1. 实验项目名称：

barnyard2的安装配置

1. 实验原理：

1)barnyard起到一个中间人的作用，将snort和数据库进行有效的连接。snort获取到数据包由barnyard进行读取并转存到数据库。

1. 实验目的：

对barnyard2的安装配置进行学习

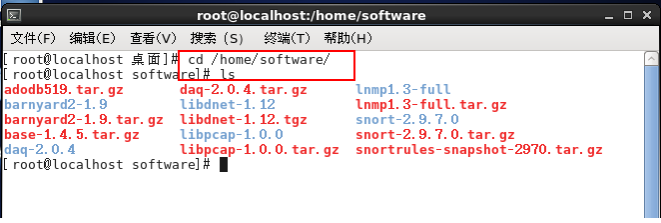
1. 实验器材（设备、虚拟机名称）：

CentOS6.5：192.168.1.2

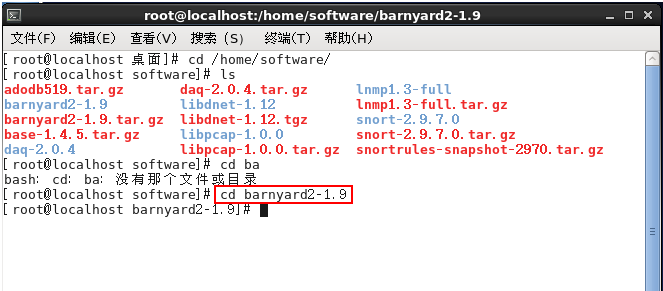
1. 实验步骤：

1. **barnyard2的安装**

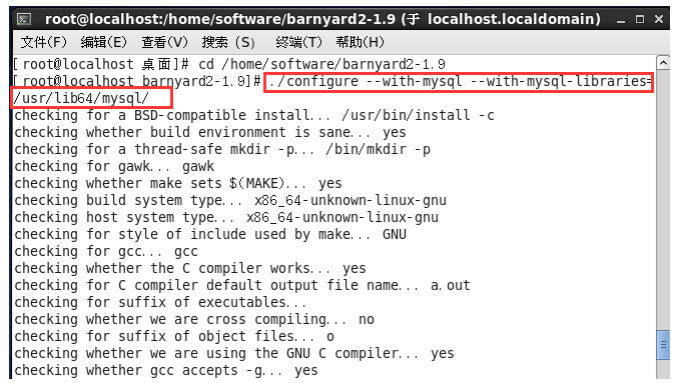
1.1    打开终端。使用命令“cd /home/software”进入目录，并查看目录下的文件。



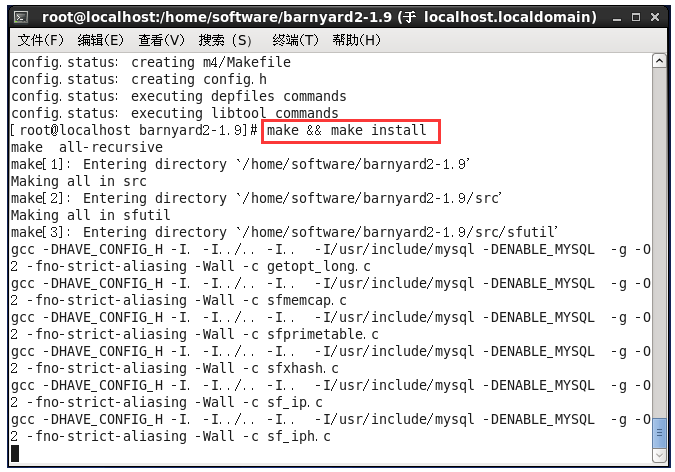
1.2    解压barnyard2-1.9,解压命令为“tar zxvf barnyard2-1.9.tar.gz”，进入barnyard2-1.9文件夹目录下（在上个实验已经解压过，跳过）。



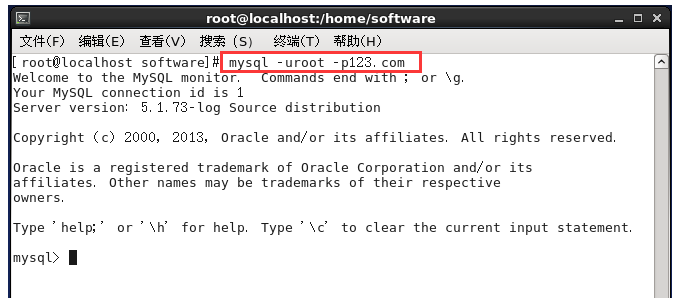
1.3    终端进入barnyard2-1.9的目录下，执行命令“./configure --with-mysql --with-mysql-libraries=/usr/lib64/mysql”进行配置。



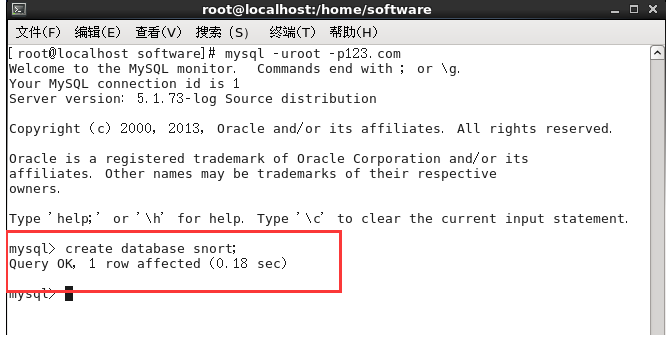
1.4    执行命令“make && make install”进行安装。



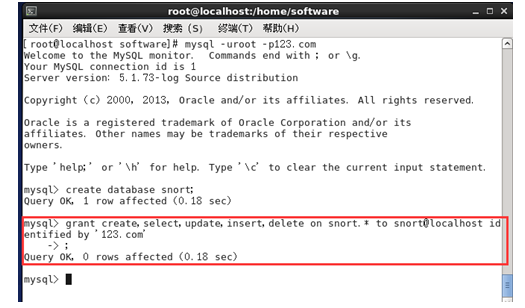
**二、配置barnyard2**

1 启动mysql，命令为“mysql –uroot –p123.com”，用户名为“root”，密码为“123.com”（在上个实验已经解压过，跳过）。

2.2 创建名为“snort”的数据库（在上个实验已经解压过，跳过）。



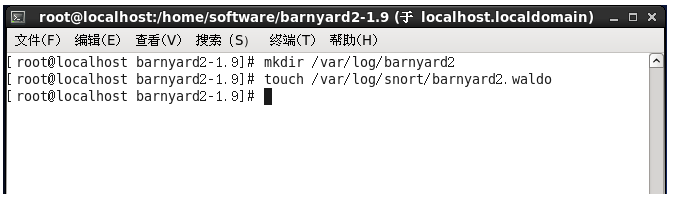
2.3  给数据库用户赋予snort数据库的权限（在上个实验已经解压过，跳过）。



2.4  退出数据库，返回终端状态输入命令“mysql –usnort –p123.com –D snort < /home/software/barnyard2-1.9/schemas/create\_mysql”将barnyard2-1.9文件中的数据导入（在上个实验已经解压过，跳过）。



2.5    创建barnyard2的文件夹，创建文件“touch /var/log/snort/barnyard2.waldo”。



2.6    将barnyard2的配置文件，复制到/etc/snort目录下。



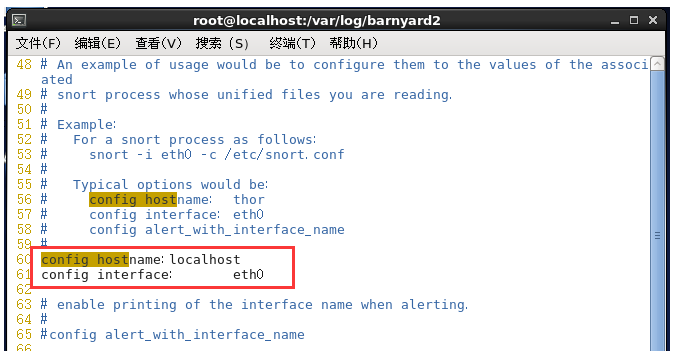
2.7    使用“vim”命令修改配置文件。



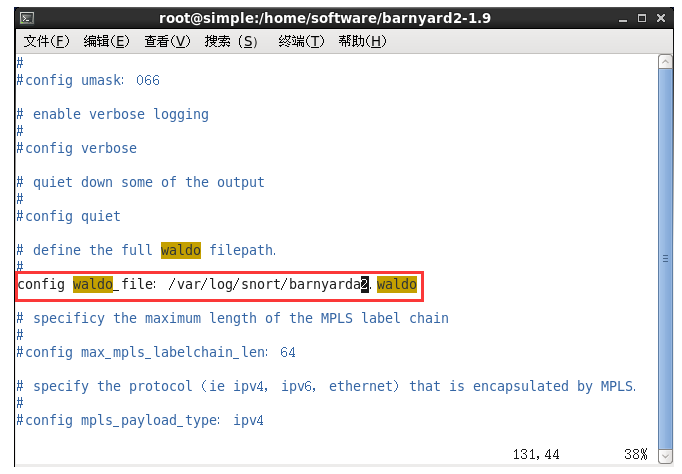
2.8    修改配置文件中的config logdir属性。



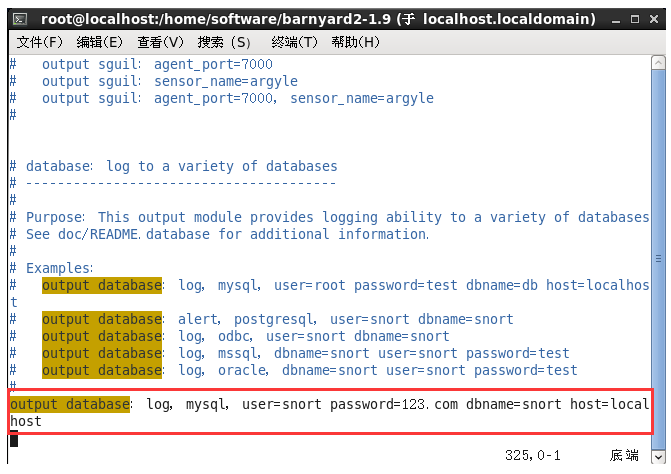
2.9    修改config hostname。



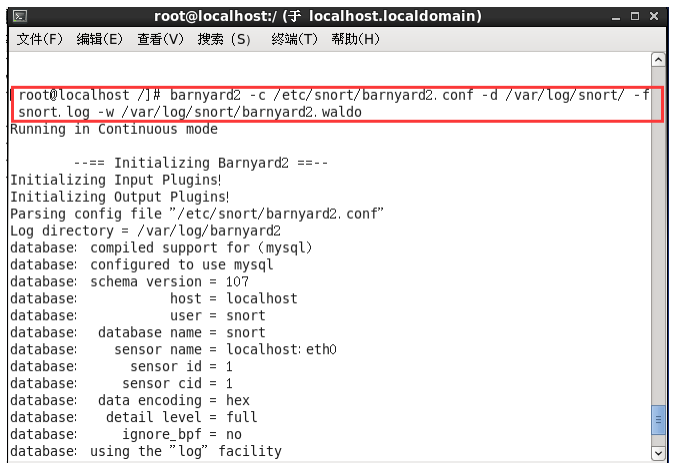
2.10 修改config waldo\_file。



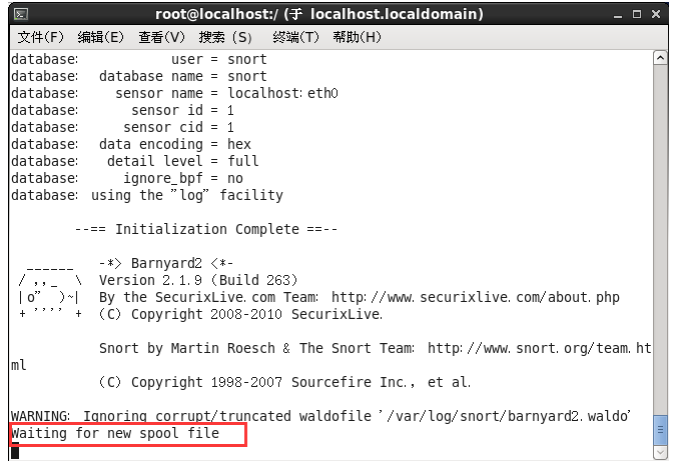
2.11    配置数据库输出选项，仿照examples编写，在文档最底部。



2.12    完成配置保存后，返回终端。输入如下命令，进行barnyard2的测试。



2.13    得到waiting for new spool file表示，barnyard2配置成功。



1. 实验结果及分析：
2. 总结及心得体会：