虚拟私有云

用户指南

文档版本 73

发布日期 2024-06-05

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 权限管理

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。

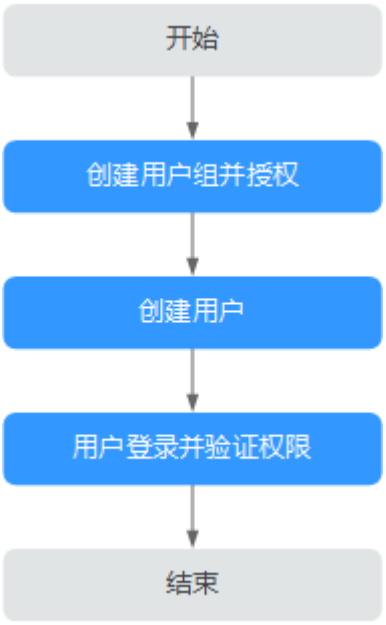
前提条件

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"
      }
   ]
}
```

2 虚拟私有云和子网

2.1 虚拟私有云和子网规划建议

在创建VPC之前，您需要根据具体的业务需求规划VPC、子网的数量及IP网段，并选择网络连通方式等。

- **如何规划VPC?**
- **如何规划子网?**
- **如何规划路由策略?**
- **如何连接本地IDC?**
- **如何连接Internet?**

如何规划 VPC?

VPC具有区域属性，默认情况下，不同VPC之间网络不通，同一个VPC内的不同子网之间网络互通。

- 一个VPC

  当各业务之间没有网络隔离需求时，您可以只使用一个VPC。
- 多个VPC

当您在当前区域下部署多套业务，且希望不同业务之间网络隔离，则您可以在当前区域内，为每个业务建立对应的VPC。

如果需要连通相同账户内或者不同账户内，不同VPC之间的网络，您可以根据VPC的区域，选择以下方式：

- 相同区域内：可以通过**对等连接**实现。
- 不同区域内：可以通过**云连接**来实现。

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**如何申请扩大配额?**

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。

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

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添加扩展网段**。

如何规划子网？

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。

- 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。
- 子网创建成功后，不支持修改网段，请提前合理规划好子网网段。同一个虚拟私有云内的子网网段不可重复。

  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。

说明

一个用户在单个区域可创建的虚拟私有云子网数量默认为100个，如果您需要提升配额，请参见**如何申请扩大配额?**

当您规划VPC子网时，可以参考以下原则：

- 合理划分子网：同一个VPC内的业务，您可以根据业务模块划分子网，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。
- 避免网段冲突：当您需要连通不同VPC的子网，或者连通云上VPC和线下IDC的网络时，要避免网络两端的子网网段冲突，否则无法正常通信。

如何规划路由策略?

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。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。默认路由表可以确保VPC内子网之间网络互通。

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，并关联至子网。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。

您可以在默认路由表和自定义路由表中添加路由，目的地址、下一跳类型、下一跳地址等信息，来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：系统自动添加且无法修改或删除的路由，表示VPC内实例互通。
- 自定义路由：可以修改和删除的路由。自定义路由的目地地址不能与系统路由的目地地址重叠。

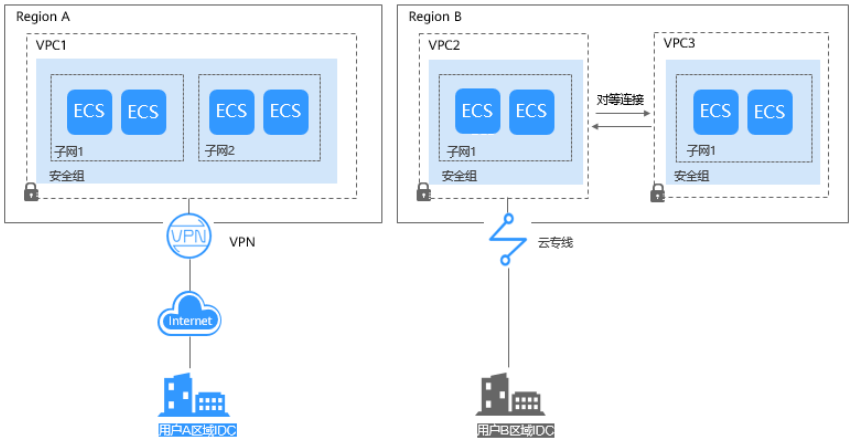
  您无法在VPC路由表中添加目的地址相同的两条路由，即使路由的下一跳类型不同也不行。因此不论路由的下一跳是何种类型，路由的优先级均取决于目的地址，遵循最长匹配原则，即优先选择匹配度更高的目的地址进行路由转发。

如何连接本地 IDC?

当您有VPC与本地IDC互通的需求时，需要确保VPC的网段和要互通的IDC内网段都不冲突。

如**图2-1**所示，比如您在A区域有一个VPC1，B区域有两个VPC，分别为VPC2和VPC3。VPC1需要连接用户A区域IDC，通过VPN走Internet互连。VPC2需要连接用户B区域IDC，通过云专线连接。同时在B区域的VPC3与VPC2通过对等连接建立连接。

图 2-1 IDC 连接



此例中，各VPC网段划分需要注意以下几点：

- VPC1的网段（CIDR）不能与区域A IDC的网段有重叠。
- VPC2的网段（CIDR）不能与区域B IDC的网段有重叠。
- VPC3和VPC2的网段也不能有重叠。

如何连接 Internet?

少量弹性云服务器通过弹性公网IP连接Internet

当您仅有少量弹性云服务器访问Internet时，您可将弹性公网IP（EIP）绑定到弹性云服务器上，弹性云服务器即可连接公网。您还可以通过动态解绑它，再绑定到NAT网关、弹性负载均衡上，使这些云产品连接公网，管理非常简单。不同弹性公网IP还可以共享带宽，减少您的带宽成本。

更多弹性公网IP（EIP）信息，请参见**弹性公网IP简介**。

大量弹性云服务器通过NAT网关连接Internet

当您有大量弹性云服务器需要访问Internet时，单纯使用弹性公网IP管理成本过高，公有云NAT网关来帮您，它提供SNAT和DNAT两种功能。SNAT可轻松实现同一VPC内的多个弹性云服务器共享一个或多个弹性公网IP主动访问公网，有效降低管理成本，减少了弹性云服务器的弹性公网IP直接暴露的风险。DNAT功能还可以实现端口级别的转发，将弹性公网IP的端口映射到不同弹性云服务器的端口上，使VPC内多个弹性云服务器共享同一弹性公网IP和带宽面向互联网提供服务。

更多NAT网关信息，请参见**《NAT网关用户指南》**。

海量高并发场景通过弹性负载均衡连接Internet

对于电商等高并发访问的场景，您可以通过弹性负载均衡（ELB）将访问流量均衡分发到多台弹性云服务器上，支撑海量用户访问。弹性负载均衡采用集群化部署，支持多可用区的同城双活容灾。同时，无缝集成了弹性伸缩，能够根据业务流量自动扩容，保证业务稳定可靠。

更多弹性负载均衡信息，请参见**《弹性负载均衡用户指南》**。

相关操作

- **应用场景**

- 私网访问
- 公网访问

2.2 虚拟私有云

2.2.1 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。

图 2-2 创建 VPC 和默认子网

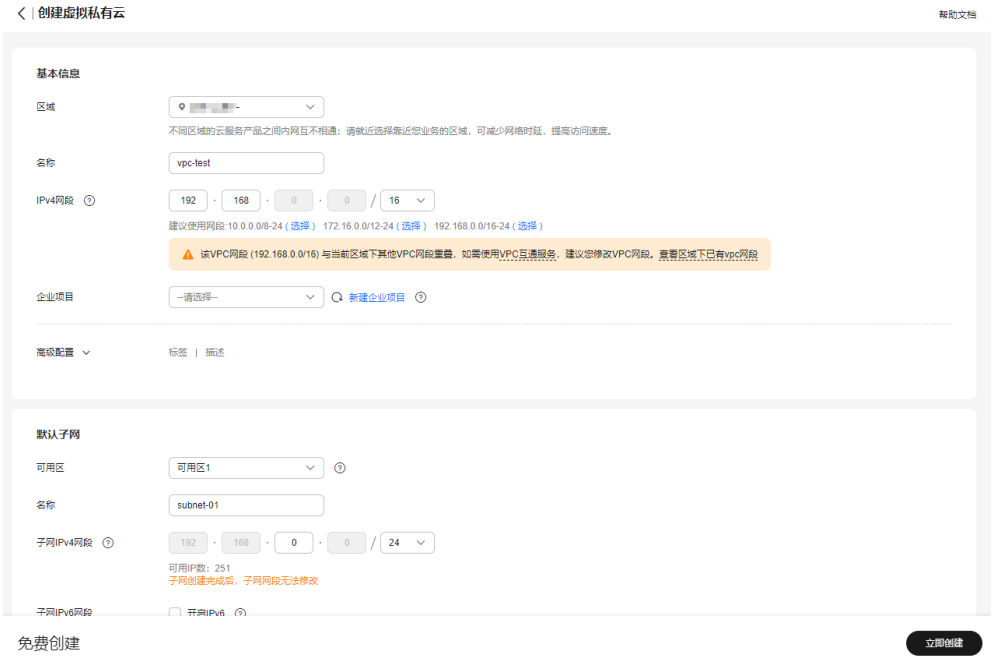


表 2-3 虚拟私有云参数说明

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

参数	说明	取值样例
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
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

参数	说明	取值样例
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
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 2-4 子网参数说明

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。 ● 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
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
子网网段	在未开启IPv4/IPv6双栈的区域，显示此参数。 设置VPC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： ● 合理划分子网：同一个VPC内的业务，您可以根据业务模块划分子网，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。 ● 避免网段冲突：当您需要连通不同VPC的子网，或者连通云上VPC和线下IDC的网络时，要避免网络两端的子网网段冲突，否则无法正常通信。 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**。	-
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

参数	说明	取值样例
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
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

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。 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 > 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
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

参数	说明	取值样例
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**。

2.2.2 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。
- 不支持添加的扩展网段范围如**表2-5**所示。

表 2-5 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 • 192.168.0.0/16 • 主网段已使用的私网网段
系统内部预留地址	• 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

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”。

2.2.3 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 2-3 VPC ID

2.2.4 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。
   - 当虚拟私有云下存在子网时，您只可以修改掩码。
6. 网段信息设置完成后，单击“确定”保存修改。

2.2.5 管理虚拟私有云标签

操作场景

标签是虚拟私有云的标识。通过为虚拟私有云添加标签，可以方便您识别和管理拥有的虚拟私有云。

您可以在创建虚拟私有云的时候添加标签，或者在已经创建的虚拟私有云详情页添加标签。

每个云资源最多可以添加20个标签。

标签共由两部分组成：“键”和“值”，“键”和“值”的命名规则如表2-6所示。

表 2-6 虚拟私有云标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一虚拟私有云键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	vpc_key1

参数	规则	样例
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	vpc-01

操作步骤

在虚拟私有云列表页，按标签的键或值搜索目标虚拟私有云。

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. 在虚拟私有云列表上方的搜索框中，单击框中任意位置，设置搜索条件。
   在“属性类型”列表中，根据需要的标签选择对应的键和值。系统会根据您设置的标签搜索条件筛选对应的资源。
   单击搜索框中任意位置，添加下一个标签键和值。
   系统支持添加多个标签，并取各个标签的交集，对目标虚拟私有云进行搜索。

在虚拟私有云的标签页，执行标签的增、删、改、查操作。

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. 在虚拟私有云列表中，单击待管理标签的虚拟私有云名称。
   系统跳转至该虚拟私有云详情页面。
5. 选择“标签”页签，对虚拟私有云的标签执行增、删、改、查。
   - 查看
     在“标签”页，可以查看当前虚拟私有云的标签详情，包括标签个数，以及每个标签的键和值。
   - 添加
     单击左上角的“添加标签”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改
     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
   - 删除
     单击标签所在行“操作”列下的“删除”，如果确认删除，在弹出的“删除标签”窗口，单击“是”。

2.2.6 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。

2.2.7 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。

2.2.8 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。

2.2.9 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

虚拟私有云为免费资源，不会收取您的任何费用。

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。

2.3 子网

2.3.1 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. 根据界面提示配置参数。

表 2-7 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
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。 ● 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： ● 合理划分子网：同一个VPC内的业务，您可以根据业务模块划分子网，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。 ● 避免网段冲突：当您需要连通不同VPC的子网，或者连通云上VPC和线下IDC的网络时，要避免网络两端的子网网段冲突，否则无法正常通信。 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**。	-
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

参数	说明	取值样例
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
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

参数	说明	取值样例
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
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。 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 > 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

参数	说明	取值样例
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。

2.3.2 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 2-8 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

参数	说明	取值样例
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
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

参数	说明	取值样例
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**。	-
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“>”。	-

2.3.3 管理子网标签

应用场景

标签是子网的标识。通过为子网添加标签，可以方便您识别和管理拥有的子网。

您可以在创建子网的时候添加标签，或者在已经创建的子网详情页添加标签。

每个云资源最多可以添加20个标签。

标签共由两部分组成：“键”和“值”，“键”和“值”的命名规则如**表2-9**所示。

表 2-9 子网标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一子网键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	subnet_key1
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	subnet-01

操作步骤

在子网列表页，按标签的键或值搜索目标子网。

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. 在子网列表上方的搜索框中，单击框中任意位置，设置搜索条件。
   在“属性类型”列表中，根据需要的标签选择对应的键和值。系统会根据您设置的标签搜索条件筛选对应的资源。
   单击搜索框中任意位置，添加下一个标签键和值。
   系统支持添加多个标签，并取各个标签的交集，对目标虚拟私有云进行搜索。

在子网的标签页，执行标签的增、删、改、查操作。

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 > 子网”。
   进入子网列表页面。
5. 在子网列表中，单击待管理的子网名称。
6. 在子网详情页面，选择“标签”页签，对子网的标签执行增、删、改、查。
   - 查看
     在“标签”页，可以查看当前子网的标签详情，包括标签个数，以及每个标签的键和值。

- 添加

  单击左上角的“添加标签”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
- 修改

  单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。
- 删除

  单击标签所在行“操作”列下的“删除”，如果确认删除，在弹出的“删除标签”窗口，单击“是”。

2.3.4 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。

2.3.5 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。

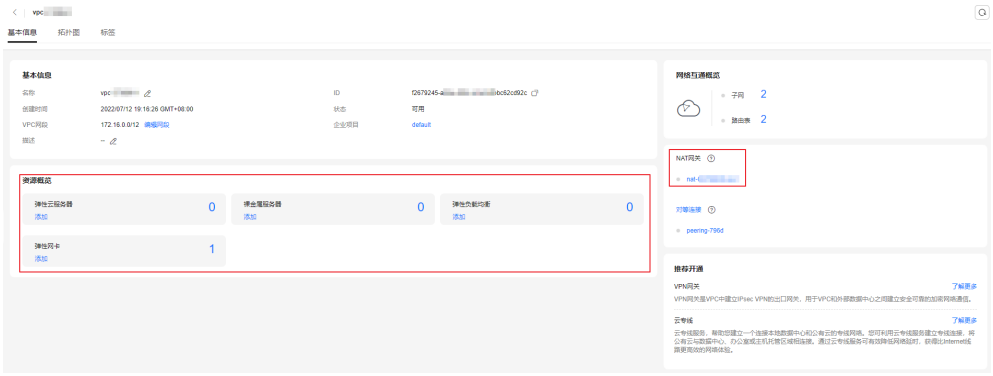
须知

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（弹性云服务器、裸金属服务器、弹性网卡、弹性负载均衡等）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。

图 2-4 查看子网内的资源



7. 执行以下操作，删除子网内的云服务资源。

表 2-10 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**。

云服务资源类型	操作指导
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**。
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**。

2.3.6 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。

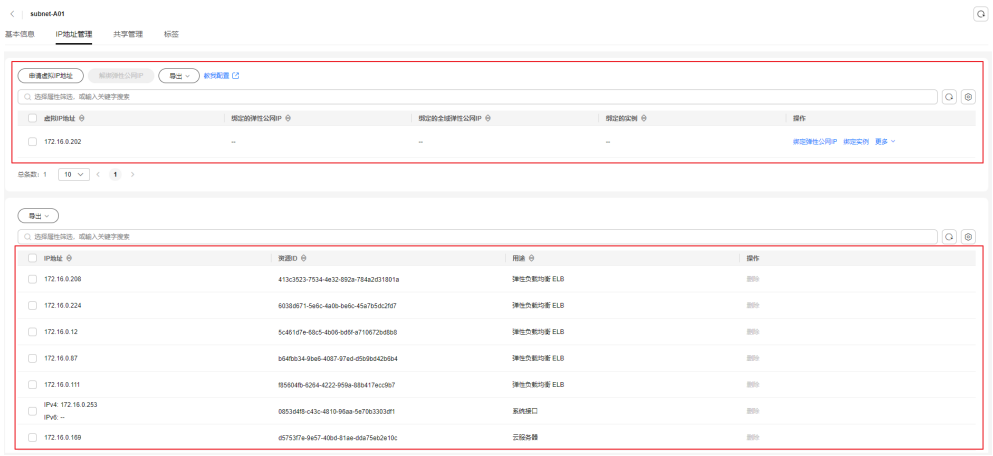
约束与限制

- 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 2-5 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**。

2.3.7 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

子网为免费资源，不会收取您的任何费用。

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

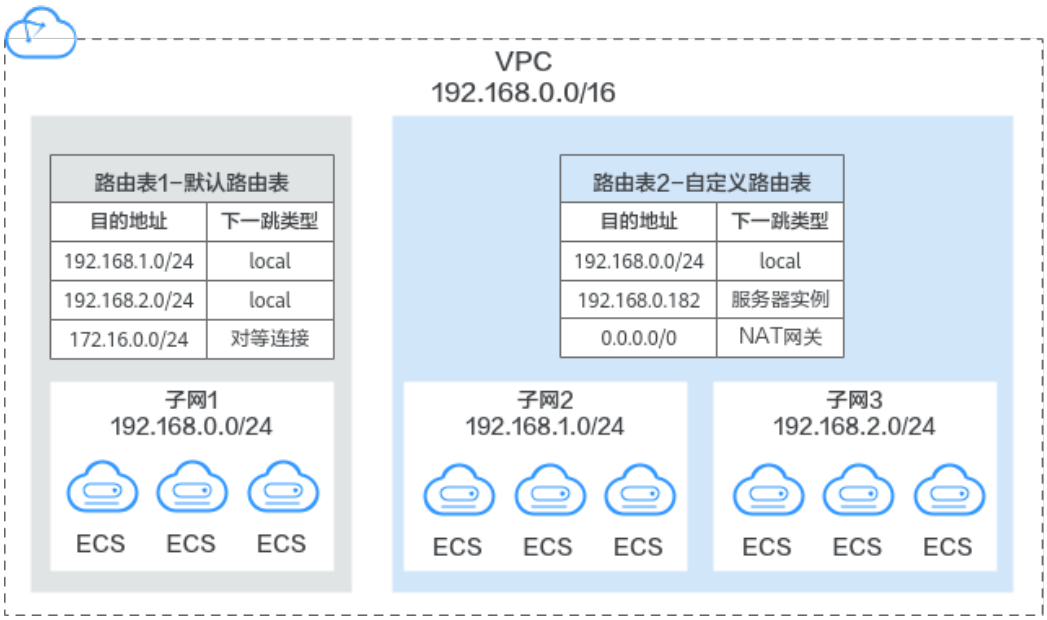
3.1 路由表和路由概述

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**如何申请扩大配额？**。

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：系统自动添加且无法修改或删除的路由。创建路由表后，系统会自动在路由表中添加以下系统路由：
  - 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：可以修改和删除的路由。自定义路由的目的地址不能与系统路由的目的地址重叠。

  您可以通过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。路由支持的下一跳类型如**表3-1**所示。

  您无法在VPC路由表中添加目的地址相同的两条路由，即使路由的下一跳类型不同也不行。因此不论路由的下一跳是何种类型，路由的优先级均取决于目的地址，遵循最长匹配原则，即优先选择匹配度更高的目的地址进行路由转发。

表 3-1 下一跳类型

下一跳类型	说明	支持添加该类型路由的路由表
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。	• 默认路由表 • 自定义路由表

下一跳类型	说明	支持添加该类型路由的路由表
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。	● 默认路由表 ● 自定义路由表
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。	● 自定义路由表
VPN网关	将指向目的地址的流量转发到一个VPN网关。	自定义路由表
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。	自定义路由表
云连接	将指向目的地址的流量转发到云连接。	自定义路由表
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。	● 默认路由表 ● 自定义路由表
NAT网关	将指向目的地址的流量转发到一个NAT网关。	● 默认路由表 ● 自定义路由表
对等连接	将指向目的地址的流量转发到一个对等连接。	● 默认路由表 ● 自定义路由表
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。	● 默认路由表 ● 自定义路由表
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。	● 默认路由表 ● 自定义路由表
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。	● 默认路由表 ● 自定义路由表
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。	● 默认路由表 ● 自定义路由表
云防火墙	将指向目的地址的流量转发到一个云防火墙。	● 默认路由表 ● 自定义路由表
互联网网关	将指向目的地址的流量转发到一个互联网网关。	● 默认路由表 ● 自定义路由表

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，也就是路由表的目的地址，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。

路由表的使用限制

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，路由优先级说明如下：
  - Local路由：类型为“系统”，用于VPC内通信的系统默认路由，优先级高于自定义路由。
  - 自定义路由：类型为“自定义”，是用户自己添加的路由或者创建其他实例自动下发的路由，自定义路由遵循最长匹配原则，即优先选择匹配度更高的目的地址进行路由转发。

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 3-2 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。

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**如何申请扩大配额？**。

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 3-3 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 导出路由表列表

操作场景

您可以将当前账号下拥有的路由表信息，以Excel文件的形式导出至本地。该文件记录了路由表的名称、ID、所属VPC、类型、关联子网个数等。

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 > 路由表”。
   进入路由表列表页面。
5. 在路由表列表页面，单击列表左上方的“导出”。
   - 导出已选中数据到XLSX：勾选一个或多个路由表，导出所选子路由表的信息。
   - 导出全部数据到XLSX：导出当前区域内所有路由表的信息。

   系统会将路由表信息自动导出为Excel文件，并下载至本地。

3.2.7 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。

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 3-4 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** • 目的地址不能与已有路由的目的地址冲突。 • 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。

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 3-5 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** • 目的地址不能与已有路由的目的地址冲突。 • 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

参数	说明	取值样例
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3-6。

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 3-6 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

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
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。

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 删除自定义路

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、云桌面）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 > 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“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**为ECS申请和绑定EIP**。
- 为弹性云服务器的虚拟IP绑定EIP，详情请参见**将虚拟IP地址绑定至弹性公网IP或实例**。

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）内所有弹性云服务器内访外配置。实例如**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

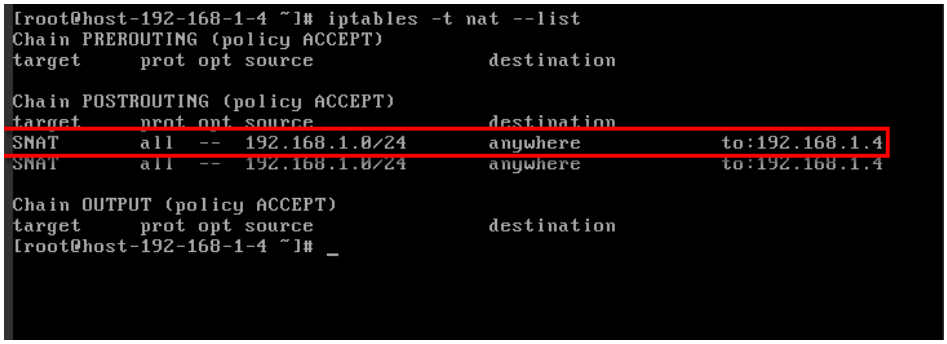
4. 执行以下命令添加rc.local文件的执行权限。

   # 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，简称VIP）是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。

同时，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之间对等连接访问，以及弹性公网IP、VPN、云专线等网络接入。

您可以为多个主备部署的弹性云服务器绑定同一个虚拟IP地址，然后为虚拟IP绑定一个弹性公网IP，搭配Keepalived，实现主服务器故障后，自动切换至备服务器，打造高可用容灾组网。

须知

通过虚拟IP和弹性云服务器构建高可用容灾组网，必须要搭配Keepalived相关配置才可以实现，具体可参考**搭建Keepalived Nginx高可用Web集群**。

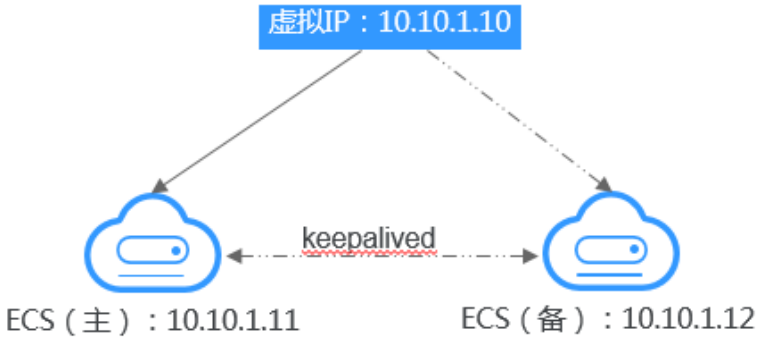
典型组网

虚拟IP主要用在弹性云服务器的主备切换，搭配Keepalived，达到高可用性HA（High Availability）的目的。当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。本节介绍两种典型的组网模式。

- **典型组网1：** HA高可用性模式

  场景举例：如果您想要提高服务的高可用性，避免单点故障，可以用“一主一备”或“一主多备”的方法组合使用弹性云服务器，这些弹性云服务器对外表现为一个虚拟IP。当主服务器故障时，备服务器可以转为主服务器，继续对外提供服务。

图 4-1 HA 高可用性模式组网图

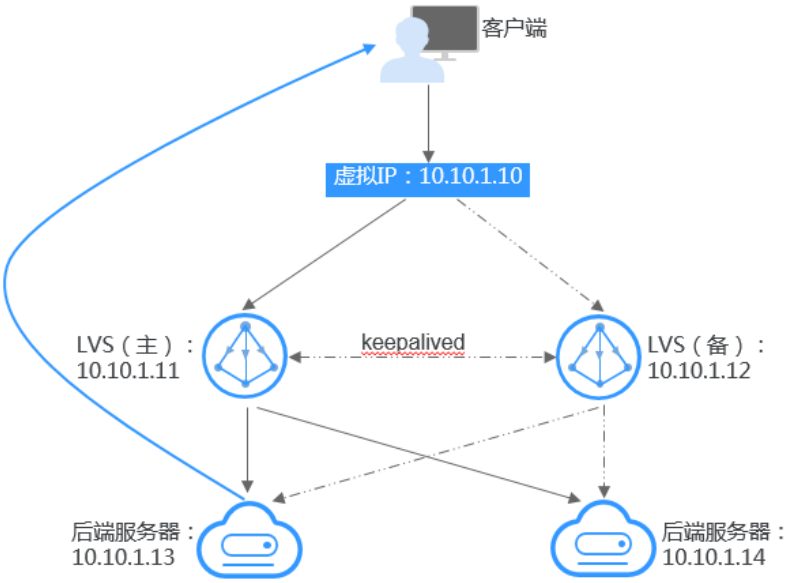


- 将2台同子网的弹性云服务器绑定同一个虚拟IP。
- 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **典型组网2：**高可用负载均衡集群

  场景举例：如果您想搭建高可用负载均衡集群服务，您可以采用Keepalived + LVS(DR)来实现。

图 4-2 高可用负载均衡集群



- 将2台弹性云服务器绑定同一个虚拟IP。
- 将绑定了虚拟IP的这2台弹性云服务器配置Keepalived+LVS（DR模式），组成LVS主备服务器。这2台服务器作为分发器将请求均衡地转发到不同的后端服务器上执行。
- 配置另外2台弹性云服务器作为后端RealServer服务器。
- 关闭2台后端RealServer弹性云服务器的源/目的检查。
- 检查LVS主备服务器的源/目的检查是否关闭，请参见**关闭ECS网卡的源/目的检查**。

若采用控制台方式将弹性云服务器与虚拟IP绑定，则源/目的检查自动关闭；若采用调用接口方式将弹性云服务器与虚拟IP绑定，则需要手动关闭源/目的检查。

Keepalived + LVS调度服务端安装配置以及后端RealServer服务器配置可以参考业内通用的配置方法，此处不做详细介绍。

应用场景

- 场景一：通过弹性公网IP访问虚拟IP。

  您的应用需要具备高可用性并通过Internet对外提供服务，推荐使用弹性公网IP绑定虚拟IP功能。
- 场景二：通过VPN/云专线/对等连接访问虚拟IP。

  您的应用需要具备高可用性并且需要通过Internet访问，同时需要具备安全性（VPN），保证稳定的网络性能（云专线），或者需要通过其他VPC访问（对等连接）。

虚拟 IP 的使用限制

- 不推荐在弹性云服务器配置多个同子网网卡的场景下，使用虚拟IP功能。若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归属VPC子网，仅支持将虚拟IP绑定至同一个子网内的云服务器。
- 使用虚拟IP构建主备场景时，备弹性云服务器需要关闭IP转发功能，具体请参见**关闭备ECS的IP转发功能**。
- 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**。

4.2 申请虚拟 IP 地址

操作场景

当弹性云服务器需要设置虚拟IP地址或预留指定的虚拟IP地址时，可以通过给子网申请虚拟IP地址的方式分配虚拟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。
6. 在“IP地址管理”页签中，单击“申请虚拟IP地址”。

7. 选择IP类型。仅在IPv6开放区域可配置。
   - IPv4
   - IPv6
8. 选择虚拟IP地址的分配方式。
   - 自动分配：系统将自动分配IP地址。
   - 手动分配：系统将分配您指定的IP地址。
9. 选择手动分配方式，请填写虚拟IP地址。
10. 单击“确定”。

在IP列表中可以查看申请的虚拟IP地址。

4.3 将虚拟 IP 地址绑定至弹性公网 IP 或实例

操作场景

您可以通过虚拟IP和弹性公网IP实现以下场景：

比如将虚拟IP绑定至多个主备部署的弹性云服务器上，并为该虚拟IP绑定一个弹性公网IP地址，可以实现通过互联网访问该主备部署集群的场景，提升业务容灾能力。

须知

虚拟IP仅提供IP地址访问能力，如果您要实现集群的主备切换或者负载均衡等自动容灾能力，必须要搭配Keepalived等相关配置才可以实现，具体可参见**搭建Keepalived Nginx高可用Web集群**。

约束与限制

- 虚拟IP只可以绑定一个弹性公网IP。
- 建议一个弹性云服务器绑定的虚拟IP数量不超过8个。
- 一个虚拟IP最多可同时绑定至10个弹性云服务器。

说明

将虚拟IP绑定至弹性云服务器时，会将虚拟IP同时关联至弹性云服务器的安全组。一个虚拟IP最多可同时关联至10个安全组。

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所属子网的名称超链接。

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

- 弹性云服务器的网卡绑定虚拟IP地址后，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**登录弹性云服务器配置虚拟IP地址**。
- 当弹性云服务器有多张网卡时，建议绑定主网卡。
- 一个弹性云服务器的网卡可以同时绑定多个虚拟IP。

登录弹性云服务器配置虚拟 IP 地址

参考以下章节，为已绑定虚拟IP的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（以下配置以“CentOS 7.2 64bit”为例）

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：

```
[172.16.0.247 pubnet0-ecs-pub0-gaea-dgdb-ipv4 ~]#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：

   ```
   [ ]#nmcli  connection up "Wired connection 1"
   Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
   ```

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**。

   ```
   [172.16.0.247_subnet0-ecs-pod6-gaea-dpdk-ipv6 ~]#ip a
   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 pfifo_fast state UP group default qlen 1000
       link/ether fa:16:3e:e5:d5:cd brd ff:ff:ff:ff:ff:ff
       inet 172.16.0.247/24 brd 172.16.0.255 scope global noprefixroute dynamic eth0
          valid_lft 86398sec preferred_lft 86398sec
       inet 172.16.0.125/32 brd 172.16.0.125 scope global noprefixroute eth0
          valid_lft forever preferred_lft forever
       inet6 2001:db8:a583:62c:7dd3:a19a:4031:d6fb/128 scope global tentative noprefixroute dynamic
          valid_lft 86400sec preferred_lft 86400sec
       inet6 fe80::5371:9bf9:b652:e35b/64 scope link noprefixroute
          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. 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（以下配置以“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，请参考以下方法进行配置。

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

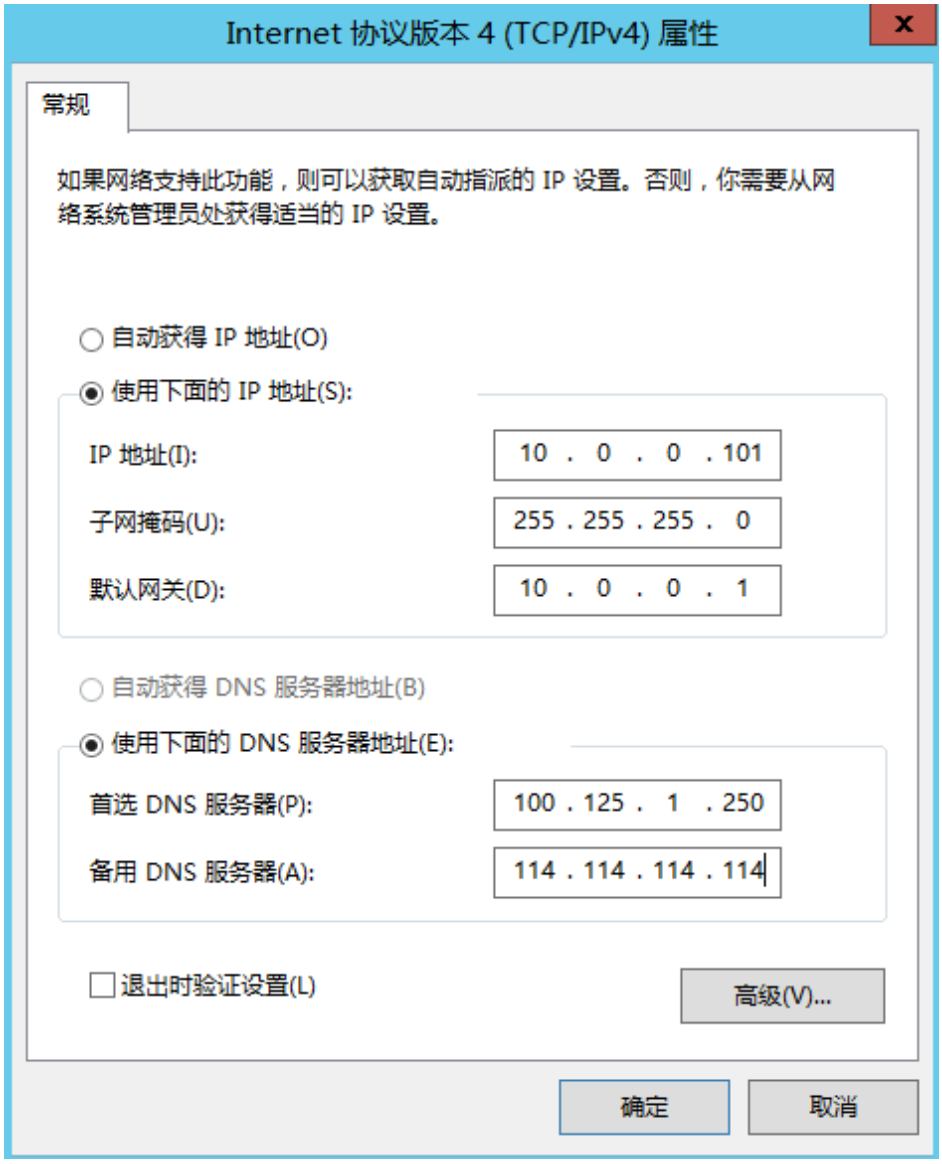
如果您需要删除已添加的虚拟IP，可以使用以下方法：

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（本文以“Windows Server”为例）

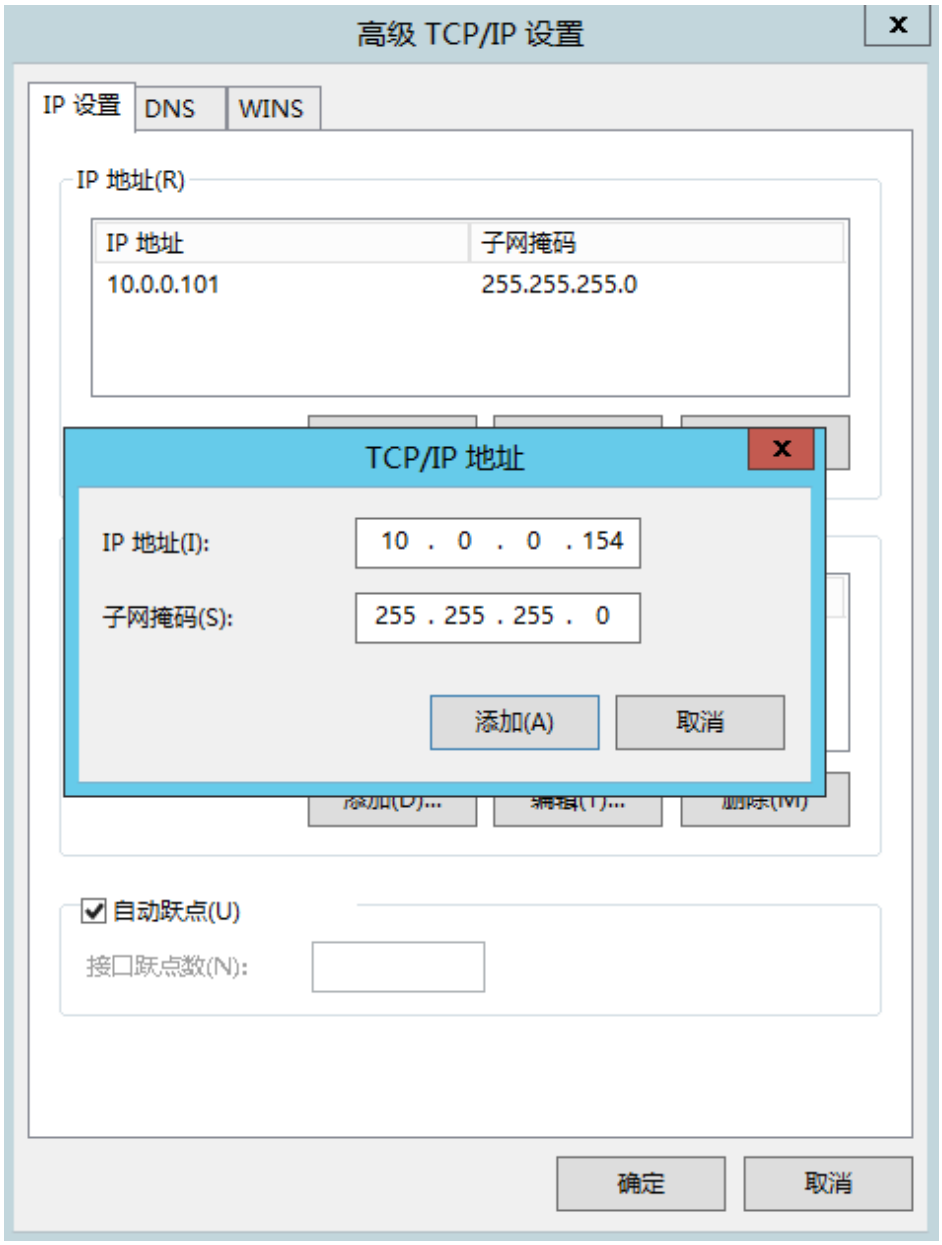
1. 在“控制面板 > 网络和共享中心”路径下，单击对应的本地连接。
2. 在打开的本地连接页面中，单击“属性”。
3. 在“网络”页签中选择“Internet 协议版本 4 （TCP/IPv4）”。
4. 单击“属性”。
5. 选择“使用下面的IP地址”，IP地址配置为弹性云服务器的私有IP地址，例如：10.0.0.101。

图 4-3 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 4-4 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?**
- **将虚拟IP地址和弹性公网IP解绑定**

4.4 为弹性公网 IP 绑定虚拟 IP 地址

操作场景

本章节指导用户为弹性公网IP绑定虚拟IP地址。

前提条件

- 已经参考**典型组网**完成弹性云服务器组网配置，确保弹性云服务器已经绑定虚拟IP。
- 已创建弹性公网IP。

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 > 弹性公网IP”。
   进入弹性公网IP列表页面。
4. 在需要绑定虚拟IP的弹性公网IP地址所在行，单击“绑定”。
5. 在“绑定弹性公网IP”弹窗中，选择实例为“虚拟IP地址”。
6. 在虚拟IP列表中，选择需要绑定的虚拟IP，单击“确定”。

   说明

   虚拟IP（VIP）主要用于弹性云服务器的主备切换，达到高可用性HA（High Availability）的目的。当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。具体请参见**搭建Keepalived Nginx高可用Web集群**。

4.5 将虚拟 IP 地址和实例解绑定

操作场景

本章节指导用户解绑虚拟IP上的实例，包括弹性云服务器以及二层连接。

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 > 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超链接。
   进入子网“基本信息”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“绑定的实例”对话框。
8. 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“是”，将虚拟IP和实例解绑。

4.6 将虚拟 IP 地址和弹性公网 IP 解绑定

操作场景

本章节指导用户解绑虚拟IP上的弹性公网IP。

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，单击虚拟IP地址所属的子网名称超链接。
   进入子网“基本信息”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“是”，将虚拟IP和弹性公网IP解绑。

4.7 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4-1**。

表 4-1 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4-5**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。 具体方法如下： • 弹性公网IP：请参见**将虚拟IP地址和弹性公网IP解绑定**。 • 弹性云服务器或者二层连接：请参见**将虚拟IP地址和实例解绑定**。 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4-6**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 4-5 虚拟 IP 无法删除-场景一

图 4-6 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“是”，删除虚拟IP地址。

4.8 关闭备 ECS 的 IP 转发功能

操作场景

使用虚拟IP构建主备场景时，您需要参考以下操作关闭备弹性云服务器的IP转发功能。

Linux 系统

1. 登录弹性云服务器。
2. 执行以下命令，切换root用户。
   su root
3. 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1，继续执行**4**。
   - 回显为0，任务结束。
4. 以下提供两种方法修改配置文件，二选一即可。
   - 方法一：使用vi打开“/etc/sysctl.conf”文件，修改net.ipv4.ip_forward = 0，按“:wq”保存退出。
   - 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
5. 执行以下命令，使修改生效。
   sysctl -p /etc/sysctl.conf

Windows 系统

1. 登录弹性云服务器。
2. 打开Windows系统的“命令提示符”窗口，执行以下命令。

   ipconfig/all

   当回显结果中，“IP 路由已启用”为 “否”， 表示IP转发功能已关闭。
3. 按“Windows+R”打开运行窗口，输入**regedit**，进入注册表编辑器。
4. 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。

4.9 关闭 ECS 网卡的源/目的检查

操作场景

使用虚拟IP构建高可用负载均衡集群场景时，您需要参考以下操作关闭弹性云服务器网卡的源/目的检查。

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. 在弹性云服务器列表中单击该弹性云服务器名称。
5. 进入弹性云服务器详情页面，单击“网卡”页签。
6. 确认网卡详情中“源/目的检查”状态已设置“关闭”。

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
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
私有IP地址	选择是否自动分配私有IP地址。	-
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，单击需要查看详情的弹性网卡名称。

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。

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“是”，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. 单击待修更改安全组的弹性网卡名称，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“关联安全组”页签下单击“配置规则”，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

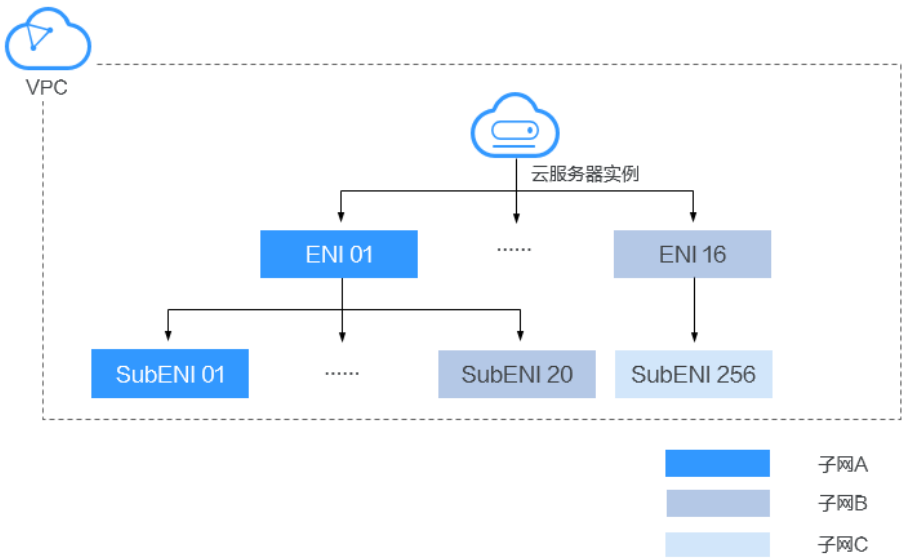
5.2.1 辅助弹性网卡概述

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

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。

图 5-1 辅助弹性网卡示意图



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

当云服务器实例所需挂载的网卡超出弹性网卡的上限时，您可以参考本章节创建辅助弹性网卡，为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。

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。
- 使用辅助弹性网卡时，您需要在云服务器实例的网卡上创建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
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	辅助弹性网卡归属的VPC，无需填写。	vpc-A
所属子网	选择辅助弹性网卡归属的子网。	subnet-A01
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“>”。	-

参数	参数说明	取值样例
创建数量	待创建的辅助弹性网卡的数量，取值范围为1~20。	1
私有IP地址	选择是否为辅助弹性网卡分配私有IPv4地址，私有IP地址仅支持内网请求。 当前版本不支持去勾选。	-
IPv4地址	选择私有IP地址的分配方式： • 自动分配IP地址：系统自动分配IP地址。 • 手动指定IP地址：系统按指定的IP地址进行分配。 若选择“手动指定IP地址”，则填写IPv4的私有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

4. 单击“确定”，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**，在云服务器实例的网卡上创建VLAN子接口并配置对应规则。

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，您还需要在云服务器实例的网卡中为该辅助弹性网卡创建VLAN子接口并配置私网IP地址、默认路由规则。

在配置之前，您需要获取辅助弹性网卡的信息，如**表5-3**所示。

表 5-3 辅助弹性网卡信息

信息	获取方式	说明
VLAN	管理控制台	在辅助弹性网卡列表中获取。 详细内容请参见**查看辅助弹性网卡基本信息**。
MAC地址		
私网IP地址		
网关		在辅助弹性网卡所在子网的详情页获取。

本操作以在云服务器实例（以CentOS 8.2为例，其余规格请参考操作系统帮助文档）的eth0网卡上创建VLAN子接口为例介绍具体的配置步骤。

在本示例中：

- VLAN：2110
- 私有IP地址：192.168.0.2/24
- 网关：192.168.0.1
- MAC地址：fa:16:3e:a1:b2:**

配置步骤

1. 登录云服务器实例。
   登录方式请参见**Linux弹性云服务器登录方式概述**。
2. 为eth0创建VLAN子接口。
   ip link add link *eth0* **name** *eth0.2110* **type vlan id** *2110*
3. 创建命名空间“ns2110”。
   ip netns add *ns2110*
4. 将VLAN子接口“eth0.2110”加入命名空间“ns2110”。
   ip link set *eth0.2110* **netns** *ns2110*
5. 修改VLAN子接口的MAC地址为“*fa:16:3e:a1:b2:***”。
   ip netns exec *ns2110* **ifconfig** *eth0.2110* **hw ether** *fa:16:3e:a1:b2:***
6. 启动VLAN子接口。
   ip netns exec *ns2110* **ifconfig** *eth0.2110* **up**
7. 为VLAN子接口配置私网IP地址“*192.168.0.2/24*”。
   ip netns exec *ns2110* **ip addr add** *192.168.0.2/24* **dev** *eth0.2110*
8. 为VLAN子接口配置默认路由，其中“*192.168.0.1*”为辅助弹性网卡所在子网的网关。
   ip netns exec *ns2110* **ip route add default via** *192.168.0.1*

验证方法

1. 通过在命名空间访问同一VPC下其他私网IP地址（例如*a.b.c.d*），验证配置辅助弹性网卡是否生效。
   ip netns exec *ns2110* **ping** *a.b.c.d*

图 5-2 成功示例

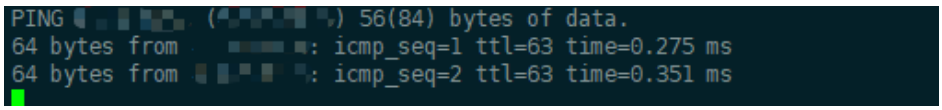
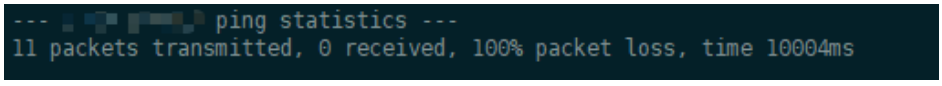


图 5-3 失败示例



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。

6 访问控制

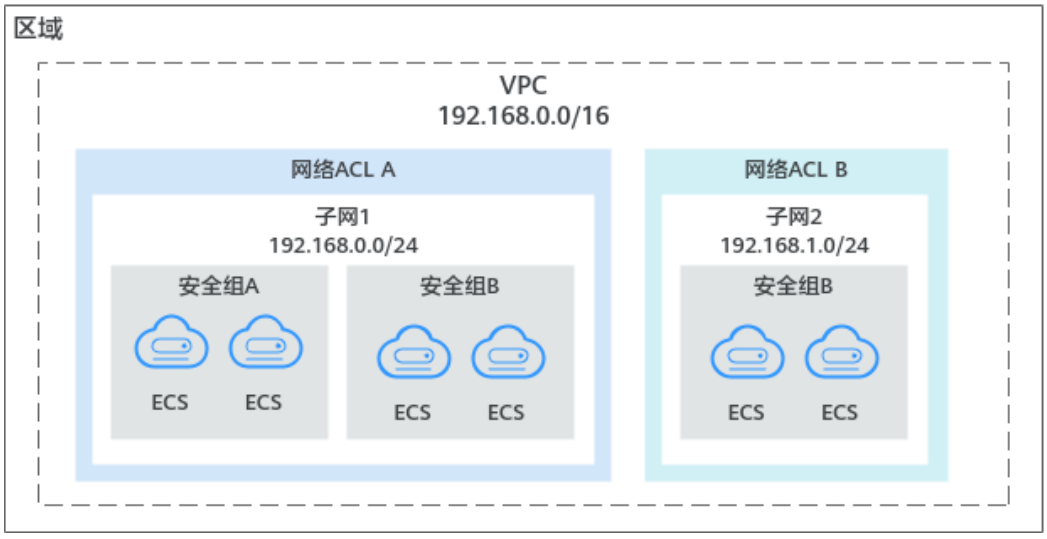
6.1 VPC 访问控制概述

虚拟私有云VPC是您在云上的私有网络，通过配置安全组和网络ACL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。

安全组和网络ACL的应用示例如图6-1所示。本示例中，安全组A和安全组B可以保护其中ECS的网络安全，通过网络ACL A和网络ACL B，可以分别保护整个子网1和子网2的安全，双层防护提升安全保障。

图 6-1 安全组与网络 ACL



安全组与网络 ACL 的区别说明

表6-1为您提供了安全组和网络ACL的详细区别。

表 6-1 安全组和网络 ACL 区别

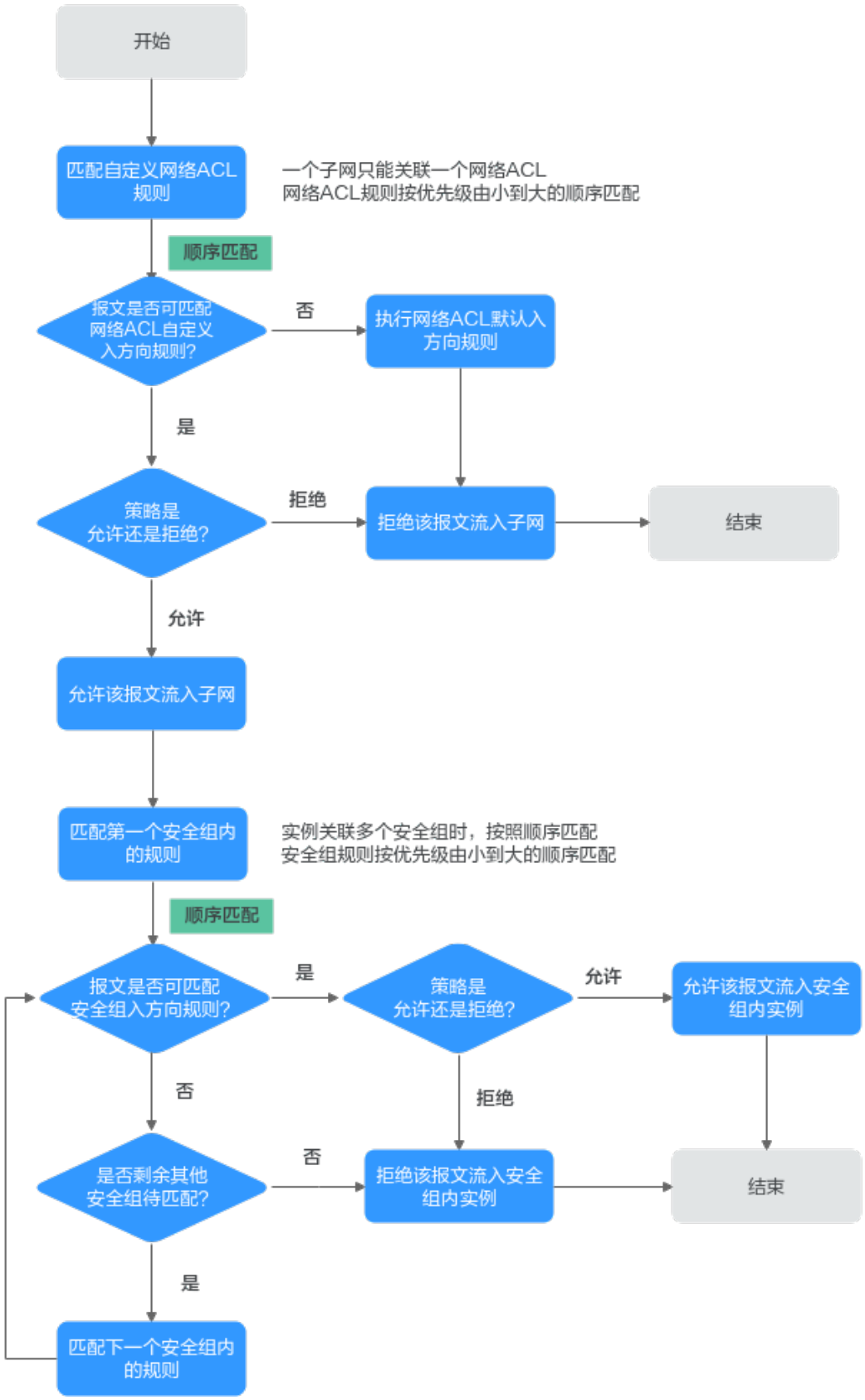
对比项	安全组	网络ACL
防护范围	实例级别：防护安全组内的实例，比如弹性云服务器、数据库、云容器实例等。	子网级别：防护整个子网，子网内的所有实例都会受到网络ACL的保护。
是否必选	必选，实例必须至少加入到一个安全组内。	非必选，您可以根据业务需求选择是否为子网关联网络ACL。
有无状态	有状态，允许入站请求/出站请求的响应流量出入实例，不受规则限制。	有状态，允许入站请求/出站请求的响应流量出入子网，不受规则限制。
规则策略	安全组支持设置允许和拒绝策略。 ● 允许策略：对于匹配成功的流量，允许流入/流出实例。 ● 拒绝策略：对于匹配成功的流量，拒绝流入/流出实例。	网络ACL支持设置允许和拒绝策略。 ● 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。
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。
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，根据规则的优先级进行生效。优先级数字越小，网络ACL规则排序越靠前，越先生效。
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。

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

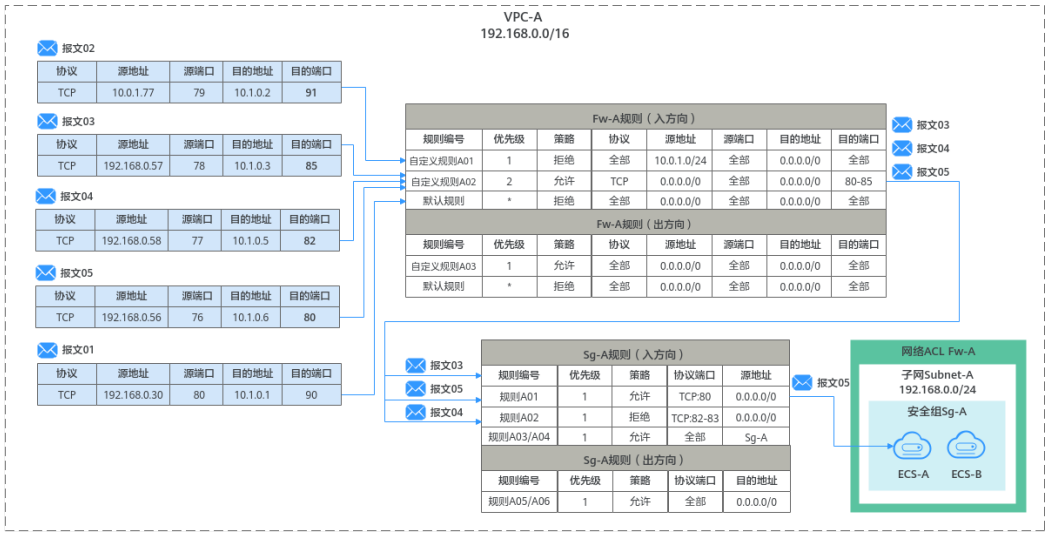


表 6-2 网络 ACL Fw-A 规则说明

方向	优先级	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	优先级	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

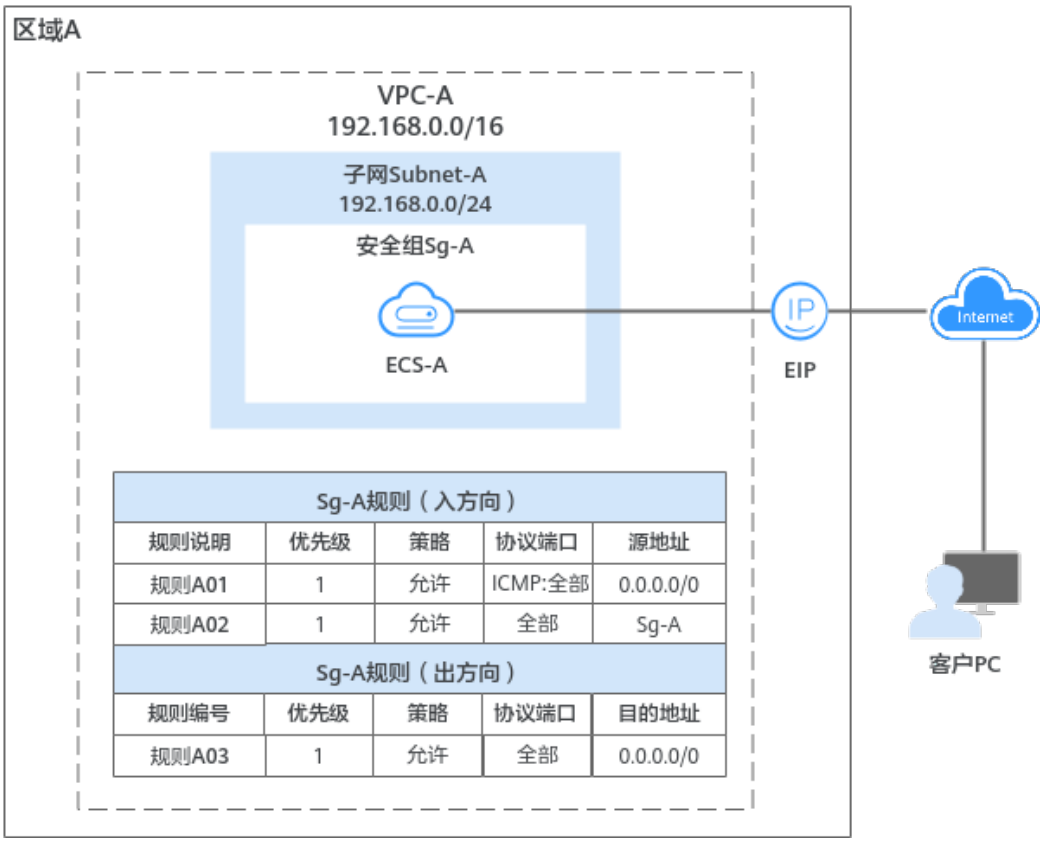
安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

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。

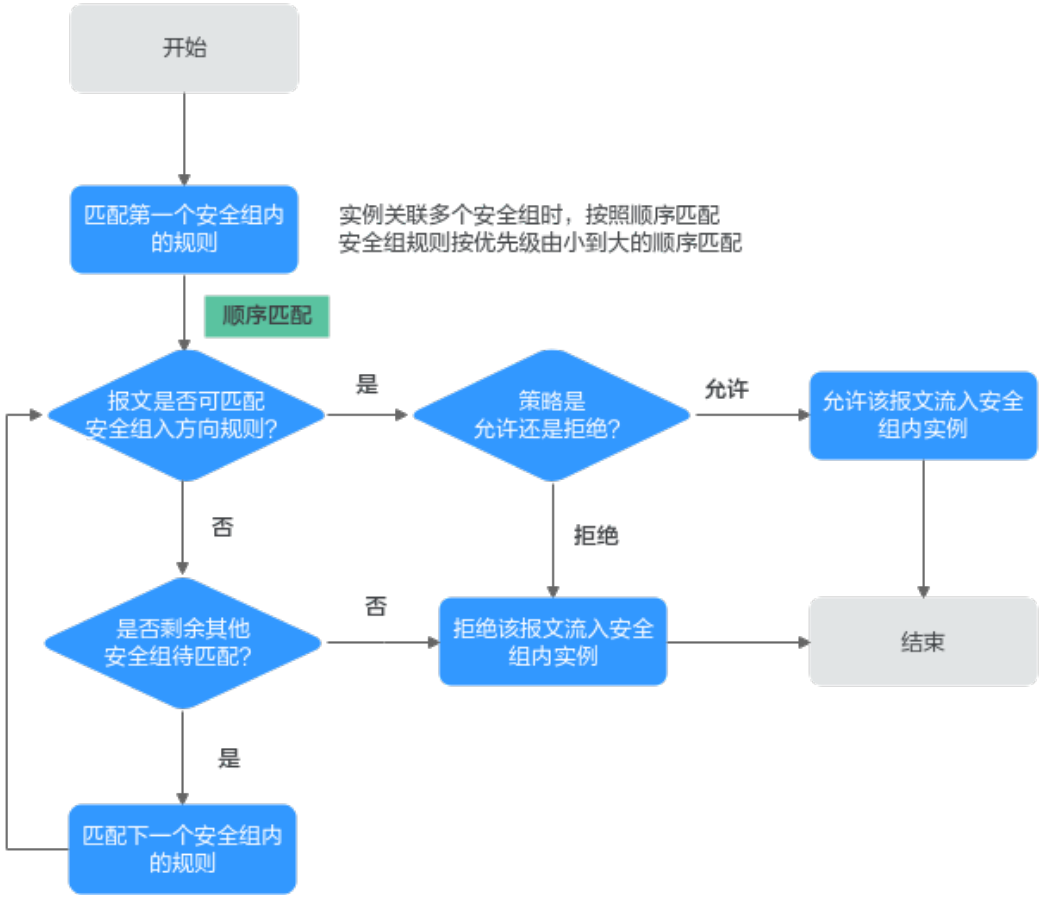
   比如，安全组A的序号为1，安全组B的序号为2，安全组A的优先级高于安全组B，流量优先匹配安全组A内的入方向规则。

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

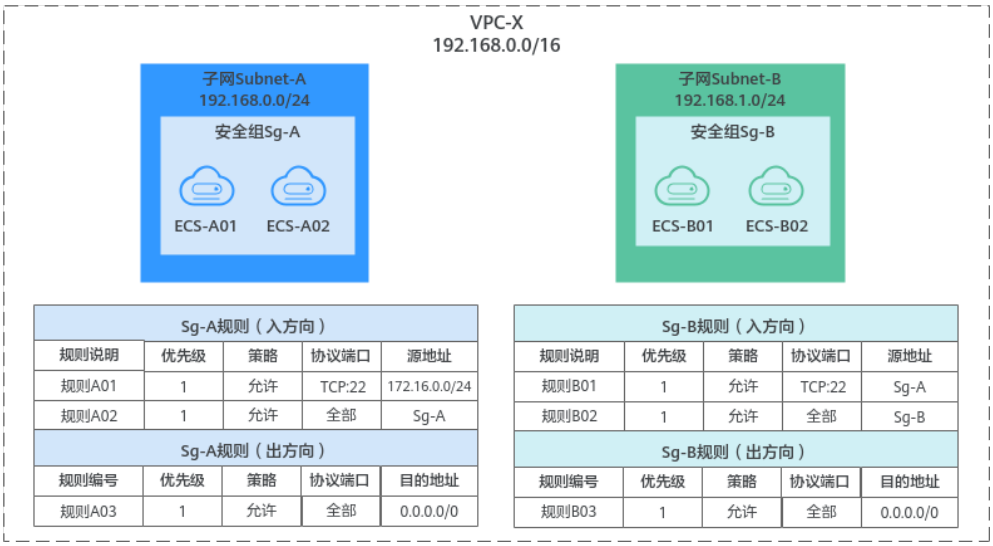
您可以在安全组内放通指定IP地址，允许指定IP地址访问安全组内实例，或者在某个安全组内放通另外一个安全组，实现不同安全组内的实例内网互通。通过安全组规则，您可以灵活控制组网内流量的走向，以确保您的网络安全，以下为您提供了典型的安全组应用示例。

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**。

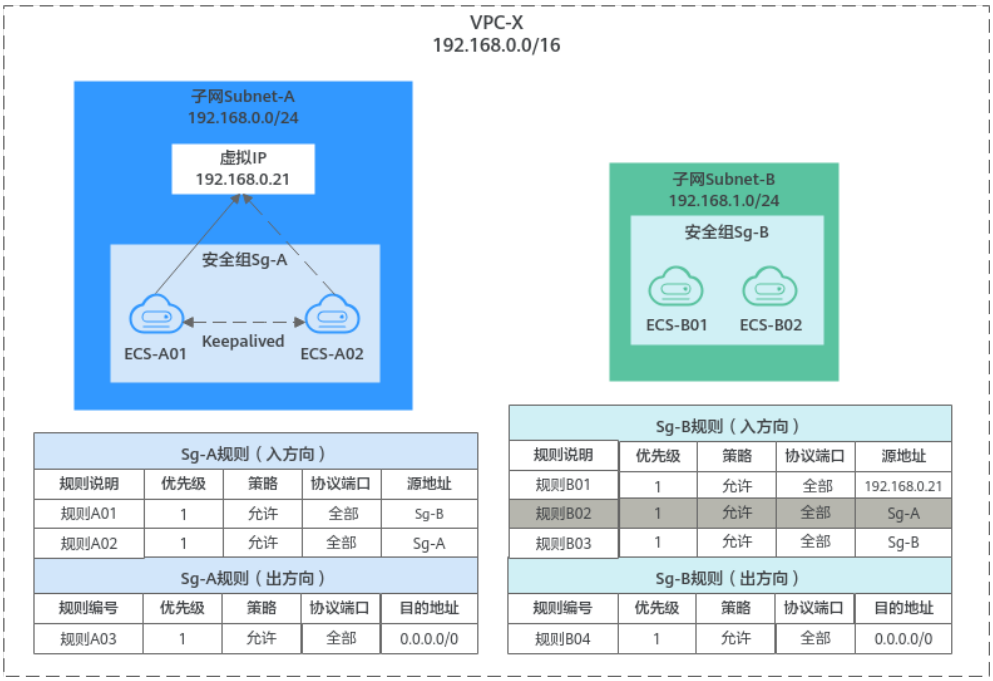
控制虚拟 IP 访问安全组内实例

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

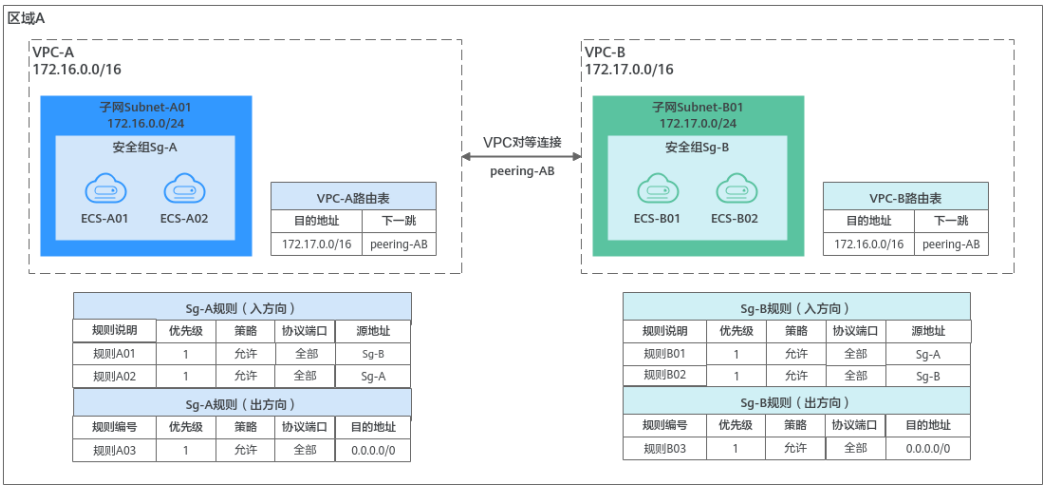
更多安全组规则配置示例，请参见**安全组配置示例**。

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模板，支持“通用Web服务器”和“开放全部端口”等模板。模板中会预置部分安全组规则，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 ≤ 128条，否则超过数量的安全组规则将不生效。出方向的限制和入方向一致。
  - 源地址是安全组时，包括本安全组和其他安全组。
  - 不连续端口号取值示例为22,25,27。
- 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6-6**了解详情。

表 6-6 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）
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

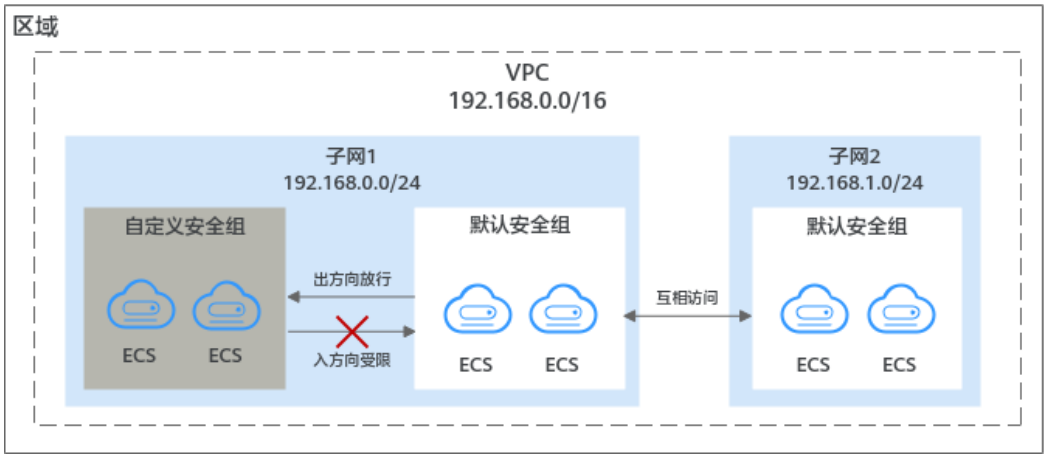
您可以免费使用安全组资源，当前不收取任何费用。

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6-7所示。

表 6-7 默认安全组规则

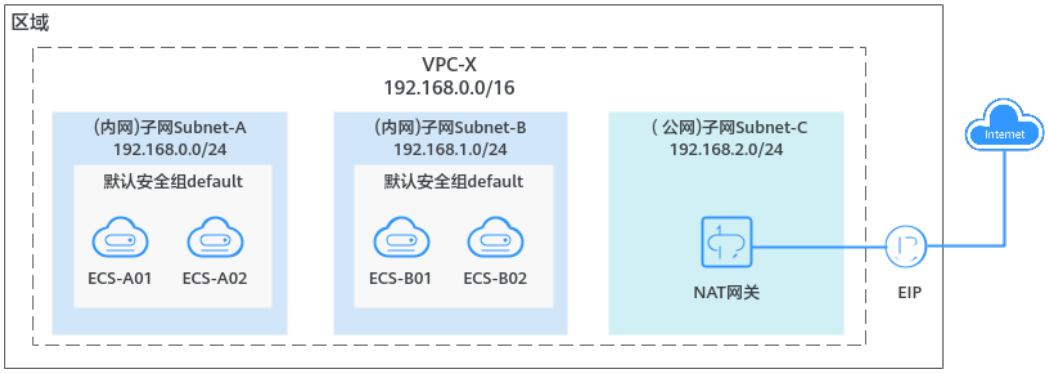
方向	策略	类型	协议端口	源地址/目的地址	描述
入方向	允许	IPv4	全部	源地址：默认安全组（default）	针对全部IPv4协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。
入方向	允许	IPv6	全部	源地址：默认安全组（default）	针对全部IPv6协议，允许安全组内的实例可使用任何协议和端口互相通信，确保安全组内实例网络互通。
出方向	允许	IPv4	全部	目的地址：0.0.0.0/0	针对全部IPv4协议，允许所有流量从安全组内实例流出，即实例可访问外部任意IP和端口。
出方向	允许	IPv6	全部	目的地址：::/0	针对全部IPv6协议，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6-8重新添加规则。

表 6-8 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6-9。
- 通过RDP远程登录Windows云服务器，需要放通RDP(3389)端口，请参见表6-10。

表 6-9 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 6-10 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，配置示例请参见**表6-11**。

表 6-11 通过特定 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 6-12 在本地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

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）**。

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 6-13 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 6-14 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 6-15 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。常见的数据库类型机器对应的端口如下：

- MySQL(3306)
- Oracle(1521)
- MS SQL(1433)
- PostgreSQL(5432)
- Redis(6379)

表 6-16 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6-18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 6-17 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。
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6-18所示。

表 6-18 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 弹性云服务器常用端口

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6-19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 6-19 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6-20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 6-20 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。

端口	协议	说明
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。
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**。

安全组模板说明

创建安全组的时候，系统为您提供了几种常见的安全组模板。安全组模板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模板，快速完成安全组的创建。安全组模板的详细说明如**表6-21**所示。

表 6-21 安全组规则说明

模板名称	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。	
		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。	

模板名称	方向	类型和协议端口	源地址/目的地址	规则说明	适用场景
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。	
快速添加规则	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。	您可以勾选常见协议端口，在入方向快速添加规则放通对应的协议及端口。 若您未勾选任何协议端口，则不会放通任何端口。请在安全组创建完成后，参考**添加安全组规则**自行添加所需的规则。
		自定义选择的端口和协议	0.0.0.0/0	针对TCP或者ICMP协议，允许外部所有IP访问安全组内云服务器的指定端口，用于实现不同的用途。	
	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。

表 6-22 参数说明

参数	参数说明	取值样例
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
模板	必选参数。 创建安全组的时候，系统为您提供了几种常见的安全组模板。安全组模板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模板，快速完成安全组的创建。 安全组模板的详细说明如**表6-21**所示。	通用Web服务器
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“>”。	-

4. 安全组参数设置完成后，可以在创建页面下方查看模板的入方向和出方向规则，确认无误后，单击“确定”。

相关操作

- 如果安全组模板内置的规则无法满足您的使用要求，那么安全组创建完成后，您可以在安全组内添加或者修改安全组规则，具体操作请参见**添加安全组规则**。
- 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**导入和导出安全组规则**。

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。

6.2.5.5 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。

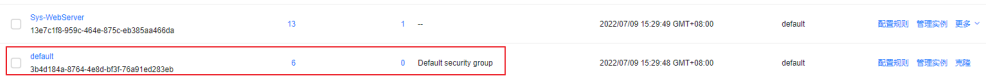
说明

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 6-12 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。

6.2.5.6 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6-23。

表 6-23 安全组标签命名规则

参数	规则	样例
键	• 对于每个安全组资源，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。 • 由英文字母、数字、下划线、中划线组成。	test
值	• 可以为空。 • 最大长度不超过256个字符。 • 由英文字母、数字、下划线、点、中划线组成。	01

约束与限制

- 每个标签由“标签键”和“标签值”组成，“标签键”不支持修改，只能修改“标签值”。
  如果需要修改“标签键”，请删除后重新添加。
- 每个云资源最多可以添加20个标签。

添加安全组标签

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. 选择“标签”页签，在标签列表左上方，单击“添加标签”。
   弹出添加标签对话框。
7. 根据界面提示，输入标签对应的“键”和“值”，并单击“确定”。
   返回标签列表，可查看已添加的标签。

修改安全组标签

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. 选择“标签”页签，在标签列表中，单击标签所在行的操作列下的“编辑”。
   弹出编辑标签对话框。
7. 根据界面提示，输入标签对应的“值”，并单击“确定”。
   返回标签列表，可查看已修改的标签。

删除安全组标签

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. 选择“标签”页签，在标签列表中，单击标签所在行的操作列下的“删除”。
   弹出删除标签对话框。
7. 确认无误后，单击“是”。
   返回标签列表，原有标签已删除。

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路流量、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**。
- 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6-24**所示。

    表 6-24 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 6-13 添加安全组入方向规则

表 6-25 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IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。 – 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。	IP地址：0.0.0.0/0
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“+”按钮，可以依次增加多条出方向规则。

图 6-14 添加安全组出方向规则

表 6-26 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IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。 – 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。	IP地址：0.0.0.0/0
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6-27中的规则，放通HTTP(80)端口。

表 6-27 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6-15，说明80端口已开通。

     图 6-15 Linux TCP 80 端口验证结果

   - **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6-16，说明TCP 80端口已开通。

     图 6-16 Windows TCP 80 端口验证结果

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**弹性云服务器常用端口**。

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 6-17 快速添加安全组入方向规则

表 6-28 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IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。 – 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。	安全组
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 6-18 快速添加安全组出方向规则

表 6-29 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IP地址框内同时输入多个IP地址，一个IP地址对应一条安全组规则。 – 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。	安全组
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6-30**所示。

表 6-30 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。

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。

约束与限制

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。

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6-31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6-31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 6-31 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 导入和导出安全组规则

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。
- 当导入的安全组规则与安全组内已有规则重复时，系统会自动帮您过滤掉重复的规则，不影响导入。
- 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6-32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 6-32 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6-33所示。

表 6-33 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
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。	-

6.2.6.7 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6-34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6-34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 6-34 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，执行以下操作，删除安全组规则。
   - 删除单个安全组规则：单击目标安全组规则所在行的操作列下的“删除”。
   - 删除多个安全组规则：勾选多个安全组规则，并单击安全组规则左上方的“删除”。
8. 在删除对话框中，确认无误后，单击“确定”，删除安全组规则。

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。

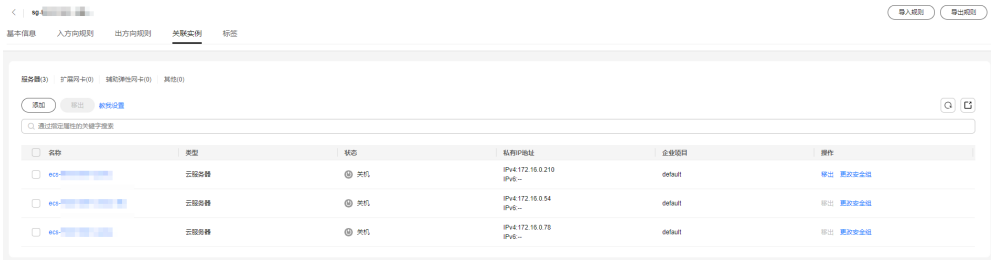
当前您可以在安全组中添加的实例类型包括服务器、扩展网卡以及辅助弹性网卡等。操作方法如下：

- **在安全组中添加实例**
- **在安全组中移出实例**

在安全组中添加实例

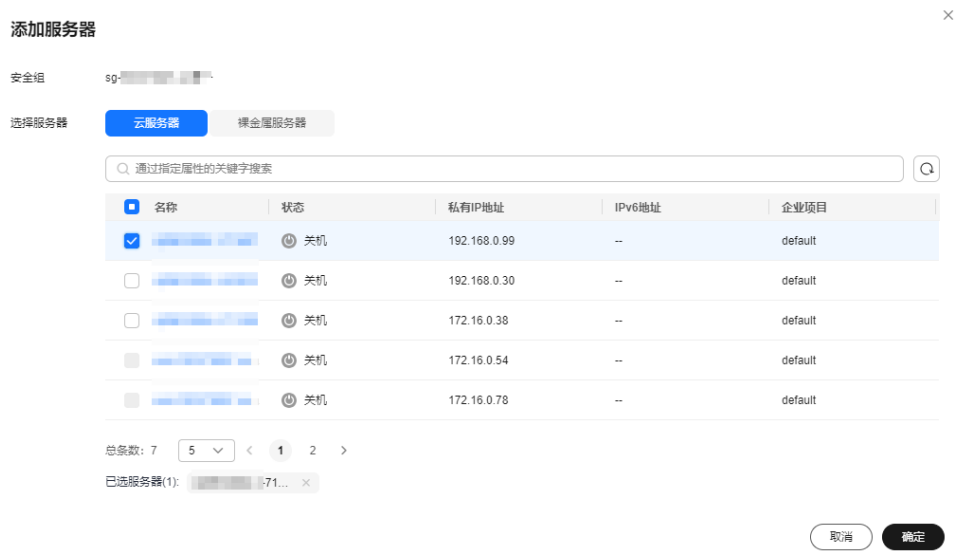
1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
4. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
5. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入实例列表页面。
6. 根据界面提示，选择目标实例类型对应的页签。
   以下操作，以选择“服务器”页签为例。

   图 6-19 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 6-20 添加服务器



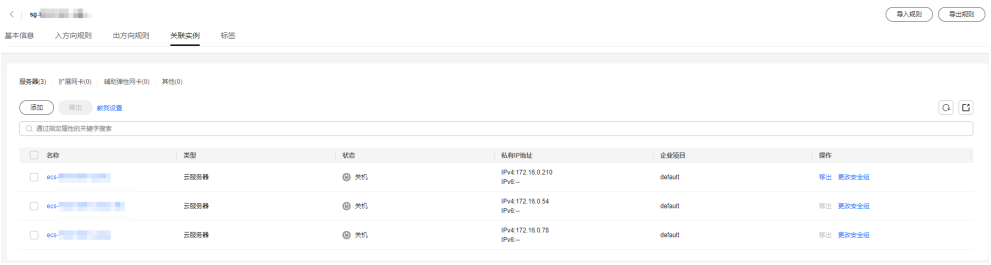
8. 在服务器列表中，选择一个或者多个服务器，并单击“确定”，将服务器加入到当前安全组中。

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 6-21 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 6-22 移出服务器

8. 确认无误后，单击“是”，将所选实例从安全组中移出。

6.2.7.2 更改弹性云服务器的安全组

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。

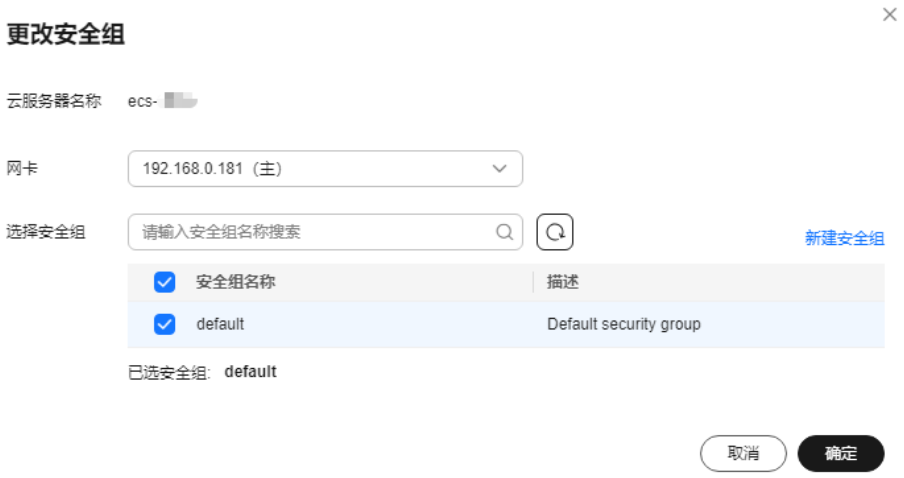
除了默认安全组，您还可以为弹性云服务器关联自定义安全组，当自定义安全组不满足需求时，您也可以更改自定义安全组。

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 > 网络设置 > 更改安全组”。

   系统弹窗显示“更改安全组”页面。

图 6-23 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6-24**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。

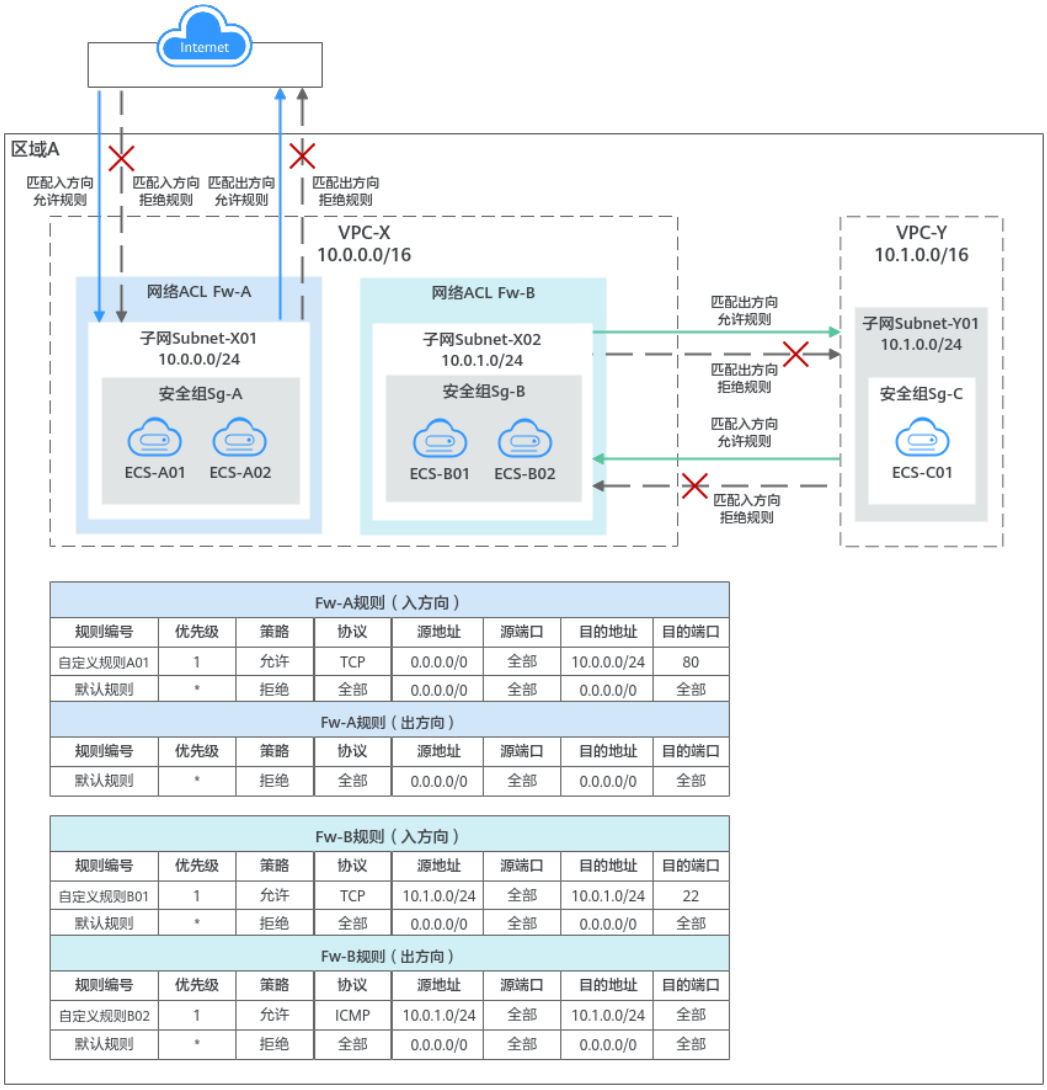
  网络ACL是有状态的，允许入站请求的响应流量出站，不受规则限制，因此Subnet-X01内实例的响应流量可流出子网。非响应流量的其他流量则匹配默认规则，无法流出子网。

- 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 6-24 网络 ACL 架构图



Fw-A规则（入方向）							
规则编号	优先级	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	优先级	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	优先级	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	优先级	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6-24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：
  - 优先级：即网络ACL规则的序号，网络ACL规则按照该序号依次排列，流量则按照规则序号进行匹配。优先级数字越小，表示规则排序越靠前，流量越先匹配该规则。

默认网络ACL规则优先级的值为“*”，排在末尾，优先级最低。

- 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、目源地址/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6-35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 6-35 网络 ACL 默认规则说明

方向	优先级	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6-36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 6-36 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

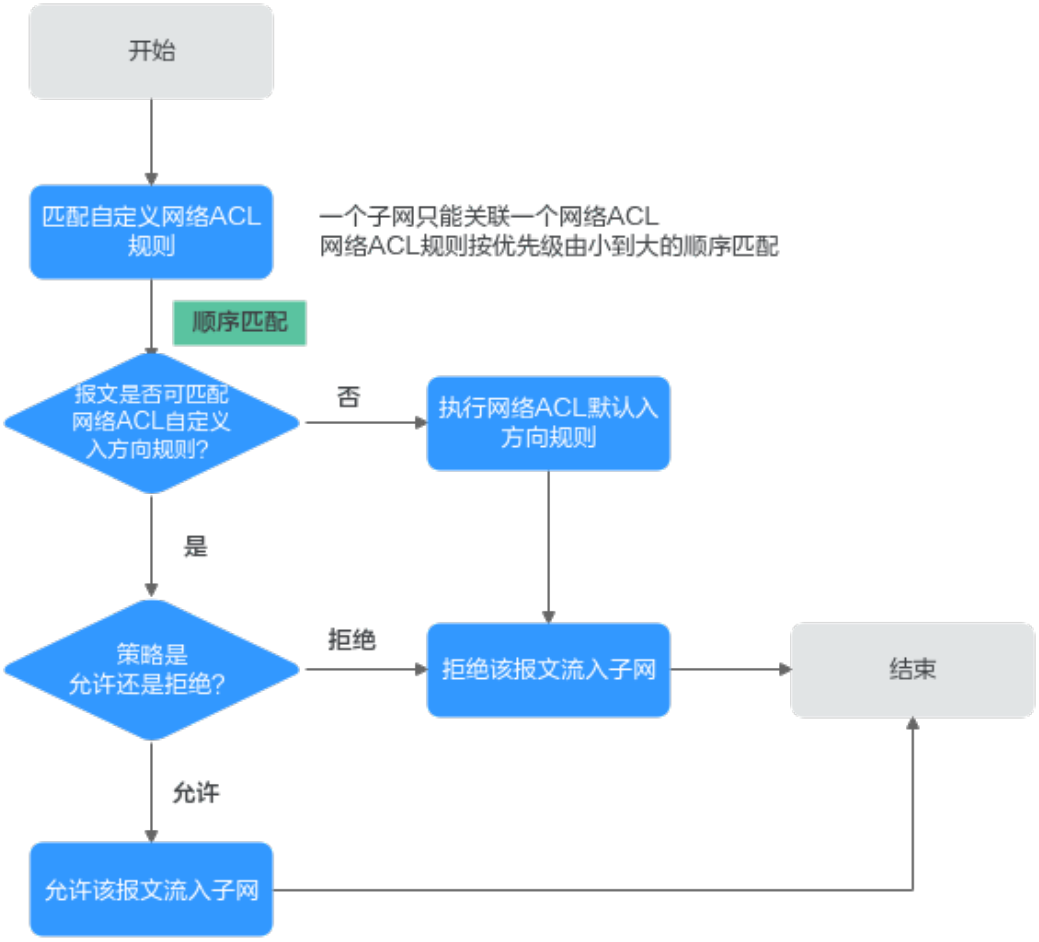
一个子网只能绑定一个网络ACL，当网络ACL存在多条规则时，流量按照规则的优先级进行匹配。优先级的数字越小，优先级越高，越先执行该规则。默认规则优先级的值为“*”，优先级最低。

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 6-25 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。

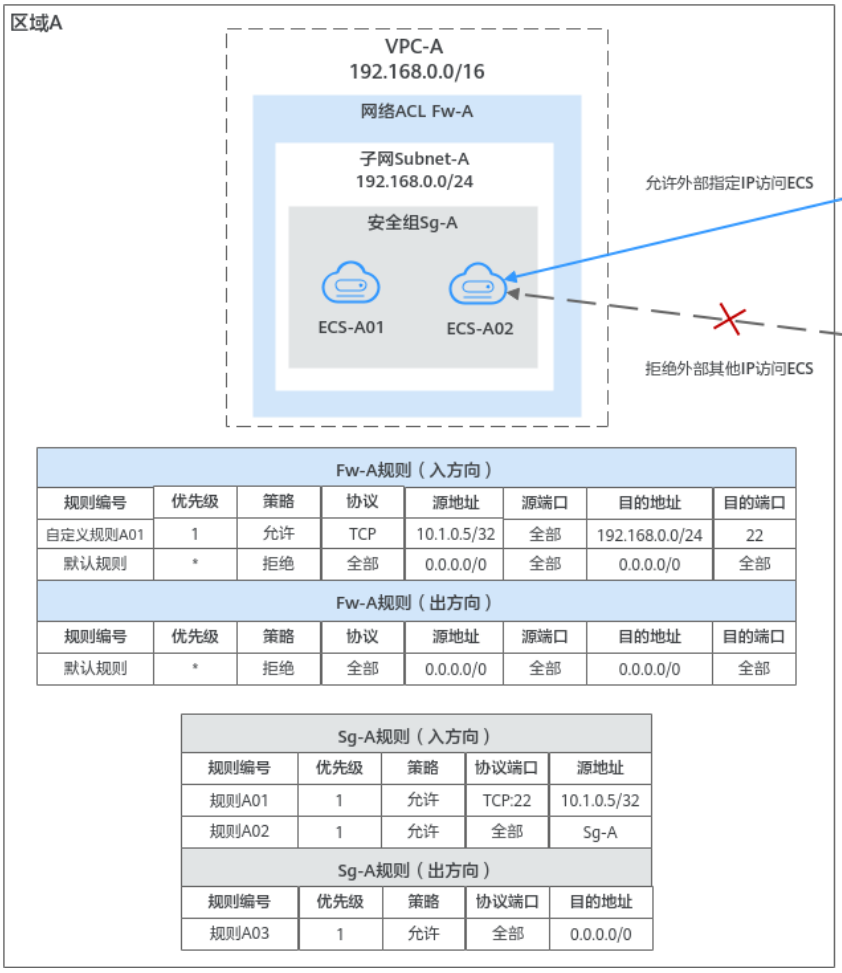
控制外部对子网内实例的访问

本示例如图6-26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 6-26 控制外部对子网内实例的访问



Fw-A规则（入方向）							
规则编号	优先级	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	优先级	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6-37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 6-37 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6-27**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

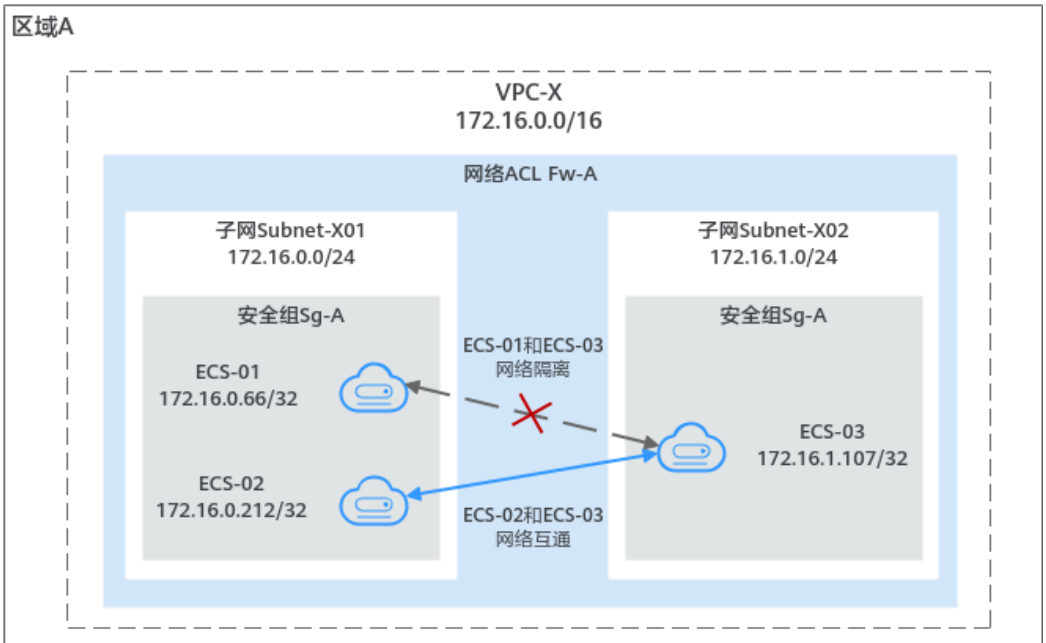
为了实现以上网络通信需求，本示例的安全组和网络ACL配置如下：

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 6-27 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	优先级	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	1	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	优先级	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	1	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 6-28 网络 ACL 配置流程

表 6-38 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（默认生效顺序） 添加网络ACL规则（自定义生效顺序）
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。
- 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6-39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 6-39 网络 ACL 默认规则说明

方向	优先级	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6-40**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 6-40 拒绝外部访问子网内实例的指定端口

方向	优先级	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6-41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 6-41 拒绝外部指定 IP 地址访问子网内实例

方向	优先级	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6-42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 6-42 网络 ACL 规则（允许外部访问子网内实例的指定端口）

方向	优先级	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	优先级	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6-43**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 6-43 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 6-44 网络 ACL 参数说明

参数	参数说明	取值样例
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。 每个云资源最多可以添加20个标签。 关于标签更详细的说明，请参见**表6-45**。	“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。	-

表 6-45 网络 ACL 标签命名规则

参数	规则	样例
键	• 对于每个网络ACL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。 • 由英文字母、数字、下划线、中划线组成。	test

参数	规则	样例
值	• 可以为空。 • 最大长度不超过256个字符。 • 由英文字母、数字、下划线、点、中划线组成。	01

4. 单击“确定”，完成创建。
5. 网络ACL参数设置完成后，单击“确定”。

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（默认生效顺序）**或者**添加网络ACL规则（自定义生效顺序）**。
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

网络ACL创建完成后处于开启状态，同时支持根据业务需求灵活开启或者关闭网络ACL。

- 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“是”，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“是”，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：规则的优先级、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 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。

6.3.3.6 管理网络 ACL 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的标签**
- **修改网络ACL的标签**
- **删除网络ACL的标签**

网络ACL标签规则的详细说明，请参见**表6-46**。

表 6-46 网络 ACL 标签命名规则

参数	规则	样例
键	• 对于每个网络ACL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。 • 由英文字母、数字、下划线、中划线组成。	test
值	• 可以为空。 • 最大长度不超过256个字符。 • 由英文字母、数字、下划线、点、中划线组成。	01

约束与限制

- 每个标签由“标签键”和“标签值”组成，“标签键”不支持修改，只能修改“标签值”。
  如果需要修改“标签键”，请删除后重新添加。
- 每个云资源最多可以添加20个标签。

添加网络 ACL 的标签

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 > 网络ACL”。
   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的基本信息页面。
6. 选择“标签”页签，并单击“添加标签”。
   弹出“添加标签”对话框。
7. 根据界面提示，设置“标签键”和“标签值”，并单击“确定”。
   返回标签列表页面，可以看到添加的标签。

修改网络 ACL 的标签

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 > 网络ACL”。
   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的基本信息页面。
6. 选择“标签”页签，并在标签列表中，单击目标标签所在行的操作列下的“编辑”。
   弹出“编辑标签”对话框。
7. 根据界面提示，修改“标签值”，并单击“确定”。
   返回标签列表页面，可以看到修改后的标签。

删除网络 ACL 的标签

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 > 网络ACL”。
   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的基本信息页面。
6. 选择“标签”页签，并在标签列表中，单击目标标签所在行的操作列下的“删除”。
   弹出删除确认对话框。
7. 确认无误后，单击“是”删除标签。
   标签删除后无法恢复，请谨慎操作。

6.3.4 管理网络 ACL 规则

6.3.4.1 添加网络 ACL 规则（默认生效顺序）

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。

通过以下操作添加网络ACL规则时，系统会按照规则添加的先后顺序生成优先级，先添加的规则排序靠前，即优先匹配流量，不支持您指定优先级。

如表6-47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的优先级为1，自定义规则B的优先级为2，默认规则的优先级最低。此时添加规则C，则系统指定规则C的优先级为3，生效顺序晚于规则A和规则B，高于默认规则。

表 6-47 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**
默认规则	*	默认规则	*

如果系统默认生成的优先级不满足您的使用要求，则您可以参考**添加网络ACL规则（自定义生效顺序）**，自定义新增网络ACL规则的生效顺序。

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。

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“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 6-48 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

参数	参数说明	取值样例
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。	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。	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。	-

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。

   – 系统会按照规则添加的先后顺序生成优先级，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。

6.3.4.2 添加网络 ACL 规则（自定义生效顺序）

操作场景

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，则可以参考以下操作，在对应规则前面或者后面插入新的规则。

如表6-49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的优先级为1，自定义规则B的优先级为2，默认规则的优先级最低。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的优先级为2，规则B的优先级顺延为3，规则C的生效顺序高于规则B。

表 6-49 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	*

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，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。

6.3.4.3 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6-50**所示。

表 6-50 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。	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。	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。

6.3.4.4 开启/关闭网络 ACL 规则

操作场景

网络ACL规则添加完成后，一般处于启动状态。您可以根据业务需求灵活开启或者关闭网络ACL自定义规则。

- 关闭网络ACL自定义规则后，规则将会失效。如果您关闭了所有自定义规则，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，关闭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。
- 开启网络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，开启操作会影响子网的网络流量走向，请您谨慎评估后再执行开启操作，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，开启或者关闭网络ACL规则。
   - 开启网络ACL规则：
     i. 选择目标网络ACL规则所在行的操作列下的“更多 > 开启”。
        弹出开启确认对话框。
     ii. 确认信息无误后，单击“是”，开启网络ACL规则。
   - 关闭网络ACL规则：
     i. 选择目标网络ACL规则所在行的操作列下的“更多 > 关闭”。
        弹出关闭确认对话框。
     ii. 确认信息无误后，单击“是”，关闭网络ACL规则。

6.3.4.5 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。

6.3.4.6 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。

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，删除网络ACL规则。
   - 删除单个网络ACL规则：单击目标网络ACL规则所在行的操作列下的“删除”。
   - 删除多个网络ACL规则：勾选多个网络ACL规则，并单击网络ACL规则左上方的“删除”。
8. 在删除对话框中，确认无误后，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（默认生效顺序）**。

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. 在子网列表中，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“是”。
        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. 在子网列表中，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“是”。
        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

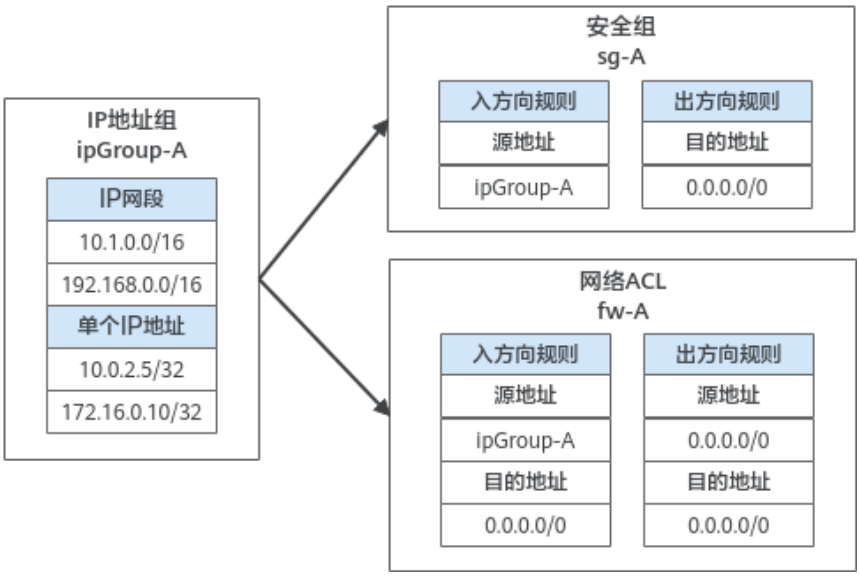
IP地址组是一个或者多个IP地址的集合，可关联至安全组、网络ACL，用于简化网络架构中IP地址的配置和管理。

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（默认生效顺序）**： • 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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。	-

7. 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 在IP地址组列表中，选择一个或多个目标IP地址组，并单击列表上方的“导出”。
   将当前IP地址组详情导出为Excel文件。

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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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。
7. 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7-6**。

表 7-6 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
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	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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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。
7. 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7-7**。

表 7-7 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

8. 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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。
7. 单击“下载模板”，将Excel格式的填写模板下载至本地。
8. 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7-8。

表 7-8 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

9. 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. 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“IP地址组”。
   进入IP地址组列表页面。
5. 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。
6. 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。

8 对等连接

8.1 对等连接概述

对等连接

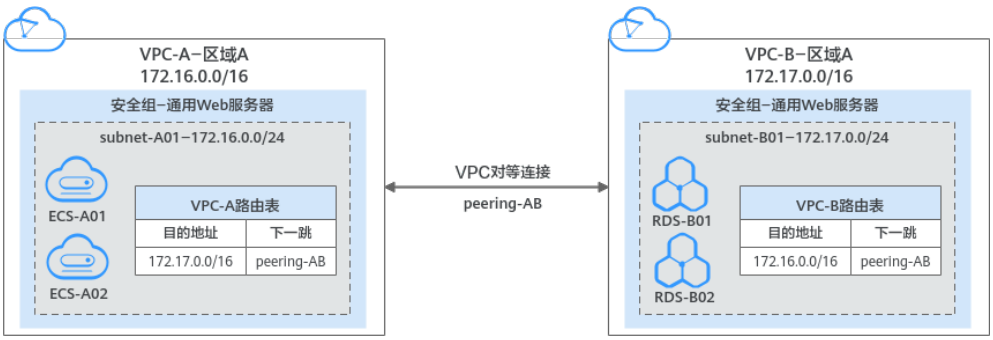
对等连接是建立在两个VPC之间的网络连接，不同VPC之间网络不通，通过对等连接可以实现不同VPC之间的云上内网通信。对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。

- 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 对等连接组网示意图



须知

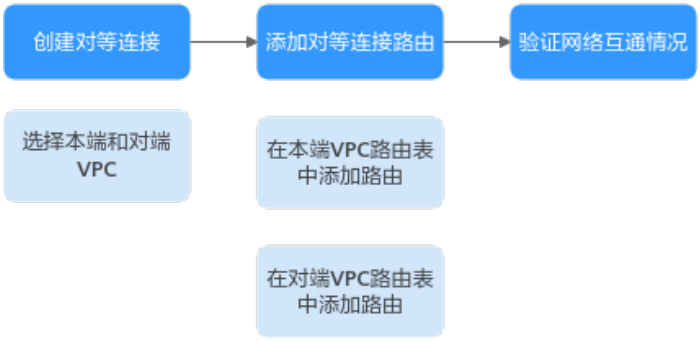
当前VPC对等连接暂不收取您的任何费用。

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：

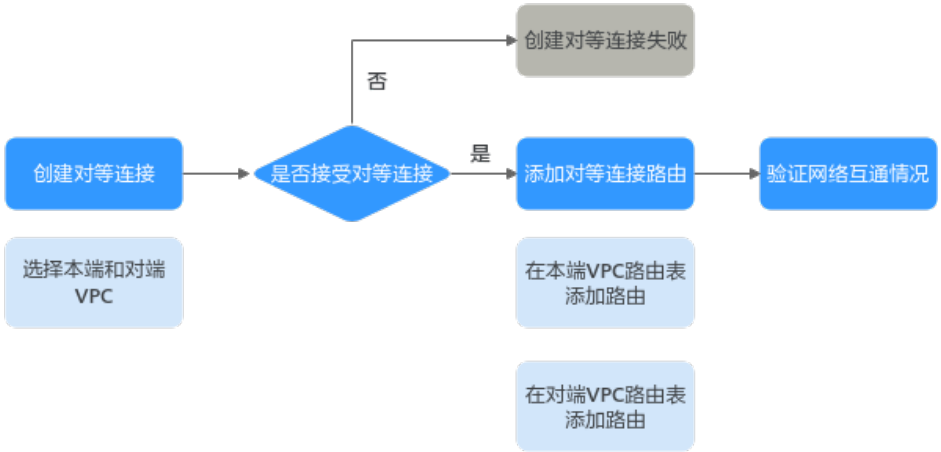
- 相同账户下的VPC对等连接创建流程如图8-2所示。
  创建对等连接的具体操作，请参见**创建相同账户下的对等连接**。

  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，以下不同情况下的组网配置示例，请您参考**对等连接使用示例**。
- 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 对等连接应用示例

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	使用示例
同区域VPC	• VPC网段：不同VPC网段不重叠 • 子网网段：不同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。	• **通过VPC对等连接实现多个VPC网络互通** • **通过VPC对等连接实现一个中心VPC与多个VPC之间网络互通** • 更多对等连接使用示例，请参见**指向整个VPC网段的对等连接配置**。
同区域VPC	• VPC网段：不同VPC网段重叠 • 子网网段：不同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。	• **通过VPC对等连接实现两个重叠网段VPC子网网络互通** • 更多对等连接使用示例，请参见**指向VPC子网的对等连接配置**。 • **通过VPC对等连接实现一个中心VPC的ECS与两个VPC的ECS对等** • 更多对等连接使用示例，请参见**指向VPC内ECS的对等连接配置**。

VPC位置	VPC网段	对等连接说明	使用示例
同区域VPC	• VPC网段：不同VPC网段重叠 • 子网网段：不同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 • 更多无效对等连接示例，请参见无效的VPC对等连接配置。

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。

通过 VPC 对等连接实现多个 VPC 网络互通

- 两个VPC网络互通：以图8-4为例，通过VPC对等连接，连通VPC-A和VPC-B之间的网络。

图 8-4 相互对等的两个 VPC(IPv4)

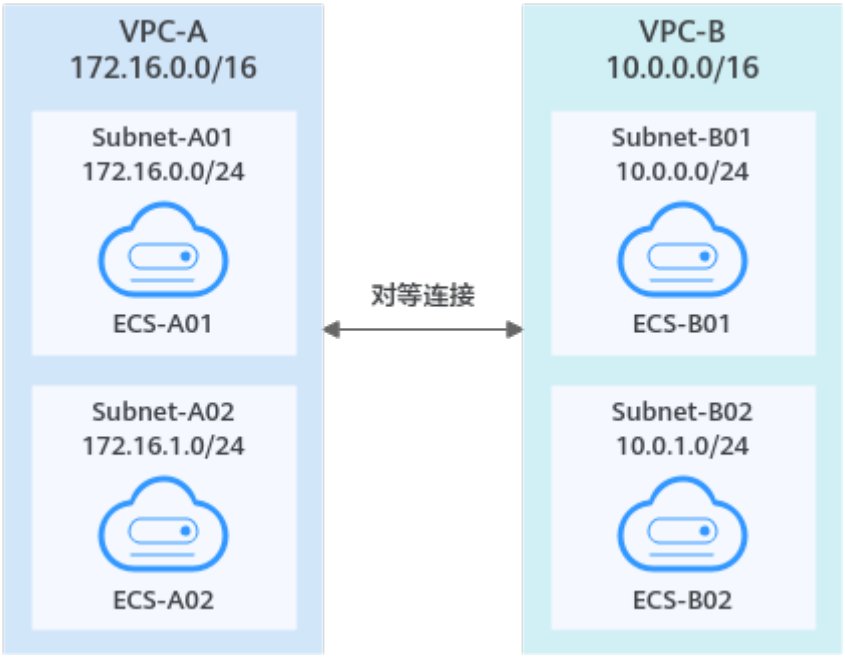


表 8-2 对等连接关系说明-相互对等的两个 VPC(IPv4)

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

表 8-3 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	10.0.0.0/16	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	172.16.0.0/16	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。

- 多个VPC网络互通：以图8-5为例，通过VPC对等连接，连通VPC-A、VPC-B和VPC-C之间的网络。

图 8-5 相互对等的多个 VPC(IPv4)

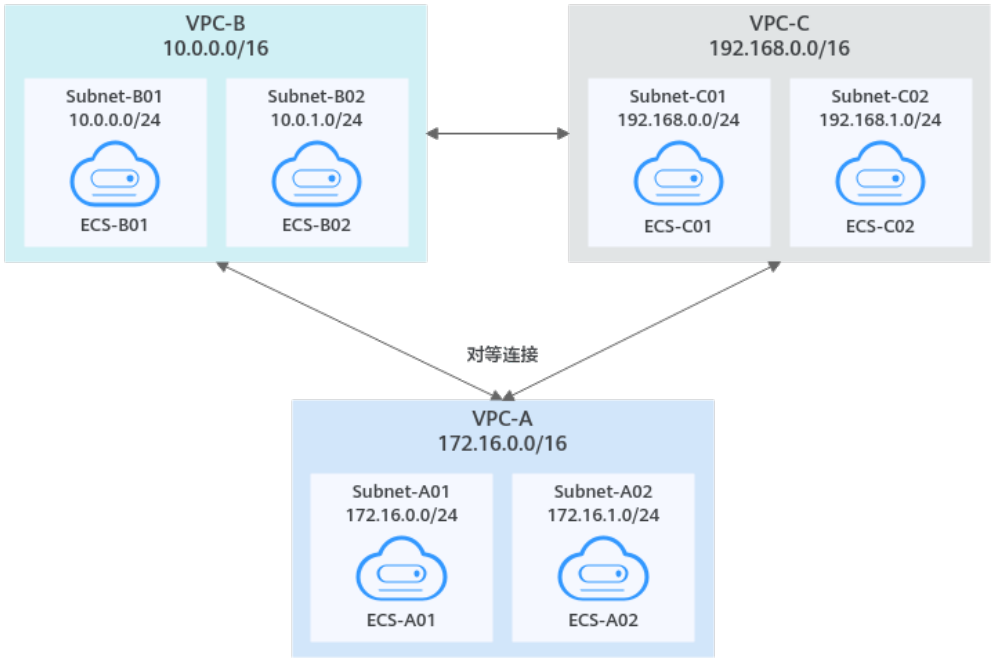


表 8-4 对等连接关系说明-相互对等的多个 VPC(IPv4)

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-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

表 8-5 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	10.0.0.0/16	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	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	172.16.0.0/16	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	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	172.16.0.0/16	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	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

如果您需要通信的VPC数量多，比如需要连通10个VPC，那么对等连接建立的组网会比较复杂，推荐您使用企业路由器服务。您可以将10个VPC接入企业路由器中，构建结构简单的中心辐射型组网，详细信息请参见**通过企业路由器实现同区域VPC互通**。

通过 VPC 对等连接实现一个中心 VPC 与多个 VPC 之间网络互通

以**图8-6**为例，通过VPC对等连接，实现VPC-B、VPC-C、VPC-D、VPC-E、VPC-F、VPC-G和中心VPC-A之间的网络通信。

图 8-6 一个中心 VPC 与多个 VPC 对等(IPv4)

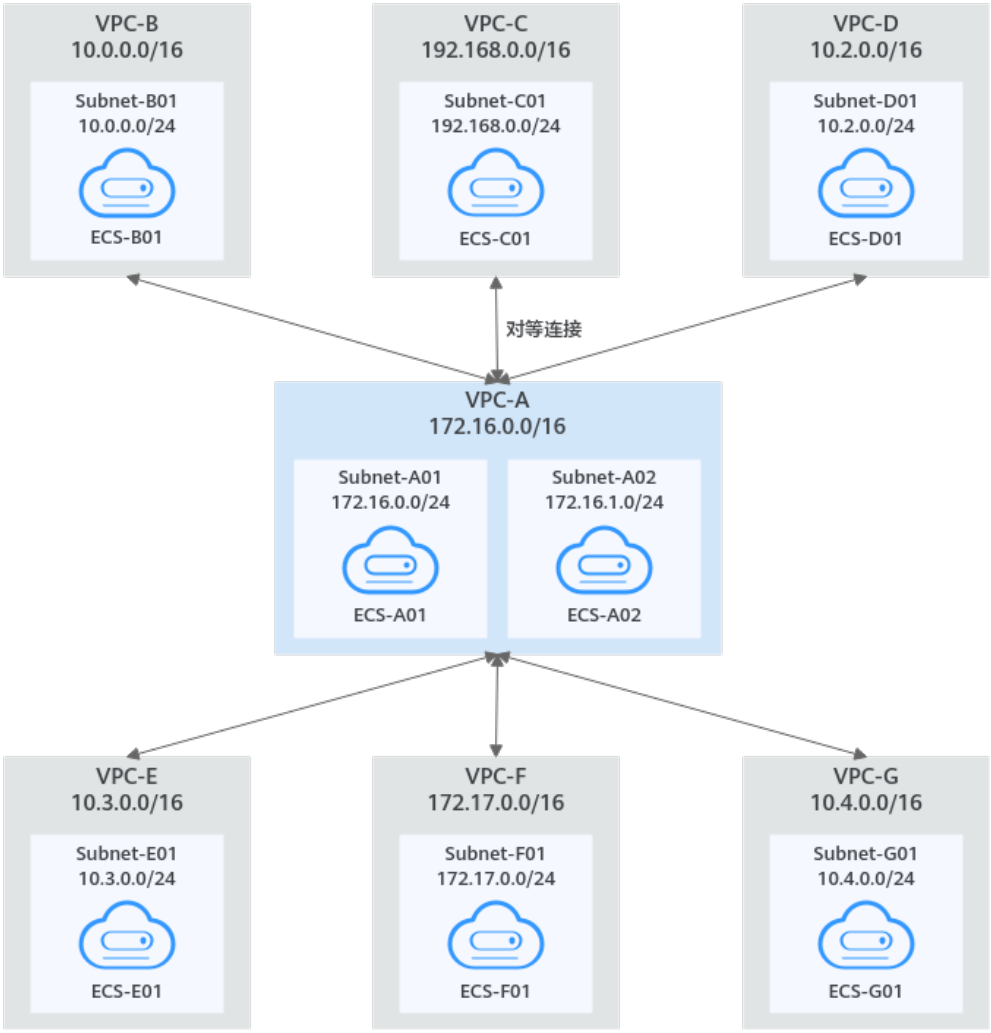


表 8-6 对等连接关系说明-一个中心 VPC 与多个 VPC 对等(IPv4)

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

表 8-7 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	10.0.0.0/16	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	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	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	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	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	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	172.16.0.0/16	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	172.16.0.0/16	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	172.16.0.0/16	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。
rtb-VPC-E	172.16.0.0/16	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	172.16.0.0/16	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	172.16.0.0/16	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。

通过 VPC 对等连接实现两个重叠网段 VPC 子网网络互通

以图8-7为例，由于VPC-A和VPC-B的网段重叠，并且Subnet-A01和Subnet-B01子网网段重叠，那么您无法通过对等连接实现整个VPC-A和VPC-B之间的网络通信。此种情况下，对等连接可以连通非重叠子网Subnet-A02和Subnet-B02之间的网络。

图 8-7 相互对等的两个重叠网段 VPC 子网(IPv4)

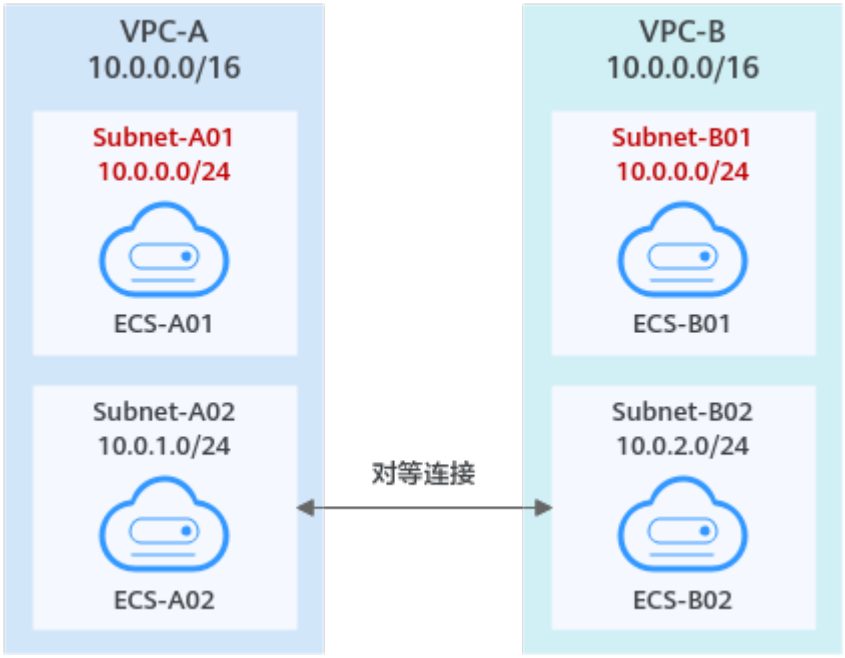


表 8-8 对等连接关系说明-相互对等的两个重叠网段 VPC 子网(IPv4)

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

表 8-9 VPC 路由表配置说明-相互对等的两个重叠网段 VPC 子网(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.2.0/24	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为Subnet-B02网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	10.0.1.0/24	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为Subnet-A02网段，下一跳指向Peering-AB的路由。

通过 VPC 对等连接实现一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等

以图8-8为例，由于VPC-B和VPC-C的网段重叠，并且Subnet-B01和Subnet-C01子网网段重叠，那么您无法同时创建VPC-A和VPC-B、VPC-A和VPC-C之间的对等连接。您可以创建ECS之间的对等连接：

- 通过对等连接Peering-AB可以连通子网Subnet-B01内的ECS和Subnet-A01内的ECS。
- 通过对等连接Peering-AC可以连通子网Subnet-C01内的ECS和Subnet-A01内的ECS。

图 8-8 一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

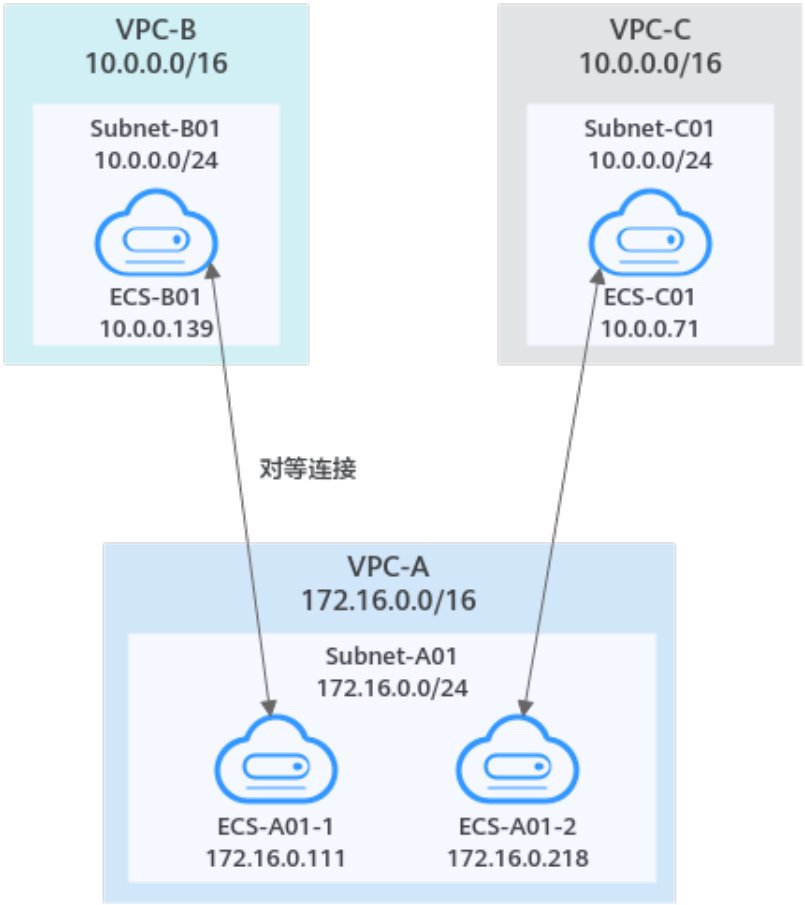


表 8-10 对等连接关系说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

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

表 8-11 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	10.0.0.139/32	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	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	172.16.0.111/32	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	172.16.0.218/32	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。

无效的 VPC 对等连接

当VPC网段重叠，且全部子网重叠时，不支持使用对等连接。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，那么路由表会由于目的地址重叠而导致流量传输错误。

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 8-9 VPC 网段重叠，且全部子网重叠(IPv4)

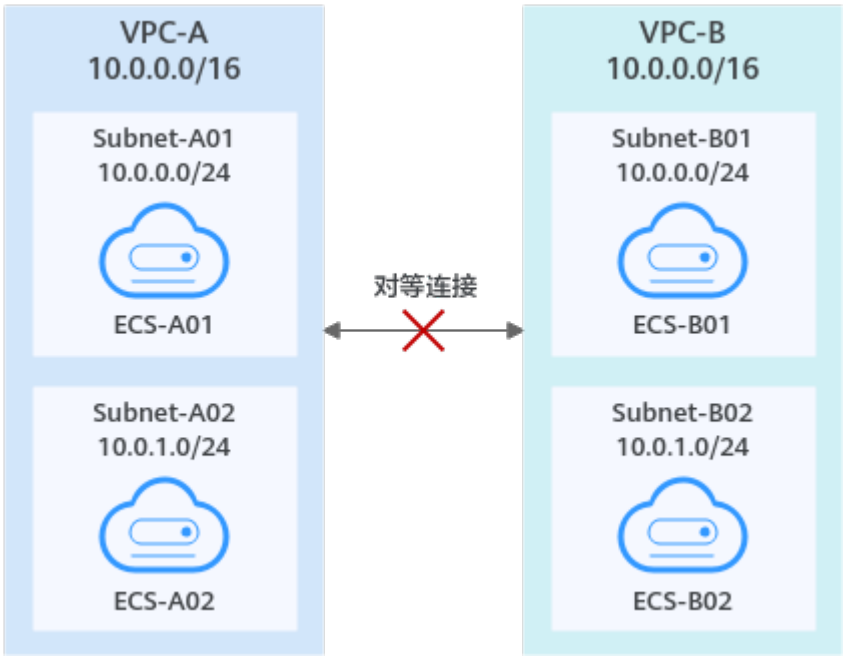


表 8-12 VPC 路由表配置说明-VPC 网段重叠，且全部子网重叠(IPv4)

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。

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。

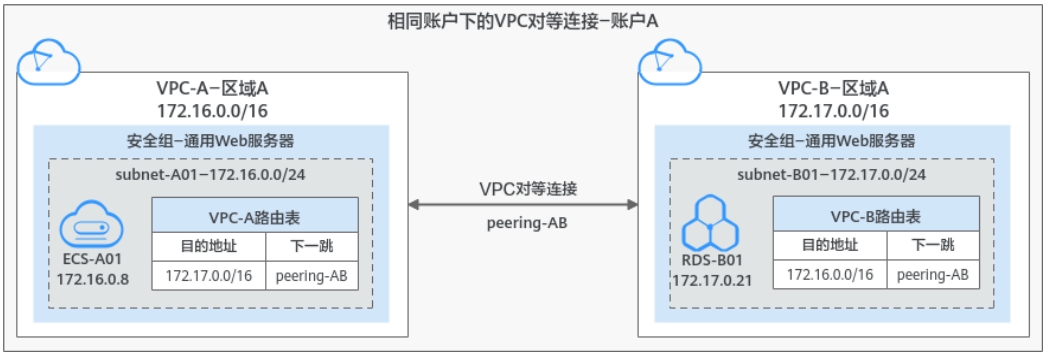
创建步骤如下：

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：验证网络互通情况

图 8-10 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，以下不同情况下的组网配置示例，请您参考**对等连接使用示例**。

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8-13**。

图 8-11 创建对等连接

表 8-13 创建对等连接-参数说明

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
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

参数	说明	取值样例
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**对等连接应用示例**。	172.17.0.0/16
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

4. 参数填写完成后，单击“确定”。
   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 8-12 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8-14所示。

表 8-14 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

参数	说明	取值样例
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**对等连接应用示例**。	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**对等连接应用示例**。	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）
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**对等连接应用示例**。	本示例为VPC-A的网段：172.16.0.0/16

参数	说明	取值样例
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，可以看到刚添加的路由。

步骤三：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和的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-A02 ~]# 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：

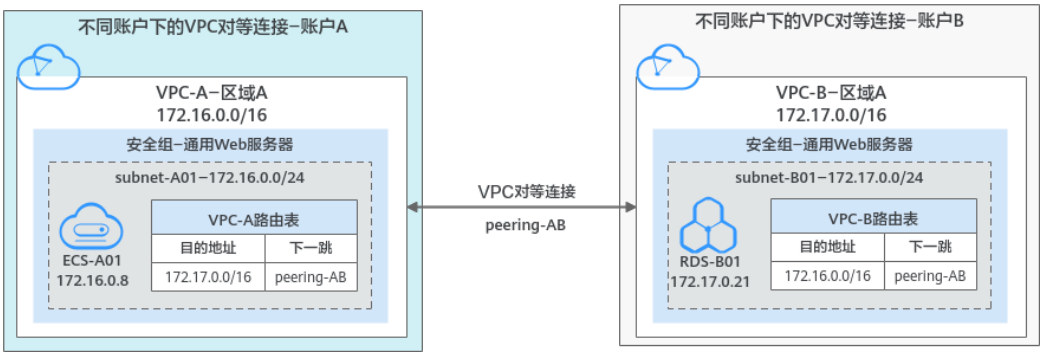
步骤一：创建VPC对等连接

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：验证网络互通情况

图 8-13 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，以下不同情况下的组网配置示例，请您参考**对等连接使用示例**。
- 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8-15**。

图 8-14 创建对等连接

表 8-15 创建对等连接-参数说明

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
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
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

4. 参数填写完成后，单击“确定”。
   - 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。

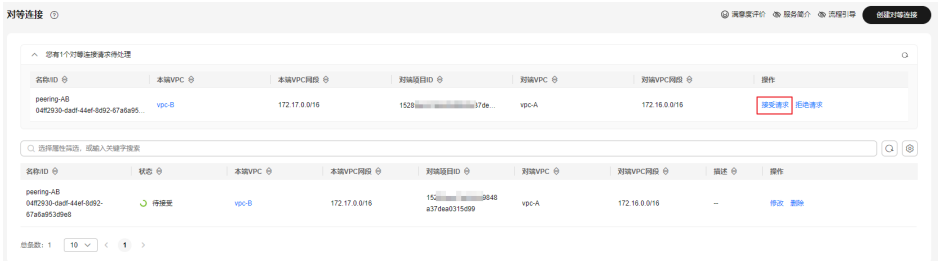
图 8-15 待接受对等连接

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 8-16 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**对等连接应用示例**。

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 8-17 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8-16**所示。

表 8-16 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）
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**对等连接应用示例**。	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

参数	说明	取值样例
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 8-18 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8-17所示。

表 8-17 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

参数	说明	取值样例
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**对等连接应用示例**。	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，可以看到刚添加的路由。

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和的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-A02 ~]# 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 8-19 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 8-20 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“是”，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

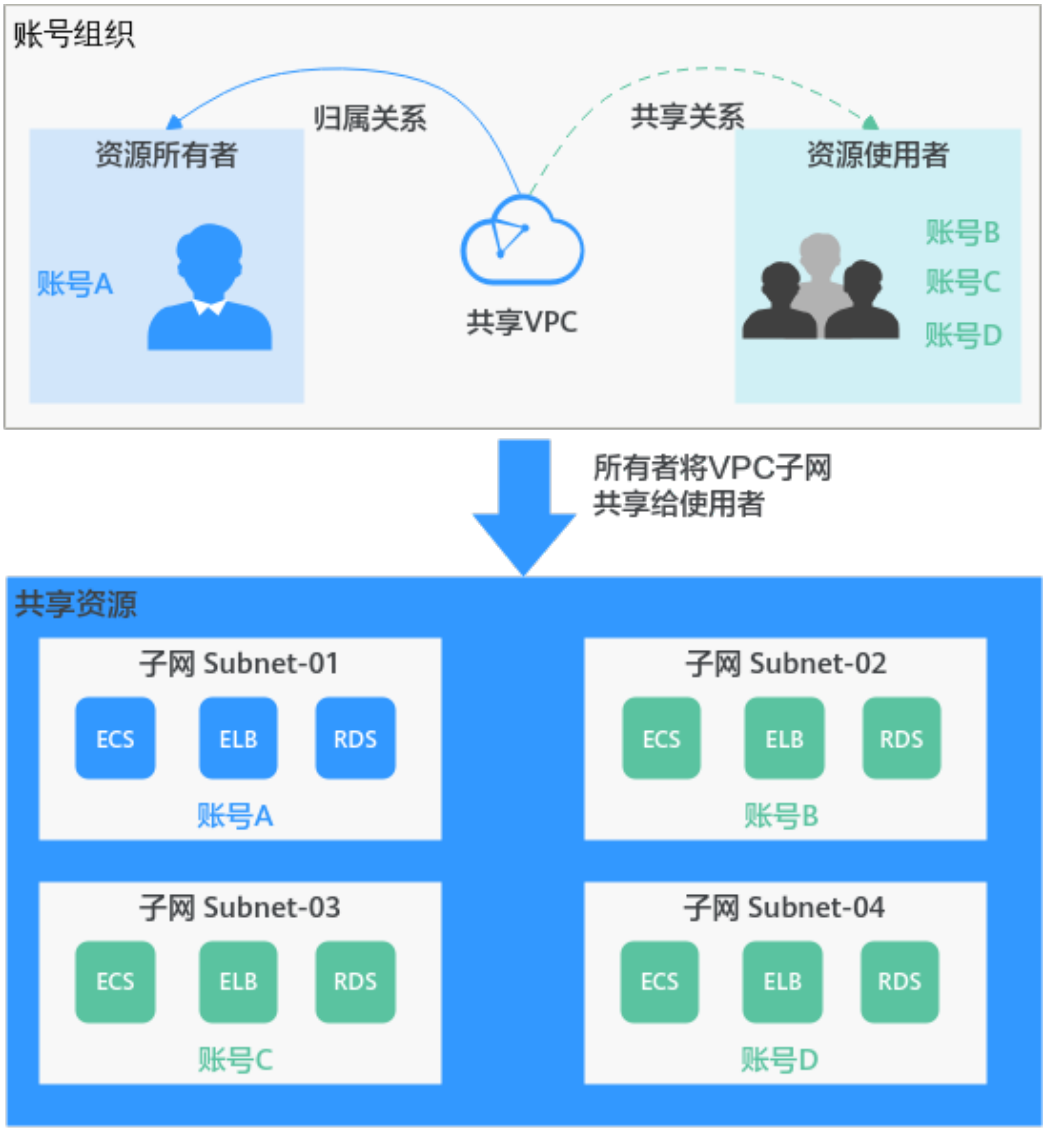
共享VPC功能支持多个账号在一个集中管理、共享的VPC内创建云资源，比如ECS、ELB、RDS等。共享VPC基于资源访问管理（Resource Access Manager，简称RAM）服务的机制，VPC的所有者可以将VPC内的子网共享给一个或者多个账号使用。通过共享VPC功能，可以简化网络配置，帮助您统一配置和运维多个账号下的资源，有助于提升资源的管控效率，降低运维成本。

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。

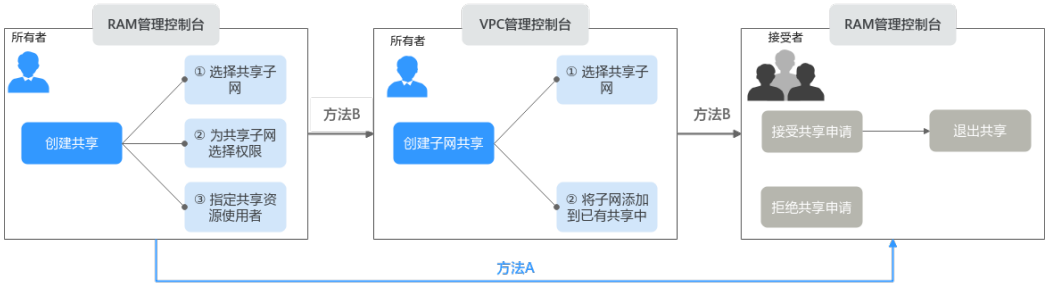
  比如不同账号下的VPC网络互通需要建立对等连接，使用共享VPC后，则不同账号用户可以在同一个VPC创建资源，免去了对等连接配置，有效的简化组网结构。
- 在一个账号内统一管理运维资源，便于企业集中配置业务安全策略，并且利于对资源使用情况的监控和审计，支撑业务的安全诉求。

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9-3**中详细为您介绍方法A和方法B。

表 9-1 共享子网创建流程说明

方法	说明	操作指导
方法A	1. 通过RAM管理控制台，所有者创建共享，将子网共享给使用者。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。 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. **创建共享** 2. **接受/拒绝共享邀请** **退出共享**
方法B	1. 通过RAM管理控制台，所有者创建共享，将子网共享给使用者。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。 2. 通过VPC管理控制台，所有者创建子网共享，将子网添加至**1**中已创建的共享中即可。 3. 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. **创建共享** 2. **将VPC子网共享给其他账号** 3. **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
  - 云数据库 GaussDB
  - 云数据库 GaussDB(for MySQL)
  - 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

9.2 共享 VPC 应用示例

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

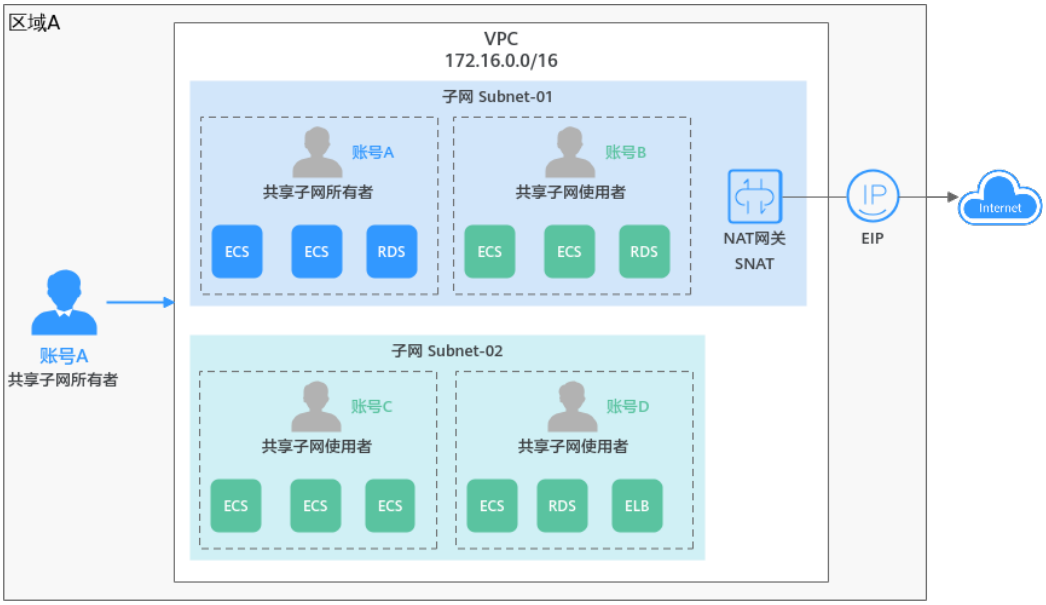


表 9-5 共享 VPC 业务规划说明

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**，创建子网共享。
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”，表示子网共享创建完成。

后续操作

共享子网创建完成后，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 IPv6 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10-1所示。

图 10-1 IPv6 双栈网络架构图(VPC/EIP)

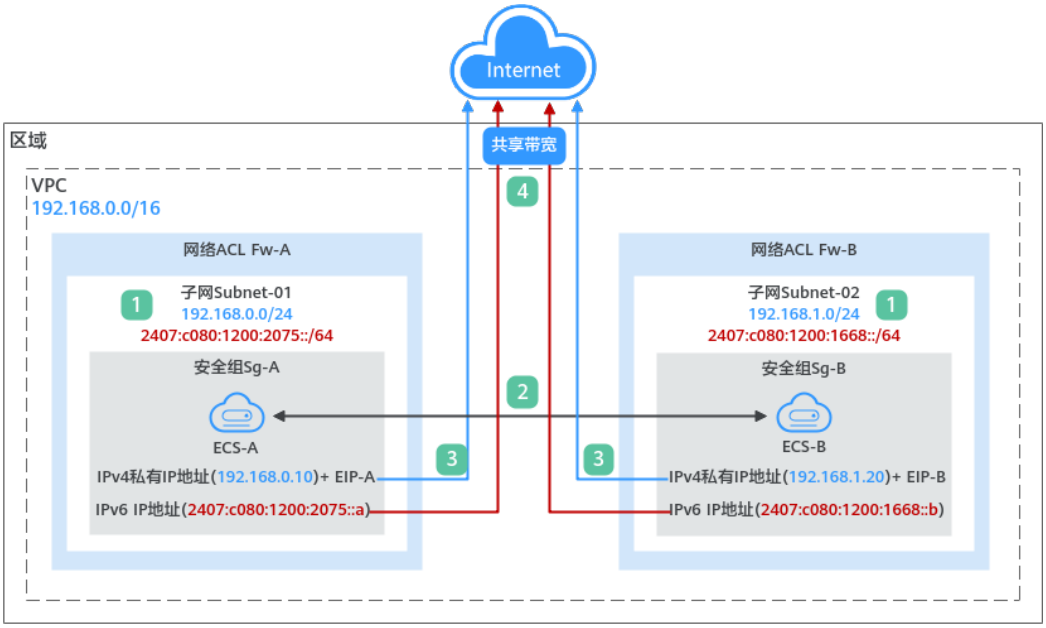


表 10-1 IPv6 双栈网络构建说明(VPC/EIP)

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。
- 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，请务必选择支持的区域和规格。

  您可以通过以下方法查看ECS哪些规格支持IPv6：
  - 通过ECS控制台查看：单击“创建弹性云服务器”，进入创建页面查看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。
  - 通过ECS文档查看IPv6是否支持。

    以通用计算增强型ECS为例，需要通过ECS文档查看通用计算增强型ECS支持IPv6的规格，步骤如下：

    i. 打开《 ECS产品介绍 》中的**ECS规格清单**页面。

    ii. 在“通用计算增强型”小结，单击“各规格详细介绍请参见通用计算增强型”中的超链接。

    图 10-2 ECS 规格清单页面

iii. 进入“通用计算增强型”章节，在表格“通用计算增强型实例特点”的“网络”列中，查看支持IPv6的规格。

图 10-3 ECS 通用计算增强型

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10-2所示。

表 10-2 IPv4/IPv6 双栈网络的应用场景及资源规划

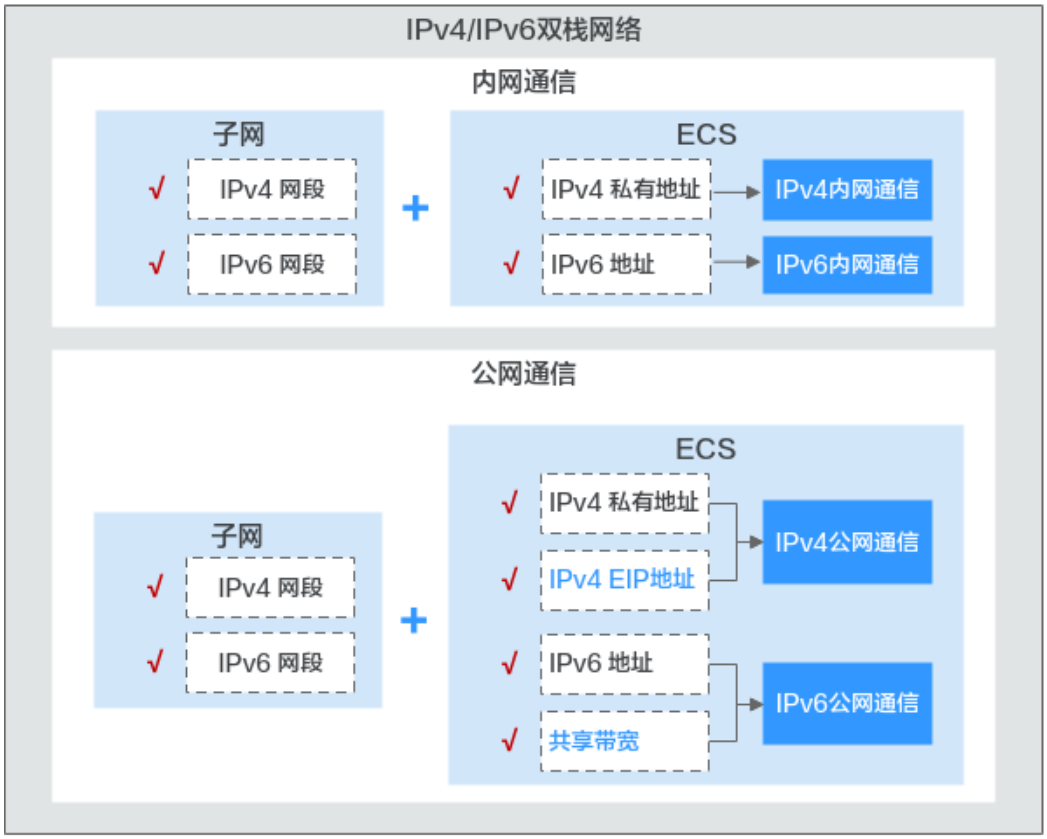
应用场景	场景说明	子网	ECS
IPv6内网通信	您在ECS上部署应用，需要与其他系统（比如数据库）之间使用IPV6进行内网互访	• IPv4网段 • IPv6网段	• IPv4私有地址：用于IPv4内网通信 • IPv6地址：用于IPv6内网通信
IPv6公网通信	您在ECS上部署应用并面向公网客户端提供服务，支持客户端通过IPv6地址访问	• IPv4网段 • IPv6网段	• IPv4私有地址+IPv4 EIP地址：用于IPv4公网通信 • IPv6地址+共享带宽：用于IPv6公网通信
	您在ECS上部署应用并面向公网客户端提供服务，既要支持客户端通过IPv6地址访问，还要对这些访问来源进行数据分析		

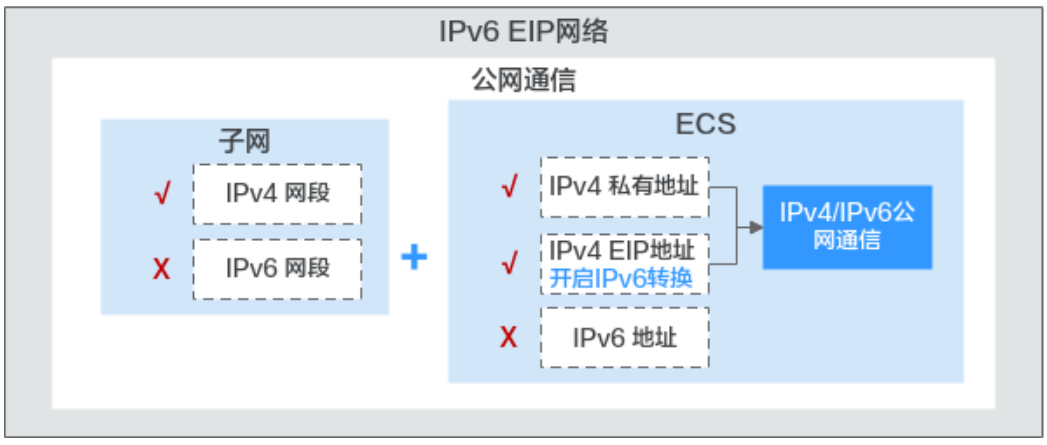
如果您的ECS规格不支持IPv6，您可以通过开启EIP的IPv6转换功能，实现IPv6公网通信，具体如表10-3所示。

表 10-3 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 10-4 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10-4**中为您提供IPv6网络配置指导。

表 10-4 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（默认生效顺序）**
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。	**管理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，你可以将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**

11 VPC 流日志

11.1 VPC 流日志概述

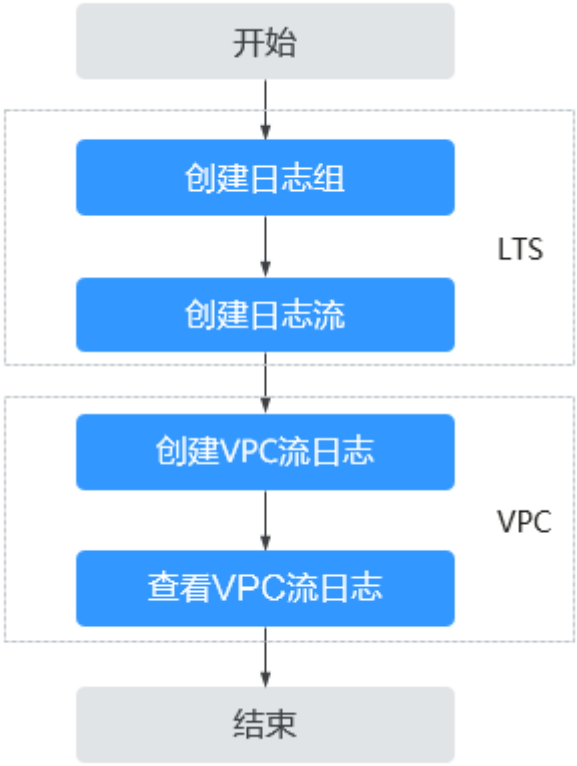
流日志

VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

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流日志功能需要与云日志服务LTS结合使用，先在云日志服务中创建日志组和日志流，然后再创建VPC流日志。配置流程如**图11-1**所示。

图 11-1 配置 VPC 流日志



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、P1、G3、Pi1、H3。

  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。

11.2 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VPC流日志”，按照提示配置参数。

表 11-1 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，目前支持网卡、子网、虚拟私有云类型。	网卡
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“确定”。

返回VPC流日志列表，可以看到刚创建的VPC流日志。

11.3 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. 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“VPC流日志”。
   进入VPC流日志列表页面。
5. 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>
   ```

   示例1：在捕获窗口中正常记录数据的流日志记录

   ```
   1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154 192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
   ```

   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。

   示例2：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
   ```

   示例3：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
   ```

   字段含义如**表11-2**所示：

表 11-2 日志字段说明

字段	说明	示例
version	VPC流日志版本。	1
project-id	项目ID。	5f67944957444bd6bb4fe3b367de8f3d
interface-id	为其记录流量的网卡的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

字段	说明	示例
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

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。

11.4 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. 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“VPC流日志”。
   进入VPC流日志列表页面。
5. 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。
6. 信息确认无误后，单击“确定”，开启或关闭VPC流日志。

11.5 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. 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“VPC流日志”。
   进入VPC流日志列表页面。
5. 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。
6. 信息确认无误后，单击“确定”，删除流日志。

12 流量镜像

12.1 流量镜像概述

流量镜像

VPC流量镜像功能可以镜像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，经过弹性网卡的流量符合筛选条件时，将被镜像到指定的云服务器网卡或者弹性负载均衡ELB实例，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12-1**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12-1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 12-1 流量镜像架构图

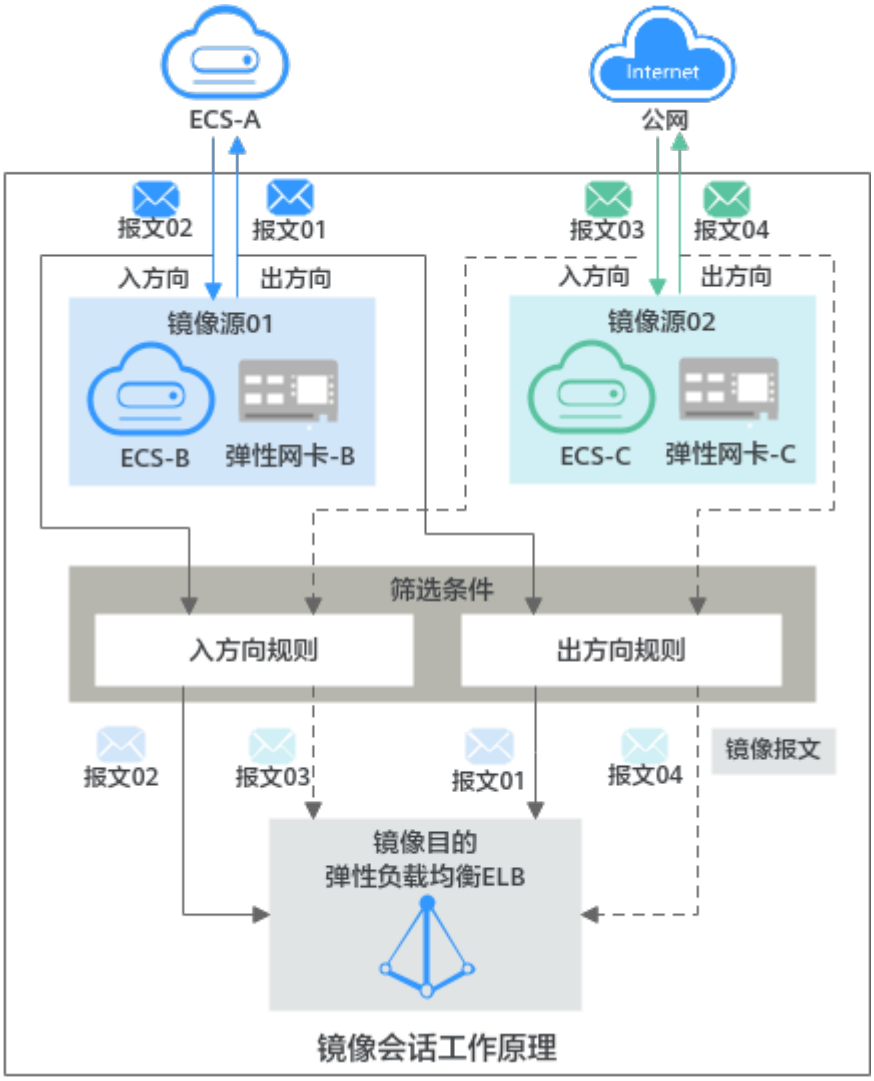


表 12-1 网络流量的镜像路径说明

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12-2**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 12-2 流量筛选说明

方向	优先级	协议类型	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。

方向	优先级	协议类型	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
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：

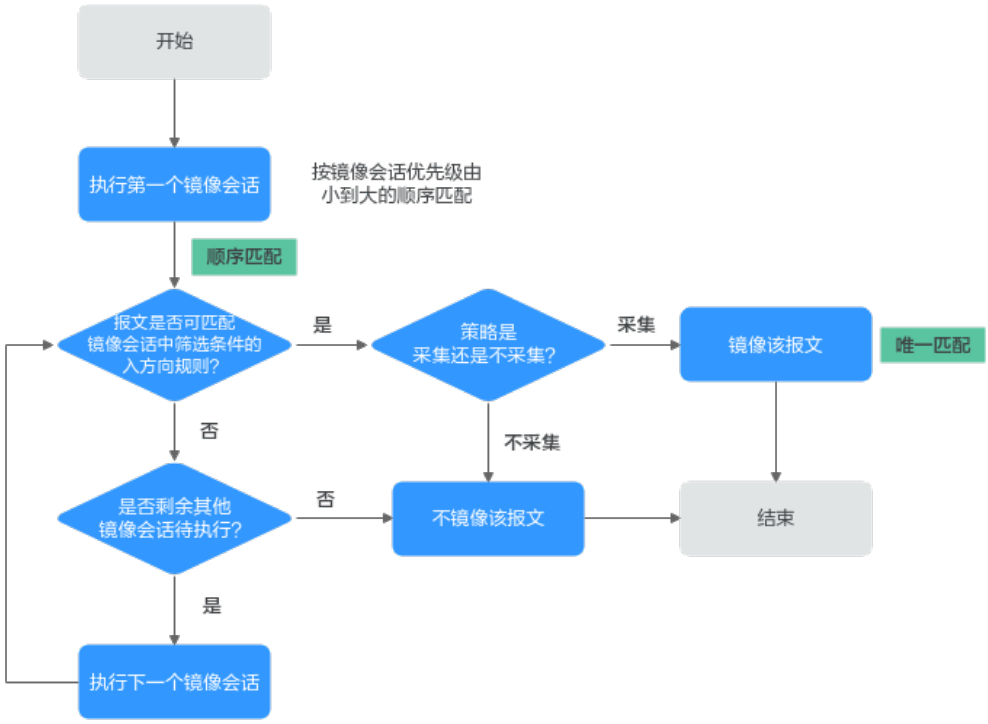
表 12-3 流量镜像匹配规则

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12-2**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。

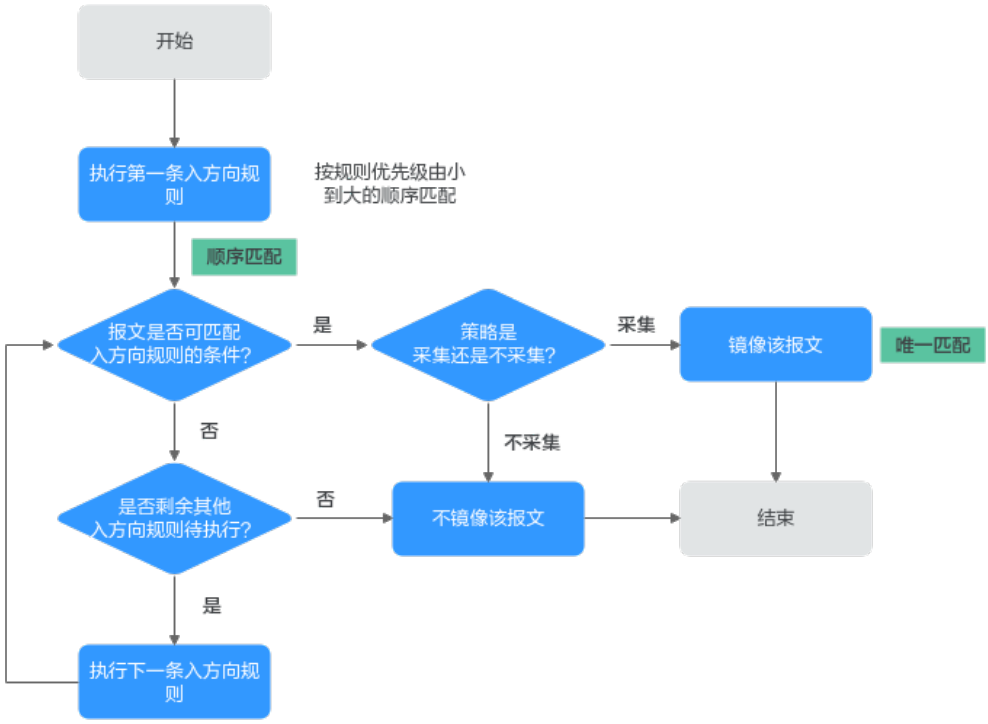
图 12-2 镜像会话匹配规则



- 筛选条件的匹配规则如图12-3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 12-3 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12-4**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 12-4 流量镜像的配额说明

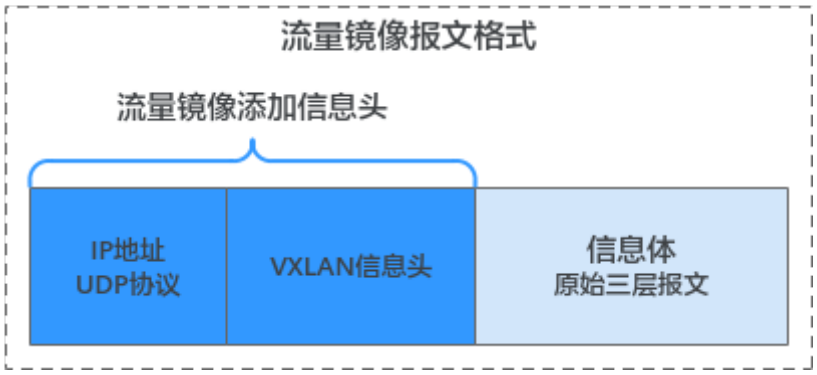
配额项目	默认配额	申请扩大配额
单个镜像会话可关联的镜像源数量	10个	申请更多配额，请参见**申请扩大配额**
单个镜像源可被关联的镜像会话数量	3个	不支持修改
单个镜像会话可关联的镜像目的数量	1个	不支持修改
单个镜像目的可被关联的镜像会话数量	• 镜像目的为云服务器网卡时：10个 • 镜像目的为弹性负载均衡时：200个	不支持修改
单个镜像会话可关联的筛选条件数量	1个	不支持修改
单个筛选条件可被关联的镜像会话数量	1000个	不支持修改

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12-4所示，流量镜像的报文采用标准的VXLAN报文格式封装，更多有关VXLAN协议的信息，请参见RFC 7348。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 12-4 流量镜像报文格式

- 当前流量镜像仅支持c7t规格云服务器的弹性网卡作为镜像源。
- 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。
- 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云服务器的规格。
- 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：入方向允许来自镜像源弹性网卡的IP访问4789端口的UDP协议报文。假如镜像源弹性网卡的IP地址为192.168.0.27，则安全组规则配置示例如表12-5所示，具体方法请参见添加安全组规则。

表 12-5 安全组规则配置示例

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：入方向允许来自镜像源弹性网卡的IP访问所有端口的UDP协议报文。假如镜像源弹性网卡的IP地址为192.168.0.27，则网络ACL规则配置示例如**表12-6**所示，具体方法请参见**添加网络ACL规则（默认生效顺序）**。

表 12-6 网络 ACL 规则配置示例

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。	IP地址：10.10.0.0/24 此处仅为示例，请根据实际情况配置。	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12-5**所示。

图 12-5 流量镜像使用流程

表 12-7 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**

步骤	说明	操作指导
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。 • 当前流量镜像仅支持c7t规格云服务器的弹性网卡作为镜像源。	
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**。	

12.2 筛选条件

12.2.1 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12-8**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 12-8 流量筛选说明

方向	优先级	协议类型	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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 根据界面提示，设置筛选条件基本信息。

表 12-9 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。	-

7. 单击入方向规则区域的“添加规则”，添加入方向规则。
   单击“+”按钮，可以依次增加多条入方向规则。

表 12-10 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
协议类型	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
IP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。	-

8. 入方向规则设置完成后，单击“确定”，保存设置。
9. 单击出方向规则区域的“添加规则”，添加出方向规则。
   单击“+”按钮，可以依次增加多条出方向规则。

表 12-11 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
协议类型	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
IP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。	-

10. 出方向规则设置完成后，单击“确定”，保存设置。
11. 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**。

12.2.2 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12-12**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 12-12 流量筛选说明

方向	优先级	协议类型	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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 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“+”按钮，可以依次增加多条入方向规则。

表 12-13 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
协议类型	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
IP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。	-

7. 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。

8. 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“+”按钮，可以依次增加多条出方向规则。

表 12-14 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
协议类型	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
IP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。	-

9. 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。

12.2.3 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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 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 12-15 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

参数	说明	取值样例
协议类型	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
IP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

参数	说明	取值样例
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。	-

7. 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。
8. 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 12-16 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

参数	说明	取值样例
协议类型	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
IP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

参数	说明	取值样例
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。	-

9. 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。

12.2.4 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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 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。

7. 确认无误后，单击“是”，删除入方向规则。
   入方向规则删除后无法恢复，请谨慎操作。
8. 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。
9. 确认无误后，单击“是”，删除出方向规则。
   出方向规则删除后无法恢复，请谨慎操作。

12.2.5 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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 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 12-17 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。	-

12.2.6 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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 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。

12.2.7 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. 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“流量镜像 > 筛选条件”。
   进入筛选条件列表页面。
5. 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。
6. 确认无误后，单击“是”，删除筛选条件。
   筛选条件删除后无法恢复，请谨慎操作。

12.3 镜像会话

12.3.1 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. 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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 根据界面提示，设置镜像会话基本信息。

表 12-18 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。	-

7. 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。
8. 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**。

9. 筛选条件关联完成后，单击“下一步”。

   进入“关联镜像源”页面。

10. 在镜像源列表中，选择镜像源。
    - 镜像源为弹性网卡，表示需要镜像该弹性网卡的流量。
    - 一个镜像会话可以关联多个镜像源。
    - 弹性网卡需要绑定至云服务器，当前流量镜像仅支持c7t规格云服务器的弹性网卡作为镜像源。

11. 镜像源关联完成后，单击“下一步”。

    进入“关联镜像目的”页面。

12. 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。

13. 镜像目的关联完成后，单击“下一步”。

    进入“确认配置”页面。

14. 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。

12.3.2 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. 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“流量镜像 > 镜像会话”。

   进入镜像会话列表页面。

5. 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。

6. 确认无误后，单击“是”，开启或者关闭镜像会话。

12.3.3 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。

- 镜像源为弹性网卡，表示需要镜像该弹性网卡的流量。
- 一个镜像会话可以关联多个镜像源。
- 弹性网卡需要绑定至云服务器，当前流量镜像仅支持c7t规格云服务器的弹性网卡作为镜像源。

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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 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。
7. 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。

12.3.4 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. 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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 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。

7. 确认无误后，单击“是”，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。

12.3.5 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. 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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 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**。

12.3.6 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。

- 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。

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“流量镜像 > 镜像会话”。

进入镜像会话列表页面。

5. 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。

6. 在镜像目的列表中，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。

12.3.7 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、优先级以及描述等信息。

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“流量镜像 > 镜像会话”。

   进入镜像会话列表页面。

5. 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。

6. 根据界面提示信息修改参数。

表 12-19 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

参数名称	参数说明	取值样例
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。	-

7. 参数修改完成后，单击“确定”，保存修改。

12.3.8 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，即弹性网卡的私有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. 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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 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。
7. 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：查看弹性网卡的私有IP地址、已绑定实例以及安全组等。

12.3.9 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. 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“流量镜像 > 镜像会话”。
   进入镜像会话列表页面。
5. 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。
6. 确认无误后，单击“是”，删除镜像会话。
   镜像会话删除后无法恢复，请谨慎操作。

13 弹性公网 IP

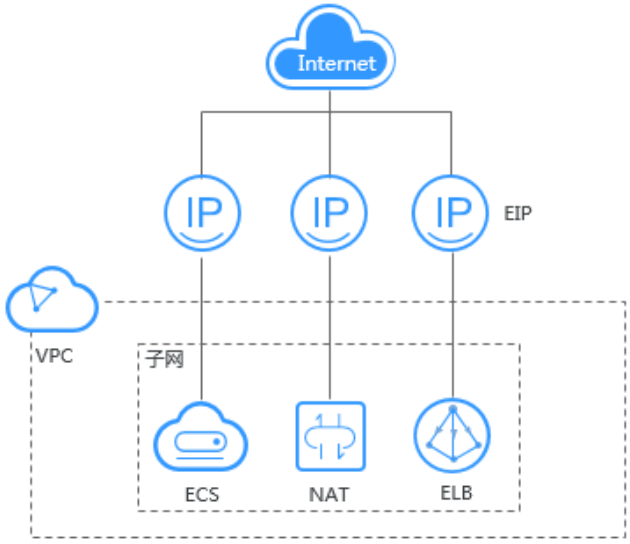
13.1 弹性公网 IP 概述

弹性公网 IP

弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。

一个弹性公网IP只能绑定一个云资源，且弹性公网IP和云资源必须位于同一个区域。

图 13-1 通过 EIP 访问公网



须知

如您违反适用法律法规的要求使用华为云EIP资源，华为云有权收回EIP资源，并暂停向您提供服务。

弹性公网 IP 的配额限制

了解一个用户在单个区域内可申请的EIP数量，请参考**怎样查看我的配额？**，登录控制台查询您的配额详情。

如果您需要提升配额，请参见**如何申请扩大配额？**。

- 提升配额时，要求当前账户下存在有效订单和持续使用的云服务资源，如您的账户之前存在多次订购资源后即时释放的情况，拒绝提升配额。
- 对于长期闲置的EIP资源配额，华为云将降低配额至默认值。

弹性公网 IP 的优势

- 弹性灵活

  EIP支持与ECS、BMS、NAT网关、ELB、虚拟IP灵活的绑定与解绑，带宽支持灵活调整，应对各种业务变化。
- 多种计费模式

  多种计费策略，支持按需计费（按带宽计费）、按需计费（按流量计费），包年包月价格更优惠 。
- 共享带宽

  EIP可以加入共享带宽，降低带宽使用成本。
- 即开即用

  即开即用，绑定解绑、带宽调整实时生效。

弹性公网 IP 的使用限制

- 通用可用区的EIP不支持绑定至边缘可用区的实例，边缘可用区的EIP也不支持绑定至通用可用区的实例。

  说明

  关于边缘可用区和普通可用区的区别请参考**《智能边缘小站用户指南》**。
- 弹性公网IP与云资源属于不同的资源，弹性公网IP的计费方式和云资源不同的情况下，不影响绑定。

  比如，包年/包月的弹性公网IP可以绑定给按需计费的弹性云服务器使用。
- 当带宽严重超限或受到攻击时（一般是受到了DDoS攻击），EIP会被封堵，但不影响对EIP资源执行绑定、解绑等操作。
- 不支持将跨账号转移弹性公网IP，即账号A下的弹性公网IP无法转移给账号B使用。

13.2 为 ECS 申请和绑定 EIP

操作场景

如果您需要公网访问、高可用性和负载均衡等功能，或者考虑安全性问题，您可以申请并绑定弹性公网IP地址到弹性云服务器实例上，以实现对弹性云服务器实例的公网访问能力及其他需求。

约束与限制

- 一个弹性公网IP只能绑定一个云资源，且弹性公网IP和云资源必须位于同一个区域。
- 通用可用区的EIP不支持绑定至边缘可用区的实例，边缘可用区的EIP也不支持绑定至通用可用区的实例。

  说明

  关于边缘可用区和普通可用区的区别请参考**《智能边缘小站用户指南》**。
- 资源欠费被冻结的EIP，或绑定的服务器对外有攻击行为等安全原因被冻结的EIP，无法进行绑定、解绑等操作。

申请弹性公网 IP

1. 进入**购买弹性公网IP**页面。
2. 根据界面提示配置参数。

图 13-2 购买 EIP

表 13-1 参数说明

参数	说明	取值样例
计费模式	计费模式分为以下两种： • 包年/包月 • 按需计费	按需计费

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。购买EIP时所选择的区域即为EIP的归属地。 **说明** 在“华北-乌兰察布一”区域购买的EIP的归属地为北京。	华东-上海一
线路	• 全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。 • 静态BGP：网络结构发生变化时，无法实时自动调整网络设置以保障用户体验。 • 优选BGP：是特定方向的优质线路。使用BGP协议与多家主流运营商线路互联对接，建立直连中国内地的公网互联路径，提供中国-香港区域与中国内地间的低时延、高质量的网络互通。（该线路资源仅在“中国-香港”区域支持。） • 边缘线路：计费模式为按需计费并且已购买边缘小站时，该项可见。边缘线路是通过靠近用户和终端的网络边缘站点，实现区域内低时延高带宽的网络服务。边缘小站详细信息请参见 **智能边缘小站**。 • 公网IP池：计费模式为按需计费时，该项可见。公网IP池是一种批量EIP开通到管理的专属解决方案。公网IP池为EIP分配全动态BGP线路，持续保证网络稳定、高效。公网IP池详细信息请参见**公网IP池简介**。 更多静态BGP与全动态BGP区别信息请参见**静态BGP与全动态BGP有何区别?**	全动态BGP
公网IP池	选择已购买的公网IP池。 仅当EIP的计费模式为按需计费，线路为公网IP池时，该项可见。	eipPool-test

参数	说明	取值样例
公网带宽	选择按需计费时，需要选择公网带宽的计费方式。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。适用于流量较大或较稳定场景使用。 • 按流量计费：指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。适用于流量小或流量波动较大的场景。 • 加入共享带宽：带宽可以加入多个弹性公网IP，带宽被多个弹性公网IP地址共用。适用于多业务流量错峰分布场景。	按带宽计费
带宽大小	带宽大小，单位Mbit/s。	100
IPv6转换	开启IPv6转换后，将提供IPv4和IPv6弹性公网IP地址，原有IPv4业务可以快速为IPv6用户提供访问能力。	开启
DDos防护	DDoS原生基础防护 免费提供不高于5Gbps的DDoS攻击防护，如超过防护阈值，EIP会被封堵。	-
弹性公网IP名称	弹性公网IP的名称。	eip-test
企业项目	申请弹性公网IP时，可以将弹性公网IP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
高级配置	单击下拉箭头，可配置弹性公网IP的高级参数，包括带宽名称、标签等。	-
带宽名称	带宽的名称。	bandwidth

参数	说明	取值样例
标签	用于标识弹性公网IP地址。包括键和值。 标签的命名规则请参考**表13-2**。 **说明** 如您的组织已经设定弹性公网IP的相关标签策略，则需按照标签策略规则为弹性公网IP添加标签。标签如果不符合标签策略的规则，则可能会导致弹性公网IP创建失败，请联系组织管理员了解标签策略详情。	• 键：Ipv4_key1 • 值：3005eip
监控	用于开启弹性公网IP的基础监控。默认开启。 开启基础监控后，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。	-
购买时长	选择包年包月计费模式时，需要选择购买时长。	1个月
自动续费	选择包年包月计费模式时，可以选择开启自动续费。自动续费周期根据用户指定的购买时长确定。 • 按月购买：自动续费周期为一个月。 • 按年购买：自动续费周期为一年。	-
购买量	弹性公网IP数量。 仅在按需计费时可以选择弹性公网IP数量。	1

表 13-2 弹性公网 IP 地址标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一弹性公网IP键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	Ipv4_key1
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	eip-01

说明

- 对于按需计费的弹性公网IP，当带宽类型选择“共享带宽”时，只能在“带宽名称”的下拉选项中选择已有的共享带宽加入。如果带宽名称不可选，说明您没有可用共享带宽，请先创建。
- 独享带宽与共享带宽不支持直接互相转换，但针对按需计费的弹性公网IP，您可以购买一个共享带宽，进行如下操作：
  - 将弹性公网IP添加到共享带宽，则弹性公网IP使用共享带宽。
  - 将弹性公网IP移出共享带宽，则弹性公网IP使用独享带宽。

3. 单击“立即购买”。

说明

- 当您创建资源时配额为0，不支持创建，如需更多配额请申请扩大配额，具体请参见**如何申请扩大配额？**。
- 当您批量创建资源时配额不足，系统会出现信息提示页面，提示所需资源配额不足，并列出参数信息“资源类型”、“所需配额”和“剩余配额”，您可以根据需要选择“申请扩大配额”或者“取消”。

4. 在产品配置信息确认页面，再次核对弹性公网IP信息，阅读并勾选“弹性公网IP服务声明”。
   - 选择按需计费的弹性公网IP时，单击“提交”。
   - 选择包年/包月计费的弹性公网IP时，单击“去支付”。

     进入订单支付页面，确认订单信息，单击“确认付款”。

绑定弹性公网 IP

1. 在“弹性公网IP”界面待绑定弹性公网IP地址所在行，单击“绑定”。
2. 选择实例。

   可绑定EIP的实例包括云服务器、裸金属服务器、虚拟IP、辅助弹性网卡等。
3. 单击“确定”。

说明

- 弹性公网IP与云资源属于不同的资源，弹性公网IP的计费方式和云资源不同的情况下，不影响绑定。

  比如，包年/包月的弹性公网IP可以绑定给按需计费的弹性云服务器使用。
- 绑定的ECS实例应满足以下条件
  - ECS实例必须处于运行中或已停止状态。
  - ECS实例的地域必须和要绑定的EIP的地域相同。
  - ECS实例没有绑定其他EIP。

相关操作

- **如何创建或找回指定的弹性公网IP？**
- **弹性公网IP绑定弹性云服务器后如何由外部进行访问？**
- **弹性公网IP是否支持变更绑定的弹性云服务器？**
- **如何排查带宽超过限制？**
- **EIP连接出现问题时，如何排查？**

13.3 解绑定和释放 ECS 的 EIP

操作场景

当弹性云服务器无需继续使用弹性公网IP，可通过解绑定和释放弹性公网IP来释放网络资源。

按需计费的弹性公网IP费用包括“弹性公网IP保有费”和“带宽费用”：

- 当与实例解绑且未释放时，您需要支付“弹性公网IP保有费”和“带宽费用”。
- 当绑定至实例时，则免除“弹性公网IP保有费”，您只需要支付“带宽费用”。

约束与限制

- 未绑定任何实例的弹性公网IP才可释放，已绑定实例的需要先从实例解绑，然后释放。
- 弹性公网IP释放后，如果被其他用户使用，则无法找回。
- 资源欠费被冻结的EIP，或绑定的服务器对外有攻击行为等安全原因被冻结的EIP，无法进行绑定、解绑等操作。

操作步骤

解绑单个弹性公网IP

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 > 弹性公网IP”
4. 在“弹性公网IP”界面待解绑定弹性公网IP地址所在行，单击“解绑”。
5. 单击“是”。

释放单个弹性公网IP

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 > 弹性公网IP”
4. 在“弹性公网IP”界面待释放弹性公网IP地址所在行，单击“更多 > 释放”。
5. 单击“是”。

批量解绑弹性公网IP

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 > 弹性公网IP”
4. 在弹性公网IP列表中勾选待解绑定的多个弹性公网IP地址。
5. 单击列表左上方的“解绑”。

6. 单击“是”。

批量释放弹性公网IP

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 > 弹性公网IP”
4. 在“弹性公网IP”列表中勾选多个待释放弹性公网IP。
5. 单击列表上方的“释放”。
6. 单击“是”。

13.4 修改 EIP 的带宽配置

操作场景

当您购买弹性公网IP时，无论是哪种计费模式，只要没有加入共享带宽，那么您的弹性公网IP使用的是独享带宽。独享带宽支持对单个弹性公网IP进行限速。

本章节指导用户修改独享带宽大小，您可以增加或者降低带宽大小，修改带宽大小不会更换EIP的地址。

当您修改带宽大小时，不同计费方式的带宽收费和生效时间不同，请您参考**表13-3**了解详情，适用于独享带宽和共享带宽两种情况。

说明

降低带宽大小，可能会影响业务流量造成丢包，请确认对业务产生的影响，谨慎操作。

表 13-3 修改带宽大小的费用情况

计费模式	计费方式	变更操作	对费用的影响
包年/包月	按带宽计费	增加带宽大小（补差价升配）	升配后，新带宽大小将在原来已有的计费周期内立即生效。 您需要按照与原带宽的价格差，结合使用周期内的剩余时间，补齐差价。 例如：（以下价格仅作示例，实际价格以控制台显示为准） 客户于2018/11/1 购买了1Mbit/s的带宽，购买时长为1个月，此时价格为18.4元/月，客户使用余额支付18.4元，实付金额为18.4元。 客户在2018/11/24 将带宽升级为5Mbit/s，价格为92元/月。 这时，剩余天数为 30 - 24 = 6天，升配费用=92 / 30 * 6 - 18.4 / 30 * 6 = 14.72元。 了解更多变更资源计费信息，请参见**变更资源费用说明**。

计费模式	计费方式	变更操作	对费用的影响
	按带宽计费	降低带宽大小（续费降配）	降配后，新带宽大小不会立即生效。 您需要选择续费时长并根据新的带宽大小进行续费，续费成功后，新带宽大小在新的计费周期内生效。 ● 续费降配订单在资源未生效前支持退订。 ● 续费降配后，当前计费周期的剩余时间内不能再对带宽进行任何修改，请谨慎操作。
	按带宽计费	临时增加带宽大小（使用带宽加油包临时升配）	带宽加油包单独计费，您可以在带宽的使用周期内选择任意时间段使用带宽加油包临时增加带宽，带宽加油包到期后带宽自动回落。
按需计费	按带宽计费	增加/降低带宽大小	增加/降低带宽大小后，新的带宽大小和计费方式将立即生效。
	按流量计费	增加/降低带宽大小	增加/降低带宽大小后，新的带宽大小将立即生效。 按流量计费的EIP，带宽仅做限速使用，带宽大小不影响实际费用。

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 > 弹性公网IP”
4. 在“操作”列，选择“更多 > 修改带宽”。
   - 按需带宽将直接进入“修改带宽”页面。
   - 包年包月带宽可根据需求选择以下任一种带宽变更方案，并单击“继续”。
     - 补差价升配
     - 续费降配
     - 使用带宽加油包临时升配
5. 根据界面提示修改带宽参数。

图 13-3 修改按需带宽

图 13-4 修改包年包月带宽

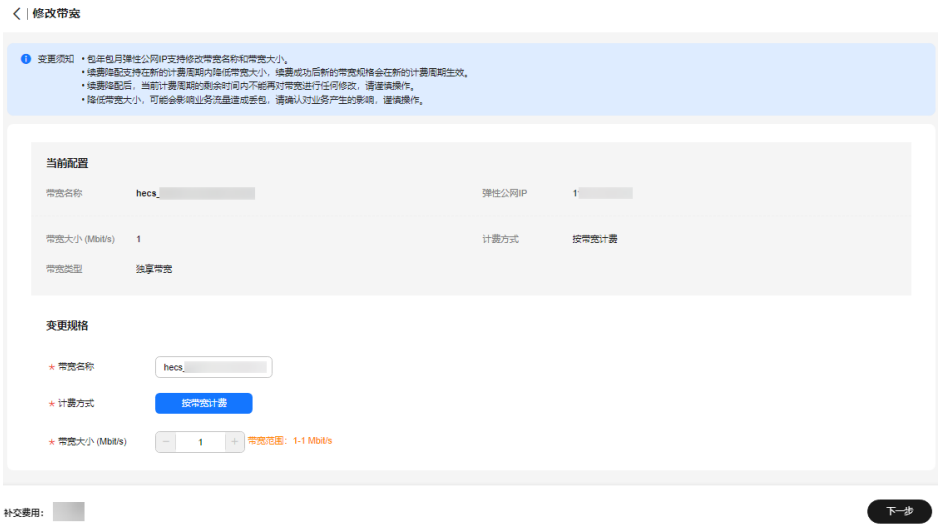


图 13-5 使用带宽加油包临时升配

6. 单击“下一步”。
7. 单击“提交”，完成修改。

您还可以同时勾选多个弹性公网IP，单击列表上方的“修改带宽”，批量修改多个弹性公网IP的带宽。批量修改操作仅支持按需且独享的带宽。

相关操作

- **如何切换计费方式中的“按带宽计费”和“按流量计费”？**
- **包年包月模式的带宽支持升配后再降配吗?**

13.5 导出弹性公网 IP 列表

操作场景

您可以将当前账号下拥有的所有信息，以Excel文件的形式导出至本地。该文件记录了弹性公网IP的ID、状态、类型、带宽名称、带宽大小等信息。

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 > 弹性公网IP”
4. 在弹性公网IP列表页，勾选一个或多个弹性公网IP，单击左上方的“导出”。
   系统会将您所选的所有弹性公网IP信息自动导出为Excel文件，并下载至本地。

13.6 管理弹性公网 IP 地址标签

操作场景

为弹性公网IP地址添加标签，可以方便用户识别和管理拥有的弹性公网IP地址。您可以在申请弹性公网IP地址时增加标签，或者在已经创建的弹性公网IP地址详情页添加标签，最多可以给弹性公网IP地址添加20个标签。

如您的组织已经设定弹性公网IP的相关标签策略，则需按照标签策略规则为弹性公网IP添加标签。标签如果不符合标签策略的规则，则可能会导致弹性公网IP创建失败，或已有弹性公网IP打标签失败，请联系组织管理员了解标签策略详情。

说明

当前Organizations服务正在公测中，使用组织合规规则功能需先申请Organizations服务公测。

标签共由两部分组成：“键”和“值”，其中，“键”和“值”的命名规则如表13-4所示。

表 13-4 弹性公网 IP 地址标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一弹性公网IP键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	Ipv4_key1
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	eip-01

操作步骤

在弹性公网IP列表页，按标签的键或值搜索目标弹性公网IP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. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性公网IP”
4. 在弹性公网IP列表上方的搜索框中，单击框中任意位置，设置搜索条件。

   在“属性类型”列表中，根据需要的标签选择对应的键和值。系统会根据您设置的标签搜索条件筛选对应的资源。

   单击搜索框中任意位置，添加下一个标签键和值。

   系统支持添加多个标签，并取各个标签筛选结果的交集，对目标弹性公网IP进行搜索。

在弹性公网IP地址的标签页，执行标签的增、删、改、查操作。

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 > 弹性公网IP”
4. 在弹性公网IP列表中，单击待管理标签的弹性公网IP地址名称。
5. 在弹性公网IP详情页面，选择“标签”页签，对弹性公网IP的标签执行增、删、改、查。
   - 查看

     在“标签”页，可以查看当前弹性公网IP地址的标签详情，包括标签个数，以及每个标签的键和值。
   - 添加

     单击左上角的“添加标签”，在弹出的“添加标签”窗口，输入新添加标签的键和值，并单击“确定”。
   - 修改

     单击标签所在行“操作”列下的“编辑”，在弹出的“编辑标签”窗口，输入修改后标签的值，并单击“确定”。

     标签键不支持修改。
   - 删除

     单击标签所在行“操作”列下的“删除”，如果确认删除，在弹出的确认窗口中单击“是”。

13.7 管理 IPv6 弹性公网 IP

简介

弹性公网IP支持IPv4地址和IPv6地址，您可以申请一个全新的IPv6弹性公网IP，也可以通过IPv6转换功能将已有的IPv4弹性公网IP映射为公网IPv6地址。

开启IPv6转换后，将提供IPv4和IPv6弹性公网IP地址，原有IPv4业务可以快速为IPv6用户提供访问能力。

IPv4弹性公网IP收取费用，IPv6弹性公网IP当前暂不收费，后续将择时收费。

IPv4/IPv6 双栈网络应用场景

如果您的ECS规格支持IPv6网络，那么您可以使用IPv4/IPv6双栈网络，场景示例和资源规划如**表13-5**所示。

说明

- 云耀云服务器 HECS不支持IPv6网络。
- 弹性云服务器ECS部分规格支持IPv6网络。关于ECS哪些规格支持IPv6网络，请参见**《弹性云服务器用户指南》**。

表 13-5 IPv4/IPv6 双栈网络的应用场景及资源规划

应用场景	场景示例	条件	子网网段类型	ECS
IPv4内网通信	在ECS上部署应用，需要与其他系统（比如数据库）之间使用**IPV4**进行内网互访。	• 实例未绑定弹性公网IP。	IPv4网段	**IPv4私网地址：**支持IPv4内网通信。
IPv4公网通信	在ECS上部署应用，需要与其他系统（比如数据库）之间使用**IPV4**进行公网互访。	• 实例绑定弹性公网IP。	IPv4网段	• **IPv4私网地址：**支持IPv4内网通信。 • **IPv4公网地址：**支持IPv4公网通信。
IPv6内网通信	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。	• VPC的子网开启IPv6。 • 创建ECS时，网络配置如下： – **规格：**选择支持IPv6网络的ECS规格。关于ECS哪些规格支持IPv6网络，请参见**《弹性云服务器用户指南》** – **VPC和子网：**选择已开启IPv6的子网及子网所属的VPC。 – 选择“**自动分配IPv6地址**”。 – **共享带宽：**暂不配置。	• IPv4网段 • IPv6网段	• **IPv4私网地址+IPv4 EIP：**实例绑定IPv4 EIP，支持IPv4公网通信。 • **IPv4私网地址：**实例不绑定IPv4 EIP，支持IPv4内网通信。 • **IPv6地址：**IPv6地址不加入共享带宽，支持IPv6内网通信。

应用场景	场景示例	条件	子网网段类型	ECS
IPv6公网通信	搭建IPv6网络，使ECS可以访问Internet上的**IPv6**服务。	• VPC的子网开启IPv6。 • 创建ECS时，网络配置如下： – **规格：**选择支持IPv6网络的ECS规格。关于ECS哪些规格支持IPv6网络，请参见**《弹性云服务器用户指南》** – **VPC和子网：**选择已开启IPv6的子网及子网所属的VPC。 – 选择“**自动分配IPv6地址**”。 – **共享带宽：**选择一个共享带宽。 **说明** 该场景的具体实现请参见**搭建IPv6网络**。	• IPv4网段 • IPv6网段	• **IPv4私网地址+IPv4 EIP：**实例绑定IPv4 EIP，支持IPv4公网通信。 • **IPv4私网地址：**实例不绑定IPv4 EIP，支持IPv4内网通信。 • **IPv6地址+共享带宽：**同时支持IPv6公网通信和IPv6内网通信。

使用IPv4/IPv6双栈网络请参考**IPv4/IPv6双栈网络**。

IPv6 转换功能应用场景

如果您想使部署应用的ECS面向Internet客户端提供IPv6服务，但您的ECS规格不支持IPv6网络，或者您不想通过搭建IPv6网络来实现该需求，那么您可以通过弹性公网IP的IPv6转换功能快速实现该能力。场景示例和资源规划如**表13-6**。

表 13-6 IPv6 EIP（开启 IPv6 转换）网络的应用场景及资源规划

应用场景	场景示例	条件	子网网段类型	ECS
IPv6公网通信	不搭建IPv6网络，使ECS为Internet上的客户端提供IPv6服务。	• 实例绑定弹性公网IP。 • 开启IPv6转换。	IPv4网段	• **IPv4私网地址：**支持IPv4内网通信。 • **IPv4 EIP地址（开启IPv6转换）：**同时支持IPv4公网通信和IPv6公网通信。

IPv6 网络应用场景及资源规划

图 13-6 IPv6 网络应用场景及资源规划

开启 IPv6 转换（申请 IPv6 弹性公网 IP）

- 方法一：

  参考**为ECS申请和绑定EIP**申请弹性公网IP，在申请页面配置参数时，请将“IPv6转换”设置为“开启”，就可以在申请IPv4地址的同时申请一个IPv6弹性公网IP。

  开启IPv6转换后，该弹性公网IP将同时拥有IPv4和IPv6地址，原有IPv4业务可以快速为IPv6用户提供访问能力。

- 方法二：

  当已有的IPv4地址的弹性公网IP需要增加IPv6地址时，可以在弹性公网IP列表页面，找到想转换的IPv4弹性公网IP，单击操作列“更多”下的“开启IPv6转换”，即可将已有的IPv4弹性公网IP转换为IPv6的。

  开启IPv6转换后，该弹性公网IP将同时拥有IPv4和IPv6地址，原有IPv4业务可以快速为IPv6用户提供访问能力。

说明

开启IPv6转换后，对原有绑定资源的使用无影响。

目前，支持开启IPv6转换的区域请参考**功能总览**，选择“IPv6转换”。

配置安全组

开启弹性公网IP的IPv6转换后，请务必在安全组的出方向和入方向中放通198.19.0.0/16网段的IP地址，如**表13-7**所示。因为IPv6 弹性公网IP采用NAT64技术，入方向的源IP地址经过NAT64转换后，会将IPv6地址转换为198.19.0.0/16之间的某个IPv4地址，源端口随机，目的IP为本机的内部私有IPv4地址，目的端口不变。

配置安全组操作请参考**《虚拟私有云用户指南》**。

表 13-7 安全组规则

方向	协议	端口和地址
入方向	全部	源地址：198.19.0.0/16
出方向	全部	目的地址：198.19.0.0/16

关闭 IPv6 转换（释放 IPv6 弹性公网 IP）

当弹性公网IP不再需要IPv6地址时，可以在弹性公网IP列表页面，找到想关闭IPv6地址的弹性公网IP ，单击“操作”列的“关闭IPv6转换”，即可删除IPv6地址。删除后，该弹性公网IP仅保留IPv4地址。

14 共享带宽

14.1 共享带宽概述

共享带宽可以实现多个弹性公网IP共同使用一条带宽，针对多个弹性公网IP进行集中限速。提供区域级别的带宽共享及复用能力，同一区域下的所有已绑定弹性公网IP的弹性云服务器、弹性负载均衡等实例共用一条带宽资源。

说明

- 共享带宽支持对单个弹性公网IP进行限速，请参见**企业级QoS功能**。

客户有大量业务在云上时，如果每个弹性云服务器单独使用一条带宽，则需要较多的带宽实例，并且总的带宽费用会较高，如果所有实例共用一条带宽，就可以节省企业的网络运营成本，同时方便运维统计。

- 节省带宽使用成本

  提供区域级别的带宽复用共享能力，节省带宽使用的运营及运维成本。
- 操作灵活

  除独享型ELB专属池（5_gray）类型的EIP以外，不区分其他弹性公网IP类型及绑定实例类型，随时从共享带宽中增加或移出按需计费的弹性公网IP。
- 计费方式灵活

  提供包年包月、按需计费两种计费模式。

您可以通过如下两种方式使用共享带宽功能：

- 申请一个共享带宽，将已经购买的按需计费的EIP添加到该共享带宽中：
  - **申请共享带宽**
  - **添加弹性公网IP到共享带宽**
- 申请一个共享带宽，新购按需计费的EIP时，“公网带宽”参数选择“加入共享带宽”：
  - **申请共享带宽**
  - **为ECS申请和绑定EIP**

共享带宽的配额限制

- 每个用户最多申请5个共享带宽，如果您需要更多共享带宽，请提交工单申请。
- 共享带宽可支持加入20个EIP，如果您需要加入更多EIP，请提交工单申请。
- 按需计费的共享带宽，需要升配扩容时，如果待升配的共享带宽已超过1G，再升配的时候，以500M为最小粒度增加。

共享带宽的使用限制

- 共享带宽只能加入按需计费的EIP。
- 共享带宽支持按带宽计费、增强型95计费。按带宽计费5Mbit/s起售，增强型95计费300Mbit/s起售。
- 通用可用区的共享带宽不支持添加边缘可用区的EIP，边缘可用区的共享带宽也不支持添加通用可用区的EIP。

  说明

  关于边缘可用区和普通可用区的区别请参考**《智能边缘小站用户指南》**。
- 包年包月共享带宽到期释放，EIP会被移出共享带宽并按照加入共享带宽之前的模式计费。
- 当共享带宽的计费方式选择“按增强型95计费”，保底百分比为20%，不支持修改。
- 共享带宽不支持跨账号使用。

说明

- 独享带宽与共享带宽不支持直接互相转换，但针对按需计费的弹性公网IP，您可以购买一个共享带宽，进行如下操作：
  - 将弹性公网IP添加到共享带宽，则弹性公网IP使用共享带宽。
  - 将弹性公网IP移出共享带宽，则弹性公网IP使用独享带宽。
- 工单提交请参见**提交工单**。

14.2 申请共享带宽

操作场景

客户有大量业务在云上时，如果每个实例单独使用一条带宽，则需要较多的带宽实例，并且总的带宽费用会较高。您可以通过申请共享带宽，将多个EIP加入共享带宽，实现所有实例共用一条带宽，从而节省企业的网络运营成本，同时方便运维统计。

共享带宽需要申请才能使用。

操作步骤

1. 进入**购买共享带宽**页面。
2. 根据界面提示配置参数。

表 14-1 参数说明

参数	说明	取值样例
计费模式	购买共享带宽时使用的计费模式，分为以下两种： ● 包年/包月：在使用前一次性支付一定期限（如1个月、1年等）的费用，后续使用期限内不再针对此共享带宽资源扣费。 ● 按需计费：按照共享带宽的使用时长进行计费。	包年/包月
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华东-上海一
线路	共享带宽的线路类型。共享带宽支持添加线路类型与带宽线路类型相匹配的EIP，具体匹配关系如下： ● 普通带宽：支持加入线路类型为**全动态BGP**、**优选BGP**类型的EIP。 ● 优选BGP：支持加入线路类型为**优选BGP**类型的EIP。 **说明** 在“中国-香港”区域，普通带宽线路类型的共享带宽仅支持加入线路类型为**全动态BGP**类型的EIP。	普通带宽
计费方式	共享带宽的计费方式。 支持按带宽计费、按增强型95计费。 **说明** ● 按需计费模式下，才能选择按增强型95计费。 ● 用户等级大于等于V4才可以选购增强型95计费。增强型95计费将按照多次去峰值后的实际使用带宽付费，按月结算。您可以设置保底带宽（带宽大小*保底百分比），如果实际的月峰值带宽小于等于保底带宽，将按照保底带宽计费，否则，将按照实际的月峰值带宽计费。 ● 如果选择增强型95计费，共享带宽300Mbit/s起售。 关于增强型95计费的更多信息请参见**什么是增强型95计费?**	按带宽计费
带宽大小	共享带宽的大小，单位Mbit/s，5M起售。	10

参数	说明	取值样例
企业级QoS功能	开启企业级QoS功能，共享带宽将支持对带宽下的单个IP限速，带宽分配更加合理，提升共享带宽利用率。设置限速，不做计费。详情请参考**企业级QoS功能**。 该功能目前已上线的区域有：西南-贵阳一、中国-香港、华南-深圳、华南-广州、华南-广州-友好用户环境、华北-北京四。	-
企业项目	申请共享带宽时，可以将共享带宽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
名称	共享带宽的名称。	Bandwidth-001
购买时长	包年包月场景需要选择，购买共享带宽的时长。	2个月
自动续费	选择包年包月计费模式时，可以选择开启自动续费。自动续费周期根据用户指定的购买时长确定。 ● 按月购买：自动续费周期为一个月。 ● 按年购买：自动续费周期为一年。	-

3. 单击“立即购买”。
4. 在产品配置信息确认页面，再次核对共享带宽信息，阅读并勾选“弹性公网IP服务声明”。
   - 选择按需计费的共享带宽时，单击“提交”。
   - 选择包年/包月计费的共享带宽时，单击“去支付”。
     进入订单支付页面，确认订单信息，单击“确认”。

14.3 添加弹性公网 IP 到共享带宽

操作场景

添加弹性公网IP到共享带宽资源。一个共享带宽中可以同时添加多个弹性公网IP。

约束与限制

- 通过流量包套餐创建的云耀云服务器（HECS），系统绑定的弹性公网IP不支持加入到共享带宽。
- 包年包月的弹性公网IP添加到共享带宽，需要先转为按需计费模式。

- “优选BGP”线路类型的共享带宽可添加优选BGP类型的EIP以及IPv6网卡。
- 通用可用区的共享带宽不支持添加边缘可用区的EIP，边缘可用区的共享带宽也不支持添加通用可用区的EIP。

说明

关于边缘可用区和普通可用区的区别请参考**《智能边缘小站用户指南》**。

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“网络 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想添加弹性公网IP的共享带宽，在“操作”列选择“添加公网IP”，勾选您想添加的弹性公网IP。

   说明

   - 弹性公网IP添加到共享带宽后，原来的独享带宽大小无效，将使用共享带宽进行限速。弹性公网IP原来的独享带宽将会被删除，不再计费，不会额外计算流量和带宽费用。
   - 在共享带宽添加弹性公网IP时，可以选择已加入其他共享带宽的弹性公网IP。弹性公网IP加入新的共享带宽时，会自动从以前的共享带宽移出。
6. 单击“确定”。

相关操作

独享带宽与共享带宽有何区别？能否互转？

14.4 从共享带宽中移出弹性公网 IP

操作场景

您可以根据需要将不需要的弹性公网IP从共享带宽中移出。

约束与限制

包年包月的弹性公网IP不能从共享带宽中移出(针对公测期间购买的共享带宽)。

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想移出弹性公网IP的共享带宽，选择“更多> 移出公网IP”，勾选您想移出的弹性公网IP。

6. 设置EIP移出后规格。支持修改EIP的计费模式和带宽大小。
7. 单击“确定”。

说明

弹性公网IP移出共享带宽后，IP地址保持不变。

14.5 修改共享带宽大小

操作场景

您可以根据需要修改共享带宽的名称和带宽大小。

- 按需计费的共享带宽，修改成功后立即生效，请参见**修改共享带宽（按需计费）**。
- 包年/包月的共享带宽，包括以下模式：
  - **补差价升配（包年/包月）**：修改成功后立即生效
  - **续费降配（包年/包月）**：修改成功后在新的计费周期生效
  - **使用带宽加油包临时升配（包年/包月）**：购买后立即生效

如果要修改共享带宽的计费方式，请参考**如何切换计费模式中的“按需”和“包年包月”？**。

修改共享带宽（按需计费）

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想修改的共享带宽，在“操作”列单击“修改带宽”，修改共享带宽的参数。
6. 单击“下一步”。
7. 单击“提交”，完成修改。
   修改完成后，新的带宽规格立即生效。

补差价升配（包年/包月）

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想修改的共享带宽，在“操作”列单击“修改带宽”。
6. 选择“补差价升配”，并单击“继续”。
7. 在“修改带宽”页面的“变更规格”区域，修改共享带宽的“带宽名称”和“带宽大小”。

8. 修改完成后，单击“下一步”。
9. 确认修改信息无误后，单击“去支付”。
   根据界面提示完成付款后，新的带宽规格立即生效。

续费降配（包年/包月）

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想修改的共享带宽，在“操作”列单击“修改带宽”。
6. 选择“续费降配”，并单击“继续”。
7. 在“修改带宽”页面的“变更规格”区域，修改共享带宽的“带宽名称”和“带宽大小”。
8. 修改完成后，单击“下一步”。
9. 确认修改信息无误后，单击“去支付”。
   根据界面提示完成付款后，新的带宽规格将在当前计费周期结束后生效。

使用带宽加油包临时升配（包年/包月）

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想修改的共享带宽，在“操作”列单击“修改带宽”。
6. 选择“使用带宽包临时升配”，并单击“继续”。
   进入“购买带宽加油包”页面。
7. 根据需要临时升配的带宽以及周期填写带宽加油包相关参数。
   详细内容请参见**购买带宽加油包**。
8. 带宽加油包参数设置完成后，单击“立即购买”。
9. 确认修改信息无误后，单击“去支付”。
   根据界面提示完成付款后，带宽加油包购买成功后立即生效，其带宽将在有效期内与共享带宽叠加使用，待有效期结束后失效。

14.6 删除共享带宽

操作场景

对于按需计费的共享带宽，当您不需要时可以直接删除。

约束与限制

- 对于包年包月的共享带宽，您可以退订，但不能直接删除。
- 要删除的共享带宽实例中，如有添加EIP，请先将EIP移出共享带宽实例。如添加边缘线路的EIP，请先释放此EIP。

前提条件

删除共享带宽前您需要先移出共享带宽内的弹性公网IP，详情请参见**从共享带宽中移出弹性公网IP**。

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 共享带宽”。
5. 在共享带宽列表中找到您想删除的按需计费的共享带宽，在“操作”列选择“更多 > 删除”。
6. 确认需删除的共享带宽信息，请输入“DELETE”，或者单击“一键输入”。
7. 单击“确定”，删除该共享带宽。

15 共享流量包

15.1 共享流量包概述

共享流量包是一款带宽流量套餐产品，使用方便，价格实惠。购买共享流量包后立即生效，并自动抵扣按需计费（按流量计费）的EIP带宽产生的流量资费，直到流量包用完或到期。共享流量包的收费标准请参考**产品价格详情**中“预付费流量包”的内容。

- 支持两种类型的共享流量包，静态BGP类型支持抵扣按需计费（按流量计费）的静态BGP带宽流量资费，动态BGP类型支持抵扣按需计费（按流量计费）的动态BGP带宽流量资费。

  说明

  目前不同区域支持的共享流量包类型不同，具体如下：

  - 动态BGP类型的共享带宽包当前支持的区域：华北-北京一、华北-北京四、华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、中国-香港、亚太-曼谷、亚太-新加坡、非洲-约翰内斯堡。
  - 静态BGP类型的共享带宽包当前支持的区域：华北-北京一、华东-上海二、华南-广州、西南-贵阳一。
- 共享流量包支持包月和包年两种规格，包年价格更优惠，支持购买多个共享流量包，优先抵扣快到期的流量包。
- 如购买的共享流量包在生效期内，扣费方式为先扣除已购买的共享流量包的流量额度后，超出部分以按需计费方式进行结算。
- 共享流量包到期后，不会影响您的EIP使用。您只需保证云服务账户有足够的余额，系统会自动以按需计费方式进行结算。

共享流量包的使用限制

- 共享流量包费用为一次性支付，即刻生效，不支持指定生效日期。
- 共享流量包一旦购买不支持修改和退订，到期后也不支持续订。
- 共享流量包支持包月和包年，到期后剩余的流量将无法再使用。
- 共享流量包只能针对按需计费（按流量计费）的带宽生效，且需要区分动态BGP和静态BGP类型。动态BGP共享流量包适用于动态BGP按需计费（按流量计费）的独享带宽，静态BGP共享流量包适用于静态BGP按需计费（按流量计费）的独享带宽。

- 共享流量包不支持对指定的某一个EIP带宽生效。
- 共享流量包不支持对共享带宽生效。
- 共享流量包不支持用于优选BGP类型的EIP。

15.2 购买共享流量包

操作场景

本章节指导用户购买共享流量包。购买后立即生效，并自动抵扣按需计费（按流量计费）的EIP带宽产生的流量资费，直到流量包用完或到期。

共享流量包的使用限制

- 共享流量包费用为一次性支付，即刻生效，不支持指定生效日期。
- 共享流量包一旦购买不支持修改和退订，到期后也不支持续订。
- 共享流量包支持包月和包年，到期后剩余的流量将无法再使用。
- 共享流量包只能针对按需计费（按流量计费）的带宽生效，且需要区分动态BGP和静态BGP类型。动态BGP共享流量包适用于动态BGP按需计费（按流量计费）的独享带宽，静态BGP共享流量包适用于静态BGP按需计费（按流量计费）的独享带宽。
- 共享流量包不支持对指定的某一个EIP带宽生效。
- 共享流量包不支持对共享带宽生效。
- 共享流量包不支持用于优选BGP类型的EIP。
- 在购买共享流量包时，如果您有订单在支付期限内未支付，则无法购买共享流量包。请取消未支付订单或支付订单后再购买共享流量包。

操作步骤

1. 进入**购买共享流量包**页面。
2. 按照提示配置参数。

表 15-1 参数说明

参数	说明	取值样例
区域	不同的区域之间的资源包不互通，每个区域需要分别购买，请根据您的实际需求谨慎选择。 具体可以参考如下示例： 如果您当前需要购买共享流量包抵扣区域A中的EIP带宽产生的流量资费，那么您必须购买区域A的共享流量包。如果购买其他区域（例如区域B）的流量包，就不能抵扣区域A中的EIP带宽产生的流量资费。	华东-上海一

参数	说明	取值样例
类型	根据弹性公网IP的带宽类型进行设置。 ● 动态BGP：支持类型为动态BGP的按需计费（按流量计费）带宽。 ● 静态BGP：支持类型为静态BGP的按需计费（按流量计费）带宽。	静态BGP
套餐有效期	套餐时长。请根据您的需要选择合适的套餐时长，流量包不支持退订，流量包购买成功后即刻生效，超过有效期后未用完的流量将无法使用。	一个月
规格	共享流量包的大小，单位GB。	10GB
购买时长	套餐时长。	Default

3. 单击“立即购买”。
4. 在产品配置信息确认页面，再次核对共享流量包信息，单击“去支付”。
5. 进入订单支付页面，确认订单信息，单击“确认”。

16 带宽加油包

16.1 带宽加油包概述

带宽加油包用来临时调大带宽上限，适用于在有效期内的包年包月独享带宽和共享带宽。

当某个时间段业务量激增（例如：双11），需要在这个时间段临时调整带宽规格，您可以通过购买带宽加油包，设置有效期时间来解决。加油包到期将自动失效，恢复到原来的带宽规格。

说明

- 带宽加油包目前支持的区域请参考**功能总览**，选择“带宽加油包”。
- 带宽加油包是从购买时选择的有效期开始时间生效的，根据您设置的有效期时间，带宽加油包支持购买后立即生效。
- 带宽加油包到期将自动失效，带宽恢复到原来的规格。
- 如果您购买带宽加油包后，带宽还是不能满足要求，可以再次购买带宽加油包叠加使用。
  目前带宽加油包支持叠加使用的区域：华北-北京四，华东-上海一，华南-广州，西南-贵阳一，中国-香港。
- 使用带宽加油包不会影响业务中断，也不需要重启实例。

带宽加油包的使用限制

- 带宽加油包只能针对包年/包月带宽生效。
- 带宽加油包1天起售，购买后不能修改起始时间及带宽大小。

16.2 购买带宽加油包

操作场景

带宽加油包需要购买才能使用。

带宽加油包的使用限制

- 带宽加油包只能针对包年/包月带宽生效。

- 带宽加油包1天起售，购买后不能修改起始时间及带宽大小。
- 在购买带宽加油包时，如果您有未支付的带宽加油包订单，则无法购买新的带宽加油包。请取消未支付订单或支付订单后再购买新的带宽加油包。

操作步骤

1. 进入**购买带宽加油包**页面。
2. 按照提示配置参数。

表 16-1 参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华东-上海一
名称	带宽加油包的名称。 输入长度范围1到64位。名称内容只能由中文、英文字母、数字、下划线、中划线、点组成。	bandpkg-001
当前带宽	加油包的作用带宽。	Bandwidth-001
新增带宽大小	需要增加的带宽大小，单位Mbit/s。	10
生效类型	带宽加油包支持即时生效和固定生效。	固定生效
到期时间	当选择即时生效时，需要设置此参数，即带宽加油包生效的结束时间，按天计算。 加油包有效期必须在带宽的有效期内。该购买操作成功后，带宽加油包将立即生效。	-
有效期	当选择固定生效时，需要设置此参数，即带宽加油包生效的开始时间和结束时间，按天计算。 加油包有效期必须在带宽的有效期内。该购买操作成功后，带宽加油包在设置的有效期内生效。	-

3. 单击“立即购买”。
4. 在产品配置信息确认页面，再次核对带宽加油包信息。
   单击“去支付”，进入订单支付页面，确认订单信息，单击“确认”。

16.3 修改带宽加油包

操作场景

您可以修改带宽加油包的名称。

约束与限制

不支持直接修改带宽加油包大小、有效期等参数。如果想修改，请先退订当前的加油包，然后重新购买新的加油包。

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 带宽加油包”。
5. 在列表中找到您想修改的带宽加油包，单击“操作”列的“修改”，修改带宽加油包的名称。
6. 单击“确定”。

16.4 退订带宽加油包

操作场景

当您想提前结束带宽加油包时，可以退订带宽加油包。已经使用的时长会收取对应的费用。

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 > 弹性公网IP”
4. 在左侧导航栏，选择“弹性公网IP和带宽 > 带宽加油包”。
5. 在列表中找到您想退订的带宽加油包，单击“操作”列的“退订”。
6. 在退订页面，确认资源信息和退款信息，选择退订原因。

   勾选提示信息“资源退订后，未放入回收站的资源将立即删除且无法恢复。我已确认数据完成备份或不再使用”。

   单击“退订”。
7. 再次核对信息，单击“退订”。

17 监控与审计

17.1 监控

17.1.1 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 17-1 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"

  }

  ],

17.1.2 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。

17.1.3 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》。

17.2 审计

17.2.1 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17-2所示。

表 17-2 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

17.2.2 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。

18 附录

18.1 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));
}
```


A 修订记录

发布日期	修改说明
2024-06-05	第七十三次正式发布。文档内容更新为： • 在**虚拟私有云和子网规划建议**章节，修改VPC网段选择建议。 • 在**共享VPC概述**章节，增加支持共享VPC的云服务资源。
2024-05-28	第七十二次正式发布。文档内容更新为： 在**网络ACL概述**、**网络ACL配置示例**和**添加网络ACL规则（自定义生效顺序）**等章节，提供网络ACL架构图、工作原理和应用示例等内容。
2024-04-25	第七十一次正式发布。文档内容更新为： • 根据控制台风格变化修改全文截图。 • 在**删除虚拟私有云**和**删除子网**章节，在控制台显示待删除VPC和子网的关联资源。 • 在**创建安全组**和**管理安全组标签**章节，增加安全组标签的说明。 • 在**创建网络ACL**和**管理网络ACL的标签**章节，增加网络ACL标签的说明。
2024-03-15	第七十次正式发布。文档内容更新为： • 在**共享VPC概述**~**停止VPC子网共享**章节，增加共享VPC内容。 • 在**创建虚拟私有云和子网**和**为虚拟私有云创建新的子网**等章节，增加标签策略说明。 • 在**导入和导出安全组规则**章节，增加安全组规则导入约束与限制说明。

发布日期	修改说明
2023-11-16	第六十九次正式发布。文档内容更新为： • 在**将子网关联至网络ACL**和**将子网和网络ACL解除关联**章节，增加通过子网列表页面，关联或者解除关联网络ACL的说明。 • 在**创建IP地址组**和**在IP地址组内添加IP地址条目**章节，增加IP地址条目描述说明。 • 新增**导出IP地址组详情**、**在IP地址组内修改IP地址条目**和**在IP地址组内批量导入IP地址条目**章节，增加IP地址组操作说明。 • 在**创建IP地址组**、**在IP地址组内添加IP地址条目**以及**在IP地址组内修改IP地址条目**章节，增加“最大条目数”参数。
2023-09-19	第六十八次正式发布。文档内容更新为： • 在**删除IP地址组**章节，增加同步删除关联资源的说明。 • 在**删除弹性网卡**和**删除辅助弹性网卡**章节，增加删除网卡的说明。 • 在**在安全组中一键放通常见端口**章节，新增一键放通常见端口要内容。 • 在**创建相同账户下的对等连接**、**创建不同账户下的对等连接**、**修改对等连接路由**、**查看对等连接路由**、**删除对等连接路由**章节，修改对等连接添加路由内容。
2023-08-31	第六十七次正式发布。文档内容更新为： • 在**流量镜像概述**~**删除镜像会话**章节，增加流量镜像功能。 • 在**安全组和安全组规则概述**和**安全组配置示例**章节，增加安全组规则介绍、配置示例等内容。
2023-07-07	第六十六次正式发布。文档内容更新为： • 在**添加安全组规则**和**快速添加多条安全组规则**章节，源地址和目的地址增加支持添加多个IP地址说明。 • 在**创建安全组**章节，增加安全组模板说明，支持快速添加安全组规则模板。
2023-06-08	第六十五次正式发布。文档内容更新为： • 在**安全组和安全组规则概述**章节，增加安全组规则示例说明。 • 在**创建安全组**章节，添加安全组规则模板说明。 • 在**添加安全组规则**、**快速添加多条安全组规则**和**导入和导出安全组规则**章节，修改源地址和目的地址参数说明。 • 在**创建网络ACL**章节，增加支持企业项目相关内容。 • 在**创建IP地址组**章节，增加支持企业项目相关内容。 • 在**添加弹性公网IP到共享带宽**章节，增加EIP跨带宽迁移能力的说明。

发布日期	修改说明
2023-04-26	第六十四次正式发布。文档内容更新为： ● 在**创建相同账户下的对等连接**和**创建不同账户下的对等连接**章节，更新界面截图和参数。 ● 在**IP地址组概述**~**删除IP地址组**章节，增加IP地址组新功能相关内容。
2023-02-25	第六十三次正式发布。文档内容更新为： ● 在**对等连接应用示例**章节，增加对等连接示例组网。 ● 增加**获取对等连接的对端项目ID**章节。 ● 增加**修改对等连接路由**章节。
2023-01-31	第六十二次正式发布。文档内容更新为： ● 在**创建虚拟私有云和子网**、**为虚拟私有云创建新的子网**和**修改子网信息**章节，增加“域名”参数。 ● 在**创建IP地址组**章节，修改IP地址组格式说明。
2022-12-23	第六十一次正式发布。文档内容更新为： ● 新增**查看并删除子网内的云服务资源**章节。 ● 新增**查看子网内IP地址的用途**章节。 ● 修改**删除虚拟私有云**和**删除子网**章节。
2022-11-15	第六十次正式发布。文档内容更新为： ● 在**共享流量包概述**章节，添加到价格计算器详情页的链接作为价格参考。 ● 新增**将虚拟IP地址和实例解绑定**和**将虚拟IP地址和弹性公网IP解绑定**章节。 ● 在**删除虚拟IP地址**章节，增加约束与限制。 ● 在**删除安全组**章节，增加安全组不收费说明。
2022-11-01	第五十九次正式发布。文档内容更新为： 在**安全组和安全组规则概述**章节，修改安全组关联实例数量。
2022-08-19	第五十八次正式发布。文档内容更新为： 根据界面“子网”“路由表”“对等连接”“弹性网卡”入口变化刷新文档。
2022-07-26	第五十七次正式发布。 新增EIP不支持跨区域使用限制、带宽加油包支持的区域、普通可用区和边缘可用区的EIP资源使用限制，更新章节： ● **弹性公网IP概述**。 ● **为ECS申请和绑定EIP**。 ● **共享带宽概述**。 ● **添加弹性公网IP到共享带宽**。 ● **带宽加油包概述**。

发布日期	修改说明
2022-07-14	第五十六次正式发布。文档内容更新为： ● 在**为ECS申请和绑定EIP**章节，优选BGP相关描述优化更新。 ● 流日志功能正式商用。
2022-06-15	第五十五次正式发布。文档内容更新为： 将虚拟私有云文档中的二层连接网关内容下线，关于二层连接网关的最新文档请参见**企业交换机**。
2022-06-10	第五十四次正式发布。文档内容更新为： ● 在**路由表和路由概述**中，增加路由下一跳为云防火墙的说明。 ● 虚拟私有云提供新版控制台，主要修改以下章节： – **创建虚拟私有云和子网** – **为虚拟私有云创建新的子网** – **创建弹性网卡** – **创建辅助弹性网卡** – **创建相同账户下的对等连接** – **申请虚拟IP地址** ● 在**创建相同账户下的对等连接**和**创建不同账户下的对等连接**章节，修改对等连接路由添加指导。
2022-05-15	第五十三次正式发布。文档内容更新为： ● 在**路由表和路由概述**中，增加不同类型路由支持默认路由表和自定义路由表的说明。 ● 在**将其他路由表中的路由复制到当前路由表**中，增加不同类型路由是否支持复制的约束与限制。
2021-12-28	第五十二次正式发布。文档内容更新为： ● 在**IPv6网络**中，增加IPv6网络的应用场景。 ● 增加**查看虚拟私有云拓扑图**章节。
2021-11-01	第五十一次正式发布。文档内容更新为： 新增“优选BGP线路”， ● 在**为ECS申请和绑定EIP**中，修改参数“线路”的描述。 ● 在**申请共享带宽**、**添加弹性公网IP到共享带宽**中，增加参数“线路”以及相关约束与限制说明。
2021-10-18	第五十次正式发布。文档内容更新为： 新增“辅助弹性网卡”章节。
2021-05-20	第四十九次正式发布。文档内容更新为： 常见问题新增“为什么VPC已删除，还存在持续计费情况？”。

发布日期	修改说明
2021-03-05	第四十八次正式发布。文档内容更新为： ● 产品介绍新增“网络服务概述”。 ● 常见问题新增“配置了IPv6双栈，为什么无法访问IPv6网站？”。
2020-12-17	第四十七次正式发布。文档内容更新为： ● 在“约束与限制”章节，增加各功能限制说明。 ● 对等连接补充图示。
2020-11-03	第四十六次正式发布。文档内容更新为： ● 调整“虚拟私有云和子网章节”结构。 ● 新增“为虚拟私有云添加扩展网段”和“删除虚拟私有云扩展网段”章节。 ● 在“网络ACL”章节，新增“拒绝某IP地址的访问”。 ● 删除常见问题：弹性云服务器关机再开机后，其绑定的弹性公网IP是否会改变?
2020-10-23	第四十五次正式发布。文档内容更新为： ● 新增“弹性网卡”章节。 ● 优化“安全组”章节。
2020-09-07	第四十四次正式发布。文档内容更新为： ● 常见问题新增“为什么配置的安全组规则不生效？”。 ● 常见问题删除“VPC对等连接出现问题时，如何排查？”。 ● 常见问题修改“为什么对等连接创建完成后不能互通？”。 ● 常见问题修改“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？”。
2020-07-23	第四十三次正式发布。文档内容更新为： 新增“IP地址组”章节，同时在安全组对应章节新增“IP地址组”字段。
2020-06-09	第四十二次正式发布。文档内容更新为： ● 常见问题新增：“配置双网卡后ping不通？”。

发布日期	修改说明
2020-05-20	第四十一次正式发布。文档内容更新为： ● 常见问题新增：“外网能访问服务器，但是服务器无法访问外网时，如何排查？”。 ● 常见问题新增：“哪些设备可以与华为云二层连接网关做对接？” ● 常见问题新增：“二层连接配置完成后状态一直显示未连接？”。 ● 常见问题新增：“二层连接状态显示已连接，但云上与云下的主机网络仍不通？”。 ● 修改常见问题“子网被相关资源占用时，会导致无法删除子网，如何排查相关资源？”。 ● 新增“克隆安全组”章节。
2020-04-15	第四十次正式发布。文档内容更新为： ● 常见问题新增“弹性公网IP是否支持跨区域绑定？”。 ● 常见问题新增“如何查询弹性公网IP归属地？”。 ● 常见问题新增“弹性公网IP是否支持转移给其他账号？”。 ● 常见问题新增“购买弹性公网IP时，是否可以指定IP地址？”。 ● 常见问题新增“购买弹性公网IP后，弹性公网IP是否会变化？”。 ● 常见问题新增“怎样切换内网DNS？”。
2020-03-30	第三十九次正式发布。文档内容更新为： ● 新增“二层连接网关（公测）”章节。 ● 在“安全组简介”及“网络ACL简介”章节补充基本信息。 ● 修改常见问题“变更安全组规则和网络ACL规则时，是否对原有流量实时生效？”。 ● 产品介绍新增“计费说明”章节。 ● 常见问题新增“计费类”。
2020-03-20	第三十八次正式发布。文档内容更新为： ● 常见问题新增“用户在弹性云服务器内手工配置的IPv6地址为什么无法通信？” ● 常见问题删除“安全组中多个安全组规则冲突时，安全组规则优先级哪个更高？”
2020-02-18	第三十七次正式发布。文档内容更新为： ● 常见问题新增“弹性公网IP如何计费？”。 ● 优化常见问题“一个弹性公网IP可以给几个弹性云服务器使用？”。
2020-02-10	第三十六次正式发布。文档内容更新为： 修改“权限管理”章节，VPC系统权限名称变更。

发布日期	修改说明
2020-01-20	第三十五次正式发布。文档内容更新为： 修改“权限管理”章节内容。
2019-12-23	第三十四次正式发布。文档内容更新为： ● 根据界面“子网”“路由表”入口及功能变化刷新文档。 ● 在常见问题新增“弹性云服务器是否支持切换虚拟私有云？”。
2019-12-03	第三十三次正式发布。文档内容更新为： ● 优化“产品介绍”描述与图示。 ● 根据统一身份认证服务界面，刷新“权限管理”章节。
2019-11-20	第三十二次正式发布。文档内容更新为： ● 在常见问题新增“弹性公网IP的分配策略是什么？”章节。 ● 在常见问题新增“静态BGP与全动态BGP有何区别？”章节。 ● 在常见问题新增“什么是增强型95计费？”章节。
2019-10-30	第三十一次正式发布。文档内容更新为： 新增附录章节“NAT64 TOA插件配置”。
2019-10-15	第三十次正式发布。文档内容更新为： ● 新增“VPC流日志（公测）”章节。 ● 根据安全组添加规则界面，刷新文档截图。 ● 在常见问题新增“为什么网络ACL添加了拒绝特定IP地址访问的规则，但仍可以访问？”章节。
2019-10-09	第二十九次正式发布。文档内容更新为： ● 在常见问题新增“弹性公网IP是否支持变更绑定的弹性云服务器？”章节。 ● 在常见问题新增“弹性云服务器关机再开机后，其绑定的弹性公网IP是否会改变？”章节。
2019-09-26	第二十八次正式发布。文档内容更新为： 优化“VPC对等连接”章节。
2019-09-12	第二十七次正式发布。文档内容更新为： ● 删除“删除VPN”章节。 ● 在常见问题新增“带宽与上传下载速率是什么关系？”章节。 ● 常见问题“删除安全组有何约束？”补充内容。

发布日期	修改说明
2019-08-15	第二十六次正式发布。文档内容更新为： ● 在“安全组配置示例”章节，新增“允许外部访问指定端口”示例。 ● 常见问题中新增“如何切换计费方式中的“按带宽计费”和“按流量计费”？”章节。 ● 常见问题中新增“带宽加油包是否支持在有效期内叠加？”章节。
2019-07-30	第二十五次正式发布。文档内容更新为： ● 新增“带宽加油包”章节。
2019-05-31	第二十四次正式发布。文档内容更新为： ● 产品介绍中新增“权限管理”章节。 ● 产品介绍中新增“区域和可用区”章节。 ● 快速入门中新增“搭建IPv4网络”和“搭建IPv6网络（公测）”。 ● 用户指南中新增“权限管理”章节。
2018-12-30	第二十三次正式发布。文档内容更新为： ● 匹配管理控制台左侧导航菜单变更，修改了安全组、网络ACL、弹性公网IP、共享带宽等的入口描述。 ● 新增“网络ACL简介”章节。 ● 新增“网络ACL配置示例”章节。
2018-11-30	第二十二次正式发布。文档内容更新为： ● 根据网络ACL界面优化同步更新对应文档。 – 新增批量删除规则、批量解除关联子网。 – 修改参数“Any”为“全部”，“动作”为“策略”等。 ● 修改FAQ“弹性云服务器IP获取不到时，如何排查”。

发布日期	修改说明
2018-09-30	第二十一次正式发布。文档内容更新为： ● 新增常见问题“云主机弹性云服务器的主网卡和扩展网卡在使用上有什么区别？”。 ● 新增常见问题“修改弹性云服务器的时间后，IP地址丢失，怎么办？”。 ● 新增“IPv4/IPv6双栈网络（公测）”章节。 ● 新增“共享流量包”章节。 ● 修改常见问题“如何切换计费模式中的“按需”和“包年包月”？”。 ● 在“创建虚拟私有云基本信息及默认子网”章节新增批创子网描述。 ● 在“添加网络ACL规则”章节新增批量添加规则描述、新增规则的“描述”参数。 ● 新增“配置SNAT服务器”章节。
2018-08-30	第二十次正式发布。文档内容更新为： ● 新增“IPv6弹性公网IP（公测）”章节。 ● 在“创建虚拟私有云基本信息及默认子网”和“创建安全组”章节新增“企业项目”参数。
2018-07-30	第十九次正式发布。文档内容更新为： ● 安全组修改： – 修改“复制安全组规则”章节。 – 新增“修改安全组规则”章节。 – 修改“删除安全组规则”章节。 – 新增“导入/导出安全组规则”章节。 – 新增“实例加入/移出安全组”章节。 ● 自定义路由修改： – 新增“简介”章节。 – 新增“VPC内自定义路由示例”章节。 – 新增“VPC外自定义路由示例”章节。 ● 在“为虚拟私有云创建新的子网”章节新增系统保留地址的说明。 ● 删除“SNAT”和“配置SNAT服务器”章节，新增“NAT网关”章节。

发布日期	修改说明
2018-06-30	第十八次正式发布。文档内容更新为： ● 共享带宽新增增强型95计费方式。 ● 优化产品介绍章节。 ● 优化安全组章节。 ● 新增“VPC网络规划”。 ● 常见问题增加分类。 ● 新增“无法访问公有云某些端口时怎么办？”。 ● 新增“TCP 25端口出方向无法访问时怎么办？”。 ● 修改“添加安全组规则”章节。 ● 修改“快速添加多条安全组规则”章节。 ● 新增“修改安全组规则”章节。
2018-05-30	第十七次正式发布。文档内容更新为： ● 新增“企业项目”参数。 ● 新增“克隆安全组规则”功能。 ● 新增安全组规则的“描述”参数。 ● 统一购买、创建、申请的界面用语。
2018-05-23	第十六次正式发布。文档内容更新为： ● 新增“修改弹性公网IP的带宽”章节，删除原“查询和修改带宽”章节。 ● 修改“如何通过扩展网卡绑定的弹性公网IP访问公网？”。 ● 修改“EIP连接出现问题时，如何排查？”。
2018-05-11	第十五次正式发布。文档内容更新为： ● 新增共享带宽相关描述。 ● 在申请弹性公网IP章节，将购买时长和数量合并，修改为购买量。 ● 新增云监控和云审计内容。 ● 修改常见问题：如何使用共享带宽。 ● 修改常见问题：带宽的限速范围是多少。
2018-04-28	第十四次正式发布。文档内容更新为： ● 新增导出虚拟私有云列表。 ● 修改弹性IP为弹性公网IP。 ● 新增常见问题：如何通过扩展网卡绑定的弹性公网IP访问公网。

发布日期	修改说明
2018-03-30	第十三次正式发布。文档内容更新为： ● 新增Cloud-init连接出现问题时，如何排查。 ● 新增EIP连接出现问题时，如何排查。 ● 新增IB网络出现问题时，如何排查。 ● 新增VPC对等连接出现问题时，如何排查。 ● 新增二三层通信出现问题时，如何排查。 ● 新增裸机网络出现问题时，如何排查。 ● 新增VPC虚拟IP无法访问时，如何排查。 ● 新增弹性云服务器IP获取不到时，如何排查。 ● 新增VPN及专线网络连接出现问题时，如何排查。
2018-02-28	第十二次正式发布。文档内容更新为： ● 新增如何切换弹性IP计费模式中的“按需”和“包年包月”。 ● 新增如何为配置了多网卡的弹性云服务器配置策略路由。 ● 新增本地主机访问使用弹性云服器搭建的网站出现间歇性中断怎么办。 ● 新增同一个子网下的弹性云服务器只能通过内网IP地址单向通信怎么办。 ● 新增同一个VPC内的两台弹性云服务器无法互通或者出现丢包等现象时，如何排查。 ● 新增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。
2018-01-30	第十一次正式发布。文档内容更新为： ● 新增批量解绑和释放弹性IP地址功能。 ● 创建安全组时，描述信息不超过64位。
2017-11-30	第十次正式发布。文档更新内容为： ● 创建子网无需配置可用区。
2017-10-30	第九次正式发布。文档内容更新为： ● 按照管理控制台最新的UI风格刷新手册截图。 ● “防火墙”名称修改为“网络ACL”。 ● 新增快速添加安全组规则的功能。 ● 新增弹性云服务器的安全组配置案例。
2017-09-30	第八次正式发布。文档内容更新为： ● 新增虚拟私有云和子网的标签特性。

发布日期	修改说明
2017-08-20	第七次正式发布。文档内容更新为： ● 根据界面优化更新“虚拟私有云和子网”和“自定义路由”章节操作步骤。 ● 根据界面优化更新申请VPC、VPN、弹性IP地址操作步骤。
2017-07-30	第六次正式发布。文档内容更新为： ● 路由表支持100条自定义路由。
2017-07-20	第五次正式发布。文档内容更新为： 新增以下特性： ● 对等连接 ● 网络ACL ● 自定义路由
2017-04-28	第四次正式发布。文档内容更新为： 修改子网信息网络信息时，可以增加多个DNS服务器地址。
2016-10-19	第三次正式发布。文档内容更新如下： ● VPN帮助中心URL改动，更新帮助中心URL。
2016-07-15	第二次正式发布。文档内容更新如下： ● 修改VPN的认证算法支持SHA2。 ● 流量计费功能性能优化，同时支持自动切换流量计费数据库。
2016-03-14	第一次正式发布。