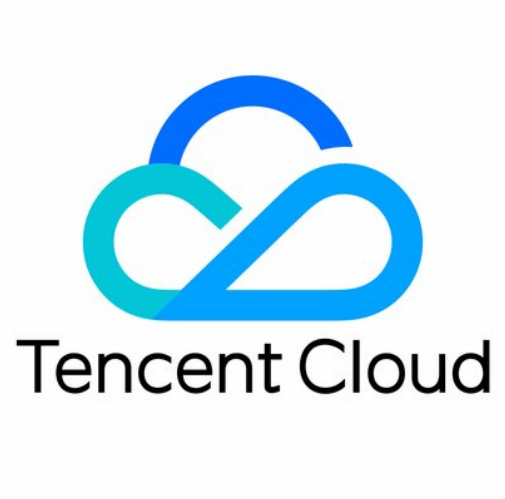
Virtual Private Cloud

Mulai Cepat

Dokumen produk



Direktori dokumen

Mulai Cepat
Perencanaan Jaringan

Waktu update terbaru：2024-01-24 17:44:04

Sebelum memulai perluasan jaringan dan pembangunan VPC, Anda perlu merencanakan jumlah dan rentang IP VPC yang sesuai dengan kebutuhan bisnis Anda.

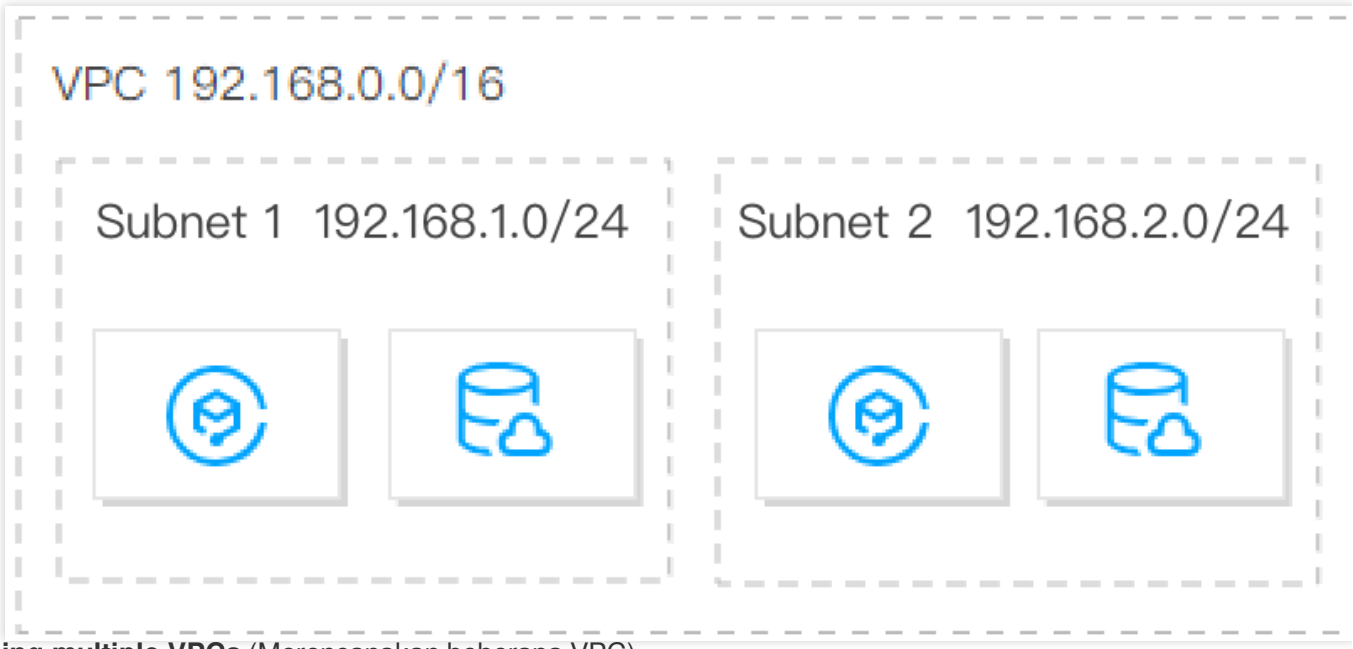
Bagaimana Cara Merencanakan Kuantitas VPC?
Bagaimana Cara Merencanakan Kuantitas Subnet?
Bagaimana Cara Merencanakan Rentang IP (Blok CIDR) VPC dan Subnet?
Bagaimana Cara Merencanakan Kuantitas Tabel Rute?
Bagaimana Cara Merencanakan Jaringan Cloud Hibrida Multi-pusat Lintas Wilayah?

Bagaimana Cara Merencanakan Kuantitas VPC?

Planning one VPC (Merencanakan satu VPC)

Jika Anda memiliki bisnis skala kecil yang di-deploy di wilayah yang sama tanpa memerlukan isolasi jaringan, sebaiknya Anda merencanakan satu VPC.

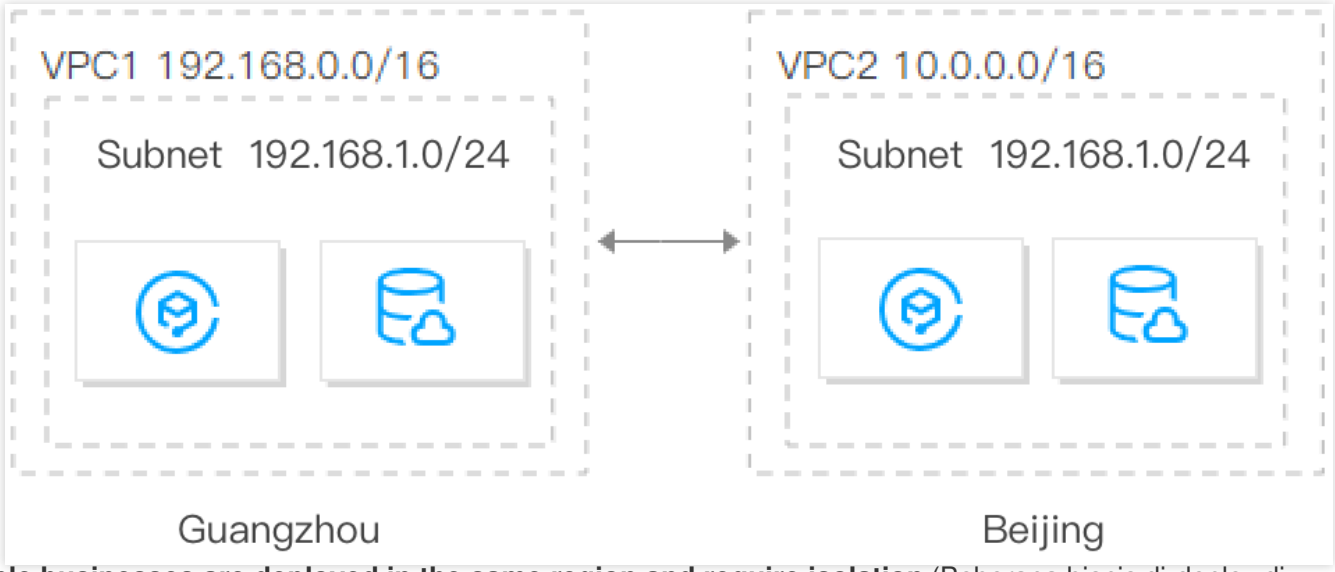
Anda dapat membuat beberapa subnet dan tabel rute dalam satu VPC untuk pengelolaan lalu lintas yang mendetail. Selain itu, kami merekomendasikan Anda men-deploy subnet di zona ketersediaan yang berbeda untuk pemulihan bencana AZ.



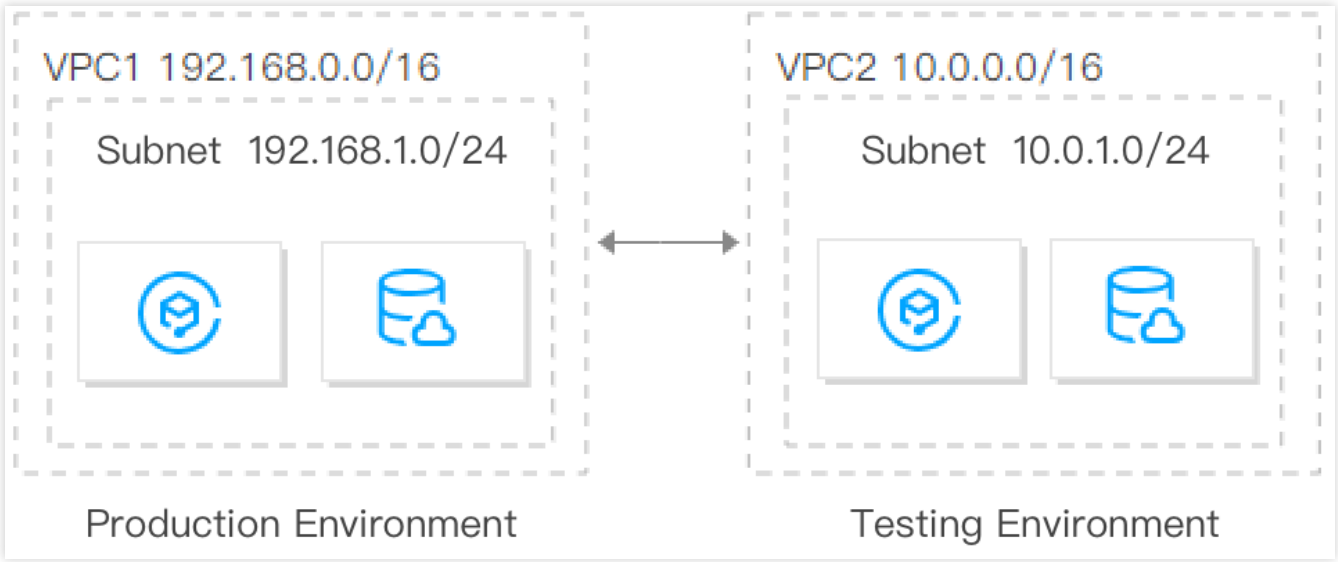
Planning multiple VPCs (Merencanakan beberapa VPC)

Kami merekomendasikan Anda untuk merencanakan beberapa VPC dalam salah satu skenario berikut:

Your business is deployed in multiple regions (Bisnis Anda di-deploy di beberapa wilayah)
Jika bisnis Anda di-deploy di beberapa wilayah, Anda perlu merencanakan beberapa VPC dan men-deploy setidaknya satu di setiap wilayah karena VPC tidak dapat di-deploy di seluruh wilayah.
Secara default, VPC tidak saling berhubungan. Untuk saling menghubungkan VPC, gunakan peering connection atau Cloud Connect Network.



Multiple businesses are deployed in the same region and require isolation (Beberapa bisnis di-deploy di wilayah yang sama dan memerlukan isolasi)
Jika Anda memiliki beberapa bisnis yang di-deploy di wilayah yang sama dan bisnis ini harus diisolasi satu sama lain, Anda perlu merencanakan beberapa VPC dan men-deploy satu VPC untuk setiap bisnis. Melakukan hal ini dapat mengisolasi bisnis karena VPC tidak saling terhubung secara default.



Bagaimana Cara Merencanakan Kuantitas Subnet?

Satu VPC dapat memiliki beberapa (100 secara default) subnet. Subnet yang berbeda dalam VPC yang sama dapat berkomunikasi satu sama lain melalui jaringan pribadi secara default.
Untuk mencapai pemulihan bencana di seluruh zona ketersediaan, kami merekomendasikan Anda membuat setidaknya dua subnet di zona ketersediaan yang berbeda untuk VPC.

Bagaimana Cara Merencanakan Rentang IP (Blok CIDR) VPC dan Subnet?

Once set, the IP range masks of VPCs and subnets cannot be modified. (Setelah diatur, mask rentang IP VPC dan subnet tidak dapat dimodifikasi.) Dengan demikian, pastikan untuk merencanakan VPC dan subnet dengan cermat berdasarkan skala bisnis dan skenario komunikasi Anda. Ini akan memfasilitasi penskalaan dan operasi yang lancar di masa mendatang.

Merencanakan rentang IP VPC

You can use any of the following IP ranges as your VPC IP ranges: (Anda dapat menggunakan salah satu rentang IP berikut sebagai rentang IP VPC Anda:)
10.0.0.0 - **10.255**.255.255 (**the mask range must be 16 to 28** (rentang mask harus 16 hingga 28))
172.16.0.0 - **172.31**.255.255 (**the mask range must be 16 to 28** (rentang mask harus 16 hingga 28))
192.168.0.0 - **192.168**.255.255 (**the mask range must be 16 to 28** (rentang mask harus 16 hingga 28))
When planning VPC IP ranges, note that: (Saat merencanakan rentang IP VPC, perhatikan bahwa:)
Jika Anda perlu membuat beberapa VPC yang berkomunikasi satu sama lain atau dengan IDC, pastikan rentang IP VPC tidak tumpang tindih.
Jika VPC Anda perlu berkomunikasi dengan jaringan klasik, rentang IP VPC yang Anda buat harus berada dalam `10.[0-47].0.0/16` (termasuk subset).
Setelah dibuat, blok CIDR dari VPC dan subnet tidak dapat diubah. Jika salah satu blok CIDR tidak mencukupi, Anda dapat membuat blok CIDR tambahan.

Merencanakan rentang IP subnet

Subnet IP range (Rentang IP Subnet) Anda dapat menggunakan rentang IP VPC atau sebagian darinya sebagai rentang IP subnet. Misalnya, jika rentang IP VPC adalah 10.0.0.0/16, rentang IP subnet dapat berada di antara 10.0.0.0/16-10.0.255.255/28.
Subnet size and IP capacity (Ukuran subnet dan kapasitas IP): setelah dibuat, subnet tidak dapat diubah. Saat membuat subnet, pastikan rentang IP subnet dapat memenuhi kebutuhan bisnis Anda. Namun, Anda juga perlu mengontrol ukuran subnet, yang memungkinkan Anda membuat subnet untuk penskalaan nanti.
Business requirements (Persyaratan bisnis): satu VPC dapat dibagi menjadi subnet berdasarkan segmen bisnis. Misalnya, Anda dapat men-deploy lapisan web, lapisan logis, dan lapisan data di subnet yang berbeda dan menggunakan ACL jaringan untuk mengimplementasikan kontrol akses.

Keterangan:

Jika VPC tempat subnet berada perlu berkomunikasi dengan VPC atau IDC lain, pastikan rentang IP subnet tidak tumpang tindih dengan rentang pasangan IP. Jika tidak, interkoneksi melalui jaringan pribadi mungkin gagal.

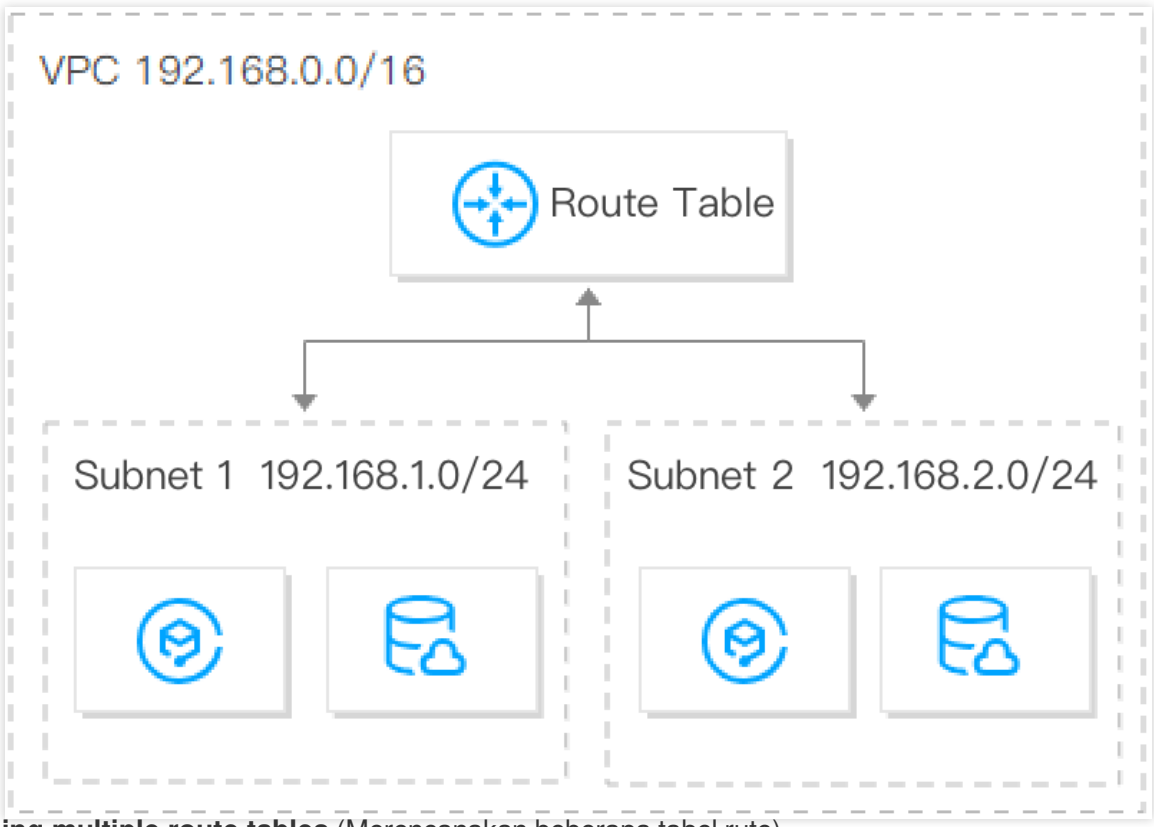
Jika rentang IP subnet tumpang tindih, Anda mengubah subnet instans dan menggunakan CCN, atau membuat VPC baru dan membeli CVM.

Bagaimana Cara Merencanakan Kuantitas Tabel Rute?

Tabel rute digunakan untuk mengontrol arah lalu lintas dalam subnet. Setiap subnet hanya dapat diikat dengan satu tabel rute. Anda dapat menggunakan tabel rute default dan tabel rute kustom di VPC Tencent Cloud.

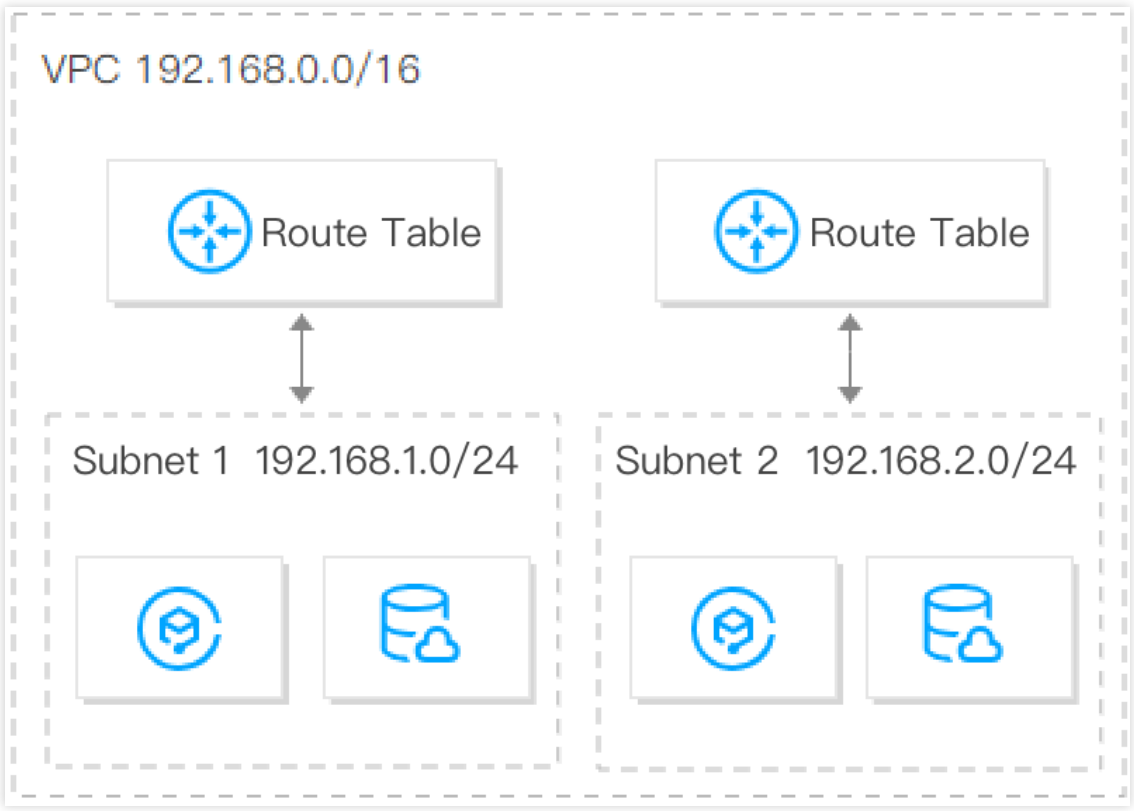
Planning one route table (Merencanakan satu tabel rute)

Jika subnet yang berbeda di VPC Anda memiliki persyaratan yang sama atau serupa untuk arah lalu lintas, sebaiknya rencanakan satu tabel rute. Kemudian, Anda dapat membuat kebijakan perutean yang berbeda untuk mengontrol arah lalu lintas.



Planning multiple route tables (Merencanakan beberapa tabel rute)

Jika subnet di VPC Anda memiliki persyaratan berbeda untuk arah lalu lintas, sebaiknya rencanakan beberapa tabel rute. Kemudian, Anda dapat mengikatnya ke subnet yang sesuai dan membuat kebijakan perutean untuk mengontrol arah lalu lintas.

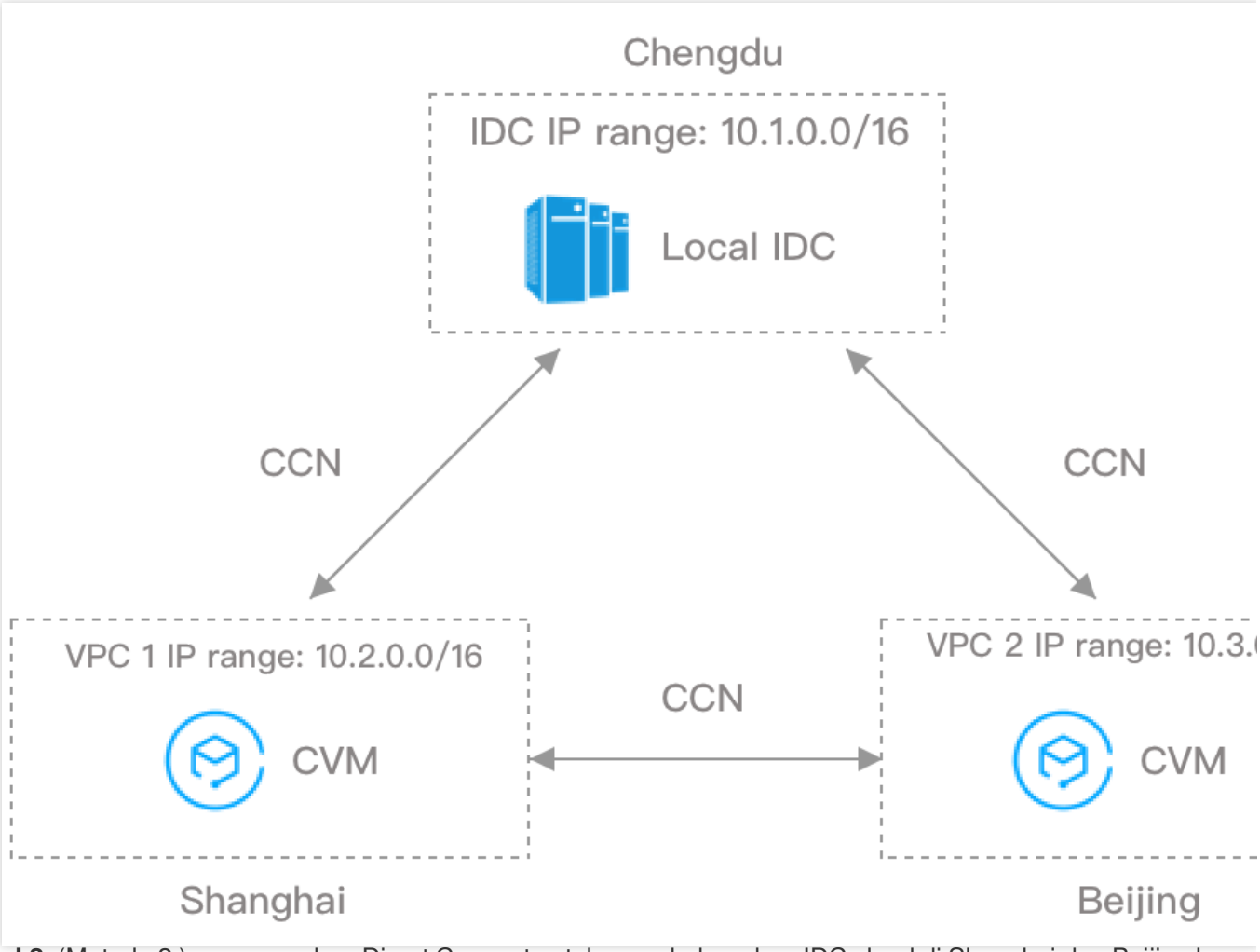


Bagaimana Cara Merencanakan Jaringan Cloud Hibrida Multi-pusat Lintas Wilayah?

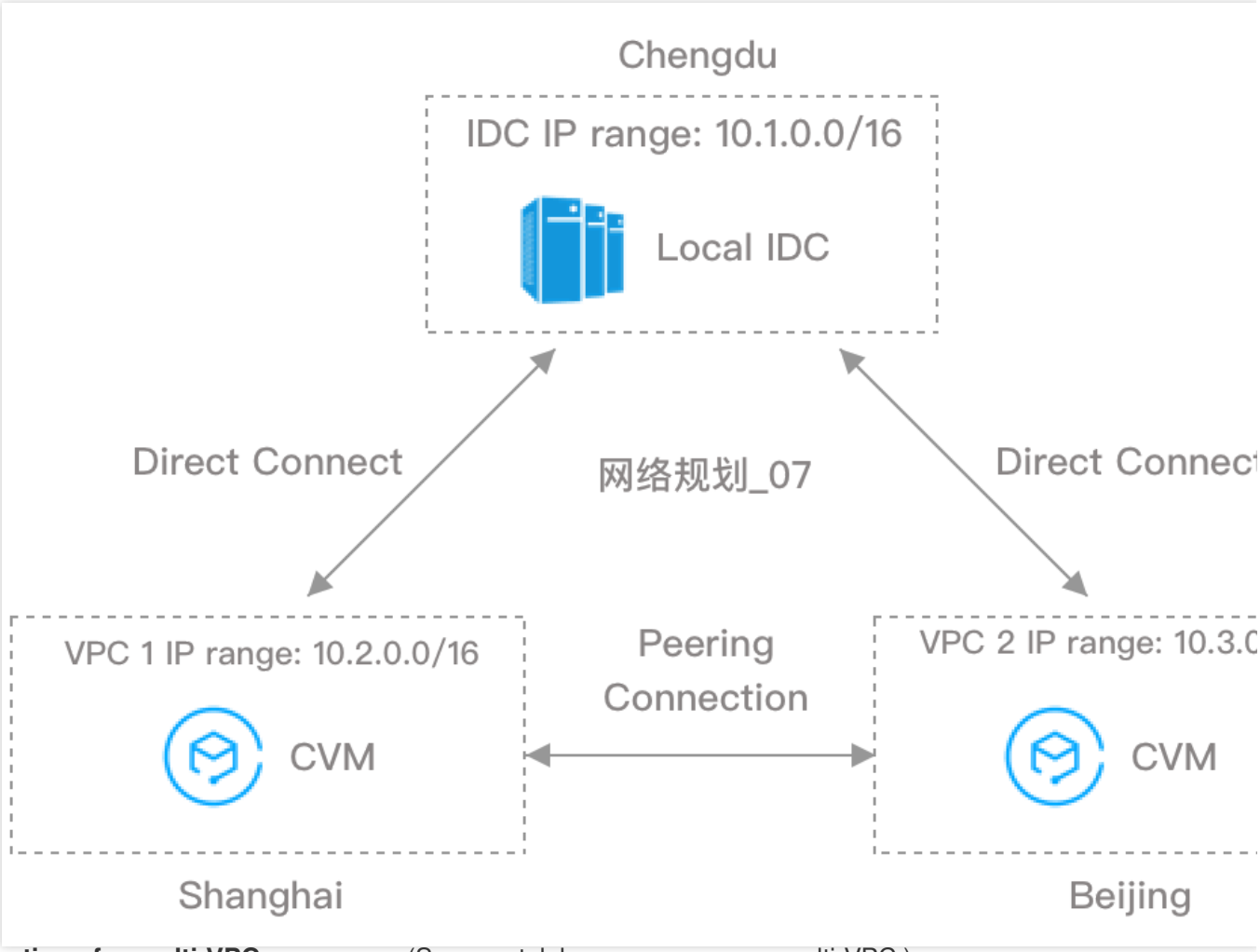
Jika Anda perlu membuat beberapa VPC yang berkomunikasi satu sama lain atau dengan IDC, pastikan rentang IP VPC tidak tumpang tindih dengan rentang pasangan IP.

Asumsikan Anda memiliki IDC lokal dengan rentang IP `10.1.0.0/16` di Chengdu, dan ingin membuat dua IDC cloud di Shanghai dan Beijing yang perlu berkomunikasi dengan IDC lokal Anda. Dalam hal ini, kami merekomendasikan Anda menggunakan `10.2.0.0/16` dan `10.3.0.0/16` sebagai rentang IP VPC dari dua IDC cloud di Shanghai dan Beijing masing-masing, untuk menghindari kegagalan komunikasi yang disebabkan oleh rentang IP yang tumpang tindih. Anda dapat mengaktifkan komunikasi antara IDC lokal dan IDC cloud dan antara IDC cloud menggunakan dua metode berikut.

Method 1: (Metode 1:) menambahkannya ke CCN untuk mengimplementasikan interkoneksi melalui jaringan publik dan pribadi.



Method 2: (Metode 2:) menggunakan Direct Connect untuk menghubungkan IDC cloud di Shanghai dan Beijing ke IDC lokal di Chengdu, sehingga memungkinkan komunikasi antara IDC lokal dan IDC cloud. Untuk mengaktifkan komunikasi antara IDC cloud di Shanghai dan Beijing, gunakan peering connection untuk menghubungkan VPC yang sesuai.



Suggestions for multi-VPC use cases: (Saran untuk kasus penggunaan multi-VPC:)

Coba rencanakan rentang IP yang berbeda untuk setiap VPC.

Coba rencanakan rentang IP yang berbeda untuk subnet VPC jika setiap VPC tidak dapat memiliki rentang IP yang berbeda.

Pastikan bahwa rentang IP subnet yang perlu berkomunikasi berbeda jika setiap subnet tidak dapat memiliki rentang IP yang berbeda.

Dokumentasi

Untuk informasi selengkapnya tentang cara cepat membangun Virtual Private Cloud (VPC) dengan blok CIDR IPv4, termasuk membuat VPC dan subnet, membeli CVM, dan mengikat EIP untuk mengaktifkan akses jaringan publik, lihat Membangun VPC IPv4.

VPC Connection
Menghubungkan ke Internet

Waktu update terbaru：2024-01-24 17:44:05

Tencent Cloud memberi Anda berbagai metode untuk mengakses Internet, seperti melalui alamat IP publik umum, EIP, NAT gateway, dan Cloud Load Balancer (CLB).

Alamat IP Publik Umum

Saat membuat instans CVM, Anda dapat menetapkan alamat IP publik umum ke instans. Sistem akan menetapkan alamat IP ke CVM Anda untuk memungkinkannya mengakses Internet serta dapat diakses melalui Internet.
Alamat IP publik umum tidak dapat secara dinamis terikat atau tidak terikat dengan sumber daya seperti CVM, tetapi Anda dapat mengonversinya menjadi EIP. Untuk mengetahui detailnya, lihat Mengonversi Alamat IP Publik menjadi EIP.

Alamat IP Elastis

Tidak seperti alamat IP publik yang perlu diterapkan dan dirilis dengan CVM, alamat IP elastis (EIP) adalah sumber informasi cloud independen yang dipisahkan dari siklus pemakaian CVM dan dapat dioperasikan secara terpisah.
Untuk informasi tentang cara mengajukan, mengikat, dan melepaskan EIP, lihat EIP - Langkah.
EIP menawarkan keuntungan sebagai berikut:
Sumber informasi cloud independen
Anda dapat mengoperasikan EIP secara mandiri, tanpa perlu membelinya dengan CVM.
Pengikatan dan pemutusan ikatan elastis dengan sumber informasi
EIP dapat terikat dan tidak terikat dengan CVM dan sumber daya lainnya kapan saja.

NAT Gateway

NAT Gateway menyediakan fitur SNAT dan DNAT, yang memungkinkan Anda membuat jalan keluar Internet dengan mudah dan menyediakan layanan untuk CVM di VPC untuk mengakses Internet dengan alamat IP publik yang sama.
Untuk informasi tentang cara mengonfigurasi NAT gateway, lihat NAT Gateway - Ikhtisar Operasi.
NAT Gateway menawarkan keuntungan sebagai berikut:
Akses Internet yang aman
NAT Gateway menyediakan fitur SNAT dan DNAT untuk menyembunyikan alamat IP CVM di VPC selama

komunikasi Internet, memastikan keamanan.
Ketersediaan tinggi
NAT Gateway menampilkan pencadangan panas master/slave, peralihan panas otomatis, dan penerusan cepat dengan kecepatan hingga 5 Gbps. Selain itu, mereka mendukung aplikasi Internet skala besar.
Konfigurasi fleksibel
Anda dapat mengubah spesifikasi NAT gateway sesuai kebutuhan kapan saja.

Cloud Load Balancer

Cloud Load Balancer (CLB) mendistribusikan lalu lintas ke beberapa CVM untuk meningkatkan kemampuan layanan eksternal sistem aplikasi. Ini menghilangkan satu titik kegagalan untuk memastikan sistem aplikasi yang sangat tersedia.
Untuk informasi tentang cara membeli dan mengonfigurasi CLB, lihat CLB - Memulai.
CLB menawarkan keuntungan sebagai berikut:
Kluster tunggal performa tinggi
Sebuah kluster CLB terdiri dari beberapa server fisik, dengan ketersediaan hingga 99,95%. Sistem kluster dapat menghapus instans yang salah dan memilih instans yang sehat untuk memastikan layanan berjalan dengan benar di server sebenarnya.
Keamanan dan stabilitas tinggi
Dengan sistem anti-DDoS BGP, CLB dapat bertahan terhadap sebagian besar serangan jaringan (seperti serangan DDoS) dan membersihkan serangan lalu lintas dalam hitungan detik, mencegah alamat IP yang diblokir atau konsumsi bandwidth penuh.

Gateway Publik

Gateway Publik adalah CVM dengan fitur penerusan yang diaktifkan. Dalam VPC, CVM tanpa alamat IP publik dapat mengakses Internet melalui gateway publik pada subnet yang berbeda. Gateway publik dapat menyembunyikan alamat sumber lalu lintas Internet dari CVM lain ke alamat IP mereka sendiri.
Untuk informasi tentang cara mengonfigurasi gateway publik, lihat Mengonfigurasi Gateway Publik.

Menghubungkan ke Instans VPC Lain

Waktu update terbaru：2024-01-24 17:44:04

Anda dapat menghubungkan instans VPC yang berbeda melalui peering connection atau CCN.

Peering Connection

Anda dapat membuat peering connection untuk menghubungkan dua instans VPC di bawah akun yang sama atau berbeda.

Membuat peering connection untuk komunikasi VPC intra-akun

Membuat peering connection untuk komunikasi VPC lintas-akun

CCN

Anda dapat menggunakan CCN untuk menghubungkan dua atau lebih instans VPC. CCN mendukung interkoneksi antara instans VPC dalam akun yang sama atau berbeda dan interkoneksi antara instans VPC dan IDC.

Interkoneksi antara instans jaringan di bawah akun yang sama

Interkoneksi antara instans jaringan di bawah akun yang berbeda

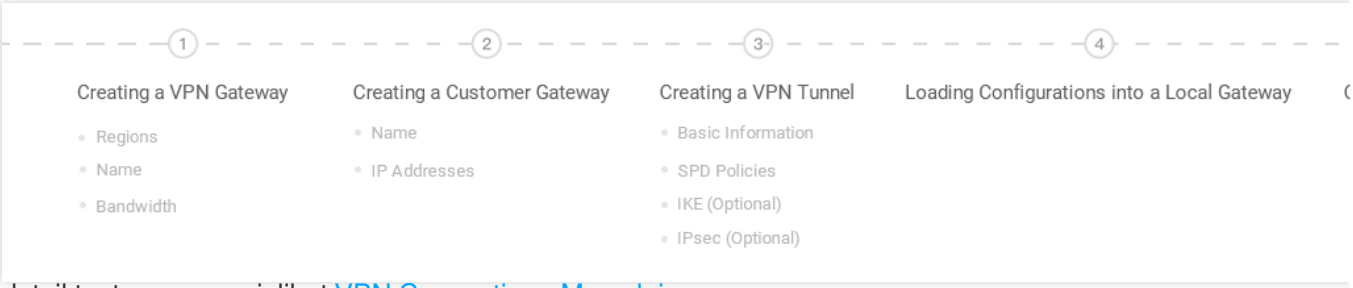
Menghubungkan ke IDC Lokal

Waktu update terbaru：2024-01-24 17:44:05

Anda dapat membuat VPN connection, direct connection, atau CCN untuk mengimplementasikan komunikasi antara instans VPC Anda dan IDC lokal.

VPN Connection

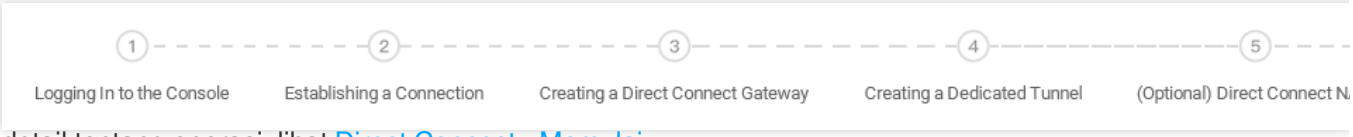
VPN connection adalah metode untuk menghubungkan IDC dan instans VPC Anda melalui tunnel terenkripsi jaringan publik. VPN connection terdiri dari tiga bagian: VPN gateway, gateway pelanggan, dan tunnel VPN.
Setiap VPN gateway dapat membuat beberapa tunnel VPN, dan setiap tunnel VPN dapat terhubung ke satu IDC lokal.



Untuk detail tentang operasi, lihat VPN Connection - Memulai.

Direct Connection

Direct connection adalah koneksi langsung fisik yang menghubungkan instans VPC dan IDC lokal. Koneksi langsung terdiri dari tiga bagian: koneksi fisik, tunnel khusus, dan direct connect gateway.
Pengguna dapat membuat koneksi fisik untuk menghubungkan sumber informasi komputasi Tencent Cloud di berbagai wilayah, mencapai deployment cloud hibrida yang fleksibel dan andal.



Untuk detail tentang operasi, lihat Direct Connect - Memulai.

Cloud Connect Network

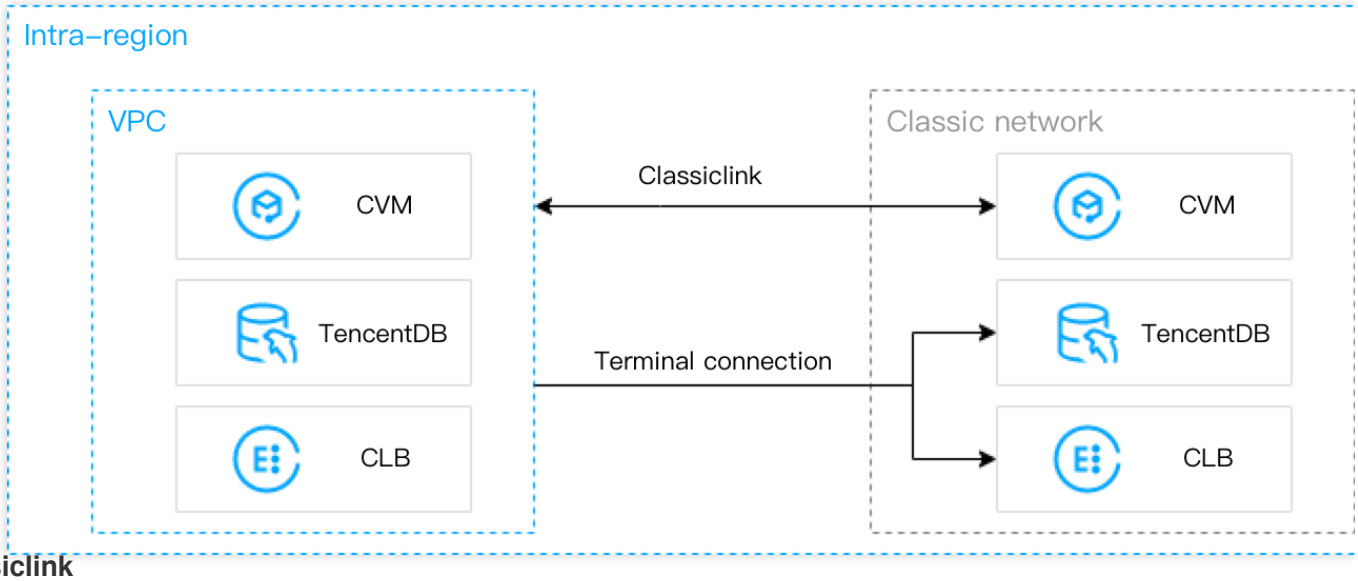
Cloud Connect Network (CCN) menghubungkan instans Tencent Cloud VPC dan menghubungkan instans VPC dengan IDC lokal.

Menghubungkan ke Jaringan Klasik

Waktu update terbaru：2024-01-24 17:44:05

Baik klasik maupun VPC adalah ruang jaringan di cloud. VPC lebih aman dan terkendali. Meskipun sebagian besar CVM di-deploy di Tencent Cloud VPC, beberapa aplikasi tetap berjalan di jaringan klasik yang memerlukan interkoneksi dengan VPC. Untuk mengatasi masalah ini, Tencent Cloud memberikan solusi berikut.

Saling Menghubungkan Jaringan Klasik dan VPC



Classiclink

Ini menghubungkan CVM berbasis jaringan klasik dengan VPC tertentu sehingga CVM ini dapat berkomunikasi dengan sumber daya VPC seperti instans CVM dan TencentDB. Namun, ini hanya menyediakan akses antara CVM berbasis VPC dan CVM berbasis jaringan klasik, alih-alih sumber daya cloud lainnya, termasuk TencentDB dan CLB dalam jaringan klasik.

Terminal connection (Koneksi terminal)

Koneksi ini membantu instans dalam VPC berkomunikasi dengan sumber daya di jaringan klasik (kecuali CVM) melalui jaringan pribadi. Koneksi terminal membuat pemetaan antara alamat IP instans jaringan klasik dan alamat IP VPC sehingga instans jaringan klasik dapat diakses dengan mengakses alamat IP VPC. Produk jaringan klasik yang mendukung koneksi terminal mencakup instans CLB, MySQL, Memcached, Redis, MariaDB, SQL Server, PostgreSQL, MongoDB, dan TDSQL.

Keterangan:

Koneksi terminal tidak mendukung komunikasi lintas wilayah atau lintas akun. Jika Anda ingin membuat koneksi terminal, harap kirim tiket.

Migrasi dari Jaringan Klasik ke VPC

Tencent Cloud VPC direkomendasikan karena keamanan, fleksibilitas, dan kemampuan kontrolnya. Saat ini, Tencent Cloud mendukung migrasi sumber daya dari jaringan klasik ke VPC. Untuk informasi selengkapnya, lihat Migrasi dari Jaringan Klasik ke VPC.

Referensi

Untuk informasi selengkapnya tentang jaringan klasik dan perbedaannya dengan VPC, lihat Jaringan Klasik.
Untuk informasi selengkapnya tentang konfigurasi Classiclink, lihat Classiclink.

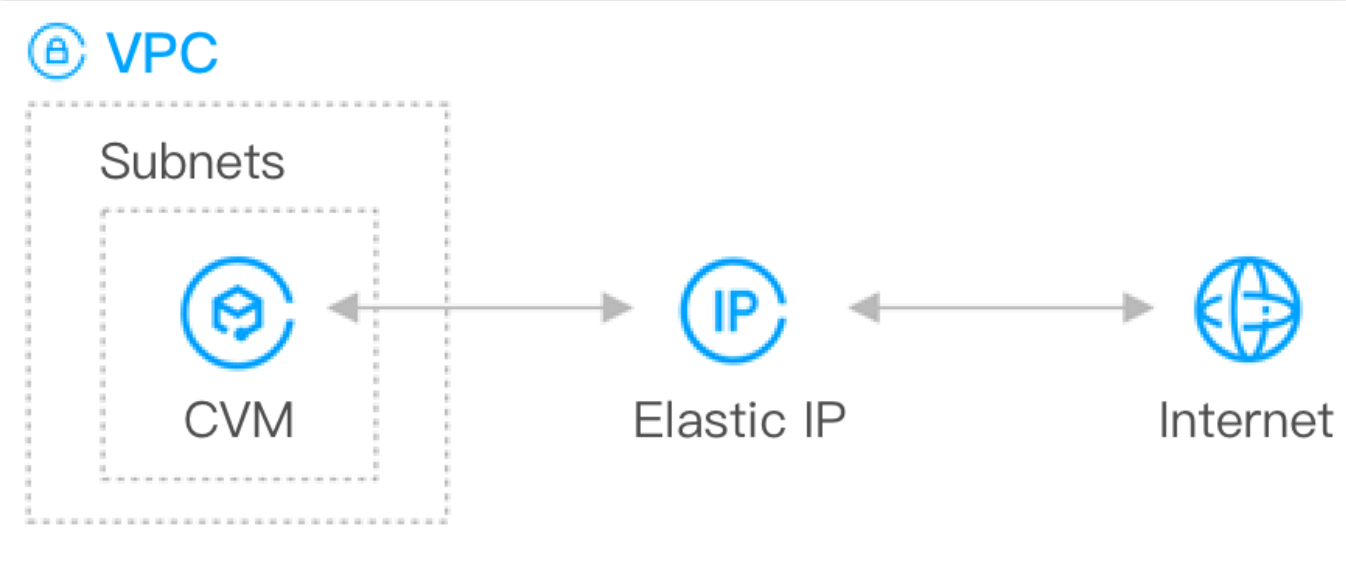
Membangun VPC IPv4

Waktu update terbaru：2024-01-24 17:44:05

Tutorial ini akan menjelaskan cara cepat membuat Virtual Private Cloud (VPC) dengan blok CIDR IPv4.

Ikhtisar

Dokumen ini akan memandu seluruh proses penyiapan VPC berbasis IPv4.



Prasyarat

Pastikan Anda telah mendaftar akun Tencent Cloud dan menyelesaikan verifikasi identitas jika Anda perlu membeli sumber daya apa pun di daratan Tiongkok.

Petunjuk

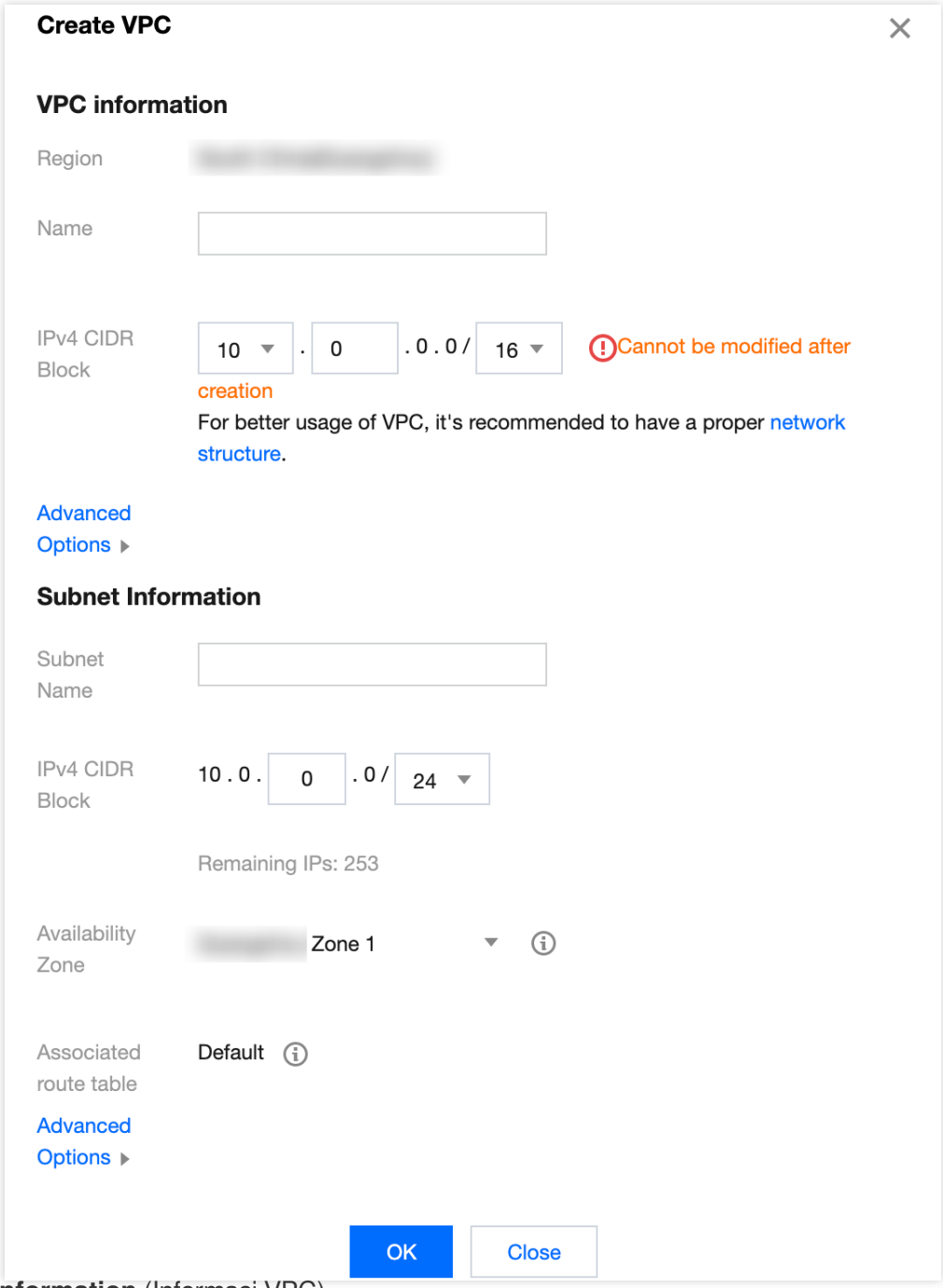
Langkah 1: buat VPC dan subnet

Keterangan:

Setelah membuat VPC dan subnet, Anda tidak dapat mengubah blok CIDR-nya. Dengan demikian, selesaikan perencanaan jaringan terlebih dahulu.

1. Login ke Konsol VPC.
2. Pilih wilayah VPC di bagian atas dan klik **+New** (+Baru).

3. Di jendela pop-up **Create VPC** (Buat VPC), konfigurasikan informasi VPC dan subnet seperti yang diinstruksikan di bawah ini.



VPC Information (Informasi VPC)

Nama: nama VPC.

Blok CIDR IPV4: Anda dapat memilih salah satu dari rentang IP **10.0**.0.0 - **10.255**.255.255, **172.16**.0.0 - **172.31**.255.255, dan

192.168.0.0 - **192.168**.255.255 sebagai rentang IP VPC. Rentang mask harus 16 hingga 28, seperti `10.0.0.0/16` .

Opsi Lanjutan: Anda dapat menambahkan tag secara opsional untuk membantu Anda mengelola izin sumber daya sub-pengguna dan kolaborator dengan lebih baik.

Subnet information (Informasi subnet)

Blok CIDR IPv4:

Anda dapat memilih rentang IP di dalam atau sama dengan rentang IP VPC. Misalnya, jika rentang IP VPC adalah 10.0.0.0/16, Anda dapat memilih rentang IP antara 10.0.0.0/16 dan 10.0.255.255/28 sebagai rentang IP subnet.

Jika VPC tempat subnet berada perlu berkomunikasi dengan VPC atau IDC lain, pastikan rentang IP subnet tidak tumpang tindih dengan rentang pasangan IP. Jika tidak, interkoneksi melalui jaringan pribadi mungkin gagal.

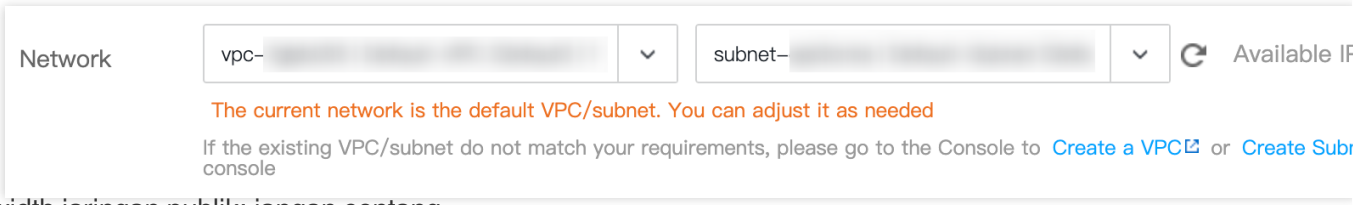
Zona Ketersediaan: pilih zona ketersediaan tempat subnet berada. VPC memungkinkan subnet di zona ketersediaan yang berbeda, dan subnet ini dapat berkomunikasi satu sama lain melalui jaringan pribadi secara default.

Opsi Lanjutan: Anda dapat menambahkan tag secara opsional untuk membantu Anda mengelola izin sumber daya sub-pengguna dan kolaborator dengan lebih baik.

Langkah 2: beli instans CVM

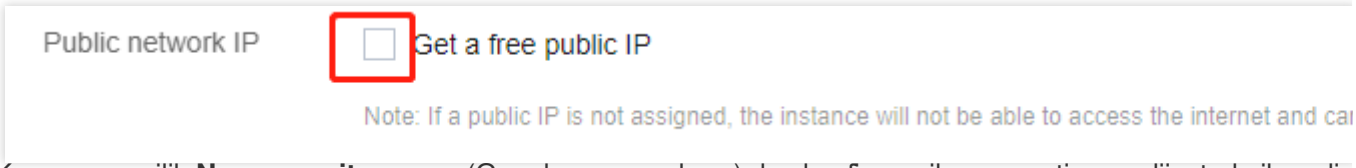
1. Masuk ke Konsol CVM untuk membuat instans CVM di VPC yang dibuat pada langkah sebelumnya.
2. Klik **Create** (Buat) di sudut kiri atas halaman daftar untuk mengakses halaman pembelian CVM.
3. Pada halaman konfigurasi kustom, konfigurasikan instans CVM lalu klik **Buy Now** (Beli Sekarang). Konfigurasi jaringan CVM adalah sebagai berikut:

Jaringan: pilih VPC dan subnet yang dibuat.

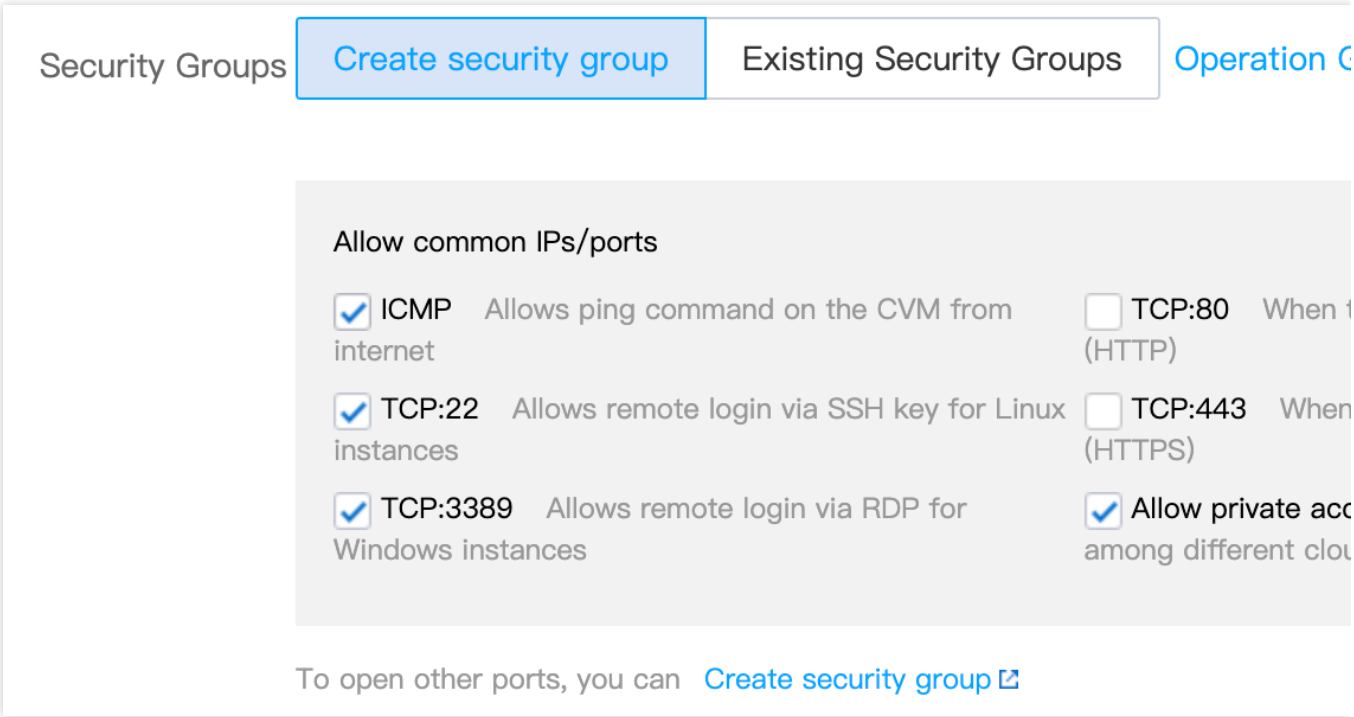


Bandwidth jaringan publik: jangan centang

.



Grup Keamanan: pilih **New security group** (Grup keamanan baru) dan konfigurasikan seperti yang diinstruksikan di Mengonfigurasi Grup Keamanan.



Langkah 3: terapkan untuk EIP dan ikat ke instans CVM

IP Elastis (EIP) adalah alamat IP publik yang dapat diterapkan dan dibeli secara mandiri. Anda dapat mengikatnya ke instans CVM untuk mengaktifkan akses jaringan publik.

1. Login ke Konsol EIP.
2. Pada halaman **EIP** (EIP), pilih wilayah tempat CVM berada. Klik **Apply** (Terapkan) di sudut kiri atas.
3. Di jendela **Apply for EIP** (Terapkan untuk EIP), konfigurasikan parameter yang relevan dan klik **OK** (Oke).
4. Pada halaman **EIP** (EIP), cari EIP yang Anda terapkan, dan klik **More** (Lainnya) > **Bind** (Ikat) di bawah kolom **Operation** (Operasi).
5. Di jendela **Bind resources** (Ikat sumber daya), pilih **CVM Instances** (Instans CVM) sebagai jenis sumber daya yang akan diikat, pilih instans CVM, dan klik **OK** (Oke).
6. Di jendela konfirmasi pop-up, klik **OK** (Oke).

Langkah 4: uji konektivitas jaringan publik

Selesaikan operasi berikut untuk menguji konektivitas jaringan publik instans CVM.

Keterangan:

Sebelum melakukan pengujian, pastikan grup keamanan mengizinkan akses ke alamat IP dan port yang sesuai. Misalnya, protokol ICMP dibuka, dan server dapat di-ping melalui jaringan publik. Untuk informasi selengkapnya, lihat Melihat Aturan Grup Keamanan.

1. Login ke instans CVM dengan EIP terikat. Untuk petunjuk mendetail, lihat Login dan Akses Jarak Jauh.
2. Jalankan perintah `ping <public IP address>` , seperti `ping www.qq.com` untuk menguji konektivitas jaringan publik.