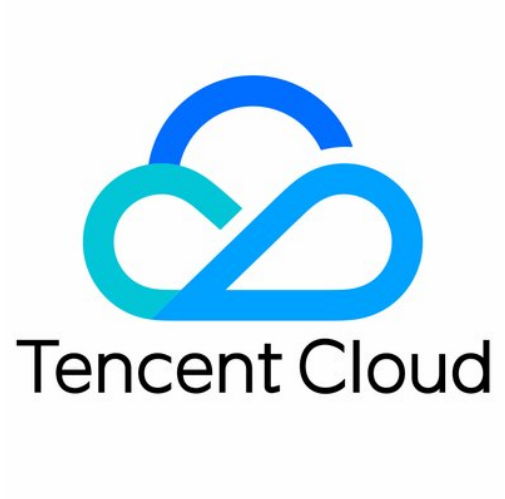
Virtual Private Cloud

FAQs

Product Documentation



Contents

FAQs
General
Concept-Related

Last updated : 2020-09-10 17:10:46

How can I establish communication between different subnets of a VPC?

- Each VPC supports private network interconnection by default, and you can find the default route in the corresponding route table. This route indicates that all resources in this VPC can connect with each other over the private network.
- Subnets in different VPC instances are not interconnected over the private network. To interconnect these subnets, establish peering connection or use Cloud Connect Network.

Can CVMs be deployed in different availability zones in the same VPC?

Yes. A VPC is a regional (such as Guangzhou, Beijing, or Seoul) resource, and the subnets in the VPC are resources in availability zones (such as Guangzhou Zone 1 or Guangzhou Zone 2). Therefore, subnets in one VPC can be deployed in different availability zones in the same region. A CVM is also availability zone specific as the subnet it belongs to. So, if you purchase CVMs under subnets in availability zones, you can deploy them in different availability zones.

How can I establish communication between CVMs and databases in different availability zones?

- In the same VPC: CVMs and databases in the same VPC are interconnected by default. If the interconnection fails, you can first troubleshoot the firewall policies of the security group and the network ACL.
- In different VPCs: CVMs and databases are isolated by default. If the interconnection is required, you can establish private network interconnection between VPC instances using peering connection or CCN.

How many private IP addresses can each VPC provide for Tencent Cloud service instances?

A VPC supports a maximum of 65,533 private IP addresses for Tencent Cloud service instances.

What is a CIDR block?

Classless Inter-Domain Routing (CIDR) is a user-specified independent network space address block. It combines IP and masking to achieve network division. Without the traditional Class A, B and C IP

addresses as well as subnet, it allocates IP address spaces more effectively. To create a VPC and subnet, you need to create IP ranges in CIDR format. In the `10.0.16.0 - 10.0.17.255` example, This IP range changes to `00001010.00000000.00010000.00000000 - 00001010.00000000.00010001.11111111` in binary format that has the same first 23 digits, and to `10.0.16.0/23` in CIDR format.

IP Range- and IP-Related

Last updated : 2020-04-02 18:19:10

What Are the Limits on the IP Ranges of VPC Instances and Subnets?

Tencent Cloud VPC CIDR supports one of the following private IP ranges:

- `10.0.0.0` - `10.255.255.255` (mask range: 16 - 28)
- `172.16.0.0` - `172.31.255.255` (mask range: 16 - 28)
- `192.168.0.0` - `192.168.255.255` (mask range: 16 - 28)

The CIDR blocks of subnets must be within or identical to those of the VPC.

Can I Modify the IP Ranges of VPC Instances and Subnets?

- When creating a VPC and subnet, you need to designate their CIDR blocks, and they cannot be changed once created.
- If you cannot establish peering connections due to VPC IP range overlapping, we recommend that you use CCN that has a smaller limit granularity (ensure that subnet IP ranges do not overlap) or migrate the instances in the VPC. For details on inter-VPC migration, see Switching VPC Instances.

What Should I Do When a Peering Connection Fails to Be Established Due to a VPC IP Range Conflict?

When you try to establish a peering connection, the CIDR blocks of VPC instances on both ends cannot overlap, otherwise the peering connection will fail to be established.

- If the subnet IP address ranges of both VPC instances that need to communicate do not overlap, you can use CCN to establish communication. CCN lowers the IP range limits to the subnet level when VPC instances communicate.
  For example, if the IP ranges of VPC instances that need to communicate with each other are both `10.0.0.0/16`, but those of the subnets are `10.0.1.0/24` and `10.0.2.0/24`, you can establish communication by using CCN. For more information, see CCN Product Documentation.
- If your needs cannot be met by using CCN, you need to migrate the resources within the overlapping subnets.
  - For information on changing the subnets of CVMs, see Changing Subnets of Instances.
  - For information on inter-VPC migration, see Switching VPC Instances.

Can I Modify the Private IP Addresses of Resources (CVMs and Databases) in VPC Instances?

- Modifying the primary private IP address of a CVM's primary ENI is supported, but modifying the primary private IP of a secondary ENI is not supported. For details, see Modifying a Private IP Address.
- The private IP addresses of private network cloud load balancers (CLBs) or cloud databases (TencentDB) cannot be modified.

Can I Switch the CVMs or Databases in a VPC to Another VPC?

- CVM migration is currently supported, but the migration of databases and other resources is not supported at this time.
- CVMs can be migrated from the current VPC to another VPC under the same account. For details on the steps and instructions, see Switching VPC Instances.

What Do EIPs Do?

EIPs apply to the following scenarios:

1. **Disaster recovery**
   We strongly recommend that you use EIPs for disaster recovery. When one of your CVMs fails to provide service, you can unbind the EIP from this CVM and rebind it to a healthy CVM to restore service quickly.
2. **Retaining a specific public IP address**
   To retain a specific public IP address under your account, you can convert it to an EIP, which then can be used to access public networks after being bound to a device. This EIP will be retained under your account until it is "released" by you.
3. **Other special scenarios**
   When you need to change an IP address in other special cases, you can convert the common public IP address to an EIP and then bind or unbind the EIP as needed. However, with limited EIP resources available, a quota is imposed on the number of EIPs for each region under a single account. Therefore, we recommend that you plan and use EIPs reasonably.

How Can I Keep a Public IP Address Unchanged?

To retain a specific public IP address under your account, you can convert it to an EIP, which then can be used to access public networks after being bound to a device. This EIP will be retained under your account until it is "released" by you.

For relevant instructions, see Converting a Public IP Address to an EIP.

Can I Convert an EIP Back to a Public IP Address?

An EIP cannot be converted back to a public IP address.

Basic Network-Related

Last updated : 2020-04-12 19:31:24

What Is the Difference Between the Basic Network and the VPC?

- A VPC is a logically isolated network space that you can establish on Tencent Cloud.
- A VPC provides more features than the basic network. For details on their differences and how to choose between them, see Managing the Basic Network.

Can I Change the Attribute of a CVM from Basic Network to VPC?

Yes, you can do this by using the service of switching a single CVM or a batch of CVMs from the basic network to VPC instances. For detailed steps and instructions, see Switching to VPC.
-> This operation cannot be undone. Be sure to carefully read the document before performing this operation.

Can I Change the Attribute of a CVM from VPC to Basic Network?

No, you cannot. Currently, changing the attribute of a CVM from VPC to basic network is not supported. A VPC supports more features with greater flexibility, and therefore we recommend that you migrate from the basic network to the VPC.

How Can I Establish Communication Between a CVM in the Basic Network and a CVM in a VPC?

You can use Classiclink to establish communication between the basic network and the VPC.
Using Classiclink is subject to the following limitations:

1. The basic network and the VPC that need to communicate with each other must be in the same region (but can be in different availability zones, such as Guangzhou Zone 1 and Guangzhou Zone 2).
2. The CIDR block (IP address range) of the VPC must be `10.[0-47].0.0/16` (including subsets), otherwise a conflict occurs.

If your basic network and VPC meet these conditions, you can configure the settings in the Classiclink area on the details page of the VPC in the console, to associate the VPC with the CVMs in the basic network for interconnection.

Can Resources Such as Cloud Load Balancers and Databases in the Basic Network Communicate with the VPC?

- A terminal connection helps establish communication between instances in a VPC and other instances in a basic network through the private network. Here, the principle is to establish mapping between basic network instance IP addresses and VPC IP addresses so that you can access a basic network instance by accessing the corresponding VPC IP address. Supported basic network products include CLB, TencentDB, CMEM, REDIS, and MongoDB. Cross-region and cross-account communication is not supported.
- Direction: one-way (the VPC accesses the basic network.)
- If you need more directions, submit a ticket to apply.

Can Basic Networks and VPC Instances Under Different Accounts Communicate with Each Other?

Currently, communication between resources (CVMs and databases) of basic networks and VPC instances under different accounts is not supported. A VPC supports more features with greater flexibility, and therefore we recommend that you migrate from the basic network to the VPC.

How Can I Disassociate a CVM from a VPC or Basic Network?

The disassociation procedure is as follows:

1. Log in to VPC Console.
2. Click the ID of the VPC that is interconnected with the basic network to enter the VPC details page.
3. Click **Classiclink**. In the list of basic network CVMs, select the CVM to be disassociated and click **Unassociate**.
4. Click **OK** to complete the disassociation.

Product Quota-Related

Last updated : 2020-04-02 18:19:12

Are There any Quota Limits for VPC instances, and How Many VPC Instances Can Be Created Under Each Account?

Some VPC resources are subject to usage quota limits. By default, up to five VPC instances can be created in each region under the same account.

How Many EIPs Can Be Applied For by Each Account?

- Each Tencent Cloud account can apply for up to 20 EIPs in each region.
- The number of purchases that can be made by each Tencent Cloud account in each region per day is the doubled quota (that is, 40 times by default). When an EIP is unbound, the number of reassignments of public IP addresses that can be performed for free by each account per day is 10.

Connection
Connecting to the Internet

Last updated : 2020-04-13 19:07:43

How Do I Apply for a Public IP Address if None Was Assigned When I Purchased the CVM?

If no public IP address was assigned when you purchased the CVM, you cannot re-apply for a common public IP address for this CVM. However, you can achieve this purpose by using EIPs. For details on how to apply for EIPs, see Applying for EIPs.

- An EIP is a public IP address that is fixed to a specific IP address in a certain region. Unlike a common public IP address, it is bound to your account. In other words, you can bind an EIP with and unbind it from different CVMs as required (only one EIP can be bound at a time.)
- Due to the nature of EIPs, if you apply for an EIP but do not bind it with an instance, idleness fees incur. For details, see EIP Billing.

How Can an Instance (CVM or Database) Access the Internet Without a Public IP Address?

An instance without a public IP address can apply for an EIP (see the previous question) or can access the Internet through the NAT gateway.
A NAT gateway provides CVMs in a VPC with the SNAT and DNAT features. If you have multiple CVMs that need to access the Internet through a public IP address, you can use a NAT gateway.

Can I Change the Public IP Address of a CVM?

Yes, you can.

- If your CVM was assigned a common public IP address at the time of purchase, see Changing Public IP Addresses.
- If your CVM is bound to an EIP, you need to unbind the EIP and apply for an EIP again or bind it to an existing EIP.

> After you convert a public IP address into an EIP, we recommend that you immediately release the EIP. Otherwise, the EIP that is not bound to any instance will incur resource occupation fees.

Can I Retrieve a Previously Used Public IP Address, and Can I Apply for a Specific EIP?

- Public IP addresses cannot be recovered after being released.
- EIPs that were once used by you and have not yet been assigned to other users can be recovered. For details, see Recovering Public IP Addresses.

Can I Increase the Quota After the Number of EIPs Reaches the Upper Limit?

Due to the limits on EIP resources, each account can apply for up to 20 EIPs in each region, and this quota cannot be increased. CVMs without public IP addresses can access the Internet through a NAT gateway or other means.

How Does a CVM Access the Internet if It Has a Public IP Address or EIP and Its Subnet Is Also Associated with a NAT Gateway?

If a CVM has a public IP address or EIP and its subnet is associated with a NAT gateway, the route table specifies that the next hop for the traffic of this subnet to access the Internet is a NAT gateway. In this case, all the traffic of this CVM to access the Internet flows through the NAT gateway by default.

If you need to modify the priorities to redirect the traffic of the CVM to access the Internet through a public IP address, see Adjusting the Priorities of NAT Gateways and Public IP Addresses.

If a CVM Accesses the Internet Through a Public Gateway or a NAT Gateway, Will the Network Fees Be Charged Twice?

No, the network fees will be charged only once. When you access the Internet through a public gateway or NAT gateway, only the network fee for using the public gateway or NAT gateway will be charged.

Inter-VPC Communication

Last updated : 2020-09-10 17:33:52

How Do CVMs or Databases Interconnect through the Private Network?

The private network communication of CVMs or databases in a VPC is actually the communication of private IP addresses at the network level, and therefore there is no difference between them. The communication methods under different private IP address scenarios are as follows:

Communication Scenario	Communication Method
Different regions	CVMs or databases in different regions belong to different VPC instances and communicate with each other through peering connections or CCN. (Both same-account and cross-account communication are supported.)
Different availability zones	Same VPC: support interconnection by default. Different VPC instances: communicate through peering connections or CCN. (Both same-account and cross-account communication are supported.)
Different VPC instances	Communicate through peering connections or CCN. (Both same-account and cross-account communication are supported.)
Different subnets	Same VPC: support interconnection by default. Different VPCs: communicate through peering connections or CCN. (Both same-account and cross-account communication are supported.)
Cross-account	Cross-account communication through peering connections or CCN. (Both same-region and cross-region communication are supported.)

⚠ Note :

- For the cross-account VPC interconnection through peering connection or CCN, take note of the following:
  - The root account owns resources. If you want to communicate with another account through peering connection or CCN, enter the root account.
  - The sub-account only has the operation permission by default. Apply for permission from the root account to establish the peering connection or CCN if needed.
- **Private network default interconnection** is present between different subnets of the same VPC (whether or not they are in the same availability zone). If they cannot connect with each other, you can first troubleshoot the firewall policies of the security group and the network ACL.

What Should I Do When a Peering Connection Fails to Be Established Due to a VPC IP Range Conflict?

When you try to establish a peering connection, the CIDR blocks of the two VPC instances cannot overlap, otherwise the peering connection cannot be established.

- If the IP ranges of both VPC instances that need to intercommunicate overlap but the subnet IP ranges do not overlap, then you can try to establish communication through CCN. CCN can lower IP address range limits to the subnet level when VPC instances communicate with each other. For example, the IP ranges of both VPC instances that need to communicate with each other are both `10.0.0.0/16`, but the subnets are `10.0.1.0/24` and `10.0.2.0/24` respectively. In this case, you can establish communication through CCN. For more information, see CCN.
- If your needs cannot be met by using CCN, you need to migrate the resources inside the overlapping subnets.
  - For details on changing the subnets of CVMs, see Changing the Subnets of Instances.
  - For details on inter-VPC migration, see Switching VPC Instances.

If VPC1 Separately Establishes Peering Connections With VPC2 and VPC3, Then Can VPC2 and VPC3 Communicate with Each Other?

No, they cannot. Two VPC instances can establish interconnection through a peering connection, but this interconnection relationship is not transitive. This means that when a peering connection is established between VPC1 and VPC2 while another peering connection is established between VPC1 and VPC3, traffic interconnection is unavailable between VPC2 and VPC3 because the peering connection is not transitive.

Classiclink-Related

Last updated : 2020-09-28 11:25:36

What is Classiclink?

The Classiclink is used to associate CVMs in the classic network to the specific VPC, enabling CVMs to communicate with Tencent Cloud services including CVMs and databases in the VPC. For more information, see Managing Classic Networks.

How can I establish communication between a CVM in a classic network and a CVM in a VPC?

You can use Classiclink to establish communication between classic networks and VPCs.
When using the Classiclink, take note of the following limits:

1. The classic network and the VPC that need to communicate with each other must be in the same region (but can be in different availability zones, such as Guangzhou Zone 1 and Guangzhou Zone 2).
2. The CIDR (IP range) of the VPC must be `10.0.0.0/16 - 10.47.0.0/16` (including subsets), otherwise a conflict occurs.

If your classic network and VPC meet these conditions, you can configure the **Classiclink** tab on the details page of the VPC in the Console to associate the VPC with the CVMs in the classic network for interconnection.

Can resources including cloud load balancers and databases in the classic network communicate with the VPC?

- A terminal connection helps establish communication between instances in a VPC and other instances in a classic network over a private network. The principle is to map the IP addresses of instances in the classic network to VPC IP addresses so that you can access a classic network instance by accessing the corresponding VPC IP address. The services that support the classic network include classic CLB, TencentDB, CMEM, REDIS, MongoDB. Cross-region/cross-account communication is not supported.
- Direction: one-way (VPC accesses the classic network).
- If you need more directions, submit a ticket to apply.

Can classic network and VPC instances under different accounts communicate with each other?

No. Currently, resources (CVMs and databases) in classic networks and VPC instances under different accounts cannot communicate with each other. A VPC supports more features with greater flexibility, so we recommend migrating from the classic network to VPC.

Security
VPC Security-Related

Last updated : 2020-04-02 18:19:17

How Do I Ensure the Security of CVMs in VPC Instances?

The VPC itself is a logically isolated network environment, and traffic can be controlled by configuring security groups and network ACLs:

- Security group: provides network traffic control for CVMs at the instance level. Traffic that is disallowed to flow in or out of the instance is automatically rejected.
- Network ACL: provides subnet-level network traffic control.

Port and Security Group-Related

Last updated : 2020-04-02 18:19:18

Port-Related Questions

Why does a port have to be enabled, and how can I enable a specific port?

You can use the services corresponding to a port only after opening the port in the security group.
For example:
To access web pages through port 8080, this port must be enabled and opened to Internet in the security group.
Step-by-step instructions for opening a certain port to the Internet are as follows:

1. Log in to Security Group Console and click the security group that is bound with this instance to go to the details page.
2. Choose **Inbound/Outbound Rules** and click **Add Rule**.
3. Enter your IP address (or IP range) and the port to be opened, and then select **Allow** to open the port.

Why is the service unavailable after the port has been modified?

After modifying the service port, you must additionally open the port in the corresponding security group before the service can be used.

Which ports are not supported by Tencent Cloud?

The following ports are blocked by the carrier due to security considerations. We recommend that you use other ports than the following for listening:

Protocol	Unsupported Ports
TCP	Ports 42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, and 9996
UDP	Ports 1026, 1027, 1434, 1068, 5554, 9996, 1028, 1433, and 135-139

Why cannot TCP port 25 be used to connect to an external address, and how can I unblock the port?

- To enhance the quality of sending emails through Tencent Cloud's IP addresses, CVMs are blocked by default from using TCP port 25 to connect to external addresses. To unblock this port, you can

log in to the console, hover over the account navigation area at the top, and click **Security Control** to view the link for unblocking port 25.
- By default, each user can unblock up to five instances in each region.

For more port-related instructions, see Common Server Ports.

Security Group-Related Questions

Why is a rejection rule set in a security group by default?

Security group rules take effect in order from top to bottom. Therefore, after the allowance rule that was set first is validated, other rules will be invalidated by default. If the rule opens all ports to the Internet, the last rejection rule will be invalid. This default setting is provided for security concerns.

If I bind an instance with the incorrect security group, what will be the impact on the instance, and how can I fix this?

- **Potential problems**
  - You may fail to remotely connect to a Linux instance (through SSH) or remotely log in to a Windows desktop instance.
  - You may fail to remotely ping the public or private IP address of a CVM instance in this security group.
  - You may fail to gain HTTP access to the web services opened by a CVM instance in this security group.
  - You may fail to access the Internet through an instance in this security group.
- **Solutions**
  - In case any of the preceding problems occurs, you can go to "Security Group Management" in the console and edit the rule for the security group, for example, to "only bind all-pass security groups by default".
  - For details on setting security group rules, see Security Groups - Security Group Rules.

What do a security group direction and a policy mean?

- Security group policies work in the directions of outbound and inbound. The outbound direction is to filter the outbound traffic of the CVM, whereas the inbound direction is to filter the inbound traffic of the CVM.
- Security group policies are divided into policies that **allow** or **reject** traffic.

What is the order in which security group policies take effect?

The order in which security group policies take effect is from top to bottom. Traffic goes through the security group's policy matching in order from top to bottom, and the first hit policy will take effect.

Why can an IP address that is rejected by the security group access the CVM?

The possible reasons for this issue are:

- The CVM may be bound to multiple security groups, and the IP address is allowed by another security group.
- The IP address belongs to an approved Tencent Cloud public service.

Does using security groups mean that iptables cannot be used?

No, security groups and iptables can be used simultaneously. In this case, your traffic will be filtered twice in the following directions:

- Outbound: processes in your instance > iptables > security groups.
- Inbound: security groups > iptables > processes in your instance.

Why cannot security groups be deleted even after all CVMs have been returned?

Check Recycle Bin for any CVMs. The deletion will fail if security groups are bound to CVMs in Recycle Bin.

Is there any cloud API that supports cloning a security group across different projects and regions?

Console support is available to customers who are using the console, but no cloud API support is available for now. You can use the original cloud APIs for importing or exporting security group rules in batches to indirectly clone a security group across different projects and regions.

When I clone security groups across projects and regions, will CVMs managed by the security groups also be copied?

No, cloning a security group across different regions clones only the inbound and outbound rules of the original security group. In this case, CVMs must be associated separately.