26. Linux系统日志

笔记本:	优秀笔记		
创建时间:	2018/12/29 15:26	**更新时间:**	2018/12/29 15:28
作者:	306798658@qq.com		

Linux系统日志

日志记录了系统每天发生的各种各样的事情，比如监测系统状况、排查系统故障等，你可以通过他来检查错误发生的原因。日志的主要功能是审计和监测，还可以实时的监测系统状态，监测和追踪侵入者等等。

1. 系统日志及切割

系统日常日志 /var/log/message； 它是核心系统日志文件，包含了系统启动时的引导消息，以及系统运行时的其他状态消息。IO错误、网络错误和其他系统错误都会记录到这个文件中。另外其他信息，比如某个人的身份切换为root以及用户自定义安装的软件（apache）的日志也会在这里列出。

```
[root@damozhiying ~]# ls /var/log/messages
/var/log/messages
[root@damozhiying ~]# du -sh /var/log/messages1.5M /var/log/messages
```

在查看日志的时候，会发现日志自动切割了。

```
[root@damozhiying ~]# ls /var/log/messages*
/var/log/messages /var/log/messages-20180603 /var/log/messages-20180618
/var/log/messages-20180528 /var/log/messages-20180610
```

linux系统中有一个logrotate服务，会自动切割日志，防止无限制的增加。

```
[root@damozhiying ~]# cat /etc/logrotate.conf
# see "man logrotate" for details# rotate log files weekly //每周轮换一次日志文件
weekly //每周切割一次

# keep 4 weeks worth of backlogs //保持4周的积压
rotate 4 //4周一次轮换

# create new (empty) log files after rotating old ones //在轮换旧的日志文件后创建新的（空的）日志文件
create //创建新的

# use date as a suffix of the rotated file //使用日期作为轮换文件的后缀
dateext //以之为后缀名

# uncomment this if you want your log files compressed //如果你想压缩日志文件，请取消注释
#compress //是否需要压缩，压缩成 .tar.gz
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
```

```
# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
monthly
create 0664 root utmp
minsize 1M
rotate 1
}

/var/log/btmp { //切割该文件，指定权限，属主，属组
missingok
monthly
create 0600 root utmp
rotate 1
}

# system-specific logs may be also be configured here. //系统特定的日志也可以在这里配置。
```

查看 /etc/logrotate.d/syslog

```
[root@damozhiying ~]# ls /etc/logrotate.d
bootlog chrony syslog wpa_supplicant yum
[root@damozhiying ~]# cat /etc/logrotate.d/syslog
/var/log/cron
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
{
missingok
sharedscripts
postrotate
/bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
endscript
}
```

- syslog文件会为cron，maillog，messages，secure，spooler这几个日志进行切割
- messages日志是由 syslogd 服务决定的，所以 kill -HUP 就会重新加载这个日志
- 还有一个脚本，shell命令行，在把日志切割后（挪走），改名字生成新的日志
- Linux系统有一个特点，一个服务写一个文件的时候，并不是按照文件名去写的，而是根据inode来写的

2. dmesg命令和dmesg日志

- dmesg命令，会把系统硬件相关的日志列出来；

```
[root@damozhiying ~]# dmesg |head -5 //页面有限，只列出5行
[ 0.000000] Initializing cgroup subsys cpuset
[ 0.000000] Initializing cgroup subsys cpu
[ 0.000000] Initializing cgroup subsys cpuacct
[ 0.000000] Linux version 3.10.0-693.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc
version 4.8.5 20150623 (Red Hat 4.8.5-16) (GCC) ) #1 SMP Tue Aug 22 21:09:27 UTC 2017
```

```
[ 0.000000] Command line: BOOT_IMAGE=/vmlinuz-3.10.0-693.el7.x86_64 root=UUID=b43ac3f1-3afe-4a10-b3b8-a9f0f498cdc0 ro crashkernel=auto rhgb quiet LANG=zh_CN.UTF-8
```

> 这个日志是保存在内存中的，并不是一个文件； 假如你的网卡有问题了，硬盘损坏了，都会记录在这个日志中

- dmesg -c 清空当前日志； 但是一重启这个系统，又会生成这些日志

```
[root@damozhiying ~]# dmesg -c //清除当前日志[root@damozhiying ~]# dmesg |head -5 //列出日志。结果没有，说明清除干净[root@damozhiying ~]#
```

- /var/log/dmesg日志文件

```
[root@damozhiying ~]# file /var/log/dmesg
/var/log/dmesg: ASCII text //文本文件
```

> **注意：**这个日志文件和 dmesg命令 没有任何关联；它是系统启动的一个日志，记录的信息。

3. last命令

last命令，查看你正确的登录历史

```
[root@damozhiying ~]# last |head -5
root pts/0 192.168.112.1 Wed Jun 20 20:58 still logged in
root pts/1 192.168.112.1 Wed Jun 20 08:40 still logged in
root pts/0 192.168.112.1 Tue Jun 19 17:43 - 10:43 (16:59)
root pts/1 192.168.112.1 Tue Jun 19 13:35 - 19:27 (05:51)
root pts/0 192.168.112.1 Tue Jun 19 09:00 - 15:39 (06:39)
```

> - 它调用的文件/var/log/wtmp。
> - 里面记录是是谁，在哪里，来源IP，时间，登录的时长都会有记录
> - /var/log/wtmp日志是一个二进制文件，不能直接cat查看的，只能用last命令去查看

4. lastb命令

lastb命令，查看登录失败的用户

```
[root@damozhiying ~]# lastb
(unknown tty1 Fri Jun 8 18:02 - 18:02 (00:00)

btmp begins Fri Jun 8 18:02:01 2018
```

- 对应的文件时/var/log/btmp 日志
- /var/log/btmp也是二进制文件，不能直接cat的

5. 安全日志

/var/log/secure 比如登录操作系统，验证成功会在这里记录一个日志，失败也会去记录

```
[root@damozhiying ~]# cat /var/log/secure |head -5
Jun 16 11:40:47 damozhiying polkitd[564]: Registered Authentication Agent for unix-process:3607:1280281 (system bus name :1.106 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale zh_CN.UTF-8)
Jun 16 08:57:12 damozhiying polkitd[576]: Loading rules from directory /etc/polkit-1/rules.d
Jun 16 08:57:12 damozhiying polkitd[576]: Loading rules from directory /usr/share/polkit-1/rules.d
Jun 16 08:57:12 damozhiying polkitd[576]: Finished loading, compiling and executing 2 rules
Jun 16 08:57:12 damozhiying polkitd[576]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
```