虚拟私有云

用户指南 (巴黎区域)

文档版本 01

发布日期 2022-10-31

华为技术有限公司

商标声明


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

注意

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

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

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 产品介绍 1
1.1 什么是虚拟私有云 1
1.2 应用场景 2
1.3 功能总览 2
1.4 VPC 连接 2
1.5 与其他服务的关系 3
1.6 用户权限 4
1.7 计费说明 4
1.8 基本概念 9
1.8.1 子网 9
1.8.2 弹性 IP 9
1.8.3 路由表 10
1.8.4 SNAT 11
1.8.5 安全组 12
1.8.6 对等连接 12
1.8.7 网络 ACL 12
1.8.8 虚拟 IP 14
1.8.9 区域和可用区 16
2 快速入门 18
2.1 入门指引 18
2.2 典型场景说明 18
2.3 配置无需访问公网的弹性云服务器的 VPC 18
2.3.1 简介 18
2.3.2 步骤 1：创建虚拟私有云基本信息及默认子网 20
2.3.3 步骤 2：为虚拟私有云创建新的子网 22
2.3.4 步骤 3：创建安全组 24
2.3.5 步骤 4：添加安全组规则 25
2.4 配置通过弹性 IP 访问公网的弹性云服务器的 VPC 27
2.4.1 简介 30
2.4.2 步骤 1：创建虚拟私有云基本信息及默认子网 31
2.4.3 步骤 2：为虚拟私有云创建新的子网 34
2.4.4 步骤 3：为弹性云服务器申请和绑定弹性 IP 35
2.4.5 步骤 4：创建安全组 37

2.4.6 步骤 5：添加安全组规则 38
2.5 搭建 IPv6 网络 40
3 虚拟私有云和子网 47
3.1 虚拟私有云和子网规划建议 47
3.2 虚拟私有云 50
3.2.1 创建虚拟私有云和子网 50
3.2.2 修改虚拟私有云信息 52
3.2.3 为虚拟私有云添加 IPv4 扩展网段 54
3.2.4 删除虚拟私有云的 IPv4 扩展网段 55
3.2.5 删除虚拟私有云 56
3.2.6 导出虚拟私有云列表 56
3.2.7 获取虚拟私有云的 ID 信息 57
3.2.8 查看虚拟私有云拓扑图 57
3.3 子网 57
3.3.1 为虚拟私有云创建新的子网 58
3.3.2 修改子网信息 59
3.3.3 管理子网标签 60
3.3.4 导出子网列表 61
3.3.5 查看并删除子网内的云服务资源 62
3.3.6 查看子网内 IP 地址的用途 63
3.3.7 删除子网 64
3.4 IPv4/IPv6 双栈网络 64
4 访问控制 69
4.1 安全组与网络 ACL 区别 69
4.2 安全组 70
4.2.1 安全组和安全组规则 70
4.2.2 默认安全组 73
4.2.3 安全组配置示例 74
4.2.4 管理安全组 78
4.2.4.1 创建安全组 78
4.2.4.2 克隆安全组 79
4.2.4.3 修改安全组基本信息 80
4.2.4.4 删除安全组 80
4.2.5 管理安全组规则 81
4.2.5.1 添加安全组规则 81
4.2.5.2 快速添加多条安全组规则 84
4.2.5.3 修改安全组规则 86
4.2.5.4 复制安全组规则 86
4.2.5.5 导入/导出安全组规则 87
4.2.5.6 删除安全组规则 89
4.2.6 管理安全组关联的实例 89
4.2.6.1 在安全组中添加或移出实例 89

4.2.6.2 查看弹性云服务器的安全组 90
4.2.6.3 变更弹性云服务器的安全组 91
4.3 网络 ACL 92
4.3.1 网络 ACL 简介 92
4.3.2 网络 ACL 配置示例 95
4.3.3 管理网络 ACL 96
4.3.3.1 创建网络 ACL 96
4.3.3.2 修改网络 ACL 97
4.3.3.3 开启/关闭网络 ACL 98
4.3.3.4 查看网络 ACL 98
4.3.3.5 删除网络 ACL 98
4.3.4 管理网络 ACL 规则 99
4.3.4.1 添加网络 ACL 规则 99
4.3.4.2 修改网络 ACL 规则 101
4.3.4.3 修改网络 ACL 规则生效顺序 102
4.3.4.4 开启/关闭网络 ACL 规则 103
4.3.4.5 导出/导入网络 ACL 规则 103
4.3.4.6 删除网络 ACL 规则 104
4.3.5 管理网络 ACL 关联的子网 104
4.3.5.1 将子网关联至网络 ACL 104
4.3.5.2 将子网和网络 ACL 解除关联 105
5 弹性 IP 106
5.1 弹性 IP 简介 106
5.2 为弹性云服务器申请和绑定弹性 IP 107
5.3 解绑定和释放弹性云服务器的弹性 IP 109
5.4 修改弹性 IP 的带宽配置 110
5.5 导出弹性 IP 列表 110
5.6 管理弹性 IP 地址标签 110
6 共享带宽 113
6.1 共享带宽简介 113
6.2 申请共享带宽 113
6.3 添加弹性 IP 到共享带宽 114
6.4 从共享带宽中移出弹性 IP 115
6.5 修改共享带宽 115
6.6 删除共享带宽 115
7 路由表 117
7.1 路由表和路由 117
7.2 管理路由表 119
7.2.1 创建自定义路由表 119
7.2.2 将路由表关联至子网 120
7.2.3 更换子网关联的路由表 121

7.2.4 查看子网关联的路由表 122
7.2.5 查看路由表信息 122
7.2.6 导出路由表列表 123
7.2.7 删除路由表 123
7.3 管理路由 124
7.3.1 添加自定义路由 124
7.3.2 修改路由 125
7.3.3 复制路由 126
7.3.4 删除路由 127
7.4 配置 SNAT 服务器 128
8 对等连接 131
8.1 对等连接简介 131
8.2 对等连接使用示例 132
8.3 创建相同账户下的对等连接 142
8.4 创建不同账户下的对等连接 146
8.5 获取对等连接的对端项目 ID 151
8.6 修改对等连接 151
8.7 查看对等连接 152
8.8 删除对等连接 152
8.9 修改对等连接路由 153
8.10 查看对等连接路由 154
8.11 删除对等连接路由 155
9 VPC 流日志 157
9.1 VPC 流日志简介 157
9.2 创建 VPC 流日志 158
9.3 查看 VPC 流日志 159
9.4 开启/关闭 VPC 流日志 161
9.5 删除 VPC 流日志 162
10 虚拟 IP 163
10.1 虚拟 IP 简介 163
10.2 申请虚拟 IP 地址 165
10.3 为虚拟 IP 地址绑定弹性 IP 或弹性云服务器 166
10.4 为弹性 IP 绑定虚拟 IP 地址 171
10.5 为虚拟 IP 解绑实例 172
10.6 为虚拟 IP 解绑弹性 IP 173
10.7 删除虚拟 IP 地址 173
10.8 关闭备弹性云服务器的 IP 转发功能 174
10.9 关闭弹性云服务器网卡的源/目的检查 175
11 审计 176
11.1 支持审计的关键操作 176
11.2 查看审计日志 178

12 监控 180
12.1 支持的监控指标 180
12.2 查看监控指标 182
12.3 创建告警规则 182
13 184
13.1 184
13.2 VPC 自定义策略 184
14 常见问题 186
14.1 通用类 186
14.1.1 什么是配额? 186
14.2 计费类 186
14.2.1 VPC 是否收费? 186
14.2.2 弹性 IP 如何计费? 187
14.2.3 如何切换计费方式中的“按需计费（按带宽计费）”和“按需计费（按流量计费）”? 190
14.2.4 为什么虚拟私有云 VPC 删除之后，仍在继续计费? 190
14.3 虚拟私有云与子网类 191
14.3.1 什么是虚拟私有云? 191
14.3.2 VPC 中可以使用哪些网段（CIDR）? 191
14.3.3 子网间是否可以通信? 192
14.3.4 子网可以使用的网段是什么? 192
14.3.5 子网的限额是多少? 192
14.3.6 虚拟私有云和子网无法删除，如何处理? 192
14.3.7 弹性云服务器是否支持切换虚拟私有云? 195
14.4 弹性 IP 类 195
14.4.1 弹性 IP、私有 IP 和虚拟 IP 之间有何区别? 195
14.4.2 如何通过扩展网卡绑定的弹性 IP 访问公网? 196
14.4.3 弹性云服务器的主网卡和扩展网卡在使用上有什么区别? 197
14.4.4 弹性 IP 使用独享带宽进行限速过后能否变更为使用共享带宽进行限速? 197
14.4.5 一个弹性 IP 可以给几个弹性云服务器使用? 198
14.4.6 如何通过外部网络访问绑定弹性 IP 的弹性云服务器? 198
14.4.7 弹性 IP 是否支持变更绑定的弹性云服务器? 198
14.4.8 如何为实例解绑已有弹性 IP，绑定新的弹性 IP? 198
14.4.9 弹性 IP 是否支持跨区域绑定? 200
14.4.10 弹性 IP 是否支持切换区域? 200
14.5 对等连接类 200
14.5.1 一个账户可以创建多少个对等连接? 200
14.5.2 对等连接是否可以连通不同区域的 VPC? 200
14.5.3 为什么对等连接创建完成后不能互通? 201
14.6 虚拟 IP 类 207
14.6.1 弹性云服务器的网卡绑定虚拟 IP 地址后，该虚拟 IP 地址无法 ping 通时，如何排查? 207
14.6.2 虚拟 IP 搭建的高可用集群执行服务器主备倒换后网络不通，如何处理? 211
14.7 带宽类 212

14.7.1 什么是入云带宽和出云带宽？ 212
14.7.2 如何排查带宽超过限制？ 212
14.7.3 公网带宽与内网带宽有何差异？ 214
14.7.4 带宽的限速范围是多少？ 214
14.7.5 带宽的类型有哪些？ 214
14.7.6 独享带宽与共享带宽有何区别？ 214
14.7.7 一个共享带宽最多能对多少个弹性 IP 进行集中限速？ 215
14.7.8 带宽与上传下载速率是什么关系？ 215
14.8 网络连接类 215
14.8.1 VPN 支持将两个 VPC 互连吗？ 215
14.8.2 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？ 215
14.8.3 同时拥有自定义路由和弹性 IP 的访问外网的优先级是什么？ 215
14.8.4 本地主机访问使用弹性云服务器搭建的网站出现间歇性中断怎么办？ 216
14.8.5 同一个子网下的弹性云服务器只能通过内网 IP 地址单向通信怎么办？ 216
14.8.6 同一个 VPC 内的两台弹性云服务器无法互通或者出现丢包等现象时，如何排查？ 217
14.8.7 Cloud-init 连接出现问题时，如何排查？ 220
14.8.8 EIP 连接出现问题时，如何排查？ 223
14.8.9 弹性云服务器 IP 获取不到时，如何排查？ 226
14.8.10 VPN 及专线网络连接出现问题时，如何排查？ 227
14.8.11 外网能访问服务器，但是服务器无法访问外网时，如何排查？ 229
14.8.12 配置了 IPv6 双栈，为什么无法访问 IPv6 网站？ 230
14.8.13 弹性云服务器防火墙配置完成后，为什么网络不通？ 231
14.9 路由类 232
14.9.1 如何配置多网卡弹性云服务器的策略路由？ 232
14.9.2 路由表可以跨 VPC 存在吗？ 233
14.9.3 1 个路由表里可以存在多少个路由？ 234
14.9.4 路由表有什么限制？ 234
14.9.5 同一个 VPC 下，专线和自定义路由是否有优先级关系？ 234
14.9.6 同一个 VPC 下，VPN 和自定义路由的优先级关系是什么？ 234
14.10 安全类 234
14.10.1 安全组规则除描述字段外，其他字段均相同，是否算作相同的安全组规则？ 234
14.10.2 如何查看安全组关联了哪些实例？ 234
14.10.3 为什么无法删除安全组？ 235
14.10.4 弹性云服务器加入安全组过后能否变更安全组？ 235
14.10.5 多通道协议相关的安全组配置方式是什么？ 235
14.10.6 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？ 236
14.10.7 安全组和安全组规则优先级哪个更高？ 236
14.10.8 为什么网络 ACL 添加了拒绝特定 IP 地址访问的规则，但仍可以访问？ 236
14.10.9 为什么配置的安全组规则不生效？ 237
A 修订记录 240

1 产品介绍

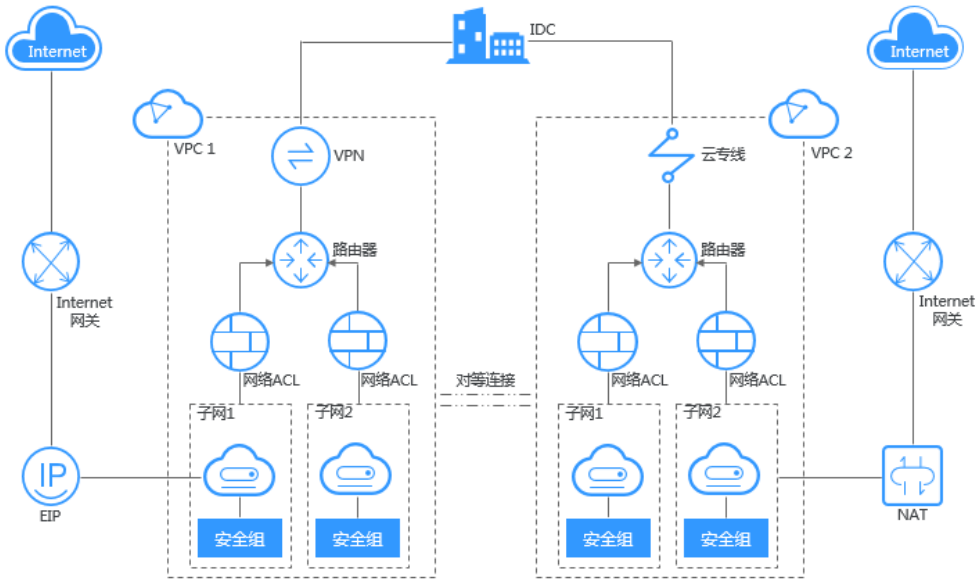
1.1 什么是虚拟私有云

简介

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 VPC 组成



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，具体操作请参见。

1.2 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连接弹性云服务器与Internet，运行弹性云服务器上部署的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服务器、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。

1.3 功能总览

列出了虚拟私有云VPC的常用功能。

在使用虚拟私有云VPC之前，建议您先通过基本概念介绍了解子网、路由表、安全组、弹性IP等基本概念，以便更好地理解虚拟私有云VPC提供的功能。

1.4 VPC 连接

为了满足您不同场景下连接Internet的需求，公有云以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。

- **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，公有云NAT网关来帮您，它提供SNAT和DNAT两种功能。SNAT可轻松实现同一VPC内的多个弹性云服务器共享一个或多个弹性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。

1.5 与其他服务的关系

- 弹性云服务器

  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。提供多种方式连接弹性云服务器与Internet。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。

- 弹性负载均衡

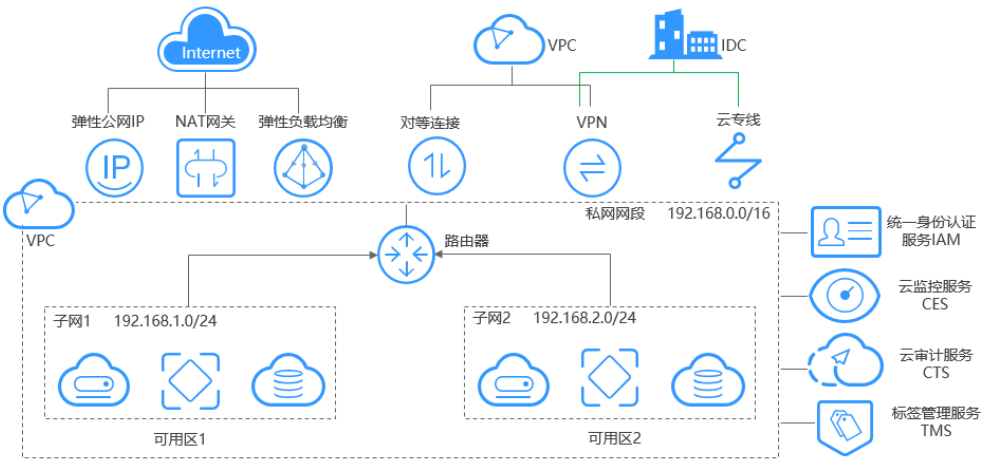
  弹性负载均衡需要使用虚拟私有云服务创建的弹性IP、带宽。

- 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。

虚拟私有云VPC服务与其他服务的关系，如图1-2所示。

图 1-2 与其他服务的关系



1.6 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。

1.7 计费说明

计费项

VPC本身不收取费用。

表 1-1 计费项信息

计费项	计费说明
弹性IP	如有互联网访问需求，您需要购买弹性IP。

弹性IP为您提供多种计费方式，供您灵活选择，本节为您详细介绍弹性IP的计费情况，主要包含以下内容：

- **弹性IP的计费情况概览**
- **如何选择弹性IP的计费方式?**
- **修改带宽大小如何收费?**
- **如何变更弹性IP的计费方式?**

弹性 IP 的计费情况概览

弹性IP提供“按需计费”的计费模式。以下为您详细介绍EIP的计费情况：

- 快速了解EIP计费情况，请参见**图1-3**。
- 详细了解EIP计费情况，请参见**表1-2**。

图 1-3 弹性 IP 计费概览

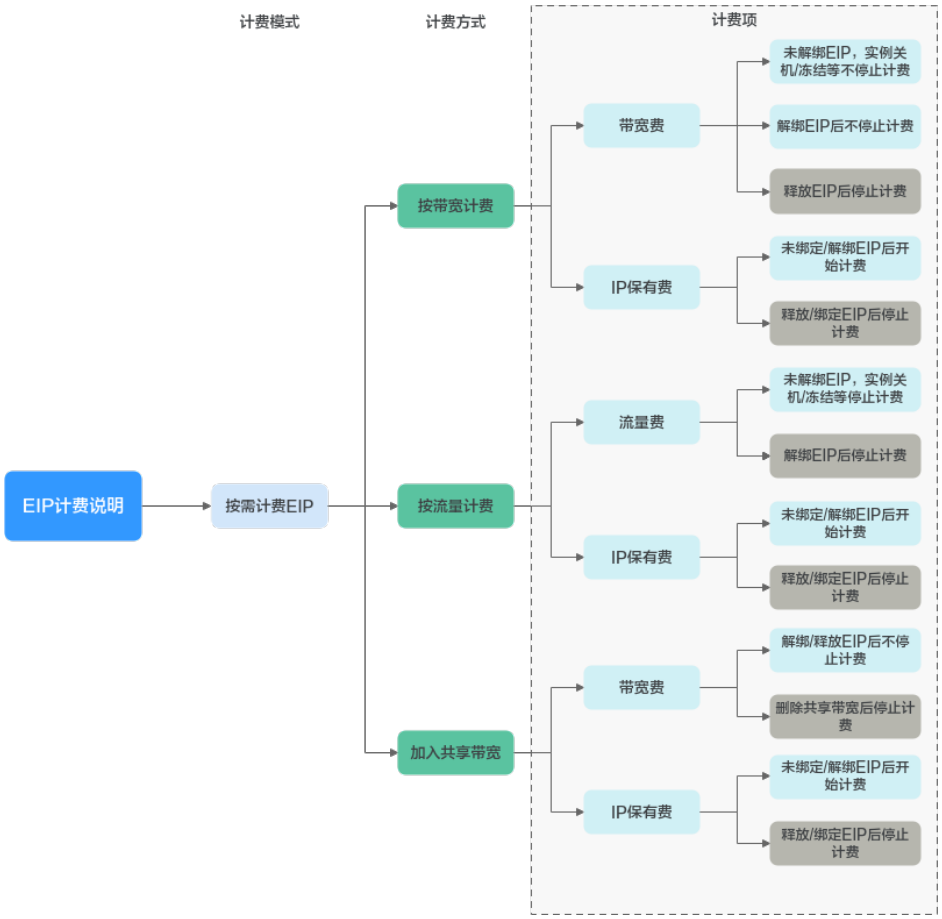


表 1-2 弹性 IP 计费情况说明

计费模式	计费方式	计费项	计费项说明	操作EIP对计费项的影响
按需计费	按带宽计费	• 带宽费 • 保有费	按需计费的EIP选择按带宽计费时，有以下两个计费项： • 带宽费：按照您指定的带宽大小及实际使用时长计费，不限流量。您购买EIP时可以指定带宽大小，后续支持修改。使用过程中，您实际的带宽不能高于指定带宽大小。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 未绑定EIP，收取带宽费和保有费。 • 绑定EIP后，收取带宽费，停止收取保有费。**无论EIP绑定的实例是否运行，不影响费用，比如ECS关机后，会继续收取带宽费，不收取保有费。** • **解绑EIP后，继续收取带宽费，同时新增保有费。** • 释放EIP后，停止收取带宽费和保有费。

计费模式	计费方式	计费项	计费项说明	操作EIP对计费项的影响
	按流量计费	• 流量费 • 保有费	按需计费的EIP选择按流量计费时，有以下两个计费项： • 流量费：按照您指定的线路类型及实际流量使用量计费，云平台仅收取出网流量费用，不收取入网流量费用。 按流量计费的EIP，带宽仅做限速使用，不收取费用。为了防止突然爆发的流量产生较高的费用，建议您购买EIP的时候指定带宽大小，为出网带宽设置一个峰值。 按流量计费的EIP使用的独享带宽，仅收取出云方向带宽费用，不收取入云方向带宽费用。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 未绑定EIP，不收取流量费，收取保有费。 • 绑定EIP后，按照实际产生的流量收取流量费用，停止收取保有费。 **EIP绑定的实例停止运行后，不产生流量则不收取流量费，比如ECS关机后，停止收取流量费，不收取保有费。** • **解绑EIP后，停止收取流量费，同时新增保有费。** • 释放EIP后，停止收取保有费。
	加入共享带宽	• 带宽费 • 保有费	按需计费的EIP选择加入共享带宽时，有以下两个计费项： • 带宽费：此处带宽费为共享带宽的费用，共享带宽中可同时加入多个EIP，这些EIP使用期间的带宽和流量均不再单独计费，以共享带宽的费用为准。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 带宽费： – **对EIP执行的任何操作，均不影响共享带宽计费情况。比如您已经释放了EIP，但是未删除共享带宽，则共享带宽会继续计费。** – 删除共享带宽，停止收取带宽费。 • 保有费： – 未绑定EIP，收取保有费。 – **解绑EIP后，新增保有费。** – 释放/绑定EIP后，停止收取保有费。

您可以将同一个区域内的多个EIP加入一条共享带宽中，实现带宽复用，为您节省费用。共享带宽单独计费，共享带宽提供“按需计费”的计费模式。共享带宽费用说明请参见表1-3。当前只有按需计费的EIP可以加入共享带宽中：

- 您可以在购买EIP时，将EIP加入共享带宽。
- 您还可以将已有的EIP加入共享带宽，EIP原有的按带宽计费或者按流量计费会停止，后续只收取共享带宽费用。

表 1-3 共享带宽计费情况说明

计费模式	计费方式	计费项	计费项说明
按需计费	按带宽计费	带宽费	按照您指定的带宽大小及实际使用时长计费，不限流量。 您购买共享带宽时可以指定带宽大小，后续支持修改。使用过程中，您实际的带宽不能高于指定带宽大小。

说明

- 带宽费、流量费，保有费三个计费项在不同区域的费用不同，请您以控制台的实际显示费用为准。
- EIP的带宽指的是出云方向的带宽，即从云平台流出到Internet方向的带宽。例如：云内的ECS对外提供服务，外部用户下载云内ECS上的资源。EIP仅对出云带宽收取费用。
  - 如果您购买/修改后的带宽大小<=10Mbit/s，则入云方向带宽为10Mbit/s，出云方向带宽大小为购买/修改后的带宽大小。
  - 如果您购买/修改后的带宽大小>10Mbit/s，则出云方向和入云方向带宽相同，均等于购买/修改后的带宽大小。

如何选择弹性 IP 的计费方式?

弹性IP支持按带宽计费和按流量计费两种方式，不同计费方式推荐的适用场景如表1-4所示。

云监控服务可以帮助您掌握您的带宽和流量等网络指标数据，通过带宽使用率可以计算出使用按带宽计费和按流量计费哪种方式更划算。按照以往的经验，为您提供如下建议供参考：

- 带宽大小低于5 Mbit/s，且使用时长不长，整体流量较小时，建议您选择按流量计费会更划算。
- 带宽大小高于5 Mbit/s，并且带宽使用率大于20%时，一般选择按带宽计费会更划算。

表 1-4 弹性 IP 计费方式适用场景

计费模式	计费方式	推荐适用场景
按需计费	按带宽计费	适用于流量大或访问量稳定场景
	按流量计费	适用于流量低或访问量波动较大场景

计费模式	计费方式	推荐适用场景
	加入共享带宽	适用于多业务流量高峰分布于不同时段，需节约公网成本场景

修改带宽大小如何收费?

弹性IP未加入共享带宽时，不管哪种计费方式，一律使用的是独享带宽。弹性IP加入共享带宽后，以共享带宽的费用为准。

当您修改带宽大小时，不同计费方式的带宽收费和生效时间不同，请您参考表1-5了解详情，适用于独享带宽和共享带宽两种情况。

说明

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

表 1-5 修改带宽大小的费用情况

计费模式	计费方式	变更操作	对费用的影响
按需计费	按带宽计费	增加/降低带宽大小	增加/降低带宽大小后，新的带宽大小和计费方式将立即生效。
	按流量计费	增加/降低带宽大小	增加/降低带宽大小后，新的带宽大小将立即生效。 按流量计费的EIP，带宽仅做限速使用，带宽大小不影响实际费用。

如何变更弹性 IP 的计费方式?

EIP提供多种计费方式供您灵活选择，EIP使用期间，不同的计费方式支持切换。

- 不同计费变更场景的详细说明，请参见表1-6。

说明

变更计费方式不会更换EIP的地址，也不会中断EIP的使用，对您的业务不会产生影响。

表 1-6 弹性 IP 计费方式变更说明

计费方式变更场景	计费变更说明
• 按需计费（按流量计费）→按需计费（按带宽计费） • 按需计费（按带宽计费）→按需计费（按流量计费）	• 按需计费（按流量计费）EIP支持直接转为按需计费（按带宽计费）EIP。 • 按需计费（按带宽计费）EIP支持直接转为按需计费（按流量计费）EIP。 该变更操作成功后，新的计费方式将立即生效。

按需计费（按带宽计费）与按需计费（按流量计费）计费方式转换的操作步骤请参考**如何切换计费方式中的“按需计费（按带宽计费）”和“按需计费（按流量计费）”？**。

1.8 基本概念

1.8.1 子网

子网是虚拟私有云内的IP地址集，可以将虚拟私有云的网段分成若干块，子网划分可以帮助您合理规划IP地址资源。虚拟私有云中的所有云资源都必须部署在子网内。同一个虚拟私有云下，子网网段不可重复。

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

  比如VPC-A的网段为10.0.0.0/16，则您可以规划子网A01的网段为10.0.0.0/24，子网A02的网段为10.0.1.0/24，子网A03的网段为10.0.3.0/24。

  说明

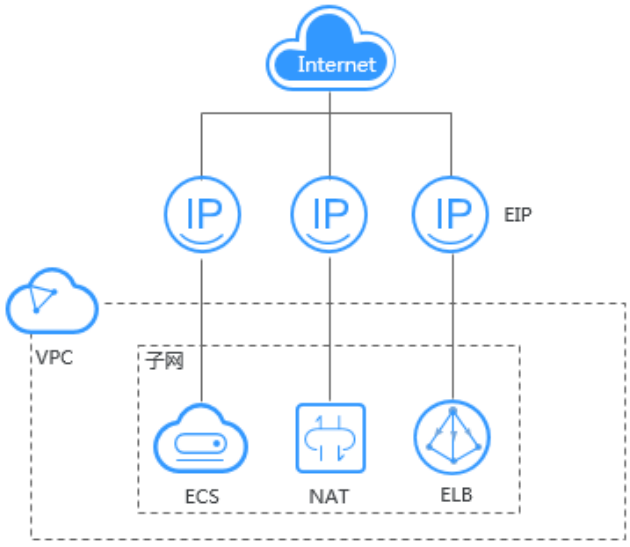
  一个用户在单个区域可创建的虚拟私有云子网数量默认为100个，如果您需要提升配额，请参见**什么是配额?**。

1.8.2 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 1-4 通过 EIP 访问公网



1.8.3 路由表

路由表

路由表由一系列路由规则组成，用于控制VPC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，一个子网只能关联一个路由表，但一个路由表可以同时关联至多个子网。

- 默认路由表：用户创建VPC时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。默认路由表可以确保VPC内子网之间网络互通。
  - 您可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。
  - 创建VPN、VPC终端节点、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。
- 自定义路由表：您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。

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

说明

路由

您可以在默认路由表和自定义路由表中添加路由，路由包括目的地址、下一跳类型、下一跳地址等信息，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。自定义路由的目的地址不能与系统路由的目的地址重叠。

  您可以通过添加自定义路由来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1-7**所示。

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

表 1-7 下一跳类型

下一跳类型	说明	支持添加该类型路由的路由表
服务器实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。	• 默认路由表 • 自定义路由表
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。	• 默认路由表 • 自定义路由表
VPN网关	将指向目的地址的流量转发到一个VPN网关。	自定义路由表
云专线网关	将指向目的地址的流量转发到一个云专线网关。	自定义路由表
NAT网关	将指向目的地址的流量转发到一个NAT网关。	• 默认路由表 • 自定义路由表
对等连接	将指向目的地址的流量转发到一个对等连接。	• 默认路由表 • 自定义路由表
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。	• 默认路由表 • 自定义路由表

说明

目前暂不支持配置云专线服务类型的路由策略，如需使用请提交工单申请。

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

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

1.8.4 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需要消耗重要资源（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）。

公有云支持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**。

1.8.5 安全组

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

安全组规则遵循白名单规则，具体说明如下：

- 入方向规则：入方向指外部访问安全组内实例的指定端口。

  当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。

  因此，默认情况下，您一般不用在入方向配置策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。
- 出方向规则：出方向指安全组内实例访问外部的指定端口。

  在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。

  0.0.0.0/0表示匹配所有IPv4地址。

1.8.6 对等连接

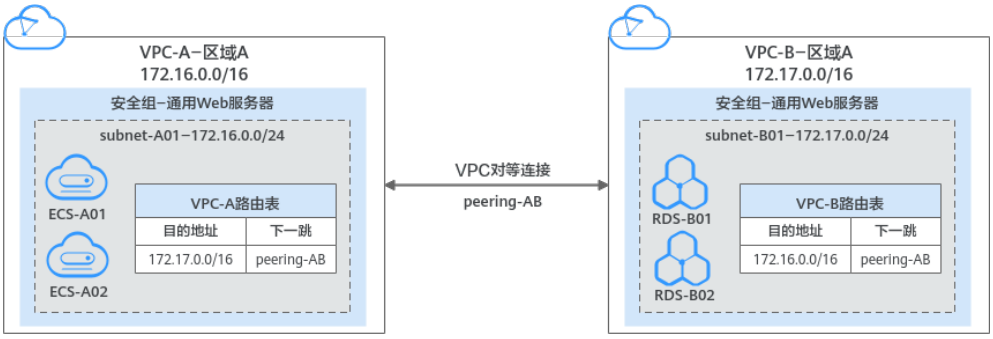
对等连接是建立在两个VPC之间的网络连接，不同VPC之间网络不通，通过对等连接可以实现不同VPC之间的云上内网通信。对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。

- 您可以通过对等连接构建不同的组网，常见的使用示例请参见**对等连接使用示例**。

接下来，通过**图1-5**中简单的组网示例，为您介绍对等连接的使用场景。

- 在区域A内，您的两个VPC分别为VPC-A和VPC-B，VPC-A和VPC-B之间网络不通。
- 您的业务服务器ECS-A01和ECS-A02位于VPC-A内，数据库服务器RDS-B01和RDS-B02位于VPC-B内，此时业务服务器和数据库服务器网络不通。
- 您需要在VPC-A和VPC-B之间建立对等连接Peering-AB，连通VPC-A和VPC-B之间的网络，业务服务器就可以访问数据库服务器。

图 1-5 对等连接组网示意图

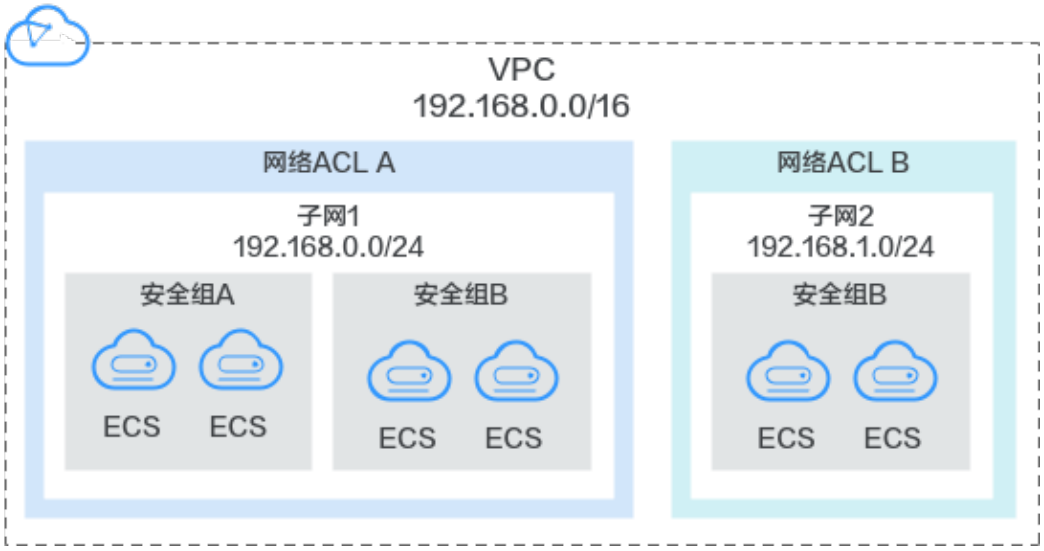


对等连接的详细内容，具体参考**对等连接**。

1.8.7 网络 ACL

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网络流量。

图 1-6 安全组与网络 ACL



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可以同时关联多个子网，但一个子网只能关联一个网络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使用连接跟踪来标识进出实例的流量信息，入方向和出方向网络ACL规则配置变更，对原有流量不会立即生效。

  当您在网络ACL内增加、删除、更新规则，或者在网络ACL内添加、移出子网时，由入方向/出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有网络ACL规则。入方向/出方向流量新建立的连接，将会匹配新的网络ACL出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

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1-8**所示。该规则不能修改和删除。

表 1-8 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

流量匹配网络 ACL 规则的顺序

- 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。

1.8.8 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。

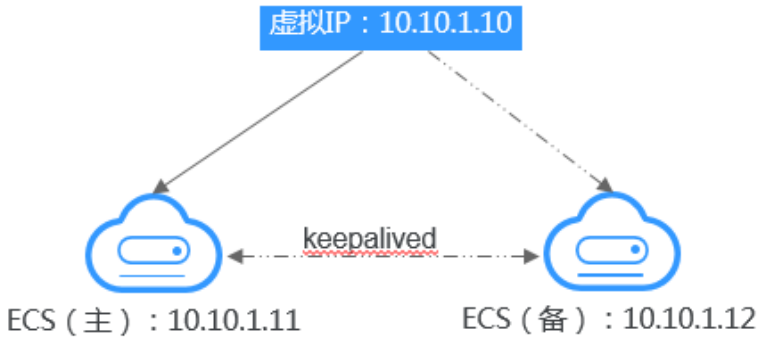
典型组网

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 1-7 HA 高可用性模式组网图

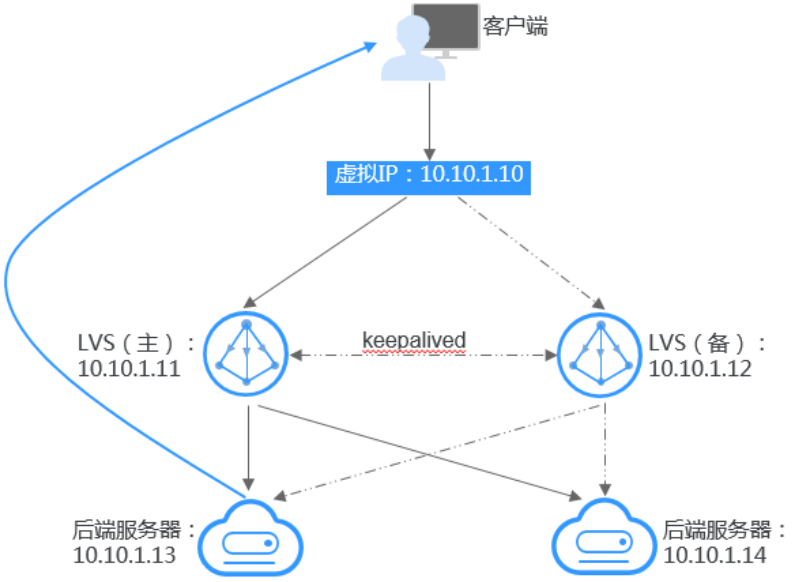
  

  - 将2台同子网的弹性云服务器绑定同一个虚拟IP。
  - 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **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 1-8 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）。

1.8.9 区域和可用区

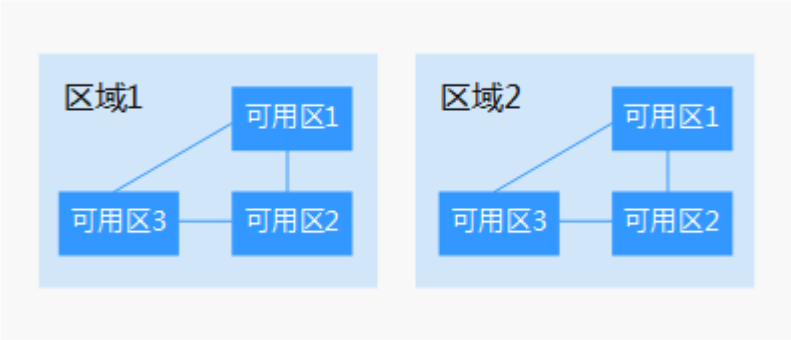
什么是区域、可用区?

区域和可用区用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1-9阐明了区域和可用区之间的关系。

图 1-9 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。有关云服务的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2 快速入门

2.1 入门指引

本文将为您介绍如何快速搭建IPv4网段或IPv6网段的VPC，以及搭建前的准备工作。

网段类型简介

IPv4：创建VPC及子网时，默认创建的网段为IPv4类型。IPv4网络无法访问Internet上的IPv6服务或为使用IPv6终端的用户提供访问服务。搭建IPv4地址网络请参见。

IPv6：当您需要访问Internet上的IPv6服务或为使用IPv6终端的用户提供访问服务时，需要在配置时开启IPv6功能，开启后，您将拥有IPv4和IPv6两个网段，可以为IPv4和IPv6终端用户提供访问服务。搭建IPv6地址网络请参见。

2.2 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。

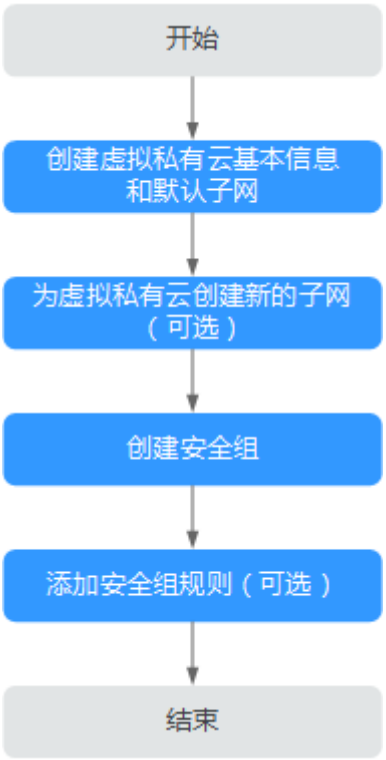
- 当弹性云服务器无需访问公网时，例如用于搭建网站的数据库节点或服务器节点的弹性云服务器无需连接公网，该类型弹性云服务器的虚拟私有云配置请参考**配置无需访问公网的弹性云服务器的VPC**。
- 当弹性云服务器需要访问公网时可通过配置弹性IP实现，例如用于搭建网站时允许接受访客通过网络访问的业务节点，该类型弹性云服务器的虚拟私有云配置请参考**配置通过弹性IP访问公网的弹性云服务器的VPC**。
- 当您需要访问Internet上的IPv6服务或为使用IPv6终端的用户提供访问服务时，需要在配置时开启IPv6功能，开启后，您将拥有IPv4和IPv6两个网段，可以为IPv4和IPv6终端用户提供访问服务。

2.3 配置无需访问公网的弹性云服务器的 VPC

2.3.1 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2-1**所示。

图 2-1 配置网络功能



配置网络流程图说明如表2-1所示。

表 2-1 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。 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。 当默认子网不能满足您的需求时，您可以创建新的子网。 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。 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。 创建安全组成功后，具备默认的访问规则。

任务	说明
添加安全组规则	可选任务。 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。

2.3.2 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 单击“创建虚拟私有云”。
   进入“创建虚拟私有云”页面。
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 2-2 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	VPC名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-test

参数	说明	取值样例
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。 目前支持网段范围： ● 10.0.0.0/8~24 ● 172.16.0.0/12~24 ● 192.168.0.0/16~24	192.168.0.0/16
高级配置	单击下拉箭头，可配置VPC的高级参数，包括标签等。	默认配置
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。	● 键：vpc_key1 ● 值：vpc-01

表 2-3 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
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。 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	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
标签	子网的标识，包括键和值。最多可以为子网创建10个标签。	• 键：subnet_key1 • 值：subnet-01

表 2-4 虚拟私有云标签命名规则

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

表 2-5 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

2.3.3 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，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。

操作步骤

1. 登录管理控制台。

2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
4. 单击“创建子网”。
   进入“创建子网”页面。
5. 根据界面提示配置参数。

表 2-6 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。	-
名称	子网的名称。 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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
高级配置/网关	子网的网关。 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
高级配置/DNS服务器地址	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x
高级配置/标签	子网的标识，包括键和值。您最多可以为子网创建10个标签。 标签的命名规则请参考**表2-7**。	• 键：subnet_key1 • 值：subnet-01

表 2-7 子网标签命名规则

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

2.3.4 步骤 3：创建安全组

操作场景

安全组实际是网络流量访问策略，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表右上方，单击“创建安全组”。
   进入“创建安全组”页面。
5. 根据界面提示，设置安全组参数。

表 2-8 参数说明

参数	参数说明	取值样例
名称	必选参数。 安全组的名称。 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。 **说明** 安全组名称创建后可以修改，建议不要重名。	sg-AB
描述	可选参数。 安全组的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

2.3.5 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，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

安全组规则遵循白名单规则，具体说明如下：

- 入方向规则：入方向指外部访问安全组内实例的指定端口。

  当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。

  因此，默认情况下，您一般不用在入方向配置策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。
- 出方向规则：出方向指安全组内实例访问外部的指定端口。

  在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。

  0.0.0.0/0表示匹配所有IPv4地址。

如果实例关联的安全组策略无法满足使用需求，比如需要开放某个TCP端口，您可以参考以下操作，通过在入方向规则添加端口，从而打开指定的TCP端口。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。

   进入安全组列表页面。

4. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。
   进入安全组规则配置页面。
5. 在“入方向规则”页签，单击“添加规则”。
   弹出“添加入方向规则”对话框。
6. 根据界面提示，设置入方向规则参数。
   单击“+”按钮，可以依次增加多条入方向规则。

表 2-9 入方向规则参数说明

参数	说明	取值样例
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	22或22-30
源地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段） 若源地址为安全组，则选定安全组内的云服务器都遵从当前所创建的规则。	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 入方向规则设置完成后，单击“确定”。
   返回入方向规则列表，可以查看添加的入方向规则。
8. 在“出方向规则”页签，单击“添加规则”。
   弹出“添加出方向规则”页签。
9. 根据界面提示，设置出方向规则参数。
   单击“+”按钮，可以依次增加多条出方向规则。

表 2-10 出方向规则参数说明

参数	说明	取值样例
类型	目的地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在出方向规则中，表示安全组内实例访问外部的指定端口。	22或22-30
目的地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

10. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

2.4 配置通过弹性 IP 访问公网的弹性云服务器的 VPC

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 单击“创建虚拟私有云”。
   进入“创建虚拟私有云”页面。
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 2-11 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	VPC名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-test
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。 目前支持网段范围： ● 10.0.0.0/8~24 ● 172.16.0.0/12~24 ● 192.168.0.0/16~24	192.168.0.0/16
高级配置	单击下拉箭头，可配置VPC的高级参数，包括标签等。	默认配置
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。	● 键：vpc_key1 ● 值：vpc-01

表 2-12 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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
子网IPv6网段	选择是否勾选开启IPv6。 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。	-

参数	说明	取值样例
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
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。 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	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x
标签	子网的标识，包括键和值。最多可以为子网创建10个标签。	• 键：subnet_key1 • 值：subnet-01

表 2-13 虚拟私有云标签命名规则

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

表 2-14 子网标签命名规则

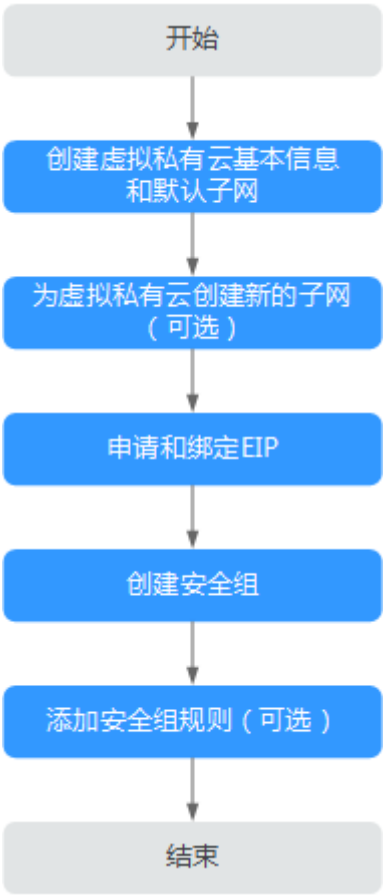
参数	规则	样例
键	• 不能为空。 • 对于同一子网键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	subnet_key1
值	• 长度不超过43个字符。	subnet-01

5. 检查当前配置，单击“立即创建”。

2.4.1 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2-2所示。

图 2-2 配置网络功能



配置网络流程图说明如表2-15所示。

表 2-15 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。 该任务是创建一个完整的虚拟私有云的第一步。 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。

任务	说明
为虚拟私有云创建新的子网	可选任务。 当默认子网不能满足您的需求时，您可以创建新的子网。 此处创建的子网就是创建弹性云服务器时添加的网卡。
申请和绑定弹性IP	必选任务。 可以通过申请弹性IP并将弹性IP绑定到上，实现弹性云服务器访公网的目的。
创建安全组	必选任务。 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，以提升访问的安全性。 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。 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。

2.4.2 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. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 单击“创建虚拟私有云”。
   进入“创建虚拟私有云”页面。
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 2-16 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	VPC名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-test
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。 目前支持网段范围： ● 10.0.0.0/8~24 ● 172.16.0.0/12~24 ● 192.168.0.0/16~24	192.168.0.0/16
高级配置	单击下拉箭头，可配置VPC的高级参数，包括标签等。	默认配置
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。	● 键：vpc_key1 ● 值：vpc-01

表 2-17 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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
子网IPv6网段	选择是否勾选开启IPv6。 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。	-

参数	说明	取值样例
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
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。 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	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x
标签	子网的标识，包括键和值。最多可以为子网创建10个标签。	• 键：subnet_key1 • 值：subnet-01

表 2-18 虚拟私有云标签命名规则

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

表 2-19 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

2.4.3 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，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。

操作步骤

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

表 2-20 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。	-
名称	子网的名称。 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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
高级配置/网关	子网的网关。 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
高级配置/DNS服务器地址	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
高级配置/标签	子网的标识，包括键和值。您最多可以为子网创建10个标签。 标签的命名规则请参考表2-21。	• 键：subnet_key1 • 值：subnet-01

表 2-21 子网标签命名规则

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

2.4.4 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. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“弹性IP”界面，单击“创建弹性IP”。

4. 根据界面提示配置参数。

表 2-22 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。创建EIP时所选择的区域即为EIP的归属地。	-
线路	全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。	全动态BGP
公网带宽	带宽类型分为以下几种： ● 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。适用于流量较大或较稳定场景使用。 ● 按流量计费：指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。适用于流量小或流量波动较大的场景。 ● 加入共享带宽：共享带宽可以针对多个弹性IP进行集中限速，可以加入多个弹性IP，被多个弹性IP地址共用。适用于多业务流量错峰分布场景。	按带宽计费
带宽大小	带宽大小，单位Mbit/s。	100
弹性IP名称	弹性IP的名称。	eip-test
带宽名称	带宽的名称。	bandwidth
标签	用于标识弹性IP地址。包括键和值。 标签的命名规则请参考**表2-23**。	● 键：Ipv4_key1 ● 值：3005eip
创建数量	弹性IP数量。	1

表 2-23 弹性 IP 地址标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一弹性IP地址键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	Ipv4_key1
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	3005eip

5. 单击“立即申请”。

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”。

2.4.5 步骤 4：创建安全组

操作场景

安全组实际是网络流量访问策略，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表右上方，单击“创建安全组”。
   进入“创建安全组”页面。
5. 根据界面提示，设置安全组参数。

表 2-24 参数说明

参数	参数说明	取值样例
名称	必选参数。 安全组的名称。 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。 **说明** 安全组名称创建后可以修改，建议不要重名。	sg-AB
描述	可选参数。 安全组的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

2.4.6 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，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

安全组规则遵循白名单规则，具体说明如下：

- 入方向规则：入方向指外部访问安全组内实例的指定端口。

  当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。

  因此，默认情况下，您一般不用在入方向配置策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。
- 出方向规则：出方向指安全组内实例访问外部的指定端口。

  在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。

  0.0.0.0/0表示匹配所有IPv4地址。

如果实例关联的安全组策略无法满足使用需求，比如需要开放某个TCP端口，您可以参考以下操作，通过在入方向规则添加端口，从而打开指定的TCP端口。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。

   进入安全组列表页面。

4. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。
   进入安全组规则配置页面。
5. 在“入方向规则”页签，单击“添加规则”。
   弹出“添加入方向规则”对话框。
6. 根据界面提示，设置入方向规则参数。
   单击“+”按钮，可以依次增加多条入方向规则。

表 2-25 入方向规则参数说明

参数	说明	取值样例
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	22或22-30
源地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段） 若源地址为安全组，则选定安全组内的云服务器都遵从当前所创建的规则。	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 入方向规则设置完成后，单击“确定”。
   返回入方向规则列表，可以查看添加的入方向规则。
8. 在“出方向规则”页签，单击“添加规则”。
   弹出“添加出方向规则”页签。
9. 根据界面提示，设置出方向规则参数。
   单击“+”按钮，可以依次增加多条出方向规则。

表 2-26 出方向规则参数说明

参数	说明	取值样例
类型	目的地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在出方向规则中，表示安全组内实例访问外部的指定端口。	22或22-30
目的地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

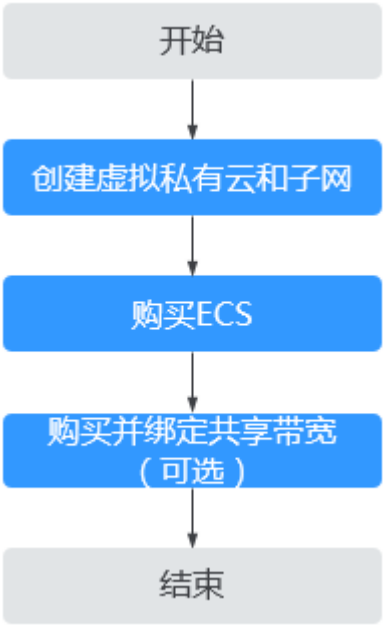
10. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

2.5 搭建 IPv6 网络

操作场景

本教程将指引您搭建一个IPv6网段的VPC，并在VPC中创建一个带有IPv6地址的ECS，使ECS可以访问Internet上的IPv6服务。配置流程如图2-3所示。

图 2-3 搭建 IPv6 网络



说明

若您已有共享带宽，在购买ECS时可直接配置IPv6访问公网。

约束与限制

- IPv6双栈，当前暂不收费，后续定价会根据运营商收费策略的变化进行调整。
- 弹性云服务器ECS部分规格支持IPv6网络，只有选择支持IPv6的ECS，才可以使用IPv4/IPv6双栈网络，请务必选择支持的区域和规格。

  您可以通过以下方法查看ECS哪些规格支持IPv6：

  - 通过ECS控制台查看：单击“创建弹性云服务器”，进入创建页面查看ECS规格列表。

    当ECS规格列表中包含“IPv6”参数，且取值为“是”时，表示该规格的ECS支持IPv6。

IPv4/IPv6 双栈网络的应用场景及资源规划

表 2-27 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 • IPv6网段	• IPv4私有地址：用于IPv4内网通信 • IPv6地址：用于IPv6内网通信

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 • IPv6网段	• IPv4私有地址+IPv4 EIP地址：用于IPv4公网通信 • IPv6地址+共享带宽：用于IPv6公网通信
	您在ECS上部署应用并面向公网客户端提供服务，既要支持客户端通过IPv6地址访问，还要对这些访问来源进行数据分析		

步骤 1：创建虚拟私有云和子网

在创建VPC之前，您需要根据具体的业务需求规划VPC的数量、子网的数量和IP网段划分等。

请按如下操作，创建一个VPC“vpc-ipv6”和一个IPv6默认子网“subnet-ipv6”。

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 单击“创建虚拟私有云”。
4. 根据界面提示配置虚拟私有云和子网参数。
   子网配置时，请务必勾选“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。

表 2-28 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	VPC名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-test
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。 目前支持网段范围： • 10.0.0.0/8~24 • 172.16.0.0/12~24 • 192.168.0.0/16~24	192.168.0.0/16

参数	说明	取值样例
高级配置	单击下拉箭头，可配置VPC的高级参数，包括标签等。	默认配置
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。	● 键：vpc_key1 ● 值：vpc-01

表 2-29 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
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。 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	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x
标签	子网的标识，包括键和值。最多可以为子网创建10个标签。	● 键：subnet_key1 ● 值：subnet-01

5. 单击“立即创建”。

步骤 2：购买 ECS

在管理控制台，选择“计算 > 弹性云服务器”，购买一个ECS实例。

网络配置请按如下设置：

- 网络：
  - 虚拟私有云：选择已创建的“vpc-ipv6”。
  - 子网：选择已创建的“subnet-ipv6”。
  - 务必选择“自动分配IPv6地址”。

    须知

    当前仅支持在创建的时候为云服务器分配IPv6地址，因此请您务必勾选“自动分配IPv6地址”，否则将无法使用IPv4/IPv6双栈网络。

  - 共享带宽
    - 当选择“暂不配置”，则仅支持VPC内的IPv6相互通信。若要开启公网访问功能，后续需要进行**（可选）步骤3：购买和加入共享带宽**。
    - 当此时新建共享带宽或选择已有共享带宽，则配置完成后IPv6 地址直接开启公网访问功能。
- 安全组：选择默认安全组“Sys-default”。默认安全组的规则是在出方向上的IPv4/IPv6数据报文全部放行，入方向访问受限，安全组内的弹性云服务器无需添加规则即可互相访问。您也可以创建新的安全组并配置规则。
- 弹性IP：选择“暂不购买”。

购买完成后，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。

动态获取IPv6地址（可选）

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。

（可选）步骤 3：购买和加入共享带宽

默认IPv6地址只具备私网通信能力，如果您需要通过该IPv6地址访问Internet或被Internet上的IPv6客户端访问，您需要购买和绑定共享带宽。

如您已有共享带宽，可以不用重新购买，直接将IPv6地址加入共享带宽即可。

购买共享带宽

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。

4. 在页面右上角，单击“申请共享带宽”，按照提示配置参数。

表 2-30 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。	-
计费方式	共享带宽的计费方式。 支持按带宽计费、按流量计费。	按带宽计费
带宽大小	共享带宽的大小，单位Mbit/s，5M起售，最大支持2000Mbit/s。	10
名称	共享带宽的名称。	Bandwidth-001

5. 单击“立即申请”。

加入共享带宽

1. 在共享带宽列表页，单击操作列的“添加公网IP”。

图 2-4 加入共享带宽入口

2. 将IPv6地址加入共享带宽。

图 2-5 添加 IPv6 双栈网卡到共享带宽

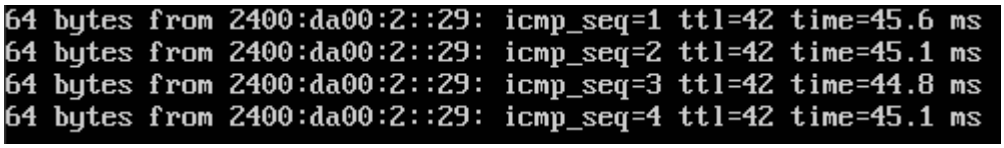
3. 单击“确定”。

结果验证

登录到ECS实例，ping一个公网上的IPv6服务，验证连通性。执行结果样例如图2-6所示。

您可以使用SSH方式、或RDP文件通过EIP地址登录该ECS。

图 2-6 结果验证



3 虚拟私有云和子网

3.1 虚拟私有云和子网规划建议

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

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

如何规划 VPC?

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

- 一个VPC

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

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

说明

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

您可以在特定的私有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。

VPC支持的网段范围如**表3-1**所示。

表 3-1 VPC 网段

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

如何规划子网?

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

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

  比如VPC-A的网段为10.0.0.0/16，则您可以规划子网A01的网段为10.0.0.0/24，子网A02的网段为10.0.1.0/24，子网A03的网段为10.0.3.0/24。

  说明

  一个用户在单个区域可创建的虚拟私有云子网数量默认为100个，如果您需要提升配额，请参见**什么是配额?** 。

当您规划VPC子网时，可以参考以下原则：

- 同一个VPC内的业务，您可以根据业务模块划分子网，比如在VPC-A内，子网A01用于Web层，子网A02用于管理层，子网A03用于数据层。根据业务划分子网模块，有利于结合网络ACL进行网络防护。
- 如果您要通过VPN/云专线连通云上VPC和线下IDC的网络，则VPC子网网段和IDC内的网段不能重叠，您在新建VPC及子网的时候务必避开IDC内的网段。

如何规划路由策略?

用户创建VPC时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。路由表由一系列路由规则组成，用于控制VPC内子网的出流量走向。默认路由表可以确保VPC内子网之间网络互通。

您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并关联至子网。自定义路由表仅影响子网的出流量走向，入流量仍然匹配默认路由表。

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

- 系统路由：系统自动添加且无法修改或删除的路由，表示VPC内实例互通。
- 自定义路由：可以修改和删除的路由。自定义路由的目地地址不能与系统路由的目地地址重叠。

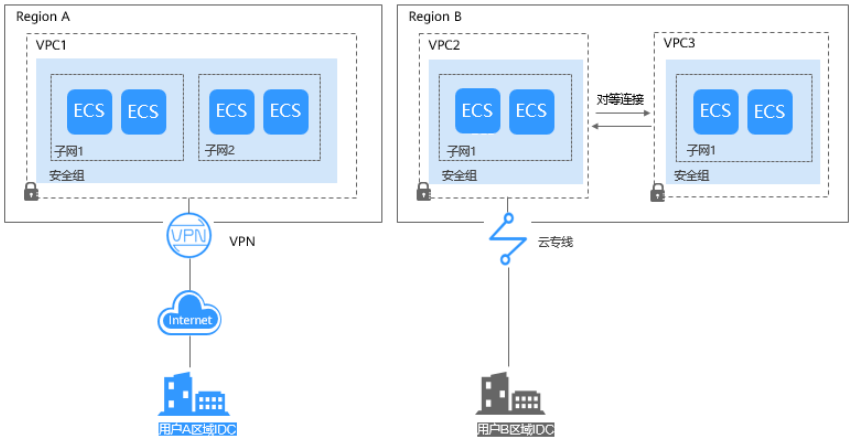
  您无法在VPC路由表中添加目的地址相同的两条路由，即使路由的下一跳类型不同也不行。因此不论路由的下一跳是何种类型，路由的优先级均取决于目的地址，遵循最长匹配原则，即优先选择匹配度更高的目的地址进行路由转发。

如何连接本地 IDC?

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

如图3-1所示，比如您在A区域有一个VPC1，B区域有两个VPC，分别为VPC2和VPC3。VPC1需要连接用户A区域IDC，通过VPN走Internet互连。VPC2需要连接用户B区域IDC，通过云专线连接。同时在B区域的VPC3与VPC2通过对等连接建立连接。

图 3-1 IDC 连接



此例中，各VPC网段划分需要注意以下几点：

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

如何连接 Internet?

少量弹性云服务器通过弹性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。

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，公有云NAT网关来帮您，它提供SNAT和DNAT两种功能。SNAT可轻松实现同一VPC内的多个弹性云服务器共享一个或多个弹性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。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。

3.2 虚拟私有云

3.2.1 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 单击“创建虚拟私有云”。
   进入“创建虚拟私有云”页面。
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 3-2 虚拟私有云参数说明

参数	说明	取值样例
区域	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。	-
名称	VPC名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	VPC-test
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。 目前支持网段范围： ● 10.0.0.0/8~24 ● 172.16.0.0/12~24 ● 192.168.0.0/16~24	192.168.0.0/16

参数	说明	取值样例
高级配置	单击下拉箭头，可配置VPC的高级参数，包括标签等。	默认配置
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。	● 键：vpc_key1 ● 值：vpc-01

表 3-3 子网参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
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。 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	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x
标签	子网的标识，包括键和值。最多可以为子网创建10个标签。	● 键：subnet_key1 ● 值：subnet-01

表 3-4 虚拟私有云标签命名规则

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

表 3-5 子网标签命名规则

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

5. 检查当前配置，单击“立即创建”。

3.2.2 修改虚拟私有云信息

操作场景

您可以参考以下操作修改虚拟私有云的信息，修改操作如下：

- **修改虚拟私有云名称和描述**
- **修改虚拟私有云网段**

须知

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

修改虚拟私有云名称和描述

1. 登录管理控制台。

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

修改虚拟私有云网段

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

须知

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

- 当虚拟私有云下不存在子网时，您可以修改IP地址和掩码。

  图 3-2 修改 IP 地址和掩码

- 当虚拟私有云下存在子网时，您只可以修改掩码。

图 3-3 修改掩码

5. 网段信息设置完成后，单击“确定”保存修改。

3.2.3 为虚拟私有云添加 IPv4 扩展网段

操作场景

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

说明

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

约束与限制

- 创建子网时候，您可以基于主网段或者扩展网段来分配子网网段，但是一个子网网段，要么属于主网段，要么属于扩展网段，不能两个网段混用。

  同一个VPC内的子网默认互通，基于主网段的子网和基于扩展网段的子网也是默认互通。
- 扩展网段的子网地址与VPC路由表中已有路由的目的地址相同或者重叠，会导致已有路由不生效。

  在扩展网段中创建子网时，系统会为该子网生成一条目的地址为子网网段，下一跳为Local的路由，Local路由属于VPC内部路由，优先级高于VPC路由表中添加的其他路由。比如，VPC路由表已有某个下一跳为对等连接的路由，其目的地址为100.20.0.0/24；新增扩展网段子网的路由，其目的地址为100.20.0.0/16，100.20.0.0/16和100.20.0.0/24网段重叠，流量优先通过扩展网段子网的路由转发，会导致对等连接的路由失效。
- VPC扩展网段支持的掩码范围为8 ~ 28。
- 不支持添加的扩展网段范围如**表3-6**所示。

表 3-6 不支持添加的扩展网段范围

网段类型	不支持的网段范围
私有网段预留地址	• 172.31.0.0/16 • 192.168.0.0/16 • 主网段已使用的私网网段

网段类型	不支持的网段范围
系统内部预留地址	• 100.64.0.0/10 • 214.0.0.0/7 • 198.18.0.0/15 • 169.254.0.0/16
公网保留地址	• 0.0.0.0/8 • 127.0.0.0/8 • 240.0.0.0/4 • 255.255.255.255/32

操作步骤

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

3.2.4 删除虚拟私有云的 IPv4 扩展网段

操作场景

当虚拟私有云的扩展网段不再使用时，您可以参考以下操作删除扩展网段。

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

操作步骤

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

3.2.5 删除虚拟私有云

操作场景

本章节指导用户删除虚拟私有云。

约束与限制

虚拟私有云通常由于被子网、自定义路由或者其他服务资源使用而导致无法删除，需要您根据控制台的提示信息删除占用虚拟私有云的资源，然后删除虚拟私有云。

请您参考**虚拟私有云和子网无法删除，如何处理？**，根据控制台提示，删除占用虚拟私有云的服务资源。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在虚拟私有云列表中，单击待删除的虚拟私有云所在行“操作”列下的“删除”。
   弹出删除确认对话框。
4. 确认无误后，单击“是”，删除虚拟私有云。

须知

如果此时虚拟私有云无法删除，那么控制台会有对应的提示信息，请您参考**虚拟私有云和子网无法删除，如何处理？**，删除占用虚拟私有云的服务资源。

3.2.6 导出虚拟私有云列表

操作场景

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

该文件记录了虚拟私有云的名称、ID、状态、网段、子网个数等信息。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在虚拟私有云列表中，单击列表右上方的 。
   系统会将您账号下，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。

3.2.7 获取虚拟私有云的 ID 信息

操作场景

本章节指导用户查看并获取虚拟私有云的ID信息，即VPC ID。

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

操作步骤

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

   单击VPC ID后面 的可以复制ID信息。

3.2.8 查看虚拟私有云拓扑图

操作场景

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

操作步骤

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

3.3 子网

3.3.1 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，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。

操作步骤

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

表 3-7 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。	-
名称	子网的名称。 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
子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配IPv6网段，暂不支持自定义设置IPv6网段。该功能一旦开启，将不能关闭。	-
关联路由表	子网创建完成后默认关联默认路由表，您也可以通过子网的更换路由表操作，切换至自定义路由表。	默认
高级配置/网关	子网的网关。 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
高级配置/DNS服务器地址	DNS服务器地址最多支持2个IP，请以英文逗号隔开。	100.125.x.x

参数	说明	取值样例
高级配置/标签	子网的标识，包括键和值。您最多可以为子网创建10个标签。 标签的命名规则请参考表3-8。	• 键：subnet_key1 • 值：subnet-01

表 3-8 子网标签命名规则

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

3.3.2 修改子网信息

操作场景

本章节指导用户修改子网名称、DNS服务器地址等。

操作步骤

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

4. 在子网列表中，单击待修改的子网名称超链接。
   进入子网详情页面。
5. 在子网的“基本信息”页签中，单击待修改参数右侧的 ，根据界面提示修改参数。

   表 3-9 参数说明

参数	说明	取值样例
名称	子网的名称。 名称只能由英文字母、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。最多支持2个IP地址，多个IP地址以英文逗号隔开。	100.125.x.x
描述	子网的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

6. 单击“确定”。

3.3.3 管理子网标签

应用场景

标签是子网的标识。通过为子网添加标签，可以方便您识别和管理拥有的子网。

您可以在创建子网的时候添加标签，或者在已经创建的子网详情页添加标签，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”，“键”和“值”的命名规则如表3-10所示。

表 3-10 子网标签命名规则

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

操作步骤

在子网列表页，按标签的键或值搜索目标子网。

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表上方的搜索框中，单击框中任意位置，设置搜索条件。
   在“属性类型”列表中，根据需要的标签选择对应的键和值。系统会根据您设置的标签搜索条件筛选对应的资源。

在子网的标签页，执行标签的增、删、改、查操作。

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，单击待查询子网的名称。
5. 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，输入修改后标签的键和值，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”。

3.3.4 导出子网列表

操作场景

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

操作步骤

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

进入虚拟私有云列表页面。

3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，勾选一个或多个子网，单击列表左上方的“导出”。
   系统会将您所选的子网信息自动导出为Excel文件，并下载至本地。

3.3.5 查看并删除子网内的云服务资源

操作场景

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

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

须知

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，找到目标子网，并单击子网名称超链接。
   进入子网详情页面。
5. 在“基本信息”页签，查看占用子网的云服务资源。
   a. 在页面下方的资源概览区域，查看占用子网的各资源（弹性云服务器、裸金属服务器、弹性网卡、弹性负载均衡等）的数量。单击资源数量超链接，查看占用子网的资源。
   b. 在页面右侧的网络互通概览区域，查看占用子网的NAT网关。
6. 执行以下操作，删除子网内的云服务资源。

表 3-11 删除子网内的云服务资源

云服务资源类型	操作指导
弹性负载均衡	当前支持通过子网页面直接跳转到目标弹性负载均衡： 1. 根据界面提示，单击弹性负载均衡区域的数量超链接。进入弹性负载均衡列表页面。 2. 确认释放资源后，单击弹性负载均衡所在行的操作列下的“删除”。

3.3.6 查看子网内 IP 地址的用途

操作场景

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

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

约束与限制

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

操作步骤

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

后续操作

如果您需要查看并删除占用子网的资源，请参见**虚拟私有云和子网无法删除，如何处理？**。

3.3.7 删除子网

操作场景

如果您的子网不需要使用，您可以参考以下操作删除子网。

约束与限制

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

请您参考**虚拟私有云和子网无法删除，如何处理？**，根据控制台提示，删除占用子网的服务资源。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，单击待删除子网所在行的操作列下的“删除”。
   弹出删除确认对话框。
5. 确认无误后，单击“是”，删除子网。

须知

如果此时子网无法删除，那么控制台会有对应的提示信息，请您参考**虚拟私有云和子网无法删除，如何处理？**，删除占用子网的服务资源。

3.4 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，通过绑定共享带宽的方式，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。

约束与限制

- IPv6双栈，当前暂不收费，后续定价会根据运营商收费策略的变化进行调整。
- 弹性云服务器ECS部分规格支持IPv6网络，只有选择支持IPv6的ECS，才可以使用IPv4/IPv6双栈网络，请务必选择支持的区域和规格。

  您可以通过以下方法查看ECS哪些规格支持IPv6：

  - 通过ECS控制台查看：单击“创建弹性云服务器”，进入创建页面查看ECS规格列表。

    当ECS规格列表中包含“IPv6”参数，且取值为“是”时，表示该规格的ECS支持IPv6。

IPv6 网络的应用场景

如果您的ECS规格支持IPv6，您可以使用IPv4/IPv6双栈网络，场景示例和资源规划如表3-12所示。

表 3-12 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 • IPv6网段	• IPv4私有地址：用于IPv4内网通信 • IPv6地址：用于IPv6内网通信
IPv6公网通信	您在ECS上部署应用并面向公网客户端提供服务，支持客户端通过IPv6地址访问	• IPv4网段 • IPv6网段	• IPv4私有地址+IPv4 EIP地址：用于IPv4公网通信 • IPv6地址+共享带宽：用于IPv6公网通信
	您在ECS上部署应用并面向公网客户端提供服务，既要支持客户端通过IPv6地址访问，还要对这些访问来源进行数据分析		

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，将在管理控制台不能关闭。

图 3-4 创建 IPv6 子网

查看已使用IPv6地址

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

添加IPv6安全组规则

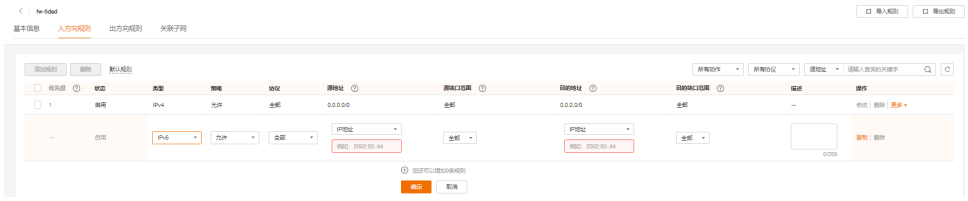
参考**添加安全组规则**添加安全组规则，类型选择“IPv6”，源地址或目的地址填写IPv6地址。

图 3-5 添加 IPv6 安全组规则

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。

图 3-6 添加 IPv6 网络 ACL 规则



添加IPv6弹性IP/IPv6双栈网卡到共享带宽

参考**添加弹性IP到共享带宽**将IPv6弹性IP、IPv6双栈网卡添加到共享带宽。

图 3-7 添加 IPv6 双栈网卡到共享带宽

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。

图 3-8 添加路由

申请IPv6虚拟IP地址

参考**申请虚拟IP地址**申请虚拟IP地址，其中IP类型可以选择“IPv4”或“IPv6”。

图 3-9 申请虚拟 IP 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

创建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。

4 访问控制

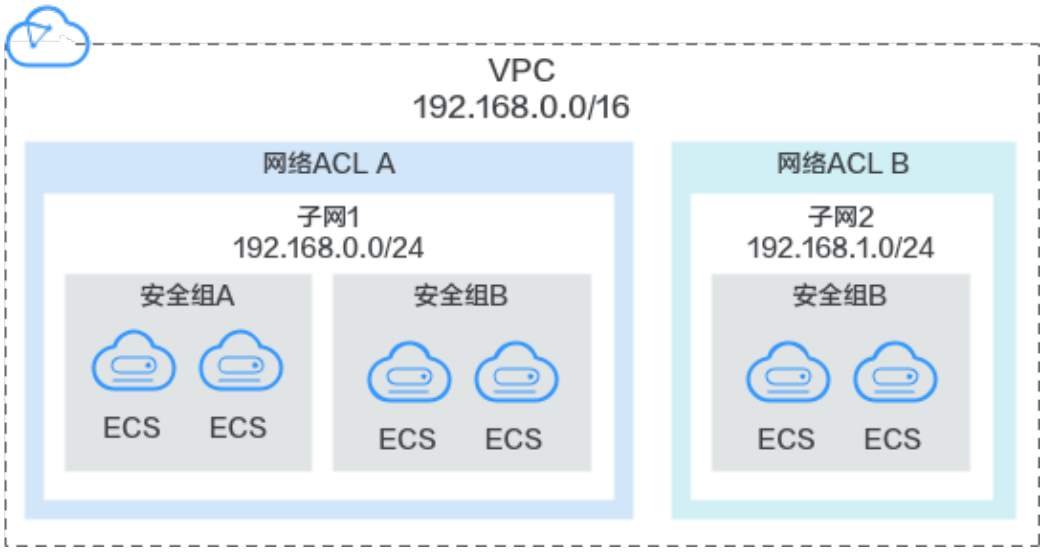
4.1 安全组与网络 ACL 区别

通过配置网络ACL和安全组策略，可以保障虚拟私有云内的实例安全运行，比如弹性云服务器、数据库、云容器实例等。

- 安全组对实例进行防护，将实例加入安全组内，该实例将会受到安全组的保护。
- 网络ACL对整个子网进行防护，将子网关联至网络ACL，则子网内的所有实例都会受到网络ACL保护。相比安全组，网络ACL的防护范围更大。

安全组和网络ACL的关系如图4-1所示。本示例中，安全组A和安全组B可以保护其中ECS的网络安全，通过网络ACL A和网络ACL B，可以分别保护整个子网1和子网2的安全，双层防护提升安全保障。

图 4-1 安全组与网络 ACL



网络ACL和安全组区别如表4-1所示。

表 4-1 安全组和网络 ACL 区别说明

对比项	安全组	网络ACL
防护范围	安全组防护安全组内的实例，比如弹性云服务器、数据库、云容器实例等。	网络ACL防护整个子网，子网内的所有实例都会受到网络ACL保护。
配置策略	不支持允许、拒绝策略。	支持允许、拒绝策略。
规则生效顺序	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	• 创建实例（比如弹性云服务器）时，必须选择一个安全组，如果当前用户名下没有安全组，则系统会自动创建一个默认安全组。 • 实例创建完成后，您可以执行以下操作： – 在安全组控制台，添加/移出实例。 – 在实例控制台，为实例添加/移除安全组。	创建子网没有网络ACL选项，需要先创建网络ACL，添加出入规则，并在网络ACL内关联子网。当网络ACL状态为已开启，将会对子网生效。
报文组	支持报文三元组（即协议、端口和源/目的地址）过滤。	支持报文五元组（即协议、源端口、目的端口、源地址和目的地址）过滤。

4.2 安全组

4.2.1 安全组和安全组规则

安全组

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

如果您未创建任何安全组，那么在首次创建需要使用安全组的实例时（比如弹性云服务器），系统会自动为您创建一个默认安全组并关联至该实例，关于默认安全组的更多信息，请参见**默认安全组**。

安全组基本信息

- 安全组是有状态的。如果您从实例发送一个出站请求，且该安全组的出方向规则是放通的话，那么无论其入方向规则如何，都将允许该出站请求的响应流量流入。同理，如果该安全组的入方向规则是放通的，那无论出方向规则如何，都将允许入站请求的响应流量可以流出。

- 安全组使用连接跟踪来标识进出实例的流量信息，入方向安全组的规则变更，对原有流量立即生效。出方向安全组规则的变更，不影响已建立的长连接，只对新建立的连接生效。

  当您在安全组内增加、删除、更新规则，或者在安全组内添加、移出实例时，系统会自动清除该安全组内所有实例入方向的连接，详细说明如下：

  - 由入方向流量建立的连接，已建立的长连接将会断开。所有入方向流量立即重新建立连接，并匹配新的安全组入方向规则。
  - 由出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有安全组规则。出方向流量新建立的连接，将会匹配新的安全组出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

安全组规则

安全组中包括入方向规则和出方向规则，用来控制安全组内实例的入方向和出方向的网络流量。安全组规则由协议端口、源地址/目的地址等组成，关键信息的说明如**表4-2**所示。

表 4-2 安全组规则详细信息

参数	说明
协议类型	安全组规则中用来匹配流量的网络协议类型。目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。
端口范围	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 ● 在入方向规则中，表示外部访问安全组内实例的指定端口。 ● 在出方向规则中，表示安全组内实例访问外部的指定端口。

参数	说明
源地址（入方向）	源地址是入方向规则中，用来匹配外部访问请求的地址，支持多种格式： ● IP地址： – 单个IPv4地址：示例为192.168.10.10/32。 – IPv4网段：示例为192.168.52.0/24。如果要匹配所有IPv4地址，设置为0.0.0.0/0。 ● 安全组：您可以选择当前账号下，同一个区域内的其他安全组作为源地址。 当安全组A内有实例a，安全组B内有实例b，在安全组A设置入方向规则时的“策略”为允许，源地址选择安全组B时，表示来自实例b的内网访问请求被允许进入实例a。
目的地址（出方向）	目的地址是出方向规则中，用来匹配内部请求访问的地址，支持多种格式： ● IP地址： – 单个IPv4地址：示例为192.168.10.10/32。 – IPv4网段：示例为192.168.52.0/24。如果要匹配所有IPv4地址，设置为0.0.0.0/0。 ● 安全组：您可以选择当前账号下，同一个区域内的其他安全组作为目的地址。 当安全组A内有实例a，安全组B内有实例b，在安全组A设置出方向规则时的“策略”为允许，目的地址选择安全组B时，表示实例a内部的请求被允许出去访问实例b。

安全组规则遵循白名单规则，具体说明如下：

- 入方向规则：入方向指外部访问安全组内实例的指定端口。

  当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。

  因此，默认情况下，您一般不用在入方向配置策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。
- 出方向规则：出方向指安全组内实例访问外部的指定端口。

  在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。

  0.0.0.0/0表示匹配所有IPv4地址。

如表4-3所示，以自定义安全组sg-AB为例，根据sg-AB的入方向和出方向规则，为您详细解释安全组的规则。

表 4-3 安全组 sg-AB 的规则说明

规则方向	协议端口	源地址/目的地址	描述
入方向规则	全部	源地址：sg-AB	针对全部IPv4协议，允许本安全组内云服务器的请求进入，即该条规则确保安全组内的云服务器网络互通。
入方向规则	TCP:22	源地址：0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的SSH(22)端口，用于远程登录Linux云服务器。
入方向规则	TCP:3389	源地址：0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的RDP(3389)端口，用于远程登录Windows云服务器。
入方向规则	TCP:80	源地址：10.5.6.30/32	针对TCP(IPv4)协议，允许外部IP(10.5.6.30)访问安全组内云服务器的80端口。
出方向规则	全部	目的地址：0.0.0.0/0	针对全部IPv4协议，允许安全组内的云服务器可访问外部IP的所有端口。

须知

- 在安全组规则中放开某个端口后，为了确保网络正常通信，您还需要确保实例内对应的端口也已经放通。
- 通常情况下，同一个安全组内的实例默认网络互通。当同一个安全组内实例网络不通时，可能情况如下：
  - 在入方向规则中，删除了同一个安全组内实例互通对应的规则。
  - 不同VPC的网络不通，所以当实例属于同一个安全组，但属于不同VPC时，网络不通。

    您可以通过**VPC对等连接**连通不同区域的VPC。

安全组的限制

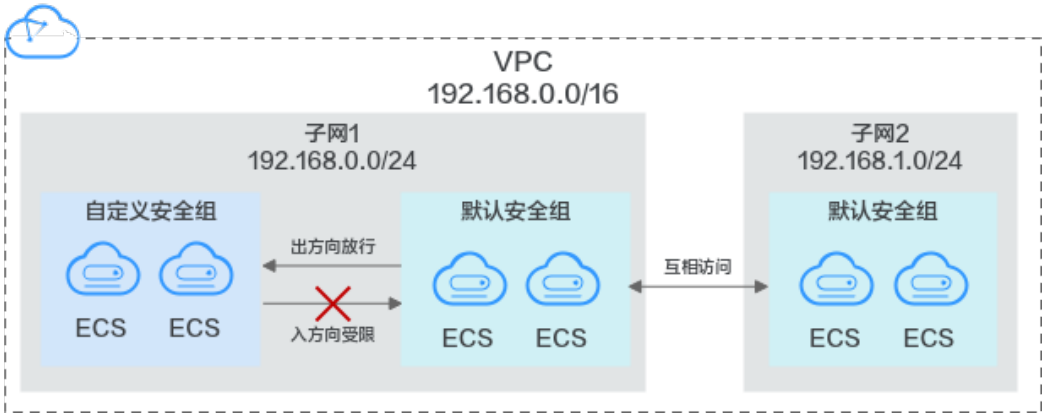
- 默认情况下，一个安全组最多只允许拥有50条安全组规则。
- 默认情况下，一个云服务器或扩展网卡最多只能被添加到5个安全组中，安全组规则取并集生效。

4.2.2 默认安全组

如果您未创建任何安全组，那么您在首次使用安全组时，系统会自动为您创建一个默认安全组，默认安全组规则说明如下：

- 入方向规则：入方向流量受限，只允许安全组内实例互通，拒绝来自安全组外部的所有访问请求。
- 出方向规则：出方向流量放行，允许所有内部请求出去，并收到该请求对应的响应流量。

图 4-2 默认安全组



说明

- 您无法删除默认安全组，可以在默认安全组内修改已有规则或者添加新的规则。
- 默认安全组拒绝所有外部请求，如果您需要登录默认安全组关联的实例，请参见**从本地服务器远程登录云服务器**添加安全组规则。

默认安全组规则如**表4-4**所示。

表 4-4 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*)	仅允许安全组内的云服务器彼此通信，丢弃其他入站流量的全部数据报文。

4.2.3 安全组配置示例

本章节为您介绍一些常用的安全组的配置示例，包括远程登录云服务器，对外提供网站访问、不同安全组内实例内网互通等。

通常情况下，安全组默认拒绝所有来自外部的请求。您需要遵循白名单原则添加安全组入方向规则，允许来自外部的特定请求访问安全组内实例。具体示例如下：

- **从本地服务器远程登录云服务器**
- **在本地服务器远程连接云服务器上传或者下载文件**
- **在云服务器上搭建网站对外提供Web服务**
- **使用ping命令验证网络连通性**
- **不同安全组内实例内网网络互通**
- **云服务器提供数据库访问服务**
- **限制云服务器访问外部网站**

安全组的出方向规则一般默认全部放通，即允许安全组内实例访问外部的所有请求出去，配置说明如表4-5所示。

表 4-5 安全组默认出方向规则

规则方向	协议端口	目的地址	描述
出方向规则	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部IP的所有端口。

从本地服务器远程登录云服务器

安全组默认拒绝所有来自外部的请求，如果您需要从本地服务器远程登录云服务器，那么需要根据您的云服务器操作系统类型，在安全组入方向添加对应的规则。

- 通过SSH远程登录Linux云服务器，需要放通SSH(22)端口，请参见表4-6。
- 通过RDP远程登录Windows云服务器，需要放通RDP(3389)端口，请参见表4-7。

表 4-6 通过 SSH 远程登录 Linux 云服务器

规则方向	协议端口	源地址
入方向规则	自定义TCP: 22	IP地址：0.0.0.0/0

表 4-7 通过 RDP 远程登录 Windows 云服务器

规则方向	协议端口	源地址
入方向规则	自定义TCP: 3389	IP地址：0.0.0.0/0

须知

源地址设置为0.0.0.0/0表示允许所有外部IP远程登录云服务器，为了确保安全，建议您遵循最小原则，根据实际情况将源IP设置为特性的IP地址，配置示例请参见表4-8。

表 4-8 通过特定 IP 地址远程登录云服务器

云服务器类型	规则方向	协议端口	源地址
Linux云服务器	入方向规则	自定义TCP: 22	IP地址：192.168.0.0/24
Windows云服务器	入方向规则	自定义TCP: 3389	IP地址：10.10.0.0/24

在本地服务器远程连接云服务器上传或者下载文件

安全组默认拒绝所有来自外部的请求，如果您需要在本地服务器远程连接云服务器上传或者下载文件，那么您需要开通FTP(20、21)端口。

表 4-9 在本地服务器远程连接云服务器上传或者下载文件

规则方向	协议端口	源地址
入方向规则	自定义TCP: 20-21	IP地址：0.0.0.0/0

须知

您需要在弹性云服务器上先安装FTP服务器程序，再查看20、21端口是否正常工作。

在云服务器上搭建网站对外提供 Web 服务

安全组默认拒绝所有来自外部的请求，如果您在云服器上搭建了可供外部访问的网站，则您需要在安全组入方向添加对应的规则，放通对应的端口，例如HTTP(80)、HTTPS(443)。

表 4-10 云服务器上搭建网站对外提供 Web 服务

规则方向	协议端口	源地址
入方向规则	自定义TCP: 80	IP地址：0.0.0.0/0
入方向规则	自定义TCP: 443	IP地址：0.0.0.0/0

使用 ping 命令验证网络连通性

安全组默认拒绝所有来自外部的请求，如果您需要在云服器上使用**ping**命令验证网络的连通性，则您需要在安全组入方向添加对应的规则，放通ICMP端口。

表 4-11 使用 ping 命令验证网络连通性

规则方向	协议端口	源地址
入方向规则	ICMP: 全部	IP地址：0.0.0.0/0

不同安全组内实例内网网络互通

同一个VPC内，位于不同安全组内的实例网络不通。如果您需要在同一个VPC内的实例之间共享数据，比如安全组sg-A内的云服务器访问安全组sg-B内的MySQL数据库，您需要通过在安全组sg-B中添加一条入方向规则，放通MySQL (3306)端口，允许来自安全组sg-A内云服务器的请求进入。

表 4-12 不同安全组内实例内网互通

规则方向	协议端口	源地址
入方向规则	自定义TCP: 3306	安全组：sg-A

云服务器提供数据库访问服务

安全组默认拒绝所有来自外部的请求，如果您在云服器上部署了数据库服务，允许其他云服务器通过内网访问数据库服务，则您需要在部署数据库云服务器所在的安全组内，添加入方向规则，放通对应的端口，例如MySQL(3306)、Oracle(1521)、MS SQL(1433)、PostgreSQL(5432)、Redis(6379)。

表 4-13 云服务器提供数据库访问服务

规则方向	协议端口	源地址	描述
入方向规则	自定义TCP: 3306	安全组：sg-A	允许安全组sg-A内云服务器访问MySQL数据库服务。
入方向规则	自定义TCP: 1521	安全组：sg-B	允许安全组sg-B内云服务器访问Oracle数据库服务。
入方向规则	自定义TCP: 1433	IP地址：172.16.3.21/32	允许私网IP地址为172.16.3.21的云服务器访问MS SQL数据库服务。
入方向规则	自定义TCP: 5432	IP地址：192.168.0.0/24	允许私网IP地址属于192.168.0.0/24网段的云服务器访问PostgreSQL数据库服务。

须知

本示例中源地址提供的配置仅供参考，请您根据实际需求设置源地址。

限制云服务器访问外部网站

安全组的出方向规则一般默认全部放通，默认规则如表4-15所示。如果您需要限制服务器只能访问特定网站，则按照如下要求配置：

1. 首先，您需要遵循白名单规则，在安全组出方向规则中添加指定的端口和IP地址。

   表 4-14 不同安全组内实例内网互通

规则方向	协议端口	源地址
出方向规则	自定义TCP: 80	IP地址：132.15.XX.XX
出方向规则	自定义TCP: 443	IP地址：145.117.XX.XX

2. 其次，删除安全组出方向中原有放通全部流量的规则，如表4-15所示。

表 4-15 安全组默认出方向规则

规则方向	协议端口	目的地址	描述
出方向规则	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部IP的所有端口。

4.2.4 管理安全组

4.2.4.1 创建安全组

操作场景

安全组实际是网络流量访问策略，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

约束与限制

如果您未创建任何安全组，那么在首次创建需要使用安全组的实例时（比如弹性云服务器），系统会自动为您创建一个默认安全组并关联至该实例。

默认安全组名称为default，详细说明请参见默认安全组。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表右上方，单击“创建安全组”。
   进入“创建安全组”页面。
5. 根据界面提示，设置安全组参数。

表 4-16 参数说明

参数	参数说明	取值样例
名称	必选参数。 安全组的名称。 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。 **说明** 安全组名称创建后可以修改，建议不要重名。	sg-AB
描述	可选参数。 安全组的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

4.2.4.2 克隆安全组

操作场景

VPC支持跨区域克隆安全组，方便您将相同的安全组规则快速应用到不同区域的弹性云服务器上。

当您遇到如下场景时，推荐您使用克隆安全组功能。

- 假设您已经在区域A创建了一个安全组sg-A，此时您需要为区域B内的弹性云服务器使用与sg-A完全相同的规则，您可以直接将sg-A克隆到区域B，而不需要在区域B重新创建安全组。
- 如果您的业务需要执行新的安全组规则，您可以克隆原有的安全组作为备份。
- 如果您需要修改当前业务使用的安全组规则，建议您可以克隆一个测试安全组，在测试环境调测成功后，再修改运行的业务安全组。

约束与限制

- 您可以在同一个区域内，或者跨区域克隆安全组。
  - 同一个区域内克隆安全组时，可以克隆安全组内的全部规则。
  - 跨区域克隆安全组时，仅支持克隆源/目的地址是IP地址或者本安全组的规则，不支持克隆源/目的地址是其他安全组的规则。
- 克隆安全组功能是克隆安全组及安全组规则，不支持克隆此安全组关联的实例。

操作步骤

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

3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表页面 ，单击目标安全组所在行的操作列下的“更多 > 克隆”。
5. 根据界面提示，选择新克隆安全组所在的区域，名称等参数 。
6. 参数设置完成后，单击“确定”，完成安全组克隆。
   您可以在对应区域的安全组列表中，查看克隆成功的安全组。

4.2.4.3 修改安全组基本信息

操作场景

安全组创建完成后，您可以参考以下操作修改安全组的名称和描述。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表页面 ，单击目标安全组所在行的操作列下的“更多 > 修改”。
   弹出“修改安全组”对话框。
5. 根据界面提示，修改安全组的名称和描述信息。
6. 参数修改完成后，单击“确定”，保存修改。

4.2.4.4 删除安全组

操作场景

当您的安全组不需要使用时，您可以参考以下操作删除不需要的安全组。

约束与限制

- 系统创建的默认安全组不支持删除，默认安全组名称为default。
- 当安全组已关联至其他服务实例时，比如云服务器、云容器、云数据库等，此安全组无法删除。请您将实例从安全组中移出后，重新尝试删除安全组，具体操作请参见**在安全组中添加或移出实例**。
- 当安全组作为“源地址”或者“目的地址”，被添加在其他安全组的规则中时，此安全组无法删除。
  需要**删除该条规则**或者**修改规则**，然后重新尝试删除安全组。
  比如，安全组sg-B中有一条安全组规则的“源地址”设置为安全组sg-A，则需要删除或者更改sg-B中的该条规则，才可以删除sg-A。

操作步骤

1. 登录管理控制台。

2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，选择目标安全组所在行的操作列下的“更多 > 删除”。
   弹出删除确认对话框。
5. 确认无误后，单击“是”，删除安全组。

4.2.5 管理安全组规则

4.2.5.1 添加安全组规则

操作场景

安全组实际是网络流量访问策略，通过访问策略可以控制流量入方向规则和出方向规则，通过这些规则可以为加入安全组内的云服务器、云容器、云数据库等实例提供安全保护。安全组的访问策略由入方向规则和出方向规则共同组成。

安全组规则遵循白名单规则，具体说明如下：

- 入方向规则：入方向指外部访问安全组内实例的指定端口。
  当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。
  因此，默认情况下，您一般不用在入方向配置策略为“拒绝”的规则，因为不匹配“允许”规则的请求均会被拦截。
- 出方向规则：出方向指安全组内实例访问外部的指定端口。
  在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。
  0.0.0.0/0表示匹配所有IPv4地址。

如果实例关联的安全组策略无法满足使用需求，比如需要开放某个TCP端口，您可以参考以下操作，通过在入方向规则添加端口，从而打开指定的TCP端口。

安全组规则配置示例

- 配置安全组规则前，您需要规划好安全组内实例的访问策略，常见安全组规则配置案例，请您参考**安全组配置示例**。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。
   进入安全组规则配置页面。

5. 在“入方向规则”页签，单击“添加规则”。
   弹出“添加入方向规则”对话框。
6. 根据界面提示，设置入方向规则参数。
   单击“+”按钮，可以依次增加多条入方向规则。

表 4-17 入方向规则参数说明

参数	说明	取值样例
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	22或22-30
源地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段） 若源地址为安全组，则选定安全组内的云服务器都遵从当前所创建的规则。	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 入方向规则设置完成后，单击“确定”。
   返回入方向规则列表，可以查看添加的入方向规则。
8. 在“出方向规则”页签，单击“添加规则”。
   弹出“添加出方向规则”页签。
9. 根据界面提示，设置出方向规则参数。
   单击“+”按钮，可以依次增加多条出方向规则。

表 4-18 出方向规则参数说明

参数	说明	取值样例
类型	目的地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在出方向规则中，表示安全组内实例访问外部的指定端口。	22或22-30
目的地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

10. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

验证安全组规则是否生效

安全组规则配置完成后，您需要添加的规则是否生效。假设您在弹性云服务器上部署了网站，希望用户能通过HTTP(80)访问到您的网站，则您需要在安全组入方向添加对应的规则，放通对应的端口，如表4-19所示。

表 4-19 安全组规则示例

方向	协议端口	源地址
入方向	自定义TCP: 80	0.0.0.0/0

Linux弹性云服务器

执行以下步骤，在Linux弹性云服务器上验证该安全组规则是否生效。

1. 登录弹性云服务器。
2. 执行以下命令，查看TCP 80端口是否被监听。
   netstat -an | grep 80
   若回显类似图4-3，说明TCP 80端口已开通。

   图 4-3 Linux TCP 80 端口验证结果

   ```
   tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
   ```

3. 打开浏览器，在地址栏里输入“http://弹性云服务器的弹性IP地址”。
   如果访问成功，说明安全组规则已经生效。

Windows弹性云服务器

Windows弹性云服务器上验证该安全组规则是否生效的步骤如下所示。

1. 登录弹性云服务器。
2. 通过“开始菜单 > 运行 > cmd”，打开命令执行窗口。
3. 执行以下命令，查看TCP 80端口是否被监听。
   netstat -an | findstr 80
   若回显类似图4-4，说明TCP 80端口已开通。

   图 4-4 Windows TCP 80 端口验证结果

   ```
   TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
   ```

4. 打开浏览器，在地址栏里输入“http://弹性云服务器的弹性IP地址”。
   如果访问成功，说明安全组规则已经生效。

4.2.5.2 快速添加多条安全组规则

操作场景

通过安全组快速添加功能，您可以快速添加部分常用端口协议对应的规则，包括远程登录和ping测试、常用Web服务和数据库服务所需的端口协议。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组所在行的操作列下的“配置规则”。
   进入安全组规则配置页面。
5. 在“入方向规则”页签，单击“快速添加规则”。
   弹出“快速添加入方向规则”对话框。
6. 根据界面提示，设置入方向规则参数。

表 4-20 入方向规则参数说明

参数	说明	取值样例
常见协议端口	提供常用的协议端口供您快速设置，选择类型如下： ● 远程登录和ping ● Web服务 ● 数据库	SSH (22)
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
源地址	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： ● 单个IP地址：192.168.10.10/32（IPv4地址）；2002:50::44/127（IPv6地址） ● IP地址段：192.168.1.0/24（IPv4地址段）；2407:c080:802:469::/64（IPv6地址段） ● 所有IP地址：0.0.0.0/0（IPv4任意地址）；::/0（IPv6任意地址） ● 安全组：sg-abc 若源地址为安全组，则选定安全组内的云服务器都遵从当前所创建的规则。	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

7. 入方向规则设置完成后，单击“确定”。
   返回入方向规则列表，可以查看添加的入方向规则。
8. 在“出方向规则”页签，单击“快速添加规则”。
   弹出“快速添加出方向规则”页签。
9. 根据界面提示，设置出方向规则参数。

表 4-21 出方向规则参数说明

参数	说明	取值样例
常见协议端口	提供常用的协议端口供您快速设置，选择类型如下： ● 远程登录和ping ● Web服务 ● 数据库	SSH (22)
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4

参数	说明	取值样例
目的地址	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： ● 单个IP地址：192.168.10.10/32（IPv4地址）；2002:50::44/127（IPv6地址） ● IP地址段：192.168.1.0/24（IPv4地址段）；2407:c080:802:469::/64（IPv6地址段） ● 所有IP地址：0.0.0.0/0（IPv4任意地址）；::/0（IPv6任意地址） ● 安全组：sg-abc	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

10. 出方向规则设置完成后，单击“确定”。
    返回出方向规则列表，可以查看添加的出方向规则。

4.2.5.3 修改安全组规则

操作场景

安全组规则设置不满足需求时，您可以通过修改安全组中不合理的安全组规则，保证云服务器等实例的网络安全。您可以修改安全组规则的端口号、协议、IP地址等。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
5. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
6. 在安全组规则列表中，单击目标规则所在行的操作列下的“修改”。
7. 根据界面提示，修改安全组规则信息，并单击“确认”，保存修改。

4.2.5.4 复制安全组规则

操作场景

您可以复制已有的安全组规则，然后基于已有的参数进行修改，快速生成一条新的规则。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
4. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
5. 在安全组规则列表中，单击目标规则所在行的操作列下的“复制”。
   弹出复制安全组规则对话框。
6. 根据界面提示，修改安全组规则信息，并单击“确定”，保存修改。

4.2.5.5 导入/导出安全组规则

操作场景

您可以在Excel格式文件中填写安全组规则参数，并将规则导入到安全组内。同时，您可以将已有安全组的规则导出至Excel格式文件中。遇到以下场景，推荐您使用该功能：

- 如果您想快速创建或恢复安全组规则，可以将导出的安全组规则文件导入到安全组中。
- 如果您想在本地备份安全组规则，可以导出安全组内的规则，会将安全组的出方向、入方向规则信息导出为Excel格式的文件。
- 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。

约束与限制

- 导入安全组规则时，请根据格式要求填写要求的参数，不能新增参数或者修改已有参数名称，否则会导入失败。
- 当导入的安全组规则与已有安全组规则重复时，则无法导入，请删除重复规则后重试。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表页面，单击目标安全组名称。
   进入安全组详情页面。
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。

  导入模板中所涉及参数如表4-22所示。

表 4-22 导入模板参数说明

参数	说明	取值样例
方向	安全组规则的方向： ● 入方向：入方向指外部访问安全组内的实例。 ● 出方向：出方向指安全组内的实例访问外部。	入方向
协议端口	安全组规则中用来匹配流量的网络协议类型。 目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。 在出方向规则中，表示安全组内实例访问外部的指定端口。	22或22-30
类型	源地址支持的IP地址类型，如下： ● IPv4 ● IPv6	IPv4
源地址	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	sg-test[96a8a93f-XXX-d7872990c314]
目的地址	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。	sg-test[96a8a93f-XXX-d7872990c314]
描述	安全组规则的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

参数	说明	取值样例
修改时间	安全组的修改时间。	-

4.2.5.6 删除安全组规则

操作场景

当您的安全组规则不需要使用时，您可以参考以下操作删除安全组规则。

约束与限制

安全组规则是白名单规则，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。安全组的规则说明如下：

- 入方向规则：当外部请求匹配上安全组中入方向规则的源地址，并且策略为“允许”时，允许该请求进入，其他请求一律拦截。
- 出方向规则：在出方向中配置目的地址匹配所有IP地址的规则，并且策略为“允许”时，允许所有的内部请求出去。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组的名称超链接。
   进入安全组详情页面。
5. 根据情况，选择“入方向规则”或者“出方向规则”页签。
   进入安全组规则列表页面。
6. 在安全组规则列表中，执行以下操作，删除安全组规则。
   - 删除单个安全组规则：单击目标安全组规则所在行的操作列下的“删除”。
   - 删除多个安全组规则：勾选多个安全组规则，并单击安全组规则左上方的“删除”。
7. 在删除对话框中，确认无误后，单击“确定”，删除安全组规则。

4.2.6 管理安全组关联的实例

4.2.6.1 在安全组中添加或移出实例

操作场景

创建实例的时候，会自动将实例加入一个安全组内，实例将会受到安全组的保护。

- 如果一个安全组无法满足您的要求，您可以将实例加入多个安全组。
- 实例必须加入一个安全组，如果您需要更换安全组，可以先将实例加入新的安全组，然后再将实例从原有安全组移出。

在安全组中添加实例

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入实例列表页面。
5. 根据界面提示，选择对应的实例类型。
   以下操作，以实例类型选择“服务器”为例。
6. 选择“服务器”页签，单击“添加”。
   弹出“添加服务器”对话框。
7. 在服务器列表中，选择一个或者多个服务器，并单击“确定”，将服务器加入到当前安全组中。

在安全组中移出实例

实例至少需要加入一个安全组，如果您要将实例移出安全组，请确保当前实例至少关联两个安全组。

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“访问控制 > 安全组”。
   进入安全组列表页面。
4. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入实例列表页面。
5. 根据界面提示，选择对应的实例类型。
   以下操作，以实例类型选择“服务器”为例。
6. 选择“服务器”页签，在服务器列表中，选择一个或者多个服务器，并单击列表左上方的“移出”。
   弹出移出确认对话框。
7. 确认无误后，单击“是”，将所选实例从安全组中移出。

4.2.6.2 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. 在页面左上角单击图标，打开服务列表，选择“计算 > 弹性云服务器”。
   进入弹性云服务器列表页面。
3. 在弹性云服务器列表中，单击弹性云服务器名称。
   进入弹性云服务器详情页面。
4. 选择“安全组”页签，查看弹性云服务器所属的安全组详情。
   您可以查看弹性云服务器关联的安全组，以及入方向、出方向规则等信息。

4.2.6.3 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。

   图 4-5 更改安全组

4. 根据界面提示，在下拉列表中选择待更改安全组的网卡，并重新选择安全组。
   您可以同时勾选多个安全组，弹性云服务器的访问规则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”。

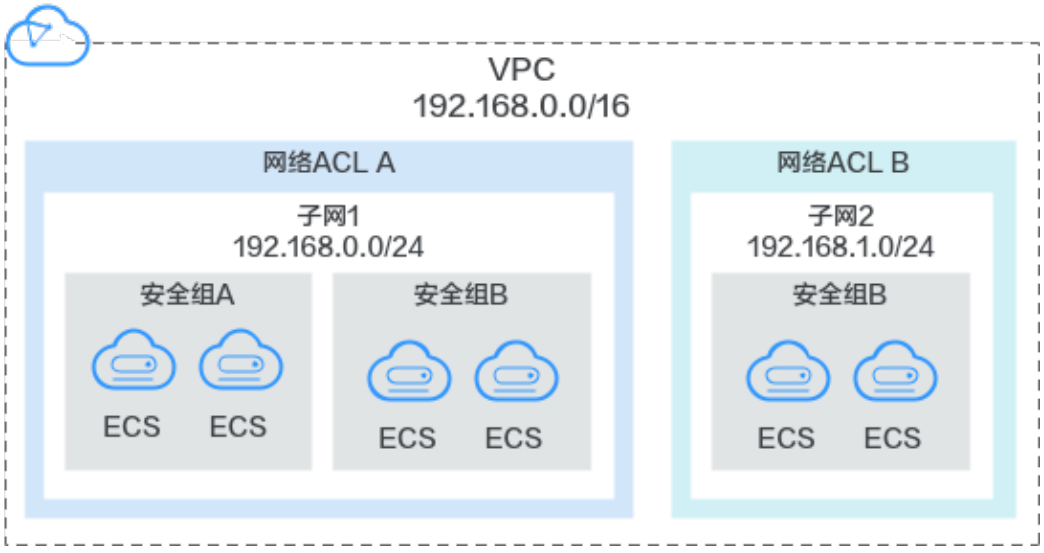
4.3 网络 ACL

4.3.1 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网络流量。

如图4-6所示。

图 4-6 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可以同时关联多个子网，但一个子网只能关联一个网络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使用连接跟踪来标识进出实例的流量信息，入方向和出方向网络ACL规则配置变更，对原有流量不会立即生效。

  当您在网络ACL内增加、删除、更新规则，或者在网络ACL内添加、移出子网时，由入方向/出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有网络

ACL规则。入方向/出方向流量新建立的连接，将会匹配新的网络ACL出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

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4-23所示。该规则不能修改和删除。

表 4-23 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

流量匹配网络 ACL 规则的顺序

- 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。

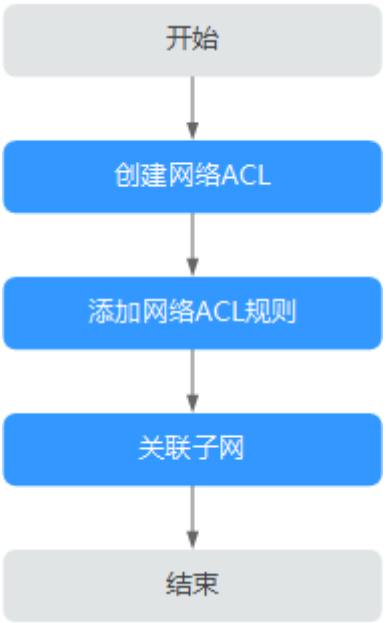
  解决方案：通过网络ACL设置南北向规则。
- 对访问频繁的应用，调整安全规则顺序，提高性能。

  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4-7所示。

图 4-7 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**将子网关联至网络ACL**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。

约束与限制

- 默认情况下，一个区域内，一个用户最多可以创建200个网络ACL。
- 建议一个网络ACL单方向拥有的规则数量不要超过20条，否则会引起网络ACL性能下降。

4.3.2 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4-24所示。

表 4-24 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4-25所示。

表 4-25 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4-26所示。

表 4-26 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。

4.3.3 管理网络 ACL

4.3.3.1 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。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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。

   表 4-27 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。 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。 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。

4.3.3.2 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. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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。

4.3.3.3 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“访问控制 > 网络ACL”。
4. 在“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。

4.3.3.4 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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。

4.3.3.5 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。

进入虚拟私有云列表页面。

3. 在左侧导航栏选择“访问控制 > 网络ACL”。
4. 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。

4.3.4 管理网络 ACL 规则

4.3.4.1 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。

约束与限制

建议一个网络ACL单方向拥有的规则数量不要超过20条，否则会引起网络ACL性能下降。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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 4-28 参数说明

参数	参数说明	取值样例
类型	开通IPv6功能后可见。 网络ACL类型。必选项，单击下拉按钮可选择。目前支持“IPv4”和“IPv6”。	IPv4
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

参数	参数说明	取值样例
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。	TCP
源地址	此方向允许的源地址，可以是IP地址、IP地址段。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	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。	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。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	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。 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。 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。

4.3.4.2 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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4-29。

表 4-29 参数说明

参数	参数说明	取值样例
类型	开通IPv6功能后可见。 网络ACL类型。必选项，单击下拉按钮可选择。目前支持“IPv4”和“IPv6”。	IPv4
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。	TCP
源地址	此方向允许的源地址，可以是IP地址、IP地址段。 • IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	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。	22或22-30

参数	参数说明	取值样例
目的地址	此方向允许的目的地址，可以是IP地址、IP地址段。 ● IP地址： – 单个IP地址：比如192.168.10.10/32（IPv4地址）、2002:50::44/128（IPv6地址） – 默认IP地址：默认IP地址可以匹配任意IP地址，比如0.0.0.0/0（IPv4地址）、::/0（IPv6地址） – IP网段：比如192.168.1.0/24（IPv4地址段）、2407:c080:802:469::/64（IPv6地址段）	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。 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。 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。

4.3.4.3 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. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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。

4.3.4.4 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. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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“更多 > 开启”或者“更多 > 关闭”。
6. 单击“是”，确认开启或关闭此规则。

4.3.4.5 导出/导入网络 ACL 规则

操作场景

您可以将已有的某一个网络ACL出方向、入方向规则导出为Excel文件，然后在另一个网络ACL直接导入。支持跨区域导入和导出。

约束与限制

- 导入/导出网络ACL规则时，建议您每次处理少于40条的规则，否则可能会影响性能。
- 导入规则是基于已有规则的增量导入，不会删除已有规则。
- 相同规则不允许重复导入。

导出网络 ACL 规则

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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，单击您需要导出的“网络ACL名称”进入网络ACL详情页面。
5. 单击  ，导出出方向和入方向的网络ACL规则，并自动保存为Excel文件，请下载到本地。

导入网络 ACL 规则

1. 登录管理控制台。

2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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，单击您需要导入的“网络ACL名称”进入网络ACL详情页面。
5. 单击  。
6. 选择本地已导出的网络ACL规则Excel文件，单击“上传”，导入规则。

4.3.4.6 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. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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”。

4.3.5 管理网络 ACL 关联的子网

4.3.5.1 将子网关联至网络 ACL

操作场景

您可以将网络ACL关联至VPC子网，为子网内的资源提供安全防护。

约束与限制

- 网络ACL可以同时关联多个子网，但一个子网只能关联一个网络ACL。
- 关联网络ACL后，系统自带的默认网络ACL规则将会拒绝所有出入子网的流量，需要您添加自定义规则放通流量，具体请参见**添加网络ACL规则**。

操作步骤

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

3. 在左侧导航栏选择“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。

4.3.5.2 将子网和网络 ACL 解除关联

操作场景

您可根据自身网络需求，将子网和网络ACL解除关联。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏选择“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”。

5 弹性 IP

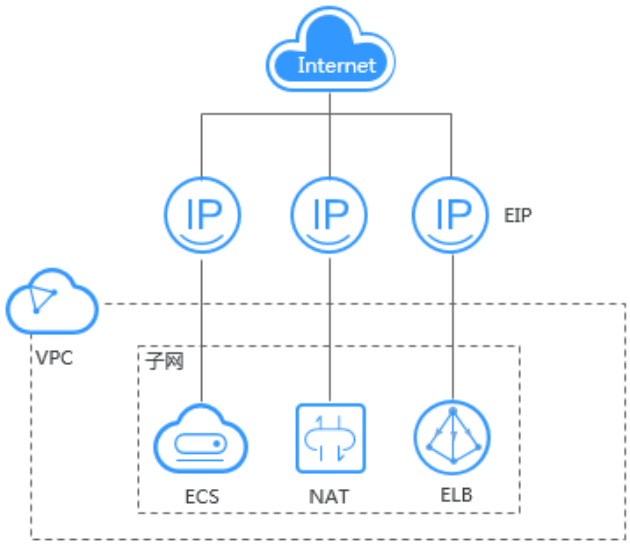
5.1 弹性 IP 简介

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。拥有多种灵活的计费方式，可以满足各种业务场景的需要。

一个弹性IP只能绑定一个云资源，且弹性IP和云资源必须位于同一个区域。

图 5-1 通过 EIP 访问公网



弹性 IP 配额说明

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

优势

- 弹性灵活
  EIP支持与ECS、BMS、NAT网关、ELB、虚拟IP灵活的绑定与解绑，带宽支持灵活调整，应对各种业务变化。
- 共享带宽
  EIP可以加入共享带宽，降低带宽使用成本。
- 即开即用
  即开即用，绑定解绑、带宽调整实时生效。

5.2 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. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“弹性IP”界面，单击“创建弹性IP”。
4. 根据界面提示配置参数。

表 5-1 参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。创建EIP时所选择的区域即为EIP的归属地。	-
线路	全动态BGP：可以根据设定的寻路协议实时自动优化网络结构，以保持客户使用的网络持续稳定、高效。	全动态BGP

参数	说明	取值样例
公网带宽	带宽类型分为以下几种： ● 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。适用于流量较大或较稳定场景使用。 ● 按流量计费：指定带宽上限，按实际使用的出公网流量计费，与使用时间无关。适用于流量小或流量波动较大的场景。 ● 加入共享带宽：共享带宽可以针对多个弹性IP进行集中限速，可以加入多个弹性IP，被多个弹性IP地址共用。适用于多业务流量错峰分布场景。	按带宽计费
带宽大小	带宽大小，单位Mbit/s。	100
弹性IP名称	弹性IP的名称。	eip-test
带宽名称	带宽的名称。	bandwidth
标签	用于标识弹性IP地址。包括键和值。 标签的命名规则请参考表5-2。	● 键：lpv4_key1 ● 值：3005eip
创建数量	弹性IP数量。	1

表 5-2 弹性 IP 地址标签命名规则

参数	规则	样例
键	● 不能为空。 ● 对于同一弹性IP地址键值唯一。 ● 长度不超过36个字符。 ● 由英文字母、数字、下划线、中划线、中文字符组成。	lpv4_key1
值	● 长度不超过43个字符。 ● 由英文字母、数字、下划线、点、中划线、中文字符组成。	3005eip

5. 单击“立即申请”。

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”。

5.3 解绑定和释放弹性云服务器的弹性 IP

操作场景

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

约束与限制

- 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，但是经典型负载均衡不支持解绑定操作。
- 未绑定任何实例的弹性IP才可释放，已绑定实例的弹性IP需要先从实例解绑，然后释放。

操作步骤

解绑单个弹性IP

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“弹性IP”界面待解绑定弹性IP地址所在行，单击“解绑”。
4. 单击“是”。

释放单个弹性IP

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“弹性IP”界面待释放弹性IP地址所在行，单击“更多 > 释放”。
4. 单击“是”。

批量解绑弹性IP

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”
3. 在弹性IP列表中勾选待解绑定的多个弹性IP地址。
4. 单击列表左上方的“解绑”。
5. 单击“是”。

批量释放弹性IP

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“弹性IP”列表中勾选多个待释放弹性IP。
4. 单击列表上方的“释放”。
5. 单击“是”。

5.4 修改弹性 IP 的带宽配置

操作场景

修改弹性IP带宽名称、大小、计费方式（按带宽计费、按流量计费）。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性IP”
3. 在“操作”列，选择“更多 > 修改带宽”。
4. 根据界面提示修改带宽参数。
   您可以修改以下参数：
   - 带宽名称
   - 计费方式：支持按带宽计费和按流量计费两种计费方式之间相互转换。
   - 带宽大小
5. 单击“下一步”。
6. 单击“提交”，完成修改。

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

5.5 导出弹性 IP 列表

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性IP”
3. 在弹性IP列表页，单击右上角的。
   系统会将您账号下，当前区域的所有弹性IP信息自动导出为Excel文件，并下载至本地。

5.6 管理弹性 IP 地址标签

操作场景

为弹性IP地址添加标签，可以方便用户识别和管理拥有的弹性IP地址。您可以在申请弹性IP地址时增加标签，或者在已经创建的弹性IP地址详情页添加标签，最多可以给弹性IP地址添加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5-3所示。

表 5-3 弹性 IP 地址标签命名规则

参数	规则	样例
键	• 不能为空。 • 对于同一弹性IP地址键值唯一。 • 长度不超过36个字符。 • 由英文字母、数字、下划线、中划线、中文字符组成。	Ipv4_key1
值	• 长度不超过43个字符。 • 由英文字母、数字、下划线、点、中划线、中文字符组成。	3005eip

操作步骤

在弹性IP列表页，按标签的键或值搜索目标弹性IP地址。

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在弹性IP列表上方的搜索框中，单击框中任意位置，设置搜索条件。

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

在弹性IP地址的标签页，执行标签的增、删、改、查操作。

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在弹性IP地址列表中，单击待管理标签的弹性IP地址名称。
4. 在弹性IP地址详情页面，选择“标签”页签，对弹性IP地址的标签执行增、删、改、查。
   - 查看

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

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

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

     标签键不支持修改。
   - 删除

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

6 共享带宽

6.1 共享带宽简介

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

说明

- 共享带宽不支持对单个弹性IP进行限速，也不支持自定义限速策略。

客户有大量业务在云上时，如果每个弹性云服务器单独使用一条带宽，则需要维护多个带宽实例。如果所有实例共用一条带宽，就可以实现VPC和区域级别的带宽统一管理，同时方便运维统计和运营成本结算。

- 节省带宽使用成本

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

  提供区域级别的带宽复用共享能力，方便运维统计、管理和运营成本结算。
- 操作灵活

  除独享型ELB专属池（5_gray）类型的EIP以外，不区分其他弹性IP类型及绑定实例类型，随时从共享带宽中增加或移出弹性IP。

6.2 申请共享带宽

操作场景

共享带宽需要申请才能使用。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”

3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。
4. 在页面右上角，单击“申请共享带宽”，按照提示配置参数。

表 6-1 参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	-
计费方式	共享带宽的计费方式。 支持按带宽计费、按流量计费。	按带宽计费
带宽大小	共享带宽的大小，单位Mbit/s，5M起售，最大支持2000Mbit/s。	10
名称	共享带宽的名称。	Bandwidth-001

5. 单击“立即申请”。

6.3 添加弹性 IP 到共享带宽

操作场景

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

约束与限制

- EIP的线路类型与要加入的共享带宽的线路类型一致。
- “普通带宽”线路类型的共享带宽可添加动态BGP类型的EIP以及IPv6网卡，“优选BGP”线路类型的共享带宽可添加优选BGP类型的EIP以及IPv6网卡。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。
4. 在共享带宽列表中找到您想添加弹性IP的共享带宽，在“操作”列选择“ 添加弹性IP”，勾选您想添加的弹性IP。

   说明

   - 弹性IP添加到共享带宽后，原来的独享带宽大小无效，将使用共享带宽进行限速。弹性IP原来的独享带宽将会被删除，不再计费，不会额外计算流量和带宽费用。
5. 单击“确定”。

6.4 从共享带宽中移出弹性 IP

操作场景

您可以根据需要将不需要的弹性IP从共享带宽中移出。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性IP”
3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。
4. 在共享带宽列表中找到您想移出弹性IP的共享带宽，选择“更多 > 移出弹性IP”，勾选您想移出的弹性IP。
5. 单击“确定”。

6.5 修改共享带宽

操作场景

本章节指导用户修改共享带宽的名称、计费方式和带宽大小（按带宽计费、按流量计费）。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 弹性IP”
3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。
4. 在共享带宽列表中找到您想修改的共享带宽，在“操作”列单击“修改带宽”，修改共享带宽的参数。

   您可以修改以下参数：

   - 带宽名称
   - 计费方式：支持按带宽计费和按流量计费两种计费方式之间相互转换。
   - 带宽大小
5. 单击“下一步”。
6. 单击“提交”，完成修改。

6.6 删除共享带宽

操作场景

您可以删除不需要的共享带宽。

前提条件

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在左侧导航栏，选择“弹性IP和带宽 > 共享带宽”。
4. 在共享带宽列表中找到您想删除的共享带宽，在“操作”列选择“更多 > 删除”。
5. 单击“确定”，删除该共享带宽。

7 路由表

7.1 路由表和路由

路由表

路由表由一系列路由规则组成，用于控制VPC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，一个子网只能关联一个路由表，但一个路由表可以同时关联至多个子网。

- 默认路由表：用户创建VPC时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。默认路由表可以确保VPC内子网之间网络互通。
  - 您可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。
  - 创建VPN、VPC终端节点、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。
- 自定义路由表：您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。

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

说明

路由

您可以在默认路由表和自定义路由表中添加路由，路由包括目的地址、下一跳类型、下一跳地址等信息，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。自定义路由的目的地址不能与系统路由的目的地址重叠。

  您可以通过添加自定义路由来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7-1**所示。

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

表 7-1 下一跳类型

下一跳类型	说明	支持添加该类型路由的路由表
服务器实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。	• 默认路由表 • 自定义路由表
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。	• 默认路由表 • 自定义路由表
VPN网关	将指向目的地址的流量转发到一个VPN网关。	自定义路由表
云专线网关	将指向目的地址的流量转发到一个云专线网关。	自定义路由表
NAT网关	将指向目的地址的流量转发到一个NAT网关。	• 默认路由表 • 自定义路由表
对等连接	将指向目的地址的流量转发到一个对等连接。	• 默认路由表 • 自定义路由表
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。	• 默认路由表 • 自定义路由表

说明

目前暂不支持配置云专线服务类型的路由策略，如需使用请提交工单申请。

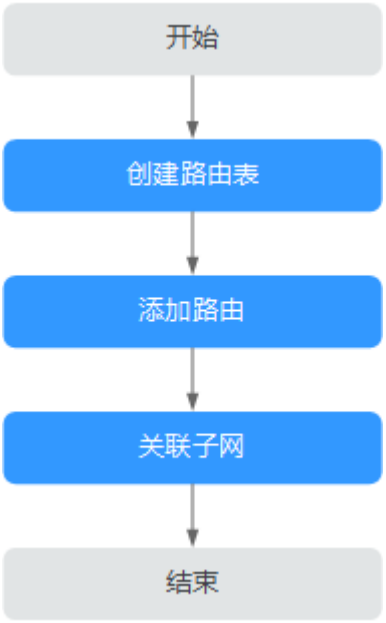
个别由系统下发的路由可供用户修改和删除，这取决于创建对端服务时是否已设置目的地址。

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

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7-1所示。

图 7-1 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**将路由表关联至子网**关联子网，关联成功后，路由规则对该子网生效。

7.2 管理路由表

7.2.1 创建自定义路由表

操作场景

创建虚拟私有云时，会同步为虚拟私有云创建一个默认路由表。当默认路由表无法满足您的使用要求时，您可参考以下操作创建自定义路由表。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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 7-2 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。 路由表的名称只能由英文字母、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。 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。 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。 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。

7.2.2 将路由表关联至子网

操作场景

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

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

须知

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

约束与限制

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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。

图 7-2 关联子网

6. 单击“确定”，完成关联。

7.2.3 更换子网关联的路由表

操作场景

更换子网已经关联的路由表为该VPC下其他的路由表。更换路由表后，子网下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. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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。

7.2.4 查看子网关联的路由表

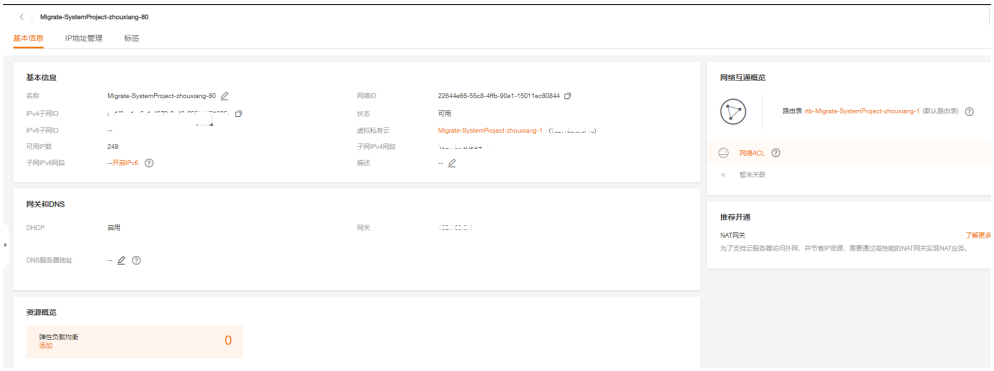
操作场景

本章节指导用户查看子网关联的路由表。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，找到目标子网，并单击子网名称超链接。
   进入子网详情页面。

   图 7-3 查看子网关联的路由表



5. 在子网详情页面右侧区域，查看子网关联的路由表。
6. 单击路由表名称超链接。
   进入路由表详情页面，您可以进一步查看路由信息。

7.2.5 查看路由表信息

操作场景

本章节指导用户查看路由表的的详细信息，主要信息如下：

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

操作步骤

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

进入虚拟私有云列表页面。

3. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
4. 在路由表列表中，单击路由表的名称超链接。

   进入路由表详情页面。

   a. 在“基本信息”页签下，查看路由表的基本信息和路由列表。
   b. 在“关联子网”页签下，查看路由表关联的子网。

7.2.6 导出路由表列表

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
4. 在子网列表中，勾选一个或多个路由表，单击列表左上方的“导出”。

   系统会将您所选的路由表信息自动导出为Excel文件，并下载至本地。

7.2.7 删除路由表

操作场景

本章节指导用户删除自定义路由表。

约束与限制

- 默认路由表无法删除。
- 当自定义路由表被关联至子网时，则无法删除。

  请先通过**更换子网关联的路由表**将子网关联到其他的路由表，然后尝试删除。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 路由表”。
4. 在路由表列表中，单击目标路由表所在行的操作列下的“删除”。

   弹出删除确认对话框。
5. 确认无误后，单击“是”，删除自定义路由表。

7.3 管理路由

7.3.1 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。除了系统默认路由，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. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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 7-3 参数说明

参数	说明	取值样例
目的地址	必选参数。 此处输入路由的目的地址，支持单个IP地址或者IP网段，格式为“IP地址/掩码”。 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。	Pv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。 **说明** 当为默认路由表添加或修改自定义路由时，下一跳类型不支持选择VPN网关与云专线网关。	对等连接
下一跳	必选参数。 选择下一跳资源。下拉列表包含资源将基于您所选的资源类型进行展示。	peer-AB
描述	可选参数。 您可以根据需要在文本框中输入路由的描述信息。	-

6. 单击“确定”，完成添加。

7.3.2 修改路由

操作场景

本章节指导用户修改VPC路由表中已有的路由。

约束与限制

- 系统自动创建的路由不支持修改，即类型为“系统”的路由不支持修改。
- 创建VPN、VPC终端节点、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。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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 7-4 参数说明

参数	说明	取值样例
目的地址	必选参数。 此处输入路由的目的地址，支持单个IP地址或者IP网段，格式为“IP地址/掩码”。 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。	Pv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。 **说明** 当为默认路由表添加或修改自定义路由时，下一跳类型不支持选择VPN网关与云专线网关。	对等连接
下一跳	必选参数。 选择下一跳资源。下拉列表包含资源将基于您所选的资源类型进行展示。	peer-AB
描述	可选参数。 您可以根据需要在文本框中输入路由的描述信息。	-

7. 单击“确定”。

7.3.3 复制路由

操作场景

本章节指导用户在一个VPC内的所有路由表之间互相复制路由信息，VPC路由表包括默认路由表和自定义路由表。

约束与限制

不同类型的路由是否支持复制的情况不同，具体请参见表7-5。

比如路由下一跳类型为服务器实例时，支持复制该路由到默认路由表或自定义路由表。当路由下一跳类型为云专线网关时，无法复制该路由到默认路由表，仅支持复制到自定义路由表。

表 7-5 路由复制情况说明

下一跳类型	是否支持复制到默认路由表	是否支持复制到自定义路由表
Local	否	否
服务器实例	是	是
扩展网卡	是	是
VPN网关	否	是
云专线网关	否	是
NAT网关	是	是
对等连接	是	是
虚拟IP	是	是

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 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”。

7.3.4 删除路由

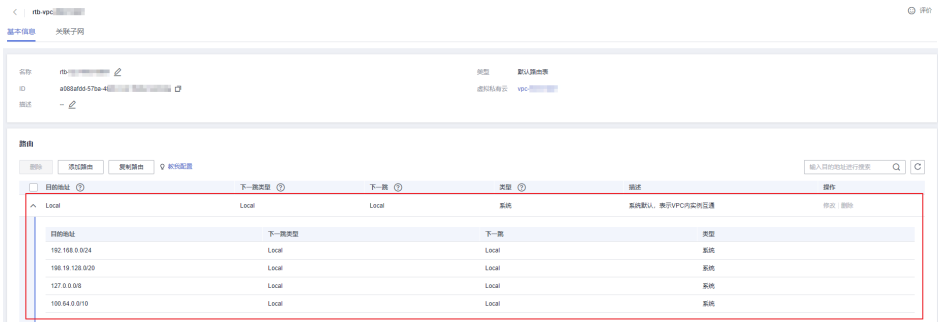
操作场景

本章节指导用户删除VPC路由表中的自定义路由，即类型为“自定义”的路由。

约束与限制

- 系统自动创建的路由不支持删除，即类型为“系统”的路由不支持删除。

  图 7-4 系统路由

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

  以VPN网关路由为例，路由如下图所示，如果您需要删除该路由，请单击下一跳对应的超链接，查看并删除对应资源。

  图 7-5 VPN 下发的路由

操作步骤

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

图 7-6 删除自定义路由

5. 在路由列表中，找到需要删除的路由，单击目标路由所在行的操作列下的“删除”。

   弹出删除确认对话框。

6. 确认无误后，单击“是”，删除自定义路由。

7.4 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. 在页面左上角单击 ☰ 图标，打开服务列表，选择“计算 > 弹性云服务器”。
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服务器上相应的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.google.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。

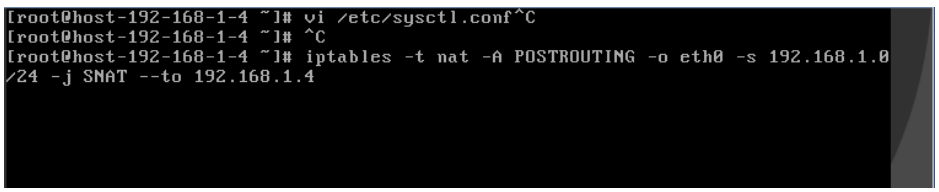
    许多操作系统支持路由报文。操作系统需要在转发报文前将报文的源IP地址转换成操作系统的IP地址，因此，发送的报文带有公共发送者的IP地址，而返回的报文能够原路返回，这种方式称为SNAT。操作系统需要跟踪转换过IP地址的报文，确保返回的报文中目的IP地址可以被重写，且报文能够转发给原始的报文发送者。这一过程实现需要启用IP转发功能，并设置SNAT规则。
11. 使用vi打开“/etc/sysctl.conf”文件，修改net.ipv4.ip_forward = 1，按“**:wq**”保存退出。
12. 执行如下命令，使修改生效。

    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7-7**所示。

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

图 7-7 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。

1. 执行以下命令进入/etc/rc.local文件。

   vi /etc/rc.local

2. 执行13配置SNAT
3. 执行以下命令保存并退出。

   :wq

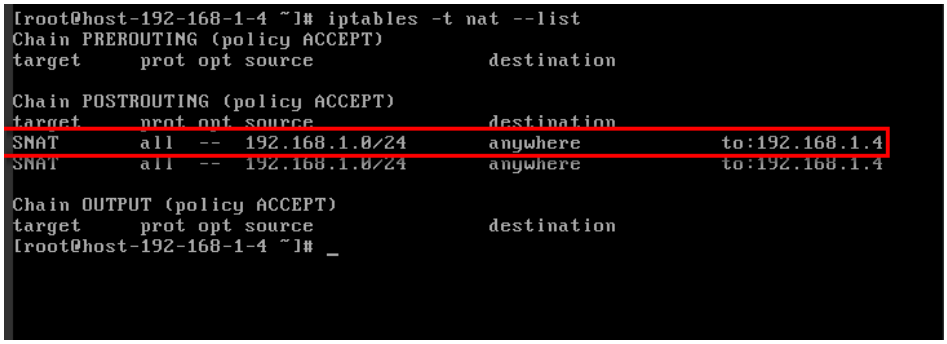
4. 执行以下命令添加rc.local文件的执行权限。

   # chmod +x /etc/rc.local

14. 执行如下命令，查看是否配置成功。如图7-8所示，则表示配置成功（例如：192.168.1.0/24）。

    iptables -t nat --list

    图 7-8 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。

8 对等连接

8.1 对等连接简介

什么是对等连接

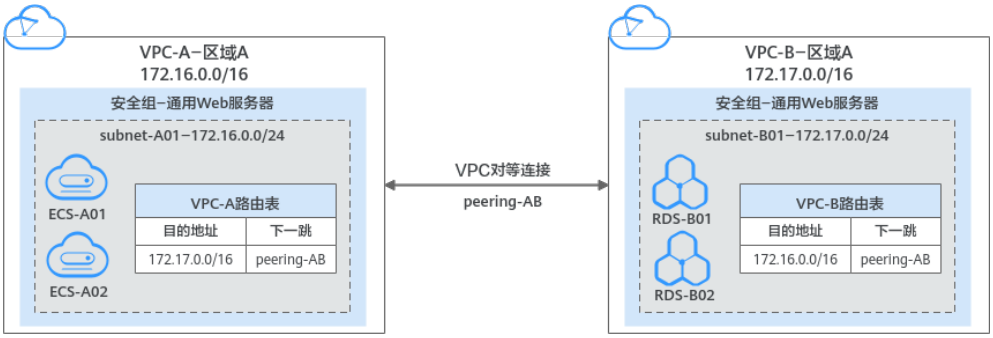
对等连接是建立在两个VPC之间的网络连接，不同VPC之间网络不通，通过对等连接可以实现不同VPC之间的云上内网通信。对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。

- 您可以通过对等连接构建不同的组网，常见的使用示例请参见**对等连接使用示例**。

接下来，通过**图8-1**中简单的组网示例，为您介绍对等连接的使用场景。

- 在区域A内，您的两个VPC分别为VPC-A和VPC-B，VPC-A和VPC-B之间网络不通。
- 您的业务服务器ECS-A01和ECS-A02位于VPC-A内，数据库服务器RDS-B01和RDS-B02位于VPC-B内，此时业务服务器和数据库服务器网络不通。
- 您需要在VPC-A和VPC-B之间建立对等连接Peering-AB，连通VPC-A和VPC-B之间的网络，业务服务器就可以访问数据库服务器。

图 8-1 对等连接组网示意图

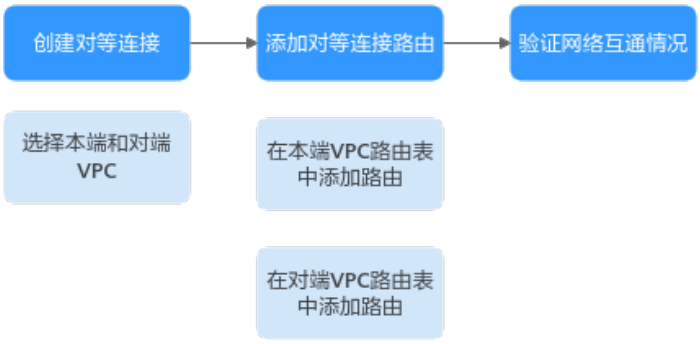


对等连接创建流程

对等连接可以连通相同账户或者不同账户下的VPC，连通的VPC位于同一个区域即可，创建流程如下：

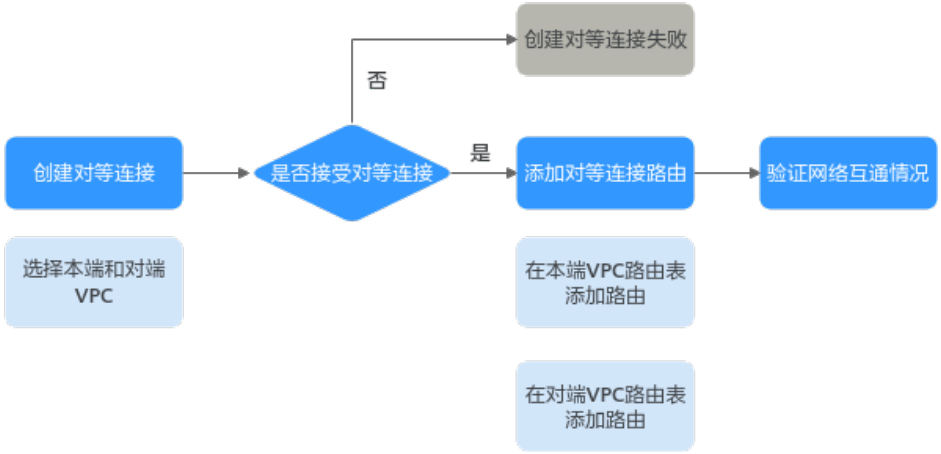
- 相同账户下的VPC对等连接创建流程如图8-2所示。
  创建对等连接的具体操作，请参见**创建相同账户下的对等连接**。

  图 8-2 相同账户下的 VPC 对等连接创建流程

- 不同账户下的VPC对等连接创建流程如图8-3所示。
  创建对等连接的具体操作，请参见**创建不同账户下的对等连接**。
  创建不同账户下的VPC对等连接时，如果在账号A下发起创建对等连接请求，需要账号B接受该请求才可以，如果账号B拒绝，则该对等连接创建失败。

  图 8-3 不同账户下的 VPC 对等连接创建流程

约束与限制

- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。

8.2 对等连接使用示例

对等连接是建立在相同区域内，两个VPC之间的网络连接，可以实现多个VPC之间的互通，本文为您详细介绍对等连接常见使用示例，具体如表8-1所示。

表 8-1 常见对等连接使用示例

VPC位置	VPC网段	对等连接说明	使用示例
同区域VPC	• VPC网段：不同VPC网段不重叠 • 子网网段：不同VPC的子网网段不重叠	您可以创建整个VPC网段之间的对等连接，VPC内的所有资源可以通过该对等连接实现网络通信。	• **通过VPC对等连接实现多个VPC网络互通** • **通过VPC对等连接实现一个中心VPC与多个VPC之间网络互通**
同区域VPC	• VPC网段：不同VPC网段重叠 • 子网网段：不同VPC的部分子网网段重叠	VPC网段重叠时，您无法创建整个VPC网段之间的对等连接，此时建议您根据业务情况，创建如下对等连接： • VPC子网之间的对等连接：指定子网之间网络互通，对等连接两端的子网网段不能重叠。 • VPC内ECS之间的对等连接：指定ECS之间网络互通，对等连接两端的ECS的私有IP地址不能相同。	• **通过VPC对等连接实现两个重叠网段VPC子网网络互通** • **通过VPC对等连接实现一个中心VPC的ECS与两个VPC的ECS对等**
同区域VPC	• VPC网段：不同VPC网段重叠 • 子网网段：不同VPC的全部子网网段重叠	此种场景下，您创建的任何对等连接均是无效的，请重新规划VPC网段。	• **无效的VPC对等连接**

通过 VPC 对等连接实现多个 VPC 网络互通

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

图 8-4 相互对等的两个 VPC(IPv4)

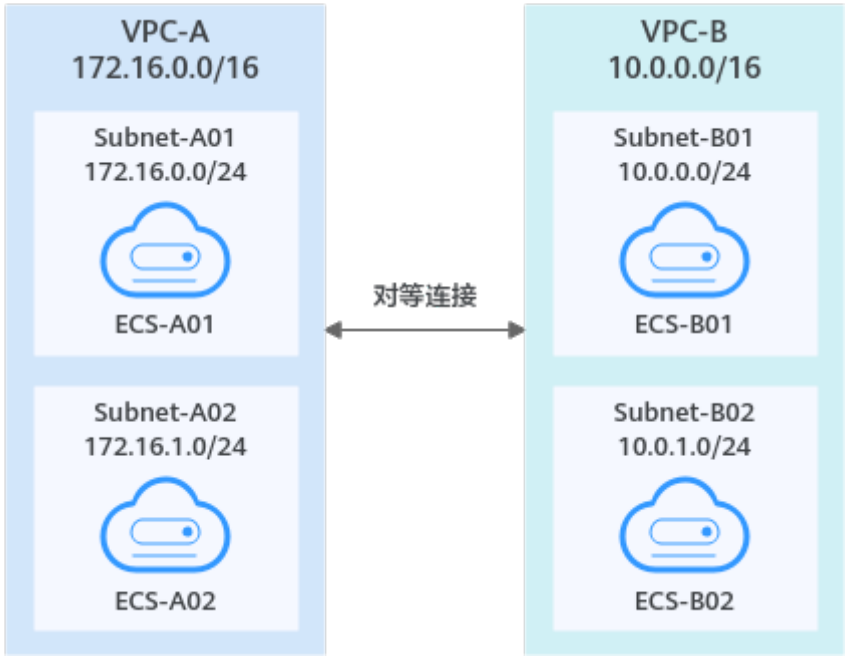


表 8-2 对等连接关系说明-相互对等的两个 VPC(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B

表 8-3 VPC 路由表配置说明-相互对等的两个 VPC(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/16	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	172.16.0.0/16	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。

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

图 8-5 相互对等的多个 VPC(IPv4)

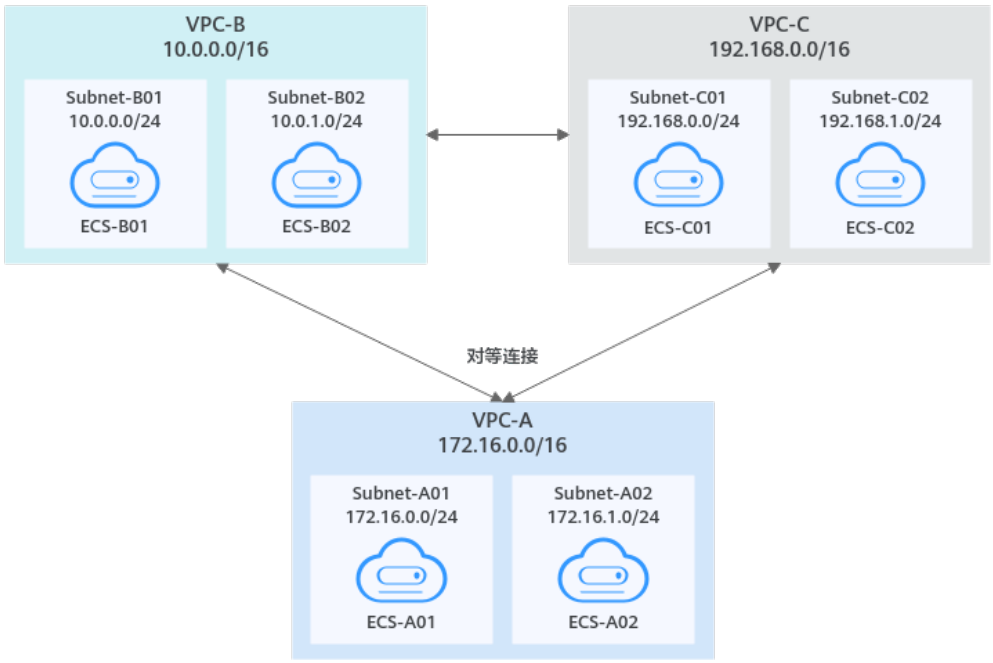


表 8-4 对等连接关系说明-相互对等的多个 VPC(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C
VPC-B和VPC-C对等	Peering-BC	VPC-B	VPC-C

表 8-5 VPC 路由表配置说明-相互对等的多个 VPC(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/16	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
rtb-VPC-B	172.16.0.0/16	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。

路由表	目的地址	下一跳	路由类型	路由说明
	192.168.0.0/16	Peering-BC	自定义	在VPC-B的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-BC的路由。
rtb-VPC-C	172.16.0.0/16	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。
	10.0.0.0/16	Peering-BC	自定义	在VPC-C的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-BC的路由。

通过 VPC 对等连接实现一个中心 VPC 与多个 VPC 之间网络互通

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

图 8-6 一个中心 VPC 与多个 VPC 对等(IPv4)

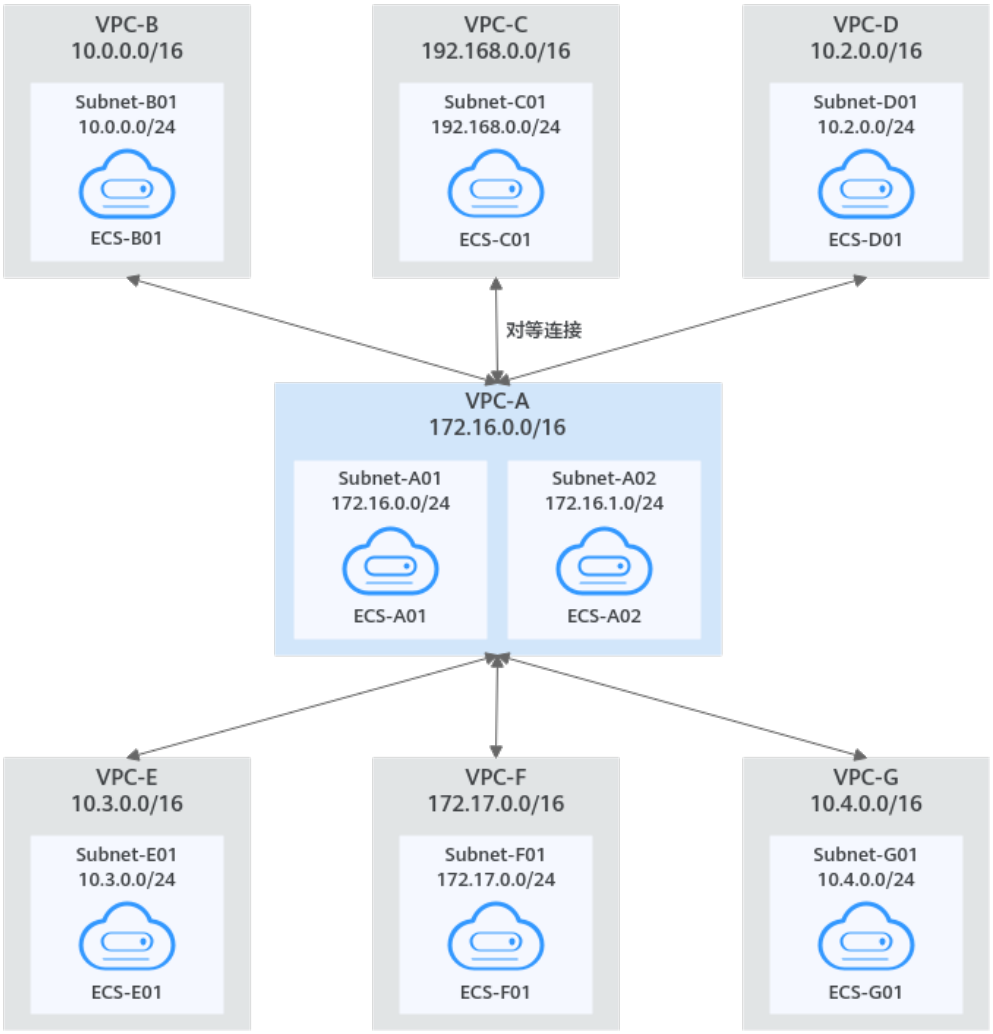


表 8-6 对等连接关系说明-一个中心 VPC 与多个 VPC 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B
VPC-A和VPC-C对等	Peering-AC	VPC-A	VPC-C
VPC-A和VPC-D对等	Peering-AD	VPC-A	VPC-D
VPC-A和VPC-E对等	Peering-AE	VPC-A	VPC-E
VPC-A和VPC-F对等	Peering-AF	VPC-A	VPC-F
VPC-A和VPC-G对等	Peering-AG	VPC-A	VPC-G

表 8-7 VPC 路由表配置说明-一个中心 VPC 与多个 VPC 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/16	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B网段，下一跳指向Peering-AB的路由。
	192.168.0.0/16	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为VPC-C网段，下一跳指向Peering-AC的路由。
	10.2.0.0/16	Peering-AD	自定义	在VPC-A的路由表中，添加目的地址为VPC-D网段，下一跳指向Peering-AD的路由。
	10.3.0.0/16	Peering-AE	自定义	在VPC-A的路由表中，添加目的地址为VPC-E网段，下一跳指向Peering-AE的路由。
	172.17.0.0/16	Peering-AF	自定义	在VPC-A的路由表中，添加目的地址为VPC-F网段，下一跳指向Peering-AF的路由。
	10.4.0.0/16	Peering-AG	自定义	在VPC-A的路由表中，添加目的地址为VPC-G网段，下一跳指向Peering-AG的路由。
rtb-VPC-B	172.16.0.0/16	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AB的路由。

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-C	172.16.0.0/16	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AC的路由。
rtb-VPC-D	172.16.0.0/16	Peering-AD	自定义	在VPC-D的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AD的路由。
rtb-VPC-E	172.16.0.0/16	Peering-AE	自定义	在VPC-E的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AE的路由。
rtb-VPC-F	172.16.0.0/16	Peering-AF	自定义	在VPC-F的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AF的路由。
rtb-VPC-G	172.16.0.0/16	Peering-AG	自定义	在VPC-G的路由表中，添加目的地址为VPC-A网段，下一跳指向Peering-AG的路由。

通过 VPC 对等连接实现两个重叠网段 VPC 子网网络互通

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

图 8-7 相互对等的两个重叠网段 VPC 子网(IPv4)

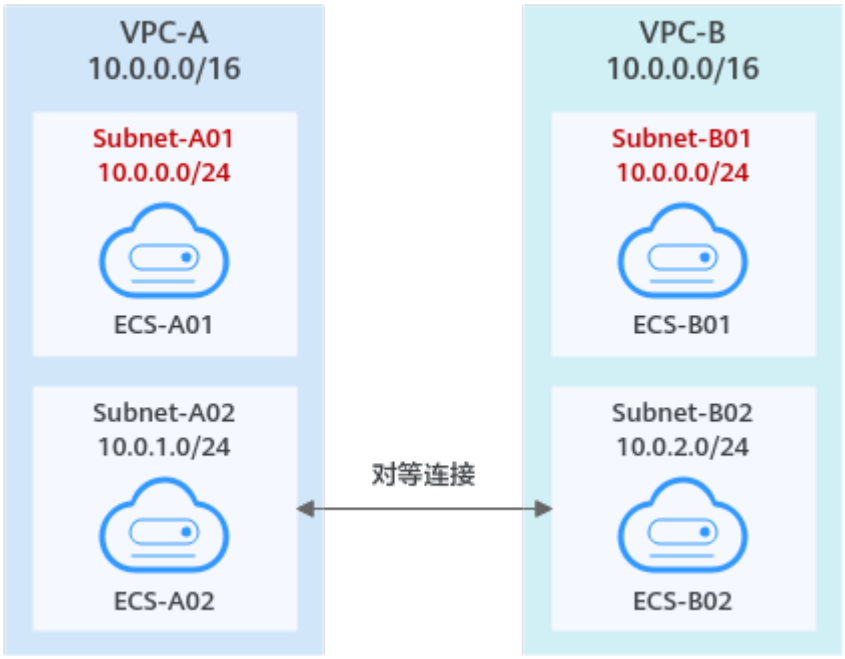


表 8-8 对等连接关系说明-相互对等的两个重叠网段 VPC 子网(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A和VPC-B对等	Peering-AB	VPC-A	VPC-B

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

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

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

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

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

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

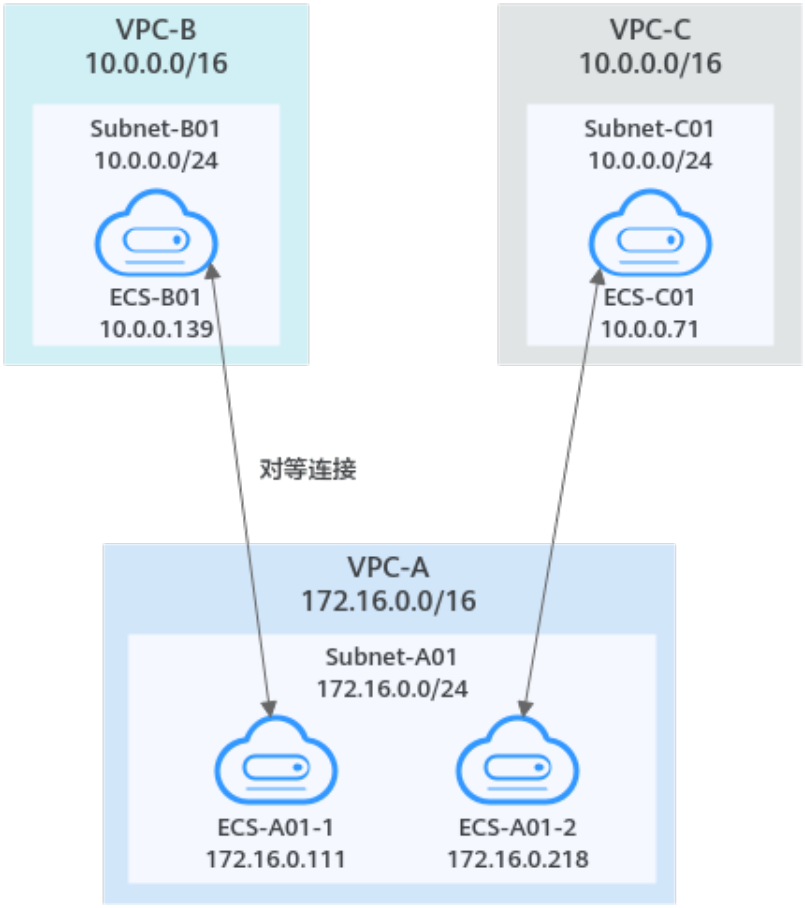


表 8-10 对等连接关系说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

VPC对等关系	对等连接名称	本端VPC	对端VPC
VPC-A内ECS-A01-1和VPC-B内ECS-B01对等	Peering-AB	VPC-A	VPC-B
VPC-A内ECS-A01-2和VPC-C内ECS-C01对等	Peering-AC	VPC-A	VPC-C

表 8-11 VPC 路由表配置说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.139/32	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为ECS-B01的私有IP地址，下一跳指向Peering-AB的路由。

路由表	目的地址	下一跳	路由类型	路由说明
	10.0.0.71/32	Peering-AC	自定义	在VPC-A的路由表中，添加目的地址为ECS-C01的私有IP地址，下一跳指向Peering-AC的路由。
rtb-VPC-B	172.16.0.111/32	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为ECS-A01-1的私有IP地址，下一跳指向Peering-AB的路由。
rtb-VPC-C	172.16.0.218/32	Peering-AC	自定义	在VPC-C的路由表中，添加目的地址为ECS-A01-2的私有IP地址，下一跳指向Peering-AC的路由。

无效的 VPC 对等连接

当VPC网段重叠，且全部子网重叠时，不支持使用对等连接。以网段和子网完全重叠的VPC-A和VPC-B为例，假如在VPC-A和VPC-B之间创建对等连接，那么路由表会由于目的地址重叠而导致流量传输错误。

在rtb-VPC-A路由表中，Local路由和对等连接路由的目的地址重叠，VPC-A往VPC-B的流量，会优先匹配Local路由，流量在VPC-A内部转发，无法送达VPC-B。

图 8-9 VPC 网段重叠，且全部子网重叠(IPv4)

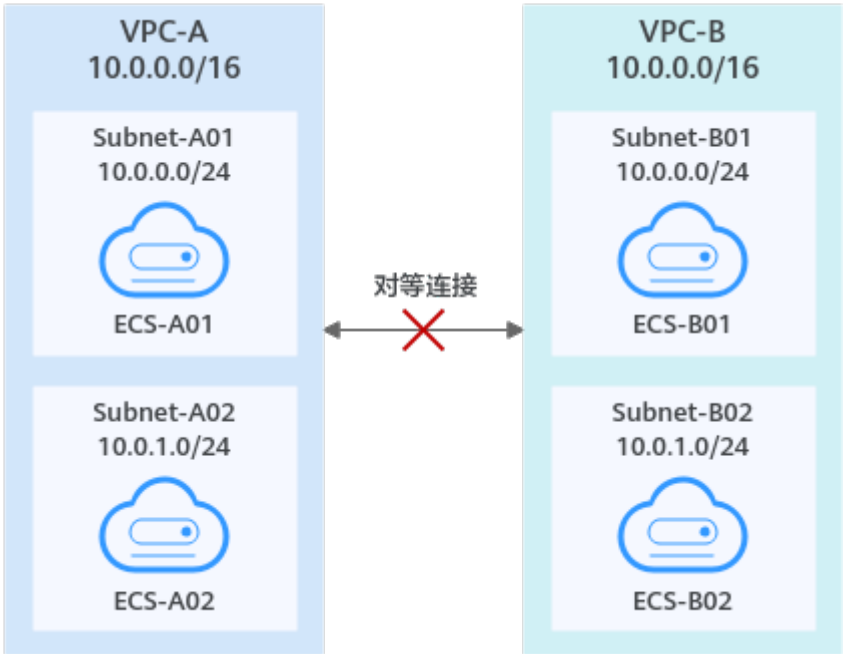


表 8-12 VPC 路由表配置说明-VPC 网段重叠，且全部子网重叠(IPv4)

路由表	目的地址	下一跳	路由类型	路由说明
rtb-VPC-A	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-B)	Peering-AB	自定义	在VPC-A的路由表中，添加目的地址为VPC-B的网段，下一跳指向Peering-AB的路由。
rtb-VPC-B	10.0.0.0/24	Local	系统路由	Local路由是系统自动添加的，用于VPC内部通信。
	10.0.1.0/24	Local	系统路由	
	10.0.0.0/16 (VPC-A)	Peering-AB	自定义	在VPC-B的路由表中，添加目的地址为VPC-A的网段，下一跳指向Peering-AB的路由。

8.3 创建相同账户下的对等连接

操作场景

不同VPC之间网络不通，您可以通过对等连接连通同一个区域下的VPC。本章节指导用户创建相同账户下的VPC对等连接，即连通的两个VPC位于同一个账户下。

本文档以在账户A下，创建VPC-A和VPC-B之间的对等连接为例，实现业务服务器ECS-A01和数据库服务器RDS-B01之间的通信。

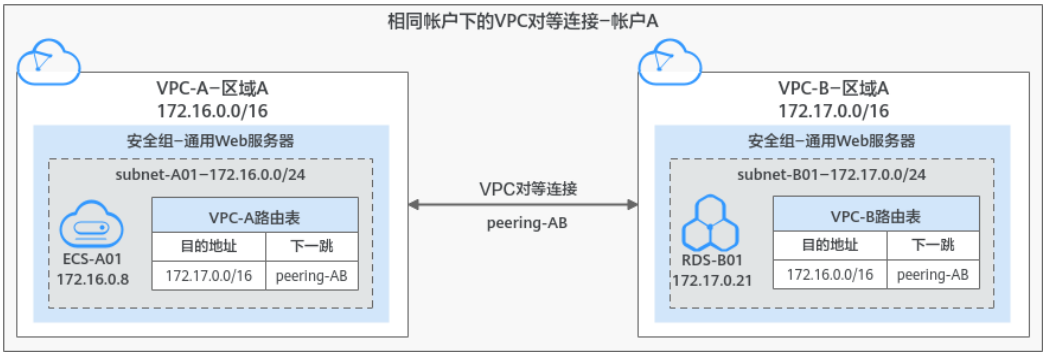
创建步骤如下：

步骤一：创建VPC对等连接

步骤二：添加VPC对等连接路由

步骤三：验证网络互通情况

图 8-10 相同账户下的对等连接组网示例



约束与限制

- 对等连接是建立在两个VPC之间的网络连接，两个VPC之间只能建立一个对等连接。
- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。

前提条件

已在同一个账号下创建两个VPC，并且VPC位于同一个区域，具体方法请参见**创建虚拟私有云和子网**。

步骤一：创建 VPC 对等连接

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在页面右上角区域，单击“创建对等连接”。
   弹出“创建对等连接”对话框。
5. 根据界面提示设置对等连接参数。
   参数详细说明请参见**表8-13**。

表 8-13 创建对等连接-参数说明

参数	说明	取值样例
对等连接名称	必选参数。 此处填写对等连接的名称。 由中文字符、英文字母、数字、中划线、下划线等构成，一般不超过64个字符。	peering-AB
本端VPC	必选参数。 此处为对等连接一端的VPC，可以在下拉框中选择已有VPC作为本端VPC。	VPC-A
本端VPC网段	此处显示已选择的本端VPC的网段。	172.16.0.0/16

参数	说明	取值样例
账户	必选参数。 • 当前账户：当对等连接中的对端VPC和本端VPC位于同一个账户下时，选择该项。 • 其他账户：当对等连接中的对端VPC和本端VPC位于不同账户下时，选择该项。	当前账户
对端项目	当账户选择“当前账户”时，系统默认填充对应的项目，无需您额外操作。 比如VPC-A和VPC-B均为账户A下的资源，并且位于区域A，那么此处系统默认显示账户A下，区域A对应的项目。	ab-cdef-1
对端VPC	当账户选择“当前账户”时，该项为必选参数。 此处为对等连接另外一端的VPC，可以在下拉框中选择已有VPC作为对端VPC。	VPC-B
对端VPC网段	此处显示已选择的对端VPC的网段。 当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效，具体请参见**对等连接使用示例**。	172.17.0.0/16
描述	可选参数。 您可以根据需要在文本框中输入对等连接的描述信息。	peering-AB连通VPC-A和VPC-B

6. 参数填写完成后，单击“确定”。
   弹出路由添加提示对话框。
7. 在路由添加提示对话框中，执行以下操作。
   a. 单击“查看路由”，跳转到“本端路由”页面，继续执行**步骤二：添加VPC对等连接路由**，添加路由。
   b. 单击“暂不添加”，返回对等连接列表页面。

步骤二：添加 VPC 对等连接路由

通常情况下，您需要在对等连接两端VPC的路由表中分别添加去程和回程路由，才可以实现通信，单击了解**对等连接使用示例**。

1. 执行以下操作，在本端VPC路由表中添加对等连接路由。
   a. 在对等连接的“本端路由”页签，根据左上方界面提示，单击路由表超链接。

进入本端VPC的默认路由表基本信息页面。

b. 单击“添加路由”，在默认路由表中添加路由。
参数说明如表8-14所示。

表 8-14 参数说明

参数	说明	取值样例
目的地址	对端VPC的地址，可以为VPC网段、子网网段、ECS IP地址等，具体请参见对等连接使用示例。	此处为VPC-B的网段：172.17.0.0/16
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-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

2. 执行以下步骤，在对端VPC路由表中添加对等连接路由。
a. 选择“对端路由”页签，根据左上方界面提示，单击路由表超链接。
进入对端VPC默认路由表的基本信息页签。
b. 单击“添加路由”，在默认路由表中添加路由。
参数说明如表8-15所示。

表 8-15 参数说明

参数	说明	取值样例
目的地址	本端VPC的地址，可以为VPC网段、子网网段、ECS IP地址等，具体请参见对等连接使用示例。	此处为VPC-A的网段：172.16.0.0/16
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-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

步骤三：验证网络互通情况

对等连接路由添加完成后，执行以下操作，验证本端VPC和对端VPC的通信情况。

1. 登录本端VPC内的弹性云服务器，本示例中为ECS-A01。
2. 执行以下命令，验证ECS-A01和的RDS-B01是否可以通信。

   ping *对端服务器的IP地址*

   命令示例：

   ping 172.17.0.21

   回显类似如下信息，表示ECS-A01与RDS-B01可以通过通信，VPC-A和VPC-B之间的对等连接创建成功。

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

须知

- 本示例中ECS-A01和RDS-B01位于同一个安全组内，因此只要VPC-A和VPC-B之间的对等连接创建成功后，就可以实现网络互通。如果您需要连通的实例位于不同的安全组内，那么您需要在安全组的入方向规则中，添加放通对端安全组的规则，具体方法请参见**不同安全组内实例内网网络互通**。
- 对于更多对等连接网络不通的问题，处理方法请参见**为什么对等连接创建完成后不能互通？**。

8.4 创建不同账户下的对等连接

操作场景

不同VPC之间网络不通，您可以通过对等连接连通同一个区域下的VPC。本章节指导用户创建不同账户下的VPC对等连接，即连通的两个VPC位于不同账户下。

本文档以在账户A下的VPC-A和账户B的VPC-B之间创建对等连接为例，实现业务服务器ECS-A01和数据库服务器RDS-B01之间的通信。

创建步骤如下：

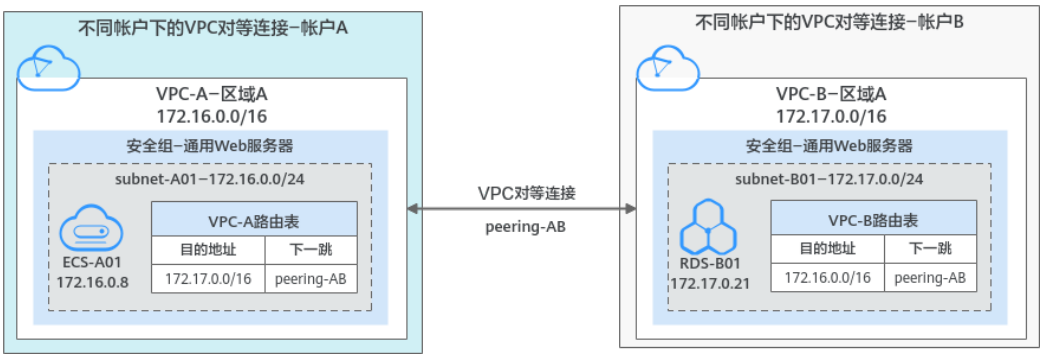
步骤一：创建VPC对等连接

步骤二：对端账户接受VPC对等连接

步骤三：添加VPC对等连接路由

步骤四：验证网络互通情况

图 8-11 不同账户下的对等连接组网示例



约束与限制

- 对等连接是建立在两个VPC之间的网络连接，两个VPC之间只能建立一个对等连接。
- 对等连接仅可以连通同区域的VPC，不同区域的VPC之间不能创建对等连接。
- 配置对等连接时，当您的本端VPC和对端VPC存在网段重叠的情况时，那么您的对等连接可能会不生效。
- 创建不同账户下的对等连接时：
  - 创建不同账户下的VPC对等连接时，如果在账号A下发起创建对等连接请求，需要账号B接受该请求才可以，如果账号B拒绝，则该对等连接创建失败。
  - 为了确保网络安全，请您不要接受来自未知账号的对等连接申请。

前提条件

已在不同账号下，分别创建两个VPC，并且VPC位于同一个区域，具体方法请参见**创建虚拟私有云和子网**。

步骤一：创建 VPC 对等连接

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在页面右上角区域，单击“创建对等连接”。
   弹出“创建对等连接”对话框。
5. 根据界面提示设置对等连接参数。
   参数详细说明请参见**表8-16**。

表 8-16 创建对等连接-参数说明

参数	说明	取值样例
对等连接名称	必选参数。 此处填写对等连接的名称。 由中文字符、英文字母、数字、中划线、下划线等构成，一般不超过64个字符。	peering-AB
本端VPC	必选参数。 此处为对等连接一端的VPC，可以在下拉框中选择已有VPC作为本端VPC。	VPC-A
本端VPC网段	此处显示已选择的本端VPC的网段。	172.16.0.0/16
账户	必选参数。 • 当前账户：当对等连接中的对端VPC和本端VPC位于同一个账户下时，选择该项。 • 其他账户：当对等连接中的对端VPC和本端VPC位于不同账户下时，选择该项。	其他账户
对端项目ID	当账户选择“其他账户”时，该项为必选参数。 对端项目ID是另一个账户下，对端VPC所在区域对应的项目ID，获取方法请参见**获取对等连接的对端项目ID**。	VPC-B在区域A对应的项目ID： 067cf8aecf3XXX08322f13b
对端VPC ID	当账户选择“其他账户”时，该项为必选参数 对端VPC ID是对等连接另一端的VPC ID，获取方法请参见**获取虚拟私有云的ID信息**。	VPC-B的ID: 17cd7278-XXX-530c952dcf35
描述	可选参数。 您可以根据需要在文本框中输入对该连接的描述信息。描述信息内容不能超过255个字符，且不能包含“<”和“>”。	peering-AB连通VPC-A和VPC-B

6. 参数填写完成后，单击“确定”。
   - 如果提示“请输入正确的VPC ID以及项目ID”，请您检查项目ID和VPC ID的正确性。
     - 项目ID：必须为对端VPC所在区域对应的项目ID。
     - 本端VPC必须和对端VPC位于同一个区域。

- 如果返回对等连接列表，且新创建的对等连接状态为“待接受”，请继续执行**步骤二：对端账户接受VPC对等连接**，联系账户B处理。

步骤二：对端账户接受 VPC 对等连接

不同账户创建对等连接，本端账户创建完成后，需要联系对端账户接受对等连接请求之后，该对等连接才算创建完成。本示例中，账户A通知账户B接受对等连接。

1. 对端账户登录管理控制台。
2. 在页面左上角单击三图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表中，找到待接受的对等连接请求。
5. 确认无误后，单击目标对等连接所在行的操作列下的“接受请求”。
   待对等连接状态变为“已接受”，表示对等连接创建完成。
6. 执行**步骤三：添加VPC对等连接路由**，为对等连接添加路由。

步骤三：添加 VPC 对等连接路由

通常情况下，您需要在对等连接两端VPC的路由表中分别添加去程和回程路由，才可以实现通信，单击了解**对等连接使用示例**。

本端账户在本端VPC的路由表中添加路由，对端账户在对端VPC的路由表中添加路由。本示例中，账户A在VPC-A的路由表中添加路由，账户B在VPC-B的路由表中添加路由。

1. 执行以下操作，在本端VPC路由表中添加对等连接路由。
   a. 在本端账户的对等连接列表中，单击目标对等连接的名称。
      进入对等连接的基本信息页面。
   b. 在对等连接的“本端路由”页签，根据左上方界面提示，单击路由表超链接。
      进入本端VPC的默认路由表基本信息页面。
   c. 单击“添加路由”，在默认路由表中添加路由。
      参数说明如**表8-17**所示。

表 8-17 参数说明

参数	说明	取值样例
目的地址	对端VPC的地址，可以为VPC网段、子网网段、ECS IP地址等，具体请参见**对等连接使用示例**。	此处为VPC-B的网段：172.17.0.0/16
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-AB

参数	说明	取值样例
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

2. 执行以下操作，在对端VPC路由表中添加对等连接路由。
a. 在对端账户的对等连接列表中，单击目标对等连接的名称。
进入对等连接的基本信息页面。
b. 在对等连接的“本端路由”页签，根据左上方界面提示，单击路由表超链接。
进入对端VPC的默认路由表基本信息页面。
c. 单击“添加路由”，在默认路由表中添加路由。
参数说明如表8-18所示。

表 8-18 参数说明

参数	说明	取值样例
目的地址	本端VPC的地址，可以为VPC网段、子网网段、ECS IP地址等，具体请参见对等连接使用示例。	此处为VPC-A的网段：172.16.0.0/16
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-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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

步骤四：验证网络互通情况

对等连接路由添加完成后，执行以下操作，验证本端VPC和对端VPC的通信情况。

1. 登录本端VPC内的弹性云服务器，本示例中为ECS-A01。
2. 执行以下命令，验证ECS-A01和的RDS-B01是否可以通信。
ping *对端服务器的IP地址*
命令示例：
ping 172.17.0.21
回显类似如下信息，表示ECS-A01与RDS-B01可以通过通信，VPC-A和VPC-B之间的对等连接创建成功。

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
```



```
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

须知

- 本示例中ECS-A01和RDS-B01位于同一个安全组内，因此只要VPC-A和VPC-B之间的对等连接创建成功后，就可以实现网络互通。如果您需要连通的实例位于不同的安全组内，那么您需要在安全组的入方向规则中，添加放通对端安全组的规则，具体方法请参见**不同安全组内实例内网网络互通**。
- 对于更多对等连接网络不通的问题，处理方法请参见**为什么对等连接创建完成后不能互通?** 。

8.5 获取对等连接的对端项目 ID

操作场景

当您创建不同账户下的VPC对等连接时，您可以参考本章节获取对端VPC所在区域对应的项目ID，即对端项目ID。

操作步骤

1. 登录管理控制台。
   此处使用对端账户登录管理控制台。
2. 在页面右上角的用户名的下拉列表中，单击“我的凭证”。
3. 在项目列表中，获取项目ID。

8.6 修改对等连接

操作场景

本章节指导用户修改对等连接的的名称。

对等连接在任何状态下，本端账户和对端账户均有权限修改对等连接。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接所在行的操作列下的“修改”。
   弹出对等连接修改对话框。

5. 修改对等连接的信息，并单击“确定”，完成信息修改。

8.7 查看对等连接

操作场景

本章节指导用户查看对等连接的基本信息，包括对等连接名称、状态、本端VPC以及对端VPC的信息。

对于连通不同账户VPC的对等连接，本端账户和对端账户均可以查看该对等连接。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页，查看对等连接的详细信息。

8.8 删除对等连接

操作场景

本章节指导用户删除对等连接。

对等连接在任何状态下，本端账户和对端账户均有权限删除对等连接。

约束与限制

对等连接双方账号都有权限删除对等连接，一方删除对等连接后，对等连接的所有信息会被立刻删除，包括本端VPC和对端VPC路由表中对等连接的路由信息。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接所在行的操作列下的“删除”。
   弹出对等连接删除确认对话框。
5. 确认无误后，单击“是”，删除对等连接。

8.9 修改对等连接路由

操作场景

本章节指导用户修改对等连接的路由，即修改本端VPC和对端VPC路由表中对等连接关联的路由。

- **修改相同账户对等连接的路由**
- **修改不同账户对等连接的路由**

如果您的对等连接路由添加错误，可以参考本章节修改本端VPC和对端VPC的路由配置。

修改相同账户对等连接的路由

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
   进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接的名称。
   进入对等连接详情页面。
5. 执行以下操作，修改本端VPC中添加的路由信息。
   a. 选择“本端路由”页签，并根据界面提示，单击路由表超链接。
      进入本端VPC默认路由表的基本信息页签。
   b. 找到需要修改的路由，单击操作列的“修改”。
      弹出修改路由对话框。
   c. 修改路由信息，并单击“确定”，完成路由修改。
6. 执行以下操作，修改对端VPC中添加的路由信息。
   a. 选择“对端路由”页签，并根据界面提示，单击路由表超链接。
      进入对端VPC默认路由表的基本信息页签。
   b. 找到需要修改的路由，单击操作列下的“修改”。
      弹出修改路由对话框。
   c. 修改路由信息，并单击“确定”，完成路由修改。

修改不同账户对等连接的路由

通过本端账户修改本端VPC的路由，通过对端账户修改对端VPC的路由，修改方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，修改本端VPC的路由。
   a. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。
      进入虚拟私有云列表页面。

b. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
进入对等连接列表页面。
c. 在对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
d. 执行以下操作，修改本端VPC中添加的路由信息。
i. 选择“本端路由”页签，并根据界面提示，单击路由表超链接。
进入本端VPC默认路由表的基本信息页签。
ii. 找到需要修改的路由，单击操作列下的“修改”。
弹出修改确认对话框。
iii. 修改路由信息，并单击“确定”，完成路由修改。

2. 使用对端账户登录管理控制台，参考1，修改对端VPC的路由。

8.10 查看对等连接路由

操作场景

本章节指导用户查看对等连接的路由，即查看本端VPC和对端VPC添加的路由信息。

- **查看相同账户对等连接的路由**
- **查看不同账户对等连接的路由**

如果您建立了对等连接，但是无法通信，可以参考本章节检查本端VPC和对端VPC的路由配置详情。

查看相同账户对等连接的路由

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
5. 执行以下操作，查看对等连接的路由。
a. 选择“本端路由”页签，可查看此对等连接的本端路由信息。
b. 选择“对端路由”页签，可查看此对等连接的对端路由信息。

查看不同账户对等连接的路由

通过本端账户查看本端VPC的路由，通过对端账户查看对端VPC的路由，查看方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，查看本端VPC的路由。
a. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。

b. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
进入对等连接列表页面。
c. 在对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
d. 选择“本端路由”页签，可查看此对等连接的本端路由信息。

2. 使用对端账户登录管理控制台，参考1，查看对端VPC的路由。

8.11 删除对等连接路由

操作场景

本章节指导用户删除对等连接的路由，即删除本端VPC和对端VPC路由表中对等连接关联的路由。

- **删除相同账户对等连接的路由**
- **删除不同账户对等连接的路由**

删除相同账户对等连接的路由

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
进入对等连接列表页面。
4. 在对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
5. 执行以下操作，删除本端VPC中添加的路由信息。
a. 选择“本端路由”页签，并根据界面提示，单击路由表超链接。
进入本端VPC默认路由表的基本信息页签。
b. 找到需要删除的路由，单击操作列下的“删除”。
弹出删除确认对话框。
c. 确认无误后，单击“是”，删除路由。
6. 执行以下操作，删除对端VPC中添加的路由信息。
a. 选择“对端路由”页签，并根据界面提示，单击路由表超链接。
进入对端VPC默认路由表的基本信息页签。
b. 找到需要删除的路由，单击操作列下的“删除”。
弹出删除确认对话框。
c. 确认无误后，单击“是”，删除路由。

删除不同账户对等连接的路由

通过本端账户删除本端VPC的路由，通过对端账户删除对端VPC的路由，删除方法相同。

1. 使用本端账户登录管理控制台，执行以下操作，删除本端VPC的路由。
   a. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。
      进入虚拟私有云列表页面。
   b. 在左侧导航栏，选择“虚拟私有云 > 对等连接”。
      进入对等连接列表页面。
   c. 在对等连接列表中，单击目标对等连接的名称。
      进入对等连接详情页面。
   d. 执行以下操作，删除本端VPC中添加的路由信息。
      i. 选择“本端路由”页签，并根据界面提示，单击路由表超链接。
         进入本端VPC默认路由表的基本信息页签。
      ii. 找到需要删除的路由，单击操作列下的“删除”。
         弹出删除确认对话框。
      iii. 确认无误后，单击“是”，删除路由。
2. 使用对端账户登录管理控制台，参考**1**，删除对端VPC的路由。

9 VPC 流日志

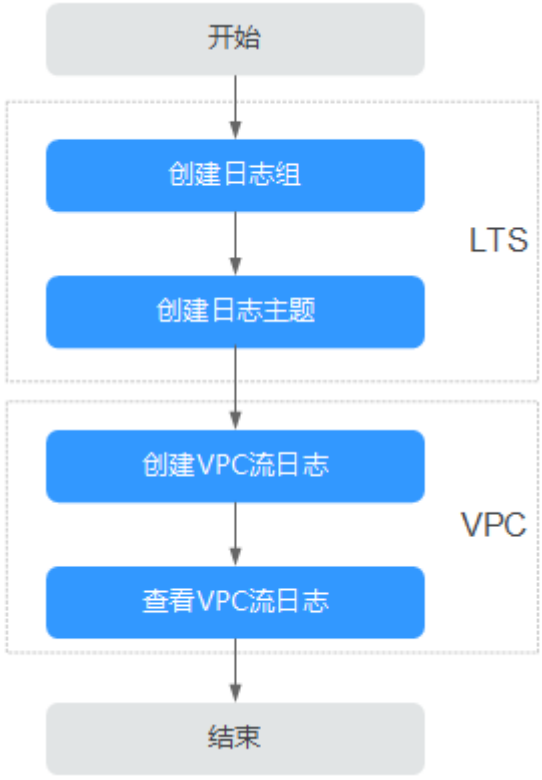
9.1 VPC 流日志简介

流日志简介

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

VPC流日志功能需要与云日志服务LTS结合使用，先在云日志服务中创建日志组和日志主题，然后再创建VPC流日志。配置流程如图9-1所示。

图 9-1 配置 VPC 流日志



约束与限制

- 目前各个区域下，支持采集流日志的云服务器规格类型如下：
  - eu-west-1： C3、CC3、S3、I3
  - eu-west-0：C3、CC3、S3、I3、P2、H1、M2
- 一个用户在单个区域内，最多可创建10个VPC流日志。

9.2 创建 VPC 流日志

操作场景

创建VPC流日志，记录虚拟私有云中的流量信息。

前提条件

在创建VPC流日志前，请确保您在云日志服务完成了如下配置：

- 创建日志组。
- 创建日志主题。

云日志服务更多内容请参见《云日志服务用户指南》。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“VPC流日志”。
4. 在页面右上角，单击“创建VPC流日志”，按照提示配置参数。

表 9-1 参数说明

参数	说明	取值样例
名称	VPC流日志的名称。 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。	flowlog-495d
资源类型	选择要采集流量的资源类型，目前支持网卡类型。	网卡
选择资源	选择需要采集流量信息的具体资源。 **说明** 建议您选择处于开机状态的弹性云服务器。如果选择了关机状态的弹性云服务器，请在VPC流日志创建完成后，重启弹性云服务器，以便准确的记录网卡流量。	-

参数	说明	取值样例
采集类型	• 全部：采集指定资源的全部流量。 • 接受：采集指定资源被安全组或网络ACL允许的流量。 • 拒绝：采集指定资源被网络ACL拒绝的流量。	全部
日志组	选择在云日志服务中创建的日志组。	lts-group-abc
日志流	选择在云日志服务中创建的日志流。	lts-topic-abc
描述	VPC流日志的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

说明

同一个资源在同一个日志组的同一个日志主题下，只能有两个不同采集类型的VPC流日志。不能重复创建相同的VPC流日志。

5. 单击“确定”。

9.3 查看 VPC 流日志

操作场景

查看流日志记录详情。

捕获窗口大约为10分钟，即每10分钟输出一次流日志记录。所以流日志创建完成后，您需要等待大约10分钟，才能查看流日志记录详情。

说明

弹性云服务器关机状态下，不显示流日志记录。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“VPC流日志”。
4. 找到需要查看的流日志，单击操作列的“查看日志”，在云日志服务中查看流日志记录。
   流日志格式：

   ```
   <version> <project-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets> <bytes> <start> <end> <action> <log-status>
   ```

   示例1：在捕获窗口中正常记录数据的流日志记录


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

VPC流日志版本为1，在2019年01月29日16:55:36-17:05:36这10分钟内，网卡（1d515d18-1b36-47dc-a983-bd6512aed4bd）允许流过的流量信息，由源端IP地址和端口（192.168.0.154，38929）通过UDP协议向目的端IP地址和端口（192.168.3.25，53）传输了1个数据包，所有数据包的大小为96 byte。

示例2：在捕获窗口中未记录数据的流日志记录

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - - - - 1431280876 1431280934 - NODATA
```

示例3：在捕获窗口中跳过了数据的流日志记录

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - - - - 1431280876 1431280934 - SKIPDATA
```

字段含义如表9-2所示：

表 9-2 日志字段说明

字段	说明	示例
version	VPC流日志版本。	1
project-id	项目ID。	5f67944957444bd6bb4fe3b367de8f3d
interface-id	为其记录流量的网卡的ID。	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	源地址。	192.168.0.154
dstaddr	目的地址。	192.168.3.25
srcport	源端口。	38929
dstport	目标端口。	53
protocol	IANA协议编号。有关更多信息，请参阅Internet协议编号。	17
packets	数据包的数量。	1
bytes	数据包的大小。	96
start	捕获窗口启动的时间，采用Unix秒的格式。	1548752136
end	捕获窗口结束的时间，采用Unix秒的格式。	1548752736
action	与流量关联的操作： • ACCEPT：安全组或网络ACL允许记录的流量。 • REJECT：安全组或者网络ACL拒绝记录的流量。	ACCEPT

字段	说明	示例
log-status	流日志的日志记录状态： ● OK：数据正常记录到选定目标。 ● NODATA：捕获窗口中没有传入或传出符合“采集类型”的网卡的网络流量。 ● SKIPDATA：捕获窗口中跳过了一些流日志记录。这可能是由于内部容量限制或内部错误。 示例： 如果您创建VPC流日志时设置“采集类型”为“接受”，当有接受流量时，“log-status”将显示为“OK”。当没有接受的流量时，不管是否有拒绝的流量，“log-status”都将显示为“NODATA”。当有一些接受流量异常跳过时，“log-status”将显示为“SKIPDATA”。	OK

同时，您也可以在云日志服务的日志主题详情页面，在搜索框中通过关键字搜索日志。

9.4 开启/关闭 VPC 流日志

操作场景

创建完VPC流日志后，VPC流日志功能会自动开启。当您不需要记录流量数据时，您可以关闭对应的VPC流日志。关闭的VPC流日志，支持再次开启。

约束与限制

- 流日志开启后，系统将会在下个日志采集周期内开始采集流日志数据。
- 流日志关闭后，系统将会在下个日志采集周期内停止采集流日志数据。对于已经生成的流日志数据，仍然会正常上报。

操作步骤

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

3. 在左侧导航栏，选择“VPC流日志”。
4. 找到需要开启或关闭的VPC流日志，单击操作列的“开启”或“关闭”。
5. 单击“是”，确认开启或关闭VPC流日志。

9.5 删除 VPC 流日志

操作场景

删除不用的VPC流日志。删除VPC流日志不会删除云日志服务中的流日志记录。

说明

如果VPC流日志关联的网卡已删除，则对应的VPC流日志会自动删除。但不会删除流日志记录。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“网络 > 虚拟私有云”。进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“VPC流日志”。
4. 找到需要删除的流日志，单击操作列的“删除”。
5. 单击“是”，确认删除。

10 虚拟 IP

10.1 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。

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。

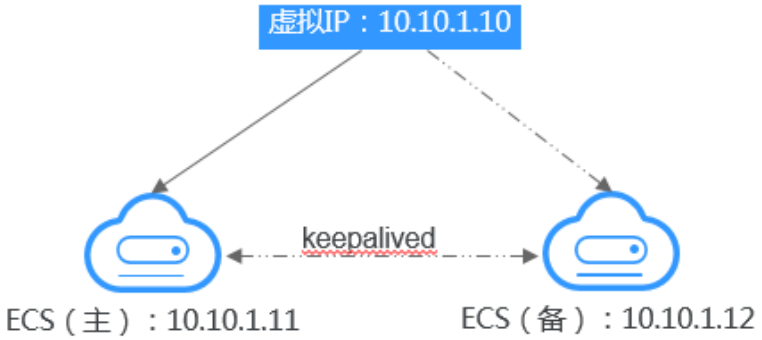
典型组网

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 10-1 HA 高可用性模式组网图

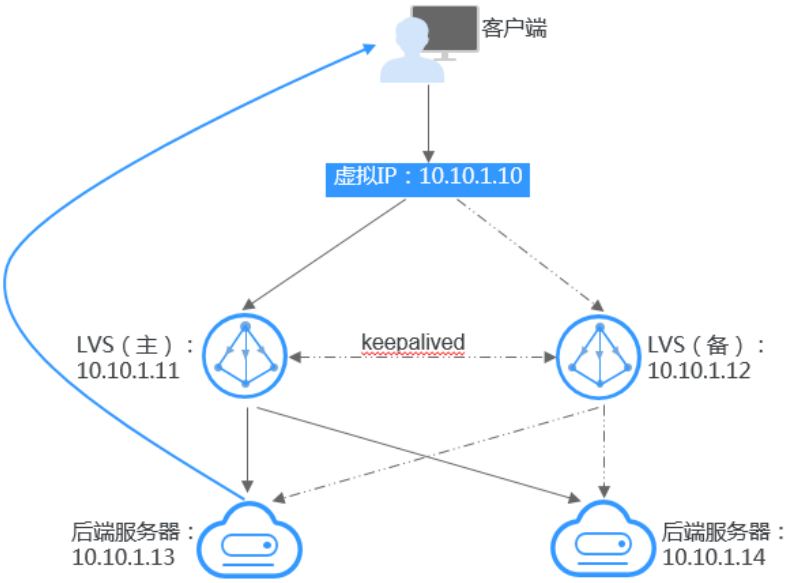


- 将2台同子网的弹性云服务器绑定同一个虚拟IP。
- 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **典型组网2：**高可用负载均衡集群

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

图 10-2 高可用负载均衡集群



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

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。
- 使用虚拟IP构建主备场景时，备弹性云服务器需要关闭IP转发功能，具体请参见**关闭备弹性云服务器的IP转发功能**。

10.2 申请虚拟 IP 地址

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 虚拟私有云”。

   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
4. 在子网列表中，单击需要申请虚拟IP地址的子网名称。
5. 在“IP地址管理”页签中，单击“申请虚拟IP地址”。
6. 选择IP类型。仅在IPv6开放区域可配置。
   - IPv4
   - IPv6
7. 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。
8. 选择手动分配方式，请填写虚拟IP地址。
9. 单击“确定”。

在IP列表中可以查看申请的虚拟IP地址。

10.3 为虚拟 IP 地址绑定弹性 IP 或弹性云服务器

操作场景

您可以通过虚拟IP和弹性IP实现以下场景：

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

约束与限制

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

  说明

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

登录控制台为虚拟 IP 绑定弹性 IP 或弹性云服务器

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏中，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，单击虚拟IP所属子网的名称超链接。
   进入子网详情页面。
5. 在“IP地址管理”页签，执行以下操作，为虚拟IP绑定弹性IP。
   a. 在虚拟IP所在行的操作列下，单击“绑定弹性IP”。
      弹出“绑定弹性IP”对话框。
   b. 在对话框中，选择弹性IP ，并单击“确定”。
      返回虚拟IP列表中，可以看到已绑定的弹性IP。
6. 在“IP地址管理”页签，执行以下操作，为虚拟IP绑定服务器。
   a. 在虚拟IP所在行的操作列下，单击“绑定服务器”。
      弹出“绑定服务器”对话框。
   b. 在对话框中，选择服务器 ，并单击“确定”。
      返回虚拟IP列表中，可以看到已绑定的服务器。

须知

- 弹性云服务器的网卡绑定虚拟IP地址后，需要在弹性云服务器上手工配置虚拟IP地址才可以使用，具体请参见**登录弹性云服务器配置虚拟IP地址**。
- 当弹性云服务器有多张网卡时，建议绑定主网卡。
- 一个弹性云服务器的网卡可以同时绑定多个虚拟IP。

登录弹性云服务器配置虚拟 IP 地址

参考以下章节，为已绑定虚拟IP的弹性云服务器手工配置虚拟IP地址。

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

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

Linux系统（以下配置以“CentOS 7.2 64bit”为例）

1. 执行以下命令，查看并记录需要绑定虚拟IP的网卡及对应连接。

   nmcli connection

   回显类似如下信息：

   ```
   [172.16.0.247_subnet0-ccs-path-gaea-dp0b-ipv4 ~]#nmcli connection
   NAME                UUID                                  TYPE      DEVICE
   Wired connection 1  5e72ec5a-6165-3bd6-a34b-ce43981acb27  ethernet  eth0
   docker0             cd351a91-c5eb-4b69-83eb-df092a2ccf6b  bridge    docker0
   ```

   本示例的回显信息说明如下：

   - **DEVICE**列的**eth0**为需要绑定虚拟IP的网卡。
   - **NAME**列的**Wired connection 1**为网卡对应的连接。

2. 执行以下命令，在目标网卡连接中添加虚拟IP。

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

   参数说明如下：

   - 网卡对应的连接名称：为1中查到的网卡对应的连接，本示例中为**Wired connection 1**。
   - 虚拟IP地址：待添加的虚拟IP地址，如果一次添加多个虚拟IP地址，多个虚拟IP地址之间用“,”隔开。

   命令示例：

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

3. 执行以下命令，使2的配置生效。

   nmcli connection up "*网卡对应的连接名称***"**

   命令示例：

   nmcli connection up "Wired connection 1"

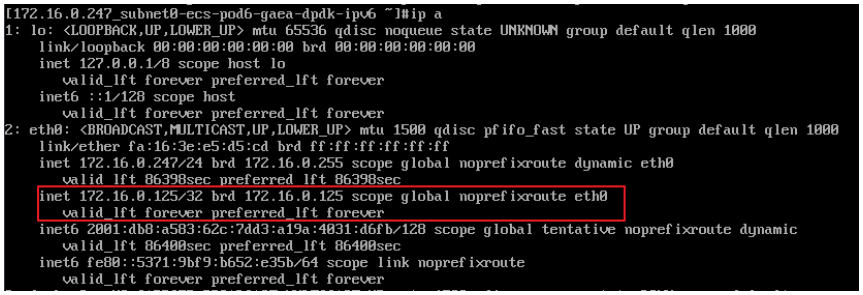
   回显类似如下信息：

   ```
   [172.16.0.247_subnet0-ccs-path-gaea-dp0b-ipv4 ~]#nmcli connection up "Wired connection 1"
   Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
   ```

4. 执行以下命令，检查虚拟IP配置是否成功。

   ip a

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



   说明

   如果您需要删除已添加的虚拟IP，可以使用以下方法：

   1. 在目标网卡连接中删除虚拟IP。

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

      一次删除多个虚拟IP地址时，多个IP之间用“,”隔开，命令示例：

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

   2. 参考**3**，使删除操作生效。

Linux系统（以下配置以“Ubuntu 22.04 server 64bit ”为例）

当弹性云服务器的操作系统为**Ubuntu 22**和**Ubuntu 20**时，请参考以下方法进行配置。

1. 执行以下命令，查看并记录需要绑定虚拟IP的网卡。

   ifconfig

   回显类似如下信息，本示例中绑定虚拟IP的网卡名称为**eth0**。

```
root@ecs-X-ubantu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.0.210  netmask 255.255.255.0  broadcast 172.16.0.255
        inet6 fe80::f816:3eff:fe01:f1c3  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:01:f1:c3  txqueuelen 1000  (Ethernet)
        RX packets 43915  bytes 63606486 (63.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3364  bytes 455617 (455.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
...
```

2. 执行以下命令，进入“/etc/netplan”目录。

   cd /etc/netplan

3. 执行以下命令，为目标网卡添加虚拟IP地址。

   a. 执行以下命令，打开配置文件“01-netcfg.yaml”。

      vim 01-netcfg.yaml

   b. 按i进入编辑模式。

   c. 在对应网卡配置区域内，添加虚拟IP地址。

      本示例为**eth0**添加虚拟IP地址，待添加内容如下：

      addresses:

- 172.16.0.26/32

添加后文件内容如下：

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

d. 添加完成后，按“ESC”，并输入“:wq!”，保存后退出文件。

4. 执行以下命令，使3的配置生效。

   netplan apply

5. 执行以下命令，检查虚拟IP配置是否成功。

   ip a

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

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

说明

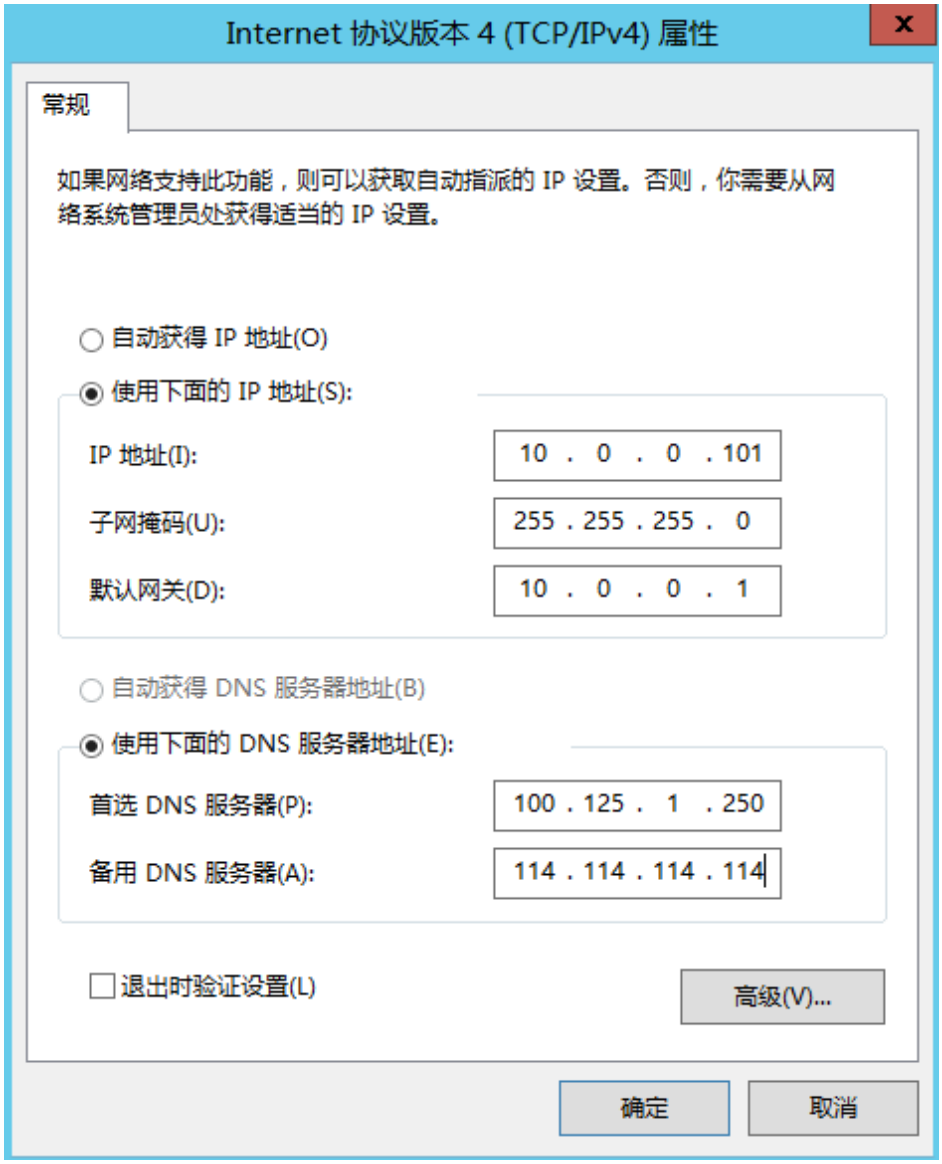
如果您需要删除已添加的虚拟IP，可以使用以下方法：

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

Windows系统（本文以“Windows Server”为例）

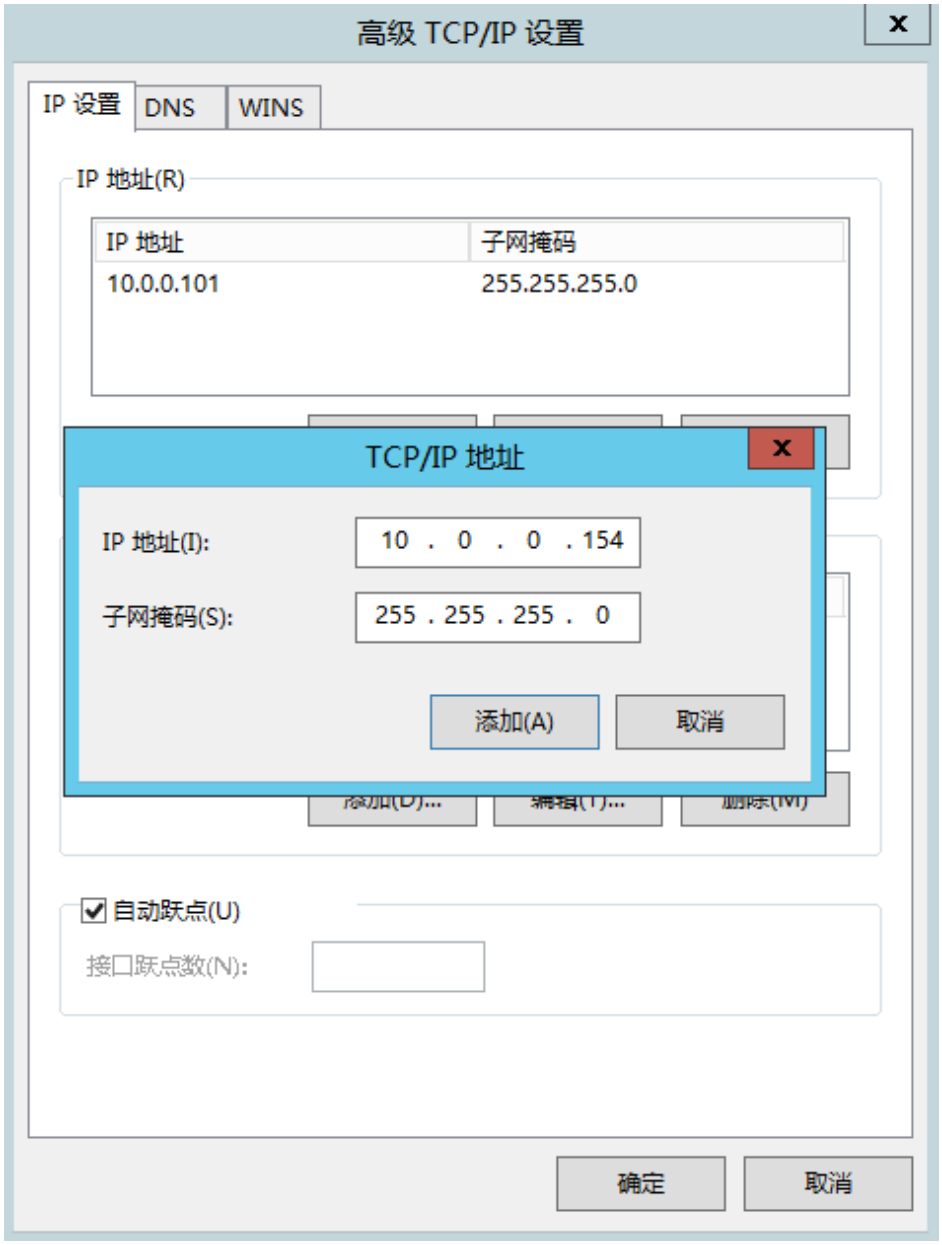
1. 在“控制面板 > 网络和共享中心”路径下，单击对应的本地连接。
2. 在打开的本地连接页面中，单击“属性”。
3. 在“网络”页签中选择“Internet 协议版本 4（TCP/IPv4）”。
4. 单击“属性”。
5. 选择“使用下面的IP地址”，IP地址配置为弹性云服务器的私有IP地址，例如：10.0.0.101。

图 10-3 配置私有 IP 地址



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

图 10-4 配置虚拟 IP 地址



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

   ipconfig /all

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

10.4 为弹性 IP 绑定虚拟 IP 地址

操作场景

本章节指导用户为弹性IP绑定虚拟IP地址。

前提条件

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 弹性IP”。
   进入弹性IP列表页面。
3. 在需要绑定虚拟IP的弹性IP地址所在行，单击“绑定”。
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”。

10.5 为虚拟 IP 解绑实例

操作场景

本章节指导用户解绑虚拟IP上的弹性云服务器。

操作步骤

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

10.6 为虚拟 IP 解绑弹性 IP

操作场景

本章节指导用户解绑虚拟IP上的弹性IP。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，选择“网络 > 虚拟私有云”。
   进入虚拟私有云列表页面。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
   进入子网列表页面。
4. 在子网列表中，单击虚拟IP地址所属的子网名称超链接。
   进入子网“基本信息”页面。
5. 选择“IP地址管理”页签。
   进入虚拟IP列表页面。
6. 在虚拟IP列表中，在目标虚拟IP所在操作列表下，单击“解绑弹性IP”。
   弹出解绑确认对话框。
7. 确认无误后，单击“是”，将虚拟IP和弹性IP解绑。

10.7 删除虚拟 IP 地址

操作场景

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

约束与限制

当虚拟IP被其他资源占用时，无法删除，请根据提示信息进行处理，具体请参见**表10-1**。

表 10-1 虚拟 IP 无法删除原因说明

提示信息	原因说明及处理方法
已绑定实例或弹性IP地址，无法执行删除操作，请先执行对应解绑操作。	当前虚拟IP可能被弹性IP、弹性云服务占用，请先解绑占用资源，再删除虚拟IP。 具体方法如下： ● 弹性IP：请参见**为虚拟IP解绑弹性IP**。 ● 弹性云服务器：请参见**为虚拟IP解绑实例**。 解绑完成后，可以重新尝试删除虚拟IP。

提示信息	原因说明及处理方法
虚拟IP已被系统组件使用，无法执行操作。	当前虚拟IP被RDS实例使用，该IP不支持单独删除。如果您不需要使用该虚拟IP，请删除RDS实例，该虚拟IP会被同时删除。

操作步骤

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

   图 10-5 删除虚拟 IP 地址

6. 确认无误后，单击“是”，删除虚拟IP地址。

10.8 关闭备弹性云服务器的 IP 转发功能

操作场景

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

Linux 系统

1. 登录弹性云服务器。
2. 执行以下命令，切换root用户。
   su root
3. 执行以下命令，查看IP转发功能是否已开启。
   cat /proc/sys/net/ipv4/ip_forward
   回显结果：1为开启，0为关闭，默认为0。
   - 回显为1，继续执行4。
   - 回显为0，任务结束。
4. 以下提供两种方法修改配置文件，二选一即可。
   - 方法一：使用vi打开“/etc/sysctl.conf”文件，修改net.ipv4.ip_forward = 0，按“:wq”保存退出。

- 方法二：执行sed命令，命令示例如下：
  sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf

5. 执行以下命令，使修改生效。
   sysctl -p /etc/sysctl.conf

Windows 系统

1. 登录弹性云服务器。
2. 打开Windows系统的“命令提示符”窗口，执行以下命令。
   ipconfig/all
   当回显结果中，“IP 路由已启用”为 “否”， 表示IP转发功能已关闭。
3. 按“Windows+R”打开运行窗口，输入**regedit**，进入注册表编辑器。
4. 编辑**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**下的**IPEnableRouter**值为0。
   - 指定值为 0：关闭 IP 转发。
   - 指定值为 1：启用 IP 转发。

10.9 关闭弹性云服务器网卡的源/目的检查

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“计算 > 弹性云服务器”。
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”。

11 审计

11.1 支持审计的关键操作

通过云审计，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。

云审计支持的虚拟私有云操作列表如表11-1所示。

表 11-1 云审计服务支持的 VPC 操作列表

操作名称	资源类型	事件名称
修改Bandwidth	bandwidth	modifyBandwidth
创建EIP	eip	createEip
释放EIP	eip	deleteEip
绑定EIP	eip	bindEip
解绑定EIP	eip	unbindEip
创建PrivateIp	privateIps	createPrivateIp
删除PrivateIp	privateIps	deletePrivateIp
创建Security Group	security_groups	createSecurity-group
更新Security Group	security_groups	updateSecurity-group
删除Security Group	security_groups	deleteSecurity-group
创建Security Group Rule	security-group-rules	createSecurity-group-rule
更新Security Group Rule	security-group-rules	updateSecurity-group-rule
删除Security Group Rule	security-group-rules	deleteSecurity-group-rule

操作名称	资源类型	事件名称
创建Subnet	subnet	createSubnet
删除Subnet	subnet	deleteSubnet
修改Subnet	subnet	modifySubnet
创建VPC	vpc	createVpc
删除VPC	vpc	deleteVpc
修改VPC	vpc	modifyVpc
创建VPN	vpn	createVpn
删除VPN	vpn	deleteVpn
修改VPN	vpn	modifyVpn
创建Router	routers	createRouter
更新Router	routers	updateRouter
Router添加接口	routers	addRouterInterface
Router删除接口	routers	removeRouterInterface
创建Port	ports	createPort
更新Port	ports	updatePort
删除Port	ports	deletePort
创建Network	networks	createNetwork
更新Network	networks	updateNetwork
删除Network	networks	deleteNetwork
批量创建和删除Subnet资源标签	tag	batchUpdateTags
批量创建和删除VPC资源标签	tag	batchUpdateVpcTags
创建RouteTable	routetables	createRouteTable
更新RouteTable	routetables	updateRouteTable
删除RouteTable	routetables	deleteRouteTable
创建VPC Peerings	vpc-peerings	createVpcPeerings
更新VPC Peerings	vpc-peerings	updateVpcPeerings
删除VPC Peerings	vpc-peerings	deleteVpcPeerings
创建网络ACL组	firewall-groups	createFirewallGroup
更新网络ACL组	firewall-groups	updateFirewallGroup

操作名称	资源类型	事件名称
删除网络ACL组	firewall-groups	deleteFirewallGroup
创建网络ACL策略	firewall-policies	createFirewallPolicy
更新网络ACL策略	firewall-policies	updateFirewallPolicy
删除网络ACL策略	firewall-policies	deleteFirewallPolicy
插入网络ACL规则	firewall-policies	insertFirewallPolicyRule
移除网络ACL规则	firewall-policies	removeFirewallPolicyRule
创建网络ACL规则	firewall-rules	createFirewallRule
更新网络ACL规则	firewall-rules	updateFirewallRule
删除网络ACL规则	firewall-rules	deleteFirewallRule
创建Address Group	address_group	createAddress_group
更新Address Group	address_group	updateAddress_group
强制删除Address Group	address_group	force_deleteAddress_group
删除Address Group	address_group	deleteAddress_group
创建Flow Log	flowlogs	createFlowLog
更新Flow Log	flowlogs	updateFlowLog
删除Flow Log	flowlogs	deleteFlowLog

11.2 查看审计日志

操作场景

在您开通了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击 图标，打开服务列表，选择“管理与部署 > 云审计服务”，进入云审计服务信息页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持不同维度的组合查询，详细信息如下：
   - 事件来源、资源类型和筛选类型。
     在下拉框中选择查询条件。

其中筛选类型选择事件名称时，还需选择某个具体的事件名称。

选择资源ID时，还需选择或者手动输入某个具体的资源ID。

选择资源名称时，还需选择或手动输入某个具体的资源名称。

- 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
- 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
- 时间范围：可选择查询“最近1小时”、“最近1天”、“最近1周”以及最近1周内自定义时间段的操作事件。

5. 在需要查看的记录左侧，单击箭头展开该记录的详细信息。
6. 在需要查看的记录右侧，单击“View Trace”，弹出的窗口显示该操作事件结构的详细信息。

12 监控

12.1 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 12-1 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。 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。 单位：比特/秒	≥ 0 bit/s	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）
upstream_bandwidth_usage	出网带宽使用率	该指标用于统计测量对象出云平台的带宽使用率，以百分比为单位。 出网带宽使用率=出网带宽指标/购买的带宽大小	0-100%	带宽或弹性IP	1分钟
downstream_bandwidth_usage	入网带宽使用率	该指标用于统计测量对象入云平台的带宽使用率，以百分比为单位。 入网带宽使用率=入网带宽指标/购买的带宽大小	0-100%	带宽或弹性IP	1分钟
up_stream	出网流量	该指标用于统计测试对象出云平台一分钟内累积的网络流量平均值。 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台一分钟内累积的网络流量平均值。 单位：字节	≥ 0 bytes	带宽或弹性IP	1分钟

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"
  }
  ],

12.2 查看监控指标

操作场景

查看带宽、弹性IP的使用情况。

具体可查看指定时间段内的入网带宽、出网带宽、入网带宽使用率、出网带宽使用率、入网流量和出网流量等使用数据信息。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“管理与部署 > 云监控服务”。
3. 单击页面左侧的“云服务监控”，选择“弹性IP和带宽”。
4. 单击“操作”列的“查看监控指标”，查看带宽或弹性IP的监控指标详情。

12.3 创建告警规则

操作场景

通过设置告警规则，用户可自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，选择“管理与部署 > 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”。
   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》。

13

13.1

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

前提条件

若您需要对除VPC之外的其他服务授权，IAM支持服务的所有策略请参见。

示例流程

1. **创建用户组并授权**

   在IAM控制台创建用户组，并授予VPC只读权限“VPCReadOnlyAccess”。
2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

   - 在“服务列表”中选择虚拟私有云，进入VPC主界面，单击右上角“创建虚拟私有云”，如果无法创建虚拟私有云（假设当前权限仅包含VPCReadOnlyAccess），表示“VPCReadOnlyAccess”已生效。

13.2 VPC 自定义策略

如果系统预置的VPC权限，不满足您的授权要求，可以创建自定义策略。

目前云平台支持以下两种方式创建自定义策略：

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

VPC 自定义策略样例

- 示例1：授权用户创建和查看VPC

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

- 示例2：拒绝用户删除VPC

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

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

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

- 示例3：多个授权项策略

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

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


14 常见问题

14.1 通用类

14.1.1 什么是配额?

什么是配额?

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

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

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

如何申请扩大配额?

目前系统暂不支持在线调整配额大小。

如您需要调整配额，请联系运营管理员。

14.2 计费类

14.2.1 VPC 是否收费?

VPC本身不收取费用。但用户在使用带宽或VPN时需要按照收费标准购买。

14.2.2 弹性 IP 如何计费?

弹性IP提供“按需计费”的计费模式。以下为您详细介绍EIP的计费情况:

- 快速了解EIP计费情况，请参见图14-1。
- 详细了解EIP计费情况，请参见表14-1。

图 14-1 弹性 IP 计费概览

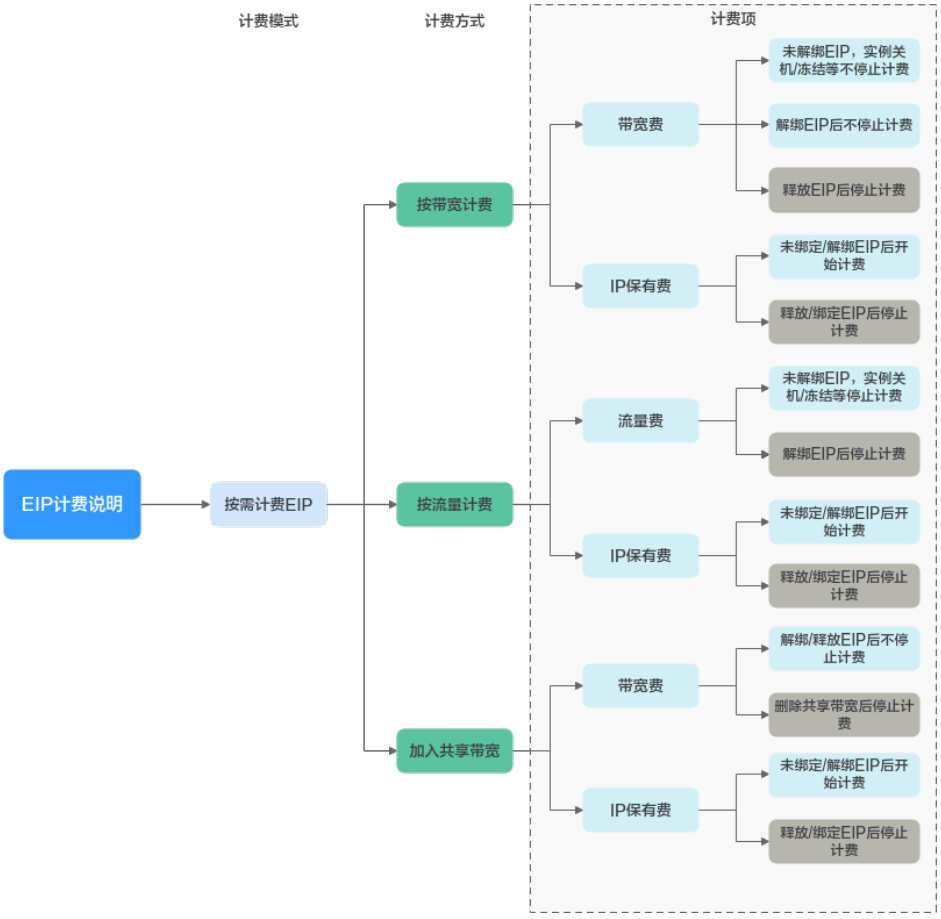


表 14-1 弹性 IP 计费情况说明

计费模式	计费方式	计费项	计费项说明	操作EIP对计费项的影响
按需计费	按带宽计费	• 带宽费 • 保有费	按需计费的EIP选择按带宽计费时，有以下两个计费项： • 带宽费：按照您指定的带宽大小及实际使用时长计费，不限流量。您购买EIP时可以指定带宽大小，后续支持修改。使用过程中，您实际的带宽不能高于指定带宽大小。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 未绑定EIP，收取带宽费和保有费。 • 绑定EIP后，收取带宽费，停止收取保有费。**无论EIP绑定的实例是否运行，不影响费用，比如ECS关机后，会继续收取带宽费，不收取保有费。** • **解绑EIP后，继续收取带宽费，同时新增保有费。** • 释放EIP后，停止收取带宽费和保有费。
	按流量计费	• 流量费 • 保有费	按需计费的EIP选择按流量计费时，有以下两个计费项： • 流量费：按照您指定的线路类型及实际流量使用量计费，云平台仅收取出网流量费用，不收取入网流量费用。按流量计费的EIP，带宽仅做限速使用，不收取费用。为了防止突然爆发的流量产生较高的费用，建议您购买EIP的时候指定带宽大小，为出网带宽设置一个峰值。 按流量计费的EIP使用的独享带宽，仅收取出云方向带宽费用，不收取入云方向带宽费用。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 未绑定EIP，不收取流量费，收取保有费。 • 绑定EIP后，按照实际产生的流量收取流量费用，停止收取保有费。**EIP绑定的实例停止运行后，不产生流量则不收取流量费，比如ECS关机后，停止收取流量费，不收取保有费。** • **解绑EIP后，停止收取流量费，同时新增保有费。** • 释放EIP后，停止收取保有费。

计费模式	计费方式	计费项	计费项说明	操作EIP对计费项的影响
	加入共享带宽	• 带宽费 • 保有费	按需计费的EIP选择加入共享带宽时，有以下两个计费项： • 带宽费：此处带宽费为共享带宽的费用，共享带宽中可同时加入多个EIP，这些EIP使用期间的带宽和流量均不再单独计费，以共享带宽的费用为准。 • 保有费：按需计费的EIP，如果未绑定至实例，并且未释放的情况下，则会收取保有费。	购买EIP后，以下操作会影响费用，具体说明如下： • 带宽费： – **对EIP执行的任何操作，均不影响共享带宽计费情况。比如您已经释放了EIP，但是未删除共享带宽，则共享带宽会继续计费。** – 删除共享带宽，停止收取带宽费。 • 保有费： – 未绑定EIP，收取保有费。 – **解绑EIP后，新增保有费。** – 释放/绑定EIP后，停止收取保有费。

您可以将同一个区域内的多个EIP加入一条共享带宽中，实现带宽复用，为您节省费用。共享带宽单独计费，共享带宽提供“按需计费”的计费模式。共享带宽费用说明请参见表14-2。当前只有按需计费的EIP可以加入共享带宽中：

- 您可以在购买EIP时，将EIP加入共享带宽。
- 您还可以将已有的EIP加入共享带宽，EIP原有的按带宽计费或者按流量计费会停止，后续只收取共享带宽费用。

表 14-2 共享带宽计费情况说明

计费模式	计费方式	计费项	计费项说明
按需计费	按带宽计费	带宽费	按照您指定的带宽大小及实际使用时长计费，不限流量。 您购买共享带宽时可以指定带宽大小，后续支持修改。使用过程中，您实际的带宽不能高于指定带宽大小。

14.2.3 如何切换计费方式中的“按需计费（按带宽计费）”和“按需计费（按流量计费）”？

表 14-3 弹性 IP 计费方式变更说明

计费方式变更场景	计费变更说明
按需计费（按流量计费）→按需计费（按带宽计费）	按需计费（按流量计费）EIP支持直接转为按需计费（按带宽计费）EIP。 该变更操作成功后，新的计费方式将立即生效。
按需计费（按带宽计费）→按需计费（按流量计费）	按需计费（按带宽计费）EIP支持直接转为按需计费（按流量计费）EIP。 该变更操作成功后，新的计费方式将立即生效。

按需计费（按流量计费）计费和按需计费（按带宽计费）互相转换

1. 登录管理控制台。
2. 在页面左上角单击 ☰ 图标，打开服务列表，选择“网络 > 弹性IP”
3. 在弹性IP列表中，在待修改弹性IP所在行的“操作”列，选择“更多 ”> “修改带宽” 。
4. 在“修改带宽”页面，根据界面提示修改计费方式。

   该界面还支持修改带宽名称和带宽大小。
5. 修改完成后，单击“下一步”。
6. 在规格确认页面，单击“提交”，完成修改。

说明

- 变更计费方式不会更换EIP的地址，也不会中断EIP的使用，对您的业务不会产生影响。

14.2.4 为什么虚拟私有云 VPC 删除之后，仍在继续计费?

问题现象

您已将账户下的虚拟私有云VPC资源全部删除，但查看费用账单时，显示虚拟私有云VPC仍在继续计费。

原因说明

VPC本身不收取费用，虚拟私有云的计费项主要为使用弹性IP时产生的费用。

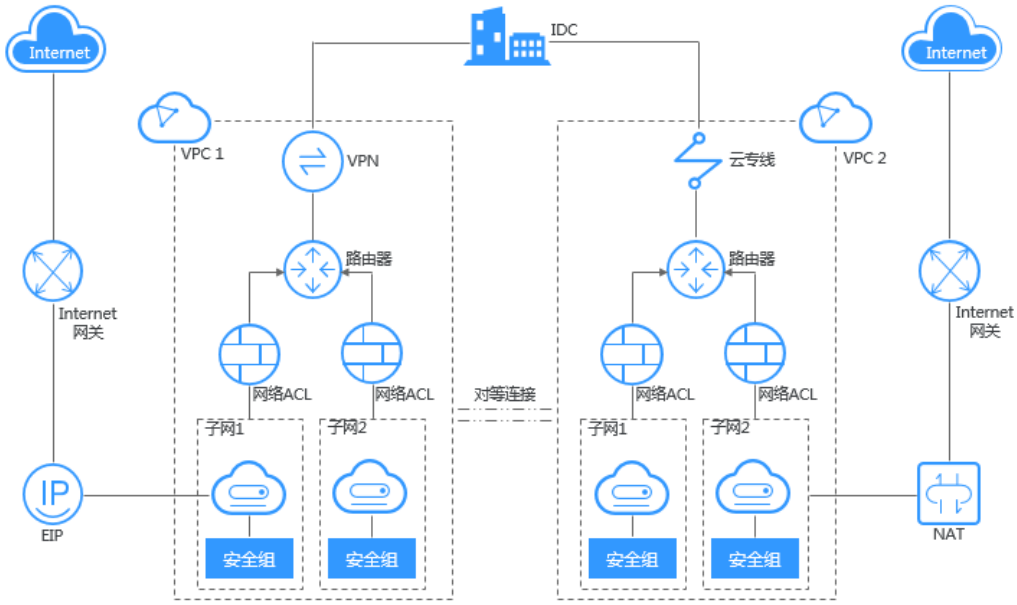
- 在其他项目或者区域还存在弹性IP资源，可在费用中心查看所有弹性IP资源，定位到资源后切换项目或区域进行删除。
- 存在延迟计费情况，一般按需计费的弹性IP资源删除后并不会立即对之前的消费进行扣款，在结算周期结束后，才会生成账单并执行扣款。

14.3 虚拟私有云与子网类

14.3.1 什么是虚拟私有云?

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 14-2 产品架构



14.3.2 VPC 中可以使用哪些网段（CIDR）?

您可以在特定的私有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。

VPC支持的网段范围如**表14-4**所示。

表 14-4 VPC 网段

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

14.3.3 子网间是否可以通信?

- 同一个VPC内的子网网络默认互通。
- 不同VPC的网络不互通，因此不同VPC内的子网也不互通，您可以通过对等连接实现同区域，不同VPC之间的通信。

说明

若子网关联了网络ACL，需先放通网络ACL。

14.3.4 子网可以使用的网段是什么?

子网是从VPC中划分的IP地址块，VPC可用的私网网段包括：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。

14.3.5 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?** 。

14.3.6 虚拟私有云和子网无法删除，如何处理?

虚拟私有云和子网通常由于被其他服务资源使用而导致无法删除，需要您根据控制台的提示信息，删除占用虚拟私有云和子网的资源，然后才可以删除虚拟私有云和子网。本文档为您提供详细的删除提示信息说明及对应的删除指导，具体如下：

- **删除子网**
- **删除虚拟私有云**

删除子网

删除子网时候，您可以参考**表14-5**，对照管理控制台的提示信息，根据对应的解决办法处理。

表 14-5 子网删除方法

提示信息	原因	处理方法
您的权限不足	您的账号没有删除子网的权限。	请您联系账号管理员为您的账号授权后，重新尝试删除虚拟私有云。
子网被自定义路由所使用，请先在路由表删除相应自定义路由再删除子网。	子网关联的路由表中，存在下一跳可能是以下类型的自定义路由： • 服务器实例 • 扩展网卡 • 虚拟IP • NAT网关	请您在子网关联的路由表中，删除自定义路由后，重新尝试删除子网。 1. 查看子网关联路由表的方法，请参见**查看子网关联的路由表**。 2. 删除自定义路由的方法，请参见**删除路由**。

提示信息	原因	处理方法
子网下仍有虚拟IP，请先在子网详情页面删除虚拟IP地址再删除子网。	子网内存在虚拟IP地址。	请您删除子网内的虚拟IP地址后，重新尝试删除子网。 删除方法，请参见**删除虚拟IP地址**。
子网被私有IP地址使用，请先在子网页面删除私有IP地址再删除子网。	子网内的私有IP地址已被占用，但是当前IP地址并未被实例使用。	请您在子网“IP地址管理”页签中，查看IP地址的用途，由于这些被占用的IP并未被实例使用，您可以直接删除，释放该私有IP地址后，重新尝试删除子网。 1. 查看子网内IP地址用途的方法，请参见**查看子网内IP地址的用途**。 2. 在私有IP地址列表中，对于未被使用的IP地址，单击操作列下的“删除”。 **须知** 已被使用的私有IP地址，不允许在私有IP列表直接删除，需要删除对应的云服务资源，请删除子网时，根据提示继续排查。
子网被计算资源使用，不能删除。	子网已被弹性云服务器ECS或者弹性负载均衡ELB使用。	请您删除使用子网的弹性云服务器ECS或者弹性负载均衡ELB后，重新尝试删除子网。 删除方法，请参见**查看并删除子网内的云服务资源**。
子网被负载均衡器使用，不能删除。	子网已被弹性负载均衡ELB使用。	请您删除使用子网的弹性负载均衡ELB后，重新尝试删除子网。 删除方法，请参见**查看并删除子网内的云服务资源**。
子网被NAT网关使用，不能删除。	子网已被NAT网关使用。	请您删除使用子网的NAT网关后，重新尝试删除子网。 删除方法，请参见**查看并删除子网内的云服务资源**。
子网正在使用中，不能删除。	子网已被其他云服务资源占用。	请您在子网“IP地址管理页签”中，查看IP地址的用途，根据IP地址的用途找到对应服务资源进行删除后，重新尝试删除子网。 1. 查看子网内IP地址用途的方法，请参见**查看子网内IP地址的用途**。 2. 根据IP地址的用途，查找对应的云服务资源。 3. 找到目标资源后，删除使用子网的资源，然后重新尝试删除子网。

删除虚拟私有云

删除虚拟私有云之前，需要确保已经删除完虚拟私有云内子网，您可以参考**表14-6**，对照管理控制台的提示信息，找到对应的解决办法处理。

表 14-6 虚拟私有云删除方法

提示信息	原因	处理方法
您的权限不足	您的账号没有删除虚拟私有云的权限。	请您联系账号管理员为您的账号授权后，重新尝试删除虚拟私有云。
VPC内存在路由，请删除路由或者占用该VPC终端节点服务，然后重试。	虚拟私有云的路由表中存在自定义路由。	请您删除路由表中的自定义路由后，重新尝试删除虚拟私有云。 1. 在虚拟私有云列表中，单击“路由表”列对应的数字超链接。 进入路由表列表页面。 2. 删除自定义路由的方法，请参见**删除路由**。
	虚拟私有云已被终端节点服务使用。	您需要在终端节点服务控制台中，查找目标终端节点服务并删除。
“暂不能对VPC执行删除操作”弹窗。	虚拟私有云已被以下资源使用： • 子网 • 对等连接 • 自定义路由表	请您根据弹窗中的提示，单击资源名称超链接，查看对应的资源。并参考以下方法进行删除： • **删除子网** • **删除对等连接** • **删除路由表**
VPC包含云专线的虚拟网关，请先删除虚拟网关后重试。	虚拟私有云已被云专线DC的虚拟网关使用。	您需要在云专线控制台中，查找目标虚拟网关并删除。
VPC包含VPN网关，请先删除VPN网关后重试。	虚拟私有云已被VPN网关使用。	您需要在虚拟专用网络控制台中，查找目标VPN网关并删除。
删除最后一个VPC时，请先删除安全组。	当您删除某个区域内的最后一个虚拟私有云时，需要先删除本区域内所有的自定义安全组。 **须知** 此处仅需要删除自定义安全组。名称为default的默认安全组不影响虚拟私有云的删除。	您需要在安全组列表中，删除所有的自定义安全组后，尝试重新删除虚拟私有云。 删除方法，请参见**删除安全组**。

提示信息	原因	处理方法
删除最后一个VPC时，请先删除公网IP。	当您删除某个区域内的最后一个虚拟私有云时，需要先释放本区域内所有的弹性IP地址。	您需要在弹性IP列表中，释放所有的弹性IP后，尝试重新删除虚拟私有云。 释放方法，请参见**解绑定和释放弹性云服务器的弹性IP**。

14.3.7 弹性云服务器是否支持切换虚拟私有云?

支持。

您可以在弹性云服务器界面的操作列单击“切换VPC”进行切换。

具体注意事项及操作步骤请参考《虚拟私有云用户指南》的“切换虚拟私有云”章节。

14.4 弹性 IP 类

14.4.1 弹性 IP、私有 IP 和虚拟 IP 之间有何区别?

云上不同IP地址实现的功能不同，**图14-3**展示了IP地址架构图，关于IP的详细介绍请参见**表14-7**。

图 14-3 IP 地址架构图

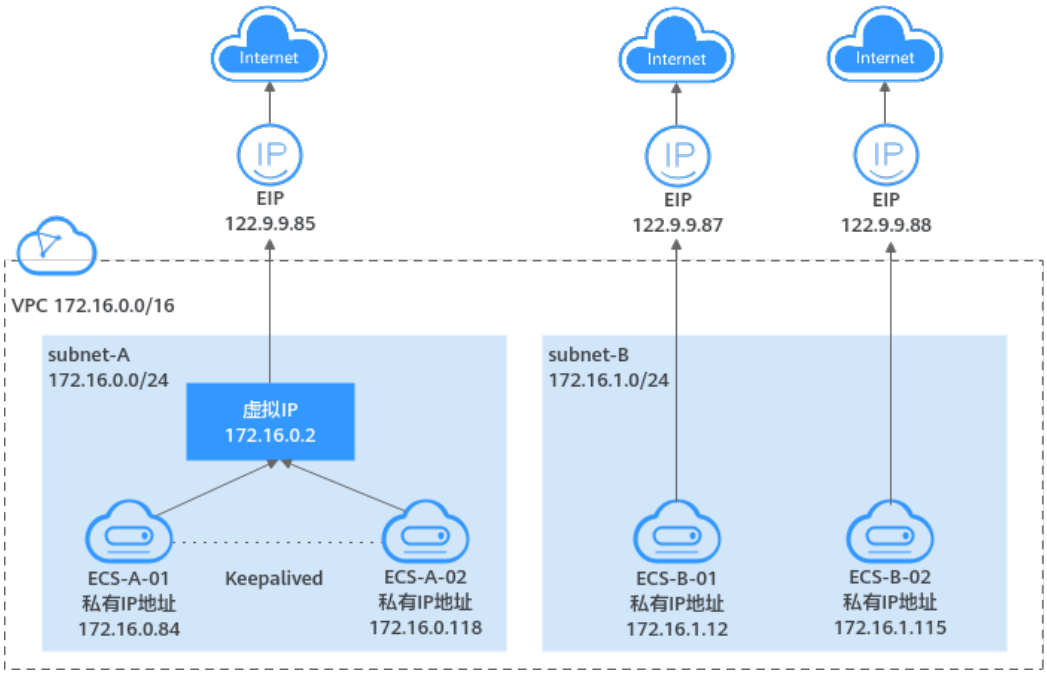


表 14-7 不同 IP 地址功能说明

IP地址分类	IP地址说明	示例
私有IP	您在VPC子网内创建弹性云服务器时，系统会基于子网内的可用IP地址，给弹性云服务器分配私有IP地址，私有IP地址主要用于云内网络通信，不能访问Internet。	• ECS-A-01的私有IP地址为172.16.0.84 • ECS-B-01的私有IP地址为172.16.1.12
虚拟IP	虚拟IP是一个未分配给真实弹性云服务器网卡的IP地址，可同时绑定至多台弹性云服务器上。虚拟IP结合keepalived，可以在主弹性云服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备弹性云服务器，继续对外提供服务，以此达到高可用性HA（High Availability）的目的。	虚拟IP（172.16.0.2）同时绑定至ECS-A-01和ECS-A-02，结合keepalived可实现ECS-A-01和ECS-A-02的主备倒换。
弹性IP	弹性IP是云上资源访问Internet使用的IP地址。 • 在虚拟IP场景，您可以将弹性IP绑定至虚拟IP，实现虚拟IP后端的弹性云服务器访问Internet。 • 您可以将弹性IP直接绑定至弹性云服务器上，实现弹性云服务器访问Internet，一个弹性IP只能绑定至一台弹性云服务器。	• 将EIP（122.9.9.85）绑定至虚拟IP（172.16.0.2），实现ECS-A-01和ECS-A-02访问Internet。 • 将EIP（122.9.9.87）绑定至ECS-B-01，实现ECS-B-01访问Internet。

14.4.2 如何通过扩展网卡绑定的弹性 IP 访问公网?

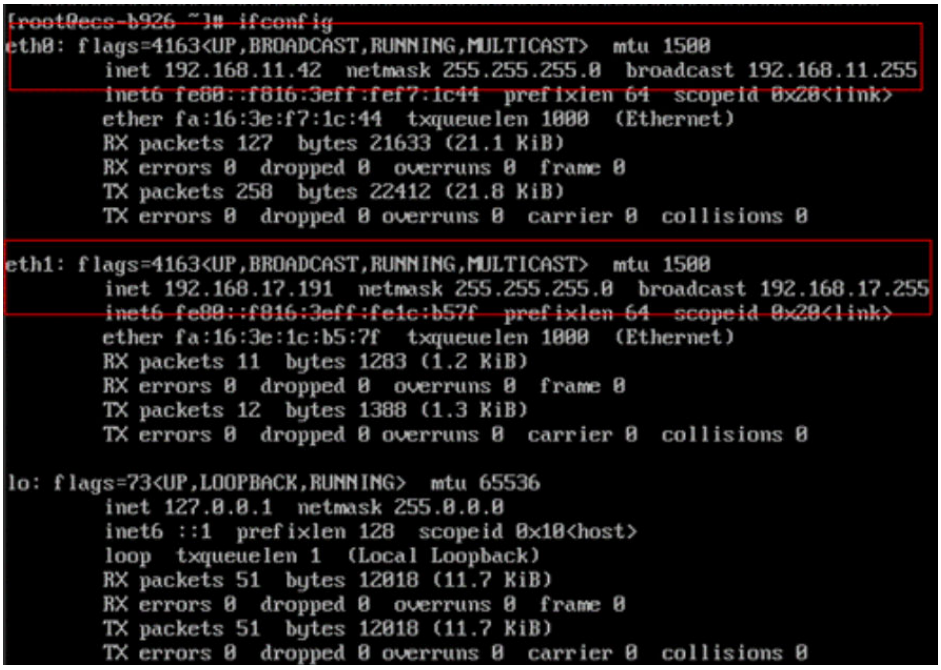
1. 弹性IP绑定扩展网卡后，进入弹性云服务器，执行**route**命令查询路由。
   route命令如果不清楚可以使用**route --help**。

   图 14-4 查看路由信息

   ```
   [root@ecs-b926 ~]# route -n
   Kernel IP routing table
   Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
   0.0.0.0         192.168.11.1    0.0.0.0         UG    0      0        0 eth0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
   169.254.0.0     0.0.0.0         255.255.0.0     U     1003   0        0 eth1
   169.254.169.254 192.168.11.1    255.255.255.255 UGH   0      0        0 eth0
   192.168.11.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
   192.168.17.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
   [root@ecs-b926 ~]#
   ```

2. 执行**ifconfig**命令查看网卡信息。

图 14-5 查看网卡信息



3. 配置默认通过扩展网卡访问公网。
   a. 执行如下命令，删除主网卡默认路由。

      route del -net 0.0.0.0 gw 192.168.11.1 dev eth0

      参数说明：192.168.11.1是网卡所在子网的网关，可以通过管理控制台，在子网的“基本信息”页签内查看网关地址。

      说明

      此操作会导致虚拟机流量中断，请谨慎操作，推荐您参考步骤4配置。

   b. 执行如下命令，配置扩展网卡默认路由。

      route add default gw 192.168.17.1

4. 按照访问的目标地址配置扩展网卡访问。

   配置通过扩展网卡访问某一网段（xx.xx.0.0/16，该网段请按实际情况设置）：

   route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1

14.4.3 弹性云服务器的主网卡和扩展网卡在使用上有什么区别?

两者主要有以下区别：

- 一般操作系统的默认路由优先使用主网卡，如果出现使用扩展网卡导致网络不通现象通常是路由配置问题。
- 默认主网卡具备与云公共服务区（PaaS、DNS等服务所在区域）互通能力，扩展网卡不具备该能力。

14.4.4 弹性 IP 使用独享带宽进行限速过后能否变更为使用共享带宽进行限速?

可以。弹性IP可以从独享带宽变更为共享带宽使用。

14.4.5 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。

14.4.6 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通过公网可以访问的服务，并且明确访问该服务的对端IP地址时，建议将安全组规则的源地址设置为包含该IP地址的网段。
- 当弹性云服务器需要提供由公网可以访问的服务，并且不明确访问该服务的对端IP地址时，建议将安全组规则的源地址设置成默认网段0.0.0.0/0，再通过配置端口提高网络安全性。

  源地址设置成默认网段0.0.0.0/0，表示允许所有IP地址访问安全组内的弹性云服务器。
- 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。

14.4.7 弹性 IP 是否支持变更绑定的弹性云服务器?

支持。

您可以先将弹性IP从原弹性云服务器解绑，如何解绑请参考**解绑定和释放弹性云服务器的弹性IP**.。

再将弹性IP绑定到目标弹性云服务器，如何绑定请参考**为弹性云服务器申请和绑定弹性IP**。

14.4.8 如何为实例解绑已有弹性 IP，绑定新的弹性 IP?

场景一：为弹性云服务器解绑已有 EIP，并绑定新的 EIP

1. 解绑已有弹性IP。
   a. 登录管理控制台。
   b. 在系统首页，选择“网络 > 弹性IP”。
   c. 在弹性IP界面待解绑定弹性IP地址所在行，单击“解绑”。
   d. 单击“是”。
2. 申请新的弹性IP。

   说明

   当您已有需要绑定的EIP时，请忽略此步骤。

   a. 登录管理控制台。
   b. 在系统首页，选择“网络 > 弹性IP”。
   c. 在“弹性IP”界面，单击“创建弹性IP”。
   d. 根据界面提示配置参数。
   e. 单击“立即购买”。

3. 绑定新申请的弹性IP。
   a. 登录管理控制台。
   b. 在系统首页，选择“网络 > 弹性IP”。
   c. 在“弹性IP”界面待绑定弹性IP地址所在行，单击“绑定”。
   d. 选择实例。
   e. 单击“确定”。
4. 释放已被解绑的弹性IP。

   说明

   当已被解绑的EIP不再使用时，您可以释放EIP。

   a. 登录管理控制台。
   b. 在系统首页，选择“网络 > 弹性IP”。
   c. 在“弹性IP”界面待释放弹性IP地址所在行，单击“更多 > 释放”。
   d. 单击“是”。

场景二：为弹性负载均衡解绑已有 EIP，并绑定新的 EIP

1. 解绑已有弹性IP。
   a. 登录管理控制台。
   b. 选择“服务列表 > 网络 > 弹性负载均衡”。
   c. 在“负载均衡器”界面，所需修改负载均衡器所在行，选择“更多 > 解绑弹性IP”。
   d. 单击“是”。
2. 申请新的弹性IP，请参考**2**。

   说明

   当您已有需要绑定的EIP时，请忽略此步骤。
3. 弹性负载均衡绑定新申请的弹性IP。
   a. 登录管理控制台。
   b. 选择“服务列表 > 网络 > 弹性负载均衡”。
   c. 在“负载均衡器”界面，所需修改负载均衡器所在行，选择“更多 > 绑定弹性IP”。
   d. 在“绑定弹性IP”弹框中，选择需要绑定EIP，单击“确定”。
4. 释放已被替换的EIP，请参考**4**。

   说明

   当已被解绑的EIP不再使用时，您可以释放EIP。

场景三：为 NAT 网关解绑已有 EIP，并绑定新的 EIP

1. 申请新的弹性IP，请参考**2**。

   说明

   当您已有需要绑定的EIP时，请忽略此步骤。

2. 修改SNAT规则。

   修改SNAT规则请参考《 NAT网关用户指南 》公网NAT网关中的“修改SNAT规则”章节，在弹性IP列表中勾选新申请的弹性IP，取消已有弹性IP。

3. 修改DNAT规则。

   修改DNAT规则请参考《 NAT网关用户指南 》公网NAT网关中的“修改DNAT规则”章节，在“弹性IP”中重新选择为新申请的弹性IP。

4. 释放已被替换的EIP，请参考4。

   说明

   当已被解绑的EIP不再使用时，您可以释放EIP。

14.4.9 弹性 IP 是否支持跨区域绑定?

弹性IP不支持跨区域绑定，弹性IP和云资源必须在同一个区域。

14.4.10 弹性 IP 是否支持切换区域?

弹性IP不支持切换区域。

例如：在区域A申请弹性IP，当区域B需要弹性IP时，不能直接将区域A的弹性IP直接切换到区域B，需要在区域B重新申请弹性IP。

14.5 对等连接类

14.5.1 一个账户可以创建多少个对等连接?

通过对等连接连通同一个区域VPC时，您可以登录控制台查询配额详情，具体请参见**怎样查看我的配额?** 。

- 相同账户的VPC对等连接：在一个区域内，您可以创建VPC对等连接数量，以实际配额为准。
- 不同账户的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账户内的配额。处于待接受状态的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账户下的VPC对等连接，比如账号A和账号B的VPC对等连接，账号A和账号C的VPC对等连接，账号A和账号D的VPC对等连接等，不受账号数量限制。

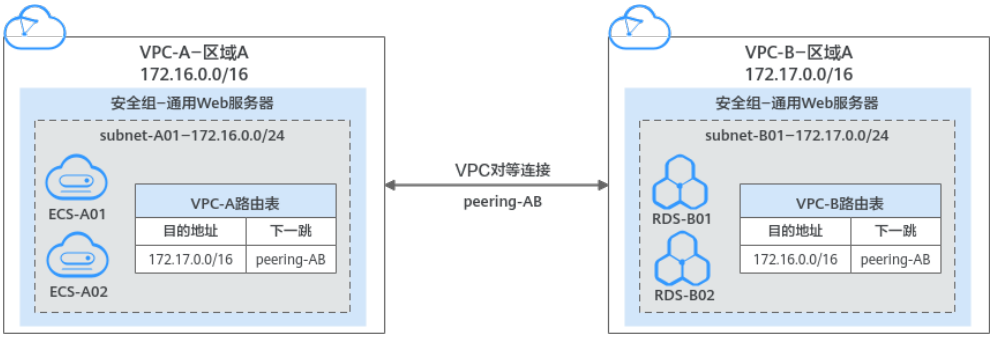
14.5.2 对等连接是否可以连通不同区域的 VPC?

VPC对等连接是用来连接相同区域的VPC，不支持连通不同区域的VPC。

接下来，通过**图14-6**中简单的组网示例，为您介绍对等连接的使用场景。

- 在区域A内，您的两个VPC分别为VPC-A和VPC-B，VPC-A和VPC-B之间网络不通。
- 您的业务服务器ECS-A01和ECS-A02位于VPC-A内，数据库服务器RDS-B01和RDS-B02位于VPC-B内，此时业务服务器和数据库服务器网络不通。
- 您需要在VPC-A和VPC-B之间建立对等连接Peering-AB，连通VPC-A和VPC-B之间的网络，业务服务器就可以访问数据库服务器。

图 14-6 对等连接组网示意图



14.5.3 为什么对等连接创建完成后不能互通?

问题描述

对等连接创建完成后，本端VPC和对端VPC网络不互通。

排查思路

问题排查思路请参见**表14-8**，以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

表 14-8 排查思路-对等连接不通

序号	可能原因	处理措施
1	对等连接中本端VPC和对端VPC网段重叠 ● VPC网段重叠，且全部子网重叠。 ● VPC网段重叠，且部分子网重叠。	当对等连接中本端VPC和对端VPC网段重叠时，对等连接可能不生效，处理方法请参见**对等连接中本端VPC和对端VPC网段重叠**。
2	对等连接路由配置错误 ● 没有在本端VPC和对端VPC内配置对等连接路由。 ● 对等连接路由地址配置错误。 ● 对于云上和云下互通的组网，检查对等连接路由是否和云专线、VPN路由的目的地址重叠。	当对等连接的路由配置错误时，会导致对等连接的网络流量无法正确送到目的地址，处理方法请参见**对等连接路由配置错误**。

序号	可能原因	处理措施
3	网络配置错误 • 检查需要通信的ECS安全组规则是否配置正确。 • 检查弹性云服务器网卡的防火墙配置。 • 检查对等连接连通的子网网络ACL规则是否配置正确。 • 对于多网卡的弹性云服务器，检查弹性云服务器内部的策略路由配置。	请参见**网络配置错误**。
4	弹性云服务器基本网络功能异常	请参见**弹性云服务器基本网络功能异常**。

对等连接中本端 VPC 和对端 VPC 网段重叠

VPC网段重叠的情况下，容易因为路由冲突导致对等连接不生效，具体如**表14-9**所示。

表 14-9 对等连接中本端 VPC 和对端 VPC 网段重叠

场景说明	场景示例	解决方法
VPC网段重叠，且全部子网重叠	组网图如**图14-7**所示，VPC-A和VPC-B网段重叠，且全部子网重叠。 • VPC-A和VPC-B的网段重叠，均为10.0.0.0/16。 • VPC-A中的子网Subnet-A01和VPC-B中的子网Subnet-B01网段重叠，均为10.0.0.0/24。 • VPC-A中的子网Subnet-A02和VPC-B中的子网Subnet-B02网段重叠，均为10.0.1.0/24。	不支持使用VPC对等连接。 本示例中，VPC-A和VPC-B无法使用对等连接连通，请重新规划网络。

场景说明	场景示例	解决方法
VPC网段重叠，且部分子网重叠	组网图如图14-8所示，VPC-A和VPC-B网段重叠，且部分子网重叠。 • VPC-A和VPC-B的网段重叠，均为10.0.0.0/16。 • VPC-A中的子网Subnet-A01和VPC-B中的子网Subnet-B01网段重叠，均为10.0.0.0/24。 • VPC-A中的子网Subnet-A02和VPC-B中的子网Subnet-B02网段不重叠。	• 无法创建指向整个VPC网段的对等连接。本示例中，对等连接无法连通VPC-A和VPC-B之间的全部网络。 • 可以创建指向子网的对等连接，对等连接两端的子网网段不能包含重叠子网。本示例中，对等连接可以连通子网Subnet-A02和Subnet-B02之间的网络，详细的配置方法请参见图14-9。

图 14-7 VPC 网段重叠，且全部子网重叠(IPv4)

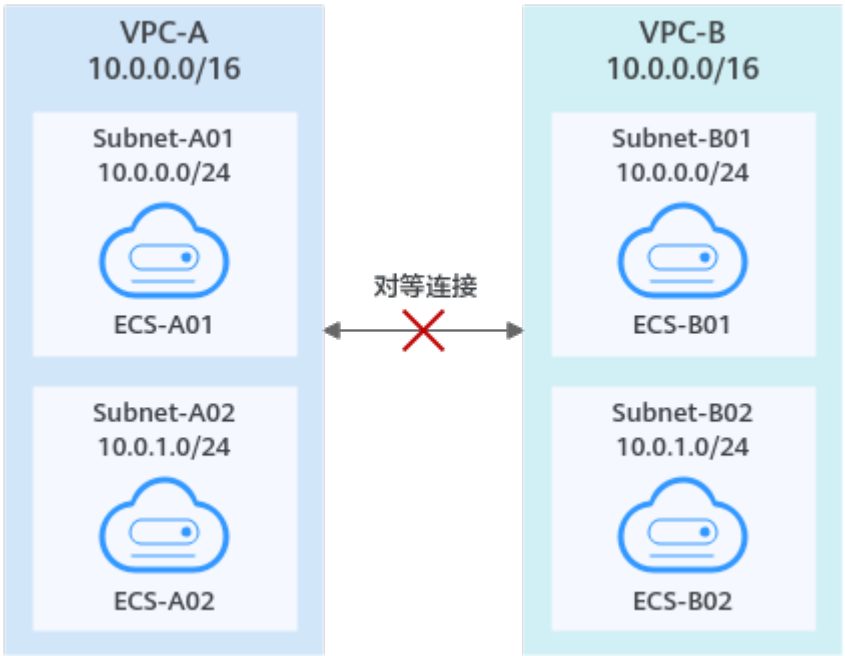
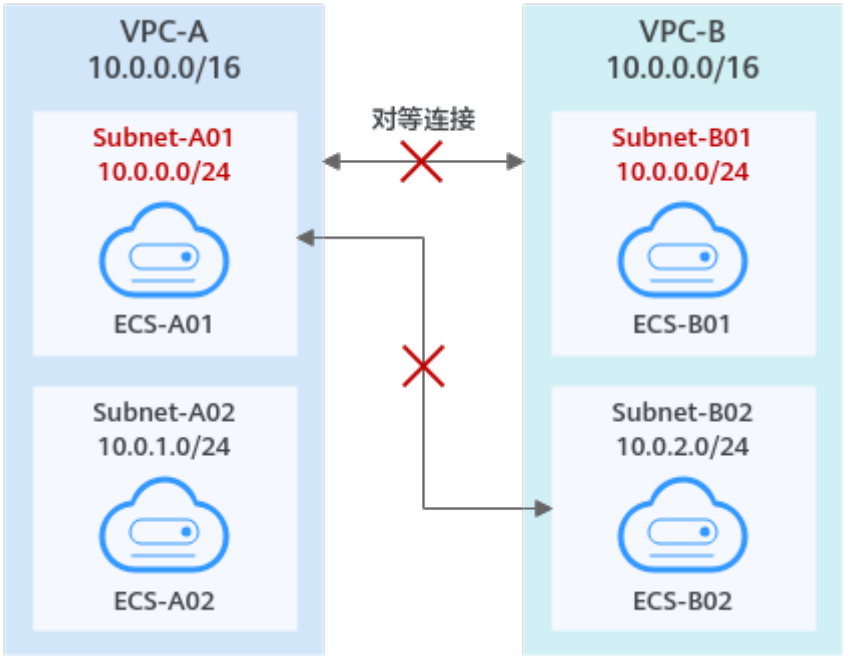


图 14-8 VPC 网段重叠，且部分子网重叠(IPv4)



当VPC网段重叠，且部分子网重叠，您可以在网段不重叠的子网之间建立对等连接。本示例为创建Subnet-A02和Subnet-B02之间的对等连接，组网图如图14-9所示，路由添加方法请参见表14-10。

图 14-9 VPC 网段重叠，部分子网重叠(IPv4)-正确配置

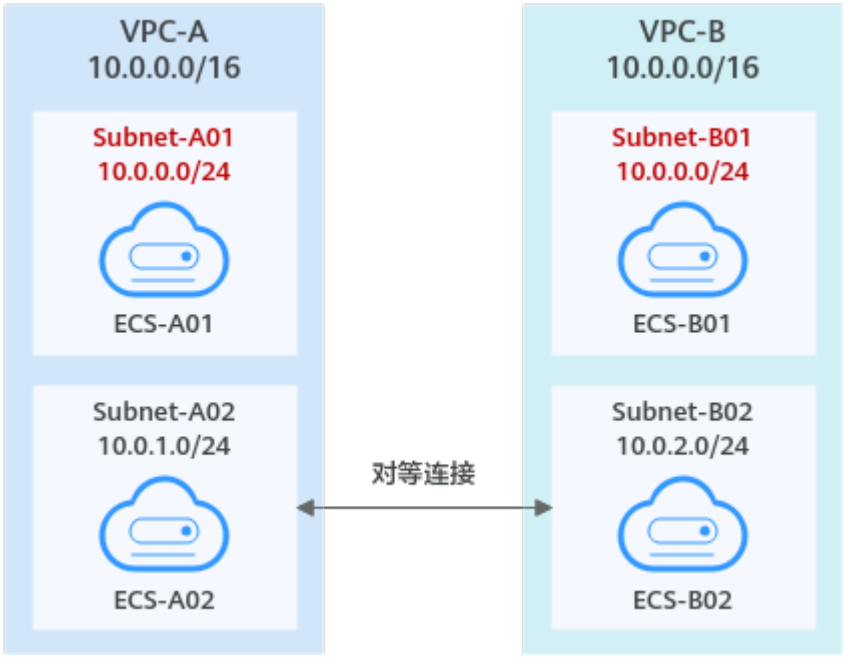


表 14-10 Subnet-A02 和 Subnet-B02 之间的对等连接

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

对等连接路由配置错误

对等连接创建完成后，请参考**查看对等连接路由**，在本端VPC和对端VPC的路由表中检查路由添加情况，检查项目如**表14-11**。

表 14-11 对等连接路由配置检查项

路由配置检查项	处理方法
在本端VPC和对端VPC的路由表中，检查是否添加路由。	如果您未添加路由，请参考以下章节中的添加路由步骤： ● **创建相同账户下的对等连接**
检查对等连接路由地址配置是否正确。 ● 在本端VPC内，检查路由的目的地址是否为对端VPC的网段，子网网段或者相关的私有IP地址。 ● 在对端VPC内，检查路由的目的地址是否为本端VPC的网段，子网网段或者相关的私有IP地址。	如果路由目的地址配置错误，请参考**修改对等连接路由**修改路由地址。
对于云上和云下互通的组网，检查对等连接路由是否和云专线、VPN路由的目的地址重叠。	查看对等连接两端的VPC下是否有VPN/云专线资源，排查路由规则的下一跳目的地址是否有重叠。 如果路由目的地址重叠，该对等连接不生效，请重新规划网络连接方案。

网络配置错误

1. 检查需要通信的云服务器的安全组规则是否配置正确，具体方法请参见**查看弹性云服务器的安全组**。
   - 如果您需要通信的云服务器位于同一个安全组内，则此项无需检查。
   - 如果您需要连通的云服务器位于不同的安全组内，那么您需要在安全组的入方向规则中，添加放通对端安全组的规则，具体方法请参见**安全组配置示例**

2. 检查云服务器网卡的防火墙配置。

   需要确认防火墙不会拦截流量，否则需要放通防火墙规则。

3. 检查对等连接连通的子网网络ACL规则是否配置正确。

   确认对等连接涉及的子网流量未被网络ACL拦截，否则需要放通对等连接涉及的网络ACL规则。

4. 对于多网卡的云服务器，检查云服务器内部的策略路由配置，确保源IP不同的报文匹配各自的路由，从各自所在的网卡发出。

   假设云服务器有两个网卡为eth0和eth1：

   - eth0的IP地址为192.168.1.10，所在子网的网关为192.168.1.1
   - eth1的IP地址为192.168.2.10，所在子网的网关为192.168.2.1

   分别执行以下命令：

   - **ping -I** *eth0的IP地址 eth0所在子网的网关地址*
   - **ping -I** *eth1的IP地址 eth1所在子网的网关地址*

   命令示例：

   - **ping -I 192.168.1.10 192.168.1.1**
   - **ping -I 192.168.2.10 192.168.2.1**

   如果网络通信情况正常，说明服务的多个网卡路由配置正常。

   否则需要为配置了多网卡的云服务器配置策略路由，具体请参见**如何配置多网卡弹性云服务器的策略路由?**

弹性云服务器基本网络功能异常

1. 登录云服务器。
2. 检查弹性云服务器网卡是否已经正确分配到IP地址。
   - Linux云服务器：执行命令**ifconfig**或**ip address**查看网卡的IP信息。
   - Windows云服务器：在搜索区域输入**cmd**并按**Enter**，打开命令输入框，执行命令**ipconfig**查看。

   若未能分配到IP地址，处理方法请参见。
3. 检查云服务器所在子网的网关是否可以ping通，即确认基本通信功能是否正常。
   a. 在弹性云服务器列表中，单击云服务器名称超链接。

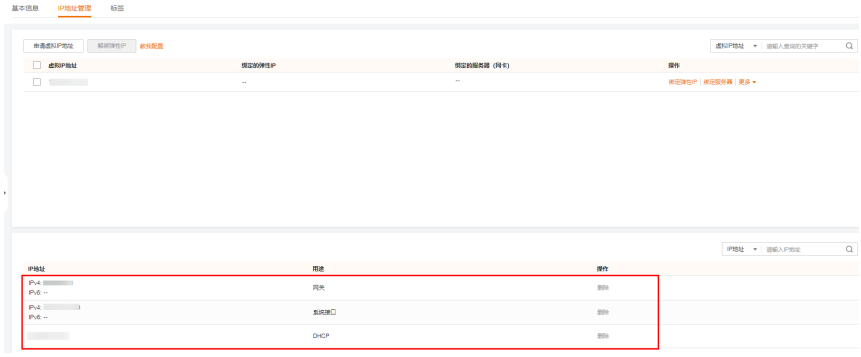
      进入云服务器详情页。
   b. 在云服务器详情页，单击虚拟有云超链接。

      进入虚拟私有云列表。
   c. 在虚拟私有云列表，单击虚拟私有云对应的“子网个数”超链接。

      进入子网列表。
   d. 在子网列表，单击子网名称超链接。

      进入子网详情页。
   e. 选择“IP地址管理”页签，查看子网的网关地址。

图 14-10 查看子网网关



f. 执行以下命令，检查网关通信是否正常。

ping *子网网关地址*

命令示例：**ping 172.17.0.1**

14.6 虚拟 IP 类

14.6.1 弹性云服务器的网卡绑定虚拟 IP 地址后，该虚拟 IP 地址无法 ping 通时，如何排查?

问题描述

ECS的网卡绑定虚拟IP地址后，该虚拟IP地址无法ping通。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-11 排查思路

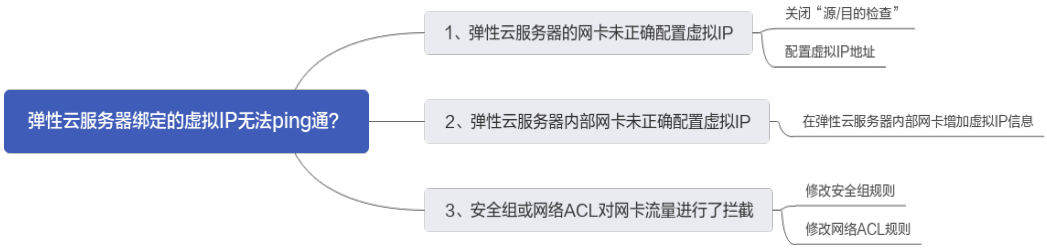


表 14-12 排查思路

可能原因	处理措施
弹性云服务器的网卡未正确配置虚拟IP	解决方法请参考**弹性云服务器的网卡未正确配置虚拟IP**。

可能原因	处理措施
弹性云服务器内部网卡未正确配置虚拟IP	解决方法请参考**弹性云服务器内部网卡未正确配置虚拟IP**。
安全组或网络ACL对网卡流量进行了拦截	解决方法请参考**安全组或网络ACL对网卡流量进行了拦截**。

弹性云服务器的网卡未正确配置虚拟 IP

查看该网卡的“源/目的检查”是否关闭，虚拟IP是否已经绑定网卡。

1. 登录管理控制台。
2. 选择“服务列表 > 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. 在弹性云服务器详情页面，单击“弹性网卡”页签。
5. 确认网卡详情中“源/目的检查”选项已设置“关闭”。
6. 确保网卡详情中的虚拟IP地址不为空。

   如果虚拟IP地址为空，单击“管理虚拟IP地址”，跳转至“IP地址管理”界面中，单击“申请虚拟IP地址”。

说明

通过此种方式，即网卡直接绑定虚拟IP的方式，不能使用**ifconfig**命令查看是否已经完成虚拟IP地址的配置，您可以使用**ip address**命令查看是否已经完成虚拟IP地址的配置。更多信息请参考。

弹性云服务器内部网卡未正确配置虚拟 IP

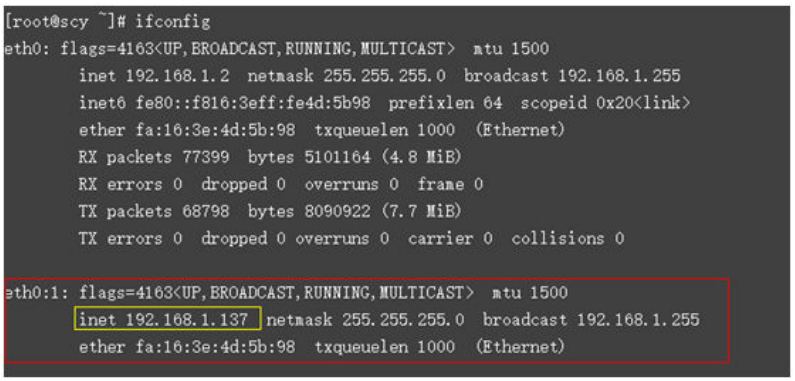
本文以Linux系统和Windows系统为例，指导您如何查看弹性云服务器内部网卡是否正确配置了虚拟IP地址。

Linux系统

1. 在弹性云服务器上执行以下命令，确认是否存在ethX:X类型的网卡。

   ifconfig

图 14-12 查看是否存在 ethX:X 类型的网卡



上图回显样例中包含ethX:X类型的网卡，样例中192.168.1.137为ECS网卡需要配置的虚拟IP地址。

- 是，弹性云服务器内部网卡子接口正常创建。
- 否，请执行如下步骤。

2. 回显中不存在ethX:X类型的网卡，请执行以下命令进入“/etc/sysconfig/network-scripts”目录。

   cd /etc/sysconfig/network-scripts

3. 执行以下命令新建并修改“ifcfg-eth0:1”文件。

   vi ifcfg-eth0:1

   在文件中增加以下网卡信息。

```
BOOTPROTO=static
DEVICE=eth0:1
HWADDR=fa:16:3e:4d:5b:98
IPADDR=192.168.1.137
GATEWAY=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
ONPARENT=yes
```

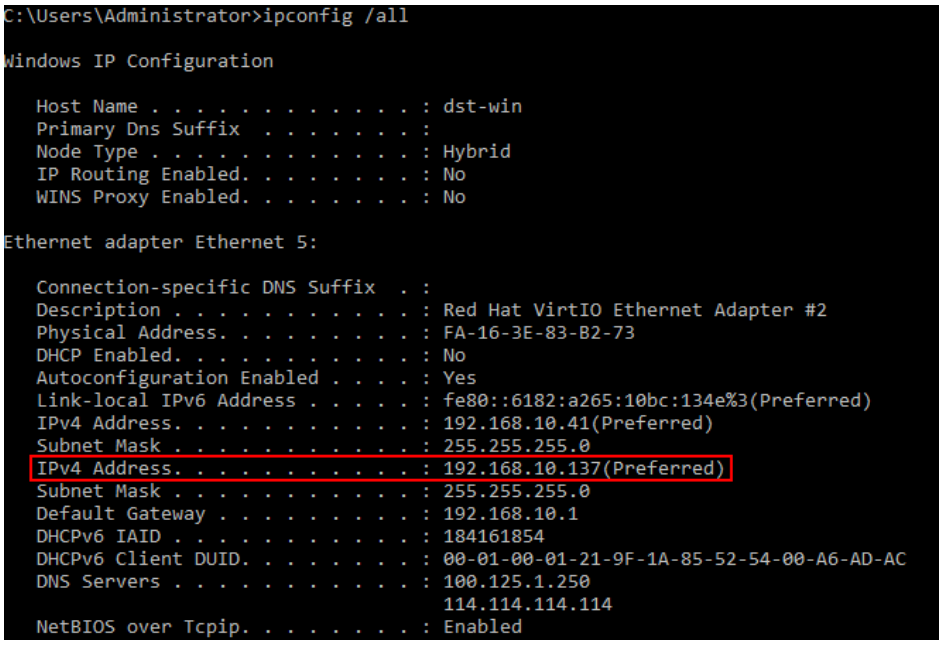
4. 按“**Esc**”输入“**:wq!**”，保存后退出文件。
5. 重启弹性云服务器，使用**ifconfig**命令再次查看是否已经完成虚拟IP地址的配置。

Windows系统

1. 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

   图 14-13 查看是否配置虚拟 IP 地址



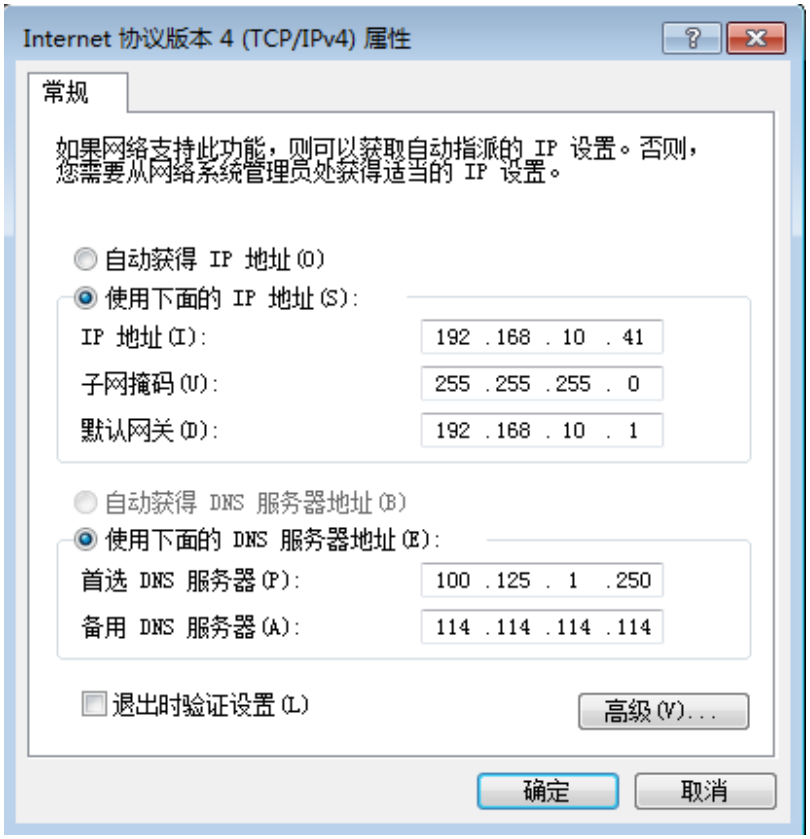
上图回显样例中IPv4 Address包含ECS网卡需要配置的虚拟IP地址192.168.10.137。

- 是，弹性云服务器内部网卡的虚拟IP地址配置正常。

- 否，请执行如下步骤。

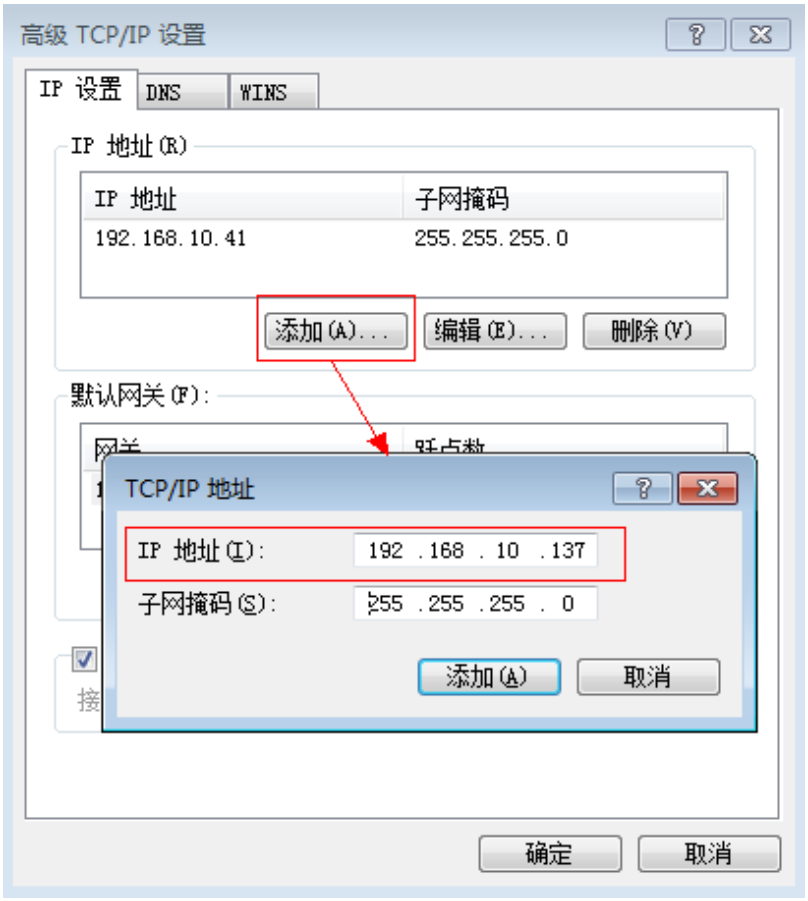
2. 在“控制面板 > 网络和Internet > 网络连接”路径下，右键单击对应的本地连接，选择“属性”。
3. 在“网络”页签内选择“Internet 协议版本 4 （TCP/IPv4）”。
4. 单击“属性”。
5. 选择“使用下面的IP地址”，IP地址配置为图14-13中显示的私有IP地址，例如：192.168.10.41。

图 14-14 配置私有 IP 地址



6. 单击“高级”。
7. 在“IP设置”页签内“IP地址”区域，单击“添加”。
   添加图14-13中的虚拟IP地址，例如：192.168.10.137。

图 14-15 配置虚拟 IP 地址



安全组或网络 ACL 对网卡流量进行了拦截

查看弹性云服务器的安全组以及网卡所在子网的ACL规则是否会对流量进行拦截。

1. 在弹性云服务器详情页面，单击“安全组”页签，确认安全组规则已经设置了虚拟IP的访问规则。如果没有，请单击“更改安全组”或“更改安全组规则”设置规则。
2. 选择“服务列表 > 网络 > 虚拟私有云 > 网络ACL”，查看网卡所在的子网的ACL规则是否拦截虚拟IP地址访问。

14.6.2 虚拟 IP 搭建的高可用集群执行服务器主备倒换后网络不通，如何处理?

对于虚拟IP和Keepalived搭建的高可用集群，当服务器进行主备倒换后，如果您发现Client端（客户端）到Server端（服务器端）网络不通，那么可能是因为您人工切换主备服务器，导致Client端的ARP表没有更新，您可以执行以下操作更新ARP表。

1. 登录Client端的服务器。
2. 执行以下步骤，尝试触发Client端ARP表的更新。
   - 方法一：执行以下命令，ping虚拟IP地址，触发Client端学习虚拟IP对应的新MAC地址。

     ping *虚拟IP地址*

     命令示例：**ping 192.168.3.22**

- 方法二：执行以下命令，在Client端，清理虚拟IP地址的ARP表中的残留表项，触发Client端学习新的ARP表。

  arp -d *虚拟IP地址*

  命令示例：**arp -d 192.168.3.22**

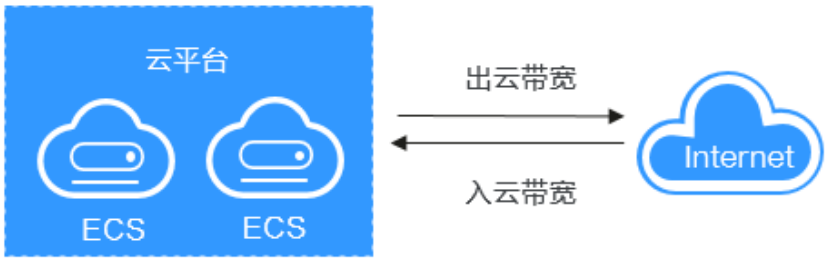
14.7 带宽类

14.7.1 什么是入云带宽和出云带宽?

入云带宽：从Internet流入云平台方向的带宽，例如，从公网下载资源到云内ECS。

出云带宽：从云平台流出到Internet方向的带宽，例如，云内的ECS对外提供服务，外部用户下载云内ECS上的资源。

图 14-16 入云带宽和出云带宽



14.7.2 如何排查带宽超过限制?

问题现象

申请独享带宽或是共享带宽时都需要选择带宽大小，该值为出云带宽的最大上限。如果出现依赖于公网的web应用程序出现卡顿等情况，请先排查该弹性云服务器绑定的EIP独享带宽是否超过带宽最大上限。

说明

带宽超限后，可能会引起随机丢包，为保证业务正常运行，推荐您对带宽进行监控。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-17 排查思路

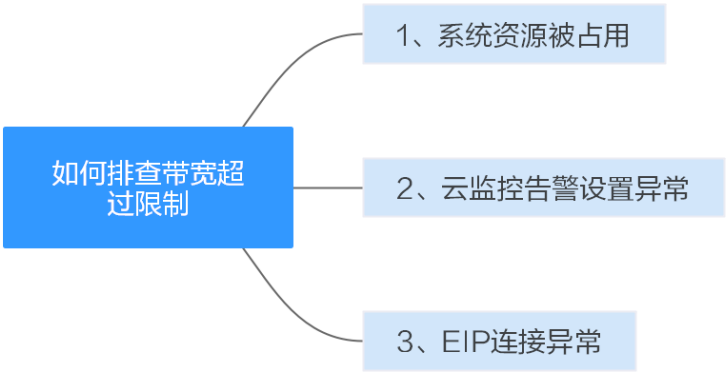


表 14-13 排查思路

可能原因	详细说明	处理措施
系统资源被占用	当系统资源被占用可能会导致CPU或带宽利用率过高，从而使系统出现卡顿或网络断开的情况。	解决方法请参考**系统资源被占用**。
云监控告警设置异常	云监控设置EIP带宽超限告警时，告警策略设置不合理，系统将发送异常的带宽超限告警信息。	解决方法请参考**云监控告警设置异常**。

系统资源被占用

当系统资源被占用可能会导致CPU或带宽利用率过高，从而使系统出现卡顿或网络断开的情况。

您可以参考以下文档定位影响云服务器带宽和CPU利用率高的进程，选择对进程优化或关闭处理。

- Windows系统：《用户指南》常见问题中的“Windows云服务器卡顿怎么办？”章节。
- Linux系统：《用户指南》常见问题中的“Linux云服务器卡顿怎么办？”章节。

云监控告警设置异常

云监控设置EIP带宽超限告警时，告警策略设置不合理，系统将发送异常的带宽超限告警信息。

当在云监控服务中创建“带宽”维度的告警规则时，若出网带宽最大值或告警周期设置过小，都将频繁收到带宽超限的告警信息。

您需要根据申请的带宽大小设置合理的告警策略。例如购买的带宽大小为5Mbit/s，您可以设置连续三个周期内最大出网带宽大于等于4.8Mbit/s时，系统发送告警通知。此时，可以考虑扩大带宽。扩大带宽的操作请参见**修改弹性IP的带宽配置**。

1. 登录管理控制台，在云监控服务中，左侧导航栏选择“告警 > 告警规则 ”。
2. 单击“创建告警规则”，配置带宽超限的告警规则。

14.7.3 公网带宽与内网带宽有何差异?

公网带宽

公网带宽是指云平台实例到Internet之间的网络带宽流量。ECS实例可以通过在创建时配置公网带宽，或创建后绑定EIP的方式来开通公网带宽，即弹性IP带宽。

公网带宽分为入云带宽和出云带宽。

入云带宽：从Internet流入云平台方向的带宽，例如，从公网下载资源到云内ECS。

出云带宽：从云平台流出到Internet方向的带宽，例如，云内的ECS对外提供服务，外部用户下载云内ECS上的资源。

内网带宽

内网带宽是指同一地域同一专有网络内的云服务器ECS实例之间传输的内网带宽流量。云服务器ECS与云数据库、负载均衡以及对象存储之间也可以使用内网相互连接。内网带宽大小跟实例规格有关。

14.7.4 带宽的限速范围是多少?

带宽的限速范围为1Mbit/s~2000Mbit/s。

如果当前带宽无法满足使用需要，您可以申请扩大配额。

操作步骤

目前系统暂不支持在线调整2000Mbit/s以上的带宽大小。

如您需要调整配额，请联系运营管理员。

14.7.5 带宽的类型有哪些?

带宽支持独享和共享两种类型。独享带宽只能针对一个弹性IP进行限速，共享带宽可以针对多个弹性IP进行集中限速。

14.7.6 独享带宽与共享带宽有何区别?

独享带宽：只针对一个弹性IP进行限速，该弹性IP只能被一个云资源（ 弹性云服务器、NAT网关、弹性负载均衡等 ）使用。

共享带宽：可以针对多个弹性IP进行集中限速，带宽可以添加多个弹性IP。弹性IP添加和移出共享带宽对业务不产生影响。

独享带宽与共享带宽不支持直接互相转换，您可以购买一个共享带宽，进行如下操作：

- 将弹性IP添加到共享带宽，则弹性IP使用共享带宽。
- 将弹性IP移出共享带宽，则弹性IP使用独享带宽。

14.7.7 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?** 。

14.7.8 带宽与上传下载速率是什么关系?

带宽单位用bps(bit/s)，表示每秒钟传输的二进制位数。下载速率单位用Bps(Byte/s)表示，表示每秒钟传输的字节数。

1Byte（字节）=8bit（位），即下载速率=带宽/8

通常1M带宽即指1Mbps=1000Kbps=1000/8KBps=125KBps一般情况下，考虑到还有其他损耗（计算机性能、网络设备质量、资源使用情况、网络高峰期等），实际速率一般小于这个速率。

14.8 网络连接类

14.8.1 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。

14.8.2 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. 在子网列表中，单击需要修改的子网名称。
4. 在子网详情页，修改子网DNS服务器地址。
5. 单击“确定”，完成修改。

14.8.3 同时拥有自定义路由和弹性 IP 的访问外网的优先级是什么?

弹性IP的优先级高于VPC路由表中的自定义路由。示例如下：

假如VPC路由表中存在一条自定义路由，目的地址为默认路由（0.0.0.0/0），下一跳为NAT网关。

如果VPC内的ECS绑定了EIP，会在ECS内增加默认网段的策略路由，并且优先级高于VPC路由表中的自定义路由，此时会导致流量转发至EIP出公网，无法抵达NAT网关。

14.8.4 本地主机访问使用弹性云服务器搭建的网站出现间歇性中断怎么办?

问题现象

在云服务器上搭建网站后，部分客户通过本地网络访问网站时出现偶发性无法访问的情况。

解决思路

1. 确认客户使用的本地网络。

   若客户的本地网络是NAT网络（本地主机通过NAT功能使用公网IP地址访问弹性云服务器），可能会导致该问题。
2. 执行以下命令，查看搭建网站的弹性云服务器是否开启了“tcp_tw_recycle”。

   sysctl -a|grep tcp_tw_recycle

   tcp_tw_recycle取值为1时，表示开启。
3. 执行以下命令，查看云服务器内核丢包数量。

   cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'

   如果ListenDrops数值非0，表示存在丢包，即存在网络问题。

解决步骤

修改云服务器的内核参数可以解决此问题。

- 临时修改参数方法（重启服务器后该设置失效），设置如下：

  sysctl -w net.ipv4.tcp_tw_recycle=0
- 永久修改参数方法：
  a. 执行以下命令，修改“/etc/sysctl.conf”文件。

     vi /etc/sysctl.conf

     在该文件中添加以下内容：

     net.ipv4.tcp_tw_recycle=0
  b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。
  c. 执行以下命令，生效配置。

     sysctl -p

14.8.5 同一个子网下的弹性云服务器只能通过内网 IP 地址单向通信怎么办?

问题现象

ecs01和ecs02是同一个VPC内同一个子网中的两个弹性云服务器，IP地址分别为192.168.1.141和192.168.1.40

ecs01可以通过内网IP地址ping通ecs02，但是ecs02无法通过内网IP地址ping通ecs01。

解决思路

1. 在ecs02上使用弹性IP地址尝试ping通ecs01。若能ping通则说明ecs01的网卡处在正常工作状态。
2. 在ecs02上执行**arp -n**命令，查看回显是否包含ecs01的MAC。如果无ecs01的MAC地址，则说明ecs02使用内网IP地址尝试ping通ecs01时，未学习到ecs01的MAC地址。
3. 在ecs01上执行**ip a**命令，查看弹性云服务器ecs01内部的网卡配置。以下图为例：

   图 14-18 查看 ecs01 网卡配置

   ```
   [root@bd-slave1 ~]# ip a
   1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
       link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
       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 qlen 1000
       link/ether fa:16:3e:62:1d:d5 brd ff:ff:ff:ff:ff:ff
       inet 192.168.1.141/24 brd 192.168.1.255 scope global eth0
       inet 192.168.1.40/32 scope global eth0
       inet6 fe80::f816:3eff:fe62:1dd5/64 scope link
          valid_lft forever preferred_lft forever
   ```

   可以从回显中得知，多配置了一个IP地址：192.168.1.40/32。该配置会导致ecs01发给ecs02的报文无法从ecs01传出。

解决步骤

修改ecs01的网卡配置，执行以下命令，删除配置在eth0上的多余IP地址，以192.168.1.40/32为例。

ip a del 192.168.1.40/32 dev eth0

14.8.6 同一个 VPC 内的两台弹性云服务器无法互通或者出现丢包等现象时，如何排查?

问题描述

同一个VPC内的两台弹性云服务器无法互通或者出现丢包等现象。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-19 排查思路

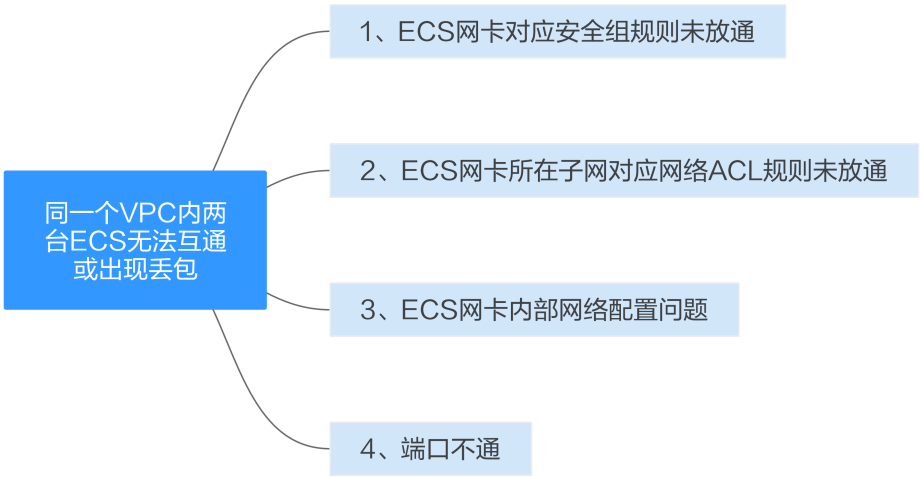


表 14-14 排查思路

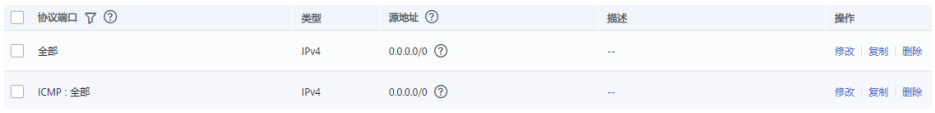
可能原因	处理措施
ECS网卡对应安全组规则未放通	解决方法请参考**ECS网卡对应安全组规则未放通**。
ECS网卡所在子网关联的网络ACL规则未放通	解决方法请参考**ECS网卡所在子网关联的网络ACL规则未放通**。
ECS网卡内部网络配置问题	解决方法请参考**ECS网卡内部网络配置问题**。
端口不通	解决方法请参考**端口不通**。

ECS 网卡对应安全组规则未放通

排查弹性云服务器网卡对应的安全组是否放通了出方向和入方向的ICMP规则。

以入方向为例，即安全组规则需要包含下图中的任意一条规则。

图 14-20 入方向安全组规则



若客户测试的是其他协议的报文，需放通相应协议的安全组规则。例如，测试的是UDP报文，则需检查安全组是否有规则放通出入方向的UDP协议。

ECS 网卡所在子网关联的网络 ACL 规则未放通

1. 查看弹性云服务器的网卡是否处于网络ACL的关联子网中。

2. 在网络ACL列表中查看网络ACL的状态。
   - 状态显示“已开启”，则表示网络ACL已经开启。执行**3**。
   - 状态显示“未开启”，则表示网络ACL已经关闭。执行**4**。
3. 单击网络ACL名称，分别在“入方向”和“出方向”的页签下添加ICMP放通规则。
4. 网络ACL关闭时，默认规则为丢弃所有出入方向的包。此时，请删除网络ACL或者开启ACL并放通ICMP规则。

ECS 网卡内部网络配置问题

以下步骤以Linux系统为例，Windows操作系统请检查系统防火墙限制。

1. 确认弹性云服务器是否有多网卡配置。如果配置多网卡且弹性IP绑定在非主网卡上，请在弹性云服务内部配置策略路由，请参考**如何配置多网卡弹性云服务器的策略路由?** 。
2. 登录弹性云服务器，执行以下命令，查看网卡是否创建且网卡获取私有IP地址。若无网卡信息或者无法获取私有IP地址，请联系技术支持。

   ifconfig

   图 14-21 查看网卡 IP 地址

   ```
   [root@ecs-acl ~]# ifconfig
   eth0      Link encap:Ethernet  HWaddr FA:16:3E:BC:B7:81
             inet addr:192.168.72.209  Bcast:192.168.72.255  Mask:255.255.255.0
             inet6 addr: fe80::f816:3eff:febc:b781/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:881 errors:0 dropped:0 overruns:0 frame:0
             TX packets:547 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:49604 (48.4 KiB)  TX bytes:44454 (43.4 KiB)
             Interrupt:46
   ```

3. 执行以下命令，查看弹性云服务器的CPU占用率是否过高，CPU占有率超过80%有可能会影响ECS通信。

   top

4. 执行以下命令，查看弹性云服务器内容部是否有安全规则的其他限制。

   iptables-save

5. 执行以下命令，查看“/etc/hosts.deny”文件中是否包含了限制通信的IP地址。

   vi /etc/hosts.deny

   如果hosts.deny文件里面包含了对端的IP地址，请将该IP从hosts.deny文件中删除并保存文件。

端口不通

1. 如果无法访问弹性云服务器的特殊端口，请排查安全组规则以及网络ACL规则中是否对端口进行放行。
2. 在Linux弹性云服务器内部通过以下命令查看弹性云服务器内部是否监听该端口。如果未对该端口进行监听，可能会影响弹性云服务器的通信。

   netstat -na | grep <*端口号*>

14.8.7 Cloud-init 连接出现问题时，如何排查?

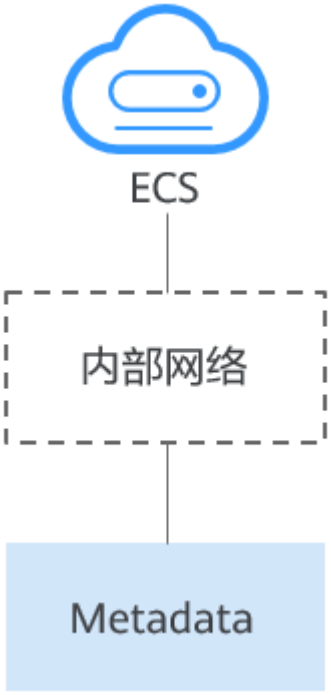
问题描述

无法正常使用Cloud-init。

排查思路

弹性云服务器获取Metadata的流程如图14-22所示:

图 14-22 获取 Metadata 流程图



您可以按照以下原因进行排查，如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-23 排查思路

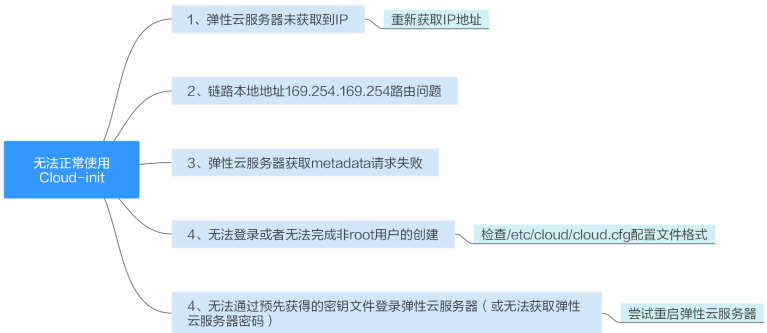


表 14-15 排查思路

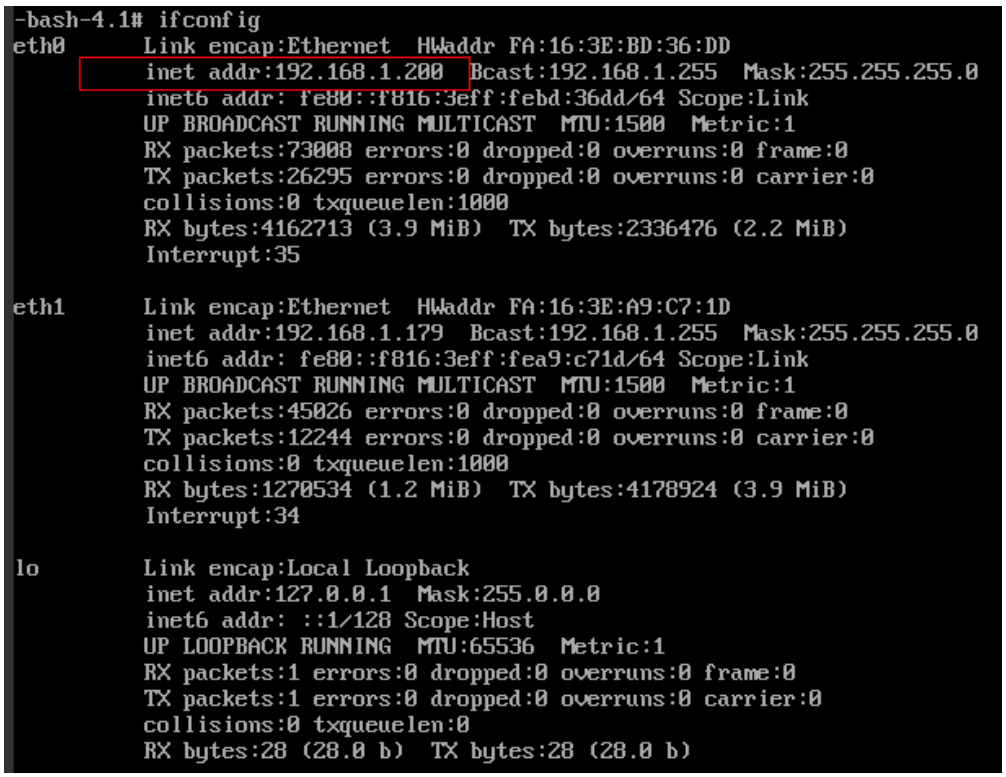
可能原因	处理措施
弹性云服务器未获取到IP	解决方法请参考**弹性云服务器未获取到IP**。
链路本地地址169.254.169.254路由问题	解决方法请参考**链路本地地址169.254.169.254路由问题**。
弹性云服务器获取metadata请求失败	解决方法请参考**弹性云服务器获取metadata请求失败**。
无法登录或者无法完成非root用户的创建	检查/etc/cloud/cloud.cfg配置文件格式，参考**无法登录或者无法完成非root用户的创建**。
无法通过预先获得的密钥文件登录弹性云服务器（或无法获取弹性云服务器密码）	重启弹性云服务器后重试解决。

弹性云服务器未获取到 IP

检查弹性云服务器是否已经获取到IP地址。

如果没有获取到IP地址，请尝试执行获取命令：**dhclient**（不同的操作系统，获取DHCP地址的命令有稍微的差别，请按照弹性云服务器的操作系统，选择相应命令）；也可以通过down/up网卡的方式尝试重新获取。

图 14-24 查看弹性云服务器 IP 地址



链路本地地址 169.254.169.254 路由问题

如果弹性云服务器ping不通169.254.169.254，请按以下步骤排查：

1. 查看弹性云服务器内169.254.169.254的默认路由：

   正常情况下，169.254.169.254的精确路由的下一跳地址，要和默认路由的下一跳地址保持一致。

   图 14-25 查看 169.254.169.254 的路由信息

   ```
   -bash-4.1# ip route
   169.254.169.254 via 192.168.1.1 dev eth0  proto static
   192.168.1.0/24 dev eth0  proto kernel  scope link  src 192.168.1.200
   192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.179
   169.254.0.0/16 dev eth0  scope link  metric 1002
   default via 192.168.1.1 dev eth0  proto static
   -bash-4.1#
   ```

2. 如果没有169.254.169.254/32位的精确路由：

   CentOS 5系列的镜像不支持opt_name为121的这种路由注入方式，所以无法注入，请尝试使用新的镜像。

3. 如果169.254.169.254/32的精确路由指向的下一跳和默认路由不一致：
   - 如果不是新建弹性云服务器，可能是开启CloudInit特性之前创建的，弹性云服务器内部service network restart重新进行dhcp请求，查看是否获取到正确的路由。

弹性云服务器获取 metadata 请求失败

弹性云服务器内部获取metadata请求的命令：

curl http://169.254.169.254/openstack/latest/meta_data.json

正确的返回结果如图14-26所示：（以下示例仅供参考，命令行有返回值即表示正确）

图 14-26 返回结果

```
-bash-4.1# curl http://169.254.169.254/openstack/latest/meta_data.json
{"random_seed": "rTVrsDlEh6AjUKLnvq51U8S0pH6xC78MFRTeWIOmunBMyqos6q/EsAEJondF8iJkMDGOTzbCTb8I5HMtS9X
XHu61u+y8fAeyWxAj6OAv8KHMPgDv6XDfhKu6qyjCrjXn5hVFvqfZ/yaJ3LrAEjB8NJ59hI+wmbPi8oYc2WzYmTqWjXYRNwpmqJM
slKYm0CLuFbwYo2aKly27/WEVZDV0QlGpRkkwNwFaCN/rQQ/hHd+3VwSJbArsqVeoWCTp5oxixLiCJzSSHAKz41ViZiRxuYwm0go
iTFtopvZTwmYEklFmkZsy7h6PPOkgmjgPn+1kZf0qqhtIvpyRr2pW4aPAeZa4z7QX1RtmwT7MUyGUbea85/lPDUE1J/GJpoH1/+z
rDyelAO9CsOG1VFuELadYDcrWA4k42fOo7dDmEyDmINnE8eeqa5r7EohbO4KTimzi+3nblOQjPq/S7J+mFM/UoZEJHObZE4uwlAj
2nhvy/pc6ho7fQKbx0C78fbiPh59CKyFOWB35nNJ/CZNNBTd3UdG25SQ7OlFnA+NtbDeo8+g05iFLvWeww0G5BLcjm1fjh9+mqot
+5ae6ZcexUsI1fscqm8jwCnCimthJlYGmbxu+6Fm9XpLDopDFrRtBUcRSMtIK67JprBSRppc+4sMyyiuKYlJOTUJYQYDBV2B7F3o
=", "uuid": "53ebb737-ddc5-4303-9fac-aa72b00b101a", "availability_zone": "eu-de-02", "hostname": "ec
s-gjm-55eb.novalocal", "launch_index": 0, "meta": {"metering.image_id": "98721f93-722f-4386-a975-3cb
df1abf56d", "metering.imagetype": "gold", "metering.resourcespeccode": "c2.large.oracle", "metering.
cloudServiceType": "sys.service.type.ec2", "image_name": "AutoC_OTC_OEL_6.8", "metering.resourcetype
": "1", "os_bit": "64", "vpc_id": "120b71c7-94ac-45b8-8ed6-30aafc8fbdba", "os_type": "Linux", "charg
ing_mode": "0"}, "project_id": "efdf974f549b4eaab05c3903ddd2ab0e", "name": "ecs-gjm-55eb"}-bash-4.1#
```

无法登录或者无法完成非 root 用户的创建

Cloud-init已配置，并且服务进程正常，但是无法登录或者无法完成非root用户的创建。

需要检查/etc/cloud/cloud.cfg配置文件格式是否严格遵循缩进了，具体要参考各大Linux OS厂商本身的要求，如下以ubuntu操作系统为例。

图 14-27 检查配置文件

```
system_info:
   # This will affect which distro class gets used
   distro: rhel
   # Default user name + that default users groups (if added/used)
   default_user:
     name: linux  //登录使用的用户名。
     lock_passwd: False  //False，表示当前不禁用密码登录的方式，注意部分操作系统此处配置为0表示不禁用。
     gecos: Cloud User
     groups: users  //可选项，将用户添加到另外的组里，groups必须是系统里/etc/group已存在的组。
     passwd: $6$I63DBVKK$Zh41chiJR7NuZvtJHsYBQJIg5RoQCRL51X2Hsgj2s5JwXI7KUO1we8WYcwbzea52VHpRuNo28vmxxCyU6LwoD0
     sudo: ["ALL=(ALL) NOPASSWD:ALL"]  //表示设置用户具有root用户的所有权限。
     shell: /bin/bash  //shell执行采用bash方式。
   # Other config here will be given to the distro class and/or path classes
   paths:
      cloud_dir: /var/lib/cloud/
      templates_dir: /etc/cloud/templates/
   ssh_svcname: sshd
```

无法通过预先获得的密钥文件登录弹性云服务器（或无法获取弹性云服务器密码）

如果某次弹性云服务器启动后通过预先获得的密钥文件无法登录弹性云服务器（或无法获取弹性云服务器密码），可以尝试通过重启弹性云服务器后重试解决。

14.8.8 EIP 连接出现问题时，如何排查?

问题描述

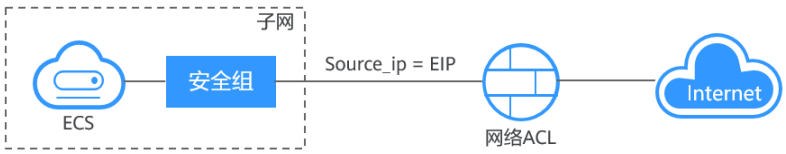
用户的弹性云服务器已绑定EIP，但是无法连接到Internet。

排查思路

排查EIP连接问题

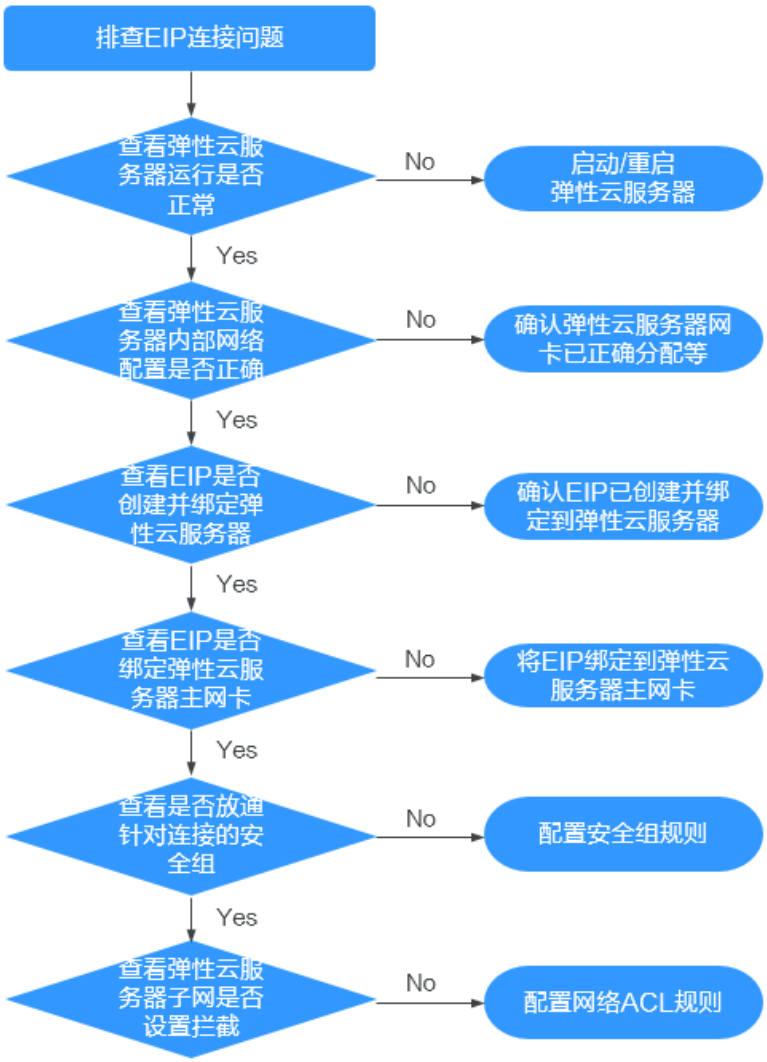
弹性云服务器通过EIP访问Internet的流程如图14-28所示：

图 14-28 EIP 网络示意图



本问题请按照以下思路进行排查处理。

图 14-29 排查思路



1. **查看弹性云服务器运行是否正常**
2. **查看弹性云服务器内部网络配置是否正确**
3. **查看EIP是否创建并绑定弹性云服务器**
4. **查看EIP是否绑定弹性云服务器主网卡**
5. **查看是否放通针对连接的安全组**
6. **查看弹性云服务器子网是否设置拦截**

步骤一：查看弹性云服务器运行是否正常

检查您的弹性云服务器是否正常运行。

弹性云服务器运行状态如果不是运行状态，请尝试启动/重启弹性云服务器。

步骤二：查看弹性云服务器内部网络配置是否正确

1. 确认弹性云服务器网卡已经正确分配到IP地址。
   登录弹性云服务器内部，使用命令**ifconfig**或**ip address**查看网卡的IP信息。

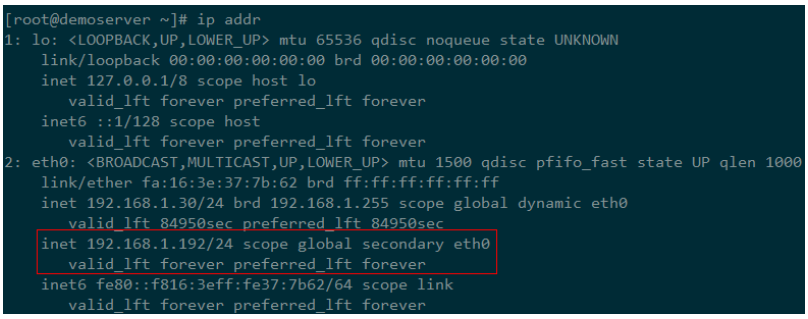
注：Windows弹性云服务器可以在命令行中执行**ipconfig**查看。

2. 确认虚拟IP地址已经正确配置在网卡上。

   当您使用了虚拟IP，需要确认虚拟IP是否正确配置在网卡上。

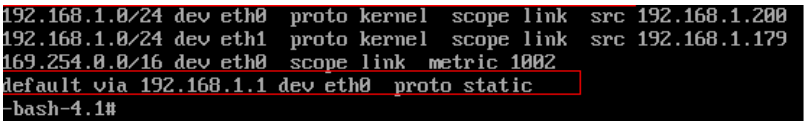
   登录弹性云服务器内部，使用命令**ifconfig**或**ip address**查看网卡的IP信息。如果没有虚拟IP地址，可以使用命令**ip addr add *虚拟IP地址* eth0**给弹性云服务器添加正确的配置。

   图 14-30 查看网卡的虚拟 IP 地址



   查看是否有默认路由信息，如果没有，则可以通过**ip route add**添加路由。

   图 14-31 查看默认路由



步骤三：查看 EIP 是否创建并绑定弹性云服务器

检查您的EIP是否已经创建并绑定到该弹性云服务器，若未创建&绑定，请先完成创建&绑定。

步骤四：查看 EIP 是否绑定弹性云服务器主网卡

检查您的EIP是否绑定在弹性云服务器的主网卡。若未绑定主网卡，需绑定至弹性云服务器的主网卡上。

您可以在弹性云服务器详情页的网卡页签下进行查看，默认列表第一条为主网卡。

步骤五：查看是否放通弹性云服务器所在的安全组

检查您的安全组规则是否已经配置。配置安全组规则请参见**添加安全组规则**。

请根据实际需求，选择性配置安全组规则（Remote IP指的是放行的IP地址，0.0.0.0/0表示放通所有的IP地址，请谨慎使用）。

步骤六：查看弹性云服务器子网是否设置拦截

检查您弹性云服务器使用的网卡所在子网的网络ACL是否会对流量进行拦截。

您可以在虚拟私有云页面左侧导航栏选择网络ACL进行配置，请确认弹性云服务器涉及的子网已放通。

14.8.9 弹性云服务器 IP 获取不到时，如何排查?

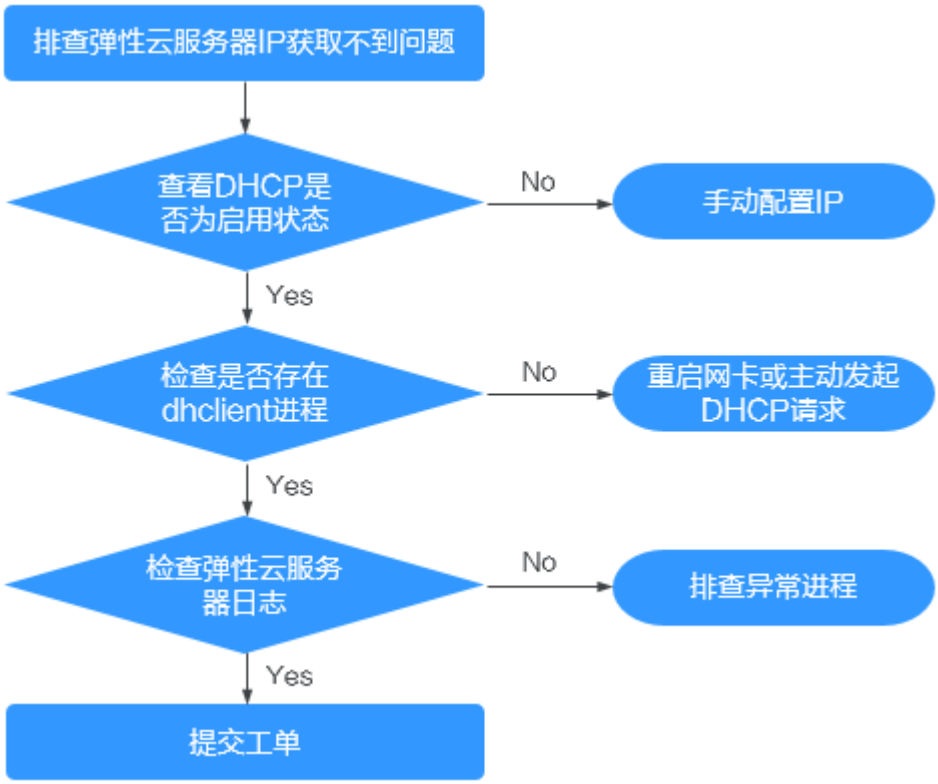
问题描述

用户无法查询到弹性云服务器私网IP地址信息。

排查思路

本问题请按照以下思路进行排查处理。

图 14-32 排查思路



1. **查看DHCP是否为启用状态**
2. **检查是否存在dhclient进程**
3. **检查弹性云服务器日志**

步骤一：查看 DHCP 是否为启用状态

检查子网的DHCP是否为启用状态（默认“启用”状态）。

进入子网详情页面，查看DHCP是否为“启用”状态，若DHCP开关为关闭状态请参考3手动配置静态IP。

步骤二：检查是否存在 dhclient 进程

1. 执行如下命令，检查是否存在dhclient进程。

   ps -ef | grep dhclient

2. 若dhclient进程不存在，登录弹性云服务器，尝试重启网卡或主动发起DHCP请求。
   - Linux系统：

     执行**dhclient ethx**命令。若不支持dhclient命令就执行**ifdown ethx;ifup ethx**（ethx代表弹性云服务器网卡，如eth0、eth1）。
   - Windows系统：

     先禁用网络连接，然后再重新启用。
3. 对于DHCP Client长期不发起请求的情况，例如：重启网卡后又复现，尝试使用以下方法配置静态IP。
   - Linux系统：
     i. 执行以下命令，打开/etc/sysconfig/network-scripts/ifcfg-eth0中的配置。

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

     ii. 修改/etc/sysconfig/network-scripts/ifcfg-eth0中的配置。

        BOOTPROTO=static

        IPADDR=192.168.1.100 #IP地址

        NETMASK=255.255.255.0 #掩码值

        GATEWAY=192.168.1.1 #网关地址

     iii. 执行以下命令，重启网络服务。

        service network restart
   - Windows系统：

     在网络连接中选择“属性 > Internet协议版本4 > 属性”，手动输入IP地址、子网掩码和默认网关。

步骤三：检查弹性云服务器日志

查看弹性云服务器的messages日志（路径为/var/log/messages）排查问题。

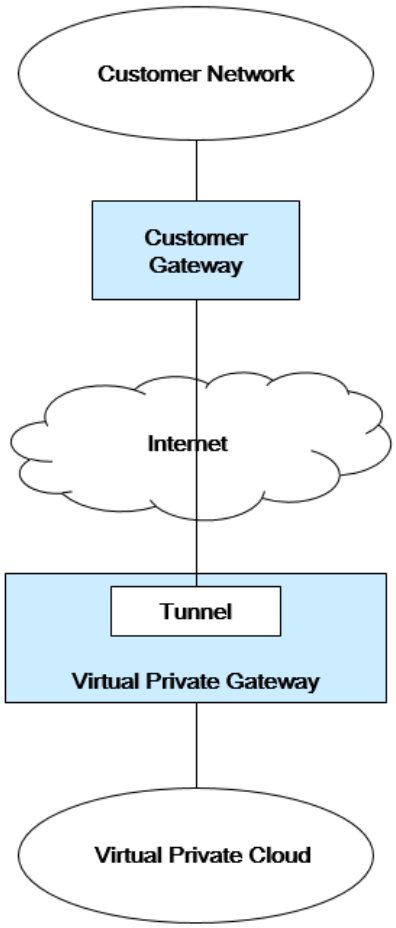
通过网卡的MAC地址过滤日志，排查是否有进程影响DHCP获取IP。

14.8.10 VPN 及专线网络连接出现问题时，如何排查?

VPN 网络示意图

图14-33显示您的网络、客户网关、通往虚拟专用网关的VPN连接以及VPC。

图 14-33 VPN 网络示意图



客户自查指导

1. 反馈您的网络信息

   确定表14-16中的信息。该表包括部分项目的示例值，您可以使用示例值或确定的实际值。您必须取得所有其他项目的实际值。

   说明

   您可以打印该表，并填入您的值。

   表 14-16 网络信息

Item	如何使用	注释	您的值
VPC CIDR 块	用于客户网关配置中。	示例：10.0.0.0/16	-
VPC ID信息	-	-	-

Item	如何使用	注释	您的值
1 号子网 CIDR 块（可与 VPC 的 CIDR 块相同）	-	示例：10.0.1.0/24	-
弹性云服务器 ID信息	-	-	-
客户网关类型 (例如：Cisco)	-	-	-
客户网关使用的公网IP地址	-	该值必须为静态。	-

2. 反馈您的网关配置的信息

   请客户通过以下步骤排查网关的连接性问题。

   您需要考虑四个方面：IKE、IPsec、ACL规则和路由选择。您可以按任何次序对这些方面进行故障排除，不过建议您从IKE开始 (位于网络堆栈的底部) 并依次向上排除。

   a. 获取您采用的网关设备的IKE策略。
   b. 获取您采用的网关设备的IPSEC策略。
   c. 获取您采用的网关设备的ACL规则。
   d. 检查您采用的网关设备与公有云的网关设备是否路由可达。

   说明

   具体网关设备采用的设备命令不同，请根据您采用的网关设备（Cisco、H3C、AR以及Fortinet设备等），采用对应设备的命令进行排查，获取上述信息。

客户需要协助做的运维操作

客户从公有云的弹性云服务器内向对端设备发起通信请求。

操作方法：

登录公有云的弹性云服务器使用ping命令，ping您自有数据中心的网络IP。

14.8.11 外网能访问服务器，但是服务器无法访问外网时，如何排查?

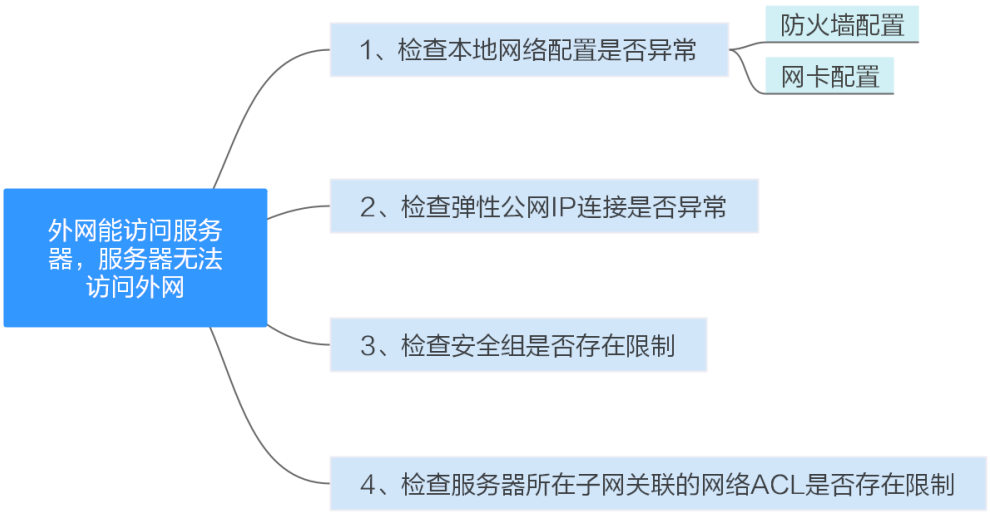
问题描述

外网能访问服务器，但是服务器无法访问外网，出不了我方的网关。

排查思路

您可以按照以下原因进行排查，如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-34 排查思路



安全组存在限制

检查服务器所在安全组出方向规则，确认是否存在限制。

安全组默认放通出方向流量，若有限制，可参考，开放允许访问的协议或端口，或单击“一键放通”取消限制。

图 14-35 一键放通

网络 ACL 存在限制

检查服务器所在子网关联的网络ACL出方向规则，确认是否存在限制。

网络ACL默认拒绝所有出站流量，需要放通服务器子网所在网关联的网络ACL出方向限制，即添加出方向规则时，选择“策略”为“允许”。

14.8.12 配置了 IPv6 双栈，为什么无法访问 IPv6 网站?

问题现象

用户的云服务器已配置了IPv6双栈，但是无法访问IPv6网站。

解决思路

- 查看IPv6双栈配置是否正确，网卡是否获取到IPv6地址。
- 查看是否已将IPv6双栈网卡添加到共享带宽。

- 当云服务器拥有多张网卡时，查看在云服务器内部，是否为这些网卡配置策略路由。

解决方案

- 购买ECS并进行网络配置时，请务必选择“自动分配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。

- 默认IPv6地址只具备私网通信能力，如果您需要通过该IPv6地址访问Internet或被Internet上的IPv6客户端访问，您需要购买和绑定共享带宽。

  如您已有共享带宽，可以不用重新购买，直接将IPv6地址加入共享带宽即可。

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

14.8.13 弹性云服务器防火墙配置完成后，为什么网络不通?

问题描述

如果您的云服务器安装完防火墙后，发现网络不通，请根据本章节指导排查原因。常见客户场景示例如下：

在同一个VPC内，客户有三台ECS，业务部署在ECS1和ECS2上，在ECSX上安装了第三方防火墙，从ECS1和ECS2出来的流量，需要通过ECSX的防火墙进行过滤。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

表 14-17 排查思路

可能原因	处理措施
检查ECS安全组是否已放通	解决方法请参考**检查ECS安全组是否已放通**。
检查网卡的“源/目的检查”开关是否关闭	解决方法请参考**检查网卡的源/目的检查开关是否关闭**。
检查VPC的自定义路由是否添加正确	解决方法请参考**检查VPC的自定义路由是否添加正确**。

检查 ECS 安全组是否已放通

同一个VPC内的子网网络互通，如果您的业务ECS和防火墙所在的ECS网络不通，可能是因为这些ECS位于不同的安全组导致的。

如果ECS位于不同的安全组内，需要您在这些ECS关联的安全组内添加对端安全组的规则，放通这些安全组的网络。

检查网卡的“源/目的检查”开关是否关闭

请检查防火墙所在ECS的网卡是否关闭“源/目的检查”开关，如果未关闭，请参考以下操作关闭该开关。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在服务列表，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，选择目标弹性云服务器，并单击名称对应的超链接。
   进入弹性云服务器“基本信息”页签。
5. 选择“弹性网卡”页签，单击 展开主网卡区域，检查“源/目的检查”是否关闭。
   如果未关闭，请关闭该开关后，重新检查网络。

检查 VPC 的自定义路由是否添加正确

请检查业务ECS所在子网的关联路由表中是否添加指向防火墙所在ECS的路由。

防火墙安装完成后，您需要在业务ECS所在子网的关联路由表中，添加下一跳为“云服务器实例”，指向防火墙所在ECS的自定义路由。

14.9 路由类

14.9.1 如何配置多网卡弹性云服务器的策略路由?

背景知识

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

操作场景

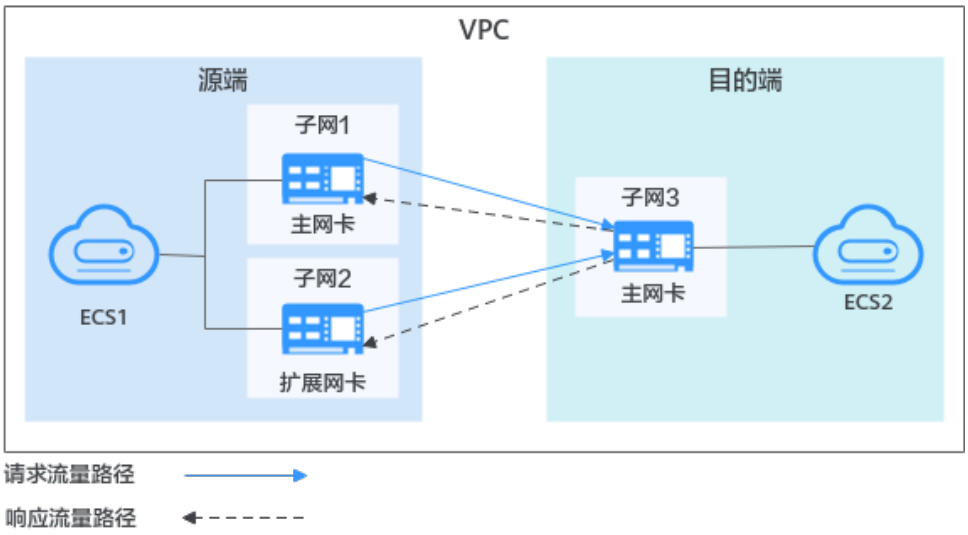
本文档以配置双网卡云服务器的策略路由为例，组网如图14-36所示，具体说明如下：

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

须知

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

图 14-36 双网卡云服务器组网示意图



操作指引

本文提供Linux和Windows云服务器的操作指导，具体请参见**表14-18**。

表 14-18 操作指引说明

操作系统类型	IP类型	操作步骤
Linux	IPv4	本文以CentOS 8.0 64bit操作系统为例：
	IPv6	
Windows	IPv4	本文以Windows 2012 64bit操作系统为例：
	IPv6	

14.9.2 路由表可以跨 VPC 存在吗?

路由表不可以跨VPC存在。

路由表由一系列路由规则组成，只能存在于某个VPC内，用于控制VPC内子网的出流量走向。一个VPC可以有多个路由表，自带一个默认路由表，您还可以根据需求自定义多个路由表。

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，但一个路由表可以同时关联多个子网。

14.9.3 1 个路由表里可以存在多少个路由?

目前，1个路由表默认可以存在100条自定义路由。

14.9.4 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。

14.9.5 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。

14.9.6 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。

14.10 安全类

14.10.1 安全组规则除描述字段外，其他字段均相同，是否算作相同的安全组规则?

是的。添加或导入安全组规则时，除描述字段外，其他字段均相同，算作相同的安全组规则，如果安全组中已经存在相同的安全组规则，那么对应规则将无法添加或导入。

14.10.2 如何查看安全组关联了哪些实例?

当您创建云服务器、云容器或者数据库等实例时，需要将实例加入安全组中。当您的安全组需要删除时，必须将安全组关联的实例全部移出安全组，才可以删除安全组。

您可以参考以下操作指导，查看安全组关联的实例。

1. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。
   进入“关联实例”页签，您可以依次查看安全组关联的服务器、扩展网卡等资源。
   如果“关联实例”页签下已无关联资源，但是系统仍然提示您安全组已被实例关联，请您继续执行以下操作。
2. 您需要进入对应服务的管理控制台，并选择和安全组相同的区域，查看是否有表14-19中列举的资源。

表 14-19 实例排查列表

产品分类	产品/实例名称
数据库	GaussDB
	DDS

产品分类	产品/实例名称
	DDM
应用中间件	Kafka
	RabbitMQ
	高可靠消息
	APIG
大数据	DataArts Studio
	DWS
	云搜索服务

14.10.3 为什么无法删除安全组?

- 系统创建的默认安全组不支持删除，默认安全组名称为default。
- 当安全组已关联至其他服务实例时，比如云服务器、云容器、云数据库等，此安全组无法删除。请您将实例从安全组中移出后，重新尝试删除安全组。
- 当安全组作为“源地址”或者“目的地址”，被添加在其他安全组的规则中时，此安全组无法删除。

  需要删除该条规则或者修改规则，然后重新尝试删除安全组。

  比如，安全组sg-B中有一条安全组规则的“源地址”设置为安全组sg-A，则需要删除或者更改sg-B中的该条规则，才可以删除sg-A。

14.10.4 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。

14.10.5 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 14-37 安全组规则

14.10.6 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?

- 安全组使用连接跟踪来标识进出实例的流量信息，入方向安全组的规则变更，对原有流量立即生效。出方向安全组规则的变更，不影响已建立的长连接，只对新建立的连接生效。

  当您在安全组内增加、删除、更新规则，或者在安全组内添加、移出实例时，系统会自动清除该安全组内所有实例入方向的连接，详细说明如下：

  - 由入方向流量建立的连接，已建立的长连接将会断开。所有入方向流量立即重新建立连接，并匹配新的安全组入方向规则。
  - 由出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有安全组规则。出方向流量新建立的连接，将会匹配新的安全组出方向规则。
- 网络ACL使用连接跟踪来标识进出实例的流量信息，入方向和出方向网络ACL规则配置变更，对原有流量不会立即生效。

  当您在网络ACL内增加、删除、更新规则，或者在网络ACL内添加、移出子网时，由入方向/出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有网络ACL规则。入方向/出方向流量新建立的连接，将会匹配新的网络ACL出方向规则。

须知

对于已建立的长连接，流量断开后，不会立即建立新的连接，需要超过连接跟踪的老化时间后，才会新建立连接并匹配新的规则。比如，对于已建立的ICMP协议长连接，当流量中断后，需要超过老化时间30s后，将会新建立连接并匹配新的规则，详细说明如下：

- 不同协议的连接跟踪老化时间不同，比如已建立连接状态的TCP协议连接老化时间是600s，ICMP协议老化时间是30s。对于除TCP和ICMP的其他协议，如果两个方向都收到了报文，连接老化时间是180s，如果只是单方向收到了报文，另一个方向没有收到报文，则连接老化时间是30s。
- TCP协议处于不同状态下的连接老化时间也不相同，比如TCP连接处于ESTABLISHED（连接已建立）状态时，老化时间是600s，处于FIN-WAIT（连接即将关闭）状态时，老化时间是30s。

14.10.7 安全组和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。

14.10.8 为什么网络 ACL 添加了拒绝特定 IP 地址访问的规则，但仍可以访问?

网络ACL存在规则优先级。优先级的数值越小，表示优先级越高，*为默认的规则，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。例如：A规则优先级为1，B规则需要优先级高于A，则向A规则前插入B规则，此时B规则优先级为1，A规则优先级为2。同样地，B规则需要优先级低于A，则向A规则后插入B规则即可。

当添加了拒绝特定IP地址访问的规则时，可以将允许所有IP访问的规则放至最后，拒绝特定IP地址访问的规则将生效。具体操作请参见。

14.10.9 为什么配置的安全组规则不生效?

问题描述

为弹性云服务器配置的安全组规则未生效。

排查思路

以下排查思路根据原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 14-38 排查思路

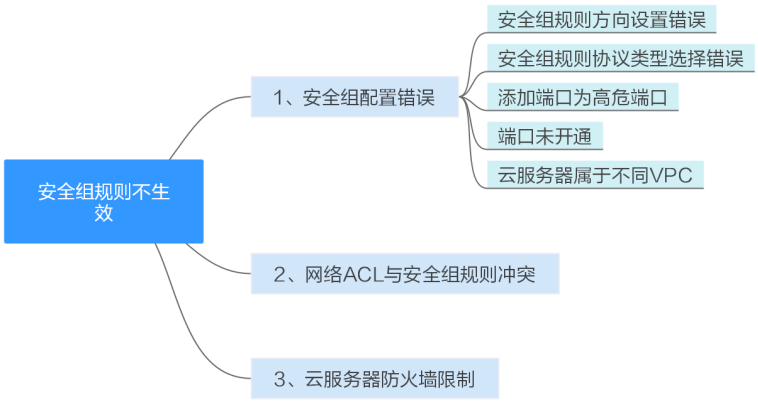


表 14-20 排查思路

可能原因	处理措施
安全组配置错误	解决方法请参考**安全组配置错误**。
网络ACL规则与安全组规则冲突	解决方法请参考**网络ACL规则与安全组规则冲突**。

安全组配置错误

当安全组规则配置有误时，无法按照规划的安全组规则对云服务器进行保护。您可以按照以下几点原因对安全组配置进行检查：

1. 安全组规则方向设置错误，例如将需要在入方向添加的规则添加到出方向规则下。
2. 安全组规则协议类型未选择正确。
3. 对应端口为高危端口，在部分地区部分运营商无法访问，建议您修改敏感端口为其他非高危端口来承载业务。
4. 对应端口未开通。您可以根据以下步骤检查对应端口在服务器中是否被正常监听。

   假设您在弹性云服务器上部署了网站，希望用户能通过TCP（80端口）访问到您的网站，您添加了一条入方向规则，如表14-21所示。

   表 14-21 安全组规则示例

方向	协议端口	源地址
入方向	自定义TCP: 80	0.0.0.0/0

   Linux弹性云服务器

   执行以下步骤，在Linux弹性云服务器上验证该安全组规则是否生效。

   a. 登录弹性云服务器。
   b. 执行以下命令，查看TCP 80端口是否被监听。

      netstat -an | grep 80

      若回显类似图14-39，说明TCP 80端口已开通。

      图 14-39 Linux TCP 80 端口验证结果

      ```
      tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
      ```

   c. 打开浏览器，在地址栏里输入“http://弹性云服务器的弹性IP地址”。

      如果访问成功，说明安全组规则已经生效。

   Windows弹性云服务器

   Windows弹性云服务器上验证该安全组规则是否生效的步骤如下所示。

   a. 登录弹性云服务器。
   b. 通过“开始菜单 > 运行 > cmd”，打开命令执行窗口。
   c. 执行以下命令，查看TCP 80端口是否被监听。

      netstat -an | findstr 80

      若回显类似图14-40，说明TCP 80端口已开通。

      图 14-40 Windows TCP 80 端口验证结果

      ```
      TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
      ```

   d. 打开浏览器，在地址栏里输入“http://弹性云服务器的弹性IP地址”。

      如果访问成功，说明安全组规则已经生效。
5. 云服务器属于不同的VPC。安全组需在网络互通的情况下生效。若云服务器属于不同VPC，但同属于一个安全组，此时云服务器不能互通。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内云服务器的流量进行访问控制。VPC连接请参见。

网络 ACL 规则与安全组规则冲突

安全组对弹性云服务器进行防护，网络ACL对子网进行防护。

例如当您设置了安全组入方向规则放通80端口，同时设置的网络ACL规则包含拒绝80端口的规则，那么此安全组规则不生效。

A 修订记录

发布日期	修改说明
2022-10-31	文档内容更新为： • 新增**弹性IP是否支持变更绑定的弹性云服务器？**章节。 • 新增**弹性IP是否支持跨区域绑定？**章节。 • 新增**带宽的类型有哪些？**章节。 • 新增**带宽与上传下载速率是什么关系？**章节。 • 新增**路由表可以跨VPC存在吗？**章节。 • 新增**安全组规则除描述字段外，其他字段均相同，是否算作相同的安全组规则？**章节。
2022-09-25	文档内容更新为： • 在**VPC流日志简介**章节，修改支持的弹性云服务器规格类型。
2022-05-25	文档内容更新为： • 在**为虚拟私有云添加IPv4扩展网段**章节，修改扩展网段支持的范围。 • 在**为弹性云服务器申请和绑定弹性IP**和**修改弹性IP的带宽配置**章节，增加弹性IP计费方式相关内容。 • 在**申请共享带宽**和**修改共享带宽**章节，增加共享带宽计费方式相关内容。
2022-01-25	文档内容更新为： 在**为虚拟私有云添加IPv4扩展网段**中增加扩展网段支持的掩码位数。
2021-08-26	文档内容更新为： • 在**修改虚拟私有云信息**章节，补充IPv4扩展网段的描述。 • 新增**为虚拟私有云添加IPv4扩展网段**、**删除虚拟私有云的IPv4扩展网段**章节。

发布日期	修改说明
2021-06-30	文档内容更新为： • 新增“**共享带宽**”章节。 • 在**虚拟私有云和子网**、**访问控制**章节，补充IPv6相关描述。 • 在**创建虚拟私有云和子网**、**为虚拟私有云创建新的子网**章节，删除参数“可用区”。
2021-04-20	文档内容更新为： • 在**VPC流日志简介**章节，新增支持的弹性云服务器规格类型。 • 在**为虚拟IP地址绑定弹性IP或弹性云服务器**章节，补充手工配置虚拟IP操作步骤。
2020-12-03	文档内容更新为： • 调整“虚拟私有云和子网章节”结构，并根据界面变化更新关于子网的操作步骤。 • 新增“**虚拟私有云和子网规划建议**”章节。 • 新增“**导出弹性IP列表**”章节。 • 新增“**VPC流日志**”章节。 • 在**变更弹性云服务器的安全组**章节，修改操作步骤。 • 常见问题中删除“路由表可以跨VPC存在吗？”。 • 根据界面更新界面词。 • 在“**虚拟IP**”章节，根据界面变化更新操作步骤。
2020-05-15	文档内容更新为： • 在“安全组配置示例”章节，新增“允许外部访问指定端口”示例。 • 删除“删除VPN”章节。 • 全文图示整改。 • 优化“网络ACL配置示例”章节描述。 • 优化“网络ACL简介”章节关于“网络ACL默认规则”的描述。 • 在“安全组简介”及“网络ACL简介”章节补充基本信息。 • 在“拒绝特定端口访问”中补充规则。 • 修改常见问题“变更安全组规则和网络ACL规则时，是否对原有流量实时生效？”。 • 修改常见问题“子网被相关资源占用时，会导致无法删除子网，如何排查相关资源？”。
2018-09-30	文档内容更新为： • 在“创建虚拟私有云基本信息及默认子网”章节新增批创子网描述。 • 在“添加网络ACL规则”章节新增批量添加规则描述、新增规则的“描述”参数。

发布日期	修改说明
2018-08-15	第一次正式发布。

