**Keepalived+ lvs**

【实验二：keepalived+LVS】(keepalived带健康检查功能 解决了lvs不带健康健康检查的功能)

proxy(主) |web1

client------->VIP --------

proxy2(备) |web2

【环境准备】

proxy主机的IP:192.168.4.5/24

proxy2主机的IP:192.168.4.6/24 (新建一台虚拟机)

web1主机的IP:192.168.4.100/24

web2主机的IP:192.168.4.200/24

#备注:我们需要做的是LVS-DR实验,所以web1和web2需要伪装VIP

#这个只要确保第一天课程LVS-DR的实验环境依然存在即可.

#【警告】实验二和实验一有冲突！！

#做实验二前一定要把web1和web2的keepalived关闭!!!!

#这个实验我们使用keepalived实现两台调度器的热备

#两台调度器的VIP是192.168.4.15

【配置proxy主机的keepalived】

[root@proxy ~]# yum -y install keepalived

[root@proxy2 ~]# yum -y install keepalived

[root@proxy ~]# vim /etc/keepalived/keepalived.conf

router\_id LVS1 #12行设置设备的ID号

vrrp\_iptables #13行手动插入该内容

interface ens34 #22行(需要使用ip a s查看下4网段的网卡名)

30,31,32行内容修改如下:

virtual\_ipaddress {

192.168.4.15

}

#35行往下的内容,修改后效果如下:

virtual\_server 192.168.4.15 80 {

delay\_loop 6

lb\_algo rr #调度算法RR轮询

lb\_kind DR #工作模式DR

persistence\_timeout 50 #【一定删除这一行】保持连接50秒

protocol TCP #协议TCP

real\_server 192.168.4.100 80 { #后端真实服务器

weight 1 #权重

TCP\_CHECK { #健康检查

connect\_timeout 3 #健康检查的超时时间3秒

nb\_get\_retry 3 #健康检查的重试次数3次

delay\_before\_retry 3 #健康检查的间隔时间3秒

}

}

real\_server 192.168.4.200 80 {

weight 1

TCP\_CHECK {

connect\_timeout 3

nb\_get\_retry 3

delay\_before\_retry 3

}

}

}

ESC,:wq保存退出编辑器

[root@proxy ~]# rm -rf /etc/sysconfig/network-scripts/ifcfg-ens34:0

把Day01这天LVS-DR实验所做的VIP删除(网卡名称不能照抄)

[root@proxy ~]# systemctl restart network

[root@proxy ~]# ipvsadm -C

[root@proxy ~]# systemctl restart keepalived

[root@proxy ~]# ip a s #查看VIP

[root@proxy ~]# ipvsadm -Ln #查看LVS

[root@proxy ~]# scp /etc/keepalived/keepalived.conf 192.168.4.6:/etc/keepalived/

备用服务器4.6上面,只需要修改VRRP的配置即可.

[root@proxy2 ~]# vim /etc/keepalived/keepalived.conf

router\_id LVS2 #12行设置设备的ID号

state BACKUP #21行

interface ens34 #22行,需要通过ip a s查看下4网段的网卡名

priority 50 #24行

[root@proxy2 ~]# systemctl restart keepalived

[root@proxy2 ~]# yum -y install ipvsadm

[root@proxy2 ~]# ipvsadm -Ln

#可以查看到LVS集群规则

[root@proxy2 ~]# ip a s ens34

#默认看不到VIP,当主服务器宕机时VIP会自动漂移过来.

补充:

proxy2关闭防火墙和SELinux

[root@proxy2 ~]# firewall-cmd --set-default-zone=trusted

[root@proxy2 ~]# sed -i '/SELINUX/s/enforcing/permissive/' /etc/selinux/config

[root@proxy2 ~]# setenforce 0