云享家
贝斯平资深专家
与您共享云端干货

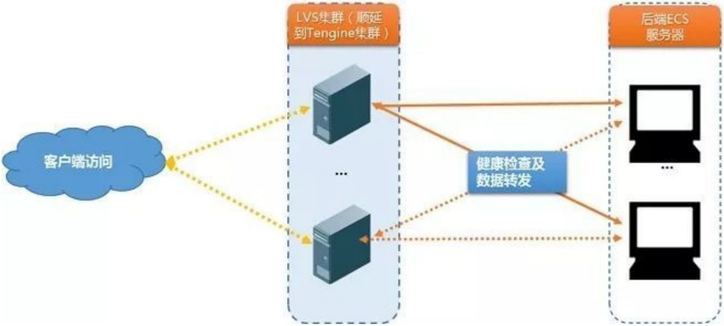
SLB (负载均衡) 健康检查过程介绍

负载均衡支持对多台ECS进行流量分发，以提升应用系统的服务能力，**长期以来都是关键业务系统的入口**。淘宝，天猫，阿里云等无不依赖负载均衡产品，**双11的流量洪峰也依赖负载均衡的调度和处理能力。**

阿里云负载均衡采用集群部署。LVS集群或Tengine集群内的相关节点服务器同时承载了数据转发和健康检查职责。

LVS集群内不同服务器分别独立、并行地根据负载均衡策略进行数据转发和健康检查操作。如果某一台LVS节点服务器对后端某一台ECS健康检查失败，则该LVS节点服务器将不会再将新的客户端请求分发给相应的异常ECS。LVS集群内所有服务器同步进行该操作。

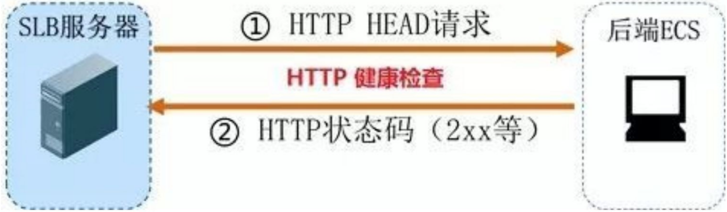
负载均衡健康检查使用的地址段是100.64.0.0/10，后端服务器务必不能屏蔽该地址段。**您无需在ECS安全组中额外针对该地址段配置放行策略（ECS安全组检测到流量来自阿里云SLB会自动方向，不会应用安全在规则）**，但如有配置iptables 等安全策略，请务必放行（100.64.0.0/10 是阿里云保留地址，其他用户无法分配到该网段内，不会存在安全风险）。



HTTP/HTTPS监听健康检查机制

针对七层（HTTP或HTTPS协议）监听，健康检查通过HTTP HEAD探测来获取状态信息，如下图所示。

对于HTTPS监听，证书在负载均衡系统中进行管理。负载均衡与后端 ECS之间的数据交互（包括健康检查数据和业务交互数据），不再通过HTTPS 进行传输，以提高系统性能。



七层监听的检查机制

Tengine节点服务器根据监听的健康检查配置，向后端ECS的内网IP+【健康检查端口】+【检查路径】发送HTTP HEAD请求（包含设置的【域名】）。

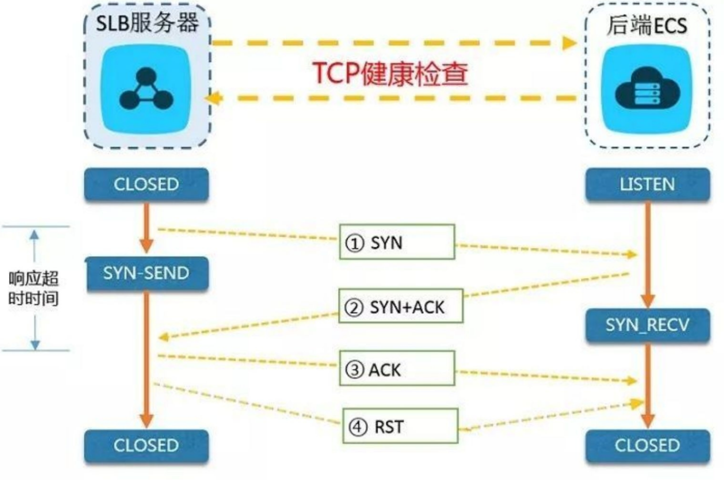
后端ECS收到请求后，根据相应服务的运行情况，返回HTTP状态码。

如果在【响应超时时间】之内，Tengine节点服务器没有收到后端ECS返回的信息，则认为服务无响应，判定健康检查失败。

如果在【响应超时时间】之内，Tengine节点服务器成功接收到后端ECS返回的信息，则将该返回信息与配置的状态码进行比对。如果匹配则判定健康检查成功，反之则判定健康检查失败。

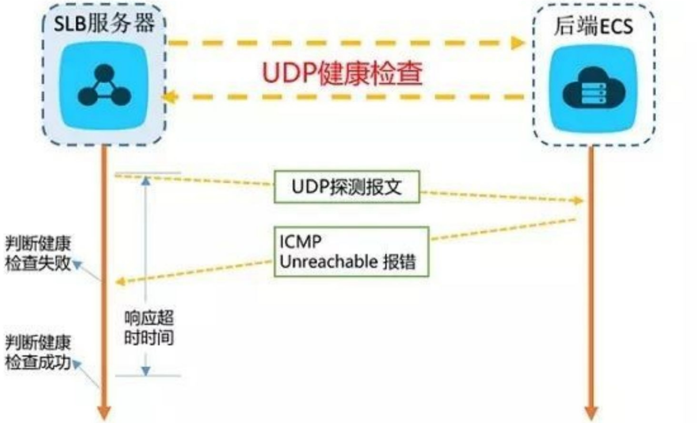
TCP监听健康检查机制

针对四层TCP监听，为了提高健康检查效率，健康检查通过定制的TCP探测来获取状态信息，如下图所示。



UDP监听健康检查

针对四层UDP监听，健康检查通过UDP报文探测来获取状态信息，如下图所示。



UDP监听的检查机制

LVS节点服务器根据监听的健康检查配置，向后端ECS的内网IP+【健康检查端口】发送UDP报文。

如果后端ECS相应端口未正常监听，则系统会返回类似返回port XX unreachable的ICMP报错信息；反之不做任何处理。

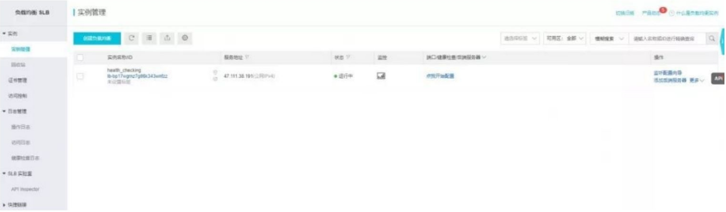
如果在【响应超时时间】之内，LVS节点服务器收到了后端ECS返回的上述错误信息，则认为服务异常，判定健康检查失败。

如果在【响应超时时间】之内，LVS节点服务器没有收到后端ECS返回的任何信息，则认为服务正常，判定健康检查成功。

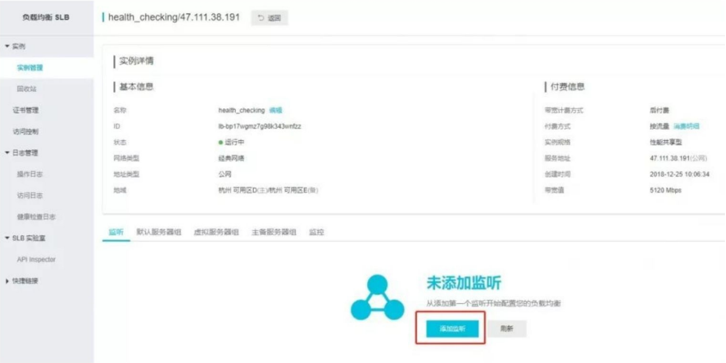
实验环境搭建

1

创建一个共享型的SLB实例，然后开始配置监听。



2 点击添加监听



health_checking/47.111.38.191

实例详情

基本信息

名称	health_checking 编辑
ID	lb-bp17wgmz7g98k343wnfzz
状态	● 运行中
网络类型	经典网络
地址类型	公网
地域	杭州 可用区D(主)/杭州 可用区E(备)

付费信息

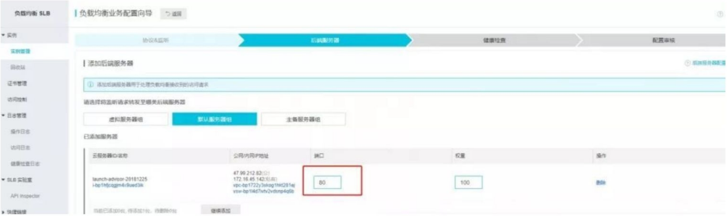
带宽计费方式	后付费
付费方式	按流量 消费明细
实例规格	性能共享型
服务地址	47.111.38.191(公网)
创建时间	2018-12-25 10:06:34
带宽值	5120 Mbps

未添加监听

从添加第一个监听开始配置您的负载均衡

3

选择默认服务器组，我这只是测试没有创建自己的服务器组，选择我刚创建的ECS，这里我为了测试只有一台ECS，在实际的使用中，SLB后端最少需要监听两台ECS，不然SLB的使用就完全没有意义了。



负载均衡业务配置向导

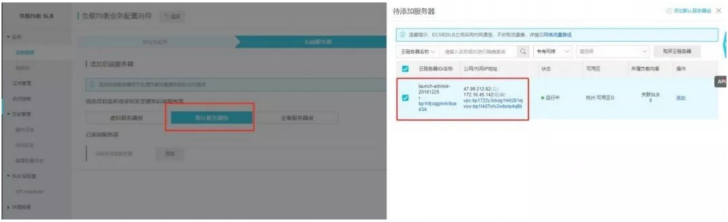
添加后端服务器

请选择将监听请求转发至哪类后端服务器

已添加服务器

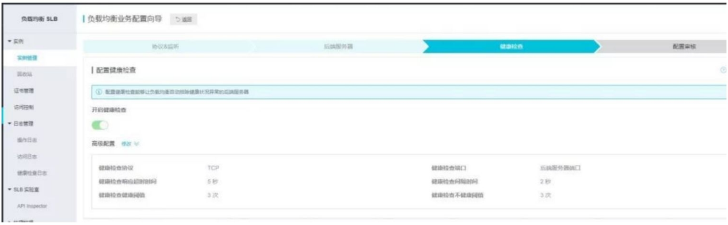
云服务器ID/名称	公网/内网IP地址	端口	权重	操作
launch-advisor-20181225	47.99.212.82(公) 172.16.45.142(私有)	80	100	删除

4 选择后端监听端口为80。



云服务器ID/名称	公网/内网IP地址	状态	可用区	所属负载均衡	操作
launch-advisor-20181225	47.99.212.82(公) 172.16.45.142(私网)	运行中	杭州 可用区G		添加

5 四层监听是默认开启健康检查的且无法关闭。



健康检查协议 TCP
健康检查端口 后端服务器端口
健康检查响应超时时间 5 秒
健康检查间隔时间 2 秒
健康检查健康阈值 3 次
健康检查不健康阈值 3 次

注意： SLB监听的ECS安全组是不会拦截SLB的连接访问，所以如果遇到问题，不需要排查安全组的问题，只需要直接排查网络和ECS内部配置。

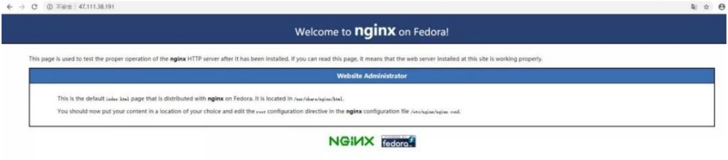
6

ECS实例安装 nginx 软件，centos 可以通过下面的命令快速安装和启动。

```
yum install nginx
service nginx start
```

7

安装完成后测试访问SLB和ECS的80端口是正常



Welcome to **nginx** on Fedora!

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 Fedora. 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`.

8

安装FTP服务器来下载抓包文件，创建了一个账号ftptest 用于FTP的下载，需要授权FTP 对指定路径的文件夹的下载权限。

```
yum install -y vsftpd
```

9

在服务器侧用tcpdump 的命令进行抓包，抓取 SLB 健康检查的网络包，然后通过 wireshark 分析抓包文件，来验证一下SLB 是否是上面描述的方式进行探测

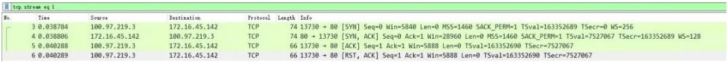
```
tcpdump tcp -i eth0 -w ./target.cap
```

验证健康检查方式

四层TCP监听

首先我这里模仿的是四层TCP监听，抓包文件分析如下，可以看出来四层的监听如上面介绍，三次握手后

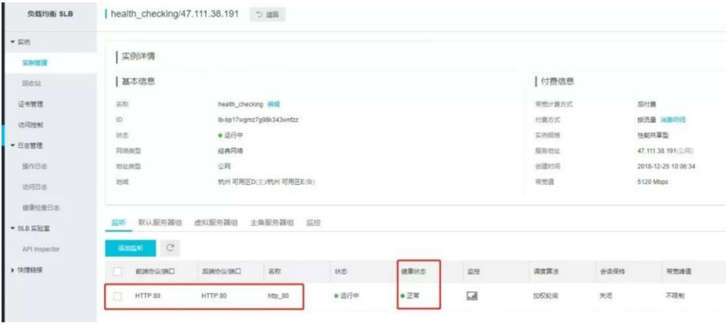
SLB 侧 RST连接：



```
tcp.stream eq 1
No.  Time      Source         Destination    Protocol Length Info
   3 0.038784  100.97.219.3   172.16.45.142  TCP      74 13730 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=163352689 TSecr=0 WS=256
   4 0.038806  172.16.45.142  100.97.219.3   TCP      74 80 → 13730 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=7527067 TSecr=163352689 WS=128
   5 0.040288  100.97.219.3   172.16.45.142  TCP      66 13730 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=163352690 TSecr=7527067
   6 0.040289  100.97.219.3   172.16.45.142  TCP      66 13730 → 80 [RST, ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=163352690 TSecr=7527067
```

七层HTTP监听

下面我将验证 七层HTTP的监听 是否如上面介绍的原理，首先删除之前四层的监听，配置七层的监听，健康检查状态正常。



health_checking/47.111.38.191

实例详情

基本信息

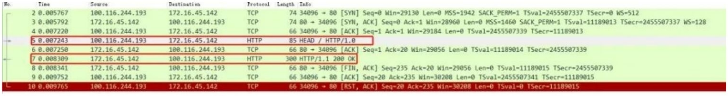
名称 health_checking 编辑
ID lb-bp17wgmz7g98k343wnfzz
状态 ● 运行中
网络类型 经典网络
地址类型 公网
地域 杭州 可用区D(主)/杭州 可用区E(备)

付费信息

带宽计费方式 后付费
付费方式 按流量 消费明细
实例规格 性能共享型
服务地址 47.111.38.191(公网)
创建时间 2018-12-25 10:06:34
带宽值 5120 Mbps

□	前端协议/端口	后端协议/端口	名称	状态	健康状态	监控	调度算法	会话保持	带宽峰值
□	HTTP:80	HTTP:80	http_80	● 运行中	● 正常	📊	加权轮询	关闭	不限制

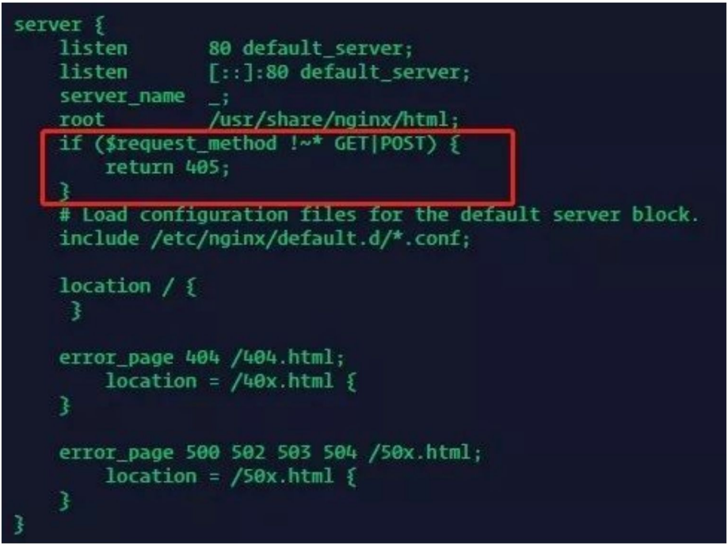
通过后端的抓包验证一下是否正确，这里可以看到确实是通过head的方式进行健康检查，正常的健康检查交互过程如下：



```
No.  Time      Source           Destination      Protocol Length Info
   2 0.005767  100.116.244.193  172.16.45.142    TCP      74 34096 → 80 [SYN] Seq=0 Win=29130 Len=0 MSS=1942 SACK_PERM=1 TSval=2455507337 TSecr=0 WS=512
   3 0.005792  172.16.45.142    100.116.244.193  TCP      74 80 → 34096 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=11189013 TSecr=2455507337 WS=128
   4 0.007220  100.116.244.193  172.16.45.142    TCP      66 34096 → 80 [ACK] Seq=1 Ack=1 Win=29184 Len=0 TSval=2455507339 TSecr=11189013
   5 0.007243  100.116.244.193  172.16.45.142    HTTP     85 HEAD / HTTP/1.0
   6 0.007250  172.16.45.142    100.116.244.193  TCP      66 80 → 34096 [ACK] Seq=1 Ack=20 Win=29056 Len=0 TSval=11189014 TSecr=2455507339
   7 0.008309  172.16.45.142    100.116.244.193  HTTP    300 HTTP/1.1 200 OK
   8 0.008341  172.16.45.142    100.116.244.193  TCP      66 80 → 34096 [FIN, ACK] Seq=235 Ack=20 Win=29056 Len=0 TSval=11189015 TSecr=2455507339
   9 0.009752  100.116.244.193  172.16.45.142    TCP      66 34096 → 80 [ACK] Seq=20 Ack=235 Win=30208 Len=0 TSval=2455507341 TSecr=11189015
  10 0.009765  100.116.244.193  172.16.45.142    TCP      66 34096 → 80 [RST, ACK] Seq=20 Ack=235 Win=30208 Len=0 TSval=0 TSecr=11189015
```

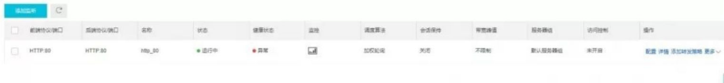
有时候会发生客户Nginx配置禁用了HEAD方法或者配置了特殊返回不正常的HTTP code，导致SLB健康检查失败，现象是SLB健康检查失败，但是直接访问后端ECS是没有问题的，客户会怀疑SLB的健康检查有问题，遇到这种问题最好

是在服务器端抓一个包，看一下服务器是否接收到SLB的健康检查， 是否返回了正确的状态，当然也可以通过SLB的健康检查日志来看一下服务器的返回健康检查是否正确。下面是NGINX配置文件修改，然后重启NGINX。



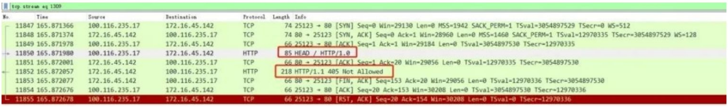
```
server {
    listen       80 default_server;
    listen       [::]:80 default_server;
    server_name  _;
    root         /usr/share/nginx/html;
    if ($request_method !~* GET|POST) {
        return 405;
    }
    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
     }

    error_page 404 /404.html;
        location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
        location = /50x.html {
    }
}
```

然后我们发现过一会SLB的健康检查会失败。



☐	前端协议/端口	后端协议/端口	名称	状态	健康状态	监控	调度算法	会话保持	带宽峰值	服务器组	访问控制	操作
☐	HTTP:80	HTTP:80	http_80	● 运行中	● 异常		加权轮询	关闭	不限制	默认服务器组	未开启	配置 详情 添加转发策略 更多

通过服务器的抓包文件我们可以看到下面现象，符合前面介绍的七层HTTP健康检查的方式，我这里返回的是405而不是设定的200，所以SLB健康检查失败。

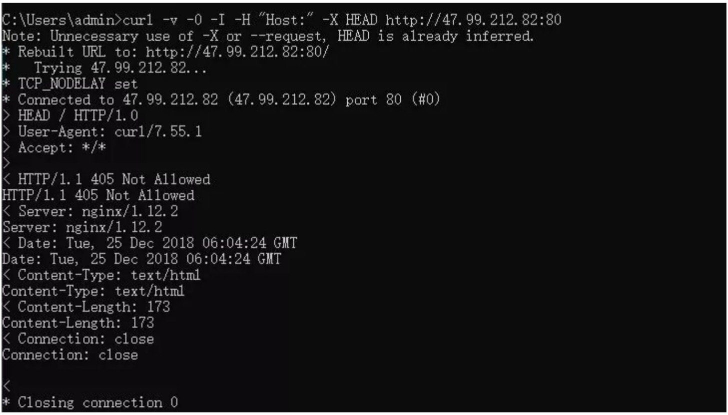


```
tcp.stream eq 1309
No.   Time        Source          Destination     Protocol Length Info
11847 165.871366  100.116.235.17  172.16.45.142   TCP      74 25123 → 80 [SYN] Seq=0 Win=29130 Len=0 MSS=1942 SACK_PERM=1 TSval=3054897529 TSecr=0 WS=512
11848 165.871374  172.16.45.142   100.116.235.17  TCP      74 80 → 25123 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=12970335 TSecr=3054897529 WS=128
11849 165.871978  100.116.235.17  172.16.45.142   TCP      66 25123 → 80 [ACK] Seq=1 Ack=1 Win=29184 Len=0 TSval=3054897530 TSecr=12970335
11850 165.871980  100.116.235.17  172.16.45.142   HTTP     85 HEAD / HTTP/1.0
11851 165.872001  172.16.45.142   100.116.235.17  TCP      66 80 → 25123 [ACK] Seq=1 Ack=20 Win=29056 Len=0 TSval=12970335 TSecr=3054897530
11852 165.872057  172.16.45.142   100.116.235.17  HTTP     218 HTTP/1.1 405 Not Allowed
11853 165.872077  172.16.45.142   100.116.235.17  TCP      66 80 → 25123 [FIN, ACK] Seq=153 Ack=20 Win=29056 Len=0 TSval=12970336 TSecr=3054897530
11854 165.872676  100.116.235.17  172.16.45.142   TCP      66 25123 → 80 [ACK] Seq=20 Ack=153 Win=30208 Len=0 TSval=3054897530 TSecr=12970336
11855 165.872678  100.116.235.17  172.16.45.142   TCP      66 25123 → 80 [RST, ACK] Seq=20 Ack=154 Win=30208 Len=0 TSval=0 TSecr=12970336
```

如果后端ECS实例的服务关闭HEAD方法，会导致健康检查失败。建议在本地用HEAD方法访问ECS公网IP地址进行测试：

```
curl -v -0 -I -H "Host:" -X HEAD http://IP:port
```

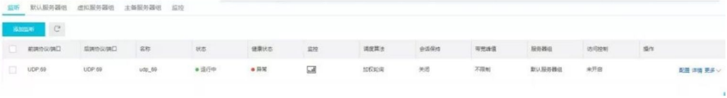
直接访问服务器是可以看HEAD方法也是返回失败的，也可以验证是健康检查失败的原因是由于服务器HEAD的方法处理不正确的原因。



```
C:\Users\admin>curl -v -0 -I -H "Host:" -X HEAD http://47.99.212.82:80
Note: Unnecessary use of -X or --request, HEAD is already inferred.
* Rebuilt URL to: http://47.99.212.82:80/
*   Trying 47.99.212.82...
* TCP_NODELAY set
* Connected to 47.99.212.82 (47.99.212.82) port 80 (#0)
> HEAD / HTTP/1.0
> User-Agent: curl/7.55.1
> Accept: */*
>
< HTTP/1.1 405 Not Allowed
HTTP/1.1 405 Not Allowed
< Server: nginx/1.12.2
Server: nginx/1.12.2
< Date: Tue, 25 Dec 2018 06:04:24 GMT
Date: Tue, 25 Dec 2018 06:04:24 GMT
< Content-Type: text/html
Content-Type: text/html
< Content-Length: 173
Content-Length: 173
< Connection: close
Connection: close

<
* Closing connection 0
```

四层UDP监听

创建一个新的 UDP 监听TFTP服务，TFTP是基于UDP协议的，创建好的监听状态是正常的。

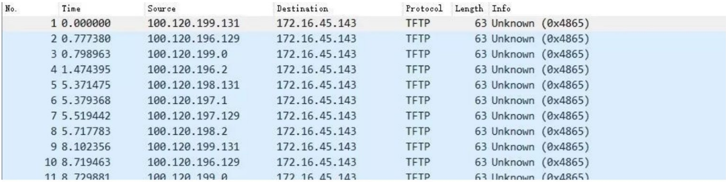


☐	前端协议/端口	后端协议/端口	名称	状态	健康状态	监控	调度算法	会话保持	带宽峰值	服务器组	访问控制	操作
☐	UDP:69	UDP:69	udp_69	● 运行中	● 异常		加权轮询	关闭	不限制	默认服务器组	未开启	配置 详情 更多

抓包命令替换为UDP协议, 服务器抓包看到SLB是不断通过UDP报文探测,服务器不反馈ICMP unreachable,SLB 即认为

ECS监听状态正常。

```
tcpdump udp -i eth0 -w ./target.cap
```



```
No.        Time          Source             Destination        Protocol  Length Info
         1 0.000000      100.120.199.131    172.16.45.143      TFTP          63 Unknown (0x4865)
         2 0.777380      100.120.196.129    172.16.45.143      TFTP          63 Unknown (0x4865)
         3 0.798963      100.120.199.0      172.16.45.143      TFTP          63 Unknown (0x4865)
         4 1.474395      100.120.196.2      172.16.45.143      TFTP          63 Unknown (0x4865)
         5 5.371475      100.120.198.131    172.16.45.143      TFTP          63 Unknown (0x4865)
         6 5.379368      100.120.197.1      172.16.45.143      TFTP          63 Unknown (0x4865)
         7 5.519442      100.120.197.129    172.16.45.143      TFTP          63 Unknown (0x4865)
         8 5.717783      100.120.198.2      172.16.45.143      TFTP          63 Unknown (0x4865)
         9 8.102356      100.120.199.131    172.16.45.143      TFTP          63 Unknown (0x4865)
        10 8.719463      100.120.196.129    172.16.45.143      TFTP          63 Unknown (0x4865)
        11 8.729881      100.120.199.0      172.16.45.143      TFTP          63 Unknown (0x4865)
```

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。**健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。**开启健康检查功能后，当后端某台ECS健康检查出现异常时，负载均衡会自动将新的请求分发到其它健康检查正常的ECS上；而当该ECS恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。如果您的业务对负载敏感性高，高频率的健康检查探测可能会对正常业务访问造成影响。**您可以结合业务情况，通过降低健康检查频率、增大健康检查间隔、七层检查修改为四层检查等方式，来降低对业务的影响。但为了保障业务的持续可用，不建议关闭健康检查。**

参考：

https://help.aliyun.com/knowledge_detail/60152.html

https://help.aliyun.com/document_detail/98226.html

https://help.aliyun.com/document_detail/85959.html

抓包文件：

https://github.com/Dushibing/SLBPacketcapture

关于贝斯平

贝斯平是一家提供端到端解决方案的云服务提供商，通过软件定义服务，利用多云及混合云部署，为企业提供快速转型方案。我们致力于利用自动化在各种不同云环境下实现新型运维模式，快速将传统应用转型到多云环境，帮助企业在云上实现成本控制及优化，并使业务更加智能。2017-2019年连续三年入

选Gartner MSP魔力象限的公司，其自主研发的智能混合多云管理平台——OpsNow可在多云接入的基础上，通过智能运维实现科技赋能，帮助企业轻松驾驭云IT，成为数字化转型中的领先者。

BESPIN GLOBAL

想了解更多云服务业务吗？
想与贝斯平云专家1对1沟通吗？

快快扫描下方二维码

微信公众账号

立即咨询