

# Virtual Private Cloud

## Início rápido

### 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

 Tencent Cloud

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

## Início rápido

- Planejamento de rede

- Conexões do VPC

  - Conexão à internet

  - Conexão a outras instâncias do VPC

  - Conexão a IDCs locais

  - Comunicação com a rede clássica

- Criação de uma VPC IPv4

# Início rápido

## Planejamento de rede

Last updated : 2024-01-24 17:44:04

Antes de iniciar a expansão da rede e a criação do seu VPC, é necessário planejar a quantidade e os intervalos de IP do VPC de acordo com suas necessidades de negócios.

[Como planejar a quantidade de VPCs?](#)

[Como planejar a quantidade de sub-redes?](#)

[Como planejar os intervalos de IP \(blocos CIDR\) de VPCs e sub-redes?](#)

[Como planejar a quantidade de tabelas de rotas?](#)

[Como planejar uma rede de nuvem híbrida multicêntrica entre regiões?](#)

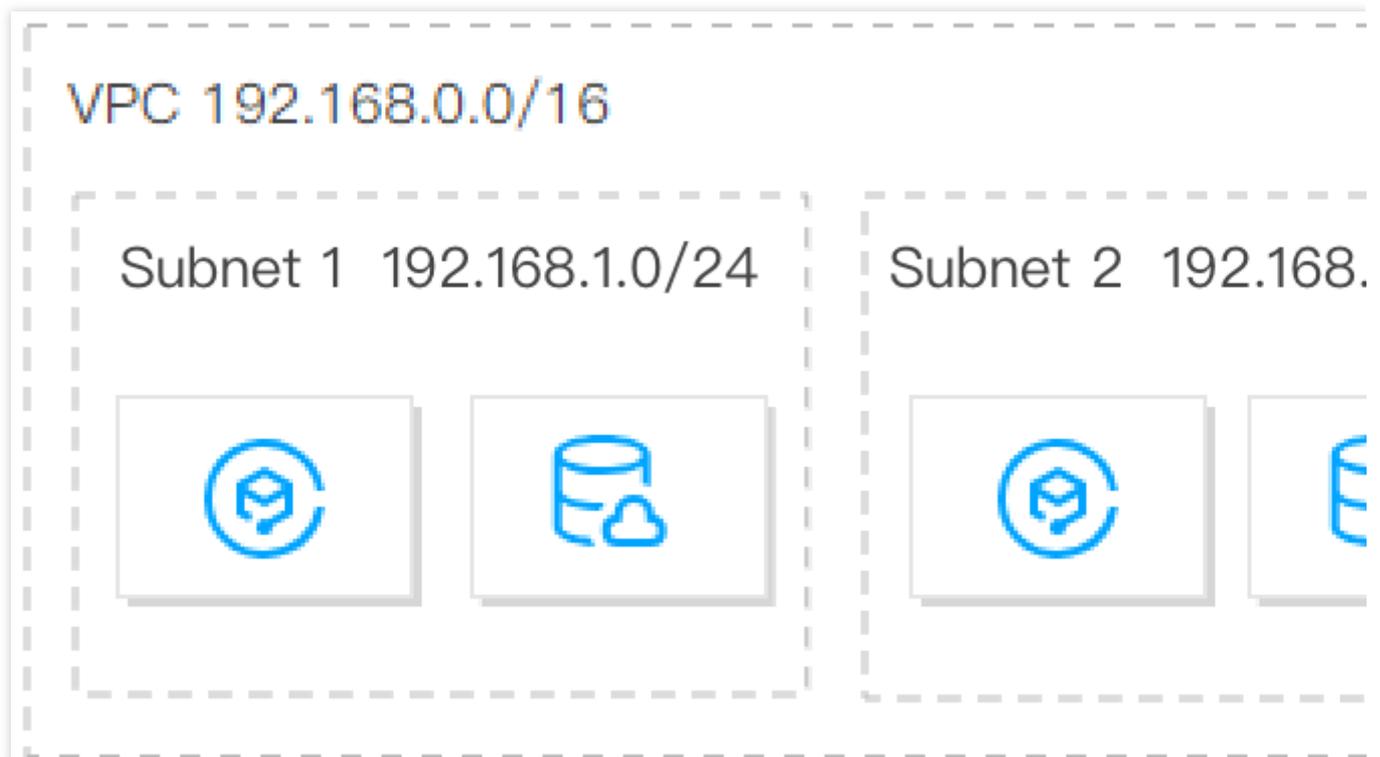
## Como planejar a quantidade de VPCs?

### Planejamento de um VPC

Se você tiver um negócio de pequeno porte implantado na mesma região sem a necessidade de isolamento de rede, recomendamos que você planeje um VPC.

É possível criar várias sub-redes e tabelas de rotas em um único VPC para gerenciamento de tráfego detalhado.

Além disso, recomendamos que você implante sub-redes em zonas de disponibilidade diferentes para a recuperação de desastre delas.



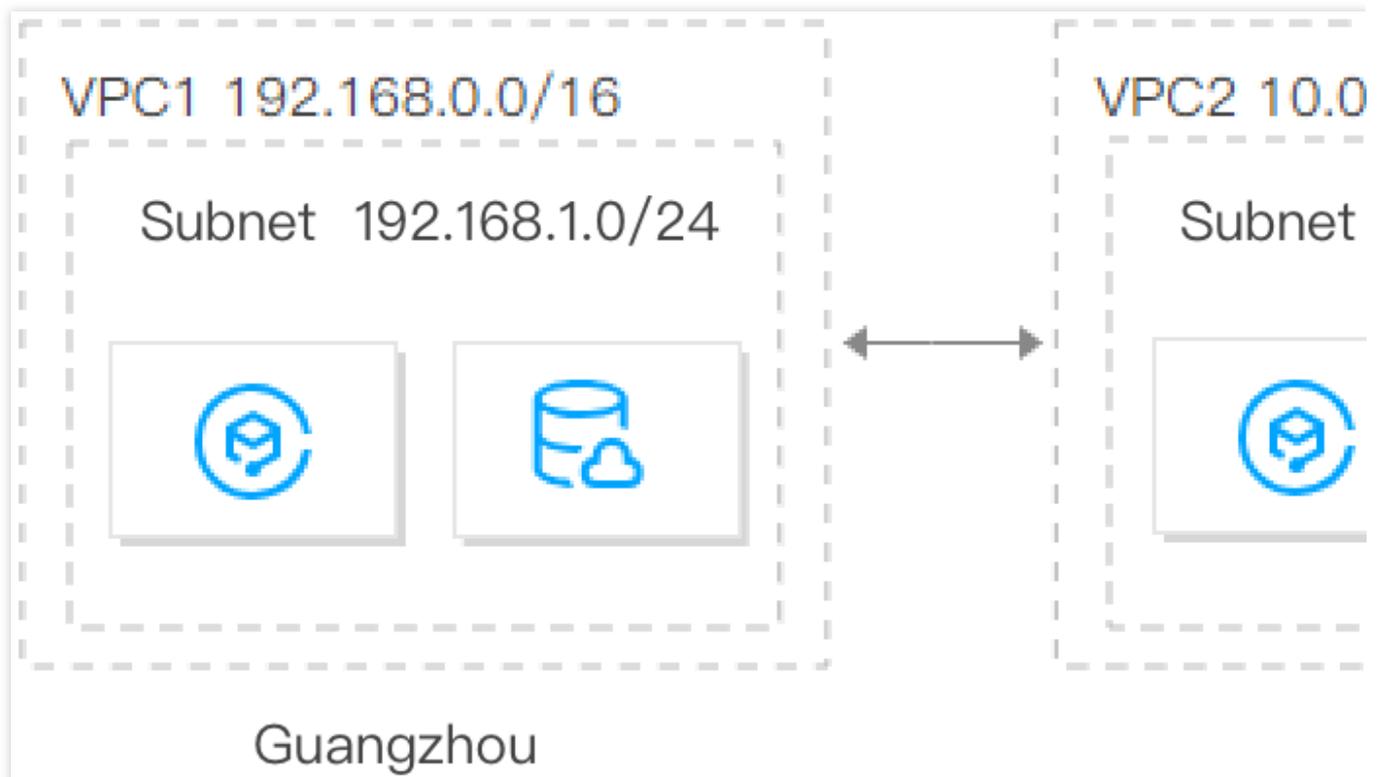
### Planejamento de vários VPCs

Recomendamos que você planeje vários VPCs em qualquer um dos seguintes cenários:

#### Seu negócio está implantado em várias regiões

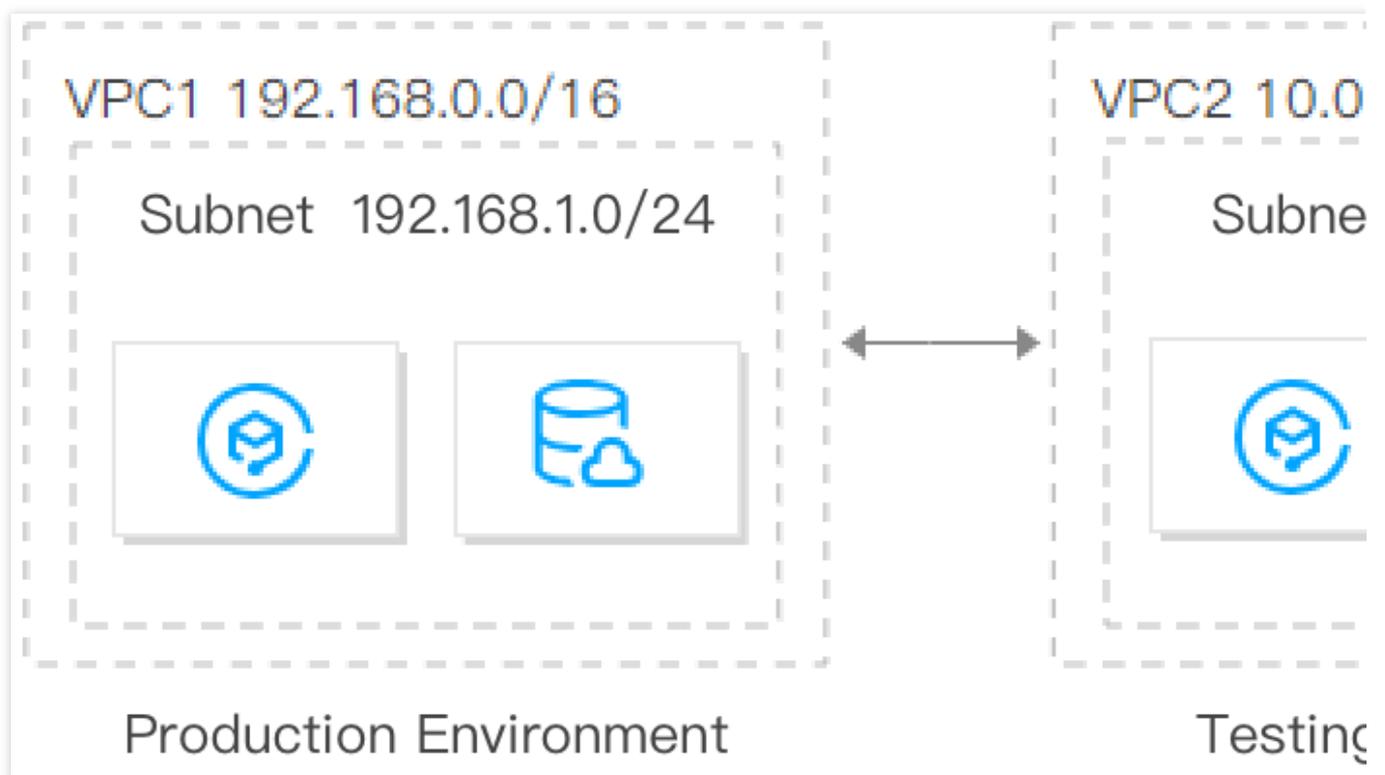
Se seu negócio estiver implantado em várias regiões, será necessário planejar vários VPCs e implantar pelo menos um em cada região, porque um VPC não pode ser implantado em mais de uma região.

Por padrão, os VPCs não são interconectados. Para interconectar os VPCs, use o [Peering Connection](#) ou o [Cloud Connect Network](#).



#### Vários negócios estão implantados na mesma região e exigem isolamento

Se você tiver vários negócios implantados na mesma região e eles precisarem ser isolados uns dos outros, será necessário planejar vários VPCs e implantar um VPC para cada negócio. Isso pode isolar os negócios, pois os VPCs não são interconectados por padrão.



## Como planejar a quantidade de sub-redes?

Um VPC pode ter várias (100, por padrão) sub-redes. Sub-redes diferentes no mesmo VPC podem se comunicar entre si por meio de uma rede privada, por padrão.

Para ter acesso a recuperação de desastre em zonas de disponibilidade, recomendamos que crie pelo menos duas sub-redes em zonas de disponibilidade diferentes para um VPC.

## Como planejar os intervalos de IP (blocos CIDR) de VPCs e sub-redes?

**Depois de definidas, as máscaras de intervalo de IP dos VPCs e das sub-redes não podem ser modificadas.** Portanto, planeje cuidadosamente os VPCs e as sub-redes com base em sua escala de negócios e cenários de comunicação. Isso facilitará um dimensionamento e operações perfeitos no futuro.

### Planejamento de intervalos de IP do VPC

**Você pode usar qualquer um dos seguintes intervalos de IP como seus intervalos de IP do VPC:**

**10.0.0.0 - 10.255.255.255 (o intervalo das máscaras deve ser de 16 a 28)**

**172.16.0.0 - 172.31.255.255 (o intervalo das máscaras deve ser de 16 a 28)**

**192.168.0.0 - 192.168.255.255 (o intervalo das máscaras deve ser de 16 a 28)**

**Ao planejar intervalos de IP do VPC, observe que:**

Se você precisar criar vários VPCs que se comunicam entre si ou com IDCs, certifique-se de que os intervalos de IP dos VPCs não se sobreponham.

Se seu VPC precisar se comunicar com a rede clássica, o intervalo de IP do VPC que você criar deve estar dentro de

`10.[0-47].0.0/16` (incluindo os subconjuntos).

Depois de criados, os blocos CIDR dos VPCs e das sub-redes não podem ser modificados. Quando os blocos CIDR forem insuficientes, é possível [criar blocos CIDR auxiliares](#).

### Planejamento de intervalos de IP da sub-rede

**Intervalo de IP da sub-rede:** é possível usar seu intervalo de IP do VPC ou parte dele como o intervalo de IP da sub-rede. Por exemplo, se o intervalo de IP do VPC for 10.0.0.0/16, o intervalo de IP da sub-rede pode estar entre 10.0.0.0/16-10.0.255.255/28.

**Tamanho da sub-rede e capacidade de IP:** depois de criadas, as sub-redes não podem ser modificadas. Ao criar sub-redes, certifique-se de que os intervalos de IP da sub-rede conseguem atender às suas necessidades de negócios. No entanto, também é necessário controlar o tamanho da sub-rede, com a possibilidade de criar sub-redes posteriormente para a expansão.

**Requisitos de negócios:** um único VPC pode ser dividido em sub-redes com base em segmentos de negócios. Por exemplo, você pode implantar a camada da web, a camada lógica e a camada de dados em sub-redes diferentes e

usar [ACLs de rede](#) para implementar o controle de acesso.

**Nota:**

Se o VPC em que as sub-redes estiverem localizadas precisar se comunicar com outros VPCs ou IDCs, certifique-se de que o intervalo de IP da sub-rede não se sobreponha ao intervalo de IP de par. Caso contrário, a interconexão por meio de uma rede privada pode falhar.

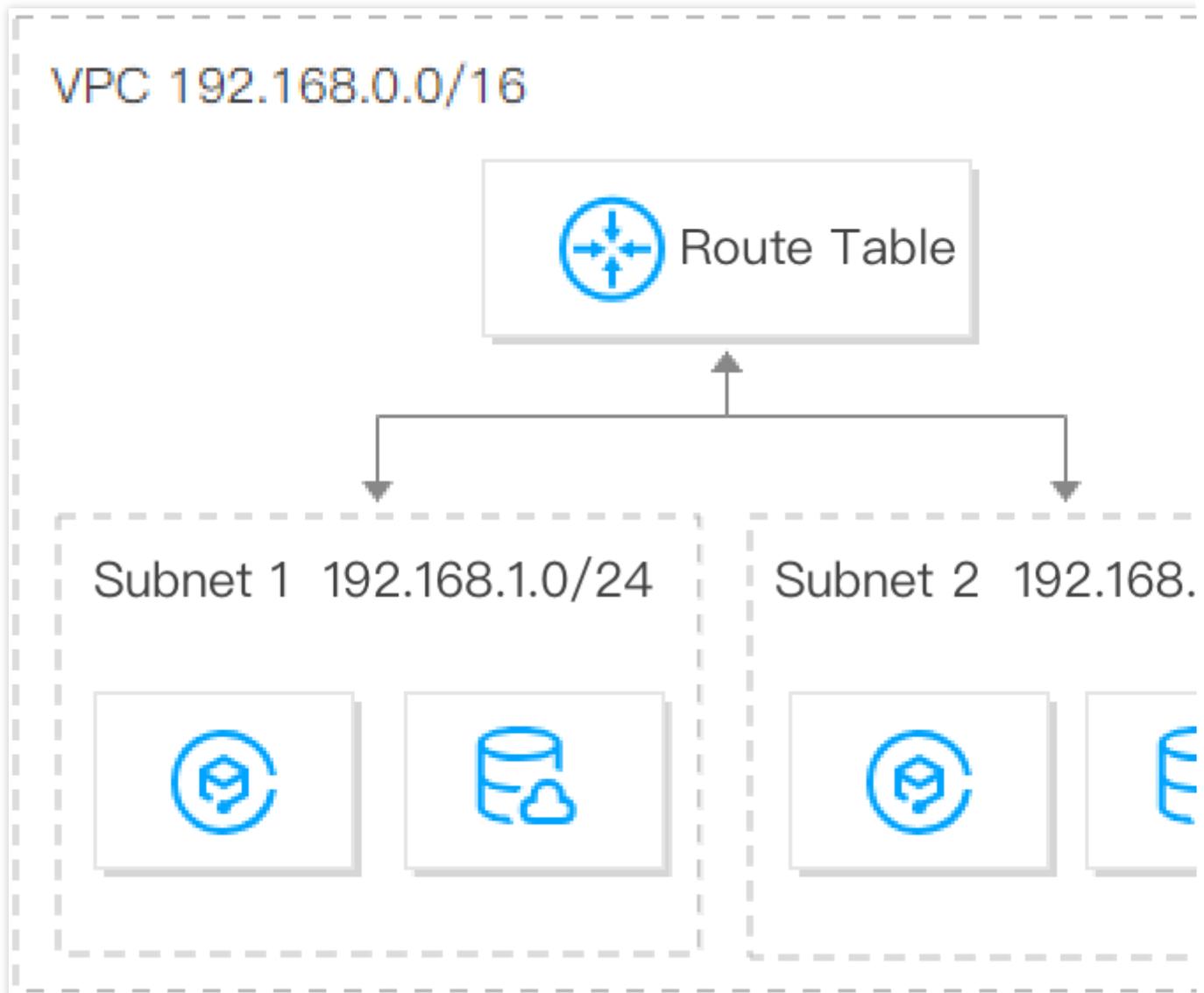
Se os intervalos de IP da sub-rede se sobrepuerem, você pode [alterar a sub-rede da instância](#) e usar o CCN ou criar um VPC novo e adquirir CVMs.

## Como planejar a quantidade de tabelas de rotas?

Uma tabela de rotas é usada para controlar a direção do tráfego em uma sub-rede. Cada sub-rede só pode ser vinculada a uma tabela de rotas. Você pode usar a tabela de rotas padrão e tabelas de rotas personalizadas nos VPCs do Tencent Cloud.

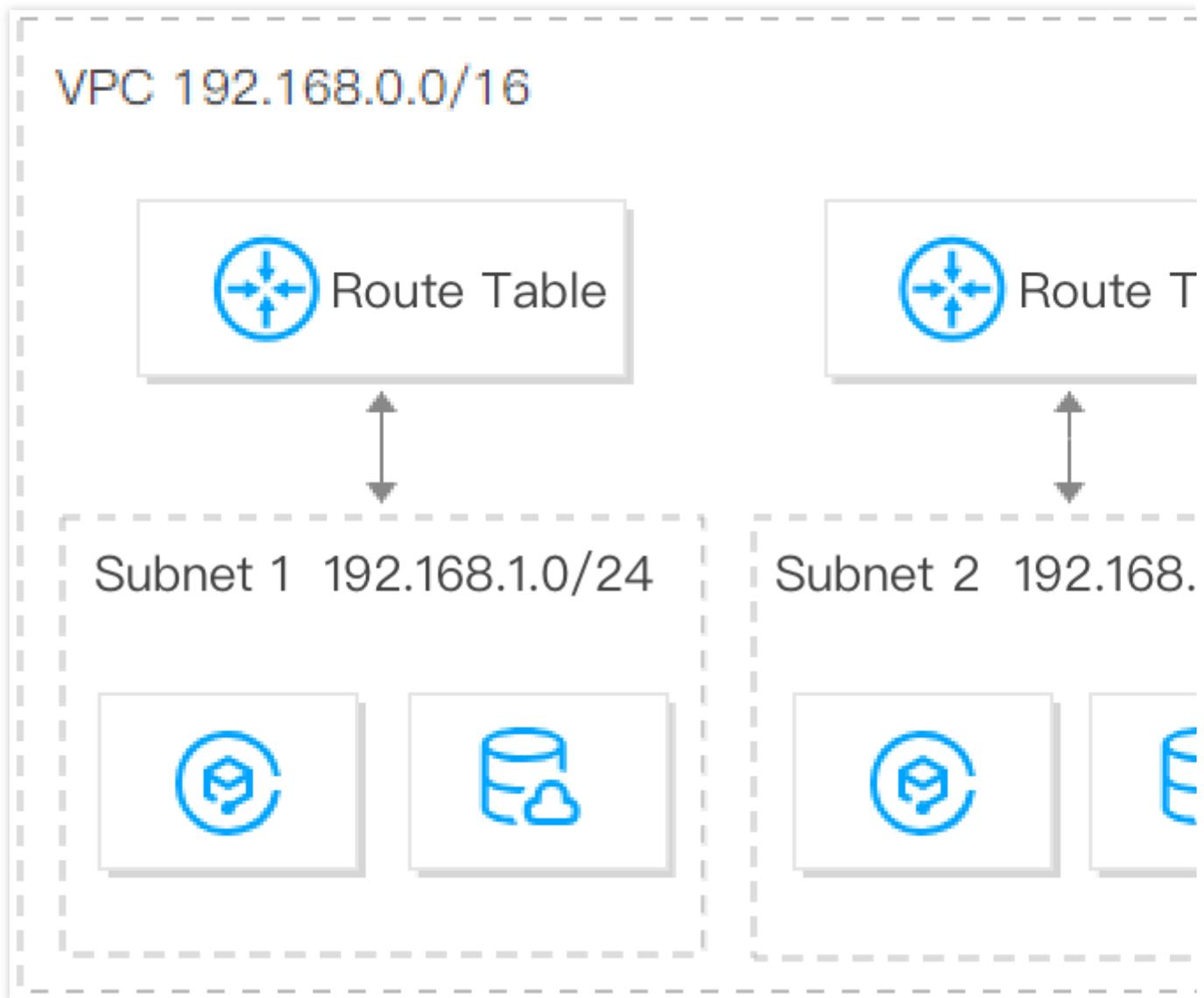
**Planejamento de uma tabela de rotas**

Se sub-redes diferentes em seu VPC tiverem requisitos iguais ou semelhantes para a direção do tráfego, recomendamos o planejamento de uma tabela de rotas. Em seguida, você pode criar políticas de roteamento diferentes para controlar a direção do tráfego.



### Planejamento de várias tabelas de rotas

Se as sub-redes em seu VPC tiverem requisitos diferentes para a direção do tráfego, recomendamos o planejamento de várias tabelas de rotas. Em seguida, você pode vinculá-las às sub-redes correspondentes e criar políticas de roteamento para controlar a direção do tráfego.

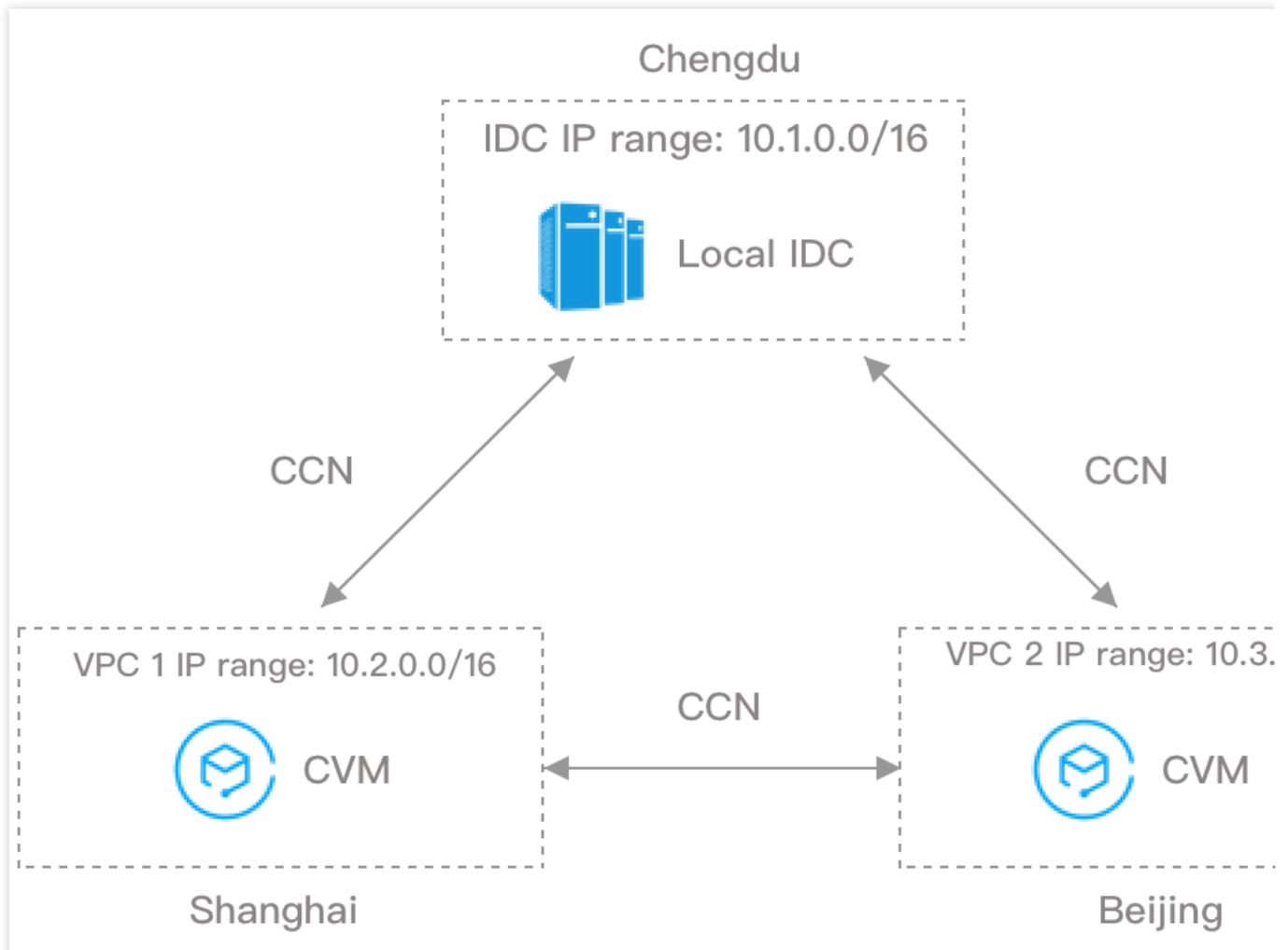


## Como planejar uma rede de nuvem híbrida multicêntrica entre regiões?

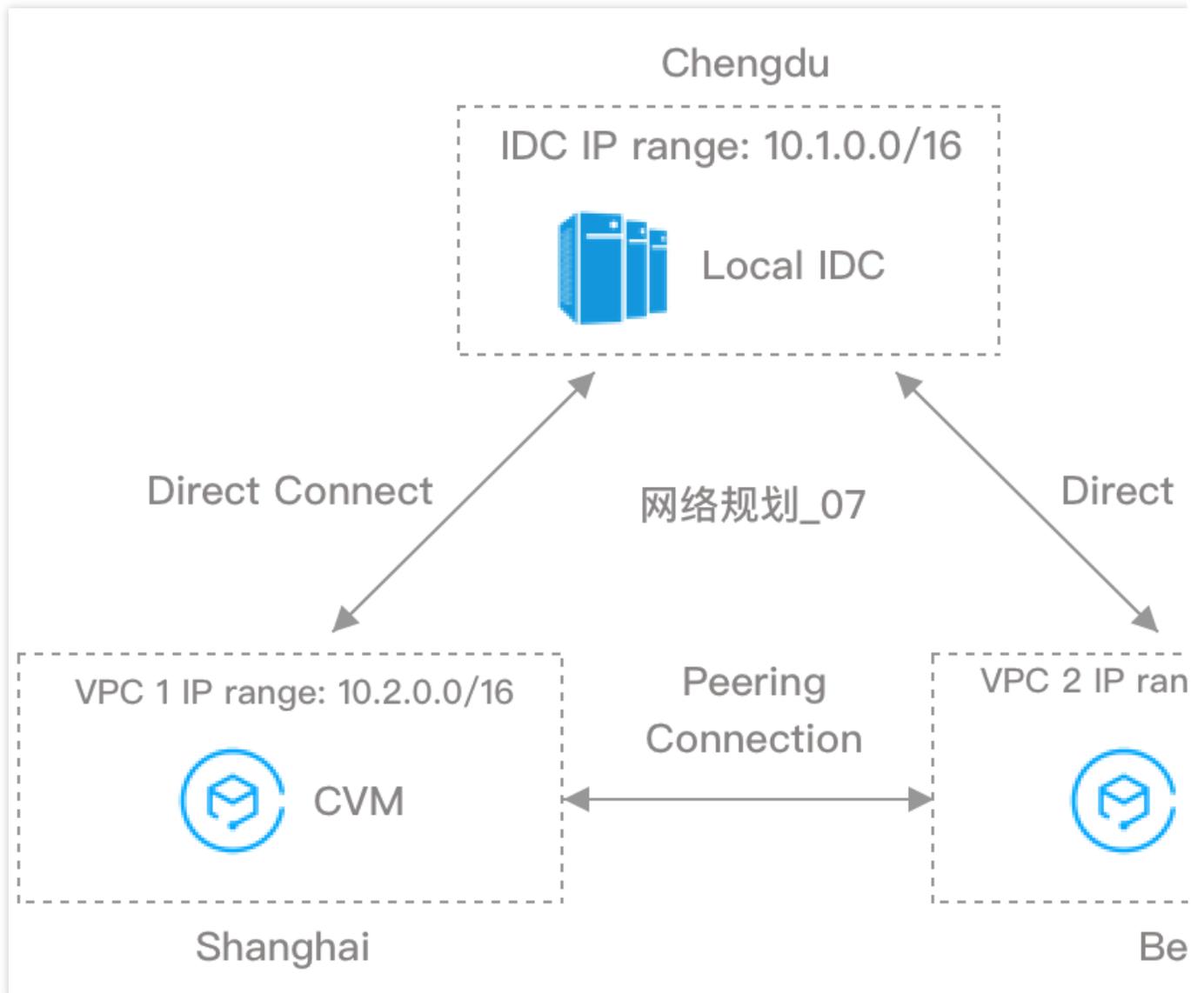
Se você precisar criar vários VPCs que se comunicam entre si ou com IDCs, certifique-se de que os intervalos de IP dos VPCs não se sobreponham ao intervalo de IP de par.

Suponha que você tenha um IDC local com intervalo de IP `10.1.0.0/16` em Chengdu e deseja criar dois IDCs em nuvem em Xangai e Pequim, que precisam se comunicar com seu IDC local. Nesse caso, recomendamos que você use `10.2.0.0/16` e `10.3.0.0/16` como os intervalos de IP do VPC dos dois IDCs de nuvem em Xangai e Pequim, respectivamente, para evitar falha de comunicação causada por intervalos de IP sobrepostos. Você pode habilitar a comunicação entre IDC local e IDCs de nuvem e entre os IDCs de nuvem usando os dois métodos abaixo.

**Método 1:** adicione-os a um CCN para implementar a interconexão na rede pública e privada.



**Método 2:** use o Direct Connect para conectar os IDCs de nuvem em Xangai e Pequim ao IDC local em Chengdu, permitindo assim a comunicação entre o IDC local e os IDCs de nuvem. Para permitir a comunicação entre os IDCs de nuvem em Xangai e Pequim, use o Peering Connection para conectar os VPCs correspondentes.



### Sugestões para casos de uso de vários VPCs:

Tente planejar intervalos de IP diferentes para cada VPC.

Tente planejar intervalos de IP diferentes para sub-redes do VPC se cada VPC não puder ter um intervalo de IP distinto.

Certifique-se de que os intervalos de IP das sub-redes que precisam se comunicar sejam diferentes se cada sub-rede não puder ter um intervalo de IP distinto.

## Documentação

Para obter mais informações sobre como criar um Virtual Private Cloud (VPC) com bloco CIDR IPv4 de forma rápida, incluindo a criação de um VPC e uma sub-rede, a aquisição de um CVM e a vinculação de um EIP para permitir o acesso à rede pública, consulte [Criação de um VPC IPv4](#).

# Conexões do VPC

## Conexão à internet

Last updated : 2024-01-24 17:44:05

O Tencent Cloud fornece vários métodos para acessar a internet, como por meio de um endereço IP público comum, EIP, NAT Gateway e Cloud Load Balancer (CLB).

## Endereços IP públicos comuns

Ao criar uma instância do CVM, é possível atribuir um endereço IP público comum à instância. O sistema atribuirá um endereço IP ao seu CVM para permitir que ele acesse a internet e seja acessível pela internet.

Os endereços IP públicos comuns não podem ser vinculados ou desvinculados dinamicamente a recursos como CVMs, mas é possível convertê-los em EIPs. Para obter detalhes, consulte [Conversão de endereços IP públicos em EIPs](#).

## Endereços IP elásticos

Diferente dos endereços IP públicos que precisam ser solicitados e liberados com os CVMs, os endereços IP elásticos (EIPs) são recursos de nuvem independentes que são desacoplados do ciclo de vida do CVM e podem ser operados separadamente.

Para obter informações sobre como solicitar, vincular e liberar EIPs, consulte [EIPs – Etapas](#).

Os EIPs oferecem as seguintes vantagens:

Recursos de nuvem independentes

É possível operar EIPs de forma independente, sem a necessidade de adquiri-los com os CVMs.

Vinculação e desvinculação elástica de recursos

Os EIPs podem ser vinculados e desvinculados dos CVMs e de outros recursos a qualquer momento.

## NAT Gateways

Um NAT Gateway fornece as funcionalidades SNAT e DNAT, o que permite estabelecer facilmente uma saída de internet e fornecer serviços para os CVMs em um VPC, a fim de acessar a internet com o mesmo endereço IP público.

Para obter informações sobre como configurar o NAT Gateway, consulte [NAT Gateways – Visão geral da operação](#).

Os NAT Gateways oferecem as seguintes vantagens:

### Acesso seguro à internet

Os NAT Gateways fornecem os recursos SNAT e DNAT para ocultar os endereços IP dos CVMs em um VPC durante a comunicação pela internet, garantindo a segurança.

### Alta disponibilidade

Os NAT Gateways oferecem backup dinâmico mestre/escravo, permutação a quente automática e encaminhamento rápido com uma taxa de até 5 Gbps. Além disso, eles são compatíveis com aplicativos de internet em grande escala.

### Configuração flexível

É possível modificar as especificações do NAT Gateway conforme necessário e a qualquer momento.

## Cloud Load Balancers

Um Cloud Load Balancer (CLB) distribui o tráfego para vários CVMs, a fim de aprimorar os recursos de serviço externo dos sistemas de aplicativos. Ele elimina pontos únicos de falha para garantir sistemas de aplicativos altamente disponíveis.

Para obter informações sobre como adquirir e configurar um CLB, consulte [CLBs – Introdução](#).

Os CLBs oferecem as seguintes vantagens:

### Cluster único de alto desempenho

Um cluster do CLB consiste em vários servidores físicos, com uma disponibilidade de até 99,95%. O sistema de clusters pode remover instâncias com falha e selecionar instâncias em bom funcionamento para garantir a execução adequada dos serviços no servidor real.

### Alta segurança e estabilidade

Com o sistema anti-DDoS do BGP, o CLB pode se defender contra a maioria dos ataques de rede (como ataques DDoS) e limpar ataques de tráfego em segundos, evitando endereços IP bloqueados ou consumo total da largura de banda.

## Gateways públicos

Um gateway público é um CVM com a funcionalidade de encaminhamento habilitada. Em um VPC, os CVMs sem um endereço IP público conseguem acessar a internet por meio de gateways públicos em sub-redes diferentes. Os gateways públicos podem converter os endereços de origem do tráfego da internet de outros CVMs para seus próprios endereços IP.

Para obter informações sobre como configurar um gateway público, consulte [Configuração de gateways públicos](#).

# Conexão a outras instâncias do VPC

Last updated : 2024-01-24 17:44:04

É possível conectar instâncias diferentes do VPC por meio do Peering Connection ou do CCN.

## Peering Connections

É possível estabelecer [Peering Connections](#) para interconectar duas instâncias do VPC na mesma conta ou em contas diferentes.

[Criação de um Peering Connection para comunicação do VPC dentro da conta](#)

[Criação de um Peering Connection para comunicação do VPC entre contas](#)

## CCNs

É possível usar um [CCN](#) para interconectar duas ou mais instâncias do VPC. Um CCN permite a interconexão entre instâncias do VPC da mesma conta ou de contas diferentes e interconexão entre instâncias do VPC e IDCs.

[Interconexão entre instâncias de rede na mesma conta](#)

[Interconexão entre instâncias de rede em contas diferentes](#)

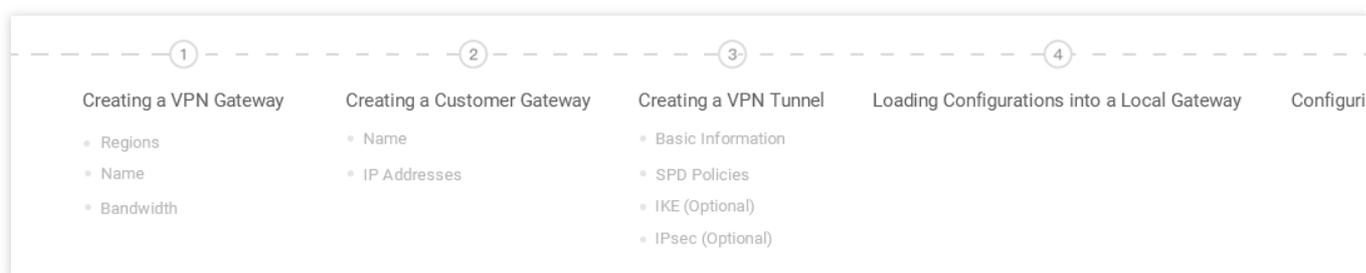
# Conexão a IDCs locais

Last updated : 2024-01-24 17:44:04

Você pode estabelecer um VPN Connection, conexão direta ou CCN para implementar a comunicação entre suas instâncias do VPC e os IDCs locais.

## VPN Connections

Um [VPN Connection](#) é um método para conectar seus IDCs e instâncias do VPC por meio de túneis criptografados de rede pública. Um VPN Connection consiste em três partes: gateway VPN, gateway do cliente e túnel VPN. Cada gateway VPN pode estabelecer vários túneis VPN e cada túnel VPN pode se conectar a um IDC local.



Para obter informações detalhadas sobre as operações, consulte [VPN Connections – Introdução](#).

## Conexões diretas

Uma [conexão direta](#) é uma conexão física direta que conecta instâncias do VPC e IDCs locais. Uma conexão direta consiste em três partes: conexão física, túnel dedicado e gateway do Direct Connect.

Os usuários podem estabelecer uma conexão física para conectar os recursos de computação do Tencent Cloud em várias regiões, obtendo uma implantação de nuvem híbrida flexível e confiável.



Para obter informações detalhadas sobre as operações, consulte [Direct Connect – Introdução](#).

## Cloud Connect Networks

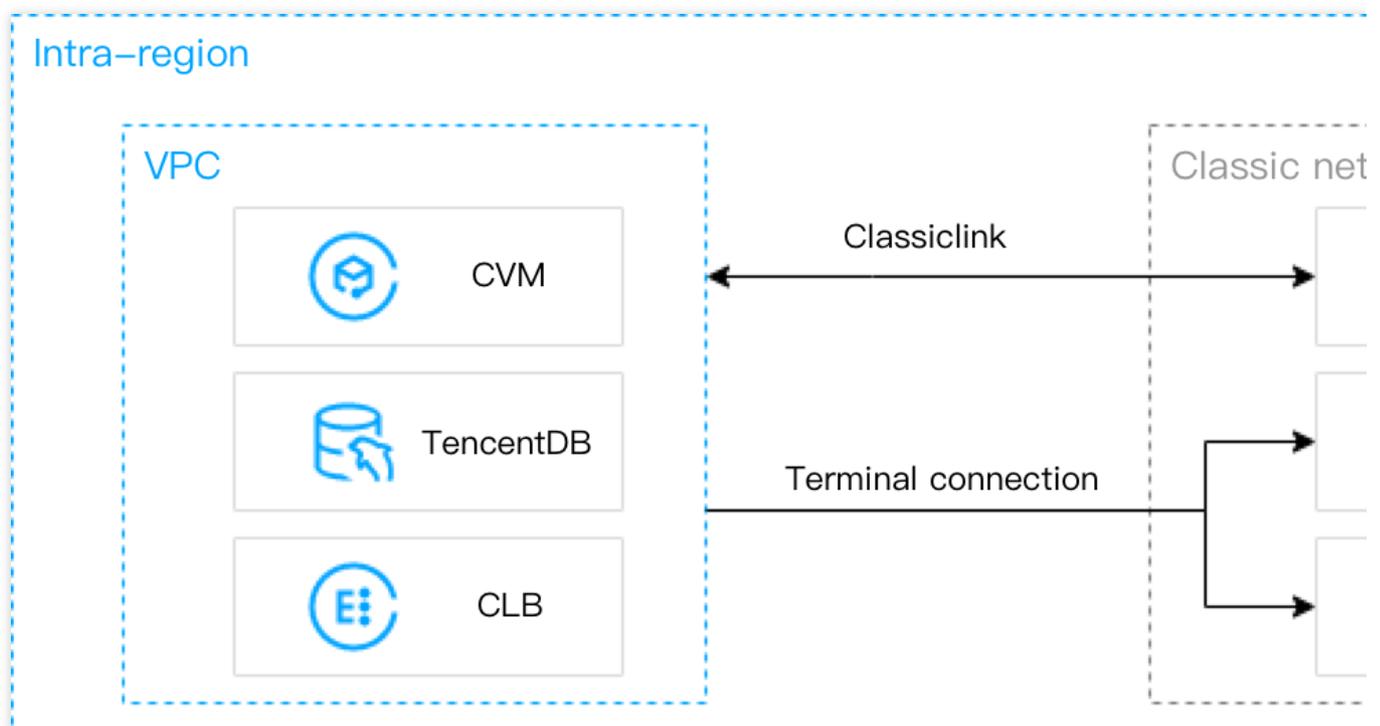
O [Cloud Connect Network \(CCN\)](#) interconecta as instâncias do VPC do Tencent Cloud e conecta instâncias do VPC com IDCs locais.

# Comunicação com a rede clássica

Last updated : 2024-01-24 17:44:04

Tanto a rede clássica quanto a VPC são espaços de rede na nuvem. A VPC é mais seguro e controlável. Embora a maioria das CVMs esteja implantada em VPCs da Tencent Cloud, algumas aplicações ainda estão sendo executadas na rede clássica que precisa de interconexão com a VPC. Para resolver esse problema, a Tencent Cloud fornece a seguinte solução.

## Interconexão entre a rede clássica e uma VPC



### Classiclink

Ele associa as CVMs baseadas na rede clássica a uma VPC especificada para permitir que essas CVMs se comuniquem com os recursos da VPC, como as instâncias da CVM e do TencentDB. No entanto, isso fornece acesso apenas entre as CVMs baseadas na VPC e as CVMs baseadas na rede clássica, em vez de outros recursos de nuvem, como o TencentDB e o CLB dentro da rede clássica.

### Conexão de terminal

Ela ajuda as instâncias em uma VPC a se comunicarem com os recursos na rede clássica (exceto as CVMs) por meio de uma rede privada. Uma conexão de terminal estabelece o mapeamento entre endereços IP de instâncias da rede clássica e endereços IP da VPC, para que as instâncias da rede clássica possam ser acessadas pelos endereços IP da VPC. Os produtos da rede clássica que aceitam as conexões de terminal incluem as instâncias do

CLB, do MySQL, do Memcached, do Redis, do MariaDB, do SQL Server, do PostgreSQL, do MongoDB e do TDSQL.

**Nota:**

Uma conexão de terminal não permite a comunicação entre regiões ou contas diferentes. Se você deseja estabelecer uma conexão de terminal, [envie um tíquete](#).

## Migração da rede clássica para uma VPC

A VPC da Tencent Cloud é recomendada por sua segurança, flexibilidade e controlabilidade. Atualmente, a Tencent Cloud permite a migração de recursos da rede clássica para uma VPC. Para mais informações, consulte [Migração da rede clássica para a VPC](#).

## Referências

Para mais informações sobre a rede clássica e suas diferenças com relação a uma VPC, consulte [Rede clássica](#).

Para mais informações sobre as configurações do Classiclink, consulte [Classiclink](#).

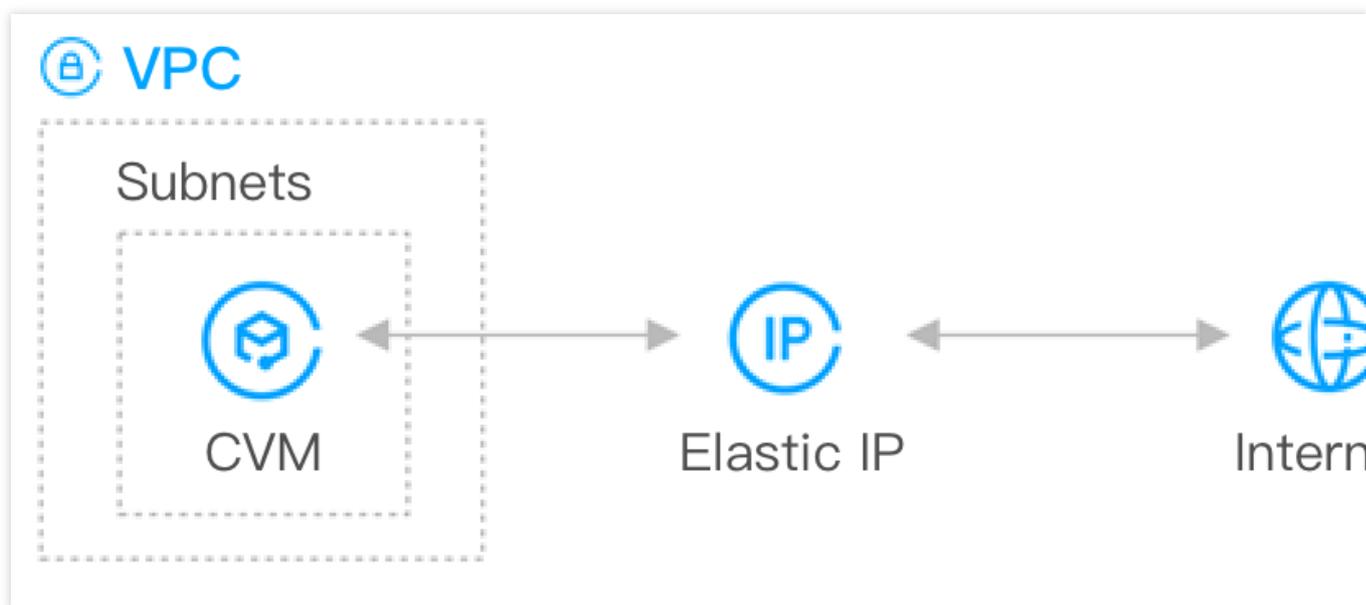
# Criação de uma VPC IPv4

Last updated : 2024-01-24 17:44:04

Este tutorial descreve como criar rapidamente uma Virtual Private Cloud (VPC) com blocos CIDR IPv4.

## Visão geral

Este documento orienta todo o processo de configuração de uma VPC baseado em IPv4.



## Pré-requisitos

Certifique-se de ter [criado uma conta da Tencent Cloud](#) e concluído a [verificação de identidade](#), se precisar adquirir recursos na China Continental.

## Instruções

### Etapa 1: criar uma VPC e uma sub-rede

#### Nota:

Após criar uma VPC e uma sub-rede, você não pode modificar os blocos CIDR. Portanto, conclua o [planejamento de rede](#) com antecedência.

1. Faça login no [Console da VPC](#).
2. Selecione a região da VPC na parte superior e clique em **+New (+Novo)**.

3. Na janela pop-up **Create VPC (Criar VPC)**, configure as informações da VPC e da sub-rede conforme as instruções abaixo.

### Create VPC

**VPC information**

Region

Name

IPv4 CIDR Block  .  . 0 . 0 /  ⚠ 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 /

Remaining IPs: 253

Availability Zone  ⓘ

Associated route table Default ⓘ

[Advanced Options](#) ▶

#### Informações da VPC

Name (Nome): o nome da VPC.

IPv4 CIDR Block (Bloco CIDR IPv4): você pode escolher qualquer um desses intervalos de IP **10.0.0.0 - 10.255.255.255**, **172.16.0.0 - 172.31.255.255** e

**192.168.0.0 - 192.168.255.255** como o intervalo de IP da VPC. O intervalo da máscara deve ser de 16 a 28, como `10.0.0.0/16`.

Advanced options (Opções avançadas): opcionalmente, é possível adicionar tags para ajudar você a melhorar o gerenciamento das permissões de recursos de subusuários e colaboradores.

### Informações da sub-rede

IPv4 CIDR Block (Bloco CIDR IPv4):

Você pode escolher um intervalo de IP dentro ou igual ao intervalo de IP da VPC. Por exemplo, se o intervalo de IP da VPC for 10.0.0.0/16, você poderá escolher um intervalo de IP entre 10.0.0.0/16 e 10.0.255.255/28 como o intervalo de IP da sub-rede.

Se a VPC em que as sub-redes estiverem localizadas precisar se comunicar com outras VPCs ou IDCs, certifique-se de que o intervalo de IP da sub-rede não se sobreponha ao intervalo de IP de par. Caso contrário, a interconexão por meio de uma rede privada pode falhar.

Availability Zone (Zona de disponibilidade): selecione uma zona de disponibilidade na qual a sub-rede está localizada. Uma VPC permite sub-redes em zonas de disponibilidade diferentes, e, por padrão, essas sub-redes podem se comunicar umas com as outras por meio de uma rede privada.

Advanced options (Opções avançadas): opcionalmente, é possível adicionar tags para ajudar você a melhorar o gerenciamento das permissões de recursos de subusuários e colaboradores.

## Etapa 2: adquirir uma instância da CVM

1. Faça login no [Console da CVM](#) para criar uma instância da CVM na VPC criado na etapa anterior.
2. Clique em **Create (Criar)** no canto superior esquerdo da página da lista para acessar a página de aquisição da CVM.
3. Na página de configuração personalizada, configure a instância da CVM e clique em **Buy Now (Comprar agora)**.

As configurações de rede da CVM são as seguintes:

Network (Rede): selecione a VPC e a sub-rede criados.

Network vpc- [dropdown] subnet- [dropdown] Available IPs in th

The current network is the default VPC/subnet. You can adjust it as needed

If the existing VPC/subnet do not match your requirements, please go to the Console to [Create a VPC](#) or [Create Subnet](#) console

Public network bandwidth (Largura de banda da rede pública): não marque



Public network IP

Get a free public IP

Note: If a public IP is not assigned, the instance will not be able to access the internet and can

Security Group (Grupo de segurança): selecione **New security group (Novo grupo de segurança)** e configure-o conforme as instruções em [Configuração de grupos de segurança](#).

Security Groups

[Create security group](#)[Existing Security Groups](#)[Operation Guide](#)

Allow common IPs/ports

- |  |   |  |   |
|--|---|--|---|
| <input checked="" type="checkbox"/> ICMP     | Allows ping command on the CVM from internet        | <input type="checkbox"/> TCP:80                          | When the CVM is used for web services (HTTP)  |
| <input checked="" type="checkbox"/> TCP:22   | Allows remote login via SSH key for Linux instances | <input type="checkbox"/> TCP:443                         | When the CVM is used for web services (HTTPS) |
| <input checked="" type="checkbox"/> TCP:3389 | Allows remote login via RDP for Windows instances   | <input checked="" type="checkbox"/> Allow private access | among different cloud resources               |

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

### Etapa 3: solicitar um EIP e vinculá-lo à instância da CVM

Um IP elástico (EIP) é um endereço IP público que pode ser solicitado e adquirido de forma independente. Você pode vinculá-lo a uma instância da CVM para habilitar o acesso à rede pública.

1. Faça login no [Console do EIP](#).
2. Na página **EIP**, selecione a região onde está localizado a CVM. Clique em **Apply (Solicitar)** no canto superior esquerdo.
3. Na janela **Apply for EIP (Solicitar EIP)**, configure os parâmetros relevantes e clique em **OK**.
4. Na página **EIP**, localize o EIP solicitado e clique em **More (Mais) > Bind (Vincular)**, na coluna **Operation (Operação)**.
5. Na janela **Bind resources (Vincular recursos)**, selecione **CVM Instances (Instâncias da CVM)** como o tipo de recurso a ser vinculado, selecione a instância da CVM e clique em **OK**.
6. Na janela pop-up de confirmação, clique em **OK**.

### Etapa 4: testar a conectividade da rede pública

Conclua as operações a seguir para testar a conectividade da rede pública da instância da CVM.

**Nota:**

Antes de realizar o teste, certifique-se de que o grupo de segurança permite o acesso ao endereço IP e à porta correspondentes. Por exemplo, o protocolo ICMP está aberto e o servidor pode receber ping da rede pública. Para mais informações, consulte [Exibição de uma regra de grupos de segurança](#).

1. Faça login na instância da CVM com um EIP vinculado. Para obter instruções detalhadas, consulte [Login e acesso remoto](#).

2. Execute o comando `ping <public IP address>`, como `ping www.qq.com` para testar a conectividade da rede pública.

```
[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
```