

# **Virtual Private Cloud**

## **Quick Start**

### **Product Documentation**



## Copyright Notice

©2013-2024 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.

# Contents

## Quick Start

- Network Planning

- VPC Connections

  - Connecting to the Internet

  - Connecting to Other VPC Instances

  - Connecting to Local IDCs

  - Connecting to the Classic Network

- Building Up an IPv4 VPC

# Quick Start

## Network Planning

Last updated : 2024-07-05 16:55:15

Prior to beginning the network scale-out and building of your VPC, you need to plan the quantity and IP ranges of the VPC commensurate with your business needs.

[How to Plan the Quantity of VPCs?](#)

[How to Plan the Quantity of Subnets?](#)

[How to Plan the IP Ranges \(CIDR Blocks\) of VPCs and Subnets?](#)

[How to Plan the Quantity of Route Tables?](#)

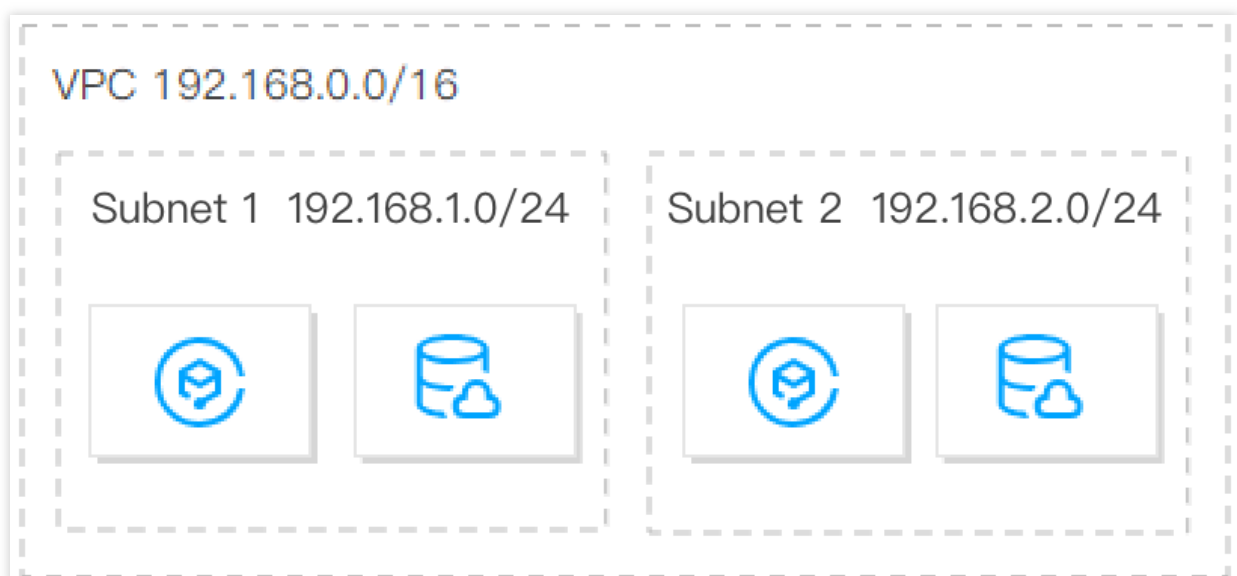
[How to Plan a Cross-region Multi-center Hybrid Cloud Network?](#)

## How to Plan the Quantity of VPCs?

### Planning one VPC

If you have a small scale business that is deployed in the same region without the need for network isolation, we recommend that you plan one VPC.

You can create multiple subnets and route tables in a single VPC for detailed traffic management. In addition, we recommend that you deploy subnets in different availability zones for AZ disaster recovery.



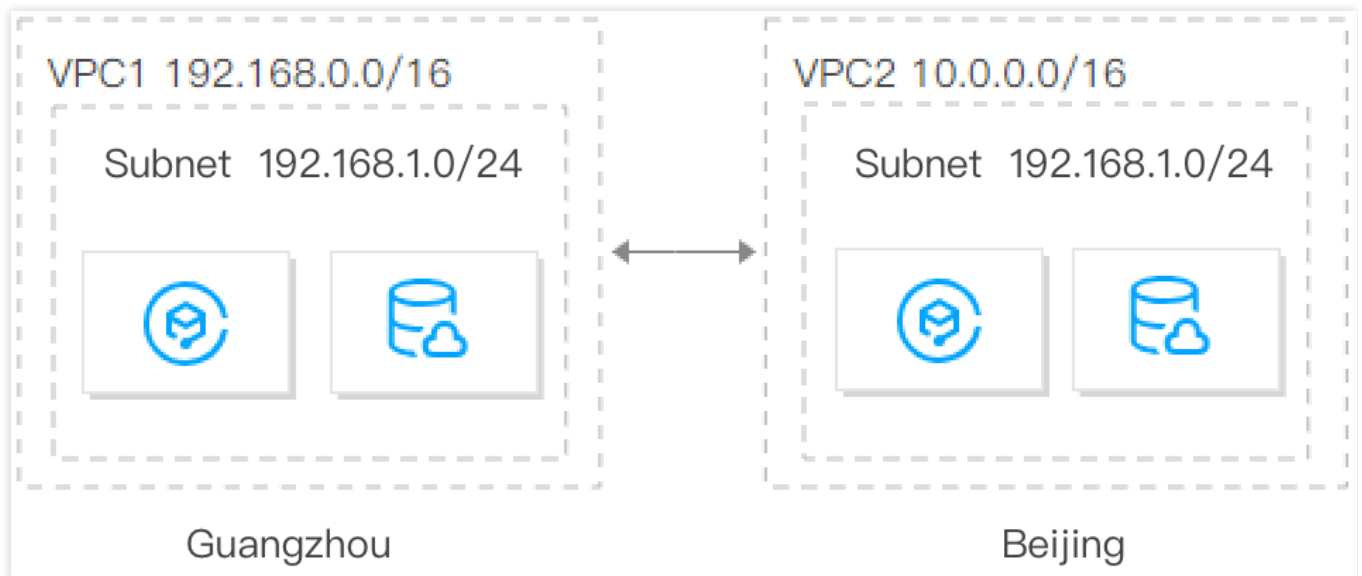
### Planning multiple VPCs

We recommend that you plan multiple VPCs in any of the following scenarios:

### Your business is deployed in multiple regions

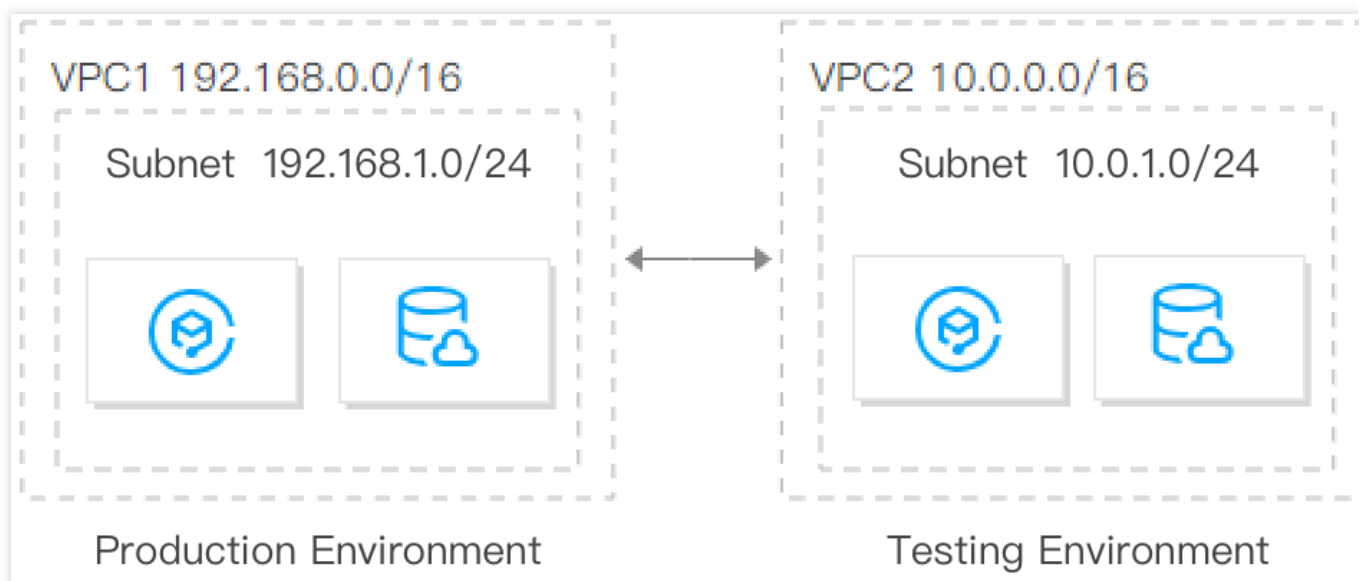
If your business is deployed in multiple regions, you need to plan multiple VPCs and deploy at least one in each region because a VPC cannot be deployed across regions.

By default, VPCs are not interconnected. To interconnect VPCs, use [Peering Connection](#) or [Cloud Connect Network](#).



### Multiple businesses are deployed in the same region and require isolation

If you have multiple businesses deployed in the same region and these businesses must be isolated from each other, you need to plan multiple VPCs and deploy one VPC for each business. Doing this can isolate businesses because VPCs are not interconnected by default.



## How to Plan the Quantity of Subnets?

One VPC can have multiple (100 by default) subnets. Different subnets in the same VPC can communicate with each other over a private network by default.

To achieve disaster recovery across availability zones, we recommend you create at least two subnets in different availability zones for each VPC.

## How to Plan the IP Ranges (CIDR Blocks) of VPCs and Subnets?

**Once set, the IP range masks of VPCs and subnets cannot be modified.** Therefore, be sure to carefully plan VPCs and subnets based on your business scale and communication scenarios. This will facilitate smooth scaling and operations in the future.

### Note

Both IPv4 and IPv6 addresses are supported in VPCs. IPv6 addresses are global unicast addresses (GUAs) rather than private addresses, so custom planning is not supported. This document describes the planning of IPv4 private address IP ranges.

IPv6 addresses are assigned based on the following rules: a `/56` IPv6 CIDR block is assigned to each VPC, a `/64` IPv6 CIDR block is assigned to each subnet, and an IPv6 address is assigned to each ENI.

### Planning VPC IP ranges

**You can use any of the following IP ranges as your VPC IP ranges:**

**10.0.0.0 - 10.255.255.255 (the mask range must be 12 to 28)**

**172.16.0.0 - 172.31.255.255 (the mask range must be 12 to 28)**

**192.168.0.0 - 192.168.255.255 (the mask range must be 16 to 28)**

**When planning VPC IP ranges, note that:**

If you need to create multiple VPCs that communicate with each other or with IDCs, make sure that the IP ranges of the VPCs do not overlap.

If your VPC needs to communicate with the [classic network](#), create a VPC with an IP range of `10.[0~47].0.0/16` and its subset, as VPCs with other IP ranges cannot communicate with the classic network.

Once created, the CIDR blocks of VPCs and subnets cannot be modified. When either CIDR blocks are insufficient, you can [create auxiliary CIDR blocks](#).

### Planning subnet IP ranges

**Subnet IP range:** you can use your VPC IP range or a part of it as the subnet IP range. For example, if the VPC IP range is 10.0.0.0/16, the subnet IP range can be between 10.0.0.0/16-10.0.255.255/28.

**Subnet size and IP capacity:** once created, subnets cannot be modified. When creating subnets, make sure that the subnet IP ranges can meet your business needs. However, you also need to control the subnet size, allowing you to create subnets later for the scale-out.

**Business requirements:** a single VPC can be divided into subnets based on business segments. For example, you can deploy the web layer, logic layer, and data layer in different subnets and use [network ACLs](#) to implement the access control.

#### Note

If the VPC in which subnets are located needs to communicate with other VPCs or IDCs, make sure that the subnet IP range does not overlap with the peer IP range. Otherwise, the interconnection via a private network may fail.

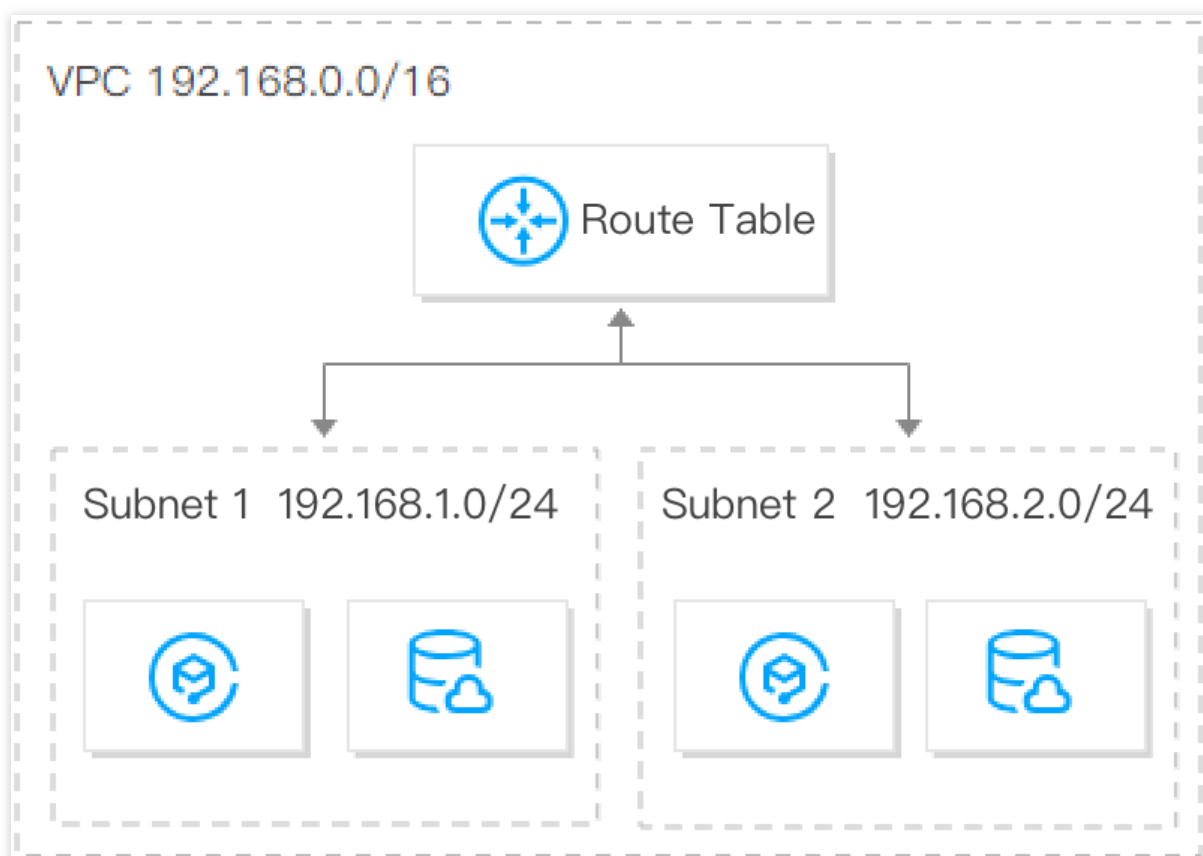
If subnet IP ranges overlap, you create a new VPC and purchase CVMs, or [Switching to VPC](#).

## How to Plan the Quantity of Route Tables?

A route table is used to control the traffic direction within a subnet. Each subnet can only be bound with one route table. You can use the default route table and custom route tables in Tencent Cloud VPCs.

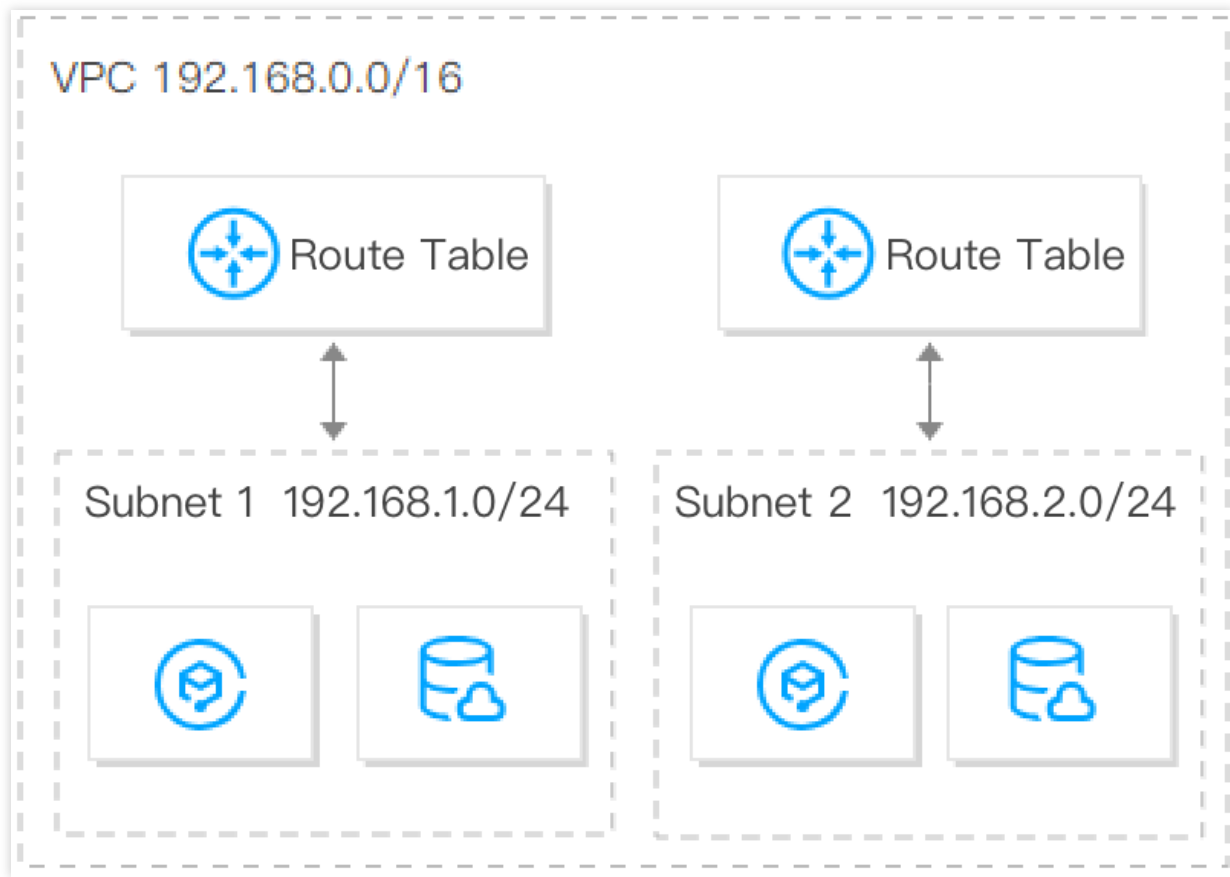
#### Planning one route table

If different subnets in your VPC have the same or similar requirements for traffic direction, we recommend that you plan 1 route table. Then, you can create different routing policies to control the traffic direction.



#### Planning multiple route tables

If different subnets in your VPC have different requirements for traffic direction, we recommend that you plan multiple route tables. Subnets with different needs are bound to corresponding routing tables respectively and use routing policies to control the traffic direction.



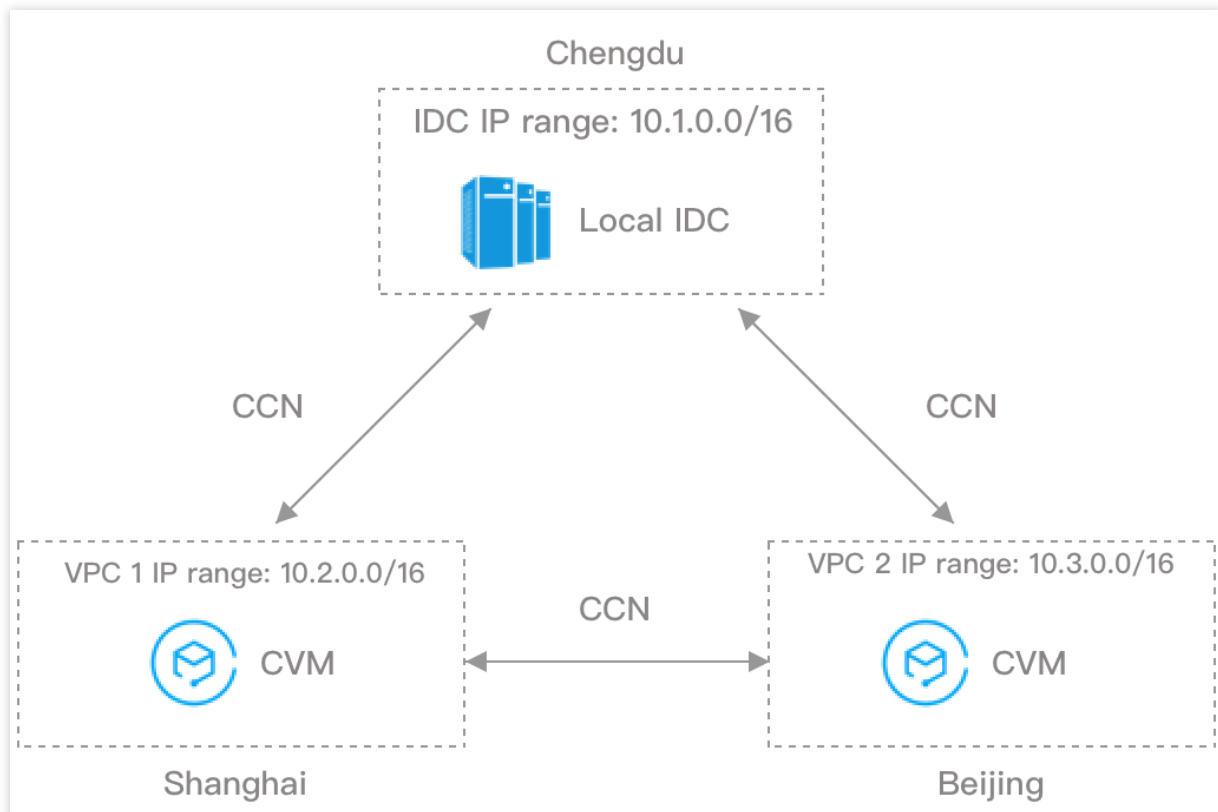
## How to Plan a Cross-region Multi-center Hybrid Cloud Network?

If you need to create multiple VPCs that communicate with each other or with IDCs, make sure that the IP ranges of the VPCs do not overlap with the peer IP range.

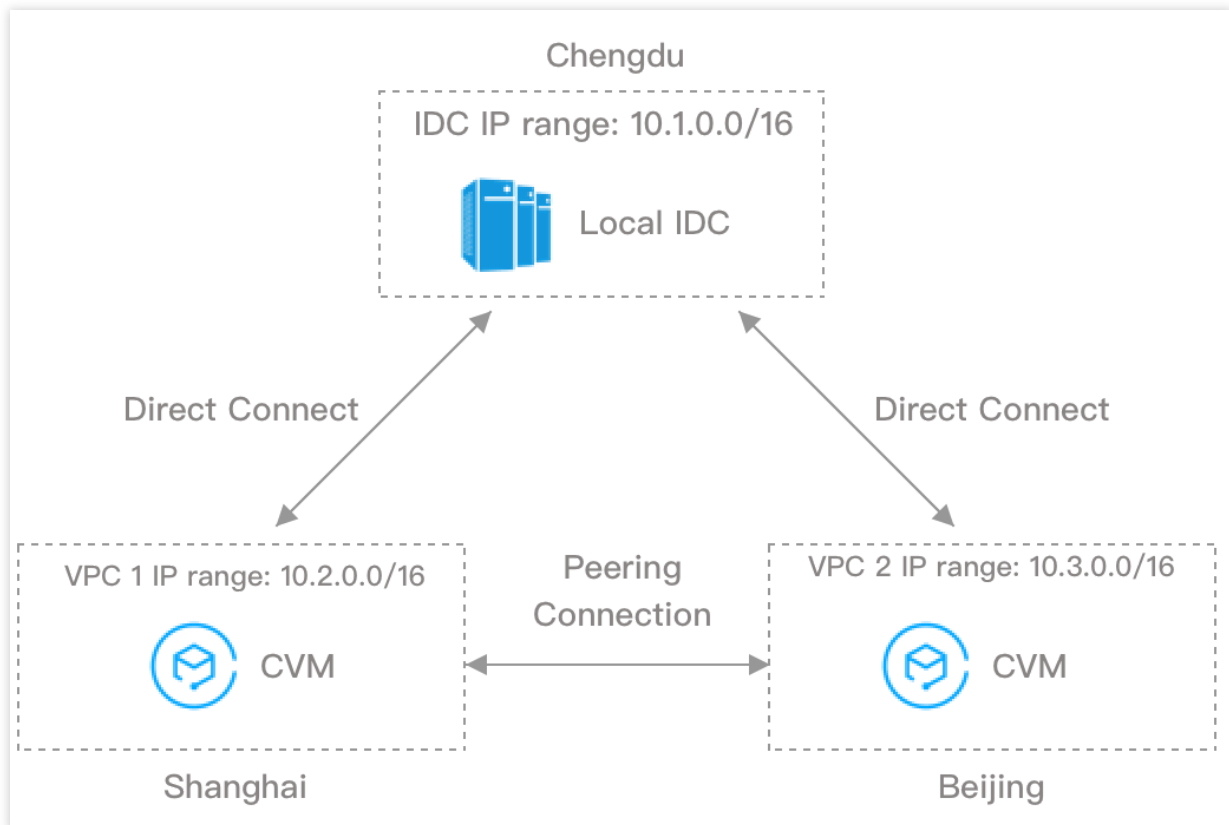
Assume that you have a local IDC with the IP range of `10.1.0.0/16` in Chengdu, and want to create two cloud IDCs in Shanghai and Beijing which need to communicate with your local IDC. In this case, we recommend that you use `10.2.0.0/16` and `10.3.0.0/16` as the VPC IP ranges of the two cloud IDCs in Shanghai and Beijing respectively, to avoid communication failure caused by overlapping IP ranges. You can enable communication between the local IDC and cloud IDCs (VPC 1 and VPC 2) and between the cloud IDCs (VPC 1 and VPC 2) using the following two methods.

**Method 1:** add them to a CCN to implement the interconnection over the public and private network.





**Method 2:** use Direct Connect to connect the cloud IDCs in Shanghai and Beijing to the local IDC in Chengdu, thus enabling communication between the local IDC and the cloud IDCs. To enable communication between the cloud IDCs in Shanghai and Beijing, use peering connection to connect the corresponding VPCs.

**Suggestions for multi-VPC use cases:**

Try to plan different IP ranges for each VPC.

Try to plan different IP ranges for VPC subnets if each VPC cannot have distinct IP range.

Ensure that the IP ranges of subnets that need to communicate are different if each subnet cannot have distinct IP range.

## References

For more information about how to quickly build a VPC with an IPv4 CIDR block, including creating a VPC and subnet, purchasing a CVM, and binding an EIP to enable the public network access, see [Building Up an IPv4 VPC](#).

# VPC Connections

## Connecting to the Internet

Last updated : 2024-01-24 17:22:28

Tencent Cloud provides you with various methods to access the Internet, such as through a common public IP address, EIP, NAT gateway, and Cloud Load Balancer (CLB).

## Common Public IP Addresses

When creating a CVM instance, you can assign a common public IP address to the instance. The system will assign an IP address to your CVM to enable it to access the Internet and also be accessible through the Internet.

Common public IP addresses cannot be dynamically bound or unbound with resources such as CVMs, but you can convert them to EIPs. For details, see [Converting Public IP Addresses into EIPs](#).

## Elastic IP Addresses

Unlike public IP addresses that need to be applied for and released with CVMs, elastic IP addresses (EIPs) are independent cloud resources that are decoupled from the CVM lifecycle and can be operated separately.

For information on how to apply for, bind, and release EIPs, see [EIPs - Steps](#).

EIPs offer the following advantages:

Independent cloud resources

You can operate EIPs independently, without needing to purchase them with CVMs.

Elastic binding and unbinding with resources

EIPs can be bound and unbound with CVMs and other resources at any time.

## NAT Gateways

A NAT gateway provides the SNAT and DNAT features, which enables you to easily establish an Internet egress and provide services for CVMs in a VPC to access the Internet with the same public IP address.

For information on how to configure the NAT gateway, see [NAT Gateways - Operation Overview](#).

NAT gateways offer the following advantages:

Secure Internet access

NAT gateways provide the SNAT and DNAT features to hide the IP addresses of CVMs in a VPC during Internet communication, ensuring security.

### High availability

NAT gateways feature master/slave hot backup, automatic hot switching, and quick forwarding with a rate up to 5 Gbps. In addition, they support large-scale Internet applications.

### Flexible configuration

You can modify NAT gateway specifications as required at any time.

## Cloud Load Balancers

A Cloud Load Balancer (CLB) distributes traffic to multiple CVMs to enhance the external service capabilities of application systems. It eliminates single points of failure to ensure highly available application systems.

For information on how to purchase and configure a CLB, see [CLBs - Getting Started](#).

CLBs offer the following advantages:

### High-performance single cluster

A CLB cluster consists of multiple physical servers, with an availability of up to 99.95%. The cluster system can remove faulty instances and select healthy instances to ensure the proper running of services on the real server.

### High security and stability

With the BGP anti-DDoS system, the CLB can defend against most network attacks (such as DDoS attacks) and cleanse traffic attacks in seconds, preventing blocked IP addresses or full bandwidth consumption.

## Public Gateways

A public gateway is a CVM with the forwarding feature enabled. In a VPC, CVMs without a public IP address can access the Internet through public gateways on different subnets. Public gateways can covert the source addresses of Internet traffic from other CVMs to their own IP addresses.

For information on how to configure a public gateway, see [Configuring Public Gateways](#).

# Connecting to Other VPC Instances

Last updated : 2024-01-24 17:22:28

You can connect different VPC instances through peering connections or a CCN.

## Peering Connections

You can establish [peering connections](#) to interconnect two VPC instances under the same or different accounts.

[Creating a peering connection for intra-account VPC communication](#)

[Creating a peering connection for cross-account VPC communication](#)

## CCNs

You can use a [CCN](#) to interconnect two or more VPC instances. A CCN supports interconnection between VPC instances under the same or different accounts and interconnection between VPC instances and IDCs.

[Interconnection between network instances under the same account](#)

[Interconnection between network instances under different accounts](#)

# Connecting to Local IDCs

Last updated : 2024-01-24 17:22:28

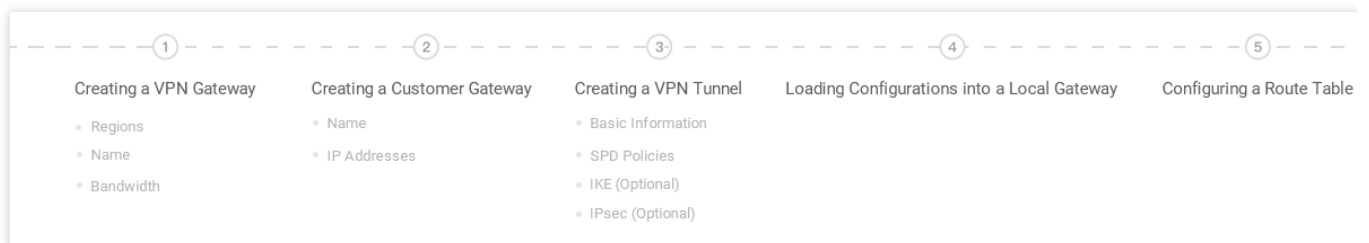
You can establish a VPN connection, direct connection, or CCN to implement communication between your VPC instances and local IDCs.

## VPN Connections

[VPN connection](#) is a method for connecting your IDCs and VPC instances through public network encrypted tunnels.

A VPN connection consists of three parts: VPN gateway, customer gateway, and VPN tunnel.

Each VPN gateway can establish multiple VPN tunnels, and each VPN tunnel can connect to one local IDC.



For details about the operations, see [VPN Connections - Getting Started](#).

## Direct Connections

A [direct connection](#) is a physical direct connection that connects VPC instances and local IDCs. A direct connection consists of three parts: physical connection, dedicated tunnel, and direct connect gateway.

Users can establish a physical connection to connect Tencent Cloud computing resources in multiple regions, achieving flexible and reliable hybrid cloud deployment.

For details about the operations, see [Direct Connect - Getting Started](#).

## Cloud Connect Networks

[Cloud Connect Network \(CCN\)](#) interconnects Tencent Cloud VPC instances and connects VPC instances with local IDCs.

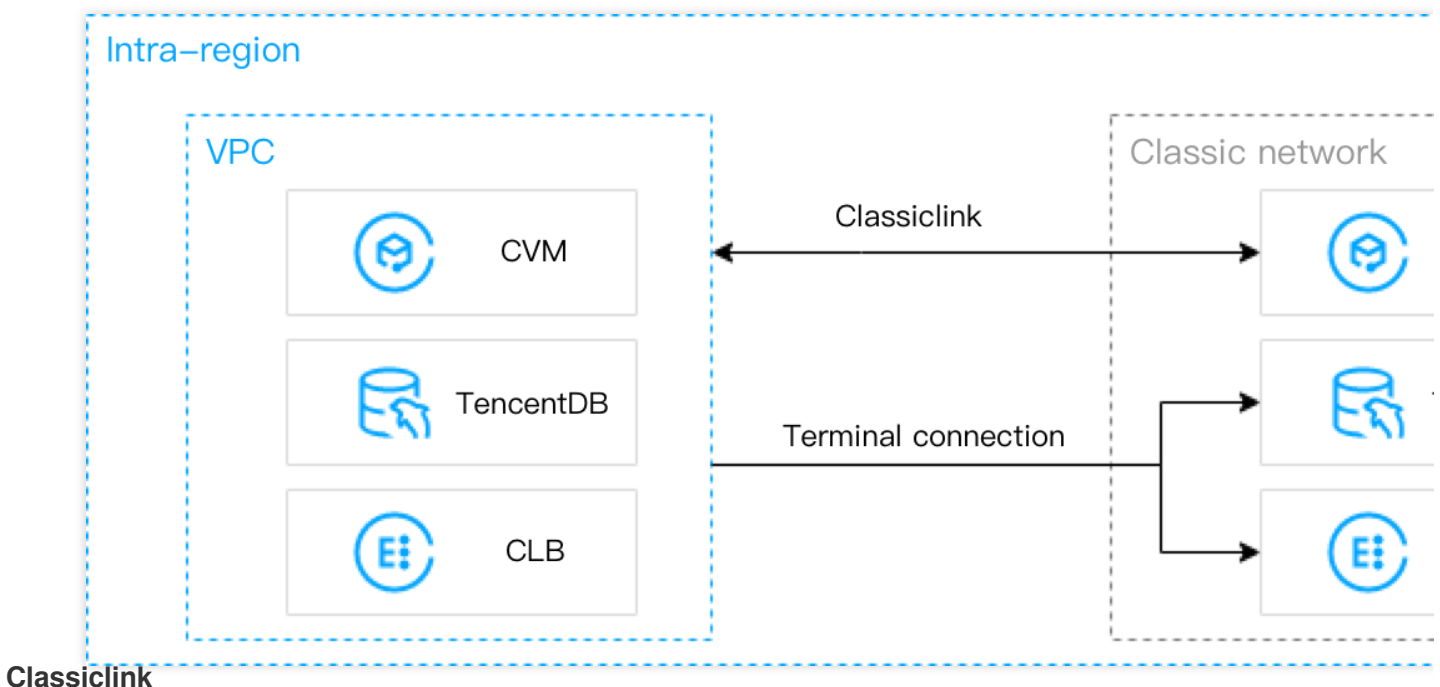
For details about the operations, see [Migrating IDC to the Cloud Through CCN](#).

# Connecting to the Classic Network

Last updated : 2024-01-24 17:22:28

Both the classic network and VPC are network spaces on the cloud. The VPC is more secure and controllable. Although most of CVMs are deployed in Tencent Cloud VPCs, a few applications are still running on the classic network that needs interconnection with the VPC. To address this problem, Tencent Cloud provides the following solution.

## Interconnecting the Classic Network and a VPC



### Classiclink

It associates the classic network-based CVMs with a specified VPC to allow these CVMs to communicate with VPC resources such as CVM and TencentDB instances. However, this only provides access between VPC-based CVMs and classic network-based CVMs rather than other cloud resources including TencentDB and CLB within the classic network.

### Terminal connection

It helps instances in a VPC to communicate with resources in the classic network (except CVMs) through a private network. A terminal connection establishes a mapping between classic network instance IP addresses and VPC IP addresses so that classic network instances can be accessed by accessing VPC IP addresses. Classic network products that support terminal connections include CLB, MySQL, Memcached, Redis, MariaDB, SQL Server, PostgreSQL, MongoDB, and TDSQL instances.

### Note:

A terminal connection does not support cross-region or cross-account communication. If you want to establish a terminal connection, please [submit a ticket](#).

## Migrating from the Classic Network to a VPC

Tencent Cloud VPC is recommended for its security, flexibility and controllability. Currently, Tencent Cloud supports migrating resources from the classic network to a VPC. For more information, see [Migrating from the Classic Network to VPC](#).

## References

For more information about the classic network and its differences from a VPC, see [Classic Network](#).  
For more information about Classiclink configurations, see [Classiclink](#).



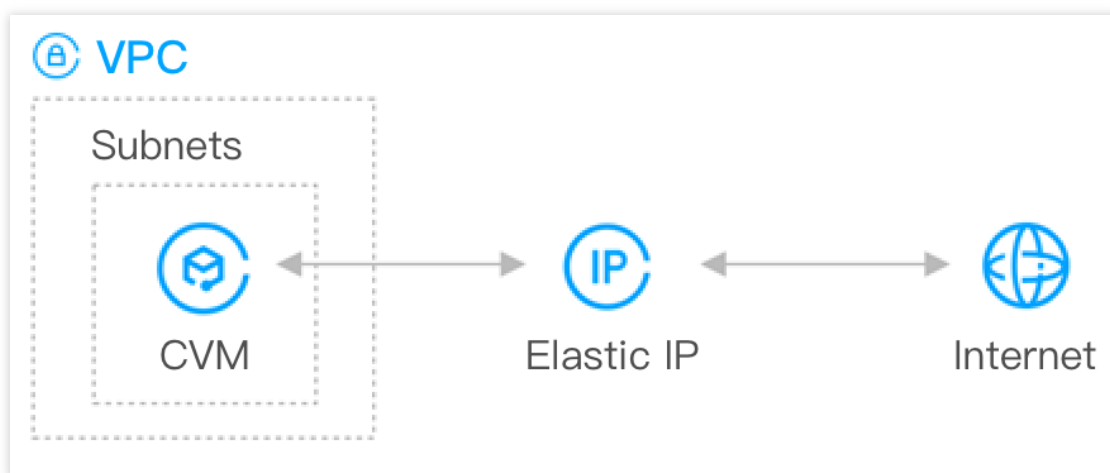
# Building Up an IPv4 VPC

Last updated : 2024-01-24 17:22:28

This tutorial describes how to quickly build up a Virtual Private Cloud (VPC) with IPv4 CIDR blocks.

## Scenarios

This document guides through whole process of setting up an IPv4-based VPC.



## Prerequisites

Before using Tencent Cloud products, [create a Tencent Cloud account](#) and complete [identity verification](#).

## Directions

### Step 1: create a VPC and subnet

#### Note:

Once created, the CIDR blocks (IP ranges) of VPCs and subnets cannot be modified. Therefore, complete [network planning](#) in advance.

1. Log in to the [VPC console](#).
2. Select a region at the top of the page and click **+ New**.
3. In the **Create VPC** pop-up window, configure the VPC and subnet information as instructed below.

Create VPC

VPC information

Region

Name

IPv4 CIDR Block

10 . 0 . 0 . 0 / 16

Cannot be modified after creation

For better usage of VPC, it's recommended to have a proper network structure.

Advanced Options

Subnet Information

Subnet Name

IPv4 CIDR Block

10 . 0 . 0 . 0 / 24

Remaining IPs: 253

Availability Zone

Zone 1

Associated route table

Default

Advanced Options

OK

Close

### VPC information

Name: the name of the VPC.

IPv4 CIDR Block: You can choose any one of the IP ranges as the VPC IP range, such as 10.0.0.0/16 .

10.0.0.0 - 10.255.255.255 (mask range: 12 to 28)

172.16.0.0 - 172.31.255.255 (mask range: 12 to 28)

192.168.0.0 - 192.168.255.255 (mask range: 16 to 28)

Tags: You can optionally add tags to help you better manage resource permissions of sub-users and collaborators.

### Subnet information

IPv4 CIDR Block:

You can choose an IP range within or the same as the VPC IP range. For example, if the VPC IP range is

`10.0.0.0/16`, you can choose an IP range between `10.0.0.0/16` and `10.0.0.248/29` as the subnet IP range.

If the VPC in which subnets are located needs to communicate with other VPCs or IDCs, make sure that the subnet IP range does not overlap with the peer IP range. Otherwise, the interconnection over a private network may fail.

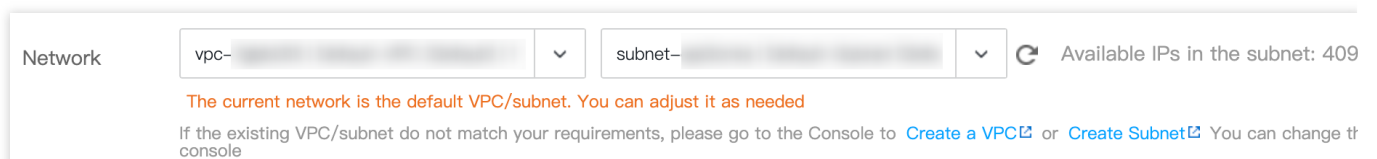
**Availability Zone:** select an availability zone in which the subnet resides. A VPC allows subnets in different availability zones, and these subnets can communicate with each other via a private network by default.

**Tags:** You can optionally add tags to help you better manage resource permissions of sub-users and collaborators.

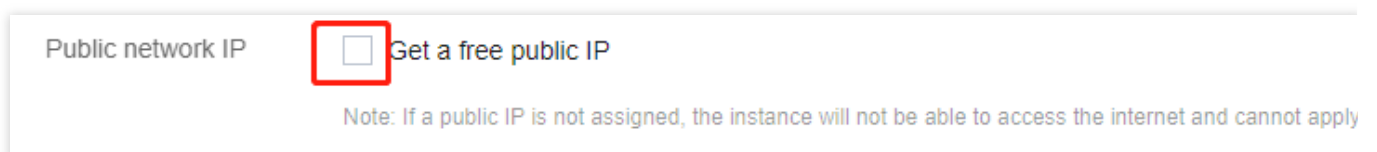
## Step 2: purchase a CVM instance

1. Log in to the [CVM console](#) to create a CVM instance in the VPC created in the previous step.
2. Click **Create** in the top-left corner of the list page to go to the [CVM purchase page](#).
3. On the custom configuration page, configure the CVM instance and then click **Buy Now**. The CVM network configurations are as follows:

**Network:** select the created VPC and subnet.



**Public network IP:** do not check

☐

**Security Group:** select **New security group** and configure it as instructed in [Configuring Security Groups](#).

Security Groups

Create security group

Existing Security Groups

Operation Guide

Allow common IPs/ports

☒ ICMP Allows ping command on the CVM from internet

☐ TCP:80 When the CVM is used (HTTP)

☒ TCP:22 Allows remote login via SSH key for Linux instances

☐ TCP:443 When the CVM is used (HTTPS)

☒ TCP:3389 Allows remote login via RDP for Windows instances

☒ Allow private access Allows priv among different cloud resources (IPv

To open other ports, you can [Create security group](#)

### Step 3: apply for an EIP and bind it to the CVM instance

An EIP is a public IP address that can be applied for and purchased independently. You can bind an EIP to a CVM instance to enable public network access.

1. Log in to the [EIP console](#).
2. On the **EIP** page, select the region where the CVM instance is located. Click **Apply** in the top-left corner.
3. In the **Apply for EIP** pop-up window, configure relevant parameters and click **OK**.
4. On the **EIP** page, locate the EIP you applied for, and click **More > Bind** in the **Operation** column.
5. In the **Bind resources** window, select **CVM Instances** as the resource type to be bound, select the CVM instance, and click **OK**.

**Bind resource** ✕

Select the cloud resources to be bound to the EIP ( )

☒ CVM instances ☐ NAT gateway ☐ ENI ☐ High availability virtual IP ☐ Private CLB

Enter name, ID or private IP

| Instance ID/Name                          | Availability zone | Private IP | Bound public IP |
|---|-------------------|------------|-----------------|
| Unnamed                                   | Guangzhou Zone 6  | 10.0.2.3   | -               |
| <input checked="" type="radio"/> in<br>em | Guangzhou Zone 6  |            | -               |
| <input type="radio"/> ins<br>e<br>6r      | Guangzhou Zone 6  |            | -               |
| <input type="radio"/> ins<br>e<br>6r      | Guangzhou Zone 6  |            | -               |

OK

Cancel

6. In the pop-up confirmation window, click **OK**.

#### Step 4: test public network connectivity

Perform the following operations to test the public network connectivity of the CVM instance.

**Note:**

Before performing the test, make sure that the security group allows access to the corresponding IP address and port. For example, the ICMP protocol is opened, and the server can be pinged over the public network. For more information, see [Viewing a Security Group Rule](#).

1. Log in to the CVM instance with an EIP bound. For more information, see [Login and Connect to Instances](#).
2. Run the `ping Another public IP` command, such as `ping www.qq.com` , to test public network connectivity.

```
[root@VM_48_15_centos ~]# ping www.qq.com
PING public-v6.sparta.mig.tencent-cloud.net (1 ) 56(84) bytes of data.
64 bytes from 1: 5 (1 5): icmp_seq=1 ttl=49 time=32.8 ms
64 bytes from 1: 5 (1 5): icmp_seq=2 ttl=49 time=32.8 ms
64 bytes from 1: 5 (1 5): icmp_seq=3 ttl=49 time=32.8 ms
64 bytes from 1: 5 (1 5): icmp_seq=4 ttl=49 time=32.8 ms
64 bytes from 1: 5 (1 5): icmp_seq=5 ttl=49 time=32.8 ms
^C
--- public-v6.sparta.mig.tencent-cloud.net ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 32.822/32.845/32.899/0.029 ms
```