Virtual Private Cloud
Product Introduction

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

Product Introduction
Overview

Last updated: 2024-01-12 14:19:05

A Virtual Private Cloud (VPC) is a logically isolated network space on Tencent Cloud. You can deploy resources, such as CVM and TencentDB instances, on VPCs to enhance their security and meet the needs in different use cases.
Watch video
This document describes the core components, connection methods, and security of VPCs.

Core Components

A VPC has three core components: VPC IP range, subnet, and route table.

VPC IP range

When you create a VPC, you need to specify a CIDR (classless inter-domain routing) block as the VPC's IP address group.
Tencent Cloud VPC supports CIDR blocks in any of the following private IP ranges:

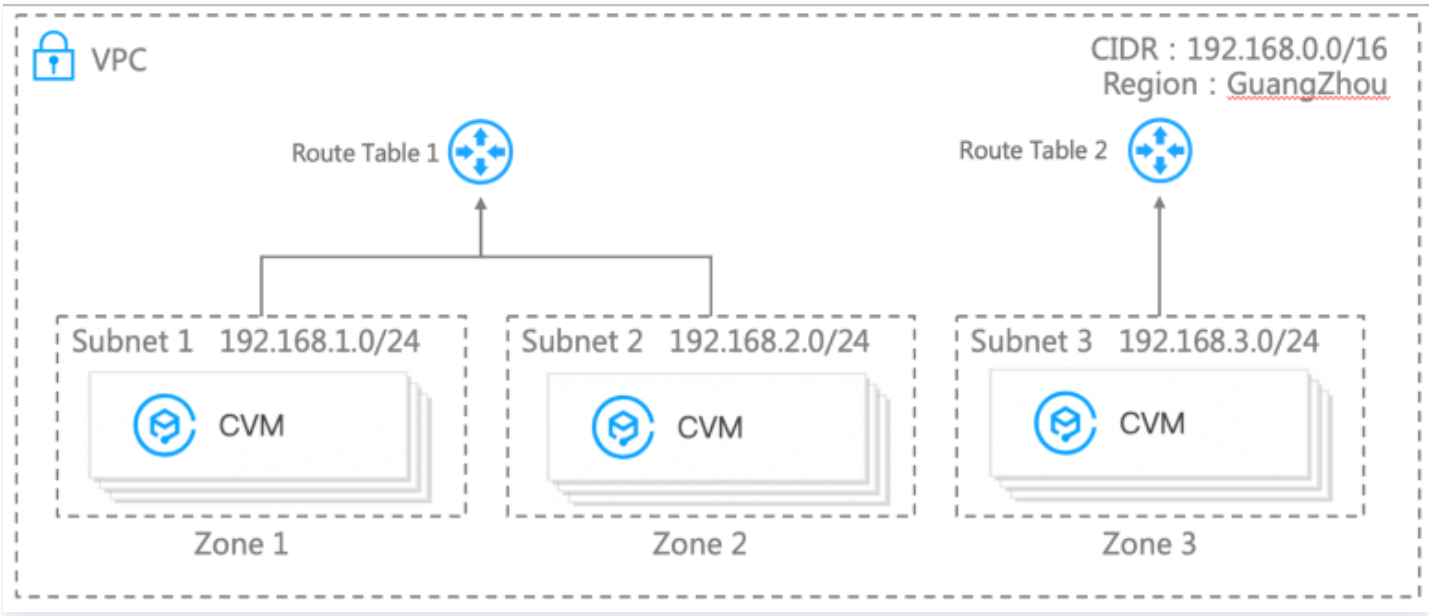
- **10.0**.0.0 - **10.255**.255.255 (**mask: 12 - 28**)
- **172.16**.0.0 - **172.31**.255.255 (**mask: 12 - 28**)
- **192.168**.0.0 - **192.168**.255.255 (**mask: 16 - 28**)

> **Note**
> The primary VPC CIDR block cannot be modified after creation. When the addresses in the primary CIDR block are not enough, you can create a secondary one to expand the IP range. For more information, see Editing IPv4 CIDR Blocks.

Subnet

Each VPC should contain at least one subnet. All Tencent Cloud resources in a VPC (such as CVM and TencentDB instances) must be deployed in a subnet, and the subnet CIDR block must be within the VPC CIDR block.
A VPC is set up at the region level (such as Guangzhou), while a subnet is set up at the availability zone level (such as Guangzhou Zone 1). You can divide a VPC into one or more subnets. Subnets in the same VPC can interconnect with one another by default, while

subnets in different VPCs are isolated by default.



Route table

When you create a VPC, the system automatically generates a default route table to ensure that all subnets in the same VPC are interconnected. If the routing policies in the default route table cannot meet your needs, you can create a custom route table.
For more information on route tables, see Overview.

VPC Connection

Tencent Cloud provides a wide range of VPC connection solutions for different use cases:

- CVMs in a VPC can be connected to the internet via an EIP or NAT gateway.
- VPCs can communicate with each other through a peering connection or over CCN.
- VPCs and local IDCs can be interconnected through VPN connections, Direct Connect or over CCN.

For more information about VPC connections, see VPC Connection Schemes Overview.

VPC Security

A VPC is a logically isolated network space in the cloud. Different VPCs are isolated from each other to protect application security.

- Security group: A security group is a stateful virtual firewall for filtering packets. As an important means of network security isolation, it can be used to control the outbound and inbound traffic for instances.
- Network ACL: A network ACL is a stateless virtual firewall for filtering packets at the subnet level. It can be used to control the inbound and outbound data streams for subnets at the protocol and port levels.

- Cloud Access Management (CAM): CAM helps you manage the access permissions for all your Tencent Cloud resources, including VPCs. You can control the access to your VPCs by user identities or custom policies.

For more information on VPC security, see Security Management.

Strengths

Last updated: 2024-01-12 14:17:19

Network Customization

VPC provides you with robust network management capabilities. You can customize IP ranges and create subnets as in a traditional network, while flexibly configuring route tables and routing policies to deploy your cloud services.
Tencent Cloud VPC also provides visualized network topologies to help you better plan the network.

Scalability

You can create different subnets in one or more VPCs to deploy your applications in a scalable VPC environment. You can also connect the VPC with local IDCs, other VPCs, and classic networks to expand the network architecture as needed.

Different Access Modes

VPC provides different access modes to meet the needs for cloud communications:

- Access the internet: You can access the internet through a public IP, EIP, NAT gateway, CLB, etc.
- Access other VPC instances: You can access other VPC instances through CCN, peering connection, etc.
- Access local IDCs: You can access local IDCs through VPN connection, Direct Connect, and CCN.
- Access classic networks: You can access applications deployed in a classic network through Classiclink.

High Security and Reliability

Based on the tunneling technology, VPC constructs virtual networks on physical networks. By utilizing virtualization technology, it ensures complete isolation between different VPCs, providing users with independent, isolated and secure cloud networks.
For CVM instances in a VPC, we offer various network access control methods, such as security groups and network ACLs.

Ease of use

You can create and manage VPC instances easily and quickly through the console and APIs, etc. The productized network features and different troubleshooting methods help reduce your Ops costs.

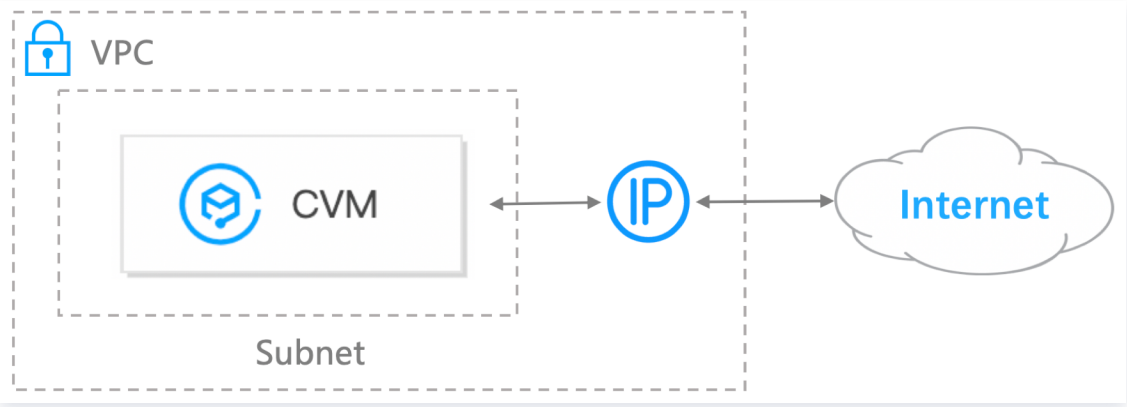
Scenarios

Last updated: 2024-01-12 14:22:27

Public Network Access

Single CVM

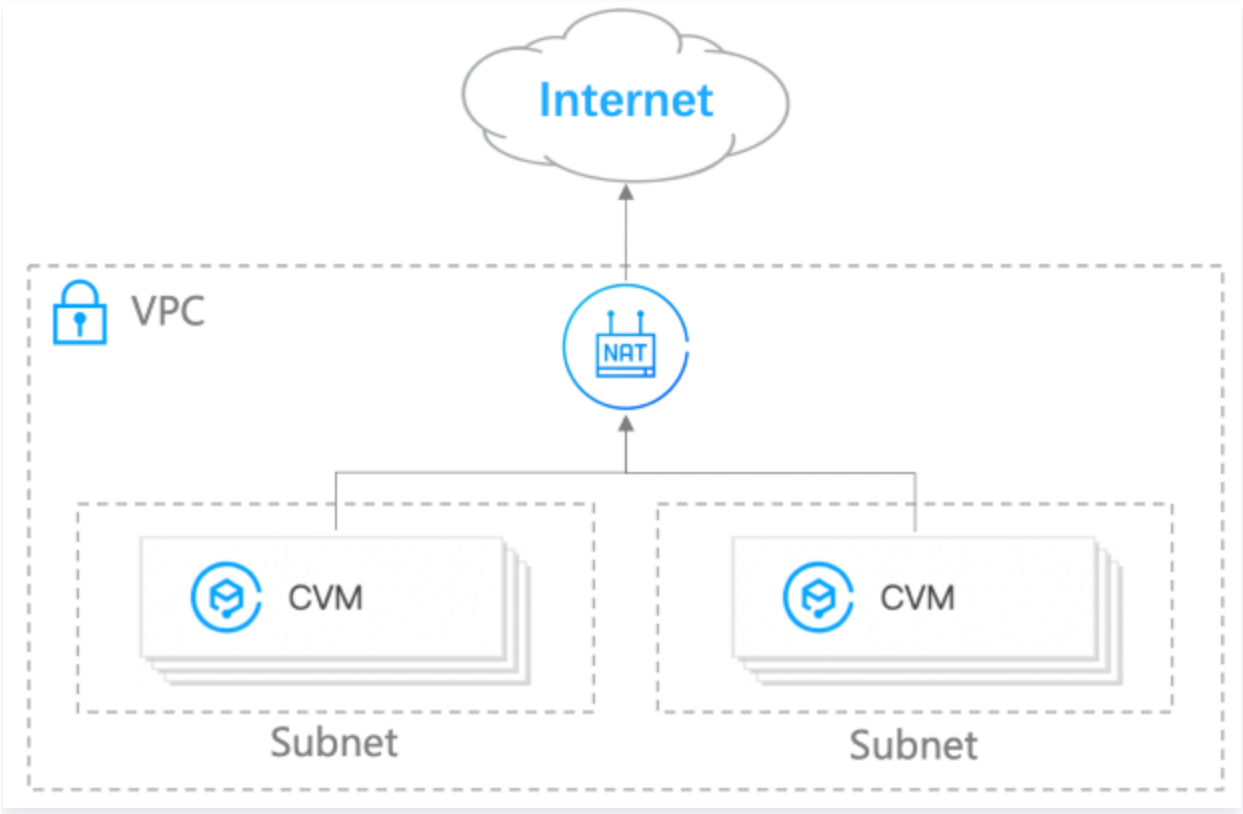
When the traffic to your application is low and only one CVM is available, you can apply for a public IP address and bind it with the CVM to gain public network access.



Multiple CVMs

When multiple CVMs need to access the public network simultaneously, and you do not want to expose their private network addresses, you can use NAT Gateway. The NAT Gateway provides the SNAT feature, and allows multiple CVMs to access the public network through the public IP addresses on the NAT gateway. Moreover, without the configuration of the DNAT feature, external users cannot directly access the NAT gateway, ensuring security. When there are multiple public IP addresses on the NAT gateway, the NAT gateway automatically

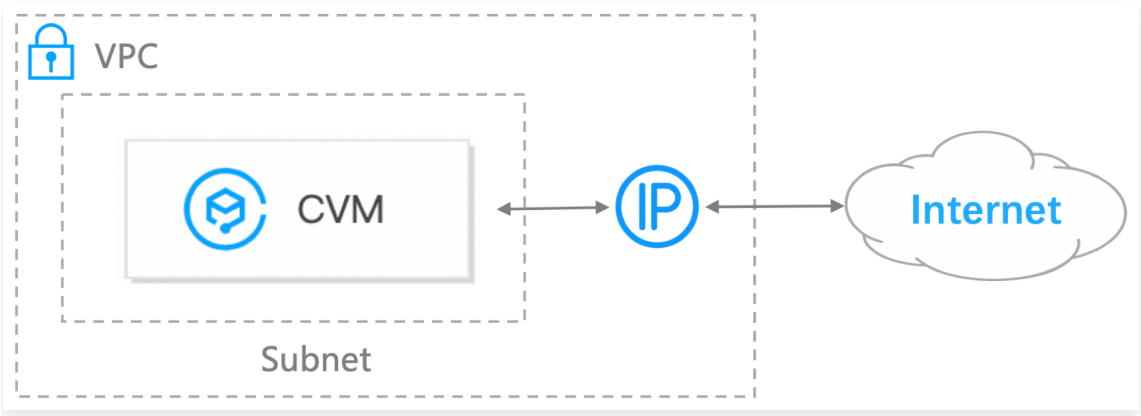
performs load balancing.



Providing Services to the Public Network

Single CVM

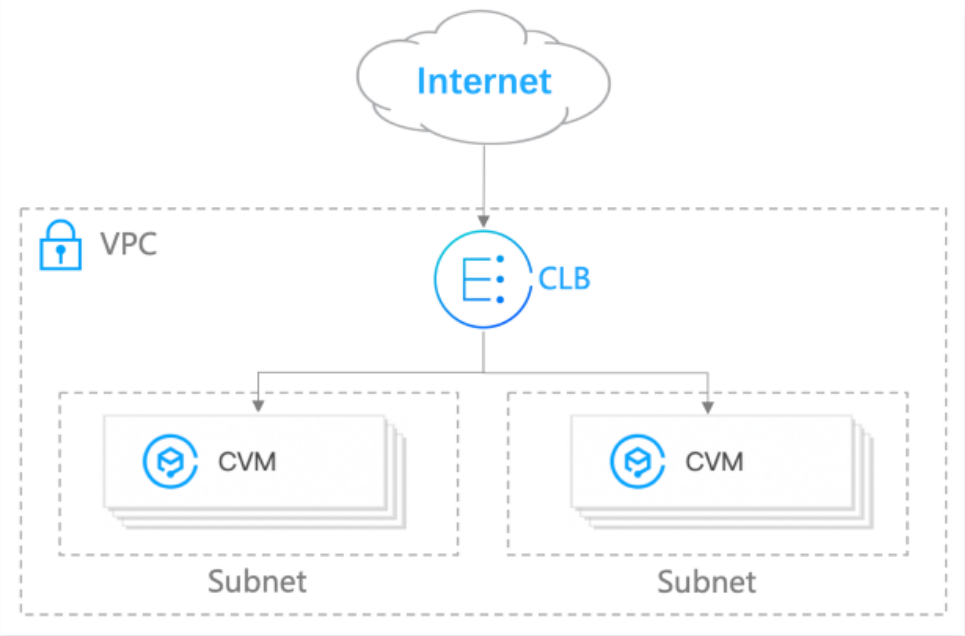
You can host services (such as website services) on a VPC-based CVM and use a public IP address to provide services to external users.



Mutiple CVMs

When you have many CVMs to deploy complex services and experience high public network traffic, you can use Cloud Load Balancer (CLB). CLB can automatically distribute application access traffic among multiple CVM instances in the cloud, enhancing fault tolerance for

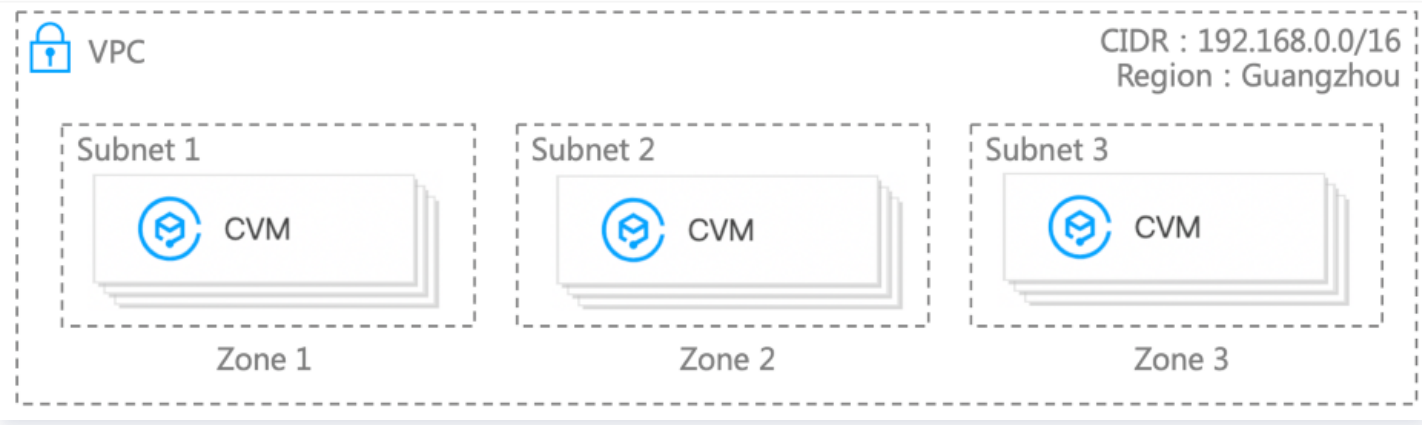
applications



Application disaster recovery

Cross-AZ disaster recovery

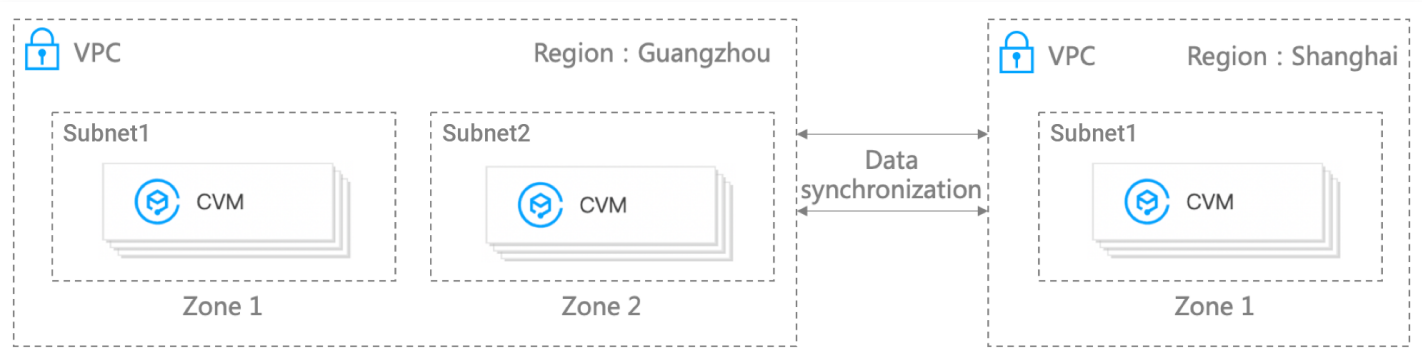
A subnet is associated with an AZ. You can create subnets in one VPC for different AZs of a region. By default, different subnets in the same VPC interconnect through the private network. You can deploy resources in subnets of different AZs to achieve cross-AZ disaster recovery.



Cross-Region Disaster Recovery

You can deploy applications across regions, and interconnect two VPCs through CCN. For example, a two-region-three-IDC solution can be implemented to achieve cross-region

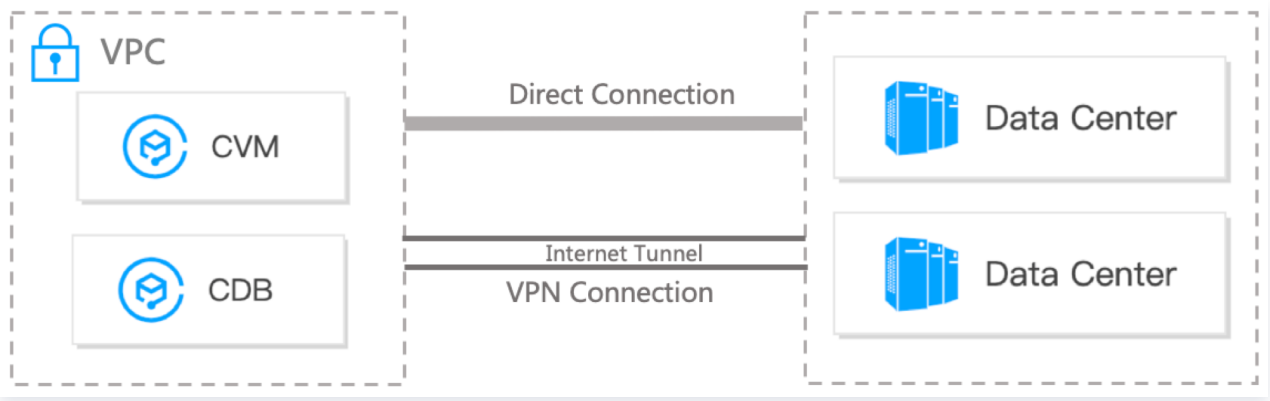
disaster recovery.



Deploying a Hybrid Cloud

Connecting to Local IDCs

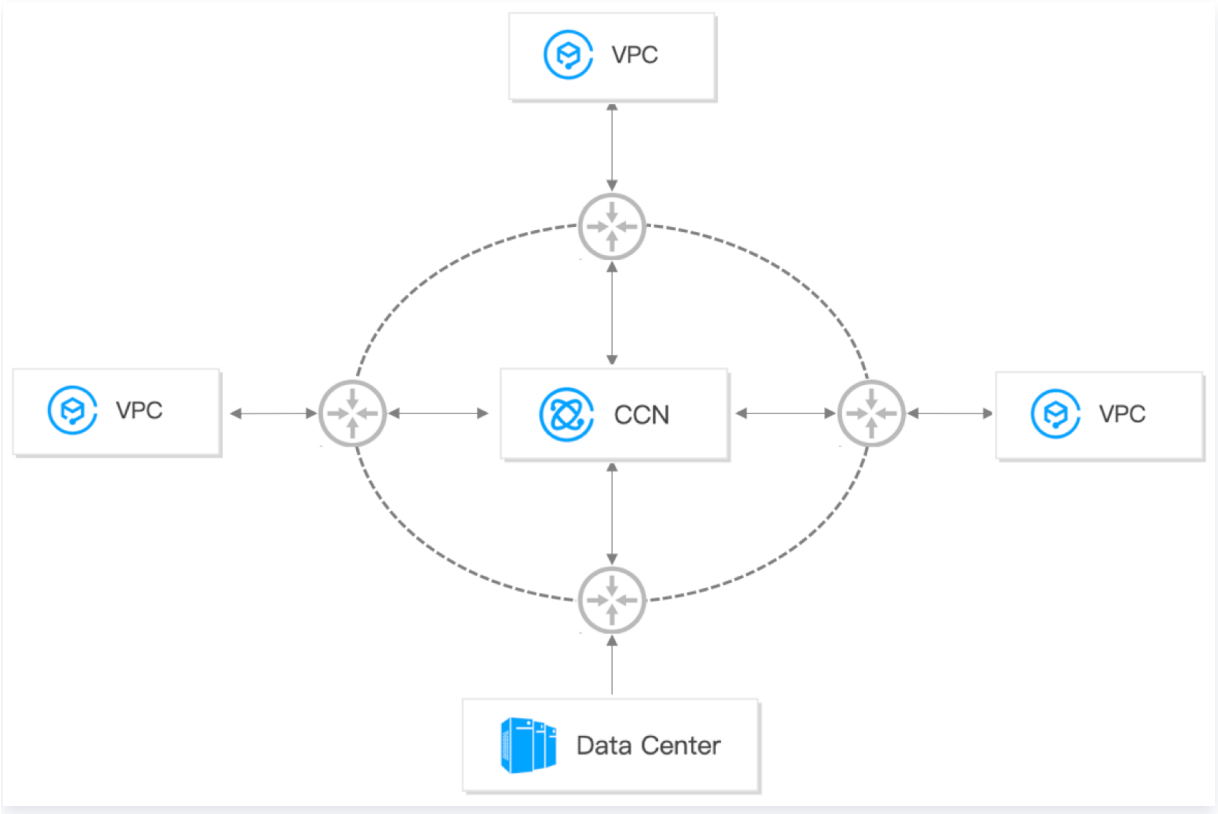
VPC provides multiple connection modes, such as Direct Connect and VPN connection, which can connect your local IDCs with VPC instances in the cloud to easily create a hybrid cloud architecture. Using local IDCs ensures the security of your core data. You can expand resources (such as CVMs and TencentDB) in the cloud based on your applications to reduce IT Ops costs.



Nationwide multipoint interconnection

When your applications are deployed across multiple regions nationwide and interconnection is required among these regions, you can use products like Cloud Connect Network and

Direct Connect to easily achieve multipoint interconnection through single-point access.



Concepts
Regions and Availability Zones

Last updated: 2024-01-12 14:22:35

Regions

Feature Overview

A region is the physical location of an IDC. In Tencent Cloud, different regions are fully isolated, ensuring maximum stability and fault tolerance among regions. To reduce access latency and increase download speeds, we recommend you select the region nearest to your customers.
You can view the following table or use the DescribeRegions API to get a complete region list.

Characteristics

- The networks of different regions are fully isolated from each other, and cloud products of different regions **cannot communicate via private network by default**.
- Tencent Cloud services in different regions can communicate with each other through public IPs over the internet, while those in different VPCs can communicate with each other through CCN, which is faster and more stable.
- Cloud Load Balancer (CLB) currently supports intra-region traffic forwarding by default. If you enable the cross-region binding feature, a CLB instance can be bound to CVM instances in another region.

> **Note**
> **Shenzhen/Shanghai Finance Zones** are tailor-made AZs for compliance with regulatory requirements in the finance industry and feature high security and isolation. Currently, they are available for Cloud Virtual Machine, finance database, Redis storage, and face recognition services. They can be activated by verified financial customers by contacting customer service. For more information, see Introduction to Finance Zones.

Availability Zones

Feature Overview

Availability Zones (AZs) refer to Tencent Cloud's physical IDCs that are in the same region. Each AZ is independently powered and have its own network resources. They are designed to

ensure that failures within one AZ can be isolated from other AZs (except for large-scale disasters or major power failures), thereby ensuring the availability and stability of user applications. By selecting instances in independent AZs, users can protect their applications from being affected by failures that occur in a single location.
You can use the DescribeZones API to get a complete list of AZs.

Characteristics

Tencent Cloud services in the same VPC are interconnected via the private network, which means they can communicate using private IPs, even if they are in different AZs of the same region.

> **Note**
> Private network interconnection refers to the interconnection of resources under the same account. Resources under different accounts are completely isolated on the private network.

China

Regions	Availability Zones
South China (Guangzhou) ap-guangzhou	Guangzhou Zone 1 (sold out) ap-guangzhou-1
	Guangzhou Zone 2 (sold out) ap-guangzhou-2
	Guangzhou Zone 3 ap-guangzhou-3
	Guangzhou Zone 4 ap-guangzhou-4
	Guangzhou Zone 6 ap-guangzhou-6
	Guangzhou Zone 7 ap-guangzhou-7
South China (Shenzhen Finance) ap-shenzhen-fsi	Shenzhen Finance Zone 1 (available exclusively for financial institutions and enterprises through online consultation) ap-shenzhen-fsi-1
	Shenzhen Finance Zone 2 (exclusive access for financial institutions and enterprises through online consultation): ap-shenzhen-fsi-2
	Shenzhen Finance Zone 3 (exclusive to financial institutions and enterprises, accessible through online consultation) - ap-shenzhen-fsi-3

East China (Shanghai) ap-shanghai	Shanghai Zone 1 (sold out) ap-shanghai-1
	Shanghai Zone 2 ap-shanghai-2
	Shanghai Zone 3 ap-shanghai-3
	Shanghai Zone 4 ap-shanghai-4
	Shanghai Zone 5 ap-shanghai-5
	Shanghai Zone 8 ap-shanghai-8
East China (Shanghai Finance) ap-shanghai-fsi	Shanghai Finance Zone 1 (only financial institutions and enterprises can apply for activation through Online Consultation) ap-shanghai-fsi-1
	Shanghai Finance Zone 2 (only financial institutions and enterprises can apply for activation through Online Consultation) ap-shanghai-fsi-2
	Shanghai Finance Zone 3 (only financial institutions and enterprises can apply for activation through Online Consultation) ap-shanghai-fsi-3
East China (Nanjing) ap-nanjing	Nanjing Zone 1 ap-nanjing-1
	Nanjing Zone 2 ap-nanjing-2
	Nanjing Zone 3 ap-nanjing-3
North China (Beijing) ap-beijing	Beijing Zone 1 (sold out) ap-beijing-1
	Beijing Zone 2 ap-beijing-2
	Beijing Zone 3 ap-beijing-3
	Beijing Zone 4 ap-beijing-4
	Beijing Zone 5 ap-beijing-5
	Beijing Zone 6 ap-beijing-6
	Beijing Zone 7 ap-beijing-7
Southwest China (Chengdu) ap-chengdu	Chengdu Zone 1 ap-chengdu-1
	Chengdu Zone 2 ap-chengdu-2
Southwest China	Chongqing Zone 1 ap-chongqing-1

(Chongqing) ap-chongqing	
Hong Kong/Macao/Taiwan (Hong Kong, China) ap-hongkong	Hong Kong Zone 1 (Nodes in Hong Kong, China can cover services in Hong Kong/Macao/Taiwan regions) (sold out) ap-hongkong-1
	Hong Kong Zone 2 (Nodes in Hong Kong, China can cover services in Hong Kong/Macao/Taiwan regions) ap-hongkong-2
	Hong Kong Zone 3 (Nodes in Hong Kong, China can cover services in Hong Kong/Macao/Taiwan regions) ap-hongkong-3

Note
The product is in beta test for Jinan, Hangzhou, Fuzhou, Wuhan, Changsha, and Shijiazhuang regions. To try it out, contact the sales rep.

Other Countries and Regions

Regions	Availability Zones
Southeast Asia (Singapore) ap-singapore	Singapore Zone 1 (Nodes in Singapore can cover services in Southeast Asia) ap-singapore-1
	Singapore Zone 2 (Nodes in Singapore can cover services in Southeast Asia) ap-singapore-2
	Singapore Zone 3 (Nodes in Singapore can cover services in Southeast Asia) ap-singapore-3
	Singapore Zone 4 (Nodes in Singapore can cover services in Southeast Asia) ap-singapore-4
Southeast Asia (Jakarta) ap-jakarta	Jakarta Zone 1 (Nodes in Jakarta can cover services in Southeast Asia) ap-jakarta-1
	Jakarta Zone 2 (Nodes in Jakarta can cover services in Southeast Asia) ap-jakarta-2
Northeast Asia (Seoul) ap-seoul	Seoul Zone 1 (Nodes in Seoul can cover services in Northeast Asia) ap-seoul-1
	Seoul Zone 2 (Nodes in Seoul can cover services in Northeast Asia) ap-seoul-2

Northeast Asia (Tokyo) ap-tokyo	Tokyo Zone 1 (Nodes in Tokyo can cover services in Northeast Asia) ap-tokyo-1
	Tokyo Zone 2 (Nodes in Tokyo can cover services in Northeast Asia) ap-tokyo-2
Southern Asia (Mumbai) ap-mumbai	Mumbai Zone 1 (Nodes in Mumbai can cover services in South Asia) ap-mumbai-1
	Mumbai Zone 2 (Nodes in Mumbai can cover services in South Asia) ap-mumbai-2
Southeast Asia (Bangkok) ap-bangkok	Bangkok Zone 1 (Nodes in Bangkok can cover services in Southeast Asia) ap-bangkok-1
	Bangkok Zone 2 (Nodes in Bangkok can cover services in Southeast Asia) ap-bangkok-2
North America (Toronto) na-toronto	Toronto Zone 1 (Nodes in Toronto can cover services in North America) na-toronto-1
South America (São Paulo) sa-saopaulo	São Paulo Zone 1 (Nodes in São Paulo can cover services in South America) sa-saopaulo-1
West US (Silicon Valley) na-siliconvalley	Silicon Valley Zone 1 (Nodes in Silicon Valley can cover services in Western US) na-siliconvalley-1
	Silicon Valley Zone 2 (Nodes in Silicon Valley can cover services in Western US) na-siliconvalley-2
East US (Virginia) na-ashburn	Virginia Zone 1 (Nodes in Virginia can cover services in Eastern US) na-ashburn-1
	Virginia Zone 2 (Nodes in Virginia can cover services in Eastern US) na-ashburn-2
Europe (Frankfurt) eu-frankfurt	Frankfurt Zone 1 (Nodes in Frankfurt can cover services in Europe) eu-frankfurt-1
	Frankfurt Zone 2 (Nodes in Frankfurt can cover services in Europe) eu-frankfurt-2

Selection of Regions and AZs

When selecting the region and AZ, consider the following factors:

- The region of the CVM and the geographical locations of you and your target users. We recommend that you select the region closest to your end users to reduce access

latency and increase the access speed.

- Relationships between the CVM and other cloud products.
  It is recommended to select the cloud products that reside in the same AZ of the same region to facilitate interconnection through private networks and to reduce access latency and increase the access speed.
- High availability of services and disaster recovery.
  Even if you have just one VPC, we still recommend that you deploy your applications in different AZs to prevent a single point of failure and enable cross-AZ disaster recovery.
- There may be higher network latency among different AZs. We recommend that you assess your requirements and find the optimal balance between high availability and low latency.
- If you need access to CVM instances in other countries or regions, we recommend you select a CVM in those other countries or regions. If you use a CVM instance in Mainland China to access servers in other countries and regions, you may encounter much higher network latency.

Resource Availability Range

The following table describes which Tencent Cloud resources are global, which are regional, and which are specific to AZs.

Resources	Resource ID Format (<Resource Abbreviation>-8-Digit String of Numbers and Characters)	Availability Range	Note
User Account	No limit	Globally unique	Users can use the same account to access Tencent Cloud resources around the world.
SSH key	skey-xxxxxxxx	Globally available	Users can use an SSH key to bind a CVM in any region under the account.
Cloud Virtual	ins-xxxxxxxx	Specific to a single AZ	A user can only create a CVM instance in a specific AZ.

Machine instance		of a region	
Custom Images	img-xxxxxxxx	Cross AZs in the same region	Custom images created for the instance are available to all AZs of the same region. Use "Copy Image" to copy a custom image if you need to use it in other regions.
Elastic IP	eip-xxxxxxxx	Cross AZs in the same region	EIPs can only be associated with instances in the same region.
Security Group	sg-xxxxxxxx	Cross AZs in the same region	Security groups can only be associated with instances in the same region. Tencent Cloud automatically creates three default security groups for users.
Cloud Block Storage	disk-xxxxxxxx	Specific to a single AZ of a region	Users can only create a cloud disk in a specific AZ and attach it to an instance in the same AZ.
Snapshot	snap-xxxxxxxx	Cross AZs in the same region	After creating a snapshot for a specific cloud disk, users can use this snapshot in this region for other operations (such as creating cloud disks).
Cloud Load Balancer	clb-xxxxxxxx	Cross AZs in the same region	A CLB instance can be bound with a CVM in a different AZ of the same region for traffic forwarding.
Virtual Private Cloud	vpc-xxxxxxxx	Cross AZs in the same region	A VPC in one region can have resources created in different AZs of the region.
Subnet	subnet-xxxxxxxx	Specific to a single AZ of a region	Users cannot create subnets across AZs.
Route Table	rtb-xxxxxxxx	Cross AZs in the same region	When creating a route table, users need to specify a VPC. Therefore, a route table is also available for multiple AZs in a region.

Related Actions

Migrating an instance to another AZ

For a launched instance, its AZ cannot be changed. But you can migrate it to another AZ. The migration process involves creating a custom image using the original instance, using the custom image to launch an instance in a new AZ, and updating the configuration of the new instance.

1. Create a custom image from the current instance. For more information, see Creating Custom Images.
2. If the instance is in the network environment of VPC, and you want to retain its current private IP address after the migration, first delete the subnet in the current AZ and then create a subnet in the new AZ with the same IP address. Note that a subnet can be deleted only when it contains no available instances. Therefore, all the instances in the current subnet should be migrated to the new subnet.
3. Create a new instance in the new AZ using the custom image you have just created. You can select the same type and configuration as those of the original instance, or choose new ones. For more information, see Creating Instances.
4. If an EIP is associated with the original instance, you need to dissociate it from the old instance and associate it with the new instance. For more information, see EIP.
5. (Optional) If the original instance is pay-as-you-go, you can choose to terminate it. For more information, see Terminating Instances. If the original instance is monthly subscribed, you can repossess it upon its expiration.

Copying images to another region

Operations such as launching and viewing instances are region-specific. If the image of the instance that you need to launch does not exist in the region, copy the image to the desired region. For more information, see Copying Images.

IPv4 and IPv6 Addresses

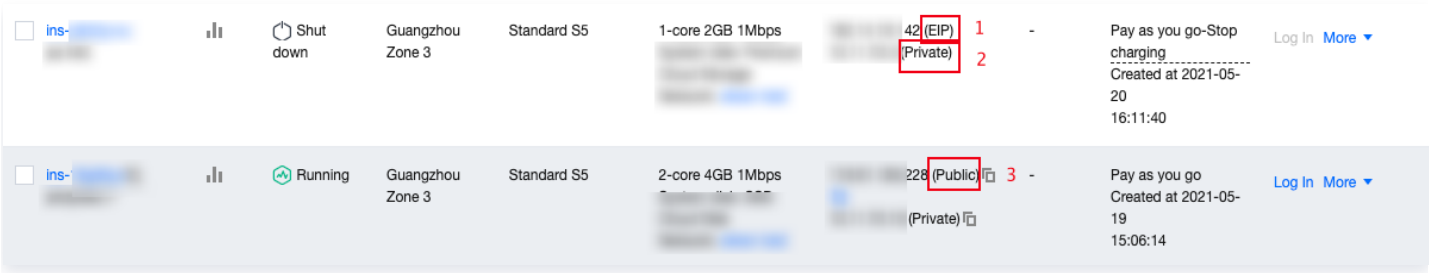
Last updated: 2024-01-12 14:22:41

IP addresses support IPv4 and IPv6 addressing protocols. IPv4 is widely used, but the number of network addresses is limited, making IPv6 a good complement.

IPv4 Addresses

Tencent Cloud offers two types of IPv4 addresses for private and public network access. A public IPv4 address can be common or elastic. As shown in the following figure, **EIP** numbered 1 is an elastic IPv4 address, **Private** numbered 2 is a private IPv4 address, and **Public** numbered 3 is a public IPv4 address. These IPs will not change unless you unbind or change them.

> **Note**
> Unless otherwise specified, private IP, public IP and EIP all refer to IPv4 addresses.



Private IPv4 addresses

A private IPv4 address is used for Tencent Cloud private network access, which cannot be used to access the internet. Once a CVM instance is created, it will be automatically assigned with a private IPv4 address. The private IPv4 address can also be customized in a VPC environment.

Attributes

- The IPv4 private network is user-specific, and different users are isolated from each other. By default, CVMs of another user cannot be accessed via the IPv4 private network.
- The IPv4 private network is region-specific, and different regions are isolated from each other. By default, CVMs and VPCs under the same account in a different region cannot be accessed via the IPv4 private network.

Scenarios

The private IPv4 address can be used for:

- Interconnection between VPC-based or classic network-based CLB and CVM instances over an IPv4 private network.
- Interconnection between VPC-based or classic network-based CVM instances over an IPv4 private network.
- Interconnection between VPC-based or classic network-based CVM instances and other Tencent Cloud services (such as TencentDB) over an IPv4 private network.

Related Actions

- For more information about how to obtain the private IPv4 address of the instance and set DNS, refer to Getting Private IP Addresses and Setting DNS.
- For more information about how to change the private IPv4 addresses of CVM instances in a VPC, see Modifying Private IP Addresses.

Public IPv4 addresses

Tencent Cloud provides public IPs and EIPs for public network access. A CVM instance with a public IPv4 address can access and be accessed over an IPv4 public network.

Comparison

The following table compares public IPs with EIPs.

Item	Public IPs	EIPs
Use Cases	If you want to create a CVM that supports public network access, you can choose to use a public IP address automatically assigned by the system at the creation of a CVM instance. This public IP address has the same lifecycle as the CVM, and will be released upon the release of the bound CVM.	If you want to use a public IP for a long time, you can choose an elastic IP (EIP) and bind it to the specified CVM as needed. EIP can be bound or unbound many times, and will still exist after the CVM is released.
Public network access	Both are public IPs and support public network access.	
Acquisition method	It can only be obtained when you purchase a CVM.	Obtain it by applying for an EIP in the console. Converting Public IP to EIP.

Features		It has the same lifecycle as the CVM, and will be released upon the release of the bound CVM.	It's independent from other resources. You can bind it to/unbind it from CVMs and NAT gateways any time. You can release it when you no longer need it.
IP Resource Fee		Only the public network fee will be charged.	The IP resource fee is a part of the EIP fee, which varies by the account type. For more information, see Fee Composition.
Quota		It is subject to the number of CVMs you purchased.	Each account can apply for 20 EIPs in each region.
		For the quota of public IPs (including EIPs) bound to a CVM, see Limits on public IPs bound to a CVM.	
Action	Converting an IP	A public IP can be converted to an EIP. The IP address will not change after the conversion. For details, see Converting Public IPs to EIPs.	An EIP cannot be converted back to a public IP.
	Changing an IP	Public IPs can be directly changed. For details, see Changing Public IPs.	EIPs cannot be directly changed. You need to unbind and release the EIP, apply for a new one, and bind it again.
	Releasing an IP	If you no longer need the public IP, you can return it in the CVM console by selecting "More" > "IP/ENI" > "Return public IP" in the operation column.	You can release an EIP in the EIP console. For details, see Releasing EIPs.
	Retrieving an IP	You can retrieve public IPs/EIPs that you have used if they are not used by other users. For details, see Retrieving Public IPs.	

Billing description

The public network traffic generated by public IPv4 addresses will be charged with public network fees. For more information, see Public Network Pricing.

IPv6 Addresses

IPv6 addresses in Tencent Cloud can serve as both private and public IPv6 addresses. By default, they are private IPv6 addresses. To enable public network capabilities, refer to Managing IPv6 Public Network to change the private IPv6 address to a public IPv6 address. The IPv6 address will not change unless you release or reallocate it.

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

Private IPv6 addresses

A private IPv6 address is used for Tencent Cloud private network access, which cannot be used to access the internet. When creating a CVM instance, if IPv6 is enabled for the subnet, you can choose to obtain an IPv6 address for free, and the system will automatically assign it. You can also choose to obtain it later after the creation. The private IPv6 address can also be customized in a VPC environment.

Attributes

- The IPv6 private network is user-specific, and different users are isolated from each other. By default, CVMs of another user cannot be accessed via the IPv6 private network.
- The IPv6 private network is region-specific, and different regions are isolated from each other. By default, CVMs and VPCs under the same account in a different region cannot be accessed via the IPv6 private network.

Scenarios

Private IPv6 addresses are used for communication between CVM instances over the IPv6 private netwin the same VPC.

Public IPv6 addresses

Upon enabling IPv6 public network capabilities for a private IPv6 address, it can be converted into a public IPv6 address, also known as elastic public IPv6. This allows access and be accessed over the IPv6 public network. For more information, see Elastic Public IPv6.

Billing description

The public network traffic generated by public IPv6 addresses will be charged with public network fees. For more information, see Billing Prices.

References

- For more information about how to quickly build an IPv4 Virtual Private Cloud (VPC), see

Building Up an IPv4 VPC.

- For more information about how to quickly build an IPv6 Virtual Private Cloud (VPC), see Building Up an IPv6 VPC.
- For more information about EIPs, see Elastic IP.

Classic network

Last updated: 2024-01-12 14:24:59

The classic network is a public network resource pool shared by all Tencent Cloud users, where the private IPs of all CVM instances are assigned by Tencent Cloud and you cannot customize IP ranges or IP addresses. The VPC with independent, controllable and more secure access has evolved from the classic network to meet the requirements of a growing number of users for more complex services.

> **Note**
> As the classic network resources become increasingly scarce and cannot be expanded, instances (including CVM and CLB) under Tencent Cloud accounts registered after June 13, 2017, 00:00:00 can only be created in a VPC rather than the classic network.

Usage Limits

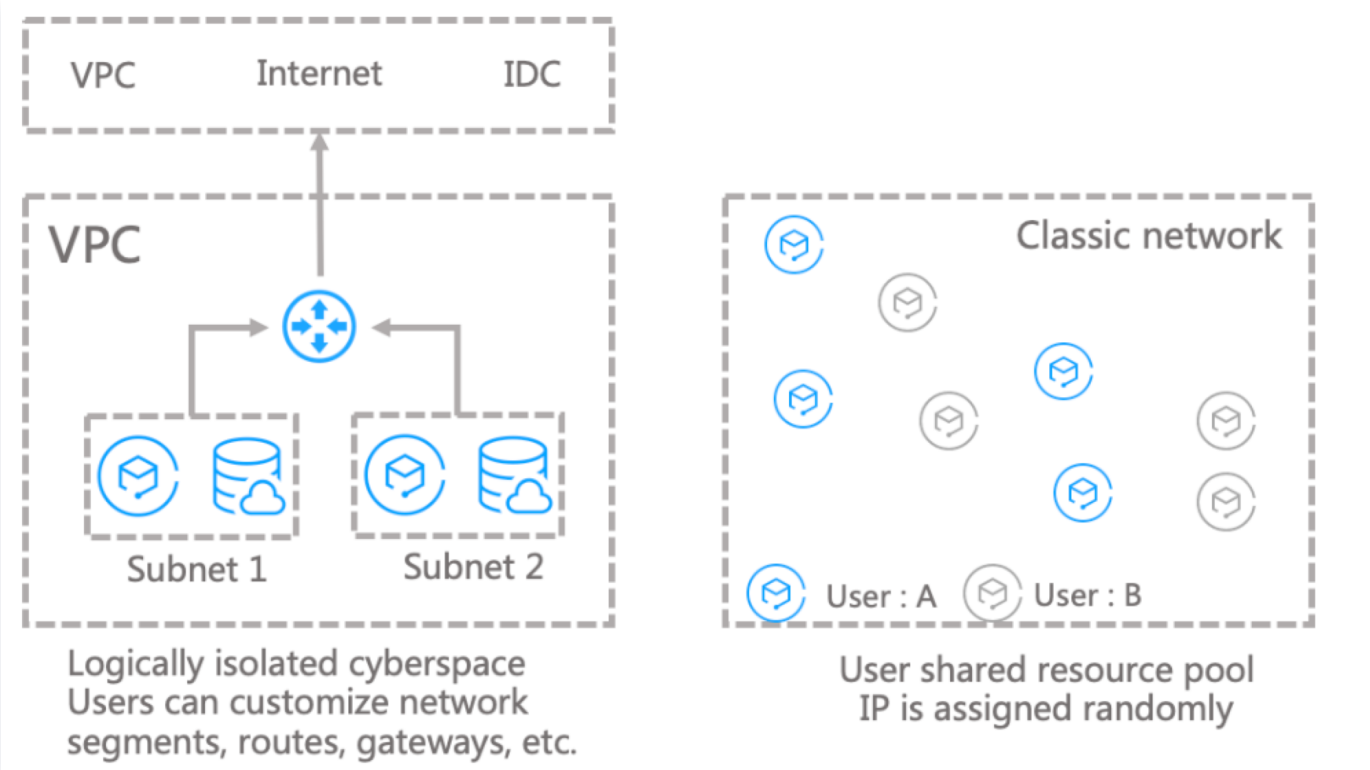
- The classic network-based CVMs do not support ENIs.
- Migrating from the classic network to VPC is irreversible.

Classic Network vs. VPC

Both classic network and VPC are network spaces on the cloud.

- The classic network is a public network resource pool for all Tencent Cloud users (as shown on the right side of the figure below). The private IPs of all CVMs are assigned by Tencent Cloud. You cannot customize IP ranges or IP addresses.
- A VPC is a logically isolated network space in Tencent Cloud (as shown on the left side of the figure below). Within a VPC, users can freely customize IP ranges, IP addresses, and routing policies. Compared to the classic network, VPC is more suitable for scenarios

requiring custom network configurations.



Note

You can query the network attributes of your account via the DescribeAccountAttributes API. If the "supportedPlatforms" value is "only-vpc", it indicates a default VPC user, who owns all cloud resources under VPCs. If the "supportedPlatforms" value is "classic", it indicates a default classic network user, who owns all cloud resources under the classic network.

Documentation

- For more information about the communication plan between a VPC and the classic network, see Communicating with Classic Network.
- For more information about Classiclink configurations, see Classiclink.
- You can migrate your instances from the classic network to a VPC. For details, see Migrating from the Classic Network to VPC.

Quota Limit

Last updated: 2024-01-12 14:25:11

VPCs and Subnets

Resources	Quota Limit
Number of VPCs per account per region	20
Number of subnets per VPC	100
Number of secondary CIDR blocks per VPC	5
Number of classic network CVM instances associated with each VPC	100

Route Tables

Resources	Quota Limit
Number of route tables per VPC	10
Number of route tables associated with each subnet	1
Number of routing policies per route table	50

ENIs

Resources	Quota Limit
Number of secondary ENIs per VPC	1000

HAVIP

Resources	Quota Limit
Number of default HAVIPs per VPC	10

Security Groups

Feature Overview	Restrictions
Number of security groups that can be created per project	Each region: 50

Number of security group rules	Inbound: 100; Outbound: 100
Number of CVM instances associated with a security group	2,000
Number of security groups that can be associated with each CVM instance	5
Number of security group IDs that can be referenced by a security group	10

Network ACLs

Resources	Restrictions
Number of network ACLs per VPC	50
Number of rules per network ACL	• Inbound: 20 • Outbound: 20
Number of network ACLs associated with each subnet	1

Parameter Templates

Instance type	Quota Limit
IP Address Objects (IPM)	Each tenant: 1,000
IP Address Group Objects (IPMG)	Each tenant: 1,000
Protocol port objects (ppm)	Each tenant: 1,000
Protocol port group objects (ppmg)	Each tenant: 1,000
IP address members in an IP address object (ipm)	Each tenant: 20
IP address object members (ipm) in an IP address group object (ipmg)	Each tenant: 20
Protocol port members in a protocol port group object (ppm)	Each tenant: 20

Protocol port object members (ppm) in a protocol port group object (ppmg)	Each tenant: 20
Number of IP address group objects (ipmg) that can reference an IP address object (ipm)	Each tenant: 50
Number of protocol port group objects (ppmg) that can reference a protocol port object (ppm)	Each tenant: 50

Network Probes

Resources	Quota Limit
Number of network probes that can be created in each VPC	50