开始使用
Cloud Volumes ONTAP

NetApp
February 17, 2026

目录

开始使用

了解Cloud Volumes ONTAP

Cloud Volumes ONTAP使您能够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：

- 存储效率

  利用内置数据重复数据删除、数据压缩、精简配置和克隆来最大限度地降低存储成本。

- 高可用性

  确保云环境出现故障时企业的可靠性和持续运行。

- 数据保护

  Cloud Volumes ONTAP利用 NetApp 业界领先的复制技术SnapMirror将本地数据复制到云端，以便轻松获得可用于多种用例的辅助副本。

  Cloud Volumes ONTAP还与NetApp Backup and Recovery集成，提供备份和恢复功能，以保护和长期存档您的云数据。

  "了解有关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，无需使应用程序离线。

- 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

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

- 隐私合规控制

  与NetApp Data Classification集成可帮助您了解数据环境并识别敏感数据。

  "了解有关数据分类的更多信息"

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"

Cloud Volumes ONTAP部署支持的ONTAP版本

当您添加Cloud Volumes ONTAP系统时， NetApp Console可让您从多个不同的ONTAP版本中进行选择。

除此处列出的版本外，Cloud Volumes ONTAP 的其他版本不可用于新部署。此处版本中的修补程序或通用（通用可用性）版本表示可用于部署的基本版本。有关可用修补程序的详细信息，请参阅每个版本的 "版本化发行说明"。

有关升级的信息，请参阅 "支持的升级路径"。

AWS

单节点

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 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

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1

- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

单节点

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA 对

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

Google Cloud

单节点

- 9.18.1
- 9.17.1 P1

- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 对

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

开始使用 **Amazon Web Services**

AWS 中的**Cloud Volumes ONTAP**快速入门

只需几个步骤即可开始在 AWS 中使用Cloud Volumes ONTAP 。

1 创建控制台代理

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

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

2 规划您的配置

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

3 设置网络

1. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

   如果您在没有互联网访问的位置部署Cloud Volumes ONTAP，则不需要执行此步骤。
3. 设置 Amazon Simple Storage Service (Amazon S3) 服务的 VPC 端点。

   如果您想将冷数据从Cloud Volumes ONTAP到低成本对象存储，则需要 VPC 端点。

"了解有关网络要求的更多信息" 。

4 设置 **AWS KMS**

如果您想将 Amazon 加密与Cloud Volumes ONTAP结合使用，则需要确保存在有效的客户主密钥 (CMK)。您还需要通过添加以_密钥用户_身份向控制台代理提供权限的 IAM 角色来修改每个 CMK 的密钥策略。"了解更多" 。

5 使用控制台启动**Cloud Volumes ONTAP**

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

相关链接

- "为 AWS 创建控制台代理"
- "从 AWS Marketplace 创建控制台代理"
- "在本地安装并设置控制台代理"
- "控制台代理的 AWS 权限"

在 **AWS** 中规划您的**Cloud Volumes ONTAP**配置

在 AWS 中部署Cloud Volumes ONTAP时，您可以选择符合您的工作负载要求的预配置系

统，也可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。

选择**Cloud Volumes ONTAP**许可证

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

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

选择支持的区域

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

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。 "AWS 文档：了解如何启用区域" 。

选择受支持的本地区域

选择本地区域是可选的。包括新加坡在内的一些 AWS 本地区域支持Cloud Volumes ONTAP 。 AWS 中的Cloud Volumes ONTAP仅支持单个可用区域中的高可用性 (HA) 模式。不支持单节点部署。

> Cloud Volumes ONTAP不支持 AWS 本地区域中的数据分层和云分层。此外，不支持具有未符合Cloud Volumes ONTAP资格的实例的本地区域。例如迈阿密，它不能用作本地区域，因为它只有不受支持且不合格的 Gen6 实例。

"AWS 文档：查看本地区域的完整列表" 。必须先启用本地区域，然后才能在这些区域中创建和管理资源。

"AWS 文档：AWS 本地区域入门" 。

选择支持的实例

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Cloud Volumes ONTAP支持的配置"

了解存储限制

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

"AWS 中Cloud Volumes ONTAP的存储限制"

在 **AWS** 中调整系统大小

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

实例类型

- 将您的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，请选择具有足够 CPU 来管理请求的实例类型。

- 如果您有一个主要用于读取的应用程序，那么请选择具有足够 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

从高层次来看，EBS 磁盘类型之间的差异如下。要了解有关 EBS 磁盘用例的更多信息，请参阅 "AWS 文档：EBS 卷类型"。

- 通用 *SSD (gp3)* 磁盘是成本最低的 SSD，可在广泛的工作负载中平衡成本和性能。性能以 IOPS 和吞吐量来定义。Cloud Cloud Volumes ONTAP 9.7 及更高版本支持 gp3 磁盘。

  当您选择 gp3 磁盘时， NetApp Console会填写默认 IOPS 和吞吐量值，这些值根据所选磁盘大小提供与 gp2 磁盘相当的性能。您可以增加这些值以更高的成本获得更好的性能，但我们不支持较低的值，因为这会导致性能下降。简而言之，坚持默认值或增加默认值。不要降低它们。 "AWS 文档：了解有关 gp3 磁盘及其性能的更多信息" 。

  请注意， Cloud Volumes ONTAP支持带有 gp3 磁盘的 Amazon EBS Elastic Volumes 功能。"了解有关弹性卷支持的更多信息" 。

- 通用 *SSD (gp2)* 磁盘可在广泛的工作负载中平衡成本和性能。性能以 IOPS 来定义。
- *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支持带有 io1 磁盘的 Amazon EBS Elastic Volumes 功能。"了解有关弹性卷支持的更多信息" 。

- 吞吐量优化 *HDD (st1)* 磁盘适用于需要以较低价格实现快速、一致吞吐量的频繁访问的工作负载。

  如果您的 Cloud Volumes ONTAP 系统位于 AWS Local Zone 中，则不支持到 Amazon Simple Storage Service (Amazon S3) 的数据分层，因为在 Local Zone 之外访问 Amazon S3 存储桶涉及更高的延迟并影响 Cloud Volumes ONTAP 活动。

EBS 磁盘大小

如果您选择的配置不支持"Amazon EBS 弹性卷功能"，那么您需要在启动Cloud Volumes ONTAP系统时选择初始磁盘大小。之后，您可以"让控制台为您管理系统容量"，但如果你想"自己创建聚合"，请注意以下事项：

- 聚合中的所有磁盘必须具有相同的大小。
- EBS 磁盘的性能与磁盘大小相关。该大小决定了 SSD 磁盘的基线 IOPS 和最大突发持续时间以及 HDD 磁盘的基线和突发吞吐量。
- 最终，您应该选择能够提供您所需的_持续性能_的磁盘大小。
- 即使您确实选择了更大的磁盘（例如，六个 4 TiB 磁盘），您也可能无法获得所有的 IOPS，因为 EC2 实例可能会达到其带宽限制。

  有关 EBS 磁盘性能的更多详细信息，请参阅 "AWS 文档：EBS 卷类型"。

  如上所述，支持 Amazon EBS Elastic Volumes 功能的Cloud Volumes ONTAP配置不支持选择磁盘大小。"了解有关弹性卷支持的更多信息" 。

查看默认系统磁盘

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

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

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

准备在 **AWS Outpost** 中部署**Cloud Volumes ONTAP**

如果您有 AWS Outpost，则可以通过在部署过程中选择 Outpost VPC 在该 Outpost 中部署Cloud Volumes ONTAP 。体验与驻留在 AWS 中的任何其他 VPC 相同。请注意，您需要首先在 AWS Outpost 中部署控制台代理。

需要指出的是，存在一些限制：

- 目前仅支持单节点Cloud Volumes ONTAP系统
- 可与Cloud Volumes ONTAP一起使用的 EC2 实例仅限于 Outpost 中可用的实例
- 目前仅支持通用 SSD（gp2）

收集网络信息

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

单个可用区中的单个节点或 **HA** 对

AWS 信息	你的价值
地区	
VPC	
子网	
安全组（如果使用您自己的）	

多个可用区中的 **HA** 对

AWS 信息	你的价值
地区	
VPC	
安全组（如果使用您自己的）	
节点 1 可用区	
节点 1 子网	
节点 2 可用区	
节点 2 子网	

AWS 信息	你的价值
中介可用区域	
调解器子网	
中介者的密钥对	
集群管理网口浮动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

控制台使您能够选择Cloud Volumes ONTAP的写入速度设置。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息"。

选择卷使用情况配置文件

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

NetApp存储效率功能具有以下优势：

精简配置

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

重复数据删除

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

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

设置网络

为Cloud Volumes ONTAP设置 AWS 网络

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

一般要求

确保您已满足 AWS 中的以下要求。

Cloud Volumes ONTAP节点的出站互联网访问

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

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

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	端点不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。
AWS 服务的确切商业端点（后缀为 `amazonaws.com`）取决于您使用的 AWS 区域。请参阅 "AWS 文档了解详细信息"。	• 云形成 • 弹性计算云（EC2） • 身份和访问管理 (IAM) • 密钥管理服务（KMS） • 安全令牌服务 (STS) • Amazon Simple Storage Service (S3)	与 AWS 服务通信。	标准和私人模式。	Cloud Volumes ONTAP无法与 AWS 服务通信以在 AWS 中执行特定操作。

端点	适用于	目的	部署模式	端点不可用时的影响
AWS 服务的具体政府端点取决于您使用的 AWS 区域。端点后缀为 `amazonaws.com` 和 `c2s.ic.gov`。参考 "AWS 开发工具包"和 "AWS 文档"了解更多信息。	• 云形成 • 弹性计算云（EC2） • 身份和访问管理(IAM) • 密钥管理服务（KMS） • 安全令牌服务(STS) • 简单存储服务（S3）	与 AWS 服务通信。	限制模式。	Cloud Volumes ONTAP无法与 AWS 服务通信以在 AWS 中执行特定操作。

HA 中介器的出站互联网访问

HA 中介实例必须具有与 AWS EC2 服务的出站连接，以便它可以协助存储故障转移。为了提供连接，您可以添加公共 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 终端节点的详细信息，请参阅 "AWS 文档：接口 VPC 终端节点 (AWS PrivateLink)"。

NetApp Console代理的网络代理配置

您可以使用NetApp Console代理的代理服务器配置来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

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

有关配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

私有 **IP** 地址

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

Console 为 Cloud Volumes ONTAP 分配的 LIF 数量取决于您是部署单节点系统还是 HA 对。LIF 是与物理端口关联的 IP 地址。

单节点系统的 **IP** 地址

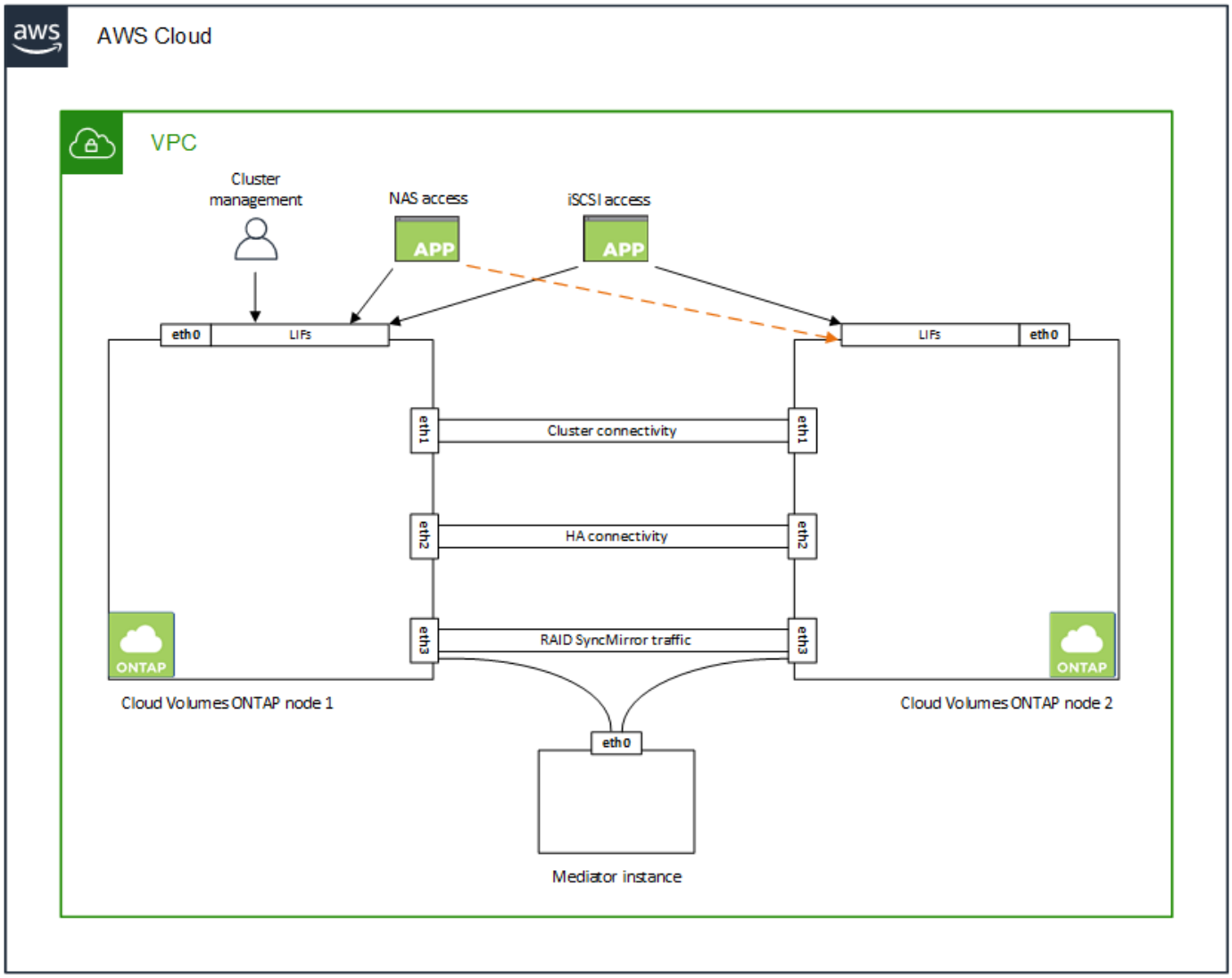
Console 为单节点系统分配 6 个 IP 地址。

下表提供了与每个私有 IP 地址关联的 LIF 的详细信息。

LIF	目的
集群管理	整个集群（HA 对）的行政管理。
节点管理	节点的行政管理。
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。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。
存储虚拟机管理	存储虚拟机管理 LIF 与SnapCenter等管理工具一起使用。

HA 对的 **IP** 地址

HA 对比单节点系统需要更多的 IP 地址。这些 IP 地址分布在不同的以太网接口上，如下图所示：



HA 对所需的私有 IP 地址数量取决于您选择的部署模型。在单个 AWS 可用区 (AZ) 中部署的 HA 对需要 15 个私有 IP 地址，而在多个 AZ 中部署的 HA 对需要 13 个私有 IP 地址。

下表提供了与每个私有 IP 地址关联的 LIF 的详细信息。

LIF	接口	节点	目的
集群管理	eth0	节点 1	整个集群（HA 对）的行政管理。
节点管理	eth0	节点 1 和节点 2	节点的行政管理。
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。
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。系统还将其用于其他重要的网络工作流程。这些 LIF 是必需的，不应删除。
集群连接	eth1	节点 1 和节点 2	使节点能够相互通信并在集群内移动数据。
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节点和中介之间的通信。
调解器	eth0	调解器	节点和中介之间的通信通道，用于协助存储接管和归还过程。

LIF	接口	节点	目的
节点管理	eth0	节点 1 和节点 2	节点的行政管理。
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	使节点能够相互通信并在集群内移动数据。
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节点和中介之间的通信。
调解器	eth0	调解器	节点和中介之间的通信通道，用于协助存储接管和归还过程。

当部署在多个可用区时，多个 LIF 与"浮动IP地址"，这不计入 AWS 私有 IP 限制。

安全组

您不需要创建安全组，因为控制台会为您完成此操作。如果您需要使用自己的，请参阅"安全组规则"。

正在寻找有关控制台代理的信息？ "查看控制台代理的安全组规则"

数据分层连接

如果要将 EBS 作为性能层，将 Amazon S3 作为容量层，则必须确保 Cloud Volumes ONTAP 具有到 S3 的连接。提供此连接的最佳方法是创建到 S3 服务的 VPC 端点。有关说明，请参阅 "AWS 文档：创建网关终端节点"。

创建 VPC 端点时，请确保选择与Cloud Volumes ONTAP实例相对应的区域、VPC 和路由表。您还必须修改安全组以添加允许流量到 S3 端点的出站 HTTPS 规则。否则， Cloud Volumes ONTAP无法连接到 S3 服务。

如果您遇到任何问题，请参阅 "AWS Support 知识中心：为什么我无法使用网关 VPC 终端节点连接到 S3 存储桶？"

与**ONTAP**系统的连接

要在 AWS 中的Cloud Volumes ONTAP系统和其他网络中的ONTAP系统之间复制数据，您必须在 AWS VPC 和其他网络（例如您的公司网络）之间建立 VPN 连接。有关说明，请参阅 "AWS 文档：设置 AWS VPN 连接"。

CIFS 的 **DNS** 和 **Active Directory**

如果您想要配置 CIFS 存储，则必须在 AWS 中设置 DNS 和 Active Directory，或者将您的本地设置扩展到 AWS。

DNS 服务器必须为 Active Directory 环境提供名称解析服务。您可以配置 DHCP 选项集以使用默认 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，请参阅 "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 版本开始，AWS 通过 VPC 共享支持Cloud Volumes ONTAP HA 对。 VPC 共享使您的组织能够与其他 AWS 账户共享子网。要使用此配置，您必须设置您的 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" 。

多可用区中 **HA** 对的要求

其他 AWS 网络要求适用于使用多个可用区 (AZ) 的Cloud Volumes ONTAP HA 配置。在启动 HA 对之前，您应该查看这些要求，因为在添加Cloud Volumes ONTAP系统时必须在控制台中输入网络详细信息。

要了解 HA 对的工作原理，请参阅"高可用性对"。

可用区域

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实例和中介实例使用专用 AZ，这为 HA 对之间提供了通信通道。

每个可用区都应该有一个子网。

用于 **NAS** 数据和集群/**SVM** 管理的浮动 **IP** 地址

多个可用区中的 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。它们无法从 VPC 外部本机访问，除非您"设置 AWS 中转网关"。

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

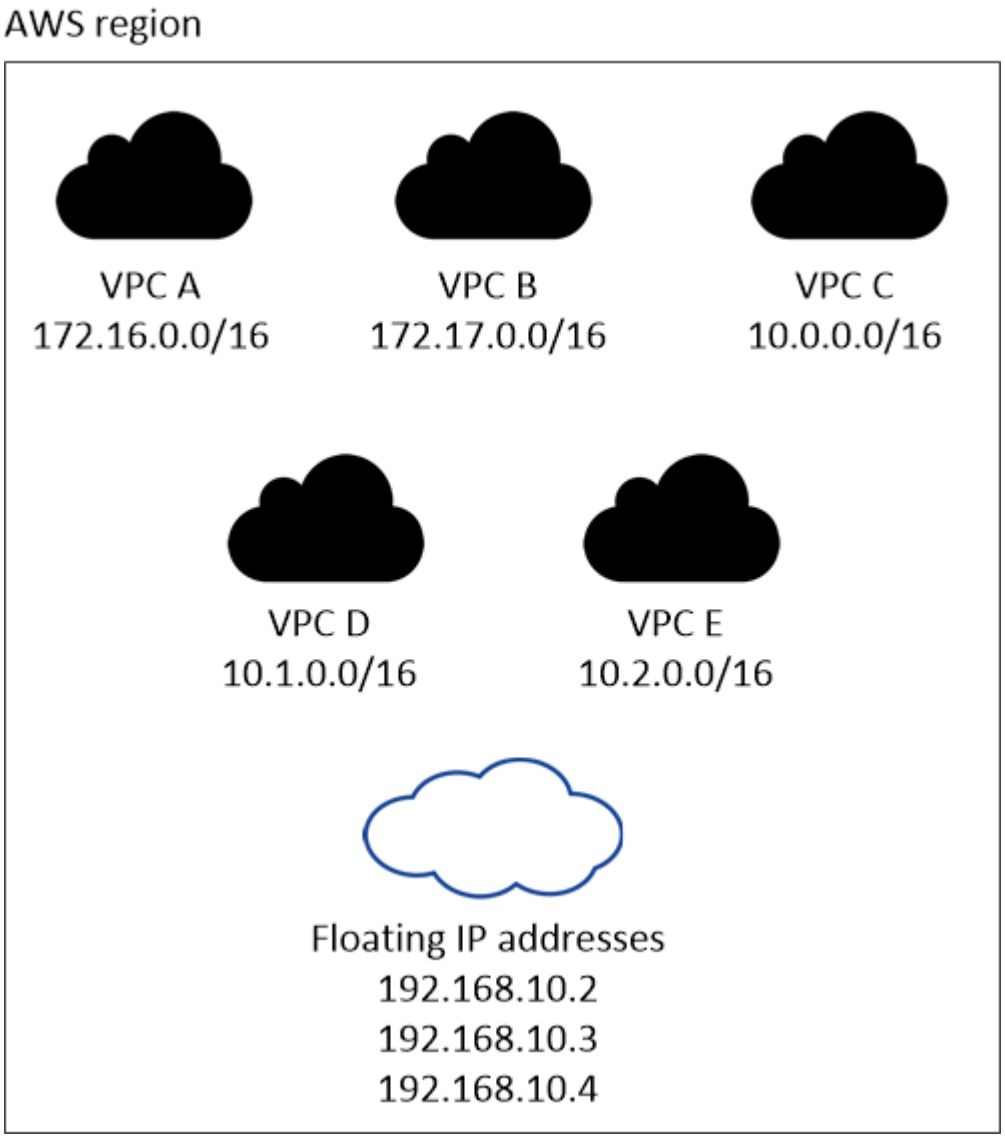
据。用于 SVM 管理的第四个浮动 IP 地址是可选的。

如果您将SnapDrive for Windows 或SnapCenter与 HA 对一起使用，则 SVM 管理 LIF 需要浮动 IP 地址。

添加Cloud Volumes ONTAP HA 系统时，需要输入浮动 IP 地址。控制台在启动系统时将 IP 地址分配给 HA 对。

浮动 IP 地址必须位于您部署 HA 配置的 AWS 区域中的所有 VPC 的 CIDR 块之外。将浮动 IP 地址视为您所在区域的 VPC 之外的逻辑子网。

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



控制台会自动创建静态 IP 地址，用于 iSCSI 访问和来自 VPC 外部客户端的 NAS 访问。您不需要满足这些类型的 IP 地址的任何要求。

中转网关，用于从 **VPC** 外部启用浮动 **IP** 访问

如果需要的话，"设置 AWS 中转网关"允许从 HA 对所在的 VPC 外部访问 HA 对的浮动 IP 地址。

路由表

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。这使得客户端可以访问 HA 对。

如果您的 VPC 中的子网只有一个路由表（主路由表），则控制台会自动将浮动 IP 地址添加到该路由表。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，您可能有两个与不同路由表关联的子网。如果您选择路由表 A，而不是路由表 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则不能访问。

有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

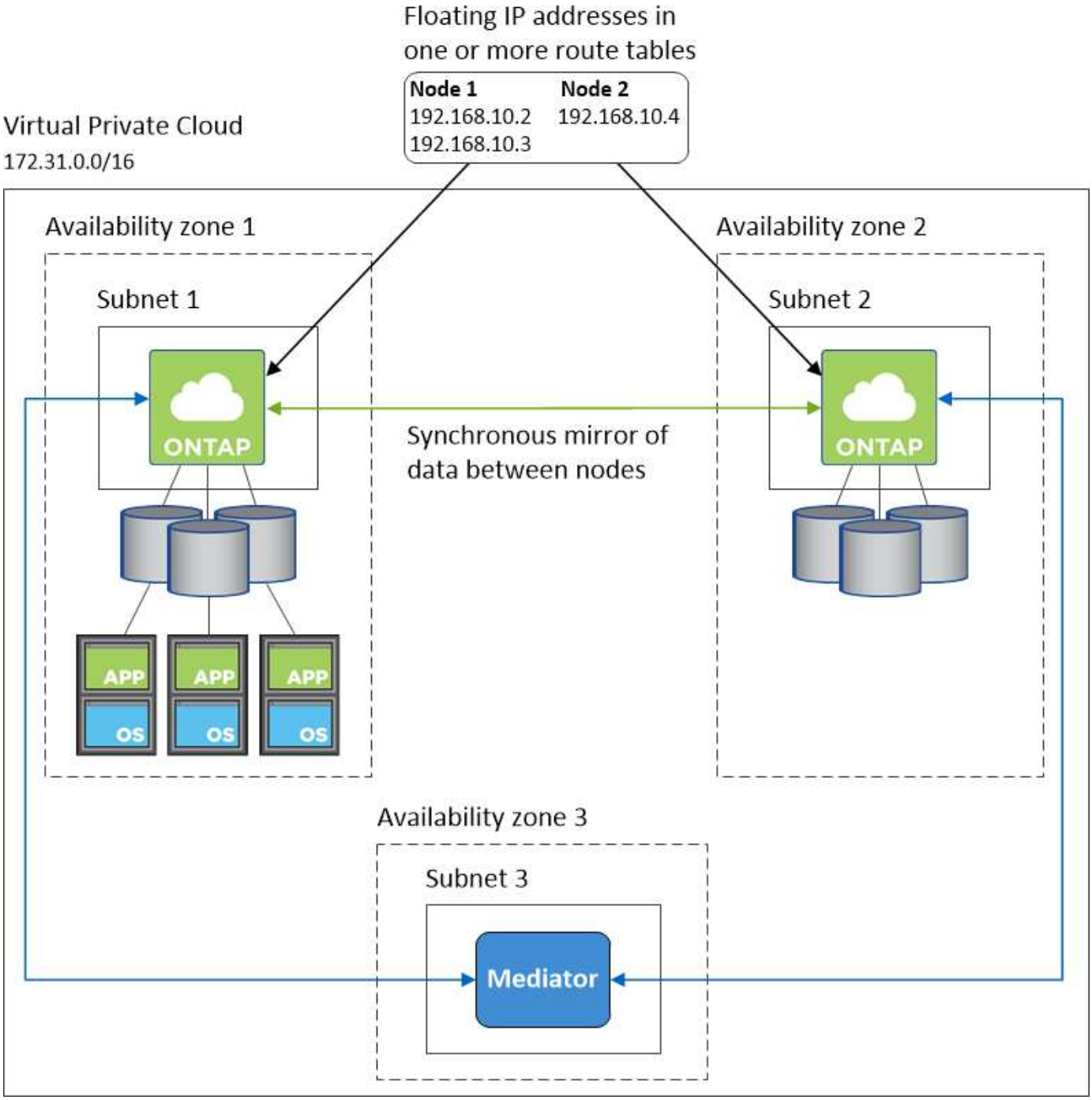
连接到**NetApp**管理工具

要将NetApp管理工具与多个 AZ 中的 HA 配置一起使用，您有两种连接选项：

1. 在不同的 VPC 中部署NetApp管理工具，并"设置 AWS 中转网关"。网关允许从 VPC 外部访问集群管理接口的浮动 IP 地址。
2. 在同一 VPC 中部署NetApp管理工具，并使用与 NAS 客户端类似的路由配置。

HA 配置示例

下图说明了多个可用区中的 HA 对特有的网络组件：三个可用区、三个子网、浮动 IP 地址和一个路由表。



控制台代理的要求

如果您尚未创建控制台代理，则应查看网络要求。

- "查看控制台代理的网络要求"
- "AWS 中的安全组规则"

相关主题

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

为**Cloud Volumes ONTAP HA** 对设置 **AWS** 传输网关

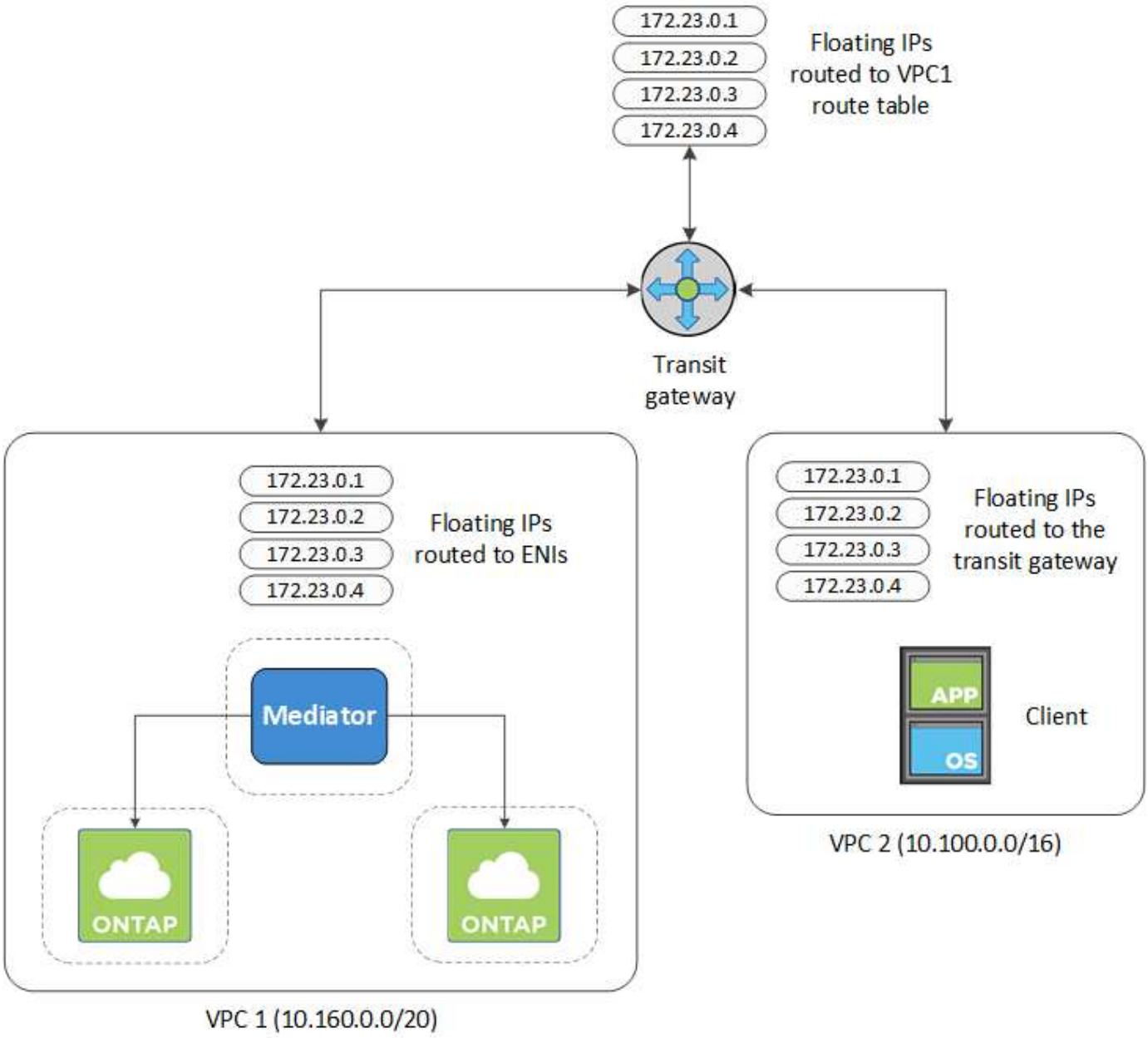
设置 AWS 中转网关以允许访问 HA 对的"浮动IP地址"来自 HA 对所在的 VPC 外部。

当Cloud Volumes ONTAP HA 配置分布在多个 AWS 可用区时，需要浮动 IP 地址才能从 VPC 内部访问 NAS 数据。当发生故障时，这些浮动 IP 地址可以在节点之间迁移，但无法从 VPC 外部进行本机访问。单独的私有 IP 地址提供从 VPC 外部的数据访问，但它们不提供自动故障转移。

集群管理接口和可选的 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 之外的 NAS 客户端和NetApp管理工具可以访问浮动 IP。

下面是一个显示通过中转网关连接的两个 VPC 的示例。 HA 系统位于一个 VPC 中，而客户端位于另一个 VPC 中。然后，您可以使用浮动 IP 地址在客户端上安装 NAS 卷。

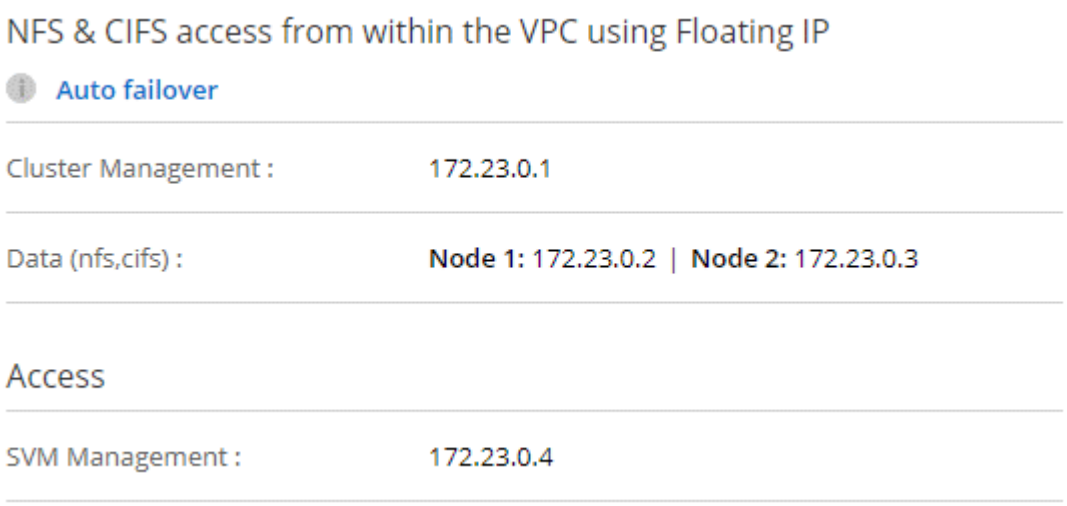


以下步骤说明如何设置类似的配置。

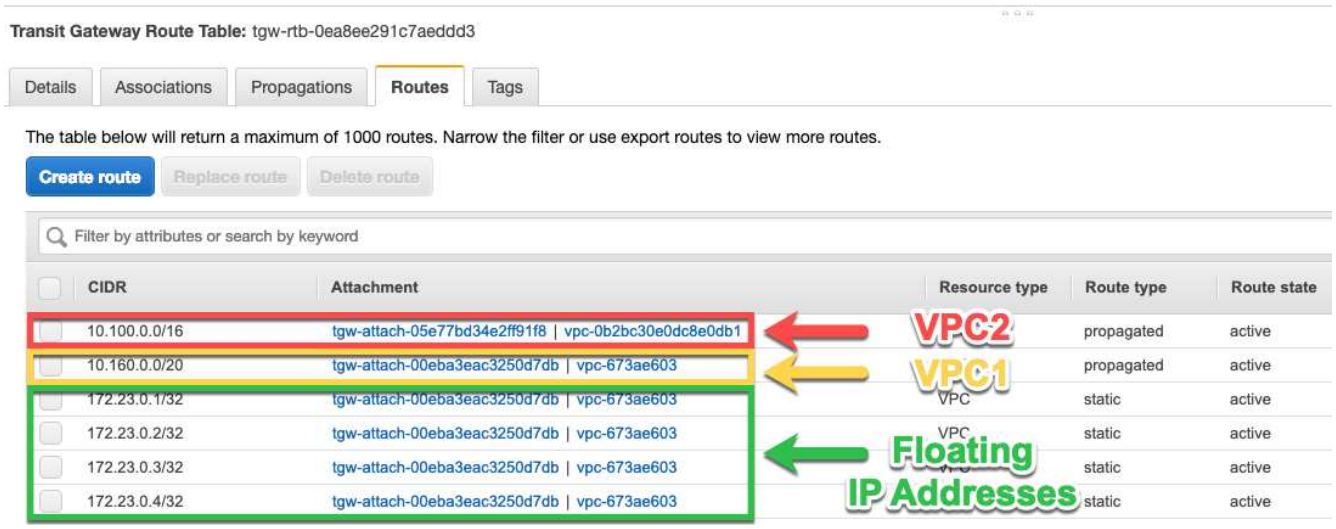
步骤

1. "创建中转网关并将 VPC 附加到该网关" 。
2. 将 VPC 与传输网关路由表关联。
   a. 在 **VPC** 服务中，单击 **Transit Gateway Route Tables**。
   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NetApp Console的系统信息页面上找到浮动 IP 地址。以下是一个例子：



   以下示例图显示了中转网关的路由表。它包括到两个 VPC 的 CIDR 块的路由和Cloud Volumes ONTAP使用的四个浮动 IP 地址。

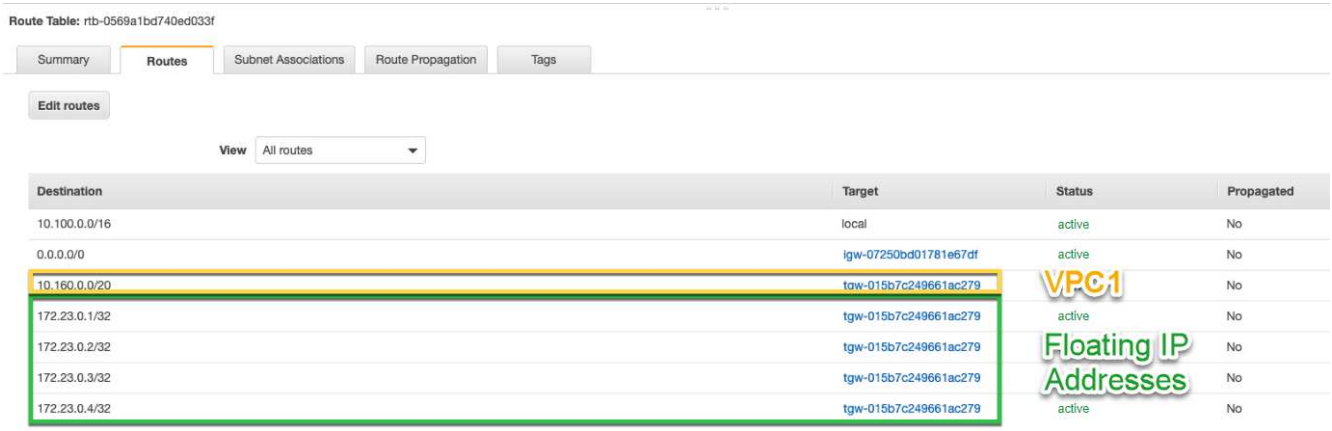


4. 修改需要访问浮动IP地址的VPC的路由表。

a. 为浮动IP地址添加路由条目。

b. 将路由条目添加到 HA 对所在 VPC 的 CIDR 块。

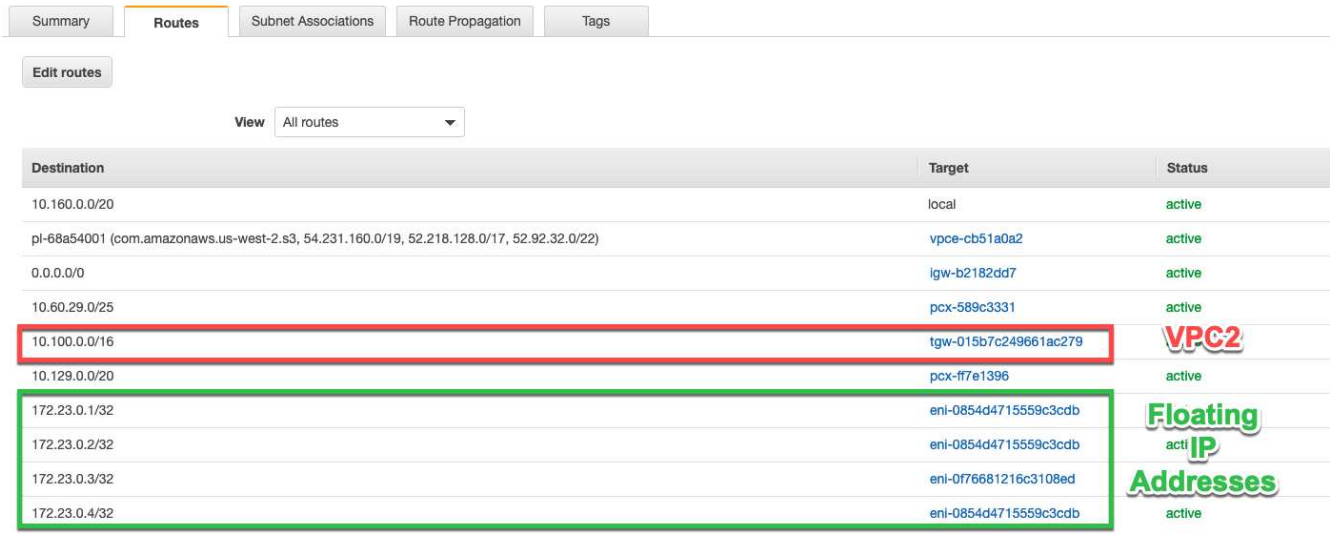
下面的示例图显示了 VPC 2 的路由表，其中包括到 VPC 1 的路由和浮动 IP 地址。



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。

这一步很重要，因为它完成了 VPC 之间的路由。

以下示例图像显示了 VPC 1 的路由表。它包括到浮动 IP 地址和客户端所在的 VPC 2 的路由。控制台在部署 HA 对时会自动将浮动 IP 添加到路由表中。



6. 将安全组设置更新为 VPC 的所有流量。

a. 在虚拟私有云下，单击*子网*。

b. 单击“路由表”选项卡，为 HA 对的其中一个浮动 IP 地址选择所需的环境。

c. 单击“安全组”。

d. 选择*编辑入站规则*。

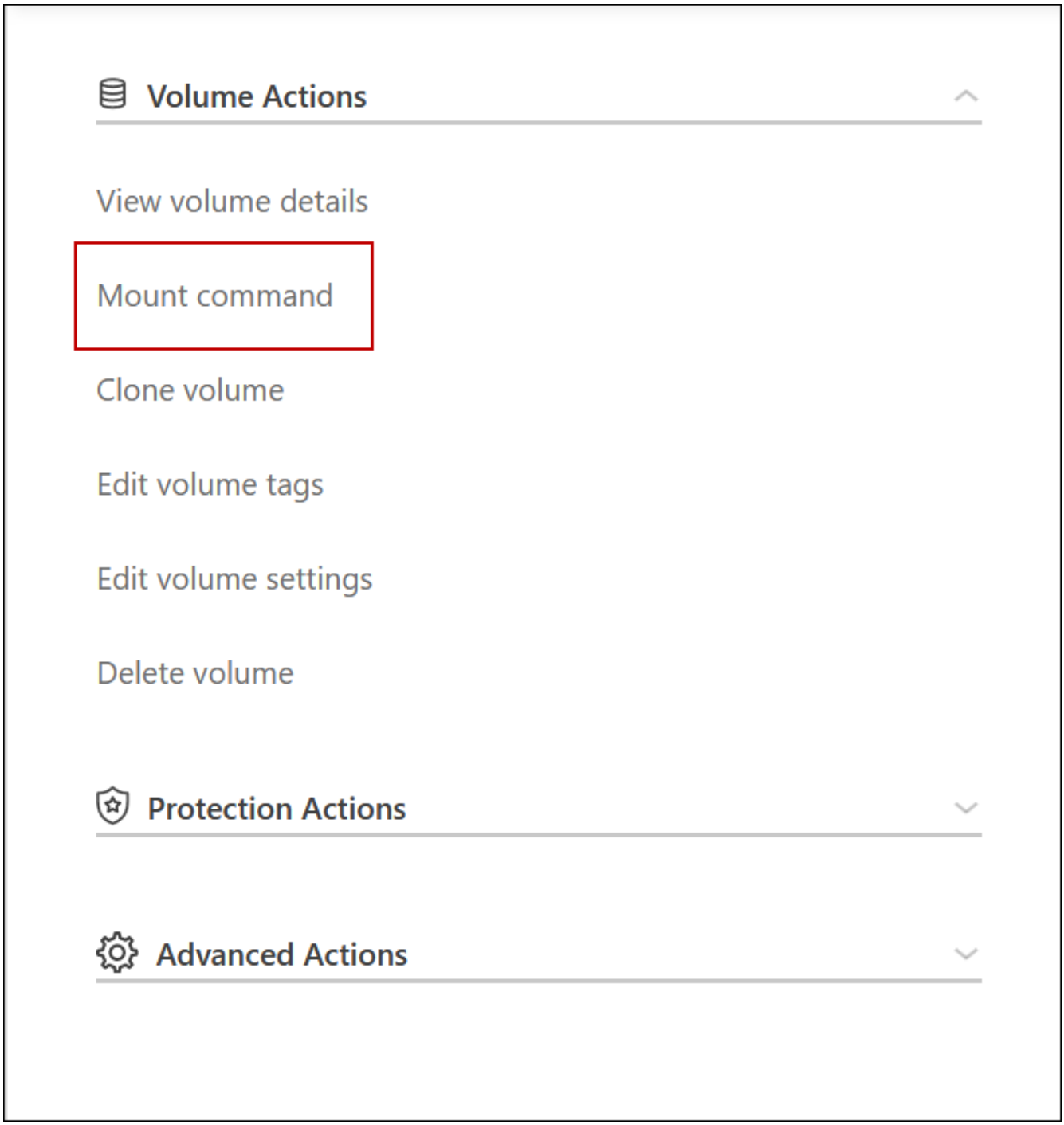
e. 单击“添加规则”。

f. 在类型下，选择*所有流量*，然后选择 VPC IP 地址。

g. 单击“保存规则”以应用更改。

7. 使用浮动 IP 地址将卷挂载到客户端。

   您可以通过控制台中“管理卷”面板下的“**Mount Command**”选项在控制台中找到正确的 IP 地址。



8. 如果您正在挂载 NFS 卷，请配置导出策略以匹配客户端 VPC 的子网。

   "了解如何编辑卷" 。

相关链接

- "AWS 中的高可用性对"
- "AWS 中Cloud Volumes ONTAP的网络要求"

在 **AWS** 共享子网中部署**Cloud Volumes ONTAP HA** 对

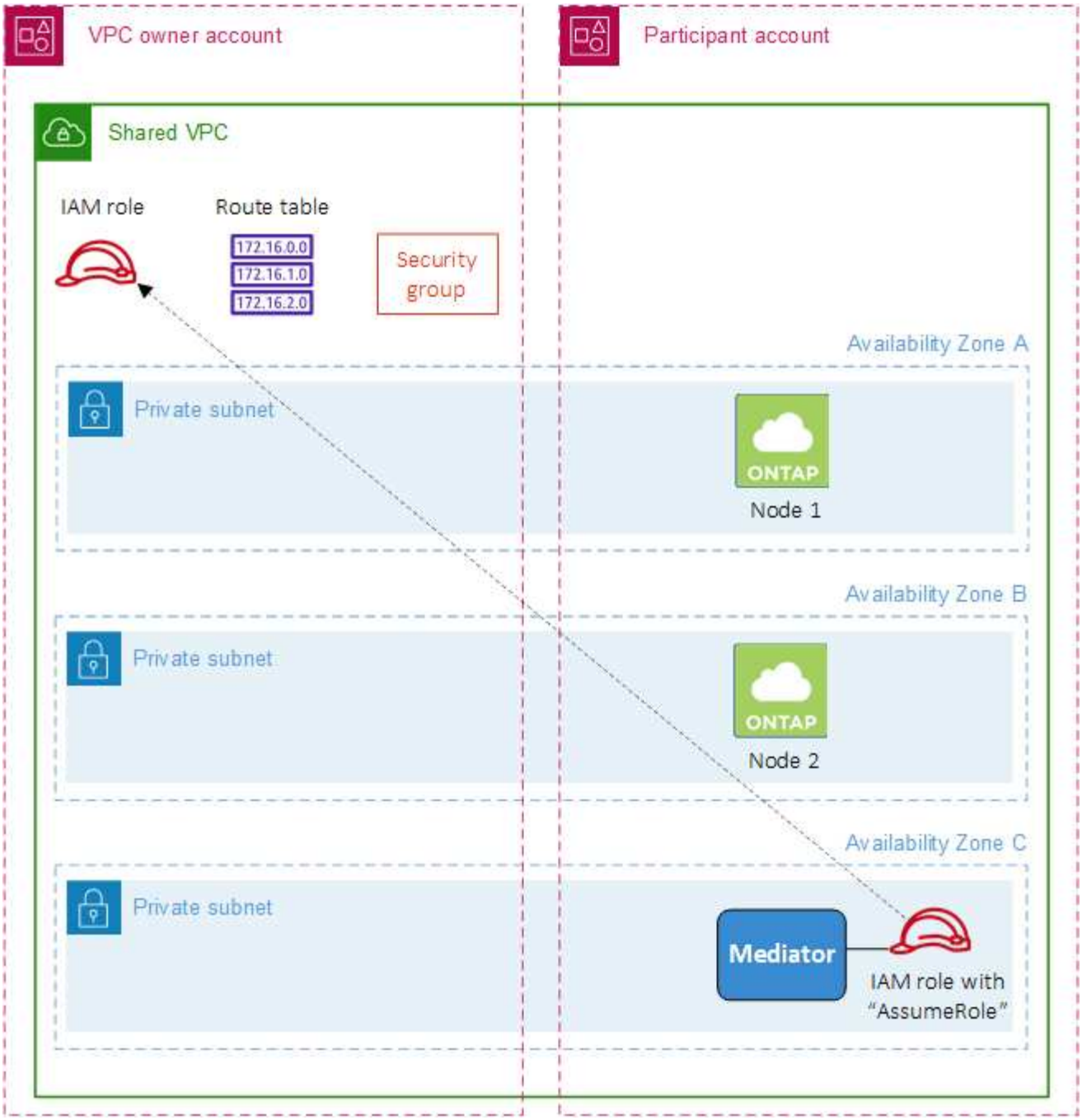
从 9.11.1 版本开始，AWS 通过 VPC 共享支持Cloud Volumes ONTAP HA 对。 VPC 共享使您的组织能够与其他 AWS 账户共享子网。要使用此配置，您必须设置您的 AWS 环境，然后使用 API 部署 HA 对。

和 "VPC共享"， Cloud Volumes ONTAP HA 配置分布在两个帐户中：

- VPC 所有者账户，拥有网络（VPC、子网、路由表和Cloud Volumes ONTAP安全组）
- 参与者账户，其中 EC2 实例部署在共享子网中（这包括两个 HA 节点和中介者）

对于跨多个可用区部署的Cloud Volumes ONTAP HA 配置，HA 中介需要特定权限才能写入 VPC 所有者帐户中的路由表。您需要通过设置调解员可以承担的 IAM 角色来提供这些权限。

下图显示了此部署所涉及的组件：



按照以下步骤所述，您需要与参与者账户共享子网，然后在 VPC 所有者账户中创建 IAM 角色和安全组。

当您创建Cloud Volumes ONTAP系统时， NetApp Console会自动创建 IAM 角色并将其附加到中介器。此角色承担您在 VPC 所有者账户中创建的 IAM 角色，以便对与 HA 对关联的路由表进行更改。

步骤

1. 与参与者账户共享 VPC 所有者账户中的子网。

   此步骤是在共享子网中部署 HA 对所必需的。

   "AWS 文档：共享子网"

2. 在 VPC 所有者账户中，为Cloud Volumes ONTAP创建一个安全组。

"请参阅Cloud Volumes ONTAP的安全组规则" 。请注意，您不需要为 HA 中介创建安全组。控制台会为您完成该操作。

3. 在 VPC 所有者账户中，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 API 创建新的Cloud Volumes ONTAP系统。

   请注意，您必须指定以下字段：

   - “安全组 ID”

     “securityGroupId”字段应指定您在 VPC 所有者帐户中创建的安全组（请参阅上面的步骤 2）。

   - “haParams”对象中的“assumeRoleArn”

     “assumeRoleArn”字段应包括您在 VPC 所有者账户中创建的 IAM 角色的 ARN（请参阅上面的步骤 3）。

     例如：

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

   +
   "了解Cloud Volumes ONTAP API"

在 **AWS** 单可用区中为**Cloud Volumes ONTAP HA** 对配置放置组创建

如果放置组创建失败，AWS 单可用区 (AZ) 中的Cloud Volumes ONTAP高可用性 (HA) 部署可能会失败并回滚。如果Cloud Volumes ONTAP节点和中介实例不可用，则放置组的创建也会失败，并且部署会回滚。为了避免这种情况，您可以修改配置，以便即使放置组创建失败也能完成部署。

绕过回滚过程后， Cloud Volumes ONTAP部署过程成功完成，并通知您放置组创建未完成。

步骤

1. 使用 SSH 连接到NetApp Console代理主机并登录。
2. 导航至 `/opt/application/netapp/cloudmanager/docker_occm/data`。
3. 编辑 `app.conf`通过改变 `rollback-on-placement-group-failure`参数 `false`。该参数的默认值是 `true`。

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. 保存文件并注销控制台代理。您不需要重新启动控制台代理。

Cloud Volumes ONTAP的 **AWS** 安全组入站和出站规则

NetApp Console创建 AWS 安全组，其中包括Cloud Volumes ONTAP成功运行所需的入站和出站规则。您可能希望参考端口以进行测试，或者您更喜欢使用自己的安全组。

Cloud Volumes ONTAP规则

Cloud Volumes ONTAP的安全组需要入站和出站规则。

入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

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

协议	端口	目的
所有 ICMP	全部	对实例执行 ping 操作
HTTP	80	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
HTTPS	443	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
SSH	22	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111	NFS 的远程过程调用
TCP	139	CIFS 的 NetBIOS 服务会话
TCP	161-162	简单网络管理协议

协议	端口	目的
TCP	445	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁守护进程
TCP	4046	NFS 网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104	SnapMirror集群间通信会话的管理
TCP	11105	使用集群间 LIF 进行SnapMirror数据传输
UDP	111	NFS 的远程过程调用
UDP	161-162	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049	NFS 服务器守护进程
UDP	4045	NFS 锁守护进程
UDP	4046	NFS 网络状态监视器
UDP	4049	NFS rquotad 协议

出站规则

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

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

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

高级出站规则

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

源是Cloud Volumes ONTAP系统上的接口（IP 地址）。

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

服务	协议	端口	源	目标	目的
备份到S3	TCP	5010	集群间 LIF	备份端点或恢复端点	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	另一个节点上的所有LIF	集群间通信（仅限Cloud Volumes ONTAP HA）
	TCP	3000	节点管理 LIF	HA介导者	ZAPI 调用（仅限Cloud Volumes ONTAP HA）
	ICMP	1	节点管理 LIF	HA介导者	保持活动状态（仅限Cloud Volumes ONTAP HA）
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档"
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53	节点管理 LIF 和数据 LIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600-18699	节点管理 LIF	目标服务器	NDMP 拷贝
SMTP	TCP	25	节点管理 LIF	邮件服务器	SMTP 警报，可用于AutoSupport
SNMP	TCP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104	集群间 LIF	ONTAP集群间 LIF	SnapMirror集群间通信会话的管理
	TCP	11105	集群间 LIF	ONTAP集群间 LIF	SnapMirror数据传输
系统日志	UDP	514	节点管理 LIF	系统日志服务器	Syslog 转发消息

HA 调解器外部安全组的规则

Cloud Volumes ONTAP HA 中介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 中介的预定义安全组包括以下入站规则。

协议	端口	源	目的
TCP	3000	控制台代理的 CIDR	通过控制台代理访问 RESTful API

出站规则

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

基本出站规则

HA 中介的预定义安全组包括以下出站规则。

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

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开 HA 中介器出站通信所需的端口。

协议	端口	目标	目的
HTTP	80	AWS EC2 实例上的控制台代理的 IP 地址	下载中介器的升级版本
HTTPS	443	ec2.amazonaws.com	协助存储故障转移
UDP	53	ec2.amazonaws.com	协助存储故障转移

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

Cloud Volumes ONTAP HA 配置的预定义内部安全组包括以下规则。该安全组支持 HA 节点之间以及中介与节点之间的通信。

控制台始终创建此安全组。您没有选择使用自己的。

入站规则

预定义安全组包括以下入站规则。

协议	端口	目的
所有流量	全部	HA 中介器和 HA 节点之间的通信

出站规则

预定义安全组包括以下出站规则。

协议	端口	目的
所有流量	全部	HA 中介器和 HA 节点之间的通信

控制台代理的规则

"查看控制台代理的安全组规则"

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

如果您想将 Amazon 加密与Cloud Volumes ONTAP一起使用，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NetApp Console和Cloud Volumes ONTAP位于同一个 AWS 账户中，也可以位于不同的 AWS 账户中。

   "AWS 文档：客户主密钥 (CMK)"

2. 通过添加以_密钥用户_身份向控制台提供权限的 IAM 角色来修改每个 CMK 的密钥策略。

   将身份和访问管理 (IAM) 角色添加为关键用户，可授予控制台使用 CMK 与Cloud Volumes ONTAP 的权限。

   "AWS 文档：编辑密钥"

3. 如果 CMK 位于不同的 AWS 账户中，请完成以下步骤：

   a. 从 CMK 所在的账户进入 KMS 控制台。

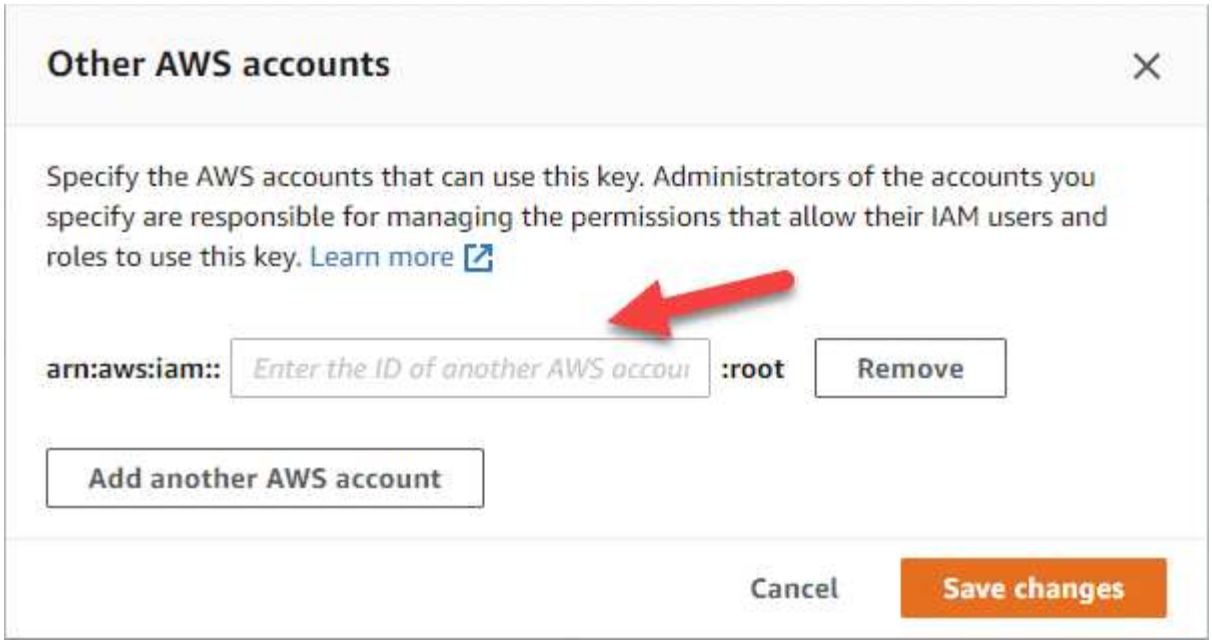
   b. 选择键。

   c. 在“常规配置”窗格中，复制密钥的 ARN。

      创建Cloud Volumes ONTAP系统时，您需要向控制台提供 ARN。

   d. 在 其他 **AWS** 账户 窗格中，添加为控制台提供权限的 AWS 账户。

      通常，这是部署控制台的帐户。如果 AWS 中未安装控制台，请使用您向控制台提供 AWS 访问密钥的帐户。



e. 现在切换到为控制台提供权限的 AWS 账户并打开 IAM 控制台。

f. 创建包含下面列出的权限的 IAM 策略。

g. 将策略附加到向控制台提供权限的 IAM 角色或 IAM 用户。

以下策略提供控制台使用来自外部 AWS 账户的 CMK 所需的权限。请务必修改“资源”部分中的区域和帐户 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
                }
            }
        }
    ]
}
```

+
有关此过程的更多详细信息，请参阅 "AWS 文档：允许其他账户中的用户使用 KMS 密钥"。

4. 如果您使用的是客户管理的 CMK，请通过将Cloud Volumes ONTAP IAM 角色添加为_密钥用户_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加密存储在 Amazon Simple Storage Service

(Amazon S3) 存储桶中的数据，则需要执行此步骤。

您需要在部署Cloud Volumes ONTAP之后执行此步骤，因为 IAM 角色是在创建Cloud Volumes ONTAP系统时创建的。 （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节点设置 AWS IAM 角色

必须将具有所需权限的 AWS 身份和访问管理 (IAM) 角色附加到每个Cloud Volumes ONTAP节点。对于 HA 调解员来说也是如此。最简单的方法是让NetApp Console为您创建 IAM 角色，但您也可以使用自己的角色。

此任务是可选的。当您创建Cloud Volumes ONTAP系统时，默认选项是让控制台为您创建 IAM 角色。如果您企业的安全策略要求您自己创建 IAM 角色，请按照以下步骤操作。

AWS Secret Cloud 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）区域

```
{
    "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"
    }]
}
```

绝密地区

```
{
    "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"
    }]
}
```

秘密区域

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

- Cloud Volumes ONTAP节点的备份策略

  如果您计划将NetApp Backup and Recovery与Cloud Volumes ONTAP系统一起使用，则节点的 IAM 角色必须包括下面显示的第二个策略。

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）区域

```
{
    "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"
        }
    ]
}
```

绝密地区

```
{
    "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"
        }
    ]
}
```

秘密区域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b: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-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA介导者

```
{
    "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. 创建一个 IAM 角色并将您创建的策略附加到该角色。

结果

现在，您拥有可以在创建新的Cloud Volumes ONTAP系统时选择的 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 中设置Cloud Volumes ONTAP许可

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

免费增值

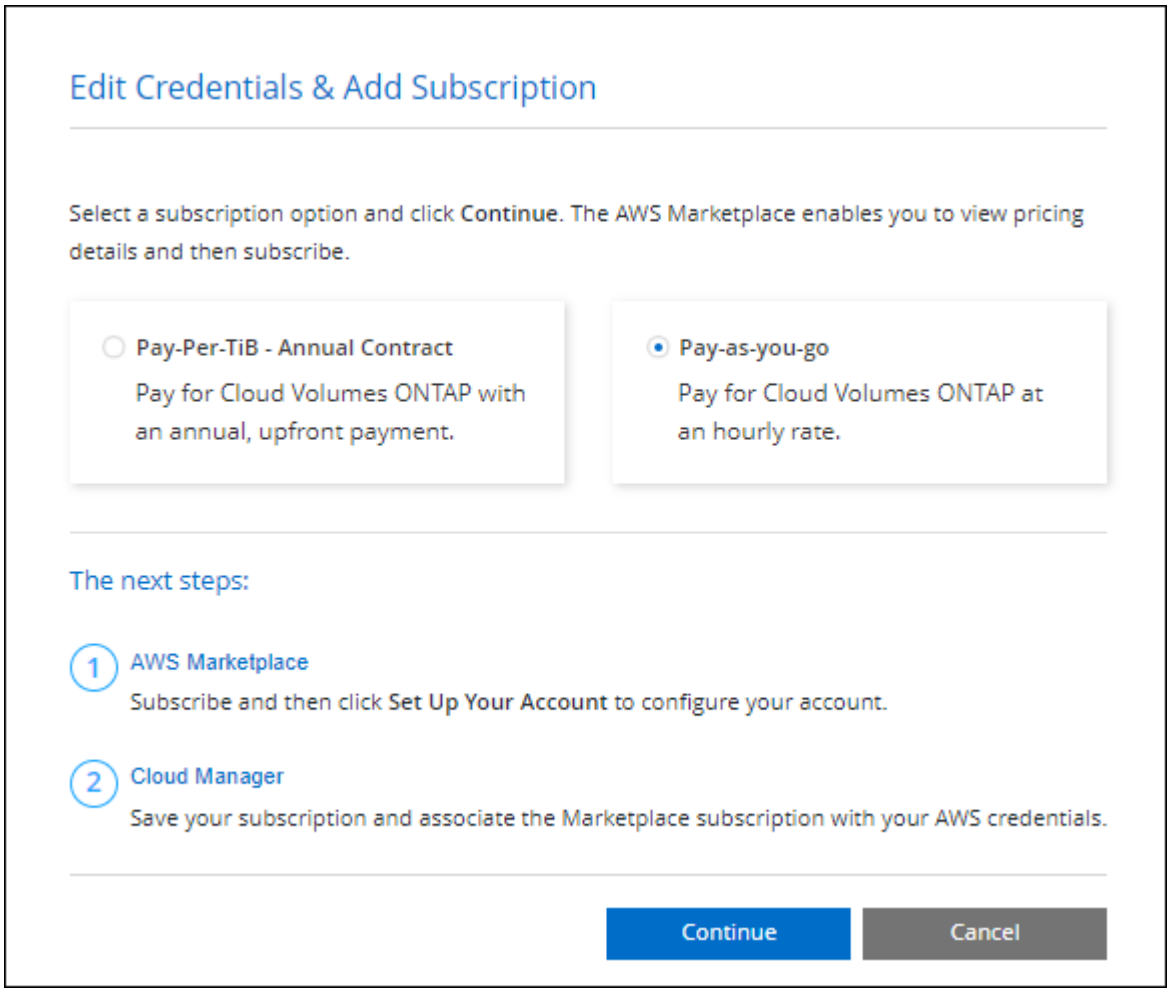
选择免费增值服务，免费使用Cloud Volumes ONTAP，最高可提供 500 GiB 的配置容量。"了解有关免费增值服务的更多信息" 。

步骤

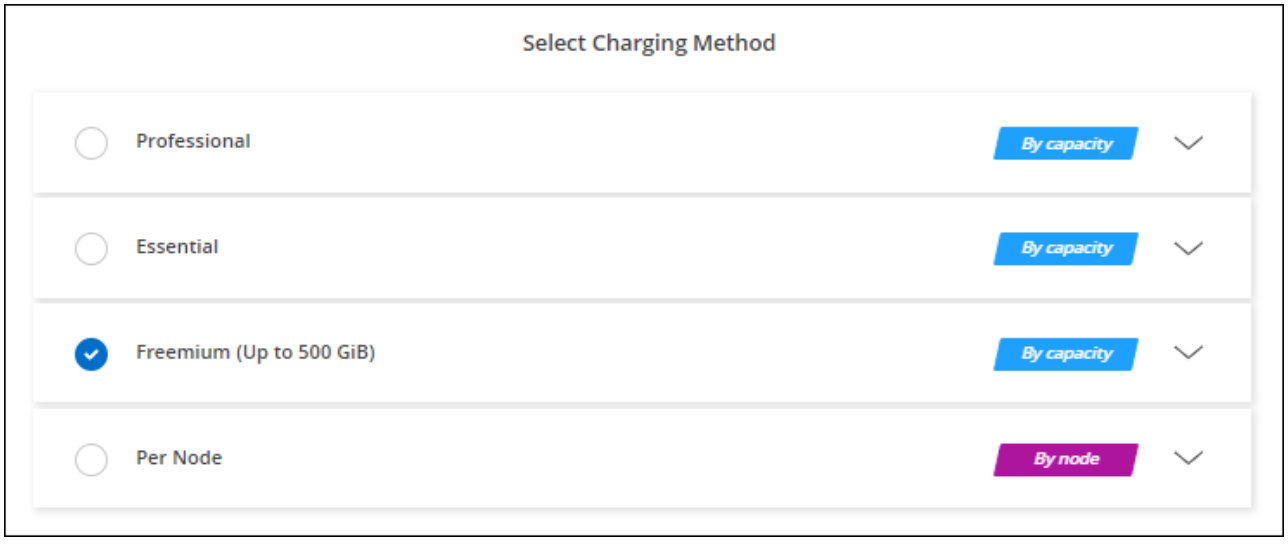
1. 从NetApp Console的左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
    a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即

用即付服务。

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



a. 返回控制台后，到达收费方式页面时选择“免费增值”。



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

基于容量的许可证

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

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

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

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

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

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

步骤

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

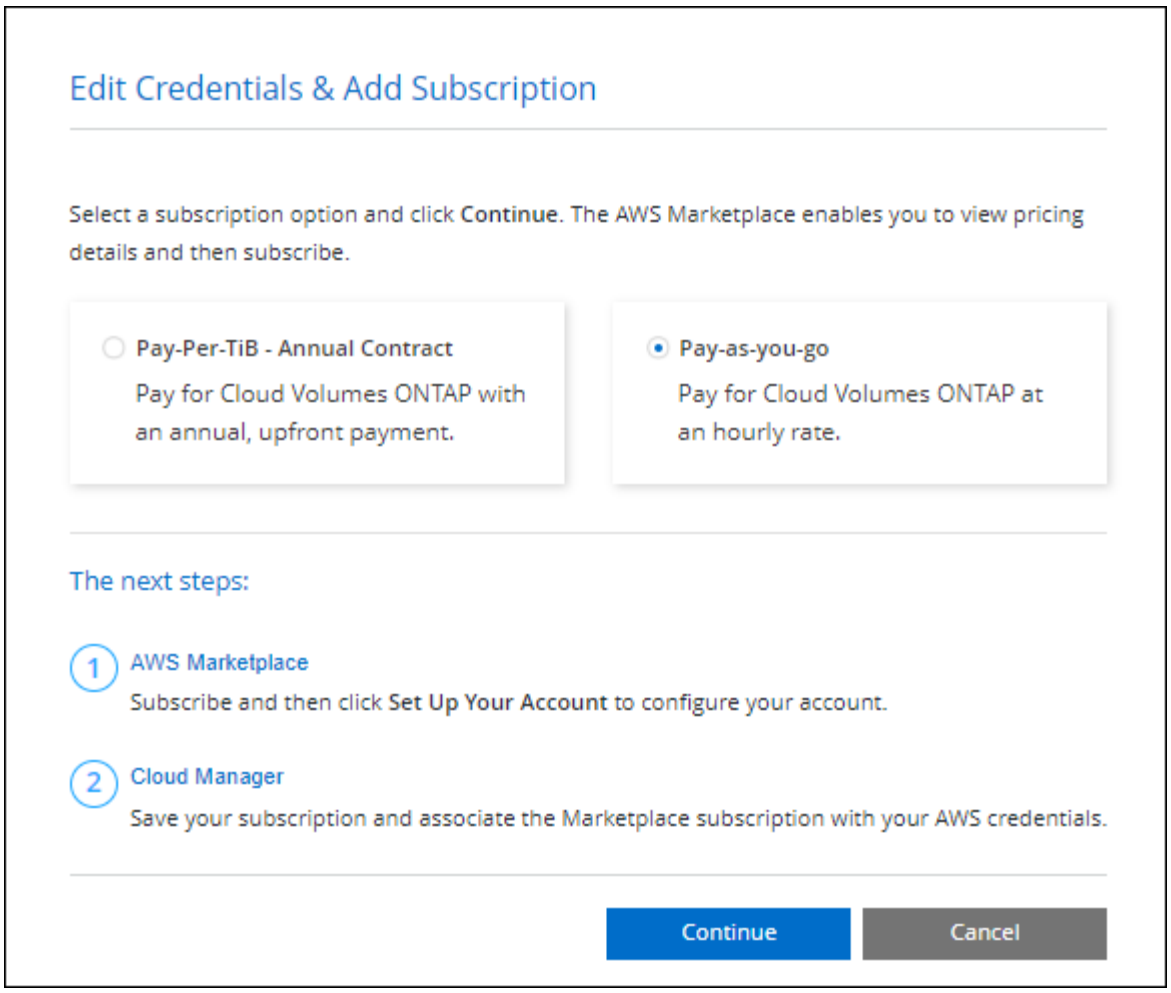
   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台会自动将许可证添加到控制台。

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

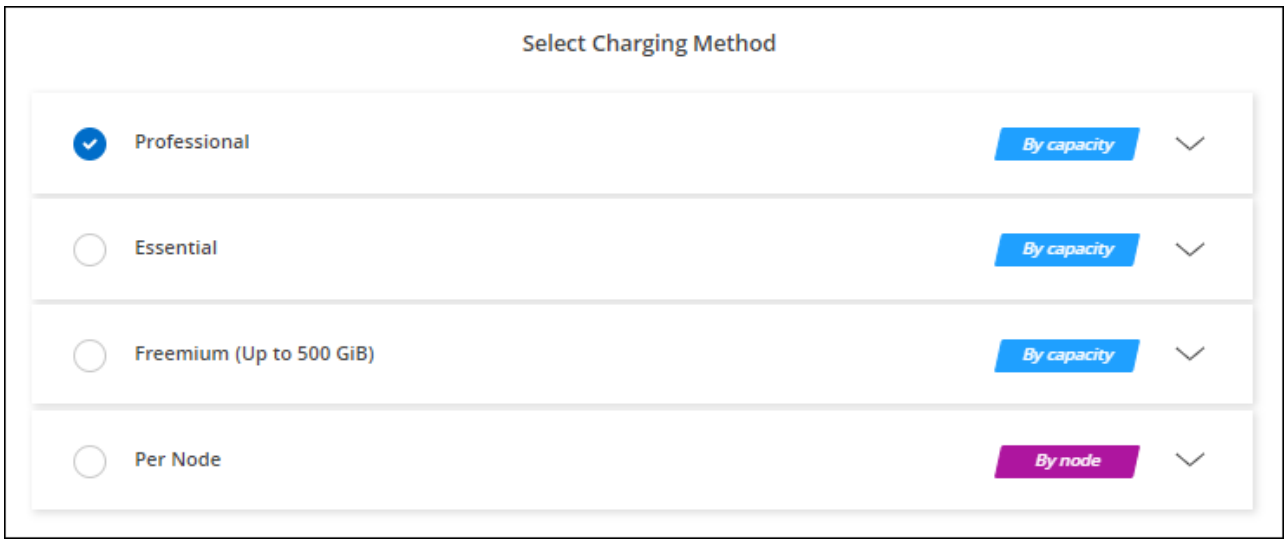
3. 在控制台的“系统”页面上，单击“添加系统”并按照步骤操作。

   a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即用即付服务。

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



a. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

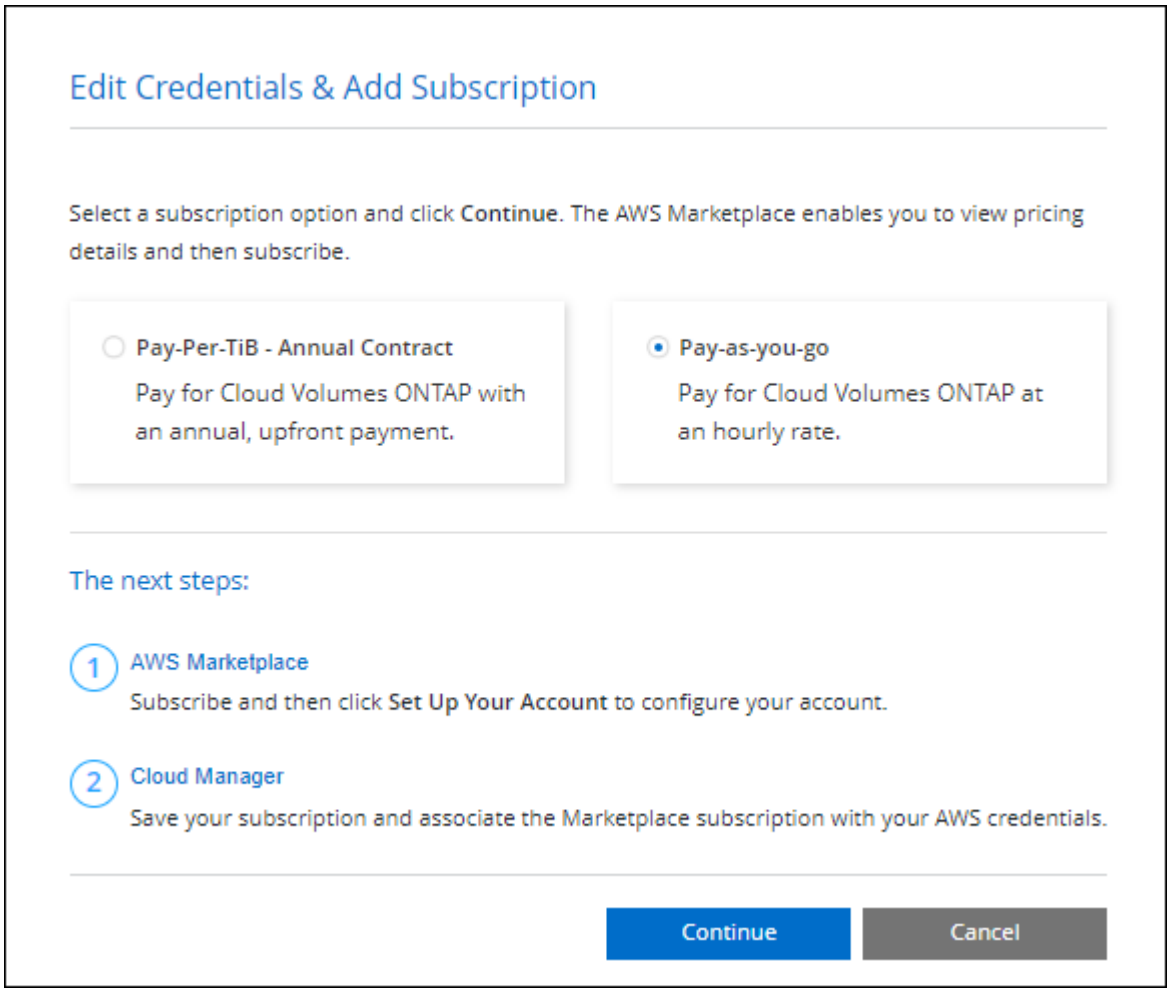
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

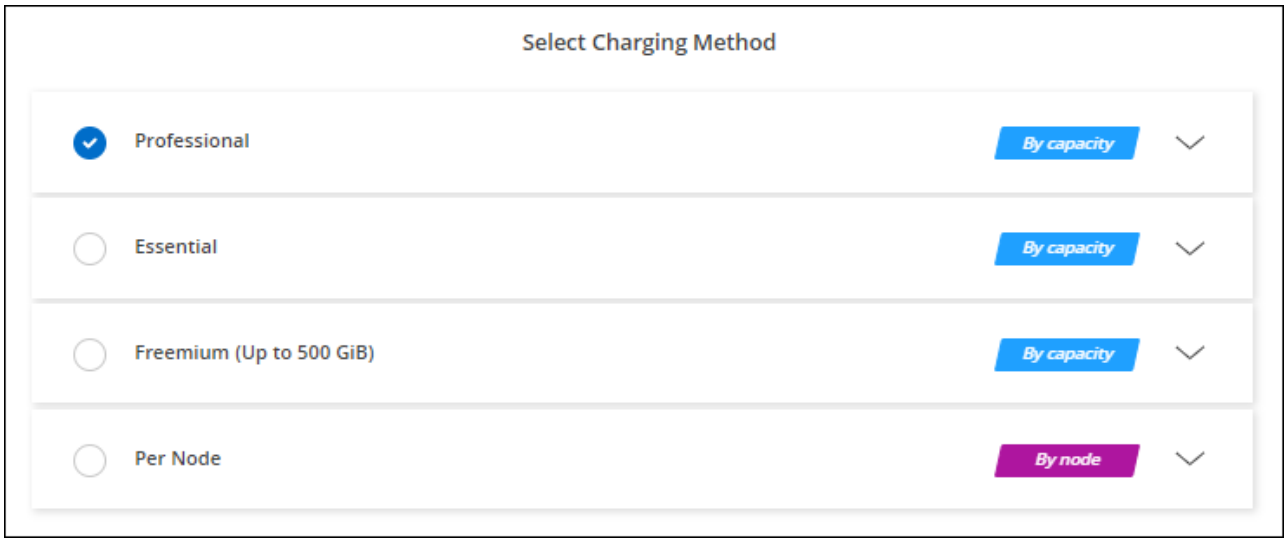
当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 AWS Marketplace 中提供的协议。然后将该订阅与系统关联以进行收费。您可以使用相同的订阅来获取其他Cloud Volumes ONTAP系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭证”页面上，单击“编辑凭证”>“添加订阅”，然后按照提示订阅 AWS Marketplace 中的即用即付服务



   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

您可以从“设置”>“凭证”页面管理与您的 AWS 账户关联的 AWS Marketplace 订阅。 "了解如何管理您的 AWS 账户和订阅"

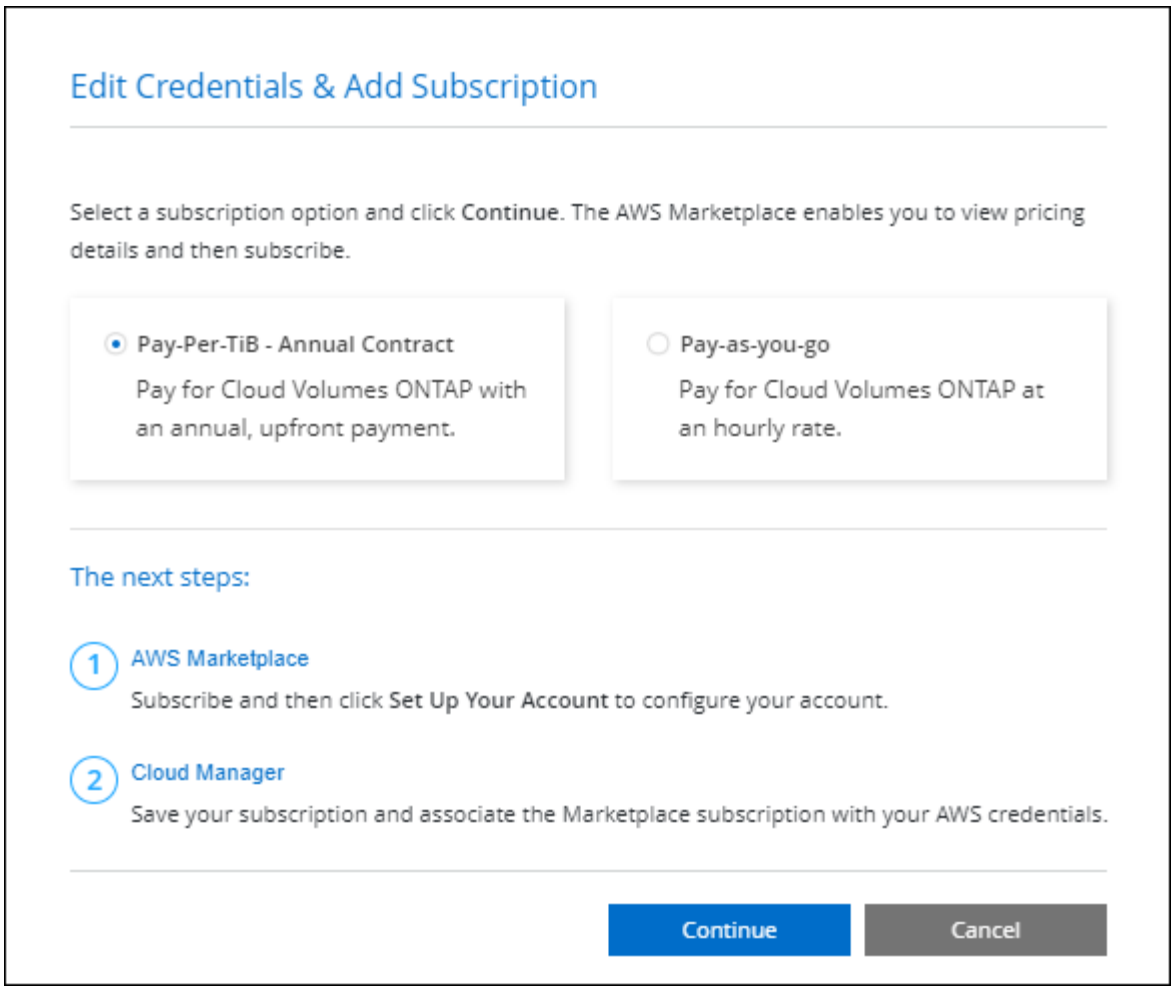
年度合同

从云提供商的市场购买年度合同，按年付款。

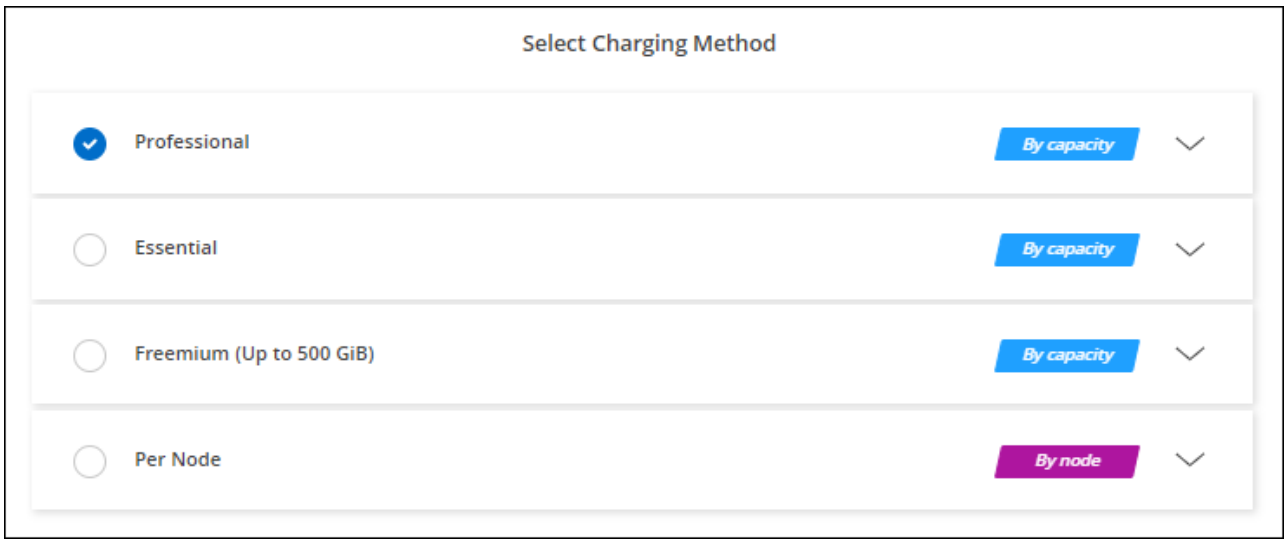
与按小时订阅类似，控制台会提示您订阅 AWS Marketplace 中提供的年度合同。

步骤

1. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在*详细信息和凭证*页面上，单击*编辑凭证 > 添加订阅*，然后按照提示在 AWS Marketplace 中订阅年度合同。



b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

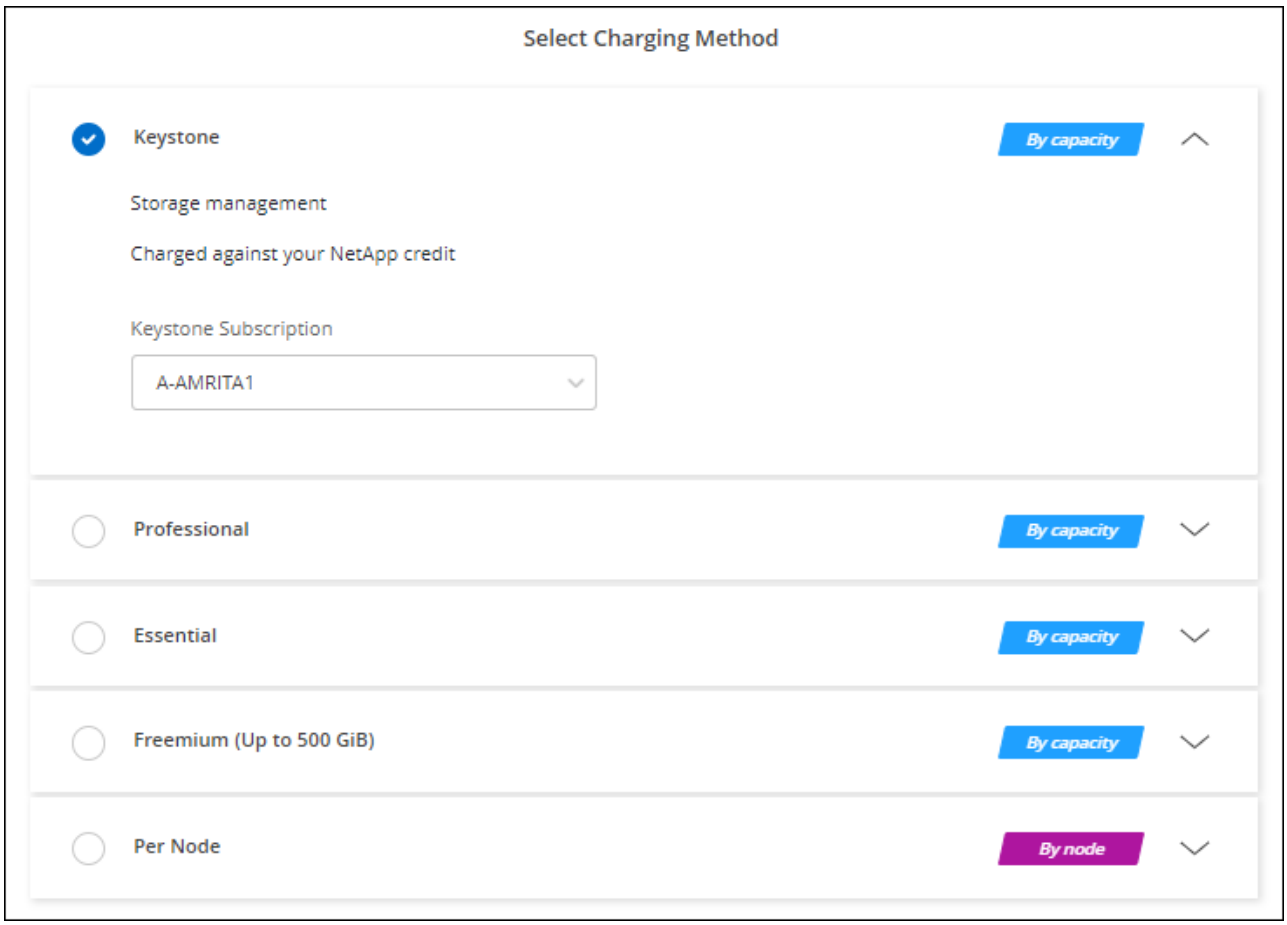
Keystone订阅

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

步骤

1. 如果您尚未订阅， "联系NetApp"
2. 联系NetApp 为您的用户帐户授权一个或多个Keystone订阅。
3. NetApp授权您的帐户后，"链接您的订阅以用于Cloud Volumes ONTAP" 。
4. 在*系统*页面上，单击*添加系统*并按照步骤操作。

    a. 当提示选择收费方式时，选择Keystone Subscription 收费方式。



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

基于节点的许可证

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

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

使用快速部署在 **AWS** 中部署**Cloud Volumes ONTAP**

您可以使用快速部署方法在 AWS 中部署Cloud Volumes ONTAP，适用于单节点和高可用性 (HA) 配置。与先进的方法相比，这种简化的流程减少了部署步骤。它还通过在单个页面上自动设置默认值并最小化导航来提供更清晰的工作流程。

开始之前

您需要以下内容才能从NetApp Console在 AWS 中添加Cloud Volumes ONTAP系统。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的项目或工作区关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。
- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。
- CIFS 配置的 DNS 和 Active Directory。

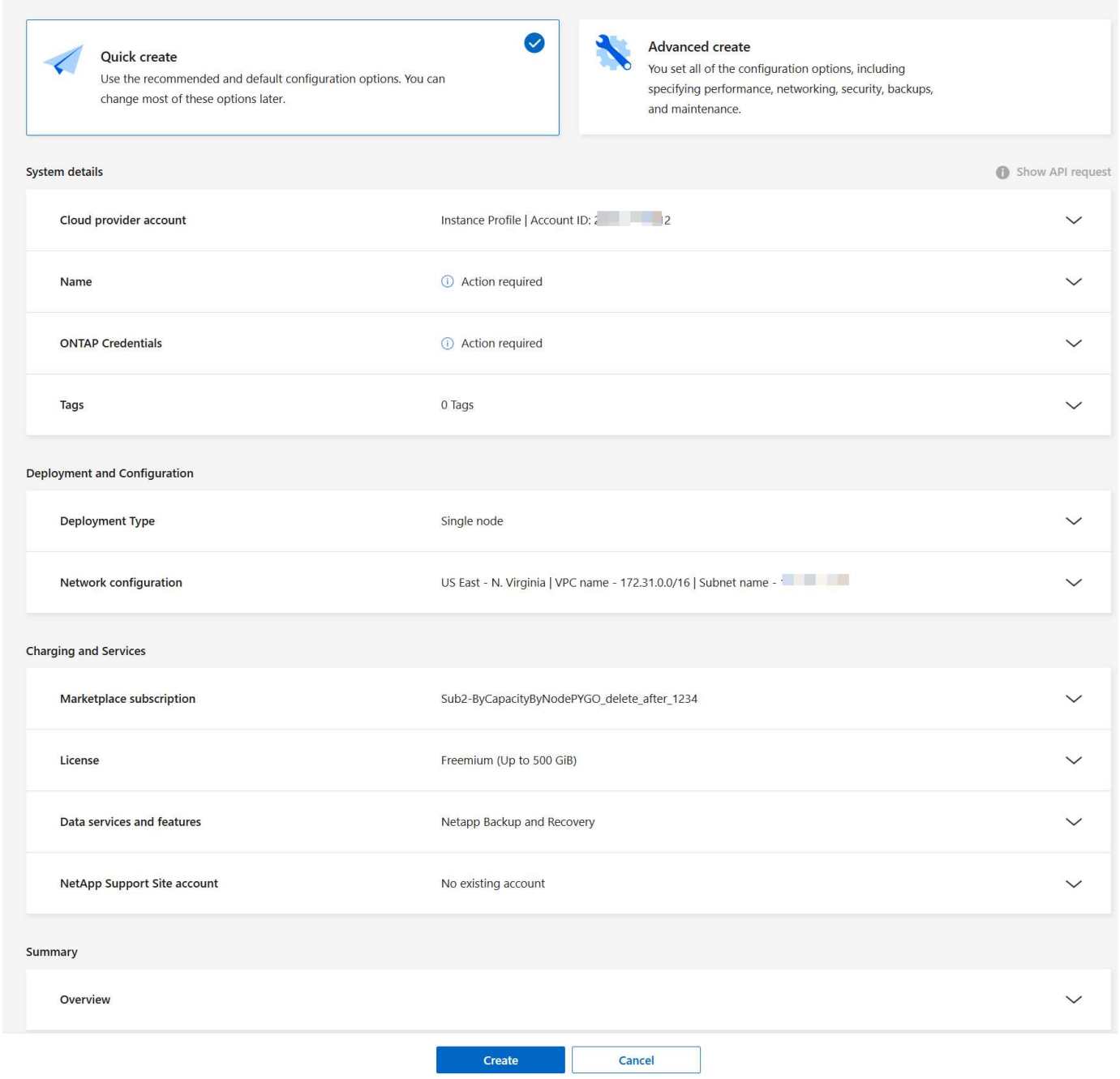
  有关详细信息，请参阅"AWS 中Cloud Volumes ONTAP的网络要求"。

关于此任务

创建Cloud Volumes ONTAP系统后， NetApp Console会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台会立即终止实例，然后开始部署系统。如果控制台无法验证连接，则系统创建失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在 Canvas 页面上，单击 添加系统 并按照提示进行操作。
3. 选择 **Amazon Web Services** > * Cloud Volumes ONTAP* > 添加新。默认情况下选择*快速创建*选项。



系统详细信息

1. 云提供商帐户：帐户详细信息将根据您选择的控制台代理自动填充。如果您有多个帐户，请选择要使用的帐户。如果控制台代理不可用，系统将提示您 "创建控制台代理"。
2. 名称：系统名称。控制台使用系统（集群）名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
3. * ONTAP凭据* 这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。您可以保留默认的_admin_用户名，也可以将其更改为自定义用户名。
4. 标签 AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建Cloud Volumes ONTAP系统时，您可以从用户界面添加最多 15 个标签，然后可以在创建后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。

部署和配置

1. 部署类型：选择您要使用的部署类型，单节点、单个可用区 (AZ) 中的高可用性 (HA) 或多个 AZ 中的 HA。
2. 网络配置：输入您在 "AWS 工作表"。
   a. **AWS** 区域：默认选择关联云账户的、拥有子网资源的 VPC 所在区域。
   b. **VPC**：输入具有子网的 AWS 区域的 VPC。如果没有子网，则选择 VPC 的默认值。
   c. 子网：您只能为 VPC 选择一个子网，以用于单节点部署或单 AZ 中的 HA 部署。

高可用性

如果您选择了 HA 配置，请输入以下信息：

单可用区高可用性

1. 调解器访问：指定调解器访问信息。调解器是一个单独的实例，用于监控 HA 对的健康状况并在发生故障时提供仲裁。提供密钥对名称以使中介实例能够连接到 AWS EC2 服务，并选择连接方法。

多个可用区中的高可用性

1. 可用区域和中介：选择每个节点的可用区域 (AZ) 以及要部署Cloud Volumes ONTAP HA 对的中介和相应子网。
2. 浮动 **IP**：如果您选择多个 AZ，请为 NFS 和 CIFS 服务以及集群和 SVM 管理指定浮动 IP 地址。 IP 地址必须位于该区域内所有 VPC 的 CIDR 块之外。有关更多详细信息，请参阅"多个可用区中Cloud Volumes ONTAP HA 的 AWS 网络要求"。
3. 调解器访问：指定调解器访问信息。调解器是一个单独的实例，用于监控 HA 对的健康状况并在发生故障时提供仲裁。提供密钥对名称以使中介实例能够连接到 AWS EC2 服务，并选择连接方法。
4. 路由表：如果您选择了多个 AZ，请选择包含到浮动 IP 地址的路由的路由表。如果您有多个路由表，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。有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

充电和服务

1. 市场订阅：选择您想要与此Cloud Volumes ONTAP系统一起使用的 AWS 市场订阅。
2. 许可证：选择您想要与此Cloud Volumes ONTAP系统一起使用的许可证类型。您可以从专业版、基本版和高级版许可证中进行选择。有关不同许可证的信息，请参阅"了解Cloud Volumes ONTAP许可证"。
3. 数据服务和功能：保持服务启用或禁用您不想与Cloud Volumes ONTAP一起使用的服务。
   - "了解有关NetApp分类的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"
   - "了解Cloud Volumes ONTAP上的 WORM 存储"

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

   - * NetApp支持站点帐户*：如果您有多个帐户，请选择要使用的帐户。

摘要

检查或编辑您输入的详细信息，然后单击*创建*。

部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

- "规划您的Cloud Volumes ONTAP配置"
- "使用高级部署在 AWS 中部署Cloud Volumes ONTAP"

在 AWS 中启动Cloud Volumes ONTAP

您可以在单系统配置中启动Cloud Volumes ONTAP ，也可以在 AWS 中以 HA 对的形式启动 Cloud Volumes ONTAP。此方法提供了高级部署体验，与快速部署方法相比，它提供了更多的配置选项和灵活性。

开始之前

开始之前您需要以下内容。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该已经做好准备，选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置"。
- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。
- CIFS 配置的 DNS 和 Active Directory。

  有关详细信息，请参阅"AWS 中Cloud Volumes ONTAP的网络要求"。

在 AWS 中启动单节点Cloud Volumes ONTAP系统

如果您想在 AWS 中启动Cloud Volumes ONTAP ，则需要在NetApp Console中创建一个新系统。

关于此任务

创建系统后，控制台会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台将立即终止实例，然后开始部署Cloud Volumes ONTAP系统。如果无法验证连接，系统创建将失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

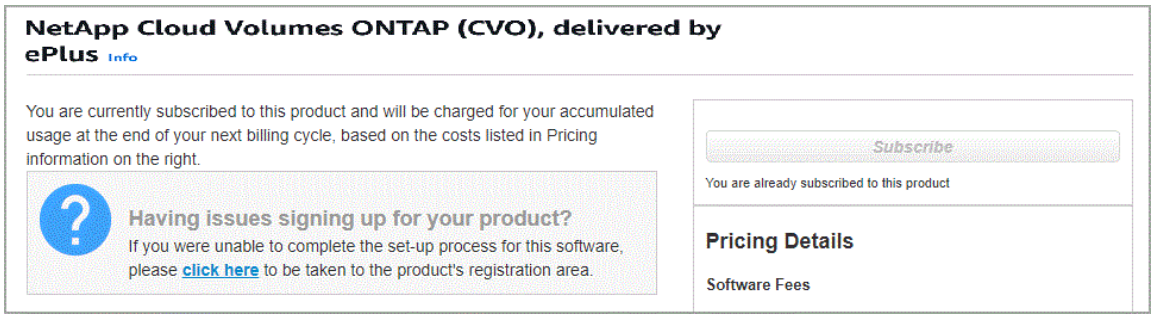
1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择 **Amazon Web Services** 和 * Cloud Volumes ONTAP Single Node*。

4. 选择*高级创建*。由于默认选择了*快速创建*模式，您可能会看到一条有关默认值的消息。单击“继续”。
5. 如果出现提示， "创建控制台代理" 。
6. 详细信息和凭证：可选择更改 AWS 凭证和订阅，输入系统名称，根据需要添加标签，然后输入密码。

   此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
添加标签	AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	选择与您要部署此系统的帐户关联的 AWS 凭证。您还可以将 AWS 市场订阅与此Cloud Volumes ONTAP系统关联起来使用。点击“添加订阅”将所选凭证与新的 AWS 市场订阅关联。订阅可以是年度合同，也可以是按小时付费的Cloud Volumes ONTAP 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何向NetApp Console添加其他 AWS 凭证"^] 。

   如果多个 IAM 用户在同一个 AWS 账户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS 市场会通知后续用户他们已经订阅，如下图所示。当 AWS 账户有订阅时，每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到下面显示的消息，请单击“单击此处”链接转到控制台网站并完成该过
   程。



7. 服务：保持服务启用或禁用您不想与Cloud Volumes ONTAP一起使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"

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

8. 位置和连接：输入您在 "AWS 工作表"。

下表描述了您可能需要指导的字段：

字段	描述
VPC	如果您有 AWS Outpost，则可以通过选择 Outpost VPC 在该 Outpost 中部署单节点Cloud Volumes ONTAP系统。体验与驻留在 AWS 中的任何其他 VPC 相同。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的来源是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的安全组	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

9. 数据加密：选择无数据加密或 AWS 管理加密。

   对于 AWS 管理的加密，您可以从您的账户或其他 AWS 账户中选择不同的客户主密钥 (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" 。

   "了解有关受支持的加密技术的更多信息" 。

10. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
    - "了解Cloud Volumes ONTAP的许可选项" 。
    - "了解如何设置许可" 。
11. * Cloud Volumes ONTAP配置*（仅限年度 AWS 市场合同）：查看默认配置并单击*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，则只需要指定一个卷，然后审核并批准该配置。

12. 预配置包：选择其中一个包以快速启动Cloud Volumes ONTAP，或单击*更改配置*以选择您自己的配置。

    如果您选择其中一个包，那么您只需要指定一个卷，然后审核并批准配置。

13. **IAM** 角色：最好保留默认选项，让控制台为您创建角色。

    如果您希望使用自己的政策，则必须满足"Cloud Volumes ONTAP节点的策略要求"。

14. 许可：根据需要更改Cloud Volumes ONTAP版本并选择实例类型和实例租赁。

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

15. 底层存储资源：选择磁盘类型，配置底层存储，并选择是否保持数据分层启用。

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，控制台将使用 AWS 中的弹性卷功能根据需要自动增加底层存储磁盘容量。您可以根据您的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 AWS 弹性卷支持的更多信息" 。
- 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使用简单配置选项时控制台创建的任何其他聚合选择磁盘大小。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。
- 如果您禁用数据分层，则可以在后续聚合上启用它。

  "了解数据分层的工作原理" 。

16. 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. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

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

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

17. 创建卷：输入新卷的详细信息或单击*跳过*。

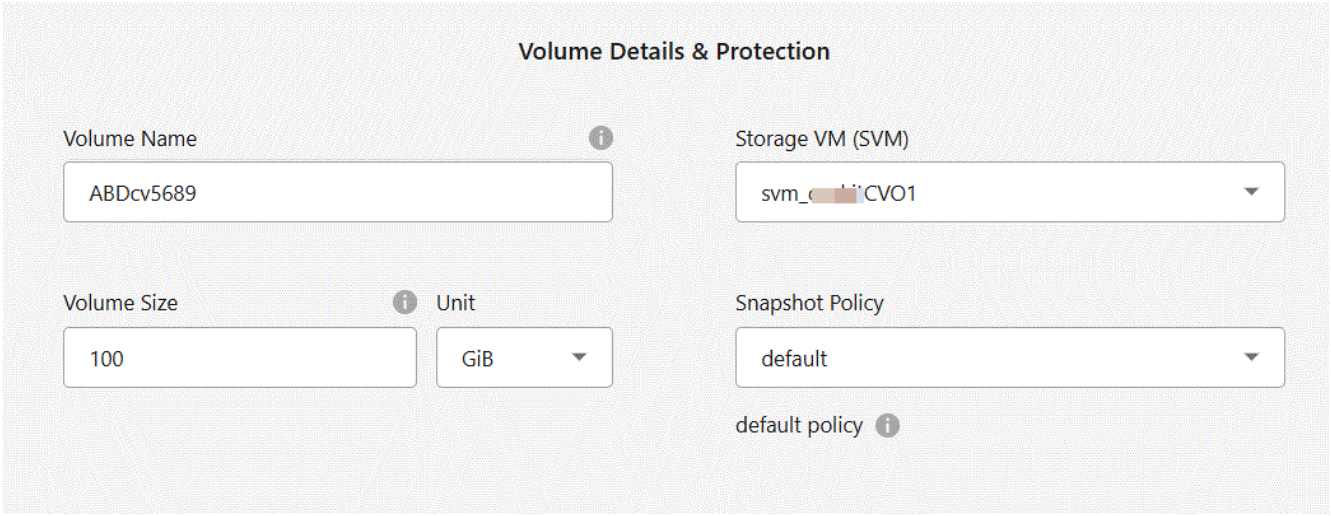
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 策略	Snapshot 副本策略指定自动创建的NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。

字段	描述
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 TCP 卸载引擎 (TOE) 卡、融合网络适配器 (CNA) 或专用主机总线适配器 (HBA) 连接到网络，并通过 iSCSI 限定名称 (IQN) 进行标识。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



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

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。如果将 AWS Managed 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存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

19. 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，并在需要时编辑卷分层策略。

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

20. 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”以查看有关支持和控制台将购买的 AWS 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台启动Cloud Volumes ONTAP实例。您可以在*审计*页面上跟踪进度。

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

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

> 部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

完成后

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

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

在 **AWS** 中启动**Cloud Volumes ONTAP HA** 对

如果您想在 AWS 中启动Cloud Volumes ONTAP HA 对，则需要在控制台中创建一个 HA 系统。

局限性

目前，AWS Outposts 不支持 HA 对。

关于此任务

创建Cloud Volumes ONTAP系统后，控制台会立即在指定的 VPC 中启动测试实例以验证连接性。如果成功，控制台将立即终止实例，然后开始部署Cloud Volumes ONTAP系统。如果无法验证连接，系统创建将失败。测试实例可以是 `t2.nano`（对于默认 VPC 租赁）或 `m3.medium`（适用于专用 VPC 租赁）。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择 **Amazon Web Services** 和 * Cloud Volumes ONTAP HA*。

   一些 AWS 本地区域可用。

您必须先启用本地区域并在 AWS 账户的本地区域中创建子网，然后才能使用 AWS 本地区域。按照*选择加入 AWS 本地区域*和*将您的 Amazon VPC 扩展到本地区域*中的步骤操作"AWS 教程“开始使用 AWS 本地区域部署低延迟应用程序"。

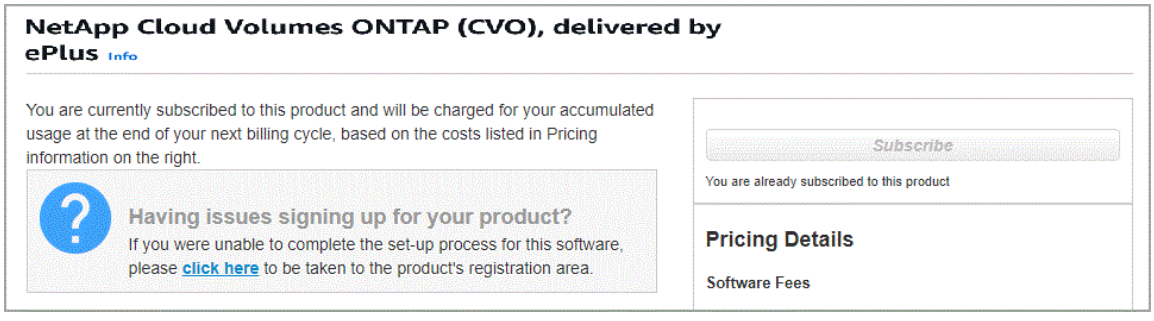
如果您运行的是控制台代理 3.9.36 或更低版本，则需要添加 `DescribeAvailabilityZones`AWS EC2 控制台中 AWS 角色的权限。

4. 详细信息和凭证：可选择更改 AWS 凭证和订阅，输入系统名称，根据需要添加标签，然后输入密码。

   此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Amazon EC2 实例。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
添加标签	AWS 标签是您的 AWS 资源的元数据。控制台将标签添加到Cloud Volumes ONTAP实例以及与该实例关联的每个 AWS 资源。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "AWS 文档：标记您的 Amazon EC2 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	选择要用于此Cloud Volumes ONTAP系统的 AWS 凭证和市场订阅。点击“添加订阅”将所选凭证与新的 AWS 市场订阅关联。订阅可以是年度合同，也可以是按小时付费的Cloud Volumes ONTAP 。如果您直接从NetApp购买了许可证（自带许可证 (BYOL)），则无需 AWS 订阅。NetApp已限制 BYOL 许可证的购买、延期和续订。有关更多信息，请参阅 "Cloud Volumes ONTAP的 BYOL 许可可用性受限" 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["了解如何向控制台添加其他 AWS 凭证"^] 。

如果多个 IAM 用户在同一个 AWS 账户中工作，则每个用户都需要订阅。第一个用户订阅后，AWS 市场会通知后续用户他们已经订阅，如下图所示。当 AWS 账户有订阅时，每个 IAM 用户都需要将自己与该订阅关联起来。如果您看到下面显示的消息，请单击“单击此处”链接转到控制台网站并完成该过
程。



5. 服务：保持服务启用或禁用您不想在此Cloud Volumes ONTAP系统中使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关备份和恢复的更多信息"

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

6. **HA** 部署模型：选择 HA 配置。

   有关部署模型的概述，请参阅"适用于 AWS 的Cloud Volumes ONTAP HA"。

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

   下表描述了您可能需要指导的字段：

字段	描述
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的来源是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的安全组	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

8. 连接和 **SSH** 身份验证：选择 HA 对和中介的连接方法。
9. 浮动 **IP**：如果您选择多个 AZ，请指定浮动 IP 地址。

   IP 地址必须位于该区域内所有 VPC 的 CIDR 块之外。有关更多详细信息，请参阅"多个可用区中Cloud Volumes ONTAP HA 的 AWS 网络要求"。

10. 路由表：如果您选择了多个 AZ，请选择应包含到浮动 IP 地址的路由的路由表。

    如果您有多个路由表，那么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。有关路由表的更多信息，请参阅 "AWS 文档：路由表"。

11. 数据加密：选择无数据加密或 AWS 管理加密。

    对于 AWS 管理的加密，您可以从您的账户或其他 AWS 账户中选择不同的客户主密钥 (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" 。

    "了解有关受支持的加密技术的更多信息" 。

12. 收费方式和 **NSS** 帐户：指定您想要在此系统中使用的收费选项，然后指定NetApp支持站点帐户。
    - "了解Cloud Volumes ONTAP的许可选项" 。
    - "了解如何设置许可" 。
13. * Cloud Volumes ONTAP配置*（仅限年度 AWS Marketplace 合同）：查看默认配置并单击*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，则只需要指定一个卷，然后审核并批准该配置。

14. 预配置包（按小时或仅限 BYOL）：选择其中一个包以快速启动Cloud Volumes ONTAP，或单击*更改配置*以选择您自己的配置。

    如果您选择其中一个包，那么您只需要指定一个卷，然后审核并批准配置。

15. **IAM** 角色：最好保留默认选项，让控制台为您创建角色。

    如果您希望使用自己的政策，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赁。

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

17. 底层存储资源：选择磁盘类型，配置底层存储，并选择是否保持数据分层启用。

    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，控制台将使用 AWS 中的弹性卷功能根据需要自动增加底层存储磁盘容量。您可以根据您的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 AWS 弹性卷支持的更多信息" 。
    - 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使用简单配置选项时控制台创建的任何其他聚合选择磁盘大小。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。
    - 如果您禁用数据分层，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. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

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

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

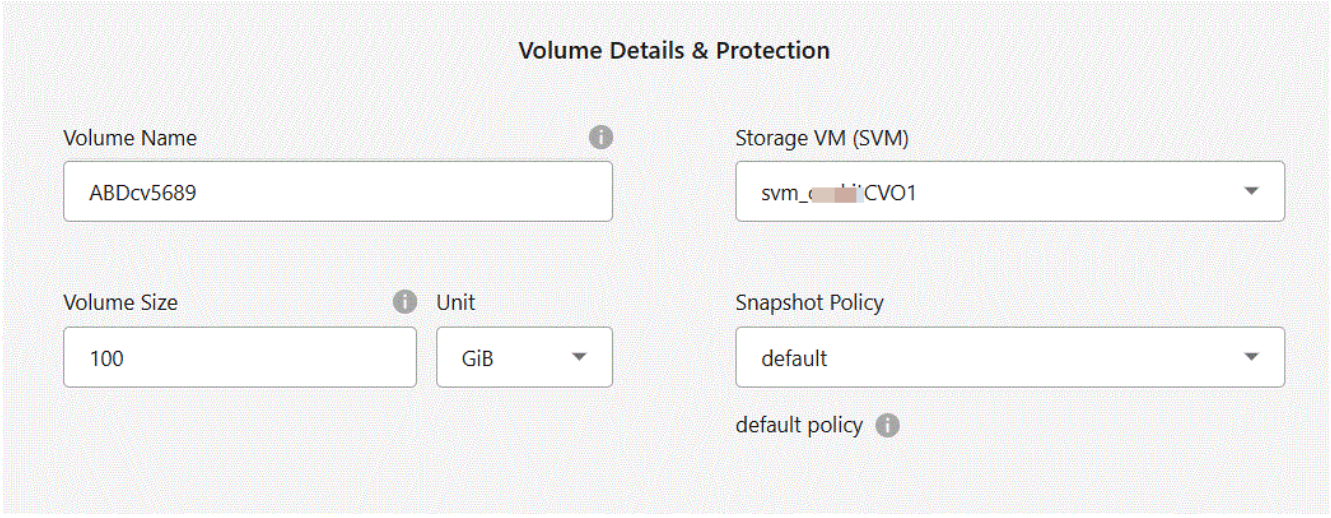
19. 创建卷：输入新卷的详细信息或单击*跳过*。

    "了解支持的客户端协议和版本" 。

此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

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

下图显示了卷创建向导的第一页：



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

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。

字段	描述
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。如果将 AWS Managed 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存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

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，并在需要时编辑卷分层策略。

    更多信息，请参阅"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”以查看有关支持和控制台将购买的 AWS 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

控制台启动Cloud Volumes ONTAP HA 对。您可以在*审计*页面上跟踪进度。

如果您在启动 HA 对时遇到任何问题，请查看失败消息。您也可以选择系统并单击重新创建环境。

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

完成后

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

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

> 部署过程完成后，请勿修改 AWS 云门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

- "规划您的Cloud Volumes ONTAP配置"
- "使用快速部署在 AWS 中部署Cloud Volumes ONTAP"

在 AWS Secret Cloud 或 AWS Top Secret Cloud 中部署Cloud Volumes ONTAP

与标准 AWS 区域NetApp Console，您可以在"AWS 秘密云"并且在"AWS 顶级机密云"部署Cloud Volumes ONTAP，为您的云存储提供企业级功能。 AWS Secret Cloud 和 Top Secret Cloud 是特定于美国情报界的封闭区域；本页上的说明仅适用于 AWS Secret Cloud 和 Top Secret Cloud 区域用户。

开始之前

在开始之前，请查看 AWS Secret Cloud 和 Top Secret Cloud 中支持的版本，并了解控制台中的私有模式。

- 查看 AWS Secret Cloud 和 Top Secret Cloud 中支持的以下版本：
  - Cloud Volumes ONTAP 9.12.1 P2
  - 控制台代理版本 3.9.32

    需要控制台代理才能在 AWS 中部署和管理Cloud Volumes ONTAP 。您将从安装在控制台代理实例上的软件登录到控制台。 AWS Secret Cloud 和 Top Secret Cloud 不支持控制台的 SaaS 网站。
- 了解私人模式

  在 AWS Secret Cloud 和 Top Secret Cloud 中，控制台以_私有模式_运行。在私人模式下，控制台与 SaaS 层没有连接。您可以通过可以访问控制台代理的本地基于 Web 的应用程序来访问控制台。

  要了解有关隐私模式工作原理的更多信息，请参阅"控制台中的私有部署模式"。

步骤 **1**：设置网络

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

步骤

1. 选择要在其中启动控制台代理实例和Cloud Volumes ONTAP实例的 VPC 和子网。
2. 确保您的 VPC 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
3. 设置 Amazon Simple Storage Service (Amazon S3) 服务的 VPC 端点。

   如果您想将冷数据从Cloud Volumes ONTAP到低成本对象存储，则需要 VPC 端点。

步骤 **2**：设置权限

设置 IAM 策略和角色，为控制台代理和Cloud Volumes ONTAP提供在 AWS Secret Cloud 或 Top Secret Cloud 中执行操作所需的权限。

您需要针对以下各项制定 IAM 策略和 IAM 角色：

- 控制台代理实例

- Cloud Volumes ONTAP实例
- 对于 HA 对， Cloud Volumes ONTAP HA 中介实例（如果您要部署 HA 对）

步骤

1. 转到 AWS IAM 控制台并单击 策略。
2. 为控制台代理实例创建策略。

> 您创建这些策略来支持 AWS 环境中的 S3 存储桶。稍后创建存储桶时，请确保存储桶名称以 `fabric-pool-`。此要求适用于 AWS Secret Cloud 和 Top Secret Cloud 区域。

秘密区域

```
{
    "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-b: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-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

绝密地区

```
{
    "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。

秘密区域

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

绝密地区

```
{
    "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"
    }]
}
```

对于 HA 对，如果您计划部署Cloud Volumes ONTAP HA 对，请为 HA 中介创建策略。

```
{
    "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": "*"
        }
    ]
}
```

4. 创建角色类型为 Amazon EC2 的 IAM 角色并附加您在前面步骤中创建的策略。

   创建角色：

   与策略类似，您应该为控制台代理设置一个 IAM 角色，为Cloud Volumes ONTAP节点设置一个 IAM 角色。对于 HA 对：与策略类似，您应该为控制台代理设置一个 IAM 角色，为Cloud Volumes ONTAP节点设置一个 IAM 角色，为 HA 中介设置一个 IAM 角色（如果您想要部署 HA 对）。

   选择角色：

   启动控制台代理实例时，必须选择控制台代理 IAM 角色。当您从控制台创建Cloud Volumes ONTAP系统时，您可以选择Cloud Volumes ONTAP的 IAM 角色。对于 HA 对，您可以在创建Cloud Volumes ONTAP系统时选择Cloud Volumes ONTAP和 HA 中介的 IAM 角色。

步骤 3：设置 AWS KMS

如果您想要将 Amazon 加密与Cloud Volumes ONTAP结合使用，请确保满足 AWS 密钥管理服务 (KMS) 的要求。

步骤

1. 确保您的账户或其他 AWS 账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 的账户不同的 AWS 账户中，则需要获取该密钥的 ARN。

   创建Cloud Volumes ONTAP系统时，您需要向控制台提供 ARN。

3. 将实例的 IAM 角色添加到 CMK 的密钥用户列表中。

这授予控制台使用 CMK 和Cloud Volumes ONTAP 的权限。

步骤 4：安装控制台代理并设置控制台

在开始使用控制台在 AWS 中部署Cloud Volumes ONTAP之前，您必须安装并设置控制台代理。它使控制台能够管理公共云环境（包括Cloud Volumes ONTAP）内的资源和流程。

步骤

1. 获取由证书颁发机构 (CA) 签名的、采用隐私增强邮件 (PEM) Base-64 编码 X.509 格式的根证书。请查阅您所在组织的政策和程序以获取证书。

   对于 AWS Secret Cloud 区域，您应该上传 `NSS Root CA 2`证书，对于 Top Secret Cloud，`Amazon Root CA 4`证书。确保仅上传这些证书而不是整个链。证书链文件较大，上传可能会失败。如果您有其他证书，您可以稍后上传，如下一步所述。

   您需要在设置过程中上传证书。控制台通过 HTTPS 向 AWS 发送请求时使用受信任的证书。

2. 启动控制台代理实例：
   a. 转到控制台的 AWS Intelligence Community Marketplace 页面。
   b. 在“自定义启动”选项卡上，选择从 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：

      - 我们推荐 t3.xlarge。
      - 您必须选择在设置权限时创建的 IAM 角色。
      - 您应该保留默认存储选项。
      - 控制台代理所需的连接方法如下：SSH、HTTP 和 HTTPS。
3. 从与实例有连接的主机设置控制台：
   a. 打开网络浏览器并输入 https://ipaddress其中 ipaddress 是安装控制台代理的 Linux 主机的 IP 地址。
   b. 指定用于连接 AWS 服务的代理服务器。
   c. 上传您在步骤 1 中获得的证书。
   d. 按照提示设置新系统。
      - 系统详细信息：输入控制台代理的名称和您的公司名称。
      - 创建管理员用户：为系统创建管理员用户。

        该用户帐户在系统本地运行。无法通过控制台连接到 auth0 服务。

      - 审核：审核详细信息，接受许可协议，然后选择*设置*。
   e. 要完成 CA 签名证书的安装，请从 EC2 控制台重新启动控制台代理实例。
4. 控制台代理重新启动后，使用您在安装向导中创建的管理员用户帐户登录。

步骤 **5**：（可选）安装私有模式证书

对于 AWS Secret Cloud 和 Top Secret Cloud 区域，此步骤是可选的，并且仅当您除了上一步中安装的根证书之外还有其他证书时才需要执行此步骤。

步骤

1. 列出现有安装的证书。
   a. 要收集 occm 容器 docker id（标识名称“ds-occm-1”），请运行以下命令：

   ```
   docker ps
   ```

   b. 要进入 occm 容器，请运行以下命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. 要从“TRUST_STORE_PASSWORD”环境变量收集密码，请运行以下命令：

   ```
   env
   ```

   d. 要列出信任库中所有已安装的证书，请运行以下命令并使用上一步收集的密码：

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 添加证书。
   a. 要收集 occm 容器 docker id（标识名称“ds-occm-1”），请运行以下命令：

   ```
   docker ps
   ```

   b. 要进入 occm 容器，请运行以下命令：

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   将新的证书文件保存在里面。

   c. 要从“TRUST_STORE_PASSWORD”环境变量收集密码，请运行以下命令：

   ```
   env
   ```

   d. 要将证书添加到信任库，请运行以下命令并使用上一步中的密码：

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 要检查证书是否已安装，请运行以下命令：

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. 要退出 occm 容器，请运行以下命令：

```
exit
```

g. 要重置 occm 容器，请运行以下命令：

```
docker restart <docker-id>
```

步骤 **6**：向控制台添加许可证

如果您从NetApp购买了许可证，则需要将其添加到控制台，以便在创建新的Cloud Volumes ONTAP系统时选择该许可证。在将这些许可证与新的Cloud Volumes ONTAP系统关联之前，它们将保持未分配状态。

步骤

1. 从左侧导航菜单中，选择*Licenses and subscriptions*。
2. 在 * Cloud Volumes ONTAP* 面板上，选择 查看。
3. 在 * Cloud Volumes ONTAP* 选项卡上，选择 许可证**>**基于节点的许可证。
4. 单击“未分配”。
5. 单击“添加未分配的许可证”。
6. 输入许可证的序列号或上传许可证文件。
7. 如果您还没有许可证文件，则需要从 netapp.com 手动上传许可证文件。
   a. 前往"NetApp许可证文件生成器"并使用您的NetApp支持站点凭据登录。
   b. 输入您的密码，选择您的产品，输入序列号，确认您已阅读并接受隐私政策，然后单击*提交*。
   c. 选择您是否希望通过电子邮件或直接下载接收 serialnumber.NLF JSON 文件。
8. 单击“添加许可证”。

结果

控制台会将许可证添加为未分配状态，直到您将其与新的Cloud Volumes ONTAP系统关联。您可以在左侧导航菜单的 **Licenses and subscriptions> Cloud Volumes ONTAP >** 查看 **>** 许可证 下看到许可证。

步骤 7：从控制台启动Cloud Volumes ONTAP

您可以通过在控制台中创建新系统来在 AWS Secret Cloud 和 Top Secret Cloud 中启动Cloud Volumes ONTAP 实例。

开始之前

对于 HA 对，需要密钥对来启用对 HA 中介的基于密钥的 SSH 身份验证。

步骤

1. 在“系统”页面上，单击“添加系统”。
2. 在“创建”下，选择Cloud Volumes ONTAP。

   对于 HA：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。

> 通过向导进行选择时，请不要选择*服务*下的*数据感知与合规性*和*备份到云*。在*预配置包*下，仅选择*更改配置*，并确保您没有选择任何其他选项。 AWS Secret Cloud 和 Top Secret Cloud 区域不支持预配置包，如果选择，您的部署将失败。

在多个可用区中部署**Cloud Volumes ONTAP HA** 的注意事项

完成 HA 对向导时请注意以下事项。

- 在多个可用区 (AZ) 中部署Cloud Volumes ONTAP HA 时，您应该配置一个传输网关。有关说明，请参阅"设置 AWS 中转网关"。
- 由于发布时 AWS Top Secret Cloud 中只有两个可用可用区，因此请按如下方式部署配置：
  - 节点 1：可用区 A
  - 节点 2：可用区 B
  - 调解员：可用区域 A 或 B

在单节点和 **HA** 节点中部署**Cloud Volumes ONTAP** 的注意事项

完成向导时请注意以下事项：

- 您应该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。如果您有使用自己的需求，可以参考下面的安全组部分。

- 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。

  您应该选择能够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，请参阅 AWS 文档。

- 磁盘大小是系统上所有磁盘的默认大小。

> 如果您稍后需要不同的大小，则可以使用高级分配选项来创建使用特定大小磁盘的聚合。

结果

Cloud Volumes ONTAP实例已启动。您可以在*审计*页面跟踪进度。

步骤 **8**：安装数据分层的安全证书

您需要手动安装安全证书才能在 AWS Secret Cloud 和 Top Secret Cloud 区域中启用数据分层。

开始之前

1. 创建 S3 存储桶。

> 确保存储桶名称带有前缀 `fabric-pool-.`例如 `fabric-pool-testbucket。

2. 保留您安装的根证书 `step 4`便利。

步骤

1. 复制您安装的根证书中的文本 `step 4`。
2. 使用 CLI 安全地连接到Cloud Volumes ONTAP系统。
3. 安装根证书。您可能需要按 `ENTER`多次键入：

```
security certificate install -type server-ca -cert-name <certificate-
name>
```

4. 出现提示时，输入复制的整个文本，包括 `----- BEGIN CERTIFICATE -----`到 `----- END CERTIFICATE -----`。
5. 保留 CA 签名的数字证书的副本以供将来参考。
6. 保留 CA 名称和证书序列号。
7. 为 AWS Secret Cloud 和 Top Secret Cloud 区域配置对象存储： `set -privilege advanced -confirmations off`
8. 运行此命令来配置对象存储。

> 所有 Amazon 资源名称 (ARN) 都应以 `-iso-b`， 例如 `arn:aws-iso-b`。例如，如果资源需要具有区域的 ARN，对于 Top Secret Cloud，请使用以下命名约定 `us-iso-b`对于 `-server`旗帜。对于 `AWS Secret Cloud`，使用 `us-iso-b-1`。

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 验证对象存储是否已成功创建： `storage aggregate object-store show -instance`
10. 将对象存储附加到聚合。对于每个新的聚合体都应重复此操作： `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`

开始使用 Microsoft Azure

了解 Azure 中的Cloud Volumes ONTAP部署选项

NetApp提供了两种在 Azure 上部署Cloud Volumes ONTAP 的选项。 Cloud Volumes ONTAP传统上依赖NetApp Console进行部署和编排。从Cloud Volumes ONTAP 9.16.1 开始，您可以利用 Azure 市场直接部署，这是一个简化的过程，可以访问有限但仍然强大的Cloud Volumes ONTAP功能和选项。

当您直接从 Azure 市场部署Cloud Volumes ONTAP时，您无需设置控制台代理或满足通过控制台部署Cloud Volumes ONTAP所需的其他安全和入职标准。从 Azure 市场，您只需单击几下即可快速部署Cloud Volumes ONTAP ，并在您的环境中探索其核心特性和功能。

在 Azure 市场完成部署后，您可以在控制台中发现这些系统。发现后，您可以将它们作为Cloud Volumes ONTAP系统进行管理，并利用所有控制台功能。请参阅"在控制台中发现已部署的系统" 。

以下是两个选项之间的功能比较。请注意，通过 Azure 市场部署的独立实例的功能在控制台中被发现时会发生变化。

	Azure 市场	**NetApp Console**
入职培训	更短、更简单，直接部署所需的准备工作最少	更长的入职流程，包括控制台代理的安装
支持的虚拟机 **(VM)** 类型	Eds_v5 和 Ls_v3 实例类型	全方位的 VM 类型。https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure 中支持的配置"^]
执照	免费许可证	任何基于容量的许可证。"Cloud Volumes ONTAP许可"
* NetApp支持*	不包括	根据许可证类型可用
容量	最多 500 GiB	可通过配置扩展
部署模型	单可用区（AZ）高可用（HA）模式部署	所有支持的配置，包括单节点和 HA 模式、单 AZ 和多 AZ 部署
支持的磁盘类型	高级 SSD v2 托管磁盘	更广泛的支持。"Cloud Volumes ONTAP的默认配置"
写入速度（快速写入模式）	不支持	根据您的配置，支持。"了解Cloud Volumes ONTAP中的写入速度" 。
编排功能	不可用	根据许可证类型，可通过NetApp Console获取

	Azure 市场	NetApp Console
支持的存储虚拟机数量	每个部署一个	根据您的配置，多个存储虚拟机。"支持的存储虚拟机数量"
更改实例类型	不支持	支持
* FabricPool分层*	不支持	支持

相关链接

- Azure 市场直接部署："从 Azure 市场部署Cloud Volumes ONTAP"
- 通过控制台部署："Azure 中的Cloud Volumes ONTAP快速入门"
- "NetApp Console文档"

开始使用NetApp Console

Azure 中的Cloud Volumes ONTAP快速入门

只需几个步骤即可开始使用Cloud Volumes ONTAP for Azure。


创建控制台代理

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

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


规划您的配置

控制台提供符合您的工作负载要求的预配置包，或者您可以创建自己的配置。如果您选择自己的配置，您应该了解可用的选项。有关信息，请参阅"在 Azure 中规划Cloud Volumes ONTAP配置"。


设置网络

1. 确保您的 VNet 和子网将支持控制台代理和Cloud Volumes ONTAP之间的连接。
2. 为NetApp AutoSupport启用从目标 VPC 的出站互联网访问。

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

"了解有关网络要求的更多信息" 。


启动Cloud Volumes ONTAP

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

相关链接

- "从控制台创建控制台代理"

- "从 Azure 市场创建控制台代理"
- "在 Linux 主机上安装控制台代理软件"
- "控制台如何处理权限"

在 **Azure** 中规划**Cloud Volumes ONTAP**配置

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

选择**Cloud Volumes ONTAP**许可证

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

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

选择支持的区域

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

选择受支持的 **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。

"Azure 中Cloud Volumes ONTAP支持的配置"

了解存储限制

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

"Azure 中Cloud Volumes ONTAP的存储限制"

在 **Azure** 中调整系统大小

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

虚拟机类型

查看受支持的虚拟机类型 "Cloud Volumes ONTAP发行说明"然后查看有关每种受支持的 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：内存优化虚拟机大小"

具有单节点系统的 **Azure** 磁盘类型

为Cloud Volumes ONTAP创建卷时，您需要选择Cloud Volumes ONTAP用作磁盘的底层云存储。

单节点系统可以使用以下类型的 Azure 托管磁盘：

- 高级 *SSD* 托管磁盘 以更高的成本为 I/O 密集型工作负载提供高性能。
- 与高级 SSD 托管磁盘相比，高级 *SSD v2* 托管磁盘 以更低的成本提供更高的性能和更低的延迟。
- _标准 SSD 托管磁盘_为需要低 IOPS 的工作负载提供一致的性能。
- 如果您不需要高 IOPS 并且想要降低成本，那么“标准 HDD 托管磁盘”是一个不错的选择。

有关这些磁盘用例的更多详细信息，请参阅 "Microsoft Azure 文档：Azure 中有哪些磁盘类型？"。

具有 **HA** 对的 **Azure** 磁盘类型

HA 系统使用高级 SSD 共享托管磁盘，它们都以更高的成本为 I/O 密集型工作负载提供高性能。 9.12.1 版本之前创建的 HA 部署使用高级页面 blob。

Azure 磁盘大小

启动Cloud Volumes ONTAP实例时，您必须选择聚合的默认磁盘大小。 NetApp Console将此磁盘大小用于初始聚合，以及使用简单配置选项时创建的任何其他聚合。您可以通过以下方式创建使用不同于默认磁盘大小的聚合："使用高级分配选项" 。

聚合中的所有磁盘必须具有相同的大小。

选择磁盘大小时，您应该考虑几个因素。磁盘大小会影响您支付的存储费用、您可以在聚合中创建的卷的大小、 Cloud Volumes ONTAP可用的总容量以及存储性能。

Azure Premium Storage 的性能与磁盘大小相关。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，但成本更高。

标准存储的磁盘大小之间没有性能差异。您应该根据所需的容量来选择磁盘大小。

请参阅 Azure 了解按磁盘大小划分的 IOPS 和吞吐量：

- "Microsoft Azure：托管磁盘定价"
- "Microsoft Azure：Page Blob 定价"

查看默认系统磁盘

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

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

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

收集网络信息

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

Azure 信息	你的价值
地区	

Azure 信息	你的价值
虚拟网络 (VNet)	
子网	
网络安全组（如果使用您自己的）	

选择写入速度

控制台使您能够选择Cloud Volumes ONTAP的写入速度设置。在选择写入速度之前，您应该了解正常设置和高设置之间的差异以及使用高写入速度时的风险和建议。"了解有关写入速度的更多信息"。

选择卷使用情况配置文件

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

NetApp存储效率功能具有以下优势：

精简配置

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

重复数据删除

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

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

为Cloud Volumes ONTAP设置 Azure 网络

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

Cloud Volumes ONTAP的要求

Azure 中必须满足以下网络要求。

出站互联网访问

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

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

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

端点	适用于	目的	部署模式	不可用时的影响
\ https://netapp-cloud-account.auth0.com	身份验证	用于控制台中的身份验证。	标准和限制模式。	用户身份验证失败，以下服务仍然不可用： • Cloud Volumes ONTAP服务 • ONTAP 服务 • 协议和代理服务
https://vault.azure.net	密钥保管库	用于在使用客户管理密钥 (CMK) 时从 Azure Key Vault 检索客户端密钥。	标准、受限和私人模式。	Cloud Volumes ONTAP服务不可用。
\ https://api.bluexp.netapp.com/tenancy	租户	用于从控制台检索Cloud Volumes ONTAP资源以授权资源和用户。	标准和限制模式。	Cloud Volumes ONTAP资源和用户未获得授权。
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	用于将AutoSupport遥测数据发送给NetApp支持。	标准和限制模式。	AutoSupport信息仍未送达。
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	公共区域	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	中国区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。

端点	适用于	目的	部署模式	不可用时的影响
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	德国地区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	政府区域	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	政府国防部地区	与 Azure 服务通信。	标准、受限和私人模式。	Cloud Volumes ONTAP无法与 Azure 服务通信以对 Azure 中的控制台执行特定操作。

NetApp Console代理的网络代理配置

您可以使用NetApp Console代理的代理服务器配置来启用来自Cloud Volumes ONTAP 的出站互联网访问。控制台支持两种类型的代理：

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

有关配置代理服务器的信息，请参阅 "配置控制台代理以使用代理服务器"。

IP 地址

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

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

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

单节点系统的 **IP** 地址

Console 为单节点系统分配 5 或 6 个 IP 地址：

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

> iSCSI IP 通过 iSCSI 协议提供客户端访问。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。

- SVM 管理（可选 - 默认未配置）

HA 对的 **IP** 地址

控制台在部署期间将 IP 地址分配给 4 个 NIC（每个节点）。

请注意，Console 在 HA 对上创建 SVM 管理 LIF，但不在 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 通过 iSCSI 协议提供客户端访问。系统还将其用于其他重要的网络工作流程。此 LIF 是必需的，不应删除。

NIC1

- 集群网络IP

NIC2

- 集群互连 IP (HA IC)

NIC3

- Pageblob NIC IP（磁盘访问）

NIC3 仅适用于使用页 Blob 存储的 HA 部署。

上述 IP 地址在故障转移事件中不会迁移。

此外，还配置了 4 个前端 IP（FIP）以在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
- NodeA 数据 IP (NFS/CIFS)
- NodeB数据IP（NFS/CIFS）
- SVM 管理 IP

与 **Azure** 服务的安全连接

默认情况下，控制台启用 Azure 专用链接，用于Cloud Volumes ONTAP和 Azure 页 Blob 存储帐户之间的连接。

在大多数情况下，您无需执行任何操作 - 控制台会为您管理 Azure 专用链接。但是如果您使用 Azure 私有 DNS，则需要编辑配置文件。您还应该了解 Azure 中控制台代理的位置要求。

如果您的业务需要，您还可以禁用专用链接连接。如果禁用该链接，控制台会将Cloud Volumes ONTAP配置为使用服务端点。

"了解有关将 Azure Private Links 或服务端点与Cloud Volumes ONTAP结合使用的更多信息" 。

用于 **Azure VNet** 加密的网络

Cloud Volumes ONTAP 支持 "Azure 虚拟网络 (VNet) 加密"对 VNet 内部或跨对等 VNet 的 VM 到 VM 流量进行加密。此功能在 Azure VNet 层配置，独立于 Cloud Volumes ONTAP 拓扑（单节点或 HA）。

只需确保在虚拟机的 NIC 上启用加速网络，并在启用该功能之前查看 Azure VNet 加密要求和限制即可。不应修改 NetApp 托管负载平衡器对象。

"Azure 文档：VNet 加密和 Accelerated Networking"。

与其他**ONTAP**系统的连接

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

有关说明，请参阅 "Microsoft Azure 文档：在 Azure 门户中创建站点到站点连接"。

HA 互连端口

Cloud Volumes ONTAP HA 对包括 HA 互连，这使得每个节点能够持续检查其伙伴节点是否正常运行，并为对方的非易失性存储器镜像日志数据。 HA 互连使用 TCP 端口 10006 进行通信。

默认情况下，HA 互连 LIF 之间的通信是开放的，并且此端口没有安全组规则。但是，如果您在 HA 互连 LIF 之间创建防火墙，则需要确保 TCP 流量对端口 10006 开放，以便 HA 对可以正常运行。

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 对使用一个专用资源组。一个资源组中仅支持一个 HA 对。

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

安全组规则

控制台创建 Azure 安全组，其中包括Cloud Volumes ONTAP成功运行的入站和出站规则。 "查看控制台代理的安全组规则" 。

Cloud Volumes ONTAP的 Azure 安全组需要打开适当的端口以进行节点之间的内部通信。 "了解ONTAP内部端口" 。

我们不建议修改预定义的安全组或使用自定义安全组。但是，如果必须这样做，请注意，部署过程要求Cloud Volumes ONTAP系统在其自己的子网内拥有完全访问权限。部署完成后，如果决定修改网络安全组，请确保保持集群端口和 HA 网络端口开放。这确保了Cloud Volumes ONTAP集群内的无缝通信（节点之间的任意通信）。

单节点系统的入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

- 仅限选定的 **VNet**：入站流量的来源是Cloud Volumes ONTAP系统的 VNet 子网范围和控制台代理所在的 VNet 子网范围。这是推荐的选项。
- 所有 **VNets**：入站流量的来源是 0.0.0.0/0 IP 范围。
- 已禁用：此选项限制对您的存储帐户的公共网络访问，并禁用Cloud Volumes ONTAP系统的数据分层。如果由于安全法规和政策，您的私有 IP 地址即使在同一个 VNet 内也不应该暴露，那么建议使用此选项。

优先级和名称	端口和协议	来源和目的地	描述
1000 入站_ssh	22 TCP	任意到任意	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
1001 入站 http	80 TCP	任意到任意	使用集群管理 LIF 的 IP 地址通过 HTTP 访问ONTAP System Manager Web 控制台
1002 inbound_111_tcp	111 TCP	任意到任意	NFS 的远程过程调用
1003 inbound_111_udp	111 UDP	任意到任意	NFS 的远程过程调用
1004 inbound_139	139 TCP	任意到任意	CIFS 的 NetBIOS 服务会话
1005 入站_161-162 _tcp	161-162 TCP	任意到任意	简单网络管理协议
1006 入站_161-162 _udp	161-162 UDP	任意到任意	简单网络管理协议

优先级和名称	端口和协议	来源和目的地	描述
1007 inbound_443	443 TCP	任意到任意	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
1008 inbound_445	445 TCP	任意到任意	使用 NetBIOS 框架的 TCP 上的 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意到任意	NFS 挂载
1010 inbound_635_udp	635 UDP	任意到任意	NFS 挂载
1011 inbound_749	749 TCP	任意到任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意到任意	NFS 服务器守护进程
1013 inbound_2049_udp	2049 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 入站_4045-4046_tcp	4045-4046 TCP	任意到任意	NFS 锁定守护进程和网络状态监视器
1016 入站_4045-4046_udp	4045-4046 UDP	任意到任意	NFS 锁定守护进程和网络状态监视器
1017 inbound_10000	10000 TCP	任意到任意	使用 NDMP 备份
1018 入站_11104-11105	11104-11105 TCP	任意到任意	SnapMirror数据传输
3000 入站拒绝 _所有_tcp	任意端口 TCP	任意到任意	阻止所有其他 TCP 入站流量
3001 入站拒绝 _所有 udp	任意端口 UDP	任意到任意	阻止所有其他 UDP 入站流量
65000 允许 VnetInBound	任意端口任意协议	虚拟网络到虚拟网络	来自 VNet 内部的入站流量
65001 允许 Azure 负载均衡器入站	任意端口任意协议	AzureLoadBalancer 到任意	来自 Azure 标准负载均衡器的数据流量
65500 拒绝所有入站	任意端口任意协议	任意到任意	阻止所有其他入站流量

HA 系统的入站规则

添加Cloud Volumes ONTAP系统并选择预定义安全组时，您可以选择允许以下之一内的流量：

- 仅限选定的 **VNet**：入站流量的来源是Cloud Volumes ONTAP系统的 VNet 子网范围和控制台代理所在的 VNet 子网范围。这是推荐的选项。
- 所有 **VNets**：入站流量的来源是 0.0.0.0/0 IP 范围。

HA 系统的入站规则少于单节点系统，因为入站数据流量通过 Azure Standard Load Balancer。因此，应打开来自 Load Balancer 的流量，如"AllowAzureLoadBalancerInBound"规则中所示。

- 已禁用：此选项限制对您的存储帐户的公共网络访问，并禁用Cloud Volumes ONTAP系统的数据分层。如果

由于安全法规和政策，您的私有 IP 地址即使在同一个 VNet 内也不应该暴露，那么建议使用此选项。

优先级和名称	端口和协议	来源和目的地	描述
100 inbound_443	443 任何协议	任意到任意	使用集群管理 LIF 的 IP 地址与控制台代理建立连接并通过 HTTPS 访问ONTAP System Manager Web 控制台
101 inbound_111_tcp	111 任何协议	任意到任意	NFS 的远程过程调用
102 inbound_2049_tcp	2049 任何协议	任意到任意	NFS 服务器守护进程
111 入站_ssh	22 任何协议	任意到任意	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
121 inbound_53	53 任何协议	任意到任意	DNS 和 CIFS
65000 允许 VnetInBound	任意端口任意协议	虚拟网络到虚拟网络	来自 VNet 内部的入站流量
65001 允许 Azure 负载均衡器入站	任意端口任意协议	AzureLoadBalancer 到任意	来自 Azure 标准负载均衡器的数据流量
65500 拒绝所有入站	任意端口任意协议	任意到任意	阻止所有其他入站流量

出站规则

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

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

端口	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

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

源是Cloud Volumes ONTAP系统上的接口（IP 地址）。

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

服务	端口	协议	源	目标	目的
配置备份	HTTP	80	节点管理 LIF	http://<控制台代理 IP 地址>/occm/offboxconfig	将配置备份发送到控制台代理。"ONTAP 文档" 。
DHCP	68	UDP	节点管理 LIF	DHCP	首次设置的 DHCP 客户端
DHCP服务	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 拷贝
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	SnapMirror集群间通信会话的管理
	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	Syslog 转发消息

控制台代理的要求

如果您尚未创建控制台代理，您也应该查看控制台代理的网络要求。

- "查看控制台代理的网络要求"
- "Azure 中的安全组规则"

相关主题

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

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

使用带有 Microsoft 管理密钥的 Azure 存储服务加密，数据在 Azure 中的Cloud Volumes ONTAP上自动加密。但是您可以按照本页上的步骤使用您自己的加密密钥。

数据加密概述

Cloud Volumes ONTAP数据在 Azure 中自动使用 "Azure 存储服务加密"。默认实现使用 Microsoft 管理的密钥。无需设置。

如果您想将客户管理的密钥与Cloud Volumes ONTAP一起使用，则需要完成以下步骤：

1. 从 Azure 创建一个密钥保管库，然后在该保管库中生成一个密钥。
2. 从NetApp Console，使用 API 创建使用密钥的Cloud Volumes ONTAP系统。

数据如何加密

控制台使用磁盘加密集，从而可以通过托管磁盘而不是页面 blob 来管理加密密钥。任何新的数据磁盘也使用相同的磁盘加密集。较低版本将使用 Microsoft 管理的密钥，而不是客户管理的密钥。

创建配置为使用客户管理密钥的Cloud Volumes ONTAP系统后， Cloud Volumes ONTAP数据将按如下方式加密。

Cloud Volumes ONTAP配置	用于密钥加密的系统磁盘	用于密钥加密的数据磁盘
单节点	• 引导 • 核 • NVRAM	• 根 • 数据
具有页 Blob 的 Azure HA 单可用性区域	• 引导 • 核 • NVRAM	无
具有共享托管磁盘的 Azure HA 单可用性区域	• 引导 • 核 • NVRAM	• 根 • 数据
具有共享托管磁盘的 Azure HA 多个可用性区域	• 引导 • 核 • NVRAM	• 根 • 数据

Cloud Volumes ONTAP的所有 Azure 存储帐户均使用客户管理的密钥加密。如果您想在创建存储帐户期间对其进行加密，则必须在Cloud Volumes ONTAP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，存储帐户仍将被加密，但控制台首先使用 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。

Cloud Volumes ONTAP中的密钥轮换

配置加密密钥时，必须使用 Azure 门户来设置并启用自动密钥轮换。创建并启用新版本的加密密钥可确保Cloud Volumes ONTAP可以自动检测并使用最新的密钥版本进行加密，从而确保您的数据保持安全而无需人工干预。

有关配置密钥和设置密钥轮换的信息，请参阅以下 Microsoft Azure 文档主题：

- "在 Azure Key Vault 中配置加密密钥自动轮换"
- "Azure PowerShell - 启用客户管理的密钥"

配置密钥后，请确保已选择 "启用自动旋转"，以便Cloud Volumes ONTAP可以在之前的密钥过期时使用新的密钥。如果您未在 Azure 门户上启用此选项， Cloud Volumes ONTAP将无法自动检测新密钥，这可能会导致存储配置问题。

创建用户分配的托管标识

您可以选择创建称为用户分配的托管标识的资源。这样做可以让您在创建Cloud Volumes ONTAP系统时加密您的存储帐户。我们建议在创建密钥保管库和生成密钥之前创建此资源。

该资源具有以下 ID： `userassignedidentity` 。

步骤

1. 在 Azure 中，转到 Azure 服务并选择 托管标识。
2. 单击“创建”。
3. 提供以下详细信息：
   - 订阅：选择订阅。我们建议选择与控制台代理的订阅相同的订阅。
   - 资源组：使用现有资源组或创建一个新的资源组。
   - 区域：可选，选择与控制台代理相同的区域。
   - 名称：输入资源的名称。
4. （可选）添加标签。
5. 单击“创建”。

创建密钥保管库并生成密钥

密钥保管库必须位于您计划创建Cloud Volumes ONTAP系统的同一 Azure 订阅和区域中。

如果你创建了用户分配的托管标识，在创建密钥保管库时，还应该为密钥保管库创建访问策略。

步骤

1. "在 Azure 订阅中创建密钥保管库" 。

   请注意密钥保管库的以下要求：

   - 密钥保管库必须与Cloud Volumes ONTAP系统位于同一区域。
   - 应启用以下选项：
     - 软删除（此选项默认启用，但不能禁用）
     - 清除保护
     - 用于卷加密的 **Azure Disk Encryption**（适用于单节点系统、多个区域中的 HA 对和 HA 单 AZ 部署）

       使用 Azure 客户管理加密密钥的前提是为密钥保管库启用 Azure 磁盘加密。
   - 如果创建了用户分配的托管标识，则应启用以下选项：
     - 保险库访问政策

2. 如果选择了“保管库访问策略”，请单击“创建”为密钥保管库创建访问策略。如果没有，请跳至步骤 3。
   a. 选择以下权限：
      - 得到
      - 列表
      - 解密
      - 加密
      - 解开密钥
      - 包装键
      - 核实
      - 符号
   b. 选择用户分配的托管标识（资源）作为主体。
   c. 审查并创建访问策略。
3. "在密钥保管库中生成密钥" 。

   请注意以下密钥要求：

   - 密钥类型必须是*RSA*。
   - 建议的 RSA 密钥大小为 **2048**，但也支持其他大小。

创建使用加密密钥的系统

创建密钥保管库并生成加密密钥后，您可以创建配置为使用该密钥的新Cloud Volumes ONTAP系统。这些步骤通过使用 API 来支持。

所需权限

如果要在单节点Cloud Volumes ONTAP系统中使用客户管理密钥，请确保控制台代理具有以下权限：

```
"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 API 调用获取 Azure 订阅中的密钥保管库列表。

   对于 HA 对： `GET /azure/ha/metadata/vaults`

对于单节点： `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 API 调用获取保管库中的密钥列表。

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

对于单节点： `GET /azure/vsa/metadata/keys-vault`

记下*keyName*。您需要在下一步中指定该值（以及保险库名称）。

"了解有关此 API 调用的更多信息"。

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

a. 对于 HA 对：

`POST /azure/ha/working-environments`

请求主体必须包含以下字段：

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

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您创建此资源是为了用于存储帐户加密，则字段。

"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`

请求主体必须包含以下字段：

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

包括 `"userAssignedIdentity": " userAssignedIdentityId"`如果您创建此资源是为了用于存储帐户加密，则字段。

"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** 中设置**Cloud Volumes ONTAP**许可

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

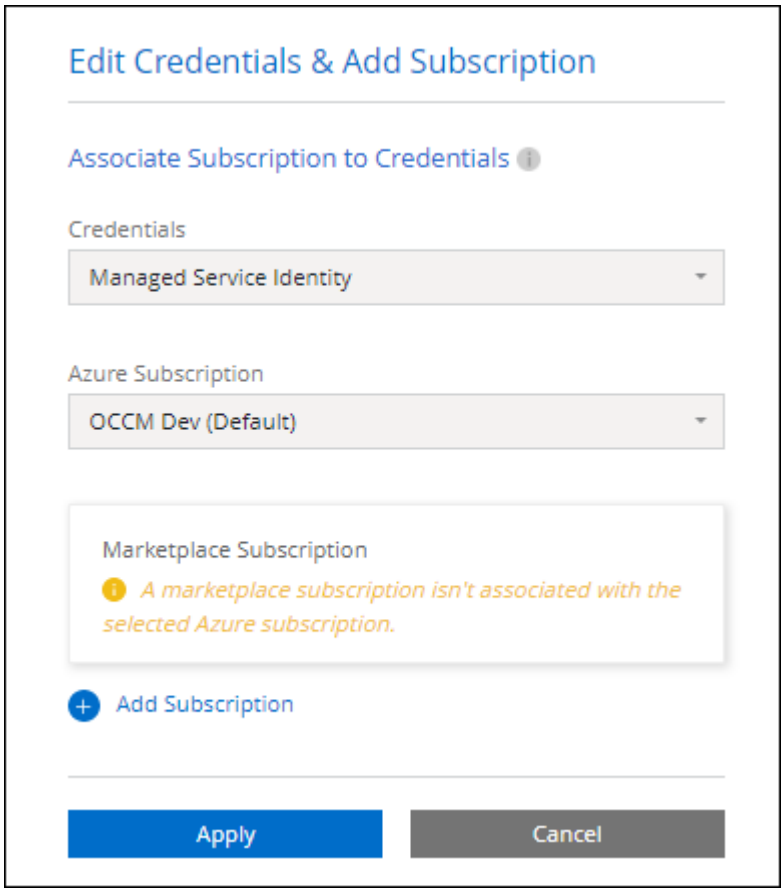
免费增值

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

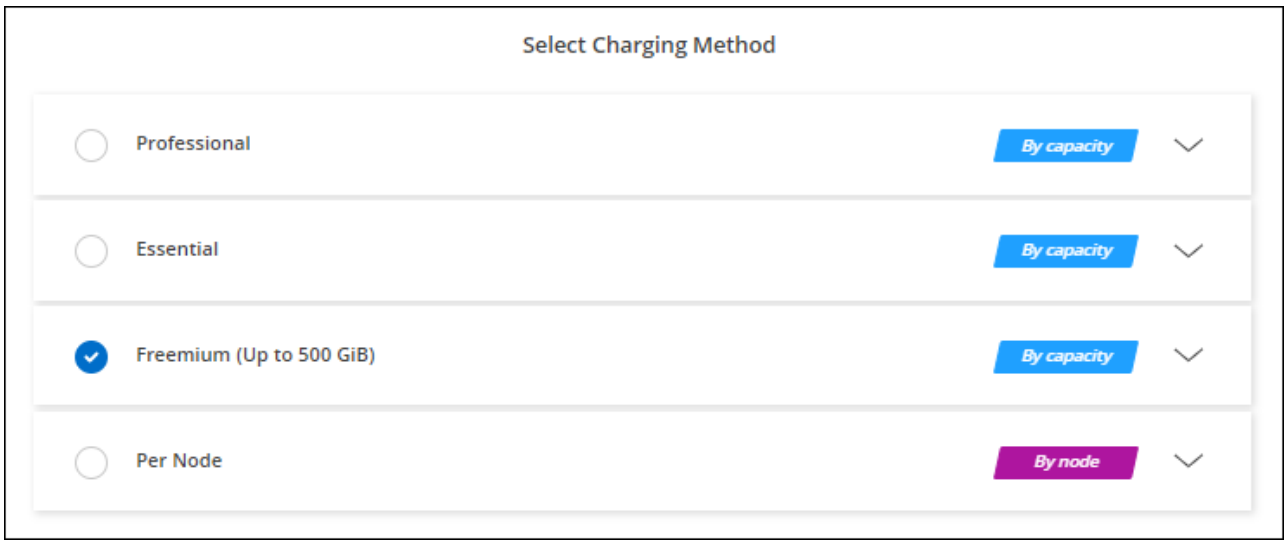
步骤

1. 从NetApp Console的左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。

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



a. 返回控制台后，到达收费方式页面时选择“免费增值”。



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

基于容量的许可证

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

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

- 从NetApp购买的许可证（自带许可证 (BYOL)）
- Azure 市场提供的按小时付费 (PAYGO) 订阅
- 年度合同

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

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

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

步骤

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

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

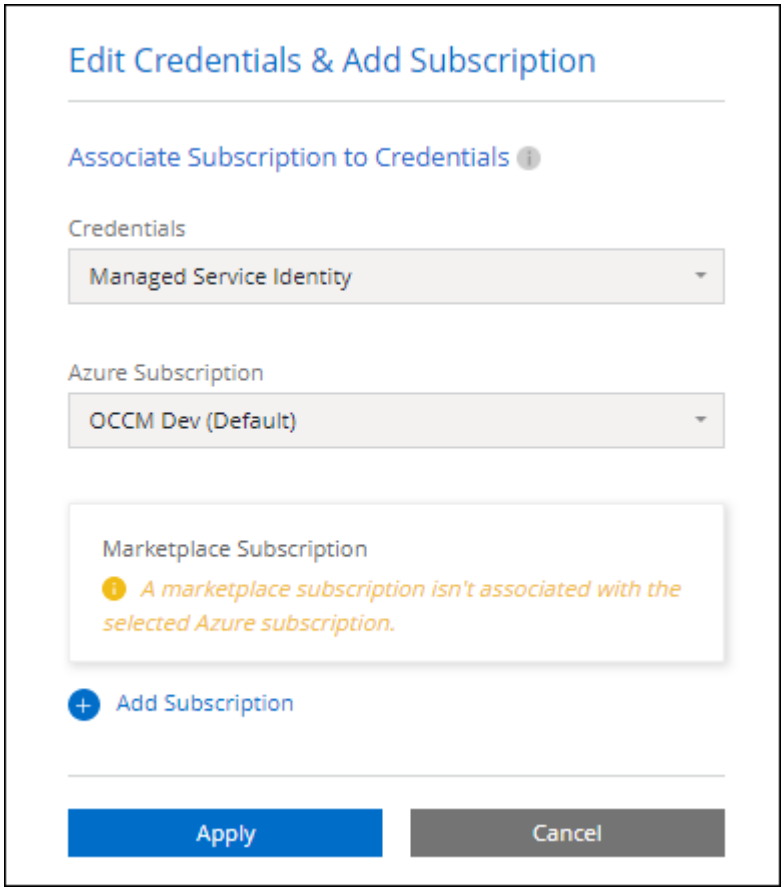
   您必须先从控制台获取许可证，然后才能将其与Cloud Volumes ONTAP一起使用。如果需要的话，你可以"

手动将许可证添加到控制台"。

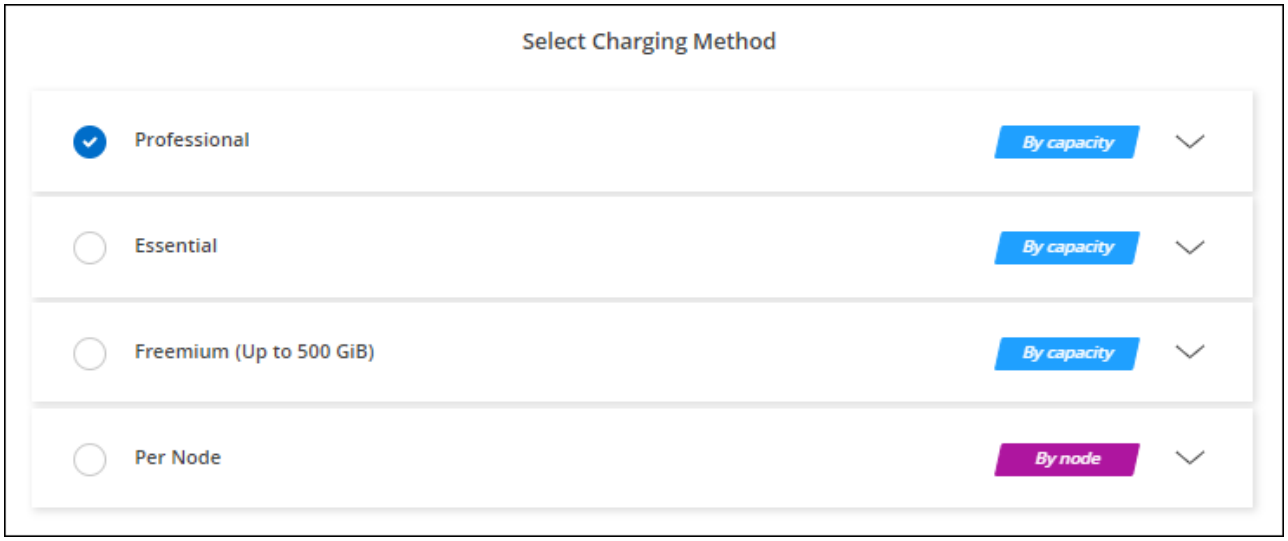
3. 在*系统*页面上，单击*添加系统*并按照步骤操作。

   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。

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



   a. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

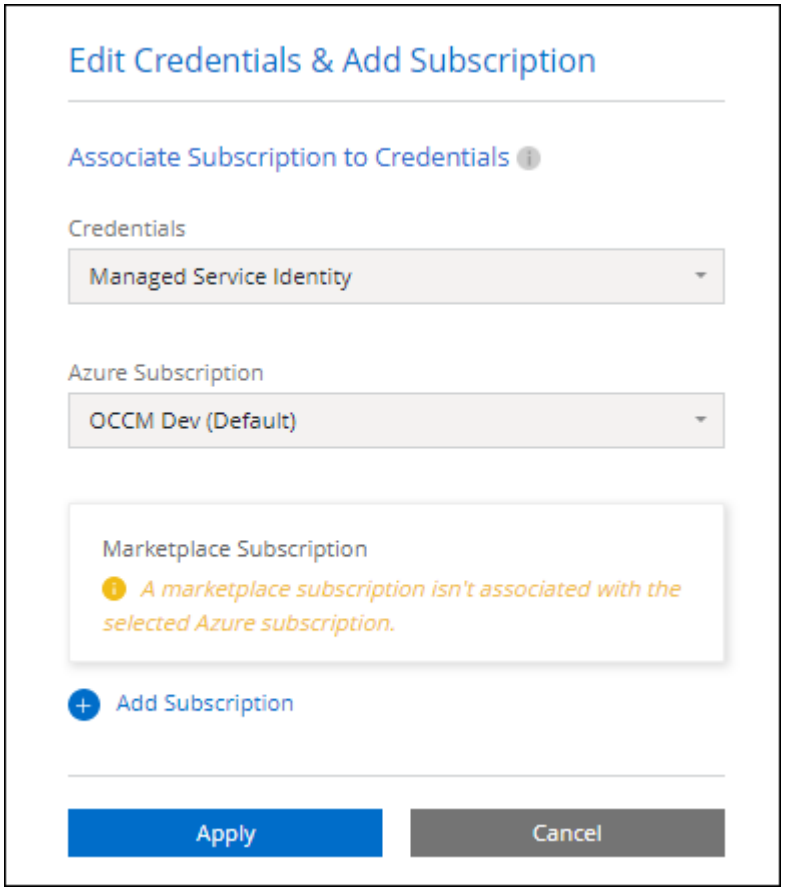
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

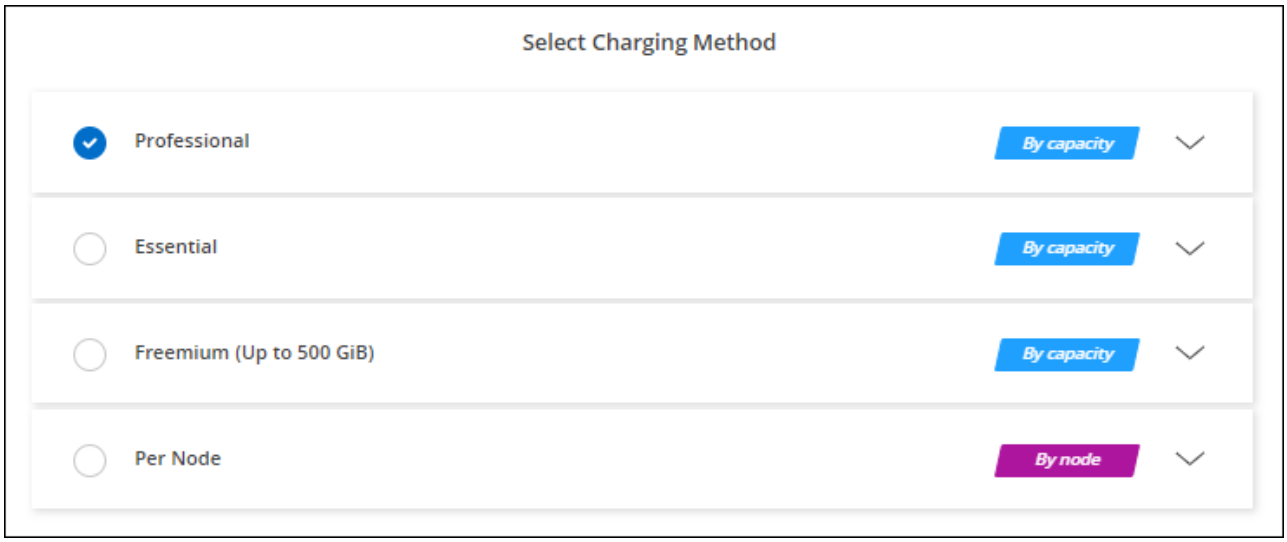
当您创建Cloud Volumes ONTAP系统时，控制台会提示您订阅 Azure 市场中提供的协议。然后将该订阅与系统关联以进行收费。您可以将同一订阅用于其他系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”，然后按照提示订阅 Azure 市场中的即用即付产品。



   b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

您可以从“设置”>“凭据”页面管理与您的 Azure 帐户关联的 Azure 市场订阅。 "了解如何管理 Azure 帐户和订阅"

年度合同

通过购买年度合同每年支付Cloud Volumes ONTAP 的费用。

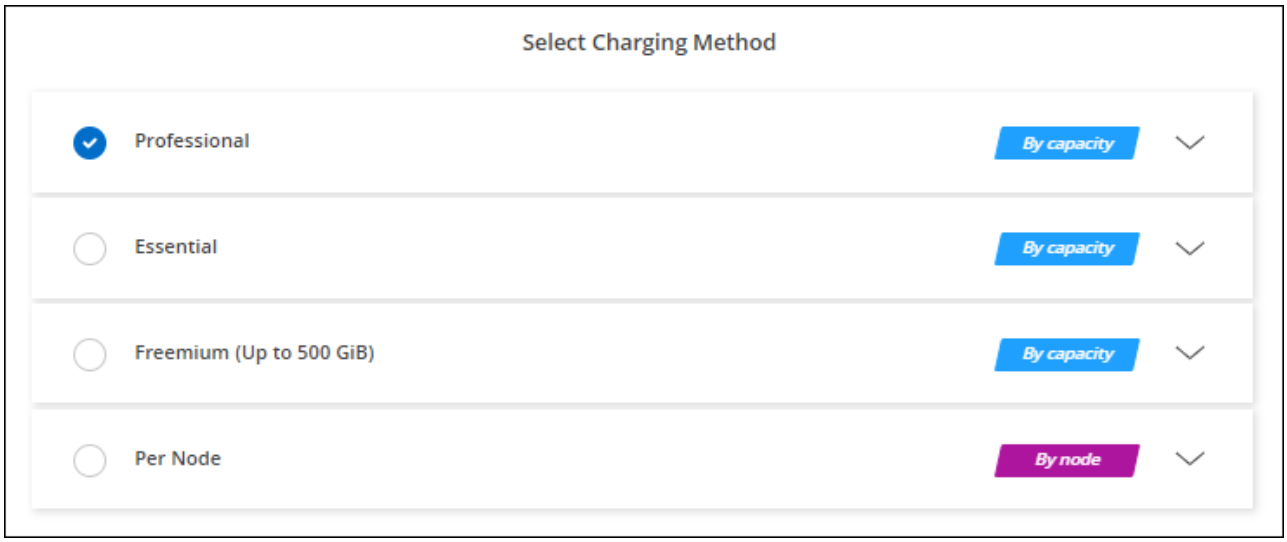
步骤

1. 联系您的NetApp销售代表购买年度合同。

   该合同在 Azure 市场中以私人优惠的形式提供。

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

2. 在*系统*页面上，单击*添加系统*并按照步骤操作。
   a. 在“详细信息和凭据”页面上，单击“编辑凭据”>“添加订阅”>“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. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



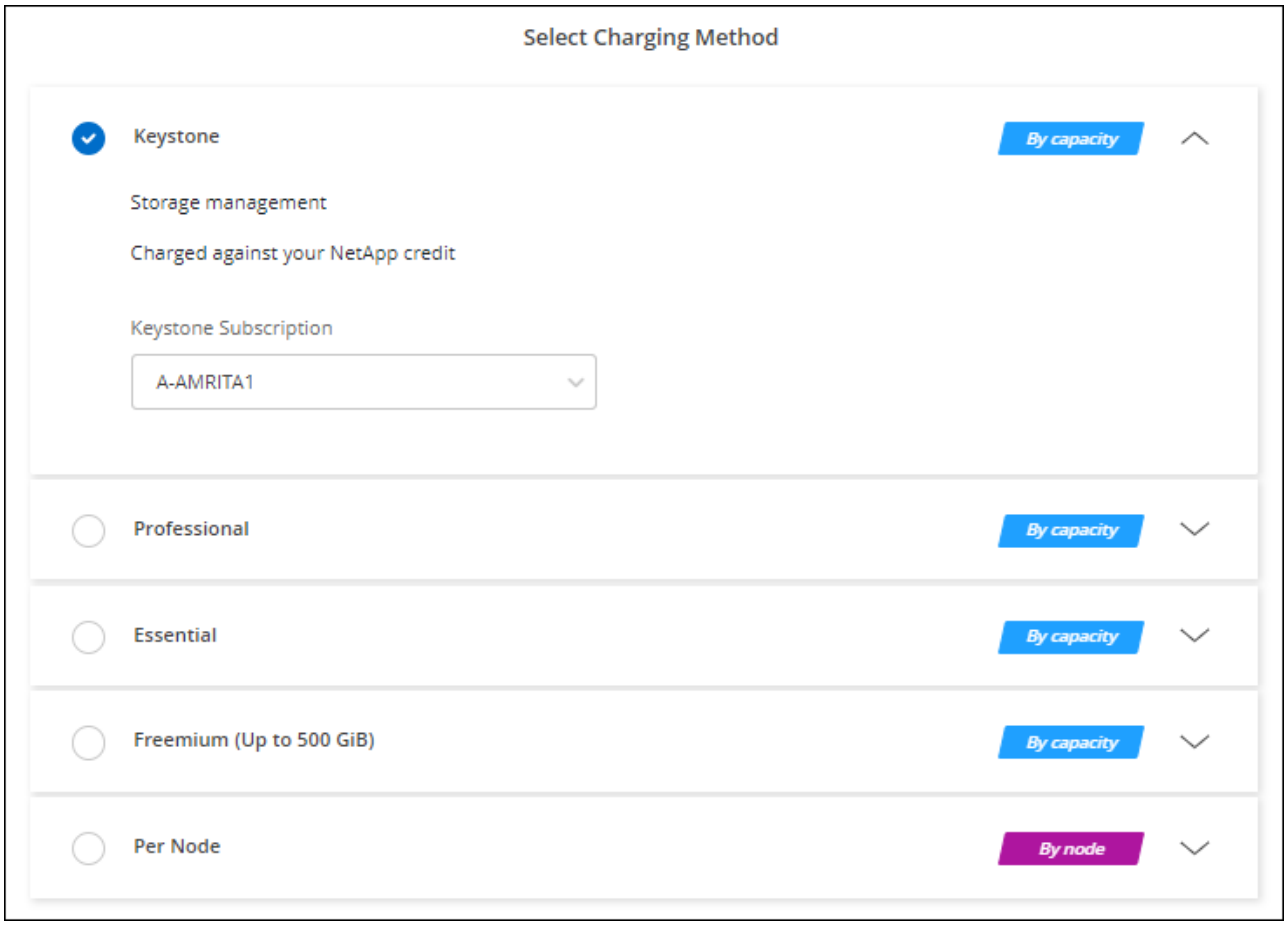
"查看在 Azure 中启动Cloud Volumes ONTAP 的分步说明" 。

Keystone订阅

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

步骤

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



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

基于节点的许可证

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

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

在 **Azure** 中为**Cloud Volumes ONTAP**启用高可用性模式

您应该启用 Microsoft Azure 的高可用性 (HA) 模式，以减少计划外故障转移时间，并为 Cloud Volumes ONTAP 启用 NFSv4 支持。如果启用此模式，您的 Cloud Volumes ONTAP HA 节点可以在 CIFS 和 NFSv4 客户端上的计划外故障转移期间实现较低（60 秒）的恢复时间目标 (RTO)。

从Cloud Volumes ONTAP 9.10.1 开始，我们减少了在 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用于Cloud Volumes ONTAP，您需要在 Azure 订阅上启用高可用性功能。

关于此任务

当需要在 Azure 订阅上启用此功能时，NetApp Console 会提示您这些详细信息。请注意以下事项：

- 您的Cloud Volumes ONTAP HA 对的高可用性没有问题。此 Azure 功能与ONTAP协同工作，以减少客户端观察到的因计划外故障转移事件导致的 NFS 协议应用程序中断时间。
- 启用此功能不会对Cloud Volumes ONTAP HA 对造成破坏。
- 在您的 Azure 订阅上启用此功能不会给其他虚拟机带来问题。
- Cloud Volumes ONTAP在 CIFS 和 NFS 客户端上的集群和 SVM 管理 LIF 故障转移期间使用内部 Azure 负载均衡器。
- 启用 HA 模式后，控制台每 12 小时扫描一次系统以更新内部 Azure 负载均衡器规则。

步骤

具有 *Owner* 权限的 Azure 用户可以从 Azure CLI 启用该功能。

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）验证该功能现在是否已注册：

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

Azure CLI 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"
}
```

相关链接

1. "Microsoft Azure 文档：高可用性端口概述"

2. "Microsoft Azure 文档：Azure CLI 入门"

在 **Azure** 中为**Cloud Volumes ONTAP**启用 **VMOrchestratorZonalMultiFD**

要在本地冗余存储 (LRS) 单可用区 (AZ) 中部署虚拟机实例，您应该激活 Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD`您的订阅功能。在高可用性 (HA) 模式下，此功能有助于在同一可用区域内的不同故障域中部署节点。

除非您激活此功能，否则不会发生区域部署，并且之前的 LRS 非区域部署将生效。

有关在单个可用区域中部署虚拟机的信息，请参阅"Azure 中的高可用性对"。

以具有“所有者”权限的用户身份执行以下步骤：

步骤

1. 从 Azure 门户访问 Azure Cloud Shell。欲了解更多信息，请参阅 "Microsoft Azure 文档：Azure Cloud Shell 入门"。
2. 注册 `Microsoft.Compute/VMOrchestratorZonalMultiFD`通过运行以下命令来启用此功能：

   ```
   az 帐户设置 -s <Azure_subscription_name_or_ID> az 功能注册 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
   ```

3. 验证注册状态及输出样例：

   ```
   az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { “id”：“/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD”， “name”：“Microsoft.Compute/VMOrchestratorZonalMultiFD”， “properties”：{ “state”：“Registered” }，“type”：“Microsoft.Features/providers/features” }
   ```

在 **Azure** 中启动**Cloud Volumes ONTAP**

您可以通过在 NetApp Console 中创建 Cloud Volumes ONTAP 系统来在 Azure 中启动单节点系统或 HA 对。

开始之前

开始之前您需要以下内容。

- 已启动并正在运行的控制台代理。
  - 你应该有一个 "与您的系统关联的控制台代理"。
  - "您应该准备好让控制台代理始终处于运行状态" 。
- 了解您想要使用的配置。

  您应该有一个配置计划，并且从管理员那里获得必要的 Azure 网络详细信息。有关详细信息，请参阅"规划您的Cloud Volumes ONTAP配置" 。

- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。

关于此任务

当控制台在 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。

> 数据丢失的可能性
>
> 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，不建议在现有的共享资源组中部署Cloud Volumes ONTAP 。虽然控制台可以在部署失败或删除的情况下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，需要在 Console 中创建单节点系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 选择位置：选择*Microsoft Azure*和* Cloud Volumes ONTAP单节点*。
4. 如果出现提示， "创建控制台代理" 。
5. 详细信息和凭据：可选择更改 Azure 凭据和订阅，指定群集名称，根据需要添加标签，然后指定凭据。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Azure 虚拟机。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
资源组标签	标签是 Azure 资源的元数据。当您在此字段中输入标签时，控制台会将它们添加到与Cloud Volumes ONTAP系统关联的资源组中。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Microsoft Azure 文档：使用标签来组织您的 Azure 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	您可以选择不同的 Azure 凭据和不同的 Azure 订阅来与此Cloud Volumes ONTAP系统一起使用。您需要将 Azure 市场订阅与选定的 Azure 订阅关联，以便部署即用即付的Cloud Volumes ONTAP系统。 "了解如何添加凭证" 。

6. 服务：启用或禁用您想要或不想与Cloud Volumes ONTAP一起使用的单个服务。
   - "了解有关NetApp Data Classification的更多信息"

- "了解有关NetApp Backup and Recovery的更多信息"

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

7. 位置：选择区域、可用区域、VNet 和子网，然后选中复选框以确认控制台代理和目标位置之间的网络连接。

对于中国区域，仅Cloud Volumes ONTAP 9.12.1 GA 和 9.13.0 GA 支持单节点部署。您可以将这些版本升级到Cloud Volumes ONTAP的更高补丁和版本，如下所示"Azure 中支持"。如果您想在中国地区部署更高版本的Cloud Volumes ONTAP ，请联系NetApp支持。中国地区仅支持直接从NetApp购买的许可证，不提供市场订阅。

8. 连接：选择一个新的或现有的资源组，然后选择是否使用预定义的安全组或使用您自己的安全组。

下表描述了您可能需要指导的字段：

字段	描述
资源组	为Cloud Volumes ONTAP创建新的资源组或使用现有的资源组。最佳做法是为Cloud Volumes ONTAP使用新的专用资源组。虽然可以在现有的共享资源组中部署Cloud Volumes ONTAP ，但由于存在数据丢失的风险，因此不建议这样做。请参阅上面的警告以了解更多详细信息。 如果您使用的 Azure 帐户具有 "所需权限"，如果部署失败或删除，控制台会从资源组中删除Cloud Volumes ONTAP资源。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果选择*仅限选定的 VNet*，则入站流量的来源是选定 VNet 的子网范围和控制台代理所在的 VNet 的子网范围。这是推荐的选项。 • 如果选择“所有 **VNets**”，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的	如果您选择现有的安全组，则它必须满足Cloud Volumes ONTAP要求。"查看默认安全组" 。

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

如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

11. 许可：如果需要，更改Cloud Volumes ONTAP版本，并选择虚拟机类型。

如果所选版本有较新的候选版本、通用版本或补丁版本，则BlueXP会在创建工作环境时将系统更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.16.1 P3 并且 9.16.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 - 例如，从 9.15 到 9.16。

12. 从 **Azure** 市场订阅：如果控制台无法启用Cloud Volumes ONTAP的编程部署，您将看到此页面。按照屏幕上列出的步骤操作。请参阅 "以编程方式部署 Marketplace 产品"了解更多信息。
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数据分层到 Blob 存储。

    请注意以下事项：

    - 如果在 VNet 中禁用了对您的存储帐户的公共访问，则您无法在Cloud Volumes ONTAP系统中启用数据分层。有关信息，请参阅"安全组规则"。
    - 磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。
    - 磁盘大小适用于初始聚合中的所有磁盘以及使用简单配置选项时控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

      有关选择磁盘类型和大小的帮助，请参阅"在 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。
    - 如果您禁用数据分层，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. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       此选项仅适用于某些 VM 类型。要了解受支持的 VM 类型，请参阅"HA 对许可证支持的配置"。

       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，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。
15. 创建卷：输入新卷的详细信息或单击*跳过*。

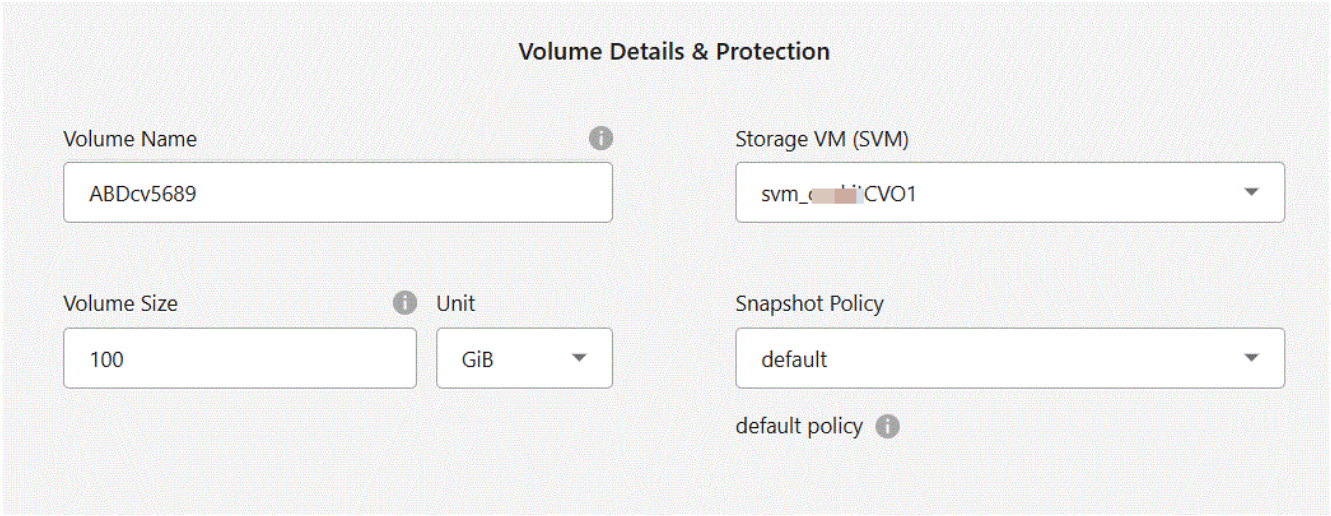
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。

字段	描述
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 策略	Snapshot 副本策略指定自动创建的NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 TCP 卸载引擎 (TOE) 卡、融合网络适配器 (CNA) 或专用主机总线适配器 (HBA) 连接到网络，并通过 iSCSI 限定名称 (IQN) 进行标识。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



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

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。

字段	描述
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Azure AD 域服务配置为Cloud Volumes ONTAP 的AD 服务器，您应该在此字段中输入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

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更改卷分层策略（如果需要）。

    更多信息，请参阅"了解卷使用情况"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”以查看有关支持和控制台将购买的 Azure 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

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

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

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

> 部署过程完成后，请勿修改 Azure 门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

完成后

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

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

在 **Azure** 中启动**Cloud Volumes ONTAP HA** 对

如果您想在 Azure 中启动Cloud Volumes ONTAP HA 对，则需要在控制台中创建一个 HA 系统。

步骤

1. 从左侧导航菜单中，选择“存储”>“管理”。
2. 在*系统*页面上，单击*添加系统*并按照提示进行操作。
3. 如果出现提示， "创建控制台代理" 。
4. 详细信息和凭据：可选择更改 Azure 凭据和订阅，指定群集名称，根据需要添加标签，然后指定凭据。

   下表描述了您可能需要指导的字段：

字段	描述
系统名称	控制台使用系统名称来命名Cloud Volumes ONTAP系统和 Azure 虚拟机。如果您选择该选项，它还会使用该名称作为预定义安全组的前缀。
资源组标签	标签是 Azure 资源的元数据。当您在此字段中输入标签时，控制台会将它们添加到与Cloud Volumes ONTAP系统关联的资源组中。创建系统时，您可以从用户界面添加最多四个标签，然后可以在创建系统后添加更多标签。请注意，创建系统时，API 不会将您限制为四个标签。有关标签的信息，请参阅 "Microsoft Azure 文档：使用标签来组织您的 Azure 资源"。
用户名和密码	这些是Cloud Volumes ONTAP集群管理员帐户的凭据。您可以使用这些凭据通过ONTAP System Manager 或ONTAP CLI 连接到Cloud Volumes ONTAP 。保留默认的_admin_用户名或将其更改为自定义用户名。
编辑凭证	您可以选择不同的 Azure 凭据和不同的 Azure 订阅来与此Cloud Volumes ONTAP系统一起使用。您需要将 Azure 市场订阅与选定的 Azure 订阅关联，以便部署即用即付的Cloud Volumes ONTAP系统。 "了解如何添加凭证" 。

5. 服务：根据您是否要将各个服务与Cloud Volumes ONTAP一起使用来启用或禁用它们。
   - "了解有关NetApp Data Classification的更多信息"
   - "了解有关NetApp Backup and Recovery的更多信息"

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

6. **HA**部署模型：
   a. 选择*单个可用区*或*多个可用区*。
      - 对于单个可用区域，请选择 Azure 区域、可用区域、VNet 和子网。

        从Cloud Volumes ONTAP 9.15.1 开始，您可以在 Azure 中的单个可用区域 (AZ) 中以 HA 模式部署虚拟机 (VM) 实例。您需要选择支持此部署的区域和地域。如果区域或地域不支持区域部署，则遵循之前LRS的非区域部署模式。要了解共享托管磁盘支持的配置，请参阅"具有共享托管磁盘的 HA 单可用区域配置"。

      - 对于多个可用区域，请选择区域、VNet、子网、节点 1 的区域以及节点 2 的区域。

   b. 选中*我已验证网络连接…*复选框。
7. 连接：选择一个新的或现有的资源组，然后选择是否使用预定义的安全组或使用您自己的安全组。

   下表描述了您可能需要指导的字段：

字段	描述
资源组	为Cloud Volumes ONTAP创建新的资源组或使用现有的资源组。最佳做法是为Cloud Volumes ONTAP使用新的专用资源组。虽然可以在现有的共享资源组中部署Cloud Volumes ONTAP ，但由于存在数据丢失的风险，因此不建议这样做。请参阅上面的警告以了解更多详细信息。 您必须为在 Azure 中部署的每个Cloud Volumes ONTAP HA 对使用专用资源组。一个资源组中仅支持一个 HA 对。如果您尝试在 Azure 资源组中部署第二个Cloud Volumes ONTAP HA 对，控制台会遇到连接问题。 如果您使用的 Azure 帐户具有 "所需权限"，如果部署失败或删除，控制台会从资源组中删除Cloud Volumes ONTAP资源。
生成的安全组	如果您让控制台为您生成安全组，则需要选择如何允许流量： • 如果选择*仅限选定的 VNet*，则入站流量的来源是选定 VNet 的子网范围和控制台代理所在的 VNet 的子网范围。这是推荐的选项。 • 如果选择“所有 **VNets**”，则入站流量的来源是 0.0.0.0/0 IP 范围。
使用现有的	如果您选择现有的安全组，则它必须满足Cloud Volumes ONTAP要求。"查看默认安全组" 。

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

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

    如果所选版本有较新的候选版本、通用版本或补丁版本，则控制台在创建系统时会将其更新到该版本。例如，如果您选择Cloud Volumes ONTAP 9.13.1 并且 9.13.1 P4 可用，则会发生更新。更新不会从一个版本发生到另一个版本 — 例如，从 9.13 到 9.14。
11. 从 **Azure** 市场订阅：如果控制台无法启用Cloud Volumes ONTAP的编程部署，请按照以下步骤操作。
12. 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数据分层到 Blob 存储。

    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控制台创建的任何其他聚合。您可以使用高级分配选项创建使用不同磁盘大小的聚合。

      有关选择磁盘大小的帮助，请参阅"在 Azure 中调整系统大小"。
    - 如果在 VNet 中禁用了对您的存储帐户的公共访问，则您无法在Cloud Volumes ONTAP系统中启用数据分层。有关信息，请参阅"安全组规则"。

- 您可以在创建或编辑卷时选择特定的卷分层策略。
- 如果您禁用数据分层，则可以在后续聚合上启用它。

  "了解有关数据分层的更多信息" 。

- 从Cloud Volumes ONTAP 9.15.0P1 开始，Azure 页面 blob 不再支持新的高可用性对部署。如果您当前在现有的高可用性对部署中使用 Azure 页 Blob，则可以迁移到 Edsv4 系列 VM 和 Edsv5 系列 VM 中较新的 VM 实例类型。

  "详细了解 Azure 中支持的配置" 。

13. 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. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

       此选项仅适用于某些 VM 类型。要了解受支持的 VM 类型，请参阅"HA 对许可证支持的配置"。

       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，恢复或降级到Cloud Volumes ONTAP 9.8 的操作将被阻止。

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

14. 与存储和 **WORM** 的安全通信：选择是否启用与 Azure 存储帐户的 HTTPS 连接，并激活一次写入、多次读取 (WORM) 存储（如果需要）。

    HTTPS 连接从Cloud Volumes ONTAP 9.7 HA 对到 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。创建系统后，您无法更改设置。

    "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*。

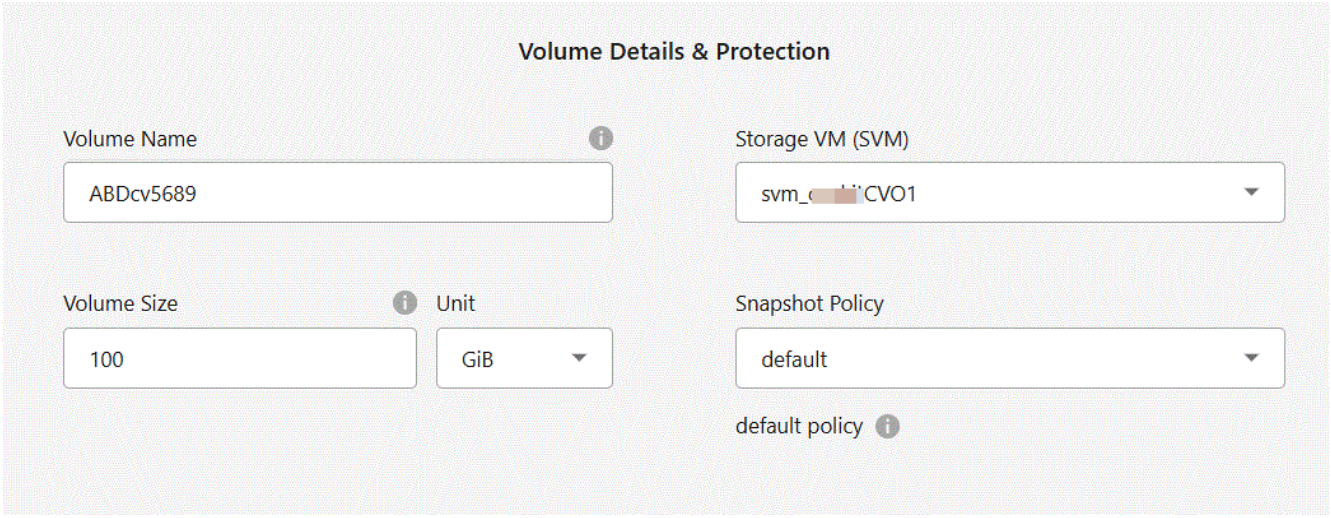
    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

字段	描述
大小	您可以输入的最大大小很大程度上取决于您是否启用精简配置，这使您能够创建比当前可用的物理存储更大的卷。
访问控制（仅适用于 NFS）	导出策略定义了子网中可以访问卷的客户端。默认情况下，控制台输入一个提供对子网中所有实例的访问权限的值。

字段	描述
权限和用户/组（仅适用于 CIFS）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL）。您可以指定本地或域 Windows 用户或组，或者 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用域\用户名格式包含用户的域。
Snapshot 策略	Snapshot 副本策略指定自动创建的NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是时间点文件系统映像，它不会影响性能并且只需要最少的存储空间。您可以选择默认策略或无策略。对于瞬态数据，您可能选择无：例如，对于 Microsoft SQL Server，请选择 tempdb。
高级选项（仅适用于 NFS）	为卷选择一个 NFS 版本：NFSv3 或 NFSv4。
启动器组和 IQN（仅适用于 iSCSI）	iSCSI 存储目标称为 LUN（逻辑单元），并作为标准块设备呈现给主机。启动器组是 iSCSI 主机节点名称表，用于控制哪些启动器可以访问哪些 LUN。iSCSI 目标通过标准以太网网络适配器 (NIC)、带有软件启动器的 TCP 卸载引擎 (TOE) 卡、融合网络适配器 (CNA) 或专用主机总线适配器 (HBA) 连接到网络，并通过 iSCSI 限定名称 (IQN) 进行标识。当您创建 iSCSI 卷时，控制台会自动为您创建一个 LUN。我们通过为每个卷创建一个 LUN 来简化操作，因此无需进行任何管理。创建卷后，"使用 IQN 从主机连接到 LUN" 。

下图显示了卷创建向导的第一页：



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

字段	描述
DNS 主 IP 地址和辅助 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含定位 CIFS 服务器将加入的域的 Active Directory LDAP 服务器和域控制器所需的服务位置记录 (SRV)。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory (AD) 域的 FQDN。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域内指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS 服务器 NetBIOS 名称	AD 域中唯一的 CIFS 服务器名称。

字段	描述
组织单位	AD 域内与 CIFS 服务器关联的组织单位。默认值为 CN=Computers。要将 Azure AD 域服务配置为Cloud Volumes ONTAP 的AD 服务器，您应该在此字段中输入 **OU=AADDC Computers** 或 **OU=AADDC Users** 。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 文档：在 Azure AD 域服务托管域中创建组织单位 (OU)"^]
DNS 域	Cloud Volumes ONTAP存储虚拟机 (SVM) 的 DNS 域。大多数情况下，该域与 AD 域相同。
NTP 服务器	选择“使用 Active Directory 域”以使用 Active Directory DNS 配置 NTP 服务器。如果您需要使用不同的地址配置 NTP 服务器，那么您应该使用 API。请参阅 "NetApp Console自动化文档"了解详情。请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。创建 CIFS 服务器后，它不可配置。

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更改卷分层策略（如果需要）。

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

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”以查看有关支持和控制台将购买的 Azure 资源的详细信息。

    c. 选中*我明白…*复选框。

    d. 单击“开始”。

结果

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

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

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

完成后

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

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

部署过程完成后，请勿修改 Azure 门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外行为或数据丢失。

相关链接

*"在 Azure 中规划Cloud Volumes ONTAP配置" *"从 Azure 市场在 Azure 中部署Cloud Volumes ONTAP"

验证 **Azure** 平台映像

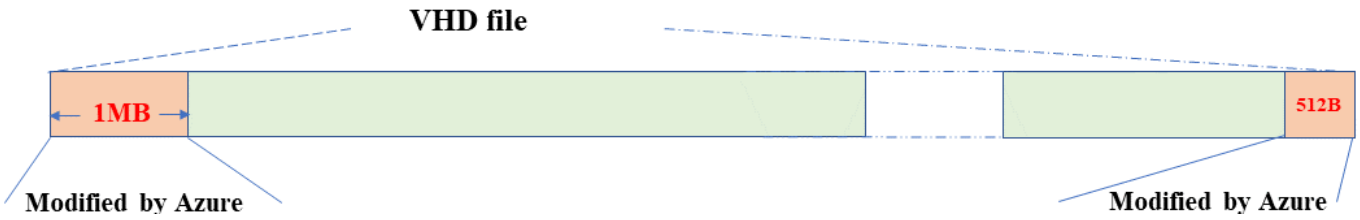
针对**Cloud Volumes ONTAP** 的**Azure** 市场映像验证

Azure 映像验证符合增强的NetApp安全要求。验证图像文件是一个简单的过程。但是，Azure 映像签名验证需要特别注意 Azure VHD 映像文件，因为它在 Azure 市场中被更改了。

Cloud Volumes ONTAP 9.15.0 及更高版本支持 Azure 映像验证。

Azure 对已发布 **VHD** 文件的更改

VHD 文件开头的 1 MB（1048576 字节）和结尾的 512 字节已被 Azure 修改。 NetApp对剩余的 VHD 文件进行签名。



在示例中，VHD 文件为 10GB。 NetApp签名的部分标记为绿色（10 GB - 1 MB - 512 字节）。

相关链接

- "页面错误博客：如何使用 OpenSSL 进行签名和验证"
- "使用 Azure Marketplace 映像为 Azure Stack Edge Pro GPU 创建 VM 映像 | Microsoft Learn"
- "使用 Azure CLI 将托管磁盘导出/复制到存储帐户 | Microsoft Learn"
- "Azure Cloud Shell 快速入门 - Bash | Microsoft Learn"
- "如何安装 Azure CLI | Microsoft Learn"
- "az 存储 blob 副本 | Microsoft Learn"
- "使用 Azure CLISign in— 登录和身份验证 | Microsoft Learn"

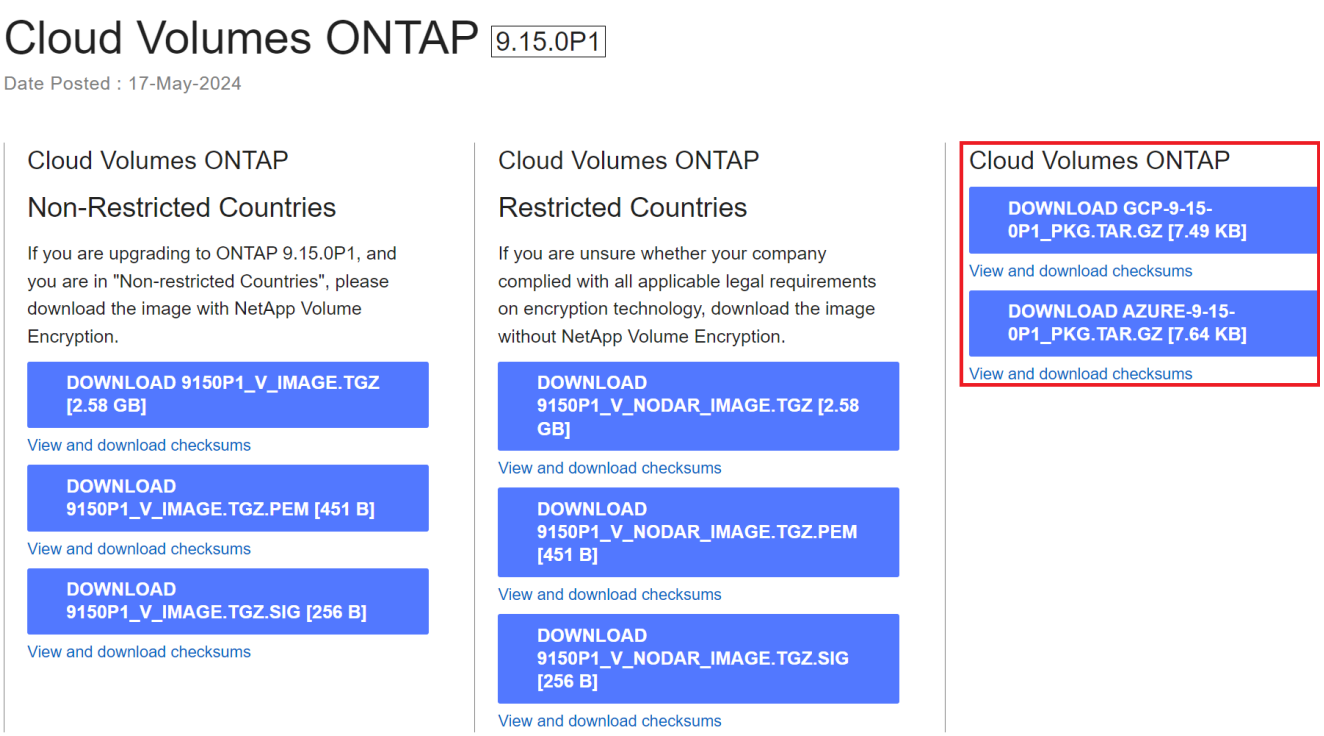
下载适用于**Cloud Volumes ONTAP** 的**Azure** 映像文件

您可以从 "NetApp 支持站点"。

tar.gz 文件包含图像签名验证所需的文件。除了 *tar.gz* 文件之外，您还应该下载图像的 *checksum* 文件。校验和文件包含 `md5`和 `sha256`*tar.gz* 文件的校验和。

步骤

1. 前往 "NetApp支持站点上的Cloud Volumes ONTAP产品页面"并从*下载*部分下载所需的软件版本。
2. 在Cloud Volumes ONTAP下载页面上，单击 Azure 映像的可下载文件并下载 *tar.gz* 文件。



3. 在 Linux 上，运行 `md5sum AZURE-<version>_PKG.TAR.GZ`。

   在 macOS 上，运行 `sha256sum AZURE-<version>_PKG.TAR.GZ`。

4. 验证 `md5sum`和 `sha256sum`值与下载的 Azure 映像中的值匹配。
5. 在 Linux 和 macOS 上，使用以下命令提取 *tar.gz* 文件 `tar -xzf`命令。

   解压后的 *tar.gz* 文件包含摘要（*.sig*）文件、公钥证书（*.pem*）文件和链证书（*.pem*）文件。

   提取 **tar.gz** 文件后的示例输出：

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

从 **Azure** 市场导出**Cloud Volumes ONTAP**的 **VHD** 映像

一旦 VHD 映像发布到 Azure 云，它就不再由NetApp管理。相反，已发布的图像被放置在 Azure 市场上。当映像在 Azure 市场上暂存和发布时，Azure 会修改 VHD 开头的 1 MB 和结尾的 512 字节。要验证VHD文件的签名，需要从Azure市场导出Azure修改后的VHD镜像。

开始之前

确保您的系统上安装了 Azure CLI，或者可以通过 Azure 门户使用 Azure Cloud Shell。有关如何安装 Azure CLI 的详细信息，请参阅 "Microsoft 文档：如何安装 Azure CLI"。

步骤

1. 使用 *version_readme* 文件的内容将系统上的Cloud Volumes ONTAP版本映射到 Azure 市场映像版本。Cloud Volumes ONTAP版本由 `buildname`Azure 市场镜像版本表示为 `version`在版本映射中。

   在以下示例中， Cloud Volumes ONTAP版本 `9.15.0P1`映射到 `Azure` 市场映像版本 `9150.01000024.05090105`。此 Azure 市场镜像版本稍后用于设置镜像 URN。

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. 确定要创建虚拟机的区域。区域名称用作 `locName`设置市场图像的 URN 时的变量。要列出可用区域，请运行以下命令：

   ```
   az account list-locations -o table
   ```

   在此表中，区域名称出现在 `Name`场地。

   ```
   $ az account list-locations -o table
   DisplayName               Name                 RegionalDisplayName
   ------------------------  -------------------
   -------------------------------------
   East US                   eastus               (US) East US
   East US 2                 eastus2              (US) East US 2
   South Central US          southcentralus       (US) South Central US
   ...
   ```

3. 查看下表中相应Cloud Volumes ONTAP版本和 VM 部署类型的 SKU 名称。 SKU 名称用作 `skuName`设置市场图像的 URN 时的变量。

   例如，所有采用Cloud Volumes ONTAP 9.15.0 的单节点部署都应使用 `ontap_cloud_byol`作为 SKU 名称。

* Cloud Volumes ONTAP版本*	通过虚拟机部署	**SKU** 名称
9.17.1 及更高版本	Azure 市场	ontap_cloud_direct_gen2
9.17.1 及更高版本	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 市场	ontap_cloud_direct
9.16.1	控制台	ontap_cloud

9.15.1	控制台	ontap_cloud
9.15.0	控制台，单节点部署	ontap_cloud_byol
9.15.0	控制台、高可用性 (HA) 部署	ontap_cloud_byol_ha

4. 映射ONTAP版本和 Azure 市场映像后，使用 Azure Cloud Shell 或 Azure CLI 从 Azure 市场导出 VHD 文件。

使用 **Linux** 上的 **Azure Cloud Shell** 导出 **VHD** 文件

从 Azure Cloud Shell，将市场映像导出到 VHD 文件（例如，*9150.01000024.05090105.vhd*），然后将其下载到本地 Linux 系统。执行以下步骤从 Azure 市场获取 VHD 映像。

步骤

1. 设置市场图像的 URN 和其他参数。 URN 格式为 `<publisher>:<offer>:<sku>:<version>`。或者，您可以列出NetApp市场图像来确认正确的图像版本。

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 从市场映像创建一个具有匹配映像版本的新托管磁盘：

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 将 VHD 文件从托管磁盘导出到 Azure 存储。创建具有适当访问级别的容器。在这个例子中，我们使用了一个名为 `vm-images`和 `Container`访问级别。从 Azure 门户获取存储帐户访问密钥：存储帐户 **> *examplesaname* >** 访问密钥 **> *key1* > *key* >** 显示 **> *<copy>***

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 将生成的图像下载到您的 Linux 系统。使用 `wget`下载VHD文件的命令：

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL 遵循标准格式。为了实现自动化，您可以获取如下所示的 URL 字符串。或者，您可以使用 Azure CLI `az`命令来获取 URL。示例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 清理托管磁盘

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

使用 **Linux** 上的 **Azure CLI** 导出 **VHD** 文件

使用本地 Linux 系统的 Azure CLI 将市场映像导出到 VHD 文件。

步骤

1. 登录到 Azure CLI 并列出市场图像：

```
% az login --use-device-code
```

2. 要登录，请使用网络浏览器打开页面 https://microsoft.com/devicelogin并输入验证码。

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 从具有匹配映像版本的市场映像创建新的托管磁盘。

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
```

为了使该过程自动化，需要从标准输出中提取 SAS。请参阅相应文档以获取指导。

4. 从托管磁盘导出 VHD 文件。

   a. 创建具有适当访问级别的容器。在此示例中，名为 `vm-images`和 `Container`使用访问级别。

   b. 从 Azure 门户获取存储帐户访问密钥：存储帐户 **> *examplesaname* >** 访问密钥 **> *key1* > *key* >** 显示 **> *<copy>***

      您还可以使用 `az`此步骤的命令。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. 检查 blob 副本的状态。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 将生成的图像下载到您的 Linux 服务器。

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL 遵循标准格式。为了实现自动化，您可以获取如下所示的 URL 字符串。或者，您可以使用 Azure CLI `az`命令来获取 URL。示例 URL：https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 清理托管磁盘

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

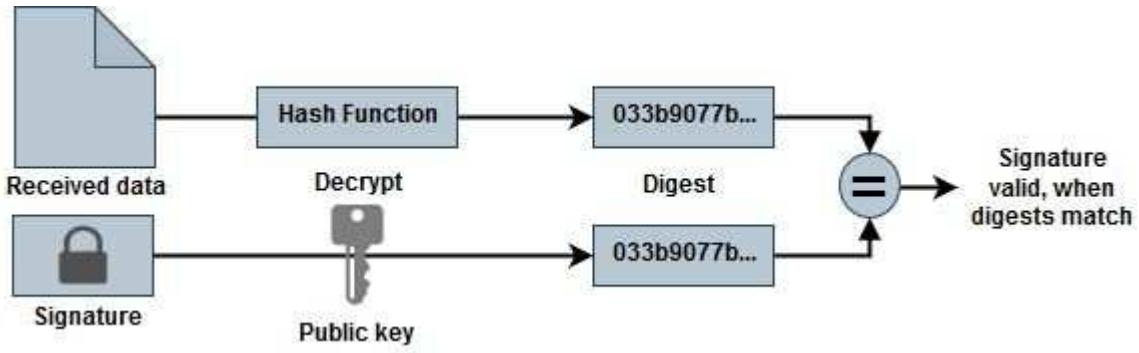
验证文件签名

针对**Cloud Volumes ONTAP** 的**Azure** 市场映像签名验证

Azure 映像验证过程通过剥离 VHD 文件的开头 1 MB 和结尾 512 字节，然后应用哈希函数来生成摘要文件。为了匹配签名程序，使用_sha256_进行散列。

文件签名验证工作流程摘要

以下是文件签名验证工作流程的概述。



- 从下载 Azure 映像 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。请参阅"下载 Azure 映像摘要文件"了解更多信息。
- 信任链的验证。
- 从公钥证书（.pem）中提取公钥（.pub）。
- 使用提取的公钥解密摘要文件。
- 将结果与从图像文件中删除开头 1 MB 和结尾 512 字节后创建的临时文件的新生成的摘要进行比较。此步骤通过使用 OpenSSL 命令行工具执行。 OpenSSL CLI 工具会在文件匹配成功或失败时显示相应的消息。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

在 Linux 上验证导出的 VHD 文件签名包括验证信任链、编辑文件和验证签名。

步骤

1. 从下载 Azure 映像文件 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。

   参考 "下载 Azure 映像摘要文件"了解更多信息。

2. 验证信任链。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 删除 VHD 文件开头的 1 MB（1,048,576 字节）和结尾的 512 字节。使用时 `tail`， 这 `-c +K`选项从文件的第 `K` 个字节生成字节。因此，它将 `1048577` 传递给 `tail -c`。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 从证书中提取公钥，并使用签名文件和公钥验证剥离的文件（sign.tmp）。

   命令提示符根据验证显示指示成功或失败的消息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作区。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

在 Linux 上验证导出的 VHD 文件签名包括验证信任链、编辑文件和验证签名。

步骤

1. 从下载 Azure 映像文件 "NetApp 支持站点"并提取摘要（.sig）文件、公钥证书（.pem）文件和链证书（.pem）文件。

   参考 "下载 Azure 映像摘要文件"了解更多信息。

2. 验证信任链。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 删除 VHD 文件开头的 1MB（1,048,576 字节）和结尾的 512 字节。使用时 `tail`， 这 `-c +K`选项从文件的第 `K` 个字节生成字节。因此，它将 `1048577` 传递给 `tail -c`。请注意，在 macOS 上，tail 命令可能需要大约十分钟才能完成。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 从证书中提取公钥，并使用签名文件和公钥验证剥离的文件（sign.tmp）。命令提示符根据验证显示指示成功或失败的消息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作区。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

从 **Azure** 市场部署**Cloud Volumes ONTAP**

您可以使用 Azure 市场直接部署来快速轻松地部署Cloud Volumes ONTAP。从 Azure 市场，您只需单击几下即可快速部署Cloud Volumes ONTAP ，并在您的环境中探索其核心特性和功能。

有关该产品的更多信息，请参阅"了解NetApp Console和市场中的Cloud Volumes ONTAP产品"。

关于此任务

使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统具有这些属性。请注意，通过 Azure 市场部署的独立实例的功能在NetApp Console中被发现时会发生变化。

- 最新的Cloud Volumes ONTAP版本（9.16.1 或更高版本）。
- Cloud Volumes ONTAP的免费许可证，限制为 500 GiB 的配置容量。此许可证不包括NetApp支持，并且没有到期日期。
- 两个节点在单个可用区 (AZ) 中以高可用性 (HA) 模式配置，并配置默认序列号。存储虚拟机（存储 VM）部署在"灵活的编排模式"。
- 默认创建的实例的聚合。
- 预置容量为 500 GiB 的高级 SSD v2 托管磁盘，以及根磁盘和数据磁盘。
- 部署了一个数据存储虚拟机，具有 NFS、CIFS、iSCSI 和 NVMe/TCP 数据服务。您不能添加任何额外的数据存储虚拟机。
- 为 NFS、CIFS (SMB)、iSCSI、自主勒索软件防护 (ARP)、 SnapLock和SnapMirror安装许可证。
- "ONTAP温度敏感存储效率 (TSSE)"、卷加密和外部密钥管理默认启用。
- 不支持以下功能：
  - FabricPool分层
  - 更改存储虚拟机类型
  - 快速写入模式

开始之前

- 确保您拥有有效的 Azure 市场订阅。
- 确保您满足"单个可用区内的高可用性部署"在 Azure 中。请参阅"为Cloud Volumes ONTAP设置 Azure 网络"。
- 您需要分配以下 Azure 角色之一才能部署Cloud Volumes ONTAP：
  - 这 `contributor`具有默认权限的角色。欲了解更多信息，请参阅 "Microsoft Azure 文档：Azure 内置角色"。
  - 具有以下权限的自定义 RBAC 角色。欲了解更多信息，请参阅 "Azure 文档：Azure 自定义角色"。

“权限”：[{“操作”：[“Microsoft.AAD/register/action”
，“Microsoft.Resources/subscriptions/resourceGroups/write”
，“Microsoft.Network/loadBalancers/write”，“Microsoft.ClassicCompute/virtualMachines/write”
，“Microsoft.Compute/capacityReservationGroups/deploy/action”
，“Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/write”，“Microsoft.Network/networkInterfaces/write”
，“Microsoft.Compute/virtualMachines/write”
，“Microsoft.Compute/virtualMachines/extensions/write”
，“Microsoft.Resources/deployments/validate/action”
，“Microsoft.Resources/subscriptions/resourceGroups/read”
，“Microsoft.Network/virtualNetworks/write”，“Microsoft.Network/virtualNetworks/read”
，“Microsoft.Network/networkSecurityGroups/write”，
“Microsoft.Network/networkSecurityGroups/read”、“Microsoft.Compute/disks/write”、“Microsoft.Compute/virtualMachineScaleSets/write”、“Microsoft.Resources/deployments/write”、“Microsoft.Network/virtualNetworks/subnets/read”、“Microsoft.Network/virtualNetworks/subnets/write”]、“notActions”：[]、“dataActions”：[]、“notDataActions”：[] }]

如果您已将资源提供程序“Microsoft.storage”注册到您的订阅，那么您不需要 `Microsoft.AAD/register/action`允许。欲了解更多信息，请参阅 "Azure 文档：Azure 存储权限"。

步骤

1. 从 Azure 市场网站搜索NetApp产品。
2. 选择* NetApp Cloud Volumes ONTAP direct*。
3. 单击“创建”以启动部署向导。
4. 选择一个计划。 *计划*列表通常显示Cloud Volumes ONTAP的最新版本。
5. 在“基本信息”选项卡中，提供以下详细信息：
   - 订阅：选择订阅。部署将与订阅号挂钩。
   - 资源组：使用现有资源组或创建一个新的资源组。资源组有助于在Cloud Volumes ONTAP系统的单个组内分配所有资源，例如磁盘和存储虚拟机。
   - 区域：选择支持在单个 AZ 中部署 Azure HA 的区域。您只会看到列表中可用的区域。
   - 大小：为支持的 Premium SSD v2 托管磁盘选择存储 VM 大小。
   - 区域：为您选择的地区选择一个区域。
   - 管理员密码：设置密码。部署完成后，您可以使用此管理员密码登录系统。
   - 确认密码：再次输入相同的密码进行确认。
     - 在“网络”选项卡中，添加虚拟网络和子网，或从列表中选择它们。

       为了遵守 Microsoft Azure 限制，您应该在设置新的虚拟网络时创建一个新的子网。同样，如果您选择现有网络，则应该选择现有子网。

     - 要选择预定义的网络安全组，请选择“是”。选择“否”以分配具有必要流量规则的预定义 Azure 网络安全组。有关详细信息，请参阅"Azure 的安全组规则" 。

- 在“高级”选项卡中确认是否已设置此部署所需的两个 Azure 功能。参考"为Cloud Volumes ONTAP单可用区部署启用 Azure 功能"和"在 Azure 中为Cloud Volumes ONTAP启用高可用性模式"。
- 您可以在“标签”选项卡中为资源或资源组定义名称和值对。
- 在“**Review + create**”选项卡中，查看详细信息并开始部署。

完成后

选择通知图标即可查看部署进度。部署Cloud Volumes ONTAP后，您可以查看列出的可供操作的存储虚拟机。

一旦可以访问，请使用ONTAP系统管理器或ONTAP CLI 通过您设置的管理员凭据登录到存储虚拟机。此后，您可以创建卷、LUN 或共享并开始利用Cloud Volumes ONTAP的存储功能。

解决部署问题

直接通过 Azure 市场部署的Cloud Volumes ONTAP系统不包括NetApp的支持。如果部署过程中出现任何问题，您可以独立排除故障并解决。

步骤

1. 在 Azure 市场网站上，转到 启动诊断 **>** 串行日志。
2. 下载并调查串行日志。
3. 请参阅产品文档和知识库 (KB) 文章以进行故障排除。
   - "Azure 市场文档"
   - "NetApp文档"
   - "NetApp知识库文章"

在控制台中发现已部署的系统

您可以发现使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统，并在控制台中的 系统 页面上对其进行管理。控制台代理发现系统、添加系统并应用必要的许可证，并为这些系统解锁控制台的全部功能。保留具有 PSSD v2 托管磁盘的单个 AZ 中的原始 HA 配置，并且系统注册到与原始部署相同的 Azure 订阅和资源组。

关于此任务

在发现使用 Azure 市场直接部署部署的Cloud Volumes ONTAP系统时，控制台代理将执行以下任务：

- 将发现系统的免费许可证替换为常规的基于容量的许可证"免费增值许可证"。
- 保留已部署系统的现有功能，并添加控制台的附加功能，例如数据保护、数据管理和安全功能。
- 使用 NFS、CIFS (SMB)、iSCSI、ARP、 SnapLock和SnapMirror的新ONTAP许可证替换节点上已安装的许可证。
- 将通用节点序列号转换为唯一序列号。
- 根据需要为资源分配新的系统标签。
- 将实例的动态 IP 地址转换为静态 IP 地址。
- 启用以下功能"FabricPool分层"，"AutoSupport" ， 和"一次写入多次读取"（WORM）存储。您可以在需要时从控制台激活这些功能。
- 将实例注册到用于发现它们的 NSS 帐户。

- 启用容量管理功能"自动和手动模式"对于已发现的系统。

开始之前

确保在 Azure 市场上部署已完成。仅当部署完成且可供发现时，控制台代理才能发现系统。

步骤

在控制台中，您可以按照标准程序来发现现有系统。请参阅"将现有的Cloud Volumes ONTAP系统添加到控制台"。

> 在发现过程中，您可能会看到失败消息，但您可以忽略它们，直到发现过程完成。在发现期间，请勿修改 Azure 市场门户中系统生成的Cloud Volumes ONTAP配置，尤其是系统标签。对这些配置所做的任何更改都可能导致意外的系统行为。

完成后

发现完成后，您可以在控制台中的“系统”页面上查看列出的系统。您可以执行各种管理任务，例如"扩大总量"，"添加卷"，"配置额外的存储虚拟机"， 和"更改实例类型"。

相关链接

有关创建存储的更多信息，请参阅ONTAP文档：

- "为 NFS 创建卷"
- "为 iSCSI 创建 LUN"
- "为 CIFS 创建共享"

开始使用 Google Cloud

Google Cloud 中的Cloud Volumes ONTAP快速入门

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

1 创建控制台代理

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

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

2 规划您的配置

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

"了解有关规划配置的更多信息" 。

3 设置网络

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

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

"了解有关网络要求的更多信息" 。

设置服务帐户

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

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

"阅读分步说明" 。

启用 **Google Cloud API**

"在您的项目中启用以下 Google Cloud API" 。部署控制台代理和Cloud Volumes ONTAP需要这些 API。

- 云部署管理器 V2 API
- 云日志 API
- 云资源管理器 API
- 计算引擎 API
- 身份和访问管理 (IAM) API

使用控制台启动**Cloud Volumes ONTAP**

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

相关链接

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

在 **Google Cloud** 中规划您的**Cloud Volumes ONTAP**配置

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

选择**Cloud Volumes ONTAP**许可证

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

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

选择支持的区域

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

选择支持的机器类型

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

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

了解存储限制

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

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

在 **Google Cloud** 中调整系统大小

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

机器类型

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

请参阅以下内容以了解更多详细信息：

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

磁盘类型

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

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

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

磁盘大小

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

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

  请参阅以下内容以了解更多详细信息：

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

查看默认系统磁盘

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

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

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

控制台代理还需要系统磁盘。 "查看控制台代理默认配置的详细信息" 。

收集网络信息

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

单节点系统的网络信息

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

多个区域中 **HA** 对的网络信息

Google Cloud 信息	你的价值
地区	

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

单个区域中 **HA** 对的网络信息

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

选择写入速度

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

选择卷使用情况配置文件

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

NetApp存储效率功能具有以下优势：

精简配置

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

重复数据删除

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

余数据块来减少存储容量要求。

数据压缩

通过压缩主存储、辅助存储和归档存储卷内的数据来减少存储数据所需的物理容量。

为Cloud Volumes ONTAP设置 Google Cloud 网络

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

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

Cloud Volumes ONTAP的要求

Google Cloud 必须满足以下要求。

特定于单节点系统的要求

如果要部署单节点系统，请确保网络满足以下要求。

一个 VPC

单节点系统需要一个虚拟私有云 (VPC)。

私有 IP 地址

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

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

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

```
skipSvmManagementLif: true
```

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

HA 对的特定要求

如果您要部署 HA 对，请确保您的网络满足以下要求。

一个或多个区域

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

- 多区域（推荐）

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

- 单区

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

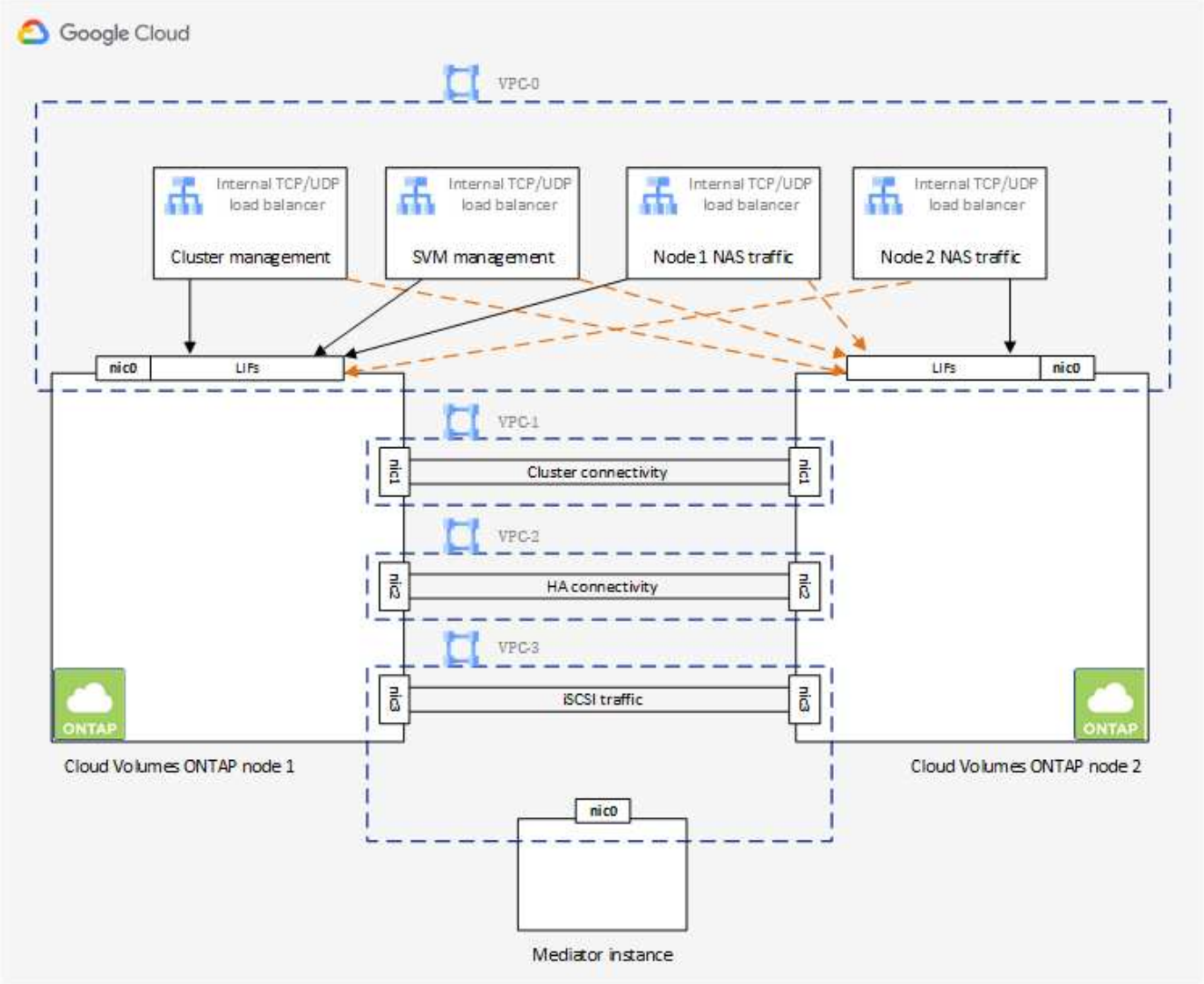
  这种部署模型确实降低了您的成本，因为区域之间没有数据流出费用。

四个虚拟私有云

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

创建 HA 对时，控制台会提示您选择四个 VPC：

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



子网

每个 VPC 都需要一个私有子网。

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

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

私有 **IP** 地址

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

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

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

- 集群管理 LIF
- iSCSI 数据 LIF

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

- NAS LIF

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

```
skipSvmManagementLif: true
```

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

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

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

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

```
skipSvmManagementLif: true
```

内部负载均衡器

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

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

每个负载均衡器的设置如下：

- 一个共享的私有 IP 地址
- 一次全球健康检查

  默认情况下，健康检查使用的端口为63001、63002、63003。

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

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

共享 VPC

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

对于单节点系统，VPC 可以是共享 VPC 或独立 VPC。

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

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

"Google Cloud 文档：共享 VPC 概览" 。

"查看控制台代理部署中涵盖的所需共享 VPC 权限"

VPC 中的数据包镜像

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

出站互联网访问

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

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

Cloud Volumes ONTAP端点

Cloud Volumes ONTAP使用这些端点与各种服务进行通信。

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

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

与其他网络中的**ONTAP**系统的连接

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

"Google Cloud 文档：Cloud VPN 概览" 。

防火墙规则

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

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

请注意，HA 配置需要两组防火墙规则：

- 针对 VPC-0 中的 HA 组件的一组规则。这些规则允许对Cloud Volumes ONTAP进行数据访问。

- 针对 VPC-1、VPC-2 和 VPC-3 中的 HA 组件的另一组规则。这些规则对于 HA 组件之间的入站和出站通信开放。了解更多 。

正在寻找有关控制台代理的信息？ "查看控制台代理的防火墙规则"

入站规则

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

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

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

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

协议	端口	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 锁守护进程
UDP	4046	NFS 网络状态监视器
UDP	4049	NFS rquotad 协议

出站规则

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

基本出站规则

Cloud Volumes ONTAP的预定义安全组包括以下出站规则。

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

高级出站规则

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

源是Cloud Volumes ONTAP系统的接口（IP 地址）。

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

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

VPC-1、**VPC-2** 和 **VPC-3** 的规则

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

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

从 HA 节点到 HA 中介的通信通过端口 3260（iSCSI）进行。

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

控制台代理的要求

如果您尚未创建控制台代理，则应查看网络要求。

- "查看控制台代理的网络要求"

- "Google Cloud 中的防火墙规则"

支持控制台代理的网络配置

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

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

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

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

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

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

相关主题

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

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

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

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

NetApp服务如何与 **VPC** 服务控制进行通信

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

根据控制台代理的部署方式，您的服务边界可能需要做出某些例外。

图片

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

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

部署控制台代理

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

部署**Cloud Volumes ONTAP**

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

下面定义了使用 VPC 服务控制拉取这些图像所需的规则示例。

VPC 服务控制边界策略

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

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

入口规则

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

或

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

或

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

出口规则

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

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

为**Cloud Volumes ONTAP**创建 **Google Cloud** 服务帐号

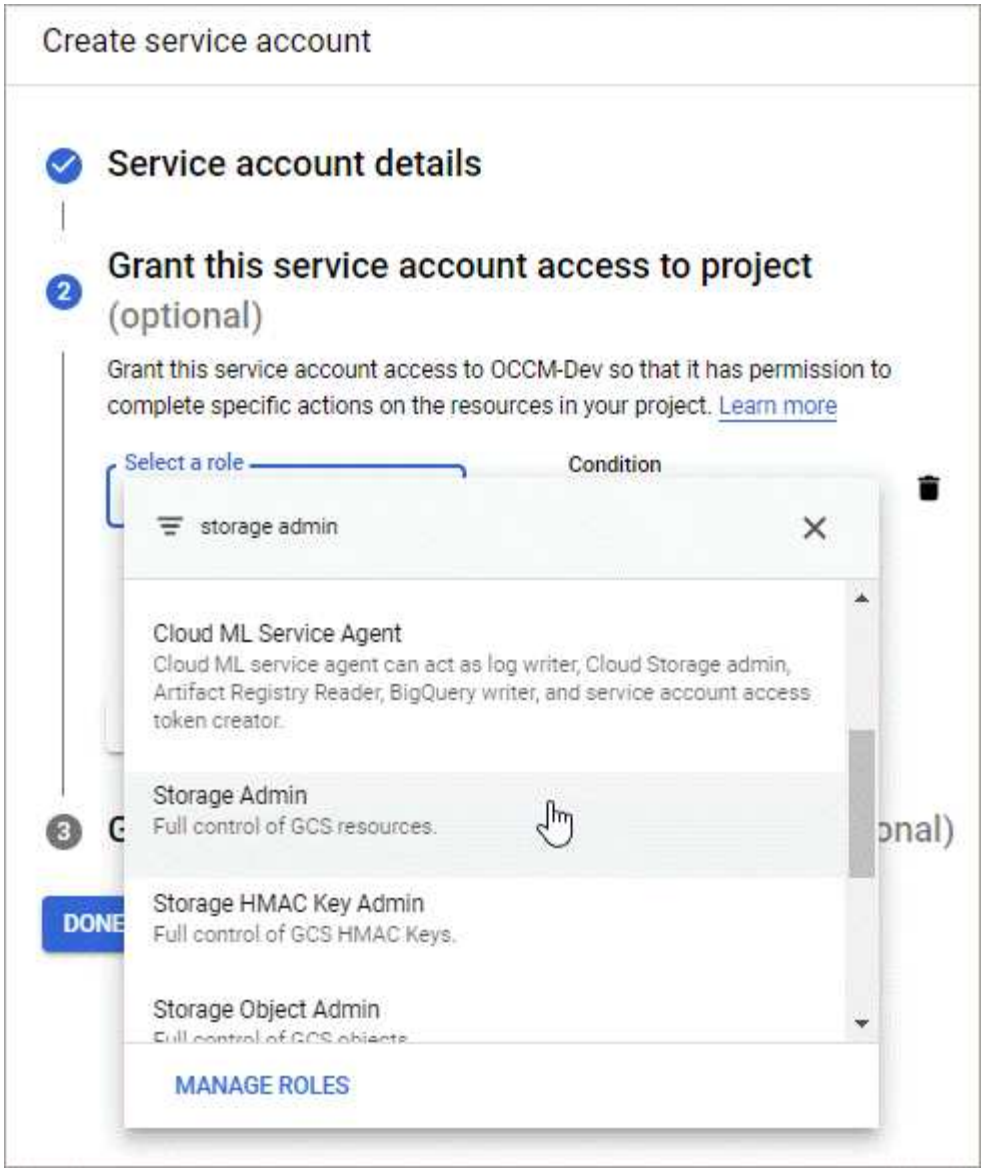
Cloud Volumes ONTAP需要 Google Cloud 服务帐户来实现两个目的。第一个是当你启用"数据分层"将冷数据分层到 Google Cloud 中的低成本对象存储。第二个是当你启用"NetApp Backup and Recovery"将卷备份到低成本的对象存储。

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

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

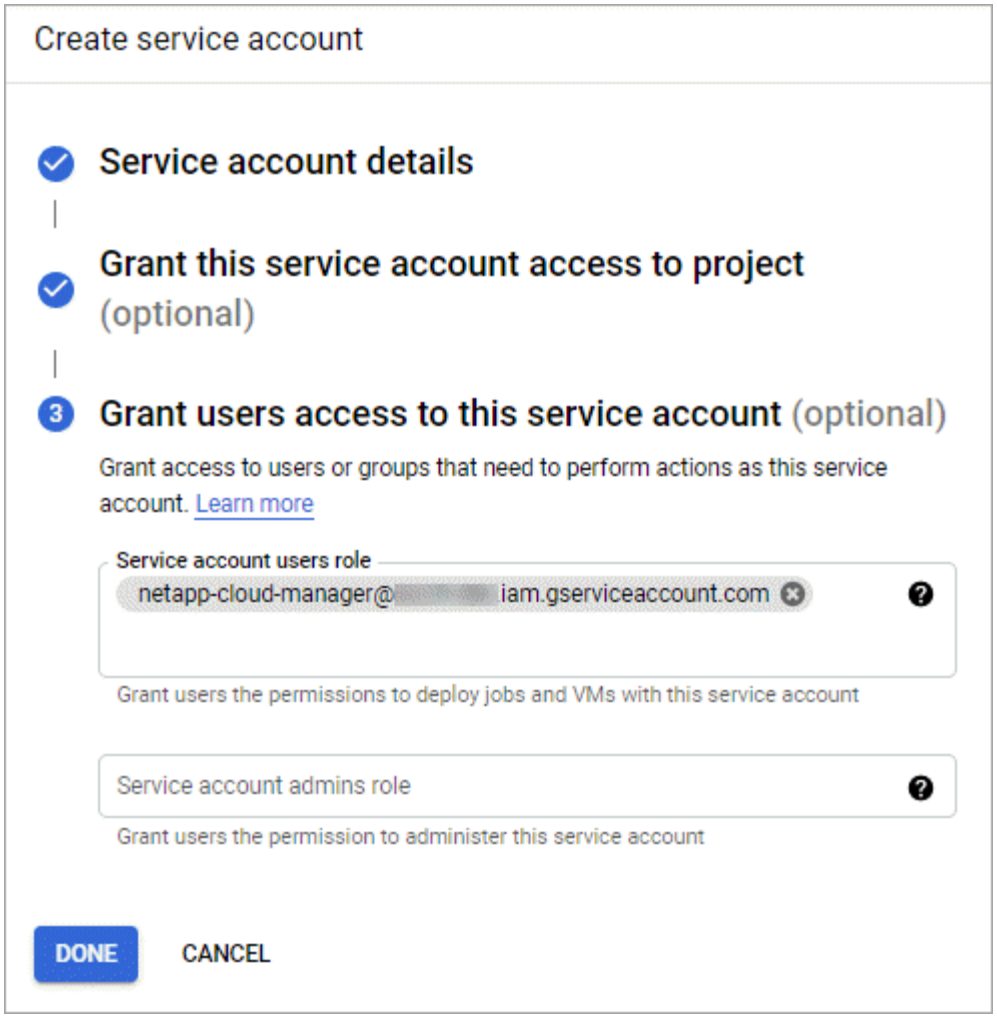
步骤

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



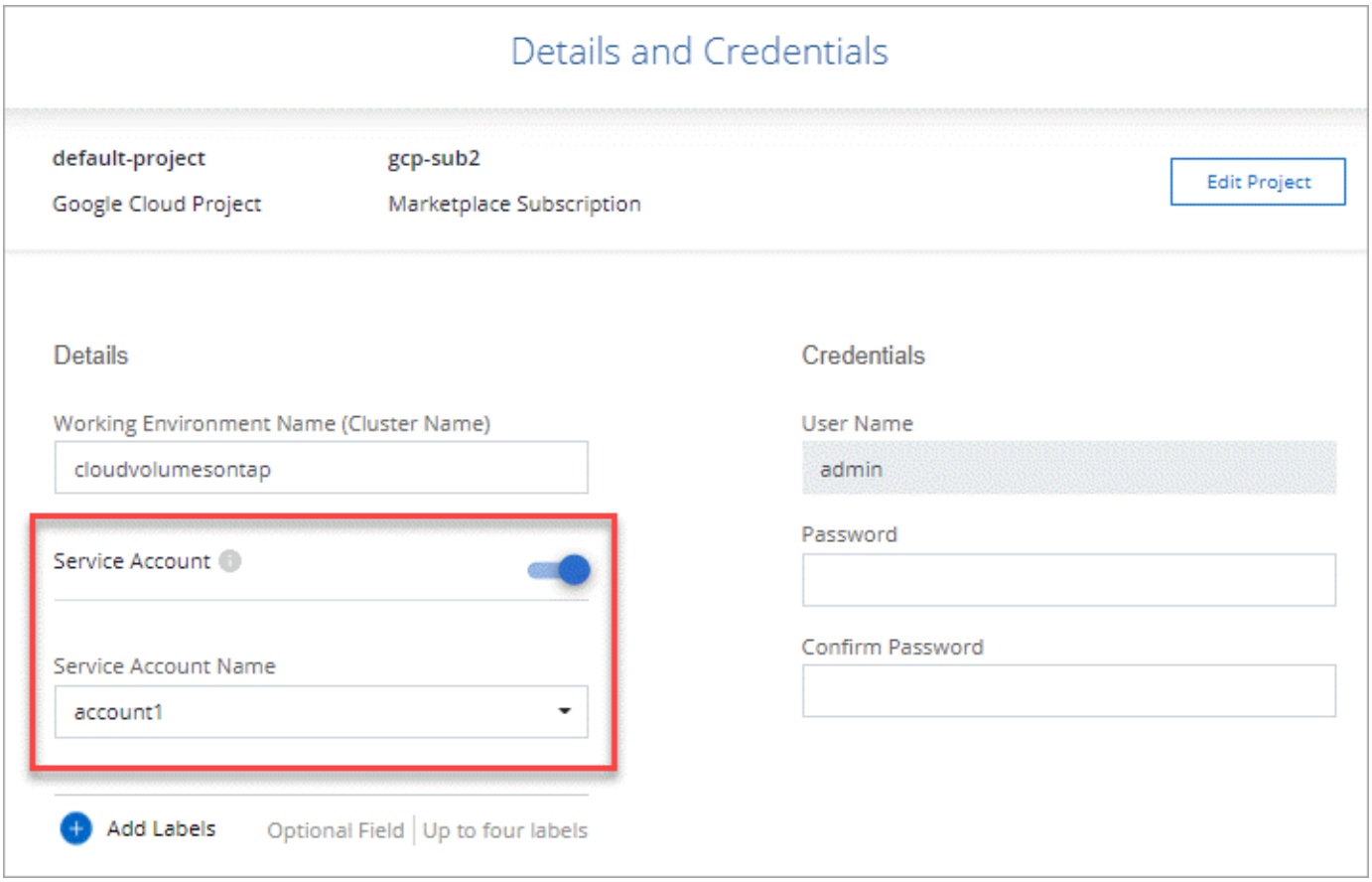
c. 授予用户访问此服务帐户的权限：将控制台代理服务帐户作为_服务帐户用户_添加到此新服务帐户。

此步骤仅对于数据分层是必需的。备份和恢复不需要它。



下一步是什么?

稍后创建Cloud Volumes ONTAP系统时，您需要选择服务帐户。



将客户管理的加密密钥与Cloud Volumes ONTAP结合使用

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

步骤

1. 确保控制台代理服务帐户在存储密钥的项目中具有项目级别的正确权限。

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

   权限如下：

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

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

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

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

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

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

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

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

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

   例子

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

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

在 Google Cloud 中设置Cloud Volumes ONTAP许可

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

免费增值

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

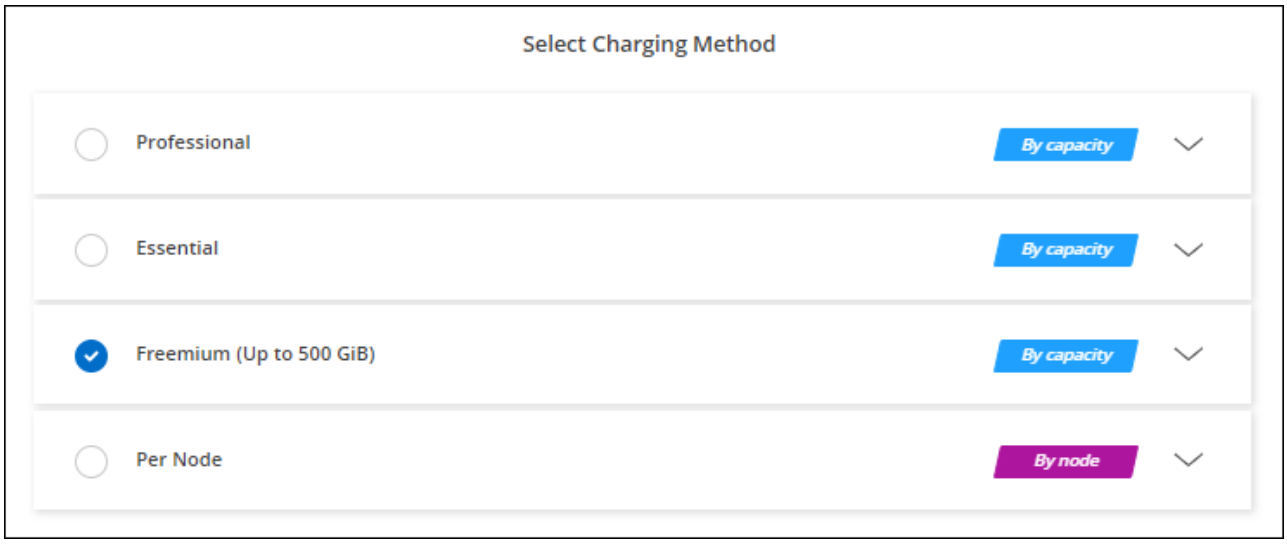
步骤

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

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

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

   b. 返回控制台后，到达收费方式页面时选择“免费增值”。



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

基于容量的许可证

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

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

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

"了解有关基于容量的许可的更多信息" 。

以下部分介绍了如何开始使用每种消费模型。

BYOL

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

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

步骤

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

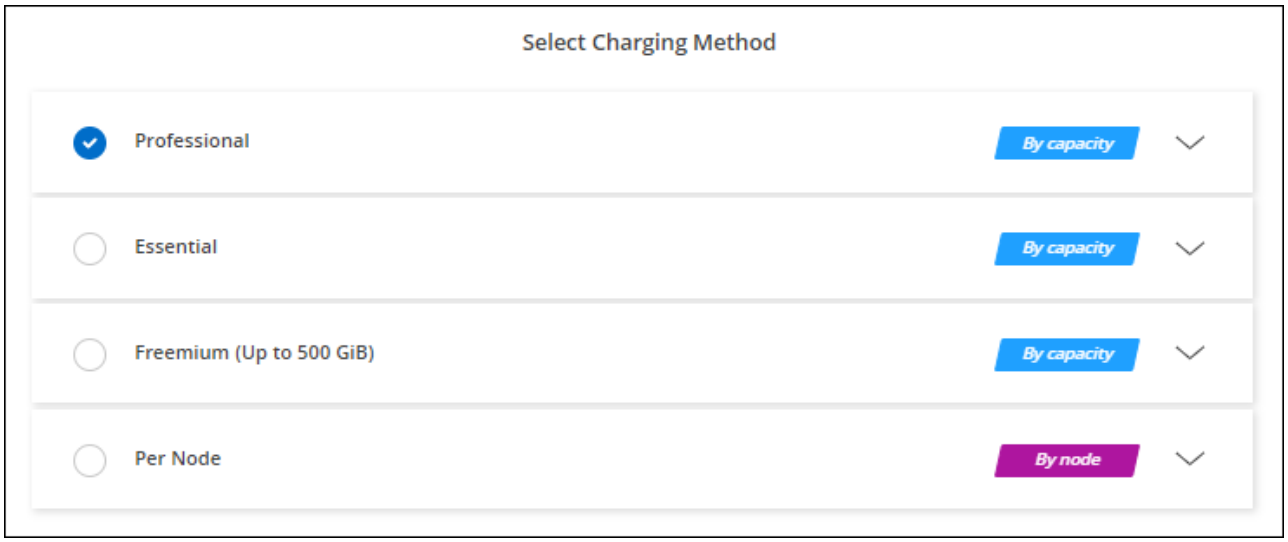
   控制台会自动查询 NetApp 的许可服务，以获取与您的NetApp支持站点帐户相关的许可证的详细信息。如果没有错误，控制台将添加许可证。

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

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

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

    b. 返回控制台后，在进入收费方式页面时选择基于容量的套餐。



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

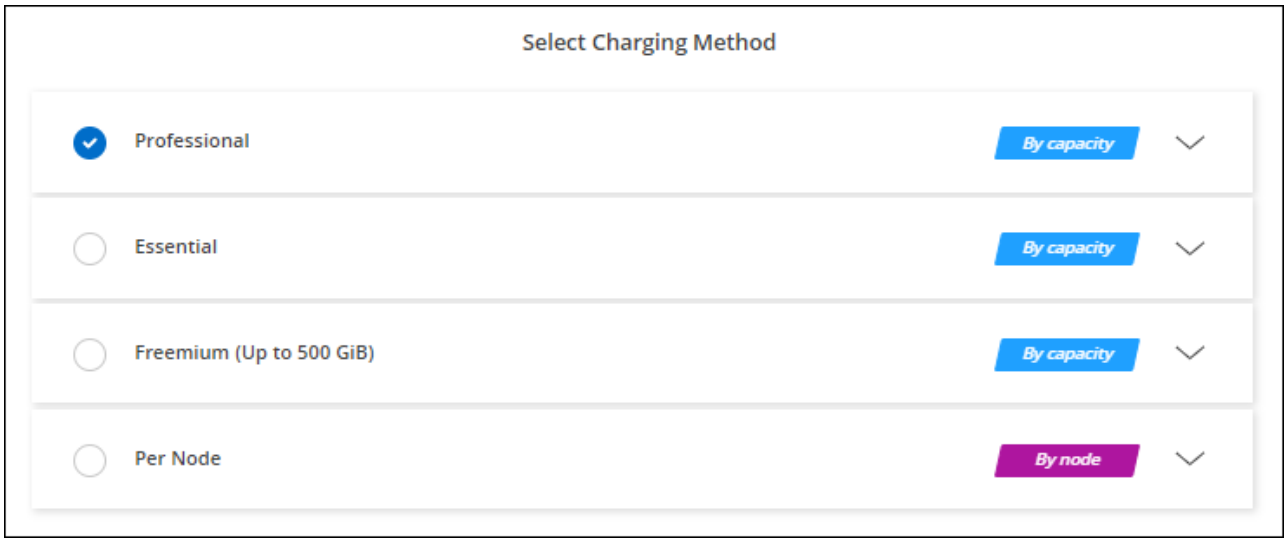
PAYGO 订阅

通过订阅云提供商市场提供的服务按小时付费。

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

步骤

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



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

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

年度合同

通过购买年度合同每年支付Cloud Volumes ONTAP 的费用。

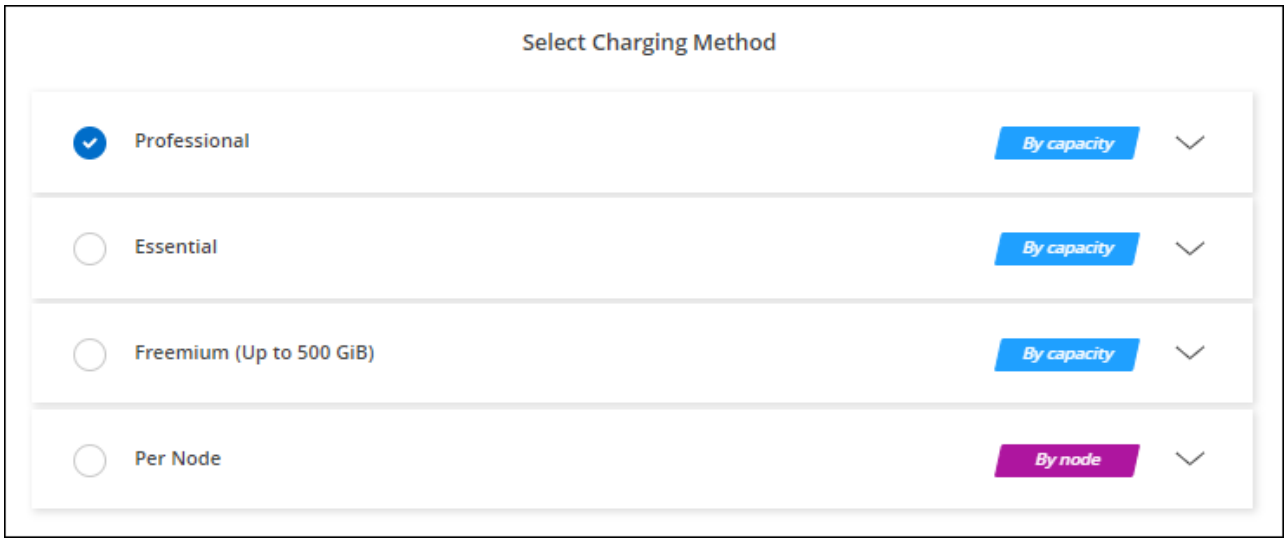
步骤

1. 联系您的NetApp销售代表购买年度合同。

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

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

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



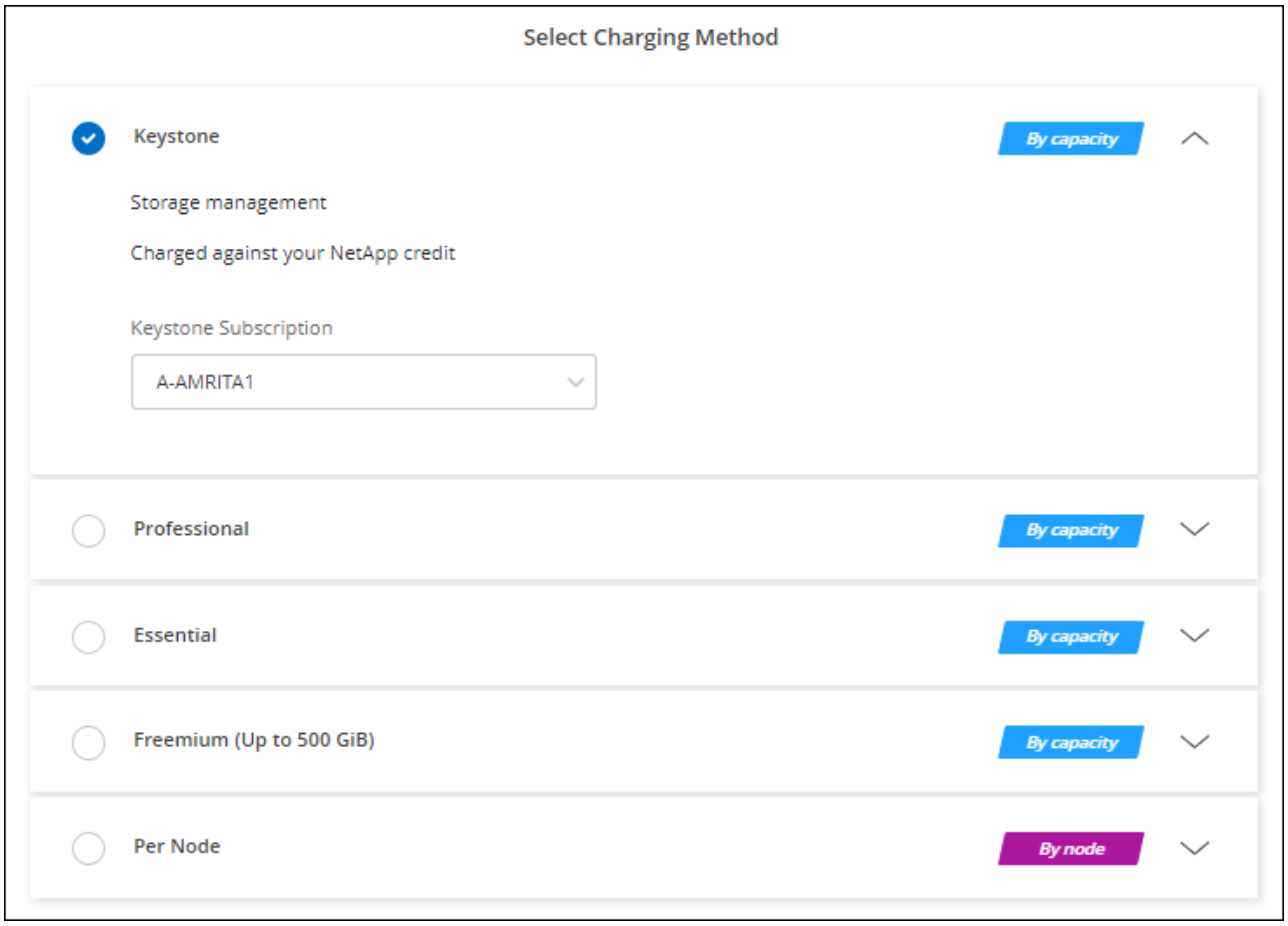
"查看在 Google Cloud 中启动Cloud Volumes ONTAP 的分步说明" 。

Keystone订阅

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

步骤

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



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

基于节点的许可证

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

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

在 Google Cloud 中启动Cloud Volumes ONTAP

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

开始之前

开始之前您需要以下内容。

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

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

- 了解您想要使用的配置。

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

- 了解设置Cloud Volumes ONTAP许可所需的条件。

  "了解如何设置许可" 。

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

在 **Google Cloud** 中启动单节点系统

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

步骤

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

   下表描述了您可能需要指导的字段：

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

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

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

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

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

   下表描述了您可能需要指导的字段：

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

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

- "了解如何设置许可"

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

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

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

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

11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

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

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

12. 闪存缓存、写入速度和 **WORM**：

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

       详细了解 "Flash Cache" 和 "写入速度"。

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

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

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

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

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

    请注意以下事项：

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

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

  "了解有关数据分层的更多信息" 。

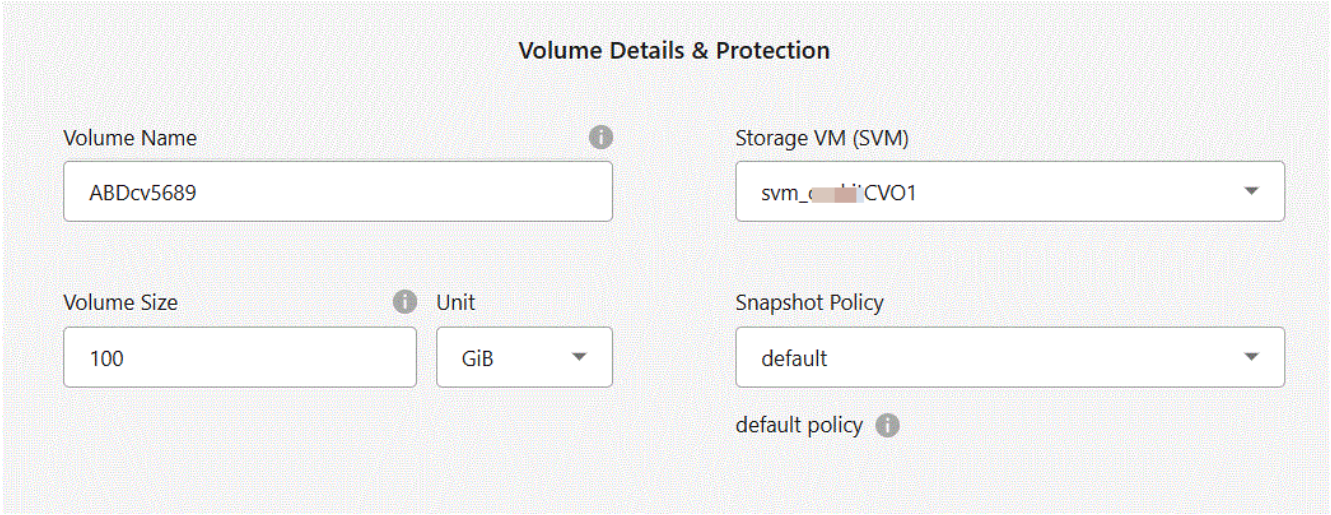
14. 创建卷：输入新卷的详细信息或单击*跳过*。

    "了解支持的客户端协议和版本" 。

    此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

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

    下图显示了卷创建向导的第一页：



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

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

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

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

17. 审核并批准：审核并确认您的选择。

    a. 查看有关配置的详细信息。

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

c. 选中*我明白…*复选框。

d. 单击“开始”。

结果

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

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

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

完成后

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

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

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

在 **Google Cloud** 中启动 **HA** 对

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

步骤

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

   下表描述了您可能需要指导的字段：

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

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

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

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

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

   "了解有关 HA 部署模型的更多信息" 。

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

   "了解有关网络要求的更多信息" 。

   下表描述了您可能需要指导的字段：

字段	描述
生成的策略	如果您让控制台为您生成防火墙策略，则需要选择如何允许流量： • 如果您选择*仅限选定的 VPC*，则入站流量的源过滤器是选定 VPC 的子网范围和控制台代理所在 VPC 的子网范围。这是推荐的选项。 • 如果您选择*所有 VPC*，则入站流量的源过滤器是 0.0.0.0/0 IP 范围。
使用现有的	如果您使用现有的防火墙策略，请确保它包含所需的规则。"了解Cloud Volumes ONTAP的防火墙规则" 。

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

- "了解如何设置许可" 。

9. 预配置包：选择其中一个包来快速部署Cloud Volumes ONTAP系统，或者单击*创建我自己的配置*。

   如果您选择其中一个套餐，您只需指定一个卷，然后审核并批准配置。

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

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

11. 底层存储资源：选择初始聚合的设置：磁盘类型和每个磁盘的大小。

    磁盘类型适用于初始卷。您可以为后续卷选择不同的磁盘类型。

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

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

12. 闪存缓存、写入速度和 **WORM**：

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

       详细了解 "Flash Cache" 和 "写入速度"。

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

    b. 如果需要，请激活一次写入、多次读取 (WORM) 存储。

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

    "了解有关 WORM 存储的更多信息" 。

    a. 如果您激活 WORM 存储，请选择保留期限。

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

    请注意以下事项：

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

服务帐户。

"了解有关数据分层的更多信息"。

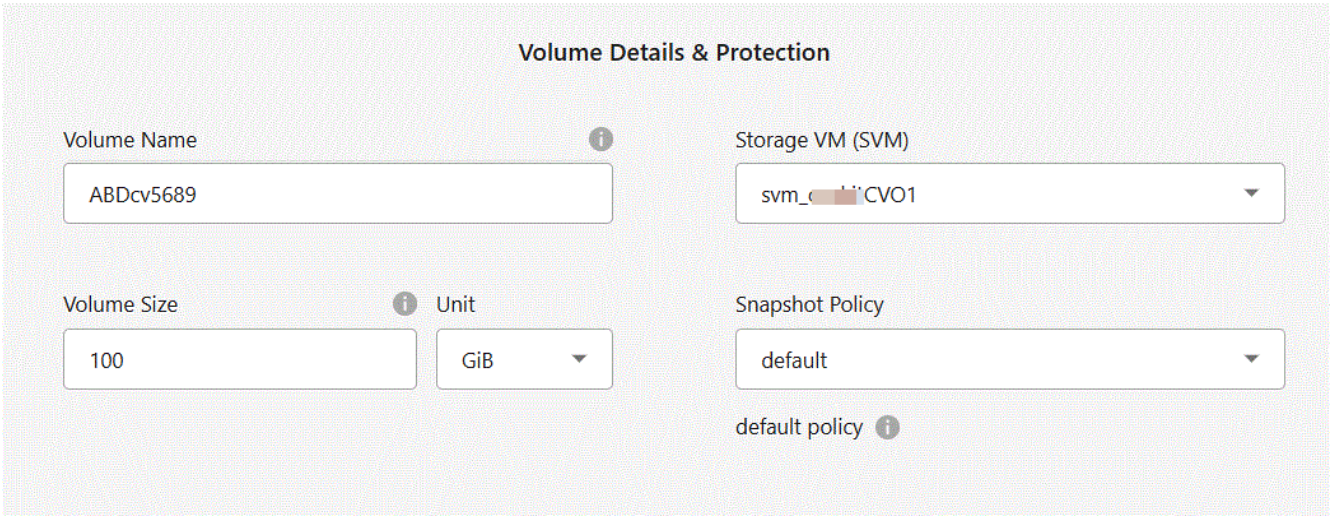
14. 创建卷：输入新卷的详细信息或单击*跳过*。

"了解支持的客户端协议和版本"。

此页面中的某些字段是不言自明的。下表描述了您可能需要指导的字段：

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

下图显示了卷创建向导的第一页：



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

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

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

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

17. 审核并批准：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 点击*更多信息*查看有关支持和控制台将购买的 Google Cloud 资源的详细信息。
    c. 选中*我明白…*复选框。
    d. 单击“开始”。

结果

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

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

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

完成后

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

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

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

相关链接

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

Google Cloud Platform 图像验证

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

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

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

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

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

为什么需要这一步？

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

用户/服务帐户需要权限才能执行以下操作：

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

要验证图像，必须将其转换为 disk.raw 格式，然后下载。

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

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

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

使用 **gcloud** 导出 **Google Cloud** 镜像

点击显示

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

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


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

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

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

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

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

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


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

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

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

解压压缩文件

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

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

图像签名验证

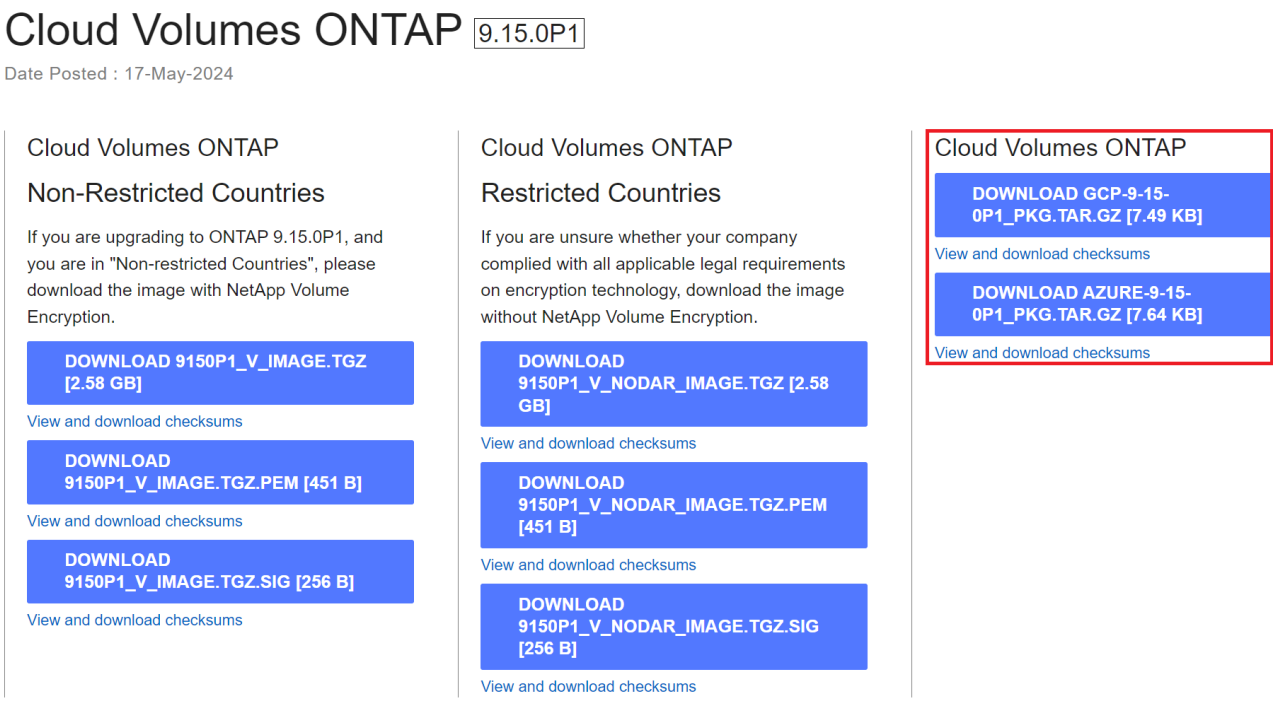
Cloud Volumes ONTAP的 Google Cloud 映像签名验证

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

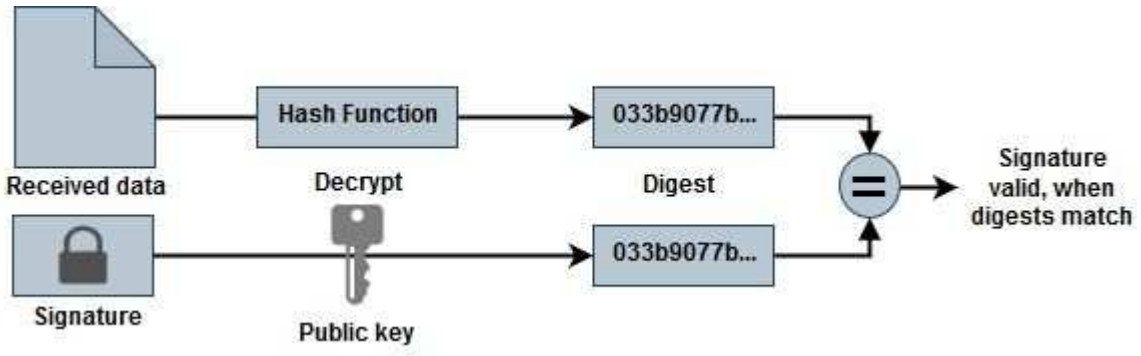
签名图像验证工作流程摘要

以下是 Google Cloud 签名图像验证工作流程的概述。

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



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



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

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

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

步骤

1. 使用 OpenSSL 验证证书。

点击显示

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

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

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

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

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

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

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

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

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

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

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

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

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

点击显示

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

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

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

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

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