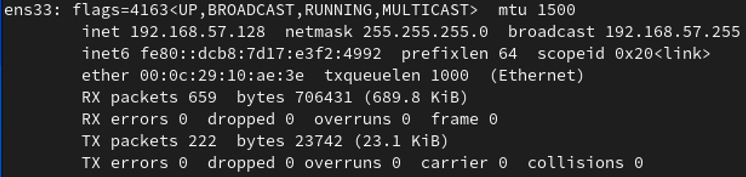
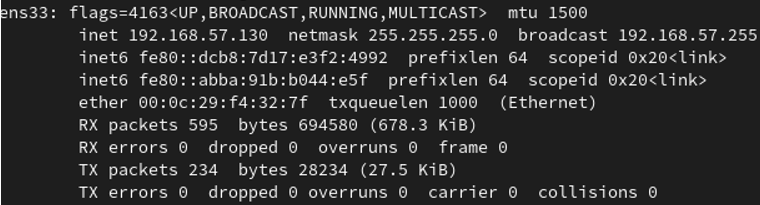
**实验：配置rsyslog并使用logger工具测试远程日志功能**

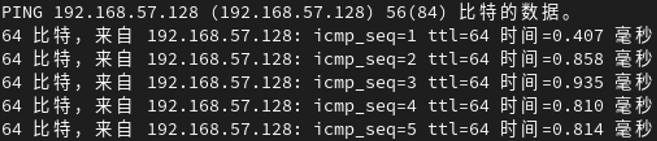
1. **复制虚拟机，并配置两台主机，使得相互之间能够ping通对方。**

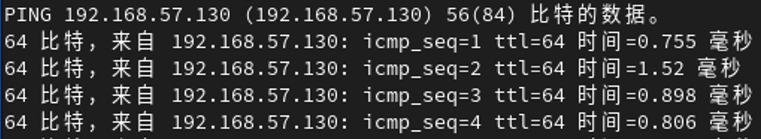
**两台主机的网卡信息：**

****

****

**互相ping通**

****

****

1. **关闭两台主机的防火墙以及SeLinux。**

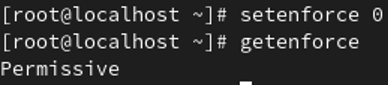
**关闭防火墙: systemctl stop firewalld.service**

**关闭selinux:**

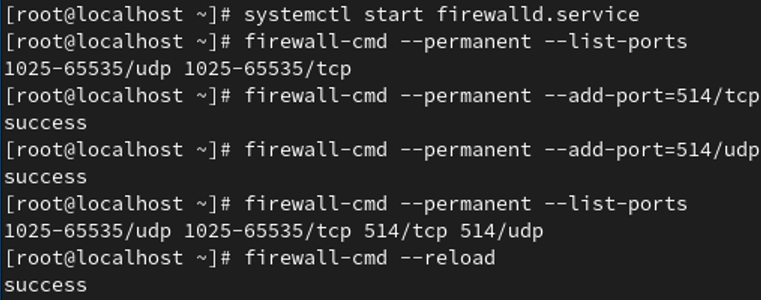
**setenforce 0 //关闭**

**getenforce //查看**

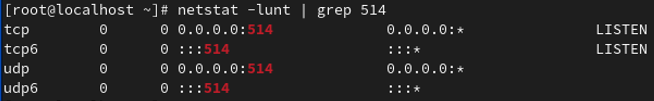
****

****

1. **配置远程日志主机，打开udp:514端口和tcp:514端口。**

****

1. **查看远程日志主机端口是否打开：netstat –lunt | grep 514**

****

1. **分别在远程主机以及本地主机上配置/etc/rsyslog.conf，对mail设备进行记录，其中本地主机的action设置为@(远程主机的)IP地址，远程日志主机的action为本地日志文件。**

****

1. **使用logger –p mail.info “测试文字” 进行测试。测试之后分别在远程主机和本地主机上查看日志文件记录/var/log/maillog。**

**本地主机：**

****

**远程主机：**

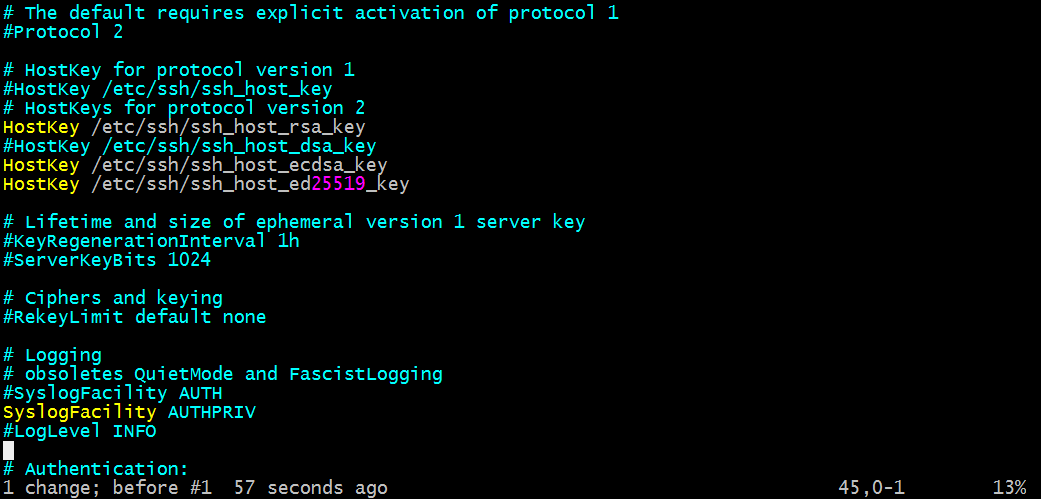
****

**（以下为选做实验）**

**实验：将ssh服务的日志换个位置存储**

vim /etc/ssh/sshd\_config

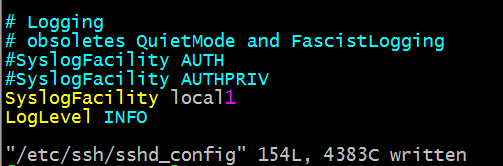
原来是这样的



#SyslogFacility AUTHPRIV 注释掉

SyslogFacility local1

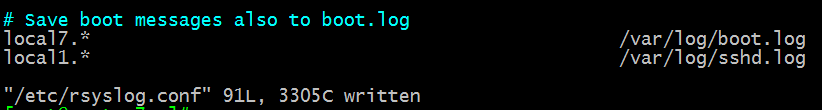
LogLevel INFO 去掉注释



vim /etc/rsyslog.conf

加上这一行

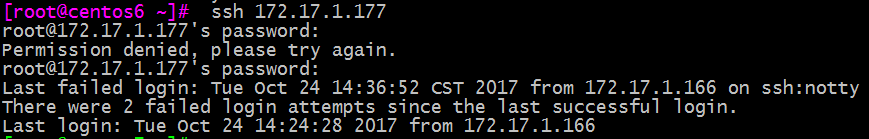
local1.\* /var/log/sshd.log



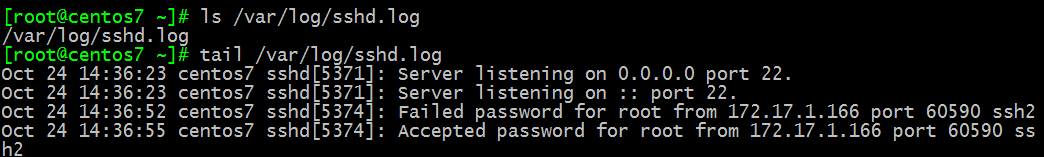
[root@centos7 ~]# systemctl restart rsyslog

[root@centos7 ~]# systemctl restart sshd

测试：从另一台机器166 ssh 172.17.1.177



在177机器上看我们指定的日志件/var/log/sshd.log是否生成,生成则成功。

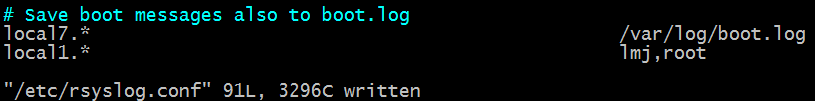


**实验：有人ssh登录发消息就通知root和lmj用户**

vim /etc/rsyslog.conf

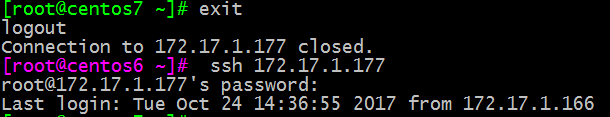
加上这一行，但这样不会写在文件里

local1.\* lmj,root



[root@centos7 ~]# systemctl restart rsyslog

测试：从另一台机器166 ssh 172.17.1.177



root用户收到通知

clip_image008

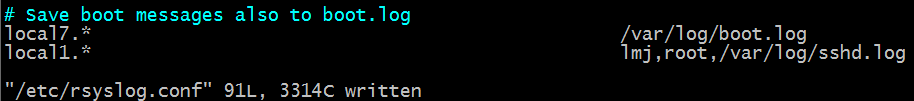
lmj用户收到通知

clip_image009

**实验：有人ssh登录发消息就通知root和lmj用户，也记录在/var/log/sshdd.log里**

vim /etc/rsyslog.conf

local1.\* lmj,root,/var/log/sshd.log



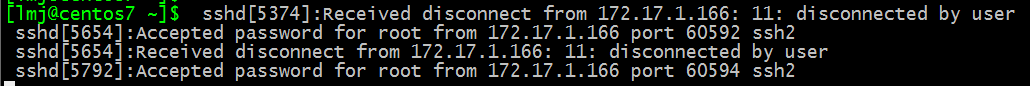
[root@centos7 ~]# systemctl restart rsyslog

测试：

clip_image011

root，lmj用户收到通知

clip_image012



文件/var/log/sshd.log 中也存储了日志

