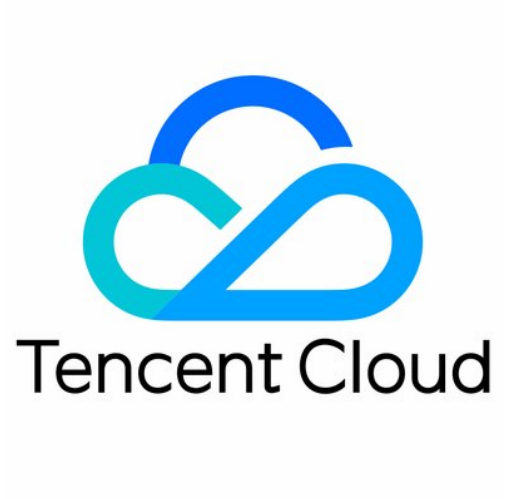
Cloud Load Balancer

Backend CVMs

Product Documentation



Contents

Backend CVMs
Real Server Overview

Last updated : 2020-04-26 17:27:11

What is a real server?

A real server is a CVM instance that is bound to the created CLB instance to process requests. When configuring a CLB listener, you need to bind a CVM instance as the real server. Through different polling methods, CLB forwards requests to the real server for processing to ensure application stability and reliability. You can bind CVM instances in one or more availability zones in the region where the CLB instance resides so as to enhance application robustness and block single points of failure.

Precautions

When adding a real server, we recommend that you:

- Install a web server (e.g., Apache or IIS) on all CVM instances to be bound to the CLB instance and ensure application consistency.
- You are recommended to enable session persistence, so that CLB can maintain a longer TCP connection for reuse by multiple requests, thereby reducing load on the web server and improving CLB throughput.
- Make sure that the real instance's security group has inbound rules for CLB listener ports and health check ports. For more information, please see Real Server Access Control.

Binding an ENI

Last updated : 2020-04-26 17:27:12

ENI Overview

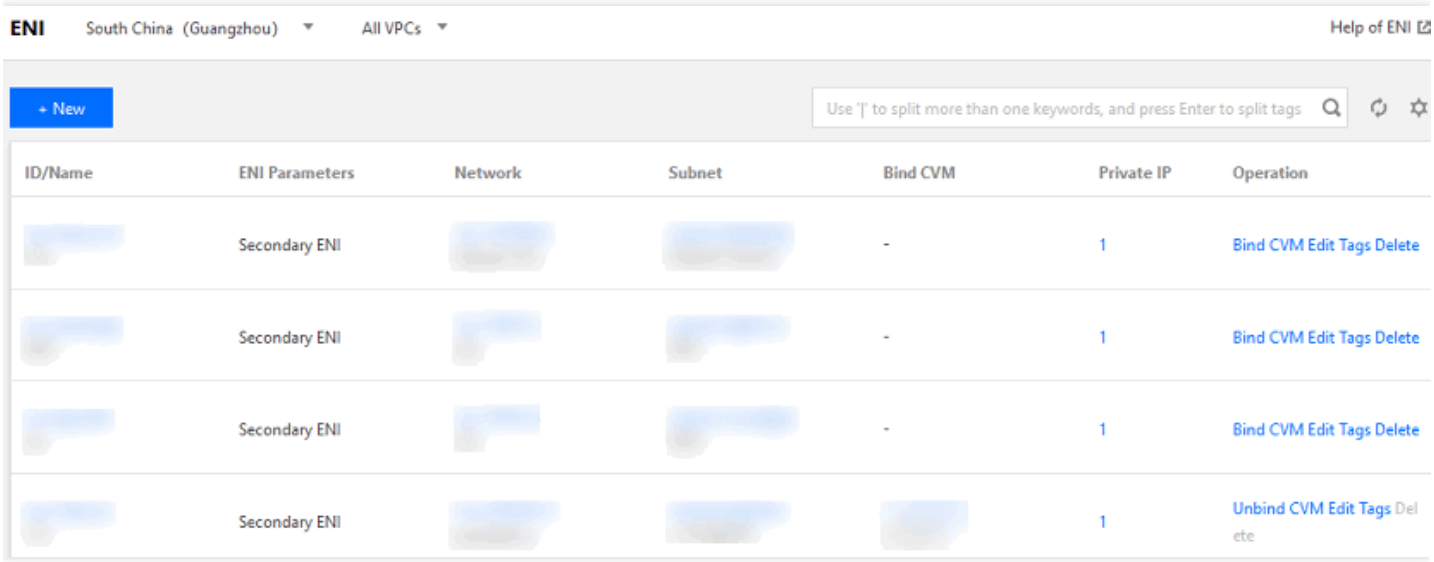
Elastic Network Interface (ENI) refers to the type of virtual network interfaces that can be bound to CVM instances in VPCs. An ENI can be migrated freely between CVM instances within the same VPC and AZ, helping you easily build high-availability clusters, implement low-cost failover, and manage networks in a more refined manner.
CLB real servers can be bound to both CVM and ENI. Specifically, a CLB instance communicates with the real server over the private network, and if multiple CVM instances and ENIs are bound to the CLB instance, access traffic will be forwarded to the private IPs of the CVM instances and ENIs.

> The ENI binding feature of CLB is currently in beta test. If you want to use it, please submit a ticket for application.

Prerequisites

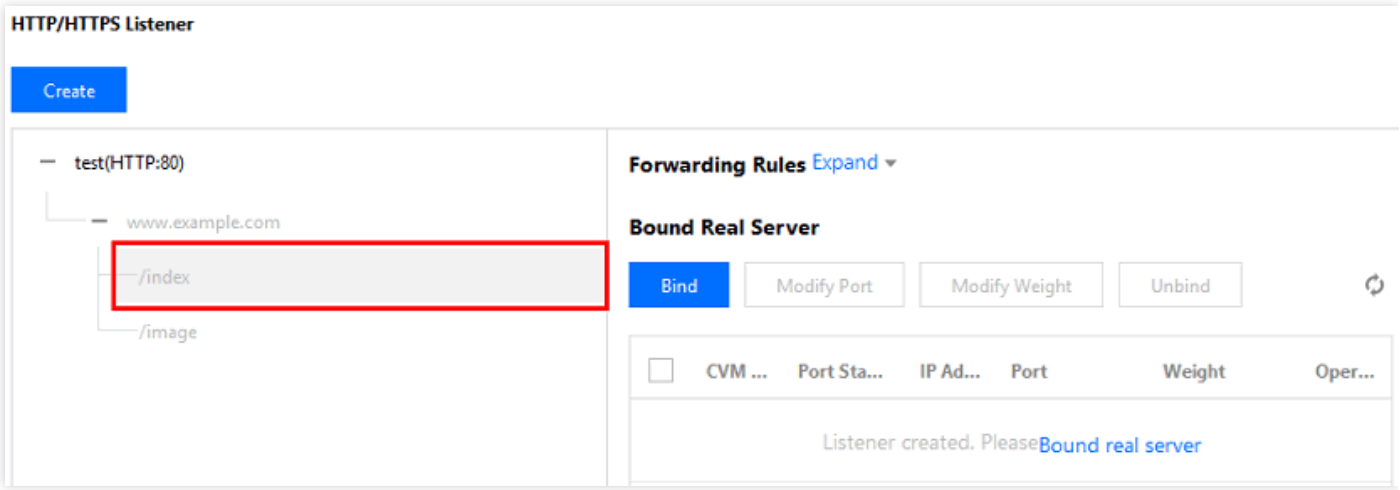
An ENI must be bound to a CVM instance first before it can be bound to a CLB instance. As a CLB instance only forwards traffic as a load balancer but does not process the business logic, the CVM instance, as a computing resource, is needed to process user requests. Please log in to the ENI

Console to bind the required ENI to the CVM instance first.



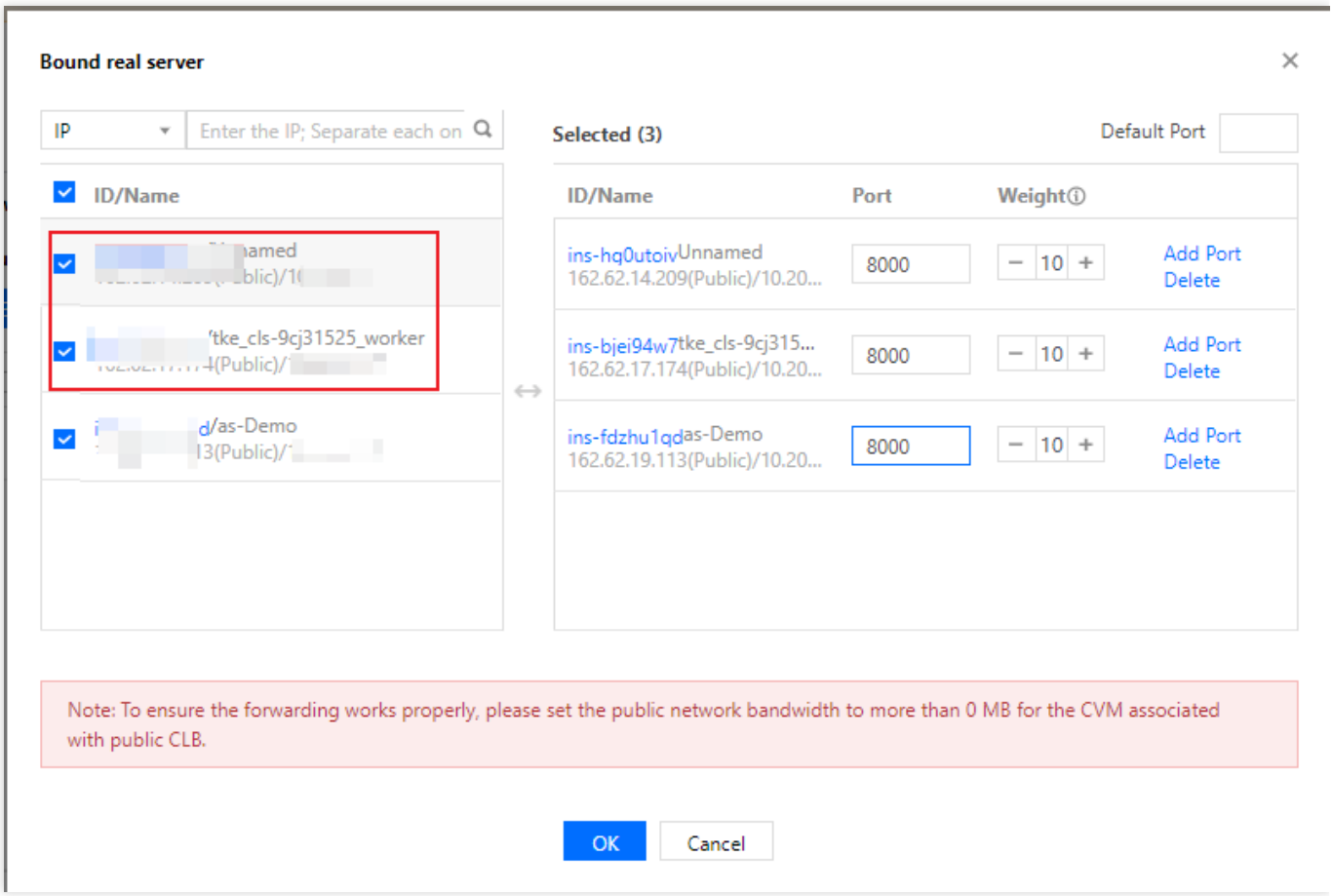
Directions

1. You need to configure a CLB listener first. For more information, please see CLB Listener Overview.
2. Click + on the left of the created listener to expand the domain names and URL paths, select the desired URL path, and view the existing real server bound on the right of the listener.

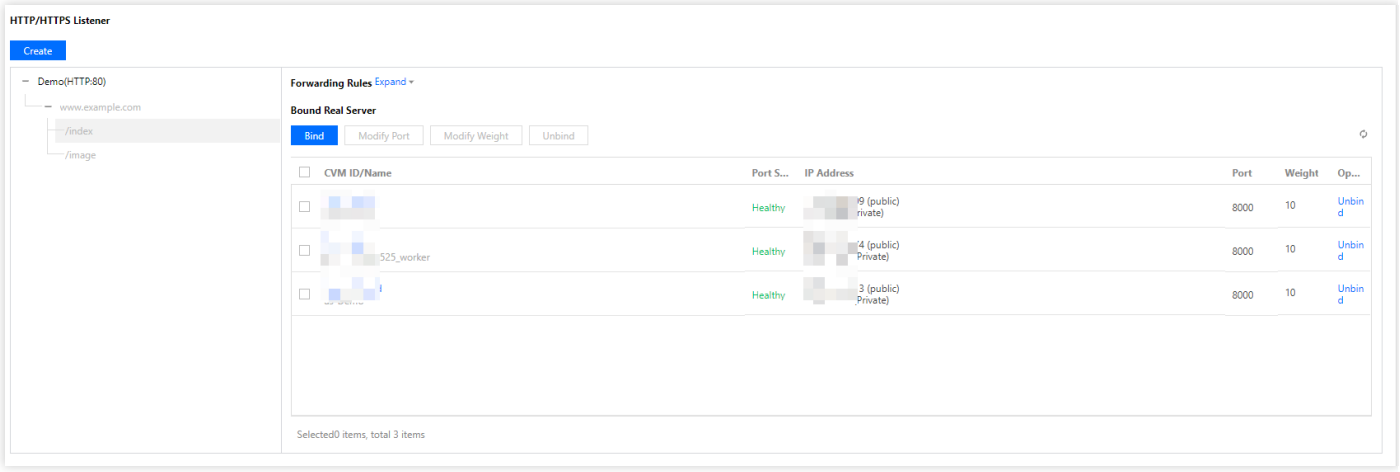


3. Click **Bind** and select the real server to be bound and configure the server port and weight in the pop-up window. You can select "CVM" or "ENI" as the real server.
   - CVM: you can bind the primary private IPs of primary ENIs of all CVM instances in the same VPC as the CLB instance.
   - ENI: you can bind all ENI IPs in the same VPC as the CLB instance except the primary private IPs of primary ENIs of CVM instances, such as secondary private IPs of primary ENIs and private IPs

of secondary ENIs. For more information on the types of ENI IPs, please see ENI - Key Concepts.



4. The specific configuration after binding is as shown below:



Hybrid Cloud Deployment

Last updated : 2020-11-13 10:36:46

In hybrid cloud deployment scenarios, you can directly bind a CLB instance to IPs in the local IDC off the cloud so as to bind it to real servers across VPCs and IDCs.
This feature is currently in beta test. For cross-region binding in Mainland China, please submit a ticket for application. For cross-region binding outside Mainland China, please contact your Tencent Cloud rep.

Scheme Advantages

- A hybrid cloud can be built quickly to seamlessly connect the environments in and off the cloud. CLB can forward requests to CVM instances in the in-cloud VPC and the off-cloud IDC at the same time.
- The high-quality public network access capabilities of Tencent Cloud can be reused.
- The rich features of CLB such as layer-4/7 access, health check, and session persistence can be reused.
- The private networks can be interconnected with each other through CCN, fine-grained routing is supported to guarantee the quality, and diversified tiered pricing is supported to reduce the costs.

Limits

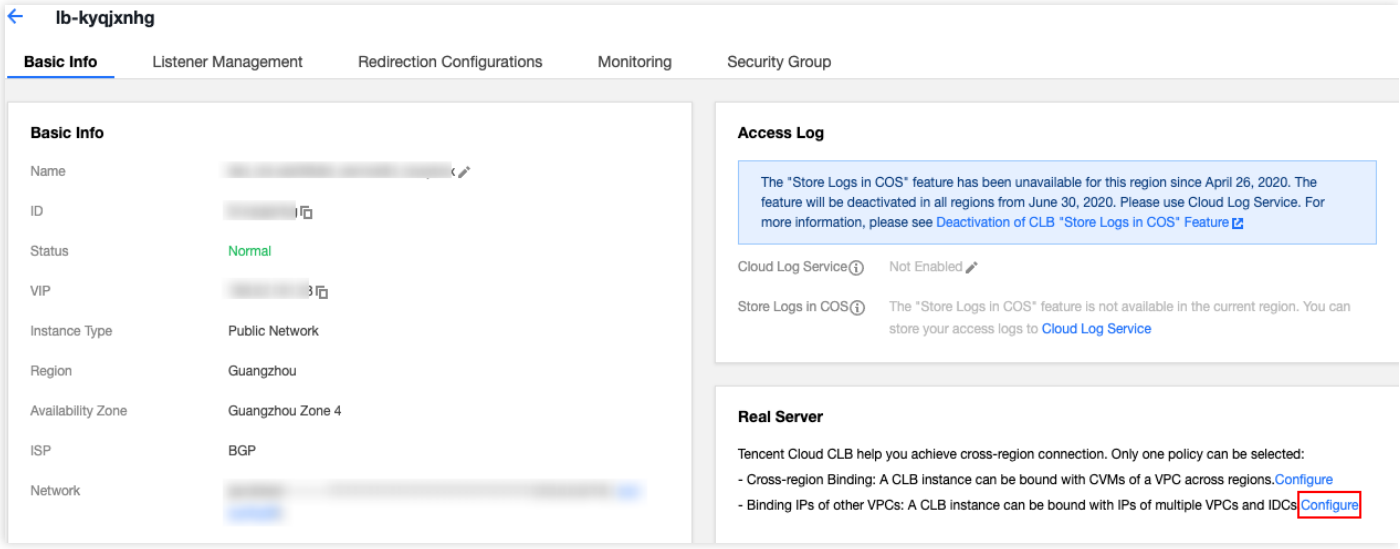
- Cross-network CVM instance binding is currently not supported for private network CLB and classic CLB.
- This feature is available only to standard accounts. You can determine the account type as instructed in Checking Account Type.
- Currently, this feature is supported only in the Beijing, Shanghai, Guangzhou, Chengdu, Chongqing, and Hong Kong (China) regions.
- TCP and TCP SSL listeners need to use TOA on the real server to get the source IP. For more information, please see Loading TOA Module.
- HTTP and HTTPS listeners need to use X-Forwarded-For (XFF) to get the source IP.
- UDP listeners cannot get the source IP.

Prerequisites

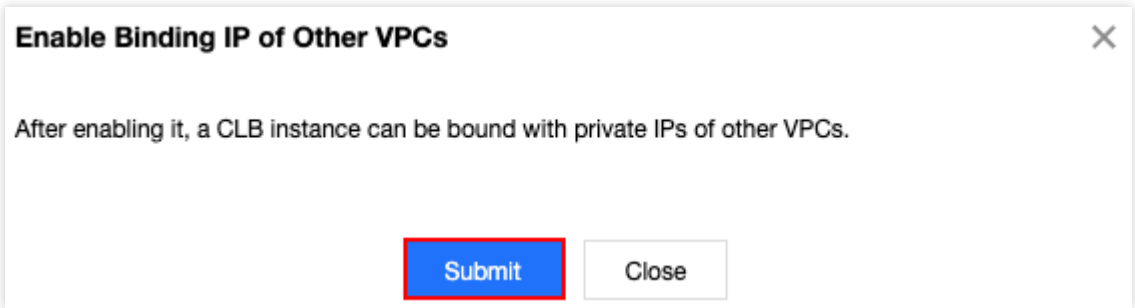
1. You have submitted the application for beta test eligibility. For cross-region binding in Mainland China, please submit a ticket for application. For cross-region binding outside Mainland China, please contact your Tencent Cloud rep.
2. You have created a CLB instance. For more information, please see Creating CLB Instances.
3. You have created a CCN instance. For more information, please see Creating a CCN Instance.
4. You have associated the Direct Connect gateway associated with the IDC and the target VPC to be bound with the created CCN instance. For more information, please see Associating Network Instances.

Directions

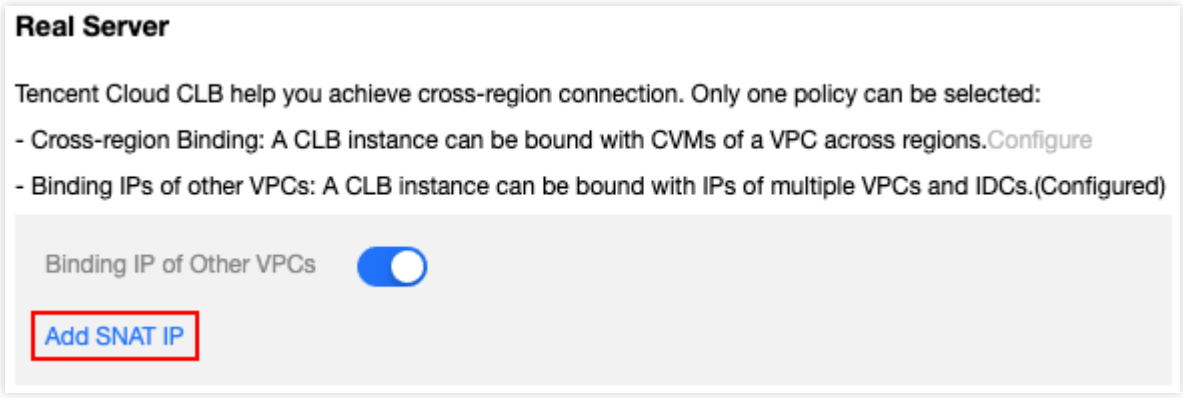
1. Log in to the CLB Console.
2. On the "Instance Management" page in the CLB Console, click the ID of the target CLB instance.
3. In the "Real Server" section on the "Basic Info" page, click **Configure** to bind a private IP not in the current VPC.



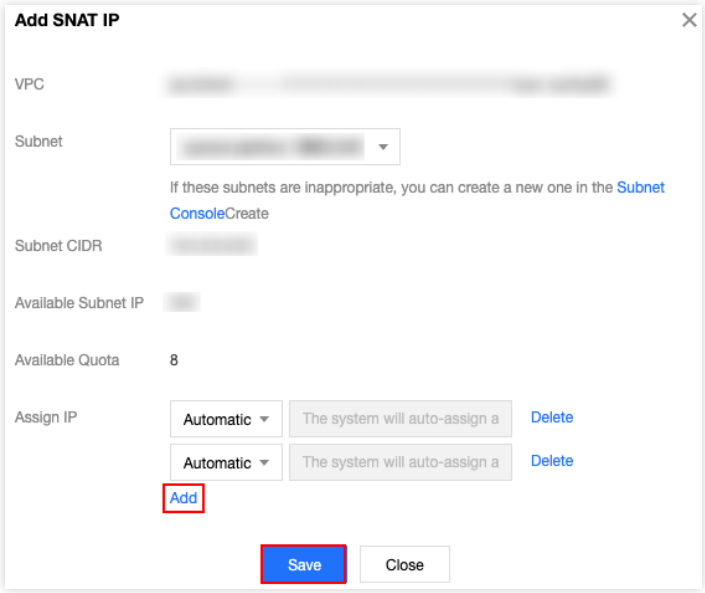
4. In the "Enable IP Not in Current VPC" dialog box that pops up, click **Submit**.



5. In the "Real Server" section on the "Basic Info" page, click **Add SNAT IP**.



6. In the "Add SNAT IP" dialog box that pops up, select "Subnet", click **Add** to assign an IP, and click **Save**.



7. On the instance details page, click the "Listener Management" tab and bind a real server to the CLB instance in the "Configure Listener" section. For more information, please see Adding real server to CLB instance.
8. In the "Bind Real Server" dialog box that pops up, select "Other Private IPs", click **Add Private IP**, enter the IDC private IP address to be bound, port, and weight, and click **OK**. For more information, please see Common Server Ports.
9. Return to the "Bound Real Servers" section and you can view the bound IDC private IP.

Cross-region Binding v2.0 (New)

Last updated : 2020-11-13 14:05:03

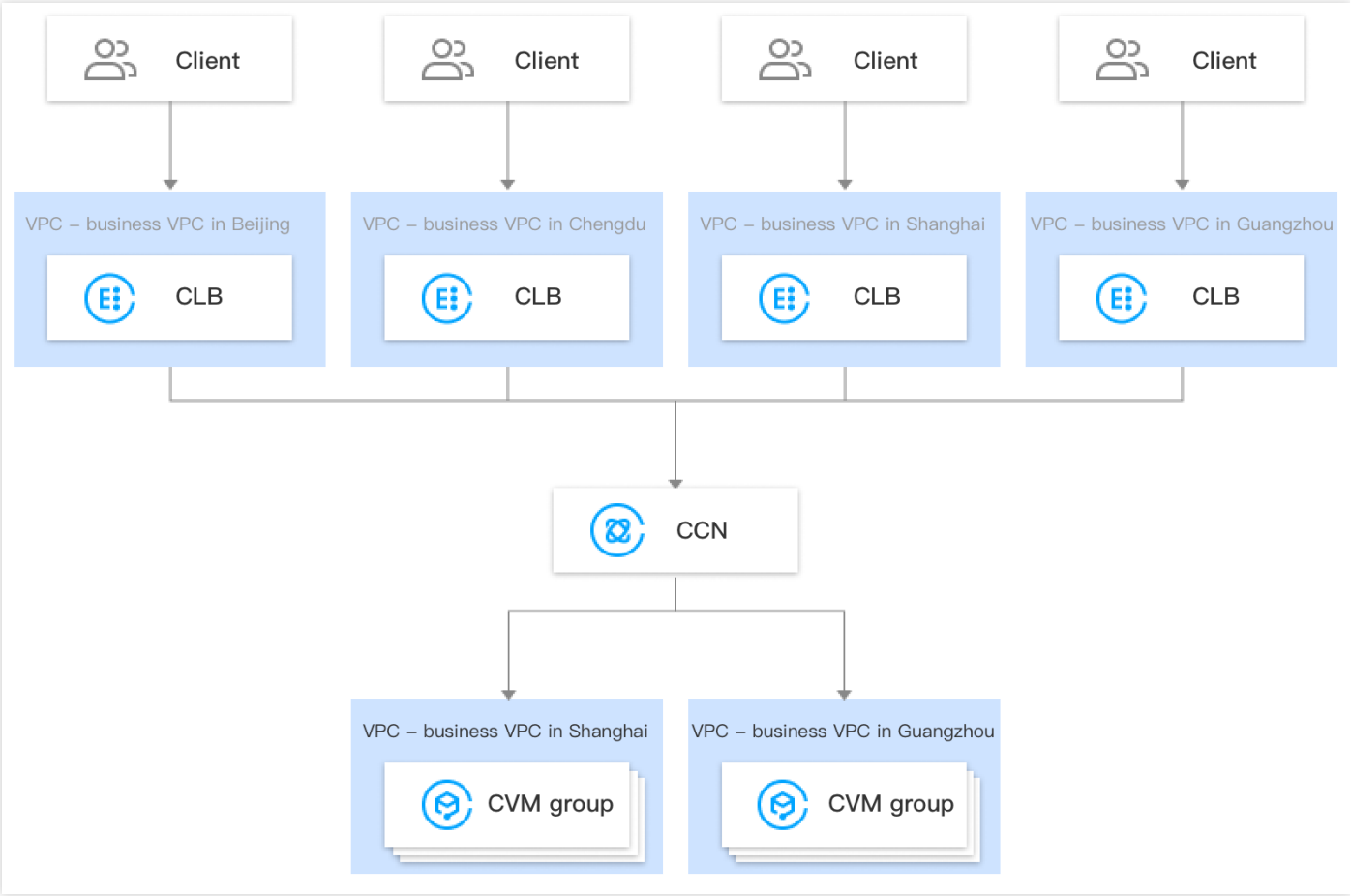
CLB can be bound to CVM instances in different regions through CCN. You can select multiple regions of real servers for cross-VPC and cross-region binding.
This feature is currently in beta test. For cross-region binding in Mainland China, please submit a ticket for application. For cross-region binding outside Mainland China, please contact your Tencent Cloud rep.

Note :

- Cross-region CVM instance binding is currently not supported for classic CLB.
- This feature is available only to standard accounts. You can determine the account type as instructed in Checking Account Type.

Use Cases

1. This feature can meet the needs in unified cross-region server scenarios for gaming businesses such as P2P. For example, if your real server cluster is deployed in Guangzhou, you can create CLB instances in Shanghai and Beijing and bind them to the same real server cluster in Guangzhou for game acceleration and traffic convergence, effectively ensuring the quality of data transfer and reducing the latency.
2. This feature can meet the needs in financial business and payment scenarios by effectively ensuring the transfer quality and consistency of data in key businesses.



Differences from Legacy Cross-region Binding

Comparison Item	Cross-region Binding v2.0 (New)	Cross-region Binding v1.0 (Legacy)
Whether binding to services in multiple regions at the same time is supported	Yes: • On the new version, a CLB instance can be bound to CVM instances in multiple regions at the same time. • For example, a CLB instance in the Beijing region can be bound to CVM instances in the Beijing and Shanghai regions at the same time.	No: • On the legacy version, a CLB instance can be bound to CVM instances in only one region. • For example, a CLB instance in the Beijing region can be bound to CVM instances in the Shanghai region but cannot be bound to those in the Beijing and Shanghai regions at the same time.
Whether intra-	Yes:	No:

region binding can be switched back after cross-region binding is used	• On the new version, the original intra-region binding can be switched back after cross-region binding is used.	• On the legacy version, after the real server region attribute is modified during cross-region binding, if the new region is different from that of the CLB instance, you cannot change back to the original intra-region binding.
Supported CLB types	Public network CLB and private network CLB.	Public network CLB.
Whether CLB is automatically unbound when a CVM instance is released	Automatic unbinding if CVM and CLB are in the same region: • If a CLB instance is bound to a CVM instance in the same region, when the CVM instance is released, the CLB instance will be automatically unbound from it. Automatic unbinding if CVM and CLB are in different regions: • If a CLB instance is bound to a CVM instance in another region, when the CVM instance is released, the CLB instance will not be automatically unbound from it, and you need to unbind them manually.	Automatic unbinding if CVM and CLB are in the same region: • If a CLB instance is bound to a CVM instance in the same region, when the CVM instance is released, the CLB instance will be automatically unbound from it. Automatic unbinding if CVM and CLB are in different regions: • If a CLB instance is bound to a CVM instance in another region, when the CVM instance is released, the CLB instance will not be automatically unbound from it.
Whether the price is favorable	It is billed in CCN. The costs are controlled in a fine-grained manner, which leads to lower prices.	-

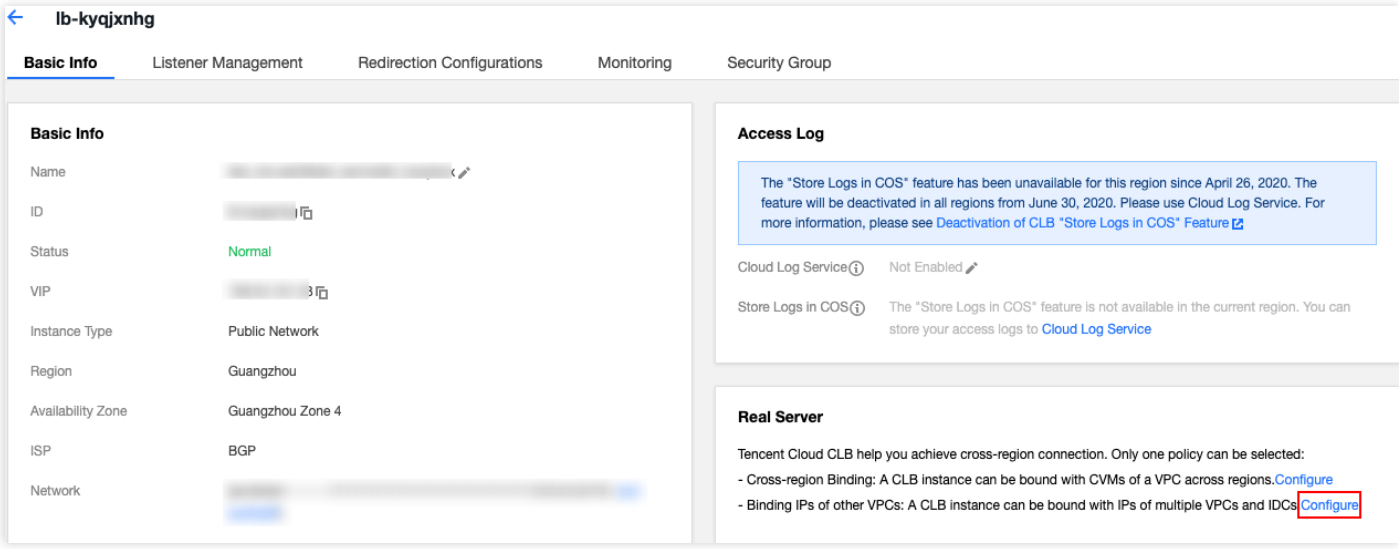
Prerequisites

1. You have submitted the application for beta test eligibility. For cross-region binding in Mainland China, please submit a ticket for application. For cross-region binding outside Mainland China, please contact your Tencent Cloud rep.
2. You have created a CLB instance. For more information, please see Creating CLB Instances.
3. You have created a CCN instance. For more information, please see Creating a CCN Instance.

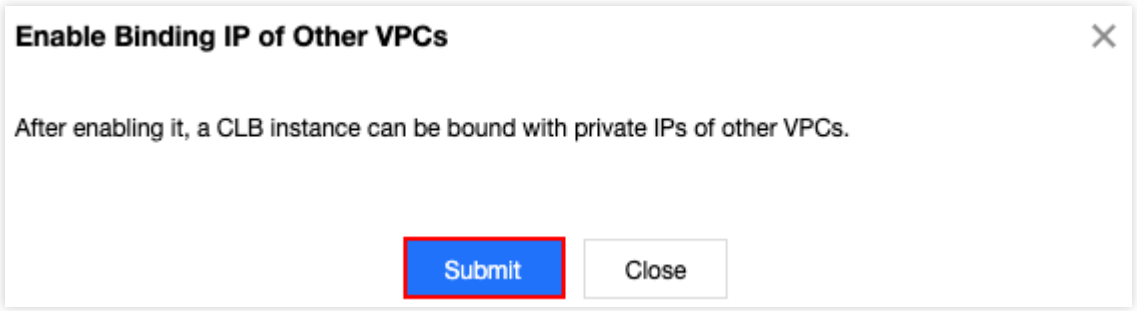
4. You have associated the target VPC to be bound with the created CCN instance. For more information, please see Associating Network Instances.

Directions

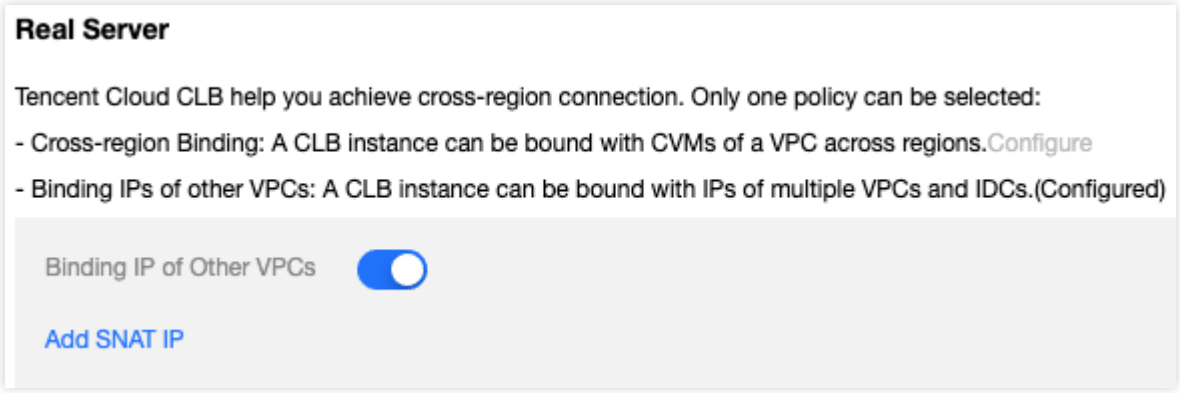
1. Log in to the CLB Console.
2. On the instance details page, click the ID of the target CLB instance.
3. In the "Real Server" section on the "Basic Info" page, click **Configure** to bind a private IP not in the current VPC.



4. In the "Enable IP Not in Current VPC" dialog box that pops up, click **Submit**.



5. In the "Real Server" section on the "Basic Info" page, you can see that "Enable IP Not in Current VPC" is enabled, which indicates that in-cloud IPs can be bound to.



6. On the instance details page, click the "Listener Management" tab and bind a real server to the CLB instance in the "Configure Listener" section. For more information, please see Adding real server to CLB instance.
7. In the "Bind Real Server" dialog box that pops up, select "Other VPCs", click **CVM**, select one or multiple CVM instances to be associated with, enter the port and weight, and click **OK**. For more information, please see Common Server Ports.
8. Return to the "Bound Real Servers" section and you can view the bound CVM instances in other regions.

Adding, Modifying, and Unbinding a Real Server

Last updated : 2020-10-10 14:24:08

CLB routes requests to real server instances that are running normally. This document describes how to add or delete real servers as needed or when you use CLB for the first time.

Prerequisites

You have created a CLB instance and configured a listener. For more information, please see Getting Started with CLB.

Directions

Adding real server to CLB instance

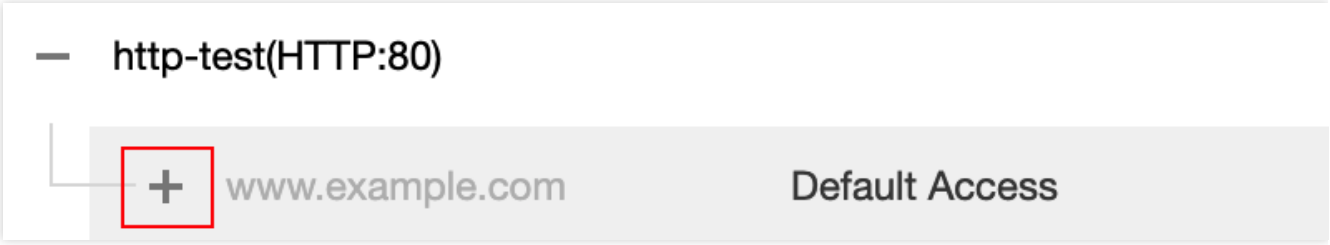
Note :

- If a CLB instance is associated with an auto scaling group, CVM instances in the group will be automatically added to the real servers of the CLB instance. When a CVM instance is removed from the auto scaling group, it will be automatically deleted from the real servers of the CLB instance.
- If you need to use API to add real servers, please see the RegisterInstancesWithLoadBalancer API.

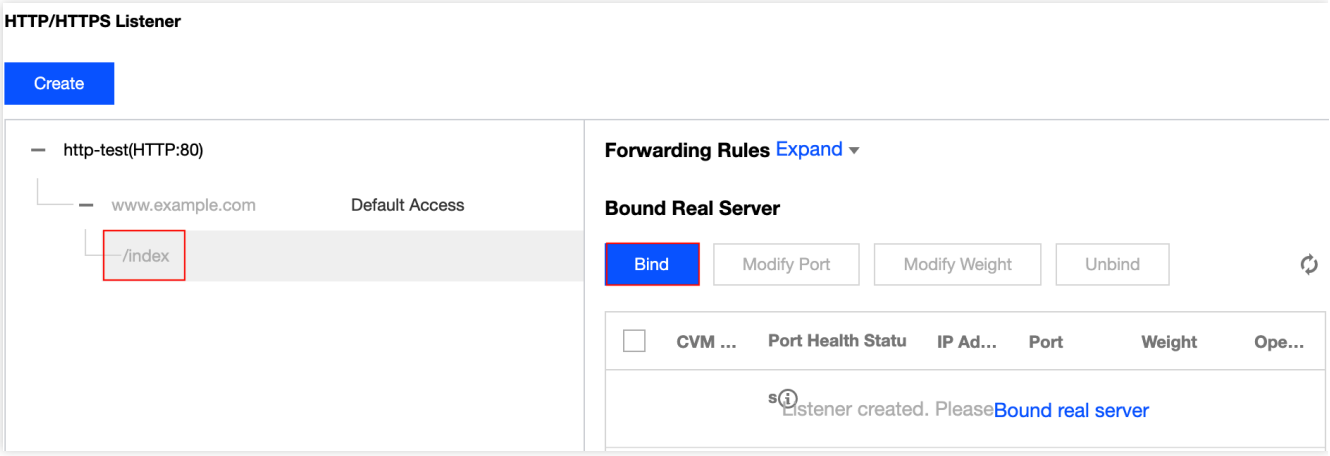
1. Log in to the CLB Console.
2. On the "Cloud Load Balancer" tab of the "Instance Management" page, click **Configure Listener** in the "Operation" column on the right of the target CLB instance.
3. In the listener configuration module, select the listener to be bound to a real server.
   - **HTTP/HTTPS Listener**

a. In the HTTP/HTTPS listener area, click "+" on the left of the target listener.

b. Click "+" on the left of the expanded domain name.



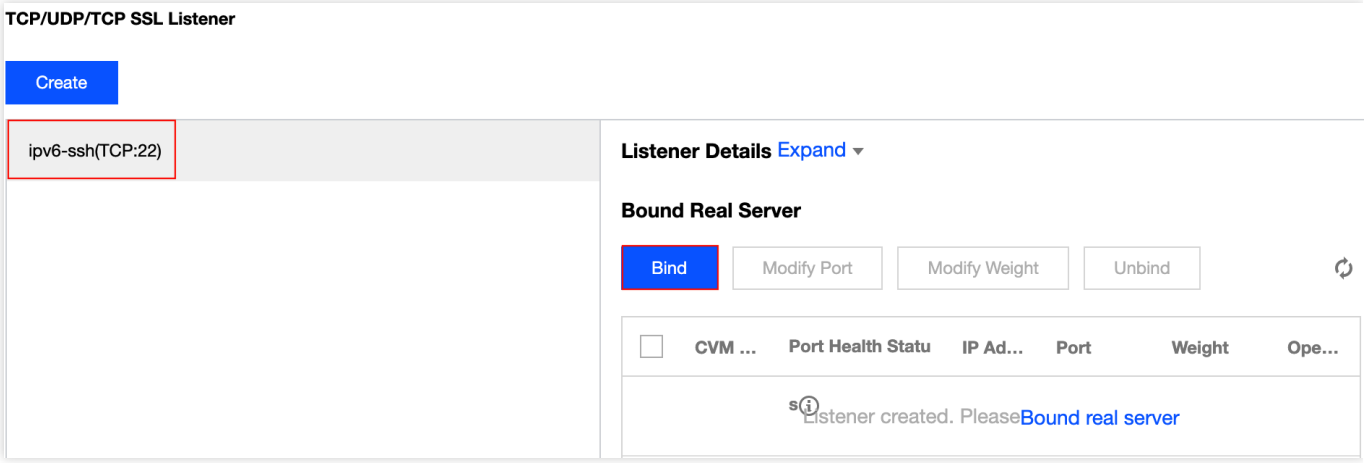
c. Select the expanded URL path and click **Bind**.



- **TCP/UDP/TCP SSL listener**

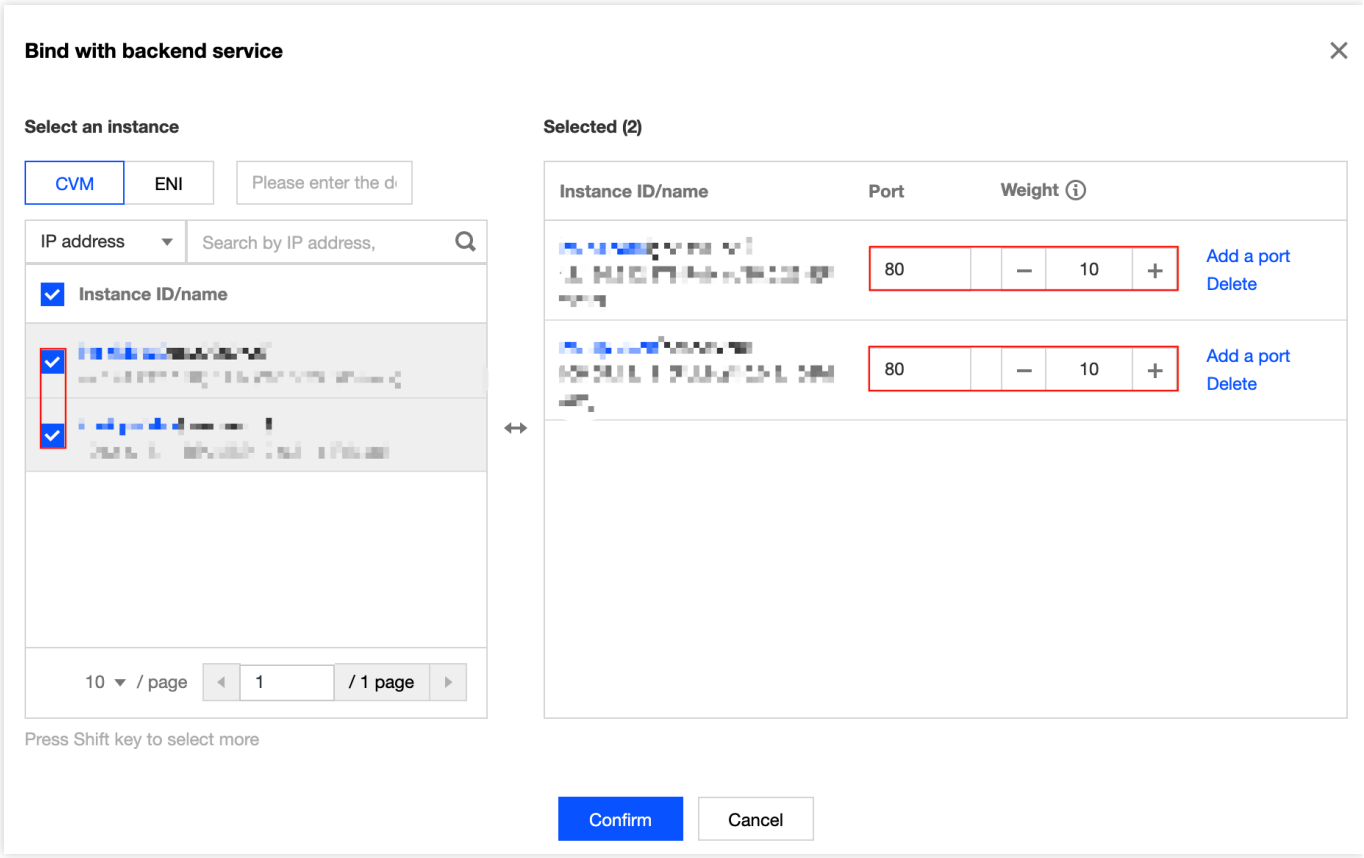
  In the list on the left of the TCP/UDP/TCP SSL listener module, select the listener to be bound to

a real server and click **Bind**.



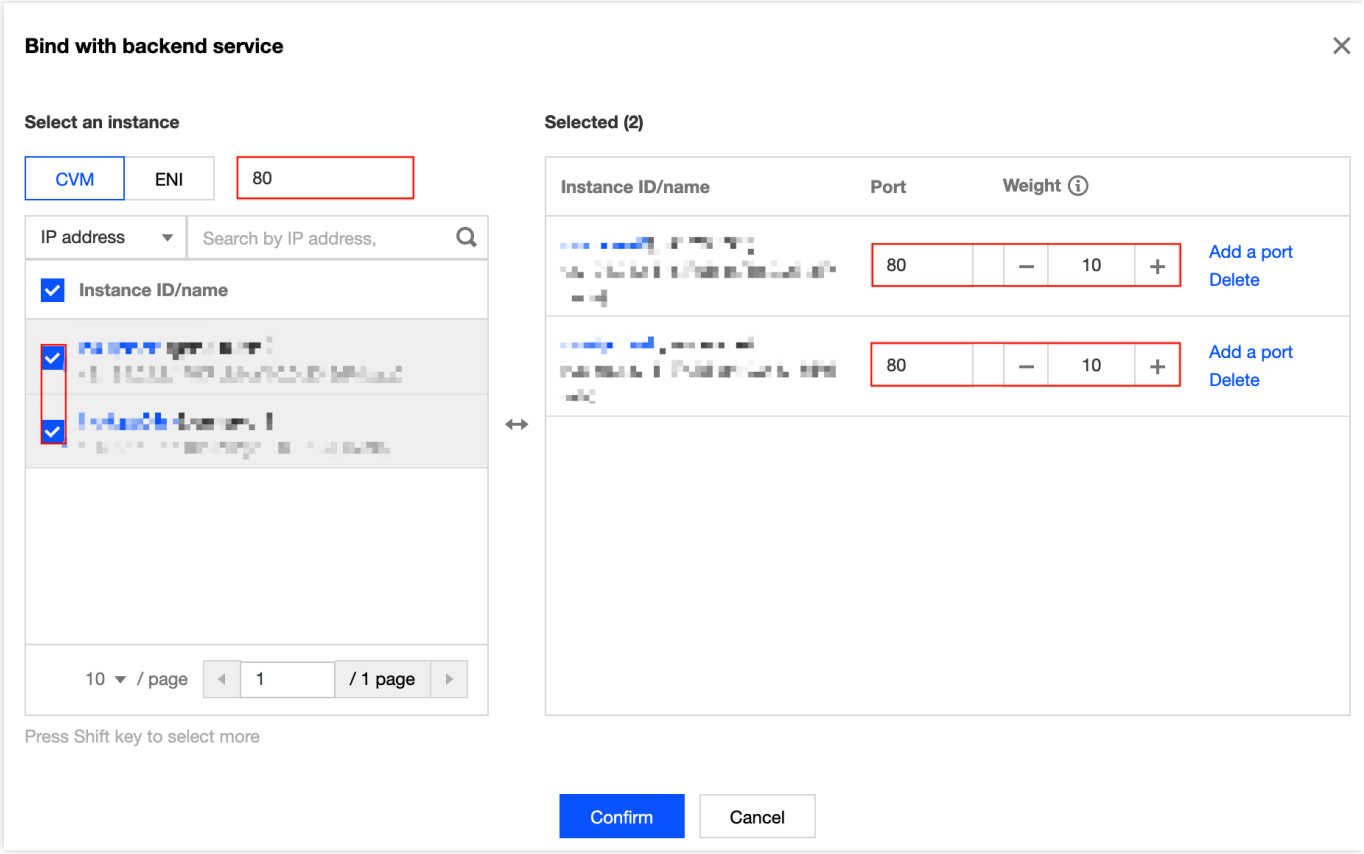
4. Bind a real server to the CLB instance.
   - **Method 1**. In the "Bind Real Server" pop-up window, click **CVM**, select one or multiple CVM instances to be associated with, enter the port and weight, and click **OK**. For more information, please see Common Server Ports.

> **Note :**
>
> - The "Bind Real Server" pop-up window only displays available CVM instances in the same region and same network environment that are not isolated and have not expired with peak bandwidth greater than 0.
> - When multiple real servers are bound, CLB will forward traffic according to the hash algorithm to balance the load.
> - The greater the weight of a server, the more the requests forwarded to it. The default value is 10, and the configurable value range is 0–100. If the weight is set to 0, the server will not accept new requests. If session persistence is enabled, it may cause uneven request distribution among real servers. For more information, please see Algorithms and Weight Configuration.



- **Method 2**. If you need to bind servers in batches with the same preset port value, you can click **CVM** in the "Bind Real Server" pop-up window, enter the default port value (for more information on port selection, please see Common Server Ports), check the target servers, set

the weight value, and click **OK**.



Modifying real server weight for CLB instance

The real server weight determines the number of CVM requests to be forwarded. When binding a real server, you need to preset its weight. The following describes how to modify the real server weight with "HTTP/HTTPS listeners" as an example (which can be modified for TCP/UDP/TCP SSL listeners in the same way).

Note :

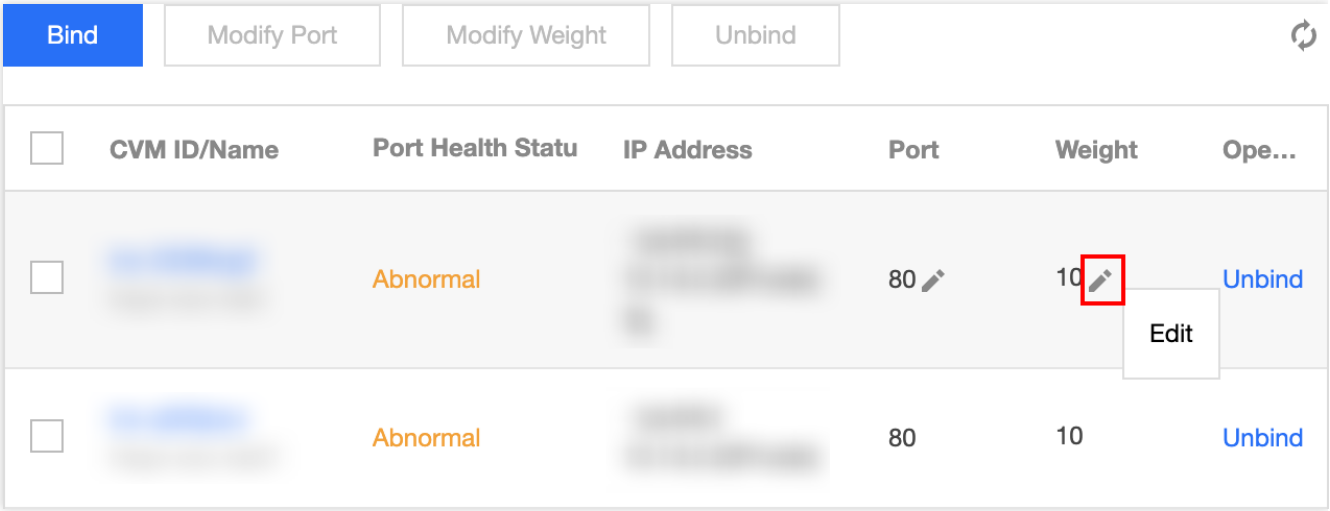
- If you need to use an API to modify real server weights, please see the ModifyLoadBalancerBackends API.
- For more information on CLB real server weight, please see CLB Polling Method.

1. Log in to the CLB Console.
2. On the "Cloud Load Balancer" tab of the "Instance Management" page, click **Configure Listener** in the "Operation" column on the right of the target CLB instance.
3. In the list on the left of the HTTP/HTTPS listener module, expand the instances and listener rules, and select a URL path.

4. In the server list on the right of the HTTP/HTTPS listener module, modify the relevant server weight.

> **Note :**
>
> The greater the weight of a server, the more the requests forwarded to it. The default value is 10, and the configurable value range is 0–100. If the weight is set to 0, the server will not accept new requests. If session persistence is enabled, it may cause uneven request distribution among real servers. For more information, please see Algorithms and Weight Configuration.

- **Method 1**. Modify the weight of one single server.
  a. Find the server whose weight needs to be modified, hover over the corresponding weight, and click .

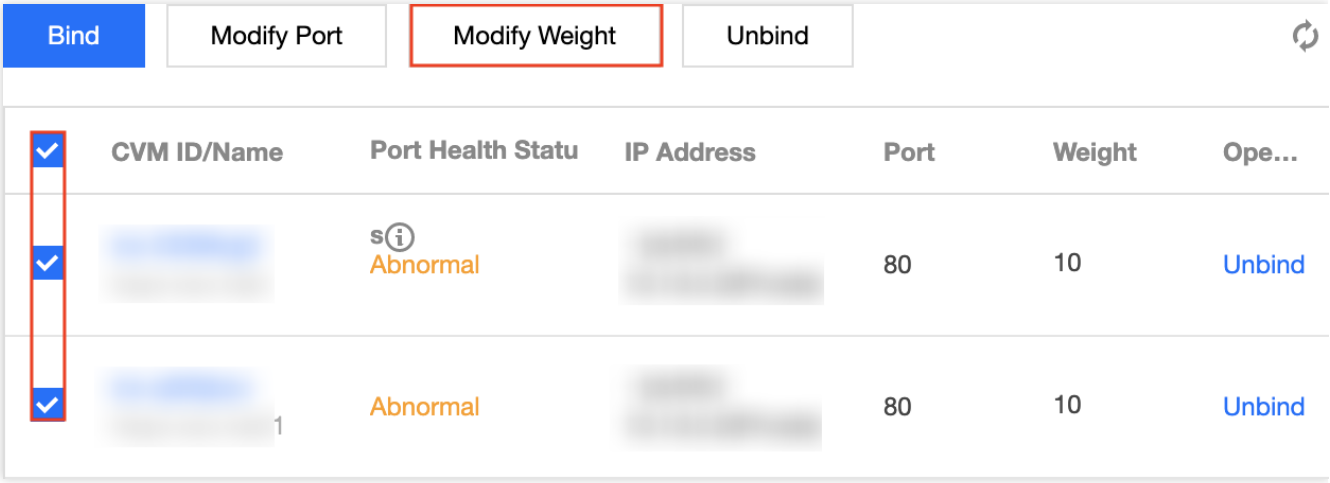


  b. In the "Modify Weight" pop-up window, enter the new weight value and click **Submit**.
- **Method 2**. Modify the weight of multiple servers in batches.

Note :

After the batch modification, the servers will have the same weight.

a. Click the checkbox in front of the servers, select multiple servers, and click **Modify Weight** at the top of the list.



b. In the "Modify Weight" pop-up window, enter the new weight value and click **Submit**.

Modifying real server port for CLB instance

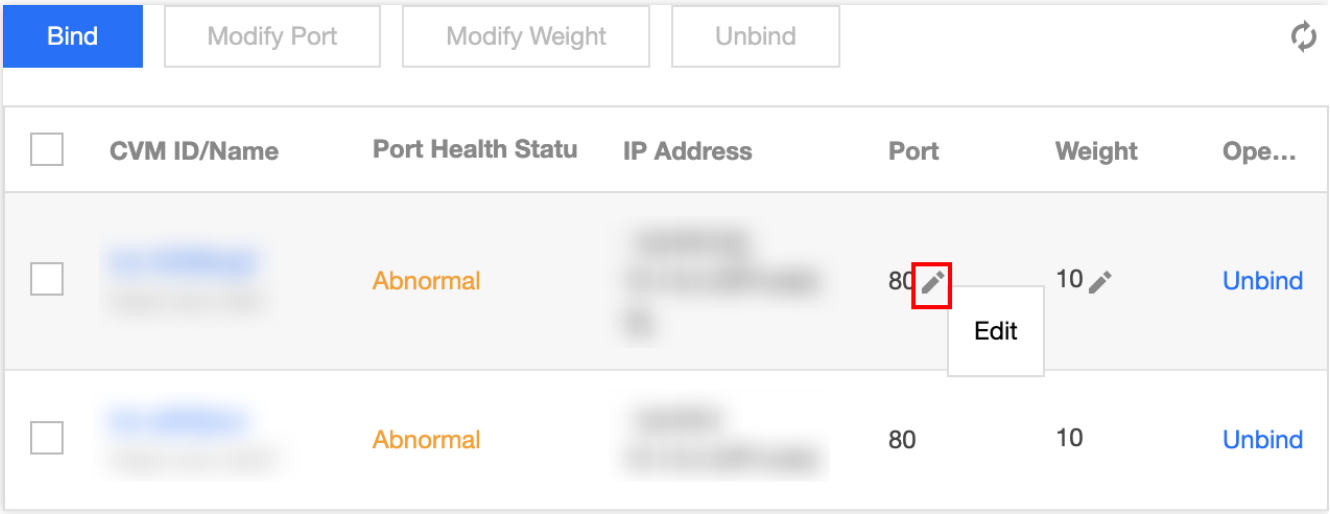
You can modify the real server port in the CLB Console. The following describes how to modify the real server weight with "HTTP/HTTPS listeners" as an example (which can be modified for TCP/UDP/TCP SSL listeners in the same way).

Note :

If you need to use API to modify real server ports, please see the ModifyTargetPort API.

1. Log in to the CLB Console.
2. On the "Cloud Load Balancer" tab of the "Instance Management" page, click **Configure Listener** in the "Operation" column on the right of the target CLB instance.
3. In the list on the left of the HTTP/HTTPS listener module, expand the instances and listener rules, and select a URL path.

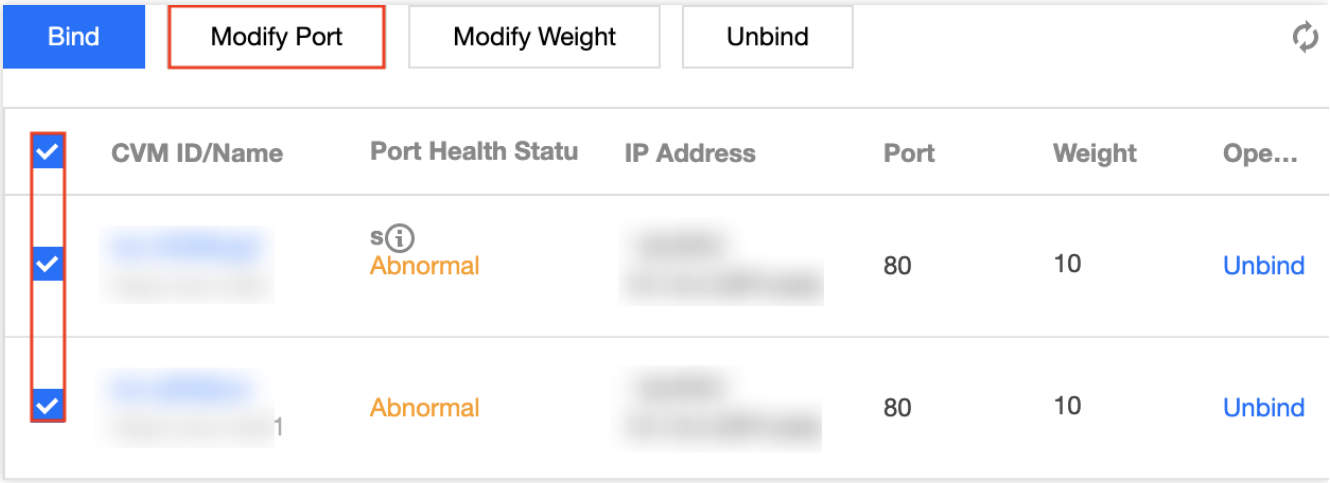
4. In the server list on the right of the HTTP/HTTPS listener module, modify the relevant server port. For more information on port selection, please see Common Server Ports.
   - **Method 1**. Modify the port of one single server.
     a. Find the server whose port needs to be modified, hover over the corresponding port, and click .



     b. In the "Modify Port" pop-up window, enter the new port value and click **Submit**.
   - **Method 2**. Modify the port of multiple servers in batches.

> **Note :**
>
> After the batch modification, the servers will have the same port.

     a. Click the checkbox in front of the servers, select multiple servers, and click **Modify Port** at the top of the list.



b. In the "Modify Port" pop-up window, enter the new port value and click **Submit**.

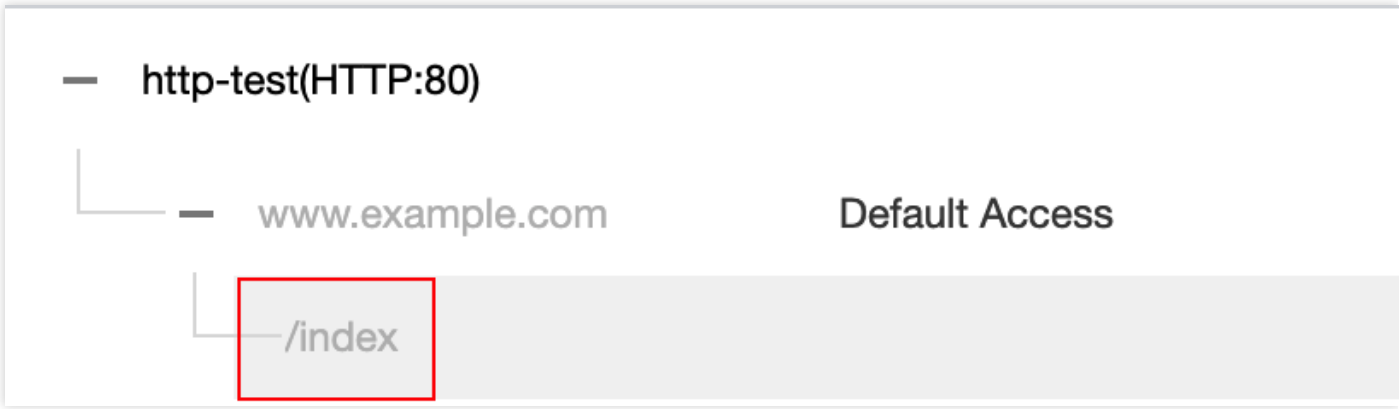
Unbinding real server from CLB instance

You can unbind bound real servers in the CLB Console. The following describes how to unbind bound real servers with "HTTP/HTTPS listeners" as an example (which can be unbound from TCP/UDP/TCP SSL listeners in the same way).

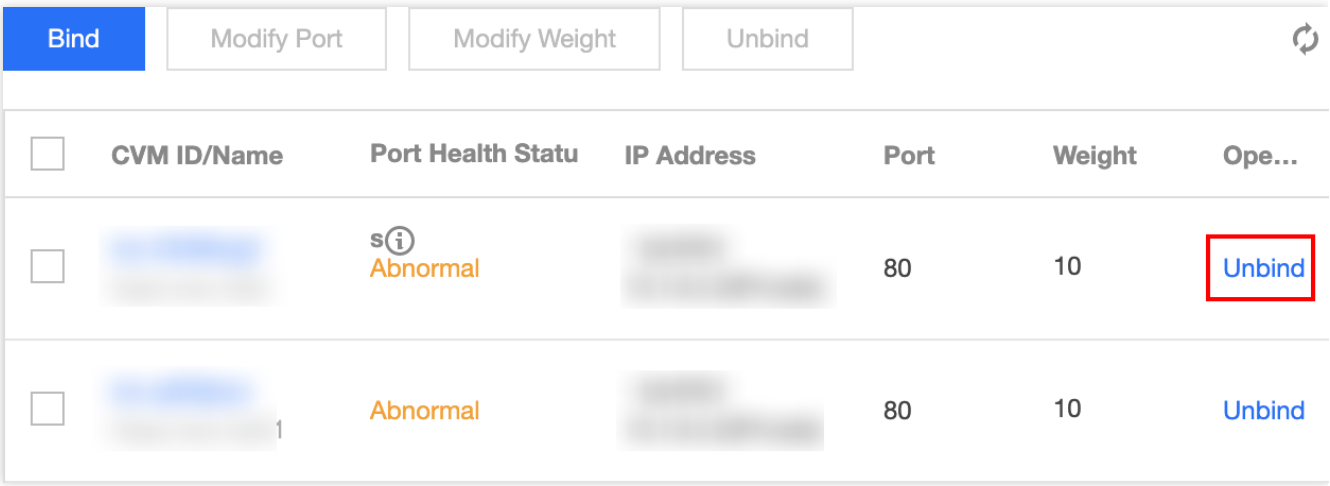
Note :

- Unbinding a real server will unbind the CLB instance from the CVM instance, and CLB will stop forwarding requests to it immediately.
- Unbinding a real server will not affect the lifecycle of your CVM instance, which can be added to the real server cluster again when necessary.
- If you need to use API to unbind real servers, please see the DeregisterTargets API.

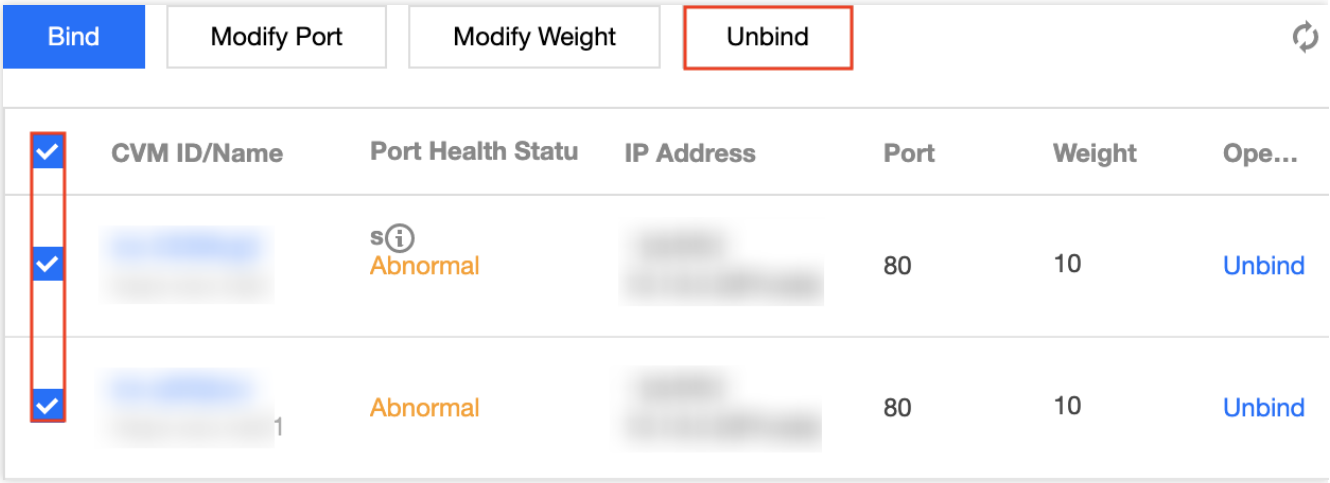
1. Log in to the CLB Console.
2. On the "Cloud Load Balancer" tab of the "Instance Management" page, click **Configure Listener** in the "Operation" column on the right of the target CLB instance.
3. In the list on the left of the HTTP/HTTPS listener module, expand the instances and listener rules, and select a URL path.



4. In the server list on the right of the HTTP/HTTPS listener module, unbind the bound real server.
   - **Method 1**. Unbind one single server.
     a. Find the server that needs to be unbound and click **Unbind** in the **Operation** column on the right.



     b. In the "Unbind" pop-up window, confirm the server to be unbound and click **Submit**.
   - **Method 2**. Unbind multiple servers in batches.
     a. Click the checkbox in front of the servers, select multiple servers, and click **Unbind** at the top of the list.



b. In the "Unbind" pop-up window, confirm the servers to be unbound and click **Submit**.

Security Group Configuration of the Real Server

Last updated : 2020-11-10 18:02:18

CVM Security Group Overview

A security group can be used for access control for real servers of CLB instances, which acts as a firewall.
You can associate one or more security groups with a real server and then add one or more rules to each security group to control the traffic access permissions of different servers. You can modify the rules of a security group at any time, and new rules will be automatically applied to all instances associated with the security group. For more information, please see Security Group Operation Guide. In the VPC environment, you can also use Network ACL for access control.

CVM Security Group Configuration Description

The client IP and service port need to be opened to the internet in the CVM security group.
If you want to use CLB to forward business traffic to CVM, the CVM security group should be configured as follows to ensure effective health checks:

1. Public network CLB: you need to open the CLB VIP to the internet on the backend CVM security group, so that CLB can use the VIP to detect the backend CVM health status.
2. Private network CLB:
   - For private network CLB (formerly "private network Application CLB"), if your CLB instance is in a VPC, the CLB VIP needs to be opened to the internet in the backend CVM security group for health checks; if your CLB instance is in the basic network, no additional configuration is needed as the health check IP is opened to the internet by default.
   - For private network classic CLB, if your CLB instance was created before December 5, 2016 and is in a VPC, the CLB VIP needs to be opened to the internet (for health checks) in the backend CVM security group; otherwise, no configuration is required.

CVM Security Group Configuration Samples

The following samples show you how to configure CVM security groups when accessing CVM through CLB. If you have also configured a security group on CLB, please see Configuring CLB Security Groups for more information on how to configure CLB security group rules.

- **Application scenario 1:**
  If a public network CLB instance is configured with a TCP:80 listener, the real server port is 8080, and you want only certain Client IPs (ClientA IP and ClientB IP) to access the CLB instance, then configure the security group inbound rules of the real server as follows:
  ```

  ClientA IP + 8080 allow
  ClientB IP + 8080 allow
  CLB VIP + 8080 allow

0.0.0.0/0 + 8080 drop

```
- **Application scenario 2:**
If a public network CLB instance is configured with a HTTP:80 listener, the real server port is 8080, and you want all Client IPs to access the CLB instance, then configure the security group inbound rules of the real server as follows:
```

0.0.0.0/0 + 8080 allow

```
- **Application scenario 3:**
For a private network CLB (formerly "private network Application CLB") instance, if the network type is VPC, the CVM security group needs to open the CLB VIP IP to the internet for health check, this CLB instance is configured with a TCP:80 listener, the real server port is 8080, and you want certain Client IPs (ClientA IP and ClientB IP) to access the CLB VIP and want the Client IPs to access only real servers bound to the CLB instance, then:
a. Configure the inbound rules for the real server security group as follows:
```

ClientA IP + 8080 allow
ClientB IP + 8080 allow
CLB VIP + 8080 allow
0.0.0.0/0 + 8080 drop

```
b. Configure the outbound rules for the client server security group as follows:
```

CLB VIP + 8080 allow
0.0.0.0/0 + 8080 drop

```
- **Application scenario 4:**
For a private network Classic CLB instance (i.e., a VPC CLB instance purchased after December 5, 2016), if the CVM security group only needs to open the Client IP to the internet (there is no ne
```
```

```
ed to open the CLB VIP, and the health check IP is opened by default), this CLB instance is confi
gured with a TCP:80 listener, the real server port is 8080, and you want certain Client IPs (Clie
ntA IP and ClientB IP) to access the CLB VIP and want the Client IPs to access only real servers
bound to the CLB instance, then:
a. Configure the inbound rules for the real server security group as follows:
```

ClientA IP + 8080 allow

ClientB IP + 8080 allow

0.0.0.0/0 + 8080 drop

```
b. Configure the outbound rules for the client server security group as follows:
```

CLB VIP + 8080 allow

0.0.0.0/0 + 8080 drop

```
- **Application scenario 5: blacklist**
If you need to configure a blacklist for some client IPs to deny their access requests, you can c
onfigure the security group associated with Tencent Cloud services. The security group rules need
to be configured as follows:
- Add the client IP and port to be rejected into the security group and select the option in the
"Policy" column to reject access from this IP.
- Add another security group rule after completing the above configuration to allow access reques
ts to the port from all IPs by default.
After the configuration is completed, the security group rules are as follows:
```

clientA IP + port drop

clientB IP + port drop

0.0.0.0/0 + port accept

```
>
>- The above configuration steps should be performed **in a correct order**; otherwise, the black
list configuration cannot take effect.
>- Security groups are stateful; therefore, the above configurations are used for **inbound rules
**, while outbound rules do not require special configuration.

## CVM Security Group Operation Guide
### Managing real server security group in console
1. Log in to the [CLB Console](https://console.cloud.tencent.com/loadbalance) and click the corre
sponding CLB instance ID to enter the CLB details page.
2. On the CVM page, click the corresponding real server ID to enter the CVM instance details pag
e.
3. Click the **Security Group** tab to bind/unbind the security group.

### Managing real server security group through TencentCloud API
For more information, please see [AssociateSecurityGroups](https://intl.cloud.tencent.com/documen
```

```
t/product/213/33265) and [DisassociateSecurityGroups](https://intl.cloud.tencent.com/document/pro
duct/213/33253).
```

CLB Instance Cross-Region Binding

Last updated : 2020-10-26 16:00:14

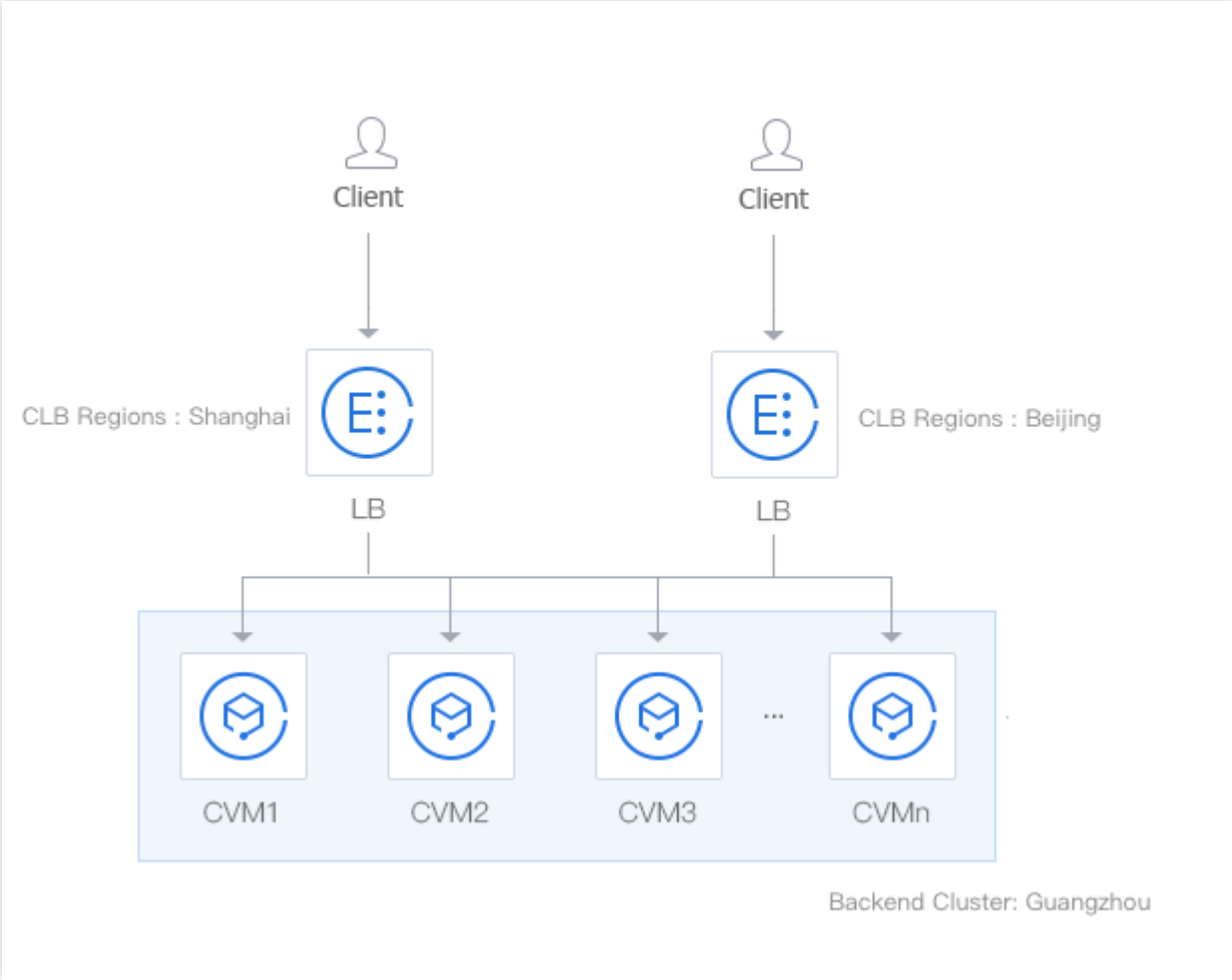
Currently, a public network CLB instance can be bound to CVM instances in another region. You can select CVM instances from the region where real servers resides and bind them across VPCs or regions. For cross-region binding in Chinese mainland, please submit a ticket. For cross-region binding outside Chinese mainland, please contact your Tencent Cloud rep.

Note :

Private network CLB and classic CLB currently are not available for cross-region CVM instance binding.

Use Cases

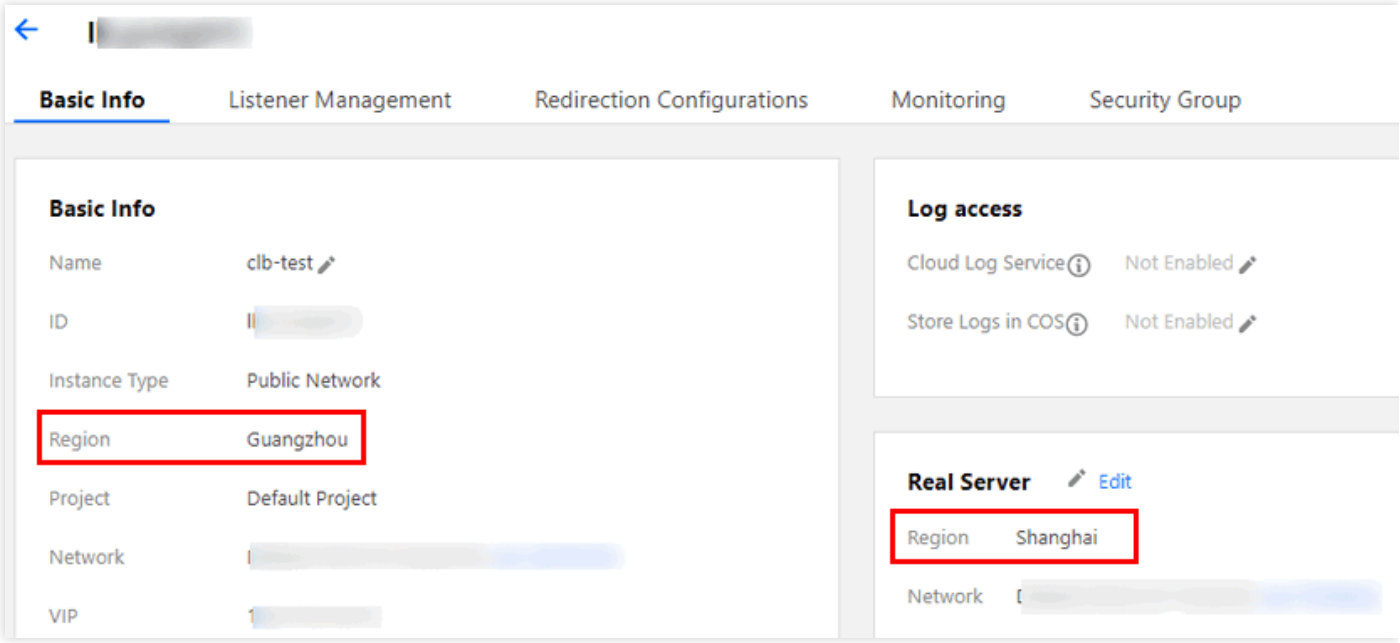
1. The cross-region binding feature can well meet the needs in P2P gaming scenarios where the same server is shared by players from different regions. For example, if your real server cluster is deployed in Guangzhou, you can create CLB instances in Shanghai and Beijing and bind them to the same real server cluster in Guangzhou to achieve game acceleration and traffic convergence, ensuring the data transfer quality and reducing the latency.
2. This feature can ensure the transfer quality and data consistency in key business transactions, meeting the stringent requirements of the financial industry and payment scenarios.



Directions

1. Log in to the CLB console.
2. Click the target CLB instance on the **Instance Management** page.
3. On the **Basic Info** page, click **Edit** next to **Real Server**, and modify the region and network attributes of the real server.

> **Note :**
>
> If a public network CLB instance has been bound to a CVM instance in the same region, unbind the CVM instance before switching the region. For more information, see Adding, Modifying, and Unbinding a Real Server.



4. In the pop-up window, select a region from the **Real Server Region** list and a network from the **Real Server Network** list, and click **Submit**.

Note :

- Currently, one CLB instance can be bound to CVM instances in only one region. For example, a CLB instance in Beijing can be bound to CVM instances in Shanghai, but cannot be bound to CVM instances in both Beijing and Shanghai.
- When the region of a real server has been modified, if the new region is different from that of the CLB instance, the change cannot be reverted.
- Currently, a CLB instance cannot be bound to CVM instances across VPCs in the same region.
- Classic network-VPC binding is supported.
- The bandwidth fee for cross-region binding will be settled daily, and the tiered pricing for bandwidth peak will be applied. For more information, see Cross-region Binding Billing.