Linux 服务器系统日志审计实验

一【实验目标】

- 了解 syslog 系统，熟悉 syslogd 的配置文件及其语法；
- 掌握系统日志的查看方法和日志滚动的实现方法。

二【实验环境】

- Ubuntu 操作系统

三【实验原理】

日志的主要用途是系统审计，监测追踪和分析统计。为了保证 Linux 系统正常运行，准确解决遇到的各种各样的系统问题，认真地读取日志文件是管理员的一项非常重要的任务。

Linux 内核有很多子系统组成，包括网络、文件访问、内存管理等，子系统需要给用户传送一些消息，这些消息内容包括消息的来源及其重要性等，所有的子系统都要把消息送到一个可以维护的公用消息区，于是就有了 syslog。

syslog 是一个综合的日志记录系统，它的主要功能是：方便日志管理和分类存放日志。syslog 使程序设计者从繁重的、机械的编写日志文件代码的工作中解脱出来，使管理员更好地控制日志的记录过程，在 syslog 出现之前，每个程序都使用自己的日志记录策略，管理员对保存什么信息或是信息存放在哪里没有控制权。

syslog 能设置成根据输出信息的程序或重要程度将信息排序到不同的文件。例如，由于核心信息更重要且需要有规律的阅读，以确定问题出在哪里，所以要把核心信息与其它信息分开来，单独定向到一个分离的文件中。管理员可以通过编辑/etc/rsyslog.conf 来配置他们的行为。

syslog 日志文件通常存放在/var/log 目录下，该目录下除了包括 syslog 记录的日志之外，同时还包含所有应用程序的日志。为了查看日志文件的内容必须要有 root 权限，日志文件中的信息很重要，只能让超级用户有访问这些文件的权限。

syslog 绝大多数日志文件是纯文本文件，每一行就是一个消息，只要是在 Linux 下能够处理纯文本的工具都能用来查看日志文件，可以使用 cat、tac、more、less 和 grep 进行查看。也有一些日志文件是二进制文件，需要使用相应的命令进行读取。

syslog 所有的日志文件都会随着时间的推移和访问次数的增加而迅速增长，因此必须对日志文件进行定期清理，以免造成磁盘空间的不必要的浪费，同时也加快了管理员查看日志所用的时间，因为打开小文件的速度比打开大文件的速度要快，因此使用日志滚动。

Linux 下有一个专门的日志滚动处理程序 logrotate，能够自动完成日志的压缩、备份、删除和日志邮寄等工作，每个日志文件都可被设置成每日、每周或每月处理，也能在文件太大时立即处理。一般把 logrotate 加入到系统每天执行的计划任务中，这样就无需管理员自己去处理。Logrotate 默认的主配置文件是/etc/logrotate.conf，管理员可以在 logrotate 的配置文件中设置日志的滚动周期，日志的备份数目，以及如何备份日志等等。

四【实验步骤】

1、打开操作机，登录的用户名密码以实际的为准，本实验中用户名为“anma”登录密码为“123456”，密码输入过程中不显示，输完请直接按“回车”键，如图 1 所示。

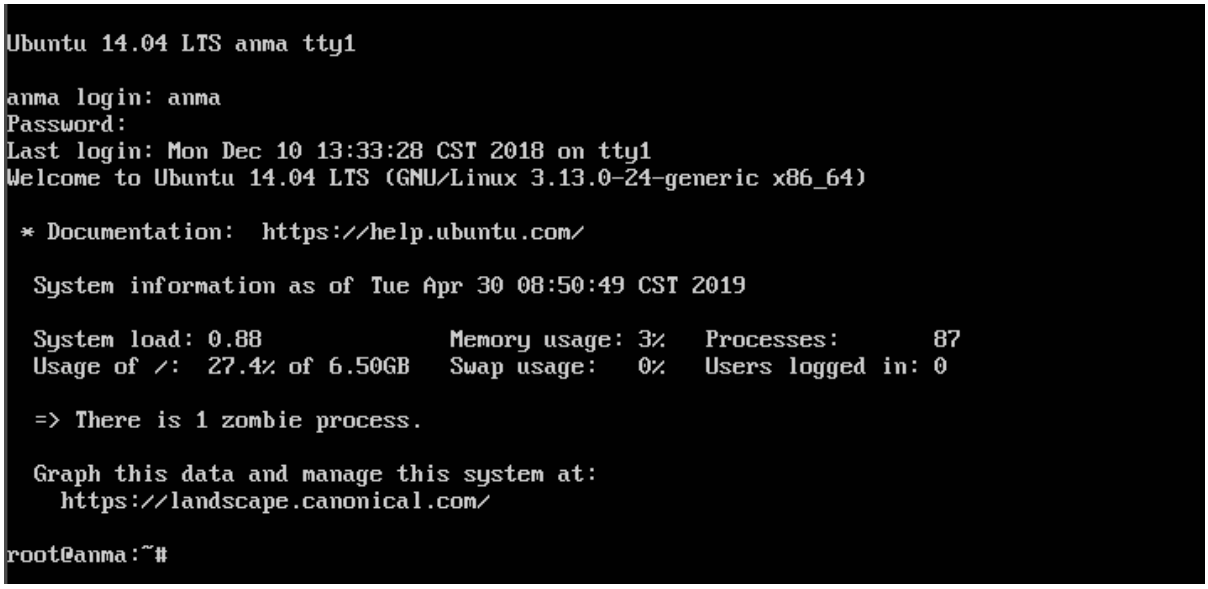

图 1

2、输入命令 cat /etc/rsyslog.conf，打开 syslog 的配置文件，查看此文件的内容。该配置文件规定了系统中需要监视的事件和相应的日志的保存位置。如图 2 所示。

```
#$InputTCPServerRun 514


#############################
#### GLOBAL DIRECTIVES ####
#############################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
```

图 2

3、输入命令 ls /var/log，查看系统中使用的日志文件。如图 3 所示。

```
root@anma:~# ls /var/log
alternatives.log       bootstrap.log  dpkg.log       lastlog        mysql.log.7.gz
alternatives.log.1     btmp           dpkg.log.1     mysql          sangfor
alternatives.log.2.gz  btmp.1         dpkg.log.2.gz  mysql.err      sangfor_vm_proxyd.log
apache2                dist-upgrade   faillog        mysql.log      sangfor_watchdog.log
apt                    dmesg          fsck           mysql.log.1.gz sfping.log
auth.log               dmesg.0        installer      mysql.log.2.gz syslog
auth.log.1             dmesg.1.gz     kern.log       mysql.log.3.gz syslog.1
auth.log.2.gz          dmesg.2.gz     kern.log.1     mysql.log.4.gz syslog.2.gz
auth.log.3.gz          dmesg.3.gz     kern.log.2.gz  mysql.log.5.gz syslog.3.gz
boot.log               dmesg.4.gz     landscape      mysql.log.6.gz syslog.4.gz
```

图 3

4、输入命令 cat /var/log/syslog，查看日志文件的格式。如图 4 所示。

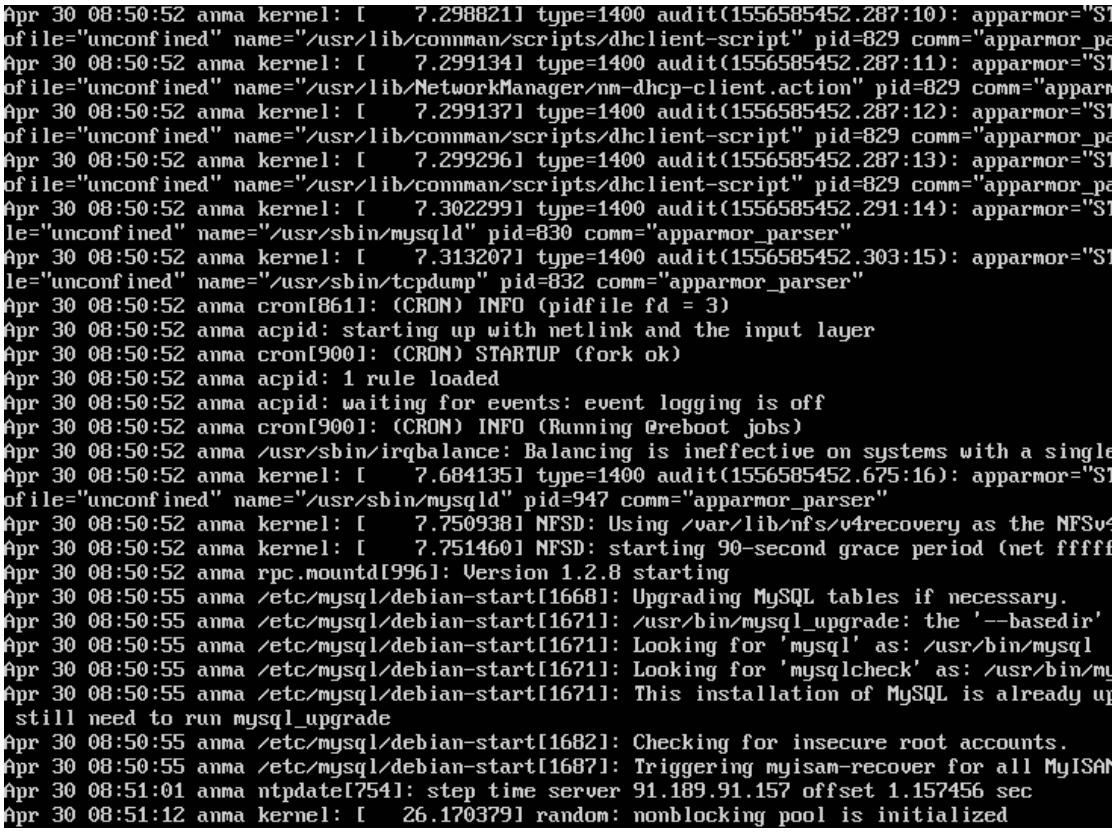

图 4

5、输入命令 lastlog，检查某特定用户上次登录的时间，并格式化输出上次登录日志/var/log/lastlog 的内容。如图 5 所示。

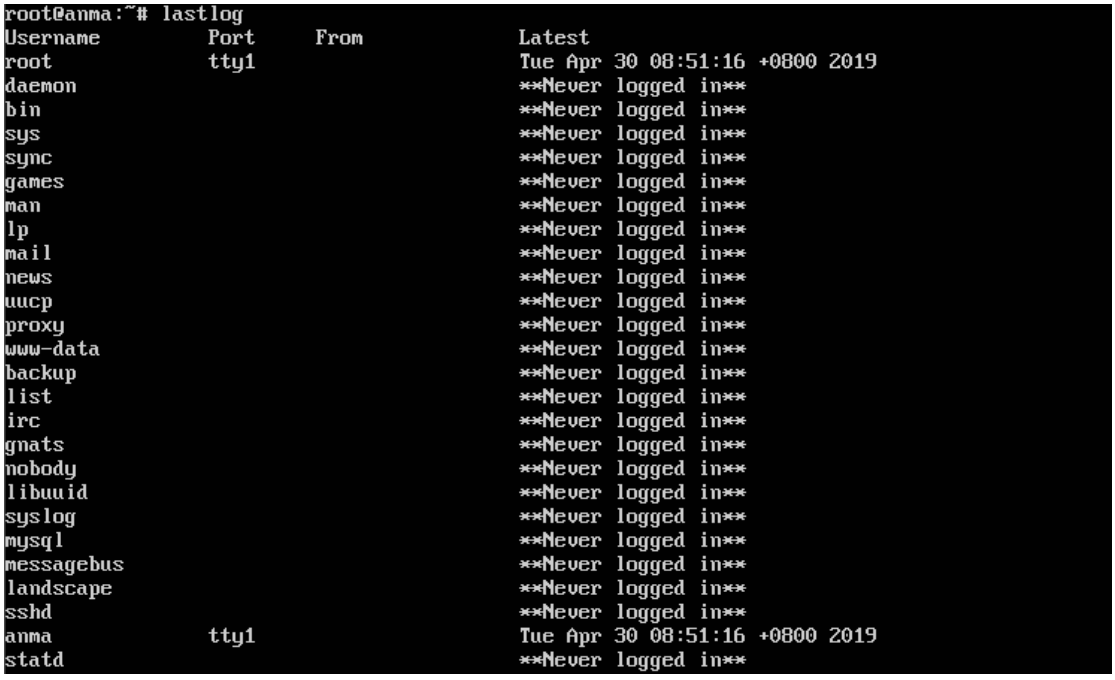

图 5

6、输入命令 last，往回搜索/var/log/wtmp 来显示自从文件第一次创建以来登录

过的用户。如图 6 所示。

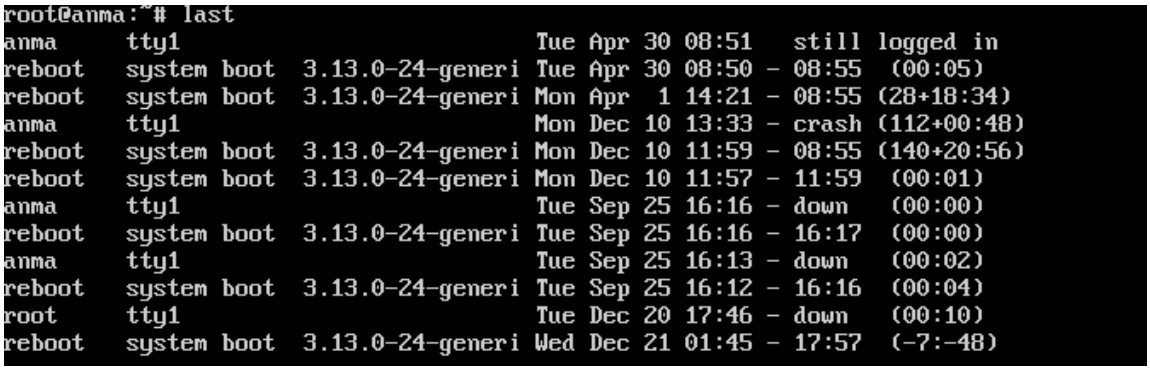

图 6

7、输入命令 lastb，搜索/var/log/btmp 来显示登录未成功的信息。如图 7 所示。

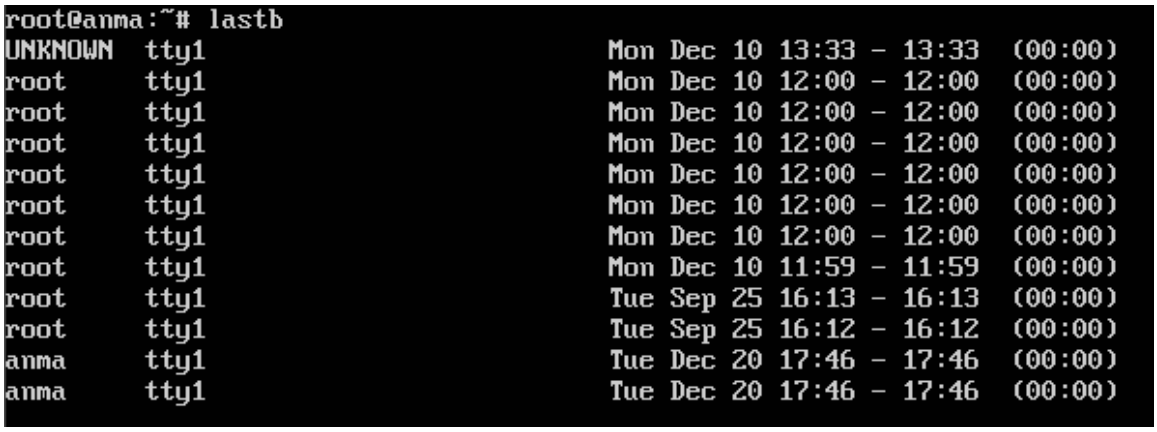

图 7

8、输入命令 who，查询 wtmp 文件并报告当前登录的每个用户。who 命令的缺省输出包括用户名、终端类型、登录日期及远程主机。如图 8 所示。

图 8

9、输入命令 logrotate -d /etc/logrotate.conf，详细显示指令执行过程。如图 9 所示。

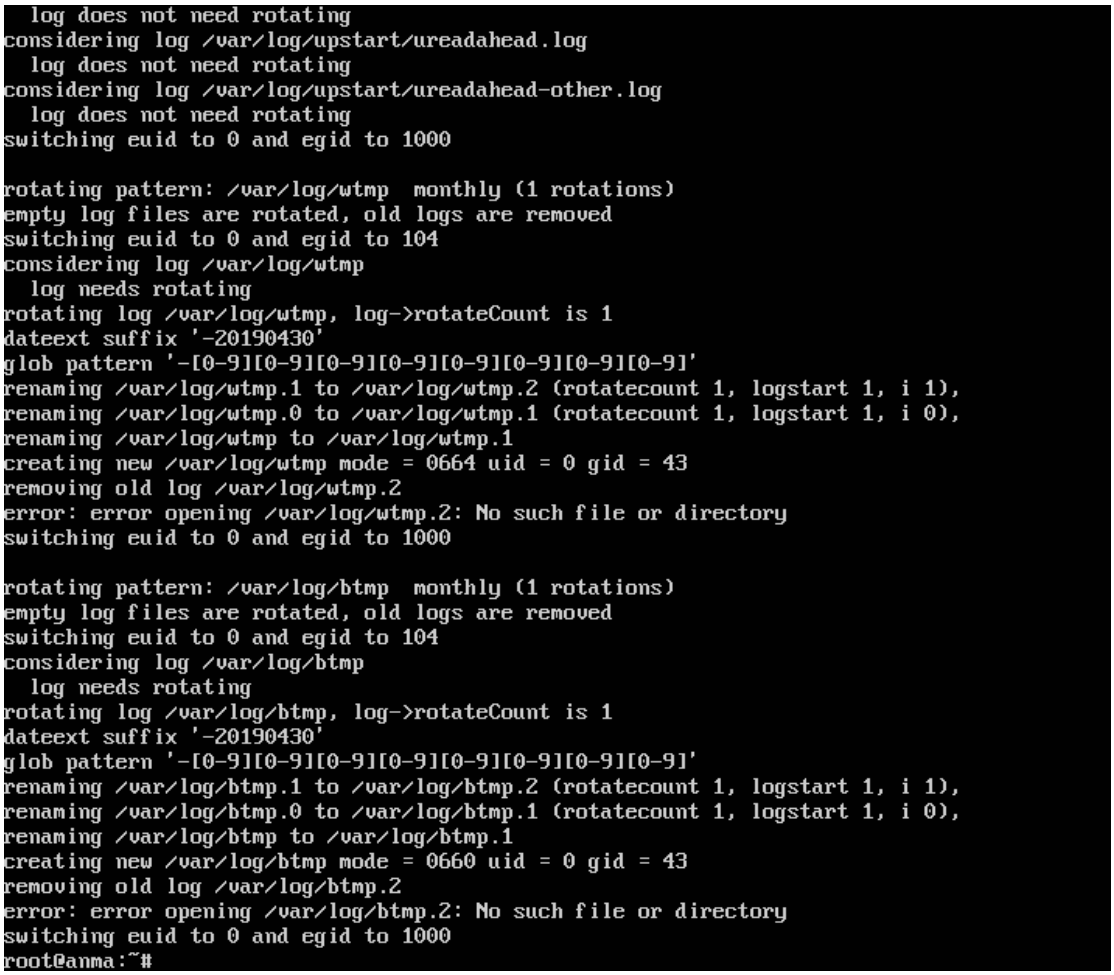

图 9

五【实验思考】

- 日志滚动是否还有另外的实现方法？