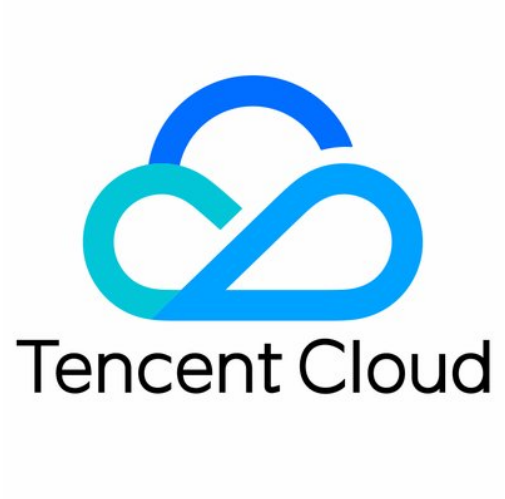
Cloud Connect Network

Troubleshooting

Product Documentation



Contents

Troubleshooting
Failed to Ping VPCs Connected with a CCN Instance

Last updated：2024-01-10 14:41:59

Symptom

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

Note:

You can use either of the following methods to test network connectivity:

Command `ping` : tests the network connectivity between a source host and a destination host. Command format: ping **Peer IP**

Command `telnet` : tests whether the port of a specified destination host is reachable. Command format: telnet **Peer IPPeer port number**

TencentDB and CFS/ES clusters prohibit the `ping` command by default. We recommend that you use the `telnet` command to test connectivity.

A private network CLB VIP can be pinged only by a local VPC client. Therefore, the connectivity between the networks connected with a CCN instance cannot be tested by pinging the private network CLB VIP of the peer network. Instead, you can ping the peer CVM instance or telnet the CLB service port.

Possible Causes

There is a Docker container route between the two CVM instances because Docker is installed on them.

Routing failed due to a subnet IP range conflict.

Security group rules are blocked.

Subnet ACL rules are blocked.

A firewall is enabled in the CVM instances.

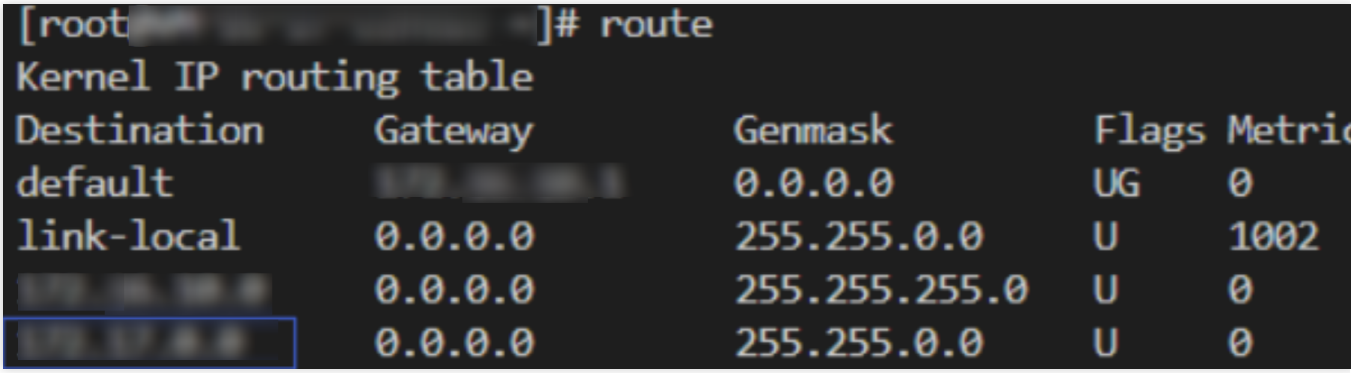
Troubleshooting

Step 1: Check whether there is a container route between the CVM instances

1. Go to the CVM console, click **Login** on the right of a CVM instance, enter the password or key as prompted to log in to the instance in the standard method, and run `route` to view the internal route 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 such a Docker container route exists, the container route will conflict with the VPC route. In this case, the system will choose the container route preferably, resulting in a failure to access the peer instance. Use a subnet with another IP range or modify the container IP range, and ping again. If the problem is solved, the process ends. If the problem persists, proceed to Step 2.

If such a Docker container route does not exist, proceed to Step 2.



Step 2: Check whether the routing failed due to a subnet IP range conflict between the two VPCs

1. Log in to the CCN console.
2. Click the ID/name of the CCN instance to enter the details page of the CCN instance.
3. Click the **Route Table** tab to check the route status.

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 no invalid route exists, proceed to Step 3.

Step 3: Check whether the security group rules for the two CVM instances are allowed

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 the ICMP protocol and the inbound and outbound security group rules for the source/destination IPs are allowed.

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. If the problem is solved, the process ends. If the problem persists, proceed to Step 4.

If the inbound and outbound rules of the security group are correct, proceed to Step 4.

Step 4: Check whether the ACL rules associated with the two subnets are allowed

1. On the CVM instance details page, click the ID/name of the subnet to which the CVM instance belongs 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 but ICMP is **rejected**, or there is no ICMP rule in the ACL, click the ACL ID to enter the ACL page, **allow** the corresponding protocol and source/destination IPs, and ping again. If the problem is solved, the process ends. If the problem persists, proceed to Step 5.

Note:

If you do not need to use ACL rules to control subnet traffic, you can also unbind ACLs. Evaluate the impact of this operation carefully before performing this operation.

Step 5: Check whether a firewall is enabled on the two CVM instances

If a firewall is enabled, ensure that the firewall does not block traffic. If the firewall blocks traffic, you need to remove the firewall restriction.

Note:

How can I remove a firewall?

If the problem persists, record the problem and submit a ticket.