# **Linux Agent部署**

# 注意点：

数据库审计防火墙需对Agent制定端口开放，默认为9999和9998，（内网环境默认放通）2、数据库服务器 和 AAS 之前如果有防火墙，注意要把TCP的9999、9998端口放开。Agent和数据库审计之间是通过TCP进行连接的，有时候虽然能ping通，但是中间的防火墙有可能会阻断TCP连接。

1. **Agent连接的前置条件是：审计设备授权已上传并且为可用状态**
2. **Agent所在主机与数据库审计之间网络可达（可以ping测试）**
3. **Agent 所运行的系统上需要先安装 libpcap 软件**

①首先根据《检验libpcap安装是否成功》判断是否已经安装了libpcap,

，若有就无需安装所提供的libpcap包。

②环境要求：因为是源码安装，故必须有gcc,felx,bison，否则

./configure会报错，缺少flex或者缺少yacc，

缺少felx，执行yum install felx，

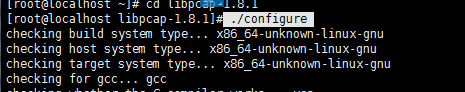
缺少yacc，执行yum install bison。

若无法编译，则需要安装gcc，yum install gcc\*

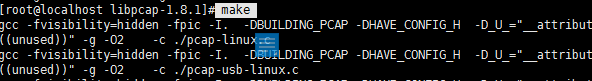
若系统内置无libpcap则将libpcap-1.8.1.tar置于任意目录，执行解压 tar -zxvf libpcap-1.8.1.tar

进入解压目录cd libpcap-1.8.1，依次执行

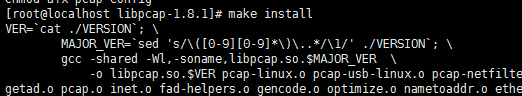
./configure



make



make install

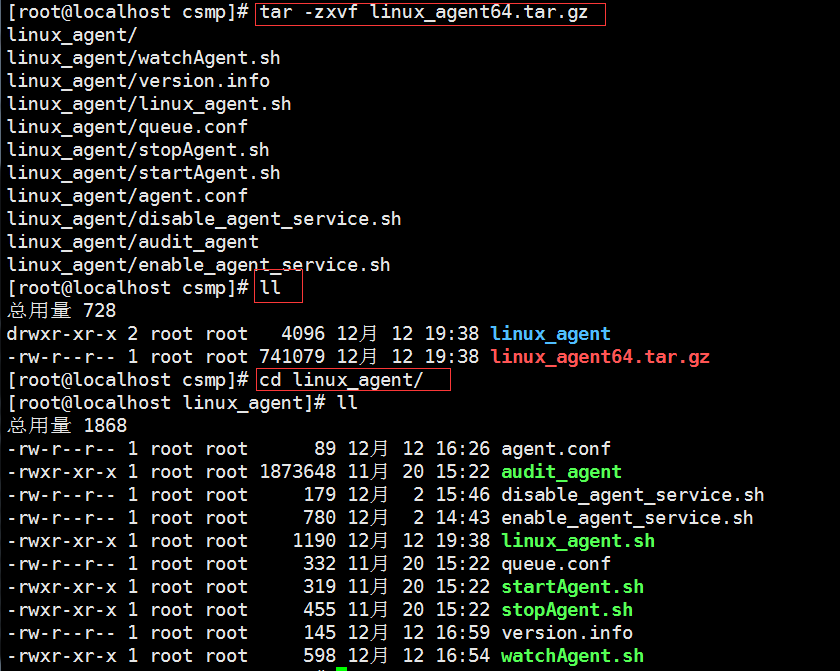


1、解压相应的Agent包

把下载的安装包上传到数据库所在的linux系统的根目录，解压

根据系统需要取相应的压缩包linux\_agent\*.tar.gz 文件，执行命令：tar -zxvf linux\_agent64.tar.gz,例如

解压后，显示如下

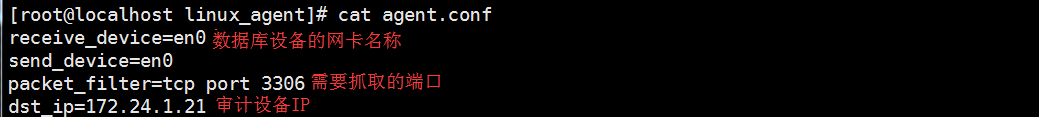


2、Agent的配置（若不配置ipv6地址则忽略此步骤）

配置agent.conf 文件，配置如下：

在Agent上进行IPV4配置：（Agent端口为9999）

vi agent.conf

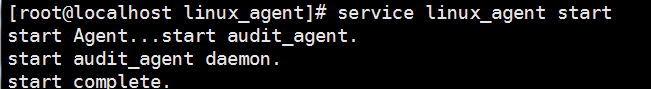


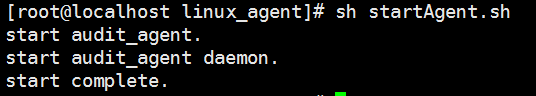
3、操作Agent

按需填好配置文件后，就可以启动Agent

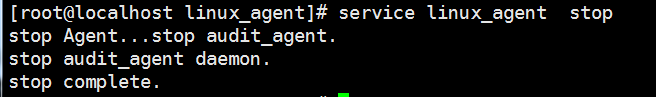
启动和停止Agent程序

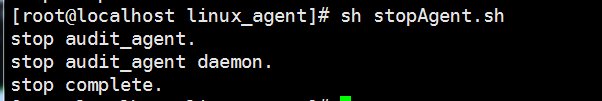
启动命令：sh startAgent.sh



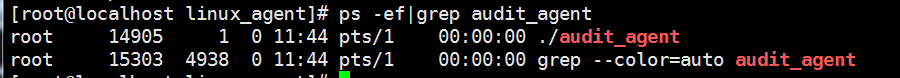


停止命令：sh stopAgent.sh

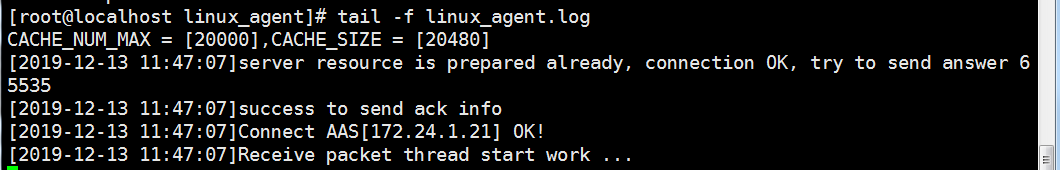




用ps -ef|grep audit\_agent 查看Agent程序是否正在运行，显示如下，说明已经在运行

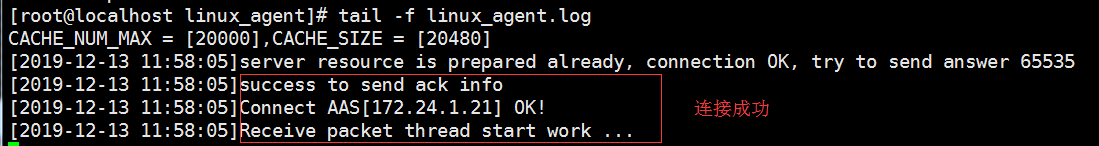


执行命令：tail -f linux\_agent.log查看Agent连接数据库审计设备是否正常，正常连接显示：



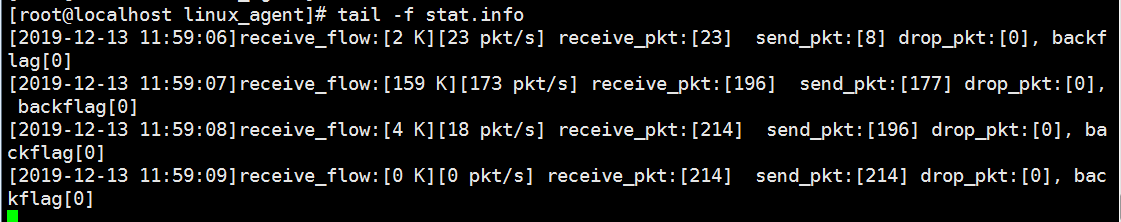
6、查看连接日志

tail -f linux\_agent.log



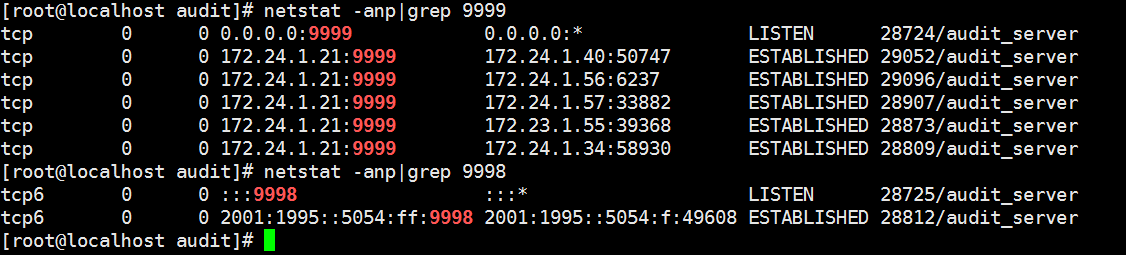
7、查看流量统计情况

tail -f stat.info



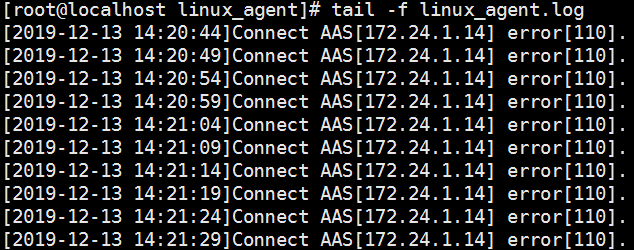
1. 在审计设备上可以查看Agent的连接情况

netstat -anp|grep 9999



9、常见报错

常见报错一：



①检查是否有证书、后台启动是否成功。在审计设备上运行netstat -anp|grep 9999命令，检查监听服务是否启动

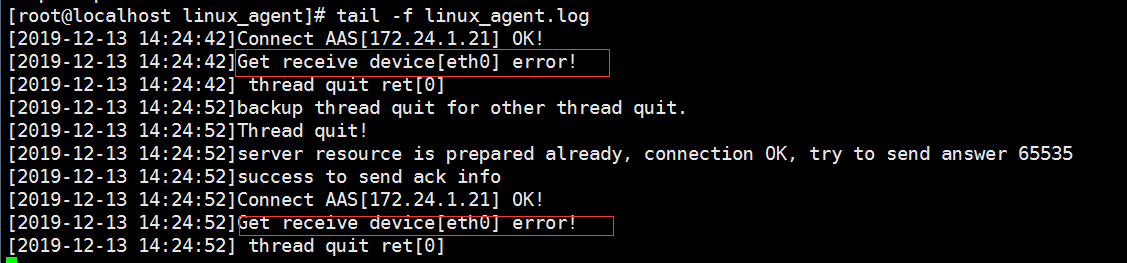


有上图监听，则代表后台启动成功。

如果没有监听那就很有可能是后台没有起来，去/home/audit/目录下执行sh audit.sh，启动后台。再次查看监听，监听还未起来就去寻找开发排查。

②相关防火墙没有开发9999或者9998端口（内网环境可忽略）

常见报错二：



agent.conf配置文件里的网卡不对。需要换成当前设备网卡。

10、其它说明

支持多个Agent 与一台数据库审计系统对接；

目前不支持一个Agent与多个数据库审计系统对接；

修改配置文件后，是需要重启Agent服务才能生效的，否则就还是按照之前配置运行