0x00 审计命令

在linux中有5个用于审计的命令：

- last：这个命令可用于查看我们系统的成功登录、关机、重启等情况；这个命令就是将/var/log/wtmp文件格式化输出。
- lastb：这个命令用于查看登录失败的情况；这个命令就是将/var/log/btmp文件格式化输出。
- lastlog：这个命令用于查看用户上一次的登录情况；这个命令就是将/var/log/lastlog文件格式化输出。
- who：这个命令用户查看当前登录系统的情况；这个命令就是将/var/log/utmp文件格式化输出。
- w：与who命令一致。

关于它们的使用：man last，last与lastb命令使用方法类似：

```
last [-R] [-num] [ -n num ] [-adFiowx] [ -f file ] [ -t YYYYMMDDHHMMSS ] [name...]
[tty...]
lastb [-R] [-num] [ -n num ] [ -f file ] [-adFiowx] [name...]  [tty...]
who [OPTION]... [ FILE | ARG1 ARG2 ]
```

参数说明：

1. 查看系统登录情况

   last：不带任何参数，显示系统的登录以及重启情况

```
[root@localhost ~]# last
root     pts/0        192.168.10.1     Mon Dec  7 04:59   still logged in
reboot   system boot  3.10.0-123.el7.x Mon Dec  7 04:58 - 05:04  (00:06)
root     pts/0        192.168.10.1     Sun Dec  6 05:31 - down   (09:48)
reboot   system boot  3.10.0-123.el7.x Sun Dec  6 05:30 - 15:20  (09:49)
root     pts/0        192.168.10.1     Thu Dec  3 05:02 - 08:54  (03:52)
reboot   system boot  3.10.0-123.el7.x Thu Dec  3 05:00 - 08:54  (03:54)
reboot   system boot  3.10.0-123.el7.x Wed Dec  2 04:40 - 08:54 (1+04:14)
root     tty1                          Tue Dec  1 09:02 - down   (00:00)
reboot   system boot  3.10.0-123.el7.x Tue Dec  1 05:04 - 09:02  (03:58)
root     tty1                          Thu Oct  8 07:19 - down   (00:00)
reboot   system boot  3.10.0-123.el7.x Thu Oct  8 07:19 - 07:19  (00:00)

wtmp begins Thu Oct  8 07:19:08 2015
[root@localhost ~]#
```

2. 只针对关机/重启

   使用 -x 参数可以针对不同的情况进行查看

```
[root@BloodZero ~]# last -x reboot
reboot   system boot  2.6.32-431.el6.x Sun Mar 29 19:52 - 19:58  (00:05)
reboot   system boot  2.6.32-431.el6.x Sat Mar 28 20:08 - 20:27  (00:19)
reboot   system boot  2.6.32-431.el6.x Fri Mar 27 21:38 - 20:27  (22:48)
reboot   system boot  2.6.32-431.el6.x Tue Mar 24 21:58 - 20:27 (3+22:28)
reboot   system boot  2.6.32-431.el6.x Wed Mar 25 05:55 - 21:57  (-7:-57)

wtmp begins Wed Mar 25 05:55:10 2015
[root@BloodZero ~]# last -x shutdown
shutdown system down  2.6.32-431.el6.x Sat Mar 28 20:27 - 19:52  (23:25)
shutdown system down  2.6.32-431.el6.x Tue Mar 24 21:58 - 21:58  (00:00)
```

3. 只针对登录

   使用 `-d` 参数，并且参数后不用跟任何选项

```
[root@localhost ~]# last -d
root     pts/0        192.168.10.1     Mon Dec  7 04:59   still logged in
reboot   system boot  0.0.0.0          Mon Dec  7 04:58 - 05:08  (00:10)
root     pts/0        192.168.10.1     Sun Dec  6 05:31 - down   (09:48)
reboot   system boot  0.0.0.0          Sun Dec  6 05:30 - 15:20  (09:49)
root     pts/0        192.168.10.1     Thu Dec  3 05:02 - 08:54  (03:52)
reboot   system boot  0.0.0.0          Thu Dec  3 05:00 - 08:54  (03:54)
reboot   system boot  0.0.0.0          Wed Dec  2 04:40 - 08:54 (1+04:14)
root     tty1         0.0.0.0          Tue Dec  1 09:02 - down   (00:00)
reboot   system boot  0.0.0.0          Tue Dec  1 05:04 - 09:02  (03:58)
root     tty1         0.0.0.0          Thu Oct  8 07:19 - down   (00:00)
reboot   system boot  0.0.0.0          Thu Oct  8 07:19 - 07:19  (00:00)

wtmp begins Thu Oct  8 07:19:08 2015
[root@localhost ~]#
```

4. 显示错误的登录信息

   lastb

5. 查看当前登录情况

   who、w

0x01 日志查看

在Linux系统中，有三类主要的日志子系统:

- 连接时间日志: 由多个程序执行，把记录写入到/var/log/wtmp和/var/run/utmp，login等程序会更新wtmp和utmp文件，使系统管理员能够跟踪谁在何时登录到系统。（utmp、wtmp日志文件是多数Linux日志子系统的关键，它保存了用户登录进入和退出的记录。有关当前登录用户的信息记录在文件utmp中; 登录进入和退出记录在文件wtmp中; 数据交换、关机以及重启的机器信息也都记录在wtmp文件中。所有的记录都包含时间戳。）
- 进程统计: 由系统内核执行，当一个进程终止时，为每个进程往进程统计文件（pacct或acct）中写一个记

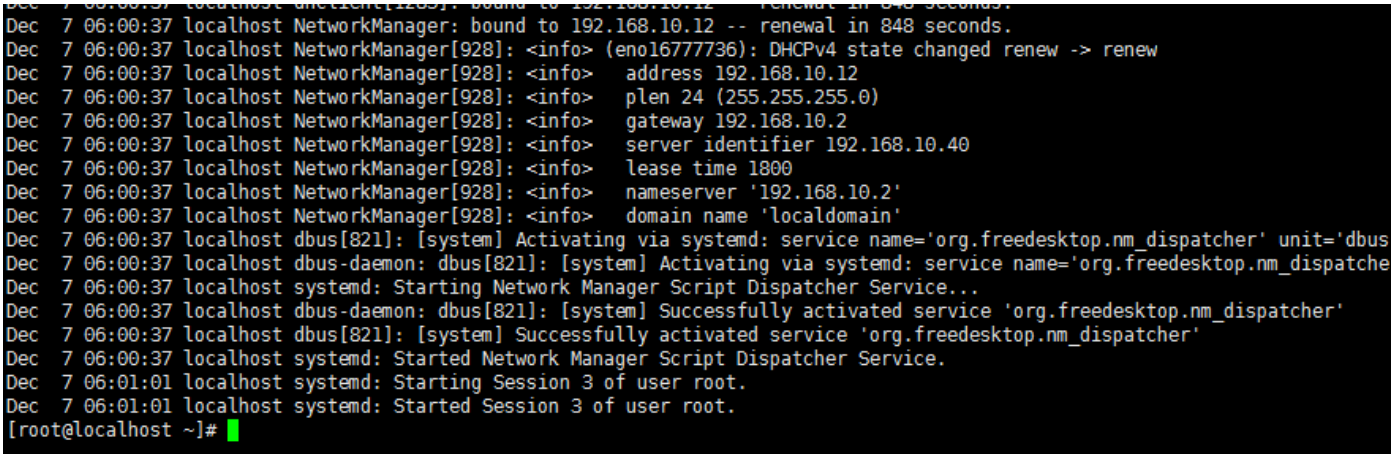
录。进程统计的目的是为系统中的基本服务提供命令使用统计。

- 错误日志: 由syslogd（8）守护程序执行，各种系统守护进程、用户程序和内核通过syslogd（3）守护程序向文件/var/log/messages报告值得注意的事件。另外有许多Unix程序创建日志。像HTTP和FTP这样提供网络服务的服务器也保持详细的日志。

日志目录： `/var/log` (默认目录)

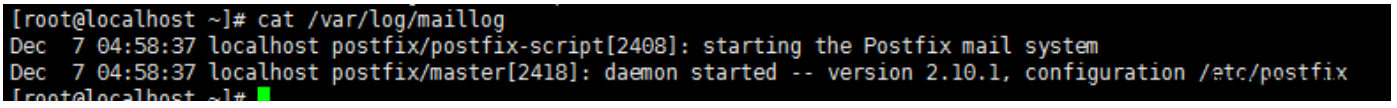
1. 查看进程日志

   ```
   cat /var/log/messages
   ```



2. 查看服务日志

   ```
   cat /var/log/maillog
   ```



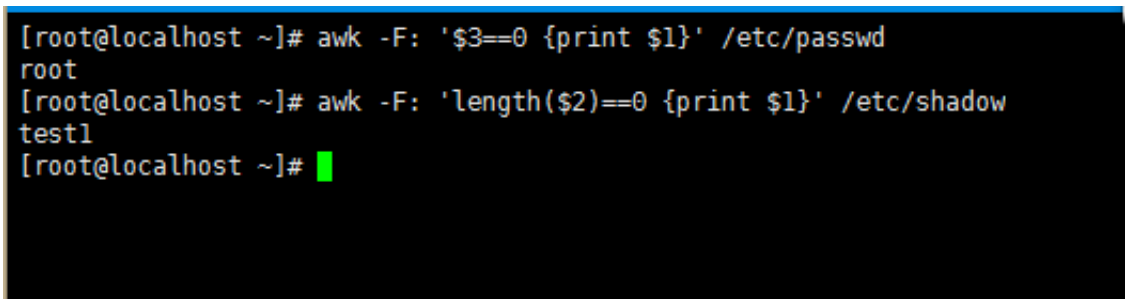
0x02 用户查看

Linux不同的用户，有不同的操作权限，但是所有用户都会在/etc/passwd /etc/shadow /etc/group /etc/group- 文件中记录；

1. 查看详细

   - less /etc/passwd：查看是否有新增用户
   - grep :0 /etc/passwd：查看是否有特权用户（root权限用户）
   - ls -l /etc/passwd：查看passwd最后修改时间
   - awk -F: '$3==0 {print $1}' /etc/passwd：查看是否存在特权用户
   - awk -F: 'length($2)==0 {print $1}' /etc/shadow：查看是否存在空口令用户

   注：linux设置空口令：passwd -d username



0x03 进程查看

1. 普通进程查看

   进程中我们一般使用ps来查看进程；man ps

   - ps -aux：查看进程
   - lsof -p pid：查看进程所打开的端口及文件

2. 检查隐藏进程

   - ps -ef | awk '{print }' | sort -n | uniq >1
   - ls /proc | sort -n |uniq >2
   - diff 1 2

   注：以上3个步骤为检查隐藏进程

0x04 其他检查

1. 检查文件

   - find / -uid 0 -print：查找特权用户文件
   - find / -size +10000k -print：查找大于10000k的文件
   - find / -name "..." -prin：查找用户名为...的文件
   - find / -name core -exec ls -l {} \;：查找core文件，并列出详细信息
   - md5sum -b filename：查看文件的md5值
   - rpm -qf /bin/ls：检查文件的完整性（还有其它/bin目录下的文件）

2. 检查网络

   - ip link | grep PROMISC：正常网卡不应该存在promisc，如果存在可能有sniffer
   - lsof -i

- netstat -nap：查看不正常端口
- arp -a：查看arp记录是否正常

3. 计划任务

- crontab -u root -l：查看root用户的计划任务
- cat /etc/crontab
- ls -l /etc/cron.*：查看cron文件是变化的详细
- ls /var/spool/cron/

4. 检查后门

对于linux的后门检查，网络上有一些公开的工具，但是在不使用这些工具的前提时，我们可以通过一些命令来获取一些信息。

首先就是检测计划任务，可以参考上面；
第二：查看ssh永久链接文件：vim $HOME/.ssh/authorized_keys
第三：lsmod：检查内核模块
第四：chkconfig --list/systemctl list-units --type=service：检查自启
第五：服务后门/异常端口（是否存在shell反弹或监听）
其它：
ls /etc/rc.d
ls /etc/rc3.d