Use journalctr Query the systemd Journal

- 請使用 `journalctl` 觀察 log ，按 `q` 離開

```
linux-za1i:~ # journalctl
```

- 請使用 `journalctl -f` 觀察 log ，按 `Ctrl + C` 離開

```
linux-za1i:~ # journalctl -f
```

LAB: 使用 rsyslog 把 ssh 額外拉出來寫成一個 log

- 請觀察相關目錄

```
linux-za1i:~ # ls /var/log/
```

- 修改 rsyslog 設定檔，請編輯 `/etc/rsyslog.conf`

```
linux-za1i:~ # vim /etc/rsyslog.conf
local4.*                                -/var/log/sshd.log
```

- 重新啟動 rsyslog

```
linux-za1i:~ # systemctl restart rsyslog.service
```

- 修改 sshd_config 設定檔，請編輯 `/etc/ssh/sshd_config` ，請搜尋 `SyslogFacility` and `LogLevel` ，並將其做備份後，再做修改

  修改前

```
linux-za1i:~ # vim /etc/ssh/sshd_config
#SyslogFacility AUTH
#LogLevel INFO
```

  修改後

```
linux-za1i:~ # vim /etc/ssh/sshd_config
SyslogFacility local4
LogLevel INFO
```

  請重啟 sshd 服務

```
linux-za1i:~ # systemctl restart sshd.service
```

- 請再次觀察相關目錄

```
linux-za1i:~ # ls /var/log/
```

- 手動建立 log

  Usage: logger -p facility.level "messages"

```
linux-za1i:~ # logger -p local4.info "Info Message1"
```

  logger -p, 優先權, 預設會是用 `user.notice`

- 請觀察資訊

```
linux-za1i:~ # ls /var/log/sshd.log
```

- 請觀察檔案內容

```
linux-za1i:~ # cat /var/log/sshd.log
```

LAB: logrotate

- **目的: 備份 ssh.log 的紀錄檔，要求如下:**

  1. 每天備份一次
  2. 紀檔檔要壓縮
  3. 備分上限 5 份，封存完，並建立空檔案

- 請編輯 `/etc/logrotate.d/sshd.log`

```
linux-za1i:~ # vim /etc/logrotate.d/sshd.log

/var/log/sshd.log{
  daily
  compress
  rotate 5
  create
  postrotate
    /usr/bin/systemctl reload syslog.service > /dev/null
  endscript
}
```

- 請觀察目錄

```
linux-za1i:~ # ls /var/log/
```

- 強制做 logrotate 動作

```
linux-za1i:~ # logrotate -f /etc/logrotate.d/sshd.log
```

- 請觀察目錄

```
linux-za1i:~ # ls /var/log/
```

Reference:

- Rsyslog
- 鳥哥私房菜-認識與分析登錄檔
- Linux環境下使用rsyslog管理日誌
- troubleshooting-rsyslog
- How to Configure Rsyslog with Any Log File; Agents Bad...No Agents Good...