LVS防火墙标记及session保持

防火墙标记

> 在Linux上实现防火墙框架的netfilter中，存在所熟知的“四表五链”，其中mange表可以定义的规则的功能是可以对通过主机的报文进行铲除、修改、封装功能。在mange表的PREROUTING链上定义规则，对通过主机的某几种不同报文(访问不服务、通过不端口等)打上统一的标记。然后利用LVS的管理工具ipvsadm定义集群服务规则。**利用通过对报文打标记的方式，带来的好处是可以对不同的服务进行统一的调度。**
>
> 在定义防火墙规则时，使用`-j MARK --set-mark NUMBER`选项对某种报文定义打标记。
>
> 定义集群服务规则时，使用`-f MARK` 选项例如`ipvsadm -A -f 10 -s rr`，进行定义。

示例

> 对通过80端口和443端口的报文进行统一标记，然后定义lvs集群服务进行统一调度

```
# 定义防火墙规则
iptables -t mangle -A PREROUTING -d 192.168.1.149 -p tcp --dport 80 -j MARK --set-mark 8
iptables -t mangle -A PREROUTING -d 192.168.1.149 -p tcp --dport 443 -j MARK --set-mark 8
#定义lvs规则
ipvsadm -A -f 8 -s rr
ipvsadm -a -f 8 -r 192.168.1.151 -g
ipvsadm -a -f 8 -r 192.168.1.152 -g
```

session保持

> lvs的sh调度算法对某一个特定服务为可以实现session保持，但对多个共享RS的集群服务，则需要统一进行绑定。lvs的persistence机制，即持久连接，可以实现将来自同一客户端的请求在一定时间内调度到同一个Real Server中。此种方式对适用于任何算法。LVS持久连接有多种方式， 要实现LVS持久连接，需要维护一个持久连接模板。记录客户端和第一个请求调度到那个Real Server中信息，及保持记录的时间。

LVS持久连接的三种方式

```
# 针对的那个服务进行持久调度
ipvsadm -A -t 192.168.1.149:80 -s rr -p
ipvsadm -a -t 192.168.1.149:80 -r 192.168.1.151 -g
ipvsadm -a -t 192.168.1.149:80 -r 192.168.1.151 -g
```

```
# 针对有防火墙标记的进行持调度
ipvsadm -A -f 10 -s rr
ipvsadm -a -f 10 -r 192.168.1.151 -g
ipvsadm -a -f 10 -r 192.168.1.152 -g
```

```
# 针对对访问的客户端进行持久调度
ipvsadm -A -t 192.168.1.149:0 -s rr -p
ipvsadm -a -t 192.168.1.149:0 -r 192.168.1.151 -g
ipvsadm -a -t 192.168.1.149:0 -r 192.168.1.151 -g
```