXP为您生成安全组、则需要选择允许流量的方式：</p> <ul style="list-style-type: none"><li>• 如果选择*仅选定vNet*、则入站流量的源是选定vNet的子网范围以及Connector所在的vNet的子网范围。这是建议的选项。</li><li>• 如果选择*所有VNets*、则入站流量的源IP范围为0.0.0.0/0。</li></ul>
使用现有	<p>如果选择现有安全组，则该组必须满足 Cloud Volumes ONTAP 要求。"查看默认安全组"。</p>

- 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"。
- \* 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。

11. 许可：根据需要更改Cloud Volumes ONTAP 版本并选择虚拟机类型。



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。

12. \*订阅Azure Marketplace\*：如果BlueXP无法启用Cloud Volumes ONTAP 的编程部署、请按照以下步骤操作。
13. \*底层存储资源\*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用到 Blob 存储的数据分层。

请注意以下事项：

- 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 Azure 中估算系统规模](#)"。

- 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它。

["了解有关数据分层的更多信息。"](#)

14. 写入速度和**WORM**：

- a. 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。"](#)

- b. 根据需要激活一次写入、多次读取(WORM)存储。

此选项仅适用于某些VM类型。要了解支持的VM类型、请参见 "[HA对支持按许可证配置](#)"。

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。

15. \*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、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，<a href="#">"使用 IQN 从主机连接到 LUN"</a>。</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

16. \* 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）。



字段	Description
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 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，应在此字段中输入 * OU=ADDC Computers * 或 * OU=ADDC Users*。 <a href="#">"Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"</a>
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="#">"BlueXP 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。

17. \* 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"](#)。

18. \* 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\*以查看有关支持和BlueXP将购买的Azure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。

## 在Azure中启动Cloud Volumes ONTAP HA对

如果要在Azure中启动Cloud Volumes ONTAP HA对、则需要在BlueXP中创建HA工作环境。

### 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. 如果出现提示，"创建连接器"。
4. \*详细信息和凭据\*：可选择更改 Azure 凭据和订阅，指定集群名称，根据需要添加标记，然后指定凭据。

下表介绍了可能需要指导的字段：

字段	Description
工作环境名称	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Azure虚拟机。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。
资源组标记	标记是 Azure 资源的元数据。在此字段中输入标记后、BlueXP会将其添加到与Cloud Volumes ONTAP 系统关联的资源组中。  在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时，API 不会将您限制为四个标记。  有关标记的信息，请参见 " <a href="#">Microsoft Azure 文档：使用标记组织 Azure 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。
【视频】编辑凭据	您可以选择不同的 Azure 凭据和不同的 Azure 订阅以用于此 Cloud Volumes ONTAP 系统。您需要将 Azure Marketplace 订阅与选定 Azure 订阅关联，才能部署按需购买的 Cloud Volumes ONTAP 系统。" <a href="#">了解如何添加凭据</a> "。

以下视频显示了如何将 Marketplace 订阅与 Azure 订阅关联：

▶ [https://docs.netapp.com/zh-cn/test//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/zh-cn/test//media/video_subscribing_azure.mp4) (video)

5. \*服务\*：保持服务处于启用状态或禁用不想在 Cloud Volumes ONTAP 中使用的单个服务。
  - "[了解有关BlueXP分类的更多信息](#)"
  - "[了解有关BlueXP备份和恢复的更多信息](#)"



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：
  - a. 选择\*单个可用性区域\*或\*多个可用性区域\*。
  - b. 位置和连接(单个AZ)和\*区域和连接\*(多个AZs)
    - 对于单个AZ、请选择一个区域、vNet和子网。

- 对于多个AZs、请为节点1选择一个区域、vNet、子网、分区以及为节点2选择分区。

c. 选中\*我已验证网络连接...\*复选框。

7. 连接：选择一个新资源组或现有资源组、然后选择是使用预定义的安全组还是使用您自己的资源组。

下表介绍了可能需要指导的字段：

字段	Description
Resource Group	<p>为 Cloud Volumes ONTAP 创建新资源组或使用现有资源组。最佳实践是为 Cloud Volumes ONTAP 使用新的专用资源组。虽然可以在现有共享资源组中部署 Cloud Volumes ONTAP，但由于存在数据丢失的风险，建议不要这样做。有关详细信息，请参见上述警告。</p> <p>您必须为在 Azure 中部署的每个 Cloud Volumes ONTAP HA 对使用一个专用资源组。一个资源组仅支持一个 HA 对。如果您尝试在 Azure 资源组中部署第二个 Cloud Volumes ONTAP HA 对、则 BlueXP 会遇到连接问题。</p> <div style="display: flex; align-items: center;">  <p>如果您正在使用的 Azure 帐户具有 <b>"所需权限"</b>、在部署失败或删除时、BlueXP 会从资源组中删除 Cloud Volumes ONTAP 资源。</p> </div>
已生成安全组	<p>如果您让 BlueXP 为您生成安全组、则需要选择允许流量的方式：</p> <ul style="list-style-type: none"> <li>• 如果选择*仅选定vNet*、则入站流量的源是选定vNet的子网范围以及Connector所在的vNet的子网范围。这是建议的选项。</li> <li>• 如果选择*所有VNets*、则入站流量的源IP范围为0.0.0.0/0。</li> </ul>
使用现有	<p>如果选择现有安全组，则该组必须满足 Cloud Volumes ONTAP 要求。 <a href="#">"查看默认安全组"</a>。</p>

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\*更改配置\*。

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 版本并选择虚拟机类型。



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。

- \*订阅 Azure Marketplace\*：如果 BlueXP 无法启用 Cloud Volumes ONTAP 的编程部署、请按照以下步骤操作。
- \*底层存储资源\*：选择初始聚合的设置：磁盘类型，每个磁盘的大小以及是否应启用到 Blob 存储的数据分层。

请注意以下事项：

- 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。

有关选择磁盘大小的帮助、请参见 ["在Azure中调整系统大小"](#)。

- 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它。

["了解有关数据分层的更多信息。"](#)

### 13. 写入速度和**WORM**:

- 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。"](#)

- 根据需要激活一次写入、多次读取(WORM)存储。

此选项仅适用于某些VM类型。要了解支持的VM类型、请参见 ["HA对支持按许可证配置"](#)。

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。"](#)

- 如果激活了WORM存储、请选择保留期限。

### 14. 安全通信到存储和**WORM**: 选择是否启用与Azure存储帐户的HTTPS连接、并根据需要激活一次写入、多次读取(WORM)存储。

HTTPS连接从Cloud Volumes ONTAP 9.7 HA对连接到Azure页面Blob存储帐户。请注意，启用此选项可能会影响写入性能。创建工作环境后，您无法更改此设置。

["了解有关 WORM 存储的更多信息。"](#)

如果启用了数据分层，则无法启用 WORM。

["了解有关 WORM 存储的更多信息。"](#)

### 15. \* 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。

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

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

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory（AD）域的 FQDN。

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 Azure AD 域服务配置为 Cloud Volumes ONTAP 的 AD 服务器，应在此字段中输入 * OU=ADDC Computers * 或 * OU=ADDC Users* 。 <a href="#">"Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU) "</a>
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="#">"BlueXP 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。

17. \* 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"](#)。

18. \* 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\*以查看有关支持和BlueXP将购买的Azure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。



# 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

6

## 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。

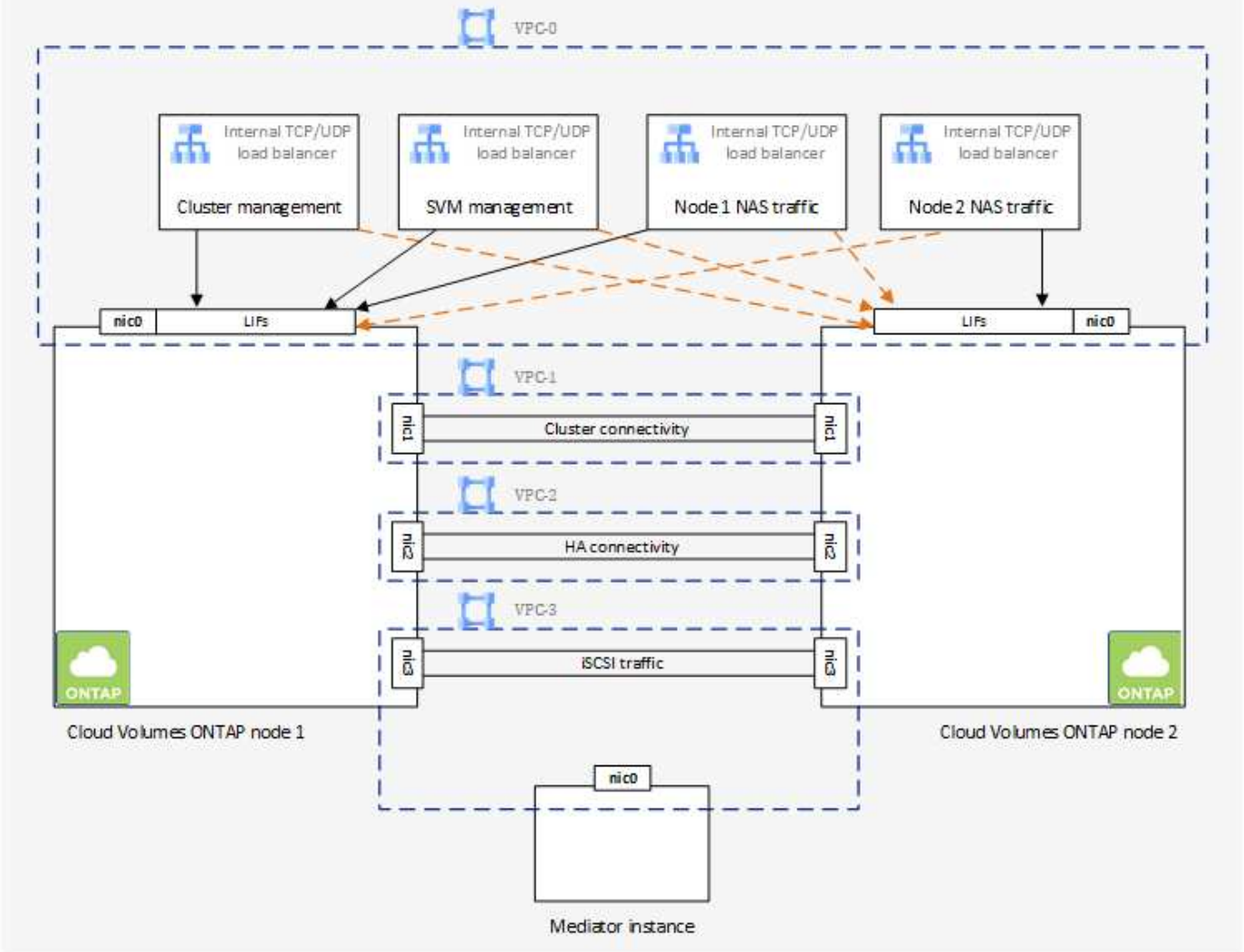
此部署模式确实可以降低成本，因为分区之间没有数据传出费用。

## 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 *14190056516*。

### 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。

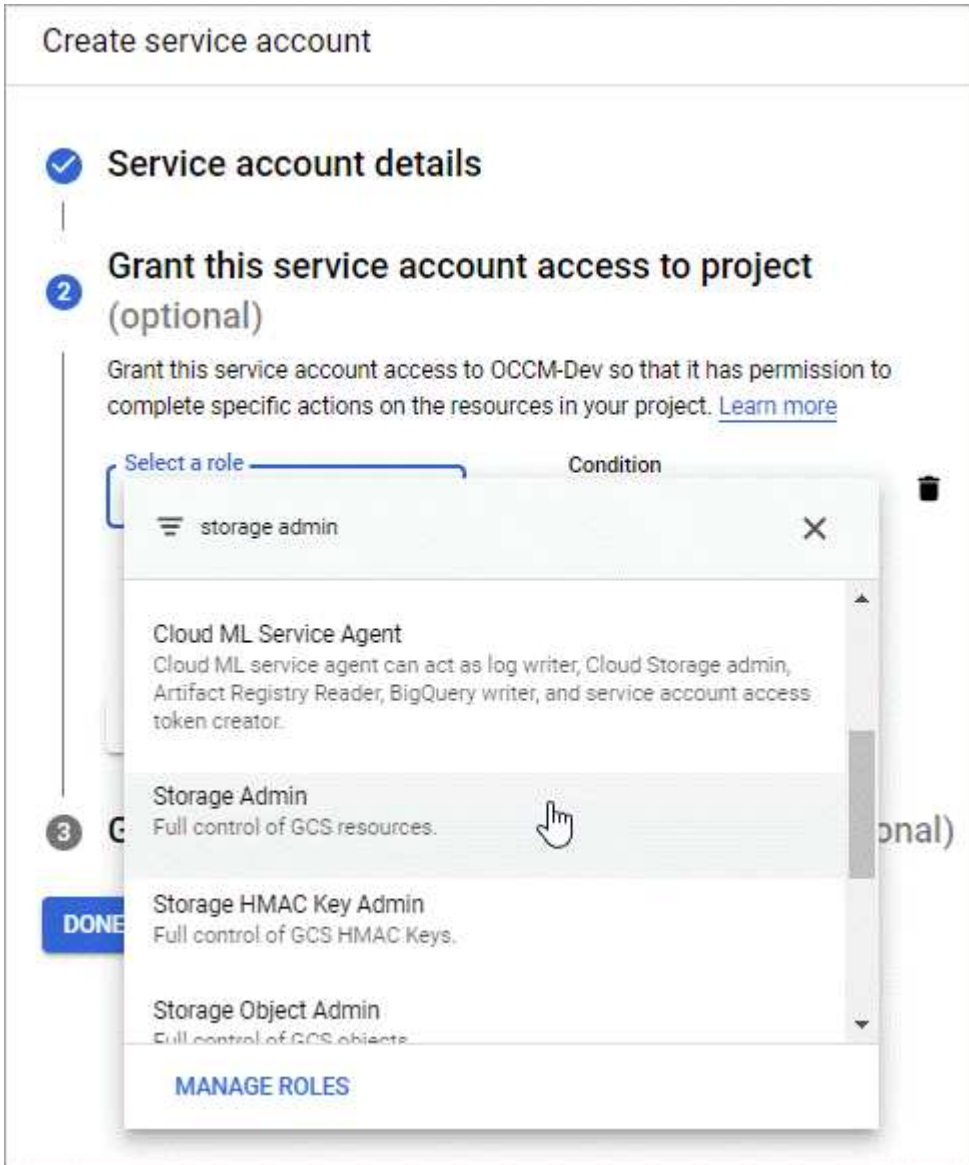
Cloud Volumes ONTAP 使用服务帐户访问和管理一个分层数据存储分段和另一个备份存储分段。

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

<b>default-project</b> Google Cloud Project	<b>gcp-sub2</b> Marketplace Subscription	<a href="#">Edit Project</a>
--	---	------------------------------

### 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、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"](#)

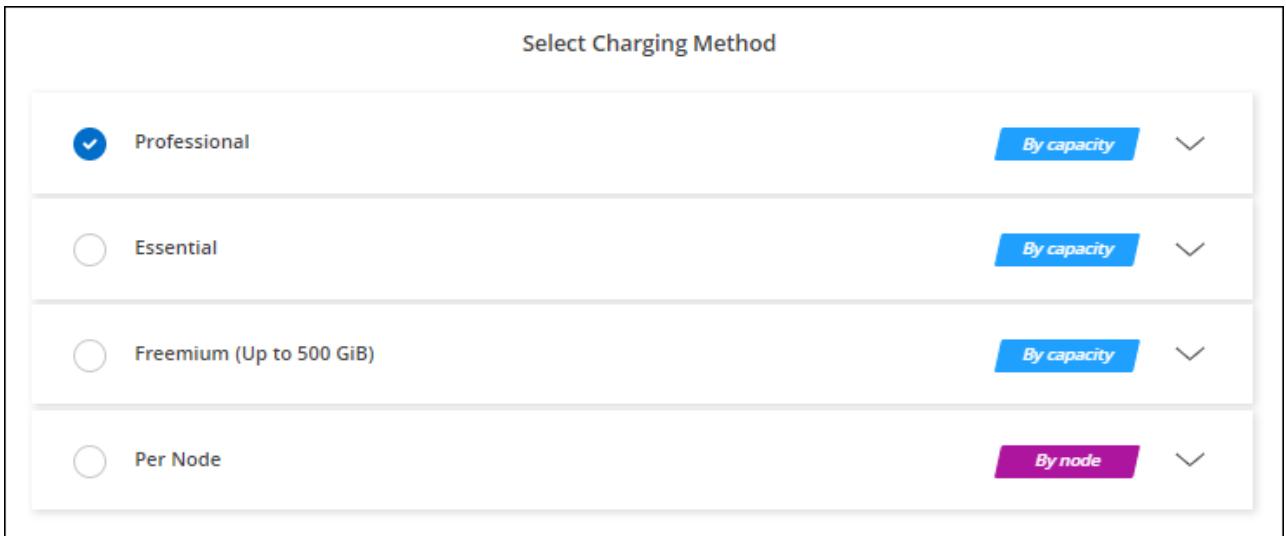
BlueXP会自动查询NetApp的许可服务、以获取与您的NetApp 支持站点 帐户关联的许可证的详细信息。如果没有错误、BlueXP会自动将许可证添加到电子钱包中。

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。



The screenshot shows a dialog box titled "Select Charging Method". It contains four rows, each with a radio button, a label, and a dropdown menu. The first row, "Professional", is selected (radio button is checked) and its dropdown menu is open, showing "By capacity". The second row, "Essential", has an unselected radio button and a dropdown menu showing "By capacity". The third row, "Freemium (Up to 500 GiB)", has an unselected radio button and a dropdown menu showing "By capacity". The fourth row, "Per Node", has an unselected radio button and a dropdown menu showing "By node".

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

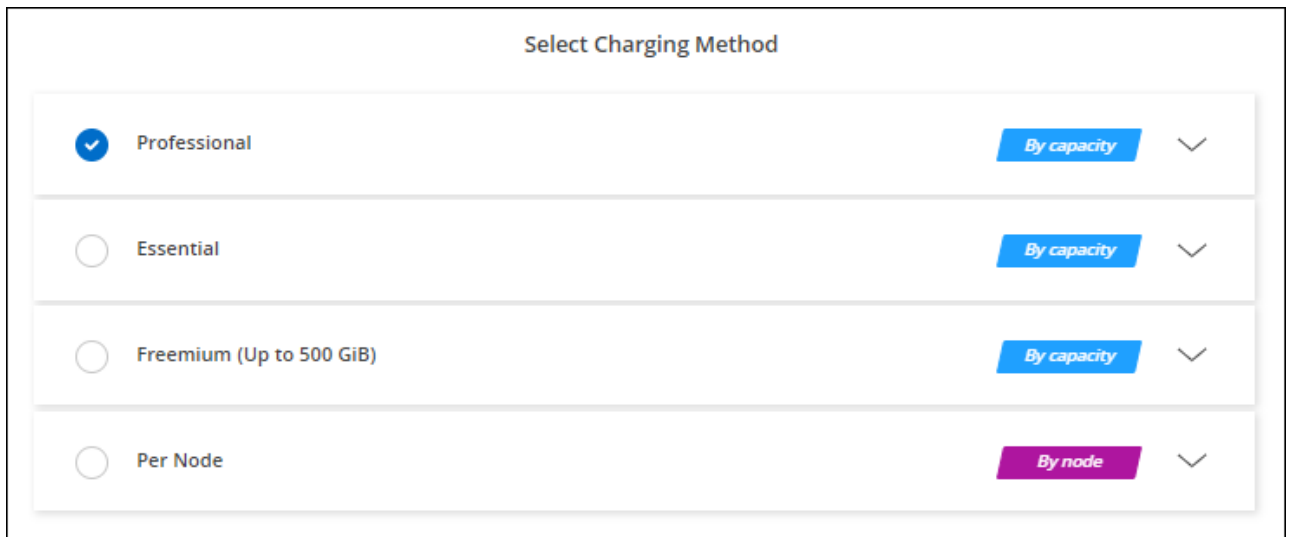
#### PAYGO订阅

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。



["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

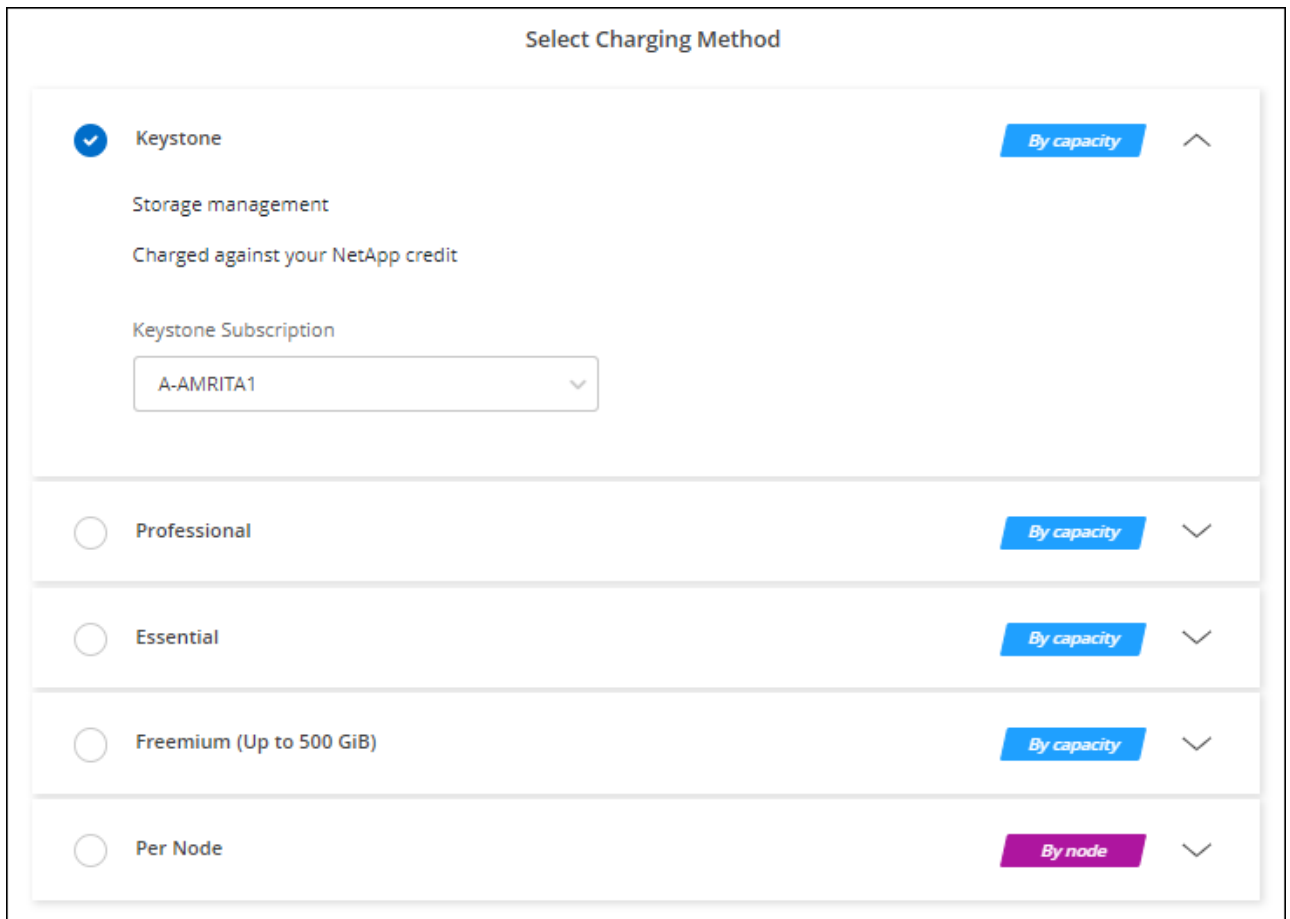
"查看在Google Cloud中启动Cloud Volumes ONTAP 的分步说明"。

### 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。



["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 <b>"数据分层"</b> 或 <b>"BlueXP备份和恢复"</b> 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。 <b>"了解如何创建服务帐户"</b> 。
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 <b>"Google Cloud 文档：标记资源"</b> 。
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、"<a href="#">如本页所述</a>"。</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](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 " <a href="#">Google Cloud 文档：配置私有 Google Access</a> "。
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"> <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。链接： <a href="https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules">https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules</a> [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，<a href="#">"使用 IQN 从主机连接到 LUN"</a>。</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><a href="#">"Google Cloud 文档: Google Managed Microsoft AD 中的组织单位"</a></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 <a href="#">"BlueXP 自动化文档"</a> 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 "<a href="#">Google Cloud 文档：标记资源</a>"。</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、"<a href="#">如本页所述</a>"。</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](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	<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"> <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	<p>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>。</p>

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* 。  <a href="#">"Google Cloud 文档： Google Managed Microsoft AD 中的组织单位"</a>
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="#">"BlueXP 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。

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/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c

```

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

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

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

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

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



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

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

## 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 workflow 摘要

下面简要介绍了Google Cloud签名映像验证 workflow 过程。

- 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 \[7.52 KB\]](#)

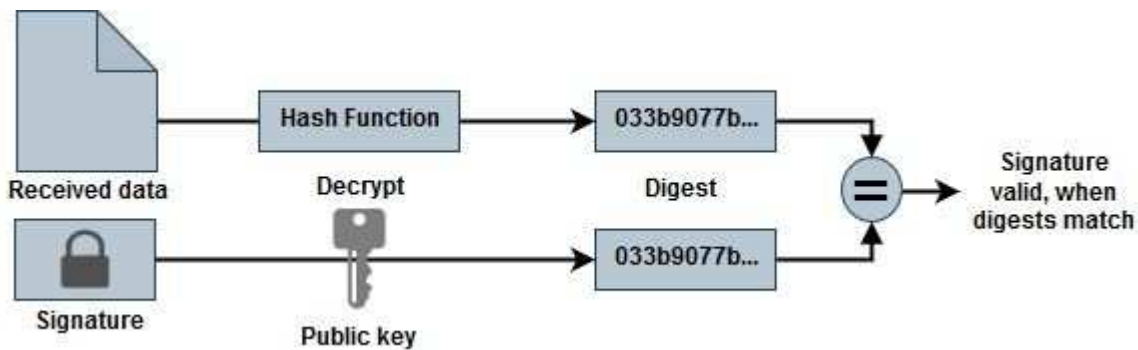
[View and download checksums](#)

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-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

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

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

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

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${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。