Cloud Load Balancer
Product Introduction
Product Documentation
Copyright Notice

©2013-2019 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
  Introduction
  Advantages
  Use Cases
  Principles
  Restrictions
  Application and Conventional CLB comparison
What is Cloud Load Balancer?

Cloud Load Balancer is a traffic delivery service for multiple CVMs. Cloud load balancer can extend application systems' external service capabilities through traffic delivery and improve their availability by eliminating single point of failure.

The Cloud Load Balance service virtualizes multiple CVM resources located in the same region into a high-performance, high-availability application service pool by setting a virtual service address (VIP), and delivers the network requests from the client to the CVM pool in a way specified by the application.

Cloud Load Balance can check the health of CVMs in the CVM Pool, and automatically isolate abnormal CVMs, thus dealing with the single point of failure (SPOF) of a single CVM and improving the overall service capability of applications.

Tencent Cloud Load Balance provides self-management, self-troubleshooting, anti-network attacks and other advanced features for enterprises, communities, e-commerce, games and other user scenarios.

Components

A cloud load balancer group that provides services typically consists of the following components:

- CloudLoadBalancer: A cloud load balancer instance for traffic delivery
- VIP (virtual IP): An IP address through which the cloud load balancer provides service to the client
- Backend/Virtual Server: A group of cloud load balancer instances on the backend for processing requests
- VPC/Basic network: The overall network environment

Access requests from other servers other than cloud load balancer is delivered through the cloud load balancer instance to the backend CVM for processing according to the associated policies and forwarding rules.
Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Full Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Load Balancer</td>
<td>Cloud Load Balancer</td>
<td>A network cloud load balance service provided by Tencent Cloud that can be combined with CVM to offer cloud load balance service based on TCP/UDP and HTTP</td>
</tr>
<tr>
<td>Load Balance Listener</td>
<td>Load Balance Listener</td>
<td>Including listening port, load balance policy and health check configuration, each item to be listened corresponds to a back-end application service</td>
</tr>
<tr>
<td>Back-end Server</td>
<td>Real Server</td>
<td>A group of CVM instances that accept load balance delivery requests. The cloud load balancing service forwards access requests to this group of back-end CVMs according to user-defined rules</td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP</td>
<td>The service address assigned by the system, which currently is an IP address. You can choose whether to open it to the internet so as to create a private-network CLB instance or a public-network CLB instance</td>
</tr>
</tbody>
</table>

How Does Cloud Load Balancer Work?

Working Principle

The cloud load balancer accepts incoming traffic from the client and routes the request to a back-end CVM instance in one or more available zones for processing.

Cloud Load Balance service is mainly provided by cloud load balancer listener. The listener is responsible for monitoring requests on the cloud load balancer instance, delivering policies to back-end CVMs and other services. By configuring the forwarding protocols and protocol ports of "client-cloud load balancer" and "cloud load balancer-backend CVM", cloud load balancer can forward the request directly to the back-end CVM.

It is recommended that you configure a back-end CVM instance of the cloud load balancer across multiple available zones. If an available area becomes unavailable, the cloud load balancer routes the traffic to other available zones for normal operation, thereby shielding off the service interruption caused by a single available zone failure.

Request Routing Selection
The client requests to access the service through domain name. Before the request is sent to the cloud load balancer, the DNS server will resolve the load balancing domain name and return the requested CVM IP address to the client. When the cloud load listener is requested, a different cloud load balancing algorithm will be used to deliver the request to the back-end CVM. Tencent Cloud currently supports Weighted Round-Robin and ip_hash balancing algorithms. It will support the Weighted Least-Connection Scheduling in the future.

**Monitoring Back-end Service Status**

The cloud load balancer also monitors the running status of back-end instances, so as to ensure that traffic is only routed to the normal running instance. When the cloud load balancer detects an abnormal instance, it stops routing traffic to that instance until the instance is detected to return to normal again.

**Related Services**

Cloud Load Balance can be used with the following services to improve application availability and scalability:

- **CVM Instance**: enables the application to run on the cloud virtual server. For more information, refer to [CVM Product Documentation](#).
- **Auto Scaling**: Controls the number of instances flexibly. When a cloud load balancer instance is enabled in Auto Scaling, the scaled instance is automatically added to the cloud load balancing group, and the terminated instance is automatically moved out of the cloud load balancing group. For more information, see [Auto Scaling Product Documentation](#).
- **Cloud Monitor**: Helps you monitor the running status of cloud load balancer and all back-end instances and perform the operations accordingly. For more information, refer to [Cloud Monitor Product Documentation](#).
Advantages

The following indicators are used to evaluate the CLB service:

- **TPS (connection per second):** the number of TCP connections created by load balancer instance per second.
- **Maximum number of concurrent connections:** Number of concurrent connections refers to the number of concurrent TCP connections to the server requested by the client, or the total number of TCP connections to the server per second.
- **QPS (query per second):** or RPS, the number of queries/requests per second. The queries/requests refer to the GET/POST/HEAD packets sent by the client to the HTTP server after the establishment of connections.
- **Throughput:** The total traffic/bandwidth that the load balancer instance can support.

Tencent Cloud provides high-performance Cloud Load Balance services:

- A single cluster of CLB supports a maximum of over 120 million concurrent connections, and can easily deal with 100 million-level Web visits.
- A single cluster of CLB is capable of handling a peak traffic of 40Gb/s, with PPS up to 6 million.
- Strict isolation of traffic for each tenant, providing active DDoS protection. Tencent Cloud CLB provides you with the capability to defend against 2-10 Gb peak traffic of DDoS attack for free.

**Note:**

Defense service against DDoS attack with higher peak traffic can be purchased separately. The maximum defense capability provided is 300 GB.
The following is an example of a two-way hiding of (outbound public network access/public network access) backend server cluster:

Cloud server (VM2, VM3) does not have public IP, and cannot take the initiative to communicate with the public network.

- When CVM cluster needs to access the public network, the routing table is configured and NAT forwarding is performed through an Internet gateway (VM1). For resources on the Internet, the request address is always the public network IP (115.159.45.144) of Internet gateway, and the resources on the Internet are never exposed to the backend server cluster.
- When resources on the Internet access services on the CVM, the access must be conducted through a unified cloud load balance service VIP (115.159.17.247). The cloud load balancer is responsible for delivering all requests to the backend servers using a certain policy, and Internet is never exposed to the backend servers.

Cloud load balance can be applied primarily to the following scenarios:

- Scaling-out service capabilities of the application system, applicable to all kinds of web servers and app servers.
- Eliminating single point of failure on the application system. If a part of the CVM instances crash, the application system can still work properly.
Traffic Delivery

- By configuring cloud load balance virtual service address (VIP) and website domain name, multiple web access layer servers are virtualized into an access layer service pool with high performance and high availability. All public network requests go through CLB, providing security while saving public IP address resource.
- Cloud load balancer will ensure that requests are evenly forwarded to each access layer server, which can carry the load using inexpensive, similarly configured virtual machines or Docker containers.

Scale-out

- Cloud load balancer, combined with Autoscaling dynamic auto scaling group, allows you to automatically create and release CVM instances. The access layer web server can adjust accordingly as the access pressure of the public network increases/decreases.
In case of "double 11", "6.18" and other large-scale promotional activities of e-commerce vendors, web traffic may surge by 10 folds in an instant, and last for only a few hours. Using cloud load balance and Autoscaling can minimize IT cost.

Service Separation

- For typical web services such as forums, websites, etc., it is recommended to separate image services, text services and other different services, which will facilitate web development and iteration.
- After the services are separated, each cloud load balancer instance and its associated backend server group will act as a separate service cluster.
- You can perform CNAME switching at DNS service providers (such as DNSpod) in order to achieve domain name redirection between different services.
- Large websites usually have hundreds of sub service modules. You can use cloud load balance and DNS resolution to converge addresses for accessing portal home page into a cloud load balancer.
public network address and a proprietary domain. This will facilitate client access.
Principles

Underlying Implementation

Tencent cloud load balance (CLB) currently provides load balancing services on layer 4 and layer 7. Tencent gateway (TGW), the unified gateway product launched by Tencent, will provide cloud load balance feature, with high reliability, scalability, high performance, strong anti-attack capability and so on. It supports large-scale concurrent access and prevents malicious attacking traffic. The product forms of CLB include: cloud load balance capabilities, converging public network IP, anti DDoS attacks, QoS, FTP and SIP support, etc.

Cloud load balance is deployed in clusters to enable session synchronization to eliminate server single point failure, improve redundancy and ensure service stability. A number of data centers are deployed in the same region to achieve local disaster recovery.

This chapter mainly introduces several key technical points of CLB and chooses different dimensions (platform, resource, business) to analyze which technologies CLB employs to realize the ability of tenant isolation, architecture disaster recovery, resource disaster recovery and anti-attack capacities of cloud platform.

Note: In this document, RS refers to the CVM that is bound with CLB. VIP refers to the IP address of the CLB for external service.

Tenant Isolation

One of the key features of cloud platform is tenant isolation. Typically, users who access the cloud don't want their business to be affected by others; at least their business should be isolated on the network so others cannot access their machine. Of course, there are many ways to realize this feature in the industry, among which the most common one is isolation on the hardware level through the use of specific connection switch and vxlan protocol to achieve isolation. The downside:

1. A special switch is needed;
2. Additional equipment is needed to establish connection between vxlan network and ordinary network, which will cause the problem of single point;
3. Poor compatibility with existing network environment.

For the above reasons, we adopted the software solution, realizing tenant isolation via IP tunnel +
From the left side of the figure, we can see that the interaction between CLB and RS uses the IP tunnel method; CVM (RS) allocates the actual private network IP, and the connection to the physical network is established. The advantage is that it's easy to achieve, and is compatible with the previous physical machine solution, but the drawback is:

1. It requires additional modules to achieve tenant isolation;
2. Private network IPs cannot be reused between tenants, thus unable to achieve free networking;
3. Since IP is unique in the private network, RS IP must be changed when migrating, which means hot migration cannot be achieved.

For the above reasons, Tencent Cloud developed VPC. In the right side of the figure, you can see that the same tenant is assigned a VPCID, and the client may perform free networking within the VPC; the tenant network itself is isolated, and the specific processing is done by the vpc.ko kernel module.

**IP Convergence**
Speaking of cloud load balance, the most famous one in the industry is LVS (Linux Virtual Server) technology.

LVS has three modes: DR mode, NAT mode and TUNNEL mode. The main restriction of DR mode is that LVS and RS must be in the same vlan, which means deployment is very limited and scalability is poor. The main drawback of NAT mode is that returned data packets for RS need to use default route, and there is also scalability problem. Therefore, we initially built LVS clusters using the TUNNEL mode. However, TUNNEL mode requires that each RS is assigned one public network IP. For Tencent Cloud and services with considerable amount of RS, public network IP is a big challenge.

For the above reasons, CLB is created.

The following figure is a diagram of previously used LVS solution and CLB solution. The main difference is:

1. CLB does not need to assign public network IP to RS, achieving IP convergence;
2. Outbound traffic still go through CLB. It’s easier to locate problems; in addition, closed-loop is formed for service traffic, playing the role of bridgehead.

---

**Highly Reliable Implementation**

High reliability is an important metric for cloud services. In order for CLB to achieve a highly reliable service, we carried out the following solutions:

1. Cluster disaster recovery;
2. Session synchronization;
3. Resource isolation;
4. Anti-DDos.

---

**Cluster Disaster Recovery and Session Synchronization**
To put it simple, cluster disaster recovery means that the failure of one server in a cluster will not affect the service capabilities of the entire cluster. The traditional cluster disaster recovery uses HA mode (vrrp protocol) and common open source solutions include LVS. The drawbacks of traditional method include: only half of the servers in a cluster can work simultaneously, while the other half of the machines are in cold backup state; switching speed after a crash is relatively slow.

This issue is taken into account at the very beginning of CLB design process. It uses ospf dynamic routing protocol to achieve cluster disaster recovery; if a machine fails, ospf protocol can ensure that the machine is removed from the cluster within 10 seconds. CLB puts one cluster under two connection switches and ensures cross-rack disaster recovery, so that failure of a single switch or power failure of a single rack will not affect the services of the cluster.

Cluster disaster recovery guarantees the availability of CLB clusters, but for a client, if the server crashes, the removal of the machine can only guarantee that new connections will not go to this machine. But persistent connections will be disconnected. To solve this problem, we realized a periodic session connection synchronization within the cluster. With this, other servers that take over the packets from the faulty machine can find the correct session and ensure service availability.

LVS solution: Synchronizes when the connection status changes; when both persistent and short connections exist, synchronization traffic for short connection services can be very large, which will
impact normal forwarding.

CLB solution: Synchronize after 5 seconds when each connection is established; Does not synchronize if connection is within 5 seconds. Only "persistent connections" are synchronized.

---

**Resource Isolation**

The resource isolation feature is to protect other services from being affected when the CLB is under high load as individual service is attacked.

This is realized by regularly (5s) checking whether CLB has reached the configured warning level for high load; if so, resource isolation is activated, and CLB will check the traffic, number of packets, number of connections for each service. Those above the limit will be discarded, so as to ensure that the load of CLB server will not reach the actual limit which would otherwise affect other services. Normally, resource isolation function is disabled. It is guaranteed to activate within 5 seconds when service volume suddenly increases, or a service is attacked which caused CLB to reach the warning level, to ensure that normal service forwarding is not affected.

Resource isolation adopts the classic token bucket algorithm. The process is: regularly place a certain amount of tokens to the bucket, and each arriving packet consumes a token. If tokens are exhausted in a period of time, packets will begin to be discarded.
### Anti DDos

Cluster disaster recovery and resource isolation are both meant to protect the CLB platform itself. However, when a single service is attacked, this service will be damaged for sure. CLB will not allow this to happen. Tencent Cloud has a very powerful Dayu system to protect services from DDoS attacks. But the checking duration of Dayu Aegis system is 10 seconds, which means the client’s RS can be already crashed before Dayu system goes into effect. In order to solve problems within this 10 seconds, we have developed the synproxy feature.

Realization: when receiving the three-step handshake request from the client, CLB executes three-step handshake as a proxy without disturbing RS before the arrival of the packet; once the first packet arrives, CLB will cache it and then execute a three-step handshake with RS. If the handshake is a success, the cached data will be sent to RS, and the subsequent process is to transmit the packet in a transparent manner. This will ensure that DDoS attacks will not reach RS. CLB will take care of the pressure instead. CLB itself has relatively strong load capacity, plus its cluster mode and the ability to isolate resources, it is difficult to crash the CLB machine within 10 seconds under normal circumstances.
Features of Different Types of Tencent Cloud Load Balancers

CLB currently offers three types of services:

- Layer 4 cloud load balance corresponding to listener's tcp and udp;
- Layer 7 cloud load balance corresponding to listener's http/https capabilities.

**Layer 4 Cloud Load Balance**

Layer 4 cloud load balance is the earliest solution CLB has ever achieved and is also a necessary feature for a cloud load balance product. The basic principle is to distinguish different services via ports in the CLB; the key of forwarding rule is vip:vport:protocol. Currently this cloud load balance mode is the most commonly used one in Tencent Cloud. However, VIP belongs to the same developer, and traffic from different developers are strictly isolated.
Layer 7 Cloud Load Balance

The solution without daily rate can cope with ordinary layer 7 cloud load balance services, but layer 7 users who require session and cookie have to build their own nginx to perform an extra reverse proxy, which can be a waste of resources and affect reliability.

Two solutions were discussed regarding the design of layer 7 cloud load balance at the beginning:

1. Public network IP is directly applied to nginx machines, building a nginx cluster
2. The nginx cluster is connected under layer 4 CLB

The weakness of solution 1 is that it's totally vulnerable to DDoS attacks. For Tencent Cloud, a VIP is required to connect to layer 4 and layer 7 at the same time, which is beyond the capacity of solution 1, thus we finally adopted solution 2. Dynamic capacity scaling is another advantage of solution 2, which helps satisfy demands in scenarios when rapid capacity increase is required by services.

However, nginx achieves cloud load balance through the use of reverse proxy and there is a fatal problem in Tencent Cloud: since vpc network is a virtual network, which relies on the parent machine to establish a connection to the physical network, nginx reverse proxy cannot be used directly between layer 7 LD and RS. Therefore, we came up with the idea of simulating layer 4 and adding 17.ko kernel module on layer 7 LD which is responsible for encapsulating the gre tunnel and IPIP tunnel for interaction with RS.
Restrictions

Last updated: 2019-07-30 16:50:15

In addition to general usage restrictions, Tencent cloud load balancer instances are also subject to specific usage restrictions depending on their types. For more information on types of cloud load balancer instances, refer to Public Network Cloud Load Balancer.

<table>
<thead>
<tr>
<th></th>
<th>Specific Use Limits</th>
<th>General Use Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application CLB instance</td>
<td>A frontend port only corresponds to one protocol within one CLB instance</td>
<td>A maximum of 100 CLB instances can be purchased for each type</td>
</tr>
<tr>
<td></td>
<td>A frontend port corresponds to multiple backend ports within one CLB instance</td>
<td>A maximum of 100 CVMs can be associated with each CLB instance</td>
</tr>
<tr>
<td></td>
<td>A maximum of 50 forwarding rules can be created in one listener</td>
<td>A maximum of 50 listeners can be created for each CLB instance</td>
</tr>
<tr>
<td></td>
<td>A maximum of 100 forwarding groups (deviceId + port, i.e. CVM + port) can be added in one forwarding rule</td>
<td>The number of ports can only be an integer within 1-65535</td>
</tr>
<tr>
<td>Conventional CLB instance</td>
<td>A frontend port only corresponds to one protocol within one CLB instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A frontend port corresponds to multiple backend ports within one CLB instance</td>
<td></td>
</tr>
</tbody>
</table>

If a CLB-associated CVM is isolated (put into the recycle bin, or removed according to the postpaid plan) due to arrears, the CLB still binds this CVM.
Application and Conventional CLB comparison

Last updated: 2020-02-26 17:00:10

CLB offers two types of instances: CLB (formerly "application CLB") and classic CLB.

- Cloud Load Balancer: support TCP/UDP/HTTP/HTTPS Protocol, provide balance based on domain name and URL path, and support flexible repost.
- Traditional Cloud Load Balancer: private network does not support HTTP/HTTPS Protocol, and the configuration method is simple.

Cloud Load Balancer can cover all the functions of the traditional Cloud Load Balancer. From Features, product performance and other considerations, it is recommended that you use the instance type is Cloud Load Balancer. A detailed comparison of the two is as follows:

<table>
<thead>
<tr>
<th>Product Type</th>
<th>Cloud Load Balance</th>
<th>Classic Cloud Load Balancer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Public network</td>
<td>Private network</td>
</tr>
<tr>
<td>Layer-7 repost (HTTP/HTTPS)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Layer-4 repost (TCP / UDP)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Layer-4 encrypts repost (TCP SSL)</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Support for HTTP/2 and websocket (secure)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cloud Load Balancer's strategy</td>
<td>IP hash (Layer-7) Weighted polling</td>
<td>IP hash (Layer-7) Weighted polling</td>
</tr>
<tr>
<td></td>
<td>Weighted Minimum Connections</td>
<td>Weighted Minimum Connections</td>
</tr>
<tr>
<td></td>
<td>IP hash (Layer-7) Weighted polling</td>
<td>IP hash (Layer-7) Weighted polling</td>
</tr>
<tr>
<td></td>
<td>Weighted Minimum Connections</td>
<td>Weighted Minimum Connections</td>
</tr>
<tr>
<td></td>
<td>WRR</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Cloud</td>
<td>Huawei</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td>Session hold</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Health check</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Customize repost rules (domain name / URL)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Support SNI multi-certificate feature</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Repost to different back-end ports</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Layer-7 personalized configuration</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Layer-7 redirect function (rewrite)</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Support cross-region binding function</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Support Layer-7 log storage to COS</td>
<td>✓</td>
<td>×</td>
</tr>
</tbody>
</table>