!"#$%&’"()*%+,(-./0’1(!"1*%*/02$34%(

-+6:’&0(;<()499*%9

5$674(!6$"(8*"$794(

!"#$%&$’"(&)*+"*,(-"(."%/$*,(0)%’123$*4*56"3&%7(.3$*

58&"*&"’$*8"*#9:6.3$*:$;)*<.3"(3.$=*

>%"$2?"*>)’’)(8*@ABC>BDE*FGH

Index

- **Introduction.**
- **Event gathering system (syslog).**
- **How to maintain log information.**
- **How to use log information.**

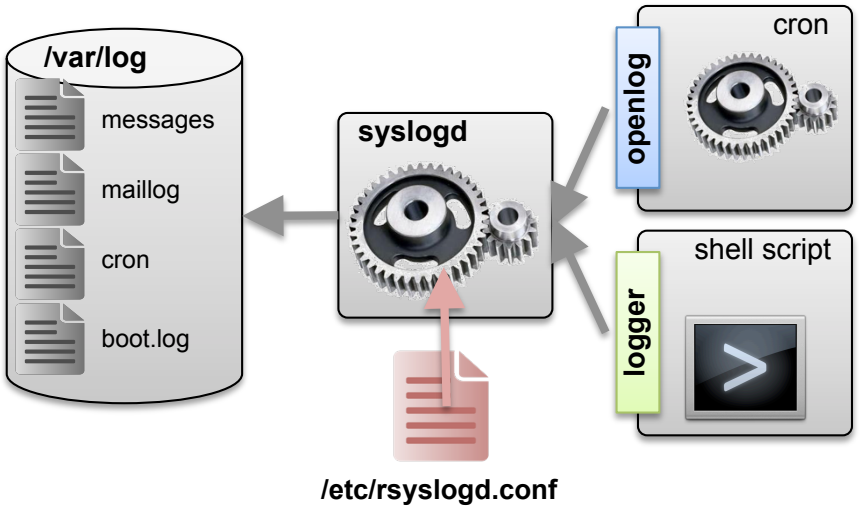
Introduction

- Kernel, services, apps generate/send **events** constantly:
  - Information about **normal activity**.
  - Information about **failures** and other anomalies.
  - **Failed booting** of system and services.
  - **Access** information (security).
- Correct management of this information is essential to discover and solve problems.
- The events from all services have a common manager:
  - Event collector employed by kernel, services and apps.
  - In UNIX, a service named **"syslog"** (rsyslog, syslog-ng).
  - Flexible, easy, safe and powerful.

Index

- Introduction.
- **Event gathering system (syslog).**
- How to maintain log information.
- How to use log information.

Syslog



- Syslog structure:
  - **syslogd:** logging service. The rest of services and apps communicate with syslogrd to send messages to log files.
  - **openlog:** libraries to use this service from another service/app:
    - Perl: use sys::syslog (openlog(), syslog().
    - C: openlog lib.
  - **logger:** command to send messages to the log file from a shell.
  - **rsyslogd.conf:** configuration of actions to be performed according to the messages sent by the services.<

Syslog

```
# Log all kernel messages to the console.
kern.*      /dev/console

# Log anything (except mail) of level info or higher .
# dont log private authentication messages!
*.info;mail.none;authpriv.none      /val/log/messages

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

- rsyslogd.conf:
  - One line per action, with the format: facility.level action.
  - Facility: short list of defined (by the kernel) values:
    - Kern, user, daemon (other service), auth (login, su, ssh…), syslog, mail, lpr, cron…
  - Notification levels:
    - emerg, alert, crit, err, warning, notice, info, debug, * (all levels).
  - Actions:
    - file: write the message to the specified file (/var/log/messages, /dev/console).
    - @hostname/@IP: send the message to the syslogd of the specified host (centralization).
    - user1, user2: send the message to users user1 and user2 if logged on.
    - *: send the message to every user logged on.

Syslog

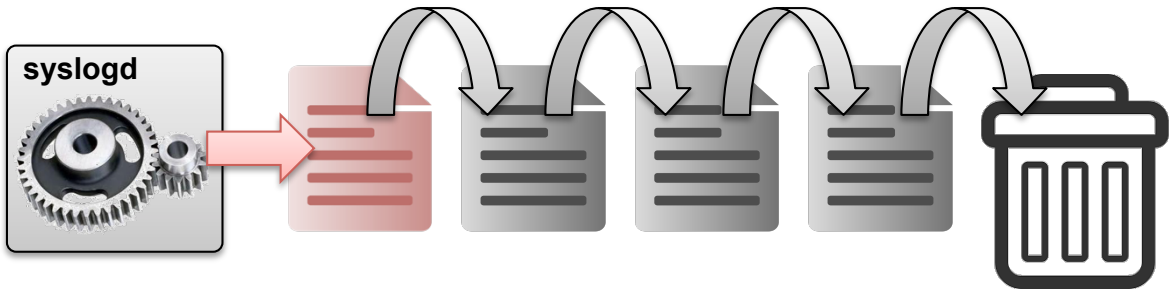
- Special Files that **do not** make use of syslog:
  - /var/log/wtmp: contains, in binary format, user loggings and system reboots:
    - Employed by last and uptime.
  - /var/log/lastlog: contains the last login of each user.
  - /var/log/dmesg: booting process events, written by kernel and init.

Index

- Introduction.
- Event gathering system (syslog).
- **How to maintain log information.**
- How to use log information.

Maintaining Log information

- Log file: basic tool for control and repair.
- The more logged information-> The more disk consumed:
  - Can exhaust disk quota.
  - Hard to find information in a file with millions of lines.
- Log rotation:
  - Mechanism consisting of periodically writing to a new log file, creating a new empty one and deleting the oldest ones.
  - Manual Rotation: Example script performing it.




```
#!/bin/sh
cd /var/log/
mv messages.2 messages.3
mv messages.1 messages.2
mv messages messages.1
cat /dev/null > messages
chmod 600 messages
#Reiniciar syslog
service restart rsyslog
```

Maintaining Log information

- Automatic Rotation: **logrotate:**
  - Unsupervised organization of log rotation. Avoids disk overflow and organizes log files according to their creation dates.
  - Configuration through the file: /etc/logrotate.conf:
    - Applied by default to every service.
  - Particularization for a service: /etc/logrotate.d/:
    - Overwrites the options in logrotate.conf.

```
/var/log/dpkg.log {
    monthly
    rotate 12
    compress
    notifempty
    create 0664 root adm
}
```

```
# rotate log files weekly, monthly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# send errors to root
errors root
# create new(empty)log files after rotating old ones
create
# compressed log files
compress
# DEB packages drop log rotation info into this dir
include /etc/logrotate.d
#no packages own lastlog or wtmp, rotate them here
/var/log/wtmp cd /var/log/{
            monthly
            create 0664 root utmp
            rotate 1
}
```

Index

- Introduction.
- Event gathering system (syslog).
- How to maintain log information.
- **How to use log information.**

Using Log information

- How to use the information of a log:
  - Debugging: increase available information when something goes wrong:
    - E.g. activate “verbose” mode for services (example, in /etc/init.d/ssh **sshd –d**).
    - Deactivate when moving back to production!!
  - Monitoring:
    - Problem: huge amount of information (not everything is useful).
    - Start being generous, reduce/remove unnecessary information gradually.
    - Make use of specialized tools to look for relevant messages:
      - Swatch: ftp://ftp.stanford.edu/general/security-tools/swatch/.
      - LogWatch: highly recommended, available in debian repository.

Using log info

- logwatch --print

```
[ root si ~ ] vi /etc/cron.daily/00logwatch
#!/bin/bash
#Check if removed-but-not-purged
test -x /usr/share/logwatch/scripts/logwatch.pl
|| exit 0
#execute
/usr/sbin/logwatch --mailto root
```

```
#################### Logwatch 7.3.1 (09/15/06) ####################
        Processing Initiated: Tue Dec  2 15:56:56 2008
        Date Range Processed: yesterday ( 2008-Dec-01 )Period is day.
        Detail Level of Output: 5
        Type of Output: unformatted
        Logfiles for Host: debian
 ##################################################################

 --------------- courier mail services Begin------------------
Courier restarted itself              4 Times
Courier was started by hand (or init) 2 Times
Courier was stopped by hand (or init) 2 Times

Failed delivery attempts: 6 Times

  because  550 User unknown. - 6 Times
     From  - 2 Times
        To root@debian.localdomain - 2 Times
     From #@[] - 2 Times
        To postmaster@debian.localdomain - 2 Times
     From root@debian.localdomain - 2 Times
        To root@debian.localdomain - 2 Times

---------------------- httpd Begin ------------------------
172.09 MB transferred in 220781 responses  (1xx 0, 2xx 3444, 3xx 96, 4xx
       217227, 5xx 14)
     1316 Images (26.44 MB),
     6985 Documents (55.30 MB),
        6 Archives (0.83 MB),
        2 Sound files (0.00 MB),
    27286 Windows executable files (7.90 MB),
   102944 Content pages (38.00 MB),
------------------- Disk Space Begin ----------------------
Filesystem         Size  Used Avail Use% Mounted on
/dev/xvda2         9.9G  1.8G  7.6G  19% /
/dev/xvda3         504M   30M  450M   7% /boot
/dev/xvda4         2.0G  182M  1.9G   9% /files
/dev/xvda5          20G  4.0G   15G  21% /var/www
/dev/xvda6         2.0G  695M  1.2G  37% /var/cache/openafs
/dev/xvdb1         917G  390G  481G  45% /data
AFS               8.6G    0  8.6G   0% /afs
---------------------- Disk Space End ------------------------

###################### Logwatch End #########################
```