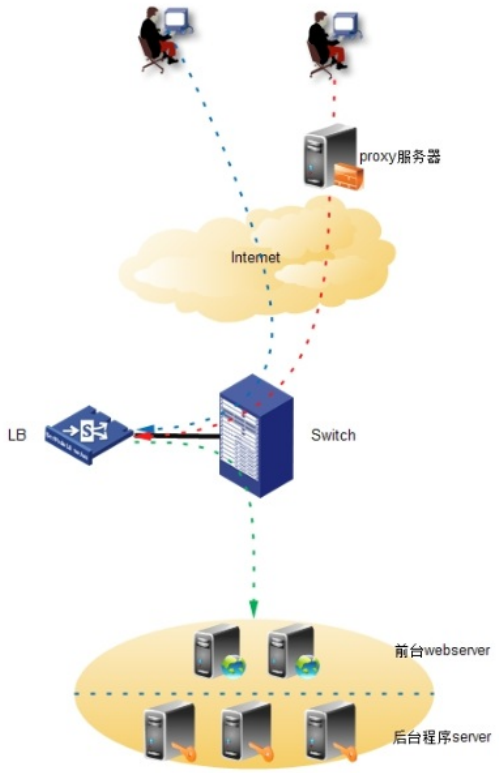
V7负载均衡七层负载源地址插入配置案例

七层服务器负载均衡　屈剑峰　2016-07-01 发表

客户为了对外提供HTTP访问服务，一般会在内网部署服务器负载均衡设备以满足高并发量的访问需求，但运行在服务器上的应用程序有时需要获取过来访问的客户端真实ip地址信息，由于在访问的过程中可能经过代理服务器、LB等设备，到达业务服务器上真实客户端ip地址被隐藏，导致服务器上的业务程序无法获取客户端真实ip地址而导致访问业务异常。因此，需要在代理服务器、负载均衡设备上开启源地址插入功能（X-Forwarded-For）,将客户端的真实ip插入HTTP报文头中，服务器上的应用程序会解析识别出HTTP请求头字段获取客户端真实ip地址。



1. 配置健康性检查策略

```
nqa template http http_check
 probe timeout 7000
  //探测本次超时7s（一次探测的超时时间，默认单位为毫秒）
 url /webapp/check.zul
 //探测的url路径
 expect data ok
  //期望应答内容为ok表示健康性检测正常；或expect status 200期望应答http状态码200，表示健康性检测正常；
```

2. 配置实服务策略

```
real-server test_134.130.3.10_10051
 ip address 134.130.3.10
 port 10051
 server-farm test            //加入实服务组中
 probe http_check            //调用七层健康性检测
real-server test_134.130.3.11_10051
 ip address 134.130.3.11
 port 10051
 server-farm test            //加入实服务组中
 probe http_check            //调用七层健康性检测
```

3. 配置持续性组策略

```
sticky-group fjtelecom_persist_sourceip type address-port   //配置持续性组
 ip source                                  //根据源ip地址进行持续性
```

timeout 1800 //超时1800秒

4. 配置SNAT地址池策略

loadbalance snat-pool snat_crm2.0

ip range start 10.10.10.52 end 10.10.10.54 //配置负载均衡SNAT地址池

5. 配置实服务组策略

server-farm test //配置实服务组并引用地址池

fail-action reschedule //重定向连接；建议keep（保持已有连接）

snat-pool snat_crm2.0 //引用snat地址池

6. 配置loadbalance策略 //配置lb-policy策略

1） 配置http header插入x-forwarded-for字段

loadbalance class c1 type http

match 1 header X-Forwarded-For value (.*)

//流匹配策略，match http-header有X-Forwarded-For且带的任意值的报文流量

match 2 source ip address 1.1.1.1

//流匹配策略，match 源ip地址为1.1.1.1

#

loadbalance action a1 type http

server-farm test sticky fjtelecom_persist_sourceip

header insert request name X-Forwarded-For value %is

//在http header插入X-Forwarded-For字段，值为源ip地址信息，%is表示往后插源ip地址（%is:%ps表示往后插源地址和源端口）。

header insert response name x-forwarded-for value %is

//在http response方向 header插入X-Forwarded-For字段，值为源ip地址信息，%is表示往后插源ip地址（%is:%ps表示往后插源地址和源端口）。

#

loadbalance action a2 type http

server-farm test sticky fjtelecom_persist_sourceip

header rewrite request name X-Forwarded-For value (.*) replace "%1, %is"

//重写http header 的X-Forwarded-For字段value值，replace中的%1表示小括号内容保持不变，%is表示往后插源ip地址。

注意：replace格式为”%1,[空格]%is”.

#

loadbalance policy lb type http

class c1 action a2 //匹配流量c1并执行a2动作

default-class action a1 //默认执行a1动作

2）配置http header插入x-clinetip字段（与插入XFF效果一样，只是插入的名字不一样，视客户服务器应用程序识别而定，不详述….）

loadbalance class c11 type http

match 2 header X-ClientIP value (.*)

#

loadbalance action a11 type http

server-farm test sticky fjtelecom_persist_sourceip

header insert request name X-ClientIP value %is

#

loadbalance action a22 type http

server-farm stest sticky fjtelecom_persist_sourceip

header rewrite request name X-ClientIP value (.*) replace "%1, %is"

#

loadbalance policy lb type http

class c11 action a22

default-class action a11

7. 配置http request逐包插入命令

[L5000C]parameter-profile test type http //配置参数模板test

[L5000C-para-http-test] header modify per-request

//对每个连接的第一个HTTP请求或应答报文的首部执行插入、删除或修改操作，默认只对同一条流的第一个http报文插入或者修改。

[L5000C-para-http-test] case-insensitive

//关闭匹配字符串大小写敏感，当前版本默认大小不敏感

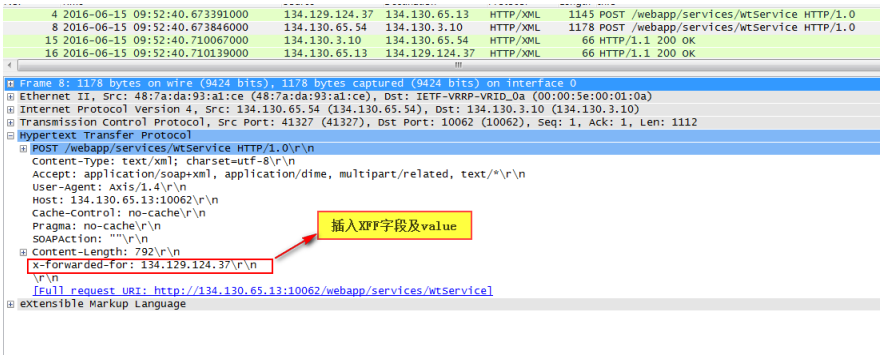
8. 配置虚服务策略

```
virtual-server vs_10.10.10.5_10062 type http
 port 10062
 virtual ip address 10.10.10.13
 lb-policy lb
 default server-farm test
    parameter http test        //虚服务调用参数模板
     service enable
```

验证测试及说明

如下图所示，http header头部插入了x-forwared-for，插入格式一般为:X-Forwarded-For: client1, proxy1, proxy2, proxy3；

特别说明：插入的字符时LB设备对大小写不敏感，即X-Forwarded-For会被插入显示为x-forwarded-for全部为小写，在之前请与客户确认和服务器程序对读取该字段是否存在大小写敏感，标准开发是不敏感的。



配置关键点及注意事项

关键点1：配置七层流量的loadbalance策略，需要match关键http流量并调用相应动作，执行源地址修改或者插入动作。

```
loadbalance class c1 type http
  match 2 header X-Forwarded-For value (.*)
#
loadbalance action a1 type http
 header insert request name X-Forwarded-For value %is
#
loadbalance action a2 type http
 header rewrite request name X-Forwarded-For value (.*) replace "%1, %is"
#
loadbalance policy lb type http
 class c1 action a2                //匹配流量c1执行a2动作
 default-class action a1           //默认执行a1动作
```

关键点2：需要修改为对http报文逐包插入，默认同一条流只对第一个http报文进行插入或者修改动作。

```
[L5000C]parameter-profile test type http
[L5000C-para-http-test] header modify per-request
```

关键点3：参数含义

要插入HTTP报文中的首部内容，为1～127个字符的字符串，也可以使用以下特定含义的字符串：

%%:表示往后插入 字符%。

%is:表示往后插入源IP地址或源IPv6地址。

%ps:表示往后插入源端口号。

%id:表示往后插入目的IP地址或目的IPv6地址。

%pd:表示往后插入目的端口号。

%[1-9]：表示Header值中通过()标记的字符串参数，如Header值为字符串(Wel)(co)(me),则%1表示”Wel”保持不变，%2表示“co”保持不变。