开始使用 **Amazon Web Services**

Cloud Volumes ONTAP

NetApp
April 23, 2024

目录

开始使用 Amazon Web Services

在 AWS 中快速启动 Cloud Volumes ONTAP

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

1 创建连接器

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

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

2 规划您的配置

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

3 设置网络

1. 确保您的 VPC 和子网支持连接器和 Cloud Volumes ONTAP 之间的连接。
2. 从NetApp AutoSupport 的目标VPC启用出站Internet访问。

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

3. 将 VPC 端点设置为 S3 服务。

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

"详细了解网络要求"。

4 设置 **AWS KMS**

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

5 使用**BlueXP**启动**Cloud Volumes ONTAP**

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

相关链接

- "从BlueXP创建连接器"
- "从 AWS Marketplace 启动 Connector"

- "在 Linux 主机上安装 Connector 软件"
- "BlueXP对AWS权限的作用"

在AWS中规划Cloud Volumes ONTAP 配置

在 AWS 中部署 Cloud Volumes ONTAP 时，您可以选择符合工作负载要求的预配置系统，也可以创建自己的配置。如果您选择自己的配置、则应了解可用的选项。

选择Cloud Volumes ONTAP 许可证

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

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

选择支持的区域

大多数 AWS 地区均支持 Cloud Volumes ONTAP 。 "查看支持的区域的完整列表"。

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

选择受支持的实例

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

"AWS 中支持的 Cloud Volumes ONTAP 配置"

了解存储限制

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

"AWS 中 Cloud Volumes ONTAP 的存储限制"

在AWS中调整系统大小

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

Instance type

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

EBS 磁盘类型

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

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

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

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

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

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

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

  ⓘ 使用吞吐量优化型 HDD （ st1 ）时，不建议将数据分层到对象存储。

EBS 磁盘大小

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

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

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

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

查看默认系统磁盘

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

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

此连接器还需要一个系统磁盘。 "查看有关连接器默认配置的详细信息"。

准备在AWS前台部署Cloud Volumes ONTAP

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

需要指出的限制如下：

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

收集网络信息

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

单个**AZ**中的单节点或**HA**对

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

HA对位于多个**AZs**中

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

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

选择写入速度

通过BlueXP、您可以为Cloud Volumes ONTAP 选择写入速度设置。在选择写入速度之前、您应该了解正常和高设置之间的差异、以及使用高速写入速度时的风险和建议。 "了解有关写入速度的更多信息。"。

选择卷使用情况配置文件

ONTAP 包含多种存储效率功能、可以减少您所需的存储总量。在BlueXP中创建卷时、您可以选择启用这些功能的配置文件或禁用这些功能的配置文件。您应该了解有关这些功能的更多信息、以帮助您确定要使用的配置文件。

NetApp 存储效率功能具有以下优势：

精简配置

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

重复数据删除

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

压缩

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

设置网络

AWS 中的 Cloud Volumes ONTAP 的网络要求

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

一般要求

以下要求必须在 AWS 中满足。

Cloud Volumes ONTAP 节点的出站 Internet 访问

Cloud Volumes ONTAP 节点需要通过出站Internet访问NetApp AutoSupport 、NetApp会主动监控系统运行状况并向NetApp技术支持发送消息。

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

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

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

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

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

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

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

HA 调解器的出站 Internet 访问

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

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

专用 IP 地址

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

BlueXP为Cloud Volumes ONTAP 分配的LIF数量取决于您部署的是单节点系统还是HA对。LIF 是与物理端口关联的 IP 地址。

单节点系统的 IP 地址

BlueXP会将6个IP地址分配给一个节点系统。

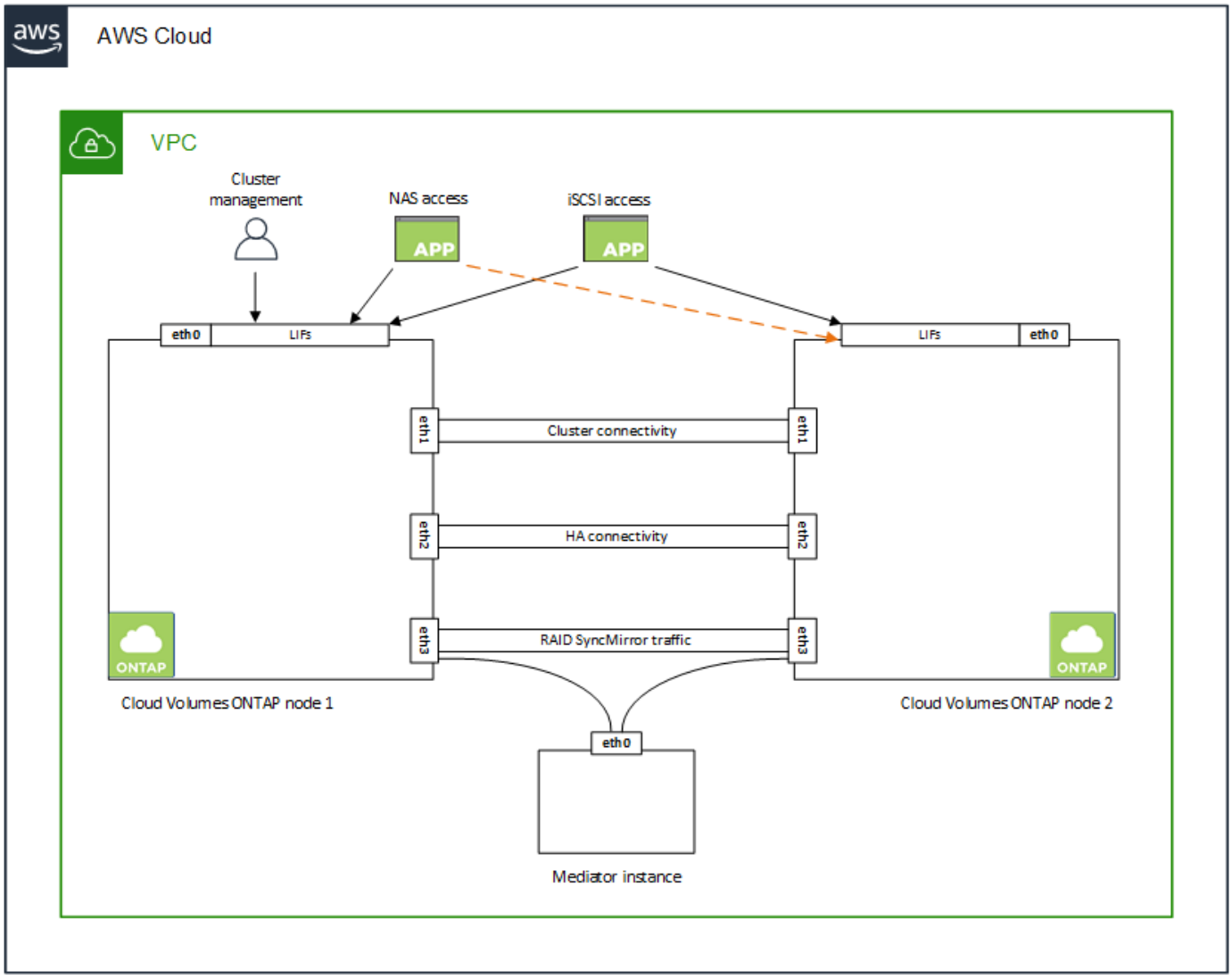
下表提供了有关与每个专用IP地址关联的LIF的详细信息。

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

LIF	目的
Storage VM管理	Storage VM 管理 LIF 与 SnapCenter 等管理工具结合使用。

HA 对的 IP 地址

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



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

下表提供了有关与每个专用 IP 地址关联的 LIF 的详细信息。

一个 AZ 中的 HA 对的 LIF

LIF	接口	Node	目的
集群管理	eth0	节点 1	对整个集群（HA 对）进行管理管理。
节点管理	eth0	节点 1 和节点 2	节点的管理管理。
集群间	eth0	节点 1 和节点 2	跨集群通信，备份和复制。

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

多个 **AZs** 中 **HA** 对的 **LIF**

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

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

安全组

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

正在查找有关连接器的信息？ "查看Connector的安全组规则"

数据分层连接

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

创建 VPC 端点时，请确保选择与 Cloud Volumes ONTAP 实例对应的区域、 VPC 和路由表。您还必须修改安

全组才能添加出站 HTTPS 规则、该规则允许通信到 S3 端点。否则， Cloud Volumes ONTAP 无法连接到 S3 服务。

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

连接到 ONTAP 系统

要在AWS中的Cloud Volumes ONTAP 系统与其他网络中的ONTAP 系统之间复制数据、您必须在AWS VPC与其他网络(例如企业网络)之间建立VPN连接。有关说明，请参见 "AWS 文档：设置 AWS VPN 连接"。

用于 CIFS 的 DNS 和 Active Directory

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

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

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

VPC共享

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

"了解如何在共享子网中部署HA对"。

多个 AZs 中 HA 对的要求

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

要了解 HA 对的工作原理，请参见 "高可用性对"。

可用性区域

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

每个可用性区域都应有一个子网。

用于 NAS 数据和集群 /SVM 管理的浮动 IP 地址

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

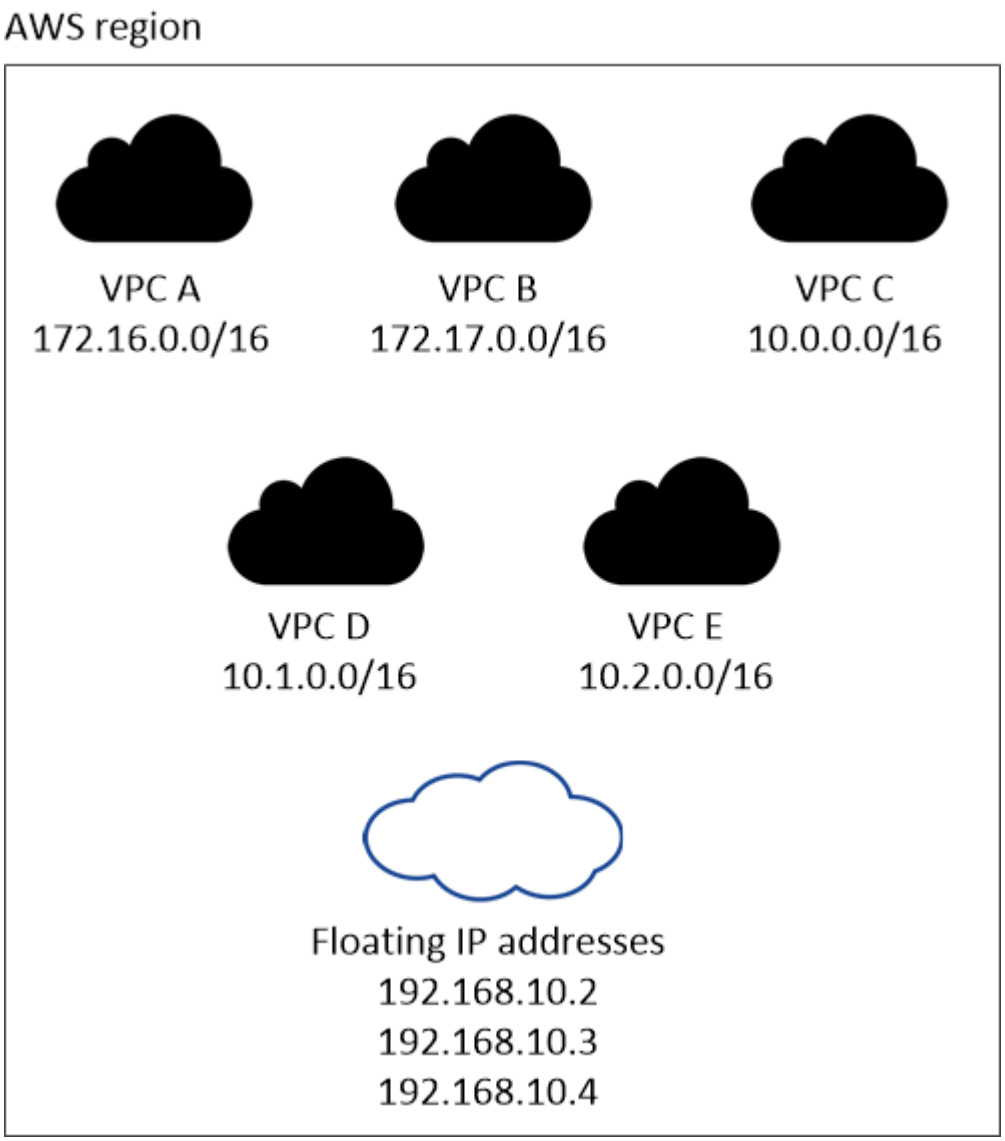
一个浮动 IP 地址用于集群管理、一个用于节点 1 上的 NFS/CIFS 数据、一个用于节点 2 上的 NFS/CIFS 数据。SVM 管理的第四个浮动 IP 地址是可选的。

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

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

对于部署 HA 配置的 AWS 区域中的所有 vPC ，浮动 IP 地址必须不在 CIDR 块的范围内。将浮动 IP 地址视为您所在地区 VPC 之外的逻辑子网。

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



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

传输网关，用于从 **VPC** 外部启用浮动 **IP** 访问

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

路由表

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

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

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

有关路由表的详细信息，请参见 "AWS 文档：路由表"。

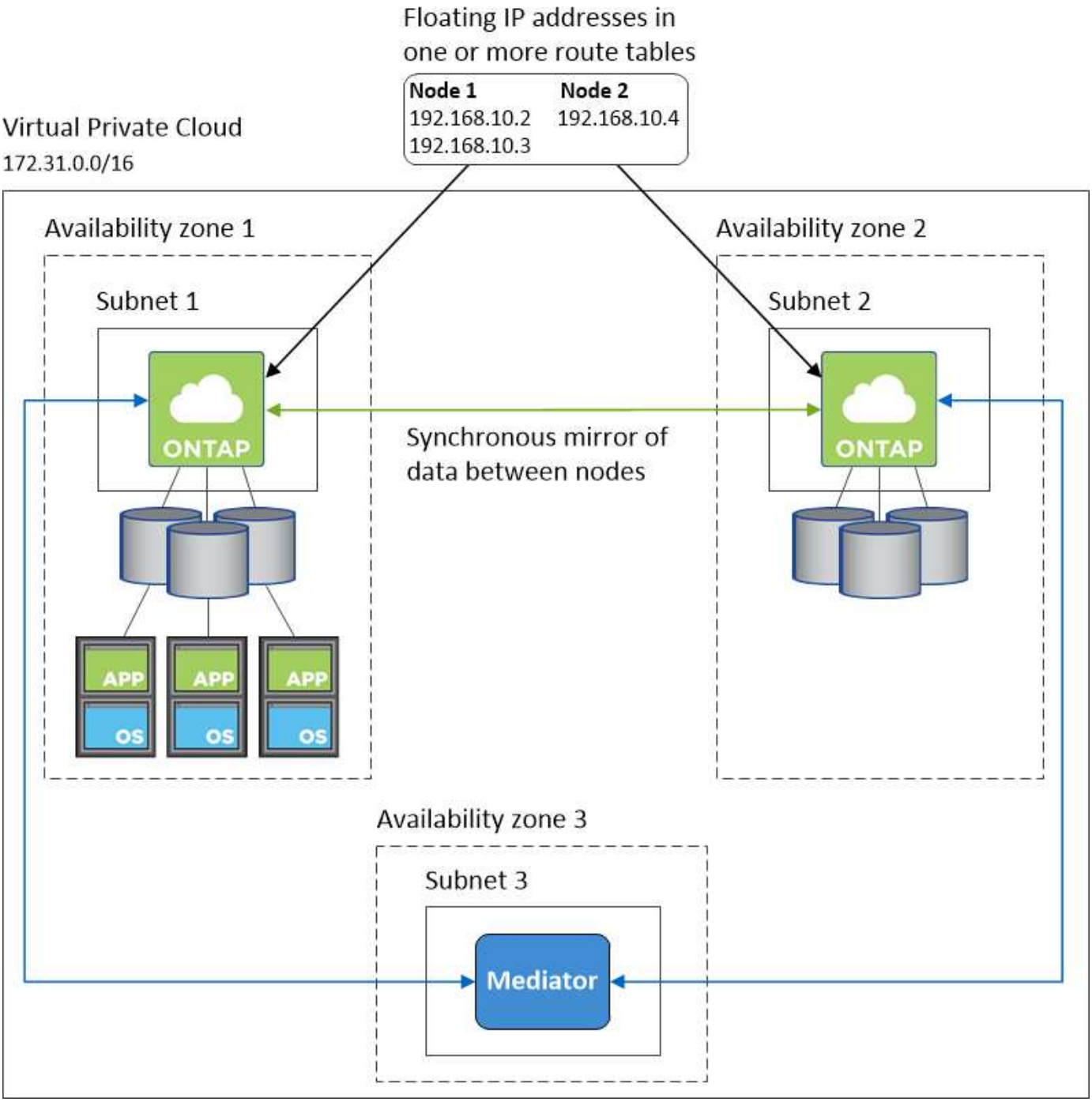
与 **NetApp** 管理工具的连接

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

1. 在其他 VPC 和中部署 NetApp 管理工具 "设置 AWS 传输网关"。通过网关，可以从 VPC 外部访问集群管理接口的浮动 IP 地址。
2. 在与 NAS 客户端具有类似路由配置的同一 VPC 中部署 NetApp 管理工具。

HA 配置示例

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



连接器的要求

如果尚未创建Connector、则还应查看Connector的网络要求。

- "查看连接器的网络要求"
- "AWS中的安全组规则"

为多个 **AZs** 中的 **HA** 对设置 **AWS** 传输网关

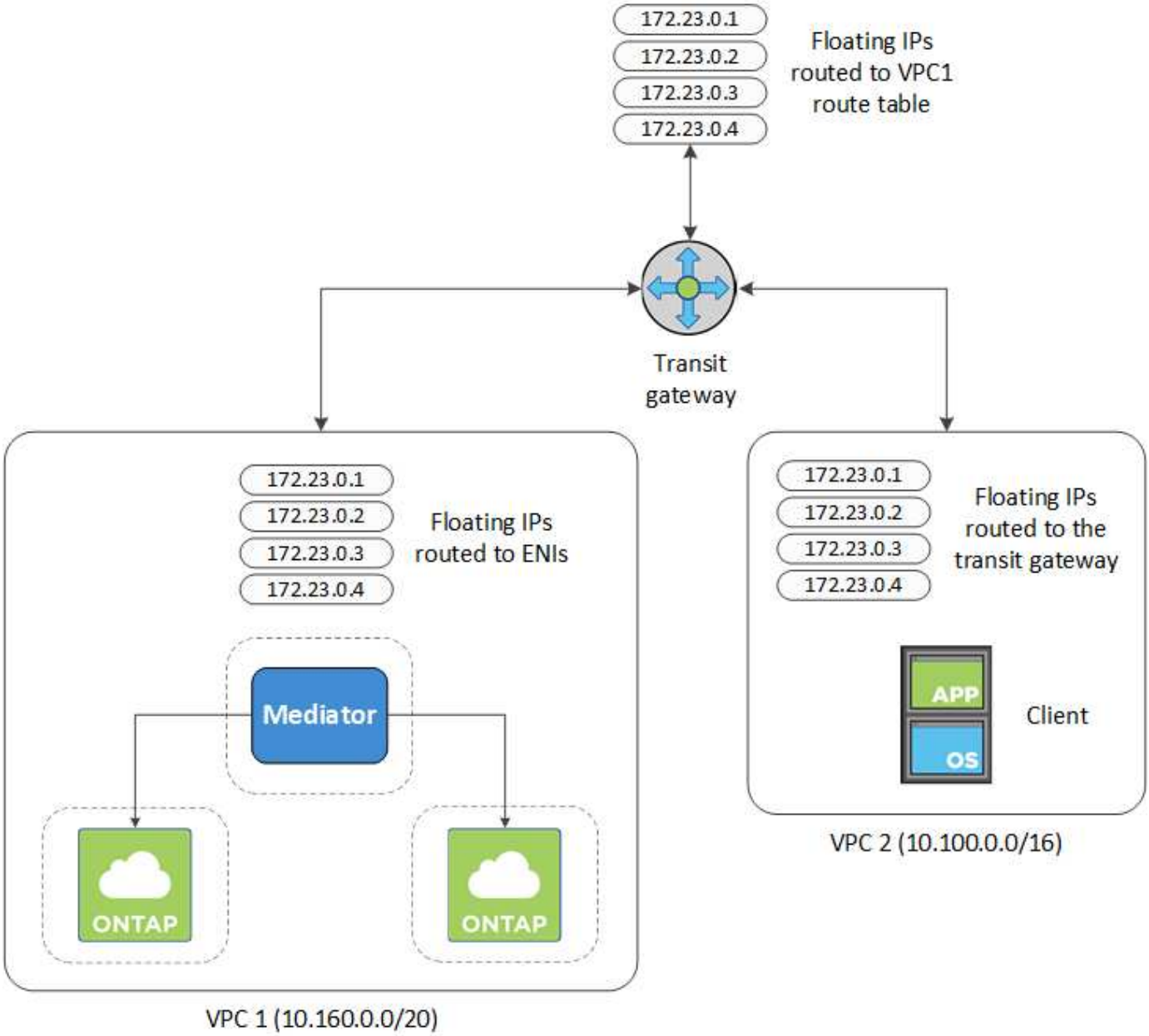
设置 AWS 传输网关以允许访问 HA 对 "浮动 IP 地址" 从 HA 对所在的 VPC 外部。

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

集群管理接口和可选 SVM 管理 LIF 也需要浮动 IP 地址。

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

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



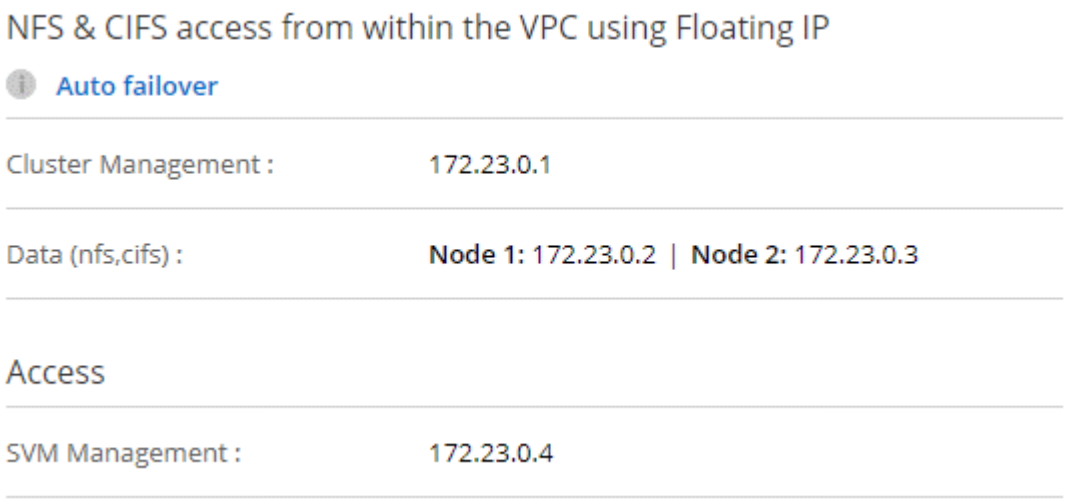
以下步骤说明了如何设置类似的配置。

步骤

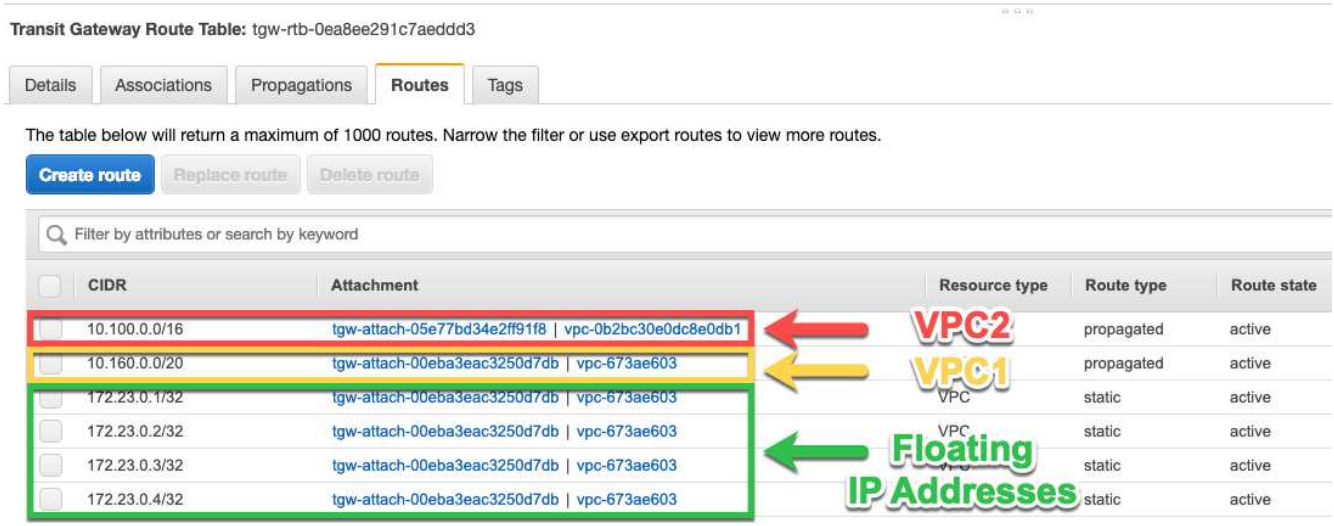
1. "创建传输网关并将 vPC 连接到该网关"。

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

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

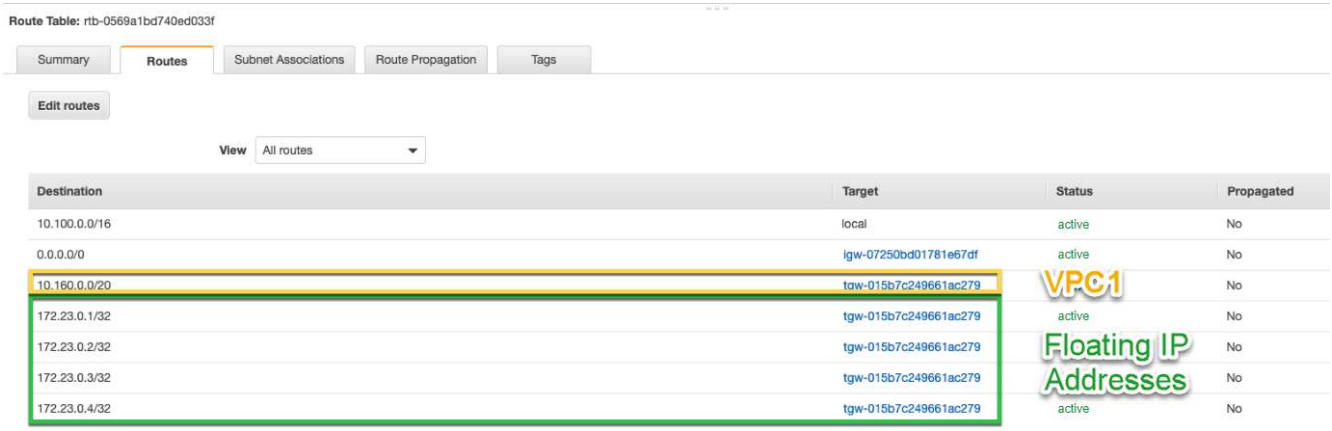


   下图示例显示了传输网关的路由表。它包括到 Cloud Volumes ONTAP 所使用的两个 vPC 的 CIDR 块和四个浮动 IP 地址的路由。



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

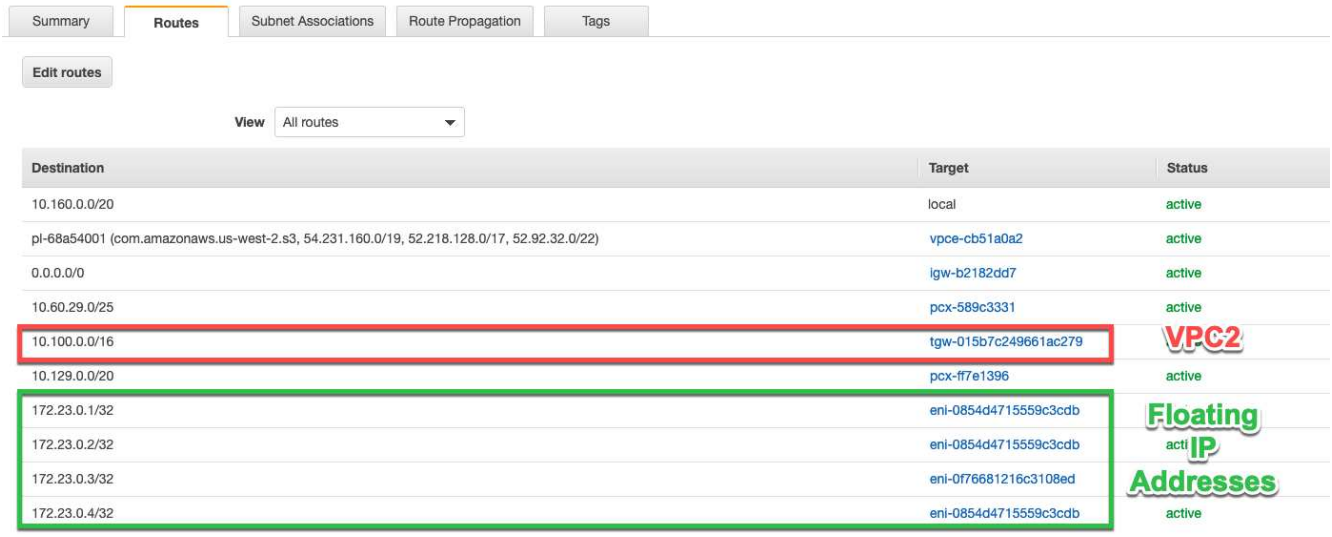
      下图示例显示了 VPC 2 的路由表，其中包括指向 VPC 1 的路由和浮动 IP 地址。



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

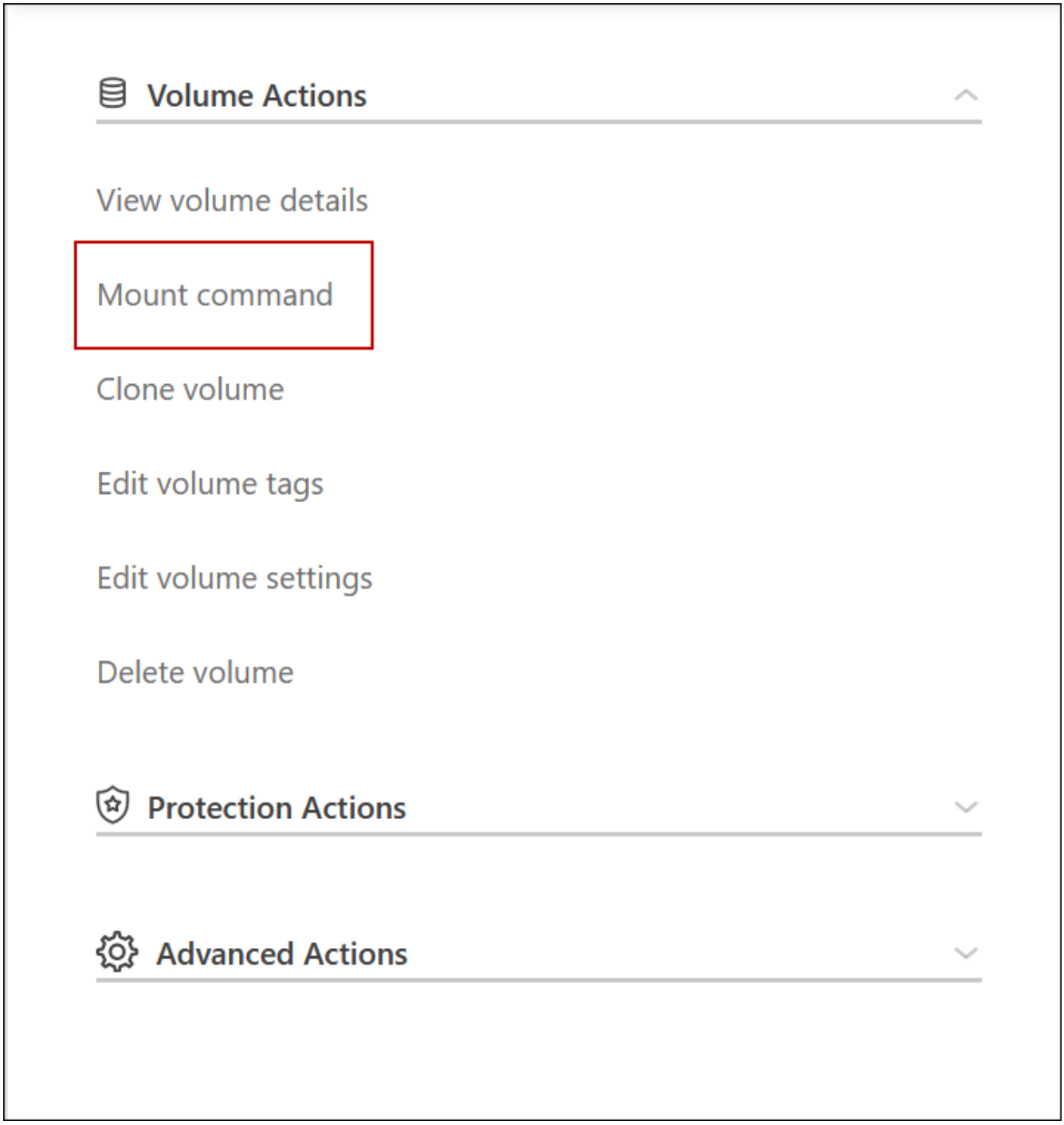
   此步骤非常重要，因为它会完成 VPC 之间的路由。

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



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BlueXP中"管理卷"面板下的*挂载命令*选项在BlueXP中找到正确的IP地址。



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

   "了解如何编辑卷"。

   - 相关链接 *
   - "AWS 中的高可用性对"
   - "AWS 中的 Cloud Volumes ONTAP 的网络要求"

在共享子网中部署HA对

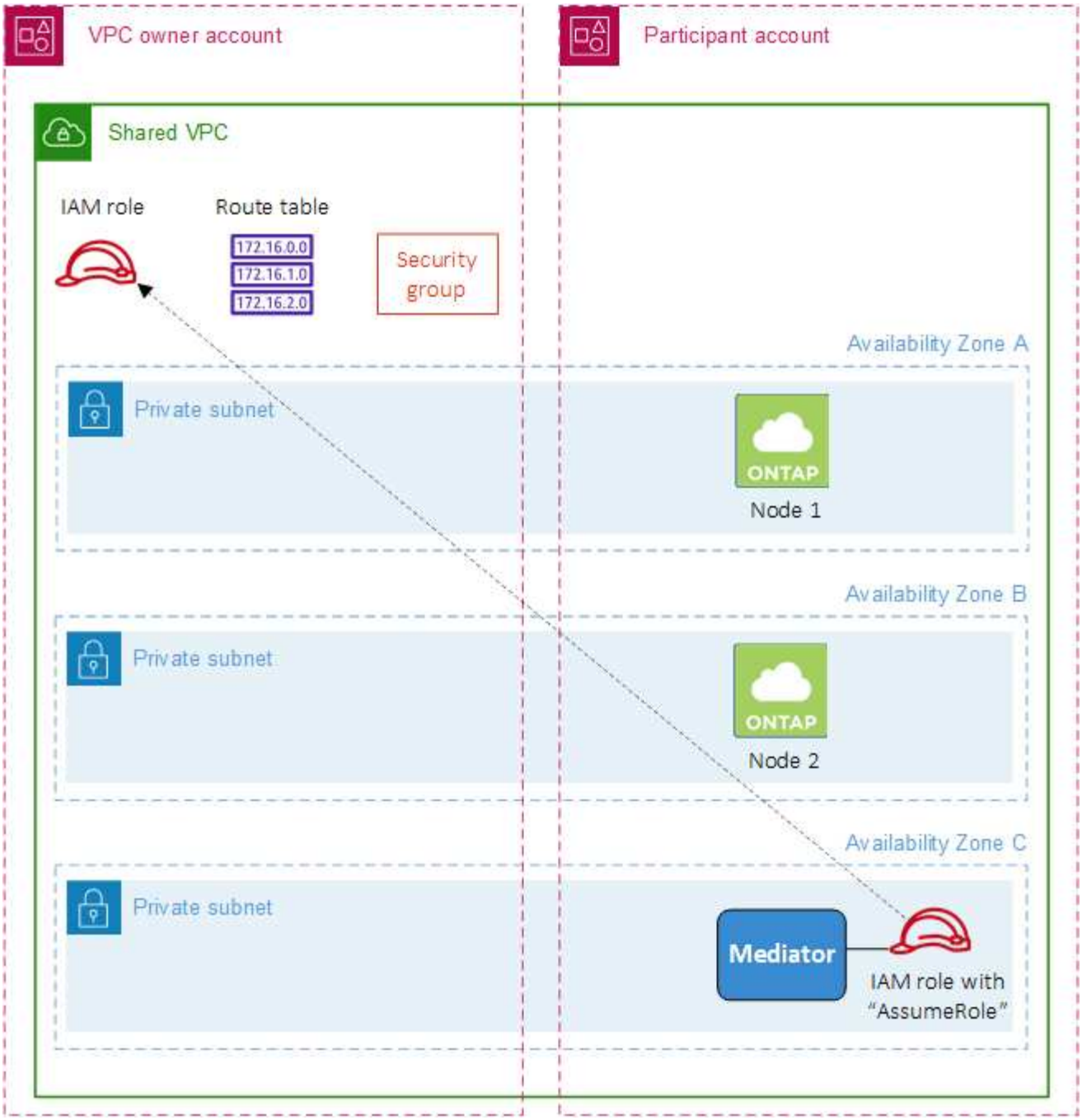
从9.11.1版开始、具有VPC共享的AWS支持Cloud Volumes ONTAP HA对。通过VPC共享、您的组织可以与其他AWS帐户共享子网。要使用此配置、您必须设置AWS环境、然后使用API部署HA对。

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

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

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

下图显示了此部署涉及的组件：



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

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

步骤

1. 与参与者帐户共享VPC所有者帐户中的子网。

   要在共享子网中部署HA对、需要执行此步骤。

   "AWS文档：共享子网"

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

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

3. 在VPC所有者帐户中、创建一个包含以下权限的IAM角色：

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

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

   请注意、您必须指定以下字段：

   - "securityGroupId"

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

   - "haParams"对象中的"assumeRoleArn"

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

     例如：

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

+
"了解Cloud Volumes ONTAP API"

AWS 的安全组规则

BlueXP会创建AWS安全组、其中包含Cloud Volumes ONTAP 成功运行所需的入站和出站规则。您可能需要参考端口进行测试，或者如果您希望使用自己的安全组。

Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

入站规则

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

- 仅选定**VPC**：入站流量的源是Cloud Volumes ONTAP 系统的VPC子网范围以及连接器所在VPC的子网范围。这是建议的选项。
- 所有vPC：入站流量的源IP范围为0.0.0.0/0。

协议	**Port**	目的
所有ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理LIF的IP地址连接Connector并通过HTTPS访问System Manager Web控制台
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049.	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049.	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

出站规则

为 Cloud Volumes ONTAP 预定义的安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您

需要更严格的规则、请使用高级出站规则。

基本外向规则

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

协议	**Port**	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

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

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

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

服务	协议	Port	源	目标	目的
AutoSupport	HTTPS	443.	节点管理 LIF	support.netapp.com	AutoSupport （默认设置为 HTTPS ）
	HTTP	80	节点管理 LIF	support.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）
	TCP	3128	节点管理 LIF	连接器	如果出站Internet连接不可用、则通过Connector上的代理服务器发送AutoSupport 消息
备份到 S3	TCP	5010	集群间 LIF	备份端点或还原端点	备份到 S3 功能的备份和还原操作
集群	所有流量	所有流量	一个节点上的所有 LIF	其它节点上的所有 LIF	集群间通信（仅限 Cloud Volumes ONTAP HA ）
	TCP	3000	节点管理 LIF	HA 调解器	ZAPI 调用（仅适用于 Cloud Volumes ONTAP HA ）
	ICMP	1.	节点管理 LIF	HA 调解器	保持活动状态（仅限 Cloud Volumes ONTAP HA ）
配置备份	HTTP	80	节点管理 LIF	\http ： //occm/offboxconfig <connector-IP-address>	将配置备份发送到Connector。 "了解配置备份文件"。
DHCP	UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
DHCP	UDP	67	节点管理 LIF	DHCP	DHCP 服务器
DNS	UDP	53.	节点管理 LIF 和数据 LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 – 18699	节点管理 LIF	目标服务器	NDMP 副本
SMTP	TCP	25.	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
SNMP	TCP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	161.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	TCP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
	UDP	162.	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控
SnapMirror	TCP	11104.	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话
	TCP	11105.	集群间 LIF	ONTAP 集群间 LIF	SnapMirror 数据传输
系统日志	UDP	514.	节点管理 LIF	系统日志服务器	系统日志转发消息

HA 调解器外部安全组的规则

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

入站规则

HA调解器的预定义安全组包括以下入站规则。

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

出站规则

HA 调解器的预定义安全组将打开所有出站通信。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

HA 调解器的预定义安全组包括以下出站规则。

协议	**Port**	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

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

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

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

HA配置内部安全组的规则

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

BlueXP始终会创建此安全组。您没有使用自己的选项。

入站规则

预定义的安全组包括以下入站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

出站规则

预定义的安全组包括以下出站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

Connector 的规则

"查看Connector的安全组规则"

设置 AWS KMS

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

步骤

1. 确保存在有效的客户主密钥（CMK）。

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

   "AWS 文档：客户主密钥（CMK）"

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

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

   "AWS 文档：编辑密钥"

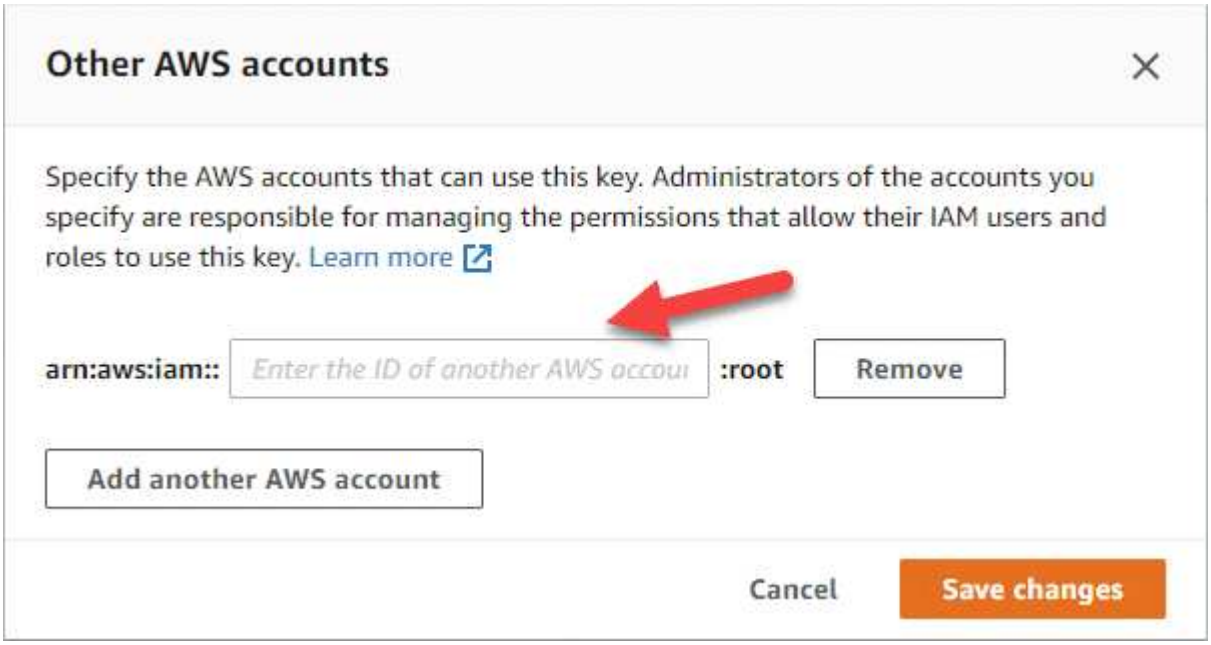
3. 如果 CMK 位于其他 AWS 帐户中，请完成以下步骤：

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

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

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

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



e. 现在、切换到为BlueXP提供权限的AWS帐户、然后打开IAM控制台。

f. 创建一个包含以下权限的 IAM 策略。

g. 将策略附加到为BlueXP提供权限的IAM角色或IAM用户。

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

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

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

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

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

要执行此步骤。

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

"AWS 文档：编辑密钥"

为Cloud Volumes ONTAP 设置IAM角色

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

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

> 在AWS商用云服务环境中、需要提供您自己的IAM角色。 "了解如何在C2S中部署Cloud Volumes ONTAP"。

步骤

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

标准区域

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

GovCloud (美国)地区

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

C2S环境

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

- Cloud Volumes ONTAP 节点的备份策略

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

标准区域

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

GovCloud (美国)地区

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

C2S环境

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

- HA 调解器

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

3. 创建IAM角色并将您创建的策略附加到该角色。

结果

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

更多信息

- "AWS文档：创建IAM策略"
- "AWS文档：创建IAM角色"

在AWS中为Cloud Volumes ONTAP 设置许可

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

免费

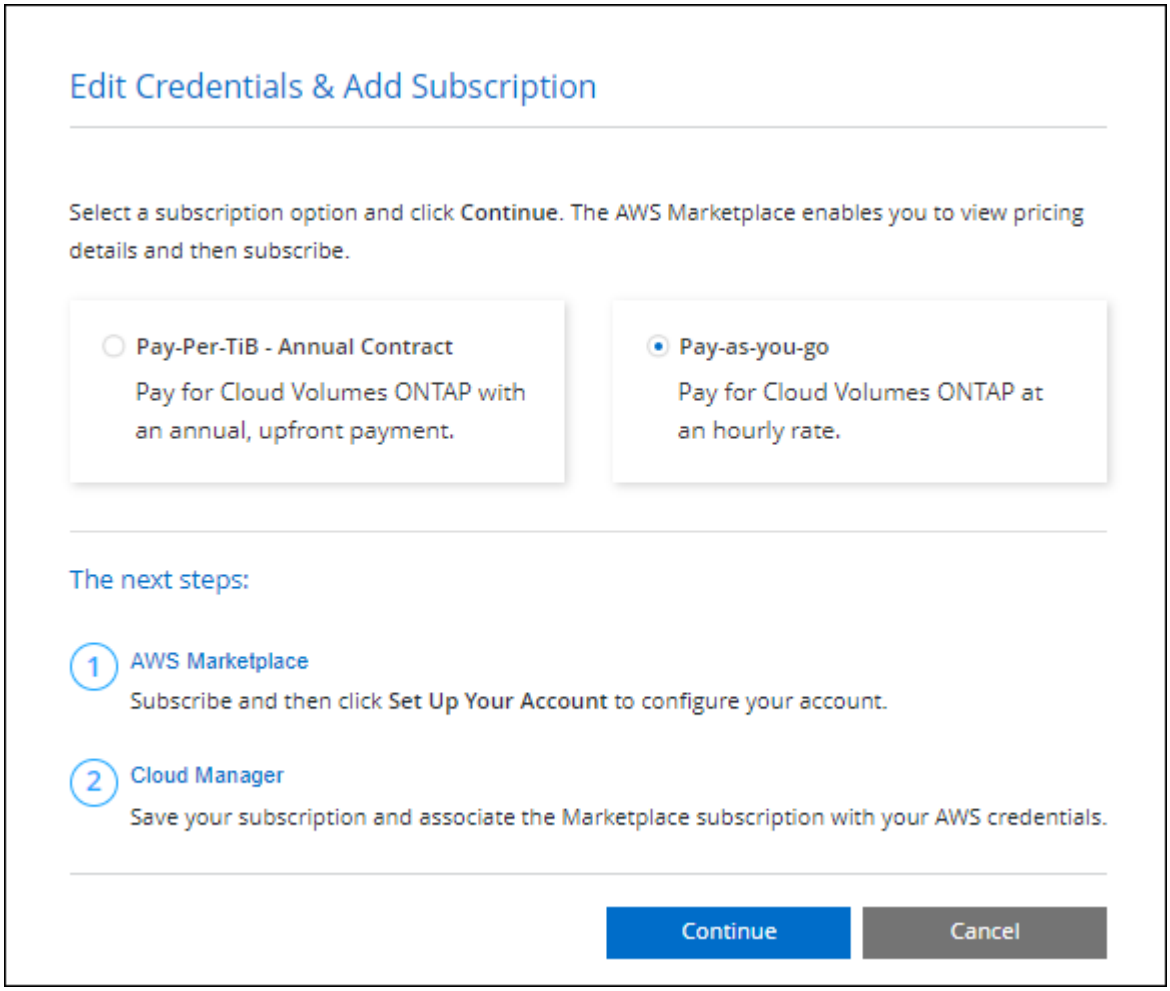
选择免费提供的Cloud Volumes ONTAP 、可在配置容量高达500 GiB的情况下免费使用。 "了解有关免费提供的更多信息"。

步骤

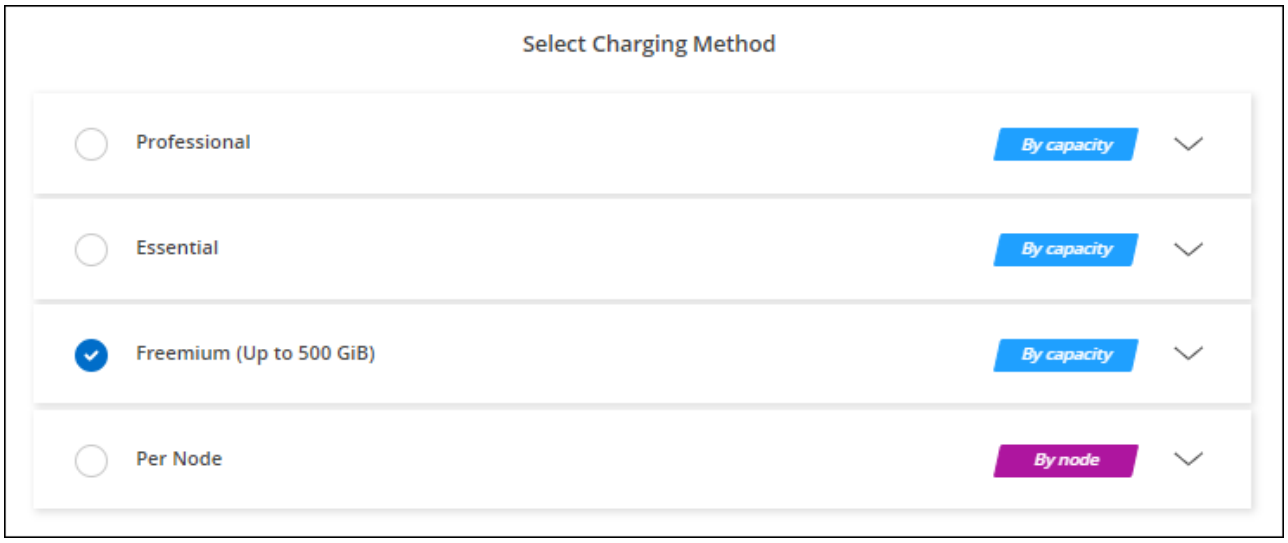
1. 从左侧导航菜单中、选择*存储>画布*。
2. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP中的步骤进行操作。

a. 在*详细信息和凭据*页面上、单击*编辑凭据>添加订阅*、然后按照提示订阅AWS Marketplace中的按需购买服务。

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



a. 返回到BlueXP后、访问充电方法页面时选择*免费*。



"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

基于容量的许可证

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

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

- 从 NetApp 购买的许可证（ BYOL ）
- AWS Marketplace提供的每小时按需购买(PAYGO)订阅
- AWS Marketplace的年度合同

"了解有关基于容量的许可的更多信息"。

以下各节介绍了如何开始使用上述每种消费模式。

BYOL

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

步骤

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

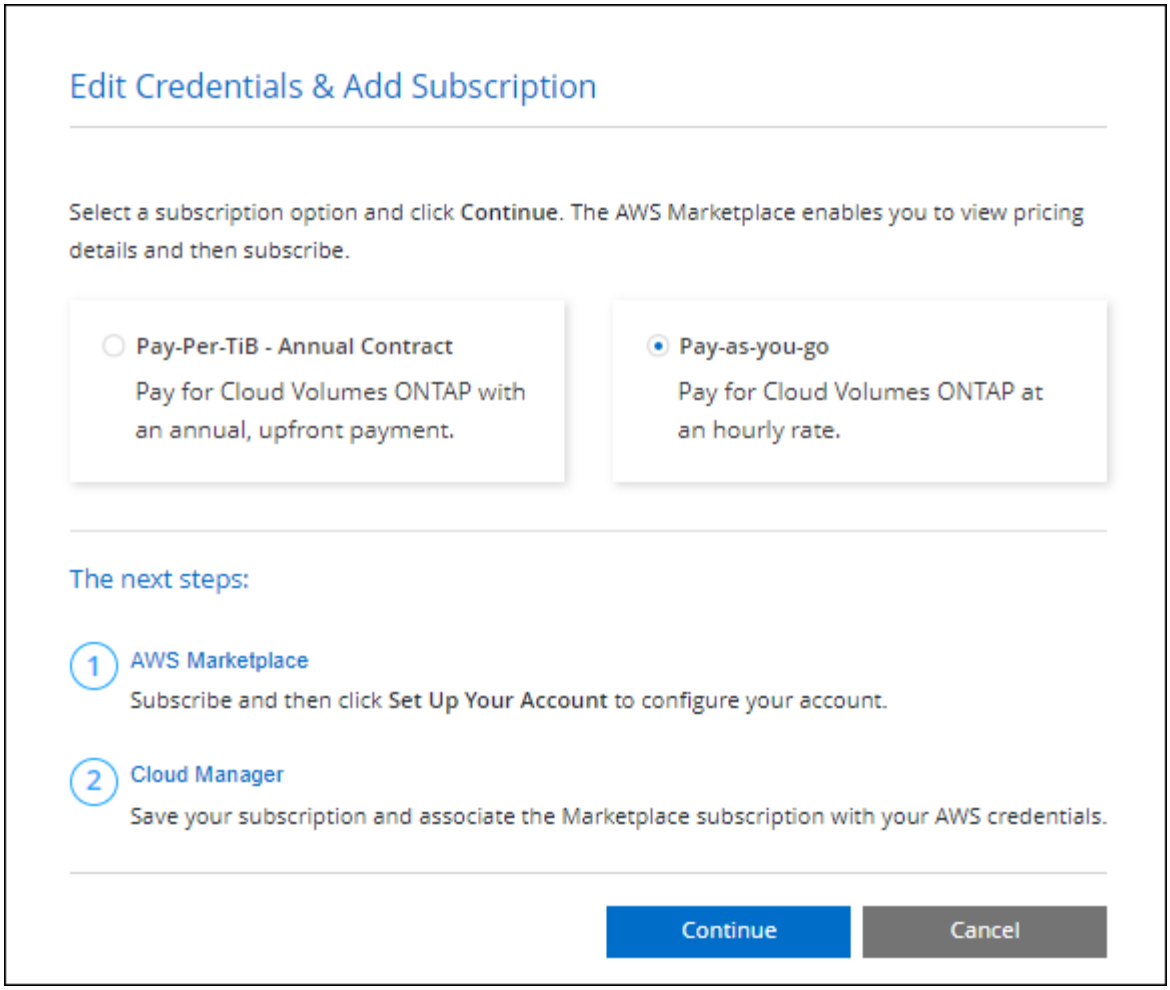
   BlueXP会自动查询NetApp的许可服务、以获取与您的NetApp 支持站点 帐户关联的许可证的详细信息。如果没有错误、BlueXP会自动将许可证添加到电子钱包中。

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

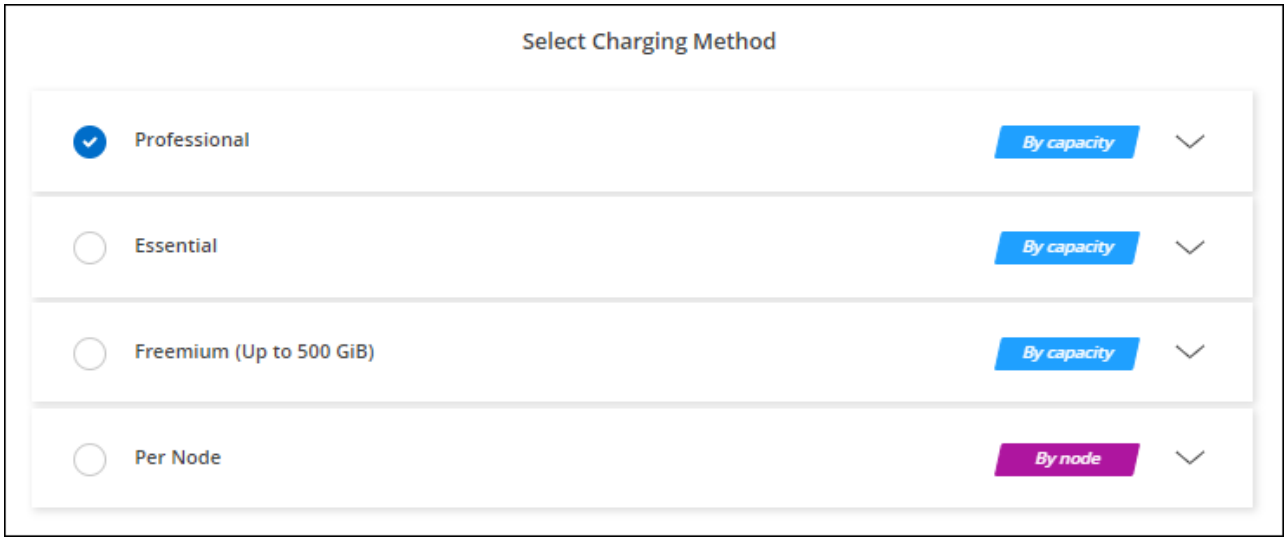
3. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP中的步骤进行操作。

   a. 在*详细信息和凭据*页面上、单击*编辑凭据>添加订阅*、然后按照提示订阅AWS Marketplace中的按需购买服务。

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



a. 返回到BlueXP后、在访问充电方法页面时选择一个基于容量的软件包。



"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

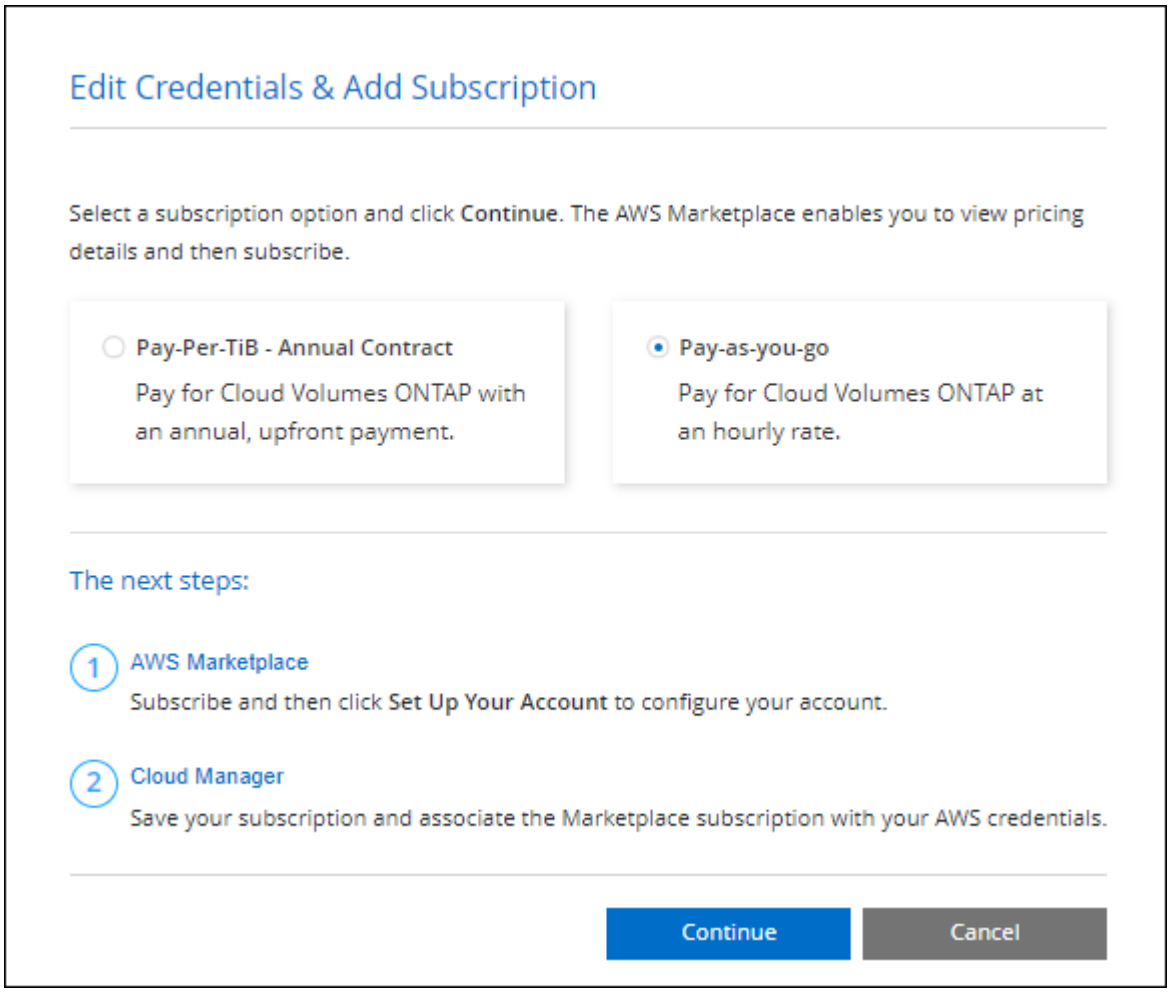
PAYGO订阅

通过从云提供商的市场订阅优惠按小时付费。

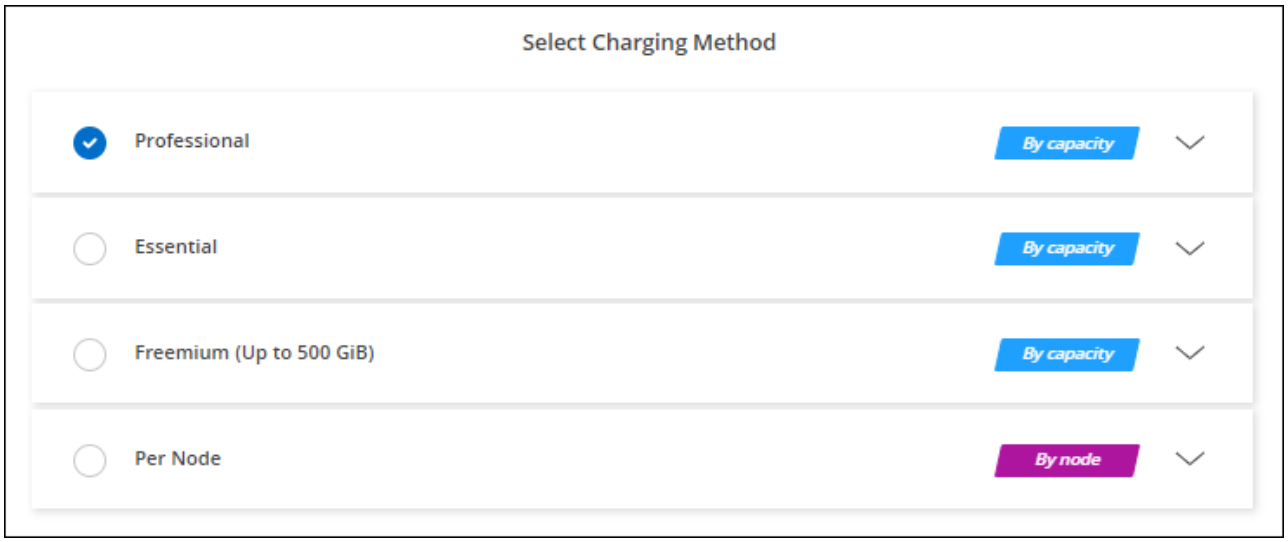
创建Cloud Volumes ONTAP 工作环境时、BlueXP会提示您订阅AWS Marketplace中提供的协议。然后、该订阅将与工作环境关联以进行收费。您可以对其他工作环境使用相同的订阅。

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP中的步骤进行操作。
   a. 在*详细信息和凭据*页面上、单击*编辑凭据>添加订阅*、然后按照提示订阅AWS Marketplace中的按需购买服务。



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



"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

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

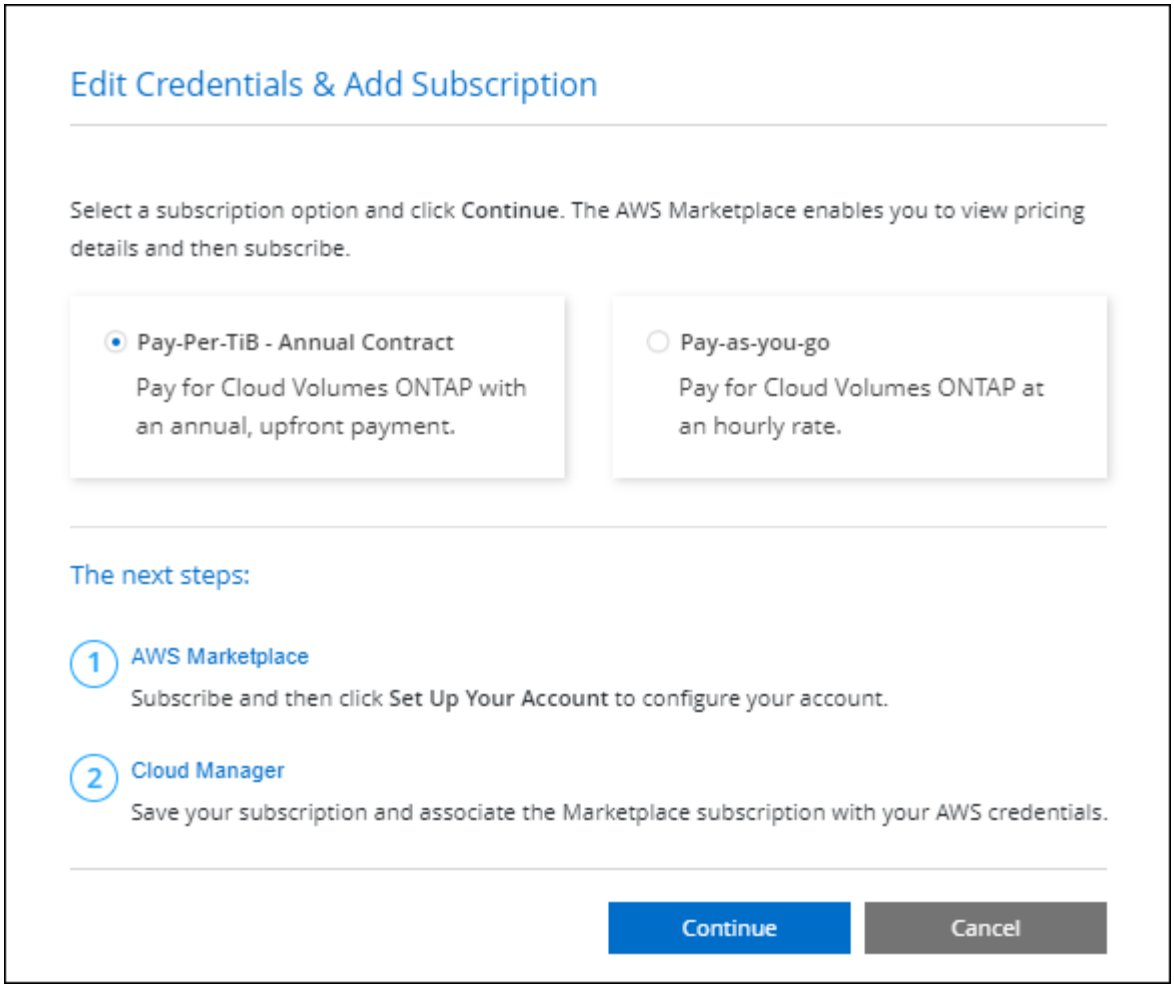
年度合同

通过从云提供商的市场购买年度合同、按年付费。

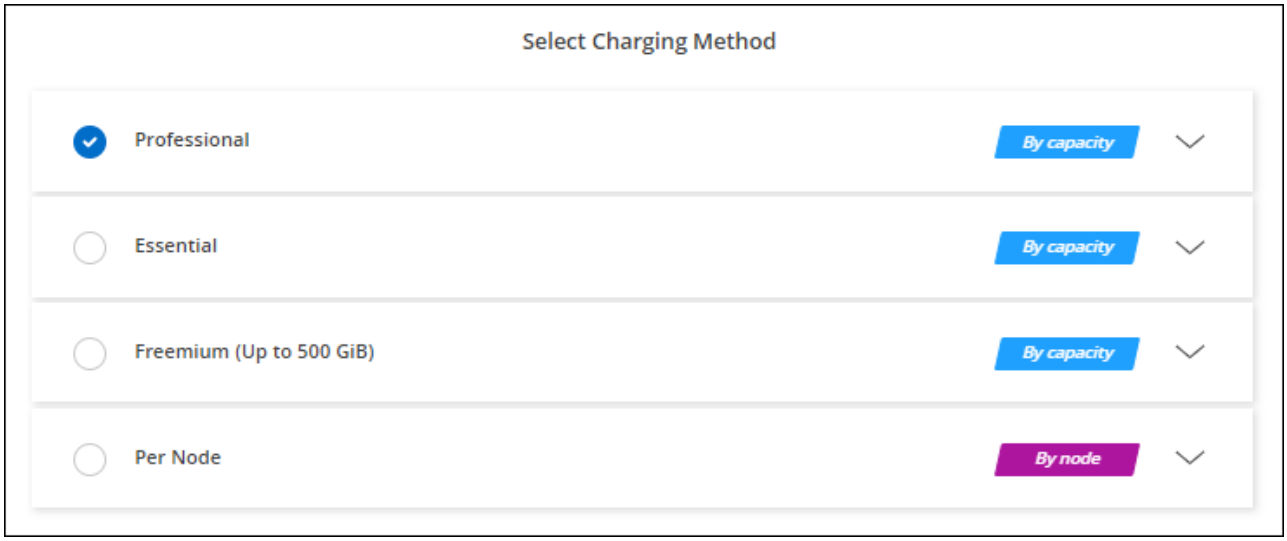
与每小时订阅类似、BlueXP会提示您订阅AWS Marketplace中提供的年度合同。

步骤

1. 在"画布"页面上、单击*添加工作环境*、然后按照BlueXP中的步骤进行操作。
    a. 在*详细信息和凭据*页面上、单击*编辑凭据>添加订阅*、然后按照提示在AWS Marketplace中订阅年度合同。



b. 返回到BlueXP后、在访问充电方法页面时选择一个基于容量的软件包。



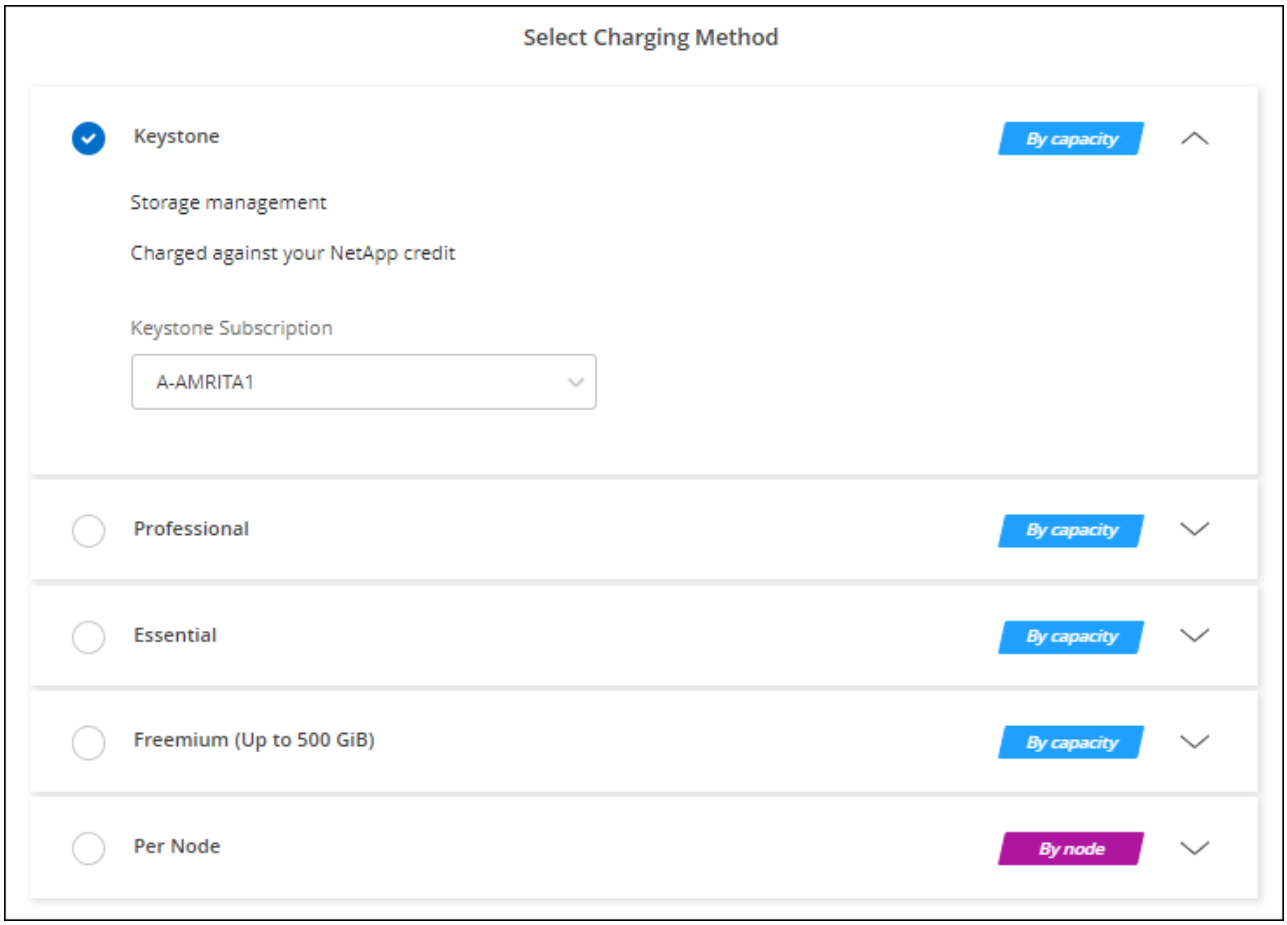
"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

Keystone订阅

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

步骤

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



"查看在AWS中启动Cloud Volumes ONTAP 的分步说明"。

在 AWS 中启动 Cloud Volumes ONTAP

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

开始之前

要创建工作环境，您需要满足以下要求。

- 已启动且正在运行的连接器。
  - 您应具有 "与工作空间关联的连接器"。

- "您应做好准备，使 Connector 始终保持运行"。

- 了解要使用的配置。

  您应该已准备好选择配置并从管理员处获取 AWS 网络信息。有关详细信息，请参见 "规划 Cloud Volumes ONTAP 配置"。

- 了解为Cloud Volumes ONTAP 设置许可所需的条件。

  "了解如何设置许可"。

- 用于 CIFS 配置的 DNS 和 Active Directory 。

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

在 AWS 中启动单节点 Cloud Volumes ONTAP 系统

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

关于此任务

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

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 【订阅】在 " 画布 " 页面上，单击 * 添加工作环境 * 并按照提示进行操作。
3. * 选择一个位置 * ： 选择 * Amazon Web Services* 和 * Cloud Volumes ONTAP Single Node* 。
4. 如果出现提示， "创建连接器"。
5. * 详细信息和凭据 * ： 可选择更改 AWS 凭据和订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

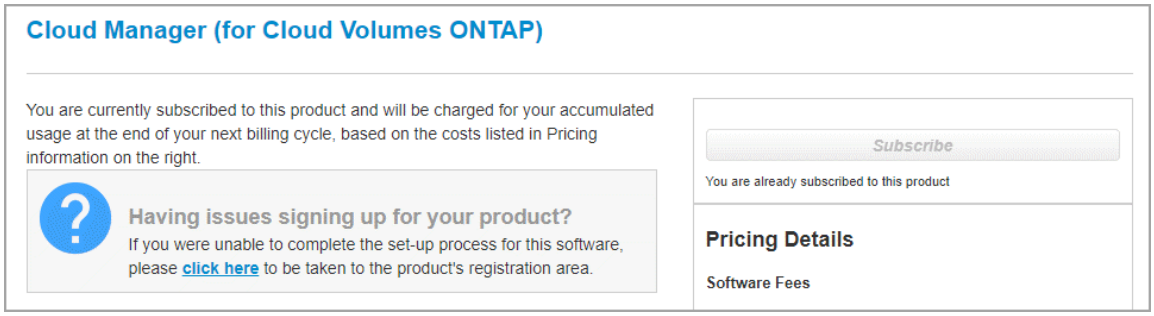
   本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	**Description**
工作环境名称	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Amazon EC2实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。
添加标记	AWS 标记是 AWS 资源的元数据。BlueXP会将标记添加到Cloud Volumes ONTAP 实例以及与该实例关联的每个AWS资源。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时， API 不会将您限制为四个标记。有关标记的信息，请参见 "AWS 文档：标记 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 System Manager 或其命令行界面连接到 Cloud Volumes ONTAP 。保留默认的 *admin* 用户名或将其更改为自定义用户名。

字段	Description
编辑凭据	选择与要部署此系统的帐户关联的 AWS 凭据。您还可以关联 AWS Marketplace 订阅以用于此 Cloud Volumes ONTAP 系统。 单击 * 添加订阅 * 将选定凭据与新的 AWS Marketplace 订阅关联。订阅可以是一份年度合同，也可以是按小时付费的 Cloud Volumes ONTAP 。 "了解如何向BlueXP添加其他AWS凭据"。

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

从AWS Marketplace订阅BlueXP

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

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

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

7. * 位置和连接 *： 输入您在中记录的网络信息 "AWS 工作表"。

   下表介绍了可能需要指导的字段：

字段	Description
VPC	如果您有 AWS 前台，则可以通过选择前台 VPC 在该前台部署单节点 Cloud Volumes ONTAP 系统。体验与 AWS 中的任何其他 VPC 相同。
已生成安全组	如果您让BlueXP为您生成安全组、则需要选择允许流量的方式： • 如果选择*仅选定VPC *、则入站流量的源是选定VPC的子网范围以及Connector所在VPC的子网范围。这是建议的选项。 • 如果选择*所有VPC*、则入站流量的源IP范围为0.0.0.0/0。

字段	Description
使用现有安全组	如果您使用现有防火墙策略、请确保该策略包含所需的规则。 "了解Cloud Volumes ONTAP 的防火墙规则"。

8. * 数据加密 * ：不选择数据加密或 AWS 管理的加密。

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

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

   "了解如何为 Cloud Volumes ONTAP 设置 AWS KMS"。

   "了解有关支持的加密技术的更多信息"。

9. * 充电方法和 NSS 帐户 * ：指定要在此系统中使用的充电选项，然后指定 NetApp 支持站点帐户。
   - "了解 Cloud Volumes ONTAP 的许可选项"。
   - "了解如何设置许可"。
10. * Cloud Volumes ONTAP 配置 * （仅限年度 Marketplace 合同）：查看默认配置，然后单击 * 继续 * 或单击 * 更改配置 * 以选择您自己的配置。

    如果保留默认配置，则只需指定一个卷，然后查看并批准该配置。

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

    如果选择其中一个软件包，则只需指定一个卷，然后查看并批准该配置。

12. * IAM角色*：最好保留默认选项、让BlueXP为您创建角色。

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

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

    > 如果选定版本具有较新的候选版本、通用可用性或修补程序版本、则在创建工作环境时、BlueXP会将系统更新到该版本。例如、如果选择Cloud Volumes ONTAP 9.10.1和9.10.1 P4可用、则会发生更新。更新不会从一个版本更新到另一个版本，例如从 9.6 到 9.7 。

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

    请注意以下事项：

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

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

  "了解数据分层的工作原理"。

15. 写入速度和**WORM**：

    a. 如果需要、选择*正常*或*高*写入速度。

    "了解有关写入速度的更多信息。"。

    b. 根据需要激活一次写入、多次读取(WORM)存储。

    如果为Cloud Volumes ONTAP 9.7及更低版本启用了数据分层、则无法启用WORM。启用WORM和分层后、将阻止还原或降级到Cloud Volumes ONTAP 9.8。

"了解有关 WORM 存储的更多信息。"。

    a. 如果激活了WORM存储、请选择保留期限。

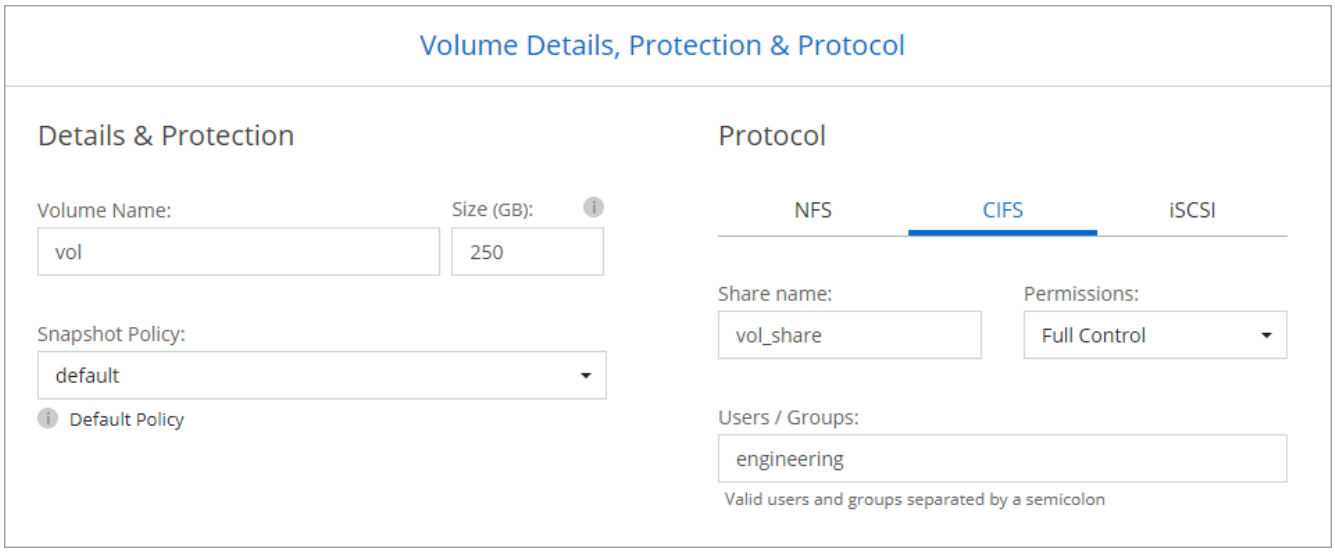
16. * 创建卷 * ：输入新卷的详细信息或单击 * 跳过 * 。

"了解支持的客户端协议和版本"。

本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

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

下图显示了已填写 CIFS 协议的卷页面：



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

字段	Description
DNS 主 IP 地址和次 IP 地址	为 CIFS 服务器提供名称解析的 DNS 服务器的 IP 地址。列出的 DNS 服务器必须包含为 CIFS 服务器将加入的域定位 Active Directory LDAP 服务器和域控制器所需的服务位置记录（服务位置记录）。
要加入的 Active Directory 域	您希望 CIFS 服务器加入的 Active Directory （AD）域的 FQDN 。
授权加入域的凭据	具有足够权限将计算机添加到 AD 域中指定组织单位 (OU) 的 Windows 帐户的名称和密码。
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers 。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，则应在此字段中输入 * OU=Computers ， OU=corp* 。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine （SVM）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器，则应使用 API 。请参见 "BlueXP 自动化文档" 了解详细信息。 请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。

18. * 使用情况配置文件，磁盘类型和分层策略 *：选择是否要启用存储效率功能并根据需要编辑卷分层策略。

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

19. * 审核并批准 *：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 单击*更多信息*可查看有关支持和BlueXP将购买的AWS资源的详细信息。

c. 选中 * 我了解 …* 复选框。

d. 单击 * 执行 * 。

结果

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

如果在启动 Cloud Volumes ONTAP 实例时遇到任何问题，请查看故障消息。您还可以选择工作环境并单击重新创建环境。

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

完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI 。

  配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

在 AWS 中启动 Cloud Volumes ONTAP HA 对

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

限制

目前， AWS 前向不支持 HA 对。

关于此任务

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

步骤

1. 从左侧导航菜单中、选择*存储>画布*。
2. 在 " 画布 " 页面上，单击 * 添加工作环境 * 并按照提示进行操作。
3. 选择一个位置：选择* Amazon Web Services*和* Cloud Volumes ONTAP HA*。
4. * 详细信息和凭据 * ：可选择更改 AWS 凭据和订阅，输入工作环境名称，根据需要添加标记，然后输入密码。

   本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

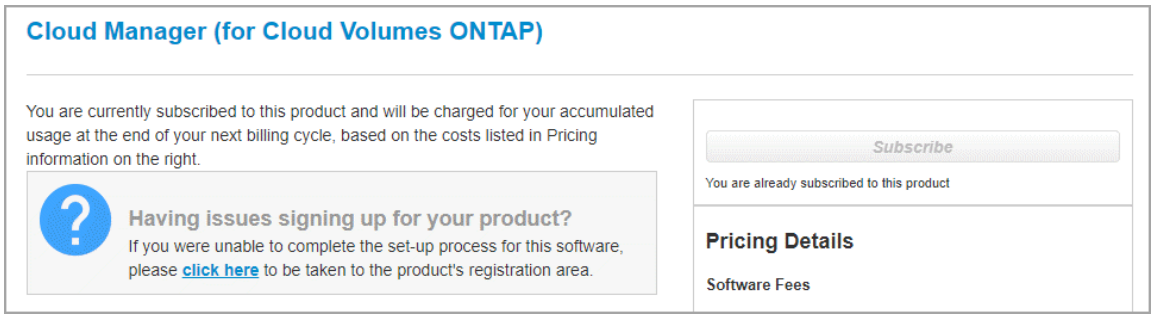
字段	Description
工作环境名称	BlueXP使用工作环境名称来命名Cloud Volumes ONTAP 系统和Amazon EC2实例。如果您选择了预定义安全组的前缀，则它还会使用该名称作为前缀。

字段	Description
添加标记	AWS 标记是 AWS 资源的元数据。BlueXP会将标记添加到Cloud Volumes ONTAP 实例以及与该实例关联的每个AWS资源。在创建工作环境时，最多可以从用户界面添加四个标签，然后可以在创建工作环境后添加更多标签。请注意，在创建工作环境时， API 不会将您限制为四个标记。有关标记的信息，请参见 "AWS 文档：标记 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 System Manager 或其命令行界面连接到 Cloud Volumes ONTAP 。保留默认的 *admin* 用户名或将其更改为自定义用户名。
编辑凭据	选择要用于此 Cloud Volumes ONTAP 系统的 AWS 凭据和 Marketplace 订阅。 单击 * 添加订阅 * 将选定凭据与新的 AWS Marketplace 订阅关联。订阅可以是一份年度合同，也可以是按小时付费的 Cloud Volumes ONTAP 。 如果直接从 NetApp （ BYOL ）购买许可证，则不需要 AWS 订阅。 "了解如何向BlueXP添加其他AWS凭据"。

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

从AWS Marketplace订阅BlueXP

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



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

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

6. * 高可用性部署模式 * ：选择一个高可用性配置。

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

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

下表介绍了可能需要指导的字段：

字段	Description
已生成安全组	如果您让BlueXP为您生成安全组、则需要选择允许流量的方式： • 如果选择*仅选定VPC *、则入站流量的源是选定VPC的子网范围以及Connector所在VPC的子网范围。这是建议的选项。 • 如果选择*所有VPC*、则入站流量的源IP范围为0.0.0.0/0。
使用现有安全组	如果您使用现有防火墙策略、请确保该策略包含所需的规则。 "了解Cloud Volumes ONTAP 的防火墙规则"。

8. * 连接和 SSH 身份验证 *： 选择 HA 对和调解器的连接方法。
9. * 浮动 IP*： 如果选择多个 AZs ，请指定浮动 IP 地址。

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

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

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

11. * 数据加密 *： 不选择数据加密或 AWS 管理的加密。

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

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

    "了解如何为 Cloud Volumes ONTAP 设置 AWS KMS"。

    "了解有关支持的加密技术的更多信息"。

12. * 充电方法和 NSS 帐户 *： 指定要在此系统中使用的充电选项，然后指定 NetApp 支持站点帐户。
    - "了解 Cloud Volumes ONTAP 的许可选项"。
    - "了解如何设置许可"。
13. * Cloud Volumes ONTAP 配置 * （仅限年度 Marketplace 合同）： 查看默认配置，然后单击 * 继续 * 或单击 * 更改配置 * 以选择您自己的配置。

    如果保留默认配置，则只需指定一个卷，然后查看并批准该配置。

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

    如果选择其中一个软件包，则只需指定一个卷，然后查看并批准该配置。

15. * IAM角色*：最好保留默认选项、让BlueXP为您创建角色。

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

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

> 如果选定版本具有较新的候选版本、通用可用性或修补程序版本、则在创建工作环境时、BlueXP会将系统更新到该版本。例如、如果选择Cloud Volumes ONTAP 9.10.1和9.10.1 P4可用、则会发生更新。更新不会从一个版本更新到另一个版本，例如从 9.6 到 9.7 。

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

    请注意以下事项：

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

      "了解数据分层的工作原理"。

18. 写入速度和**WORM**：

    a. 如果需要、选择*正常*或*高*写入速度。

       "了解有关写入速度的更多信息。"。

    b. 根据需要激活一次写入、多次读取(WORM)存储。

       如果为Cloud Volumes ONTAP 9.7及更低版本启用了数据分层、则无法启用WORM。启用WORM和分层后、将阻止还原或降级到Cloud Volumes ONTAP 9.8。

    "了解有关 WORM 存储的更多信息。"。

    a. 如果激活了WORM存储、请选择保留期限。

19. * 创建卷 * ：输入新卷的详细信息或单击 * 跳过 * 。

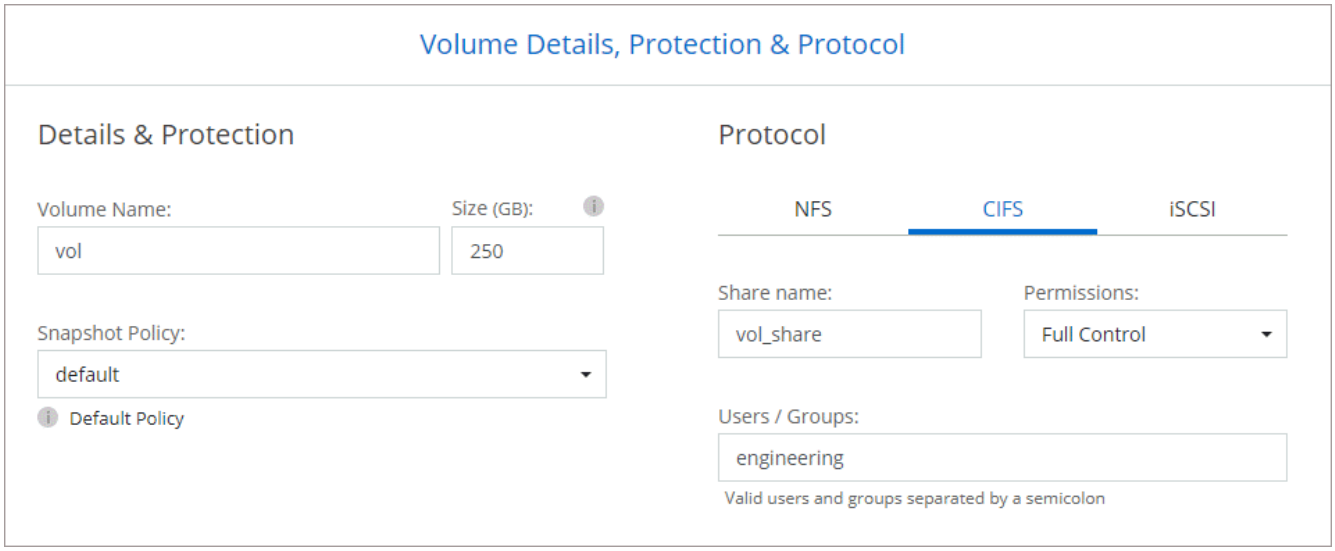
    "了解支持的客户端协议和版本"。

    本页中的某些字段是不言自明的。下表介绍了可能需要指导的字段：

字段	**Description**
Size	您可以输入的最大大小在很大程度上取决于您是否启用精简配置、这样您就可以创建一个大于当前可用物理存储的卷。
访问控制（仅适用于 NFS）	导出策略定义子网中可以访问卷的客户端。默认情况下、BlueXP输入一个值、用于访问子网中的所有实例。

字段	Description
权限和用户 / 组（仅限 CIFS ）	这些字段使您能够控制用户和组对共享的访问级别（也称为访问控制列表或 ACL ）。您可以指定本地或域 Windows 用户或组、 UNIX 用户或组。如果指定域 Windows 用户名，则必须使用 domain\username 格式包含用户的域。
快照策略	Snapshot 副本策略指定自动创建的 NetApp Snapshot 副本的频率和数量。NetApp Snapshot 副本是一个时间点文件系统映像、对性能没有影响、并且只需要极少的存储。您可以选择默认策略或无。您可以为瞬态数据选择无：例如， Microsoft SQL Server 的 tempdb 。
高级选项（仅适用于 NFS ）	为卷选择 NFS 版本： NFSv3 或 NFSv4 。
启动程序组和 IQN （仅适用于 iSCSI ）	iSCSI 存储目标称为 LUN （逻辑单元），并作为标准块设备提供给主机。启动程序组是包含 iSCSI 主机节点名称的表，用于控制哪些启动程序可以访问哪些 LUN 。iSCSI 目标通过标准以太网网络适配器（ NIC ），带软件启动程序的 TCP 卸载引擎（ TOE ）卡，融合网络适配器（ CNA ）或专用主机总线适配器（ HBA ）连接到网络，并通过 iSCSI 限定名称（ IQN ）进行标识。创建iSCSI卷时、BlueXP会自动为您创建LUN。我们通过为每个卷仅创建一个 LUN 来简化此过程，因此无需进行管理。创建卷后， "使用 IQN 从主机连接到 LUN"。

下图显示了已填写 CIFS 协议的卷页面：



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

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

字段	Description
CIFS server NetBIOS name	在 AD 域中唯一的 CIFS 服务器名称。
组织单位	AD 域中要与 CIFS 服务器关联的组织单元。默认值为 cn = computers 。如果将 AWS 托管 Microsoft AD 配置为 Cloud Volumes ONTAP 的 AD 服务器，则应在此字段中输入 * OU=Computers ， OU=corp* 。
DNS 域	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）的 DNS 域。在大多数情况下，域与 AD 域相同。
NTP 服务器	选择 * 使用 Active Directory 域 * 以使用 Active Directory DNS 配置 NTP 服务器。如果需要使用其他地址配置 NTP 服务器，则应使用 API 。请参见 "BlueXP 自动化文档" 了解详细信息。 请注意，只有在创建 CIFS 服务器时才能配置 NTP 服务器。在创建 CIFS 服务器后，它不可配置。

21. * 使用情况配置文件，磁盘类型和分层策略 * ：选择是否要启用存储效率功能并根据需要编辑卷分层策略。

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

22. * 审核并批准 * ：审核并确认您的选择。
    a. 查看有关配置的详细信息。
    b. 单击*更多信息*可查看有关支持和BlueXP将购买的AWS资源的详细信息。
    c. 选中 * 我了解 …* 复选框。
    d. 单击 * 执行 * 。

结果

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

如果在启动 HA 对时遇到任何问题、请查看故障消息。您还可以选择工作环境并单击重新创建环境。

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

完成后

- 如果配置了 CIFS 共享、请授予用户或组对文件和文件夹的权限、并验证这些用户是否可以访问该共享并创建文件。
- 如果要对卷应用配额、请使用 System Manager 或 CLI 。

  配额允许您限制或跟踪用户、组或 qtree 使用的磁盘空间和文件数量。

开始在 AWS C2S 环境中使用 Cloud Volumes ONTAP

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

C2S中支持的版本

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

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

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

C2S 中支持的功能

在 C2S 环境中， Cloud Manager 提供了以下功能：

- Cloud Volumes ONTAP
- 数据复制
- 审核时间表

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

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

限制

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

部署概述

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

1. 准备AWS环境

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

2. 安装Connector并设置Cloud Manager

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

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

3. 从Cloud Manager启动Cloud Volumes ONTAP

下面介绍了其中的每个步骤。

准备AWS环境

您的 AWS 环境必须满足一些要求。

设置网络

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

步骤

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

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

订阅 **Cloud Volumes ONTAP**

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

步骤

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

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

设置权限

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

您需要为以下每项设置一个 IAM 策略和 IAM 角色：

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

步骤

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

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
```

```
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
```

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

3. 为 Cloud Volumes ONTAP 创建策略。

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

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

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

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

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

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

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

设置 **AWS KMS**

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

步骤

1. 确保您的帐户或其他 AWS 帐户中存在有效的客户主密钥（ CMK ）。

   CMK 可以是 AWS 管理的 CMK 或客户管理的 CMK 。

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

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

3. 将Connector实例的IAM角色添加到CMK的关键用户列表中。

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

安装**Connector**并设置**Cloud Manager**

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

步骤

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

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

2. 启动 Connector 实例：

   a. 转到 Cloud Manager 的 AWS 智能社区市场页面。

   b. 在自定义启动选项卡上，选择用于从 EC2 控制台启动实例的选项。

   c. 按照提示配置实例。

      配置实例时，请注意以下事项：

      - 我们建议使用 T3.xlarge 。
      - 您必须选择在准备 AWS 环境时创建的 IAM 角色。

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

从Cloud Manager启动Cloud Volumes ONTAP

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

您需要的内容

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

步骤

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

    完成向导后，请注意以下事项：

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

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

    - 您必须选择在准备 AWS 环境时创建的 IAM 角色。

- 底层 AWS 磁盘类型适用于初始 Cloud Volumes ONTAP 卷。

  您可以为后续卷选择不同的磁盘类型。

- AWS 磁盘的性能取决于磁盘大小。

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

- 磁盘大小是系统上所有磁盘的默认大小。

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

- 存储效率功能可以提高存储利用率并减少所需的总存储量。

结果

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

安全组规则

Cloud Manager 创建的安全组包含 Cloud Manager 和 Cloud Volumes ONTAP 在云中成功运行所需的入站和出站规则。您可能需要参考端口进行测试，或者如果您希望使用自己的安全组。

Connector 的安全组

Connector 的安全组需要入站和出站规则。

入站规则

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

出站规则

Connector 的预定义安全组包括以下出站规则。

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

Cloud Volumes ONTAP 的安全组

Cloud Volumes ONTAP 节点的安全组需要入站和出站规则。

入站规则

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

- 仅选定**VPC**：入站流量的源是Cloud Volumes ONTAP 系统的VPC子网范围以及连接器所在VPC的子网范围。这是建议的选项。
- 所有vPC：入站流量的源IP范围为0.0.0.0/0。

协议	**Port**	目的
所有ICMP	全部	Ping 实例
HTTP	80	使用集群管理 LIF 的 IP 地址对系统管理器 Web 控制台进行 HTTP 访问
HTTPS	443.	使用集群管理 LIF 的 IP 地址对 System Manager Web 控制台进行 HTTPS 访问
SSH	22.	SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111.	远程过程调用 NFS
TCP	139.	用于 CIFS 的 NetBIOS 服务会话
TCP	161-162.	简单网络管理协议
TCP	445	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049.	NFS 服务器守护进程
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定守护进程
TCP	4046	NFS 的网络状态监视器
TCP	10000	使用 NDMP 备份
TCP	11104.	管理 SnapMirror 的集群间通信会话
TCP	11105.	使用集群间 LIF 进行 SnapMirror 数据传输
UDP	111.	远程过程调用 NFS
UDP	161-162.	简单网络管理协议
UDP	635	NFS 挂载
UDP	2049.	NFS 服务器守护进程
UDP	4045	NFS 锁定守护进程
UDP	4046	NFS 的网络状态监视器
UDP	4049.	NFS Rquotad 协议

出站规则

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

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

HA 调解器的外部安全组

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

入站规则

入站规则的源是来自连接器所在 VPC 的流量。

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

出站规则

HA 调解器的预定义安全组包括以下出站规则。

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

HA 调解器的内部安全组

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

入站规则

预定义的安全组包括以下入站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信

出站规则

预定义的安全组包括以下出站规则。

协议	Port	目的
所有流量	全部	HA 调解器和 HA 节点之间的通信