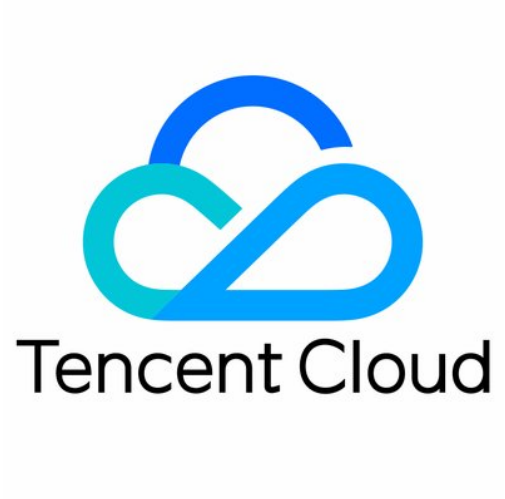
Cloud Load Balancer

FAQs

Product Documentation



Contents

FAQs
CLB Configuration

Last updated : 2020-09-04 16:54:14

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 an 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 need to open the CLB VIP, and the health check IP is opened by default), 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
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: blocklist**
  If you need to configure a blocklist for some client IPs to deny their access requests, you can configure 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 requests 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 blocklist 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 and click the corresponding 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 page.
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 and DisassociateSecurityGroups.

Why is the 843 listener Telnet connected without being created?

By default, CLB opens the 843 port to Internet for resetting access to Flash. To close the port, you only need to leave the TCP: 843 listener unbound to the real server.

HTTPS

Last updated : 2020-05-12 16:18:57

What encryption suites are supported by HTTPS?

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK

Which versions of SSL/TLS security protocols are supported by HTTPS?

CLB HTTPS currently supports the following SSL protocols: TLS 1, TLS 1.1, and TLS 1.2.

Which port does an HTTPS listener use?

There is no mandatory requirement for this. Port 443 is recommended.

Why HTTPS mutual authentication is needed?

Some users such as financial service providers have higher requirement for data security. They require HTTPS authentication on both the server and client. To meet their needs, HTTPS mutual authentication is provided.

Why does the HTTPS protocol actually generate more traffic than the billed traffic?

If the HTTPS protocol is used, it actually generates more traffic than the billed traffic as some of the traffic is used for protocol handshake.

Will requests from a CLB instances to a real server still be transferred over HTTP after an HTTPS listener is added?

Yes. After an HTTPS listener is added, requests from the client to the CLB instance will be encrypted over HTTPS, but requests from the CLB instance to the real server will still be transferred over HTTP. Therefore, there is no need to configure SSL on the real server.

What types of certificates does CLB currently support?

CLB currently supports server certificates and CA certificates. For a server certificate, both certificate content and private key need to be uploaded. For a CA certificate, only certificate content needs to

be uploaded. For both types of certificates, only certificates in PEM encoding format can be uploaded.

How many HTTPS certificates can be bound to a listener?

If HTTPS one-way authentication is used, only one server certificate can be bound to a listener. If HTTPS mutual authentication is used, one server certificate and one CA certificate need to be bound to a listener.

How many CLB instances or listeners can a certificate be applied to?

A certificate can be applied to one or multiple CLB instances or listeners.

How do I upload a certificate?

You can upload it by using an API or CLB Console.

Is a certificate region-specific?

Yes. If a certificate needs to be used in multiple regions, it is necessary to upload it in all those regions separately to ensure security and performance.

Does a certificate need to be uploaded to a backend CVM instance?

No. CLB HTTPS provides a certificate management system to manage and store user certificates. Certificates do not need to be uploaded to backend CVM instances, and all the private keys uploaded to the certificate management system are stored in an encrypted manner.

What can I do after a certificate expires?

After the current certificate expires, you need to update the certificate manually.

What can I do when a certificate error occurs?

This may be caused by wrong content of the private key. In this case, you need to replace it with a new certificate that meets the requirement.

WS/WSS Protocol Support

Last updated : 2020-03-09 14:59:39

Product Content

What is WS/WSS?

WebSocket (WS) is a protocol that provides full-duplex communication channels over a single TCP connection.
WebSocket facilitates data exchange between the client and server, and allows active data push from the server to client. In WebSocket API, only one handshake is required between the browser and server to create a persistent connection and carry out bi-directional data transmission.

Why should WS/WSS be used?

Without WebSocket, the client has to pull data from the server through polling.
There are two shortcomings in this data exchange method:

1. Low efficiency. To pull real-time data, the client has to frequently initiate the Ajax request.
2. The server cannot push data proactively.
   WebSocket is designed to solve these problems. As a new protocol released when HTML5 was launched, WebSocket achieves full-duplex communication between the browser and server. It can transmit message-based text and binary data, solving HTTP problems at the protocol level.

Key advantages of WebSocket:

1. Less overhead. After the connection is established, the packet header used for control is small. Compared to a HTTP request that requires a complete header, WebSocket helps reduce the overhead.
2. Real-time push. As a full-duplex protocol, WebSocket can achieve real-time data push from server to client.
3. Persistent connection.

Product Purchase

How is WS/WSS billed?

CLB supports WS/WSS by default and no additional fees will be charged.

Product Implementation

How to enable WS/WSS on CLB?

WS/WSS is enabled by default and no additional configuration is required.

If the listener listens to HTTP, WS is supported by default. If it listens to HTTPS, WSS is supported by default.

When WSS is used, CLB will carry out SSL offloading.

Which regions support WS/WSS?

Currently, WS/WSS protocols are supported in **all regions**.

Access Log

Last updated : 2020-07-07 11:42:09

How do I change the access log storage location from COS to CLS?

Please configure access log storage in CLS first and then disable access log storage in COS, as the feature of storing access logs in COS will be officially deactivated after 00:00:00, June 30, 2020, and access logs cannot be directly written to COS after then.

What is the difference between storing access logs in CLS and COS?

Compared to storing access logs in COS, storing access logs in CLS can provide:

- Real-time logging at a minute-level granularity and diversified online search based on full-text, key-value, and fuzzy keywords.
- Multi-region coverage and other capabilities, making it more suitable for large-scale use in production environments.

For detailed comparison, please see Access Log Overview.

Is it possible to store access logs in both COS and CLS?

It is possible to store access logs in both COS and CLS:

- Before the feature of storing access logs in COS is officially deactivated (i.e., before 23:59:59, May 31, 2020), existing access logs stored in COS will not be affected, and access logs will be written to CLS and COS at the same time.
- After the feature of storing access logs in COS is officially deactivated at 00:00:00, June 30, 2020, new access logs cannot be directly written to COS, and existing access logs in COS remain.

After storing access logs in CLS, certain CLS features can be used to store logs in COS. For example, latest logs (generated in the last 3 days) can be stored in CLS for easy query, while historical logs (generated more than 3 days ago) can be transferred to COS from CLS. For more information, please see CLS - Shipping Overview.

Will more fees be incurred by using CLS?

The access log service for CLB is free of charge. You only need to pay CLS or COS fees.

HTTP/2 Protocol Support

Last updated : 2020-09-10 15:21:30

Product Introduction

What is HTTP/2?

- HTTP/2 (Hypertext Transfer Protocol Version 2) is a major revision of the HTTP protocol used in web services.
- HTTP/2 is designed to address the performance issues in HTTP1.X to better use network resources and reduce network application latency.
- HTTP/2 is backward compatible with HTTP1.X.

Why should I use HTTP/2?

Compared with HTTP1.X, HTTP/2 can make the response be more fast and efficient. HTTP/2 has the following advantages:

- Multiplex: concurrent processing leads to a faster response.
- Server push: the server proactively pushes resources needed by the client, reducing the number of requests.
- More features include bandwidth limit, request priority, header compression, and binary framing.

Product Purchase

How is HTTP/2 billed?

CLB supports the HTTP/2 protocol without charging extra fees.

Product Implementation

How do I enable HTTP/2 on CLB?

1. Enable HTTP/2 on HTTPS listeners
   - CLB instance: you can enable or disable the HTTP/2 protocol in a CLB instance. To do this, see Configuring an HTTPS Listener.
   - Classic CLB instance: HTTPS listeners created for Classic CLB before April 2018 do not support the HTTP/2 protocol. HTTPS listeners created after April 2018 support but cannot disable the

HTTP/2 protocol.

2. Agree on the protocol at client access
   When the client accesses an HTTP/2-enabled listener, the protocol version will be negotiated during the handshake process of HTTPS. The client uses ALPN (Application-Layer Protocol Negotiation) to inform the server of a list of supported protocols. The server selects HTTP/2 or HTTP1.X according to the protocol list. If the client does not support HTTP/2, the server will be automatically backward compatible without requiring additional configuration.

⚠ Note :

1. The HTTP listener does not support HTTP/2. Mainstream browsers and web servers only support the TLS-based HTTP/2 protocol.
2. The HTTP1.X protocol is still used between the CLB and the real server.

Which regions support HTTP/2?

Currently, all regions support HTTP/2.