虚拟私有云

常见问题

文档版本	01
发布日期	2025-01-24

华为云计算技术有限公司

商标声明


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

注意

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

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

目 录

1 计费类

1.1 VPC 是否收费?

虚拟私有云VPC服务下包含了多种产品资源，部分资源可以免费使用，部分资源需要支付费用，表1-1中为您详细介绍了虚拟私有云VPC各项资源的收费情况。

表 1-1 VPC 资源收费一览表

产品资源	收费情况说明
虚拟私有云	免费
子网	免费
路由表	免费
对等连接	免费
弹性网卡	免费
辅助弹性网卡	免费
IP地址组	免费
安全组	免费
网络ACL	免费
边缘网关	免费
VPC流日志	免费
流量镜像	免费

产品资源	收费情况说明
弹性公网IP和带宽	如果您使用了弹性公网IP和带宽的相关资源，则需要支付费用，费用账单中计费的“产品”项目说明如下： ● 弹性公网IP：收取弹性公网IP保有费。 您购买的按需计费弹性公网IP未绑定至任何实例（如ECS、ELB）时，会收取弹性公网IP保有费。 ● 固定带宽：收取的可能是以下资源的费用。 – 弹性公网IP的带宽费用：包年/包月弹性公网IP的带宽费用、按需计费(按带宽计费)弹性公网IP的带宽费用、按需计费(按流量计费)弹性公网IP的流量费用。 – 共享带宽的费用 – 共享流量包的费用 以上计费项目的详细说明，请参见**弹性公网IP计费说明**。
VPC终端节点	如果您使用了VPC终端节点资源，则需要支付费用。 详细计费说明请参见**VPC终端节点计费说明**。

说明

针对免费资源，当前暂不收费。待后续启动收费时，将会提前通知您。

1.2 为什么虚拟私有云 VPC 删除之后，仍在继续计费?

问题现象

如**图1-1**所示，您已将账户下的虚拟私有云VPC资源全部删除，但查看费用账单时，显示虚拟私有云VPC仍在继续计费。

图 1-1 虚拟私有云列表

原因说明

- 在费用中心中，当“产品类型”为“虚拟私有云VPC”时，其下存在的计费资源如**表1-2**所示，请您查看是否存在以下资源产生计费。查看方法请参见**如何查看虚拟私有云VPC的费用账单?** 。

表 1-2 虚拟私有云 VPC 计费产品说明

产品类型	产品
虚拟私有云VPC	弹性公网IP
	固定带宽
	带宽加油包
	VPCEP终端节点

- 由于存在计费延迟情况，按需计费的资源删除后，并不会立刻对之前的消费进行扣款结算。在结算周期结束之后，才会生成账单并执行扣款。

1.3 如何查看虚拟私有云 VPC 的费用账单?

虚拟私有云VPC服务下包含了多种产品资源，部分资源您可以免费使用，部分资源需要支付费用，计费资源详情请参见**表1-3**。

表 1-3 虚拟私有云 VPC 计费产品说明

产品类型	产品
虚拟私有云VPC	弹性公网IP
	固定带宽
	带宽加油包
	VPCEP终端节点

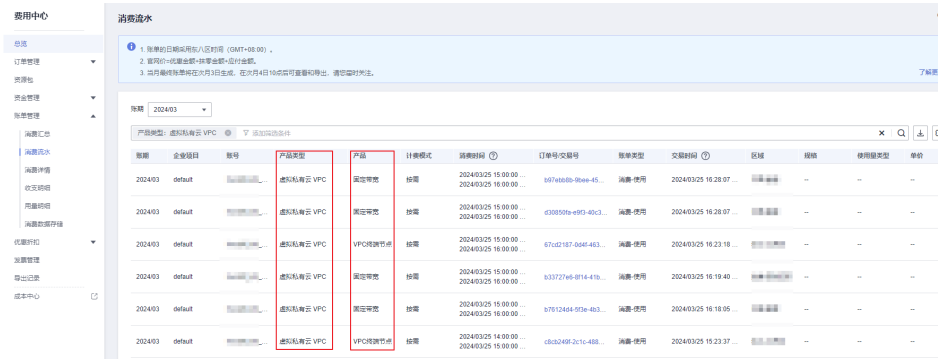
当您在费用中心查看账单时，产生费用的产品类型为“虚拟私有云 VPC”时，您可以参考以下操作查看对应的账单。

操作步骤

1. 在控制台右上方区域，选择“费用与成本 > 费用账单”。
   进入消费汇总页面。
2. 在左侧导航栏，选择“消费流水”。
   进入消费流水列表页面。
3. 在消费流水列表中，产品类型筛选“虚拟私有云 VPC”，系统过滤出相关的资源费用情况。
   - 弹性公网IP：表示收取的是弹性公网IP的保有费。
     您购买的按需计费弹性公网IP未绑定至任何实例（如ECS、ELB）时，会收取弹性公网IP保有费。
   - 固定带宽：表示收取的可能是以下资源的费用。
     - 弹性公网IP的带宽费用：
       - 包年/包月弹性公网IP的带宽费用：按照带宽大小和购买时长一次性收取带宽费用。

    - 按需计费弹性公网IP的带宽费用：如果您购买的弹性公网IP属于按需计费(按带宽计费)，则会按照带宽大小和使用时长收取带宽费用。
    - 按需计费弹性公网IP的流量费用：如果您购买的弹性公网IP属于按需计费(按流量计费)，则会按照您实际使用的流量收取流量费用。
  - 共享带宽的费用
  - 共享流量包的费用
- VPC终端节点：收取VPC终端节点的费用。

图 1-2 消费流水列表



1.4 弹性公网 IP 如何计费?

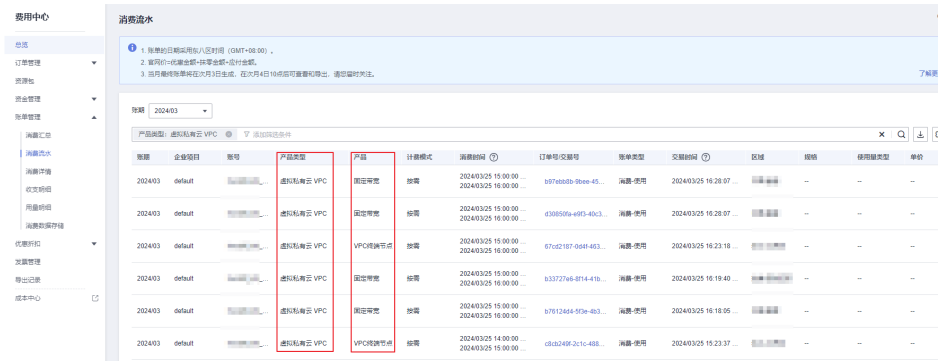
弹性公网IP和带宽的费用账单归属在虚拟私有云 VPC服务下，费用账单中计费的“产品”项目说明如下：

- 弹性公网IP：表示收取的是弹性公网IP的保有费。

  您购买的按需计费弹性公网IP未绑定至任何实例（如ECS、ELB）时，会收取弹性公网IP保有费。
- 固定带宽：表示收取的可能是以下资源的费用。
  - 弹性公网IP的带宽费用：
    - 包年/包月弹性公网IP的带宽费用：按照带宽大小和购买时长一次性收取带宽费用。
    - 按需计费弹性公网IP的带宽费用：如果您购买的弹性公网IP属于按需计费(按带宽计费)，则会按照带宽大小和使用时长收取带宽费用。
    - 按需计费弹性公网IP的流量费用：如果您购买的弹性公网IP属于按需计费(按流量计费)，则会按照您实际使用的流量收取流量费用。
  - 共享带宽的费用
  - 共享流量包的费用

以上计费项目的详细说明，请参见**弹性公网IP计费说明**。

图 1-3 消费流水列表

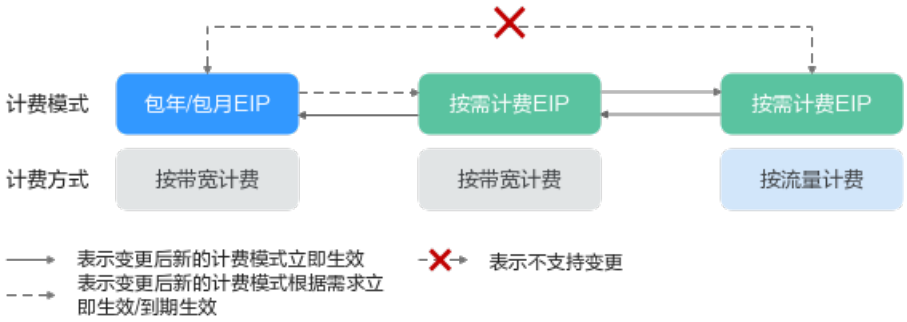


1.5 如何切换 EIP 计费方式中的“按需计费”和“包年/包月计费”？

表 1-4 弹性公网 IP 计费方式变更说明

计费方式变更场景	计费变更说明
包年/包月→按需计费	• 包年/包月EIP支持直接转为按需计费（按带宽计费）EIP。 • 包年/包月EIP不支持直接转为按需计费（按流量计费）EIP。变更方法如下： 1. 包年/包月EIP转为按需计费（按带宽计费）EIP。 2. 按需计费（按带宽计费）EIP转为按需计费（按流量计费）EIP。 选择到期后转为按需计费（按带宽计费）EIP，变更操作成功后，新的计费方式不会立即生效，需要等包年/包月EIP到期后，新的计费方式才会生效。 选择即时转为按需计费（按带宽计费）EIP，变更操作成功后，新的计费方式将立即生效。
按需计费→包年/包月	• 按需计费（按带宽计费）EIP支持直接转为包年/包月EIP。 • 按需计费（按流量计费）EIP不支持直接转为包年/包月EIP。变更方法如下： 1. 按需计费（按流量计费）EIP转为按需计费（按带宽计费）的EIP。 2. 按需计费（按带宽计费）EIP转为包年/包月EIP。 该变更操作成功后，新的计费方式将立即生效。

图 1-4 EIP 计费模式变更



包年/包月到期转按需计费（按带宽计费）

1. 进入**EIP列表页面**。
2. 在弹性公网IP列表中，支持操作单个弹性公网IP或者批量操作多个弹性公网IP，请您根据需要选择以下指导，将包年/包月EIP转为按需计费（按带宽计费）EIP：
   - 单个弹性公网IP:
     在弹性公网IP所在行的“操作”列下，选择“更多 ”>“到期转按需”。
   - 多个弹性公网IP：
     勾选多个弹性公网IP，在列表左上方“更多”下，单击“到期转按需”。
3. 在确认弹窗中，确认无误后，单击“是”。
   跳转至费用中心的到期转按需页面 。
4. 确认IP信息，单击“到期转按需”，完成修改。

按需计费（按带宽计费）转包年/包月

1. 进入**EIP列表页面**。
2. 在弹性公网IP列表中，支持操作单个弹性公网IP或者批量操作多个弹性公网IP，请您根据需要选择以下指导，将按需计费（按带宽计费）EIP转为包年/包月EIP：
   - 单个弹性公网IP:
     在弹性公网IP所在行的“操作”列下，选择“更多 ”>“转包年/包月”。
   - 多个弹性公网IP：
     勾选多个弹性公网IP，在列表左上方，选择“更多 ”>“转包年/包月”。
3. 在确认弹窗中，确认无误后，单击“是”。
4. 在“按需转包年/包月”页面，设置续费时长等参数。
5. 设置完成后，单击“去支付”，并根据界面引导完成支付即可。

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

表 1-5 弹性公网 IP 计费方式变更说明

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

按需计费（按流量计费）计费和按需计费（按带宽计费）互相转换

1. 进入**EIP列表页面**。
2. 在弹性公网IP列表中，在待修改弹性公网IP所在行的“操作”列，选择“更多 ”>“修改带宽”。
3. 在“修改带宽”页面，根据界面提示修改计费方式。
   该界面还支持修改带宽名称和带宽大小。
4. 修改完成后，单击“下一步”。
5. 在规格确认页面，单击“提交”，完成修改。

说明

- 变更计费方式不会更换EIP的地址，也不会中断EIP的使用，对您的业务不会产生影响。
- 以上变更场景仅适用于**按需计费模式**的弹性公网IP。
- **包年/包月计费**的EIP不支持直接转为**按需计费（按流量计费）**的EIP。如需转换，请参考**如何切换EIP计费方式中的“按需计费”和“包年/包月计费”？**。

2 虚拟私有云与子网类

2.1 什么是虚拟私有云?

虚拟私有云（Virtual Private Cloud，VPC）是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。VPC丰富的功能帮助您灵活管理云上网络，包括创建子网、设置安全组和网络ACL、管理路由表等。此外，您可以通过弹性公网IP连通云内VPC和公网网络，通过云专线、虚拟专用网络等连通云内VPC和线下数据中心，构建混合云网络，灵活整合资源。

虚拟私有云产品架构

接下来，本文档将从虚拟私有云VPC的基本元素、VPC的网络安全、VPC的网络连接以及VPC的网络运维方面进行介绍，带您详细了解VPC的产品架构。

图 2-1 VPC 产品架构

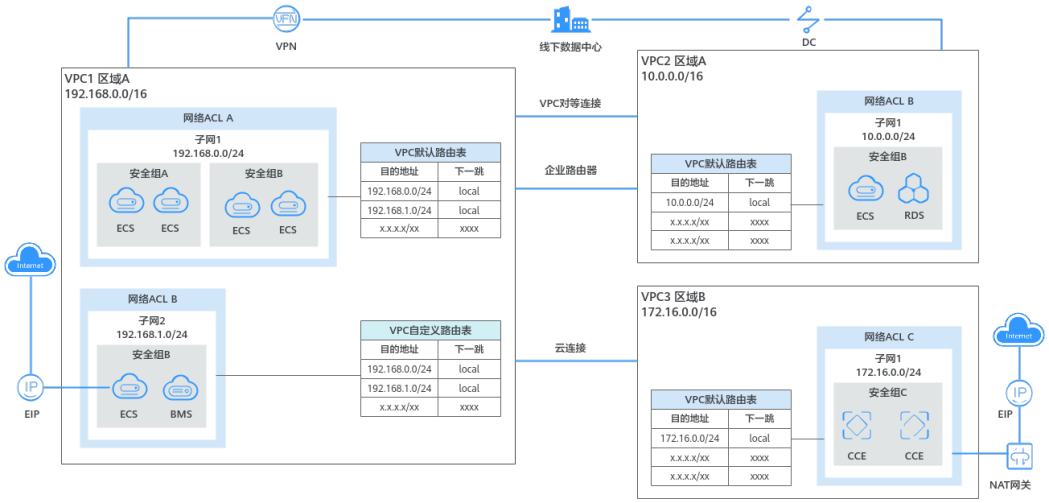


表 2-1 VPC 的产品架构介绍

项目分类	简要说明	详细说明
VPC的基本元素	VPC是您在云上的私有网络，您可以指定VPC的IP地址范围，然后通过在VPC内划分子网来进一步细化IP地址范围。同时，您可以配置VPC内的路由表来控制网络流量走向。 不同VPC之间的网络不通，同一个VPC内的多个子网之间网络默认互通。	• IP地址范围：您在创建VPC时，需要指定VPC的IP网段，支持的网段为10.0.0.0/8~24、172.16.0.0/12~24和192.168.0.0/16~24。 • 子网：您可以根据业务需求在VPC内划分子网，VPC内至少需要包含一个子网。实例（云服务器、云容器、云数据库等）必须部署在子网内，实例的私有IP地址从子网网段中分配。 更多信息请参见**子网**。 • 路由表：在创建VPC时，系统会为您自动创建一个默认路由表，默认路由表确保同一个VPC内的子网网络互通。您可以在默认路由表中添加路由来管控网络，如果默认路由表无法满足需求时，您还可以创建自定义路由表。 更多信息请参见**路由表和路由概述**。
VPC的网络安全	安全组与网络ACL（Access Control List）用于保障VPC内部署实例的安全。	• 安全组：对实例进行防护，您可以在安全组中设置入方向和出方向规则，将实例加入安全组内后，该实例会受到安全组的保护。 更多信息请参见**安全组和安全组规则概述**。 • 网络ACL：对整个子网进行防护，您可以在网络ACL中设置入方向和出方向规则，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。 更多信息请参见**网络ACL概述**。 相比安全组，网络ACL的防护范围更大。当安全组和网络ACL同时存在时，流量优先匹配网络ACL规则，然后匹配安全组规则。 更多信息请参见**VPC访问控制概述**。

项目分类	简要说明	详细说明
VPC的网络连接	您可以使用VPC和云上的其他网络服务，基于您的业务诉求，构建不同功能的组网。 • 连通同区域VPC：通过VPC对等连接或者企业路由器ER，连通同区域的不同VPC。 • 连通跨区域VPC：通过云连接CC，连通不同区域的VPC。 • 连通VPC和公网：通过弹性公网IP (EIP)或者NAT网关，连通云内VPC和公网。 • 连通VPC和线下数据中心：通过云专线DC或者虚拟专用网络VPN，连通云内VPC和线下数据中心。	• 连通同区域VPC – VPC对等连接：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。 更多信息请参见**对等连接概述**。 – 企业路由器ER：企业路由器作为一个云上高性能集中路由器，可以同时接入多个VPC，实现同区域VPC互通。 更多信息请参见**什么是企业路由器**。 对等连接免费，企业路由器收费，相比使用VPC对等连接，企业路由器连接VPC构成中心辐射性组网，网络结构更加简洁，方便扩容和运维。 • 连通跨区域VPC 云连接CC：云连接可以接入不同区域的VPC，快速实现跨区域网络构建。更多信息请参见**什么是云连接**。 • 连通VPC和公网 – EIP：EIP是独立的公网IP地址，可以为实例绑定EIP，为实例提供访问公网的能力。 更多信息请参见**什么是弹性公网IP**。 – NAT网关：公网NAT网关能够为VPC内的实例（ECS、BMS等），提供最高20Gbit/s能力的网络地址转换服务，实现多个实例使用一个EIP访问公网。 更多信息请参见**什么是NAT网关**。 • 连通VPC和线下数据中心 – DC：DC用于搭建线下数据中心和云上VPC之间高速、低时延、稳定安全的专属连接通道，通过DC可以构建大规模混合云组网。 更多信息请参见**什么是云专线**。 – VPN：VPN用于在线下数据中心和云上VPC之间建立一条安全加密的公网通信隧道。 更多信息请参见**什么是虚拟专用网络**。 相比通过DC构建混合云，使用VPN更加快速，成本更低。

项目分类	简要说明	详细说明
VPC的网络运维	VPC流日志和流量镜像可以监控VPC内的流量，用于网络运维。	• 流日志：通过流日志功能可以实时记录VPC中的流量日志信息。通过这些日志信息，您可以优化安全组和网络ACL的控制规则，监控网络流量、进行网络攻击分析等。更多信息请参见**VPC流日志概述**。 • 流量镜像：通过流量镜像功能可以镜像弹性网卡符合筛选条件的报文到目的实例中，在目的实例中进行流量分析，不会影响运行业务的实例，适用于网络流量检查、审计分析以及问题定位等场景。更多信息请参见**流量镜像概述**。

2.2 VPC 中可以使用哪些网段（CIDR）？

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

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

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

表 2-2 VPC 网段（RFC 1918）

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

除了上述地址，您还可以使用任何可公共路由的IPv4地址（非RFC 1918指定的私有IPv4地址范围），但是必须排除**表2-3**中的系统预留地址和公网保留地址：

表 2-3 系统预留地址和公网保留地址

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

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

2.3 一个用户可以创建多少个 VPC?

默认情况下，一个用户在单个区域可创建的VPC数量为5个。

但是，不同用户根据其账户类型和服务等级享有不同的默认资源配额。具体请您在**配额限制**查看您的个人配额详情。

如果当前配额无法满足实际需求，请您**提交工单**申请提升配额。

2.4 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。

  您可以使用以下方法连通不同VPC之间的网络：
  - 通过VPC对等连接或者企业路由器ER，连通同区域的不同VPC。

    对等连接，请参见**对等连接简介**。

    企业路由器，请参见**什么是企业路由器**。
  - 通过云连接CC，连通不同区域的VPC。

    云连接，请参见**什么是云连接**。
- 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2-4**。

图 2-2 一个 VPC 内不同子网通信组网图

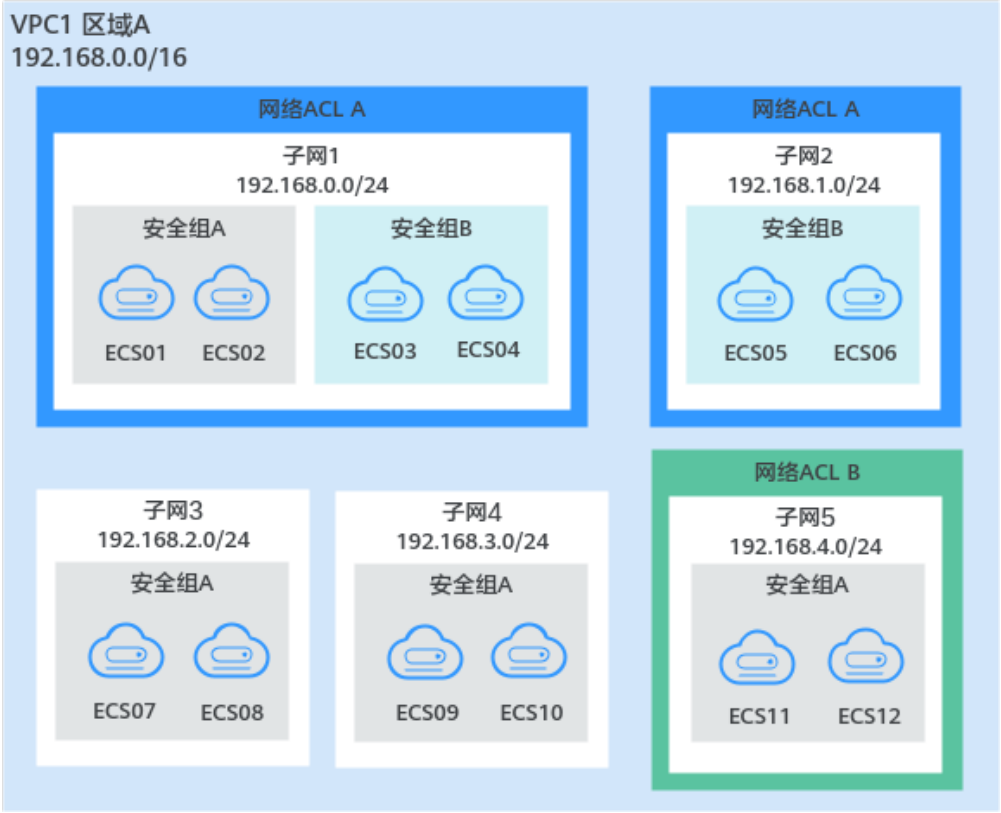


表 2-4 一个 VPC 内不同子网通信场景说明

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。

2.5 子网可以使用的网段是什么?

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

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

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

2.6 子网的网段是否可以修改?

子网创建成功后，不支持修改网段。

请您结合业务，提前合理规划好子网网段。

- 子网网段不能太小，需要确保子网内可用IP地址数量可以满足业务需求。子网网段中第一个地址和后三个地址为系统预留地址，不能供实际业务使用，比如子网（10.0.0.0/24）中，10.0.0.1为网关地址、10.0.0.253为系统接口、10.0.0.254为DHCP使用、10.0.0.255为广播地址。
- 子网网段也不能太大，以免后续扩展新的业务时，VPC内可用网段不够再创建新的子网。
- 子网网段避免冲突：如果子网所在的VPC与其他VPC、或者VPC与云下数据中心需要通信时，则VPC子网网段和网络对端网段不能相同，否则无法正常通信。

2.7 一个用户可以创建多少个子网?

默认情况下，一个用户在单个区域可创建的子网数量为100个。

但是，不同用户根据其账户类型和服务等级享有不同的默认资源配额。具体请您在**配额限制**查看您的个人配额详情。

如果当前配额无法满足实际需求，请您**提交工单**申请提升配额。

2.8 修改子网的 DHCP 租约时间如何立即生效?

场景说明

当您修改了子网的DHCP租约时间，对于子网内的实例（比如ECS）来说，当实例下一次续租时，新的租约时间将会生效，实例续租分为自动更新租约和手动更新租约两种，续租不会改变实例当前的IP地址。

- 如果需要新的DHCP租约时间立即生效，则需要参考本文档手动更新租约。手动更新租约可能会导致业务中断，请评估后谨慎操作。
- 如果不需要新的DHCP租约时间立即生效，则可以等待实例自动更新租约。待实例当前租约剩余一半时会首次尝试续租，如果续租失败，则等待当前租约剩余八分之一时，二次尝试续租，此时如果续租失败，那么租约到期后，IP地址将会被释放。为了避免IP地址被释放，建议您尝试手动更新租约。

关于DHCP租约更新时间的详细信息，如**表2-5**所示。

表 2-5 DHCP 租约时间更新说明

生效情况	更新方法	详细说明
DHCP租约时间会立即生效。	手动更新租约	手动触发实例续租，详细操作方法请参见**查看/更新DHCP租约到期时间（Windows系统）**或者**查看/更新DHCP租约到期时间（Linux系统）**。 如果业务允许，您也可以直接重启实例，重启后租约即会自动更新。 **须知** 手动更新租约和自动更新租约不同，手动更新租约时，会先释放当前实例已有的IP地址，再重新获取IP地址，所以在获取到新的租约前实例会暂时失去IP地址，可能导致业务流量中断，请先评估影响。

生效情况	更新方法	详细说明
DHCP租约时间不会立即生效。	自动更新租约	等待实例自动续租，实例会根据情况，在DHCP租约到期前，触发续租。 ● 首次续租：当原有租约时间剩余一半时，实例会启动首次自动续租。续租成功后，将会执行新的租约时间。续租失败时，则在DHCP租约到期前，尝试二次续租。 ● 二次续租：当首次续租失败时，则在原有租约时间剩余八分之一时，实例会再次自动续租。续租成功后，将会执行新的租约时间。续租失败时，则在DHCP租约到期后，IP地址会被释放。 比如，ECS的DHCP租约时间为30天，到期时间为2024-01-30。若您在2024-01-02将DHCP租约时间修改为10天。 ● 首次续租：当原租约时间剩余一半，即2024-01-15时，ECS会自动续租，续租成功后，新的租约将会在2024-01-25到期。当新的租约剩余一半时，即2024-01-20，ECS将会触发下一次续租。 ● 二次续租：当2024-01-15续租失败时，则在原租约时间剩余八分之一，即2024-01-26时，ECS会自动续租，续租成功后，新的租约将会在2024-02-05到期。如果二次续租失败，则在2024-01-30会释放ECS的IP地址。

查看/更新 DHCP 租约到期时间（Windows 系统）

1. 在控制台修改子网DHCP租约时间后，登录待刷新租约的云服务器。
2. 在搜索框中输入“cmd”，打开命令执行窗口。
3. 执行以下命令，查看云服务器当前DHCP租约的过期时间。
   ipconfig /all
4. 执行以下命令，更新DHCP租约。
   ipconfig /release && ipconfig /renew
5. 再次执行以下命令，查看新的DHCP租约过期时间。
   ipconfig /all

查看/更新 DHCP 租约到期时间（Linux 系统）

1. 在控制台修改子网DHCP租约时间后，登录待刷新租约的云服务器。
2. 执行以下命令，确认提供DHCP服务的客户端为dhclient。
   ps -ef | grep dhclient
   - 回显类似如下信息，表示存在dhclient对应进程，说明客户端是dhclient。其中**-lf**参数后，类型为**lease**的文件中存有租约信息。

     ```
     [root@ecs-A ~]# ps -ef | grep dhclient
     root       580   526  0 18:49 ?        00:00:00 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf /var/run/dhclient-eth0.pid -lf /var/lib/NetworkManager/
     ```

```
dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease -cf /var/lib/NetworkManager/
dhclient-eth0.conf eth0
root      1512  1470  0 18:50 pts/0    00:00:00 grep --color=auto dhclient
```

- 如果不存在dhclient进程，则本文档可能不适用，请您查找对应DHCP客户端的操作指令。

3. 执行以下命令，查看2的**lease**文件中当前DHCP租约信息。

   cat *lease*文件名称

   命令示例：

   cat /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease

   回显类似如下信息，**lease**文件中会保存历史DHCP租约信息，最后一个是最新的DHCP租约信息。

```
[root@ecs-A ~]# cat /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-
eth0.lease
lease {
  interface "eth0";
  fixed-address 172.16.0.54;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 108000000;
  option routers 172.16.0.1;
  option dhcp-message-type 5;
  option dhcp-server-identifier 172.16.0.254;
  option domain-name-servers 100.125.1.250,100.125.64.250;
  option interface-mtu 1500;
  option dhcp-renewal-time 54000000;
  option dhcp-rebinding-time 94500000;
  option rfc3442-classless-static-routes 0,172,16,0,1,32,169,254,169,254,172,16,0,1;
  option broadcast-address 172.16.0.255;
  option host-name "host-172-16-0-54";
  option domain-name "openstacklocal";
  renew 3 2025/06/18 21:46:42;
  rebind 3 2027/01/20 04:46:44;
  expire 5 2027/06/25 10:46:44;
}
lease {
  interface "eth0";
  fixed-address 172.16.0.54;
  option subnet-mask 255.255.255.0;
  option routers 172.16.0.1;
  option dhcp-lease-time 108000000;
  option dhcp-message-type 5;
  option domain-name-servers 100.125.1.250,100.125.64.250;
  option dhcp-server-identifier 172.16.0.254;
  option interface-mtu 1500;
  option dhcp-renewal-time 54000000;
  option broadcast-address 172.16.0.255;
  option rfc3442-classless-static-routes 0,172,16,0,1,32,169,254,169,254,172,16,0,1;
  option dhcp-rebinding-time 94500000;
  option host-name "host-172-16-0-54";
  option domain-name "openstacklocal";
  renew 3 2025/08/20 23:57:15;
  rebind 3 2027/01/20 04:50:00;
  expire 5 2027/06/25 10:50:00;
}
```

4. 执行以下命令，释放当前云服务器的IP地址。

   dhclient -r

5. 执行以下命令，获取新的DHCP租约。

   killall dhclient && systemctl restart NetworkManager

6. 执行以下命令，查看2的**lease**文件中最新的DHCP租约信息。

   cat *lease*文件名称

命令示例：

cat /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease

回显类似如下信息，**lease**文件中会保存历史DHCP租约信息，最后一个是更新后的DHCP租约信息。

```
[root@ecs-A ~]# cat /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease
lease {
  interface "eth0";
  fixed-address 172.16.0.54;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 108000000;
  option routers 172.16.0.1;
  option dhcp-message-type 5;
  option dhcp-server-identifier 172.16.0.254;
  option domain-name-servers 100.125.1.250,100.125.64.250;
  option interface-mtu 1500;
  option dhcp-renewal-time 54000000;
  option dhcp-rebinding-time 94500000;
  option rfc3442-classless-static-routes 0,172,16,0,1,32,169,254,169,254,172,16,0,1;
  option broadcast-address 172.16.0.255;
  option host-name "host-172-16-0-54";
  option domain-name "openstacklocal";
  renew 3 2025/08/20 23:57:15;
  rebind 3 2027/01/20 04:50:00;
  expire 5 2027/06/25 10:50:00;
}
lease {
  interface "eth0";
  fixed-address 172.16.0.54;
  option subnet-mask 255.255.255.0;
  option routers 172.16.0.1;
  option dhcp-lease-time 108000000;
  option dhcp-message-type 5;
  option domain-name-servers 100.125.1.250,100.125.64.250;
  option dhcp-server-identifier 172.16.0.254;
  option interface-mtu 1500;
  option dhcp-renewal-time 54000000;
  option broadcast-address 172.16.0.255;
  option rfc3442-classless-static-routes 0,172,16,0,1,32,169,254,169,254,172,16,0,1;
  option dhcp-rebinding-time 94500000;
  option host-name "host-172-16-0-54";
  option domain-name "openstacklocal";
  renew 4 2025/07/03 00:34:04;
  rebind 3 2027/01/20 04:52:43;
  expire 5 2027/06/25 10:52:43;
}Sub-eni
```

2.9 修改子网内的域名后，如何立即生效?

您可以在新创建子网，通过控制台中的“域名”参数，设置DNS域名后缀，访问某个域名时，只需要输入域名前缀，子网内的云服务器会自动匹配设置的域名后缀。子网创建完成后，“域名”参数支持修改，修改完成后的生效策略如表2-6所示。

表 2-6 不同云服务器生效策略

云服务器情况	生效策略
子网内新创建的云服务器	自动同步域名配置，无需额外配置。

云服务器情况	生效策略
子网内的存量云服务器	需要执行以下操作，更新DHCP配置使域名生效。以下方法任意选择一种即可： • 重启云服器 • 重启DHCP Client服务：**service dhcpd restart** • 重启网络服务：**service network restart** **说明** 对于不同操作系统的云服务器，更新DHCP配置的命令不同，此处命令仅供您参考。

2.10 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**

须知

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

如果您的虚拟私有云和子网无法删除，请您**提交工单**联系客服处理。

删除子网

删除子网时候，您可以参考**表2-7**，对照管理控制台的提示信息，根据对应的解决办法处理。

表 2-7 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。 VPC权限的详细说明，请参见**权限管理**。

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，快速查找服务资源，请参见**快速查找账号下的云服务资源**。 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2-8**，对照管理控制台的提示信息，找到对应的解决办法处理。

表 2-8 虚拟私有云删除方法

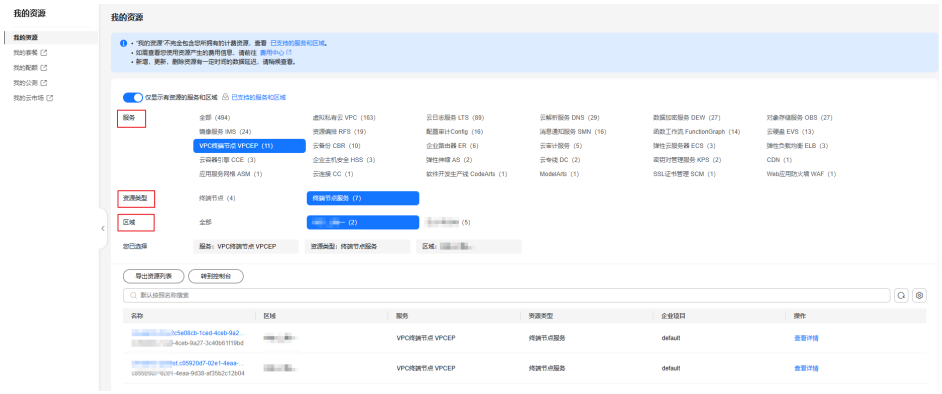
提示信息	原因	处理方法
您的权限不足	您的账号没有删除虚拟私有云的权限。	请您联系账号管理员为您的账号授权后，重新尝试删除虚拟私有云。 VPC权限的详细说明，请参见**权限管理**。
VPC的路由表中存在自定义路由，或者VPC被终端节点服务使用，请删除对应资源后重试。	虚拟私有云的路由表中存在自定义路由。	请您删除路由表中的自定义路由后，重新尝试删除虚拟私有云。 1. 在虚拟私有云列表中，单击“路由表”列对应的数字超链接。 进入路由表列表页面。 2. 删除自定义路由的方法，请参见**删除路由**。
	虚拟私有云已被终端节点服务使用。	您需要在终端节点服务控制台中，查找目标终端节点服务并删除。 删除方法，请参见**删除终端节点服务**。
VPC被VPCEP终端节点服务使用，请删除对应资源后重试。	虚拟私有云已被终端节点服务使用。	您需要在终端节点服务控制台中，查找目标终端节点服务并删除。 删除方法，请参见**删除终端节点服务**。

提示信息	原因	处理方法
“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** • **删除自定义路由表**
VPC已被云专线DC的虚拟网关使用，请删除资源后重试。	虚拟私有云已被云专线DC的虚拟网关使用。	您需要在云专线控制台中，查找目标虚拟网关并删除。 删除方法，请参见**删除虚拟网关**。
VPC已被VPN网关使用，请删除资源后重试。	虚拟私有云已被VPN网关使用。	您需要在虚拟专用网络控制台中，查找目标VPN网关并删除。 删除方法，请参见**删除VPN网关**。
VPC已被云连接CC使用，请在CC中移除VPC后重试。	虚拟私有云已被云连接CC使用。	您需要在云连接控制台中，查找目标云连接，并移出云连接中的虚拟私有云。 移除方法，请参见**移除云连接中的虚拟私有云**。
删除最后一个VPC时，请删除本区域内所有的自定义安全组后重试。	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，请删除本区域内所有的EIP后重试。	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**释放弹性公网IP**。

快速查找账号下的云服务资源

1. 登录管理控制台。
2. 在控制台右上角，单击“资源”，选择“我的资源”。
   进入“我的资源”页面。

图 2-3 我的资源



3. 在“我的资源”页面，设置搜索条件，快速匹配可能使用子网的资源。
   - 服务：使用子网的常用服务资源，如表2-9所示。
     表格中仅列举部分常用资源，如果您还有其他资源，请逐一排查。
   - 资源类型：服务细分不同的资源类型，请按照实际界面展示，逐一排查。
   - 区域：VPC和子网只能给同区域的资源使用，此处请选择VPC和子网所在的区域，筛查同一个区域的云服务资源。

表 2-9 使用子网的常用资源

产品分类	产品/实例名称
计算	弹性云服务器ECS
	裸金属服务器BMS
	云容器引擎 CCE
	云容器实例 CCI
容器服务	应用服务网格 ASM
网络	弹性负载均衡 ELB
	NAT网关
	VPC终端节点
数据库	云数据库 GaussDB
	云数据库 RDS
	文档数据库服务 DDS
	分布式数据库中间件 DDM
应用服务	分布式缓存服务 DCS： • Redis实例 • Memcached实例

产品分类	产品/实例名称
	分布式消息服务 DMS： • Kafka实例 • RabbitMQ实例
EI企业智能	MapReduce服务
	数据仓库服务 DWS
	云搜索服务 CSS

如果已完成资源排查后，仍然无法正常删除子网，请**提交工单**联系客服。

2.11 ECS 是否支持切换虚拟私有云?

支持。

您可以在弹性云服务器界面的操作列单击“切换VPC”进行切换。

具体注意事项及操作步骤请参考：**切换虚拟私有云**。

2.12 修改 ECS 的系统时间后，IP 地址丢失怎么办?

问题原因

当ECS系统时间修改跨度超过您的DHCP租约到期时间，可能会导致IP地址丢失。

因为ECS修改后的系统时间超过了DHCP租约到期时间时，ECS实例将会触发续租，即自动更新DHCP租约时间，如果续租失败，则会导致IP地址丢失。

解决方法

如果您必须要进行大跨度的时间更改，在修改之前请先把弹性云服务器的IP地址获取方式修改为静态配置。

2.13 怎样修改云服务器的 DNS 服务器地址?

操作场景

您可以参考本章节修改ECS的DNS服务器地址，并使新的DNS地址在ECS内立即生效。

本章节以将公共DNS服务器地址修改为华为云提供的默认DNS服务器地址为例，具体操作步骤如下。

1. **查询ECS的DNS服务器地址**
2. **切换DNS服务器为内网DNS**
3. **更新ECS内的DNS服务器地址**

背景知识

通过华为云创建的ECS默认使用华为云提供的内网DNS进行解析。内网DNS不影响ECS对公网域名的访问。同时，还可以不经公网，直接通过内网DNS访问其他云上服务内部地址，如OBS、SMN等，访问时延小，性能高。

在内网域名功能上线之前创建的ECS，其关联VPC子网默认设置的DNS服务器为公共DNS，IP地址为114.114.114.114。为了使这部分ECS服务器能够使用内网域名功能，建议将ECS服务器关联VPC子网的DNS服务器修改为华为云的内网DNS。内网DNS地址请参见**华为云提供的内网DNS地址是多少？**。

查询 ECS 的 DNS 服务器地址

1. 登录管理控制台。
2. 选择“计算 > 弹性云服务器 ECS”。
   进入“弹性云服务器”页面。
3. 在ECS列表中，单击目标ECS服务器名称。
4. 在ECS服务器详情页面，单击“虚拟私有云”对应的VPC名称。
   进入“虚拟私有云”页面。
5. 在“虚拟私有云”页面的VPC列表中，单击“子网”列的子网数量。
   进入“子网”页面。
6. 在“子网”页面，单击子网列表中的子网名称。
   在子网“基本信息”的“网关和DNS”区域可查看当前ECS服务器使用的DNS服务器地址。

切换 DNS 服务器为内网 DNS

如果ECS服务器当前DNS不是华为云内网DNS，要使用华为云内网DNS进行解析，需要切换DNS服务器为华为云内网DNS。

1. 在子网“基本信息”的“网关和DNS”区域，单击“DNS服务器地址”后面的“  ”。
2. 修改子网的“DNS服务器地址”为华为云内网DNS。

更新 ECS 内的 DNS 服务器地址

VPC子网的DNS服务器地址修改后，ECS服务器的DNS不会立即更新。

如果要立即更新ECS服务器的DNS，可以采用以下两种方法。

- 重启操作系统，ECS服务器重新向DHCP服务器获取DNS信息。

  须知

  重启操作系统会造成业务中断，请在业务低峰期谨慎操作。

  ECS服务器的DHCP租约期结束后，DHCP服务器会重新向ECS服务器分配IP地址、更新DNS信息。
- 通过dhclient，获取修改后的DNS服务器地址。

a. 登录云服务器。

ECS有多种登录方法，具体请参见**登录弹性云服务器**。

b. 执行以下命令，查看当前云服务器的DNS配置地址。

cat /etc/resolv.conf

回显类似如下信息，114.114.114.114是旧的DNS服务器地址。

```
[root@ecs-[redacted]-01 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search openstacklocal
nameserver 114.114.114.114
options timeout:1 single-request-reopen
```

c. 执行以下命令，查看dhclient进程是否已存在。

ps -ef | grep dhclient | grep -v grep

回显类似如下信息，以CentOS 8.1为例，表示没有进程。

需要执行**dhclient**命令启动进程，并再次确认dhclient进程存在。

```
[root@ecs-[redacted] ~]# ps -ef | grep dhclient | grep -v grep
[root@ecs-[redacted] ~]# dhclient
[root@ecs-[redacted] ~]# ps -ef | grep dhclient | grep -v grep
root        5712       1  0 09:52 ?        00:00:00 dhclient
```

回显类似如下信息，以CentOS 7.2为例，表示已有进程。

```
[root@ecs-[redacted]-01 ~]# ps -ef | grep dhclient | grep -v grep
root      651   472  0 10:36 ?        00:00:00 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf /var/run/dhclient-eth0.pid -lf /var/lib/NetworkManager/dhclient-5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03-eth0.lease -cf /var/lib/NetworkManager/dhclient-eth0.conf eth0
```

d. 执行以下命令，释放旧的DNS服务器地址。

dhclient -r

e. 执行以下命令，重新启动dhclient进程，获取新的DNS服务器地址。

dhclient

f. 执行以下命令，查看当前云服务器的DNS配置地址。

cat /etc/resolv.conf

回显类似如下信息，100.125.1.250和100.125.64.250是新的DNS服务器地址。

```
[root@ecs-[redacted]-01 ~]# dhclient -r
[root@ecs-[redacted]-01 ~]# dhclient
[root@ecs-[redacted]-01 ~]# cat /etc/resolv.conf
options timeout:1 single-request-reopen
; generated by /usr/sbin/dhclient-script
search openstacklocal
nameserver 100.125.1.250
nameserver 100.125.64.250
```

3 弹性公网 IP 类

3.1 如何创建或找回指定的弹性公网 IP?

当您想找回已释放的弹性公网IP或申请一个指定的弹性公网IP时，您可以通过API接口来实现。在申请弹性公网IP时请将“ip_address”的值设置为您想找回或指定的IP地址。详情请参见**《弹性公网IP API参考》**。

说明

- 如果该地址已被分配给其他用户则无法申请成功。
- 管理控制台不支持找回或创建指定的弹性公网IP。

3.2 弹性公网 IP、私有 IP 和虚拟 IP 之间有何区别?

云上不同IP地址实现的功能不同，**图3-1**展示了IP地址架构图，关于IP的详细介绍请参见**表3-1**。

图 3-1 IP 地址架构图

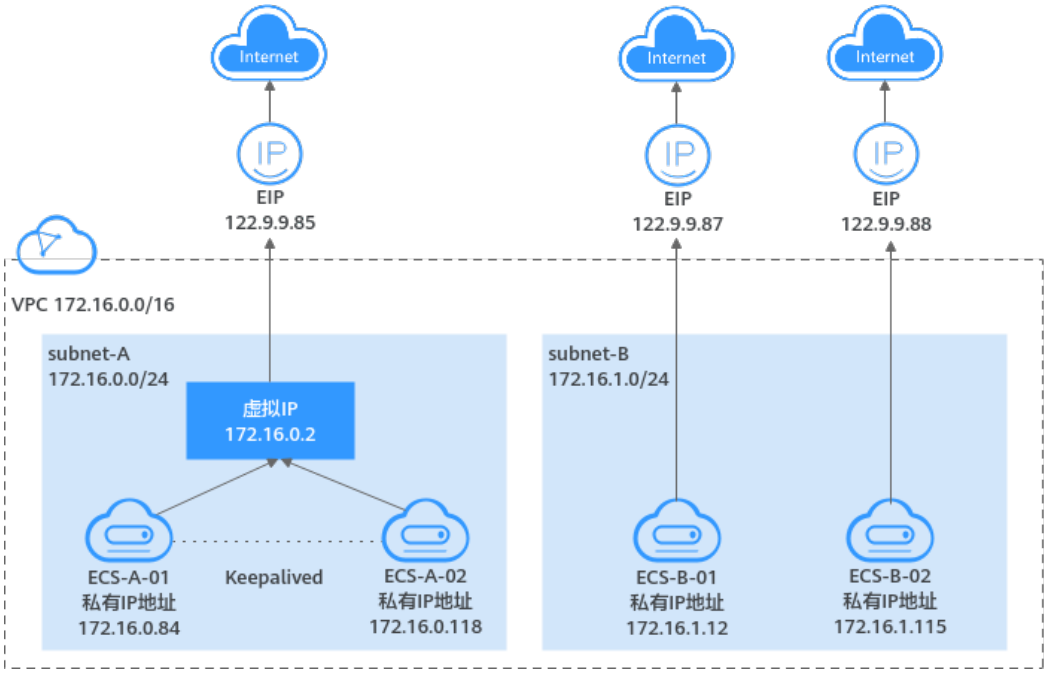


表 3-1 不同 IP 地址功能说明

IP地址分类	IP地址说明	示例
私有IP	您在VPC子网内创建弹性云服务器时，系统会基于子网内的可用IP地址，给弹性云服务器分配私有IP地址，私有IP地址主要用于云内网络通信，不能访问Internet。	• ECS-A-01的私有IP地址为172.16.0.84 • ECS-B-01的私有IP地址为172.16.1.12

IP地址分类	IP地址说明	示例
虚拟IP	虚拟IP（Virtual IP Address）是从VPC子网网段中划分的一个内网IP地址，是一种可以独立申请和删除的内网IP地址，适用于以下场景： • 将一个或者多个虚拟IP同时绑定至一个云服务器，可以通过任意一个IP地址（私有IP/虚拟IP）访问云服务器。通常当单个云服务器内同时部署了多种业务，此时可以通过不同的虚拟IP访问各个业务。 • 将一个虚拟IP同时绑定至多个云服务器，虚拟IP需要搭配高可用软件（比如Keepalived），用来搭建高可用的主备集群。为了提升服务的高可用性，避免单点故障，您可以用“一主一备”或“一主多备”的方法组合使用云服务器，这些云服务器对外呈现为一个虚拟IP。当主云服务器故障时，备云服务器可以转为主云服务器并继续对外提供服务，以此达到高可用性HA（High Availability）的目的。 虚拟IP的更多介绍请参见**虚拟IP简介**，高可用集群搭建方法请参见**使用虚拟IP和Keepalived搭建高可用Web集群**。	虚拟IP（172.16.0.2）同时绑定至ECS-A-01和ECS-A-02，结合keepalived可实现ECS-A-01和ECS-A-02的主备倒换。
弹性公网IP	弹性公网IP是云上资源访问Internet使用的IP地址，可以和实例灵活绑定或者解绑。 • 在虚拟IP场景，您可以将弹性公网IP绑定至虚拟IP，实现虚拟IP后端的弹性云服务器访问Internet。 • 您可以将弹性公网IP直接绑定至弹性云服务器上，实现弹性云服务器访问Internet。 弹性公网IP的更多介绍请参见**弹性公网IP简介**。	• 将EIP（122.9.9.85）绑定至虚拟IP（172.16.0.2），实现ECS-A-01和ECS-A-02访问Internet。 • 将EIP（122.9.9.87）绑定至ECS-B-01，实现ECS-B-01访问Internet。

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

可以。

按需计费的弹性公网IP可以从独享带宽变更为共享带宽使用。

包年/包月的弹性公网IP不能从独享带宽变更为共享带宽使用。

3.4 一个 EIP 可以绑定至几个 ECS 使用?

一个EIP只能绑定至一个ECS使用。

一个EIP无法直接供多个ECS共同使用，且EIP和ECS必须在同一个区域。如要实现多个ECS共用EIP，您需要搭配NAT网关服务，可实现VPC内的多个ECS共享一个EIP主动访问公网或者面向公网提供服务。

更多内容请参见**《NAT网关用户指南》**。

3.5 如何通过外部网络访问绑定 EIP 的 ECS?

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(Linux SSH“TCP22”端口、Windows RDP “TCP3389”端口除外)，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。

3.6 弹性公网 IP 的分配策略是什么?

新 申请的弹性公网IP默认是随机分配。

为防止误删除操作，EIP存在24小时缓存机制，对于已释放过弹性公网IP的用户，24小时内会优先分配之前使用过的EIP。

若超过24小时，需要找回已释放的EIP，请参见**如何创建或找回指定的弹性公网IP?** 。

如需申请新的弹性公网IP地址，建议您先申请新的EIP后再释放旧的EIP。

3.7 弹性公网 IP 是否支持变更绑定的弹性云服务器?

支持。

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

再将弹性公网IP绑定到目标弹性云服务器，如何绑定请参考**绑定云资源**。

相关操作：为弹性云服务器更换绑定的弹性公网IP，请参考**更换弹性公网IP**。

3.8 购买弹性公网 IP 时，是否可以指定 IP 地址?

新申请的弹性公网IP默认是随机分配。

- 用户释放弹性公网IP后，24小时内重新申请EIP时，会优先分配被释放的这个EIP。
- 用户释放弹性公网IP24小时后，其他用户才可以通过调用API的方式申请被释放的这个EIP。

申请指定的弹性公网IP地址只能通过调用API的方式，API信息请参见**申请弹性公网IP**。

3.9 如何查询 EIP 归属地?

如您需查询已购买EIP资源的归属地，可通过第三方网站进行查询，例如：**https://www.ipip.net/ip.html** 。

- 第三方网站可能会有IP地址数据库更新不及时的情况，会出现查询结果与实际区域不同的情况，请酌情选择。
- 如果其他第三方网站的查询结果和**https://www.ipip.net/ip.html**不一致，请以**https://www.ipip.net/ip.html**为准 。
- 如果**https://www.ipip.net/ip.html**查询结果和购买时选择的EIP区域不一致，请以购买时选择的区域为准。

  说明

  在“华北-乌兰察布一”区域购买的EIP的归属地为北京。
- 如果您的业务调用第三方数据库查询到的EIP归属地和实际归属地不符，导致业务受到影响，请您**提交工单**。

如您对EIP归属仍有疑问，可以**提交工单**进行查询。

3.10 如何为实例解绑已有弹性公网 IP 并绑定新的弹性公网 IP?

场景一：为弹性云服务器解绑已有 EIP 并绑定新的 EIP

1. 解绑已有弹性公网IP。
   a. 进入**EIP列表页面**。
   b. 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”。
   c. 单击“是”。
2. 申请新的弹性公网IP。

   说明

   当您已有需要绑定的EIP时，请忽略此步骤。

   a. 进入**EIP列表页面**。
   b. 在“弹性公网IP”界面，单击“购买弹性公网IP”。

c. 根据界面提示配置参数。
d. 单击“立即购买”。

3. 绑定新申请的弹性公网IP。
   a. 进入**EIP列表页面**。
   b. 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”。
   c. 选择实例。
   d. 单击“确定”。
4. 释放已被解绑的弹性公网IP。

   说明

   当已被解绑的EIP不再使用时，您可以释放EIP。解绑后如果不及时释放该弹性公网IP，会产生弹性公网IP保有费。

   a. 进入**EIP列表页面**。
   b. 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”。
   c. 单击“是”。

场景二：为弹性负载均衡解绑已有 EIP，并绑定新的 EIP

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

   说明

   当您已有需要绑定的EIP时，请忽略此步骤。

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

   说明

   当已被解绑的EIP不再使用时，您可以释放EIP。解绑后如果不及时释放该弹性公网IP，会产生弹性公网IP保有费。

场景三：为 NAT 网关解绑已有 EIP 并绑定新的 EIP

1. 申请新的弹性公网IP，请参考**2**。

说明

当您已有需要绑定的EIP时，请忽略此步骤。

2. 修改SNAT规则。

   修改SNAT规则请参考**修改SNAT规则**，在弹性公网IP列表中勾选新申请的弹性公网IP，取消已有弹性公网IP。

3. 修改DNAT规则。

   修改DNAT规则请参考**修改DNAT规则**，在“弹性公网IP”中重新选择为新申请的弹性公网IP。

4. 释放已被替换的EIP，请参考**4**。

说明

当已被解绑的EIP不再使用时，您可以释放EIP。解绑后如果不及时释放该弹性公网IP，会产生弹性公网IP保有费。

3.11 EIP 是否支持跨区域绑定?

弹性公网IP不支持跨区域绑定。

弹性公网IP和云资源必须在同一个区域。

例如“中国-香港”的弹性公网IP不能绑定到“亚太-新加坡”的云资源上。

3.12 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。

示例情况如下：

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。

4 对等连接类

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。

4.2 对等连接是否可以连通不同区域的 VPC?

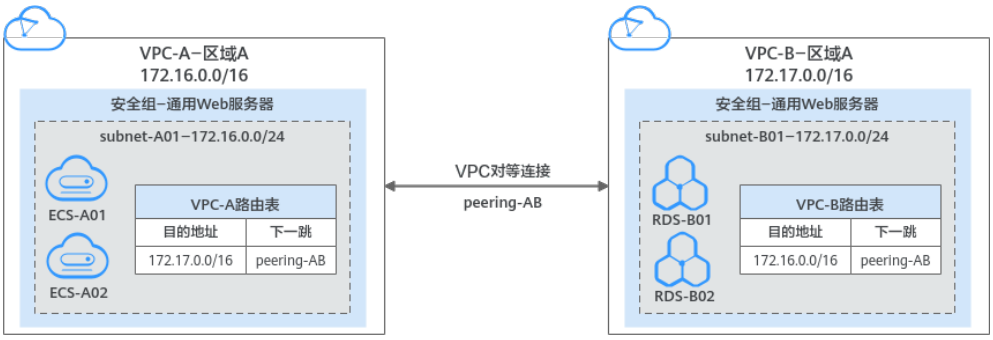
VPC对等连接是用来连接相同区域的VPC，不支持连通不同区域的VPC。

VPC对等连接仅支持连通同区域VPC，如果您的VPC位于不同的区域，则请您使用**云连接**。

接下来，通过**图4-1**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 4-1 对等连接组网



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图4-2，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。

图 4-2 对等连接网络不通排查思路

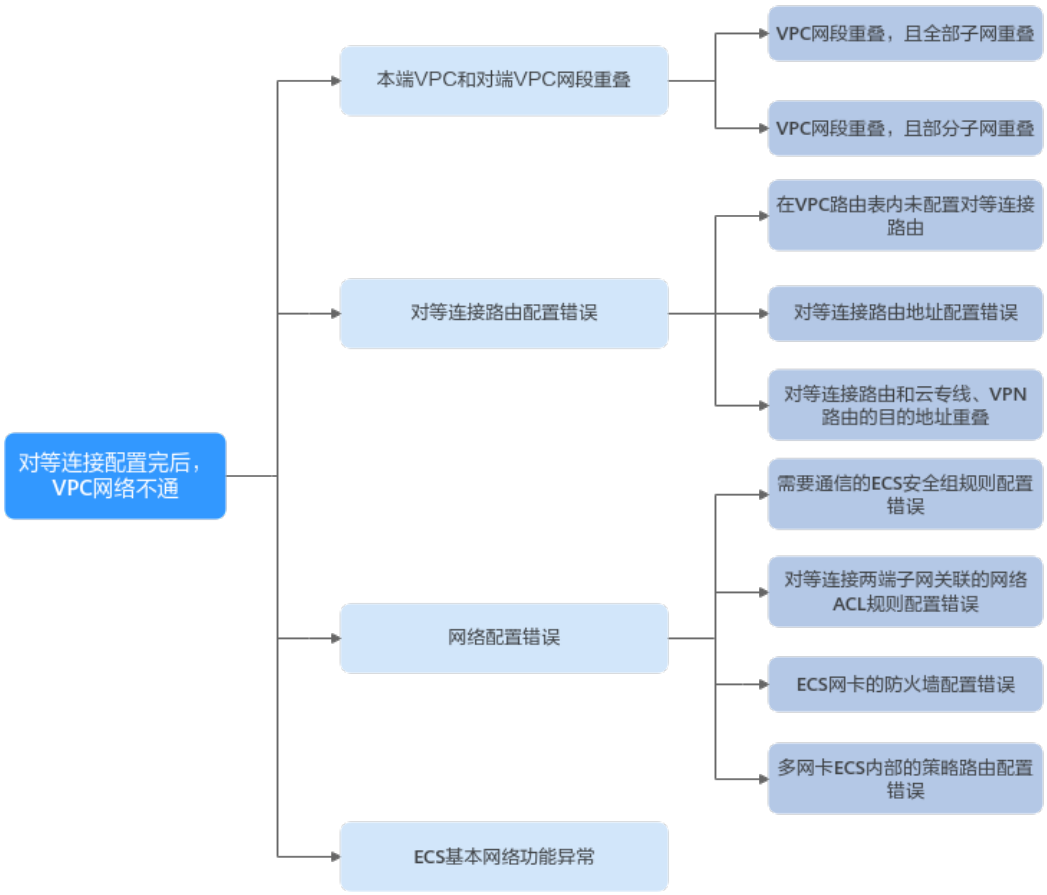


表 4-1 排查思路-对等连接不通

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

须知

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

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4-2**所示。

表 4-2 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4-3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。
VPC网段重叠，且部分子网重叠	组网图如图4-4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4-5。

图 4-3 VPC 网段重叠，且全部子网重叠(IPv4)

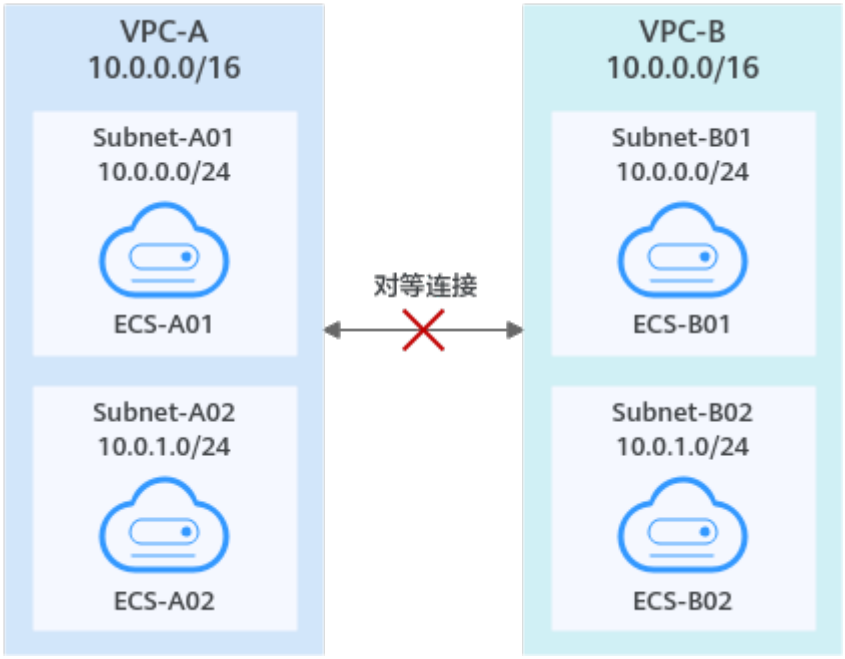
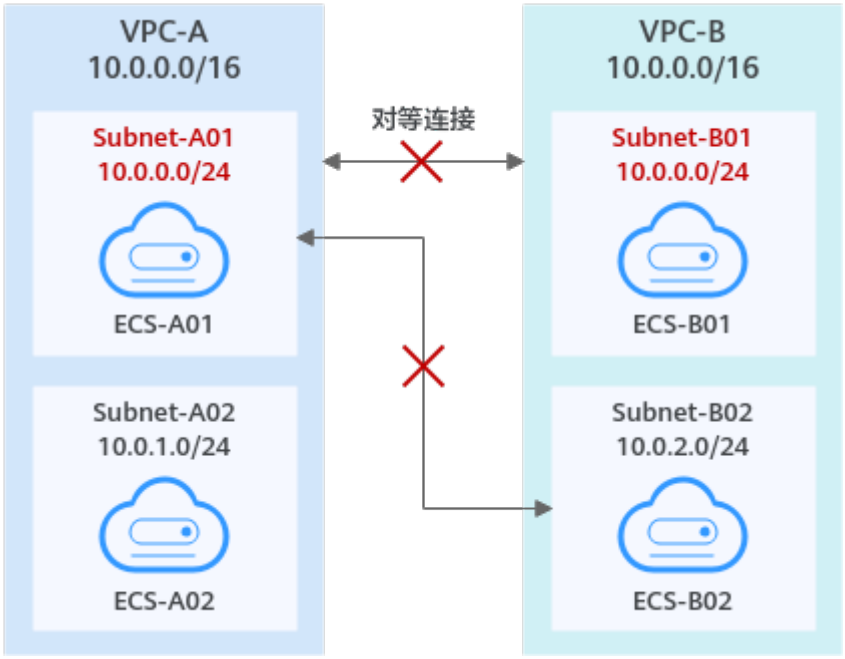


图 4-4 VPC 网段重叠，且部分子网重叠(IPv4)



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4-5所示，路由添加方法请参见表4-3。

图 4-5 VPC 网段重叠，部分子网重叠(IPv4)-正确配置

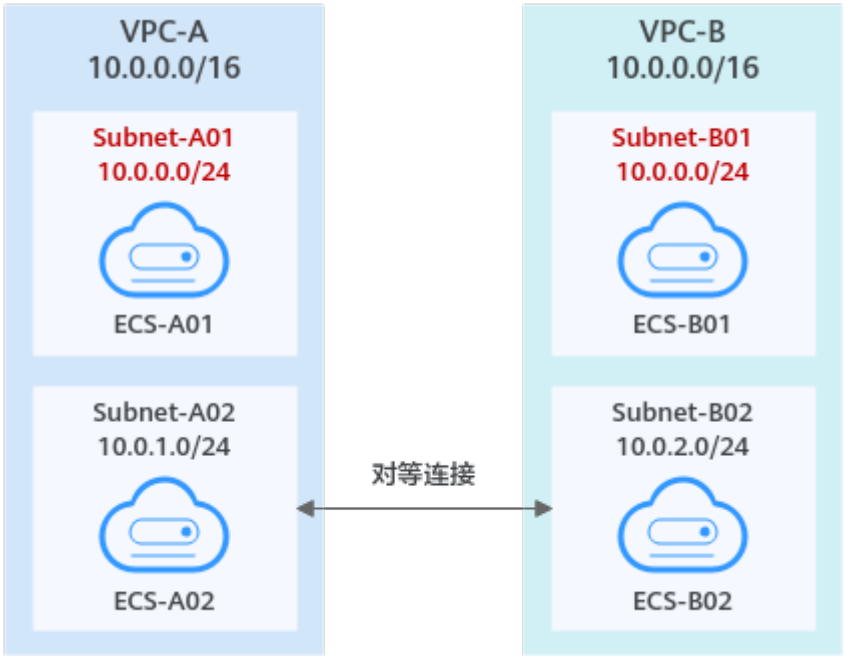


表 4-3 Subnet-A02 和 Subnet-B02 之间的对等连接

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。

须知

- 由于网段重叠导致对等连接不生效的详细原理说明，请参见**无效的VPC对等连接配置**。
- 该限制同样适用于IPv6场景，即使您只需要使用对等连接实现不同VPC之间的IPv6通信，此时如果对等连接两端VPC的IPv4网段和子网重叠，那么您创建的对等连接也不会生效。

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4-4**。

表 4-4 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** • **创建不同账户下的对等连接**
检查对等连接路由地址配置是否正确。 • 在本端VPC内，检查路由的目的地址是否为对端VPC的网段，子网网段或者相关的私有IP地址。 • 在对端VPC内，检查路由的目的地址是否为本端VPC的网段，子网网段或者相关的私有IP地址。	如果路由目的地址配置错误，请参考**修改对等连接路由**修改路由地址。
对于云上和云下互通的组网，检查对等连接路由是否和云专线、VPN路由的目的地址重叠。	查看对等连接两端的VPC下是否有VPN/云专线资源，排查路由规则的下一跳目的地址是否有重叠。 如果路由目的地址重叠，该对等连接不生效，请重新规划网络连接方案。

网络配置错误

1. 检查需要通信的云服务器的安全组规则是否配置正确，具体方法请参见**查看安全组**。
   - 同一个账户下的对等连接：请参见**创建相同账户下的对等连接**中的“步骤三：配置对等连接两端VPC内实例的安全组规则”中的安全组规则说明进行检查。
   - 不同账户下的对等连接：请参见**创建不同账户下的对等连接**中的“步骤四：配置对等连接两端VPC内实例的安全组规则”中的安全组规则说明进行检查。
2. 检查云服务器网卡的防火墙配置。

   需要确认防火墙不会拦截流量，否则需要放通防火墙规则。
3. 检查对等连接连通的子网网络ACL规则是否配置正确。

   确认对等连接涉及的子网流量未被网络ACL拦截，否则需要放通对等连接涉及的网络ACL规则。
4. 对于多网卡的云服务器，检查云服务器内部的策略路由配置，确保源IP不同的报文匹配各自的路由，从各自所在的网卡发出。

   假设云服务器有两个网卡为eth0和eth1：
   - eth0的IP地址为192.168.1.10，所在子网的网关为192.168.1.1
   - eth1的IP地址为192.168.2.10，所在子网的网关为192.168.2.1

   分别执行以下命令：

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

命令示例：

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

如果网络通信情况正常，说明服务的多个网卡路由配置正常。

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

ECS 基本网络功能异常

1. 登录云服务器。

   弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

2. 检查ECS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**弹性云服务器IP获取不到时，如何排查?** 。

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ECS列表中，单击云服务器名称超链接。

      进入云服务器详情页。

   b. 在云服务器详情页，单击虚拟有云超链接。

      进入虚拟私有云列表。

   c. 在虚拟私有云列表，单击虚拟私有云对应的“子网个数”超链接。

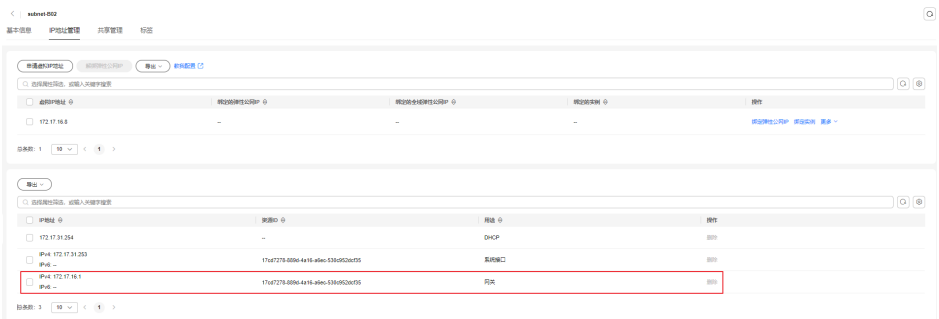
      进入子网列表。

   d. 在子网列表，单击子网名称超链接。

      进入子网详情页。

   e. 选择“IP地址管理”页签，查看子网的网关地址。

      图 4-6 查看子网网关

   f. 执行以下命令，检查网关通信是否正常。

      ping *子网网关地址*

      命令示例：**ping 172.17.0.1**

如果无法ping通子网网关，则需首先排查二三层网络问题，具体请参见**二三层通信出现问题时，如何排查?**。

5 虚拟 IP 类

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

问题描述

ECS的网卡绑定虚拟IP地址后，该虚拟IP地址无法ping通。

排查思路

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

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 5-1 排查思路

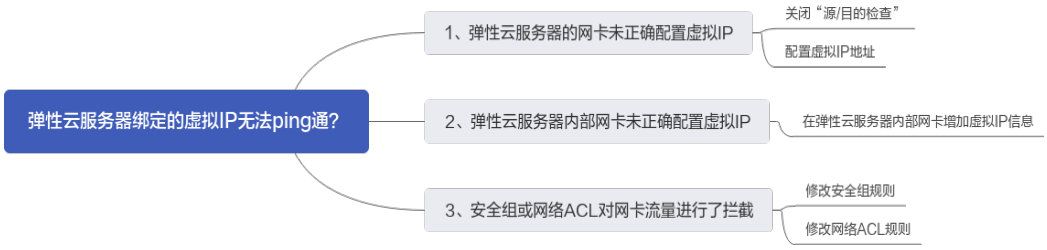


表 5-1 排查思路

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

可能原因	处理措施
安全组或网络ACL对网卡流量进行了拦截	解决方法请参考**安全组或网络ACL对网卡流量进行了拦截**。

弹性云服务器的网卡未正确配置虚拟 IP

查看该网卡的“源/目的检查”是否关闭，虚拟IP是否已经绑定网卡。

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

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

说明

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

弹性云服务器内部网卡未正确配置虚拟 IP

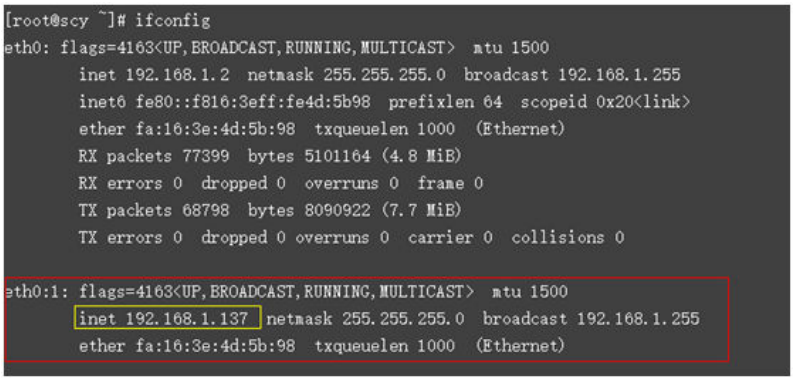
本文以Linux系统和Windows系统为例，指导您如何查看弹性云服务器内部网卡是否正确配置了虚拟IP地址。

Linux系统

1. 在弹性云服务器上执行以下命令，确认是否存在ethX:X类型的网卡。

   ifconfig

   图 5-2 查看是否存在 ethX:X 类型的网卡



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

- 是，弹性云服务器内部网卡子接口正常创建。
- 否，请执行如下步骤。

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

   cd /etc/sysconfig/network-scripts

3. 执行以下命令新建并修改“ifcfg-eth0:1”文件。

   vi ifcfg-eth0:1

   在文件中增加以下网卡信息。

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

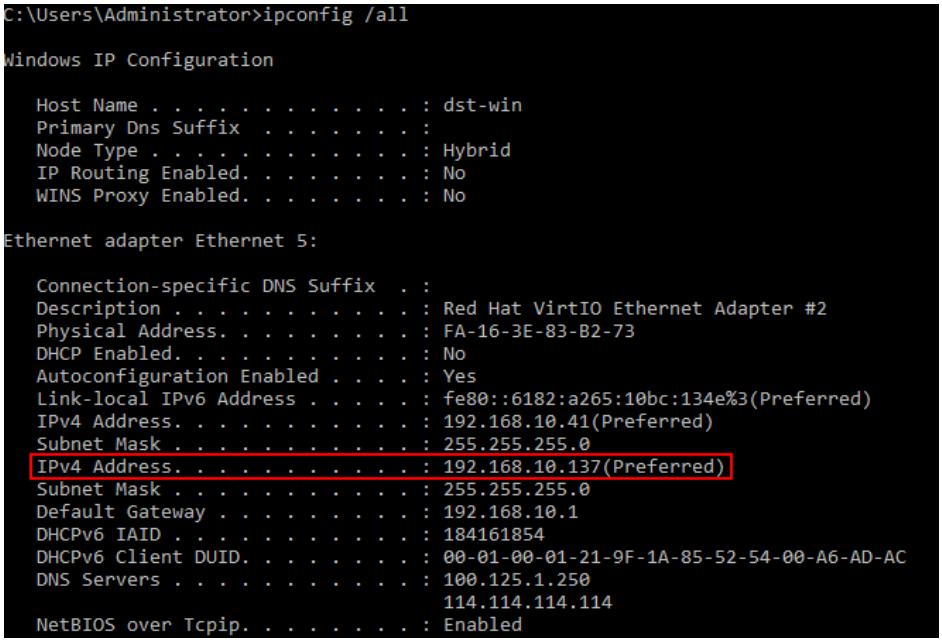
4. 按“**Esc**”输入“**:wq!**”，保存后退出文件。
5. 重启弹性云服务器，使用**ifconfig**命令再次查看是否已经完成虚拟IP地址的配置。

Windows系统

1. 在“开始”菜单中打开Windows命令行窗口，执行以下命令确认是否配置了虚拟IP地址。

   ipconfig /all

   图 5-3 查看是否配置虚拟 IP 地址

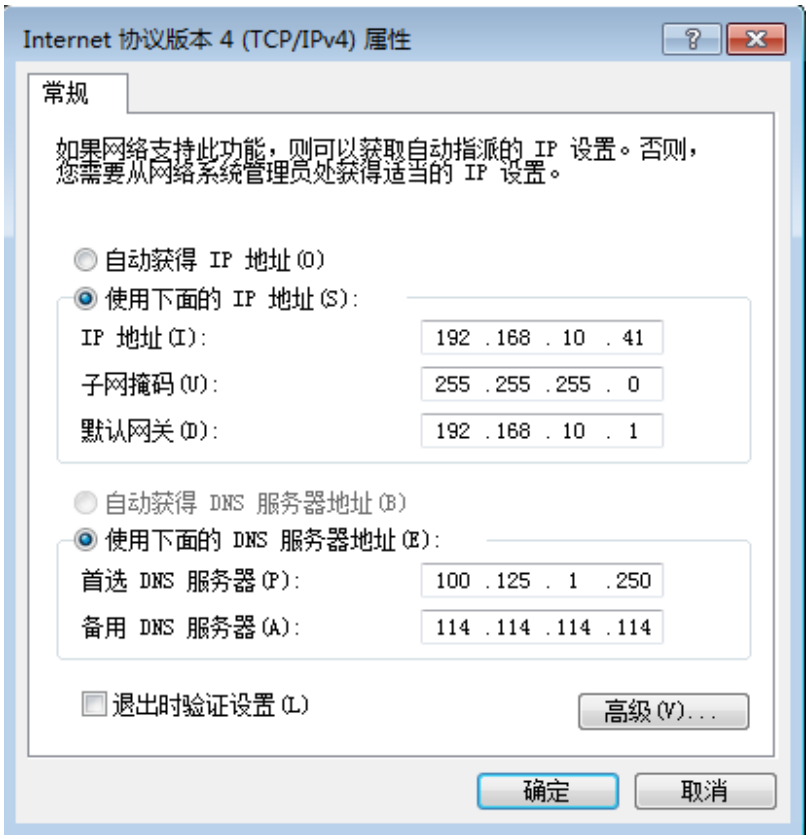
   

   上图回显样例中IPv4 Address包含ECS网卡需要配置的虚拟IP地址192.168.10.137。

   - 是，弹性云服务器内部网卡的虚拟IP地址配置正常。
   - 否，请执行如下步骤。

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

图 5-4 配置私有 IP 地址



6. 单击“高级”。
7. 在“IP设置”页签内“IP地址”区域，单击“添加”。
   添加图5-3中的虚拟IP地址，例如：192.168.10.137。

图 5-5 配置虚拟 IP 地址

安全组或网络 ACL 对网卡流量进行了拦截

查看弹性云服务器的安全组以及网卡所在子网的ACL规则是否会对流量进行拦截。

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

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

5.2 华为云上的虚拟 IP 如何绑定 IDC 内的主机?

前提条件:

- 已创建虚拟IP，详细操作，请参考**申请虚拟IP地址**。
- 已创建虚拟IP所在子网的二层连接，详细操作，请参考**购买企业交换机**。

操作步骤

1. 登录管理控制台。
2. 在系统首页，选择“网络>虚拟私有云”。
3. 在左侧导航栏选择“企业交换机”。
4. 在下方“二层连接拓扑”右侧单击“管理虚拟IP”。
5. 在IP地址管理列表中的选择对应虚拟IP地址，单击“绑定实例”。
6. 在绑定实例页面中，实例类型选择“二层连接”，并选择对应二层连接，单击“确认”。

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

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

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

     ping *虚拟IP地址*

     命令示例：**ping 192.168.3.22**
   - 方法二：执行以下命令，在Client端，清理虚拟IP地址的ARP表中的残留表项，触发Client端学习新的ARP表。

     arp -d *虚拟IP地址*

     命令示例：**arp -d 192.168.3.22**

6 带宽类

6.1 什么是入云带宽和出云带宽?

带宽是指在单位时间（一般指的是1秒钟）内能传输的数据量，带宽数值越大表示传输能力越强，即在单位时间内传输的数据量越多。带宽分为公网带宽和内网带宽。

公网带宽是指华为云到Internet之间的网络带宽流量。公网带宽分为出云带宽和入云带宽。本文主要介绍出云带宽和入云带宽，具体内容参见表6-1。

- **出云带宽**在云监控指标中对应的是**上行带宽**/**上行流量**指标。
- **入云带宽**在云监控指标中对应的是**下行带宽**/**下行流量**指标。

图 6-1 入云带宽和出云带宽

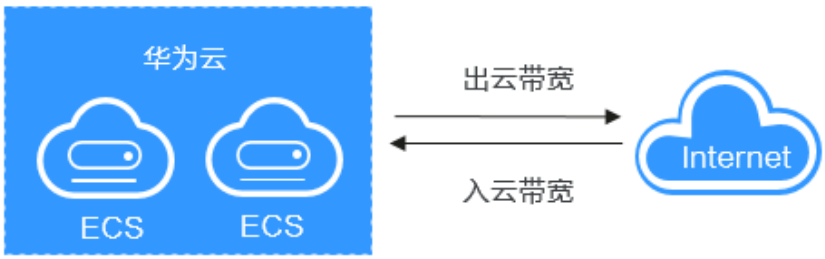


表 6-1 出云带宽和入云带宽

带宽类别	描述
出云带宽	从华为云流出到Internet方向的带宽。例如，云服务器对外提供访问，或者在外网的FTP客户端下载云服务器内部的资源等方式都是使用出云带宽。在云监控指标中对应的是上行带宽/上行流量指标。 **目前，华为云仅对出云带宽（即上行带宽/上行流量）收取费用。** **说明** • 如果您需要**查看带宽使用情况**，请参见**查看监控指标**。 • 如果您需要**查看带宽的计费详情**，请参见**费用账单**。
入云带宽	从Internet流入华为云方向的带宽。例如，在云服务器内部下载外部网络资源，或者在外网的FTP客户端上传云服务器内部的资源等方式都是使用入云带宽。在云监控指标中对应的是下行带宽/下行流量指标。 入云带宽的最大值受用户购买的出云带宽值影响，带宽限速规则如下： • 若您的带宽大小小于或等于10Mbit/s，则入云方向带宽为10Mbit/s，出云方向带宽大小为您的实际带宽大小。 • 若您的带宽大小大于10Mbit/s，则出云方向和入云方向带宽相同，都等于您的实际带宽大小。 上述带宽限速规则不适用华北-北京一、华东-上海二区域。

6.2 静态 BGP、全动态 BGP、优选 BGP 之间有何区别?

BGP（Border Gateway Protocol，边界网关协议）是运行于TCP上的一种自治系统（AS）的路由协议，是唯一能够妥善处理不相关路由域间的多路连接的协议。可同时满足电信、联通和其它运营商（如移动、教育网、铁通、长城宽带等）线路访问业务。

在创建EIP时，需要选择线路类型，其中常用的EIP线路类型如下：

- 静态BGP线路类型是由网络运营商手动配置的路由信息。
- 全动态BGP线路类型是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。
- 优选BGP线路类型是特定方向的优质线路。使用BGP协议与多家主流运营商线路互联对接，建立直连中国内地的公网互联路径，提供中国-香港区域与中国内地间的低时延、高质量的网络互通。（该线路资源仅在“中国-香港”区域支持。）

EIP不支持线路类型转换，例如全动态BGP不能转为静态BGP，全动态BGP和静态BGP是在不同的IP地址池中，无法互相转换。

静态BGP、全动态BGP、优选BGP具体内容和区别参见**表6-2**。

表 6-2 静态 BGP、全动态 BGP、优选 BGP 的区别

对比维度	静态BGP	全动态BGP	优选BGP
定义	由网络运营商手动配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，运营商需要手动去修改路由表中相关的静态路由信息。	使用BGP协议同时接入多个运营商，可以根据设定的寻路协议实时自动优化网络结构，保持客户使用的网络持续稳定，高效。	优选BGP是特定方向的优质线路。使用BGP协议与多家主流运营商线路互联对接，建立直连中国内地的公网互联路径，提供中国-香港区域与中国内地间的低时延、高质量的网络互通。
保障性	当静态BGP中网络结构发生变化，运营商是无法在第一时间自动调整网络设置，而是通过其他技术进行切换，所以静态BGP时延一般略大。 如用户选择静态BGP，需要自身应用系统具备容灾功能。	多线接入的BGP，能够感知接入线路及运营商内部网络状况，运营商内部故障时，能够快速切换到其他运营商接入链路，保证用户能够正常访问，而不是访问中断。 相比于优选BGP，全动态BGP不保证从中国-香港等区域到中国内地方向的稳定访问，可能出现包括但不限于丢包、闪断等情况。 全动态BGP目前支持的运营商线路包括：电信、移动、联通、教育网、广电、鹏博士等 。	线路保障能力与全动态BGP一致，多线接入的BGP，在遇到运营商内部故障时，能够快速切换到其他运营商接入链路，保证用户能够正常访问。 除此之外，质量更高，时延更低。 目前支持中国-香港当地主流运营商线路。
优势	通过单个网络运营商访问公网，成本低且便于自主调度。	BGP公网出口支持秒级跨域切换，保证您的用户无论使用哪种网络，均能享受高速、安全的网络质量。	• 避免绕行国际运营商出口网络。 • 延时更低，可有效提升境外业务对中国大陆用户覆盖质量。
服务可用性	99%	99.95%	99.95%
计费	优选BGP > 全动态BGP > 静态BGP。更多计费详情请参见**产品价格详情**中“弹性公网IP”的内容。		

说明

关于服务可用性的更多信息请参见**云服务等级协议**。

6.3 如何排查带宽超过限制?

问题现象

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

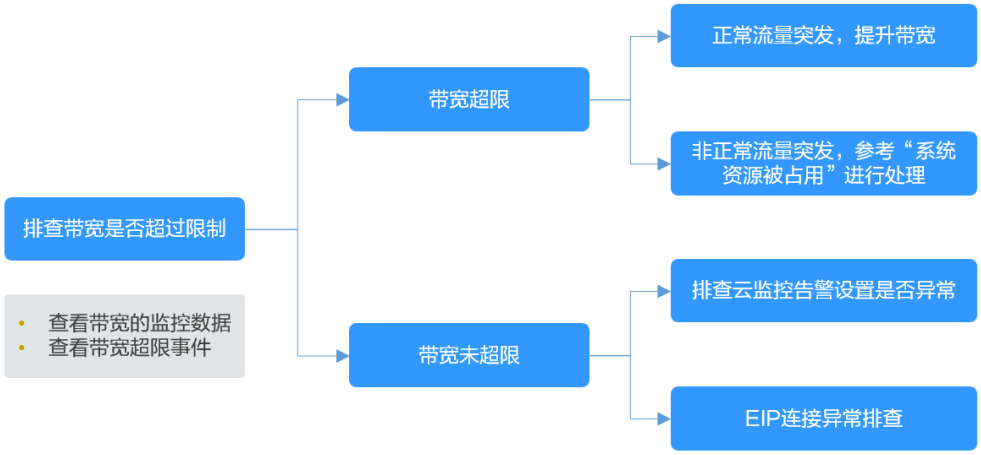
说明

带宽超限后，会影响服务器的远程登录或者引起随机丢包，为保证业务正常运行，推荐您对带宽进行监控。

排查步骤

根据以下排查思路，如果解决完某个可能原因后，问题仍未解决，请继续排查其他可能原因。如果以下方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

图 6-2 排查思路



步骤1 确定带宽是否超过限制

1. 查看带宽的监控数据。

   查看出入云带宽和带宽使用率等数据是否有超带宽，查看方法请参考**导出监控指标**。

2. 查看带宽超限事件。

   查看方法请参考**查询EIP独享带宽历史超限情况**。

   如果未设置EIP带宽超限事件，请**设置EIP带宽超限事件**。当系统出现异常丢包或卡顿情况，您就可以通过“事件监控”查看EIP独享带宽历史超限详情。

偶尔短暂的超带宽不影响业务的情况下，可以忽略。如果持续超带宽或者多次瞬时超带宽，可参考**步骤2**排查处理。

步骤2 带宽超限处理方法

流量突发可能会导致带宽瞬时超出上限，造成云服务器丢包。

建议您确认流量突发是否正常：

1. 正常流量突发，建议参考**修改带宽**提升带宽。

2. 非正常流量突发（比如攻击类流量导致的超带宽等），可参考**系统资源被占用**进行处理。

步骤3 带宽未超限处理方法

根据**步骤1**中数据排查结果，带宽未超过限制，或未超过购买时的带宽大小，您可以考虑如下处理方法。

- 排查云监控告警设置是否异常

  云监控设置EIP带宽超限告警时，告警策略设置不合理，系统将发送异常的带宽超限告警信息。解决方法请参考**云监控告警设置异常**。

- EIP连接异常

  EIP已绑定EIP，但是无法连接到Internet。解决方法请参考**EIP连接出现问题时，如何排查？**。

----结束

系统资源被占用

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

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

- Windows系统：**Windows云服务器带宽和CPU利用率高问题排查方法**
- Linux系统：**Linux云服务器带宽和CPU占用率高问题排查方法**

云监控告警设置异常

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

- **解决方案一：设置合理的带宽告警策略**

  当在云监控服务中创建“带宽”维度的告警规则时，若出网带宽最大值或告警周期设置过小，都将频繁收到带宽超限的告警信息。您需要根据购买的带宽大小设置合理的告警策略。例如购买的带宽大小为5Mbit/s，您可以设置连续三个周期内最大出网带宽大于等于4.8Mbit/s时，系统发送告警通知。创建告警规则步骤如下：

  a. 登录管理控制台，在云监控服务中，左侧导航栏选择“告警 > 告警规则 ”。

  b. 单击“创建告警规则”，配置带宽超限的告警规则。

- **解决方案二：设置EIP带宽超限事件**

  说明

  目前该功能的监控对象只针对EIP，共享带宽的超限情况暂不支持在“事件监控”中展示。

  设置EIP带宽超限事件的步骤参考如下：

  a. 登录管理控制台，在云监控服务中，左侧导航栏选择“事件监控”。

  b. 单击“创建告警规则”，配置EIP带宽超限事件的告警规则。

  设置EIP带宽超限事件后，当系统出现异常丢包或卡顿情况，您就可以通过“事件监控”查看EIP独享带宽历史超限详情。

当您需要查询EIP独享带宽历史超限情况时，可以参考以下步骤操作：

a. 在云监控服务中，单击“事件监控”。
b. 进入事件监控列表页，在对应的事件监控中单击操作列的“查看监控图表”。
c. 进入系统事件列表页，在对应的监控对象中单击操作列的“查看事件”，查看超限详情。

   如果没有“EIP带宽超限事件”显示，说明当前EIP的独享带宽未超限，请排查其他原因。

   如果有“EIP带宽超限事件”显示，说明当前EIP的独享带宽已经超限，如需保证业务正常，请扩大带宽。扩大带宽的操作请参见“**修改弹性公网IP的带宽**”。

   告警基础功能免费，触发产生的告警消息由SMN发送，可能产生少量费用，具体费用由SMN结算。详情请参见**《云监控服务用户指南》**。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

6.4 EIP 带宽与内网带宽有何差异?

公网带宽

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

公网带宽分为入云带宽和出云带宽。

入云带宽：从Internet流入华为云方向的带宽，例如，从公网下载资源到云内ECS。

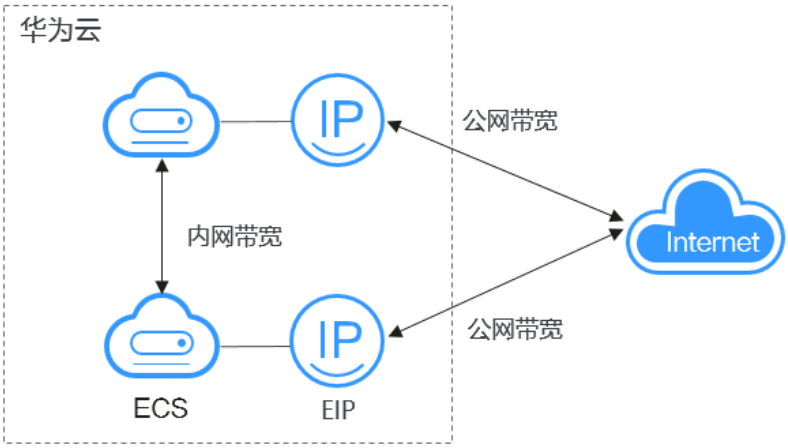
出云带宽：从华为云流出到Internet方向的带宽，例如，云内的ECS对外提供服务，外部用户下载云内ECS上的资源。

内网带宽

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

详细请参见**弹性云服务器实例类型**。

图 6-3 公网带宽和内网带宽



6.5 带宽的类型有哪些?

EIP的带宽有独享和共享两种类型。

当您购买EIP时，无论是哪种计费模式，只要没有加入共享带宽，那么您的EIP使用的是独享带宽。

- 独享带宽只能针对一个EIP进行限速。
- 共享带宽可以针对多个EIP进行集中限速。

6.6 独享带宽与共享带宽有何区别？能否互转?

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

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

独享带宽与共享带宽不支持直接互相转换，但针对按需计费的弹性公网IP，您可以购买一个共享带宽，进行如下操作：

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

6.7 一个共享带宽最多能对多少个 EIP 进行集中限速?

共享带宽可以实现多个EIP共同使用一条带宽，针对多个EIP进行集中限速。

默认情况下，一个共享带宽最多可对20个EIP进行集中限速。

如果当前规格无法满足实际需求，请您提交工单申请扩容。

6.8 包年/包月模式的带宽支持升配后再降配吗?

带宽支持升配后再降配。

如果需要调整带宽大小，您可以参考**修改弹性公网IP的带宽**。

- 增加带宽大小（补差价升配）：带宽升配后，新带宽大小将在原来已有的计费周期内立即生效。

  您需要按照与原带宽的价格差，结合使用周期内的剩余时间，补齐差价。
- 降低带宽大小（续费降配）：带宽降配后，新带宽大小不会立即生效。

  您需要选择续费时长并根据新的带宽大小进行续费，续费成功后，新带宽大小在新的计费周期内生效。
- 降低带宽大小（即时降配）：降配后，新的带宽大小将立即生效。

  您的带宽降配成功后，新的带宽大小将在当前计费周期内立即生效，会退还您新老配置的差价。

6.9 带宽与上传下载速率是什么关系?

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

1Byte（字节）=8bit（位），即下载速率=带宽/8

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

7 网络连接类

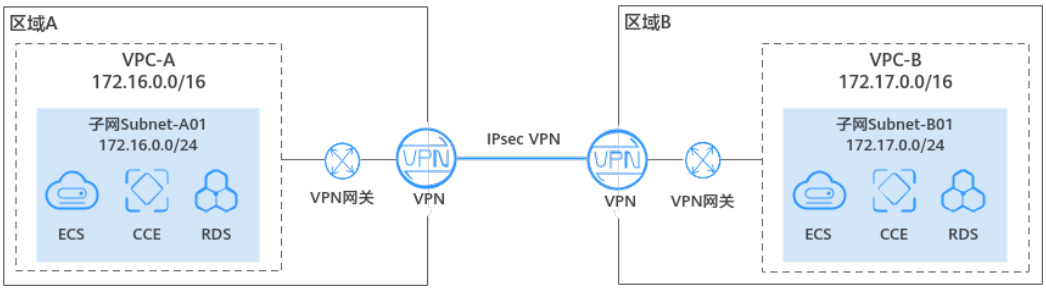
7.1 VPN 支持将两个 VPC 互连吗?

如果两个VPC位于同一区域内，可以使用VPC对等连接互连。

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

如图7-1所示，在区域A内通过一个VPN连接VPC-A，在区域B内通过另一个VPN连接VPC-B，两端VPC可以通过VPN的加密通道实现网络互通，相比云专线，VPN开通更快速且成本较低。

图 7-1 通过 VPN 连通不同区域 VPC



7.2 ECS 有多个网卡时，为何无法通过域名访问公网网站及云中的内部域名?

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

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

1. 登录管理控制台。
2. 在系统首页，选择“网络>虚拟私有云”。

3. 在左侧导航栏选择“虚拟私有云”。
4. 在虚拟私有云列表中，单击需要修改子网的虚拟私有云名称。
5. 在“子网”列表待修改子网所在行，单击“修改”，根据界面提示修改子网DNS服务器地址。
6. 单击“确定”，完成修改。

7.3 同时拥有自定义路由和 EIP 的 ECS 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。

7.4 本地主机访问使用弹性云服务器搭建的网站出现间歇性中断怎么办?

问题现象

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

解决思路

1. 确认客户使用的本地网络。

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

   sysctl -a|grep tcp_tw_recycle

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

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

   如果ListenDrops数值非0，表示存在丢包，即存在网络问题。

解决步骤

修改云服务器的内核参数可以解决此问题。

- 临时修改参数方法（重启服务器后该设置失效），设置如下：

  sysctl -w net.ipv4.tcp_tw_recycle=0
- 永久修改参数方法：

  a. 执行以下命令，修改“/etc/sysctl.conf”文件。

  vi /etc/sysctl.conf

在该文件中添加以下内容：

net.ipv4.tcp_tw_recycle=0

b. 按“**Esc**”输入“**:wq!**”，保存后退出文件。

c. 执行以下命令，生效配置。

sysctl -p

7.5 同一个子网下的弹性云服务器只能通过内网 IP 地址单向通信怎么办?

问题现象

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

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

解决思路

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

图 7-2 查看 ecs01 网卡配置

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

解决步骤

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

ip a del 192.168.1.40/32 dev eth0

7.6 同一个 VPC 内的两台弹性云服务器无法互通或者出现丢包等现象时，如何排查?

问题描述

同一个VPC内的两台弹性云服务器无法互通或者出现丢包等现象。

排查思路

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

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 7-3 排查思路

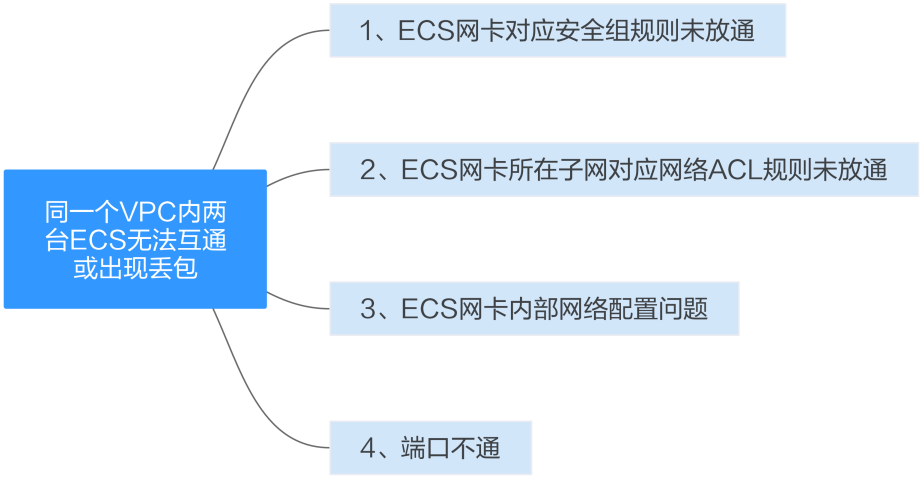


表 7-1 排查思路

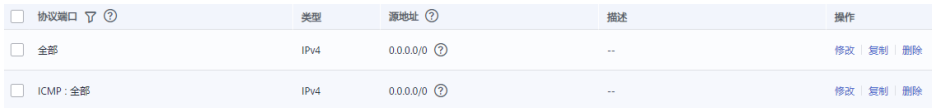
可能原因	处理措施
ECS网卡对应安全组规则未放通	解决方法请参考**ECS网卡对应安全组规则未放通**。
ECS网卡所在子网关联的网络ACL规则未放通	解决方法请参考**ECS网卡所在子网关联的网络ACL规则未放通**。
ECS网卡内部网络配置问题	解决方法请参考**ECS网卡内部网络配置问题**。
端口不通	解决方法请参考**端口不通**。

ECS 网卡对应安全组规则未放通

排查弹性云服务器网卡对应的安全组是否放通了出方向和入方向的ICMP规则。

以入方向为例，即安全组规则需要包含下图中的任意一条规则。

图 7-4 入方向安全组规则



若客户测试的是其他协议的报文，需放通相应协议的安全组规则。例如，测试的是UDP报文，则需检查安全组是否有规则放通出入方向的UDP协议。

ECS 网卡所在子网关联的网络 ACL 规则未放通

1. 查看弹性云服务器的网卡是否处于网络ACL的关联子网中。
2. 在网络ACL列表中查看网络ACL的状态。
   - 状态显示“已开启”，则表示网络ACL已经开启。执行**3**。
   - 状态显示“未开启”，则表示网络ACL已经关闭。执行**4**。
3. 单击网络ACL名称，分别在“入方向”和“出方向”的页签下添加ICMP放通规则。
4. 网络ACL关闭时，默认规则为丢弃所有出入方向的包。此时，请删除网络ACL或者开启ACL并放通ICMP规则。

ECS 网卡内部网络配置问题

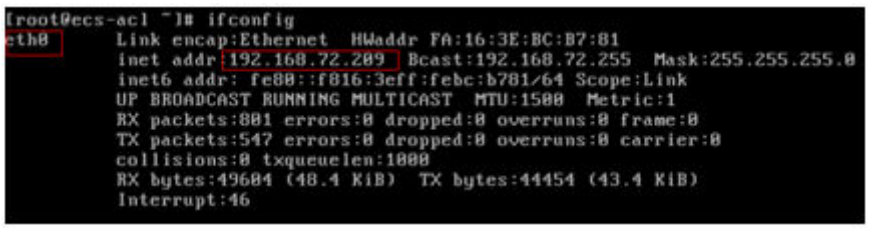
以下步骤以Linux系统为例，Windows操作系统请检查系统防火墙限制。

1. 确认弹性云服务器是否有多网卡配置。如果配置多网卡且弹性公网IP绑定在非主网卡上，请在弹性云服务内部配置策略路由。

   具体请参见**如何配置多网卡弹性云服务器的策略路由？** 。
2. 登录弹性云服务器，执行以下命令，查看网卡是否创建且网卡获取私有IP地址。若无网卡信息或者无法获取私有IP地址，请联系技术支持。

   ifconfig

   图 7-5 查看网卡 IP 地址

3. 执行以下命令，查看弹性云服务器的CPU占用率是否过高，CPU占有率超过80%有可能会影响ECS通信。

   top
4. 执行以下命令，查看弹性云服务器内容部是否有安全规则的其他限制。

   iptables-save

5. 执行以下命令，查看“/etc/hosts.deny”文件中是否包含了限制通信的IP地址。
   vi /etc/hosts.deny
   如果hosts.deny文件里面包含了对端的IP地址，请将该IP从hosts.deny文件中删除并保存文件。

端口不通

1. 如果无法访问弹性云服务器的特殊端口，请排查安全组规则以及网络ACL规则中是否对端口进行放行。
2. 在Linux弹性云服务器内部通过以下命令查看弹性云服务器内部是否监听该端口。如果未对该端口进行监听，可能会影响弹性云服务器的通信。
   netstat -na | grep <*端口号*>

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

7.7 Cloud-init 连接出现问题时，如何排查?

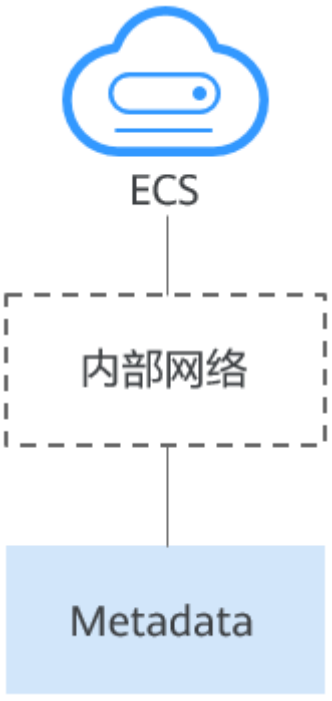
问题描述

无法正常使用Cloud-init。

排查思路

弹性云服务器获取Metadata的流程如**图7-6**所示：

图 7-6 获取 Metadata 流程图



您可以按照以下原因进行排查，如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 7-7 排查思路

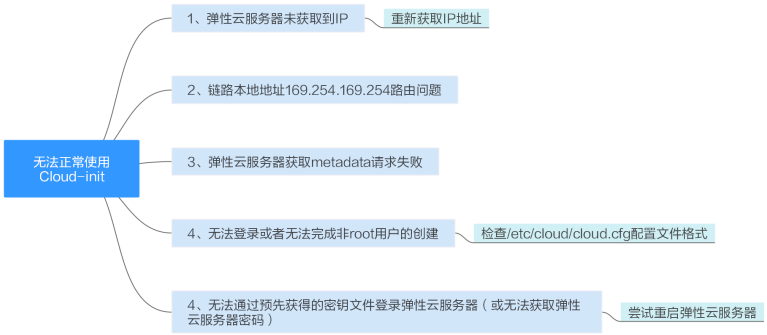


表 7-2 排查思路

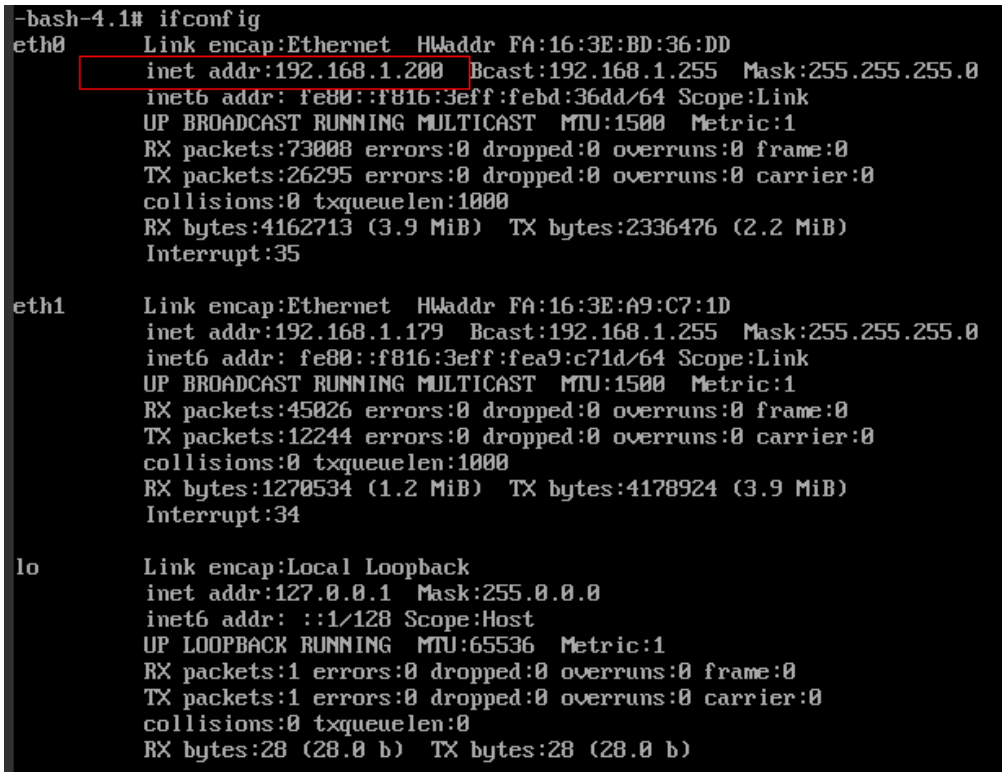
可能原因	处理措施
弹性云服务器未获取到IP	解决方法请参考**弹性云服务器未获取到IP**。
链路本地地址169.254.169.254路由问题	解决方法请参考**链路本地地址169.254.169.254路由问题**。
弹性云服务器获取metadata请求失败	解决方法请参考**弹性云服务器获取metadata请求失败**。
无法登录或者无法完成非root用户的创建	检查/etc/cloud/cloud.cfg配置文件格式，参考**无法登录或者无法完成非root用户的创建**。
无法通过预先获得的密钥文件登录弹性云服务器（或无法获取弹性云服务器密码）	重启弹性云服务器后重试解决。

弹性云服务器未获取到 IP

检查弹性云服务器是否已经获取到IP地址。

如果没有获取到IP地址，请尝试执行获取命令：**dhclient**（不同的操作系统，获取DHCP地址的命令有稍微的差别，请按照弹性云服务器的操作系统，选择相应命令）；也可以通过down/up网卡的方式尝试重新获取。

图 7-8 查看弹性云服务器 IP 地址



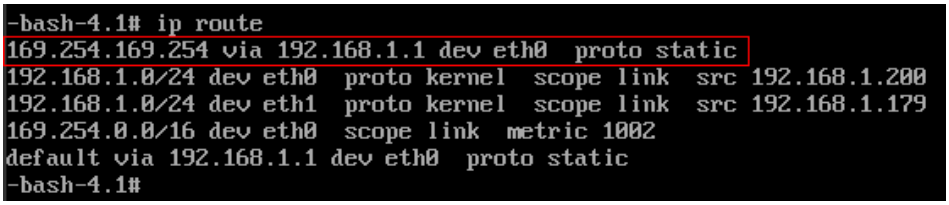
链路本地地址 169.254.169.254 路由问题

如果弹性云服务器ping不通169.254.169.254，请按以下步骤排查：

1. 查看弹性云服务器内169.254.169.254的默认路由：

   正常情况下，169.254.169.254的精确路由的下一跳地址，要和默认路由的下一跳地址保持一致。

   图 7-9 查看 169.254.169.254 的路由信息

2. 如果没有169.254.169.254/32位的精确路由：

   CentOS 5系列的镜像不支持opt_name为121的这种路由注入方式，所以无法注入，请尝试使用新的镜像。

3. 如果169.254.169.254/32的精确路由指向的下一跳和默认路由不一致：
   - 如果不是新建弹性云服务器，可能是开启CloudInit特性之前创建的，弹性云服务器内部service network restart重新进行dhcp请求，查看是否获取到正确的路由。
   - 如果是新建弹性云服务器，请**提交工单**，联系技术支持人员。

弹性云服务器获取 metadata 请求失败

弹性云服务器内部获取metadata请求的命令：

curl http://169.254.169.254/openstack/latest/meta_data.json

正确的返回结果如图7-10所示：（以下示例仅供参考，命令行有返回值即表示正确）

图 7-10 返回结果

无法登录或者无法完成非 root 用户的创建

Cloud-init已配置，并且服务进程正常，但是无法登录或者无法完成非root用户的创建。

需要检查/etc/cloud/cloud.cfg配置文件格式是否严格遵循缩进了，具体要参考各大Linux OS厂商本身的要求，如下以ubuntu操作系统为例。

图 7-11 检查配置文件

```
system_info:
   # This will affect which distro class gets used
   distro: rhel
   # Default user name + that default users groups (if added/used)
   default_user:
     name: linux  //登录使用的用户名。
     lock_passwd: False  //False，表示当前不禁用密码登录的方式，注意部分操作系统此处配置为0表示不禁用。
     gecos: Cloud User
     groups: users  //可选项，将用户添加到另外的组里，groups必须是系统里/etc/group已存在的组。
     passwd: $6$I6JDBVKK$Zh41chiJR7HuZvtJHsYBQJIg5RoQCRLS1X2Hsgj2s5JwXI7KUO1we8WYcwbzeaS2VHpRmNo28vmxxCyU6LwoD0
     sudo: ["ALL=(ALL) NOPASSWD:ALL"]  //表示设置用户具有root用户的所有权限。
     shell: /bin/bash  //shell执行采用bash方式。
   # Other config here will be given to the distro class and/or path classes
   paths:
      cloud_dir: /var/lib/cloud/
      templates_dir: /etc/cloud/templates/
   ssh_svcname: sshd
```

无法通过预先获得的密钥文件登录弹性云服务器（或无法获取弹性云服务器密码）

如果某次弹性云服务器启动后通过预先获得的密钥文件无法登录弹性云服务器（或无法获取弹性云服务器密码），可以尝试通过重启弹性云服务器后重试解决。

提交工单

如果按照以上步骤执行后，仍然无法正常使用Cloud-init，请提交工单寻求更多帮助。

您需要向技术支持人员提供如下表格中的信息：

Item	如何使用	注释	您的值
VPC CIDR 块	用于客户网关配置	示例：10.0.0.0/16	-
VPC ID信息	-	示例：120b71c7-94ac-45b8-8ed6-30aafc8fbdba	-
1 号子网 CIDR 块（可与 VPC 的 CIDR 块相同）	-	示例：10.0.1.0/24	-
弹性云服务器ID信息	-	-	-
弹性云服务器IP信息	-	示例：192.168.1.192/24	-
弹性云服务器路由信息	-	-	-

7.8 EIP 连接出现问题时，如何排查?

问题描述

用户的弹性云服务器已绑定EIP，但是无法连接到Internet。

排查思路

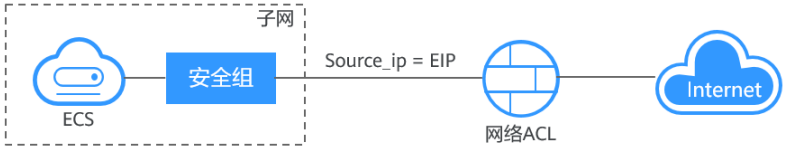
排查EIP问题

- 查看EIP是否被封堵，EIP封堵及解封的详细内容请参见**EIP出现封堵后，如何处理?**
- 查看EIP是否被冻结，EIP冻结及解除被冻结的详细内容请参见**EIP资源在什么情况下会被冻结，如何解除被冻结的EIP资源?**

排查EIP连接问题

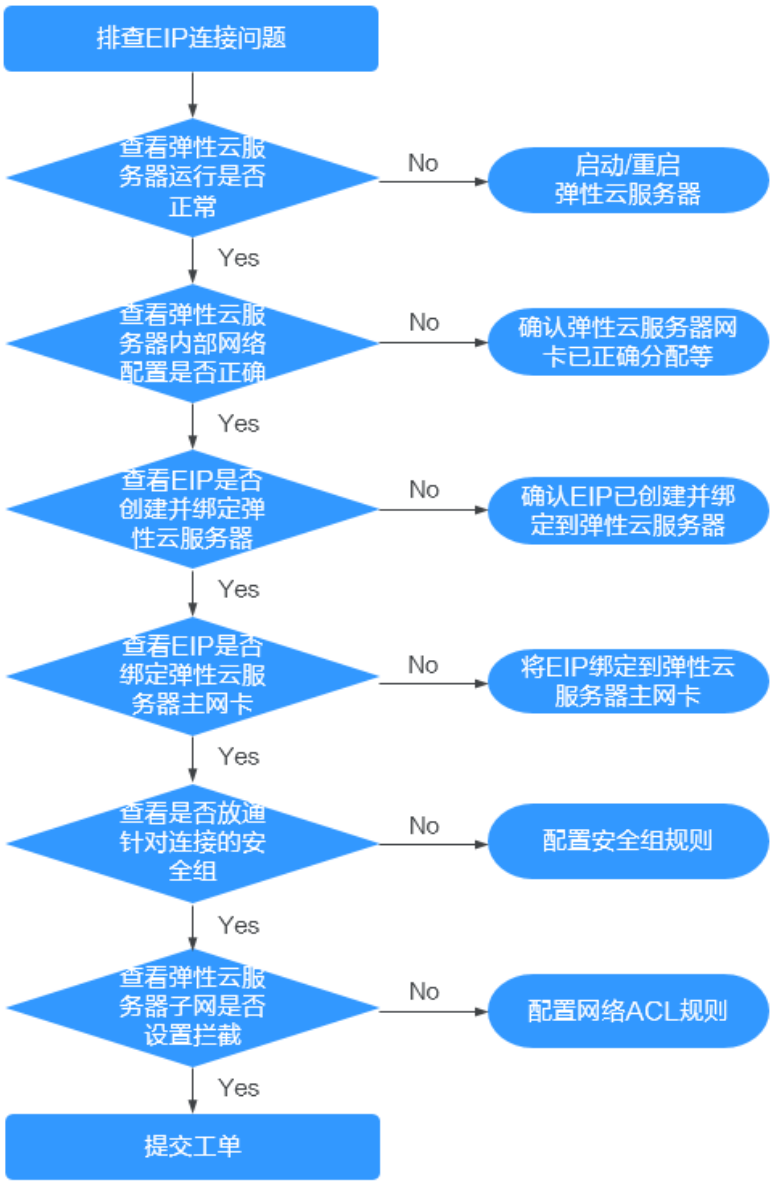
弹性云服务器通过EIP访问Internet的流程如**图7-12**所示：

图 7-12 EIP 网络示意图



本问题请按照以下思路进行排查处理。

图 7-13 排查思路



1. **查看弹性云服务器运行是否正常**
2. **查看弹性云服务器内部网络配置是否正确**
3. **查看EIP是否创建并绑定弹性云服务器**
4. **查看EIP是否绑定弹性云服务器主网卡**
5. **查看是否放通针对连接的安全组**
6. **查看弹性云服务器子网是否设置拦截**

步骤一：查看弹性云服务器运行是否正常

检查您的弹性云服务器是否正常运行。

弹性云服务器运行状态如果不是运行状态，请尝试启动/重启弹性云服务器。

图 7-14 检查弹性云服务器状态

步骤二：查看弹性云服务器内部网络配置是否正确

1. 确认弹性云服务器网卡已经正确分配到IP地址。

   登录弹性云服务器内部，使用命令**ifconfig**或**ip address**查看网卡的IP信息。

   如果弹性云服务器配置了扩展网卡，且主网卡和扩展网卡均绑定了EIP，则需检查是否配置了策略路由。如未配置策略路由，请参考**为多网卡Linux云服务器配置策略路由 (IPv4/IPv6)**。

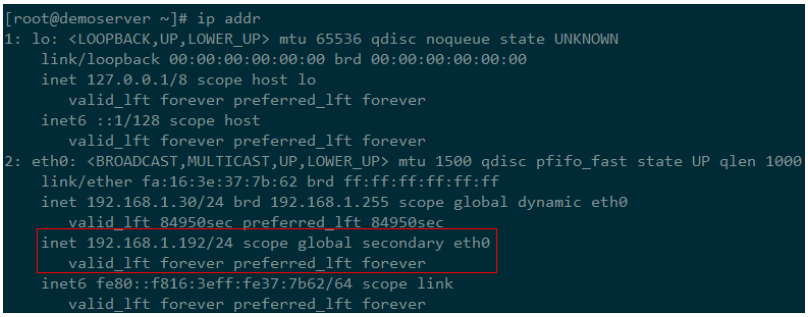
   注：Windows弹性云服务器可以在命令行中执行**ipconfig**查看。

2. 确认虚拟IP地址已经正确配置在网卡上。

   当您使用了虚拟IP，需要确认虚拟IP是否正确配置在网卡上。

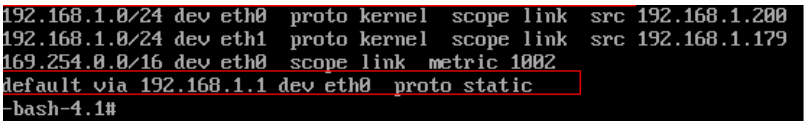
   登录弹性云服务器内部，使用命令**ifconfig**或**ip address**查看网卡的IP信息。如果没有虚拟IP地址，可以使用命令**ip addr add *虚拟IP地址* eth0**给弹性云服务器添加正确的配置。

图 7-15 查看网卡的虚拟 IP 地址



查看是否有默认路由信息，如果没有，则可以通过**ip route add**添加路由。

图 7-16 查看默认路由



步骤三：查看 EIP 是否创建并绑定弹性云服务器

检查您的EIP是否已经创建并绑定到该弹性云服务器，若未创建&绑定，请先完成创建&绑定。

如图7-17所示，仅有私有IP，未绑定EIP。

图 7-17 检查 EIP 是否绑定

步骤四：查看 EIP 是否绑定弹性云服务器主网卡

检查您的EIP是否绑定在弹性云服务器的主网卡。若未绑定主网卡，需绑定至弹性云服务器的主网卡上。

您可以在弹性云服务器详情页的网卡页签下进行查看，默认列表第一条为主网卡。

如下图所示，EIP绑定在主网卡上。

图 7-18 查看 EIP 是否绑定主网卡

步骤五：查看是否放通弹性云服务器所在的安全组

检查您的安全组规则是否已经配置。配置安全组规则请参见**添加安全组规则**。

请根据实际需求，选择性配置安全组规则（Remote IP指的是放行的IP地址，0.0.0.0/0表示放通所有的IP地址，请谨慎使用）。

步骤六：查看弹性云服务器子网是否设置拦截

检查您弹性云服务器使用的网卡所在子网的网络ACL是否会对流量进行拦截。

您可以在虚拟私有云页面左侧导航栏选择网络ACL进行配置，请确认弹性云服务器涉及的子网已放通。

提交工单

如果按照以上步骤执行后，仍然无法正常使用EIP，请**提交工单**进行解决。

您需要向技术支持人员提供如下表格中的信息：

Item	如何使用	注释	您的值
VPC CIDR 块	用于客户网关配置	示例：10.0.0.0/16	-
VPC ID信息	-	示例：120b71c7-94ac-45b8-8ed6-30aafc8fbdba	-

Item	如何使用	注释	您的值
1 号子网 CIDR 块（可与 VPC 的 CIDR 块相同）	-	示例：10.0.1.0/24	-
弹性云服务器ID信息	-	-	-
弹性云服务器IP信息	-	示例：192.168.1.192/24	-
弹性云服务器路由信息	-	-	-
EIP地址	用于客户弹性云服务器访问Internet	示例：10.154.55.175	-
EIP地址的带宽	用于客户弹性云服务器访问Internet的最大线速	示例：1M	-
EIP ID信息	-	示例：b556c80e-6345-4003-b512-4e6086abbd48	-

7.9 二三层通信出现问题时，如何排查?

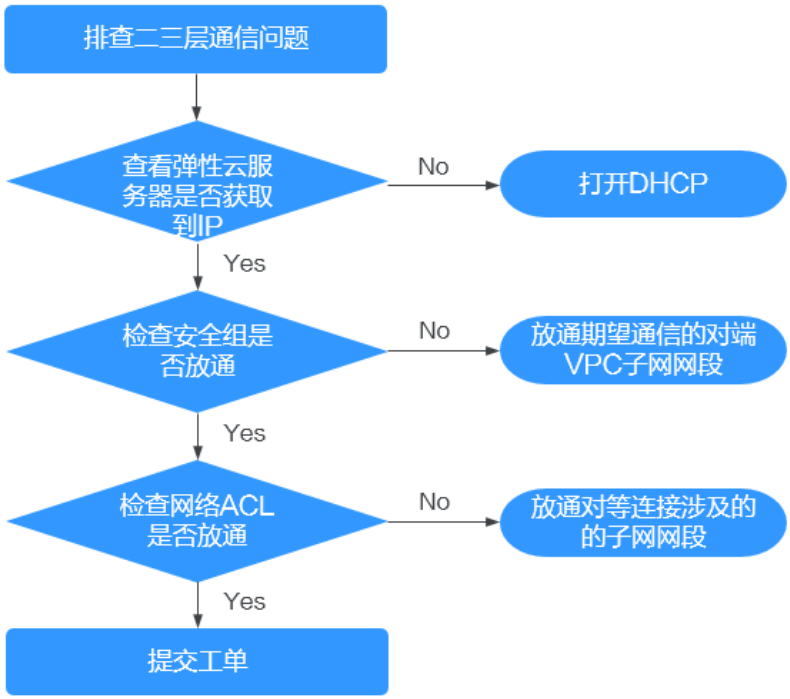
问题描述

用户云服务器基本网络功能异常，无法完成基本通信。从弹性云服务器内部ping所在子网的网关，无法ping通，则需首先排查二三层网络问题。

排查思路

本问题请按照以下思路进行排查处理。

图 7-19 排查思路



1. **检查弹性云服务器是否获取到IP**：检查弹性云服务器是否获取到IP。
2. **查看安全组是否放通**：检查弹性云服务器所使用网卡所在安全组配置，期望进行通信的对端VPC的子网网段是否已放通。
3. **查看网络ACL是否放通**：检查网络ACL配置，对等连接涉及的子网是否已放通。

步骤一：检查弹性云服务器是否获取到 IP

登录弹性云服务器内部，使用命令ifconfig或ip address查看网卡的IP信息。Windows弹性云服务器可以在命令行中执行ipconfig查看。

若弹性云服务器没有获取到IP，请检查您子网的enable_dhcp开关是否打开。

您可以进入子网详情页面，查看DHCP开关是否打开。

具体操作可参考**弹性云服务器IP获取不到时，如何排查？**。

步骤二：查看安全组是否放通

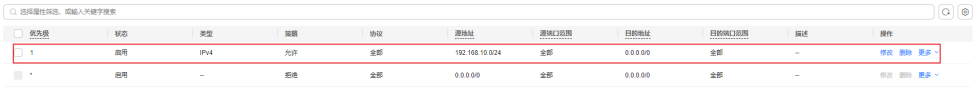
弹性云服务器详情页面中可以查看网卡使用的安全组。需要包含期望进行通信的对端VPC的子网网段。

图 7-20 查看安全组是否放通

步骤三：查看网络 ACL 是否放通

虚拟私有云页面左侧导航栏选择网络ACL，选择对等连接涉及的子网所关联的网络ACL，并在网络ACL详情页查看对等连接涉及的子网是否已放通。

图 7-21 查看网络 ACL 是否放通



提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

7.10 裸机网络出现问题时，如何排查?

1. 裸机内网口是否组bond。

   ifconfig

   图 7-22 检查裸机内网口是否组 bond

```
[root@bms2 rhel]# ifconfig
bond0     Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          inet addr:192.168.2.46  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fee9:b08a/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MASTER MULTICAST  MTU:8888  Metric:1
          RX packets:188108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42689694 (40.7 MiB)  TX bytes:82939564 (79.0 MiB)

bond0.2966 Link encap:Ethernet  HWaddr FA:16:3E:60:9C:CF
          inet addr:192.168.4.113  Bcast:192.168.4.255  Mask:255.255.255.0
          inet6 addr: fe80::f816:3eff:fe60:9ccf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:8888  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:660 (660.0 b)  TX bytes:720 (720.0 b)

eth0      Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:174667 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41874228 (39.9 MiB)  TX bytes:82939564 (79.0 MiB)

eth1      Link encap:Ethernet  HWaddr FA:16:3E:E9:B0:8A
          UP BROADCAST RUNNING SLAVE MULTICAST  MTU:8888  Metric:1
          RX packets:13441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:815466 (796.3 KiB)  TX bytes:0 (0.0 b)
```

   正常裸机在操作系统里会对网口进行组bond操作，如果裸机内执行ifconfig命令没有看到bond接口，说明组bond失败。请联系技术支持人员。

2. 裸机内路由信息是否正确。

   route –n

   图 7-23 检查裸机内路由信息是否正确

```
[root@bms2 rhel]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
169.254.169.254 192.168.2.1     255.255.255.255 UGH   0      0        0 bond0
192.168.4.0     0.0.0.0         255.255.255.0   U     0      0        0 bond0.2966
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 bond0
169.254.0.0     0.0.0.0         255.255.0.0     U     1006   0        0 bond0
169.254.0.0     0.0.0.0         255.255.0.0     U     1007   0        0 bond0.2966
0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 bond0
[root@bms2 rhel]#
```

需要重点排查是否有全0的默认路由：

图 7-24 排查默认路由

```
0.0.0.0         192.168.2.1     0.0.0.0         UG    0      0        0 bond0
[root@bms2 rhel]#
```

需要重点排查是否有到169.254.169.254的网段路由：

图 7-25 排查 169.254.169.254 的网段路由

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
169.254.169.254 192.168.2.1     255.255.255.255 UGH   0      0        0 bond0
```

如果路由存在异常，请联系技术支持人员。

3. 裸机二三层、EIP通信异常。

   各类网络流量与弹性云服务器没有差异，请参考弹性云服务器相关FAQ进行排查。

4. 客户需要协助的运维操作

   客户需要在console上查询VPC、裸机ID等信息，并向技术支持人员提供如下表格中的信息：

Item	如何使用	注释	您的值
VPC 1 ID	VPC1的ID	示例：fef65559-c154-4229-afc4-9ad0314437ea	-
BMS 1 ID	VPC1下的裸机1 ID	示例：f7619b12-3683-4203-9271-f34f283cd740	-
BMS 2 ID	VPC1下的裸机2 ID	示例：f75df766-68aa-4ef3-a493-06cdc26ac37a	-

7.11 弹性云服务器 IP 获取不到时，如何排查?

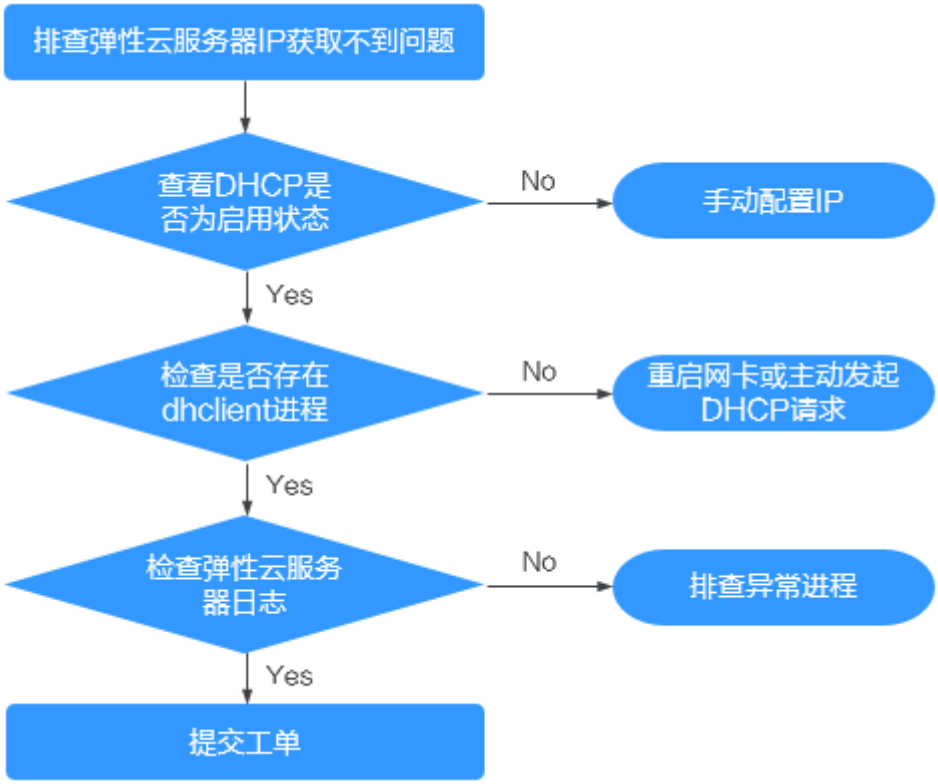
问题描述

用户无法查询到弹性云服务器私网IP地址信息。

排查思路

本问题请按照以下思路进行排查处理。

图 7-26 排查思路



1. **查看DHCP是否为启用状态**
2. **检查是否存在dhclient进程**
3. **检查弹性云服务器日志**

步骤一：查看 DHCP 是否为启用状态

检查子网的DHCP是否为启用状态（默认“启用”状态）。

进入子网详情页面，查看DHCP是否为“启用”状态，若DHCP开关为关闭状态请参考3手动配置静态IP。

步骤二：检查是否存在 dhclient 进程

1. 执行如下命令，检查是否存在dhclient进程。

   ps -ef | grep dhclient

2. 若dhclient进程不存在，登录弹性云服务器，尝试重启网卡或主动发起DHCP请求。
   - Linux系统：

     执行**dhclient ethx**命令。若不支持dhclient命令就执行**ifdown ethx;ifup ethx**（ethx代表弹性云服务器网卡，如eth0、eth1）。
   - Windows系统：

     先禁用网络连接，然后再重新启用。
3. 对于DHCP Client长期不发起请求的情况，例如：重启网卡后又复现，尝试使用以下方法配置静态IP。

- Linux系统：
  i. 执行以下命令，打开/etc/sysconfig/network-scripts/ifcfg-eth0中的配置。
     vi /etc/sysconfig/network-scripts/ifcfg-eth0
  ii. 修改/etc/sysconfig/network-scripts/ifcfg-eth0中的配置。
     BOOTPROTO=static
     IPADDR=192.168.1.100 #IP地址
     NETMASK=255.255.255.0 #掩码值
     GATEWAY=192.168.1.1 #网关地址
  iii. 执行以下命令，重启网络服务。
     service network restart
- Windows系统：
  在网络连接中选择“属性 > Internet协议版本4 > 属性”，手动输入IP地址、子网掩码和默认网关。

步骤三：检查弹性云服务器日志

查看弹性云服务器的messages日志（路径为/var/log/messages）排查问题。

通过网卡的MAC地址过滤日志，排查是否有进程影响DHCP获取IP。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

您需要协助的运维操作：

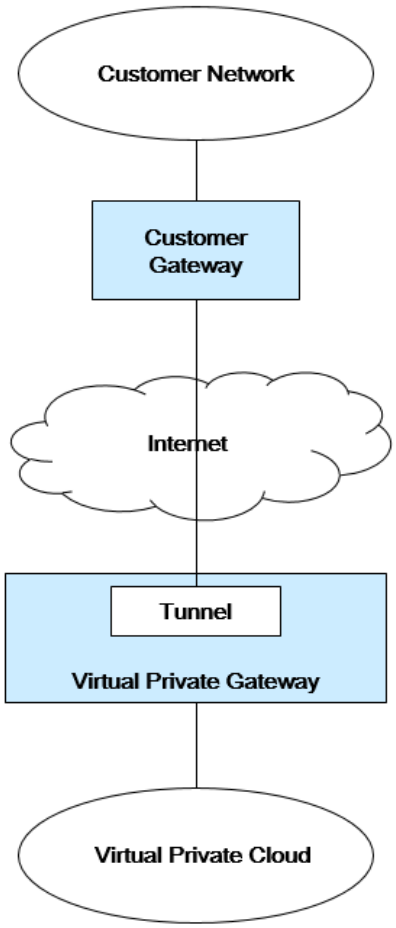
请将弹性云服务器的ID、所在子网的ID、VPC的ID提供给技术支持。

7.12 VPN 及专线网络连接出现问题时，如何排查?

VPN 网络示意图

图7-27显示您的网络、客户网关、通往虚拟专用网关的VPN连接以及VPC。

图 7-27 VPN 网络示意图



客户自查指导

1. 反馈您的网络信息

   确定表7-3中的信息。该表包括部分项目的示例值，您可以使用示例值或确定的实际值。您必须取得所有其他项目的实际值。

   说明

   您可以打印该表，并填入您的值。

   表 7-3 网络信息

Item	如何使用	注释	您的值
VPC CIDR 块	用于客户网关配置中。	示例：10.0.0.0/16	-
VPC ID信息	-	-	-

Item	如何使用	注释	您的值
1 号子网 CIDR 块（可与 VPC 的 CIDR 块相同）	-	示例：10.0.1.0/24	-
弹性云服务器 ID信息	-	-	-
客户网关类型 (例如：Cisco)	-	-	-
客户网关使用的公网IP地址	-	该值必须为静态。	-

2. 反馈您的网关配置的信息

   请客户通过以下步骤排查网关的连接性问题。

   您需要考虑四个方面：IKE、IPsec、ACL规则和路由选择。您可以按任何次序对这些方面进行故障排除，不过建议您从IKE开始 (位于网络堆栈的底部) 并依次向上排除。

   a. 获取您采用的网关设备的IKE策略。
   b. 获取您采用的网关设备的IPSEC策略。
   c. 获取您采用的网关设备的ACL规则。
   d. 检查您采用的网关设备与公有云的网关设备是否路由可达。

   说明

   具体网关设备采用的设备命令不同，请根据您采用的网关设备（Cisco、H3C、AR以及Fortinet设备等），采用对应设备的命令进行排查，获取上述信息。

客户需要协助做的运维操作

客户从公有云的弹性云服务器内向对端设备发起通信请求。

操作方法：

登录公有云的弹性云服务器使用ping命令，ping您自有数据中心的网络IP。

7.13 外网能访问服务器，但是服务器无法访问外网时，如何排查?

问题描述

外网能访问服务器，但是服务器无法访问外网，出不了我方的网关。

排查思路

您可以按照以下原因进行排查，如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 7-28 排查思路

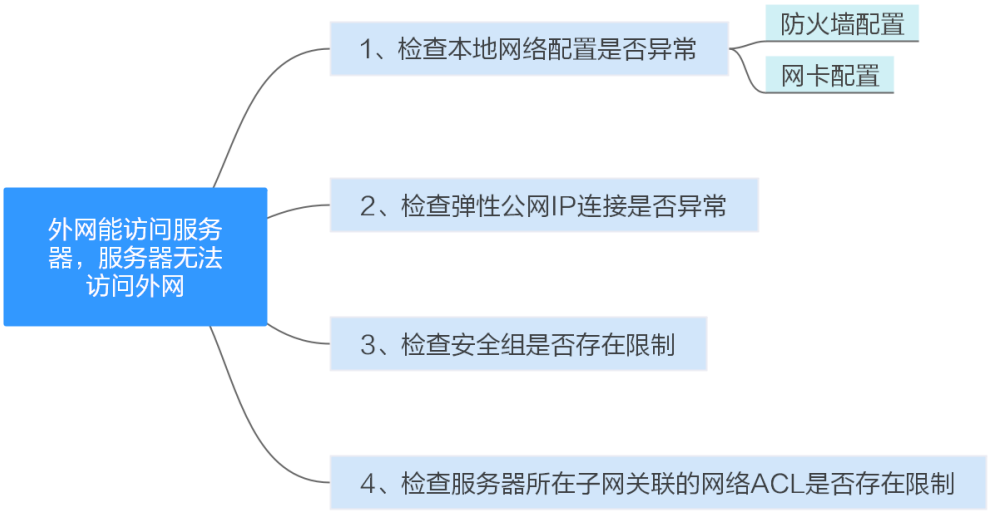


表 7-4 排查思路

可能原因	处理措施
本地网络配置异常	需要确保本地网络配置无异常，如：防火墙、网卡等配置。解决方法请参考**本地网络配置异常**。
弹性公网IP连接异常	弹性公网IP问题排查，请参见**EIP连接出现问题时，如何排查？** 。
安全组存在限制	安全组限制了云服务器出方向的流量，导致无法访问外网，解决方法请参考**安全组存在限制**。
网络ACL存在限制	网络ACL限制了云服务器所在子网出方向的流量，导致无法访问外网，解决方法请参考**网络ACL存在限制**。

本地网络配置异常

- 防火墙拦截
  查看并禁用Windows弹性云服务器防火墙策略，禁用后检查是否可以连通网络。
  - Linux系统请参考**检查防火墙配置**。
  - Windows系统请参考**检查云服务器的防火墙**。
- 网卡配置异常
  检查网卡配置、DNS配置是否正确。
  - Linux系统请参考**检查网卡配置**。
  - Windows系统请参考**检查网卡配置**。

安全组存在限制

检查服务器所在安全组出方向规则，确认是否存在限制。

安全组默认放通出方向流量，若有限制，可参考**修改安全组规则配置**，开放允许访问的协议或端口，或使用安全组的一键放通常用端口功能。

网络 ACL 存在限制

检查服务器所在子网关联的网络ACL出方向规则，确认是否存在限制。

网络ACL默认拒绝所有出站流量，需要放通服务器子网所在网关联的网络ACL出方向限制，即添加出方向规则时，选择“策略”为“允许”。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

7.14 配置了 IPv6 双栈，为什么无法访问 IPv6 网站?

问题现象

用户的云服务器已配置了IPv6双栈，但是无法访问IPv6网站。

解决思路

- 查看IPv6双栈配置是否正确，网卡是否获取到IPv6地址。
- 查看是否已将IPv6双栈网卡添加到共享带宽。
- 当云服务器拥有多张网卡时，查看在云服务器内部，是否为这些网卡配置策略路由。

图 7-29 查看网卡信息

解决方案

- 购买ECS并进行网络配置时，请务必选择“自动分配IPv6地址”。

  如果自动分配IPv6地址失败，或者您选的其他镜像不支持自动分配IPv6地址，请参考**动态获取IPv6地址**手动获取IPv6地址。

  - Windows公共镜像默认已开启IPv6动态获取功能，无需额外配置。
  - Linux公共镜像开启动态获取IPv6功能时，需要先判断是否支持IPv6协议栈，再判断是否已开启动态获取IPv6功能。

    目前，所有Linux公共镜像均已支持IPv6协议栈。并且Ubuntu 16操作系统已默认开启动态获取IPv6功能，即Ubuntu 16操作系统无需额外配置，其他Linux公共镜像需要执行开启动态获取IPv6的操作。
- 默认IPv6地址只具备私网通信能力，如果您需要通过该IPv6地址访问Internet或被Internet上的IPv6客户端访问，您需要购买和绑定共享带宽。具体请参考**购买和加入共享带宽**。

  如您已有共享带宽，可以不用重新购买，直接将IPv6地址加入共享带宽即可。

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

  如果您的云服务器是Linux云服务器，具体操作指导请参考**为多网卡Linux云服务器配置策略路由（IPv4/IPv6）**。

  如果您的云服务器是Windows云服务器，具体操作指导请参考**为多网卡Windows云服务器配置策略路由（IPv4/IPv6）**。

7.15 弹性云服务器防火墙配置完成后，为什么网络不通?

问题描述

如果您的云服务器安装完防火墙后，发现网络不通，请根据本章节指导排查原因。常见客户场景示例如下：

在同一个VPC内，客户有三台ECS，业务部署在ECS1和ECS2上，在ECSX上安装了第三方防火墙，从ECS1和ECS2出来的流量，需要通过ECSX的防火墙进行过滤。

排查思路

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

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

表 7-5 排查思路

可能原因	处理措施
检查ECS安全组是否已放通	解决方法请参考**检查ECS安全组是否已放通**。
检查网卡的“源/目的检查”开关是否关闭	解决方法请参考**检查网卡的源/目的检查开关是否关闭**。
检查VPC的自定义路由是否添加正确	解决方法请参考**检查VPC的自定义路由是否添加正确**。

检查 ECS 安全组是否已放通

同一个VPC内的子网网络互通，如果您的业务ECS和防火墙所在的ECS网络不通，可能是因为这些ECS位于不同的安全组导致的。

如果ECS位于不同的安全组内，需要您在这些ECS关联的安全组内添加对端安全组的规则，放通这些安全组的网络。

具体操作请参见**添加安全组规则**。

检查网卡的“源/目的检查”开关是否关闭

请检查防火墙所在ECS的网卡是否关闭“源/目的检查”开关，如果未关闭，请参考以下操作关闭该开关。

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在服务列表，选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中，选择目标弹性云服务器，并单击名称对应的超链接。
   进入弹性云服务器“基本信息”页签。
5. 选择“弹性网卡”页签，单击 展开主网卡区域，检查“源/目的检查”是否关闭。
   如果未关闭，请关闭该开关后，重新检查网络。

检查 VPC 的自定义路由是否添加正确

请检查业务ECS所在子网的关联路由表中是否添加指向防火墙所在ECS的路由。

防火墙安装完成后，您需要在业务ECS所在子网的关联路由表中，添加下一跳为“云服务器实例”，指向防火墙所在ECS的自定义路由。

具体操作请参见**添加自定义路由**。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

8 路由类

8.1 如何配置多网卡弹性云服务器的策略路由?

背景知识

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

操作场景

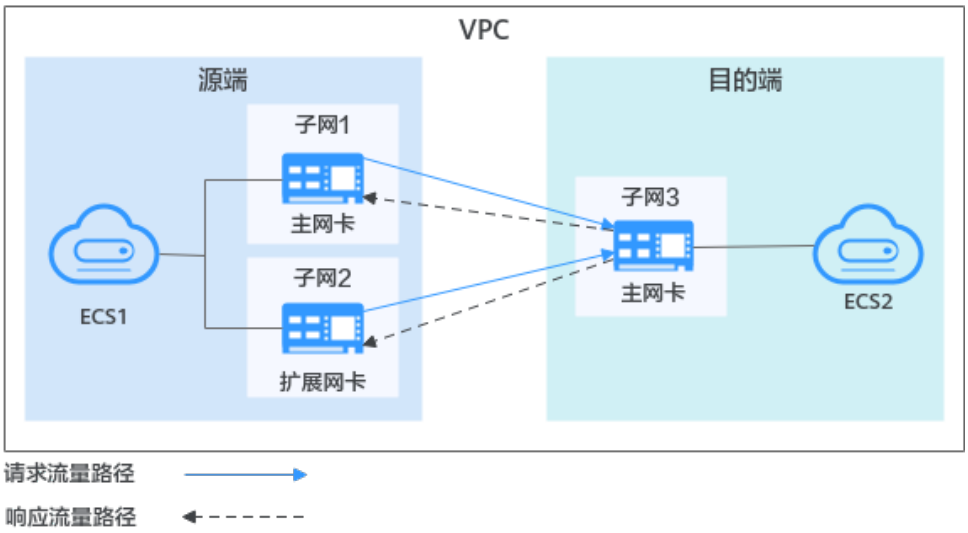
本文档以配置双网卡云服务器的策略路由为例，组网如图8-1所示，具体说明如下：

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

须知

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

图 8-1 双网卡云服务器组网示意图



操作指引

本文提供Linux和Windows云服务器的操作指导，具体请参见**表8-1**。

表 8-1 操作指引说明

操作系统类型	IP类型	操作步骤
Linux	IPv4	本文以CentOS 8.0 64bit操作系统为例： **为多网卡Linux云服务器配置策略路由（IPv4/IPv6）**
	IPv6	
Windows	IPv4	本文以Windows 2012 64bit操作系统为例： **为多网卡Windows云服务器配置策略路由（IPv4/IPv6）**
	IPv6	

8.2 路由表可以跨 VPC 存在吗？

路由表不可以跨VPC存在。

路由表由一系列路由规则组成，只能存在于某个VPC内，用于控制VPC内出入子网的流量走向。一个VPC可以有多个路由表，自带一个默认路由表，您还可以根据需求自定义多个路由表。

VPC中的每个子网都必须关联一个路由表，一个子网一次只能关联一个路由表，但一个路由表可以同时关联多个子网。

8.3 路由表有什么限制？

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

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

9 安全类

9.1 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。

9.2 TCP 25 端口出方向无法访问时怎么办?

问题描述

无法使用TCP 25端口连接外部地址。例如，运行Telnet smtp.***.com 25，该命令执行失败。

问题原因

为了提升华为云IP地址发邮件的质量，基于安全考虑，TCP 25端口出方向默认被封禁，无法使用TCP 25端口连接外部地址。

如果没有在云上部署邮件服务的需求，该限制不会影响您的服务。

说明

目前仅华北-北京一的TCP 25端口出方向默认被封禁，其他区域TCP 25端口不会封禁。

解决方案

建议您使用第三方邮件服务商支持的465端口。

9.3 如何查看安全组关联了哪些实例?

当您创建云服务器、云容器或者数据库等实例时，需要将实例加入安全组中。当您的安全组需要删除时，必须将安全组关联的实例全部移出安全组，才可以删除安全组。

您可以参考以下操作指导，查看安全组关联的实例。

1. 在安全组列表中，单击目标安全组所在行的操作列下的“管理实例”。

   进入“关联实例”页签，您可以依次查看安全组关联的服务器、扩展网卡等资源。

   如果“关联实例”页签下已无关联资源，但是系统仍然提示您安全组已被实例关联，请您继续执行以下操作。
2. 在管理控制台右上角，选择“资源 > 我的资源”，查看和安全组相同区域内，是否有表9-1中列举的资源。

表格中仅列举部分常用资源，如果您还有其他资源，请逐一排查。

同时，因为安全组一般是通过端口和各种实例进行关联，您可以通过API接口**查询端口列表**，使用待删除安全组的ID过滤，查询安全组关联的端口信息，包括name（端口名称）、device_id（端口所属设备ID）、device_owner（端口所属设备）、instance_id（端口所属实例ID）、instance_type（端口所属实例类型）等信息。通过端口信息，可以帮助您排查安全组关联的资源。

如果排查完可能关联安全组的资源后，仍然无法正常删除安全组，请**提交工单**联系客服。

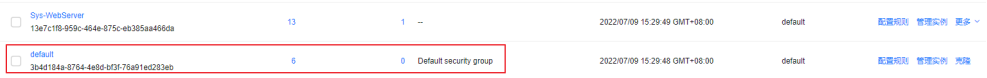
表 9-1 实例排查列表

产品分类	产品/实例名称
数据库	云数据库 GaussDB
	云数据库 RDS
	文档数据库服务 DDS
	云数据库 GaussDB NoSQL
	分布式数据库中间件 DDM
应用服务	分布式缓存服务 DCS： • Redis实例 • Memcached实例
	分布式消息服务 DMS： • Kafka实例 • RabbitMQ实例
	API网关 APIG
EI企业智能	MapReduce服务
	数据仓库服务 DWS
	云搜索服务 CSS

9.4 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。

图 9-1 默认安全组



- 当安全组已关联至其他服务实例时，比如云服务器、云容器、云数据库等，此安全组无法删除。请您将实例从安全组中移出后，重新尝试删除安全组。

  查看安全组关联的实例，具体操作请参见**如何查看安全组关联了哪些实例?** 。

- 当安全组作为“源地址”或者“目的地址”，被添加在其他安全组的规则中时，此安全组无法删除。

  需要删除该条规则或者修改规则，然后重新尝试删除安全组。

  比如，安全组sg-B中有一条安全组规则的“源地址”设置为安全组sg-A，则需要删除或者更改sg-B中的该条规则，才可以删除sg-A。

须知

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

9.5 ECS 加入安全组过后能否变更安全组?

可以。

ECS必须加入一个安全组，您可以随时变更ECS的安全组。

请您登录管理控制台，进入目标ECS详情界面，变更安全组。

详细操作，请参见**更改安全组**。

9.6 多通道协议相关的安全组配置方式是什么?

用户配置弹性云服务器

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

用户安全组配置

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

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

图 9-2 安全组规则

9.7 无法访问华为云 ECS 的某些端口时怎么办?

添加安全组规则时，需要您指定通信所需的端口或者端口范围，然后安全组根据规则，决定允许或是拒绝相关流量转发至ECS实例。

表9-2中提供了部分运营商判断的高危端口，这些端口默认被屏蔽。即使您已经添加安全组规则放通了这些端口，在受限区域仍然无法访问，此时建议您将端口修改为其他非高危端口。

表 9-2 高危端口

协议	端口
TCP	42 135 137 138 139 444 445 593 1025 1068 1433 1434 3127 3128 3129 3130 4444 4789 5554 5800 5900 8998 9995 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9995 9996

9.8 为什么网络 ACL 添加了拒绝特定 IP 地址访问的规则，但仍可以访问?

网络ACL存在规则优先级。优先级的数值越小，表示优先级越高，*为默认的规则，优先级最低。

多个网络ACL规则冲突，优先级高的规则生效，优先级低的不生效。

若某个规则需要优先或落后生效，可在对应规则（需要优先或落后于某个规则生效的规则）前面或后面插入此规则。例如：A规则优先级为1，B规则需要优先级高于A，则向A规则前插入B规则，此时B规则优先级为1，A规则优先级为2。同样地，B规则需要优先级低于A，则向A规则后插入B规则即可。

当添加了拒绝特定IP地址访问的规则时，可以将允许所有IP访问的规则放至最后，拒绝特定IP地址访问的规则将生效。具体操作请参见**添加网络ACL规则（自定义生效顺序）**。

9.9 为什么配置的安全组规则不生效?

问题描述

实例（如ECS）安全组规则配置完成后，实际未生效。比如，添加的安全组规则是允许来自特定IP的流量访问安全组内实例，结果该流量还是无法访问实例。

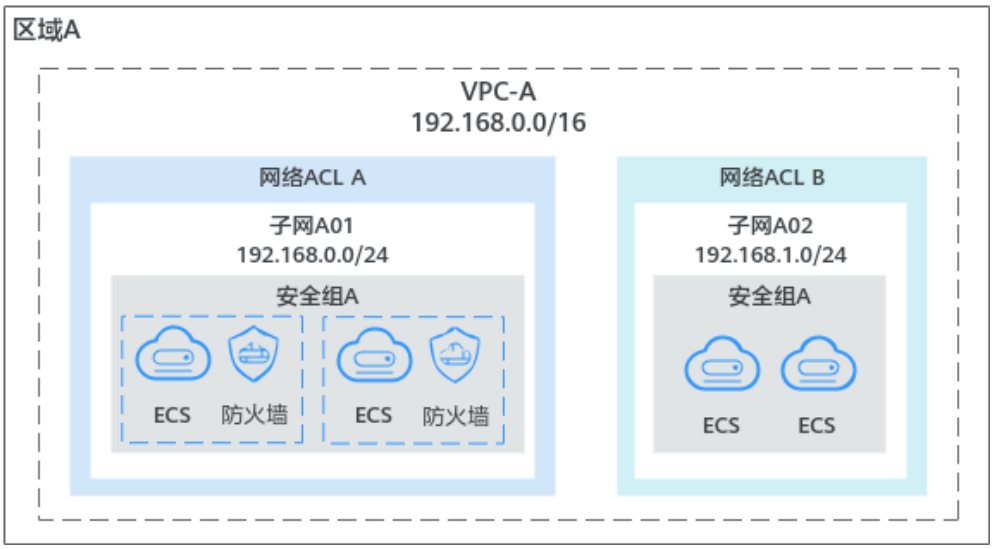
背景知识

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。

除了VPC提供的安全策略，通常情况下您还可以配置实例的防火墙，进一步提升实例的安全。不同安全策略配合使用的工作原理图如**图9-3**所示。

图 9-3 VPC 安全策略



基于以上情况，如果您的安全组规则配置完未生效，除了安全组本身参数的配置可能有误，还有可能是不同的安全策略之间存在冲突，具体请您参考以下指导处理。

排查思路

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

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 9-4 排查思路

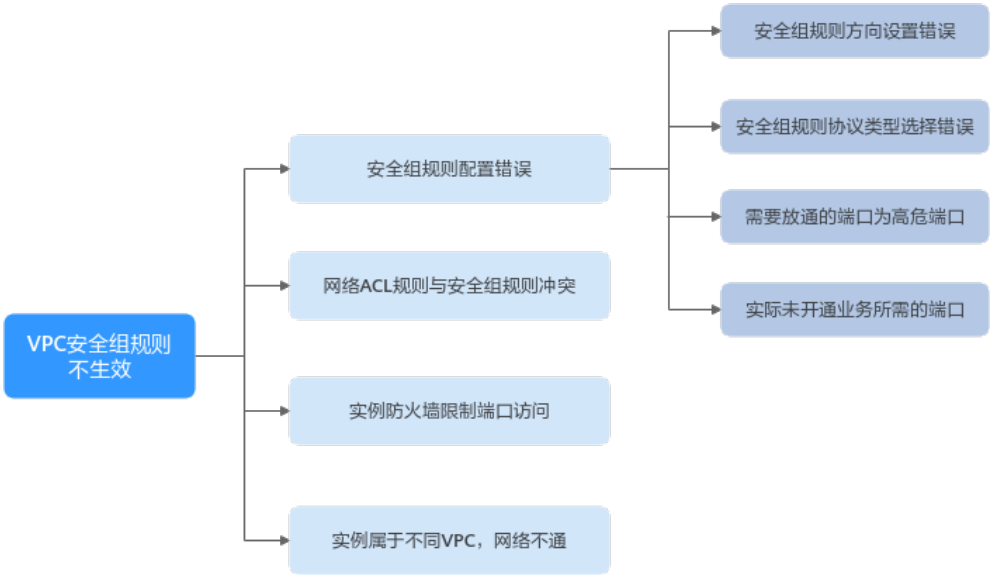


表 9-3 排查思路

可能原因	处理措施
安全组规则配置错误	解决方法请参考**安全组规则配置错误**。
网络ACL规则与安全组规则冲突	解决方法请参考**网络ACL规则与安全组规则冲突**。
实例防火墙限制端口访问	解决方法请参考**实例防火墙限制端口访问**。
实例属于不同VPC，网络不通	解决方法请参考**实例属于不同VPC，网络不通**。

安全组规则配置错误

当安全组规则配置有误时，无法按照规划的安全组规则对实例进行保护。您可以按照以下几点原因对安全组配置进行检查：

1. 安全组规则方向设置错误，例如将需要在入方向添加的规则添加到出方向规则下。

   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，控制的是流入实例的流量。
   - 出方向规则控制安全组内实例访问外部的请求，控制的是从实例流出的流量。

2. 安全组规则协议类型未选择正确。

   网络协议即匹配流量的协议类型，支持TCP、UDP、ICMP和GRE协议，请正确选择安全组规则协议类型。

3. 添加的端口是高危端口，对于运营商判断的高危端口，这些端口默认被屏蔽，在受限区域无法访问，此时建议您将端口修改为其他非高危端口。

   常用端口说明及高危端口请参考**弹性云服务器常用端口**。

4. 实际未开通业务所需的端口。

   在安全组规则中放开某个端口后，您还需要确保实例（如ECS）内对应的端口也已经放通，安全组规则才会对实例生效。

   请参考**添加安全组规则**中的“检查安全组规则是否生效”小节，检查ECS内端口开放情况，并验证配置是否生效。

当找到问题原因后，您可以参考**添加安全组规则**或**修改安全组规则**选择正确的方向或协议类型、放通需要开放的端口。

网络 ACL 规则与安全组规则冲突

安全组对实例（如ECS）进行防护，网络ACL对子网进行防护。网络ACL规则与安全组规则冲突时，优先匹配网络ACL规则，可能会导致安全组规则不生效。

例如当您的安全组入方向规则放通80端口，但是同时设置的网络ACL规则拒绝80端口的访问，那么流量优先匹配网络ACL规则，此安全组规则不生效。

您可以参考**添加网络ACL规则**或**修改网络ACL规则**放通对应协议端口。

实例防火墙限制端口访问

安全组和防火墙都可以对实例（如ECS）进行防护，当在安全组中开通某个端口的访问时，ECS的防火墙可能限制该端口的访问，您需要关闭防火墙，或者在防火墙配置例外端口。

您可以参考**Windows云服务器怎样关闭防火墙、添加例外端口？**或**Linux云服务器怎样关闭防火墙、添加例外端口？**开放例外端口。

实例属于不同 VPC，网络不通

安全组需在网络通信正常的情况下生效。若实例属于同一安全组，但是属于不同VPC，此时由于不同VPC网络不通，因此实例之间不能通信。

比如，您可以使用对等连接连通不同VPC网络，安全组才能对不同VPC内ECS的流量进行访问控制。VPC连接请参见**应用场景**。

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。