NASA 2016 HW5 SA2

B03902086 李鈺昇

1 System Log

1.1

My distribution: 14.04.1-Ubuntu

1.1.1

Reference: http://www.thegeekstuff.com/2012/08/lsof-command-examples/

After `lsof /dev/log`, I found out that it's the `rsyslogd` command(process) which listens on `/dev/log`. Then `which rsyslogd` shows its path `/usr/sbin/rsyslogd`. Finally, `dpkg -S /usr/sbin/rsyslogd` lets me know it belongs to the `rsyslog` package.

1.1.2

References:

http://man7.org/linux/man-pages/man1/logger.1.html

http://man7.org/linux/man-pages/man1/ls.1.html

http://stackoverflow.com/questions/567757/how-do-i-distinguish-between-binary-and-text-files

First I `cd /var/log`, and then type `logger hello`. Then `ls -ltr` helps me find out the message was written to `syslog`, by observing the closest modification time. Next, `file syslog` tells me that it's a text file. The line is:

```
May 17 21:56:07 nasa-VirtualBox nasa: hello
```

1.1.3

No.

The message of command **a** was stored in three files: syslog, mail.log, and mail.err.

The message of command **b** was stored in auth.log.

The message of command **c** was stored in syslog.

I think the best way to distinguish messages by users between those by system services is to adopt good log tag, though it’s not perfectly reliable.

1.2
My distribution: 4.5.1-1-ARCH

1.2.1
Reference: https://wiki.archlinux.org/index.php/systemd

After typing systemctl --version, I got

```
systemd 229
```

followed by a long line of +… and -….

1.2.2
Reference: https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs

No.

```
mkdir -p /var/log/journal
```

1.2.3
Reference: https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs

```
journalctl -k -b 1
```

1.2.4
Reference: http://unix.stackexchange.com/questions/114189/where-are-my-sshd-logs

```
journalctl -u sshd
```

1.2.5

Reference: https://www.freedesktop.org/software/systemd/man/journalctl.html

```
journalctl _UID=0 _UID=81
```

1.2.6

Reference: https://www.freedesktop.org/software/systemd/man/journalctl.html

```
journalctl /usr/bin/sudo
```