Virtual Private Cloud
Getting Started

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

Getting Started
Network planning

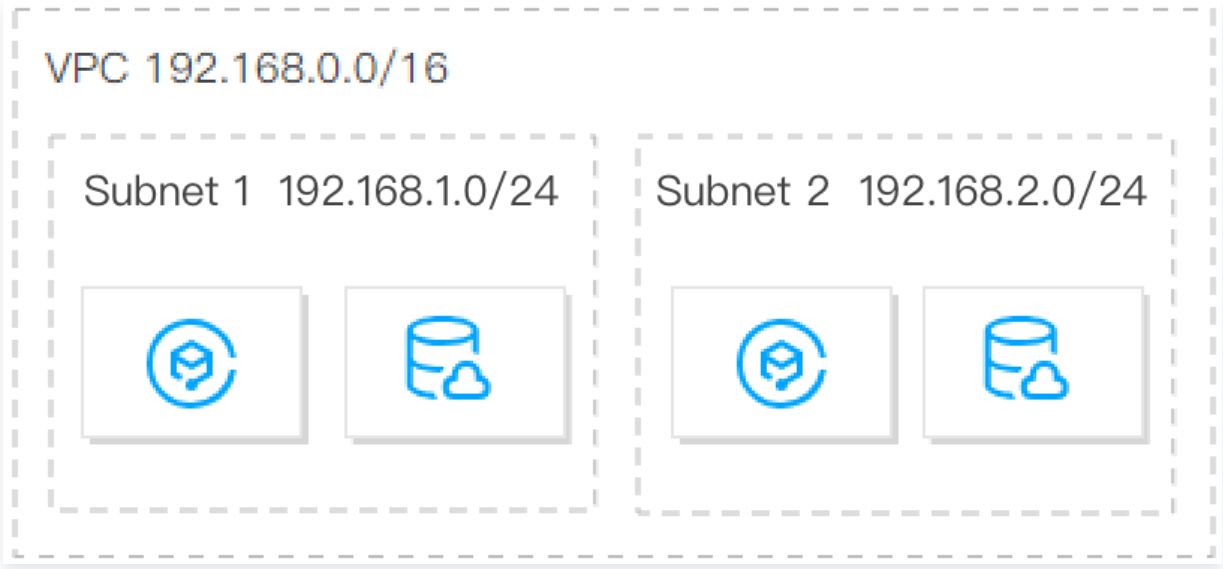
Last updated：2024-01-12 14:25:51

Plan your VPC network properly to ensure that the network meets your business requirements.

- Number of VPCs
- Number of subnets
- IP ranges (CIDR blocks) of VPCs and subnets
- Number of route tables
- Cross-region multi-IDC hybrid cloud network

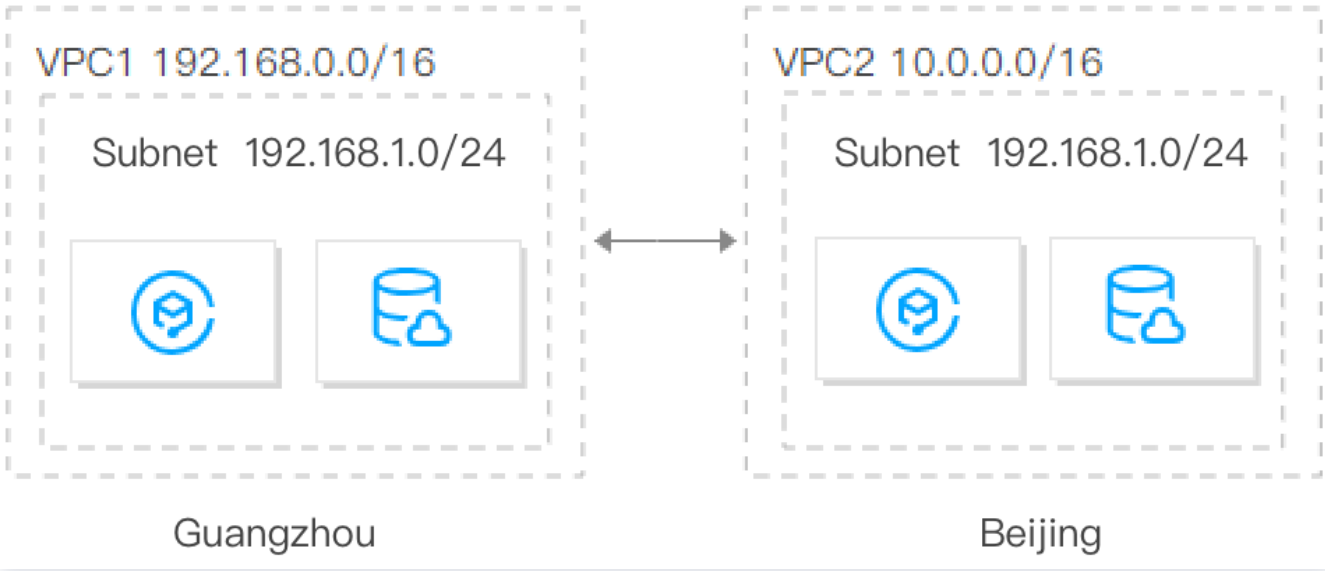
Number of VPCs

- **Single VPC**
  It's suitable for small-scale scenarios where services are deployed within the same region, and there is no need to isolate service through VPCs.
  You can create multiple subnets and route tables in a single VPC for fine-grained traffic management. Additionally, it is recommended to distribute multiple subnets across AZs to enable disaster recovery.

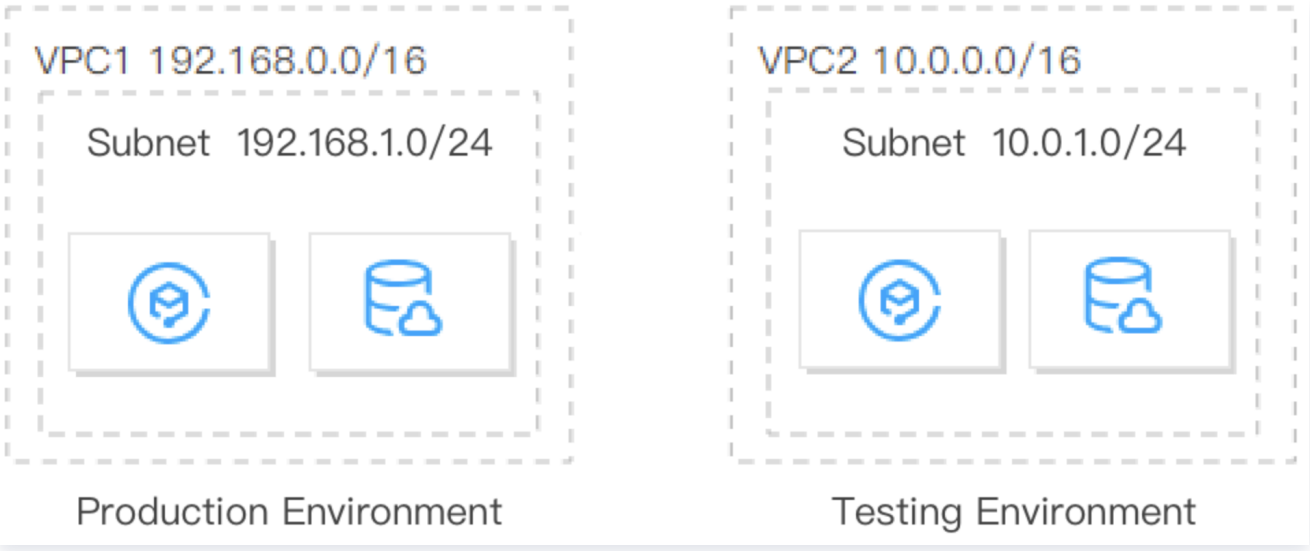


- **Multiple VPCs**
  A multi-VPC architecture is recommended in the following cases:
  - **Deploy services in multiple regions**
    When deploying your applications across multiple regions, you need to plan for multiple VPCs. As a single VPC cannot span across regions, you must deploy at least one VPC

in each region.
By default, VPCs do not communicate with each other. To connect VPCs, you can establish connections using Peering Connections or CCN.



- **Deploy multiple services in the same region and isolate them**
  When you have multiple services deployed in the same region and need to isolate them from one another, you need to create multiple VPCs, assigning one VPC for each service. Since VPCs are not interconnected by default, no additional actions are required to achieve isolation between services.



Number of subnets

- One VPC can have multiple subnets (100 by default). Different subnets in the same VPC can communicate with each other over a private network.
- To achieve disaster recovery across AZs, you can create at least two subnets in different AZs for each VPC.

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 service scale and scenarios. This will facilitate smooth scaling and Ops in the future.

Notes

- 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 (**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**)
- **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.
  - After a VPC and subnet is created, the CIDR block cannot be modified. When there are not enough addresses, you can create secondary CIDR blocks.

Planning subnet IP ranges

- **Subnet IP range**: You can set a subnet IP range within the VPC IP range, or even the same as the VPC 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**: After a subnet is created, the subnet size cannot be modified. When creating subnets, make sure that the subnet IP ranges can meet your application needs. However, you also need to control the subnet size, allowing you to create subnets later for the scale-out.
- **Service requirements**: A single VPC can be divided into subnets based on the service

modules. 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.

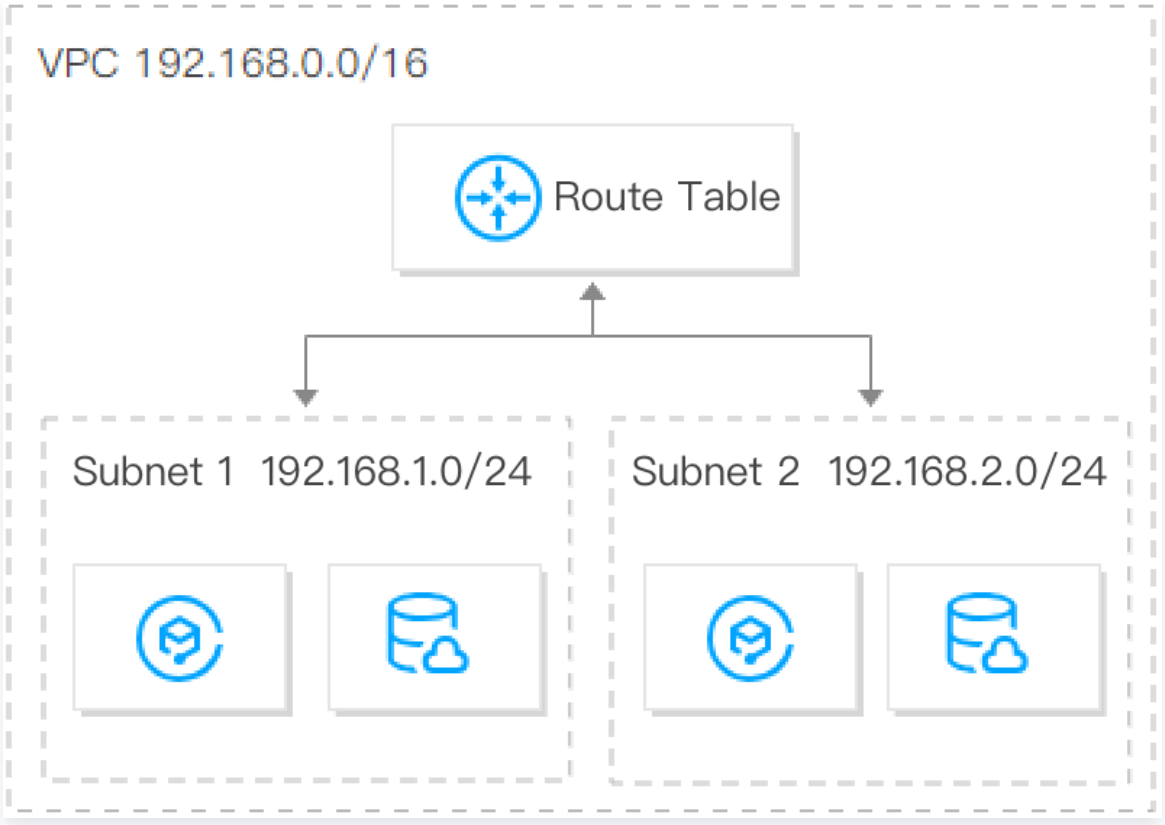
Notes

- 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 can change the instance subnet and use CCN, or create a new VPC and purchase CVMs.

Number of route tables

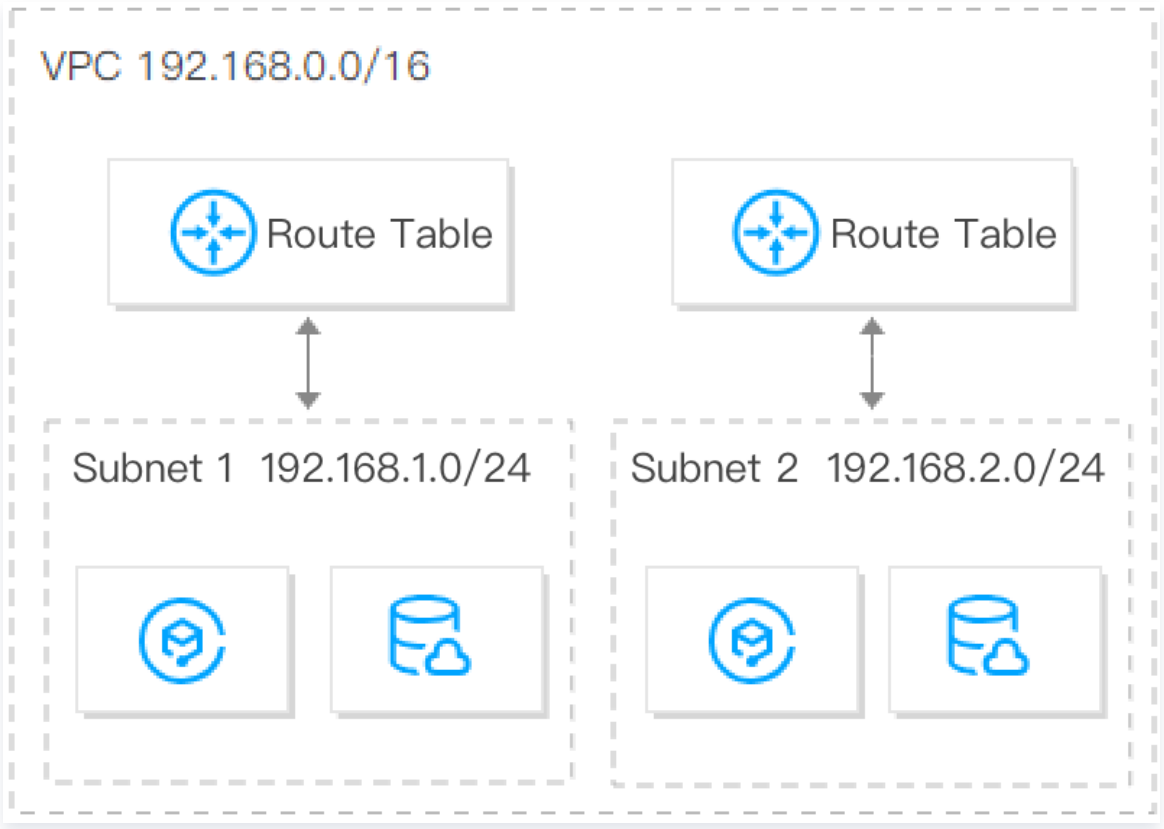
A route table is used to control the traffic direction within a subnet. Each subnet can only be bound with one route table. You can use the default route table and custom route tables in Tencent Cloud VPCs.

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



- **Multiple route tables**
  If different subnets in your VPC have different requirements for traffic direction, we

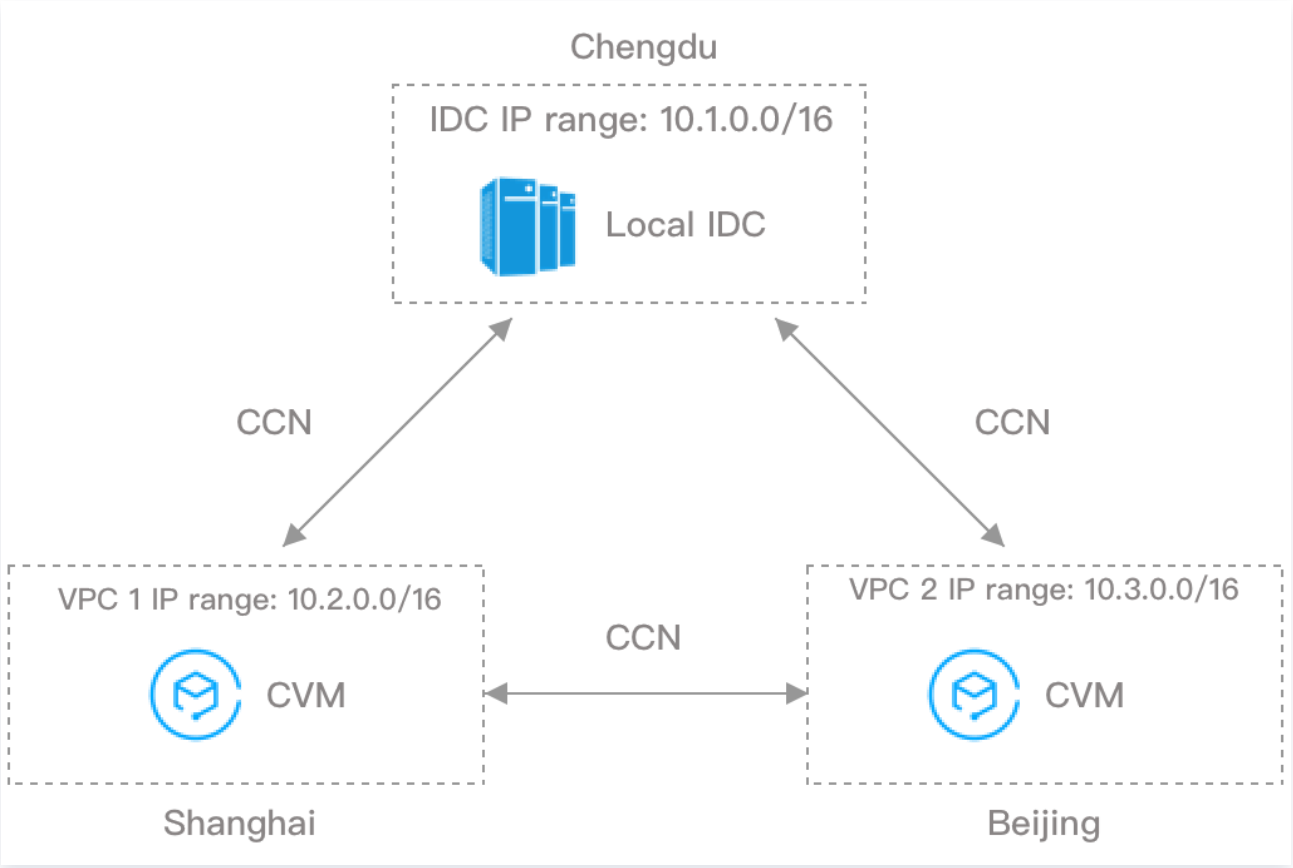
recommend that you plan multiple route tables. Subnets with different needs are bound to corresponding route tables respectively, and traffic direction is controlled with routing policies.



Cross-region multi-IDC hybrid cloud network

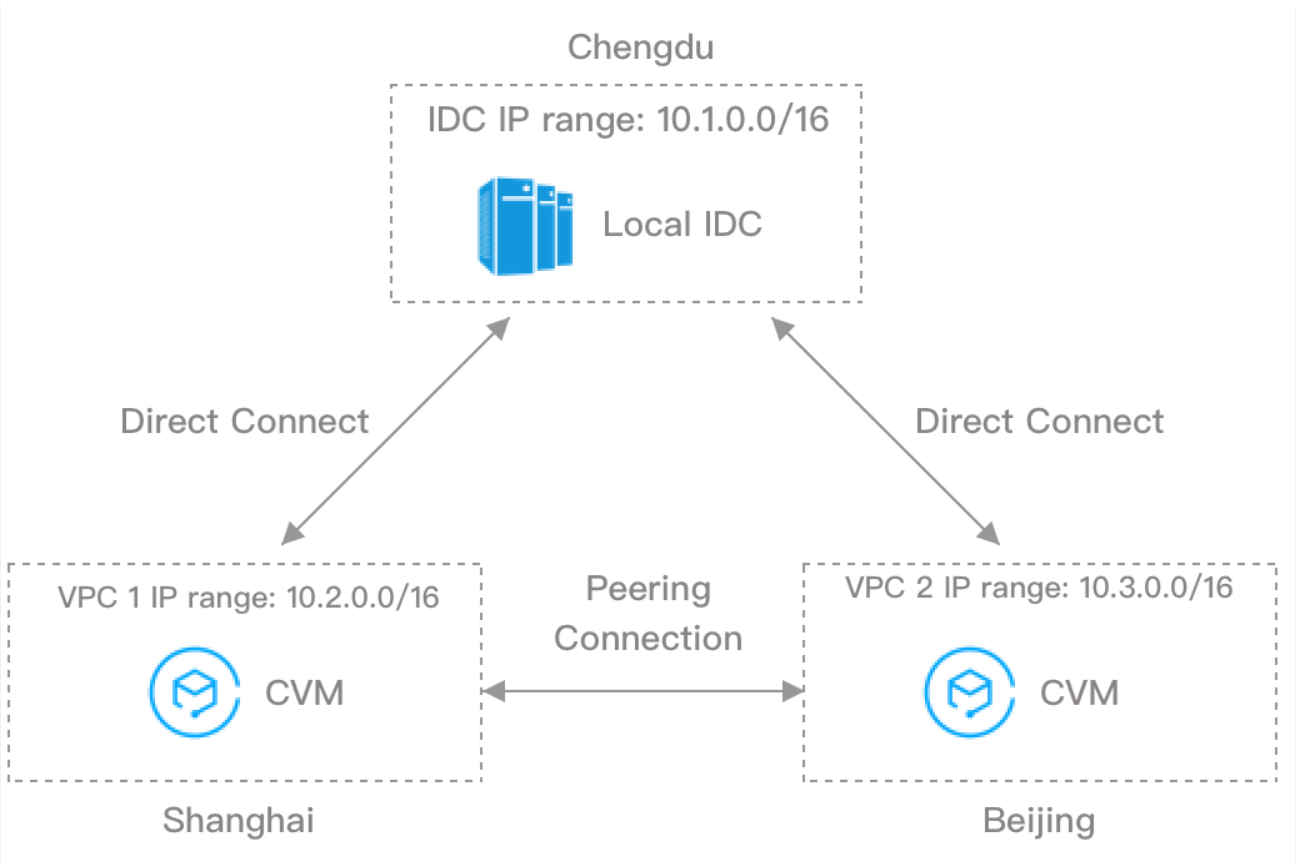
If you need to create multiple VPCs that communicate with each other or with IDCs, make sure that the IP ranges of the VPCs do not overlap with the peer IP range.
Assume that you have a local IDC with the IP range of `10.1.0.0/16` in Chengdu, and want to create two cloud IDCs in Shanghai and Beijing 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.

Documentation

- 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.
- For more information about how to build a VPC with an IPv6 CIDR block and enable IPv6 for CVMs within the VPC, see Building Up an IPv6 VPC.

VPC Connections
Overview of VPC Connection Solutions

Last updated: 2024-01-12 14:26:10

Tencent Cloud provides an extensive range of solutions to enable instances within a VPC, such as CVMs and databases, to connect to the public network (internet), connect to instances in other VPCs, or interconnect with local IDCs. Please watch the following video to learn about Virtual Private Cloud (VPC) and its connection options.
Watch video

Public network connection

You can use the following products or features to enable access between a VPC and the public network.

Product	Features	Characteristics
Public IP	It supports mutual access between the CVM and the public network.	You can choose whether to allocate a public IP when purchasing a CVM instance. If not allocated during purchase, please use EIP or NAT Gateway.
Elastic IP (EIP)	One or more EIPs can be bound to a single CVM instance for public network access.	• An IP resource that can be purchased and owned independently. For more information, see EIP – Billing Overview. • It can be bound to and unbound from CVM and NAT gateway instances. • You can adjust the bandwidth limit of the EIP at any time as needed.
NAT Gateway	• SNAT: It supports access to the public network by multiple CVM instances in a VPC through a single public IP address.	• Multiple CVMs can access the public network through a NAT gateway. • You can adjust the bandwidth limit of the NAT gateway at any

	• DNAT: It allows mapping of private IPs, protocols and ports of a CVM in a VPC to public IPs, protocols and ports, enabling services on the CVM to be accessed from the public network.	time as needed.
Cloud Load Balancer	It provides services by averagely distributing access traffic to multiple CVMs.	• It provides layer-4 and layer-7 load balancing features based on ports, and allows users to access CVMs over the public network through the CLB. • It eliminates single points of failure, enhancing the availability of application systems.
Public Gateway	It is a type of CVM with the forwarding feature enabled. CVMs without public IP addresses can access the public network through public gateways in different subnets.	• The difference between the public gateways and CVMs with public IPs is that public gateways can forward the public network access traffic of CVMs in other subnets, whereas CVMs with public IPs can only satisfy their own demand for public network access. • As of December 6, 2019, Tencent Cloud no longer supports configuring a CVM as the public gateway on the CVM purchase page. Using a single CVM as the public gateway carries a risk of a single point of failure. It is recommended to use the NAT Gateway.

Connecting to Other VPCs

You can use the following products or features to enable inter-VPC communication.

Product	Features	Characteristics
Peering Connections	It is used for private network	• The CIDR blocks of the VPCs cannot overlap. • Manual routing configuration is required.

	communication between VPCs.	• Interconnection between VPCs under different accounts in different regions is supported.
CCN	It is used for private network communication between two or more VPCs.	• The CIDR blocks of subnets cannot overlap. • The configuration is simple, and routing is automatically delivered. • After being added to CCN, all instances are interconnected by default. Routing can be enabled or disabled as needed. • Interconnection between VPCs under different accounts in different regions is supported, and interconnection between a VPC and an IDC is also supported.

Private Link

Feature: It is used for one-way communication from a VPC to another through a private network.
Characteristics: It provides high-bandwidth, low-latency one-way access between VPCs. You can securely manage the access permissions of service users, ensuring safer communication. You only need to establish a connection between the service user and provider to achieve secure network access, without the need for complex routing configurations.

Connecting to Local IDCs

You can use the following products or features to enable interconnection between a VPC and a local IDC.

Product	Features	Characteristics
VPN Connection	It is used to connect local IDCs and VPCs through encrypted public network channels.	• Network quality depends on the public network. • Network transmission is based on the PSK encryption of the IKE protocol.
Direct Connect	It is used to connect a VPC and a local IDC through a connection.	• A static network latency is guaranteed. • Network links are exclusive, which ensures high security.

		• The network address translation service can be configured on gateways to resolve address conflict.
CCN	It is used to connect VPCs and local IDCs through Tencent Cloud's private network, which enables communication among all VPCs and IDCs.	• The configuration is simple, and routing is automatically delivered. • After the instances are added, interconnection with multiple VPCs and IDCs is supported. Routing can be enabled or disabled as needed. • Interconnection between intra-region instances is free of charge.

Connecting to the Classic Network

You can use the following products or features to enable interconnection between VPCs and the classic network.

Product	Features	Characteristics
Classiclink	It is used to associate CVMs in the classic network with specified VPCs, thus allowing the classic network-based CVMs to communicate with cloud services in VPCs such as CVMs and databases.	• The classic network-based CVMs can communicate with VPC resources such as CVM, TencentDB, private network CLB, Redis/CMEM, etc. • CVMs in a VPC can only access the interconnected classic network-based CVMs, but not other computing resources in the classic network.

See Also

- For information on how to access the public network (internet) using public IPs, EIPs, NAT gateways and CLBs, see Connecting to the Public Network.
- For information on how to connect VPCs through peering connections and CCN, see Connecting to Other VPCs.
- For information on how to establish communication between a VPC and a local IDC using VPN connection, Direct Connect or CCN, see Connecting to a Local IDC.
- For information on how to enable communication between a VPC and the classic network using Classiclink, see Communicating with the Classic Network.

Connection to Public Network

Last updated: 2024-01-12 14:26:17

You can connect a VPC to the public network (internet) in several ways, including public IPs, EIPs, NAT gateways, and CLBs. Please watch the following video to learn more.
Watch video

Public IP

When creating a Cloud Virtual Machine (CVM) instance, you can choose to allocate a common public IP address. The system will assign an IP address to your CVM, enabling it to access and be accessed by the public network.
Common public IP addresses cannot be dynamically unbound or bound to resources like CVMs. However, you can convert a common public IP address to an Elastic IP (EIP). For detailed instructions, please refer to Converting a Common Public IP to an EIP.

Elastic IP (EIP)

Elastic IP (EIP) is an independently owned IP resource. Unlike public IP addresses, which can only be applied for and released with a Cloud Virtual Machine (CVM), EIPs can be decoupled from the CVM lifecycle and managed as separate cloud resources.
For EIP application, binding, and release operations, please refer to Operation Overview.
EIPs offer the following advantages:

- Independent resource ownership
  Elastic IPs can be owned independently under your account, without the need to be purchased and bound with a Cloud Virtual Machine. They can be managed as standalone cloud resources.
- Flexible bindings
  EIPs can be flexibly bound to and unbound from resources such as CVMs at any time, providing high availability.

NAT Gateway

If you have multiple Cloud Virtual Machines that need to access the public network through a single public IP address, a NAT gateway can meet your requirements. NAT gateways provide SNAT and DNAT functionality for Cloud Virtual Machines within a Virtual Private Cloud, making it easy to set up public network egress and offer services.
For NAT gateway configuration and operations, please refer to NAT Gateway – Operation Overview.
NAT gateways offer the following advantages:

- Secure public network access:

NAT gateways provide SNAT and DNAT functionality, enabling communication with the public network while concealing the IP addresses of hosts within the VPC, ensuring security.

- High Availability:
  NAT gateways feature dual-server hot backup and automatic hot switching, supporting up to 5 Gbps forwarding capabilities, providing robust support for your large-scale public network applications.
- Flexible configuration
  You can modify the NAT gateway specifications as needed at any time.

Cloud Load Balancer

Cloud Load Balancer (CLB) is a service that distributes traffic among multiple Cloud Virtual Machines (CVMs). By distributing traffic, CLB enhances the external service capabilities of application systems and improves their availability by eliminating single points of failure.
For purchasing and configuring Cloud Load Balancer, please refer to Cloud Load Balancer Quick Start.
Cloud Load Balancer offers the following advantages:

- High performance
  A CLB cluster consists of multiple physical servers, offering an availability of up to 99.95%. Faulty instances are removed automatically to ensure the normal operation of applications on the backend server.
- Secure and stable
  CLB is combined with Anti-DDoS to defend against most network attacks (such as DDoS attacks). Attacking traffic can be cleansed in seconds, which greatly avoids IP blocking and bandwidth overload.

Public Gateway

A public gateway is a CVM that works as a forwarder. With public gateways in different subnets, CVMs in a VPC can access the internet even if they don't have public IPs. A public gateway translates the source address for public network traffic, which means that when CVMs accessing the internet over the public gateway, their IPs will be translated to the public gateway IPs.
For details on public gateway configuration, see Configuring a Public Gateway.

Connecting to Other VPC Instances

Last updated: 2024-01-12 14:26:22

You can connect to different VPCs through Peering Connection or Cloud Connect Network (CCN). Please watch the following video to learn more.
Watch video

Peering Connection

You can establish communication between two VPCs using Peering Connection, which supports both intra-account VPC connections and cross-account VPC connections.

- Creating Intra-account Peering Connection
- Creating Cross-account Peering Connection

Cloud Connect Network (CCN)

You can establish communication between two or more VPCs using Cloud Connect Network (CCN), which supports both intra-account VPC connections and cross-account VPC connections (CCN also supports interconnection between VPCs and IDCs).

- Connecting Network Instances Under the Same Account
- Connecting Network Instances Across Accounts

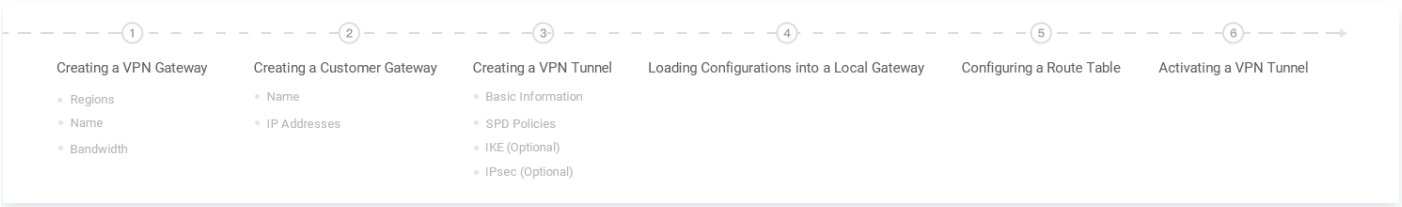
Connecting to Local IDCs

Last updated: 2024-01-12 14:26:27

You can establish communication between a VPC and a local IDC using VPN connection, Direct Connect or CCN. To learn more about connecting to a local IDC, please watch the following video.
Watch video

VPN connection

VPN connection is a method to connect your local IDC and VPC through an encrypted tunnel over a public network. A VPN connection consists of three components: 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 detailed instructions, please refer to VPN Connection – Quick Start Guide.

Direct Connect

Direct Connect connects a VPC and a local IDC through a connection. Direct Connect consists of three components: Connection, dedicated channel, and Direct Connect gateway. Users can connect to Tencent Cloud computing resources in multiple regions with a single connection, enabling flexible and reliable hybrid cloud deployment.
For details, see Direct Connect – Getting Started.

CCN

Cloud Connect Network (CCN) provides interconnection services between VPCs on the cloud and between a VPC and a local IDC, enabling communication among all VPCs and local IDCs.
For details, see Direct Connect – Connecting an IDC to the Cloud via CCN.

Connecting to the Classic Network

Last updated: 2024-01-12 14:26:34

The classic network is an earlier cloud network provided by Tencent Cloud. The VPC with an independent, controllable and more secure access are evolved from the classic network to meet the requirements of a growing number of users for more services. 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 solutions.

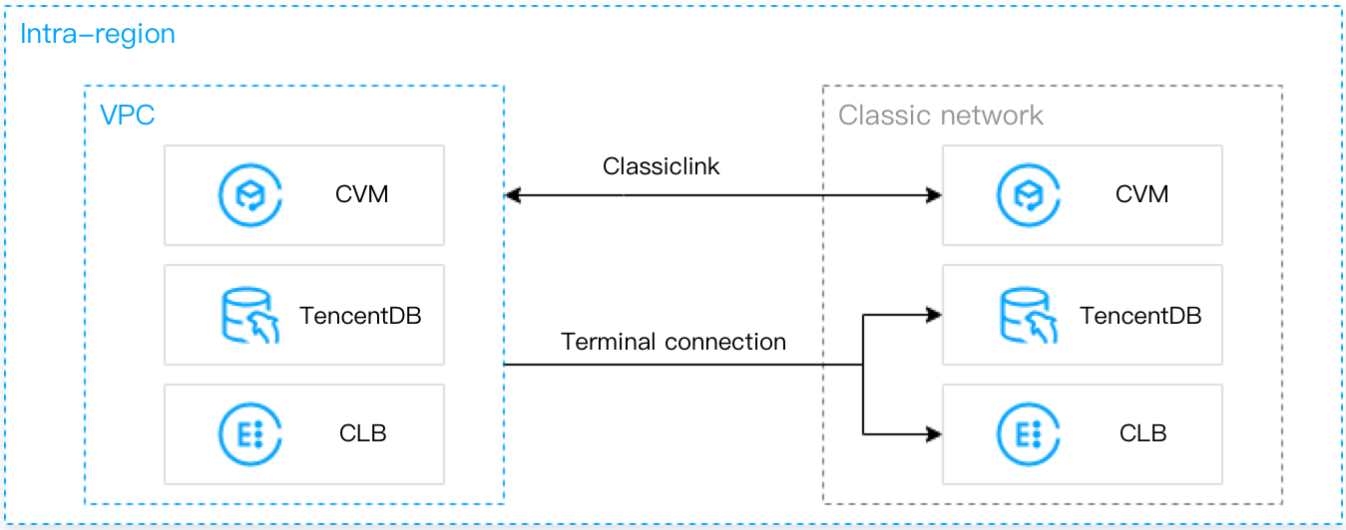
> **Note**
> For more information about the classic network, see Classic Network.

Establishing Communication between VPC and Classic Network

Tencent Cloud offers the two solutions for establishing communication between a VPC and the classic network.

- **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, the VPC-based CVMs can access the classic network-based CVMs rather than other cloud resources such as TencentDB and CLB instances in the classic network. For details, see ClassicLink.
- **Terminal connection**
  Terminal connection is a supplementary solution to **ClassicLink**. 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 the VPC IP address so that classic network instances can be accessed by accessing the VPC IP address. Classic network products that support terminal connection 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 contact the Online Consultation.



Migrating from the Classic Network to VPC

Tencent Cloud VPC offers you with secure network environment and flexible configuration options. It is recommended to migrate your applications in the classic network to a VPC. For more information, see Migrating from the Classic Network to VPC.

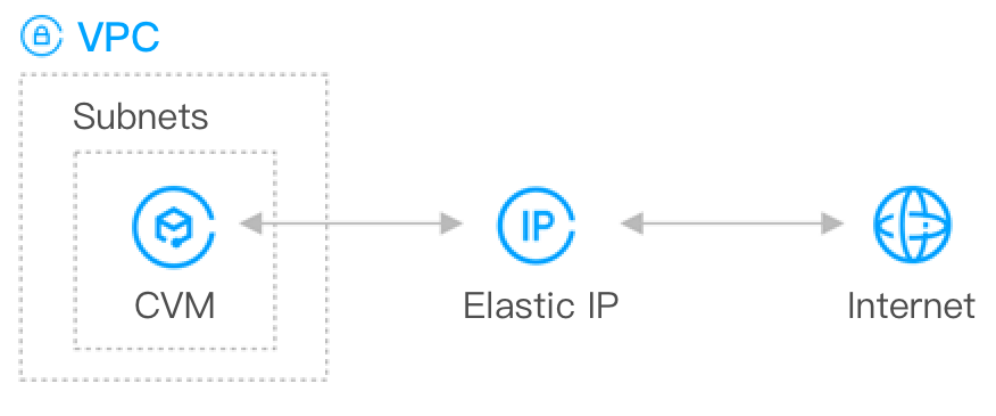
Building Up an IPv4 VPC

Last updated: 2024-01-12 14:26:40

This document describes how to quickly build up an IPv4 VPC.

Scenario

In this document, we will guide you through the whole process of building up a VPC that is with IPv4 CIDR blocks.



Preparations

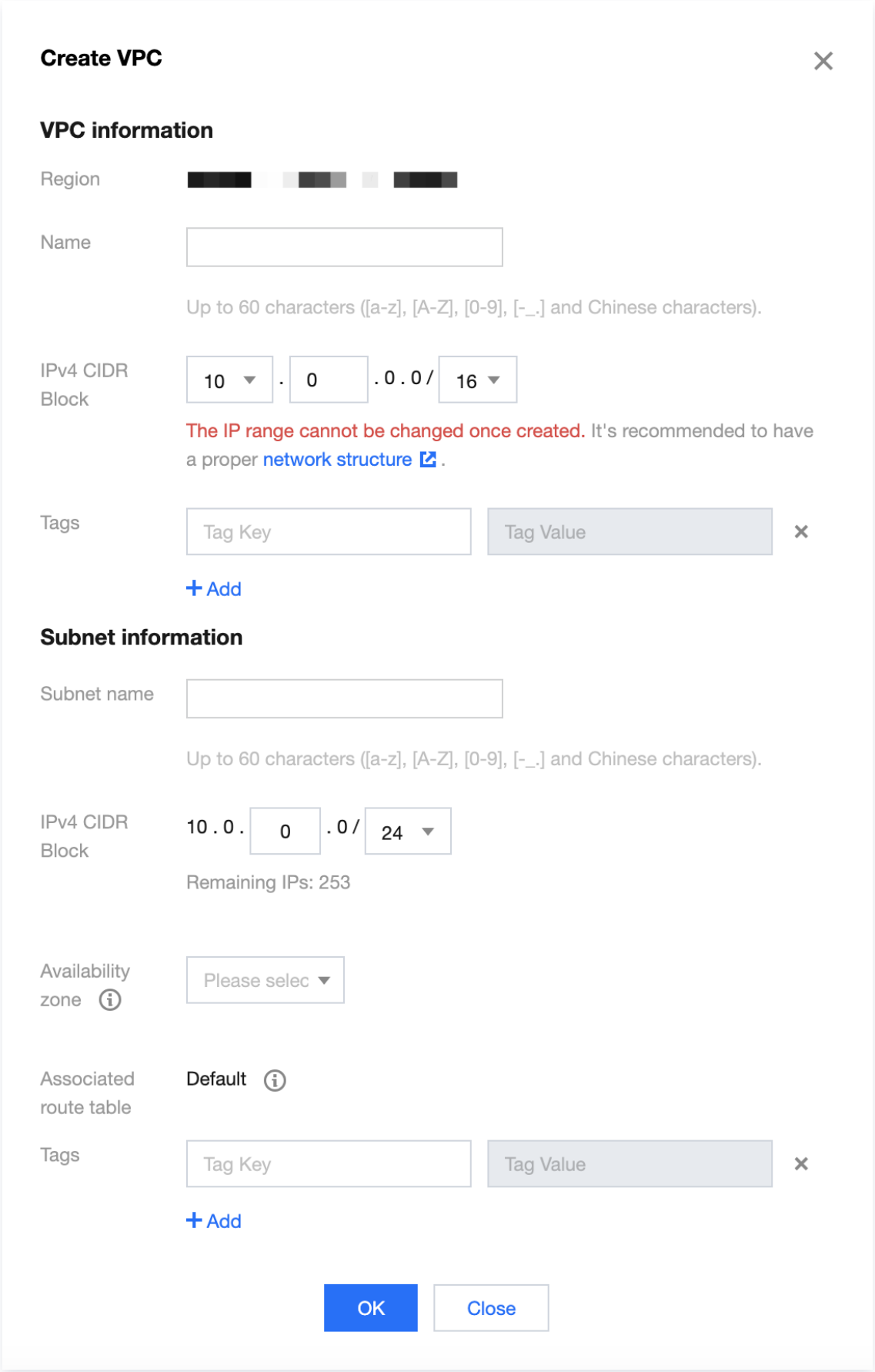
Before using Tencent Cloud products, create a Tencent Cloud account and complete identity verification.

Instructions

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 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, and then click **OK**.



- **VPC information**

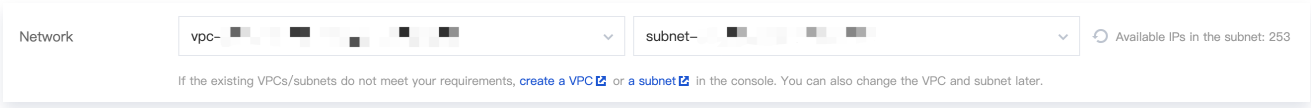
- Name: The name of the VPC.
- IPV4 CIDR block: You can choose any one of the IP ranges as the VPC IP range, such as `10.0.0.0/16`.
  - `10.0.0.0` – `10.255.255.255` (mask range: 12 to 28)
  - `172.16.0.0` – `172.31.255.255` (mask range: 12 to 28)
  - `192.168.0.0` – `192.168.255.255` (mask range: 16 to 28)
- Tags: You can optionally add tags to help you better manage resource permissions of sub-users and collaborators.

- **Subnet information**
  - IPv4 CIDR:
    - 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 via 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.

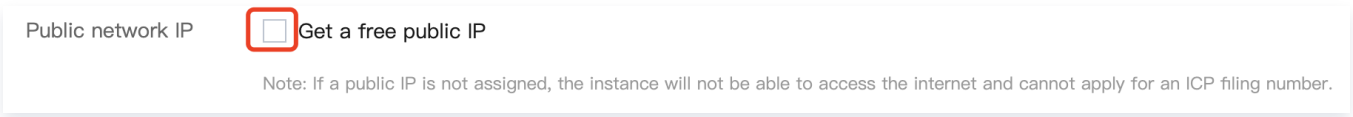
Step 2. Purchase a CVM instance

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:

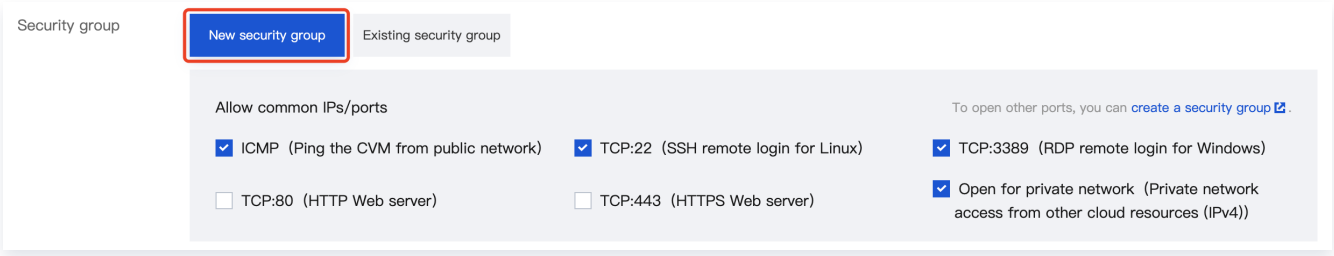
- Network: Select the created VPC and subnet.



- Public bandwidth: Do not select.



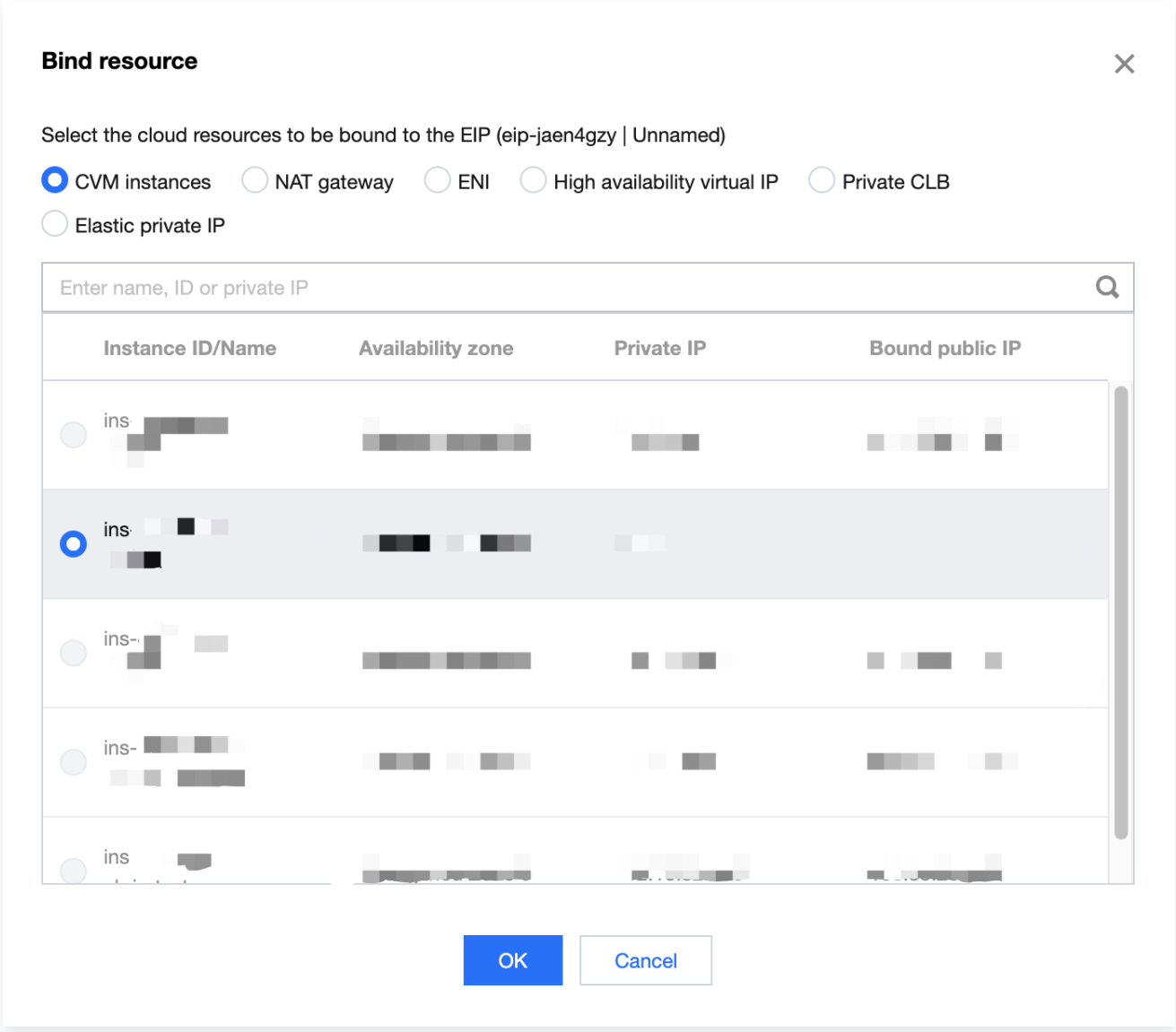
- Security group: Choose to create a new security group and configure it as instructed in Configuring Security Groups.



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 is located. Click **Apply**.
3. In the "Apply for EIP" pop-up window, configure the 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** pop-up window, select **CVM instances** as the resource type, locate the created CVM instance, and click **OK**.



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.

Quick Establishment of IPv6 VPC
Set up an IPv6 Private Network

Last updated: 2024-01-12 14:31:18

This document describes how to build up an IPv6-based Virtual Private Cloud (VPC), and enable IPv6 for CVMs in the VPC.

Scenario

- Enable IPv6 for a CVM and interconnect the CVM with other CVMs in the VPC via IPv6 over the private network.
- Enable IPv6 for Cloud Virtual Machines and facilitate bidirectional communication with IPv6 users on the Internet.

Preparations

The IPv6/IPv4 dual-stack VPC feature is currently in beta. To try it out, please submit an application.

Notes

- Before using Tencent Cloud products, create a Tencent Cloud account first.
- Currently, IPv6 is supported in the following regions: Beijing, Shanghai, Guangzhou, Shanghai Finance, Shenzhen Finance, Beijing Finance, Chengdu, Chongqing, Nanjing, Hong Kong (China), Singapore, and Virginia.
- Global Unicast Addresses (GUA) are used. Each VPC is assigned a `/56` IPv6 CIDR block, each subnet is assigned a `/64` IPv6 CIDR block, and each ENI is assigned a single IPv6 address.
- Both primary ENIs and secondary ENIs support IPv6 address. For more information, see ENI documentation.

Instructions

Step 1. Assign IPv6 CIDR block to the VPC

1. Log in to the VPC console.
2. Select an IPv6-supported region, and in the right-hand action column of the VPC row, choose **More** > **Edit IPv6 CIDR**.
3. In the **Edit IPv6 CIDR** dialog box, click **Get**, confirm the relevant information, and then click **OK**.

The system will assign a `/56` IPv6 address block to the VPC, and you can view the detailed information of the IPv6 address block in the list.

Step 2. Assign IPv6 CIDR block to the subnet

1. Log in to the VPC console.
2. Select **Subnet** on the left sidebar to enter the subnet list page.
3. In Step 1, under the operation column of the subnet belonging to the VPC, select **More** > **Obtain IPv6 CIDR** and confirm the action. The system will allocate a `/64` IPv6 CIDR from the VPC's `/56` IPv6 CIDR.

Step 3. Purchase a CVM instance and configure IPv6

After assigning an IPv6 CIDR block to the VPC and subnet, you need to create a CVM instance with an IPv6 address in that subnet, or obtain an IPv6 address for a running CVM instance in the subnet.

> **Notes**
> Since IPv6 addresses are not currently automatically assigned to ENIs, after obtaining an IPv6 address in the console, you need to log in to the CVM instance and configure the IPv6 address on its ENI.

1. Go to the CVM purchase page.
2. Complete configurations for the CVM instance on the custom configuration page. For more information, see Building Up an IPv4 VPC.

> **Notes**
> When selecting a model, please pay attention to the following parameters:
> - Regions: Beijing, Shanghai, Guangzhou, Shanghai Finance, Shenzhen Finance, Chengdu, Nanjing, Hong Kong (China), Singapore, Virginia.
> - Network: Select the VPC from Step 1 and the subnet from Step 2.
> - IPv6 address: Select **Allocate IPv6 addresses for free**.

3. Confirm your configuration and complete the purchase.
4. After successfully purchasing a Cloud Virtual Machine, you can view the IPv6 address information in the Cloud Virtual Machine Instance List.

> **Notes**
> - If the Cloud Virtual Machine was not assigned an IPv6 address during purchase, you can allocate an IPv6 address to the primary ENI by selecting **More** > **IP/ENI** >

Manage IPv6 Address in the corresponding Cloud Virtual Machine instance's operation column.

- To assign IPv6 addresses to other ENIs of the CVM instance, see Applying and Releasing IPv6 Addresses.

5. Log in to the CVM instance to configure IPv6. The configuration methods for IPv6 vary by the CVM operating systems. For details, see Configuring IPv6 for Linux CVMs and Configuring IPv6 for Windows CVMs.

Step 4. Enable public network access for the IPv6 address of the CVM

By default, the IPv6 address of a CVM instance only has private network access capabilities. If you want to access to or be accessed from the public network through the IPv6 address, you need to enable public network access for the IPv6 address using an elastic public IPv6.

1. Log in to the VPC console.
2. On the left sidebar in the console, select **IP and ENI** > **Elastic Public IPv6**.
3. Select the region where the CVM instance is located, and click **Apply**.
4. On the page that appears, select the IPv6 address for the CVM instance, set the target bandwidth limit, and click **Submit**.

Notes

- When a CVM instance is assigned an IPv6 address, public network access is disabled by default. You can manage IPv6 public network access. For details, see Managing IPv6 Public Network Access.
- When the ISP type is BGP, the elastic public IPv6 address is the IPv6 address obtained by the CVM instance. You need to ensure that the CVM instance has already obtained an IPv6 address.
- You can enable public network access for up to 100 IPv6 addresses simultaneously. Operate in batches if there are more than 100 IPv6 addresses.

Step 5. Configure security group rules for IPv6

Notes

- Inbound and outbound security group rules support configuring the source to be a single IPv6 address or IPv6 CIDR block, where `::/0` represents all IPv6 source addresses.
- For more information on security groups, see Security Group and Instance Port Verification.

1. Log in to the VPC console.
2. On the left sidebar, select **Security** > **Security Group**, and click the ID of the security group bound to the CVM instance to enter the details page.
3. Add inbound and outbound rules on the details page:
   - Select **Inbound rules** > **Add rule**, add an IPv6 inbound security group rule, and click **OK**.
   - Select **Outbound rules** > **Add rule**, add an IPv6 outbound security group rule, and click **OK**.

Step 6. Test IPv6 connectivity

The following sections describe how to test IPv6 connectivity for Linux CVMs and Windows CVMs.

Notes

- To test public network connectivity, ensure that you have configured IPv6 policies in "Security Group" and configured IPv6 public bandwidth in **Elastic Public IPv6**.
- If the subnet where the CVM instance resides is associated with a network ACL, you also need to configure an IPv6 policy in the corresponding network ACL. To enable additional IPv6 public network access capabilities, please submit a ticket.
- If IPv6 public network access is not enabled, and you need to test the connectivity of IPv6 CVMs (Ping, SSH, RDP), you can use another CVM with an IPv6 address in the same VPC for connectivity test.
- If the Cloud Virtual Machine image has IPv6 enabled, the system will automatically assign a link-local address starting with "FE80" to each ENI. However, this link-local address cannot be used as an IPv6 address for internal and external communication.
- We recommend that you select a nearby test point for Ping tests.

Linux CVM

Linux Cloud Virtual Machines can test IPv6 connectivity through operations such as Ping or SSH.

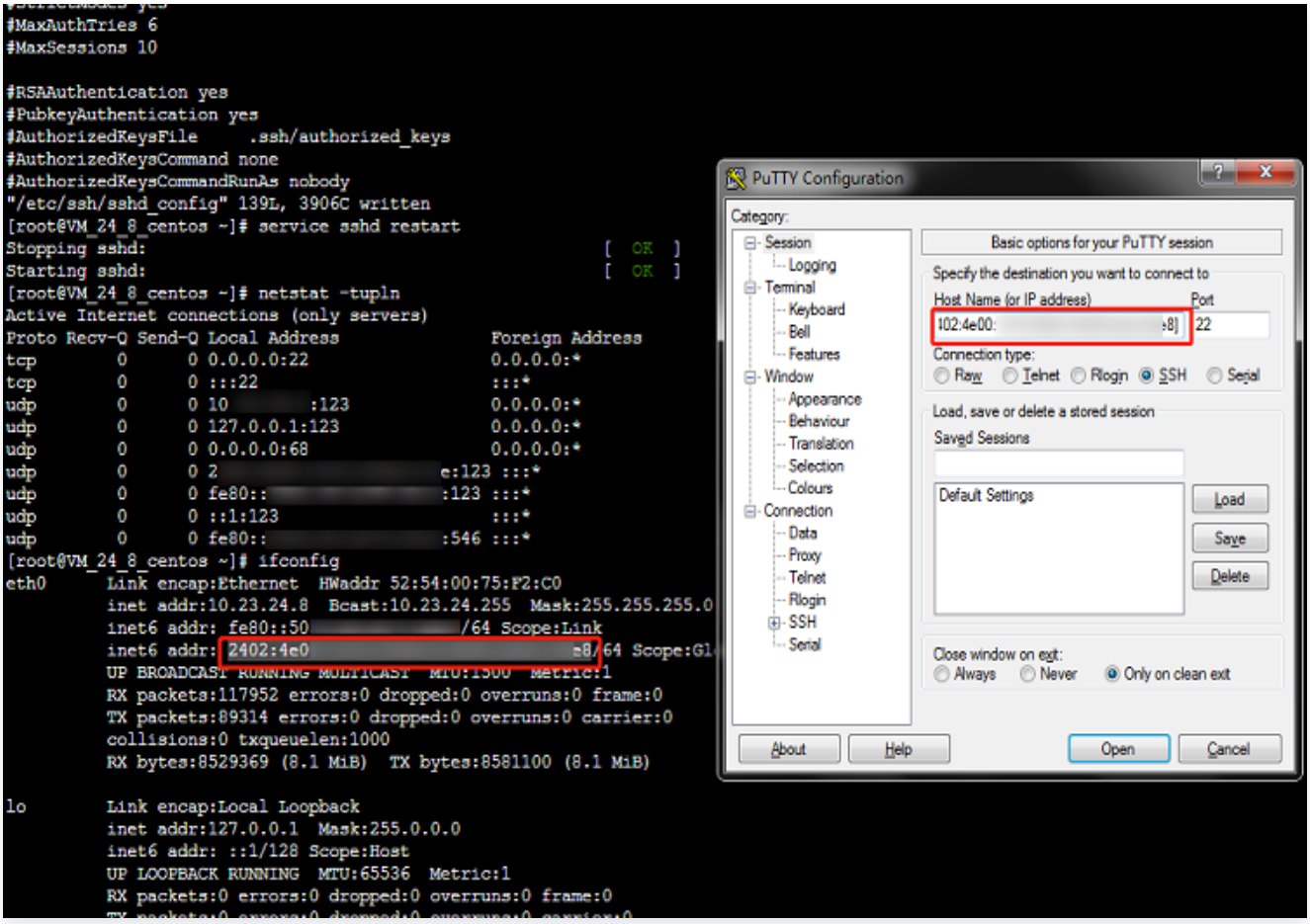
- **Method 1:** Conduct a test using Ping, as follows:
  Execute `ping6 IPv6 address` in the Cloud Virtual Machine for testing, for instance, `ping6 240c::6666`, `ping6 www.qq.com`, `ping6 IPv6 address under the same private network`. The successful result is shown in

the following figure:

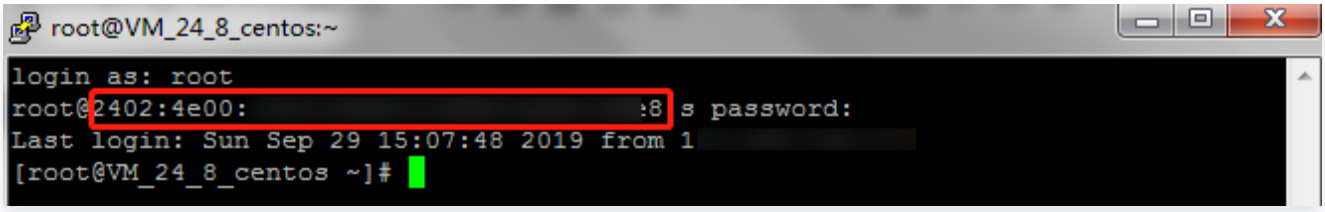
```
[root@VM-25-3-centos ~]# ping6 240c::6666
PING 240c::6666(240c::6666) 56 data bytes
64 bytes from 240c::6666: icmp_seq=1 ttl=53 time=10.3 ms
64 bytes from 240c::6666: icmp_seq=2 ttl=53 time=10.3 ms
^C
--- 240c::6666 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 10.264/10.285/10.306/0.021 ms
[root@VM-25-3-centos ~]# ping6 www.qq.com
PING www.qq.com(2402:4e00:1020:1404:0:9227:71a3:83d2 (2402:4e00:1020:1404:0:9227:71a3:83d2)) 56 data bytes
64 bytes from 2402:4e00:1020:1404:0:9227:71a3:83d2 (2402:4e00:1020:1404:0:9227:71a3:83d2): icmp_seq=1 ttl=55 time=27.0 ms
64 bytes from 2402:4e00:1020:1404:0:9227:71a3:83d2 (2402:4e00:1020:1404:0:9227:71a3:83d2): icmp_seq=2 ttl=55 time=27.0 ms
64 bytes from 2402:4e00:1020:1404:0:9227:71a3:83d2 (2402:4e00:1020:1404:0:9227:71a3:83d2): icmp_seq=3 ttl=55 time=27.0 ms
^C
--- www.qq.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 27.005/27.018/27.046/0.190 ms
[root@VM-25-3-centos ~]#
```

- **Method 2:** SSH into the Cloud Virtual Machine via IPv6 address as follows:
  Execute the command below to view the IPv6 address, and use software such as PuTTY or Xshell to test whether you can SSH into the Cloud Virtual Machine via the IPv6 address.

```
ifconfig
```



The following figure shows the successful result.



Windows CVM instances

Windows Cloud Virtual Machines can test IPv6 connectivity using Ping or Remote Desktop.

- **Method 1**: Test using Ping, as follows:

  In the operating system interface, select the bottom-left corner, click, open the **Windows PowerShell** window, and execute `ping -6 IPv6 address` for testing, for example, `ping -6 240c::6666` or `ping -6 IPv6 address within the same Virtual Private Cloud`. Success is shown in the image below.
- **Method 2**: Use an IPv6 address for remote desktop access. For detailed remote desktop operations, please refer to Logging in to a Windows Instance Using Remote Desktop Connection.