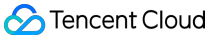
Virtual Private Cloud

FAQs

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

FAQs
General
Concepts and Features

Last updated: 2024-01-12 15:04:43

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?

CIDR (Classless Inter-Domain Routing) is a method of allocating IP addresses and routing Internet Protocol packets. It eliminates the traditional concepts of Class A, Class B, and Class C addresses and subnet divisions, allowing for more efficient allocation of IP address space. When creating a VPC and its subnets, you need to specify the address range in CIDR format. For example, to create a range of `10.0.16.0 - 10.0.17.255`:
`10.0.16.0 - 10.0.17.255` in binary is `00001010.00000000.00010000.00000000 - 00001010.00000000.00010001.11111111`. The first 23 bits are the same, so the CIDR format 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, see Terminating Instances.

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: 2024-01-12 15:04:49

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: 12 - 28)
- `172.16.0.0` – `172.31.255.255` (mask: 12 - 28)
- `192.168.0.0` – `192.168.255.255` (mask: 16 - 28)

The subnet CIDR block must be within or the same as the VPC CIDR block.

Can I modify the IP ranges of VPCs and subnets?

- No. The IP ranges of VPCs and subnets cannot be modified after the creation.
- If you cannot establish a peering connection due to the overlapping of VPC IP ranges, you can try Cloud Connect Network, whose IP conflict limit is set at the subnet level. You can also 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?

In a peering connection, the CIDR blocks of the two peers cannot overlap.

- In this case, you can try CCN. CCN lowers the IP range limits to the subnet level, which means you can connect two subnets whose IP ranges do not overlap, regardless of the related VPC IP range.
  For example, if the IP ranges of the two VPCs are both `10.0.0.0/16`, and the subnets are `10.0.1.0/24` and `10.0.2.0/24` respectively, you can establish communication via CCN. For more information, see Cloud Connect Network.
- If the subnets are overlap, you need to migrate the resources in 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)?

- The primary private IP of the main ENI of a Cloud Virtual Machine can be modified, while the primary private IP of the auxiliary NIC cannot be modified. For more information, please 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**
   When one of your CVMs fails, 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**
   To retain a specific public IP under your account, you can convert it to an EIP, and bind it with a resource to access the public network. This EIP is retained under your account unless you release it.
3. **Other cases**
   When you need to change the public IP of a resource, you can convert the public IP to an EIP and then bind/unbind the EIP. Note that the number of EIPs owned by an account is limited per region.

How can I retain a public IP?

To retain a specific public IP under your account, you can convert it to an EIP, and bind it with a resource to access the public network. This EIP is retained under your account unless you release it.
For details, see Converting Public IPs to EIPs.

Can I convert an EIP to a public IP?

No. An EIP cannot be converted back to a public IP.

About Classic Network

Last updated: 2024-01-12 15:05:34

> **Note**
> Tencent Cloud has stopped supporting the creation of any new resources in the classic network on March 31, 2022, and has officially discontinued the service of classic network since December 31, 2022. The corresponding services are provided by Virtual Private Cloud (VPC) products.

Are my resources running in the classic network still available after March 31, 2022?

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

Will my services 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 short while. We recommend you migrate during off-peak hours.
- CLB doesn't support direct migration. You can rebuild instances with the same configuration and gradually migrate the applications.

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 private 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?

Both classic network and VPC are cyberspaces in the cloud. Their differences are as follows:

- The classic network is a public network resource pool shared by all Tencent Cloud users. The private IPs of all CVM instances 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. For details, 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 are located in the same region (they can be in different AZs, 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?

The procedure for disassociation is as follows:

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: 2024-01-12 15:05:52

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

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

How many EIPs can be applied for under an account?

- Up to 20 EIPs can be applied for under a Tencent Cloud account in each region.
- Each Tencent Cloud account can apply for Elastic IPs in each region up to a daily quota of twice the allocated amount (default is 40 times). When unbinding an EIP, each account can reallocate public IPs for free up to 10 times per day.
- Each bill-by-CVM account has a free daily quota of 10 chances to get public IPs after unbinding an EIP. For more information, see EIP quota limits.

Connection
Connection to Public Network

Last updated: 2024-01-12 15:06:00

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 feature can be accomplished using EIPs. For more information, 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?

Instances without a public IP can apply for an EIP (refer to the previous question) or access the public network through a NAT gateway.
NAT Gateway provides SNAT and DNAT features for CVM instances in VPCs. If you have multiple CVM instances that need to access the public network through a single 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 an EIP is bound to your CVM instance, you need to unbind the EIP first and then apply for another EIP or bind an existing EIP.

> **Note**
> After converting a regular public IP to an Elastic Public IP, it is recommended to release it immediately. Otherwise, an unbound EIP will incur a certain IP resource fee.

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, see Retrieving Public Network IPs.

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 EIPs per region under an account, 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 Priorities of NAT Gateways and EIPs.

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

No, only one network fee will be charged. When accessing the public network through a public network gateway or NAT gateway, the network fee for the public network gateway or NAT gateway will be charged.

Inter-VPC Communication

Last updated: 2024-01-12 15:06:06

How do CVMs or databases interconnect over a private network?

The private network communication of both CVMs and databases is implemented by private IPs. See below to learn how they are connected in different scenarios:

Scenario	How to connect
Cross-region	CVMs/databases in different regions are in different VPCs. You can connect them via Peering Connections or CCN instances. Cross-account connection is supported.
Cross-AZ	Intra-VPC: Resources in the same VPC are interconnected by default. Cross-VPC: You can connect them via Peering Connections or CCN instances. Cross-account connection is supported.
Cross-VPC	You can connect them via Peering Connections or CCN instances. Cross-account connection is supported.
Cross-subnet	Intra-VPC: Resources in the same VPC are interconnected by default. Cross-VPC: You can connect them via Peering Connections or CCN instances. Cross-account connection is supported.
Cross-account	You can connect resources under different accounts via Peering Connections or CCN instances. Cross-region connection is supported.

Notes

- For the cross-account connection of VPCs via Peering Connections or CCN:
  - If the resources of both peers are owned by the root accounts, enter the root account of the other user when you create the cross-account peering connection or CCN instance.
  - If you are using a sub-account, get the permission to create peering connection or CCN instances from the root account.
- Resources on different subnets under the same VPC are interconnected by default, regardless of the AZ. If they are not interconnected, please first check the firewall policies of the security group and network ACL.

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

In a peering connection, the CIDR blocks of the two peers cannot overlap.

- In this case, you can try CCN. CCN lowers the IP range limits to the subnet level, which means you can connect two subnets whose IP ranges do not overlap, regardless of the related VPC IP range.
  For example, if the IP ranges of the two VPCs are both `10.0.0.0/16`, and the subnets are `10.0.1.0/24` and `10.0.2.0/24` respectively, you can establish communication via CCN. For more information, see Cloud Connect Network.
- If the subnets are overlap, you need to migrate the resources in the overlapping subnets.
  - For details on changing the subnets of CVMs, see Changing Subnets of Instances.
  - For details on migrating instances between VPCs, see Switching VPCs.

VPC1 is connected to VPC2 and VPC3 via peering connections separately. Can VPC2 and VPC3 communicate with each other?

No. A peering connection only allows the communication of VPCs on the two peers. This interconnection relationship is not transitive. This means that when a peering connection is established between VPC1 and VPC2 while there is also a peering connection established between VPC1 and VPC3, there can be no interconnection of traffic between VPC2 and VPC3.

Classiclink-Related

Last updated: 2024-01-12 15:06:11

What is Classiclink?

Classiclink refers to associating Cloud Virtual Machines (CVMs) in the classic network with a specified Virtual Private Cloud (VPC), enabling communication between classic network-based CVMs and VPC-based CVMs, databases, and other cloud services. For more information, see Managing Classic Network.

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 are located in the same region (they can be in different AZs, such as Guangzhou Zone 1 and Guangzhou Zone 2).
2. The VPC's CIDR block (IP range) must be within `10.0.0.0/16 - 10.47.0.0/16` (including subsets) to avoid 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 through a private network. It maps classic network instance IPs to VPC IPs, 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, please 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.

Security
VPC Security Related

Last updated: 2024-01-12 15:06:17

How do you ensure the security of CVMs in VPCs?

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

- Security group: It provides network traffic control at the CVM instance level. Traffic that is not allowed to be in or out of the instance is automatically rejected.
- Network ACL: It provides network traffic control at the subnet level.

Port and Security Group

Last updated: 2024-01-12 15:06:23

Port

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 VPC console and select Security Group in the left sidebar. Click the ID/name of the security group bound with the instance to enter its details page.
2. Select "Inbound rules" or "Outbound rules", and click **Add rule**.
3. Enter your IP address (range) and information of the port you want to open, then select "Allow".
   For details, see Adding Security Group Rules.

Why is my application not accessible after I modified the port?

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

What 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、9996
UDP	1026、1027、1434、1068、5554、9996、1028、1433、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, see Common Server Ports.

Security Group

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.
  - The CVM instance under this security group may fail to access internet services.
- **Solutions**
  - If any of the aforementioned problems occur, you can go to "Security Group" in the console and modify the security group rule. For example, you can change the rule to "bind only all-ports-open 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 **Reject**.

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. When traffic passes through the security group, policy matching is performed from top to bottom. A policy takes effect once matching is successful.

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

- Check whether the CVM is bound 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?

There are a few possible reasons for this:

- 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 simultaneously. 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 can't the security groups be deleted even though all the CVMs have been returned?

Besides CVMs, a security group can also be bound with CLB, ENI and TencentDB 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, cloning a security group across different regions will only clone the entry and exit rules of the original security group. The CVM needs to be associated separately.