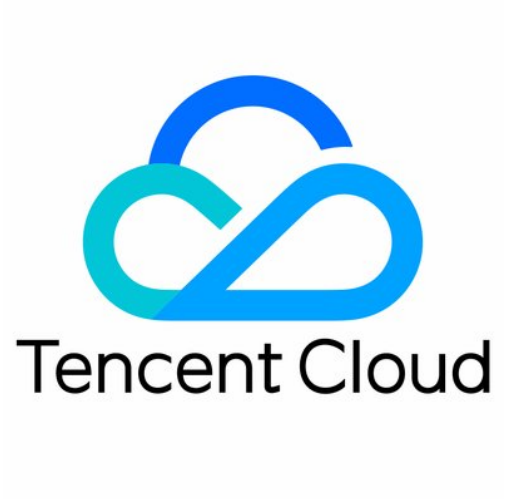
Virtual Private Cloud

FAQs

Product Documentation



Contents

FAQs
General
Concepts and Features

Last updated：2024-01-24 17:22:28

How do you establish communication between different subnets of a VPC?

Each VPC has private network interconnections by default, and you can see a default route in the corresponding route table. This route indicates that all resources in this VPC can connect with each other by private network.
Subnets in different VPCs cannot interconnect over the private network and can communicate with each other only by using Peering Connections or CCN.

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

Yes. A VPC has a region attribute (such as Guangzhou, Beijing, or Seoul), and the subnets in the VPC have an availability zone attribute (such as Guangzhou Zone 1 or Guangzhou Zone 2), so subnets in the same VPC can be deployed in different availability zones in the same region. The availability zone attribute of a CVM inherits that of the subnet it belongs to, and CVMs are purchased under subnets in availability zones. Therefore, it is possible for different CVMs to be deployed in different availability zones.

How do you establish communication between CVMs and databases in different availability zones?

Same VPC: there is interconnection by default. If they do not connect, you can give priority to troubleshooting the firewall policies of the security group and the network ACL.
Different VPCs: you can use Peering Connections or CCN to implement interconnection over the private network between two VPCs.

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

Each VPC can provide up to 65,533 private IP addresses for Tencent Cloud service instances.

What is CIDR?

Classless Inter-Domain Routing (CIDR) implements overall division of the network by using the independent network space address block designated by you together with IP and mask. It eliminates the traditional concepts of class A, class B, and class C address ranges and subnetting and allocates IP address space more effectively. When creating a VPC and subnet, you need to create the corresponding IP range in the form of CIDR block. For example, to create an IP range of `10.0.16.0 - 10.0.17.255`, then:
Convert `10.0.16.0 - 10.0.17.255` to the binary format `00001010.00000000.00010000.00000000 -`

`00001010.00000000.00010001.11111111` , with the first 23 bits being the same. The CIDR block format after conversion is `10.0.16.0/23` .

Why can't I delete the VPC and subnet after manually terminating a TencentDB for Redis instance?

If there is only one TencentDB for Redis instance in the VPC, after the instance is manually terminated, it will be moved to the TencentDB recycle bin. At this time, the Redis resources have not really been released, so the VPC cannot be deleted immediately. You can solve this problem in the following ways:
In the TencentDB recycle bin, **eliminate** the TencentDB for Redis instance and then delete the VPC and subnet.
Wait for the TencentDB for Redis instance to automatically expire in the TencentDB recycle bin and then delete the VPC and subnet.
For more information, please see Terminating Instance.

Why does an application for an EIP fail?

When the EIP quota is exceeded, the application for EIP will fail. For more information on how to view the quota details, please see EIP quota limit.

IP and IP Ranges

Last updated：2024-01-24 17:22:29

What are the limits on the IP ranges of VPCs and subnets?

Tencent Cloud VPC CIDR block supports the use of any one of the following private IP ranges:
`10.0.0.0` - `10.255.255.255` (mask range between 12 and 28)
`172.16.0.0` - `172.31.255.255` (mask range between 12 and 28)
`192.168.0.0` - `192.168.255.255` (mask range between 16 and 28)
The subnet CIDR block must be within or the same as the VPC CIDR block.

Can the IP ranges of VPCs and subnets be modified?

When creating the VPC and subnet, you need to designate their CIDR blocks, and they cannot be changed once they are created.
If you cannot establish a peering connection due to the overlapping of VPC IP ranges, you can try Cloud Connect Network, which has smaller limit granularity (only subnet IP ranges cannot overlap) or migrate the instances to another VPC. For details, see Switching to VPC.

What should be done when a peering connection fails to be established because of a VPC IP range conflict?

When establishing a peering connection, the CIDR blocks of the two VPCs cannot overlap, or else the peering connection will fail to be established.
If the subnet IP ranges of two VPCs that need to communicate do not overlap, then you can use CCN to establish communication. CCN lowers the IP range limits to the subnet level when VPCs communicate.
For example, if the IP ranges of the two VPCs that need to communicate with each other are `10.0.0.0/16`, but the subnets are respectively `10.0.1.0/24` and `10.0.2.0/24`, then you can establish communication using CCN. Refer to CCN Product Documentation.
If your needs are not met by using CCN, then you need to migrate the resources inside the overlapping subnets.
For details on changing the subnet of the CVM, see Changing Instance Subnet.
Migrate the instances within VPC as instructed in Switching to VPC.

Can I modify the private IPs of resources in VPCs (CVMs and databases)?

You can modify the primary private IP of a CVM's primary ENI, but the primary private IP of a secondary ENI cannot be modified. For details, see Modifying Private IP Addresses.
You can modify the private IP of TencentDB instances (such as MySQL instances). See Customizing IP and Port.
The private IP of CLB cannot be modified.

Can I migrate CVMs or databases from one VPC to another?

For now, you can migrate CVM instances and TencentDB for MySQL instances to another VPC under the same account. Other TencentDB instances are not supported.
To migrate CVM instances, see Switching to VPC.
To migrate TencentDB for MySQL instances, see Network Switch.

What do EIPs do?

EIPs are applicable to the following scenarios:
1. **Disaster recovery**
We strongly recommend that you use EIPs for disaster recovery. When one of your CVMs fails to normally provide services, you can unbind the EIP from this CVM and rebind it to a healthy CVM to resume service quickly.
2. **Retaining a specific public IP**
If you need to retain a specific public IP under your account, you can convert it to an EIP, which then can be used to access public networks after being bound to the 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 in other special cases, you can convert the ordinary public IP to an EIP and then bind/unbind the EIP. However, with limited EIP resources available, a quota is imposed on the number of EIPs for each region under a single account. Therefore, reasonable planning and use of EIPs are very important.

How do I keep a public IP unchanged?

If you need to retain a specific public IP under your account, you can convert it to an EIP, which then can be used to access public networks after being bound to the device. This EIP will be retained under your account until it is "released" by you.
For directions, see Converting common public IPs to EIPs.

Can an EIP be converted back to a public IP?

An EIP cannot be converted back to a public IP.

About Classic Network

Last updated：2024-01-24 17:22:29

Note:
Tencent Cloud plans to discontinue the service of classic network. Staring from **January 31, 2022**, no more new resource can be created on the classic network. The classic network service will be officially discontinued on **December 31, 2022**. After that, all classic network-based resources will be migrated to VPC.

Are my resources running on the classic network still available after January 31, 2022?

Your existing resources running on the classic network are still available till **December 31, 2022**. We recommend you migrate your resources to a VPC as soon ass possible. For more information, see Migration Solutions.

Will my business be interrupted during the migration from the classic network to VPC?

This depends on the specific Tencent Cloud service that you use:
For TencentDB services, your services are not affected as dual-IP accessing is supported during migration.
To migration a CVM instance, the instance must be shut down, which will interrupt your service for a shor while. We recommend you migrate during off-peak hours.

Will the billing mode change after the migration from the classic network to VPC?

The billing mode is not changed.

Will the original private IP of the instance change after the migration from the classic network to VPC?

If the IP of the instance is within the target VPC IP range, you can keep the private IP unchanged by specifying it as the new IP. Otherwise, the IP will change.

Will the original public IP of the instance change after the migration from the classic network to VPC?

The original public IP will remain the same.

Can I migrate a CVM from a VPC to the classic network?

No.

What are the differences between the classic network and VPC?

The classic network is a public network resource pool shared by all Tencent Cloud users. The private IPs of all CVMs are assigned by Tencent Cloud. You cannot customize IP ranges or IP addresses.

A VPC is a logically isolated network space in Tencent Cloud. In a VPC, you can customize IP ranges, IP addresses, and routing policies, making it more suitable for use cases requiring custom configurations.

What are the strengths of a VPC?

It allows you to customize IP ranges, IP addresses, and routing policies.
It supports more complex scenarios such as ENI, network ACL, and cross-region communication.
It improves the disaster recovery capability and availability greatly.

Can I migrate a CVM from the classic network to a VPC?

Yes. You can migrate CVMs from the classic network to a VPC. See Switching to VPC.

Note:

This operation cannot be undone. Be sure to carefully read the document before performing this operation.

Which Tencent Cloud products support the classic network?

Classic network servers: CVM, GPU Cloud Computing, and FPGA Cloud Computing.
Classic network database: TencentDB for MySQL, Redis, SQL Server, PostgreSQL, and MongoDB, as well as TDSQL for MySQL.
Classic network load balancer: classic CLB and CLB
Others: classic network CFS and classic network CKafka.

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

You can use Classiclink to establish communication between the classic network and VPCs.
Note the following limitations when using Classiclink:
1. Both the classic network and the VPC to be communicated with are located in the same region (they can be in different availability zones, such as Guangzhou Zone 1 and Guangzhou Zone 2).
2. The VPC CIDR block (IP range) must fall within `10.[0-47].0.0/16` (including subsets). Otherwise, there will be conflicts.
If these conditions are met, you can configure Classiclink on the VPC details page in the console, to associate the classic network-based CVMs with the VPC for interconnection.

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

A terminal connection helps instances in a VPC to communicate with instances in the classic network instances through a private network. It maps classic network instance IPs to VPC IP addresses, allowing you to access the classic network instances through the VPC IPs. Classic network products that support terminal connections include CLB, TencentDB, CMEM, Redis, and MongoDB. However, cross-region or cross-account communication is not supported.

Direction: one-way (the VPC accesses the classic network).

If needed, submit a ticket.

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

No. A VPC supports more features with greater flexibility, and therefore we recommend that you migrate resources from the classic network to a VPC.

How can I disassociate a VPC from a CVM in the classic network?

1. Log in to the VPC console.
2. Click the **ID/Name** of the VPC which needs Classiclink to access the details page.
3. Click **Classiclink**. Select the classic network-based CVM to be disassociated and click **Disassociate**.
4. Click **OK**.

For step-by-step instructions, see Classiclink Overview.

About Product Quota

Last updated：2024-01-24 17:22:28

Is there a quota limit for VPC instances? How many VPCs can be created for each account?

Some VPC resources are subject to usage quota limits. By default, an account can create up to 20 VPCs in each region.

How many EIPs can one account apply for?

Each Tencent Cloud account can apply for up to 20 EIPs in each region.
For each Tencent Cloud account, the daily upper limit of purchase chances defaults to 40 (quota * 2). After an EIP is unbound, each account can be reassigned with public IP addresses for 10 times per day free of charge.
Each bill-by-CVM account has a free daily quota of 10 chances to get public IP addresses after unbinding an EIP. For more information, see the **Quota Limits** section in Elastic IP (EIP).

Connection

Connection to Public Network

Last updated：2024-01-24 17:22:28

How do I apply for a public IP if one was not assigned at the time of purchasing the CVM?

If a public IP was not assigned when you purchased the CVM, then there is no way to re-apply for an ordinary public IP for this CVM. However, the same function can be accomplished using EIPs. For more information on how to use this, please see Applying for EIPs.

An EIP is a type of public IP that is fixed to a specific public IP address in a certain region. Unlike an ordinary public IP, it is bound to your account. In other words, you can bind and unbind an EIP with different CVMs as required (only one can be bound at a time).

Due to the special nature of an EIP, if you apply for an EIP but do not bind it to an instance, IP resource fees will be incurred. For details, please see EIP Billing.

How can an instance (CVM or database) access the public network without a public IP address?

An instance without a public IP can apply for an EIP (see the previous question) or can access the public network through NAT gateway.

NAT gateway can provide SNAT and DNAT features for CVM instances in VPCs. If you have multiple instances and want them to access the public network through the same public IP, you can use a NAT gateway.

Can the public IP of a CVM be changed?

Yes.

If your CVM instance uses the public IP assigned at the time of purchase, please see Changing Public IP Addresses.

If your CVM instance is bound to an EIP, you need to unbind the EIP first and then apply for another EIP or bind an existing EIP.

Note:

We recommend you immediately release the EIP after it is converted from a public IP. Otherwise, the EIP that is not bound to an instance will incur IP resource fees.

Can a previously used public IP be recovered? Can a specific EIP be applied for?

You can recover public IPs that you have previously used and are not currently assigned to other users. Recovered public IPs are all EIPs. For more information, please see Retrieve the public network IP address.

Can an increased quota be requested after the number of EIPs reaches the top limit?

Due to the limited EIP resources, you can apply for only 20 ones per account per region, and you cannot request an increased quota. CVM instances without public IPs can use NAT gateways and other methods to access the public network.

How does a CVM access the public network if it has a public IP or EIP and its subnet is also associated with a NAT gateway?

If a CVM has a public IP or EIP and its subnet is also associated with a NAT gateway (meaning the route table specifies that the next hop for the traffic of this subnet to access the public network is a NAT gateway), then the default setting is for all the traffic of this CVM to access the public network through the NAT gateway.
If you need to modify the priority so that the traffic from the CVM instance to the public network passes the public IP, please see Adjusting the Priorities of NAT Gateways and EIPs.

When a CVM instance accesses the public network through public gateway or NAT gateway, will the network fee be charged twice?

No, the network fee will only be charged once. When accessing the public network through public gateway or NAT gateway, only the corresponding public gateway network fee or NAT gateway network fee will be charged.

Inter-VPC Communication

Last updated：2024-01-24 17:22:29

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：2024-01-24 17:22:28

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：2024-01-24 17:22:28

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

Last updated：2024-01-24 17:22:28

Port-related FAQs

Which ports should I open before logging in to an instance?

Generally, you need to open port 22 for a Linux instance, or port 3389 for a Windows instance. For more information, see Application Cases of Security Groups.

Why should I open a port, and how?

You should open the port in the security group to use related services.

For example, if you want to access web pages using port 8080, you should open this port in the security group.

Steps to open a port:

1. Log in to the security group console, and click the ID/name of the security group bound with this instance to enter its details page.
2. Select **Inbound/Outbound rule** and click **Add a Rule**.
3. Enter your IP address (range) and port to be opened, and then select **Allow**.

For details of directions, see Adding a Security Group Rule.

My business is not accessible after I modified the port.

After modifying the service port, you need to open the corresponding port in the security group.

Which ports are not supported by Tencent Cloud?

The following ports are not allowed as they have security risks and are very likely to be blocked by ISPs.

Protocol	Unsupported ports
TCP	42, 135, 137, 138, 139, 445, 593, 1025, 1434, 1068, 3127, 3128, 3129, 3130, 4444, 5554, 5800, 5900 and 9996
UDP	1026, 1027, 1434, 1068, 5554, 9996, 1028, 1433 and 135 - 139

I cannot connect to an external address through TCP port 25.

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

Each account supports unblocking the CVMs 5 times. Note that pay-as-you-go CVMs are not supported.
For more information about ports, see Common Server Ports.

Security Group-related FAQs

What if an improper security group is selected? How can this be fixed?

Risks

Fail to remotely connect to a Linux instance (SSH) or remotely log in to desktop Windows instance.
Fail to ping the public/private IP of the CVMs in this security group.
Fail to access over HTTP the web services exposed by the CVM instance in this security group.
You may fail to access the Internet with the instance under this security group.

Solutions

In case any of the above problems happens, you can go to "Security Group Management" in the console and reset the rule for the security group, for example, to "only bind all-pass security groups by default".
For details of setting security group rules, see Security Group - Security Group Rules.

What do security group direction and policy mean?

The security group policy works in the directions of outbound and inbound. The former is to filter the outbound traffic of the CVM, and the latter is to filter the inbound traffic of the CVM.
Security group policies include **Allow** and **Refuse**.

What is the order in which security group policies to go into effect?

The order that security group policies go into effect is from top to bottom. Traffic passes through the security group's matching sequence from top to bottom, and the policy goes into effect as soon as there is a successful match.

I opened a port in the security group, but the CVM is still not accessible.

Check whether the CVM is bound to with another higher-priority security group, which reject this port.
The port is blocked by the network ACL or firewall.
The service corresponding to the port is not started.
The port is not open in the system firewall.

How come an IP that is not allowed in the security group can still access the CVM?

Possible reasons:
The CVM is bound to multiple security groups, and the IP is allowed by another security group.
This IP address belongs to an approved Tencent Cloud public service.

Can iptables be used along with security groups?

Yes. Security groups and iptables can be used at the same time. 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.

I have returned all CVMs associated with the security group. But I still cannot delete the security group.

Besides CVMs, a security group can also be bound with CLB, ENI and cloud database instances. Please make sure that all resources bound with the security group have been disassociated.

When I clone a security group to another region, can the source and destination security group share the same name?

Yes.

Can I clone a security group to another project or region using an API?

Yes. For details, see CloneSecurityGroup.

When I clone a security group to another project or region, will the CVMs associated with the security groups also be cloned?

No. Only the inbound and outbound rules of the security group are cloned. You need to associate CVMs again after cloning.