keepalived热备:

global\_defs : 为全局配置 , 无实质性功能

vrrp : 虚拟路由热备

virtual\_serber : LVS虚拟服务器

smtp : 没配post无作用

state MASTER           //主服务器为MASTER（备服务器需要修改为BACKUP）

priority 100                 //服务器优先级,优先级高优先获取VIP (浮动ip)

virtual\_ipaddress { //谁是主服务器谁获得该VIP（实验需要修改）

192.168.4.80

auth\_pass 1111          //主备服务器密码必须一致

注 :

攻击方式 : 不需要破解密码与漏洞 , 也可在另一台服务器搭一个keepalived , 把优先级改的比目前高 , 谁优先级高 , 谁就是主服务器 , 就访问谁 , 那么正常网站就打不开

优先级最高255

若优先级相等 , 谁IP大 , 谁的优先级高

两个台keepalived 密码 1111 相同 , 优先级不同 , 无密码就不能访问

若改了一台密码 , 另一台也得改

启动keepalived会自动添加一个drop的防火墙规则(非firewall)需要iptables -F清空

搭建好keepalived后 , 使用 ip a s eth0 检查 , 那个有VIP , 那个就是主服务器

curl http:// VIP

Keepalived+LVS

步骤一 :

web1 设置伪装ip 4.15 lo:0 web2同样操作

防止以后IP冲突 /etc/sysconfig/**network-scripts/**

上两行 禁止进入 (别人ping ip时不搭理)

下两行 禁止出去(不发arp广播)

Ip冲突原因 : ping或以广播形式发数据包 , 有两个人同时回信息就不知道信谁

(并不是两台电脑有相同ip)

步骤二 : web1 web2 搭Apache

步骤三 : proxy1 proxy2 两台LVS调度器装包keepalived

先改配置 ----> 热备

virtual\_server : 用户访问的服务器 -----> virtual\_server这一点就是自动配LVS

转发到

每个real\_server : web服务器 100 200

调度算法 rr 工作模式 DR (伪装不能用NAT)

persistence\_timeout 50 必须注释或删除 , (保持50秒内不跳转) 不删也不会产生语法报错

TCP协议

健康检查就是对 web1 web2检查

对网页健康检查方式 : (不可在已坏的机器上运行脚本检查)

curl 测ip(是否开机)+网页+端口

ping 测ip(是否开机)

systemctl status 必须开机才能测试 (网页的哈希值)

curl +http://(web1或web2)ip地址 | md5sum ----->底下输出ID (一改就变)

TCP\_CHECK{} : 仅检查端口 , 被攻击是没法检查,如在网页上传攻击文件

(填多久检查一次即可) (注入攻击)

HTTP\_GET{} : 检查端口页面内容 ,

SSL\_GET{}

做健康检查必须步骤:

connect\_timeout 3 #每隔3秒测一次(测网页占cpu)

nb\_get\_retry 3 #重复3次

delay\_before\_retry 3 #超时时间3秒 , 若不回就删除

HAProxy 纯粹的调度器

支持正则 ,

支持健康检查 ,

支持权重设置 ,

调度算法丰富

4层调度很稳定(TCP , 可以对Mysql进行负载均衡)

-效率 负载均衡速度 , 高于nginx , 低于LVS

-正则弱于nginx

-日志依赖于syslogd (无独立日志) F5硬件 F5 big-ip

HAProxy原理与nginx一样 , 帮忙访问web

日志依赖其他软件

Pidfile 放 /var/run/haproxy.pid

Maxconn 并发量

Mode 集群 http 4层调度器

HAProxy做集群:

Listen websrv(自定义名字) \*:80

Server inter 检查