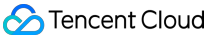
Virtual Private Cloud Troubleshooting

Copyright Notice

Trademark Notice



Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Troubleshooting
VPCs or Subnets Cannot Be Deleted

Last updated: 2026-03-17 14:20:50

Problem

VPCs or Subnets Cannot Be Deleted

Common Causes

The current deletion criteria for VPCs and subnets are as follows:

- VPC: A VPC can only be deleted when there is no resource (Peering Connections, ClassicLink, NAT Gateway, VPN Gateway, Direct Connect Gateway, CCN, and Private Link) associated other than empty subnets (IPs in the subnet are not used), route tables, and network ACLs.
- Subnet: A subnet can only be deleted when it's not associated with any resource.

> **Note**
> Currently, Tencent Cloud resources that involve IP use in subnets include CVM, private network CLB, ENI, HAVIP, SCF, TKE, and TencentDB (for MySQL, Redis, TDSQL, etc.).

According to the rules above, VPCs and subnets cannot be deleted in the following cases:

- There are cloud resources that have not been completely deleted. For example, after a database is terminated, it is in **Isolated** status, and the database resources in this status actually are not completely released and continue to use the IP resources of the VPC. Therefore, the VPC or subnet cannot be deleted immediately.
- Some resources cannot be deleted in the VPC console.

Instructions

1. Log in to VPC console.
2. Click **Delete** on the right of the VPC to be deleted, and check the associated resources.

> **Note**
> Note that public network CLB instances don't use VPC resources.

3. Click the **VPC ID** to enter the details page, click the corresponding cloud resource to enter its details page, and release it.

- If the direction to a resource fails, search for the corresponding product in the Tencent Cloud console, go to the resource's console, search for the resource under the VPC ID, and release it.
- A TencentDB instance is put into the **Isolated** status for a certain period after being terminated, during which the resources are not actually released. You need to click **Eliminate Now** or wait until the instance is automatically eliminated before you can delete the VPC or subnet.

> **Note**
> - The **Eliminate Now** operation in TencentDB is async. There may be a delay in the repossession of some resources, so the VPC or subnet cannot be deleted immediately. In this case, wait a while.
> - For more information, see Terminating Instances (for CVM), Deleting CLB Instances, Deleting an ENI, Deleting a Peering Connection, Deleting a Classiclink, Deleting NAT Gateway, Deleting a VPN Gateway, Deleting Direct Connect Gateway, Delete Flow Logs, Deleting Network Probe, Releasing HAVIPs, Terminating Instance (for TencentDB for Redis), and Terminating Instance (for TencentDB for MySQL).

4. After the resources are completely released, delete the VPC and subnet again.
   - Deletion succeeds and the process ends.
   - If the problem persists, please contact Online Support for assistance.

Network Disconnection After Connecting Two VPCs over CCN

Last updated: 2024-01-12 15:04:22

Problem

Two VPCs are connected through CCN, but a ping failure occurs.

> **Note**
> - There are two ways to test the network connectivity.
> - **ping**: Run "ping **peer IP**" to test whether the source server and the target server are connected.
> - Telnet command: Used to test whether the specified target host's port is reachable. Usage: telnet **remote IP address remote port number**.
> - Tencent Cloud databases, CFS/ES clusters, and others, by default, disable ping. It is recommended to use telnet for connectivity checks.
> - VIPs of private CLBs only support ping commands from clients in the same VPC. When you want to test the CCN connection of two network resources, ping the IP of peer CVM or telnet to the CLB service port.

Common Causes

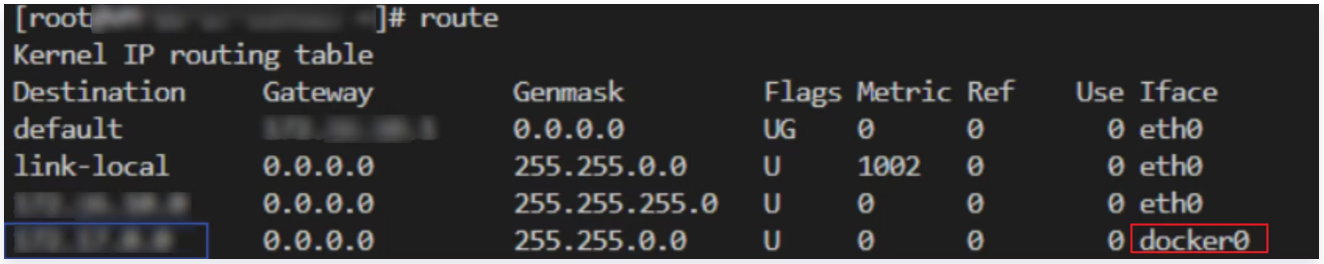
- A Docker container is installed in the CVM instance, and there is a container route.
- Routing failed due to a subnet IP range conflict.
- Blocked by the security group rules
- Blocked by the subnet ACL rules
- Blocked by the CVM firewall

Instructions

Step 1. Check for Docker route on the two CVM instances

1. Navigate to the CVM console, click **Login** on the right side of the CVM instance, enter the password or key as prompted, log in to the CVM instance using the standard method, and execute the route command to view the internal routing table of the system.
2. Check whether there is a Docker container route in the system with the same IP range as the subnet of the peer CVM instance.

- If so, the container route will conflict with the VPC route. In this case, the system will select the container route preferably, leading to inaccessibility to the peer. You need to use a subnet with another IP range or modify the container IP range, and then ping again to test whether the problem is solved. If not, go to Step 2.
- If there is no container route, go to Step 2.



Step 2. Determine whether the route failed due to the conflict between two VPC subnet IP ranges

1. Log in to the VPC console and click **CCN** to enter the CCN console.
2. Click the ID/name of the CCN instance to enter the details page.
3. Click the **Route table** tab to check if there is an **invalid** route as shown in the figure below.

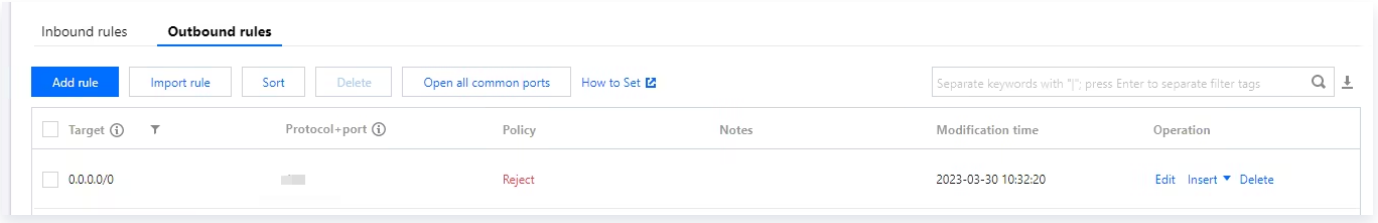
- If an **invalid** route exists, for example, two routes with the same destination exist as shown in the figure below, a route conflict occurs. Delete/Disable the conflicting route, enable the route needed, and ping again. If the problem is solved, the process ends. If the problem persists, proceed to Step 3.
- If there is no invalid route, go to step 3.

Step 3. Check the security group rules for the two CVM instances

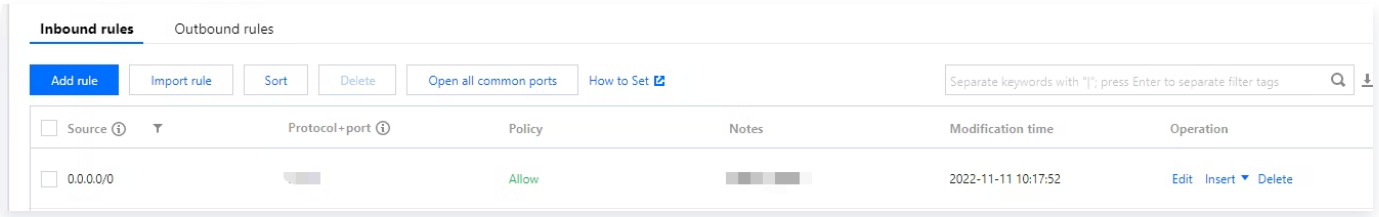
1. Log in to the CVM console.
2. Click a CVM instance ID to enter the details page.
3. Click the **Security Group** tab to check whether access is allowed in the ICMP protocol and the inbound and outbound security group rules for the source/destination IPs.

- If there is no protocol rule, or the rule is **Rejected**, click **Edit** to modify the security group rule for the protocol, and then ping again to see whether the problem is solved. If not, go to step 4.
- If the inbound and outbound rules of the security group are correct, proceed to Step 4.

Rejected:



Allowed:



Step 4. Check the ACL rules associated with the two subnets

1. On the CVM instance details page, click the subnet ID of the CVM instance to enter the subnet details page.
2. Click the **ACL Rule** tab to check whether the subnet is bound to a network ACL, whether there are rules that reject the ICMP protocol, and whether the source/destination IPs are allowed in the inbound and outbound ACL rules.
   - If no ACL is bound, proceed to Step 5.
   - If an ACL is bound and the ACL rule already allows the corresponding protocol and IPs, proceed to Step 5.
   - If an ACL is bound and ICMP is **Rejected** in the ACL, or there is no ICMP rule in the ACL, then click the ACL ID to enter the ACL page, **allow** the protocol and source/destination IPs, and then ping again to test whether the problem is solved. If not, go to step 5.

> **Note**
> You can also disassociate ACL rules if you do not need them to control subnet traffic. Evaluate the impact before you disassociate them.

Step 5. Check the firewall on the two CVM instances

Check whether the firewall of the CVM blocks the connection. If yes, lift the firewall.

> **Note**
> - For more information on how to lift the firewall, see Firewall.
> - If the problem persists after troubleshooting all the issues mentioned above, please record the problem and contact our online support team for assistance.

Failed to Ping CVMs in the Same VPC

Last updated: 2024-01-12 15:04:26

Problem

Failed to ping two CVM instances in the Same VPC.

Common Causes

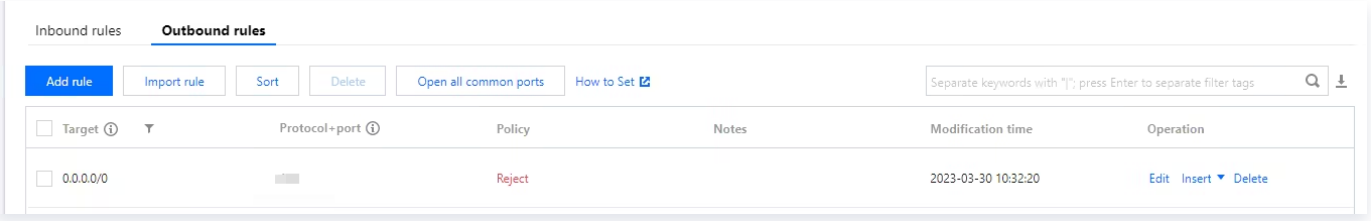
- The access is blocked by the security group rules of the CVM.
- The access is blocked by the network ACL rules of the subnet.
- There is a container route in a CVM instance.

Instructions

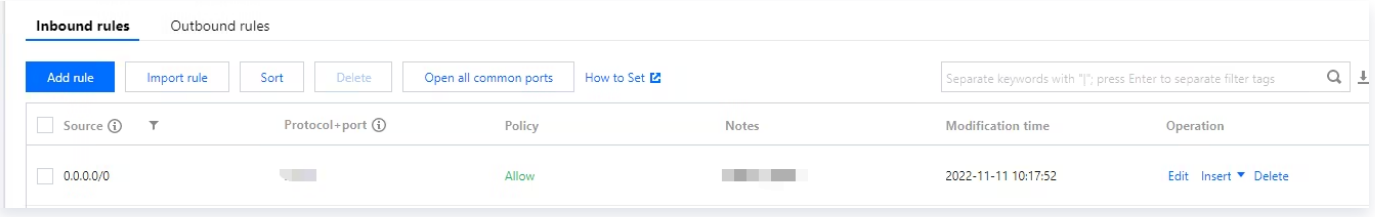
Checking the security group rules

1. Log in to the CVM console.
2. Click a CVM instance ID to enter the details page.
3. Click the **Security group** tab to check whether access is allowed in the ICMP protocol and the inbound and outbound security group rules for the source/destination IPs.
   - If there is no corresponding protocol rule, or the rule is **Reject**, click **Edit** to modify the security group rule for the protocol, and then ping again to see whether the problem is solved.
   - If the inbound and outbound rules of the security group are correct, proceed to the next step.

Rejected:



Allowed:

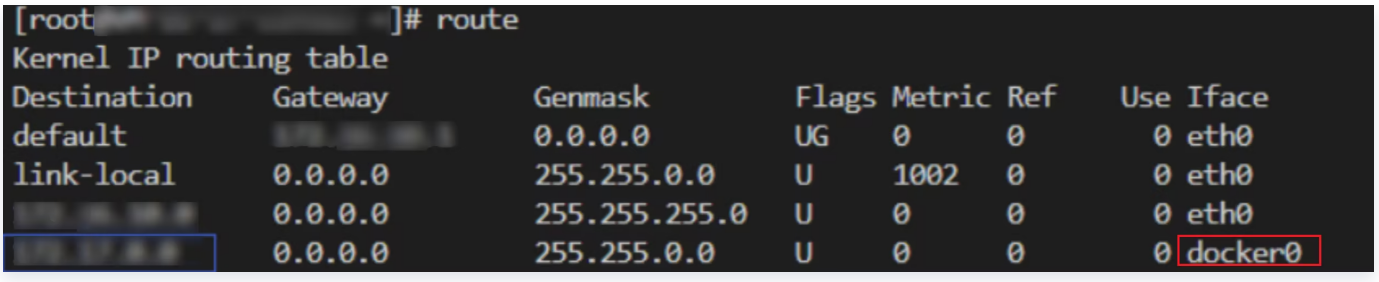


Checking the network ACL rules associated with the subnet

1. Log in to the CVM console.
2. Click a CVM instance ID to enter the details page.
3. Go to **Instance details** > **Basic information**, click the subnet ID in **Network information** section.
4. On the **Basic information** tab, check whether the subnet is bound to a network ACL. On the "ACL rule" tab, check whether there are rules that reject the ICMP protocol, and whether the source/destination IPs are allowed in the inbound and outbound ACL rules.
   - If an ACL is bound and ICMP is **rejected** in the ACL, or there is no ICMP rule in the ACL, then click the ACL ID to enter the ACL page, **allow** the corresponding protocol and source/destination IPs, and move the rule to the first place so that it will be matched first. Then, ping again to see whether the problem is solved, and if not, proceed to the next step.
   - If no ACL is bound, or the ACL rule already allows the corresponding protocol and IPs, proceed to the next step.

Checking for container route in CVM instances

1. Navigate to the Cloud Server Console, click **Login** on the right side of the cloud server, follow the interface prompts to enter the password or key, log in to the cloud server in a standard manner, and execute the route command to view the internal routing table of the system.



2. Check whether there is a Docker container route in the system with the same IP range as the subnet of the accessed CVM instance.
   - If yes, this problem is caused by the conflict with the container route. You need to delete the corresponding subnet.

- If no, please contact Online Support for assistance.