设置网络
Cloud Volumes ONTAP

NetApp
July 11, 2022

目录

设置网络

AWS 中的 Cloud Volumes ONTAP 的网络要求

Cloud Manager 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 节点需要出站 Internet 访问才能向 NetApp AutoSupport 发送消息、 NetApp AutoSupport 主动监控存储的运行状况。

路由和防火墙策略必须允许 AWS HTTP/HTTPS 流量传输到以下端点，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。

"了解如何配置 AutoSupport"。

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

Cloud Manager 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。

Cloud Manager 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

Cloud Manager 会将 6 个 IP 地址分配给一个节点系统：

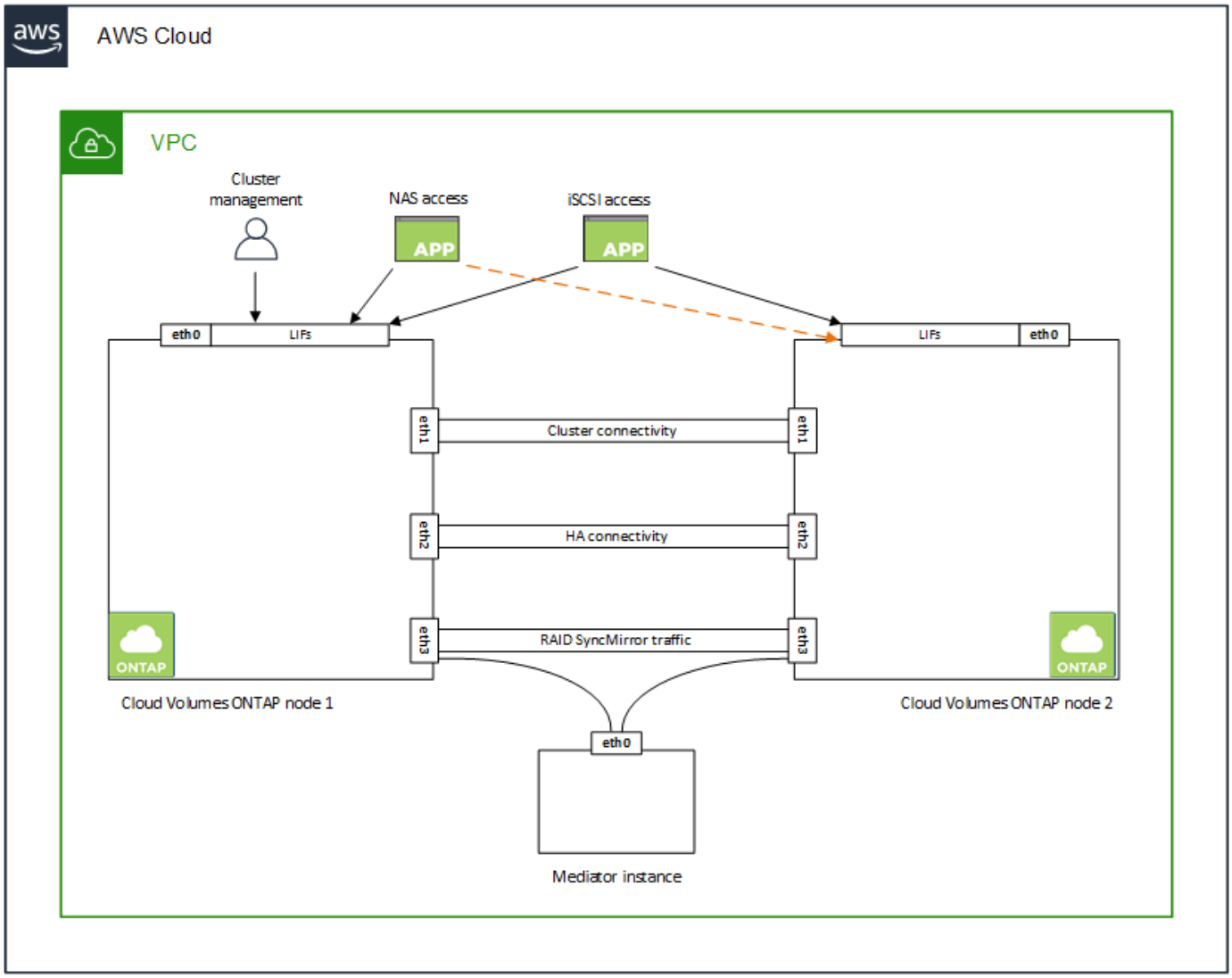
- 集群管理 LIF
- 节点管理 LIF

- 集群间 LIF
- NAS 数据 LIF
- iSCSI 数据 LIF
- Storage VM 管理 LIF

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

HA 对的 IP 地址

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



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

下表提供了有关与每个专用 IP 地址关联的 LIF 的详细信息。

一个 **AZ** 中的 **HA** 对的 **LIF**

LIF	接口	Node	目的
集群管理	eth0	节点 1	对整个集群（ HA 对）进行管理管理。
节点管理	eth0	节点 1 和节点 2	节点的管理管理。
集群间	eth0	节点 1 和节点 2	跨集群通信，备份和复制。
NAS 数据	eth0	节点 1	通过 NAS 协议进行客户端访问。
iSCSI 数据	eth0	节点 1 和节点 2	通过 iSCSI 协议进行客户端访问。
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。此 LIF 还可管理节点之间浮动 IP 地址的迁移。
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

您不需要创建安全组，因为 Cloud Manager 可以为您提供这些功能。如果您需要使用自己的，请参见 "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 Cloud Manager 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。

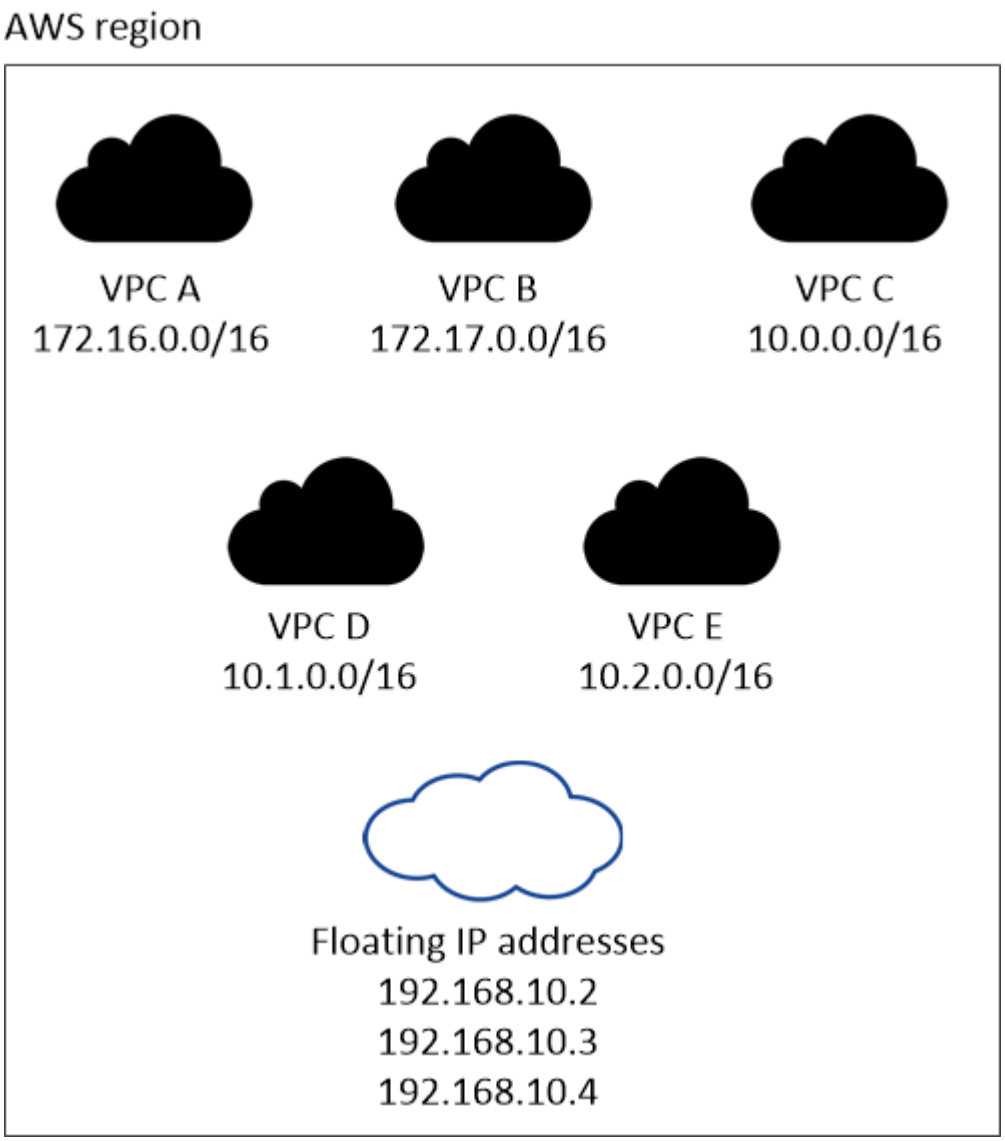
> ⓘ 如果将 SnapDrive for Windows 或 SnapCenter 与 HA 对结合使用，则 SVM 管理 LIF 需要浮动 IP 地址。

创建 Cloud Volumes ONTAP HA 工作环境时，您需要在 Cloud Manager 中输入浮动 IP 地址。在启动系统时

，Cloud Manager 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。



Cloud Manager 可自动创建用于 iSCSI 访问和从 VPC 外部的客户端进行 NAS 访问的静态 IP 地址。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 Cloud Manager 中指定浮动 IP 地址后，系统会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 Cloud Manager 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"。

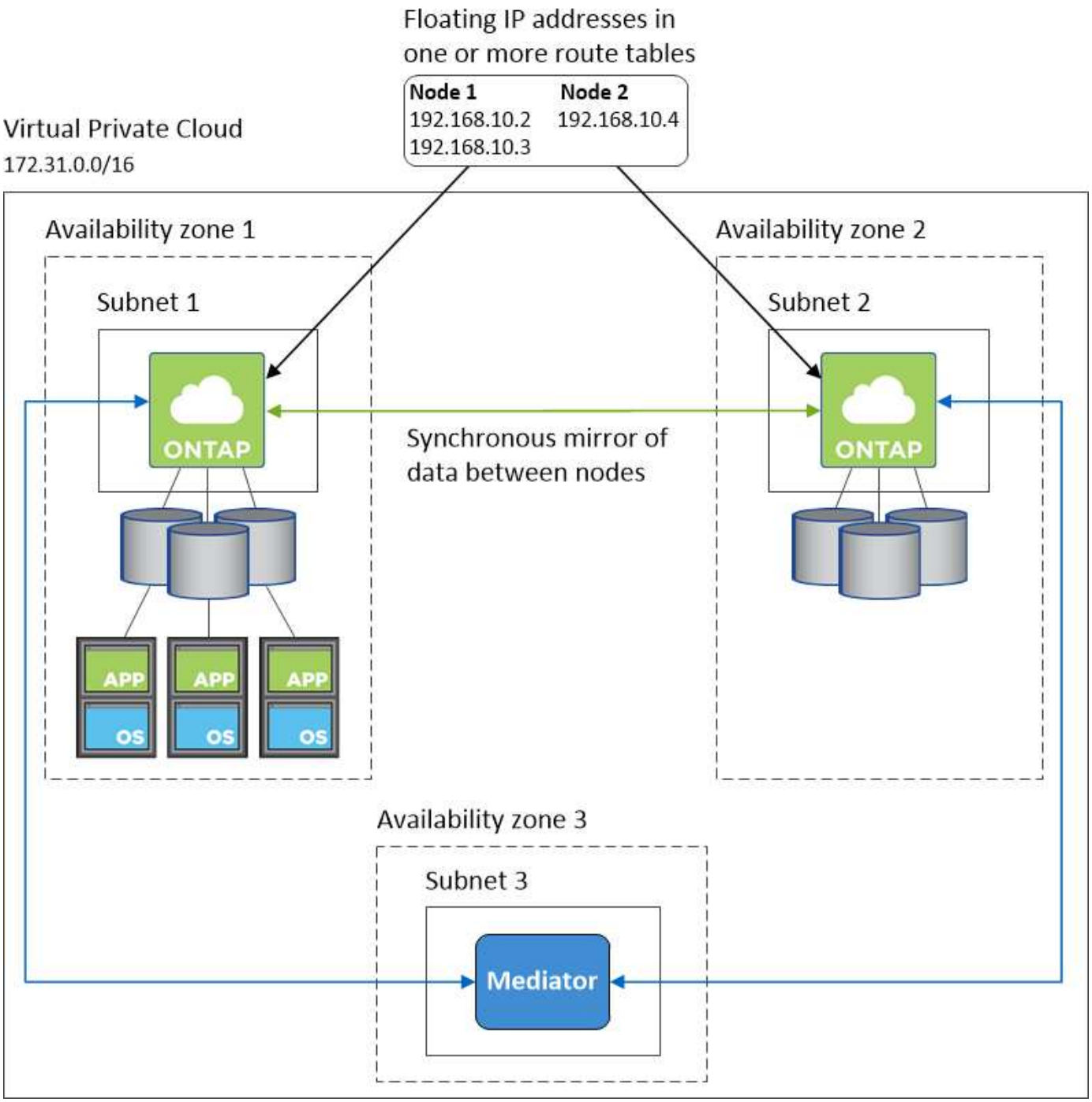
与 **NetApp** 管理工具的连接

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

设置您的网络，以便 Connector 能够管理公有云环境中的资源和流程。最重要的步骤是确保对各种端点的出站 Internet 访问。

如果您的网络使用代理服务器与 Internet 进行所有通信，则可以从设置页面指定代理服务器。请参见 "将 Connector 配置为使用代理服务器"。

连接到目标网络

连接器要求与要部署 Cloud Volumes ONTAP 的 VPC 和 VN 集建立网络连接。

例如，如果您在公司网络中安装了连接器，则必须设置与启动 Cloud Volumes ONTAP 的 VPC 或 vNet 的 VPN 连接。

出站 **Internet** 访问

连接器需要通过出站 Internet 访问来管理公有云环境中的资源和流程。

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

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

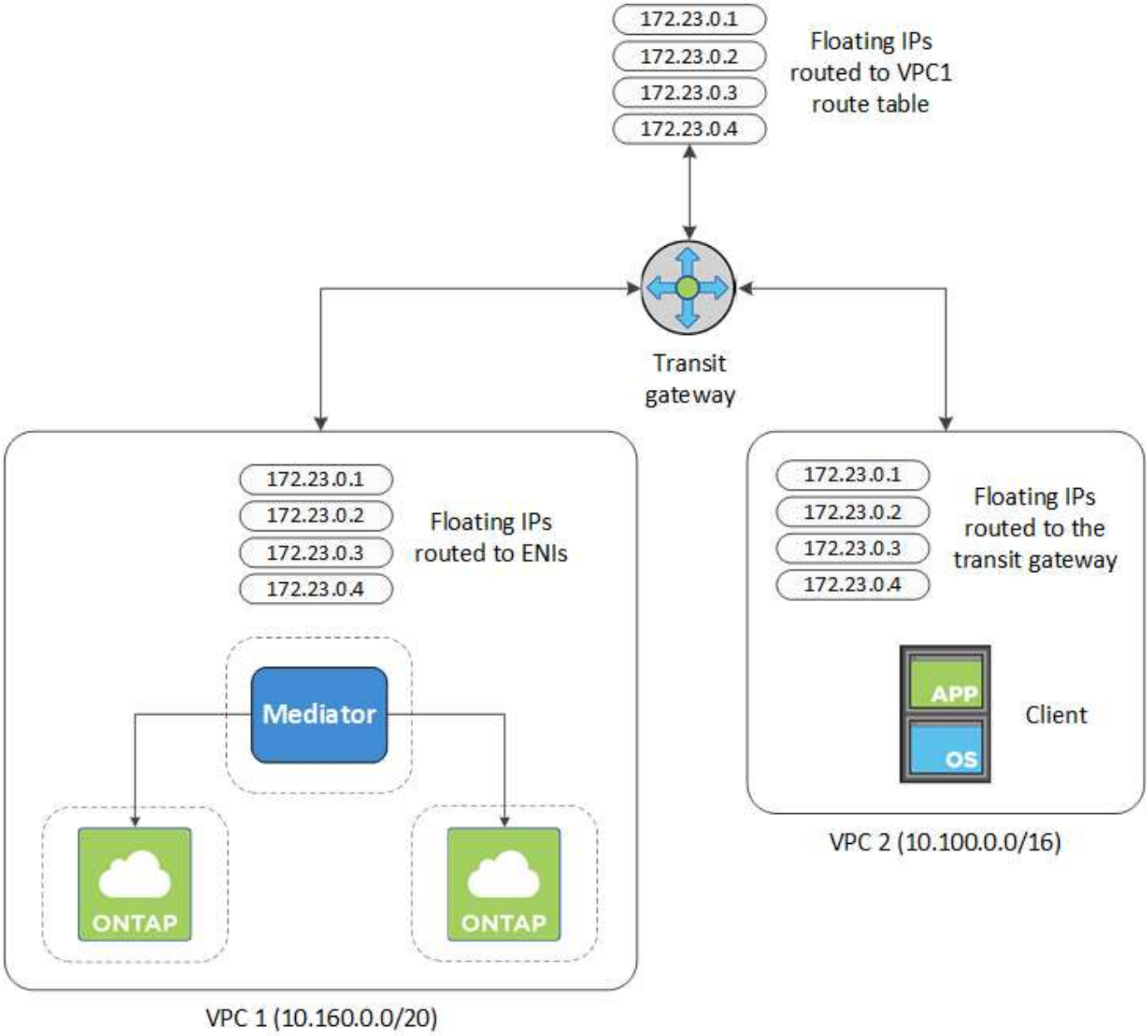
设置 AWS 传输网关以允许访问 HA 对 "浮动 IP 地址" 从 HA 对所在的 VPC 外部。

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。

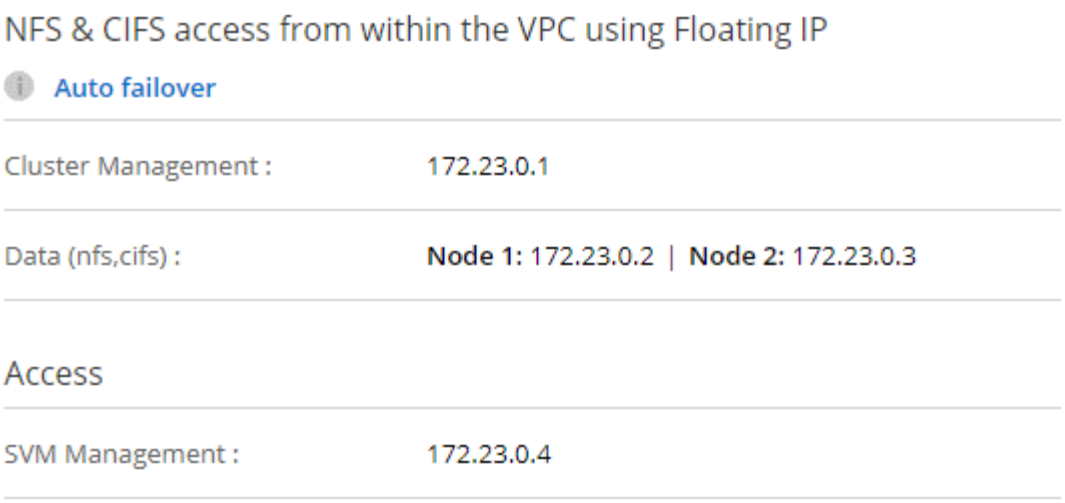


以下步骤说明了如何设置类似的配置。

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 Cloud Manager 的 " 工作环境信息 " 页面上找到浮动 IP 地址。以下是一个示例：



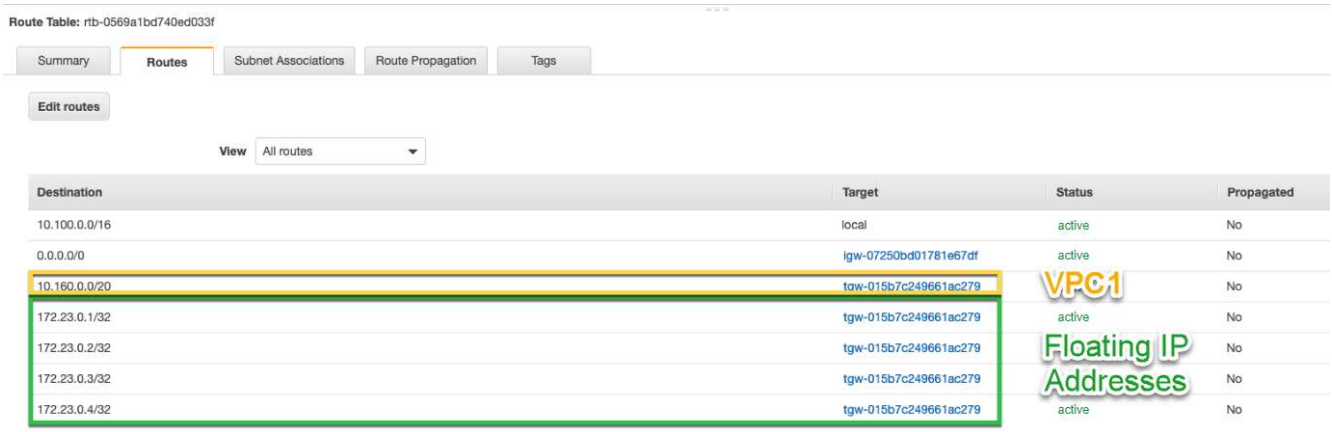
下图示例显示了传输网关的路由表。它包括到 Cloud Volumes ONTAP 所使用的两个 vPC 的 CIDR 块和四个浮动 IP 地址的路由。

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。

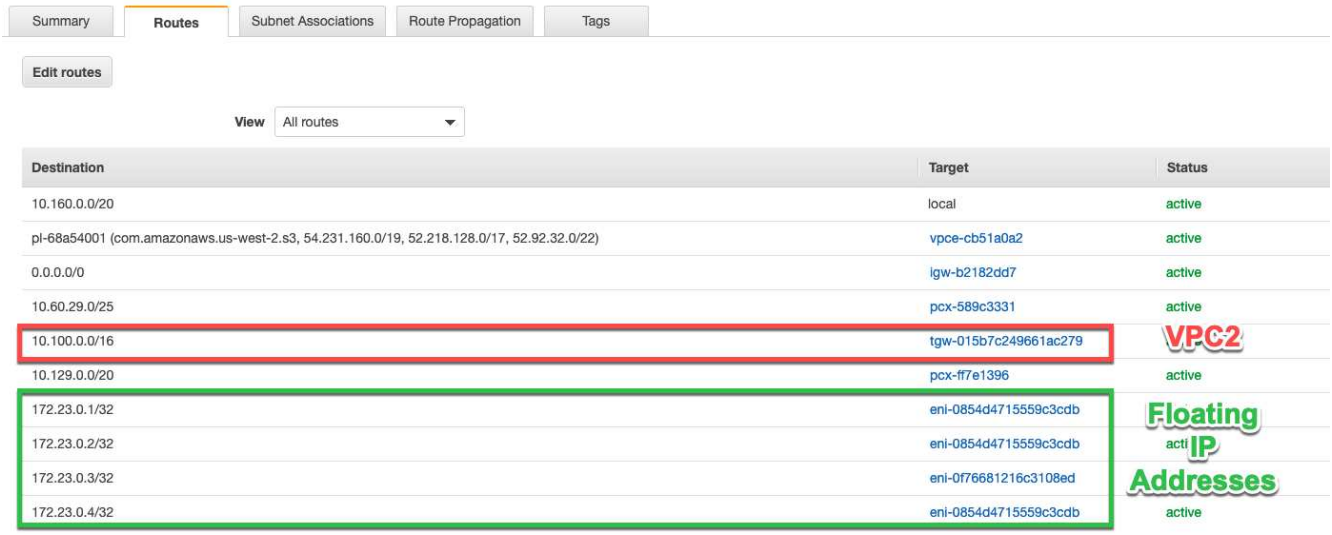
      下图示例显示了 VPC 2 的路由表，其中包括指向 VPC 1 的路由和浮动 IP 地址。



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。

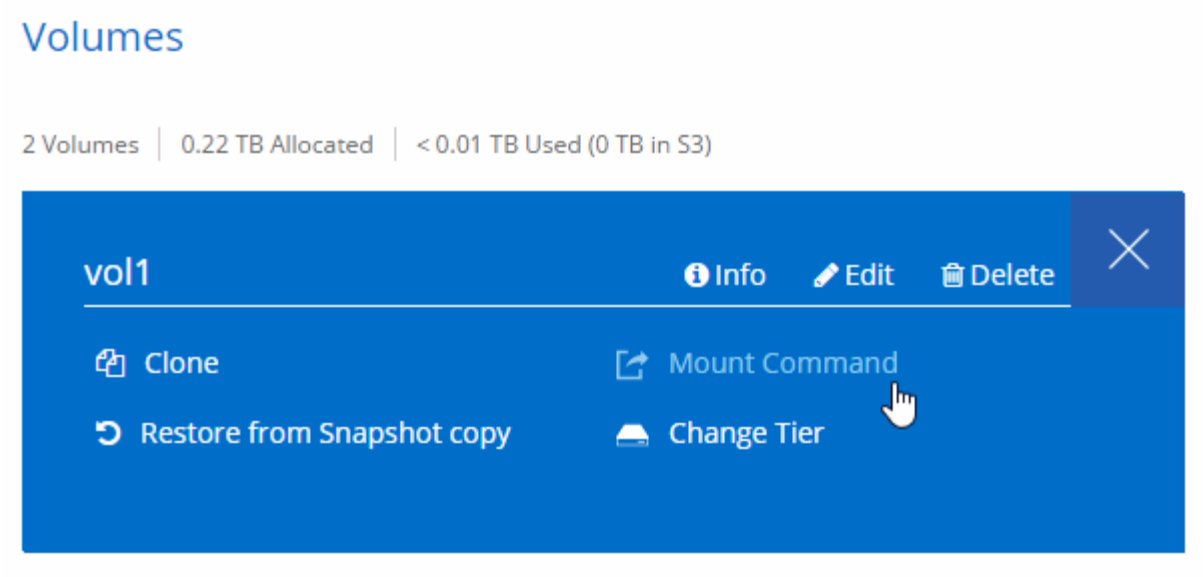
   此步骤非常重要，因为它会完成 VPC 之间的路由。

   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。Cloud Manager 在部署 HA 对时会自动将浮动 IP 添加到路由表中。



6. 使用浮动 IP 地址将卷挂载到客户端。

   通过选择卷并单击 * 挂载命令 * ，您可以在 Cloud Manager 中找到正确的 IP 地址。



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

"了解如何编辑卷"。

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

在共享子网中部署HA对

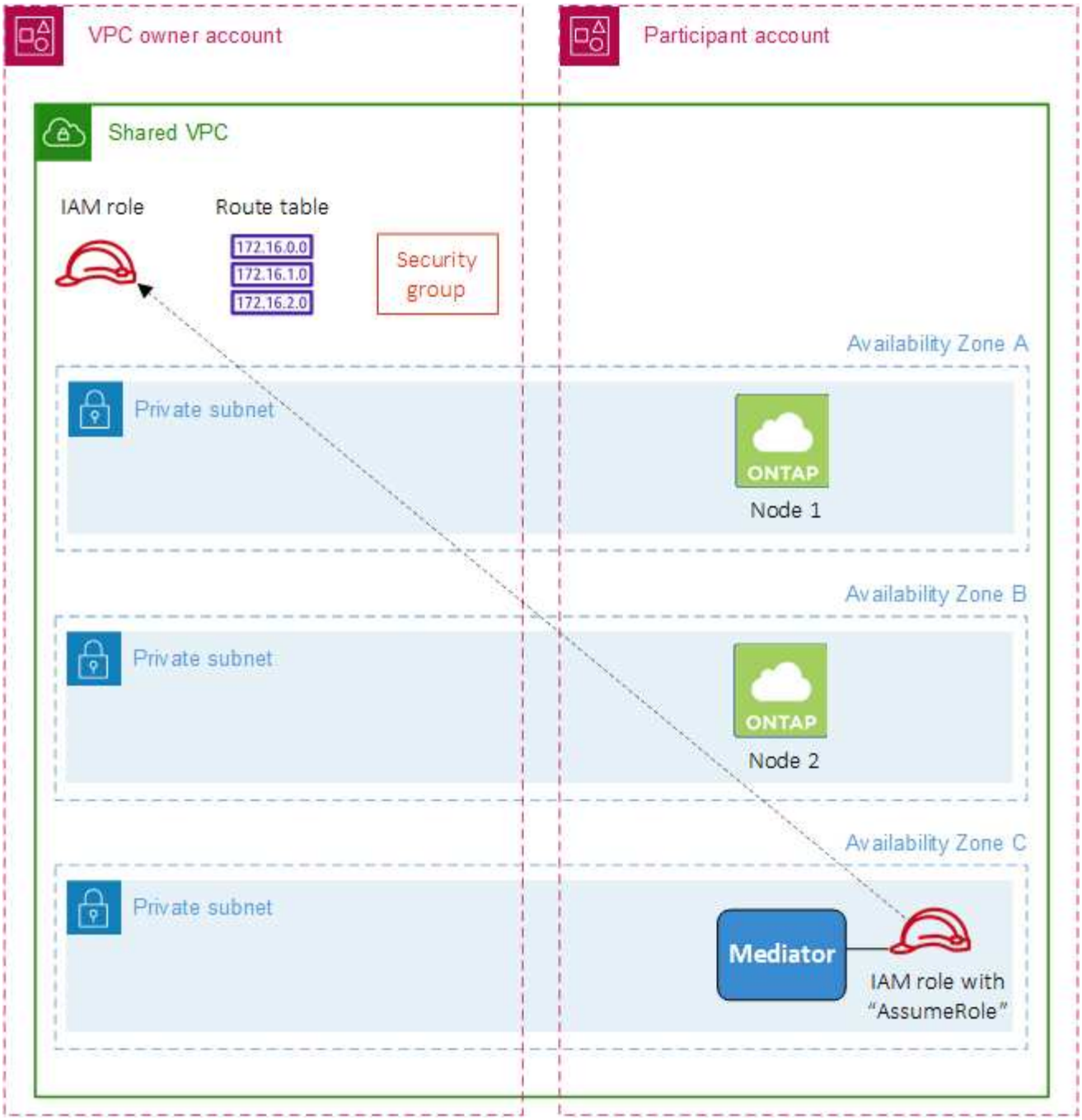
从9.11.1版开始、具有VPC共享的AWS支持Cloud Volumes ONTAP HA对。通过VPC共享、您的组织可以与其他AWS帐户共享子网。要使用此配置、您必须设置AWS环境、然后使用API部署HA对。

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

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

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

下图显示了此部署涉及的组件：



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

创建Cloud Volumes ONTAP 工作环境时、Cloud Manager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。云管理器可以为您提供这种功能。

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Cloud Manager 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

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

Cloud Volumes ONTAP 的规则

Cloud Volumes ONTAP 的安全组需要入站和出站规则。

入站规则

预定义安全组中入站规则的源代码为 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 预定义的安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

基本外向规则

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

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

高级出站规则

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

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

服务	协议	Port	源	目标	目的
Active Directory	TCP	88	节点管理 LIF	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	节点管理 LIF	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	节点管理 LIF	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	节点管理 LIF	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	节点管理 LIF	Active Directory 目录林	LDAP
	TCP	445	节点管理 LIF	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	UDP	464.	节点管理 LIF	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	节点管理 LIF	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）
	TCP	88	数据 LIF （ NFS ， CIFS ， iSCSI ）	Active Directory 目录林	Kerberos V 身份验证
	UDP	137.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 名称服务
	UDP	138.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 数据报服务
	TCP	139.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	NetBIOS 服务会话
	TCP 和 UDP	389.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	LDAP
	TCP	445	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
	TCP	464.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ set_change ）
	UDP	464.	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos 密钥管理
	TCP	749	数据 LIF （ NFS 、 CIFS ）	Active Directory 目录林	Kerberos V 更改和设置密码（ RPCSEC_GSS ）
AutoSupport	HTTPS	443.	节点管理 LIF	support.netapp.com	AutoSupport （默认设置为 HTTPS ）
	HTTP	80	节点管理 LIF	support.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）

服务	协议	Port	源	目标	目的
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 ）
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

入站规则的源代码为 0.0.0.0/0 。

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	连接器 IP 地址	下载调解器升级
HTTPS	443.	AWS API 服务	帮助进行存储故障转移
UDP	53.	AWS API 服务	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。

Cloud Manager 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

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 访问以及从 Cloud Data sense 建立的连接
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问
TCP	3128	如果您的 AWS 网络不使用 NAT 或代理，则可为云数据感知实例提供 Internet 访问

出站规则

连接器的预定义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

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

高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。

源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP ，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
API 调用	TCP	3000	ONTAP HA 调解器	与 ONTAP HA 调解器通信
	TCP	8088	备份到 S3	对备份到 S3 进行 API 调用
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

服务	协议	**Port**	目标	目的
云数据感知	HTTP	80	云数据感知实例	适用于 Cloud Volumes ONTAP 的云数据感知