Cloud Load Balance

Best Practise

Product Introduction

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

Best Practise

Enabling Gzip Configuration & Testing

Last updated：2017-12-15 16:09:22

In the **public network application-based and public network (with static IP) cloud load balancer** instances, **HTTP/HTTPS protocol** is supported to enable gzip compression by users by default. Compressing web pages via the gzip feature can effectively reduce the amount of data transmitted on the network and improve the access speed of the client browser. When using the feature, please keep the following in mind:

1. Notes

- **GZIP of back-end CVM is required to be enabled synchronously**
  For common Nginx service containers, you must enable GZIP in their configuration files (nginx.conf by default) and restart the service

  ```
  gzip on;
  ```

- **Now the cloud load balancer supports file types below. And you can specify the file type in the gzip_types configuration item for compressing**

  ```
  application/atom+xml application/javascript application/json application/rss+xml application/vnd.ms-fontobject application/x-font-ttf application/x-web-app-manifest+json application/xhtml+xml application/xml font/opentype image/svg+xml image/x-icon text/css text/plain text/x-component;
  ```

  Note: GZIP support for the above file types must be enabled synchronously in the backend ECS business software of cloud load balancer.

- **A compression request flag must be contained in the client request**
  You need to enable compression, and the client must carry the following flag for requests:

  ```
  Accept-Encoding: gzip,deflate,sdch
  ```

2. Example of GZIP Enabling Process by Backend CVM

Operating environment of example Cloud Vitural Machine: Debian 6

1. Use vim to open the Nginx configuration file by user path:

   ```
   vim /etc/nginx/nginx.conf
   ```

2. Find the following codes:

```
gzip on;
gzip_min_length 1k;
gzip_buffers 4 16k;
gzip_http_version 1.1;
gzip_comp_level 2;
gzip_types text/html application/json;
```

Detailed syntax of the above codes:

gzip: enable or disable gzip module.

```
Syntax: gzip on/off
```

Scope: http, server, location

gzip_min_length: Set the minimum bytes for a page allowed to be compressed. The number of bytes for a page is obtained from the Content-Length of header. The default value is 1k.

```
Syntax: gzip_min_length length
```

Scope: http, server, location

gzip_buffers: Set how many units of cache are used by system to store the gzip compressed result data flow. 4 16k represents the unit is 16k, and memory is applied by four times of 16k according to the original data size.

```
Syntax: gzip_buffers number size
```

Scope: http, server, location

gzip_comp_level: gzip compression ratio. The range is 1 ~ 9. 1 presents the minimum compression ratio with the fastest processing speed, while 9 presents the maximum compression ratio with the slowest processing speed (faster transmission but more CPU consumption).

```
Syntax: gzip_comp_level 1..9
```

```
Scope: http, server, location
```

gzip_http_level: The lowest version of HTTP allowed to use the gzip feature. If HTTP/1.0 is set, the gzip feature can be used for HTTP/1.0 and is upward compatible with HTTP/1.1. Since Tencent Cloud now supports HTTP/1.1 across the network, no changes are required.

```
Syntax: gzip_http_version 1.0 | 1.1;
Scope: http, server, location
```

gzip_types: Match MIME types for compression. "text/html" type will be compressed by default. In addition, gzip under Nginx does not compress static resource files such as javascript and images by default. You can specify the MIME types to be compressed via gzip_types, and other types will not be compressed. ***For example, if json format data needs to be compressed, you need to add application/json data in this statement***
The supported types are as follows:

```
text/html text/plain text/css application/x-javascript text/javascript application/xml

Syntax: gzip_types mime-type [mime-type ...]
Scope: http, server, location
```

3 . If the configuration changes, save the file and exit, go to the Nginx bin file directory, and execute the following command to reload Nginx

```
./nginx -s reload
```

1. Use the curl command to test whether gzip was successfully enabled

   ```
   curl -I -H "Accept-Encoding: gzip, deflate" "http://cloud.tencent.com/example/"
   ```

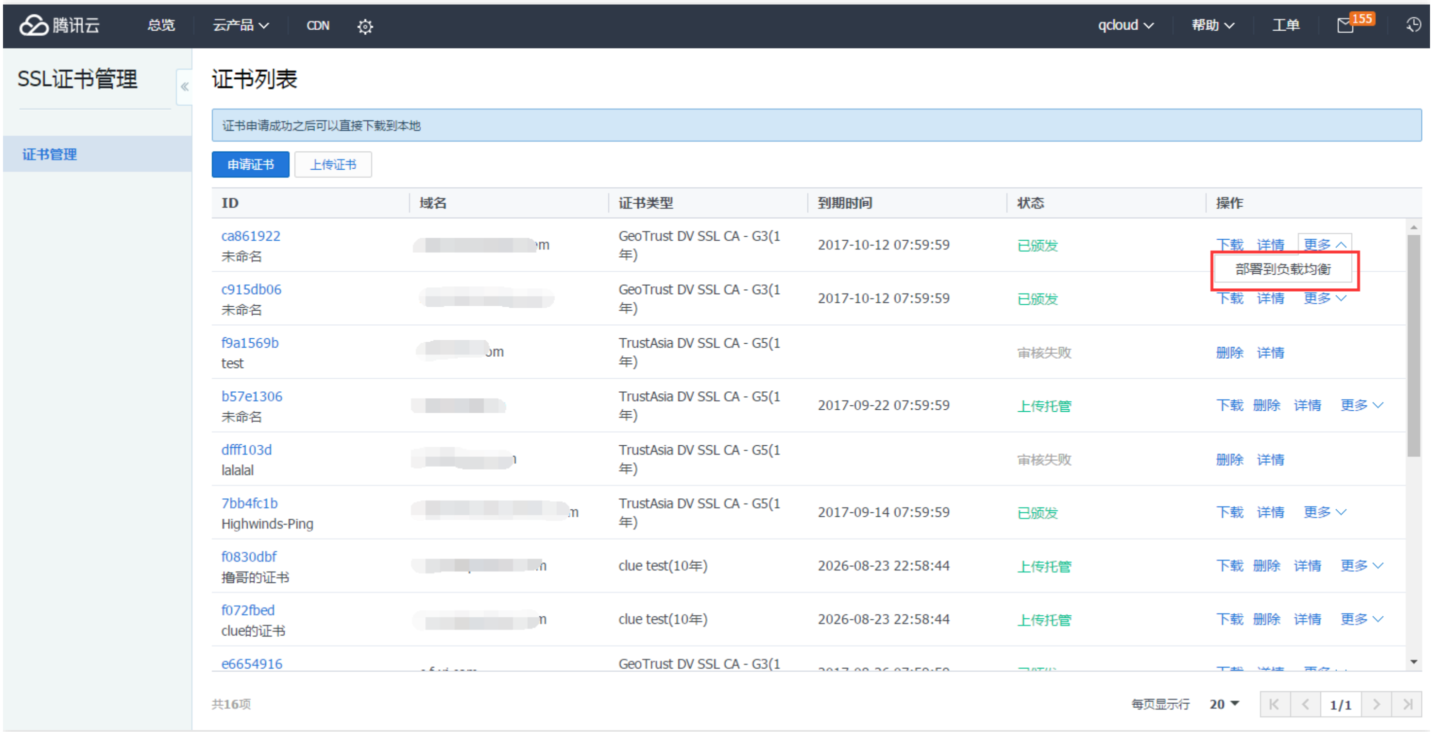
Deploy Certificate to Load Balancer

Last updated：2017-12-05 17:20:43

SSL certificates can be deployed to the cloud load balancer as follows:

1. Select a Certificate

Apply for a certificate (refer to Apply for a Free Domain Certificate or select a certificate to upload, expand "More" operation, and select "Deploy to Cloud Load Balancer".



证书列表

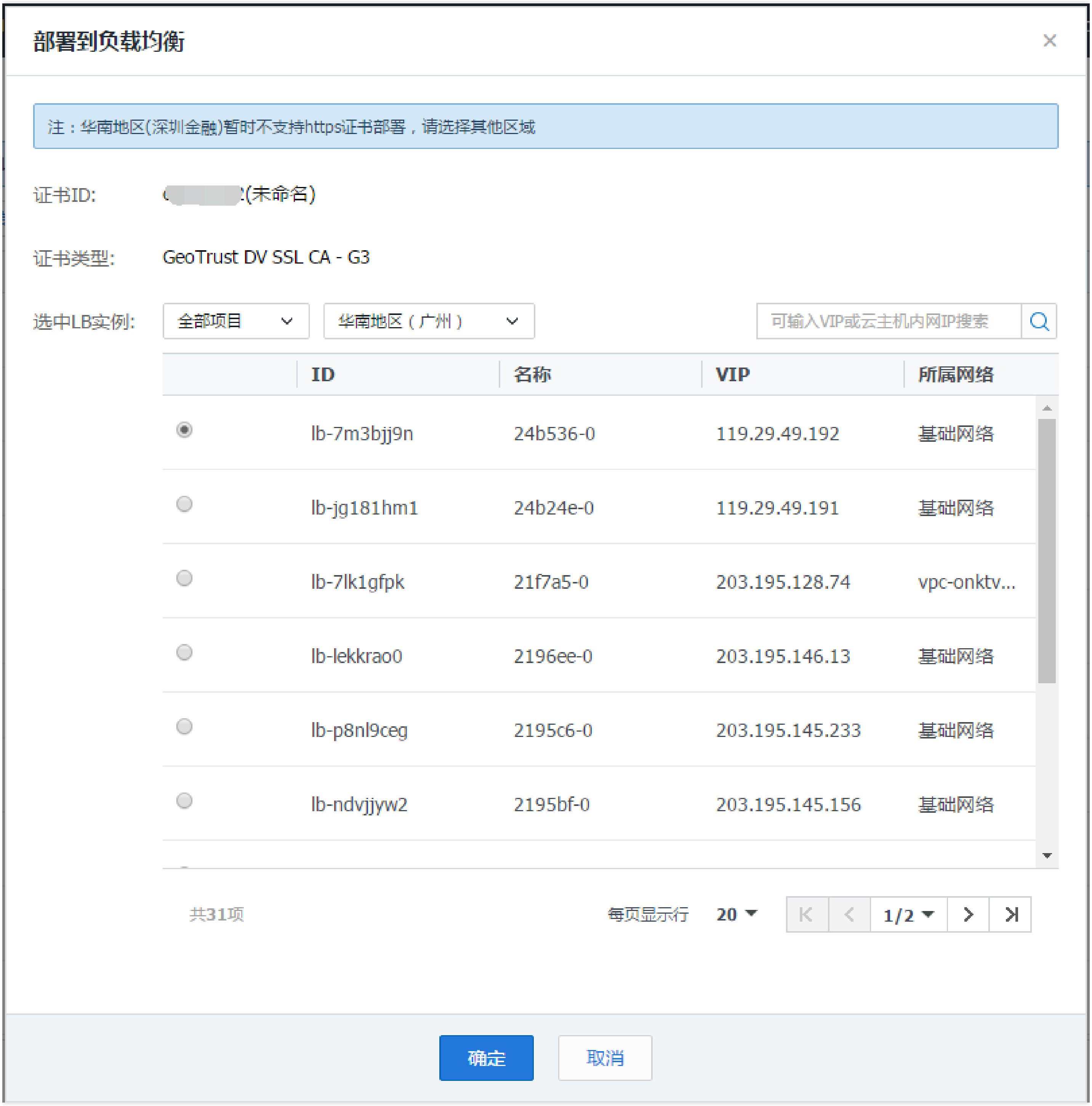
证书申请成功之后可以直接下载到本地

ID	域名	证书类型	到期时间	状态	操作
ca861922 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)	2017-10-12 07:59:59	已颁发	下载 详情 更多
c915db06 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)	2017-10-12 07:59:59	已颁发	下载 详情 更多
f9a1569b test	[redacted]	TrustAsia DV SSL CA - G5(1年)		审核失败	删除 详情
b57e1306 未命名	[redacted]	TrustAsia DV SSL CA - G5(1年)	2017-09-22 07:59:59	上传托管	下载 删除 详情 更多
dfff103d lalalal	[redacted]	TrustAsia DV SSL CA - G5(1年)		审核失败	删除 详情
7bb4fc1b Highwinds-Ping	[redacted]	TrustAsia DV SSL CA - G5(1年)	2017-09-14 07:59:59	已颁发	下载 详情 更多
f0830dbf 撸哥的证书	[redacted]	clue test(10年)	2026-08-23 22:58:44	上传托管	下载 删除 详情 更多
f072fbed clue的证书	[redacted]	clue test(10年)	2026-08-23 22:58:44	上传托管	下载 删除 详情 更多
e6654916		GeoTrust DV SSL CA - G3(1			

共16项

2. Select an LB Instance

Select only one LB instance according to the project and region (South China region - Shenzhen Finance not supported).



部署到负载均衡

注：华南地区(深圳金融)暂时不支持https证书部署，请选择其他区域

证书ID: [redacted](未命名)

证书类型: GeoTrust DV SSL CA - G3

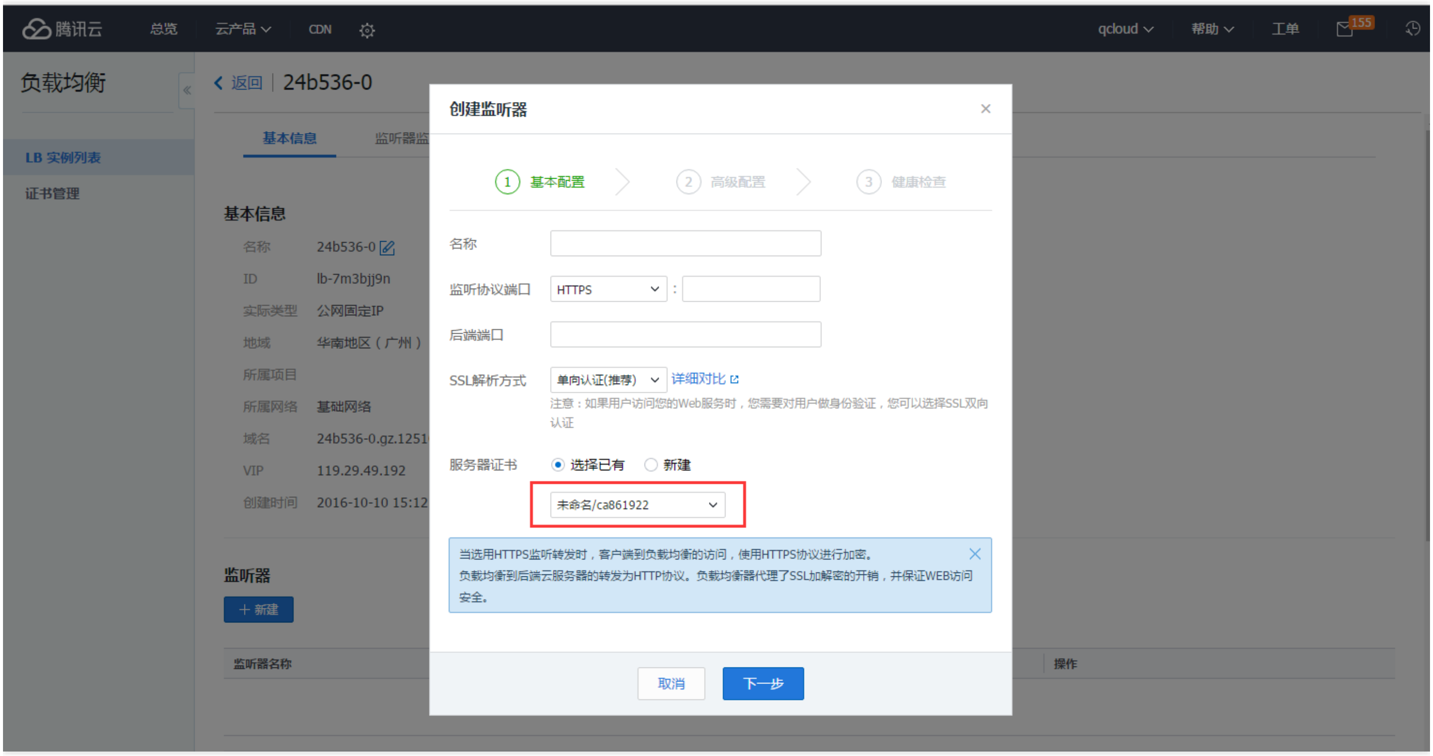
选中LB实例: 全部项目 华南地区（广州） 可输入VIP或云主机内网IP搜索

	ID	名称	VIP	所属网络
●	lb-7m3bjj9n	24b536-0	119.29.49.192	基础网络
○	lb-jg181hm1	24b24e-0	119.29.49.191	基础网络
○	lb-7lk1gfpk	21f7a5-0	203.195.128.74	vpc-onktv...
○	lb-lekkrao0	2196ee-0	203.195.146.13	基础网络
○	lb-p8nl9ceg	2195c6-0	203.195.145.233	基础网络
○	lb-ndvjjyw2	2195bf-0	203.195.145.156	基础网络

共31项 每页显示行 20 1/2

3. Create a Listener

Go to the CLB console, open the "Create a Listener" pop-up window, switch the protocol port to Https, select the specified server certificate, and then complete the rest configurations.



24b536-0

基本信息

名称	24b536-0
ID	lb-7m3bjj9n
实际类型	公网固定IP
地域	华南地区（广州）
所属项目	
所属网络	基础网络
域名	24b536-0.gz.1251
VIP	119.29.49.192
创建时间	2016-10-10 15:12

监听器

创建监听器

名称

监听协议端口 HTTPS :

后端端口

SSL解析方式 单向认证(推荐) 详细对比

注意：如果用户访问您的Web服务时，您需要对用户做身份验证，您可以选择SSL双向认证

服务器证书 ● 选择已有 ○ 新建

未命名/ca861922

当选用HTTPS监听转发时，客户端到负载均衡的访问，使用HTTPS协议进行加密。负载均衡到后端云服务器的转发为HTTP协议。负载均衡器代理了SSL加解密的开销，并保证WEB访问安全。

4. Complete Other Configurations

Continue completing other configurations to create a listener, and then you can get a cloud load balancer with Https.

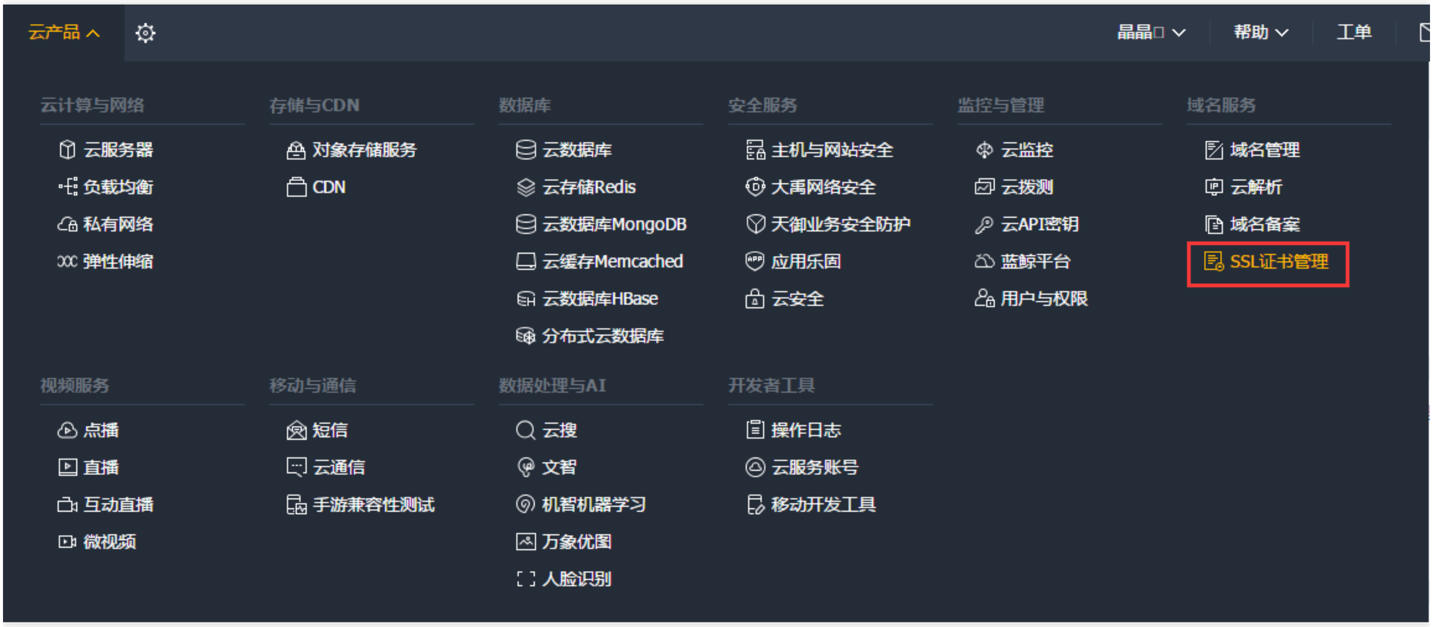
Apply for HTTPS Certificate

Last updated：2018-05-28 18:22:50

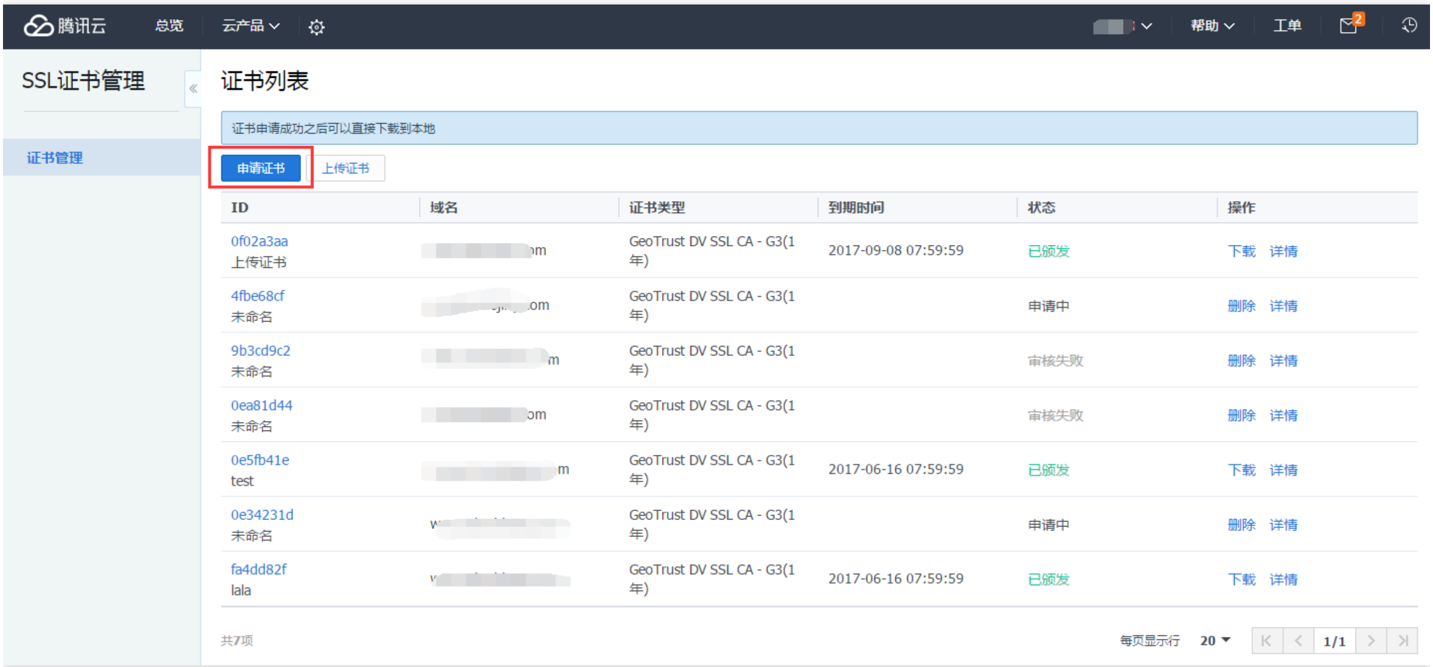
Applying for Domain Validation (DV) SSL Certificate

1. Application Entry

Enter the SSL certificate management console



Click "Apply for Certificate"



证书列表

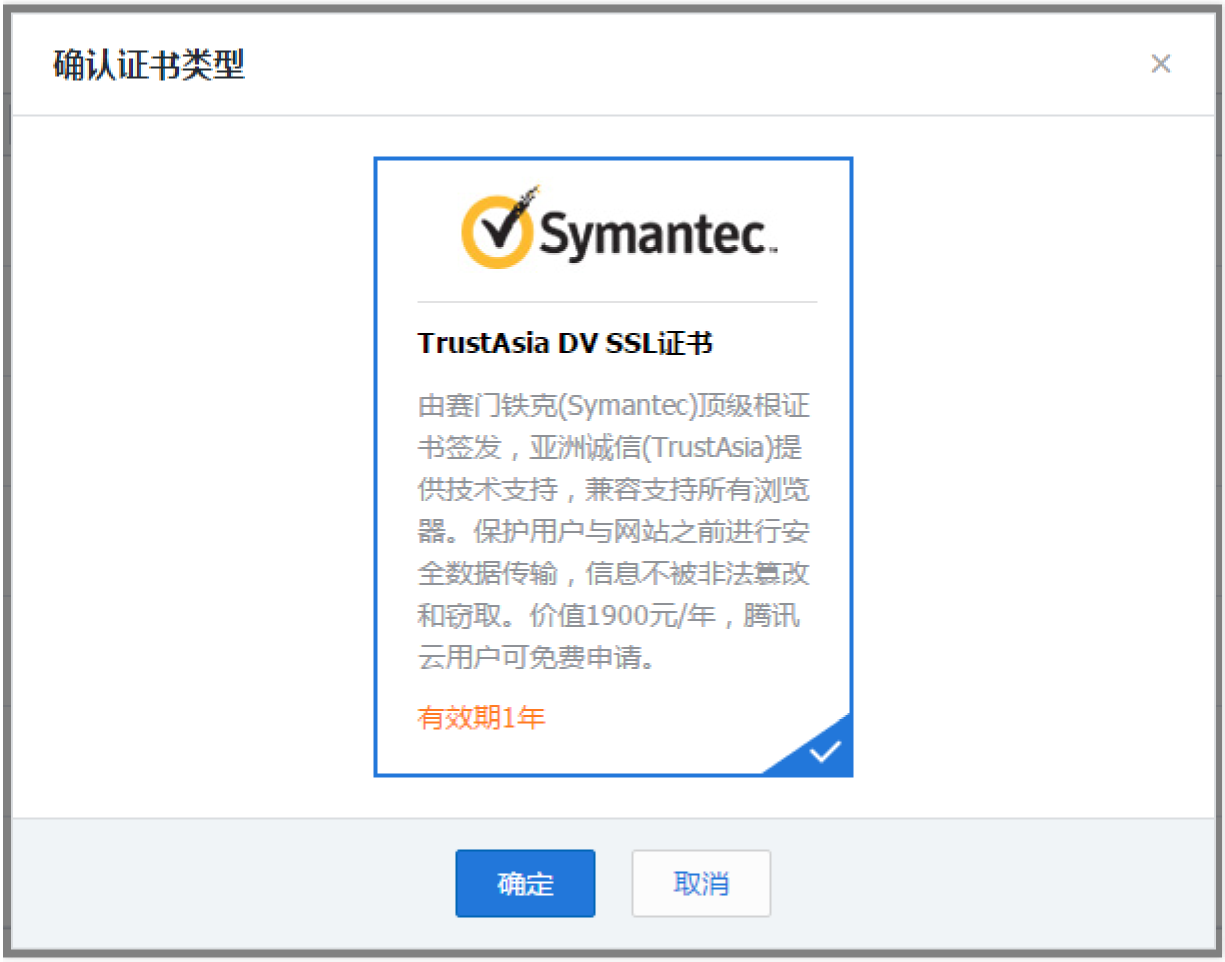
证书申请成功之后可以直接下载到本地

申请证书 上传证书

ID	域名	证书类型	到期时间	状态	操作
0f02a3aa 上传证书	[redacted]	GeoTrust DV SSL CA - G3(1年)	2017-09-08 07:59:59	已颁发	下载 详情
4fbe68cf 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)		申请中	删除 详情
9b3cd9c2 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)		审核失败	删除 详情
0ea81d44 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)		审核失败	删除 详情
0e5fb41e test	[redacted]	GeoTrust DV SSL CA - G3(1年)	2017-06-16 07:59:59	已颁发	下载 详情
0e34231d 未命名	[redacted]	GeoTrust DV SSL CA - G3(1年)		申请中	删除 详情
fa4dd82f lala	[redacted]	GeoTrust DV SSL CA - G3(1年)	2017-06-16 07:59:59	已颁发	下载 详情

共7项 每页显示行 20 1/1

View the model of the applied domain validation certificate, and click "OK"



确认证书类型

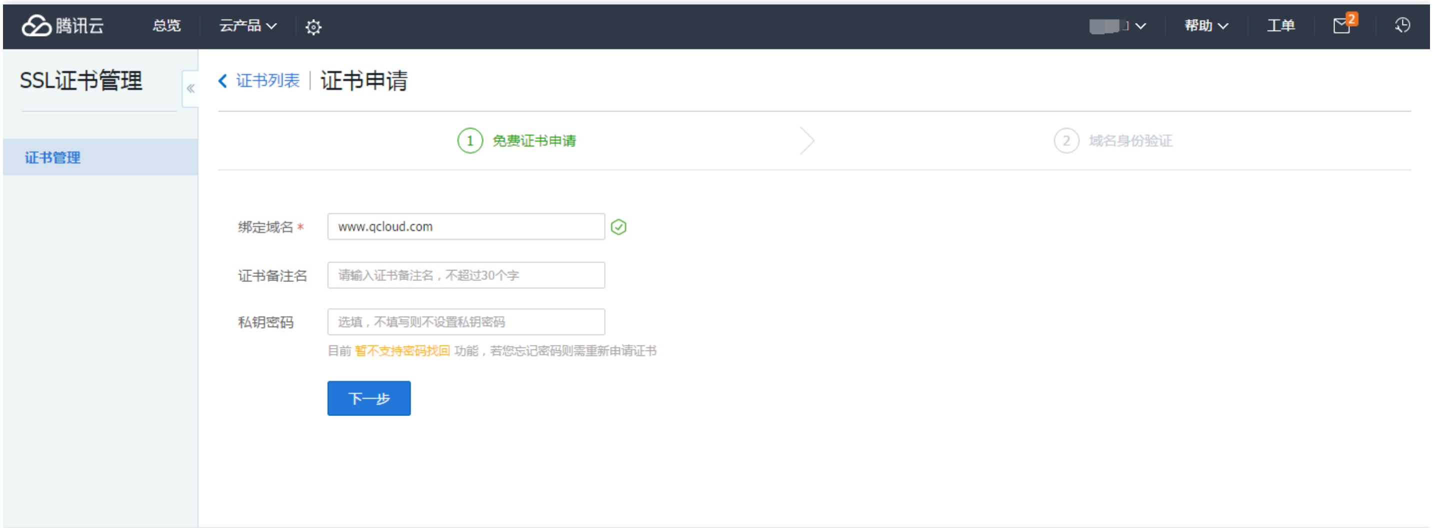
TrustAsia DV SSL证书

由赛门铁克(Symantec)顶级根证书签发，亚洲诚信(TrustAsia)提供技术支持，兼容支持所有浏览器。保护用户与网站之前进行安全数据传输，信息不被非法篡改和窃取。价值1900元/年，腾讯云用户可免费申请。

有效期1年

2. Filling in the Application

Fill in the applied domain, note that it is not supported to apply for top-level domains (e.g. qcloud com), please enter second-level, third-level domains such as cloud.tencent.com, demo.test.qlcoud.com.



绑定域名 * www.qcloud.com

证书备注名 请输入证书备注名，不超过30个字

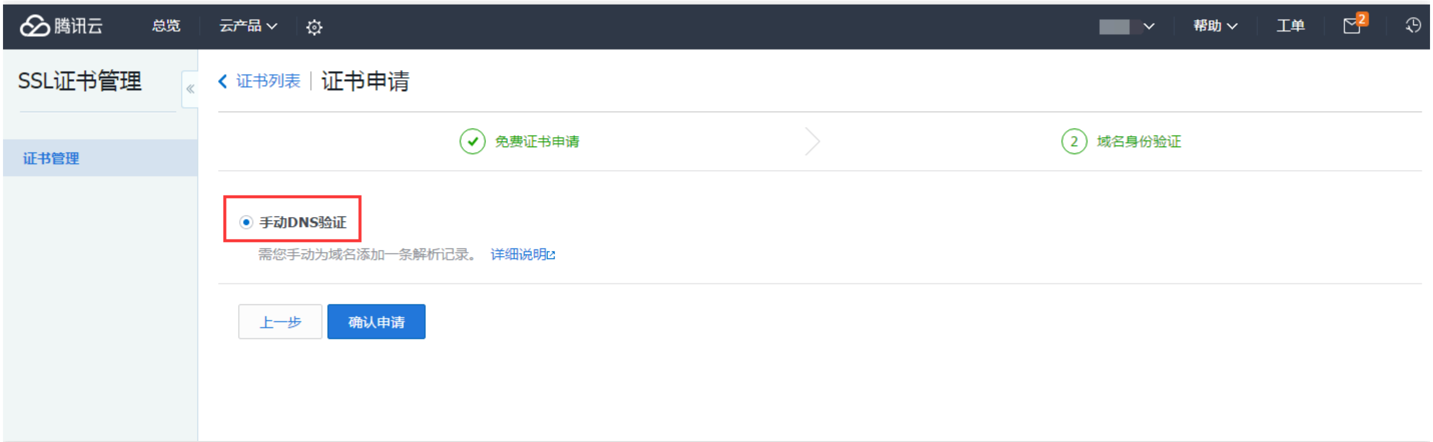
私钥密码 选填，不填写则不设置私钥密码

目前 暂不支持密码找回 功能，若您忘记密码则需重新申请证书

3. DNS Verification

3.1 Manual DNS Verification

Certificates support manual DNS verification by default, please refer to Details for detailed verification method.

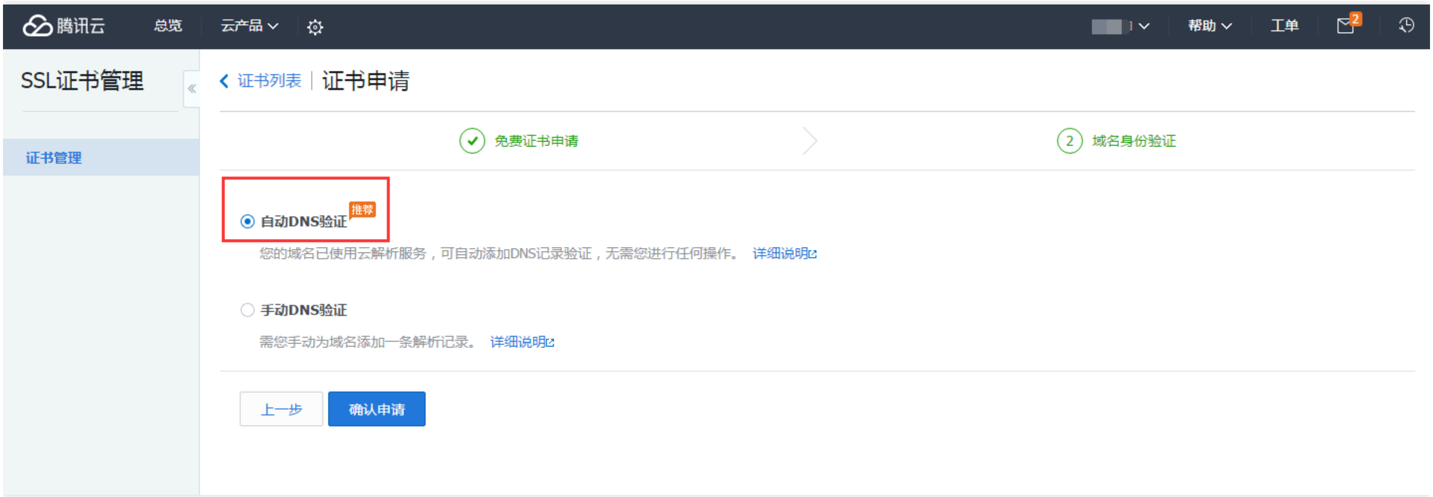


● 手动DNS验证

需您手动为域名添加一条解析记录。 详细说明

3.2 Choosing Automatic DNS Verification

If Cloud Resolution Platform is added successfully for the applied domain, the domain will support automatic DNS verification. Refer to Details for detailed verification method.



● 自动DNS验证

您的域名已使用云解析服务，可自动添加DNS记录验证，无需您进行任何操作。

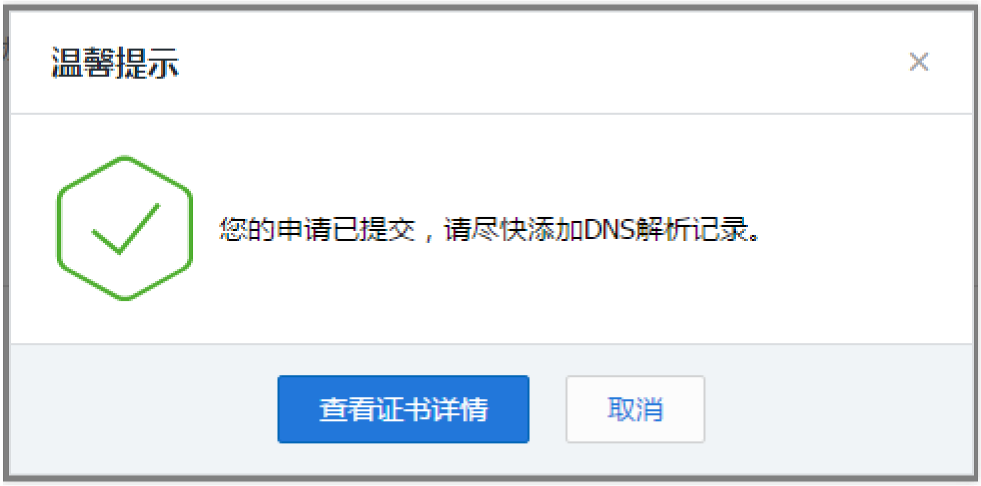
○ 手动DNS验证

需您手动为域名添加一条解析记录。

4. Submitting the Application

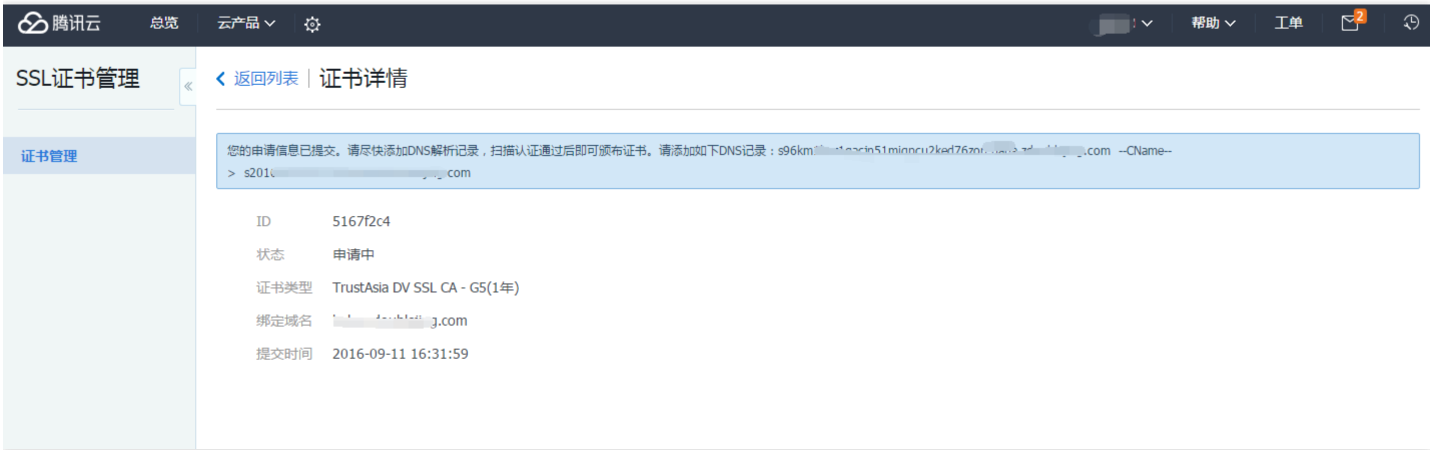
4.1 Identity Verification after Submission

When application is successfully submitted, a pop-up window will appear, notifying that you need to go to the "Certificate Detail Page" to obtain the CName record and add resolution:



您的申请已提交，请尽快添加DNS解析记录。

The process of obtaining the CName record is shown in Tips, please add resolution as soon as possible so that it can be approved by CA:

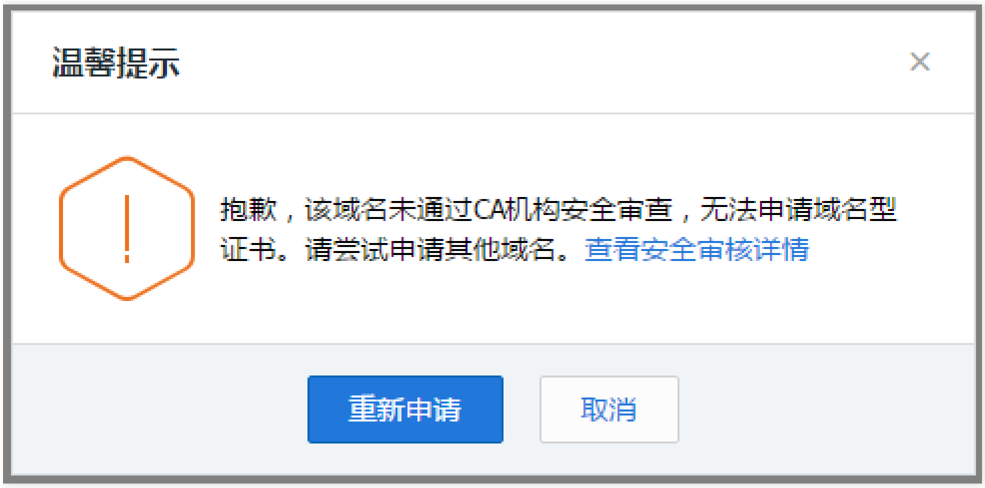


您的申请信息已提交。请尽快添加DNS解析记录，扫描认证通过后即可颁布证书。请添加如下DNS记录：s96km[redacted].com --CName--> s201[redacted]com

ID	5167f2c4
状态	申请中
证书类型	TrustAsia DV SSL CA - G5(1年)
绑定域名	[redacted]g.com
提交时间	2016-09-11 16:31:59

4.2 Failed to Submit Application

The pop-up window shown below indicates that the submitted domain is not approved by CA's security verification. Refer to Reasons for Failed Security Verification for detailed reasons.



抱歉，该域名未通过CA机构安全审查，无法申请域名型证书。请尝试申请其他域名。查看安全审核详情

HTTPS Forwarding Configurations

Last updated：2018-08-23 16:04:52

1. About Cloud Load Balance Capability

Tencent Cloud's CLB has achieved significant improvement in HTTPS performance based on the deep optimization of protocol stack and servers. At the same time, our cooperation with world-leading certificate providers saves the cost on certificates. Tencent Cloud's CLB brings substantial benefits for your business in the following aspects:

1. The use of HTTPS does not affect the access speed of Client.
2. A single CVM in a cluster features a fast SSL encryption and decryption capability, with the full handshakes reaching up to 65,000 cps. This is at least 3.5 times faster than that when high-performance CPU is relied on, which greatly reduces the server costs, enhances the service capacity at the time of business volume and traffic surges and achieves a stronger computing-based anti-attack capability.
3. CLB supports the unmount and translation of a variety of protocols. CLB reduces business backend's stress of supporting various protocols for the client. Business backend just needs to support HTTP1.1 to use various versions of protocols such as HTTP2, SPDY, SSL3.0 and TLS1.2.
4. One-stop service covering SSL certificate application, monitoring and replacement. By working with world-leading certificate vendors including Comodo and Symantec, we have significantly simplified certificate application procedures and reduced relevant costs.
5. Anti-CC and WAF features CLB can effectively prevent application-level attacks such as slow connection, high-frequency targeted attack, SQL injection and website malicious code.

2. HTTP and HTTPS Header Identifier

CLB acts as a proxy for HTTPS. Both HTTP and HTTPS requests become HTTP requests when forwarded to the backend CVM by CLB. In this case, the developer is not able to distinguish whether the frontend request is HTTP or HTTPS.

Tencent CLB implants X-Client-Proto into the header when it forwards the request to the backend CVM:

X - Client - Proto: http (frontend request is an HTTP request)
X - Client - Proto: https (frontend request is an HTTPS request)

3. Starting Configuration

Assume that a user needs to configure the website https://example.com. The developer wants users to directly access the website securely through HTTPS protocol by simply entering www.example.com in the browser.

In this case, www.example.com request entered by the user is forwarded as follows:

1. The request is transmitted via HTTP protocol and accesses port 80 of the load balancer listener via VIP. Then it is forwarded to port 8080 of the backend CVM.

2. By configuring rewrite operation on nginx of the Tencent Cloud backend server, the request is pass through port 8080 and is re-written to the https://example.com page.

3. Then the browser sends https://example.com request to the corresponding HTTPS site again. The request accesses port 443 of the load balancer listener via VIP, and then it is forwarded to port 80 of the backend CVM.

At this point, the request forwarding process is finished.

This operation rewrites user's HTTP request into a more secure HTTPS request without being noticed. To achieve the above request forwarding operation, the user can configure the backend server as follows:

```
server {

listen 80;
server_name example.qcloud.com;

location / {

#! customized_conf_begin;
client_max_body_size 200m;
rewrite ^/.(.*) https://$host/$1 redirect;

}
}
```

Alternatively, in the new version of nginx, redirect the nginx http page to the https page with 301 redirection method (recommended):

```
server {
listen 80;
server_name example.qcloud.com;
return 301 https://$server_name$request_uri;
}
```

```
server {
listen 443 ssl;
server_name example.qcloud.com;
[....]
}
```

Obtain Acutual IP for Layer 7 Load Balancing

Last updated：2018-06-12 17:29:58

- As Layer-4 cloud load balance (TCP protocol) can directly access the real IP address of the visitor on the backend CVM, and no additional configuration is required. The following description is only for Layer-7 (HTTP protocol) cloud load balance.
- Layer-7 cloud load balance system provides X-Forwarded-For method to obtain the visitor's real IP, which is enabled by default.

The common options for application server configuration are described below.

1. IIS 6 Configuration Option

1) Install the plugin F5XForwardedFor.dll. Copy `F5XForwardedFor.dll` under the x86\Release or x64\Release directory to a specific directory according to your own server operating system version, which is assumed to be `C:\ISAPIFilters` here. In addition, you should ensure that the IIS process has read access to the directory.

2) Open the IIS manager, find the currently opened site, right-click on the site to select "Properties" and open the property page.

3) In the property page, go to "ISAPI Filter" and click "Add" button. The "Add" window will appear.

4) In the "Add" window, fill in "F5XForwardedFor" for "Filter Name", and the full path of `F5XForwardedFor.dll` for "Executable File" and then click OK.

5) Restart IIS server, waiting for the configuration to take effect.

2. IIS 7 Configuration Option

1) Download and install the plugin F5XForwardedFor module. Copy `F5XFFHttpModule.dll` and `F5XFFHttpModule.ini` under `x86\Release` or `x64\Release` directory to a specific directory according to your own server operating system version, which is assumed to be `C: \F5XForwardedFor` here. Make sure that the IIS process has read access to the directory.

2) Select "IIS Server" option, and select the "Module" function.

3) Double-click the "Module" function, and click "Configure Local Module".

4) Click the "Register" button in the pop-up box.

5) Add the downloaded DLL file.

6) After the file is added, check it and click "OK".

7) Add these two DLLs to "API and CGI Restrictions" and change their setting to "allow".

8) Restart the IIS server, waiting for the configuration to take effect.

3. Apache Configuration Option

1) Install apache third party module "mod_rpaf"

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2) Modify the apache configuration `/etc/httpd/conf/httpd.conf` , and add at the end:

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips ip address (this ip address is not the public network ip provided by the cloud load balancer, and the specific ip addresses can be viewed in the apache log. Usually, there are two, both of which should be added)
RPAFheader X-Forwarded-For
```

3) Restart apache after completing the adding

```
/usr/sbin/apachectl restart
```

4. Nginx Configuration Option

1) As cloud load balancer, Nginx uses http_realip_module to get real ip; since the default installation for Nginx does not include this module, you need to recompile Nginx to add --with-http_realip_module:

```
wget http://soft.phpwind.me/top/nginx-1.0.12.tar.gz
tar zxvf nginx-1.0.12.tar.gz
```

```
cd nginx-1.0.12
./configure --user=www --group=www --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2) Modify nginx.conf

```
vi /etc/nginx/nginx.conf
```

Modify the following red parts:

```


fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;

set_real_ip_from ip address; (this ip address is not the public network ip provided by the cloud loa
Real_ip_header X-Forwarded-For;
```

3) Restart nginx

```
service nginx restart
```

SANT and Non-SANT of Private Network CLB

Last updated：2017-03-24 16:00:18

Starting from December 15th, 2016, newly purchased private network-based Cloud Load Balancers under Virtual Private Cloud (choose private network VPC) will no longer undergo SNAT processing, that is, the access IP received from server end is the real client IP. To ensure that your business operates properly, please note the followings:

- i. For private network-based CLB newly purchased after 15th, after security group policy is enabled, you must allow all inbound rules of client IPs to ensure normal access.
- i. If necessary, you can switch the existing private network-based CLB to the new one by submitting a ticket to the after-sales team. After the switching, the access IP acquired from the server side is the client IP. Your business will not be interrupted during the switching process

Configure Multiple Availability Zones

Last updated：2017-03-28 10:44:21

Multiple Availability Zones for Cloud Load Balancer

The cloud load balancer (CLB) supports disaster tolerance across availability zones. For example, multiple clusters are deployed in two availability zone (of one region) in Shenzhen Finance Zone I and II to achieve disaster tolerance across availability zones in one region. This capability allows the cloud load balancer to forward the front-end access traffic of one availability zone to other availability zones in the same region within 10 seconds to restore service capabilities in case of failure of the former available zone

Q & A

Q1: Shenzhen Finance Zone I and II share a cloud load balancer test1. What is the strategy of public network inbound traffic for the client?

- A: There is a pair of IP resource pools at data centers of Shenzhen Zone I and II, which can be understood as peering IP resources. Developers do not need to distinguish between the master cluster and the backup cluster, for both of them have equal cloud load capacity. When the developer buys a cloud load balancer and binds it to the CVM, it generates two sets of rules to write the cluster, and it has gained high availability.

Q2: Shenzhen Finance Zone I and II share a cloud load balancer test1, whose back-end binds 100 CVMs at each availability zone of I and II. 1 million HTTP persistent connections (TCP connection not closed) are established when the business is in operation. If the cloud load balancer clusters in Finance Zone I all break down at this point, what will happen to the business?

- A: When the cloud load balancers in Finance Zone I fail, all persistent connections will be disconnected and short connections will not be affected. The disaster tolerance system will automatically bind the 100 CVMs in Zone I to the load balancer in Zone II within 10 seconds. The business capability is immediately restored without manual intervention.

Q3: Which type of CLB is compatible with the capability of "disaster tolerance across availability zones"? Do I need to pay extra for such capability?

- A: This capability is currently free of charge. It is compatible with the application-based CLB and the public network (with static IP) CLB. It also supports http/https/tcp/udp and other protocols.

Register Domain Names and Add CNAME Records

Last updated：2018-08-23 16:06:37

Currently, Cloud Load Balance ***public network products with static IPs*** support the binding of A record and CNAME. Users can access the domain by registering one then adding A record and CNAME record.

1. Domain Name Registration

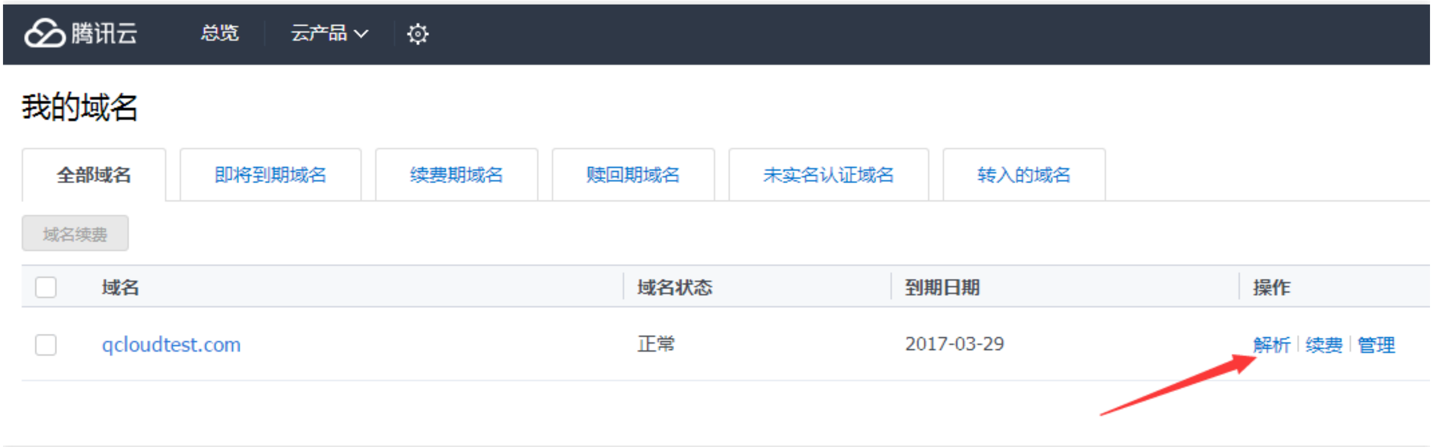
You can open the Domain Registration Page to query and register domains.

Refer to How to Register a Domain for relevant documents

2. Adding CNAME record

2.1. Enter the Domain Resolution Page

Log in to Tencent Cloud "Console" - "Cloud Services" - "Domain Management" - "Resolution", the example main domain is qcloudtest.com.



	域名	域名状态	到期日期	操作
□	qcloudtest.com	正常	2017-03-29	解析 | 续费 | 管理

2.2. Add CNAME Record

Click "Add" in "Resolution" page to add CNAME record. Instructions are shown below:

a. Enter the host record as required:
A host record is domain prefix. Common usage are as follows:

- www: resolved domain is www.qcloudtest.com
- @: Directly resolve the main domain qcloudtest.com
- *: Wildcard resolution, matches all other domains* .qcloudtest.com

b. For record type, users may choose the CNAME record
Each record type is shown below:

- A Record: address record, which is used to specify IPv4 address of the domain (e.g. 8.8.8.8), if you need to direct the domain to an IP address, A Record must be added.
- CNAME: You need to add CNAME Record if the domain is required to point to another domain which provides the IP address.
- TXT: You can enter anything here, the length limit is 255. Most TXT records are used as SPF records (anti-spam).
- NS: Domain server record. This is needed if you need to deliver the sub-domain to other DNS service providers for resolution.
- AAAA: Used to specify the corresponding IPv6 address (such as ff06:0:0:0:0:0:0:c3) record of the host name (or domain name).
- MX: This is need if you need to set up an e-mail to receive mails.
- Explicit URL: Explicit URL record is needed when an address 301 redirects to another address (Note: Currently DNSPod only supports 301 redirection).
- Implicit URL: Similar to explicit URL. The difference is that implicit URL will not change the domain in the address bar.
- SRV: Records which services are provided by certain computers. Format: + dot + . For example: _xmpp-server._tcp.

c. Line is used to specify users of specific lines to access this IP
Choose "Default" if the domain provider only provided one IP address or domain
Common usage:

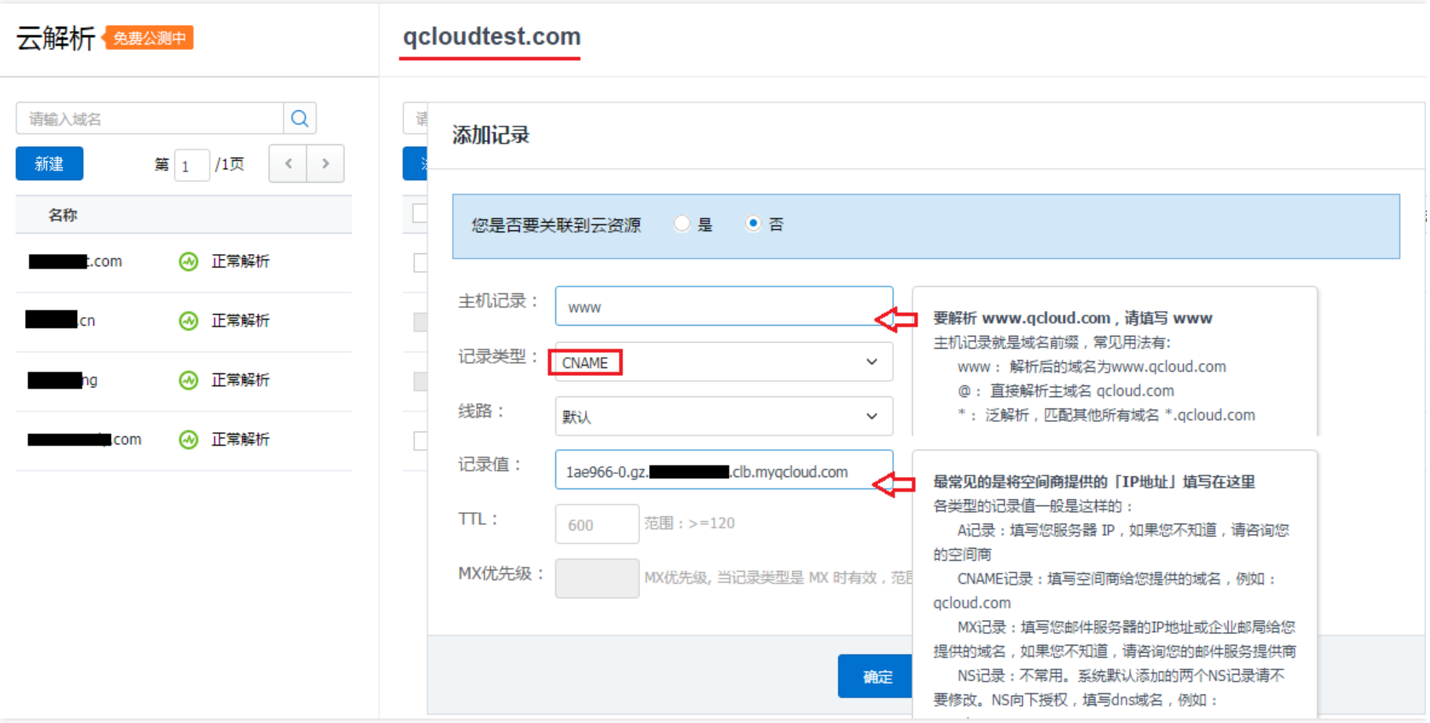
- Default: Must be added, otherwise your website can only be accessed by specially specified lines. If it is dual-line resolution, it is recommended to enter [China Telecom IP] for [Default] line
- China Unicom: Specify server IP for [China Unicom Users]. Other users still access the [Default] one
- Search engines: Specify a server IP for web crawlers to capture

d. For CNAME record, mainly enter the domain provided by your domain provider
Record values of various types are usually like these:

- A Record: Enter your server IP, ask your domain provider if you're not sure
- CNAME Record: Enter the domain provided by your domain provider. ***For example: Domain of the LB instance in cloud load balancer, 1b16c9-0.gz.12345678.clb.myqcloud.com***

- MX Record: Enter the IP address of your e-mail server or the domain provided by your enterprise e-mail provider. Ask your e-mail service provider if you're not sure
- TXT Record: Usually used in anti-spam configurations of enterprise e-mails (such as Google, QQ and so on)
- Explicit URL Record: Enter the URL to redirect to, for example: http://cloud.tencent.com
- Implicit URL Record: Enter the URL whose content is to be referenced, for example: http://cloud.tencent.com
- AAAA: Rarely used. IPv6 address to be resolved.
- NS Record: Rarely used. Please do not modify the two NS records added by the system by default. NS downward authorization. Enter the DNS domain, for example: f1g1ns1.dnspod.net
- SRV Record: Rarely Used Format: , space, , space, , space, . Once the record is generated, it is normal that a "." will be added at the end. For example: 5 0 5269 xmpp-server.l.google.com.

For the other values, you can use their default. Click "OK" when you've completed the settings.



[redacted].com 正常解析

[redacted]cn 正常解析

[redacted]ng 正常解析

[redacted]com 正常解析

添加记录

您是否要关联到云资源 ○ 是 ● 否

主机记录： www

记录类型： CNAME

线路： 默认

记录值： 1ae966-0.gz.[redacted].clb.myqcloud.com

TTL： 600 范围：>=120

MX优先级： MX优先级，当记录类型是 MX 时有效，范

要解析 www.qcloud.com，请填写 www
主机记录就是域名前缀，常见用法有:
www： 解析后的域名为www.qcloud.com
@： 直接解析主域名 qcloud.com
*： 泛解析，匹配其他所有域名 *.qcloud.com

最常见的是将空间商提供的「IP地址」填写在这里
各类型的记录值一般是这样的：
A记录：填写您服务器 IP，如果您不知道，请咨询您的空间商
CNAME记录：填写空间商给您提供的域名，例如：qcloud.com
MX记录：填写您邮件服务器的IP地址或企业邮局给您提供的域名，如果您不知道，请咨询您的邮件服务提供商
NS记录：不常用。系统默认添加的两个NS记录请不要修改。NS向下授权，填写dns域名，例如：

2.3. View CNAME Record

You can view the added CNAME records in "Resolution" page and perform actions such as modify, manage.

2.4. Test Resolution Result

To test whether the domain is resolved normally, users can directly access the bound CNAME domain (such as www.qcloudtest.com mentioned in the example). Note: It will take about 10 minutes for the resolution to take effect.

SSL Certificate Format

Last updated：2018-06-01 17:16:11

1. How to apply for common certificates

- Generate private key locally: openssl genrsa -out privateKey.pem 2048, where privateKey.pem is your private key file. Please keep it well.
- Generate certificate request file: openssl req -new -key privateKey.pem -out server.csr, where server.csr is your certificate request file which is used to apply for certificate.
- Obtain the content of the request file and go to the CA site to apply for the certificate.

2. Certificate format

- The format of the certificate to be applied for is a .pem file under Linux environment. Load balancer does not support the certificates of other formats. For more information, please see "the certificate format supported by load balancer and conversion method" in this document.

- The certificate issued by root CA is unique. Without additional certificates, your configured site will be considered trusted by the browser and other accessing devices.

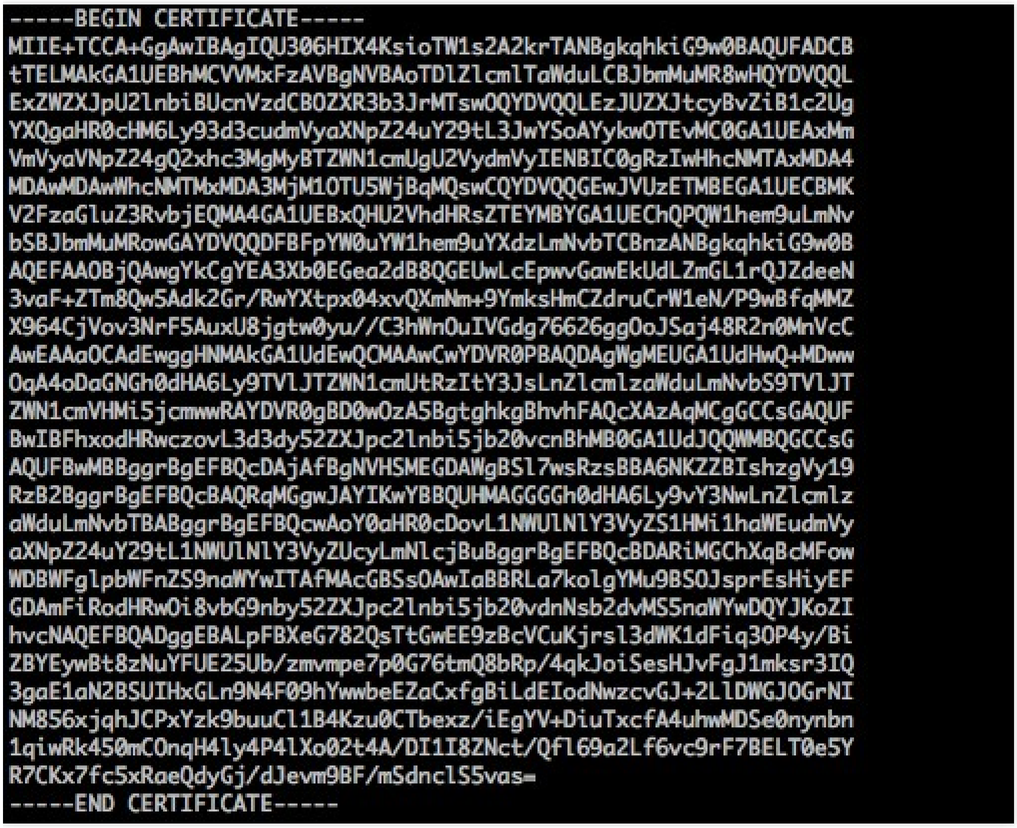
- The certificate file issued by an intermediate CA can contain multiple certificates. In this case, you need to manually concatenate the server certificate and intermediate certificates before uploading them.

- If your certificate has a certificate chain, convert its content into PEM format, and upload it along with the certificate content.

- Concatenation rule: The server certificate comes first, followed by the intermediate certificate. No blank line is allowed in between. Note: Generally, a CA provides instructions when issuing certificates. Make sure to carefully read the instructions.

Here are examples of certificate format and certificate chain format. Confirm that the formats are correct before uploading:

1. Certificate issued by root CA: Certificate is in the pem format under Linux environment. Example:



```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

Rules for certificate:

- [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] are the beginning and end, which should be uploaded with the content.

- Each line contains 64 characters, and the last line is limited to 64 characters.

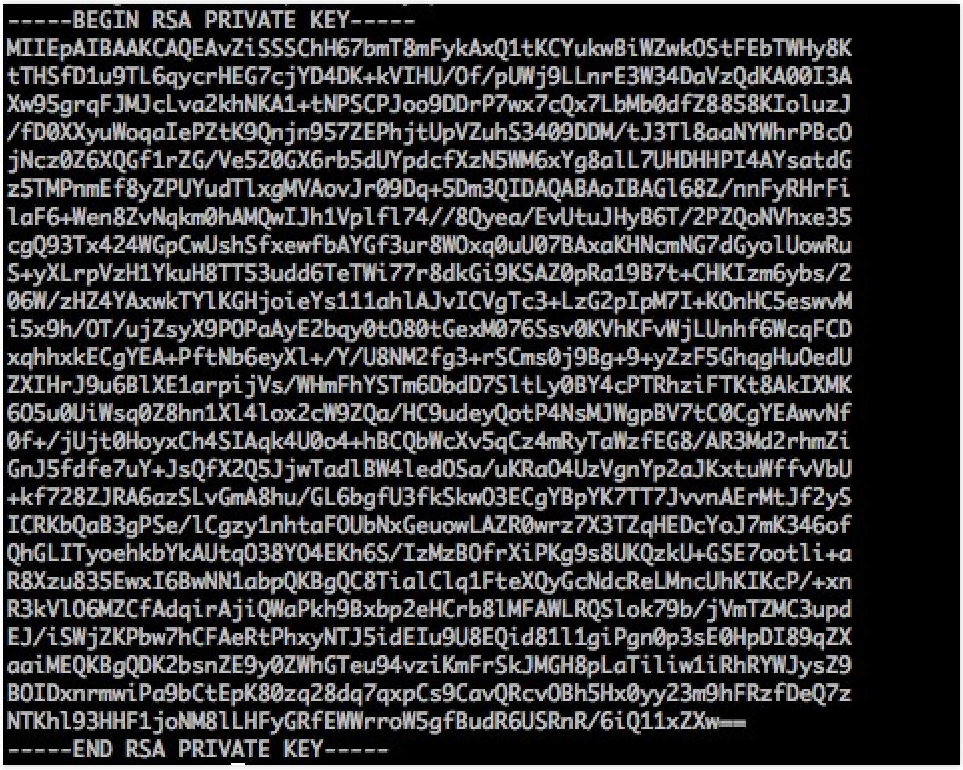
- Certificate chain issued by intermediate CA:
  ---BEGIN CERTIFICATE---
  ---END CERTIFICATE---
  ---BEGIN CERTIFICATE---
  ---END CERTIFICATE---
  ---BEGIN CERTIFICATE---
  ---END CERTIFICATE---

Rules for certificate chain:

- No blank line is allowed between certificates.
- Each certificate should comply with the certificate format rules described in Item 1.

3. RSA private key format

Example:



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K
tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A
Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ
/fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO
jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG
z5TMPnmEf8yZPUYudTlxgMVAovJr09Dq+5Dm3QIDAQABAoIBAGl68Z/nnFyRHrFi
laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35
cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8WOxq0uU07BAxaKHNcmNG7dGyolUowRu
S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2
06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM
i5x9h/OT/ujZsyX9POPaAyE2bqy0tO80tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD
xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHuOedU
ZXIHrJ9u6BlXE1arpijVs/WHmFhYSTm6DbdD7SltLy0BY4cPTRhziFTKt8AkIXMK
6O5u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf
0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi
GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU
+kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkwO3ECgYBpYK7TT7JvvnAErMtJf2yS
ICRKbQaB3gPSe/lCgzy1nhtaFOUbNxGeuowLAZR0wrz7X3TZqHEDcYoJ7mK346of
QhGLITyoehkbYkAUtqO38YO4EKh6S/IzMzBOfrXiPKg9s8UKQzkU+GSE7ootli+a
R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn
R3kVlO6MZCfAdqirAjiQWaPkh9Bxbp2eHCrb8lMFAWLRQSlok79b/jVmTZMC3upd
EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid81l1giPgn0p3sE0HpDI89qZX
aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9
BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcvOBh5Hx0yy23m9hFRzfDeQ7z
NTKhl93HHF1joNM8lLHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw==
-----END RSA PRIVATE KEY-----
```

RSA private key can include all private keys (RSA and DSA), public keys (RSA and DSA), and (x509) certificates. It stores DER data encoded with Base64 and is enclosed by ASCII header, thus is suitable for textual transfer between systems.

Rules for RSA private key:

- [---BEGIN RSA PRIVATE KEY---, ---END RSA PRIVATE KEY---] are the beginning and end, which should be uploaded with the content.
- Each line contains 64 characters, and the last line can contain less than 64 characters.

If the private key is not generated using the above method or has a format of [--- BEGIN PRIVATE KEY ---, --- END PRIVATE KEY ---], you can convert the format as follows:

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Then upload the content of new_server_key.pem along with the certificate.

4. How to convert certificate into PEM format

Load balancer only supports PEM certificates. Any certificate with other format must be converted to PEM format before being uploaded to load balancer. It is recommended to use openssl tool for the conversion. Here are some common methods for converting the certificate format to PEM.

4.1. Certificate conversion from DER format to PEM format

DER certificates are generally used on Java platforms.

Certificate conversion: `openssl x509 -inform der -in certificate.cer -out certificate.pem`

Private key conversion: `openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem`

4.2. Certificate conversion from P7B format to PEM format

P7B certificates are generally used in Windows Server and Tomcat.

Certificate conversion: `openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer`

Obtain [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] content in outcertificat.cer as a certificate for upload.

Private key conversion: Private key can be exported from IIS server

4.3. Certificate conversion from PFX format to PEM format

PFX certificates are generally used in Windows Server.

Certificate conversion: `openssl pkcs12 -in certname.pfx -nokeys -out cert.pem`

Private key conversion: `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`

4.4. Certificate conversion from CER/CRT format to PEM format

You can convert CER/CRT certificates by directly modifying the certificate file extension. For example, directly rename the certificate file "servertest.crt" to "servertest.pem" to complete the conversion.

Algorithms and Weight Configuration

Last updated：2017-12-15 16:28:57

1. Comparative analysis of Cloud Load Balancing Algorithm

1.1. Weighted Round-Robin Scheduling

- **Principle**: Round-Robin Scheduling means dispatching requests to different servers in sequence in a round-robin approach. By performing i = (i + 1) mod n for each dispatching request, the i server will be selected. Weighted Round-Robin Scheduling is used to solve problems caused by performance inconsistency issues between servers. It uses corresponding weight values to represent each server's performance level and distribute requests to the servers according to these weight values and round-robin method. Servers with high weight values will receive connections first. They process more connections than those with low weight values. Servers with the same weight value will process the same number of connections.

- **Advantage**: This scheduling method is simple and practical. There's no need to record the statuses of current connections. It's a stateless scheduling method.

- **Disadvantage**: Weighted Round-Robin Scheduling is relatively simple but isn't suitable for situations where the service time of a request changes a lot, or where each request needs a different time length. In these cases, this round-robin scheduling will cause imbalanced load distribution among servers.

- **Applicable Scenario**: Back-end service time needed by each request is relatively identical, in which case load distribution situation would be optimal. This is commonly used for short connection services, such as HTTP, etc.

- **Recommendation to Users**: If users have known that each request costs basically the same amount of back-end service time, and that the RS (real server) processes requests of the same type or of similar types, it is recommended to choose Weighted Round-Robin Scheduling. Weighted Round-Robin Scheduling is also recommended when the time needed by requests varies little, because this scheduling method costs little resource, has no need for traversing and is highly efficient.

1.2. Weighted Least-Connection Scheduling

- **Principle**: In practice, each request service from the client may stay at the server for different time lengths. If a simple round-robin or random balancing scheduling method is used, the numbers of connection processes on each server may vary greatly as time passes by, which means load balance is not actually achieved. Weighted Least-Connection Scheduling is a dynamic scheduling method which estimates a server's load situation according to its current number of active connections. Opposite from Round-Robin Scheduling, Weighted Least-Connection Scheduling is a dynamic scheduling method which estimates a server's load situation according to its current number of active connections. The scheduler needs to record the number of established connections for every server. This number increases by 1 when a request is dispatched to the server, and decreases by 1 when a connection is terminated or is timed out. Based on Least-Connection Scheduling, Weighted Least-Connection Scheduling assigns different weight values to servers based on their processing performance, which allows the servers to receive a number of service requests according to their weight values. This method is an improved version of the original Least-Connection Scheduling.

1) Assuming that the weight values for back-end servers are w1, w2...wi, and their numbers of current connections are c1, c2...ci, the values of ci/wi are calculated in succession, and the RS with the smallest value will be the next one to which the request will be distributed.

2) If there are RSs with the same ci/wi value, the scheduling will be done using Weighted Round-Robin Scheduling.

- **Advantage**: This balancing method is suitable for request services that need a long time to process, such as FTP, etc.

- **Disadvantage**: Due to API restrictions, currently you cannot enable Least-Connection and session persistence at the same time.

- **Applicable Scenario**: Back-end service time needed by each request varies greatly. This is commonly used for persistent connection services.

- **Recommendation to Users**: When users need to process different requests and the back-end service time needed by these requests varies greatly (such as 3ms and 3s), it is recommended to use Weighted Least-Connection Scheduling to achieve load balance.

1.3. Source Hashing Scheduling (ip_hash)

- **Principle**: Use the source IP address of the request as Hash Key and find the corresponding server from the statically distributed hash table. The request will be sent to this server if the server is available and not overloaded, otherwise the response will be empty.

- **Advantages**: ip_hash can achieve similar effects of the session persistence feature by remembering the source IP, so that requests from a certain client can be constantly mapped to the same RS through the hash table. Thus, ip_hash can be used for scheduling in scenarios where session persistence is not supported.

- **Recommendation to Users**: Hash the source address of the request and dispatch request to a matching server according to server weight. This will allow all requests from the same client IP to be constantly dispatched to a certain server. This scheduling method is suitable for TCP protocols for cloud load balancer without cookie feature.

2. Choosing Load Balance Scheduling Method and Configuring Weight

According to the new features of the upcoming cloud load balancer, ***Layer-7 forwarding will support the Least-Connection balance method.*** In order to allow RS clusters to undertake business in a stable manner in different scenarios, we've provided several reference cases regarding how to choose cloud load balance scheduling method and configure weight.

- Scenario 1:
  Suppose there are three RSs with the same configuration (CPU/RAM), since they have the same performance level, the user may configure their weight as 10. Now, each RS has established 100 TCP connections with clients. Then we add another RS. In this scenario, it is recommended for users to choose Least-Connection Scheduling, which will quickly distribute load to the fourth RS and lower pressure on the other three RSs.

- Scenario 2:
  Suppose a user has just begun to use Cloud Services, and the user website is relatively new and has low website load, it is recommended for the user to purchase RSs with the same configuration, because all RSs are identical access layer servers. In this scenario, the user can configure the weight for all RSs as 10 and use Weighted Round-Robin Scheduling to distribute traffic.

- Scenario 3:
  Suppose a user uses 5 servers to satisfy the access need for a simple static website, and the ratio of their computing capability is 9:3:3:3:1 (calculated by considering their CPUs and RAMs): In this scenario, the user can set the weights of these RSs as 90, 30, 30, 30, 10, respectively. Most access requests towards static websites are short connection requests, thus, by using Weighted Round-Robin Scheduling, the CLB will distribute requests according to the performance ratio of the RSs.

- Scenario 4:
  Suppose a user uses 10 RSs to support huge amount of Web access requests, and is not planning to

purchase additional RSs in order to save cost, and one of the RSs often restarts due to overload: In this scenario, it is recommended for the user to set up weight based on the performance levels of the RSs and set a relatively low weight value for the RS whose load is too high. In addition, the user can use Least-Connection cloud load balance method to distribute requests to RSs which have fewer active connections, in order to reduce pressure on the overloading RS.

- Scenario 5:

  Suppose a user uses 3 RSs to process several persistent connection requests, and the ratio of these servers' computing capability is 3:1:1 (calculated by considering their CPUs and RAMs). In this case, the server with the best performance processes more requests. To avoid overloading, the user hopes to distribute new requests to idle servers. In this scenario, the user can use Least-Connection balance method and lower the weight of the busy server by a certain extent, after which CLB will distribute requests to RSs with fewer active connections, achieving a balanced load distribution.

- Scenario 6:

  Suppose a user wishes that requests from subsequent clients can be distributed to the same server. However, Weighted Round-Robin or Weighted Least-Connection scheduling method cannot guarantee that requests from the same client will be distributed to the same server. In this scenario, in order to meet user's demand for specific application servers and ensure "stickiness" or "persistence" of client sessions, we can use ip_hash balance method to distribute traffic. This method ensures that requests from the same client are always distributed to the same RS. (Not including situations when there is a change in the number of servers, or the server becomes unavailable)