虚拟私有云

用户指南（安卡拉区域）

文档版本 01

发布日期 2024-04-15

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 什么是虚拟私有云

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、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。

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《虚拟私有云API参考》。

1.2 产品优势

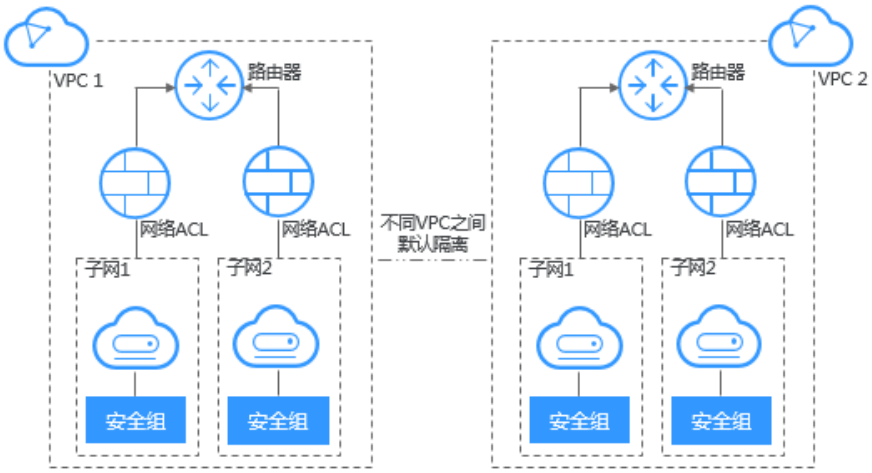
灵活配置

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

安全可靠

VPC之间通过隧道技术进行100%逻辑隔离，不同VPC之间默认不能通信。网络ACL对子网进行防护，安全组对弹性云服务器进行防护，多重防护您的网络更安全。

图 1-1 安全可靠



互联互通

默认情况下，VPC与公网是不能通信访问的，可以使用弹性公网IP、弹性负载均衡等多种方式连接公网。

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

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

高速访问

使用全动态BGP协议接入多个运营商，可支持20多条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅。

优势对比

虚拟私有云相比传统IDC的优势如表1-1所示。

表 1-1 虚拟私有云与传统 IDC 对比

对比项	虚拟私有云	传统IDC
部署周期	• 用户无需工程规划，布线等复杂工程部署的工作。 • 用户基于业务需求在云平台上自主规划私有网络、子网和路由。	用户需要自行搭建网络并进行测试，整个周期很长，而且需要专业技术支持。

对比项	虚拟私有云	传统IDC
总成本	云平台网络服务提供了多种灵活的计费方式，加上客户无需前期投入和后期网络运维，整体上降低了TCO。	用户需要机房、供电、施工、硬件物料等固定重资产投入，也需要专业的运维团队来保障网络安全。随着业务变化，资产管理成本也会随之上升。
灵活性	云平台提供多种网络服务，用户可以根据具体需求搭配服务。当业务发展需要更多的网络资源（如带宽资源）时，可以方便快捷的进行动态扩展。	业务部署需要严格遵守前期网络规划，当业务需求发生变化时，无法便捷的动态调整网络。
安全性	VPC逻辑隔离，结合网络控制网络ACL、安全组功能和DDoS等安全服务，保障了云上资源的安全使用。	网络很难得到专业维护，安全性较差，需要配置专业的网络安全人员来看护。

1.3 应用场景

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。

1.4 VPC 连接

为了满足您不同场景下连接Internet的需求，云平台以VPC为基础提供了弹性公网IP、弹性负载均衡、NAT网关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公网IP连接Internet**

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

- **大量弹性云服务器通过NAT网关连接Internet**

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

- **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。

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公网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。

1.6 权限管理

如果您需要对云平台上创建的VPC资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云平台资源的访问。

通过IAM，您可以在云平台账号中给员工创建IAM用户，并授权来控制员工对云平台资源的访问范围。例如您的员工中有负责软件开发的人员，您希望员工拥有VPC的使用权限，但是不希望员工拥有删除VPC等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用VPC，但是不允许删除VPC的权限，控制员工对VPC资源的使用范围。

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用户进行权限管理，您可以跳过本章节，不影响您使用VPC服务的其他功能。

IAM是云平台提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《统一身份认证服务用户指南》中“产品简介”章节。

VPC 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

VPC部署时通过物理区域划分。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问VPC时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于云平台各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。

- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对VPC服务，管理员能够控制IAM用户仅能对某一类网络资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，虚拟私有云（VPC）支持的API授权项请参见《虚拟私有云API参考》中“权限策略和授权项 > 策略及授权项说明”章节。

如表1-2所示，包括了VPC的所有系统权限。

表 1-2 VPC 系统权限

策略名称	描述	策略类别	依赖关系
VPC FullAccess	虚拟私有云的所有执行权限。	系统策略	如果您需要使用VPC流日志功能，则依赖云日志服务的只读权限LTS ReadOnlyAccess。
VPC ReadOnlyAccess	虚拟私有云的只读权限。	系统策略	无
VPC Administrator	虚拟私有云的大部分操作权限，不包括创建、修改、删除、查看安全组以及安全组规则。 拥有该权限的用户必须同时拥有Tenant Guest和Server Administrator权限。	系统角色	依赖Tenant Guest和Server Administrator策略，在同项目中勾选依赖的策略。

表1-3列出了VPC常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-3 常用操作与系统权限的关系

操作	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
创建VPC	x	√	√
修改VPC	x	√	√
删除VPC	x	√	√
查看VPC	√	√	√
创建子网	x	√	√
查看子网	√	√	√
修改子网	x	√	√
删除子网	x	√	√

操作	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
创建安全组	x	x	√
查看安全组	√	x	√
修改安全组	x	x	√
删除安全组	x	x	√
添加安全组规则	x	x	√
查看安全组规则	√	x	√
修改安全组规则	x	x	√
删除安全组规则	x	x	√
创建网络ACL	x	√	√
查看网络ACL	√	√	√
修改网络ACL	x	√	√
删除网络ACL	x	√	√
添加网络ACL规则	x	√	√
修改网络ACL规则	x	√	√
删除网络ACL规则	x	√	√
创建对等连接	x	√	√
修改对等连接	x	√	√
删除对等连接	x	√	√
查询对等连接	√	√	√
接受对等连接	x	√	√
拒绝对等连接	x	√	√
创建路由表	x	√	√
删除路由表	x	√	√
修改路由表	x	√	√
将路由表关联至子网	x	√	√

操作	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
添加路由	x	√	√
修改路由	x	√	√
删除路由	x	√	√

1.7 基本概念

1.7.1 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。

- 默认情况下，同一个VPC中，不同子网内的所有实例网络互通。同一个VPC内的子网可以位于不同可用区，不影响通信。比如VPC-A内有子网A01（可用区A）和子网A02（可用区B），子网A01和子网A02的网络默认互通。
- 子网创建成功后，不支持修改网段，请提前合理规划好子网网段。同一个虚拟私有云内的子网网段不可重复。

  子网的网段必须在VPC网段范围内，子网网段的掩码长度范围是：所在VPC的掩码位数至28位，比如VPC网段为10.0.0.0/16，VPC的掩码为16，则子网的掩码可在16~28范围内选择。

  比如VPC-A的网段为10.0.0.0/16，则您可以规划子网A01的网段为10.0.0.0/24，子网A02的网段为10.0.1.0/24，子网A03的网段为10.0.2.0/24。

  说明

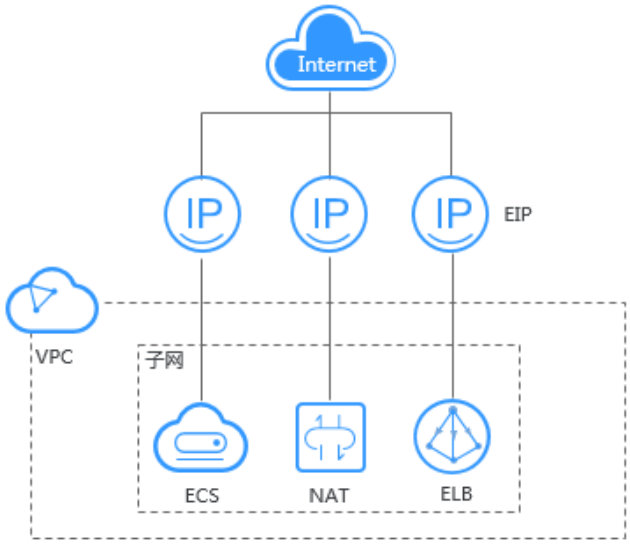
  一个用户在单个区域可创建的虚拟私有云数量默认为5个，如果您需要提升配额，请参见《虚拟私有云用户指南》的“什么是配额？”章节。

1.7.2 弹性公网 IP

弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。

一个弹性公网IP只能绑定一个云资源使用。

图 1-2 通过 EIP 访问公网



1.7.3 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VPC终端节点时，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1-4**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 1-4 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
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

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。

1.7.4 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。允许用户将弹性公网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）。

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

1.7.5 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。

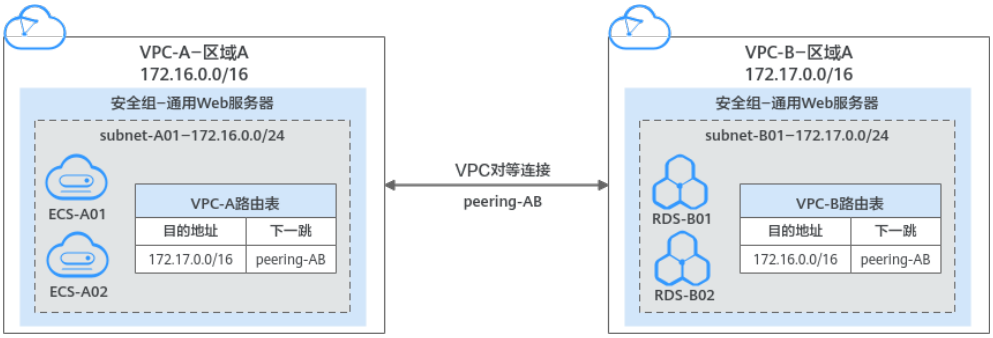
1.7.6 对等连接

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。

接下来，通过图1-3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。

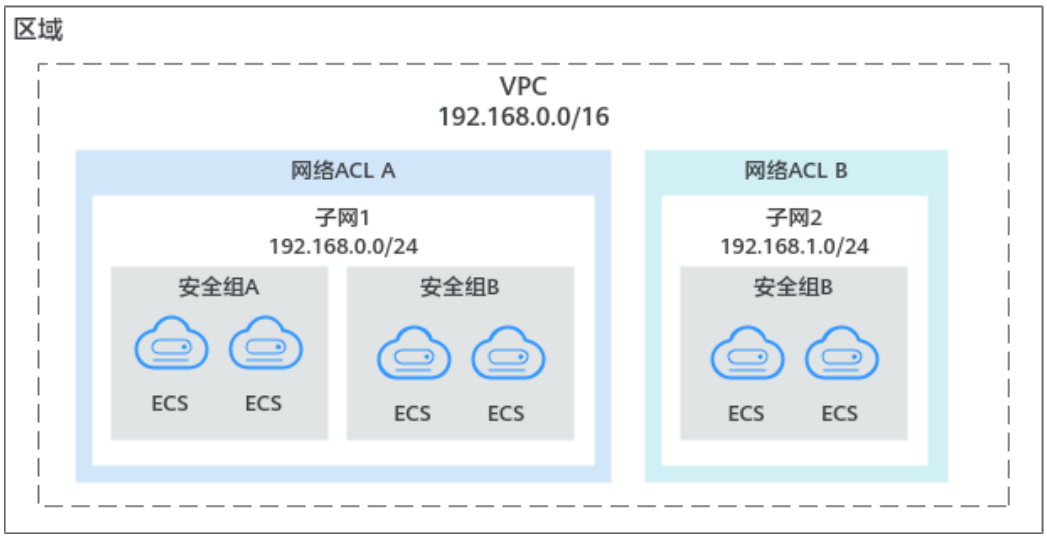
图 1-3 对等连接组网示意图



1.7.7 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 1-4 安全组与网络 ACL



1.7.8 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，以及弹性公网IP等网络接入。

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

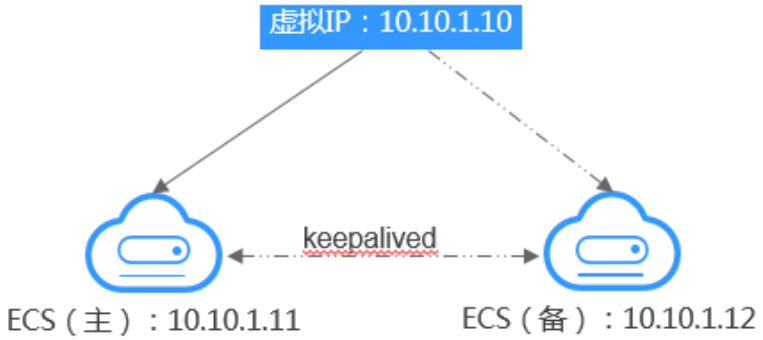
典型组网

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 1-5 HA 高可用性模式组网图

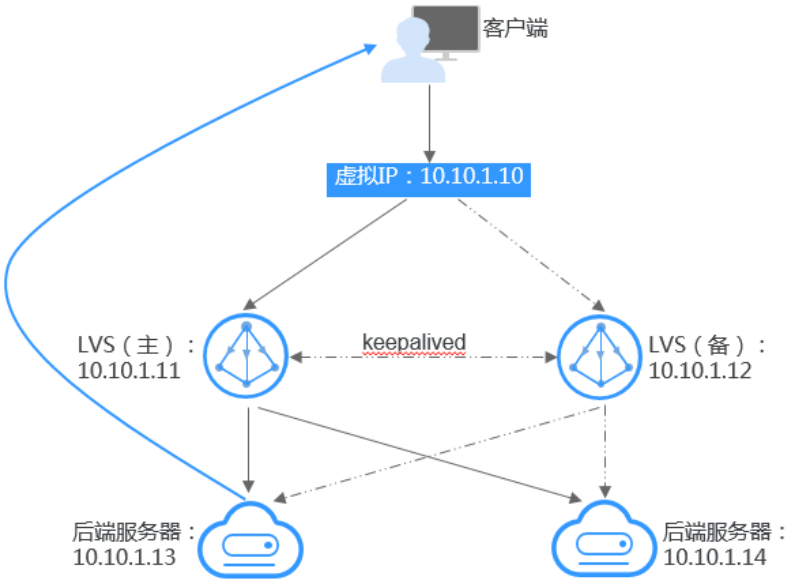


- 将2台同子网的弹性云服务器绑定同一个虚拟IP。
- 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **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 1-6 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：通过弹性公网IP访问虚拟IP。

  您的应用需要具备高可用性并通过Internet对外提供服务，推荐使用弹性公网IP绑定虚拟IP功能。

- 场景二：通过对等连接访问虚拟IP。

  您的应用需要具备高可用性并且需要通过Internet访问，同时需要通过其他VPC访问（对等连接）。

1.7.9 区域和可用区

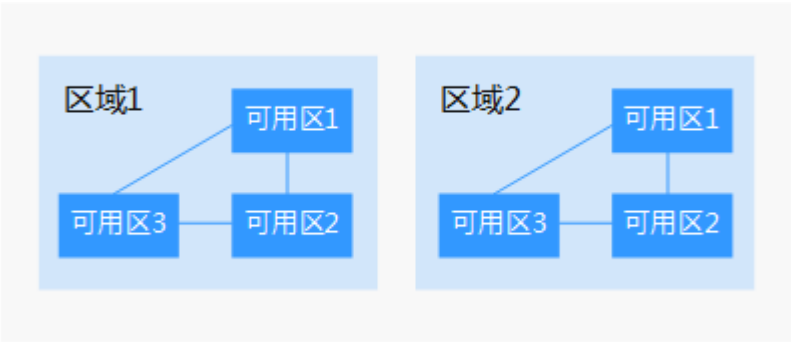
什么是区域、可用区?

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1-7阐明了区域和可用区之间的关系。

图 1-7 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 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。

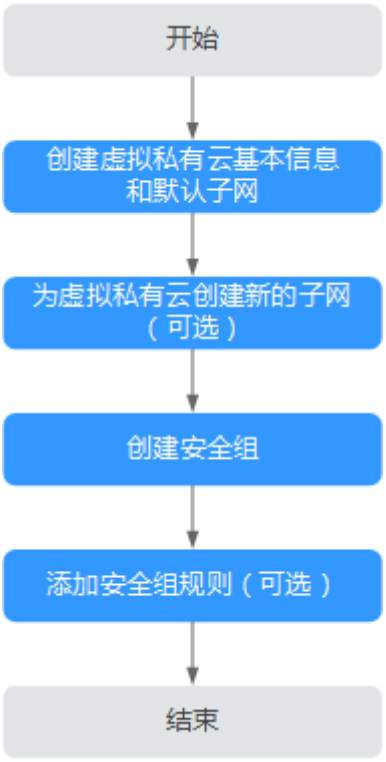
- 当弹性云服务器无需访问公网时，例如用于搭建网站的数据库节点或服务器节点的弹性云服务器无需连接公网，该类型弹性云服务器的虚拟私有云配置请参考**配置无需访问公网的弹性云服务器的VPC**。
- 当弹性云服务器需要访问公网时可通过配置弹性公网IP实现，例如用于搭建网站时允许接受访客通过网络访问的业务节点，该类型弹性云服务器的虚拟私有云配置请参考**配置通过弹性公网IP访问公网的弹性云服务器的VPC**。
- 当您需要访问Internet上的IPv6服务或为使用IPv6终端的用户提供访问服务时，需要在配置时开启IPv6功能，开启后，您将拥有IPv4和IPv6两个网段，可以为IPv4和IPv6终端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

2.2 配置无需访问公网的弹性云服务器的 VPC

2.2.1 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。

2.2.2 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、申请弹性公网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”。
4. 在“创建虚拟私有云”页面，根据界面提示配置参数。
   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 参数说明

分类	参数	说明	取值样例
基本信息	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。	-
基本信息	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-001

分类	参数	说明	取值样例
基本信息	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
基本信息	高级配置	单击下拉箭头，可配置VPC的高级参数等。	默认配置
基本信息	描述	VPC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“>”。	-
子网配置	可用区	VPC子网的可用区。	sa-fb-1
子网配置	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-001
子网配置	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
子网配置	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。	-
子网配置	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
子网配置	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
子网配置	网关	子网的网关。	192.168.0.1
子网配置	DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x
子网配置	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“>”。	-

5. 单击“立即创建”。

2.2.3 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。

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 2-3 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。	-
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 可用区设置规则说明如下： ● 同一个VPC内的子网可用区不用保持一致。比如子网A位于可用区1，子网B位于可用区3。 ● 使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。	sa-fb-1
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
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。	-
网关	子网的网关。	192.168.0.1

参数	说明	取值样例
DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x

6. 单击“确定”。

注意事项

子网创建成功后，有以下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
- 192.168.0.255：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。

2.2.4 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，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

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 2-4 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
模板	必选参数。 模板自带安全组规则，方便您快速创建安全组。提供如下几种模板： ● 自定义：用户自定义安全组规则。 ● 通用Web服务器：默认会配置放通22、3389、80、443端口和ICMP协议。 ● 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。	通用Web服务器
描述	可选参数。 安全组的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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”。

2.2.5 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，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

在安全组内添加安全组规则

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 > 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 2-5 入方向规则参数说明

参数	说明	取值样例
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	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。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0 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 2-6 出方向参数说明

参数	说明	取值样例
协议/应用	网络协议。目前支持“All”、“TCP”、“UDP”和“ICMP”等协议。	TCP
端口和目的地址	端口：允许弹性云服务器访问远端地址的指定端口，取值范围为：1～65535。	22或22-30

参数	说明	取值样例
	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： ● xxx.xxx.xxx.xxx/32（IPv4地址） ● xxx.xxx.xxx.0/24（子网） ● 0.0.0.0/0（任意地址） ● sg-abc（安全组）	0.0.0.0/0
描述	安全组规则的描述信息，非必填项。 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。

2.3 配置通过弹性公网 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”。
4. 在“创建虚拟私有云”页面，根据界面提示配置参数。
   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 2-7 参数说明

分类	参数	说明	取值样例
基本信息	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。	-
基本信息	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-001
基本信息	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

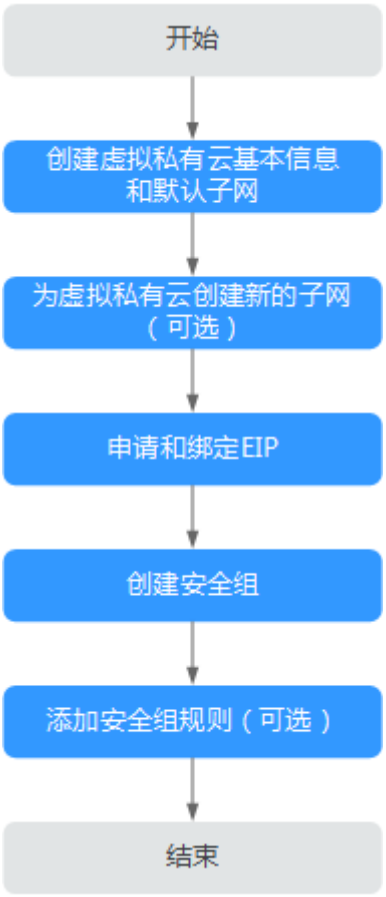
分类	参数	说明	取值样例
基本信息	高级配置	单击下拉箭头，可配置VPC的高级参数等。	默认配置
基本信息	描述	VPC的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
子网配置	可用区	VPC子网的可用区。	sa-fb-1
子网配置	名称	子网的名称。 名称只能由英文字母、数字、“_”、“-”和“.”组成，且不能有空格，长度不能大于64个字符。	Subnet-001
子网配置	子网IPv4网段	子网的地址范围，需要在VPC的地址范围内。	192.168.0.0/24
子网配置	子网IPv6网段	选择是否勾选开启IPv6。 开启IPv6功能后，将自动为子网分配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。	-
子网配置	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
子网配置	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
子网配置	网关	子网的网关。	192.168.0.1
子网配置	DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x
子网配置	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“>”。	-

5. 单击“立即创建”。

2.3.1 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，可以通过绑定弹性公网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2-8**所示。

表 2-8 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。
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。
申请和绑定弹性公网IP	必选任务。 可以通过申请弹性公网IP并将弹性公网IP绑定到上，实现弹性云服务器访公网的目的。

任务	说明
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。

2.3.2 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、申请弹性公网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”。
4. 在“创建虚拟私有云”页面，根据界面提示配置参数。
   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 2-9 参数说明

分类	参数	说明	取值样例
基本信息	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。	-

分类	参数	说明	取值样例
基本信息	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-001
基本信息	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
基本信息	高级配置	单击下拉箭头，可配置VPC的高级参数等。	默认配置
基本信息	描述	VPC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“>”。	-
子网配置	可用区	VPC子网的可用区。	sa-fb-1
子网配置	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-001
子网配置	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
子网配置	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。	-
子网配置	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
子网配置	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
子网配置	网关	子网的网关。	192.168.0.1
子网配置	DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x

分类	参数	说明	取值样例
子网配置	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“>”。	-

5. 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。

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 2-10 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。	-
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 可用区设置规则说明如下： ● 同一个VPC内的子网可用区不用保持一致。比如子网A位于可用区1，子网B位于可用区3。 ● 使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。	sa-fb-1
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

参数	说明	取值样例
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。	-
网关	子网的网关。	192.168.0.1
DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x

6. 单击“确定”。

注意事项

子网创建成功后，有以下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
- 192.168.0.255：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：为弹性云服务器申请和绑定弹性公网 IP

操作场景

可以通过申请弹性公网IP并将弹性公网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。

申请弹性公网 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 > 弹性公网IP”
3. 在“弹性公网IP”界面，单击“创建弹性公网IP”。
4. 根据界面提示配置参数。

表 2-11 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： ● 独享带宽：独享带宽只能针对一个弹性公网IP进行限速。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公网IP进行集中限速，可以加入多个弹性公网IP，被多个弹性公网IP地址共用。适用于多业务流量错峰分布场景。	独享带宽
带宽大小	带宽大小，单位Mbit/s。	100
弹性公网IP名称	弹性公网IP的名称。	eip-test
带宽名称	带宽的名称。	bandwidth
规格	弹性公网IP地址所连接的外部网络	5_bgp
数量	弹性公网IP数量。	1

5. 单击“立即申请”。
6. 单击“提交”。

绑定弹性公网 IP

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

2.3.5 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，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

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 2-12 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
模板	必选参数。 模板自带安全组规则，方便您快速创建安全组。提供如下几种模板： ● 自定义：用户自定义安全组规则。 ● 通用Web服务器：默认会配置放通22、3389、80、443端口和ICMP协议。 ● 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。	通用Web服务器
描述	可选参数。 安全组的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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”。

2.3.6 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，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

在安全组内添加安全组规则

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 > 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 2-13 入方向规则参数说明

参数	说明	取值样例
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	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。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0 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。
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。

3 虚拟私有云和子网

3.1 虚拟私有云

3.1.1 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、申请弹性公网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”。
4. 在“创建虚拟私有云”页面，根据界面提示配置参数。
   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 3-1 参数说明

分类	参数	说明	取值样例
基本信息	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。	-

分类	参数	说明	取值样例
基本信息	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-001
基本信息	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
基本信息	高级配置	单击下拉箭头，可配置VPC的高级参数等。	默认配置
基本信息	描述	VPC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“>”。	-
子网配置	可用区	VPC子网的可用区。	sa-fb-1
子网配置	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-001
子网配置	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
子网配置	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。	-
子网配置	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
子网配置	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
子网配置	网关	子网的网关。	192.168.0.1
子网配置	DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x

分类	参数	说明	取值样例
子网配置	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“>”。	-

5. 单击“立即创建”。

3.1.2 为虚拟私有云添加 IPv4 扩展网段

操作场景

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

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。
- 不支持添加的扩展网段范围如**表3-2**所示。

表 3-2 不支持添加的扩展网段范围

网段类型	不支持的网段范围
私有网段预留地址	• 172.31.0.0/16 • 192.168.0.0/16 • 主网段已使用的私网网段
系统内部预留地址	• 100.64.0.0/10 • 214.0.0.0/7 • 198.18.0.0/15 • 169.254.0.0/16

网段类型	不支持的网段范围
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”。

3.1.3 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**

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

3.1.4 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。

3.1.5 查看虚拟私有云拓扑图

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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绑定弹性公网IP、更改ECS的安全组。

3.1.6 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。

3.1.7 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。

3.1.8 删除虚拟私有云

操作场景

当您的虚拟私有云不需要使用时，您可以参考以下操作删除。

约束与限制

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

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 子网

3.2.1 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。

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 3-3 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。	-
可用区	可用区是指在同一地域内，电力和网络互相独立的物理区域。在同一VPC网络内可用区与可用区之间内网互通，可用区之间能做到物理隔离。 可用区设置规则说明如下： ● 同一个VPC内的子网可用区不用保持一致。比如子网A位于可用区1，子网B位于可用区3。 ● 使用子网的云资源，其可用区和子网的可用区不用保持一致。比如位于可用区1的云服务器，可以使用可用区3的子网。	sa-fb-1
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
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。	-
网关	子网的网关。	192.168.0.1
DNS服务器地址	默认配置了2个DNS服务器地址，您可以根据需要修改。多个IP地址以英文逗号隔开。	100.125.x.x

6. 单击“确定”。

注意事项

子网创建成功后，有以下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
- 192.168.0.255：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。

3.2.2 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 3-4 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

6. 单击“确定”。

3.2.3 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、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、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 3-5 删除子网内的云服务资源

云服务资源类型	操作指导
弹性云服务器	当前不支持通过子网页面直接跳转到目标弹性云服务器，您需要在弹性云服务器列表中，查找目标云服务器并删除。 1. 在弹性云服务器列表中，单击名称超链接。进入弹性云服务器详情页面。 2. 在详情页面的“网卡”区域，查看弹性云服务器关联的子网名称。
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”。

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

3.2.4 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？**。

3.2.5 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. 在子网列表页，单击右上角的。
   系统会将您账号下，当前区域的所有子网信息自动导出为Excel文件，并下载至本地。

3.2.6 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(ECS、ELB、NAT网关)占用而导致无法删除，需要您根据控制台的提示信息删除占用子网的资源，然后删除子网。

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。

3.3 管理 IPv4/IPv6 双栈网络

IPv4/IPv6 双栈网络介绍

IPv4/IPv6双栈网络，表示为您的实例提供两个版本的IP地址，包括IPv4 IP地址和IPv6 IP地址。以ECS为例，IPv4/IPv6双栈网络架构如**图3-1**所示。

图 3-1 IPv6 双栈网络架构图(VPC/EIP)

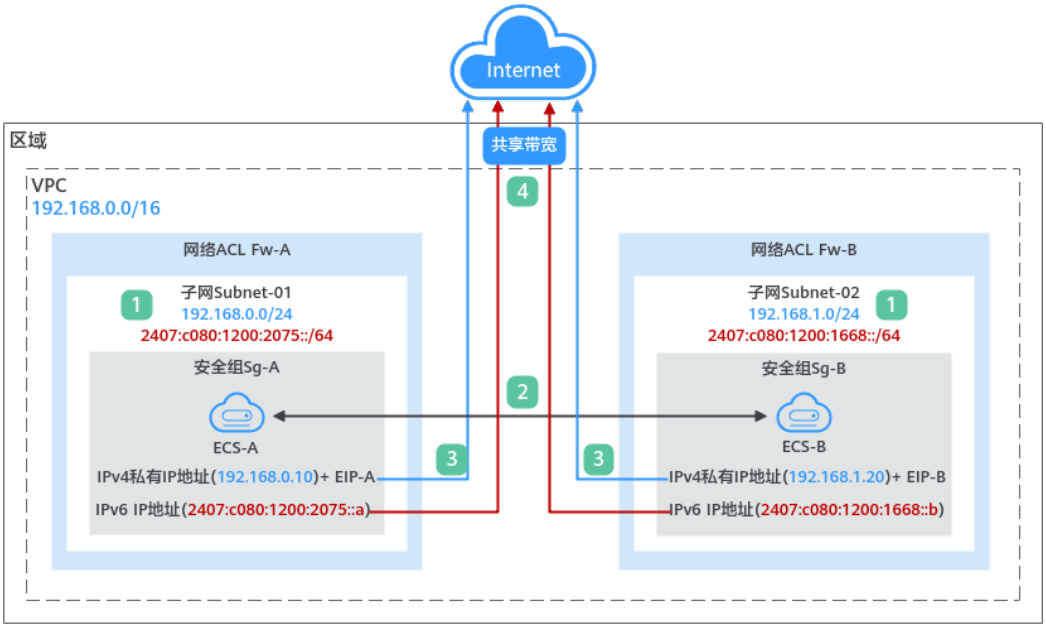


表 3-6 IPv6 双栈网络构建说明(VPC/EIP)

步骤	说明
1	在创建虚拟私有云VPC子网时，开启IPv6功能，则系统会自动为子网分配IPv6网段，当前不支持自定义IPv6网段。

步骤	说明
2	相同VPC内的不同子网之间网络默认互通，网络ACL可以防护子网的网络安全，安全组防护实例的网络安全。 1. 不同网络ACL之间网络隔离，如果两个子网关联了不同的网络ACL，则需要添加规则放通不同的网络ACL。 2. 不同安全组之间网络隔离，实例都必须关联安全组，如果两个实例关联了不同的安全组，则需要添加规则放通不同的安全组。 当网络ACL和安全组均放通后，实例之间可以内网互通，即ECS-A和ECS-B通过内网可以互相通信。 ● 使用IPv4私有IP地址，实现ECS内网通信。 ● 使用IPv6 IP地址，实现双栈ECS内网通信。
3	实现IPv4公网通信时，需要创建弹性公网IP(EIP)，并将EIP绑定到实例上。一个EIP可以绑定一个实例。 比如，将EIP-A绑定至ECS-A，ECS-A可以通过EIP-A连通公网。将EIP-B绑定至ECS-B，ECS-B可以通过EIP-B连通公网。
4	实现IPv6公网通信时，需要创建EIP共享带宽，并将实例的IPv6地址添加至共享带宽即可。一个共享带宽中可以添加多个IP。 比如，将ECS-A和ECS-B的IPv6地址分别添加至共享带宽中，ECS-A和ECS-B可以通过IPv6地址连通公网。

IPv6 网络操作指导

IPv6网络的操作与IPv4网络基本相同，仅部分功能配置存在差异，**表3-7**中为您提供IPv6网络配置指导。

表 3-7 IPv6 网络操作指导

操作场景	说明	指导
创建IPv6子网	创建子网时，勾选“开启IPv6”，则系统会自动为子网分配IPv6网段。 ● 暂不支持自定义IPv6网段。 ● 子网的IPv6功能开启后暂不支持关闭。 ● 对于已创建完成的子网，如果未开启IPv6功能，您可以选择开启。	**为虚拟私有云创建新的子网**
查看子网中已使用的IPv6地址	在子网列表中单击子网名称，在“IP地址管理”页签可以查看已经使用的IPv4地址和IPv6地址。	**查看子网内IP地址的用途**
添加IPv6安全组规则	添加安全组规则时，类型选择“IPv6”，源地址/目的地址填写IPv6地址。	**添加安全组规则**
添加IPv6网络ACL规则	添加网络ACL规则时，类型选择“IPv6”，源地址/目的地址填写IPv6地址。	**添加网络ACL规则**

操作场景	说明	指导
创建IPv6弹性公网IP	在创建EIP时，勾选“IPv6转换”，或者在EIP列表中，为已有IPv4 EIP执行“开启IPv6转换”操作。开启IPv6转换后，则系统为您提供IPv4和IPv6 EIP地址。	**管理IPv6弹性公网IP**
将IPv6弹性公网IP/IPv6地址添加到公网带宽中	创建共享带宽后，你可以将IPv6 EIP地址或者实例的IPv6地址添加到共享带宽中。	**添加弹性公网IP到共享带宽**
在VPC路由表中添加IPv6自定义路由	添加自定义路由时，目的地址和下一跳地址可以配置IPv4网段或IPv6网段。 • 如果目的地址是IPv6网段，则下一跳地址暂时只能使用同一VPC内的地址。 • 路由的目的地址为IPv6网段时，对应下一跳类型仅支持ECS实例、扩展网卡、虚拟IP，同时下一跳资源需要具备IPv6地址。	**添加自定义路由**
申请IPv6虚拟IP地址	当VPC子网开启IPv6后，申请虚拟IP时，类型可以选择“IPv6”。	**申请虚拟IP地址**

4 路由表

4.1 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VPC终端节点时，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4-1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 4-1 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
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

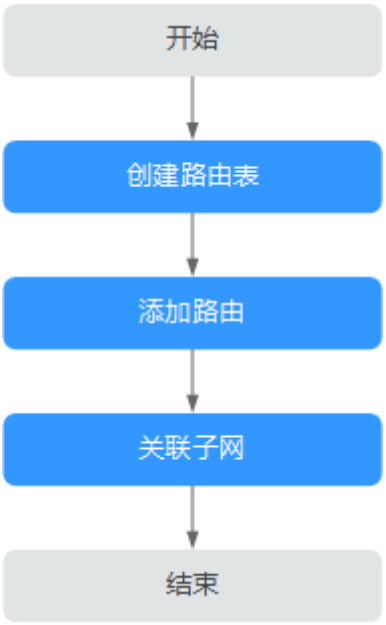
说明

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。

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4-1所示。

图 4-1 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。

4.2 管理路由表

4.2.1 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 4-2 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。

4.2.2 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。
6. 单击“确定”，完成关联。

4.2.3 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。

4.2.4 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。

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。

4.2.5 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。

4.2.6 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. 在路由表列表页，单击右上角的  。
   系统会将您账号下，当前区域的所有路由表信息自动导出为Excel文件，并下载至本地。

4.2.7 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。

4.3 管理路由

4.3.1 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 4-3 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”。 **须知** • 目的地址不能与已有路由的目的地址冲突。 • 如果IP地址中存在“起始IP-末尾IP”形式的网段，则不支持。 不支持IP地址示例：192.168.0.1-192.168.0.62，请修改成IP网段/掩码的形式，比如192.168.0.0/26。	IPv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。	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。

4.3.2 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。

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 4-4 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”。 **须知** • 目的地址不能与已有路由的目的地址冲突。 • 如果IP地址中存在“起始IP-末尾IP”形式的网段，则不支持。 不支持IP地址示例：192.168.0.1-192.168.0.62，请修改成IP网段/掩码的形式，比如192.168.0.0/26。	IPv4: 192.168.0.0/16
下一跳类型	必选参数。 选择下一跳资源类型。	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”。

4.3.3 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4-5。

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。

表 4-5 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

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
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”。

4.3.4 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。

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。
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。

4.4 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公网IP**。
   - 为弹性云服务器的虚拟IP绑定EIP，详情请参见**为虚拟IP地址绑定弹性公网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。

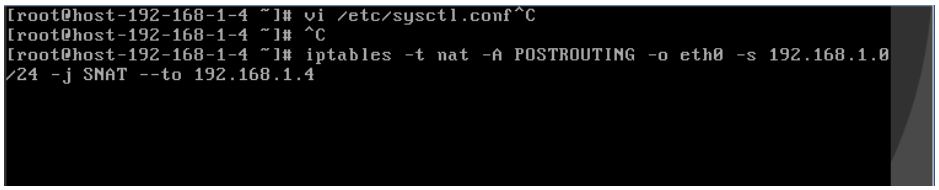
    sysctl -p /etc/sysctl.conf

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4-2**所示。

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

    图 4-2 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

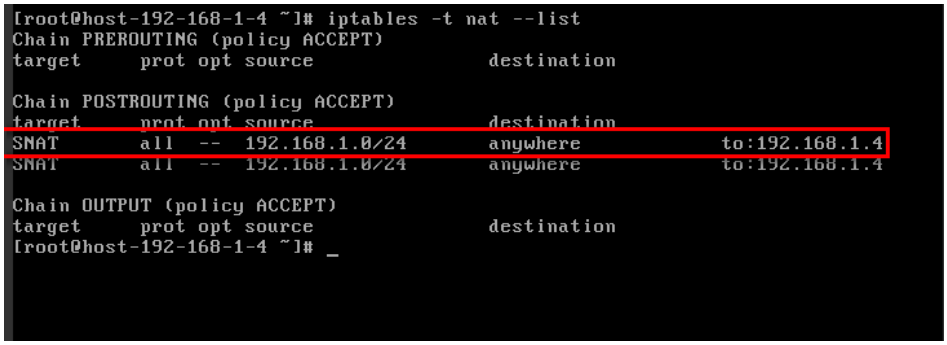
    4. 执行以下命令添加rc.local文件的执行权限。

       # chmod +x /etc/rc.local

14. 执行如下命令，查看是否配置成功。如**图4-3**所示，则表示配置成功（例如：192.168.1.0/24）。

    iptables -t nat --list

图 4-3 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。

5 虚拟 IP

5.1 虚拟 IP 概述

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，以及弹性公网IP等网络接入。

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

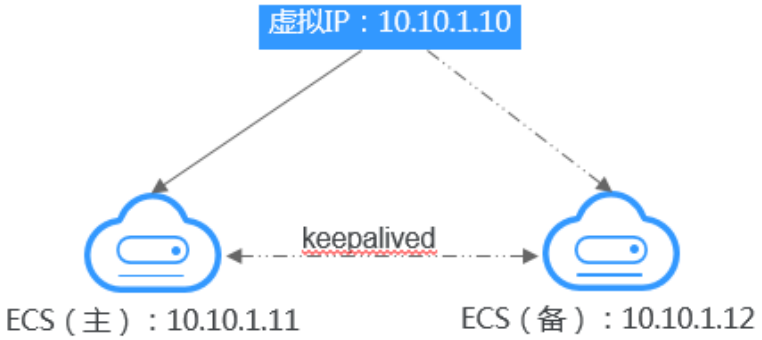
典型组网

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 5-1 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。

应用场景

- 场景一：通过弹性公网IP访问虚拟IP。

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

5.2 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”页签中，单击“申请虚拟IP地址”。
6. 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。
7. 选择手动分配方式，请填写虚拟IP地址。
8. 单击“确定”。

在IP列表中可以查看申请的虚拟IP地址。

5.3 为虚拟 IP 地址绑定弹性公网 IP 或弹性云服务器

操作场景

您可以通过虚拟IP和弹性公网IP实现以下场景：

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

约束与限制

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

  说明

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

登录控制台为虚拟 IP 绑定弹性公网 IP 或弹性云服务器

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

- 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。

5.4 为弹性公网 IP 绑定虚拟 IP 地址

操作场景

本章节指导用户为弹性公网IP绑定虚拟IP地址。

前提条件

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

操作步骤

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

5.5 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. 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。

5.6 为虚拟 IP 解绑弹性公网 IP

操作场景

本章节指导用户解绑虚拟IP上的弹性公网IP。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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“解绑弹性公网IP”。
   弹出解绑确认对话框。
7. 确认无误后，单击“是”，将虚拟IP和弹性公网IP解绑。

5.7 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5-1**。

表 5-1 虚拟 IP 无法删除原因说明

提示信息	原因说明及处理方法
已绑定实例或弹性公网IP地址，无法执行删除操作，请先执行对应解绑操作。	当前虚拟IP可能被弹性公网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： ● 弹性公网IP：请参见**为虚拟IP解绑弹性公网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。
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。
6. 确认无误后，单击“是”，删除虚拟IP地址。

5.8 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。

5.9 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”。

6 弹性网卡和辅助弹性网卡

6.1 弹性网卡

6.1.1 弹性网卡概述

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

弹性网卡类型

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

应用场景

- 灵活迁移

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

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

6.1.2 创建弹性网卡

操作场景

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

约束与限制

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

说明

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

操作步骤

1. 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 > 弹性网卡”。
4. 单击“创建弹性网卡”。
5. 配置弹性网卡参数，如表6-1所示。

表 6-1 参数说明

参数	参数说明	取值样例
名称	弹性网卡的名称，必填项。 弹性网卡的名称只能由英文字母、数字、下划线、中划线、点组成，且不能有空格，长度不能大于64个字符。	networkInterface-891e
虚拟私有云	选择弹性网卡归属的VPC，必填项。	vpc-001
子网	选择弹性网卡归属的子网，必填项。	subnet-001
私有IP地址	选择是否自动分配私有IP地址。	-
安全组	选择弹性网卡所属安全组。	sg-001

6. 单击“确定”，完成创建。

6.1.3 查看弹性网卡基本信息

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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 > 弹性网卡”。
4. 在弹性网卡列表页，单击需要查看详情的弹性网卡名称。

其他操作

在弹性网卡详情页可以修改以下信息：

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

6.1.4 绑定弹性网卡到云服务器实例

操作场景

通过将弹性网卡与弹性云服务器绑定，可以实现灵活、高可用的网络方案配置。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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 > 弹性网卡”。
4. 在弹性网卡列表页，单击操作列的“绑定实例”，选择需要绑定的云服务器实例。
5. 单击“确定”，完成绑定。

6.1.5 绑定弹性网卡到弹性公网 IP

操作场景

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

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

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

操作步骤

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

4. 在弹性网卡列表页，单击操作列的“绑定弹性公网IP”，选择需要绑定的弹性公网IP。
5. 单击“确定”，完成绑定。

6.1.6 绑定弹性网卡到虚拟 IP

操作场景

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

未绑定云服务器实例的弹性网卡不能绑定虚拟IP。

更多虚拟IP信息请参见**虚拟IP概述**。

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

6.1.7 解绑定云服务器或弹性公网 IP

操作场景

本章节指导您如何将弹性网卡与云服务器或弹性公网IP进行解绑。

约束与限制

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

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 > 弹性网卡”。
4. 在弹性网卡列表页，单击操作列的“解绑实例”或“解绑弹性公网IP”。
5. 单击“是”，完成解绑。
   解绑弹性公网IP时，可选择同时释放该弹性公网IP。

6.1.8 更改弹性网卡所属安全组

操作场景

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

操作步骤

在弹性网卡列表页，更改所属安全组

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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 > 弹性网卡”。
4. 在弹性网卡列表页，单击操作列的“更多 > 更改安全组”。
5. 在“更改安全组”页面勾选需要关联的安全组，单击“确定”，完成更改。

在弹性网卡详情页，更改所属安全组

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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 > 弹性网卡”。
4. 单击待修更改安全组的弹性网卡名称，进入弹性网卡详情页。
5. 在“关联安全组”页签下，单击“更改安全组”。
6. 在“更改安全组”页面勾选需要关联的安全组，单击“确定”，完成更改。

更多操作

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

6.1.9 删除弹性网卡

操作场景

本章节指导用户删除不再使用的弹性网卡资源。

约束与限制

- 主弹性网卡跟随实例一同创建，您不能直接删除主弹性网卡，也不能解除主弹性网卡和实例的绑定关系，需要删除主弹性网卡绑定的实例，该网卡将被同步删除。

- 当扩展弹性网卡已绑定实例时，无法直接删除，请**解绑实例**后重试。
- 删除弹性网卡时，会同步删除弹性网卡绑定的辅助弹性网卡。
- 删除弹性网卡时，会解除网卡和弹性公网IP的绑定关系，您可以选择是否释放该弹性公网IP。
- 删除弹性网卡时，如果弹性网卡已被其他资源使用，会同步删除关联资源中使用弹性网卡的条目，删除操作无法恢复，请谨慎操作。

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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 > 弹性网卡”。
4. 在弹性网卡列表中，选择目标弹性网卡所在行的操作列下的“更多 > 删除”。

   弹出删除确认对话框。
5. 确认无误后，单击是，删除弹性网卡。

6.2 辅助弹性网卡

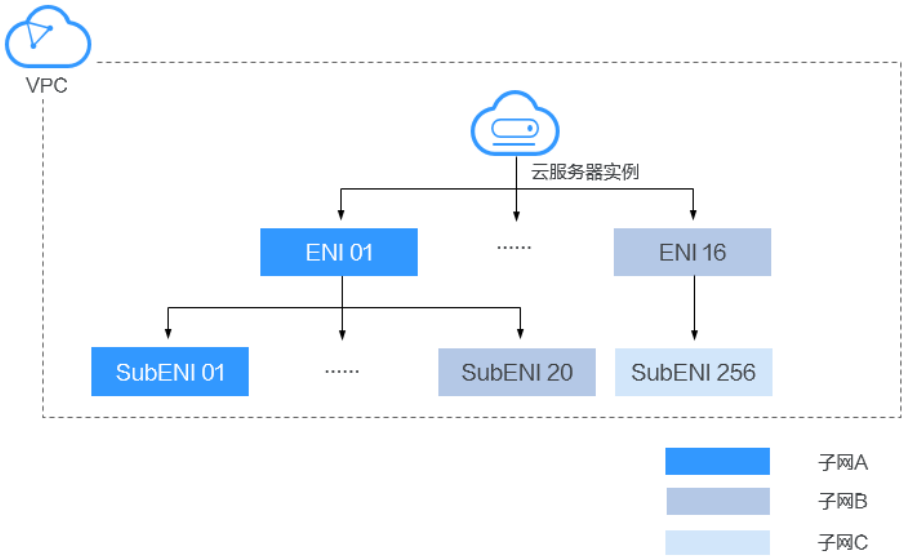
6.2.1 辅助弹性网卡概述

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

应用场景

辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，其组网示意图如**图6-1**所示。

图 6-1 辅助弹性网卡示意图



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

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

约束与限制

- 单个云服务器实例支持绑定的辅助弹性网卡实例上限为256个，但不是所有规格的云服务器实例均支持绑定256个辅助弹性网卡，具体可绑定的辅助弹性网卡数量由云服务器实例规格决定。
- 云服务器实例不支持通过辅助弹性网卡的私网IP使用CloudInit。
- 辅助弹性网卡不支持绑定虚拟IP。
- 不支持单独收集辅助弹性网卡的流日志，辅助弹性网卡的流日志信息跟随所属的弹性网卡一同生成。

6.2.2 创建辅助弹性网卡

操作场景

当云服务器实例所需挂载的网卡超出弹性网卡的上限时，您可以参考本章节创建辅助弹性网卡，为云服务器实例挂载更多网卡，实现灵活、高可用的网络方案配置。

约束与限制

- 辅助弹性网卡与所属的弹性网卡必须在同一个虚拟私有云，可以属于不同子网以及安全组。
- 使用辅助弹性网卡时，您需要在云服务器实例的网卡上创建VLAN子接口并配置对应规则，具体请参见**配置辅助弹性网卡**。

创建辅助弹性网卡

1. 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 > 弹性网卡”。
4. 在页面右上角，单击“创建辅助弹性网卡”。
5. 配置辅助弹性网卡参数，如表6-2所示。

表 6-2 参数说明

参数	参数说明	取值样例
所属弹性网卡	辅助弹性网卡所挂载的弹性网卡。 您可以通过下拉列表框选择支持挂载辅助弹性网卡的弹性网卡。	--(172.16.0.145)
所属VPC	辅助弹性网卡归属的VPC，无需填写。	vpc-A
所属子网	选择辅助弹性网卡归属的子网。	subnet-A01
描述	辅助弹性网卡的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-
创建数量	待创建的辅助弹性网卡的数量，取值范围为1~20。	1
私有IP地址	选择是否为辅助弹性网卡分配私有IPv4地址，私有IP地址仅支持内网请求。 当前版本不支持去勾选。	-
IPv4地址	选择私有IP地址的分配方式： • 自动分配IP地址：系统自动分配IP地址。 • 手动指定IP地址：系统按指定的IP地址进行分配。 若选择“手动指定IP地址”，则填写IPv4的私有IP地址。	自动分配IP地址
安全组	选择辅助弹性网卡所属安全组。	sg-001

6. 单击“确定”，完成创建。

须知

辅助网卡创建完成后不能直接使用，您还需要**配置辅助弹性网卡**，在云服务器实例的网卡上创建VLAN子接口并配置对应规则。

配置辅助弹性网卡

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

在配置之前，您需要获取辅助弹性网卡的信息，如**表6-3**所示。

表 6-3 辅助弹性网卡信息

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

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

在本示例中：

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

配置步骤

1. 登录云服务器实例。

   。
2. 为eth0创建VLAN子接口。

   ip link add link *eth0* **name** *eth0.2110* **type vlan id** *2110*
3. 创建命名空间“ns2110”。

   ip netns add *ns2110*
4. 将VLAN子接口“eth0.2110”加入命名空间“ns2110”。

   ip link set *eth0.2110* **netns** *ns2110*
5. 修改VLAN子接口的MAC地址为“*fa:16:3e:a1:b2:***”。

   ip netns exec *ns2110* **ifconfig** *eth0.2110* **hw ether** *fa:16:3e:a1:b2:***
6. 启动VLAN子接口。

   ip netns exec *ns2110* **ifconfig** *eth0.2110* **up**
7. 为VLAN子接口配置私网IP地址“*192.168.0.2/24*”。

   ip netns exec *ns2110* **ip addr add** *192.168.0.2/24* **dev** *eth0.2110*
8. 为VLAN子接口配置默认路由，其中“*192.168.0.1*”为辅助弹性网卡所在子网的网关。

   ip netns exec *ns2110* **ip route add default via** *192.168.0.1*

验证方法

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

   ip netns exec *ns2110* **ping** *a.b.c.d*

   图 6-2 成功示例

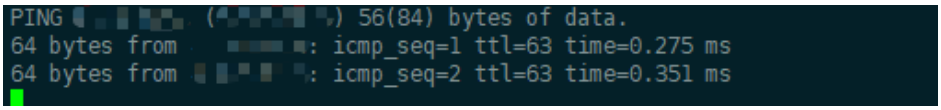
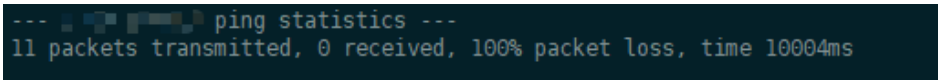
   

   图 6-3 失败示例

6.2.3 查看辅助弹性网卡基本信息

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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 > 弹性网卡”。
4. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
5. 在辅助弹性网卡列表中，单击需要查看详情的辅助“私有IP地址”，打开辅助弹性网卡的详情页。
   - “基本信息”页签：显示辅助弹性网卡的ID、所属弹性网卡、VLAN、所属VPC、所属子网、服务地址、MAC地址等信息。
   - “关联安全组”页签：显示辅助弹性网卡关联的安全组及其规则。

其他操作

在辅助弹性网卡详情页可以修改以下信息：

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

6.2.4 绑定/解绑定辅助弹性网卡到弹性公网 IP

操作场景

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

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

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

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

绑定操作

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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 > 弹性网卡”。
4. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
5. 在辅助弹性网卡列表，单击操作列的“绑定弹性公网IP”，选择需要绑定的弹性公网IP。
6. 单击“确定”，完成绑定。

解绑定操作

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

6.2.5 更改辅助弹性网卡所属安全组

操作场景

辅助弹性网卡创建完成后，您可以更改其所属的安全组。

更改辅助弹性网卡所属的安全组有两种方法：

- 在辅助弹性网卡列表中进行更改。

- 进入辅助弹性网卡详情页进行更改。

操作步骤

在辅助弹性网卡列表中，更改所属安全组

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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 > 弹性网卡”。
4. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
5. 在辅助弹性网卡列表中，单击操作列的“更改安全组”。
6. 在“更改安全组”页面勾选需要关联的安全组。
7. 单击“确定”，完成更改。

在辅助弹性网卡详情页，更改所属安全组

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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 > 弹性网卡”。
4. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
5. 单击待修更改安全组的辅助弹性网卡的“私有IP地址”，进入辅助弹性网卡详情页。
6. 在“关联安全组”页签下，单击“更改安全组”。
7. 在“更改安全组”页面勾选需要关联的安全组。
8. 单击“确定”，完成更改。

6.2.6 删除辅助弹性网卡

操作场景

您可以删除不再使用的辅助弹性网卡。

约束与限制

- 删除辅助弹性网卡时，会解除辅助弹性网卡和弹性网卡的绑定关系。
- 删除辅助弹性网卡时，会解除网卡和弹性公网IP的绑定关系，您可以选择是否释放该弹性公网IP。
- 删除辅助弹性网卡时，如果辅助弹性网卡已被其他资源使用，会同步删除关联资源中使用辅助弹性网卡的条目，删除操作无法恢复，请谨慎操作。
  比如，在VPC路由表中，存在自定义路由的下一跳是辅助弹性网卡，则删除辅助弹性网卡时，则会同步删除相关路由。

操作步骤

1. 登录管理控制台。

2. 在页面左上角单击☰图标，打开服务列表，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 > 弹性网卡”。
4. 在“弹性网卡”页面，选择“辅助弹性网卡”页签。
5. 在辅助弹性网卡列表中，单击操作列的“删除”。
6. 单击“是”，完成删除。
   删除辅助弹性网卡会同步清理云服务器实例上配置的VLAN子接口，无需单独删除。

7 访问控制

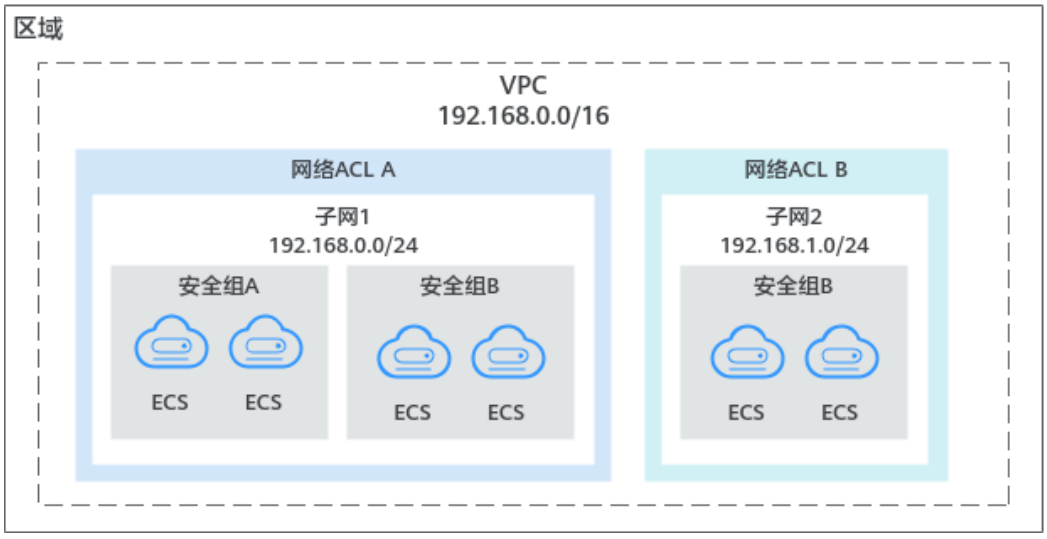
7.1 VPC 访问控制概述

虚拟私有云VPC是您在云上的私有网络，通过配置安全组和网络ACL策略，可以保障VPC内部署的实例安全运行，比如弹性云服务器、数据库、云容器等。

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

安全组和网络ACL的应用示例如图7-1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 7-1 安全组与网络 ACL



安全组与网络 ACL 的区别说明

表7-1为您提供了安全组和网络ACL的详细区别。

表 7-1 安全组和网络 ACL 区别

对比项	安全组	网络ACL
防护范围	实例级别：防护安全组内的实例，比如弹性云服务器、数据库、云容器实例等。	子网级别：防护整个子网，子网内的所有实例都会受到网络ACL的保护。
是否必选	必选，实例必须至少加入到一个安全组内。	非必选，您可以根据业务需求选择是否为子网关联网络ACL。
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。

7.2 安全组

7.2.1 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。

安全组规则

- 安全组中包括入方向规则和出方向规则，用来控制安全组内实例的入方向和出方向的网络流量。
  - 入方向规则：控制外部请求访问安全组内的实例，即流量流入实例。
  - 出方向规则：控制安全组内实例访问外部的请求，即流量从实例流出。
- 安全组规则由协议端口、源地址/目的地址等组成，关键信息说明如下：

- 协议端口：包括网络协议类型和端口范围。
  - 网络协议：匹配流量的协议类型，支持TCP、UDP、ICMP和GRE协议。
  - 端口范围：匹配流量的目的端口，取值范围为：1～65535。
- 源地址或目的地址：在入方向中，匹配流量的源地址。在出方向中，匹配流量的目的地址。

安全组及规则的工作原理

- 安全组是有状态的。如果您从实例发送一个出站请求，且该安全组的出方向规则是放通的话，那么无论其入方向规则如何，都将允许该出站请求的响应流量流入。同理，如果该安全组的入方向规则是放通的，那无论出方向规则如何，都将允许入站请求的响应流量可以流出。
- 安全组使用连接跟踪来标识进出实例的流量信息，入方向安全组的规则变更，对原有流量立即生效。出方向安全组规则的变更，不影响已建立的长连接，只对新建立的连接生效。

  当您在安全组内增加、删除、更新规则，或者在安全组内添加、移出实例时，系统会自动清除该安全组内所有实例入方向的连接，详细说明如下：
  - 由入方向流量建立的连接，已建立的长连接将会断开。所有入方向流量立即重新建立连接，并匹配新的安全组入方向规则。
  - 由出方向流量建立的连接，已建立的长连接不会断开，依旧遵循原有安全组规则。出方向流量新建立的连接，将会匹配新的安全组出方向规则。

须知

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

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

安全组的限制

- 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。

7.2.2 默认安全组和规则

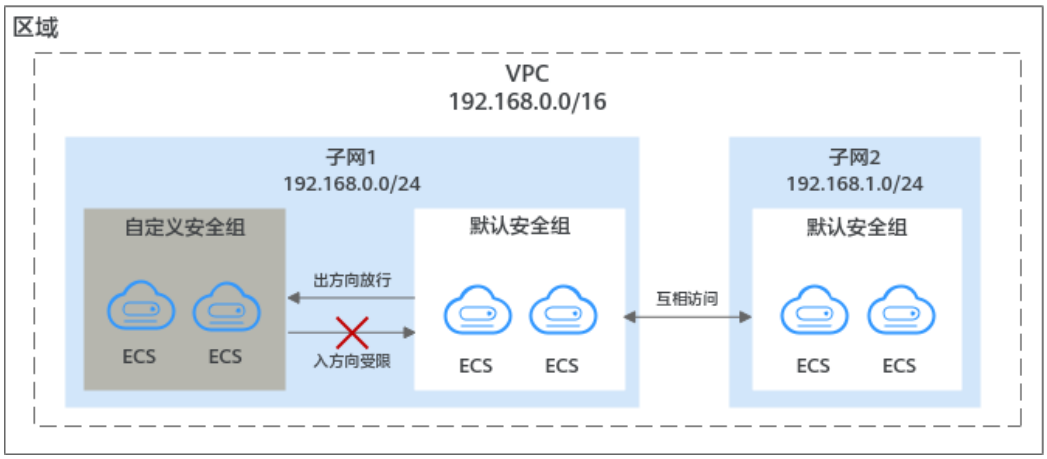
如果您未创建任何安全组，那么您在首次使用安全组时，系统会自动为您创建一个默认安全组。

默认安全组规则说明

默认安全组规则说明如下：

- 入方向规则：入方向流量受限，只允许安全组内实例互通，拒绝来自安全组外部的所有请求进入实例。
- 出方向规则：出方向流量放行，允许所有请求从安全组内实例流出。

图 7-2 默认安全组



默认安全组规则的详细说明如表7-2所示。

表 7-2 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。

7.2.3 安全组配置示例

当您在VPC子网内创建实例（云服务器、云容器、云数据库等）时，您可以使用系统提供的默认安全组default，您也可以创建其他安全组。无论是默认安全组，还是您创建的安全组，您均可以在安全组内设置出方向和入方向规则，以此控制出入实例的流量。以下为您介绍一些常用的安全组的配置示例：

- **通过本地服务器远程登录云服务器**
- **在本地服务器远程连接云服务器上传或者下载文件（FTP）**
- **在云服务器上搭建网站对外提供Web服务**
- **验证网络连通性**
- **实现不同安全组的实例内网网络互通**
- **云服务器提供数据库访问服务**

- 限制云服务器访问外部网站

使用须知

在配置安全组规则之前，您需要先了解以下信息：

- 不同安全组之间的实例默认网络隔离，无法互相访问。
- 安全组默认拒绝所有来自外部的请求，即本安全组内的实例网络互通，外部无法访问安全组内的实例。

  您需要遵循白名单原则添加安全组入方向规则，允许来自外部的特定请求访问安全组内的实例。
- 安全组的出方向规则一般默认全部放通，即允许安全组内的实例访问外部。

  如果出方向规则被删除，将会导致安全组内实例无法正常访问外部，您可以参考表7-3重新添加规则。

表 7-3 安全组默认出方向规则

方向	协议端口	目的地址	描述
出方向	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。

通过本地服务器远程登录云服务器

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

- 通过SSH远程登录Linux云服务器，需要放通SSH(22)端口，请参见表7-4。
- 通过RDP远程登录Windows云服务器，需要放通RDP(3389)端口，请参见表7-5。

表 7-4 通过 SSH 远程登录 Linux 云服务器

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

表 7-5 通过 RDP 远程登录 Windows 云服务器

方向	协议端口	源地址
入方向	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7-6**。

表 7-6 通过特定 IP 地址远程登录云服务器

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

在本地服务器远程连接云服务器上传或者下载文件（FTP）

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

表 7-7 在本地服务器远程连接云服务器上传或者下载文件

方向	协议端口	源地址
入方向	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，如果您在云服务器上搭建了可供外部访问的网站，则您需要在安全组入方向添加对应的规则，放通对应的端口，例如HTTP(80)、HTTPS(443)。

表 7-8 在云服务器上搭建网站对外提供 Web 服务

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

验证网络连通性

ICMP协议用于网络消息的控制和传递，因此在进行一些基本测试操作之前，需要开通ICMP协议访问端口。比如，您需要在某个个人PC上使用**ping**命令来验证云服务器的网络连通性，则您需要在云服务器所在安全组的入方向添加以下规则，放通ICMP端口。

表 7-9 使用 ping 命令验证网络连通性

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

实现不同安全组的实例内网网络互通

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

表 7-10 实现不同安全组的实例网络互通

方向	协议端口	源地址
入方向	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，允许其他实例通过内网访问数据库服务，则您需要在部署数据库服务器所在的安全组内，添加入方向规则，放通对应的端口，实现其他实例通过内网获取数据库数据的请求。常见的数据库类型机器对应的端口如下：

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

表 7-11 云服务器提供数据库访问服务

方向	协议端口	源地址	描述
入方向	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	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。

方向	协议端口	源地址	描述
入方向	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	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7-13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 7-12 限制云服务器访问外部网站

方向	协议端口	目的地址	描述
出方向	自定义 TCP: 80	IP地址：132.15.XX.XX	允许安全组内云服务器访问指定的外部网站，网站地址为http://132.15.XX.XX:80。
出方向	自定义 TCP: 443	IP地址：145.117.XX.XX	允许安全组内云服务器访问指定的外部网站，网站地址为https://145.117.XX.XX:443。

2. 其次，删除安全组出方向中原有放通全部流量的规则，如表7-13所示。

   表 7-13 安全组默认出方向规则

方向	协议端口	目的地址	描述
出方向	全部	0.0.0.0/0	针对全部IPv4协议，允许安全组内的实例可访问外部任意IP和端口。

7.2.4 管理安全组

7.2.4.1 创建安全组

操作场景

安全组实际是网络流量访问策略，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

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 7-14 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
模板	必选参数。 模板自带安全组规则，方便您快速创建安全组。提供如下几种模板： ● 自定义：用户自定义安全组规则。 ● 通用Web服务器：默认会配置放通22、3389、80、443端口和ICMP协议。 ● 开放全部端口：开放全部端口有一定安全风险，请谨慎选择。	通用Web服务器
描述	可选参数。 安全组的描述信息。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	-

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”。

7.2.4.2 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。

7.2.5 管理安全组规则

7.2.5.1 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，由入方向规则和出方向规则共同组成。您可以参考以下章节添加安全组规则，用来控制流入/流出安全组内实例（如ECS）的流量。

使用须知

- 配置安全组规则前，您需要规划好安全组内实例的访问策略，常见安全组规则配置案例请参见**安全组配置示例**。
- 安全组的规则数量有限制，请您尽量保持安全组内规则的简洁，详细约束请参见**安全组的限制**。
- 通常情况下，同一个安全组内的实例默认网络互通。当同一个安全组内实例网络不通时，可能情况如下：
  - 当实例属于同一个VPC时，请您检查入方向规则中，是否删除了同一个安全组内实例互通对应的规则，规则详情如**表7-15**所示。

表 7-15 安全组内实例互通规则

方向	协议端口	源地址/目的地址
入方向	全部	源地址：当前安全组（Sg-A）

- 不同VPC的网络不通，所以当实例属于同一个安全组，但属于不同VPC时，网络不通。
  您可以通过**VPC对等连接**连通不同区域的VPC。

在安全组内添加安全组规则

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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 7-16 入方向规则参数说明

参数	说明	取值样例
协议端口	安全组规则中用来匹配流量的网络协议类型，目前支持TCP、UDP、ICMP和GRE协议。	TCP
	安全组规则中用来匹配流量的目的端口，取值范围为：1～65535。 在入方向规则中，表示外部访问安全组内实例的指定端口。	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。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0 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 7-17 出方向参数说明

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

7.2.5.2 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。
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。
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。

7.2.5.3 在安全组中一键放通常见端口

操作场景

您可以通过使用该功能，在安全组中一键放通常见端口。适用于以下场景：

- 远程登录云服务器
- 在云服务器内使用ping命令测试网络连通性
- 云服务器用作Web服务器对外提供网站访问服务

您可以一键放通的常见端口详细说明如表7-18所示。

表 7-18 一键放通常见端口说明

方向	类型和协议端口	源地址/目的地址	规则用途
入方向	TCP: 22（IPv4）	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的SSH(22)端口，用于远程登录Linux云服务器。
	TCP: 3389（IPv4）	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的RDP(3389)端口，用于远程登录Windows云服务器。
	TCP: 80（IPv4）	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的HTTP(80)端口，用于通过HTTP协议访问网站。
	TCP: 443（IPv4）	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的HTTPS(443)端口，用于通过HTTPS协议访问网站。

方向	类型和协议端口	源地址/目的地址	规则用途
	TCP：20-21 (IPv4)	0.0.0.0/0	针对TCP(IPv4)协议，允许外部所有IP访问安全组内云服务器的FTP(20和21)端口，用于远程连接云服务器上传或者下载文件。
	ICMP: 全部 (IPv4)	0.0.0.0/0	针对ICMP(IPv4)协议，允许外部所有IP访问安全组内云服务器的所有端口，用于通过ping命令测试云服务器的网络连通性。
出方向	全部 (IPv4)	0.0.0.0/0	针对全部协议，允许安全组内的云服务器可访问外部任意IP和端口。

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击☰图标，打开服务列表，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，单击“一键放通常见端口”。
   弹出常见端口列表页面。
6. 根据界面提示，单击“确定”。
   完成操作后，可以在安全组规则列表页面查看添加的安全组规则。

7.2.5.4 修改安全组规则

操作场景

当安全组规则设置不满足需求时，您可以参考以下操作修改安全组中的规则，保证云服务器等实例的网络安全。您可以修改安全组规则的端口号、协议、IP地址等。

约束与限制

当您修改安全组规则前，请您务必了解该操作可能带来的影响，避免误操作造成网络中断或者引入不必要的网络安全问题。

安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。

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。

7.2.5.5 复制安全组规则

操作场景

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

操作步骤

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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。

7.2.5.6 导入和导出安全组规则

操作场景

您可以在Excel格式文件中填写安全组规则参数，并将规则导入到安全组内。同时，您可以将已有安全组的规则导出至Excel格式文件中。

当您遇到如下场景时，推荐您使用导入和导出安全组功能。

- 本地备份安全组规则：如果您想在本地备份安全组规则，可以导出安全组内的规则，将安全组的出方向、入方向规则信息导出为Excel格式文件。
- 快速创建和恢复安全组规则：如果您想快速创建或恢复安全组规则，可以将安全组规则文件导入到已有安全组中。

- 快速迁移安全组规则：将某个安全组的规则快速应用到其他安全组。
- 批量修改安全组规则：将当前安全组的规则导出后，在Excel文件批量修改完成后，重新导入即可。

约束与限制

- 导入安全组规则时，请根据格式要求填写要求的参数，不能新增参数或者修改已有参数名称，否则会导入失败。
- 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。

7.2.5.7 删除安全组规则

操作场景

当您不需要通过某条安全组规则控制流量流入/流出安全组内实例时，您可以参考以下操作删除安全组规则。

约束与限制

当您删除安全组规则前，请您务必了解该操作可能带来的影响，避免误删除造成网络中断或者引入不必要的网络安全问题。

安全组规则遵循白名单原理，当在规则中没有明确定义允许或拒绝某条流量时，安全组一律拒绝该流量流入或者流出实例。

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。

7.2.6 管理安全组关联的实例

7.2.6.1 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，选择目标实例类型对应的页签。
   以下操作，以选择“服务器”页签为例。
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，选择目标实例类型对应的页签。
   以下操作，以选择“服务器”页签为例。
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。

7.2.6.2 更改弹性云服务器的安全组

操作场景

创建弹性云服务器时，必须将其加入一个安全组内，如果您未创建任何安全组，那么首次使用安全组时，系统会自动为您创建一个**默认安全组default**并关联至弹性云服务器。当默认安全组无法满足您的需求，您可以参考以下操作为弹性云服务器更改安全组。

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

操作步骤

1. 登录管理控制台。
2. 选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表中，单击“操作”列下的“更多 > 网络设置 > 更改安全组”。
   系统弹窗显示“更改安全组”页面。
4. 根据界面提示，在下拉列表中选择待更改安全组的网卡，并重新选择安全组。
   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”。

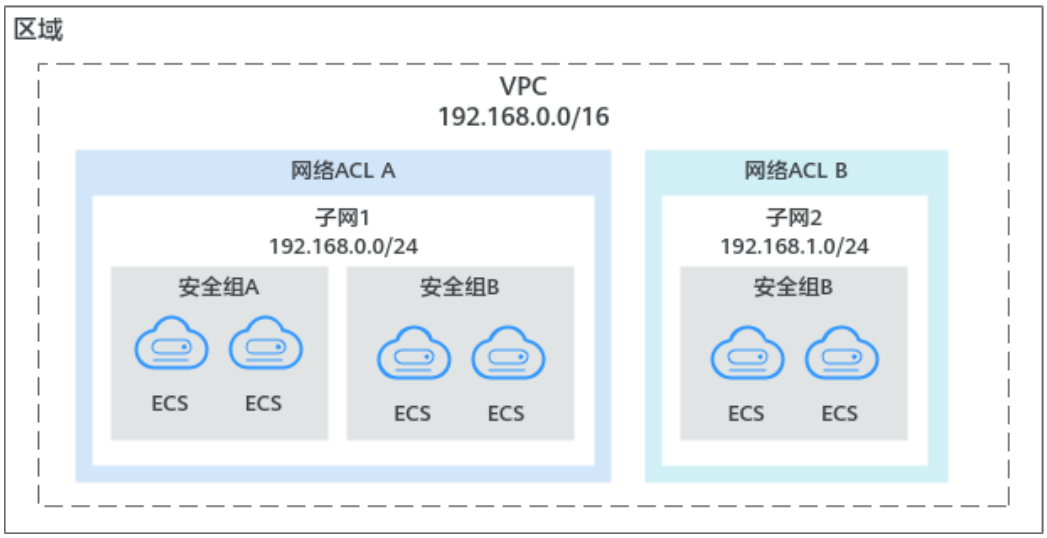
7.3 网络 ACL

7.3.1 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7-3**所示。

图 7-3 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**VPC访问控制概述**。

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7-19所示。该规则不能修改和删除。

表 7-19 网络 ACL 默认规则

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

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7-4所示。

图 7-4 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。

7.3.2 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7-20所示。

表 7-20 网络 ACL 规则

方向	动作	协议	源地址	源端口范围	目的地址	目的端口范围	说明
入方向	拒绝	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	拒绝所有IP地址通过TCP 445端口入站访问
入方向	允许	全部	0.0.0.0/0	1-65535	0.0.0.0/0	全部	放通所有入站流量

说明

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

允许某些协议端口的访问

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

网络ACL配置

需要添加的网络ACL入方向、出方向规则如表7-21所示。

表 7-21 网络 ACL 规则

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

安全组配置

需要添加的安全组入方向、出方向规则如表7-22所示。

表 7-22 安全组规则

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

7.3.3 管理网络 ACL

7.3.3.1 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 7-23 参数说明

参数	参数说明	取值样例
名称	网络ACL的名称，必填项。 网络ACL的名称只能由英文字母、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。

7.3.3.2 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。

7.3.3.3 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。

7.3.3.4 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。

7.3.3.5 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。

7.3.4 管理网络 ACL 规则

7.3.4.1 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 7-24 参数说明

参数	参数说明	取值样例
策略	网络ACL策略。必选项，单击下拉按钮可选择。目前支持“允许”和“拒绝”。	允许
协议	网络ACL支持的协议。必选项，单击下拉按钮可选择。 目前只支持选择TCP、UDP、全部、ICMP协议。	TCP

参数	参数说明	取值样例
源地址	此方向允许的源地址，可以是IP地址、IP地址段。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0	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。 选择TCP或UDP协议时必须填写。	22或22-30
目的地址	此方向允许的目的地址，可以是IP地址、IP地址段。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0	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。

7.3.4.2 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7-25**。

表 7-25 参数说明

参数	参数说明	取值样例
策略	网络ACL策略。必选项，单击下拉按钮可选择。目前支持“允许”和“拒绝”。	允许
协议	网络ACL支持的协议。必选项，单击下拉按钮可选择。 目前只支持选择TCP、UDP、全部、ICMP协议。	TCP
源地址	此方向允许的源地址，可以是IP地址、IP地址段。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0	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。 选择TCP或UDP协议时必须填写。	22或22-30
目的地址	此方向允许的目的地址，可以是IP地址、IP地址段。 ● IPv4地址：xxx.xxx.xxx.xxx/32 ● 子网：xxx.xxx.xxx.0/24 ● 任意地址：0.0.0.0/0	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。

7.3.4.3 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。

7.3.4.4 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“开启”或者“关闭”。
6. 单击“是”，确认开启或关闭此规则。

7.3.4.5 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”。

批量删除多条网络ACL规则

您还可以同时勾选多条网络ACL规则，单击列表上方的“删除”，批量删除多条网络ACL规则。

7.3.5 管理网络 ACL 关联的子网

7.3.5.1 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。

7.3.5.2 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”。

批量解除关联子网

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

8 对等连接

8.1 对等连接概述

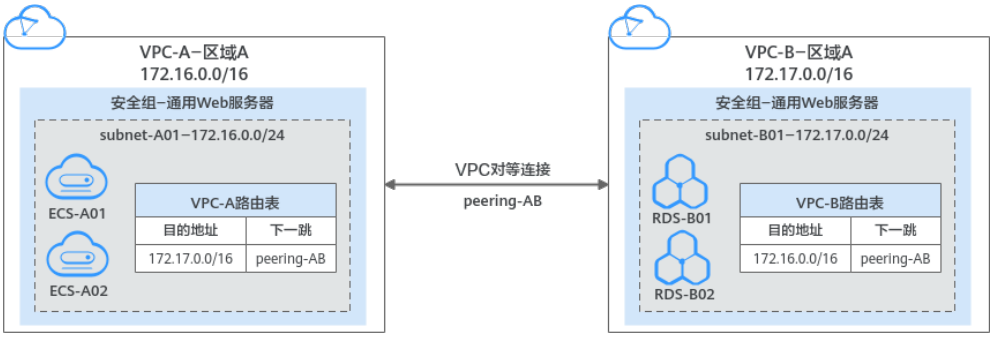
什么是对等连接

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。

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

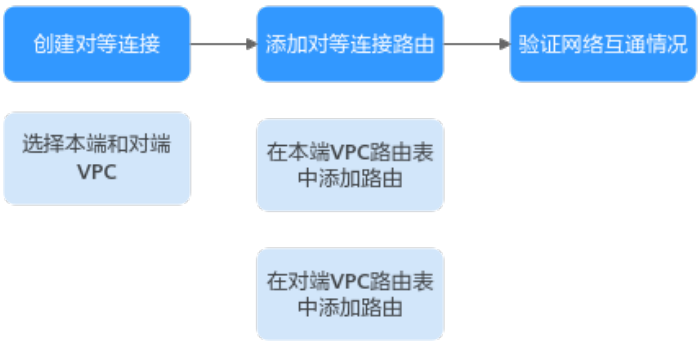


对等连接创建流程

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：

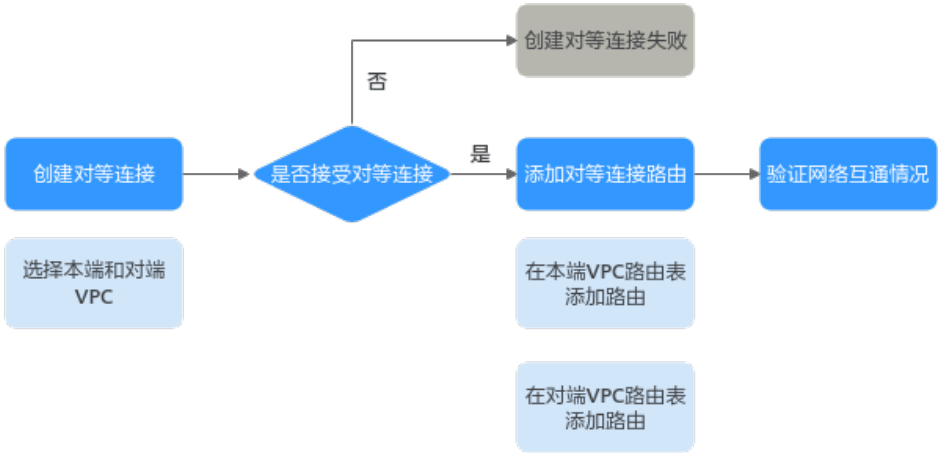
- 相同账户下的VPC对等连接创建流程如图8-2所示。
  创建对等连接的具体操作，请参见创建相同账户下的对等连接。

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。
- VPC-A和VPC-B之间创建对等连接，默认情况下，VPC-B不能通过VPC-A的EIP访问公网。您可以使用NAT网关服务或配置SNAT服务器，使得VPC-B下的弹性云服务器可以通过VPC-A下绑定了EIP的弹性云服务器访问Internet。

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)

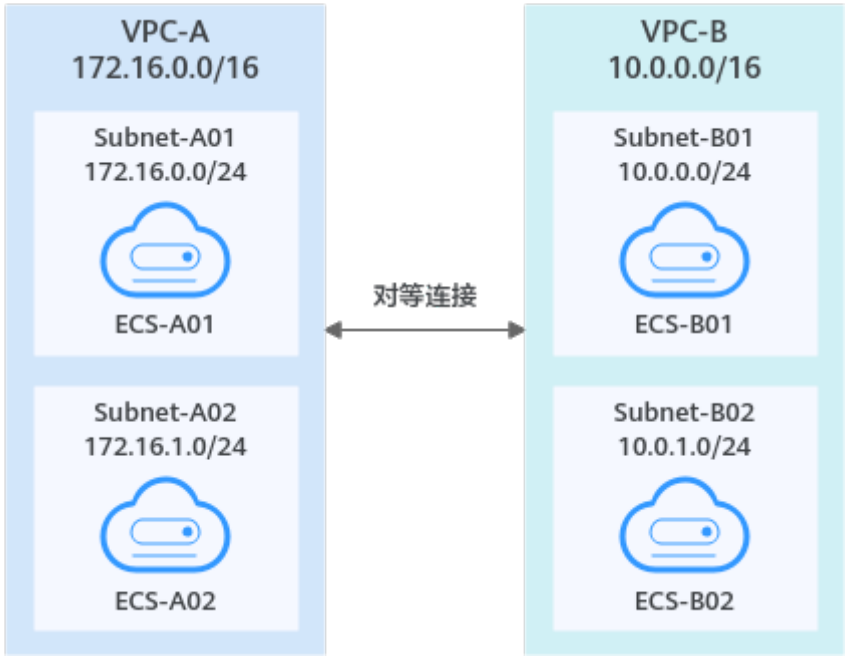


表 8-2 对等连接关系说明-相互对等的两个 VPC(IPv4)

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)

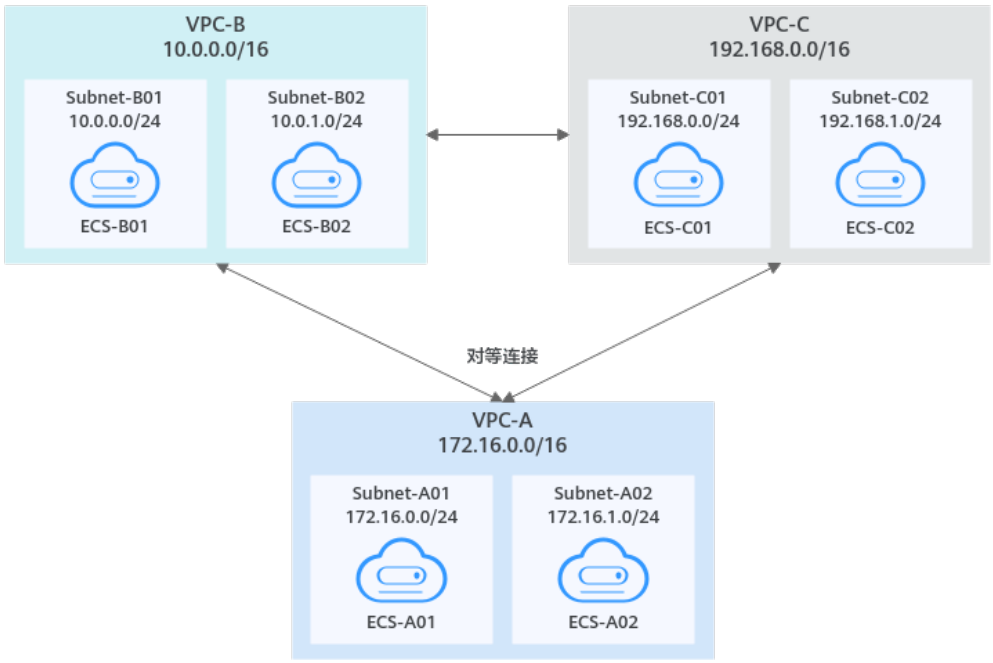


表 8-4 对等连接关系说明-相互对等的多个 VPC(IPv4)

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)

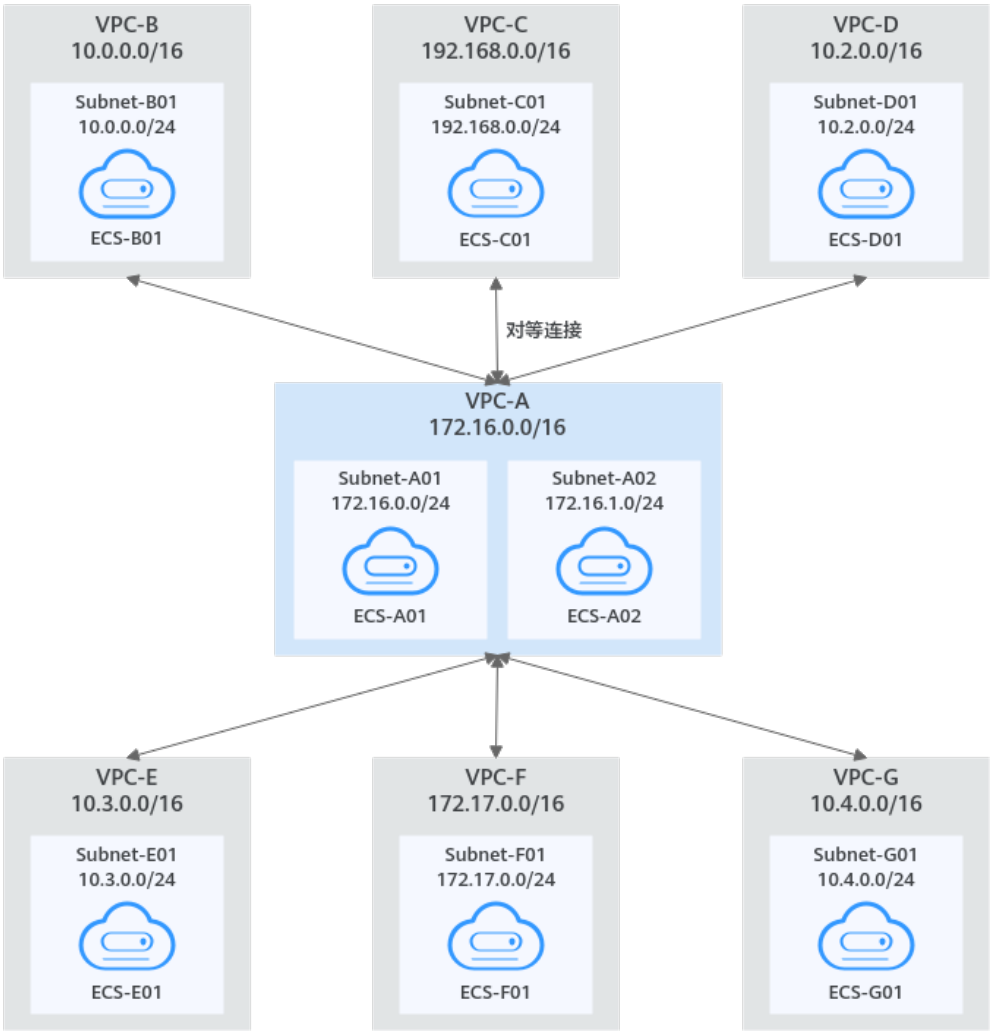


表 8-6 对等连接关系说明-一个中心 VPC 与多个 VPC 对等(IPv4)

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)

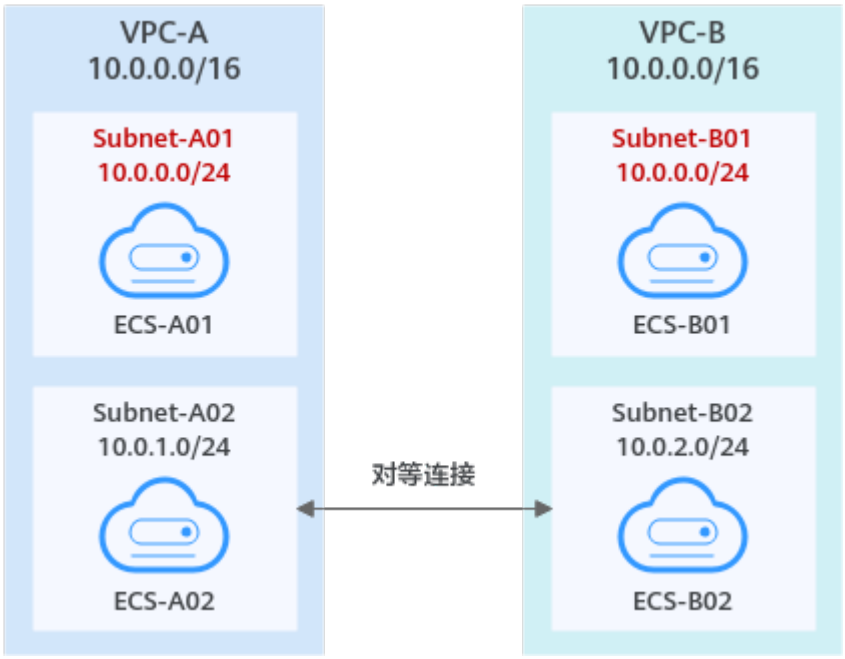


表 8-8 对等连接关系说明-相互对等的两个重叠网段 VPC 子网(IPv4)

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)

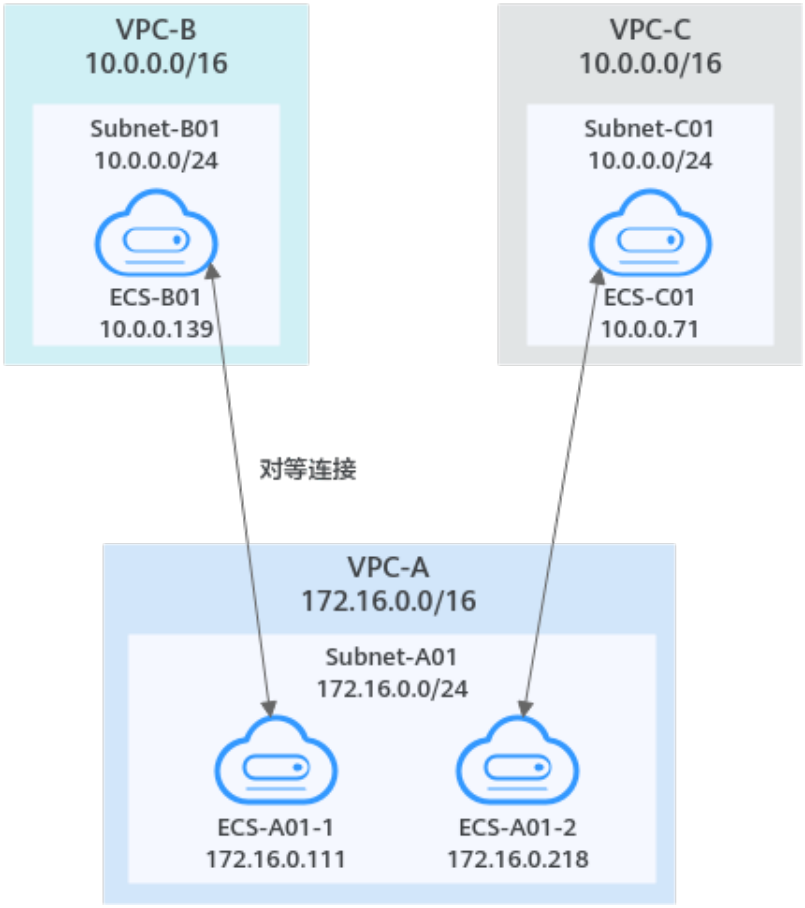


表 8-10 对等连接关系说明-一个中心 VPC 的 ECS 与两个 VPC 的 ECS 对等(IPv4)

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)

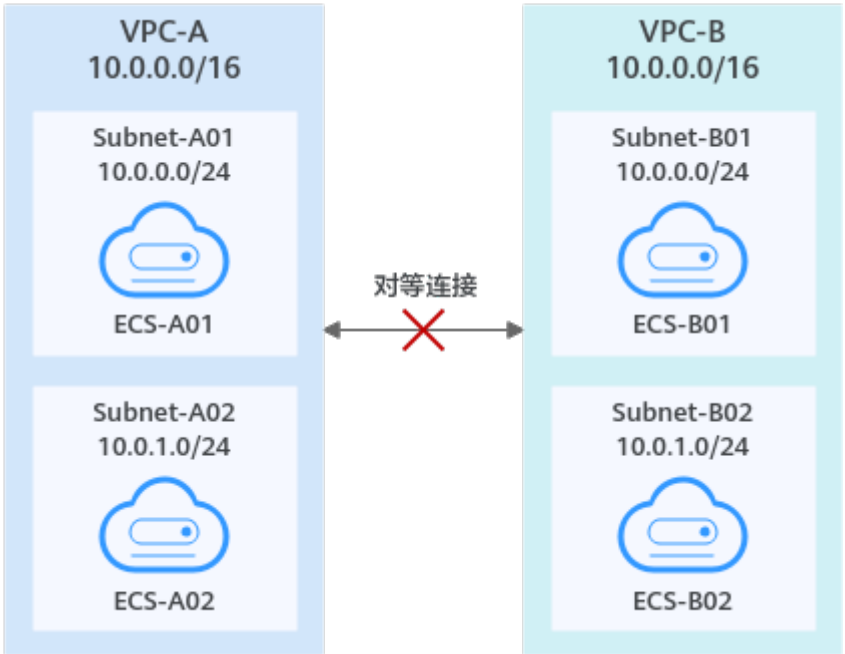


表 8-12 VPC 路由表配置说明-VPC 网段重叠，且全部子网重叠(IPv4)

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。

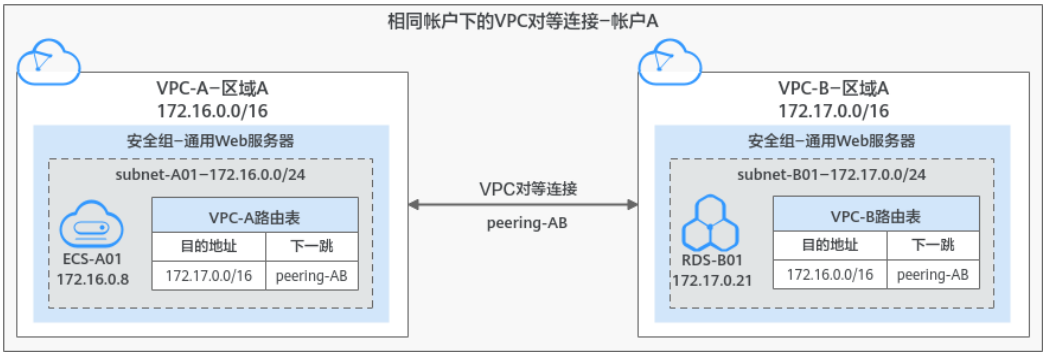
创建步骤如下：

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，单击“立即添加”，跳转到对等连接详情页面，继续执行**步骤二：添加VPC对等连接路由**，添加路由。

步骤二：添加 VPC 对等连接路由

1. 在对等连接详情页面下方区域，单击“添加路由”。
   弹出对等连接的“添加路由”对话框。
2. 根据界面提示，在VPC路由表中添加路由。
   参数说明如**表8-14**所示。

表 8-14 参数说明

参数	说明	取值样例
虚拟私有云	选择对等连接两端中的任意一个VPC。	VPC-A
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 ● 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 ● 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-A（默认路由表）
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接使用示例**。	本示例为VPC-B的网段：172.17.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	本端VPC-A到对端VPC-B的去程路由。
添加另一端VPC的路由	勾选该参数，可同时添加对等连接另一端VPC内的回程路由。 通常情况下，您需要在对等连接两端VPC的路由表中分别添加去程和回程路由，才可以实现通信，单击了解**对等连接使用示例**。	勾选
虚拟私有云	系统默认填写对等连接两端的另一个VPC，您无需选择。	VPC-B
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 ● 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 ● 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-B（默认路由表）

参数	说明	取值样例
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接使用示例**。	本示例为VPC-A的网段：172.16.0.0/16
下一跳地址	系统默认选择当前对等连接，无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	对端VPC-B到本端VPC-A的回程路由。

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

步骤三：验证网络互通情况

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

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

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

须知

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

8.4 创建不同账户下的对等连接

操作场景

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

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

创建步骤如下：

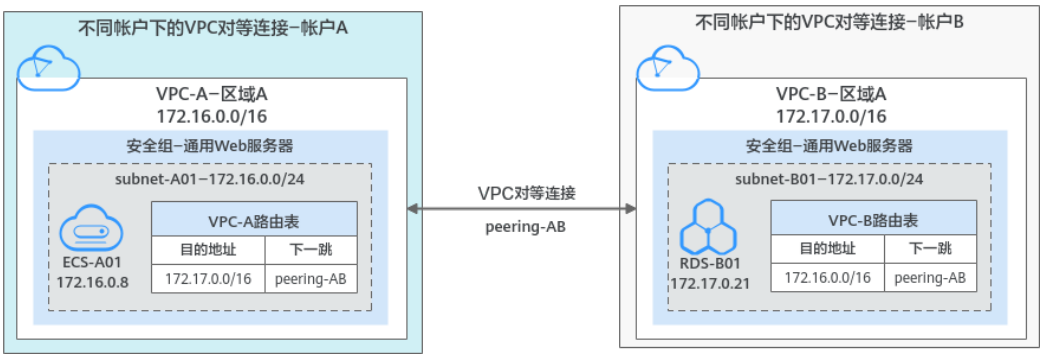
步骤一：创建VPC对等连接

步骤二：对端账户接受VPC对等连接

步骤三：添加VPC对等连接路由

步骤四：验证网络互通情况

图 8-11 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8-15**。

表 8-15 创建对等连接-参数说明

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

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. 在页面左上角单击图标，打开服务列表，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。
      进入对等连接详情页面。
   b. 在对等连接详情页面下方区域，单击“添加路由”。
      弹出对等连接的“添加路由”对话框。
   c. 根据界面提示，在VPC路由表中添加路由。
      参数说明如**表8-16**所示。

表 8-16 参数说明

参数	说明	取值样例
虚拟私有云	系统默认填写对等连接中当前账户内的VPC，您无需选择。	VPC-A

参数	说明	取值样例
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 ● 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 ● 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-A（默认路由表）
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接使用示例**。	本示例为VPC-B的网段：172.17.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	本端VPC-A到对端VPC-B的去程路由。

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

2. 执行以下操作，在对端VPC路由表中添加对等连接路由。
a. 在对端账户的对等连接列表中，单击目标对等连接的名称。
进入对等连接详情页面。
b. 在对等连接详情页面下方区域，单击“添加路由”。
弹出对等连接的“添加路由”对话框。
c. 根据界面提示，在VPC路由表中添加路由。
参数说明如**表8-17**所示。

表 8-17 参数说明

参数	说明	取值样例
虚拟私有云	系统默认填写对等连接中当前账户内的VPC，您无需选择。	VPC-B

参数	说明	取值样例
路由表	选择VPC的路由表，路由信息将会添加在该路由表中。 VPC创建完成后自带一个默认路由表，用来控制VPC内子网出方向的流量走向。除了默认路由表，您还可以创建自定义路由表，并关联至子网，则该子网的出方向流量由自定义路由表控制。 • 如果路由表的下拉列表中只有默认路由表，则选择默认路由表即可。 • 如果路由表的下拉列表中同时存在默认路由表和其他自定义路由表，则选择对等连接连通的子网所关联的路由表。	rtb-VPC-B（默认路由表）
目的地址	对等连接另一端VPC内的地址，可以为VPC网段、子网网段、ECS IP地址等，具体路由配置示例请参见**对等连接使用示例**。	本示例为VPC-A的网段：172.16.0.0/16
下一跳地址	系统默认填写当前对等连接，您无需选择。	peering-AB
描述	路由的描述信息，非必填项。 描述信息内容不能超过255个字符，且不能包含“<”和“>”。	对端VPC-B到本端VPC-A的回程路由。

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

步骤四：验证网络互通情况

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

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

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


须知

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

8.5 获取对等连接的对端项目 ID

操作场景

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

操作步骤

1. 登录管理控制台。
   此处使用对端账户登录管理控制台。
2. 在页面右上角的用户名的下拉列表中，单击“我的凭证”。
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. 在页面下方的路由列表中，单击目标路由对应的路由表超链接。
   进入路由表详情页面。
6. 在路由详情页面的路由列表中，单击目标路由操作列下的“修改”。
7. 根据界面提示，修改路由信息，并单击“确定”，完成路由修改。

修改不同账户对等连接的路由

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

1. 使用本端账户登录管理控制台，执行以下操作，修改本端VPC的路由。
   a. 在页面左上角单击 ☰ 图标，打开服务列表，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. 在页面下方的路由列表中，单击目标路由对应的路由表超链接。
      进入路由表详情页面。
   e. 在路由详情页面的路由列表中，单击目标路由操作列下的“修改”。
   f. 根据界面提示，修改路由信息，并单击“确定”，完成路由修改。
2. 使用对端账户登录管理控制台，参考**1**，修改对端VPC的路由。

8.10 查看对等连接路由

操作场景

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

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

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

查看相同账户对等连接的路由

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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. 在页面下方的路由列表中，可以查看路由信息。
   路由信息包括目的地址，对应的虚拟私有云、下一跳地址、路由表等信息。

查看不同账户对等连接的路由

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

1. 使用本端账户登录管理控制台，执行以下操作，查看本端VPC的路由。
   a. 在页面左上角单击图标，打开服务列表，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. 在页面下方的路由列表中，可以查看路由信息。
      路由信息包括目的地址，对应的虚拟私有云、下一跳地址、路由表等信息。
2. 使用对端账户登录管理控制台，参考1，查看对端VPC的路由。

8.11 删除对等连接路由

操作场景

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

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

删除相同账户对等连接的路由

1. 登录管理控制台。
2. 在页面左上角单击图标，打开服务列表，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. 在页面下方的路由列表中，单击目标路由操作列下的“删除”。
   弹出删除确认对话框。
6. 确认无误后，单击“确定”，删除路由。

删除不同账户对等连接的路由

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

1. 使用本端账户登录管理控制台，执行以下操作，删除本端VPC的路由。
   a. 在页面左上角单击图标，打开服务列表，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. 在页面下方的路由列表中，单击目标路由操作列下的“删除”。
      弹出删除确认对话框。
   e. 确认无误后，单击“确定”，删除路由。
2. 使用对端账户登录管理控制台，参考1，删除对端VPC的路由。

9 VPC 流日志

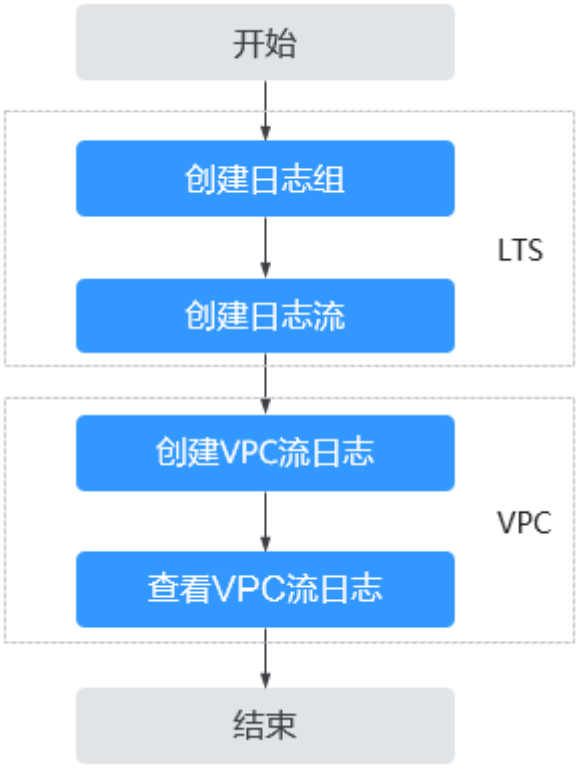
9.1 VPC 流日志概述

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流，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

- 目前支持采集流日志的云服务器规格类型为S2、Sn2、Sc2、M2、El2、Hc2、Hl1、H2、D2、I2、P1、P2、G3、Pi1、Fp1、S3、C3、M3、M3se、H3、Hl3、Hi3、His3、D3、Ir3、I3、Sn3、E3、C3ne、M3ne、G5、P2v、Ai1、C6、M6、D6、S6、C6s、C6nl、C6ie、S7、C7、M7、E7、D7、Ir7、I7、S7n、C7n、M7n、I7n。
- 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。
- 创建日志流。

云日志服务更多内容请参见《云日志服务用户指南》。

操作步骤

1. 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、子网、虚拟私有云类型。	网卡
选择资源	选择需要采集流量信息的具体资源。 **说明** 建议您选择处于开机状态的弹性云服务器。如果选择了关机状态的弹性云服务器，请在VPC流日志创建完成后，重启弹性云服务器，以便准确的记录网卡流量。	-

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流下，只能有两个不同采集类型的VPC流日志。不能重复创建相同的VPC流日志。

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流详情页面，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 弹性公网 IP

10.1 为弹性云服务器申请和绑定弹性公网 IP

操作场景

可以通过申请弹性公网IP并将弹性公网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。

申请弹性公网 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 > 弹性公网IP”
3. 在“弹性公网IP”界面，单击“创建弹性公网IP”。
4. 根据界面提示配置参数。

表 10-1 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： ● 独享带宽：独享带宽只能针对一个弹性公网IP进行限速。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公网IP进行集中限速，可以加入多个弹性公网IP，被多个弹性公网IP地址共用。适用于多业务流量错峰分布场景。	独享带宽
带宽大小	带宽大小，单位Mbit/s。	100
弹性公网IP名称	弹性公网IP的名称。	eip-test
带宽名称	带宽的名称。	bandwidth
规格	弹性公网IP地址所连接的外部网络	5_bgp
数量	弹性公网IP数量。	1

5. 单击“立即申请”。
6. 单击“提交”。

绑定弹性公网 IP

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

10.2 解绑定和释放弹性云服务器的弹性公网 IP

操作场景

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

约束与限制

- 未绑定任何实例的弹性公网IP才可释放，已绑定实例的弹性公网IP需要先从实例解绑，然后释放。

操作步骤

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

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

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

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

10.3 修改弹性公网 IP 的带宽配置

操作场景

修改弹性公网IP带宽名称、大小。

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 > 弹性公网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。
5. 单击“下一步”。
6. 单击“提交”，完成修改。

10.4 管理 IPv6 弹性公网 IP

简介

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

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

IPv4/IPv6 双栈网络应用场景

如果您的ECS规格支持IPv6网络，那么您可以使用IPv4/IPv6双栈网络，场景示例和资源规划如表10-2所示。

表 10-2 IPv4/IPv6 双栈网络的应用场景及资源规划

应用场景	场景示例	条件	子网网段类型	ECS
IPv4内网通信	在ECS上部署应用，需要与其他系统（比如数据库）之间使用**IPV4**进行内网互访。	• 实例未绑定弹性公网IP。	IPv4网段	**IPv4私网地址：**支持IPv4内网通信。
IPv4公网通信	在ECS上部署应用，需要与其他系统（比如数据库）之间使用**IPV4**进行公网互访。	• 实例绑定弹性公网IP。	IPv4网段	• **IPv4私网地址：**支持IPv4内网通信。 • **IPv4公网地址：**支持IPv4公网通信。

应用场景	场景示例	条件	子网网段类型	ECS
IPv6内网通信	在ECS上部署应用，需要与其他系统（比如数据库）之间使用**IPV6**进行内网互访。	• VPC的子网开启IPv6。 • 创建ECS时，网络配置如下： – **VPC和子网：**选择已开启IPv6的子网及子网所属的VPC。 – **共享带宽：**暂不配置。	• IPv4网段 • IPv6网段	• **IPv4私网地址+IPv4 EIP：**实例绑定IPv4 EIP，支持IPv4公网通信。 • **IPv4私网地址：**实例不绑定IPv4 EIP，支持IPv4内网通信。 • **IPv6地址：**IPv6地址不加入共享带宽，支持IPv6内网通信。
IPv6公网通信	搭建IPv6网络，使ECS可以访问Internet上的**IPv6**服务。	• VPC的子网开启IPv6。 • 创建ECS时，网络配置如下： – **VPC和子网：**选择已开启IPv6的子网及子网所属的VPC。 – **共享带宽：**选择一个共享带宽。	• IPv4网段 • IPv6网段	• **IPv4私网地址+IPv4 EIP：**实例绑定IPv4 EIP，支持IPv4公网通信。 • **IPv4私网地址：**实例不绑定IPv4 EIP，支持IPv4内网通信。 • **IPv6地址+共享带宽：**同时支持IPv6公网通信和IPv6内网通信。

使用IPv4/IPv6双栈网络请参考《虚拟私有云用户指南》的“IPv4/IPv6双栈网络”章节。

IPv6 转换功能应用场景

如果您想使部署应用的ECS面向Internet客户端提供IPv6服务，但您的ECS规格不支持IPv6网络，或者您不想通过搭建IPv6网络来实现该需求，那么您可以通过弹性公网IP的IPv6转换功能快速实现该能力。场景示例和资源规划如**表10-3**。

表 10-3 IPv6 EIP（开启 IPv6 转换）网络的应用场景及资源规划

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

开启 IPv6 转换（申请 IPv6 弹性公网 IP）

- 方法一：

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

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

- 方法二：

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

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

配置安全组

开启弹性公网IP的IPv6转换后，请务必在安全组的出方向和入方向中放通198.19.0.0/16网段的IP地址，如**表10-4**所示。因为IPv6 弹性公网IP采用NAT64技术，入方向的源IP地址经过NAT64转换后，会将IPv6地址转换为198.19.0.0/16之间的某个IPv4地址，源端口随机，目的IP为本机的内部私有IPv4地址，目的端口不变。

配置安全组操作请参考《虚拟私有云用户指南》中的“添加安全组规则”章节。

表 10-4 安全组规则

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

关闭 IPv6 转换（释放 IPv6 弹性公网 IP）

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

11 共享带宽

11.1 共享带宽概述

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

说明

- 共享带宽不支持对单个弹性公网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。

- 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，不区分其他弹性公网IP类型及绑定实例类型，随时从共享带宽中增加或移出弹性公网IP。

  说明

  独享型ELB专属池的5_gray类型的EIP不建议和其他类型EIP使用同一个共享带宽，两种类型的EIP加入同一个共享带宽会导致限速策略失效。

11.2 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 > 弹性公网IP”
3. 在左侧导航栏，选择“弹性公网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 11-1 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。	sa-fb-1
带宽大小	共享带宽的大小，单位Mbit/s，最大支持300Mbit/s。	10
名称	共享带宽的名称。	Bandwidth-001

5. 单击“立即创建”。

11.3 添加弹性公网 IP 到共享带宽

操作场景

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

约束与限制

- EIP的线路类型与要加入的共享带宽的线路类型一致。

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 > 弹性公网IP”
3. 在左侧导航栏，选择“弹性公网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公网IP的共享带宽，在“操作”列选择“ 添加弹性公网IP”，勾选您想添加的弹性公网IP。

   说明

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

11.4 从共享带宽中移出弹性公网 IP

操作场景

您可以根据需要将不需要的弹性公网IP从共享带宽中移出。

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 > 弹性公网IP”
3. 在左侧导航栏，选择“弹性公网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公网IP的共享带宽，选择“更多 > 移出弹性公网IP”，勾选您想移出的弹性公网IP。
5. 单击“确定”。

11.5 修改共享带宽大小

操作场景

您可以根据需要修改共享带宽的名称和带宽大小。

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 > 弹性公网IP”
3. 在左侧导航栏，选择“弹性公网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。
5. 单击“下一步”。
6. 单击“提交”，完成修改。

11.6 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公网IP，详情请参见**从共享带宽中移出弹性公网IP**。

操作步骤

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

12 监控

12.1 支持的监控指标

功能说明

本节定义了弹性公网IP和带宽上报云监控的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控提供的管理控制台或API接口来检索弹性公网IP和带宽产生的监控指标和告警信息。

命名空间

SYS.VPC

监控指标

表 12-1 弹性公网 IP 和带宽支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
upstream_bandwidth	出网带宽	该指标用于统计测试对象出云平台的网络速度。 单位：比特/秒	≥ 0 bit/s	带宽或弹性公网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	带宽或弹性公网IP	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
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	带宽或弹性公网IP	1分钟
down_stream	入网流量	该指标用于统计测试对象入云平台一分钟内累积的网络流量平均值。 单位：字节	≥ 0 bytes	带宽或弹性公网IP	1分钟

维度

Key	Value
publicip_id	弹性公网IP ID
bandwidth_id	带宽ID

对于有多个测量维度的测量对象，使用接口查询监控指标时，所有测量维度均为必选。

- 查询单个监控指标时，多维度dim使用样例：dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a。
- 批量查询监控指标时，多维度dim使用样例：

  "dimensions": [

  {

  "name": "bandwidth_id",

  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"

  }

  {

  "name": "publicip_id",

  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"

  }

  ],

12.2 查看监控指标

操作场景

查看带宽、弹性公网IP的使用情况。

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

操作步骤

1. 登录管理控制台。
2. 在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“弹性公网IP和带宽”。
4. 单击“操作”列的“查看监控图表”，查看带宽或弹性公网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 权限管理

13.1 创建用户并授权使用 VPC

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

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

如果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。

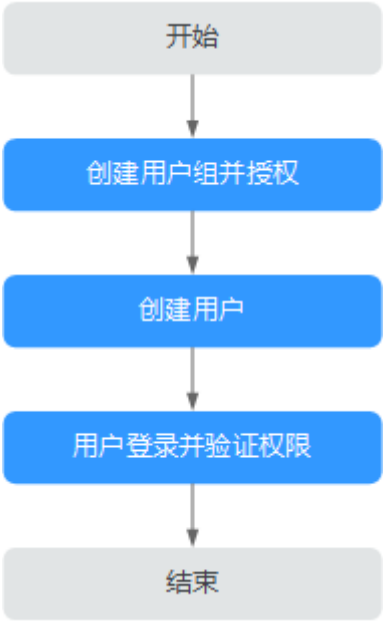
本章节为您介绍对用户授权的方法，操作流程如**图13-1**所示。

前提条件

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

示例流程

图 13-1 给用户授权 VPC 权限流程



1. 创建用户组并授权

   在IAM控制台创建用户组，并在“操作”列下选择“授权”，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，并在“操作”列下选择“授权”，并将其加入1中创建的用户组。

3. 用户登录并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：

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

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。自定义策略中可以添加的授权项（Action）请参见《虚拟私有云API参考》中“权限和授权项 > 权限及授权项说明”章节。

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。

具体创建步骤请参见：《统一身份认证服务》中“用户指南 > 管理细粒度策略 > 创建自定义策略”章节。本章为您介绍常用的VPC自定义策略样例。

VPC 自定义策略样例

- 示例1：授权用户创建和查看VPC

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

- 示例2：拒绝用户删除VPC

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

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

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

- 示例3：多个授权项策略

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

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


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。

在联系运营管理员之前，请您准备好以下信息：

- 账号名，获取方式如下：
  登录云账户管理控制台，在右上角单击用户名，选择“我的凭证”，在“我的凭证”页面获取“账号名”。
- 配额信息，包括：服务名、配额类别、需要的配额值。

14.2 虚拟私有云与子网类

14.2.1 什么是虚拟私有云?

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

14.2.2 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14-1所示。

表 14-1 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

14.2.3 VPC 的子网间是否可以通信?

- 不同VPC之间的网络默认不通，因此不同VPC的子网网络也不互通。
- 同一个VPC内的子网网络默认互通。当您的组网中使用网络ACL和安全组防护网络安全时，也会影响子网之间的网络通信。
  - 网络ACL：您可以根据实际情况选择是否为子网关联网络ACL，当子网关联了网络ACL，不同网络ACL的网络默认隔离。那么如果同一个VPC的子网关联不同的网络ACL，并且未添加放通规则时，网络默认不通。
  - 安全组：VPC子网内部署的实例（如ECS）必须关联安全组，不同安全组的网络默认隔离。那么如果同一个VPC内的实例关联不同安全组，并且未添加放通规则时，网络默认不通。

  当网络ACL和安全组同时存在时，流量优先匹配网络ACL规则，详细说明如表14-2。

图 14-1 一个 VPC 内不同子网通信组网图

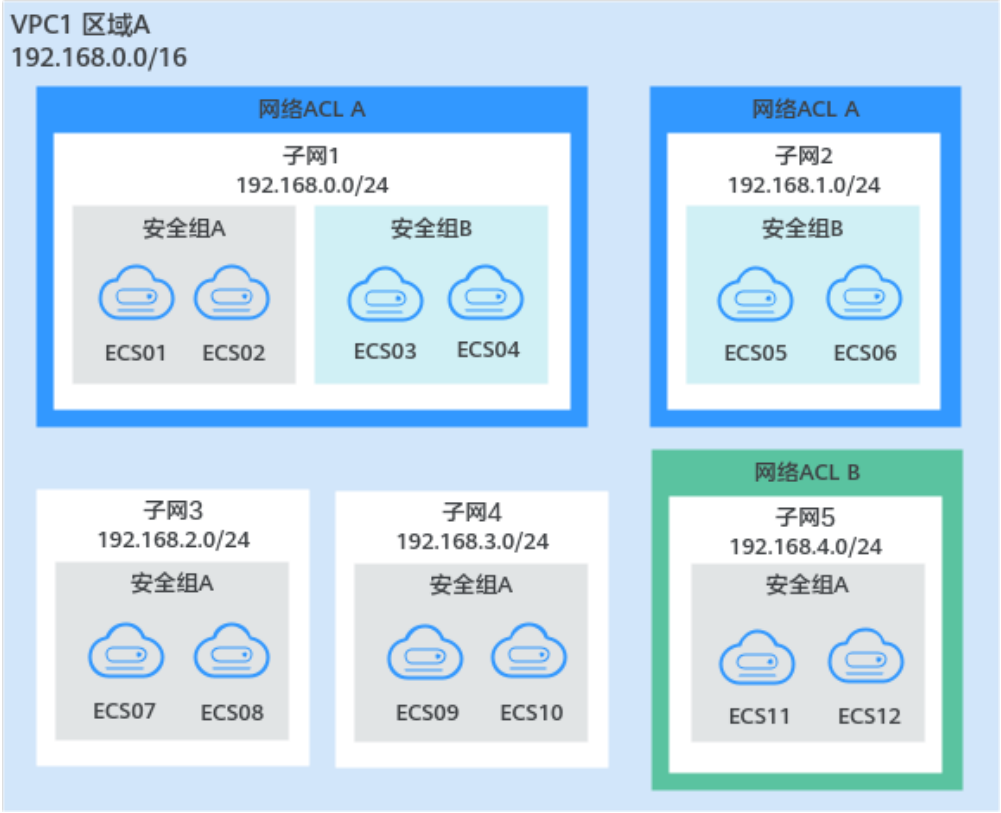


表 14-2 一个 VPC 内不同子网通信场景说明

网络通信场景	网络安全配置	网络通信情况说明
不同子网之间通信	子网未关联网络ACL 实例关联相同安全组	• 子网网络默认互通：子网3和子网4未关联网络ACL，那么子网3和子网4网络互通。 • 子网内实例网络默认互通：ECS07、ECS08、ECS09和ECS10均关联安全组A，那么这些ECS网络互通。
	子网关联相同网络ACL 实例关联不同安全组	• 子网网络默认互通：子网1和子网2均关联网络ACL A，那么子网1和子网2网络互通。 • 子网内实例网络默认不通：子网1内的ECS01和ECS02关联安全组A，子网2内的ECS05和ECS06关联安全组B，那么安全组A和安全组B未添加放通规则时，不同安全组内的ECS网络不通，比如ECS01和ECS05网络不通。

网络通信场景	网络安全配置	网络通信情况说明
	子网关联不同网络ACL	子网网络默认不通：子网1关联网络ACL A，子网5关联网络ACL B，那么网络ACL A和网络ACL B未添加放通规则时，子网1和子网5的网络不通。 此时子网网络不通，因此不论子网内ECS是否属于同一个安全组，网络均不通。
一个子网内通信	实例关联不同安全组	子网内实例网络默认不通：子网1内的ECS01和ECS02关联安全组A，ECS03和ECS04关联安全组B，那么安全组A和安全组B未添加放通规则时，即使在同一个子网内，不同安全组内的ECS网络不通，比如ECS01和ECS03网络不通。

14.2.4 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子网所在VPC掩码~28。

14.2.5 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？**。

14.2.6 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14-3**，对照管理控制台的提示信息，根据对应的解决办法处理。

表 14-3 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。

提示信息	原因	处理方法
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**。
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**。

提示信息	原因	处理方法
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14-4**，对照管理控制台的提示信息，找到对应的解决办法处理。

表 14-4 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。
“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**
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**。
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公网IP地址。	您需要在弹性公网IP列表中，释放所有的弹性公网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公网IP**。

14.3 弹性公网 IP 类

14.3.1 一个弹性公网 IP 可以给几个弹性云服务器使用?

一个弹性公网IP只能绑定一个弹性云服务器使用。

14.3.2 如何通过外部网络访问绑定弹性公网 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。

14.3.3 弹性公网 IP 是否支持切换区域?

弹性公网IP不支持切换区域。

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

14.4 对等连接类

14.4.1 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。

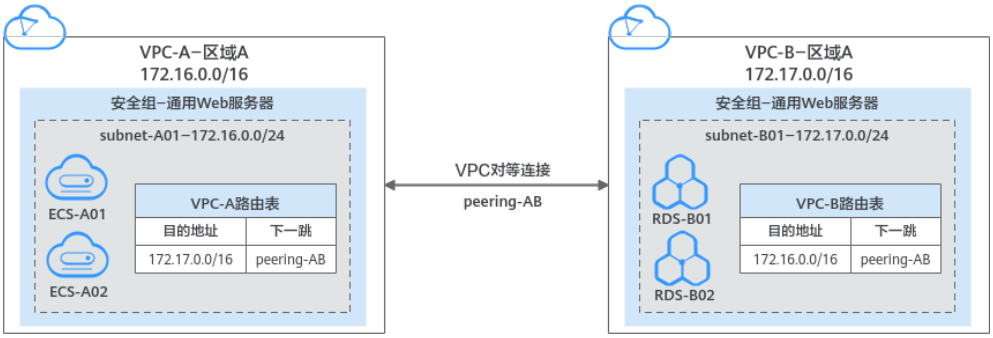
14.4.2 对等连接是否可以连通不同区域的 VPC?

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14-2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 14-2 对等连接组网示意图



14.4.3 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14-5，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 14-5 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。	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14-6**所示。

表 14-6 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14-3**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14-4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14-5。

图 14-3 VPC 网段重叠，且全部子网重叠(IPv4)

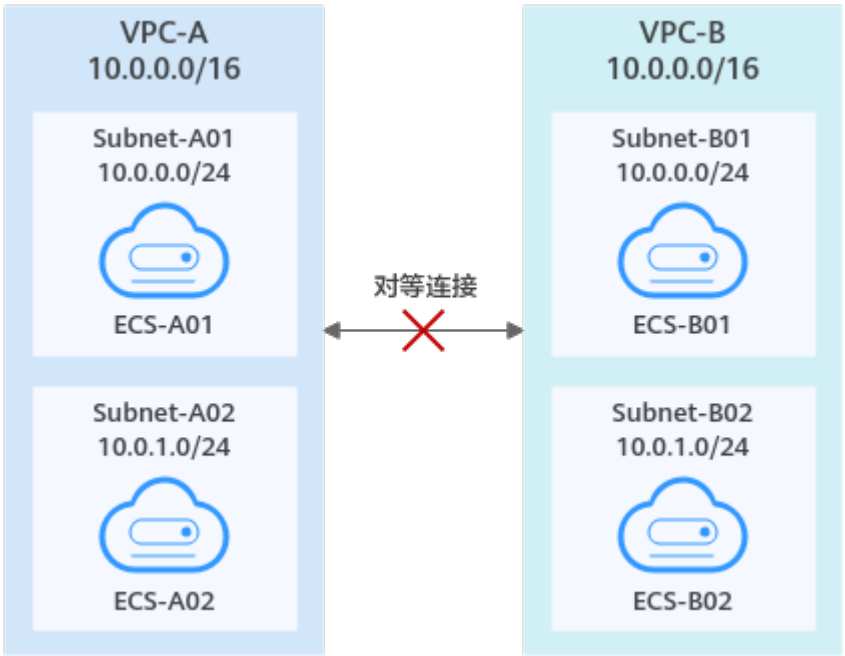
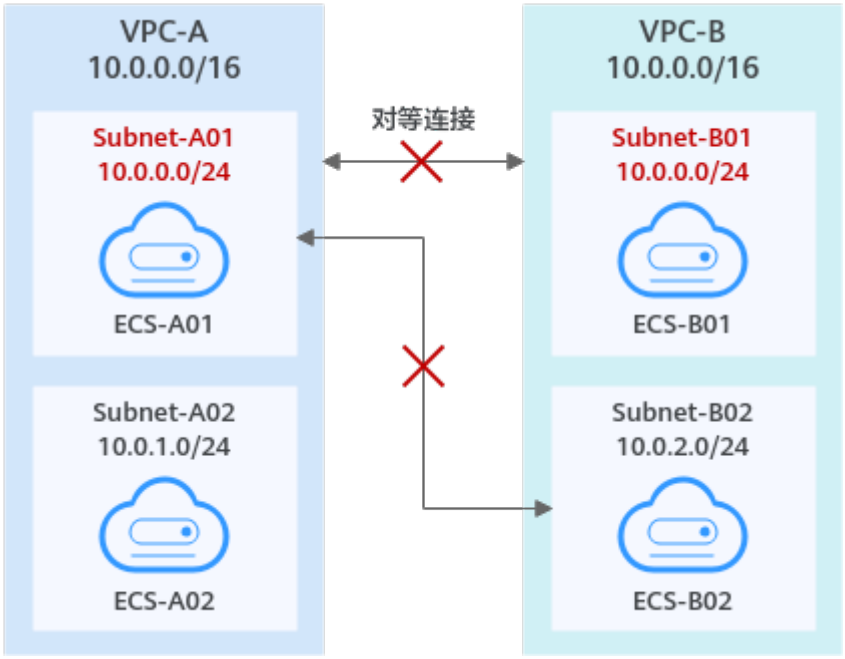


图 14-4 VPC 网段重叠，且部分子网重叠(IPv4)



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14-5所示，路由添加方法请参见表14-7。

图 14-5 VPC 网段重叠，部分子网重叠(IPv4)-正确配置

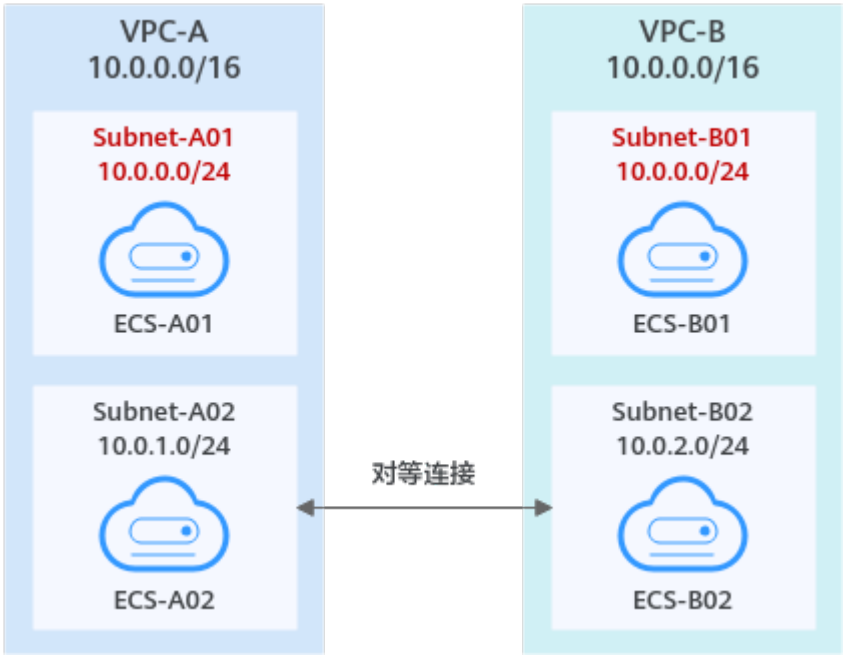


表 14-7 Subnet-A02 和 Subnet-B02 之间的对等连接

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14-8**。

表 14-8 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。

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。
   - 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。

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。
   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**

14.5 带宽类

14.5.1 带宽的限速范围是多少?

带宽的限速范围为1Mbit/s~300Mbit/s。

14.5.2 一个共享带宽最多能对多少个弹性公网 IP 进行集中限速?

一个共享带宽最多针对20个弹性公网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?** 。

14.6 网络连接类

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

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

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

1. 登录管理控制台。
2. 在系统首页，选择“网络 > 虚拟私有云”。
3. 在左侧导航栏，选择“虚拟私有云 > 子网”。
4. 在子网列表中，单击需要修改的子网名称。
5. 在子网详情页，修改子网DNS服务器地址。
6. 单击“确定”，完成修改。

14.6.2 同时拥有自定义路由和弹性公网 IP 的访问外网的优先级是什么?

弹性公网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。

14.7 路由类

14.7.1 1 个路由表里可以存在多少个路由?

每个路由表默认可以存在200条路由，包括专线路由和对等连接路由等其他路由。

14.7.2 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绑定的弹性公网IP都会失效。

14.8 安全类

14.8.1 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。

14.8.2 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。

14.8.3 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。

14.8.4 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。

14.8.5 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。

A 修订记录

发布日期	修改说明
2024-04-15	第一次正式发布。