天翼云

# 虚拟私有云

## 用户手册

天翼云科技有限公司

# 目录


1 产品动态 ..... 6
2 产品介绍 ..... 7
什么是虚拟私有云？ ..... 7
虚拟私有云的优势 ..... 7
如何访问虚拟私有云 ..... 8
虚拟私有云应用场景 ..... 8
虚拟私有云其他服务的关系 ..... 10
用户权限 ..... 10
虚拟私有云相关术语解释 ..... 10
子网 ..... 10
弹性 IP ..... 11
路由表 ..... 11
SNAT ..... 15
带宽 ..... 16
安全组 ..... 16
对等连接 ..... 16
网络 ACL ..... 17
IPv4/IPv6 双栈 ..... 17
虚拟 IP ..... 18
区域与可用区 ..... 20
什么是区域、可用区？ ..... 20
如何选择区域？ ..... 20
如何选择可用区？ ..... 21
3 计费说明 ..... 21
产品规格和价格 ..... 21
4 快速入门 ..... 22
典型场景说明 ..... 22
配置无需访问公网的弹性云服务器的 VPC ..... 23
简介 ..... 23
步骤 1：创建虚拟私有云基本信息及默认子网 ..... 24
步骤 2：为虚拟私有云创建新的子网 ..... 28
步骤 3：创建安全组 ..... 30
步骤 4：添加安全组规则 ..... 31
配置通过弹性 IP 访问公网的弹性云服务器的 VPC ..... 33
简介 ..... 33

步骤 1：创建虚拟私有云基本信息及默认子网 ..... 35
步骤 2：为虚拟私有云创建新的子网 ..... 39
步骤 3：为弹性云服务器申请和绑定弹性 IP ..... 41
步骤 4：创建安全组 ..... 43
步骤 5：添加安全组规则 ..... 44
5 用户指南 ..... 46
虚拟私有云和子网 ..... 46
虚拟私有云 ..... 46
子网 ..... 52
安全性 ..... 62
安全组 ..... 62
网络 ACL ..... 75
弹性 IP 管理 ..... 88
申请弹性 IP ..... 88
绑定弹性 IP ..... 89
解除弹性 IP ..... 89
删除弹性 IP ..... 90
IPv4/IPv6 双栈管理 ..... 91
创建 IPv4/IPv6 双栈子网 ..... 91
添加 IPv4/IPv6 双栈网卡到共享带宽 ..... 92
设置 IPv4/IPv6 双栈管理安全组 ..... 93
为 IPv4/IPv6 双栈网络配置 ACL ..... 94
添加 IPv6 自定义路由 ..... 95
虚拟 IP ..... 96
虚拟 IP 简介 ..... 96
申请虚拟 IP 地址 ..... 98
为虚拟 IP 地址绑定弹性 IP 或弹性云服务器 ..... 100
为弹性 IP 地址绑定虚拟 IP 地址 ..... 106
通过 VPN 访问虚拟 IP ..... 107
通过云专线访问虚拟 IP ..... 107
通过对等链接访问虚拟 IP ..... 107
关闭备弹性云服务器 IP 转发功能 ..... 108
关闭源/目的检查（适用于高可用负载均衡集群场景） ..... 108
删除虚拟 IP 地址 ..... 109
VPC 对等连接 ..... 111
对等连接创建流程 ..... 111
对等连接路由配置方案 ..... 112
创建同一帐户下的对等连接 ..... 115

创建不同帐户下的对等连接 ..... 119
查看对等连接 ..... 123
修改对等连接 ..... 123
删除对等连接 ..... 124
查看对等连接路由 ..... 124
删除对等连接路由 ..... 125
路由表（已解耦） ..... 127
路由表简介 ..... 127
创建自定义路由表 ..... 130
添加自定义路由 ..... 131
关联子网与路由表 ..... 132
更换子网关联的路由表 ..... 132
查询路由表 ..... 133
删除路由表 ..... 133
修改路由 ..... 133
删除路由 ..... 135
复制路由 ..... 135
导出路由表列表 ..... 136
路由表（未解耦） ..... 137
路由表简介 ..... 137
配置 SNAT 服务器 ..... 137
添加自定义路由 ..... 140
查询路由表 ..... 141
修改路由 ..... 141
删除路由 ..... 142
监控 ..... 143
支持的监控指标 ..... 143
查看监控指标 ..... 144
创建告警规则 ..... 145
6 最佳实践 ..... 146
VPC 公网访问 ..... 146
VPC 连接 ..... 148
基于 NAT 网关和 VPC 对等连接实现跨 VPC 访问公网和对公网提供服务 ..... 150
最佳实践概述 ..... 150
方案正文 ..... 151
7 常见问题 ..... 153
通用类 ..... 153
虚拟私有云与子网类 ..... 154

弹性 IP 类.....156
带宽类.....157
连接类.....157
路由类.....160
安全类.....160

# 1 产品动态

| 序号 | 时间节点 | 功能名称 | 功能描述 |
| --- | --- | --- | --- |
| 1 | 2022.08 | VPC 帮助中心更新 | 新增 VPC 相关术语解释，增加使用场景，更新部分产品功能。 |
| 2 | 2022.06 | VPC 帮助中心优化 | 优化目录结构，合并对等连接帮助文档，更新相关内容。 |

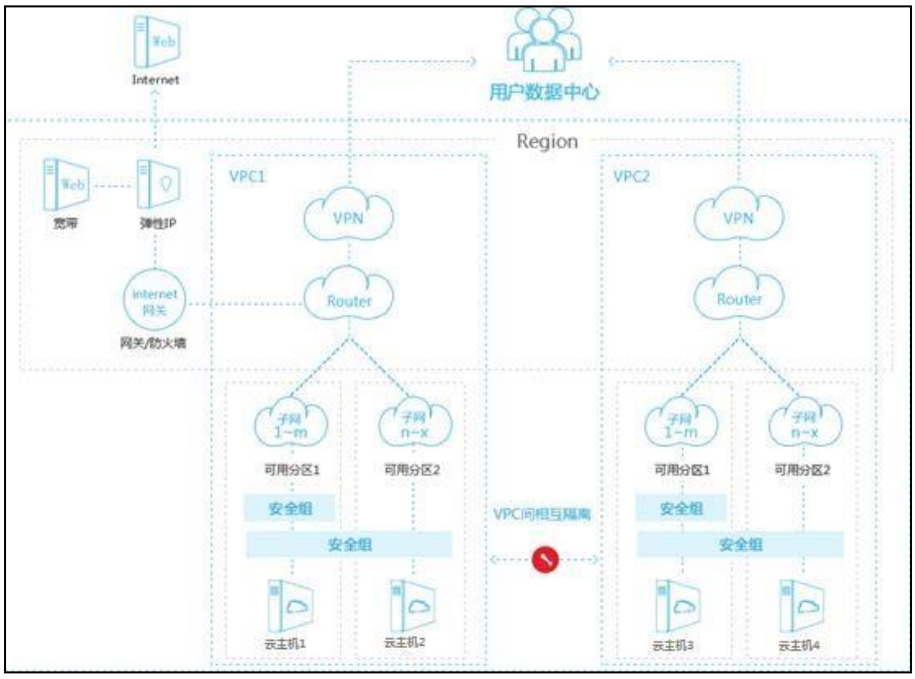
# 2 产品介绍

## 什么是虚拟私有云?

虚拟私有云（CT-VPC ，Virtual Private Cloud）为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

您可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性。用户可以通过 VPC 方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

图2-1 虚拟私有云




## 虚拟私有云的优势

灵活配置

自定义虚拟私有网络，按需划分子网，配置 IP 地址段、路由表等服务。支持跨 AZ 部署弹性云服务器。

安全可靠

VPC 之间通过隧道技术进行 100%逻辑隔离，不同 VPC 之间默认不能通信。网络

ACL 对子网进行防护，安全组对云服务器、云容器、云数据库等实例进行防护，多重防护您的网络更安全。

互联互通

默认情况下，VPC 与公网是不能通信访问的，我们提供了弹性 IP、弹性负载均衡、NAT 网关、虚拟专用网络、云专线等多种方式连接公网。

默认情况下，两个 VPC 之间也是不能通信访问的，我们提供对等连接的方式，使用私有 IP 地址在两个 VPC 之间进行通信。

提供多种连接选择，满足企业云上多业务需求，让您轻松部署企业应用，降低企业 IT 运维成本。

高速访问

使用全动态 BGP 协议接入多个运营商，支持多达 21 条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅。

## 如何访问虚拟私有云

通过管理控制台、基于 HTTPS 请求的 API（Application Programming Interface）两种方式访问虚拟私有云。

管理控制台方式

管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录管理控制台，从主页选择“虚拟私有云”。

API 方式

如果用户需要将云平台上的虚拟私有云集成到第三方系统，用于二次开发，请使用 API 方式访问虚拟私有云。

## 虚拟私有云应用场景

通用性 Web 应用

在 VPC 中托管 Web 应用或网站，可以像使用普通网络一样使用 VPC。通过弹性 IP 连接弹性云主机与 Internet，运行弹性云主机上部署的 Web 应用程序。系统通过 VPN 网关与云端业务系统建立 VPN 通道，保证网站业务系统高速互通。

高安全性服务

将多层 Web 应用划分到不同的安全域中，按需在各个安全域中设置访问控制策略，可以通过创建一个 VPC，将 Web 服务器和数据库服务器划分到不同的安全组中。Web 服务器所在的子网实现互联网访问，而数据库服务器只能通过内网访问，保护数据库服务器的安全，满足高安全场景。

将公司网络扩展到云中

将 VPC 连接到企业内部的私有云中。通过 VPN 在传统数据中心与 VPC 之间建立通信隧道，可方便地 使用弹性云主机、块存储等资源；应用程序转移到云中、启动额外的 Web 服务器、增加网络的计算容量，从而实现企业的混合云架构，既降低了企业 IT 运维成本，又不用担心企业核心数据的扩散。VPC 能够跨 AZ 部署，提升了电商平台的高可用性。

VPC 连接

为了满足您不同场景下连接 Internet 的需求，云平台以 VPC 为基础提供了弹性 IP、弹性负载均衡、NAT 网关、虚拟专用网络、云专线等多种公网连接产品，降低部署难度，支撑您快速上云。

- 少量弹性云服务器通过弹性 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 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。

- 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 IP 管理成本过高，云平台 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 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 IP 直接暴露的风险。支持最大 100 万并发连接、3 万新建连接。DNAT 功能还可以实现端口级别的转发，将弹性 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 IP 和带宽面向互联网提供服务。

- 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。

- 自有 IDC 场景通过虚拟专用网络/云专线连接 Internet

  对于自建 IDC 机房的用户，由于利旧和平滑演进的原因，并非所有的业务都能放置在云上，这个时候就可以基于虚拟专用网络（VPN）或云专线（DC）产品，实现云上 VPC 与云下 IDC 之间的互联。VPN 走 Internet，公网的价格私网的享受。云专线走专属线路，带给您更高的传输效率和更私密的用户体验。

## 虚拟私有云其他服务的关系

弹性云主机

VPC 为弹性云主机构建隔离的、用户自主配置和管理的虚拟网络环境。提供多种方式连接弹性云主机与 Internet。同时，用户可以自定义安全组内与组间弹性云主机的访问规则，加强弹性云主机的安全保护。

弹性负载均衡

弹性负载均衡需要使用虚拟私有云服务创建的弹性 IP、带宽。

云监控

当用户开通了虚拟私有云服务后，无需额外安装其他插件，即可在云监控查看对应服务的实例状态。

## 用户权限

系统默认提供两种权限：用户管理权限和资源管理权限。用户管理权限可以管理用户、用户组及用户组的权限。资源管理权限可以控制用户对云服务资源执行的操作。

## 虚拟私有云相关术语解释

### 子网

子网是虚拟私有云内的 IP 地址块，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。同一个虚拟私有云下，子网网段不可重复。

默认情况下，同一个 VPC 的所有子网内的弹性云服务器均可以进行通信，不同 VPC 的弹性云服务器不能进行通信。

不同 VPC 的可通过创建对等连接通信，具体参见对等连接创建流程。

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。

VPC 支持的网段如下，子网的网段须在 VPC 网段范围内，且子网的掩码范围为：子网所在 VPC 掩码~29。

- 10.0.0.0/8~24

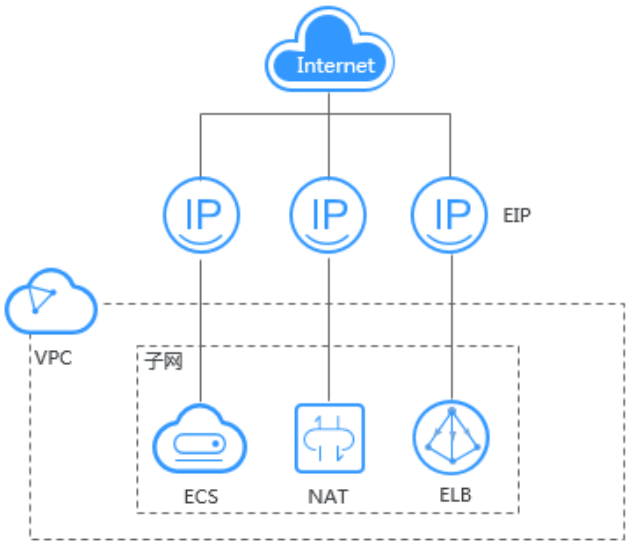
- 172.16.0.0/12~24
- 192.168.0.0/16~24

### 弹性 IP

弹性 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。

一个弹性 IP 只能绑定一个云资源使用。

**图2-2** 通过 EIP 访问公网




### 路由表

#### 相关背景

当前在部分区域中，路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，支持路由表与子网关联功能，请以实际界面为准。

未解耦：在虚拟私有云详情页的"路由表"页签，可对路由表进行操作。

已解耦：在进入"网络 > 虚拟私有云"后，在左侧导航栏直接选择"路由表"，可对路由表进行操作。

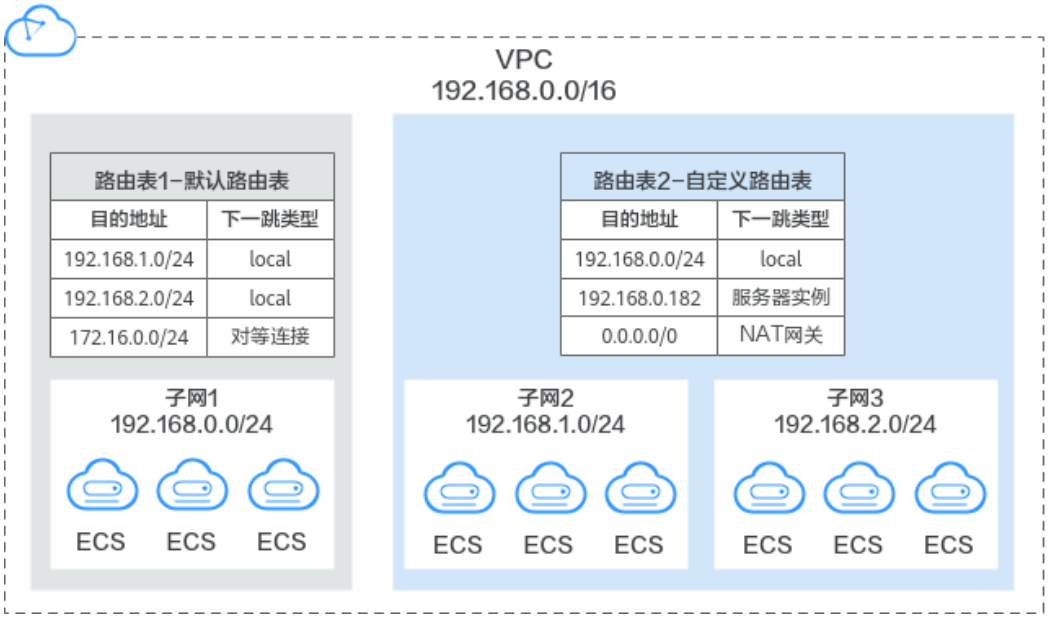
已解耦的区域请参考路由表(已解耦)、默认路由表和自定义路由表和路由的相关描

述。
未解耦的区域请参考路由表(未解耦)相关描述。

路由表(已解耦)

路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。VPC 中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。

图2-3 路由表




默认路由表和自定义路由表

用户创建虚拟私有云时，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。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，您可以将子网关联到自定义路由表或者复制该条路由到自定义路由表中，在自定义路由表中添加、修改和删除路由。
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。

**说明**

当前自定义路由表需提交工单申请，如需使用自定义路由表，请在创建路由表页面单击"申请扩大配额"。

路由

路由即路由规则，在路由中通过配置目的地址、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。

创建路由表后，系统会自动在路由表中添加如下的系统路由，表示 VPC 内实例互通。

目的地址是 100.64.0.0/10、198.19.128.0/20 的路由。

目的地址是子网网段的路由，包括 IPv4 和 IPv6 地址。

**说明**

除以上系统路由外，系统还会自动添加目的地址是 127.0.0.0/8 的路由，表示本地回环地址。

- 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。

  您可以通过添加自定义路由来自定义网络流量的走向，您需要指定目的地址、下一跳类型、下一跳地址。支持的下一跳类型如表 1-1 所示。

**表4-1** 下一跳类型

| 下一跳类型 | 说明 |
| --- | --- |
| 服务器实例 | 将指向目的地址的流量转发到虚拟私有云内的一台 ECS 实例。 |
| 扩展网卡 | 将指向目的地址的流量转发到虚拟私有云内的一台 ECS 实例的扩展网卡。 |
| VPN 网关 | 将指向目的地址的流量转发到一个 VPN 网关。 |
| 云专线网关 | 将指向目的地址的流量转发到一个云专线网关。 |
| NAT 网关 | 将指向目的地址的流量转发到一个 NAT 网关。 |
| 对等连接 | 将指向目的地址的流量转发到一个对等连接。 |
| 虚拟 IP | 将指向目的地址的流量转发到一个虚拟 IP 地址，可以通过该虚拟 IP 地址将流量转发到主备 ECS。 |
| VPC 终端节点 | 将指向目的地址的流量转发到一个 VPC 终端节点。 |

**说明**

- 当为默认路由表添加自定义路由时，下一跳类型不支持选择 VPN 网关与云专线网关。
- 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。

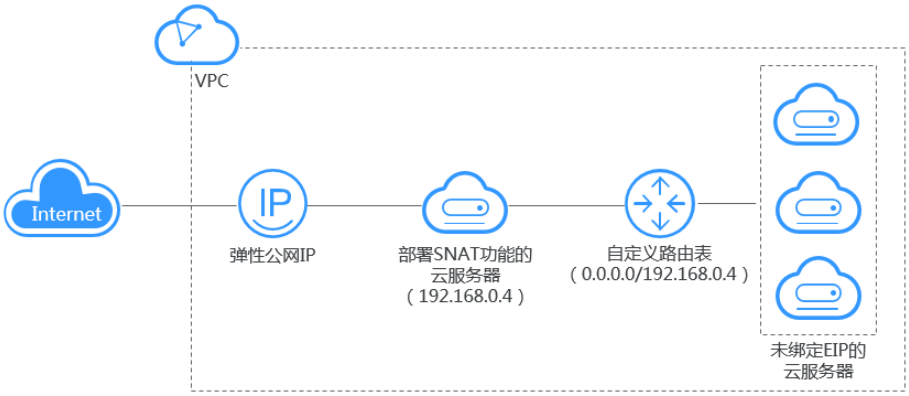
例如，创建 NAT GateWay 时，没有指定目的地址，系统会自动下发一条自定义类型的路由，可供用户自行调整。而创建 VPN 网关与云专线网关时，可以指定远端子网，也就是路由表的目的地址，系统将下发系统类型的路由。如果在路由表页面更改将会导致与对端数据不一致，您可以前往对端服务页面修改远端子网来调整路由表中的路由规则。

路由表(未解耦)

路由表是决定网络流量流向的规则集合。路由表允许用户添加自定义路由，使 VPC 内其他弹性云服务器通过绑定弹性 IP 的服务器访问 Internet 网络。
用户可以使用如下单点方式或者主备方式使用路由表功能通过绑定弹性 IP 的服务器访问 Internet 网络。

- 单点路由表场景如图 1-4 所示。

图2-4 单点路由表

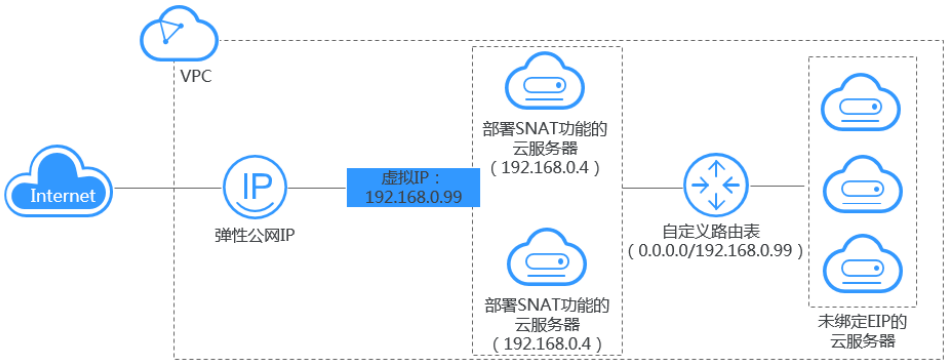



单点方式，VPC 内没有绑定弹性 IP 的弹性云服务器通过路由到一台绑定了弹性 IP 且具有 SNAT 功能的弹性云服务器访问 Internet。

单点方式通过为其他弹性云服务器所在的 VPC 增加路由表，使该 VPC 下的弹性云服务器可以访问 Internet，其中路由表的下一跳地址为绑定了弹性 IP 的弹性云服务器的私有 IP 地址（即 SNAT 服务器的私有 IP 地址）。

- 主备式路由表场景如图 1-5 所示。

图2-5 主备路由表




主备方式，VPC 内没有绑定弹性 IP 的弹性云服务器通过路由到一组分别绑定了弹性 IP 且具有 SNAT 功能的弹性云服务器访问 Internet。

主备方式通过为其他弹性云服务器所在的 VPC 增加路由表，使该 VPC 下的弹性云服务器可以访问 Internet，其中路由表的下一跳地址为两台绑定了弹性 IP 的弹性云服务器的虚拟 IP 地址。

单点方式和主备方式中，绑定了弹性 IP 的弹性云服务器需要具备 SNAT 功能，有关 SNAT 描述请参考 SNAT，如何配置弹性云服务器为 SNAT 服务器请参考配置 SNAT 服务器。

**须知**

- SNAT 需要您自行部署，具体部署参考配置 SNAT 服务器。
- 作为 SNAT 的弹性云服务器，只允许有一个网卡。
- 作为 SNAT 的弹性云服务器要关闭"源/目的检查"。

## SNAT

一些弹性云服务器不仅需要使用系统提供的服务，还需要访问外网以获取信息或下载软件。允许用户将弹性 IP 绑定到弹性云服务器的虚拟网卡（端口），从而使弹性云服务器能够与外网通信。但是，给弹性云服务器分配公网 IP 需要消耗稀缺资源（如 IPv4 地址），增加额外的成本，并有可能增加虚拟环境遭受攻击的几率。因此，多个弹性云服务器共享同一公网 IP 是一种可行的方法，具体实施方法为源地址转换（SNAT）。

云平台支持 SNAT 实例。为一个弹性云服务器配置公网 IP，该弹性云服务器作为来自同一子网或 VPC 的若干弹性云服务器的 SNAT 路由器/网关。
SNAT 实例配置参见配置 SNAT 服务器。

### 带宽

通过带宽展示网络的使用情况，作为服务计费的依据，同时，可以对已申请的弹性 IP 的带宽进行修改。

### 安全组

安全组是一个逻辑上的分组，为同一个 VPC 内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。系统会为每个用户默认创建一个安全组，默认安全组的规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的实例无需添加规则即可互相访问。

### 对等连接

对等连接是指两个 VPC 之间的网络连接。您可以使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。同一区域内，您可以在自己的 VPC 之间创建对等连接，也可以在自己的 VPC 与其他帐户的 VPC 之间创建对等连接。不同区域间的 VPC 之间不能创建对等连接。
通过对等连接连通同一个区域 VPC 时，一个租户在一个区域内的对等连接默认配额是 50 个。

- 同帐户的 VPC 对等连接：在一个区域内，您可以创建 50 个 VPC 对等连接。
- 跨账户的 VPC 对等连接：在一个区域内，已接受的 VPC 对等连接会占用双方帐户内的配额。处于待接受状的 VPC 对等连接占用发起方的配额，不占用接受方的配额。

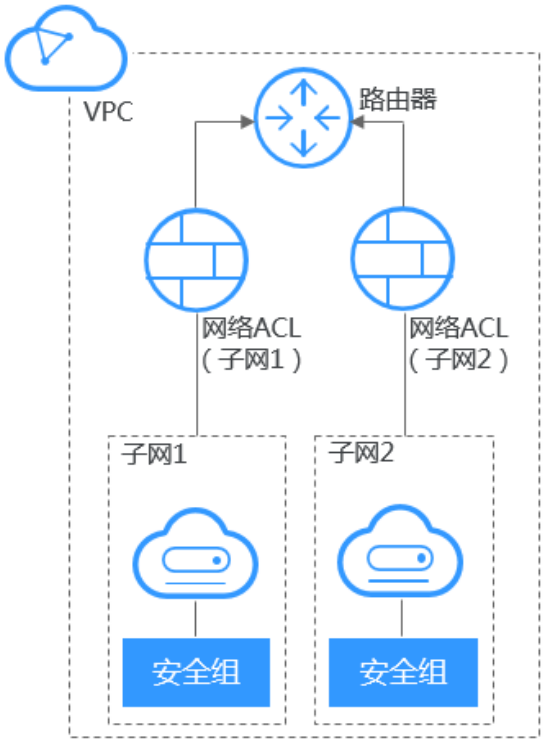
  您可以在配额范围内创建多个帐户下的 VPC 对等连接，比如帐号 A 和帐号 B 的 VPC 对等连接，帐号 A 和帐号 C 的 VPC 对等连接，帐号 A 和帐号 D 的 VPC 对等连接等等，不受帐号数量限制。

  对等连接的详细内容，具体参考 VPC 对等连接。

## 网络 ACL

网络 ACL 是对一个或多个子网的访问控制策略系统，根据与子网关联的入方向/出方向规则，判断数据包是否被允许流入/流出关联子网。

图2-6 安全组与网络 ACL




## IPv4/IPv6 双栈

IPv4/IPv6 双协议栈技术就是指在一个实例上同时启用 IPv4 协议栈和 IPv6 协议栈。如此，这个实例既能和 IPv4 网络通信，又能和 IPv6 网络通信。比如 VPC 内的一台云主机，它同时拥有 IPv4 地址和 IPv6 地址，并具备同时处理这两个协议地址的功能。

## 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 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 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。

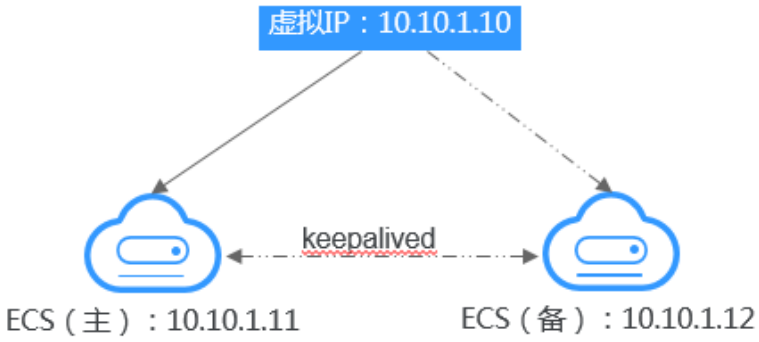
### 典型组网

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2-7 HA 高可用性模式组网图

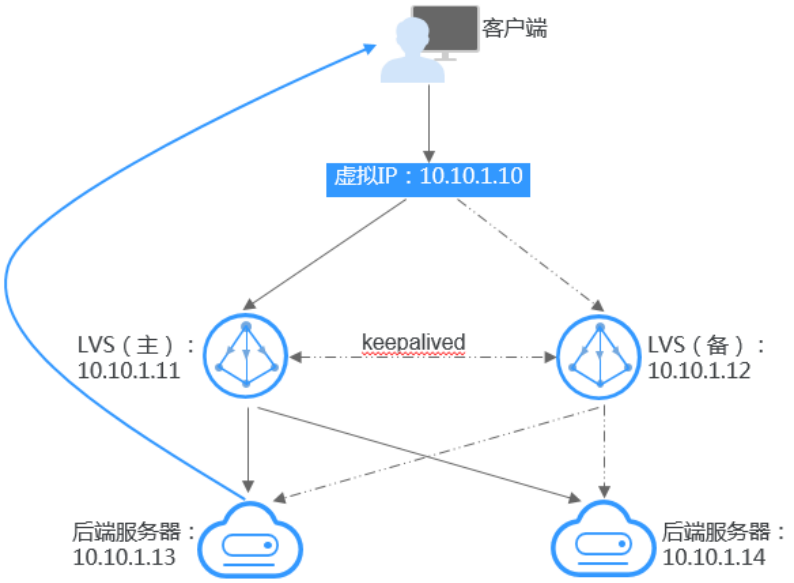



- 将 2 台同子网的弹性云服务器绑定同一个虚拟 IP。
- 将这 2 台弹性云服务器配置 Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived 可参考业内通用的配置方法，此处不做详细介绍。

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2-8 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。

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 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 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）。

## 区域与可用区

### 什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。

可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图 2-9 阐明了区域和可用区之间的关系。

图2-9 区域和可用区


### 如何选择区域?

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

### 如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

### 区域和终端节点

当您通过 API 使用资源时，您必须指定其区域终端节点。请向管理员获取区域和终端节点信息。

# 3 计费说明

### 产品规格和价格

免费提供。但虚拟私有云内的云主机、弹性 IP、公网带宽等产品会按照这些产品的收费标准进行收费。

VPN 价格请联系客户经理或拨打 400-810-9889 进行垂询。

# 4 快速入门

## 典型场景说明

虚拟私有云就是为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

当弹性云服务器无需访问公网时，例如用于搭建网站的数据库节点或服务器节点的弹性云服务器无需连接公网，该类型弹性云服务器的虚拟私有云配置请参考配置无需访问公网的弹性云服务器的 VPC。

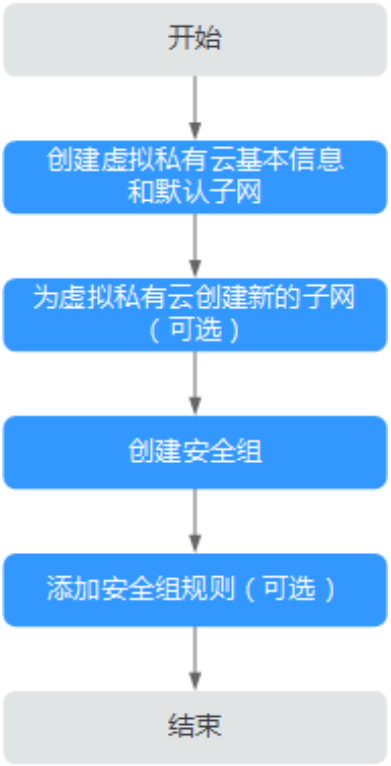
当弹性云服务器需要访问公网时可通过配置弹性 IP 实现，例如用于搭建网站时允许接受访客通过网络访问的业务节点，该类型弹性云服务器的虚拟私有云配置请参考配置通过弹性 IP 访问公网的弹性云服务器的 VPC。

# 配置无需访问公网的弹性云服务器的 VPC

## 简介

当弹性云服务器无需访问公网时，例如用于搭建网站的数据库节点或服务器节点的弹性服务器无需连接公网，虚拟私有云的配置流程如图 4-1 所示。

**图4-1** 配置网络功能




配置网络流程图说明如表 4-1 所示。

**表4-2** 配置流程说明

| 任务 | 说明 |
| --- | --- |
| 创建虚拟私有云基本信息和默认子网 | 必选任务。<br>创建虚拟私有云的基本信息及默认子网后还需要根据您的实际网络需求，继续创建虚拟私有云中的其他网络资源。 |
| 为虚拟私有云创建新的子网 | 可选任务。 |

| 任务 | 说明 |
| --- | --- |
| | 当默认子网不能满足您的需求时，您可以创建新的子网。<br>此处创建的子网就是创建弹性云服务器时添加的网卡。 |
| 创建安全组 | 必选任务。<br>您可以创建安全组，将虚拟私有云中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。<br>创建安全组成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的弹性云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。 |
| 添加安全组规则 | 可选任务。<br>安全组创建成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的弹性云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。 |

### 步骤 1：创建虚拟私有云基本信息及默认子网

#### 操作场景

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

要拥有一个完整的虚拟私有云，第一步请参考本章节任务创建虚拟私有云的基本信息及默认子网；然后再根据您的实际网络需求，参考后续章节继续创建子网、申请弹性 IP、安全组等网络资源。

#### 操作步骤

1. 登录管理控制台。

2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 单击“创建虚拟私有云”。
4. 在“创建虚拟私有云”页面，根据界面提示配置虚拟私有云参数。

   创建虚拟私有云时会同时创建一个默认子网，您还可以单击“添加子网”创建多个子网。

表4-3 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。 | - |
| 名称 | VPC 名称。<br>名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | VPC-test |
| 网段/IPv4 网段 | VPC 的地址范围，VPC 内的子网地址必须在 VPC 的地址范围内。<br>目前支持网段范围：<br>10.0.0.0/8~24<br>172.16.0.0/12~24<br>192.168.0.0/16~24<br>未开启 IPv4/IPv6 双栈的区域显示参数“网段”，开启 IPv4/IPv6 双栈的区域显示参数“IPv4 网段”。 | 192.168.0.0/16 |
| 标签 | 虚拟私有云的标识，包括键和值。可以为虚拟私有云创建 10 个标签。<br>标签的命名规则请参见表 3-4。 | 键：vpc_key1<br>值：vpc-01 |

表4-4 子网参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、"_"、"-"和"."组成，且不能有空格，长度不能大于 64 个字符。 | subnet-01 |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。<br>已申请 IPv6 公测的用户显示此配置项。 | 192.168.0.0/24 |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。 | 默认配置 |
| 网关 | 子网的网关。<br>通向其他子网的 IP 地址，用于实现与其他子网的通信。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| 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。单位：天。 | 365 天 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参见表 4-5。 | 键：subnet_key1<br>值：subnet-01 |

**表4-5** 虚拟私有云标签命名规则

| 参数 | 规则 | 样例 |
| --- | --- | --- |
| 键 | 不能为空。<br>对于同一虚拟私有云键值唯一。<br>长度不超过 36 个字符。<br>由英文字母、数字、下划线、中划线、中文字符组成。 | vpc_key1 |
| 值 | 长度不超过 43 个字符。<br>由英文字母、数字、下划线、点、中划线、中文字符组成。 | vpc-01 |

**表4-6** 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

## 步骤 2：为虚拟私有云创建新的子网

### 操作场景

申请 VPC 时会创建默认子网，当默认子网不能满足需求时，您可以创建新的子网。子网默认配置 DHCP 协议，即使用该 VPC 的弹性云服务器启动后，会通过 DHCP 协议自动获取到 IP 地址。

**说明**

当前在部分区域中，子网已从虚拟私有云中解耦，解耦后子网拥有独立入口。

- 未解耦：在虚拟私有云详情页的“子网”页签，可对子网进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。本小节的操作步骤指导以此入口为例。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“子网”。
4. 单击“创建子网”。
5. 根据界面提示配置参数。

表4-7 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 虚拟私有云 | 选择待创建子网的 VPC。<br>当“子网”独立存在于导航栏时，本参数可见。 | - |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | Subnet |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | 已申请 IPv6 公测的用户显示此配置项。 | |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。<br>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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。 | - |
| 网关 | 子网的网关。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| NTP 服务器地址 | NTP 时间服务器 IP 地址，非必填项。<br>您可以根据需要设置子网需要新增的 NTP 服务器 IP 地址，该地址不会影响默认 NTP 服务器地址。为空，表示不新增 NTP 服务器 IP 地址。<br>最多允许设置 4 个 IP 地址，每个 IP 地址以逗号隔开。 | 192.168.2.1 |
| 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。单位：天。<br>DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | 365 天 |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参考表 4-7。 | 键：subnet_key1<br>值：subnet-01 |

表4-8 子网标签命名规则

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

6. 单击“确定”。

## 注意事项

子网创建成功后，有 5 个系统保留地址您不能使用。以 192.168.0.0/24 的子网为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有 IP 地址范围开始，不作分配
- 192.168.0.1：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

如果您在创建子网时选择了自定义配置，系统保留地址可能与上面默认的不同，系统会根据您的配置进行自动分配。

## 步骤 3：创建安全组

## 操作场景

您可以创建安全组并定义安全组中的规则，比如，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。建议您将不同公网访问策略的弹性云服务器划分到不同的安全组。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击“创建安全组”。
5. 在“创建安全组”界面，根据界面提示配置参数，参数说明参考表 4-8。

**表4-9** 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 安全组的名称，必填项。<br>安全组的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。<br>说明<br>安全组名称创建后可以修改，建议不要重名。 | sg-318b |
| 描述 | 安全组的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 单击“确定”。

步骤 4：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，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器、云数据库等实例提供安全保护。

如果您的实例关联的安全组策略无法满足使用需求，比如需要新开放某个 TCP 端口，请参考本章节添加入方向规则，打开指定的 TCP 端口。

- 入方向：指从外部访问安全组规则下的实例。
- 出方向：指安全组规则下的实例访问安全组外的实例。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在入方向规则页签，单击“添加规则”，添加入方向规则。

   单击“+”可以依次增加多条入方向规则。

**表4-10** 入方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |
| 端口和源地址 | 端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1~65535。 | 22 或 22-30 |
| | 源地址：可以是 IP 地址、安全组。用于放通来自 IP 地址或另一安全组内的实例的访问。例如：<br>xxx.xxx.xxx.xxx/32（IPv4 地址）<br>xxx.xxx.xxx.0/24（子网）<br>0.0.0.0/0（任意地址）<br>sg-abc（安全组） | 0.0.0.0/0 |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 在出方向规则页签，单击“添加规则”，添加出方向规则。

   单击“+”可以依次增加多条出方向规则。

**表4-11** 出方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 端口和目的地址 | 端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1～65535。 | 22 或 22-30 |
| | 目的地址：可以是 IP 地址、安全组。允许访问目的 IP 地址或另一安全组内的实例。例如：<br>xxx.xxx.xxx.xxx/32（IPv4 地址）<br>xxx.xxx.xxx.0/24（子网）<br>0.0.0.0/0（任意地址）<br>sg-abc（安全组） | 0.0.0.0/0 |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含"<"和">"。 | - |

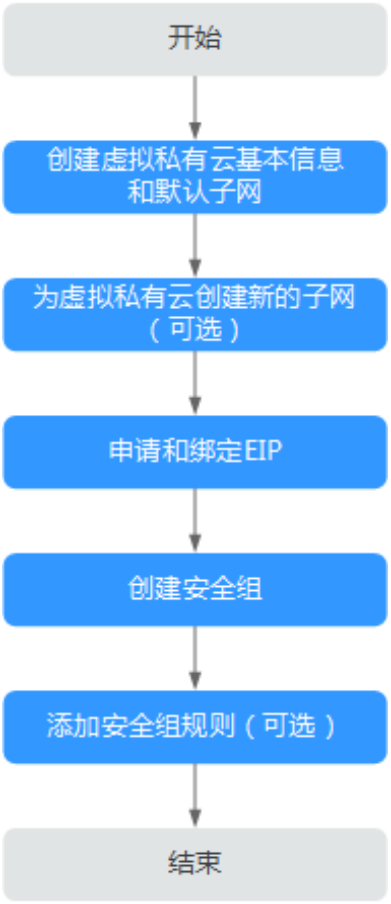
7. 单击"确定"。

## 配置通过弹性 IP 访问公网的弹性云服务器的 VPC

### 简介

当弹性云服务器需要访问公网时，例如用于搭建网站时允许接受访客通过网络访问的业务节点，可以通过绑定弹性 IP 来实现。具体的配置流程如图 4-2 所示。

图4-2 配置网络功能




配置网络流程图说明如表 4-11 所示。

表4-12 配置流程说明

| 任务 | 说明 |
| --- | --- |
| 创建虚拟私有云基本信息和默认子网 | 必选任务。<br>该任务是创建一个完整的虚拟私有云的第一步。<br>创建虚拟私有云的基本信息及默认子网后还需要根据您的实际网络需求，继续创建虚拟私有云中的其他网络资源。 |
| 为虚拟私有云创建新的子网 | 可选任务。<br>当默认子网不能满足您的需求时，您可以创建新的子网。<br>此处创建的子网就是创建弹性云服务器时添加的网 |

| 任务 | 说明 |
| --- | --- |
| | 卡。 |
| 申请和绑定弹性 IP | 必选任务。<br>可以通过申请弹性 IP 并将弹性 IP 绑定到弹性云服务器上，实现弹性云服务器访公网的目的。 |
| 创建安全组 | 必选任务。<br>您可以创建安全组，将虚拟私有云中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。<br>创建安全组成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的弹性云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。 |
| 添加安全组规则 | 可选任务。<br>安全组创建成功后，具备默认的访问规则。默认规则是在出方向上的数据报文全部放行，安全组内的弹性云服务器无需添加规则即可互相访问。当默认访问规则可以满足需求时，则无需单独再为该安全组添加安全组规则。 |

## 步骤 1：创建虚拟私有云基本信息及默认子网

### 操作场景

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。

要拥有一个完整的虚拟私有云，第一步请参考本章节任务创建虚拟私有云的基本信息及默认子网；然后再根据您的实际网络需求，参考后续章节继续创建子网、申请弹性 IP、安全组等网络资源。

### 操作步骤

1. 登录管理控制台。

2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 单击“创建虚拟私有云”。
4. 在“创建虚拟私有云”页面，根据界面提示配置虚拟私有云参数。

   创建虚拟私有云时会同时创建一个默认子网，您还可以单击“添加子网”创建多个子网。

表4-13 虚拟私有云参数说明

| 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。 | - |
| 名称 | VPC 名称。<br>名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | VPC-test |
| 网段/IPv4 网段 | VPC 的地址范围，VPC 内的子网地址必须在 VPC 的地址范围内。<br>目前支持网段范围：<br>10.0.0.0/8~24<br>172.16.0.0/12~24<br>192.168.0.0/16~24<br>未开启 IPv4/IPv6 双栈的区域显示参数“网段”，开启 IPv4/IPv6 双栈的区域显示参数“IPv4 网段”。 | 192.168.0.0/16 |
| 标签 | 虚拟私有云的标识，包括键和值。可以为虚拟私有云创建 10 个标签。<br>标签的命名规则请参见表 4-14。 | 键：vpc_key1<br>值：vpc-01 |

表4-14 子网参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、"_"、"-"和"."组成，且不能有空格，长度不能大于 64 个字符。 | subnet-01 |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。<br>已申请 IPv6 公测的用户显示此配置项。 | 192.168.0.0/24 |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。 | 默认配置 |
| 网关 | 子网的网关。<br>通向其他子网的 IP 地址，用于实现与其他子网的通信。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| 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。单位：天。 | 365 天 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参见表 4-15。 | 键：subnet_key1<br>值：subnet-01 |

**表4-15** 虚拟私有云标签命名规则

| 参数 | 规则 | 样例 |
| --- | --- | --- |
| 键 | 不能为空。<br>对于同一虚拟私有云键值唯一。<br>长度不超过 36 个字符。<br>由英文字母、数字、下划线、中划线、中文字符组成。 | vpc_key1 |
| 值 | 长度不超过 43 个字符。<br>由英文字母、数字、下划线、点、中划线、中文字符组成。 | vpc-01 |

**表4-16** 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

## 步骤 2：为虚拟私有云创建新的子网

### 操作场景

申请 VPC 时会创建默认子网，当默认子网不能满足需求时，您可以创建新的子网。子网默认配置 DHCP 协议，即使用该 VPC 的弹性云服务器启动后，会通过 DHCP 协议自动获取到 IP 地址。

**说明**

当前在部分区域中，子网已从虚拟私有云中解耦，解耦后子网拥有独立入口。

- 未解耦：在虚拟私有云详情页的"子网"页签，可对子网进行操作。
- 已解耦：在进入"网络 > 虚拟私有云"后，在左侧导航栏直接选择"子网"，可对子网进行操作。本小节的操作步骤指导以此入口为例。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择"网络 > 虚拟私有云"。
3. 在左侧导航栏选择"子网"。
4. 单击"创建子网"。
5. 根据界面提示配置参数。

**表4-17** 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 虚拟私有云 | 选择待创建子网的 VPC。<br>当"子网"独立存在于导航栏时，本参数可见。 | - |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、"_"、"-"和"."组成，且不能有空格，长度不能大于 64 个字符。 | Subnet |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | 已申请 IPv6 公测的用户显示此配置项。 | |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。<br>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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。 | - |
| 网关 | 子网的网关。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| NTP 服务器地址 | NTP 时间服务器 IP 地址，非必填项。<br>您可以根据需要设置子网需要新增的 NTP 服务器 IP 地址，该地址不会影响默认 NTP 服务器地址。为空，表示不新增 NTP 服务器 IP 地址。<br>最多允许设置 4 个 IP 地址，每个 IP 地址以逗号隔开。 | 192.168.2.1 |
| 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。单位：天。<br>DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | 365 天 |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参考表 4-17。 | 键：subnet_key1<br>值：subnet-01 |

表4-18 子网标签命名规则

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

6. 单击“确定”。

### 注意事项

子网创建成功后，有 5 个系统保留地址您不能使用。以 192.168.0.0/24 的子网为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有 IP 地址范围开始，不作分配
- 192.168.0.1：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

如果您在创建子网时选择了自定义配置，系统保留地址可能与上面默认的不同，系统会根据您的配置进行自动分配。

## 步骤 3：为弹性云服务器申请和绑定弹性 IP

### 操作场景

可以通过申请弹性 IP 并将弹性 IP 绑定到弹性云服务器上，实现弹性云服务器访问公网的目的。

### 申请弹性 IP

1. 登录管理控制台。

2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树，选择“弹性 IP 和带宽 > 弹性 IP”。
4. 在“弹性 IP”界面，单击“购买弹性 IP”。
5. 根据界面提示配置参数。

表4-19 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：<br>包年/包月<br>按需计费 | 按需计费 |
| 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。 | - |
| 计费方式 | 按带宽计费或按流量计费。 | 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 |
| 带宽名称 | 带宽的名称。 | bandwidth |
| 监控 | 用于开启弹性 IP 的基础监控。默认开启。<br>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。 | - |
| 购买量 | 选择包年包月计费模式时，需要选择购买时长。<br>选择按需计费模式时，需要选择弹性 IP 数量。 | 1 |

6. 单击“立即购买”。

### 绑定弹性 IP

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

## 步骤 4：创建安全组

### 操作场景

您可以创建安全组并定义安全组中的规则，比如，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。建议您将不同公网访问策略的弹性云服务器划分到不同的安全组。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击“创建安全组”。
5. 在“创建安全组”界面，根据界面提示配置参数，参数说明参考表 4-19。

**表4-20** 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 安全组的名称，必填项。<br>安全组的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。<br>说明<br>安全组名称创建后可以修改，建议不要重名。 | sg-318b |
| 描述 | 安全组的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“< | - |

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| | 和“>”。 | |

6. 单击“确定”。

### 步骤 5：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，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器、云数据库等实例提供安全保护。

如果您的实例关联的安全组策略无法满足使用需求，比如需要新开放某个 TCP 端口，请参考本章节添加入方向规则，打开指定的 TCP 端口。

- 入方向：指从外部访问安全组规则下的实例。
- 出方向：指安全组规则下的实例访问安全组外的实例。

#### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在入方向规则页签，单击“添加规则”，添加入方向规则。

   单击“+”可以依次增加多条入方向规则。

**表4-21** 入方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |
| 端口和源地址 | 端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1~65535。 | 22 或 22-30 |
| | 源地址：可以是 IP 地址、安全组。用于放通来自 IP 地址或另一安全组内的实例的访问。例如： | 0.0.0.0/0 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | xxx.xxx.xxx.xxx/32（IPv4 地址）<br>xxx.xxx.xxx.0/24（子网）<br>0.0.0.0/0（任意地址）<br>sg-abc（安全组） | |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 在出方向规则页签，单击“添加规则”，添加出方向规则。

   单击“+”可以依次增加多条出方向规则。

**表4-22** 出方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |
| 端口和目的地址 | 端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1～65535。 | 22 或 22-30 |
| | 目的地址：可以是 IP 地址、安全组。允许访问目的 IP 地址或另一安全组内的实例。例如：<br>xxx.xxx.xxx.xxx/32（IPv4 地址）<br>xxx.xxx.xxx.0/24（子网）<br>0.0.0.0/0（任意地址）<br>sg-abc（安全组） | 0.0.0.0/0 |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

7. 单击“确定”。

# 5 用户指南

## 虚拟私有云和子网

### 虚拟私有云

#### 创建虚拟私有云和子网

#### 操作场景

虚拟私有云可以为您的弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境。
要拥有一个完整的虚拟私有云，第一步请参考本章节任务创建虚拟私有云的基本信息及默认子网；然后再根据您的实际网络需求，参考后续章节继续创建子网、申请弹性 IP、安全组等网络资源。

#### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 单击“创建虚拟私有云”。
4. 在“创建虚拟私有云”页面，根据界面提示配置虚拟私有云参数。

创建虚拟私有云时会同时创建一个默认子网，您还可以单击"添加子网"创建多个子网。

**表5-1** 虚拟私有云参数说明

| 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。 | - |
| 名称 | VPC 名称。<br>名称只能由中文、英文字母、数字、"_"、"-"和"."组成，且不能有空格，长度不能大于 64 个字符。 | VPC-test |
| 网段/IPv4 网段 | VPC 的地址范围，VPC 内的子网地址必须 | 192.168.0.0/16 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | 在 VPC 的地址范围内。<br>目前支持网段范围：<br>• 10.0.0.0/8~24<br>• 172.16.0.0/12~24<br>• 192.168.0.0/16~24<br>未开启 IPv4/IPv6 双栈的区域显示参数"网段"，开启 IPv4/IPv6 双栈的区域显示参数"IPv4 网段"。 | |
| 标签 | 虚拟私有云的标识，包括键和值。可以为虚拟私有云创建 10 个标签。<br>标签的命名规则请参见表 5-3。 | • 键：vpc_key1<br>• 值：vpc-01 |

表5-2 子网参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、"_"、"-"和"."组成，且不能有空格，长度不能大于 64 个字符。 | subnet-01 |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。<br>已申请 IPv6 公测的用户显示此配置项。 | 192.168.0.0/24 |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数， | 默认配置 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | 包括网关、DNS 服务器地址等。 | |
| 网关 | 子网的网关。<br>通向其他子网的 IP 地址，用于实现与其他子网的通信。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| 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。单位：天。<br>DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | 365 天 |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参见表 5-4。 | • 键：subnet_key1<br>• 值：subnet-01 |

表5-3 虚拟私有云标签命名规则

| 参数 | 规则 | 样例 |
| --- | --- | --- |
| 键 | • 不能为空。<br>• 对于同一虚拟私有云键值唯一。<br>• 长度不超过 36 个字符。<br>• 由英文字母、数字、下划线、中划线、中文字符组成。 | vpc_key1 |
| 值 | • 长度不超过 43 个字符。<br>• 由英文字母、数字、下划线、点、中划线、中文字符组成。 | vpc-01 |

表5-4 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

## 修改虚拟私有云基本信息

### 操作场景

修改虚拟私有云的名称、网段。

例如：当虚拟私有云的 CIDR 和 VPN 地址有冲突时，可以通过修改虚拟私有云基本信息来调整 VPC 的地址范围。

### 约束与限制

修改 VPC 网段时需注意以下两点：

- 修改的 VPC 网段须在支持的网段内。当前 VPC 支持的网段有：10.0.0.0/8~24、172.16.0.0/12~24、192.168.0.0/16~24。
- 若该 VPC 下已有子网，修改网段必须包含所有子网网段。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中待修改的虚拟私有云所在行的“操作”列下单击“编辑网段”。
5. 在“编辑网段”页面，根据界面提示修改参数。可以修改虚拟私有云的名称、VPC 网段。
6. 单击“确定”。

## 删除虚拟私有云

### 操作场景

当无需使用网络资源，需要释放对应的虚拟私有云时，可以删除虚拟私有云。
删除 VPC 前，请确保 VPC 内的 IP 没有被占用，同时 VPC 内没有资源。
当 VPC 中存在子网、VPN、自定义路由或对等连接路由时，VPC 不能删除。需要删掉这些资源后，才能进行 VPC 删除。

- 删除子网请参见删除子网。
- 自定义路由删除请参考删除路由或删除路由。
- 删除对等连接请参见删除对等连接。

### 约束与限制

当存在弹性 IP 和安全组资源时，最后一个 VPC 不能删除。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
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”。
5. 单击“是”。

## 管理虚拟私有云标签

### 应用场景

私有云标签是虚拟私有云的标识。为虚拟私有云添加标签，可以方便用户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增加标签，或者在已经创建的虚拟私有云详情页添加标签，最多可以给虚拟私有云添加 10 个标签。
标签共由两部分组成：“键”和“值”，其中，“键”和“值”的命名规则如表 3-5 所示。

**表5-5** 虚拟私有云标签命名规则

| 参数 | 规则 | 样例 |
| --- | --- | --- |
| 键 | • 不能为空。<br>• 对于同一虚拟私有云键值唯一。<br>• 长度不超过 36 个字符。 | vpc_key1 |

| 参数 | 规则 | 样例 |
| --- | --- | --- |
| | • 由英文字母、数字、下划线、中划线、中文字符组成。 | |
| 值 | • 长度不超过 43 个字符。<br>• 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. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏单击“虚拟私有云”。
4. 单击虚拟私有云列表右上角的“标签搜索”，展开查询页。
5. 输入待查询虚拟私有云的标签键和值。
6. 键和值均不能为空，当键和值全匹配时，系统可以自动查询到目标虚拟私有云。
7. 单击“+”，添加下一个标签键和值。
8. 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。
9. 单击“搜索”。

系统根据标签键和值搜索目标虚拟私有云。

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. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏单击“虚拟私有云”。
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”。

### 导出虚拟私有云列表

#### 操作场景

您可以将当前帐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。

#### 操作步骤

1. 登录管理控制台。
2. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表页，单击右上角的  。

系统会将您帐号下，当前区域的所有虚拟私有云信息自动导出为 Excel 文件，并下载至本地。

## 子网

### 为虚拟私有云创建新的子网

#### 操作场景

申请 VPC 时会创建默认子网，当默认子网不能满足需求时，您可以创建新的子网。
子网默认配置 DHCP 协议，即使用该 VPC 的弹性云服务器启动后，会通过 DHCP 协议自动获取到 IP 地址。

**说明**

当前在部分区域中，子网已从虚拟私有云中解耦，解耦后子网拥有独立入口。

- 未解耦：在虚拟私有云详情页的“子网”页签，可对子网进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。本小节的操作步骤指导以此入口为例。

#### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“子网”。
4. 单击“创建子网”。
5. 根据界面提示配置参数。

表5-6 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 虚拟私有云 | 选择待创建子网的 VPC。<br>当“子网”独立存在于导航栏时，本参数可见。 | - |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | Subnet |
| 子网网段 | 子网的地址范围，需要在 VPC 的地址范围内。 | 192.168.0.0/24 |
| 子网 IPv4 网段 | 子网的地址范围，需要在 VPC 的地址范围内。<br>已申请 IPv6 公测的用户显示此配置项。 | 192.168.0.0/24 |
| 子网 IPv6 网段 | 选择是否勾选开启 IPv6。<br>已申请 IPv6 公测的用户显示此配置项。<br>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。 | - |
| 高级配置 | 单击下拉箭头，可配置子网的高级参数，包括网关、DNS 服务器地址等。 | - |
| 网关 | 子网的网关。 | 192.168.0.1 |
| 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。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| NTP 服务器地址 | NTP 时间服务器 IP 地址，非必填项。<br>您可以根据需要设置子网需要新增的 NTP 服务器 IP 地址，该地址不会影响默认 NTP 服务器地址。为空，表示不新增 NTP 服务器 IP 地址。<br>最多允许设置 4 个 IP 地址，每个 IP 地址以逗号隔开。 | 192.168.2.1 |
| 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。单位：天。<br>DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | 365 天 |
| 标签 | 子网的标识，包括键和值。可以为子网创建 10 个标签。<br>标签的命名规则请参考表 5-7。 | • 键：subnet_key1<br>• 值：subnet-01 |

表5-7 子网标签命名规则

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

6. 单击“确定”。

### 注意事项

子网创建成功后，有 5 个系统保留地址您不能使用。以 192.168.0.0/24 的子网为例，默认的系统保留地址如下：

- 192.168.0.0：网络标识符，私有 IP 地址范围开始，不作分配
- 192.168.0.1：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

如果您在创建子网时选择了自定义配置，系统保留地址可能与上面默认的不同，系统会根据您的配置进行自动分配。

## 修改子网网络信息

### 操作场景

本章节指导用户修改子网名称、DNS 服务器地址等。

**说明**

当前在部分区域中，子网已从虚拟私有云中解耦，解耦后子网拥有独立入口。

- 未解耦：在虚拟私有云详情页的“子网”页签，可对子网进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。本小节的操作步骤指导以此入口为例。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。

4. 在虚拟私有云列表中，单击需要修改子网的虚拟私有云名称。
5. 在“子网”列表待修改子网所在行，单击“修改”。根据界面提示修改参数。

表5-8 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 子网的名称。<br>名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | Subnet |
| DNS 服务器地址 | 默认配置了 2 个 DNS 服务器地址，您可以根据需要修改。多个 IP 地址以英文逗号隔开。 | 100.125.x.x |
| 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。单位：天。<br>DHCP 租约时间修改后，会在一段时间后自动生效（与您的 DHCP 租约时长有关），如果需要立即生效，请重启 ECS 或者在实例中主动触发 DHCP 更新。 | 365 天 |
| NTP 服务器地址 | NTP 时间服务器 IP 地址，非必填项。<br>您可以根据需要设置子网需要新增的 NTP 服务器 IP 地址，该地址不会影响默认 NTP 服务器地址。为空，表示不新增 NTP 服务器 IP 地址。 | 192.168.2.1 |

6. 单击“确定”。

## 删除子网

### 操作场景

当无需使用子网、需要释放网络资源时，可删除子网。

### 前提条件

在删除子网前，请确保子网内的 IP 没有被占用，同时子网内没有资源。
您可以通过控制台首页查看帐户下所有资源，根据子网信息排查各资源是否在待删除的子网中。先删除子网中的全部资源，再删除子网。
可参考以下常用的资源实例进行排查，具体请以帐户下资源为准。

- 弹性云服务器
- 裸金属服务器
- RDS 实例
- Workspace
- 弹性负载均衡器
- VPN
- 私有 IP 地址
- 自定义路由
- NAT 网关
- 终端节点与终端节点服务

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要删除子网的虚拟私有云名称。
5. 在“子网”界面待删除子网所在行，单击“删除”。
6. 单击“是”。

## 管理子网标签

### 应用场景

子网标签是子网的标识。为子网添加标签，可以方便用户识别和管理拥有的子网。您可以在创建子网时增加标签或者在已经创建的子网详情页添加标签，最多可以给子网添加 10 个标签。
标签共由两部分组成：“键”和“值”，其中，“键”和“值”的命名规则如表 5-9 所示。

**表5-9** 子网标签命名规则

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

**说明**

当前在部分区域中，子网已从虚拟私有云中解耦，解耦后子网拥有独立入口。

- 未解耦：在虚拟私有云详情页的“子网”页签，可对子网进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“子网”，可对子网进行操作。本小节的操作步骤指导以此入口为例。

## 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. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏单击“虚拟私有云”。
4. 在虚拟私有云列表中，单击待查询子网所在的虚拟私有云名称。
5. 单击子网列表右上角的“标签搜索”，展开查询页。
6. 输入待查询子网的标签值。
7. 键和值均不能为空，当键和值全匹配时，系统可以自动查询到目标子网。
8. 单击“+”，添加输入的标签值。
9. 系统支持添加多个标签值，并取各个标签值的交集，对目标子网进行搜索。
10. 单击“搜索”。
11. 系统根据标签的键和值搜索目标子网。

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. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏单击“虚拟私有云”。
4. 在虚拟私有云列表中，单击待查询子网所在的虚拟私有云名称。
5. 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”。

# IPv4/IPv6 双栈网络

## 什么是 IPv4/IPv6 双栈网络

IPv4/IPv6 双栈网络，表示为您的实例（例如 ECS）提供两个版本的的 IP 地址：IPv4 IP 地址和 IPv6 IP 地址，这两个 IP 地址都可以进行内网或者公网访问。以 ECS 为例，使用 IPv4/IPv6 双栈网络可实现以下功能：

- 使用 IPv4 私有 IP 地址，实现 ECS 在内网之间互访。
- 使用 IPv4 私有 IP 地址，通过绑定弹性公网 IP 的方式，实现 ECS 和公网之间互访。
- 使用 IPv6 IP 地址，实现双栈 ECS 在内网之间互访。
- 使用 IPv6 IP 地址，通过绑定带宽的方式，实现 ECS 和公网之间互访。

**说明**

创建子网时，勾选"开启 IPv6"，将自动为当前子网分配 IPv6 网段。

IPv4/IPv6 双栈网络的基本操作与之前的 IPv4 网络相同。只有部分页面的配置参数会略有差异，具体请以管理控制台显示为准。

## IPv6 网络的应用场景

**表5-10** IPv4/IPv6 双栈网络的应用场景及资源规划

| 应用场景 | 场景示例 | 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<br>• IPv6 网段 | • IPv4 私有地址：用于 IPv4 内网通信<br>• 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<br>• IPv6 网段 | • IPv4 私有地址+IPv4 EIP 地址：用于 IPv4 公网通信<br>• 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 | | |

表5-11 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<br>• IPv4 EIP 地址（开启 IPv6 转换）：用于 IPv4 和 IPv6 公网通信 |

图5-1 IPv6 网络应用场景及资源规划


## 基本操作

创建 IPv6 子网

参考为虚拟私有云创建新的子网创建子网，勾选“开启 IPv6”，将自动为子网分配 IPv6 网段。该功能一旦开启，将不能关闭。暂不支持自定义设置 IPv6 网段。

查看已使用 IPv6 地址

在子网列表中单击子网名称，在“已用 IP 地址”页签可以查看已经使用的 IPv4 地址和 IPv6 地址。

添加 IPv6 安全组规则

参考添加安全组规则添加安全组规则，类型选择"IPv6"，源地址或目的地址填写 IPv6 地址。

添加 IPv6 网络 ACL 规则

参考添加网络 ACL 规则添加网络 ACL 规则，类型选择"IPv6"，源地址或目的地址填写 IPv6 地址。

创建 IPv6 弹性 IP

您可以创建 IPv6 弹性 IP ，或者将已有 IPv4 弹性 IP 转换为 IPv6 弹性 IP。

添加 IPv6 弹性 IP/IPv6 双栈网卡到共享带宽

将 IPv6 弹性 IP、IPv6 双栈网卡添加到共享带宽。

添加 IPv6 自定义路由

参考添加自定义路由添加自定义路由，其中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。

**说明**

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，同时下一跳资源具备 IPv6 地址。

**说明**

IPv6 的虚拟 IP 仅支持绑定一个网卡（双栈网卡）。

动态获取 IPv6 地址

购买的 IPv6 双栈 ECS 实例后，您可以在 ECS 详情页查看自动分配的 IPv6 地址，也可以登录到 ECS，通过 ifconfig 查看分配的 IPv6 地址。

如果自动分配 IPv6 地址失败，或者您选的其他镜像不支持自动分配 IPv6 地址，请参考《弹性云服务器用户指南》的"动态获取 IPv6 地址"章节，手动获取 IPv6 地址。

**说明**

如果云服务器使用的是公共镜像，则支持情况如下：

Linux 公共镜像开启动态获取 IPv6 功能时，需要先判断是否支持 IPv6 协议栈，再判断是否已开启动态获取 IPv6。目前，所有 Linux 公共镜像均已支持 IPv6 协议栈，并且 Ubuntu 16 操作系统已默认开启动态获取 IPv6。即 Ubuntu 16 操作系统无需配置，其他 Linux 公共镜像需要执行开启动态获取 IPv6 的操作。

# 安全性

## 安全组

### 安全组简介

#### 安全组

安全组是一个逻辑上的分组，为同一个 VPC 内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。
系统会为每个用户默认创建一个默认安全组，默认安全组的规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的实例无需添加规则即可互相访问。默认安全组您可以直接使用，详情请参见默认安全组和规则。
您也可以根据需要创建自定义的安全组，请参见创建安全组。

#### 安全组基本信息

- 服务器及扩展网卡等实例可以关联一个或多个安全组。

  您可以更改与服务器、扩展网卡等实例关联的安全组。默认情况下创建实例时，除非您指定了其他安全组，否则实例与 VPC 的默认安全组关联。
- 如果您创建了放通同安全组的安全组规则，则允许安全组内实例互相访问。

  对于 IPv4 类型的地址，安全组只支持加入 32 位前缀的地址，对于 IPv6 类型的地址，安全组只支持加入 128 位前缀的地址。具体如何更改实例安全组，请参见实例加入/移出安全组。
- 安全组是有状态的。如果您从实例发送一个出站请求，且该安全组的出站规则是放通的话，那么无论其入站规则如何，都将允许该出站请求的响应流量流入。同理，如果该安全组的入站规则是放通的，那无论出站规则如何，都将允许入站请求的响应流量可以出站。

  安全组使用连接跟踪来跟踪有关进出实例的流量信息，将基于流量的连接状态应用规则以确定允许还是拒绝流量。在安全组规则增加、删除、更新时，或者该安全组下实例创建、删除时，会自动清除该安全组下所有实例入方向的连接跟踪，此时，流入或流出实例的流量会被当作新的连接，需要重新匹配相应入方向或出方向的安全组规则，以保证规则能立即生效，从而保障流入实例的流量的安全。

  除此以外，流入或流出实例的流量如果长时间没有报文，超过连接跟踪老化时间以后也会被当作新的连接需要重新匹配出、入方向规则。不同协议的连接跟踪老化时间不同，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一个或多个包，另一个方向没有收到包时，老化时间是 30s。对于除 TCP、UDP 或 ICMP 以外的协议，仅跟踪 IP 地址和协议编号。

**说明**

安全组需在网络互通的情况下生效。若实例属于不同 VPC，但同属于一个安全组，此时实例不能互通。您可以使用对等连接等产品建立 VPC 连接互通，安全组才能对不同 VPC 内实例的流量进行访问控制。

### 安全组规则

安全组创建后，您可以在安全组中设置出方向、入方向规则，这些规则会对安全组内部的实例出入方向网络流量进行访问控制，当实例加入该安全组后，即受到这些访问规则的保护。
每个安全组都自带默认安全组规则，详情请参见表 4-1。您也可以自定义添加安全组规则，请参见添加安全组规则。

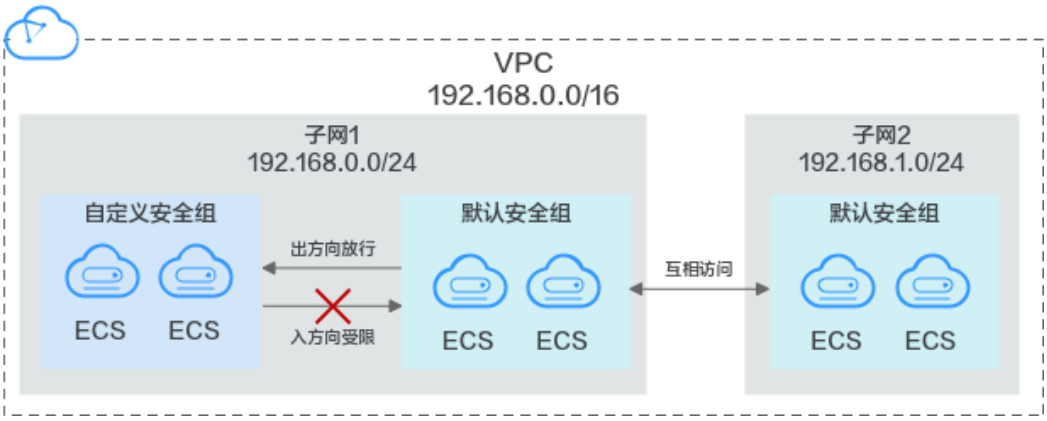
### 安全组的限制

- 默认情况下，一个用户可以创建 100 个安全组。
- 默认情况下，一个安全组最多只允许拥有 50 条安全组规则。
- 默认情况下，一个云服务器或扩展网卡最多只能被添加到 5 个安全组中，安全组规则取并集生效。
- 在创建私网弹性负载均衡时，需要选择弹性负载均衡所在的安全组。请勿删除默认规则或者确保满足以下规则：
  - 出方向：允许发往同一个安全组的报文可以通过，或者允许对端负载均衡器报文通过。
  - 入方向：允许来自同一个安全组的报文可以通过，或者允许对端负载均衡器报文通过。

### 默认安全组和规则

系统会为每个用户默认创建一个安全组，默认安全组的规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的实例无需添加规则即可互相访问。
默认安全组的放通规则如图 4-1 所示，以之间的访问为例。

图5-2 默认安全组




默认安全组规则如表 5-12 所示：

表5-12 默认安全组规则

| 方向 | 协议 | 端口范围 | 目的地址/源地址 | 说明 |
| --- | --- | --- | --- | --- |
| 出方向 | 全部 | 全部 | 目的地址：0.0.0.0/0 | 允许所有出站流量的数据报文通过。 |
| 入方向 | 全部 | 全部 | 源地址：当前安全组(例如：sg-*xxxxx*) | 仅允许安全组内的彼此通信，丢弃其他入站流量的全部数据报文。 |

## 安全组配置示例

介绍常见的安全组配置示例。如下示例中，出方向默认全通，仅介绍入方向规则配置方法。

- 允许外部访问指定端口
- 不同安全组内的弹性云服务器内网互通
- 仅允许特定 IP 地址远程连接弹性云服务器
- SSH 远程连接 Linux 弹性云服务器
- RDP 远程连接 Windows 弹性云服务器
- 公网 ping ECS 弹性云服务器
- 弹性云服务器作 Web 服务器
- 弹性云服务器作 DNS 服务器
- 使用 FTP 上传或下载文件

您需要提前准备好安全组，可以是默认的安全组，也可以是自定义创建的安全组，具体操作请参见创建安全组、添加安全组规则。

### 允许外部访问指定端口

- 场景举例：

  部署业务之后，为了让指定业务端口（例如：1100）可以被外部访问，您可以添加安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | TCP | 1100 | 0.0.0.0/0 |

### 不同安全组内的弹性云服务器内网互通

- 场景举例：

  在同一个 VPC 内，用户需要将某个安全组内一台弹性云服务器上的资源拷贝到另一个安全组内的弹性云服务器上时，用户可以将两台弹性云服务器设置为内网互通后再拷贝资源。

- 安全组配置方法：

  同一个 VPC 内，在同一个安全组内的弹性云服务器默认互通。但是，在不同安全组内的弹性云服务器默认无法通信，此时需要添加安全组规则，使得不同安全组内的弹性云服务器内网互通。

  在两台弹性云服务器所在安全组中分别添加一条入方向安全组规则，放通来自另一个安全组内的实例的访问，实现内网互通，安全组规则如下所示。

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | 设置内网互通时使用的协议类型 | 设置端口范围 | 另一个安全组的 ID |

### 仅允许特定 IP 地址远程连接弹性云服务器

- 场景举例：

  为了防止弹性云服务器被网络攻击，用户可以修改远程登录端口号，并设置安全组规则只允许特定的 IP 地址远程登录到弹性云服务器。

- 安全组配置方法：

  以仅允许特定 IP 地址（例如，192.168.20.2）通过 SSH 协议访问 Linux 操作系统的弹性云服务器的 22 端口为例，安全组规则如下所示。

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | SSH（22） | 22 | IPv4 CIDR 或者另一个安全组的 ID。<br>例如：192.168.20.2/32 |

### SSH 远程连接 Linux 弹性云服务器

- 场景举例：

  创建 Linux 弹性云服务器后，为了通过 SSH 远程连接到弹性云服务器，您可以添加安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | SSH（22） | 22 | 0.0.0.0/0 |

### RDP 远程连接 Windows 弹性云服务器

- 场景举例：

  创建 Windows 弹性云服务器后，为了通过 RDP 远程连接弹性云服务器，您可以添加安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | RDP（3389） | 3389 | 0.0.0.0/0 |

### 公网 ping ECS 弹性云服务器

- 场景举例：

  创建弹性云服务器后，为了使用 ping 程序测试弹性云服务器之间的通讯状况，您需要添加安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | ICMP | 全部 | 0.0.0.0/0 |

### 弹性云服务器作 Web 服务器

- 场景举例：

  如果您在弹性云服务器上部署了网站，即弹性云服务器作 Web 服务器用，希望用户能通过 HTTP 或 HTTPS 服务访问到您的网站，您需要在弹性云服务器所在安全组中添加以下安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | HTTP（80） | 80 | 0.0.0.0/0 |
| 入方向 | HTTPS（443） | 443 | 0.0.0.0/0 |

### 弹性云服务器作 DNS 服务器

- 场景举例：

  如果您将弹性云服务器设置为 DNS 服务器，则必须确保 TCP 和 UDP 数据可通过 53 端口访问您的 DNS 服务器。您需要在弹性云服务器所在安全组中添加以下安全组规则。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | TCP | 53 | 0.0.0.0/0 |
| 入方向 | UDP | 53 | 0.0.0.0/0 |

### 使用 FTP 上传或下载文件

- 场景举例：

  如果您需要使用 FTP 软件向弹性云服务器上传或下载文件，您需要添加安全组规则。

**说明**

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。

- 安全组配置方法：

| 方向 | 协议/应用 | 端口 | 源地址 |
| --- | --- | --- | --- |
| 入方向 | TCP | 20-21 | 0.0.0.0/0 |

## 创建安全组

### 操作场景

您可以创建安全组并定义安全组中的规则，比如，将 VPC 中的弹性云服务器划分成不同的安全域，以提升弹性云服务器访问的安全性。建议您将不同公网访问策略的弹性云服务器划分到不同的安全组。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击“创建安全组”。
5. 在“创建安全组”界面，根据界面提示配置参数，参数说明参考表 5-13。

表5-13 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 安全组的名称，必填项。<br>安全组的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。<br>说明<br>安全组名称创建后可以修改，建议不要重名。 | sg-318b |
| 描述 | 安全组的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 单击“确定”。

# 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，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器、云数据库等实例提供安全保护。
如果您的实例关联的安全组策略无法满足使用需求，比如需要新开放某个 TCP 端口，请参考本章节添加入方向规则，打开指定的 TCP 端口。

- 入方向：指从外部访问安全组规则下的实例。
- 出方向：指安全组规则下的实例访问安全组外的实例。

默认安全组规则请参见默认安全组和规则。常用的安全组规则配置示例请参见安全组配置示例。

## 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在入方向规则页签，单击“添加规则”，添加入方向规则。
   单击“+”可以依次增加多条入方向规则。

表5-14 入方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |
| 端口和源地址 | 端口：允许远端地址访问弹性云服务器指定端口，取值范围为：1～65535。 | 22 或 22-30 |
| | 源地址：可以是 IP 地址、安全组。用于放通来自 IP 地址或另一安全组内的实例的访问。例如：<br>• xxx.xxx.xxx.xxx/32（IPv4 地址）<br>• xxx.xxx.xxx.0/24（子网）<br>• 0.0.0.0/0（任意地址）<br>• sg-abc（安全组） | 0.0.0.0/0 |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 在出方向规则页签，单击“添加规则”，添加出方向规则。
   单击“+”可以依次增加多条出方向规则。

表5-15 出方向参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 协议/应用 | 网络协议。目前支持“All”、“TCP”、“UDP”、“ICMP”和“GRE”等协议。 | TCP |
| 端口和目的地址 | 端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1～65535。 | 22 或 22-30 |
| | 目的地址：可以是 IP 地址、安全组。允许访问目的 IP 地址或另一安全组内的实例。例如：<br>• xxx.xxx.xxx.xxx/32（IPv4 地址）<br>• xxx.xxx.xxx.0/24（子网）<br>• 0.0.0.0/0（任意地址）<br>• sg-abc（安全组） | 0.0.0.0/0 |
| 描述 | 安全组规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

7. 单击“确定”。

## 快速添加多条安全组规则

### 操作场景

系统提供了部分常用的协议端口，您可以一次性添加多条不同协议端口的安全组规则，满足您快速添加安全组规则的需求。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“配置规则”，进入安全组详情界面。
5. 在入方向规则页签，单击“快速添加规则”，同时添加多条不同协议端口的安全组入方向规则。
6. 在出方向规则页签，单击“快速添加规则”，同时添加多条不同协议端口的安全组出方向规则。
7. 单击“确定”。

## 复制安全组规则

### 操作场景

复制已有的安全组规则，然后生成一条新的安全组规则。复制时，支持自定义修改规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击安全组名，进入安全组详情界面。
5. 找到需要复制的安全组规则，单击规则所在行的“复制”。
   您可以根据需要修改安全组规则，然后快速生成一条新的安全组规则。
6. 单击“确定”。

## 修改安全组规则

### 操作场景

当安全组规则不能满足需要时，您可以修改安全组规则的端口号、协议、IP 地址等。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击安全组名，进入安全组详情界面。
5. 找到您想修改的安全组规则，单击规则所在行的“修改”。
6. 修改规则，单击“确认”。

## 删除安全组规则

### 操作场景

当安全组规则入方向、出方向源地址/目的地址有变化时，可以通过先删除安全组规则、之后重新添加安全组规则的方式进行安全组规则的更新。

**说明**

由于安全组规则是白名单规则，因此删除安全组规则后，可能会导致弹性云服务器的网络访问出现异常，请谨慎操作。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击安全组名，进入安全组详情界面。
5. 当不需要安全组规则时，单击规则所在行的“删除”。
6. 单击“是”。

**批量删除多条安全组规则**

您还可以同时勾选多条安全组规则，单击列表上方的“删除”，批量删除多条安全组规则。

## 导入/导出安全组规则

### 操作场景

如果您想将某个安全组的规则快速应用到另外一个安全组，或者批量修改当前安全组的规则，可以使用安全组规则的导入/导出功能来实现。

安全组的出方向、入方向规则导出为 Excel 格式的文件。

### 约束与限制

导出修改时，只能基于模板已有字段进行内容修改，不能新增字段和修改字段名称，否则会导入失败。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面，单击安全组名，进入安全组详情界面。
5. 导出/导入安全组规则。
   - 单击  ，将当前安全组规则导出为 Excel 文件。
   - 单击  ，将 Excel 文件中的安全组规则导入到当前安全组。

## 删除安全组

### 操作场景

本章节指导用户删除不需要的安全组。

### 约束与限制

- 系统自带的默认安全组不能删除。

- 当安全组被除服务器和扩展网卡之外的资源关联时，此安全组无法删除。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在“安全组”界面待删除的安全组所在行，选择“更多 > 删除”。
5. 单击“是”。

## 实例加入/移出安全组

### 操作场景

当您创建好安全组后，可以将加入到该安全组，使这些实例受到安全组的保护。当您不需要时，也可以从该安全组移出对应的。
支持批量添加、移出操作。

### 加入安全组

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“关联实例”。
5. 在“服务器”页签，单击“添加”，将一个或多个服务器加入到当前安全组中。
6. 在“扩展网卡”页签，单击“添加”，将一个或多个扩展网卡加入到当前安全组中。
7. 单击“确定”。

### 移出安全组

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航树选择“访问控制 > 安全组”。
4. 在安全组界面，单击操作列的“关联实例”。
5. 在“服务器”页签，找到需要移出的服务器，单击操作列的“移出”，将服务器从当前安全组中移出。
6. 在“扩展网卡”页签，找到需要移出的扩展网卡，单击操作列的“移出”，将扩展网卡从当前安全组中移出。
7. 单击“确定”。

**批量移出安全组**
同时勾选多个服务器，单击列表上方的“移出”，将多个服务器从当前安全组中全部移出。
同时勾选多个扩展网卡，单击列表上方的“移出”，将多个扩展网卡从当前安全组中全部移出。

## 查看弹性云服务器的安全组

### 操作场景

查看弹性云服务器所属的安全组出方向、入方向的规则详情。

### 操作步骤

1. 登录管理控制台。
2. 选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击弹性云服务器名称。
4. 选择“安全组”页签，查看弹性云服务器所属的安全组详情。

## 变更弹性云服务器的安全组

### 操作场景

变更弹性云服务器网卡所属的安全组。

### 操作步骤

1. 登录管理控制台。
2. 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。
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遵循几个安全组规则的并集。

   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”。

## 弹性云服务器常用端口

弹性云服务器常用端口如表 5-16 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。

表5-16 弹性云服务器常用端口

| 协议 | 端口 | 说明 |
| --- | --- | --- |
| FTP | 21 | FTP 服务上传和下载文件。 |
| SSH | 22 | 远程连接 Linux 弹性云服务器。 |
| Telnet | 23 | 使用 Telnet 协议远程登录弹性云服务器。 |
| HTTP | 80 | 使用 HTTP 协议访问网站。 |
| POP3 | 110 | 使用 POP3 协议接收邮件。 |
| IMAP | 143 | 使用 IMAP 协议接收邮件。 |
| HTTPS | 443 | 使用 HTTPS 服务访问网站。 |
| SQL Server | 1433 | SQL Server 的 TCP 端口，用于供 SQL Server 对外提供服务。 |
| SQL Server | 1434 | SQL Server 的 UDP 端口，用于返回 SQL Server 使用了哪个 TCP/IP 端口。 |
| Oracle | 1521 | Oracle 通信端口，弹性云服务器上部署了 Oracle SQL 需要放行的端口。 |
| MySQL | 3306 | MySQL 数据库对外提供服务的端口。 |
| Windows Server Remote Desktop Services | 3389 | 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。 |
| 代理 | 8080 | 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。 |
| NetBIOS | 137、138、139 | NetBIOS 协议常被用于 Windows 文件、打印机共享和 Samba。<br>• 137、138：UDP 端口，通过网上邻居传输文件时使用的端口。<br>• 139：通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。 |

**无法访问云平台某些端口**

**问题现象：**访问云平台特定端口，在部分地区部分运营商无法访问，而其他端口访问正常。

**问题分析：**部分运营商判断如下表的端口为高危端口，默认被屏蔽。

表5-17 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 9996 |
| UDP | 135~139 1026 1027 1028 1068 1433 1434 4789 5554 9996 |

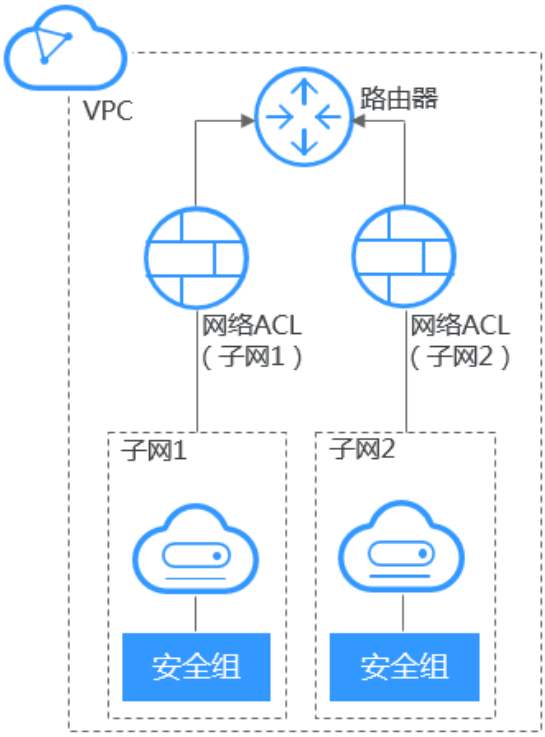
**解决方案：**建议您修改敏感端口为其他非高危端口来承载业务。

# 网络 ACL

## 网络 ACL 简介

网络 ACL 是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。如图 5-4 所示。

表5-18 安全组与网络 ACL




网络 ACL 与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络 ACL。安全组只有“允许”策略，但网络 ACL 可以“拒绝”和“允许”，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 与安全组的详细区别请参见安全组与网络 ACL 区别。

## 网络 ACL 基本信息

- 您的 VPC 默认没有网络 ACL。当您需要时，可以创建自定义的网络 ACL 并将其与子网关联。关联子网后，网络 ACL 默认拒绝所有出入子网的流量，直至添加放通规则。
- 网络 ACL 可以关联多个子网，但一个子网同一时间只能关联一个网络 ACL。
- 每个新创建的网络 ACL 最初都为未激活状态，直至您关联子网为止。

## 网络 ACL 默认规则

每个网络 ACL 都包含一组默认规则，如下所示：

- 默认放通同一子网内的流量。
- 默认放通目的 IP 地址为 255.255.255.255/32 的广播报文。用于配置主机的启动信息。
- 默认放通目的网段为 224.0.0.0/24 的组播报文。供路由协议使用。
- 默认放通目的 IP 地址为 169.254.169.254/32，TCP 端口为 80 的 metadata 报文。用于获取元数据。
- 默认放通公共服务预留网段资源的报文，例如目的网段为 100.125.0.0/16 的报文。
- 除上述默认放通的流量外，其余出入子网的流量全部拒绝，如表 4-7 所示。该规则不能修改和删除。

表5-19 网络 ACL 默认规则

| 方向 | 优先级 | 动作 | 协议 | 源地址 | 目的地址 | 说明 |
|---|---|---|---|---|---|---|
| 入方向 | * | 拒绝 | 全部 | 0.0.0.0/0 | 0.0.0.0/0 | 拒绝所有入站流量 |
| 出方向 | * | 拒绝 | 全部 | 0.0.0.0/0 | 0.0.0.0/0 | 拒绝所有出站流量 |

## 规则优先级

- 网络 ACL 规则的优先级使用“优先级”值来表示，优先级的值越小，优先级越高，最先应用。优先级的值为“*”的是默认规则，优先级最低。
- 多个网络 ACL 规则冲突，优先级高的规则生效，优先级低的不生效。若某个规则需要优先或落后生效，可在对应规则（需要优先或落后于某个规则生效的规则）前面或后面插入此规则。

## 应用场景

- 由于应用层需要对外提供服务，因此入方向规则必须放通所有地址，如何防止恶意用户的非正常访问呢？

  解决方案：通过网络 ACL 添加拒绝规则，拒绝恶意 IP 的访问。
- 隔离具有漏洞的应用端口，比如 Wanna Cry，关闭 445 端口

  解决方案：通过网络 ACL 添加拒绝规则，拒绝恶意协议和端口，比如 TCP：445 端口。
- 子网间东西向无防护诉求，仅有南北向的访问限制。

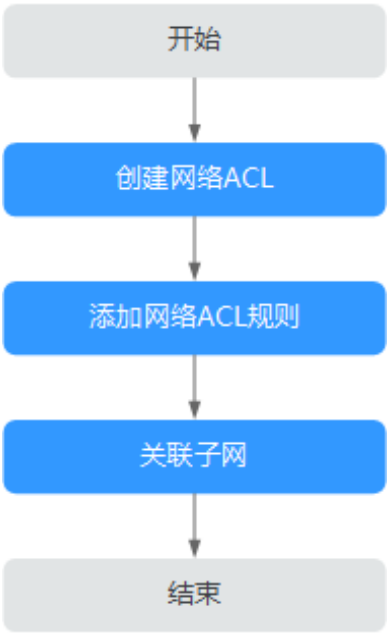
  解决方案：通过网络 ACL 设置南北向规则。
- 对访问频繁的应用，调整安全规则顺序，提高性能。

解决方案：网络 ACL 支持规则编排，可以把访问频繁的规则置顶。

## 网络 ACL 配置流程

子网配置网络 ACL 的流程，如图 4-3 所示。

图5-3 网络 ACL 配置流程




1. 参考创建网络 ACL 创建网络 ACL。
2. 参考添加网络 ACL 规则添加网络 ACL 规则。
3. 参考将子网和网络 ACL 关联将子网与网络 ACL 关联。子网关联后，网络 ACL 将自动开启并生效。

## 网络 ACL 配置示例

介绍常见的网络 ACL 配置示例。

- 拒绝特定端口访问
- 允许某些协议端口的访问

## 拒绝特定端口访问

在本示例中，假设要防止勒索病毒 Wanna Cry 的攻击，需要隔离具有漏洞的应用端口，例如 TCP 445 端口。您可以在子网层级添加网络 ACL 拒绝规则，拒绝所有对 TCP 445 端口的入站访问。

**网络 ACL 配置**

需要添加的入方向规则如表 5-18 所示。

表5-20 网络 ACL 规则

| 方向 | 动作 | 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 | 拒绝 | TCP | 0.0.0.0/0 | 1-65535 | 0.0.0.0/0 | 445 | 拒绝所有 IP 地址通过 TCP 445 端口入站访问 |
| 入方向 | 允许 | 全部 | 0.0.0.0/0 | 1-65535 | 0.0.0.0/0 | 全部 | 放通所有入站流量 |

**说明**

- 网络 ACL 默认拒绝所有入站流量，需先放通所有入站流量。
- 当添加了拒绝的规则，并且希望拒绝规则优先匹配时，需要将拒绝的规则放到允许规则的前面，匹配到拒绝规则的流量将会生效。具体操作请参见修改网络 ACL 规则生效顺序。

## 允许某些协议端口的访问

在本示例中，假设子网内的某个弹性云服务器做 Web 服务器，入方向需要放通 HTTP 80 和 HTTPS 443 端口，出方向全部放通。当子网开启网络 ACL 时，需要同时配置网络 ACL 和安全组规则。

**网络 ACL 配置**

需要添加的网络 ACL 入方向、出方向规则如表 5-19 所示。

表5-21 网络 ACL 规则

| 方向 | 动作 | 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 | 允许 | TCP | 0.0.0.0/0 | 1-65535 | 0.0.0.0/0 | 80 | 允许所有 IP 地址通过 HTTP 协议入站访问子网内的弹性云服务器的 80 端口 |
| 入方向 | 允许 | TCP | 0.0.0.0/0 | 1-65535 | 0.0.0.0/0 | 443 | 允许所有 IP 地址通过 HTTPS 协议入站访问子网内的弹性云服务器的 443 端口 |
| 出方向 | 允许 | 全部 | 0.0.0.0/0 | 全部 | 0.0.0.0/0 | 全部 | 允许子网内所有出站流量的数据报文通过 |

**安全组配置**

需要添加的安全组入方向、出方向规则如表 4-10 所示。

表5-22 安全组规则

| 方向 | 协议/应用 | 端口 | 源地址/目的地址 | 说明 |
|---|---|---|---|---|
| 入方向 | TCP | 80 | 源地址：0.0.0.0/0 | 允许所有 IP 地址通过 HTTP 协议 |

| 方向 | 协议/应用 | 端口 | 源地址/目的地址 | 说明 |
| --- | --- | --- | --- | --- |
| | | | | 入站访问安全组内的弹性云服务器的 80 端口 |
| 入方向 | TCP | 443 | 源地址：0.0.0.0/0 | 允许所有 IP 地址通过 HTTPS 协议入站访问安全组内的弹性云服务器的 443 端口 |
| 出方向 | 全部 | 全部 | 目的地址：0.0.0.0/0 | 允许安全组内所有出站流量的数据报文通过 |

网络 ACL 相当于一个额外的保护层，就算不小心配置了比较宽松的安全组规则，网络 ACL 规则也仅允许 HTTP 80 和 HTTPS 443 的访问，拒绝其他的入站访问流量。

## 创建网络 ACL

### 操作场景

您可以创建自定义网络 ACL。默认情况下，创建的网络 ACL 没有关联子网和出入规则且处于停用状态。每个用户默认可以创建 200 个网络 ACL。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在页面右侧区域，单击“创建网络 ACL”。
5. 在“创建网络 ACL”页面，根据提示，填写网络 ACL 参数，参数参见表 5-22。

**表5-23** 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 网络 ACL 的名称，必填项。<br>网络 ACL 的名称只能由中文、英文字母、数字、下划线、中划线组成，且不能有空格，长度不能大于 64 个字符。 | fw-92d3 |
| 描述 | 网络 ACL 的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含<、>符号。 | - |

6. 单击“确定”，完成创建。

## 添加网络 ACL 规则

### 操作场景

您可根据自身网络需求，在出方向和入方向添加相应规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击目标“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在入方向规则或出方向规则页签，单击“添加规则”，添加入方向或出方向规则。
   - 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5-24 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 策略 | 网络 ACL 策略。必选项，单击下拉按钮可选择。目前支持“允许”和“拒绝”。 | 允许 |
| 协议 | 网络 ACL 支持的协议。必选项，单击下拉按钮可选择。目前只支持选择 TCP、UDP、全部、ICMP 协议，当选择全部或者 ICMP 时，端口信息不可填写。 | TCP |
| 源地址 | 此方向允许的源地址。可以是 IP 地址、IP 地址段。<br>默认值为 0.0.0.0/0，代表支持所有的 IP 地址。<br>例如：<br>• xxx.xxx.xxx.xxx/32（IP 地址）<br>• xxx.xxx.xxx.0/24（子网）<br>• 0.0.0.0/0（任意地址） | 0.0.0.0/0 |
| 源端口范围 | 源端口范围，取值范围是 1～65535 的数字。表示某一范围时，两个数字必须以短划线分隔。例如，1-100。<br>选择 TCP 或 UDP 协议时必须填写。 | 22 或 22-30 |
| 目的地址 | 此方向允许的目的地址。可以是 IP 地址、IP 地址段。<br>默认值为 0.0.0.0/0，代表支持所有的 IP 地址。<br>例如：<br>• xxx.xxx.xxx.xxx/32（IP 地址） | 0.0.0.0/0 |

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| | • xxx.xxx.xxx.0/24（网段）<br>• 0.0.0.0/0（任意地址） | |
| 目的端口范围 | 目的端口范围，取值范围是介于 1～65535 的数字。表示某一范围时，两个数字必须以短划线分隔。例如，1-100。<br>选择 TCP 或 UDP 协议时必须填写。 | 22 或 22-30 |
| 描述 | 网络 ACL 规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含<、>符号。 | - |

6. 单击“确定”，添加网络 ACL 规则。

## 将子网和网络 ACL 关联

### 操作场景

当用户需进行子网关联时，可进入该网络 ACL 详情页面的添加关联子网。关联子网后，网络 ACL 默认拒绝所有出入子网的流量，直至添加放通规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要关联的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在详情页面，单击“关联子网”页签。
6. 在“关联子网”页签区域，单击“关联”按钮，弹出添加关联子网页面。
7. 在弹出的关联子网页面，勾选需要进行关联的子网，单击“确定”，完成子网关联。

**说明**

已关联网络 ACL 的子网将不会展示在添加关联子网页面中，即暂不支持一键式解绑子网与关联子网操作，若用户需要关联已绑定网络 ACL 的子网，需要先解除绑定再进行关联。

## 解除关联子网

### 操作场景

您可根据自身网络需求，解除网络 ACL 与子网关联。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要修改的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在详情页面，单击“关联子网”页签。
6. 在“关联子网”页签详情区域，选择对应子网的“操作”列，单击“取消关联”。
7. 单击“是”。

**批量解除关联子网**

同时勾选多个子网，单击列表上方的“取消关联子网”，将多个子网从当前网络 ACL 中全部移出。

## 修改网络 ACL 规则生效顺序

### 操作场景

若某个规则需要优先或落后生效，可在对应规则（需要优先或落后于某个规则生效的规则）前面或后面插入此规则。

多个网络 ACL 规则冲突，更靠前的规则生效，优先级低的不生效。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要修改的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在入方向规则或出方向规则页签，选择需要优先或落后生效规则的“操作”列，单击“更多 > 向前插规则”或“更多 > 向后插规则”。
6. 根据弹出框提示，填写需要插入规则的参数，单击“确定”插入规则。

## 修改网络 ACL 规则

### 操作场景

您可根据自身网络需求，修改出方向和入方向的规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。

3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要修改的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在入方向规则或出方向规则页签，单击“操作”列的“修改”，根据界面提示修改相关参数。参数说明参见表 5-25。

表5-25 参数说明

| 参数 | 参数说明 | 取值样例 |
| --- | --- | --- |
| 策略 | 网络 ACL 策略。必选项，单击下拉按钮可选择。目前支持“允许”和“拒绝”。 | 允许 |
| 协议 | 网络 ACL 支持的协议。必选项，单击下拉按钮可选择。目前只支持选择 TCP、UDP、全部、ICMP 协议，当选择全部或者 ICMP 时，端口信息不可填写。 | TCP |
| 源地址 | 此方向允许的源地址。可以是 IP 地址、IP 地址段。<br>默认值为 0.0.0.0/0，代表支持所有的 IP 地址。<br>例如：<br>• xxx.xxx.xxx.xxx/32（IP 地址）<br>• xxx.xxx.xxx.0/24（子网）<br>• 0.0.0.0/0（任意地址） | 0.0.0.0/0 |
| 源端口范围 | 源端口范围，取值范围是 1～65535 的数字。表示某一范围时，两个数字必须以短划线分隔。例如，1-100。<br>选择 TCP 或 UDP 协议时必须填写。 | 22 或 22-30 |
| 目的地址 | 此方向允许的目的地址。可以是 IP 地址、IP 地址段。<br>默认值为 0.0.0.0/0，代表支持所有的 IP 地址。<br>例如：<br>• xxx.xxx.xxx.xxx/32（IP 地址）<br>• xxx.xxx.xxx.0/24（网段）<br>• 0.0.0.0/0（任意地址） | 0.0.0.0/0 |
| 目的端口范围 | 目的端口范围，取值范围是介于 1～65535 的数字。表示某一范围时，两个数字必须以短划线分隔。例如，1-100。<br>选择 TCP 或 UDP 协议时必须填写。 | 22 或 22-30 |
| 描述 | 网络 ACL 规则的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含<、>符号。 | - |

6. 单击“确定”，修改网络 ACL 规则。

## 开启/关闭网络 ACL 规则

### 操作场景

您可根据自身网络需求，开启或关闭已创建的出方向和入方向的规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要修改的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在入方向规则或出方向规则页签，单击“操作”的“开启”或者“关闭”。
6. 单击“是”，确认开启或关闭此规则。

## 删除网络 ACL 规则

### 操作场景

您可根据自身网络需求，删除已创建的出方向和入方向的规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧在“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您需要修改的“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在入方向规则或出方向规则页签，单击“操作”列的“删除”。
6. 单击“是”。

## 查看网络 ACL

### 操作场景

您可以随时查看已创建网络 ACL 的详细信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。

3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您对应“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在详情页面，单击“入方向规则”、“出方向规则”、“关联子网”页签可查看详细的入方向、出方向、关联子网的详细信息。

## 修改网络 ACL

### 操作场景

您可根据自身网络需求，修改已创建的网络 ACL 的名称、描述。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧“网络 ACL”列表区域，选择网络 ACL 的名称列，单击您对应“网络 ACL 名称”进入网络 ACL 详情页面。
5. 在详情页面，单击“名称”后的  ，编辑网络 ACL 名称。
6. 单击“√”，保存网络 ACL 名称。
7. 单击“描述”后的  ，编辑网络 ACL 说明内容。
8. 单击“√”，保存网络 ACL 描述。

## 开启/关闭网络 ACL

### 操作场景

网络 ACL 创建成功后，用户可以根据自身网络需求，选择是否启用或关闭此网络 ACL。启用网络 ACL 前，请确认网络 ACL 已添加关联子网和出入网络 ACL 的规则。
关闭网络 ACL 后，用户自定义的规则将失效，只有网络 ACL 的默认规则有效。此操作可能会导致网络流量中断，请谨慎操作。网络 ACL 的默认规则请参见网络 ACL 默认规则。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧“网络 ACL”列表区域，选择对应网络 ACL 的“操作”列，单击“更多 > 开启”或“更多 > 关闭”，启用或关闭此网络 ACL。
5. 根据弹出框中警告信息，单击“是”，确认启动或关闭此网络 ACL。

## 删除网络 ACL

### 操作场景

您可以随时删除已创建网络 ACL。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“访问控制 > 网络 ACL”。
4. 在右侧在“网络 ACL”列表区域，选择网络 ACL 的“操作”列，单击“更多 > 删除”。
5. 单击“是”，删除网络 ACL。

**说明**

删除网络 ACL 同时解除与网络 ACL 关联的子网，删除网络 ACL 中已添加的规则。

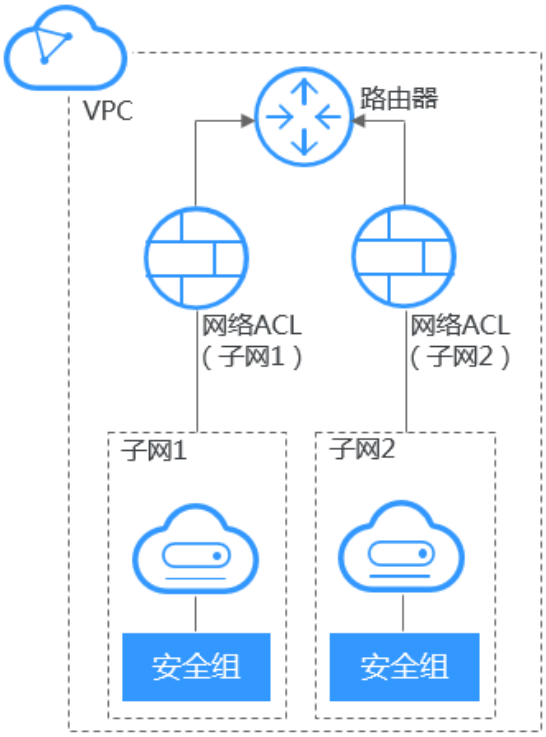
## 安全组与网络 ACL 区别

通过配置网络 ACL 和安全组策略，保障 VPC 内的弹性云服务器安全使用。

- 安全组对弹性云服务器进行防护。
- 网络 ACL 对子网进行防护。

如图 5-4 所示。

图5-4 安全组与网络 ACL




网络 ACL 和安全组区别如表 5-26 所示。

表5-26 安全组和网络 ACL

| 对比项 | 安全组 | 网络 ACL |
| --- | --- | --- |
| 防护对象 | 弹性云服务器级别操作。 | 子网级别操作。 |
| 配置策略 | 仅支持允许策略。 | 支持允许、拒绝策略。 |
| 优先级 | 多个规则冲突，取其并集生效。 | 多个规则冲突，优先级高的规则生效，优先级低的不生效。 |
| 应用操作 | 创建弹性云服务器默认必须选择安全组，默认安全组自动应用到弹性云服务器。 | 创建子网没有网络 ACL 选项，必须创建网络 ACL、添加关联子网、添加出入规则，并启用网络 ACL，才可应用到关联子网及子网下的弹性云服务器。 |
| 报文组 | 仅支持报文三元组（即协议、端口和对端地址）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。 |

# 弹性 IP 管理

## 申请弹性 IP

1、登录天翼云控制中心；

2、在系统首页，单击【网络 > 虚拟私有云】；

3、在【弹性 IP】界面，单击【申请弹性 IP】；

4、在【申请弹性 IP】下拉区域，根据界面提示配置参数；


参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 带宽的名称 | Subnet |
| 带宽 | 带宽大小 | 100 |
| 数量 | 弹性IP数量 | 1 |

说明：带宽只限制出方向的大小，入方向带宽当前不做限制。

5、单击【立即购买】。

6、确认订单并阅读服务协议后，勾选同意服务协议并单击【立即申请】。

7、弹性 IP 购买后只能升级，不支持降级操作。

## 绑定弹性 IP

将弹性 IP 地址绑定到弹性云主机上，可以实现弹性云主机访问公网的目的。

1、在【弹性 IP】界面待绑定弹性 IP 地址所在行，单击【绑定】；

2、在【绑定 IP】界面，点击【选择云服务器】，并选择需绑定的云主机和云主机网卡；

3、单击【确定】。

## 解除弹性 IP

1. 登录天翼云控制中心；
2. 在系统首页，单击【网络 > 虚拟私有云】；
3. 在【弹性 IP】界面，单击【申请弹性 IP】；
4. 在弹性 IP 购买页面，根据界面提示配置参数；
5. 在【弹性 IP】界面待解绑定弹性 IP 地址所在行，单击【解绑定】。


说明：在弹性负载均衡服务下创建并绑定的弹性 IP 地址，在虚拟私有云的弹性 IP 地址列表中可以显示，但是不能进行解绑定操作。

## 删除弹性 IP

1. 在【弹性 IP】界面待绑定弹性 IP 地址所在行，单击【释放】；

2. 在【删除弹性 IP】弹出框，点击【确认】。


说明：

- 未绑定的弹性 IP 地址才可释放，已绑定的弹性 IP 地址需要先解绑定后才能释放。
- 在弹性负载均衡服务下创建并绑定的弹性 IP 地址，在虚拟私有云的弹性 IP 地址列表中可以显示，但是不能进行释放操作。

# IPv4/IPv6 双栈管理

## 创建 IPv4/IPv6 双栈子网

1. 登录控制中心；

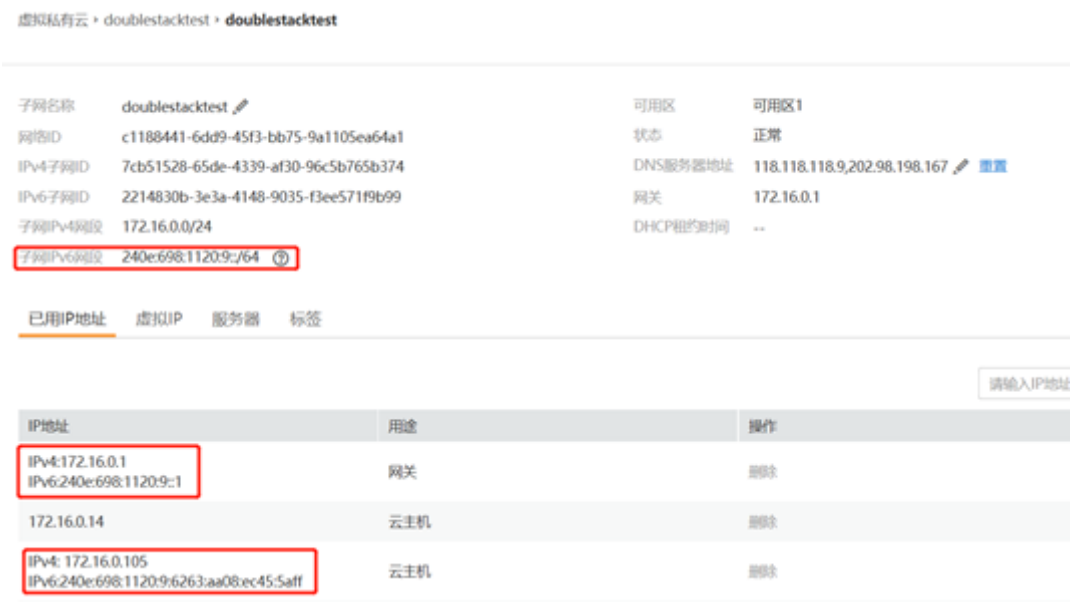
2. 在系统首页，单击【网络 > 虚拟私有云】；

3. 选择需要创建子网的 VPC，并单击【子网】，在【子网】页签，单击【创建子网】；


4. 在【创建子网】下拉区域，根据界面提示配置参数；

5. 勾选“开启 IPv6”，将自动为子网分配 IPv6 网段。该功能一旦开启，将不能关闭。暂不支持自定义设置 IPv6 网段。如下图：


6. 在子网列表中单击子网名称，在“已用 IP 地址”页签可以查看已经使用的 IPv4 地址和 IPv6 地址。



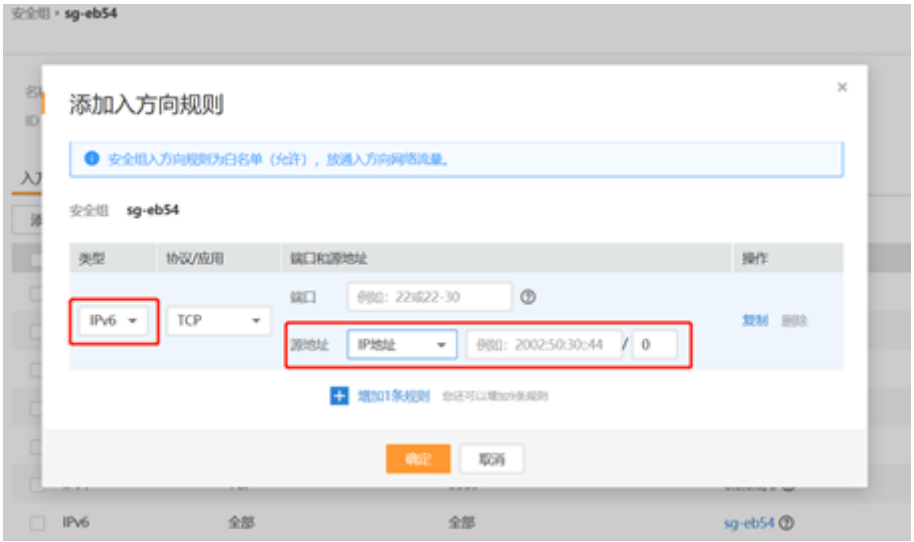

## 添加 IPv4/IPv6 双栈网卡到共享带宽

添加 IPv6 弹性公网 IP/IPv6 双栈网卡到共享带宽


参考“添加弹性 IP 到共享带宽”，在共享带宽详情页中选择“IPv6 双栈网卡”→“添加”，选择相应的 VPC、子网和双栈网卡即可将 IPv6 双栈网卡添加到共享带宽。

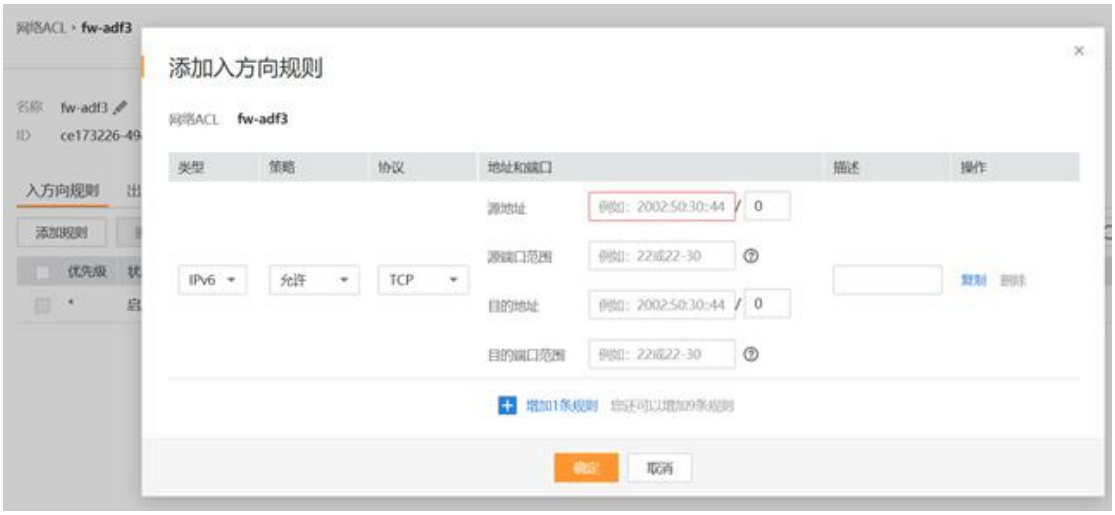
## 设置 IPv4/IPv6 双栈管理安全组

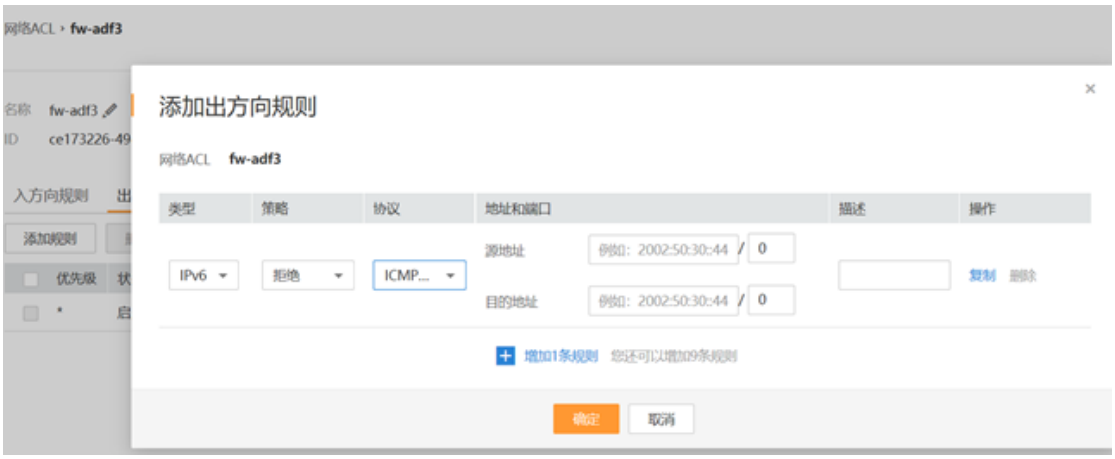
在“网络控制台”→“访问控制”→“安全组”中，可点击安全组名称进行 IPv6 出、入方向规则设置。具体可参考“添加安全组规则”部分，并在类型选择“IPv6”,源地址或目的地址填写 IPv6 地址。




为 IPv4/IPv6 双栈网络配置 ACL

在【网络控制台】→【访问控制】→【网络 ACL】中，可配置 IPv6 的出入方向规则






添加 IPv6 自定义路由

添加 IPv6 自定义路由的方式与 IPv4 相同，只需在添加路由信息时输入 IPv6 地址即可，如下图：

# 虚拟 IP

## 虚拟 IP 简介

### 什么是虚拟 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 IP、VPN、云专线等网络接入。

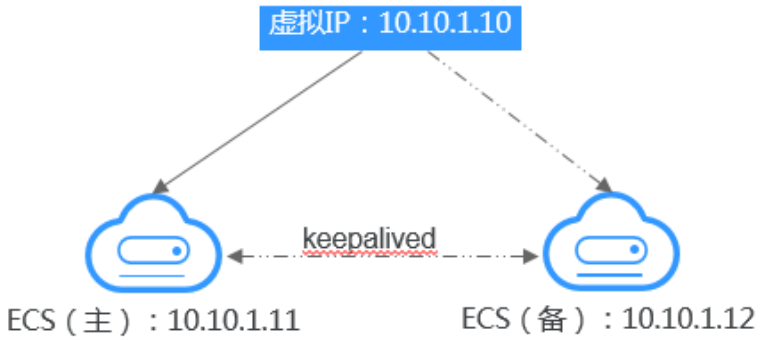
多个主备部署的弹性云服务器可以在绑定虚拟 IP 地址时选择同一个虚拟 IP 地址。用户可以为该虚拟 IP 地址绑定一个弹性 IP 地址，从互联网可以访问后端绑定了同一个虚拟 IP 地址的多个主备部署的弹性云服务器，增强容灾性能。

### 典型组网

虚拟 IP 主要用在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。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。

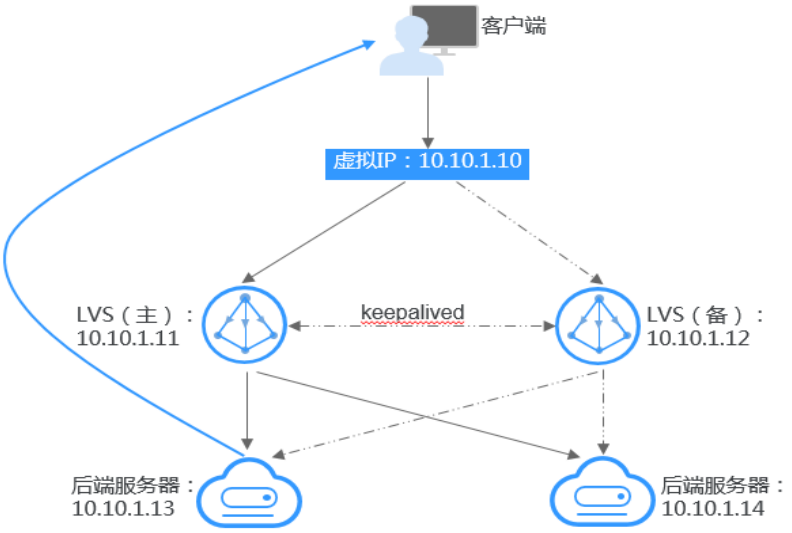



  - 将 2 台同子网的弹性云服务器绑定同一个虚拟 IP。

- 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。




- 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。
- 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；若采用接口调用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 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 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）。

### 约束与限制

- 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 仅能绑定到同一个子网下的云服务器
- 备弹性云服务器需要关闭 IP 转发功能。确认方式如下：

a. 登录弹性云服务器执行如下命令，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，执行 b 和 c 关闭 IP 转发功能。
- 回显为 0，操作完成。

b. 使用 vi 打开"/etc/sysctl.conf"文件，修改 net.ipv4.ip_forward = 0，按":wq"保存退出。或使用 sed 命令修改，参考命令如下：

   sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf

c. 执行如下命令，使修改生效。

   sysctl -p /etc/sysctl.conf

- 虚拟 IP 仅支持绑定一个弹性 IP。
- 建议一个 ECS 绑定的虚拟 IP 不要超过 8 个。
- 建议一个虚拟 IP 绑定的 ECS 不要超过 10 个。
- IPv6 的虚拟 IP 仅支持绑定一个网卡（双栈网卡），如需进行服务器的主备切换，请通过调用 API 方式。

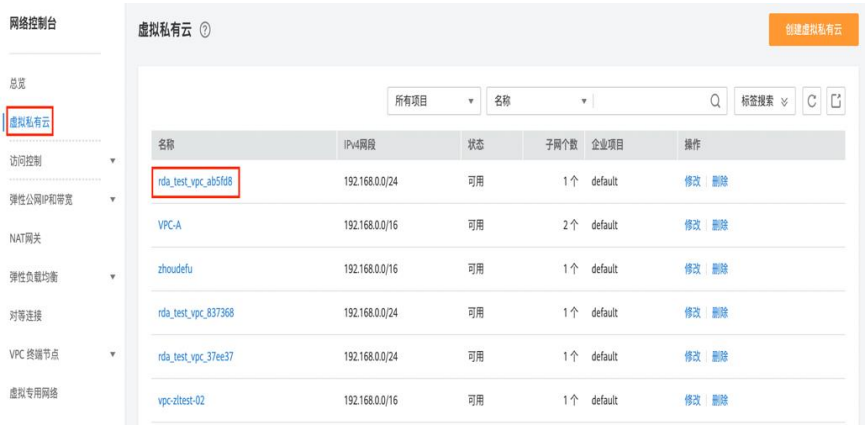
## 申请虚拟 IP 地址

### 操作场景

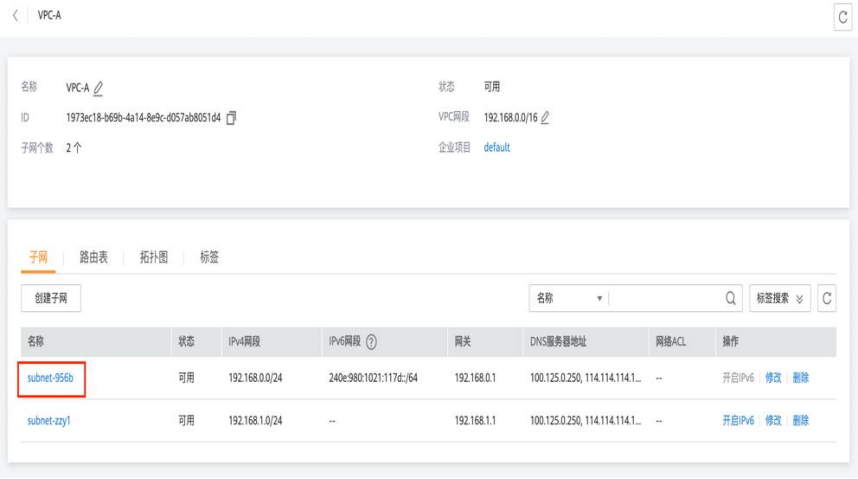
当弹性云服务器需要设置虚拟 IP 地址或预留指定的虚拟 IP 地址时，可以通过给子网申请虚拟 IP 地址的方式分配虚拟 IP 地址。

操作步骤

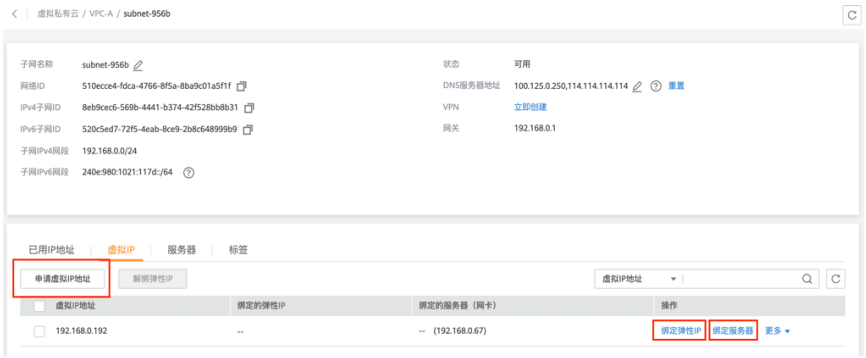
1. 登录管理控制台。
2. 在系统首页，选择【网络>—虚拟私有云】。
3. 在左侧导航栏选择【虚拟私有云】。
4. 在虚拟私有云列表中，单击需要申请虚拟 IP 地址的子网所在的虚拟私有云名称。




5. 在【子网】页签中，单击需要申请虚拟 IP 地址的子网名称。




6. 选择【虚拟 IP】，单击【申请虚拟 IP 地址】。
7. 在左侧导航栏选择【子网】。




8. 选择 IP 类型，仅在 IPv6 开放区域可配置。
9. 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。

10. 选择手动分配方式，请填写虚拟 IP 地址。
11. 单击“确定”。


在 IP 列表中可以查看申请的虚拟 IP 地址。

为虚拟 IP 地址绑定弹性 IP 或弹性云服务器

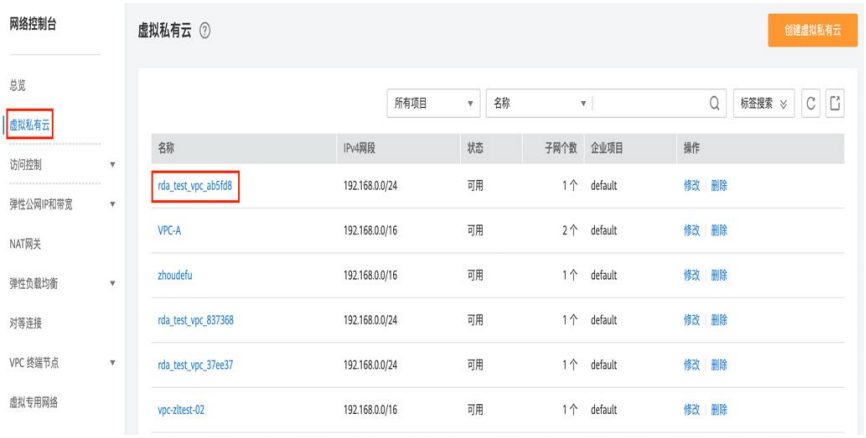
操作场景

用户可以为虚拟 IP 地址绑定一个弹性 IP 地址，从互联网可以访问后端绑定了同一个

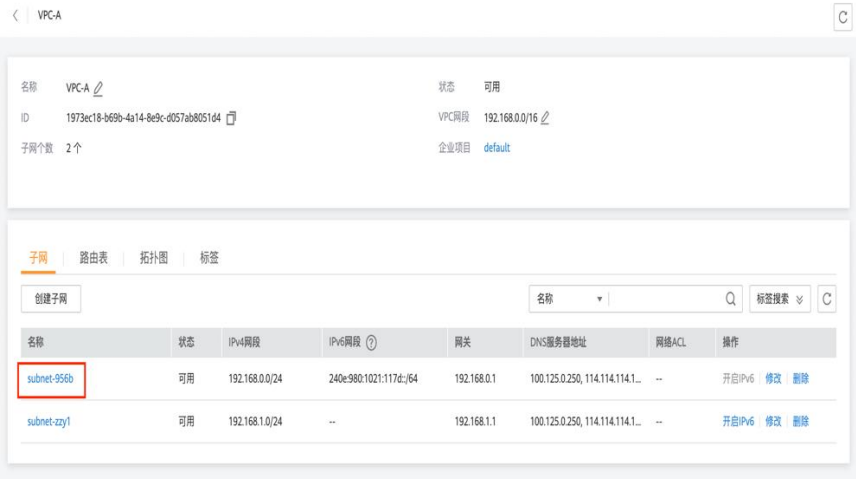
虚拟 IP 地址的多个主备部署的弹性云服务器，增强容灾性能。

## 操作步骤

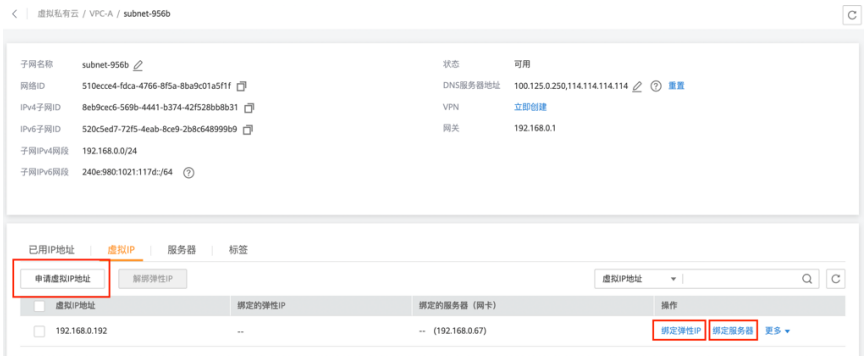
1. 登录管理控制台。
2. 在系统首页，选择【网络>—虚拟私有云】。
3. 在左侧导航栏选择【虚拟私有云】。
4. 在虚拟私有云列表中，单击虚拟 IP 地址所属的虚拟私有云名称。




5. 在【子网】页签中，单击虚拟 IP 地址所属子网名称。




6. 选择【虚拟 IP】页签，在需要绑定弹性 IP 或者弹性云服务器的虚拟 IP 地址所在行的操作列下，单击【绑定弹性 IP】或者【绑定云服务器】。




7. 选择需要绑定的弹性 IP 地址或弹性云服务器（及网卡）。


**说明**

- 弹性云服务器多网卡时，建议绑定主网卡。
- 一个弹性云服务器的网卡可以绑定多个虚拟 IP。
- IPv6 的虚拟 IP 仅支持绑定一个网卡（双栈网卡），如需进行服务器的主备切换，请通过调用 API 方式。

8. 单击“确定”。

9. 为已绑定虚拟 IP 的弹性云服务器手工配置虚拟 IP 地址。

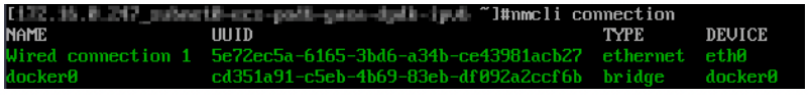
   弹性云服务器的网卡绑定虚拟 IP 地址后，需要在弹性云服务器上手工配置虚拟 IP 地址。

   Linux 系统(本文以“CentOS 7.2 64bit”为例)

   a. 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：



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。

b. 执行以下命令，在目标连接中添加虚拟 IP。

nmcli connection modify "CONNECTION" ipv4.addresses VIP 参数说明如下:

- CONNECTION:为查到的网卡对应的连接。
- VIP: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。
  - 如果已有虚拟 IP 地址，此时还需要新增虚拟 IP 地址，那么命令中除了包含新的虚拟 IP 地址，也需要包含原有虚拟 IP 地址。

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

c. 执行以下命令，使配置生效。

nmcli connection up "CONNECTION"

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)
```

d. 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
```

Windows 系统(本文以"Windows Server"为例)

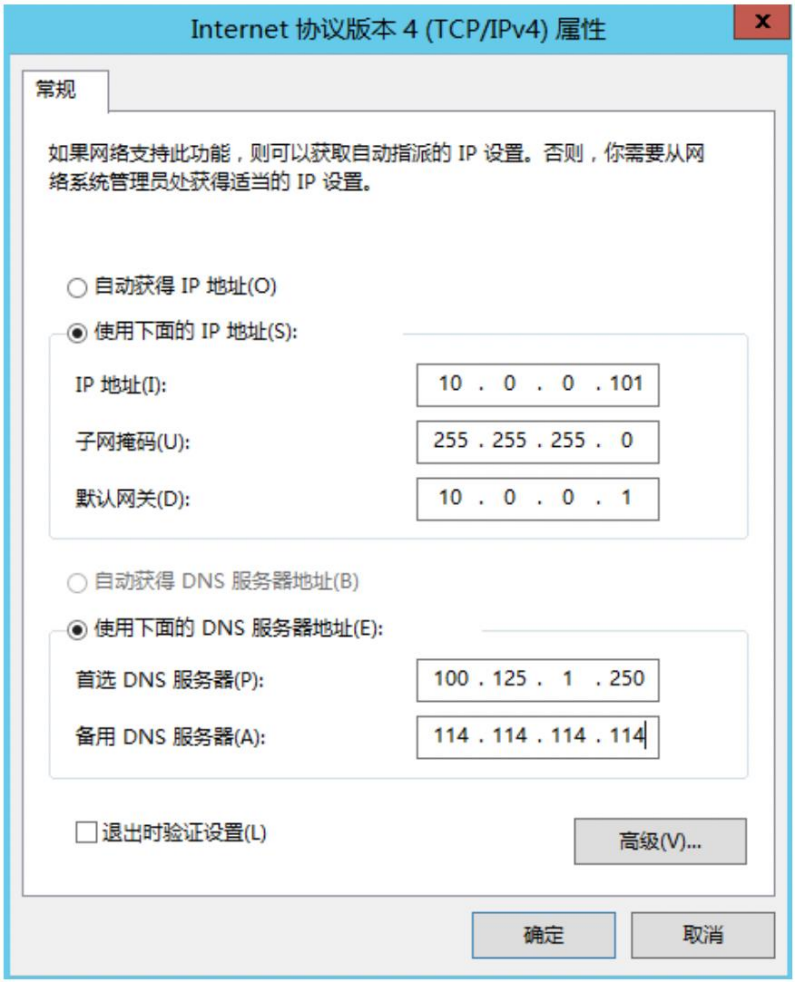
a. 在"控制面板 > 网络和共享中心"路径下，单击对应的本地连接。

b. 在打开的本地连接页面中，单击"属性"。

c. 在"网络"页签中选择"Internet 协议版本 4 (TCP/IPv4)"。

d. 单击"属性"。

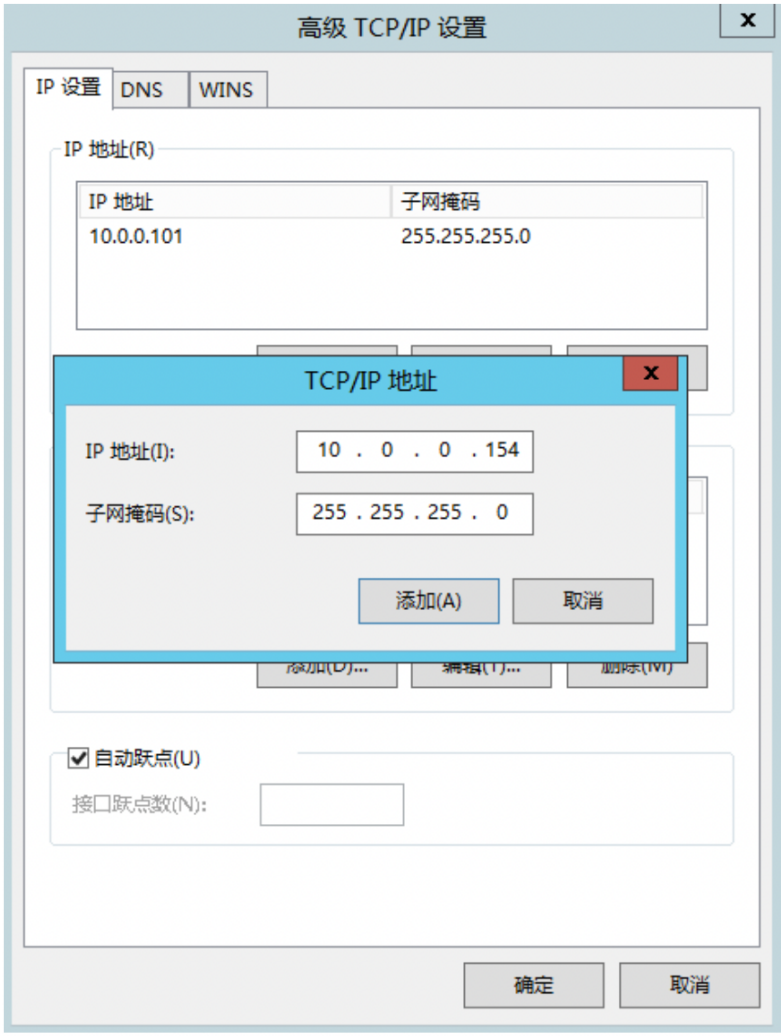
e. 选择"使用下面的 IP 地址"，IP 地址配置为弹性云服务器的私有 IP 地址，例如:10.0.0.101。



f. 单击“高级”。

g. 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。




h. 单击“确定”，保存更改。

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。

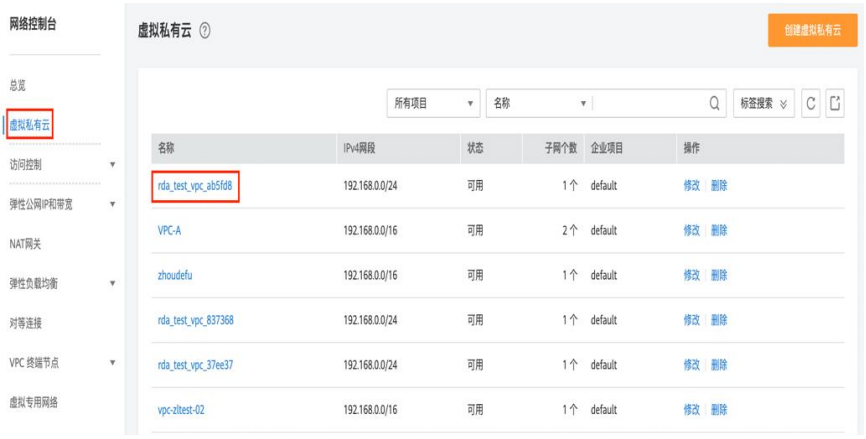
为弹性 IP 地址绑定虚拟 IP 地址

## 前提条件

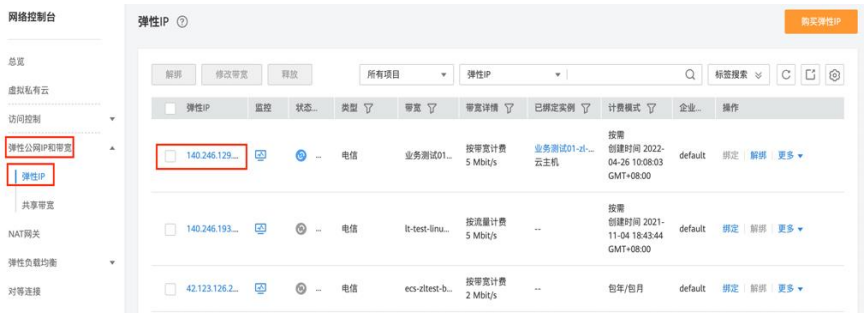
- 参考典型组网完成弹性云服务器组网配置，确保弹性云服务器已经绑定虚拟 IP。
- 已创建弹性 IP。

## 操作步骤

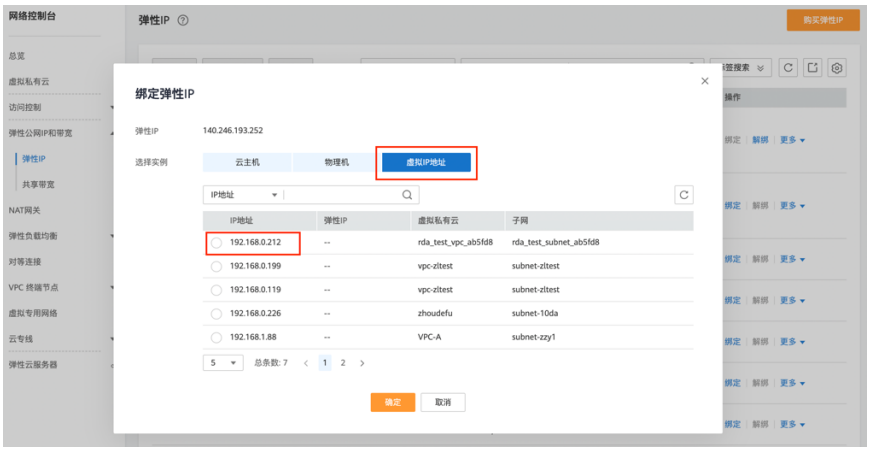
1. 登录管理控制台。
2. 在系统首页，选择【网络 > 虚拟私有云】。




3. 在左侧导航树，选择【弹性 IP 和带宽 > 弹性 IP】。




4. 在【绑定弹性 IP】弹窗中，选择实例为【虚拟 IP 地址】。




5. 在虚拟 IP 列表中，选择需要绑定的虚拟 IP，单击【确定】。

通过 VPN 访问虚拟 IP

操作步骤

1. 参考典型组网完成弹性云服务器组网配置。
2. 创建 VPN。

   创建的 VPN 可以访问弹性云服务器的虚拟 IP。

通过云专线访问虚拟 IP

操作步骤

1. 参考典型组网完成弹性云服务器组网配置。
2. 创建云专线。

   创建的云专线可以访问弹性云服务器的虚拟 IP。

通过对等链接访问虚拟 IP

操作步骤

1. 参考典型组网完成弹性云服务器组网配置。
2. 创建对等连接。

## 关闭备弹性云服务器 IP 转发功能

### 操作步骤

Linux 系统

1. 登录弹性云服务器执行如下命令，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，执行 2 和 3 关闭 IP 转发功能。

– 回显为 0，操作完成。

2. 使用 vi 打开"/etc/sysctl.conf"文件，修改 net.ipv4.ip_forward = 0，按":wq"保存退出。
   或使用 sed 命令修改，参考命令如下:
   sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
3. 执行如下命令，使修改生效。
   sysctl -p /etc/sysctl.conf

Windows 系统

1. 在 Windows 系统的"开始 > 命令提示符"执行如下命令。
   ipconfig /all
   回显结果中:"IP 路由已启用"为"否"，则 IP 转发功能已关闭。
2. 按"Windows+R"打开运行窗口，输入 regedit，进入注册表编辑器。
   3. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip \Parameters 下的 IPEnableRouter 值为 0。

– 指定值为 0:关闭 IP 转发。

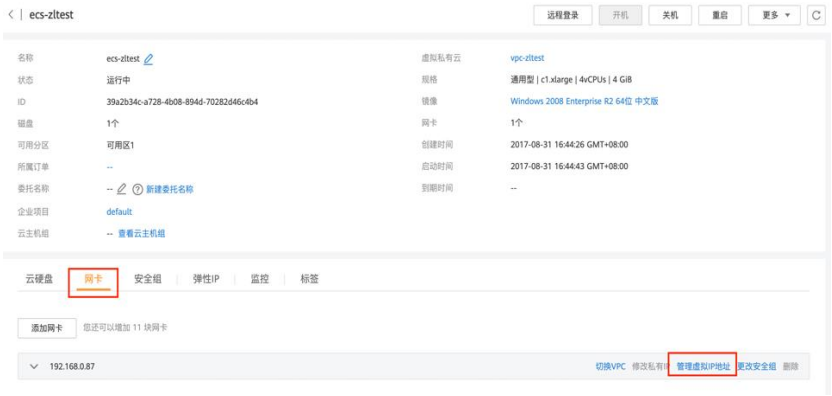
– 指定值为 1:启用 IP 转发。

## 关闭源/目的检查（适用于高可用负载均衡集群场景）

### 操作步骤

1. 登录管理控制台。
2. 选择【计算 > 弹性云服务器】。

3. 在弹性云服务器列表中单击该弹性云服务器名称。
4. 进入弹性云服务器详情页面，单击【网卡】页签。




5. 确认网卡详情中【源/目的检查】状态已设置【关闭】。


## 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。

### 前提条件

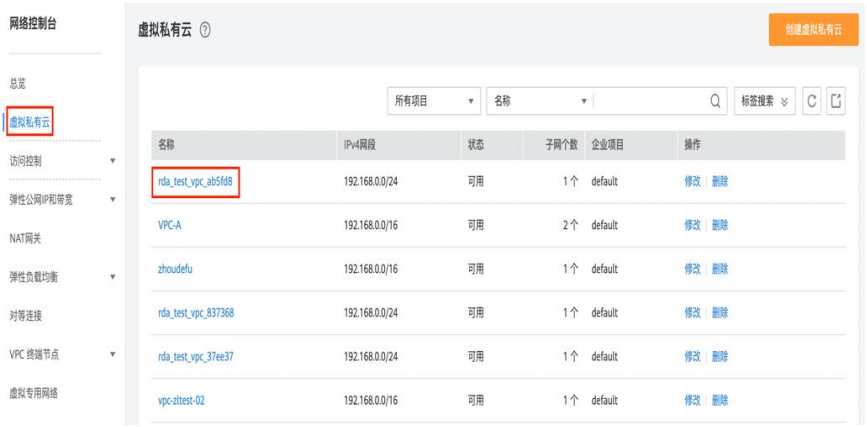
在删除虚拟 IP 前，请确保您已经将虚拟 IP 与以下资源解绑：

- 弹性云服务器
- 弹性 IP
- CCE 集群

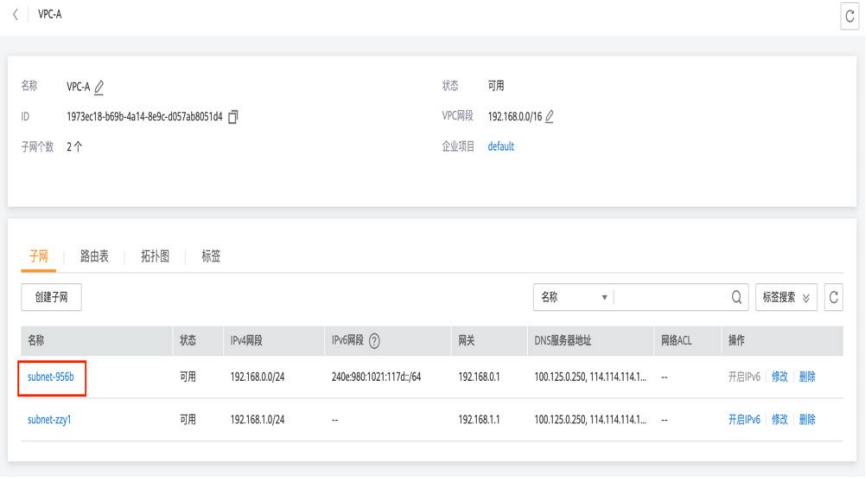
### 操作步骤

1. 登录管理控制台。

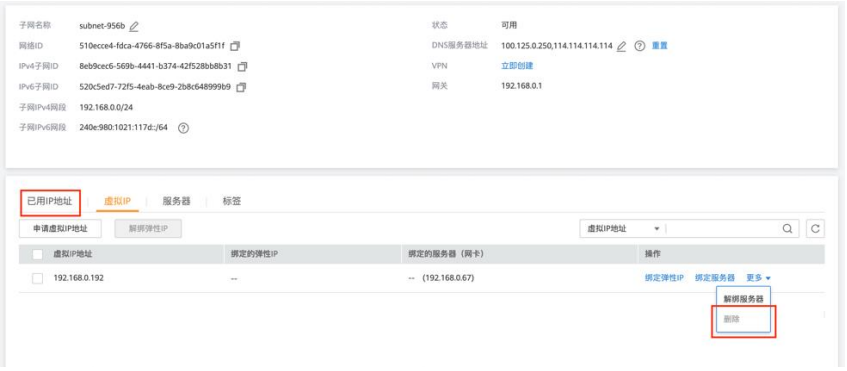
2. 在系统首页，选择【网络 > 虚拟私有云】。
3. 在左侧导航栏选择【虚拟私有云】。
4. 在虚拟私有云列表中，单击需要删除虚拟 IP 地址的子网所在的虚拟私有云名称。




5. 在【子网】页签中，单击需要删除虚拟 IP 地址的子网名称。




6. 选择【虚拟 IP】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】。



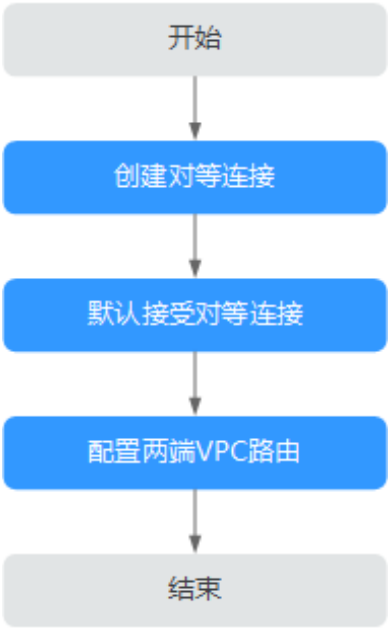
7. 单击【是】。

## VPC 对等连接

### 对等连接创建流程

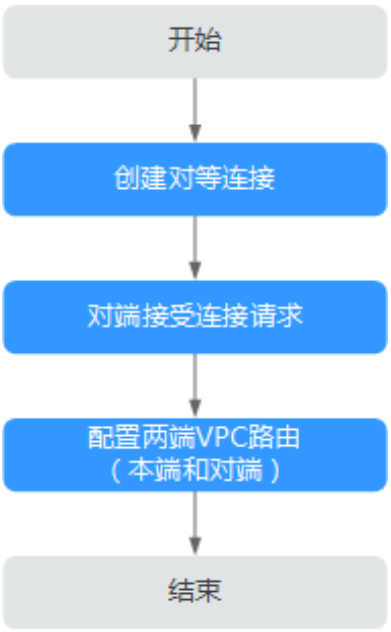
对等连接是指两个 VPC 之间的网络连接。您可以使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。同一区域内，您可以在自己的 VPC 之间创建对等连接，也可以在自己的 VPC 与其他帐户的 VPC 之间创建对等连接。不同区域间的 VPC 之间不能创建对等连接。

- 同帐户的 VPC 创建对等连接流程。




在同一个帐户下，创建对等连接后，状态是已接受。您需要在两端 VPC 内添加对等连接路由信息，才能使两个 VPC 互通。

- 跨帐户的 VPC 创建对等连接流程。




跨帐户创建 VPC 对等连接时，一端 VPC 发起创建对等连接请求，对等连接状态为待接受。待对方接受该创建请求后，对等连接状态变为已接受，请求方和接受方须分别配置对等连接路由信息，才能使两个 VPC 互通。

添加对等连接路由信息时，如果两个 VPC 网段有重叠，这个对等连接添加的路由将可能会失效。如果要在具有重叠 CIDR 的 VPC 间建立对等连接，确保两个 VPC 下的所有子网 CIDR 都不重叠，此时，您可以通过 VPC 对等连接建立子网之间的对等关系。

对等连接创建完成后，可以使用"ping"命令检查本端网络是否连通，不支持通过"ping"命令检查对端子网网关是否连通。

## 对等连接路由配置方案

当您需要同区域的 VPC 互相通信时，可以将 VPC 两两建立对等连接 。建立 VPC 对等连接，对 VPC 及子网网段有要求，如表 5-27 所示。

**表5-27** 对等连接-VPC 及子网网段要求说明

| 场景说明 | 对等连接说明 |
| --- | --- |
| VPC：所有 VPC 网段不重叠<br>子网：子网网段不限制 | 可以创建指向整个 VPC 网段的对等连接，即路由的目的地址可以添加整个 VPC 网段。<br>详细说明请参见指向整个 VPC 的对等连接路由配 |

| 场景说明 | 对等连接说明 |
| --- | --- |
| | 置。 |
| VPC：VPC 网段存在重叠<br>子网：对等连接两端的子网网段不能重叠 | 可以创建指向 VPC 子网的对等连接，即路由的目的地址可以添加子网网段。<br>详细说明请参见指向子网的对等连接路由配置。 |

### 指向整个 VPC 的对等连接路由配置

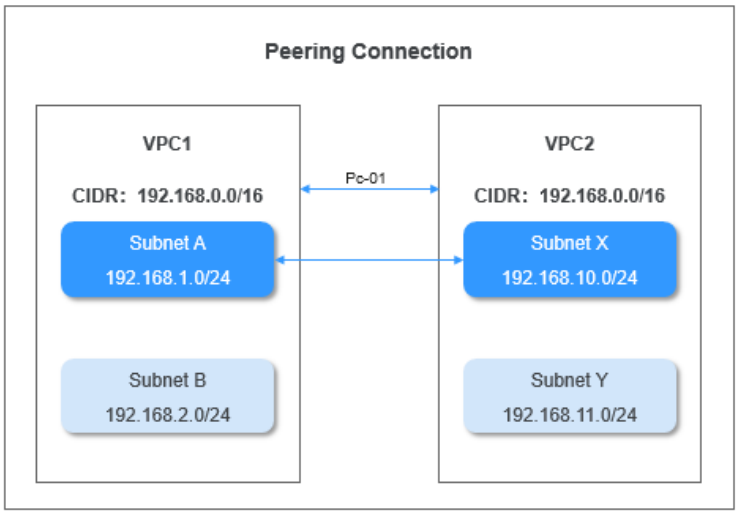
- 指向整个 VPC 的对等连接包含以下几种情况：
  - 两个 VPC 之间建立对等连接。
  - 多个 VPC 之间建立对等连接。
- 不论是哪种情况，只要是指向整个 VPC 的对等连接路由配置，建立对等连接的所有 VPC 的 CIDR 都不能重叠，否则连接失效，路由不通。
- 指向整个 VPC 的对等连接的路由配置，目的地址为对端 VPC 的 CIDR，下一跳地址为对等连接 ID。

### 指向子网的对等连接路由配置

如果 VPC 间的 CIDR 有重叠，建立对等连接时，只能针对子网建立对等关系。如果 VPC 下的子网网段有重叠，那么该对等关系不生效。建立对等连接时，请确保 VPC 之间没有重叠的子网。

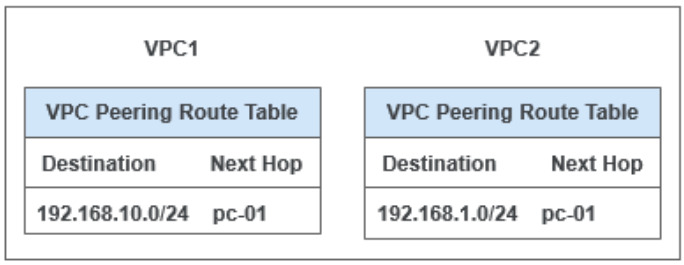
假设 VPC1 和 VPC2 的 CIDR 相同且相互之间子网没有重叠，那么，可以在两个不同的子网间建立对等连接，具体是哪些子网具有对等关系，是在路由表里体现的。对等关系如图 5-4。图中 VPC1 的子网 A 和 VPC2 的子网 X 需要通过添加路由来建立对等关系。

图5-4 子网 A 和子网 X 建立对等连接



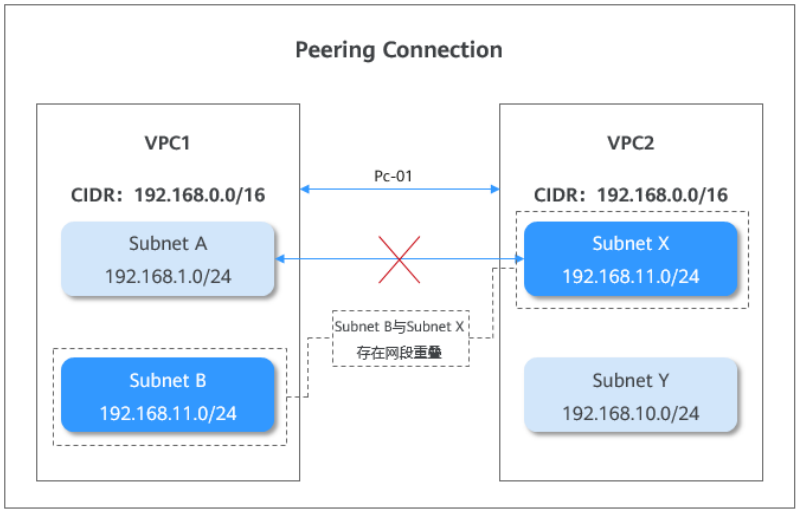

子网 A 和子网 X 的对等连接路由配置如图 5-5 所示，配置完成后，子网 A 与子网 X 就建立了对等关系，可以相互通信。

图5-5 子网 A 和子网 X 的对等连接路由表




如果两个 VPC 之间的子网网段有重叠，那么建立的对等连接将无效，无法相互通信。如图 5-6 所示，目前需要在 VPC1 的子网 A 和 VPC2 的子网 X 建立对等连接，其中 VPC1 的子网 B 和 VPC2 的子网 X 网段重叠。当在 VPC1 的路由表中添加到 VPC2 子网 X 的路由时，此路由（192.168.11.0/24）和 VPC1 子网 B 的系统路由冲突，子网 A 会优先访问子网 B 的系统路由，导致子网 A 和子网 X 无法建立对等关系。

图5-6 无效的对等连接




当 VPC1 与多个 VPC （比如：VPC2、VPC3、VPC4）建立对等连接时，VPC1 与这些 VPC 下的子网 CIDR 都不能重叠。如果 VPC2、VPC3、VPC4 具有重叠子网，重叠子网不能同时作为对等子网与 VPC1 的子网建立对等关系。1 个子网与其他 N 个子网建立对等关系时，所有子网的网段彼此都不能重叠。

## 创建同一帐户下的对等连接

### 操作场景

创建对等连接首先要向需要建立对等连接的 VPC 发送请求，您可以和自己帐户内相同区域的其他 VPC 申请对等连接，同帐户内同区域的 VPC 创建对等连接，默认自动接受。

**说明**

当前在部分区域中，由于路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，配置 VPC 对等连接路由时，需要前往路由表界面进行操作。具体配置时请根据界面提示为准。

- 未解耦：在虚拟私有云详情页的“路由表”页签，可对路由表进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“路由表”，可对路由表进行操作。

若您所在区域，路由表未解耦，请参考添加 VPC 对等连接路由（路由表未解耦）。

若您所在区域，路由表已解耦，请参考添加 VPC 对等连接路由（路由表已解耦）。

### 前提条件

已创建相同区域内的两个 VPC。

### 创建 VPC 对等连接

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在界面右侧详情区域单击“创建对等连接”。
5. 根据界面提示配置参数，其中“帐户”选择“当前帐户”，相关参数如表 5-28 所示。

**表5-28** 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 对等连接名称。<br>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-001 |
| 本端 VPC | 本端 VPC。可在下拉框中选择。 | vpc_002 |
| 本端 VPC 网段 | 本端 VPC 网段。 | 192.168.10.0/24 |
| 帐户 | 建立对等连接的帐号：<br>当前帐户：表示在同一个帐户内、同一个区域下的不同 VPC 间建立对等连接。<br>其他帐户：表示在同一个区域下的不同帐户的 VPC 间建立对等连接。 | 当前帐户 |
| 对端项目 | 对端项目名称，默认为当前项目的项目名称。选择默认项目名称，即和同帐户下 VPC 创建对等连接。支持与同区域的专属云下的 VPC 创建对等连接。选择对应专属云的项目名称，即可选择同帐户的专属云下的 VPC 创建对等连接。 | aaa |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 对端 VPC | 对端 VPC。同帐户 Peer VPC 可在下拉框中选择。 | vpc_fab1 |
| 对端 VPC 网段 | 对端 VPC 网段。<br>对端 VPC 网段不能和本端 VPC 网段相同或有重叠网段，否则对等连接路由可能会失效。 | 192.168.2.0/24 |

6. 单击“确定”。

### 添加 VPC 对等连接路由（路由表未解耦）

相同帐户创建 VPC 对等连接，默认自动接受请求，要使对等连接的 VPC 可以路由数据，还需要添加 VPC 对等连接本端、对端路由信息。

1. 在系统首页，选择“网络 > 虚拟私有云”。
2. 在左侧导航栏选择“对等连接”。
3. 在对等连接列表中，查找需要添加路由信息的对等连接。
4. 单击对等连接名称，进入对等连接详情页面。
5. 在 VPC 对等连接详情页面，单击“本端路由”。
6. 在“本端路由”页签区域，单击“添加本端路由”添加本端路由信息，参数说明参考表 5-29。

表5-29 路由参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 目的地址，对端 VPC 或子网的网段。 | 192.168.2.0/24 |
| 下一跳地址 | 下一跳地址，即对等连接 ID，默认不用配置。 | d1a7863b-9d5e-4d27-8eaf-ab14d2a9148b |

7. 单击“确定”，回到对等连接详情界面。
8. 在对等连接详情界面，单击“对端路由”。
9. 在“对端路由”页签区域，单击“添加对端路由”添加对端路由信息。
10. 单击“确定”，完成添加 VPC 对等连接路由信息。

对等连接建立后，您可以使用私有 IP 地址在两个 VPC 之间进行通信。您可以使用“ping”命令检查网络两端是否连通。

如果两个 VPC 不能互通，请参考为什么对等连接创建完成后不能互通？检查相关配置。

### 添加 VPC 对等连接路由（路由表已解耦）

相同帐户创建 VPC 对等连接，默认接受请求，要使对等连接的 VPC 可以路由数据，还需要在路由表中添加 VPC 对等连接本端、对端路由信息。

1. 在系统首页，选择“网络 > 虚拟私有云”。
2. 在左侧导航栏选择“路由表”。
3. 查找或创建本端 VPC 对应的路由表，添加本端路由。参数说明如表 5-30 所示。

表5-30 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 对端 VPC 的网段。 | 192.168.0.0/16 |
| 下一跳类型 | 选择“对等连接”。 | 对等连接 |
| 下一跳 | 选择当前对等连接的名称。 | peering-001 |
| 描述 | 路由的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

4. 查找或创建对端 VPC 对应的路由表，添加对端路由。

对等连接建立后，您可以使用私有 IP 地址在两个 VPC 之间进行通信。您可以使用“ping”命令检查网络两端是否连通。

如果两个 VPC 不能互通，请参考为什么对等连接创建完成后不能互通？检查相关配置。

# 创建不同帐户下的对等连接

## 操作场景

VPC 支持本帐户与其他帐户内相同区域的 VPC 创建对等连接。与其他帐户内相同区域的 VPC 创建对等连接时，需要对端帐户接受对等连接请求，才能建立有效对等连接。

**说明**

当前在部分区域中，由于路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，配置 VPC 对等连接路由时，需要前往路由表界面进行操作。具体配置时请根据界面提示为准。

- 未解耦：在虚拟私有云详情页的"路由表"页签，可对路由表进行操作。
- 已解耦：在进入"网络 > 虚拟私有云"后，在左侧导航栏直接选择"路由表"，可对路由表进行操作。

若您所在区域，路由表未解耦，请参考添加 VPC 对等连接路由（路由表未解耦）。

若您所在区域，路由表已解耦，请参考添加 VPC 对等连接路由（路由表已解耦）。

## 创建 VPC 对等连接

1. 登录管理控制台。
2. 在系统首页，选择"网络 > 虚拟私有云"。
3. 在左侧导航栏选择"对等连接"。
4. 在界面右侧详情区域单击"创建对等连接"。
5. 根据界面提示配置参数，其中"帐户"选择"其他帐户"。

表5-31 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 名称 | 对等连接名称。<br>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-001 |
| 本端 VPC | 本端 VPC。可在下拉框中选择。 | vpc_002 |
| 帐户 | 建立对等连接的帐号：<br>• 当前帐户：表示在同一个帐户内、同一个区域下的不同 VPC 间建立对等连接。 | 其他帐户 |

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| | • 其他帐户：表示在同一个区域下的不同帐户的 VPC 间建立对等连接。 | |
| 对端项目 ID | 选择“其他帐户”时，有此参数。<br>对端项目 ID 获取参考如何获取对端项目 ID。 | - |
| 对端 VPC ID | 选择“其他帐户”时，有此参数。<br>对端 VPC ID 获取请参考如何获取对端 VPC ID。 | 65d062b3-40fa-4204-8181-3538f527d2ab |
| 描述 | 对等连接的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 单击“确定”。

## 接受对等连接

不同帐户创建对等连接，由于本端帐户没有对端帐号权限，要使对等连接生效，需对端帐户接受对等连接。

1. 对端帐户登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在对等连接列表中，找到需要接受请求的对等连接，单击操作列的“接受请求”。
5. 单击“是”，接受对等连接。

## 拒绝对等连接

不同帐户创建对等连接，由于本端帐户没有对端帐户权限，对端帐户如果不同意创建对等连接，可以选择拒绝对等连接请求，拒绝后本次创建对等连接结束。拒绝的对等连接，需要删除后，才能再次发起请求。

1. 对端帐户登录管理控制台。

2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在对等连接列表中，找到需要拒绝请求的对等连接，单击操作列的“拒绝请求”。
5. 单击“是”。拒绝对等连接。

### 添加 VPC 对等连接路由（路由表未解耦）

不同帐户创建 VPC 对等连接，接受请求后，要使对等连接的 VPC 可以相互通信，还需要添加 VPC 对等连接路由信息。由于本端帐户没有对端帐户权限，本端帐户只可以添加本端路由信息，对端路由信息需要对端帐户添加相应路由信息。本端帐户添加路由信息和对端帐户添加路由信息操作相同，具体操作如下。

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在已创建对等连接列表，查找需要添加路由信息对等连接名。
5. 单击对等连接名称链接，进入对等连接详情页面。
6. 在 VPC 对等连接详情页面，单击“本端路由”。
7. 在“本端路由”页签区域，单击“添加本端路由”添加本端路由信息。

**表5-32** 路由参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 目的地址，对端 VPC 或子网的网段。 | 192.168.2.0/24 |
| 下一跳地址 | 下一跳地址，即对等连接 ID，默认不用配置。 | d1a7863b-9d5e-4d27-8eaf-ab14d2a9148b |

8. 单击“确定”，完成添加 VPC 对等连接路由信息。

对等连接建立后，您可以使用私有 IP 地址在两个 VPC 之间进行通信。您可以使用“ping”命令检查网络两端是否连通。

如果两个 VPC 不能互通，请参考为什么对等连接创建完成后不能互通？检查相关配置。

### 添加 VPC 对等连接路由（路由表已解耦）

不同帐户创建 VPC 对等连接，接受请求后，要使对等连接的 VPC 可以相互通信，还需要在路由表中添加 VPC 对等连接路由信息。由于本端帐户没有对端帐户权限，本端帐户只可以添加本端路由信息，对端路由信息需要对端帐户添加相应路由信息。本端帐户添加路由信息和对端帐户添加路由信息操作相同，具体操作如下。

1. 在系统首页，选择“网络 > 虚拟私有云”。
2. 在左侧导航栏选择“路由表”。
3. 查找或创建本端 VPC 对应的路由表，添加本端路由。参数说明如表 5-33 所示。

表5-33 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 对端 VPC 的网段。 | 192.168.0.0/16 |
| 下一跳类型 | 选择“对等连接”。 | 对等连接 |
| 下一跳 | 选择当前对等连接的名称。 | peering-001 |
| 描述 | 路由的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

4. 单击“确定”，完成添加 VPC 对等连接路由信息。

对等连接建立后，您可以使用私有 IP 地址在两个 VPC 之间进行通信。您可以使用“ping”命令检查网络两端是否连通。

如果两个 VPC 不能互通，请参考为什么对等连接创建完成后不能互通？检查相关配置。

### 如何获取对端项目 ID

1. 使用对端帐户登录管理控制台。
2. 在用户名的下拉列表中，单击“我的凭证”。
3. 在“项目列表”页签中查看项目 ID。

### 如何获取对端 VPC ID

1. 使用对端帐户登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏，选择“虚拟私有云”。
4. 单击 VPC 名称，在 VPC 详情页查看 VPC ID。

## 查看对等连接

### 操作场景

已创建的对等连接或等待接受的对等连接，两端帐户均可在对等连接中查看对等连接信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在界面右侧详情区域可通过创建的对等连接状态或对等连接名称筛选查看对等连接。
5. 单击对应的对等连接名称，进入对等连接详情界面，可查看对等连接路由等详细信息。

## 修改对等连接

### 操作场景

对等连接在任何状态下，两端帐户均有权限修改对等连接。可以修改对等连接的名称。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。

4. 在界面右侧详情区域可通过创建的对等连接状态或对等连接名称筛选查看对等连接。
5. 单击操作列的“修改”，修改对等连接信息。
6. 单击“确定”，完成信息修改。

## 删除对等连接

### 操作场景

对等连接在任何状态下，两端帐户均有权限删除对等连接。对等连接删除时，会自动删除两端 VPC 关联的路由信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在界面右侧详情区域可通过创建的对等连接状态或对等连接名称筛选查看对等连接。
5. 单击操作列的“删除”，删除对等连接信息。
6. 单击“是”。

## 查看对等连接路由

### 操作场景

对等连接路由信息添加后，两端帐户均有权限在对等连接详情界面查看对等连接路由信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在对等连接列表中，查找需要查看路由信息的对等连接。
5. 单击对等连接名称，进入对等连接详情页面。

6. 在 VPC 对等连接详情页面，单击“本端路由”页签，可查看此对等连接的本端路由信息。
7. 在对等连接详情界面，单击“对端路由”页签，可查看此对等连接的对端路由信息。

## 删除对等连接路由

### 操作场景

对等连接路由添加后，两端帐户均有权限在对等连接详情界面或路由表界面（已解耦）删除对等连接路由信息。

**说明**

当前在部分区域中，由于路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，配置 VPC 对等连接路由时，需要前往路由表界面进行操作。具体配置时请根据界面提示为准。

- 未解耦：在虚拟私有云详情页的“路由表”页签，可对路由表进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“路由表”，可对路由表进行操作。

若您所在区域，路由表未解耦，请参考操作步骤（路由表未解耦）。

若您所在区域，路由表已解耦，请参考操作步骤（路由表已解耦）。

### 操作步骤（路由表未解耦）

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“对等连接”。
4. 在对等连接列表中，查找需要删除路由信息的对等连接。
5. 单击对等连接名称，进入对等连接详情页面。
6. 在对等连接详情页面，单击“本端路由”页签，可查看此对等连接的本端路由信息。
7. 在“本端路由”页签，选中需要删除的本端路由信息，单击操作列的“删除”，弹出删除告警框。
8. 单击“是”，确认删除。
9. 在对等连接详情界面，单击“对端路由”页签，可查看此对等连接的对端路由信息。
10. 在“对端路由”页签，选中需要删除的对端路由信息，单击操作列的“删除”，弹出删除告警框。
11. 单击“是”，确认删除。

操作步骤（路由表已解耦）

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，查找需要删除路由信息的路由表。
5. 单击路由表名称，进入路由表详情页面。
6. 找到需要删除的路由，单击操作列的“删除”。
7. 单击“是”，确认

# 路由表（已解耦）

## 路由表简介

### 相关背景

当前在部分区域中，路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，支持路由表与子网关联功能，请以实际界面为准。

- 未解耦：在虚拟私有云详情页的"路由表"页签，可对路由表进行操作。
- 已解耦：在进入"网络 > 虚拟私有云"后，在左侧导航栏直接选择"路由表"，可对路由表进行操作。

本章节适用于路由表已解耦区域，未解耦的区域用户请参考路由表（未解耦）。

### 路由表

路由表由一系列路由规则组成，用于控制虚拟私有云内子网的出流量走向。VPC 中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以关联多个子网。

### 默认路由表和自定义路由表

用户创建虚拟私有云时，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。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，您可以将子网关联到自定义路由表或者复制该条路由到自定义路由表中，在自定义路由表中添加、修改和删除路由。
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。

**说明**

- 子网关联自定义路由表仅影响子网的出流量走向，入流量仍然匹配默认路由表。
- 当前自定义路由表需提交工单申请，如需使用自定义路由表，请在创建路由表页面单击"申请扩大配额"。

创建自定义路由表的方法请参见创建自定义路由表。

### 路由

路由即路由规则，在路由中通过配置目的地址、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。

  创建路由表后，系统会自动在路由表中添加如下的系统路由，表示 VPC 内实例互通。

- 目的地址是 100.64.0.0/10、198.19.128.0/20 的路由。
- 目的地址是子网网段的路由。

**说明**

除以上系统路由外，系统还会自动添加目的地址是 127.0.0.0/8 的路由，表示本地回环地址。

- 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。

  您可以通过添加自定义路由来自定义网络流量的走向，您需要指定目的地址、下一跳类型、下一跳地址。支持的下一跳类型如表 5-34 所示。

表5-34 下一跳类型

| 下一跳类型 | 说明 |
| --- | --- |
| 服务器实例 | 将指向目的地址的流量转发到虚拟私有云内的一台服务器实例。 |
| 扩展网卡 | 将指向目的地址的流量转发到虚拟私有云内的一台服务器实例的扩展网卡。 |
| 裸金属服务器自定义网络 | 将指向目的地址的流量转发到虚拟私有云内的一台裸金属服务器实例的自定义网络。 |
| VPN 网关 | 将指向目的地址的流量转发到一个 VPN 网关。 |
| 云专线网关 | 将指向目的地址的流量转发到一个云专线网关。 |
| NAT 网关 | 将指向目的地址的流量转发到一个 NAT 网关。 |
| 对等连接 | 将指向目的地址的流量转发到一个对等连接。 |
| 虚拟 IP | 将指向目的地址的流量转发到一个虚拟 IP 地址，可以通过该虚拟 IP 地址将流量转发到主备 ECS。 |
| VPC 终端节点 | 将指向目的地址的流量转发到一个 VPC 终端节点。 |

**说明**

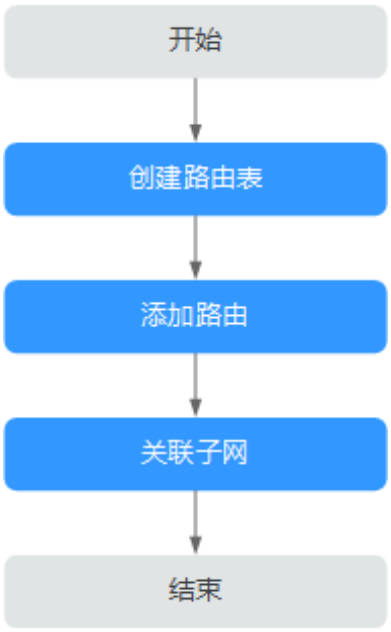
- 当为默认路由表添加自定义路由时，下一跳类型不支持选择 VPN 网关与云专线网关。
- 个别由系统下发的路由可供用户修改和删除，这取决于创建对端服务时是否已设置目的地址。

  例如，创建 NAT GateWay 时，没有指定目的地址，系统会自动下发一条自定义类型的路由，可供用户自行调整。而创建 VPN 网关与云专线网关时，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。

## 自定义路由表配置流程

创建并配置自定义路由表的流程如图 5-7 所示。

图5-7 路由表配置流程




1. 参考创建自定义路由表创建自定义路由表。
2. 参考添加自定义路由添加自定义路由规则。
3. 参考关联子网与路由表关联子网，关联成功后，路由规则对该子网生效。

## 约束与限制

- 每个虚拟私有云最多可以创建 10 个路由表，包含默认路由表。
- 每个路由表最多添加 200 个路由。
- 默认路由表不能删除。
- 系统路由不能修改和删除。
- 由 VPN、云专线下发到默认路由表中的路由不能修改和删除。
- 由 VPC 终端节点服务下发到默认路由表的网关类型终端节点的路由不能修改、复制和删除，并且自定义路由表中的网关类型终端节点的路由也不能修改和删除。
- 当为默认路由表添加自定义路由时，下一跳类型不支持选择 VPN 网关。

# 创建自定义路由表

## 操作场景

当您不想使用默认路由表时，可以创建自定义路由表。

当前自定义路由表需提交工单申请，如需使用自定义路由表，请在创建路由表页面单击“申请扩大配额”。

## 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏，选择“路由表”。
4. 在页面右上角，单击“创建路由表”，按照提示配置参数。

**表5-35** 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 路由表名称 | 路由表的名称，必填项。<br>路由表的名称只能由中文、英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于 64 个字符。 | rtb-001 |
| 所属 VPC | 选择路由表归属的 VPC，必填项。 | vpc-001 |
| 描述 | 路由表的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |
| 添加路由 | 路由规则信息，非必填项。<br>路由规则可以在此处添加，也可以在路由表创建完成后，参考添加自定义路由添加。<br>单击“+”可以依次增加多条路由。 | - |

5. 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。

## 添加自定义路由

### 操作场景

每个路由表会自带一条系统默认路由，含义为 VPC 内实例互通。您可以根据需要添加自定义路由规则，将指向目的地址的流量转发到指定的下一跳地址。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击需要添加路由规则的路由表名称。
5. 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5-36** 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 目的地址网段。<br>目的地址不能与已有路由冲突，目的地址也不能与 VPC 下子网网段冲突。 | 192.168.0.0/16 |
| 下一跳类型 | 选择下一跳资源类型。支持的资源类型请参见表 7-1。<br>说明<br>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 网关与云专线网关。 | ECS 实例 |
| 下一跳 | 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。 | ecs-001 |
| 描述 | 路由的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

6. 单击“确定”，完成添加。

## 关联子网与路由表

### 操作场景

为路由表关联子网。关联后，该路由表的路由规则将对该子网生效，该子网下的云资源将启用这个新的路由策略，请确认对业务造成的影响，谨慎操作。

### 约束与限制

一个子网只能关联一个路由表。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击操作列的“关联子网”。
5. 选择需要关联的子网。
6. 单击“确定”，完成关联。

## 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，子网下资源将启用新路由表策略，请确认对业务造成的影响。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击路由表名称。
5. 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。
6. 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策略。

## 查询路由表

### 操作场景

查看路由表基本信息、路由、关联的子网等信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击路由表的名称，查看详情。

## 删除路由表

### 操作场景

自定义路由表可以删除，系统默认路由表不能删除。

### 前提条件

删除路由表之前，请确保该自定义路由表下面没有关联子网。如果存在关联子网，请通过“更换路由表”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. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，找到需要删除的路由表，单击操作列的“删除”。
5. 单击“是”。

## 修改路由

### 操作场景

修改已经存在的路由。

## 约束与限制

- 系统路由不能修改。
- 由 VPN、云专线服务下发到默认路由表中的路由不能修改。由 VPC 终端节点服务下发到默认路由表的网关类型终端节点的路由不能修改，并且自定义路由表中的网关类型终端节点的路由也不能修改。

## 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击路由表名称。
5. 找到需要修改的路由，单击操作列的“修改”。
6. 根据弹出框提示，修改路由规则。

**表5-37** 参数说明

| 参数 | 说明 | 取值样例 |
| --- | --- | --- |
| 目的地址 | 目的地址网段。<br>目的地址不能与已有路由冲突，目的地址也不能与 VPC 下子网网段冲突。 | 192.168.0.0/16 |
| 下一跳类型 | 选择下一跳资源类型。支持的资源类型请参见表 5-34。<br>说明<br>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 网关与云专线网关。 | ECS 实例 |
| 下一跳 | 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。 | ecs-001 |
| 描述 | 路由的描述信息，非必填项。<br>描述信息内容不能超过 255 个字符，且不能包含“<”和“>”。 | - |

7. 单击“确定”。

## 删除路由

### 操作场景

您可以随时删除已创建的自定义路由。

### 约束与限制

- 系统路由不能删除。
- 由 VPN、云专线服务下发到默认路由表中的路由不能删除。由 VPC 终端节点服务下发到默认路由表的网关类型终端节点的路由不能删除，并且自定义路由表中的网关类型终端节点的路由也不能删除。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表中，单击路由表名称。
5. 找到需要删除的路由，单击操作列的“删除”。
6. 单击“是”。

## 复制路由

### 操作场景

您可以随时复制已创建的路由。

### 约束与限制

- 由 VPC 终端节点服务下发到默认路由表的网关类型终端节点的路由不能复制。
- 由 VPN 服务下发到默认路由表中的路由不能复制。
- 手工开通方式的云专线下发至默认路由表中的路由不能复制。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。

4. 在路由表列表中，单击操作列的“复制路由”。
5. 根据界面提示，选择需要复制的路由和目标路由表。

   页面所列路由为目标路由表中不存在的路由。您可以选择一个或多个路由复制到目标路由表。
6. 单击“确定”。

## 导出路由表列表

### 操作场景

您可以将当前帐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. 选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“路由表”。
4. 在路由表列表页，单击右上角的 。

   系统会将您帐号下，当前区域的所有路由表信息自动导出为 Excel 文件，并下载至本地

# 路由表（未解耦）

## 路由表简介

路由表中包含一系列被称为路由的规则，可用于判断网络流量的导向目的地。

### 相关背景

当前在部分区域中，路由表已从虚拟私有云中解耦，解耦后路由表拥有独立入口，支持路由表与子网关联功能，请以实际界面为准。

- 未解耦：在虚拟私有云详情页的“路由表”页签，可对路由表进行操作。
- 已解耦：在进入“网络 > 虚拟私有云”后，在左侧导航栏直接选择“路由表”，可对路由表进行操作。

本章节适用于路由表未解耦区域，已解耦的区域用户请参考路由表（已解耦）。

## 配置 SNAT 服务器

### 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。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，单击“计算 > 弹性云服务器”。
3. 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。
4. 在弹性云服务器详情页面单击“网卡”页签。

5. 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。

6. 绑定 EIP。

   - 为弹性云服务器的私有 IP 绑定 EIP，详情请参见为弹性云服务器申请和绑定弹性 IP。
   - 为弹性云服务器的虚拟 IP 绑定 EIP，详情请参见为虚拟 IP 地址绑定弹性 IP 或弹性云服务器。

7. 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。

8. 执行如下命令，输入 root 密码，切换至 root。

   su - root

9. 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 服务器上响应的 IPtables 规则，开放安全组规则。

   ping www.google.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 www.google.com
   PING www.a.shifen.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
   ```

10. 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 13。
    - 否，执行 11，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。

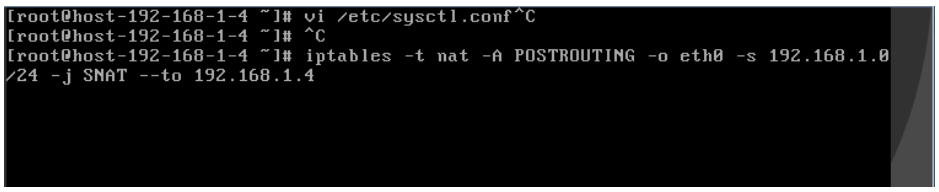
11. 使用 vi 打开"/etc/sysctl.conf"文件，修改 net.ipv4.ip_forward = 1，按":wq"保存退出。
12. 执行如下命令，使修改生效。

    sysctl -p /etc/sysctl.conf
13. 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 5-8 所示。

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

    图5-8 配置 SNAT

**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。
- 执行以下命令进入/etc/rc.local 文件。

  vi /etc/rc.local

1. 执行 14 配置 SNAT
2. 执行以下命令保存并退出。

   :wq
3. 执行以下命令添加 rc.local 文件的执行权限。

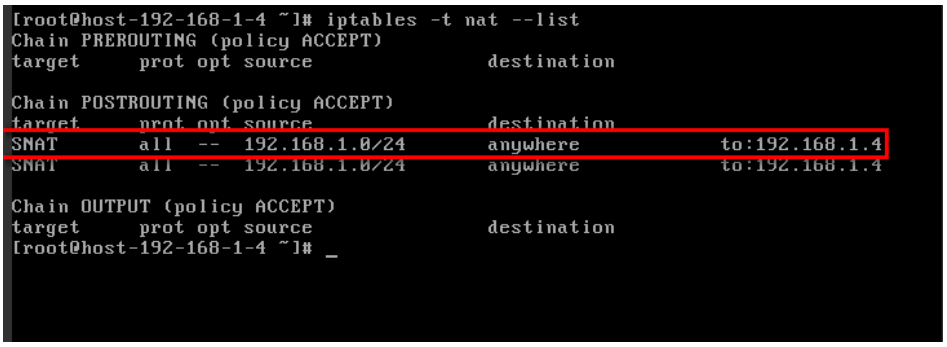
   # chmod +x /etc/rc.local

- 为保证配置正常生效，请执行 iptables -L 命令查看已配置的规则是否有冲突。

14. 执行如下命令，查看是否配置成功。如图 5-9 所示，则表示配置成功（例如：192.168.1.0/24）。

    iptables -t nat --list

图5-9 验证设置




15. 添加自定义路由，详见添加自定义路由。

    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。

## 添加自定义路由

### 操作场景

当 VPC 内的弹性云服务器需要访问 Internet，用户可以添加自定义路由，通过绑定弹性 IP 的服务器访问 Internet 网络。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要添加路由的虚拟私有云名称。
5. 在“路由表”页签，单击“添加路由信息”。
6. 根据弹出框中提示，填写路由信息。
   - “目的地址”是目的网段，默认是 0.0.0.0/0，如果是 VPC 内部发起的流量，则"目的地址"可以为该 VPC 下的子网地址。如果是 VPC 外部发起的流量，则"目的地址"不能与该 VPC 下子网网段冲突。但是，每条路由信息的目的地址不能重复。
   - “下一跳地址”是 VPC 内的私有 IP 地址或虚拟 IP。

**说明**

如果下一跳地址是虚拟 IP，这个虚拟 IP 必须绑定 EIP，否则无法通过自定义路由到虚拟 IP 访问 Internet。

7. 单击“确定”，完成创建。

## 查询路由表

### 操作场景

已经创建的路由表，您可以随时查询单个路由表或所有路由表的信息。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要查询路由的虚拟私有云名称。
5. 在路由表列中查看单个路由表或者所有路由表信息。

## 修改路由

### 操作场景

修改路由的目的地址、下一跳地址。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要修改路由的虚拟私有云名称。
5. 在“路由表”页签中，单击需要修改的路由信息所在行的“操作”列下的“修改”。根据弹出框提示，修改路由信息。
6. 单击“确定”，完成修改。

## 删除路由

### 操作场景

您可以随时删除已创建的路由。

### 操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要删除路由的虚拟私有云名称。
5. 在“路由表”页签中，单击需要删除的路由信息所在行的“操作”列下的“删除”。
6. 单击“是”，完成删除。

# 监控

## 支持的监控指标

### 功能说明

本节定义了弹性 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 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5-38 弹性 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。<br>单位：比特/秒 | ≥ 0 bit/s | 带宽或弹性 IP | 1 分钟 |
| 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。<br>单位：比特/秒 | ≥ 0 bit/s | 带宽或弹性 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的网络流量。<br>单位：字节 | ≥ 0 bytes | 带宽或弹性 IP | 1 分钟 |
| down_stream | 入网流量 | 该指标用于统计测试对象入云平 | ≥ 0 bytes | 带宽或弹性 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） |
|---|---|---|---|---|---|
| | | 台的网络流量。<br>单位：字节 | | | |

维度

| Key | Value |
|---|---|
| publicip_id | 弹性 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"

  }

  ],

查看监控指标

操作场景

查看带宽、弹性 IP 的使用情况。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“管理与监管 > 云监控服务”。
3. 单击页面左侧的“云服务监控”，选择“虚拟私有云”。
4. 单击“操作”列的“查看监控图表”，查看带宽或弹性 IP 的监控指标详情。

## 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. 在系统首页，选择“管理与监管 > 云监控服务”。
3. 在左侧导航栏，选择“告警 > 告警规则”。
4. 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。
5. 规则参数设置完成后，单击“确定”。
6. 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》。

# 6 最佳实践

## VPC 公网访问

### 公网产品

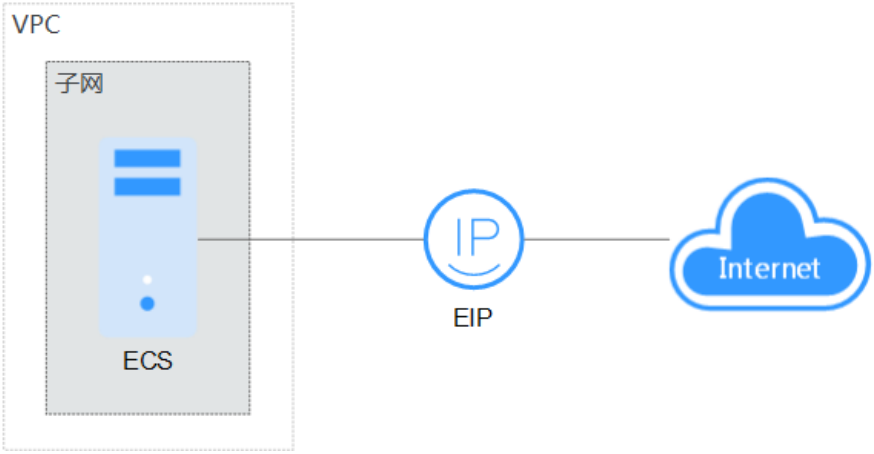
公有云提供弹性公网 IP（EIP）、NAT 网关、弹性负载均衡（ELB）等方式连接公网。

- EIP
  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。
- ELB
  ELB 将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用容错。为负载均衡器配置需要监听的端口信息以及弹性云服务器，通过监听器来检查后端弹性云服务器的运行状态，确保将请求发送到正常的弹性云服务器上，提高系统可用性。
- NAT 网关
  NAT 网关能够为 VPC 内的弹性云服务器提供 SNAT 和 DNAT 功能，通过灵活简易的配置，即可轻松构建 VPC 的公网出入口。

### 对外提供服务

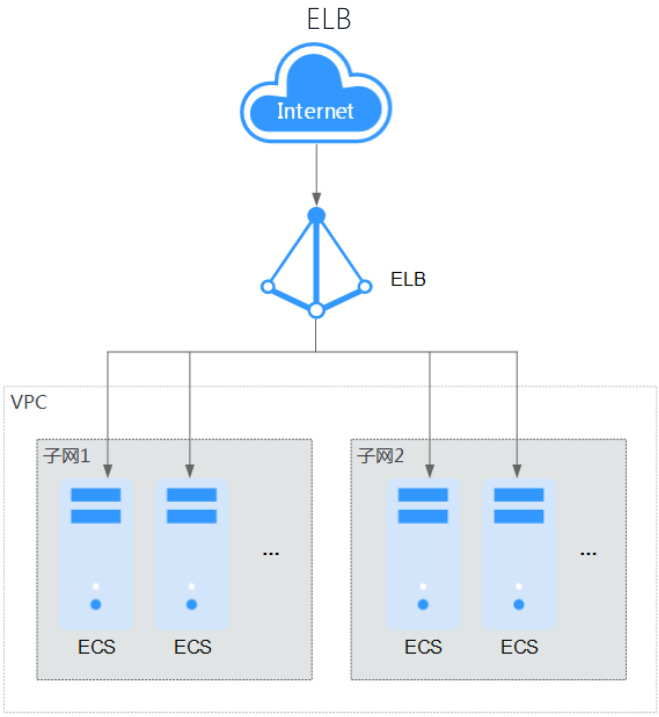
- 单个 ECS 对外提供服务

当您仅有单个应用服务，业务量较小时，您可申请一个 EIP，绑定到 ECS 上，该 ECS 即可连接公网提供服务。




- 多个 ECS 负载均衡

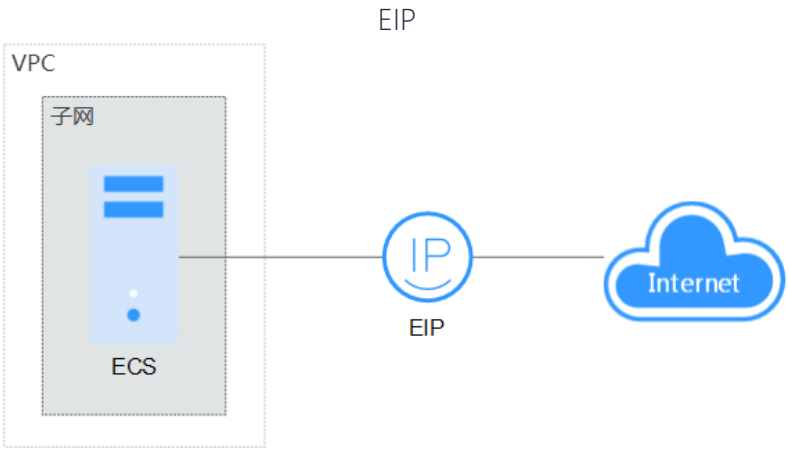
  对于电商等高并发访问的场景，您可以通过 ELB 将访问流量均衡分发到多台弹性云服务器上，支撑海量用户访问。天翼云 ELB 无缝集成了弹性伸缩服务，能够根据业务流量自动扩容，保证业务稳定可靠。




主动访问公网

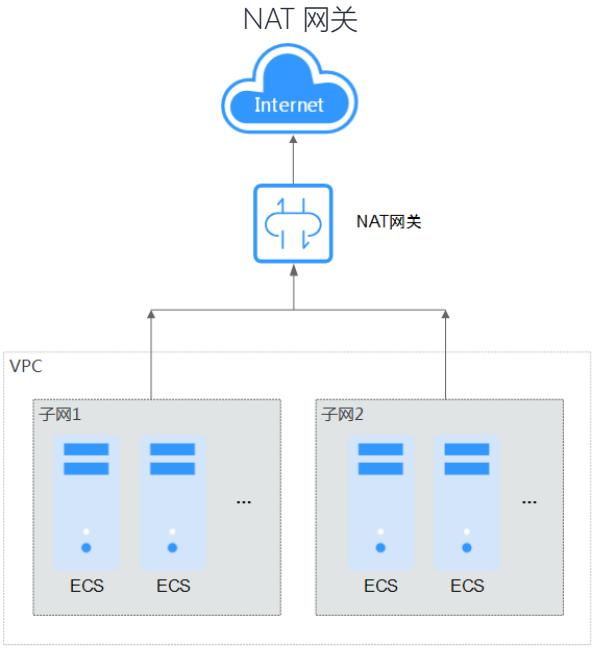
- 单个 ECS 访问公网

  当您的某台 ECS 需要主动访问公网，可以为 ECS 绑定 EIP，即可实现公网访问。天翼云提供多种计费方式（按需、按流量等）供您选择，无需使用时支持灵活解绑。




- 多个 ECS 访问公网

  当您的 VPC 内 ECS 都有公网访问需求时，可以使用 NAT 网关服务，按子网配置 SNAT 规则，轻松构建 VPC 的公网出口。对比 EIP 访问公网，在未配置 DNAT 规则时，外部用户无法通过公网直接访问 NAT 网关的公网地址，保证了 ECS 的相对安全。




# VPC 连接

云上 VPC 互联

VPC 与 VPC 之间要建立连接，可以通过如下云产品实现。

| 云产品 | 应用场景 | 描述 | 相关操作 |
| --- | --- | --- | --- |
| 对等连接 | 同区域的 VPC 互连 | 对于同一区域的 VPC，可以通过对等连接进行互连，同一帐号与不同帐号的连接方式略有差异。对等连接免费。 | 创建同一帐户下的对等连接，<br>创建不同帐户下的对等连接. |
| 虚拟专用网络 VPN | 使用公网低成本连接跨区域 VPC | 基于 Internet 使用加密隧道将不同区域的 VPC 连接起来。具备成本低、配置简单、即开即用等优点。但它的网络质量依赖 Internet。 | 通过 VPN 连接 VPC， |

云上 VPC 互联

对于自建本地数据中心（IDC）的用户，由于利旧和平滑演进的原因，并非所有的业务都能放置在云上，这个时候就可以通过如下产品构建混合云，实现云上 VPC 与云下 IDC 之间的互连。

| 云产品 | 应用场景 | 描述 | 相关操作 |
| --- | --- | --- | --- |
| 虚拟专用网络 VPN | 使用公网低成本连接 VPC 与 | 基于 Internet 使用加密隧道将 VPC 与本地数据中心连接起来。具备成本低、配置简单、即开即用等优 | 通过 VPN 连接 VPC， |

| 云产品 | 应用场景 | 描述 | 相关操作 |
| --- | --- | --- | --- |
| | 本地IDC | 点。但它的网络质量依赖 Internet。 | |
| 云专线 | 铺设物理专线高质量连接 VPC 与本地 IDC | 使用物理专线将 VPC 与本地数据中心连接起来。具备低时延、高安全、专用等优点。适用对网络传输质量和安全等级要求较高的场景 。 | 通过用户专线访问多个 VPC |

# 基于 NAT 网关和 VPC 对等连接实现跨 VPC 访问公网和对公网提供服务

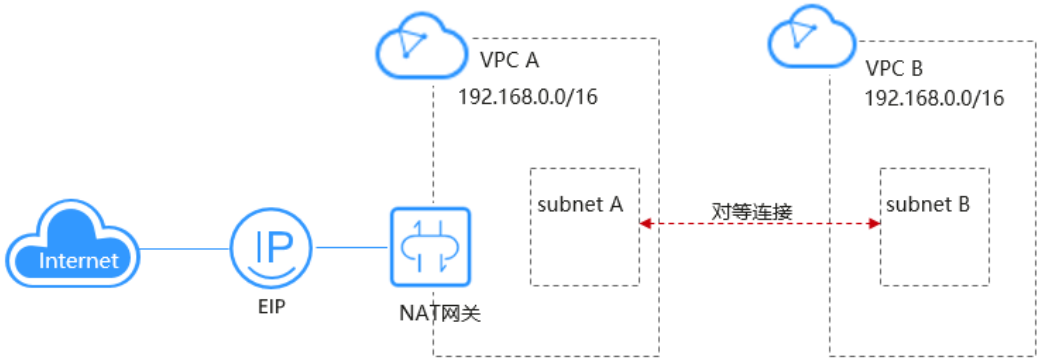
## 最佳实践概述

### 操作场景

在同一区域下有两个虚拟私有云 VPC A 和 VPC B 以及对应的子网 subnet A 和 subnet B，VPC A 中 subnet A 配置 NAT 网关，通过添加 SNAT 和 DNAT 规则可以实现访问公网和对公网提供服务；VPC B 中的 subnet B 不再另配置 NAT 网关，通过对等连接连通 subnet A，使用 subnet A 的 NAT 网关访问公网和对公网提供服务。详情见下方的组网图。

### 技术架构图

本实践方案基于如下图所示的技术架构和主要流程。




## 方案优势

两个 VPC 只需配置一个 NAT 网关实现两个 VPC 下的云服务器都能访问公网和对公网提供服务，达到节省资源的目的。

## 方案正文

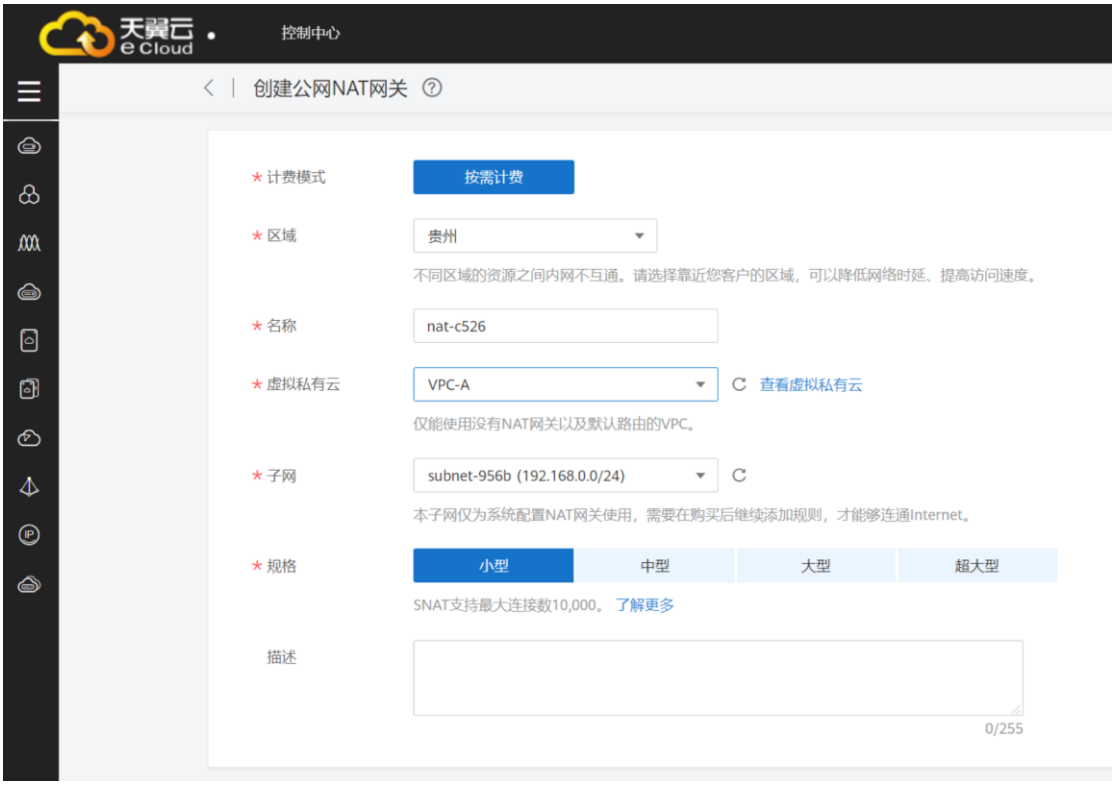
### 步骤 1 创建 VPC A 和 VPC B 及其对应的子网 subnet A 和 subnet B

具体操作请参考创建虚拟私有云和子网。

### 步骤 2 创建对等连接

在 subnet A 和 subnet B 间创建对等连接。

## 步骤 3 购买公网 NAT 网关




## 步骤 4 添加 SNAT 规则

1. 为 subnet A 添加 SNAT 规则，使用场景选择“虚拟私有云”，子网选择 subnet A。
2. 为 subnet B 添加 SNAT 规则，使用场景选择“云专线/云连接”，网段填写 subnet B.

## 步骤 5 添加 DNAT 规则

1. 为 subnet A 添加 DNAT 规则，使用场景选择“虚拟私有云”，私网 IP 填写 subnet A 中的云服务器 IP 地址。
2. 为 subnet B 添加 DNAT 规则，使用场景选择“云专线/云连接”，私网 IP 填写 subnet B 网段。

## 步骤 6 配置验证

配置完成，测试连通性。

1. 登录 subnet B 中的云服务器，ping 公网地址。
2. 登录任一不属于 VPC A 和 VPC B 的云服务器，curl 子网 subnet B 对应 DNAT 规则绑定的弹性公网 IP

# 7 常见问题

## 通用类

### 什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少个虚拟私有云。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

### 怎样查看我的配额?

1. 登录管理控制台。
2. 单击页面右上角的“My Quota”图标  。
3. 系统进入“服务配额”页面。
4. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
5. 如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

### 如何申请扩大配额?

目前系统暂不支持在线调整配额大小。如您需要调整配额，请拨打热线或发送邮件至客服，客服会及时为您处理配额调整的需求，并以电话或邮件的形式告知您实时进展。

在拨打热线或发送邮件之前，请您准备好以下信息：

帐号名，获取方式如下：

登录云帐户管理控制台，在右上角单击帐户名，选择“我的凭证”，在“我的凭证”页面获取“帐号名”。

配额信息，包括：服务名、配额类别、需要的配额值。

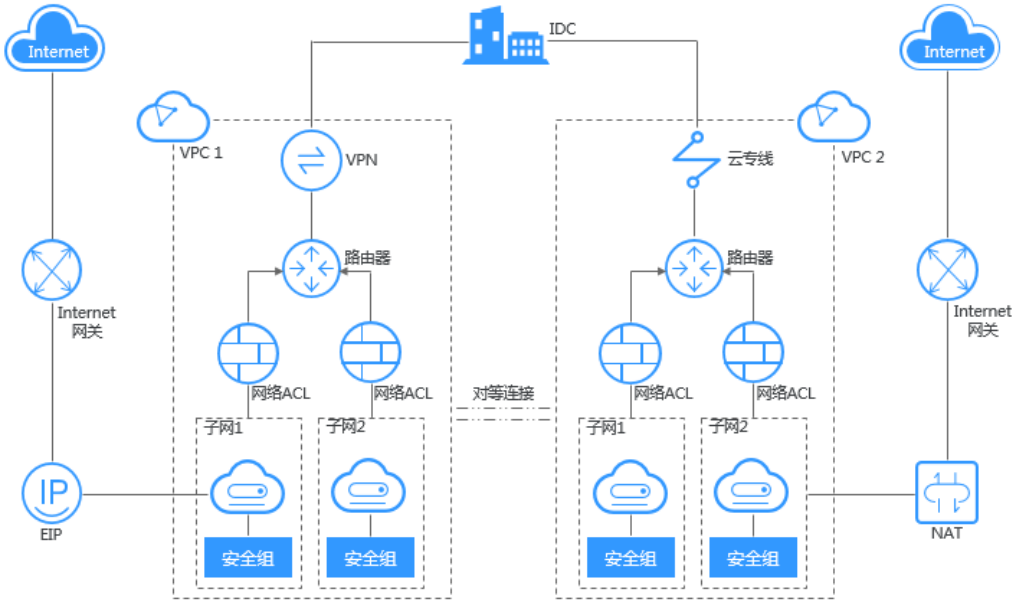
# 虚拟私有云与子网类

## 什么是虚拟私有云?

虚拟私有云（Virtual Private Cloud，以下简称 VPC），为弹性云服务器构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。

您可以在 VPC 中定义安全组、VPN、IP 地址段、带宽等网络特性。用户可以通过 VPC 方便地管理、配置内部网络，进行安全、快捷的网络变更。同时，用户可以自定义安全组内与组间弹性云服务器的访问规则，加强弹性云服务器的安全保护。

图1-1 产品架构




## VPC 中可以使用哪些网段（CIDR）?

您可以在指定的私有 IP 网段范围内，选择 VPC 的网段。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 IP 地址冲突。

当前 VPC 支持的网段如下：

| VPC 网段 | IP 地址范围 | 最大 IP 地址数 |
| --- | --- | --- |
| • 10.0.0.0/8~24 | • 10.0.0.0-10.255.255.255 | • 2^24-2=16777214 |
| • 172.16.0.0/12~24 | • 172.16.0.0-172.31.255.255 | • 2^20-2=1048574 |
| • 192.168.0.0/16~24 | • 192.168.0.0-192.168.255.255 | • 2^16-2=65534 |

## 子网间是否可以通信?

子网是属于 VPC 的资源，一个 VPC 内的子网默认可以进行通信，不同 VPC 的子网默认不能进行通信，可以通过创建对等连接使不同 VPC 的子网通信。

**说明**

- 若子网关联了网络 ACL，需先放通网络 ACL。

## 子网可以使用的网段是什么?

子网的网段要在 VPC 的网段内部，VPC 提供三段私网网段，10.0.0.0/8~24、172.16.0.0/12~24 和 192.168.0.0/16~24，子网的网段须在这些范围内，且子网的掩码范围为子网所在 VPC 掩码~29。

## 子网的限额是多少?

一个租户可以创建 100 个子网，如果无法满足实际需求，可以申请扩大配额，申请扩大配额请参考什么是配额？。

## 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?

虚拟私有云允许您创建私有、隔离的虚拟网络环境。在虚拟私有云中，可以对私有 IP 地址范围、子网和网络网关等进行控制。弹性云服务器、裸金属服务器、数据库和部分应用等会在虚拟私有云中创建的安全网络。

子网被相关资源使用时，无法删除子网。

您可以通过控制台首页查看帐户下所有资源，根据子网信息排查各资源是否在待删除的子网中。先删除子网中的全部资源，再删除子网。

可参考以下常用的资源实例进行排查，具体请以帐户下资源为准。

- 弹性云服务器
- 裸金属服务器
- RDS 实例
- Workspace
- 弹性负载均衡器
- VPN
- 私有 IP 地址
- 自定义路由
- NAT 网关
- 终端节点与终端节点服务

# 弹性 IP 类

## 一个弹性 IP 可以给几个弹性云服务器使用?

一个弹性 IP 只能绑定一个弹性云服务器使用。

## 如何通过外部网络访问绑定弹性 IP 的弹性云服务器?

为保证弹性云服务器的安全性，每个弹性云服务器创建成功后都会加入到一个安全组中，安全组默认 Internet 对内访问是禁止的，所以需要在安全组中添加对应的入方向规则，才能从外部访问该弹性云服务器。

在安全组规则设置界面用户可根据实际情况选择 TCP、UDP、ICMP 或 All 类型。

当弹性云服务器需要提供由公网可以访问到的服务且知道对端 IP 地址或无需提供由公网可以访问到的服务时，建议根据业务需要，将源地址设置为允许已知 IP 地址所在的网段访问该安全组。

当弹性云服务器需要提供由公网可以访问到的服务且不知道对端的 IP 地址时，建议使用默认的源地址 0.0.0.0/0，再通过配置端口提高网络安全性。

建议将不同公网访问策略的弹性云服务器划分到不同的安全组。

**说明**

- 源地址默认的 IP 地址 0.0.0.0/0 是指允许所有 IP 地址访问安全组内的弹性云服务器。

# 带宽类

## 带宽的限速范围是多少?

带宽的限速范围为 1Mbit/s~100Mbit/s。

## 如何使用共享带宽?

1. 登录管理控制台。
2. 在系统首页，选择"网络 > 虚拟私有云"。
3. 在左侧导航树，选择"弹性 IP 和带宽 > 共享带宽"。
4. 在页面右上角，单击"购买共享带宽"，按照提示配置参数，购买共享带宽。

## 一个共享带宽最多能对多少个弹性 IP 进行集中限速?

一个共享带宽最多针对 20 个弹性 IP 进行集中限速。如果无法满足需求，可以申请扩大配额，申请扩大配额请参考什么是配额? 。

# 连接类

## VPN 支持将两个 VPC 互连吗?

如果两个 VPC 位于同一区域内，可以使用 VPC 对等连接互连。

如果两个 VPC 位于不同区域，可以通过 VPN 连接，分别把这两个 VPC 的 CIDR 作为本端子网和远端子网。

## 弹性云服务器有多个网卡时，为何无法通过域名访问公网网站及云中的内部域名?

拥有多个网卡的弹性云服务器，如果每个网卡对应的子网中的 DNS 服务器地址配置不一致时，通过该弹性云服务器将无法访问公网网站或云中的内部域名。

请确保虚拟私有云的多个子网中的 DNS 服务器地址配置一致。您可以通过以下步骤，修改虚拟私有云子网的 DNS 服务器。

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要修改子网的虚拟私有云名称。
5. 在“子网”列表待修改子网所在行，单击“修改”，根据界面提示修改子网 DNS 服务器地址。
6. 单击“确定”，完成修改。

## 对等连接有哪些限制?

配置对等连接时，不建议两端 VPC 的网段（CIDR）存在重叠，可能会造成路由冲突，导致配置不生效。

对等连接创建完成后，可以使用“ping”命令检查本端网络是否连通，不支持通过“ping”命令检查对端子网网关是否连通。

如果两个 VPC 的 CIDR 有重叠，建立对等连接时，只能针对子网建立对等关系。如果两个 VPC 下的子网网段有重叠，那么该对等关系可能不生效。建立对等连接时，请确保对等连接两端不包含重叠的子网。

VPC A 与 VPC B、VPC C 分别建立对等连接，如果 VPC B 和 VPC C 的网段有重叠，那么 VPC A 中无法添加具有相同目的网段的路由。

两个 VPC 之间不能同时建立多个 VPC 对等连接。

不同区域的 VPC 不能创建对等连接。

VPC1 与 VPC2 创建对等连接，默认情况下 VPC2 不能通过 VPC1 的 EIP 访问公网。您可以通过使用 NAT 网关服务或配置 SNAT 服务器，使得 VPC2 下的弹性云服务器可以通过 VPC1 下绑定了 EIP 的弹性云服务器访问 Internet。。

跨租户申请 VPC 对等连接，需要对端租户接受后，才能生效。同租户申请对等连接默认已接受。

为了安全起见，请不要接受来自未知帐号的对等连接申请。

对等连接双方帐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，包括对等连接关联的路由信息。

对等连接建立后，需要在本端 VPC、对端 VPC 分别添加对方子网的路由才能通信。

VPC 对等连接路由存在时，VPC 无法被删除。

对等连接支持同区域下云平台的 VPC 与 DeC 下的 VPC 互通。跨租户申请对等连接时，为了安全，需要从 DeC 端发起申请，无法从云平台的 VPC 发起。

对等连接支持同区域的同租户的 DeC 下的 VPC 互通。

对等连接申请时，如果对端 VPC 属于某个 DeC，无法跨租户申请此对等连接。

## 为什么对等连接创建完成后不能互通?

1. 检查对等连接的两个 VPC 是否已创建对等连接，主要检查对等连接的 VPC ID。
2. 检查对等连接下的两个 VPC 是否都已添加到对端的路由信息。
3. 检查对等连接下的路由信息是否正确，当两个 VPC 网段重叠时，要配置对端子网的路由。
4. 检查对等连接的两个 VPC 的所有子网网段，是否有重叠的。
5. 检查对等连接两端要互通的弹性云服务器是否开放了安全组规则，弹性云服务器的 iptables 或防火墙是否加了限制规则。
6. 如果添加对等连接路由时，报错"路由已存在"，请检查：VPN、对等连接等路由的目的地址是否已存在。
7. 对等连接的路由 VPN 路由的目的地址有重叠，此时路由有可能失效。
8. 如果以上问题均已排除，请联系客服。

## 对等连接的配额是多少?

通过对等连接连通同一个区域 VPC 时，一个租户在一个区域内的对等连接默认配额是 50 个。

同帐户的 VPC 对等连接：在一个区域内，您可以创建 50 个 VPC 对等连接。

跨账户的 VPC 对等连接：在一个区域内，已接受的 VPC 对等连接会占用双方帐户内的配额。处于待接受状的 VPC 对等连接占用发起方的配额，不占用接受方的配额。

您可以在配额范围内创建多个帐户下的 VPC 对等连接，比如帐号 A 和帐号 B 的 VPC 对等连接，帐号 A 和帐号 C 的 VPC 对等连接，帐号 A 和帐号 D 的 VPC 对等连接等等，不受帐号数量限制。

## 同时拥有自定义路由和弹性 IP 的弹性云服务器访问外网的优先级是什么?

弹性 IP 的优先级高于自定义路由。

# 路由类

## 1 个路由表里可以存在多少个路由?

每个路由表默认可以存在 200 条路由，包括专线路由和对等连接路由等其他路由。

## 路由表有什么限制?

做 SNAT 的弹性云服务器要开启“解除 IP 和 MAC 绑定”。

路由表中每条路由信息的目的地址唯一，下一跳地址必须是该 VPC 下的私有 IP 地址或虚拟 IP，否则，路由表不会生效。

虚拟 IP 作为下一跳地址，该 VPC 下的虚拟 IP 绑定的弹性 IP 都会失效。

## 路由表收费吗?

路由表功能本身不收费，但是，弹性云服务器、带宽等是收费的。

## 同一个 VPC 下，专线和自定义路由是否有优先级关系?

专线和自定义路由使用场景是不一样的，不会出现路由优先级竞争。

## 同一个 VPC 下，VPN 和自定义路由的优先级关系是什么?

自定义路由和 VPN 的优先级是相同的。

# 安全类

## 弹性云服务器加入安全组过后能否变更安全组?

可以。进入弹性云服务器详情界面，在网卡下拉窗口选择更改安全组。

## 一个用户能拥有多少个安全组?

一个用户最多可以拥有 100 个安全组，5000 条安全组规则。

创建弹性云服务器时，可以选择多个安全组（建议不超过 5 个）。

## 多通道协议相关的安全组配置方式是什么？

用户配置弹性云服务器

TFTP 守护程序有没有数据端口配置范围的配置文件，由用户使用的 TFTP 守护程序决定，如果用户使用可配置数据通道端口的 TFTP 配置文件，建议用户配置一个没有其他监听的较小的端口范围。

用户安全组配置

用户配置安全组 69 端口，同时将 TFTP 使用的数据通道端口范围配置在安全组上；(RFC1350 定义了 FTP 协议，TFTP 协议定义了数据通道的端口范围(0，65535))；一般不同应用的 TFTP 守护程序实际上不会使用整个(0，65535)端口来做数据通道协商端口，由 TFTP 守护程序确定，推荐用户 TFTP 守护程序使用较小端口范围；

如果用户使用的数据通道端口范围为 60001-60100，则安全组规则如下所示。

图7-2 安全组规则

| Type | Protocol | Port/Range | Source |
| --- | --- | --- | --- |
| IPv4 | All | All | sg-test |
| IPv4 | UDP | 60001-60100 | 0.0.0.0/0 |

## 一个用户可以拥有多少个网络 ACL?

一个用户最多可以拥有 200 个网络 ACL，每个网络 ACL 出方向或入方向建议最多创建 20 条规则，超过 20 条会影响转发性能 。

## 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?

安全组是有状态的，即无论安全组入方向的规则如何，都允许对出方向流量的响应流入实例，反之亦然。安全组使用连接跟踪来跟踪有关进出实例的流量信息，在安全组规则增加、删除、更新时，或者该安全组下实例创建、删除时，会自动清除该安全组下所有实例入方向的连接跟踪，此时，流入或流出实例的流量会被当做新的连接，需要重新匹配相应入方向或出方向的安全组规则，以保证规则能立即生效，从而保障流入实例的流量的安全。

网络 ACL 规则配置变更，对于原有流量不会立刻生效。用户需断开变更规则所影响的流量一段时间（约 120 秒）后，变更后的规则才能对流量生效。如要确保流量在变更规则时能立即中断，建议使用安全组进行安全策略配置。

## 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?

安全组添加的规则是白名单，多个安全组规则冲突，安全组取其并集生效。