Manage log and journal

Content

I. What are logs and journaling?

II. Logging in Linux

III. Optimising log writing

I. Log

- For keeping track of (timeline of events)
  - User activities
  - Application information
  - System performance
  - Operations
  - Events
- Linux log is a set of notifications generated by systems, saving in logging files.
- Notification can be
  - Notification of OS
  - Errors or faulty in operations
  - Log in/out
  - Notification from applications

Questions need to be answered

- What to log?
- How to log?
  - Facilities
- Where to log?
  - Destination

Log mechanism

- Independent
  - Each application writes log files to separate directories
  - Hard to keep track log files
  - System logging is not an application
  - Applications are hard to use others’ logs
  - Hard to detect “problems” of applications
- Centralised
  - Each application sends notifications to a single log application
  - Suitable information is written accordingly

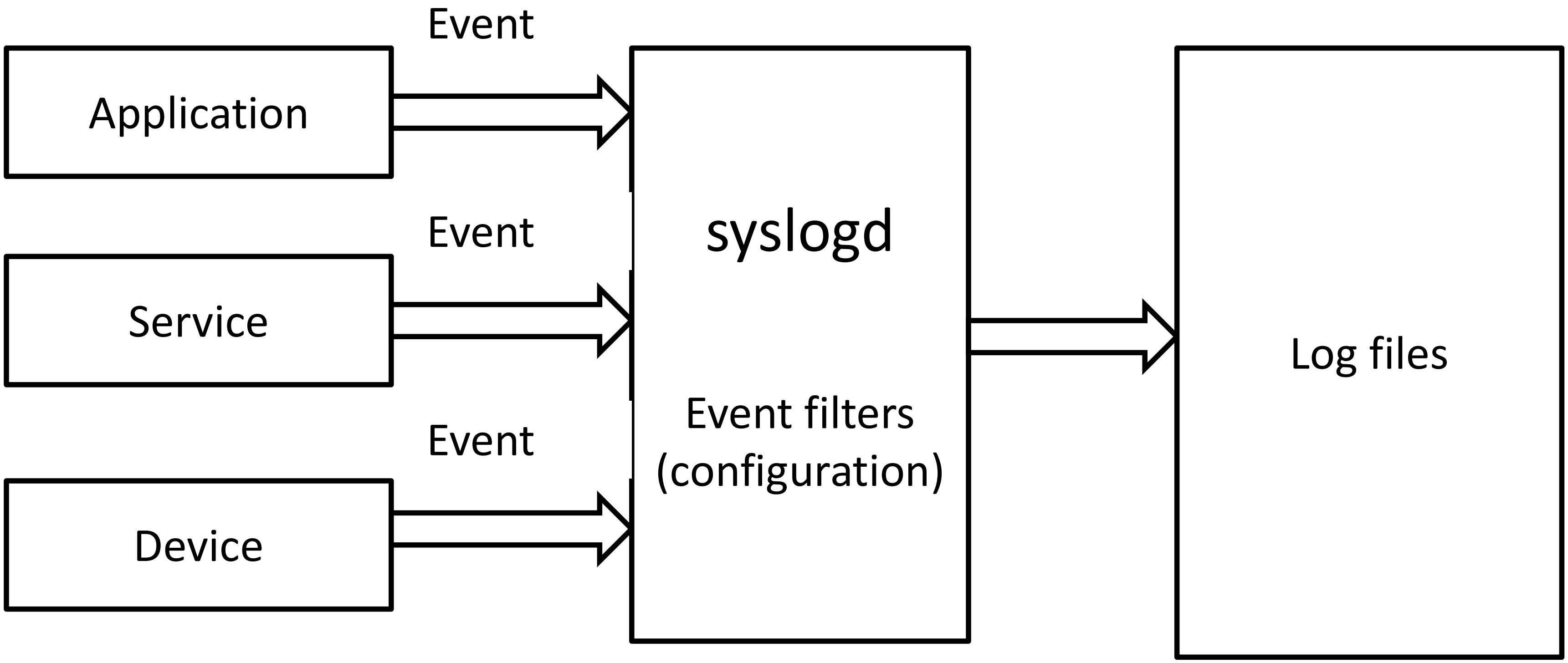
Content

I. What are logs and journaling?

II. Logging in Linux

III. Optimising log writing

II. Logging in Linux

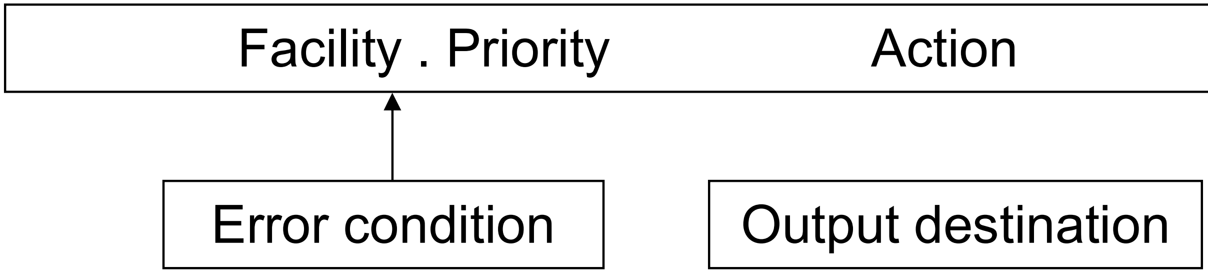


syslog

- The syslogd daemon logs all system messages
  - **syslogd daemon service**.
- It reads and forwards system messages to the appropriate log files and/or users
- Start with system booting
  - The configuration file **/etc/syslog.conf**

/etc/syslog.conf

- Each line has the format



Facility . Priority Action

Error condition

Output destination

- Facility is the source of notification
- “**priority**” is the important level of the notification
- Action is the operation executed when receiving the notification
  - Write to files, send email, ….

Facility types

Facility	Meaning
auth :	Notification about authentication
authpriv :	Notification about access permission
cron :	Crond notification
ftp :	ftp notification
kern :	Kernel notification
lpr :	Lpr notification (printing service)
mail :	Email notification
news :	news service notification
syslog :	Syslogd notification
user :	User application notification
uucp :	(Unix to Unix Copy) – remote execution of commands and transfer files
daemon :	Daemon uucp
local0-7 :	User defined

Priority

Priority	Meaning
emerg	Emergency
alert	Alert
crit	Critical hardware errors, cannot recover
err	Normal error
warning	Warning only
notice	Notification
info	Information
debug	Debugging information

Operation

Characters	Operation
/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

Listing of /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
```

Current logging system

- syslog was replaced by rsyslog
- rsyslog is an upgraded version of syslog, supporting client/ server mechanism.
- rsyslog works as a system service
  - systemctl start/ enable/ status rsyslog
- Configuration file /etc/rsyslog.conf
- Beside traditional mechanism, it supports modules
  - module(load="imfile" PollingInterval="10")
  - input(type="imfile"

    File="/var/log/apache2/access.log"

    Tag="apache-access"

    Severity="info")

Important log files

- ***Directory /var/log/***
  -

File	Meaning
cron	Crond notification
maillog	Email notification
messages	Notification except security, email, and news
secure	Security notification
boot.log	Start and shut down service
dmesg	Kernel notification
lastlog	Notification about the last login of users
wtmp	Notification about the user operations

Content

I. What are logs and journaling?

II. Logging in Linux

III. Optimising log writing

Other tools

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

```
logger  program myscipt ERR
```

- ***Logrotate:*** update, rotate, and compress log files
- Configuration file **/etc/logrotate.conf**.

Logrotate

- Rotate log files
- Backup and compress old log files (but might be needed in the future)
- Can be activated by time or size
- Configuration file /etc/logrotate.d/

Configure logrotae

```
# see "man logrotate" for details # rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own wtmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}
# system-specific logs may be also be configured here.
```

Configure for a service

```
[root@localhost root]# cat /etc/logrotate.d/httpd
/var/log/httpd/*log {
    missingok
    notifempty
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/httpd.pid 2>/dev/null` 2> /dev/null || true
    endscript
}
```

Options for logrotate

- weekly .
- rotate 52.
- compress
- missingok
- notifempty
- sharedscripts
- postrotate <command> endscript