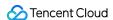


Cloud Dedicated Zone Operation Guide Product Documentation



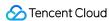


Copyright Notice

©2013-2025 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.

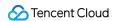
Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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

Operation Guide

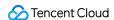
Cloud Service Category

Cloud Service Overview

Difference Description

Resource Usage Level Query

Public Network Access Instructions



Operation Guide Cloud Service Category Cloud Service Overview

Last updated: 2025-12-05 18:42:11

Cloud Dedicated Zone (CDZ) provides you with a cloud service experience basically consistent with that of the public cloud, covering full-stack product capabilities such as computing, storage, networking, databases, and security.

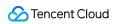
The following table lists the cloud service status of various products that have access to CDZ, helping you quickly plan your business architecture.



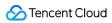
Note:

Reuse of Public Cloud Capabilities means that this capability is not deployed separately in the local CDZ; instead, the standard capability of the public cloud is reused.

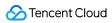
Product Categor y	Overview	Product Name	Local Deployment Within CDZ	Reuse of Public Cloud Capabilities
		Cloud Virtual Machine (CVM)	\mathscr{S}	-
		Cloud Bare Metal (CBM)	\mathscr{C}	-
	CDZ provides full- stack computing	Cloud GPU Service	\mathscr{C}	-
Comput ation	capabilities, supporting various scenarios ranging from general	Hyper Computing Cluster	V	-
perfor	computing to high- performance computing.	Auto Scaling (AS)	-	\mathscr{C}
		TencentCloud Automation Tools (TAT)	-	V
		Image	\mathscr{C}	-



		Cloud SSD/Premium Disk/Balanced SSD	V	-
		Snapshot	\mathscr{C}	_
Storage	CDZ provides complete data storage solutions, including block storage, file storage, and object storage.	CDZ – Cloud Storage Private (CSP)	① Note: Some Cloud Object Storage (COS) features are unsupported . For details, see Difference Description.	
		COS	€	-
		Cloud File Storage (CFS)	\mathscr{O}	_
Network	CDZ provides	Virtual Private Cloud (VPC)	\mathscr{C}	-
	connectivity capabilities	Elastic Network Interface (ENI)	\mathscr{C}	-
	consistent with the public cloud	Security Group	\mathscr{Q}	_
	experience, supporting interconnection and	Cloud Load Balancer (CLB)	⊘	-
	communication with	Elastic IP (EIP)	V	_
	other zones, and	NAT Gateway	V	-
	local IDCs.	Private Link	⊘	-



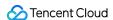
		Direct Connect (DC)	S	_
		Cloud Connect Network (CCN)	V	_
		Flow Logs (FL) / Bandwidth Package (BWP)	-	\mathcal{S}
		TencentDB for MySQL	\mathscr{C}	-
		TencentDB for PostgreSQL	\mathscr{S}	-
		TDSQL-C	V	-
	CDZ features	TencentDB for SQL Server	\mathscr{O}	-
Databas	allowing you to	TencentDB for Redis®	\mathscr{C}	_
е		TencentDB for MongoDB	\mathscr{C}	_
		Data Transfer Service (DTS)	-	\mathscr{C}
		Database Expert Service (DBexpert)	-	\mathscr{C}
		TencentDB for DBbrain (DBbrain)	-	\mathscr{C}
Cloud manage ment	age CDZ seamlessly integrates with	Cloud Access Management (CAM)	_	\mathscr{C}
platform		Console	-	V
		Tencent Cloud Observability	-	\mathscr{C}



	and transparency of your business.	Platform (TCOP)		
		TencentCloud Managed Service for Prometheus (TMP)/Tencent Cloud Managed Service for Grafana (TCMG)	_	
		CloudAudit/Co nfig	_	\mathscr{O}
		Billing related	_	⊘
		Tencent Cloud Smart Advisor (TSA)	_	\mathscr{C}
		TencentCloud API	_	€
		SDK Center	_	€
		Tag	_	\checkmark
Containe r and middlew are	CDZ provides complete application lifecycle	Tencent Kubernetes Engine for Serverless	\mathscr{O}	-
	management capabilities for containerized applications and integrates commonly used middleware services to help you build modern, scalable application architectures.	Tencent Kubernetes Engine (TKE)	\mathscr{C}	-
		Tencent Container Registry (TCR)	_	\mathscr{C}
		TACO LLM Inference Acceleration Engine	$ ot\!$	_



		TDMQ for CKafka	\mathscr{O}	_
		Anti-DDoS	V	-
		Cloud Firewall (CFW)	V	-
	CDZ seamlessly	Web Application Firewall (WAF)	\mathscr{O}	-
	integrates Tencent Cloud-native security capabilities, providing comprehensive Security Protection for your dedicated resources from the infrastructure layer to the application layer to ensure business security and compliance.	Cloud Workload Protection Platform (CWPP)	\mathscr{O}	_
Security		Tencent Container Security Service (TCSS)	\mathscr{O}	_
		Cloud Security Center (CSC)	\mathscr{O}	-
		Bastion Host (BH)	_	V
		Key Management Service (KMS)	_	V



Difference Description

Last updated: 2025-12-05 18:42:25

Cloud Dedicated Zone (CDZ) provides you with an operating experience and APIs that are basically consistent with those of the public cloud. However, due to the characteristics of its deployment environment and exclusive resources, some product features may have differences.

This document details the differences between CDZ and the standard public cloud in terms of product features, performance, and usage limits, helping you better plan and use CDZ resources.

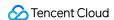
Storage Product Differences

CDZ - CSP

CDZ – Cloud Storage Private (CSP) is a localized and exclusive version of Tencent Cloud Object Storage (COS). It is deployed in your CDZ environment to provide you with object storage services featuring localized data and exclusive resources.

Feature Limitations

- Compared with COS, CSP currently has the following limitations:
 - Object upload and download operations in the console are not supported.
 - Only the standard storage layer is supported. Other storage layers, such as infrequent access and archive storage, are not supported.
 - Static website hosting is not supported.
 - Object origin-pull settings are not supported.
 - Temporary link access is not supported.
 - Server-end encryption is not supported.
 - Object tags are not supported.
 - Hotlink protection and cross-origin access settings are not supported.
 - Bucket replication is not supported.
 - O Domain name transfer and management are not supported.
 - Up to 20 million objects per bucket are supported.
- In addition, some features that require integration with other cloud products are also temporarily not supported:
 - Log management is not supported.
 - Content review is not supported.
 - Data processing is not supported.
 - Data workflow is not supported.



- Function calculation is not supported.
- File system gateway is not supported.
- Compared with COS, CSP also has performance limitations.

Since all loads are handled by on–premises servers, the achievable performance levels depend on the scale of the on–premises servers. In addition, all operations of CSP require authentication through Cloud Access Management (CAM) of the public cloud, so the additional network latency will also reduce the performance of CDZ – CSP. For example, in a typical cluster with 3 storage nodes, the expected performance level is 1,000 QPS (for small file scenarios) or 500 MB/s bandwidth (for large file scenarios), which is lower than the 30,000 QPS or 15 Gbit/s per bucket of the public cloud.

Product Billing Rule Description

The payment mode is prepaid, requiring the purchase of CSP resources through a capacity-based committed use method. After that, Tencent Cloud will deploy the cluster according to the purchased scale and provide storage services.

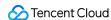
Billing Item	Billi ng Cycl e	Billi ng Mod e	Billing Rule
Storage capacity fee	Mon th	Pay - as- you -go	 Monthly settlement Storage capacity fee = Monthly storage capacity x Unit price of storage capacity Monthly storage capacity = Sum of daily storage capacity in the current month/30 Daily storage capacity = Average capacity obtained from time-based sampling on the day
Read–write request fee	Mon th	Pay - as- you -go	 The number of read-write requests refers to the number of request instructions sent. The fee is calculated based on the total number of requests in the month. Requests are charged regardless of success or failure. The minimum billing unit for requests is 10,000 times. If the number of requests in the month is less than 10,000, the fee is calculated based on the actual number of requests.



Public network	Pay Mon th	 Traffic that generated when data is downloaded from the cloud to your local end or client through the regular network (the public Internet). Pay-as-you-go: Public network downstream traffic (GB) x Unit price per GB. 	
traffic fee		you –go	① Note: This part is usually not included in committed use and requires payment based on actual public network usage.

Usage Instructions

- Configuration management: The CSP console is integrated into the Tencent Cloud console. You can select a dedicated cluster in the availability zone (AZ) of CDZ in the COS console to perform operations such as bucket creation, deletion, and configuration, which is consistent with the experience of using COS.



Resource Usage Level Query

Last updated: 2025-12-05 18:42:34

The resource usage level monitoring system of Cloud Dedicated Zone (CDZ) offers real-time, accurate, and visual resource usage insights to help you manage the resource lifecycle efficiently and ensure stable business operations.

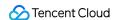
Resource Usage Level Query

- 1. Log in to the CDZ console, select the Resource Utilization tab to view resource consumption status.
- 2. Click View Details Only to obtain the resource detailed report.



Note:

You can also obtain the resource usage level by calling the API.



Public Network Access Instructions

Last updated: 2025-12-05 18:42:45

Overview

This document provides a detailed description of the solutions for implementing public network access in Cloud Dedicated Zone (CDZ).

Solution Comparison

CDZ provides three distinct architecture solutions to ensure secure and efficient public network access for your business. The following is a detailed comparison of these solutions to help you select the most suitable one based on your actual business scenarios:

Soluti on	[Common] Solution 1	Solution 2	Solution 3
Soluti on Desc riptio n	Access the public network through the public network product in the (primary) region where your CDZ is located.	Access the public network through the self-owned Internet Data Center (IDC).	Access the public network through the local public network cluster in CDZ.
Scen arios	General scenarios.	A local public network egress exists.	High network performance, large-scale traffic egress, and self-owned public network resources are required.
Prere quisit es	Supported by default.	 Deployment of a Direct Connect (DC) gateway is required during CDZ activation. The self-owned IDC and public network access capability are required. 	 Self-owned IP ranges are usually required. Confirmation of the need to deploy the local public network cluster in CDZ during CDZ activation is required
Core Path	Use the public network capabilities of the region where your CDZ is located.	CVM in CDZ → Direct Connect (DC) → Private network of the self-owned IDC → Public network	Use the local public network cluster to access the Internet.



		cluster in the IDC \rightarrow the Internet.	
Billin g Rule	Pay for the resources of Elastic IP (EIP) and Cloud Load Balancer (CLB) in the public cloud based on actual consumption.	Committed use fee of the DC gateway cluster in CDZ.	Committed use fee of the local public network cluster in CDZ.
Com plexit y	Low (simple cloud configuration)	High (requiring proper configuration of the DC gateway and network interconnection with the local IDC)	Low (provided by Tencent Cloud)

[Common] Solution 1: Accessing the Public Network Through the Product Network Product in the (Primary) Region Where Your CDZ Is Located

Scenarios

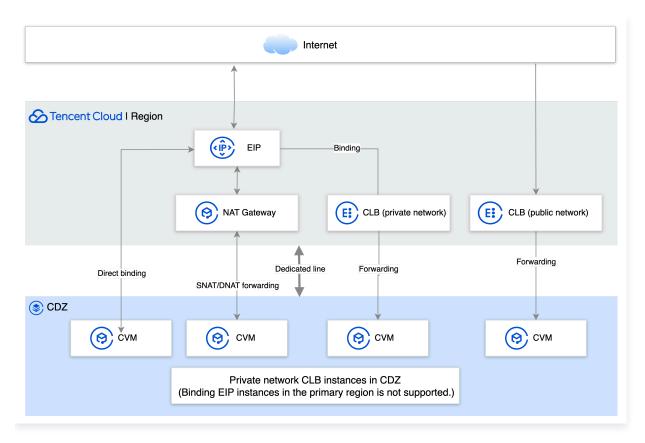
This solution is suitable for scenarios where no local public network cluster is deployed in the CDZ environment and traffic forwarding through the self-owned IDC is not required. In this case, the Internet access can be achieved by using the public network capabilities of the primary region of Tencent Cloud. This solution offers high flexibility in deployment and is applicable to most general scenarios, especially the following scenarios:

- Requirement for rapid business launch: The need to quickly establish public network access capabilities without going through complex local egress deployment processes.
- No IDC infrastructure: Enterprises do not have self-built IDCs, or their existing IDCs cannot access the public network.
- Operational agility and elasticity: The need to use EIP or public network CLB resources on the cloud, and take advantage of their benefits such as on-demand configuration, flexible scaling, and convenient maintenance.

Prerequisite Dependencies

- A connection between CDZ and the primary region is established. DC is supported by default.
- The traffic for public network access cannot exceed the bandwidth supported by DC.

Network Architecture

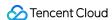


Operation Process

We provide 4 sub-solutions based on the inbound and outbound scenarios.

Soluti on	[Recommende d] A	[Recommended] B	[Recommended] C	D
Soluti on Descri ption	Bind EIP to CVM.	Bind NAT Gateway to CVM.	Regional public network CLB.	Regional private network CLB and EIP.
Billing Mode	Pay-as-you- go: EIP fee	Pay-as-you-go: NAT Gateway instance fee + EIP fee	Pay-as-you-go: CLB instance fee + EIP fee	Pay-as-you- go: CLB instance fee + EIP fee

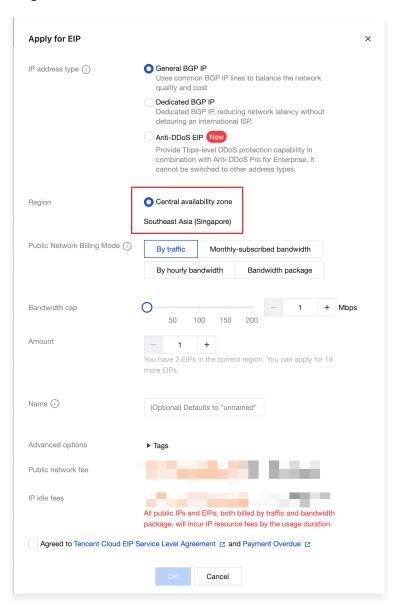
Solution A: [Recommended] Binding EIP to CVM Scenarios



This solution is suitable for business scenarios where an EIP needs to be directly provided for the CVM instance in CDZ. Public network traffic is forwarded to the interior of CDZ through the EIP of the primary region.

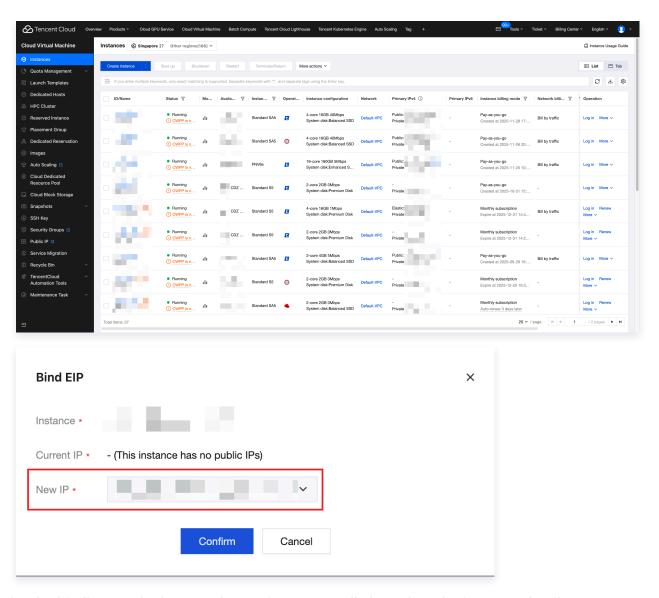
Operation Process

- 1. Apply for an EIP: On the Public IP page in the console, apply for an EIP in the central AZ of CDZ's primary region. For detailed operations, see Applying for an EIP.
- 2. Bind an EIP:
 - 2.1 Log in to the CVM console.

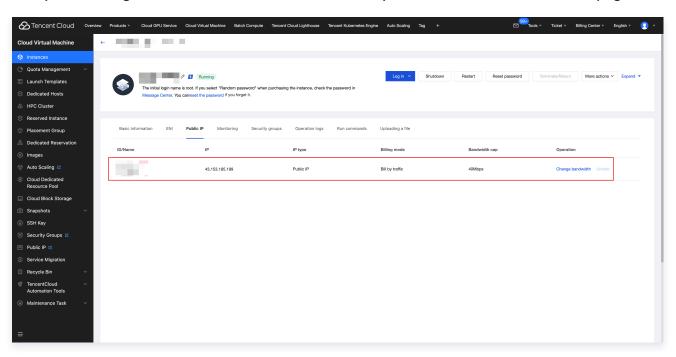


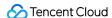
- 2.2 Select the CVM instance in CDZ to which you want to bind the EIP.
- 2.3 On the instance details page, choose IP/NIC > Bind Elastic IP.
- 2.4 Select the applied EIP to complete the binding.





3. Verify the binding result: Confirm the EIP is successfully bound on the instance details page.





4. Test public network connectivity: Log in to the CVM instance from the console and use the pin

```
g command to test public network connectivity.
```

```
Welcome to TencentOS Server 4 x86_64

Version 4.4 20250805

[root@VM-0-7-tencentos ~]# ping www.qq.com

PING ins-r23tsuuf.ias.tencent-cloud.net (109.244.211.100) 56(84) bytes of data.
64 bytes from 109.244.211.100 (109.244.211.100): icmp_seq=1 ttl=57 time=3.02 ms
64 bytes from 109.244.211.100 (109.244.211.100): icmp_seq=2 ttl=57 time=3.21 ms
64 bytes from 109.244.211.100 (109.244.211.100): icmp_seq=3 ttl=57 time=3.20 ms
64 bytes from 109.244.211.100 (109.244.211.100): icmp_seq=4 ttl=57 time=3.21 ms
64 bytes from 109.244.211.100 (109.244.211.100): icmp_seq=5 ttl=57 time=3.20 ms
```

Solution B: [Recommended] Binding NAT Gateway to CVM

Scenarios

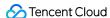
This sub-solution is suitable for users who expect to access the public network without exposing the private IP addresses of their CVM instances. The public network NAT Gateway provides public network access capabilities for multiple CVM instances (without EIPs) in a Virtual Private Cloud (VPC). It also supports mapping EIPs and ports to the private IP addresses and ports of the CVM instances, enabling public network access to CVM instances in the VPC.

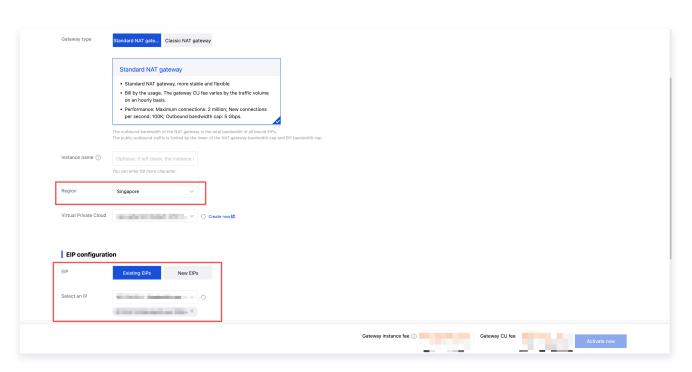
Tencent Cloud NAT Gateway supports multiple features, including Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT), gateway traffic control, traffic alarms, Bandwidth Package, security protection, and automatic disaster recovery. It features high performance, large capacity, and cross–availability zone disaster recovery capabilities.

Operation Process

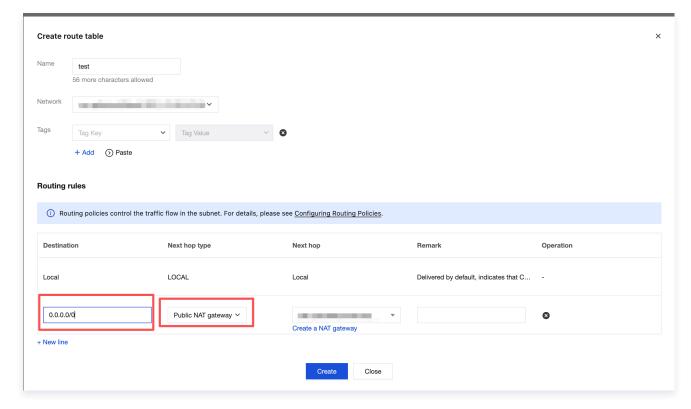
- 1. Create a NAT Gateway and bind an EIP:
 - 1.1 Log in to the NAT Gateway console, select a region, and click Create.
 - 1.2 Create a public network NAT Gateway with the configuration as follows:
 - Region: Select the CDZ primary region.
 - VPC: The selected VPC must include the CDZ subnet.
 - O EIP:
 - Existing EIP: Use an existing EIP under your account.
 - Create an EIP: An EIP is automatically assigned by the system to the NAT Gateway.

For other parameter configurations, see Creating a NAT Gateway.





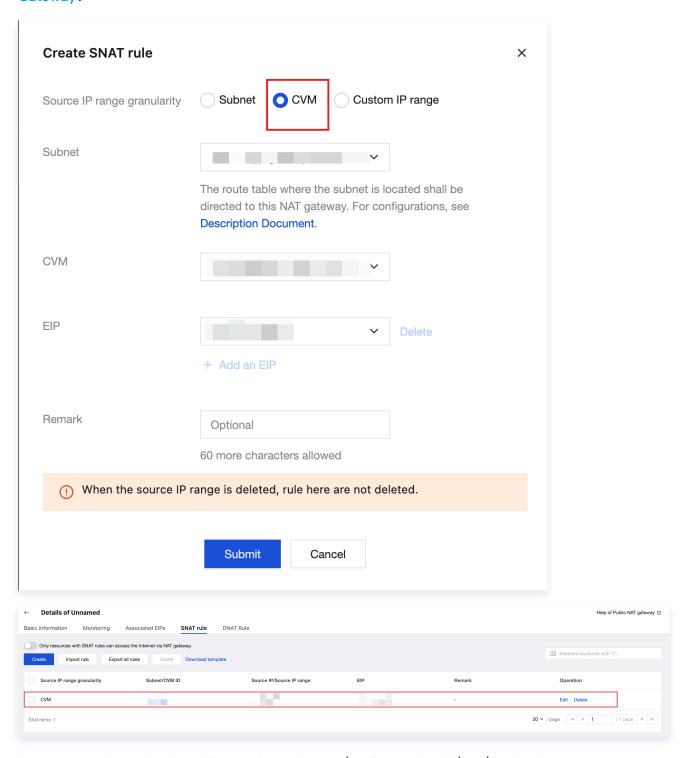
- 2. Configure a route pointing to the NAT Gateway: From the NAT instance list, access the subnet routing table of the VPC where the instance is located, and add a routing rule:
 - O Destination: Enter 0.0.0.0/0.
 - Next Hop Type: Select Public NAT Gateway.
 - O Next Hop: Select the NAT Gateway created in the previous step.



For detailed operations, see Configuring a Route Pointing to the NAT Gateway.

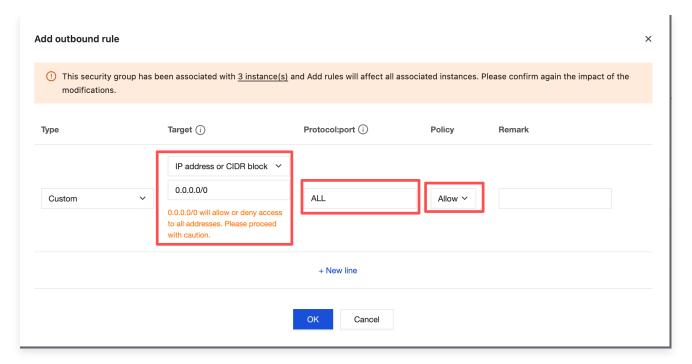


3. Configure SNAT rules: You can configure SNAT rules for the NAT Gateway to provide public network access for CVM instances in the VPC. When the NAT Gateway is bound to multiple EIPs, you can specify EIPs for public network access for the CVM instances in different groups based on the SNAT rules. For detailed operations, see Configuring a Route Pointing to the NAT Gateway.



4. Configure outbound rules: Allow outbound ports (such as TCP:80/443) in the CVM security group.





5. Test the public network connectivity: Log in to the CVM in the CDZ and use the ping command to test public network connectivity.

```
[root@VM-0-11-tencentos ~]# ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

64 bytes from 8.8.8.8: icmp_seq=1 ttl=104 time=173 ms

64 bytes from 8.8.8.8: icmp_seq=2 ttl=104 time=174 ms

64 bytes from 8.8.8.8: icmp_seq=3 ttl=104 time=176 ms

64 bytes from 8.8.8.8: icmp_seq=4 ttl=104 time=173 ms

64 bytes from 8.8.8.8: icmp_seq=5 ttl=104 time=177 ms

64 bytes from 8.8.8.8: icmp_seq=6 ttl=104 time=173 ms

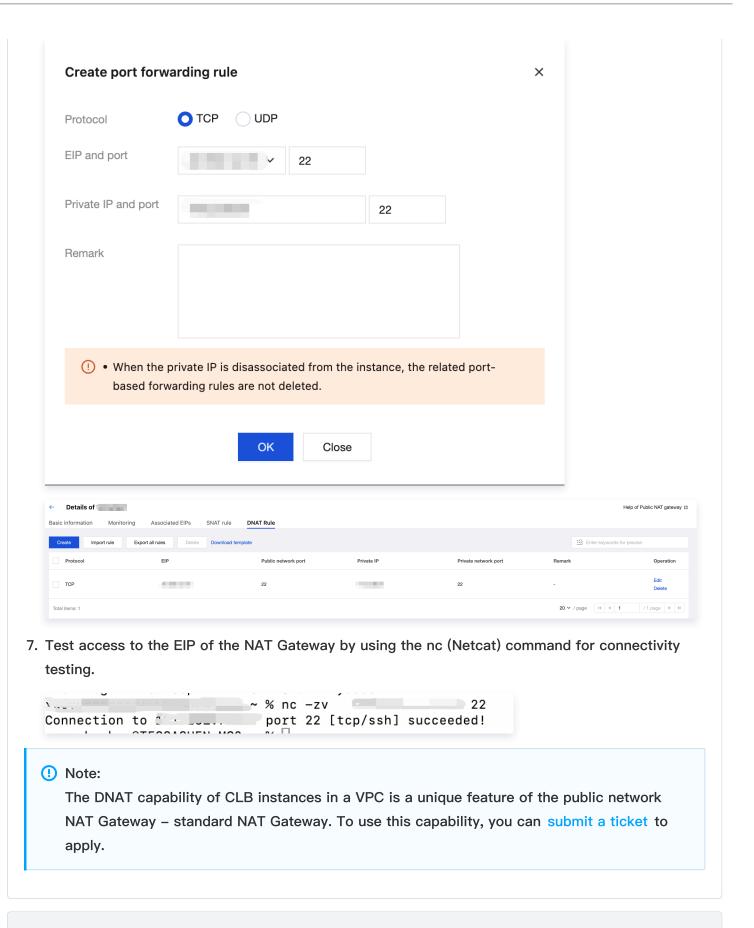
64 bytes from 8.8.8.8: icmp_seq=6 ttl=104 time=174 ms

64 bytes from 8.8.8.8: icmp_seq=8 ttl=104 time=176 ms

64 bytes from 8.8.8.8: icmp_seq=8 ttl=104 time=176 ms
```

- 6. Configure DNAT rules: The port forwarding table is a configuration table on the NAT Gateway for configuring the DNAT feature. It maps the private IP address, protocol, and port of instances (such as CVM, ENI, CLB, and cloud database instances) in the VPC to a public IP address, protocol, and port, making resources on the CVM instances accessible from the public network. For detailed operations, see Managing DNAT Rules.
 - Elastic IP and Exposed Port: Select the EIP bound to the NAT Gateway and the externally exposed port.
 - Private IP and Port: Specify the private IP address of the CVM instance and the service listening port.





Solution C: [Recommended] Public Network CLB



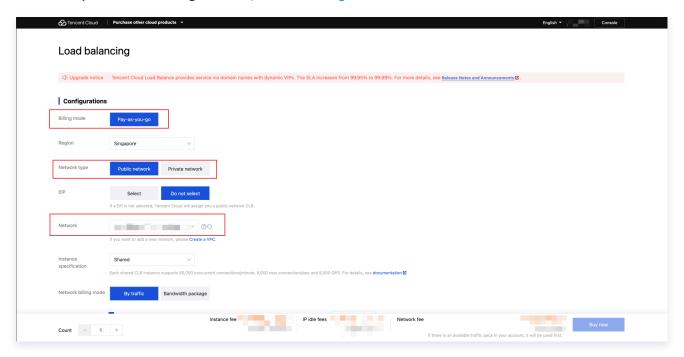
Scenarios

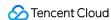
This sub-solution is suitable for web services or API services that require high-availability public network access capability. By creating a public network CLB instance in the primary region and adding CVM instances in a CDZ as backend servers, it enables public network access and traffic distribution.

Operation Process

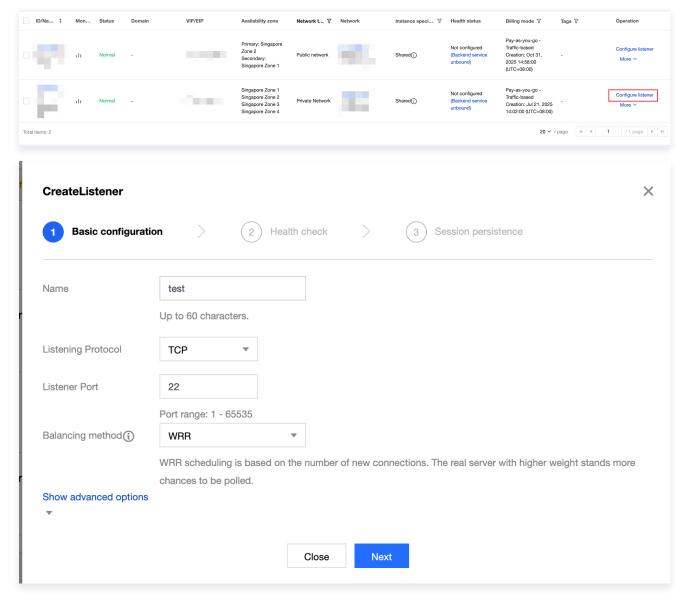
- Create a public network CLB instance: Log in to the CLB console, create a new public network CLB instance in the CDZ primary region. On the CLB console page, click Create and configure the CLB instance as follows:
 - Network Type: Select Public Network.
 - O Region: Select the region where the CDZ is located.
 - O EIP:
 - Not Select Elastic IP: An EIP is automatically assigned by the system to the CLB instance. The EIP is strongly bound to the CLB instance and will be released when the CLB instance is deleted.
 - Elastic IP: Use an existing EIP in your own account. The IP address exists as an independent EIP resource and is decoupled from the CLB instance.
 - Associated Network: Select a VPC that includes the CDZ subnet to use the public network
 CLB instance in the region (Region–CLB) and support EIP binding for public network access.

For other parameter configurations, see Creating a CLB Instance.



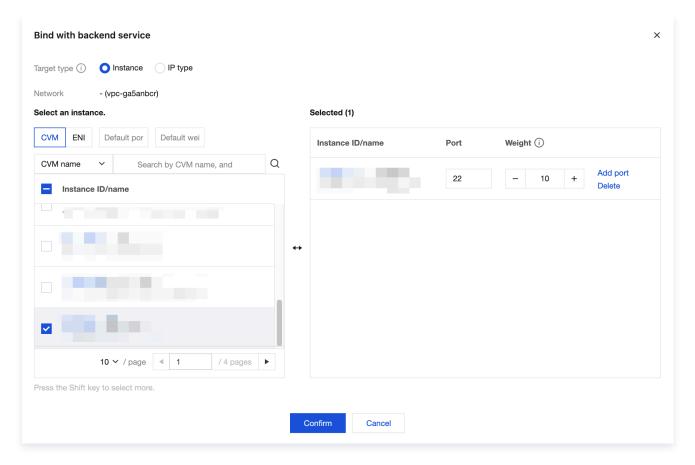


2. Configure a listener: On the CLB instance management page, click Configure Listener in the Operation column of the target CLB instance to create a listener.



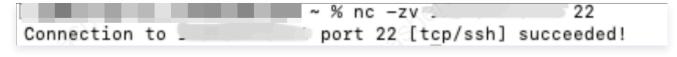
3. Bind CVM instances: Select the created listener, click Bind to bind the backend service, select and add CVM instances in the CDZ in sequence, and configure ports and weights.





Check the port health status to confirm that it is Healthy.

4. Test connectivity: Use the nc (Netcat) command to test connectivity, or log in to the CVM instance in the console and use the ping command to test public network connectivity.



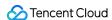
Solution D: Using Private Network CLB + EIP

Scenarios

This sub-solution is suitable for enterprises that already have a regional private network CLB architecture and wish to extend public network access capability to CVM instances within a CDZ. This sub-solution requires creating a private network CLB instance in the region and binding an EIP to it, then using the CLB instance to forward traffic to backend servers in the CDZ.

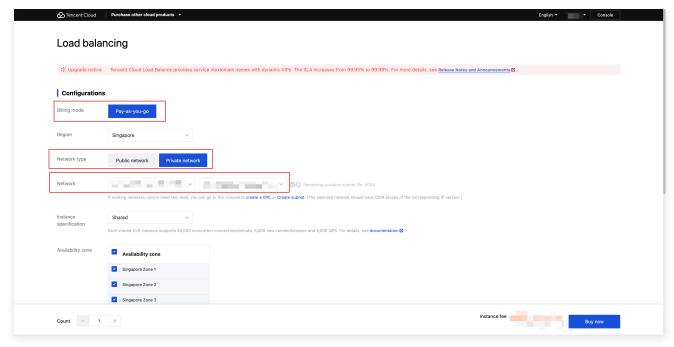
Operation Process

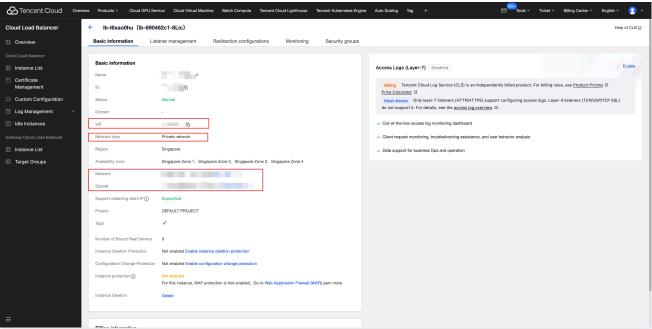
Create a private network CLB instance: Log in to the CLB console, create a public network CLB instance in the CDZ primary region. On the CLB console page, click Create and configure the CLB instance as follows:

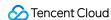


- O Billing Mode: Select Pay-as-You-Go Billing.
- O Region: Select the region where the CDZ is located.
- Network Type: Select Private Network.
- O Availability Zone: Select an AZ in the region.
- O Network:
 - VPC selection: Select a VPC that includes the CDZ subnet.
 - Subnet: Select a non-CDZ subnet to support EIP binding and realize public network access.

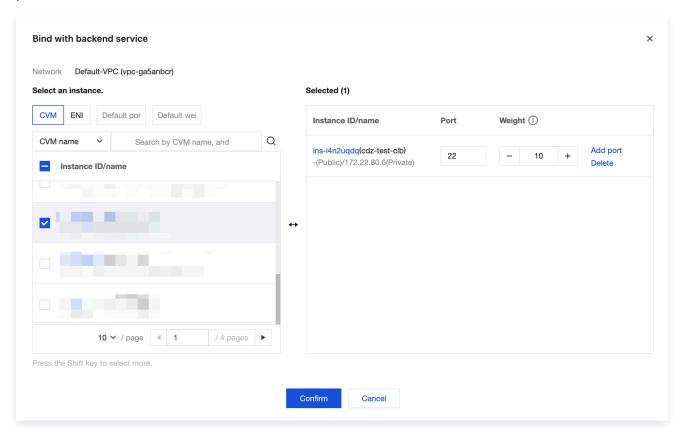
For other parameter configurations, see Creating a CLB Instance.



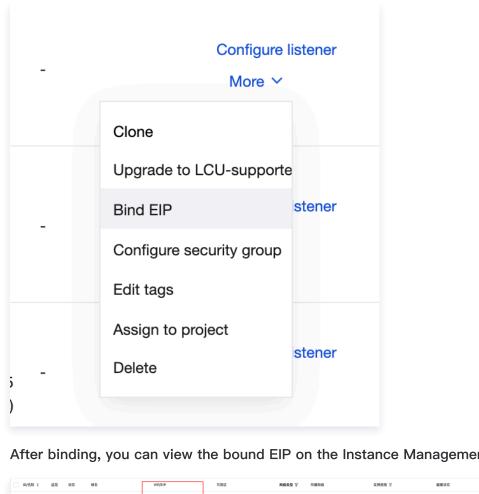




2. Configure listeners and backend services: Configure listeners and backend services on the private network CLB instance.



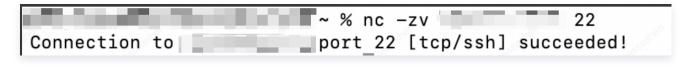
- 3. Apply for an EIP: In the EIP console, apply for an EIP.
- 4. Bind an EIP:
 - 4.1 Go to the CLB Instance Management page.
 - 4.2 In the operation column, choose More > Bind Elastic IP.
 - 4.3 Select the applied EIP to complete the binding.



After binding, you can view the bound EIP on the Instance Management page in the CLB console.



5. Test connectivity: Use the nc (Netcat) command to test connectivity, or log in to the CVM instance in the console and use the ping command to test public network connectivity.



FAQs

Q: Can the private network CLB instance in CDZ be bound to a regional EIP?

A: The private network CLB instance in CDZ cannot be directly bound to a regional EIP. The private network CLB instance in CDZ is a load balancing service designed for internal traffic scenarios in a VPC. It provides only private IP addresses and does not have public network access capability itself, nor does it support binding to a regional EIP or exposing public IP addresses. Therefore:

 If you select CDZ subnet when creating a CLB instance, the system will use the CLB cluster in CDZ by default. This CLB instance does not support EIP binding, and no CLB instance fee is charged. An error will occur if you bind an EIP to a CLB cluster in CDZ subnet:



• If you select a non-CDZ subnet when creating a CLB instance, it supports binding to a regional EIP, and a CLB instance fee is charged.

Therefore, we recommend that you create the CLB in a different subnet of the same VPC as CDZ to obtain complete public network access capability.

Subnet	CLB Cluster Used	Support for EIP Binding	Billing
CDZ subnet	CLB cluster built in CDZ (cdz-clb)	X EIP binding is not supported.	No CLB instance fee is charged.
Non-CDZ subnet	Primary region CLB cluster (region-clb)		The CLB instance fee is charged.

Solution 2: Accessing the Public Network Through the Self-Owned IDC

Scenarios

This solution is suitable for enterprises that have built a complete self-owned IDC network and hope that public network traffic will be transmitted back to the enterprise IDC through a connection, and then access the Internet through the public network egress of the IDC. Applicable scenarios include:

- Reuse of existing infrastructure: Enterprises have a mature IDC network architecture and security system, and wish to make full use of existing investments.
- Compliance and regulatory requirements: Due to data sovereignty, industry regulation, or internal compliance requirements, all public network traffic must pass through the self-owned egress.
- Unified hybrid cloud management: In hybrid cloud scenarios, unified network policies, security protection, and access control should be implemented.
- Fully autonomous and controllable egress: Enterprises want to perform fully independent management and audit on the public network egress.

Prerequisite Dependencies

Connection:

Establishing a connection between Tencent Cloud CDZ and your self-owned IDC is a prerequisite and should be completed first.

Depend ency	Detailed Explanation and Requirement
Connect ion readines s	 Application and activation: You have applied for a connection in the Tencent Cloud console and completed the survey and implementation. The connection status is activated.



- Access point: The access point of the connection should be within a reasonable distance from your IDC location to ensure transmission quality and low latency. Bandwidth specification: The connection bandwidth should meet the peak egress traffic demand of your cloud business accessing the public network, with a certain amount of redundancy reserved. Network connectivity: Create a dedicated tunnel on the Tencent Cloud side and complete the Layer-3 network interconnection configuration with the boundary router on your IDC side. Dedicat BGP session: A BGP session must be successfully configured and established on ed the dedicated tunnel to exchange routing information dynamically. This is the tunnel key to achieving route reachability. configur ation Redundancy design (optional but recommended): To ensure high service availability, it is strongly recommended to deploy two or more connections to form a primary-secondary or load-sharing architecture.
- Self-owned IDC network and public network egress



⚠ Note:

Tencent Cloud is only responsible for delivering traffic to your IDC boundary through a connection. The design and configuration of egress from IDC to the public network should be done manually.

This is the final egress for traffic and the policy execution point, which requires corresponding processing capabilities.

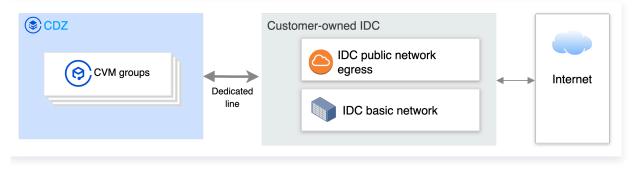
Depende ncy	Detailed Explanation and Requirement
Boundary router configura tion	 Route advertisement: The router on your IDC side must be able to advertise a default route (0.0.0.0/0) or specific public network IP ranges you want to access from the cloud to the Tencent Cloud DC gateway through a BGP session. Routing reception: It should be correctly configured to receive and learn the private IP range routes of CDZ from Tencent Cloud.
Public network egress device	 Egress capability: Equipment with public network egress capability (such as firewalls, routers, or dedicated NAT gateways) should be deployed in the IDC, and public network lines (such as fiber cable or metropolitan area networks) from the internet service provider (ISP) have been applied for. Public IP addresses: Ensure that the egress equipment has one or more available public IP addresses.



IDC private network planning

- Routing guide: The private network of your IDC can correctly route traffic received from DC (with the public network as the destination) to the public network egress equipment.
- Bandwidth and performance: The throughput performance of internal IDC equipment (such as core switches and firewalls) should be able to bear the additional public network traffic pressure brought by cloud services.

Network Architecture



Operation Process

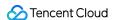
Complete the operation process for DC access in the Tencent Cloud console. For details, see Operation Process.

Solution 3: Accessing the Public Network Through Local Public Network Clusters in CDZ

Scenarios

This solution provides public network egress capability for cloud resources deployed in CDZ through a local public network cluster within CDZ. Public network traffic is forwarded within CDZ without passing through Tencent Cloud center regions or your self-owned IDC, thereby achieving minimal network latency and maximum bandwidth performance. It is suitable for the following scenarios:

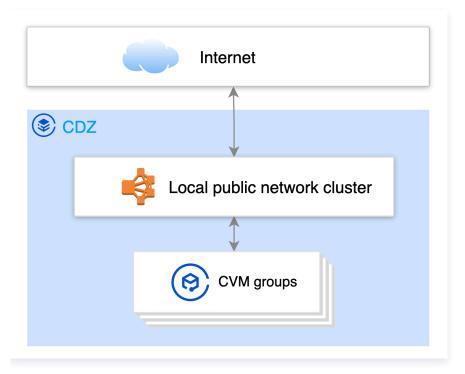
- Ultra-low latency business: Businesses highly sensitive to network latency, such as high-frequency trading systems, Tencent Real-Time Communication (TRTC), and Massively Multiplayer Online (MMO) games.
- High-traffic public network service: Scenarios with massive inbound and outbound public network traffic, such as CDN edge nodes, and big data file distribution and download centers.
- Compliance and sovereignty requirements: Industries with compliance requirements for independent public network egress, such as finance and government service, must meet regulatory requirements for data localization.
- Simplified Ops: Enterprises want public network capabilities to be uniformly provided and maintained by cloud vendors locally, simplifying their own network management.



Prerequisite Dependencies

- Local public network cluster: The deployment of a local public network cluster has been confirmed and completed during CDZ activation planning.
- Public IP address resource
 - IP source: Generally, the Bring Your Own IP (BYOIP) method is used, or you can apply for IP addresses from a local ISP. Tencent Cloud will assist in importing and managing the IP range into the public network cluster of CDZ.
 - IP authorization: Ensure that the provided IP range has been authorized by the corresponding Internet registration authority and can be broadcast normally.

Network Architecture

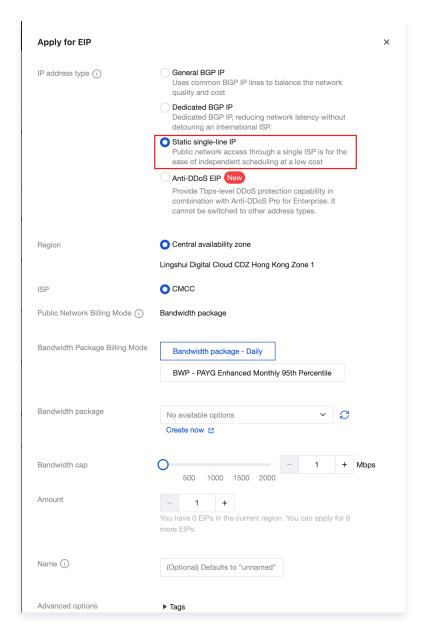


Operation Process

- 1. Create an EIP: Log in to the EIP console and click Apply.
 - IP Address Type: Select Static Single-Line IP.
 - Region: Select the region where your CDZ is located.

Click Apply Now to complete the creation. In this case, the EIP has been allocated from the local public network cluster in CDZ.





- 2. Bind the EIP to a CVM instance: In the EIP list, locate the applied EIP, choose More > Bind in the Operation column. In the Bind Resource pop-up window:
 - O Resource Type: Select CVM Instance.
 - Binding an Instance: Select the CVM instance in your CDZ that needs to access the public network.
- 3. Complete the verification: After successful binding, you can access the Internet through the private IP plus EIP of the CVM instance. You can log in to the CVM instance and run the ping or tracer
 - command to test public network connectivity. The traffic will directly pass through the local egress of CDZ.