

# L5000基于URL的二次跳转重定向七层负载业务异常案例

七层服务器负载均衡 吴昊A 2023-12-28 发表

## 组网及说明

客户端--LB--实服务器

## 问题描述

设备LB基于URL做七层负载，客户端请求来的流量先请求带有testzzwxyURL的域名，然后通过后再跳转请求带有ish URL的域名，测试时发现客户端无法访问成功。

主要地址如下：

虚服务地址：192.140.203.12

SNAT地址：192.140.203.12

testzzwxy实服务器地址：192.141.83.3 8081

ish实服务器地址：192.141.8.73 8081 192.141.8.74 8081

LB主要配置如下：

```
#  
virtual-server gjjzzgrwsyw type http  
port 443  
virtual ip address 192.140.203.12  
parameter http pp-gjj  
lb-policy gjj_zzgrwsyw  
sticky COOKIE1  
ssl-server-policy gjj-20221221  
route-advertisement enable  
service enable  
#  
parameter-profile pp-gjj type http  
rebalance per-request  
#  
sticky-group COOKIE1 type http-COOKIE  
COOKIE insert  
check all-packet  
#  
loadbalance policy gjj_zzgrwsyw type http  
class gjj_zzgrwsyw_ish action https-upgrade  
class gjj_zzgrwsyw_testzzwx action gjjxcx_testzzwx  
#  
loadbalance class gjj_zzgrwsyw_ish type http match-any  
match 1 url ish  
#  
loadbalance class gjj_zzgrwsyw_testzzwx type http match-any  
match 1 url testzzwx  
#  
loadbalance action gjjxcx_testzzwx type http  
server-farm gjjxcx_testzzwx sticky COOKIE1  
header insert both name x-forwarded-for value %is  
#  
loadbalance action https-upgrade type http  
server-farm gjjzzgrwsyw_sf sticky COOKIE1  
header insert both name x-forwarded-for value %is  
header insert response name content-security-policy value upgrade-insecure-requests  
#  
server-farm gjjxcx_testzzwx  
predictor random  
snat-pool gjjzzgrwsyw_snat  
probe t1  
success-criteria at-least 1  
real-server gjjxcx_192.141.83.3_8081_testzzwx port 8081  
success-criteria at-least 1  
probe t1  
#
```

```

real-server gjjxcx_192.141.83.3_8081_testzzwx
ip address 192.141.83.3
port 8081
probe t1
success-criteria at-least 1
#
server-farm gjjzzgrwsyw_sf
predictor hash address source
snat-pool gjjzzgrwsyw_snat
probe t1
#
real-server gjjzzgrwsyw_192.141.80.73_8081
ip address 192.141.80.73
port 8081
server-farm gjjzzgrwsyw_sf
#
real-server gjjzzgrwsyw_192.141.80.74_8081
ip address 192.141.80.74
port 8081
server-farm gjjzzgrwsyw_sf
#

```

### 过程分析

通过再LB设备上抓包，发现LB七层负载代理请求时，针对testzzwxy URL的域名请求，设备可以正常转发到实服务器192.141.83.3 8081服务上，后续的域名跳转到ish后，设备依旧往192.141.83.3上负载，而不是向192.141.8.73/74上负载，导致服务器侧回复了404无效请求文件报错。

No.	time	Source	Destination	Protocol	Length	TB ID	Info
12 0.0005815	192.140.203.12	192.141.83.3		HTTP	74	0x00000000 (28566)	38111 + 8881 [SYN] Seq=1677886387 Win=65335 Len=0 RSSI=
13 0.0005895	192.141.83.3	192.140.203.12		TCP	24	0x00000000 (0)	38011 + 38111 [SYN, ACK] Seq=2158864499 Ack=1657706188
14 0.009326	192.140.203.12	192.141.83.3		TCP	66	0x07e7e (26597)	38111 + 8881 [ACK] Seq=1057806388 Ack=2568864391 Win=6
15 0.009364	192.140.203.12	192.141.83.3		HTTP	941	0x067e7 (26599)	GET /testzzwxy/gotccff.jsp?t=20231222000000000000 HTTP/1.1
15 0.010127	192.140.203.12	192.140.203.12		TCP	66	0x0f19f (64415)	38011 + 38111 [ACK] Seq=2568864391 Ack=1057807263 Win=2
17 0.011313	192.141.83.3	192.140.203.12		TCP	1374	0x0edc4 (28100)	38011 + 3881 [ACK] Seq=2568864399 Ack=1057807263 Win=2
20 0.012199	192.141.83.3	192.140.203.12		HTTP	1083	0x0fe7c (65223)	HTTP/1.1 200 OK (text/html)
22 0.012354	192.140.203.12	192.141.83.3		TCP	66	0x0e812 (26642)	38111 + 8881 [ACK] Seq=1057807263 Ack=256886636 Win=6
22 0.775661	192.140.203.12	192.141.83.3		HTTP	935	0x0ba40 (46656)	GET /ish/perm.jsp?t=20231222000000000000 HTTP/1.1
93 3.277165	192.141.83.3	192.140.203.12		HTTP	1071	0x0ab0f (40975)	HTTP/1.1 404 Not Found (text/html)
93 3.277165	192.140.203.12	192.141.83.3		HTTP	65	0x0a000 (0)	38111 + 3881 [ACK] Seq=1057808129 Ack=2568867641 Win=6
1875 11.707525	192.140.203.12	192.141.83.3		HTTP	993	0x0e599 (1489)	GET /testzzwxy/gotccff.jsp?t=20231222000000000000 HTTP/1.1
1876 11.718191	192.141.83.3	192.140.203.12		TCP	1374	0x0d52 (56402)	38011 + 38111 [ACK] Seq=2568867641 Ack=1057809059 Win=2
1879 11.718049	192.141.83.3	192.140.203.12		HTTP	1083	0x0dc54 (56404)	HTTP/1.1 200 OK (text/html)
1881 11.718049	192.140.203.12	192.141.83.3		TCP	66	0x0e18e (1758)	38111 + 3881 [ACK] Seq=1057809059 Ack=2568869886 Win=6
1881 11.797755	192.140.203.12	192.141.83.3		HTTP	899	0x0a08a (1486)	GET /ish/perm.jsp?t=20231222000000000000 HTTP/1.1
1887 11.799381	192.141.83.3	192.140.203.12		HTTP	1871	0x0ef2f (28463)	HTTP/1.1 404 Not Found (text/html)
1889 11.973444	192.140.203.12	192.141.83.3		TCP	66	0x01cf (7359)	38111 + 8881 [ACK] Seq=1057809988 Ack=2568870891 Win=6
1891 12.493791	192.140.203.12	192.141.83.3		HTTP	941	0x0bd5d (19293)	GET /testzzwxy/gotccff.jsp?t=20231222000000000000 HTTP/1.1
1893 12.495890	192.141.83.3	192.140.203.12		TCP	1374	0x0edc4 (28100)	38011 + 38111 [ACK] Seq=2568870891 Ack=1057810855 Win=2

根据抓包定位问题出现在这个地方，针对这种二次跳转域名，并且域名服务器地址或者端口不同的业务模型，需要开启逐次请求转发，即每来一个报文设备就重新根据LB policy策略进行负载调度。查看配置中是配置了并且调用了模版参数：

```

#
virtual-server gjjzzgrwsyw type http
port 443
virtual ip address 192.140.203.12
parameter http pp-gjj
lb-policy gjj_zzgrwsyw
sticky COOKIE1
ssl-server-policy gjj-20221221
route-advertisement enable
service enable
#
parameter-profile pp-gjj type http
rebalance per-request
#

```

正常情况下调用了逐次请求后，这种业务模型会重新负载到对应的域名服务器上请求报文，但是现场配置中在虚服务下调用了持续性组，虚服务下调度的持续性优先级最高，过来的流量匹配了持续性组后，就不会继续匹配lb-policy，所以导致后续跳转的ish域名请求不会负载到正确的实服务器上。

```

#
virtual-server gjjzzgrwsyw type http
port 443
virtual ip address 192.140.203.12
parameter http pp-gjj
lb-policy gjj_zzgrwsyw
sticky COOKIE1
ssl-server-policy gjj-20221221
ssn

```

```
route-advertisement enable
service enable
#
sticky-group COOKIE1 type http-COOKIE
COOKIE insert
check all-packet
#
```

### 解决方法

解决方案是取消虚服务下调用的持续性组

```
#  
virtual-server gjjzzgrwsyw type http  
port 443  
virtual ip address 192.140.203.12  
parameter http pp-gjj  
lb-policy gjj_zzgrwsyw  
sticky COOKIE1 undo掉  
ssl-server-policy gjj-20221221  
route-advertisement enable  
service enable  
#  
如果客户又持续性组的需求，可以在负载动作中进行调用，例如：  
#  
loadbalance action gjjxcx_testzzwx type http  
server-farm gjjxcx_testzzwx sticky COOKIE1  
header insert both name x-forwarded-for value %is  
#  
loadbalance action https-upgrade type http  
server-farm gjjzzgrwsyw_sf sticky COOKIE1  
header insert both name x-forwarded-for value %is  
header insert response name content-security-policy value upgrade-insecure-requests  
#
```

附件下载: zhuabao.rar