

Virtual Private Cloud Private Network and Subnet Product Documentation



Copyright Notice

©2013–2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Private Network and Subnet

Last updated : 2019-09-24 17:19:00

Virtual Private Cloud (VPC)

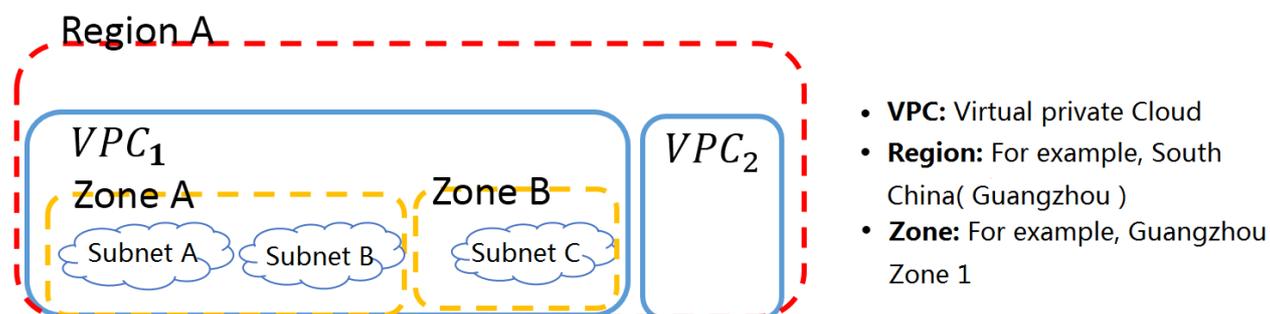
Virtual Private Cloud allows you to build an independent network space on Tencent Cloud, similar to the traditional network you hosted in a data center. However, what hosted in Tencent Cloud VPC are your service resources on Tencent Cloud, which include: [Cloud Virtual Machine](#), [Cloud Load Balance](#), [Cloud Database](#) and other resources of cloud services on your Tencent Cloud. Tencent Cloud VPC can provide you with the following features:

- Customize network segmentation, IP address and routing policy via the console and APIs
- Access Internet flexibly via [Elastic IP](#), [NAT Gateway](#) and Public Network Gateway
- Connect VPC with your data center via [VPN](#) and Direct Connect
- "One server covering the globe" and disaster recovery at "two regions, three centers" can be achieved via [Peering Connection](#)
- Through basic network interconnection, hosts in basic network and VPC can communicate via private network
- The [Security Group](#) and [Network ACL](#) can satisfy your network security requirement in a multi-dimensional and all-round manner.

When creating a VPC, the user needs to specify an IP address group for VPC in the form of a classless inter-domain routing (CIDR) block (e.g, 10.0.0.0/16). VPC is region related. For example VPC A in southern China (Guangzhou), users cannot create a cross-region VPC.

Subnet

Subnet is the IP address block within VPC, and all cloud resources in the VPC must be deployed in subnet. Subnet is availability zone related, as shown in the following figure. After creating a VPC, you can add a subnet to each availability zone under the region to which the VPC belongs. Availability zone is designed to isolate failures from other availability zone. By starting an instance in an independent availability zone, users can protect their applications from being affected by the failures occurring in a single point.



VPC IP Address

You can specify the CIDR (Classless Inter-Domain Routing) to implement the overall IP division of the VPC and subnets. IP address used in the Tencent Cloud VPC is divided into three categories:

- **Private IP:** It is the IP address that must be assigned to an instance within VPC for communication between instances in VPC, but it cannot be used for Internet communication.
- **Public IP:** It is the IP address used for Internet access and can be used for communication between instances and the Internet or other Tencent Cloud resources (such as CDB) that have common terminal nodes.
- **Elastic IP (EIP):** It is the public IP that can be requested separately. Dynamic binding and unbinding it with CVM/NAT gateway instances is supported.

CIDR

CIDR (Classless Inter-Domain Routing) is a user-specified independent network space address block, which enables the overall division of the network by combining IP with mask. Take `10.1.0.0/16` as an example, the left side of the slash is the IP of the network block, and the right side of the slash is the mask of the network block. You can adjust the size of the network block by setting the value of the mask. Number of IPs that the network block contains equals $2^{(32-\text{mask})}$, so the `10.1.0.0/16` network block contains up to 65,536 IP addresses.

When planning CIDR, it is important to note:

- You must specify CIDR when VPC is created and it cannot be modified later.
- CIDR of a subnet must be part of the CIDR of the VPC to which the subnet belongs.
- Currently, VPC supports private IPs of three network segments: `10.a.0.0/8` ("a" is a number in range of 0 to 255), `172.b.0.0/16` ("b" is a number in range of 0 to 31) and `192.168.0.0/16`. VPC CIDR can be one of the above three network segments, or part of a network segment.
- At present, VPC CIDR supports mask between `/28` and `/16`, that is, VPC space contains at least 16 and at most 65536 IP addresses.
- For VPCs that have established peering connection, their CIDRs cannot overlap.
- The basic network interconnection service only supports VPCs of `10.[0~47].0.0/16` and its subsets.
- Each SPD policy for a VPN connection corresponds to a local network segment (VPC segment) and a peer network segment (your IDC network segment), and both network segments cannot overlap.

Region

Data centers hosted by Tencent Cloud are distributed in different locations worldwide, which are divided into regions and availability zones.

When creating a VPC, you need to select a region. When creating a subnet, you need to select an availability zone where its VPC locates.

Region is named as "coverage + city where data center locates". The first half represents the coverage capability of the data center, and the second half indicates the city where the data center is located or near to. Tencent Cloud currently offers the following regions for your option:

- Mainland China: South China (Guangzhou), East China (Shanghai), East China (Shanghai Finance), North China (Beijing).
- Overseas: China (Hong Kong) , North America (Toronto) and Southeast Asia (Singapore).

What you need to know about regions:

- When you purchase cloud services, it is recommended to choose the region that is closest to your customers to minimize the access latency.
- The cloud products in the same region interconnect through private network (cloud resources of different users are isolated by default).
- Cloud services in different regions cannot interconnect over private network by default, e.g., cross-region mutual access of CVM over private network, or cross-region access to the cloud database and cloud cache Memcached are not supported.
- When binding Cloud Load Balance to a server, only CVM in the local region is allowed.
- Supported Regions for Tencent Cloud VPC service are shown in the table below. Blank means "supported" and X means "not supported". Before deploying your application, make sure you can create the required resources in that region or in the availability zones.

| Region | VPC (subnet) | Regional Peering Connection | Cross-region Peering Connection | Basic Network Interconnection | NAT Gateway | Public Network Gateway | VPN Gateway | Direct Connect Gateway |
|--------------------------------|--------------|-----------------------------|---------------------------------|-------------------------------|-------------|------------------------|-------------|------------------------|
| South China (Guangzhou) | | | | | | | | |
| South China (Guangzhou Open) | | | × | | × | | × | × |
| South China (Shenzhen Finance) | | | | | | | | |
| East China (Shanghai) | | | | | | | | |
| East China (Shanghai Finance) | | | | | | | | |
| North China (Beijing) | | | | | | | | |
| China (Hong Kong) | | | - | | | | | |
| South East Asia (Singapore) | | | - | | | | | × |

| Region | VPC (subnet) | Regional Peering Connection | Cross-region Peering Connection | Basic Network Interconnection | NAT Gateway | Public Network Gateway | VPN Gateway | Direct Connect Gateway |
|-------------------------|--------------|-----------------------------|---------------------------------|-------------------------------|-------------|------------------------|-------------|------------------------|
| North America (Toronto) | | | - | | | | | × |

Note:

- Blank means "supported"; X means "not supported".
- For more questions, please consult service department.

Availability Zone

Availability zones are physical zones under the same region but each with independent power and network (it is usually a physical data center), named as "city + No.". For example, there are two availability zones under South China (Guangzhou), i.e., Guangzhou Zone 1 and Guangzhou Zone 2, as shown below.

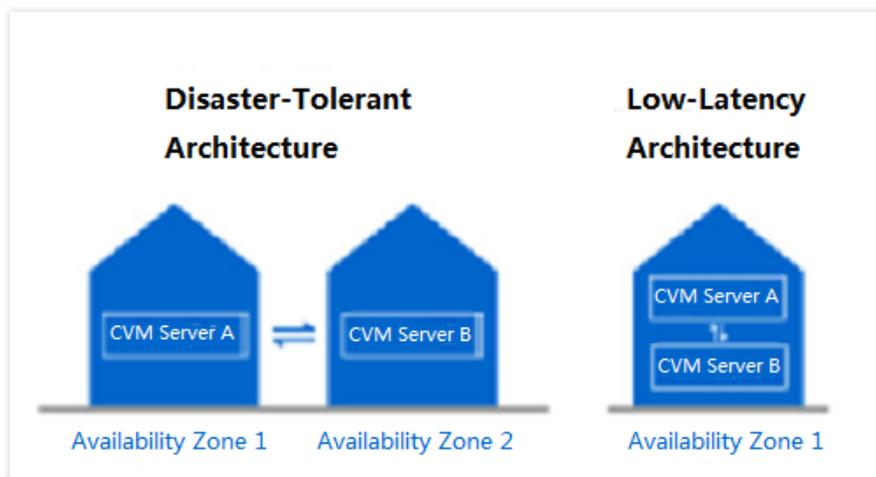


The availability zone is designed to ensure that failure of any zone can be isolated (except for large-scale disaster or major power failure) without spreading to and affecting other zones so that users' online services will not interrupt. For large-scale applications, disaster recovery is an important guarantee for service availability, and multiple data center deployment is a common practice of disaster recovery; for ordinary users, the multiple data center deployment is a luxury investment, but Tencent Cloud's multiple availability zones is designed as such that each customer can implement disaster recovery deployment across multiple data centers while not incurring additional cost and the complexity of operation and maintenance.

For example, if you have deployed the same service in Zone 1 and Zone 2, the power failure in Zone 1 will not affect Zone 2, which provides you with stable and highly available services, as shown below.



- **Disaster recovery architecture:** When your service needs higher availability, multiple data center deployment across the availability zones is to ensure low latency while providing users with high disaster recovery capacity. For example: You can purchase CVM in Guangzhou Zone 1 and Zone 2, respectively, and failure that happens in one zone will not affect the normal operation of cloud services in the other zone.
- **Low latency architecture:** If the application is more focused on low network latency, you can deploy the services in the same availability zone.



Usage Constraints

What you need to be aware of about VPC and subnets:

- VPC is region related and can be deployed between multiple availability zones in the same region.
- After a VPC is created, you cannot change its size. You can delete the current VPC and create a new one as necessary.
- VPC does not support multicast or broadcast.
- A VPC may contain multiple subnets. Network blocks of each subnet are a subset of a VPC CIDR, and CIDR network blocks of multiple subnets cannot overlap.
- The subnet is availability zone related and cannot be deployed across one more availability zones. The availability zone of the subnet is limited to the one in its VPC region. The CVMs in the subnet should be in the same availability zone as the subnet.

- Creation of new VPC and subnet require you to specify CIDR, which you cannot change later. It is thus recommended that you reserve enough IP resources for VPC and subnet during creation to prevent insufficient network resources caused by service expansion.
- For each subnet, Tencent Cloud reserves its first two IP and the last IP for IP networking purposes.
- After a VPC is created and its subnets are divided, the user can then deploy cloud service resources in the VPC, such as CVM and database.
- When you add a CVM to a VPC, the system randomly assigns a private IP to its instance within the specified subnet, and the user can reassign the private IP for each CVM after their submachine are created.
- Once a VPC is selected for a CVM, it cannot be changed, but it's allowed to change subnets within a VPC.
- After its private IP of the VPC is changed, CVM will restart in about two minutes although the time differs.
- A CVM in a VPC can bind only one private IP and one public IP
- Each subnet must be associated with a [Routing Table](#), which allows the user to specify the network routing for the subnet.

The following table shows the number limit on VPCs and subnets:

| Resource | Limit |
|--|--------------------------|
| Number of region-wide VPCs | 5 |
| Number of subnets per VPC | 10 |
| Lower limit of size of subnet | /28 (or 14 IP addresses) |
| Number of routing tables per VPC | 10 |
| Number of routing tables associated per subnet | 1 |

For more information, please click to view [Usage Constraints on Other VPC Products](#).

Billing Method

Free Products:

- Use of VPC, subnet, routing table, network ACL, security group is free of charge.
- Private network communication is free. Bandwidth costs are not applicable to inter-instance communication within different subnets.
- VPC cloud services is priced the same as the basic network cloud services; no additional fees are applicable, such as CVM, cloud database and so on.

Paid-for products:

- Communication via public network/direct connection is charged, Click to view [the details on public network communication charges](#).
- Cross-region peer connection, VPN gateway, NAT gateway are charged, Click to view [charge details](#).

Operating Instructions

Creating VPC and Initializing Subnets and Routing Tables

A VPC contains at least one subnet. Cloud service resources can only be added to subnet.

- 1) Log in to [Tencent Cloud Console](#). Click "Virtual Private Cloud" in the navigation bar to enter the [VPC Console](#).
- 2) Select a region in the drop-down box above the list and click "New" to create a VPC under this region.
- 3) Fill in the name for the VPC and its subnet and their [CIDR \(Click to view the constraints on CIDR planning\)](#), and select the availability zone of subnets.
- 4) Click "Create" to complete the creation of VPC and its subnet.

Adding Subnet

Users can create one or more subnets at the same time.

- 1) Click "Subnet" in the left navigation bar of [VPC Console](#).
- 2) Select a region and VPC for which you want to create subnets.
- 3) Click "New", and fill in subnet name, CIDR, availability zone and associated routing table.
- 4) (Optional) Click "New Line" to create multiple subnets at the same time.
- 5) Click "Create" button to complete the creation of subnet.

Associating Subnets with Routing Tables

Each subnet must be associated with a [Routing Table](#) to specify the outbound route for the subnet, and you can change the routing table associated with the subnet at any time. If you need to create a new routing table, please refer to [Creating Routing Table](<https://intl.cloud.tencent.com/doc/product/215/4954#.E5.88.9B.E5.BB.BA.E8.87.AA.E5.AE.9A.E4.B9.89.E8.B7.Af.E7.94.B1.E8.A1.A8>).

- 1) Enter the [VPC Console](#) to select "Subnet" in the left navigation bar.
- 2) Move the cursor to the "subnet" line to be modified and select "Change Routing Table" in Operation column.
- 3) Click "Save" button to complete the association of the subnet with the routing table.

Adding CVM to Subnet

- 1) Enter the [VPC Console](#) to select "Subnet" in the left navigation bar.
- 2) In the line containing the subnet that needs to add a CVM, click the Add CVM icon.

Or you can:

- 1) On the [CVM Overview](#), click "Buy Now" button.
- 2) In the third step, select a storage and network, and select the corresponding VPC and subnet.

Viewing All Resources in VPC

- 1) Click "Virtual Private Cloud" in the left navigation bar of [VPC Console](#).
- 2) Above the list, select the region where the VPC you want to view is located.
- 3) Click VPC ID to enter its details page to view all the resources in the VPC.

Modifying CVM's Private IP

Modification to primary private IP of CVM primary ENI is supported, while modification to primary private IP of secondary ENI is not supported. The operating steps are as follows:

- 1) Enter the [CVM Console](#), and click the CVM in the navigation bar to enter the CVM list page.
- 2) Click the CVM ID to enter the CVM details page, and click the "ENI" tab on the top.
- 3) Click "Modify primary IP".
- 4) Fill in the new IP and save it.



You can also modify the primary private IP on the ENI details page. Click to view [Operation Details](#).

Deleting Virtual Private Cloud (VPC)

The prerequisite for deleting a VPC is that IPs in the VPC is not occupied and there are no resources (for example, subnets, NAT gateways, etc.) in the VPC.

- 1) Click "Virtual Private Cloud" in the left navigation bar of [VPC Console](#).
- 2) Above the list, select its region for the VPC that you want to delete.
- 3) Select the line where the VPC you want to delete is located and click "Delete" in the Operation column.

Deleting Subnet

The prerequisite for deleting a subnet is that the IPs in the subnet is not occupied and there are no resources (such as a CVM) in the subnet.

- 1) Click "Subnet" in the left navigation bar of [VPC Console](#).
- 2) Select the region and VPC where the subnet to be deleted locates.
- 3) Select the line where subnet to be deleted is located and click "Delete".

API Overview

You can use API to set up and manage your VPCs and subnets. Click to view [Overview of All VPC APIs](#).