链滴

Linux 限制 ip 登录

作者：MingGH
原文链接：https://ld246.com/article/1595585545617
来源网站：链滴

登录后台的时候发现服务器被尝试登录300多次，没想到，找了个简单的办法，还真有效

1. 查看服务器失败登录ip，以及时间

lastb > temp.txt

```
avanthi  ssh:notty    79.182.96.157    Sat Jul  4 20:38 - 20:38  (00:00)
avanthi  ssh:notty    79.182.96.157    Sat Jul  4 20:38 - 20:38  (00:00)
root     ssh:notty    58.62.167.126    Sat Jul  4 18:43 - 18:43  (00:00)
root     ssh:notty    58.62.167.126    Sat Jul  4 18:42 - 18:42  (00:00)
root     ssh:notty    58.62.167.126    Sat Jul  4 18:42 - 18:42  (00:00)
root     ssh:notty    58.62.167.126    Sat Jul  4 18:42 - 18:42  (00:00)
dircreat ssh:notty    36.72.10.177     Fri Jul  3 00:27 - 00:27  (00:00)
dircreat ssh:notty    36.72.10.177     Fri Jul  3 00:27 - 00:27  (00:00)
guest    ssh:notty    87.116.175.8     Thu Jul  2 19:51 - 19:51  (00:00)
guest    ssh:notty    87.116.175.8     Thu Jul  2 19:51 - 19:51  (00:00)
sniffer  ssh:notty    157.32.175.94    Thu Jul  2 18:02 - 18:02  (00:00)
sniffer  ssh:notty    157.32.175.94    Thu Jul  2 18:01 - 18:01  (00:00)
Administ ssh:notty    124.120.3.40     Thu Jul  2 14:50 - 14:50  (00:00)
Administ ssh:notty    124.120.3.40     Thu Jul  2 14:50 - 14:50  (00:00)
root     ssh:notty    179.132.253.70   Thu Jul  2 13:33 - 13:33  (00:00)
ubnt     ssh:notty    179.132.253.70   Thu Jul  2 13:33 - 13:33  (00:00)
ubnt     ssh:notty    179.132.253.70   Thu Jul  2 13:33 - 13:33  (00:00)
root     ssh:notty    179.132.253.70   Thu Jul  2 13:33 - 13:33  (00:00)
root     ssh:notty    179.132.253.70   Thu Jul  2 13:33 - 13:33  (00:00)
admin    ssh:notty    78.83.123.73     Thu Jul  2 08:02 - 08:02  (00:00)
admin    ssh:notty    78.83.123.73     Thu Jul  2 08:02 - 08:02  (00:00)
admin    ssh:notty    37.152.131.25    Thu Jul  2 08:02 - 08:02  (00:00)
admin    ssh:notty    37.152.131.25    Thu Jul  2 08:02 - 08:02  (00:00)
support  ssh:notty    78.229.91.207    Thu Jul  2 03:53 - 03:53  (00:00)
support  ssh:notty    78.229.91.207    Thu Jul  2 03:53 - 03:53  (00:00)
noc      ssh:notty    183.82.102.190   Wed Jul  1 19:22 - 19:22  (00:00)
noc      ssh:notty    183.82.102.190   Wed Jul  1 19:22 - 19:22  (00:00)
tech     ssh:notty    202.129.196.98   Wed Jul  1 14:53 - 14:53  (00:00)
tech     ssh:notty    202.129.196.98   Wed Jul  1 14:53 - 14:53  (00:00)
tech     ssh:notty    171.228.176.206  Wed Jul  1 14:44 - 14:44  (00:00)
tech     ssh:notty    171.228.176.206  Wed Jul  1 14:44 - 14:44  (00:00)
nagesh   ssh:notty    180.183.233.69   Wed Jul  1 14:43 - 14:43  (00:00)
nagesh   ssh:notty    180.183.233.69   Wed Jul  1 14:43 - 14:43  (00:00)
admina   ssh:notty    85.132.4.134     Wed Jul  1 14:34 - 14:34  (00:00)
admina   ssh:notty    85.132.4.134     Wed Jul  1 14:34 - 14:34  (00:00)
sniffer  ssh:notty    1.54.45.248      Wed Jul  1 14:29 - 14:29  (00:00)
sniffer  ssh:notty    1.54.45.248      Wed Jul  1 14:29 - 14:29  (00:00)
administ ssh:notty    124.13.9.44      Wed Jul  1 11:46 - 11:46  (00:00)
```

想着搞破坏的人还不少

然后将其中的ip通过正则提取出来

正则表达式
(([01]{0,1}\d{0,1}\d|2[0-4]\d|25[0-5])\.){3}([01]{0,1}\d{0,1}\d|2[0-4]\d|25[0-5])

2. 禁用ip登录

vim /etc/hosts.deny

将上面的提取的ip添加进去

sshd:ip地址

保存即可，测试过指定ip的确实登录不了了

原文链接：Linux 限制 ip 登录

3. 后续

后来吧，我嫌弃这种方式太麻烦了，得完全手动操作，为啥不写个shell脚本呢

```
#bin/bash
#脚本产生日志文件位置
logFile=/root/limitLogin/log/limitlogin.log
#脚本产生的临时文件，执行完会自动删除，不用修改，默认是linux临时目录
tmpLogFile=/usr/lib/tmpfiles.d/login.tmp.txt
#禁用ip登录的文件，不用修改
denyfile=/etc/hosts.deny

#开始执行
echo "start limit login task,now is `date` " >> $logFile

# 从lastb命令创建临时文件
lastb > $tmpLogFile
if [ -f $tmpLogFile ];then
   echo "login file already created,now begin handler" >> $logFile
fi

#处理文件，正则过滤，然后去重，判断hosts.deny文件中是否已经存在这个ip，不存在的话进行追加
grep  '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}' $tmpLogFile -o | sort -u | while read li
e
do
   if [ `grep -c "${line}" $denyfile` -eq '0' ];then
      echo "sshd:$line" >> $denyfile
   else
      echo "$line already exist" >> $logFile
   fi

done

echo "end limit login task,now is `date` " >> $logFile
#删除临时文件
rm $tmpLogFile
```

再做一个定时任务，每天执行一下

3.1 安装crond

```
yum install vixie-cron
yum install crontabs
```

编写定时任务

```
crontab -e
```

进入编辑模式，每一行就是一个定时任务

```
0 1 * * * /root/loginLimitTask/limit.sh >> /root/loginLimitTask/limitTaskLog.log
```

每天1点执行一次

开启crond开机启动，打开crond

```
systemctl start crond
```

将脚本权限改一下

```
chmod -x /root/loginLimitTask/limit.sh
```

4. 注意事项

不要把你自己的IP加到hosts.deny文件中，不然只能通过云服务器控制台进行连接