System Logging

rsyslogd

DE HOGESCHOOL
MET HET NETWERK

Hogeschool PXL – Dep. PXL-IT – Elfde-Liniestraat 26 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

Rsyslog-daemon

- rsyslogd
- Rocket-Fast System for Log processing
- Versie kan je bekijken via
  - rsyslogd -v
    - Geeft 7.4.4

Rsyslog-daemon

- rsyslogd configuratie
  - /etc/rsyslog.conf
    - hierin staat dat default-logging-rules staan in /etc/rsyslog.d/50-default.conf
  - /etc/rsyslog.d/50-default.conf
    - hier zie je wat gelogd moet worden en naar welke log-file

Rsyslog-daemon

- Opmaak van een rsyslogd-configuratiebestand
  - facility.priority /path_to_logfile
  - facility
    - geeft het systeem aan dat het log-bericht heeft aangemaakt (=de origine)
      - bvb “kern” voor de messages afkomstig van de kernel
    - kan zijn: auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp en local0-local7
    - alle logs van dit systeem met de aangegeven priority

Rsyslog-daemon

- facility.priority /path_to_logfile
- priority
  - geeft de ernst van het log-bericht aan
  - kan zijn: debug, info, notice, warning, err, crit, alert en emerg
  - vanaf de aangegeven priority en hogere zullen voor het aangegeven systeem(=facility) gelogd worden
- path_to_logfile
  - geeft aan naar welk bestand deze logs gestuurd worden

Rsyslog-daemon

- Voorbeelden voor rsyslogd-configuratiebestand
  - facility.priority /path_to_logfile
    - *.info;mail.none;news.none /var/log/syslog
      - alle log-berichten met een prioriteit hoger dan of gelijk aan info,

        behalve logberichten van mail en news worden gelogd naar /var/log/syslog
    - authpriv.* /var/log/secure
      - alle logberichten van authpriv worden gelogd naar /var/log/secure

Rsyslog-daemon

- Voorbeelden voor rsyslogd-configuratiebestand
  - facility.priority /path_to_logfile
    - *.*;auth,authpriv.none -/var/log/syslog
    - wil zeggen alles behalve auth en authpriv loggen naar /var/log/syslog
      - “;” is scheiden van meerdere selectors
      - “,” is scheiden van meerdere facilities met dezelfde prioriteit
      - “-” voor het pad wil zeggen dat de kernel-buffer niet telkens moet geflushed worden als er een logbericht wordt weggeschreven. In de meeste distributies wordt sowieso niet geflushed en wordt het minteken dus ook niet in rekening gebracht.

Rsyslog-daemon

- Voorbeelden voor rsyslogd-configuratiebestand
  - facility.priority /path_to_logfile
    - kern.err /var/log/kern.log
      - alle log-berichten met als ernst meer of gelijk aan error
    - kern.!err /var/log/kern.log
      - alle log-berichten met als ernst minder dan “error”
    - kern.=info /var/log/kern.log
      - Alle log-berichten met als ernst het type “info”
    - kern.!=info /var/log/kern.log
      - alle log-berichten behalve die met als ernst het type “info”

Belangrijke logfiles

- /var/log/syslog
  - hiernaar wordt bijna alles gelogd door de syslog-daemon
  - het is de “General System Activity-log”
- /var/log/auth.log
  - bevat de user login en authorizations (ook sudo-cmd’s)
- /var/log/faillog
  - bevat de foutieve login-pogingen
  - gebruik het commando “faillog” om de logfile te bekijken

Belangrijke logfiles

- /var/log/boot.log
  - bevat de logs van de systeem-opstart-scripts van de vorige keren dat er geboot is
- /var/log/kern.log
  - bevat kernel-logs
- /var/log/dmesg
  - bevat een dump van de kernel-message-buffer sinds boot
  - de kernel-logs van tijdens het booten kunnen ook bekeken worden met het commando “dmesg”

Belangrijke logfiles

- /var/log/btmp
  - bevat logs van mislukte login-pogingen
  - te bekijken via: lastb of last -f /var/log/btmp | less
- /var/log/wtmp
  - bevat records van logins en logouts, reboots en shutdowns
  - gebruik het commando “last” om deze file te tonen
  - om de laatste login-tijd te zien per gebruiker kan je ook het commando “lastlog” bekijken
  - “who” gebruikt deze file ook om te kijken wie ingelogd is

Belangrijke logfiles

- /var/log/apport.log
  - logfiles van crashes van applicaties
- /var/log/dpkg.log
  - bevat de logs van het Package-management-systeem
- /var/log/secure
  - login-logs van ssh, proftp, …
- /var/log/<daemon>/….
  - bepaalde daemons plaatsen hun logs in een subdir van /var/log

Logrotatie

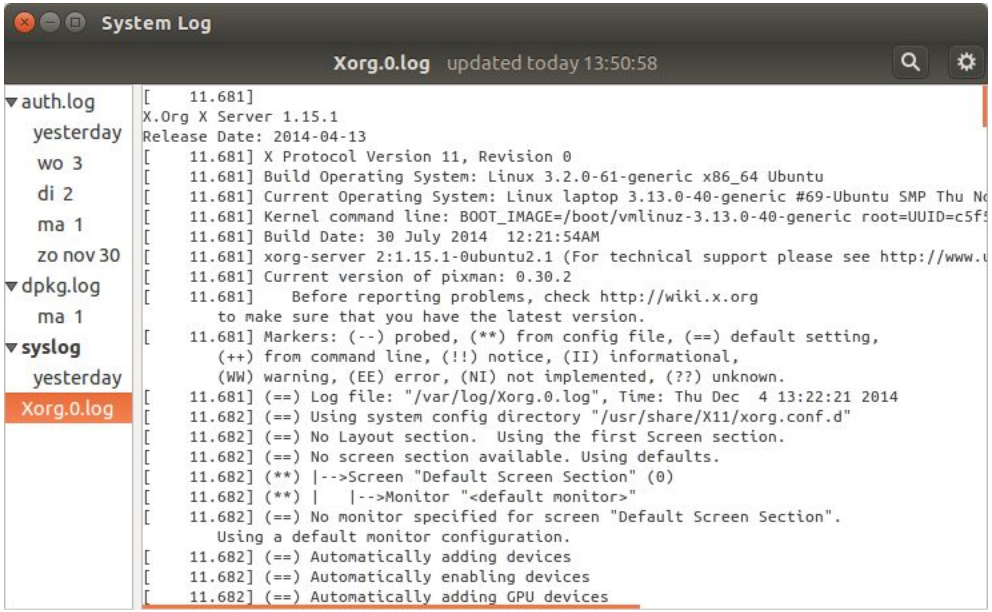
- Sommige logfiles hebben een logrotatie
  - logrotate-daemon
    - zorgt voor automatische rotatie, verwijdering en compressie van logfiles
      - bvb: syslog , syslog.1 , syslog.2.gz , … , syslog.7.gz
  - De algemene config-file is /etc/logrotate.conf
    - iedere daemon kan voor zijn log-rotatie een config-file aanmaken in /etc/logrotate.d/
      - daily, weekly of monthly of met een size van xxxMB
      - met een rotatie van n-files
      - met compressie, ...

Logfiles bekijken

- cat /var/log/syslog
- more /var/log/syslog
- less /var/log/syslog
- grep -i dhclient /var/log/syslog
- tail -f /var/log/syslog
  - -f van follow
  - toont onmiddelijk de laatste 10 regels van de logfile
  - houdt de file open en toont ook de nieuwe log-berichten als de logfile groeit

Logfiles bekijken in de GUI

- Klik op de Dash
  - Zoek naar System Log



Nieuwe logs die bijkomen worden in het vet gezet.

Met CTRL-F kan je zoeken in de log-berichten.

Via het Wieltje in de rechterbovenhoek kan je logfiles met “Open” gaan toevoegen.

Zelf iets loggen

```
logger "Gebruiker $USER ingelogd"
logger -p kern.err "Couldn't find apache module"
logger -p kern.err -t kernel "Couldn't find apache module"
```

```
Jan  6 11:35:42 ubserv student: Gebruiker student ingelogd
Jan  6 11:35:46 ubserv student: Couldn't find apache module
Jan  6 11:35:49 ubserv kernel: Couldn't find apache module
```

- Zelf iets naar syslog sturen kan met
  - het commando “logger”
    - logger “Gebruiker $USER ingelogd”
    - logger met de optie -p
      - hiermee kan men aangeven van welke facility en met welke priority er gelogd wordt. Dit wordt door de daemon gebruikt om de log-entry in de juiste logfiles te plaatsen
        - logger -p kernel.err “Couldn’t find apache module”
    - logger met de optie -t
      - hiermee kan men in de logfiles weergeven aangeven van