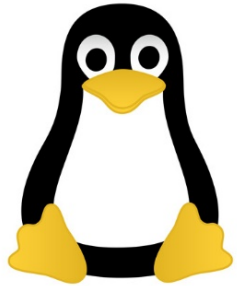
QUẢN LÝ NHẬT KÝ

TS. Trần Hải Anh

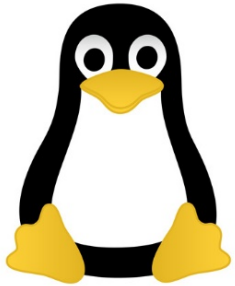
1. KHÁI NIỆM GHI NHẬT KÝ TRONG HĐH LINUX

I. Khái niệm log-nhật ký



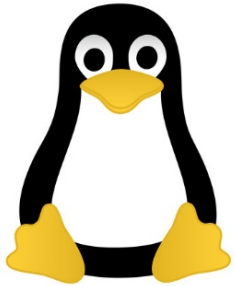
- Để có thông tin về các thao tác đã được thực hiện
- Để có thông tin về các sự kiện đã xảy ra
- Log-nhật ký là tập hợp các thông báo được hệ thống sinh ra, lưu trong các tệp nhật ký-log file.
- Các thông báo có thể là
  - Thông báo của hệ thống
  - Lỗi trong các thao tác của hệ thống
  - Quá trình đăng nhập, đăng xuất
  - Thông báo từ một số ứng dụng

Các vấn đề cần quan tâm



- Ghi nhật ký về cái gì?
- Ghi nhật ký như thế nào?
  - Facilities
- Ghi nhật ký vào đâu?
  - Destination

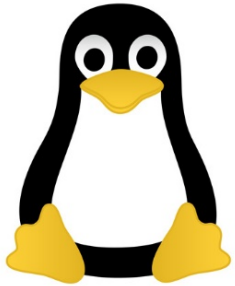
Cơ chế ghi nhật ký

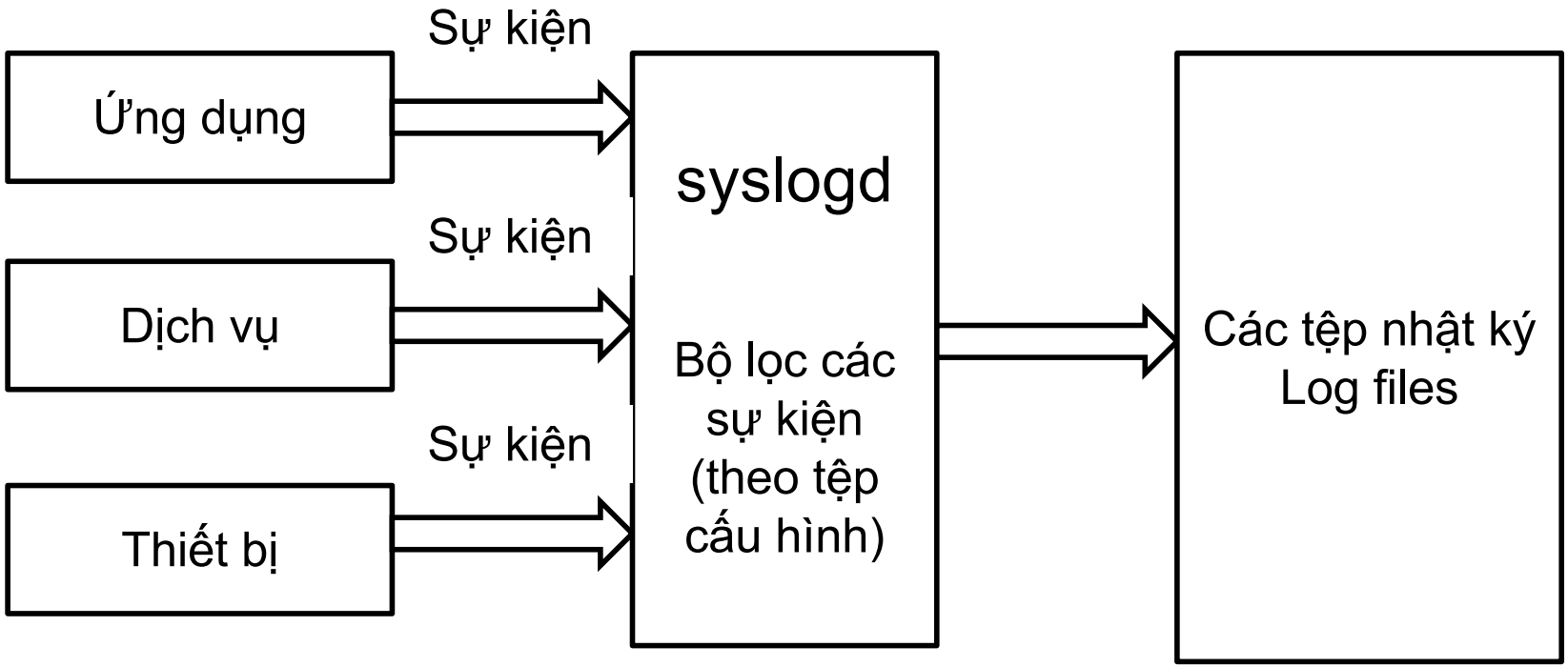


- Độc lập
  - Các ứng dụng tự ghi nhật ký vào các thư mục riêng rẽ
  - Khó theo dõi các nhật ký
  - Nhật ký nhân hệ điều hành không phải là ứng dụng
  - Các ứng dụng khó sử dụng nhật ký của nhau
  - Khó phát hiện ứng dụng “có vấn đề”
- Tập trung
  - Các ứng dụng gửi thông báo chung cho một ứng dụng chịu trách nhiệm ghi nhật ký
  - Tùy theo mức độ ứng dụng nhật ký sẽ ghi các thông tin phù hợp vào nhật ký

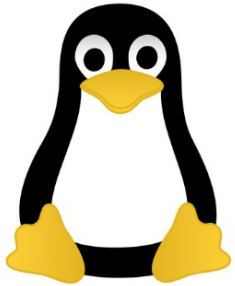
2. NHẬT KÝ TRONG LINUX

II. Cơ chế ghi nhật ký-linux





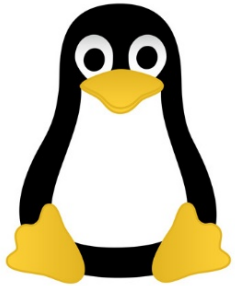
syslogd



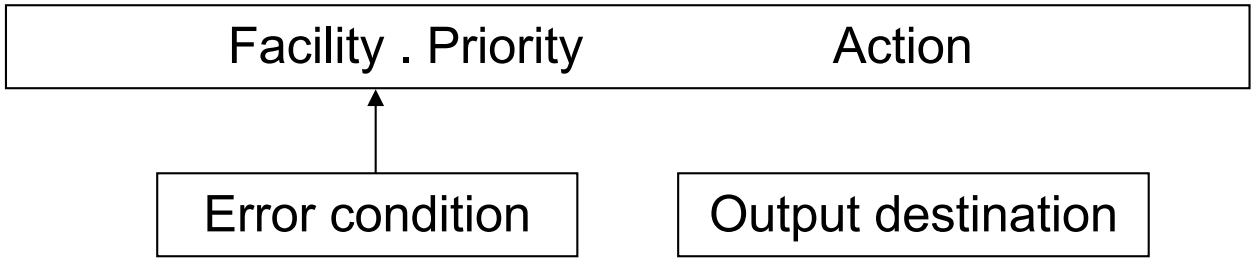
- Chương trình quản lý các thông báo từ các thành phần của hệ thống
- Được thực hiện bằng **syslogd daemon**.
- Khởi động cùng hệ thống

  /etc/init.d/syslog { start | stop | reload }
- Cấu hình của syslog được lưu trong tệp **/etc/syslog.conf**
- Lưu ý: Ubuntu sử dụng **rsyslog**, file cấu hình là: */etc/rsyslog.d/50-default.conf*

Tệp cấu hình /etc/syslog.conf

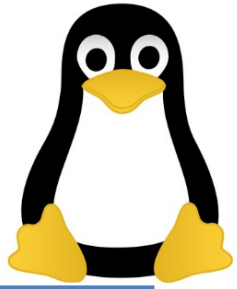


- Các dòng của tệp cấu hình có dạng



- Facility là nguồn gốc sinh ra thông báo
- "**priority**" là mức độ quan trọng của thông báo
- Action là thao tác thực hiện khi nhận được thông báo
  - Ghi vào tệp, gửi email, ….

Các loại Facility



Facility	Ý nghĩa
auth :	Thông báo về bảo mật hệ thống liên quan đến việc xác thực
authpriv :	Thông báo về bảo mật hệ thống liên quan đến quyền truy cập
cron :	Thông báo của crond
ftp :	Thông báo của dịch vụ ftp
kern :	Thông báo của nhân HĐH
lpr :	Thông báo của hệ thống in ấn lpr
mail :	Thông báo liên quan đến email
news :	Thông báo liên quan đến news service
syslog :	Thông báo của syslogd
user :	Thông báo của các ứng dụng NSD
uucp :	Copy file bằng UUCP(Unix to Unix Copy)
daemon :	Chung của các daemon
local0-7 :	NSD định nghĩa

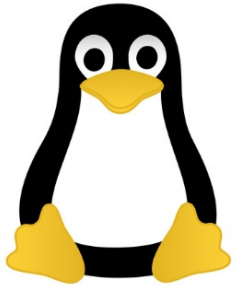
Priority

Priority	Ý nghĩa
emerg	Thông báo khẩn “cấp cứu”
alert	Báo động
crit	Lỗi phần cứng, không thể khắc phục
err	Lỗi thông thường
warning	Cảnh báo
notice	Nhắc nhở
info	Thông tin
debug	Thông tin kỹ thuật

Thao tác

Ký hiệu	Thao tác
/file_name	Ghi vào tệp *file_name*
@ hostname	Chuyển đến máy *hostname*
user_name	Gửi thông báo cho NSD *user_name*
*	Gửi thông báo cho tất cả NSD đang đăng nhập vào hệ thống

Ví dụ về /etc/syslog.conf



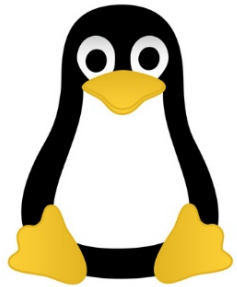
```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  /var/log/maillog

# Log cron stuff
cron.*                                                  /var/log/cron
```

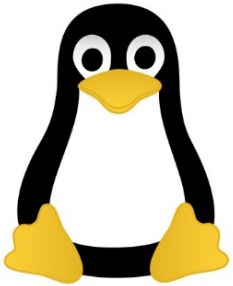
Listing of /etc/syslog.conf



```
# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg                                         *
*.emerg                                         @10.1.1.254

# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
 #
news.=crit                                      /var/log/news/news.crit
news.=err                                       /var/log/news/news.err
news.notice                                     /var/log/news/news.notice
```

Syslog – Ví dụ

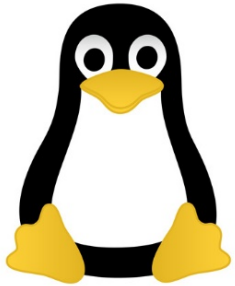


- Ghi ‘kern.info’ and ‘daemon.notice’ vào‘/var/log/log’ file.

```
kern.info;daemon.notice /var/log/log
```

```
cron,news.debug /var/log/debug
```

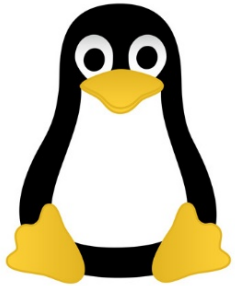
Các tệp log quan trọng



- ***Thư mục /var/log/***
  - –

Tên tệp	Ý nghĩa
cron	Thông báo từ các thao tác của crond
maillog	Thông báo liên quan đến email
messages	Các thông báo ngoài bảo mật, email, news
secure	Bảo mật
boot.log	Khởi động và tắt dịch vụ
dmesg	Thông báo của nhân hệ điều hành
lastlog	Thông báo về quá trình đăng nhập của NSD
wtmp	Thông báo về quá trình hoạt động của tất cả NSD

Công cụ khác



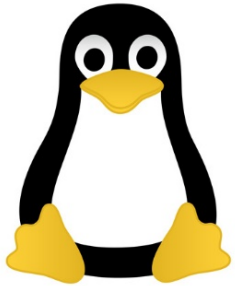
- ***logger:*** logs messages to the /var/log/messages file

```
logger  program myscipt ERR
```

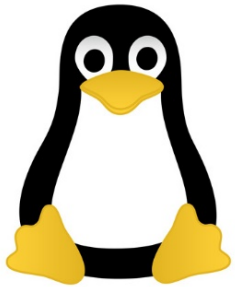
- ***Logrotate:*** Cập nhật và nén các tệp log
- Cấu hình **/etc/logrotate.conf**.

3. TỐI ƯU HÓA QUÁ TRÌNH GHI NHẬT KÝ

Logrotate



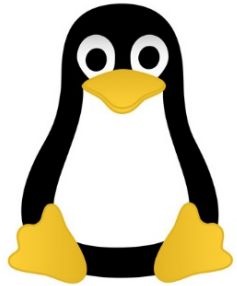
- Xoay vòng các tệp log
- Sao lưu và nén các dữ liệu log đã cũ (nhưng vẫn có thể cần đến)
- Có thể được kích hoạt theo thời gian hoặc theo kích thước
- Cấu hình /etc/logrotate.d/



- /etc/logrotate.d/apache2.conf

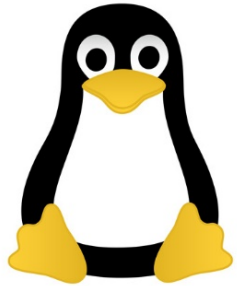
```
/var/log/apache2/*
weekly
rotate 3
size 10M
compress
delaycompress
```

Các tùy biến của logrotate



- weekly : Các tệp nhật ký được thực hiện nếu ngày trong tuần hiện tại nhỏ hơn ngày trong tuần khi thực hiện kiểm tra tệp nhật ký hoặc đã kiểm tra được hơn 01 tuần.
- rotate 52 : Tệp nhật ký được xử lý 52 lần trước khi bị xóa đi hoặc gửi theo email.
- compress : Các tệp lưu trữ cũ của nhật ký được nén (để tiết kiệm không gian đĩa).
- missingok : Nếu tệp nhật ký không có, tiếp tục xử lý các tệp nhật ký tiếp theo. Không thông báo lỗi.
- notifempty : Không xử lý nếu nhật ký rỗng.
- sharedscripts : Các tệp nhật ký cùng thực hiện một kịch bản sẽ chỉ thực hiện kịch bản một lần. Nếu không có nhật ký nào được xử lý, kịch bản dùng chung này sẽ không thực hiện.
- postrotate câu lệnh endscript : Câu lệnh thực hiện sau khi xử lý xong tệp nhật ký.

Bài tập



- Đăng nhập vào hệ thống bằng tài khoản người quản trị, xem nội dung tệp /var/log/messages. Câu lệnh nào cho biết các sự kiện mới nhất xảy ra trong hệ thống.
- Theo dõi tệp nói trên sử dụng lệnh tail
- Căn cứ vào tệp cấu hình của logrotate, giải thích tệp /var/log/messages được xử lý thế nào.