

Virtual Private Cloud

Deskripsi Produk

Dokumen produk



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.

Direktori dokumen

Deskripsi Produk

Ikhtisar

Kekuatan

Kasus Penggunaan

Konsep

Wilayah dan Zona Ketersediaan

Alamat IP

Jaringan Klasik

Batas Kuota

Deskripsi Produk

Ikhtisar

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

Virtual Private Cloud (VPC) adalah ruang jaringan virtual yang terisolasi secara logis di Tencent Cloud. Dengan VPC, Anda dapat mengonfigurasi ruang jaringan yang terisolasi secara logis untuk sumber daya Anda seperti [CVM](#) dan [database cloud](#). Produk ini memberikan keamanan sumber daya cloud yang lebih baik dan dapat memenuhi kebutuhan Anda dalam berbagai skenario.

Dokumen ini memperkenalkan komponen inti, mode koneksi, dan keamanan VPC.

Komponen Inti

Instans VPC memiliki tiga komponen inti: Rentang IP VPC, subnet, dan tabel rute.

Rentang IP VPC

Saat membuat VPC, Anda perlu menentukan blok CIDR [classless inter-domain routing](#) sebagai grup alamat IP VPC. Tencent Cloud VPC mendukung blok CIDR di salah satu rentang IP pribadi berikut:

10.0.0.0 - 10.255.255.255 (the mask range must be 16 to 28) (rentang mask harus 16 hingga 28))

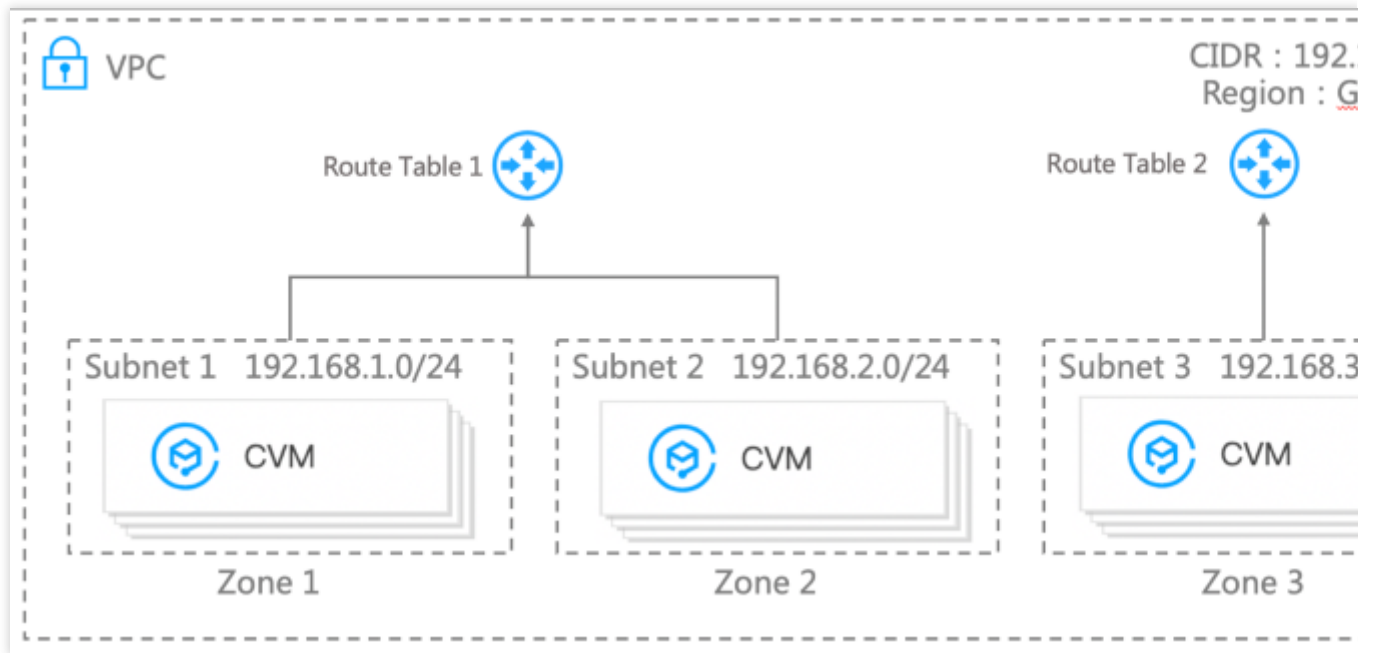
172.16.0.0 - 172.31.255.255 (the mask range must be 16 to 28) (rentang mask harus 16 hingga 28))

192.168.0.0 - 192.168.255.255 (the mask range must be 16 to 28) (rentang mask harus 16 hingga 28))

Subnet

VPC terdiri dari setidaknya satu subnet. Semua sumber daya cloud di VPC (seperti CVM dan database cloud) harus di-deploy di subnet, dan blok CIDR subnet harus berada di dalam blok CIDR VPC.

VPC disiapkan di tingkat [wilayah](#) (seperti Guangzhou), sedangkan subnet diatur di level [zona ketersediaan](#) (seperti Zona Guangzhou 1). Anda setidaknya dapat membagi VPC menjadi satu subnet. Subnet pada VPC yang sama dapat saling terhubung secara default, sementara subnet pada VPC yang berbeda diisolasi secara default.



Tabel rute

Saat Anda membuat VPC, sistem secara otomatis membuat tabel rute default untuk memastikan bahwa semua subnet di VPC saling terhubung. Jika kebijakan perutean di tabel rute default tidak dapat memenuhi kebutuhan bisnis Anda, Anda bisa membuat tabel rute kustom.

Untuk informasi selengkapnya tentang tabel rute, lihat [Ikhtisar Tabel Rute](#).

Koneksi VPC

Tencent Cloud menyediakan berbagai solusi koneksi VPC untuk berbagai skenario.

CVM dan database cloud di VPC dapat terhubung ke Internet melalui IP Elastis dan NAT Gateway.

Koneksi Peering dan Jaringan Cloud Connect digunakan untuk mengaktifkan komunikasi antar VPC.

VPC dan IDC lokal saling terhubung melalui Koneksi VPN, Direct Connect, dan Cloud Connect Network.

Keamanan VPC

VPC adalah ruang jaringan virtual yang terisolasi secara logis di Tencent Cloud. VPC yang berbeda saling terisolasi untuk melindungi keamanan bisnis.

Grup keamanan: grup keamanan adalah firewall virtual stateful yang mampu memfilter. Grup keamanan ini mengontrol lalu lintas masuk dan keluar pada tingkat instans dan merupakan sarana penting untuk isolasi keamanan jaringan.

Access Control List (ACL) Jaringan: jaringan ACL adalah firewall virtual stateless untuk memfilter paket di tingkat subnet. Dapat digunakan untuk mengontrol aliran data masuk dan keluar subnet pada protokol dan granularitas port.

Cloud Access Management (CAM): CAM membantu Anda mengelola akses ke sumber daya Tencent Cloud dengan aman. Misalnya, CAM menyediakan manajemen identitas dan manajemen kebijakan agar Anda dapat mengontrol siapa yang memiliki akses ke VPC Anda.

Untuk informasi selengkapnya tentang keamanan VPC, lihat [Manajemen Keamanan](#).

Kekuatan

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

Kustomisasi Jaringan

VPC memberi Anda kemampuan manajemen jaringan yang kuat. Anda dapat menyesuaikan rentang IP dan membuat subnet seperti di jaringan tradisional, sambil mengonfigurasi tabel rute dan kebijakan perutean secara fleksibel untuk men-deploy layanan cloud Anda.

Tencent Cloud VPC juga menyediakan topologi jaringan untuk membantu Anda memvisualisasikan dan merencanakan jaringan.

Dapat Diskalakan

Anda dapat membuat subnet yang berbeda dalam satu atau beberapa VPC untuk men-deploy bisnis Anda di lingkungan VPC yang dapat diskalakan. Anda juga dapat menghubungkan VPC dengan IDC lokal, VPC lain, dan jaringan klasik untuk memperluas arsitektur jaringan sesuai kebutuhan.

Mode Akses Berbeda

VPC menyediakan mode akses yang berbeda untuk memenuhi kebutuhan komunikasi cloud:

Akses Internet: Anda dapat mengakses Internet melalui IP publik, EIP, NAT Gateway, CLB, dll.

Akses instans VPC lainnya: Anda dapat mengakses instans VPC lain melalui CCN, koneksi peering, dll.

Akses IDC lokal: Anda dapat mengakses IDC lokal melalui koneksi VPN, Direct Connect, dan CCN.

Akses jaringan klasik: Anda dapat mengakses bisnis yang di-deploy di jaringan klasik melalui Classiclink.

Keamanan dan Keandalan

VPC menggunakan teknologi tunneling untuk membangun jaringan virtual di jaringan fisik, dan teknologi Overlay untuk mencapai isolasi jaringan pribadi antar instans VPC. VPC memberi Anda jaringan cloud yang independen, terisolasi, dan aman.

Untuk CVM dalam VPC, kami juga memberi Anda kontrol akses di berbagai tingkat, seperti grup keamanan dan ACL jaringan.

Kemudahan Penggunaan

Anda dapat membuat dan mengelola instans VPC dengan mudah dan cepat melalui konsol, API, dll. Fitur jaringan yang dihasilkan dan metode pemecahan masalah yang berbeda membantu mengurangi biaya OPS Anda.

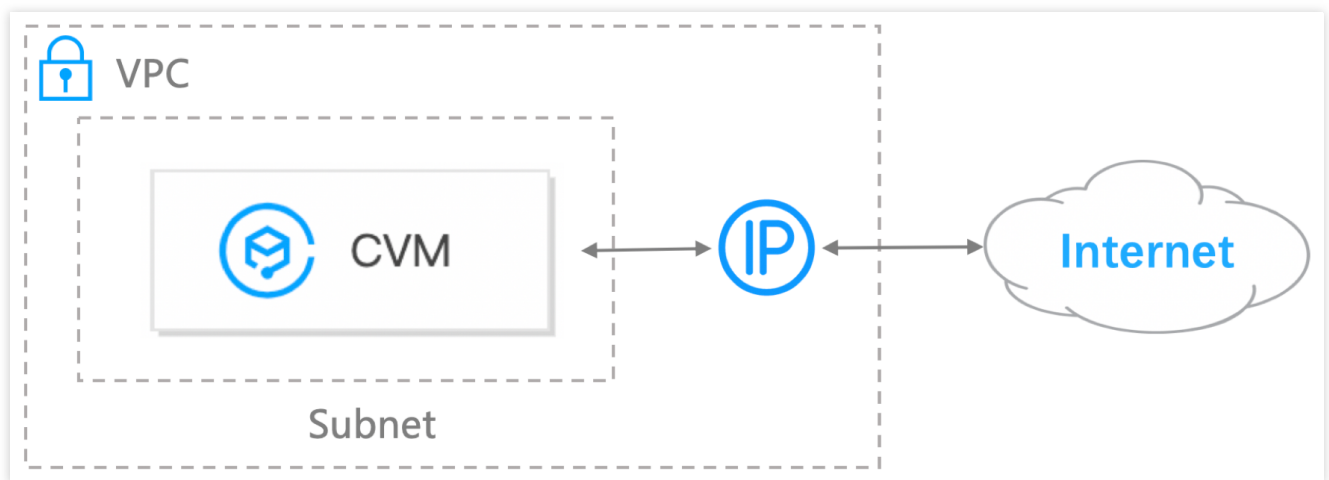
Kasus Penggunaan

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

Mengakses Internet

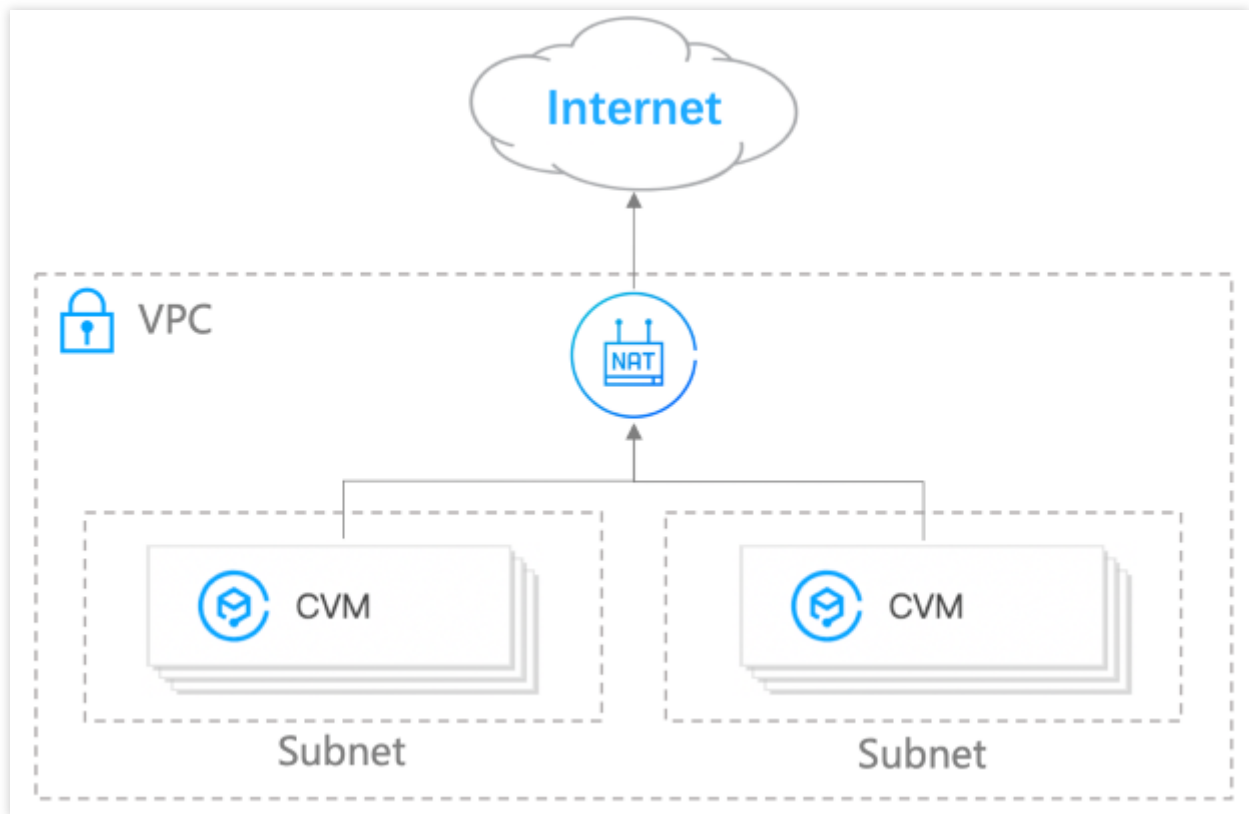
Satu CVM

Ketika lalu lintas ke bisnis Anda rendah dan hanya satu CVM yang tersedia, Anda dapat menerapkan untuk alamat IP publik dan mengikatnya dengan CVM untuk mendapatkan akses ke Internet.



Beberapa CVM

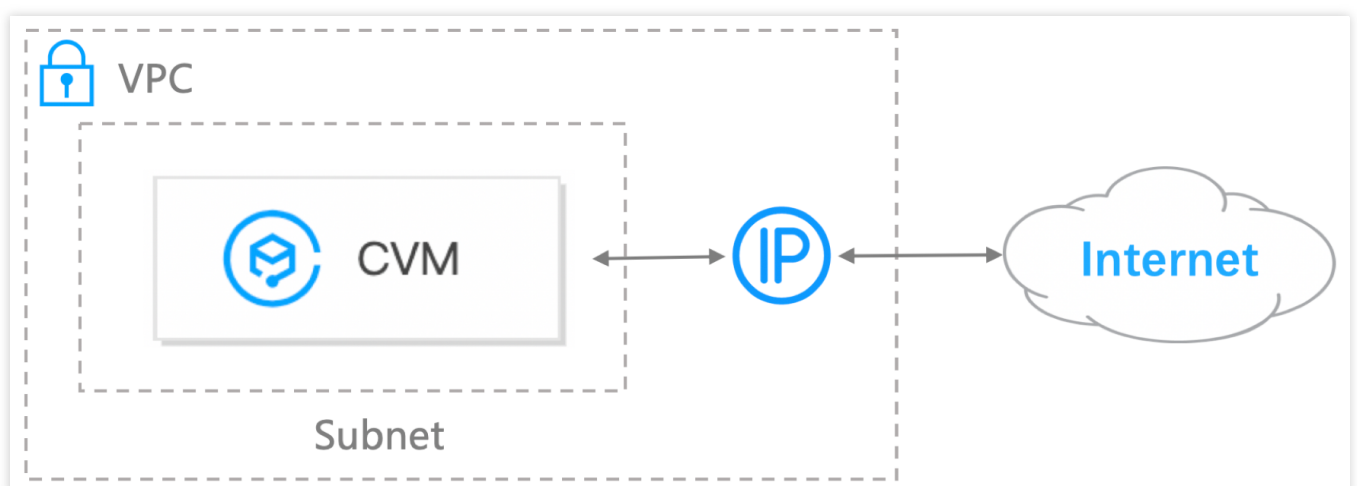
Bila Anda memiliki beberapa CVM yang perlu mengakses Internet secara bersamaan dan Anda tidak ingin alamat jaringan pribadi CVM terekspos, Anda dapat menggunakan [Gateway NAT](#). Gateway NAT menyediakan fitur SNAT dan memungkinkan beberapa CVM untuk mengakses Internet dengan alamat IP publik di gateway NAT. Selain itu, tanpa konfigurasi fitur DNAT, pengguna eksternal tidak dapat mengakses langsung gateway NAT, yang memastikan keamanannya. Ketika beberapa alamat IP publik ada di gateway NAT, gateway NAT secara otomatis melakukan penyeimbangan beban.



Menyediakan Layanan ke Internet

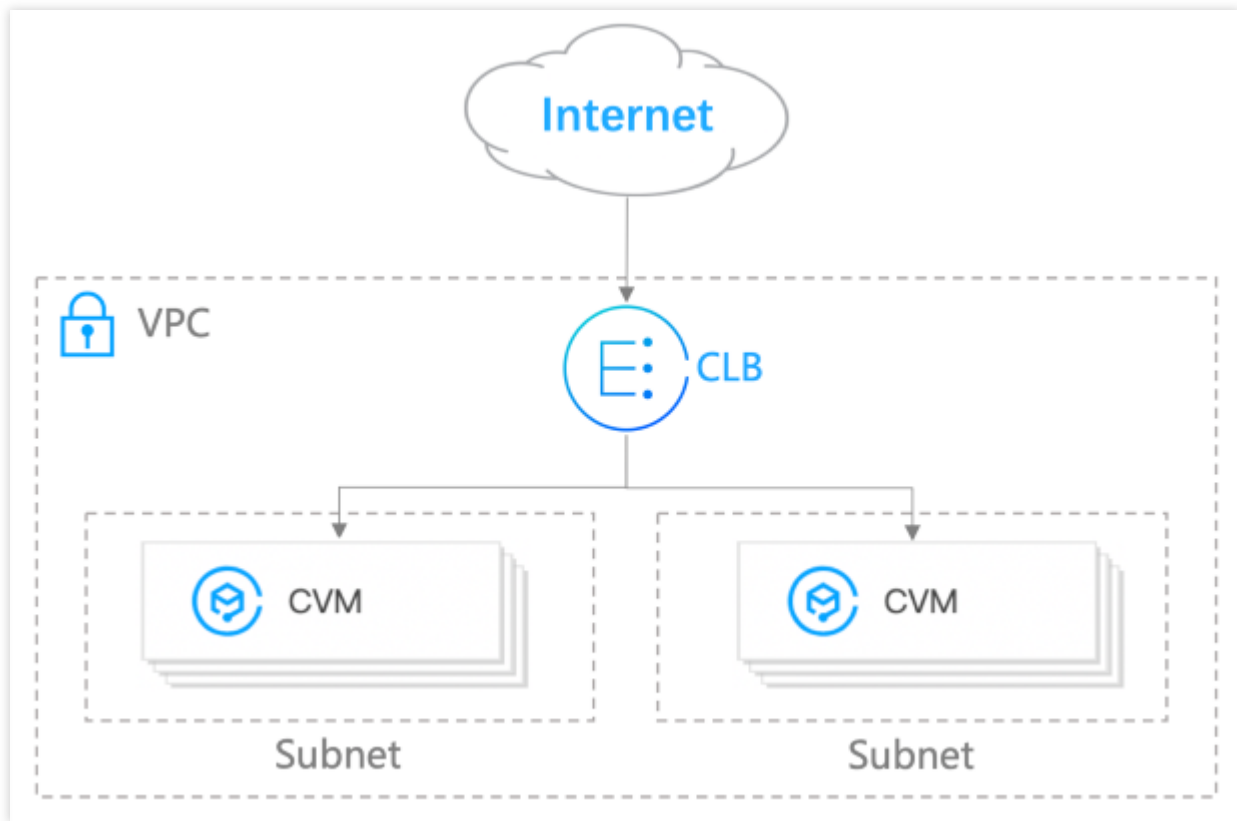
Satu CVM

Anda dapat mengelola layanan (seperti layanan situs web) pada CVM berbasis VPC dan menggunakan alamat IP publik untuk menyediakan layanan kepada pengguna eksternal.



Beberapa CVM

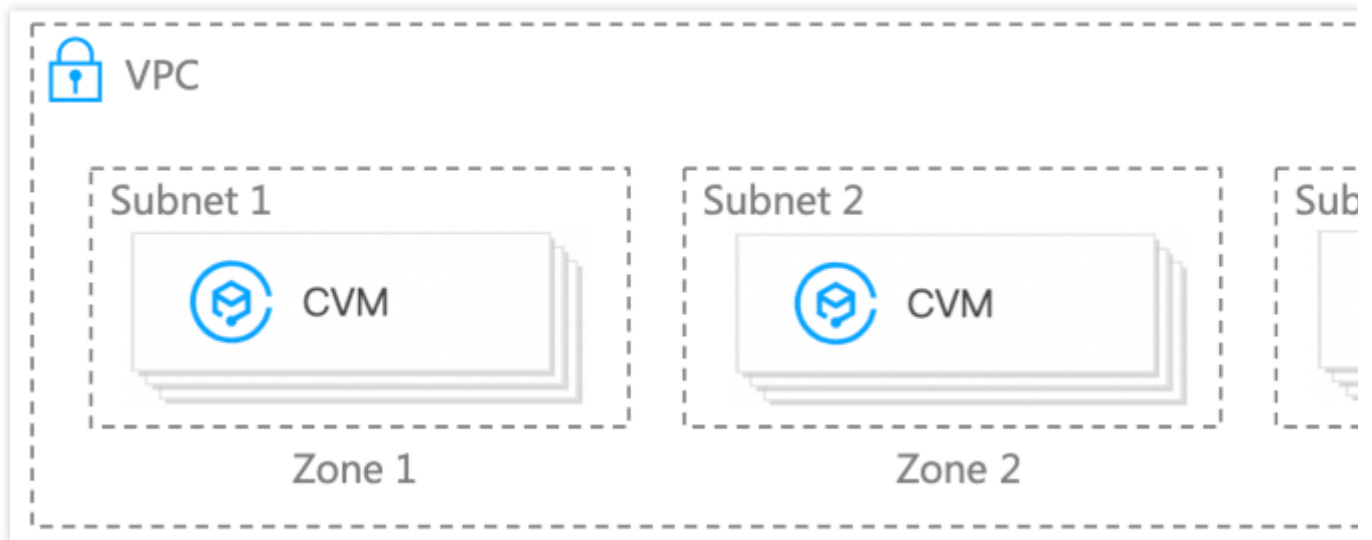
Ketika Anda memiliki banyak CVM untuk men-deploy layanan kompleks dan lalu lintas Internet tinggi, Anda dapat menggunakan [Cloud Load Balancer \(CLB\)](#). CLB dapat secara otomatis mendistribusikan lalu lintas akses aplikasi di antara instans CVM di cloud, yang meningkatkan toleransi kesalahan untuk aplikasi.



Pemulihan Bencana untuk Aplikasi

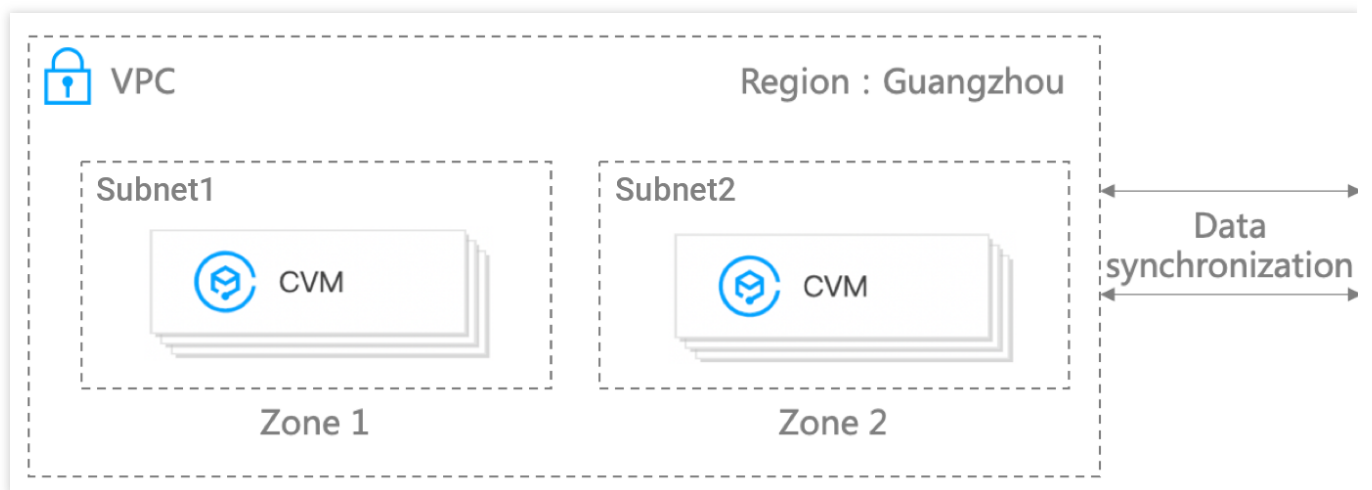
Pemulihan Bencana Zona Ketersediaan Lintas

Subnet dikaitkan dengan zona ketersediaan. Anda dapat membuat subnet di zona ketersediaan yang berbeda dari satu VPC di suatu wilayah. Secara default, subnet yang berbeda dari VPC yang sama saling terhubung melalui jaringan pribadi. Anda dapat men-deploy sumber daya di subnet dari zona ketersediaan yang berbeda untuk mencapai pemulihan bencana zona lintas-ketersediaan.



Pemulihan Bencana Lintas-Wilayah

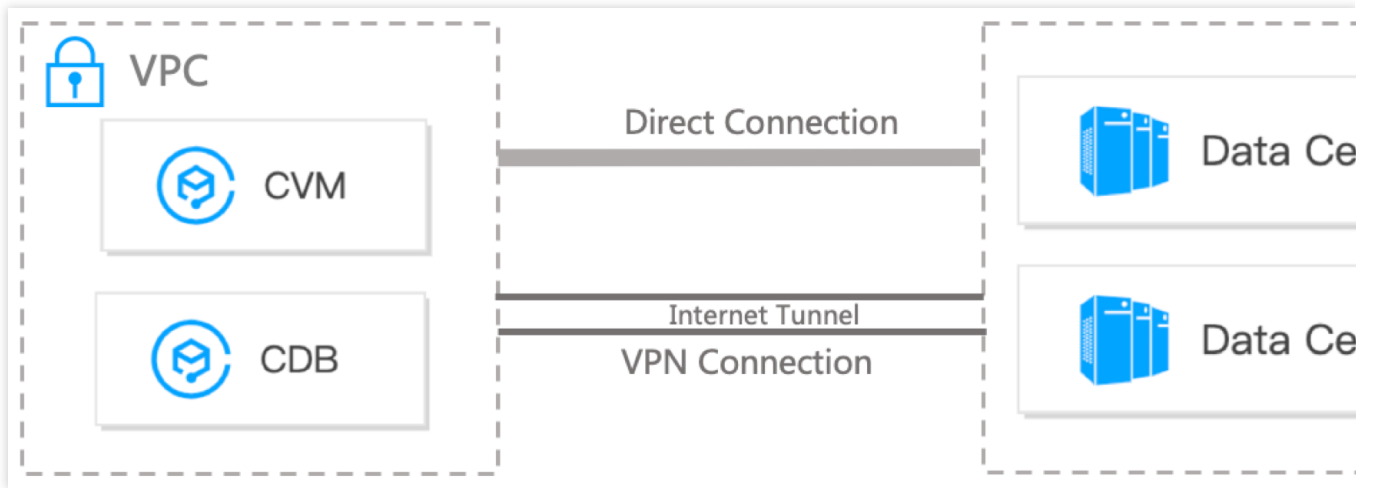
Anda dapat men-deploy bisnis di seluruh wilayah (misalnya, solusi 2-region-3-DC) untuk mencapai pemulihan bencana lintas wilayah.



Men-deploy Cloud Hibrida

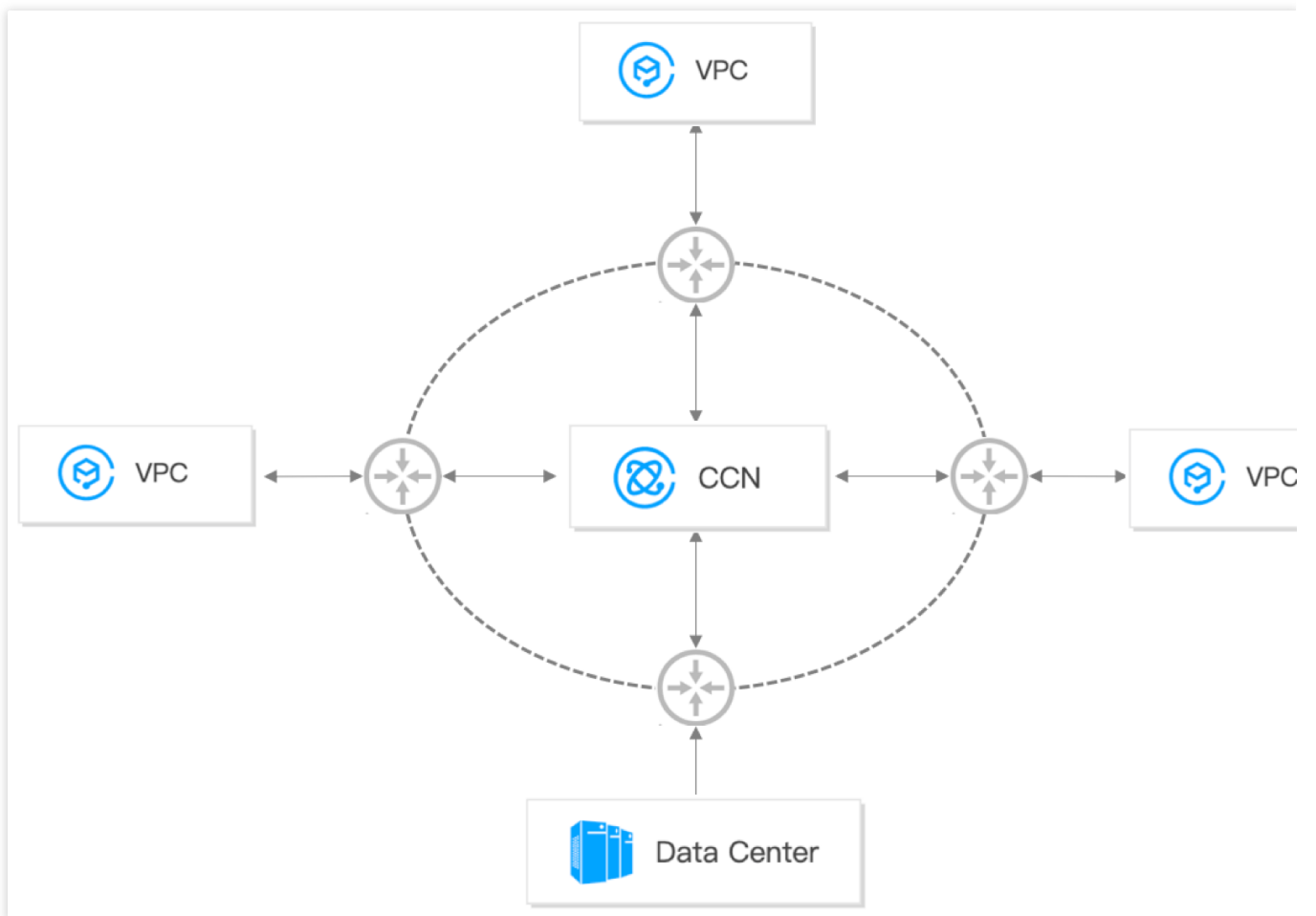
Menghubungkan ke IDC Lokal

VPC menyediakan beberapa mode koneksi, seperti koneksi langsung dan koneksi VPN, yang dapat menghubungkan IDC lokal Anda dengan instans VPC di cloud untuk membuat arsitektur cloud hibrida dengan mudah. Menggunakan IDC lokal memastikan keamanan data inti Anda. Anda dapat memperluas sumber daya (seperti CVM dan TencentDB) di cloud berdasarkan volume bisnis Anda untuk mengurangi biaya Operasi TI.



Interkoneksi Multi-Titik Global

Saat Anda memiliki bisnis yang di-deploy di beberapa wilayah di seluruh dunia dan memerlukan interkoneksi lintas wilayah, Anda dapat menggunakan produk seperti [CCN](#) dan [Direct Connect](#) untuk mengaktifkan interkoneksi multi-titik global melalui akses titik-tunggal.



Konsep Wilayah dan Zona Ketersediaan

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

Wilayah

Ikhtisar

Wilayah adalah lokasi fisik dari IDC. Di Tencent Cloud, wilayah sepenuhnya terisolasi satu sama lain, memastikan stabilitas lintas wilayah dan toleransi kesalahan. Sebaiknya Anda memilih wilayah yang paling dekat dengan pengguna akhir Anda untuk meminimalkan latensi akses dan meningkatkan kecepatan akses.

Silakan lihat tabel berikut atau gunakan [DescribeRegions](#) API untuk mendapatkan daftar wilayah dengan daftar wilayah lengkap.

Karakteristik

Jaringan dari berbagai wilayah sepenuhnya terisolasi. Layanan Tencent Cloud di berbagai wilayah **cannot communicate via a private network by default** (tidak dapat berkomunikasi melalui jaringan pribadi secara default).

Layanan Tencent Cloud di seluruh wilayah dapat saling berkomunikasi melalui [IP publik](#) melalui Internet, sedangkan layanan di VPC yang berbeda dapat saling berkomunikasi melalui [CCN](#), yang lebih cepat dan lebih stabil.

[Cloud Load Balancer \(CLB\)](#) saat ini mendukung penerusan lalu lintas dalam wilayah secara default. Jika Anda mengaktifkan fitur [Cross-Region Binding 2.0 \(New\) \(Pengikatan Lintas Wilayah 2.0 \(Baru\)\)](#), pengikatan lintas wilayah instans CLB dan CVM didukung.

Zona Ketersediaan

Ikhtisar

Zona ketersediaan (Zona) mengacu pada pusat data fisik Tencent Cloud yang kekuatan dan jaringannya saling independen dalam wilayah yang sama. Zona-zona ini dirancang untuk memastikan bahwa kegagalan dalam zona ketersediaan dapat diisolasi (kecuali untuk bencana skala besar atau kegagalan daya besar) tanpa menyebar ke zona lain, untuk memastikan stabilitas bisnis Anda. Dengan memulai instans di zona ketersediaan independen, pengguna dapat melindungi aplikasi mereka agar tidak terpengaruh oleh satu titik kegagalan.

Silakan lihat tabel berikut atau gunakan [DescribeZones](#) API untuk mendapatkan daftar zona ketersediaan lengkap.

Karakteristik

Layanan Tencent Cloud di VPC yang sama saling terhubung melalui jaringan pribadi, yang berarti mereka dapat berkomunikasi menggunakan [IP pribadi](#), meskipun berada di zona ketersediaan yang berbeda dengan wilayah yang sama.

Keterangan:

Interkoneksi jaringan pribadi mengacu pada interkoneksi sumber daya dalam akun yang sama. Sumber daya dalam akun yang berbeda sepenuhnya terisolasi di jaringan pribadi.

Tiongkok

Wilayah	AZ
Tiongkok Selatan (Guangzhou)ap-guangzhou	Zona 1 Guangzhou (terjual habis) ap-guangzhou-1
	Zona 2 Guangzhou (terjual habis)ap-guangzhou-2
	Zona 3 Guangzhou ap-guangzhou-3
	Zona 4 Guangzhouap-guangzhou-4
	Zona 6 Guangzhouap-guangzhou-6
	Zona 7 Guangzhouap-guangzhou-7
Tiongkok Timur (Shanghai)ap-shanghai	Zona 1 Shanghaiap-shanghai-1
	Zona 2 Shanghaiap-shanghai-2
	Zona 3 Shanghaiap-shanghai-3
	Zona 4 Shanghaiap-shanghai-4
	Zona 5 Shanghai ap-shanghai-5
Tiongkok Timur (Nanjing)ap-nanjing	Zona 1 Nanjingap-nanjing-1
	Zona 2 Nanjingap-nanjing-2
	Zona 3 Nanjingap-nanjing-3
Tiongkok Utara (Beijing)ap-beijing	Zona 1 Beijingap-beijing-1
	Zona 2 Beijingap-beijing-2

	Zona 3 Beijingap-beijing-3
	Zona 4 Beijingap-beijing-4
	Zona 5 Beijing ap-beijing-5
	Zona 6 Beijingap-beijing-6
	Zona 7 Beijingap-beijing-7
Tiongkok Barat Daya (Chengdu)ap-chengdu	Zona 1 Chengduap-chengdu-1
	Zona 2 Chengduap-chengdu-2
Tiongkok Barat Daya (Chongqing)ap-chongqing	Zona 1 Chongqingap-chongqing-1
Hong Kong, Makau dan Taiwan, Tiongkok (Hong Kong)ap-hongkong	Zona 1 Hong Kong (Node di Hong Kong, Tiongkok dapat mencakup layanan di wilayah Hong Kong/Makau/Taiwan)ap-hongkong-1
	Zona 2 Hong Kong (Node di Hong Kong, Tiongkok dapat mencakup layanan di wilayah Hong Kong/Makau/Taiwan)ap-hongkong-2
	Zona 3 Hong Kong (Node di Hong Kong, Tiongkok dapat mencakup wilayah Hong Kong/Makau/Taiwan)ap-hongkong-3

Negara dan wilayah lain

Wilayah	AZ
Asia Tenggara (Singapura)ap-singapore	Zona 1 Singapura (Node di Singapura dapat mencakup Asia Tenggara)ap-singapore-1
	Zona 2 Singapura (Node di Singapura dapat mencakup Asia Tenggara)ap-singapore-2
	Zona 3 Singapura (Node di Singapura dapat mencakup Asia Tenggara)ap-singapore-3
Asia Timur Laut (Seoul)ap-seoul	Zona 1 Seoul (Node di Seoul dapat mencakup Asia Timur Laut)ap-seoul-1

	Zona 2 Seoul (Node di Seoul dapat mencakup Asia Timur Laut)ap-seoul-2
Asia Timur Laut (Tokyo)ap-tokyo	Zona 1 Tokyo (Node di Tokyo dapat mencakup Asia Timur Laut)ap-tokyo-1
	Zona 2 Tokyo (Node di Tokyo dapat mencakup Asia Timur Laut)ap-tokyo-2
Asia Selatan (Mumbai)ap-mumbai	Zona 1 Mumbai (Node di Mumbai dapat mencakup Asia Selatan)ap-mumbai-1
	Zona 2 Mumbai (Node di Mumbai dapat mencakup Asia Selatan)ap-mumbai-2
Asia Tenggara (Bangkok)ap-bangkok	Zona 1 Bangkok (Node di Bangkok dapat mencakup Asia Tenggara)ap-bangkok-1
	Zona 2 Bangkok (Node di Bangkok dapat mencakup Asia Tenggara)ap-bangkok-2
Amerika Utara (Toronto)na-toronto	Zona 1 Toronto (Node di Toronto dapat mencakup Amerika Utara)na-toronto-1
AS Barat (Silicon Valley)na-siliconvalley	Zona 1 Silicon Valley (Node di Silicon Valley dapat mencakup AS Barat)na-siliconvalley-1
	Zona 2 Silicon Valley (Node di Silicon Valley dapat mencakup AS Barat)na-siliconvalley-2
AS Timur (Virginia)na-ashburn	Zona 1 Virginia (Node di Virginia dapat mencakup AS Timur)na-ashburn-1
	Zona 2 Virginia (Node di Virginia dapat mencakup AS Timur)na-ashburn-2
Eropa (Frankfurt)eu-frankfurt	Zona 1 Frankfurt (Node di Frankfurt dapat mencakup Eropa)eu-frankfurt-1
	Zona 2 Frankfurt (Node di Frankfurt dapat mencakup Eropa)eu-frankfurt-2
Eropa (Moskow)eu-moscow	Zona 1 Moskow (Node di Moskow dapat mencakup Eropa)eu-moscow-1

Cara memilih wilayah dan zona ketersediaan

Saat memilih wilayah dan zona ketersediaan, pertimbangkan hal berikut:

Lokasi Anda, lokasi pengguna Anda, dan wilayah instans CVM.

Sebaiknya Anda memilih wilayah yang paling dekat dengan pengguna akhir Anda saat membeli instans CVM untuk meminimalkan latensi akses dan meningkatkan kecepatan akses.

Layanan Tencent Cloud lain yang Anda gunakan.

Saat Anda memilih layanan Tencent Cloud lainnya, sebaiknya Anda mencoba menempatkan semuanya di wilayah dan zona ketersediaan yang sama agar layanan dapat berkomunikasi satu sama lain melalui jaringan pribadi, mengurangi latensi akses dan meningkatkan kecepatan akses.

Ketersediaan tinggi dan pemulihan bencana.

Meskipun Anda hanya memiliki satu VPC, kami tetap menyarankan agar Anda men-deploy bisnis Anda di zona ketersediaan yang berbeda untuk mencegah satu titik kegagalan dan mengaktifkan pemulihan bencana lintas-AZ.

Mungkin ada latensi jaringan di antara zona ketersediaan yang berbeda. Sebaiknya Anda menilai kebutuhan bisnis Anda dan menemukan keseimbangan optimal antara ketersediaan tinggi dan latensi rendah.

Ketersediaan Sumber Daya

Tabel berikut menjelaskan sumber daya Tencent Cloud mana yang bersifat global, yang bersifat regional, dan yang khusus untuk zona ketersediaan.

Sumber Daya	Format ID Sumber Daya -8-Digit String Angka dan Huruf	Jenis	Deskripsi
Akun Pengguna	Tidak ada batasan	Unik secara global	Pengguna dapat menggunakan akun yang sama untuk mengakses sumber daya Tencent Cloud seluruh dunia.
Kunci SSH	skey-xxxxxxx	Global	Pengguna dapat menggunakan kunci SSH untuk mengikat CVM di wilayah mana pun dalam akun.
Instans CVM	ins-xxxxxxx	Instans CVM khusus untuk zona ketersediaan	Pengguna hanya dapat membuat instans CVM di AZ tertentu.
Citra Kustom	img-xxxxxxx	Regional	Pengguna dapat membuat Citra kustom untuk instans yang dapat digunakan di zona ketersediaan berbeda di wilayah yang sama. Salin citra kustom ke wilayah lain menggunakan fungsi salin citra untuk menggunakannya di wilayah tersebut.

EIP	eip-xxxxxxx	Dapat digunakan di beberapa AZ di suatu wilayah	EIP (IP Elastis) hanya dapat dibuat di suatu wilayah dan dikaitkan dengan instans di wilayah yang sama.
Grup Keamanan	sg-xxxxxxx	Dapat digunakan di beberapa AZ di suatu wilayah	Grup Keamanan hanya dapat dikaitkan dengan instans di wilayah yang sama. Tencent Cloud secara otomatis membuat 3 Grup Keamanan default untuk pengguna.
Cloud Block Storage	disk-xxxxxxx	Disk CBS khusus untuk zona ketersediaan.	Pengguna hanya dapat membuat disk Cloud Block Storage di AZ tertentu dan memasangnya ke instans di zona ketersediaan yang sama.
Snapshot	snap-xxxxxxx	Dapat digunakan di beberapa AZ di suatu wilayah	Snapshot yang dibuat dari disk cloud dapat digunakan untuk tujuan lain (seperti membuat disk cloud) di wilayah ini.
Cloud Load Balancer	clb-xxxxxxx	Dapat digunakan di beberapa Zona Ketersediaan di suatu wilayah	Cloud Load Balancer dapat diikat dengan CVM di zona ketersediaan yang berbeda dari satu wilayah untuk penerusan lalu lintas.
VPC	vpc-xxxxxxx	Tersedia di beberapa zona ketersediaan di satu wilayah	VPC di satu wilayah dapat memiliki sumber daya yang dibuat di zona ketersediaan yang berbeda di wilayah tersebut.
Subnet	subnet-xxxxxxx	Subnet khusus untuk zona ketersediaan.	Pengguna tidak dapat membuat subnet di seluruh zona ketersediaan.
Tabel Rute	rtb-xxxxxxx	Dapat digunakan di beberapa AZ di suatu wilayah	Saat membuat tabel rute, pengguna harus menentukan VPC. Oleh karena itu, tabel rute juga bersifat regional.

Referensi

Memigrasikan instans ke zona ketersediaan lain

Untuk instans yang sudah dimulai, zona ketersediaannya tidak dapat diubah, tetapi penggunaannya dapat memigrasikannya ke zona ketersediaan lain dengan cara lain. Proses migrasi melibatkan pembuatan citra kustom dari instans asli, menggunakan citra kustom untuk memulai instans di zona ketersediaan baru dan memperbarui konfigurasi instans baru.

1. Buat citra kustom untuk instans sumber. [Membuat Citra Kustom](#)

2. Jika [lingkungan jaringan](#) instans saat ini adalah VPC dan alamat IP pribadi harus tetap dipertahankan setelah migrasi, hapus subnet di zona ketersediaan saat ini, lalu buat subnet di zona ketersediaan baru dengan rentang alamat IP yang sama dengan subnet asli. Perhatikan bahwa subnet hanya dapat dihapus jika tidak ada instans yang tersedia. Oleh karena itu, semua instans di subnet saat ini harus dimigrasikan ke subnet baru.
3. Buat instans baru di Zona Ketersediaan baru menggunakan citra kustom yang baru saja Anda buat. Anda dapat memilih jenis dan konfigurasi yang sama seperti instans asli, atau memilih yang baru. Untuk informasi selengkapnya, lihat [Membuat Instans melalui Halaman Pembelian CVM](#).
4. Jika instans sumber dikaitkan dengan EIP, batalkan pengaitan EIP dan kaitkan dengan instans baru. Untuk informasi selengkapnya tentang mematikan instans, lihat [Mematikan Instans](#).
5. Untuk informasi selengkapnya, lihat [Menghentikan Instans](#).

Menyalin citra ke wilayah lain

Atribut wilayah dibedakan untuk semua perilaku, seperti mengaktifkan dan melihat instans oleh pengguna. Jika citra instans yang perlu diaktifkan oleh pengguna tidak ada di wilayah tersebut, maka citranya perlu disalin ke wilayah saat ini. [Menyalin Citra](#)

Alamat IP

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


Alamat IP mendukung protokol pengalamatan IPv4 dan IPv6. IPv4 banyak digunakan, tetapi jumlah alamat jaringannya terbatas, menjadikan IPv6 sebagai pelengkap yang baik.

Alamat IPv4

Tencent Cloud menyediakan alamat IPv4 untuk akses jaringan pribadi dan publik. Alamat IPv4 publik dapat bersifat umum atau elastis. Seperti yang ditunjukkan pada gambar berikut, **EIP** (EIP) menunjukkan alamat IPv4 elastis, **Private** (Pribadi) menunjukkan alamat IPv4 pribadi, dan **Public** (Publik) menunjukkan alamat IPv4 publik. IP ini tidak akan berubah kecuali Anda melepas ikatan atau mengubahnya.

Keterangan:

Kecuali ditentukan lain, IP pribadi, IP publik, dan EIP semuanya merujuk ke alamat IPv4.



<input type="checkbox"/>	ins-	Shut down	Guangzhou Zone 3	Standard S5	1-core 2GB 1Mbps	42 (EIP) (Private)	1
<input type="checkbox"/>	ins-	Running	Guangzhou Zone 3	Standard S5	2-core 4GB 1Mbps	228 (Public) (Private)	2

Alamat IPv4 Pribadi

Alamat IPv4 pribadi digunakan untuk akses jaringan pribadi Tencent Cloud, yang tidak dapat digunakan untuk mengakses internet. Setelah instans CVM dibuat, instans tersebut akan secara otomatis ditetapkan dengan alamat IPv4 pribadi. Alamat IPv4 pribadi juga dapat dikustomisasi dalam lingkungan VPC.

Atribut

Jaringan pribadi IPv4 spesifik pengguna, dan pengguna yang berbeda saling terisolasi. Secara default, layanan cloud pengguna lain tidak dapat diakses melalui jaringan pribadi IPv4.

Jaringan pribadi IPv4 spesifik wilayah, dan wilayah yang berbeda saling terisolasi. Secara default, layanan cloud yang menggunakan akun yang sama di wilayah yang berbeda tidak dapat diakses melalui jaringan pribadi IPv4.

Kasus penggunaan

Alamat IPv4 pribadi dapat digunakan untuk:

Interkoneksi antara instans CLB dan CVM berbasis jaringan klasik atau berbasis VPC melalui jaringan pribadi IPv4.

Interkoneksi antara instans CVM berbasis jaringan klasik atau berbasis VPC melalui jaringan pribadi IPv4.

Interkoneksi antara instans CVM berbasis jaringan atau klasik berbasis VPC dan layanan Tencent Cloud lainnya (seperti TencentDB) melalui jaringan pribadi IPv4.

Operasi yang relevan

Untuk informasi selengkapnya tentang cara mendapatkan alamat IPv4 pribadi instans dan DNS yang ditetapkan, lihat [Mendapatkan Alamat IP Pribadi dan Mengatur DNS](#).

Untuk informasi selengkapnya tentang cara mengubah alamat IPv4 pribadi instans CVM di VPC, lihat [Memodifikasi Alamat IP Pribadi](#).

Alamat IPv4 publik

Tencent Cloud menyediakan IP dan EIP publik untuk akses jaringan publik. Instans CVM dengan alamat IPv4 publik dapat mengakses dan diakses melalui jaringan publik IPv4.

Perbandingan

Tabel berikut membandingkan IP publik dengan EIP.

Item	IP Publik	EIP
Kasus penggunaan	Jika Anda ingin membuat CVM yang mendukung akses jaringan publik, Anda dapat memilih menggunakan alamat IP publik yang ditetapkan secara otomatis oleh sistem saat membuat instans CVM. Alamat IP publik ini memiliki siklus pemakaian yang sama dengan CVM, dan akan dilepas setelah pelepasan CVM yang terikat.	Jika ingin menggunakan IP publik dalam waktu lama, Anda dapat memilih IP elastis (EIP) dan mengikatnya ke CVM yang ditentukan sesuai kebutuhan. EIP dapat diikat atau dilepas ikatannya berkali-kali, dan akan tetap ada setelah CVM dilepas.
Akses jaringan publik	Keduanya mendukung akses jaringan publik.	
Metode akuisisi	Metode ini hanya dapat diperoleh ketika Anda membeli CVM.	<ol style="list-style-type: none"> 1. Terapkan untuk EIP di konsol. 2. Ubah alamat IP publik menjadi EIP.
Fitur	Alamat IP ini memiliki siklus pemakaian yang sama dengan CVM, dan akan dilepas setelah pelepasan CVM yang terikat.	Tidak terikat dari sumber daya lain. Anda dapat mengikatnya ke atau melepaskannya dari CVM dan NAT Gateway kapan saja.

			Anda dapat melepaskan EIP saat Anda tidak lagi membutuhkannya.
Biaya		Hanya biaya jaringan publik yang akan dikenakan biaya.	Biaya sumber daya IP adalah bagian dari biaya EIP, yang berbeda-beda, tergantung jenis akunnya. Untuk informasi selengkapnya, silakan lihat Memeriksa Jenis Akun .
Kuota		Tergantung jumlah CVM yang Anda beli.	Setiap akun dapat menerapkan 20 EIP di setiap wilayah.
		Untuk kuota IP publik (termasuk EIP) yang terikat pada CVM, lihat batasan pada IP publik yang terikat pada CVM.	
Operasi	Mengonversi IP	IP publik dapat dikonversi menjadi EIP. Alamat IP tidak akan berubah setelah konversi.	EIP tidak bisa dikonversi kembali ke IP publik.
	Mengubah IP	IP publik dapat langsung diubah. Untuk informasi selengkapnya, lihat Mengubah Alamat IP Publik	EIP tidak dapat langsung diubah. Anda perlu melepaskan ikatan dan melepaskan EIP, menerapkan yang baru, dan mengikatnya lagi.
	Melepaskan IP	Jika Anda tidak memerlukan IP publik lagi, Anda dapat masuk ke konsol CVM , cari IP publik, dan di kolom Operasi , pilih Selengkapnya > IP/ENI > Kembalikan IP Publik untuk mengembalikannya.	Anda dapat melepaskan EIP di konsol EIP.
	Mengambil IP	Anda dapat mengambil IP/EIP publik yang telah Anda gunakan jika belum digunakan oleh pengguna lain.	

Penagihan

Lalu lintas jaringan publik yang dihasilkan oleh alamat IPv4 publik akan dikenakan biaya jaringan publik. Untuk informasi selengkapnya, lihat [Harga Jaringan Publik](#).

Informasi yang Relevan

Untuk informasi selengkapnya tentang cara cepat membangun IPv4 Virtual Private Cloud (VPC), lihat [Membangun VPC IPv4](#).

Untuk informasi selengkapnya tentang EIP, lihat [IP Elastis](#).

Jaringan Klasik

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

Jaringan dasar adalah kumpulan sumber daya jaringan publik untuk semua pengguna Tencent Cloud. IP pribadi dari semua CVM ditetapkan oleh Tencent Cloud. Anda tidak dapat menyesuaikan rentang IP atau alamat IP. VPC dengan akses yang independen, dapat dikontrol, dan lebih aman dikembangkan dari jaringan klasik untuk memenuhi kebutuhan semakin banyaknya pengguna akan layanan yang lebih kompleks.

Keterangan:

Karena sumber daya jaringan klasik menjadi semakin langka dan tidak dapat diperluas, akun Tencent Cloud yang terdaftar setelah 13 Juni 2017 00:00:00 dapat membuat instans (termasuk CVM dan TencentDB) hanya di VPC, bukan di jaringan klasik. Jika Anda perlu menggunakan layanan jaringan klasik, kirimkan permohonan.

Batasan Penggunaan

CVM berbasis jaringan klasik tidak mendukung ENI.

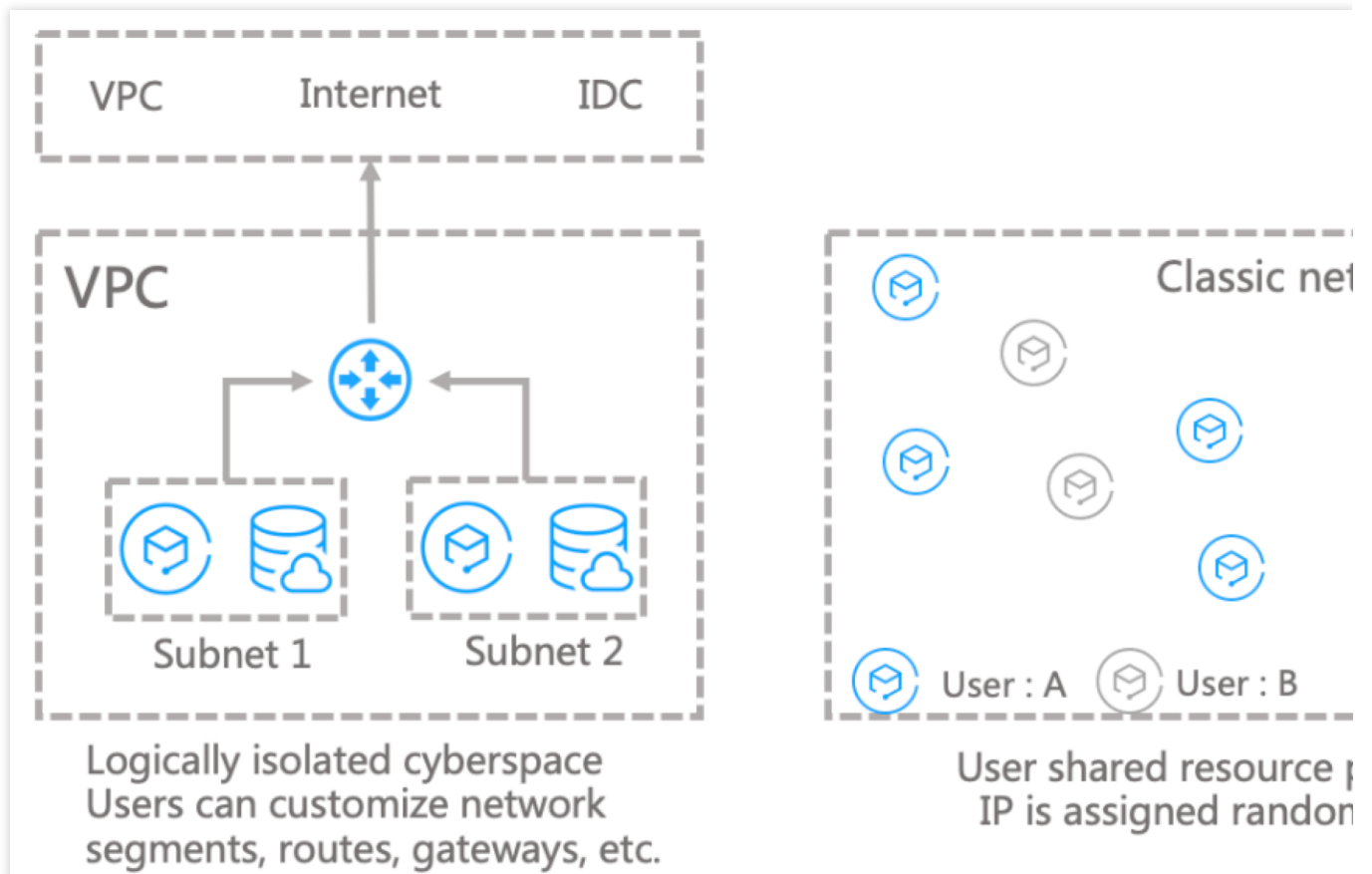
Migrasi dari jaringan klasik ke VPC tidak dapat dikembalikan.

Jaringan Klasik vs. VPC

Baik jaringan klasik maupun VPC adalah ruang jaringan di cloud.

Jaringan klasik adalah kumpulan sumber informasi jaringan publik untuk semua pengguna Tencent Cloud (seperti yang ditampilkan di sisi kanan gambar di bawah). IP pribadi dari semua CVM ditetapkan oleh Tencent Cloud. Anda tidak dapat menyesuaikan rentang IP atau alamat IP.

Sebaliknya, VPC adalah ruang jaringan yang terisolasi secara logis di Tencent Cloud (seperti yang ditampilkan di sisi kiri gambar di bawah). Di VPC, Anda dapat menyesuaikan rentang IP, alamat IP, dan kebijakan perutean. VPC lebih cocok untuk kasus penggunaan yang memerlukan konfigurasi kustom.

**Keterangan:**

Anda dapat menggunakan `DescribeAccountAttributes` API untuk mengkueri atribut jaringan sebuah akun. Jika nilai `supportedPlatforms` adalah `only-vpc`, akun tersebut adalah pengguna VPC default, yang memiliki semua sumber daya cloud di bawah VPC. Jika nilai `supportedPlatforms` adalah `classic`, akun tersebut adalah pengguna jaringan klasik default, yang memiliki semua sumber daya cloud di bawah jaringan klasik.

Referensi

Untuk informasi selengkapnya tentang rencana komunikasi antara VPC dan jaringan klasik, lihat [Berkomunikasi dengan Jaringan Klasik](#).

Untuk informasi selengkapnya tentang konfigurasi Classiclink, lihat [Classiclink](#).

Anda dapat memigrasikan instans Anda dari jaringan klasik ke VPC untuk memfasilitasi penggunaan VPC Anda.

Untuk petunjuk mendetail, lihat [Beralih dari Jaringan Klasik ke VPC](#).

Batas Kuota

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

VPC dan Subnet

Sumber Daya	Batas Kuota
Jumlah VPC per akun per wilayah	20
Jumlah subnet per VPC	100
Jumlah blok CIDR sekunder per VPC	5
Jumlah instans CVM jaringan klasik yang dikaitkan dengan setiap VPC	100

Tabel Rute

Sumber Daya	Batas Kuota
Jumlah tabel rute per VPC	10
Jumlah tabel rute yang dikaitkan ke setiap subnet	1
Jumlah kebijakan perutean per tabel rute	50

ENI

Sumber Daya	Batas Kuota
Jumlah ENI sekunder per VPC	1.000

HAVIP

Sumber Daya	Batas Kuota
Jumlah HAVIP default per VPC	10

Grup Keamanan

Item	Deskripsi
Jumlah grup keamanan	50 per wilayah
Jumlah aturan dalam grup keamanan	100 untuk aturan masuk dan 100 untuk aturan

	keluar
Jumlah instans CVM yang dikaitkan dengan grup keamanan	2.000
Jumlah grup keamanan yang dikaitkan dengan instans CVM	5
Jumlah grup keamanan yang dapat diimpor oleh grup keamanan	10

ACL Jaringan

Sumber Daya	Pembatasan
Jumlah ACL jaringan per VPC	50 partisi
Jumlah aturan per jaringan ACL	Masuk: 20Keluar: 20
Jumlah ACL jaringan yang dikaitkan ke setiap subnet	1 partisi

Templat Parameter

Jenis Sumber Daya	Batas Kuota
Objek alamat IP (ipm)	Maks.: 1.000
Objek grup alamat IP (ipmg)	Maks.: 1.000
Objek port protokol (ppm)	Maks.: 1.000
Objek grup port protokol (ppmg)	Maks.: 1.000
Anggota alamat IP dalam objek alamat IP (ipm)	Maks.: 20
Anggota objek alamat IP (ipm) dalam objek grup alamat IP (ipmg)	Maks.: 20
Anggota port protokol dalam objek grup port protokol (ppm)	Maks.: 20
Anggota objek port protokol (ppm) dalam objek grup port protokol (ppmg)	Maks.: 20
Objek grup alamat IP (ipmg) yang dapat mereferensikan pada objek alamat IP (ipm) yang sama	Maks.: 50

Objek grup port protokol (ppmg) yang dapat mereferensikan objek port protokol yang sama (ppm)

Maks.: 50

Probe Jaringan

Sumber Daya	Batas Kuota
Jumlah probe jaringan yang dibuat di setiap VPC	50