负载均衡

最佳实践

产品文档

腾讯云

文档目录

最佳实践
负载均衡开启Gzip配置及检测方法说明

最近更新时间：2017-12-15 16:09:22

在**公网应用型负载均衡、公网固定IP型负载均衡**实例中，**HTTP/HTTPS协议**默认支持用户开启gzip压缩功能。开启gzip功能对网页进行压缩，可以有效降低网络传输的数据量，提升客户端浏览器的访问速度。在使用过程中，需要注意以下事项：

1. 注意事项

- **需要后端CVM同步开启GZIP支持**
  对于常见的Nginx服务容器，必须在其配置文件（默认为nginx.conf）中，开启GZIP并重启服务

```
gzip on;
```

- **当前负载均衡支持的文件类型如下，您可以在gzip_types配置项中指定文件类型进行压缩**

```
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;
```

  注：负载均衡后端ECS业务软件中必须同步开启对上述文件类型的GZIP支持。
- **客户端请求中必须带有压缩请求标记**
  需要启用压缩，还要求客户端请求时必须携带如下标记：

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

2. 后端CVM开启GZIP流程支持示例

示例云服务器运行环境：Debian 6

1 . 使用vim依据用户路径打开Nginx配置文件：

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

2 . 找到如下代码：

```
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;
```

上述代码的语法详解：

gzip：开启或关闭gzip模块。

> 语法：gzip on/off
>
> 作用域：http, server, location

gzip_min_length：设置允许压缩的页面最小字节数，页面字节数从header头中的Content-Length中进行获取。默认值是1k。

> 语法：gzip_min_length **length**
>
> 作用域：http, server, location

gzip_buffers：设置系统获取几个单位的缓存用于存储gzip的压缩结果数据流。4 16k 代表以 16k 为单位，按照原始数据大小以 16k 为单位的4倍申请内存。

> **语法: gzip_buffers number size**
>
> 作用域: http, server, location

gzip_comp_level：gzip压缩比，范围为1~9。1 压缩比最小处理速度最快，9 压缩比最大但处理最慢（传输快但比较消耗cpu）。

> 语法: **gzip_comp_level** 1..9
>
> 作用域: http, server, location

gzip_http_level：代表可以使用gzip功能的HTTP最低版本，设置HTTP/1.0代表了需要使用gzip功能的HTTP最低版本，因此可以向上兼容HTTP/1.1。由于腾讯云现已全网支持HTTP/1.1，因此无需进行更改。

语法: gzip_http_version 1.0 | 1.1;
作用域: http, server, location

gzip_types：匹配MIME类型进行压缩，默认"text/html" 类型是会被压缩的。 此外，Nginx下的gzip默认不压缩javascript、图片等静态资源文件，可以通过gzip_types指定需要压缩的MIME类型,非设置值则不进行压缩 ***例如，如果需要对json格式数据进行压缩，则需要在此语句中添加application/json类型数据***
支持的类型如下：

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

语法: gzip_types mime-type [mime-type ...]
作用域: http, server, location

3 . 如对配置有修改，则首先将文件保存退出，进入到Nginx bin文件目录，执行如下命令重新加载Nginx

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

4 . 最后使用curl命令测试gzip是否成功开启

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

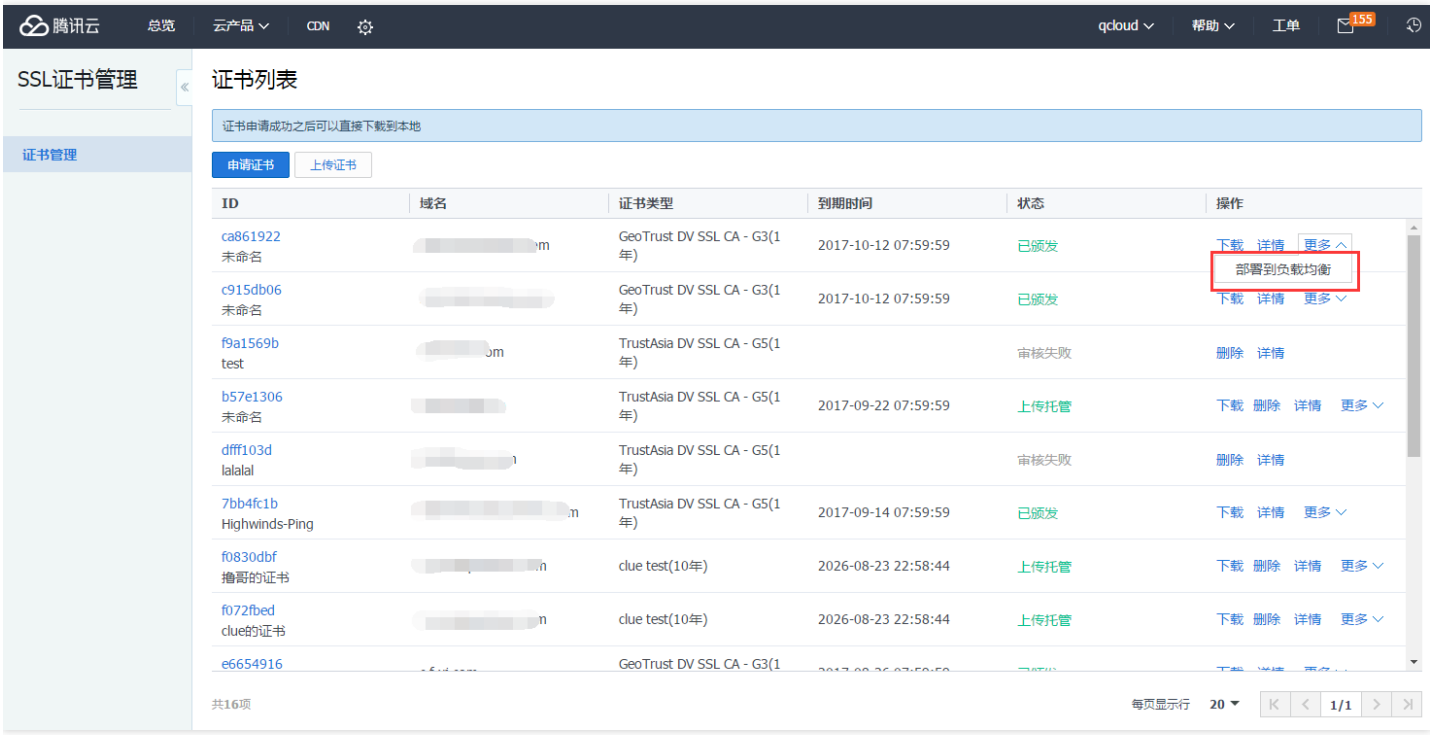
部署证书到负载均衡

最近更新时间：2017-12-05 17:20:43

SSL证书支持部署到负载均衡，步骤如下所示：

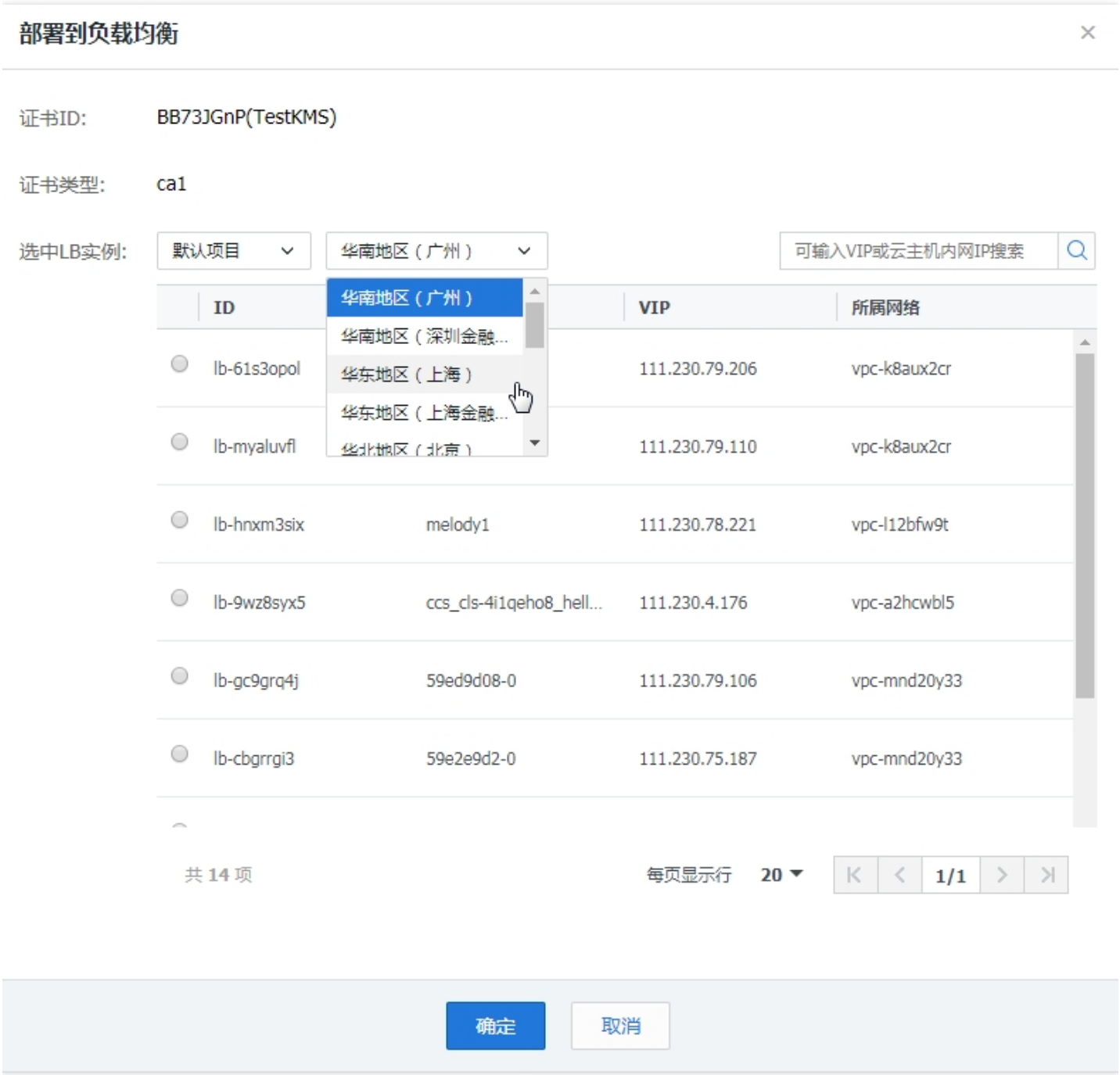
1. 选择证书

首先成功申请获取证书（参考如何免费申请域名型证书），或者选择上传的证书，展开【更多】操作，选择【部署到负载均衡】。



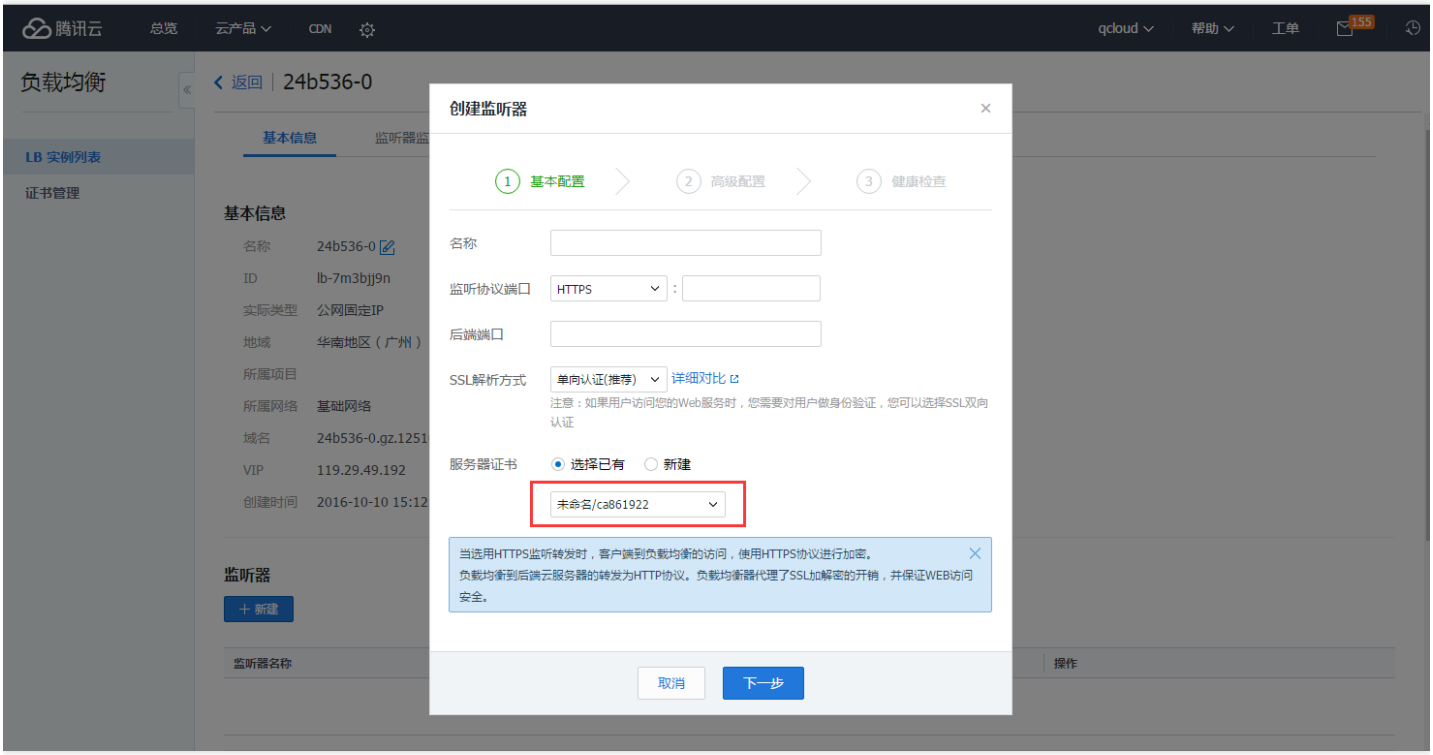
2. 选择LB实例

根据项目和地区筛选LB实例，且只能选择一个实例。



3. 创建监听器

跳转到负载均衡控制台，打开创建监听器弹窗，并且监听协议端口已切换到HTTPS，服务器证书为已选中的证书，然后完成剩余的基本配置。



4. 继续完成配置

继续完成创建监听器的其他配置，即可实现负载均衡的HTTPS转发。

HTTPS 证书申请流程

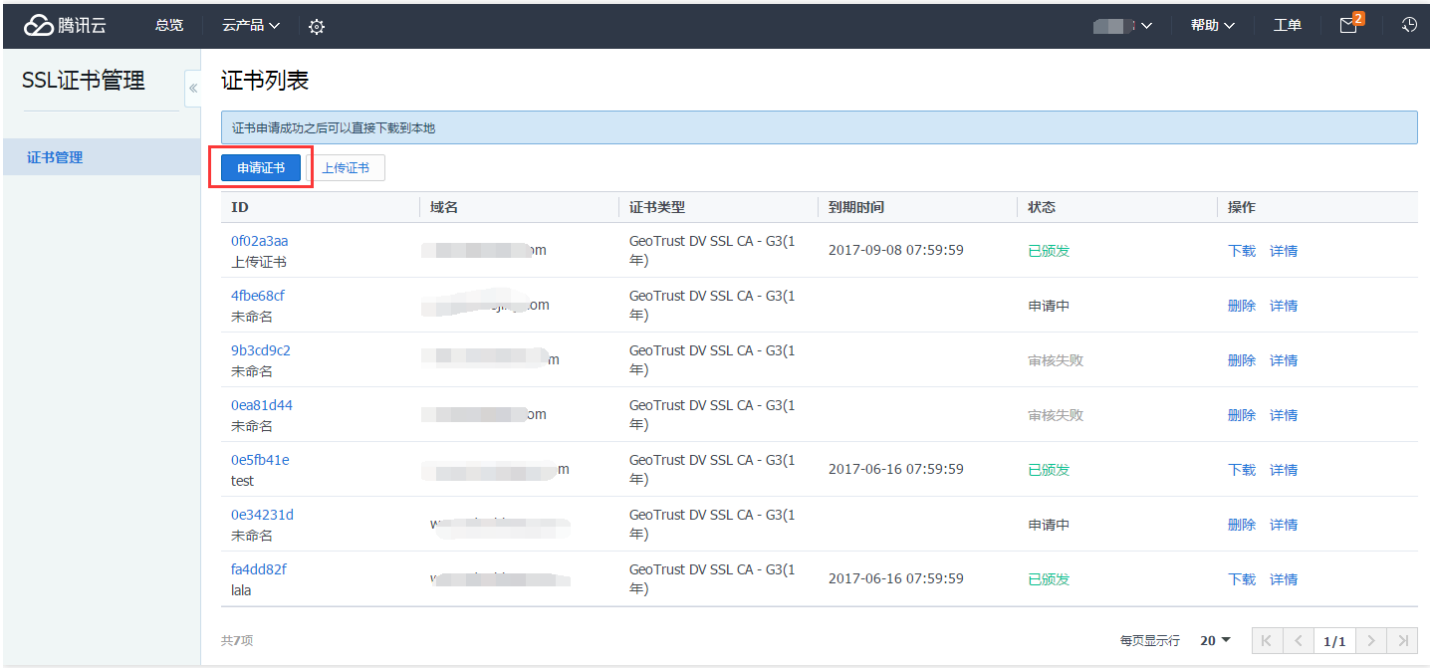
最近更新时间：2018-05-28 18:22:50

申请域名型（DV）SSL证书

1. 申请入口

进入SSL证书管理控制台

单击【申请证书】



查看申请域名型证书型号，单击【确定】

2. 填写申请

填写申请域名，注意不支持一级域名申请（例如qcloud.com），请填写例如cloud.tencent.com，demo.test.qlcoud.com形式二级、三级等域名。

3. DNS验证

3.1 手动DNS验证方式

证书默认支持收到DNS验证，验证方法可查看详情。

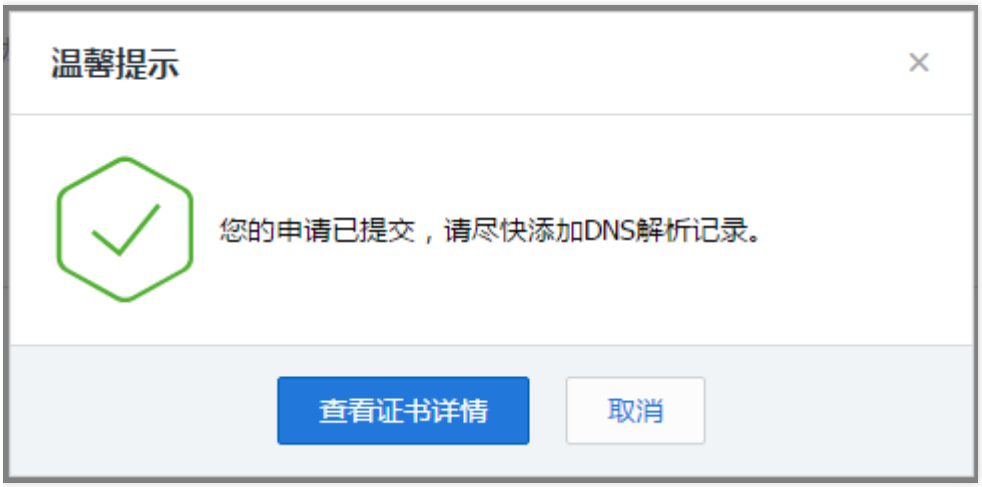
3.2 选择自动DNS验证方式

如果所申请域名成功添加云解析平台，可以支持自动DNS验证，验证方法可查看详情。

4. 提交申请

4.1 提交申请后验证身份

提交申请成功后弹窗提示如下，需要前往【证书详情页】获取CName记录添加解析：



获取CName记录如Tips中显示，需要尽快成功添加解析，方可通过CA机构审核：

4.2 提交申请失败

如遇到下图所示弹窗，是提交域名未通过CA机构安全审核，具体原因参考安全审核失败原因。

HTTPS转发配置入门指南

最近更新时间：2018-08-23 16:04:52

1. 负载均衡能力说明

腾讯云 CLB 负载均衡器通过对协议栈及服务端的深度优化，实现了 HTTPS 性能的巨大提升。同时，我们也通过证书的国际合作，极大降低了证书的成本。腾讯云 CLB 在如下几个方面能够为业务带来非常显著的收益：

1. 使用 HTTPS 并不会降低 Client 端的访问速度。
2. 集群内单台服务器 SSL 加解密性能，高达 6.5W cps 的完全握手。相比高性能 CPU 提升了至少3.5倍，节省了服务端成本，极大提升了业务运营及流量突涨时的服务能力，增强了计算型的防攻击能力。
3. 支持多种协议卸载及转换。减少业务适配客户端各种协议的压力，业务后端只需要支持 HTTP1.1 就能使用 HTTP2、SPDY、SSL3.0 及 TLS1.2等各版本协议。
4. 一站式 SSL 证书申请、监控、替换。我们和国际顶级的证书厂商 comodo，symantec 展开对话，探讨合作，大幅缩减证书申请流程及成本。
5. 防 CC 及 WAF 功能。能够有效杜绝慢连接、高频定点攻击、SQL 注入、网页挂马等应用层攻击。

2. HTTP、HTTPS 头部标识

CLB 对 HTTPS 进行代理，无论是 HTTP 还是 HTTPS 请求，到了 CLB 转发给后端 CVM 时，都是 HTTP 请求。这时开发者无法分辨前端的请求是 HTTP 还是 HTTPS。

腾讯云 CLB 在将请求转发给后端 CVM 时，头部 header 会植入 X-Client-Proto：

X-Client-Proto: HTTP（前端为 HTTP 请求）
X-Client-Proto: HTTPS（前端为 HTTPS 请求）

3. 入门配置

假定用户需要配置网站 https://example.com 。开发者希望用户在浏览器中输入网址时，直接键入 www.example.com 即可通过 HTTPS 协议安全访问。

此时用户输入的 www.example.com 请求转发流程如下：

1. 该请求以 HTTP 协议传输，通过 VIP 访问负载均衡监听器的 80 端口，并被转发到后端云服务器的 8080 端口。

2. 通过在腾讯云后端服务器的 nginx 上配置 rewrite 操作，该请求经过 8080 端口，并被重写到 https://example.com 页面。

3. 此时浏览器再次发送 https://example.com 请求到相应的 HTTPS 站点，该请求通过 VIP 访问负载均衡监听器的 443 端口，并被转发到后端云服务器的 80 端口。

至此，请求转发完成。

该操作在浏览器用户未感知的情况下，将用户的 HTTP 请求重写为更加安全的 HTTPS 请求。为实现以上请求转发操作，用户可以对后端服务器做如下配置：

```
server {

listen 80;
server_name example.qcloud.com;

location / {

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

}
}
```

或者在nginx新版本中，采用推荐的301重定向配置方法，将nginx HTTP 页面重定向到 HTTPS 页面：

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

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

七层转发获取来访真实IP的方法

最近更新时间：2018-06-12 17:29:58

- 由于4层负载均衡（TCP协议）服务可以直接在后端CVM上获取来访者真实IP地址，无需进行额外的配置，以下介绍的内容均是针对7层（HTTP协议）的负载均衡服务而言。
- 7层负载均衡系统提供X-Forwarded-For的方式获取访问者真实IP，LB侧默认开启，需要后端服务做相应配置来获取client IP。

以下针对常见的应用服务器配置方案进行介绍。

1. IIS 6 配置方案

1) 安装插件F5XForwardedFor.dll，根据自己的服务器操作系统版本将x86\Release或者x64\Release目录下的 F5XForwardedFor.dll 拷贝到某个目录，这里假设为 C:\ISAPIFilters ，同时确保对IIS进程对该目录有读取权限。

2) 打开IIS管理器，找到当前开启的网站，在该网站上右键选择“属性”，打开属性页。

3) 在属性页切换至“ISAPI筛选器”，单击“添加”按钮，出现添加窗口。

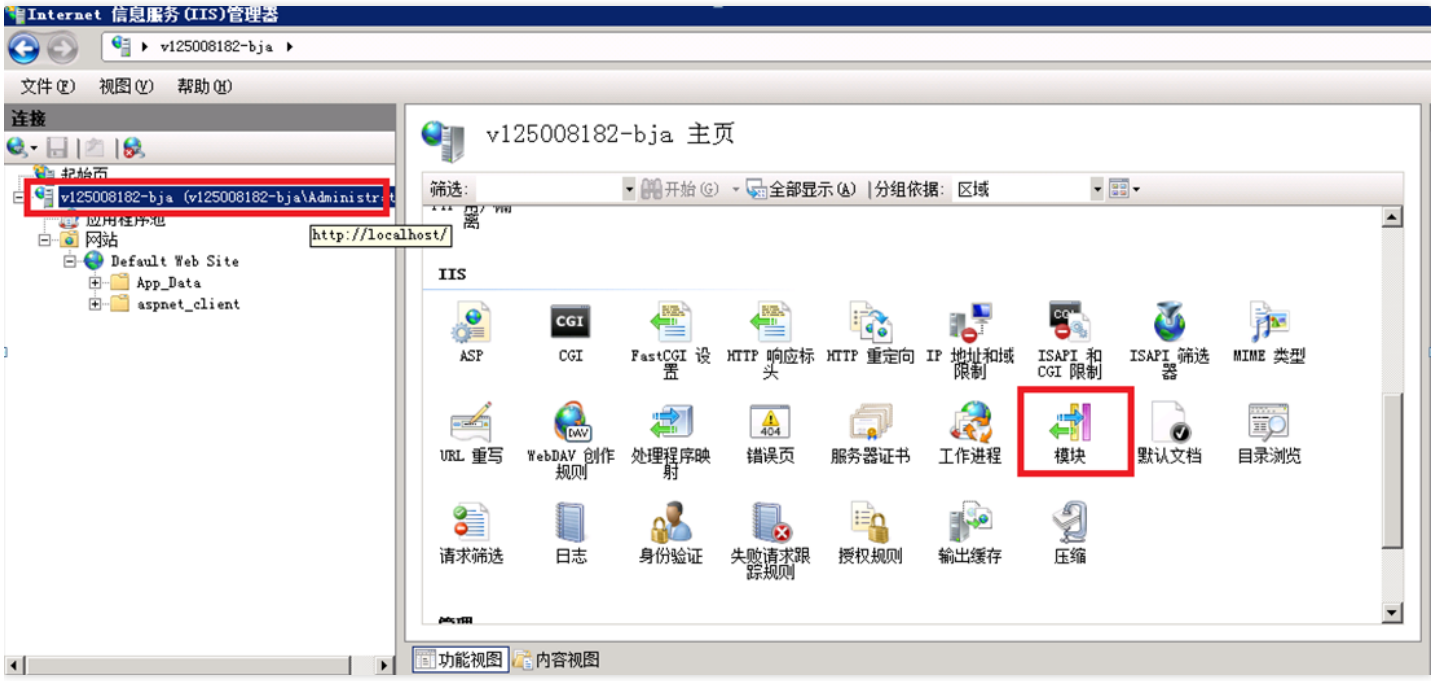
4) 在添加窗口“筛选器名称”填写“F5XForwardedFor”，“可执行文件”填写 F5XForwardedFor.dll 的完整路径，单击确定。

5) 重启IIS服务器，等待配置生效。

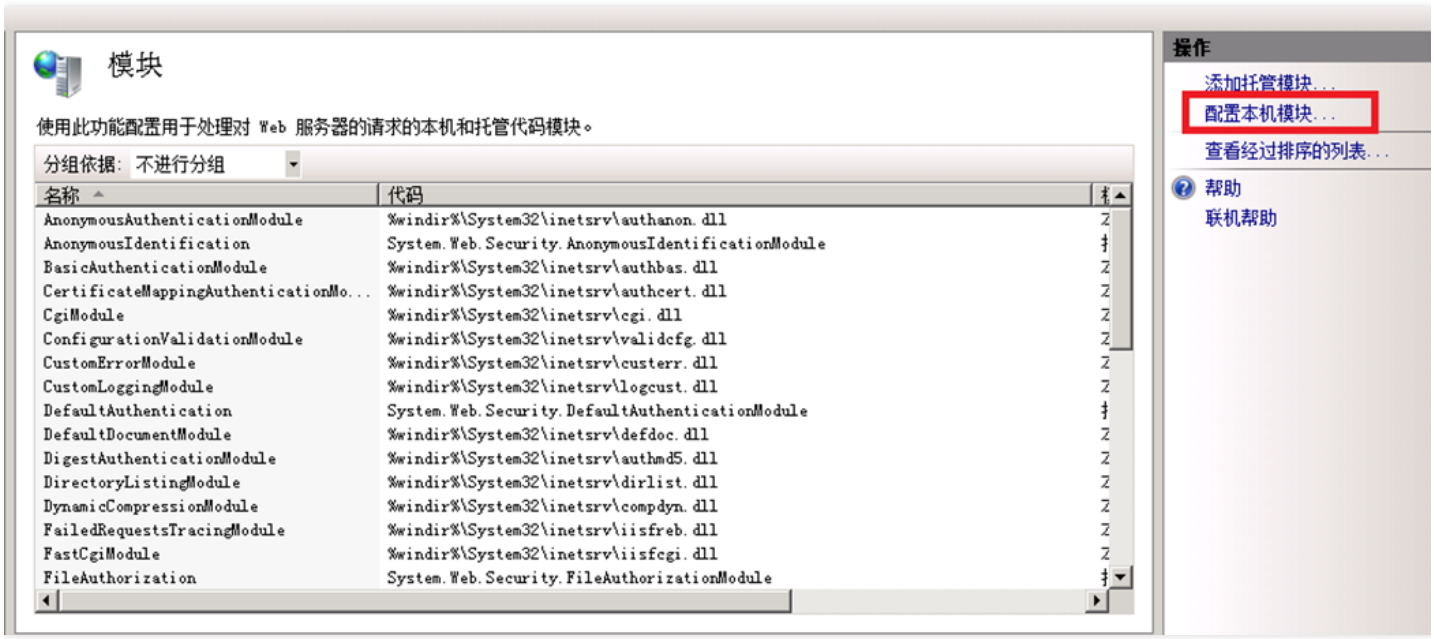
2. IIS 7 配置方案

1) 下载与安装插件F5XForwardedFor模块，根据自己的服务器操作系统版本将 x86\Release 或者 x64\Release 目录下的 F5XFFHttpModule.dll 和 F5XFFHttpModule.ini 拷贝到某个目录，这里假设为 C: \F5XForwardedFor ，确保对IIS进程对该目录有读取权限。

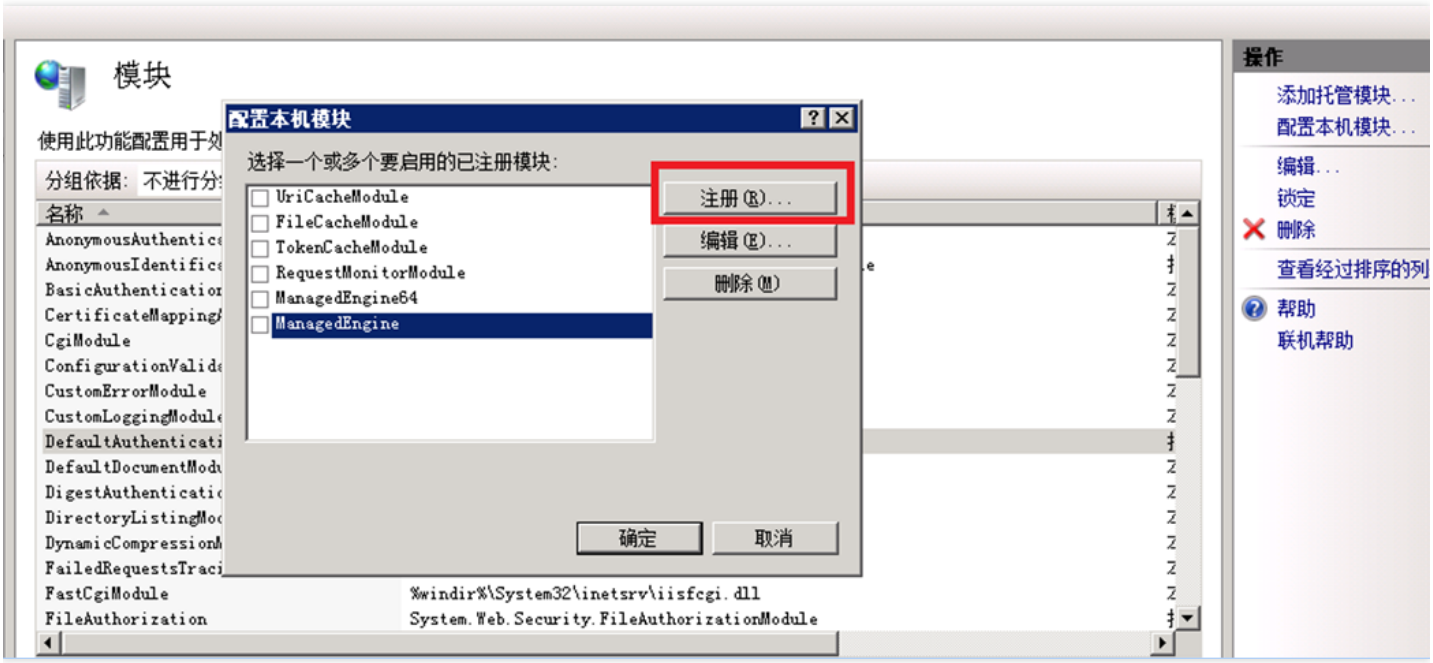
2) 选择“IIS服务器”选项，按图所示选择“模块”功能：



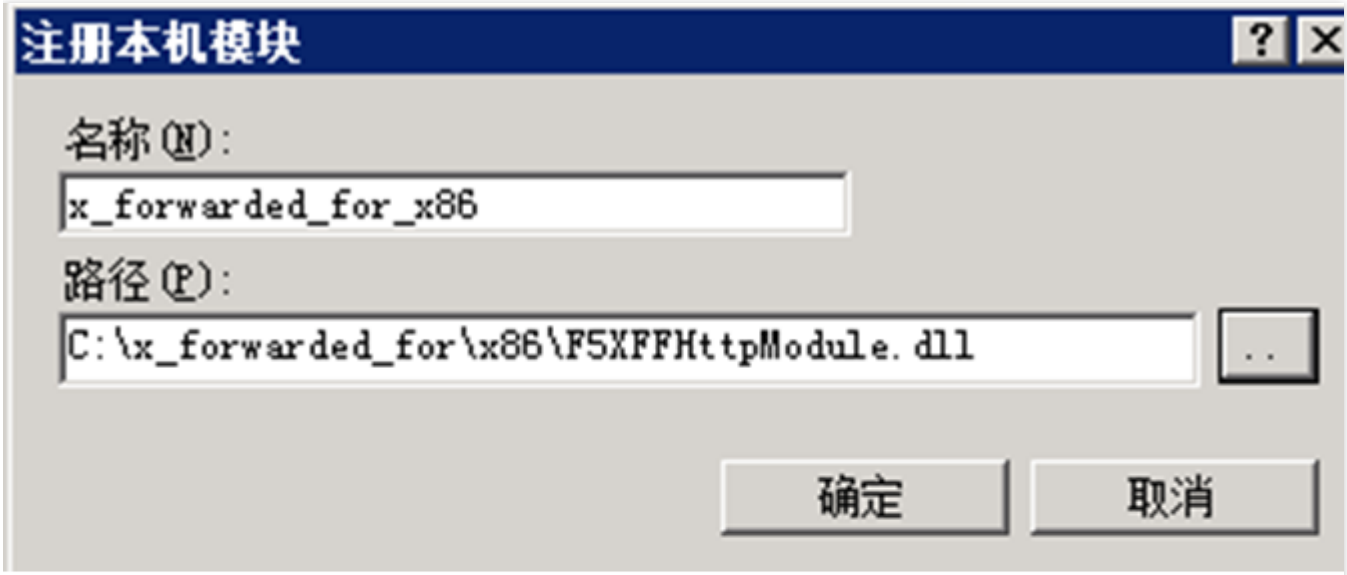
3) 双击“模块”功能，单击“配置本机模块”：



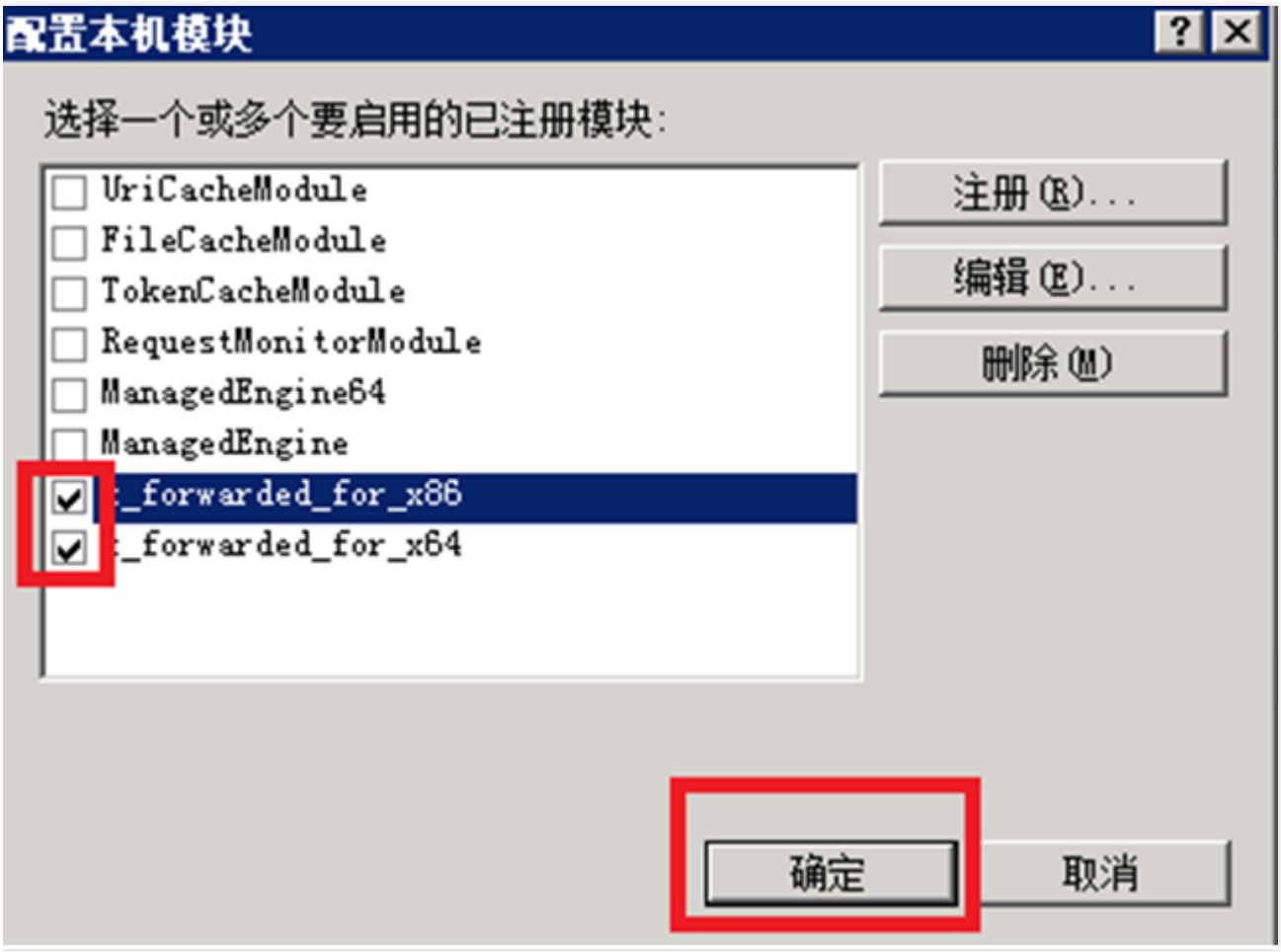
4) 在弹出框中单击“注册”按钮：



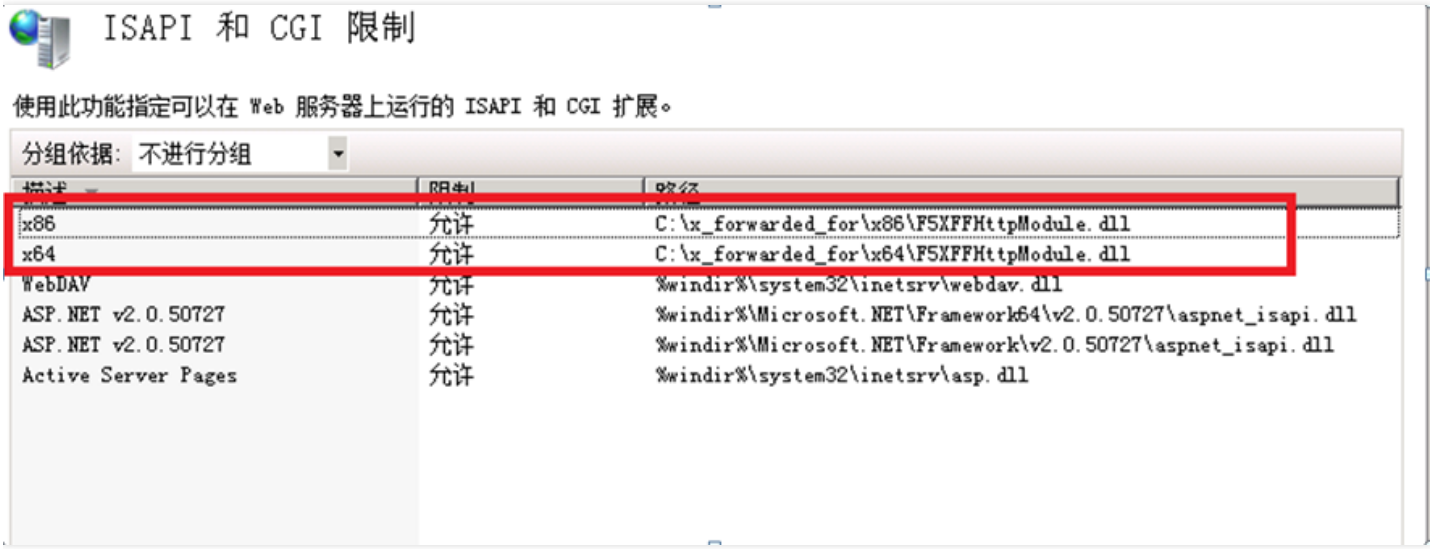
5) 添加下载的DLL文件，如下图：



6) 添加完成后，勾选并单击“确定”：



7) 把这两个DLL在 “API 和CGI限制”进行添加，并改为允许：



8) 重启IIS服务器，等待配置生效。

3. Apache配置方案

1) 安装apache第三方模块“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) 修改apache配置 `/etc/httpd/conf/httpd.conf` ，在最末尾添加：

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips IP地址（这个IP地址首先不是负载均衡提供的公网IP，具体IP多少可以看一下apache日志，通常会有2个 都要写上）
RPAFheader X-Forwarded-For
```

3) 添加完成后重启apache

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

4. Nginx配置方案

1) Nginx作为负载均衡获取真实IP是使用http_realip_module，默认安装的Nginx是没有安装这个模块的，需要重新编译Nginx增加 --with-http_realip_module：

```
wget http://nginx.org/download/nginx-1.14.0.tar.gz
tar zxvf nginx-1.14.0.tar.gz
cd nginx-1.14.0
./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) 修改nginx.conf

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

修改如下红色部分：

```
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地址;（这个IP地址首先不是负载均衡提供的公网IP，具体IP多少可以看一下之前nginx日志，
real_ip_header X-Forwarded-For;
```

3) 重启nginx

```
service nginx restart
```

内网CLB关于SNAT与非SANT的说明

最近更新时间：2017-03-24 16:00:18

从2016年12.15日起，新购买的私有网络下内网型负载均衡（选择私有网络VPC）不再进行SNAT处理，即从server端获取的访问ip，为客户端的真实ip。为了保证您的业务运行正常，请注意以下事项：

- 1、 对于15日后新购买的内网型CLB，当开启安全组策略后，必须放通所有的client ip的入规则，以保证正常访问。
- 2、 存量的内网型CLB，如有需要，可向售后团队提交工单，进行切换。切换后，从server端获取的访问ip，为client端ip。切换过程中不会出现业务中断

多可用区高可用配置说明

最近更新时间：2017-03-28 10:44:21

负载均衡器多可用区高可用

CLB负载均衡器支持『多可用区容灾』的能力，如在深圳一区、二区金融两个可用区（同一个地域），会分别部署多套集群，以实现同Region下的跨可用区容灾。通过该特性可实现当整个可用区故障时，负载均衡10s内，将前端访问流量切换到同一地域下的其它可用区，以恢复服务能力

具体场景&疑问解答

疑问1：深圳金融区A、B，有负载均衡器test1，client端公网入流量的策略是？

- 答：在深圳一区、二区机房，有一对ip资源池，可理解为对等的ip资源。开发者无需理解，一区，二区哪个是主集群，哪个是备集群，两个集群拥有同等的负载能力。当开发者购买负载均衡器，并绑定CVM时，会生成两套规则写入套集群，此时就已经获得了高可用能力。

疑问2：深圳金融区A、B，有负载均衡器test1，后端在A、B可用区各绑定了100台服务器。业务运行中，各建立100万HTTP长连接（TCP连接不关闭）。此时当金融区A的负载均衡器集群整体瘫痪，不可用时，业务的感受是？

- 答：当金融区A的负载均衡器失去服务能力后，当前的所有长连接会断开，短连接不受影响。容灾架构会在10s内，将A/B区的各100台服务器，会立刻自动绑定到金融区B的负载均衡器上，业务能力立即恢复，无需人工介入。

疑问3：『多可用区容灾』的能力，支持哪种类型的负载均衡器，会额外收费么？

- 目前多可用区是免费的，不会额外收取费用。应用型CLB、公网固定IP型CLB已支持。支持http/https/tcp/udp等协议

注册域名并添加CNAME记录的方法

最近更新时间：2018-08-23 16:06:37

目前负载均衡**公网有固定 IP 型产品**支持 A 记录和 CNAME 的绑定，用户可通过注册域名并添加 A 记录和 CNAME 记录进行访问。

1. 域名注册

注册域名可以通过 域名注册页面 进行域名查询和注册。

相关文档可以参考 如何注册域名。

2. 添加 CNAME 记录

2.1. 进入域名解析页面

登录腾讯云【管理中心】>【云产品】>【域名管理】>【解析】，示例的主域名为 qcloudtest.com。

2.2. 添加 CNAME 记录

在【解析】页面，单击【添加】，用户可以添加 CNAME 记录，操作指引如下：

a. 主机记录可以按照需求说明填写：
主机记录就是域名前缀，常见用法有：

- www：解析后的域名为 www.qcloudtest.com
- @：直接解析主域名 qcloudtest.com
- *：泛解析，匹配其他所有域名 *.qcloudtest.com

b. 记录类型用户可选 CNAME 记录
各个记录类型如下：

- A 记录：地址记录，用来指定域名的 IPv4 地址（如：8.8.8.8），如果需要将域名指向一个 IP 地址，就需要添加 A 记录。
- CNAME： 如果需要将域名指向另一个域名，再由另一个域名提供 IP 地址，就需要添加 CNAME 记录。
- TXT：在这里可以填写任何东西，长度限制 255。绝大多数的TXT记录是用来做 SPF 记录（反垃圾邮件）。
- NS：域名服务器记录，如果需要把子域名交给其他DNS服务商解析，就需要添加 NS 记录。
- AAAA：用来指定主机名（或域名）对应的 IPv6 地址（例如：ff06:0:0:0:0:0:0:c3）记录。
- MX：如果需要设置邮箱，让邮箱能收到邮件，就需要添加MX记录。
- 显性 URL：从一个地址301重定向到另一个地址的时候，就需要添加显性 URL 记录（注：DNSPod 目前只支持301重定向）。
- 隐性 URL：类似于显性URL，区别在于隐性 URL 不会改变地址栏中的域名。
- SRV：记录了哪台计算机提供了哪个服务。格式为：服务的名字、点、协议的类型，例如：_xmpp-server._tcp。

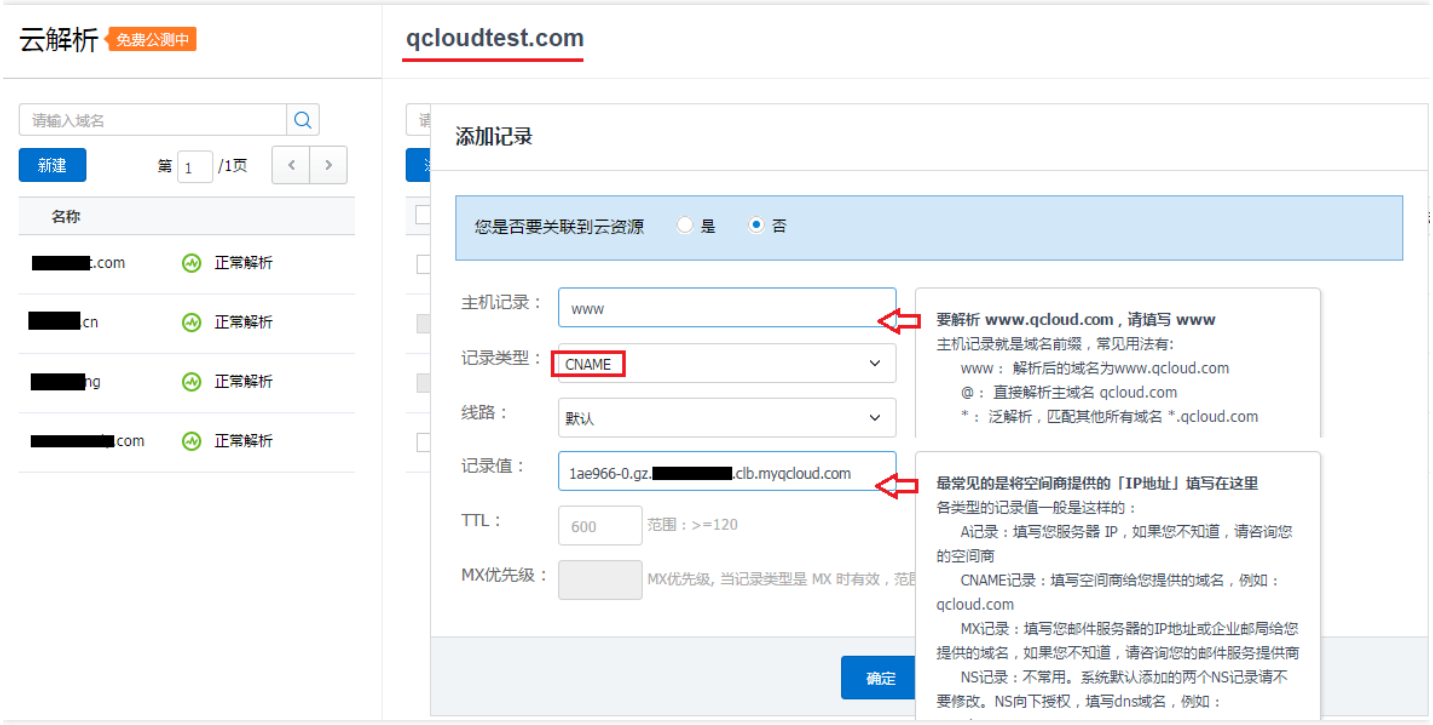
c. 线路是为了让指定线路的用户访问这个 IP
若空间商只提供了一个 IP 地址或域名，选择「默认」即可。
常见用法有：

- 默认：必须添加，否则只有单独指定的线路才能访问您的网站。如果双线解析，建议「默认」线路填写「电信 IP」。
- 联通：单独为「联通用户」指定服务器 IP，其他用户依然访问「默认」。
- 搜索引擎：指定一个服务器 IP 让蜘蛛抓取。

d. CNAME 记录值主要填写空间商给您提供的域名。
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：负载均衡中 LB 实例的域名1b16c9-0.ap-guangzhou.12345678.clb.myqcloud.com。**
- MX 记录：填写您邮件服务器的 IP 地址或企业邮箱给您提供的域名，如果您不知道，请咨询您的邮件服务提供商。
- TXT 记录：一般用于 Google、QQ 等企业邮箱的反垃圾邮件设置。
- 显性 URL 记录：填写要跳转到的网址，例如：http://cloud.tencent.com 。
- 隐性 URL 记录：填写要引用内容的网址，例如：http://cloud.tencent.com 。
- AAAA：不常用。解析到 IPv6 的地址。
- 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：f1g1ns1.dnspod.net。
- SRV 记录：不常用。格式为：优先级、空格、权重、空格、端口、空格、主机名，记录生成后会自动在域名后面补一个“.”，这是正常现象。例如：5 0 5269 xmpp-server.l.google.com.

其余值可以按照默认进行操作。添加完毕后，单击【确定】。



2.3. 查看 CNAME 记录

添加记录完毕后，可以在【解析】页面查看所添加的 CNAME 记录，并对其进行修改、管理等操作。

2.4. 测试解析结果

用户为测试域名是否解析正常，可以直接访问绑定后的 CNAME 域名（如例子中的www.qcloudtest.com ）。

注意:
解析大概需要十分钟左右生效。

SSL证书格式要求及格式转换说明

最近更新时间：2018-06-01 17:16:11

1. 常用证书申请流程

- 本地生成私钥:openssl genrsa -out privateKey.pem 2048 其中privateKey.pem为您的私钥文件，请妥善保管
- 生成证书请求文件:openssl req -new -key privateKey.pem -out server.csr 其中server.csr是您的证书请求文件，可用其去申请证书
- 获取请求文件中的内容前往CA等机构站点申请证书

2. 证书格式要求

- 用户要申请的证书为：linux环境下pem格式的证书。负载均衡不支持其他格式的证书，如是其它格式的证书请参考本文 “负载均衡支持的证书格式及转换方式” 部分内容。
- 如果是通过root CA机构颁发的证书， 您拿到的证书为唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。
- 如果是通过中级CA机构颁发的证书，您拿到的证书文件包含多份证书，需要人为的将服务器证书与中间证书合并在一起上传。
- 当您的证书有证书链时，请将证书链内容，转化为PEM格式内容，与证书内容合并上传。
- 拼接规则为：服务器证书放第一份，中间证书放第二份，中间不要有空行。注：一般情况下，机构在颁发证书的时候会有对应说明， 请注意规则说明。

以下为证书格式和证书链格式范例，请确认格式正确后上传：

1、root CA机构颁发的证书：证书格式为linux环境下pem格式。样例如下：

```
-----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-----
```

证书规则为：

- [———-BEGIN CERTIFICATE———-, ———-END CERTIFICATE———-] 开头和结尾；请将这些内容一并上传；
- 每行64字符，最后一行不超过64字符；

2、中级机构颁发的证书链：

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

证书链规则：

- 证书之间不能有空行；
- 每一份证书遵守第一点关于证书的格式说明；

3. RSA私钥格式要求

样例如下：

rsa私钥可以包括所有私钥（RSA 和 DSA）、公钥（RSA 和 DSA）和 (x509) 证书。它存储用 Base64 编码的 DER 格式数据，用 ascii 报头包围，因此适合系统之间的文本模式传输。

rsa私钥规则：

- [———-BEGIN RSA PRIVATE KEY———-, ———-END RSA PRIVATE KEY———-] 开头结尾；请将这些内容一并上传；
- 每行64字符，最后一行长度可以不足64字符。

如果您不是按照上述方案生成私钥，得到[———-BEGIN PRIVATE KEY———-, ———-END PRIVATE KEY———-] 这种样式的私钥，您可以按照如下方式转换：

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

然后将new_server_key.pem的内容与证书一起上传。

4. 证书转换为PEM格式说明

目前负载均衡只支持PEM格式的证书，其他格式的证书需要转换成PEM格式后才能上传到负载均衡中，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为PEM格式的方法。

4.1. DER格式证书转换为PEM格式

DER格式一般出现在java平台中。

证书转换： `openssl x509 -inform der -in certificate.cer -out certificate.pem`

私钥转换： `openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem`

4.2. P7B格式证书转换为PEM格式

P7B格式一般出现在windows server和tomcat中。

证书转换： `openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer`

获取outcertificat.cer里面 [——-BEGIN CERTIFICATE——-， ——-END CERTIFICATE——-] 的内容作为证书上传。

私钥转换：私钥一般在IIS服务器里可导出

4.3. PFX格式证书转换为PEM格式

PFX格式一般出现在windows server中。

证书转换： `openssl pkcs12 -in certname.pfx -nokeys -out cert.pem`

私钥转换： `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`

4.4. CER/CRT格式证书转换为PEM格式

对于 CER/CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将“servertest.crt”证书文件直接重命名为“servertest.pem”即可。

均衡算法选择与权重配置实例

最近更新时间：2017-12-15 16:28:57

1. 负载均衡算法比较分析

1.1. 加权轮询算法 Weighted Round-Robin Scheduling

- **原理**：轮叫调度算法就是以轮叫的方式依次将请求调度不同的服务器，即每次调度执行i = (i + 1) mod n，选出第i台服务器。加权轮叫调度算法可以解决服务器间性能不一的情况，它用相应的权值表示服务器的处理性能，按权值的高低和轮叫方式分配请求到各服务器。权值高的服务器先收到的连接，权值高的服务器比权值低的服务器处理更多的连接，相同权值的服务器处理相同数目的连接数。

- **优势**：算法的优点是其简洁性，和实用性。它无需记录当前所有连接的状态，所以它是一种无状态调度。

- **劣势**：加权轮叫调度算法相对简单，但不适用于请求服务时间变化比较大，或者每个请求所消耗的时间不一致的情况，此时轮叫调度算法容易导致服务器间的负载不平衡。

- **适用场景**：每个请求所占用的后端时间基本相同，负载情况最好。常用于短连接服务，例如 HTTP 等服务。

- **用户推荐**：用户可知每个请求所占用后端时间基本相同时，如已知rs处理的都是同类型或者相似类型的请求时，推荐选择加权轮询的方式。当请求时间相差较小时也推荐使用加权轮询的方式，因为该实现方式消耗小，无需遍历，效率较高。

1.2. 加权最小连接数 Weighted Least-Connection Scheduling

- **原理**：在实际情况中，客户端的每一次请求服务在服务器停留的时间可能会有较大的差异，随着工作时间的延伸，如果采用简单的轮询或随机均衡算法，每一台服务器上的连接进程数目可能会产生极大的不同，这样实际上并没有达到真正的负载均衡。最小连接调度是一种动态调度算法，它通过服务器当前所活跃的连接数来估计服务器的负载情况。与轮询调度算法相反，最小连接调度是一种动态调度算法，它通过服务器当前所活跃的连接数来估计服务器的负载情况。调度器需要记录各个服务器已建立连接的数目，当一个请求被调度到某台服务器，其连接数加1; 当连接中止或超时，其连接数减一。权重最少连接数调度算法是在做少连接数调度算法的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权值，使其能够接受相应权值数的服务请求，是在最少连接数调度算法的基础上的改进。
  1）假设各台rs的权值依次为wi,当前连接数依次为ci,依次计算ci/wi,值最小的rs作为下一个分配的rs
  2）如果存在ci/wi相同的rs，这些rs再使用加权轮训的方式调度

- **优势**：此种均衡算法适合长时处理的请求服务，如FTP等应用。

- **劣势**：由于接口限制，目前最小连接数和会话保持功能不能同时开启。
- **适用场景**：每个请求所占用的后端时间相差较大的场景。常用于长连接服务。
- **用户推荐**：如果用户需要处理不同的请求，且请求所占用后端时间相差较大，如3ms和3s这种数量级的差距时，推荐使用加权最小连接数算法实现负载均衡。

1.3. 源地址散列调度算法 ip_hash

- **原理**：根据请求的源IP地址，作为散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则返回空
- **优势**：ip_hash可以实现部分会话保持的效果，能够记住源ip，使某一client请求通过hash表一直映射在同一台rs上。因此在不支持会话保持的场景可以使用ip_hash进行调度。
- **用户推荐**：将请求的源地址进行hash运算，并结合后端的服务器的权重派发请求至某匹配的服务器，这可以使得同一个客户端IP的请求始终被派发至某特定的服务器。该方式适合负载均衡无cookie功能的TCP协议。

2. 均衡算法选取及权重配置实例

在负载均衡即将发布的新功能中，***七层转发将支持最小连接数的均衡方式***，为了让用户在不同场景下，能够让RS集群稳定的承接业务，因此我们给出几个负载均衡选择与权重配置的实例供用户进行参考。

- 场景1：

  设有3台配置相同（CPU / 内存）的RS，由于性能一致，用户可以将RS权重都设置为10。设现在每台RS与client端建立了100个TCP链接，此时新增1台RS。在此场景下，推荐用户使用最小连接数的均衡方式，这种配置能快速的让第四台RS的负载提升，降低另外3台RS的压力。

- 场景2：

  设用户首次接触云服务，且建站时间不长，网站负载较低，则建议购买相同配置的RS，因此RS都是无差别的接入层服务器。在此场景下，用户可以将RS权重都设为10，采用加权轮询的均衡方式进行流量分发。

- 场景3：

  用户有5台服务器，用与承载简单的静态网站访问，且5台服务器的计算能力的比例为 9：3：3：3：1（按CPU、内存换算）。在此场景下，用户可以依次将RS权重比例设置为90，30，30，30，10，由于静态网站访问大多数是短连接请求，因此可以采用加权轮询的均衡方式，让CLB按RS的性能比例分配请求。

- 场景4：

  某用户有10台RS用于承担海量的WEB访问请求，且不希望多购置RS增加支出。 某台RS经常会因为负载过高，导致服务器重启。在此场景下，建议用户根据RS的性能进行相应的权重设置，给负载过高的RS设置较小的权值。除此之外，可以采用最小连接数的负载均衡方式，将请求分配到活跃连接数较少的RS上，从而解决某台RS负载过高的问题。

- 场景5：

  某用户有3台RS用于处理若干长连接请求，且这3太服务器的计算能力比例为3：1：1（按CPU、内存换算）。 此时性能最好的服务器处理请求较多，用户不希望过载此服务器，希望能够将新的请求分配到空闲服务器上。在此场景下，可以采用最小连接数的均衡方式，并适当降低繁忙服务器的权重，便于CLB将请求分配到活跃数较少的RS上，实现负载均衡。

- 场景6：

  某用户希望后续客户端的请求可以分配到同一服务器上。而采用加权轮询或加权最小连接数的方式，不能保证相同客户端的请求被分到固定某台服务器上去。为了配合客户特定应用程序服务器的需求，保证客户端的会话具有“粘性”或是“持续性”，在此场景下，我们可以采用ip_hash的均衡方式进行流量分发。此方法可以确保来自同一客户端的请求总被定向分发到同一RS上去。（服务器数量变化或是该服务器不可用时除外）