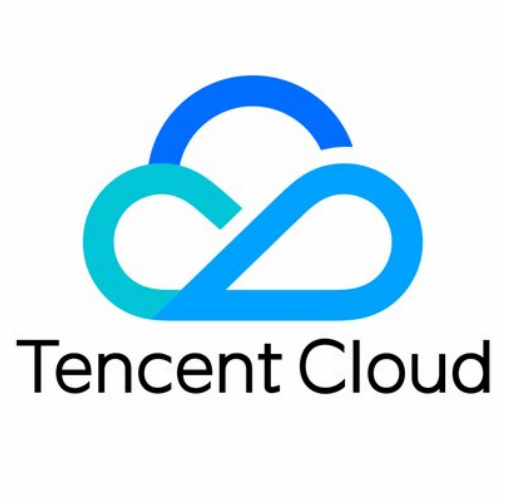
Virtual Private Cloud

Troubleshooting

Product Documentation



Contents

Troubleshooting
VPCs or Subnets Cannot Be Deleted

Last updated：2022-05-06 18:40:59

Error Description

VPCs or subnets cannot be deleted.

Common Causes

- VPC: A VPC can only be deleted when there is no resource associated other than empty subnets (IPs in the subnet are not used), routing tables, and network ACLs.
- Subnet: A subnet can only be deleted when it’s not associated with any resource.

> Note：
> Resources that can be associated with the subnet 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 can not be deleted in the VPC console.

Troubleshooting Procedure

1. Log in to the 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** in TencentDB is an async operation. It may take some time for the returning of operation result. You need to wait till the TencentDB instance is completely released.
     - 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, 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.
   - If the problem persists, contact us for assistance.

Network Disconnection After Connecting Two VPCs over CCN

Last updated：2022-06-27 14:15:13

Issue Description

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

Note：

- You can test network connectivity in one of the following methods:
- ping command: Run the "ping **peer IP**" command to test whether the source server and the target server are connected.
- telnet command: Run the "telnet **peer IP peer port number**" command to test whether the port of the specified target server is reachable.
- As ping is forbidden for TencentDB and CFS/ES clusters by default, we recommend you use telnet to test the connectivity.
- As the virtual IP (VIP) of a private network CLB instance can be pinged only from a client in the same VPC, you cannot ping the peer VIP to test the connectivity of the network connected over CCN; instead, you can ping the peer CVM or telnet the CLB service port.

Possible Causes

- A Docker container is installed in the CVM instance, and there is a container route.
- Subnet IP ranges conflict, causing the route to fail.
- The security group rule does not allow access.
- The subnet ACL rule does not allow access.
- The firewall is enabled in the CVM instance.

Troubleshooting

Step 1. Check for any Docker route in the CVM instances at both sides of the communication

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 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 a CCN instance ID to enter the details page.
3. Click the **Route Table** tab to check the route status.

- If there is an **Invalid** route; that is, if there are two routes to the same destination as shown below, thereby causing the route conflict, delete or disable the route with the conflicting IP range according to the actual situation, enable the route that you need for communication, and then ping again to test whether the problem is solved. If not, go to step 3.
- If there is no invalid route, go to step 3.

Step 3. Check whether the security group rules of the CVM instances at both sides of the communication allow access

1. Log in to the CVM console.
2. Click the 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 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, go to step 4.
  Rejected:

Allowed:

Step 4. Check whether the ACL rules associated with the subnets at both sides of the communication allow access

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, go to step 5.
- If an ACL is bound, and the ACL rule already allows the protocol and IPs, go 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 whether the firewall is enabled in the CVM instances at both sides of the communication

Confirm whether the firewall is enabled in the CVM instance and make sure that it will not block the communication traffic; otherwise, remove the firewall.

> Note：
>
> - For more information on how to remove a firewall, see Firewall.
> - If the problem persists, record it and submit a ticket for assistance.

Failed to Ping CVMs in the Same VPC

Last updated：2022-03-01 17:48:12

Error Description

The ping between two CVM instances in the same VPC fails.

Common Causes

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

Troubleshooting Procedure

Check 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 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 to see whether the problem is solved.
- If the inbound and outbound rules of the security group are correct, proceed to the next step.
  Reject:

  Allow:

Check the network ACL rules associated with subnets

1. Log in to the CVM console.
2. Click a CVM instance ID to enter the details page.

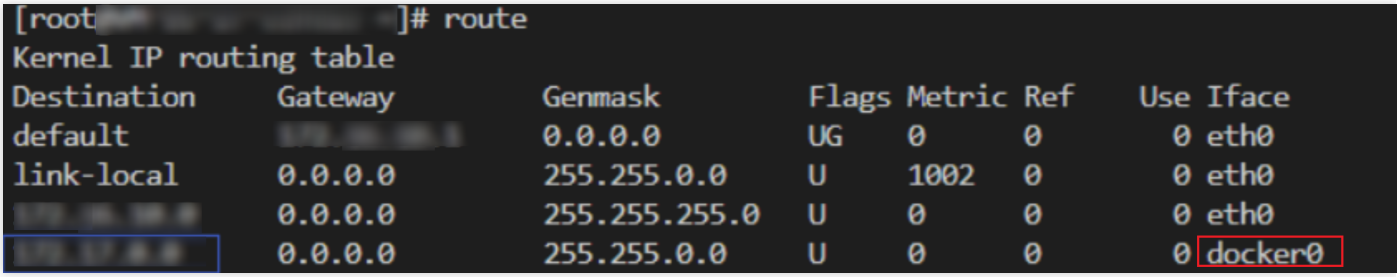
3. Click the **ACL Rule** tab to check whether the subnet is bound to a network ACL, whether there are rules that reject the ICMP protocol, and whether the source/destination IPs are allowed in the inbound and outbound ACL rules.

- If 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 instance

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 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, contact us for assistance.