Cloud Load Balance

Quick Start

Product Introduction

Copyright Notice

Trademark Notice

Tencent Cloud

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

Quick Start

Getting Started

Last updated：2018-06-13 10:33:43

This document will use an example to help new users understand how to use Tencent Cloud's Cloud Load Balance: Create a public network-based (with daily rate) cloud load balancer instance named `clb-test`, and bind it to a custom domain to forward HTTP request to the two backend CVMs when this domain is accessed.

Preconditions

- Cloud load balancer is only responsible for forwarding the traffic, and is not capable of processing requests. Therefore, you need a running CVM instance to process user's requests. Here, you just need two CVM instances. You can also specify the number of CVMs to which the requests are forwarded. In this example, two CVM instances, `rs-1` and `rs-2`, have been created in Beijing region. For information on how to create a CVM instance, refer to Purchase and Enable CVM Instance.
- Here we take HTTP forwarding as an example. A Web server, such as Apache, Nginx and IIS, must be deployed on the CVMs. In this example, for the purpose of result verification, Apache is deployed on both `rs-1` and `rs-2`, with HTML text "This is rs-1" and "This is rs-2" returned respectively. For more information on how to deploy services on CVM, refer to Installation and Configuration of IIS and PHP on Windows and Environment Configuration of Linux System (CentOS).

> Note: In this example, the returned values vary with the services deployed on backend CVMs. In practice, the services deployed on CVMS are exactly the same to provide a consistent experience for all users.

Purchasing and Creating a Cloud Load Balancer Instance

> Please note that the cloud load balancer can only forward the traffic to the CVM instances within the same region. So please create the cloud load balancer instances within the same region where both CVMs reside in as described in "Preconditions".

1) Log in to Tencent Cloud, go to Cloud Load Balance Purchase Page.

2) In this example, select "North China (Beijing)", where the CVMs reside in, as the region, select "Public Network (with Daily Rate)" as the instance type, and select "Basic Network" as the network environment.

3) Click "Buy Now" to make the payment.

For more information on cloud load balancer instances, refer to Public Network-based Cloud Load Balancer Instance and Private Network-based Cloud Load Balancer Instance.

Creating Cloud Load Balancer Listener

The cloud load balancer listener forwards the requests via specified protocol and port. In this example, the cloud load balancer listener will be set to forward HTTP requests from client.

1) Log in to Tencent Cloud Console and click "Cloud Products" - "Cloud Load Balance" to enter the Cloud Load Balance console.

2) In the "LB instance list", find the public network-based (with daily rate) cloud load balancer instance you just created, and click its ID to enter the cloud load balancer details page.

3) In "Basic Info", click the icon next to the name to change the name to "clb-test".

4) In "Listener", click "Create" button to create a new cloud load balancer listener.

5) Enter the following information:

- The custom name is "Listener1";
- The listened protocol and port are `HTTP: 80`
- The backend port is `80` ;
- The balancing method is `Weighted Round Robin` ;
- Do not check "Session Persistence";
- Check "Health Check".

Click "OK" to complete the creation of cloud load balancer listener.

For more information on cloud load balancer listeners, refer to Cloud Load Balancer Listener Overview.

Binding Backend CVM

1) Log in to Tencent Cloud Console and click "Cloud Products" - "Cloud Load Balance" to enter the Cloud Load Balance console.

2) In the "LB instance list", find `clb-test` you just created, and click its ID to enter the cloud load balancer details page.

3) In "Bind to CVM", click "Bind to CVM" button, then select the CVM instances `rs-1` and `rs-2` within the same region described in "Preconditions", and set the weight to 10 (default).

4) Click "OK".

Testing Cloud Load Balancer

Enter the public network domain name (`www.qcloudtest.com`) configured for the cloud load balancer instance in the browser. Check the test result to verify whether the cloud load balancer instance has been configured successfully.

According to the following figures, the cloud load balancer can access the two bound backend CVMs based on the configurations made by the user.

- If the user enables the session persistence feature, or disables this feature but selects "ip_hash" for scheduling, the requests will be allocated to one backend CVM all the time.
- If the user disables the session persistence feature and selects "Weighted Round Robin" for scheduling, the requests will be allocated to multiple backend CVMs in sequence.

Getting Started with Public Application CLB

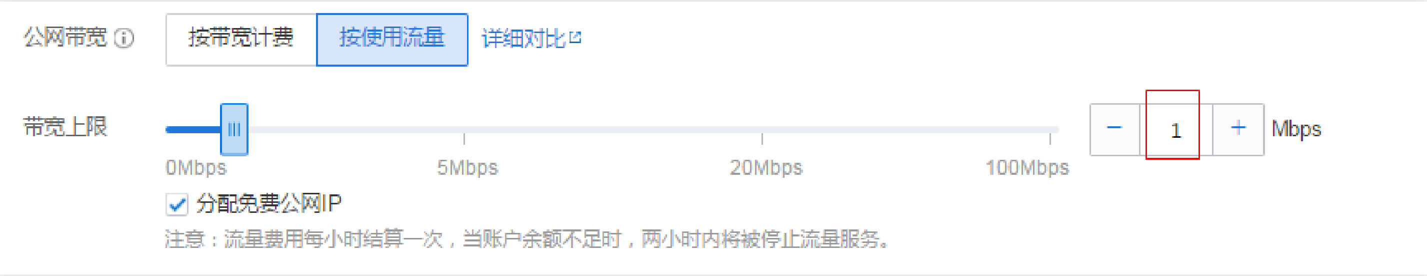
Last updated：2018-06-13 10:39:40

The public network application-based cloud load balancer launched by Tencent Cloud allows users to configure the domain name/URL-based forwarding rules to forward requests to different real servers. Also, the redirection feature of public network application-based cloud load balancer support redirecting http requests as https requests, enabling some mobile http requests to automatically return https respond through the LoadBalance proxy. Here we show you the new features of public network application-based cloud load balancer via detailed configurations.

1. Creating CVMs and Building nginx Service.

1.1 Purchasing CVMs

On the Purchasing CVMs page, select the appropriate models and images, set the initial password of the CVM, and then configure the security group (here for the convenience of test, you can open all the ports to Internet first and make restrictions in the future). In addition, make sure to activate public network traffic when purchasing CVM. Otherwise access may fail after LB is associated.



公网带宽：按使用流量

带宽上限：1 Mbps

☑ 分配免费公网IP

注意：流量费用每小时结算一次，当账户余额不足时，两小时内将被停止流量服务。

The CVM environment parameters used in this test are as follows (two CVMs was purchased):

> **CVM Information**
> Region Guangzhou
> Availability zone Guangzhou Zone 3
> CVM billing method Postpaid
> Network billing method Bill-by-traffic
> Network Basic network

> **Machine Configuration**
> OS CentOS 6.8 64-bit
> CPU 1-core
> Memory 2GB
> System disk 20GB (cloud block storage)
> Data disk 380 GB (Premium cloud storage)
> Public network bandwidth 1 Mbps

1.2 Building Environment

After purchasing, click the **Login** button on the CVM details page to directly log in to CVM, and then enter your user name and password to start building the nginx environment. Here we apply the easiest way to install nginx. If you need to install the latest version of nginx, go to the official website to download and decompress one for installation.
Install nginx:

```
yum -y install nginx
```

Start nginx and an error occurs

```
service nginx start
```

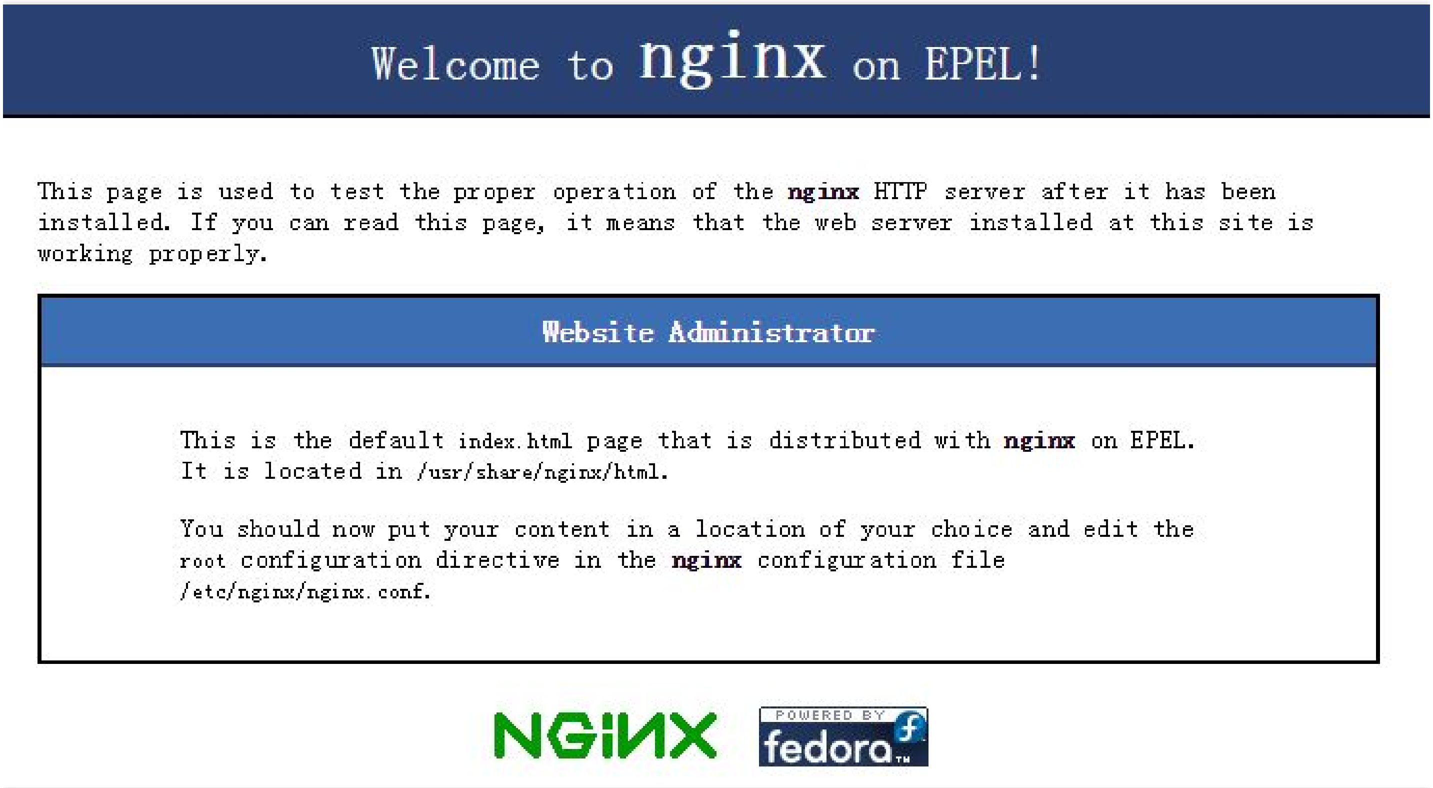
Modify the configuration file

```
vim /etc/nginx/conf.d/default.conf

listen       80 default_server;
listen       [::]:80 default_server;

Change the configuration to:
listen       80;   #Listening port 80
#listen       [::]:80 default_server;
```

Restart nginx

```
sudo service nginx restart
```

Now visit the public IP address of the CVM, you can see the page below:



Welcome to nginx on EPEL!

This page is used to test the proper operation of the nginx HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

Website Administrator

This is the default index.html page that is distributed with nginx on EPEL. It is located in /usr/share/nginx/html.

You should now put your content in a location of your choice and edit the root configuration directive in the nginx configuration file /etc/nginx/nginx.conf.

The default root directory of nginx is /usr/share/nginx/html, so you can directly modify or move the index.html static page under html to identify the particularity of this page.

```
vim /usr/share/nginx/html/index.html
```

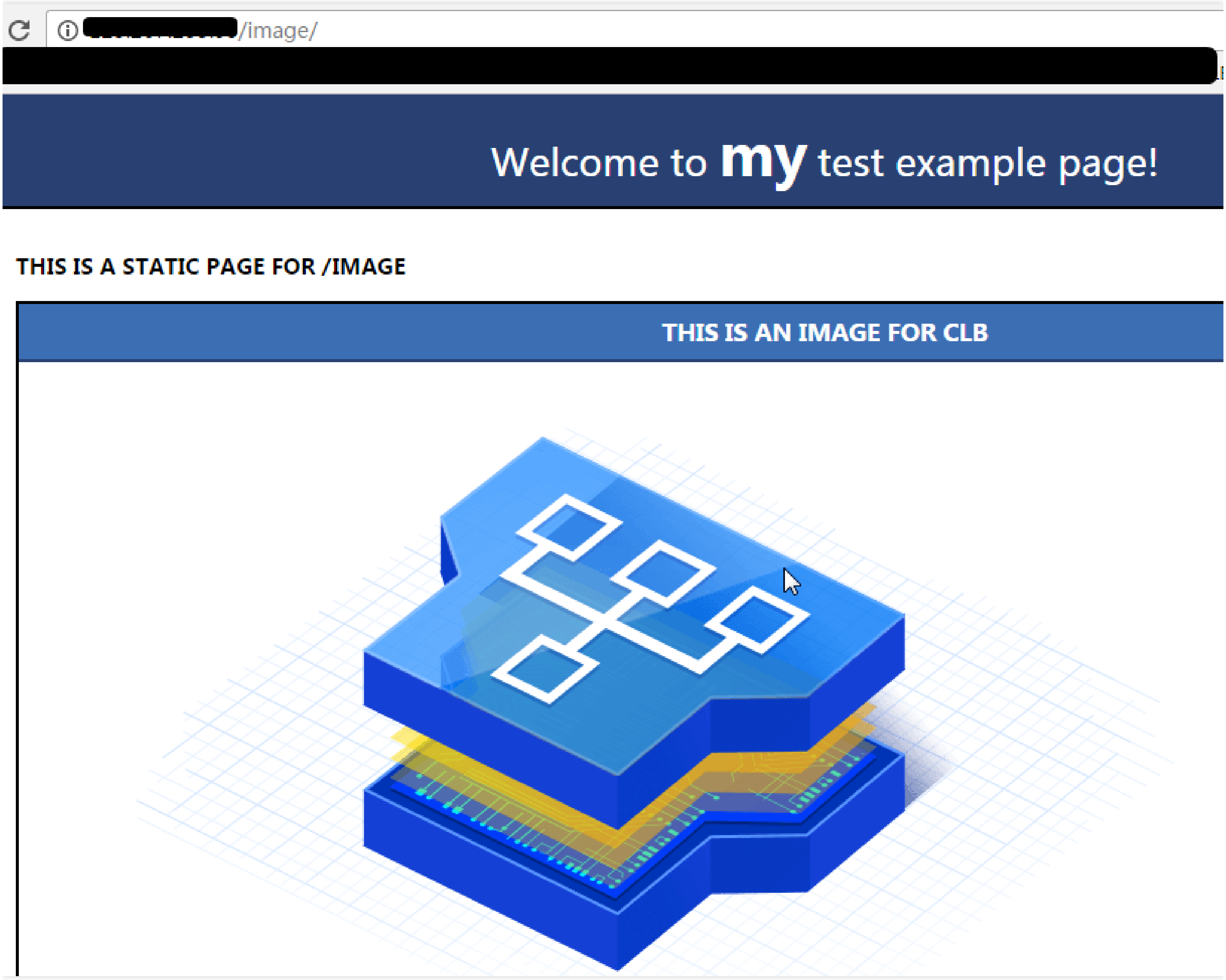
Because application-based cloud load balancer can forward requests based on the path of RS, you can configure services under different paths to facilitate subsequent request distribution for cloud load balancer. We deploy the static pages under /image/ path of CVM1 and /text/ path of CVM2 respectively as follows:

Relevant commands are as follows:

```
cd /usr/share/nginx/html/
mkdir image/
cp -r index.html image/    # For the other CVM, you can deploy the page to the text path
```

1.3 Authentication Service

Now, if the deployed page displays when you access the CVM's public network IP+ path, it indicates that the deployment in the first step is successful.
CVM1 /image page



[redacted]/image/

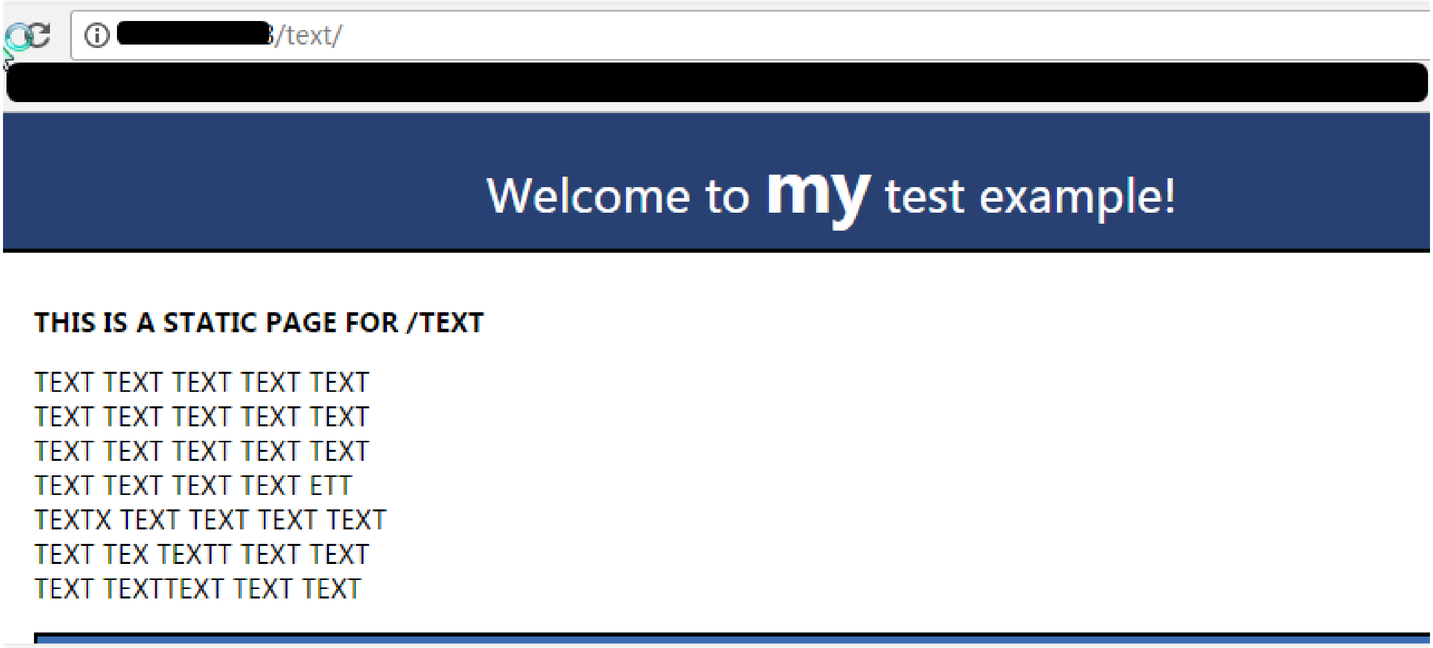
[redacted]

Welcome to **my** test example page!

THIS IS A STATIC PAGE FOR /IMAGE

THIS IS AN IMAGE FOR CLB

CVM2 /text page



[redacted]/text/

[redacted]

Welcome to **my** test example!

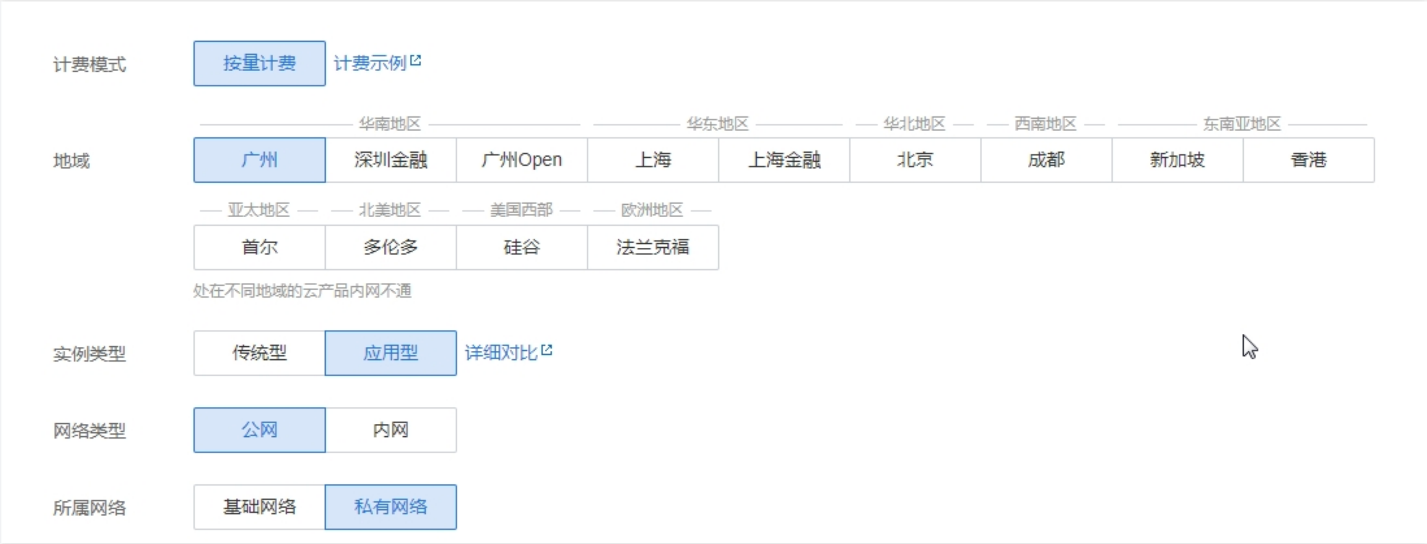
THIS IS A STATIC PAGE FOR /TEXT

TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT ETT
TEXTX TEXT TEXT TEXT TEXT
TEXT TEX TEXTT TEXT TEXT
TEXT TEXTTEXT TEXT TEXT

2. Purchasing and Configuring Public Network Application-based LB

2.1 Purchasing Application-based Cloud Load Balancer

Select application-based cloud load balancer on the Purchasing CLBs page. Please note that after you select the cloud load balancer in a region (for example, LB in Guangzhou), you can only bind intra-region backend CVMs of different availability zones (for example, CVMs in Guangzhou Zone 2 and Guangzhou Zone 3). After the application-based LB is created, you can explore the rich features of it.



计费模式 [✓ 按量计费] 计费示例

地域
华南地区: [✓ 广州] 深圳金融 广州Open
华东地区: 上海 上海金融
华北地区: 北京
西南地区: 成都
东南亚地区: 新加坡 香港
亚太地区: 首尔
北美地区: 多伦多
美国西部: 硅谷
欧洲地区: 法兰克福
处在不同地域的云产品内网不通

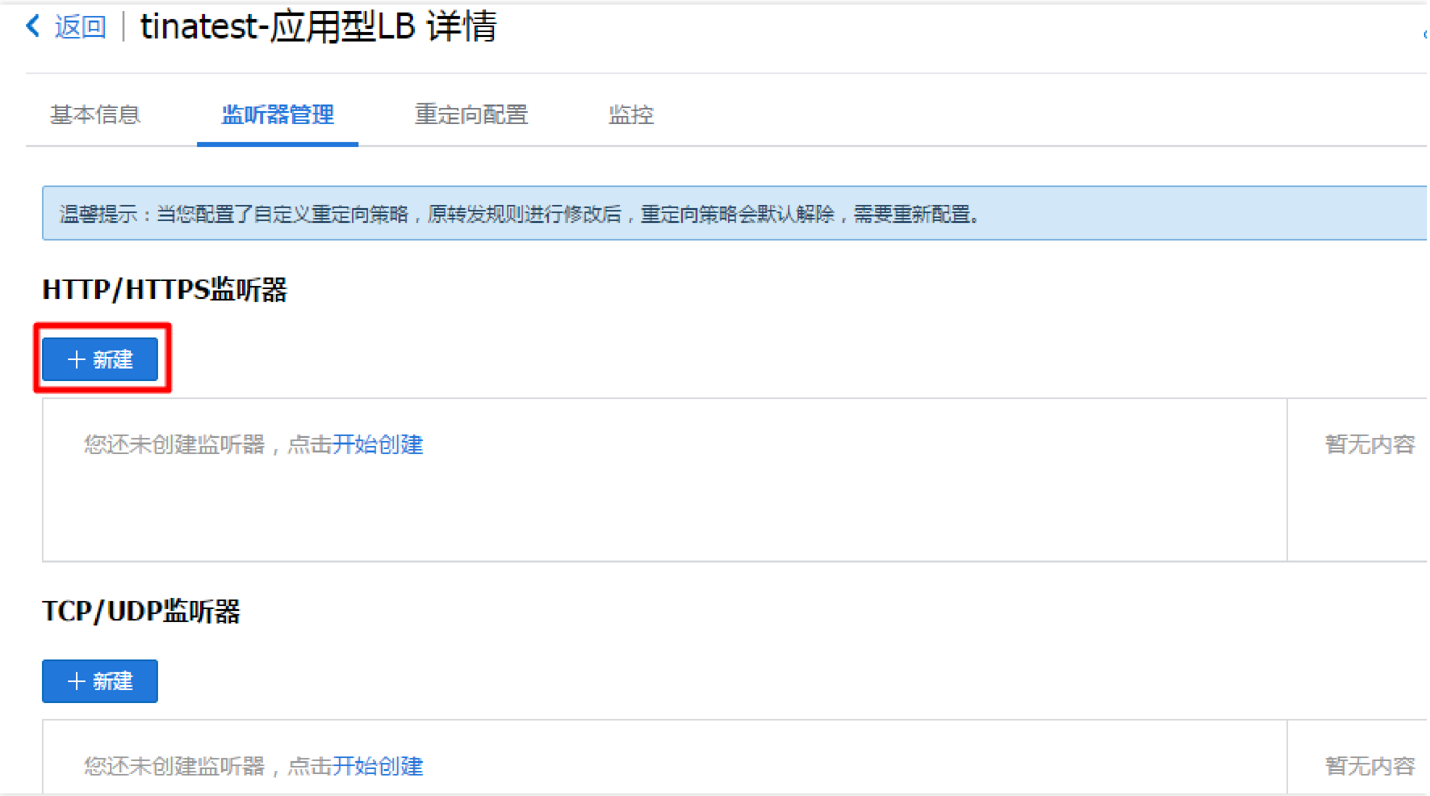
实例类型 传统型 [✓ 应用型] 详细对比

网络类型 [✓ 公网] 内网

所属网络 基础网络 [✓ 私有网络]

2.2 Configuring Listeners, Forwarding Groups and Forwarding Rules, and Binding CVMs

After purchasing, you can view the information of listener bound to the LB instance on the **LB Details** -> **Listener Management** page. Click **New** to create an HTTP listener.



温馨提示：当您配置了自定义重定向策略，原转发规则进行修改后，重定向策略会默认解除，需要重新配置。

HTTP/HTTPS监听器

您还未创建监听器，点击开始创建

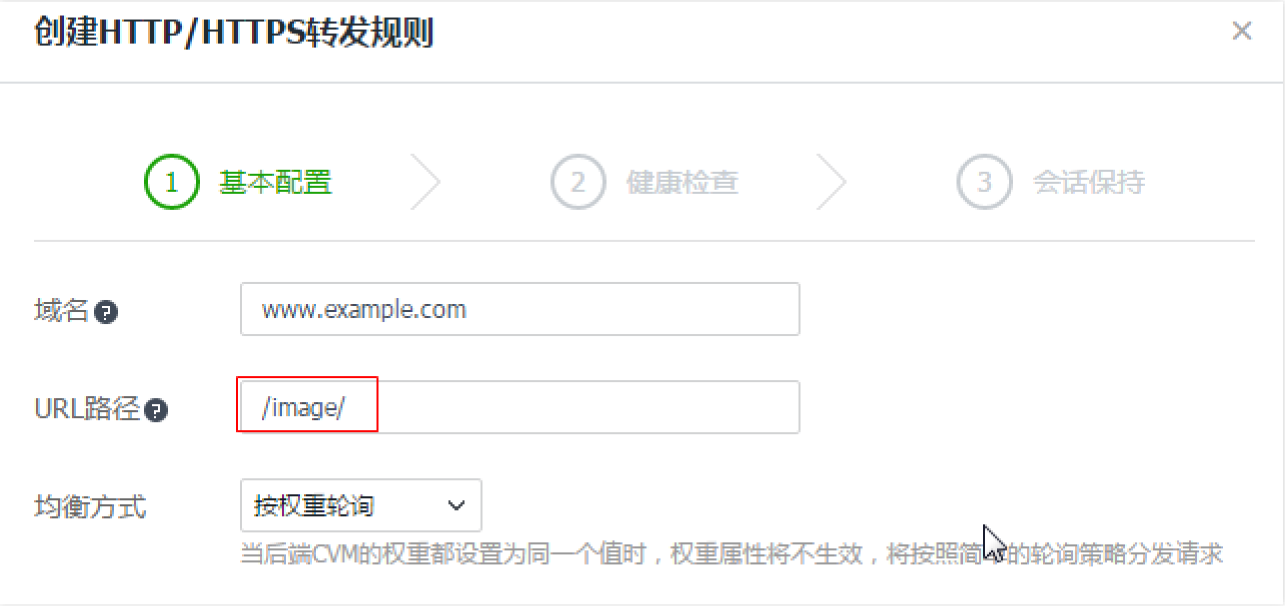
暂无内容

TCP/UDP监听器

您还未创建监听器，点击开始创建

暂无内容

Enter the listener name and listening port (here is port 80 by default) when creating the Layer-7 HTTP listener. After the listener is created, click **Create Forwarding Rule** to configure a domain name and URL for the listener. Wildcard and regularization are supported, but there are some restrictions. For more information, please see Configuration Description. For load balancing mode, you can select polling by weight. If you do not want the connection to fall on the same backend CVM, you can set the session persistence to be disabled by default in the step 3 of configuration.



创建HTTP/HTTPS转发规则

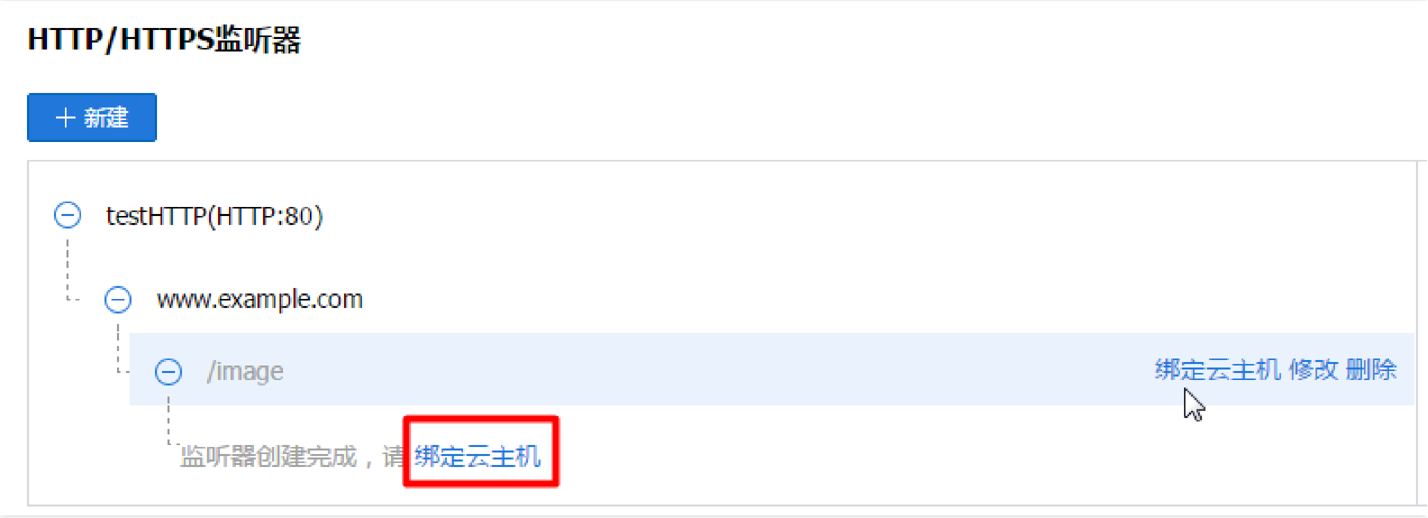
域名 www.example.com

URL路径 /image/

均衡方式 按权重轮询

当后端CVM的权重都设置为同一个值时，权重属性将不生效，将按照简单的轮询策略分发请求

After the forwarding rule is created, you can see that forwarding groups and forwarding rules have been configured for www.example.com/image/ under the listener. Then you can click **Bind CVM** to select the CVM for which we have just configured the service. When binding CVM, the backend port 80 is set as the default listening port. The configuration of application-based cloud load balancer is flexible, so you can bind CVMs of different backend ports under the same listener.



HTTP/HTTPS监听器

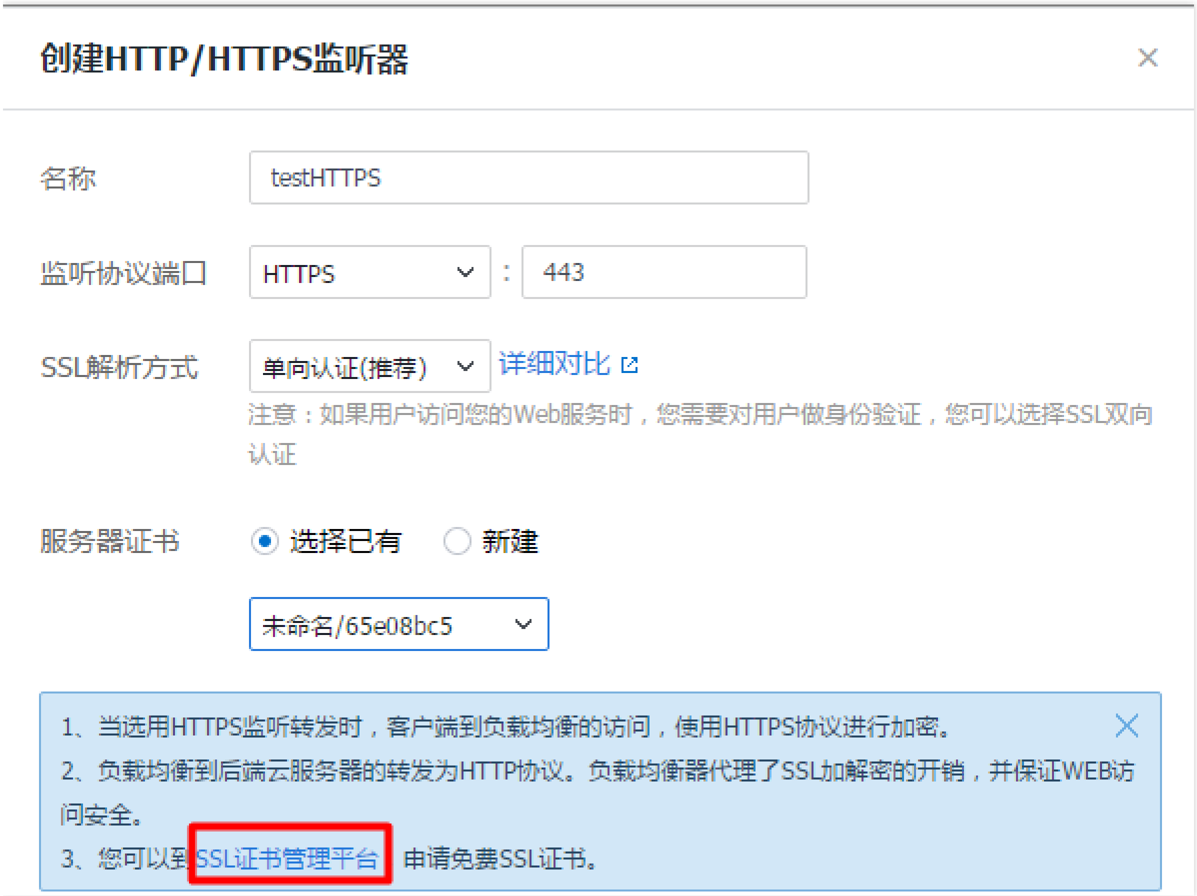
testHTTP(HTTP:80)

www.example.com

/image

监听器创建完成，请绑定云主机

Next, we can continue to create an HTTPS listener, which requires a server certificate at least for one-way authentication. Here you can upload your own certificates, or select the existing certificates, or apply for a certificate on the SSL certificate platform. We set port 443 for HTTPS protocol by default.



创建HTTP/HTTPS监听器

名称: testHTTPS

监听协议端口: HTTPS : 443

SSL解析方式: 单向认证(推荐) 详细对比

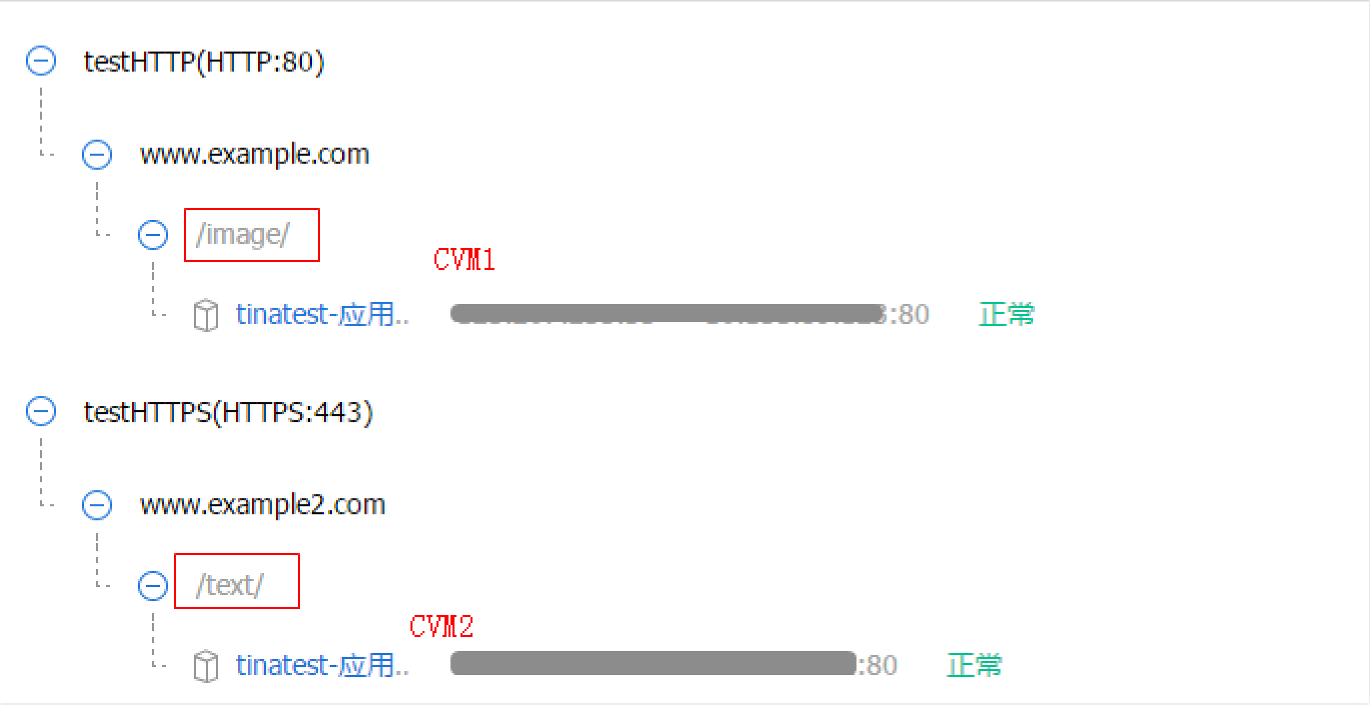
注意：如果用户访问您的Web服务时，您需要对用户做身份验证，您可以选择SSL双向认证

服务器证书: ● 选择已有 ○ 新建

未命名/65e08bc5

1、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。
2、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。
3、您可以到SSL证书管理平台 申请免费SSL证书。

The subsequent listener configuration procedures are similar. After the configuration is completed, we can view the architecture under the LB:

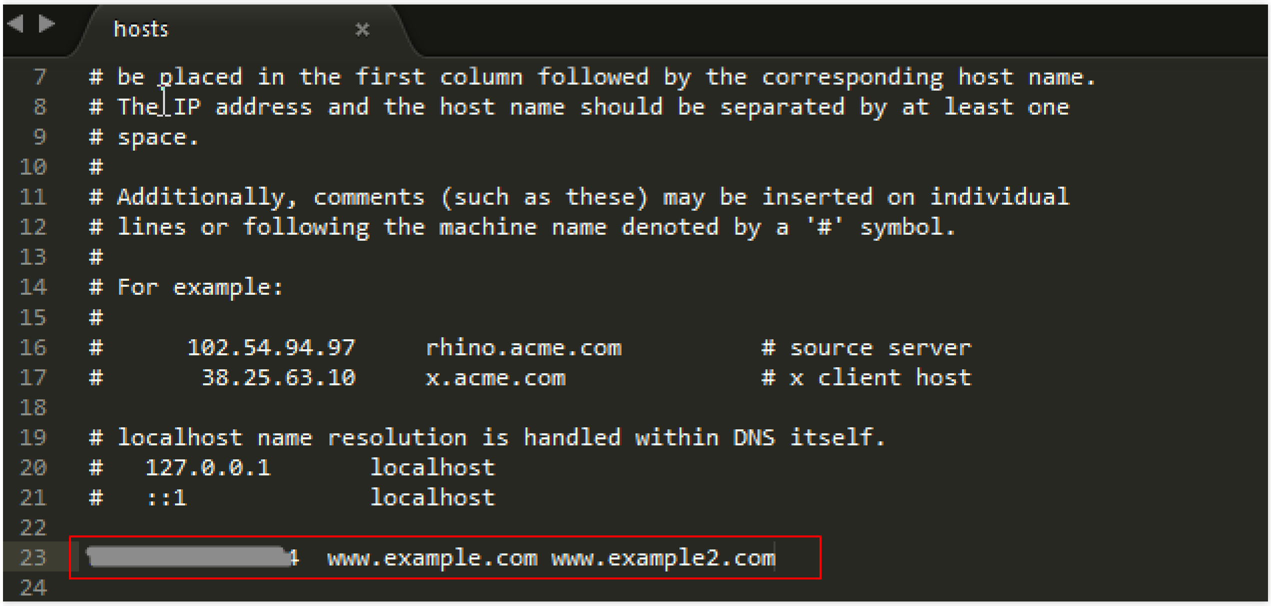


testHTTP(HTTP:80)
www.example.com
/image/
CVM1
tinatest-应用.. [redacted]:80 正常

testHTTPS(HTTPS:443)
www.example2.com
/text/
CVM2
tinatest-应用.. [redacted]:80 正常

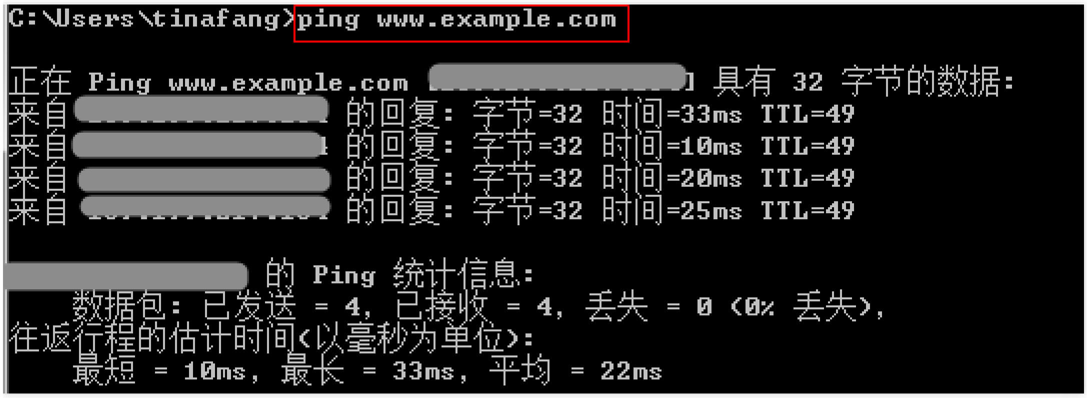
2.2 Authentication Service

After finishing the configuration, we can verify whether the architecture takes effect. First, we need to perform the hosts operation for domain names of the two listeners. That is, modify the hosts file in C:\Windows\System32\drivers\etc to map the VIP of LB instance to the two domains.



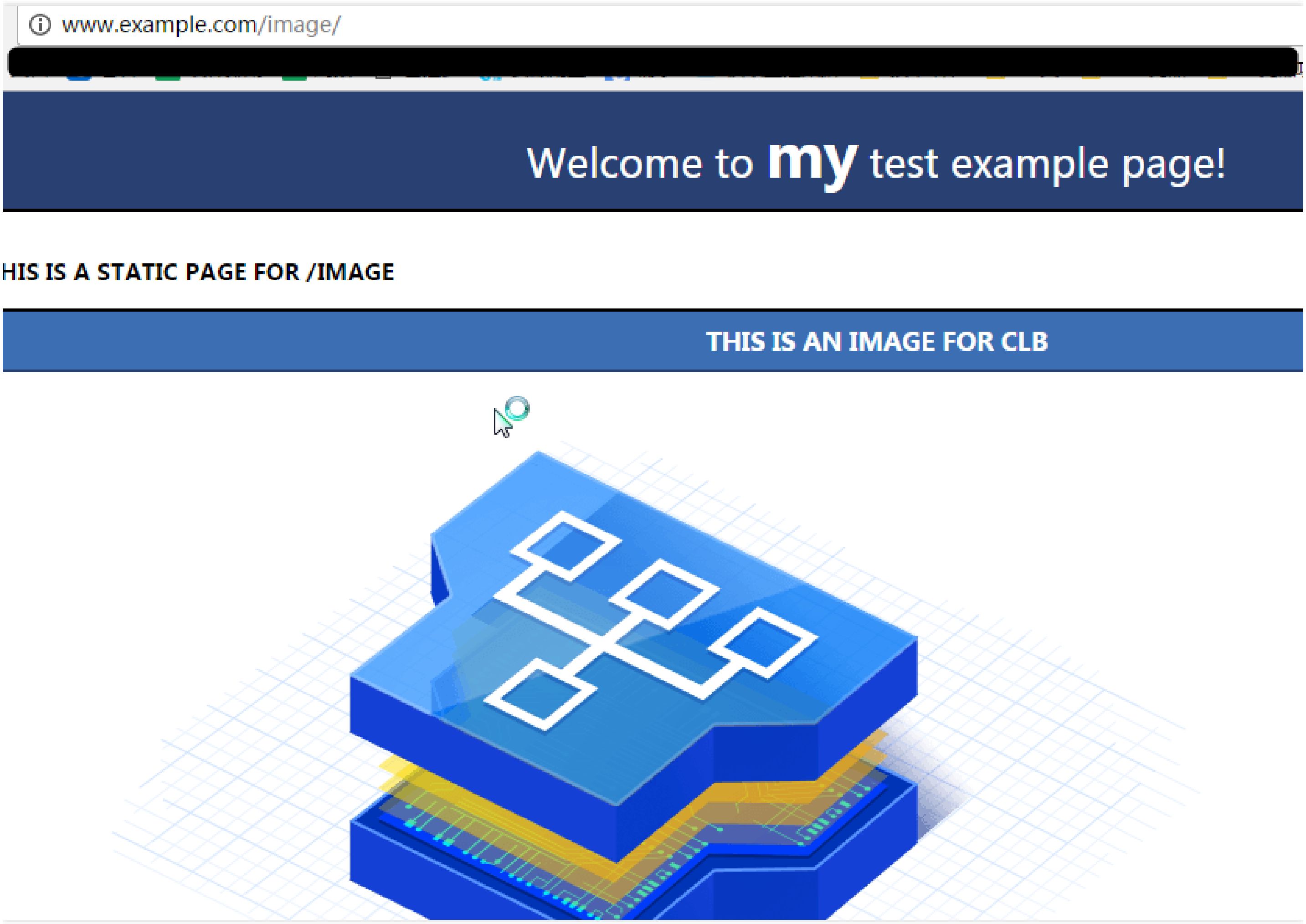
```
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost

[redacted]   www.example.com www.example2.com

```

To verify whether the hosts operation is successful or not, you can type "cmd" into the search bar on the local machine, and then use the ping command to check whether the domain name is successfully bound to the VIP. If there is a data packet, it indicates that the binding is successful.



```
C:\Users\tinafang>ping www.example.com

正在 Ping www.example.com [redacted] 具有 32 字节的数据:
来自 [redacted] 的回复: 字节=32 时间=33ms TTL=49
来自 [redacted] 的回复: 字节=32 时间=10ms TTL=49
来自 [redacted] 的回复: 字节=32 时间=20ms TTL=49
来自 [redacted] 的回复: 字节=32 时间=25ms TTL=49

[redacted] 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 10ms，最长 = 33ms，平均 = 22ms
```

Next, you can enter http://www.example.com/image/ and https://www.example2.com/text/ to test whether a request can access RS via LB. (Note: the "/" of image/ and text/ is required, because it indicates image and text are two default directories instead of files with names of "image" and "text".)



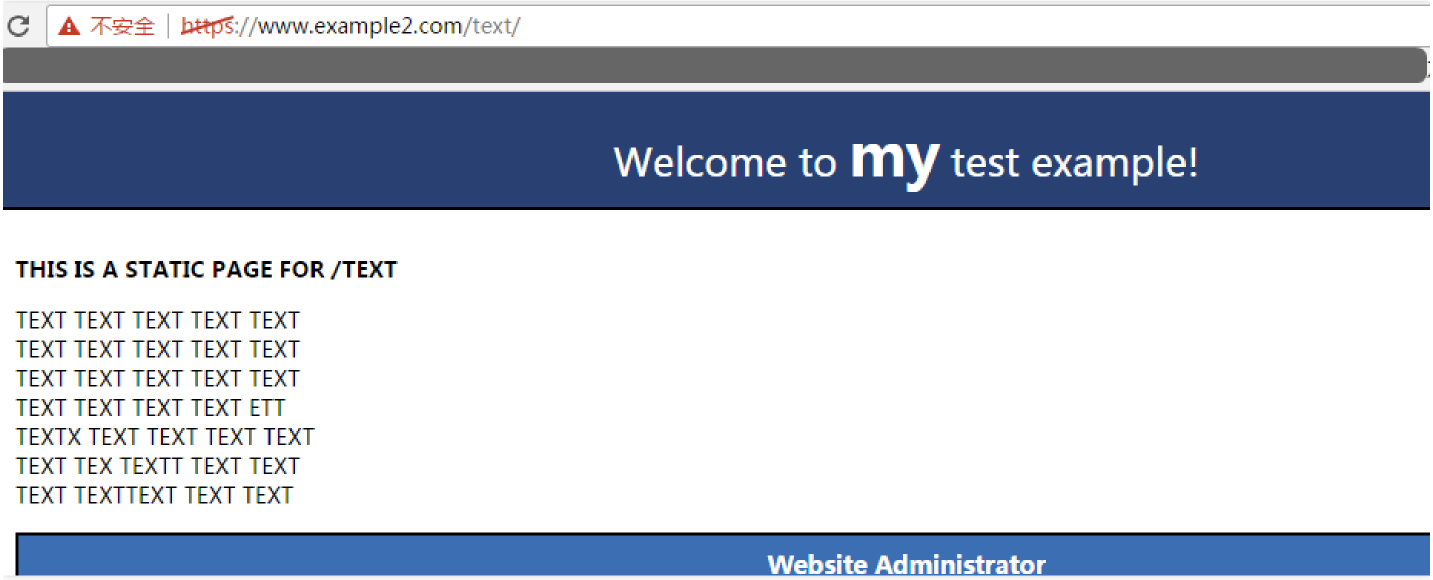
ⓘ www.example.com/image/

[redacted]

Welcome to **my** test example page!

HIS IS A STATIC PAGE FOR /IMAGE

THIS IS AN IMAGE FOR CLB



▲ 不安全 | ~~https~~://www.example2.com/text/

[redacted]

Welcome to **my** test example!

THIS IS A STATIC PAGE FOR /TEXT

TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT ETT
TEXTX TEXT TEXT TEXT TEXT
TEXT TEX TEXTT TEXT TEXT
TEXT TEXTTEXT TEXT TEXT

Website Administrator

The results shown in the above figure indicate that we can access different backend CVMs via different ***domain names + URLs*** under a LB instance, that is, ***"content-based routing"*** feature is realized. Then, the redirection feature can work in the two scenarios below:

(1) Forced https: When Web service is accessed by PC and mobile browsers via http requests, you want https respond to be returned through LoadBalance proxy. By default, https is used by browsers to access web pages.

(2) Custom redirection: When Web services need to be temporarily deactivated (in case of selling-out of e-commerce, page maintenance, and upgrade), redirect capability is necessary. Without redirections, visitors can only get a 404/503 error message due to the old address in users' favorites and search engine database, which reduces user experience and results in access traffic loss. In addition, the search engine scores accumulated on this page are also wasted.

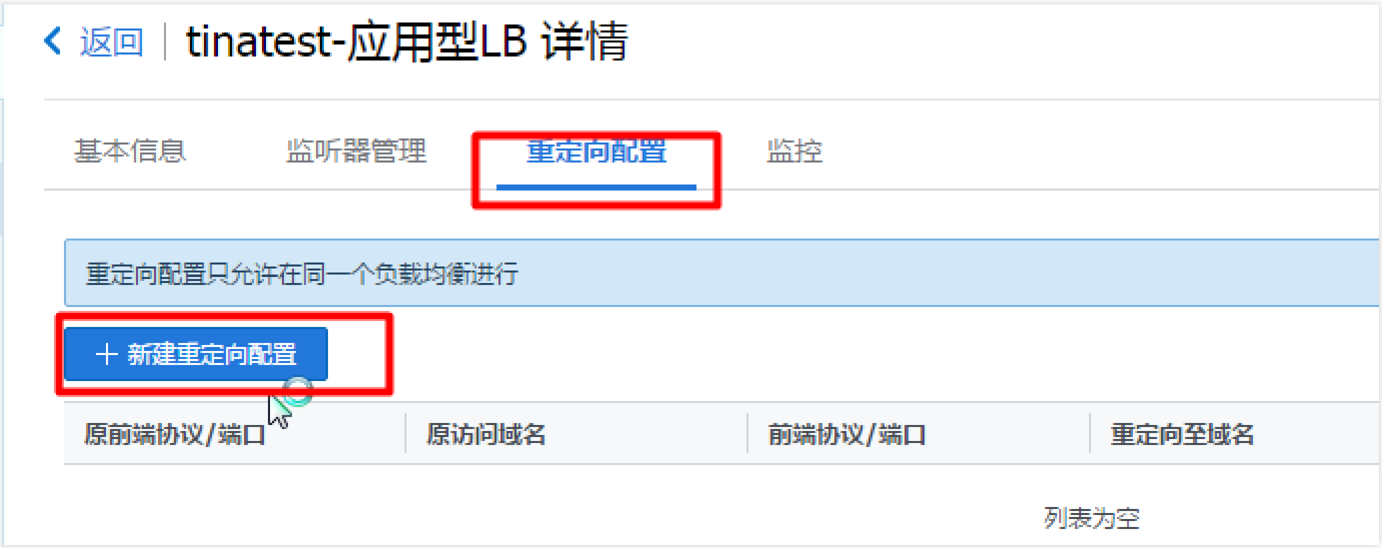
Next, we can experience this feature through actual operations, that is, redirect the requests in the configured HTTP listener to the HTTPS listener.

3. Configuring Redirection

The redirection configuration is divided into manual redirection and automatic redirection. Automatic redirection is mainly designed for such situation: there are many paths under the domain name, and the system needs to automatically create an HTTP listener for the existing HTTPS: 443 listener for forwarding. After the HTTP listener is created successfully, the HTTP: 80 address can be automatically redirected as HTTPS address: 443 for access. We use manual redirection configuration in this document. For more information, please see Redirection Configuration.

3.1 Manual Redirection Configuration

Select the Redirection Configuration tab on the LB details page, and create a new manual redirection configuration.

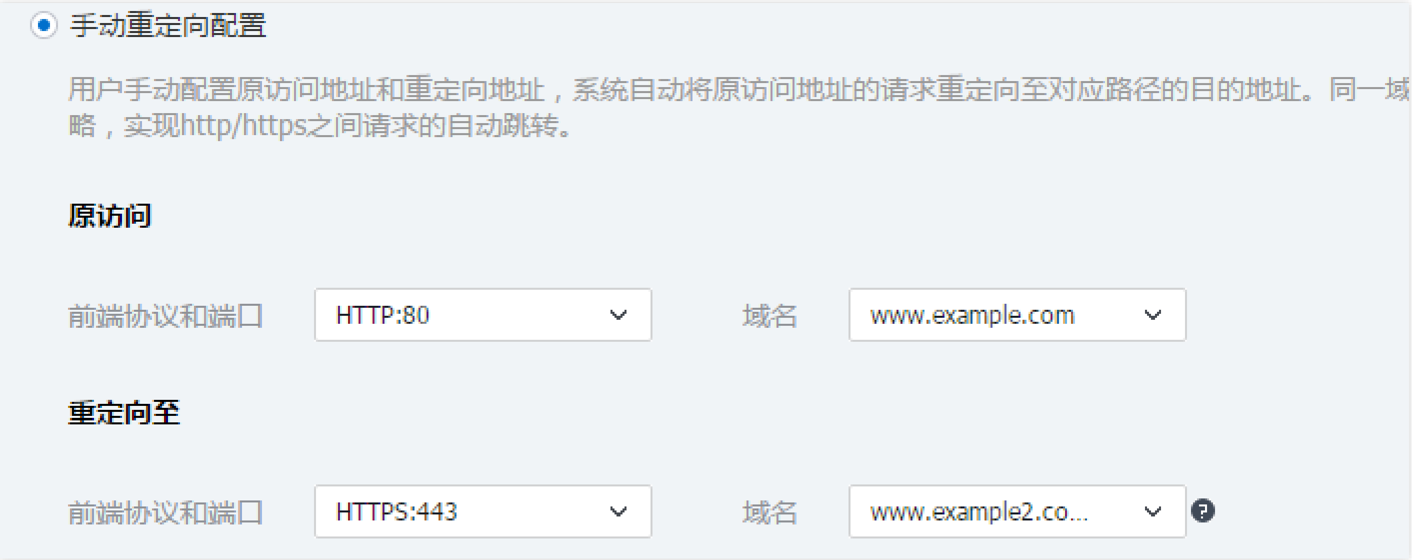


重定向配置只允许在同一个负载均衡进行

原前端协议/端口	原访问域名	前端协议/端口	重定向至域名

列表为空

Then select the original access protocol, port and domain name, and specify the destination protocol, port and domain name.


● 手动重定向配置

用户手动配置原访问地址和重定向地址，系统自动将原访问地址的请求重定向至对应路径的目的地址。同一域
略，实现http/https之间请求的自动跳转。

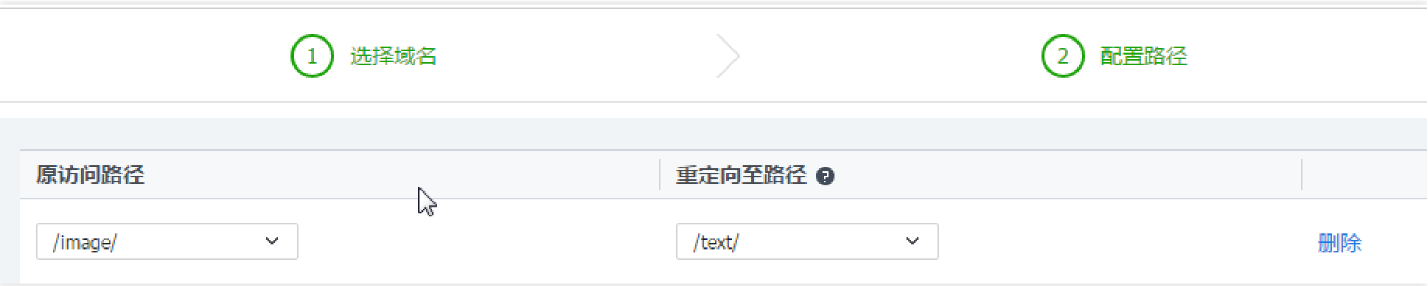
原访问

前端协议和端口 HTTP:80　域名 www.example.com

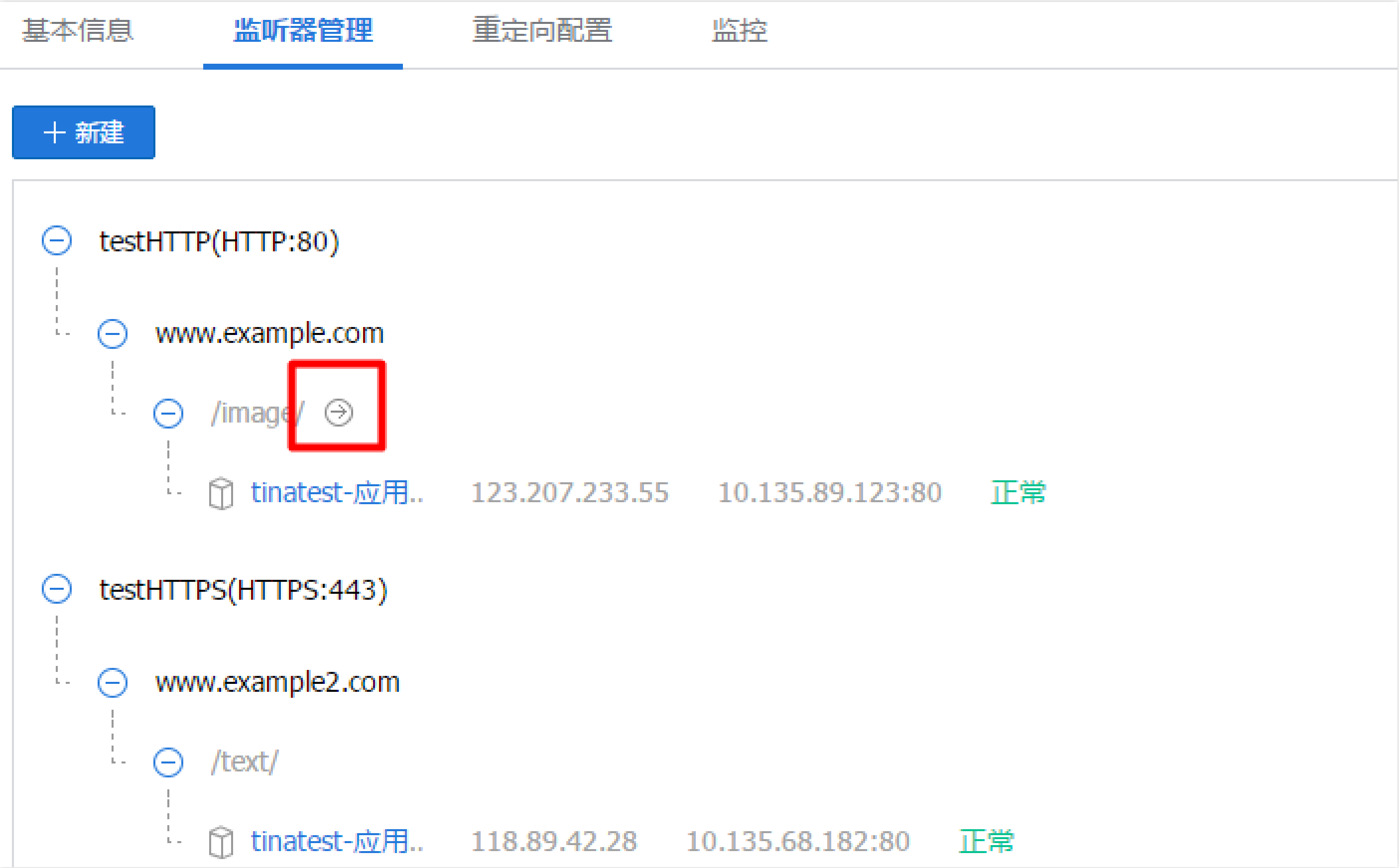
重定向至

前端协议和端口 HTTPS:443　域名 www.example2.co...

Click **Next** to select the original and redirected access paths. If there are many paths under the domain name, you can add multiple paths for redirection. Note: The path configuration does not allow loopback (that is, A-> B B-> C), and the configuration can only be performed in the same LB instance for now.



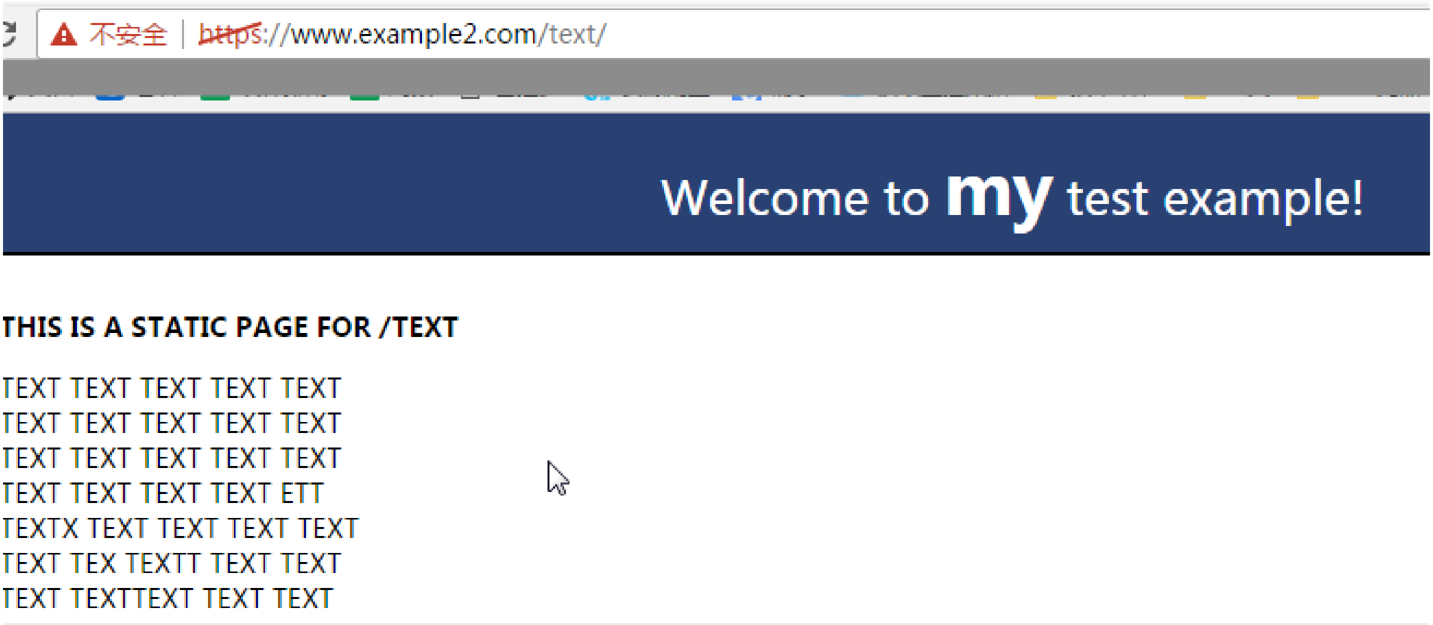
After the redirection policy is configured, you can view the policy on the LB redirection configuration details page. In addition, you can find that in the original listener tree diagram, a redirection identifier is added to the path of the HTTP listener to indicate that the bound real servers in this path will no longer receive requests because requests will be redirected to the HTTPS listener you just configured.



3.2 Authentication Service

Finally, we can access `http://www.example.com/image/` to verify whether the request is automatically redirected to the address `https://www.example2.com/text/` .

If the following page appears after you enter `http://www.example.com/image/` , the redirection is configured successfully.



▲ 不安全 | ~~https~~://www.example2.com/text/

Welcome to **my** test example!

THIS IS A STATIC PAGE FOR /TEXT

TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT TEXT
TEXT TEXT TEXT TEXT ETT
TEXTX TEXT TEXT TEXT TEXT
TEXT TEX TEXTT TEXT TEXT
TEXT TEXTTEXT TEXT TEXT