Lab: 取得系統資訊

```
#dmesg | more                          <觀察開機資訊>
#uname -r                              <觀察 kernel 版本>
#chkconfig --list                      <觀察系統服務>
#cat /etc/*release                     <觀察系統版本資訊>
#uptime                                <觀察系統 loading>
#lscpu                                 <觀察 CPU 資訊>
#netstat -tupln                        <觀察 network port>
```

**Lab: Syslog-ng**

目的: 指定 pure-ftpd 的記錄檔存檔路徑

```
#netstat -tupln | grep :21             <觀察 port 21 有沒有服務>
#grep -i syslog /etc/pure-ftpd/pure-ftpd.conf   <觀察 Facility 為 ftp>
        SyslogFacility ftp
#rcpure-ftpd start                     <啟動 pure-ftpd 服務>
#netstat -tupln | grep :21             <觀察 port 21 有沒有服務>
#ftp 127.0.0.1                         <請嘗試以 ftp 登入, 輸入 bye -->離開>
#tail /var/log/messages                <請觀察資訊>
```

修改 syslog-ng 的設定, 新增以下設定

```
#vi /etc/syslog-ng/syslog-ng.conf

filter f_ftp { level(debug .. emerg) and facility(ftp); };  <指定 Facility 及 Priorities>

destination ftpall { file("/var/log/ftpmesg"); };           <指定 log 檔的位置>

log { source(src); filter(f_ftp); destination(ftpall); };

#rcsyslog restart                      <重新啟動 syslog 服務>
#ftp 127.0.0.1                         <請嘗試以以 ftp 登入, 輸入 bye -->離開>
#ls /var/log                           <請觀察資訊>
#cat /var/log/ftpmesg                  <請觀察資訊>
```

Q:如果針對 Ftp 的 log
只允許寫入到 /var/log/ftpmesg
不允許寫入到 /var/log/messages
請問該如何設定?

Lab: logrotate

目的: 備份 pure-ftpd 的紀錄檔

要求如下
1.每天備份一次
2.紀錄檔要壓縮
3 備份上限 5 份,封存完建立空檔案

#vi /etc/logrotate.d/ftp

```
/var/log/ftpmesg{
daily
compress
rotate 5
create
postrotate
        /etc/init.d/syslog reload
endscript
}
```

#ls /var/log <請觀察資訊>
#logrotate -f /etc/logrotate.d/ftp <強制作 logrotate 動作>
#ls /var/log <請觀察資訊>

optional Lab: Log Server

Server :
加入以下設定 允許 UDP 514 port 傳送 log

#vi /etc/syslog-ng/syslog-ng.conf

```
source  s_udp  {  udp( ip("0.0.0.0")  port(514)  );  };
destination  s_udp  { file("/var/log/from_net");  };
log  {  source(s_udp);  destination(s_udp);  };
```

#rcsyslog restart <重新啟動 syslog 服務>

Client:

修改設定檔, 將 log 傳到 log server
#vi /etc/syslog-ng/syslog-ng.conf

```
destination  logserver  {  udp("伺服器 IP" port(514)); };
log { source(src); destination(logserver); };
```

#rcsyslog restart <重新啟動 syslog 服務>

測試

Server:
#ls /var/log <請觀察資訊>

Client:
#rcsyslog restart <重新啟動 syslog 服務>

Server:
#ls /var/log <請觀察資訊>