虚拟私有云

用户指南

文档版本 01

发布日期 2025-01-24

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 通过 IAM 授予使用 VPC 的权限

1.1 创建用户并授权使用 VPC

如果您需要对您所拥有的VPC进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用VPC资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将VPC资源委托给更专业、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用VPC服务的其他功能。

本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

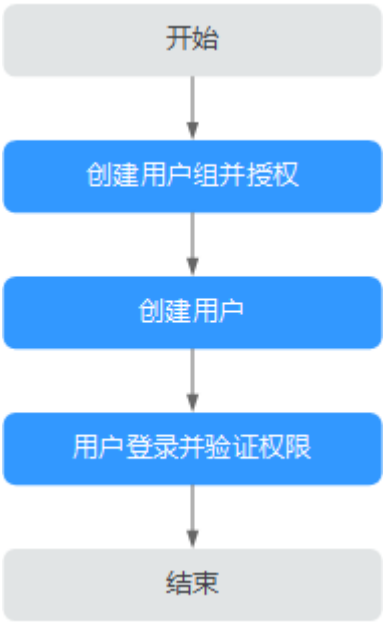
前提条件

给用户组授权之前，请您了解用户组可以添加的VPC系统权限，并结合实际需求进行选择，VPC支持的系统权限，请参见：**权限管理**。

若您需要对除VPC之外的其他服务授权，IAM支持服务的所有策略请参见**权限策略**。

示例流程

图 1-1 给用户授权 VPC 权限流程



1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予VPC只读权限“VPCReadOnlyAccess”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。

3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   - 在“服务列表”中选择虚拟私有云，进入VPC主界面，单击右上角“创建虚拟私有云”，如果无法创建虚拟私有云（假设当前权限仅包含VPCReadOnlyAccess），表示“VPCReadOnlyAccess”已生效。
   - 在“服务列表”中选择除虚拟私有云外（假设当前策略仅包含ECS Viewer）的任一服务，若提示权限不足，表示“VPCReadOnlyAccess”已生效。

1.2 VPC 自定义策略

如果系统预置的VPC权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参见**策略及授权项说明**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的VPC自定义策略样例。

VPC 自定义策略样例

- 示例1：授权用户创建和查看VPC

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "
                vpc:vpcs:create
                vpc:vpcs:list
             "
         ]
      }
   ]
}
```

- 示例2：拒绝用户删除VPC

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Alow和Deny，则遵循Deny优先。

  如果您给用户授予VPC FullAccess的系统策略，但不希望用户拥有VPC FullAccess中定义的删除VPC权限，您可以创建一条拒绝删除VPC的自定义策略，然后同时将VPC FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以对VPC执行除了删除外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
       "Effect": "Deny",
            "Action": [
                "vpc:vpcs:delete"
            ]
        }
    ]
}
```

- 示例3：多个授权项策略

  一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。多个授权语句策略描述如下:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "vpc:vpcs:create",
            "vpc:vpcs:update"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:servers:delete"
         ],
         "Effect": "Allow"
      }
   ]
}
```

- 示例4：授权用户查看关联资源

  查看资源A关联了哪些其他资源，不仅需要授权资源A的查询策略，还需要授权其他资源的查询策略。以查看安全组关联实例举例，安全组可以关联的实例类型包

括服务器、扩展网卡、辅助弹性网卡等。查看安全组关联实例列表的授权语句策略描述如下：

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
                "vpc:ports:get",
                "vpc:securityGroups:get",
                "vpc:subNetworkInterfaces:list"
            "
         ]
      }
   ]
}
```

2 虚拟私有云和子网

2.1 虚拟私有云和子网规划建议

当您需要使用虚拟私有云VPC和子网搭建您的云上网络时，请您参考以下规划建议，并结合实际业务情况，规划您的VPC和子网数量、VPC和子网IP网段。同时，如果需要连通不同VPC网络，或者连通VPC和云下数据中心网络时，需要额外注意通信的网段之间不能冲突。合理规划VPC和子网，可以避免网段临时扩容或者IP网段冲突可能导致的问题。详细规划建议，请您参见以下内容：

- **如何规划VPC的数量?**
- **如何规划子网的数量?**
- **如何规划VPC和子网的IP网段?**
- **如何规划路由表的数量?**
- **当VPC与其他VPC通信或者VPC与云下数据中心通信时如何规划网络?**

如何规划 VPC 的数量?

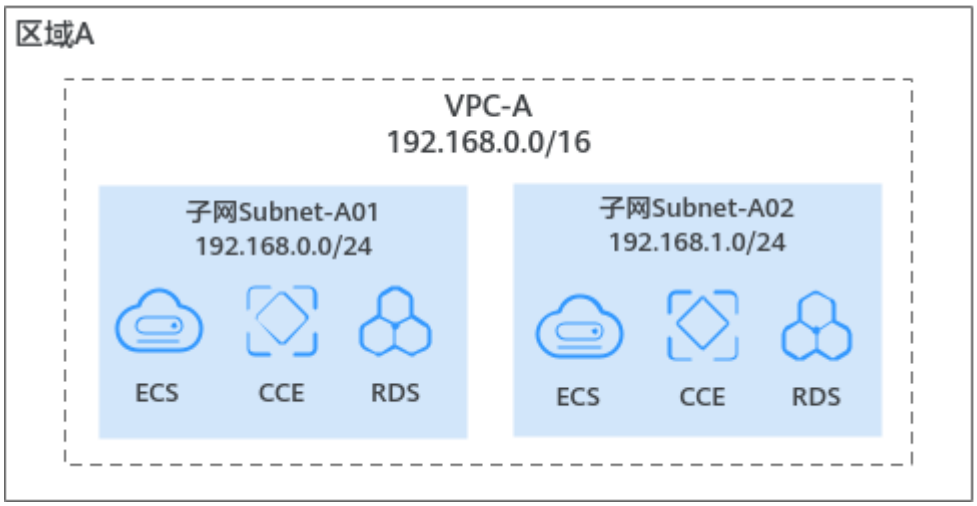
VPC具有区域属性，VPC内的云资源（比如ECS、CCE、RDS等）必须和VPC位于同一个区域内。默认情况下，不同VPC之间网络隔离，同一个VPC内的不同子网之间网络互通。

规划一个 VPC

如果您的业务部署在一个区域，并且业务量不大，不同业务之间不需要网络隔离，那么推荐您规划一个VPC。

您可以在一个VPC中创建多个子网和路由表。子网可以将VPC网段划分成若干段，不同子网承载不同的业务。同时，您还可以将不同子网关联至不同的路由表，灵活控制子网的网络流量。如**图2-1**所示，在区域A内，业务部署在VPC-A内的不同子网。

图 2-1 规划 1 个 VPC



规划多个 VPC

当您的业务有以下任意一个需求时，则一个VPC无法满足业务要求，推荐您规划多个VPC。

- **业务需要部署在多个区域**

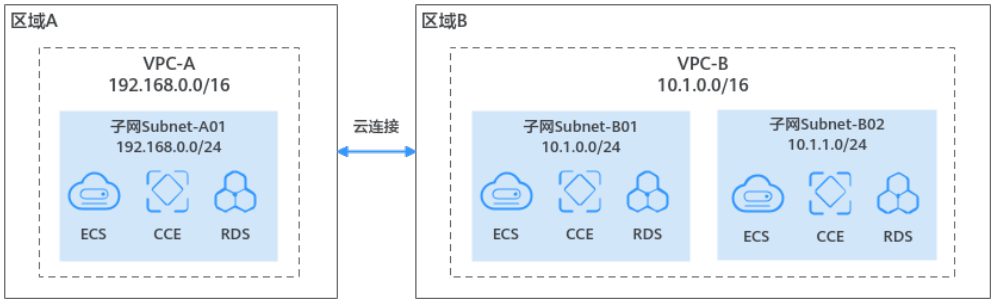
  VPC是区域级别的服务，一个VPC无法实现跨区域部署业务。如果您的业务同时部署在多个区域，则在每个区域下，至少需要规划一个VPC。

  不同VPC之间网络隔离，您可以搭配网络连通服务连通不同VPC的网络。

  - 连通相同区域内的不同VPC：您可以使用**对等连接**或者**企业路由器**来实现。
  - 连通不同区域内的VPC：您可以使用**云连接**来实现。

  如图2-2所示，一部分业务部署在区域A内的VPC-A中，一部分业务部署在区域B内的VPC-B中，通过云连接连通VPC-A和VPC-B的网络。

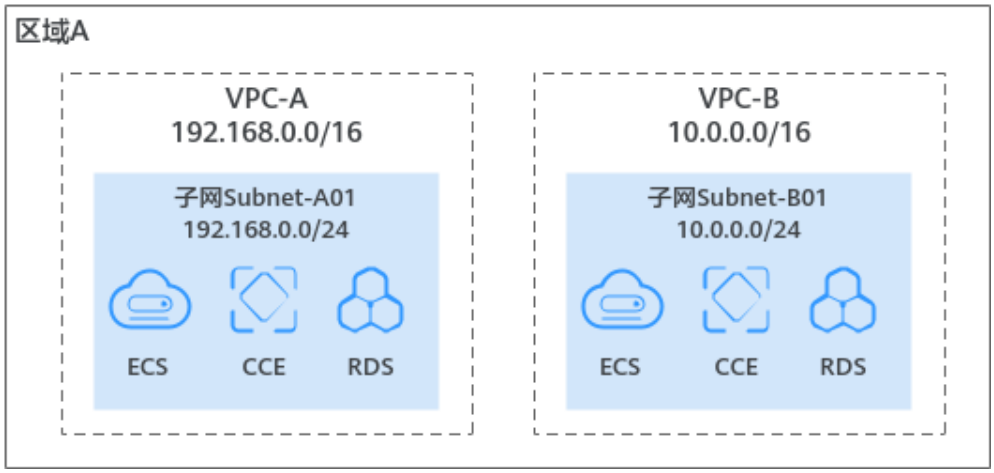
  图 2-2 规划多个 VPC（业务需要部署在多个区域）

- **业务部署在一个区域且网络隔离**

  如果您的业务部署在一个区域，并且不同业务之间网络隔离，则您需要在同一个区域下规划多个VPC，由于不同VPC之间网络隔离，则每个业务独立部署在一个VPC上即可满足要求。如图2-3所示，在区域A内，一部分业务部署在VPC-A中，一部分业务部署在VPC-B中，两个VPC之间网络隔离。

图 2-3 规划多个 VPC（业务部署在一个区域且网络隔离）



说明

一个用户在单个区域可创建的虚拟私有云数量默认为5个，如果您需要提升配额，请参见**申请扩大配额**。

如何规划子网的数量?

子网是VPC内的IP地址集，可以将VPC的网段分成若干块，子网划分可以帮助您合理规划IP地址资源。VPC中的所有云资源都必须部署在子网内。

通常情况下，部署在同一个VPC内的业务，您可以根据业务模块来划分子网，比如在VPC-A内，子网A01用于Web层，子网A02用于管理层，子网A03用于数据层。根据业务划分子网模块，有利于结合网络ACL进行网络防护。

关于子网和云资源可用区的选择，您还需要了解以下原则：

- 默认情况下，同一个VPC中，不同子网内的所有实例网络互通。同一个VPC内的子网可以位于不同可用区，不影响通信。比如VPC-A内有子网A01（可用区A）和子网A02（可用区B），子网A01和子网A02的网络默认互通。
- 同时，使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。假如可用区3发生故障，此时可用区1的云服务器可以继续使用可用区3的子网，不会影响云服务器上部署的业务。

说明

一个用户在单个区域可创建的子网数量默认为100个，如果您需要提升配额，请参见**申请扩大配额**。

如何规划 VPC 和子网的 IP 网段?

VPC和子网创建完成后，则无法修改网段。因此创建VPC和子网之前，请您务必结合业务规模和通信需求，合理规划VPC和子网网段，以便于业务的平滑扩展和运维。

说明

私有网络支持IPv4和IPv6网段地址。您可以自定义IPv4网段，不支持自定义IPv6网段，系统自动为每个子网分配一个掩码为64位的IPv6网段，比如2407:c080:802:1b32::/64。

规划 VPC 网段

创建VPC的时候，您需要为VPC指定IPv4网段。VPC网段的选择需要考虑以下原则：

- IP地址数量：要为业务预留足够的IP地址，防止业务扩展给网络带来冲击。
- IP地址网段：当您要创建多个VPC，并且VPC与其他VPC、或者VPC与云下数据中心需要通信时，要避免网络两端的网段冲突，否则无法正常通信。

创建VPC时，您配置的IPv4网段是VPC的主网段。当VPC创建完成后，主网段不支持修改，若主网段不够分配，您可以**为VPC添加IPv4扩展网段**。

在创建VPC的时候，建议您使用**RFC 1918**中指定的私有IPv4地址范围，作为VPC的网段，具体如**表2-1**所示。

表 2-1 VPC 网段（RFC 1918）

VPC网段	IP地址范围	掩码范围	VPC网段示例
10.0.0.0/8-24	10.0.0.0~10.255.255.255	8~24	10.0.0.0/8
172.16.0.0/12-24	172.16.0.0~172.31.255.255	12~24	172.30.0.0/16
192.168.0.0/16-24	192.168.0.0~192.168.255.255	16~24	192.168.0.0/24

除了上述地址，您还可以使用任何可公共路由的IPv4地址（非RFC 1918指定的私有IPv4地址范围），但是必须排除**表2-2**中的系统预留地址和公网保留地址：

表 2-2 系统预留地址和公网保留地址

系统预留地址	公网保留地址
• 100.64.0.0/10 • 214.0.0.0/7 • 198.18.0.0/15 • 169.254.0.0/16	• 0.0.0.0/8 • 127.0.0.0/8 • 240.0.0.0/4 • 255.255.255.255/32

规划子网网段

- 子网掩码规划：子网的网段必须在VPC网段范围内，同一个VPC内的子网网段不可重复。子网网段的掩码长度范围是：所在VPC掩码~29，比如VPC网段为10.0.0.0/16，VPC的掩码为16，则子网的掩码可在16~29范围内选择。

  比如VPC-A的网段为10.0.0.0/16，则您可以规划子网A01的网段为10.0.0.0/24，子网A02的网段为10.0.1.0/24，子网A03的网段为10.0.2.0/24。
- 子网内可用IP数量：子网创建成功后，不支持修改网段，请您结合业务所需的IP地址数量，提前合理规划好子网网段。
  - 子网网段不能太小，需要确保子网内可用IP地址数量可以满足业务需求。子网网段中第一个地址和后三个地址为系统预留地址，不能供实际业务使用，

比如子网（10.0.0.0/24）中，10.0.0.1为网关地址、10.0.0.253为系统接口、10.0.0.254为DHCP使用、10.0.0.255为广播地址。

- 子网网段也不能太大，以免后续扩展新的业务时，VPC内可用网段不够再创建新的子网。

- 子网网段避免冲突：如果子网所在的VPC与其他VPC、或者VPC与云下数据中心需要通信时，则VPC子网网段和网络对端网段不能相同，否则无法正常通信。

  如果网络两端的子网网段已经相同，您可以创建新的子网，请参见**为虚拟私有云创建新的子网**。

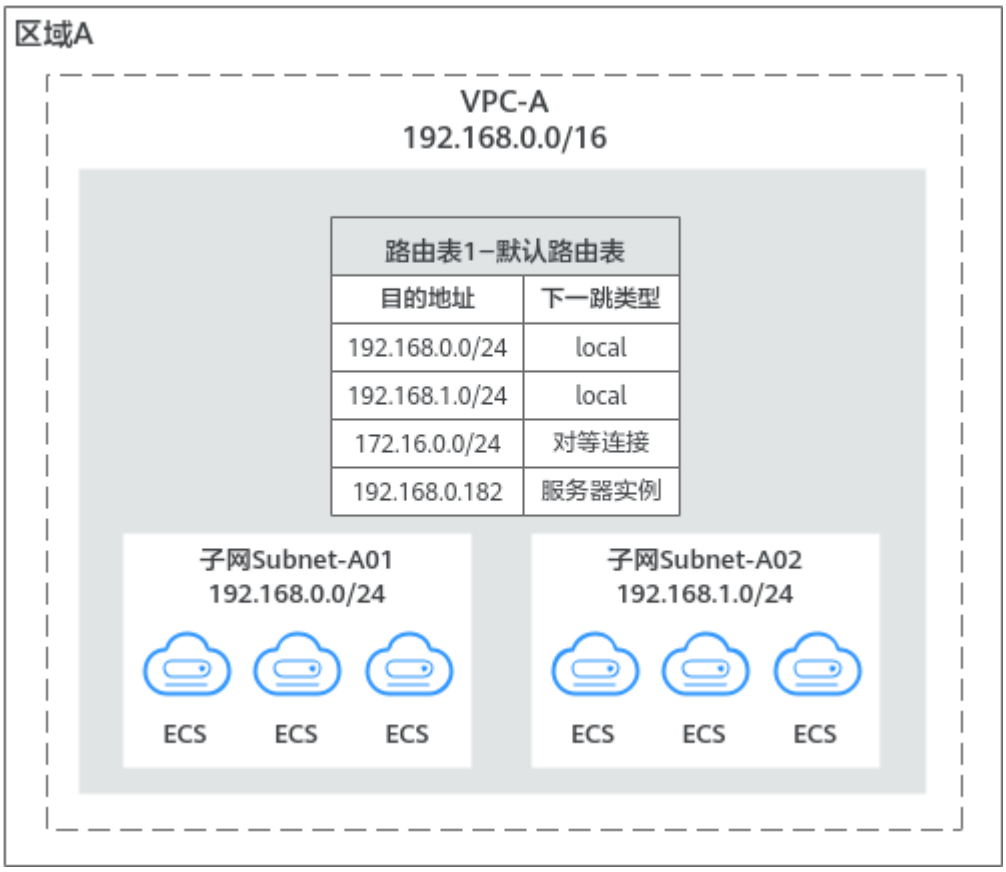
如何规划路由表的数量?

路由表由一系列路由规则组成，路由规则包括流量的目的地址和下一跳等信息，用于控制出入VPC内子网的流量走向。一个VPC内可以拥有多个路由表，请您参考以下建议规划路由表。

规划一个路由表

当VPC内不同子网的网络流量走向需求相同或者差异不大，则推荐您规划一个路由表。用户创建VPC时，系统会自动生成一个默认路由表，子网会自动关联默认路由表，您可以在默认路由表中添加不同的路由来控制流量走向。如图2-4所示，VPC-A中只有一个默认路由表，子网Subnet-A01和Subnet-A02均关联至默认路由表。

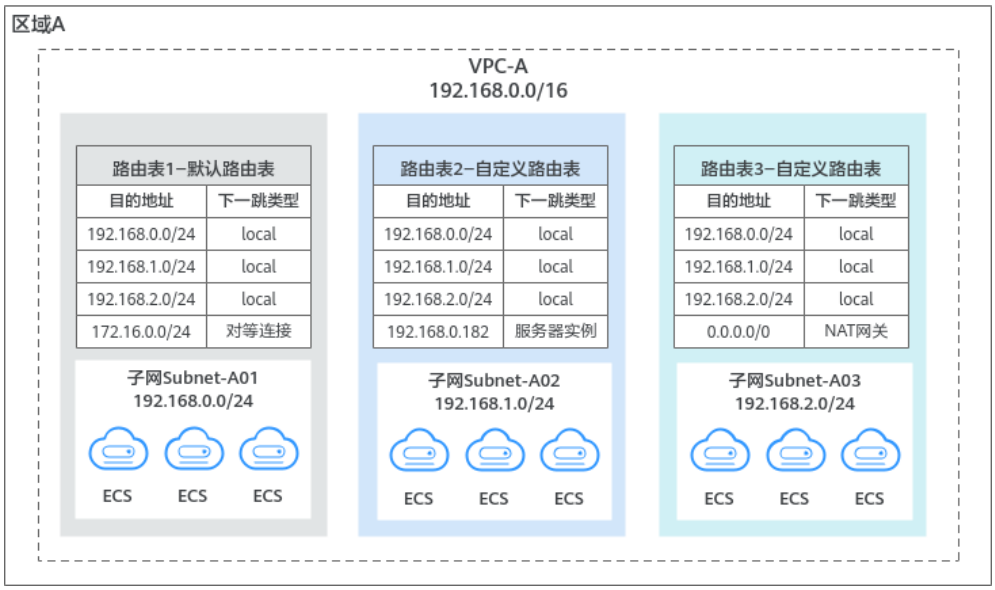
图 2-4 规划一个路由表



规划多个路由表

当VPC内不同子网的网络流量走向差异较大，则一个默认路由表无法满足业务需求，此时推荐您创建自定义路由表，将不同的子网关联至不同的路由表，实现不同流量走向的控制。如图2-5所示，VPC-A中有三个路由表，子网Subnet-A01关联至路由表1（默认路由表），子网Subnet-A02关联至路由表2（自定义路由表），子网Subnet-A03关联至路由表3（自定义路由表）。

图 2-5 规划多个路由表



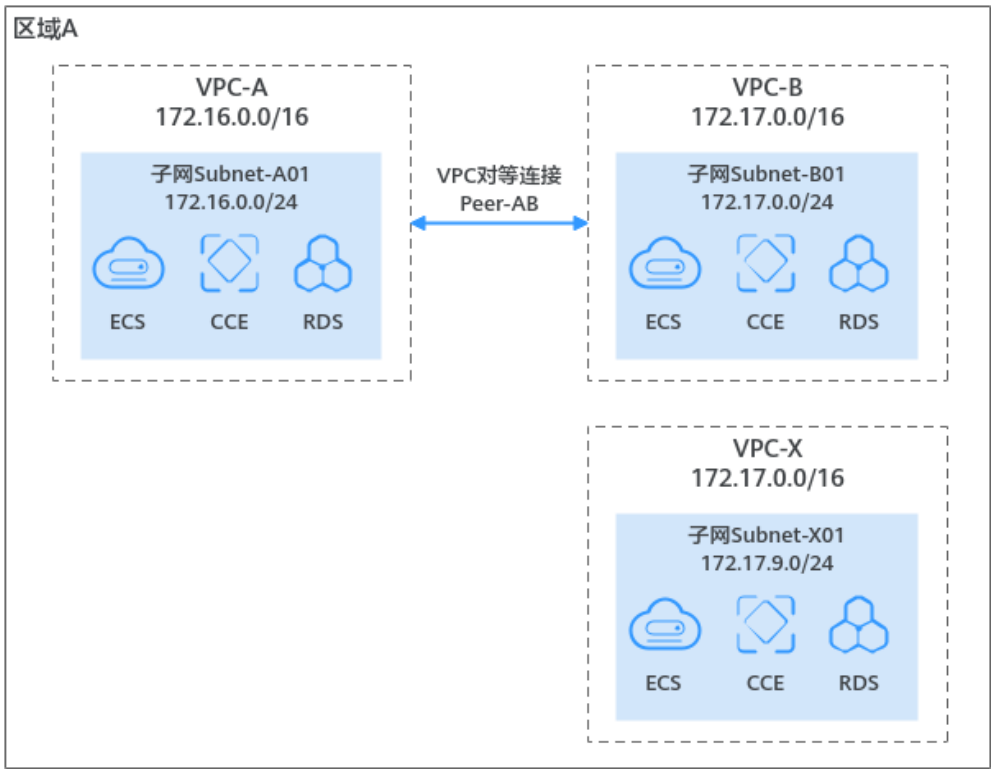
当 VPC 与其他 VPC 通信或者 VPC 与云下数据中心通信时如何规划网络?

如果您有VPC与其他VPC通信，或者VPC与云下数据中心通信的需求时，请确保VPC网段和需要通信的对端网段没有冲突。以下为您提供典型组网的网段规划示例。

连通 VPC 与其他 VPC

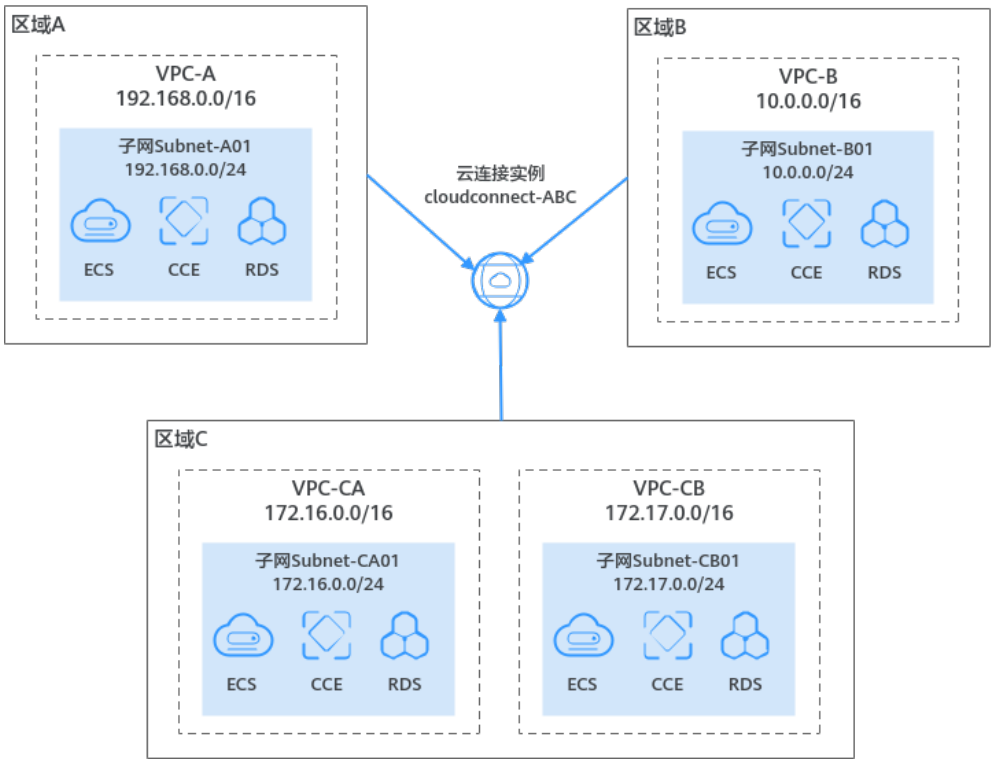
- 连通同区域的VPC：如图2-6所示，在区域A内，一共有三个VPC，分别为VPC-A、VPC-B和VPC-X。由于业务需求，需要连通VPC-A和VPC-B的网络，VPC-X不需要和其他VPC连通。
  - 由于VPC-A和VPC-B需要通信，则VPC-A和VPC-B的网段不能相同，通过对等连接连通VPC之间的内网网络。
  - 由于VPC-X和其他VPC之间不需要连通，因此VPC-X的网段可以和VPC-B相同，当前不会影响通信。但是基于业务的变化考虑，如果后续VPC-X和VPC-B需要通信，则在网段相同的基础上，建议VPC-B和VPC-X内的子网网段不能相同，则可以建立子网之间的对等连接。

图 2-6 连通同区域的 VPC



- 连通不同区域的VPC：如图2-7所示，业务需要部署在三个不同的区域内的VPC，分别为VPC-A、VPC-B、VPC-CA和VPC-CB。使用云连接可以快速连通不同区域的VPC，VPC基于云内骨干网络实现内网通信，需要通信的VPC网段不能相同。

图 2-7 连通不同区域的 VPC

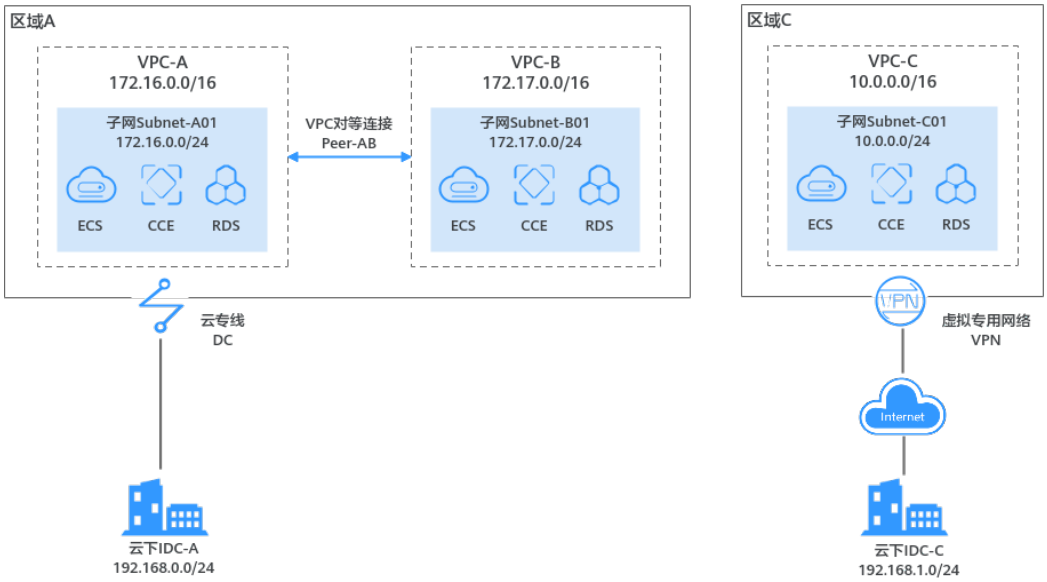


连通 VPC 和云下数据中心

如图2-8所示，在区域A内，VPC-A和VPC-B之间需要互通，并且VPC-A需要连通云下数据中心IDC-A。在区域C内，VPC-C需要连通云下数据中心IDC-C。

- 在区域A内，VPC-A和VPC-B的网段不同，可以通过对等连接连通网络。VPC-A和IDC-A通过云专线连通，VPC-A和IDC-A的网段不能相同。
- 在区域C内，VPC-C和IDC-C使用VPN通过互联网连通，VPC-C和IDC-C的网段不能相同。

图 2-8 连通 VPC 和云下数据中心



相关文档

- 您可以通过VPC快速搭建一个具有IPv4地址段的云上私有网络，同时，还可以通过EIP实现云上网络和公网通信的需求，具体请参见**通过VPC快速搭建IPv4网络**。
- 您可以通过VPC快速搭建一个同时具有IPv4和IPv6地址段的云上私有网络。同时，还可以通过EIP和共享带宽，实现IPv4和IPv6公网通信需求，具体请参见**通过VPC快速搭建IPv4/IPv6双栈网络**。

2.2 虚拟私有云网络连接方案

2.2.1 VPC 网络连接方案概述

华为云拥有丰富的网络服务，可以搭建安全、可扩展的云上网络环境。同时华为云提供了高速、可靠的云上云下网络连接服务，能够实现VPC和其他VPC之间的网络互通、VPC内实例（比如ECS、RDS）访问公网、以及云上VPC和云下数据中心（IDC）网络互通的需求。以下为您详细介绍各类网络服务的功能和主要特点，您可以根据网络需求灵活搭配VPC和其他网络服务。

- **连通VPC和其他VPC的网络**
- **连通VPC和公网的网络**

- 连通VPC和云下数据中心的网络

连通 VPC 和其他 VPC 的网络

通过表2-3中介绍的网络服务，您可以灵活连通不同VPC之间的网络，包括同区域内VPC的网络，不同区域内VPC的网络，或者不同账号内VPC的网络等。

表 2-3 网络服务（连通 VPC 和其他 VPC 的网络）

网络服务	功能介绍	主要特点
对等连接	对等连接是建立在两个VPC之间的网络连接，用于连通同一个区域内的VPC，可以实现不同VPC之间的云上内网通信。对等连接可以连通相同账号或者不同账号下的VPC网络。	• 成本低，当前VPC对等连接不收取任何费用 • 需要手动配置路由
企业路由器（ER）	对于同一个区域的VPC，可以在一个企业路由器中接入相同账号或者不同账号下的多个VPC，构建中心辐射型组网。企业路由器可以同时连接多个VPC，相比对等连接，企业路由器更适用于多VPC互联的复杂组网。	• 分钟级连通同区域内的多个VPC • 配置简单，可自动配置路由 • 低时延、高速率 • 网络拓扑简洁且扩展性高
云连接（CC） • 云连接实例 • 云连接中心网络	对于不同区域的VPC，不论VPC属于同一个账号还是不同账号，都可以接入云连接中实现内网通信。云连接提供以下两种方案： • 云连接实例：直接将不同区域的VPC接入云连接实例连通网络。 • 中心网络：将同区域的VPC接入企业路由器连通网络，再将不同区域的企业路由器接入中心网络连通跨区域网络。该方案的网络架构扩展性更强，适用于多VPC互联的复杂组网。	• 分钟级连通跨区域的VPC网络 • 配置简单，可自动配置路由 • 低时延、高速率
虚拟专用网络（VPN）	基于公网，通过VPN的加密通道连通不同区域的VPC。	• 成本低 • 配置简单 • 即开即用 • 网络质量依赖公网
云专线（DC）	基于物理专线，通过云专线可以连通不同区域的VPC。	• 高安全的专属网络通道 • 低时延、高速率

连通 VPC 和公网的网络

通过表2-4中介绍的网络服务，您可以连通VPC和公网的网络，实现VPC内的实例主动访问公网、或者面向公网提供服务。

表 2-4 网络服务（连通 VPC 和公网的网络）

网络服务	功能介绍	主要特点
弹性公网IP（EIP）	EIP是一个独立的公网IP地址，可以将EIP绑定至实例（比如ECS、NAT网关、ELB），实例即可连接公网，实现主动访问公网或面向公网提供服务。	• 和实例动态绑定/解绑定 • 搭配使用共享带宽和共享流量包，降低公网成本 • 支持随时调整EIP带宽
NAT网关（NAT） • **NAT网关（SNAT）** • **NAT网关（DNAT）**	NAT网关提供SNAT和DNAT两种功能： • SNAT可实现VPC内的多个ECS共用一个或多个EIP主动访问公网。 – **同一个VPC内的ECS共用EIP** – **不同VPC内的ECS共用EIP** • DNAT可以实现端口级别的转发，将EIP的端口映射到不同ECS的端口上，使VPC内多个ECS共用同一EIP和带宽面向公网提供服务，但没有均衡流量的功能。	• 降低成本，NAT网关实现多个ECS共用EIP访问公网 • 高安全，IP映射避免ECS绑定的EIP直接暴露 • 多种NAT网关规格灵活可选
弹性负载均衡（ELB）	**ELB**可以将访问流量均衡分发到多个后端服务器（比如ECS），并且配合EIP，支撑海量用户从公网访问云上部署的业务。	• 具备强大的四层和七层处理能力，支持多种应用协议和转发策略 • 消除服务器单点故障，实现业务高可用

连通 VPC 和云下数据中心的网络

对于拥有云下数据中心的用户，由于利旧和平滑演进的原因，并非所有的业务都可以迁移至云上，通过**表2-5**中介绍的网络服务，可以连通VPC和云下数据中心网络，构建混合云组网。

表 2-5 网络服务（连通 VPC 和云下数据中心的网络）

网络服务	功能介绍	主要特点
虚拟专用网络（VPN）	基于公网，通过**VPN**的加密通道连通VPC和云下数据中心网络。	• 成本低 • 配置简单 • 即开即用 • 网络质量依赖公网

网络服务	功能介绍	主要特点
云专线（DC）	基于物理专线，通过云专线可以连通VPC和云下数据中心网络。	• 高安全的专属网络通道 • 低时延、高速率
对等连接	对等连接是建立在两个VPC之间的网络连接，用于连通同一个区域内的VPC，可以实现不同VPC之间的云上内网通信。对等连接可以连通相同账号或者不同账号下的VPC网络。搭配对等连接和云专线或者VPN，可以实现云上多个VPC和云下IDC的网络通信。	• 成本低，当前VPC对等连接不收取任何费用 • 需要手动配置路由
企业路由器（ER）	在企业路由器中，接入同一个区域内的多个VPC，并结合云专线的全球接入网关或者VPN的能力，快速实现多个VPC和云下数据中心的网络互通。	• 配置简单，支持路由学习，无需手工配置路由 • 支持多条DC/VPN链路之间联动，实现负载分担或互为主备
云连接 • 云连接实例 • 云连接中心网络	当需要连通多个区域内的VPC和云下IDC的网络时，可以使用云专线或者VPN连通云下IDC网络，同时搭配云连接实例或者中心网络，构建多VPC连接云下IDC的跨区域混合云组网。以搭配云专线为例，云连接提供以下两种方案： • 云连接实例：直接将不同区域的VPC接入云连接实例，为每个需要连通云下IDC的VPC单独创建云专线的虚拟网关VGW。 • 云连接中心网络：使用云连接中心网络搭配企业路由器的方案，需要先将同区域的VPC和云专线的全球接入网关DGW接入企业路由器，再将不同区域的企业路由器接入中心网络，可以将多个区域的VPC和多个城市的云下IDC连通起来。该方案相比使用云连接实例，网络架构更简单，且扩展性更强。	• 配置简单，支持路由学习，无需手工配置路由 • 灵活定义网络互通策略

2.2.2 连通 VPC 和其他 VPC 的网络（私网网络）

连通相同区域的 VPC 网络

如果您需要连通网络的VPC位于同一个区域，您可以使用VPC对等连接、企业路由器，以下为您提供典型的网络连接方案。

关于不同网络连接服务的详细介绍和主要特点，请您参见**连通VPC和其他VPC的网络**。

须知

连通VPC和其他VPC时，您需要提前做好网络规划，建议网络两端通信的VPC网段不要重叠，否则可能导致无法通信。

对等连接

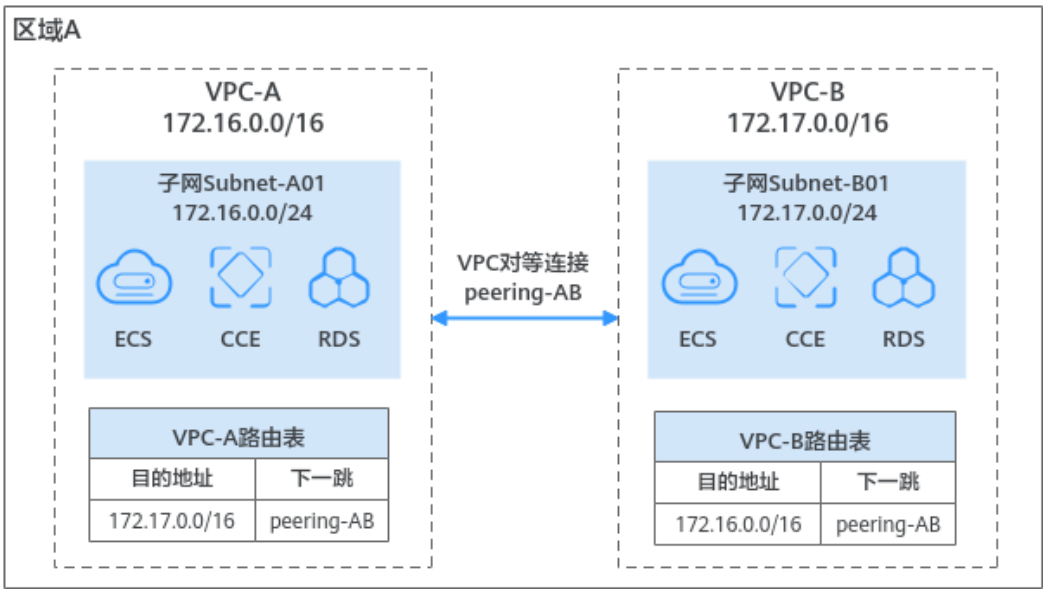
对等连接是建立在两个VPC之间的网络连接，用于连通同一个区域内的VPC，可以实现不同VPC之间的云上内网通信。对等连接可以连通相同账号或者不同账号下的VPC网络。

详情请参见：

- **创建同一账户下的对等连接**
- **创建不同账户下的对等连接**

如**图2-9**所示，在区域A内，通过在VPC-A和VPC-B之间建立对等连接peering-AB，连通VPC-A和VPC-B之间的网络。

图 2-9 通过对等连接连通同区域 VPC



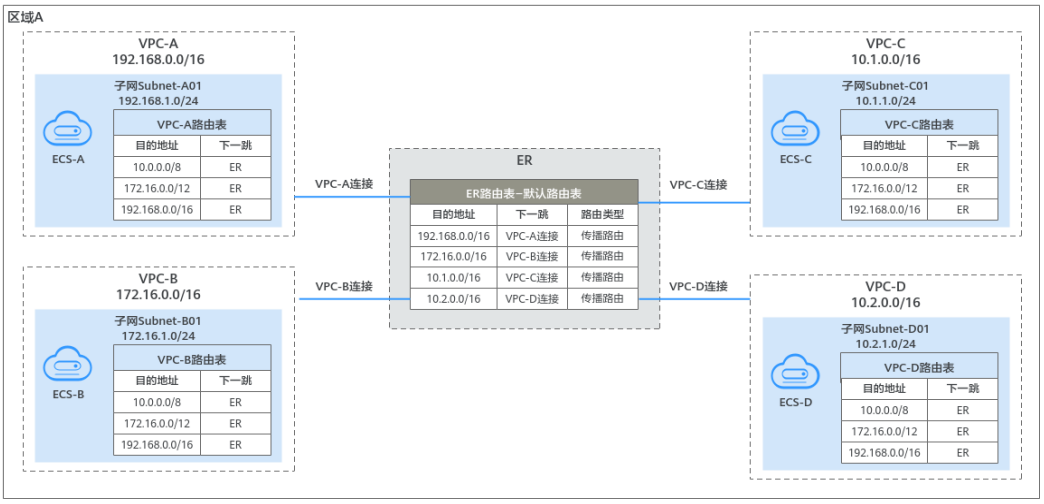
企业路由器（ER）

对于同一个区域的VPC，可以在一个企业路由器中接入相同账号或者不同账号下的多个VPC，构建中心辐射型组网。企业路由器可以同时连接多个VPC，相比对等连接，企业路由器更适用于多VPC互联的复杂组网。

详情请参见**通过企业路由器实现同区域VPC互通**。

如**图2-10**所示，在区域A内创建一个企业路由器ER，并将VPC接入ER内，系统会自动配置VPC侧和ER侧的路由，则ER可以在4个VPC之间转发流量，实现网络互通。

图 2-10 通过企业路由器连通同区域 VPC



连通不同区域的 VPC 网络

如果您需要连通网络的VPC位于不同区域，您可以使用云连接、云专线或者虚拟专用网络，以下为您提供典型的网络连接方案。

关于不同网络连接服务的详细介绍和主要特点，请您参见**连通VPC和其他VPC的网络**。

须知

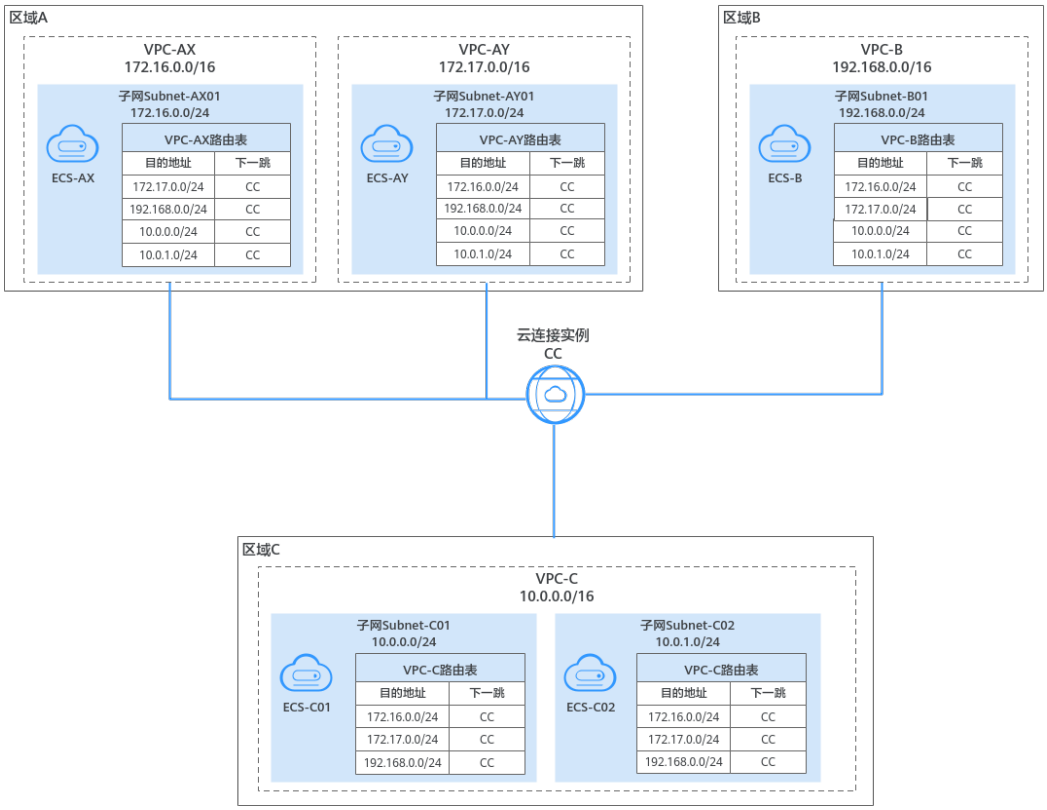
连通VPC和其他VPC时，您需要提前做好网络规划，建议网络两端通信的VPC网段不要重叠，否则可能导致无法通信。

云连接实例

您可以直接将不同区域的VPC接入云连接实例，不论VPC属于同一个账号还是不同账号，都可以接入云连接中实现内网通信。详情请参见**跨区域VPC互通**。

如**图2-11**所示，将区域A的VPC-AX和VPC-AY、区域B的VPC-B以及区域C的VPC-C均接入云连接实例中，连通跨区域VPC的内网网络。

图 2-11 通过云连接实例连通不同区域 VPC



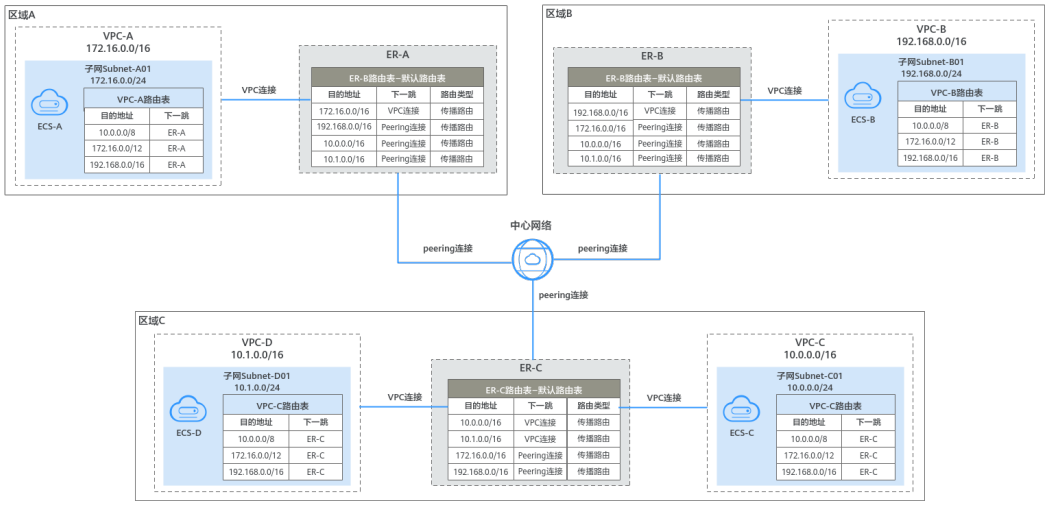
云连接中心网络

您可以先将同区域的VPC接入企业路由器连通网络，再将不同区域的企业路由器接入中心网络连通跨区域网络。该方案的网络架构扩展性更强，适用于多VPC互联的复杂组网。

详情请参见**通过企业路由器和云连接中心网络实现跨区域VPC互通**。

如**图2-12**所示，在区域A内将VPC-A接入ER-A，在区域B内将VPC-B接入ER-B，在区域C内将VPC-C和VPC-D接入ER-C，分别通过企业路由器连通同区域VPC网络。然后通过中心网络连通ER-A、ER-B以及ER-C，实现了跨区域网络互通。相比云连接实例直连VPC的方案，如果后续需要连通更多的VPC，只需要将VPC接入同区域的企业路由器即可，网络拓扑更加简洁。

图 2-12 通过中心网络连通不同区域 VPC

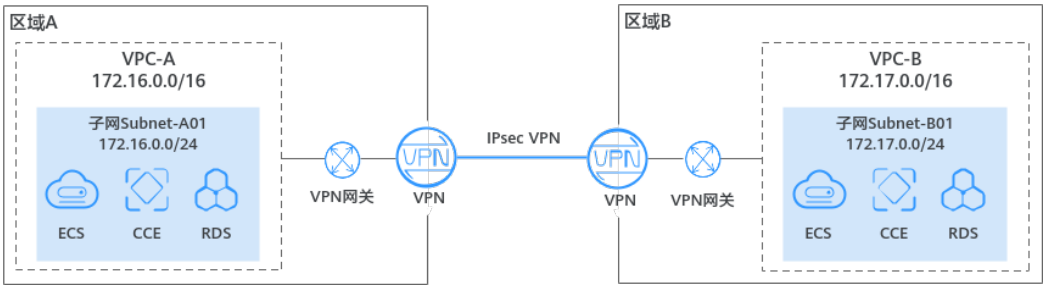


虚拟专用网络（VPN）

基于公网，通过**VPN**的加密通道连通不同区域的VPC。

如**图2-13**所示，在区域A内通过一个VPN连接VPC-A，在区域B内通过另一个VPN连接VPC-B，两端VPC可以通过VPN的加密通道实现网络互通，相比云专线，VPN开通更快速且成本较低。

图 2-13 通过 VPN 连通不同区域 VPC

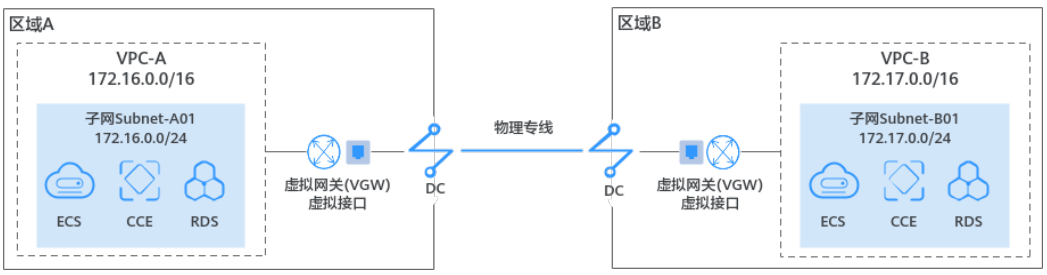


云专线（DC）

基于物理专线，通过**云专线**可以连通不同区域的VPC。

如**图2-14**所示，在区域A内通过一个云专线连接VPC-A，在区域B内通过另一个云专线连接VPC-B，两端VPC可以通过云专线的专属通道实现网络互通，相比VPN，专属网络通道更高速、稳定。

图 2-14 通过 DC 连通不同区域 VPC



2.2.3 连通 VPC 和公网的网络（公网网络）

如果您需要连通VPC和公网网络，可以使用弹性公网IP、NAT网关或者弹性负载均衡，以下为您提供典型的网络连接方案。

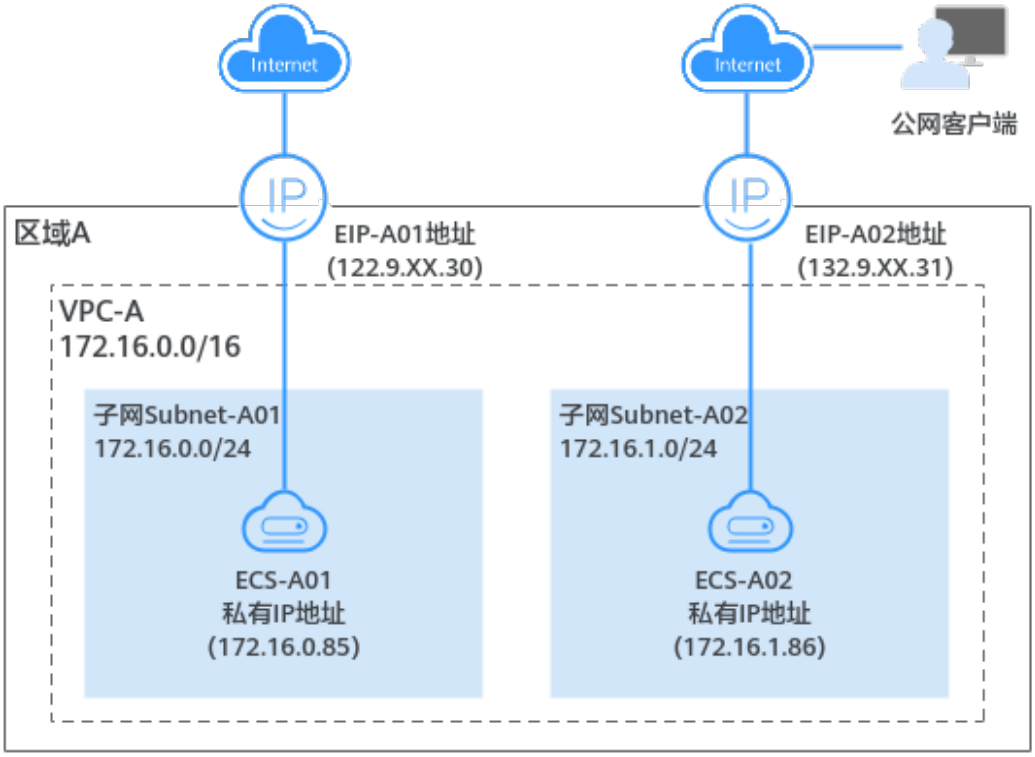
弹性公网 IP（EIP）

EIP是一个独立的公网IP地址，可以将EIP绑定至实例（比如ECS、NAT网关、ELB），实例即可连接公网，实现主动访问公网或面向公网提供服务。

- IPv4网络：详情请参见**通过VPC和EIP快速搭建可访问公网的IPv4网络**。
- IPv4/IPv6双栈网络：详情请参见**通过VPC快速搭建IPv4/IPv6双栈网络**。

如**图2-15**所示，在区域A内，子网Subnet-A01部署的ECS-A01需要访问公网，将EIP-A01绑定至ECS-A01，ECS-A01即可访问公网。子网Subnet-A02部署的ECS-A02需要面向公网提供Web服务，将EIP-A02绑定至ECS-A02，ECS-A02即可连通公网。

图 2-15 通过 EIP 连通 VPC 和公网



NAT 网关（SNAT）

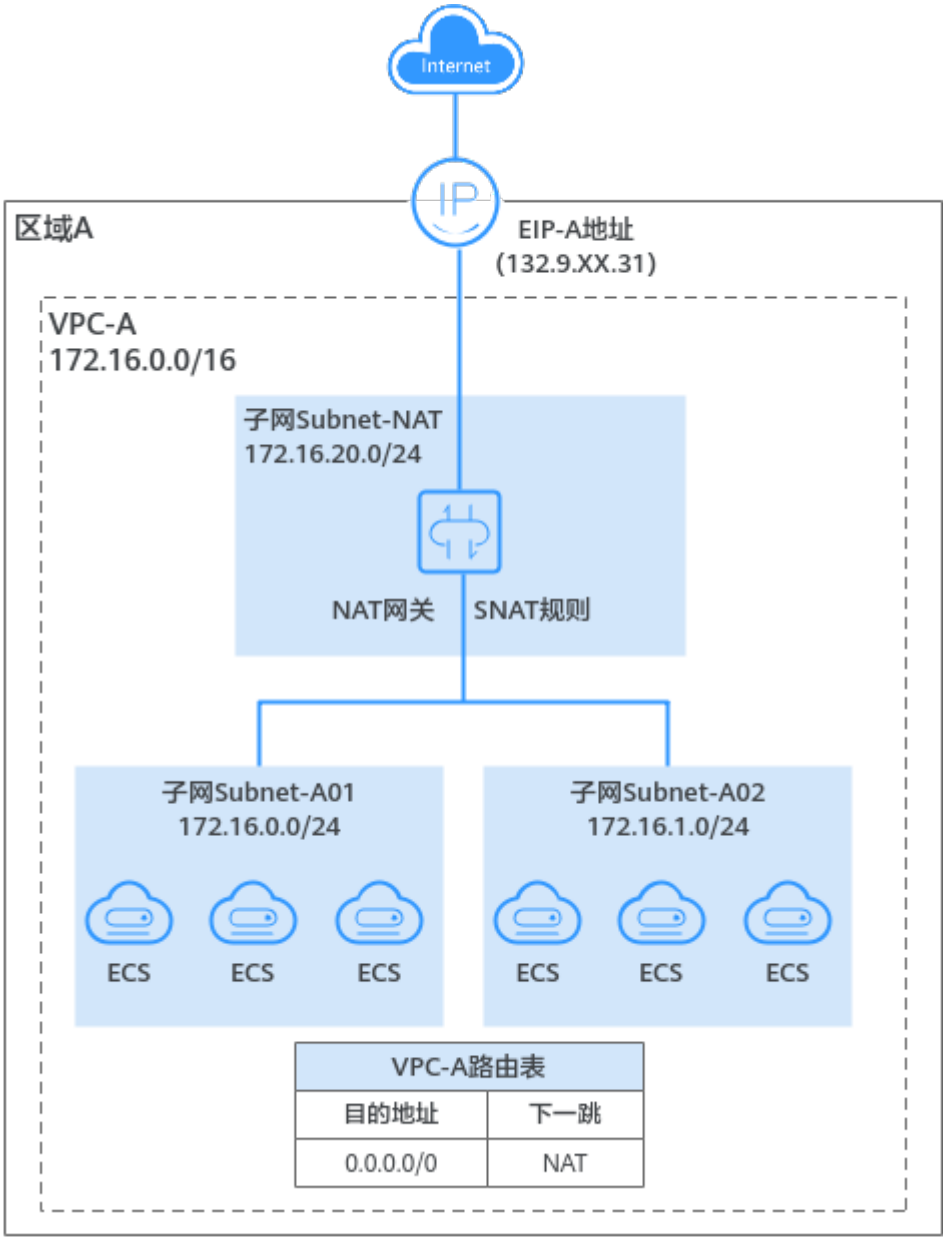
使用公网NAT网关，并配置SNAT规则，可实现VPC内的多个ECS共享一个或多个EIP主动访问公网。对比为ECS直接绑定EIP访问公网，只配置SNAT规则且未配置DNAT规则时，外部用户无法通过公网直接访问NAT网关的公网地址，保证了ECS的相对安全。

- 同一个VPC内的ECS共用EIP：详情请参见**通过公网NAT网关的SNAT规则访问公网**。
- 不同VPC内的ECS共用EIP：详情请参见**通过企业路由器和NAT网关实现多个VPC共享SNAT访问公网**。

同一个 VPC 内的 ECS 共用 EIP

如图2-16所示，在区域A内，VPC-A的子网Subnet-A01和Subnet-A02的业务ECS需要访问公网。首先在子网Subnet-NAT中创建公网NAT网关，其次在公网NAT网关中，分别配置Subnet-A01和Subnet-A02的子网网段对应的SNAT规则，可以实现Subnet-A01和Subnet-A02中所有ECS共用EIP-A访问公网的需求。

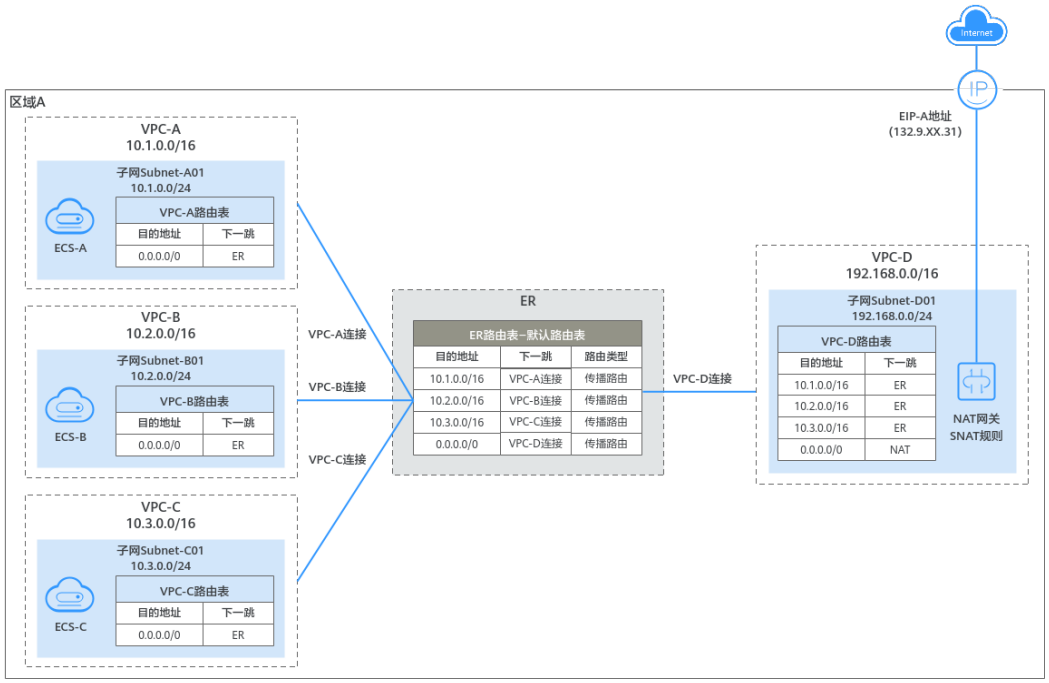
图 2-16 通过 NAT 网关实现 VPC 内 ECS 访问公网（同一个 VPC 内的 ECS 共用 EIP）



不同 VPC 内的 ECS 共用 EIP

如图2-17所示，在区域A内，VPC-A、VPC-B和VPC-C需要网络互通，并且可以共用VPC-D中部署的NAT网关访问公网。首先将四个VPC接入企业路由器ER中，其次在VPC和ER路由表中配置路由，最后在公网NAT网关中配置SNAT规则，可以实现不同VPC的网络互通，并且共用EIP-A访问公网的需求。

图 2-17 通过 NAT 网关实现 VPC 内 ECS 访问公网（不同 VPC 内的 ECS 共用 EIP）



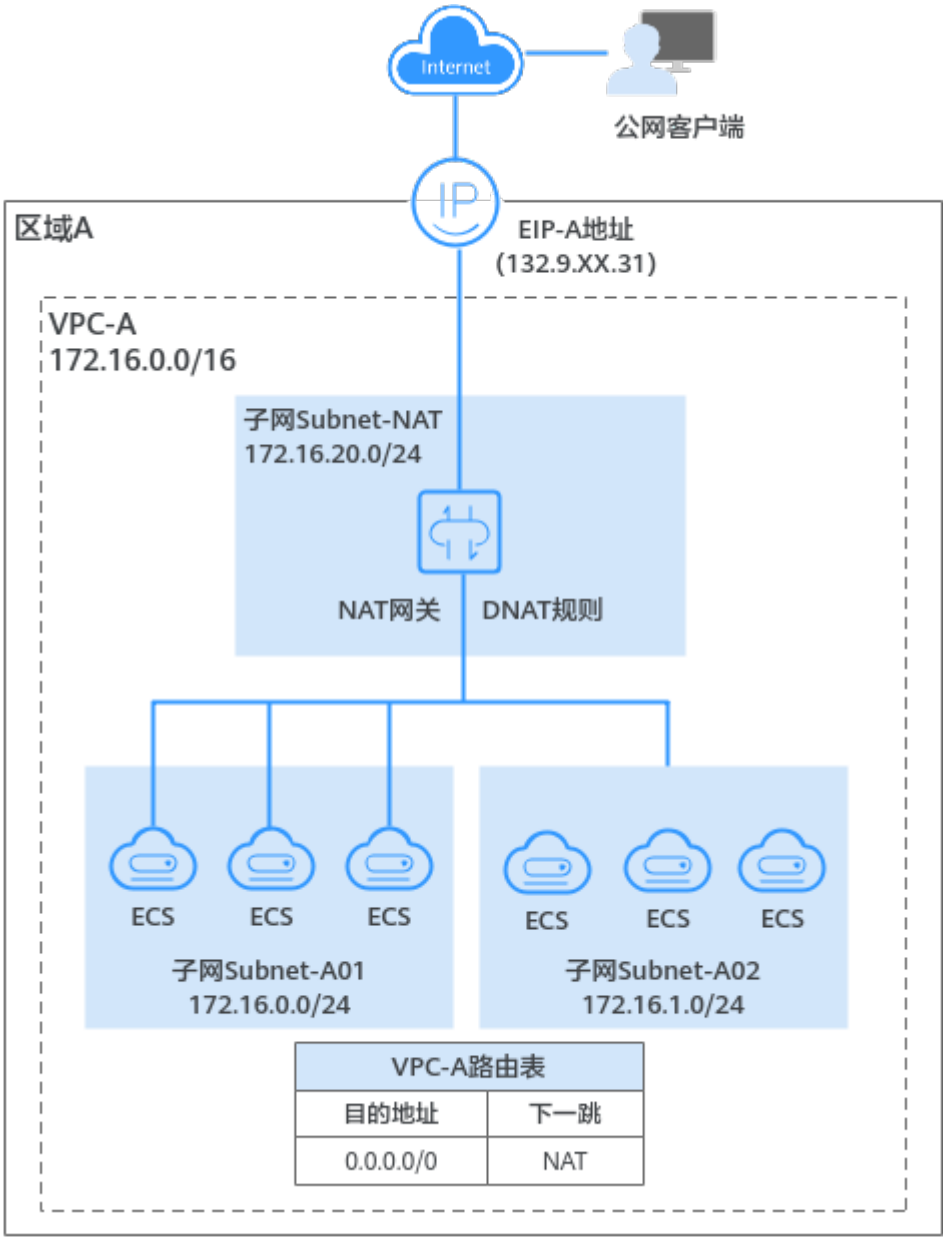
NAT 网关（DNAT）

基于公网NAT网关的DNAT功能可以实现端口级别的转发，将EIP的端口映射到不同ECS的端口上，使VPC内多个ECS共用同一EIP和带宽面向公网提供服务，但没有均衡流量的功能。

详情请参见**通过公网NAT网关的DNAT规则面向公网提供服务**。

如**图2-18**所示，在区域A内，VPC-A的子网Subnet-A01和Subnet-A02的中部署的ECS需要面向公网提供Web服务。首先在子网Subnet-NAT中创建公网NAT网关，其次在公网NAT网关中，分别配置ECS或者私网网段对应的DNAT规则，可以实现Subnet-A01和Subnet-A02中所有ECS共用EIP-A面向公网提供服务的需求。

图 2-18 通过 NAT 网关实现 VPC 内 ECS 面向公网提供服务



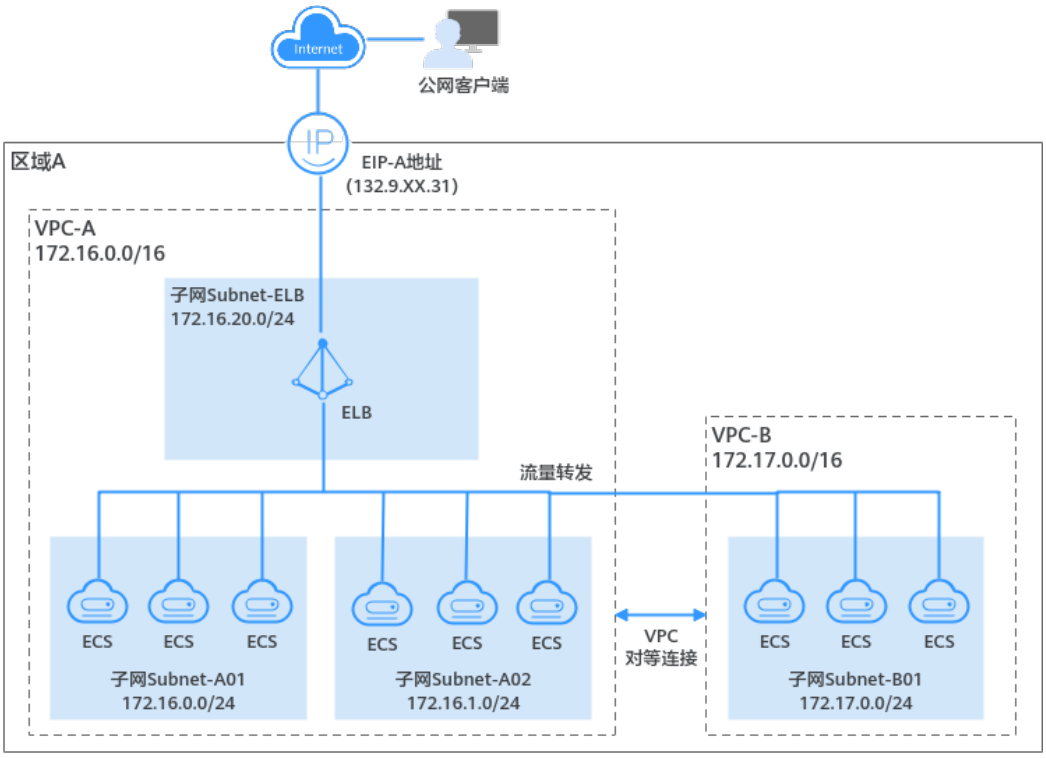
弹性负载均衡（ELB）

ELB可以将访问流量均衡分发到多个后端服务器（比如ECS），并且配合EIP，支撑海量用户从公网访问云上部署的业务。

详情请参见**实现Web应用的负载均衡**。

如**图2-19**所示，在区域A内，客户部署Web应用，由于业务量比较大，需要多个ECS进行流量负载分发，因此在子网VPC-A和VPC-B内均部署了ECS作为Web服务器。通过ELB进行业务流量分发时，如果需要添加多个VPC内的ECS作为后端服务器，则需要确保这些VPC的内网已经连通。本示例中采用VPC对等连接连通VPC-A和VPC-B。

图 2-19 通过 ELB 实现公网访问流量均衡分发



2.2.4 连通 VPC 和云下数据中心的网络（混合云网络）

连通单个 VPC 和云下 IDC 的网络

如果您需要连通单个VPC和云下IDC的网络，可以使用云专线或者虚拟专用网络，以下为您提供典型的网络连接方案。

对于不同网络连接服务的详细介绍和主要特点，请您参见**连通VPC和云下数据中心的网络**。

须知

连通VPC和云下IDC时，您需要提前做好网络规划，连通的VPC子网网段和IDC侧网段不要重叠，否则可能导致无法通信。

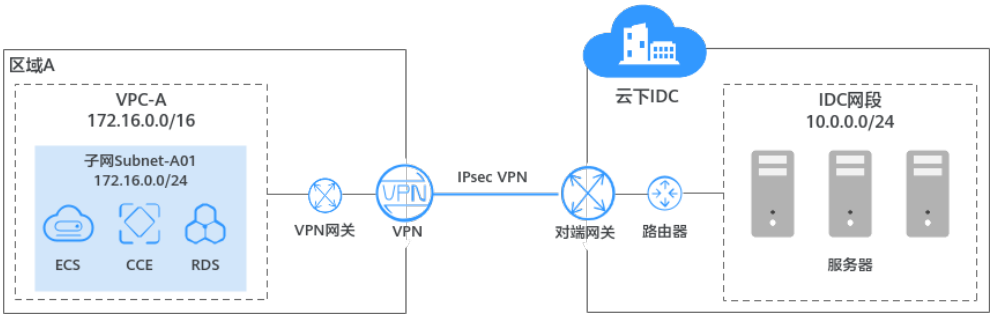
虚拟专用网络（VPN）

基于公网，通过**VPN**的加密通道连通VPC和云下数据中心网络。

详情请参见**通过企业版站点入云VPN实现数据中心和VPC互通**。

如**图2-20**所示，用户的业务一部分部署在云上区域A的VPC-A内，一部分部署在云下IDC中，通过VPN基于公网的加密通道，可以快速连通云上和云下的网络通信。相比云专线，使用VPN，配置更简单且成本较低。

图 2-20 通过 VPN 连通 VPC 和云下 IDC



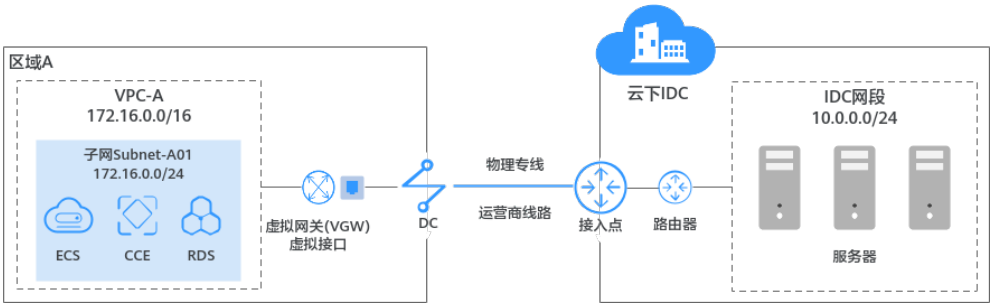
云专线（DC）

基于物理专线，通过**云专线**可以连通VPC和云下数据中心网络。

详情请参见**用户通过单专线BGP协议访问VPC**。

如**图2-21**所示，用户的业务一部分部署在云上区域A的VPC-A内，一部分部署在云下IDC中，通过云专线的专属通道实现网络互通，相比VPN，专属网络通道更高速、稳定。

图 2-21 通过 DC 连通 VPC 和云下 IDC



连通同区域的多个 VPC 和云下 IDC 的网络

如果您需要连通某个区域内的多个VPC和云下IDC的网络，您可以使用云专线或者虚拟专用网络连通线下IDC网络，同时搭配VPC对等连接或者企业路由器连通多个VPC网络，构建多VPC连接云下IDC的混合云组网，以下为您提供典型的网络连接方案。

以下示例使用云专线连通云下IDC，专属网络通道更高速、稳定。如果您希望降低网络成本，推荐您使用VPN代替云专线。对于不同网络连接服务的详细介绍和主要特点，请您参见**连通VPC和云下数据中心的网络**。

须知

连通多个VPC和云下IDC时，您需要提前做好网络规划，请遵循以下原则：

- 连通VPC和云下IDC网络时，连通的VPC子网网段和IDC侧网段不要重叠，否则可能导致无法通信。
- 连通VPC和其他VPC网络时，建议网络两端通信的VPC网段不要重叠，否则可能导致无法通信。

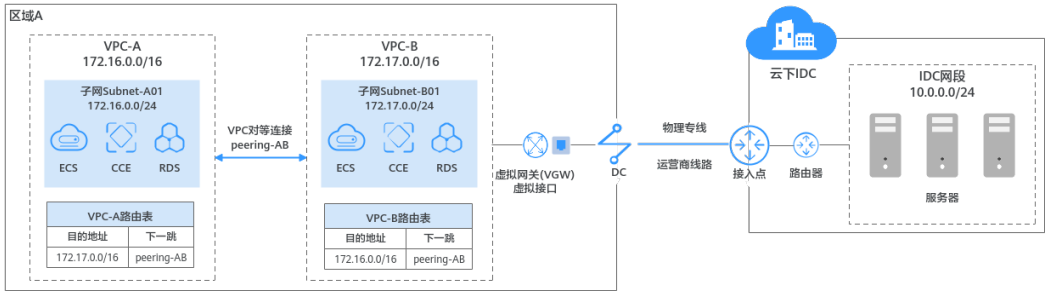
对等连接

对等连接是建立在两个VPC之间的网络连接，用于连通同一个区域内的VPC，可以实现不同VPC之间的云上内网通信。对等连接可以连通相同账号或者不同账号下的VPC网络。搭配对等连接和云专线或者VPN，可以实现云上多个VPC和云下IDC的网络通信。

详情请参见**通过对等连接连通同区域的多个VPC和云下IDC的网络**。

如图2-22所示，用户的业务一部分部署在云上区域A的VPC-A和VPC-B内，一部分部署在云下IDC中。首先通过云专线的专属通道连通VPC-B和云下IDC的网络，其次通过对等连接连通VPC-A和VPC-B的云内网络，此时VPC-A和VPC-B均可以访问云下IDC。

图 2-22 通过对等连接连通同区域的多个 VPC 和云下 IDC 的网络



企业路由器（ER）

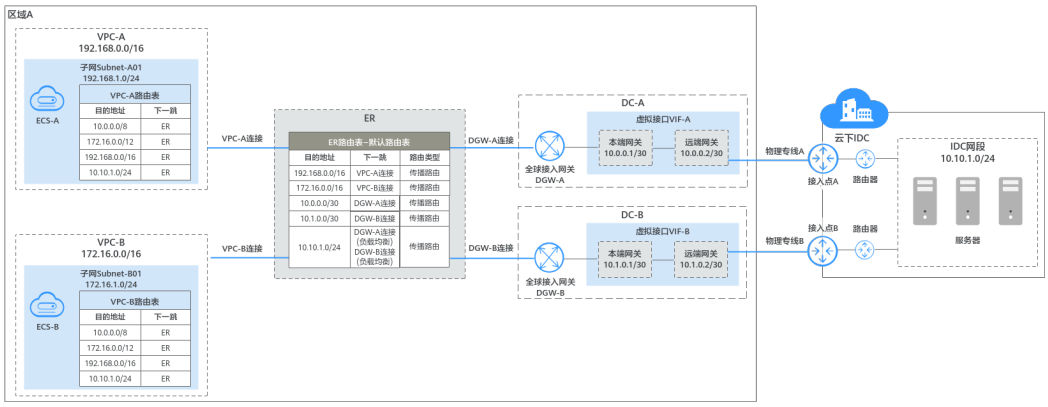
在企业路由器中，接入同一个区域内的多个VPC，并结合云专线的全球接入网关或者VPN的能力，快速实现多个VPC和云下数据中心的网络互通。

- **通过企业路由器和云专线构建混合云组网（全球接入网关DGW）**
- **通过企业路由器构建DC双链路负载混合云组网（全球接入网关DGW）**
- **通过企业路由器构建DC双链路主备混合云组网（全球接入网关DGW）**
- **通过企业路由器构建DC/VPN双链路主备混合云组网（全球接入网关DGW）**

如图2-23所示，用户的业务一部分部署在云上区域A的VPC-A和VPC-B内，一部分部署在云下IDC中。将VPC-A、VPC-B以及全球接入网关接入企业路由器中，VPC-A和VPC-B网络互通，并且均可以和云下IDC通信。

本示例中为了提升混合云组网的网络性能以及可靠性，同时部署了两条专线DC链路，两条DC链路形成负载均衡。当两条DC链路网络均正常，同时工作可提升网络传输能力。当其中一条DC链路故障时，另外一条DC链路可确保整个混合云组网的正常运行，避免了单点故障带来的业务中断。

图 2-23 通过企业路由器连通同区域的多个 VPC 和云下 IDC



连通不同区域的多个 VPC 和云下 IDC 的网络

如果您需要连通多个区域内的VPC和云下IDC的网络，您可以使用云专线或者虚拟专用网络连通线下IDC网络，同时搭配云连接实例或者中心网络，构建多VPC连接云下IDC的跨区域混合云组网，以下为您提供典型的网络连接方案。

以下示例使用云专线连通云下IDC，专属网络通道更高速、稳定。如果您希望降低网络成本，推荐您使用VPN代替云专线。对于不同网络连接服务的详细介绍和主要特点，请您参见**连通VPC和云下数据中心的网络**。

须知

连通多个VPC和云下IDC时，您需要提前做好网络规划，请遵循以下原则：

- 连通VPC和云下IDC网络时，连通的VPC子网网段和IDC侧网段不要重叠，否则可能导致无法通信。
- 连通VPC和其他VPC网络时，建议网络两端通信的VPC网段不要重叠，否则可能导致无法通信。

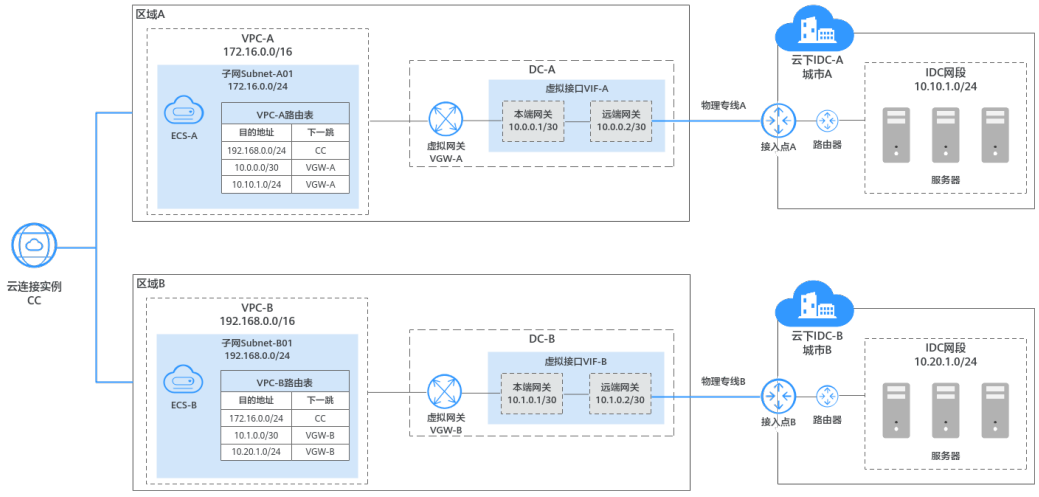
云连接实例

通过云连接实例连通不同区域的VPC，并为每个需要连通云下IDC的VPC单独创建云专线（虚拟网关VGW），可以将多个区域的VPC和多个城市的云下IDC连通起来。

详情请参见**通过云专线和云连接实现云下多IDC与云上多区域VPC互通**。

如**图2-24**所示，首先，通过云专线DC-A连通区域A的VPC-A和城市A的IDC-A、DC-B连通区域B的VPC-B和城市B的IDC-B。其次将VPC-A和VPC-B接入云连接实例中连通云内网络，就可以实现VPC-A、VPC-B、IDC-A、IDC-B的网络互通。

图 2-24 通过云连接实例连通不同区域的多个 VPC 和云下 IDC

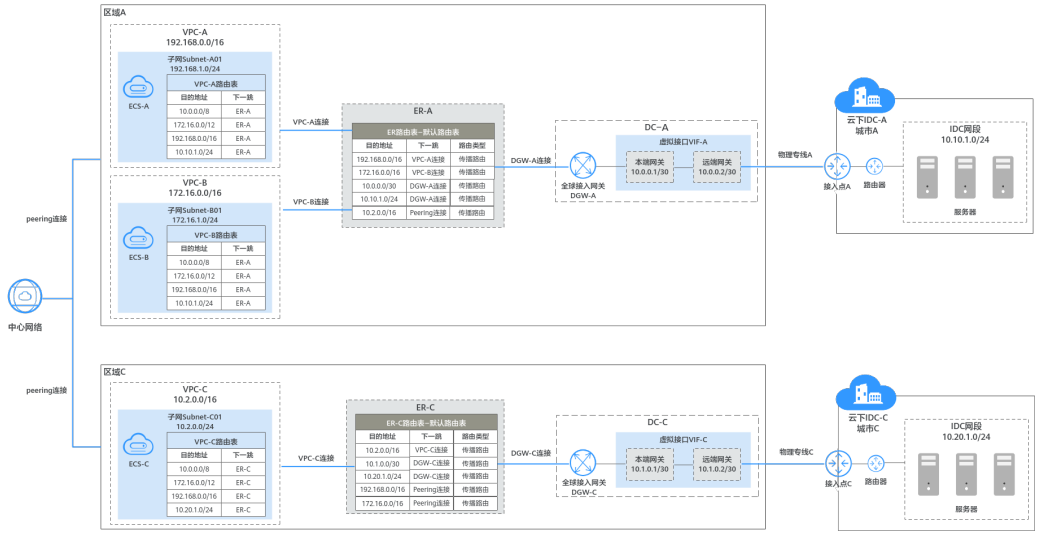


云连接中心网络

使用云连接中心网络搭配企业路由器的方案，需要先将同区域的VPC和云专线（全球接入网关DGW）接入企业路由器，再将不同区域的企业路由器接入**中心网络**，可以将多个区域的VPC和多个城市的云下IDC连通起来。该方案相比使用云连接实例，网络架构更简单，且扩展性更强。

如图2-25所示，首先，在每个区域的企业路由器中，接入当前区域内的VPC，并结合云专线的全球接入网关能力，快速实现多个VPC和云下数据中心的网络互通。其次将ER-A和ER-C接入中心网络中，连通不同区域的云内网络，就可以实现VPC-A、VPC-B、VPC-C和IDC-A、IDC-C的网络互通。相比云连接实例，该方案不用将所有需要互通的VPC接入云连接，只需要将每个区域的ER接入云连接中心网络中，简化了网络架构。同时，将专线接入ER中，多个VPC可以共用专线，ER的路由学习能力可以免去繁复的配置，降低维护难度。

图 2-25 通过中心网络连通不同区域的多个 VPC 和云下 IDC



2.3 虚拟私有云

2.3.1 创建虚拟私有云和子网

操作场景

虚拟私有云VPC是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。

您可以参考以下操作，自主选择IP网段来创建VPC，同时至少需要创建一个子网。创建VPC时，系统会为您生成一个默认路由表，默认路由表可以确保VPC内多个子网之间网络互通。

操作步骤

1. 进入**创建虚拟私有云页面**。
2. 在“创建虚拟私有云”页面，根据界面提示配置VPC和子网的参数。

   单击⊕，可以依次添加多个子网，一次最多可创建3个子网。

图 2-26 创建 VPC 和子网

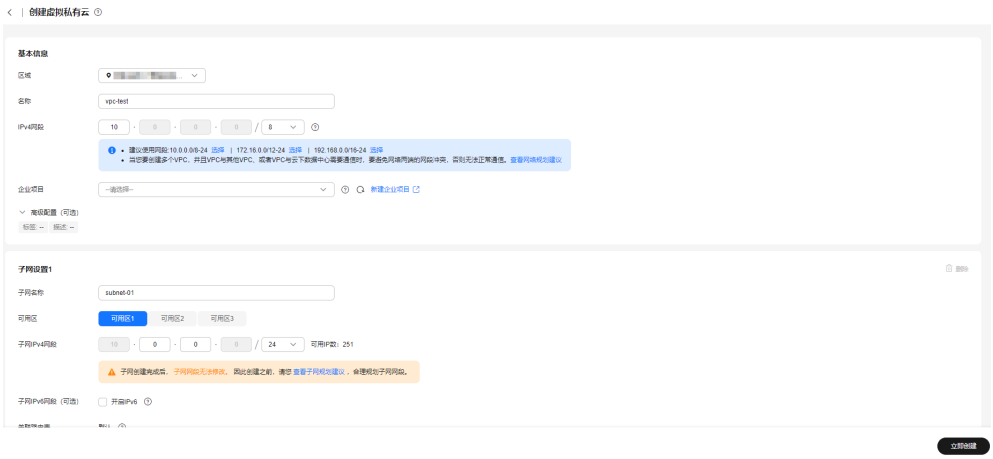


表 2-6 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-上海一
名称	输入VPC的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	vpc-test

参数	说明	取值样例
IPv4网段	设置VPC的IPv4网段范围，VPC网段的选择需要考虑以下两点： ● IP地址数量：要为业务预留足够的IP地址，防止业务扩展给网络带来冲击。 ● IP地址网段：当前VPC与其他VPC、云下数据中心连通时，要避免网络两端的IP地址冲突，否则无法正常通信。 建议您使用**RFC 1918**中指定的私有IPv4地址范围，作为VPC的网段，具体如下： ● 10.0.0.0/8-24：IP地址范围为10.0.0.0~10.255.255.255，掩码范围为8~24。 ● 172.16.0.0/12-24：IP地址范围为172.16.0.0~172.31.255.255，掩码范围为12~24。 ● 192.168.0.0/16-24：IP地址范围为192.168.0.0-192.168.255.255，掩码范围为16~24。 除了上述地址，您还可以使用任何可公共路由的IPv4地址（非RFC 1918指定的私有IPv4地址范围），但是必须排除以下系统预留地址和公网保留地址： ● 系统预留地址： – 100.64.0.0/10 – 214.0.0.0/7 – 198.18.0.0/15 – 169.254.0.0/16 ● 公网保留地址： – 0.0.0.0/8 – 127.0.0.0/8 – 240.0.0.0/4 – 255.255.255.255/32 关于VPC规划更详细的说明，请参见**虚拟私有云和子网规划建议**。	10.0.0.0/8
企业项目	创建VPC时，可以将VPC加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**。	default

参数	说明	取值样例
高级配置 > 标签	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以在创建VPC的时候为VPC绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。 关于标签更详细的说明，请参见**管理虚拟私有云标签**。 **说明** 如您的组织已经设定虚拟私有云的相关标签策略，则需按照标签策略规则为虚拟私有云添加标签。标签如果不符合标签策略的规则，则可能会导致虚拟私有云创建失败，请联系组织管理员了解标签策略详情。	• 键：vpc_key1 • 值：vpc-01
高级配置 > 描述	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以根据需要在文本框中输入对该VPC的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

表 2-7 子网参数说明

参数	说明	取值样例
子网名称	输入子网的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	subnet-01

参数	说明	取值样例
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 一个区域内有多个可用区，一个可用区发生故障后不会影响同一区域内的其它可用区。 **当页面显示“边缘可用区”时，您需要根据业务规划选择边缘可用区。不显示“边缘可用区”时，您无需设置子网可用区，不会影响实际使用。** ● 默认情况下，同一个VPC中，不同子网内的所有实例网络互通。同一个VPC内的子网可以位于不同可用区，不影响通信。比如VPC-A内有子网A01（可用区1）和子网A02（可用区2），子网A01和子网A02的网络默认互通。 ● 使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。假如可用区3发生故障，此时可用区1的云服务器可以继续使用可用区3的子网，不会影响您的业务。 ● 通用可用区：使用未发放至边缘小站的业务资源。该场景下和华为云上普通使用云服务方法完全一致。 ● 边缘可用区：使用已发放至边缘小站的业务资源。用户业务数据运行在用户数据中心边缘小站内（即本地）。边缘小站详细信息请参见 **智能边缘小站**。 关于可用区更详细的说明，请参见**区域和可用区**。	可用区1
子网网段	在未开启IPv4/IPv6双栈的区域，显示此参数。 设置VPC子网的IPv4网段范围，参数填写说明请参见“子网IPv4网段”。	10.0.0.0/24

参数	说明	取值样例
子网IPv4网段	在开启IPv4/IPv6双栈的区域，显示此参数。 设置子网的IPv4网段范围，子网是VPC内的IP地址块，可以将VPC的网段分成若干块，建议您规划子网时，遵循以下原则： ● 子网内可用IP数量：子网创建成功后，不支持修改网段，请您结合业务所需的IP地址数量，提前合理规划好子网网段。 – 子网网段不能太小，需要确保子网内可用IP地址数量可以满足业务需求。子网网段中第一个地址和后三个地址为系统预留地址，不能供实际业务使用，比如子网（10.0.0.0/24）中，10.0.0.1为网关地址、10.0.0.253为系统接口、10.0.0.254为DHCP使用、10.0.0.255为广播地址。 – 子网网段也不能太大，以免后续扩展新的业务时，VPC内可用网段不够再创建新的子网。 ● 子网网段避免冲突：如果子网所在的VPC与其他VPC、或者VPC与云下数据中心需要通信时，则VPC子网网段和网络对端网段不能相同，否则无法正常通信。 如果网络两端的子网网段已经相同，您可以创建新的子网，请参见**为虚拟私有云创建新的子网**。 子网的网段必须在VPC网段范围内，子网网段的掩码长度范围为“子网所在VPC的掩码~29”，比如VPC网段为10.0.0.0/16，掩码为16，则子网的掩码可在16~29范围内选择。 关于VPC子网规划更详细的说明，请参见**虚拟私有云和子网规划建议**。	10.0.0.0/24
子网IPv6网段	在开启IPv4/IPv6双栈的区域，显示此参数。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。 关于IPv4/IPv6双栈网络更详细的说明，请参见**IPv6网络**。	-

参数	说明	取值样例
关联路由表	路由表由一系列路由规则组成，用于控制VPC内出入子网的流量走向。创建VPC时会创建一个默认路由表，子网自动关联至默认路由表。默认路由表可以确保VPC内子网之间网络互通。 如果默认路由表无法满足使用需求，VPC创建完成后，您还可以创建自定义路由表，并将子网关联至自定义路由表，此时子网入流量仍然依据默认路由表，出流量会依据自定义路由表。关于自定义路由表更详细的说明，请参见**创建自定义路由表**。	-
高级配置 > 网关	单击 ，展开折叠的高级配置区域，可以设置该参数。 子网的网关，如果没有特殊需求，建议保持系统默认设置。	10.0.0.1
高级配置 > DNS服务器地址	单击 ，展开折叠的高级配置区域，可以设置该参数。 此处默认填写华为云的DNS服务器地址，可实现云服务器在VPC内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务。 若您由于业务原因需要指定其他DNS服务器地址，您可以修改默认的DNS服务器地址。如果您删除默认的DNS服务器地址，可能会导致您无法访问云上其他服务，请谨慎操作。 您也可以通过“DNS服务器地址”右侧的“重置”将DNS服务器地址恢复为默认值。 DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
高级配置 > 域名	单击 ，展开折叠的高级配置区域，可以设置该参数。 此处填写DNS域名后缀，支持填写多个域名，不同的域名之间以空格分隔，单个域名长度不超过63个字符，并且域名总长度不超过254个字符。 访问某个域名时，只需要输入域名前缀，子网内的云服务器会自动匹配设置的域名后缀。 域名设置完成后，子网内新创建的云服务器会自动同步该配置。 子网内的存量云服务器，需要更新DHCP配置使域名生效，您可以重启云服器、重启DHCP Client服务或者重启网络服务。 **说明** 对于不同操作系统云服务器，更新DHCP配置的命令不同，以下命令供您参考。 • 重启DHCP Client服务：**service dhcpd restart** • 重启网络服务：**service network restart**	test.com
高级配置 > DHCP租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在未开启IPv4/IPv6双栈的区域，显示该参数。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 • 期限租约：设置DHCP租约期限，单位为天或者小时。 • 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-

参数	说明	取值样例
高级配置 > IPv4 DHCP租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在开启IPv4/IPv6双栈的区域，显示该参数。 您可以设置IPv4地址的DHCP租约时间。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 ● 期限租约：设置DHCP租约期限，单位为天或者小时。 ● 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-
高级配置 > IPv6 DHCP租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在开启IPv4/IPv6双栈的区域，当“子网IPv6网段”选择“开启IPv6”时，显示该参数。 您可以设置IPv6地址的DHCP租约时间。IPv6 地址和IPv4地址的租约时间设置方法、生效情况相同。	-
高级配置 > NTP服务器地址	单击 ，展开折叠的高级配置区域，可以设置该参数。 如果您需要为当前子网新增NTP服务器地址，则需要填写该地址。此处填写的地址不会影响默认NTP服务器地址。 ● 新增或修改原有子网的NTP服务器地址后，需要子网内的ECS重新获取一次DHCP租约，或者重启ECS，才能生效。 ● 清空NTP服务器地址时，需要子网内的ECS重新获取一次DHCP租约，重启ECS无法生效。	192.168.2.1

参数	说明	取值样例
高级配置 > 标签	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以在创建子网的时候为子网绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。 关于标签更详细的说明，请参见**管理子网标签**。 **说明** 如您的组织已经设定子网的相关标签策略，则需按照标签策略规则为子网添加标签。标签如果不符合标签策略的规则，则可能会导致子网创建失败，请联系组织管理员了解标签策略详情。	• 键：subnet_key1 • 值：subnet-01
高级配置 > 描述	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以根据需要在文本框中输入对该子网的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

3. 参数设置完成后，单击“立即创建”。
   返回VPC列表，可以查看新创建的VPC。

后续操作

VPC和子网无法独立使用，您需要在VPC和子网内创建其他云资源，详细操作请参见**通过VPC快速搭建IPV4网络**和**通过VPC快速搭建IPV4/IPv6双栈网络**。

2.3.2 为虚拟私有云添加 IPv4 扩展网段

操作场景

创建虚拟私有云VPC时，您配置的IPv4网段是VPC的主网段。当VPC创建完成后，主网段不支持修改，若主网段不够分配，您可以参考以下操作为VPC添加扩展网段。

说明

如果当前区域已支持**添加IPv4扩展网段**功能，则不再支持通过控制台修改虚拟私有云网段。您可以通过API接口修改原有的VPC网段，具体请参见**更新VPC**。

约束与限制

- 创建子网时候，您可以基于主网段或者扩展网段来分配子网网段，但是一个子网网段，要么属于主网段，要么属于扩展网段，不能两个网段混用。
  同一个VPC内的子网默认互通，基于主网段的子网和基于扩展网段的子网也是默认互通。
- 扩展网段的子网地址与VPC路由表中已有路由的目的地址相同或者重叠，会导致已有路由不生效。

在扩展网段中创建子网时，系统会为该子网生成一条目的地址为子网网段，下一跳为Local的路由，Local路由属于VPC内部路由，优先级高于VPC路由表中添加的其他路由。比如，VPC路由表已有某个下一跳为对等连接的路由，其目的地址为100.20.0.0/24；新增扩展网段子网的路由，其目的地址为100.20.0.0/16，100.20.0.0/16和100.20.0.0/24网段重叠，流量优先通过扩展网段子网的路由转发，会导致对等连接的路由失效。

- VPC扩展网段支持的掩码范围为3 ~ 28。
- 表2-8中为您提供了扩展网段不支持的范围，以网段范围192.168.0.0/16~192.168.255.255/32为例，表示该网段范围内包含的所有IP地址均不支持作为扩展网段，比如192.168.0.0/16、192.168.31.0/24、192.168.100.0/24、192.168.255.255/32等。

表 2-8 不支持添加的扩展网段范围

网段类型	不支持的网段范围
私有网段预留地址	• 172.31.0.0/16~172.31.255.255/32 • 192.168.0.0/16~192.168.255.255/32 • 主网段已使用的私网网段
系统内部预留地址	• 100.64.0.0/10~100.127.255.255/32 • 214.0.0.0/7~215.255.255.255/32 • 198.18.0.0/15~198.19.255.255/32 • 169.254.0.0/16~169.254.255.255/32
公网保留地址	• 0.0.0.0/8~0.255.255.255/32 • 127.0.0.0/8~127.255.255.255/32 • 240.0.0.0/4~255.255.255.255/32

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击目标虚拟私有云所在行的操作列下的“编辑网段”。弹出“编辑网段”对话框。
5. 在“编辑网段”对话框中，单击“添加IPv4扩展网段”。
6. 输入扩展网段，单击“确定”。

2.3.3 获取虚拟私有云的 ID 信息

操作场景

本章节指导用户查看并获取虚拟私有云的ID信息，即VPC ID。

当您创建不同账户下的VPC对等连接时，需要获取对端VPC所在区域对应的项目ID，即对端项目ID。您可以将此章节推荐给对端项目ID账户的用户，以获取对端项目ID。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击需要查看VPC ID的虚拟私有云名称。
   进入虚拟私有云详情页。
5. 在基本信息区域，查看VPC ID信息。

   单击VPC ID后面 的可以复制ID信息。

图 2-27 VPC ID

2.3.4 修改虚拟私有云信息

操作场景

您可以参考以下操作修改虚拟私有云的信息，修改操作如下：

- **修改虚拟私有云名称和描述**
- **修改虚拟私有云网段**

须知

如果当前区域已支持**添加IPv4扩展网段**功能，则不再支持通过控制台修改虚拟私有云网段。您可以通过API接口修改原有的VPC网段，具体请参见**更新VPC**。

修改虚拟私有云名称和描述

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。

4. 执行以下操作，通过两种方法修改虚拟私有云名称和描述。
   - 方法一：
     i. 在虚拟私有云列表中，单击虚拟私有云名称右侧的。
     ii. 在对话框中输入虚拟私有云名称，并单击“确定”，完成修改。
   - 方法二：
     i. 在虚拟私有云列表中，单击虚拟私有云名称对应的超链接。
     进入基本信息页面。
     ii. 根据页面提示，单击名称或者描述右侧的，在对话框中输入待修改信息，并单击，完成修改。

修改虚拟私有云网段

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击目标虚拟私有云所在行的操作列下的“编辑网段”。
   弹出“编辑网段”对话框。
5. 根据界面提示，修改虚拟私有云网段信息。

须知

修改VPC网段时，您必须在VPC支持的网段范围内选择：10.0.0.0/8~24、172.16.0.0/12~24、192.168.0.0/16~24。

- 当虚拟私有云下不存在子网时，您可以修改IP地址和掩码。

  图 2-28 修改 IP 地址和掩码

- 当虚拟私有云下存在子网时，您只可以修改掩码。

图 2-29 修改掩码

6. 网段信息设置完成后，单击“确定”保存修改。

2.3.5 查看虚拟私有云拓扑图

操作场景

本章节指导用户查看VPC的拓扑图，拓扑图直观的为您展示VPC内的子网，以及子网内的弹性云服务器。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击需要查看拓扑图的VPC名称。
   进入虚拟私有云详情页。
5. 选择“拓扑图”页签，查看VPC拓扑图。
   拓扑图直观的为您展示当前VPC内的子网，以及子网内的ECS。
   您还可以通过拓扑图提供的功能，对子网和ECS执行部分常见操作，具体说明如下：
   - 修改子网、删除子网。
   - 在子网内添加新的ECS、为ECS绑定弹性公网IP、更改ECS的安全组。

2.3.6 导出虚拟私有云列表

操作场景

您可以将当前账号下拥有的所有虚拟私有云信息，以Excel文件的形式导出至本地。

该文件记录了虚拟私有云的名称、ID、状态、网段、子网个数等信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。

3. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表页面，单击列表左上方的“导出”。
   - 导出已选中数据到XLSX：勾选一个或多个虚拟私有云，导出所选虚拟私有云的信息。
   - 导出全部数据到XLSX：导出当前区域内所有虚拟私有云的信息。

   系统会将虚拟私有云信息自动导出为Excel文件，并下载至本地。

2.3.7 管理虚拟私有云标签

操作场景

标签用于标识云资源，您可以通过标签实现对虚拟私有云资源的分类和搜索。您可以参考以下操作管理虚拟私有云标签：

- 添加虚拟私有云标签
- 修改虚拟私有云标签
- 删除虚拟私有云标签

如您的组织已经设定虚拟私有云的相关标签策略，则需按照标签策略规则为虚拟私有云添加标签。标签如果不符合标签策略的规则，则可能会导致虚拟私有云创建失败，请联系组织管理员了解标签策略详情。

虚拟私有云标签规则的详细说明，请参见表2-9。

表 2-9 虚拟私有云标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	vpc_key1
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	vpc-01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击目标虚拟私有云名称超链接。
   进入虚拟私有云详情页面。
5. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
6. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击+，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的×，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

2.3.8 删除虚拟私有云的 IPv4 扩展网段

操作场景

当虚拟私有云的扩展网段不再使用时，您可以参考以下操作删除扩展网段。

- 虚拟私有云的IPv4扩展网段支持删除，主网段不支持删除。
- 当扩展网段下存在子网时，不支持删除，请删除该子网后重试。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击目标虚拟私有云所在行的操作列下的“编辑网段”。
   弹出“编辑网段”对话框。
5. 在“编辑网段”对话框中，单击IPv4扩展网段右侧的“删除”。
6. 删除完成后，单击“确定”，保存修改。

2.3.9 删除虚拟私有云

操作场景

当您的虚拟私有云不需要使用时，您可以参考以下操作删除。

须知

VPC服务下实际包含了多种产品资源，其中虚拟私有云资源可以免费使用，部分资源需要支付费用，VPC服务资源收费一览表请参见**计费说明**。

约束与限制

虚拟私有云通常由于被子网、自定义路由等资源占用而导致无法删除，需要您根据控制台的提示信息删除占用虚拟私有云的资源，然后删除虚拟私有云。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在虚拟私有云列表中，单击待删除的虚拟私有云所在行“操作”列下的“删除”。
   弹出删除确认对话框。
   如果当前虚拟私有云被其他资源占用而无法删除，您需要根据界面提示信息，逐次删除对应的资源后，重新尝试删除虚拟私有云。
5. 当虚拟私有云满足删除条件时，根据界面提示信息输入DELETE，并单击“确定”，删除虚拟私有云。

2.4 子网

2.4.1 为虚拟私有云创建新的子网

操作场景

子网是虚拟私有云内的IP地址集，可以将虚拟私有云的网段分成若干块，子网划分可以帮助您合理规划IP地址资源。虚拟私有云中的所有云资源都必须部署在子网内。

创建VPC的同时，您至少需要创建一个子网，当一个子网无法满足需求时，您可以参考以下操作为VPC创建新的子网。

约束与限制

子网创建成功后，有以下系统保留地址您不能使用。以子网网段是192.168.0.0/24为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有IP地址范围的开始，不作分配。
- 192.168.0.1：子网的网关地址。
- 192.168.0.253：系统接口，用于VPC对外通信。
- 192.168.0.254：DHCP服务地址。

- 192.168.0.255：广播地址。

以上默认地址仅为示例，系统会根据您子网的实际参数设置，分配系统保留地址。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
5. 单击“创建子网”。
   进入“创建子网”页面。
6. 根据界面提示配置子网参数。

   单击，可以依次添加多个子网，一次最多可创建3个子网。

表 2-10 子网参数说明

参数	说明	取值样例
区域	子网必须归属于某个VPC，请选择目标VPC所在的区域。	华东-上海一
虚拟私有云	请选择待创建子网的VPC。	vpc-test
子网名称	输入子网的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	subnet-01

参数	说明	取值样例
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 一个区域内有多个可用区，一个可用区发生故障后不会影响同一区域内的其它可用区。 **当页面显示“边缘可用区”时，您需要根据业务规划选择边缘可用区。不显示“边缘可用区”时，您无需设置子网可用区，不会影响实际使用。** ● 默认情况下，同一个VPC中，不同子网内的所有实例网络互通。同一个VPC内的子网可以位于不同可用区，不影响通信。比如VPC-A内有子网A01（可用区1）和子网A02（可用区2），子网A01和子网A02的网络默认互通。 ● 使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。假如可用区3发生故障，此时可用区1的云服务器可以继续使用可用区3的子网，不会影响您的业务。 关于可用区更详细的说明，请参见**区域和可用区**。	可用区1
子网网段	在未开启IPv4/IPv6双栈的区域，显示此参数。 设置子网的IPv4网段范围，参数填写说明请参见“子网IPv4网段”。	10.0.0.0/24

参数	说明	取值样例
子网IPv4网段	在开启IPv4/IPv6双栈的区域，显示此参数。 设置子网的IPv4网段范围，子网是VPC内的IP地址块，可以将VPC的网段分成若干块，建议您规划子网时，遵循以下原则： ● 子网内可用IP数量：子网创建成功后，不支持修改网段，请您结合业务所需的IP地址数量，提前合理规划好子网网段。 – 子网网段不能太小，需要确保子网内可用IP地址数量可以满足业务需求。子网网段中第一个地址和后三个地址为系统预留地址，不能供实际业务使用，比如子网（10.0.0.0/24）中，10.0.0.1为网关地址、10.0.0.253为系统接口、10.0.0.254为DHCP使用、10.0.0.255为广播地址。 – 子网网段也不能太大，以免后续扩展新的业务时，VPC内可用网段不够再创建新的子网。 ● 子网网段避免冲突：如果子网所在的VPC与其他VPC、或者VPC与云下数据中心需要通信时，则VPC子网网段和网络对端网段不能相同，否则无法正常通信。 如果网络两端的子网网段已经相同，您可以创建新的子网，请参见**为虚拟私有云创建新的子网**。 子网的网段必须在VPC网段范围内，子网网段的掩码长度范围为，子网所在VPC的掩码~29，比如VPC网段为10.0.0.0/16，掩码为16，则子网的掩码可在16~29范围内选择。 如果子网所属的VPC创建了扩展网段，您可以根据业务需要选择主网段或扩展网段作为子网所属的网段。	10.0.0.0/24
子网IPv6网段	在开启IPv4/IPv6双栈的区域，显示此参数。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。 关于IPv4/IPv6双栈网络更详细的说明，请参见**IPv6网络**。	-

参数	说明	取值样例
关联路由表	路由表由一系列路由规则组成，用于控制VPC内出入子网的流量走向。创建VPC时会创建一个默认路由表，子网自动关联至默认路由表。默认路由表可以确保VPC内子网之间网络互通。 如果默认路由表无法满足使用需求，VPC创建完成后，您还可以创建自定义路由表，并将子网关联至自定义路由表，此时子网入流量仍然依据默认路由表，出流量会依据自定义路由表。关于自定义路由表更详细的说明，请参见**创建自定义路由表**。	-
高级配置 > 网关	单击 ，展开折叠的高级配置区域，可以设置该参数。 子网的网关，如果没有特殊需求，建议保持系统默认设置。	10.0.0.1
高级配置 > DNS服务器地址	单击 ，展开折叠的高级配置区域，可以设置该参数。 此处默认填写华为云的DNS服务器地址，可实现云服务器在VPC内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务。 若您由于业务原因需要指定其他DNS服务器地址，您可以修改默认的DNS服务器地址。如果您删除默认的DNS服务器地址，可能会导致您无法访问云上其他服务，请谨慎操作。 您也可以通过“DNS服务器地址”右侧的“重置”将DNS服务器地址恢复为默认值。 DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
高级配置 > 域名	单击 ，展开折叠的高级配置区域，可以设置该参数。 此处填写DNS域名后缀，支持填写多个域名，不同的域名之间以空格分隔，单个域名长度不超过63个字符，并且域名总长度不超过254个字符。 访问某个域名时，只需要输入域名前缀，子网内的云服务器会自动匹配设置的域名后缀。 域名设置完成后，子网内新创建的云服务器会自动同步该配置。 子网内的存量云服务器，需要更新DHCP配置使域名生效，您可以重启云服器、重启DHCP Client服务或者重启网络服务。 **说明** 对于不同操作系统云服务器，更新DHCP配置的命令不同，以下命令供您参考。 ● 重启DHCP Client服务：**service dhcpd restart** ● 重启网络服务：**service network restart**	test.com
高级配置 > NTP服务器地址	单击 ，展开折叠的高级配置区域，可以设置该参数。 如果您需要为当前子网新增NTP服务器地址，则需要填写该地址。此处填写的地址不会影响默认NTP服务器地址。 ● 新增或修改原有子网的NTP服务器地址后，需要子网内的ECS重新获取一次DHCP租约，或者重启ECS，才能生效。 ● 清空NTP服务器地址时，需要子网内的ECS重新获取一次DHCP租约，重启ECS无法生效。	192.168.2.1

参数	说明	取值样例
高级配置 > DHCP租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在未开启IPv4/IPv6双栈的区域，显示该参数。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 ● 期限租约：设置DHCP租约期限，单位为天或者小时。 ● 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-
高级配置 > IPv4 DHCP租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在开启IPv4/IPv6双栈的区域，显示该参数。 您可以设置IPv4地址的DHCP租约时间。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 ● 期限租约：设置DHCP租约期限，单位为天或者小时。 ● 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-

参数	说明	取值样例
高级配置 > IPv6 DHCP 租约时间	单击 ，展开折叠的高级配置区域，可以设置该参数。 在开启IPv4/IPv6双栈的区域，当“子网IPv6网段”选择“开启IPv6”时，显示该参数。 您可以设置IPv6地址的DHCP租约时间。IPv6地址和IPv4地址的租约时间设置方法、生效情况相同。	-
高级配置 > 标签	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以在创建子网的时候为子网绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。 关于标签更详细的说明，请参见**管理子网标签**。 **说明** 如您的组织已经设定子网的相关标签策略，则需按照标签策略规则为子网添加标签。标签如果不符合标签策略的规则，则可能会导致子网创建失败，请联系组织管理员了解标签策略详情。	• 键：subnet_key1 • 值：subnet-01
高级配置 > 描述	单击 ，展开折叠的高级配置区域，可以设置该参数。 您可以根据需要在文本框中输入对该子网的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 参数设置完成后，单击“立即创建”。
   返回子网列表，可以查看新创建的子网。

2.4.2 修改子网信息

操作场景

本章节指导用户修改子网名称、DNS服务器地址、NTP服务器地址等。

约束与限制

子网创建完成后，可用区不支持修改。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。

进入虚拟私有云列表页面。

4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击待修改的子网名称超链接。
   进入子网详情页面。
6. 在子网的“基本信息”页签中，单击待修改参数右侧的 ，根据界面提示修改参数。

表 2-11 参数说明

参数	说明	取值样例
名称	子网的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	Subnet
DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。最多支持2个IP地址，多个IP地址以英文逗号隔开。 此处默认填写华为云的DNS服务器地址，可实现云服务器在VPC内直接通过内网域名互相访问。同时，还支持不经公网，直接通过内网DNS访问云上服务。 若您由于业务原因需要指定其他DNS服务器地址，您可以修改默认的DNS服务器地址。如果您删除默认的DNS服务器地址，可能会导致您无法访问云上其他服务，请谨慎操作。 您也可以通过“DNS服务器地址”右侧的“重置”将DNS服务器地址恢复为默认值。 DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
域名	此处填写DNS域名后缀，支持填写多个域名，不同的域名之间以空格分隔，单个域名长度不超过63个字符，并且域名总长度不超过254个字符。 访问某个域名时，只需要输入域名前缀，子网内的云服务器会自动匹配设置的域名后缀。 域名设置完成后，子网内新创建的云服务器会自动同步该配置。 子网内的存量云服务器，需要更新DHCP配置使域名生效，您可以重启云服器、重启DHCP Client服务或者重启网络服务。 **说明** 对于不同操作系统云服务器，更新DHCP配置的命令不同，以下命令供您参考。 • 重启DHCP Client服务：**service dhcpd restart** • 重启网络服务：**service network restart**	test.com
DHCP租约时间	在未开启IPv4/IPv6双栈的区域，显示该参数。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 • 期限租约：设置DHCP租约期限，单位为天或者小时。 • 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-

参数	说明	取值样例
IPv4 DHCP租约时间	在开启IPv4/IPv6双栈的区域，显示该参数。 您可以设置IPv4地址的DHCP租约时间。 DHCP租约时间是指DHCP服务器自动分配给客户端的IP地址的使用期限。超过租约时间，IP地址将被收回，需要重新分配。 ● 期限租约：设置DHCP租约期限，单位为天或者小时。 ● 无限租约：设置DHCP不过期。 DHCP租约时间修改后，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效。实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。如果需要DHCP租约立即生效，请在实例中手动更新租约或者重启实例。 详细信息请参见**修改子网的DHCP租约时间如何立即生效**。	-
IPv6 DHCP租约时间	在开启IPv4/IPv6双栈的区域，当“子网IPv6网段”选择“开启IPv6”时，显示该参数。 您可以设置IPv6地址的DHCP租约时间。IPv6 地址和IPv4地址的租约时间设置方法、生效情况相同。	-
NTP服务器地址	NTP时间服务器IP地址，非必填项。 您可以根据需要为子网新增NTP服务器IP地址，该地址不会影响默认NTP服务器地址。该地址为空，表示不新增NTP服务器IP地址。 最多允许输入4个格式正确且不重复的IP地址，多个IP地址请用半角逗号隔开。新增或修改原有子网的NTP服务器地址后，需要子网内的ECS重新获取一次DHCP租约，或者重启ECS，才能生效。清空NTP服务器地址时，需要子网内的ECS重新获取一次DHCP租约，重启ECS无法生效。	192.168.2.1
描述	子网的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

2.4.3 导出子网列表

操作场景

您可以将当前账号下拥有的所有虚拟私有云子网信息，以Excel文件的形式导出至本地。该文件记录了子网的名称、ID、所属VPC、网段、关联路由表等信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表页面，单击列表左上方的“导出”。
   - 导出已选中数据到XLSX：勾选一个或多个子网，导出所选子网的信息。
   - 导出全部数据到XLSX：导出当前区域内所有子网的信息。

   系统会将子网信息自动导出为Excel文件，并下载至本地。

2.4.4 查看并删除子网内的云服务资源

操作场景

云服务实例的私有IP地址需要从VPC子网内分配，本章节指导用户查看占用子网的云服务资源，如果这些云服务器资源您不再使用，可以删除。

当前支持查看的云服务资源包括弹性云服务器ECS、裸金属服务器、弹性网卡、弹性负载均衡ELB、NAT网关。

须知

如果您执行本章节操作后，发现子网内没有云服务资源，但是删除子网时，仍提示“子网正在使用中，不能删除”，则请您进一步查看占用子网的私有IP地址，具体请参见**查看子网内IP地址的用途**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。

5. 在子网列表中，找到目标子网，并单击子网名称超链接。
   进入子网详情页面。
6. 在“基本信息”页签，查看占用子网的云服务资源。
   a. 在页面下方的资源概览区域，查看占用子网的各资源的数量。单击资源数量超链接，查看占用子网的资源。
   b. 在页面右侧的网络互通概览区域，查看占用子网的NAT网关。
7. 执行以下操作，删除子网内的云服务资源。

表 2-12 删除子网内的云服务资源

云服务资源类型	操作指导
弹性云服务器	当前不支持通过子网页面直接跳转到目标弹性云服务器，您需要在弹性云服务器列表中，查找目标云服务器并删除。 1. 在弹性云服务器列表中，单击名称超链接。 进入弹性云服务器详情页面。 2. 在详情页面的“网卡”区域，查看弹性云服务器关联的子网名称。 3. 确认无误后，**删除弹性云服务器**。
裸金属服务器	当前不支持通过子网页面直接跳转到目标裸金属服务器，您需要在裸金属服务器列表中，查找目标云服务器并删除。 1. 在裸金属服务器列表中，单击名称超链接。 进入裸金属服务器详情页面。 2. 在详情页面的“网卡”页签，查看裸金属服务器关联的子网名称。 3. 确认无误后，**释放裸金属服务器**。
弹性负载均衡	当前支持通过子网页面直接跳转到目标弹性负载均衡： 1. 根据界面提示，单击弹性负载均衡区域的数量超链接。 进入弹性负载均衡列表页面。 2. 确认释放资源后，单击弹性负载均衡所在行的操作列下的“删除”。 详细操作，请参见**删除负载均衡器**。
弹性网卡	当前支持通过子网页面直接跳转到目标弹性网卡： 1. 根据界面提示，单击弹性网卡区域的数量超链接。 进入弹性网卡列表页面。 2. 确认释放资源后，选择弹性网卡所在行的操作列下的“更多 > 删除”。 详细操作，请参见**删除弹性网卡**。

云服务资源类型	操作指导
NAT网关	当前支持通过子网页面直接跳转到目标NAT网关： 1. 根据界面提示，单击NAT网关区域的名称超链接。进入NAT网关资源详情页面。 2. 单击  ，返回NAT网关列表。 3. 确认释放资源后，选择NAT网关所在行的操作列下的“更多 > 删除”。 ● 公网NAT网关：请参见**删除/退订公网NAT网关**。 ● 私网NAT网关：请参见**删除私网NAT网关**。

2.4.5 查看子网内 IP 地址的用途

操作场景

子网是VPC内划分的一个地址块，包含若干个IP地址，本章节指导用户查看子网内已被占用的IP地址用途，具体如下：

- 虚拟IP地址
- 私有IP地址：用作其他资源的私有IP地址。
  - 子网自身占用，比如网关、系统接口、DHCP等。
  - 分配给云服务资源，比如弹性云服务器ECS、弹性负载均衡ELB、云数据库RDS等。

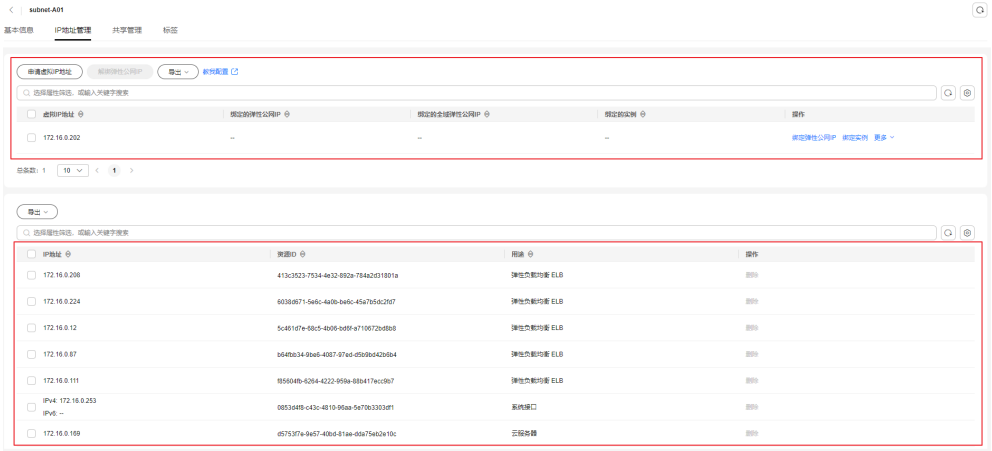
约束与限制

- 子网中存在虚拟IP、分配给云服务资源的IP地址时，子网无法删除。
- 子网自身占用的IP地址，不影响删除子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击  ，选择区域和项目。
3. 在页面左上角单击  图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，找到目标子网，并单击子网名称超链接。
   进入子网详情页面。
6. 选择“IP地址管理”页签，查看子网内的IP地址信息。
   a. 在页面上方的虚拟IP地址列表中，可以查看子网内分配的虚拟IP地址。
   b. 在页面下方的私有IP列表中，可以查看占用子网的私有IP地址、用途及占用子网的资源ID。

图 2-30 查看子网内的 IP 地址



后续操作

如果您需要查看并删除占用子网的资源，请参见**删除提示信息详细说明**。

2.4.6 管理子网标签

应用场景

标签用于标识云资源，您可以通过标签实现对子网资源的分类和搜索。您可以参考以下操作管理子网标签：

- 添加子网标签
- 修改子网标签
- 删除子网标签

如您的组织已经设定子网的相关标签策略，则需按照标签策略规则为子网添加标签。标签如果不符合标签策略的规则，则可能会导致子网创建失败，请联系组织管理员了解标签策略详情。

子网标签规则的详细说明，请参见**表2-13**所示。

表 2-13 子网标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	subnet_key1

参数	规则	样例
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	subnet-01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击目标子网名称超链接。
   进入子网详情页面。
6. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
7. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击+，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的×，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

2.4.7 删除子网

操作场景

如果您的子网不需要使用，您可以参考以下操作删除子网。

须知

VPC服务下实际包含了多种产品资源，其中子网资源可以免费使用，部分资源需要支付费用，VPC服务资源收费一览表请参见**计费说明**。

约束与限制

子网通常由于被自定义路由、虚拟IP或者其他服务资源(ECS、ELB、NAT网关)占用而导致无法删除，需要您根据控制台的提示信息删除占用子网的资源，然后删除子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击待删除子网所在行的操作列下的“删除”。
   弹出删除确认对话框。
   如果当前子网被其他资源占用而无法删除，您需要根据界面提示信息，逐次删除对应的资源后，重新尝试删除子网。
6. 当子网满足删除条件时，根据界面提示信息输入DELETE，并单击“确定”，删除子网。

3 路由表和路由

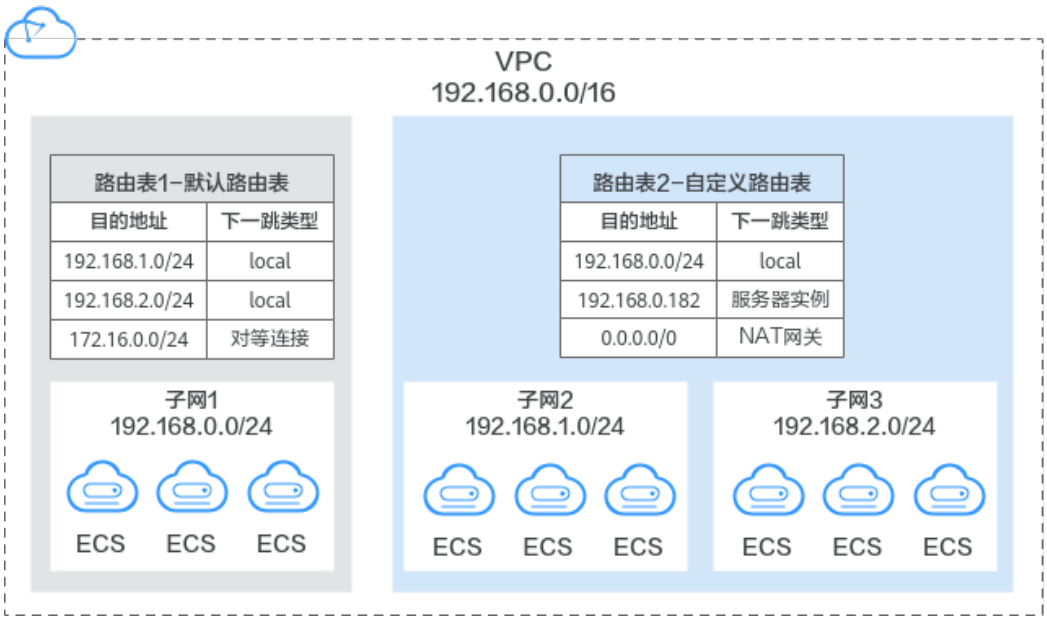
3.1 路由表和路由概述

路由表

路由表由一系列路由规则组成，用于控制VPC内出入子网的流量走向。VPC中的每个子网都必须关联一个路由表，一个子网只能关联一个路由表，但一个路由表可以同时关联至多个子网。

路由表支持添加IPv4和IPv6路由。

图 3-1 路由表



- 默认路由表：用户创建VPC时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。默认路由表可以确保VPC内，不同子网的内网网络互通。

  - 您可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。
  - 创建VPN、云专线、云连接服务时，默认路由表会自动下发路由，该路由不能删除和修改。
- 自定义路由表：您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。

  子网关联自定义路由表仅影响子网的出流量走向，入流量仍然匹配子网所在VPC的默认路由表。

说明

默认情况下，您没有创建自定义路由表的配额，因此创建自定义路由表时，请您根据界面提示“申请扩大配额”，具体请参见**申请扩大配额**。

路由

您可以在默认路由表和自定义路由表中添加路由，路由包括目的地址、下一跳类型、下一跳地址等信息，可以决定网络流量的走向。路由分为系统路由和自定义路由。

- 系统路由：系统路由一般为VPC服务或者其他服务（比如VPN、DC等）自动在路由表添加的路由，无法删除或修改。

  创建路由表时，VPC服务会自动在路由表中添加下一跳为Local的路由，通常情况下，路由表中有以下Local的路由：
  - 目的地址是100.64.0.0/10，该路由用于子网内实例访问云上公共服务，比如访问DNS服务器等。
  - 目的地址是198.19.128.0/20，表示系统内部服务使用的网段地址，比如VPCEP等服务。
  - 目的地址是127.0.0.0/8，表示本地回环地址。
  - 目的地址是子网网段，该路由用于当前VPC内，不同子网的内网网络互通。

    您在创建子网时，开启IPv6功能，系统将自动为当前子网分配IPv6网段，就可以在路由表中看到IPv6路由。子网网段目的地址示例如下：
    - IPv4地址：192.168.2.0/24。
    - IPv6地址：2407:c080:802:be7::/64。
- 自定义路由：路由表创建完成后，您可以添加自定义路由来控制网络流量的走向，需要指定路由的目的地址和下一跳等信息。除了手动添加自定义路由，当您使用其他云服务时（比如云容器引擎CCE或者NAT网关），其他服务会自动在VPC路由表中添加自定义路由。

  路由表包括默认路由表和自定义路由表，不同路由表中支持添加自定义路由的下一跳类型有差异，详情请参见**表3-1**和**表3-2**。相比自定义路由表，默认路由表支持添加自定义路由的下一跳类型较少，是由于部分服务（比如VPN、云专线、云连接等）会自动在默认路由表中添加路由，无需您手动在默认路由表中添加自定义路由。

表 3-1 默认路由表支持的下一跳类型

下一跳类型	说明
服务器实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。
辅助弹性网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的辅助弹性网卡。
NAT网关	将指向目的地址的流量转发到一个NAT网关。
对等连接	将指向目的地址的流量转发到一个对等连接。
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。
VPC终端节点	将指向目的地址的流量转发到一个VPC终端节点。
云容器引擎	将指向目的地址的流量转发到一个云容器引擎的节点。
企业路由器	将指向目的地址的流量转发到一个企业路由器。
云防火墙	将指向目的地址的流量转发到一个云防火墙。
全域互联网网关	将指向目的地址的流量转发到一个全域互联网网关。

表 3-2 自定义路由表支持下一跳类型

下一跳类型	说明
服务器实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。
裸金属服务器自定义网络	将指向目的地址的流量转发到一个裸金属服务器自定义网络。
VPN网关	将指向目的地址的流量转发到一个VPN网关。
云专线网关	将指向目的地址的流量转发到一个云专线网关。
云连接	将指向目的地址的流量转发到云连接。
辅助弹性网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的辅助弹性网卡。
NAT网关	将指向目的地址的流量转发到一个NAT网关。
对等连接	将指向目的地址的流量转发到一个对等连接。

下一跳类型	说明
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。
VPC终端节点	将指向目的地址的流量转发到一个VPC终端节点。
云容器引擎	将指向目的地址的流量转发到一个云容器引擎的节点。
企业路由器	将指向目的地址的流量转发到一个企业路由器。
云防火墙	将指向目的地址的流量转发到一个云防火墙。
全域互联网网关	将指向目的地址的流量转发到一个全域互联网网关。

说明

个别由系统下发的路由可供用户修改和删除，这取决于创建对端服务时是否已设置目的地址。

例如，创建NAT网关时，系统会自动下发一条自定义类型的路由，没有明确指定目的地址（默认为0.0.0.0/0）,此时用户可修改该目的地址。而创建VPN网关时，可以指定远端子网，也就是路由的目的地址，系统将下发系统类型的路由。如果在路由表页面更改路由将会导致与对端数据不一致，您可以前往对端服务页面修改远端子网来调整路由表中的路由规则。

不支持手动在VPC路由表中添加下一跳类型为“VPC终端节点”或者“云容器引擎”的路由，通常您在配置VPC终端节点或者云容器引擎服务时，由该服务自动添加在VPC路由表中。

路由表和路由的使用限制

当您创建VPC时，系统会同步为VPC创建一个默认路由表。除此之外，您还可以创建自定义路由表。

- 在一个VPC内，最多可关联5个路由表，包括1个默认路由表和4个自定义路由表。
- 在一个VPC内的所有路由表中，最多可容纳1000条路由。系统自动创建的路由，即类型为“系统”的路由不占用该配额。

在VPC路由表中，存在系统添加的Local路由以及自定义路由。

- 通常情况下，自定义路由的目的地址不能与系统添加的Local路由的目的地址重叠。Local路由的目的地址一般有子网网段地址，以及系统内部通信的网段地址。
- 您无法在VPC路由表中添加目的地址相同的两条自定义路由，即使路由的下一跳类型不同也不行。
- 在VPC路由表中，路由的优先级说明请参见**表3-3**。

表 3-3 VPC 路由优先级说明

路由优先级	说明
Local路由最优先匹配	Local路由用于VPC内通信的系统默认路由，优先级最高。

路由优先级	说明
最精确路由优先匹配	除去Local路由，当路由表中同时有多条路由规则可以匹配目的IP 地址时，此时遵循最长匹配原则，即优先采用掩码最长，最精确匹配的一条路由并确定下一跳。 示例： ● 流量的目的地址为192.168.1.12/32。 ● 路由A的目的地址为192.168.0.0/16，下一跳为ECS-A。 ● 路由B的目的地址为192.168.1.0/24，下一跳为对等连接。 则根据最长匹配原则，该流量和路由B的目的地址匹配度更高，将去往对等连接。
弹性公网IP（EIP）优先级高于默认路由	当路由表中存在默认路由（默认路由目的地址为0.0.0.0/0，表示匹配任何流量），并且子网内的ECS关联了EIP，则EIP的优先级高于默认路由，流量将会通过EIP访问公网。 示例： ● 路由A的目的地址为0.0.0.0/0，下一跳为NAT网关。 ● VPC子网内的ECS关联了EIP。 则ECS出方向的流量将去往公网，不会去往NAT网关。

图 3-2 VPC 路由表

自定义路由表配置流程

图 3-3 自定义路由表配置流程

表 3-4 自定义路由表配置流程说明

序号	步骤	说明	操作指导
1	创建自定义路由表	当默认路由表无法满足您的使用需求时，您可以创建自定义路由表。 子网关联自定义路由表仅影响子网的出流量走向，入流量仍然匹配子网所在VPC的默认路由表。	创建自定义路由表
2	添加自定义路由	您可以通过添加自定义路由来控制网络流量的走向，您需要指定路由的目的地址和下一跳等信息。	在路由表中添加路由
3	将路由表关联至子网	路由表和子网关联后，该路由表的路由规则将对该子网生效，子网下的云资源将启用新的路由规则。	将路由表关联至子网

3.2 管理路由表

3.2.1 创建自定义路由表

操作场景

创建虚拟私有云时，会同步为虚拟私有云创建一个默认路由表。当默认路由表无法满足您的使用要求时，您可参考以下操作创建自定义路由表，并将自定义路由表关联至子网，则子网流量走向会依据新的路由表。

约束与限制

默认情况下，您没有创建自定义路由表的配额，因此创建自定义路由表时，请您根据界面提示“申请扩大配额”，具体请参见**申请扩大配额**。

操作步骤

1. 进入**路由表列表页面**。
2. 在页面右上角，单击“创建路由表”，按照提示配置参数。

表 3-5 参数说明

参数	说明	取值样例
路由表名称	必选参数。 输入路由表的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	rtb-001

参数	说明	取值样例
所属VPC	必选参数。 选择路由表归属的VPC，即该路由表可以关联至所选VPC的子网。	vpc-001
描述	可选参数。 您可以根据需要在文本框中输入对该路由表的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
添加路由	可选参数。 路由规则可以在此处添加，也可以在路由表创建完成后，参考**在路由表中添加路由**添加。 单击⊕，可以依次增加多条路由。	-

3. 单击“确定”，完成创建。

   系统出现信息提示页面，您可根据提示选择是否立即关联子网。若您想要立即关联子网，请参考以下步骤进行关联：

   a. 单击“关联子网”，进入路由表详情页面的“关联子网”页签。
   b. 单击“关联子网”，选择需要关联的子网。
   c. 单击“确定”，完成关联。

3.2.2 将路由表关联至子网

操作场景

子网创建完成后，系统会将子网关联至VPC默认路由表。如果您需要为子网使用特定路由，则可以参考以下操作将子网关联至自定义路由表。

如果将子网关联至自定义路由表，那么自定义路由表仅影响子网的出流量走向，入流量仍然匹配默认路由表。

须知

路由表和子网关联后，该路由表的路由规则将对该子网生效，子网下的云资源将启用新的路由规则，请确认对业务造成的影响，谨慎操作。

约束与限制

- 子网必须关联路由表，一个子网只能关联一个路由表。
- 一个路由表可以同时关联多个子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，单击操作列的“关联子网”。
6. 选择需要关联的子网。
7. 单击“确定”，完成关联。

3.2.3 更换子网关联的路由表

操作场景

更换子网已经关联的路由表为该VPC下其他的路由表。更换路由表后，子网下云资源将启用新路由表规则，请确认对业务造成的影响。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
5. 在路由表列表中，单击路由表名称。
6. 在关联子网页签下，单击操作列的“更换路由表”，根据提示，选择新的路由表。
7. 单击“确定”，完成更换。
   更换路由表后，子网下资源将启用新路由表的路由规则。

3.2.4 查看子网关联的路由表

操作场景

您可以参考以下操作查看子网关联的路由表以及路由信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。

4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，找到目标子网，并单击子网名称超链接。
   进入子网详情页面。
6. 在子网详情页面右侧区域，查看子网关联的路由表。
7. 单击路由表名称超链接。
   进入路由表详情页面，您可以进一步查看路由信息。

3.2.5 查看路由表信息

操作场景

您可以参考以下操作，查看路由表的详细信息，主要信息如下：

- 基本信息：路由表的名称，类型（分为默认路由表和自定义路由）、ID等。
- 路由列表：路由表中包含的路由信息，包括路由目的地址、下一跳、路由类型（分为系统和自定义）等。
- 关联子网：路由表所关联的子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，单击路由表的名称超链接。
   进入路由表详情页面。
   a. 在“基本信息”页签下，查看路由表的基本信息和路由列表。
   b. 在“关联子网”页签下，查看路由表关联的子网。

3.2.6 删除路由表

操作场景

当您的自定义路由表不需要使用时，您可以参考以下操作删除自定义路由表。

约束与限制

- 默认路由表无法删除。
  默认路由表和自定义路由表均不收取任何费用，当您删除虚拟私有云的的时候，会一并删除默认路由表。
- 当自定义路由表被关联至子网时，则无法删除。
  请先通过**更换子网关联的路由表**将子网关联到其他的路由表，然后尝试删除。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，单击目标路由表所在行的操作列下的“删除”。
   弹出删除确认对话框。
6. 根据界面提示完成信息确认后，单击“确定”，删除自定义路由表。

3.3 管理路由

3.3.1 在路由表中添加路由

操作场景

每个路由表会自带系统默认路由，用来控制子网内实例访问云上公共服务，或者VPC内不同子网的内网通信。除了系统默认路由，您可以根据需要添加自定义路由，控制子网的流量走向。

当您的路由表已关联子网时，添加路由会影响子网的网络流量走向，请您谨慎评估后再执行操作，避免对业务造成影响。

约束与限制

- 通常情况下，自定义路由的目的地址不能与系统添加的Local路由的目的地址重叠。Local路由的目的地址一般有子网网段地址，以及系统内部通信的网段地址。
- 您无法在VPC路由表中添加目的地址相同的两条自定义路由，即使路由的下一跳类型不同也不行。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，找到目标路由表，并单击路由表名称超链接。
   进入路由表详情页面。
6. 单击“添加路由”，按照提示配置参数。
   单击，可以依次增加多条路由。

表 3-6 参数说明

参数	说明	取值样例
目的地址类型	必选参数。 目的地址类型支持“IP地址”，表示可以填写单个IP地址或者IP网段。	IP地址
目的地址	必选参数。 此处输入路由的目的地址，支持单个IP地址或者IP网段，格式为“IP地址/掩码”。 **须知** 如果IP地址中存在“起始IP-末尾IP”形式的网段，则不支持。 不支持IP地址示例：192.168.0.1-192.168.0.62，请修改成IP网段/掩码的形式，比如192.168.0.0/26。	IPv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。 **说明** 当为默认路由表添加或修改自定义路由时，下一跳类型不支持选择VPN网关、云专线网关以及云连接。	对等连接
下一跳	必选参数。 选择下一跳资源。下拉列表包含资源将基于您所选的资源类型进行展示。	peer-AB
描述	可选参数。 您可以根据需要在文本框中输入路由的描述信息。	-

7. 参数设置完成后，单击“确定”，完成添加。
   返回路由列表，可以看到刚添加的路由信息。

3.3.2 修改路由

操作场景

您可以参考以下操作，修改VPC路由表中已有的路由。

当您的路由表已关联子网时，修改路由会影响子网的网络流量走向，请您谨慎评估后再执行操作，避免对业务造成影响。

约束与限制

- 系统自动创建的路由不支持修改，即类型为“系统”的路由不支持修改。
- 创建VPN、云专线、云连接服务时，默认路由表会自动下发路由，该路由不能删除和修改。
- 云容器引擎类型的路由不支持修改和删除。

- VPC终端节点类型的路由不支持修改和删除。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，找到目标路由表，并单击路由表名称超链接。
   进入路由表详情页面。
6. 在路由列表中，单击目标路由所在行的操作列下的“修改”。
7. 根据弹出框提示，修改路由规则。

表 3-7 参数说明

参数	说明	取值样例
目的地址类型	必选参数。 目的地址类型支持“IP地址”，表示可以填写单个IP地址或者IP网段。	IP地址
目的地址	必选参数。 此处输入路由的目的地址，支持单个IP地址或者IP网段，格式为“IP地址/掩码”。 **须知** 如果IP地址中存在“起始IP-末尾IP”形式的网段，则不支持。 不支持IP地址示例：192.168.0.1-192.168.0.62，请修改成IP网段/掩码的形式，比如192.168.0.0/26。	IPv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。 **说明** 当为默认路由表添加或修改自定义路由时，下一跳类型不支持选择VPN网关、云专线网关以及云连接。	对等连接
下一跳	必选参数。 选择下一跳资源。下拉列表包含资源将基于您所选的资源类型进行展示。	peer-AB
描述	可选参数。 您可以根据需要在文本框中输入路由的描述信息。	-

8. 参数设置完成后，单击“确定”，完成修改。

3.3.3 将其他路由表中的路由复制到当前路由表

操作场景

您可以参考以下操作，在一个VPC内的所有路由表之间互相复制路由信息，实现快速添加路由。支持在默认路由表和自定义路由表之间互相复制路由信息。

约束与限制

不同类型的路由是否支持复制的情况不同，具体请参见表3-8。

例如，当路由下一跳类型为服务器实例时，支持复制该路由到默认路由表或自定义路由表。

例如，当路由下一跳类型为云专线网关时，无法复制该路由到默认路由表，仅支持复制到自定义路由表。

表 3-8 路由复制情况说明

下一跳类型	是否支持复制到默认路由表	是否支持复制到自定义路由表
Local	否	否
服务器实例	是	是
扩展网卡	是	是
裸金属服务器自定义网络	否	是
VPN网关	否	是
云专线网关	否	是
云连接	否	是
辅助弹性网卡	是	是
NAT网关	是	是
对等连接	是	是
虚拟IP	是	是
VPC终端节点	否	否
云容器引擎	否	否
企业路由器	是	是
云防火墙	是	是

说明

- 当为手工开通方式的云专线时，不支持将下发至默认路由表中的路由复制到自定义路由表。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，找到目标路由表，并单击路由表名称超链接。
   进入路由表详情页面。
6. 单击“复制路由”，并根据界面提示，选择目标路由表和需要复制的路由。
7. 单击“确定”，完成路由复制。

3.3.4 删除路由

操作场景

您可以参考以下操作，删除VPC路由表中的自定义路由，即类型为“自定义”的路由。

当您的路由表已关联子网时，删除路由会影响子网的网络流量走向，请您谨慎评估后再执行操作，避免对业务造成影响。

约束与限制

- 系统自动创建的路由不支持删除，即类型为“系统”的路由不支持删除。

  图 3-4 系统路由

- 由VPN、云专线、云连接服务自动下发到VPC默认表的中的路由不能删除，路由的下一条类型分别如下：
  - VPN：VPN网关
  - 云专线：云专线网关
  - 云连接：云连接

  如果您要删除以上路由，则需要删除路由对应的网络实例。

- 云容器引擎类型的路由不支持修改和删除。
- VPC终端节点类型的路由不支持修改和删除。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表中，找到目标路由表，并单击路由表名称超链接。
   进入路由表详情页面。

   图 3-5 查看自定义路

6. 在路由列表中，找到需要删除的路由，单击目标路由所在行的操作列下的“删除”。
   弹出删除确认对话框。
7. 根据界面提示完成信息确认后，单击“确定”，删除自定义路由。

3.4 路由配置示例

3.4.1 基于 ECS 自建 SNAT 服务器实现多个 ECS 共享 EIP 访问公网

操作场景

当您在使用VPC的路由表功能时，需要在弹性云服务器上部署SNAT，使得VPC内其他没有绑定EIP的弹性云服务器可以通过它访问Internet。

该配置对VPC内所有子网生效。

前提条件

- 已拥有需要部署SNAT的弹性云服务器。
- 待部署SNAT的弹性云服务器操作系统为Linux操作系统。
- 待部署SNAT的弹性云服务器网卡已配置为单网卡。

SNAT 服务器与 NAT 网关服务差异

NAT网关（NAT Gateway）能够为虚拟私有云内的云主机（弹性云服务器、裸金属服务器等）或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供网络地址转换服务，使多个云主机可以共享弹性IP弹性公网IP访问Internet或使云主机提供互联网服务。

对比SNAT服务器实例，NAT网关具有配置简单、灵活易用、支持跨子网部署、跨可用区部署、支持多种网关规格等优势，您可以在管理控制台选择“网络网络 > NAT网关”进行体验。

更多内容请参见**《NAT网关用户指南》**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“计算 > 弹性云服务器”。
4. 在右侧弹性云服务器界面，单击需要设置SNAT的弹性云服务器名称，进入弹性云服务器详情页面。
5. 在弹性云服务器详情页面单击“弹性网卡”页签。
6. 单击网卡IP地址，在展开的网卡详情区域内设置“源/目的检查”状态为“关闭”。

   默认情况下，“源/目的检查”状态为“启用”，系统会检查弹性云服务器发送的报文中源IP地址是否正确，否则不允许弹性云服务器发送该报文。这有助于防止伪装报文攻击，提升安全性。但在SNAT场景中，SNAT实例起转发作用，这种保护机制会导致报文的发送者无法接收到返回的报文。这种保护机制可以通过设置“源/目的检查”状态为禁用。
7. 绑定EIP。
   - 为弹性云服务器的私有IP绑定EIP。详情请参见**将弹性公网IP绑定至实例**。
   - 为弹性云服务器的虚拟IP绑定EIP，详情请参见**将虚拟IP绑定至实例或者EIP**。
8. 打开待配置SNAT弹性云服务器详情页面，通过remote login登录服务器。
9. 执行如下命令，输入root密码，切换至root。

   su - root
10. 执行如下命令，检测弹性云服务器是否可以正常连接Internet。

    说明

    执行如下命令前，关闭SNAT服务器上相应的IPtables 规则，开放安全组规则。

    ping support.huawei.com

    回显如下所示，表示弹性云服务器可以正常连接Internet。

    ```
    [root@localhost ~]# ping support.huawei.com
    PING support.huawei.com (xxx.xxx.xxx.xxx) 56(84) bytes of data.
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
    64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
    ```
11. 执行如下命令，查看Linux操作系统的IP转发功能是否已开启。

    cat /proc/sys/net/ipv4/ip_forward

    回显结果：1为开启，0为关闭，默认为0。

- 是，执行14。
- 否，执行12，开启Linux的IP转发功能。

许多操作系统支持路由报文。操作系统需要在转发报文前将报文的源IP地址转换成操作系统的IP地址，因此，发送的报文带有公共发送者的IP地址，而返回的报文能够原路返回，这种方式称为SNAT。操作系统需要跟踪转换过IP地址的报文，确保返回的报文中目的IP地址可以被重写，且报文能够转发给原始的报文发送者。这一过程实现需要启用IP转发功能，并设置SNAT规则。

12. 使用vi打开“/etc/sysctl.conf”文件，修改net.ipv4.ip_forward = 1，按“**:wq**”保存退出。
13. 执行如下命令，使修改生效。

    sysctl -p /etc/sysctl.conf
14. 配置SNAT。

    执行如下命令，允许网段（例如：192.168.1.0/24）内所有ECS访问外网。示例如图3-6所示。

    iptables -t nat -A POSTROUTING -o eth0 -s subnet -j SNAT --to nat-instance-ip

    图 3-6 配置 SNAT

    ```
    [root@host-192-168-1-4 ~]# vi /etc/sysctl.conf^C
    [root@host-192-168-1-4 ~]# ^C
    [root@host-192-168-1-4 ~]# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0
    /24 -j SNAT --to 192.168.1.4
    ```

    说明

    如需实现重启后规则不丢失，则需把规则写在/etc/rc.local文件中。

    1. 执行以下命令进入/etc/rc.local文件。

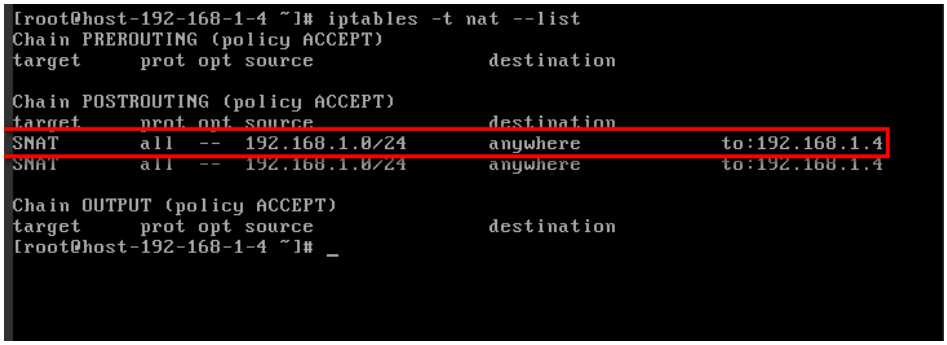
       vi /etc/rc.local
    2. 执行14配置SNAT
    3. 执行以下命令保存并退出。

       :wq
    4. 执行以下命令添加rc.local文件的执行权限。

       # chmod +x /etc/rc.local
15. 执行如下命令，查看是否配置成功。如图3-7所示，则表示配置成功（例如：192.168.1.0/24）。

    iptables -t nat --list

图 3-7 验证设置



16. 添加自定义路由，详见**在路由表中添加路由**。

    目的地址是0.0.0.0/0，下一跳地址是SNAT服务器的私有IP或者虚拟IP（例如：192.168.1.4）。

按以上操作完成配置后，如果出现网络不通等情况，请检查您的安全组、网络ACL配置，是否放通了对应流量。

4 虚拟 IP 地址

4.1 虚拟 IP 地址概述

虚拟 IP

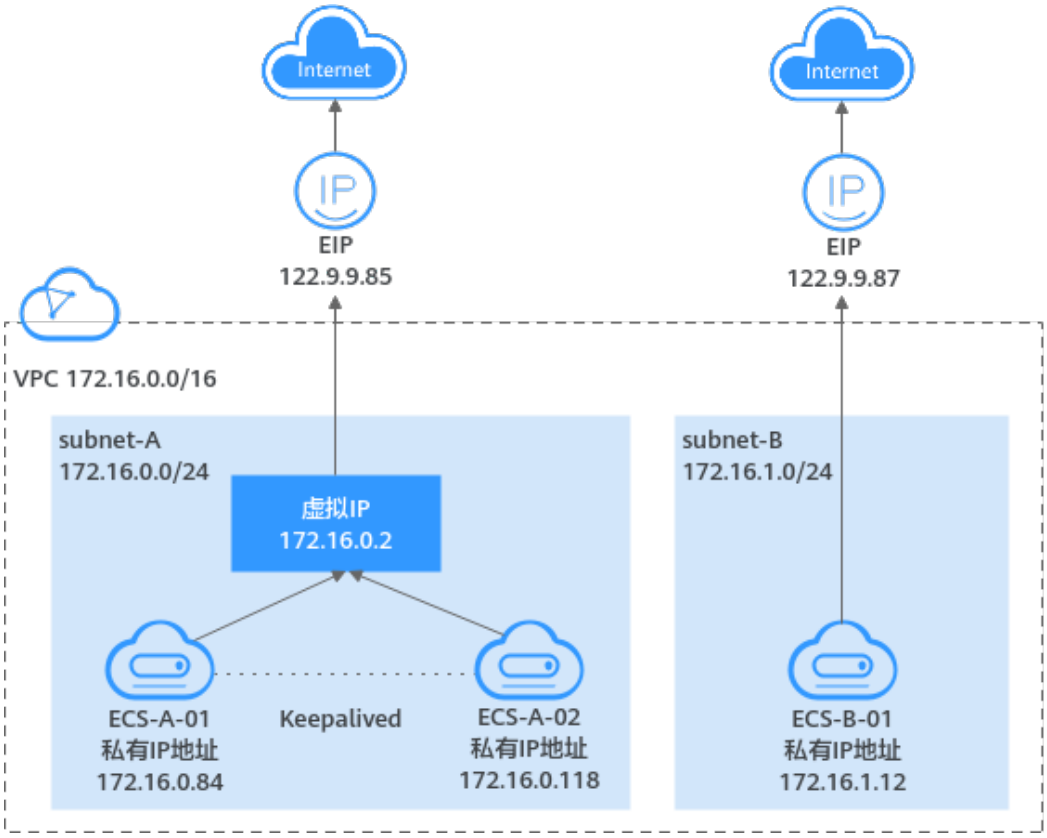
虚拟IP（Virtual IP Address）是从VPC子网网段中划分的一个内网IP地址，是一种可以独立申请和删除的内网IP地址，适用于以下场景：

- 将一个或者多个虚拟IP同时绑定至一个云服务器，可以通过任意一个IP地址（私有IP/虚拟IP）访问云服务器。通常当单个云服务器内同时部署了多种业务，此时可以通过不同的虚拟IP访问各个业务。
- 将一个虚拟IP同时绑定至多个云服务器，虚拟IP需要搭配高可用软件（比如Keepalived），用来搭建高可用的主备集群。为了提升服务的高可用性，避免单点故障，您可以用“一主一备”或“一主多备”的方法组合使用云服务器，这些云服务器对外呈现为一个虚拟IP。当主云服务器故障时，备云服务器可以转为主云服务器并继续对外提供服务，以此达到高可用性HA（High Availability）的目的。

通常情况下，云服务器使用私有IP地址进行内网通信，虚拟IP地址拥有私有IP地址同样的网络接入能力，包括VPC内二三层通信、VPC之间对等连接通信、EIP公网通信、接入VPN和云专线的能力。云服务器的私有IP、虚拟IP以及EIP的典型使用场景示意图，请参见图4-1。

- 私有IP地址：用于内网通信，不能访问公网。
- 虚拟IP：搭配Keepalived构建高可用集群，多个ECS构建的集群对外呈现一个虚拟IP。
- EIP：用于公网通信。

图 4-1 云服务器（ECS）不同 IP 地址的使用场景示意图



虚拟 IP 应用场景

通常情况下，虚拟IP搭配Keepalived使用，搭建高可用的主备集群。当主云服务器发生故障无法对外提供服务时，系统动态将虚拟IP切换到备云服务器，通过备云服务器继续对外提供服务。以下为您详细介绍虚拟IP典型的使用场景。

使用虚拟 IP 和 Keepalived 搭建高可用集群

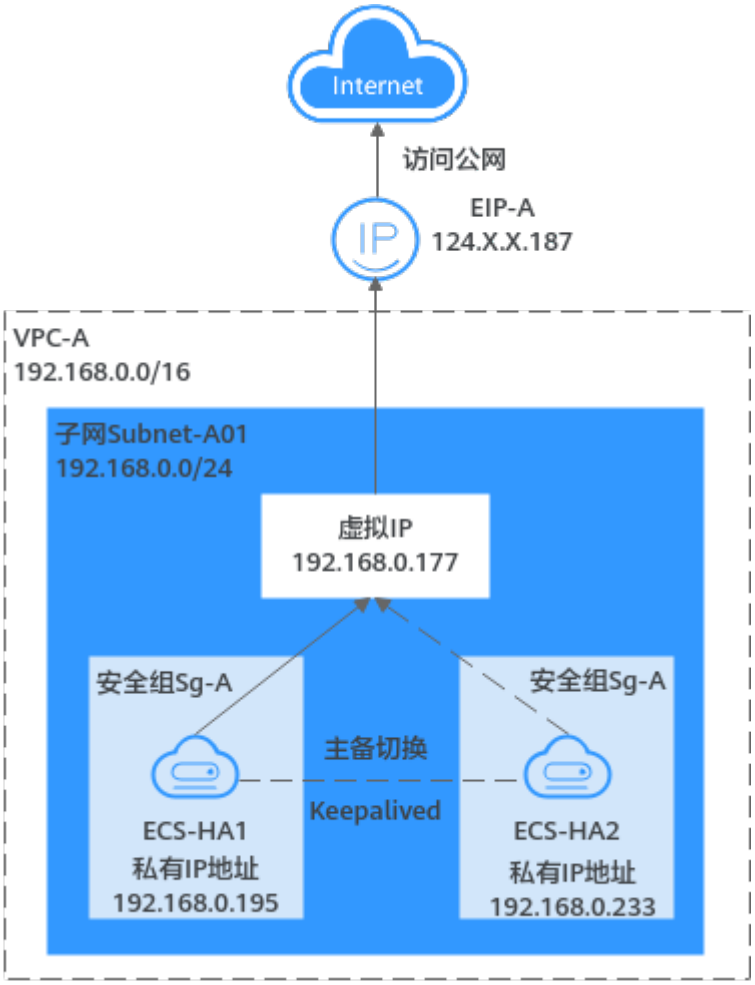
如图4-2所示，基于虚拟IP，并配合使用Keepalived，搭建高可用集群。详细说明如下：

1. 将虚拟IP同时绑定至ECS-HA1和ECS-HA2，在ECS-HA1和ECS-HA2上配置Keepalived，构建主备云服务器。
2. 同时为虚拟IP绑定EIP，该集群可以面向公网提供Web访问服务。

当高可用集群搭建完成后，ECS-HA1作为主云服务器，通过与虚拟IP绑定的EIP对外提供服务，ECS-HA2作为备服务器不承载实际业务。当ECS-HA1发生故障时，此时会自动启用ECS-HA2，ECS-HA2将会接管业务并对外提供服务，实现业务不中断的高可用需求。

高可用集群的具体搭建方法，请您参见**使用虚拟IP和Keepalived搭建高可用Web集群**。

图 4-2 使用虚拟 IP 和 Keepalived 搭建高可用集群



使用虚拟 IP 和 Keepalived/LVS 搭建高可用负载集群

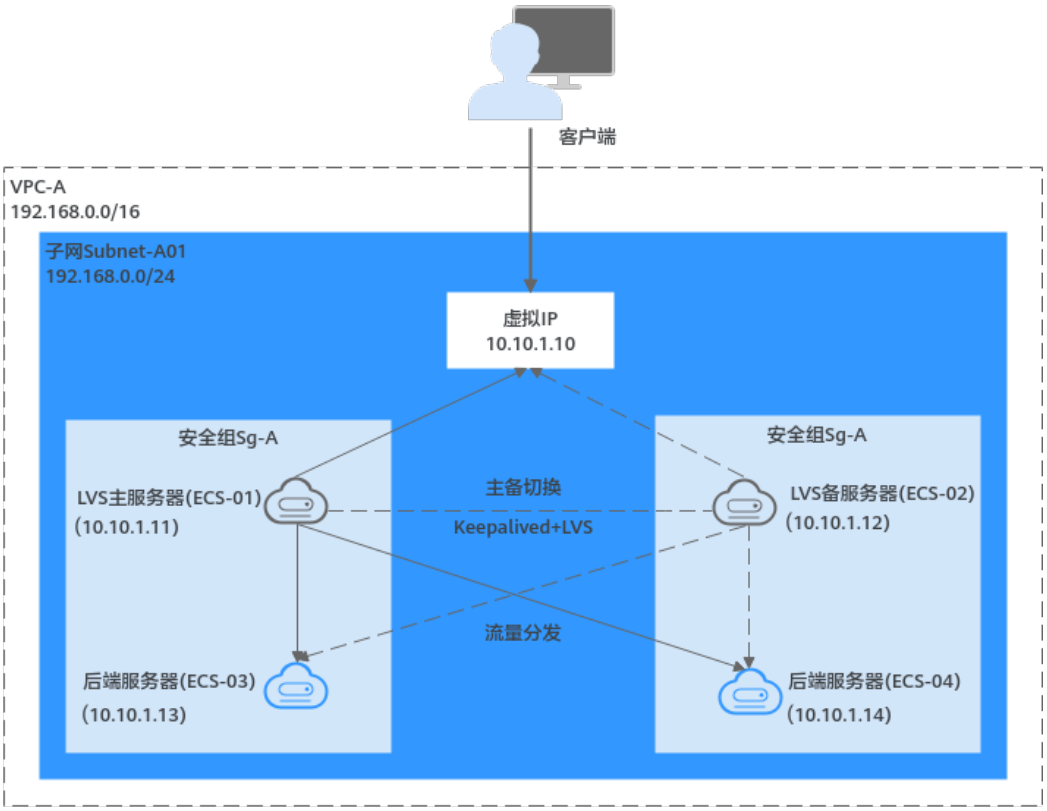
如图4-3所示，基于虚拟IP，并配合使用Keepalived和LVS，用于搭建高可用负载均衡集群服务，LVS用来实现负载均衡，Keepalived用来实现LVS集群的高可用。详细说明如下：

1. 将虚拟IP同时绑定至ECS-01和ECS-02。在ECS-01和ECS-02上配置Keepalived和LVS（DR模式），构建主备LVS服务器，可以将来自客户端的请求均衡的分发到不同的后端服务器上。
2. 配置ECS-03和ECS-04作为后端服务器，处理实际的业务请求。
3. 检查四台ECS网卡的“源/目的检查”功能是否关闭。

   将虚拟IP绑定至ECS时，系统会自动关闭ECS网卡的“源/目的检查”功能，如果未关闭，则请关闭该功能。

当高可用负载集群搭建完成后，ECS-01作为主服务器，分发来自客户端的请求。当ECS-01发生故障时，此时会自动启用ECS-02继续分发客户端的请求，确保LVS集群的高可用性。

图 4-3 使用虚拟 IP 和 Keepalived/LVS 搭建高可用负载集群



说明

Keepalived和LVS服务的安装及配置、后端服务器的配置请您参考业内通用的配置方法，此处不做详细介绍。

虚拟 IP 的配额限制

虚拟IP功能的各项配额说明如表4-1所示，部分默认配额可以提升，您可以根据提示申请扩大配额。

表 4-1 虚拟 IP 的配额说明

配额项目	默认配额	申请扩大配额
一个用户在单个区域可申请的虚拟IP数量	2个	申请更多配额，请参见管理VPC配额
单个虚拟IP地址可绑定的弹性公网IP数量	1个	不支持修改
单个虚拟IP支持同时绑定的实例数量（实例包括云服务器、网卡等）	10个	不支持修改

虚拟 IP 的使用限制

- 当云服务器具有多个网卡，并且这些网卡都归属一个子网时，不推荐使用虚拟IP功能。如果在该场景下使用虚拟IP功能，弹性云服务器内部会存在路由冲突，导致虚拟IP通信异常。
- 虚拟IP是从VPC子网内划分的一个内网地址，因此仅支持将虚拟IP绑定至当前子网内的云服务器，不支持跨子网绑定云服务器。
- 使用IPv6地址的虚拟IP仅支持绑定一个网卡，如需进行服务器的主备切换，请通过调用API方式实现。具体请参考**配置云服务器高可用的IPv6虚拟IP功能**。
- 虚拟IP及扩展弹性网卡不支持直接访问华为云内网云服务，如内网DNS等，推荐使用VPCEP访问华为云内网云服务，具体参见**购买连接“接口”型终端节点服务的终端节点**。

4.2 申请虚拟 IP 地址

操作场景

虚拟IP是从VPC子网网段中划分的一个内网IP地址，是一种可以独立申请和删除的内网IP地址，您可以参考以下操作申请虚拟IP地址。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
5. 在子网列表中，单击需要申请虚拟IP地址的子网名称。
   进入子网详情页面。
6. 在“IP地址管理”页签中，单击“申请虚拟IP地址”。
   进入虚拟IP申请页面。
7. 根据界面提示，设置申请虚拟IP所需的参数。

表 4-2 虚拟 IP 参数

参数	说明	取值样例
当前子网	虚拟IP所属的子网，无需选择，默认在您当前所选的子网内申请虚拟IP。	Subnet-A01
IP类型	当虚拟IP所属子网开启IPv6时，您才可以选择IP类型。支持的IP类型如下： • IPv4 • IPv6	IPv4

参数	说明	取值样例
创建方式	当前支持以下两种创建方式： ● 自动分配：表示系统自动从子网网段中选取一个IP地址。 ● 手动分配：表示您可以自行从子网网段中选取一个IP地址。	手动分配
IP地址	如果创建方式选择了“手动分配”，则需要设置IP地址。 从子网网段中选择一个可用的IP地址。	192.168.0.15

8. 参数设置完成后，单击“确定”。
   返回虚拟IP列表，可以查看申请的虚拟IP地址。

4.3 将虚拟 IP 绑定至实例或者 EIP

操作场景

您可以参考以下操作，将虚拟IP绑定至实例或者弹性公网IP，实例包括云服务器、网卡以及二层连接。

- 将虚拟IP绑定至实例，根据您不同的业务需求，您可以任意组合虚拟IP和实例：
  - 为一个实例同时绑定一个或者多个虚拟IP
  - 将一个虚拟IP同时绑定至多个实例
- 将虚拟IP绑定至弹性公网IP，实现公网访问需求。

约束与限制

建议一个ECS绑定的虚拟IP数量不超过8个。如果一个ECS绑定多个虚拟IP，通常不同的虚拟IP承载不同业务，业务过多的情况下，不同业务可能会导致云服务器超负荷从而影响实际体验。

登录控制台为虚拟 IP 绑定弹性公网 IP 或实例

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击虚拟IP所属子网的名称。
   进入子网详情页面。
6. 在“IP地址管理”页签，执行以下操作，为虚拟IP绑定弹性公网IP。

a. 在虚拟IP所在行的操作列下，单击“绑定弹性公网IP”。
弹出“绑定弹性公网IP”对话框。
b. 在对话框中，选择弹性公网IP ，并单击“确定”。
返回虚拟IP列表中，可以看到已绑定的弹性公网IP。

7. 在“IP地址管理”页签，执行以下操作，为虚拟IP绑定实例。
a. 在虚拟IP所在行的操作列下，单击“绑定实例”。
弹出“绑定实例”对话框。
b. 在对话框中，选择实例 ，并单击“确定”。
返回虚拟IP列表中，可以看到已绑定的实例。

须知

- 当您为一个ECS绑定一个或者多个虚拟IP时，则在控制台上绑定完成后，还需要在弹性云服务器上手工配置虚拟IP地址才可以使用，具体请参见**登录ECS配置虚拟IP地址**。
- 当您将一个虚拟IP同时绑定至多个ECS，并且配合Keepalived搭建高可用集群时，则请参见**使用虚拟IP和Keepalived搭建高可用Web集群**。

登录 ECS 配置虚拟 IP 地址

当为一个ECS绑定一个虚拟IP或者多个虚拟IP时，在控制台执行完绑定虚拟IP的操作后，您还需要参考以下章节，登录弹性云服务器手工配置虚拟IP地址。

本文提供以下操作系统的配置示例，其他操作系统，请您参考对应官网帮助文档进行配置。

- Linux系统：CentOS 7.2 64bit、Ubuntu 22.04 server 64bit
- Windows系统：Windows Server

Linux 系统（CentOS）

以下操作以“CentOS 7.2 64bit”为例，供您参考。

1. 执行以下命令，查看并记录需要绑定虚拟IP的网卡及对应连接。
nmcli connection
回显类似如下信息：

```
[root@ecs-test-0001 ~]#nmcli connection
NAME                UUID                                  TYPE      DEVICE
Wired connection 1  5e72ec5a-6165-3bd6-a34b-ce43981acb27  ethernet  eth0
docker0             cd351a91-c5eb-4b69-83eb-df092a2ccf6b  bridge    docker0
```

本示例的回显信息说明如下：
– **DEVICE**列的**eth0**为需要绑定虚拟IP的网卡。
– **NAME**列的**Wired connection 1**为网卡对应的连接。
2. 执行以下命令，在目标网卡连接中添加虚拟IP。
nmcli connection modify "*网卡对应的连接名称***" +ipv4.addresses** *虚拟IP地址*
参数说明如下：
– 网卡对应的连接名称：为1中查到的网卡对应的连接，本示例中为**Wired connection 1**。

- 虚拟IP地址：待添加的虚拟IP地址，如果一次添加多个虚拟IP地址，多个虚拟IP地址之间用“,”隔开。

命令示例：

- 添加单个虚拟IP：**nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125**
- 添加多个虚拟IP：**nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125,172.16.0.126**

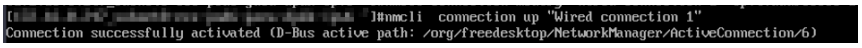
3. 执行以下命令，使2的配置生效。

   nmcli connection up "*网卡对应的连接名称*"

   命令示例：

   nmcli connection up "Wired connection 1"

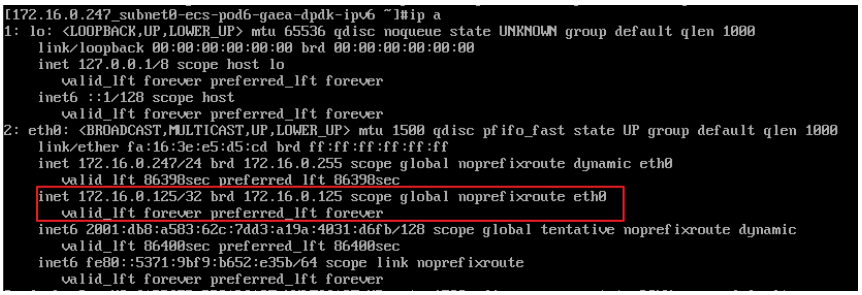
   回显类似如下信息：

4. 执行以下命令，检查虚拟IP配置是否成功。

   ip a

   回显类似如下信息，可以看到eth0网卡下存在虚拟IP地址，为**172.16.0.125**。

说明

如果您需要删除已添加的虚拟IP，可以使用以下方法：

1. 在目标网卡连接中删除虚拟IP。

   nmcli connection modify "*网卡对应的连接名称*" -ipv4.addresses *虚拟IP地址*

   一次删除多个虚拟IP地址时，多个IP之间用“,”隔开，命令示例：

   - 删除单个虚拟IP：**nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125**
   - 删除多个虚拟IP：**nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125,172.16.0.126**

2. 参考3，使删除操作生效。

Linux 系统（Ubuntu）

以下操作以“Ubuntu 22.04 server 64bit”为例，当弹性云服务器的操作系统为**Ubuntu 22**和**Ubuntu 20**时，请您参考下述方法。

1. 执行以下命令，查看并记录需要绑定虚拟IP的网卡。

   ifconfig

   回显类似如下信息，本示例中绑定虚拟IP的网卡名称为**eth0**。

```
root@ecs-X-ubantu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.210  netmask 255.255.255.0  broadcast 172.16.0.255
```



```
        inet6 fe80::f816:3eff:fe01:f1c3  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:01:f1:c3  txqueuelen 1000  (Ethernet)
        RX packets 43915  bytes 63606486 (63.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3364  bytes 455617 (455.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

2. 执行以下命令，进入“/etc/netplan”目录。

   cd /etc/netplan

3. 执行以下命令，为目标网卡添加虚拟IP地址。

   a. 执行以下命令，打开配置文件“01-netcfg.yaml”。

      vim 01-netcfg.yaml

   b. 按i进入编辑模式。

   c. 在对应网卡配置区域内，添加虚拟IP地址。

      本示例为**eth0**添加虚拟IP地址，待添加内容如下：

      addresses:

      - 172.16.0.26/32

      添加后文件内容如下：

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    eth0:
      dhcp4: true
      addresses:
      - 172.16.0.26/32
    eth1:
      dhcp4: true
    eth2:
      dhcp4: true
    eth3:
      dhcp4: true
    eth4:
      dhcp4: true
```

   d. 添加完成后，按“ESC”，并输入“:wq!”，保存后退出文件。

4. 执行以下命令，使**3**的配置生效。

   netplan apply

5. 执行以下命令，检查虚拟IP配置是否成功。

   ip a

   回显类似如下信息，可以看到eth0网卡下存在虚拟IP地址，为**172.16.0.26**。

```
root@ecs-X-ubantu:/etc/netplan# ip a
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether fa:16:3e:01:f1:c3 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 172.16.0.26/32 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet 172.16.0.210/24 brd 172.16.0.255 scope global dynamic noprefixroute eth0
       valid_lft 107999971sec preferred_lft 107999971sec
    inet6 fe80::f816:3eff:fe01:f1c3/64 scope link
       valid_lft forever preferred_lft forever
```


说明

如果您需要删除已添加的虚拟IP，可以使用以下方法：

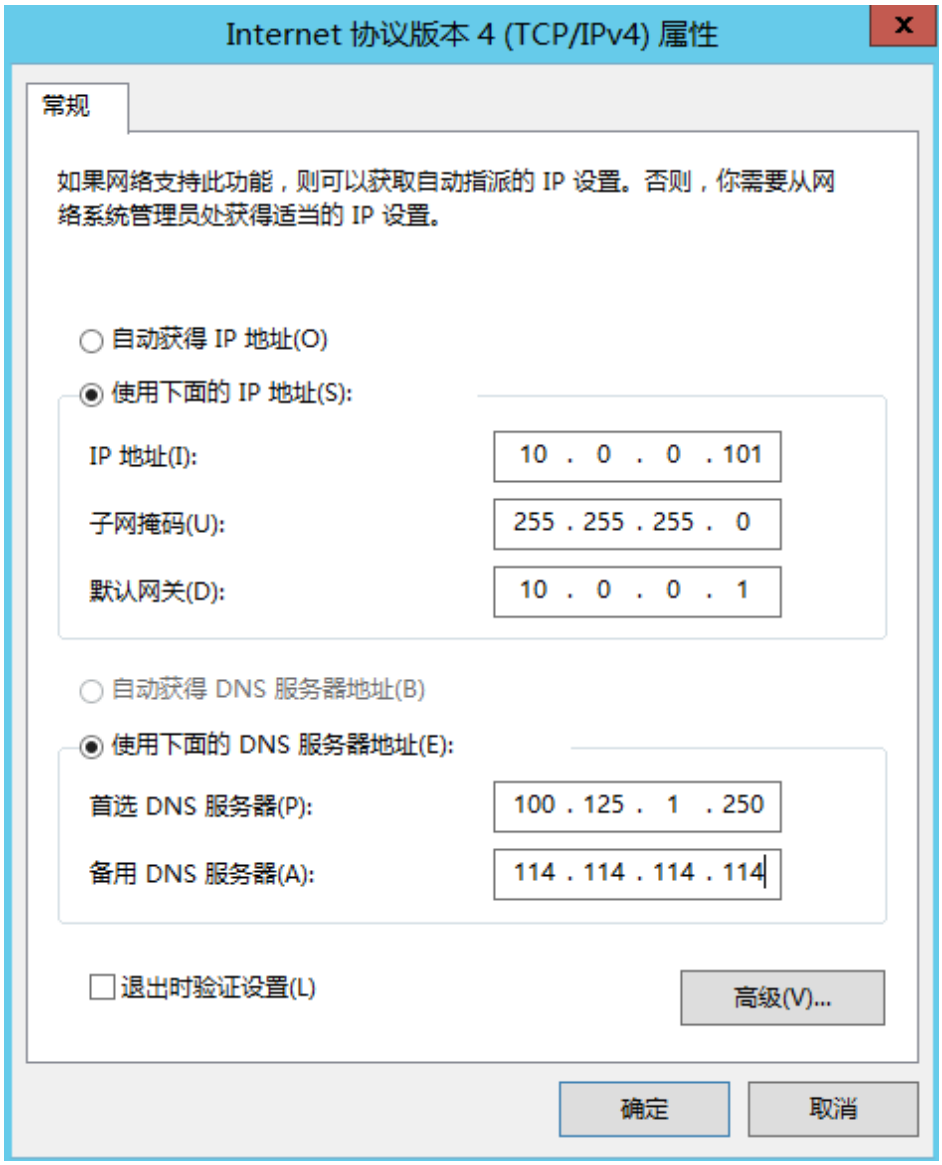
1. 参考3，打开配置文件“01-netcfg.yaml”，并删除对应网卡下虚拟IP的地址。
2. 参考4，使删除操作生效。

Windows 系统（Windows Server）

以下操作以“Windows Server”为例，供您参考。

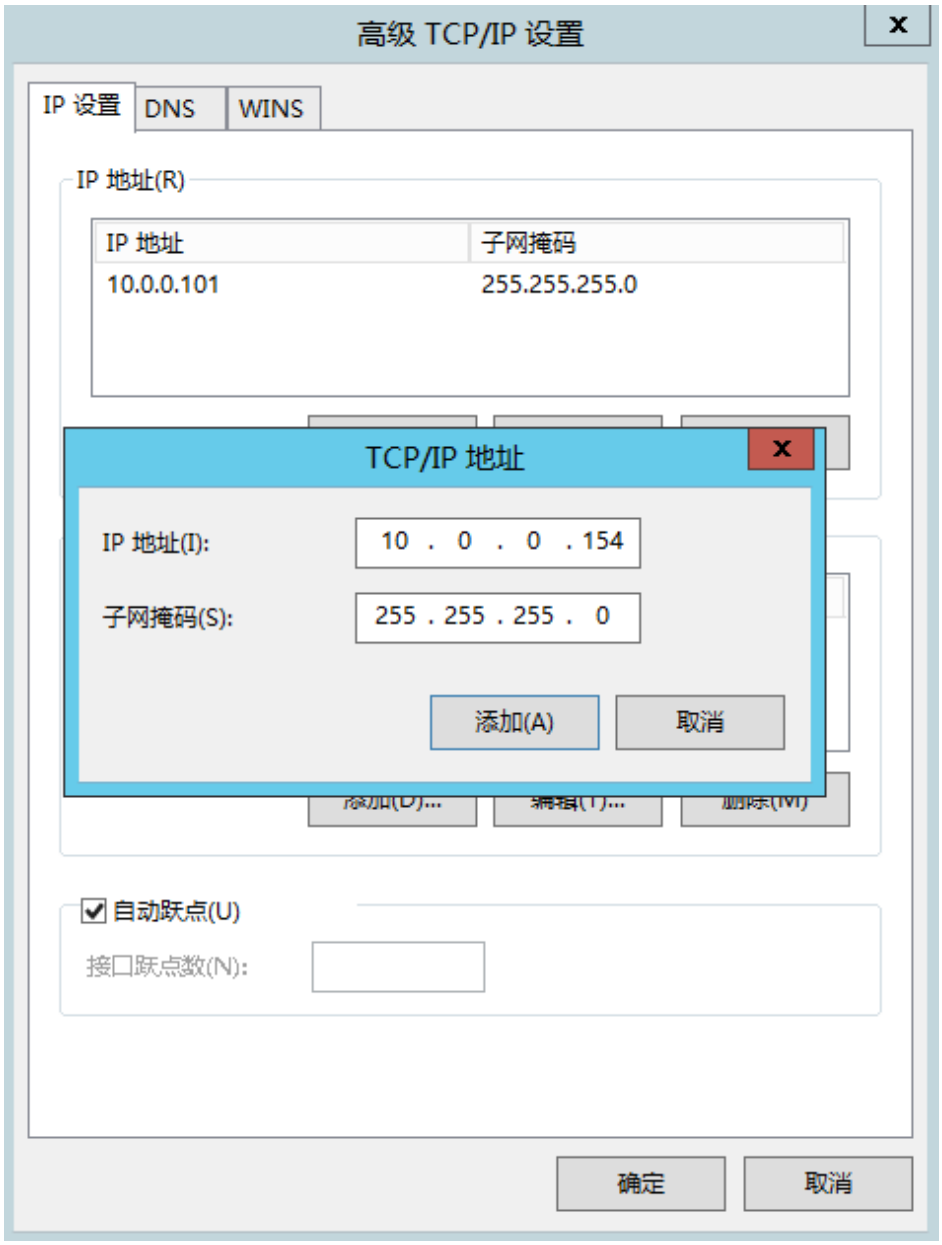
1. 在“控制面板 > 网络和共享中心”路径下，单击对应的本地连接。
2. 在打开的本地连接页面中，单击“属性”。
3. 在“网络”页签中选择“Internet 协议版本 4（TCP/IPv4）”。
4. 单击“属性”。
5. 选择“使用下面的IP地址”，IP地址配置为弹性云服务器的私有IP地址，例如：10.0.0.101。

图 4-4 配置私有 IP 地址



6. 单击“高级”。
7. 在“IP设置”页签内“IP地址”区域，单击“添加”。
   添加虚拟IP地址，例如：10.0.0.154。

   图 4-5 配置虚拟 IP 地址



8. 单击“确定”，保存更改。
9. 在“开始”菜单中打开Windows命令行窗口，执行以下命令确认是否配置了虚拟IP地址。

   ipconfig /all

   回显样例中IPv4 Address包含虚拟IP地址10.0.0.154，表示弹性云服务器内部网卡的虚拟IP地址配置正常。

相关操作

- 弹性云服务器的网卡绑定虚拟IP地址后，该虚拟IP地址无法ping通时，如何排查?
- 弹性公网IP、私有IP和虚拟IP之间有何区别?

4.4 将虚拟 IP 从实例或者 EIP 上解绑定

操作场景

您可以参考以下操作，将虚拟IP从实例或者弹性公网IP解绑定，实例包括云服务器、网卡以及二层连接。

- 将虚拟IP从实例上解绑定
- 将虚拟IP从弹性公网IP上解绑定

将虚拟 IP 从实例上解绑定

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击虚拟IP地址所属的子网名称。
   进入子网详情页面。
6. 选择“IP地址管理”页签。
   进入虚拟IP列表页面。
7. 在虚拟IP列表中，在目标虚拟IP所在操作列下，选择“更多 > 解绑实例”。
   弹出解绑实例对话框。
8. 在解绑实例对话框中，执行以下操作，解绑虚拟IP绑定的实例。
   a. 选择绑定的实例类型，系统会展示对应的实例列表。
   b. 在目标实例所在行的操作列下，单击“解绑”。
      弹出解绑确认对话框。
   c. 确认无误后，单击“确定”，将虚拟IP和实例解绑。

将虚拟 IP 从弹性公网 IP 上解绑定

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。

5. 在子网列表中，单击虚拟IP地址所属的子网名称。
   进入子网详情页面。
6. 选择“IP地址管理”页签。
   进入虚拟IP列表页面。
7. 在虚拟IP列表中，在目标虚拟IP所在操作列表下，单击“解绑弹性公网IP”。
   弹出解绑确认对话框。
8. 确认无误后，单击“确定”，将虚拟IP和弹性公网IP解绑。

4.5 删除虚拟 IP 地址

操作场景

当无需使用子网的虚拟IP地址或预留虚拟IP地址、需要释放网络资源时，可删除子网的虚拟IP地址。

约束与限制

当虚拟IP被其他资源占用时，无法删除，请根据提示信息进行处理，具体请参见**表4-3**。

表 4-3 虚拟 IP 无法删除原因说明

提示信息	原因说明及处理方法
已绑定实例或弹性公网IP地址，无法执行删除操作，请先执行对应解绑操作。 如**图4-6**所示。	当前虚拟IP可能被弹性公网IP、弹性云服务等资源占用，请先解绑占用资源，再删除虚拟IP。请参见**将虚拟IP从实例或者EIP上解绑定**。 解绑完成后，可以重新尝试删除虚拟IP。
虚拟IP已被系统组件使用，无法执行操作。 如**图4-7**所示。	当前虚拟IP被其他服务实例使用，该IP不支持单独删除。如果您不需要使用该虚拟IP，请删除对应的实例，该虚拟IP会被同时删除。 请根据虚拟IP控制台显示的实例信息，查找对应实例并删除，常见的服务如下： ● RDS实例：请参见**云数据库RDS帮助文档**，查找删除方法。 ● CCE实例：请参见**容器引擎 CCE帮助文档**，查找删除方法。 ● API网关实例：请参见**API网关帮助文档**，查找删除方法。

图 4-6 虚拟 IP 无法删除-场景一

图 4-7 虚拟 IP 无法删除-场景二

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
5. 在子网列表中，单击虚拟IP地址所属子网名称。
6. 选择“IP地址管理”页签，在需要删除虚拟IP地址所在行的操作列下，单击“更多 > 删除”。
   弹出删除确认对话框。
7. 确认无误后，单击“确定”，删除虚拟IP地址。

4.6 虚拟 IP 配置示例

4.6.1 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群

应用场景

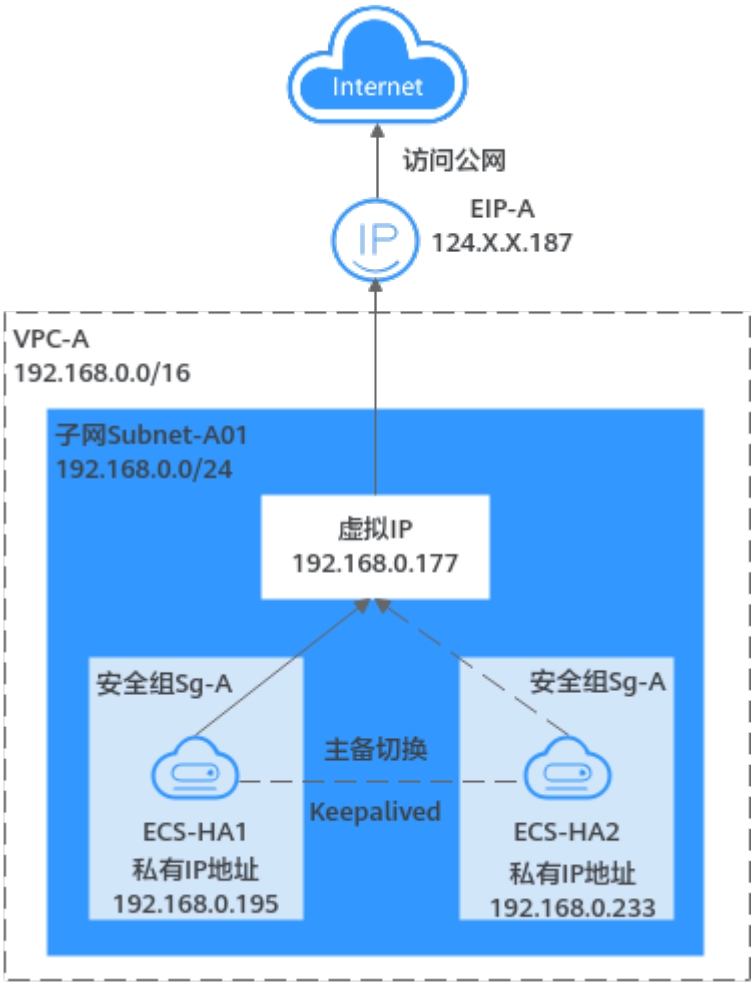
虚拟IP（Virtual IP Address）是从VPC子网网段中划分的一个内网IP地址，通常搭配高可用软件（比如Keepalived）使用，主要用来搭建高可用的主备集群。多个云服务器形成主备集群，当主云服务器发生故障无法对外提供服务时，系统动态将虚拟IP切换到备云服务器，通过备云服务器继续对外提供服务。本文档为您详细介绍使用虚拟IP和Keepalived搭建高可用Web集群的方法。

方案架构

本示例中，高可用Web集群架构如图4-8所示，将虚拟IP同时绑定至ECS-HA1和ECS-HA2，使用Keepalived搭建一个高可用集群。同时，为虚拟IP绑定EIP，该集群具备公网访问能力，可以面向公网提供Web访问服务。实现原理如下：

1. ECS-HA1作为主云服务器，通过与虚拟IP绑定的EIP对外提供服务，ECS-HA2作为备云服务器不承载实际业务。
2. 当ECS-HA1发生故障时，此时会自动启用ECS-HA2，ECS-HA2将会接管业务并对外提供服务，实现业务不中断的高可用需求。

图 4-8 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群



方案优势

基于虚拟IP和Keepalived能力，采用“一主一备”或“一主多备”的方法组合使用云服务器，这些云服务器对外呈现为一个虚拟IP。当主云服务器故障时，备云服务器可以转为主云服务器并继续对外提供服务，以此达到高可用性HA（High Availability）的目的，可以解决用户由于云服务器故障导致的对外服务中断问题。

约束与限制

使用虚拟IP搭建的高可用集群，所有服务器必须位于同一个虚拟私有云的子网内。

资源规划说明

本示例中，虚拟私有云VPC和子网、虚拟IP、弹性公网IP以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

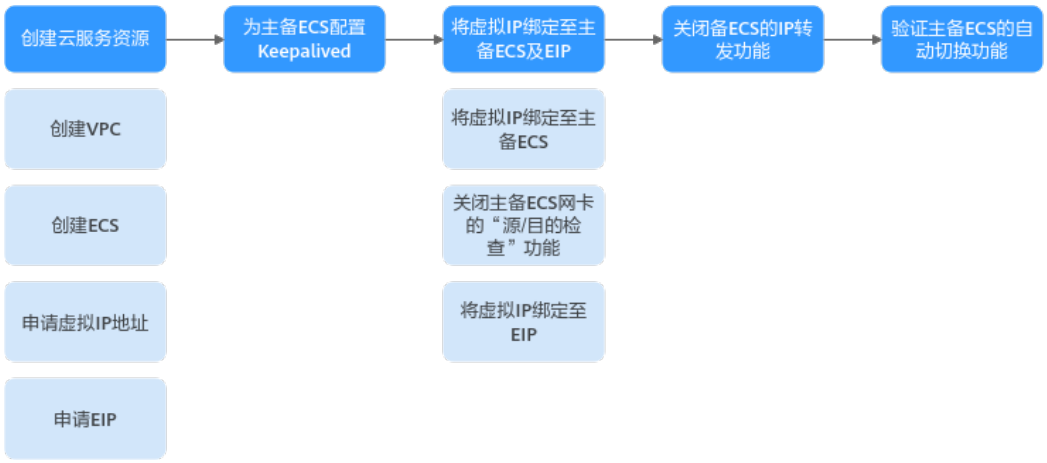
表 4-4 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群资源规划总体说明

资源类型	资源数量	说明
虚拟私有云VPC和子网	1	• VPC名称：请根据实际情况填写，本示例为VPC-A。 • IPv4网段：请根据实际情况填写，本示例为192.168.0.0/16。 • 子网名称：请根据实际情况填写，本示例为Subnet-A01。 • 子网IPv4网段：请根据实际情况填写，本示例为192.168.0.0/24。
弹性云服务器ECS	2	本示例中，需要两个ECS作为主备倒换，配置说明如下： • 名称：根据实际情况填写，本示例分别为ECS-HA1和ECS-HA2。 • 镜像：请根据实际情况选择，本示例为公共镜像（CentOS 7.8 64bit）。 • 系统盘：通用型SSD盘，40GB。 • 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘，并切实考虑两个ECS节点之间的业务数据一致性问题。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例为VPC-A。 – 子网：选择子网，本示例为Subnet-A01。 • 安全组：请根据实际情况选择，本示例中ECS-HA1和ECS-HA2使用同一个安全组，安全组名称为Sg-A。 • 私有IP地址：ECS-HA1为192.168.0.195，ECS-HA2为192.168.0.233
虚拟IP	1	在子网Subnet-A01中申请虚拟IP地址： • 创建方式：根据实际情况填写，本示例为自动分配。 • 虚拟IP地址：本示例为192.168.0.177。 • 绑定实例：将虚拟IP绑定至ECS-HA1和ECS-HA2。 • 绑定弹性公网IP：将虚拟IP绑定至EIP-A。
弹性公网IP	1	• 计费模式：请根据情况选择计费模式，本示例为按需计费。 • EIP名称：请根据实际情况填写，本示例为EIP-A。 • EIP地址：EIP地址系统随机分配，本示例为124.X.X.187。

操作流程

使用虚拟IP和Keepalived搭建高可用Web集群，流程如**图4-9**所示。

图 4-9 使用虚拟 IP 和 Keepalived 搭建高可用 Web 集群



步骤一：创建云服务资源

1. 创建1个VPC和1个子网。

   具体方法请参见**创建虚拟私有云和子网**。

2. 创建2个ECS，分别作为主ECS和备ECS。

   具体方法请参见**自定义购买ECS**。

   本示例中，ECS的网络配置详情如下：

   - 网络：选择已创建的虚拟私有云和子网，VPC-A和Subnet-A01。
   - 安全组：新建一个安全组Sg-A，并添加入方向和出方向规则。您在创建安全组的时候，系统会自动添加部分规则，您需要根据实际情况进行检查修改。

     本示例中，ECS-HA1和ECS-HA2属于同一个安全组，您需要确保**表4-5**中的规则均已正确添加。

     表 4-5 安全组 Sg-A 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址：0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址：0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	TCP: 80	源地址：0.0.0.0/0	放通安全组内ECS的HTTP(80)端口，用于外部通过HTTP协议访问ECS上部署的网站。
入方向	允许	IPv4	全部	源地址：当前安全组Sg-A	针对IPv4，用于安全组内ECS之间网络互通。
入方向	允许	IPv6	全部	源地址：当前安全组Sg-A	针对IPv6，用于安全组内ECS之间网络互通。

方向	策略	类型	协议端口	源地址/目的地址	描述
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

须知

本示例中，源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，为了确保安全，建议您遵循最小原则，根据实际情况将源IP设置为特定的IP地址，比如，源地址设置为您的本地PC地址。

如果您的ECS位于不同的安全组，比如ECS-HA1属于Sg-A，ECS-HA2属于Sg-B，则除了在两个安全组中分别配置表4-5中的规则，您还需要添加表4-6中的规则，放通两个安全组之间的内网网络流量。

表 4-6 安全组 Sg-A 和 Sg-B 规则说明

安全组	方向	策略	类型	协议端口	源地址/目的地址	描述
Sg-A	入方向	允许	IPv4	全部	源地址：Sg-B	针对全部IPv4协议，允许来自Sg-B内实例的流量访问Sg-A内的实例。
Sg-B	入方向	允许	IPv4	全部	源地址：Sg-A	针对全部IPv4协议，允许来自Sg-A内实例的流量访问Sg-B内的实例。

- 弹性公网IP：选择“暂不购买”。

3. 在子网Subnet-A01内，申请虚拟IP地址。
   具体方法请参见**申请虚拟IP地址**。
4. 申请弹性公网IP。
   具体方法请参见**购买弹性公网IP**。

步骤二：为主备 ECS 配置 Keepalived

1. 执行以下操作，为ECS-HA1配置Keepalived。
   a. 将EIP绑定至ECS-HA1。
      具体方法请参见**绑定弹性公网IP**。
   b. 远程登录ECS-HA1。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。

c. 执行以下命令，安装Nginx、Keepalived软件包及相关依赖包。

yum install nginx keepalived -y

回显类似如下信息，表示安装完成。

```
[root@ecs-ha1 ~]# yum install nginx keepalived -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base
                         | 3.6 kB  00:00:00
epel
                         | 4.3 kB  00:00:00
extras
                         | 2.9 kB  00:00:00
updates
                          | 2.9 kB  00:00:00
(1/7): epel/x86_64/
group
        | 399 kB  00:00:00
(2/7): epel/x86_64/
updateinfo
         | 1.0 MB  00:00:00
(3/7): base/7/x86_64/
primary_db
         | 6.1 MB  00:00:00
(4/7): base/7/x86_64/
group_gz
        | 153 kB  00:00:00
(5/7): epel/x86_64/
primary_db
          | 8.7 MB  00:00:00
(6/7): extras/7/x86_64/
primary_db
       | 253 kB  00:00:00
(7/7): updates/7/x86_64/primary_db

.....
Dependency Installed:
  centos-indexhtml.noarch 0:7-9.el7.centos                  gperftools-libs.x86_64
0:2.6.1-1.el7                lm_sensors-libs.x86_64 0:3.4.0-8.20160601gitf9185e5.el7_9.1
  net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4             net-snmp-libs.x86_64
1:5.7.2-49.el7_9.4            nginx-filesystem.noarch 1:1.20.1-10.el7
  openssl11-libs.x86_64 1:1.1.1k-7.el7

Complete!
```

d. 执行以下操作，修改Nginx配置文件，添加80端口相关配置。

i. 执行以下命令，打开“/etc/nginx/nginx.conf”文件。

vim /etc/nginx/nginx.conf

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
user root;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
     worker_connections 1024;
     }
http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr  - $remote_user [$time_local] "$request" '
    # '$status $body_bytes_sent  "$http_referer" '
    # '"$http_user_agent"  "$http_x_forwarded_for"';
    #access_log logs/access.log main;
```



```
    sendfile on;
    #tcp_nopush on;
    #keepalive_timeout 0;
    keepalive_timeout 65;
    #gzip on;
    server {
        listen 80;
        server_name localhost;
        #charset koi8-r;
        #access_log logs/host.access.log main;
        location / {
                root html;
                index index.html index.htm;
                }
        #error_page 404  /404.html;
        # redirect server error pages to the static page /50x.html
        error_page 500 502 503 504 /50x.html;
        location =  /50x.html {
                        root html;
                        }
        }
}
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下操作，修改index.html文件内容，用来验证网站的访问情况。

i. 执行以下命令，打开“/usr/share/nginx/html/index.html”文件。

vim /usr/share/nginx/html/index.html

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
Welcome to ECS-HA1
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

f. 执行以下命令，设置Nginx服务开机自启动，并启动Nginx服务。

systemctl enable nginx

systemctl start nginx.service

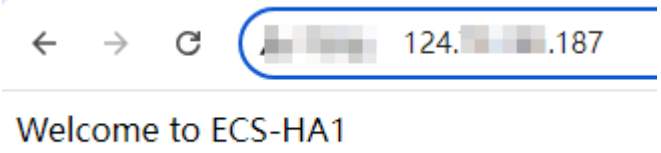
回显类似如下信息：

```
[root@ecs-ha1 ~]# systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[root@ecs-ha1 ~]# systemctl start nginx.service
```

g. 打开浏览器，并输入EIP地址（124.X.X.187），验证Nginx单节点的访问情况。

网页如下图所示，表示ECS-HA1的Nginx配置成功。

图 4-10 ECS-HA1 访问验证



h. 执行以下操作，修改Keepalived配置文件。

i. 执行以下命令，打开“/etc/keepalived/keepalived.conf”文件。

vim /etc/keepalived/keepalived.conf

ii. 按**i**进入编辑模式。

iii. 根据实际情况，替换配置文件中的IP参数，并将文件中原有的内容，全部替换成以下内容。

- mcast_src_ip和unicast_src_ip：替换为ECS-HA1的私有IP地址，本示例为192.168.0.195。
- virtual_ipaddress：替换为虚拟IP地址，本示例为192.168.0.177。

```
! Configuration File for keepalived
global_defs {
router_id master-node
}
vrrp_script chk_http_port {
        script  "/etc/keepalived/chk_nginx.sh"
        interval 2
        weight -5
        fall 2
        rise 1
       }
vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    mcast_src_ip 192.168.0.195
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
            auth_type PASS
            auth_pass 1111
            }
    unicast_src_ip 192.168.0.195
    virtual_ipaddress {
                192.168.0.177
              }
track_script {
    chk_http_port
    }
}
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

i. 执行以下操作，配置Nginx监控脚本。

i. 执行以下命令，打开“/etc/keepalived/chk_nginx.sh”文件。

vim /etc/keepalived/chk_nginx.sh

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
    sleep 2
    counter=$(ps -C nginx  --no-heading|wc -l)
    if [ "${counter}" =  "0" ]; then
        systemctl stop keepalived.service
    fi
fi
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

j. 执行以下命令，为“chk_nginx.sh”文件添加执行权限。

chmod +x /etc/keepalived/chk_nginx.sh

k. 执行以下命令，设置Keepalived服务开机自启动，并启动Keepalived服务。

systemctl enable keepalived

systemctl start keepalived.service

l. 将EIP和ECS-HA1解绑定。
具体方法请参见**解绑弹性公网IP**。

2. 执行以下操作，为ECS-HA2配置Keepalived。

a. 将EIP绑定至ECS-HA2。
具体方法请参见**绑定弹性公网IP**。

b. 远程登录ECS-HA2。
ECS有多种登录方法，具体请参见**登录弹性云服务器**。

c. 执行以下命令，安装Nginx、Keepalived软件包及相关依赖包。
yum install nginx keepalived -y
回显类似如下信息，表示安装完成。

```
[root@ecs-ha2 ~]# yum install nginx keepalived -y
Loaded plugins: fastestmirror
Determining fastest mirrors
base
                         | 3.6 kB  00:00:00
epel
                         | 4.3 kB  00:00:00
extras
                         | 2.9 kB  00:00:00
updates
                           | 2.9 kB  00:00:00
(1/7): epel/x86_64/
group
        | 399 kB  00:00:00
(2/7): epel/x86_64/
updateinfo
          | 1.0 MB  00:00:00
(3/7): base/7/x86_64/
primary_db
         | 6.1 MB  00:00:00
(4/7): base/7/x86_64/
group_gz
        | 153 kB  00:00:00
(5/7): epel/x86_64/
primary_db
           | 8.7 MB  00:00:00
(6/7): extras/7/x86_64/
primary_db
        | 253 kB  00:00:00
(7/7): updates/7/x86_64/primary_db


.....
Dependency Installed:
  centos-indexhtml.noarch 0:7-9.el7.centos                  gperftools-libs.x86_64
0:2.6.1-1.el7                lm_sensors-libs.x86_64 0:3.4.0-8.20160601gitf9185e5.el7_9.1
  net-snmp-agent-libs.x86_64 1:5.7.2-49.el7_9.4             net-snmp-libs.x86_64
1:5.7.2-49.el7_9.4              nginx-filesystem.noarch 1:1.20.1-10.el7
  openssl11-libs.x86_64 1:1.1.1k-7.el7

Complete!
```

d. 执行以下操作，修改Nginx配置文件，添加80端口相关配置。

i. 执行以下命令，打开“/etc/nginx/nginx.conf”文件。
vim /etc/nginx/nginx.conf

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
user root;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
```



```
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
     worker_connections 1024;
     }
http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr  - $remote_user [$time_local] "$request" '
    # '$status $body_bytes_sent  "$http_referer" '
    # '"$http_user_agent"  "$http_x_forwarded_for"';
    #access_log logs/access.log main;
    sendfile on;
    #tcp_nopush on;
    #keepalive_timeout 0;
    keepalive_timeout 65;
    #gzip on;
    server {
        listen 80;
        server_name localhost;
        #charset koi8-r;
        #access_log logs/host.access.log main;
        location / {
                root html;
                index index.html index.htm;
                }
        #error_page 404  /404.html;
        # redirect server error pages to the static page /50x.html
        error_page 500 502 503 504 /50x.html;
        location =  /50x.html {
                        root html;
                        }
        }
}
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下操作，修改index.html文件内容，用来验证网站的访问情况。

i. 执行以下命令，打开“/usr/share/nginx/html/index.html”文件。

vim /usr/share/nginx/html/index.html

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
Welcome to ECS-HA2
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

f. 执行以下命令，设置Nginx服务开机自启动，并启动Nginx服务。

systemctl enable nginx

systemctl start nginx.service

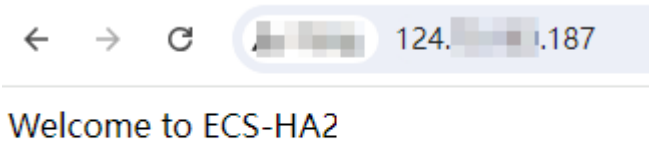
回显类似如下信息：

```
[root@ecs-ha2 ~]# systemctl enable nginx
Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.
[root@ecs-ha2 ~]# systemctl start nginx.service
```

g. 打开浏览器，并输入EIP地址（124.X.X.187），验证Nginx单节点的访问情况。

网页如下图所示，表示ECS-HA2的Nginx配置成功。

图 4-11 ECS-HA2 访问验证



h. 执行以下操作，修改Keepalived配置文件。

i. 执行以下命令，打开“/etc/keepalived/keepalived.conf”文件。

vim /etc/keepalived/keepalived.conf

ii. 按**i**进入编辑模式。

iii. 根据实际情况，替换配置文件中的IP参数，并将文件中原有的内容，全部替换成以下内容。

- mcast_src_ip和unicast_src_ip：替换为ECS-HA2的私有IP地址，本示例为192.168.0.233。
- virtual_ipaddress：替换为虚拟IP地址，本示例为192.168.0.177。

```
! Configuration File for keepalived
global_defs {
router_id master-node
}
vrrp_script chk_http_port {
         script  "/etc/keepalived/chk_nginx.sh"
         interval 2
         weight -5
         fall 2
         rise 1
       }
vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    mcast_src_ip 192.168.0.233
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
            auth_type PASS
            auth_pass 1111
            }
    unicast_src_ip 192.168.0.233
    virtual_ipaddress {
                192.168.0.177
              }
track_script {
    chk_http_port
    }
}
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

i. 执行以下操作，配置Nginx监控脚本。

i. 执行以下命令，打开“/etc/keepalived/chk_nginx.sh”文件。

vim /etc/keepalived/chk_nginx.sh

ii. 按**i**进入编辑模式。

iii. 将文件中原有的内容，全部替换成以下内容。

```
#!/bin/bash
counter=$(ps -C nginx --no-heading|wc -l)
```

```
if [ "${counter}" = "0"  ]; then
    systemctl start nginx.service
    sleep 2
    counter=$(ps -C nginx  --no-heading|wc -l)
    if [ "${counter}" =  "0" ]; then
        systemctl stop keepalived.service
    fi
fi
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

j. 执行以下命令，为“chk_nginx.sh”文件添加执行权限。

chmod +x /etc/keepalived/chk_nginx.sh

k. 执行以下命令，设置Keepalived服务开机自启动，并启动Keepalived服务。

systemctl enable keepalived

systemctl start keepalived.service

l. 将EIP和ECS-HA2解绑定。

具体方法请参见**解绑弹性公网IP**。

步骤三：将虚拟 IP 绑定至主备 ECS 及 EIP

1. 将虚拟IP分别绑定至主备ECS上，本示例中需要绑定ECS-HA1和ECS-HA2。

   具体操作请参见**将虚拟IP地址绑定至实例或EIP**。

2. 关闭主备ECS网卡的“源/目的检查”功能。

   将虚拟IP绑定至ECS时，系统会自动关闭ECS网卡的“源/目的检查”功能，您需要参考以下操作检查关闭情况。如果未关闭，则请关闭该功能。

   a. 在ECS列表中，单击目标ECS的名称。

   进入ECS详情页。

   b. 选择“弹性网卡”页签，并单击 展开ECS的网卡详情区域，可以查看“源/目的检查”功能。

   如图4-12所示，表示“源/目的检查”功能已关闭。

图 4-12 关闭网卡的“源/目的检查”功能

3. 将虚拟IP绑定至EIP上，本示例中需要绑定EIP-A。
   具体操作请参见**将虚拟IP地址绑定至实例或EIP**。

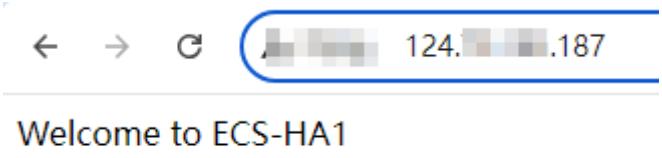
步骤四：关闭备 ECS 的 IP 转发功能

使用虚拟IP构建主备场景的高可用集群时，需要关闭备ECS的IP转发功能，当主备ECS切换后，则需要确保新的备ECS也关闭IP转发功能。

为了避免ECS主备切换后遗漏配置，建议您将主备ECS的IP转发功能全都关闭。

1. 打开浏览器，并输入EIP地址（124.X.X.187），通过网页确认主ECS。
   网页如下图所示，表示此时主ECS是ECS-HA1。

   图 4-13 主 ECS 验证

2. 远程登录备ECS，本示例是ECS-HA2。
   ECS有多种登录方法，具体请参见**登录弹性云服务器**。
3. 请根据ECS的操作系统，在**表4-7**中选择关闭IP转发功能的操作，本示例ECS为Linux操作系统。

表 4-7 关闭 IP 转发功能

操作系统	操作指导
Linux系统	1. 执行以下命令，切换root用户。 **su root** 2. 执行以下命令，查看IP转发功能是否已开启。 **cat /proc/sys/net/ipv4/ip_forward** 回显结果：1为开启，0为关闭，默认为0。 ● 回显为0，任务结束。 ● 回显为1，继续执行以下操作。 3. 以下提供两种方法修改配置文件，二选一即可。 方法一： a. 执行以下命令，打开“/etc/sysctl.conf”文件。 **vim /etc/sysctl.conf** b. 按**i**进入编辑模式。 c. 修改net.ipv4.ip_forward = 0。 d. 按**ESC**退出，并输入**:wq!**保存配置。 方法二： 执行sed命令，命令示例如下： **sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf** 4. 执行以下命令，使修改生效。 **sysctl -p /etc/sysctl.conf**
Windows系统	1. 在搜索框中输入**cmd**，打开Windows系统的“命令提示符”窗口，执行以下命令。 **ipconfig/all** ● 回显结果中，“IP 路由已启用”为 “否”， 表示IP转发功能已关闭。 ● 回显结果中，“IP 路由已启用”为 “是”， 表示IP转发功能未关闭，继续执行以下操作。 2. 在搜索框中输入**regedit**，打开注册表编辑器。 3. 编辑**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**下的**IPEnableRouter**值为0。 ● 指定值为 0：关闭 IP 转发。 ● 指定值为 1：启用 IP 转发。

步骤五：验证主备 ECS 的自动切换功能

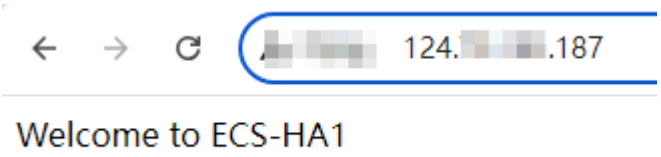
1. 执行以下操作，分别重启主备ECS。
   a. 远程登录ECS-HA1。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。
   b. 执行以下命令，重启ECS-HA1。
      reboot

c. 参考1.a~1.b，重启ECS-HA2。

2. 执行以下操作，验证主ECS的网页访问情况。

a. 打开浏览器，并输入EIP地址（124.X.X.187），验证主ECS的网页访问情况。网页如下图所示，表示此时主ECS是ECS-HA1，且网页访问正常。

图 4-14 主 ECS 验证（ECS-HA1）



b. 远程登录ECS-HA1，并执行以下命令，查看虚拟IP是否已绑定到ECS-HA1的eth0网卡上。

ip addr show

回显类似如下信息，可以看到虚拟IP（192.168.0.177）已绑定至eth0网卡上，再次确认ECS-HA1为主ECS。

```
[root@ecs-ha1 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:fe:56:19 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.195/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0
       valid_lft 107898685sec preferred_lft 107898685sec
    inet 192.168.0.177/32 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fefe:5619/64 scope link
       valid_lft forever preferred_lft forever
```

c. 执行以下命令，停止主ECS的Keepalived服务，本示例中主ECS为ECS-HA1。

systemctl stop keepalived.service

3. 执行以下命令，验证主ECS是否切换成ECS-HA2。

a. 远程登录ECS-HA2，并执行以下命令，查看虚拟IP是否已绑定到ECS-HA2的eth0网卡上。

ip addr show

回显类似如下信息，可以看到虚拟IP（192.168.0.177）已绑定至eth0网卡上，此时确认ECS-HA2为主ECS。

```
[root@ecs-ha2 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:fe:56:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.233/24 brd 192.168.0.255 scope global noprefixroute dynamic eth0
       valid_lft 107898091sec preferred_lft 107898091sec
    inet 192.168.0.177/32 scope global eth0
```

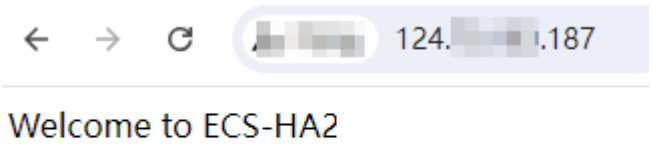


```
    valid_lft forever preferred_lft forever
inet6 fe80::f816:3eff:fefe:563f/64 scope link
    valid_lft forever preferred_lft forever
```

b. 打开浏览器，并输入EIP地址（124.X.X.187），验证ECS-HA2作为主ECS时的网页访问情况。

网页如下图所示，表示此时主ECS是ECS-HA2，且网页访问正常。

图 4-15 主 ECS 验证（ECS-HA2）



Welcome to ECS-HA2

5 弹性网卡和辅助弹性网卡

5.1 弹性网卡

5.1.1 弹性网卡概述

弹性网卡（Elastic Network Interfaces，以下简称ENI）即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的云服务器实例（包括弹性云服务器和裸金属服务器）上，实现灵活、高可用的网络方案配置。

弹性网卡类型

- 主弹性网卡：在创建实例时，随实例默认创建的弹性网卡称作主弹性网卡。无法解除主弹性网卡和实例的绑定关系。
- 扩展弹性网卡：您在弹性网卡控制台创建的是扩展弹性网卡，可以将网卡绑定到实例上，也可以解除网卡和实例的绑定关系。

弹性网卡应用场景

- 灵活迁移

  通过将弹性网卡从云服务器实例解绑后再绑定到另外一台服务器实例，保留已绑定私网IP、弹性公网IP和安全组策略，无需重新配置关联关系，将故障实例上的业务流量快速迁移到备用实例，实现服务快速恢复。
- 业务分离管理

  可以为服务器实例配置多个分属于同一VPC内不同子网的弹性网卡，特定网卡分别承载云服务器实例的内网、外网、管理网流量。针对子网可独立设置访问安全控制策略与路由策略，弹性网卡也可配置独立安全组策略，从而实现网络隔离与业务流量分离。

弹性网卡的使用限制

- 云服务器可绑定的扩展弹性网卡数量由云服务器实例规格决定，具体请参见**规格清单**。
- 扩展弹性网卡不支持直接访问华为云内公共云服务，如内网DNS等，推荐使用VPCEP访问华为云公共云服务，具体参见**购买连接“接口”型终端节点服务的终端节点**。

5.1.2 创建弹性网卡

操作场景

主弹性网卡随实例默认创建，您可以参考以下操作，在弹性网卡控制台创建扩展弹性网卡。

约束与限制

通过管理控制台创建的扩展弹性网卡，必须和其绑定的实例属于同一个虚拟私有云，可以属于不同安全组。

说明

此限制仅针对管理控制台，通过API创建扩展弹性网卡可以与其绑定的实例属于不同的虚拟私有云。

操作步骤

1. 进入**弹性网卡列表页面**。
2. 单击“创建弹性网卡”。
3. 配置弹性网卡参数，如**表5-1**所示。

表 5-1 参数说明

参数	参数说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-上海一
名称	输入弹性网卡的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	networkInterface-891e
虚拟私有云	选择弹性网卡所属的VPC。	vpc-001
所属子网	选择弹性网卡所属的子网。	subnet-001
IPv4地址	为弹性网卡分配IPv4类型的私有IP地址，当前支持以下两种分配私有IP地址的方式： • 自动分配IP地址：表示系统自动从子网网段中选取一个IP地址。 • 手动指定IP地址：表示您可以自行从子网网段中选取一个IP地址。 若选择“手动指定IP地址”，则填写IPv4私有IP地址。	192.168.0.15
安全组	选择弹性网卡所属安全组。	sg-001

4. 单击“确定”，完成创建。

5.1.3 查看弹性网卡基本信息

操作场景

您可以在控制台查看您所拥有的弹性网卡基本信息，包括名称、ID、类型、所属VPC、绑定的实例及关联的安全组等信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击目标弹性网卡的私有IP地址。

其他操作

在弹性网卡详情页可以修改以下信息：

- 根据页面提示修改弹性网卡名称、服务地址信息、绑定解绑实例等。
- 设置中止时删除功能：
  - 关闭：系统默认关闭中止时删除功能，当弹性网卡与对应实例解绑，或对应实例被删除时，弹性网卡不会被同步删除，您可以将该弹性网卡绑定至其他实例。
  - 开启：中止时删除功能开启时，解绑实例后将默认删除弹性网卡。

  当前仅有部分区域支持中止时删除功能，请以控制台实际显示为准。

5.1.4 将弹性网卡绑定至云服务器实例

操作场景

通过将弹性网卡与弹性云服务器或裸金属服务器绑定，可以实现灵活、高可用的网络方案配置。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击操作列的“绑定实例”，选择需要绑定的云服务器实例。

6. 单击“确定”，完成绑定。

相关操作

弹性网卡绑定服务器后，建议您设置网卡多队列以提升网络性能，具体请参见**开启网卡多队列功能**。

5.1.5 将弹性网卡绑定至弹性公网 IP

操作场景

通过将弹性公网IP与弹性网卡绑定，您可以构建更灵活，扩展性更强的IT解决方案。

弹性网卡本身提供一个私网IP，与弹性公网IP绑定后，相当于同时具备了私网IP和公网IP。弹性网卡和弹性公网IP的绑定关系不随弹性网卡解绑云服务器而变化，当弹性网卡从云服务器上迁移时，即可同时完成私网IP和公网IP的迁移。

一个云服务器可以绑定多个弹性网卡，当为每个弹性网卡分别绑定一个弹性公网IP时，这个云服务器就拥有了多个弹性公网IP，可以提供更灵活的外部访问服务。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击操作列的“绑定弹性公网IP”，选择需要绑定的弹性公网IP。
6. 单击“确定”，完成绑定。

5.1.6 将弹性网卡绑定至虚拟 IP 地址

操作场景

通过将弹性网卡与虚拟IP绑定，使用户可以通过绑定的虚拟IP访问该弹性网卡绑定的服务器。

未绑定云服务器实例的弹性网卡不能绑定虚拟IP。

更多虚拟IP信息请参见**虚拟IP地址概述**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。

4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击操作列的“更多 > 绑定虚拟IP”。
   进入虚拟IP列表页。
6. 在需要绑定的虚拟IP操作列，单击“绑定服务器”。
7. 选择服务器及网卡，单击“确定”。

5.1.7 将弹性网卡和云服务器或弹性公网 IP 解绑定

操作场景

本章节指导您如何将弹性网卡与云服务器或弹性公网IP进行解绑。

约束与限制

- 当弹性网卡的“中止时删除”功能开启时，解绑实例时，会同步删除弹性网卡。
  - 删除弹性网卡时，会同步删除弹性网卡绑定的辅助弹性网卡，并清理实例内部对应的VLAN子接口。
  - 删除弹性网卡时，会解除网卡和弹性公网IP的绑定关系。
- 当弹性网卡的“中止时删除”功能关闭时，解绑实例时，只是解除弹性网卡和实例的绑定关系，不会删除弹性网卡。
  如果弹性网卡已绑定弹性公网IP，则解绑实例时，不仅解除弹性网卡和实例的绑定关系，也会同步解除弹性网卡和弹性公网IP的绑定关系。

说明

解除弹性网卡和弹性公网IP的绑定关系后，如果不释放弹性公网IP，将会继续收取费用，您可以将其绑定给其他云资源使用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击操作列的“解绑实例”或“解绑弹性公网IP”。
6. 单击“确定”，完成解绑。
   解绑弹性公网IP时，可选择同时释放该弹性公网IP。

5.1.8 更改弹性网卡所属的安全组

操作场景

您可以在弹性网卡列表页更改所属安全组，也可以进入弹性网卡详情页更改所属安全组。

操作步骤

在弹性网卡列表页，更改所属安全组

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表页，单击操作列的“更多 > 更改安全组”。
6. 在“更改安全组”页面勾选需要关联的安全组，单击“确定”，完成更改。

在弹性网卡详情页，更改所属安全组

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 单击目标弹性网卡的私有IP地址，进入弹性网卡详情页。
6. 在“关联安全组”页签下，单击“更改安全组”。
7. 在“更改安全组”页面勾选需要关联的安全组，单击“确定”，完成更改。

更多操作

您可以在弹性网卡详情页的“关联安全组”页签下，单击安全组所在行的“配置规则”按钮，对安全组规则进行配置。配置安全组规则请参见**添加安全组规则**。

5.1.9 删除弹性网卡

操作场景

本章节指导用户删除不再使用的弹性网卡资源。

约束与限制

- 主弹性网卡跟随实例一同创建，您不能直接删除主弹性网卡，也不能解除主弹性网卡和实例的绑定关系，需要删除主弹性网卡绑定的实例，该网卡将被同步删除。
- 当扩展弹性网卡已绑定实例时，无法直接删除，请**解绑实例**后重试。
- 删除弹性网卡时，会同步删除弹性网卡绑定的辅助弹性网卡。
- 删除弹性网卡时，会解除网卡和弹性公网IP的绑定关系，您可以选择是否释放该弹性公网IP。

  如果不释放弹性公网IP，将会继续收取费用，您可以将其绑定给其他云资源使用。
- 删除弹性网卡时，如果弹性网卡已被其他资源使用，会同步删除关联资源中使用弹性网卡的条目，删除操作无法恢复，请谨慎操作。

比如，在VPC路由表中，存在自定义路由的下一跳是弹性网卡，则删除弹性网卡时，则会同步删除相关路由。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在弹性网卡列表中，选择目标弹性网卡所在行的操作列下的“更多 > 删除”。弹出删除确认对话框。
6. 根据界面提示完成信息确认后，删除弹性网卡。

5.2 辅助弹性网卡

5.2.1 辅助弹性网卡概述

辅助弹性网卡是一种基于弹性网卡的衍生资源，用于解决单个云服务器实例挂载的弹性网卡超出上限，不满足用户使用需要的问题。辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个云服务器实例挂载更多网卡，实现灵活、高可用的网络方案配置。

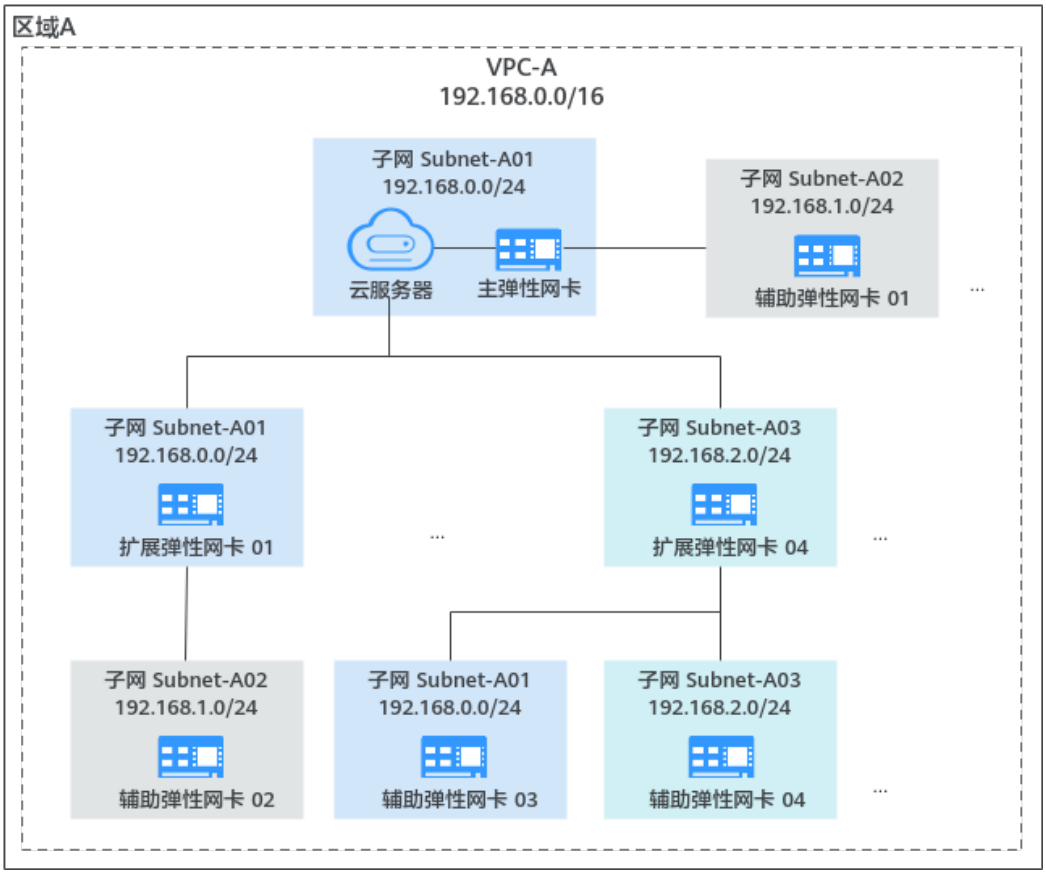
辅助弹性网卡应用场景

单个云服务器实例支持绑定的弹性网卡数量有限，当因业务需要绑定超过弹性网卡上限的网卡时，可以通过为弹性网卡挂载辅助弹性网卡实现。

- 为云服务器实例配置多个分属于同一VPC内不同子网的辅助弹性网卡，每个辅助弹性网卡拥有不同的私网IP、弹性公网IP，可以分别承载云服务器实例的内网、外网和管理网流量。
- 辅助弹性网卡可配置独立安全组策略，从而实现网络隔离与业务流量分离。

辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，其组网示意图如图5-1所示，云服务器的主网卡和扩展网卡均支持挂载辅助弹性网卡。

图 5-1 辅助弹性网卡挂载示意图



辅助弹性网卡的使用限制

- 单个云服务器实例支持绑定的辅助弹性网卡实例上限为256个，但不是所有规格的云服务器实例均支持绑定256个辅助弹性网卡，具体可绑定的辅助弹性网卡数量由云服务器实例规格决定。支持辅助弹性网卡的云服务器实例规格如下：

  弹性云服务器规格：C7、S7、M7，规格详情请参见**规格清单**。

  云容器节点规格：c6ne
- 云服务器实例不支持通过辅助弹性网卡的私网IP使用CloudInit。
- 辅助弹性网卡不支持绑定虚拟IP。
- 不支持单独收集辅助弹性网卡的流日志，辅助弹性网卡的流日志信息跟随所属的弹性网卡一同生成。

5.2.2 创建辅助弹性网卡

操作场景

当实例所需挂载的弹性网卡超过上限时，您可以参考以下操作创建辅助弹性网卡，辅助弹性网卡可以挂载在实例的弹性网卡上（包括主网卡和扩展网卡）。通过辅助弹性网卡功能，您可以为实例挂载更多网卡，实现灵活、高可用的网络方案配置。

约束与限制

- 辅助弹性网卡与所属的弹性网卡必须在同一个虚拟私有云，可以属于不同子网以及安全组。

- 辅助弹性网卡创建完成后，您需要在实例的弹性网卡上创建VLAN子接口并配置对应规则，具体请参见**配置辅助弹性网卡**。

创建辅助弹性网卡

1. 进入**辅助弹性网卡列表页面**。
2. 在页面右上角，单击“创建辅助弹性网卡”。
3. 配置辅助弹性网卡参数，如**表5-2**所示。

表 5-2 参数说明

参数	参数说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-上海一
所属弹性网卡	辅助弹性网卡所挂载的弹性网卡。 您可以通过下拉列表框选择支持挂载辅助弹性网卡的弹性网卡。	--(172.16.0.145)
所属VPC	辅助弹性网卡所在的VPC，和其所属弹性网卡的VPC保持一致，无需填写。	vpc-A
所属子网	选择辅助弹性网卡所在的子网，辅助弹性网卡和所属弹性网卡可以位于不同子网，请根据实际情况设置。	subnet-A01
创建数量	待创建的辅助弹性网卡的数量。	1
私有IP地址	选择为辅助弹性网卡申请的私有IP地址类型。 • IPv4：支持IPv4私网访问。 • IPv6：支持IPv6私网和公网访问。 当辅助弹性网卡所属子网开启IPv6时，您才可以选择IPv6。	IPv4
IPv4地址	为辅助弹性网卡分配IPv4类型的私有IP地址，当前支持以下两种分配私有IP地址的方式： • 自动分配IP地址：表示系统自动从子网网段中选取一个IP地址。 • 手动指定IP地址：表示您可以自行从子网网段中选取一个IP地址。 若选择“手动指定IP地址”，则填写IPv4私有IP地址。	自动分配IP地址

参数	参数说明	取值样例
IPv6地址	如果“私有IP地址”参数选择了“IPv6”，则需要设置IPv6地址。 为辅助弹性网卡分配IPv6类型的私有IP地址，当前支持以下两种分配私有IP地址的方式： • 自动分配IP地址：表示系统自动从子网网段中选取一个IP地址。 • 手动指定IP地址：表示您可以自行从子网网段中选取一个IP地址。 若选择“手动指定IP地址”，则填写IPv6私有IP地址。	自动分配IP地址
安全组	选择辅助弹性网卡所属安全组。	sg-001
描述	辅助弹性网卡的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

4. 单击“立即创建”，完成创建。

须知

辅助网卡创建完成后不能直接使用，您还需要**配置辅助弹性网卡**，在弹性网卡上为辅助弹性网卡创建VLAN子接口等。

配置辅助弹性网卡

当通过管理控制台创建辅助弹性网卡后，您需要参考以下操作，在实例的弹性网卡上，为该辅助弹性网卡创建VLAN子接口并配置私有IP地址、默认路由规则等。

在配置辅助弹性网卡之前，您需要根据以下说明获取辅助弹性网卡，以及辅助弹性网卡所属的弹性网卡信息。

- 配置Linux ECS的辅助弹性网卡，需要获取**表5-3**中的辅助弹性网卡及其所属子网的信息。
- 配置Windows ECS的辅助弹性网卡，需要获取**表5-3**中的辅助弹性网卡及其所属子网的信息、**表5-4**中的弹性网卡及其所属子网的信息。

表 5-3 辅助弹性网卡及子网信息

信息	获取方法
辅助弹性网卡的VLAN 辅助弹性网卡的MAC地址 辅助弹性网卡的私有IP地址	1. 在辅助弹性网卡列表中，单击辅助弹性网卡私有IP地址。 进入网卡基本信息页面。 2. 在基本信息页面，查看并记录辅助弹性网卡的以下信息： ● VLAN ● MAC地址 ● 私有IP地址
辅助弹性网卡所属子网的掩码 辅助弹性网卡所属子网的网关	1. 在辅助弹性网卡列表中，单击“所属网络”的子网名称超链接。 进入子网基本信息页面。 2. 在基本信息页面，查看并记录子网的以下信息： ● 子网掩码：子网IPv4网段中的掩码，比如子网IPv4网段为192.168.0.0/24，则掩码为24。 ● 子网网关：在“网关和DNS”区域，查看网关地址。

表 5-4 辅助弹性网卡所属的弹性网卡及子网信息

信息	获取方法
弹性网卡的MAC地址 弹性网卡的私有IP地址	1. 在ECS列表中，单击ECS名称。 进入ECS基本信息页面。 2. 选择“弹性网卡”页签，单击 ⌄ 展开弹性网卡的折叠区域，查看并记录弹性网卡的以下信息： ● MAC地址 ● 私有IP地址
弹性网卡所属子网的掩码 弹性网卡所属子网的网关	1. 在弹性网卡列表中，单击“所属网络”的子网名称超链接。 进入子网基本信息页面。 2. 在基本信息页面，查看并记录子网的以下信息： ● 子网掩码：子网IPv4网段中的掩码，比如子网IPv4网段为192.168.0.0/24，则掩码为24。 ● 子网网关：在“网关和DNS”区域，查看网关地址。

Linux 系统

本操作以CentOS 7.8为例，在ECS的弹性网卡上为辅助弹性网卡配置VLAN子接口。本示例中，辅助弹性网卡及其所属子网的信息如下：

- VLAN：1937
- MAC地址：fa:16:3e:6d:c5:5a
- 私有IP地址：192.168.0.149
- 所属子网的掩码：24
- 所属子网的网关：192.168.0.1

说明

本示例中辅助弹性网卡所属的弹性网卡为ECS的主网卡，如果您需要为ECS的扩展网卡配置辅助弹性网卡，则操作类似。

1. 登录ECS实例。

   登录方式请参见**Linux弹性云服务器登录方式概述**。

2. 执行以下命令，查看并记录ECS实例的弹性网卡名称。

   ifconfig

   回显类似如下信息，本示例中，弹性网卡的名称为eth0。

   ```
   [root@ecs-subeni-linux ~]# ifconfig
   eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
         inet 192.168.0.125  netmask 255.255.255.0  broadcast 192.168.0.255
         inet6 fe80::f816:3eff:fe6d:c542  prefixlen 64  scopeid 0x20<link>
         ether fa:16:3e:6d:c5:42  txqueuelen 1000  (Ethernet)
         RX packets 78131  bytes 111604802 (106.4 MiB)
         RX errors 0  dropped 0  overruns 0  frame 0
         TX packets 8686  bytes 1422159 (1.3 MiB)
         TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
   ...
   ```

3. 执行以下命令，在弹性网卡上创建VLAN子接口。

   ip link add link *弹性网卡名称* **name** *VLAN子接口名称* **type vlan id** *辅助弹性网卡的VLAN*

   命令中的参数说明如下：

   - 弹性网卡名称：2中查询到的网卡名称，本示例为**eth0**。
   - VLAN子接口名称：建议命名规则采用“弹性网卡名称.辅助弹性网卡的VLAN”，本示例为**eth0.1937**。
   - 辅助弹性网卡的VLAN：本示例为**1937**。

   命令示例：

   ip link add link eth0 name eth0.1937 type vlan id 1937

4. 执行以下命令，创建命名空间。

   ip netns add *命名空间名称*

   命名空间名称：建议命名规则采用“ns辅助弹性网卡VLAN”，本示例为**ns1937**。

   命令示例：

   ip netns add ns1937

5. 执行以下命令，将已创建的VLAN子接口加入到命名空间中。

   ip link set *VLAN子接口名称* **netns** *命名空间名称*

   命令示例：

   ip link set eth0.1937 netns ns1937

6. 执行以下命令，将VLAN子接口的MAC地址修改为辅助弹性网卡的MAC地址。

   ip netns exec *命名空间名称* **ifconfig** *VLAN子接口名称* **hw ether** *辅助弹性网卡的MAC地址*

命令示例：

ip netns exec ns1937 ifconfig eth0.1937 hw ether fa:16:3e:6d:c5:5a

7. 执行以下命令，启动VLAN子接口。

   ip netns exec *命名空间名称* **ifconfig** *VLAN子接口名称* **up**

   命令示例：

   ip netns exec ns1937 ifconfig eth0.1937 up

8. 执行以下命令，为VLAN子接口配置私有IP地址。

   ip netns exec *命名空间名称* **ip addr add** *私有IP地址* **dev** *VLAN子接口名称*

   私有IP地址：辅助弹性网卡的私有IP地址/辅助弹性网卡所属子网的掩码，本示例为**192.168.0.149/24**。

   命令示例：

   ip netns exec ns1937 ip addr add 192.168.0.149/24 dev eth0.1937

9. 执行以下命令，为VLAN子接口配置默认路由。

   ip netns exec *命名空间名称* **ip route add default via** *辅助弹性网卡所属子网的网关*

   命令示例：

   ip netns exec ns1937 ip route add default via 192.168.0.1

10. 执行以下命令，验证辅助弹性网卡的配置是否生效。

    a. 执行以下命令，验证弹性网卡和测试ECS的网络通信情况。

       ping *测试ECS的私有IP地址*

       建议测试ECS和弹性网卡所在的ECS位于同一个VPC中，并且使用同一个安全组，此时两个ECS网络默认互通。

       命令示例：

       ping 192.168.0.133

       回显类似如下信息，表示通信正常。当弹性网卡和测试ECS通信正常时，再执行**10.b**验证辅助弹性网卡的通信情况。

       ```
       [root@ecs-subeni-linux ~]# ping 192.168.0.133
       PING 192.168.0.133 (192.168.0.133) 56(84) bytes of data.
       64 bytes from 192.168.0.133: icmp_seq=1 ttl=64 time=0.302 ms
       64 bytes from 192.168.0.133: icmp_seq=2 ttl=64 time=0.262 ms
       ...
       --- 192.168.0.133 ping statistics ---
       2 packets transmitted, 2 received, 0% packet loss, time 999ms
       rtt min/avg/max/mdev = 0.262/0.282/0.302/0.020 ms
       ```

    b. 执行以下命令，验证辅助弹性网卡和测试ECS的网络通信情况。

       ip netns exec *命名空间名称* **ping** *测试ECS的私有IP地址*

       建议测试ECS和辅助弹性网卡所在的ECS位于同一个VPC中，并且使用同一个安全组，此时两个ECS网络默认互通。

       命令示例：

       ip netns exec ns1937 ping 192.168.0.133

       回显类似如下信息，表示通信正常，说明辅助弹性网卡的配置已生效。

       ```
       [root@ecs-subeni-linux ~]# ip netns exec ns1937 ping 192.168.0.133
       PING 192.168.0.133 (192.168.0.133) 56(84) bytes of data.
       64 bytes from 192.168.0.133: icmp_seq=1 ttl=64 time=0.420 ms
       64 bytes from 192.168.0.133: icmp_seq=2 ttl=64 time=0.233 ms
       ...
       --- 192.168.0.133 ping statistics ---
       ```



```
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.233/0.326/0.420/0.095 ms
```

须知

- 以上配置的路由为临时路由，配置完立即生效，当ECS重启后临时路由会丢失。请继续执行11配置永久路由，避免ECS重启后网络中断。
- 如果ECS需要通过辅助弹性网卡访问外部域名，则需要为辅助弹性网卡配置DNS，请继续执行11，重启ECS后DNS配置才会生效。

11. 执行以下步骤，为辅助弹性网卡配置永久路由和DNS，该配置重启ECS后会生效。
    a. 执行以下步骤，为辅助弹性网卡配置永久路由。
        i. 执行以下命令，打开“/etc/rc.local”文件。
        vi /etc/rc.local
        ii. 按**i**进入编辑模式。
        iii. 在文件末尾添加以下配置。
        该配置中参数需要和3~9中的命令保持一致。
        ```
        ip link add link eth0 name eth0.1937 type vlan id 1937
        ip netns add ns1937
        ip link set eth0.1937 netns ns1937
        ip netns exec ns1937 ifconfig eth0.1937 hw ether fa:16:3e:6d:c5:5a
        ip netns exec ns1937 ifconfig eth0.1937 up
        ip netns exec ns1937 ip addr add 192.168.0.149/24 dev eth0.1937
        ip netns exec ns1937 ip route add default via 192.168.0.1
        ```
        iv. 按**ESC**退出，并输入**:wq!**保存配置。
        v. 执行以下命令，为“/etc/rc.local”文件添加执行权限。
        chmod +x /etc/rc.local

        说明

        如果您的操作系统为Redhat、EulerOS，执行完11.a.v后，还需要执行以下命令，权限才会添加成功。

        chmod +x /etc/rc.d/rc.local

    b. （可选）如果ECS需要通过辅助弹性网卡访问外部域名，则请执行以下步骤，为辅助弹性网卡配置DNS。
    如果不需要DNS，请直接执行11.c重启ECS。
        i. 执行以下命令，进入/etc/sysconfig/network-scripts/路径，该路径下存放网络接口配置文件。
        cd /etc/sysconfig/network-scripts/
        ii. 执行以下命令，修改弹性网卡的网络接口配置文件。
        vi ifcfg-*弹性网卡名称*
        弹性网卡名称：2中查询到的网卡名称，命令示例为**vi ifcfg-eth0**。
        iii. 按**i**进入编辑模式。
        iv. 在文件末尾添加以下配置。
        其中，114.114.114.114为公共DNS地址。
        ```
        DNS1=114.114.114.114
        ```
        v. 按**ESC**退出，并输入**:wq!**保存配置。

c. 执行以下命令，重启ECS。

reboot

d. 参考**10**，验证永久路由配置是否生效。

e. （可选）如果配置了DNS，则请执行以下步骤，验证DNS配置是否生效。

i. 为辅助弹性网卡绑定EIP，具体请参见**将辅助弹性网卡和弹性公网IP绑定/解绑定**。

ii. 执行以下命令，验证辅助弹性网卡是否可以访问公网域名。

ip netns exec *命名空间名称* **ping** *公网域名*

命令示例：

ip netns exec ns1937 ping support.huaweicloud.com

回显类似如下信息，表示通信正常，说明辅助弹性网卡的DNS配置已生效。

```
[root@ecs-subeni-linux ~]# ip netns exec ns1937 ping support.huaweicloud.com
PING support.huaweicloud.com (36.150.72.70) 56(84) bytes of data.
64 bytes from 36.150.72.70 (36.150.72.70): icmp_seq=1 ttl=54 time=2.68 ms
64 bytes from 36.150.72.70 (36.150.72.70): icmp_seq=2 ttl=54 time=2.61 ms
64 bytes from 36.150.72.70 (36.150.72.70): icmp_seq=3 ttl=54 time=2.60 ms
^C
--- support.huaweicloud.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 2.604/2.633/2.681/0.068 ms
```

12. （可选）如果您需要使用辅助弹性网卡的私有IP地址远程登录所属的ECS，则需要执行以下操作，放通辅助弹性网卡的SSH(22)端口。

a. 在辅助弹性网卡所在安全组中，添加入方向规则放通SSH(22)端口。

具体方法请参见**添加安全组规则**。

表 5-5 安全组规则（放通 SSH(22)端口）

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义 TCP: 22	根据实际情况设置IP地址，比如通过本地PC远程登录ECS，则源地址为本地PC的IP地址。

b. 执行以下命令，检查是否开启命名空间中22端口的监听。

ip netns exec *命名空间名称* **netstat -antp | grep 22**

命令示例：

ip netns exec ns1937 netstat -antp | grep 22

- 如果回显为空，表示未开启命名空间中22端口的监听，请执行**12.c**。
- 如果回显类似如下信息，表示已开启命名空间中22端口的监听，任务结束。

```
[root@ecs-subeni-linux ~]# ip netns exec ns1937 netstat -antp | grep 22
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2797/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      2979/sshd
```

c. 执行以下命令，启动SSH服务，开启22端口的监听。

ip netns exec *命名空间名称* **/sbin/sshd**

命令示例：

ip netns exec ns1937 /sbin/sshd

d. 执行以下命令，检查是否开启命名空间中22端口的监听。

ip netns exec *命名空间名称* **netstat -antp | grep 22**

命令示例：

ip netns exec ns1937 netstat -antp | grep 22

回显类似如下信息，表示已开启命名空间中22端口的监听。

```
[root@ecs-subeni-linux ~]# ip netns exec ns1937 netstat -antp | grep 22
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      2797/sshd
tcp6       0      0 :::22               :::*                LISTEN      2979/sshd
```

13. （可选）如果ECS需要通过辅助弹性网卡对外提供Web访问服务，则需要执行以下操作，放通辅助弹性网卡的HTTP(80)端口。

a. 在辅助弹性网卡所在安全组中，添加入方向规则放通HTTP(80)端口。

具体方法请参见**添加安全组规则**。

表 5-6 安全组规则（放通 HTTP(80)端口）

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义 TCP: 80	0.0.0.0/0 表示允许任意地址访问当前辅助弹性网卡的80端口。

b. 执行以下命令，检查是否开启命名空间中80端口的监听。

ip netns exec *命名空间名称* **netstat -antp | grep 80**

命令示例：

ip netns exec ns1937 netstat -antp | grep 80

- 如果回显为空，表示未开启命名空间中80端口的监听。此时请根据您部署的Web服务，开启相应服务的80端口监听。
- 如果回显类似如下信息，表示已开启命名空间中80端口的监听，任务结束。

```
[root@ecs-subeni-linux ~]# ip netns exec ns1937 netstat -antp | grep 80
tcp6       0      0 :::80               :::*                LISTEN      ...
```

Windows 系统

本操作以Windows Server 2019 Standard 64bit为例，在ECS的弹性网卡上为辅助弹性网卡配置VLAN子接口。本示例中，辅助弹性网卡、主网卡及所属子网的信息如下：

- 辅助弹性网卡：
  - VLAN：1229
  - MAC地址：fa:16:3e:6d:c5:db
  - 私有IP地址：192.168.0.22
  - 所属子网的掩码：24（255.255.255.0）

  - 所属子网的网关：192.168.0.1
- 弹性网卡：
  - MAC地址：fa:16:3e:6d:c5:d5
  - 私有IP地址：192.168.0.16
  - 所属子网的掩码：24（255.255.255.0）
  - 所属子网的网关：192.168.0.1

说明

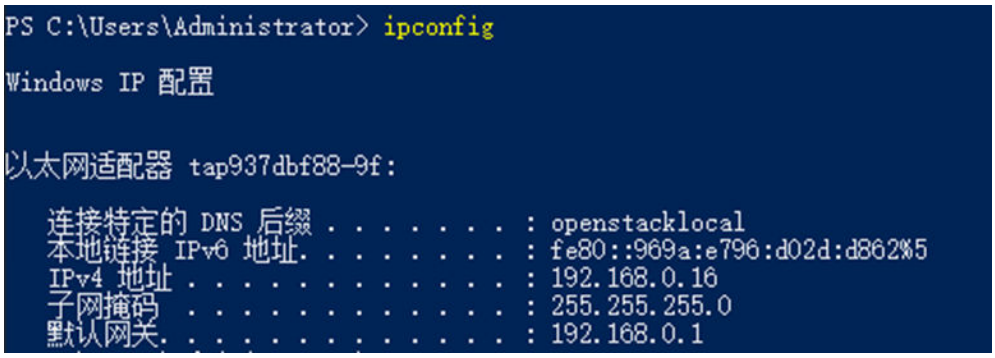
本示例中辅助弹性网卡所属的弹性网卡为ECS的主网卡，如果您需要为ECS的扩展网卡配置辅助弹性网卡，则操作类似。

1. 登录ECS实例。

   登录方式请参见**Windows ECS登录方式概述**。
2. 在桌面的搜索区域输入“Windows PowerShell”，搜索并打开ECS的Windows PowerShell命令行界面。
3. 在Windows PowerShell命令行界面，执行以下命令，查询弹性网卡的以太网适配器信息。

   ipconfig

   回显类似如下信息，查询并记录弹性网卡的以太网适配器信息，本示例中为**tap937dbf88-9f**。

4. 执行以下步骤，使用在OS内组bond的方法配置自定义VLAN网络。

   a. 执行以下命令，创建自定义VLAN网络的bond组。

      New-NetLbfoTeam -Name *bond组名称* **-TeamMembers "***弹性网卡的以太网适配器信息***" -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses -Confirm:$false**

      其中，

      - bond组名称：自定义VLAN网络的bond组成名，本示例为**Team1**。
      - 弹性网卡的以太网适配器信息：3中查询到的信息，本示例为**tap937dbf88-9f**。

      命令示例：

      New-NetLbfoTeam -Name Team1 -TeamMembers "tap937dbf88-9f" -TeamingMode SwitchIndependent -LoadBalancingAlgorithm IPAddresses -Confirm:$false

      回显类似如下信息：


```
PS C:\Users\Administrator> New-NetLbfoTeam -Name Team1 -TeamMembers "tap937dbf88-9f" -TeamingMode SwitchIndependent -
LoadBalancingAlgorithm IPAddresses -Confirm:$false


Name                   : Team1
Members                : tap937dbf88-9f
TeamNics               : Team1
TeamingMode            : SwitchIndependent
LoadBalancingAlgorithm : IPAddresses
Status                 : Up
```

b. 执行以下命令，查询创建成功的bond组。

Get-NetLbfoTeamMember

回显类似如下信息：

```
PS C:\Users\Administrator> Get-NetLbfoTeamMember


Name                      : tap937dbf88-9f
InterfaceDescription      : Red Hat VirtIO Ethernet Adapter
Team                      : Team1
AdministrativeMode        : Active
OperationalStatus         : Active
TransmitLinkSpeed(Gbps)   : 100
ReceiveLinkSpeed(Gbps)    : 100
FailureReason             : NoFailure
```

Get-NetAdapter

回显类似如下信息：

```
PS C:\Users\Administrator> Get-NetAdapter

Name                      InterfaceDescription                    ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                    ------- ------       ----------             ---------
tap937dbf88-9f            Red Hat VirtIO Ethernet Adapter               5 Up           FA-16-3E-6D-C5-D5      100 Gbps
Team1                     Microsoft Network Adapter Multiplexo...       9 Up           FA-16-3E-6D-C5-D5      100 Gbps
```

5. 执行以下步骤，配置自定义VLAN网络。

a. 执行以下命令，创建VLAN子接口。

Add-NetLbfoTeamNIC -Team "*bond组名称***" -VlanID** *辅助弹性网卡的VLAN* **-Confirm:$false**

命令示例

Add-NetLbfoTeamNIC -Team "Team1" -VlanID 1229 -Confirm:$false

回显类似如下信息：

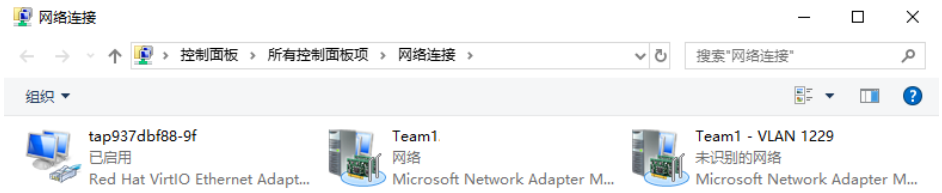
```
PS C:\Users\Administrator> Add-NetLbfoTeamNIC -Team "Team1" -VlanID 1229 -Confirm:$false


Name                      : Team1 - VLAN 1229
InterfaceDescription      : Microsoft Network Adapter Multiplexor Driver #2
Team                      : Team1
VlanID                    : 1229
Primary                   : False
Default                   : False
TransmitLinkSpeed(Gbps)   : 100
ReceiveLinkSpeed(Gbps)    : 100
```

b. 执行以下命令，打开网络连接页面。

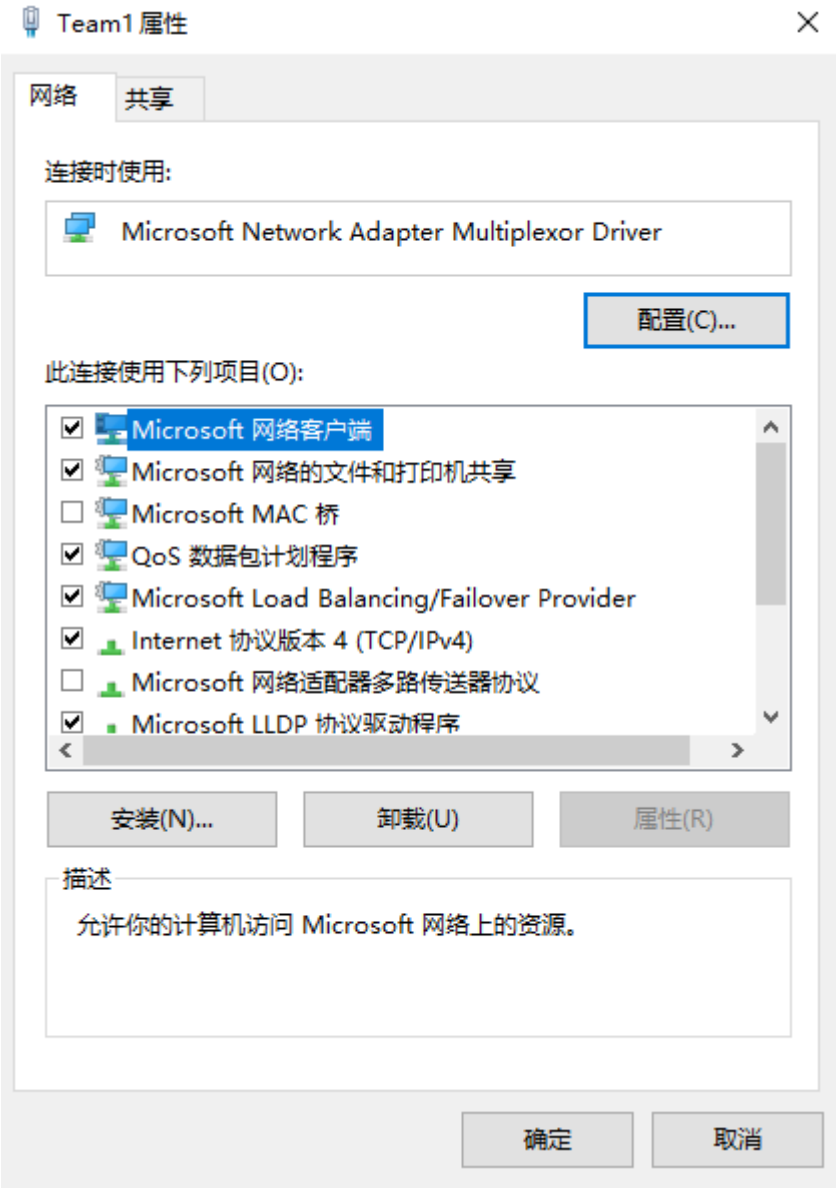
ncpa.cpl

进入网络连接页面，其中，Team1是**4.a**创建的bond组，Team1 - VLAN 1229是**5.a**创建的VLAN子接口。

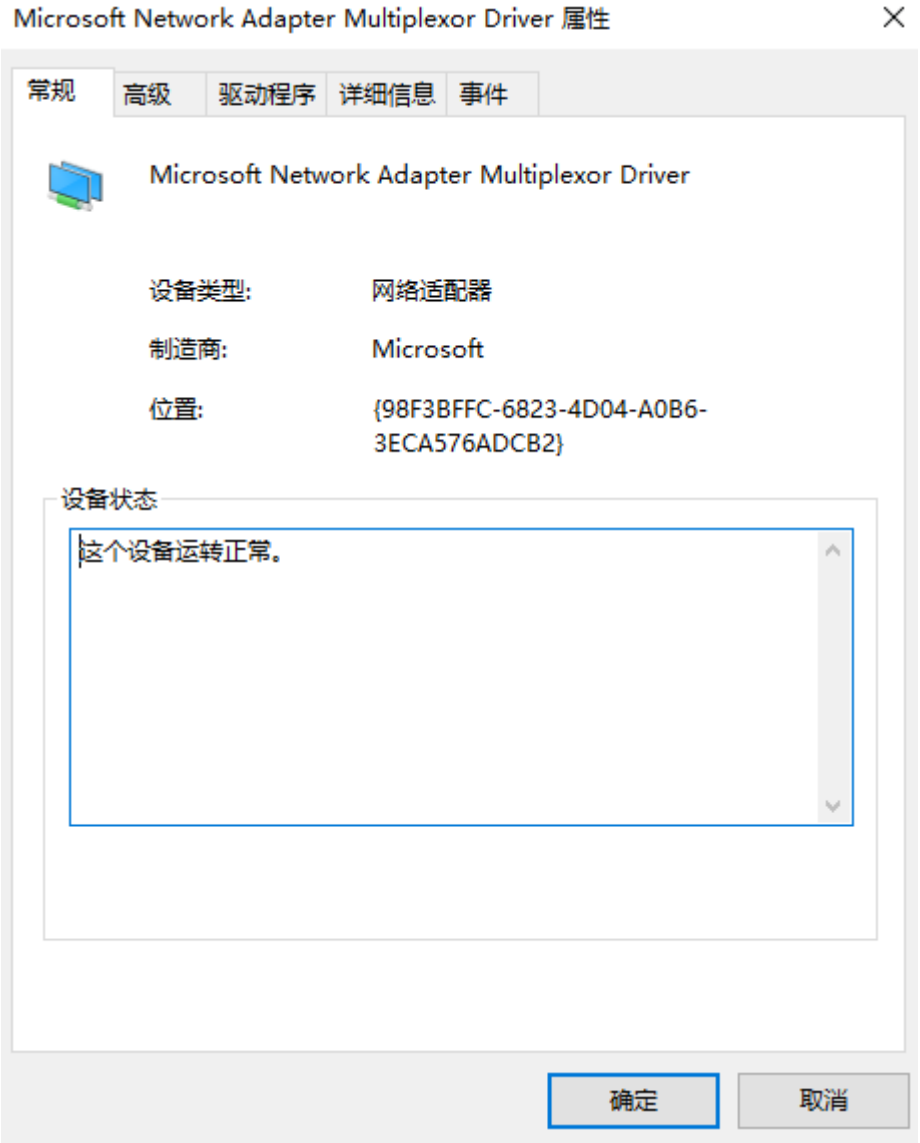


6. 执行以下步骤，配置弹性网卡的网络。
   a. 在网络连接页面，双击Team1。
      进入Team1状态页面。

   b. 在Team1状态页面，单击“属性”。
      进入Team1属性页面。

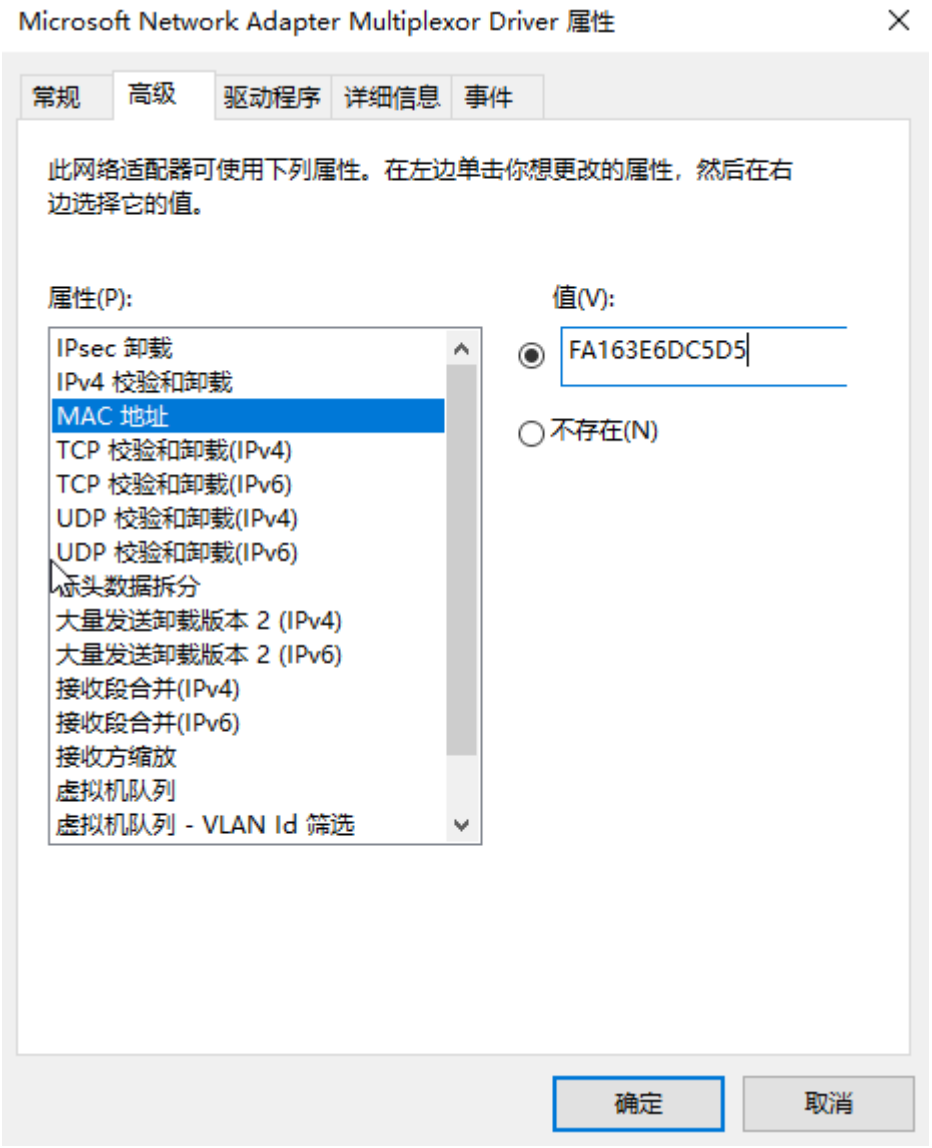


c. 在Team1属性页面，单击“配置(C)...”。
进入Microsoft Network Adapter Multiplexor Driver属性页面。

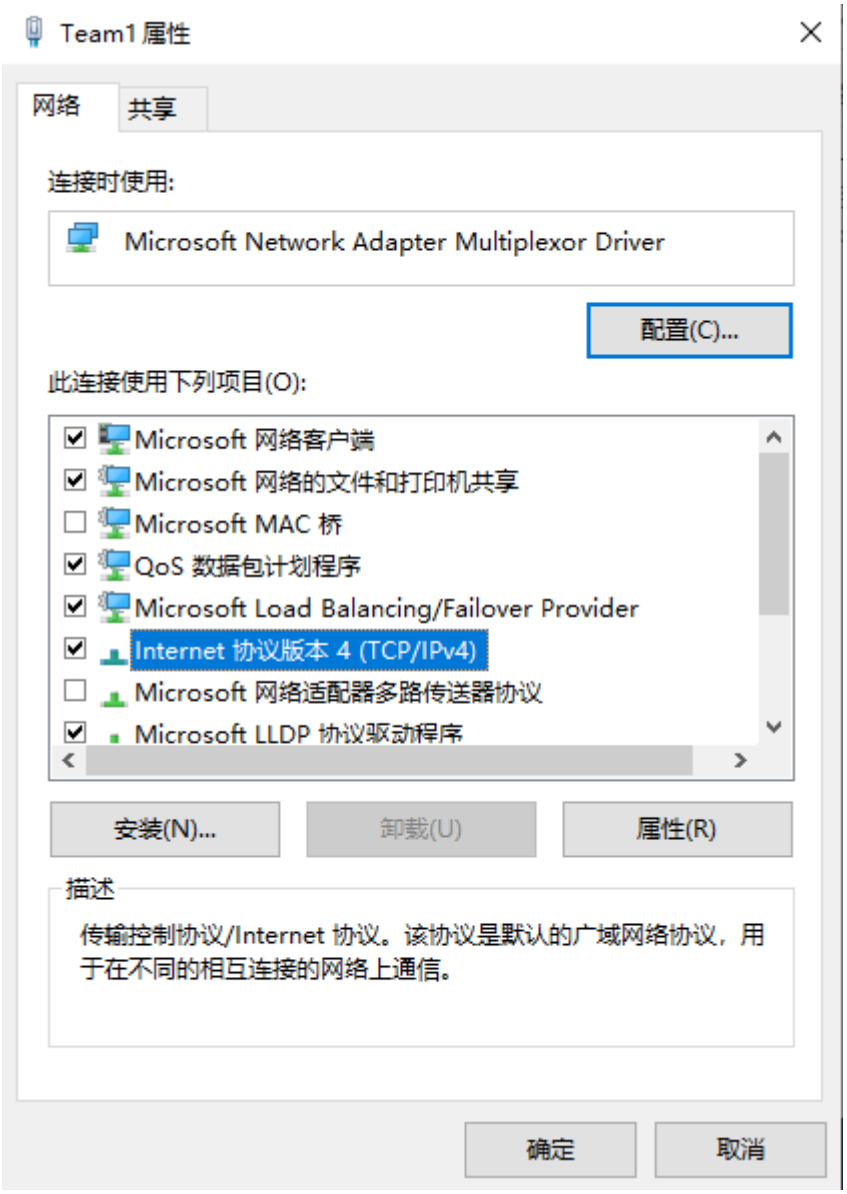


d. 在Microsoft Network Adapter Multiplexor Driver属性页面，选择“高级”页签，在MAC 地址对应的输入框中，输入弹性网卡的MAC地址并单击“确定”。

输入MAC地址时，需要去掉连接符号“:”。本示例中查询到的弹性网卡MAC地址为fa:16:3e:6d:c5:d5，此处输入FA163E6DC5D5。



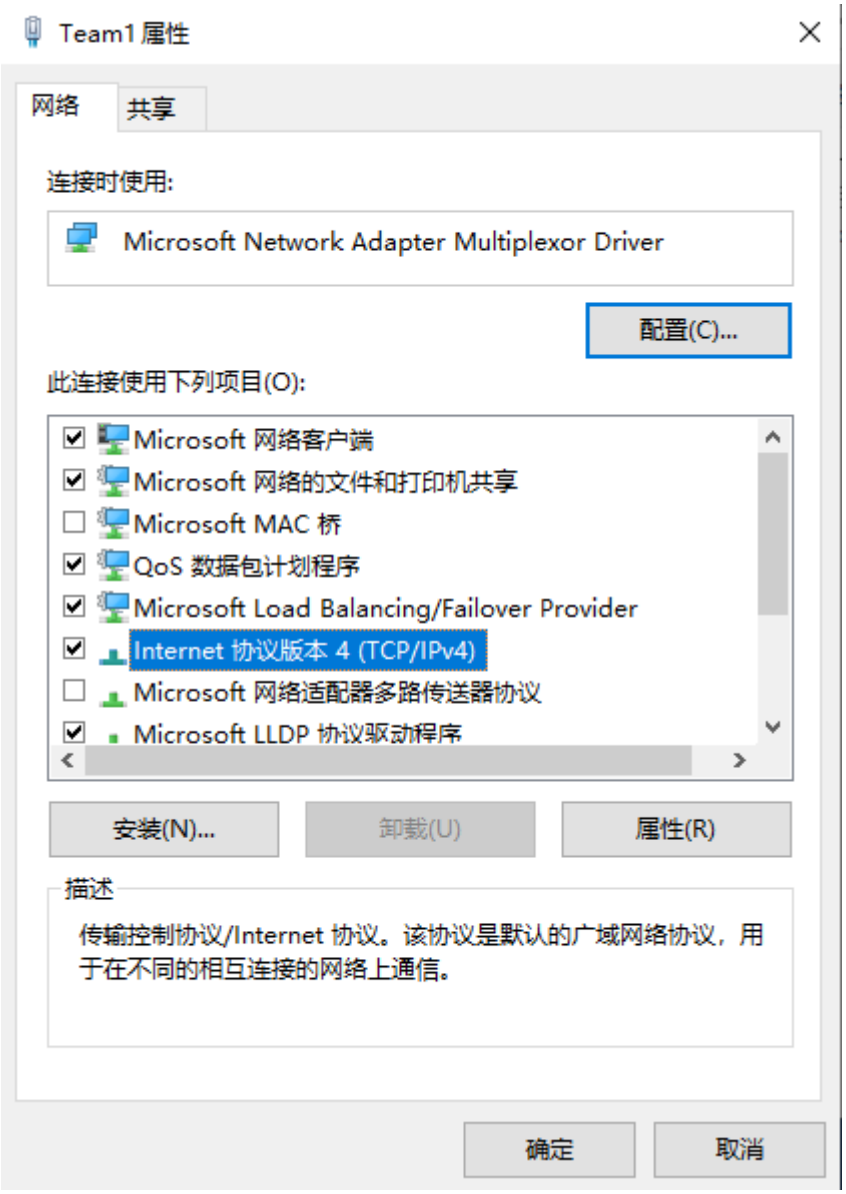
e. 在Team1属性页面，双击“Internet 协议版本 4（TCP/IPv4）”。
打开Internet 协议版本 4（TCP/IPv4）属性页面。



f. 在Internet 协议版本 4（TCP/IPv4）属性页面，配置弹性网卡的网络信息，并单击“确定”。

- 选择“使用下面的IP地址(S)”
- IP地址(I)：输入弹性网卡的私有IP地址，本示例为192.168.0.16。
- 子网掩码(U)：输入弹性网卡所属子网的掩码，本示例为255.255.255.0。
- 默认网关(D)：输入弹性网卡所属子网的网关，本示例为192.168.0.1。

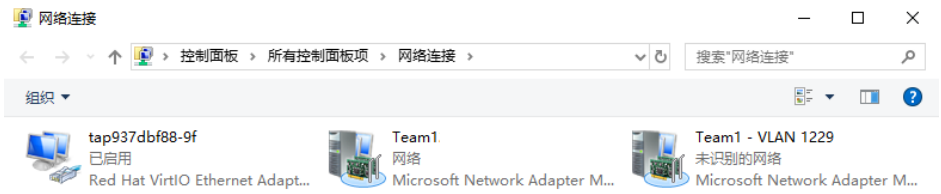
g. 在Team1属性页面，单击“确定”，保存修改。



h. 在Team1状态页面，单击“详细信息(E)...”。
进入网络连接详细信息页面，确认以下信息配置是否正确。

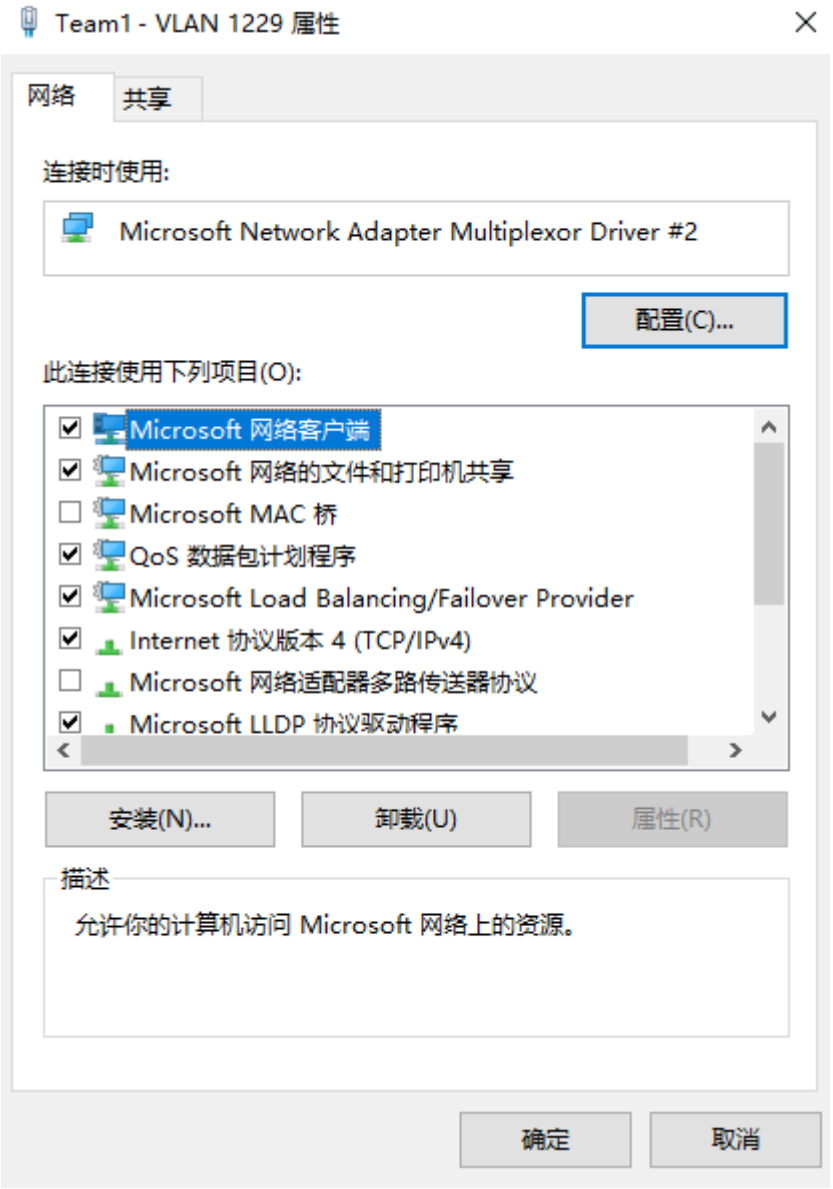
- 物理地址：弹性网卡的MAC地址。
- IPv4 地址：弹性网卡的私有IP地址。
- IPv4 子网掩码：弹性网卡所属子网的掩码。
- IPv4 默认网关：弹性网卡所属子网的网关。

i. 检查无误后，关闭弹窗。
返回网络连接页面。

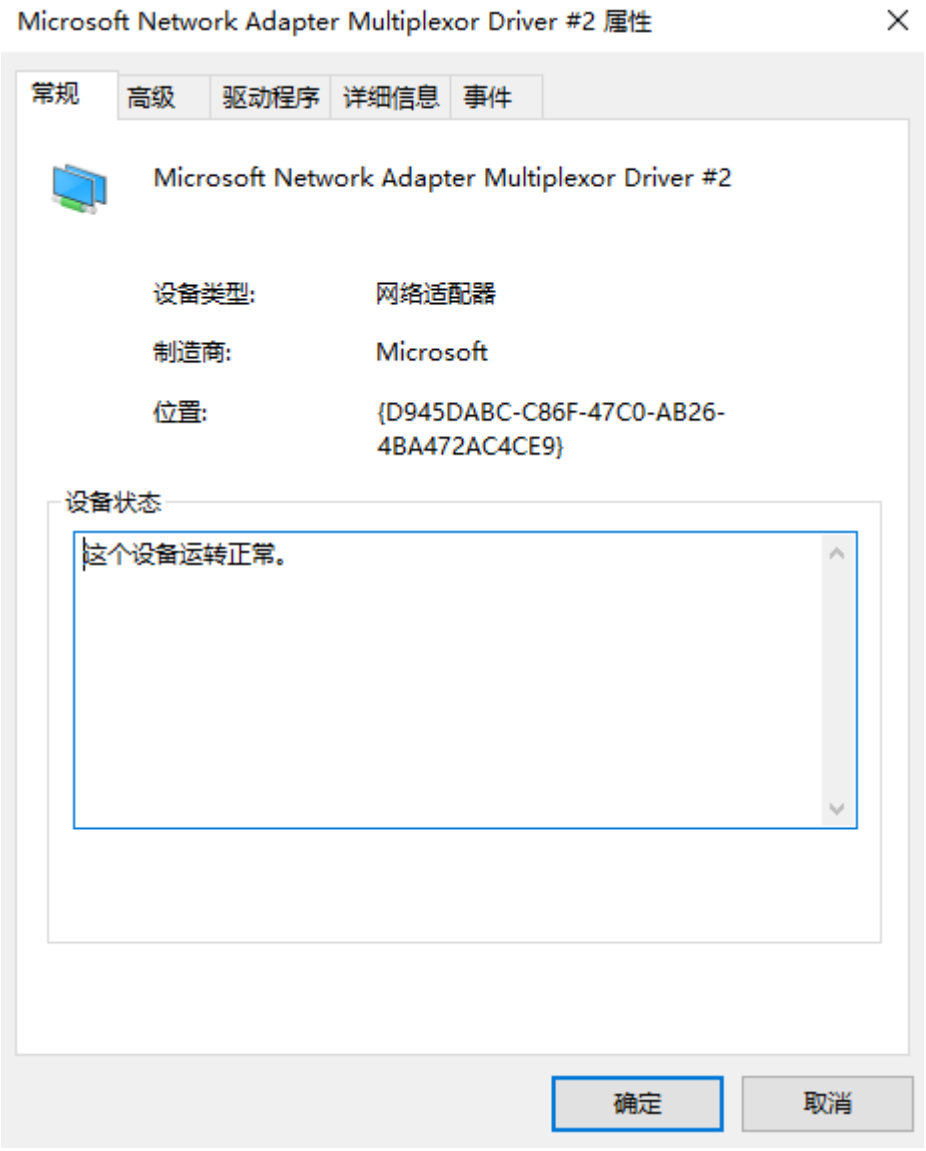


7. 执行以下步骤，配置辅助弹性网卡的网络信息。
   a. 在网络连接页面，双击Team1 - VLAN 1229。
   进入Team1 - VLAN 1229状态页面。

b. 在Team1 - VLAN 1229状态页面，单击“属性”。
进入Team1 - VLAN 1229属性页面。

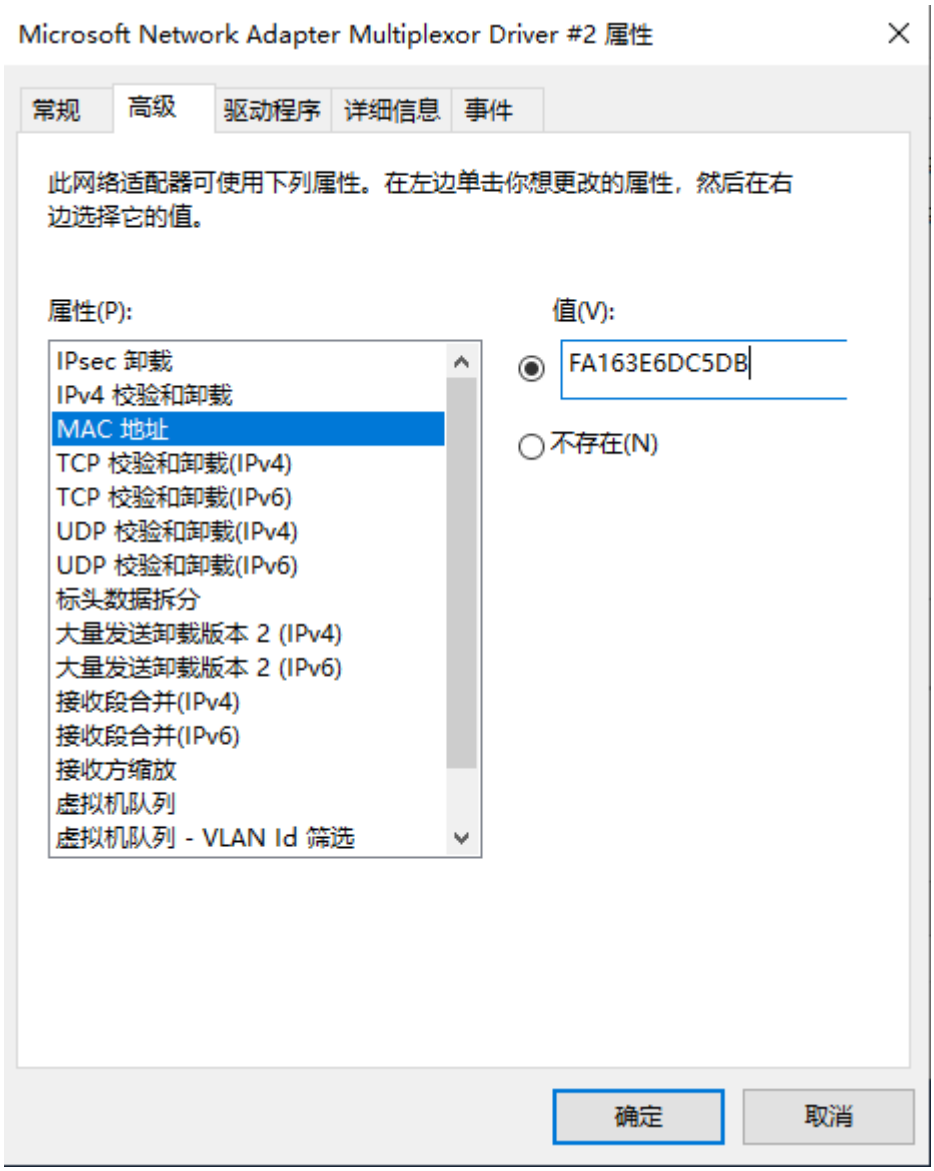


c. 在Team1 - VLAN 1229属性页面，单击“配置(C)...”。
进入Microsoft Network Adapter Multiplexor Driver #2属性页面。



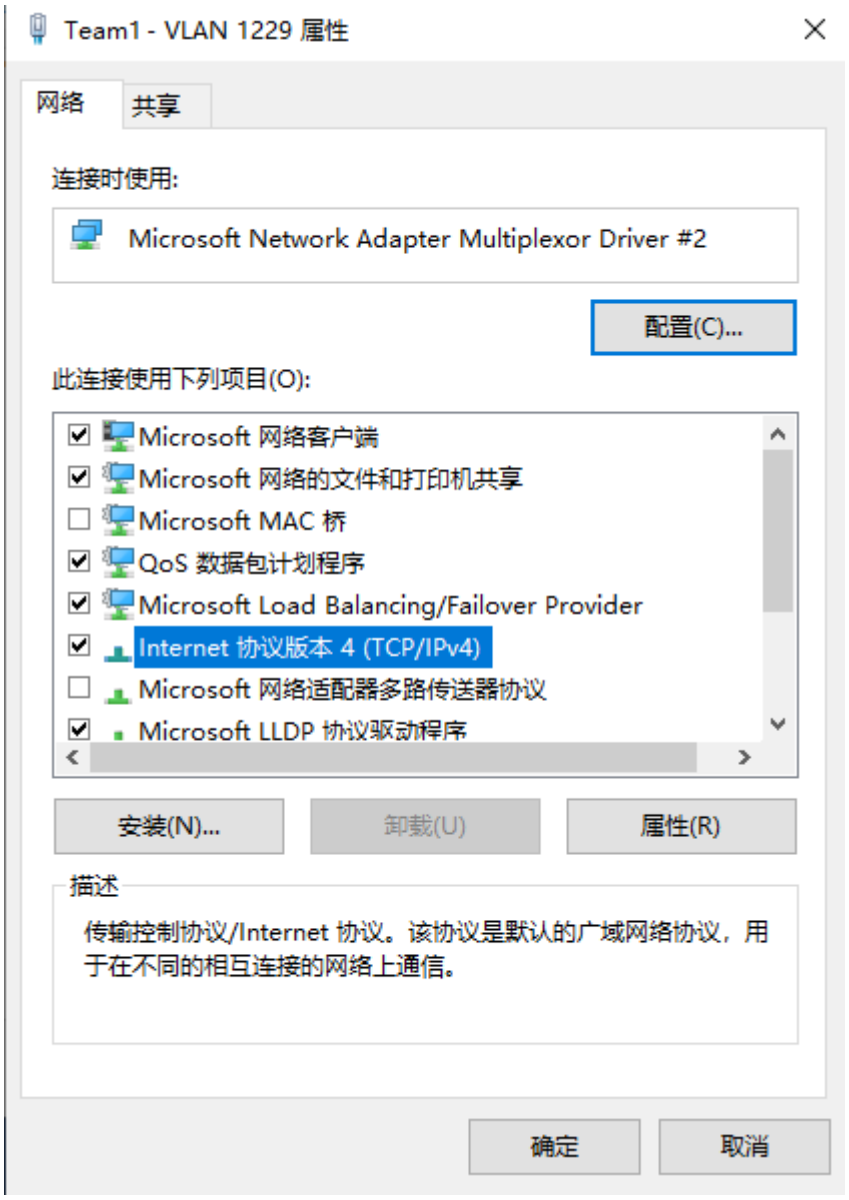
d. 在Microsoft Network Adapter Multiplexor Driver #2属性页面，选择“高级”页签，在MAC 地址对应的输入框中，输入弹性网卡的MAC地址并单击“确定”。

输入MAC地址时，需要去掉连接符号“:”，本示例中查询到的辅助弹性网卡MAC地址为fa:16:3e:6d:c5:db，此处输入FA163E6DC5DB。



e. 在Team1 - VLAN 1229属性页面，双击“Internet 协议版本 4（TCP/IPv4）”。

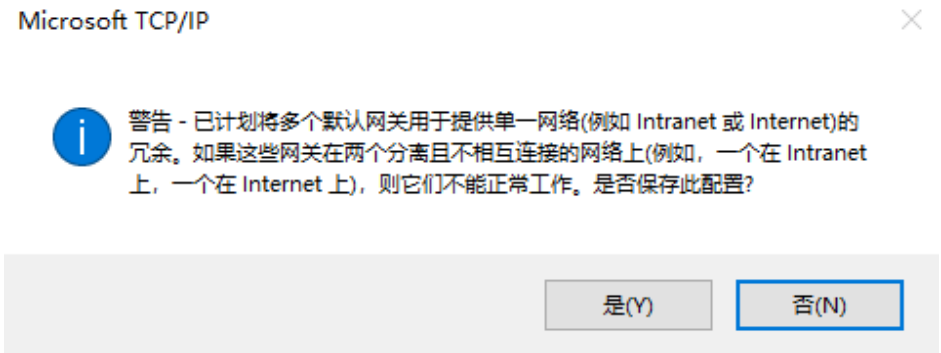
打开Internet 协议版本 4（TCP/IPv4）属性页面。



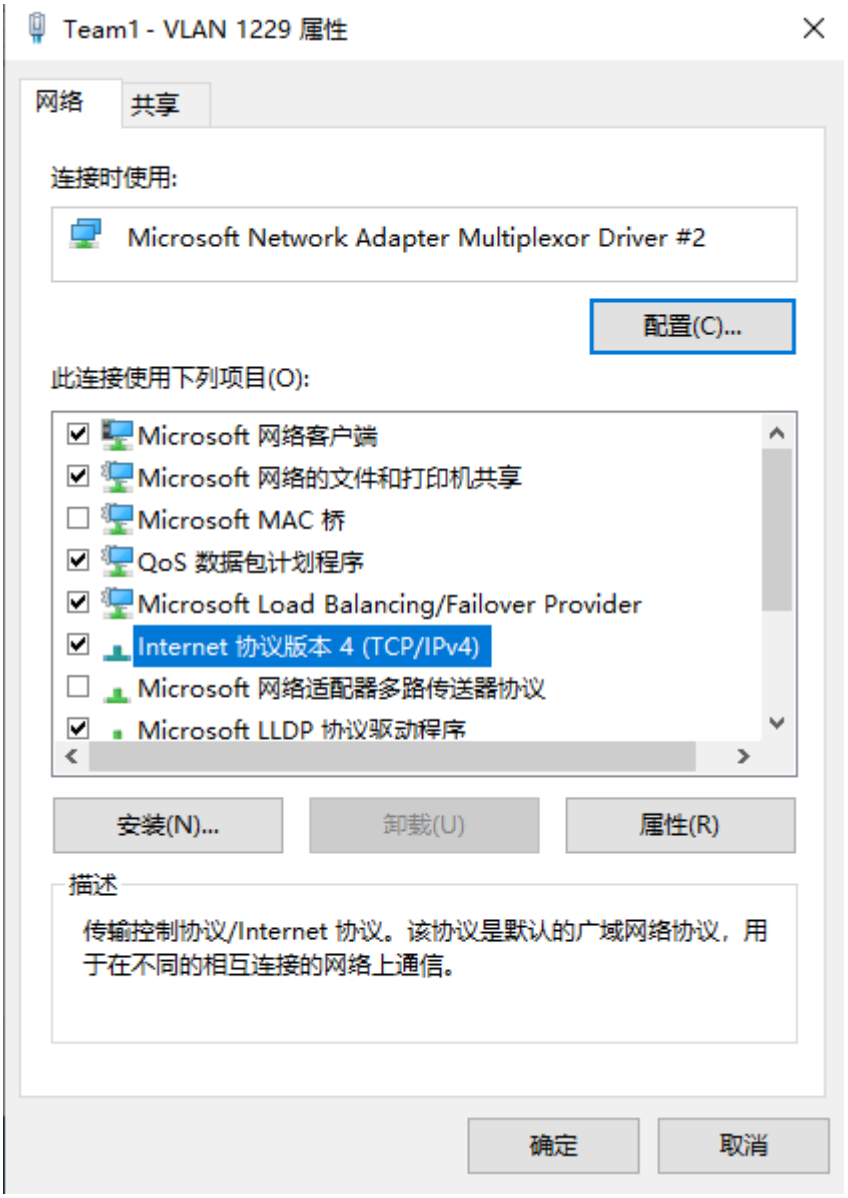
f. 在Internet 协议版本 4（TCP/IPv4）属性页面，配置辅助弹性网卡的网络信息，并单击“确定”。

- 选择“使用下面的IP地址(S)”
- IP地址(I)：输入辅助弹性网卡的私有IP地址，本示例为192.168.0.22。
- 子网掩码(U)：输入辅助弹性网卡所属子网的掩码，本示例为255.255.255.0。
- 默认网关(D)：输入辅助弹性网卡所属子网的网关，本示例为192.168.0.1。

如果弹出以下警告弹窗，单击“是”，关闭弹窗即可。



g. 在Team1 - VLAN 1229属性页面，单击“确定”，保存修改。



h. 在Team1 - VLAN 1229状态页面，单击“详细信息(E)...”。
进入网络连接详细信息页面，确认以下信息配置是否正确。

- 物理地址：辅助弹性网卡的MAC地址。
- IPv4 地址：辅助弹性网卡的私有IP地址。
- IPv4 子网掩码：辅助弹性网卡所属子网的掩码。
- IPv4 默认网关：辅助弹性网卡所属子网的网关。

i. 检查无误后，关闭弹窗。

8. 在Windows PowerShell命令行界面，执行以下步骤，验证弹性网卡和辅助弹性网卡的通信功能是否正常。

   a. 执行以下命令，验证弹性网卡和测试ECS的网络通信情况。

      Ping *测试ECS的私有IP地址* **-S** *弹性网卡的私有IP地址*

      建议测试ECS和弹性网卡所在的ECS位于同一个VPC中，并且使用同一个安全组，此时两个ECS网络默认互通。

      命令示例：

      Ping 192.168.0.133 -S 192.168.0.16

      回显类似如下信息，表示通信正常。


```
PS C:\Users\Administrator> Ping 192.168.0.133 -S 192.168.0.16

正在 Ping 192.168.0.133 从 192.168.0.16 具有 32 字节的数据:
来自 192.168.0.133 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.0.133 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.133 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.0.133 的回复: 字节=32 时间<1ms TTL=64

192.168.0.133 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

b. 执行以下命令，验证辅助弹性网卡和测试ECS的网络通信情况。

Ping *测试ECS的私有IP地址* **-S** *辅助弹性网卡的私有IP地址*

建议测试ECS和辅助弹性网卡所在的ECS位于同一个VPC中，并且使用同一个安全组，此时两个ECS网络默认互通。

命令示例：

Ping 192.168.0.133 -S 192.168.0.22

回显类似如下信息，表示通信正常。

```
PS C:\Users\Administrator> Ping 192.168.0.133 -S 192.168.0.22

正在 Ping 192.168.0.133 从 192.168.0.22 具有 32 字节的数据:
来自 192.168.0.133 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.0.133 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.0.133 的回复: 字节=32 时间<1ms TTL=64

192.168.0.133 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 3, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

5.2.3 查看辅助弹性网卡基本信息

操作场景

您可以在控制台查看您所拥有的辅助弹性网卡基本信息，包括ID、所属弹性网卡、VLAN、所属VPC、所属子网、私网IP、绑定的弹性公网IP、MAC地址及关联的安全组等信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 在辅助弹性网卡列表中，单击需要查看详情的辅助“私有IP地址”，打开辅助弹性网卡的详情页。
   - “基本信息”页签：显示辅助弹性网卡的ID、所属弹性网卡、VLAN、所属VPC、所属子网、服务地址、MAC地址等信息。

- “关联安全组”页签：显示辅助弹性网卡关联的安全组及其规则。

其他操作

在辅助弹性网卡详情页可以修改以下信息：

- 在“基本信息”页签，可以修改辅助弹性网卡的“描述”信息，以及变更绑定的弹性公网IP。
- 在“关联安全组”页签，可以修改关联的安全组，详细内容请参考**更改辅助弹性网卡所属的安全组**。

5.2.4 将辅助弹性网卡和弹性公网 IP 绑定/解绑定

操作场景

通过为辅助弹性网卡绑定弹性公网IP，您可以构建更灵活，扩展性更强的组网方案。

辅助弹性网卡本身可以提供一个私网IP，与弹性公网IP绑定后，相当于同时具备了私网IP和公网IP。辅助弹性网卡和弹性公网IP的绑定关系不随弹性网卡解绑云服务器实例而变化，当辅助弹性网卡随同挂载的弹性网卡从云服务器上迁移时，可以同时完成私网IP和公网IP的迁移。

一个弹性网卡可以挂载多个辅助弹性网卡，当为每个辅助弹性网卡分别绑定一个弹性公网IP时，这个弹性网卡所绑定的云服务器就拥有了多个弹性公网IP，可以提供更灵活的外部访问服务。

当无需使用公网IP，或想要删除辅助弹性网卡时，您可以解绑定辅助弹性网卡到弹性公网IP。

绑定操作

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 在辅助弹性网卡列表，单击操作列的“绑定弹性公网IP”，选择需要绑定的弹性公网IP。
7. 单击“确定”，完成绑定。

解绑定操作

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。

5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 在辅助弹性网卡列表，单击操作列的“解绑定弹性公网IP”，选择需要解绑定的弹性公网IP。
7. 单击“确定”，完成解绑定。

5.2.5 更改辅助弹性网卡所属的安全组

操作场景

辅助弹性网卡创建完成后，您可以更改其所属的安全组。

更改辅助弹性网卡所属的安全组有两种方法：

- 在辅助弹性网卡列表中进行更改。
- 进入辅助弹性网卡详情页进行更改。

操作步骤

在辅助弹性网卡列表中，更改所属安全组

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 在辅助弹性网卡列表中，单击操作列的“更改安全组”。
7. 在“更改安全组”页面勾选需要关联的安全组。
8. 单击“确定”，完成更改。

在辅助弹性网卡详情页，更改所属安全组

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 单击待修更改安全组的辅助弹性网卡的“私有IP地址”，进入辅助弹性网卡详情页。
7. 在“关联安全组”页签下，单击“更改安全组”。
8. 在“更改安全组”页面勾选需要关联的安全组。
9. 单击“确定”，完成更改。

5.2.6 删除辅助弹性网卡

操作场景

您可以删除不再使用的辅助弹性网卡。

约束与限制

- 删除辅助弹性网卡时，会解除辅助弹性网卡和弹性网卡的绑定关系。
- 删除辅助弹性网卡时，会解除网卡和弹性公网IP的绑定关系，您可以选择是否释放该弹性公网IP。

  如果不释放弹性公网IP，将会继续收取费用，您可以将其绑定给其他云资源使用。
- 删除辅助弹性网卡时，如果辅助弹性网卡已被其他资源使用，会同步删除关联资源中使用辅助弹性网卡的条目，删除操作无法恢复，请谨慎操作。

  比如，在VPC路由表中，存在自定义路由的下一跳是辅助弹性网卡，则删除辅助弹性网卡时，则会同步删除相关路由。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 弹性网卡”。
5. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
6. 在辅助弹性网卡列表中，单击操作列的“删除”。

   弹出删除确认对话框。
7. 根据界面提示完成信息确认后，删除辅助弹性网卡。

   删除辅助弹性网卡会同步清理云服务器实例上配置的VLAN子接口，无需单独删除。

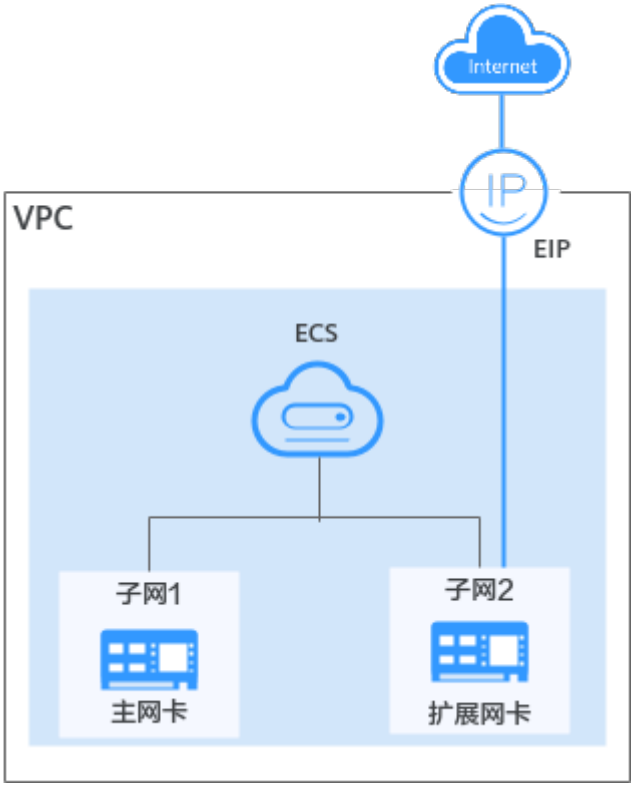
5.3 弹性网卡配置示例

5.3.1 为 ECS 的扩展网卡绑定 EIP 并实现公网通信

操作场景

本示例如图5-2所示，ECS有两个网卡，包括主网卡和扩展网卡。您可以参考以下操作，为扩展网卡绑定EIP，并配置策略路由，确保ECS可以通过扩展网卡绑定的EIP访问公网。

图 5-2 通过 ECS 扩展网卡访问公网的组网示意图



说明

本文操作以Linux系统的ECS为例，供您参考。

步骤一：创建资源并绑定扩展网卡

1. 创建一个VPC，并在VPC下添加两个子网。

   本示例中，ECS主网卡和扩展网卡位于同一个VPC内的不同子网。

   具体请参见**创建虚拟私有云和子网**。
2. 基于已有的VPC和子网，创建一个ECS。

   具体方法请参见**自定义购买ECS**。
3. 创建弹性网卡，并将弹性网卡绑定至ECS，用作扩展网卡。

   创建弹性网卡时，请选择VPC下的另一个子网，和ECS的主网卡所属不同的子网，具体请参见**创建弹性网卡**。

   将弹性网卡绑定至ECS，具体请参见**将弹性网卡绑定至云服务器实例**。
4. 购买一个EIP，并将EIP绑定至ECS的扩展网卡。

   购买EIP，具体操作请参见**申请弹性公网IP**。

   将EIP绑定至ECS的扩展网卡，具体操作请参见**将弹性网卡绑定至弹性公网IP**。

步骤二：获取云服务器网络信息

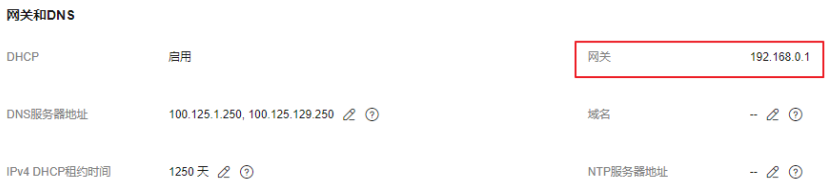
配置ECS扩展网卡的路由之前，您执行以下操作，收集**表5-7**中的信息。

表 5-7 获取云服务器网络信息

类型	主网卡	扩展网卡
网卡的私有IP地址	192.168.11.42	192.168.17.191
子网网关地址	192.168.11.1	192.168.17.1

1. 执行以下操作，获取ECS网卡的私有IP地址。
   a. 登录管理控制台。
   b. 在管理控制台左上角单击 ，选择区域和项目。
   c. 在服务列表，选择“计算 >弹性云服务器”。
   d. 在弹性云服务器列表中，选择目标ECS，并单击名称对应的超链接。
      进入弹性云服务器“基本信息”页签。
   e. 选择“弹性网卡”页签，查看云服务器主网卡和扩展网卡对应的私有IP地址。
2. 执行以下操作，获取子网的网关地址。
   a. 登录管理控制台。
   b. 在管理控制台左上角单击 ，选择区域和项目。
   c. 在服务列表，选择“计算 >弹性云服务器”。
   d. 在弹性云服务器列表中，选择目标ECS，并单击名称对应的超链接。
      进入弹性云服务器“基本信息”页签。
   e. 在云服务器信息区域，单击虚拟私有云对应的超链接。
      进入“虚拟私有云”页面。
   f. 在虚拟私有云列表中，单击“子网个数”所在列的数字超链接。
      进入“子网”页面。
   g. 在子网列表中，单击子网名称对应的超链接。
      进入子网的“基本信息”页面。
   h. 在“网关和DNS”区域，查看目标子网对应的网关地址。

   图 5-3 子网网关地址



步骤三：为扩展网卡配置策略路由

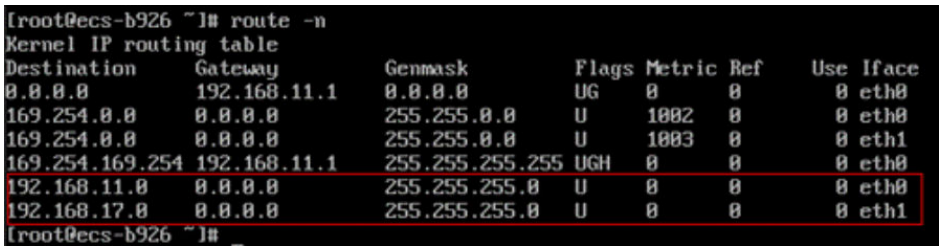
1. 远程登录ECS。
   ECS有多种登录方法，具体请参见**登录弹性云服务器**。

2. 执行以下命令，查询网卡的路由信息。

   route -n

   显示如下图所示，本示例中：

   - 主网卡路由的目的地址为192.168.11.0/24。
   - 扩展网卡路由的目的地址为192.168.17.0/24。

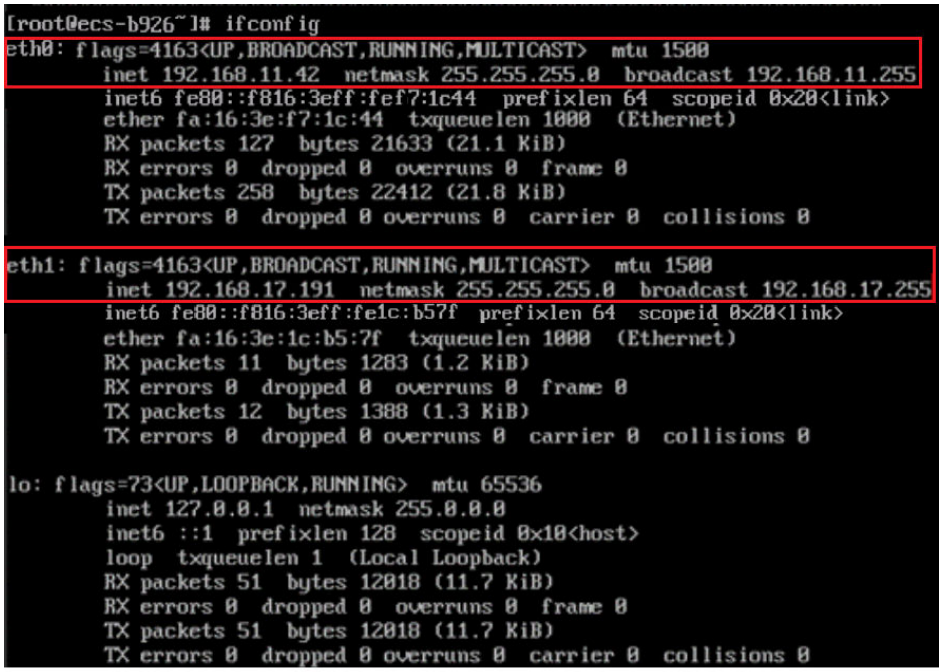


3. 执行以下命令，查看云服务器网卡名称。

   ifconfig

   显示如下图所示，通过网卡地址查找对应的网卡名称，本示例中：

   - 192.168.11.42为主网卡地址，对应的名称为eth0。
   - 192.168.17.191为扩展网卡地址，对应的名称为eth1。



4. 执行以下步骤，设置网络默认通过扩展网卡访问公网。

   a. 执行如下命令，删除主网卡默认路由。

      route del -net 0.0.0.0 gw *子网网关* **dev** *网卡名称*

      参数说明如下：

      - 0.0.0.0：目的地址，表示匹配多有IP，请不要修改。
      - 子网网关：填写**表5-7**中收集的主网卡所在子网的网关地址。
      - 网卡名称：填写**3**中所查的主网卡名称。

      命令示例：

route del -net 0.0.0.0 gw 192.168.11.1 dev eth0

说明

此操作会导致ECS流量中断，请谨慎操作。

b. 执行如下命令，配置扩展网卡默认路由。

route add default gw *子网网关*

参数说明如下：

子网网关：填写表5-7中收集的扩展网卡所在子网的网关地址。

命令示例：

route add default gw 192.168.17.1

5. 验证网络通信情况。

执行以下命令，验证ECS是否可以访问公网。

ping *公网IP地址或者域名*

命令示例：

ping support.huaweicloud.com

回显类似如下信息，表示ECS可以访问公网。

```
[root@ecs-a01 ~]# ping support.huaweicloud.com
PING hcdnw.cbg-notzj.c.cdnhwc2.com (203.193.226.103) 56(84) bytes of data.
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=1 ttl=51 time=2.17 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=2 ttl=51 time=2.13 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=3 ttl=51 time=2.10 ms
64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=4 ttl=51 time=2.09 ms
...
--- hcdnw.cbg-notzj.c.cdnhwc2.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 2.092/2.119/2.165/0.063 ms
```

5.3.2 为多网卡 ECS 配置策略路由

5.3.2.1 方案概述

背景知识

当云服务器拥有多张网卡时，主网卡默认可以和外部正常通信，扩展网卡无法和外部正常通信，此时需要在云服务器内部为这些网卡配置策略路由，才可以确保多张网卡均可以和外部正常通信。

操作场景

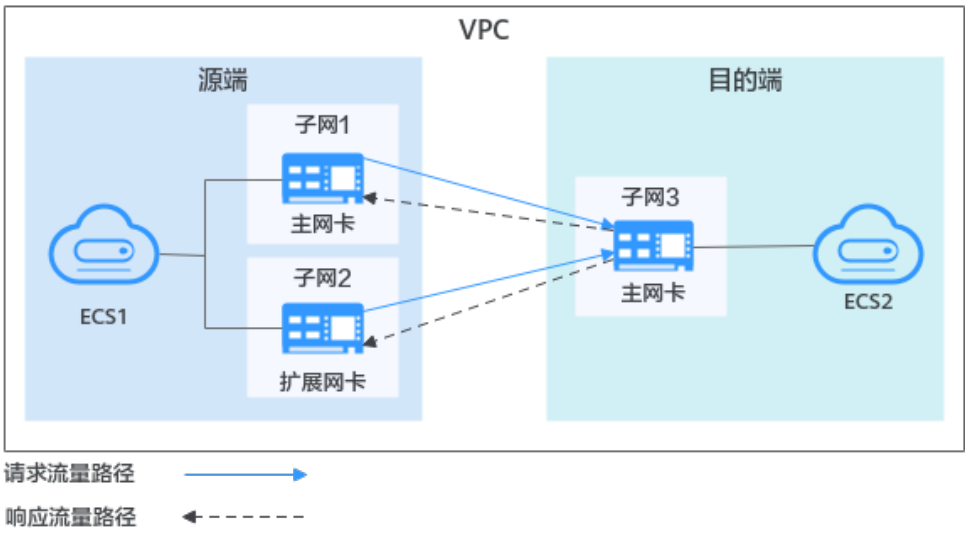
本文档以配置双网卡云服务器的策略路由为例，组网如图5-4所示，具体说明如下：

- 源端云服务器主网卡和扩展网卡位于同一个VPC内的不同子网。
- 源端云服务器和目的端云服务器位于同一个VPC内的不同子网，因此网络互通，即配置策略路由前，源端云服务器的主网卡可以和目的端云服务器正常通信。
- 为源端云服务器双网卡配置策略路由后，主网卡和扩展网卡都可以作为独立网卡和目的端云服务器正常通信。

须知

您可以根据实际情况选择目的端地址，请在配置双网卡策略路由前，确保源端云服务器主网卡和目的端已正常通信。

图 5-4 双网卡云服务器组网示意图



操作指引

本文提供Linux和Windows云服务器的操作指导，具体请参见表5-8。

表 5-8 操作指引说明

操作系统类型	IP类型	操作步骤
Linux	IPv4 IPv6	以CentOS 8.0 64bit操作系统为例： 为多网卡Linux云服务器配置IPv4和IPv6策略路由（CentOS） 以Ubuntu 22.04 server 64bit操作系统为例： 为多网卡Linux云服务器配置IPv4和IPv6策略路由（Ubuntu）
Windows	IPv4 IPv6	以Windows 2012 64bit操作系统为例： 为多网卡Windows云服务器配置IPv4和IPv6策略路由

5.3.2.2 收集云服务器网络信息

操作场景

为多网卡云服务器配置策略路由之前，您需要收集云服务器的网络信息，请根据云服务器操作系统及IP类型参考对应的指导，具体说明如下：

- 对于Linux IPv4场景，您需要收集的信息如表5-9所示。

  表 5-9 Linux IPv4 场景信息说明

类型	主网卡	扩展网卡	获取方法
源端	• 网卡地址：10.0.0.115 • 子网网段：10.0.0.0/24 • 子网网关：10.0.0.1	• 网卡地址：10.0.1.183 • 子网网段：10.0.1.0/24 • 子网网关：10.0.1.1	• 获取云服务器网卡地址 • 获取子网网段和网关地址
目的端	网卡地址：10.0.2.12	不涉及	

- 对于Linux IPv6场景，您需要收集的信息如表5-10所示。

  表 5-10 Linux IPv6 场景信息说明

类型	主网卡	扩展网卡	获取方法
源端	• IPv4网卡地址：10.0.0.102 • IPv6网卡地址：2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 • 子网IPv6网段：2407:c080:1200:1dd8::/64 • 子网IPv6网关：2407:c080:1200:1dd8::1	• IPv4网卡地址：10.0.1.191 • IPv6网卡地址：2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 • 子网IPv6网段：2407:c080:1200:1a9c::/64 • 子网IPv6网关：2407:c080:1200:1a9c::1	• 获取云服务器网卡地址 • 获取子网网段和网关地址
目的端	• IPv4网卡地址：10.0.2.3 • IPv6网卡地址：2407:c080:1200:1dd9:16a7:fe7a:8f71:7044	不涉及	

- 对于Windows IPv4场景，您需要收集的信息如表5-11所示。

表 5-11 Windows IPv4 场景信息说明

类型	主网卡	扩展网卡	获取方法
源端	• 网卡地址：10.0.0.59 • 子网网关：10.0.0.1	• 网卡地址：10.0.1.104 • 子网网关：10.0.1.1	• 获取云服务器网卡地址 • 获取子网网段和网关地址
目的端	网卡地址：10.0.2.12	不涉及	

- 对于Windows IPv6场景，您需要收集的信息如表5-12所示。

表 5-12 Windows IPv6 场景信息说明

类型	主网卡	扩展网卡	获取方法
源端	网卡地址：2407:c080:802:aba:6788:fb94:d71f:8deb	网卡地址：2407:c080:802:be6:71c8:42e0:d44e:eeb4	获取云服务器网卡地址
目的端	网卡地址：2407:c080:802:be7:c2e6:d99c:b685:c6c8	不涉及	

须知

以上表格中收集的信息仅为示例，具体信息请您以实际环境为准。

获取云服务器网卡地址

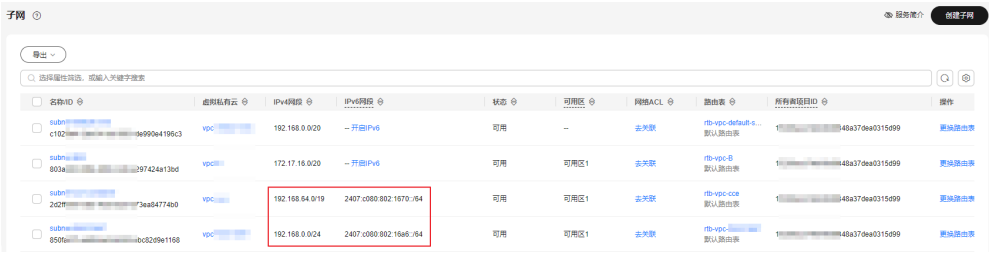
1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在服务列表，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，选择目标弹性云服务器，并单击名称对应的超链接。
   进入弹性云服务器“基本信息”页签。
5. 在网卡区域，查看云服务器主网卡和扩展网卡对应IP地址。
   支持查看IPv4及IPv6地址。

图 5-5 查看云服务器网卡地址

获取子网网段和网关地址

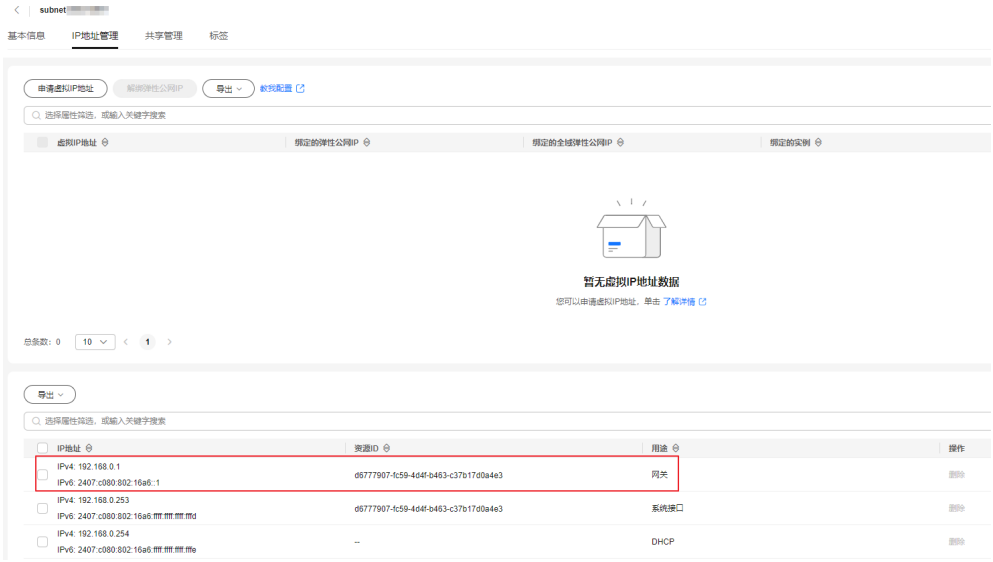
1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在服务列表，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，选择目标弹性云服务器，并单击名称对应的超链接。
   进入弹性云服务器“基本信息”页签。
5. 在云服务器信息区域，单击虚拟私有云对应的超链接。
   进入“虚拟私有云”页面。
6. 在虚拟私有云列表中，单击“子网个数”所在列的数字。
   进入“子网”页面。
7. 在子网列表中，查看目标子网对应的网段。
   支持查看IPv4和IPv6地址。

图 5-6 查看子网网段



8. 在子网列表中，单击子网名称对应的超链接。
   进入子网的“基本信息”页签。
9. 选择“IP地址管理”页签，查看目标子网对应的网关地址。
   支持查看IPv4和IPv6地址。

图 5-7 查看子网对应的网关地址



5.3.2.3 为多网卡 Linux 云服务器配置 IPv4 和 IPv6 策略路由（CentOS）

操作场景

本文档以CentOS 8.0 64bit为例，指导用户为双网卡Linux云服务器配置策略路由。

- IPv4：**Linux IPv4操作步骤 (CentOS)**
- IPv6：**Linux IPv6操作步骤 (CentOS)**

关于云服务器双网卡的背景知识及组网说明，请参见**方案概述**。

Linux IPv4 操作步骤 (CentOS)

1. 收集配置策略路由需要的云服务器网卡地址等信息。
   具体操作请参见**收集云服务器网络信息**。
   本示例中，云服务器的网络信息如**表5-13**所示。

   表 5-13 Linux IPv4 场景信息说明（CentOS）

类型	主网卡	扩展网卡
源端	• 网卡地址：10.0.0.115 • 子网网段：10.0.0.0/24 • 子网网关：10.0.0.1	• 网卡地址：10.0.1.183 • 子网网段：10.0.1.0/24 • 子网网关：10.0.1.1
目的端	网卡地址：10.0.2.12	不涉及

2. 登录源端云服务器。
   ECS有多种登录方法，具体请参见**登录弹性云服务器**。
3. 执行以下命令，检查源端云服务器主网卡和目的端云服务器通信情况。

配置多网卡策略路由前，请务必确保源端主网卡和目的端通信正常。

ping -I *源端云服务器主网卡地址 目的端云服务器地址*

命令示例：

ping -I 10.0.0.115 10.0.2.12

回显类似如下信息，表示可以正常通信。

```
[root@ecs-resource ~]# ping -I 10.0.0.115 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.0.115 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=0.775 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.167 ms
^C
--- 10.0.2.12 ping statistics ---
```

4. 执行以下命令，查看云服务器网卡名称。

   ifconfig

   回显类似如下信息，通过网卡地址查找对应的网卡名称，本示例中：

   - 10.0.0.115为主网卡地址，对应的名称为eth0。
   - 10.0.1.183为扩展网卡地址，对应的名称为eth1。

```
[root@ecs-resource ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.0.115  netmask 255.255.255.0  broadcast 10.0.0.255
      inet6 fe80::f816:3eff:fe92:6e0e  prefixlen 64  scopeid 0x20<link>
      ether fa:16:3e:92:6e:0e  txqueuelen 1000  (Ethernet)
      RX packets 432288  bytes 135762012 (129.4 MiB)
      RX errors 0  dropped 0  overruns 0  frame 1655
      TX packets 423744  bytes 106716932 (101.7 MiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.1.183  netmask 255.255.255.0  broadcast 10.0.1.255
      inet6 fe80::f816:3eff:febf:5818  prefixlen 64  scopeid 0x20<link>
      ether fa:16:3e:bf:58:18  txqueuelen 1000  (Ethernet)
      RX packets 9028  bytes 536972 (524.3 KiB)
      RX errors 0  dropped 0  overruns 0  frame 1915
      TX packets 6290  bytes 272473 (266.0 KiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. 执行以下步骤，为云服务器配置临时路由。

须知

临时路由配置完后立即生效，当云服务器重启后临时路由会丢失，请执行完5配置完临时路由后，继续执行6配置永久路由，避免云服务器重启后网络中断。

a. 依次执行以下命令，添加主网卡和扩展网卡的策略路由。

   - 主网卡

     ip route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

     ip route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

     ip rule add from *网卡地址* **table** *路由表名称*

   - 扩展网卡

     ip route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

     ip route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

ip rule add from *网卡地址* **table** *路由表名称*

参数说明如下：

- 网卡名称：填写4中所查名称。
- 路由表名称：自定义路由表名称，此处请使用数字命名路由表。
- 其他网络信息：填写1中收集的地址。

命令示例：

- 主网卡

  ip route add default via 10.0.0.1 dev eth0 table 10

  ip route add 10.0.0.0/24 dev eth0 table 10

  ip rule add from 10.0.0.115 table 10

- 扩展网卡

  ip route add default via 10.0.1.1 dev eth1 table 20

  ip route add 10.0.1.0/24 dev eth1 table 20

  ip rule add from 10.0.1.183 table 20

说明

如果云服务器有多张网卡，请依次为所有网卡添加策略路由。

b. 依次执行以下命令，确认策略路由是否添加成功。

ip rule

ip route show table *主网卡路由表名称*

ip route show table *扩展网卡路由表名称*

其中，路由表名称为5.a中自定义的名称。

命令示例：

ip rule

ip route show table 10

ip route show table 20

回显类似如下信息，表示策略路由添加成功。

```
[root@ecs-resource ~]# ip rule
0:      from all lookup local
32764:  from 10.0.1.183 lookup 20
32765:  from 10.0.0.115 lookup 10
32766:  from all lookup main
32767:  from all lookup default
[root@ecs-resource ~]# ip route show table 10
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0 scope link
[root@ecs-resource ~]# ip route show table 20
default via 10.0.1.1 dev eth1
10.0.1.0/24 dev eth1 scope link
```

c. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

ping -I *源端云服务器主网卡地址 目的端云服务器地址*

ping -I *源端云服务器扩展网卡地址 目的端云服务器地址*

命令示例：

ping -I 10.0.0.115 10.0.2.12

ping -I 10.0.1.183 10.0.2.12

回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。

```
[root@ecs-resource ~]# ping -I 10.0.0.115 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.0.115 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=0.775 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.268 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.167 ms
^C
--- 10.0.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 102ms
rtt min/avg/max/mdev = 0.167/0.357/0.775/0.244 ms
[root@ecs-resource ~]# ping -I 10.0.1.183 10.0.2.12
PING 10.0.2.12 (10.0.2.12) from 10.0.1.183 : 56(84) bytes of data.
64 bytes from 10.0.2.12: icmp_seq=1 ttl=64 time=2.84 ms
64 bytes from 10.0.2.12: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 10.0.2.12: icmp_seq=3 ttl=64 time=0.234 ms
64 bytes from 10.0.2.12: icmp_seq=4 ttl=64 time=0.153 ms
^C
--- 10.0.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 92ms
rtt min/avg/max/mdev = 0.153/0.871/2.840/1.137 ms
```

6. 执行以下步骤，为云服务器配置永久路由。

   a. 执行以下命令，打开“/etc/rc.local”文件。

      vi /etc/rc.local

   b. 按**i**进入编辑模式。

   c. 在文件末尾添加以下配置。

```
# check eth0
for ((x=0; x<10; x++)); do
  if (ip addr show eth0 | grep -w 10.0.0.115 >/dev/null 2>&1); then
    break
  fi
  sleep 1
done

# Add v4 routes for eth0
ip route flush table 10
ip route add default via 10.0.0.1 dev eth0 table 10
ip route add 10.0.0.0/24 dev eth0 table 10
ip rule add from 10.0.0.115 table 10

# check eth1
for ((x=0; x<10; x++)); do
  if (ip addr show eth1 | grep -w 10.0.1.183 >/dev/null 2>&1); then
    break
  fi
  sleep 1
done

# Add v4 routes for eth1
ip route flush table 20
ip route add default via 10.0.1.1 dev eth1 table 20
ip route add 10.0.1.0/24 dev eth1 table 20
ip rule add from 10.0.1.183 table 20
# Add v4 routes for cloud-init
ip rule add to 169.254.169.254 table main
```

   其中，参数说明如下：

   - check eth0：循环检查主网卡eth0是否获取到IPv4地址（eth0网卡地址为10.0.0.115），每秒检查一次，重试次数为10次。

- Add v4 routes for eth0：主网卡的策略路由，和5.a配置保持一致。
- check eth1：循环检查扩展网卡eth1是否获取到IPv4地址（eth1网卡地址为10.0.1.183），每秒检查一次，重试次数为10次。
- Add v4 routes for eth1：扩展网卡的策略路由，和5.a配置保持一致。
- Add v4 routes for cloud-init：配置cloud-init地址，请和本示例中的配置保持一致，不要修改。

d. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下命令，为“/etc/rc.local”文件添加执行权限。

chmod +x /etc/rc.local

说明

如果您的操作系统为Redhat、EulerOS，执行完6.e后，还需要执行以下命令，权限才会添加成功。

chmod +x /etc/rc.d/rc.local

f. 执行以下命令，重启云服务器。

reboot

须知

“/etc/rc.local”文件添加中添加的策略路由，需要重启云服务器后才会生效，此处请确保不影响业务再重启云服务器操作。

g. 参考5.b~5.c，检查策略路由添加情况，并验证源端和目的通信是否正常。

Linux IPv6 操作步骤（CentOS）

1. 收集配置策略路由需要的云服务器网卡地址等信息。

   具体操作请参见**收集云服务器网络信息**。

表 5-14 Linux IPv6 场景信息说明(CentOS)

类型	主网卡	扩展网卡
源端	• IPv4网卡地址：10.0.0.102 • IPv6网卡地址：2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 • 子网IPv6网段：2407:c080:1200:1dd8::/64 • 子网IPv6网关：2407:c080:1200:1dd8::1	• IPv4网卡地址：10.0.1.191 • IPv6网卡地址：2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 • 子网IPv6网段：2407:c080:1200:1a9c::/64 • 子网IPv6网关：2407:c080:1200:1a9c::1

类型	主网卡	扩展网卡
目的端	• IPv4网卡地址：10.0.2.3 • IPv6网卡地址：2407:c080:1200:1dd9:16a7:fe7a:8f71:7044	不涉及

2. 登录源端云服务器。

   ECS有多种登录方法，具体请参见**登录弹性云服务器**。

3. 执行以下步骤，确保云服务器已开启IPv6协议栈，并且正常获取到IPv6地址。

   须知

   对于源端和目的端的IPv6云服务器，均需要执行该操作，确保云服务器已获取到IPv6地址，否则云服务器无法通过IPv6地址进行通信。

   本章节云服务器使用的操作系统为CentOS 8.0 64bit公共镜像，以下针对该操作系统举例，更多操作系统配置指导，请参见**动态获取IPv6地址**的“Linux操作系统（手动配置启用IPv6）”小节。

   a. 执行以下命令，检查云服务器是否可以获取到IPv6地址。

      ip addr

      回显类似如下信息，eth0和eth1为云服务器的网卡，只有一行inet6地址，为fe80开头，表示该云服务器已开启IPv6协议栈，但是未获取到IPv6地址，需要继续执行**3.b**~**3.g**，获取IPv6地址。

      ```
      [root@ecs-resource ~]# ip addr
      ...
      2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
          link/ether fa:16:3e:22:22:88 brd ff:ff:ff:ff:ff:ff
          inet 10.0.0.102/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
             valid_lft 107943256sec preferred_lft 107943256sec
          inet6 fe80::f816:3eff:fe22:2288/64 scope link
             valid_lft forever preferred_lft forever
      3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
          link/ether fa:16:3e:22:23:e1 brd ff:ff:ff:ff:ff:ff
          inet 10.0.1.191/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
             valid_lft 107943256sec preferred_lft 107943256sec
          inet6 fe80::f816:3eff:fe22:23e1/64 scope link
             valid_lft forever preferred_lft forever
      ```

   b. 执行以下命令，查看云服务器网卡名称。

      ifconfig

      回显类似如下信息，通过网卡地址查找对应的网卡名称，本示例中：

      - 10.0.0.102为主网卡地址，对应的名称为eth0。
      - 10.0.1.191为扩展网卡地址，对应的名称为eth1。

      ```
      [root@ecs-resource ~]# ifconfig
      eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 10.0.0.102  netmask 255.255.255.0  broadcast 10.0.0.255
            inet6 fe80::f816:3eff:fe22:2288  prefixlen 64  scopeid 0x20<link>
            ether fa:16:3e:22:22:88  txqueuelen 1000  (Ethernet)
            RX packets 135116  bytes 132321802 (126.1 MiB)
      ```



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 60963  bytes 23201005 (22.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.191  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe22:23e1  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:22:23:e1  txqueuelen 1000  (Ethernet)
        RX packets 885  bytes 97676 (95.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 4478 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

c. 执行以下步骤，编辑主网卡的ifcfg文件。

i. 执行以下命令，打开主网卡的ifcfg文件。

vi /etc/sysconfig/network-scripts/ifcfg-*主网卡名称*

其中，主网卡名称为**3.b**中查询到的名称。

命令示例：

vi /etc/sysconfig/network-scripts/ifcfg-eth0

ii. 按**i**进入编辑模式。

iii. 在文件末尾添加以下配置。

```
IPV6INIT="yes"
DHCPV6C="yes"
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

d. 执行以下步骤，编辑扩展网卡的ifcfg文件。

i. 执行以下命令，打开扩展网卡的ifcfg文件。

vi /etc/sysconfig/network-scripts/ifcfg-*扩展网卡名称*

其中，扩展网卡名称为**3.b**中查询到的名称。

命令示例：

vi /etc/sysconfig/network-scripts/ifcfg-eth1

ii. 按**i**进入编辑模式。

iii. 在文件末尾添加以下配置。

```
IPV6INIT="yes"
DHCPV6C="yes"
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下步骤，编辑“/etc/sysconfig/network”文件。

i. 执行以下命令，打开“/etc/sysconfig/network”文件。

vi /etc/sysconfig/network

ii. 按**i**进入编辑模式。

iii. 在文件末尾添加以下配置。

```
NETWORKING_IPV6="yes"
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

f. 执行以下命令，重启网络服务使配置生效。

systemctl restart NetworkManager

g. 执行以下命令，检查云服务器是否可以获取到IPv6地址。

ip addr

回显类似如下信息，eth0和eth1网卡有两行inet6地址，新增一行2407开头的地址，表示配置成功。


```
[root@ecs-resource ~]# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether fa:16:3e:22:22:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.102/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 107999994sec preferred_lft 107999994sec
    inet6 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9/128 scope global dynamic noprefixroute
       valid_lft 7195sec preferred_lft 7195sec
    inet6 fe80::f816:3eff:fe22:2288/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
default qlen 1000
    link/ether fa:16:3e:22:23:e1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.191/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
       valid_lft 107999994sec preferred_lft 107999994sec
    inet6 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8/128 scope global dynamic noprefixroute
       valid_lft 7198sec preferred_lft 7198sec
    inet6 fe80::f816:3eff:fe22:23e1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

h. 登录目的端云服务器，参考3.a~3.g，配置目的云服务器获取IPv6地址。

4. 登录源端云服务器，执行以下命令，检查源端云服务器主网卡和目的端云服务器通信情况。

   配置多网卡策略路由前，请务必确保源端主网卡和目的端通信正常。

   ping6 -I *源端云服务器主网卡地址 目的端云服务器地址*

   命令示例：

   ping6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044

   回显类似如下信息，表示可以正常通信。

```
[root@ecs-resource ~]# ping6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044(2407:c080:1200:1dd9:16a7:fe7a:8f71:7044) from
2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64 time=0.635 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64 time=0.320 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64 time=0.287 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=4 ttl=64 time=0.193 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.193/0.358/0.635/0.167 ms
```

5. 登录源端云服务器，执行以下步骤，为云服务器配置临时路由。

须知

临时路由配置完后立即生效，当云服务器重启后临时路由会丢失，请执行5配置完临时路由后，继续执行6配置永久路由，避免云服务器重启后网络中断。

a. 依次执行以下命令，添加主网卡和扩展网卡的策略路由。

- 主网卡

  ip -6 route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

  ip -6 route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

  ip -6 rule add from *网卡地址* **table** *路由表名称*

- 扩展网卡

ip -6 route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

ip -6 route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

ip -6 rule add from *网卡地址* **table** *路由表名称*

参数说明如下：

- 网卡名称：填写3.b中所查名称。
- 路由表名称：自定义路由表名称，此处请使用数字命名路由表。
- 其他网络信息：填写1中收集的地址。

命令示例：

- 主网卡

  ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table 10

  ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10

  ip -6 rule add from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 table 10

- 扩展网卡

  ip -6 route add default via 2407:c080:1200:1a9c::1 dev eth1 table 20

  ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20

  ip -6 rule add from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 table 20

说明

如果云服务器有多张网卡，请依次为所有网卡添加策略路由。

b. 依次执行以下命令，确认策略路由是否添加成功。

ip -6 rule

ip -6 route show table *主网卡路由表名称*

ip -6 route show table *扩展网卡路由表名称*

其中，路由表名称为5.a中自定义的名称。

命令示例：

ip -6 rule

ip -6 route show table 10

ip -6 route show table 20

回显类似如下信息，表示策略路由添加成功。

```
[root@ecs-resource ~]# ip -6 rule
0:      from all lookup local
32764:  from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 lookup 20
32765:  from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 lookup 10
32766:  from all lookup main
[root@ecs-resource ~]# ip -6 route show table 10
2407:c080:1200:1dd8::/64 dev eth0 metric 1024 pref medium
default via 2407:c080:1200:1dd8::1 dev eth0 metric 1024 pref medium
[root@ecs-resource ~]# ip -6 route show table 20
2407:c080:1200:1a9c::/64 dev eth1 metric 1024 pref medium
default via 2407:c080:1200:1a9c::1 dev eth1 metric 1024 pref medium
```


c. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

ping -6 -I *源端云服务器主网卡地址 目的端云服务器地址*

ping -6 -I *源端云服务器扩展网卡地址 目的端云服务器地址*

命令示例：

ping -6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044

ping -6 -I 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044

回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。

```
[root@ecs-resource ~]# ping -6 -I 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044(2407:c080:1200:1dd9:16a7:fe7a:8f71:7044) from
2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64 time=0.770 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64 time=0.295 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64 time=0.245 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2080ms
rtt min/avg/max/mdev = 0.245/0.436/0.770/0.237 ms
[root@ecs-resource ~]# ping -6 -I 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8
2407:c080:1200:1dd9:16a7:fe7a:8f71:7044
PING 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044(2407:c080:1200:1dd9:16a7:fe7a:8f71:7044) from
2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=1 ttl=64 time=0.922 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=2 ttl=64 time=0.307 ms
64 bytes from 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044: icmp_seq=3 ttl=64 time=0.174 ms
^C
--- 2407:c080:1200:1dd9:16a7:fe7a:8f71:7044 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2059ms
rtt min/avg/max/mdev = 0.174/0.467/0.922/0.326 ms
```

6. 执行以下步骤，为云服务器配置永久路由。

a. 执行以下命令，打开“/etc/rc.local”文件。

vi /etc/rc.local

b. 按**i**进入编辑模式。

c. 在文件末尾添加以下配置。

```
# check eth0
for ((x=0; x<10; x++)); do
  if (ip addr show eth0 | grep -w 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 >/dev/null 2>&1);
then
    break
  fi
  sleep 1
done

# Add v6 routes for eth0
ip -6 route flush table 10
ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table 10
ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10
ip -6 rule add from 2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9 table 10

# check eth1
for ((x=0; x<10; x++)); do
  if (ip addr show eth1 | grep -w 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 >/dev/null 2>&1);
then
    break
  fi
  sleep 1
done
```



```
# Add v6 routes for eth1
ip -6 route flush table 20
ip -6 route add default via 2407:c080:1200:1a9c::1 dev eth1 table 20
ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20
ip -6 rule add from 2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8 table 20
```

其中，参数说明如下：

- check eth0：循环检查主网卡eth0是否获取到IPv6地址（eth0网卡地址为2407:c080:1200:1dd8:859c:e5d5:8b3d:a2d9），每秒检查一次，重试次数为10次。
- Add v6 routes for eth0：主网卡的策略路由，和5.a配置保持一致。
- check eth1：循环检查扩展网卡eth1是否获取到IPv6地址（eth1网卡地址为2407:c080:1200:1a9c:7cc0:63b5:8e65:4dd8），每秒检查一次，重试次数为10次。
- Add v6 routes for eth1：扩展网卡的策略路由，和5.a配置保持一致。

d. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下命令，为“/etc/rc.local”文件添加执行权限。

chmod +x /etc/rc.local

说明

如果您的操作系统为Redhat、EulerOS，执行完6.e后，还需要执行以下命令，权限才会添加成功。

chmod +x /etc/rc.d/rc.local

f. 执行以下命令，重启云服务器。

reboot

须知

“/etc/rc.local”文件添加中添加的策略路由，需要重启云服务器后才会生效，此处请确保不影响业务再重启云服务器操作。

g. 参考5.b~5.c，检查策略路由添加情况，并验证源端和目的通信是否正常。

5.3.2.4 为多网卡 Linux 云服务器配置 IPv4 和 IPv6 策略路由（Ubuntu）

操作场景

本文档以Ubuntu 22.04 server 64bit为例，为指导您为多网卡的云服务器配置策略路由。

- IPv4：**Linux IPv4操作步骤 (Ubuntu)**
- IPv6：**Linux IPv6操作步骤 (Ubuntu)**

关于云服务器双网卡的背景知识及组网说明，请参见**方案概述**。

Linux IPv4 操作步骤 (Ubuntu)

1. 收集配置策略路由需要的云服务器网卡地址等信息。
   具体操作请参见**收集云服务器网络信息**。

本示例中，云服务器的网络信息如表5-15所示。

表 5-15 Linux IPv4 场景信息说明（Ubuntu）

类型	主网卡	扩展网卡
源端	• 网卡地址：10.0.0.138 • 子网网段：10.0.0.0/24 • 子网网关：10.0.0.1	• 网卡地址：10.0.1.25 • 子网网段：10.0.1.0/24 • 子网网关：10.0.1.1
目的端	网卡地址：10.0.2.146	不涉及

2. 登录源端云服务器。

   ECS有多种登录方法，具体请参见登录弹性云服务器。

3. 执行以下命令，检查源端云服务器主网卡和目的端云服务器通信情况。

   配置多网卡策略路由前，请务必确保源端主网卡和目的端通信正常。

   ping -I *源端云服务器主网卡地址 目的端云服务器地址*

   命令示例：

   ping -I 10.0.0.138 10.0.2.146

   回显类似如下信息，表示可以正常通信。

```
root@ecs-s:~# ping -I 10.0.0.138 10.0.2.146
PING 10.0.2.146 (10.0.2.146) from 10.0.0.138 : 56(84) bytes of data.
64 bytes from 10.0.2.146: icmp_seq=1 ttl=64 time=0.247 ms
64 bytes from 10.0.2.146: icmp_seq=2 ttl=64 time=0.194 ms
64 bytes from 10.0.2.146: icmp_seq=3 ttl=64 time=0.190 ms
^C
--- 10.0.2.146 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2049ms
rtt min/avg/max/mdev = 0.190/0.210/0.247/0.025 ms
```

4. 执行以下命令，查看云服务器网卡名称。

   ip addr

   回显类似如下信息，通过网卡地址查找对应的网卡名称，本示例中：

   - 10.0.0.138为主网卡地址，对应的名称为eth0。
   - 10.0.1.25为扩展网卡地址，对应的名称为eth1。

```
root@ecs-s:~# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether fa:16:3e:22:22:ac brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.0.0.138/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 107999167sec preferred_lft 107999167sec
    inet6 fe80::f816:3eff:fe22:22ac/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen
1000
    link/ether fa:16:3e:22:23:3b brd ff:ff:ff:ff:ff:ff
    altname enp4s1
    inet 10.0.1.25/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
       valid_lft 107999167sec preferred_lft 107999167sec
    inet6 fe80::f816:3eff:fe22:233b/64 scope link
       valid_lft forever preferred_lft forever
```


5. 执行以下步骤，为云服务器配置临时路由。

须知

临时路由配置完后立即生效，当云服务器重启后临时路由会丢失，请执行完5配置完临时路由后，继续执行6配置永久路由，避免云服务器重启后网络中断。

a. 依次执行以下命令，添加主网卡和扩展网卡的策略路由。

- 主网卡
  ip route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*
  ip route add *子网网段* **dev** *网卡名称* **table** *路由表名称*
  ip rule add from *网卡地址* **table** *路由表名称*
- 扩展网卡
  ip route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*
  ip route add *子网网段* **dev** *网卡名称* **table** *路由表名称*
  ip rule add from *网卡地址* **table** *路由表名称*

参数说明如下：

- 网卡名称：填写4中所查名称。
- 路由表名称：自定义路由表名称，此处请使用数字命名路由表。
- 其他网络信息：填写1中收集的地址。

命令示例：

- 主网卡
  ip route add default via 10.0.0.1 dev eth0 table 10
  ip route add 10.0.0.0/24 dev eth0 table 10
  ip rule add from 10.0.0.138 table 10
- 扩展网卡
  ip route add default via 10.0.1.1 dev eth1 table 20
  ip route add 10.0.1.0/24 dev eth1 table 20
  ip rule add from 10.0.1.25 table 20

说明

如果云服务器有多张网卡，请依次为所有网卡添加策略路由。

b. 依次执行以下命令，确认策略路由是否添加成功。
ip rule
ip route show table *主网卡路由表名称*
ip route show table *扩展网卡路由表名称*
其中，路由表名称为5.a中自定义的名称。
命令示例：
ip rule

ip route show table 10

ip route show table 20

回显类似如下信息，表示策略路由添加成功。

```
root@ecs-s:~# ip rule
0:      from all lookup local
32764:  from 10.0.1.25 lookup 20
32765:  from 10.0.0.138 lookup 10
32766:  from all lookup main
32767:  from all lookup default
root@ecs-s:~# ip route show table 10
default via 10.0.0.1 dev eth0
10.0.0.0/24 dev eth0 scope link
root@ecs-s:~# ip route show table 20
default via 10.0.1.1 dev eth1
10.0.1.0/24 dev eth1 scope link
```

c. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

ping -I *源端云服务器主网卡地址 目的端云服务器地址*

ping -I *源端云服务器扩展网卡地址 目的端云服务器地址*

命令示例：

ping -I 10.0.0.138 10.0.2.146

ping -I 10.0.1.25 10.0.2.146

回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。

```
root@ecs-s:~# ping -I 10.0.0.138 10.0.2.146
PING 10.0.2.146 (10.0.2.146) from 10.0.0.138 : 56(84) bytes of data.
64 bytes from 10.0.2.146: icmp_seq=1 ttl=64 time=0.258 ms
64 bytes from 10.0.2.146: icmp_seq=2 ttl=64 time=0.242 ms
64 bytes from 10.0.2.146: icmp_seq=3 ttl=64 time=0.165 ms
^C
--- 10.0.2.146 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.165/0.221/0.258/0.040 ms
root@ecs-s:~# ping -I 10.0.1.25 10.0.2.146
PING 10.0.2.146 (10.0.2.146) from 10.0.1.25 : 56(84) bytes of data.
64 bytes from 10.0.2.146: icmp_seq=1 ttl=64 time=0.498 ms
64 bytes from 10.0.2.146: icmp_seq=2 ttl=64 time=0.427 ms
64 bytes from 10.0.2.146: icmp_seq=3 ttl=64 time=0.185 ms
^C
--- 10.0.2.146 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.185/0.370/0.498/0.133 ms
```

6. 执行以下步骤，为云服务器配置永久路由。

a. 执行以下命令，为systemd服务创建一个新的“network-routes.service”文件。

vi /etc/systemd/system/network-routes.service

b. 按**i**进入编辑模式。

c. 在文件末尾添加以下配置。

```
[Unit]
Description=Network Routes Configuration
After=network.target

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/bin/bash -c 'for((x=0; x<10; x++)); do [[ $(ip addr show eth0 | grep -w 10.0.0.138
>/dev/null 2>&1 && echo 1) ]] && break; sleep 1; done; ip route flush table 10; ip route add
default via  10.0.0.1 dev eth0 table 10; ip route add 10.0.0.0/24 dev eth0 table 10; ip rule add
from 10.0.0.138 table 10; for((x=0; x<10; x++)); do [[ $(ip addr show eth1 | grep -w 10.0.1.25
>/dev/null 2>&1 && echo 1) ]] && break; sleep 1; done; ip route flush table 20; ip route add
```



```
default via 10.0.1.1 dev eth1 table 20; ip route add 10.0.1.0/24 dev eth1 table 20; ip rule add
from 10.0.1.25 table 20; ip rule add to 169.254.169.254 table main'

[Install]
WantedBy=multi-user.target
```

其中，参数说明如下：

- for循环：循环检查主网卡eth0或者扩展网卡eth1是否获取到IPv4地址（eth0网卡地址为10.0.0.138，eth1网卡地址为10.0.1.25），每秒检查一次，重试次数为10次。
- ip route flush table 路由表名称：假如路由表有残留路由，使用该命令会清空指定路由表中残留的路由，避免影响本次配置新的路由。
- 主网卡的策略路由，和**5.a**配置保持一致。
- 扩展网卡的策略路由，和**5.a**配置保持一致。
- ip rule add to 169.254.169.254 table main：配置cloud-init地址，请和本示例中的配置保持一致，不要修改。

d. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下命令，重新加载systemd配置，并启动服务。

systemctl daemon-reload

systemctl enable network-routes.service

回显类似如下信息，表示启动成功。

```
root@ecs-s:~# systemctl daemon-reload
root@ecs-s:~# systemctl enable network-routes.service
Created symlink /etc/systemd/system/multi-user.target.wants/network-routes.service → /etc/
systemd/system/network-routes.service.
```

f. 执行以下命令，重启云服务器。

reboot

须知

“network-routes.service”文件添加中添加的策略路由，需要重启云服务器后才会生效，此处请确保不影响业务再重启云服务器操作。

g. 参考**5.b**~**5.c**，检查策略路由添加情况，并验证源端和目的通信是否正常。

Linux IPv6 操作步骤（Ubuntu）

1. 收集配置策略路由需要的云服务器网卡地址等信息。

   具体操作请参见**收集云服务器网络信息**。

   本示例中，云服务器的网络信息如**表5-16**所示。

表 5-16 Linux IPv6 场景信息说明（Ubuntu）

类型	主网卡	扩展网卡
源端	• IPv4网卡地址：10.0.0.138 • IPv6网卡地址：2407:c080:1200:1dd8:1473:49db:22d7:13c7 • 子网IPv6网段：2407:c080:1200:1dd8::/64 • 子网IPv6网关：2407:c080:1200:1dd8::1	• IPv4网卡地址：10.0.1.25 • IPv6网卡地址：2407:c080:1200:1a9c:691e:fffe:7e22:12c4 • 子网IPv6网段：2407:c080:1200:1a9c::/64 • 子网IPv6网关：2407:c080:1200:1a9c::1
目的端	• IPv4网卡地址：10.0.2.146 • IPv6网卡地址：2407:c080:1200:1dd9:f5e1:94d1:2822:dede	不涉及

2. 登录源端云服务器。

   ECS有多种登录方法，具体请参见**登录弹性云服务器**。

3. 执行以下步骤，确保云服务器已开启IPv6协议栈，并且正常获取到IPv6地址。

须知

对于源端和目的端的IPv6云服务器，均需要执行该操作，确保云服务器已获取到IPv6地址，否则云服务器无法通过IPv6地址进行通信。

本章节云服务器使用的操作系统为Ubuntu 22.04 server 64bit公共镜像，以下针对该操作系统举例，更多操作系统配置指导，请参见**动态获取IPv6地址**的“Linux操作系统（手动配置启用IPv6）”小节。

a. 执行以下命令，检查云服务器是否可以获取到IPv6地址。

   ip addr

   回显类似如下信息，eth0和eth1为云服务器的网卡，只有一行inet6地址，为fe80开头，表示该云服务器已开启IPv6协议栈，但是未获取到IPv6地址，需要继续执行**3.b**~**3.h**，获取IPv6地址。

```
root@ecs-s:~# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:22:22:ac brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.0.0.138/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 107999781sec preferred_lft 107999781sec
    inet6 fe80::f816:3eff:fe22:22ac/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:22:23:3b brd ff:ff:ff:ff:ff:ff
    altname enp4s1
    inet 10.0.1.25/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
       valid_lft 107999781sec preferred_lft 107999781sec
```



```
   inet6 fe80::f816:3eff:fe22:233b/64 scope link
      valid_lft forever preferred_lft forever
```

b. 执行以下命令，查看云服务器网卡名称。

ifconfig

回显类似如下信息，通过网卡地址查找对应的网卡名称，本示例中：

- 10.0.0.138为主网卡地址，对应的名称为eth0。
- 10.0.1.25为扩展网卡地址，对应的名称为eth1。

```
root@ecs-s:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.138  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::f816:3eff:fe22:22ac  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:22:22:ac  txqueuelen 1000  (Ethernet)
        RX packets 863  bytes 269089 (269.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1117  bytes 359807 (359.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.1.25  netmask 255.255.255.0  broadcast 10.0.1.255
        inet6 fe80::f816:3eff:fe22:233b  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:22:23:3b  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 1358 (1.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 973 (973.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

c. 执行以下步骤，配置“01-netcfg.yaml”文件。

i. 执行以下命令，进入“/etc/netplan/”目录。

cd /etc/netplan

ii. 执行以下命令，打开“01-netcfg.yaml”文件。

vi 01-netcfg.yaml

iii. 按**i**进入编辑模式。

iv. 按照以下示例，分别在待配置的网卡下添加内容**dhcp6: true**，注意新添加内容和已有内容格式保持统一。

本示例中，**3.b**中查询到的主网卡名称为eth0、扩展网卡名称为eth1。

```
network:
    version: 2
    renderer: NetworkManager
    ethernets:
        eth0:
            dhcp4: true
            dhcp6: true
        eth1:
            dhcp4: true
            dhcp6: true
        eth2:
            dhcp4: true
        eth3:
            dhcp4: true
        eth4:
            dhcp4: true
```

v. 按**ESC**退出，并输入**:wq!**保存配置。

d. 执行以下命令，修改“01-netcfg.yaml”文件权限，确保只有文件所有者拥有读写的权限。

chmod 600 /etc/netplan/01-netcfg.yaml

chown root:root /etc/netplan/01-netcfg.yaml

e. 执行以下命令，使配置修改生效。

netplan apply

f. 执行以下步骤，配置“NetworkManager.conf”文件。

i. 执行以下命令，打开“NetworkManager.conf”文件。

vi /etc/NetworkManager/NetworkManager.conf

ii. 按**i**进入编辑模式。

iii. 按照以下示例，在文件中添加内容**dhcp=dhclient**，注意新添加内容和已有内容格式保持统一。

```
[main]
plugins=ifupdown,keyfile
dhcp=dhclient

[ifupdown]
managed=true

[device]
wifi.scan-rand-mac-address=no
```

iv. 按**ESC**退出，并输入**:wq!**保存配置。

g. 执行以下命令，重启网络服务使配置生效。

systemctl restart NetworkManager

h. 执行以下命令，检查云服务器是否可以获取到IPv6地址。

ip addr

回显类似如下信息，eth0和eth1网卡有两行inet6地址，新增一行2407开头的地址，表示配置成功。

```
root@ecs-s:/etc/netplan# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:22:22:ac brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
    inet 10.0.0.138/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
       valid_lft 107999982sec preferred_lft 107999982sec
    inet6 2407:c080:1200:1dd8:1473:49db:22d7:13c7/128 scope global dynamic noprefixroute
       valid_lft 7182sec preferred_lft 7182sec
    inet6 fe80::f816:3eff:fe22:22ac/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:22:23:3b brd ff:ff:ff:ff:ff:ff
    altname enp4s1
    inet 10.0.1.25/24 brd 10.0.1.255 scope global dynamic noprefixroute eth1
       valid_lft 107999982sec preferred_lft 107999982sec
    inet6 2407:c080:1200:1a9c:691e:fffe:7e22:12c4/128 scope global dynamic noprefixroute
       valid_lft 7182sec preferred_lft 7182sec
    inet6 fe80::f816:3eff:fe22:233b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

i. 登录目的端云服务器，参考**3.a**~**3.h**，配置目的云服务器获取IPv6地址。

回显类似如下信息，eth0有两行inet6地址，新增一行2407开头的地址，表示目的云服务器已成功获取IPv6地址。

```
root@ecs-d:/etc/netplan# ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
qlen 1000
    link/ether fa:16:3e:22:24:b4 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
```



```
    inet 10.0.2.146/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 107999994sec preferred_lft 107999994sec
    inet6 2407:c080:1200:1dd9:f5e1:94d1:2822:dede/128 scope global dynamic noprefixroute
       valid_lft 7195sec preferred_lft 7195sec
    inet6 fe80::f816:3eff:fe22:24b4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

4. 登录源端云服务器，执行以下命令，检查源端云服务器主网卡和目的端云服务器通信情况。

   配置多网卡策略路由前，请务必确保源端主网卡和目的端通信正常。

   ping6 -I *源端云服务器主网卡地址 目的端云服务器地址*

   命令示例：

   ping6 -I 2407:c080:1200:1dd8:1473:49db:22d7:13c7 2407:c080:1200:1dd9:f5e1:94d1:2822:dede

   回显类似如下信息，表示可以正常通信。

```
root@ecs-s:/etc/netplan# ping6 -I 2407:c080:1200:1dd8:1473:49db:22d7:13c7
2407:c080:1200:1dd9:f5e1:94d1:2822:dede
PING 2407:c080:1200:1dd9:f5e1:94d1:2822:dede(2407:c080:1200:1dd9:f5e1:94d1:2822:dede) from
2407:c080:1200:1dd8:1473:49db:22d7:13c7 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=1 ttl=64 time=0.244 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=2 ttl=64 time=0.212 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=3 ttl=64 time=0.169 ms
^C
--- 2407:c080:1200:1dd9:f5e1:94d1:2822:dede ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2033ms
rtt min/avg/max/mdev = 0.169/0.208/0.244/0.030 ms
```

5. 登录源端云服务器，执行以下步骤，为云服务器配置临时路由。

   须知

   临时路由配置完后立即生效，当云服务器重启后临时路由会丢失，请执行5配置完临时路由后，继续执行6配置永久路由，避免云服务器重启后网络中断。

   a. 依次执行以下命令，添加主网卡和扩展网卡的策略路由。

      - 主网卡

        ip -6 route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

        ip -6 route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

        ip -6 rule add from *网卡地址* **table** *路由表名称*

      - 扩展网卡

        ip -6 route add default via *子网网关* **dev** *网卡名称* **table** *路由表名称*

        ip -6 route add *子网网段* **dev** *网卡名称* **table** *路由表名称*

        ip -6 rule add from *网卡地址* **table** *路由表名称*

      参数说明如下：

      - 网卡名称：填写3.b中所查名称。
      - 路由表名称：自定义路由表名称，此处请使用数字命名路由表。
      - 其他网络信息：填写1中收集的地址。

      命令示例：

- 主网卡

  ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table 10

  ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10

  ip -6 rule add from 2407:c080:1200:1dd8:1473:49db:22d7:13c7 table 10

- 扩展网卡

  ip -6 route add default via 2407:c080:1200:1a9c::1 dev eth1 table 20

  ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20

  ip -6 rule add from 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 table 20

说明

如果云服务器有多张网卡，请依次为所有网卡添加策略路由。

b. 依次执行以下命令，确认策略路由是否添加成功。

ip -6 rule

ip -6 route show table *主网卡路由表名称*

ip -6 route show table *扩展网卡路由表名称*

其中，路由表名称为**5.a**中自定义的名称。

命令示例：

ip -6 rule

ip -6 route show table 10

ip -6 route show table 20

回显类似如下信息，表示策略路由添加成功。

```
root@ecs-s:/etc/netplan# ip -6 rule
0:      from all lookup local
32764:  from 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 lookup 20
32765:  from 2407:c080:1200:1dd8:1473:49db:22d7:13c7 lookup 10
32766:  from all lookup main
root@ecs-s:/etc/netplan# ip -6 route show table 10
2407:c080:1200:1dd8::/64 dev eth0 metric 1024 pref medium
default via 2407:c080:1200:1dd8::1 dev eth0 metric 1024 pref medium
root@ecs-s:/etc/netplan# ip -6 route show table 20
2407:c080:1200:1a9c::/64 dev eth1 metric 1024 pref medium
default via 2407:c080:1200:1a9c::1 dev eth1 metric 1024 pref medium
```

c. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

ping -6 -I *源端云服务器主网卡地址 目的端云服务器地址*

ping -6 -I *源端云服务器扩展网卡地址 目的端云服务器地址*

命令示例：

ping6 -I 2407:c080:1200:1dd8:1473:49db:22d7:13c7 2407:c080:1200:1dd9:f5e1:94d1:2822:dede

ping6 -I 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 2407:c080:1200:1dd9:f5e1:94d1:2822:dede

回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。

```
root@ecs-s:/etc/netplan# ping6 -I 2407:c080:1200:1dd8:1473:49db:22d7:13c7
2407:c080:1200:1dd9:f5e1:94d1:2822:dede
```



```
PING 2407:c080:1200:1dd9:f5e1:94d1:2822:dede(2407:c080:1200:1dd9:f5e1:94d1:2822:dede)
from 2407:c080:1200:1dd8:1473:49db:22d7:13c7 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=1 ttl=64 time=0.260 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=2 ttl=64 time=0.248 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=3 ttl=64 time=0.165 ms
^C
--- 2407:c080:1200:1dd9:f5e1:94d1:2822:dede ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.165/0.224/0.260/0.042 ms
root@ecs-s:/etc/netplan# ping6 -I 2407:c080:1200:1a9c:691e:fffe:7e22:12c4
2407:c080:1200:1dd9:f5e1:94d1:2822:dede
PING 2407:c080:1200:1dd9:f5e1:94d1:2822:dede(2407:c080:1200:1dd9:f5e1:94d1:2822:dede)
from 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 : 56 data bytes
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=1 ttl=64 time=0.592 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=2 ttl=64 time=0.208 ms
64 bytes from 2407:c080:1200:1dd9:f5e1:94d1:2822:dede: icmp_seq=3 ttl=64 time=0.162 ms
^C
--- 2407:c080:1200:1dd9:f5e1:94d1:2822:dede ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.162/0.320/0.592/0.192 ms
```

6. 执行以下步骤，为云服务器配置永久路由。
   a. 执行以下命令，为systemd服务创建一个新的文件“network-routes6.service”。

      vi /etc/systemd/system/network-routes6.service

   b. 按**i**进入编辑模式。
   c. 在文件末尾添加以下配置。

```
[Unit]
Description=Network Routes Configuration
After=network.target

[Service]
Type=oneshot
RemainAfterExit=yes

ExecStart=/bin/bash -c 'for((x=0; x<10; x++)); do [[ $(ip addr show eth0 | grep -w
2407:c080:1200:1dd8:1473:49db:22d7:13c7 >/dev/null 2>&1 && echo 1) ]] && break; sleep 1;
done; ip route flush table 10; ip -6 route add default via 2407:c080:1200:1dd8::1 dev eth0 table
10; ip -6 route add 2407:c080:1200:1dd8::/64 dev eth0 table 10; ip -6 rule add from
2407:c080:1200:1dd8:1473:49db:22d7:13c7 table 10; for((x=0; x<10; x++)); do [[ $(ip addr show
eth1 | grep -w 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 >/dev/null 2>&1 && echo 1) ]] &&
break; sleep 1; done; ip route flush table 20; ip -6 route add default via 2407:c080:1200:1a9c::1
dev eth1 table 20; ip -6 route add 2407:c080:1200:1a9c::/64 dev eth1 table 20; ip -6 rule add
from 2407:c080:1200:1a9c:691e:fffe:7e22:12c4 table 20'

[Install]
WantedBy=multi-user.target
```

      其中，参数说明如下：

      - for循环：检查主网卡eth0或者扩展网卡eth1是否获取到IPv6地址（eth0网卡IPv6地址为2407:c080:1200:1dd8:1473:49db:22d7:13c7，eth1网卡IPv6地址为2407:c080:1200:1a9c:691e:fffe:7e22:12c4），间隔时间为1s，重试次数为10次。
      - ip route flush table 路由表名称：假如路由表有残留路由，假如路由表有残留路由，使用该命令会清空指定路由表中残留的路由，避免影响本次配置新的路由。
      - 主网卡的策略路由，和**5.a**配置保持一致。
      - 扩展网卡的策略路由，和**5.a**配置保持一致。

   d. 按**ESC**退出，并输入**:wq!**保存配置。

e. 执行以下命令，重新加载systemd配置，并启动服务。

systemctl daemon-reload

systemctl enable network-routes6.service

回显类似如下信息，表示启动成功。

```
root@ecs-s:/etc/netplan# systemctl daemon-reload
root@ecs-s:/etc/netplan# systemctl enable network-routes6.service
Created symlink /etc/systemd/system/multi-user.target.wants/network-routes6.service → /etc/systemd/system/network-routes6.service.
```

f. 执行以下命令，重启云服务器。

reboot

须知

“network-routes6.service”文件添加中添加的策略路由，需要重启云服务器后才会生效，此处请确保不影响业务再重启云服务器操作。

g. 参考5.b~5.c，检查策略路由添加情况，并验证源端和目的通信是否正常。

5.3.2.5 为多网卡 Windows 云服务器配置 IPv4 和 IPv6 策略路由

操作场景

本文档以Windows 2012 64bit为例，指导用户为双网卡Windows云服务器配置策略路由。

- IPv4：**Windows IPv4操作步骤**
- IPv6：**Windows IPv6操作步骤**

关于云服务器双网卡的背景知识及组网说明，请参见**方案概述**。

Windows IPv4 操作步骤

1. 收集配置策略路由需要的云服务器网卡地址等信息。

   具体操作请参见**收集云服务器网络信息**。

   本示例中，云服务器的网络信息如**表5-17**所示。

   表 5-17 Windows IPv4 场景信息说明

类型	主网卡	扩展网卡
源端	• 网卡地址：10.0.0.59 • 子网网关：10.0.0.1	• 网卡地址：10.0.1.104 • 子网网关：10.0.1.1
目的端	网卡地址：10.0.2.12	不涉及

2. 登录源端云服务器。

   ECS有多种登录方法，具体请参见**登录弹性云服务器**。

3. 执行以下命令，检查源端云服务器主网卡和目的端云服务器通信情况。

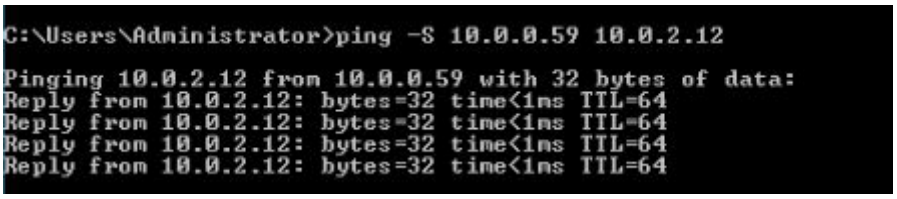
配置多网卡策略路由前，请务必确保源端主网卡和目的端通信正常。

ping -S *源端云服务器主网卡地址 目的端云服务器地址*

命令示例：

ping -S 10.0.0.59 10.0.2.12

回显类似如下信息，表示可正常通信。



4. 执行以下命令，添加扩展网卡的策略路由。

   route add -p 0.0.0.0 mask 0.0.0.0 *扩展网卡子网网关* **metric** *路由优先级*

   参数说明如下：

   - **0.0.0.0/0**：默认路由，请不要修改。
   - 扩展网卡子网网关：填写**1**中收集的地址。
   - 路由优先级：扩展网卡优先级必须小于主网卡，数字越大优先级越低，此处配置为261。

   命令示例：

   route add -p 0.0.0.0 mask 0.0.0.0 10.0.1.1 metric 261

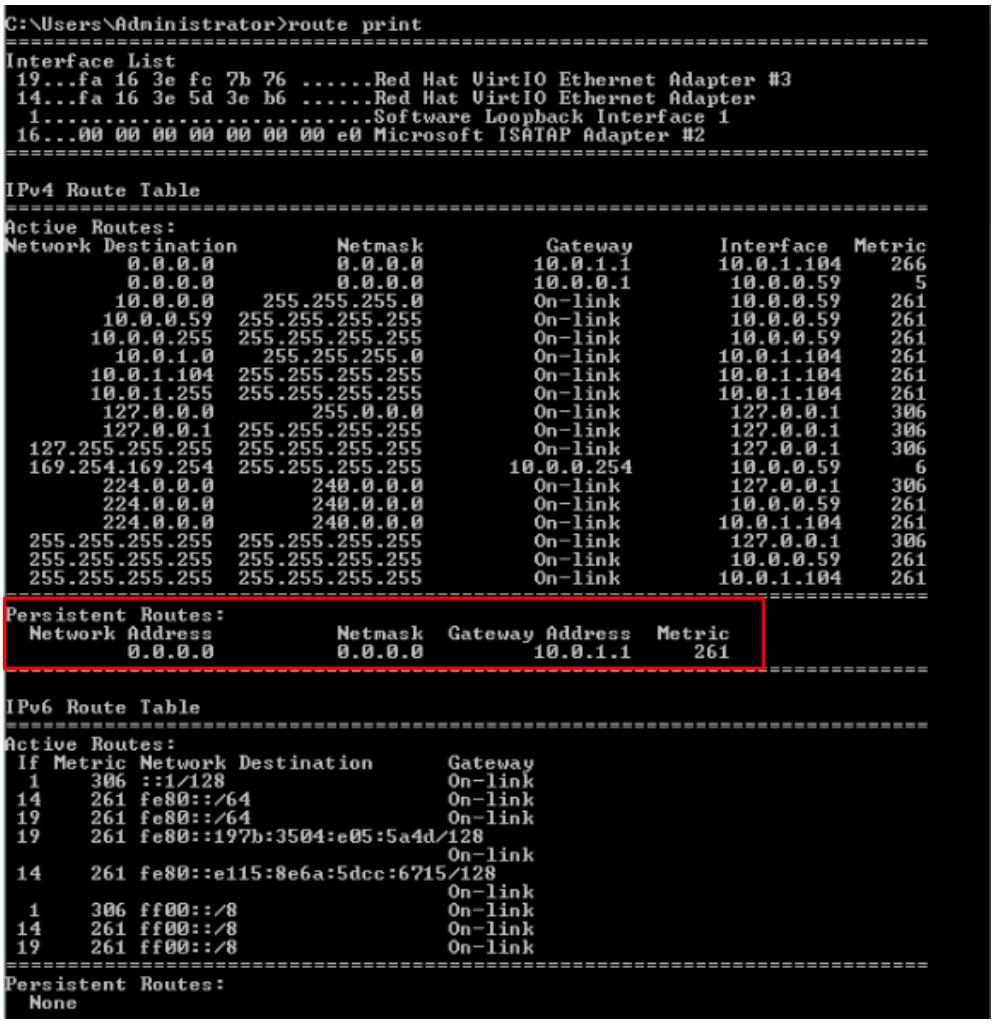
   说明

   - 主网卡策略路由系统已有，不需要添加。
   - 如果云服务器有多张扩展网卡，请依次为所有扩展网卡添加策略路由。

5. 执行以下命令，确认策略路由是否添加成功。

   route print

   回显类似如下信息，表示策略路由添加成功。该路由为永久路由，重启后不会丢失。



6. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

   ping -S *源端云服务器主网卡地址 目的端云服务器地址*

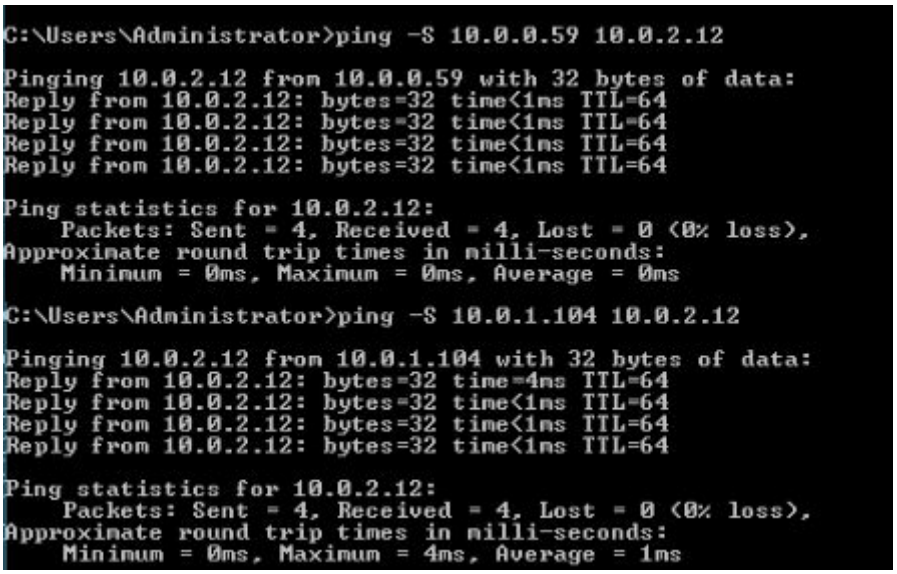
   ping -S *源端云服务器扩展网卡地址 目的端云服务器地址*

   命令示例：

   ping -S 10.0.0.59 10.0.2.12

   ping -S 10.0.1.104 10.0.2.12

   回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。



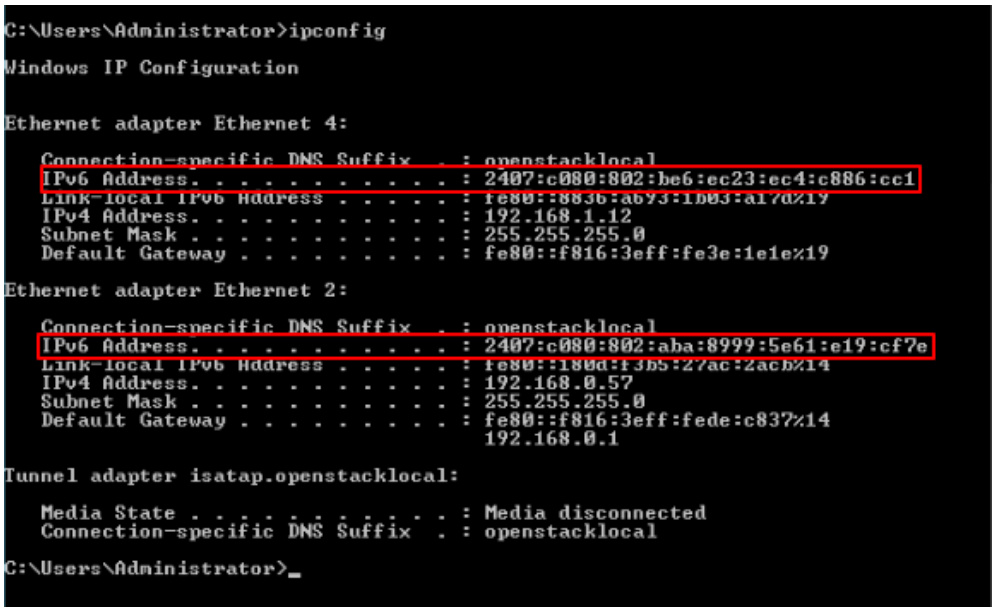
Windows IPv6 操作步骤

1. 收集配置策略路由需要的云服务器网卡地址等信息。
   具体操作请参见**收集云服务器网络信息**。
   本示例中，云服务器的网络信息如**表5-18**所示。

   表 5-18 Windows IPv6 场景信息说明

类型	主网卡	扩展网卡
源端	网卡地址： 2407:c080:802:aba:6788:fb94:d71f:8deb	网卡地址： 2407:c080:802:be6:71c8:42e0:d44e:eeb4
目的端	网卡地址： 2407:c080:802:be7:c2e6:d99c:b685:c6c8	不涉及

2. 登录源端云服务器。
   ECS有多种登录方法，具体请参见**登录弹性云服务器**。
3. 执行以下命令，确保云服务器已开启IPv6协议栈，并且正常获取到IPv6地址。
   ipconfig
   回显类似如下信息，每个网卡可以查看到IPv6地址，为2407开头的地址，表示可以自动获取到IPv6地址，不用进行配置。



须知

对于源端和目的端的IPv6云服务器，均需要执行该操作，确保云服务器已获取到IPv6地址，否则云服务器无法通过IPv6地址进行通信。

本章节云服务器使用的操作系统为Windows 2012 64bit公共镜像，无需额外配置，云服务器可自动获取获取到IPv6地址。如果您的云服务器无法自动获取到IPv6地址，请参见**动态获取IPv6地址**的“Windows 2012操作系统”和“Windows 2008操作系统”小节进行配置。

4. 执行以下命令，验证源端云服务器和目的端云服务器是否可以正常通信。

   ping -6 -S *源端云服务器主网卡地址 目的端云服务器地址*

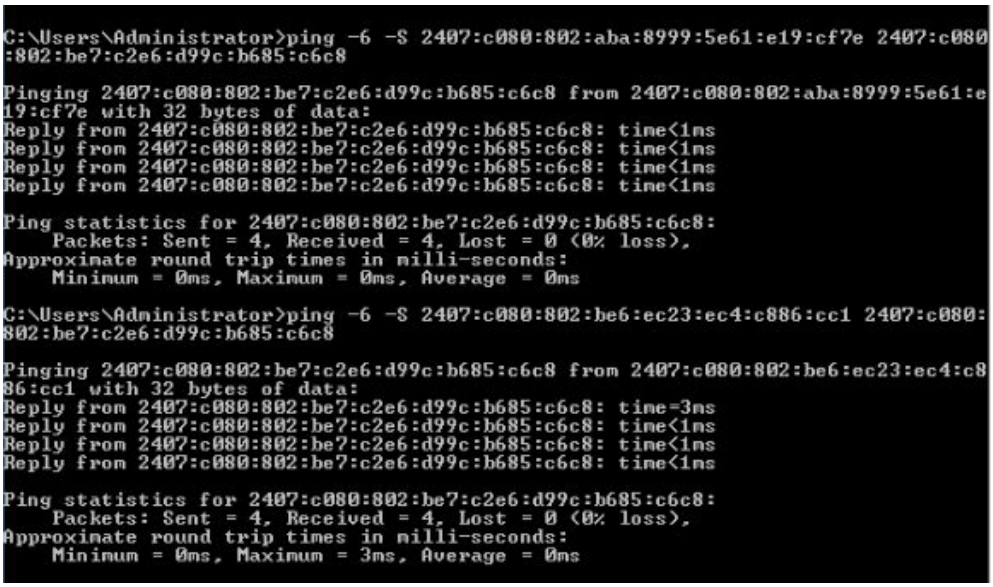
   ping -6 -S *源端云服务器扩展网卡地址 目的端云服务器地址*

   命令示例：

   ping -6 -S 2407:c080:802:aba:8999:5e61:e19:cf7e 2407:c080:802:be7:c2e6:d99c:b685:c6c8

   ping -6 -S 2407:c080:802:be6:ec23:ec4:c886:cc1 2407:c080:802:be7:c2e6:d99c:b685:c6c8

   回显类似如下信息，两个网卡均可以和目的端正常通信，表示策略路由配置成功。



须知

本章节示例中，云服务器使用Windows 2012 64bit公共镜像，对于IPv6场景，不需要在云服务器内配置策略路由，双网卡可正常通信。

6 访问控制

6.1 VPC 访问控制概述

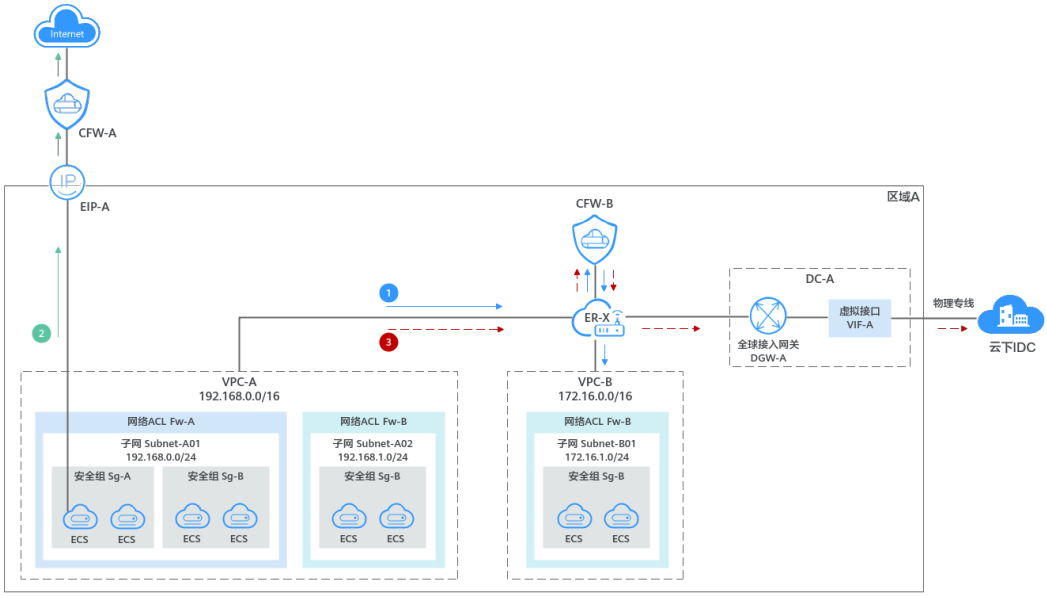
虚拟私有云VPC是您在云上的私有网络，通过配置安全策略，可以保障VPC内部署的实例安全运行，比如弹性云服务器、数据库、云容器等。

- 安全组对实例进行防护，将实例加入安全组内后，该实例将会受到安全组的保护。
- 网络ACL对整个子网进行防护，将子网关联至网络ACL，则子网内的所有实例都会受到网络ACL保护。相比安全组，网络ACL的防护范围更大。
- 云防火墙（Cloud Firewall，CFW）对VPC边界网络防护，可以对不同VPC之间、VPC和公网之间、VPC与云下IDC之间的流量防护，实现业务互访活动的可视化与安全防护。相比安全组和网络ACL，防护范围更大。

安全组、网络ACL和云防火墙的应用示例如**图6-1**所示。本示例中：

- 安全组：使用安全组Sg-A和安全组Sg-B，来防护安全组内ECS的流量。
- 网络ACL：使用网络ACL Fw-A防护子网Subnet-A01内所有ECS的流量，网络ACL Fw-B防护子网Subnet-A02和子网Subnet-B01内所有ECS的流量，网络ACL和安全组一起使用，双层防护提升安全保障。
- 云防火墙：
  - 防护VPC和公网之间的流量：ECS通过EIP-A访问公网，从EIP-A送达公网的流量需要经过云防火墙CFW-A的清洗。
  - 防护不同VPC之间的流量：通过ER-X连通VPC-A和VPC-B的网络，VPC之间互访的流量需要经过云防火墙CFW-B清洗。
  - 防护VPC和云下IDC之间的流量：通过ER-X和DC-A，连通VPC-A和云下IDC之间的网络，VPC-A去往DC-A的流量需要经过云防火墙CFW-B清洗，最终确保通过DC-A送至IDC的流量安全。

图 6-1 VPC 访问控制防护示意图



VPC 访问控制策略的区别说明

表6-1为您提供了不同VPC访问控制策略的区别，您可以根据业务需求按需选择。

表 6-1 不同 VPC 访问控制策略的区别

对比项	安全组	网络ACL	云防火墙 CFW
防护范围	实例级别：防护安全组内的实例，比如弹性云服务器、数据库、云容器实例等。	子网级别：防护整个子网，子网内的所有实例都会受到网络ACL的保护。	VPC边界网络防护：支持不同VPC之间、VPC和公网之间、VPC与云下IDC之间的流量防护，实现业务互访活动的可视化与安全防护。
是否必选	必选，实例必须至少加入到一个安全组内。	非必选，您可以根据业务需求选择是否为子网关联网络ACL。	非必选，您可以根据业务需求选择是否开启VPC边界防火墙防护。
是否收费	不收取费用	不收取费用	收取费用
有无状态	有状态，允许入站请求/出站请求的响应流量出入实例，不受规则限制。	有状态，允许入站请求/出站请求的响应流量出入子网，不受规则限制。	有状态，允许入站请求/出站请求的响应流量出入公网、VPC或者云专线，不受规则限制。

对比项	安全组	网络ACL	云防火墙 CFW
规则策略	安全组支持设置允许和拒绝策略。 ● 允许策略：对于匹配成功的流量，允许流入/流出实例。 ● 拒绝策略：对于匹配成功的流量，拒绝流入/流出实例。	网络ACL支持设置允许和拒绝策略。 ● 允许策略：对于匹配成功的流量，允许流入/流出子网。 ● 拒绝策略：对于匹配成功的流量，拒绝流入/流出子网。	云防火墙支持设置允许和拒绝策略。 允许策略：对于匹配成功的流量，允许流入/流出公网、VPC或者云专线。 拒绝策略：对于匹配成功的流量，拒绝流入/流出公网、VPC或者云专线。
规则报文组	支持报文三元组（即协议、端口和源/目的地址）过滤。	支持报文五元组（即协议、源端口、目的端口、源地址和目的地址）过滤。	支持报文五元组（即协议、源端口、目的端口、源地址、目的地址）以及域名、IP地理位置、七层应用协议等过滤。
规则生效顺序	当实例上绑定多个安全组，并且安全组中存在多条规则时，生效顺序如下： 1. 首先根据实例绑定安全组的顺序生效，排在前面的安全组优先级高。 2. 然后根据安全组内规则的优先级生效，优先级的数字越小，优先级越高。 3. 当优先级相同的情况下，再按照策略匹配，拒绝策略高于允许策略。	一个子网只能绑定一个网络ACL，当网络ACL存在多条规则时，根据规则的生效顺序依次匹配流量。序号越小，排序越靠前，表示流量优先匹配该规则。	当云防火墙实例上设置多条防护规则时，根据规则的优先级进行生效。优先级数字越小，规则排序越靠前，越先生效。

对比项	安全组	网络ACL	云防火墙 CFW
应用操作	• 创建实例（比如弹性云服务器）时，必须选择一个安全组，如果当前用户名下没有安全组，则系统会自动创建默认安全组。 • 实例创建完成后，您可以执行以下操作： – 在安全组控制台，添加/移出实例。 – 在实例控制台，为实例添加/移除安全组。	创建子网没有网络ACL选项，需要先创建网络ACL，添加出入规则，并在网络ACL内关联子网。当网络ACL状态为已开启，将会对子网生效。	创建云防火墙（专业版）并配置企业路由器，将流量引至云防火墙，通过防护规则放行或者拦截流量，放行后的流量需要经过入侵防御IPS、病毒防御等功能的多重检测。

须知

如果需要使用高阶防护能力（比如通过域名/地理位置/时间计划进行访问控制、IPS入侵检测、反病毒等七层防护能力），或者您的业务有高等级保护要求，推荐您使用**云防火墙CFW**。

流量匹配安全组和网络 ACL 规则的顺序

当安全组和网络ACL同时存在时，流量优先匹配网络ACL的规则，然后匹配安全组规则。如**图6-2**所示，以入方向流量为例，为您详细介绍安全组和网络ACL规则的匹配顺序。

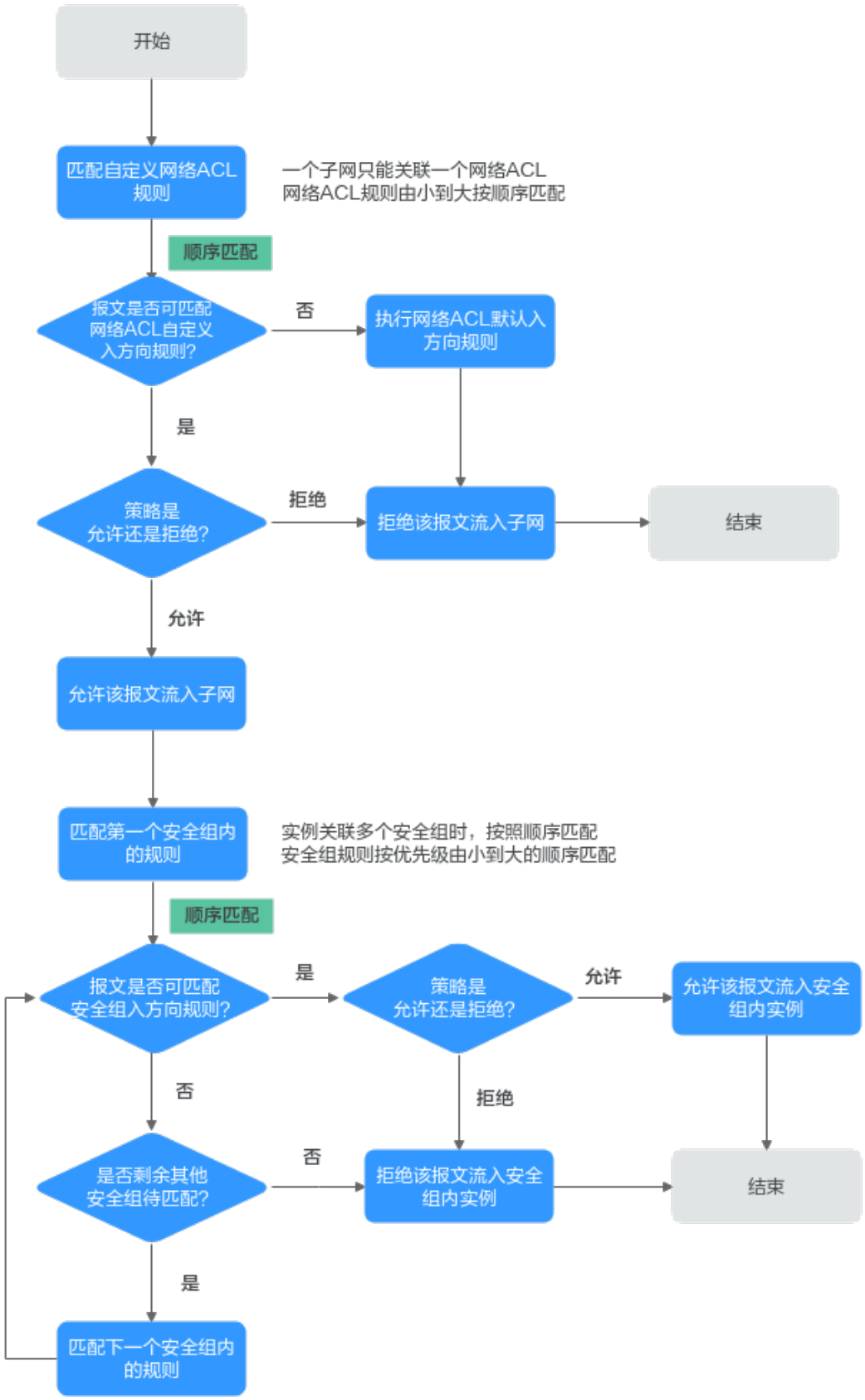
1. 流量优先匹配网络ACL规则：
   - 当流量未匹配上任何自定义网络ACL规则，则流量执行默认网络ACL规则，拒绝流量流入子网。
   - 当流量匹配上自定义网络ACL规则，则根据网络ACL规则策略决定流量走向。
     - 当策略为拒绝时，则拒绝该流量流入子网。
     - 当策略为允许时，则允许该流量流入子网。
2. 当流量通过网络ACL进入子网时，流量进一步匹配安全组规则：
   a. 当实例关联多个安全组时，流量按照安全组的顺序进行匹配。首先匹配第一个安全组内的规则。
      i. 当流量未匹配上任何安全组规则时，则拒绝该流量进入实例。

ii. 当流量匹配上安全组规则，则根据安全组规则策略决定流量走向。
    - 当策略为拒绝时，则拒绝该流量流入实例。
    - 当策略为允许时，则允许该流量流入实例。

b. 对于未成功匹配第一个安全组内规则的流量，继续匹配第二个安全组内的规则。

c. 当遍历了所有安全组的入方向规则，流量均没有匹配上时，则拒绝该流量流入实例。

图 6-2 网络 ACL 和安全组的匹配顺序



如图6-3所示，以下为您提供具体的流量匹配示例。VPC-A内有子网Subnet-A，Subnet-A内有两台弹性云服务器ECS-A和ECS-B。安全防护策略如下：

- 子网Subnet-A上关联了网络ACL Fw-A。Fw-A中的默认规则不能删除，流量优先匹配已添加的自定义规则，网络ACL规则示例请参见表6-2。
- 弹性云服务器ECS-A和ECS-B由安全组Sg-A来防护。创建安全组Sg-A时，您可以选择已有模板，模板中会自带部分安全组规则。您可以对系统自带的规则进行修改或者删除，也可以添加自定义规则，安全组规则示例请参见表6-3。

图 6-3 网络 ACL 和安全组的匹配顺序示例

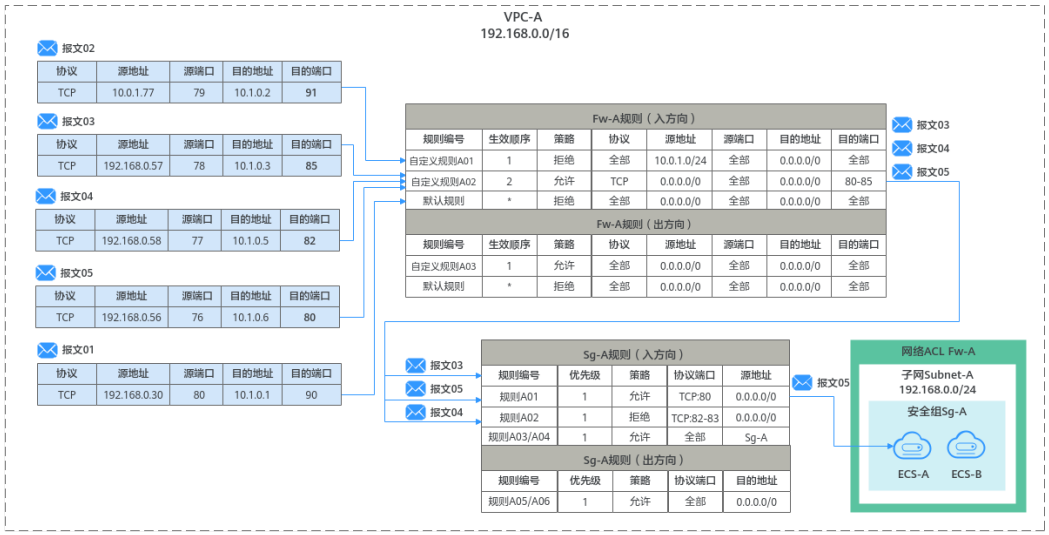


表 6-2 网络 ACL Fw-A 规则说明

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	说明
入方向	1	IPv4	拒绝	全部	10.0.1.0/24	全部	0.0.0.0/0	全部	自定义网络ACL规则A01：拒绝来自特定IP地址10.0.1.0/24网段的流量流入子网内
入方向	2	IPv4	允许	TCP	0.0.0.0/0	全部	0.0.0.0/0	80-85	自定义网络ACL规则A02：允许所有流量访问子网内实例的80-85端口
入方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认网络ACL规则：拒绝所有流量流入子网
出方向	1	IPv4	允许	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	自定义网络ACL规则A03：允许所有流量从子网流出

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	说明
出方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认网络ACL规则：拒绝所有流量从子网流出

表 6-3 安全组 Sg-A 规则说明

方向	优先级	策略	类型	协议端口	源地址/目的地址	描述
入方向	1	允许	IPv4	自定义 TCP：80	源地址：0.0.0.0/0	安全组规则A01：针对全部IPv4协议，允许所有流量访问安全组内实例的80端口
入方向	1	拒绝	IPv4	自定义 TCP：82-83	源地址：0.0.0.0/0	安全组规则A02：针对全部IPv4协议，拒绝所有流量访问安全组内实例的82和83端口
入方向	1	允许	IPv4	全部	源地址：当前安全组（Sg-A）	安全组规则A03：针对全部IPv4协议，确保安全组内实例网络互通
入方向	1	允许	IPv6	全部	源地址：当前安全组（Sg-A）	安全组规则A04：针对全部IPv6协议，确保安全组内实例网络互通
出方向	1	允许	IPv4	全部	目的地址：0.0.0.0/0	安全组规则A05：针对全部IPv4协议，允许所有流量从安全组内实例流出
出方向	1	允许	IPv6	全部	目的地址：::/0	安全组规则A06：针对全部IPv6协议，允许所有流量从安全组内实例流出

基于以上场景，不同入方向报文对规则的匹配情况如下：

- **报文01：**报文01无法匹配上Fw-A中的自定义网络ACL规则，则匹配默认规则，拒绝该报文流入子网。
- **报文02：**报文02可匹配上Fw-A中的自定义网络ACL规则A01，根据规则策略，拒绝该报文流入子网。
- **报文03：**报文03可匹配上Fw-A中的自定义网络ACL规则A02，根据规则策略，允许该报文流入子网。该报文继续匹配安全组规则，无法匹配上Sg-A的任何入方向规则，拒绝该报文流入实例。

- **报文04：**报文04可匹配上Fw-A中的自定义网络ACL规则02，根据规则策略，允许该报文流入子网。该报文继续匹配安全组规则，可匹配上Sg-A的安全组规则A02，根据规则策略，拒绝该报文流入实例。
- **报文05：**报文05可匹配上Fw-A中的自定义网络ACL规则02，根据规则策略，允许该报文流入子网。该报文继续匹配安全组规则，可匹配上Sg-A的安全组规则A01，根据规则策略，允许该报文流入实例。

6.2 安全组

6.2.1 安全组和安全组规则概述

安全组

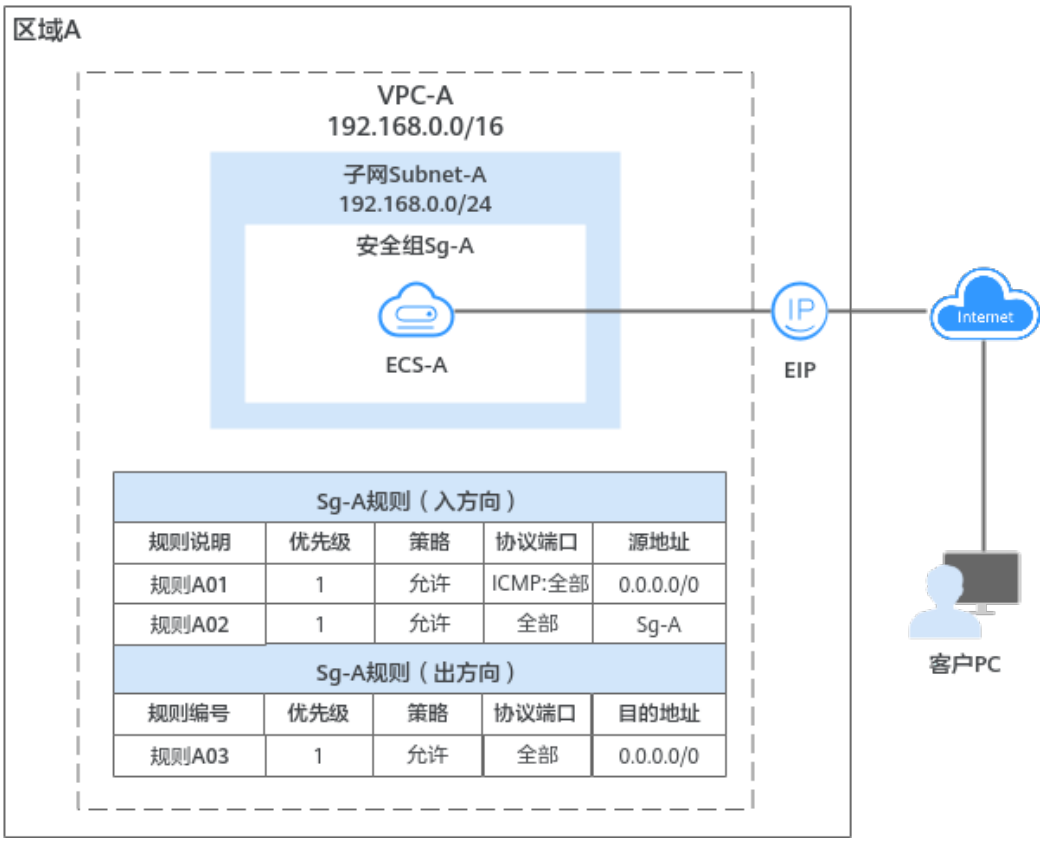
安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

您在创建实例时（比如云服务器），必须将实例加入一个安全组，如果此前您还未创建任何安全组，那么系统会自动为您创建**默认安全组**并关联至该实例。除了默认安全组，您还可以根据业务需求创建自定义安全组并关联至实例。一个实例可以关联多个安全组，多个安全组按照优先级顺序依次匹配流量。

安全组中包括入方向规则和出方向规则，您可以针对每条入方向规则指定来源、端口和协议，针对出方向规则指定目的地、端口和协议，用来控制安全组内实例入方向和出方向的网络流量。以**图6-4**为例，在区域A内，某客户有一个虚拟私有云VPC-A和子网Subnet-A，在子网Subnet-A中创建一个云服务器ECS-A，并为ECS-A关联一个安全组Sg-A来保护ECS-A的网络安全。

- 安全组Sg-A的入方向存在一条放通ICMP端口的自定义规则，因此可以通过个人PC(计算机)**ping**通ECS-A。但是安全组内未包含允许SSH流量进入实例的规则，因此您无法通过个人PC远程登录ECS-A。
- 当ECS-A需要通过EIP访问公网时，由于安全组Sg-A的出方向规则允许所有流量从实例流出，因此ECS-A可以访问公网。

图 6-4 安全组架构图



说明

您可以免费使用安全组资源，当前不收取任何费用。

安全组规则

- 安全组中包括入方向规则和出方向规则，用来控制安全组内实例的入方向和出方向的网络流量。
  - 入方向规则：控制外部请求访问安全组内的实例，即流量流入实例。
  - 出方向规则：控制安全组内实例访问外部的请求，即流量从实例流出。
- 安全组规则由协议端口、源地址/目的地址等组成，关键信息说明如下：
  - 策略：支持允许或拒绝。当流量的协议、端口、源地址/目的地址成功匹配某个安全组规则后，会对流量执行规则对应的策略，允许或拒绝流量。
  - 优先级：优先级可选范围为1-100，数字越小，规则优先级级别越高。安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。
  - 类型：支持设置IPv4和IPv6协议的规则。
  - 协议端口：包括网络协议类型和端口范围。
    - 网络协议：匹配流量的协议类型，支持TCP、UDP、ICMP和GRE协议。
    - 端口范围：匹配流量的目的端口，取值范围为：1～65535。
  - 源地址或目的地址：在入方向中，匹配流量的源地址。在出方向中，匹配流量的目的地址。

您可以使用IP地址、安全组、IP地址组作为源地址或者目的地址。

- IP地址：某个固定的IP地址或者网段，支持IPv4和IPv6地址。比如：192.168.10.10/32（IPv4地址）、192.168.1.0/24（IPv4网段）、2407:c080:802:469::/64（IPv6网段）
- 安全组：目标安全组和当前安全组位于同一区域，表示流量匹配目标安全组内所有实例的私有IP地址。比如：当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。
- IP地址组：**IP地址组**是一个或者多个IP地址的集合，对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。

安全组及规则的工作原理

- 安全组是有状态的。如果您从实例发送一个出站请求，且该安全组的出方向规则是放通的话，那么无论其入方向规则如何，都将允许该出站请求的响应流量流入。同理，如果该安全组的入方向规则是放通的，那无论出方向规则如何，都将允许入站请求的响应流量可以流出。
- 安全组使用连接跟踪来标识进出实例的流量信息，入方向安全组的规则变更，对原有流量立即生效。出方向安全组规则的变更，不影响已建立的长连接，只对新建立的连接生效。

  当您在安全组内增加、删除、更新规则，或者在安全组内添加、移出实例时，系统会自动清除该安全组内所有实例入方向的连接，详细说明如下：
  - 由入方向流量建立的连接，已建立的长连接将会断开。所有入方向流量立即重新建立连接，并匹配新的安全组入方向规则。
  - 由出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有安全组规则。出方向流量新建立的连接，将会匹配新的安全组出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

- 安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。
  - 在入方向中，当请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。因此，默认情况下您一般不用在入方向配置策略为“拒绝”的规则。

表6-4中的入方向规则，确保安全组内实例内网网络互通，不建议您删除或者修改该安全组规则。

- 在出方向中，表6-4中的出方向规则允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。如果您删除了该规则，则安全组内的实例无法访问外部，请您谨慎操作。

表 6-4 安全组规则说明

方向	策略	类型	协议端口	源地址/目的地址
入方向	允许	IPv4	全部	源地址：当前安全组
入方向	允许	IPv6	全部	源地址：当前安全组
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0
出方向	允许	IPv6	全部	目的地址：::/0

流量匹配安全组规则的顺序

一个实例可以关联多个安全组，并且一个安全组内可以包含多个安全组规则。安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略匹配，拒绝策略高于允许策略。如图6-5所示，以入方向的流量为例，实例的网络流量将按照以下原则匹配安全组规则，入方向和出方向的流量匹配顺序相同。

1. 首先，流量按照安全组的顺序进行匹配。您可以自行调整安全组顺序，安全组序号越小，表示优先级越高。

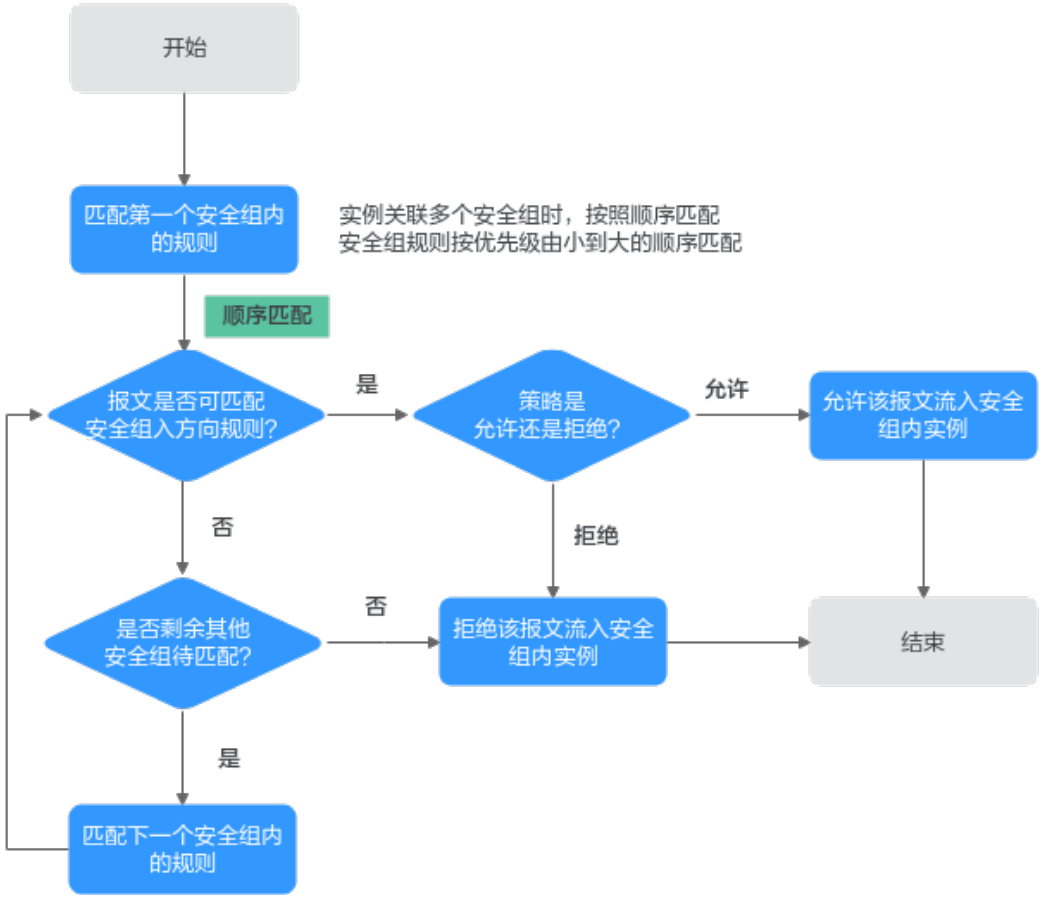
   比如，安全组A的序号为1，安全组B的序号为2，安全组A的优先级高于安全组B，流量优先匹配安全组A内的入方向规则。

2. 其次，流量按照安全组规则的优先级和策略进行匹配。
   a. 先按照安全组规则优先级匹配，优先级的数字越小，优先级越高。

      比如安全组规则A的优先级为1，安全组规则B的优先级为2，安全组规则A的优先级高于安全组规则B，流量优先匹配安全组规则A。

   b. 安全组规则优先级相同的情况下，再按照策略匹配，拒绝策略高于允许策略。
3. 流量按照协议端口和源地址，遍历了所有安全组内的入方向规则。
   - 如果成功匹配某个规则，则执行以下操作：
     - 如果规则的策略是允许，则允许该流量访问安全组内实例。
     - 如果规则的策略是拒绝，则拒绝该流量访问安全组内实例。
   - 如果未匹配上任何规则，则拒绝该流量访问安全组内的实例。

图 6-5 安全组匹配顺序



安全组配置示例

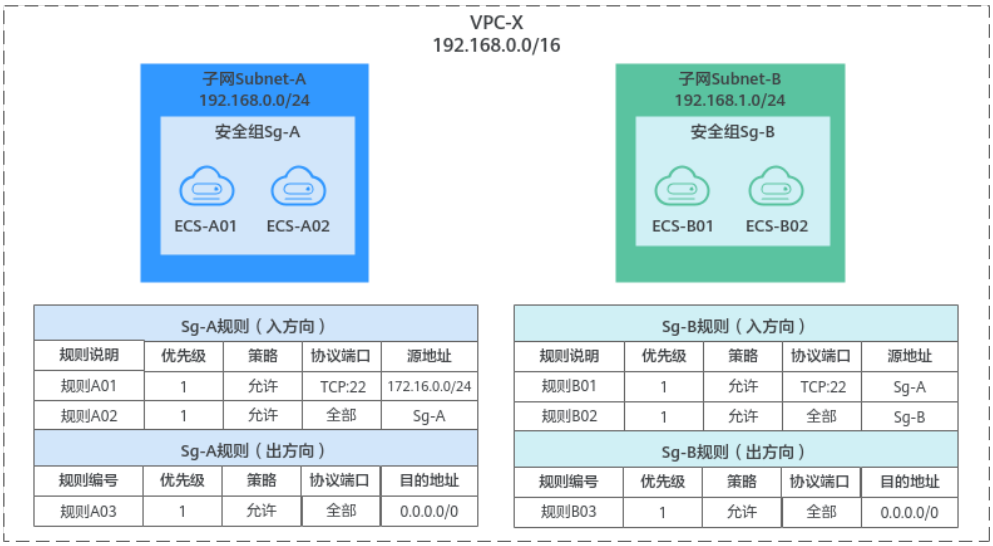
您可以在安全组内放通指定IP地址，允许指定IP地址访问安全组内实例，或者在某个安全组内放通另外一个安全组，实现不同安全组内的实例内网互通。通过安全组规则，您可以灵活控制组网内流量的走向，以确保您的网络安全，以下为您提供了典型的安全组应用示例。

控制外部指定 IP 地址或安全组对实例的访问

如图6-6所示，在VPC-X中有两个子网Subnet-A和Subnet-B，Subnet-A中的ECS承载同一类业务，需要相同的网络连接请求，因此均关联至安全组Sg-A。同理，Subnet-B中的ECS均关联至另外一个安全组Sg-B。

- 安全组Sg-A入方向规则A01允许从指定IP地址 (172.16.0.0/24)访问安全组内实例的SSH(22)端口，用于远程登录安全组内的Linux云服务器。
- 安全组Sg-A入方向规则A02允许安全组内的实例可使用任何协议和端口互相通信，即子网Subnet-A内的ECS网络互通。
- 安全组Sg-B入方向规则B01允许Sg-A内的实例访问Sg-B内实例的SSH(22)端口，即通过子网Subnet-A的ECS可远程登录Subnet-B内的ECS。
- 安全组Sg-B入方向规则B02允许安全组内的实例可使用任何协议和端口互相通信，即子网Subnet-B内的ECS网络互通。
- 两个安全组的出方向规则允许所有流量从安全组内实例流出。

图 6-6 控制外部指定 IP 地址或安全组对实例的访问



说明

更多安全组规则配置示例，请参见**安全组配置示例**。

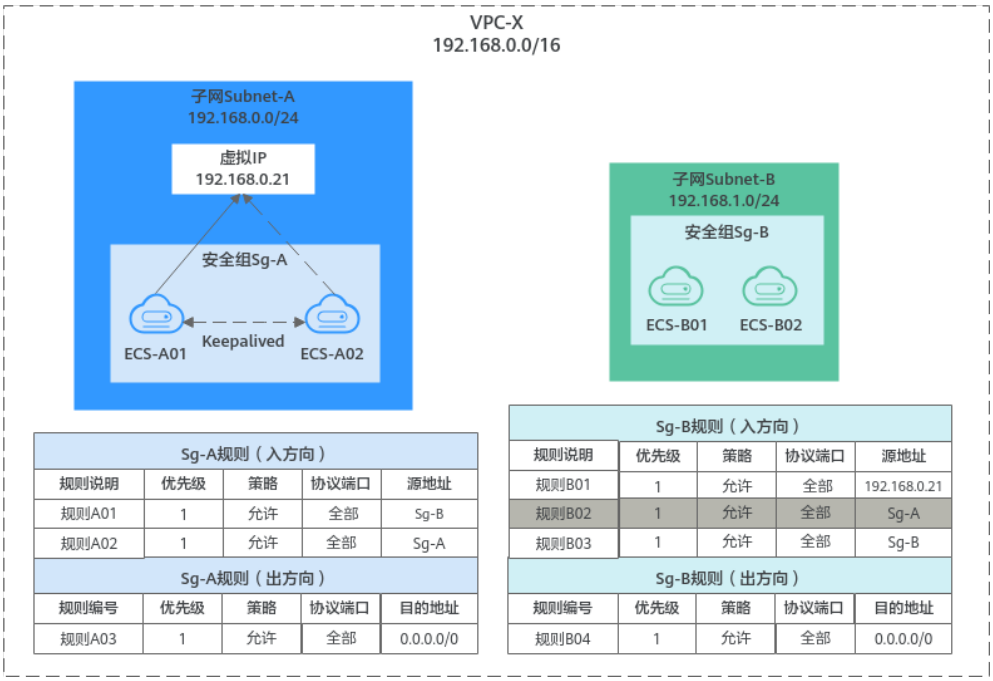
控制虚拟 IP 访问安全组内实例

如果您通过中间网络实例在不同子网的实例之间转发流量，比如图6-7中，子网Subnet-A的ECS通过虚拟IP和子网Subnet-B的ECS互相通信。由于存在中间网络实例，此时安全组规则的源地址选择实例所在的安全组时，无法放通中间网络实例转发的流量，源地址必须设置成中间网络实例的私有IP地址或者子网网段。

在VPC-X中有两个子网Subnet-A和Subnet-B，Subnet-A中的ECS关联至安全组Sg-A，Subnet-B中的ECS关联至安全组Sg-B。通过虚拟IP将Subnet-A中的ECS搭建成Keepalived高可用集群，后端服务器ECS-A01和ECS-A02形成主备模式，对外使用虚拟IP进行通信。

- 安全组Sg-A入方向规则A01允许Sg-B内的实例使用任何协议和端口访问Sg-A内的实例。
- 安全组Sg-B入方向规则说明如下：
  - 规则B02：允许Sg-A内的实例使用私有IP地址访问Sg-B内实例，但是当前组网下，Sg-A内的实例和Sg-B内的实例通信需要经过虚拟IP，此时虚拟IP的流量无法流入Sg-B内的实例，该规则不适用于当前组网。
  - 规则B01：允许虚拟IP(192.168.0.21)使用任何协议和端口访问Sg-B内的实例。当前组网中，您还可以将源地址设置成子网Subnet-A的网段192.168.0.0/24。

图 6-7 控制虚拟 IP 访问安全组内实例



Sg-A规则（入方向）

规则说明	优先级	策略	协议端口	源地址
规则A01	1	允许	全部	Sg-B
规则A02	1	允许	全部	Sg-A

Sg-A规则（出方向）

规则编号	优先级	策略	协议端口	目的地址
规则A03	1	允许	全部	0.0.0.0/0

Sg-B规则（入方向）

规则说明	优先级	策略	协议端口	源地址
规则B01	1	允许	全部	192.168.0.21
规则B02	1	允许	全部	Sg-A
规则B03	1	允许	全部	Sg-B

Sg-B规则（出方向）

规则编号	优先级	策略	协议端口	目的地址
规则B04	1	允许	全部	0.0.0.0/0

说明

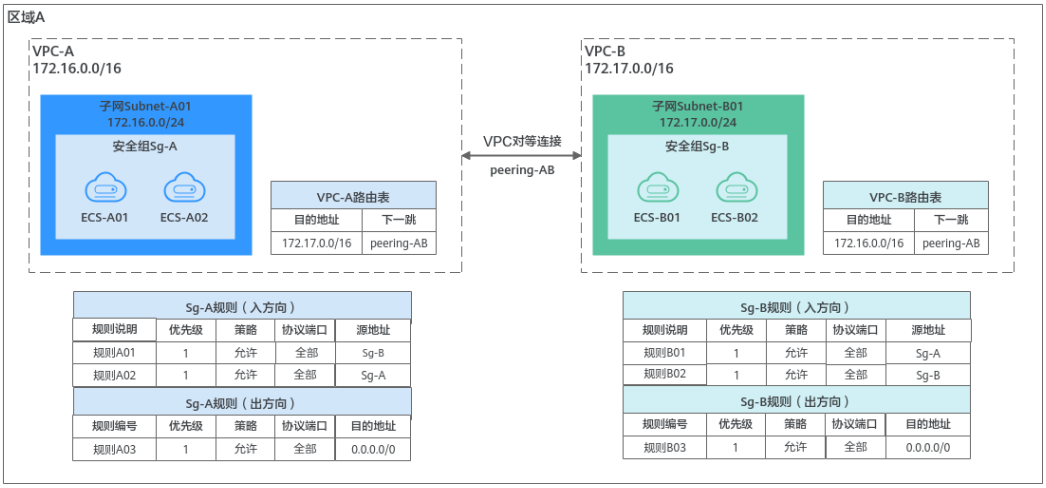
更多安全组规则配置示例，请参见**安全组配置示例**。

控制对等连接两端 VPC 内的实例互访

如图6-8所示，在区域A内，通过VPC对等连接连通VPC-A和VPC-B之间的网络。对等连接路由配置完成后，子网Subnet-A01和子网Subnet-B01之间网络已连通。但是由于两个子网内的ECS分别关联了不同的安全组，此时ECS之间仍然网络不通，您还需要放通安全组Sg-A和Sg-B的网络，才可以实现对等连接两端的ECS网络互通。

- 在安全组Sg-A中，规则A01允许来自Sg-B内实例的流量访问Sg-A内的实例，源地址为安全组Sg-B。
- 在安全组Sg-B中，规则B01允许来自Sg-A内实例的流量访问Sg-B内的实例，源地址为安全组Sg-A。

图 6-8 控制对等连接两端 VPC 内的实例互访



说明

更多安全组规则配置示例，请参见**安全组配置示例**。

安全组配置流程

图 6-9 安全组配置流程

表 6-5 安全组配置流程说明

序号	步骤	说明	操作指导
1	创建安全组	创建安全组时候，您可以使用系统提供的规则。预置的部分安全组规则，详细信息请参见**安全组模板说明**。	**创建安全组**
2	配置安全组规则	安全组创建完成后，如果模板里面的规则不能满足业务要求，您还可以在安全组中添加新的安全组规则，或者修改已有的安全组规则。	**添加安全组规则** **快速添加多条安全组规则**
3	在安全组中添加实例	创建实例的时候，会自动将实例加入一个安全组内，实例将会受到安全组的保护。 如果一个安全组无法满足您的要求，您可以将实例加入多个安全组。	**在安全组中添加或移出实例**

安全组的使用限制

- 为了确保良好的网络性能体验，建议一个实例最多关联5个安全组。

- 建议一个安全组关联的实例数量不应超过6000个，否则会引起安全组性能下降。
- 在一个安全组中，对于入方向规则来说，源地址是安全组的规则数量+源地址是IP地址组的规则数量+端口是不连续端口号的规则数量 ≤ 120条，否则超过数量的安全组规则将不生效。当同时存在IPv4和IPv6类型的安全组规则时，两种类型的安全组规则单独计算，即IPv4规则和IPv6规则可以各有120条。

  对于安全组出方向规则来说，目的地址和端口存在一样的限制。

  以安全组Sg-A的入方向IPv4规则为例，表6-6中提供了部分符合限制条件的规则供您参考。其中，当一条安全组规则同时符合多个限制时，比如规则A02即使用了不连续端口，又使用了安全组作为源地址，此时只占用一条配额。

  表 6-6 入方向安全组规则示例

规则编号	策略	类型	协议端口	源地址
规则A01	允许	IPv4	全部	**当前安全组：Sg-A**
规则A02	允许	IPv4	**TCP: 22,25,27**	**其他安全组：Sg-B**
规则A03	允许	IPv4	TCP: 80-82	**IP地址组：ipGroup-A**
规则A04	允许	IPv4	**TCP: 22-24,25**	IP地址: 192.168.0.0/16

- 如果您添加安全组规则时，使用IP地址组或者不连续端口，那么该安全组规则对不同规格云服务器的生效情况存在差异，为了避免您的安全组规则不生效，请您查看表6-7了解详情。

  表 6-7 安全组规则限制

安全组规则	云服务器类型
添加安全组规则时，“源地址”和“目的地址”可选择“IP地址组”	不支持的X86云服务器规格如下： • 通用计算型（S1型、C1型、C2型 ） • 内存优化型（M1型 ） • 高性能计算型（H1型 ） • 磁盘增强型（ D1型 ） • GPU加速型（G1型、G2型 ） • 超大内存型（E1型、E2型、ET2型 ）

安全组规则	云服务器类型
添加安全组规则时，“协议端口”可配置为不连续端口号	不支持的X86云服务器规格如下： • 通用计算型（S1型、C1型、C2型 ） • 内存优化型（M1型） • 高性能计算型（H1型） • 磁盘增强型（ D1型） • GPU加速型（G1型、G2型） • 超大内存型（E1型、E2型、ET2型）
	所有鲲鹏云服务器规格不支持配置不连续端口。 如果您在鲲鹏云服务器中添加安全组规则时，使用了不连续端口号，那么除了该条规则不会生效，该规则后的其他规则也不会生效。比如： 您先配置了安全组规则A（不连续端口号22,24），再配置了下一条安全组规则B（独立端口号9096），则安全组规则A和B均不会生效。

说明

- X86云服务器规格详情，请参见**规格清单（X86）**。
- 鲲鹏云服务器规格详情，请参见**规格清单（鲲鹏）**。

- 当您的组网中存在以下情况时，来自ELB和VPCEP的流量不受网络ACL和安全组规则的限制。
  - ELB实例的监听器开启“获取客户端IP”功能时，不受限制。
    比如规则已明确拒绝来自ELB实例的流量进入后端云服务器，此时该规则无法拦截来自ELB的流量，流量依然会抵达后端云服务器。
  - VPCEP实例类型为“专业型”时，不受限制。

实践建议

- 请您遵循白名单原则配置安全组规则，即安全组内实例默认拒绝所有外部的访问请求，通过添加允许规则放通指定的网络流量。
- 添加安全组规则时，请遵循最小授权原则。例如，放通22端口用于远程登录云服务器时，建议仅允许指定的IP地址登录，谨慎使用0.0.0.0/0（所有IP地址）。
- 请您尽量保持单个安全组内规则的简洁，通过不同的安全组来管理不同用途的实例。如果您使用一个安全组管理您的所有业务实例，可能会导致单个安全组内的规则过于冗余复杂，增加维护管理成本。
- 您可以将实例按照用途加入到不同的安全组内。例如，当您具有面向公网提供网站访问的业务时，建议您将运行公网业务的Web服务器加入到同一个安全组，此时仅需要放通对外部提供服务的特定端口，例如80、443等，默认拒绝外部其他的访问请求。同时，请避免在运行公网业务的Web服务器上运行内部业务，例如MySQL、Redis等，建议您将内部业务部署在不需要连通公网的服务器上，并将这些服务器关联至其他安全组内。
- 对于安全策略相同的多个IP地址，您可以将其添加到一个IP地址组内统一管理，并在安全组内添加针对该IP地址组的授权规则。当IP地址发生变化时，您只需要在IP

地址组内修改IP地址，那么IP地址组对应的安全组规则将会随之变更，无需逐次修改安全组内的规则，降低了安全组管理的难度，提升效率。具体方法，请参见**使用IP地址组提升安全组规则管理效率**。

- 请您尽量避免直接修改已运行业务的安全组规则。如果您需要修改使用中的安全组规则，建议您先克隆一个测试安全组，然后在测试安全组上进行调试，确保测试安全组内实例网络正常后，再修改使用中的安全组规则，减少对业务的影响。具体方法，请参见**克隆安全组**。
- 您在安全组内新添加实例，或者修改安全组的规则后，此时不需要重启实例，安全组规则会自动生效。

  如果您的安全组规则配置完未生效，请参考**为什么配置的安全组规则不生效?** 。

6.2.2 默认安全组概述

如果您未创建任何安全组，那么您在首次使用安全组时，系统会自动为您创建一个默认安全组。

- 默认安全组名称为default，为了区分默认安全组和您自己创建的安全组，不支持修改默认安全组名称。
- 您无法删除默认安全组，可以在默认安全组内修改已有规则或者添加新的规则。
- 默认安全组仅确保安全组内实例互通，默认拒绝所有外部请求进入实例，如果您需要登录默认安全组关联的实例，请参见**通过本地服务器远程登录云服务器**添加安全组规则放通指定端口。
- 如果实际业务对不同用途实例的安全要求存在差异，那么建议您创建自定义安全组，并将实例按照用途加入到不同的安全组内。

说明

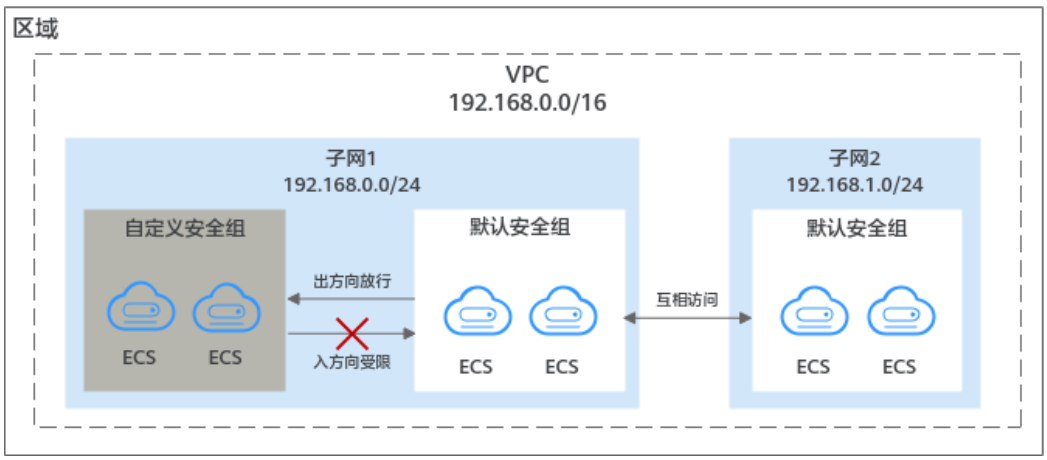
您可以免费使用安全组资源，当前不收取任何费用。

默认安全组规则说明

默认安全组规则说明如下：

- 入方向规则：入方向流量受限，只允许安全组内实例互通，拒绝来自安全组外部的所有请求进入实例。
- 出方向规则：出方向流量放行，允许所有请求从安全组内实例流出。

图 6-10 默认安全组



默认安全组规则的详细说明如表6-8所示。

表 6-8 默认安全组规则

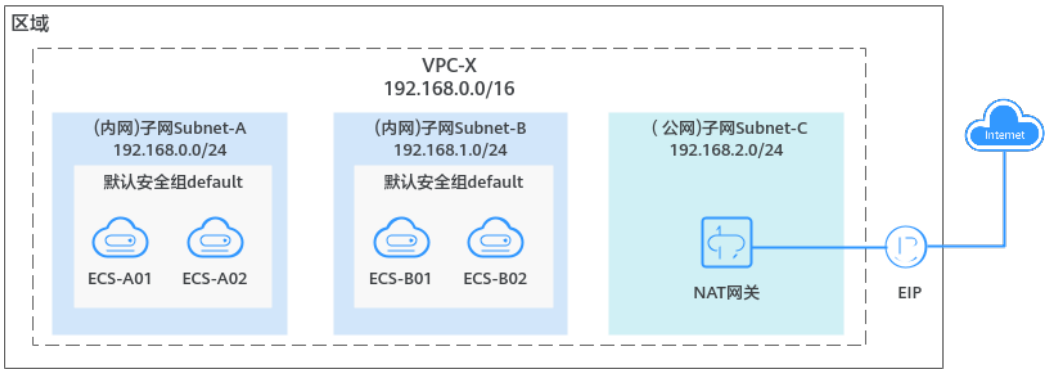
方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	全部	源地址：默认安全组（default）	针对全部IPv4协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。
入方向	允许	IPv6	全部	源地址：默认安全组（default）	针对全部IPv6协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对全部IPv4协议，允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。
出方向	允许	IPv6	全部	目的地址：::/0	针对全部IPv6协议，允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。

默认安全组应用示例

如图6-11所示，VPC-X内有三个子网，其中子网Subnet-A和Subnet-B中的ECS均关联默认安全组，默认安全组仅确保安全组内实例互通，默认拒绝所有外部请求进入实例。ECS-A01、ECS-A02、ECS-B01和ECS-B02之间内网网络互通，但是无法接受来自NAT网关的流量。

如果您需要放通NAT网关的流量，您可以在默认安全组中添加对应的规则，或者创建新的安全组，并关联给实例使用。

图 6-11 默认安全组应用示例



6.2.3 安全组配置示例

当您在VPC子网内创建实例（云服务器、云容器、云数据库等）时，您可以使用系统提供的默认安全组default，您也可以创建其他安全组。无论是默认安全组，还是您创建的安全组，您均可以在安全组内设置出方向和入方向规则，以此控制出入实例的流量。以下为您介绍一些常用的安全组的配置示例：

- 通过本地服务器远程登录云服务器
- 在本地服务器远程连接云服务器上传或者下载文件（FTP）
- 在云服务器上搭建网站对外提供Web服务
- 使用ping命令验证网络连通性
- 实现不同安全组的实例内网网络互通
- 云服务器提供数据库访问服务
- 限制云服务器访问外部网站

须知

如果您的安全组规则配置完成后不生效，请您提交工单联系客服处理。

使用须知

在配置安全组规则之前，您需要先了解以下信息：

- 不同安全组之间的实例默认网络隔离，无法互相访问。
- 安全组默认拒绝所有来自外部的请求，即本安全组内的实例网络互通，外部无法访问安全组内的实例。

  您需要遵循白名单原则添加安全组入方向规则，允许来自外部的特定请求访问安全组内的实例。
- 安全组入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例，如果将“22、3389、8848”等高危端口暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。
- 安全组的出方向规则一般默认全部放通，即允许安全组内的实例访问外部。

  如果出方向规则被删除，将会导致安全组内实例无法正常访问外部，您可以参考表6-9重新添加规则。

表 6-9 安全组默认出方向规则

方向	优先级	策略	类型	协议端口	目的地址	描述
出方向	1	允许	IPv4	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。
出方向	1	允许	IPv6	全部	::/0	针对全部IPv6协议，允许安全组内的实例可访问外部任意IP和端口。

通过本地服务器远程登录云服务器

安全组默认拒绝所有来自外部的请求，如果您需要通过本地服务器远程登录安全组内的云服务器，那么需要根据您的云服务器操作系统类型，在安全组入方向添加对应的规则。

- 通过SSH远程登录Linux云服务器，需要放通SSH(22)端口，请参见**表6-10**。
- 通过RDP远程登录Windows云服务器，需要放通RDP(3389)端口，请参见**表6-11**。

表 6-10 通过 SSH 远程登录 Linux 云服务器

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 22	IP地址：0.0.0.0/0

表 6-11 通过 RDP 远程登录 Windows 云服务器

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 3389	IP地址：0.0.0.0/0

须知

源地址设置为0.0.0.0/0表示允许所有外部IP地址远程登录云服务器，如果将当前端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，配置示例请参见**表6-12**。

表 6-12 通过已知 IP 地址远程登录云服务器

云服务器类型	方向	优先级	策略	类型	协议端口	源地址
Linux云服务器	入方向	1	允许	IPv4	自定义 TCP: 22	IP地址: 192.168.0.0/24
Windows云服务器	入方向	1	允许	IPv4	自定义 TCP: 3389	IP地址: 10.10.0.0/24

在本地服务器远程连接云服务器上传或者下载文件（FTP）

安全组默认拒绝所有来自外部的请求，如果您需要在本地服务器远程连接云服务器上传或者下载文件，那么您需要开通FTP(20、21)端口。

表 6-13 通过任意服务器远程连接云服务器上传或者下载文件

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 20-21	IP地址：0.0.0.0/0

须知

- 源地址设置为0.0.0.0/0表示允许所有外部IP地址远程连接云服务器上传或者下载文件，如果将当前端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，配置示例请参见**表6-14**。
- 您需要在弹性云服务器上先安装FTP服务器程序，再查看20、21端口是否正常工作。安装FTP服务器的操作请参见**搭建FTP站点（Windows）**、**搭建FTP站点（Linux）**。

表 6-14 通过已知的服务器远程连接云服务器上传或者下载文件

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 20-21	IP地址：192.168.0.0/24

在云服务器上搭建网站对外提供 Web 服务

安全组默认拒绝所有来自外部的请求，如果您在云服务器上搭建了可供外部访问的网站，则您需要在安全组入方向添加对应的规则，放通对应的端口，例如HTTP(80)、HTTPS(443)。

表 6-15 在云服务器上搭建网站对外提供 Web 服务

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 80	IP地址：0.0.0.0/0
入方向	1	允许	IPv4	自定义TCP: 443	IP地址：0.0.0.0/0

使用 ping 命令验证网络连通性

ICMP协议用于网络消息的控制和传递，因此在进行一些基本测试操作之前，需要开通ICMP协议访问端口。比如，您需要在某个个人PC上使用**ping**命令来验证云服务器的网络连通性，则您需要在云服务器所在安全组的入方向添加以下规则，放通ICMP端口。

表 6-16 使用 ping 命令验证网络连通性

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	ICMP: 全部	IP地址：0.0.0.0/0
入方向	1	允许	IPv6	ICMP: 全部	IP地址：::/0

实现不同安全组的实例内网网络互通

同一个VPC内，位于不同安全组内的实例网络不通。如果您需要在同一个VPC内的实例之间共享数据，比如安全组sg-A内的云服务器访问安全组sg-B内的MySQL数据库，您需要通过在安全组sg-B中添加一条入方向规则，允许来自安全组sg-A内云服务器的内网请求进入。

表 6-17 实现不同安全组的实例网络互通

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 3306	安全组：sg-A

须知

如果您通过中间网络实例在不同子网的实例之间转发流量，如**安全组配置示例**中的示例二，子网Subnet-A的ECS通过虚拟IP和子网Subnet-B的ECS互相通信。由于存在中间网络实例，此时安全组规则的源地址选择实例所在的安全组时，无法放通中间网络实例转发的流量，源地址必须设置成中间网络实例的私有IP地址或者子网网段。

云服务器提供数据库访问服务

安全组默认拒绝所有来自外部的请求，如果您在云服器上部署了数据库服务，允许其他实例通过内网访问数据库服务，则您需要在部署数据库服务器所在的安全组内，添加入方向规则，放通对应的端口，实现其他实例通过内网获取数据库数据的请求。常见的数据库类型及其对应的端口如下：

- MySQL(3306)
- Oracle(1521)
- MS SQL(1433)
- PostgreSQL(5432)

- Redis(6379)

表 6-18 云服务器提供数据库访问服务

方向	优先级	策略	类型	协议端口	源地址	描述
入方向	1	允许	IPv4	自定义 TCP: 3306	安全组: sg-A	允许安全组sg-A内云服务器访问MySQL数据库服务。
入方向	1	允许	IPv4	自定义 TCP: 1521	安全组: sg-B	允许安全组sg-B内云服务器访问Oracle数据库服务。
入方向	1	允许	IPv4	自定义 TCP: 1433	IP地址: 172.16.3.21/32	允许私网IP地址为172.16.3.21的云服务器访问MS SQL数据库服务。
入方向	1	允许	IPv4	自定义 TCP: 5432	IP地址: 192.168.0.0/24	允许私网IP地址属于192.168.0.0/24网段的云服务器访问PostgreSQL数据库服务。
入方向	1	允许	IPv4	自定义 TCP: 6379	IP地址组: ipGroup-A	允许私网IP地址属于IP地址组ipGroup-A范围内的云服务器访问Redis数据库服务。

须知

本示例中源地址提供的配置仅供参考，请您根据实际需求设置源地址。

限制云服务器访问外部网站

安全组的出方向规则一般默认全部放通，默认规则如表6-20所示。如果您需要限制服务器只能访问特定网站，则按照如下要求配置：

1. 首先，您需要遵循白名单规则，在安全组出方向规则中添加指定的端口和IP地址。

表 6-19 限制云服务器访问外部网站

方向	优先级	策略	类型	协议端口	目的地址	描述
出方向	1	允许	IPv4	自定义 TCP: 80	IP地址: 132.15.XX.XX	允许安全组内云服务器访问指定的外部网站，网站地址为http://132.15.XX.XX:80。

方向	优先级	策略	类型	协议端口	目的地址	描述
出方向	1	允许	IPv4	自定义TCP:443	IP地址：145.117.XX.XX	允许安全组内云服务器访问指定的外部网站，网站地址为https://145.117.XX.XX:443。

2. 其次，删除安全组出方向中原有放通全部流量的规则，如表6-20所示。

表 6-20 安全组默认出方向规则

方向	优先级	策略	类型	协议端口	目的地址	描述
出方向	1	允许	IPv4	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。
出方向	1	允许	IPv6	全部	::/0	针对全部IPv6协议，允许安全组内的实例可访问外部任意IP和端口。

6.2.4 ECS 常用端口

添加安全组规则时，需要您指定通信所需的端口或者端口范围，然后安全组根据策略，决定允许或是拒绝相关流量转发至ECS实例。以通过SSH方式远程登录ECS为例，当安全组检测到SSH请求后，会检查发送请求的设备IP地址、登录所需的22端口是否已在安全组入方向中被放行，只有和安全组入方向规则匹配成功，该请求才会被放行，否则无法建立数据通信。

表6-21中提供了部分运营商判断的高危端口，这些端口默认被屏蔽。即使您已经添加安全组规则放通了这些端口，在受限区域仍然无法访问，此时建议您将端口修改为其他非高危端口。

表 6-21 高危端口

协议	端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1433 1434 3127 3128 3129 3130 4444 4789 5554 5800 5900 8998 9995 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9995 9996

常用端口

弹性云服务器常用端口如表6-22所示。您可以通过配置安全组规则放通弹性云服务器对应的端口，详情请参见添加安全组规则。关于Windows下更多的服务应用端口说明，请参考微软官方文档：Windows的服务概述和网络端口要求。

表 6-22 弹性云服务器常用端口

端口	协议	说明
21	FTP	FTP服务开放的端口，用于上传和下载文件。配置示例请参见**在本地服务器远程连接云服务器上传或者下载文件（FTP）**。
22	SSH	SSH端口，用于远程连接Linux弹性云服务器。配置示例请参见**通过本地服务器远程登录云服务器**。 登录方法请参见**Linux弹性云服务器登录方式概述**。
23	Telnet	Telnet端口，用于通过Telnet协议远程登录弹性云服务器。
25	SMTP	SMTP服务器开放的端口，用于发送邮件。 基于安全考虑，TCP 25端口出方向默认被封禁，申请解封请参考**TCP 25端口出方向无法访问时怎么办？** 。
80	HTTP	使用HTTP协议访问网站。配置示例请参见**在云服务器上搭建网站对外提供Web服务**。
110	POP3	使用POP3协议接收邮件。
143	IMAP	使用IMAP协议接收邮件。
443	HTTPS	使用HTTPS服务访问网站。配置示例请参见**在云服务器上搭建网站对外提供Web服务**。
1433	SQL Server	SQL Server的TCP端口，用于供SQL Server对外提供服务。配置示例请参见**云服务器提供数据库访问服务**。
1434	SQL Server	SQL Server的UDP端口，用于返回SQL Server使用了哪个TCP/IP端口。配置示例请参见**云服务器提供数据库访问服务**。
1521	Oracle	Oracle通信端口，弹性云服务器上部署了Oracle SQL需要放行的端口。配置示例请参见**云服务器提供数据库访问服务**。
3306	MySQL	MySQL数据库对外提供服务的端口。配置示例请参见**云服务器提供数据库访问服务**。
3389	Windows Server Remote Desktop Services	Windows远程桌面服务端口，通过这个端口可以连接Windows弹性云服务器。配置示例请参见**通过本地服务器远程登录云服务器**。 登录方法请参见**Windows弹性云服务器登录方式概述**。
8080	代理	同80端口一样，8080 端口常用于WWW代理服务，实现网页浏览。如果您使用了8080端口，访问网站或使用代理服务器时，需要在IP地址后面加上**:8080**。安装Apache Tomcat服务后，默认服务端口为8080。

端口	协议	说明
137、138、139	NetBIOS	NetBIOS协议常被用于Windows文件、打印机共享和Samba。 • 137、138：UDP端口，通过网上邻居传输文件时使用的端口。 • 139：通过这个端口进入的连接试图获得NetBIOS/SMB服务。

6.2.5 管理安全组

6.2.5.1 创建安全组

操作场景

安全组实际是网络流量访问策略，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

您在创建实例时（如ECS），必须将实例加入一个安全组，如果此前您还未创建任何安全组，那么系统会自动为您创建**默认安全组**并关联至该实例。除了默认安全组，您还可以参考以下操作创建自定义安全组，并配置安全组规则控制特定流量的访问请求。了解安全组的更多信息，请参见**安全组和安全组规则概述**。

预设安全组规则说明

创建安全组的时候，您可以选择系统预设规则。安全组预设规则中预先配置了入方向规则和出方向规则，您可以根据业务选择所需的预设规则，快速完成安全组的创建。安全组预设规则的详细说明如**表6-23**所示。

表 6-23 安全组规则说明

预设规则	方向	类型和协议端口	源地址/目的地址	规则说明	适用场景
通用Web服务器	入方向规则	TCP: 22 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的SSH(22)端口，用于远程登录Linux实例。	• 外部远程登录安全组内实例（如ECS） • 外部使用**ping**命令验证安全组内实例的网络连通性 • 安全组内实例用作Web服务器对外提供网站访问服务
		TCP: 3389 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的RDP(3389)端口，用于远程登录Windows实例。	

预设规则	方向	类型和协议端口	源地址/目的地址	规则说明	适用场景
		TCP: 80 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的HTTP(80)端口，用于通过HTTP协议访问网站。	
		TCP: 443 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内实例的HTTPS(443)端口，用于通过HTTPS协议访问网站。	
		ICMP: 全部 (IPv4)	0.0.0.0/0	针对ICMP(IPv4)协议，允许外部所有IP访问安全组内实例的所有端口，用于外部使用**ping**命令验证安全组内实例的网络连通性。	
		全部 (IPv4) 全部 (IPv6)	当前安全组	针对全部协议，允许安全组内实例通过内网网络相互通信。	
	出方向规则	全部 (IPv4) 全部 (IPv6)	0.0.0.0/0 ::/0	针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。	
开放全部端口	入方向规则	全部 (IPv4) 全部 (IPv6)	当前安全组	针对全部协议，允许安全组内实例通过内网网络相互通信。	开放全部端口即允许任意流量出入安全组内的实例，此操作存在一定安全风险，请您谨慎选择。
		全部 (IPv4) 全部 (IPv6)	0.0.0.0/0 ::/0	针对全部协议，允许外部所有IP访问安全组内实例的所有端口，即任意流量可流入安全组内实例。	
	出方向规则	全部 (IPv4) 全部 (IPv6)	0.0.0.0/0 ::/0	针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。	

预设规则	方向	类型和协议端口	源地址/目的地址	规则说明	适用场景
自定义	入方向规则	全部(IPv4) 全部(IPv6)	当前安全组	针对全部协议，允许安全组内实例通过内网网络相互通信。	该预设规则的入方向未放通任何端口，即外部任意流量均无法流入安全组内实例。请您根据业务需求自行添加安全组规则。
	出方向规则	全部(IPv4) 全部(IPv6)	0.0.0.0/0 ::/0	针对全部协议，允许所有流量从安全组内实例流出，用于访问外部。	

操作步骤

1. 进入**安全组列表页面**。
2. 在安全组列表右上方，单击“创建安全组”。
   进入“创建安全组”页面。
3. 根据界面提示，设置安全组参数。

图 6-12 创建安全组

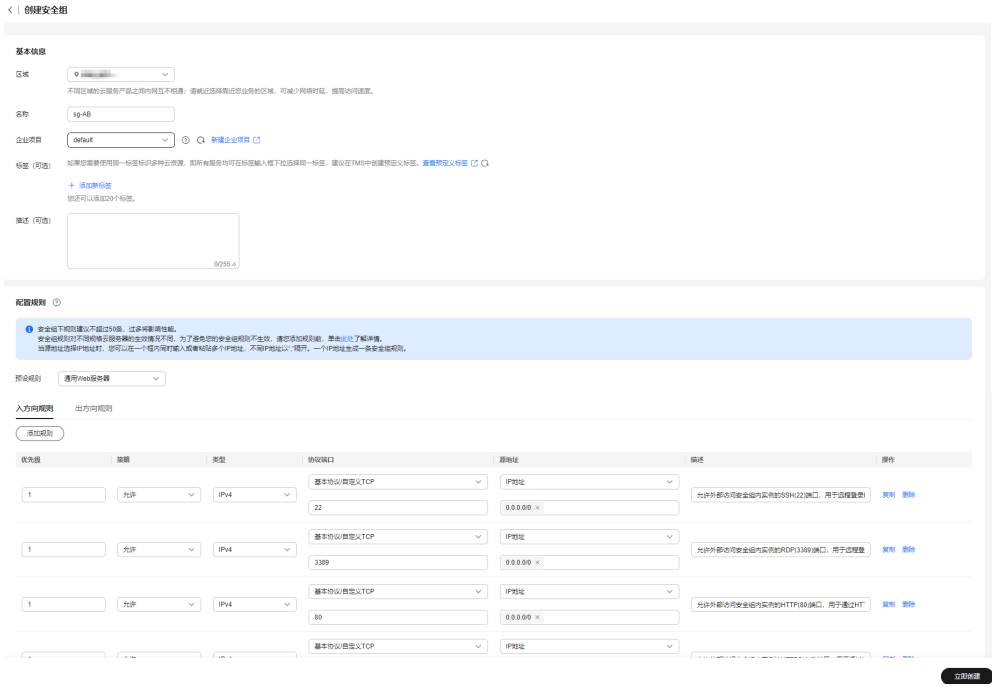


表 6-24 参数说明

参数	参数说明	取值样例
区域	必选参数。 不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。 安全组和实例必须位于同一个区域内，才可以将实例添加到安全组内。	华东-上海一
名称	必选参数。 输入安全组的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 **说明** 安全组名称创建后可以修改，建议不要重名。	sg-AB
企业项目	必选参数。 创建安全组时，可以将安全组加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**。	default
标签	可选参数。 您可以在创建安全组的时候为安全组绑定标签，标签用于标识安全组资源，可通过标签实现对安全组资源的分类和搜索。 关于标签更详细的说明，请参见**管理安全组标签**。	“标签键”：test “标签值”：01
描述	可选参数。 安全组的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
预设规则	必选参数 安全组预设规则中预先配置了入方向规则和出方向规则，您可以根据业务选择所需的预设规则，快速完成安全组的创建。 安全组预设规则的详细说明和适用场景，具体请参见**表6-23**。	通用Web服务器

4. 安全组参数设置完成后，可以在创建页面下方查看预设规则，并可以执行以下操作。
   - 添加规则

- 复制规则
- 修改规则
- 删除规则

须知

- 入方向规则的参数说明请参见**表6-27**，出方向规则的参数说明请参见**表6-28**。
- 入方向规则中，源地址为当前安全组的规则不支持修改，如果您删除该规则，将会导致安全组内实例的内网网络无法互通，请谨慎操作。
- 出方向规则中，目的地址为0.0.0.0/0和::/0的规则不支持修改，如果您删除该规则，将会导致安全组内实例无法访问外部网络，请谨慎操作。

5. 规则设置完成后，单击“立即创建”，完成创建。

相关操作

为了保护云服务器的网络安全，每台云服务器至少加入一个安全组，您可以根据业务需要，将云服务器加入一个或多个安全组，体操作请参见**在安全组中添加或移出实例**。

6.2.5.2 克隆安全组

操作场景

VPC支持同区域或者跨区域克隆安全组，方便您将相同的安全组规则快速应用到不同区域的弹性云服务器上。

当您遇到如下场景时，推荐您使用克隆安全组功能。

- 假设您已经在区域A创建了一个安全组sg-A，此时您需要为区域B内的弹性云服务器使用与sg-A完全相同的规则，您可以直接将sg-A克隆到区域B，而不需要在区域B重新创建安全组。
- 如果您的业务需要执行新的安全组规则，您可以克隆原有的安全组作为备份。
- 如果您需要修改当前业务使用的安全组规则，建议您可以克隆一个测试安全组，在测试环境调测成功后，再修改运行的业务安全组。

约束与限制

- 您可以在同一个区域内，或者跨区域克隆安全组。
  - 同一个区域内克隆安全组时，可以克隆安全组内的全部规则。
  - 跨区域克隆安全组时，仅支持克隆源/目的地址是IP地址或者本安全组的规则，不支持克隆源/目的地址是其他安全组和IP地址组的规则。
- 克隆安全组功能是克隆安全组及安全组规则，不支持克隆此安全组关联的实例。
- 克隆安全组支持在同一个账号内使用，如果您需要跨账号快速创建安全组，则推荐您使用导入/导出安全组规则功能，具体请参见**导入/导出安全组规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表页面 ，单击目标安全组所在行的操作列下的“更多 > 克隆”。
6. 根据界面提示，选择新克隆安全组所在的区域，名称等参数 。
7. 参数设置完成后，单击“确定”，完成安全组克隆。
   您可以在对应区域的安全组列表中，查看克隆成功的安全组。

6.2.5.3 修改安全组基本信息

操作场景

安全组创建完成后，您可以参考以下操作修改安全组的名称和描述。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表页面 ，单击目标安全组所在行的操作列下的“更多 > 修改”。
   弹出“修改安全组”对话框。
6. 根据界面提示，修改安全组的名称和描述信息。
7. 参数修改完成后，单击“确定”，保存修改。

6.2.5.4 查看安全组

操作场景

您可以参考以下操作查看您的安全组，包括安全组名称、安全组规则以及安全组关联的实例等信息。

同时，您可以通过搜索功能，使用安全组名称、ID以及描述等关键信息快速搜索目标安全组。

操作步骤

1. 登录管理控制台。

2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表上方的搜索框中，选择支持的筛选条件，快速搜索目标安全组。
6. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面
7. 在安全组详情页面，选择不同的页签，查看安全组信息。
   - 基本信息：安全组名称、ID以及描述等信息。
   - 入方向规则：安全组入方向规则的优先级、策略、源地址以及修改时间等信息。
   - 出方向规则：安全组出方向规则的优先级、策略、目的地址以及修改时间等信息。
   - 关联实例：安全组关联的实例信息，实例类型包括服务器、扩展网卡、辅助弹性网卡等。
   - 标签：安全组的标签，包括标签的键和值。

6.2.5.5 管理安全组标签

操作场景

标签用于标识云资源，您可以通过标签实现对安全组资源的分类和搜索。您可以参考以下操作管理安全组标签：

- 添加安全组标签
- 修改安全组标签
- 删除安全组标签

安全组标签规则的详细说明，请参见表6-25。

表 6-25 安全组标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	test

参数	规则	样例
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 进入**安全组列表页面**。
5. 在安全组列表中，单击目标安全组名称超链接。
   进入安全组详情页面。
6. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
7. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击+，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的×，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

6.2.5.6 删除安全组

操作场景

当您的安全组不需要使用时，您可以参考以下操作删除不需要的安全组。

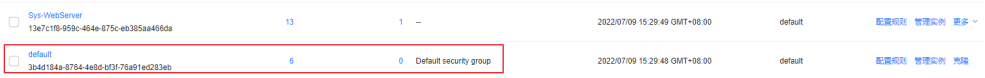
说明

系统创建的默认安全组和您创建的自定义安全组均不收取费用。

约束与限制

- 系统创建的默认安全组不支持删除，默认安全组名称为default。

图 6-13 默认安全组



- 当安全组已关联至其他服务实例时，比如云服务器、云容器、云数据库等，此安全组无法删除。请您将实例从安全组中移出后，重新尝试删除安全组，具体操作请参见**在安全组中添加或移出实例**。

  查看安全组关联的实例，具体操作请参见**如何查看安全组关联了哪些实例？** 。
- 当安全组作为“源地址”或者“目的地址”，被添加在其他安全组的规则中时，此安全组无法删除。

  需要**删除该条规则**或者**修改规则**，然后重新尝试删除安全组。

  比如，安全组sg-B中有一条安全组规则的“源地址”设置为安全组sg-A，则需要删除或者更改sg-B中的该条规则，才可以删除sg-A。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。

   进入安全组列表页面。
5. 在安全组列表中，选择目标安全组所在行的操作列下的“更多 > 删除”。

   弹出删除确认对话框。
6. 根据界面提示完成确认，确认无误后单击“确定”，删除安全组。

6.2.6 管理安全组规则

6.2.6.1 添加安全组规则

操作场景

安全组实际是网络流量访问策略，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

常见的安全组规则应用场景包括：允许或者拒绝特定来源的网络流量、允许或拒绝特定协议的网络流量、屏蔽不需要开放的端口、以及配置服务器的特定访问权限等。

使用须知

- 配置安全组规则前，您需要规划好安全组内实例的访问策略，常见安全组规则配置案例请参见**安全组配置示例**。
- 安全组的规则数量有限制，请您尽量保持安全组内规则的简洁，详细约束请参见**安全组的使用限制**。
- 在安全组规则中放开某个端口后，您还需要确保实例内对应的端口也已经放通，安全组规则才会对实例生效，具体请参见**检查安全组规则是否生效**。

- 安全组入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例，如果将“22、3389、8848”等**高危端口**暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。
- 通常情况下，同一个安全组内的实例默认网络互通。当同一个安全组内实例网络不通时，可能情况如下：
  - 当实例属于同一个VPC时，请您检查入方向规则中，是否删除了同一个安全组内实例互通对应的规则，规则详情如**表6-26**所示。

    表 6-26 安全组内实例互通规则

方向	优先级	策略	类型	协议端口	源地址/目的地址
入方向	1	允许	IPv4	全部	源地址：当前安全组（Sg-A）
入方向	1	允许	IPv6	全部	源地址：当前安全组（Sg-A）

  - 不同VPC的网络不通，所以当实例属于同一个安全组，但属于不同VPC时，网络不通。

    您可以通过**VPC对等连接**连通不同区域的VPC。

在安全组内添加安全组规则

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。

   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。

   进入安全组规则配置页面。
6. 在“入方向规则”页签，单击“添加规则”。

   弹出“添加入方向规则”对话框。
7. 根据界面提示，设置入方向规则参数。

   单击，可以依次增加多条入方向规则。

图 6-14 添加安全组入方向规则

表 6-27 入方向规则参数说明

参数	说明	取值样例
优先级	安全组规则优先级。 优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。	1
策略	安全组规则策略，支持的策略如下： • 如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。 • 如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。	允许
类型	源地址支持的IP地址类型，如下： • IPv4 • IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。 端口填写支持下格式： • 单个端口：例如22 • 连续端口：例如22-30 • 多个端口：例如22,23-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 • 全部端口：为空或1-65535	22或22-30 或20,22-30

参数	说明	取值样例
源地址	在入方向规则中，用来匹配外部请求的源地址，支持以下格式： ● IP地址：表示源地址为某个固定的IP地址。当源地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示源地址为另外一个安全组，您可以在下拉列表中，选择同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。 ● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	IP地址： 192.168.52.0/24,10.0.0.0/24
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

8. 入方向规则设置完成后，单击“确定”。
   返回入方向规则列表，可以查看添加的入方向规则。
9. 在“出方向规则”页签，单击“添加规则”。
   弹出“添加出方向规则”页签。
10. 根据界面提示，设置出方向规则参数。
    单击⊕，可以依次增加多条出方向规则。

图 6-15 添加安全组出方向规则

表 6-28 出方向规则参数说明

参数	说明	取值样例
优先级	安全组规则优先级。 优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。	1
策略	安全组规则策略，支持的策略如下： • 如果“策略”设置为允许，表示允许安全组内的云服务器访问目的地址的指定端口。 • 如果“策略”设置为拒绝，表示拒绝安全组内的云服务器访问目的地址的指定端口。 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。	允许
类型	目的地址支持的IP地址类型，如下： • IPv4 • IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在出方向规则中，表示安全组内实例访问外部地址的指定端口。 端口填写支持下格式： • 单个端口：例如22 • 连续端口：例如22-30 • 多个端口：例如22,23-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 • 全部端口：为空或1-65535	22或22-30 或20,22-30

参数	说明	取值样例
目的地址	在出方向规则中，用来匹配内部请求的目的地址。支持以下格式： ● IP地址：表示目的地址为某个固定的IP地址。当目的地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示目的地址为另外一个安全组，您可以在下拉列表中，选择当前账号下，同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的出方向规则放通目的地址为安全组B的流量，则实例a访问实例b的内网请求被允许流出。 ● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	IP地址： 192.168.52.0/24,10.0.0.0/24
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

11. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

检查安全组规则是否生效

在安全组规则中放开某个端口后，您还需要确保实例内对应的端口也已经放通，安全组规则才会对实例生效。

假设您在某台ECS上部署了网站，希望用户能通过HTTP(80)端口访问到您的网站，则您需要先在ECS所在安全组的入方向中，添加**表6-29**中的规则，放通HTTP(80)端口。

表 6-29 安全组规则示例

方向	优先级	策略	类型	协议端口	源地址
入方向	1	允许	IPv4	自定义TCP: 80	IP地址：0.0.0.0/0

安全组规则添加完成后，您需要执行以下操作，检查云服务器内端口开放情况，并验证配置是否生效。

1. 登录云服务器，检查云服务器端口开放情况。
   - **检查Linux云服务器端口**

     执行以下命令，查看TCP 80端口是否被监听。

     netstat -an | grep 80

     若回显类似图6-16，说明80端口已开通。

     图 6-16 Linux TCP 80 端口验证结果

     ```
     tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
     ```

   - **检查Windows云服务器端口**

     i. 通过“开始菜单 > 运行 > cmd”，打开命令执行窗口。

     ii. 执行以下命令，查看TCP 80端口是否被监听。

     netstat -an | findstr 80

     若回显类似图6-17，说明TCP 80端口已开通。

     图 6-17 Windows TCP 80 端口验证结果

     ```
     TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
     ```

2. 打开浏览器，在地址栏里输入“http://云服务器的弹性公网IP地址”。

   如果访问成功，说明安全组规则已经生效。

6.2.6.2 快速添加多条安全组规则

操作场景

通过安全组快速添加功能，您可以快速添加部分常用端口协议对应的规则，包括远程登录和ping测试、常用Web服务和数据库服务所需的端口协议。

云服务器的常用端口介绍，请参见**ECS常用端口**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。

   进入安全组列表页面。

5. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。
   进入安全组规则配置页面。
6. 在“入方向规则”页签，单击“快速添加规则”。
   弹出“快速添加入方向规则”对话框。
7. 根据界面提示，设置入方向规则参数。

图 6-18 快速添加安全组入方向规则

表 6-30 入方向规则参数说明

参数	说明	取值样例
常见协议端口	提供常用的协议端口供您快速设置，选择类型如下： • 远程登录和ping • Web服务 • 数据库	SSH (22)
类型	源地址支持的IP地址类型，如下： • IPv4 • IPv6	IPv4

参数	说明	取值样例
源地址	在入方向规则中，用来匹配外部请求的源地址，支持以下格式： ● IP地址：表示源地址为某个固定的IP地址。当源地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示源地址为另外一个安全组，您可以在下拉列表中，选择同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的入方向规则中，放通源地址为安全组B的流量，则来自实例b的内网访问请求被允许进入实例a。 ● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	IP地址： 192.168.52.0/24,10.0.0.0/24
策略	安全组规则策略，支持的策略如下： ● 如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。 ● 如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。	允许
优先级	安全组规则优先级。 优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。	1
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

8. 入方向规则设置完成后，单击“确定”。

返回入方向规则列表，可以查看添加的入方向规则。

9. 在“出方向规则”页签，单击“快速添加规则”。
   弹出“快速添加出方向规则”页签。
10. 根据界面提示，设置出方向规则参数。

图 6-19 快速添加安全组出方向规则

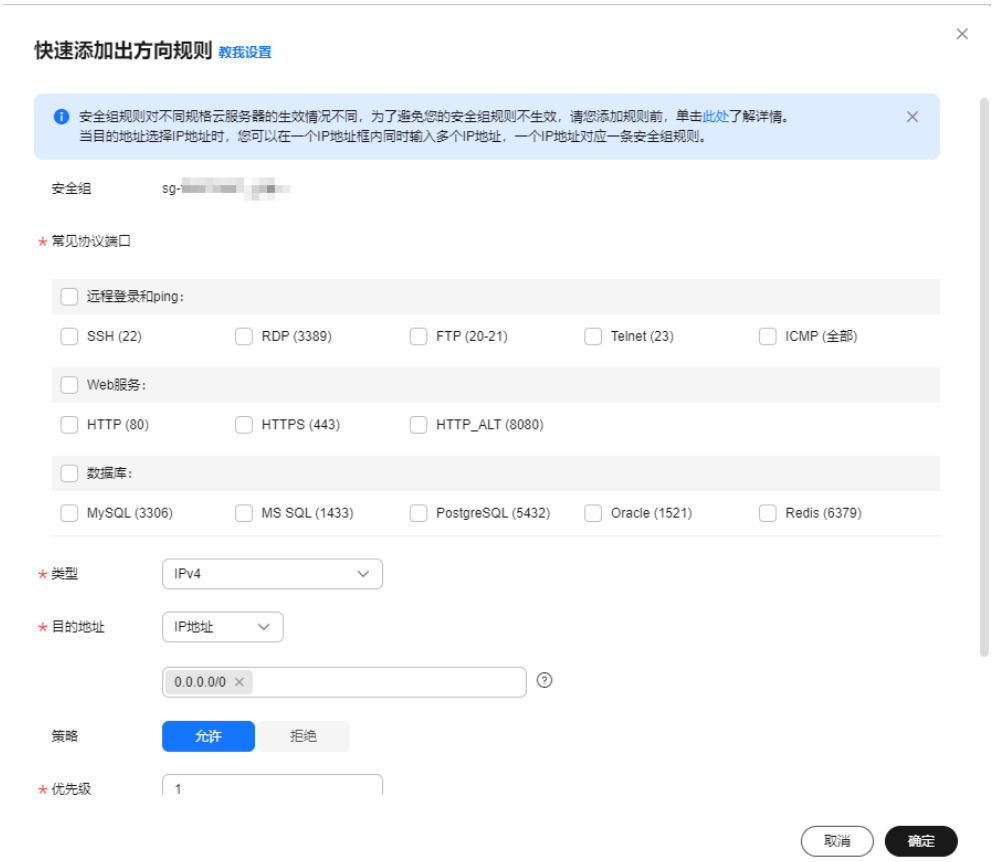


表 6-31 出方向规则参数说明

参数	说明	取值样例
常见协议端口	提供常用的协议端口供您快速设置，选择类型如下： • 远程登录和ping • Web服务 • 数据库	SSH（22）
类型	源地址支持的IP地址类型，如下： • IPv4 • IPv6	IPv4

参数	说明	取值样例
目的地址	在出方向规则中，用来匹配内部请求的目的地址。支持以下格式： ● IP地址：表示目的地址为某个固定的IP地址。当目的地址选择IP地址时，您可以在一个框内同时输入或者粘贴多个IP地址，不同IP地址以“,”隔开。一个IP地址生成一条安全组规则。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示目的地址为另外一个安全组，您可以在下拉列表中，选择当前账号下，同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A的出方向规则放通目的地址为安全组B的流量，则实例a访问实例b的内网请求被允许流出。 ● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	IP地址： 192.168.52.0/24,10.0.0.0/24
优先级	安全组规则优先级。 优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。	1
策略	安全组规则策略，支持的策略如下： ● 如果“策略”设置为允许，表示允许安全组内的云服务器访问目的地址的指定端口。 ● 如果“策略”设置为拒绝，表示拒绝安全组内的云服务器访问目的地址的指定端口。 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。	允许
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

11. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

6.2.6.3 在安全组中一键放通常见端口

操作场景

您可以通过使用该功能，在安全组中一键放通常见端口。适用于以下场景：

- 远程登录云服务器
- 在云服务器内使用ping命令测试网络连通性
- 云服务器用作Web服务器对外提供网站访问服务

您可以一键放通的常见端口详细说明如表6-32所示。

表 6-32 一键放通常见端口说明

方向	类型和协议端口	源地址/目的地址	规则用途
入方向	TCP: 22 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的SSH(22)端口，用于远程登录Linux云服务器。
	TCP: 3389 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的RDP(3389)端口，用于远程登录Windows云服务器。
	TCP: 80 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的HTTP(80)端口，用于通过HTTP协议访问网站。
	TCP: 443 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的HTTPS(443)端口，用于通过HTTPS协议访问网站。
	TCP : 20-21 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的FTP(20和21)端口，用于远程连接云服务器上传或者下载文件。
	ICMP: 全部 (IPv4)	0.0.0.0/0	针对ICMP(IPv4)协议，允许外部所有IP访问安全组内云服务器的所有端口，用于通过ping命令测试云服务器的网络连通性。
出方向	全部 (IPv4) 全部 (IPv6)	0.0.0.0/0 ::/0	针对全部协议，允许安全组内的云服务器可访问外部任意IP和端口。

须知

安全组入方向规则的源地址设置为0.0.0.0/0或::/0，表示允许或拒绝所有外部IP地址访问您的实例，如果将“22、3389、8848”等**高危端口**暴露到公网，可能导致网络入侵，造成业务中断、数据泄露或数据勒索等严重后果。建议您将安全组规则设置为仅允许已知的IP地址访问。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签，单击“一键放通常见端口”。
   弹出常见端口列表页面。
7. 根据界面提示，单击“确定”。
   完成操作后，可以在安全组规则列表页面查看添加的安全组规则。

6.2.6.4 修改安全组规则

操作场景

当安全组规则设置不满足需求时，您可以参考以下操作修改安全组中的规则，保证云服务器等实例的网络安全。您可以修改安全组规则的端口号、协议、IP地址等。

当您修改安全组规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断或者引入不必要的网络安全问题。

约束与限制

安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。

- 在入方向中，**表6-33**中的入方向规则，确保安全组内实例的内网网络互通，不建议您修改该安全组规则。
- 在出方向中，**表6-33**中的出方向规则，允许所有流量从安全组内实例流出。如果您修改了该规则，可能导致安全组内的实例无法访问外部，请您谨慎操作。

表 6-33 安全组规则说明

方向	策略	类型	协议端口	源地址/目的地址
入方向	允许	IPv4	全部	源地址：当前安全组
入方向	允许	IPv6	全部	源地址：当前安全组
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0
出方向	允许	IPv6	全部	目的地址：::/0

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
7. 在安全组规则列表中，单击目标规则所在行的操作列下的“修改”。
8. 根据界面提示，修改安全组规则信息，并单击“确认”，保存修改。

6.2.6.5 复制安全组规则

操作场景

您可以复制安全组内已有的规则，然后基于已有的参数进行修改，快速生成一条新的规则。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
5. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。

6. 在安全组规则列表中，单击目标规则所在行的操作列下的“复制”。
   弹出复制安全组规则对话框。
7. 根据界面提示，修改安全组规则信息，并单击“确定”，保存修改。

6.2.6.6 启用/停用安全组规则

操作场景

安全组规则添加完成后，处于启用状态。您可以根据业务需求灵活启用或者停用安全组规则。

- 停用安全组规则后，规则将会失效。如果您停用了所有安全组规则，则此时拒绝任何流量流入或流出安全组内实例。当您的安全组已关联实例时，停用所有安全组规则的操作会导致相关实例的网络流量中断，请您谨慎评估后再执行该操作，避免对业务造成影响。
- 启用安全组规则后，规则将会生效。如果您的安全组已关联实例，启用安全组规则的操作会影响实例的网络流量走向，请您谨慎评估后再执行启用操作，避免对业务造成影响。

启用/停用单个安全组规则

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
7. 在安全组规则列表中，执行以下操作，启用或者停用安全组规则。
   - 启用安全组规则：
     i. 选择目标安全组规则所在行的操作列下的“更多 > 启用”。
        弹出启用确认对话框。
     ii. 确认信息无误后，单击“确定”，启用安全组规则。
   - 停用安全组规则：
     i. 选择目标安全组规则所在行的操作列下的“更多 > 停用”。
        弹出停用确认对话框。
     ii. 确认信息无误后，单击“确定”，停用安全组规则。

6.2.6.7 导入/导出安全组规则

操作场景

您可以在Excel格式文件中填写安全组规则参数，并将规则导入到安全组内。同时，您可以将已有安全组的规则导出至Excel格式文件中。

当您遇到如下场景时，推荐您使用导入和导出安全组功能。

- 本地备份安全组规则：如果您想在本地备份安全组规则，可以导出安全组内的规则，将安全组的出方向、入方向规则信息导出为Excel格式文件。
- 快速创建和恢复安全组规则：如果您想快速创建或恢复安全组规则，可以将安全组规则文件导入到已有安全组中。
- 快速迁移安全组规则：将某个安全组的规则快速应用到其他安全组。
- 批量修改安全组规则：将当前安全组的规则导出后，在Excel文件批量修改完成后，重新导入即可。

约束与限制

- 导入安全组规则时，请根据格式要求填写要求的参数，不能新增参数或者修改已有参数名称，否则会导入失败。
- 导入安全组规则时，当源地址/目的地址设置为安全组或者IP地址组时，请务必填写正确的ID信息，否则会导入失败。
- 当本次导入的安全组规则与安全组内已有规则重复，或者本次导入的安全组规则存在重复，系统将会自动忽略掉重复规则，不影响您执行导入操作。如表6-34所示，规则A、规则B以及规则C均为重复规则。
  - 规则A和规则B：规则的方向、策略、类型、协议端口、源地址/目的地址均相同，优先级不同时，为重复规则。
  - 规则A和规则C：规则的方向、优先级、策略、类型、协议端口、源地址/目的地址均相同时，为重复规则。

  表 6-34 规则重复示例

规则	方向	优先级	策略	类型	协议端口	目的地址
规则A	入方向	1	允许	IPv4	TCP：22	0.0.0.0/0
规则B	入方向	5	允许	IPv4	TCP：22	0.0.0.0/0
规则C	入方向	1	允许	IPv4	TCP：22	0.0.0.0/0

- 对于同一个方向的安全组规则，当类型、协议端口、源地址/目的地址均相同时，不允许这两条规则的策略相反，即不能规则A设置为允许，规则B设置为拒绝，示例如表6-35所示。
  - 当表格中的规则与安全组内已有规则的策略冲突时，安全组会导入失败，请根据界面提示排查修改。
  - 当表格中的规则策略冲突时，安全组会导入失败，请根据界面提示排查修改。

表 6-35 规则策略相反示例

规则	方向	优先级	策略	类型	协议端口	目的地址
规则A	入方向	1	**允许**	IPv4	TCP：22	0.0.0.0/0
规则B	入方向	5	**拒绝**	IPv4	TCP：22	0.0.0.0/0

- 当您在同一个账号内，跨区域导入安全组规则时，即将区域A的安全组规则导入到区域B时，不支持导入授权安全组访问或者授权IP地址组访问的安全组规则。
- 当您跨账号导入安全组规则时，即将账号A的安全组规则导入到账号B时，不支持导入授权安全组访问或者授权IP地址组访问的安全组规则。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表页面，单击目标安全组名称。
   进入安全组详情页面。
6. 导出/导入安全组规则。
   - 单击 “导出规则”，将当前安全组规则导出为Excel文件。
   - 单击 “导入规则”，将Excel文件中的安全组规则导入到当前安全组。
     导入模板中所涉及参数如**表6-36**所示。

     表 6-36 导入模板参数说明

参数	说明	取值样例
方向	安全组规则的方向： ● 入方向：入方向指外部访问安全组内的实例。 ● 出方向：出方向指安全组内的实例访问外部。	入方向
优先级	优先级可选范围为1-100，默认值为1，即最高优先级。优先级数字越小，规则优先级级别越高。	1
策略	安全组规则策略，支持的策略如下： ● 如果“策略”设置为允许，表示允许源地址访问安全组内云服务器的指定端口。 ● 如果“策略”设置为拒绝，表示拒绝源地址访问安全组内云服务器的指定端口。 安全组规则匹配流量时，首先按照优先级进行排序，其次按照策略排序，拒绝策略高于允许策略，更多信息请参见**流量匹配安全组规则的顺序**。	允许

参数	说明	取值样例
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。 在出方向规则中，表示安全组内实例访问外部地址的指定端口。 端口填写支持下格式： ● 单个端口：例如22 ● 连续端口：例如22-30 ● 多个端口：例如22,23-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 ● 全部端口：为空或1-65535	22或22-30或20,22-30
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
源地址	源地址是入方向规则中，用来匹配外部请求的地址，支持以下格式： ● IP地址：表示源地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示源地址为另外一个安全组，您可以选择当前账号下，同一个区域内的其他安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A设置入方向规则时的“策略”为允许，源地址选择安全组B时，表示来自实例b的内网访问请求被允许进入实例a。 安全组格式填写要求：安全组名称(安全组ID)，例如，sg-test(96a8a93f-XXX-d7872990c314) ● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 IP地址组格式填写要求：IP地址组名称(IP地址组ID)，例如，ipGroup-test(96a8a93f-XXX-d7872990c314)	sg-test[96a8a93f-XXX-d7872990c314]

参数	说明	取值样例
目的地址	目的地址是出方向规则中，用来匹配内部请求的地址，支持以下格式： ● IP地址：表示目的地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● 安全组：表示目的地址为另外一个安全组。当安全组A内有实例a，安全组B内有实例b，在安全组A设置出方向规则时的“策略”为允许，目的地址选择安全组B时，表示实例a内部的请求被允许出去访问实例b。 安全组格式填写要求：安全组名称(安全组ID)，例如，sg-test(96a8a93f-XXX-d7872990c314) ● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 IP地址组格式填写要求：IP地址组名称(IP地址组ID)，例如，ipGroup-test(96a8a93f-XXX-d7872990c314)	sg-test[96a8a93f-XXX-d7872990c314]
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
修改时间	安全组的修改时间。	-

6.2.6.8 删除安全组规则

操作场景

当您不需要通过某条安全组规则控制流量流入/流出安全组内实例时，您可以参考以下操作删除安全组规则。

约束与限制

当您删除安全组规则前，请您务必了解该操作可能带来的影响，避免误删除造成网络中断或者引入不必要的网络安全问题。

安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。

- 在入方向中，表6-37中的入方向规则，确保安全组内实例的内网网络互通，不建议您删除该安全组规则。
- 在出方向中，表6-37中的出方向规则，允许所有流量从安全组内实例流出。如果您删除了该规则，则安全组内的实例无法访问外部，请您谨慎操作。

表 6-37 安全组规则说明

方向	策略	类型	协议端口	源地址/目的地址
入方向	允许	IPv4	全部	源地址：当前安全组
入方向	允许	IPv6	全部	源地址：当前安全组
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0
出方向	允许	IPv6	全部	目的地址：::/0

删除单个安全组规则

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
7. 在安全组规则列表中，单击目标安全组规则所在行的操作列下的“删除”。
   弹出删除确认对话框。
8. 确认无误后，单击“确定”，删除安全组规则。

批量删除多个安全组规则

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组的名称超链接。

进入安全组详情页面。

6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
7. 在安全组规则列表中，勾选多个安全组规则，并单击列表左上方的“删除”。
   弹出删除确认对话框。
8. 确认无误后，单击“确定”，删除安全组规则。

6.2.6.9 查询安全组规则的变更记录

操作场景

基于云审计，系统可以记录VPC安全组规则变更的操作记录，您可以参考以下操作，查询安全组规则的变更记录，支持以下操作：

- 查询安全组规则的新增记录
- 查询安全组规则的修改记录
- 查询安全组规则的删除记录

使用须知

- 您需要**开通云审计服务**后，才可以通过云审计服务记录VPC安全组规则的变更操作。
- 在云审计的操作事件列表中，记录了各种云服务的操作事件。您可以通过操作事件名称或者资源类型，并结合操作时间，精准定位到操作记录，VPC安全组规则支持的操作事件名称和资源类型如**表6-38**所示。

表 6-38 VPC 安全组规则操作事件列表

操作名称	事件名称	资源类型
添加安全组规则	createSecurity-group-rule	security-group-rules
修改安全组规则	updateSecurity-group-rule	security-group-rules
删除安全组规则	deleteSecurity-group-rule	security-group-rules

操作步骤

以在安全组Sg-A中新增**表6-39**中的安全组规则为例，以下为您提供查看操作记录的步骤。

表 6-39 新增安全组规则

方向	策略	类型	协议端口	源地址	修改时间
入方向	允许	IPv4	TCP: 23	10.0.0.0/16	2024/06/19 10:46:07 GMT+08:00

1. 打开云审计控制台，通过事件名称，搜索添加安全组规则的操作事件，然后通过修改时间定位对应的记录。

   本示例中，通过“createSecurity-group-rule”搜索添加安全组规则的操作记录，查看操作事件的方法，请参见**查看审计事件**。

   图 6-20 事件列表（添加安全组规则）

2. 在事件列表中，单击目标事件名称对应的超链接。

   进入事件概览页面，您可以查看本次操作的详细信息，**表6-40**中为您提供关键信息样例和说明，包含执行该操作的用户信息以及安全组规则的详情。

   说明

   表6-40的样例仅供参考，实际信息以您查询到的为准。

   表 6-40 事件样例（添加安全组规则）

回显样例	说明
"source_ip": "124.71.XX.146",	执行该操作的客户端IP地址，如果为空，表示系统操作，本示例为124.71.XX.146。

回显样例	说明
"user": { "access_key_id": "HSTA205XXXXXC4MHAE", "account_id": "3c24f6f885294XXXXX93ce075fbd", "user_name": "cts-test-01", **"domain": {** **"name": "cts-test",** **"id": "3c24f6f885294XXXXX93ce075fbd"** **},** **"name": "cts-test-01",** "principal_is_root_user": "false", **"id": "a26ee7e7224XXXXXe4a28a9ce503",**	您可以在回显中查看执行操作的账号信息，关键参数说明如下： • **domain下的name**：账号名，本示例为cts-test。 • **domain下的id**：账号ID，本示例为3c24f6f885294XXXXX93ce075fbd。 • **name**：IAM用户名，本示例为cts-test-01，是账号cts-test下的一个用户。 • **id**：IAM用户ID，本示例为a26ee7e7224XXXXXe4a28a9ce503。 关于云审计事件的更多参数说明，请参见**事件结构**中的响应参数说明。
"response": "{\"request_id \":\"8d2d1111cafaXXX9b49d53e2da38f \",\"security_group_rules\":[{\"id\":\"b6acda6e-0976- XXXX-82bc-a8093cbd591d\",\"project_id \":\"15289aca74eXXXa37dea0315d99\",\"security_group _id\":\"3730d371-3111-4ace-XXXX- b00b7259e178\",\"remote_group_id\":null,**\"direction \":\"ingress\",\"protocol\":\"tcp\"**,\"description \":\"\",\"created_at\":\"2024-06-19T02:46:07Z \",\"updated_at\":\"2024-06-19T02:46:07Z \",**\"ethertype\":\"IPv4\",\"remote_ip_prefix \":\"10.0.0.0/16\",\"multiport \":\"23\"**,\"remote_address_group_id\":null,**\"action \":\"allow\",\"priority\":1**}]}",	您可以在**response**中查看安全组规则的详情，关键参数说明如下： • **direction**：安全组规则的方向，**ingress**表示入方向，**egress**表示出方向，本示例为入方向。 • **protocol**：安全组规则的协议类型，本示例为TCP。 • **ethertype**：安全组规则的类型，本示例为IPv4。 • **remote_ip_prefix**：安全组规则的源地址/目的地址，本示例中，由于添加的是入方向规则，因此表示源地址，取值为10.0.0.0/16。 • **multiport**：安全组规则的端口，本示例为23。 • **action**：安全组规则的策略，**allow**表示允许，**deny**表示拒绝，本示例为允许。 • **priority**：安全组规则的优先级，本示例为1。 关于安全组规则的更多参数说明，请参见**查询安全组规则**中的响应参数说明。

6.2.7 管理安全组关联的实例

6.2.7.1 在安全组中添加或移出实例

操作场景

创建实例的时候，会自动将实例加入一个安全组内，实例将会受到安全组的保护。

- 如果一个安全组无法满足您的要求，您可以将实例加入多个安全组。
- 实例必须加入一个安全组，如果您需要更换安全组，可以先将实例加入新的安全组，然后再将实例从原有安全组移出。

当前您可以在安全组中添加的实例类型包括服务器、扩展网卡以及辅助弹性网卡等。操作方法如下：

- **在安全组中添加实例**
- **在安全组中移出实例**

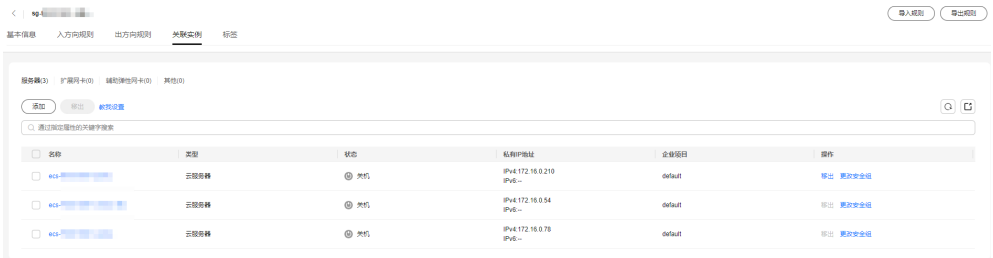
约束与限制

当查看安全组关联实例时，如果管理控制台提示您的权限不足，则除了安全组查看权限，还需要添加关联实例（如服务器、扩展网卡以及辅助弹性网卡等）对应资源的查看权限，具体请参见**•示例4：授权用户查看关联资源**。

在安全组中添加实例

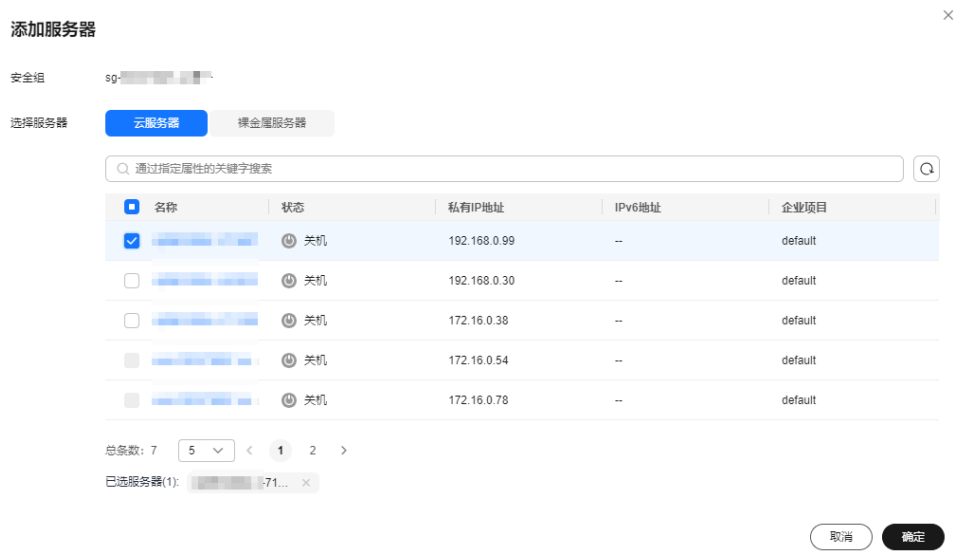
1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入实例列表页面。
6. 根据界面提示，选择目标实例类型对应的页签。
   以下操作，以选择“服务器”页签为例。

   图 6-21 关联实例（服务器页签）

7. 选择“服务器”页签，单击“添加”。
   弹出“添加服务器”对话框。

图 6-22 添加服务器



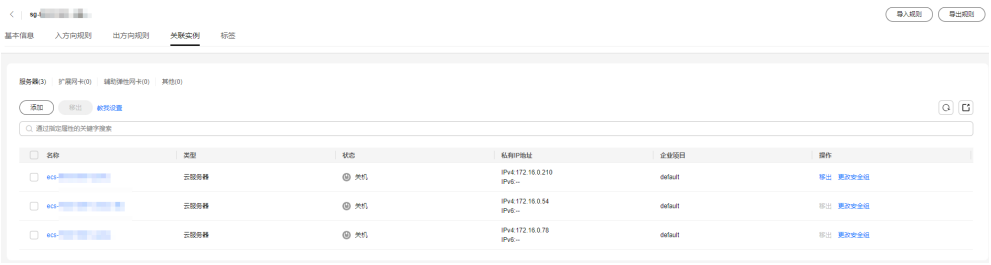
8. 在服务器列表中，选择一个或者多个服务器，并单击“确定”，将服务器加入到当前安全组中。

在安全组中移出实例

实例至少需要加入一个安全组，如果您要将实例移出安全组，请确保当前实例至少关联两个安全组。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入实例列表页面。
6. 根据界面提示，选择目标实例类型对应的页签。
   以下操作，以选择“服务器”页签为例。

图 6-23 关联实例（服务器页签）



7. 选择“服务器”页签，在服务器列表中，选择一个或者多个服务器，并单击列表左上方的“移出”。

弹出移出确认对话框。

图 6-24 移出服务器

8. 确认无误后，单击“确定”，将所选实例从安全组中移出。

6.2.7.2 更改 ECS 的安全组

操作场景

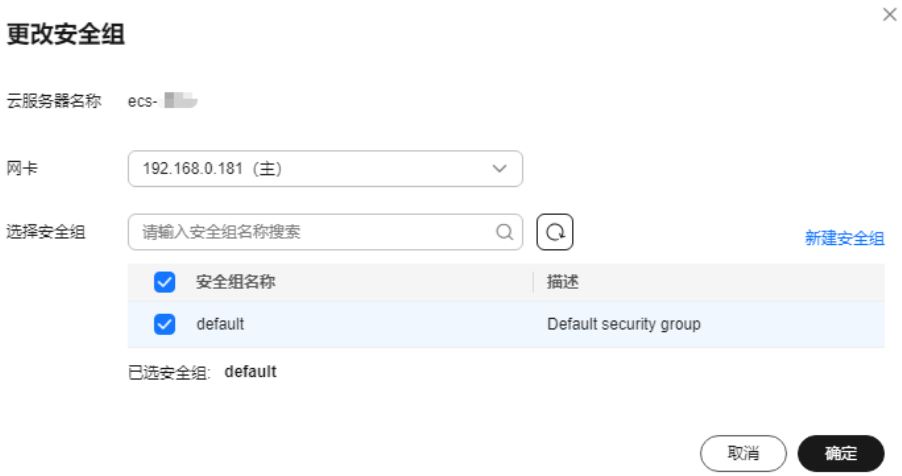
创建弹性云服务器时，必须将其加入一个安全组内，如果您未创建任何安全组，那么首次使用安全组时，系统会自动为您创建一个**默认安全组default**并关联至弹性云服务器。当默认安全组无法满足您的需求，您可以参考以下操作为弹性云服务器更改安全组。

除了默认安全组，您还可以为弹性云服务器关联自定义安全组，当自定义安全组不满足需求时，您也可以更改自定义安全组。

更改安全组（单台云服务器）

1. 登录管理控制台。
2. 单击“ ☰ ”，选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络/安全组 > 更改安全组”。
   系统弹窗显示“更改安全组”页面。

图 6-25 更改安全组



4. 根据界面提示，在下拉列表中选择待更改安全组的网卡，并重新选择安全组。

   您可以同时勾选多个安全组，弹性云服务器的访问规则先根据绑定安全组的顺序，再根据组内规则的优先级生效。

   如需创建新的安全组，请单击“新建安全组”。

   说明

   使用多个安全组可能会影响弹性云服务器的网络性能，建议您选择安全组的数量不多于5个。

5. 单击“确定”。

6.3 网络 ACL

6.3.1 网络 ACL 概述

网络 ACL

网络ACL是一个子网级别的可选安全防护层，您可以在网络ACL中设置入方向和出方向规则，并将网络ACL绑定至子网，可以精准控制出入子网的流量。

网络ACL与安全组的防护范围不同，安全组对云服务器、云容器、云数据库等实例进行防护，网络ACL对整个子网进行防护。安全组是必选的安全防护层，当您还想增加额外的安全防护层时，就可以启用网络ACL。两者结合起来，可以实现更精细、更复杂的安全访问控制。

网络ACL中包括入方向规则和出方向规则，您可以针对每条规则指定协议、来源端口和地址、目的端口和地址。以**图6-26**为例，在区域A内，某客户的虚拟私有云VPC-X有两个子网，子网Subnet-X01关联网络ACL Fw-A，Subnet-X01内部署的实例面向互联网提供Web服务。子网Subnet-X02关联网络ACL Fw-B，基于对等连接连通Subnet-X02和Subnet-Y01的网络，通过Subnet-Y01内的实例远程登录Subnet-X02内的实例。

- Fw-A的规则说明：

  入方向自定义规则，允许外部任意IP地址，通过TCP (HTTP)协议访问Subnet-X01内实例的80端口。如果流量未匹配上自定义规则，则匹配默认规则，无法流入子网。

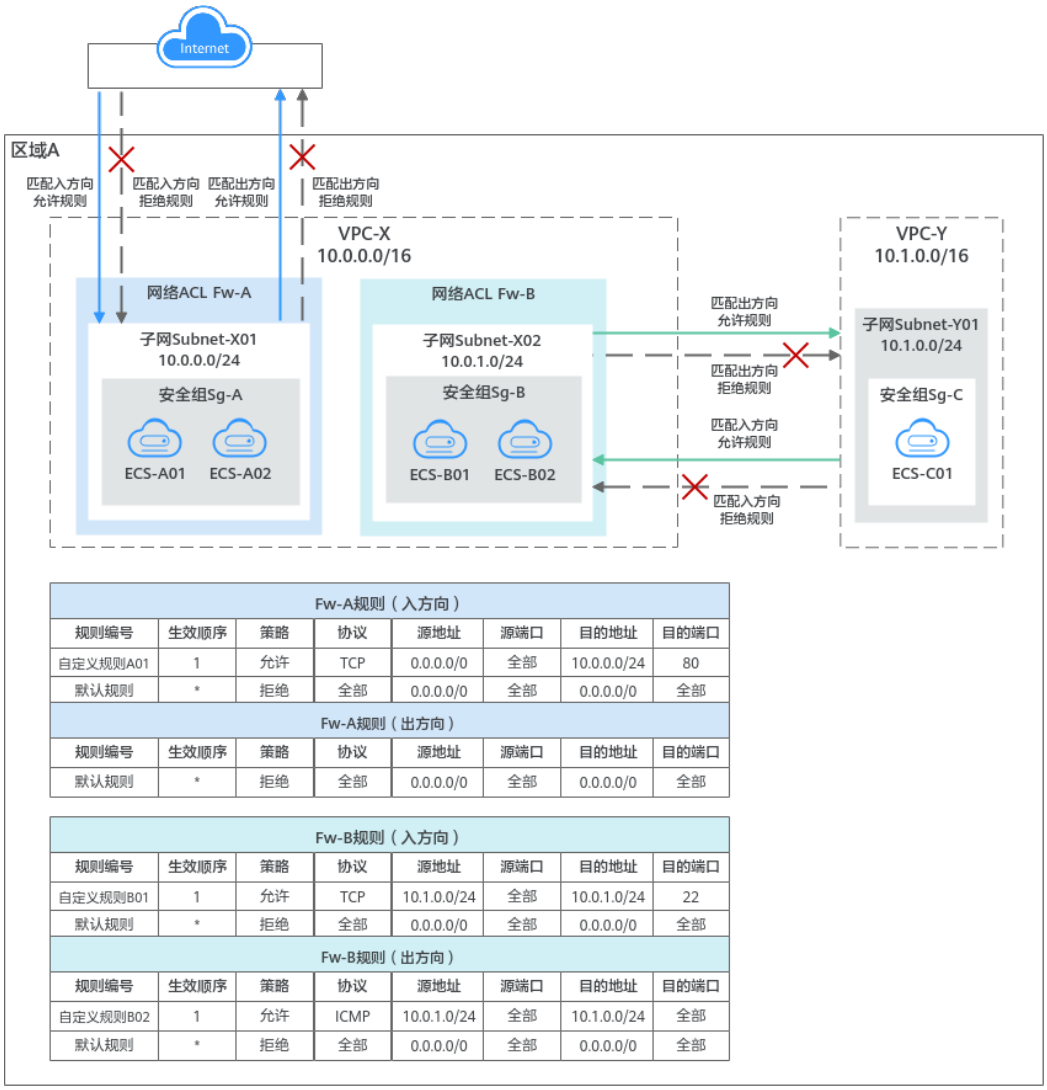
  网络ACL是有状态的，允许入站请求的响应流量出站，不受规则限制，因此Subnet-X01内实例的响应流量可流出子网。非响应流量的其他流量则匹配默认规则，无法流出子网。

- Fw-B的规则说明：

  入方向自定义规则，允许来自Subnet-Y01的流量，通过TCP (SSH)协议访问子网Subnet-X02内实例的22端口。

  出方向自定义规则，放通ICMP协议全部端口，当在Subnet-X02内实例**ping**测试网络连通性时，允许去往Subnet-Y01的流量流出子网。

图 6-26 网络 ACL 架构图



Fw-A规则（入方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A01	1	允许	TCP	0.0.0.0/0	全部	10.0.0.0/24	80
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
Fw-A规则（出方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Fw-B规则（入方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则B01	1	允许	TCP	10.1.0.0/24	全部	10.0.1.0/24	22
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
Fw-B规则（出方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则B02	1	允许	ICMP	10.0.1.0/24	全部	10.1.0.0/24	全部
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

说明

图中提供的示例仅为您展示了网络ACL对出入子网的流量控制。在实际业务中，除了网络ACL，实例上绑定的安全组也会影响出入实例的流量。进一步了解网络ACL与安全组的详细信息，请参见**VPC访问控制概述**。

网络 ACL 规则

- 网络ACL中包括入方向规则和出方向规则，用来控制VPC子网入方向和出方向的网络流量。
  - 入方向规则：控制外部请求访问子网内的实例，即流量流入子网。
  - 出方向规则：控制子网内实例访问外部的请求，即流量流出子网。
- 网络ACL规则由协议、源端口/目的端口、源地址/目的地址等组成，关键信息说明如下：
  - 生效顺序：网络ACL规则按照生效顺序依次排列，序号越小，排序越靠前，表示流量优先匹配该规则。

    默认网络ACL规则的序号为*，排在末尾，表示流量最后匹配该规则。

- 状态：网络ACL规则有“启用”和“停用”状态。启用时，网络ACL规则生效，停用时，网络ACL规则不生效。
- 类型：支持设置IPv4和IPv6协议的规则。
- 策略：支持允许或拒绝。当流量的协议、源端口/目的端口、源地址/目的地址成功匹配某个网络ACL规则后，会对流量执行规则对应的策略，允许或拒绝流量。
- 协议：匹配流量的网络协议类型，支持TCP、UDP、ICMP协议。
- 源地址/目的地址：匹配流量的源地址或者目的地址。

  您可以使用IP地址和IP地址组作为源地址或者目的地址。

  - IP地址：某个固定的IP地址或者网段，支持IPv4和IPv6地址。比如：192.168.10.10/32（IPv4地址）、192.168.1.0/24（IPv4网段）、2407:c080:802:469::/64（IPv6网段）
  - IP地址组：**IP地址组**是一个或者多个IP地址的集合，对于安全策略相同的IP网段和IP地址，建议您使用IP地址组简化管理。
- 源端口范围/目的端口范围：匹配流量的源端口或者目的端口，取值范围为1～65535。

网络 ACL 及规则的工作原理

- 网络ACL创建完成后，需要将网络ACL关联至目标子网，网络ACL规则才能控制出入该子网的流量。网络ACL可以同时关联多个子网，但一个子网只能关联一个网络ACL。
- 网络ACL是有状态的。如果您从实例发送一个出站请求，且该网络ACL的出方向规则是放通的话，那么无论其入方向规则如何，都将允许该出站请求的响应流量流入。同理，如果该网络ACL的入方向规则是放通的，那无论出方向规则如何，都将允许该入站请求的响应流量可以流出。
- 网络ACL使用连接跟踪来标识进出实例的流量信息，入方向和出方向网络ACL规则配置变更，对原有流量不会立即生效。

  当您在网络ACL内增加、删除、更新规则，或者在网络ACL内添加、移出子网时，由入方向/出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有网络ACL规则。入方向/出方向流量新建立的连接，将会匹配新的网络ACL出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

- 在网络ACL中，存在如表6-41所示的默认规则。当网络ACL中没有其他允许流量出入的自定义规则时，则匹配默认规则，拒绝任何流量流入或流出子网。在您将网络ACL关联至目标子网时，请确保已添加自定义规则放通业务流量，或者子网内无实际业务，避免默认规则造成业务流量中断。

  表 6-41 网络 ACL 默认规则说明

方向	生效顺序	策略	协议	源地址	源端口范围	目的地址	目的端口范围
入方向	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
出方向	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

- 网络ACL规则不会匹配筛选表6-42中的流量，即对应的流量被允许流入或者流出子网，不受网络ACL默认规则以及自定义规则限制。

  表 6-42 不受网络 ACL 规则限制的流量

方向	规则说明
入方向	放通当前子网内的流量，即允许同一个子网内实例互通。
	放通目的地址为255.255.255.255/32的广播流量。
	放通目的地址为224.0.0.0/24的组播流量。
出方向	放通当前子网内的流量，即允许同一个子网内实例互通。
	放通目的地址为255.255.255.255/32的广播流量。
	放通目的地址为224.0.0.0/24的组播流量。
	放通基于TCP协议，目的地址为169.254.169.254/32 ，目的端口为80的云服器元数据(metadata)流量。
	放通目的地址为100.125.0.0/16的流量，该网段是云上公共服务预留地址，比如DNS服务器地址、NTP服务器地址等。

流量匹配网络 ACL 规则的顺序

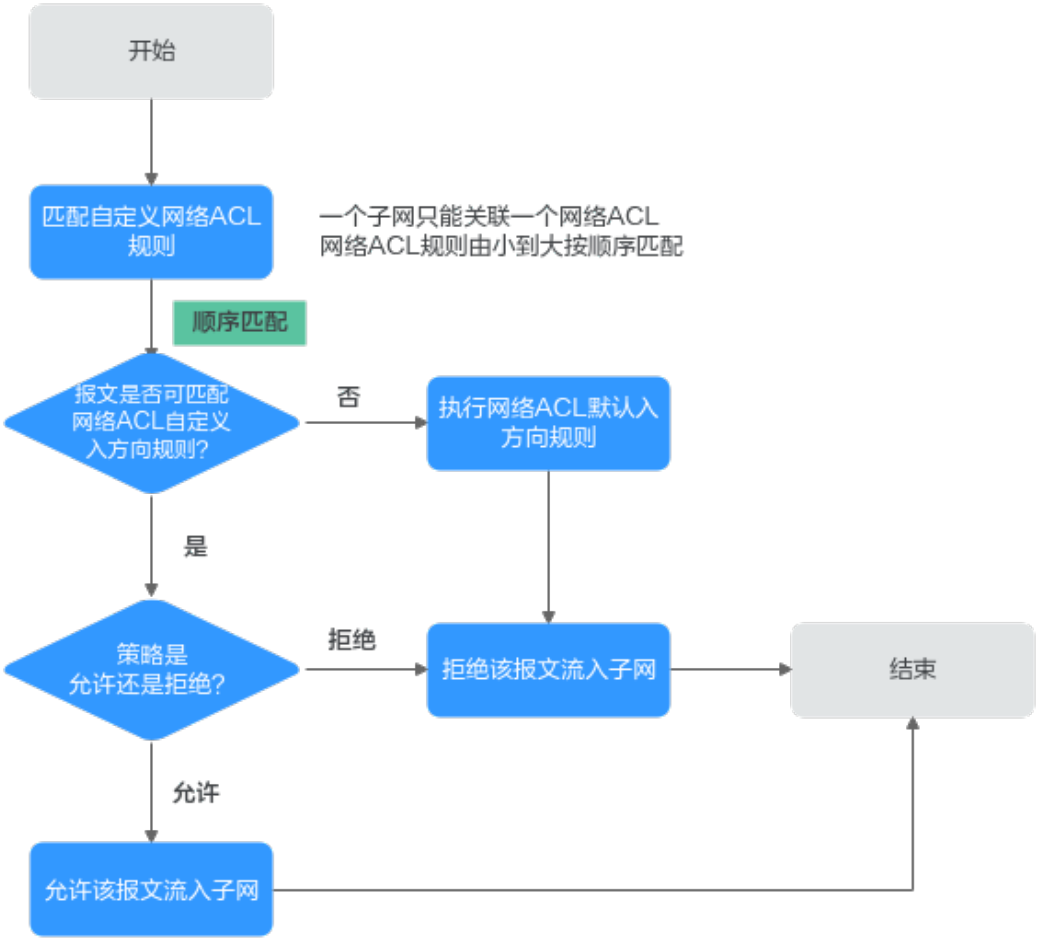
一个子网只能绑定一个网络ACL，当网络ACL存在多条规则时，流量按照规则的生效顺序进行匹配。序号越小，排序越靠前，越先执行该规则。默认网络ACL规则的序号为*，排在末尾，流量最后匹配该规则。

以入方向的流量为例，子网的网络流量将按照以下原则匹配网络ACL规则，入方向和出方向的流量匹配顺序相同。

- 当流量匹配上自定义规则，则根据规则策略决定流量走向。
  - 当策略为拒绝时，则拒绝该流量流入子网。
  - 当策略为允许时，则允许该流量流入子网。

- 当流量未匹配上任何自定义规则，则执行默认规则，拒绝流量流入子网。

图 6-27 网络 ACL 匹配顺序



网络 ACL 配置示例

网络ACL可以控制流入/流出子网的流量，当网络ACL和安全组同时存在时，流量先匹配网络ACL规则，然后匹配安全组规则。您可以灵活调整安全组的规则，并使用网络ACL作为子网的额外防护。以下为您提供了典型的网络ACL应用示例。

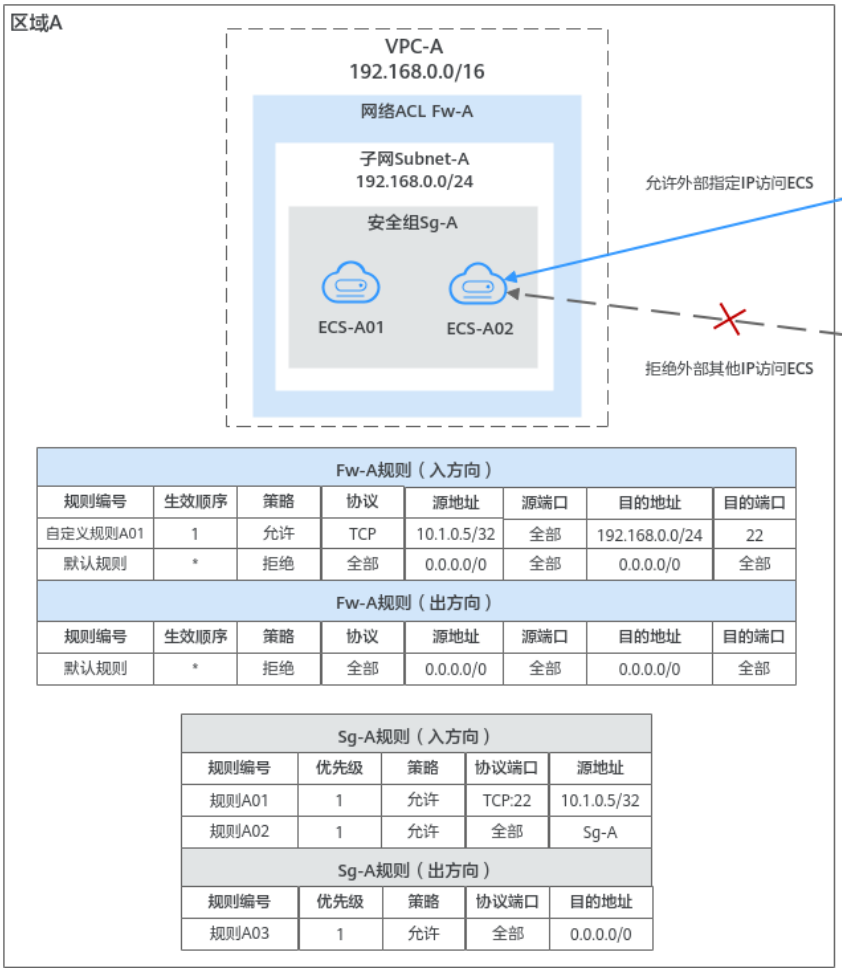
控制外部对子网内实例的访问

本示例如图6-28所示，子网Subnet-A内的两个业务实例ECS-A01和ECS-A02网络互通，并允许白名单实例远程登录业务实例，白名单实例的IP地址为10.1.0.5/32。白名单实例可能是VPC-A的其他子网或者其他VPC内的实例，也可以是本地计算机，可远程连接业务实例执行运维操作。因此，网络ACL和安全组规则需要放通白名单实例的流量，拦截来自其他网络的流量，规则配置如下：

- 网络ACL规则：
  - 入方向：自定义规则A01允许白名单实例，通过SSH远程登录子网Subnet-A内的实例。默认规则拒绝其他网络流量流入子网。
  - 出方向：网络ACL是有状态的，允许入站请求的响应流量流出，因此不用额外添加规则放通白名单实例的响应流量。默认规则拒绝其他网络流量流出子网。

- 安全组规则：
  - 入方向：规则A01允许白名单实例，通过SSH远程登录子网Subnet-A内的实例。规则A02允许安全组内实例互通。其他流量无法流入安全组内实例。
  - 出方向：规则A03允许所有流量从安全组内实例流出。

图 6-28 控制外部对子网内实例的访问



Fw-A规则（入方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A01	1	允许	TCP	10.1.0.5/32	全部	192.168.0.0/24	22
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Fw-A规则（出方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Sg-A规则（入方向）				
规则编号	优先级	策略	协议端口	源地址
规则A01	1	允许	TCP:22	10.1.0.5/32
规则A02	1	允许	全部	Sg-A

Sg-A规则（出方向）				
规则编号	优先级	策略	协议端口	目的地址
规则A03	1	允许	全部	0.0.0.0/0

如果您设置了过于宽松的安全组规则，此时网络ACL规则会作为额外防护。如表6-43所示，安全组规则允许任意IP地址远程登录安全组内实例。此时子网Subnet-A关联的网络ACL Fw-A，其入方向规则仅允许指定IP地址(10.1.0.5/32)访问Subnet-A内的实例，默认规则会拒绝其他流量流入子网，消除可能存在的安全风险。

表 6-43 安全组规则

方向	优先级	策略	类型	协议端口	源地址	规则作用
入方向	1	允许	IPv4	自定义 TCP: 22	IP地址：0.0.0.0/0	允许任意IP地址通过SSH远程登录安全组内实例

说明

更多网络ACL规则配置示例，请参见**网络ACL配置示例**。

控制不同子网内实例的互通和隔离

本示例如**图6-29**所示，VPC-X内有两个子网Subnet-X01和Subnet-X02，ECS-01和ECS-02属于Subnet-X01，ECS-03属于Subnet-X02。三台ECS的网络通信需求如下：

- ECS-02和ECS-03网络互通
- ECS-01和ECS-03网络隔离

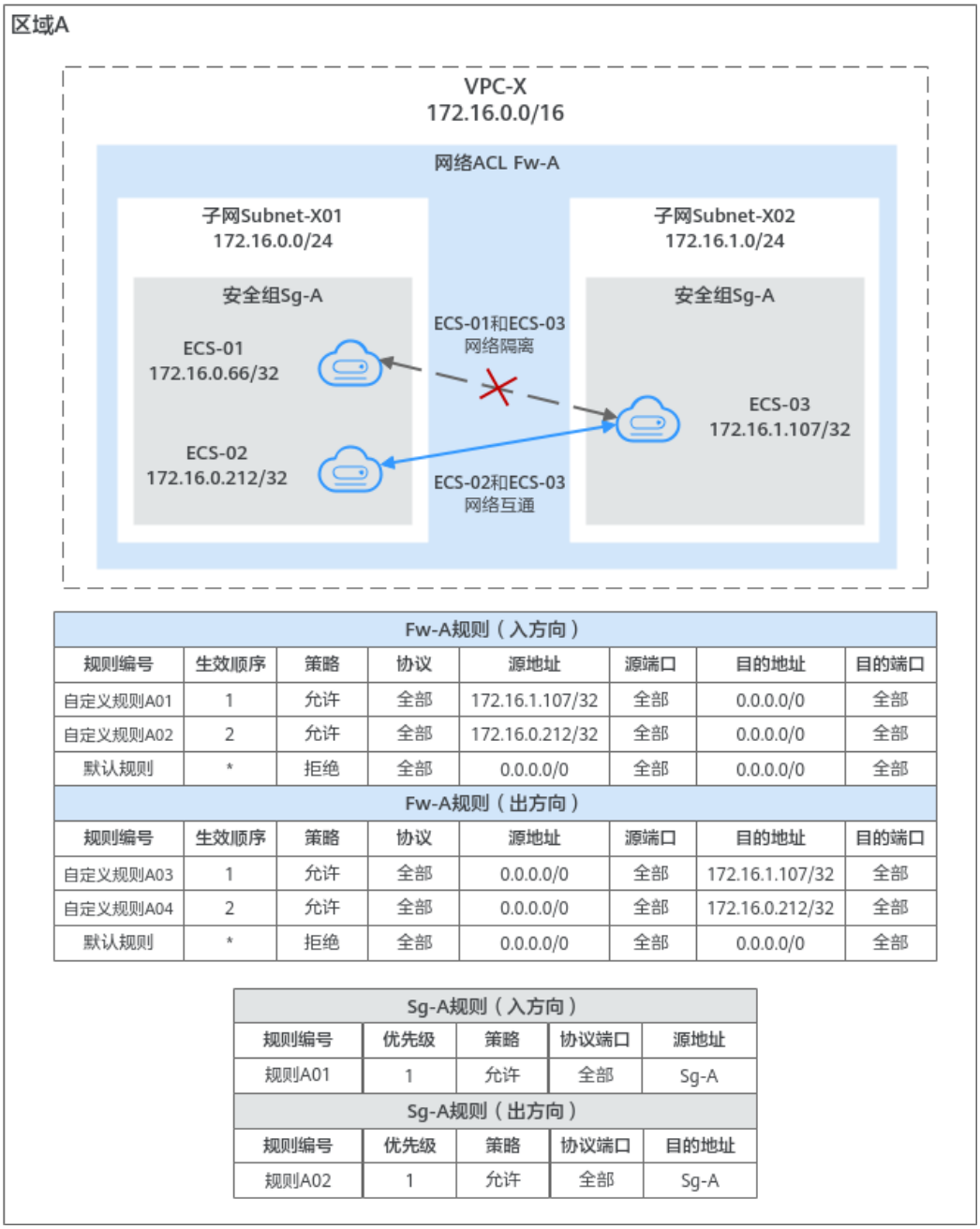
为了实现以上网络通信需求，本示例的安全组和网络ACL配置如下：

1. 三台ECS属于同一个安全组Sg-A，在Sg-A中添加入方向和出方向规则，确保安全组内实例网络互通。

   此时子网还未关联网络ACL，安全组规则配置完成后，ECS-01、ECS-02均可以和ECS-03进行通信。
2. 将两个子网均关联至网络ACL Fw-A。

   当Fw-A中只有默认规则时，同一个子网内实例网络互通，不同子网内实例网络隔离。此时ECS-01和ECS-02网络互通，ECS-01和ECS-03网络隔离、ECS-02和ECS-03网络隔离。
3. 在网络ACL Fw-A中添加自定义规则，放通ECS-02和ECS-03之间的网络。
   - 自定义规则A01：允许来自ECS-03的流量流入子网。
   - 自定义规则A02：允许来自ECS-02的流量流入子网。
   - 自定义规则A03：允许访问ECS-03的流量流出子网。
   - 自定义规则A04：允许访问ECS-02的流量流出子网。

图 6-29 控制不同子网内实例的互通和隔离



Fw-A规则（入方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A01	1	允许	全部	172.16.1.107/32	全部	0.0.0.0/0	全部
自定义规则A02	2	允许	全部	172.16.0.212/32	全部	0.0.0.0/0	全部
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
Fw-A规则（出方向）							
规则编号	生效顺序	策略	协议	源地址	源端口	目的地址	目的端口
自定义规则A03	1	允许	全部	0.0.0.0/0	全部	172.16.1.107/32	全部
自定义规则A04	2	允许	全部	0.0.0.0/0	全部	172.16.0.212/32	全部
默认规则	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

Sg-A规则（入方向）				
规则编号	优先级	策略	协议端口	源地址
规则A01	1	允许	全部	Sg-A
Sg-A规则（出方向）				
规则编号	优先级	策略	协议端口	目的地址
规则A02	1	允许	全部	Sg-A

说明

更多网络ACL规则配置示例，请参见**网络ACL配置示例**。

网络 ACL 配置流程

图 6-30 网络 ACL 配置流程

表 6-44 网络 ACL 配置流程说明

序号	步骤	说明	操作指导
1	创建网络ACL	网络ACL创建完成后，自带入方向和出方向默认规则，拒绝出入子网的流量。	**创建网络ACL**
2	配置网络ACL规则	网络ACL默认规则不支持删除和修改，您需要根据业务需求添加自定义规则，用于控制流入或流出子网的流量，流量将会优先匹配自定义规则。	**添加网络ACL规则**
3	将子网关联至网络ACL	您需要将子网关联至网络ACL，并且当网络ACL状态为“已开启”时，网络ACL规则会对出入子网的流量生效。 一个子网只能关联一个网络ACL。	**将子网关联至网络ACL**

网络 ACL 的使用限制

- 在一个区域内，单个用户默认最多可以创建200个网络ACL。
- 建议一个网络ACL单方向拥有的规则数量不要超过100条，否则会引起网络ACL性能下降。
- 在一个网络ACL的入方向中，最多可以有124条规则关联IP地址组，出方向同理。
- 在一个网络ACL中，对于入方向规则来说，源地址是IP地址组的规则数量+目的地址是IP地址组的规则数量+源端口是不连续端口号的规则数量+目的端口是不连续端口号的规则数量 ≤ 120条，否则超过数量的网络ACL规则将不生效。当同时存在IPv4和IPv6类型的网络ACL规则时，两种类型的网络ACL规则单独计算，即IPv4规则和IPv6规则可以各有120条。

  对于网络ACL出方向规则来说，源地址、目的地址、源端口和目的端口存在一样的限制。

  以网络ACL Fw-A的入方向IPv4规则为例，**表6-45**中提供了部分符合限制条件的规则供您参考。其中，当一条网络ACL规则同时符合多个限制时，比如规则A02即使用了不连续端口作为源端口，又使用了IP地址组作为源地址，此时只占用一条配额。

表 6-45 入方向网络 ACL 规则说明

规则编号	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围
规则A01	1	IPv4	拒绝	TCP	0.0.0.0/0	**22,25,27**	0.0.0.0/0	1-65535
规则A02	2	IPv4	允许	TCP	**IP地址组：ipGroup-A**	**22-24,25**	0.0.0.0/0	1-65535

规则编号	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围
规则A03	3	IPv4	允许	全部	0.0.0.0/0	全部	**IP地址组：ipGroup-B**	全部
规则A04	4	IPv4	允许	UDP	0.0.0.0/0	1-65535	0.0.0.0/0	**80-83,87**

- 当您的组网中存在以下情况时，来自ELB和VPCEP的流量不受网络ACL和安全组规则的限制。
  - ELB实例的监听器开启“获取客户端IP”功能时，不受限制。
    比如规则已明确拒绝来自ELB实例的流量进入后端云服务器，此时该规则无法拦截来自ELB的流量，流量依然会抵达后端云服务器。
  - VPCEP实例类型为“专业型”时，不受限制。

6.3.2 网络 ACL 配置示例

网络ACL可以控制流入/流出子网的流量，当网络ACL和安全组同时存在时，流量先匹配网络ACL规则，然后匹配安全组规则。您可以灵活调整安全组的规则，并使用网络ACL作为子网的额外防护。以下为您提供了典型的网络ACL应用示例。

- **拒绝外部访问子网内实例的指定端口**
- **拒绝外部指定IP地址访问子网内实例**
- **允许外部访问子网内实例的指定端口**

须知

如果您的网络ACL规则配置完成后不生效，请您**提交工单**联系客服处理。

使用须知

在配置规则之前，请您先了解以下信息：

- 在网络ACL中，存在如**表6-46**所示的默认规则。当网络ACL中没有其他允许流量出入的自定义规则时，则匹配默认规则，拒绝任何流量流入或流出子网。

表 6-46 网络 ACL 默认规则说明

方向	生效顺序	策略	协议	源地址	源端口范围	目的地址	目的端口范围
入方向	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部
出方向	*	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部

- 您无需单独添加放通响应流量的规则，因为网络ACL是有状态的，允许响应流量流入/流出子网，不受规则限制。

关于网络ACL规则的更多工作原理，请参见**网络ACL及规则的工作原理**。

拒绝外部访问子网内实例的指定端口

在本示例中，防止勒索病毒Wanna Cry对实例的攻击，因此隔离具有漏洞的应用端口，例如TCP 445端口。您可以为子网关联网络ACL，并添加对应入方向规则，如**表6-47**所示，其中目的地址10.0.0.0/24为需要防护的子网网段。

1. 网络ACL默认规则拒绝任何流量流入子网，因此需要先添加自定义规则02，放通入方向流量。
2. 添加自定义规则01，拒绝所有外部请求访问子网内实例的TCP 445端口。此时拒绝规则必须早于允许规则生效，因此需要将拒绝的规则插入到允许规则的前面，具体操作请参见**添加网络ACL规则（自定义生效顺序）**。

表 6-47 拒绝外部访问子网内实例的指定端口

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	规则说明
入方向	1	IPv4	拒绝	TCP	0.0.0.0/0	全部	10.0.0.0/24	445	自定义规则01
入方向	2	IPv4	允许	全部	0.0.0.0/0	全部	10.0.0.0/24	全部	自定义规则02
入方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认规则

拒绝外部指定 IP 地址访问子网内实例

本示例中，需要拦截异常IP访问子网内实例，例如拒绝来自IP地址（10.1.1.12/32）的流量流入子网，您可以为子网关联网络ACL，并添加对应入方向规则，如**表6-48**所示，其中目的地址10.5.0.0/24为需要防护的子网网段。

1. 网络ACL默认规则拒绝任何流量流入子网，因此需要先添加自定义规则02，放通入方向流量。
2. 添加自定义规则01，拒绝来自外部IP地址（10.1.1.12/32）的流量流入子网。此时拒绝规则必须早于允许规则生效，因此需要将拒绝的规则插入到允许规则的前面，具体操作请参见**添加网络ACL规则（自定义生效顺序）**。

表 6-48 拒绝外部指定 IP 地址访问子网内实例

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	规则说明
入方向	1	IPv4	拒绝	TCP	10.1.1.12/32	全部	10.5.0.0/24	全部	自定义规则01
入方向	2	IPv4	允许	全部	0.0.0.0/0	全部	10.5.0.0/24	全部	自定义规则02
入方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认规则

允许外部访问子网内实例的指定端口

本示例中，在子网内的实例上搭建了可供外部访问的网站，实例作为Web服务器，需要放通入方向的HTTP(80)和HTTPS(443)端口。当子网关联了网络ACL时，需要同时在网络ACL和安全组添加对应的规则。

1. 在网络ACL中，添加如**表6-49**所示的规则。
   - 添加定义规则01，允许任意IP地址通过HTTP协议，访问子网内实例的80端口。
   - 添加定义规则02，允许任意IP地址通过HTTPS协议，访问子网内实例的443端口。

   其中目的地址10.8.0.0/24为需要防护的子网网段。

表 6-49 网络 ACL 规则（允许外部访问子网内实例的指定端口）

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	规则说明
入方向	1	IPv4	允许	TCP	0.0.0.0/0	全部	10.8.0.0/24	80	自定义规则01

方向	生效顺序	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围	规则说明
入方向	2	IPv4	允许	TCP	0.0.0.0/0	全部	10.8.0.0/24	443	自定义规则02
入方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认规则
出方向	*	--	拒绝	全部	0.0.0.0/0	全部	0.0.0.0/0	全部	默认规则

2. 在安全组中，添加如**表6-50**所示的规则。
   - 入方向规则01：允许任意IP地址通过HTTP协议，访问实例的80端口。
   - 入方向规则02：允许任意IP地址通过HTTPS协议，访问实例的443端口。
   - 出方向规则03：允许任何流量从安全组内实例流出。

     安全组的出方向规则设置比较宽松，本示例中出方向通过网络ACL默认规则防护，仅允许入站流量的响应流量出站，会拦截其他流量出站。

表 6-50 安全组规则（允许外部访问子网内实例的指定端口）

方向	优先级	策略	类型	协议端口	源地址/目的地址	规则说明
入方向	1	允许	IPv4	自定义TCP:80	IP地址：0.0.0.0/0	规则01
入方向	1	允许	IPv4	自定义TCP:443	IP地址：0.0.0.0/0	规则02
出方向	1	允许	IPv4	全部	IP地址：0.0.0.0/0	规则03

6.3.3 管理网络 ACL

6.3.3.1 创建网络 ACL

操作场景

网络ACL与安全组的防护范围不同，安全组对云服务器、云容器、云数据库等实例进行防护，网络ACL对整个子网进行防护。安全组是必选的安全防护层，当您还想增加额外的安全防护层时，可以参考以下章节创建网络ACL。两者结合起来，可以实现更精细、更复杂的安全访问控制。

操作步骤

1. 进入**网络ACL列表页面**。
2. 在网络ACL列表右上方，单击“创建网络ACL”。
3. 根据界面提示信息，设置网络ACL的参数。

表 6-51 网络 ACL 参数说明

参数	参数说明	取值样例
区域	必选参数。 网络ACL必须和待绑定的子网位于同一个区域。	-
名称	必选参数。 网络ACL的名称。 网络ACL的名称只能由中文、英文字母、数字、下划线（_）、中划线（-）和点（.）组成，且不能有空格，长度不能大于64个字符。	fw-A
企业项目	必选参数。 创建网络ACL时，可以将网络ACL加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**。	default
标签	可选参数。 您可以在创建网络ACL的时候为网络ACL绑定标签，标签用于标识网络ACL资源，可通过标签实现对网络ACL资源的分类和搜索。 关于标签更详细的说明，请参见**管理网络ACL标签**。	“标签键”：test “标签值”：01
描述	网络ACL的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含<、>符号。	-

4. 网络ACL参数设置完成后，单击“立即创建”，完成创建。

后续操作

1. 网络ACL创建完成后，自带入方向和出方向默认规则，拒绝出入子网的流量。您需要根据业务需求添加自定义规则，流量将会优先匹配自定义规则，具体操作请参见**添加网络ACL规则**。
2. 您需要将子网关联至网络ACL，并且当网络ACL状态为“已开启”时，网络ACL规则会对出入子网的流量生效，具体操作请参见**将子网关联至网络ACL**。

6.3.3.2 修改网络 ACL 基本信息

操作场景

网络ACL创建完成后，您可以参考以下操作修改网络ACL的名称和描述。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 在网络ACL基本信息区域，根据界面提示，修改名称和描述。

6.3.3.3 开启/关闭网络 ACL

操作场景

- 关闭网络ACL后，自定义规则将会失效，只有默认规则生效，此时拒绝任何流量流入或流出子网。当您的网络ACL已关联子网时，关闭操作会导致相关子网的网络流量中断，请您谨慎评估后再执行关闭操作，避免对业务造成影响。
- 开启网络ACL后，自定义规则和默认规则都会生效。如果您的网络ACL已关联子网，并且只有默认规则时，开启操作会导致相关子网的网络流量中断，请您谨慎评估后再执行开启操作，避免对业务造成影响。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，开启或者关闭目标网络ACL。
   - 开启网络ACL：
     i. 选择目标网络ACL所在行的操作列下的“更多 > 开启”。
        弹出开启确认对话框。
     ii. 确认信息无误后，单击“确定”，开启网络ACL。
   - 关闭网络ACL：

i. 选择目标网络ACL所在行的操作列下的“更多 > 关闭”。
弹出关闭确认对话框。
ii. 确认信息无误后，单击“确定”，关闭网络ACL。

6.3.3.4 查看网络 ACL

操作场景

您可以参考以下操作查看您的网络ACL，包括网络ACL名称、网络ACL规则以及网络ACL关联的子网等信息。

同时，您可以通过搜索功能，使用网络ACL名称、ID以及描述等关键信息快速搜索目标网络ACL。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
进入网络ACL详情页。
6. 在网络ACL详情页面，可以查看以下信息。
   - 基本信息：网络ACL的名称、ID、状态和描述信息等。
   - 入方向规则和出方向规则：规则的状态、协议、源地址、源端口、目的地址以及目的端口等。
   - 关联子网：网络ACL关联的子网，一个网络ACL可以同时关联多个子网。
   - 标签：网络ACL的标签信息。

6.3.3.5 管理网络 ACL 标签

操作场景

标签用于标识云资源，您可以通过标签实现对网络ACL资源的分类和搜索。您可以参考以下操作管理网络ACL标签：

- 添加网络ACL标签
- 修改网络ACL标签
- 删除网络ACL标签

网络ACL标签规则的详细说明，请参见**表6-52**。

表 6-52 网络 ACL 标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	test
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 进入**网络ACL列表页面**。
5. 在网络ACL列表中，单击目标网络ACL名称超链接。
   进入网络ACL详情页面。
6. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
7. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

6.3.3.6 删除网络 ACL

操作场景

当您的网络ACL不需要使用时，您可以参考以下操作删除不需要的网络ACL。

当网络ACL已关联子网时，删除网络ACL时，会将子网和网络ACL解除关联，该操作可能会影响相关子网的网络流量，请您谨慎评估后再执行删除操作，避免对业务造成影响。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，选择目标网络ACL所在行的操作列下的“更多 > 删除”。
   弹出删除确认对话框。
6. 根据界面提示完成信息确认后，删除网络ACL。

6.3.4 管理网络 ACL 规则

6.3.4.1 添加网络 ACL 规则

操作场景

您可以在网络ACL中添加入方向和出方向规则，用于控制流入和流出子网的流量。添加网络ACL规则时，您可以使用系统默认的规则生效顺序，也可以指定规则生效顺序，详细如下：

- **添加网络ACL规则（默认生效顺序）**：系统会按照规则添加的时间生成生效顺序，先添加的规则排序靠前，即优先匹配流量，不支持您指定生效顺序。
  如**表6-53**所示，网络ACL入方向中已有两条自定义规则（规则A、规则B）和一条默认规则，自定义规则A的生效顺序为1，自定义规则B的生效顺序为2，默认规则的生效顺序排在末尾。此时添加规则C，则系统指定规则C的生效顺序为3，生效顺序晚于规则A和规则B，高于默认规则。

表 6-53 规则排序示例说明（默认生效顺序）

添加规则C前的排序情况		添加规则C后的排序情况	
自定义规则A	1	自定义规则A	1
--	--	自定义规则B	2
自定义规则B	2	**自定义规则C**	**3**

添加规则C前的排序情况		添加规则C后的排序情况	
默认规则	*	默认规则	*

- **添加网络ACL规则（自定义生效顺序）**：如果您新增的网络ACL规则生效顺序需要早于或者晚于已有的某条规则，则可以在对应规则前面或者后面插入新的规则。

  如表6-54所示，网络ACL入方向中已有两条自定义规则（规则A、规则B）和一条默认规则，自定义规则A的生效顺序为1，自定义规则B的生效顺序为2，默认规则的生效顺序排在末尾。比如，当新增规则C的生效顺序需要高于规则B时，则可以在规则B前面插入规则C。规则C添加完成后，规则C的生效顺序为2，规则B的生效顺序顺延为3，规则C的生效顺序高于规则B。

  表 6-54 规则排序示例说明（自定义生效顺序）

插入规则C前的排序情况		插入规则C后的排序情况	
自定义规则A	1	自定义规则A	1
--	--	**自定义规则C**	**2**
自定义规则B	2	自定义规则B	3
默认规则	*	默认规则	*

约束与限制

建议一个网络ACL单方向拥有的规则数量不要超过100条，否则会引起网络ACL性能下降。

添加网络 ACL 规则（默认生效顺序）

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 在“入方向规则”或者“出方向规则”页签，单击“添加规则”。
   弹出“添加入方向规则”或者“添加出方向规则”对话框。
7. 据界面提示，设置入方向或者出方向规则参数。
   - 单击，可以依次增加多条规则。
   - 单击网络ACL规则操作列下的“复制”，复制已有的网络ACL规则。

表 6-55 参数说明

参数	参数说明	取值样例
类型	规则支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
策略	网络ACL规则策略，支持的策略如下： ● 如果“策略”设置为允许，表示允许成功匹配规则的流量流入或者流出子网。 ● 如果“策略”设置为拒绝，表示拒绝成功匹配规则的流量流入或者流出子网。	允许
协议	网络ACL规则中用来匹配流量的网络协议类型，支持TCP、UDP、ICMP协议。	TCP
源地址	源地址用来匹配流量的来源网址，支持以下格式： ● IP地址：表示源地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。同一个网络ACL规则中，源地址和目的地址只能有一方可以使用IP地址组。例如，源地址使用了IP地址组，则目的地址不能使用IP地址组。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	192.168.0.0/24

参数	参数说明	取值样例
源端口范围	网络ACL规则中用来匹配流量的源端口，取值范围为：1～65535。 端口填写支持下格式： ● 单个端口：例如22 ● 连续端口：例如22-30 ● 多个端口：例如22,24-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 ● 全部端口：为空或1-65535	22-30
目的地址	目的地址用来匹配流量的目的网址，支持以下格式： ● IP地址：表示目的地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 同一个网络ACL规则中，源地址和目的地址只能有一方可以使用IP地址组。例如，源地址使用了IP地址组，则目的地址不能使用IP地址组。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	0.0.0.0/0

参数	参数说明	取值样例
目的端口范围	网络ACL规则中用来匹配流量的目的端口，取值范围为：1～65535。 端口填写支持下格式： ● 单个端口：例如22 ● 连续端口：例如22-30 ● 多个端口：例如22,23-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 ● 全部端口：为空或1-65535	22-30
描述	网络ACL规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含<、>符号。	-

8. 规则设置完成后，单击“确定”。
   返回规则列表，可以查看添加的规则。
   - 规则按照添加时间自动排序，先添加的规则排序靠前，优先匹配流量。
   - 新添加的规则，状态为“启用”，表示规则生效。

添加网络 ACL 规则（自定义生效顺序）

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据需求选择“入方向规则”或者“出方向规则”页签，在指定位置插入新规则。
   - 选择目标网络ACL规则所在行的操作列下的“更多 > 向前插规则”，则新规则生效顺序早于当前规则。
   - 选择目标网络ACL规则所在行的操作列下的“更多 > 向后插规则”，则新规则生效顺序晚于当前规则。

6.3.4.2 修改网络 ACL 规则

操作场景

当网络ACL规则设置不满足需求时，您可以参考以下操作修改网络ACL中的规则，保证子网内实例的网络安全。您可以修改网络ACL规则的端口、协议、IP地址等。

当您的网络ACL已关联子网时，修改操作会影响子网的网络流量走向，请您谨慎评估后再执行修改，避免对业务造成影响。

约束与限制

网络ACL默认规则不支持任何修改和删除操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据需求选择“入方向规则”或者“出方向规则”页签，单击目标网络ACL规则所在行的操作列下的“修改”，并根据界面提示修改相关参数。参数说明如表6-56所示。

表 6-56 参数说明

参数	参数说明	取值样例
类型	规则支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
策略	网络ACL规则策略，支持的策略如下： ● 如果“策略”设置为允许，表示允许成功匹配规则的流量流入或者流出子网。 ● 如果“策略”设置为拒绝，表示拒绝成功匹配规则的流量流入或者流出子网。	允许
协议	网络ACL规则中用来匹配流量的网络协议类型，支持TCP、UDP、ICMP协议。	TCP

参数	参数说明	取值样例
源地址	源地址用来匹配流量的来源网址，支持以下格式： ● IP地址：表示源地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● IP地址组：表示源地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。同一个网络ACL规则中，源地址和目的地址只能有一方可以使用IP地址组。例如，源地址使用了IP地址组，则目的地址不能使用IP地址组。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	192.168.0.0/24
源端口范围	网络ACL规则中用来匹配流量的源端口，取值范围为：1～65535。 端口填写支持下格式： ● 单个端口：例如22 ● 连续端口：例如22-30 ● 多个端口：例如22,24-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 ● 全部端口：为空或1-65535	22-30

参数	参数说明	取值样例
目的地址	目的地址用来匹配流量的目的网址，支持以下格式： ● IP地址：表示目的地址为某个固定的IP地址。 – 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 – IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 – 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。 ● IP地址组：表示目的地址为一个IP地址组，IP地址组是一个或者多个IP地址的集合。您可以在下拉列表中，选择可用的IP地址组。对于安全策略相同的IP网段和IP地址，此处建议您使用IP地址组简化管理。 同一个网络ACL规则中，源地址和目的地址只能有一方可以使用IP地址组。例如，源地址使用了IP地址组，则目的地址不能使用IP地址组。 如果没有可用的IP地址组，请您参见**创建IP地址组**进行创建。	0.0.0.0/0
目的端口范围	网络ACL规则中用来匹配流量的目的端口，取值范围为：1～65535。 端口填写支持下格式： ● 单个端口：例如22 ● 连续端口：例如22-30 ● 多个端口：例如22,23-30，一次最多支持20个不连续端口组， 端口组之间不能重复。 ● 全部端口：为空或1-65535	22-30
描述	网络ACL规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含<、>符号。	-

7. 修改完成后，并单击“确认”，保存修改。

6.3.4.3 启用/停用网络 ACL 规则

操作场景

网络ACL规则添加完成后，一般处于启用状态。您可以根据业务需求灵活启用或者停用网络ACL自定义规则。

- 停用网络ACL自定义规则后，规则将会失效。如果您停用了所有自定义规则，则只有默认规则生效，此时拒绝任何流量流入或流出子网。当您的网络ACL已关联子网时，停用所有自定义规则的操作会导致相关子网的网络流量中断，请您谨慎评估后再执行该操作，避免对业务造成影响。
- 启用网络ACL自定义规则后，规则将会生效。如果您的网络ACL已关联子网，启用操作会影响子网的网络流量走向，请您谨慎评估后再执行启用操作，避免对业务造成影响。

当您需要对单个网络ACL规则执行操作时，请参见**启用/停用单个网络ACL规则**。

当您需要对多个网络ACL规则批量执行操作时，请根据需求选择适合的方法，具体如下：

- 当您要操作的规则数量较少，可以在控制台的网络ACL规则列表中，直接勾选多个规则后批量操作，请参见**批量启用/停用多个网络ACL规则（通过控制台批量勾选规则）**。
- 当您要操作的规则数量较多，在控制台直接勾选网络ACL规则时需要大量重复工作，则推荐您先**将当前网络ACL内的规则导出为本地Excel表格文件**，然后在表格中筛选并保留待操作的规则。Excel表格文件处理完成后，将Excel表格文件导入控制台，则系统会根据表格自动匹配网络ACL内的规则，并勾选待处理的规则，可提升处理效率，请参见**批量启用/停用多个网络ACL规则（通过Excel文件快速匹配规则）**。

约束与限制

网络ACL默认规则不支持任何修改和删除操作。

启用/停用单个网络 ACL 规则

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入网络ACL规则列表页面。
7. 在网络ACL规则列表中，执行以下操作，启用或者停用网络ACL规则。
   - 启用网络ACL规则：
     i. 选择目标网络ACL规则所在行的操作列下的“更多 > 启用”。

弹出启用确认对话框。

ii. 确认信息无误后，单击“确定”，启用网络ACL规则。

- 停用网络ACL规则：

i. 选择目标网络ACL规则所在行的操作列下的“更多 > 停用”。
弹出停用确认对话框。

ii. 确认信息无误后，单击“确定”，停用网络ACL规则。

批量启用/停用多个网络 ACL 规则（通过控制台批量勾选规则）

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
进入网络ACL详情页。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
进入网络ACL规则列表页面。
7. 在网络ACL规则列表中，勾选多个网络ACL规则。
8. 在网络ACL规则列表上方，执行以下操作，批量启用或者停用网络ACL规则。
   - 启用网络ACL规则：
     i. 在网络ACL规则列表上方，选择“更多 > 启用”。
     弹出启用确认对话框。
     ii. 确认信息无误后，单击“确定”，启用网络ACL规则。
   - 停用网络ACL规则：
     i. 在网络ACL规则列表上方，选择“更多 > 停用”。
     弹出停用确认对话框。
     ii. 确认信息无误后，单击“确定”，停用网络ACL规则。

批量启用/停用多个网络 ACL 规则（通过 Excel 文件快速匹配规则）

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
进入网络ACL详情页。

6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入网络ACL规则列表页面。
7. 在网络ACL规则列表上方，单击“批量筛选”。
   弹出“批量筛选”对话框。
8. 执行以下操作，选择适合您业务的方法，在Excel表格文件中处理待操作的网络ACL规则。
   - 方法一：单击“下载模板”，将Excel表格文件下载至本地，并根据模板要求在表格中填写待操作的网络ACL规则。
   - 方法二：**将当前网络ACL内的规则导出为本地Excel表格文件**，然后在表格中筛选并保留待操作的网络ACL规则。

   Excel表格文件处理完成后，请继续执行**9**导入Excel表格文件，随后系统会根据您导入的表格自动筛选出目标网络ACL规则。
9. 在“批量筛选”对话框中，单击“添加文件”，导入Excel表格文件。
   系统开始对表格中的规则和网络ACL内已有的规则进行匹配，并展示匹配结果。网络ACL规则的匹配项包括：类型、策略、协议、源地址、源端口范围、目的地址、目的端口范围。
   - 匹配成功的规则会显示“校验通过”：当表格中的规则匹配上当前网络ACL内已有规则时，才可以对规则进行操作。
   - 未匹配成功的规则会显示失败原因，通常有以下原因：
     - 表格中的规则未匹配上当前网络ACL内已有规则，即在网络ACL中不存在表格中的规则。
     - 表格中规则的方向与当前操作的方向不一致，比如表格中规则的方向为出方向，而您本次在“入方向规则”页签下执行操作。
     - 表格中存在多条相同的规则，系统会自动将多余的重复规则过滤掉。
10. 在“批量筛选”对话框中，当您确认本次批量操作的规则无误后，单击“确定”。
    进入网络ACL规则列表页面，此时系统会自动勾选待操作的规则。
11. 在网络ACL规则列表上方，执行以下操作，批量启用或者停用网络ACL规则。
    - 启用网络ACL规则：
      i. 在网络ACL规则列表上方，选择“更多 > 启用”。
         弹出启用确认对话框。
      ii. 确认信息无误后，单击“确定”，启用网络ACL规则。
    - 停用网络ACL规则：
      i. 在网络ACL规则列表上方，选择“更多 > 停用”。
         弹出停用确认对话框。
      ii. 确认信息无误后，单击“确定”，停用网络ACL规则。

6.3.4.4 导出/导入网络 ACL 规则

操作场景

您可以在Excel格式文件中填写网络ACL规则参数，并将规则导入到网络ACL内。同时，您可以将已有网络ACL的规则导出至Excel格式文件中。

当您遇到如下场景时，推荐您使用导入和导出网络ACL功能。

- 本地备份网络ACL规则：如果您想在本地备份网络ACL规则，可以导出网络ACL内的规则，将网络ACL的出方向、入方向规则信息导出为Excel格式文件。
- 快速创建和恢复网络ACL规则：如果您想快速创建或恢复网络ACL规则，可以将网络ACL规则文件导入到已有网络ACL中。
- 快速迁移网络ACL规则：将某个网络ACL的规则快速应用到其他网络ACL。
- 批量修改网络ACL规则：将当前网络ACL的规则导出后，在Excel文件批量修改完成后，重新导入即可。

约束与限制

- 导入/导出网络ACL规则时，建议您每次处理少于40条的规则，否则可能会影响性能。40条是入方向和入方向规则的总和。
- 导入规则是基于已有规则的增量导入，不会删除已有规则。
- 相同规则不允许重复导入。
- 默认规则不支持导出，您可以导出自定义规则。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 导出/导入网络ACL规则。
   - 单击 “导出规则”，将当前网络ACL规则导出为Excel文件。
   - 单击 “导入规则”，将Excel文件中的网络ACL规则导入到当前网络ACL。

6.3.4.5 删除网络 ACL 规则

操作场景

当您不需要通过某条网络ACL规则控制流量出入子网时，您可以参考以下操作删除网络ACL规则。

当您的网络ACL已关联子网时，删除操作会影响子网的网络流量走向，请您谨慎评估后再执行修改，避免对业务造成影响。

当您需要对单个网络ACL规则执行操作时，请参见**删除单个网络ACL规则**。

当您需要对多个网络ACL规则批量执行操作时，请根据需求选择适合的方法，具体如下：

- 当您要删除的规则数量较少，可以在控制台的网络ACL规则列表中，直接勾选多个规则后批量删除，请参见**批量删除多个网络ACL规则（通过控制台批量勾选规则）**。
- 当您要删除的规则数量较多，在控制台直接勾选网络ACL规则时需要大量重复工作，则推荐您先**将当前网络ACL内的规则导出为本地Excel表格文件**，然后在表格中筛选并保留待操作的规则。Excel表格文件处理完成后，将Excel表格文件导入控制台，则系统会根据表格自动匹配网络ACL内的规则，并勾选待处理的规则，可提升处理效率，请参见**批量删除多个网络ACL规则（通过Excel文件快速匹配规则）**。

约束与限制

网络ACL默认规则不支持任何修改和删除操作。

批量删除网络ACL规则时，一次最多可删除50条规则。

删除单个网络 ACL 规则

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入网络ACL规则列表页面。
7. 在网络ACL规则列表中，单击目标网络ACL规则所在行的操作列下的“删除”。
   弹出删除确认对话框。
8. 确认无误后，单击“确定”，删除网络ACL规则。

批量删除多个网络 ACL 规则（通过控制台批量勾选规则）

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入网络ACL规则列表页面。

7. 在网络ACL规则列表中，勾选多个网络ACL规则，并单击列表左上方的“删除”。
   弹出删除确认对话框。
8. 确认无误后，单击“确定”，删除网络ACL规则。

批量删除多个网络 ACL 规则（通过 Excel 文件快速匹配规则）

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏中，选择“访问控制 > 网络ACL”。
   进入网络ACL列表页面。
5. 在网络ACL列表中，单击网络ACL名称。
   进入网络ACL详情页。
6. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入网络ACL规则列表页面。
7. 在网络ACL规则列表上方，单击“批量筛选”。
   弹出“批量筛选”对话框。
8. 执行以下操作，选择适合您业务的方法，在Excel表格文件中处理待操作的网络ACL规则。
   - 方法一：单击“下载模板”，将Excel表格文件下载至本地，并根据模板要求在表格中填写待操作的网络ACL规则。
   - 方法二：**将当前网络ACL内的规则导出为本地Excel表格文件**，然后在表格中筛选并保留待操作的网络ACL规则。

   Excel表格文件处理完成后，请继续执行**9**导入Excel表格文件，随后系统会根据您导入的列表快速筛选出目标网络ACL规则。
9. 在“批量筛选”对话框中，单击“添加文件”，导入Excel表格文件。
   系统开始对表格中的规则和网络ACL内已有的规则进行匹配，并展示匹配结果。网络ACL规则的匹配项包括：类型、策略、协议、源地址、源端口范围、目的地址、目的端口范围。
   - 匹配成功的规则会显示“校验通过”：当表格中的规则匹配上当前网络ACL内已有规则时，才可以对规则进行操作。
   - 未匹配成功的规则会显示失败原因，通常有以下原因：
     - 表格中的规则未匹配上当前网络ACL内已有规则，即在网络ACL中不存在表格中的规则。
     - 表格中规则的方向与当前操作的方向不一致，比如表格中规则的方向为出方向，而您本次在“入方向规则”页签下执行操作。
     - 表格中存在多条相同的规则，系统会自动将多余的重复规则过滤掉。
10. 在“批量筛选”对话框中，当您确认本次批量操作的规则无误后，单击“确定”。
    进入网络ACL规则列表页面，此时系统会自动勾选待操作的规则。
11. 在网络ACL规则列表上方，单击“删除”。

弹出删除确认对话框。

12. 确认信息无误后，单击“确定”，删除网络ACL规则。

6.3.5 管理网络 ACL 关联的子网

6.3.5.1 将子网关联至网络 ACL

操作场景

您需要将子网关联至网络ACL，并且当网络ACL状态为“已开启”时，网络ACL规则会对出入子网的流量生效。

当您将子网关联至网络ACL时，关联操作会影响子网的网络流量走向，请您谨慎评估后再执行修改，避免对业务造成影响。

约束与限制

- 网络ACL可以同时关联多个子网，但一个子网只能关联一个网络ACL。
- 子网关联网络ACL后，系统自带的默认规则将会拒绝所有出入子网的流量，需要您添加自定义规则放通流量，具体请参见**添加网络ACL规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 您可以通过以下两个操作入口，将子网关联至网络ACL。
   - 入口一：在子网列表中，选择目标子网，并将子网关联至网络ACL。
     i. 在左侧导航栏，选择“子网”。
        进入子网列表页面。
     ii. 在子网列表中，单击目标子网对应的“网络ACL”列下的“去关联”。
        进入关联网络ACL页面。
     iii. 在“网络ACL”参数对应的下拉框中，选择网络ACL。
        如果没有网络ACL，可以单击下拉框中的，新建网络ACL。
     iv. 选择完成后，单击“确定”。
        返回子网列表，可以在子网对应的“网络ACL”列下看到已关联的网络ACL。
   - 入口二：在网络ACL列表中，选择目标网络ACL，为网络ACL关联子网。
     i. 在左侧导航栏，选择“访问控制 > 网络ACL”。
        进入网络ACL列表页面。
     ii. 在网络ACL列表中，单击目标网络ACL所在行的操作列下的“关联子网”。
        进入“关联子网”页签。

iii. 在“关联子网”页签中，单击“关联”。
弹出“关联子网”对话框。
iv. 在“关联子网”对话框的子网列表中，选择目标子网，并单击“确定”。
返回“关联子网”页签的子网列表中，可以看到网络ACL关联的所有子网。

说明

已关联网络ACL的子网将不会展示在“关联子网”对话框的子网列表中，如果您需要将已关联其他网络ACL的子网关联至当前网络ACL，需要先解除子网和其他网络ACL的关联关系，然后再将子网关联至当前网络ACL。

6.3.5.2 将子网和网络 ACL 解除关联

操作场景

您可根据自身网络需求，将子网和网络ACL解除关联。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
4. 您可以通过以下多个操作入口，将子网和网络ACL解除关联。
   - 入口一：在子网列表中，选择目标子网，解除子网和网络ACL的关联关系。
     i. 在左侧导航栏，选择“子网”。
     进入子网列表页面。
     ii. 在子网列表中，单击目标子网对应的名称超链接。
     进入子网详情页面。
     iii. 在子网详情页面的右上方区域，单击网络ACL资源后的“取消关联”。
     弹出取消关联确认对话框。
     iv. 确认无误后，单击“确定”。
     返回子网详情页，可以看到网络ACL区域显示“暂未关联”。
   - 入口二：在子网列表中，选择目标子网，并跳转到关联的网络ACL页面，解除子网和网络ACL的关联关系。
     i. 在左侧导航栏，选择“子网”。
     进入子网列表页面。
     ii. 在子网列表中，单击目标子网对应的“网络ACL”列下的资源超链接。
     进入网络ACL详情页面。
     iii. 选择“关联子网”页签，勾选一个或多个目标子网，单击“取消关联”。
     弹出取消关联确认对话框。

iv. 确认无误后，单击“确定”。

返回“关联子网”页签的子网列表中，已无法看到解除关联网络ACL的子网。

- 入口三：在网络ACL列表中，选择目标网络ACL，解除网络ACL和子网的关联关系。

i. 在左侧导航栏，选择“访问控制 > 网络ACL”。

进入网络ACL列表页面。

ii. 在网络ACL列表中，单击目标网络ACL所在行的操作列下的“关联子网”。

进入“关联子网”页签。

iii. 在“关联子网”页签中，勾选一个或多个目标子网，单击“取消关联”。

弹出取消关联确认对话框。

iv. 确认无误后，单击“确定”。

返回“关联子网”页签的子网列表中，已无法看到解除关联网络ACL的子网。

7 IP 地址组

7.1 IP 地址组概述

IP 地址组

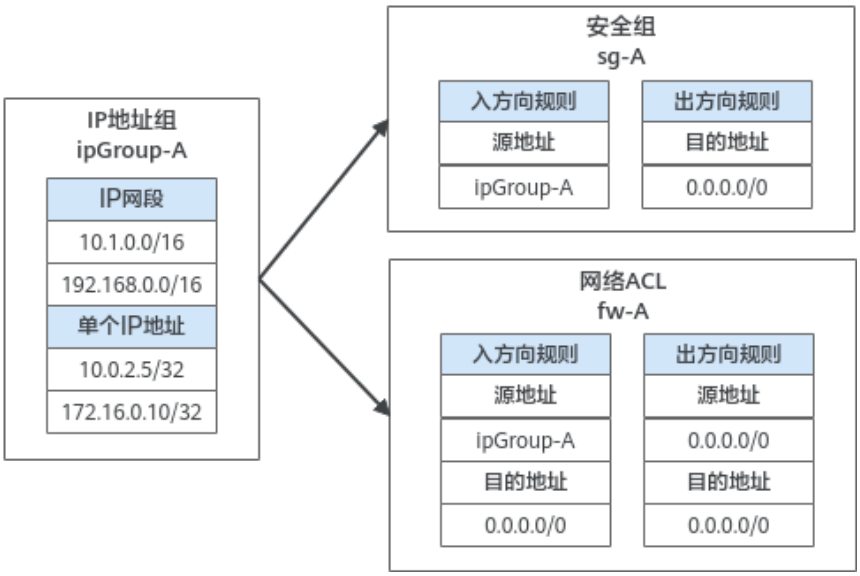
IP地址组是一个或者多个IP地址的集合，可关联至安全组、网络ACL，用于简化网络架构中IP地址的配置和管理。

对于需要统一管理的IP网段、单个IP地址，您可以将其添加到一个IP地址组内。IP地址组无法独立使用，需要将IP地址组关联至对应的资源，可关联IP地址组的资源说明如表7-1所示。

表 7-1 IP 地址组关联资源说明

资源	说明	示例
安全组	添加安全组规则的时候，源地址和目的地址可以选择IP地址组。	如图7-1所示，安全组sg-A的的入方向规则的源地址使用IP地址组ipGroup-A。
网络ACL	添加网络ACL规则的时候，源地址和目的地址可以选择IP地址组。	如图7-1所示，网络ACLfw-A的入方向规则的源地址使用IP地址组ipGroup-A。

图 7-1 IP 地址组使用场景



IP 地址组应用示例

对于安全策略相同的多个IP地址，您可以将其添加到一个IP地址组内统一管理，并在安全组内添加针对该IP地址组的授权规则。当IP地址发生变化时，您只需要在IP地址组内修改IP地址，那么IP地址组对应的安全组规则将会随之变更，无需逐次修改安全组内的规则，降低了安全组管理的难度，提升效率。具体方法，请参见**使用IP地址组提升安全组规则管理效率**。

IP 地址组的使用限制

- 对于关联IP地址组的安全组，其中IP地址组相关的规则对某些类型的云服务器不生效，不支持的规则如下：
  - 通用计算型（S1型、C1型、C2型 ）
  - 内存优化型（M1型）
  - 高性能计算型（H1型）
  - 磁盘增强型（ D1型）
  - GPU加速型（G1型、G2型）
  - 超大内存型（E1型、E2型、ET2型）
- 在网络ACL的规则中使用IP地址组时，有以下限制：
  - 对于入方向规则，源地址和目的地址只能有一方使用IP地址组。
  - 对于出方向规则，源地址和目的地址只能有一方使用IP地址组。

  比如网络ACL入方向规则中的源地址已使用IP地址组，则目的地址只能是IP地址，无法选择IP地址组。

7.2 管理 IP 地址组

7.2.1 创建 IP 地址组

操作场景

本章节指导用户创建IP地址组，IP地址组是一个或者多个IP地址的集合，可关联至安全组、网络ACL中，用于简化网络架构中IP地址的配置和管理。

操作指导

1. 进入**创建IP地址组页面**。
2. 根据界面提示设置IP地址组参数。
   参数详细说明请参见**表7-2**。

表 7-2 IP 地址组参数说明

参数	参数说明	取值样例
区域	必选参数。 不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。 IP地址组只能关联至同区域的资源。	区域A
名称	必选参数。 此处填写IP地址组的名称。 ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 您可以自定义IP地址组名称，IP地址组的唯一性由系统分配的ID号保证。	ipGroup-A
最大条目数	必选参数。 此处设置IP地址组内支持添加的IP地址条目数量，系统默认显示当前支持的最大条目数，您可以自行减少最大条目数。 如果需要提升IP地址组的最大条目数，您需要**提交工单**进行申请。	20
IP类型	必选参数。 此处设置IP地址组内支持的IP类型，具体如下： ● IPv4 ● IPv6	IPv4

参数	参数说明	取值样例
IP地址条目	可选参数。 您可以在IP地址组内添加多个不同格式的IP地址，每个IP地址输入完成后，按回车键换行。 IP地址条目支持的格式为“IP地址 | 描述”，描述为可选参数，其长度范围为0-255个字符，不能包含<>。配置示例如下： • IPv4网段：IP地址/掩码，例如192.168.0.0/16或者192.168.0.0/16 | ECS01 • 单个IPv4地址：IP地址，例如192.168.10.10或者192.168.10.10 | ECS01 • IPv6网段：IP地址/掩码，例如2001:db8:a583:6e::/64或者2001:db8:a583:6e::/64 | ECS01 • 单个IPv6地址：IP地址，例如2001:db8:a583:6e::5c或者2001:db8:a583:6e::5c | ECS01	• 不带IP地址描述：192.168.0.0/16 • 带IP地址描述：192.168.0.0/16 | ECS01
企业项目	必选参数。 创建IP地址组时，可以将IP地址组加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 关于创建和管理企业项目的详情，请参见《企业管理用户指南》。	default
描述	可选参数。 您可以根据需要在文本框中输入IP地址组的描述信息。	-

3. 基本信息设置完成后，单击“立即创建”。
   返回IP地址组列表，创建成功的IP地址组状态为“正常”。

须知

IP地址组无法独立使用，需要将IP地址组关联至对应的资源，具体请参见**将IP地址组关联至资源**。

7.2.2 将 IP 地址组关联至资源

操作场景

IP地址创建完成后无法独立使用，本章节指导用户将IP地址组关联至对应的资源投入使用。

IP地址组可关联至安全组，网络ACL中。

前提条件

- 已创建完成IP地址组，具体请参见**创建IP地址组**。
- 已在IP地址组内添加IP地址条目，具体请参见**在IP地址组内添加IP地址条目**。

操作步骤

您需要将已创建的IP地址组关联至对应的资源投入使用，操作指导如**表7-3**所示。

表 7-3 IP 地址组关联资源指导

资源	说明	操作指导
安全组	添加安全组规则的时候，源地址和目的地址可以选择IP地址组。	**添加安全组规则**： • 添加入方向规则：“源地址”选择IP地址组。 • 添加出方向规则：“目的地址”选择IP地址组。
网络ACL	添加网络ACL规则的时候，源地址和目的地址可以选择IP地址组。	**添加网络ACL规则**： • 添加入方向规则：“源地址”或者“目的地址”选择IP地址组，源地址和目的地址只能有一方使用IP地址组。 • 添加出方向规则：“源地址”或者“目的地址”选择IP地址组，源地址和目的地址只能有一方使用IP地址组。

7.2.3 将 IP 地址组和资源解除关联

操作场景

如果您的IP地址已经不需要使用，本章节指导用户解除IP地址组和资源的关联关系。

IP地址组可关联至安全组，网络ACL中。

约束与限制

解除关联IP地址组后，资源相关的网络规则将会失效，并且无法恢复，请您谨慎操作。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，在目标IP地址组所在行的“关联资源”列下，单击资源超链接。

   进入“关联资源”详情页。
3. 在关联资源列表中，单击对应的资源名称超链接。

   进入资源的详情页，解除IP地址组和资源的关联关系操作指导如**表7-4**所示。

表 7-4 IP 地址组解除关联资源指导

资源	说明	操作指导
安全组	在安全组入方向或者出方向规则中，修改或者删除IP地址组对应的规则。	• **修改安全组规则**： – 入方向规则：修改“源地址”。 – 出方向规则：修改“目的地址”。 • **删除安全组规则**
网络ACL	在网络ACL入方向或者出方向规则中，修改或者删除IP地址组对应的规则。	• **修改网络ACL规则**： – 入方向规则：修改“源地址”或者“目的地址”。 – 出方向规则：修改“源地址”或者“目的地址”。 • **删除网络ACL规则**

7.2.4 修改 IP 地址组基本信息

操作场景

本章节指导用户修改IP地址组的基本信息，包括如下信息：

- IP地址组名称
- IP地址组最大条目数
- IP地址组描述

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。

   进入IP地址组的基本信息页面。
3. 在IP地址组的“基本信息”页签，单击目标参数右侧的  ，根据界面提示修改对应的参数。

   参数详细说明请参见**表7-5**。

表 7-5 IP 地址组参数说明

参数	参数说明	取值样例
名称	必选参数。 此处填写IP地址组的名称。 ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。 您可以自定义IP地址组名称，IP地址组的唯一性由系统分配的ID号保证。	ipGroup-A
最大条目数	必选参数。 此处设置IP地址组内支持添加的IP地址条目数量，系统默认显示当前支持的最大条目数，您可以自行减少最大条目数。 如果需要提升IP地址组的最大条目数，您需要**提交工单**进行申请。	20
描述	可选参数。 您可以根据需要在文本框中输入IP地址组的描述信息。	-

4. 修改完成后，单击 保存修改。

7.2.5 导出 IP 地址组详情

操作场景

本章节指导用户导出IP地址组的详情，包括如下信息：

- IP地址组的基本信息，包括IP地址组的名称、ID、创建时间等。
- IP地址组内添加的IP地址条目。
- IP地址组关联的资源。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表页面，单击列表左上方的“导出”。
   - 导出已选中数据到XLSX：勾选一个或多个IP地址组，导出所选IP地址组的信息。
   - 导出全部数据到XLSX：导出当前区域内所有IP地址组的信息。

   系统会将IP地址组信息自动导出为Excel文件，并下载至本地。

7.2.6 查看 IP 地址组详情

操作场景

本章节指导用户查看IP地址组的详情，包括如下信息：

- IP地址组的基本信息，包括IP地址组的名称、ID、创建时间等。
- IP地址组内添加的IP地址条目。
- IP地址组关联的资源。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。
   进入IP地址组的基本信息页面。
3. 选择不同的页签，查看需要的信息。
   a. 在“基本信息”页签下，查看IP地址组基本信息和IP地址条目。
   b. 在“关联资源”页签下，查看IP地址组已关联的资源。

7.2.7 管理 IP 地址组标签

操作场景

标签用于标识云资源，您可以通过标签实现对IP地址组资源的分类和搜索。您可以参考以下操作管理IP地址组标签：

- 添加IP地址组标签
- 修改IP地址组标签
- 删除IP地址组标签

IP地址组标签规则的详细说明，请参见**表7-6**。

表 7-6 IP 地址组标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	test

参数	规则	样例
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 进入**IP地址组列表页面**。
5. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
6. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

7.2.8 删除 IP 地址组

操作场景

本章节指导用户删除IP地址组。

约束与限制

如果IP地址组已关联至资源，删除IP地址组时，将会同步删除关联资源中使用IP地址组的网络规则，会对网络产生影响，请谨慎操作。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，执行以下操作，删除IP地址组。

- 单个删除：
  i. 在IP地址列表中，单击目标IP地址所在行的删除。
     弹出删除确认对话框。
  ii. 确认无误后，单击“确定”，删除IP地址组。
- 批量删除：
  i. 在IP地址条目列表中，勾选多个目标IP地址组。
  ii. 单击列表左上方的“删除”。
     弹出删除确认对话框。
  iii. 确认无误后，单击“确定”，删除IP地址。
     如果提示存在已关联资源无法删除的IP地址组，请根据界面提示跳转到对应资源的详情页，**将IP地址组和资源解除关联**。

7.3 管理 IP 地址组内的 IP 地址条目

7.3.1 在 IP 地址组内添加 IP 地址条目

操作场景

本章节指导用户在IP地址组内添加IP地址条目。

约束与限制

如果IP地址组已关联至资源，添加IP地址条目后，会对已关联资源的网络产生影响，并且无法恢复，请您谨慎操作。

对安全组和网络ACL来说，IP地址组相关的规则将会发生改变。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。
   进入IP地址组的基本信息页面。
3. 在IP地址条目列表左上方，单击“添加”。
   弹出“添加IP地址条目”对话框。
4. 根据界面提示，在IP地址组内添加IP地址条目。
   - 方法一：
     i. 在“IP地址条目”对话框中输入IP地址，参数详细说明请参见**表7-7**。

表 7-7 IP 地址组参数说明

参数	参数说明	取值样例
名称	IP地址组的名称。	ipGroup-A

参数	参数说明	取值样例
最大条目数	必选参数。 此处设置IP地址组内支持添加的IP地址条目数量，系统默认显示当前支持的最大条目数，您可以自行减少最大条目数。 如果需要提升IP地址组的最大条目数，您需要**提交工单**进行申请。	20
IP类型	IP地址组内支持的IP地址类型，创建IP地址组的时候设置该参数，不支持修改。支持的类型具体如下： • IPv4 • IPv6	IPv4
IP地址条目	必选参数。 您可以在IP地址组内添加多个不同格式的IP地址，每个IP地址输入完成后，按回车键换行。 IP地址条目支持的格式为“IP地址 | 描述”，描述为可选参数，其长度范围为0-255个字符，不能包含<>。配置示例如下： • IPv4网段：IP地址/掩码，例如192.168.0.0/16或者192.168.0.0/16 | ECS01 • 单个IPv4地址：IP地址，例如192.168.10.10或者192.168.10.10 | ECS01 • IPv6网段：IP地址/掩码，例如2001:db8:a583:6e::/64或者2001:db8:a583:6e::/64 | ECS01 • 单个IPv6地址：IP地址，例如2001:db8:a583:6e::5c或者2001:db8:a583:6e::5c | ECS01	• 不带IP地址描述：192.168.0.0/16 • 带IP地址描述：192.168.0.0/16 | ECS01

ii. IP地址条目添加完成后，单击“确定”。

返回IP地址条目列表，可以看到新添加的IP地址。

- 方法二：

单击“IP地址条目”对话框下方的“批量导入”，并在“批量导入IP地址条目”对话框导入IP地址条目，具体请参见**在IP地址组内批量导入IP地址条目**。

7.3.2 在 IP 地址组内修改 IP 地址条目

操作场景

本章节指导用户在IP地址组内修改IP地址条目，包括IP地址的网段以及描述信息。

约束与限制

如果IP地址组已关联至资源，修改IP地址条目的网段后，会对已关联资源的网络产生影响，并且无法恢复，请您谨慎操作。

对安全组和网络ACL来说，IP地址组相关的规则将会发生改变。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。
   进入IP地址组的基本信息页面。
3. 在IP地址条目列表左上方，单击“修改”。
   弹出“修改IP地址条目”对话框。
4. 根据界面提示，修改IP地址条目信息。
   参数详细说明请参见**表7-8**。

表 7-8 修改 IP 地址条目参数说明

参数	参数说明	取值样例
名称	IP地址组的名称。	ipGroup-A
最大条目数	必选参数。 此处设置IP地址组内支持添加的IP地址条目数量，系统默认显示当前支持的最大条目数，您可以自行减少最大条目数。 如果需要提升IP地址组的最大条目数，您需要**提交工单**进行申请。	20
IP类型	IP地址组内支持的IP地址类型，创建IP地址组的时候设置该参数，不支持修改。支持的类型具体如下： • IPv4 • IPv6	IPv4

参数	参数说明	取值样例
IP地址条目	您可以在IP地址组内修改已有的IP地址条目，包括IP地址条目的网段以及描述信息。 IP地址条目支持的格式为“IP地址 | 描述”，描述为可选参数，其长度范围为0-255个字符，不能包含<>。配置示例如下： • IPv4网段：IP地址/掩码，例如192.168.0.0/16或者192.168.0.0/16 | ECS01 • 单个IPv4地址：IP地址，例如192.168.10.10或者192.168.10.10 | ECS01 • IPv6网段：IP地址/掩码，例如2001:db8:a583:6e::/64或者2001:db8:a583:6e::/64 | ECS01 • 单个IPv6地址：IP地址，例如2001:db8:a583:6e::5c或者2001:db8:a583:6e::5c | ECS01	• 不带IP地址描述：192.168.0.0/16 • 带IP地址描述：192.168.0.0/16 | ECS01

5. IP地址条目信息修改完成后，单击“确定”。
   返回IP地址条目列表，可以看到已修改的IP地址条目。

7.3.3 在 IP 地址组内批量导入 IP 地址条目

操作场景

您可以在Excel格式文件中填写IP地址条目的网段和描述信息，并将该信息批量导入至IP地址组，方便您快速添加多个IP地址条目。

约束与限制

- 导入IP地址条目有数量限制，超过数量的条目不允许导入，具体数量请以控制台显示为准。
- 相同的IP地址条目不允许重复导入。包括以下场景：
  - IP地址网段和描述均相同，不能导入。
  - IP地址网段相同，但是描述不同，不能导入。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。
   进入IP地址组的基本信息页面。
3. 在IP地址条目列表左上方，单击“导入”。
   弹出“批量导入IP地址条目”对话框。

4. 单击“下载模板”，将Excel格式的填写模板下载至本地。
5. 在Excel文件中，填写IP地址条目的网段和描述信息，填写完成后保存。
   Excel文件内参数详细说明请参见表7-9。

   表 7-9 导入 IP 地址条目参数说明

参数	参数说明	取值样例
IP地址条目	必选参数。 在“IP地址条目”列中输入IP网段或者单个IP地址，每行填写一个IP地址。支持IP地址格式如下： ● IPv4网段：IP地址/掩码，例如192.168.0.0/16 ● 单个IPv4地址：IP地址，例如192.168.10.10 ● IPv6网段：IP地址/掩码，例如2001:db8:a583:6e::/64 ● 单个IPv6地址：IP地址，例如2001:db8:a583:6e::5c	192.168.0.0/16
描述	可选参数。 在“描述”列中输入IP地址条目的描述信息，其长度范围为0-255个字符，不能包含<>。	ECS01

6. 在“批量导入IP地址条目”对话框中，单击“添加文件”，选择Excel文件，并单击“导入”。
   导入完成后，可在IP地址条目列表中查看新导入的IP地址条目网段和描述信息。

7.3.4 删除 IP 地址组内的 IP 地址条目

操作场景

本章节指导用户在IP地址组内删除IP地址条目。

约束与限制

如果IP地址组已关联至资源，删除IP地址条目后，会对已关联资源的网络产生影响，并且无法恢复，请您谨慎操作。

对安全组和网络ACL来说，IP地址组相关的规则将会发生改变。

操作步骤

1. 进入**IP地址组列表页面**。
2. 在IP地址组列表中，单击目标IP地址组名称超链接。
   进入IP地址组的基本信息页面。

3. 执行以下操作，删除IP地址条目。
   - 单个删除：
     i. 在IP地址条目列表中，单击目标IP地址所在行的删除。
        弹出删除确认对话框。
     ii. 确认无误后，单击“确定”，删除IP地址。
   - 批量删除：
     i. 在IP地址条目列表中，勾选多个目标IP地址。
     ii. 单击列表左上方的“删除”。
        弹出删除确认对话框。
     iii. 确认无误后，单击“确定”，删除IP地址。

7.4 IP 地址组配置示例

7.4.1 使用 IP 地址组提升安全组规则管理效率

应用场景

IP地址组是一个或者多个IP地址的集合，您可以在配置安全组规则的时候使用IP地址组。如果您变更了IP地址组内的IP地址，则相当于直接变更了这些IP地址对应的安全组规则，免去逐条修改安全组规则的工作量。

通常情况下，针对金融，证券等企业，在规划云上组网业务时，对安全性要求较高，实例内的访问控制需要针对IP粒度进行配置。为了既能实现针对IP粒度的精细控制，又能确保安全组规则配置的简洁性，对于安全策略相同的IP网段和IP地址，建议您使用IP地址组降低管理安全组规则的工作量。关于IP地址组的更多信息，请参见**IP地址组简介**。

例如，某企业在云上部署在线办公系统，为企业内不同部门提供服务，并且按照业务安全等级，将实例划分到多个安全组内。这些实例需要被企业内多个部门同时访问，企业内用户IP地址数量众多，且经常会发生变动。

- 不使用IP地址组的情况下，工程师需要在多个安全组内，分别维护针对不同授权对象的多条安全组规则。一旦企业用户的IP地址发生变动，工程师需要逐个调整每个安全组内对应的规则。安全组数量和规则数量越多，管理工作量越大。
- 使用IP地址组的情况下，工程师可以将企业用户的IP地址添加到IP地址组内，并在安全组内添加针对该IP地址组的授权规则。当企业用户的IP地址发生变化时，工程师只需要在IP地址组内修改IP地址，那么IP地址组对应的安全组规则将会随之变更，无需修改每个安全组内的规则，降低了安全组管理的难度，提升效率。

方案架构

本示例中，用户根据不同的安全要求，将实例划分在三个安全组内，同时，这些实例均需要允许特定IP地址访问SSH(22)端口，为了方便维护，采用IP地址组方案。

1. 创建一个IP地址组，并添加待授权的IP地址。
2. 分别在三个安全组入方向中，添加授权IP地址组访问的规则。

表 7-10 安全组入方向规则说明

方向	策略	类型	协议端口	源地址
入方向	允许	IPv4	TCP: 22	IP地址组

3. 如果后续允许访问实例的IP地址有变化，此时需要在IP地址组内修改IP地址条目，对应的安全组规则会自动生效。

约束与限制

对于关联IP地址组的安全组，其中IP地址组相关的规则对某些类型的云服务器不生效，不支持的类型如下：

- 通用计算型（S1型、C1型、C2型 ）
- 内存优化型（M1型）
- 高性能计算型（H1型）
- 磁盘增强型（ D1型）
- GPU加速型（G1型、G2型）
- 超大内存型（E1型、E2型、ET2型）

资源规划

本示例中需要规划的IP地址组和安全组资源需要位于同一个区域内，详细说明如**表7-11**所示。以下资源规划详情仅为示例，您可以根据需要自行修改。

表 7-11 资源规划说明

资源类型	资源数量	说明
IP地址组	1	创建IP地址组，并添加指定IP地址。 ● 名称：ipGroup-A ● 最大条目数：请根据实际情况填写，本示例为20。 ● IP类型：请根据实际情况填写，本示例为IPv4。 ● IP地址条目： – 11.xx.xx.64/32 – 116.xx.xx.252/30 – 113.xx.xx.0/25 – 183.xx.xx.208/28
安全组	3	在3个安全组中，均需要添加授权IP地址组访问的规则，具体如**表7-12**所示。

表 7-12 安全组入方向规则说明

方向	策略	类型	协议端口	源地址
入方向	允许	IPv4	TCP: 22	ipGroup-A

操作步骤

步骤1 创建一个IP地址组，并添加指定IP地址。

具体操作请参见**创建IP地址组**。

步骤2 在3个安全组中，分别添加授权IP地址组访问的规则。

具体操作请参见**添加安全组规则**。

添加完成后，允许来自11.xx.xx.64/32、116.xx.xx.252/30、113.xx.xx.0/25、183.xx.xx.208/28的流量访问安全组内实例的SSH(22)端口，通常用于远程登录Linux云服务器。

步骤3 修改IP地址组内的IP地址条目。

如果添加安全组规则后，又需要为新增的IP地址添加授权规则，此时您需要在IP地址组内增加新的IP地址即可。比如，在IP地址组内增加网段117.xx.xx.0/25后，安全组规则自动生效，允许来自117.xx.xx.0/25的流量访问安全组内实例的SSH(22)端口。

具体操作请参见**管理IP地址组内的IP地址条目**。

----结束

8 对等连接

8.1 对等连接概述

对等连接

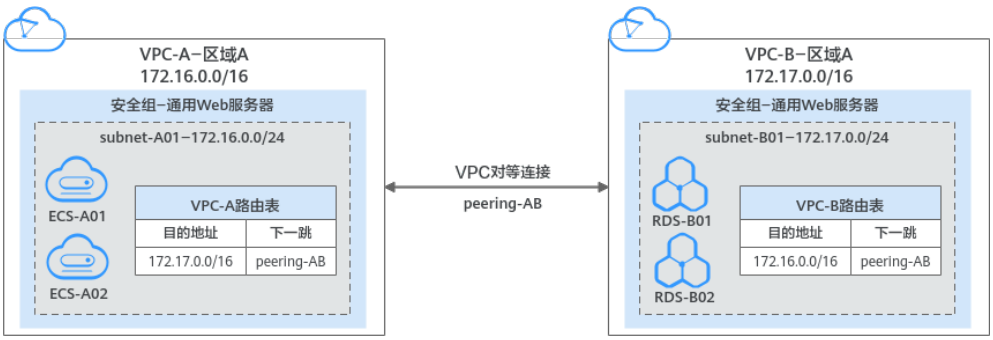
对等连接是建立在两个VPC之间的网络连接，不同VPC之间网络不通，通过对等连接可以实现不同VPC之间的云上内网通信。对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。

- 对等连接用于连通同一个区域的VPC，如果您要连通不同区域的VPC，请使用**云连接**。
- 您可以通过对等连接构建不同的组网，常见的使用示例请参见**对等连接使用示例**。

接下来，通过**图8-1**中简单的组网示例，为您介绍对等连接的使用场景。

- 在区域A内，您的两个VPC分别为VPC-A和VPC-B，VPC-A和VPC-B之间网络不通。
- 您的业务服务器ECS-A01和ECS-A02位于VPC-A内，数据库服务器RDS-B01和RDS-B02位于VPC-B内，此时业务服务器和数据库服务器网络不通。
- 您需要在VPC-A和VPC-B之间建立对等连接Peering-AB，连通VPC-A和VPC-B之间的网络，业务服务器就可以访问数据库服务器。

图 8-1 对等连接组网



须知

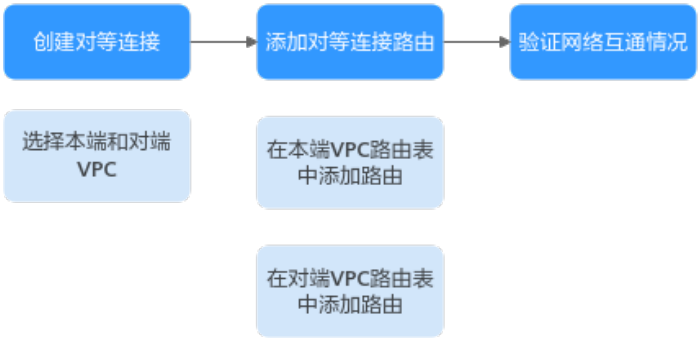
当前VPC对等连接暂不收取您的任何费用。

对等连接创建流程

对等连接可以连通相同账户或者不同账户下的VPC，连通的VPC位于同一个区域即可，创建流程如下：

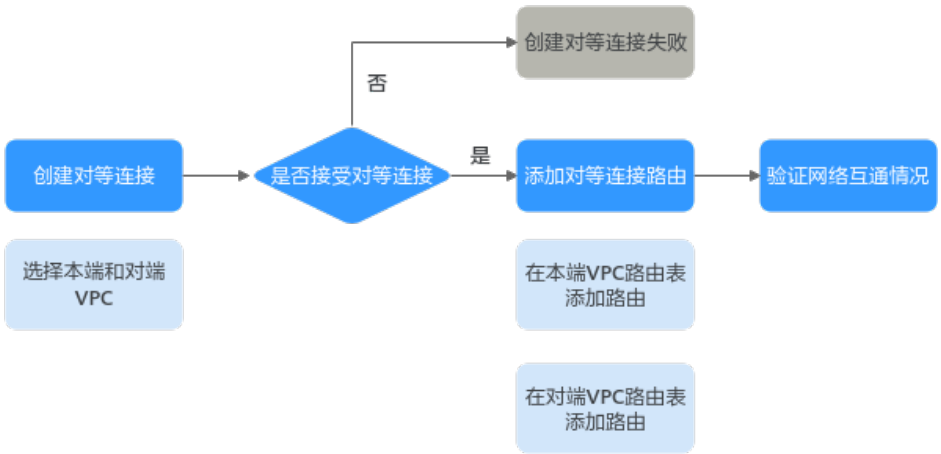
- 相同账户下的VPC对等连接创建流程如图8-2所示。
  创建对等连接的具体操作，请参见**创建相同账户下的对等连接**。

  图 8-2 相同账户下的 VPC 对等连接创建流程



- 不同账户下的VPC对等连接创建流程如图8-3所示。
  创建对等连接的具体操作，请参见**创建不同账户下的对等连接**。
  创建不同账户下的VPC对等连接时，如果在账号A下发起创建对等连接请求，需要账号B接受该请求才可以，如果账号B拒绝，则该对等连接创建失败。

  图 8-3 不同账户下的 VPC 对等连接创建流程



对等连接的使用限制

- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
  - 您可以通过对等连接连通位于华为云中国站和国际站相同区域的VPC，比如VPC-A位于中国站的“中国-香港”区域，VPC-B位于国际站的“中国-香港”区域，可以通过对等连接连通VPC-A和VPC-B。

  - 若要实现不同区域VPC之间互通，您可以使用云连接，详细内容请参见**跨区域VPC互通**。
  - 若您仅需要不同区域的几台ECS之间互通，您可以**为ECS申请和绑定弹性公网IP**，通过EIP实现ECS外网互通。此场景适用于ECS数量较少的情况。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。

  针对该情况，您可以参考**对等连接使用示例**进行相关组网配置。
- 位于两个边缘小站的不同VPC，无法通过对等连接实现通信。
- VPC-A和VPC-B之间创建对等连接，默认情况下，VPC-B不能通过VPC-A的EIP访问公网。您可以使用NAT网关服务或配置SNAT服务器，使得VPC-B下的弹性云服务器可以通过VPC-A下绑定了EIP的弹性云服务器访问Internet。具体实现方式请参见**无公网IP的弹性云服务器访问Internet**。

8.2 对等连接配置示例

8.2.1 对等连接配置示例概述

对等连接是建立在相同区域内，两个VPC之间的网络连接，可以实现多个VPC之间的互通，本文为您详细介绍对等连接常见使用示例，具体如**表8-1**所示。

表 8-1 常见对等连接使用示例

VPC位置	VPC网段	对等连接说明	配置示例
同区域VPC	• VPC网段：两端VPC网段不重叠 • 子网网段：两端VPC的子网网段不重叠	您可以创建整个VPC网段之间的对等连接，VPC内的所有资源可以通过该对等连接实现网络通信。	**连通整个VPC网络的对等连接配置示例**
同区域VPC	• VPC网段：两端VPC网段重叠 • 子网网段：两端VPC的部分子网网段重叠	VPC网段重叠时，您无法创建整个VPC网段之间的对等连接，此时建议您根据业务情况，创建如下对等连接： • VPC子网之间的对等连接：指定子网之间网络互通，对等连接两端的子网网段不能重叠。 • VPC内ECS之间的对等连接：指定ECS之间网络互通，对等连接两端的ECS的私有IP地址不能相同。	**连通VPC子网网络的对等连接配置示例** **连通VPC内ECS网络的对等连接配置示例**

VPC位置	VPC网段	对等连接说明	配置示例
同区域VPC	• VPC网段：两端VPC网段重叠 • 子网网段：两端VPC的全部子网网段重叠	此种场景下，您创建的任何对等连接均是无效的，请重新规划VPC网段。	无效的VPC对等连接配置示例

须知

VPC对等连接仅支持连通同区域VPC，如果您的VPC位于不同的区域，则请您使用云连接。

除了VPC对等连接，您还可以使用企业路由器连通同区域的VPC网络，企业路由器更适用于多VPC的复杂组网，构建的网络拓扑更简洁且扩展性高。

在一个VPC内的所有路由表中，最多可容纳1000条路由。如果您要建立多个VPC之间的对等连接，规划组网时，请务必考虑该限制。

8.2.2 连通整个 VPC 网络的对等连接配置示例

您可以参考以下示例，配置连通整个VPC网络的对等连接，在VPC路由表中添加的路由目的地址为对端VPC网段，此时通过对等连接可以连通整个VPC内的所有资源，示例场景如表8-2所示。

表 8-2 指向整个 VPC 网段的对等连接场景说明

组网示例	推荐场景	IP类型	配置示例
相互对等的两个VPC	当您需要两个VPC之间彼此资源互访时，可以参考本示例规划组网。 比如，人力资源部门使用VPC-A，财务部门使用VPC-B，需要这两个VPC之间资源无限制互访。	IPv4	配置相互对等的两个VPC (IPv4)
		IPv6	配置相互对等的两个VPC (IPv6)
相互对等的多个VPC	当您需要多个VPC之间彼此资源互访时，可以参考本示例规划组网。 比如，人力资源部门使用VPC-A，财务部门使用VPC-B，市场部门使用VPC-C，需要多个VPC之间资源无限制互访	IPv4	配置相互对等的多个VPC (IPv4)
		IPv4	基于对等连接的传递性配置相互对等的多个VPC(IPv4)
		IPv6	配置相互对等的多个VPC (IPv6)

组网示例	推荐场景	IP类型	配置示例
一个中心VPC与两个VPC对等	当您需要一个中心VPC和其他两个VPC之间资源互访时，要求其他两个VPC可以访问中心VPC的所有资源，但彼此之间隔离时，可以参考本示例规划组网。 比如，您的中心VPC-A上部署有公共服务（例如数据库），VPC-B和VPC-C均需要访问该数据库，但是VPC-B和VPC-C之间无需资源互访。	IPv4	**配置一个中心VPC与两个VPC对等（IPv4）**
		IPv6	**配置一个中心VPC与两个VPC对等（IPv6）**
一个中心VPC的主网段和扩展网段与两个VPC对等	本示例与上述示例类似，只是中心VPC存在主网段和扩展网段。	IPv4	**配置一个中心VPC的主网段和扩展网段与两个VPC对等（IPv4）**
一个中心VPC与多个VPC对等	当您需要一个中心VPC和其他多个VPC之间资源互访时，要求其他多个VPC可以访问中心VPC的所有资源，但彼此之间隔离时，可以参考本示例规划组网。 比如，您的中心VPC-A上部署有公共服务（例如数据库），VPC-B、VPC-C、VPC-D、VPC-E、VPC-F以及VPC-G均需要访问该数据库，但是这些VPC之间无需资源互访。	IPv4	**配置一个中心VPC与多个VPC对等（IPv4）**
		IPv6	**配置一个中心VPC与多个VPC对等（IPv6）**

约束与限制

配置指向整个VPC网段的对等连接时，相互对等的VPC网段不能重叠，否则会导致对等连接不生效，详细示例请参见**VPC网段重叠可能导致对等连接不生效**。

即使您的VPC对等连接仅用于IPv6通信，VPC的IPv4网段也不能重叠。本章节所有示例中，对等连接两端VPC的IPv4网段均不重叠。

配置相互对等的两个 VPC（IPv4）

本示例中，在VPC-A和VPC-B之间创建对等连接Peering-AB，VPC-A和VPC-B的网段不能重叠。

- 资源规划详情，请参见**表8-3**。
- 对等连接关系，请参见**表8-4**。

图 8-4 相互对等的两个 VPC(IPv4)

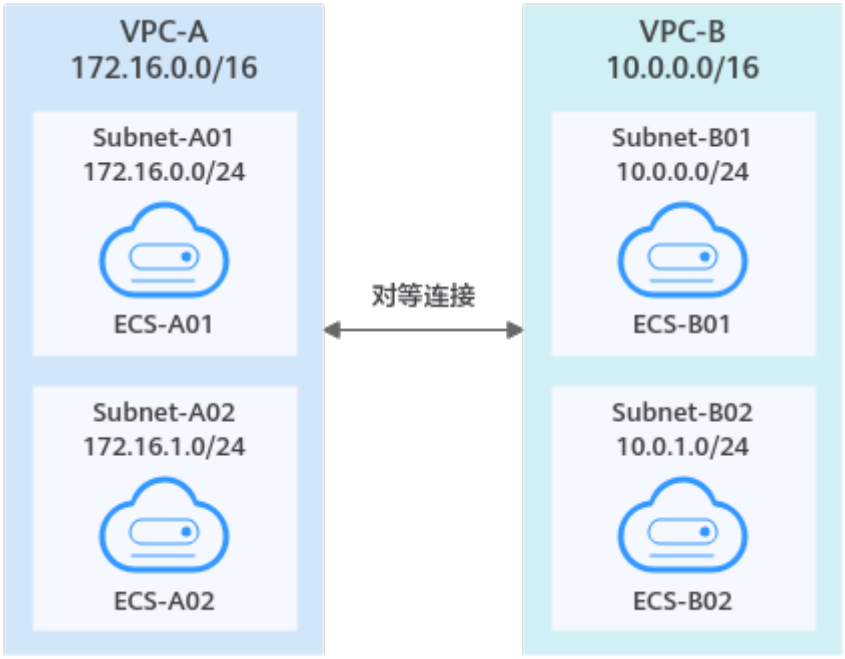


表 8-3 资源规划详情-相互对等的两个 VPC(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167

表 8-4 对等连接关系说明-相互对等的两个 VPC(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-5 VPC 路由表配置说明-相互对等的两个 VPC(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

配置相互对等的两个 VPC（IPv6）

本示例中，在VPC-A和VPC-B之间创建对等连接Peering-AB，VPC-A和VPC-B内的子网都具有IPv6网段，并且IPv4网段不能重叠。

- 资源规划详情，请参见**表8-6**。
- 对等连接关系，请参见**表8-7**。

图 8-5 相互对等的两个 VPC(IPv6)

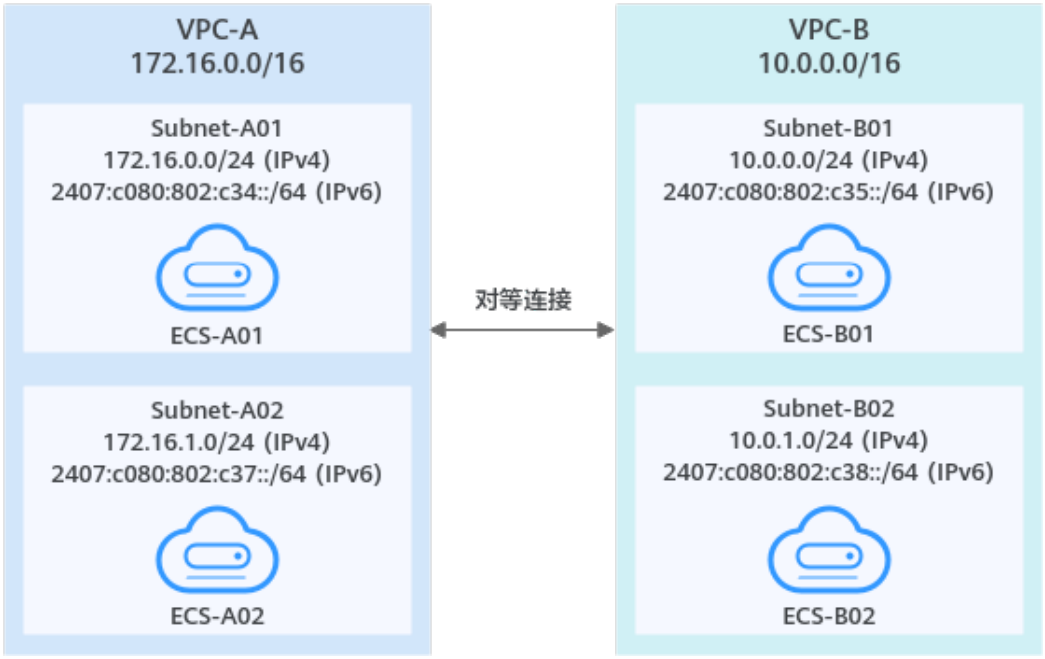


表 8-6 资源规划详情-相互对等的两个 VPC(IPv6)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	• IPv4: 172.16.0.0/24 • IPv6: 2407:c080:802:c34::/64	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	• IPv4: 172.16.0.111 • IPv6: 2407:c080:802:c34:a925:f12e:cfa0:8edb
		Subnet-A02	• IPv4: 172.16.1.0/24 • IPv6: 2407:c080:802:c37::/64	rtb-VPC-A	ECS-A02		• IPv4: 172.16.1.91 • IPv6: 2407:c080:802:c37:594b:4c0f:2fcd:8b72

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-B	10.0.0.0/16	Subnet-B01	• IPv4: 10.0.0.0/24 • IPv6: 2407:c080:802:c35::/64	rtb-VPC-B	ECS-B01		• IPv4: 10.0.0.139 • IPv6: 2407:c080:802:c35:493:33f4:4531:5162
		Subnet-B02	• IPv4: 10.0.1.0/24 • IPv6: 2407:c080:802:c38::/64	rtb-VPC-B	ECS-B02		• IPv4: 10.0.1.167 • IPv6: 2407:c080:802:c38:b9a9:aa03:2700:c1cf

表 8-7 对等连接关系说明-相互对等的两个 VPC(IPv6)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-8 VPC 路由表配置说明-相互对等的两个 VPC(IPv6)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c37::/64	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-B01和Subnet-B02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c38::/64 (Subnet-B02)	Peering-AB	自定义	
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c35::/64	Local	系统路由	
	10.0.1.0/24	Local	系统路由	
	2407:c080:802:c38::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AB	自定义	

说明

当前支持通过管理控制台获取VPC子网的IPv6地址，为了实现整个VPC资源互访，此处您需要逐次添加VPC内所有子网的IPv6网段。

配置相互对等的多个 VPC（IPv4）

本示例中，为了实现多个VPC通信，您需要在每个VPC之间两两建立对等连接，并且VPC-A、VPC-B和VPC-C的网段不能重叠。

- 资源规划详情，请参见**表8-9**。
- 对等连接关系，请参见**表8-10**。

图 8-6 相互对等的多个 VPC(IPv4)

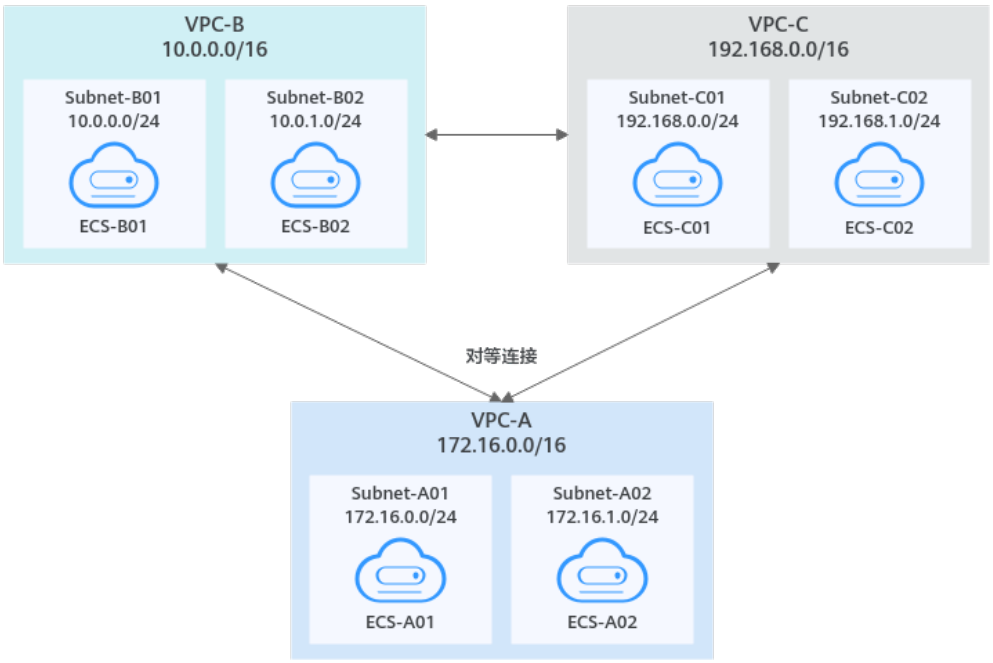


表 8-9 资源规划详情-相互对等的多个 VPC(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167
VPC-C	192.168.0.0/16	Subnet-C01	192.168.0.0/24	rtb-VPC-C	ECS-C01		192.168.0.194
		Subnet-C02	192.168.1.0/24	rtb-VPC-C	ECS-C02		192.168.1.200

表 8-10 对等连接关系说明-相互对等的多个 VPC(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C
VPC-B和VPC-C对等	Peering-BC	VPC-B	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-11 VPC 路由表配置说明-相互对等的多个 VPC(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-BC	自定义	在VPC-B的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-BC的路由。
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	192.168.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。

路由表	目的地址	下一跳	路由类型	路由说明
	10.0.0.0/16 (VPC-B)	Peering-BC	自定义	在VPC-C的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-BC的路由。

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

基于对等连接的传递性配置相互对等的多个 VPC(IPv4)

对等连接具有传递性，如图8-7所示，在VPC-A和VPC-B、VPC-A和VPC-C之间创建对等连接，如果还需要实现VPC-B和VP-C之间的通信，您可以通过以下两种方案实现：

- 建立VPC-B和VPC-C之间的对等连接，具体配置请参见**配置相互对等的多个VPC (IPv4)**。
- 通过路由配置，可以基于VPC-A实现VPC-B和VPC-C之间的流量转发，具体请参见**表8-14**

图 8-7 对等连接具有传递性

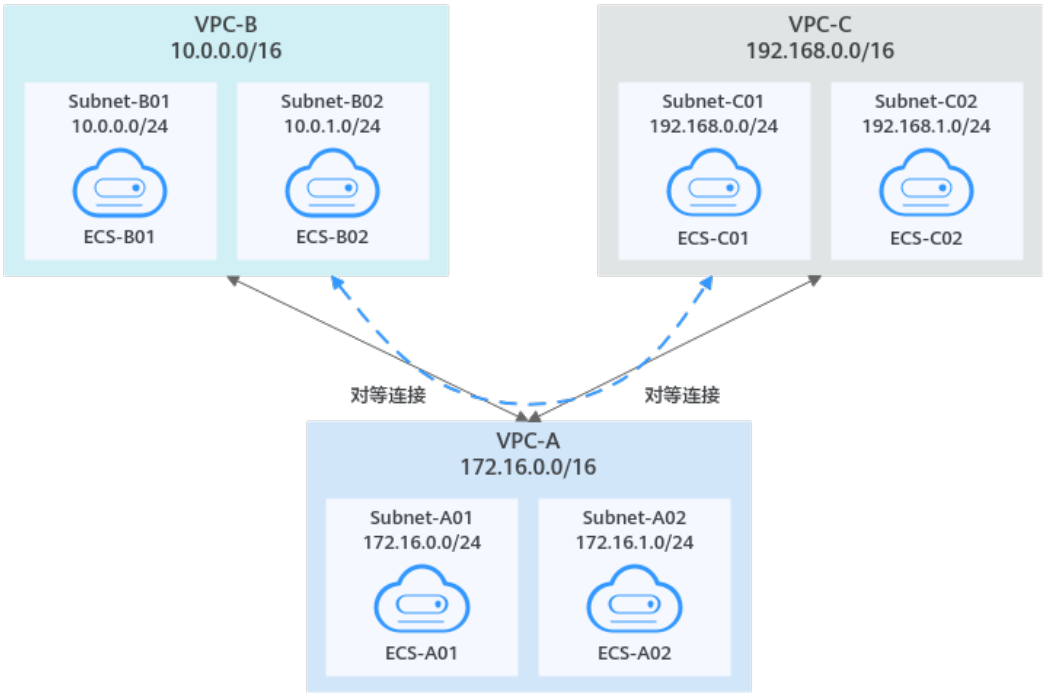


表 8-12 资源规划详情-基于对等连接的传递性配置相互对等的多个 VPC(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167
VPC-C	192.168.0.0/16	Subnet-C01	192.168.0.0/24	rtb-VPC-C	ECS-C01		192.168.0.194
		Subnet-C02	192.168.1.0/24	rtb-VPC-C	ECS-C02		192.168.1.200

表 8-13 对等连接关系说明-基于对等连接的传递性配置相互对等的多个 VPC(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-14 VPC 路由表配置说明-基于对等连接的传递性配置相互对等的多个 VPC(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。

路由表	目的地址	下一跳	路由类型	路由说明
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	192.168.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。
	10.0.0.0/16 (VPC-B)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AC的路由。

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

配置相互对等的多个 VPC（IPv6）

本示例中，为了实现多个VPC通信，您需要在每个VPC之间两两建立对等连接，VPC-A、VPC-B和VPC-C内的子网都具有IPv6网段，并且VPC-A、VPC-B和VPC-C的IPv4网段不能重叠。

- 资源规划详情，请参见**表8-15**。
- 对等连接关系，请参见**表8-16**。

图 8-8 相互对等的多个 VPC(IPv6)

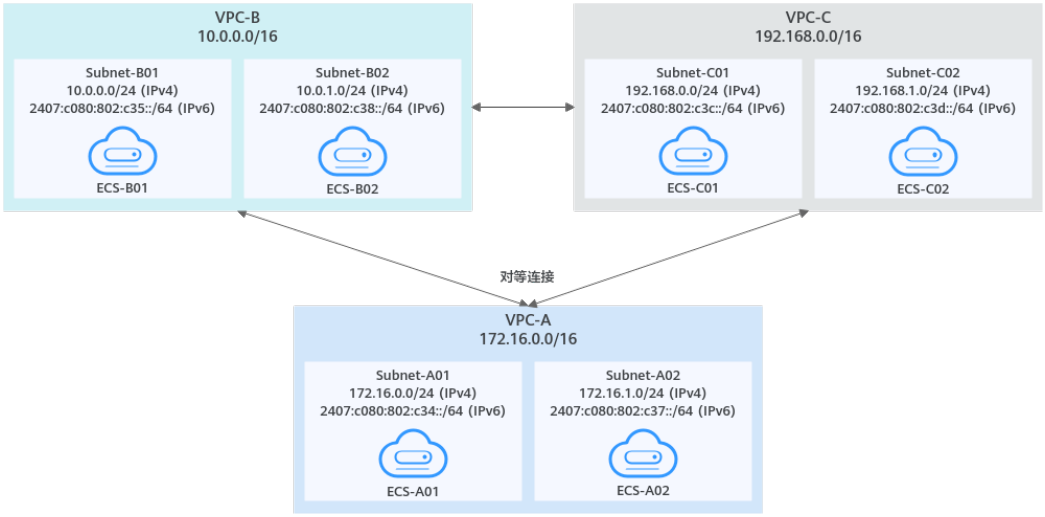


表 8-15 资源规划详情-相互对等的多个 VPC(IPv6)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	• IPv4: 172.16.0.0/24 • IPv6: 2407:c080:802:c34::/64	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	• IPv4: 172.16.0.111 • IPv6: 2407:c080:802:c34:a925:f12e:cfa0:8edb
		Subnet-A02	• IPv4: 172.16.1.0/24 • IPv6: 2407:c080:802:c37::/64	rtb-VPC-A	ECS-A02		• IPv4: 172.16.1.91 • IPv6: 2407:c080:802:c37:594b:4c0f:2fcd:8b72

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-B	10.0.0.0/16	Subnet-B01	• IPv4: 10.0.0.0/24 • IPv6: 2407:c080:802:c35::/64	rtb-VPC-B	ECS-B01		• IPv4: 10.0.0.139 • IPv6: 2407:c080:802:c35:493:33f4:4531:5162
		Subnet-B02	• IPv4: 10.0.1.0/24 • IPv6: 2407:c080:802:c38::/64	rtb-VPC-B	ECS-B02		• IPv4: 10.0.1.167 • IPv6: 2407:c080:802:c38:b9a9:aa03:2700:c1cf
VPC-C	192.168.0.0/16	Subnet-C01	• IPv4: 192.168.0.0/24 • IPv6: 2407:c080:802:c3c::/64	rtb-VPC-C	ECS-C01		• IPv4: 192.168.0.194 • IPv6: 2407:c080:802:c3c:d2f3:d891:24f5:f4af
		Subnet-C02	• IPv4: 192.168.1.0/24 • IPv6: 2407:c080:802:c3d::/64	rtb-VPC-C	ECS-C02		• IPv4: 192.168.1.200 • IPv6: 2407:c080:802:c3d:e9ca:169a:390c:74d1

表 8-16 对等连接关系说明-相互对等的多个 VPC(IPv6)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C
VPC-B和VPC-C对等	Peering-BC	VPC-B	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-17 VPC 路由表配置说明-相互对等的多个 VPC(IPv6)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	
	2407:c080:802:c37::/64	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-B01和Subnet-B02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c38::/64 (Subnet-B02)	Peering-AB	自定义	
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由，用于IPv4通信。
	2407:c080:802:c3c::/64 (Subnet-C01)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-C01和Subnet-C02的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	2407:c080:802:c3d::/64 (Subnet-C02)	Peering-AC	自定义	

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c35::/64	Local	系统路由	
	10.0.1.0/24	Local	系统路由	
	2407:c080:802:c38::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AB	自定义	
	192.168.0.0/16 (VPC-C)	Peering-BC	自定义	在VPC-B的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-BC的路由，用于IPv4通信。
	2407:c080:802:c3c::/64 (Subnet-C01)	Peering-BC	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-C01和Subnet-C02网段的IPv6，下一跳指向Peering-BC的路由，用于IPv6通信。
	2407:c080:802:c3d::/64 (Subnet-C02)	Peering-BC	自定义	
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c3c::/64	Local	系统路由	
	192.168.1.0/24	Local	系统路由	
	2407:c080:802:c3d::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由，用于IPv4通信。

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AC	自定义	
	10.0.0.0/16 (VPC-B)	Peering-BC	自定义	在VPC-C的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-BC的路由，用于IPv4通信。
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-BC	自定义	在VPC-C的路由表中，添加目的地址为子网Subnet-B01和Subnet-B02的IPv6网段，下一跳指向Peering-BC的路由，用于IPv6通信。
	2407:c080:802:c38::/64 (Subnet-B02)	Peering-BC	自定义	

说明

当前支持通过管理控制台获取VPC子网的IPv6地址，为了实现整个VPC资源互访，此处您需要逐次添加VPC内所有子网的IPv6网段。

配置一个中心 VPC 与两个 VPC 对等（IPv4）

本示例中，在VPC-A和VPC-B之间创建对等连接Peering-AB，在VPC-A和VPC-C之间创建对等连接Peering-AC，并且VPC-A、VPC-B和VPC-C的网段不能重叠。

- 资源规划详情，请参见**表8-18**。
- 对等连接关系，请参见**表8-19**。

图 8-9 一个中心 VPC 与两个 VPC 对等(IPv4)

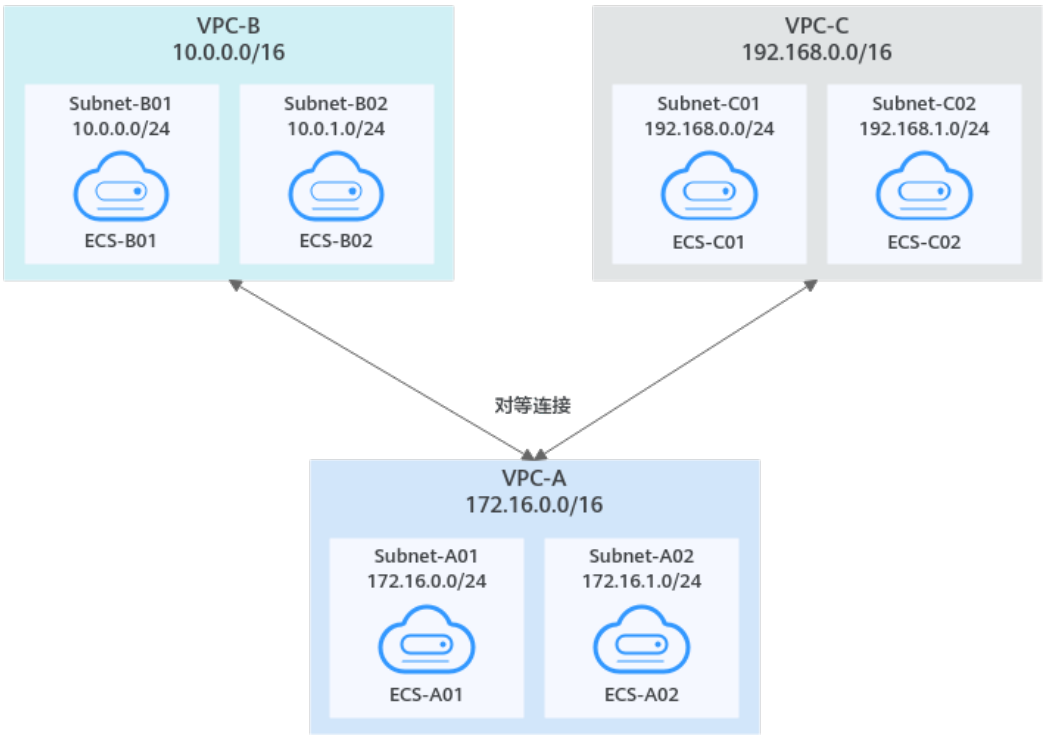


表 8-18 资源规划详情-一个中心 VPC 与两个 VPC 对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167
VPC-C	192.168.0.0/16	Subnet-C01	192.168.0.0/24	rtb-VPC-C	ECS-C01		192.168.0.194
		Subnet-C02	192.168.1.0/24	rtb-VPC-C	ECS-C02		192.168.1.200

表 8-19 对等连接关系说明-一个中心 VPC 与两个 VPC 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-20 VPC 路由表配置说明-一个中心 VPC 与两个 VPC 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	192.168.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

配置一个中心 VPC 与两个 VPC 对等（IPv6）

本示例中，在VPC-A和VPC-B之间创建对等连接Peering-AB，在VPC-A和VPC-C之间创建对等连接Peering-AC。VPC-A、VPC-B和VPC-C内的子网都具有IPv6网段，并且VPC-A、VPC-B和VPC-C的IPv4网段不能重叠。

- 资源规划详情，请参见表8-21。
- 对等连接关系，请参见表8-22。

图 8-10 一个中心 VPC 与两个 VPC 对等(IPv6)

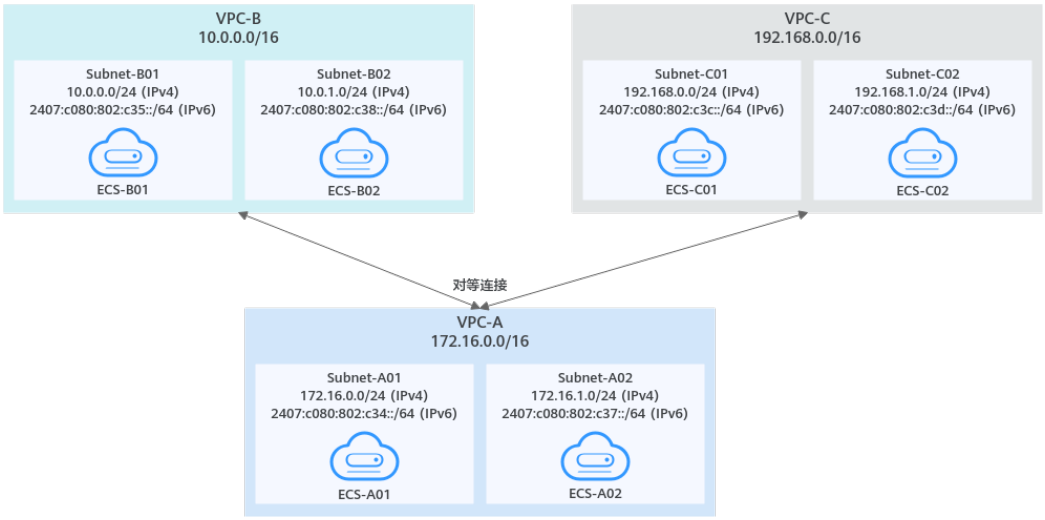


表 8-21 资源规划详情-一个中心 VPC 与两个 VPC 对等(IPv6)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	• IPv4: 172.16.0.0/24 • IPv6: 2407:c080:802:c34::/64	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	• IPv4: 172.16.0.111 • IPv6: 2407:c080:802:c34:a925:f12e:cfa0:8edb

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
		Subnet-A02	• IPv4: 172.16.1.0/24 • IPv6: 2407:c080:802:c37::/64	rtb-VPC-A	ECS-A02		• IPv4: 172.16.1.91 • IPv6: 2407:c080:802:c37:594b:4c0f:2fcd:8b72
VPC-B	10.0.0.0/16	Subnet-B01	• IPv4: 10.0.0.0/24 • IPv6: 2407:c080:802:c35::/64	rtb-VPC-B	ECS-B01		• IPv4: 10.0.0.139 • IPv6: 2407:c080:802:c35:493:33f4:4531:5162
		Subnet-B02	• IPv4: 10.0.1.0/24 • IPv6: 2407:c080:802:c38::/64	rtb-VPC-B	ECS-B02		• IPv4: 10.0.1.167 • IPv6: 2407:c080:802:c38:b9a9:aa03:2700:c1cf
VPC-C	192.168.0.0/16	Subnet-C01	• IPv4: 192.168.0.0/24 • IPv6: 2407:c080:802:c3c::/64	rtb-VPC-C	ECS-C01		• IPv4: 192.168.0.194 • IPv6: 2407:c080:802:c3c:d2f3:d891:24f5:f4af

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
		Subnet-C02	• IPv4: 192.168.1.0/24 • IPv6: 2407:c080:802:c3d::/64	rtb-VPC-C	ECS-C02		• IPv4: 192.168.1.200 • IPv6: 2407:c080:802:c3d:e9ca:169a:390c:74d1

表 8-22 对等连接关系说明-一个中心 VPC 与两个 VPC 对等(IPv6)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-23 VPC 路由表配置说明-一个中心 VPC 与两个 VPC 对等(IPv6)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	
	2407:c080:802:c37::/64	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由，用于IPv4通信。

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-B01和Subnet-B02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c38::/64 (Subnet-B02)	Peering-AB	自定义	
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由，用于IPv4通信。
	2407:c080:802:c3c::/64 (Subnet-C01)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-C01和Subnet-C02的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	2407:c080:802:c3d::/64 (Subnet-C02)	Peering-AC	自定义	
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c35::/64	Local	系统路由	
	10.0.1.0/24	Local	系统路由	
	2407:c080:802:c38::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AB	自定义	
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c3c::/64	Local	系统路由	
	192.168.1.0/24	Local	系统路由	

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c3d::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AC	自定义	

说明

当前支持通过管理控制台获取VPC子网的IPv6地址，为了实现整个VPC资源互访，此处您需要逐次添加VPC内所有子网的IPv6网段。

配置一个中心 VPC 的主网段和扩展网段与两个 VPC 对等（IPv4）

本示例中，在VPC-A和VPC-B之间创建对等连接Peering-AB，在VPC-A和VPC-C之间创建对等连接Peering-AC，其中VPC-A有主网段和扩展网段，并且VPC-A、VPC-B和VPC-C的网段不能重叠。

- 资源规划详情，请参见**表8-24**。
- 对等连接关系，请参见**表8-25**。

图 8-11 一个中心 VPC 的主网段和扩展网段与两个 VPC 对等(IPv4)

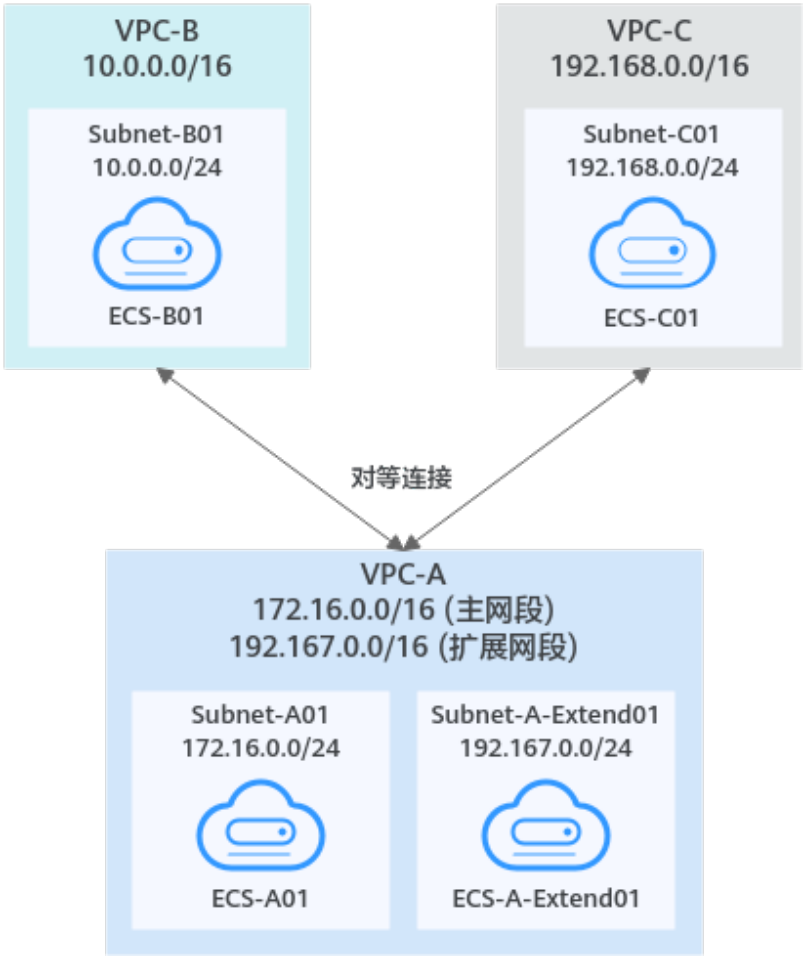


表 8-24 资源规划详情-一个中心 VPC 的主网段和扩展网段与两个 VPC 对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	主网段：172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
	扩展网段：192.167.0.0/16	Subnet-A-Extend01	192.167.0.0/24	rtb-VPC-A	ECS-A-Extend01		192.167.0.100
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-C	192.168.0.0/16	Subnet-C01	192.168.0.0/24	rtb-VPC-C	ECS-C01		192.168.0.194

表 8-25 对等连接关系说明-一个中心 VPC 的主网段和扩展网段与两个 VPC 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-26 VPC 路由表配置说明-一个中心 VPC 的主网段和扩展网段与两个 VPC 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	192.167.0.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A主网段)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A主网段和扩展网段，下一跳指向Peering-AB的路由。
	192.167.0.0/16 (VPC-A扩展网段)	Peering-AB	自定义	

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A主网段)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A主网段和扩展网段，下一跳指向Peering-AC的路由。
	192.167.0.0/16 (VPC-A扩展网段)	Peering-AC	自定义	

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

配置一个中心 VPC 与多个 VPC 对等 (IPv4)

本示例中，在VPC-A和VPC-B、VPC-C、VPC-D、VPC-E、VPC-F以及VPC-G之间创建对等连接，并且VPC-A、VPC-B、VPC-C、VPC-D、VPC-E、VPC-F以及VPC-G的网段不能重叠。

- 资源规划详情，请参见**表8-27**。
- 对等连接关系，请参见**表8-28**。

图 8-12 一个中心 VPC 与多个 VPC 对等(IPv4)

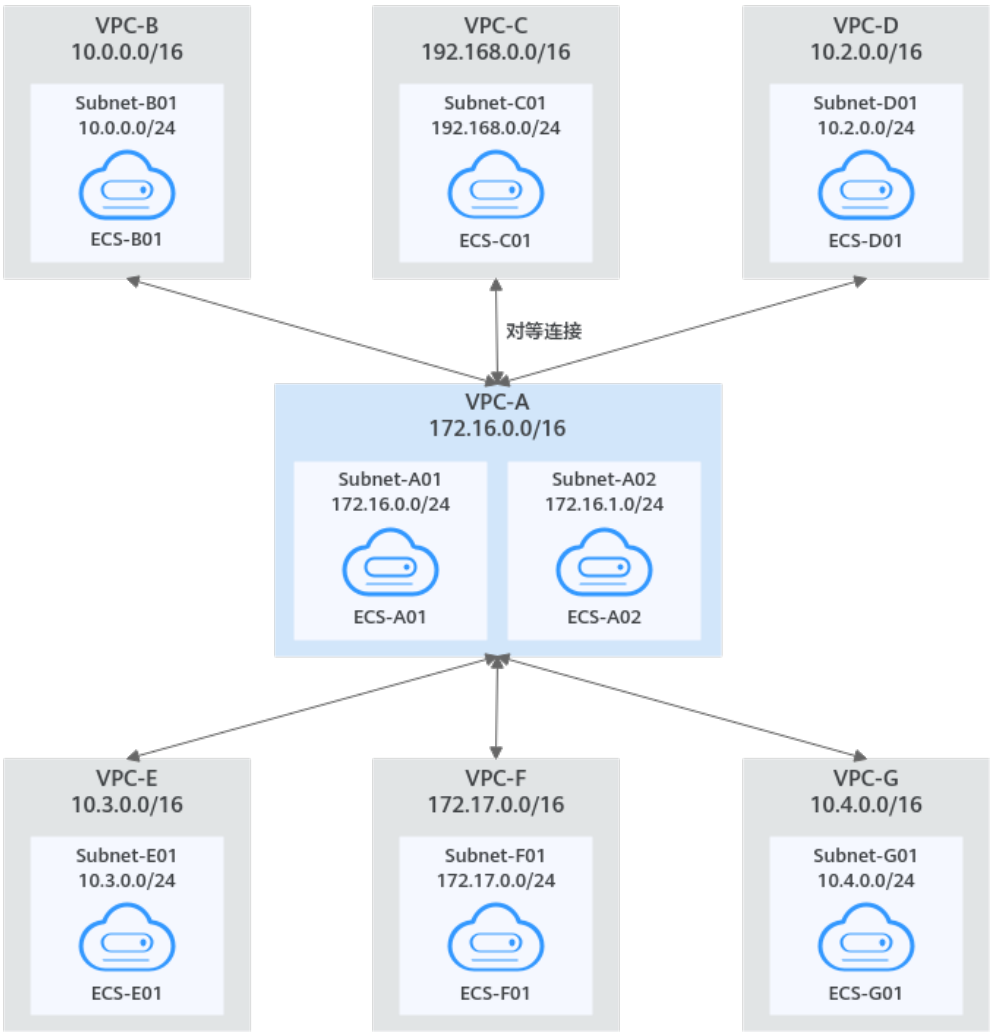


表 8-27 资源规划详情-一个中心 VPC 与多个 VPC 对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
VPC-C	192.168.0.0/16	Subnet-C01	192.168.0.0/24	rtb-VPC-C	ECS-C01		192.168.0.194

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-D	10.2.0.0/16	Subnet-D01	10.2.0.0/24	rtb-VPC-D	ECS-D01		10.2.0.237
VPC-E	10.3.0.0/16	Subnet-E01	10.3.0.0/24	rtb-VPC-E	ECS-E01		10.3.0.87
VPC-F	172.17.0.0/16	Subnet-F01	172.17.0.0/24	rtb-VPC-F	ECS-F01		172.17.0.103
VPC-G	10.4.0.0/16	Subnet-G01	10.4.0.0/24	rtb-VPC-G	ECS-G01		10.4.0.10

表 8-28 对等连接关系说明-一个中心 VPC 与多个 VPC 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C
VPC-A和VPC-D对等	Peering-AD	VPC-A	VPC-D
VPC-A和VPC-E对等	Peering-AE	VPC-A	VPC-E
VPC-A和VPC-F对等	Peering-AF	VPC-A	VPC-F
VPC-A和VPC-G对等	Peering-AG	VPC-A	VPC-G

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-29 VPC 路由表配置说明-一个中心 VPC 与多个 VPC 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
	10.2.0.0/16 (VPC-D)	Peering-AD	自定义	在VPC-A的路由表中，添加目的地址为VPC-D网段，下一跳指向Peering-AD的路由。
	10.3.0.0/16 (VPC-E)	Peering-AE	自定义	在VPC-A的路由表中，添加目的地址为VPC-E网段，下一跳指向Peering-AE的路由。
	172.17.0.0/16 (VPC-F)	Peering-AF	自定义	在VPC-A的路由表中，添加目的地址为VPC-F网段，下一跳指向Peering-AF的路由。
	10.4.0.0/16 (VPC-G)	Peering-AG	自定义	在VPC-A的路由表中，添加目的地址为VPC-G网段，下一跳指向Peering-AG的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。
rtb-VPC-D	10.2.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AD	自定义	在VPC-D的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AD的路由。

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-E	10.3.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AE	自定义	在VPC-E的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AE的路由。
rtb-VPC-F	172.17.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AF	自定义	在VPC-F的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AF的路由。
rtb-VPC-G	10.4.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AG	自定义	在VPC-G的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AG的路由。

说明

路由目的地址配置为对方VPC网段，可以访问对方VPC内的所有资源，VPC网段不能重叠。

配置一个中心 VPC 与多个 VPC 对等（IPv6）

本示例中，在VPC-A和VPC-B、VPC-C、VPC-D、VPC-E、VPC-F以及VPC-G等之间创建对等连接。VPC-A、VPC-B、VPC-C、VPC-D、VPC-E、VPC-F以及VPC-G内的子网都具有IPv6网段，并且这些VPC的IPv4网段不能重叠。

- 资源规划详情，请参见**表8-30**。
- 对等连接关系，请参见**表8-31**。

图 8-13 一个中心 VPC 与多个 VPC 对等(IPv6)

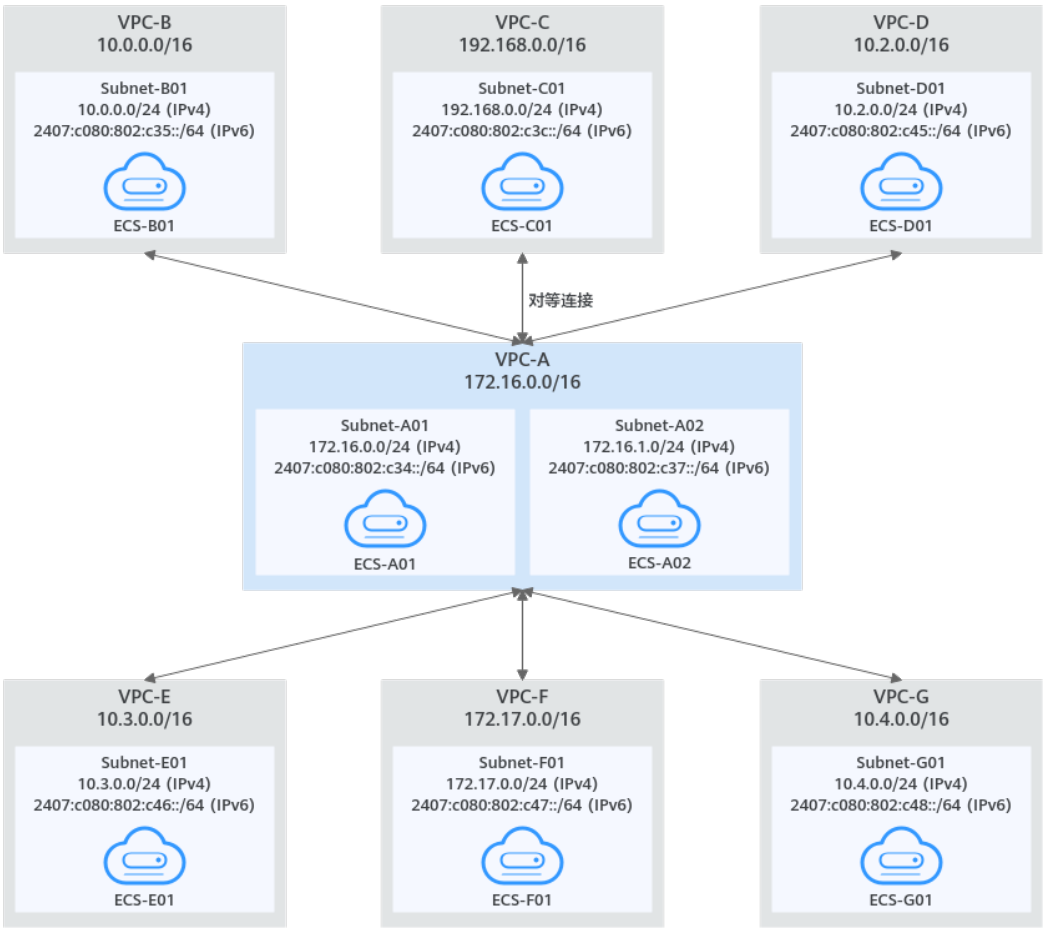


表 8-30 资源规划详情-一个中心 VPC 与多个 VPC 对等(IPv6)

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	• IPv4: 172.16.0.0/24 • IPv6: 2407:c080:802:c34::/64	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	• IPv4: 172.16.0.111 • IPv6: 2407:c080:802:c34:a925:f12e:cfa0:8edb

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
		Subnet-A02	• IPv4: 172.16.1.0/24 • IPv6: 2407:c080:802:c37::/64	rtb-VPC-A	ECS-A02		• IPv4: 172.16.1.91 • IPv6: 2407:c080:802:c37:594b:4c0f:2fcd:8b72
VPC-B	10.0.0.0/16	Subnet-B01	• IPv4: 10.0.0.0/24 • IPv6: 2407:c080:802:c35::/64	rtb-VPC-B	ECS-B01		• IPv4: 10.0.0.139 • IPv6: 2407:c080:802:c35:493:33f4:4531:5162
VPC-C	192.168.0.0/16	Subnet-C01	• IPv4: 192.168.0.0/24 • IPv6: 2407:c080:802:c3c::/64	rtb-VPC-C	ECS-C01		• IPv4: 192.168.0.194 • IPv6: 2407:c080:802:c3c:d2f3:d891:24f5:f4af
VPC-D	10.2.0.0/16	Subnet-D01	• IPv4: 10.2.0.0/24 • IPv6: 2407:c080:802:c45::/64	rtb-VPC-D	ECS-D01		• IPv4: 10.2.0.237 • IPv6: 2407:c080:802:c45:6bb7:f161:3596:6e4c

VPC名称	VPC网段	子网名称	子网网段	子网关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-E	10.3.0.0/16	Subnet-E01	• IPv4: 10.3.0.0/24 • IPv6: 2407:c080:802:c46::/64	rtb-VPC-E	ECS-E01		• IPv4: 10.3.0.87 • IPv6: 2407:c080:802:c46:2a2f:558a:85da:4c70
VPC-F	172.17.0.0/16	Subnet-F01	• IPv4: 172.17.0.0/24 • IPv6: 2407:c080:802:c47::/64	rtb-VPC-F	ECS-F01		• IPv4: 172.17.0.103 • IPv6: 2407:c080:802:c47:b5e2:e6f0:c42b:44fd
VPC-G	10.4.0.0/16	Subnet-G01	• IPv4: 10.4.0.0/24 • IPv6: 2407:c080:802:c48::/64	rtb-VPC-G	ECS-G01		• IPv4: 10.4.0.10 • IPv6: 2407:c080:802:c48:3020:f48c:4e54:aa17

表 8-31 对等连接关系说明-一个中心 VPC 与多个 VPC 对等(IPv6)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-D对等	Peering-AD	VPC-A	VPC-D
VPC-A和VPC-E对等	Peering-AE	VPC-A	VPC-E
VPC-A和VPC-F对等	Peering-AF	VPC-A	VPC-F
VPC-A和VPC-G对等	Peering-AG	VPC-A	VPC-G

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-32 VPC 路由表配置说明-一个中心 VPC 与多个 VPC 对等(IPv6)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	
	2407:c080:802:c37::/64	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-B01的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	192.168.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由，用于IPv4通信。
	2407:c080:802:c3c::/64 (Subnet-C01)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-C01的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	10.2.0.0/16 (VPC-D)	Peering-AD	自定义	在VPC-A的路由表中，添加目的地址为VPC-D网段，下一跳指向Peering-AD的路由，用于IPv4通信。

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c45::/64 (Subnet-D01)	Peering-AD	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-D01的IPv6网段，下一跳指向Peering-AD的路由，用于IPv6通信。
	10.3.0.0/16 (VPC-E)	Peering-AE	自定义	在VPC-A的路由表中，添加目的地址为VPC-E网段，下一跳指向Peering-AE的路由，用于IPv4通信。
	2407:c080:802:c46::/64 (Subnet-E01)	Peering-AE	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-E01的IPv6网段，下一跳指向Peering-AE的路由，用于IPv6通信。
	172.17.0.0/16 (VPC-F)	Peering-AF	自定义	在VPC-A的路由表中，添加目的地址为VPC-F网段，下一跳指向Peering-AF的路由，用于IPv4通信。
	2407:c080:802:c47::/64 (Subnet-F01)	Peering-AF	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-F01的IPv6网段，下一跳指向Peering-AF的路由，用于IPv6通信。
	10.4.0.0/16 (VPC-G)	Peering-AG	自定义	在VPC-A的路由表中，添加目的地址为VPC-G网段，下一跳指向Peering-AG的路由，用于IPv4通信。
	2407:c080:802:c48::/64 (Subnet-G01)	Peering-AG	自定义	在VPC-A的路由表中，添加目的地址为子网Subnet-G01的IPv6网段，下一跳指向Peering-AG的路由，用于IPv6通信。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c35::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AB	自定义	
rtb-VPC-C	192.168.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c3c::/64	Local	系统路由	

路由表	目的地址	下一跳	路由类型	路由说明
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AC的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AC	自定义	
rtb-VPC-D	10.2.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c45::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AD	自定义	在VPC-D的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AD的路由，用于IPv4通信。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AD	自定义	在VPC-D的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AD的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AD	自定义	
rtb-VPC-E	10.3.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c46::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AE	自定义	在VPC-E的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AE的路由。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AE	自定义	在VPC-E的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AE的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AE	自定义	
rtb-VPC-F	172.17.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c47::/64	Local	系统路由	

路由表	目的地址	下一跳	路由类型	路由说明
	172.16.0.0/16 (VPC-A)	Peering-AF	自定义	在VPC-F的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AF的路由。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AF	自定义	在VPC-F的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AF的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AF	自定义	
rtb-VPC-G	10.4.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c48::/64	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AG	自定义	在VPC-G的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AG的路由。
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AG	自定义	在VPC-G的路由表中，添加目的地址为子网Subnet-A01和Subnet-A02的IPv6网段，下一跳指向Peering-AG的路由，用于IPv6通信。
	2407:c080:802:c37::/64 (Subnet-A02)	Peering-AG	自定义	

说明

当前支持通过管理控制台获取VPC子网的IPv6地址，为了实现整个VPC资源互访，此处您需要逐次添加VPC内所有子网的IPv6网段。

8.2.3 连通 VPC 子网网络的对等连接配置示例

您可以参考以下示例，配置连通VPC部分子网网络的对等连接，在VPC路由表中添加的路由目的地址为对端VPC子网网段，此时对等连接两端连通的是VPC内指定子网的资源，示例场景如**表8-33**所示。

表 8-33 指向 VPC 子网的对等连接场景说明

组网示例	场景推荐	IP类型	配置示例
两个VPC与一个中心VPC的两个子网对等	当您需要一个中心VPC和其他多个VPC之间资源互访，中心VPC部署的资源类型不同，要求其他多个VPC只能访问中心VPC的特定资源，且彼此之间隔离，可以参考本示例规划组网。 • 中心VPC具有多个子网，不同子网中部署不同类型的资源。 • 其他VPC根据业务需要访问中心VPC内特定子网的资源。	IPv4	**配置两个VPC与一个中心VPC的两个子网对等（IPv4）**
		IPv6/IPv4	**配置两个VPC与一个中心VPC的两个子网对等（IPv6/IPv4）**
一个中心VPC与两个VPC的特定子网对等	当您需要一个中心VPC和其他多个VPC之间资源互访，中心VPC部署某类公共资源，其他VPC只有特定子网可以访问中心VPC内的资源，且彼此之间隔离，可以参考本示例规划组网。 • 中心VPC部署的公共资源没有分类，其他VPC可以访问中心VPC内的所有资源。 • 其他VPC具有多个子网，根据业务需要指定某个子网访问中心VPC内的资源。	IPv4	**配置一个中心VPC与两个VPC的特定子网对等（IPv4）**
一个中心VPC与两个VPC的重叠子网对等	本示例与上面的场景类似，当其他多个VPC和中心VPC对等的子网网段重叠时，可能会导致流量无法被转发到正确的目的地址，请参考本示例规划组网，避免发生该情况。	IPv4	**配置一个中心VPC与两个VPC的重叠子网对等（IPv4）**

配置两个 VPC 与一个中心 VPC 的两个子网对等（IPv4）

本示例中，中心VPC-A拥有两个子网，并分别关联至不同的路由表。在子网Subnet-A01和VPC-B之间创建对等连接Peering-AB，在子网Subnet-A02和VPC-C之间创建对等连接Peering-AC。此处VPC-B和VPC-C网段重叠，由于VPC-A的两个子网关联至不同的路由表，因此对等连接路由不会冲突。

- 资源规划详情，请参见**表8-34**。
- 对等连接关系，请参见**表8-35**。

图 8-14 两个 VPC 与一个中心 VPC 的两个子网对等(IPv4)

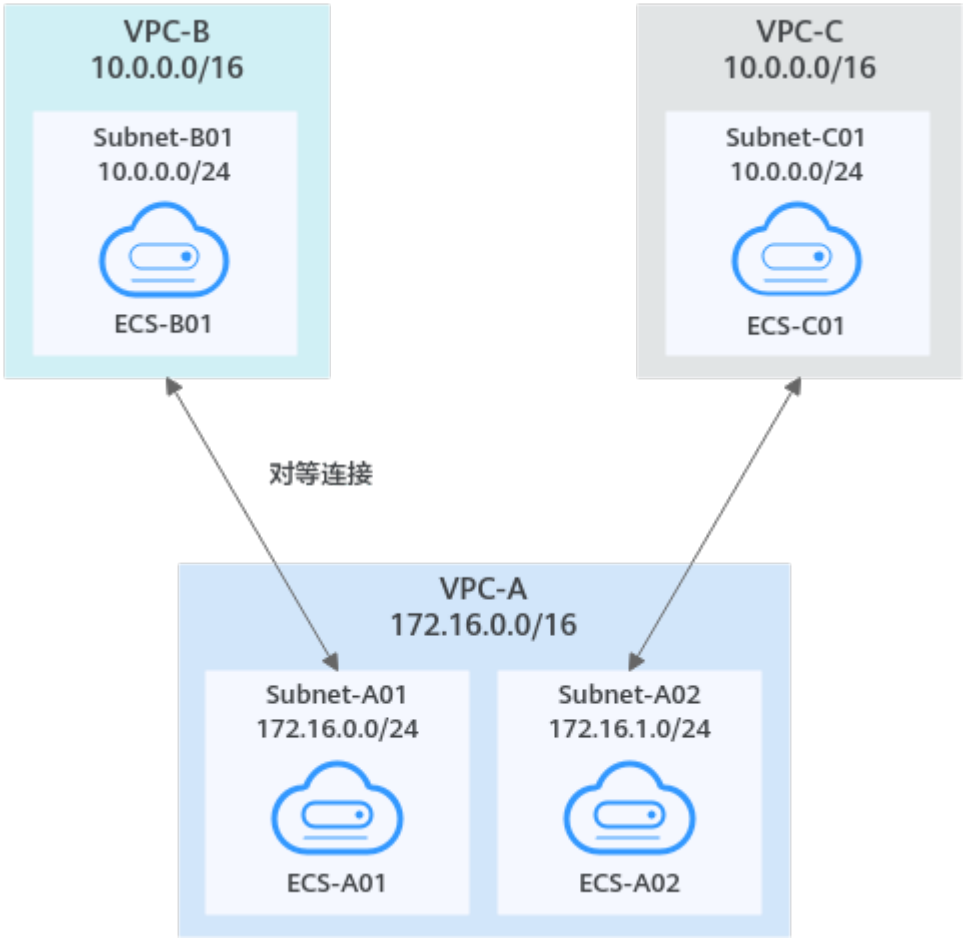


表 8-34 资源规划详情-两个 VPC 与一个中心 VPC 的两个子网对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A01	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A02	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71

说明

VPC-A有两张路由表，分别关联不同的子网，路由表rtb-VPC-A01关联子网Subnet-A01，路由表子网rtb-VPC-A02关联子网Subnet-A02，两个子网间可正常通信。

表 8-35 对等连接关系说明-两个 VPC 与一个中心 VPC 的两个子网对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A的子网Subnet-A01和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A的子网Subnet-A02和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-36 VPC 路由表配置说明-两个 VPC 与一个中心 VPC 的两个子网对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A01	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表rtb-VPC-A01中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
rtb-VPC-A02	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表rtb-VPC-A02中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/24 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为Subnet-A01的网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。

路由表	目的地址	下一跳	路由类型	路由说明
	172.16.1.0/24 (Subnet-A02)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为Subnet-A02的网段，下一跳指向Peering-AC的路由。

配置两个 VPC 与一个中心 VPC 的两个子网对等 (IPv6/IPv4)

本示例中，中心VPC-A拥有两个子网，并分别关联至不同的路由表。在子网Subnet-A01和VPC-B之间创建对等连接Peering-AB，用于IPv6通信。在子网Subnet-A02和VPC-C之间创建对等连接Peering-AC，用于IPv4通信。此处VPC-B和VPC-C网段重叠，由于VPC-A的两个子网关联至不同的路由表，因此对等连接路由不会冲突。

- 资源规划详情，请参见**表8-37**。
- 对等连接关系，请参见**表8-38**。

图 8-15 两个 VPC 与一个中心 VPC 的两个子网对等(IPv6/IPv4)

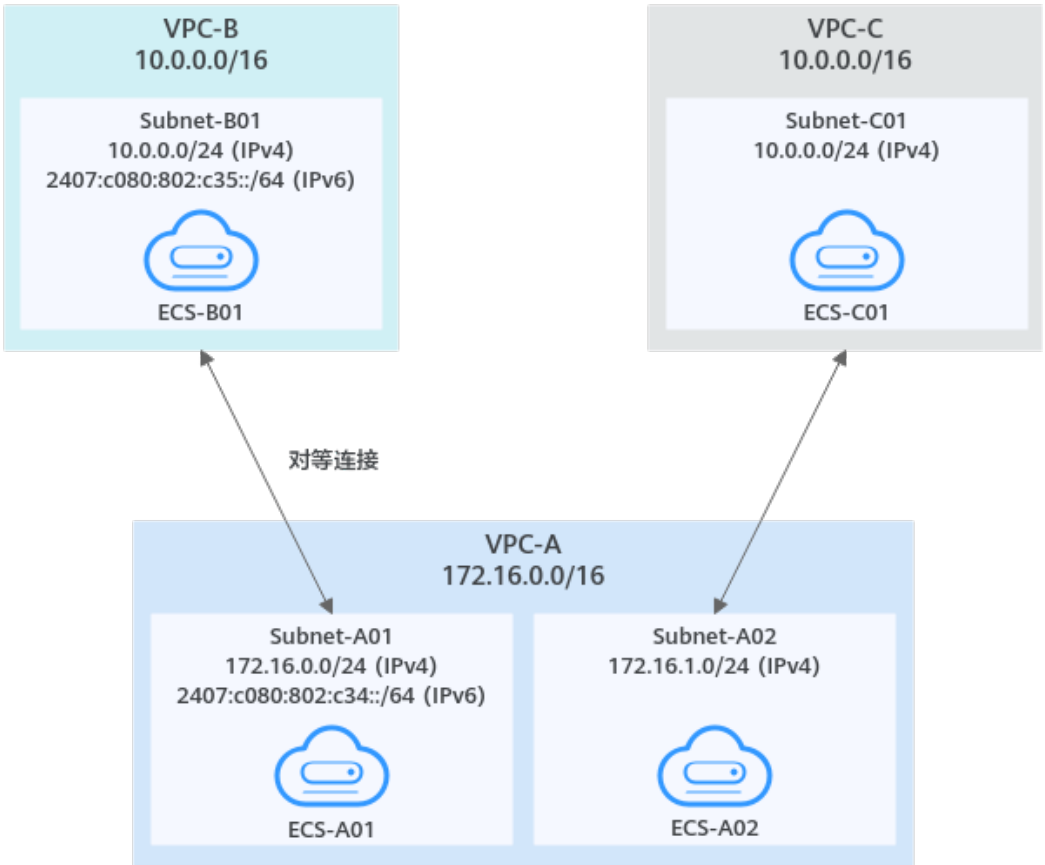


表 8-37 资源规划详情-两个 VPC 与一个中心 VPC 的两个子网对等(IPv6/IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	• IPv4: 172.16.0.0/24 • IPv6: 2407:c080:802:c34::/64	rtb-VPC-A01	ECS-A01	sg-web：通用Web服务器	• IPv4: 172.16.0.111 • IPv6: 2407:c080:802:c34:a925:f12e:cfa0:8edb
		Subnet-A02	172.16.1.0/24	rtb-VPC-A02	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	• IPv4: 10.0.0.0/24 • IPv6: 2407:c080:802:c35::/64	rtb-VPC-B	ECS-B01		• IPv4: 10.0.0.139 • IPv6: 2407:c080:802:c35:493:33f4:4531:5162
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71

说明

VPC-A有两张路由表，分别关联不同的子网，路由表rtb-VPC-A01关联子网Subnet-A01，路由表子网rtb-VPC-A02关联子网Subnet-A02，两个子网间可正常通信。

表 8-38 对等连接关系说明-两个 VPC 与一个中心 VPC 的两个子网对等(IPv6/IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A的子网Subnet-A01和VPC-B对等(IPv6)	Peering-AB	VPC-A	VPC-B

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A的子网Subnet-A02和VPC-C对等(IPv4)	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-39 VPC 路由表配置说明-两个 VPC 与一个中心 VPC 的两个子网对等(IPv6/IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A01	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表rtb-VPC-A01中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由，用于IPv4通信。
	2407:c080:802:c35::/64 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表rtb-VPC-A01中，添加目的地址为子网Subnet-B01的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
rtb-VPC-A02	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c34::/64	Local	系统路由	
	172.16.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表rtb-VPC-A02中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由，用于IPv4通信。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	2407:c080:802:c35::/64	Local	系统路由	
	172.16.0.0/24 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为Subnet-A01的网段，下一跳指向Peering-AB的路由，用于IPv4通信。

路由表	目的地址	下一跳	路由类型	路由说明
	2407:c080:802:c34::/64 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为子网Subnet-A01的IPv6网段，下一跳指向Peering-AB的路由，用于IPv6通信。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24 (Subnet-A02)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为子网Subnet-A02的网段，下一跳指向Peering-AC的路由，用于IPv4通信。

配置一个中心 VPC 与两个 VPC 的特定子网对等（IPv4）

本示例中，在中心VPC-A和Subnet-B01之间创建对等连接Peering-AB，在中心VPC-A和Subnet-C02之间创建对等连接Peering-AC。此处VPC-B和VPC-C的VPC网段重叠，但是Subnet-B01和Subnet-C02子网网段不重叠，不会造成路由冲突。

- 资源规划详情，请参见**表8-40**。
- 对等连接关系，请参见**表8-41**。

图 8-16 一个中心 VPC 与两个 VPC 的特定子网对等(IPv4)

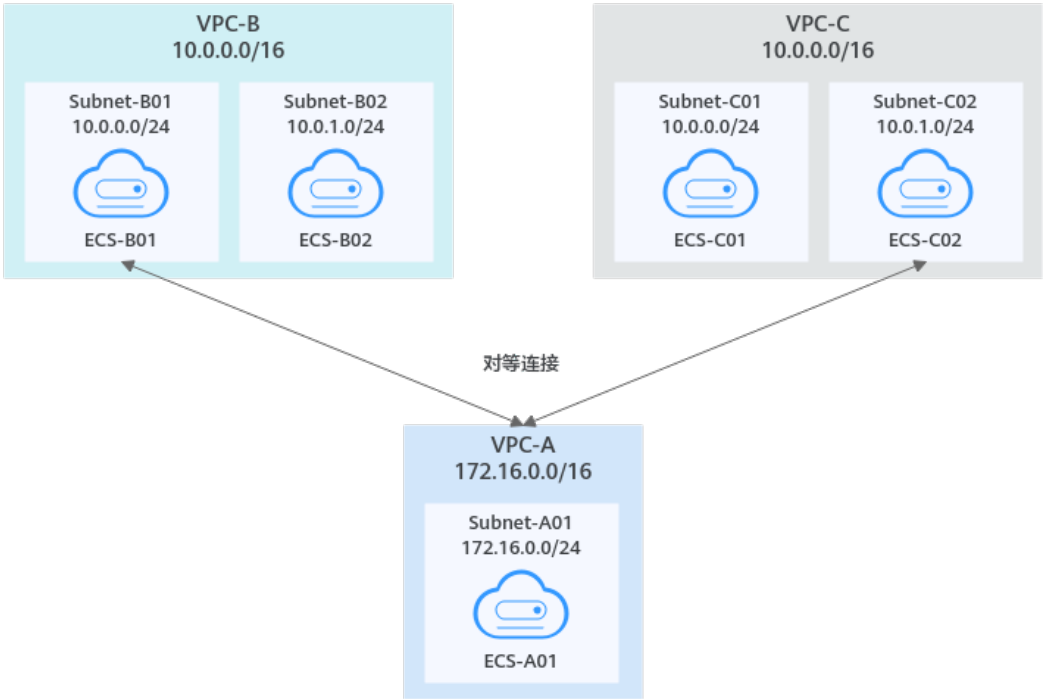


表 8-40 资源规划详情-一个中心 VPC 与两个 VPC 的特定子网对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71
		Subnet-C02	10.0.1.0/24	rtb-VPC-C	ECS-C02		10.0.1.116

表 8-41 对等连接关系说明-一个中心 VPC 与两个 VPC 的特定子网对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B的子网Subnet-B01对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C的子网Subnet-C02对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您需要在本端和对端VPC路由表中，添加以下路由：

表 8-42 VPC 路由表配置说明-一个中心 VPC 与两个 VPC 的特定子网对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.0.0/24 (Subnet-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为Subnet-B01的网段，下一跳指向Peering-AB的路由。
	10.0.1.0/24 (Subnet-C02)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为Subnet-C02的网段，下一跳指向Peering-AC的路由。

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AC的路由。

配置一个中心 VPC 与两个 VPC 的重叠子网对等 (IPv4)

如果同一个VPC要与多个网段重叠的VPC子网创建对等连接，那么配置路由的时候，请确保路由的目的地址不会出现冲突，并且流量可以正确的转发。

在本示例中，在中心VPC-A和Subnet-B02之间创建对等连接Peering-AB，在中心VPC-A和Subnet-C02之间创建对等连接Peering-AC。此处Subnet-B02和Subnet-C02子网网段重叠，并且云服务器ECS-B02私有IP地址和ECS-C02的私有IP地址一样，均为10.0.1.167/32。

- 资源规划详情，请参见**表8-43**。
- 对等连接关系，请参见**表8-44**。

图 8-17 一个中心 VPC 与两个 VPC 的重叠子网对等(IPv4)

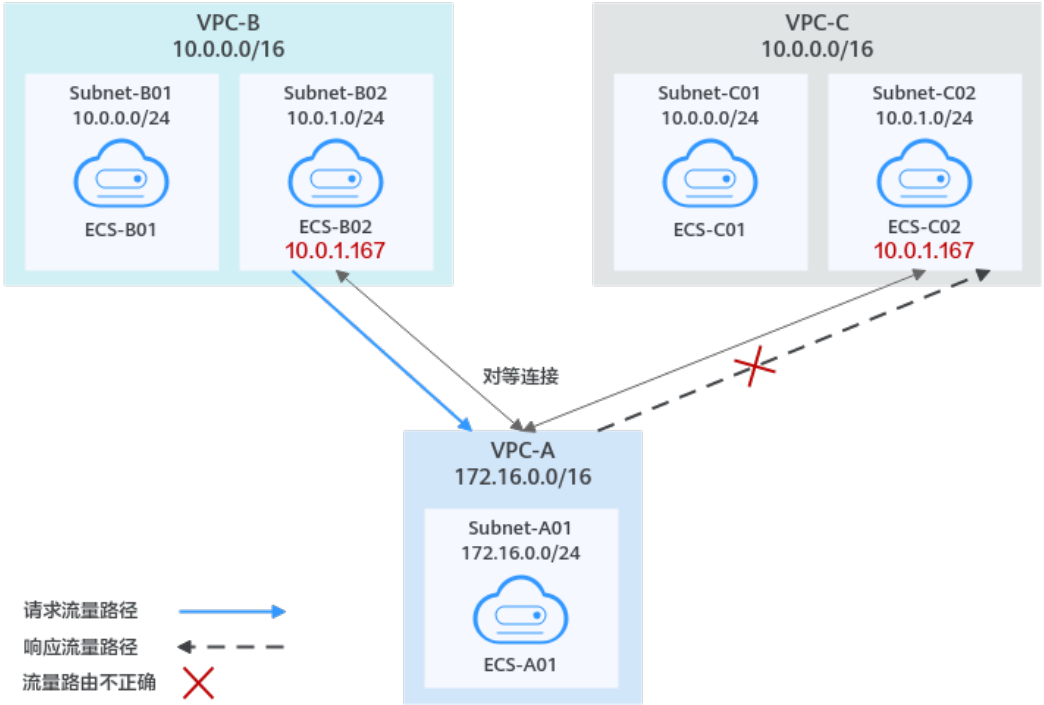


表 8-43 资源规划详情-一个中心 VPC 与两个 VPC 的重叠子网对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
		Subnet-B02	10.0.1.0/24	rtb-VPC-B	ECS-B02		10.0.1.167
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71
		Subnet-C02	10.0.1.0/24	rtb-VPC-C	ECS-C02		10.0.1.167

表 8-44 对等连接关系说明-一个中心 VPC 与两个 VPC 的重叠子网对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B的子网Subnet-B02对等	Peering-AB	VPC-A	VPC-B

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-C的子网Subnet-C02对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您在本端和对端VPC路由表中，如果按照**表8-45**添加路由，那么会导致响应流量无法正确返回，具体说明如下：

1. VPC-B子网Subnet-B02中的云服务器ECS-B02向VPC-A发送请求流量，通过rtb-VPC-B路由表中Peering-AB对应的路由将流量转发到VPC-A。
2. VPC-A收到来自云服务器ECS-B02的请求流量，期望的结果是将响应流量返回到ECS-B02。但是在rtb-VPC-A路由表中，目的地址为10.0.1.167/32时，只能匹配到Peering-AC的路由，因此响应流量被错误的返回到VPC-C。
3. 此时VPC-C的子网Subnet-C02中存在云服务器ECS-C02，与ECS-B02私有IP地址相同，均为10.0.1.167/32，则响应流量最终错误的返回到ECS-C02，ECS-B02无法收到响应流量。

表 8-45 VPC 路由表配置说明-一个中心 VPC 与两个 VPC 的重叠子网对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24 (Subnet-C02)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为Subnet-C02的网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AC的路由。

对于存在重叠子网的情况，为了避免流量被错误转发，我们给您的路由配置建议如下：

- 建议1：在rtb-VPC-A路由表中，添加下一跳为Peering-AB的路由，目的地址为ECS-B02的私有IP地址。这样遵循路由的最长匹配原则，会优先匹配10.0.1.167/32这条路由，确保VPC-A会将响应流量送达ECS-B02。关于更多指向ECS的对等连接配置，请参见**连通VPC内ECS网络的对等连接配置示例**。

表 8-46 VPC 路由表配置-建议 1

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.167/32 (ECS-B02)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为ECS-B02的私有IP地址，下一跳指向Peering-AB的路由。
	10.0.1.0/24 (Subnet-C02)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为Subnet-C02的网段，下一跳指向Peering-AC的路由。

- 建议2：在rtb-VPC-A路由表中，需要将Peering-AC的路由目的地址由Subnet-C02的网段改为Subnet-C01网段。然后添加下一跳为Peering-AB的路由，目的地址为Subnet-B02，确保VPC-A可以将响应流量返回到VPC-B的子网Subnet-B02。

表 8-47 VPC 路由表配置-建议 2

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24 (Subnet-B02)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为Subnet-B02的网段，下一跳指向Peering-AB的路由。
	10.0.0.0/24 (Subnet-C01)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为Subnet-C01的网段，下一跳指向Peering-AC的路由。

8.2.4 连通 VPC 内 ECS 网络的对等连接配置示例

您可以参考以下示例，配置连通VPC内ECS网络的对等连接，在VPC路由表中添加的路由目的地址为ECS的私有IP地址，此时对等连接连通的是不同VPC内的ECS。

当您需要在网段及子网重叠的多个VPC之间创建对等连接时，为了确保路由的正确转发，建议您可以根据组网要求缩小对等连接范围，比如配置不同ECS之间的对等，示例场景如**表8-48**所示。

表 8-48 指向 VPC 内 ECS 的对等连接场景

组网示例	场景推荐	IP类型	配置示例
一个中心VPC的ECS与两个VPC的ECS对等	一个中心VPC和其他两个VPC之间资源互访，其他两个VPC之间隔离。 此场景下，另外两个VPC的网段及子网重叠，此时为了避免中心VPC内的路由冲突，您可以参考本示例，缩小对等连接范围，创建不同VPC内ECS之间的对等连接。	IPv4	**配置一个中心VPC的ECS与两个VPC的ECS对等（IPv4）**
一个中心VPC通过最长匹配原则与两个VPC对等	本示例与上面的场景类似，相比于配置ECS之间的对等连接，您还可以利用路由的最长匹配原则，创建如下两种对等关系： • 在中心VPC和一个VPC的ECS之间创建对等连接 • 在中心VPC和另外一个VPC子网之间创建对等连接 相比ECS对等的组网，该配置方案扩大了对等连接的通信范围。	IPv4	**配置一个中心VPC通过最长匹配原则与两个VPC对等（IPv4）**

配置一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等（IPv4）

如果在一个VPC和其他多个网段重叠的VPC之间创建对等连接，那么配置路由的时候，您可以参考本示例，将路由的目的地址范围缩小，配置成ECS的私有IP地址。路由目的地址规划不当，会导致流量无法正确转发，错误示例及原因详解，可参见**配置一个中心VPC与两个VPC的重叠子网对等（IPv4）**。

在本示例中，在中心VPC-A内ECS-A01-1和VPC-B内ECS-B01之间创建对等连接Peering-AB，在中心VPC-A内ECS-A01-2和VPC-C内ECS-C01之间创建对等连接Peering-AC。由于Subnet-B01和Subnet-C01子网网段重叠，请确保云服务器ECS-B01和ECS-C01的私有IP地址不同，否则会由于目的地址冲突无法在VPC-A的路由表中添加路由。

- 资源规划详情，请参见**表8-49**。
- 对等连接关系，请参见**表8-50**。

图 8-18 一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

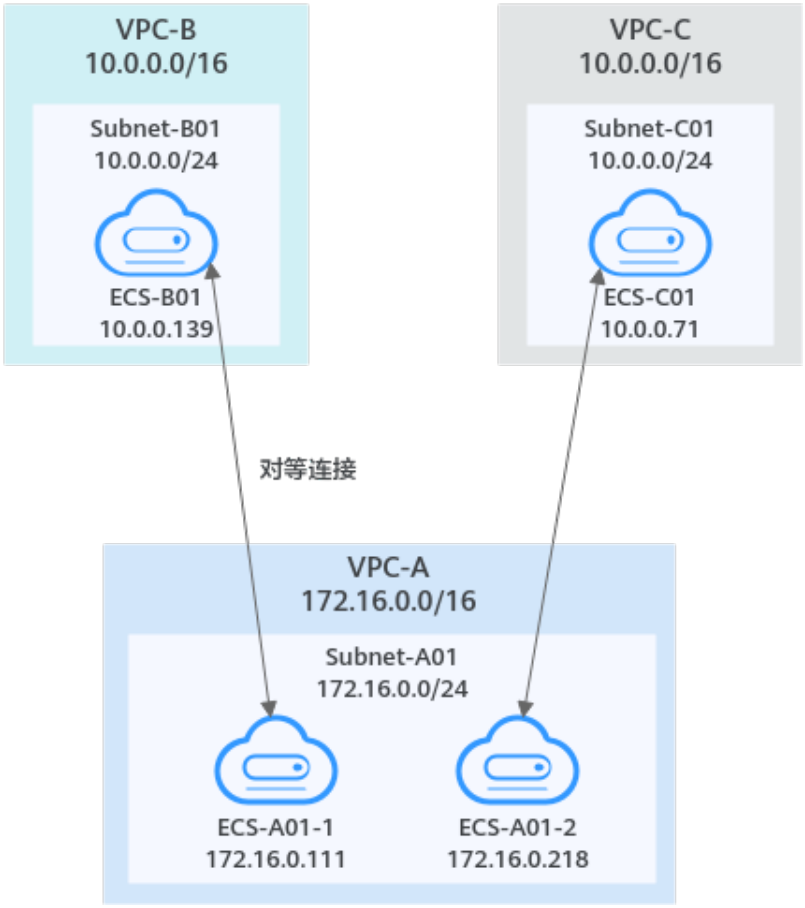


表 8-49 资源规划详情-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01-1	sg-web：通用Web服务器	172.16.0.111
					ECS-A01-2		172.16.0.218
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71

表 8-50 对等连接关系说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A内ECS-A01-1和VPC-B内ECS-B01对等	Peering-AB	VPC-A	VPC-B
VPC-A内ECS-A01-2和VPC-C内ECS-C01对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您在本端和对端VPC路由表中，添加以下路由：

表 8-51 VPC 路由表配置说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.0.139/32 (ECS-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为ECS-B01的私有IP地址，下一跳指向Peering-AB的路由。
	10.0.0.71/32 (ECS-C01)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为ECS-C01的私有IP地址，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.111/32 (ECS-A01-1)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为ECS-A01-1的私有IP地址，下一跳指向Peering-AB的路由。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.218/32 (ECS-A01-2)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为ECS-A01-2的私有IP地址，下一跳指向Peering-AC的路由。

配置一个中心 VPC 通过最长匹配原则与两个 VPC 对等（IPv4）

如果在一个VPC和其他多个网段重叠的VPC之间创建对等连接，那么配置路由的时候，您可以参考本示例，将路由的目的地址范围缩小，配置成ECS的私有IP地址。路由目的地址规划不当，会导致流量无法正确转发，错误示例及原因详解，可参见**配置一个中心VPC与两个VPC的重叠子网对等（IPv4）**。

在本示例中，在中心VPC-A和VPC-B内ECS-B01之间创建对等连接Peering-AB，在中心VPC-A和VPC-C之间创建对等连接Peering-AC。Subnet-B01和Subnet-C01子网网段重叠，因此添加路由时，可以使用路由的最长匹配原则，控制流量的转发路径。

- 资源规划详情，请参见表8-52。
- 对等连接关系，请参见表8-53。

图 8-19 一个中心 VPC 通过最长匹配原则与两个 VPC 对等(IPv4)

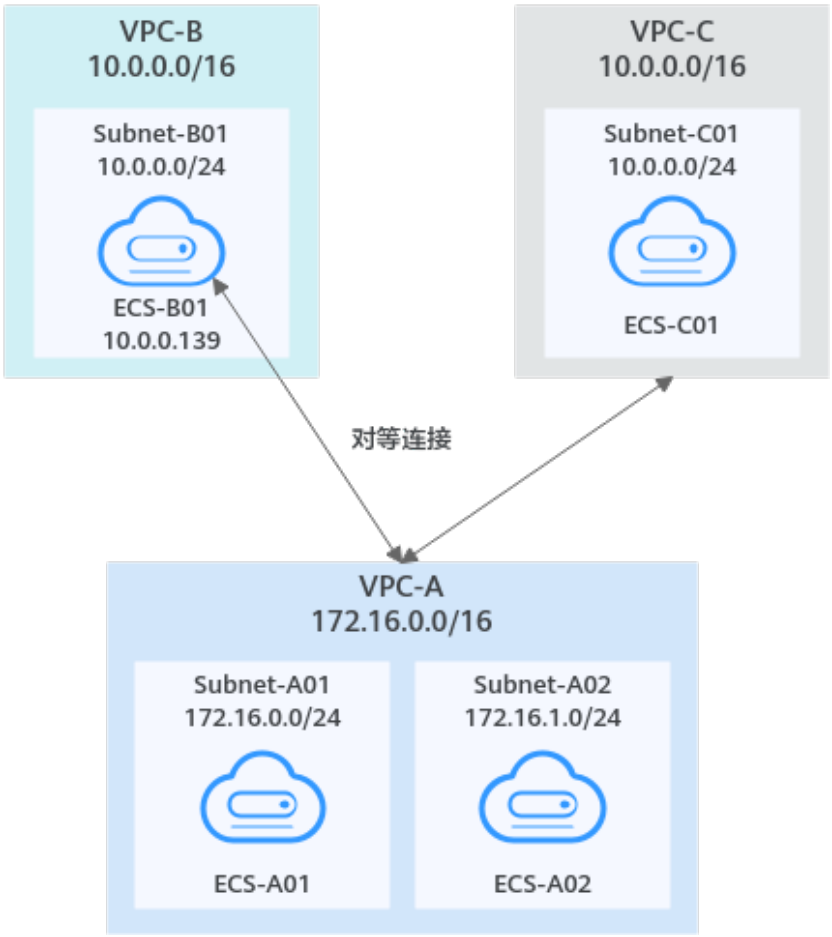


表 8-52 资源规划详情-一个中心 VPC 通过最长匹配原则与两个 VPC 对等(IPv4)

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-A	172.16.0.0/16	Subnet-A01	172.16.0.0/24	rtb-VPC-A	ECS-A01	sg-web：通用Web服务器	172.16.0.111
		Subnet-A02	172.16.1.0/24	rtb-VPC-A	ECS-A02		172.16.1.91
VPC-B	10.0.0.0/16	Subnet-B01	10.0.0.0/24	rtb-VPC-B	ECS-B01		10.0.0.139

VPC名称	VPC网段	子网名称	子网网段	关联VPC路由表	ECS名称	安全组	私有IP地址
VPC-C	10.0.0.0/16	Subnet-C01	10.0.0.0/24	rtb-VPC-C	ECS-C01		10.0.0.71

表 8-53 对等连接关系说明-一个中心 VPC 通过最长匹配原则与两个 VPC 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B内ECS-B01对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C

对等连接创建完成后，您在本端和对端VPC路由表中，添加以下路由：

表 8-54 VPC 路由表配置说明-一个中心 VPC 通过最长匹配原则与两个 VPC 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	172.16.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.1.0/24	Local	系统路由	
	10.0.0.139/32 (ECS-B01)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为ECS-B01的私有IP地址，下一跳指向Peering-AB的路由。
	10.0.0.0/16 (VPC-C)	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C的网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	172.16.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AB的路由。
rtb-VPC-C	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。

路由表	目的地址	下一跳	路由类型	路由说明
	172.16.0.0/16 (VPC-A)	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AC的路由。

8.2.5 无效的 VPC 对等连接配置示例

操作场景

VPC对等连接针对部分场景的配置是无效的，具体如表8-55所示。

表 8-55 无效的 VPC 对等连接场景

场景说明	配置示例
• VPC网段重叠，且全部子网重叠 此种场景下，不支持使用VPC对等连接。 • VPC网段重叠，且部分子网重叠 此时无法创建指向整个VPC网段的对等连接，可以创建指向子网的对等连接，对等连接两端的子网网段不能包含重叠子网。	**VPC网段重叠可能导致对等连接不生效** • **VPC网段重叠，且全部子网重叠** • **VPC网段重叠，且部分子网重叠**
基于VPC对等连接，无法实现多个ECS共用EIP访问公网。 比如，在VPC-A和VPC-B之间创建对等连接，VPC-A内的云服务器ECS-A01绑定了EIP用来访问公网，此时VPC-B内的云服务器ECS-B01无法通过ECS-A01的EIP访问公网。	**VPC对等连接不支持共用EIP**

VPC 网段重叠可能导致对等连接不生效

VPC网段重叠的情况下，容易因为路由冲突导致对等连接不生效，以下为您提供原因说明和配置建议，请根据您的VPC资源情况进行选择：

- VPC网段重叠，且全部子网重叠

  此场景下，不支持使用对等连接。如图8-20所示，以网段和子网完全重叠的VPC-A和VPC-B为例，假如在VPC-A和VPC-B之间创建对等连接，那么路由表如表8-56所示。

  在rtb-VPC-A路由表中，Local路由和对等连接路由的目的地址重叠，VPC-A往VPC-B的流量，会优先匹配Local路由，流量在VPC-A内部转发，无法送达VPC-B。

图 8-20 VPC 网段重叠，且全部子网重叠(IPv4)

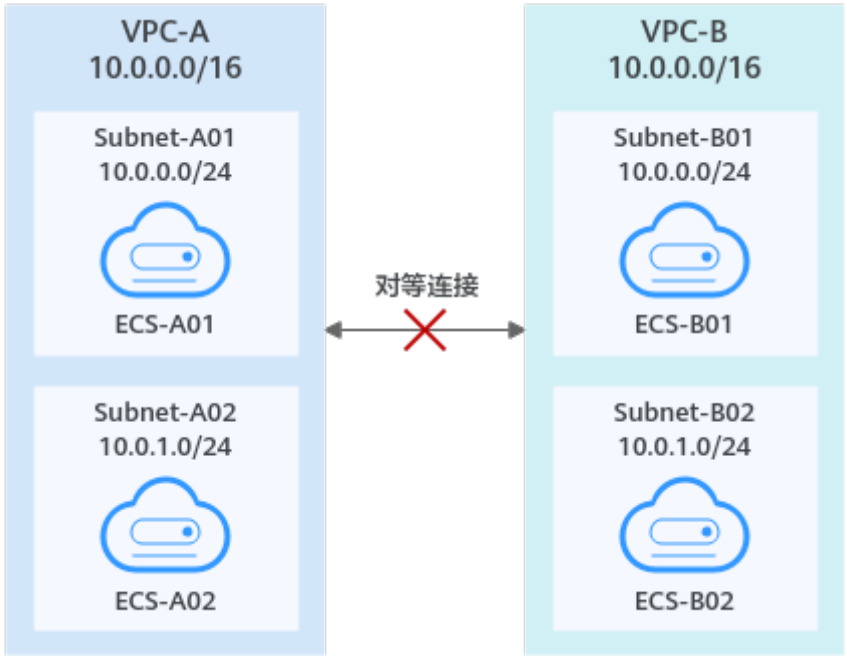
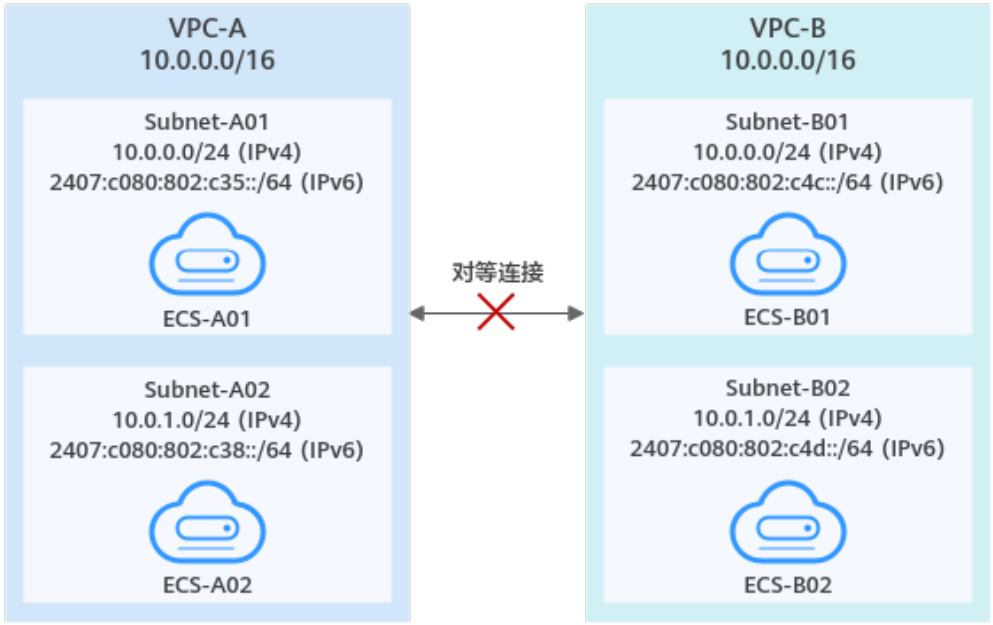


表 8-56 VPC 路由表配置说明-VPC 网段重叠，且全部子网重叠(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B的网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AB的路由。

以上限制同样适用于IPv6场景，即使您只需要使用对等连接实现不同VPC之间的IPv6通信，此时如果对等连接两端VPC的IPv4网段和子网重叠，那么您创建的对等连接也不会生效。

图 8-21 VPC 网段重叠，且全部子网重叠(IPv6)



- VPC网段重叠，且部分子网重叠

  创建VPC对等连接时，如果两端的VPC网段和部分子网重叠，那么请您避免创建以下场景的对等连接：

  - 指向整个VPC网段的对等连接将不生效。

    如图8-22所示，假如创建VPC-A和VPC-B之间的对等连接，由于VPC-A和VPC-B网段重叠，那么对等连接将不生效。

  - 指向VPC子网的对等连接，如果对等连接两端包含重叠子网，将不会生效。

    如图8-22所示，创建Subnet-A01和Subnet-B02之间的对等连接，那么路由表如表8-57所示。在rtb-VPC-B路由表中，Local路由和对等连接的路由目的地址重叠，Subnet-B02往Subnet-A01的流量，会优先匹配Local路由，流量在Subnet-B02内部转发，无法送达Subnet-A01。

图 8-22 VPC 网段重叠，且部分子网重叠(IPv4)

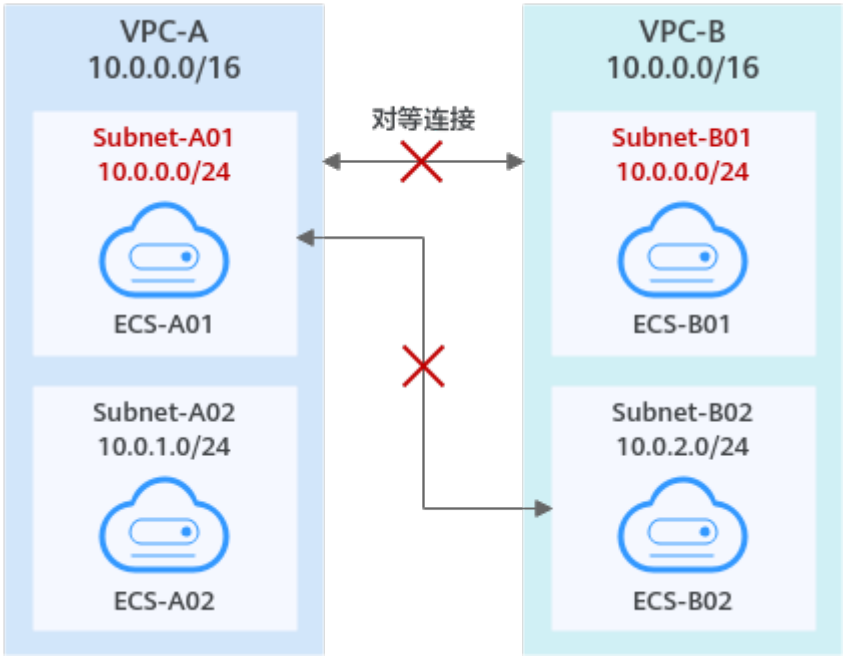
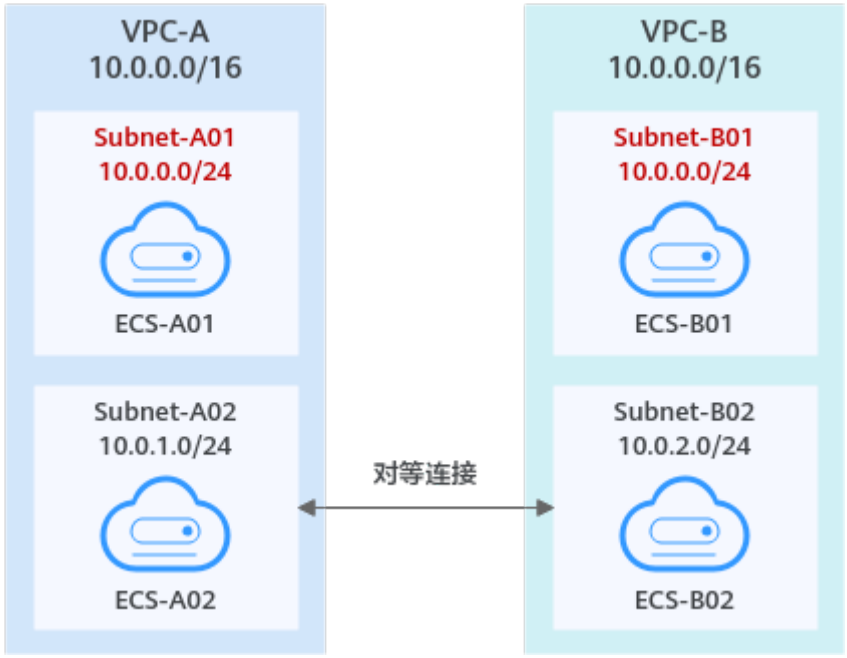


表 8-57 VPC 路由表配置说明-VPC 网段重叠，且部分子网重叠(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	10.0.2.0/24 (Subnet-B02)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为Subnet-B02子网网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.2.0/24	Local	系统路由	
	10.0.0.0/24 (Subnet-A01)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为Subnet-A01子网网段，下一跳指向Peering-AB的路由。

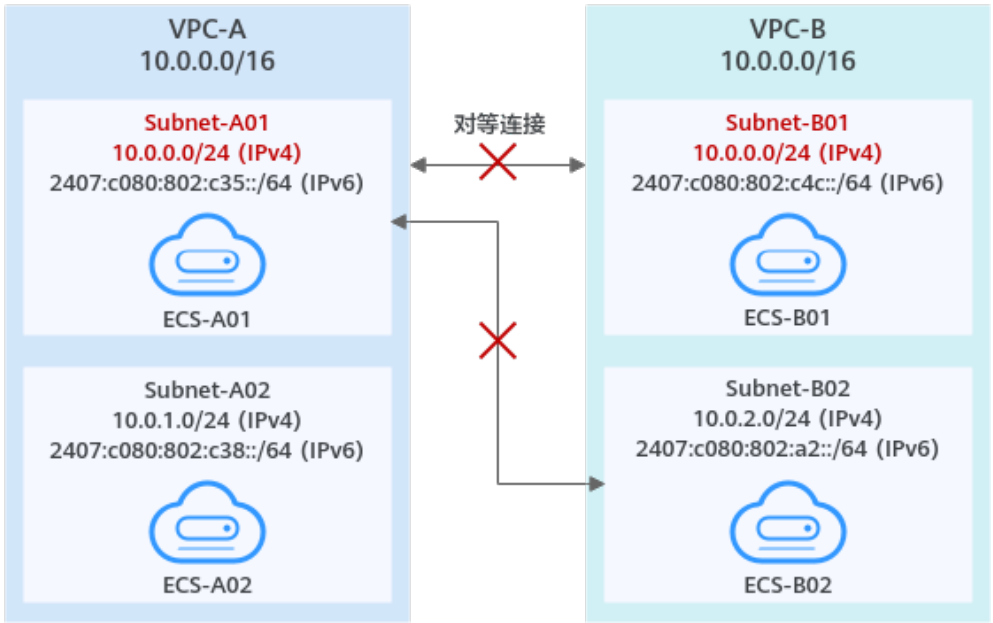
对于此场景，对等连接两端不能包含重叠子网。如图8-23所示，您可以创建Subnet-A02和Subnet-B02之间的对等连接，此时路由不会冲突，对等连接生效。

图 8-23 VPC 网段重叠，部分子网重叠(IPv4)-正确配置



以上限制同样适用于IPv6场景，即使您只需要使用对等连接实现不同VPC之间的IPv6通信，此时如果对等连接两端VPC的IPv4网段和子网重叠，那么您创建的对等连接也不会生效。

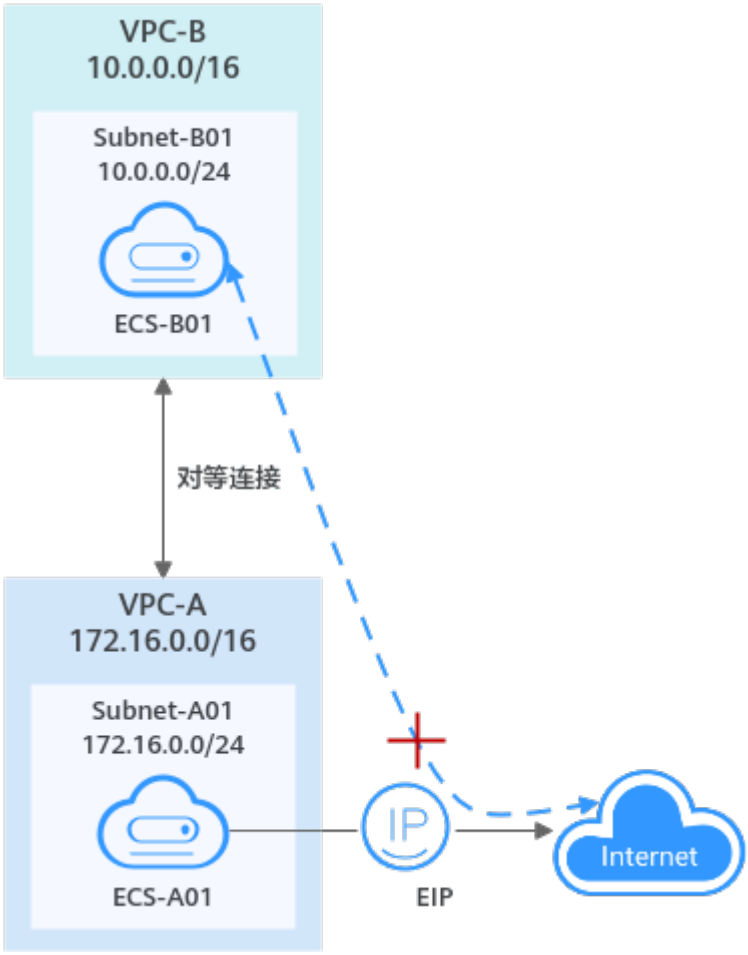
图 8-24 VPC 网段重叠，且部分子网重叠(IPv6)



VPC 对等连接不支持共用 EIP

如图8-25所示，在VPC-A和VPC-B之间建立对等连接，ECS-A01绑定了EIP用来访问公网，此时ECS-B01无法通过ECS-A01的EIP访问公网。

图 8-25 VPC 对等连接不支持共用 EIP



8.3 创建相同账户下的对等连接

操作场景

不同VPC之间网络不通，您可以通过对等连接连通同一个区域下的VPC。本章节指导用户创建相同账户下的VPC对等连接，即需要连通的两个VPC位于同一个账户下。

本文档以在账户A下，创建VPC-A和VPC-B之间的对等连接为例，实现业务服务器ECS-A01和数据库服务器RDS-B01之间的通信。

创建步骤如下：

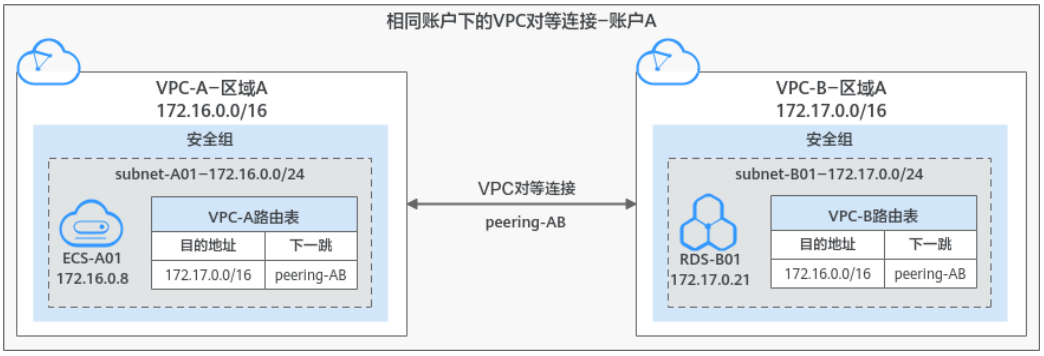
步骤一：创建VPC对等连接

步骤二：添加VPC对等连接路由

步骤三：配置对等连接两端VPC内实例的安全组规则

步骤四：验证网络互通情况

图 8-26 相同账户下的对等连接组网示例



须知

当前VPC对等连接暂不收取您的任何费用。

约束与限制

- 对等连接是建立在两个VPC之间的网络连接，两个VPC之间只能建立一个对等连接。
- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
  - 您可以通过对等连接连通位于华为云中国站和国际站相同区域的VPC，比如VPC-A位于中国站的“中国-香港”区域，VPC-B位于国际站的“中国-香港”区域，可以通过对等连接连通VPC-A和VPC-B。
  - 若要实现不同区域VPC之间互通，您可以使用云连接，详细内容请参见**跨区域VPC互通**。
  - 若您仅需要不同区域的几台ECS之间互通，您可以**为ECS申请和绑定弹性公网IP**，通过EIP实现ECS外网互通。此场景适用于ECS数量较少的情况。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。

  针对该情况，您可以参考**对等连接使用示例**进行相关组网配置。

前提条件

已在同一个账号下创建两个VPC，并且VPC位于同一个区域，具体方法请参见**创建虚拟私有云和子网**。

步骤一：创建 VPC 对等连接

1. 进入**对等连接列表页面**。
2. 在页面右上角区域，单击“创建对等连接”。

   进入“创建对等连接”页面。
3. 根据界面提示设置对等连接参数。

   参数详细说明请参见**表8-58**。

图 8-27 创建对等连接

表 8-58 创建对等连接-参数说明

参数	说明	取值样例
区域	必选参数。 不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-上海一

参数	说明	取值样例
对等连接名称	必选参数。 此处填写对等连接的名称。 由中文字符、英文字母、数字、中划线、下划线等构成，一般不超过64个字符。	peering-AB
描述	可选参数。 您可以根据需要在文本框中输入对等连接的描述信息。	peering-AB连通VPC-A和VPC-B
本端VPC	必选参数。 此处为对等连接一端的VPC，可以在下拉框中选择已有VPC作为本端VPC。	VPC-A
本端VPC网段	此处显示已选择的本端VPC的网段。	172.16.0.0/16
账户	必选参数。 • 当前账户：当对等连接中的对端VPC和本端VPC位于同一个账户下时，选择该项。 • 其他账户：当对等连接中的对端VPC和本端VPC位于不同账户下时，选择该项。	当前账户
对端项目	当账户选择“当前账户”时，系统默认填充对应的项目，无需您额外操作。 比如VPC-A和VPC-B均为账户A下的资源，并且位于区域A，那么此处系统默认显示账户A下，区域A对应的项目。	ab-cdef-1
对端VPC	当账户选择“当前账户”时，该项为必选参数。 此处为对等连接另外一端的VPC，可以在下拉框中选择已有VPC作为对端VPC。	VPC-B
对端VPC网段	此处显示已选择的对端VPC的网段。 当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效，具体请参见**对等连接配置示例概述**。	172.17.0.0/16

4. 参数填写完成后，单击“立即创建”。
   弹出路由添加提示对话框。

5. 在路由添加提示对话框中，单击“立即添加”，跳转到对等连接详情页面，继续执行**步骤二：添加VPC对等连接路由**，添加路由。

步骤二：添加 VPC 对等连接路由

1. 在对等连接详情页面下方区域，单击“添加路由”。
   弹出对等连接的“添加路由”对话框。

   图 8-28 添加对等连接路由

2. 根据界面提示，在VPC路由表中添加路由。
   参数说明如**表8-59**所示。

表 8-59 参数说明

参数	说明	取值样例
虚拟私有云	选择对等连接两端中的任意一个VPC。	VPC-A
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 ● 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 ● 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-A（默认路由表）
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接配置示例概述**。	本示例为VPC-B的网段：172.17.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	本端VPC-A到对端VPC-B的去程路由。
添加另一端VPC的路由	勾选该参数，可同时添加对等连接另一端VPC内的回程路由。 通常情况下，您需要在对等连接两端VPC的路由表中分别添加去程和回程路由，才可以实现通信，单击了解**对等连接配置示例概述**。	勾选
虚拟私有云	系统默认填写对等连接两端的另一个VPC，您无需选择。	VPC-B
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 ● 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 ● 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-B（默认路由表）

参数	说明	取值样例
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接配置示例概述**。	本示例为VPC-A的网段：172.16.0.0/16
下一跳地址	系统默认选择当前对等连接，无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	对端VPC-B到本端VPC-A的回程路由。

3. 路由信息设置完成后，单击“确定”。
   返回路由列表，可以看到已添加的路由。

步骤三：配置对等连接两端 VPC 内实例的安全组规则

本示例中，实例（如ECS和RDS）安全组采用的预设规则为“自定义”，预设的安全组规则如**表8-60**所示。

表 8-60 安全组的预设规则（自定义）

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	全部	源地址：当前安全组	针对全部IPv4协议，允许安全组内实例通过内网网络相互通信。
入方向	允许	IPv6	全部	源地址：当前安全组	针对全部IPv6协议，允许安全组内实例通过内网网络相互通信。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对全部IPv4协议，允许所有流量从安全组内实例流出，用于访问外部。
出方向	允许	IPv6	全部	目的地址：::/0	针对全部IPv6协议，允许所有流量从安全组内实例流出，用于访问外部。

基于预设规则，可以看到该规则的初始配置只可以确保当前安全组内实例内网互通，拒绝任何访问当前安全组内实例的外部流量，因此，您需要根据实际业务情况，添加放通外部流量的安全组规则。具体操作请参见**添加安全组规则**。

- 当对等连接两端VPC内实例位于同一个安全组时，只要VPC-A和VPC-B之间的对等连接创建成功后，就可以实现内网网络互通。
  比如，ECS-A01和RDS-B01均属于安全组Sg-AB，您只需要执行**1.放通远程登录实例的流量**。
- 当对等连接两端VPC内的实例位于不同的安全组时，如果未在安全组中分别放通实例互访的流量，则对等连接创建成功后，安全组会拦截实例互访的流量。
  比如，ECS-A01属于安全组Sg-A，RDS-B01属于安全组Sg-B，您需要执行**1.放通远程登录实例的流量**和**2.放通对等连接两端实例内网互通的流量**。

1. 在安全组中添加**表8-61**中的规则，放通远程登录安全组内实例的流量。

表 8-61 安全组规则（远程登录）

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	TCP: 22	IP地址：0.0.0.0/0	针对IPv4协议，放通安全组内实例的SSH(22)端口，用于远程登录Linux 实例。
入方向	允许	IPv4	TCP: 3389	IP地址：0.0.0.0/0	针对IPv4协议，放通安全组内实例的RDP(3389)端口，用于远程登录Windows 实例。

须知

本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

2. （可选）当对等连接两端的实例位于不同安全组内时，您需要分别在两端的安全组中添加以下规则，放通对等连接两端实例内网互通的流量。

   以下为您提供两种方案，请您根据业务实际需要选择一个即可。

   - 表8-62中提供方案一：源地址填写对端VPC网段或者子网网段，放通对等连接两端VPC或者子网之间的内网网络流量。

     表 8-62 安全组规则（网段）

安全组	方向	策略	类型	协议端口	源地址	描述
Sg-A	入方向	允许	IPv4	全部	IP地址：172.17.0.0/16（VPC-B的网段）	针对全部IPv4协议，允许来自172.17.0.0/16网段范围的流量访问Sg-A内的实例。
Sg-B	入方向	允许	IPv4	全部	IP地址：172.16.0.0/16（VPC-A网段）	针对全部IPv4协议，允许来自172.16.0.0/16网段范围的流量访问Sg-B内的实例。

   - 表8-63中提供方案二：源地址选择对端实例的安全组，放通两个安全组之间的内网网络流量。

表 8-63 安全组规则（安全组）

安全组	方向	策略	类型	协议端口	源地址	描述
Sg-A	入方向	允许	IPv4	全部	Sg-B	针对全部IPv4协议，允许来自Sg-B内实例的流量访问Sg-A内的实例。
Sg-B	入方向	允许	IPv4	全部	Sg-A	针对全部IPv4协议，允许来自Sg-A内实例的流量访问Sg-B内的实例。

步骤四：验证网络互通情况

对等连接路由添加完成后，执行以下操作，验证本端VPC和对端VPC的通信情况。

1. 登录本端VPC内的弹性云服务器，本示例中为ECS-A01。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。
2. 执行以下命令，验证ECS-A01和RDS-B01是否可以通信。

   ping *对端服务器的IP地址*

   命令示例：

   ping 172.17.0.21

   回显类似如下信息，表示ECS-A01与RDS-B01可以通过通信，VPC-A和VPC-B之间的对等连接创建成功。

```
[root@ecs-A01 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

须知

本示例中ECS-A01和RDS-B01位于同一个安全组内，因此只要VPC-A和VPC-B之间的对等连接创建成功后，就可以实现网络互通。如果您需要连通的实例位于不同的安全组内，那么您需要在安全组的入方向规则中，添加放通对端安全组的规则，具体方法请参见**实现不同安全组的实例内网网络互通**。

对于更多对等连接网络不通的问题，处理方法请参见**为什么对等连接创建完成后不能互通？**。

8.4 创建不同账户下的对等连接

操作场景

不同VPC之间网络不通，您可以通过对等连接连通同一个区域下的VPC。本章节指导用户创建不同账户下的VPC对等连接，即需要连通的两个VPC位于不同账户下。

本文档以在账户A下的VPC-A和账户B的VPC-B之间创建对等连接为例，实现业务服务器ECS-A01和数据库服务器RDS-B01之间的通信。

创建步骤如下：

步骤一：创建VPC对等连接

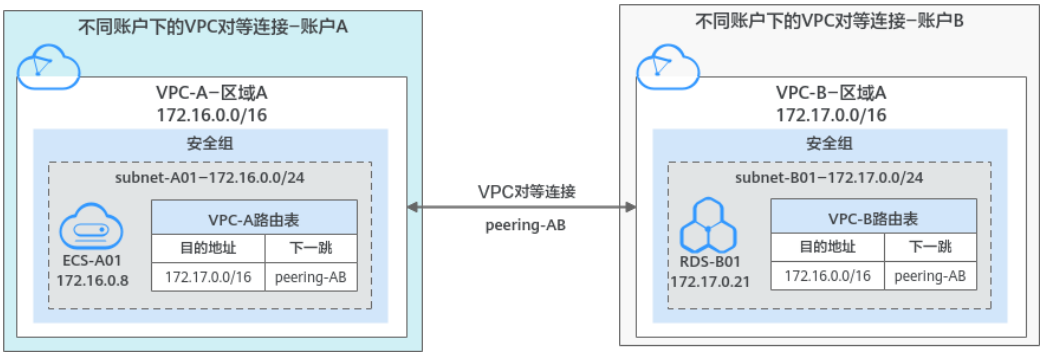
步骤二：对端账户接受VPC对等连接

步骤三：添加VPC对等连接路由

步骤四：配置对等连接两端VPC内实例的安全组规则

步骤五：验证网络互通情况

图 8-29 不同账户下的对等连接组网示例



须知

当前VPC对等连接暂不收取您的任何费用。

约束与限制

- 对等连接是建立在两个VPC之间的网络连接，两个VPC之间只能建立一个对等连接。
- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
  - 您可以通过对等连接连通位于华为云中国站和国际站相同区域的VPC，比如VPC-A位于中国站的“中国-香港”区域，VPC-B位于国际站的“中国-香港”区域，可以通过对等连接连通VPC-A和VPC-B。
  - 若要实现不同区域VPC之间互通，您可以使用云连接，详细内容请参见**跨区域VPC互通**。
  - 若您仅需要不同区域的几台ECS之间互通，您可以**为ECS申请和绑定弹性公网IP**，通过EIP实现ECS外网互通。此场景适用于ECS数量较少的情况。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。

  针对该情况，您可以参考**对等连接使用示例**进行相关组网配置。
- 创建不同账户下的对等连接时：
  - 创建不同账户下的VPC对等连接时，如果在账号A下发起创建对等连接请求，需要账号B接受该请求才可以，如果账号B拒绝，则该对等连接创建失败。

- 为了确保网络安全，请您不要接受来自未知账号的对等连接申请。

前提条件

已在不同账号下，分别创建两个VPC，并且VPC位于同一个区域，具体方法请参见**创建虚拟私有云和子网**。

步骤一：创建 VPC 对等连接

1. 进入**对等连接列表页面**。
2. 在页面右上角区域，单击“创建对等连接”。
   进入“创建对等连接”页面。
3. 根据界面提示设置对等连接参数。
   参数详细说明请参见**表8-64**。

图 8-30 创建对等连接

表 8-64 创建对等连接-参数说明

参数	说明	取值样例
区域	必选参数。 不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	华东-上海一
对等连接名称	必选参数。 此处填写对等连接的名称。 由中文字符、英文字母、数字、中划线、下划线等构成，一般不超过64个字符。	peering-AB
描述	可选参数。 您可以根据需要在文本框中输入对该连接的描述信息。描述信息内容不能超过255个字符，且不能包含“<”和“>”。	peering-AB连通VPC-A和VPC-B
本端VPC	必选参数。 此处为对等连接一端的VPC，可以在下拉框中选择已有VPC作为本端VPC。	VPC-A
本端VPC网段	此处显示已选择的本端VPC的网段。	172.16.0.0/16
账户	必选参数。 • 当前账户：当对等连接中的对端VPC和本端VPC位于同一个账户下时，选择该项。 • 其他账户：当对等连接中的对端VPC和本端VPC位于不同账户下时，选择该项。	其他账户
对端项目ID	当账户选择“其他账户”时，该项为必选参数。 对端项目ID是另一个账户下，对端VPC所在区域对应的项目ID，获取方法请参见**获取对等连接的对端项目ID**。	VPC-B在区域A对应的项目ID： 067cf8aecf3XXX08322f13b
对端VPC ID	当账户选择“其他账户”时，该项为必选参数 对端VPC ID是对等连接另一端的VPC ID，获取方法请参见**获取虚拟私有云的ID信息**。	VPC-B的ID: 17cd7278-XXX-530c952dcf35

4. 参数填写完成后，单击“立即创建”。

- 如果提示“请输入正确的VPC ID以及项目ID”，请您检查项目ID和VPC ID的正确性。
  - 项目ID：必须为对端VPC所在区域对应的项目ID。
  - 本端VPC必须和对端VPC位于同一个区域。
- 如果返回对等连接列表，且新创建的对等连接状态为“待接受”，请继续执行**步骤二：对端账户接受VPC对等连接**，联系账户B处理。

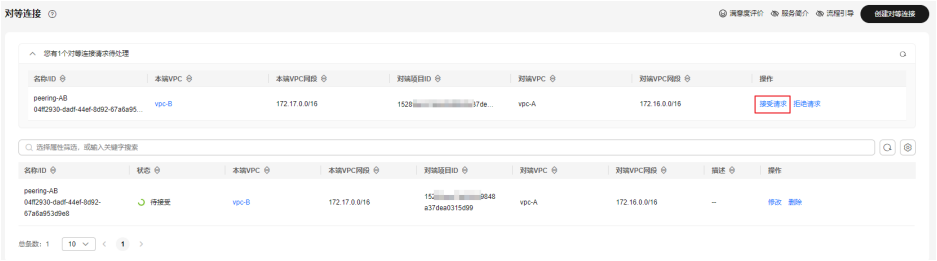
图 8-31 待接受对等连接

步骤二：对端账户接受 VPC 对等连接

不同账户创建对等连接，本端账户创建完成后，需要联系对端账户接受对等连接请求之后，该对等连接才算创建完成。本示例中，账户A通知账户B接受对等连接。

1. 对端账户登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表上方，找到待接受的对等连接请求。

图 8-32 接受对等连接



5. 确认无误后，单击目标对等连接所在行的操作列下的“接受请求”。
   待对等连接状态变为“已接受”，表示对等连接创建完成。
6. 执行**步骤三：添加VPC对等连接路由**，为对等连接添加路由。

步骤三：添加 VPC 对等连接路由

通常情况下，您需要在对等连接两端VPC的路由表中分别添加去程和回程路由，才可以实现通信，单击了解**对等连接配置示例概述**。

本端账户在本端VPC的路由表中添加路由，对端账户在对端VPC的路由表中添加路由。本示例中，账户A在VPC-A的路由表中添加路由，账户B在VPC-B的路由表中添加路由。

1. 执行以下操作，在本端VPC路由表中添加对等连接路由。
   a. 在本端账户的对等连接列表中，单击目标对等连接的名称。

进入对等连接详情页面。

b. 在对等连接详情页面下方区域，单击“添加路由”。
弹出对等连接的“添加路由”对话框。

图 8-33 添加对等连接路由

c. 根据界面提示，在VPC路由表中添加路由。
参数说明如表8-65所示。

表 8-65 参数说明

参数	说明	取值样例
虚拟私有云	系统默认填写对等连接中当前账户内的VPC，您无需选择。	VPC-A
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 • 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 • 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-A（默认路由表）

参数	说明	取值样例
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接配置示例概述**。	本示例为VPC-B的网段：172.17.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	本端VPC-A到对端VPC-B的去程路由。

d. 路由信息设置完成后，单击“确定”。
返回路由列表，可以看到刚添加的路由。

2. 执行以下操作，在对端VPC路由表中添加对等连接路由。
a. 在对端账户的对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
b. 在对等连接详情页面下方区域，单击“添加路由”。
弹出对等连接的“添加路由”对话框。

图 8-34 添加对等连接路由

c. 根据界面提示，在VPC路由表中添加路由。
参数说明如**表8-66**所示。

表 8-66 参数说明

参数	说明	取值样例
虚拟私有云	系统默认填写对等连接中当前账户内的VPC，您无需选择。	VPC-B
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 • 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 • 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-B（默认路由表）
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接配置示例概述**。	本示例为VPC-A的网段：172.16.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	对端VPC-B到本端VPC-A的回程路由。

d. 路由信息设置完成后，单击“确定”。

返回路由列表，可以看到已添加的路由。

步骤四：配置对等连接两端 VPC 内实例的安全组规则

本示例中，实例（如ECS和RDS）安全组采用的预设规则为“自定义”，预设的安全组规则如**表8-67**所示。

表 8-67 安全组的预设规则（自定义）

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	全部	源地址：当前安全组	针对全部IPv4协议，允许安全组内实例通过内网网络相互通信。
入方向	允许	IPv6	全部	源地址：当前安全组	针对全部IPv6协议，允许安全组内实例通过内网网络相互通信。

方向	策略	类型	协议端口	源地址/目的地址	描述
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对全部IPv4协议，允许所有流量从安全组内实例流出，用于访问外部。
出方向	允许	IPv6	全部	目的地址：::/0	针对全部IPv6协议，允许所有流量从安全组内实例流出，用于访问外部。

基于预设规则，可以看到该规则的初始配置只可以确保当前安全组内实例内网互通，拒绝任何访问当前安全组内实例的外部流量，因此，您需要根据实际业务情况，添加放通外部流量的安全组规则。具体操作请参见**添加安全组规则**。

当您创建不同账户下的对等连接时，则对等连接两端VPC内的实例位于不同的安全组，如果未在安全组中分别放通实例互访的流量，则对等连接创建成功后，安全组会拦截实例互访的流量。比如，ECS-A01属于安全组Sg-A，RDS-B01属于安全组Sg-B，您需要执行以下操作，同时放通远程登录实例的流量和对等连接两端实例内网互通的流量。

1. 在安全组中添加**表8-68**中的规则，放通远程登录安全组内实例的流量。

   表 8-68 安全组规则（远程登录）

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	TCP: 22	IP地址：0.0.0.0/0	针对IPv4协议，放通安全组内实例的SSH(22)端口，用于远程登录Linux 实例。
入方向	允许	IPv4	TCP: 3389	IP地址：0.0.0.0/0	针对IPv4协议，放通安全组内实例的RDP(3389)端口，用于远程登录Windows 实例。

   须知

   本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

2. 分别在两端的安全组中添加**表8-69**中的规则，放通对等连接两端实例内网互通的流量。

   源地址填写对端VPC网段或者子网网段，放通对等连接两端VPC或者子网之间的内网网络流量。

表 8-69 安全组规则（网段）

安全组	方向	策略	类型	协议端口	源地址	描述
Sg-A	入方向	允许	IPv4	全部	IP地址：172.17.0.0/16（VPC-B的网段）	针对全部IPv4协议，允许来自172.17.0.0/16网段范围的流量访问Sg-A内的实例。
Sg-B	入方向	允许	IPv4	全部	IP地址：172.16.0.0/16（VPC-A网段）	针对全部IPv4协议，允许来自172.16.0.0/16网段范围的流量访问Sg-B内的实例。

步骤五：验证网络互通情况

对等连接路由添加完成后，执行以下操作，验证本端VPC和对端VPC的通信情况。

1. 登录本端VPC内的弹性云服务器，本示例中为ECS-A01。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

2. 执行以下命令，验证ECS-A01和RDS-B01是否可以通信。

   ping *对端服务器的IP地址*

   命令示例：

   ping 172.17.0.21

   回显类似如下信息，表示ECS-A01与RDS-B01可以通过通信，VPC-A和VPC-B之间的对等连接创建成功。

```
[root@ecs-A01 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

须知

本示例中ECS-A01和RDS-B01位于同一个安全组内，因此只要VPC-A和VPC-B之间的对等连接创建成功后，就可以实现网络互通。如果您需要连通的实例位于不同的安全组内，那么您需要在安全组的入方向规则中，添加放通对端安全组的规则，具体方法请参见**实现不同安全组的实例内网网络互通**。

对于更多对等连接网络不通的问题，处理方法请参见**为什么对等连接创建完成后不能互通？**。

8.5 获取对等连接的对端项目 ID

操作场景

当您创建不同账户下的VPC对等连接时，您可以参考本章节获取对端VPC所在区域对应的项目ID，即对端项目ID。

操作步骤

1. 登录管理控制台。
   此处使用对端账户登录管理控制台。
2. 在页面右上角的用户名的下拉列表中，单击“我的凭证”。
   进入“我的凭证”页面。

   图 8-35 我的凭证

3. 在项目列表中，获取项目ID。
   找到对端VPC的“所属区域”，然后获取该区域对应的“项目ID”。

   图 8-36 对端项目 ID

8.6 修改对等连接

操作场景

本章节指导用户修改对等连接的基本信息，包括对等连接名称和描述。

对等连接在任何状态下，本端账户和对端账户均有权限修改对等连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
5. 在对等连接列表中，单击目标对等连接所在行的操作列下的“修改”。
   弹出对等连接修改对话框。
6. 修改对等连接的信息，并单击“确定”，完成信息修改。

8.7 查看对等连接

操作场景

本章节指导用户查看对等连接的基本信息，包括对等连接名称、状态、本端VPC以及对端VPC的信息。

对于连通不同账户VPC的对等连接，本端账户和对端账户均可以查看该对等连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
5. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页，查看对等连接的详细信息。

8.8 删除对等连接

操作场景

本章节指导用户删除对等连接。

对等连接在任何状态下，本端账户和对端账户均有权限删除对等连接。

约束与限制

对等连接双方账号都有权限删除对等连接，一方删除对等连接后，对等连接的所有信息会被立刻删除，包括本端VPC和对端VPC路由表中对等连接的路由信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
5. 在对等连接列表中，单击目标对等连接所在行的操作列下的“删除”。
   弹出对等连接删除确认对话框。
6. 确认无误后，单击“确定”，删除对等连接。

8.9 修改对等连接路由

操作场景

本章节指导用户修改对等连接的路由，即修改本端VPC和对端VPC路由表中对等连接关联的路由。

- **修改相同账户对等连接的路由**
- **修改不同账户对等连接的路由**

如果您的对等连接路由添加错误，可以参考本章节修改本端VPC和对端VPC的路由配置。

修改相同账户对等连接的路由

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。

4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
5. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页面。
6. 在页面下方的路由列表中，单击目标路由对应的路由表超链接。
   进入路由表详情页面。
7. 在路由详情页面的路由列表中，单击目标路由操作列下的“修改”。
8. 根据界面提示，修改路由信息，并单击“确定”，完成路由修改。

修改不同账户对等连接的路由

通过本端账户修改本端VPC的路由，通过对端账户修改对端VPC的路由，修改方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，修改本端VPC的路由。
   a. 在管理控制台左上角单击 ，选择区域和项目。
   b. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
      进入虚拟私有云列表页面。
   c. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
      进入对等连接列表页面。
   d. 在对等连接列表中，单击目标对等连接的名称。
      进入对等连接详情页面。
   e. 在页面下方的路由列表中，单击目标路由对应的路由表超链接。
      进入路由表详情页面。
   f. 在路由详情页面的路由列表中，单击目标路由操作列下的“修改”。
   g. 根据界面提示，修改路由信息，并单击“确定”，完成路由修改。
2. 使用对端账户登录管理控制台，参考1，修改对端VPC的路由。

8.10 查看对等连接路由

操作场景

本章节指导用户查看对等连接的路由，即查看本端VPC和对端VPC添加的路由信息。

- **查看相同账户对等连接的路由**
- **查看不同账户对等连接的路由**

如果您建立了对等连接，但是无法通信，可以参考本章节检查本端VPC和对端VPC的路由配置详情。

查看相同账户对等连接的路由

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。

3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
5. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页面。
6. 在页面下方的路由列表中，可以查看路由信息。
   路由信息包括目的地址，对应的虚拟私有云、下一跳地址、路由表等信息。

查看不同账户对等连接的路由

通过本端账户查看本端VPC的路由，通过对端账户查看对端VPC的路由，查看方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，查看本端VPC的路由。
   a. 在管理控制台左上角单击，选择区域和项目。
   b. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
      进入虚拟私有云列表页面。
   c. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
      进入对等连接列表页面。
   d. 在对等连接列表中，单击目标对等连接的名称。
      进入对等连接详情页面。
   e. 在页面下方的路由列表中，可以查看路由信息。
      路由信息包括目的地址，对应的虚拟私有云、下一跳地址、路由表等信息。
2. 使用对端账户登录管理控制台，参考1，查看对端VPC的路由。

8.11 删除对等连接路由

操作场景

本章节指导用户删除对等连接的路由，即删除本端VPC和对端VPC路由表中对等连接关联的路由。

- **删除相同账户对等连接的路由**
- **删除不同账户对等连接的路由**

删除相同账户对等连接的路由

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。

进入对等连接列表页面。

5. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页面。
6. 在页面下方的路由列表中，单击目标路由操作列下的“删除”。
   弹出删除确认对话框。
7. 确认无误后，单击“确定”，删除路由。

删除不同账户对等连接的路由

通过本端账户删除本端VPC的路由，通过对端账户删除对端VPC的路由，删除方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，删除本端VPC的路由。
   a. 在管理控制台左上角单击 ，选择区域和项目。
   b. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
      进入虚拟私有云列表页面。
   c. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
      进入对等连接列表页面。
   d. 在对等连接列表中，单击目标对等连接的名称。
      进入对等连接详情页面。
   e. 在页面下方的路由列表中，单击目标路由操作列下的“删除”。
      弹出删除确认对话框。
   f. 确认无误后，单击“确定”，删除路由。
2. 使用对端账户登录管理控制台，参考**1**，删除对端VPC的路由。

9 共享 VPC

9.1 共享 VPC 概述

共享 VPC

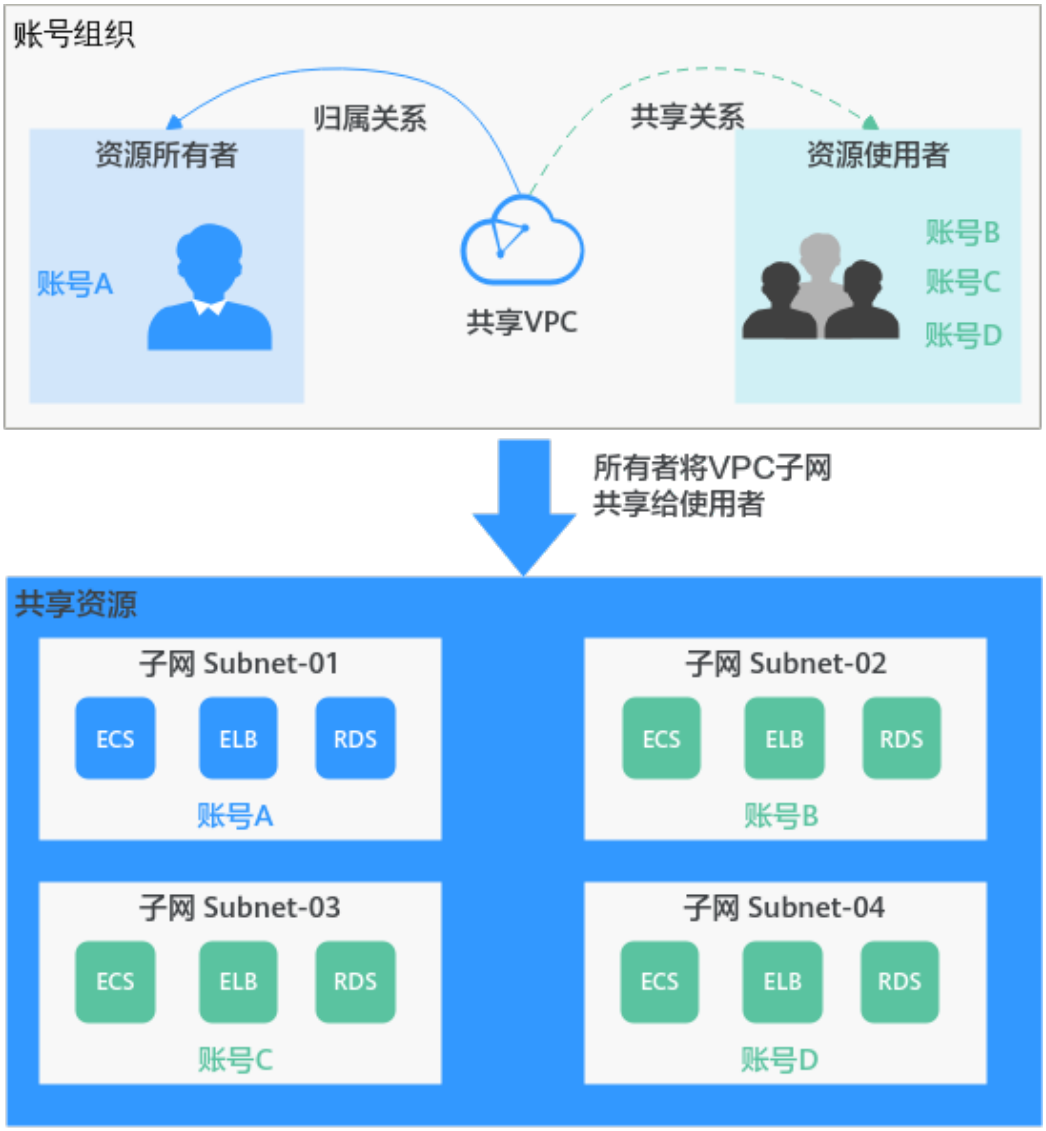
共享VPC功能支持多个账号在一个集中管理、共享的VPC内创建云资源，比如ECS、ELB、RDS等。共享VPC基于资源访问管理（ Resource Access Manager，简称RAM ）服务的机制，VPC的所有者可以将VPC内的子网共享给一个或者多个账号使用。通过共享VPC功能，可以简化网络配置，帮助您统一配置和运维多个账号下的资源，有助于提升资源的管控效率，降低运维成本。

以下为您详细介绍共享VPC的使用场景，如图9-1所示。

- 账号A：企业的IT管理账号，共享VPC和子网的所有者。

  账号A创建VPC和子网，并将子网共享给其他账号，同时也在子网Subnet-01下创建资源。
- 账号B：企业的业务账号，共享子网的使用者。使用子网Subnet-02创建资源。
- 账号C：企业的业务账号，共享子网的使用者。使用子网Subnet-03创建资源。
- 账号D：企业的业务账号，共享子网的使用者。使用子网Subnet-04创建资源。

图 9-1 共享 VPC 场景



须知

所有者和使用者的子网在同一个VPC内，子网默认网络互通。但是由于使用者和所有者位于共享子网内的资源关联不同的安全组内，因此资源之间网络隔离，如果需要资源之间互通，需要添加安全组规则放通不同安全组之间的网络，具体方法请参见**添加安全组规则**。

比如，放通账号A和账号B内两个ECS的安全组，则需要分别在两个安全组内添加入方向规则，源地址选择对方安全组。

共享 VPC 的优势

对于金融企业以及其他大企业的基础IT系统，资源在多个账号下分权管理，通常面临以下问题：

- 同时存在网络账号、安全账号、业务账号等多个账号，跨账号的资源管理，提升运维难度。

- 现有的跨账号网络配置导致组网结构复杂，用户操作体验下降并且效率较低。

为了更好的解决以上问题，我们推荐您使用共享VPC功能。企业可以按照组织结构或业务形态，将不同账号有序组织，并集中进行管理。

- 在一个账号内统一创建资源，并将资源共享给其他账号，其他账号无需创建重复资源，可以精简资源数量以及网络架构，提升管理效率并节约成本。

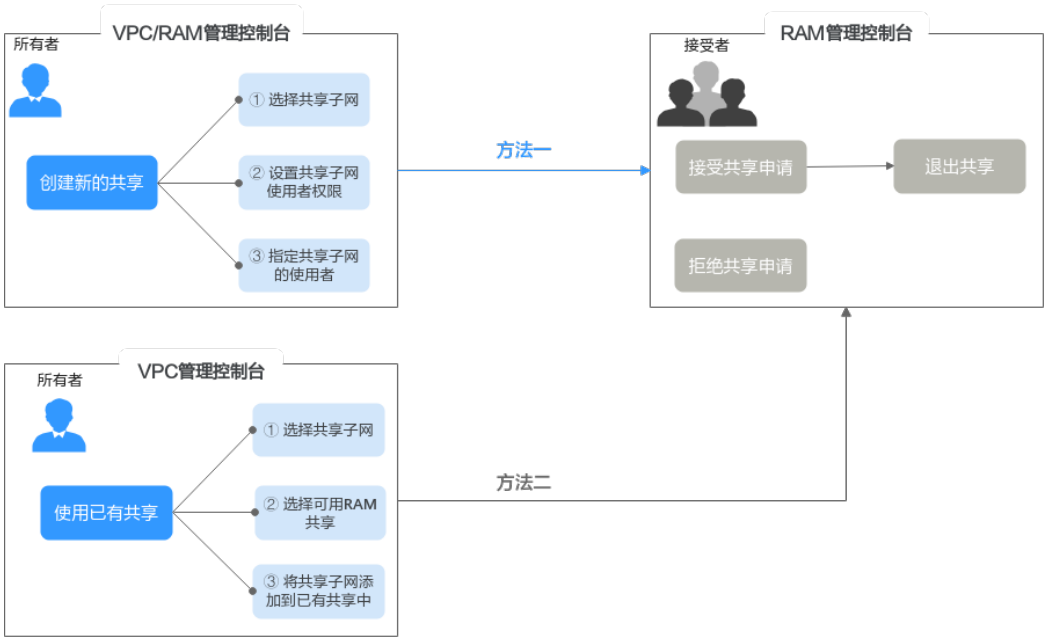
  比如不同账号下的VPC网络互通需要建立对等连接，使用共享VPC后，则不同账号用户可以在同一个VPC创建资源，免去了对等连接配置，有效的简化组网结构。
- 在一个账号内统一管理运维资源，便于企业集中配置业务安全策略，并且利于对资源使用情况的监控和审计，支撑业务的安全诉求。

共享 VPC 子网创建流程

使用共享VPC功能之前，您需要启用账号内的资源访问管理RAM服务，详情请参见 **资源访问管理 RAM 帮助文档**。

作为虚拟私有云子网的所有者，您可以将VPC内的子网共享给其他账号的使用者，使用者接受该共享请求后，子网共享才会成功。共享子网创建流程如**图9-2**所示。

图 9-2 共享子网创建流程



您可以使用RAM管理控制台或者VPC管理控制台，创建子网共享，**表9-1**中详细为您介绍两种方法。

表 9-1 共享子网创建流程说明

方法	说明	操作指导
方法一	所有者创建新的共享： 1. 所有者选择待共享的子网，可在子网详情页的“共享管理”页签下，跳转到RAM管理控制台创建新的共享，将子网共享给使用者。创建共享的具体配置如下： a. 选择共享子网。 b. 为共享子网选择权限，即指定使用者对该共享子网具备的权限。 c. 指定共享子网的使用者，可以指定多个使用者。 2. 共享创建完成后，通过RAM管理控制台，使用者可以选择接受或者拒绝共享申请。 ● 使用者接受共享申请，子网共享成功。如果后续使用者不再需要使用该共享子网，可以退出该共享。 ● 使用者拒绝共享申请，子网共享失败。	1. 所有者：**创建共享** 2. 使用者：**接受/拒绝共享邀请** **退出共享**
方法B	将子网添加到已有的共享中： 1. 所有者选择待共享的子网，可在子网详情页的“共享管理”页签下，选择已创建的共享，将子网加入到该共享内。 2. 共享创建完成后，通过RAM管理控制台，使用者可以选择接受或者拒绝共享申请。 ● 使用者接受共享申请，子网共享成功。如果后续使用者不再需要使用该共享子网，可以退出该共享。 ● 使用者拒绝共享申请，子网共享失败。	1. 所有者：**将VPC子网共享给其他账号** 2. 使用者：**接受/拒绝共享邀请** **退出共享**

共享 VPC 内所有者和使用者的权限

所有者将VPC子网共享给使用者后，所有者和使用者对共享子网、以及子网内关联云资源的操作权限如**表9-2**所示。

表 9-2 共享 VPC 内所有者和使用者的权限

角色	所有者将子网共享给使用者时	所有者停止子网共享后	使用者退出子网共享后
所有者	• 所有者可以对VPC内的资源执行的操作详细如表9-3所示。 • 所有者不可以修改、删除使用者创建的资源，比如ECS、ELB、RDS实例等。 • 在子网的“IP地址管理”页面中，所有者可以查看使用者创建资源的IP地址和资源ID等信息。	• 所有者可以正常使用、删除、管理VPC下的所有资源。 • 如果使用者在已停止共享的子网中仍拥有资源，则所有者无法删除共享子网或共享子网所在的VPC。	• 所有者可以正常使用、删除、管理VPC下的所有资源。 • 如果使用者退出子网共享后，在共享的子网中仍拥有资源，则所有者无法删除共享子网或共享子网所在的VPC。
使用者	• 使用者可以对VPC内的资源执行的操作详细如表9-3所示。 • 使用者可以在共享VPC子网内新建资源，比如ECS、ELB、RDS实例等。 • 在子网的“IP地址管理”页面中，使用者可以查看自己创建资源的IP地址和资源ID等信息，无法查看所有者和其他使用者创建的资源信息。	使用者可以继续使用自己创建的资源，无法在该共享子网内新创建资源。	使用者可以继续使用自己创建的资源，无法在该共享子网内新创建资源。

所有者和使用者对共享子网及其关联资源的使用操作权限不同，具体如表9-3所示。

表 9-3 共享 VPC 内所有者和使用者的权限（共享时）

资源	资源所有者的操作权限	资源使用者的操作权限
虚拟私有云	所有者拥有虚拟私有云的全部操作权限。	使用者可以查看共享子网所在的虚拟私有云，无法对虚拟私有云执行任何操作。

资源	资源所有者的操作权限	资源使用者的操作权限
子网	所有者拥有子网的全部操作权限。同时，所有者可以查看共享者位于共享子网内的虚拟IP和弹性网卡。	使用者可以查看共享子网，无法对共享子网执行以下操作： ● 修改子网信息 ● 删除子网 ● 添加、修改以及删除子网标签 使用者可以在共享子网内，创建虚拟IP和弹性网卡。
路由表	所有者拥有路由表的全部操作权限。	● 使用者无法在共享子网所在虚拟私有云内新建路由表。 ● 使用者可以在查看共享子网关联的路由表及路由表内路由，无法对该路由表及表内路由执行任何操作。
网络ACL	所有者拥有网络ACL的全部操作权限。	● 使用者可以在查看共享子网关联的网络ACL，无法对该网络ACL执行任何操作。 ● 使用者无法将所有者的网络ACL关联至自己名下的子网。

资源	资源所有者的操作权限	资源使用者的操作权限
安全组	• 安全组资源是独立的，所有者可以创建自己的安全组。 • 所有者只拥有自己安全组的操作权限，无法操作使用者的安全组。 • 对于同一个共享子网下的资源所关联的安全组，所有者在自己的安全组内添加安全组规则时，“源地址”可以选择使用者创建的安全组。 例如，在共享子网Subnet-X内，存在以下资源： – 所有者创建了云服务器ECS-X，关联安全组Sys-X。 – 使用者A创建了云服务器ECS-A，关联安全组Sys-A。 – 使用者B创建了数据库RDS-B，关联安全组Sys-B。 所有者为Sys-X添加安全组规则时，“源地址”可以选择安全组Sys-A或者安全组Sys-B。	• 安全组资源是独立的，使用者可以创建自己的安全组。 • 使用者只拥有自己安全组的操作权限，无法操作所有者和其他使用者的安全组。 • 对于同一个共享子网下的资源所关联的安全组，使用者在自己的安全组内添加安全组规则时，“源地址”可以选择所有者和其他使用者创建的安全组。 例如，在共享子网Subnet-X内，存在以下资源： – 所有者创建了云服务器ECS-X，关联安全组Sys-X。 – 使用者A创建了云服务器ECS-A，关联安全组Sys-A。 – 使用者B创建了数据库RDS-B，关联安全组Sys-B。 使用者A为Sys-A添加安全组规则时，“源地址”可以选择所有者的安全组Sys-X或者使用者B的安全组Sys-B。
IP地址组	IP地址组资源是独立的，所有者可以创建IP地址组，并将IP地址组关联至自己的安全组。	IP地址组资源是独立的，使用者可以创建IP地址组，并将IP地址组关联至自己的安全组。
流日志	• 所有者可以创建“资源类型”为“虚拟私有云”或者“子网”的流日志，该流日志可以对使用者位于该共享子网下的弹性网卡生效。 • 所有者可以创建“资源类型”为“网卡”的流日志，该流日志仅对所有者自己的弹性网卡生效。	使用者只可以创建“资源类型”为“网卡”的流日志，该流日志对使用者自己的弹性网卡生效。
对等连接	所有者创建VPC之间的对等连接时，可以选择共享VPC。	使用者创建VPC之间的对等连接时，无法选择共享VPC。
NAT网关	所有者可以在共享子网内创建并管理NAT网关。	使用者无法在共享子网中创建NAT网关。

资源	资源所有者的操作权限	资源使用者的操作权限
虚拟专用网络 VPN	所有者可以在共享子网内创建并管理VPN网关。	使用者无法在共享子网内创建VPN网关。
企业路由器 ER	在企业路由器中添加“虚拟私有云”连接时，所有者可以选择共享子网所在的VPC，将VPC接入企业路由器中。	在企业路由器中添加“虚拟私有云”连接时，使用者无法选择共享子网所在的VPC。
企业交换机 ESW	所有者可以在共享子网内创建并管理企业交换机。	使用者无法在共享子网内创建企业交换机。
云专线 DC	所有者可以在共享子网内创建并管理云专线。	使用者无法在共享子网内创建云专线。
云连接 CC	在云连接中添加VPC时，所有者可以选择共享子网。	在云连接中添加VPC时，使用者无法选择共享子网。
终端节点服务 VPCEP	所有者可以在共享子网内创建并管理终端节点。	使用者无法在共享子网内创建终端节点。
标签	所有者可以在共享子网内创建并管理标签。	使用者无法在共享子网内创建标签。

共享 VPC 计费说明

在共享VPC中，使用者只需要为自己所创建的资源付费，比如ECS、ELB以及RDS实例等。各种资源的计费详情，请参见对应云资源的计费说明。

共享 VPC 的配额限制

共享VPC的各项配额说明如表9-4所示，当前配额项均不支持提升，请合理规划您的资源。

表 9-4 共享 VPC 的配额说明

配额项目	默认配额
单个资源使用者支持接收的共享子网数量	100个
单个子网支持共享至资源使用者的最大数量	100个

共享 VPC 的使用限制

- 单个使用者最多可同时接收100个共享子网，当共享子网数量超过100个时，使用者将无法接收到超出数量的共享子网。
- 单个子网最多可同时共享给100个使用者，当使用者数量超过100个时，超出数量的使用者将无法接收到共享子网。

- 支持在共享VPC子网内创建以下云服务资源：
  - 弹性云服务器 ECS
  - 裸金属服务器 BMS
  - 弹性负载均衡 ELB
  - 云容器引擎 CCE
  - API网关 APIG
  - 分布式消息服务Kafka版
  - 应用管理与运维平台 ServiceStage
  - 微服务引擎 CSE
  - 函数工作流 FunctionGraph
  - 分布式缓存服务 DCS
  - 云数据库 GaussDB
  - 云数据库 TaurusDB
  - 云数据库 GeminiDB (Influx实例)
  - 云数据库 GeminiDB (Redis实例)
  - 云数据库 GeminiDB (Cassandra实例)
  - 云数据库 RDS (for MySQL)
  - 云数据库 RDS (for PostgreSQL)
  - 云数据库 RDS (for SQL Server)
  - 文档数据库服务 DDS
  - 数据加密服务 DEW
  - 数据安全中心 DSC
  - 数据库安全服务 DBSS
  - 云堡垒机 CBH
  - 数据仓库服务 GaussDB(DWS)
  - 数据治理中心 DataArts Studio
  - 云搜索服务 CSS
  - 数据湖探索 DLI
  - 云数据迁移 CDM
  - 云桌面 Workspace

9.2 共享 VPC 配置示例

某企业的云上业务主要分为两类，一类业务需要连接公网，一类业务不需要连接公网。为了规范管理各类资源，该企业使用账号A作为IT管理账号，用来管理基础公共资源，主要包括VPC、子网、路由表等。同时，账号A需要将子网共享给其他账号共同使用（账号B，账号C以及账号D），其他账号可以在子网内创建各自的资源，例如ECS、RDS以及ELB等。共享VPC的业务规划示意图如图9-3所示，详细账号和资源规划请参见表9-5。

图 9-3 共享 VPC 业务规划示意图

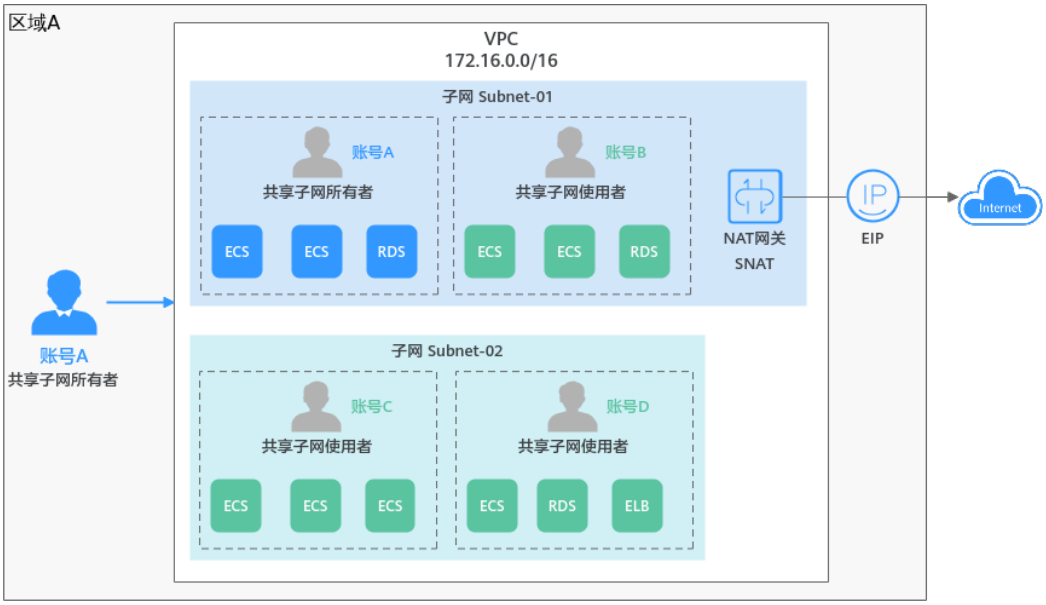


表 9-5 共享 VPC 业务规划说明

账号	账号角色	资源说明
账号A	共享VPC和子网的所有者	• 账号A创建VPC和子网，并将子网共享给其他账号。 • 账号A创建NAT网关以及EIP资源，通过配置SNAT使子网Subnet-01连通公网。
账号B	共享子网的使用者	账号B在子网Subnet-01创建ECS和RDS资源，用来部署面向公网的应用程序。
账号C和账号D	共享子网的使用者	账号C和账号D共同使用子网Subnet-02，在子网内创建各自业务所需的ECS、RDS以及ELB等资源，不需要连通公网。

同一个VPC内的不同子网网络默认互通，但是由于不同账号下的资源需要关联各自的安全组，不同安全组之间网络隔离，因此如果有网络互通需求，需要放通资源对应安全组之间的网络。

- 账号A内的资源属于安全组Sg-A。
- 账号B内的资源属于安全组Sg-B。
- 账号C内的资源属于安全组Sg-C。
- 账号D内的资源属于安全组Sg-D。

如果需要账号C和账号D内的资源网络互通，则需要在Sg-C和Sg-D的入方向分别添加以下规则：

表 9-6 放通 Sg-C 和 Sg-D 的网络

安全组	方向	优先级	策略	类型	协议端口	源地址
Sg-C	入方向	1	允许	IPv4	根据业务需求选择该项。 示例：全部协议	安全组：Sg-D
Sg-D	入方向	1	允许	IPv4	根据业务需求选择该项。 示例：全部协议	安全组：Sg-C

9.3 将 VPC 子网共享给其他账号

操作场景

VPC的所有者可以将VPC内的子网共享给使用者，您可以参考以下操作，将子网添加至已创建的共享中，已创建的共享中设置了子网使用者的权限以及使用者的账号。共享子网成功后，使用者可以在共享子网内创建实例。

前提条件

您需要将子网添加至已有的共享中，因此请确保已创建共享，具体请参见**创建共享**。

约束与限制

- 单个使用者最多可同时接收100个共享子网，当共享子网数量超过100个时，使用者将无法接收到超出数量的共享子网。
- 单个子网最多可同时共享给100个使用者，当使用者数量超过100个时，超出数量的使用者将无法接收到共享子网。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 找到待共享的子网，并单击子网名称超链。
   进入子网“基本信息”页签。

6. 选择“共享管理”页签，单击“共享子网”。
   弹出“共享子网”对话框。
7. 在共享列表中，选择一个可用的共享。
   如果列表中没有可供选择的共享，请执行以下操作，创建共享。
   a. 单击“取消”，关闭“共享子网”对话框。
      返回“共享管理”页签。
   b. 单击“创建共享”。
      进入RAM管理控制台，创建共享，具体请参见**创建共享**。
   c. 共享创建完成后，重新执行**6**~**7**，在已有的共享中添加子网。
8. 共享选择完成后，单击“确定”。
   返回“共享管理”页签，可以在列表中看到已创建的共享，状态为“共享中”，表示已将子网共享给其他账号。

后续操作

将子网共享给其他账号，需要使用者在一定时间内接受共享申请，才可以使用该子网，具体请参见**接受/拒绝共享邀请**。

9.4 查看 VPC 共享子网详情

操作场景

共享子网的所有者和使用者，可以参考以下操作查看共享子网详情，包括该子网加入的共享名称以及共享状态等。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
   - 如果您是共享子网的所有者，子网对应的“所有者项目ID”列显示ID值，例如“06057680XXXa3a509”。
   - 如果您是共享子网的使用者，子网对应的“所有者项目ID”列显示ID值和子网共享状态，例如“0605767829XXXdd2f1148(共享中)”。
5. 找到目标子网，并单击子网名称超链接。
   进入子网“基本信息”页签。
6. 选择“共享管理”页签，在共享列表中，可查看子网加入的共享的名称和状态。
   - 如果您是共享子网的所有者，您可以通过共享名称，在RAM管理控制台，找到对应的共享，查看共享内的资源情况、资源的权限以及资源的使用者，具体操作请参见**查看共享**。

- 如果您是共享子网的使用者，您可以通过共享名称，在RAM管理控制台，找到对应的共享，查看共享内的资源情况、资源的权限以及资源的所有者，具体操作请参见**查看共享给您的资源**。

9.5 停止 VPC 子网共享

操作场景

共享子网的所有者可以参考以下操作停止子网共享，停止共享之后，使用者将无法继续在该子网内创建新的资源，已有资源可以正常使用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
5. 找到待共享的子网，并单击子网名称超链接。
   进入子网“基本信息”页签。
6. 选择“共享管理”页签，在共享列表中，找到目标共享，并单击操作列下的“停止共享”。
   弹出确认对话框。
7. 确认无误后，单击“确定”。
   返回“共享管理”页签，可以在列表中看到已停止的共享，状态为“停止共享”。

10 边缘网关

10.1 边缘网关概述

边缘网关

边缘网关是指在同一个虚拟私有云内，用来连接边缘可用区子网和中心可用区子网、以及不同边缘可用区子网之间的云内网络。

说明

当前“非洲-约翰内斯堡”区域支持边缘网关功能。

边缘网关功能当前暂不收费。待后续启动收费时，将会提前通知您。

边缘网关应用场景

图 10-1 边缘网关组网架构图

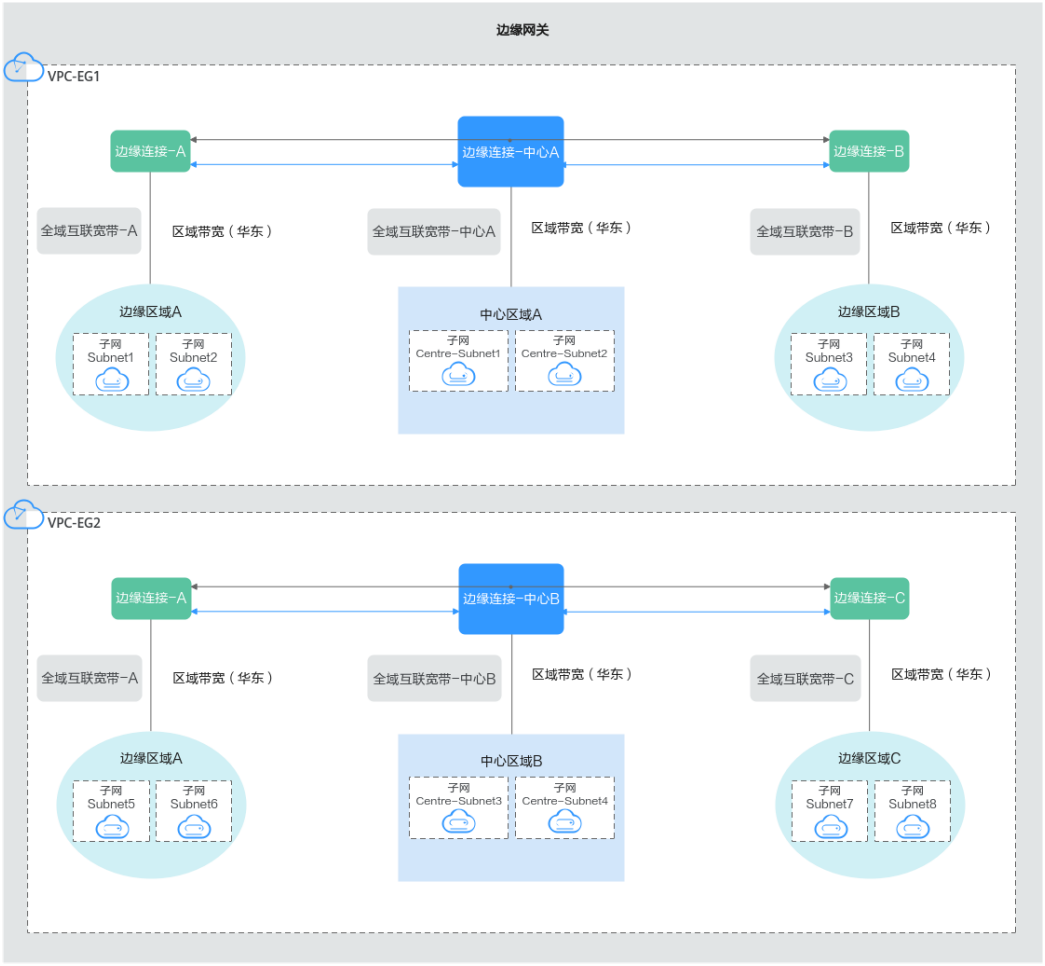


表 VPC及子网资源规划说明介绍了边缘网关云内资源的规划，配置虚拟私有云VPC2个，子网12个，可用区12个，对应区域5个。

表 10-1 VPC 及子网资源规划说明

虚拟私有云	子网	可用区	区域
VPC-EG1	Subnet1	边缘可用区AZ1	边缘区域A
	Subnet2	边缘可用区AZ2	
	Subnet3	边缘可用区AZ3	边缘区域B
	Subnet4	边缘可用区AZ4	
	Centre-Subnet1	中心可用区AZ1	中心区域A
	Centre-Subnet2	中心可用区AZ2	
VPC-EG2	Subnet5	边缘可用区AZ5	边缘区域A

虚拟私有云	子网	可用区	区域
	Subnet6	边缘可用区AZ6	
	Subnet7	边缘可用区AZ7	边缘区域C
	Subnet8	边缘可用区AZ8	
	Centre-Subnet3	中心可用区AZ3	中心区域B
	Centre-Subnet4	中心可用区AZ4	

表 边缘网关及连接资源规划说明介绍了边缘网关内可用区通信资源的规划，配置边缘网关1个，可用区12个，对应区域5个，边缘连接5个，全域互联带宽-区域带宽（华东）5个。

表 10-2 边缘网关及连接资源规划说明

边缘网关	可用区	区域	边缘连接	全域互联带宽-区域带宽（华东）
边缘网关	• 边缘可用区AZ1 • 边缘可用区AZ2 • 边缘可用区AZ5 • 边缘可用区AZ6	边缘区域A	边缘连接-A	全域互联带宽-A
	• 边缘可用区AZ3 • 边缘可用区AZ4	边缘区域B	边缘连接-B	全域互联带宽-B
	• 边缘可用区AZ7 • 边缘可用区AZ8	边缘区域C	边缘连接-C	全域互联带宽-C
	• 中心可用区AZ1 • 中心可用区AZ2	中心区域A	边缘连接-中心A	全域互联带宽-中心A
	• 中心可用区AZ3 • 中心可用区AZ4	中心区域B	边缘连接-中心B	全域互联带宽-中心B

根据**图 边缘网关组网架构图**、**表 边缘网关连接应用场景说明**，同一个边缘网关中关联虚拟私有云VPC-EG1、VPC-EG2，边缘网关主要有以下应用场景。

表 10-3 边缘网关连接应用场景说明

场景说明	所需资源	举例说明	操作指导
虚拟私有云VPC-EG1内，连接边缘可用区子网和中心可用区子网。	• VPC • 边缘可用区子网 • 边缘区域边缘连接 • 边缘区域全域互联带宽 • 中心可用区子网 • 中心区域边缘连接 • 中心区域全域互联带宽	同一个虚拟私有云VPC-EG1内，边缘可用区AZ1子网Subnet1和中心可用区AZ1子网Centre-Subnet1需要云内通信。 • 边缘可用区AZ1子网Subnet1对应的边缘区域A要创建边缘连接（边缘连接-A），并绑定全域互联带宽（全域互联带宽-A）。 • 中心可用区AZ1子网Centre-Subnet1对应的中心区域A要创建边缘连接（边缘连接-中心A），并绑定全域互联带宽（全域互联带宽-中心A）。	1. **购买边缘网关**：购买一个边缘网关，其中可以关联一个或多个虚拟私有云。 2. **在边缘网关中关联虚拟私有云**：在边缘网关中关联虚拟私有云，不同规格的边缘网关支持关联的虚拟私有云数量不同。 3. **创建边缘连接**：创建边缘连接，同一个区域下有不同的可用区，这些可用区共用区域下的同一个边缘连接。 4. **为边缘连接绑定全域互联带宽**：绑定全域互联带宽，每一个边缘连接需要绑定一个全域互联带宽。

场景说明	所需资源	举例说明	操作指导
虚拟私有云VPC-EG1内，连接不同边缘区域子网。	• VPC • 边缘可用区子网 • 边缘区域边缘连接 • 边缘区域全域互联带宽 • 中心区域边缘连接 • 中心区域全域互联带宽	同一个虚拟私有云VPC-EG1内，边缘可用区AZ1子网Subnet1和边缘可用区AZ3子网Subnet3需要云内通信。 • 边缘可用区AZ1子网Subnet1对应的边缘区域A要创建边缘连接（边缘连接-A），并绑定全域互联带宽（全域互联带宽-A）。 • 边缘可用区AZ3子网Subnet3对应的边缘区域B要创建边缘连接（边缘连接-B），并绑定全域互联带宽（全域互联带宽-B）。 • 边缘可用区AZ1和边缘可用区AZ3对应的中心区域A创建边缘连接（边缘连接-中心A），并绑定全域互联带宽（全域互联带宽-中心A）。 **说明** 无论是实现中心区域和边缘区域、还是不同边缘区域之间的通信，都需要创建中心区域对应的边缘连接。	1. **购买边缘网关**：购买一个边缘网关，其中可以关联一个或多个虚拟私有云。 2. **在边缘网关中关联虚拟私有云**：在边缘网关中关联虚拟私有云，不同规格的边缘网关支持关联的虚拟私有云数量不同。 3. **创建边缘连接**：创建边缘连接，本次创建两个边缘区域和一个中心区域的边缘连接。 4. **为边缘连接绑定全域互联带宽**：绑定全域互联带宽，每一个边缘连接需要绑定一个全域互联带宽。
虚拟私有云VPC-EG2内，连接边缘可用区子网和中心可用区子网。	• VPC • 边缘可用区子网 • 边缘区域边缘连接 • 边缘区域全域互联带宽 • 中心可用区子网 • 中心区域边缘连接 • 中心区域全域互联带宽	同一个虚拟私有云VPC-EG2内，边缘可用区AZ5子网Subnet5和中心可用区AZ3子网Centre-Subnet3需要云内通信。 • 边缘可用区AZ5子网Subnet5对应的边缘区域A在VPC-EG1内连接时已经创建了边缘连接和绑定全域互联带宽。此次可以直接使用，不用重新建立。 • 中心可用区AZ3子网Centre-Subnet3对应的中心区域B要创建边缘连接（边缘连接-中心B），并绑定全域互联带宽（全域互联带宽-中心B）。 **说明** 不同虚拟私有云VPC-EG1、VPC-EG2位于同一个边缘网关内时，可以复用边缘连接。	1. **购买边缘网关**：购买一个边缘网关，其中可以关联一个或多个虚拟私有云。 2. **在边缘网关中关联虚拟私有云**：在边缘网关中关联虚拟私有云，不同规格的边缘网关支持关联的虚拟私有云数量不同。 3. **创建边缘连接**：创建边缘连接，同一边缘网关内，不同虚拟私有云可以使用同一个边缘连接。本次仅创建一个中心区域的边缘连接。 4. **为边缘连接绑定全域互联带宽**：绑定全域互联带宽，每一个边缘连接需要绑定一个全域互联带宽。

场景说明	所需资源	举例说明	操作指导
虚拟私有云VPC-EG2内，连接不同边缘区域子网。	• VPC • 边缘可用区子网 • 边缘区域边缘连接 • 边缘区域全域互联带宽 • 中心区域边缘连接 • 中心区域全域互联带宽	同一个虚拟私有云VPC-EG2内，边缘可用区AZ5子网Subnet5和边缘可用区AZ7子网Subnet云内通信。 • 边缘可用区AZ5子网Subnet5对应的边缘区域A在VPC-EG1内连接时已经创建了边缘连接和绑定全域互联带宽。此次可以直接使用，不用重新建立。 • 边缘可用区AZ7子网Subnet7对应的边缘区域C要创建边缘连接（边缘连接-C），并绑定全域互联带宽（全域互联带宽-C）。 • 边缘可用区AZ5和边缘可用区AZ7对应的中心区域B创建边缘连接（边缘连接-中心B），并绑定全域互联带宽（全域互联带宽-中心B）。	1. **购买边缘网关**：购买一个边缘网关，其中可以关联一个或多个虚拟私有云。 2. **在边缘网关中关联虚拟私有云**：在边缘网关中关联虚拟私有云，不同规格的边缘网关支持关联的虚拟私有云数量不同。 3. **创建边缘连接**：创建边缘连接，同一边缘网关内，不同虚拟私有云可以使用同一个边缘连接。本次仅创建一个边缘可用区AZ7对应的边缘连接和一个中心区域的边缘连接。 4. **为边缘连接绑定全域互联带宽**：绑定全域互联带宽，每一个边缘连接需要绑定一个全域互联带宽。

10.2 购买边缘网关

操作场景

您可以参考以下操作购买边缘网关，通过边缘网关和全域互联带宽，可以实现同一个VPC内资源，中心和边缘，边缘和边缘之间的云内网络通信。

说明

当前“非洲-约翰内斯堡”区域支持边缘网关功能。

边缘网关功能当前暂不收费。待后续启动收费时，将会提前通知您。

操作步骤

1. 进入**边缘网关列表页面**。
2. 在页面右上角，单击“购买边缘网关”。
   进入“购买边缘网关”页面。
3. 根据界面提示，配置边缘网关的基本信息，如**表10-4**所示。

表 10-4 参数说明

参数名称	参数说明	取值样例
计费模式	必选参数。 按需计费：后付费。按照边缘网关的使用时长计费。按秒计费，按小时结算，不足一小时以实际使用时长为准。 边缘网关功能当前暂不收费。待后续启动收费时，将会提前通知您。	按需计费
区域	必选参数。 不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	必选参数。 输入全域互联带宽的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	-
规格	必选参数。 选择边缘连接网关的规格，具体说明如下： ● 基础版：基础版边缘网关支持同时添加2个虚拟私有云。 ● 企业版：企业版边缘网关支持同时添加10个虚拟私有云。 ● 企业增强版：企业增强版边缘网关支持同时添加30个虚拟私有云。 边缘网关购买完成后，规格支持修改，具体请参见**修改边缘网关规格**。	基础版
虚拟私有云	必选参数。 在边缘连接中关联虚拟私有云，此处可关联一个或多个虚拟私有云。 关联至边缘网关的虚拟私有云，可以实现中心站点子网和边缘站点子网之间、不同边缘站点子网之间的云内网络通信。 边缘网关购买完成后，支持**新关联虚拟私有云**，或者**解除已关联的虚拟私有云**。	vpc-test01 vpc-test02
高级配置/描述	可选参数。 您可以根据需要在文本框中输入对该边缘网关的描述信息。	-

参数名称	参数说明	取值样例
高级配置/标签	可选参数。 您可以在创建边缘网关的时候为边缘网关绑定标签，标签用于标识云资源，可通过标签实现对云资源的分类和搜索。 关于标签更详细的说明，请参见**管理边缘网关的标签**。	“标签键”：test “标签值”：01

4. 基本信息设置完成后，单击“立即购买”。
5. 在产品配置信息确认页面，再次核对边缘网关的信息，确认无误后，单击“提交订单”。

   返回边缘网关列表页面。
6. 在边缘网关列表页面，查看边缘网关状态。

   当边缘网关状态为“运行中”，表示购买成功。

后续操作

- 必选操作：边缘网关不能单独使用，需要关联虚拟私有云，具体请参见**在边缘网关中关联虚拟私有云**。
- 必选操作：在边缘网关中，创建边缘智能连接，用来连通中心站点和边缘站点、不同边缘站点之间的云内网络，具体请参见**创建边缘连接**。
- 必选操作：需要为边缘连接绑定全域互联带宽才可以实现云内网络通信，每个连接需要一条带宽，具体请参见**为边缘连接绑定全域互联带宽**。

10.3 在边缘网关中关联/解除关联 VPC

操作场景

您可以参考以下操作，在边缘网关中关联或者解除关联虚拟私有云VPC：

- **在边缘网关中关联虚拟私有云**：支持单个关联或者批量关联。不同规格的边缘网关支持关联的虚拟私有云数量不同：
  - 基础版：基础版边缘网关支持同时添加2个虚拟私有云。
  - 企业版：企业版边缘网关支持同时添加10个虚拟私有云。
  - 企业增强版：企业增强版边缘网关支持同时添加30个虚拟私有云。
- **在边缘网关中解除关联虚拟私有云**：支持单个解除或者批量解除，在边缘网关中解除已关联的虚拟私有云时，请确保该虚拟私有云上没有相关业务运行，否则会导致业务中断。

在边缘网关中关联虚拟私有云

1. 进入**边缘网关列表页面**。
2. 在边缘网关列表中，通过搜索或者直接查找，找到目标边缘网关。
3. 单击边缘网关名称超链接。

   进入“基本信息”页签。

4. 选择“虚拟私有云”页签，单击“关联”。
   弹出“关联虚拟私有云”对话框。
5. 在虚拟私有云列表中，关联一个或多个虚拟私有云，并单击“确定”
   返回虚拟私有云列表，可以看到当前边缘网关已关联的虚拟私有云。

在边缘网关中解除关联虚拟私有云

1. 进入**边缘网关列表页面**。
2. 在边缘网关列表中，通过搜索或者直接查找，找到目标边缘网关。
3. 单击边缘网关名称超链接。
   进入“基本信息”页签。
4. 选择“虚拟私有云”页签，在虚拟私有云列表中，解除已关联的虚拟私有云。
   - 解除关联的单个虚拟私有云：
     i. 在虚拟私有云列表中，单击目标虚拟私有云所在行的操作列下的“解除关联”。
        弹出解除关联确认对话框。
     ii. 确认无误后，单击“确定”，解除关联的虚拟私有云。
        返回虚拟私有云列表，已无法看到解除的虚拟私有云。
   - 批量解除关联的虚拟私有云：
     i. 在虚拟私有云列表中，关联多个目标虚拟私有云，并单击列表左上方的“解除关联”。
        弹出解除关联确认对话框。
     ii. 确认无误后，单击“确定”，解除关联的虚拟私有云。
        返回虚拟私有云列表，已无法看到解除的虚拟私有云。

10.4 管理边缘网关

操作场景

您可以参考以下操作，管理您的边缘网关资源：

- **修改边缘网关规格**
- **查看边缘网关信息**
- **删除边缘网关**

约束与限制

- 待删除的边缘网关中不能关联虚拟私有云，否则无法删除，请参考**在边缘网关中解除关联虚拟私有云**处理。
- 待删除的边缘网关中不能存在边缘连接，否则无法删除，请参考**删除边缘连接**处理。

修改边缘网关规格

1. 进入**边缘网关列表页面**。

2. 在边缘网关列表中，通过搜索或者直接查找，找到目标边缘网关。
3. 单击目标边缘网关所在行的操作列下的“修改规格”。
   进入“修改规格”页面。
4. 根据界面提示，为边缘网关选择新的规格。
   选择边缘连接网关的规格，具体说明如下：
   - 基础版：基础版边缘网关支持同时添加2个虚拟私有云。
   - 企业版：企业版边缘网关支持同时添加10个虚拟私有云。
   - 企业增强版：企业增强版边缘网关支持同时添加30个虚拟私有云。
5. 修改完成后，单击“下一步”。
6. 在修改规格确认页面，再次核对边缘网关的信息，确认无误后，单击“提交订单”。
   返回边缘网关列表，可以看到边缘网关的规格已刷新。

查看边缘网关信息

1. 进入**边缘网关列表页面**。
2. 在边缘网关列表中，通过搜索或者直接查找，找到目标边缘网关。
3. 单击边缘网关名称超链接。
   进入“基本信息”页签，查看更多信息。

删除边缘网关

1. 进入**边缘网关列表页面**。
2. 在边缘网关列表中，通过搜索或者直接查找，找到目标边缘网关。
3. 单击目标边缘网关所在行的操作列下的“删除”。
   弹出删除确认对话框。
4. 确认无误后，单击“确定”，删除边缘网关。
   返回边缘网关列表，已无法看到删除的边缘网关。

10.5 管理边缘网关的标签

操作场景

标签用于标识云资源，您可以通过标签实现对边缘网关资源的分类和搜索。您可以参考以下操作管理边缘网关标签：

- 添加边缘网关标签
- 修改边缘网关标签
- 删除边缘网关标签

边缘网关标签规则的详细说明，请参见**表10-5**。

表 10-5 边缘网关标签命名规则

参数	规则	样例
键	• 对于云资源，每个“标签键”都必须是唯一的，每个“标签键”只能有一个“标签值”。 • 不能为空。 • 最大长度不超过128个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格、不能以_sys_开头。	test
值	• 可以为空。 • 最大长度不超过255个字符。 • 由任意语种字母、数字、空格、“_”、“.”、“:”、“/”、“=”、“+”、“-”、“@”组成。 • 首尾不能含有空格。	01

约束与限制

每个云资源最多可以添加20个标签。

操作步骤

1. 进入**边缘网关列表页面**。
2. 选择“标签”页签，在标签列表左上方，单击“编辑标签”。
   进入“编辑标签”页面。
3. 根据需要，参考以下步骤对标签执行对应的操作。
   - 添加标签：单击+，在文本框中输入标签键和标签值对应的取值，并单击“确定”。
   - 修改标签：单击目标标签键或者标签值后方的×，删掉原有取值，输入新的取值，并单击“确定”。
   - 删除标签：单击目标标签后方的“删除”，并单击“确定”。

10.6 创建边缘连接

操作场景

您可以参考以下操作创建边缘连接，边缘连接用来连通VPC内中心可用区子网和边缘可用区子网、以及不同边缘可用区子网之间的云内网络。

约束与限制

- 边缘连接需要绑定全域互联带宽，通过全域互联带宽实现中心站点和边缘站点、以及不同边缘站点之间的网络通信。
- 无论是实现中心区域和边缘区域、还是不同边缘区域之间的通信，都需要创建中心区域对应的边缘连接，边缘区域对应的连接请根据实际通信需要创建。

  例如，同一虚拟私有云VPC-EG1内，不同区域中，边缘可用区AZ1子网Subnet1和边缘可用区AZ3子网Subnet3通信，此时您需要创建中心可用区AZ1、边缘可用区AZ1以及边缘可用区AZ3各自对应边缘区域的边缘连接。
- 不同虚拟私有云位于同一个边缘网关内时，可以复用边缘连接。

  例如，边缘网关内关联VPC-EG1和VPC-EG2，边缘可用区AZ5子网Subnet5和中心可用区AZ3子网Centre-Subnet3通信，边缘可用区AZ1对应的边缘区域A已经创建边缘连接-A，边缘可用区AZ5属于边缘区域A，此次可以直接使用，不用重新建立。只需建立中心可用区AZ3对应区域的边缘连接，并且绑定全域互联带宽。

表 10-6 示例资源配置

边缘网关	虚拟私有云	子网	可用区	对应区域	边缘连接	全域互联带宽-区域带宽（华东）
边缘网关	VPC-EG1	Subnet1	边缘可用区AZ1	边缘区域A	边缘连接-A	全域互联带宽-A
		Subnet3	边缘可用区AZ3	边缘区域B	边缘连接-B	全域互联带宽-B
		Centre-Subnet1	中心可用区AZ1	中心区域A	边缘连接-中心A	全域互联带宽-中心A
	VPC-EG2	Subnet5	边缘可用区AZ5	边缘区域A	边缘连接-A	全域互联带宽-A
		Centre-Subnet3	中心可用区AZ3	中心区域B	边缘连接-中心B	全域互联带宽-中心B

操作步骤

1. 进入**边缘网关列表页面**。
2. 单击边缘网关名称超链接。

   进入“基本信息”页签。
3. 选择“边缘连接”页签，单击“创建边缘连接”。

   弹出“创建边缘连接”对话框。
4. 根据界面提示，创建边缘连接的基本信息，如**表10-7**所示。

表 10-7 参数说明

参数名称	参数说明	取值样例
名称	必选参数。 输入边缘连接的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	-
可用区	必选参数。 相同公网边界组的可用区只可以创建一个边缘连接。 具有相同公网边界组的可用区位于同一个边缘站点内，您可以选择同一个边缘站点内的任意一个可用区创建边缘连接。	-
描述	可选参数。 您可以根据需要在文本框中输入对该边缘连接的描述信息。	-

5. 参数设置完成，单击“确定”。

后续操作

需要为边缘连接绑定全域互联带宽才可以实现云内网络通信，每个连接需要一条带宽，具体请参见**为边缘连接绑定全域互联带宽**。

10.7 为边缘连接绑定/解绑全域互联带宽

操作场景

您可以参考以下操作，为边缘连接绑定/解绑全域互联带宽：

- **为边缘连接绑定全域互联带宽**：通过全域互联带宽实现中心站点和边缘站点、以及不同边缘站点之间的网络通信。
- **为边缘连接解绑全域互联带宽**：为边缘连接解绑全域互联带宽时，请确保该连接上没有相关业务运行，否则会导致业务中断。

同时，您还可以参考**修改边缘连接绑定的全域互联带宽**，修改带宽名称和大小等信息。

为边缘连接绑定全域互联带宽

1. 进入**边缘网关列表页面**。
2. 单击边缘网关名称超链接。
   进入“基本信息”页签。
3. 选择“边缘连接”页签，在边缘连接列表中，通过搜索或者直接查找，找到目标边缘连接。

4. 在目标边缘连接右侧单击“绑定全域互联带宽”，
   弹出绑定确认对话框。
5. 根据页面提示，选择合适的全域互联带宽，单击“确定”。

   说明

   如果没有可用的全域互联带宽，需要购买全域互联带宽，具体操作为**购买全域互联带宽**。
6. 查看目标边缘连接右侧“绑定全域互联带宽”，链接变成灰色状态，说明绑定成功。

为边缘连接解绑全域互联带宽

1. 进入**边缘网关列表页面**。
2. 单击边缘网关名称超链接。
   进入“基本信息”页签。
3. 选择“边缘连接”页签，在边缘连接列表中，通过搜索或者直接查找，找到目标边缘连接。
4. 单击目标边缘连接所在行右侧的操作列下的“更多>解绑全域互联带宽”，
   弹出解绑确认对话框。
5. 确认无误后，单击“确定”，解绑关联的全域互联带宽。
6. 查看目标边缘连接右侧“绑定全域互联带宽”，链接变成黑色状态，说明解除绑定成功。

修改边缘连接绑定的全域互联带宽

您可以修改边缘连接绑定的全域互联带宽，包括带宽名称和带宽大小等信息。

具体操作请参见**修改全域互联带宽**。

10.8 管理边缘连接

操作场景

您可以参考以下操作，管理您的边缘连接资源：

- **查看边缘连接**
- **删除边缘连接**

约束与限制

待删除的边缘连接中不能绑定全域互联带宽，否则无法删除，请参考**为边缘连接解绑全域互联带宽**处理。

查看边缘连接

1. 进入**边缘网关列表页面**。
2. 单击边缘网关名称超链接。
   进入“基本信息”页签。
3. 选择“边缘连接”页签，在边缘连接列表中，您可以查看边缘连接对应的可用区名称以及绑定的全域互联带宽。

删除边缘连接

1. 进入**边缘网关列表页面**。
2. 单击边缘网关名称超链接。
   进入“基本信息”页签。
3. 选择“边缘连接”页签，单击目标边缘连接所在行右侧的操作列下的“更多>删除”，
   弹出删除确认对话框。
4. 确认无误后，单击“确定”，删除边缘连接。
   返回边缘连接列表，已无法看到删除的边缘连接。

11 IPv4/IPv6 双栈网络

IPv4/IPv6 双栈网络介绍

IPv4/IPv6双栈网络，表示为您的实例提供两个版本的IP地址，包括IPv4 IP地址和IPv6 IP地址。以ECS为例，IPv4/IPv6双栈网络架构如图11-1所示。

图 11-1 IPv6 双栈网络架构图(VPC/EIP)

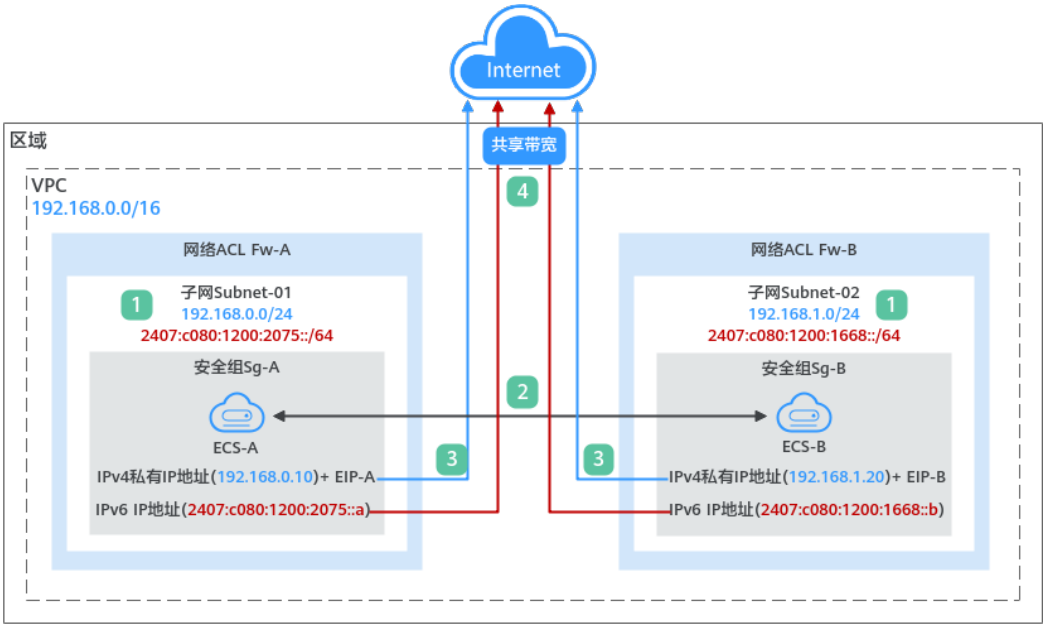


表 11-1 IPv6 双栈网络构建说明(VPC/EIP)

步骤	说明
1	在创建虚拟私有云VPC子网时，开启IPv6功能，则系统会自动为子网分配IPv6网段，当前不支持自定义IPv6网段。

步骤	说明
2	相同VPC内的不同子网之间网络默认互通，网络ACL可以防护子网的网络安全，安全组防护实例的网络安全。 1. 不同网络ACL之间网络隔离，如果两个子网关联了不同的网络ACL，则需要添加规则放通不同的网络ACL。 2. 不同安全组之间网络隔离，实例都必须关联安全组，如果两个实例关联了不同的安全组，则需要添加规则放通不同的安全组。 当网络ACL和安全组均放通后，实例之间可以内网互通，即ECS-A和ECS-B通过内网可以互相通信。 ● 使用IPv4私有IP地址，实现ECS内网通信。 ● 使用IPv6 IP地址，实现双栈ECS内网通信。
3	实现IPv4公网通信时，需要创建弹性公网IP(EIP)，并将EIP绑定到实例上。一个EIP可以绑定一个实例。 比如，将EIP-A绑定至ECS-A，ECS-A可以通过EIP-A连通公网。将EIP-B绑定至ECS-B，ECS-B可以通过EIP-B连通公网。
4	实现IPv6公网通信时，需要创建EIP共享带宽，并将实例的IPv6地址添加至共享带宽即可。一个共享带宽中可以添加多个IP。 比如，将ECS-A和ECS-B的IPv6地址分别添加至共享带宽中，ECS-A和ECS-B可以通过IPv6地址连通公网。

约束与限制

- 当前IPv4/IPv6双栈网络暂不收费，后续定价会根据运营商收费策略的变化进行调整。
- 云耀云服务器L实例、旧版云耀云服务器不支持IPv6网络。
- IPv6功能目前仅在部分区域公测，具体公测区域请参见**功能总览**中“IPv4/IPv6双栈”功能的发布区域。申请公测权限后，才可以体验IPv6功能。
- 弹性云服务器ECS部分规格支持IPv6网络，只有选择支持IPv6的ECS，才可以使用IPv4/IPv6双栈网络。

  在ECS控制台，单击“购买弹性云服务器”，进入购买页面查看ECS规格列表。当ECS规格列表中包含“IPv6”参数，且取值为“是”时，表示该规格的ECS支持IPv6网络。

图 11-2 ECS 规格列表

IPv4/IPv6 双栈网络的应用场景

当您的ECS规格支持IPv6，您可以搭建IPv4/IPv6双栈网络实现内网和公网通信。IPv4/IPv6双栈网络的应用场景说明和资源规划如表11-2所示。

表 11-2 IPv4/IPv6 双栈网络的应用场景及资源规划

应用场景	场景说明	子网	ECS
IPv6内网通信	您在ECS上部署应用，需要与其他系统（比如数据库）之间使用IPV6进行内网互访	• IPv4网段 • IPv6网段	• IPv4私有地址：用于IPv4内网通信 • IPv6地址：用于IPv6内网通信
IPv6公网通信	您在ECS上部署应用并面向公网客户端提供服务，支持客户端通过IPv6地址访问	• IPv4网段 • IPv6网段	• IPv4私有地址+IPv4 EIP地址：用于IPv4公网通信 • IPv6地址+共享带宽：用于IPv6公网通信
	您在ECS上部署应用并面向公网客户端提供服务，既要支持客户端通过IPv6地址访问，还要对这些访问来源进行数据分析		

如果您的ECS规格不支持IPv6，您可以通过开启EIP的IPv6转换功能，实现IPv6公网通信，具体如表11-3所示。

表 11-3 IPv6 EIP 的应用场景及资源规划

应用场景	场景示例	子网	ECS
IPv6公网通信	您在ECS上部署应用并面向公网客户端提供服务，支持客户端通过IPv6地址访问	IPv4网段	• IPv4私有地址 • IPv4 EIP地址（开启IPv6转换）：用于IPv4和IPv6公网通信

图 11-3 IPv6 网络应用场景及资源规划

IPv6 网络操作指导

IPv6网络的操作与IPv4网络基本相同，仅部分功能配置存在差异，**表11-4**中为您提供IPv6网络配置指导。

表 11-4 IPv6 网络操作指导

操作场景	说明	指导
创建IPv6子网	创建子网时，勾选“开启IPv6”，则系统会自动为子网分配IPv6网段。 • 暂不支持自定义IPv6网段。 • 子网的IPv6功能开启后暂不支持关闭。 • 对于已创建完成的子网，如果未开启IPv6功能，您可以选择开启。	**为虚拟私有云创建新的子网**
查看子网中已使用的IPv6地址	在子网列表中单击子网名称，在“IP地址管理”页签可以查看已经使用的IPv4地址和IPv6地址。	**查看子网内IP地址的用途**
添加IPv6安全组规则	添加安全组规则时，类型选择“IPv6”，源地址/目的地址填写IPv6地址。	**添加安全组规则**
添加IPv6网络ACL规则	添加网络ACL规则时，类型选择“IPv6”，源地址/目的地址填写IPv6地址。	**添加网络ACL规则**
购买IPv6弹性公网IP	在购买EIP时，勾选“IPv6转换”，或者在EIP列表中，为已有IPv4 EIP执行“开启IPv6转换”操作。开启IPv6转换后，则系统为您提供IPv4和IPv6 EIP地址。	**IPv6弹性公网IP**
将IPv6弹性公网IP/IPv6地址添加到公网带宽中	购买共享带宽后，可以将IPv6 EIP地址或者实例的IPv6地址添加到共享带宽中。	**添加弹性公网IP到共享带宽**
在VPC路由表中添加IPv6自定义路由	添加自定义路由时，目的地址和下一跳地址可以配置IPv4网段或IPv6网段。 • 如果目的地址是IPv6网段，则下一跳地址暂时只能使用同一VPC内的地址。 • 路由的目的地址为IPv6网段时，对应下一跳类型仅支持ECS实例、扩展网卡、虚拟IP，同时下一跳资源需要具备IPv6地址。	**在路由表中添加路由**
申请IPv6虚拟IP地址	当VPC子网开启IPv6后，申请虚拟IP时，类型可以选择“IPv6”。	**申请虚拟IP地址**

12 VPC 流日志

12.1 VPC 流日志概述

VPC 流日志

使用VPC流日志功能，可以帮您采集指定VPC内网络实例的流量信息，包括入方向和出方向的流量。创建流日志后，您可以在配置的日志组中查看流日志记录。

通过流日志功能，可以满足以下业务场景的需求：

- 监控安全组和网络ACL的流量，帮您优化安全组和网络ACL的控制规则。
- 监控网络实例的流量情况，可以进行网络攻击分析等。
- 用于判断网络接口上出入流量的方向。

系统采集流日志数据不会影响您实际网络的吞吐量或者时延等，您可以根据需求创建或者删除流日志，不会对实际运行的网络造成任何风险。

须知

VPC流日志功能目前部分区域支持，具体请打开**VPC功能总览**，并选择“VPC流日志”查看。

VPC流日志本身是免费的，您只需要为使用过程中用到的其他云资源付费。 例如，数据存储在云日志服务中，将按日志服务的标准收费，详情请参见**《云日志服务用户指南》**。

VPC 流日志数据说明

您可以为网卡、子网、虚拟私有云创建流日志。如果流日志的采集对象是子网或者虚拟私有云，则会监控子网或者虚拟私有云内的每个网络接口。

被监控的网络接口的流量将会被采集，生成流日志数据，流日志数据中包括流量的网卡ID，源地址、目的地址、源端口、目标端口以及数据包大小等字段。

表 12-1 流日志字段说明

字段	说明	示例
version	VPC流日志版本。	1
project-id	流日志采集对象所在的项目ID。	5f67944957444bd6bb4fe3b367de8f3d
interface-id	流日志数据所属的网卡ID。	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	源地址。	192.168.0.154
dstaddr	目的地址。	192.168.3.25
srcport	源端口。	38929
dstport	目标端口。	53
protocol	IANA协议编号。有关更多信息，请参阅**Internet协议编号**。	17
packets	数据包的数量。	1
bytes	数据包的大小。	96
start	捕获窗口启动的时间，采用Unix秒的格式。	1548752136
end	捕获窗口结束的时间，采用Unix秒的格式。	1548752736
action	与流量关联的操作： • ACCEPT：安全组或网络ACL允许记录的流量。 • REJECT：安全组或者网络ACL拒绝记录的流量。	ACCEPT
log-status	流日志的日志记录状态： • OK：数据正常记录到选定目标。 • NODATA：捕获窗口中没有传入或传出符合“采集类型”的网卡的网络流量。 • SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。 示例： 如果您创建VPC流日志时设置“采集类型”为“接受”，当有接受流量时，“log-status”将显示为“OK”。当没有接受的流量时，不管是否有拒绝的流量，“log-status”都将显示为“NODATA”。当有一些接受流量异常跳过时，“log-status”将显示为“SKIPDATA”。	OK

VPC 流日志的使用限制

- 目前支持采集流日志的云服务器规格类型为S2、M2、Hc2、H2、D2、P1、G3、Pi1、fp1、S3、C3、M3、H3、D3、Ir3、I3、Sn3、S6、E3、C3ne、M3ne、G5、P2v、Ai1、C6、M6、D6。

  弹性云服务器类型具体信息请参见**实例类型**。
- 一个用户在单个区域内，最多可创建10个VPC流日志。

12.2 创建 VPC 流日志

操作场景

创建VPC流日志，记录虚拟私有云中的流量信息。

前提条件

在创建VPC流日志前，请确保您在云日志服务完成了如下配置：

- 创建日志组。
- 创建日志流。

云日志服务更多内容请参见**《云日志服务用户指南》**。

操作步骤

1. 进入**VPC流日志列表页面**。
2. 在页面右上角，单击“创建流日志”，按照提示配置参数。

表 12-2 参数说明

参数	说明	取值样例
名称	VPC流日志的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	flowlog-495d
资源类型	选择要采集流量的资源类型，目前支持以下类型： ● 网卡 ● 子网 ● 虚拟私有云	网卡

参数	说明	取值样例
选择资源	选择需要采集流量信息的具体资源。 **说明** 建议您选择处于开机状态的弹性云服务器。如果选择了关机状态的弹性云服务器，请在VPC流日志创建完成后，重启弹性云服务器，以便准确的记录网卡流量。	-
采集类型	• 全部：采集指定资源的全部流量。 • 接受：采集指定资源被安全组或网络ACL允许的流量。 • 拒绝：采集指定资源被网络ACL拒绝的流量。	全部
日志组	选择在云日志服务中创建的日志组。	lts-group-abc
日志流	选择在云日志服务中创建的日志流。	lts-topic-abc
描述	VPC流日志的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

说明

同一个资源在同一个日志组的同一个日志流下，只能有两个不同采集类型的VPC流日志。不能重复创建相同的VPC流日志。

3. 参数设置完成后，单击“立即创建”。

   返回VPC流日志列表，可以看到刚创建的VPC流日志。

12.3 查看 VPC 流日志

操作场景

您可以参考以下操作，查看流日志记录详情。

流日志的捕获窗口大约为10分钟，即每10分钟输出一次流日志记录。所以流日志创建完成后，您需要等待大约10分钟，才能查看流日志记录详情。

说明

如果流日志开启之后，无法采集到流日志，可能是以下情况：

- 弹性云服务器处于关机状态时，不显示流日志记录。
- 流日志采集配额不足，如果您希望继续采集流日志，请**设置日志配额**。

操作步骤

1. 进入**VPC流日志列表页面**。
2. 找到需要查看的流日志，单击操作列的“查看日志”，在云日志服务中查看流日志记录。

流日志格式：

```
<version> <project-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>
```

表12-3中为您提供流日志示例。

表 12-3 流日志示例说明

场景	示例
在捕获窗口中正常记录数据的流日志记录	VPC流日志版本为1，在2019年01月29日16:55:36-17:05:36这10分钟内，网卡（1d515d18-1b36-47dc-a983-bd6512aed4bd）允许流过的流量信息，由源端IP地址和端口（192.168.0.154，38929）通过UDP协议向目的端IP地址和端口（192.168.3.25，53）传输了1个数据包，所有数据包的大小为96 byte。 1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
在捕获窗口中未记录数据的流日志记录	1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - - - - 1431280876 1431280934 - NODATA
在捕获窗口中跳过了数据的流日志记录	1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - - - - 1431280876 1431280934 - SKIPDATA

同时，您也可以在云日志服务的日志流详情页面，在搜索框中通过关键字搜索日志。

12.4 开启/关闭 VPC 流日志

操作场景

创建完VPC流日志后，VPC流日志功能会自动开启。当您不需要记录流量数据时，您可以关闭对应的VPC流日志。关闭的VPC流日志，支持再次开启。

约束与限制

- 流日志开启后，系统将会在下个日志采集周期内开始采集流日志数据。
- 流日志关闭后，系统将会在下个日志采集周期内停止采集流日志数据。对于已经生成的流日志数据，仍然会正常上报。

操作步骤

1. 进入**VPC流日志列表页面**。
2. 在VPC流日志列表中，找单击目标流日志所在行的操作列下的“开启”或“关闭”。

   弹出操作确认对话框。

3. 信息确认无误后，单击“确定”，开启或关闭VPC流日志。

12.5 删除 VPC 流日志

操作场景

您可以参考以下操作，删除不用的VPC流日志。删除VPC流日志不会删除云日志服务中的流日志记录。

说明

如果VPC流日志关联的网卡已删除，则对应的VPC流日志会自动删除。但不会删除流日志记录。

操作步骤

1. 进入**VPC流日志列表页面**。
2. 在VPC流日志列表中，找单击目标流日志所在行的操作列下的“更多 > 删除”。
   弹出删除确认对话框。
3. 信息确认无误后，单击“确定”，删除流日志。

13 流量镜像

13.1 流量镜像概述

流量镜像

VPC流量镜像功能可以镜像指定镜像源实例（如弹性网卡）符合筛选条件的报文。您需要设置入方向和出方向的筛选条件，经过镜像源实例的流量符合筛选条件时，将被镜像到指定的镜像目的实例（如云服务器网卡或者弹性负载均衡ELB），适用于网络流量检查、审计分析以及问题定位等场景。

须知

流量镜像功能当前暂不收费。待后续启动收费时，将会提前通知您。

目前部分区域支持流量镜像功能，具体请打开**功能总览**，并选择“流量镜像”查看。

流量镜像概念

首先，为您介绍流量镜像功能中的基础概念：

- 筛选条件：筛选条件包含入方向规则和出方向规则，规则由优先级、流量采集策略以及匹配条件组成。
  - 入方向规则：用来匹配镜像源接收到的流量。
  - 出方向规则：用来匹配镜像源发送出去的流量。
- 镜像源：镜像源为弹性网卡，表示需要镜像该弹性网卡的流量。
- 镜像目的：镜像目的为云服务器网卡或者弹性负载均衡实例，用来接受镜像的流量。
- 镜像会话：使用流量镜像功能，您需要创建镜像会话，通过在镜像会话中关联筛选条件、镜像源和镜像目的，将镜像源符合筛选条件的流量镜像到镜像目的实例。

流量镜像工作原理

以下为您介绍流量镜像的工作原理，以图13-1为例，在镜像会话中，关联了两个镜像源，一个筛选条件以及一个镜像目的，详细介绍如下：

- 镜像源01是弹性网卡-B，弹性网卡-B属于ECS-B。本示例中，ECS-B访问ECS-A，需要镜像弹性网卡-B的出方向和入方向流量。
- 镜像源02是弹性网卡-C，弹性网卡-C属于ECS-C。本示例中，公网客户端访问ECS-C，需要镜像弹性网卡-C的入方向和出方向流量。
- 筛选条件包含流量的入方向规则和出方向规则。
- 镜像目的使用弹性负载均衡ELB实例，用来接受镜像的流量。

在表13-1中，以镜像源弹性网卡-B和弹性网卡-C为例，为您介绍网络流量的镜像原理。

图 13-1 流量镜像架构图

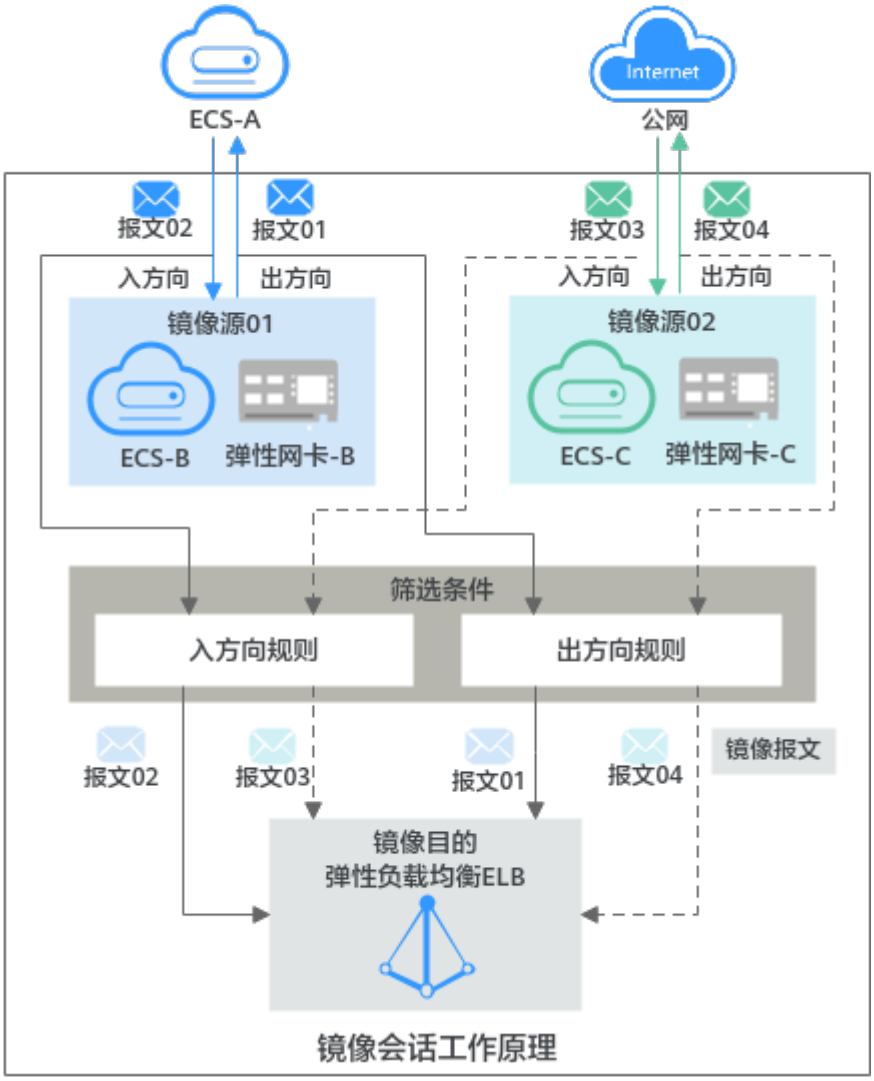


表 13-1 网络流量的镜像路径说明

镜像源	访问路径	报文	方向	说明
弹性网卡-B	ECS-B访问ECS-A	请求报文：报文01	出方向	从ECS-B发出的请求报文01，对弹性网卡-B来说，属于出方向。当报文01匹配上筛选条件的出方向规则时，则将报文01镜像到ELB实例。
		响应报文：报文02	入方向	从ECS-A返回的响应报文02，对弹性网卡-B来说，属于入方向。当该报文匹配上筛选条件的入方向规则时，则将报文02镜像到ELB实例。
弹性网卡-C	公网访问ECS-C	请求报文：报文03	入方向	从公网发出的请求报文03，对弹性网卡-C来说，属于入方向。当报文03匹配上筛选条件的入方向规则时，则将报文03镜像到ELB实例。
		响应报文：报文04	出方向	从ECS-C返回的响应报文04，对弹性网卡-C来说，属于出方向。当报文04匹配上筛选条件的出方向规则时，则将报文04镜像到ELB实例。

筛选条件配置示例如**表13-2**所示，结合配置示例，为您介绍镜像会话是如何筛选网络流量的。

表 13-2 流量筛选说明

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围	筛选示例说明
入方向	1	TCP	采集	IPv4	172.16.0.0/24	10000-10001	10.0.0.3/32	80-80	当网络流量进入镜像源的弹性网卡时，镜像会话将会镜像符合以下条件的报文： 使用TCP (IPv4)协议，源地址网段为172.16.0.0/24、源端口为10000或者10001，目的地址为10.0.0.3/32、目的端口为80。
出方向	1	全部	不采集	IPv4	192.168.0.0/24	全部	10.2.0.0/24	全部	当网络流量从镜像源的弹性网卡出去时，镜像会话将不会镜像符合以下条件的报文： 使用全部 (IPv4)协议，源地址网段为192.168.0.0/24、源端口为全部，目的地址网段为10.2.0.0/24、目的端口为全部。

流量镜像应用场景

- 网络流量检查：

  当您需要进行网络入侵检测时，通过流量镜像功能可以镜像您所需的网络流量。获取到流量后，您可以使用安全软件对流量进行全面分析检查，快速查找安全漏洞，确保网络安全。

- 网络流量审计：

  通过流量镜像功能，您可以将流量镜像到指定的平台进行审计分析，适用于金融等对安全性要求比较高的业务场景。

- 网络问题定位：

  通过流量镜像功能，运维工程师直接查看镜像的流量来排查问题，而不用通过业务服务器抓取报文，避免了运维期间可能对业务造成的影响。

流量镜像匹配规则

根据流量镜像的匹配规则，当同一个镜像源的同一个报文同时符合多个筛选条件规则时，该报文也仅会被匹配一次，匹配原则详细说明如下：

表 13-3 流量镜像匹配规则

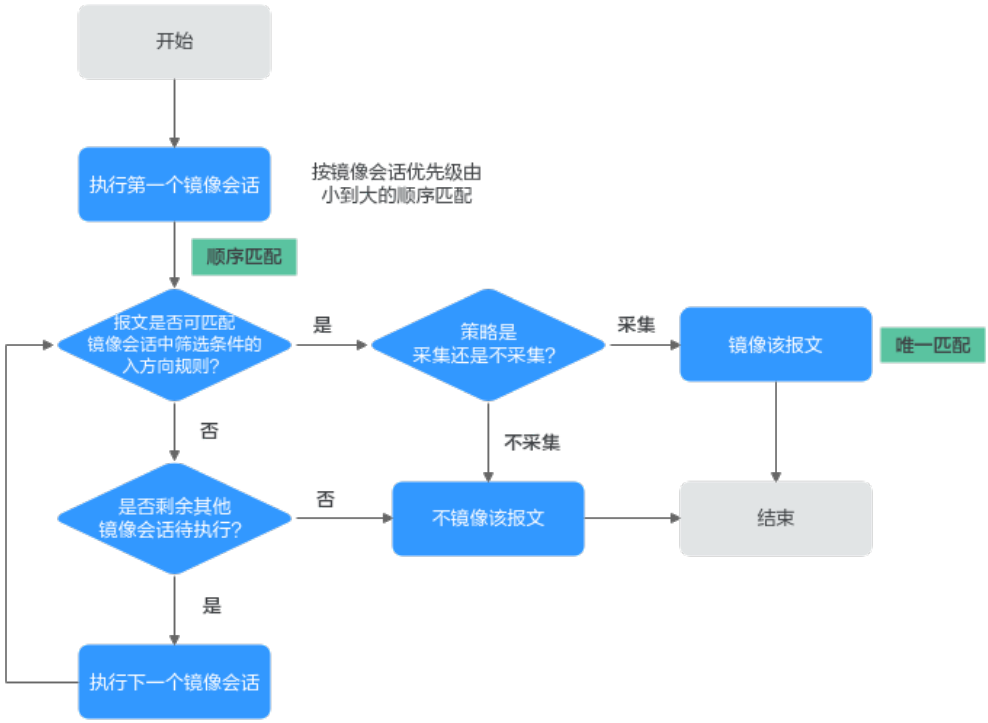
匹配原则	说明
顺序匹配	根据优先级从高到低按顺序进行匹配。优先级的数字越小，优先级越高，比如1的优先级高于2。 • 镜像会话优先级：同一个镜像源可同时被关联至多个镜像会话，此时根据镜像会话的优先级，按照从高到低的顺序匹配。 镜像会话的匹配规则请参见**镜像会话的匹配规则**。 • 筛选条件规则优先级：一个镜像会话只可以关联一个筛选条件，一个筛选条件中可以包含多个规则，此时根据规则的优先级，按照从高到低的顺序匹配。 筛选条件规则分为入方向规则和出方向规则，包含优先级、流量采集策略以及匹配条件。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。
唯一匹配	报文只要与一个筛选条件规则匹配，就不会再去尝试匹配其他规则。

- 镜像会话的匹配规则如**图13-2**所示。当一个镜像源同时被多个镜像会话关联时，以入方向的报文为例，报文根据镜像会话的优先级，按照从高到低的顺序匹配。
  - 当报文匹配上某个镜像会话中的筛选条件入方向规则，则执行以下操作：
    - 如果该规则的策略是采集，则镜像该报文。
    - 如果该规则的策略是不采集，则不会镜像该报文。
  - 当遍历了所有镜像会话中的筛选条件入方向规则，报文均没有匹配上，则不会镜像该报文，结束。

  示例：某个镜像源同时被镜像会话A和镜像会话B关联，镜像会话A的优先级是1，镜像会话B的优先级是2。当镜像源入方向的某个报文同时符合镜像会话A和镜像

会话B里的筛选条件规则，此时根据镜像会话优先级，该报文优先匹配镜像会话A中的筛选条件规则，并执行该规则的采集策略，结束后，该报文不会继续匹配镜像会话B。

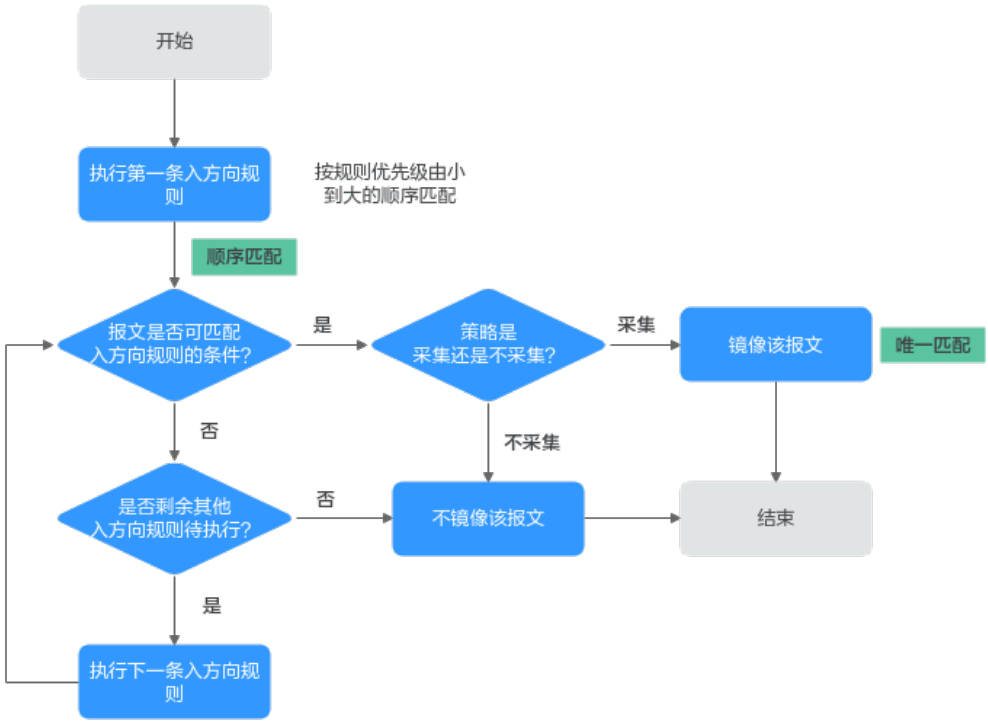
图 13-2 镜像会话匹配规则



- 筛选条件的匹配规则如图13-3所示。当一个镜像源只被一个镜像会话关联时，以入方向的报文为例，报文根据入方向规则的优先级，按照从高到低的顺序匹配：
  - 当报文匹配上筛选条件的某个入方向规则，则执行以下操作：
    - 如果该规则的策略是采集，则镜像该报文。
    - 如果该规则的策略是不采集，则不会镜像该报文。
  - 当遍历了筛选条件中的所有入方向规则，报文均没有匹配上，则不会镜像该报文，结束。

  示例：当某个镜像源被镜像会话A关联，在镜像会话A的筛选条件中，入方向规则A和规则B的流量匹配条件相同，但优先级和流量采集策略不同。规则A的优先级为1，策略为不采集。规则B的优先级为2，策略为采集。当镜像源入方向的某个报文同时符合规则A和规则B的流量匹配条件时，此时根据规则优先级，该报文优先匹规则A，并执行不采集策略，即不镜像该报文，结束后，该报文不会继续匹配规则B。

图 13-3 筛选条件匹配规则



流量镜像的配额限制

流量镜像功能的各项配额说明如**表13-4**所示，部分默认配额可以提升，您可以根据提示申请扩大配额。

表 13-4 流量镜像的配额说明

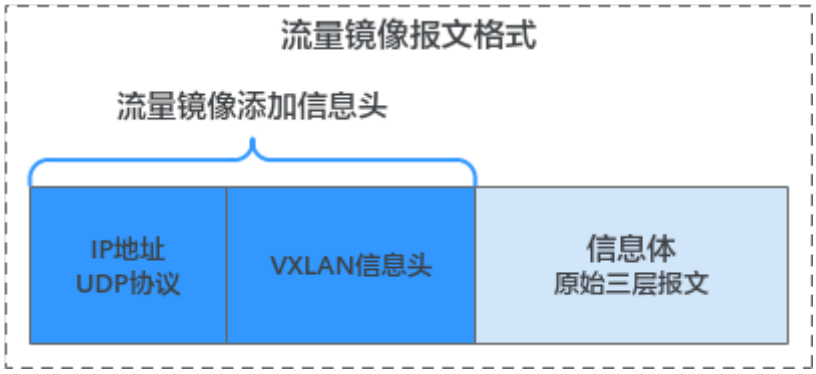
配额项目	默认配额	申请扩大配额
单个镜像会话可关联的镜像源数量	10个	申请更多配额，请参见**管理VPC配额**
单个镜像源可被关联的镜像会话数量	3个	不支持修改
单个镜像会话可关联的镜像目的数量	1个	不支持修改
单个镜像目的可被关联的镜像会话数量	• 镜像目的为云服务器网卡时：10个 • 镜像目的为弹性负载均衡时：200个	不支持修改
单个镜像会话可关联的筛选条件数量	1个	不支持修改
单个筛选条件可被关联的镜像会话数量	1000个	不支持修改

配额项目	默认配额	申请扩大配额
单个筛选条件可添加的规则数量	• 入方向规则：10个 • 出方向规则：10个	不支持修改
一个用户在单个区域可创建的镜像会话数量	20000个	不支持修改

流量镜像的使用限制

- 如图13-4所示，流量镜像的报文采用标准的VXLAN报文格式封装。当被镜像的报文长度加上VXLAN报文长度大于镜像源实例的MTU值时，系统会对报文进行截断。为了防止报文被截断，建议您在IPv4场景下，设置弹性网卡的MTU值比链路支持的MTU值至少小64字节。

图 13-4 流量镜像报文格式



- 表13-5和表13-6中为您提供了不同类型镜像源和镜像目的详细限制说明。

表 13-5 镜像源限制说明

镜像源类型	约束与限制
弹性网卡	• 当镜像源为弹性网卡时，弹性网卡需要绑定至ECS，当前流量镜像仅支持部分规格ECS的弹性网卡作为镜像源，包括c7t、aC7等。 查询其余ECS规格支持情况，推荐您使用**查询ECS规格详情API**，并通过**network_interface:traffic_mirroring_supported**参数的响应值来判断ECS规格是否支持流量镜像。 • 如果一个弹性网卡已被用作镜像源，则镜像目的不能使用该弹性网卡。 • 流量镜像会占用弹性网卡绑定实例的带宽，并且不做独立限速。

表 13-6 镜像目的限制说明

镜像目的类型	约束与限制
云服务器网卡	• 当一个镜像目的实例需要接收来自多个镜像源的流量镜像时，为了确保正常使用，请您根据业务实际需要合理规划弹性网卡所属云服务器的规格。 • 如果一个弹性网卡已被用作镜像源，则镜像目的不能使用该弹性网卡。
弹性负载均衡	由于封装的镜像报文为IPv4 UDP协议，因此当弹性负载均衡ELB作为镜像目的接收镜像流量时，需要使用支持UDP协议的IPv4独享型ELB。

- 根据流量镜像的匹配规则，同一个镜像源的同一个报文同时符合多个筛选条件规则，也仅会被匹配一次，并且根据采集策略决定是否镜像到目的实例。
- 对于镜像源弹性网卡已被安全组或者网络ACL拦截丢弃的报文，流量镜像不会镜像该部分报文。
- 当镜像源的报文符合筛选条件被镜像时，该报文不受镜像源安全组或者网络ACL出方向规则约束，即您无需在镜像源的安全组或者网络ACL做额外配置。但是如果需要将报文镜像到镜像目的实例时，则需要为镜像目的实例所在的安全组和网络ACL配置以下规则：
  - 安全组规则：允许来自镜像源的UDP协议报文访问镜像目的的4789端口。

    假如镜像源弹性网卡的私有IP地址为192.168.0.27，则安全组规则配置示例如**表13-7**所示，具体方法请参见**添加安全组规则**。

    表 13-7 安全组规则配置示例（弹性网卡）

规则类别	策略	类型	协议端口	源地址
入方向规则	允许	IPv4	自定义UDP:4789	IP地址：192.168.0.27/32 此处仅为示例，请根据实际情况配置。

  - 网络ACL规则：允许来自镜像源的UDP协议报文访问镜像目的的4789端口。

    假如镜像源弹性网卡的私有IP地址为192.168.0.27，则网络ACL规则配置示例如**表13-8**所示，具体方法请参见**添加网络ACL规则**。

表 13-8 网络 ACL 规则配置示例（弹性网卡）

规则类别	类型	策略	协议	源地址	源端口范围	目的地址	目的端口范围
入方向规则	IPv4	允许	UDP	IP地址：192.168.0.27/32 此处仅为示例，请根据实际情况配置。	此处为空，表示全部端口。	• 镜像目的为云服务器网卡时，建议配置网卡的IPv4私有地址，例如192.168.1.24/32。 • 镜像目的为弹性负载均衡时，建议配置ELB服务地址中的IPv4私有地址，例如192.168.1.25/32。 此处仅为示例，请根据实际情况配置，确保网段覆盖镜像目的IP地址即可。	4789 必须放通4789端口，其他端口请根据实际情况配置。

- 不同的虚拟私有云VPC之间网络不通，如果镜像源和镜像目的实例不在同一个VPC内，则您需要使用VPC对等连接或者企业路由器连通VPC之间的网络。
  - VPC对等连接的使用方法，请参见**对等连接简介**。
  - 企业路由器的使用方法，请参见**通过企业路由器实现同区域VPC互通**。

流量镜像使用流程

使用流量镜像功能，您需要创建镜像会话，通过在镜像会话中关联筛选条件、镜像源和镜像目的，实现指定流量的镜像，使用流程如**图13-5**所示。

图 13-5 流量镜像使用流程

表 13-9 流量镜像使用流程说明

步骤	说明	操作指导
设置镜像会话基本信息	设置镜像会话的名称，优先级等参数，开始创建镜像会话。	创建镜像会话
关联筛选条件	选择网络流量的筛选条件，关联至镜像会话。 一个镜像会话可以关联一个筛选条件，如果没有合适的筛选条件，您可以创建筛选条件，具体请参见创建筛选条件。	
关联镜像源	选择弹性网卡作为镜像源，关联至镜像会话。 一个镜像会话可关联多个镜像源。	
关联镜像目的	选择云服务器网卡或者弹性负载均衡ELB实例作为镜像目的，关联至镜像会话。	
创建完成	镜像会话创建完成并开启后，对于镜像源符合筛选条件的网络流量，将被镜像到镜像目的实例。 如果您在创建镜像会话期间关闭了镜像会话，则无法监控镜像源的网络流量，开启镜像会话，具体请参见开启/关闭镜像会话。	

13.2 筛选条件

13.2.1 创建筛选条件

操作场景

您可以参考以下指导创建筛选条件，筛选条件包含入方向规则和出方向规则，规则由优先级、流量采集策略以及匹配条件组成。

- 入方向规则：用来匹配镜像源接收到的流量。
- 出方向规则：用来匹配镜像源发送出去的流量。

筛选条件无法独立使用，需要被关联至镜像会话才可以使用。

筛选条件规则配置示例

筛选条件配置示例如表13-10所示，结合配置示例，为您介绍镜像会话是如何筛选网络流量的。

表 13-10 流量筛选说明

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围	筛选示例说明
入方向	1	TCP	采集	IPv4	172.16.0.0/24	10000-10001	10.0.0.3/32	80-80	当网络流量进入镜像源的弹性网卡时，镜像会话将会镜像符合以下条件的报文： 使用TCP (IPv4)协议，源地址网段为172.16.0.0/24、源端口为10000或者10001，目的地址为10.0.0.3/32、目的端口为80。
出方向	1	全部	不采集	IPv4	192.168.0.0/24	全部	10.2.0.0/24	全部	当网络流量从镜像源的弹性网卡出去时，镜像会话将不会镜像符合以下条件的报文： 使用全部 (IPv4)协议，源地址网段为192.168.0.0/24、源端口为全部，目的地址网段为10.2.0.0/24、目的端口为全部。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表右上方，单击“创建筛选条件”。
   进入“创建筛选条件”页面。
3. 根据界面提示，设置筛选条件基本信息。

   表 13-11 筛选条件基本信息参数说明

参数名称	参数说明	取值样例
名称	必选参数。 此处输入筛选条件的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	mirror-filter-01
描述	可选参数。 您可以根据需要在文本框中输入对该筛选条件的描述信息。	-

4. 单击入方向规则区域的“添加规则”，添加入方向规则。
   单击⊕，可以依次增加多条入方向规则。

表 13-12 入方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	TCP
策略	针对镜像源入方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	采集
类型	入方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
源地址	入方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.0.0.0/24
源端口范围	入方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	22-23
目的地址	入方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	0.0.0.0/0
目的端口范围	入方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	1-65535
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

5. 入方向规则设置完成后，单击“确定”，保存设置。
6. 单击出方向规则区域的“添加规则”，添加出方向规则。

   单击⊕，可以依次增加多条出方向规则。

表 13-13 出方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	全部
策略	针对镜像源出方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	不采集
类型	出方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
源地址	出方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	192.168.0.0/24
源端口范围	出方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
目的地址	出方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.2.0.0/24
目的端口范围	出方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

7. 出方向规则设置完成后，单击“确定”，保存设置。
8. 筛选条件参数设置完成后，单击“立即创建”。
   返回筛选条件列表页面。

后续操作

筛选条件创建完成后，需要被关联至镜像会话才可以使用。一个镜像会话可关联一个筛选条件，具体操作如下：

- 如果您还未创建镜像会话，请参见**创建镜像会话**。
- 如果您已创建镜像会话，当您需要更换镜像会话的筛选条件时，请参见**更换镜像会话的筛选条件**。

13.2.2 添加筛选条件入/出方向规则

操作场景

您可以参考以下指导在筛选条件中添加入方向和出方向规则。

- 入方向规则：用来匹配镜像源接收到的流量。
- 出方向规则：用来匹配镜像源发送出去的流量。

筛选条件规则配置示例

筛选条件配置示例如**表13-14**所示，结合配置示例，为您介绍镜像会话是如何筛选网络流量的。

表 13-14 流量筛选说明

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围	筛选示例说明
入方向	1	TCP	采集	IPv4	172.16.0.0/24	10000-10001	10.0.0.3/32	80-80	当网络流量进入镜像源的弹性网卡时，镜像会话将会镜像符合以下条件的报文： 使用TCP (IPv4)协议，源地址网段为172.16.0.0/24、源端口为10000或者10001，目的地址为10.0.0.3/32、目的端口为80。
出方向	1	全部	不采集	IPv4	192.168.0.0/24	全部	10.2.0.0/24	全部	当网络流量从镜像源的弹性网卡出去时，镜像会话将不会镜像符合以下条件的报文： 使用全部 (IPv4)协议，源地址网段为192.168.0.0/24、源端口为全部，目的地址网段为10.2.0.0/24、目的端口为全部。

操作步骤

1. 进入**筛选条件列表页面**。

2. 在筛选条件列表中，单击目标筛选条件“入/出方向规则”列下的超链接。
   进入“入方向规则”页签。
3. 在入方向规则列表左上方，单击“添加规则”，添加入方向规则。
   单击⊕，可以依次增加多条入方向规则。

表 13-15 入方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	TCP
策略	针对镜像源入方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	采集
类型	入方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
源地址	入方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.0.0.0/24
源端口范围	入方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	22-23
目的地址	入方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	0.0.0.0/0
目的端口范围	入方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	1-65535
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

4. 入方向规则设置完成后，单击“确定”，保存设置。
   您可以在列表中查看已添加的入方向规则。

5. 选择“出方向规则”页签，在出方向规则列表左上方，单击“添加规则”，添加出方向规则。

   单击⊕，可以依次增加多条出方向规则。

   表 13-16 出方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	全部
策略	针对镜像源出方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	不采集
类型	出方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
源地址	出方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	192.168.0.0/24
源端口范围	出方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
目的地址	出方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.2.0.0/24
目的端口范围	出方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

6. 出方向规则设置完成后，单击“确定”，保存设置。
   您可以在列表中查看已添加的出方向规则。

13.2.3 修改筛选条件入/出方向规则

操作场景

您可以参考以下指导修改筛选条件的入方向和出方向规则。

- 入方向规则：用来匹配镜像源接收到的流量。
- 出方向规则：用来匹配镜像源发送出去的流量。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表中，单击目标筛选条件“入/出方向规则”列下的超链接。
   进入“入方向规则”页签。
3. 在入方向规则列表中，单击目标规则所在行的操作列下的“修改”，修改入方向规则。

表 13-17 入方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	TCP

参数	说明	取值样例
策略	针对镜像源入方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	采集
类型	入方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
源地址	入方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.0.0.0/24
源端口范围	入方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	22-23
目的地址	入方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	0.0.0.0/0

参数	说明	取值样例
目的端口范围	入方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	1-65535
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

4. 入方向规则修改完成后，单击“确定”，保存设置。
   您可以在列表中查看已修改的入方向规则。
5. 选择“出方向规则”页签，在出方向规则列表中，单击目标规则所在行的操作列下的“修改”，修改出方向规则。

表 13-18 出方向规则参数说明

参数	说明	取值样例
优先级	筛选条件规则的优先级，填写说明如下： ● 优先级取值可选范围为1~65535，优先级数字越小，表示规则优先级越高。 ● 同一个筛选条件内，入方向规则的优先级不能重复。 一个筛选条件中可以包含多个规则，此时根据规则的优先级，遵循从小到大的顺序匹配。 筛选条件的匹配规则请参见**筛选条件的匹配规则**。	1
协议	此处选择网络协议，支持以下协议： ● TCP：选择TCP协议，可以自定义源端口范围和目的端口范围。 ● UDP：选择UDP协议，可以自定义源端口范围和目的端口范围。 ● ICMP：“IP类型”选择“IPv4”时，可选择ICMP协议，源端口范围和目的端口范围默认为全部端口。 ● ICMPV6：“IP类型”选择“IPv6”时，可选择ICMPV6协议，源端口范围和目的端口范围默认为全部端口。 ● 全部：表示支持全部网络协议，源端口范围和目的端口范围默认为全部端口。	全部

参数	说明	取值样例
策略	针对镜像源出方向网络流量的采集策略，对于符合筛选条件的流量，执行以下操作： ● 如果“策略”设置为采集，将镜像该流量到镜像目的。 ● 如果“策略”设置为不采集，将不会镜像该流量到镜像目的。	不采集
类型	出方向网络流量支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
源地址	出方向网络流量的源地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	192.168.0.0/24
源端口范围	出方向网络流量的源端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
目的地址	出方向网络流量的目的地址，您可以填写IP地址，支持格式如下： ● 单个IP地址：IP地址/掩码。 单个IPv4地址示例为192.168.10.10/32。 单个IPv6地址示例为2002:50::44/128。 ● IP网段：IP地址/掩码。 IPv4网段示例为192.168.52.0/24。 IPv6网段示例为2407:c080:802:469::/64。 ● 所有IP地址： 0.0.0.0/0表示匹配所有IPv4地址。 ::/0表示匹配所有IPv6地址。	10.2.0.0/24

参数	说明	取值样例
目的端口范围	出方向网络流量的目的端口范围，填写说明如下： ● 端口取值范围是1~65535 ● 使用中划线(-)连接起始端口和结束端口，即“起始端口-结束端口”，结束端口取值应大于等于起始端口，例如22-23 ● 不填或者填写“1-65535”，表示全部端口	全部
描述	您可以根据需要在文本框中输入对该筛选条件规则的描述信息。	-

6. 出方向规则修改完成后，单击“确定”，保存设置。
   您可以在列表中查看已修改的出方向规则。

13.2.4 删除筛选条件入/出方向规则

操作场景

您可以参考以下指导删除筛选条件的入方向和出方向规则。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表中，单击目标筛选条件“入/出方向规则”列下的超链接。
   进入“入方向规则”页签。
3. 在入方向规则列表中，单击目标规则所在行的操作列下的“删除”。
   弹出删除确认对话框。
4. 确认无误后，单击“确定”，删除入方向规则。
   入方向规则删除后无法恢复，请谨慎操作。
5. 选择“出方向规则”页签，在出方向规则列表中，单击目标规则所在行的操作列下的“删除”。
   弹出删除确认对话框。
6. 确认无误后，单击“确定”，删除出方向规则。
   出方向规则删除后无法恢复，请谨慎操作。

13.2.5 修改筛选条件基本信息

操作场景

您可以参考以下指导修改筛选条件的基本信息，包括筛选条件名称和描述。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表中，单击目标筛选条件名称对应的超链接。

进入“入方向规则”页签。

3. 选择“基本信息”页签，根据界面提示信息修改参数。

   a. 单击待修改参数后面的  ，并在文本框中输入信息。

   b. 修改完成后，单击  保存修改。

表 13-19 筛选条件基本信息参数说明

参数名称	参数说明	取值样例
名称	必选参数。 此处输入筛选条件的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	mirror-filter-01
描述	可选参数。 您可以根据需要在文本框中输入对该筛选条件的描述信息。	-

13.2.6 查看筛选条件

操作场景

您可以参考以下指导查看筛选条件的信息：

- 基本信息：筛选条件名称、ID以及创建时间等。
- 入/出方向规则：筛选条件的入/出方向规则详情，包括规则的优先级、协议类型以及策略等。
- 关联镜像会话：筛选条件已关联的镜像会话，包括镜像会话名称、镜像目的以及镜像状态等。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表中，单击目标筛选条件名称对应的超链接。
   进入“入方向规则”页签。
3. 执行以下操作，分别选择不同的页签，查看筛选条件的信息。
   - 在“基本信息”页签：查看筛选条件名称、ID以及创建时间等。
   - 在“入方向规则”页签：查看筛选条件的入方向规则详情，包括规则的优先级、协议类型以及策略等。
   - 在“出方向规则”页签：查看筛选条件的出方向规则详情，包括规则的优先级、协议类型以及策略等。
   - 在“关联镜像会话”页签：查看筛选条件已关联的镜像会话，包括镜像会话名称、镜像目的以及镜像状态等。

13.2.7 删除筛选条件

操作场景

如果筛选条件不需要继续使用，您可以参考以下指导删除筛选条件。

约束与限制

当筛选条件已关联镜像会话时，不支持删除，请解除关联后重试。

- 一个镜像会话必须关联一个筛选条件，您需要将镜像会话的筛选条件更换成其他筛选条件，具体请参见**更换镜像会话的筛选条件**。
- 如果您的镜像会话不需要使用，也可以删除镜像会话，具体请参见**删除镜像会话**。

操作步骤

1. 进入**筛选条件列表页面**。
2. 在筛选条件列表中，单击目标筛选条件所在行的操作列下的“删除”。
   弹出删除确认对话框。
3. 确认无误后，单击“确定”，删除筛选条件。
   筛选条件删除后无法恢复，请谨慎操作。

13.3 镜像会话

13.3.1 创建镜像会话

操作场景

使用流量镜像功能，您需要创建镜像会话，通过在镜像会话中关联筛选条件、镜像源和镜像目的，将镜像源符合筛选条件的流量镜像到镜像目的。您可以参考以下指导创建镜像会话。

镜像会话的详细信息，请参见**流量镜像概述**。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表右上方，单击“创建镜像会话”。
   进入“创建镜像会话”页面。
3. 根据界面提示，设置镜像会话基本信息。

表 13-20 镜像会话基本信息参数说明

参数名称	参数说明	取值样例
名称	必选参数。 此处输入镜像会话的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	mirror-session-01
优先级	必选参数。 镜像会话的优先级，填写说明如下： ● 优先级取值范围为1~32766，数字越小，表示优先级越高。 ● 同一个账号在同一个区域内的镜像会话优先级不能重复。 同一个镜像源可同时被关联至多个镜像会话，此时根据镜像会话的优先级，按照从小到大的顺序匹配。 镜像会话的匹配规则请参见**镜像会话的匹配规则**。	1
VXLAN网络标识	可选参数。 VXLAN网络标识（VXLAN Network Identifier），简称为VNI，取值范围为0~16777215。由于一个镜像目的可以被关联至多个镜像会话，因此对于镜像目的来说，VNI用来区分不同的镜像会话。 如果此处不填写，默认为1。	1
镜像报文长度	可选参数。 该参数表示符合筛选条件，被镜像的报文长度，取值范围为1~1460 bytes。 如果此处不填写，默认为96 bytes。	96
是否开启	可选参数。 ● 镜像会话关闭后，将无法监控镜像源的网络流量。 ● 镜像会话开启后，将监控镜像源的网络流量。	开启
描述	可选参数。 您可以根据需要在文本框中输入对该镜像会话的描述信息。	-

4. 镜像会话基本信息设置完成后，单击“下一步”。
   进入“关联筛选条件”页面。
5. 在筛选条件列表中，选择筛选条件。

一个镜像会话只能关联一个筛选条件。

如果没有合适的筛选条件，您可以创建新的筛选条件，具体请参见**创建筛选条件**。

6. 筛选条件关联完成后，单击“下一步”。

   进入“关联镜像源”页面。

7. 在镜像源列表中，选择镜像源。

   为镜像会话关联镜像源时，请您了解镜像源的约束限制，具体请参见**表13-5**。

8. 镜像源关联完成后，单击“下一步”。

   进入“关联镜像目的”页面。

9. 在镜像目的列表中，选择镜像目的。

   - 镜像目的为云服务器网卡或者弹性负载均衡实例，用来接受镜像的流量。
   - 一个镜像会话只能关联一个镜像目的。

     了解更多镜像目的的约束限制，具体请参见**表13-6**。

10. 镜像目的关联完成后，单击“下一步”。

    进入“确认配置”页面。

11. 配置确认无误后，单击“立即创建”，开始创建镜像会话。

    创建成功后，返回镜像会话列表，可以看到已创建的镜像会话。

13.3.2 开启/关闭镜像会话

操作场景

您可以参考以下指导开启或者关闭镜像会话。

- 镜像会话关闭后，将无法监控镜像源的网络流量。
- 镜像会话开启后，将监控镜像源的网络流量。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话所在行的操作列下的“开启”或者“关闭”。

   弹出确认对话框。

3. 确认无误后，单击“确定”，开启或者关闭镜像会话。

13.3.3 将镜像源关联至镜像会话

操作场景

您可以参考以下指导将镜像源关联至镜像会话。

约束与限制

为镜像会话关联镜像源时，请您了解镜像源的约束限制，具体请参见**表13-5**。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话名称对应的超链接。
   进入“基本信息”页签。
3. 选择“镜像源”页签，并在镜像源列表左上方，单击“关联”。
   弹出“关联镜像源”对话框。
4. 在镜像源列表中，勾选目标镜像源，并单击“确定”。
   关联成功后，返回镜像源列表，可以看到已关联的镜像源。

13.3.4 将镜像源和镜像会话解除关联

操作场景

您可以参考以下指导解除镜像源和镜像会话之间的关联。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话名称对应的超链接。
   进入“基本信息”页签。
3. 选择“镜像源”页签，并在镜像源列表中，单击目标镜像源所在行的操作列下的“解除关联”。
   弹出解除关联确认对话框。
4. 确认无误后，单击“确定”，解除镜像会话所关联的镜像源。
   解除关联成功后，返回镜像源列表。

13.3.5 更换镜像会话的筛选条件

操作场景

一个镜像会话只能关联一个筛选条件，如果当前筛选条件无法满足需求，您可以参考以下指导更换镜像会话的筛选条件。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话所在行的操作列下的“更多 > 更换筛选条件”。
   弹出“更换筛选条件”对话框。
3. 在筛选条件列表中，选择筛选条件，并单击“确定”。
   更换成功后，返回镜像会话列表页面，可以看到目标镜像筛选条件列下的信息已更新。
   如果没有合适的筛选条件，您可以创建新的筛选条件，具体请参见**创建筛选条件**。

13.3.6 更换镜像会话的镜像目的

操作场景

一个镜像会话只能关联一个镜像目的，您可以参考以下指导更换镜像会话的镜像目的。

约束与限制

- 镜像目的为云服务器网卡或者弹性负载均衡实例，用来接受镜像的流量。
- 一个镜像会话只能关联一个镜像目的。

  了解更多镜像目的的约束限制，具体请参见**表13-6**。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话所在行的操作列下的“更多 > 更换镜像目的”。

   弹出“更换镜像目的”对话框。
3. 在镜像目的的列表中，选择镜像目的，并单击“确定”。

   更换成功后，返回镜像会话列表页面，可以看到目标镜像的镜像目的列下的信息已更新。

13.3.7 修改镜像会话基本信息

您可以参考以下指导修改镜像会话基本信息，包括镜像会话名称和描述信息。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话所在行的操作列下的“修改”。

   弹出“修改镜像会话”对话框。
3. 根据界面提示信息修改参数。

表 13-21 镜像会话基本信息参数说明

参数名称	参数说明	取值样例
名称	必选参数。 此处输入镜像会话的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。	mirror-session-01
描述	可选参数。 您可以根据需要在文本框中输入对该镜像会话的描述信息。	-

4. 参数修改完成后，单击“确定”，保存修改。

13.3.8 查看镜像会话

操作场景

您可以参考以下指导查看镜像会话的信息：

- 基本信息：镜像会话名称、优先级以及描述等。
- 筛选条件：镜像会话关联的筛选条件。
- 镜像源：镜像会话关联的镜像源，比如弹性网卡的私有IP地址、已绑定实例以及安全组等。
- 镜像目的：镜像会话关联的镜像目的，即云服务器网卡或者弹性负载均衡实例。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，可以查看镜像会话名称、筛选条件、镜像目的等信息。
3. 在镜像会话列表中，单击目标镜像会话名称对应的超链接。
   进入“基本信息”页签。
4. 执行以下操作，分别选择不同的页签，查看镜像会话的信息。
   - 在“基本信息”页签：查看镜像会话名称、优先级以及描述等。
   - 在“镜像源”页签：查看镜像源的信息，比如弹性网卡的私有IP地址、已绑定实例以及安全组等。

13.3.9 删除镜像会话

操作场景

如果镜像会话不需要继续使用，您可以参考以下指导删除镜像会话。

操作步骤

1. 进入**镜像会话列表页面**。
2. 在镜像会话列表中，单击目标镜像会话所在行的操作列下的“更多 > 删除”。
   弹出删除确认对话框。
3. 确认无误后，单击“确定”，删除镜像会话。
   镜像会话删除后无法恢复，请谨慎操作。

13.4 流量镜像配置示例

13.4.1 将源弹性网卡的入方向 TCP 流量镜像到单个目的弹性网卡

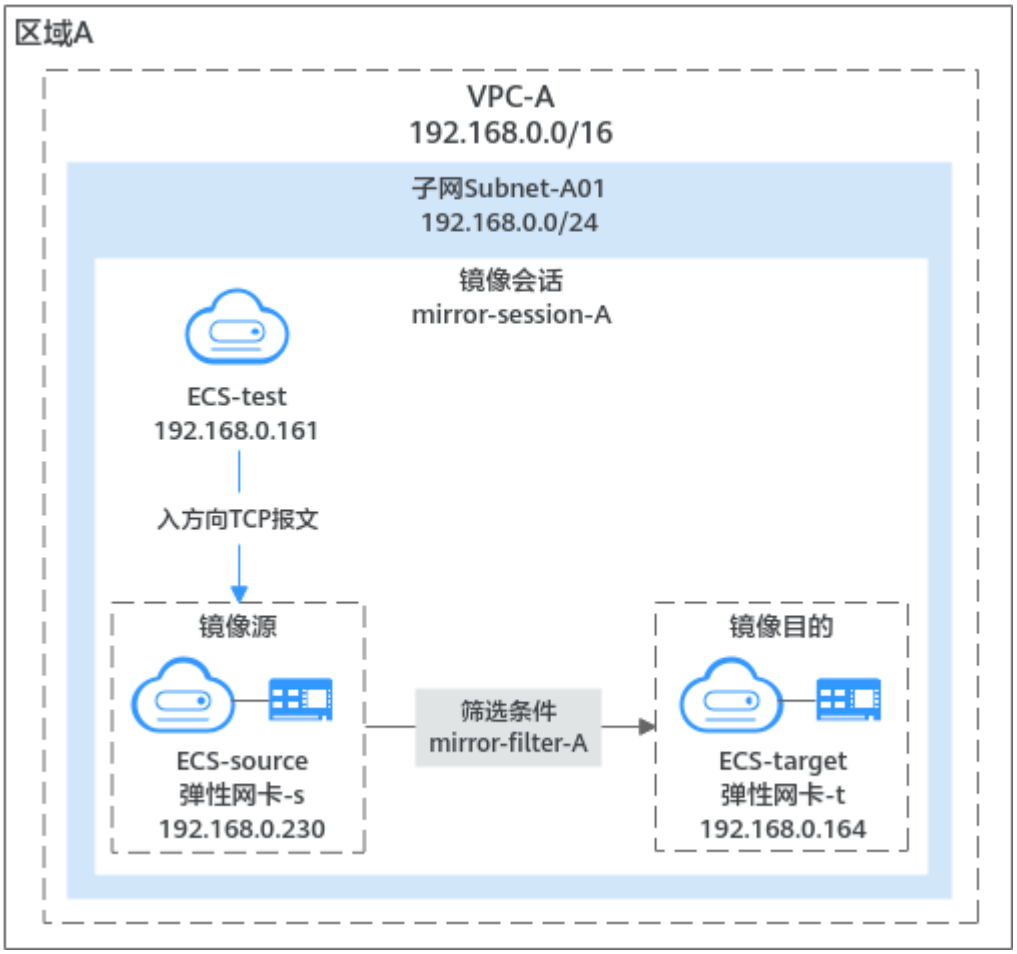
方案架构

当您需要将镜像源（弹性网卡）的入方向TCP流量，镜像到单个镜像目的（弹性网卡）时，您可以参考本文的配置示例。如**图13-6**所示，在VPC-A中，ECS-test访问ECS-

source，需要将ECS-source入方向TCP流量镜像到ECS-target中，则您创建一个镜像会话可以实现需求，详细设置如下：

- 镜像源是ECS-source的弹性网卡-s，表示需要镜像弹性网卡-s入方向的TCP流量。
- 镜像目的是ECS-target的弹性网卡-t，表示将弹性网卡-s入方向的TCP流量镜像到弹性网卡-t中。
- 镜像会话的筛选条件中需要添加采集入方向TCP流量的规则。

图 13-6 镜像入方向 TCP 流量



约束与限制

关于流量镜像的使用限制，具体请查看**流量镜像的使用限制**。

资源规划说明

本示例中，虚拟私有云VPC和子网、弹性公网IP以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 13-22 镜像入方向 TCP 流量资源规划总体说明

资源类型	资源数量	说明
虚拟私有云VPC和子网	VPC：1 子网：1	• VPC名称：请根据实际情况设置，本示例为VPC-A。 • IPv4网段：请根据实际情况设置，本示例为192.168.0.0/16。 • 子网名称：请根据实际情况设置，本示例为Subnet-A01。 • 子网IPv4网段：请根据实际情况设置，本示例为192.168.0.0/24。
弹性云服务器ECS	3	本示例中，共需要三个ECS，配置说明如下： • 名称：根据实际情况设置，本示例分别为ECS-source、ECS-target和ECS-test。 • 实例规格类型：本示例中镜像源ECS-source使用通用计算增强型c7t，当前仅支持部分规格ECS的弹性网卡作为镜像源，具体请参见**流量镜像的使用限制**。其他ECS的规格类型不做限制。 • 镜像：请根据实际情况设置，本示例为公共镜像（Huawei Cloud EulerOS 2.0 标准版 64位）。 • 系统盘：通用型SSD盘，40GB。 • 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例为VPC-A。 – 子网：选择子网，本示例为Subnet-A01。 • 安全组：本示例中，3个ECS属于同一个安全组Sg-X，需要确保**表13-23**中的规则均已正确添加即可。 如果ECS属于不同的安全组，则除了分别在不同安全组配置**表13-23**中的规则外，还需要添加以下规则： – 如果访问镜像源的测试ECS和镜像源ECS属于不同安全组，比如ECS-test属于Sg-X，ECS-source属于Sg-A，则需要在Sg-A中额外添加**表13-24**中的规则，允许ECS-test的流量进入。 – 如果镜像源ECS和镜像目的ECS属于不同安全组，比如ECS-source属于Sg-A，ECS-target属于Sg-B，则需要在Sg-B中额外添加**表13-25**中的规则，允许来自镜像源封装的UDP协议报文访问镜像目的的4789端口。 • 弹性公网IP：选择“暂不购买”。 • 私有IP地址：ECS-source为192.168.0.230，ECS-target为192.168.0.164，ECS-test为192.168.0.161

资源类型	资源数量	说明
弹性公网IP	1	• 计费模式：请根据情况选择计费模式，本示例为按需计费。 • EIP名称：请根据实际情况设置，本示例为EIP-A。 • EIP地址：EIP地址系统随机分配，本示例为124.X.X.187。
筛选条件	1	• 名称：请根据实际情况设置，本示例为mirror-filter-A。 • 入方向规则：添加1条入方向规则，该规则表示从ECS-test发送到镜像源（ECS-source）1234端口的TCP报文将会被镜像，规则详情请参见**表13-26**。
镜像会话	1	• 镜像会话基本信息： – 名称：请根据实际情况设置，本示例为mirror-session-A。 – 优先级：请根据实际情况设置，本示例为1。 – VXLAN网络标识：请根据实际情况设置，本示例为1。 – 镜像报文长度：请根据实际情况设置，本示例为96。 – 是否开启：开启，镜像会话开启后，才会监控镜像源的网络流量。 • 关联筛选条件：请根据实际情况设置，本示例为mirror-filter-A。 • 关联镜像源：请根据实际情况设置，本示例为ECS-source的弹性网卡，私有IP地址为192.168.0.230。 • 关联镜像目的： – 类型：云服务器网卡 – 网卡：请根据实际情况设置，本示例为ECS-target的弹性网卡，私有IP地址为192.168.0.164。

表 13-23 安全组 Sg-X 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址：0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址：0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	全部	源地址：当前安全组Sg-X	针对IPv4，用于安全组内ECS之间网络互通。

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv6	全部	源地址：当前安全组Sg-X	针对IPv6，用于安全组内ECS之间网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

须知

本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

表 13-24 安全组 Sg-A 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	TCP:1234	访问镜像源的测试ECS的地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	针对IPv4，允许来自ECS-test的TCP协议报文访问镜像源ECS-source的1234端口。

表 13-25 安全组 Sg-B 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	UDP:4789	镜像源的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	针对IPv4，允许来自镜像源ECS-source封装的UDP协议报文访问镜像目的ECS-target的4789端口。

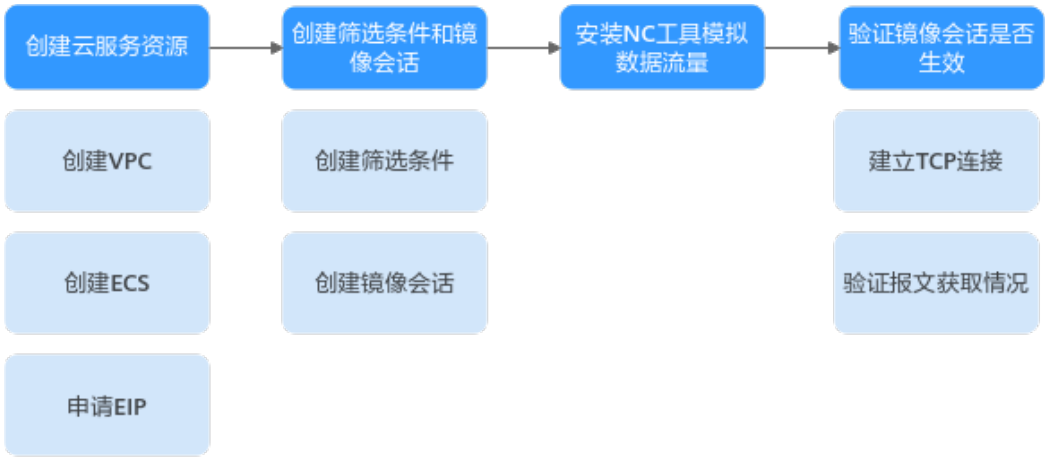
表 13-26 筛选条件的入方向规则

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围
入方向	1	TCP	采集	IPv4	报文的来源地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	全部	报文的目的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	本示例为ECS-source的1234端口： 1234-1234

操作流程

将源弹性网卡的入方向TCP流量镜像到单个目的弹性网卡，流程如图13-7所示。

图 13-7 镜像入方向 TCP 流量



步骤一：创建云服务资源

1. 创建1个VPC和1个子网。
   具体方法请参见**创建虚拟私有云和子网**。
2. 创建3个ECS。
   具体方法请参见**自定义购买ECS**。
3. 申请弹性公网IP。
   具体方法请参见**购买弹性公网IP**。

步骤二：创建筛选条件和镜像会话

1. 创建1个筛选条件。
   具体方法请参见**创建筛选条件**。
2. 创建1个镜像会话，关联筛选条件、镜像源以及镜像目的。
   具体方法请参见**创建镜像会话**。

步骤三：安装 NC 工具模拟数据流量

本文使用NC工具模拟数据流量，NC工具是一个通过TCP/UDP协议在网络中读写数据的工具，常用于网络端口测试等，需要在ECS-source和ECS-test中安装NC工具。

1. 在ECS-source中安装NC工具。
   a. 下载NC工具需要连接公网，将EIP绑定至ECS-source。
      具体方法请参见**绑定弹性公网IP**。
   b. 远程登录ECS-source。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。
   c. 依次执行以下命令，安装NC工具。
      sudo yum update
      回显类似如下信息：
      ```
      [root@ecs-source ~]# sudo yum update
      HCE 2.0
      base
              55 MB/s | 6.1 MB     00:00
      HCE 2.0
      updates
                98 MB/s |  14 MB     00:00
      Last metadata expiration check: 0:00:01 ago on Tue 10 Sep 2024 05:54:28 PM CST.
      Dependencies resolved.
      Nothing to do.
      Complete!
      ```
      sudo yum install nc
      回显类似如下信息，请根据回显提示输入**y**，并按回车。
      ```
      [root@ecs-source ~]# sudo yum install nc
      Last metadata expiration check: 0:00:12 ago on Tue 10 Sep 2024 05:54:28 PM CST.
      Dependencies resolved.
      ...
      Install  2 Packages

      Total download size: 6.1 M
      Installed size: 25 M
      Is this ok [y/N]: y
      Downloading Packages:
      ...
      Importing GPG key 0xA8DEF926:
       Userid     : "HCE <support@huaweicloud.com>"
       Fingerprint: C1BA 9CD4 9D03 A206 E241 F176 28DA 5B77 A8DE F926
       From       : http://repo.huaweicloud.com/hce/2.0/updates/RPM-GPG-KEY-HCE-2
      Is this ok [y/N]: y
      ...
      Installed:
        libssh2-1.10.0-2.r10.hce2.x86_64
      nmap-2:7.92-2.r4.hce2.x86_64

      Complete!
      ```
   d. ECS-source的NC工具安装完成后，解绑EIP。
      具体方法请参见**解绑弹性公网IP**。
2. 参考**1.a**~**1.d**，在ECS-test中安装NC工具，并解绑EIP。
3. EIP解绑后，删除EIP。
   本示例中不再需要使用EIP，因此删除EIP，具体方法请参见**解绑弹性公网IP**。如果不删除EIP，则EIP会持续计费。

步骤三：验证镜像会话是否生效

1. 执行以下操作，建立ECS-source和ECS-test之间的TCP连接。

   本文在ECS-test向ECS-source发送TCP报文，查看ECS-source是否可以收到该报文。

   a. 在ECS-source中，执行以下命令，开启1234端口的监听。

      nc -l *镜像源ECS-source的监听端口*

      命令示例：

      nc -l 1234

      此处回显为空，表示监听已正常开启。

   b. 在ECS-test中，执行以下命令，建立ECS-source和ECS-test之间的TCP连接。

      nc *镜像源ECS-source的私有IP地址 镜像源ECS-source的监听端口*

      命令示例：

      nc 192.168.0.230 1234

      此处回显为空，在ECS-test中，输入任意信息（比如**hello**），并按回车，测试TCP连接是否建立成功。

      ```
      [root@ecs-test ~]# nc 192.168.0.230 1234
      hello
      ```

   c. 在ECS-source中，查看是否收到来自ECS-test的信息。

      回显类似如下信息，可正常收到信息，表示TCP连接建立成功。

      ```
      [root@ecs-source ~]# nc -l 1234
      hello
      ```

2. 执行以下操作，测试ECS-source入方向的报文是否可以镜像到ECS-target。

   当ECS-test实时向镜像源ECS-source发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target是否可以获取到该报文的数据包，如果获取成功，则表示镜像会话配置生效。

   a. 远程登录ECS-target。

      ECS有多种登录方法，具体请参见**登录弹性云服务器**。

   b. 在ECS-target中，执行以下命令，查看镜像目的对应的网卡名称。

      ifconfig

      回显类似如下信息，本示例中镜像目的对应的网卡名称为eth0。

      ```
      [root@ecs-target ~]# ifconfig
      eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 192.168.0.164  netmask 255.255.255.0  broadcast 192.168.0.255
            inet6 fe80::f816:3eff:fe7e:d67a  prefixlen 64  scopeid 0x20<link>
            ether fa:16:3e:7e:d6:7a  txqueuelen 1000  (Ethernet)
            RX packets 29043  bytes 32268398 (30.7 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 13811  bytes 3961116 (3.7 MiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
      ...
      ```

   c. 在ECS-target中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

      tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

      命令示例：

      tcpdump -i eth0 udp port 4789 -nne

      回显类似如下信息：

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      ```


d. 在ECS-test中，输入任意信息（比如**12345**），并按回车，向ECS-source发送TCP报文。

回显类似如下信息：

```
[root@ecs-test ~]# nc 192.168.0.230 1234
hello
12345
```

e. 在ECS-source中，查看是否收到来自ECS-test的信息。

回显类似如下信息，可正常收到信息。

```
[root@ecs-source ~]# nc -l 1234
hello
12345
```

f. 在ECS-target中，查看是否可以获取到报文的数据包。

回显类似如下信息，可以看到TCPDUMP工具启动后，ECS-test发送的信息**12345**对应的数据包。其中，**vni 1**为镜像会话的标识，表示通过镜像会话，ECS-target可成功获取到数据包，数据包内容分为两部分，详细说明请参见**表13-27**。

```
[root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:12:25.839624 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:7a, ethertype IPv4 (0x0800), length 122:
192.168.0.230.32838 > 192.168.0.164.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 72: 192.168.0.161.38944 >
192.168.0.230.1234: Flags [P.], seq 2063075043:2063075049, ack 1116663338, win 502, options
[nop,nop,TS val 969673134 ecr 605179348], length 6
```

表 13-27 数据包说明

数据包示例	数据包说明
19:12:25.839624 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:7a, ethertype IPv4 (0x0800), length 122: 192.168.0.230.32838 > 192.168.0.164.4789: VXLAN, flags [I] (0x08), vni 1	流量镜像封装的VXLAN报文。报文格式如下： <Timestamp><SMacAddr><DMacAddr><EthernetType><Length><Sip><Sport><Dip><Dport><VXLAN Flags><VNI> 封装报文的字段说明如下： • Timestamp：由TCPDUMP工具生成，表示获取报文的时间 • SMacAddr：VXLAN报文来源实例的MAC地址，此处为网关实例的MAC地址 • DMacAddr：VXLAN报文目的实例的MAC地址，此处为镜像目的实例的MAC地址 • EthernetType：报文的以太网类型，0x0800表示协议是IPv4 • Length：报文的长度 • Sip：镜像源地址 • Sport：镜像源端口 • Dip：镜像目的地址 • Dport：镜像目的端口，通常为接收VXLAN报文的端口4789 • VXLAN Flags：通常为0x08，表示为VXLAN报文 • VNI：镜像会话的VXLAN网络标识
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 72: 192.168.0.161.38944 > 192.168.0.230.1234: Flags [P.], seq 2063075043:2063075049, ack 1116663338, win 502, options [nop,nop,TS val 969673134 ecr 605179348], length 6	原始报文。 原始报文字段属于通用网络知识，此处不做详细说明。

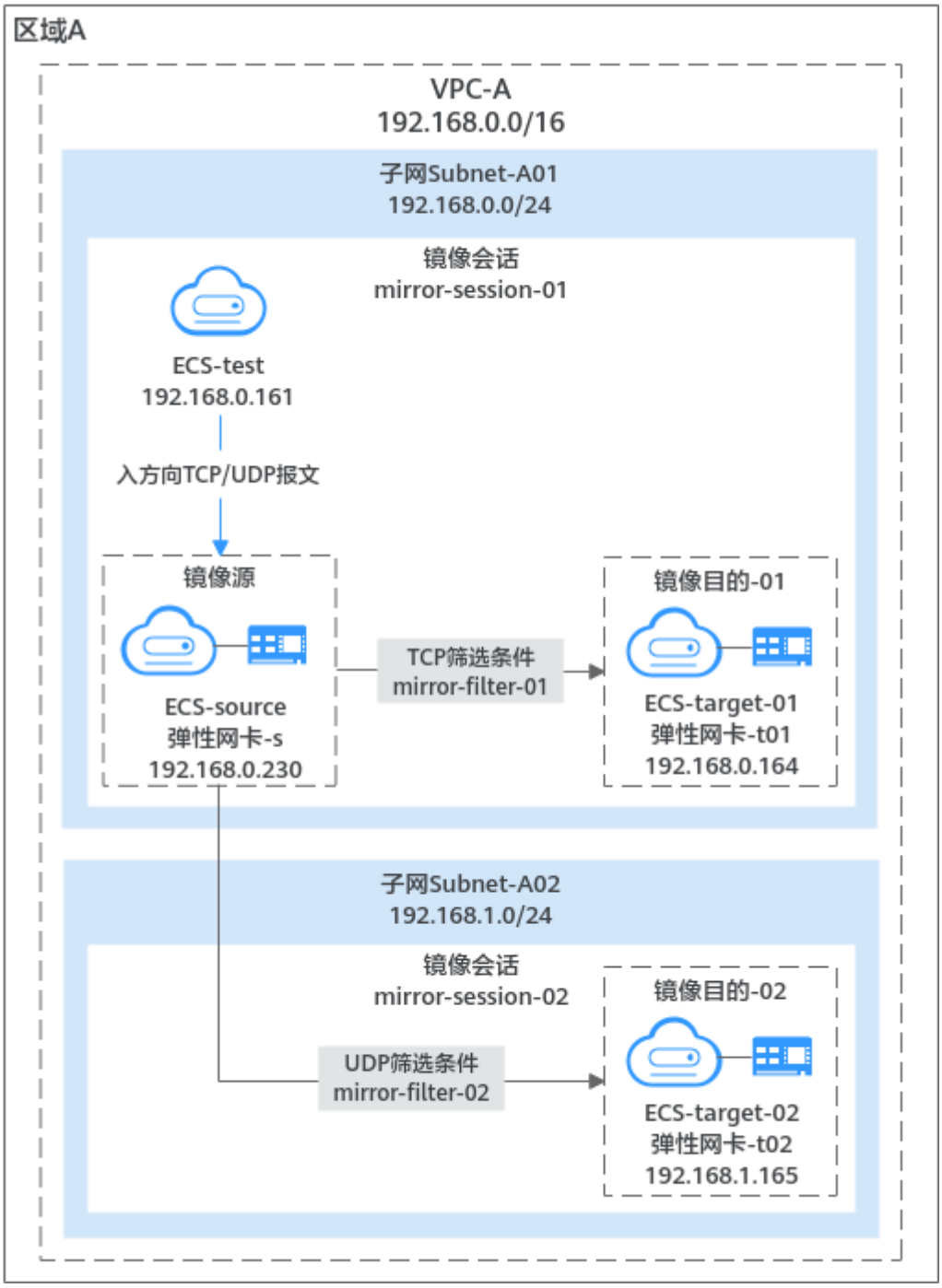
13.4.2 将源弹性网卡的入方向 TCP/UDP 流量镜像到不同的目的弹性网卡

方案架构

当您需要将镜像源（弹性网卡）的入方向TCP和UDP流量，分别镜像到不同的镜像目的（弹性网卡）时，您可以参考本文的配置示例。如图13-8所示，在VPC-A中，ECS-test访问ECS-source，需要将ECS-source入方向TCP流量镜像到ECS-target-01中，并将入方向UDP流量镜像到ECS-target-02，由于一个镜像会话只可以关联一个镜像目的，则您创建两个镜像会话可以实现需求，详细设置如下：

- 镜像会话mirror-session-01：
  - 镜像源是ECS-source的弹性网卡-s，表示需要镜像弹性网卡-s入方向的TCP流量。
  - 镜像目的是ECS-target-01的弹性网卡-t01，表示将弹性网卡-s入方向的TCP流量镜像到弹性网卡-t01中。
  - 镜像会话的筛选条件mirror-filter-01中，需要添加采集入方向TCP流量的规则。
- 镜像会话mirror-session-02：
  - 镜像源是ECS-source的弹性网卡-s，表示需要镜像弹性网卡-s入方向的UDP流量。
  - 镜像目的是ECS-target-02的弹性网卡-t02，表示将弹性网卡-s入方向的UDP流量镜像到弹性网卡-t02中。
  - 镜像会话的筛选条件mirror-filter-02中，需要添加采集入方向UDP流量的规则。

图 13-8 镜像入方向 TCP/UDP 流量



约束与限制

关于流量镜像的使用限制，具体请查看**流量镜像的使用限制**。

资源规划说明

本示例中，虚拟私有云VPC和子网、弹性公网IP以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 13-28 镜像入方向 TCP/UDP 流量资源规划总体说明

资源类型	资源数量	说明
虚拟私有云 VPC和子网	VPC：1 子网：2	• VPC名称：请根据实际情况设置，本示例为VPC-A。 • IPv4网段：请根据实际情况设置，本示例为192.168.0.0/16。 • 子网名称：请根据实际情况设置，本示例共2个子网，分别为Subnet-A01和Subnet-A02。 • 子网IPv4网段：请根据实际情况设置，本示例Subnet-A01为192.168.0.0/24，Subnet-A02为192.168.1.0/24。

资源类型	资源数量	说明
弹性云服务器ECS	4	本示例中，共需要四个ECS，配置说明如下： • 名称：根据实际情况设置，本示例分别为ECS-source、ECS-target-01、ECS-target-02和ECS-test。 • 实例规格类型：本示例中镜像源ECS-source使用通用计算增强型c7t，当前仅支持部分规格ECS的弹性网卡作为镜像源，具体请参见**流量镜像的使用限制**。其他ECS的规格类型不做限制。 • 镜像：请根据实际情况设置，本示例为公共镜像（Huawei Cloud EulerOS 2.0 标准版 64位）。 • 系统盘：通用型SSD盘，40GB。 • 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例为VPC-A。 – 子网：选择子网，本示例ECS-source、ECS-target-01、ECS-test的子网为Subnet-A01，ECS-target-02的子网为Subnet-A02。 • 安全组：本示例中，4个ECS属于同一个安全组Sg-X，需要确保**表13-29**中的规则均已正确添加即可。 如果ECS属于不同的安全组，则除了分别在不同安全组配置**表13-29**中的规则外，还需要添加以下规则： – 如果访问镜像源的测试ECS和镜像源ECS属于不同安全组，比如ECS-test属于Sg-X，ECS-source属于Sg-A，则需要在Sg-A中额外添加**表13-30**中的规则，允许ECS-test的流量进入。 – 如果镜像源ECS和镜像目的ECS属于不同安全组，比如ECS-source属于Sg-A，ECS-target-01属于Sg-B，则需要在Sg-B中额外添加**表13-31**中的规则，允许来自镜像源封装的UDP协议报文访问镜像目的的4789端口。ECS-target-02同理。 • 弹性公网IP：选择“暂不购买”。 • 私有IP地址：ECS-source为192.168.0.230，ECS-target-01为192.168.0.164，ECS-target-02为192.168.1.165，ECS-test为192.168.0.161
弹性公网IP	1	• 计费模式：请根据情况选择计费模式，本示例为按需计费。 • EIP名称：请根据实际情况设置，本示例为EIP-A。 • EIP地址：EIP地址系统随机分配，本示例为124.X.X.187。

资源类型	资源数量	说明
筛选条件	2	• 1个采集TCP流量的筛选条件： – 名称：请根据实际情况设置，本示例为mirror-filter-01。 – 入方向规则：添加1条入方向规则，该规则表示从ECS-test发送到镜像源（ECS-source）1234端口的TCP报文将会被镜像，规则详情请参见**表13-32**。 • 1个采集UDP流量的筛选条件： – 名称：请根据实际情况设置，本示例为mirror-filter-02。 – 入方向规则：添加1条入方向规则，该规则表示从ECS-test发送到镜像源（ECS-source）1235端口的UDP报文将会被镜像，规则详情请参见**表13-32**。

资源类型	资源数量	说明
镜像会话	2	1个采集TCP流量的镜像会话： ● 镜像会话基本信息： – 名称：请根据实际情况设置，本示例为mirror-session-01。 – 优先级：请根据实际情况设置，本示例为1。 – VXLAN网络标识：请根据实际情况设置，本示例为1。 – 镜像报文长度：请根据实际情况设置，本示例为96。 – 是否开启：开启，镜像会话开启后，才会监控镜像源的网络流量。 ● 关联筛选条件：请根据实际情况设置，本示例为mirror-filter-01。 ● 关联镜像源：请根据实际情况设置，本示例为ECS-source的弹性网卡，私有IP地址为192.168.0.230。 ● 关联镜像目的： – 类型：云服务器网卡 – 网卡：请根据实际情况设置，本示例为ECS-target-01的弹性网卡，私有IP地址为192.168.0.164。 1个采集UDP流量的镜像会话： ● 镜像会话基本信息： – 名称：请根据实际情况设置，本示例为mirror-session-02。 – 优先级：请根据实际情况设置，本示例为2。 – VXLAN网络标识：请根据实际情况设置，本示例为2。 – 镜像报文长度：请根据实际情况设置，本示例为96。 – 是否开启：开启，镜像会话开启后，才会监控镜像源的网络流量。 ● 关联筛选条件：请根据实际情况设置，本示例为mirror-filter-02。 ● 关联镜像源：请根据实际情况设置，本示例为ECS-source的弹性网卡，私有IP地址为192.168.0.230。 ● 关联镜像目的： – 类型：云服务器网卡 – 网卡：请根据实际情况设置，本示例为ECS-target-02的弹性网卡，私有IP地址为192.168.1.165。

表 13-29 安全组 Sg-X 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址：0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址：0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	全部	源地址：当前安全组Sg-X	针对IPv4，用于安全组内ECS之间网络互通。
入方向	允许	IPv6	全部	源地址：当前安全组Sg-X	针对IPv6，用于安全组内ECS之间网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

须知

本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

表 13-30 安全组 Sg-A 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	TCP: 1234	访问镜像源的测试ECS的地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	针对IPv4，允许来自ECS-test的TCP协议报文访问镜像源ECS-source的1234端口。
入方向	允许	IPv4	UDP: 1235	访问镜像源的测试ECS的地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	针对IPv4，允许来自ECS-test的UDP协议报文访问镜像源ECS-source的1235端口。

表 13-31 安全组 Sg-B 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	UDP: 4789	镜像源的地址，本示例为ECS-source的私有IP地址：192.168.0.230/32	针对IPv4，允许来自镜像源ECS-source封装的UDP协议报文访问镜像目的ECS-target-01的4789端口。

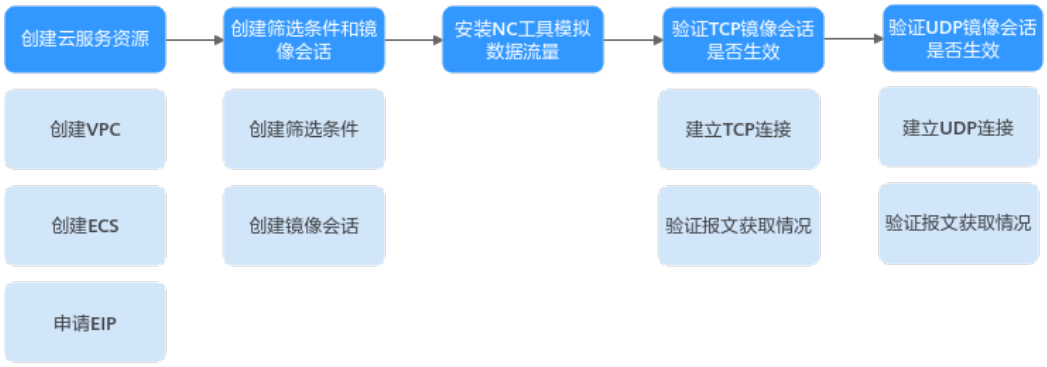
表 13-32 筛选条件的入方向规则

名称	方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围
mirror-filter-01	入方向	1	TCP	采集	IPv4	报文的来源地址，本示例为ECS-test的私有IP地址：192.168.0.161/32	全部	报文的目的地址，本示例为ECS-source的私有IP地址：192.168.0.230/32	本示例为ECS-source的1234端口：1234-1234
mirror-filter-02	入方向	1	UDP	采集	IPv4	报文的来源地址，本示例为ECS-test的私有IP地址：192.168.0.161/32	全部	报文的目的地址，本示例为ECS-source的私有IP地址：192.168.0.230/32	本示例为ECS-source的1235端口：1235-1235

操作流程

将源弹性网卡的入方向TCP流量和UDP流量镜像到不同的目的弹性网卡，流程如图13-9所示。

图 13-9 镜像入方向 TCP/UDP 流量



步骤一：创建云服务资源

1. 创建1个VPC和2个子网。
   具体方法请参见**创建虚拟私有云和子网**。
2. 创建4个ECS。
   具体方法请参见**自定义购买ECS**。
3. 申请弹性公网IP。
   具体方法请参见**购买弹性公网IP**。

步骤二：创建筛选条件和镜像会话

1. 创建2个筛选条件。
   具体方法请参见**创建筛选条件**。
2. 创建2个镜像会话，关联筛选条件、镜像源以及镜像目的。
   具体方法请参见**创建镜像会话**。

步骤三：安装 NC 工具模拟数据流量

本文使用NC工具模拟数据流量，NC工具是一个通过TCP/UDP协议在网络中读写数据的工具，常用于网络端口测试等，需要在ECS-source和ECS-test中安装NC工具。

1. 在ECS-source中安装NC工具。
   a. 下载NC工具需要连接公网，将EIP绑定至ECS-source。
      具体方法请参见**绑定弹性公网IP**。
   b. 远程登录ECS-source。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。
   c. 依次执行以下命令，安装NC工具。

      sudo yum update

      回显类似如下信息：

```
[root@ecs-source ~]# sudo yum update
HCE 2.0
base
        55 MB/s | 6.1 MB     00:00
HCE 2.0
updates
          98 MB/s |  14 MB     00:00
Last metadata expiration check: 0:00:01 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
Nothing to do.
Complete!
```

      sudo yum install nc

      回显类似如下信息，请根据回显提示输入**y**，并按回车。

```
[root@ecs-source ~]# sudo yum install nc
Last metadata expiration check: 0:00:12 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
...
Install  2 Packages

Total download size: 6.1 M
Installed size: 25 M
Is this ok [y/N]: y
Downloading Packages:
...
Importing GPG key 0xA8DEF926:
```



```
 Userid     : "HCE <support@huaweicloud.com>"
 Fingerprint: C1BA 9CD4 9D03 A206 E241 F176 28DA 5B77 A8DE F926
 From       : http://repo.huaweicloud.com/hce/2.0/updates/RPM-GPG-KEY-HCE-2
Is this ok [y/N]: y
...
Installed:
  libssh2-1.10.0-2.r10.hce2.x86_64
nmap-2:7.92-2.r4.hce2.x86_64

Complete!
```

d. ECS-source的NC工具安装完成后，解绑EIP。

具体方法请参见**解绑弹性公网IP**。

2. 参考**1.a**~**1.d**，在ECS-test中安装NC工具，并解绑EIP。
3. EIP解绑后，删除EIP。

本示例中不再需要使用EIP，因此删除EIP，具体方法请参见**解绑弹性公网IP**。如果不删除EIP，则EIP会持续计费。

步骤四：验证采集 TCP 流量的镜像会话是否生效

1. 执行以下操作，建立ECS-source和ECS-test之间的TCP连接。

本文在ECS-test向ECS-source发送TCP报文，查看ECS-source是否可以收到该报文。

a. 在ECS-source中，执行以下命令，开启1234端口的监听。

nc -l *镜像源ECS-source的监听端口*

命令示例：

nc -l 1234

此处回显为空，表示监听已正常开启。

b. 在ECS-test中，执行以下命令，建立ECS-source和ECS-test之间的TCP连接。

nc *镜像源ECS-source的私有IP地址 镜像源ECS-source的监听端口*

命令示例：

nc 192.168.0.230 1234

此处回显为空，在ECS-test中，输入任意信息（比如**hello**），并按回车，测试TCP连接是否建立成功。

```
[root@ecs-test ~]# nc 192.168.0.230 1234
hello
```

c. 在ECS-source中，查看是否收到来自ECS-test的信息。

回显类似如下信息，可正常收到信息，表示TCP连接建立成功。

```
[root@ecs-source ~]# nc -l 1234
hello
```

2. 执行以下操作，测试ECS-source入方向的TCP报文是否可以镜像到ECS-target-01。

当ECS-test实时向镜像源ECS-source发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target-01是否可以获取到该报文的数据包，如果获取成功，则表示镜像会话配置生效。

a. 远程登录ECS-target-01。

ECS有多种登录方法，具体请参见**登录弹性云服务器**。

b. 在ECS-target-01中，执行以下命令，查看镜像目的对应的网卡名称。

ifconfig

回显类似如下信息，本示例中镜像目的对应的网卡名称为eth0。


```
[root@ecs-target-01 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.164  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fe7e:d67a  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:7e:d6:7a  txqueuelen 1000  (Ethernet)
        RX packets 283560  bytes 116380316 (110.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 276486  bytes 104575280 (99.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

c. 在ECS-target-01中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

命令示例：

tcpdump -i eth0 udp port 4789 -nne

回显类似如下信息：

```
[root@ecs-target-01 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

d. 在ECS-test中，输入任意信息（比如**tcp**），并按回车，向ECS-source发送TCP报文。

回显类似如下信息：

```
[root@ecs-test ~]# nc 192.168.0.230 1234
hello
tcp
```

e. 在ECS-source中，查看是否收到来自ECS-test的信息。

回显类似如下信息，可正常收到信息。

```
[root@ecs-source ~]# nc -l 1234
hello
tcp
```

f. 在ECS-target-01中，查看是否可以获取到报文的数据包。

回显类似如下信息，可以看到TCPDUMP工具启动后，ECS-test发送的信息**tcp**对应的数据包。其中，**vni 1**为镜像会话mirror-session-01的标识，表示通过mirror-session-01，ECS-target-01可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

```
[root@ecs-target-01 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:04:54.038631 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:7a, ethertype IPv4 (0x0800), length 120:
192.168.0.230.32782 > 192.168.0.164.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 70: 192.168.0.161.55602 >
192.168.0.230.1234: Flags [P.], seq 1838246001:1838246005, ack 2529760424, win 502, options
[nop,nop,TS val 1116821333 ecr 752395830], length 4
```

步骤五：验证采集 UDP 流量的镜像会话是否生效

1. 执行以下操作，建立ECS-source和ECS-test之间的UDP连接。

   本文在ECS-test向ECS-source发送UDP报文，查看ECS-source是否可以收到该报文。

   a. 在ECS-source中，执行以下命令，开启1235端口的监听。

   nc -ul *镜像源ECS-source的监听端口*

   命令示例：

nc -ul 1235

此处回显为空，表示监听已正常开启。

b. 在ECS-test中，执行以下命令，建立ECS-source和ECS-test之间的UDP连接。

nc *镜像源ECS-source的私有IP地址 镜像源ECS-source的监听端口* **-u**

命令示例：

nc 192.168.0.230 1235 -u

此处回显为空，在ECS-test中，输入任意信息（比如**hello**），并按回车，测试UDP连接是否建立成功。

```
[root@ecs-test ~]# nc 192.168.0.230 1235 -u
hello
```

c. 在ECS-source中，查看是否收到来自ECS-test的信息。

回显类似如下信息，可正常收到信息，表示UDP连接建立成功。

```
[root@ecs-source ~]# nc -ul 1235
hello
```

2. 执行以下操作，测试ECS-source入方向的UDP报文是否可以镜像到ECS-target-02。

当ECS-test实时向镜像源ECS-source发送UDP报文时，通过TCPDUMP工具，查看镜像目的ECS-target-02是否可以获取到该报文的数据包，如果获取成功，则表示镜像会话配置生效。

a. 远程登录ECS-target-02。

ECS有多种登录方法，具体请参见**登录弹性云服务器**。

b. 在ECS-target-02中，执行以下命令，查看镜像目的对应的网卡名称。

ifconfig

回显类似如下信息，本示例中镜像目的对应的网卡名称为eth0。

```
[root@ecs-target-02 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.165  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::f816:3eff:fe7e:d77b  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:7e:d7:7b  txqueuelen 1000  (Ethernet)
        RX packets 81142  bytes 112091279 (106.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11848  bytes 2318498 (2.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

c. 在ECS-target-02中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

命令示例：

tcpdump -i eth0 udp port 4789 -nne

回显类似如下信息：

```
[root@ecs-target-02 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

d. 在ECS-test中，输入任意信息（比如**udp**），并按回车，向ECS-source发送UDP报文。

回显类似如下信息：

```
[root@ecs-test ~]# nc 192.168.0.230 1235 -u
hello
udp
```


e. 在ECS-source中，查看是否收到来自ECS-test的信息。

回显类似如下信息，可正常收到信息。

```
[root@ecs-source ~]# nc -ul 1235
hello
udp
```

f. 在ECS-target-02中，查看是否可以获取到报文的数据包。

回显类似如下信息，可以看到TCPDUMP工具启动后，ECS-test发送的信息**udp**对应的数据包。其中，**vni 2**为镜像会话mirror-session-02的标识，表示通过mirror-session-02，ECS-target-02可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

```
[root@ecs-target-02 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:09:36.275574 fa:16:3e:18:32:b8 > fa:16:3e:7e:d7:7b, ethertype IPv4 (0x0800), length 96:
192.168.0.230.32830 > 192.168.1.165.4789: VXLAN, flags [I] (0x08), vni 2
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 46: 192.168.0.161.46546 >
192.168.0.230.1235: UDP, length 4
```

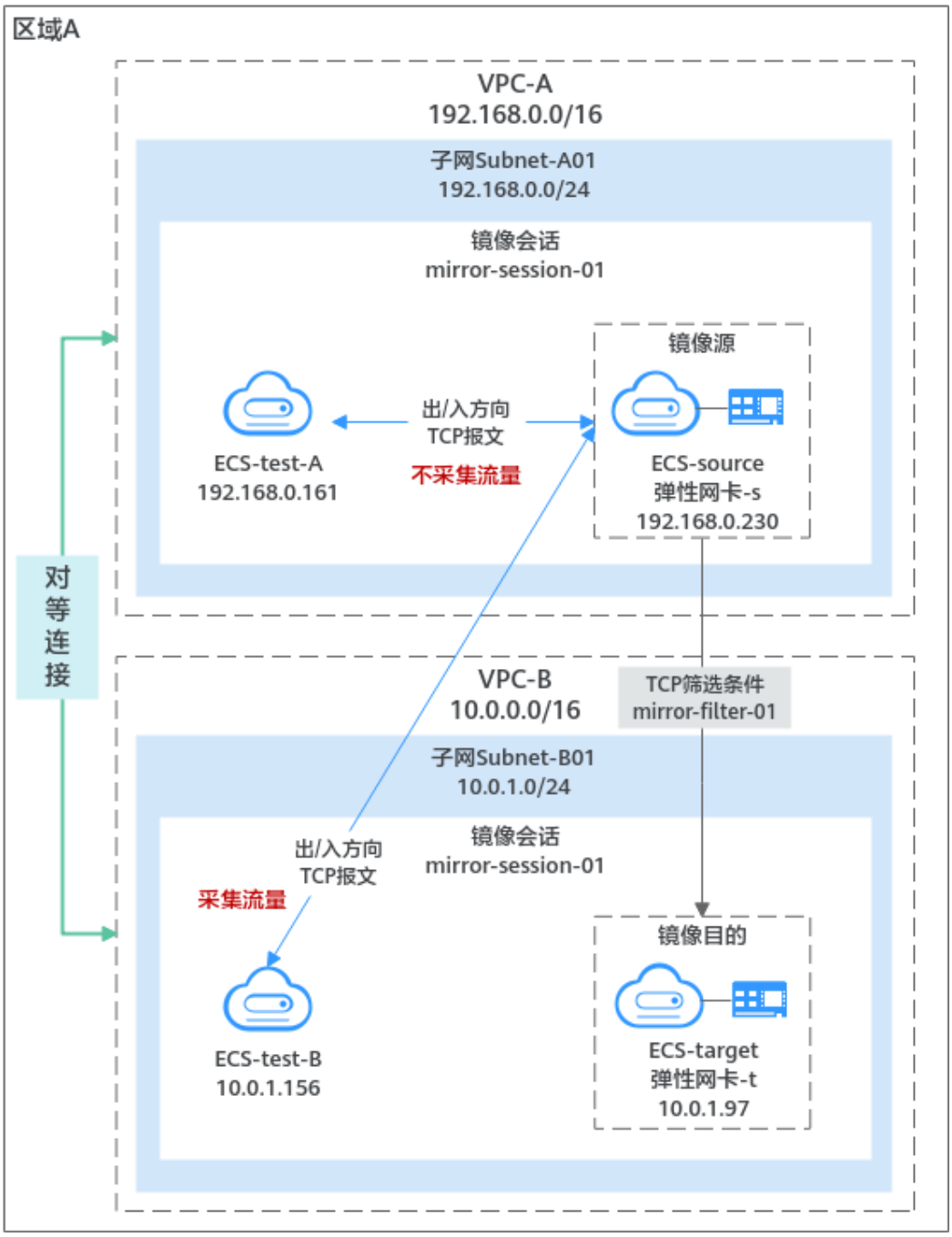
13.4.3 将源弹性网卡的出/入方向 TCP 流量镜像到其他 VPC 内的目的弹性网卡

方案架构

当您需要将镜像源（弹性网卡）和指定实例通信产生的出/入方向TCP流量，镜像到其他VPC内的镜像目的（弹性网卡）时，您可以参考本文的配置示例。如**图13-10**所示，镜像源ECS-source和镜像目的ECS-target分别位于VPC-A和VPC-B中，由于不同VPC默认网络隔离，需要先使用对等连接连通两个VPC之间的网络。本示例中，通过镜像会话将VPC-A内的ECS-source和VPC-B内的ECS-test-B之间的互访流量，镜像到VPC-B内的ECS-target中，不需要镜像VPC-A内的ECS-source和ECS-test-A之间的互访流量，则您创建1个镜像会话可以实现需求。本示例中，在镜像会话mirror-session-01进行如下配置：

- 镜像源是ECS-source的弹性网卡-s，表示需要镜像弹性网卡-s出方向和入方向的TCP流量。
- 镜像目的是ECS-target的弹性网卡-t，表示将弹性网卡-s的TCP流量镜像到弹性网卡-t中。
- 镜像会话的筛选条件mirror-filter-01中，出方向和入方向需要分别添加以下规则：
  - 两条出方向规则：规则1不采集ECS-source去往ECS-test-A的TCP流量，规则2采集ECS-source去往ECS-test-B的TCP流量。
  - 两条入方向规则：规则1不采集ECS-test-A进入ECS-source的TCP流量，规则2采集ECS-test-B进入ECS-source的TCP流量。

图 13-10 镜像出/入方向 TCP 流量到其他 VPC 内的镜像目的



约束与限制

关于流量镜像的使用限制，具体请查看**流量镜像的使用限制**。

资源规划说明

本示例中，虚拟私有云VPC和子网、弹性公网IP以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 13-33 镜像出/入方向 TCP 流量资源规划总体说明

资源类型	资源数量	说明
虚拟私有云VPC和子网	VPC：2 子网：2	本示例中，共需要2个VPC，配置说明如下： ● VPC名称：请根据实际情况设置，本示例分别为VPC-A和VPC-B。 ● IPv4网段：请根据实际情况设置，本示例VPC-A为192.168.0.0/16、VPC-B为10.0.0.0/16。 ● 子网名称：请根据实际情况设置，本示例共2个子网，VPC-A内的子网为Subnet-A01、VPC-B内的子网为Subnet-B01。 ● 子网IPv4网段：请根据实际情况设置，本示例Subnet-A01为192.168.0.0/24，Subnet-B01为10.0.1.0/24。

资源类型	资源数量	说明
弹性云服务器ECS	4	本示例中，共需要4个ECS，配置说明如下： • 名称：根据实际情况设置，本示例分别为ECS-source、ECS-target、ECS-test-A和ECS-test-B。 • 实例规格类型：本示例中镜像源ECS-source使用通用计算增强型c7t，当前仅支持部分规格ECS的弹性网卡作为镜像源，具体请参见**流量镜像的使用限制**。其他ECS的规格类型不做限制。 • 镜像：请根据实际情况设置，本示例为公共镜像（Huawei Cloud EulerOS 2.0 标准版 64位）。 • 系统盘：通用型SSD盘，40GB。 • 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例ECS-source和ECS-test-A为VPC-A、ECS-target和ECS-test-B为VPC-B。 – 子网：选择子网，本示例ECS-source和ECS-test-A为Subnet-A01、ECS-target和ECS-test-B为Subnet-B01。 • 安全组：本示例中，4个ECS属于同一个安全组Sg-X，需要确保**表13-34**中的规则均已正确添加即可。 如果ECS属于不同的安全组，则除了分别在不同安全组配置**表13-34**中的规则外，还需要添加以下规则： – 如果访问镜像源的测试ECS和镜像源ECS属于不同安全组，比如ECS-test-A属于Sg-X，ECS-source属于Sg-A，则需要在Sg-A和Sg-X中额外添加**表13-35**中的规则，允许ECS-test-A和ECS-source流量互访。ECS-test-B同理。 – 如果镜像源ECS和镜像目的ECS属于不同安全组，比如ECS-source属于Sg-A，ECS-target属于Sg-B，则需要在Sg-B中额外添加**表13-36**中的规则，允许来自镜像源封装的UDP协议报文访问镜像目的的4789端口。 • 弹性公网IP：选择“暂不购买”。 • 私有IP地址：ECS-source为192.168.0.230，ECS-target为10.0.1.97，ECS-test-A为192.168.0.161，ECS-test-B为10.0.1.156
弹性公网IP	1	• 计费模式：请根据情况选择计费模式，本示例为按需计费。 • EIP名称：请根据实际情况设置，本示例为EIP-A。 • EIP地址：EIP地址系统随机分配，本示例为124.X.X.187。

资源类型	资源数量	说明
VPC对等连接	1	• 名称：请根据实际情况设置，本示例为Peering-AB。 • 本端VPC：请根据实际情况设置，本示例为VPC-A，网段为192.168.0.0/16。 • 账户：本示例中VPC-A和VPC-B属于同一个账户，选择“当前账户”。 如果您的两个VPC属于不同账号，则流量镜像不支持跨账号使用。 • 对端项目：保持默认选择。 • 对端VPC：请根据实际情况设置，本示例为VPC-B，网段为10.0.0.0/16。 • 对等连接路由，请根据实际情况设置，本示例路由规划详情请参见**表13-37**。
筛选条件	1	• 名称：请根据实际情况设置，本示例为mirror-filter-01。 • 入方向规则：添加2条入方向规则，规则详情请参见**表13-38**。 – 规则1：表示不采集VPC-A内所有实例进入镜像源ECS-source的TCP流量。ECS-test-A属于VPC-A，本示例中不采集ECS-test-A进入ECS-source的TCP流量。 – 规则2：表示采集VPC-B内所有实例进入镜像源ECS-source的TCP流量。ECS-test-B属于VPC-B，本示例中采集ECS-test-B进入ECS-source的TCP流量。 • 出方向规则：添加2条出方向规则，规则详情请参见**表13-38**。 – 规则1：表示不采集镜像源ECS-source去往VPC-A内所有实例的TCP流量。ECS-test-A属于VPC-A，本示例中不采集ECS-source去往ECS-test-A的TCP流量。 – 规则2：表示采集镜像源ECS-source去往VPC-B内所有实例的TCP流量。ECS-test-B属于VPC-B，本示例中采集ECS-source去往ECS-test-B的TCP流量。

资源类型	资源数量	说明
镜像会话	1	• 镜像会话基本信息： – 名称：请根据实际情况设置，本示例为mirror-session-01。 – 优先级：请根据实际情况设置，本示例为1。 – VXLAN网络标识：请根据实际情况设置，本示例为1。 – 镜像报文长度：请根据实际情况设置，本示例为96。 – 是否开启：开启，镜像会话开启后，才会监控镜像源的网络流量。 • 关联筛选条件：请根据实际情况设置，本示例为mirror-filter-01。 • 关联镜像源：请根据实际情况设置，本示例为ECS-source的弹性网卡，私有IP地址为192.168.0.230。 • 关联镜像目的： – 类型：云服务器网卡 – 网卡：请根据实际情况设置，本示例为ECS-target的弹性网卡，私有IP地址为10.0.1.97。

表 13-34 安全组 Sg-X 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址：0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址：0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	全部	源地址：当前安全组Sg-X	针对IPv4，用于安全组内ECS之间网络互通。
入方向	允许	IPv6	全部	源地址：当前安全组Sg-X	针对IPv6，用于安全组内ECS之间网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

须知

本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

表 13-35 安全组 Sg-A 和 Sg-X 规则说明（允许 ECS 流量互访）

安全组	方向	策略	类型	协议端口	源地址	描述
Sg-A	入方向	允许	IPv4	TCP: 1234	本示例放通ECS-test-A所在安全组的流量 安全组：Sg-X	针对IPv4，允许来自ECS-test-A的TCP协议报文访问镜像源ECS-source的1234端口。
Sg-X	入方向	允许	IPv4	TCP: 全部	本示例放通ECS-source所在安全组的流量 安全组：Sg-A	针对IPv4，允许来自镜像源ECS-source的TCP协议报文访问ECS-test-A的全部端口。

表 13-36 安全组 Sg-B 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	UDP: 4789	镜像源的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	针对IPv4，允许来自镜像源ECS-source封装的UDP协议报文访问镜像目的ECS-target的4789端口。

表 13-37 VPC 对等连接路由

虚拟私有云	路由表	目的地址	下一跳	描述
VPC-A	rtb-VPC-A（默认路由表）	本示例为VPC-B的网段： 10.0.0.0/16	对等连接：Peering-AB	本端VPC-A到对端VPC-B的去程路由。
VPC-B	rtb-VPC-B（默认路由表）	本示例为VPC-A的网段： 192.168.0.0/16	对等连接：Peering-AB	对端VPC-B到本端VPC-A的回程路由。

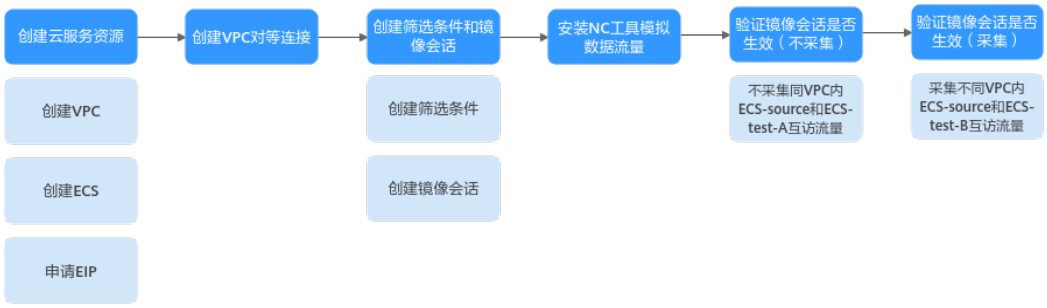
表 13-38 筛选条件的入方向和出方向规则

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围
入方向	1	TCP	不采集	IPv4	报文的来源地址，本示例为VPC-A的网段： 192.168.0.0/16	全部	报文的目的地址，本示例为VPC-A的网段： 192.168.0.0/16	全部
入方向	2	TCP	采集	IPv4	报文的来源地址，本示例为VPC-B的网段： 10.0.0.0/16	全部	报文的目的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	本示例为ECS-source的1234端口： 1234-1234
出方向	1	TCP	不采集	IPv4	报文的来源地址，本示例为VPC-A的网段： 192.168.0.0/16	全部	报文的目的地址，本示例为VPC-A的网段： 192.168.0.0/16	全部
出方向	2	TCP	采集	IPv4	报文的来源地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	全部	报文的目的地址，本示例为VPC-B的网段： 10.0.0.0/16	本示例为ECS-test-B的1234端口： 1234-1234

操作流程

将源弹性网卡和指定实例通信产生的出/入方向TCP流量，镜像到其他VPC内的弹性网卡，流程如图13-11所示。

图 13-11 镜像出/入方向 TCP 流量到其他 VPC 内的镜像目的



步骤一：创建云服务资源

1. 创建2个VPC和2个子网。
   具体方法请参见**创建虚拟私有云和子网**。
2. 创建4个ECS。
   具体方法请参见**自定义购买ECS**。
3. 申请弹性公网IP。
   具体方法请参见**购买弹性公网IP**。

步骤二：创建 VPC 对等连接

创建VPC对等连接，连通VPC-A和VPC-B之间的网络，具体方法请参见**创建相同账户下的对等连接**。

对等连接创建完成，需要在VPC-A和VPC-B的路由表分别添加连通去程和回程的路由，两端VPC才可以通信，本示例的路由规划详情请参见**表13-37**。

步骤三：创建筛选条件和镜像会话

1. 创建1个筛选条件。
   具体方法请参见**创建筛选条件**。
2. 创建1个镜像会话，关联筛选条件、镜像源以及镜像目的。
   具体方法请参见**创建镜像会话**。

步骤四：安装 NC 工具模拟数据流量

本文使用NC工具模拟数据流量，NC工具是一个通过TCP/UDP协议在网络中读写数据的工具，常用于网络端口测试等，需要在ECS-source、ECS-test-A和ECS-test-B中安装NC工具。

1. 在ECS-source中安装NC工具。
   a. 下载NC工具需要连接公网，将EIP绑定至ECS-source。
      具体方法请参见**绑定弹性公网IP**。
   b. 远程登录ECS-source。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。
   c. 依次执行以下命令，安装NC工具。
      sudo yum update
      回显类似如下信息：

```
[root@ecs-source ~]# sudo yum update
HCE 2.0
base
        55 MB/s | 6.1 MB     00:00
HCE 2.0
updates
          98 MB/s |  14 MB     00:00
Last metadata expiration check: 0:00:01 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
Nothing to do.
Complete!
```

      sudo yum install nc
      回显类似如下信息，请根据回显提示输入**y**，并按回车。

```
[root@ecs-source ~]# sudo yum install nc
Last metadata expiration check: 0:00:12 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
...
Install  2 Packages

Total download size: 6.1 M
Installed size: 25 M
Is this ok [y/N]: y
Downloading Packages:
...
Importing GPG key 0xA8DEF926:
 Userid     : "HCE <support@huaweicloud.com>"
 Fingerprint: C1BA 9CD4 9D03 A206 E241 F176 28DA 5B77 A8DE F926
 From       : http://repo.huaweicloud.com/hce/2.0/updates/RPM-GPG-KEY-HCE-2
Is this ok [y/N]: y
...
Installed:
  libssh2-1.10.0-2.r10.hce2.x86_64
nmap-2:7.92-2.r4.hce2.x86_64

Complete!
```

d. ECS-source的NC工具安装完成后，解绑EIP。

具体方法请参见**解绑弹性公网IP**。

2. 参考**1.a**~**1.d**，在ECS-test-A中安装NC工具，并解绑EIP。
3. 参考**1.a**~**1.d**，在ECS-test-B中安装NC工具，并解绑EIP。
4. EIP解绑后，删除EIP。

本示例中不再需要使用EIP，因此删除EIP，具体方法请参见**解绑弹性公网IP**。如果不删除EIP，则EIP会持续计费。

步骤五：验证镜像会话是否对 ECS-source 和 ECS-test-A 互访的流量生效

本示例中，将验证镜像会话不采集相同VPC内，ECS-source和ECS-test-A互访的流量。

1. 执行以下操作，建立ECS-source和ECS-test-A之间的TCP连接。

本示例在ECS-source向ECS-test-A发送TCP报文，查看ECS-test-A是否可以收到该报文。

a. 在ECS-source中，执行以下命令，开启1234端口的监听。

nc -l *镜像源ECS-source的监听端口*

命令示例：

nc -l 1234

此处回显为空，表示监听已正常开启。

b. 在ECS-test-A中，执行以下命令，建立ECS-source和ECS-test-A之间的TCP连接。

nc *镜像源ECS-source的私有IP地址 镜像源ECS-source的监听端口*

命令示例：

nc 192.168.0.230 1234

此处回显为空，表示TCP连接已建立。

c. 在ECS-source中，输入任意信息（比如**hello**），并按回车，测试TCP连接是否建立成功。

```
[root@ecs-source ~]# nc -l 1234
hello
```

d. 在ECS-test-A中，查看是否收到来自ECS-source的信息。

回显类似如下信息，可正常收到信息，表示TCP连接建立成功。

```
[root@ecs-test-a ~]# nc 192.168.0.230 1234
hello
```

2. 执行以下操作，测试ECS-source去往ECS-test-A的出方向TCP报文，是否可以镜像到ECS-target。

   当镜像源ECS-source实时向ECS-test-A发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target是否可以获取到该报文的数据包，如果获取不到，则表示出方向的不采集规则配置生效。

   a. 远程登录ECS-target。

      ECS有多种登录方法，具体请参见**登录弹性云服务器**。

   b. 在ECS-target中，执行以下命令，查看镜像目的对应的网卡名称。

      ifconfig

      回显类似如下信息，本示例中镜像目的对应的网卡名称为eth0。

      ```
      [root@ecs-target ~]# ifconfig
      eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 10.0.1.97  netmask 255.255.255.0  broadcast 10.0.1.255
            inet6 fe80::f816:3eff:fea0:a101  prefixlen 64  scopeid 0x20<link>
            ether fa:16:3e:a0:a1:01  txqueuelen 1000  (Ethernet)
            RX packets 103445  bytes 119352826 (113.8 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 34118  bytes 15630293 (14.9 MiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
      ...
      ```

   c. 在ECS-target中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

      tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

      命令示例：

      tcpdump -i eth0 udp port 4789 -nne

      回显类似如下信息：

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      ```

   d. 在ECS-source中，输入任意信息（比如**to testa**），并按回车，向ECS-test-A发送TCP报文。

      回显类似如下信息：

      ```
      [root@ecs-source ~]# nc -l 1234
      hello
      to testa
      ```

   e. 在ECS-test-A中，查看是否收到来自ECS-source的信息。

      回显类似如下信息，可正常收到信息。

      ```
      [root@ecs-test-a ~]# nc 192.168.0.230 1234
      hello
      to testa
      ```

   f. 在ECS-target中，查看是否可以获取到报文的数据包。

      回显类似如下信息，可以看到TCPDUMP工具启动后，没有获取到ECS-source发送至ECS-test-A的信息**to testa**对应的数据包，表示出方向的不采集规则设置成功。

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      ```

3. 执行以下操作，测试ECS-test-A进入ECS-source的入方向TCP报文，是否可以镜像到ECS-target。

当ECS-test-A实时向镜像源ECS-source发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target是否可以获取到该报文的数据包，如果获取不到，则表示入方向的不采集规则配置生效。

a. 在ECS-test-A中，输入任意信息（比如**testa to source**），并按回车，向ECS-source发送TCP报文。

回显类似如下信息：

```
[root@ecs-test-a ~]# nc 192.168.0.230 1234
hello
to testa
testa to source
```

b. 在ECS-source中，查看是否收到来自ECS-test-A的信息。

回显类似如下信息，可正常收到信息。

```
[root@ecs-source ~]# nc -l 1234
hello
to testa
testa to source
```

c. 在ECS-target中，查看是否可以获取到报文的数据包。

回显类似如下信息，可以看到TCPDUMP工具启动后，没有获取到ECS-test-A发送至ECS-source的信息**testa to source**对应的数据包，表示入方向的不采集规则设置成功。

```
[root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

步骤六：验证镜像会话是否对 ECS-source 和 ECS-test-B 互访的流量生效

本示例中，将验证镜像会话采集不同VPC内，ECS-source和ECS-test-B互访的流量。

1. 执行以下操作，建立ECS-source和ECS-test-B之间的TCP连接。

本示例在ECS-test-B向ECS-source发送TCP报文，查看ECS-source是否可以收到该报文。

a. 在ECS-test-B中，执行以下命令，开启1234端口的监听。

nc -l *ECS-test-B的监听端口*

命令示例：

nc -l 1234

此处回显为空，表示监听已正常开启。

b. 在ECS-source中，执行以下命令，建立ECS-source和ECS-test-B之间的TCP连接。

nc *ECS-test-B的私有IP地址 ECS-test-B的监听端口*

命令示例：

nc 10.0.1.156 1234

此处回显为空，表示TCP连接已建立。

c. 在ECS-test-B中，输入任意信息（比如**hello**），并按回车，测试TCP连接是否建立成功。

```
[root@ecs-test-b ~]# nc -l 1234
hello
```

d. 在ECS-source中，查看是否收到来自ECS-test-B的信息。

回显类似如下信息，可正常收到信息，表示TCP连接建立成功。


```
[root@ecs-source ~]# nc 10.0.1.156 1234
hello
```

2. 执行以下操作，测试ECS-source去往ECS-test-B的出方向TCP报文，是否可以镜像到ECS-target。

   当镜像源ECS-source实时向ECS-test-B发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target是否可以获取到该报文的数据包，如果可以获取到，则表示出方向的采集规则配置生效。

   a. 远程登录ECS-target。

      ECS有多种登录方法，具体请参见**登录弹性云服务器**。

   b. 在ECS-target中，执行以下命令，查看镜像目的对应的网卡名称。

      ifconfig

      回显类似如下信息，本示例中镜像目的对应的网卡名称为eth0。

      ```
      [root@ecs-target ~]# ifconfig
      eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 10.0.1.97  netmask 255.255.255.0  broadcast 10.0.1.255
            inet6 fe80::f816:3eff:fea0:a101  prefixlen 64  scopeid 0x20<link>
            ether fa:16:3e:a0:a1:01  txqueuelen 1000  (Ethernet)
            RX packets 103445  bytes 119352826 (113.8 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 34118  bytes 15630293 (14.9 MiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
      ...
      ```

   c. 在ECS-target中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

      tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

      命令示例：

      tcpdump -i eth0 udp port 4789 -nne

      回显类似如下信息：

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      ```

   d. 在ECS-source中，输入任意信息（比如**to testb**），并按回车，向ECS-test-B发送TCP报文。

      回显类似如下信息：

      ```
      [root@ecs-source ~]# nc 10.0.1.156 1234
      hello
      to testb
      ```

   e. 在ECS-test-B中，查看是否收到来自ECS-source的信息。

      回显类似如下信息，可正常收到信息。

      ```
      [root@ecs-test-b ~]# nc -l 1234
      hello
      to testb
      ```

   f. 在ECS-target中，查看是否可以获取到报文的数据包。

      回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-source发送至ECS-test-B的信息**to testb**对应的数据包，时间为**17:28:48.772658**，表示出方向的采集规则设置成功。其中，**vni 1**为镜像会话mirror-session-01的标识，表示通过mirror-session-01，ECS-target可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      ```



```
17:28:48.772658 fa:16:3e:6e:42:80 > fa:16:3e:a0:a1:01, ethertype IPv4 (0x0800), length 125:
192.168.0.230.32821 > 10.0.1.97.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:bc > fa:16:3e:d1:6b:5d, ethertype IPv4 (0x0800), length 75: 192.168.0.230.44906 >
10.0.1.156.1234: Flags [P.], seq 935460393:935460402, ack 4279496885, win 502, options
[nop,nop,TS val 1414482596 ecr 3323401462], length 9
```

3. 执行以下操作，测试ECS-test-B进入ECS-source的入方向TCP报文，是否可以镜像到ECS-target。

   当ECS-test-B实时向镜像源ECS-source发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target是否可以获取到该报文的数据包，如果可以获取到，则表示入方向的采集规则配置生效。

   a. 在ECS-test-B中，输入任意信息（比如**testb to source**），并按回车，向ECS-source发送TCP报文。

      回显类似如下信息：

      ```
      [root@ecs-test-b ~]# nc -l 1234
      hello
      to testb
      testb to source
      ```

   b. 在ECS-source中，查看是否收到来自ECS-test-B的信息。

      回显类似如下信息，可正常收到信息。

      ```
      [root@ecs-source ~]# nc 10.0.1.156 1234
      hello
      to testb
      testb to source
      ```

   c. 在ECS-target中，查看是否可以获取到报文的数据包。

      回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-test-B发送至ECS-source的信息**testb to source**对应的数据包，时间为**17:30:26.193420**，表示入方向的采集规则设置成功。其中，**vni 1**为镜像会话mirror-session-01的标识，表示通过mirror-session-01，ECS-target可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

      ```
      [root@ecs-target ~]# tcpdump -i eth0 udp port 4789 -nne
      dropped privs to tcpdump
      tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
      listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
      17:28:48.772658 fa:16:3e:6e:42:80 > fa:16:3e:a0:a1:01, ethertype IPv4 (0x0800), length 125:
      192.168.0.230.32821 > 10.0.1.97.4789: VXLAN, flags [I] (0x08), vni 1
      fa:16:3e:7e:d6:bc > fa:16:3e:d1:6b:5d, ethertype IPv4 (0x0800), length 75: 192.168.0.230.44906 >
      10.0.1.156.1234: Flags [P.], seq 935460393:935460402, ack 4279496885, win 502, options
      [nop,nop,TS val 1414482596 ecr 3323401462], length 9
      17:30:26.193420 fa:16:3e:6e:42:80 > fa:16:3e:a0:a1:01, ethertype IPv4 (0x0800), length 116:
      192.168.0.230.32821 > 10.0.1.97.4789: VXLAN, flags [I] (0x08), vni 1
      fa:16:3e:7e:d6:bc > fa:16:3e:d1:6b:5d, ethertype IPv4 (0x0800), length 66: 192.168.0.230.44906 >
      10.0.1.156.1234: Flags [.], ack 17, win 502, options [nop,nop,TS val 1414580016 ecr
      3323563970], length 0
      ```

13.4.4 将源弹性网卡的出/入方向 TCP 流量镜像到目的 ELB

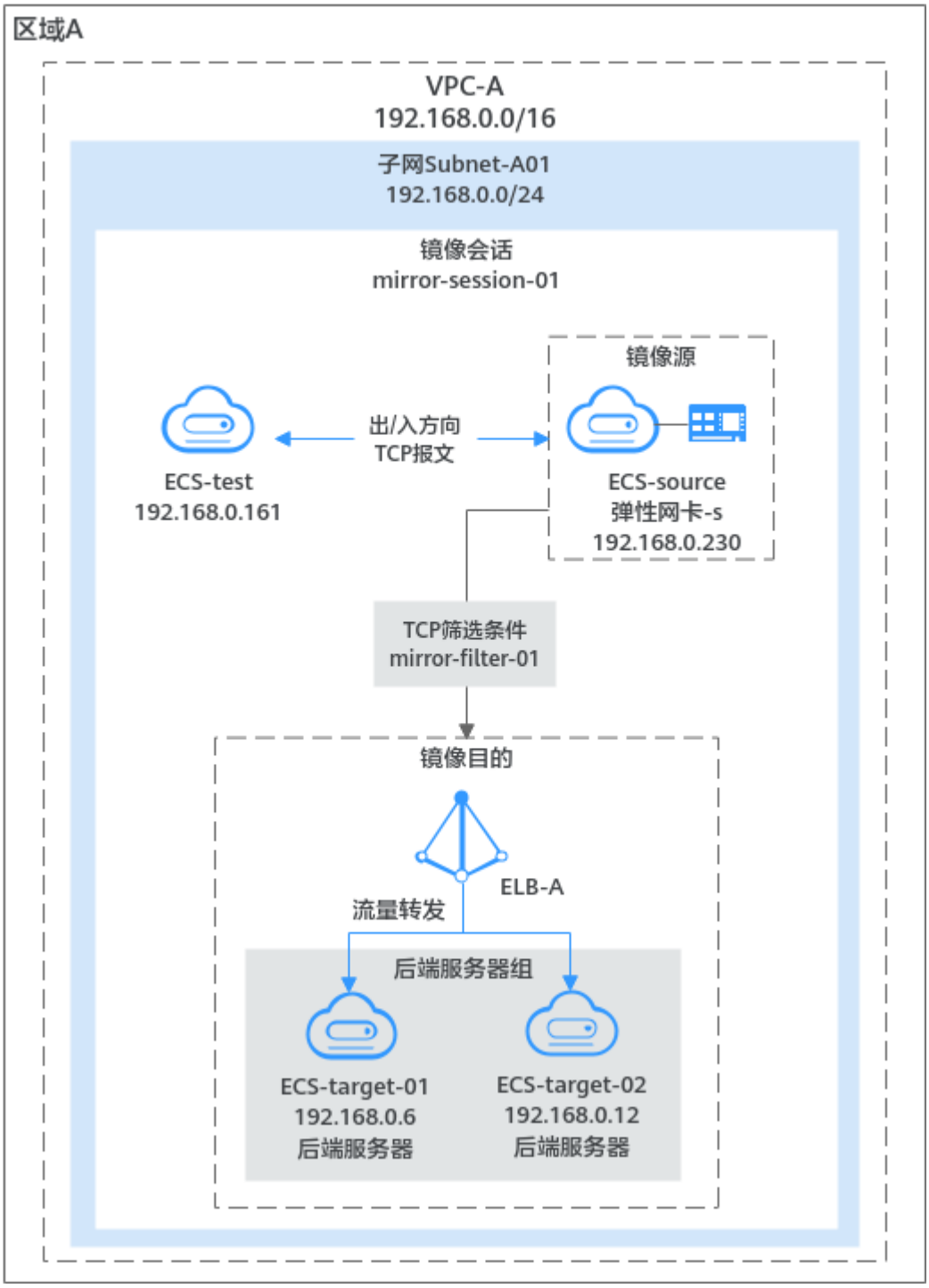
方案架构

当您需要将镜像源（弹性网卡）和指定实例通信产生的出/入方向TCP流量，镜像到弹性负载均衡ELB时，您可以参考本文的配置示例。如**图13-12**所示，在VPC-A中，通过镜像会话将ECS-source和ECS-test之间互访的TCP流量镜像到ELB-A中，则您创建1个镜像会话可以实现需求。本示例中，在镜像会话mirror-session-01进行如下配置：

- 镜像源是ECS-source的弹性网卡-s，表示需要镜像弹性网卡-s出方向和入方向的TCP流量。

- 镜像目的是ELB-A，表示将弹性网卡-s的TCP流量镜像到ELB-A中，ELB-A将根据流量分发策略，将镜像流量分发至两台后端服务器ECS-target-01和ECS-target-02。
- 镜像会话的筛选条件mirror-filter-01中，出方向和入方向需要分别添加以下规则：
  - 出方向规则：采集ECS-source去往ECS-test的TCP流量。
  - 入方向规则：采集ECS-test进入ECS-source的TCP流量。

图 13-12 镜像出/入方向 TCP 流量到目的 ELB



约束与限制

关于流量镜像的使用限制，具体请查看**流量镜像的使用限制**。

资源规划说明

本示例中，虚拟私有云VPC和子网、弹性公网IP、弹性负载均衡ELB以及弹性云服务器ECS等资源只要位于同一个区域内即可，可用区可以任意选择，无需保持一致。

说明

以下资源规划详情仅为示例，您可以根据需要自行修改。

表 13-39 镜像出/入方向 TCP 流量到目的 ELB 资源规划总体说明

资源类型	资源数量	说明
虚拟私有云VPC和子网	VPC：1 子网：1	• VPC名称：请根据实际情况设置，本示例为VPC-A。 • IPv4网段：请根据实际情况设置，本示例为192.168.0.0/16。 • 子网名称：请根据实际情况设置，本示例为Subnet-A01。 • 子网IPv4网段：请根据实际情况设置，本示例为192.168.0.0/24。

资源类型	资源数量	说明
弹性云服务器ECS	4	本示例中，共需要4个ECS，配置说明如下： • 名称：根据实际情况设置，本示例分别为ECS-source、ECS-target-01、ECS-target-02和ECS-test。 • 实例规格类型：本示例中镜像源ECS-source使用通用计算增强型c7t，当前仅支持部分规格ECS的弹性网卡作为镜像源，具体请参见**流量镜像的使用限制**。其他ECS的规格类型不做限制。 • 镜像：请根据实际情况设置，本示例为公共镜像（Huawei Cloud EulerOS 2.0 标准版 64位）。 • 系统盘：通用型SSD盘，40GB。 • 数据盘：本示例未选购数据盘，请您根据实际业务需求选购数据盘。 • 网络： – 虚拟私有云：选择您的虚拟私有云，本示例ECS均选择VPC-A。 – 子网：选择子网，本示例ECS均选择Subnet-A01。 • 安全组：本示例中，4个ECS属于同一个安全组Sg-X，需要确保**表13-40**中的规则均已正确添加即可。 如果ECS属于不同的安全组，则除了分别在不同安全组配置**表13-40**中的规则外，还需要添加以下规则： – 如果访问镜像源的测试ECS和镜像源ECS属于不同安全组，比如ECS-test属于Sg-X，ECS-source属于Sg-A，则需要在Sg-A和Sg-X中额外添加**表13-41**中的规则，允许ECS-test和ECS-source流量互访。 – 如果镜像源ECS和镜像目的ECS属于不同安全组，比如ECS-source属于Sg-A，ECS-target-01属于Sg-B，则需要在Sg-B中额外添加**表13-42**中的规则，允许来自镜像源封装的UDP协议报文访问镜像目的的4789端口。ECS-target-02同理。 • 弹性公网IP：选择“暂不购买”。 • 私有IP地址：ECS-source为192.168.0.230，ECS-target-01为192.168.0.6，ECS-target-02为192.168.0.12，ECS-test为192.168.0.161
弹性公网IP	1	• 计费模式：请根据情况选择计费模式，本示例为按需计费。 • EIP名称：请根据实际情况设置，本示例为EIP-A。 • EIP地址：EIP地址系统随机分配，本示例为124.X.X.187。

资源类型	资源数量	说明
弹性负载均衡	1	● 实例类型：当前仅独享型ELB支持作为镜像目的，请选择独享型。 ● 名称：请根据实际情况设置，本示例为ELB-A。 ● 实例规格：由于封装的镜像报文为IPv4 UDP协议，此处ELB必须支持UDP协议，因此本示例选择网络型（TCP/UDP/TLS）。不同区域的实例规格存在差异，如果您所在区域没有网络型（TCP/UDP/TLS），选择网络型（TCP/UDP）即可。 ● 网络类型：由于封装的镜像报文为IPv4 UDP协议，此处ELB必须支持IPv4，因此本示例选择IPv4私网。 ● 所属VPC：请根据实际情况设置，本示例为VPC-A。 ● 前端子网：请根据实际情况设置，本示例为Subnet-A01。 ● IPv4地址：请根据实际情况设置，本示例为自动分配IP地址。 ● 后端子网：请根据实际情况设置，本示例为与前端子网保持一致。 ● IP类型后端（跨VPC后端）：本示例中后端服务器位于同一VPC中，因此未开启，请您根据实际情况设置。 ● 弹性公网IP：请根据实际情况设置，本示例为暂不购买。

资源类型	资源数量	说明
监听器	1	• 配置监听器： – 名称：请根据实际情况设置，本示例为listener-A。 – 前端协议：由于封装的镜像报文为UDP协议，此处请选择UDP。 – 前端端口：镜像目的接受流量的固定端口为4789，此处请填写4789。 – 访问控制：本示例选择允许所有IP访问，请您根据实际情况设置，如果选择白名单，需要确保镜像源IP地址在白名单中。 • 配置后端分配策略： – 转发模式：请根据实际情况设置，本示例为负载均衡。 – 服务器组类型：请根据实际情况设置，本示例为混合类型。 – 名称：请根据实际情况设置，本示例为serve_group-A。 – 后端协议：由于封装的镜像报文为UDP协议，此处请选择UDP。 – 全端口转发：请根据实际情况设置，本示例不开启。 – 分配策略类型：请根据实际情况设置，本示例为加权轮询算法。 – 会话保持：请根据实际情况设置，本示例不开启。 • 添加后端服务器 – 在“云服务器”页签下，选择后端服务器，本示例选择ECS-target-01和ECS-target-02。 业务端口固定为4789，权重请根据实际情况设置，本示例为1。 – 健康检查：本示例为不开启，由于后端服务器并未启动监听4789端口的进程，而健康检查需要保证后端服务器的4789端口处于监听状态。此时如果开启健康检查，会导致后端服务器的健康状态异常，ELB将无法将流量转发至后端服务器。
筛选条件	1	• 名称：请根据实际情况设置，本示例为mirror-filter-01。 • 入方向规则：添加1条入方向规则，采集ECS-test进入ECS-source的TCP流量。 • 出方向规则：添加1条出方向规则，采集ECS-source去往ECS-test的TCP流量。 规则详情请参见**表13-43**。

资源类型	资源数量	说明
镜像会话	1	• 镜像会话基本信息： – 名称：请根据实际情况设置，本示例为mirror-session-01。 – 优先级：请根据实际情况设置，本示例为1。 – VXLAN网络标识：请根据实际情况设置，本示例为1。 – 镜像报文长度：请根据实际情况设置，本示例为96。 – 是否开启：开启，镜像会话开启后，才会监控镜像源的网络流量。 • 关联筛选条件：请根据实际情况设置，本示例为mirror-filter-01。 • 关联镜像源：请根据实际情况设置，本示例为ECS-source的弹性网卡，私有IP地址为192.168.0.230。 • 关联镜像目的： – 类型：弹性负载均衡 – 网卡：请根据实际情况设置，本示例为ELB-A，私有IP地址为192.168.0.147。

表 13-40 安全组 Sg-X 规则说明

方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	TCP: 22	源地址：0.0.0.0/0	放通安全组内ECS的SSH(22)端口，用于远程登录Linux ECS。
入方向	允许	IPv4	TCP: 3389	源地址：0.0.0.0/0	放通安全组内ECS的RDP(3389)端口，用于远程登录Windows ECS。
入方向	允许	IPv4	全部	源地址：当前安全组Sg-X	针对IPv4，用于安全组内ECS之间网络互通。
入方向	允许	IPv6	全部	源地址：当前安全组Sg-X	针对IPv6，用于安全组内ECS之间网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对IPv4，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。
出方向	允许	IPv6	全部	目的地址：::/0	针对IPv6，用于安全组内ECS访问外部，允许流量从安全组内ECS流出。

须知

本示例中，入方向源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，如果将22或3389端口暴露到公网，可能存在网络安全风险，建议您将源IP设置为已知的IP地址，比如设置为您的本地PC地址。

表 13-41 安全组 Sg-A 和 Sg-X 规则说明（允许 ECS 流量互访）

安全组	方向	策略	类型	协议端口	源地址	描述
Sg-A	入方向	允许	IPv4	TCP: 1234	本示例放通ECS-test所在安全组的流量 安全组：Sg-X	针对IPv4，允许来自ECS-test的TCP协议报文访问镜像源ECS-source的1234端口。
Sg-X	入方向	允许	IPv4	TCP: 全部	本示例放通ECS-source所在安全组的流量 安全组：Sg-A	针对IPv4，允许来自镜像源ECS-source的TCP协议报文访问ECS-test的全部端口。

表 13-42 安全组 Sg-B 规则说明

方向	策略	类型	协议端口	源地址	描述
入方向	允许	IPv4	UDP: 4789	镜像源的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	针对IPv4，允许来自镜像源ECS-source封装的UDP协议报文访问镜像目的ECS-target-01的4789端口。

表 13-43 筛选条件的入方向和出方向规则

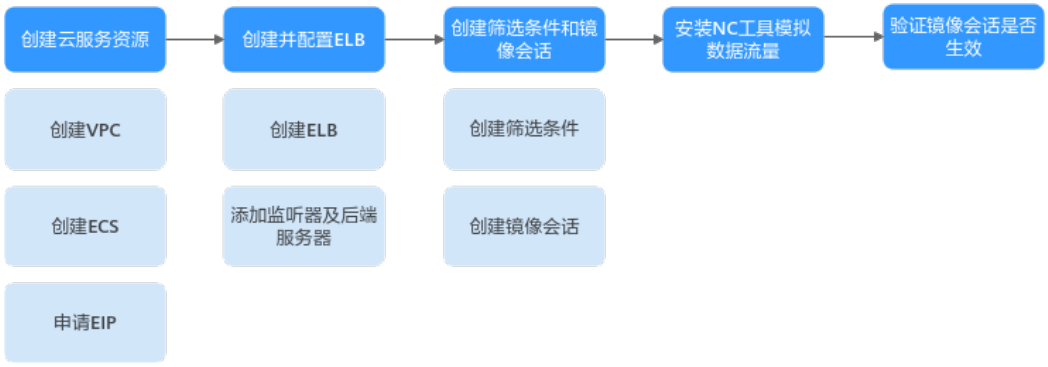
方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围
入方向	1	TCP	采集	IPv4	报文的来源地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	全部	报文的目的地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	本示例为ECS-source的1234端口： 1234-1234

方向	优先级	协议	策略	类型	源地址	源端口范围	目的地址	目的端口范围
出方向	1	TCP	采集	IPv4	报文的来源地址，本示例为ECS-source的私有IP地址： 192.168.0.230/32	本示例为ECS-source的1234端口： 1234-1234	报文的目的地址，本示例为ECS-test的私有IP地址： 192.168.0.161/32	全部

操作流程

将源弹性网卡和指定实例通信产生的出/入方向TCP流量，镜像到ELB，流程如图13-13所示。

图 13-13 镜像出/入方向 TCP 流量到目的 ELB



步骤一：创建云服务资源

1. 创建1个VPC和1个子网。
   具体方法请参见**创建虚拟私有云和子网**。
2. 创建4个ECS。
   具体方法请参见**自定义购买ECS**。
3. 申请弹性公网IP。
   具体方法请参见**购买弹性公网IP**。

步骤二：创建并配置 ELB

1. 创建独享型ELB。
   具体方法请参见**购买独享型负载均衡器**。
2. 为ELB添加UDP监听器，并配置后端服务器。
   体方法请参见**添加UDP监听器**。

步骤三：创建筛选条件和镜像会话

1. 创建1个筛选条件。
   具体方法请参见**创建筛选条件**。
2. 创建1个镜像会话，关联筛选条件、镜像源以及镜像目的。
   具体方法请参见**创建镜像会话**。

步骤四：安装 NC 工具模拟数据流量

本文使用NC工具模拟数据流量，NC工具是一个通过TCP/UDP协议在网络中读写数据的工具，常用于网络端口测试等，需要在ECS-source和ECS-test中安装NC工具。

1. 在ECS-source中安装NC工具。
   a. 下载NC工具需要连接公网，将EIP绑定至ECS-source。
      具体方法请参见**绑定弹性公网IP**。
   b. 远程登录ECS-source。
      ECS有多种登录方法，具体请参见**登录弹性云服务器**。
   c. 依次执行以下命令，安装NC工具。
      sudo yum update
      回显类似如下信息：

```
[root@ecs-source ~]# sudo yum update
HCE 2.0
base
         55 MB/s | 6.1 MB     00:00
HCE 2.0
updates
           98 MB/s |  14 MB     00:00
Last metadata expiration check: 0:00:01 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
Nothing to do.
Complete!
```

      sudo yum install nc
      回显类似如下信息，请根据回显提示输入**y**，并按回车。

```
[root@ecs-source ~]# sudo yum install nc
Last metadata expiration check: 0:00:12 ago on Tue 10 Sep 2024 05:54:28 PM CST.
Dependencies resolved.
...
Install  2 Packages

Total download size: 6.1 M
Installed size: 25 M
Is this ok [y/N]: y
Downloading Packages:
...
Importing GPG key 0xA8DEF926:
 Userid     : "HCE <support@huaweicloud.com>"
 Fingerprint: C1BA 9CD4 9D03 A206 E241 F176 28DA 5B77 A8DE F926
 From       : http://repo.huaweicloud.com/hce/2.0/updates/RPM-GPG-KEY-HCE-2
Is this ok [y/N]: y
...
Installed:
  libssh2-1.10.0-2.r10.hce2.x86_64
nmap-2:7.92-2.r4.hce2.x86_64

Complete!
```

   d. ECS-source的NC工具安装完成后，解绑EIP。
      具体方法请参见**解绑弹性公网IP**。

2. 参考1.a~1.d，在ECS-test中安装NC工具，并解绑EIP。
3. EIP解绑后，删除EIP。

   本示例中不再需要使用EIP，因此删除EIP，具体方法请参见**解绑弹性公网IP**。如果不删除EIP，则EIP会持续计费。

步骤五：验证镜像会话是否生效

1. 执行以下操作，建立ECS-source和ECS-test之间的TCP连接。

   本示例在ECS-source向ECS-test发送TCP报文，查看ECS-test是否可以收到该报文。

   a. 在ECS-source中，执行以下命令，开启1234端口的监听。

      nc -l *镜像源ECS-source的监听端口*

      命令示例：

      nc -l 1234

      此处回显为空，表示监听已正常开启。

   b. 在ECS-test中，执行以下命令，建立ECS-source和ECS-test之间的TCP连接。

      nc *镜像源ECS-source的私有IP地址 镜像源ECS-source的监听端口*

      命令示例：

      nc 192.168.0.230 1234

      此处回显为空，表示TCP连接已建立。

   c. 在ECS-source中，输入任意信息（比如**hello**），并按回车，测试TCP连接是否建立成功。

      ```
      [root@ecs-source ~]# nc -l 1234
      hello
      ```

   d. 在ECS-test中，查看是否收到来自ECS-source的信息。

      回显类似如下信息，可正常收到信息，表示TCP连接建立成功。

      ```
      [root@ecs-test ~]# nc 192.168.0.230 1234
      hello
      ```

2. 执行以下操作，测试ECS-source去往ECS-test的出方向TCP报文，是否可以镜像到ELB-A的后端服务器ECS-target-01和ECS-target-02。

   当镜像源ECS-source实时向ECS-test发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target-01和ECS-target-02是否可以获取到该报文的数据包，如果可以获取到，则表示出方向的采集规则配置生效。

   a. 远程登录ECS-target-01。

      ECS有多种登录方法，具体请参见**登录弹性云服务器**。

   b. 在ECS-target-01中，执行以下命令，查看镜像目的对应的网卡名称。

      ifconfig

      回显类似如下信息，本示例中镜像目的ECS-target-01对应的网卡名称为eth0。

      ```
      [root@ecs-target-01 ~]# ifconfig
      eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 192.168.0.6  netmask 255.255.255.0  broadcast 192.168.0.255
            inet6 fe80::f816:3eff:fe7e:d6dc  prefixlen 64  scopeid 0x20<link>
            ether fa:16:3e:7e:d6:dc  txqueuelen 1000  (Ethernet)
            RX packets 87498  bytes 114570302 (109.2 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 18337  bytes 6613541 (6.3 MiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
      ...
      ```

c. 在ECS-target-01中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

命令示例：

tcpdump -i eth0 udp port 4789 -nne

回显类似如下信息：

```
[root@ecs-target-01 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

d. 远程登录ECS-target-02。

ECS有多种登录方法，具体请参见**登录弹性云服务器**。

e. 在ECS-target-02中，执行以下命令，查看镜像目的对应的网卡名称。

ifconfig

回显类似如下信息，本示例中镜像目的ECS-target-02对应的网卡名称为eth0。

```
[root@ecs-target-02 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.12  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::f816:3eff:fe7e:d6e2  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:7e:d6:e2  txqueuelen 1000  (Ethernet)
        RX packets 87009  bytes 114283412 (108.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17015  bytes 6492086 (6.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

f. 在ECS-target-02中，执行以下命令，通过TCPDUMP工具观察数据包获取情况。

tcpdump -i *镜像目的对应的网卡名称* **udp port 4789 -nne**

命令示例：

tcpdump -i eth0 udp port 4789 -nne

回显类似如下信息：

```
[root@ecs-target-02 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

g. 在ECS-source中，输入任意信息（比如**source to test**），并按回车，向ECS-test发送TCP报文。

回显类似如下信息：

```
[root@source ~]# nc -l 1234
hello
source to test
```

h. 在ECS-test中，查看是否收到来自ECS-source的信息。

回显类似如下信息，可正常收到信息。

```
[root@ecs-test ~]# nc 192.168.0.230 1234
hello
source to test
```

i. 分别在ECS-target-01和ECS-target-02中，查看是否可以获取到报文的数据包。

- ECS-target-01：

  回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-source发送至ECS-test的信息**source to test**对应的数据包，时间为

19:09:21.273376，表示出方向的采集规则设置成功。其中，**vni 1**为镜像会话mirror-session-01的标识，表示通过mirror-session-01，ECS-target-01可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

```
[root@ecs-target-01 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:09:21.273376 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:dc, ethertype IPv4 (0x0800), length 131:
192.168.0.230.32816 > 192.168.0.6.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:bc > fa:16:3e:7e:d6:77, ethertype IPv4 (0x0800), length 81:
192.168.0.230.1234 > 192.168.0.161.57032: Flags [P.], seq 4181467553:4181467568, ack
3509843935, win 510, options [nop,nop,TS val 476501697 ecr 998055381], length 15
```

- ECS-target-02：

  回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-test响应ECS-source请求发送的数据包，时间为**19:09:21.273429**。

```
[root@ecs-target-02 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:09:21.273429 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:e2, ethertype IPv4 (0x0800), length
116: 192.168.0.230.32805 > 192.168.0.12.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 66:
192.168.0.161.57032 > 192.168.0.230.1234: Flags [.], ack 4181467568, win 502, options
[nop,nop,TS val 998154498 ecr 476501697], length 0
```

3. 执行以下操作，测试ECS-test进入ECS-source的入方向TCP报文，是否可以镜像到ELB-A的后端服务器ECS-target-01和ECS-target-02。

   当ECS-test实时向镜像源ECS-source发送TCP报文时，通过TCPDUMP工具，查看镜像目的ECS-target-01和ECS-target-02是否可以获取到该报文的数据包，如果可以获取到，则表示入方向的采集规则配置生效。

   a. 在ECS-test中，输入任意信息（比如**test to source**），并按回车，向ECS-source发送TCP报文。

      回显类似如下信息：

```
[root@ecs-test ~]# nc 192.168.0.230 1234
hello
source to test
test to source
```

   b. 在ECS-source中，查看是否收到来自ECS-test的信息。

      回显类似如下信息，可正常收到信息。

```
[root@ecs-source ~]# nc -l 1234
hello
source to test
test to source
```

   c. 分别在ECS-target-01和ECS-target-02中，查看是否可以获取到报文的数据包。

      - ECS-target-01：

        回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-test发送至ECS-source的信息**test to source**对应的数据包，时间为**19:10:04.772581**，表示入方向的采集规则设置成功。其中，**vni 1**为镜像会话mirror-session-01的标识，表示通过mirror-session-01，ECS-target-01可成功获取到数据包，数据包内容分为两部分，一部分是流量镜像封装的VXLAN报文，一部分是原始报文，详细说明请参见**表13-27**。

```
[root@ecs-target-01 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
```



```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:09:21.273376 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:dc, ethertype IPv4 (0x0800), length 131:
192.168.0.230.32816 > 192.168.0.6.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:bc > fa:16:3e:7e:d6:77, ethertype IPv4 (0x0800), length 81:
192.168.0.230.1234 > 192.168.0.161.57032: Flags [P.], seq 4181467553:4181467568, ack
3509843935, win 510, options [nop,nop,TS val 476501697 ecr 998055381], length 15
19:10:04.772581 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:dc, ethertype IPv4 (0x0800), length 131:
192.168.0.230.32805 > 192.168.0.6.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 81:
192.168.0.161.57032 > 192.168.0.230.1234: Flags [P.], seq 1:16, ack 15, win 502, options
[nop,nop,TS val 998197997 ecr 476501697], length 15
```

- ECS-target-02：

  回显类似如下信息，可以看到TCPDUMP工具启动后，获取到ECS-source响应ECS-test请求发送的数据包，时间为**19:10:04.772601**。

```
[root@ecs-target-02 ~]# tcpdump -i eth0 udp port 4789 -nne
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:09:21.273429 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:e2, ethertype IPv4 (0x0800), length
116: 192.168.0.230.32805 > 192.168.0.12.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:77 > fa:16:3e:7e:d6:bc, ethertype IPv4 (0x0800), length 66:
192.168.0.161.57032 > 192.168.0.230.1234: Flags [.], ack 4181467568, win 502, options
[nop,nop,TS val 998154498 ecr 476501697], length 0
19:10:04.772601 fa:16:3e:d1:6b:5d > fa:16:3e:7e:d6:e2, ethertype IPv4 (0x0800), length
116: 192.168.0.230.32816 > 192.168.0.12.4789: VXLAN, flags [I] (0x08), vni 1
fa:16:3e:7e:d6:bc > fa:16:3e:7e:d6:77, ethertype IPv4 (0x0800), length 66:
192.168.0.230.1234 > 192.168.0.161.57032: Flags [.], ack 15, win 510, options [nop,nop,TS
val 476545196 ecr 998197997], length 0
```

14 监控与审计

14.1 使用 CES 服务监控 VPC 网络指标

14.1.1 VPC 支持的监控指标

功能说明

本节定义了弹性公网IP和带宽上报云监控的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控提供的管理控制台或API接口来检索弹性公网IP和带宽产生的监控指标和告警信息。

命名空间

SYS.VPC

监控指标

表 14-1 弹性公网 IP 和带宽支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
upstream_bandwidth	出网带宽	该指标用于统计测试对象出云平台的网络速度（原指标为上行带宽）。 单位：比特/秒	≥ 0 bit/s	带宽或弹性公网IP	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
downstream_bandwidth	入网带宽	该指标用于统计测试对象入云平台的网络速度（原指标为下行带宽）。 单位：比特/秒	≥ 0 bit/s	带宽或弹性公网IP	1分钟
upstream_bandwidth_usage	出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。 出网带宽使用率=出网带宽指标/购买的带宽大小	0-100%	带宽或弹性公网IP	1分钟
downstream_bandwidth_usage	入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。 入网带宽使用率=入网带宽指标/购买的带宽大小	0-100%	带宽或弹性公网IP	1分钟
up_stream	出网流量	该指标用于统计测试对象出云平台一分钟内的网络流量累加值（原指标为上行流量）。 单位：字节	≥ 0 bytes	带宽或弹性公网IP	1分钟
down_stream	入网流量	该指标用于统计测试对象入云平台一分钟内的网络流量累加值（原指标为下行流量）。 单位：字节	≥ 0 bytes	带宽或弹性公网IP	1分钟

维度

Key	Value
publicip_id	弹性公网IP ID
bandwidth_id	带宽ID

对于有多个测量维度的测量对象，使用接口查询监控指标时，所有测量维度均为必选。

- 查询单个监控指标时，多维度dim使用样例：dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a。
- 批量查询监控指标时，多维度dim使用样例：

  "dimensions": [

  {

  "name": "bandwidth_id",

  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"

  }

  {

  "name": "publicip_id",

  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"

  }

  ],

14.1.2 查看 VPC 的监控指标

操作场景

查看带宽、弹性公网IP的使用情况。

具体可查看指定时间段内的入网带宽、出网带宽、入网带宽使用率、出网带宽使用率、入网流量和出网流量等使用数据信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“管理与监管 > 云监控服务”。
4. 单击页面左侧的“云服务监控”，选择“弹性公网IP和带宽”。
5. 单击“操作”列的“查看监控指标”，查看带宽或弹性公网IP的监控指标详情。

14.1.3 创建告警规则

操作场景

通过设置告警规则，用户可自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“管理与监管 > 云监控服务”。
4. 在左侧导航栏，选择“告警 > 告警规则”。
5. 在“告警规则”界面，单击“创建告警规则”进行添加，或者选择已有的告警规则进行修改。
6. 规则参数设置完成后，单击“确定”。
   告警规则设置完成后，当符合规则的告警产生时，系统会自动进行通知。

   说明

   更多关于监控规则的信息，请参见《云监控用户指南》。

14.2 使用 CTS 服务审计 VPC 关键操作

14.2.1 VPC 支持审计的关键操作

通过云审计，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。

云审计支持的虚拟私有云操作列表如表14-2所示。

表 14-2 云审计服务支持的 VPC 操作列表

操作名称	资源类型	事件名称
修改Bandwidth	bandwidth	modifyBandwidth
创建EIP	eip	createEip
释放EIP	eip	deleteEip
绑定EIP	eip	bindEip
解绑定EIP	eip	unbindEip
创建PrivateIp	privateIps	createPrivateIp
删除PrivateIp	privateIps	deletePrivateIp
创建Security Group	security_groups	createSecurity-group
更新Security Group	security_groups	updateSecurity-group
删除Security Group	security_groups	deleteSecurity-group
创建Security Group Rule	security-group-rules	createSecurity-group-rule
更新Security Group Rule	security-group-rules	updateSecurity-group-rule

操作名称	资源类型	事件名称
删除Security Group Rule	security-group-rules	deleteSecurity-group-rule
创建Subnet	subnet	createSubnet
删除Subnet	subnet	deleteSubnet
修改Subnet	subnet	modifySubnet
创建VPC	vpc	createVpc
删除VPC	vpc	deleteVpc
修改VPC	vpc	modifyVpc
创建VPN	vpn	createVpn
删除VPN	vpn	deleteVpn
修改VPN	vpn	modifyVpn
创建Router	routers	createRouter
更新Router	routers	updateRouter
Router添加接口	routers	addRouterInterface
Router删除接口	routers	removeRouterInterface
创建Port	ports	createPort
更新Port	ports	updatePort
删除Port	ports	deletePort
创建Network	networks	createNetwork
更新Network	networks	updateNetwork
删除Network	networks	deleteNetwork
批量创建和删除Subnet资源标签	tag	batchUpdateTags
批量创建和删除VPC资源标签	tag	batchUpdateVpcTags
创建RouteTable	routetables	createRouteTable
更新RouteTable	routetables	updateRouteTable
删除RouteTable	routetables	deleteRouteTable
创建VPC Peerings	vpc-peerings	createVpcPeerings
更新VPC Peerings	vpc-peerings	updateVpcPeerings
删除VPC Peerings	vpc-peerings	deleteVpcPeerings

操作名称	资源类型	事件名称
创建网络ACL组	firewall-groups	createFirewallGroup
更新网络ACL组	firewall-groups	updateFirewallGroup
删除网络ACL组	firewall-groups	deleteFirewallGroup
创建网络ACL策略	firewall-policies	createFirewallPolicy
更新网络ACL策略	firewall-policies	updateFirewallPolicy
删除网络ACL策略	firewall-policies	deleteFirewallPolicy
插入网络ACL规则	firewall-policies	insertFirewallPolicyRule
移除网络ACL规则	firewall-policies	removeFirewallPolicyRule
创建网络ACL规则	firewall-rules	createFirewallRule
更新网络ACL规则	firewall-rules	updateFirewallRule
删除网络ACL规则	firewall-rules	deleteFirewallRule
创建Address Group	address_group	createAddress_group
更新Address Group	address_group	updateAddress_group
强制删除Address Group	address_group	force_deleteAddress_group
删除Address Group	address_group	deleteAddress_group
创建Flow Log	flowlogs	createFlowLog
更新Flow Log	flowlogs	updateFlowLog
删除Flow Log	flowlogs	deleteFlowLog
创建公网NAT网关	natgateway	createNatGateway
修改公网NAT网关	natgateway	updateNatGateway
删除公网NAT网关	natgateway	deleteNatGateway
创建公网NAT网关DNAT规则	dnatrule	createDnatRule
修改公网NAT网关DNAT规则	dnatrule	updateDnatRule
删除公网NAT网关DNAT规则	dnatrule	deleteDnatRule
创建公网NAT网关SNAT规则	snatrule	createSnatRule
修改公网NAT网关SNAT规则	snatrule	updateSnatRule

操作名称	资源类型	事件名称
删除公网NAT网关SNAT规则	snatrule	deleteSnatRule

14.2.2 查看 VPC 的审计日志

操作场景

在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

须知

云审计服务仅保存最近7天的事件，如果您希望长期保存事件，则可以对追踪器执行OBS转储的相关配置，将事件同步、长期保存至OBS桶。具体操作请参考**配置追踪器**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击，选择区域和项目。
3. 在页面左上角单击图标，打开服务列表，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。
4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持不同维度的组合查询，详细信息如下：
   - 事件类型：可选项为“管理事件”、“数据事件”。
   - 事件来源、资源类型和筛选类型。

     在下拉框中选择查询条件。

     其中筛选类型选择事件名称时，还需选择某个具体的事件名称。

     选择资源ID时，还需选择或者手动输入某个具体的资源ID。

     选择资源名称时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询“最近1小时”、“最近1天”、“最近1周”以及最近1周内自定义时间段的操作事件。
6. 在需要查看的记录左侧，单击箭头展开该记录的详细信息。

7. 在需要查看的记录右侧，单击“查看事件”，弹出的窗口显示该操作事件结构的详细信息。

15 管理 VPC 配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个虚拟私有云。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 15-1 我的配额

4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

图 15-2 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 15-3 申请扩大配额

4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

A 附录

A.1 NAT64 TOA 插件配置

操作场景

用户使用IPv6地址通信需要获取来访者的真实IPv6地址。TOA内核模块主要用来获取经NAT64转化过的来访者真实IPv6地址，该插件安装在后端服务器。

当用户需要在操作系统中编译NAT64 TOA内核模块时，可参考本文档进行配置。本操作当前仅支持华东-上海一和华北-北京四区域。

说明

- TOA不支持UDP协议。
- TOA模块在以下操作系统中验证可以正常工作，其他内核版本安装方法类似。
  - CentOS 7/7.2 (Kernel version 3.10.0)
  - Ubuntu 14.04.3(Kernel version 3.12.0)
  - Ubuntu 16.04.3 (Kernel version 4.4.0)

前提条件

- 编译内核模块开发环境需与当前内核版本开发环境一致。
- 确保虚拟机可以访问开放源。
- 如果是非root用户，需拥有sudo权限。

操作步骤

编译并加载TOA模块

以下操作步骤是针对Linux内核版本为3.0以上的操作系统。

1. 准备编译环境。

   说明

   安装内核模块开发包的过程中，如果源里面找不到对应内核版本的安装包，需要自行去网上下载需要的安装包。

以下是不同Linux发行版本的操作说明，请根据环境选择对应的方案。

- CentOS环境下的操作步骤。
  i. 执行如下命令，安装gcc编译器。
     sudo yum install gcc
  ii. 执行如下命令，安装make工具。
     sudo yum install make
  iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。
     sudo yum install kernel-devel-`uname -r`

     说明

     如果自带源里没有对应的内核开发包，可以到如下地址中去下载对应的rpm包。
     地址：https://mirror.netcologne.de/oracle-linux-repos/ol7_latest/getPackage/
     以3.10.0-693.11.1.el7.x86_64为例，下载后执行以下命令安装：
     rpm -ivh kernel-devel-3.10.0-693.11.1.el7.x86_64.rpm。
- Ubuntu、Debian环境下的操作步骤。
  i. 执行如下命令，安装gcc编译器。
     sudo apt-get install gcc
  ii. 执行如下命令，安装make工具。
     sudo apt-get install make
  iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。
     sudo apt-get install linux-headers-`uname -r`
- SUSE环境下的操作步骤。
  i. 执行如下命令，安装gcc编译器。
     sudo zypper install gcc
  ii. 执行如下命令，安装make工具。
     sudo zypper install make
  iii. 执行如下命令，安装内核模块开发包，开发包头文件与库的版本需要与内核版本一致。
     sudo zypper install enel-default-devel
- CoreOS环境下的操作步骤。
  CoreOS环境下在容器内进行内核模块的编译时，需要先启动一个用于内核模块开发的容器，然后再进行编译。
  详细过程参见CoreOS官方文档，获取方式如下链接所示。
  https://coreos.com/os/docs/latest/kernel-modules.html

2. 编译内核模块。
   a. 使用git工具，执行如下命令，下载TOA内核模块源代码。
      git clone https://github.com/huaweicloud/elb-toa
      git checkout IPv6

说明

如果未安装git工具，请进入以下链接下载TOA模块源代码。

https://github.com/huaweicloud/elb-toa/tree/IPv6

b. 执行如下命令，进入源码目录，编译模块。

cd src

make

编译过程未提示warning或者error，说明编译成功，检查当前目录下是否已经生成toa.ko文件。

3. 加载内核模块。

a. 执行如下命令，加载内核模块。

sudo insmod toa.ko

b. 执行如下命令，验证模块加载情况，查看内核输出信息。

dmesg | grep TOA

若提示信息包含“TOA: toa loaded”，说明内核模块加载成功。

说明

CoreOS在容器中编译完内核模块后，需要将内核模块复制到宿主系统，然后在宿主系统中加载内核模块。由于编译内核模块的容器和宿主系统共享/lib/modules目录，可以在容器中将内核模块复制到该目录下，以供宿主系统使用。

4. 自动加载内核模块。

为了使TOA内核模块在系统启动时生效，可以将加载TOA内核模块的命令加到客户的启动脚本中。

自动加载内核模块的方法有以下两种方法：

- 客户可以根据自身需求，在自定义的启动脚本中添加加载TOA内核模块的命令。
- 参考以下操作步骤配置启动脚本。

i. 在“/etc/sysconfig/modules/”目录下新建toa.modules文件。该文件包含了TOA内核模块的加载脚本。

toa.modules文件内容，请参考如下示例：

```
#!/bin/sh
/sbin/modinfo -F filename /root/toa/toa.ko > /dev/null 2>&1
if [ $? -eq 0 ]; then
/sbin/insmod /root/toa/toa.ko
fi
```

其中“/root/toa/toa.ko”为TOA内核模块文件的路径，客户需要将其替换为自己编译的TOA内核模块路径。

ii. 执行以下命令，为toa.modules启动脚本添加可执行权限。

sudo chmod +x /etc/sysconfig/modules/toa.modules

说明

客户升级内核后，会导致现有TOA内核模块不匹配，因此需要重新编译TOA内核模块。

5. 安装多节点。

如果要在相同的客户操作系统中加载此内核模块，可以将toa.ko文件拷贝到需要加载此模块的虚拟机中，然后参照3加载内核模块。

内核模块加载成功以后，应用程序可以正常获取访问者的真实源IPv6地址。

说明

节点的操作系统发行版与内核版本必须相同。

后端服务器适配

使用NAT64的TOA源地址透传功能，后端服务器应用程序源码应该做以下适配（以下为C语言示例）：

1. 定义用来保存地址的数据结构。

   struct toa_nat64_peer uaddr

2. 调用函数，获得IPv6地址。

   getsockopt(connfd, IPPROTO_IP, TOA_SO_GET_LOOKUP, &uaddr, &len)

   其中

   connfd：服务器端提供服务连接的socket fd

   IPPROTO_IP：固定

   len：sizeof(struct toa_nat64_peer)

   TOA_SO_GET_LOOKUP：常量值4096

   uaddr：用来保存NAT64 TOA数据结构的变量

3. 输出地址并保存。

   uaddr.saddr

4. 参考代码示例：

```
//定义保存nat64 toa信息的数据结构和变量
enum {
    TOA_BASE_CTL            = 4096,
    TOA_SO_SET_MAX          = TOA_BASE_CTL,
    TOA_SO_GET_LOOKUP       = TOA_BASE_CTL,
    TOA_SO_GET_MAX          = TOA_SO_GET_LOOKUP,
};

struct toa_nat64_peer {
    struct in6_addr saddr;
    uint16_t sport;
};
struct toa_nat64_peer uaddr;
......
//获取服务端的socket
sockaddr.sin_family = AF_INET;
sockaddr.sin_addr.s_addr = htonl(INADDR_ANY);
sockaddr.sin_port = htons(PORT);
listenfd = socket(AF_INET,SOCK_STREAM,0);
bind(listenfd, (struct sockaddr *)&sockaddr, sizeof(sockaddr))
......
//监听对应的socket
connfd = accept(listenfd, (struct sockaddr*)&caddr, &length);

//获取对应nat64 toa的信息
char from[40];
int len = sizeof(struct toa_nat64_peer);
if (getsockopt(connfd, IPPROTO_IP, TOA_SO_GET_LOOKUP, &uaddr, &len) == 0) {
inet_ntop(AF_INET6, &uaddr.saddr, from, sizeof(from));
//获取源IP和源port的信息
printf("real client [%s]:%d\n", from, ntohs(uaddr.sport));
}
```