设置网络

Cloud Volumes ONTAP

NetApp
February 13, 2026

目录

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。

端点	适用于	目的	部署模式	端点不可用时的影响
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。
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

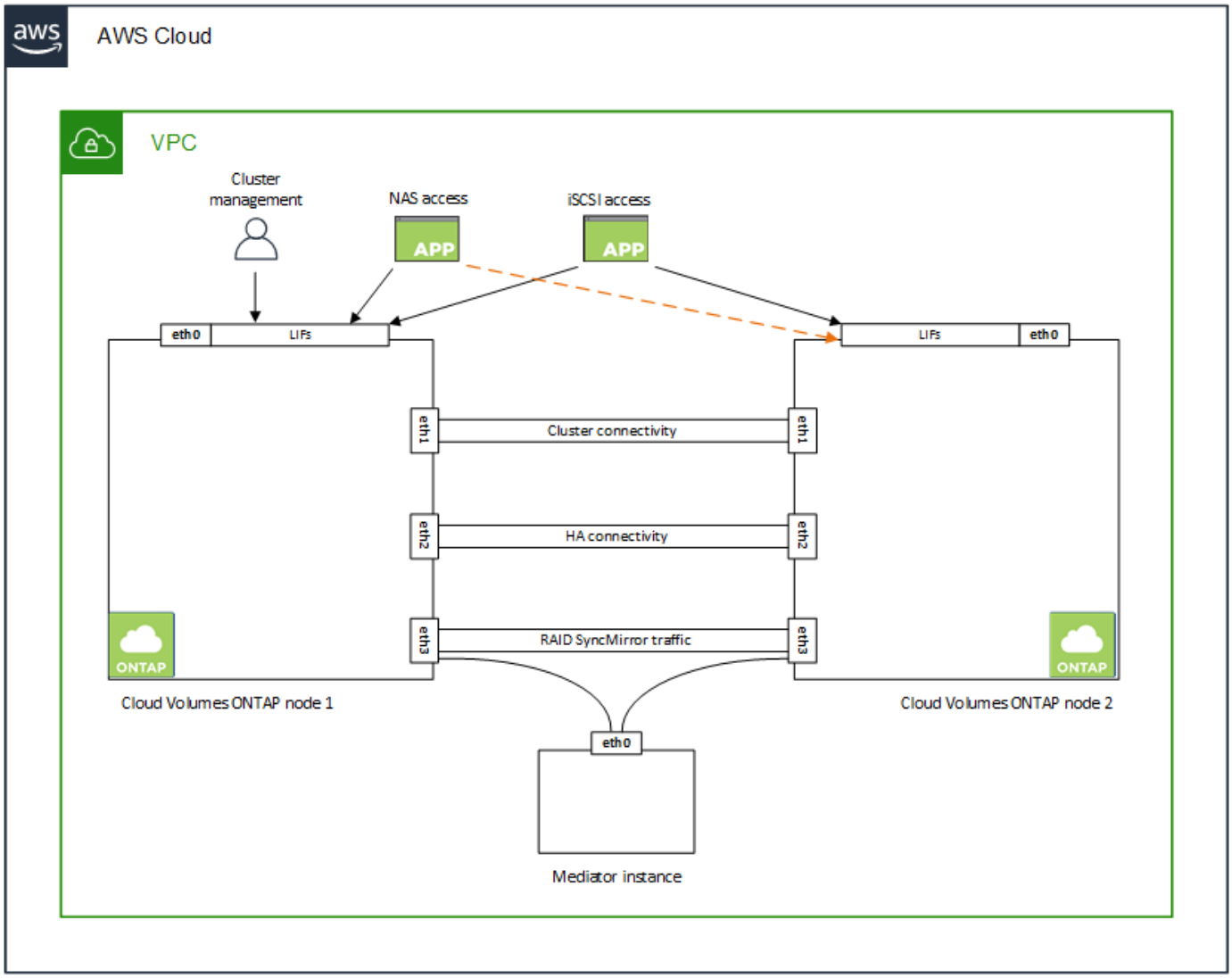
Console 为单节点系统分配 6 个 IP 地址。

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。

LIF	接口	节点	目的
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"。

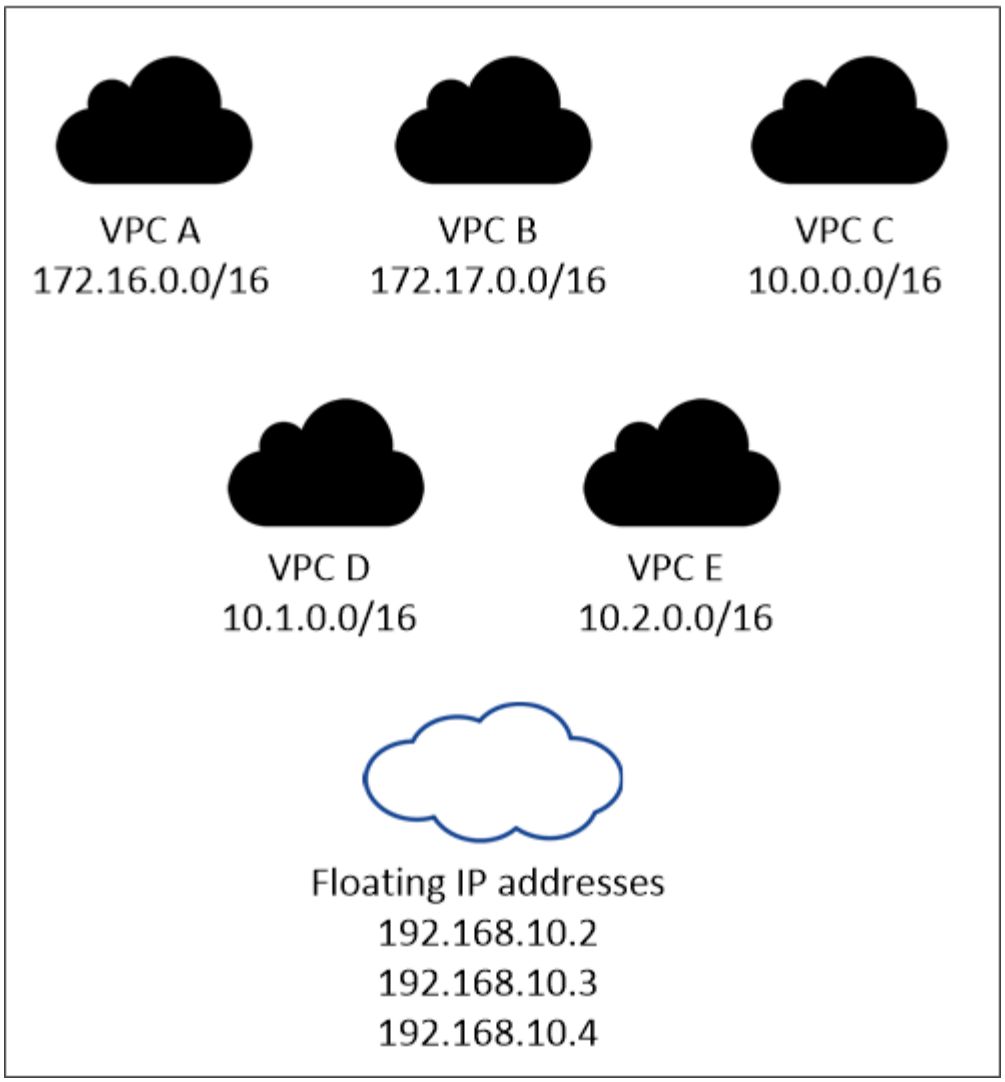
一个浮动 IP 地址用于集群管理，一个用于节点 1 上的 NFS/CIFS 数据，一个用于节点 2 上的 NFS/CIFS 数据。用于 SVM 管理的第四个浮动 IP 地址是可选的。

> ⓘ 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"。

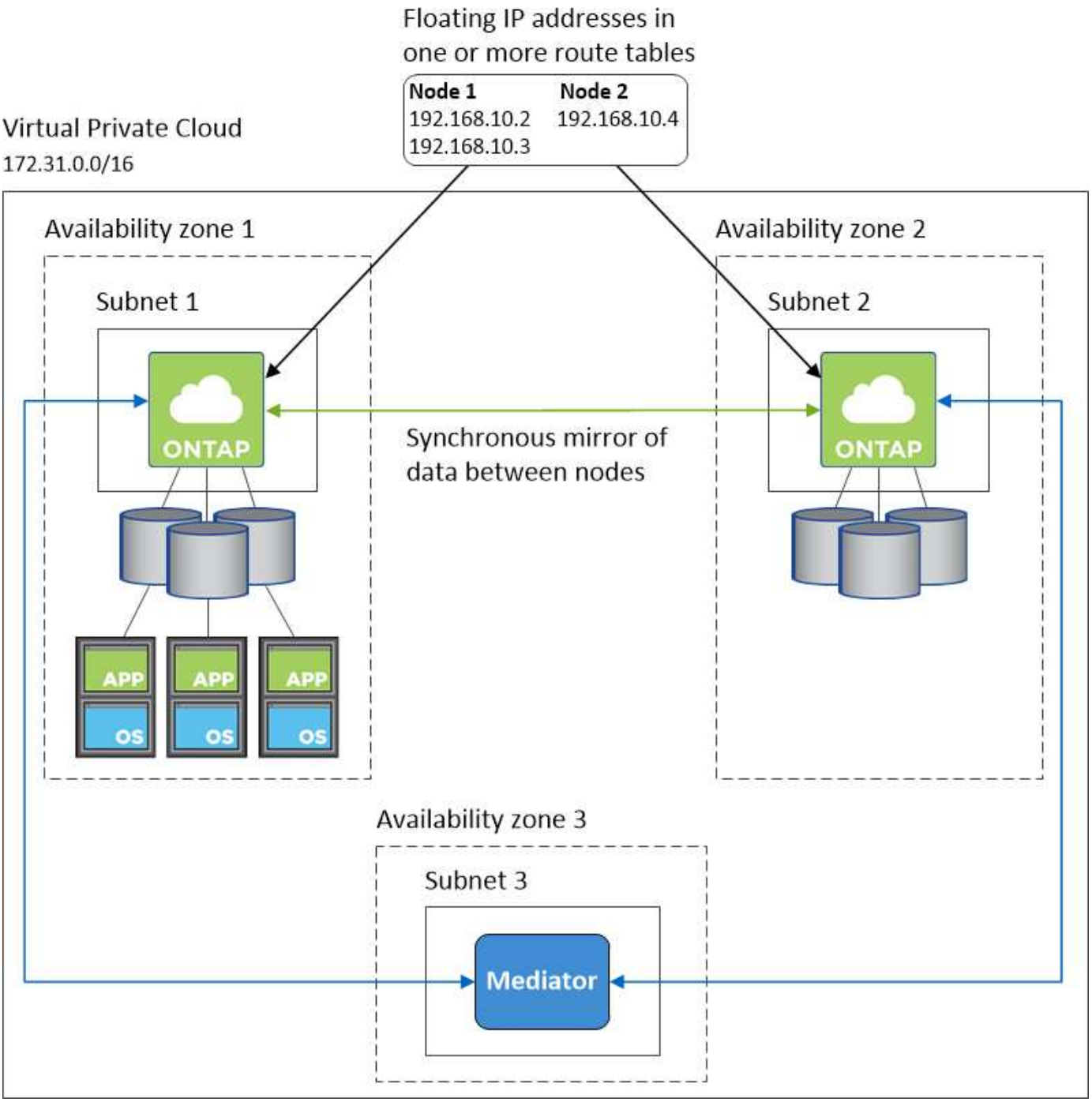
连接到NetApp管理工具

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

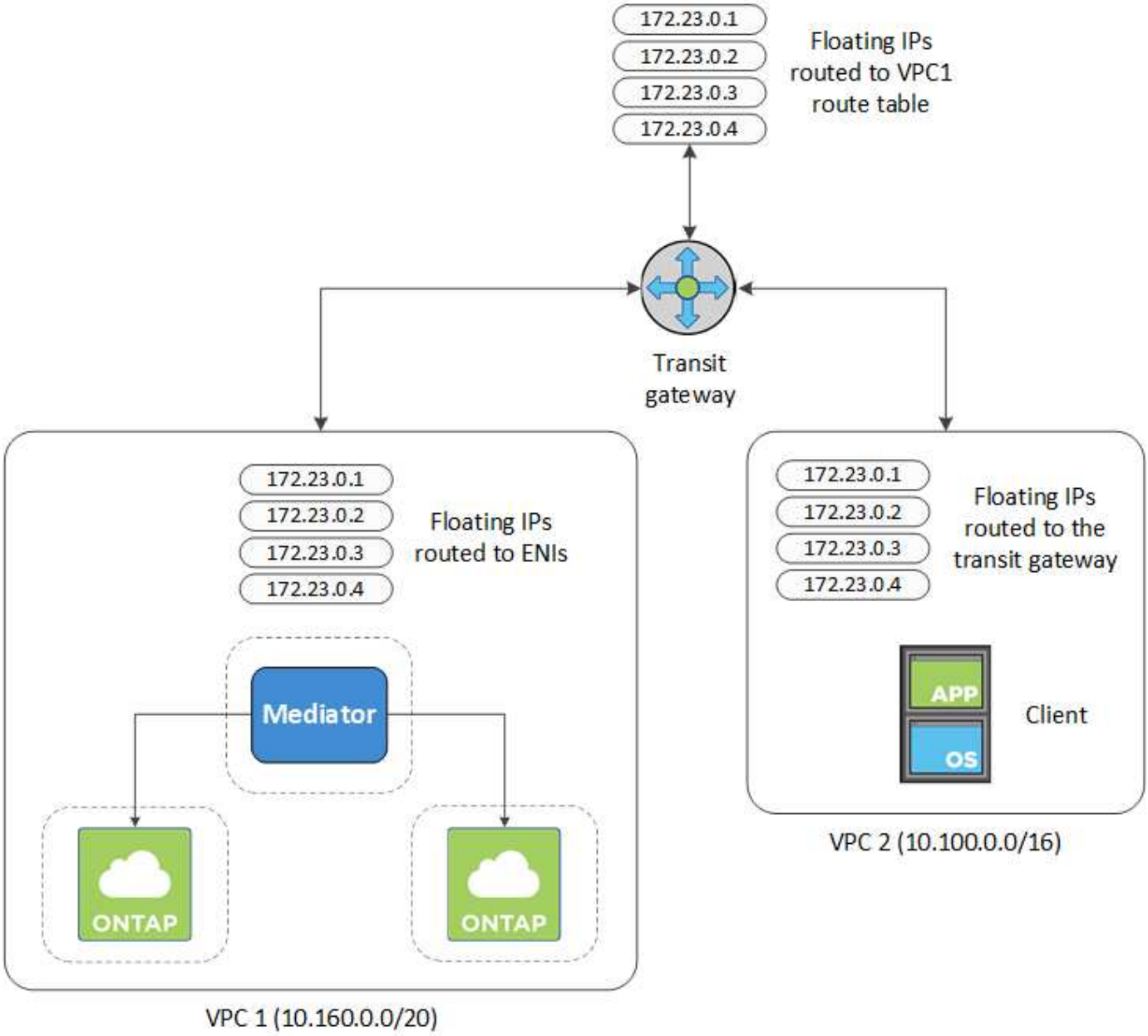
设置 AWS 中转网关以允许访问 HA 对的"浮动IP地址"来自 HA 对所在的 VPC 外部。

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。

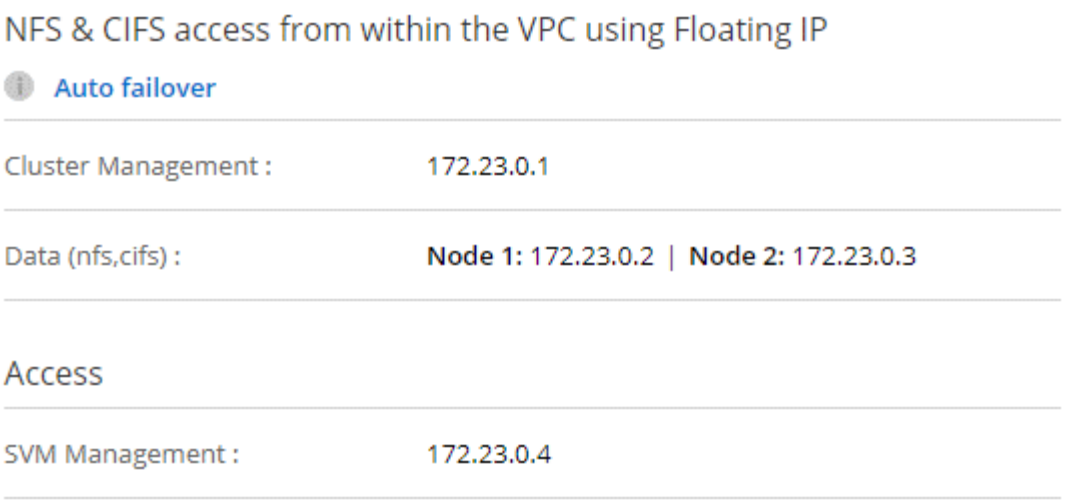


以下步骤说明如何设置类似的配置。

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：



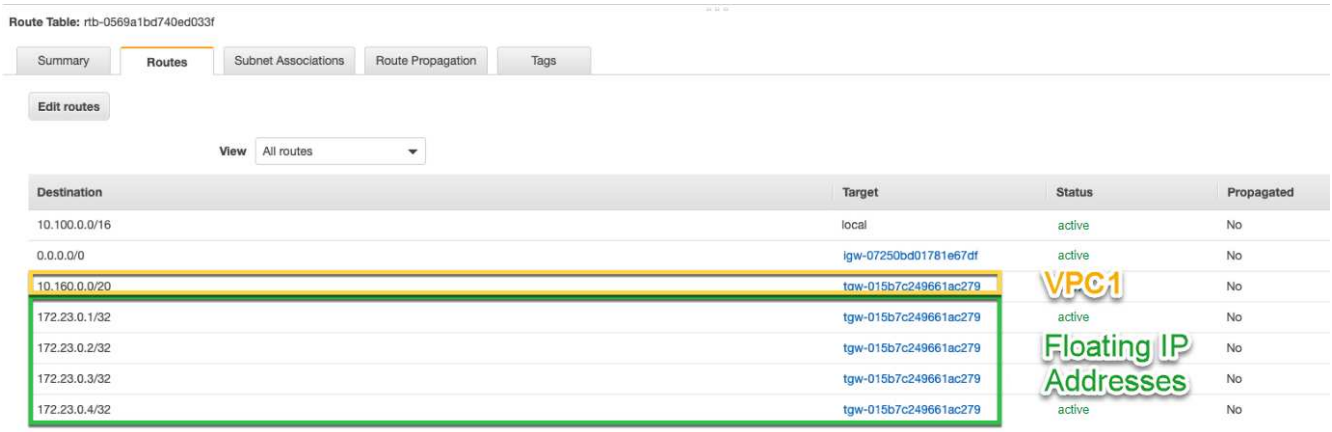
以下示例图显示了中转网关的路由表。它包括到两个 VPC 的 CIDR 块的路由和Cloud Volumes ONTAP使用的四个浮动 IP 地址。

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。

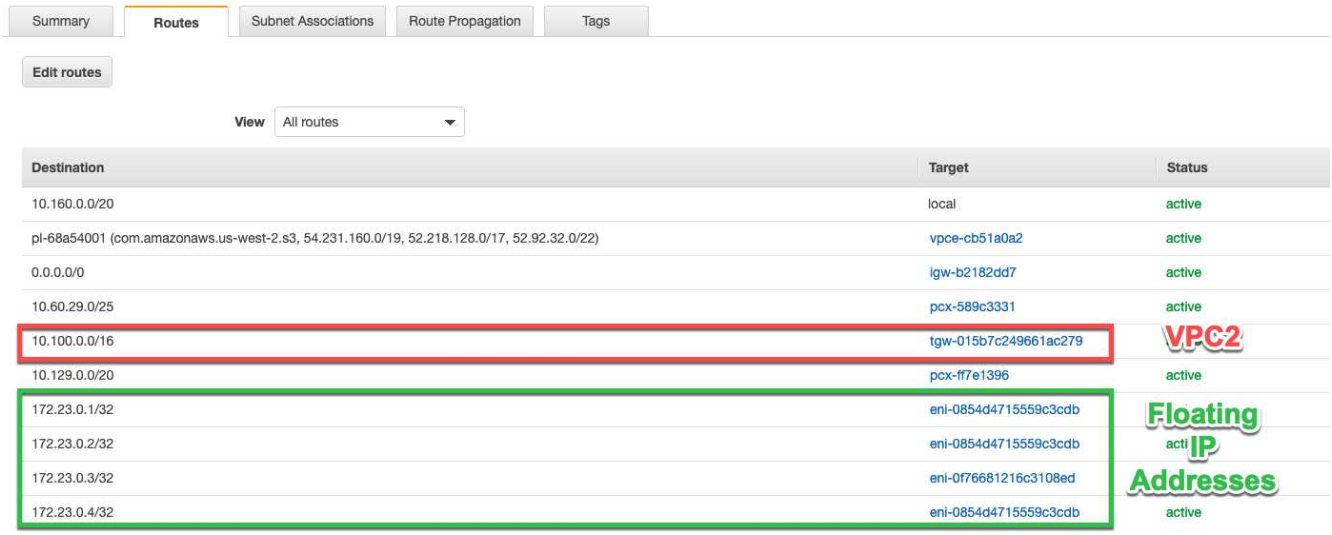
      下面的示例图显示了 VPC 2 的路由表，其中包括到 VPC 1 的路由和浮动 IP 地址。



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。

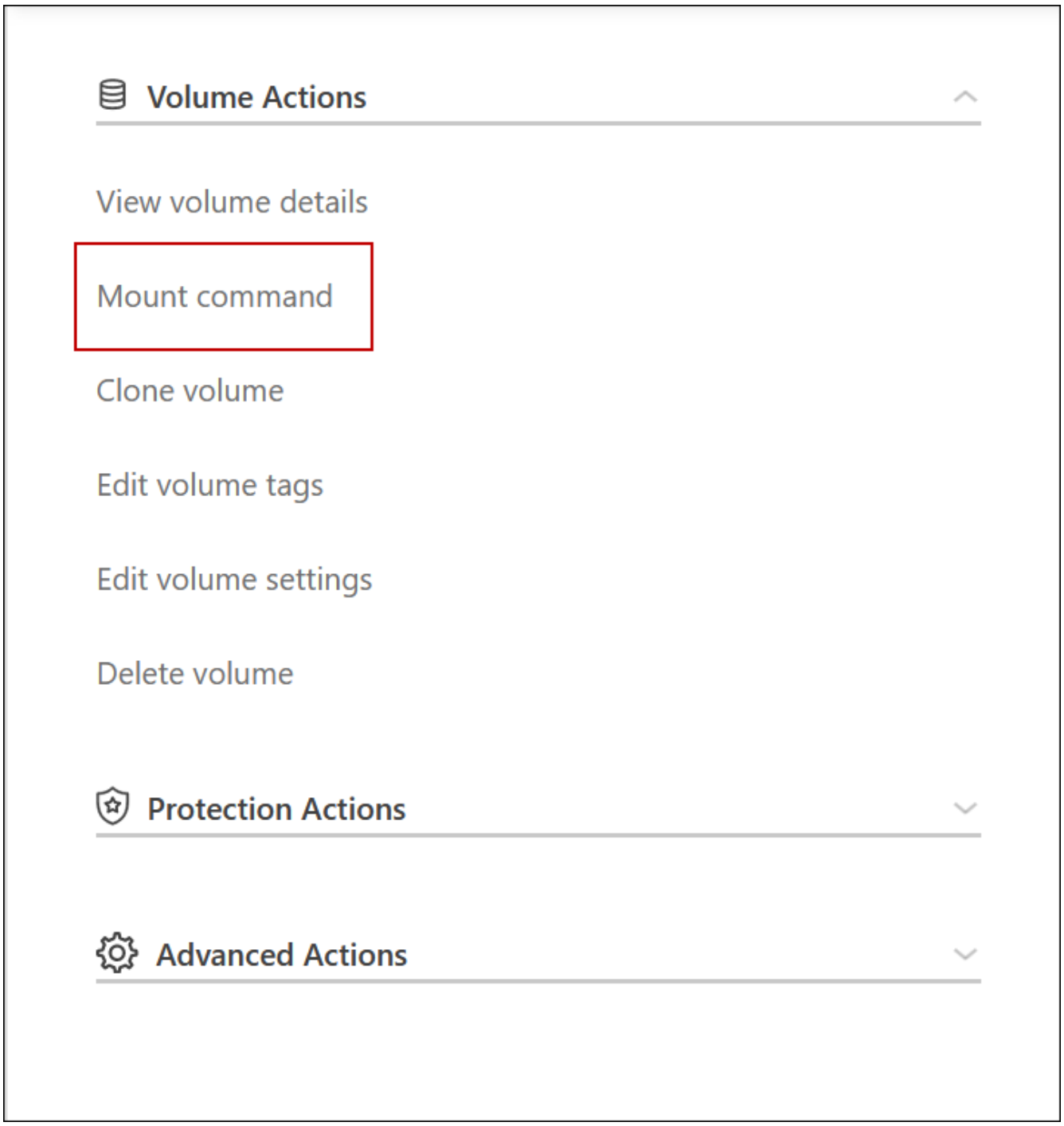
   这一步很重要，因为它完成了 VPC 之间的路由。

   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

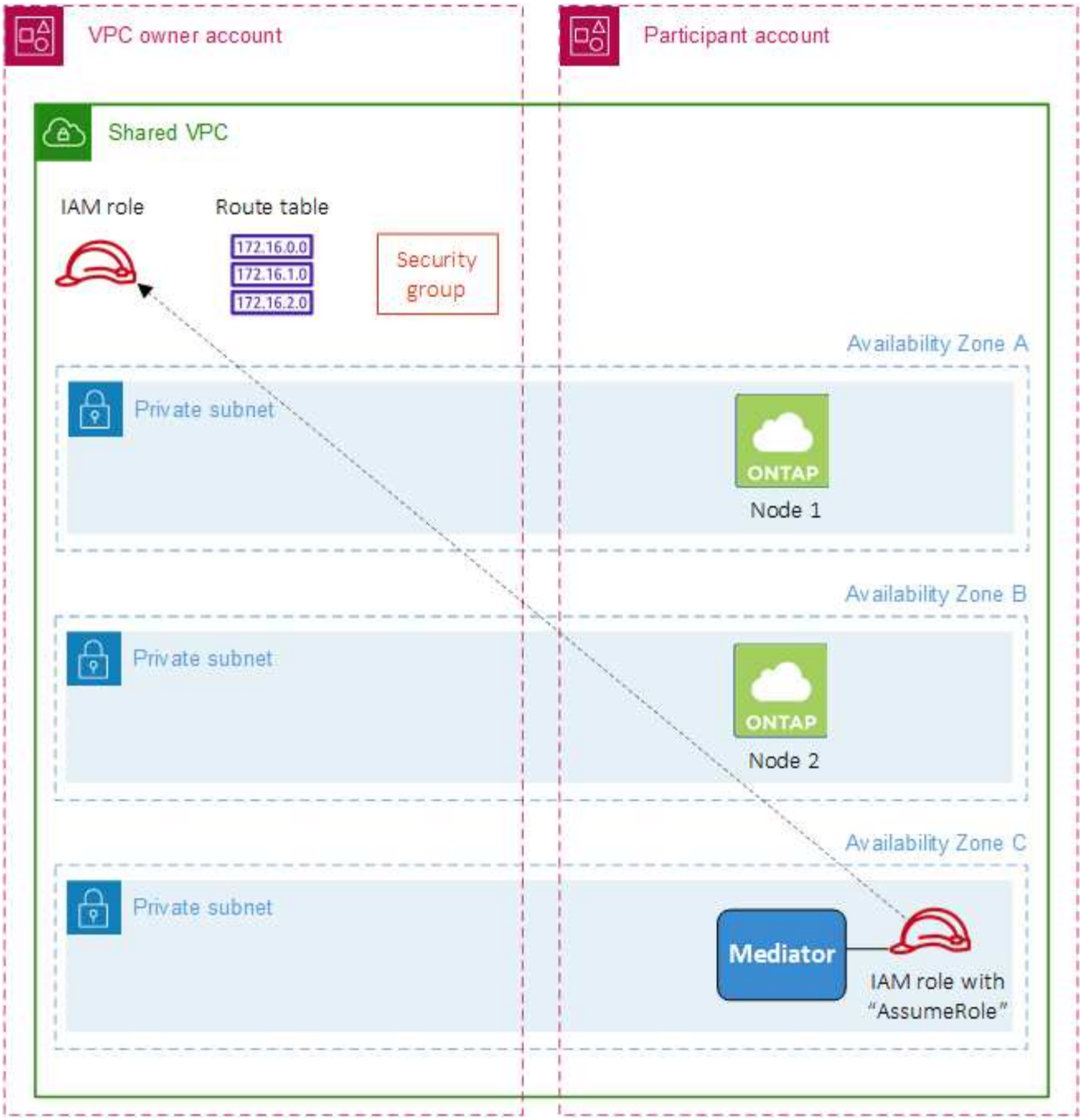
从 9.11.1 版本开始，AWS 通过 VPC 共享支持Cloud Volumes ONTAP HA 对。 VPC 共享使您的组织能够与其他 AWS 账户共享子网。要使用此配置，您必须设置您的 AWS 环境，然后使用 API 部署 HA 对。

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

协议	端口	目的
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
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）

服务	协议	端口	源	目标	目的
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
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"