

云联网 故障处理 产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【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。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。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模式的承诺或保证。

文档目录

故障处理

使用云联网打通两个 VPC 后网络不通

故障处理

使用云联网打通两个 VPC 后网络不通

最近更新时间：2024-01-10 14:58:51

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

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。

2. 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@ ~]# route
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref
default          0.0.0.0         0.0.0.0        UG    0     0
link-local       0.0.0.0         255.255.0.0    U     1002  0
0.0.0.0         0.0.0.0         255.255.255.0  U     0     0
0.0.0.0         0.0.0.0         255.255.0.0    U     0     0
```

步骤二：判断两个 VPC 子网网段是否冲突导致路由失效

1. 登录 [私有网络控制台](#)，单击云联网，进入云联网控制台。
2. 单击云联网实例 ID，进入详情页面。
3. 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](#)。

步骤三：检查通信两端云服务器的安全组规则是否放通

1. 登录 [云服务器控制台](#)。
2. 单击云服务器实例 ID，进入实例详情界面。
3. 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](#)。

步骤四：检查通信两端子网关联的 ACL 规则是否放通

1. 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。
2. 单击 ACL 规则页签，查看子网是否绑定了网络 ACL，且 ACL 出入站规则中，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。

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 [提交工单](#)。