

Virtual Private Cloud

Product Introduction

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



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

Product Introduction

Overview

Strengths

Use Cases

Concepts

Regions and Availability Zones

IPv4 Addresses

Classic Network

Quota Limit

Product Introduction

Overview

Last updated : 2024-01-24 17:22:28

A Virtual Private Cloud (VPC) is a logically isolated network space that can be customized for resources in Tencent Cloud such as [CVM](#) and [TencentDB](#) to enhance their security and meet the needs in different use cases. 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 (the mask range must be 12 to 28)

172.16.0.0 - 172.31.255.255 (the mask range must be 12 to 28)

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

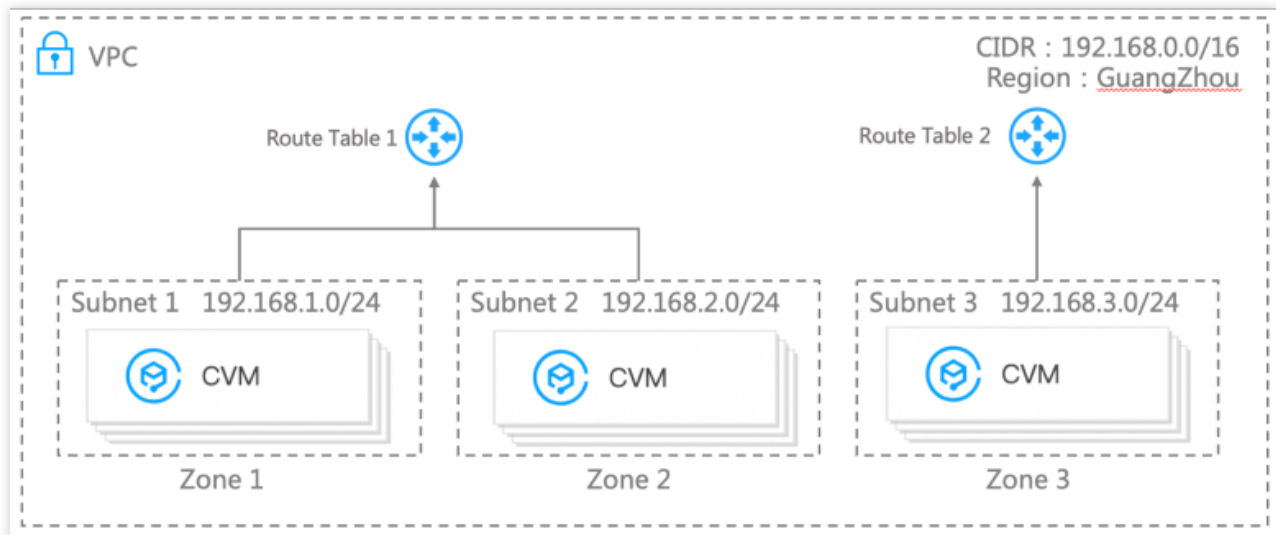
Note:

The VPC CIDR block (primary) cannot be modified after creation. When the primary CIDR block cannot support business allocation, you can create a secondary one to expand the IP range. For more information on the secondary CIDR block, see [Editing IPv4 CIDR Blocks](#).

Subnet

A VPC consists of 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 business 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:

CVM and TencentDB instances in a VPC can connect to the public network 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 or Direct Connect or over CCN.

VPC Security

A VPC is a logically isolated network space in the cloud. Different VPCs are isolated from each other to protect business 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 Access Control List (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 granularities.

Cloud Access Management (CAM): CAM helps you securely manage the access permissions for all your Tencent Cloud resources. It allows you to manage access to VPCs. For example, it allows you to control user access to VPCs through identity management and policy management.

For more information on VPC security, see [Security Management](#).

Strengths

Last updated : 2024-01-24 17:22:28

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 network topologies to help you visualize and plan the network.

Scalability

You can create different subnets in one or more VPCs to deploy your businesses 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 businesses deployed in a classic network through Classiclink.

Security and Reliability

VPC uses the tunneling technology to build virtual networks on physical networks, and the virtualization technology to achieve private network isolation between VPC instances. It provides you with independent, isolated, and secure cloud networks.

For CVMs within a VPC, we also provide you with access controls at different levels, such as security groups and network ACLs.

Ease of Use

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

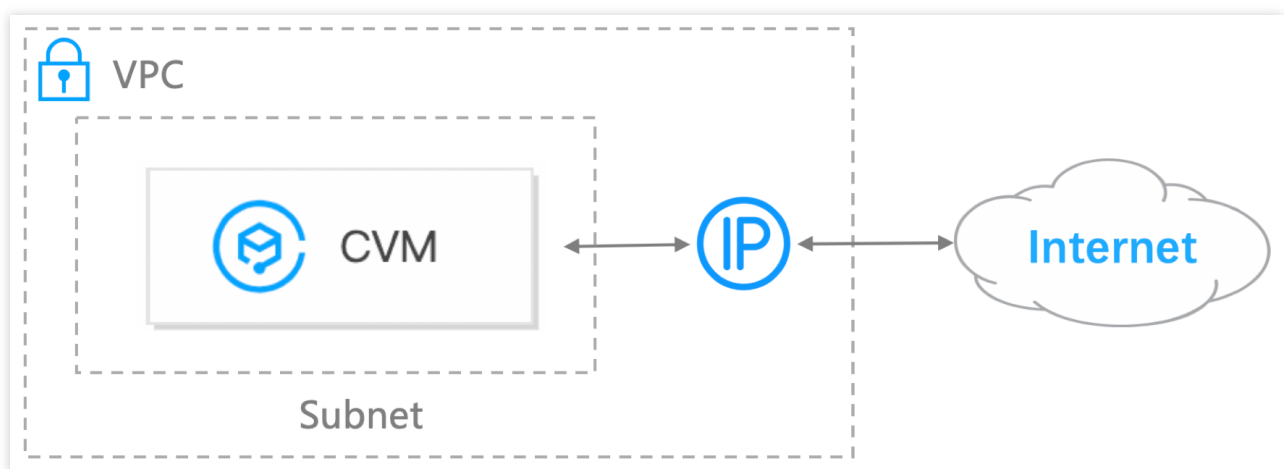
Use Cases

Last updated : 2024-01-24 17:22:28

Accessing the Internet

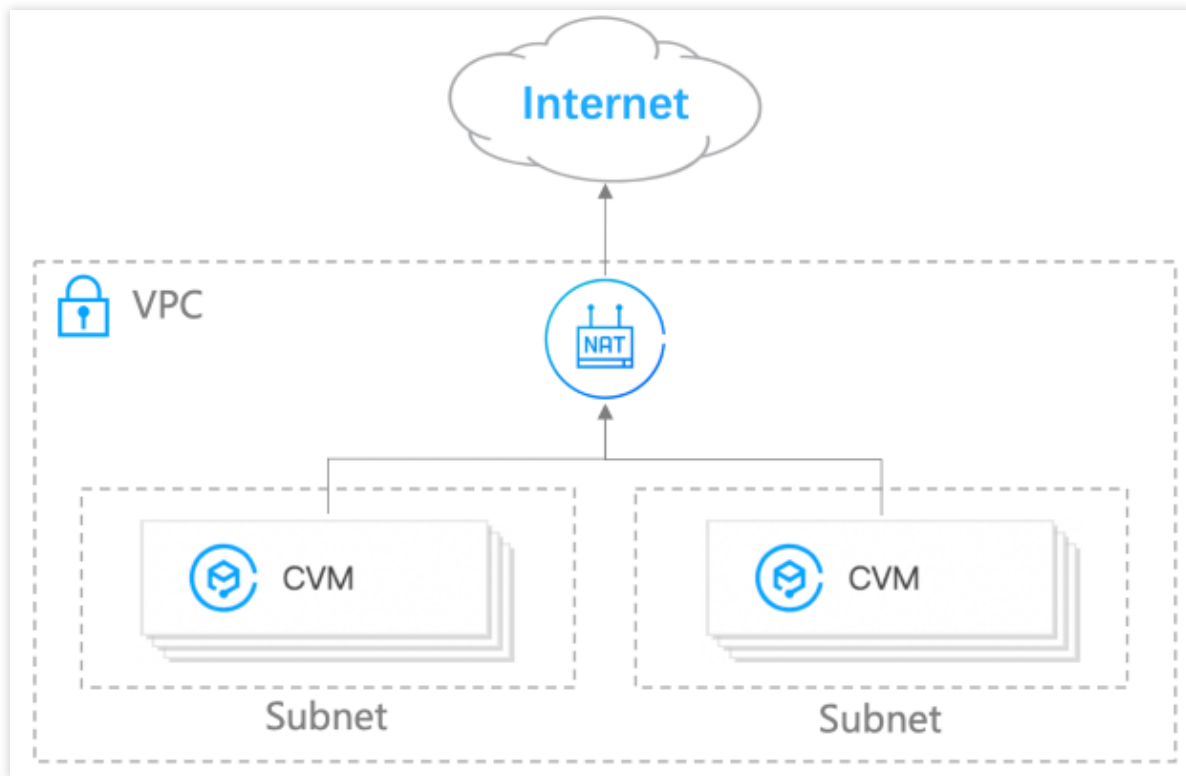
Single CVM

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



Multiple CVMs

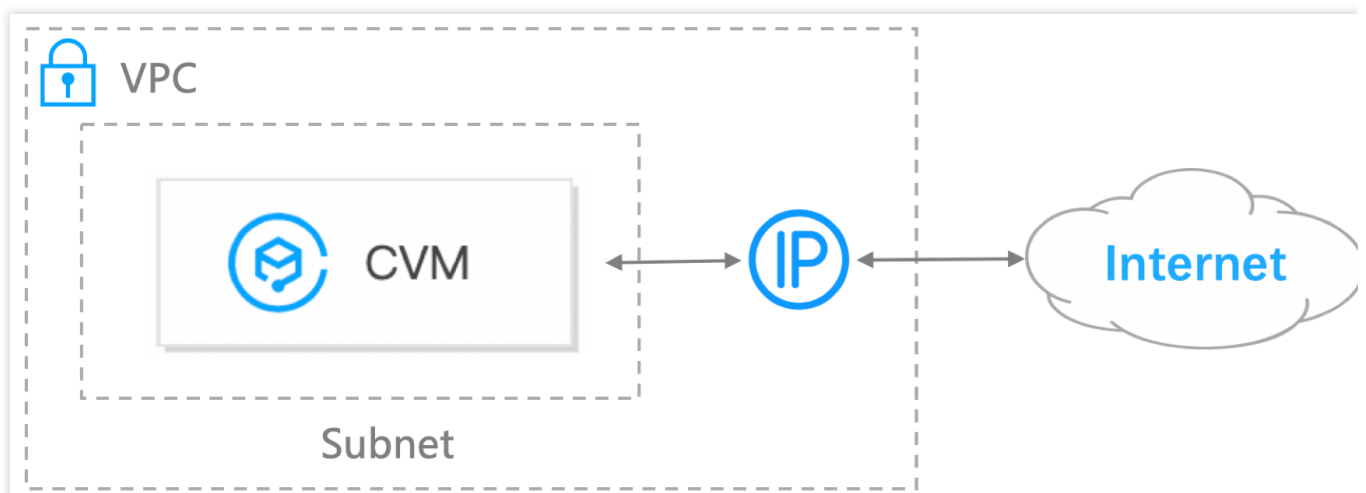
When you have multiple CVMs that need to access the Internet simultaneously and you do not want the private network addresses of the CVMs to be exposed, you can use [NAT Gateway](#). The NAT gateway provides the SNAT feature and allows multiple CVMs to access the Internet with public IP addresses on the NAT gateway. Moreover, without the configuration of the DNAT feature, external users cannot directly access the NAT gateway, ensuring security. When multiple public IP addresses exist on the NAT gateway, the NAT gateway automatically performs load balancing.



Providing Services to the Internet

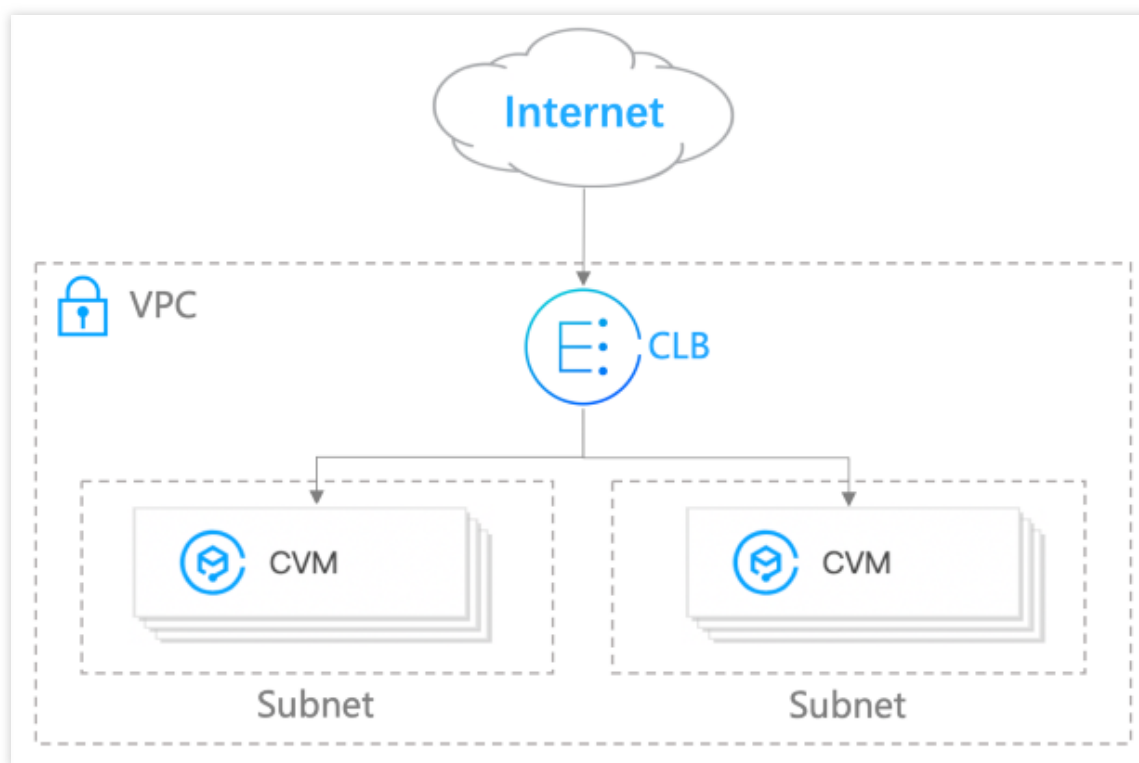
Single CVM

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.



Multiple CVMs

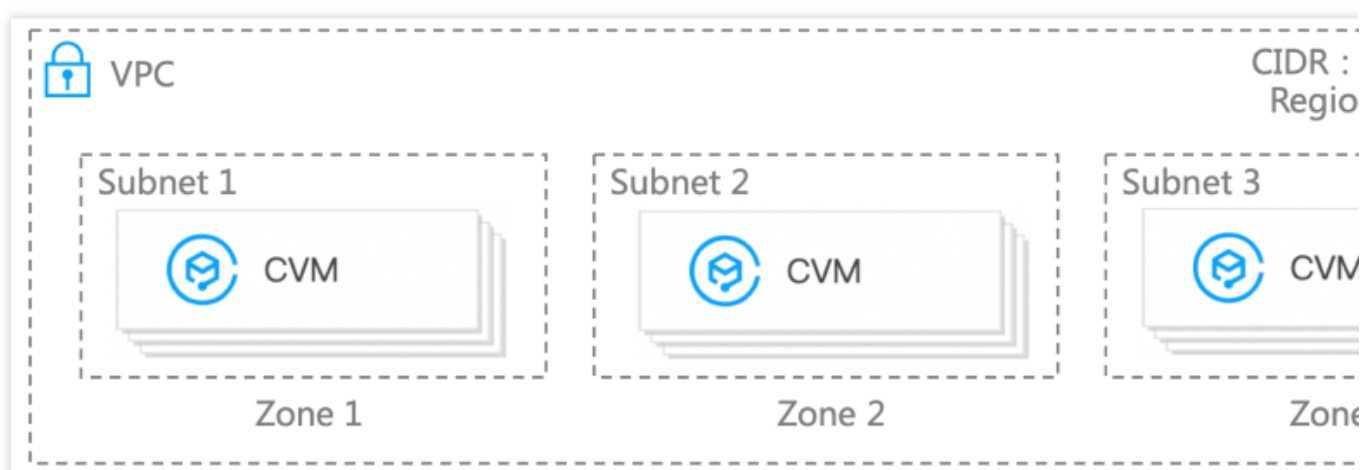
When you have many CVMs for deploying complex services and the Internet traffic is high, you can use the [Cloud Load Balancer \(CLB\)](#). The CLB can automatically distribute application access traffic among CVM instances in the cloud, enhancing fault tolerance for applications.



Disaster Recovery for Applications

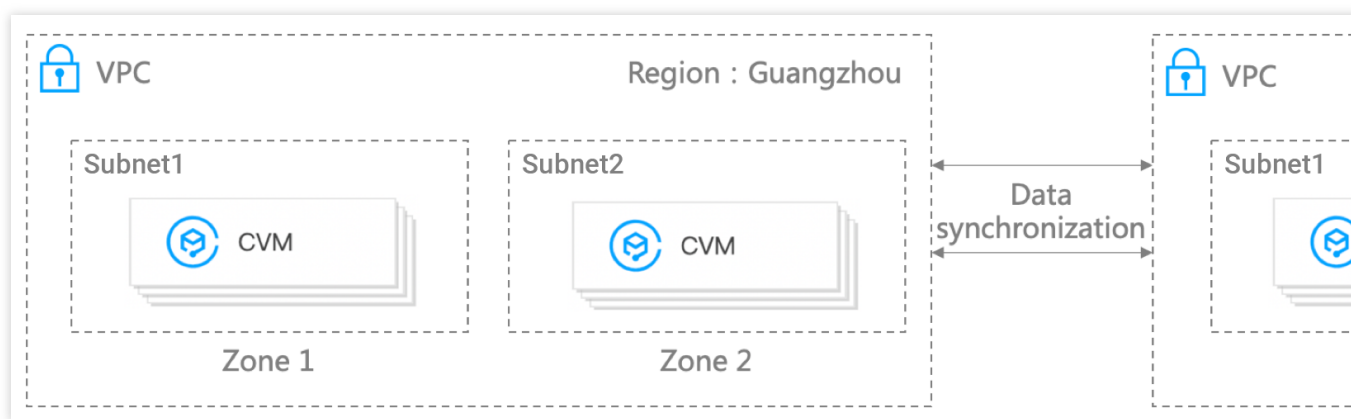
Cross-Availability Zone Disaster Recovery

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



Cross-Region Disaster Recovery

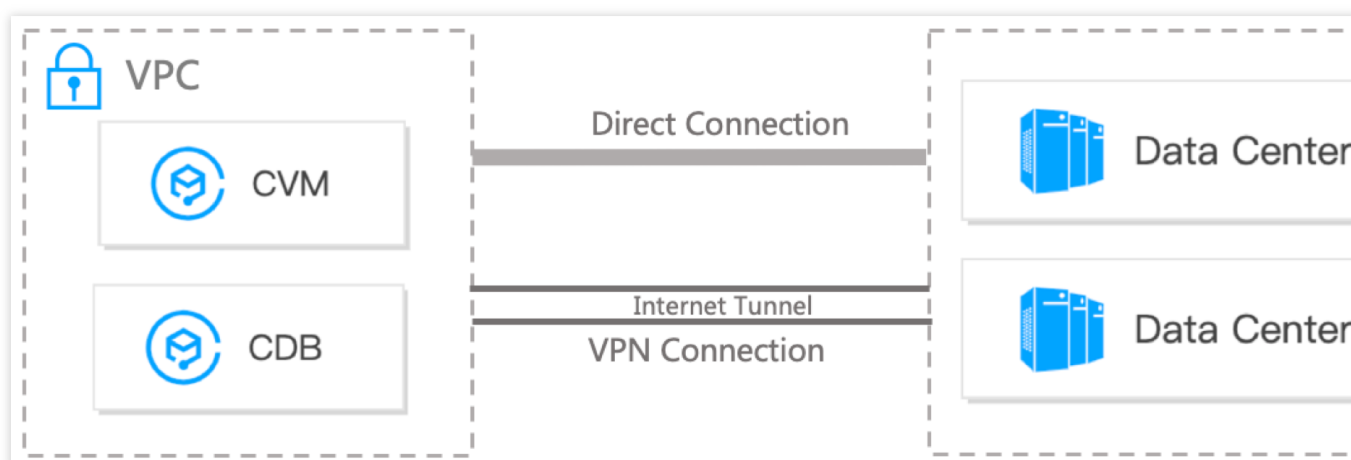
You can deploy businesses across regions (for example, the 2-region-3-DC solution) to achieve cross-region disaster recovery.



Deploying a Hybrid Cloud

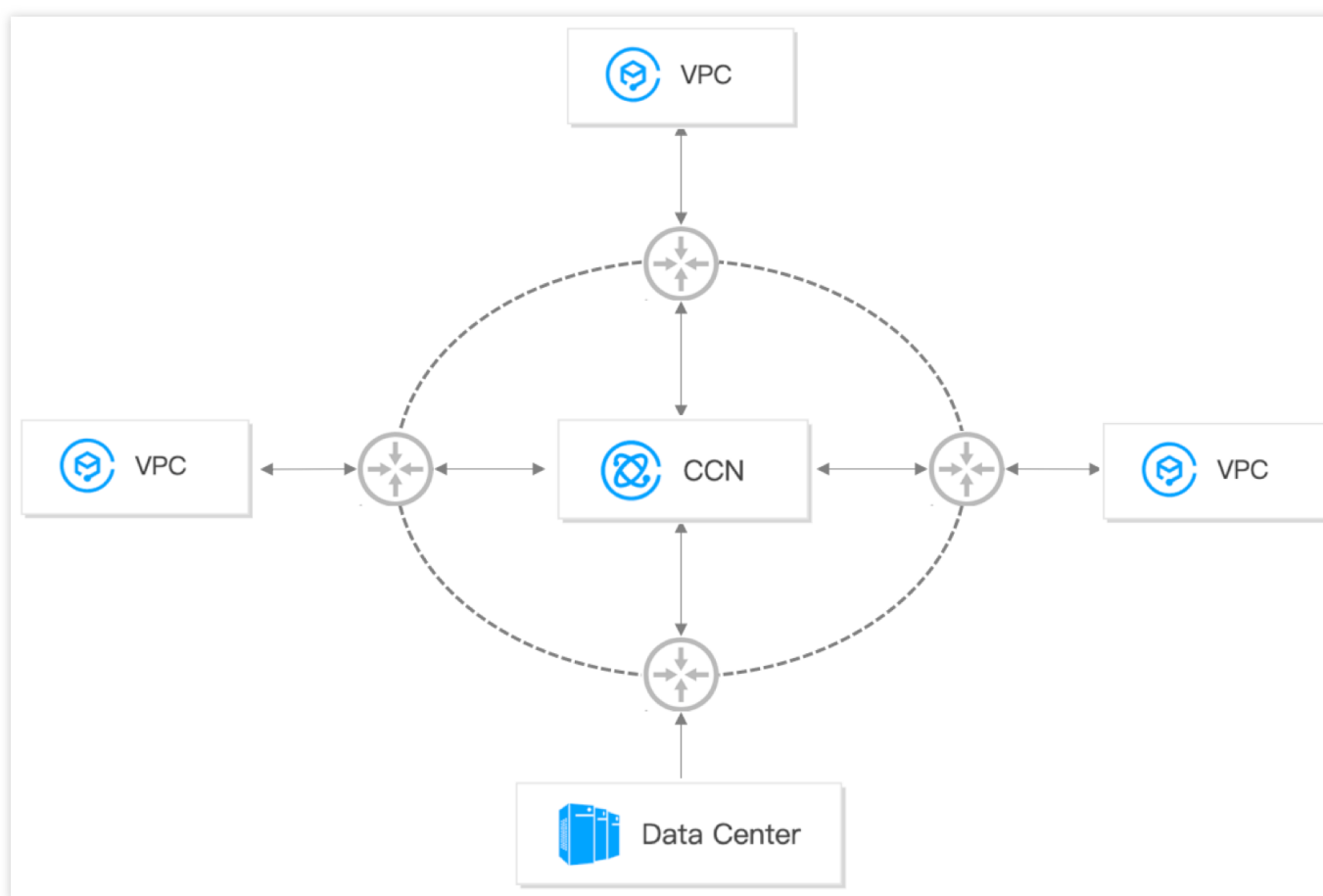
Connecting to Local IDCs

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 business volume to reduce IT Ops costs.



Global Multi-Point Interconnection

When you have businesses deployed in multiple regions around the world and require cross-region interconnection, you can use products such as [CCN](#) and [Direct Connect](#) to enable global multi-point interconnection through single-point access.



Concepts

Regions and Availability Zones

Last updated : 2024-01-24 17:22:28

Regions

Overview

A region is the physical location of an IDC. In Tencent Cloud, regions are fully isolated from each other, ensuring cross-region stability and fault tolerance. We recommend that you choose the region closest to your end users to minimize access latency and improve access speed.

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. Tencent Cloud services in different regions **cannot communicate via a private network by default**.

Tencent Cloud services across 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 2.0 \(New\)](#) feature, cross-region binding of CLB and CVM instances is supported.

Availability Zone

Overview

Availability zones (Zone) refer to Tencent Cloud's physical data centers whose power and network are independent from each other within the same region. They are designed to ensure that failures within an availability zone can be isolated (except for large-scale disaster or major power failure) without spreading to other zones, so as to ensure your business stability. By starting an instance in an independent availability zone, users can protect their applications from being affected by the failures occurring in a single location.

You can view the following table or use the [DescribeZones](#) API to get a complete availability zone list.

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 availability zones 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

Region	AZ
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 4ap-guangzhou-4
	Guangzhou Zone 6ap-guangzhou-6
	Guangzhou Zone 7ap-guangzhou-7
East China (Shanghai)ap-shanghai	Shanghai Zone 1ap-shanghai-1
	Shanghai Zone 2ap-shanghai-2
	Shanghai Zone 3ap-shanghai-3
	Shanghai Zone 4ap-shanghai-4
	Shanghai Zone 5 ap-shanghai-5
	Shanghai Zone 8 ap-shanghai-8
East China (Nanjing)ap-nanjing	Nanjing Zone 1ap-nanjing-1
	Nanjing Zone 2ap-nanjing-2
	Nanjing Zone 3ap-nanjing-3
North China (Beijing)ap-beijing	Beijing Zone 1ap-beijing-1
	Beijing Zone 2ap-beijing-2
	Beijing Zone 3ap-beijing-3
	Beijing Zone 4ap-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) ap-chongqing	Chongqing Zone 1 ap-chongqing-1
Hong Kong, Macao and Taiwan, China (Hong Kong) ap-hongkong	Hong Kong Zone 1 (Nodes in Hong Kong, China can cover services in Hong Kong/Macao/Taiwan regions) 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 Hong Kong/Macao/Taiwan regions) ap-hongkong-3

Other countries and regions

Region	AZ
Southeast Asia (Singapore) ap-singapore	Singapore Zone 1 (Nodes in Singapore can cover Southeast Asia) ap-singapore-1
	Singapore Zone 2 (Nodes in Singapore can cover Southeast Asia) ap-singapore-2
	Singapore Zone 3 (Nodes in Singapore can cover Southeast Asia) ap-singapore-3
	Singapore Zone 4 (Nodes in Singapore can cover Southeast Asia) ap-singapore-4
Southeast Asia (Jakarta) ap-jakarta	Jakarta Zone 1 (Nodes in Jakarta can cover Southeast Asia) ap-jakarta-1
	Jakarta Zone 2 (Nodes in Jakarta can cover Southeast Asia) ap-jakarta-2
Northeast Asia (Seoul) ap-seoul	Seoul Zone 1 (Nodes in Seoul can cover Northeast Asia) ap-seoul-1

	Seoul Zone 2 (Nodes in Seoul can cover Northeast Asia)ap-seoul-2
Northeast Asia (Tokyo)ap-tokyo	Tokyo Zone 1 (Nodes in Tokyo can cover Northeast Asia)ap-tokyo-1
	Tokyo Zone 2 (Nodes in Tokyo can cover Northeast Asia)ap-tokyo-2
South Asia (Mumbai)ap-mumbai	Mumbai Zone 1 (Nodes in Mumbai can cover South Asia)ap-mumbai-1
	Mumbai Zone 2 (Nodes in Mumbai can cover South Asia) ap-mumbai-2
Southeast Asia (Bangkok)ap-bangkok	Bangkok Zone 1 (Nodes in Bangkok can cover Southeast Asia)ap-bangkok-1
	Bangkok Zone 2 (Nodes in Bangkok can cover Southeast Asia)ap-bangkok-2
North America (Toronto)na-toronto	Toronto Zone 1 (Nodes in Toronto can cover North America)na-toronto-1
South America (Saopaulo) South America (Saopaulo)	Saopaulo Zone 1 (Nodes in Saopaulo can cover South America)sa-saopaulo-1
Western US (Silicon Valley)na-siliconvalley	Silicon Valley Zone 1 (Nodes in Silicon Valley can cover Western US)na-siliconvalley-1
	Silicon Valley Zone 2 (Nodes in Silicon Valley can cover Western US)na-siliconvalley-2
Eastern US (Virginia)na-ashburn	Virginia Zone 1 (Nodes in Virginia can cover Eastern US)na-ashburn-1
	Virginia Zone 2 (Nodes in Virginia can cover Eastern US)na-ashburn-2
Europe (Frankfurt)eu-frankfurt	Frankfurt Zone 1 (Nodes in Frankfurt can cover Europe)eu-frankfurt-1
	Frankfurt Zone 2 (Nodes in Frankfurt can cover Europe)eu-frankfurt-2
Europe (Moscow)eu-moscow	Moscow Zone 1 (Nodes in Moscow can cover Europe)eu-moscow-1

How to select the region and availability zone

When selecting a region and availability zone, take the following into consideration:

Your location, the location of your users, and the region of the CVM instances.

We recommend that you choose the region closest to your end users when purchasing CVM instances to minimize access latency and improve access speed.

Other Tencent Cloud services you use.

When you select other Tencent Cloud services, we recommend you try to locate them all in the same region and availability zone to allow them to communicate with each other through the private network, reducing access latency and increasing access speed.

High availability and disaster recovery.

Even if you have just one VPC, we still recommend that you deploy your businesses in different availability zones to prevent a single point of failure and enable cross-AZ disaster recovery.

There may be network latency among different availability zones. We recommend that you assess your business requirements and find the optimal balance between high availability and low latency.

Resource Availability

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

Resource	Resource ID Format -8-Digit String of Numbers and Letters	Type	Description
User Account	No limit	Globally unique	Users can use the same account to access Tencent Cloud resources around the world.
SSH Keys	skey-xxxxxxx	Global	Users can use an SSH key to bind a CVM in any region under the account.
CVM Instances	ins-xxxxxxx	CVM instances are specific to an availability zone	Users can only create a CVM instance in a specific AZ.
Custom Images	img-xxxxxxx	Regional	Users can create custom Image for instances which can be used in different availability zones of the same region Please copy custom image to other regions using the copy image function to use it in those regions.

EIPs	eip-xxxxxxx	Can be used in multiple AZs in a region	EIPs (Elastic IPs) can only be created in a region and be associated with instances in the same region.
Security Groups	sg-xxxxxxx	Can be used in multiple AZs in a region	Security Group is created under a certain region, and can only be associated with instance in the same region. Tencent Cloud automatically creates 3 default Security Groups for users.
Cloud Block Storage	disk-xxxxxxx	CBS disks are specific to an availability zone.	Users can only create a Cloud Block Storage disk in a specific AZ and mount it to instances in the same availability zone.
Snapshots	snap-xxxxxxx	Can be used in multiple AZs in a region	A snapshot created from a cloud disk can be used for other purposes (such as creating cloud disks) in this region.
Cloud Load Balancer	clb-xxxxxxx	Can be used in multiple AZs in a region	Cloud Load Balancer can be bound with CVMs in different availability zones of a single region for traffic forwarding.
VPC	vpc-xxxxxxx	Available in multiple availability zones of a single region	A VPC in one region can have resources created in different availability zones of the region.
Subnets	subnet-xxxxxxx	Subnets are specific to an availability zone.	Users cannot create subnets across availability zones.
Route Tables	rtb-xxxxxxx	Can be used in multiple AZs in a region	When creating a route table, users need to specify a VPC. Therefore, route tables are regional as well.

References

Migrating an instance to another availability zone

For an instance that is already started, its availability zone cannot be changed, but its user can migrate it to another availability zone by other means. The migration process involves creating a custom image from the original instance, using the custom image to start an instance in a new availability zone and updating the configuration of the new instance.

1. Create a custom image for the source instance. [Creating Custom Images](#)
2. If the [network environment](#) of the current instance is VPC and the private IP address must be retained after migration, you need to delete the subnet in the current availability zone and then create a subnet in the new availability zone with the same IP address range as that of the original subnet. Please note that a subnet can be deleted only when it contains no available instance. Thus, all the instances in the current subnet should be migrated to the new subnet.
3. Create a new instance in the new AZ by using the created custom image. You can choose the same type and configuration as those of the original instance, or choose new ones. For more information, see [Creating Instances via CVM Purchase Page](#).
4. If the source instance is associated with an EIP, disassociate the EIP and associate it with the new instance. For more information about shutting down an instance, please see [Shutdown Instances](#).
5. For more information, see [Terminating Instances](#).

Copying images to other regions

Region attribute is differentiated for all behaviors such as enabling and viewing instances by users. If image of the instance that the users need to enable does not exist in the region, then the image needs to be copied to current region. [Copying Images](#).

IPv4 Addresses

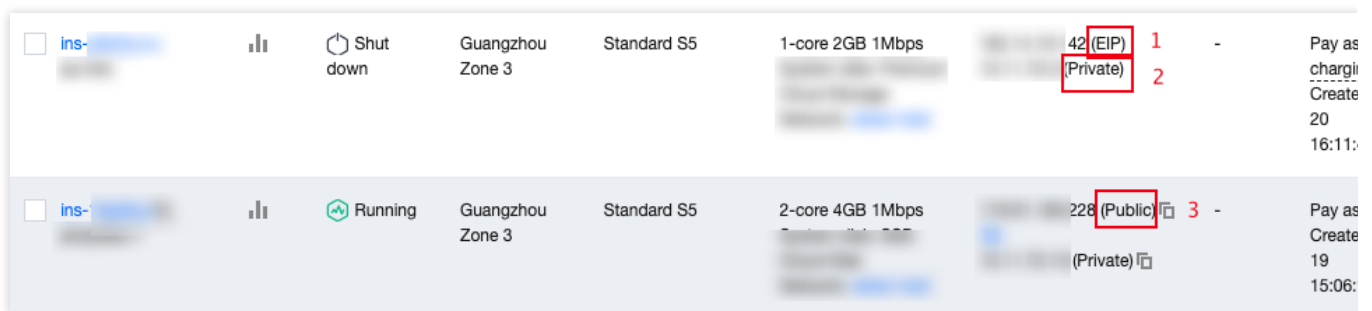
Last updated : 2024-05-23 10:45:03

IPv4 Addresses

Tencent Cloud provides IPv4 addresses for both the private and public network access. A public IPv4 address can be common or elastic. As shown in the following figure, **EIP** indicates an elastic IPv4 address, **Private** indicates a private IPv4 address, and **Public** indicates 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.



<input type="checkbox"/>	ins-			Guangzhou Zone 3	Standard S5	1-core 2GB 1Mbps	42 (EIP)	1	-	Pay as charged
<input type="checkbox"/>	ins-			Guangzhou Zone 3	Standard S5	2-core 4GB 1Mbps	228 (Public)	3	-	Create 19 15:06

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, cloud services 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, cloud services under the same account in a different region cannot be accessed via the IPv4 private network.

Use cases

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.

Relevant operations

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 support public network access.	
Acquisition method	It can only be obtained when you purchase a CVM.	1. Apply for an EIP in the console. 2. Convert a public IP address to an EIP.
Features	It has the same lifecycle as the CVM, and will be released upon the release of the bound CVM.	It is independent from other resources. You can bind it to or unbind it from CVMs and NAT Gateways at anytime. You can release an EIP when you no longer need it.
Fees	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 Checking Account Type .
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 the limits on public IPs bound to a CVM.	
Operations	Converting an IP	A public IP can be converted to an EIP. The IP address will not change after the conversion.	An EIP cannot be converted back to a public IP.
	Changing an IP	A public IP can be directly changed. For more information, see Changing Public IP Addresses	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 a public IP, you can log in to the CVM console , locate the public IP, and in the Operation column, select More > IP/ENI > Return Public IP to return it.	You can release an EIP in the EIP console.
	Retrieving an IP	You can retrieve public IPs/EIPs that you have used if they have not been used by other users.	

Billing

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

Relevant Information

For more information about how to quickly build an IPv4 Virtual Private Cloud (VPC), see [Building Up an IPv4 VPC](#).
For more information about EIPs, see [Elastic IP](#).

Classic Network

Last updated : 2024-01-24 17:22:28

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

Note:

As the classic network resources become increasingly scarce and cannot be expanded, Tencent Cloud accounts registered after June 13, 2017, 00:00:00 can create instances (including CVM and CLB) only in a VPC rather than the classic network. If you need to use classic network service, please submit an application.

Use Limits

The classic network-based CVMs do not support ENIs.

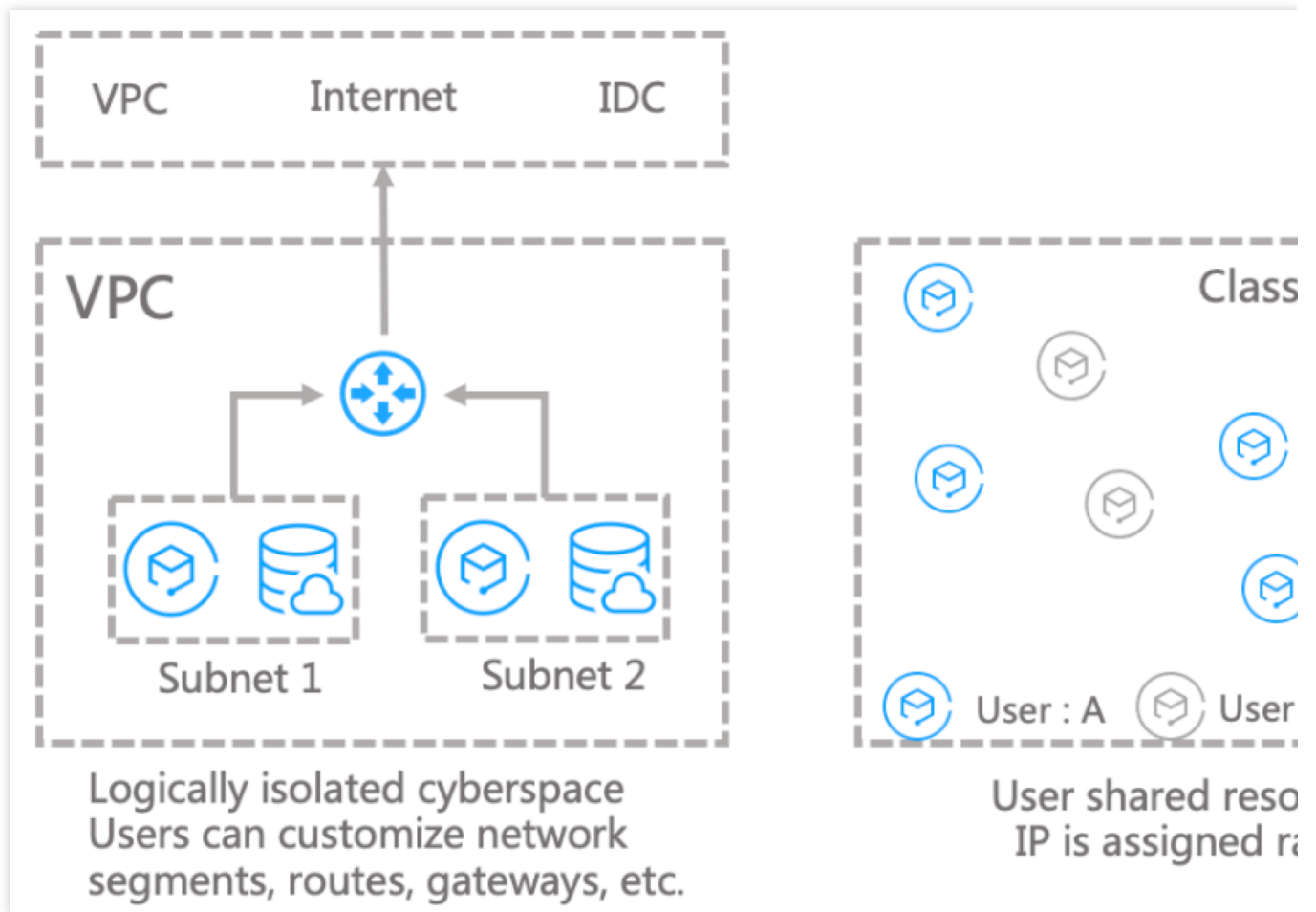
Migrating from the classic network to VPC is irreversible.

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.

By contrast, the VPC is a logically isolated network space in Tencent Cloud (as shown on the left side of the figure below). In a VPC, you can customize IP ranges, IP addresses, and routing policies. VPC is more suitable for use cases requiring custom configurations.

**Note:**

You can use the `DescribeAccountAttributes` API to query the network attributes of an account. If the `supportedPlatforms` value is `only-vpc`, the account is a default VPC user, who owns all cloud resources under VPCs. If the `supportedPlatforms` value is `classic`, the account is a default classic network user, who owns all cloud resources under the classic network.

Reference

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 detailed directions, see [Migrating from the Classic Network to VPC](#).

Quota Limit

Last updated : 2024-01-24 17:22:28

VPCs and Subnets

Resource	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

Resource	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

Resource	Quota Limit
Number of secondary ENIs per VPC	1,000

HAVIPs

Resource	Quota Limit
Number of default HAVIPs per VPC	10

Security Groups

Item	Description
Number of security groups	50 per region

Number of rules in a security group	100 for inbound rules and 100 for outbound rules
Number of CVM instances associated with a security group	2,000
Number of security groups associated with a CVM instance	5
Number of security groups that can be imported by a security group	10

Network ACLs

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

Parameter Templates

Resource Type	Quota Limit
IP address objects (ipm)	Max.: 1,000
IP address group objects (ipmg)	Max.: 1,000
Protocol port objects (ppm)	Max.: 1,000
Protocol port group objects (ppmg)	Max.: 1,000
IP address members in an IP address object (ipm)	Max.: 20
IP address object members (ipm) in an IP address group object (ipmg)	Max.: 20
Protocol port members in a protocol port group object (ppm)	Max.: 20
Protocol port object members (ppm) in a protocol port group object (ppmg)	Max.: 20
IP address group objects (ipmg) that can reference the same IP address object (ipm)	Max.: 50
Protocol port group objects (ppmg) that can reference the same protocol port object (ppm)	Max.: 50

Network Probes

--	--

Resource	Quota Limit
Number of network probes created in each VPC	50