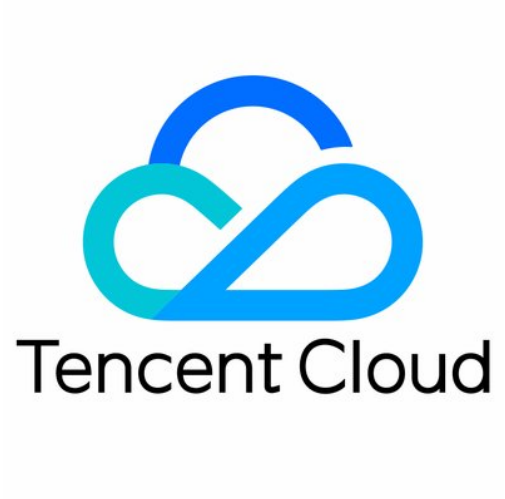
Virtual Private Cloud

FAQ

Product Documentation



Contents

FAQ
Basic

Last updated：2019-07-30 18:21:11

1. What does VPC (Virtual Private Cloud) consist of?

Tencent Cloud VPC consists of various services which should appear very similar to customers who own a VPC:
1) Software Defined Network: You can customize your VPC network segment, subnet segment and routing policy:

- **Virtual Private Cloud (VPC)** is a logically separated virtual network in Tencent Cloud. Define the IP space of the VPC from selected range.
- **Subnet** is a segment within the IP range of the VPC, where you can place groups of isolated resources.
- **Router** consists of a series of routing policies, which are used to define the traffic direction of each subnet within the VPC.

2) Internet Connection: There are three types of flexible, high-performance Internet connection methods:

- **NAT Gateway** is a highly available Network Address Translation (NAT) service, which helps resources in private subnets access the Internet.
- **Elastic IP** (EIP) is an independent public IP address you can apply for, which is used for public network access. You can dynamically bind/unbind this IP to or from instances (such as CVMs and NAT gateways) and use it to avoid instance failures.
- **Public Network Gateway** is a type of CVM which is able to forward the traffic between Internet and VPCs. A CVM can access the Internet via public network gateway if it needs to do so, but does not have a public IP.

3) Deploy Hybrid Cloud Connect your data center and your VPC.

- **VPN Connection** is a method you can use to connect your IDC and VPC through public network encrypted tunnel. It consists of three components: VPN gateway, peering gateway and VPN tunnel.
- **Direct Connection** provides a fast approach to connect Tencent Cloud with local data centers. You can simply use one physical direct connection line to access Tencent Cloud computing resources in multiple regions in one go. It consists of three components: physical direct connection, direct connection tunnel and direct connection gateway:

4) Resource Interconnection between Clouds is used to communicate with resources from other VPCs and basic networks.

- **Peering Connection**: This service is used to connect two VPCs. You can use it to connect the traffic between two VPCs of different accounts or regions, after which the resources (such as CVMs and cloud databases) from the two ends will be able to access each other
- **Basic Network Interconnection**: This service is used to associate CVMs in the basic network with specified VPCs, thus allowing the CVMs and VPCs in the basic network to communicate with each other

5) Security Control

- **Security Group**: is a stateful packet filtering virtual firewall, which is used to control the outbound/inbound traffic of a single or multiple CVMs (accuracy up to protocol and port dimensions).
- **Network Access Control List (ACL)** is an optional stateless packet filtering virtual firewall (of subnet level), which is used to control the inbound/outbound data traffic that goes through the subnet (accuracy up to protocol and port dimensions).

2. How to start using VPC?

You can start using VPC either from the Tencent Cloud Console, or by using cloud APIs.

- **Console** Quick Guide
- **API** Quick Guide

3. Is the VPC able to communicate with basic network/public network/other VPCs (of different accounts and regions)/my data center?

Yes. The following table lists your demands and their corresponding features:

User Demand	Corresponding VPC Feature
Communication between VPC and CVM within the basic network	Basic Network Interconnection
Access public network	Elastic IP / NAT Gateway(High performance)/ Public Network Gateway

User Demand	Corresponding VPC Feature
Other VPCs	Peering Connection(Cross-region and cross-account are supported)
My data center	VPN Connection / Direct Connect

4. How many VPCs, subnets, routing tables, public network gateways, NAT gateways, peering connections, VPN gateways, VPN tunnels, network ACLs can I create, respectively?

View Detailed Resource Quota in the VPC, please submit a ticket to apply for a higher quota if needed.

5. What's the difference between basic network and VPC?

VPC is able to achieve all functions that can be provided by the basic network, without additional fee. VPC is able to satisfy more demands for network customization. Please Refer to Details about Differences between Basic Network and VPC.

6. I have a VPC. How do I configure it to allow only some of the CVMs in it to access the public network through the gateway?

Place the CVMs that need to access the public network into a certain subnet, then configure routing policy on the routing table which is bound to this subnet and direct data packets to access via the gateway if their destination is the public network. Detailed procedure is shown below:

1) **Create Subnet** and place the CVMs that need to access the public network into this subnet: purchase CVMs from the Subnet Console / choose this subnet from the Purchased Network Configuration section of the CVM Introduction Page.
2) **Purchase the corresponding gateway equipment**. There are two types of gateway equipments in Tencent Cloud VPC that can access the public network: NAT Gateway and Public Network Gateway. Click to View Their Differences. You may purchase the corresponding gateway equipment according to your

business needs. Instruction on how to allow CVMs without Public IPs to Access the Public Network via Public Network Gateway / instruction on how to Use NAT Gateway to Access the Internet.

7. I have a VPC, can I create CVMs in different availability zones and how do I do that? Such as creating CVMs in both Guangzhou Zone 2 and Guangzhou Zone 3.

Yes. There are two preconditions:

1) You can only create CVMs within availability zones of the region to which the VPC belongs. For example, if your CVM belongs to the region Guangzhou, you can create CVMs in Guangzhou Zone 2 and Zone 3, but you cannot create CVMs in Guangzhou Zone 2 and Beijing Zone 1 at the same time, in this VPC. Click to View Detailed Distribution of Regions and Availability Zones
2) You must create a subnet in the availability zone before you can create CVMs in this availability zone.

The detailed procedure regarding how to create CVMs in different availability zones is shown below:

1) Create Subnets in **different** availability zones under this VPC.
2) Create CVM. Purchase CVMs from the Subnet Console / choose subnets of **different availability zones** from the Purchased Network Configuration section of the CVM Introduction Page.

8. Can I modify the private IP of cloud virtual machine (CVM)/private cloud load balancer (LB)/cloud database (CDB)?

You can modify the primary private IP of the CVM's primary NIC. You cannot modify the primary private IP of secondary NIC. Click to View Instructions.
You cannot modify private IP of private cloud load balancer (LB) or cloud database (CDB).

Pricing and Billing

Last updated：2018-10-18 16:12:32

1. How will I be charged for my use of VPC/subnet/routing table/NAT gateway/peering connection/public network gateway/VPN connection/network ACL?

Paid services include: cross-region peering connection, public network gateway, NAT gateway, and VPN gateway. These services are chargeable because they have CVMs or license involved in their costs. Click to view the billing details.
Except the paid services mentioned above, the other services are free.

2. Are there additional network charges for services (CVMs, databases, etc.) within a VPC?

No. Network fee is only charged once.

- For accesses to the Internet through **public network gateways and NAT gateways**, a network fee for **public network gateways and NAT gateways** is charged.
- For accesses to services in other VPCs through **cross-region peering connections**, a network fee for **peering connections** is charged.
- For accesses to other services through **VPN connections**, a fee for **VPN gateways** is charged.

IP and Routing Table

Last updated：2018-10-18 16:12:26

1. What IP address ranges can be used in VPCs and subnets?

- VPC supports private IPs within three network segments: `10.a.0.0/8` (a ranges from 0 to 255), `172.b.0.0/16` (b ranges from 0 to 31), and `192.168.0.0/16`. CIDR of VPC can be the above three network segments, or a part of a network segment.
- The number of IPs contained in a network block = `2^(32-mask)`. So the `10.1.0.0/16` network block may contain up to 65,536 IP addresses.

2. What is CIDR, and what should be paid attention to when assigning a CIDR for a VPC?

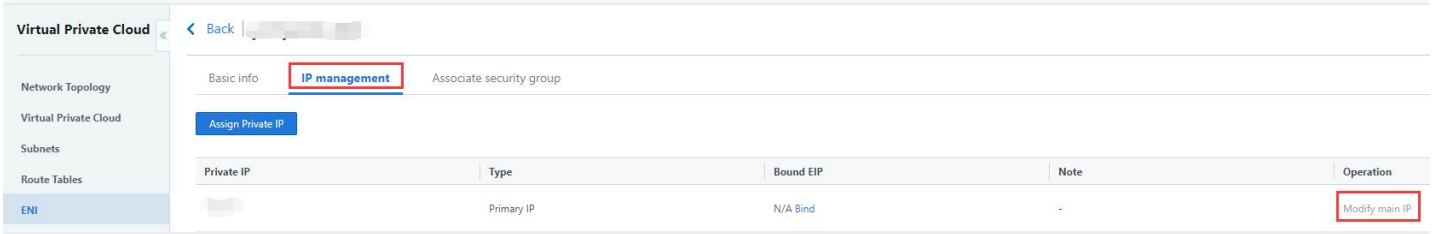
CIDR (Classless Inter-Domain Routing) is a user-specified independent network space address block, which achieves the division of the whole network by combining IP and mask. Click to view what should be paid attention to when assigning a CIDR for a VPC.

3. In the routing table, the access to the public network within a subnet is set to be made through NAT gateways, but the CVMs in the subnet are configured with elastic IPs. So whether these CVMs access the public network through NAT gateways or elastic IPs?

Through the NAT gateways. Click to view routing rule priority.

4. How to modify the private IP of a CVM?

The primary private IP of the primary ENI of a CVM can be modified, while the primary private IP of the secondary ENI cannot be modified. The steps are as follows:
(1) Enter the CVM Console, click the CVM in the left navigation bar to enter the CVM list page.
(2) Click the CVM ID to enter the CVM details page, and click the top tab: ENI.
(3) Click to modify the main IP.
(4) Input the new IP and save it.



You can also modify the primary private IP on the ENI details page. Click to view details.

Connections
FAQ for Internet Connection

Last updated：2018-10-18 16:12:20

1. How do instances without public IP addresses (CVMs, databases) access the Internet?

They can access the Internet through NAT gateways/public network gateways.

- NAT gateways. By creating NAT gateways and configuring the routing table associated with relevant subnet, the instances within the subnet can access the Internet. Click to view the operation instructions.
- Public network gateways. CVMs without public IPs can access the Internet via public network gateways located in different subnets.

2. What is the difference between public network gateways and CVMs with public IPs?

A public IP coming with a CVM is equivalent to an additional public network NIC, enabling the CVM to freely access the Internet.

3. Why cannot a routing policy be forwarded after the policy is configured for a subnet and directed to a public network gateway?

When the CVM that accesses the Internet through a public network gateway and the public network gateway are in the same subnet, the forwarding function will fail. Please arrange the CVM and the public network gateway in different subnets.

4. In the routing table, the access to the public network within a subnet is set to be made through NAT gateways, but the CVMs in the subnet are configured with elastic IPs. So

whether these CVMs access the public network through NAT gateways or elastic IPs?

Through the **NAT gateways**. Click to view routing rule priority.

FAQ for VPN Connection

Last updated：2019-07-30 18:24:45

1. Can a VPC connect to multiple IDCs through VPN connections?

Yes. Currently, a VPC can establish VPN gateways and set up multiple VPN tunnels on each VPN gateway. Each VPN tunnel can connect with one local IDC.

2. Can the communication between two VPCs be achieved via VPN connections?

Yes. You need to purchase VPN gateways, and configure VPN tunnels and peer gateways in two VPCs. Since the configuration is complicated, we recommend you use a peering connection. Peering connection uses Tencent Backbone Network to connect two VPCs, which can ensure the communication quality.

3. How is the network quality between the VPC and the IDC connected through the VPN ensured?

- The communication between the VPC and the IDC is made through a public network, which therefore depends on the quality of the public network. Latency, packet loss, and jitter are all possible. If you need more stable communication quality, we recommend that you use the Direct Connect service.
- The VPN backend will monitor the network quality throughout the day, including keepalive and network latency. If there are network anomalies, it will inform the O&M personnel to deal with them in a timely manner. You can also monitor the traffic status of VPN gateways and tunnels in real time in the console. Contact us if you find anomalies.

FAQ for Classiclink

Last updated：2018-10-18 16:12:08

1. Is the CVM in a basic network interconnecting with a VPC a part of VPC?

No. No VPC private IP address will be assigned to the CVM for interconnection in a basic network.

2. Is Classiclink available to all VPCs?

Classiclink is only supported for VPCs within the network segment of `10.[0~47].0.0/16`.

3. Can the traffic from the CVM interconnecting with a VPC via a basic network go through the VPC through network perimeter services (peering connection, public network gateway, NAT gateway, VPN gateway, Direct Connect gateway)?

No.

4. Will the CVM that interconnects with a VPC via a basic network be assigned to a new private IP address?

No.

FAQ for Peering Connection

Last updated：2018-10-18 16:12:03

1. Can a peering connection be established between two VPCs with overlapped IP addresses?

No. The IP ranges of the VPCs at the two sides of the peering connection must not overlap. Click to view the usage constraints for peering connections.

2. If a peering connection is established between VPC A and VPC B, and another peering connection is established between VPC B and VPC C, does it mean VPC A and VPC C are connected?

No. Peering connections are non-transitive.

3. Is there a bandwidth limit for peering connections?

A bandwidth limit can be set when a **cross-region peering connection** is created using an API. Bandwidth limit for the console will be supported in the near future.
For the **peering connection within the same region**, there is no bandwidth fee and no bandwidth limit.

4. If I delete the peering connection on my side, can the other side access my VPC?

No. Either of the two sides of the peering connection can interrupt the peering connection at any time.

Security

Last updated：2018-10-18 16:13:24

1. How to ensure the security of CVMs running in a VPC?

A VPC is a network environment that is logically isolated, and security groups and network ACLs can be used for traffic control:

- **Security groups** can be used to specify the inbound and outbound network traffic that is allowed to enter or exit each CVM. Traffic which is not explicitly allowed to or from an instance is automatically denied.
- **Access Control List (ACL)** can also allow or deny the network traffic entering or exiting each subnet.

2. What are the differences between security groups and network ACLs in VPCs?

Click to view the differences between security groups and network ACLs.