

# 私有网络 故障处理



腾讯云

**【 版权声明 】**

©2013–2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 商标声明 】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 服务声明 】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。

您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【 联系我们 】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

## 文档目录

### 故障处理

无法删除 VPC 或子网

使用云联网打通两个 VPC 后网络不通

同 VPC 下两台云服务器无法 ping 通

Linux 云服务器增加弹性网卡后无法从外部访问

## 故障处理

# 无法删除 VPC 或子网

最近更新时间：2024-11-05 15:06:32

### 现象描述

无法删除 VPC 或子网。

### 可能原因

目前 VPC 和子网的删除条件为：

- VPC：除空子网（指子网内无 IP 占用）、路由表、网络 ACL 之外，没有其他资源（对等连接、基础网络互通、NAT 网关、VPN 网关、专线网关、云联网、私有连接）时，可删除 VPC。
- 子网：子网内无资源占用 IP。

#### ❗ 说明：

目前子网中涉及 IP 占用的云资源包括：云服务器、内网负载均衡、弹性网卡、HAVIP、云函数 SCF、容器服务、云数据库（例如 MySQL、Redis、TDSQL）等。

基于以上删除条件的分析，VPC 和子网无法立即删除可能存在如下原因：

- 存在未彻底删除的云资源，如数据库被销毁后，处于**隔离中**，该状态下的数据库资源未彻底释放，会继续占用 VPC 的 IP 资源，导致不能立即删除 VPC 或子网。
- 部分资源在控制台暂无跳转，导致无法准确释放资源。

### 处理步骤

1. 登录 [私有网络控制台](#)。
2. 首先单击待删除 VPC 右侧的**删除**，查看弹框中提示 VPC 包含的云资源。

#### ❗ 说明：

此处负载均衡仅为内网负载均衡，公网负载均衡不占用 VPC 内资源。



3. 单击 **VPC ID** 进入详情页，单击对应的云资源，跳转到对应的资源界面，并释放云资源。

- 如果资源无法跳转，请在腾讯云控制台搜索对应产品，前往对应资源控制台，搜索该 VPC ID 下的对应资源，进行资源释放。
- 如果是云数据库实例，在实例销毁后一定时间实例处于**隔离中**，该状态的实例实际并未释放资源，需执行**立即下线**或等待至实例自动下线后，才可执行删除 VPC 或子网操作。

**说明：**

- 云数据库中**立即下线**操作为异步操作，部分资源的回收可能存在延迟，请稍作等待，确保实例已完成下线后，再去删除 VPC 或子网。
- 此处列举部分常用资源的释放指导，可参考：[删除云服务器](#)、[删除负载均衡](#)、[删除弹性网卡](#)、[删除对等连接](#)、[删除基础网络互通](#)、[删除 NAT 网关](#)、[删除 VPN 网关](#)、[删除专线网关](#)、[删除流日志](#)、[删除网络探测](#)、[删除 HAVIP](#)、[销毁云数据库 Redis](#)、[销毁云数据库 MySQL](#)。

4. 资源完全释放后，执行 **删除 VPC** 和 **删除子网** 验证是否可以删除成功。

- 删除成功，结束。
- 依然无法删除，请联系 [售后在线支持](#)。

# 使用云联网打通两个 VPC 后网络不通

最近更新时间：2024-11-22 09:25:52

## 现象描述

通过云联网打通两个 VPC 网络后，发现网络 ping 不通。

### 说明

- 测试网络连通性可使用如下方式之一：
  - ping 命令：用于测试源主机与目标主机网络是否连通，使用方式：ping 对端 IP。
  - telnet 命令：用于测试指定目标主机的端口是否可达，使用方式：telnet 对端 IP地址对端端口号。
  - 腾讯云数据库、CFS/ES 集群等默认禁 ping，建议使用 telnet 检测连通性。
  - 内网负载均衡的 VIP（virtual IP）仅支持来自本 VPC 的客户端 ping，因此使用云联网打通的网络，不能通过网络 ping 对端网络的内网负载均衡的 VIP 来测试网络连通性，可以使用 ping 对端 CVM，或 telnet CLB 服务端口。

## 可能原因

- 云服务器内部安装了 docker 容器，存在容器路由
- 通信子网间网段冲突，导致路由失效
- 安全组规则未放通
- 子网 ACL 规则未放通
- 云服务器内部开启了防火墙

## 处理步骤

### 步骤一：检查通信两端云服务器是否存在 docker 路由

- 进入 [云服务器控制台](#)，单击云服务器右侧的登录，按照界面提示输入密码或密钥，以 [标准方式登录云服务器](#)，并执行 route 查看系统内部路由表。
- 查看系统内是否存在 docker 容器网段路由，且与对端云服务器所在子网网段相同。
  - 如存在容器网段路由，且容器网段与对端子网网段重叠，容器网段路由与 VPC 互通路由将发生冲突，此时系统将优先选择容器路由，从而导致与对端访问不通。请更换为其他网段的通信子网，或修改容器网段，处理后请再次尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查 [步骤二](#)。
  - 如不存在，请继续排查 [步骤二](#)。

```
[root@xxxxx ~]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 0.0.0.0 0.0.0.0 UG 0 0 0 eth0
link-local 0.0.0.0 255.255.0.0 U 1002 0 0 eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.0.0.0 0.0.0.0 255.255.0.0 U 0 0 0 docker0
```

### 步骤二：判断两个 VPC 子网网段是否冲突导致路由失效

- 登录 [私有网络控制台](#)，单击云联网，进入云联网控制台。
- 单击云联网实例 ID，进入详情页面。
- 单击路由表页签，查看是否有如下图所示的失效路由。
  - 如存在失效路由，即如下图所示存在两条到相同目的端的路由条目，从而导致路由冲突失效，请根据实际情况删除/禁用冲突网段的路由，启用需要通信的路由，然后再尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查 [步骤三](#)。

- 如不存在失效路由，请继续排查 [步骤三](#)。

ccn- 详情 云联网帮助文档

关联实例 监控 带宽管理 **路由表**

2020年9月15日之后创建的专线网关默认发布路由方式为VPC网段，[点击查看详情](#)

多个关键字用竖线“|”分隔，多个过滤标签用回车键分隔

目的端	状态	下一跳	下一跳所属地域	更新时间	启用路由
10.0.0.0/24	有效	vpc-		2021-11-02 15:58:34	<input checked="" type="checkbox"/>
10.0.2.0/24	有效	vpc-		2021-11-02 15:58:34	<input checked="" type="checkbox"/>
10.0.0.0/24	失效	vpc-		2021-11-02 16:23:24	<input type="checkbox"/>
10.0.3.0/24	有效	vpc-		2021-11-02 16:12:53	<input checked="" type="checkbox"/>

### 步骤三：检查通信两端云服务器的安全组规则是否放通

- 登录 [云服务器控制台](#)。
- 单击云服务器实例 ID，进入实例详情界面。
- 单击安全组页签，查看是否有放通 ICMP 协议，及对应来源 IP/目的 IP 的出入站安全组规则。
  - 如无对应协议规则，或规则为拒绝，请单击编辑修改对应协议的安全组规则，然后尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查 [步骤四](#)。
  - 如安全组出入站规则均正确，请继续排查 [步骤四](#)。

#### 异常示例：

安全组规则 关联实例

入站规则 **出站规则**

添加规则 导入规则 排序 删除 一键放通 教我设置

目标	协议端口	策略	备注	修改时间	操作
0.0.0.0/0	ICMP	拒绝	支持Ping服务	2021-11-02 21:51:55	编辑 插入 删除
0.0.0.0/0	ALL	允许		2021-11-02 21:33:24	编辑 插入 删除

#### 正常示例：

sg- )

安全组规则 关联实例

入站规则 **出站规则**

添加规则 导入规则 排序 删除 一键放通 教我设置

来源	协议端口	策略	备注	修改时间	操作
0.0.0.0/0	ICMP	允许	支持Ping服务	2021-11-02 21:43:42	编辑 插入 删除

### 步骤四：检查通信两端子网关联的 ACL 规则是否放通

- 在云服务器详情页，单击该云服务器所属子网 ID 进入子网详情界面。

云服务器

- 实例自助检测
- 自动化助手
- 实例与镜像
  - 实例
  - 实例启动模板
  - 专用宿主机
  - 置放群组
  - 专有预扣资源池
- 镜像
- SSH密钥
- 回收站
- 网络与安全

基本信息 弹性网卡 公网IP 监控 安全组

实例信息

名称: test2

实例ID: ins-

UUID:

实例规格: 标准型S6 | S6.MEDIUM2

地域: 广州

可用区: 广州七区

网络信息

所属网络: vpc-

所属子网: subnet-

2. 单击 **ACL 规则** 页签，查看子网是否绑定了网络 ACL，且 ACL 出站规则中，是否有拒绝 ICMP 协议，及来源/目标 IP 的规则。

- 如未绑定 ACL，请继续排查 [步骤五](#)。
- 如绑定了 ACL，且 ACL 规则已允许相应协议及 IP，则继续排查 [步骤五](#)。
- 如绑定了 ACL，但 ICMP 规则为**拒绝**，或 ACL 中无 ICMP 规则，请单击 ACL ID，进入 ACL 界面，修改使得对应协议及来源/目标 IP 的规则为**允许**，然后尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查 [步骤五](#)。

#### 说明

如确认不需要使用 ACL 规则对子网流量进行控制，也可以解绑 ACL，该操作需谨慎评估影响后再执行。

基本信息 入站规则 **出站规则**

规则列表 编辑 导入规则 导出规则

目标IP	协议类型	端口	策略	备注
::/0	All traffic	ALL	拒绝	-
10	ICMP	-	拒绝	-

### 步骤五：请检查通信两端云服务器是否开启了防火墙

请自行确认云服务器是否开启防火墙，如开启请确保防火墙不会对通信流量进行拦截，否则需要放通防火墙的限制。

#### 说明

- 清除防火墙的操作方法请参见 [如何清除防火墙](#)。
- 如已完成上述所有问题排查但问题依然存在，请做好问题记录，并联系 [售后在线支持](#)。

# 同 VPC 下两台云服务器无法 ping 通

最近更新时间：2023-09-06 09:50:11

## 现象描述

同一 VPC 内的两台云服务器无法 ping 通。

## 可能原因

- 云服务器安全组规则未放通。
- 云服务器所在子网的网络 ACL 规则未放通。
- 云服务器内存在容器路由。

## 处理步骤

### 检查云服务器实例关联的安全组规则

- 登录 [云服务器控制台](#)。
- 单击云服务器实例 ID，进入实例详情界面。
- 单击安全组页签，查看是否有放通 ICMP 协议，及对应来源 IP/目的 IP 的出入站安全组规则。
  - 如无对应协议规则，或规则为拒绝，请单击编辑修改对应协议的安全组规则，然后尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查。
  - 如安全组出入站规则均正确，请继续排查。

#### 异常示例：

目标	协议端口	策略	备注	修改时间	操作
0.0.0.0/0	ICMP	拒绝	支持Ping服务	2021-11-02 21:51:55	编辑 插入 删除
0.0.0.0/0	ALL	允许		2021-11-02 21:33:24	编辑 插入 删除

#### 正常示例：

来源	协议端口	策略	备注	修改时间	操作
0.0.0.0/0	ICMP	允许	支持Ping服务	2021-11-02 21:43:42	编辑 插入 删除

### 检查子网关联的网络 ACL 规则

- 登录 [云服务器控制台](#)。
- 单击云服务器实例 ID，进入实例详情界面。
- 在实例详情 > 基本信息页面，单击网络信息模块下的 所属子网 ID。

4. 在子网基本信息页面，可查看子网是否绑定了网络 ACL，且 ACL 出入站规则页签中，是否有拒绝 ICMP 协议，及来源/目标 IP 的规则。

- 如绑定了 ACL，且 ACL 中 ICMP 规则为拒绝，或 ACL 中无 ICMP 规则，请单击 ACL ID，进入 ACL 界面，将对应协议，及来源/目标 IP 的规则修改为允许，并将该条规则移到第一条，确保规则优先匹配，然后尝试 ping 测试问题是否解决，解决则结束，未解决则继续排查。
- 如未绑定 ACL，或 ACL 规则已允许相应协议及 IP，请继续排查。

目标IP ⓘ	协议类型	端口 ⓘ	策略	备注
::/0	All traffic	ALL	拒绝	-
10	ICMP	-	拒绝	-

### 检查云服务器内是否存在容器路由

1. 进入 [云服务器控制台](#)，单击云服务器右侧的登录，按照界面提示输入密码或密钥，以 [标准方式登录云服务器](#)，并执行 route 查看系统内部路由表。

```
[root@ ~]# route
Kernel IP routing table
Destination      Gateway         Genmask       Flags Metric Ref    Use Iface
default          0.0.0.0        0.0.0.0      UG    0     0     0 eth0
link-local      0.0.0.0        255.255.0.0  U     1002  0     0 eth0
0.0.0.0         0.0.0.0        255.255.255.0 U     0     0     0 eth0
0.0.0.0         0.0.0.0        255.255.0.0  U     0     0     0 docker0
```

2. 查看系统内是否存在 docker 容器网段路由，且与被访问的云服务器所在子网网段相同。

- 如存在容器网段路由，且容器网段与子网网段相同，容器网段路由与 VPC 系统内路由冲突，也可能导致此问题，可删除对应子网。
- 如不存在，请记录问题，并联系 [售后在线支持](#)。

# Linux 云服务器增加弹性网卡后无法从外部访问

最近更新时间：2023-08-01 17:40:53

## 现象描述

某用户云服务器主网卡无公网 IP，主要用于内网通信，因有公网业务的需求，故绑定了一个弹性网卡（辅助网卡），并在弹性网卡上绑定了弹性公网 IP，但无法从外部正常访问。

```
root@cloud:~# ping 139.129.129.129
PING 139.129.129.129 (139.129.129.129): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
```

## 可能原因

云服务器绑定弹性网卡后，如需从外部访问，需要为弹性网卡绑定弹性公网 IP（EIP），并配置正确的网卡策略路由，该问题可从如下原因逐个排查定位：

- 弹性网卡未正确绑定到云服务器上
- 弹性网卡内网 IP 未正确配置到弹性网卡上
- 路由表中默认路由由内网网卡路由由优先级高于外网网卡
- 未配置网卡的策略路由表
- 策略路由表中未添加网卡的默认网关
- 未配置弹性网卡的策略路由规则

## 处理步骤

### 步骤一：检查弹性网卡是否已正确绑定到了云服务器上

1. 登录 [云服务器控制台](#)，单击云服务器实例 ID，进入实例详情页。

ID/名称	监控	状态	可用区	实例类型	实例配置	主IPv4地址	主IPv6地址	实例计费模式	操作
ins- <span style="border: 1px solid red; padding: 2px;">xxxxxx</span>		运行中	成都一区	标准型SA2	1核 1GB 1Mbps 系统盘：高性能云硬盘 网络：	<span style="background-color: #ccc; padding: 2px;">xxxxxx</span> (弹) <span style="background-color: #ccc; padding: 2px;">xxxxxx</span>	-	按量计费 2021-10-13 16:41:42创建	<a href="#">登录</a> <a href="#">更多</a>

2. 单击弹性网卡页签，查看云服务器是否有弹性网卡，以及是否绑定了 EIP。

- 如有弹性网卡，且正确绑定了 EIP，如下图所示，则继续排查 [步骤二](#)。
- 如没有，请参考 [绑定并配置弹性网卡](#) 和 [绑定弹性公网 IP](#) 配置后，再尝试外网访问，问题解决则结束，未解决则继续排查。

ins- [实例ID] 登录 更多操

基本信息 **弹性网卡** 公网IP 监控 安全组 操作日志 执行命令

实例绑定弹性网卡后，您需登录实例配置IP及路由，点击查看操作指南

绑定弹性网卡

ins- [实例ID] (主网卡) 分配内网IP 解绑

enitest- [实例ID] (辅助网卡) 分配内网IP 解绑

内网IP	类型	普通公网IP/EIP	备注	操作
10.0. [IP]	主IP	139. [IP] eip- [ID] <span>解绑</span>	-	修改主IP

## 步骤二：检查弹性网卡内网 IP 是否正确配置到弹性网卡上

1. 单击云服务器详情页弹性网卡页签下的弹性网卡 ID，进入弹性网卡详情页。

en- [实例ID] **eni- [网卡ID]** (辅助网卡) 分配内网IP 解绑

内网IP	类型	普通公网IP/EIP	备注	操作
10.0. [IP]	主IP	139. [IP]	-	修改主IP

2. 记录弹性网卡的 MAC 地址，并单击IPv4 地址管理页签，记录弹性网卡的内网 IP 地址。

• MAC 地址：

eni- [网卡ID] 详情

基本信息 **IPv4 地址管理** IPv6 地址管理 关联安全组

名称	en- [实例ID]
ID	eni- [网卡ID]
MAC地址	20: [MAC]:83

• 弹性网卡内网 IP：

enit 详情

基本信息 IPv4 地址管理 IPv6 地址管理 关联安全组

分配内网IP

内网IP	类型	普通公网IP/EIP	备注
10.0	主IP	139.	-

3. 返回 [云服务器控制台](#)，单击云服务器右侧的登录，按照界面提示输入密码或密钥，以 [标准方式登录云服务器](#)。

ID/名称	监控	状态	可用区	实例类型	实例配置	主IPv4地址	主IPv6地址	实例计费模式	操作
ins-		运行中	成都一区	标准型SA2	1核 1GB 1Mbps 系统盘：高性能云硬盘 网络：	42.	-	按量计费 2021-10-13 16:41:42创建	登录 更多

4. 执行如下命令，查看弹性网卡的内网 IP 和 MAC 地址与 [步骤2](#) 记录的是否一致。

```
ip address
```

```
[root@VM- centos ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet  scope host lo
       valid_lft forever preferred_lft forever
   inet6  ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 52:54:00:d2:4e:3b brd ff:ff:ff:ff:ff:ff
   inet  brd  ; scope global eth0
       valid_lft forever preferred_lft forever
   inet6  scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether 20:  : brd ff:ff:ff:ff:ff:ff
[root@VM- centos ~]#
```

- 如一致，请继续排查 [步骤三](#)。
- 如不一致或缺失，请执行 [步骤5](#) 进行修改。

5. 执行如下命令重新修改弹性网卡的配置文件。

**说明**

此处以 Centos7.8 为例，Centos7 系统网卡配置文件一般存放在“/etc/sysconfig/network-scripts”目录，保存在“ifcfg-网卡名称”文件。

5.1 执行如下命令，进入配置文件。

```
cd /etc/sysconfig/network-scripts/ #进入配置文件所在目录
vim ifcfg-eth1 #编辑弹性网卡配置文件
```

5.2 按 **i** 开始编辑。

```
DEVICE='eth1' #弹性网卡的网卡名
```

```
HWADDR=20:90:6F:63:98:CC #弹性网卡的 MAC 地址
NM_CONTROLLED='yes'
ONBOOT='yes'
IPADDR='10.0.0.14' # 此处填写弹性网卡上的内网 IP 地址, 请根据实际情况填写
NETMASK='255.255.255.0' # 此处填写子网掩码, 请根据实际情况填写
GATEWAY='10.0.0.1' # 填写网卡所在子网的网关 IP 地址, 请根据实际情况填写
```

5.3 按“ESC”，并输入“:wq!”保存并退出。

5.4 执行如下命令，重启网络，使配置生效。

```
systemctl restart network
```

5.5 再次执行 `ip address`，确认内网 IP 已经配置到弹性网卡上，如下图所示。

```
[root@VM- -centos network-scripts]# systemctl restart network
[root@VM- -centos network-scripts]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 20:90:6f:63:98:cc brd ff:ff:ff:ff:ff:ff
    inet scope global eth0
        valid_lft forever preferred_lft forever
    inet6 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 20:90:6f:63:98:cc brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.14/24 brd 10.0.0.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 scope link
        valid_lft forever preferred_lft forever
```

### 步骤三（可选）：检查路由表中默认路由由内网网卡的路由优先级是否高于外网网卡的优先级

#### ! 说明

- 本例 eth0 无弹性公网 IP，主要用于内网通信，为内网网卡；eth1 配置了弹性公网 IP，为外网网卡。
- 如路由表中无内网明细路由（如下图中10.0.0.0/24的路由条目），调整外网网卡路由优先级，有可能导致内网流量被转发到外网网卡，可能会对业务有影响，如担心此风险，可跳过该步骤，直接按照 [步骤四](#) 开始排查，即排查每个网卡，确保配置了独立的策略路由表，策略路由表的优势在于保证流量源进源出。
- 如路由表中有明细路由，可按照此方法排查并修复故障效率会更高。

1. 在云服务器登录界面，执行 `route` 命令查看当前云服务器的路由表，可以看到有两条“default”路由，这两条默认路由由接口分别为“eth0”内网和“eth1”外网，其中“eth0”这条“default”对应 metric 为100，“eth1”的 metric 为101，路由优选了“eth0”（metric 数值越小越优）走了内网卡，导致数据返回 Internet 失败，因此需要将“eth1”对应的路由优先级调高。

```
[root@VM- -centos ~]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default _gateway 0.0.0.0 UG 100 0 0 eth0
default _gateway 0.0.0.0 UG 101 0 0 eth1
10.0.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 101 0 0 eth1
[root@VM- -centos ~]#
```

2. 执行如下命令调整外网网卡路由由优先级比内网网卡路由由优先级高（metric 值越小优先级越高），然后再尝试外网访问，问题解决则结束，未解决请联系 [在线支持](#) 进一步定位处理。

```
ip route add default dev eth1 via 10.0.0.1 metric 10 #10.0.0.1请更换为弹性网卡的网关 IP，  
metric 值修改为比内网网卡的 metric 值100小即可，此处举例设置为10
```

#### 步骤四：检查是否配置了网卡的策略路由表

1. 在云服务器登录界面，执行如下命令查看是否已创建策略路由表。

```
cat /etc/iproute2/rt_tables
```

无策略路由表如下图所示：

```
[root@VM- .centos network-scripts]# cat /etc/iproute2/rt_tables  
#  
# reserved values  
#  
255     local  
254     main  
253     default  
0       unspec  
#  
# local  
#  
#1      inr.ruhep
```

- 如无，请执行 [步骤2](#) 创建策略路由表。
- 如有，请继续排查 [步骤五](#)。

2. 创建两张策略路由表。

```
echo "10 t1" >> /etc/iproute2/rt_tables #10为自定义的路由ID，t1为自定义的路由表名称，请根据实际填写。  
echo "20 t2" >> /etc/iproute2/rt_tables #20为自定义的路由ID，t2为自定义的路由表名称，请根据实际填写。
```

已配置好策略路由表如下图所示：

```
[root@VM-0-11-centos ~]# cat /etc/iproute2/route/tables
#
# reserved values
#
255     local
254     main
253     default
0       unspec
#
# local
#
#1      inr.ruhep
10 t1
20 t2
```

### 步骤五：检查是否将每个网卡的默认网关配置到策略路由表中

#### ! 说明

配置好策略路由表后，需要针对每个网卡配置网卡的默认路由到策略路由表中。

1. 在云服务器登录界面，执行如下命令，可看到默认路由表中已经有弹性网卡的内网路由信息。

```
ip route show
```

```
[root@VM-0-11-centos ~]# ip route show
default via 10.0.0.1 dev eth0 默认路由
10.0.0.0 dev eth0 proto kernel scope link src 10.0.0.11 主网卡的内网路由
10.0.0.0 dev eth1 proto kernel scope link src 10.0.0.12 弹性网卡的内网路由
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.0.0/16 dev eth1 scope link metric 1003
```

2. 依次执行如下命令，查看 table 10 和 table 20 路由表是否已配置默认网关。

```
ip route show table 10
ip route show table 20
```

- 如下图所示，无返回信息，表示未配置默认网关，请执行 [步骤3](#) 为策略路由表添加默认网关。
- 如有返回信息，且正确，则继续排查 [步骤六](#)。

```
[root@VM-0-11-centos ~]# ip route show table 10
[root@VM-0-11-centos ~]#
```

3. 执行如下命令为两个路由表分别配置默认网关。

```
ip route add default dev eth0 via 10.0.1.1 table 10 #10.0.1.1为eth0的默认网关，请根据实际情况填写
ip route add default dev eth1 via 10.0.0.1 table 20 #10.0.0.1为eth1的默认网关，请根据实际情况填写
```

#### ⚠ 注意

- 每个 table 都需要检查，因为不同的 table 设置了不同网卡的默认路由。
- 请一定确认网关与网卡名对应一致，此处经常出现将 eth0 的网关配置到 eth1 上而导致配置问题，因此请务必做好检查。
- 此处配置为临时路由，重启网络后路由会消失，如需配置永久路由，请参见 [配置永久路由](#)。

配置后可查询到两个路由表中配置的默认路由条目：

```
[root@VM- centos ~]# ip route show table 10
default via 10. .1 dev eth0
[root@VM- -centos ~]# ip route show table 20
default via 10. .1 dev eth1
```

### 步骤六：检查是否配置了正确的策略路由规则

#### ❗ 说明

配置好默认路由后，目前系统已经知道哪个路由表走哪个网关出去，但还不知道某个网卡来的流量，要到哪个路由表上，因此需要查看是否为每个网卡配置了策略规则。

1. 执行 `ip rule list` 命令，查看是否有策略路由规则。

- 如仅有0、32766、32767三条默认规则，表示弹性网卡未配策略路由规则，请执行 [步骤2](#) 配置。
- 如已配置如红框所示的策略规则，且仍然无法 ping 通，请联系 [在线支持](#) 进一步定位处理。

```
[root@VM- -centos ~]# ip rule show
0:      from all lookup local
32764:  from 10. .12 lookup t2
32765:  from 10. .11 lookup t1
32766:  from all lookup main
32767:  from all lookup default
```

2. 按照如下步骤配置策略路由规则。

```
ip rule add from 10.0.1.3 table 10 # IP为主网卡的 IP, 10为主网卡的策略路由表代号, 请根据实际情况填写。
ip rule add from 10.0.0.14 table 20 # IP为弹性网卡的 IP, 20为弹性网卡的策略路由表代号, 请根据实际情况填写。
```

3. 配置后，在外网 ping 弹性网卡的EIP验证问题是否解决。

- 如返回如下报文，表示已 ping 通，问题解决，结束。
- 如依然无法 ping 通，请记录问题信息，并联系 [在线支持](#) 进一步定位处理。

```
( ) ~ % ping 139.
PING 139. (139.): 56 data bytes
64 bytes from 139.: icmp_seq=0 ttl=64 time=64.250 ms
64 bytes from 139.: icmp_seq=1 ttl=64 time=64.720 ms
64 bytes from 139.: icmp_seq=2 ttl=64 time=65.025 ms
```