UPMC
PARIS UNIVERSITAS

Préparation LPI

Exam 102

108.2. Journaux syslog

108.2 – Domaines de connaissances

- Poids : 2
- Configuration de syslog
- Syslog
- Connaître les facility, priorités et actions standards

Sommaire

- syslogd
- logger
- logrotate

108.2 Gestion des journaux

- Journaux ou fichiers de log : fichiers textes
- Localisés dans le répertoire `/var/log`
- Dans certains cas, des sous-répertoires dédiés à des services ou applications
  - `/var/log/cups`
  - `/var/log/mail`
  - `/var/log/httpd`
- Localisation paramétrable dans le fichier de conf du service
- Sur un serveur, intérêt à ce que `/var` soit dans une partition distincte de `/`
- Intérêt de la rotation des fichiers de log pour limiter l'espace utilisé (cf. plus loin)

- Journaux importants :
  - `boot.log` : messages relatifs à la séquence de boot
  - `cron` : messages relatifs à l'utilitaire cron
  - `maillog` : messages relatifs au système de courrier
  - `messages` : la presque totalité des messages qui ne sont pas dirigés dans un fichier spécifique
  - `auth` ou `secure` : messages relatifs à l'authentification des utilisateurs sur le système (locale ou distante avec telnet ou ssh)
  - `dmesg` : messages envoyés par le noyau
  - `yum.log` : messages relatifs au gestionnaire de paquetage yum

- `dmesg` : également une commande permettant d'examiner le kernel ring buffer
  - Taille du buffer limitée à 16384 octets
  - `-n` *`level`* : demande à n'afficher sur la console que les messages d'un certain niveau
    `dmesg -n 1` : affiche uniquement à la console les messages de type PANIC
  - `-s` : vide le buffer
- Différence entre le fichier `/var/log/dmesg` et la commande `dmesg`
  - `/var/log/dmesg` : uniquement les messages générés par le noyau durant la séquence de boot
  - `dmesg` : affiche tous les messages du noyau au cours de la vie du système

```
[root@localhost ~]# dmesg | wc -l
584
[root@localhost ~]# cat /var/log/dmesg | wc -l
500
```

- Action : insertion d'un clef USB

```
[root@localhost ~]# dmesg | wc -l
604
[root@localhost ~]# cat /var/log/dmesg | wc -l
500
```

- Examen des journaux
- Chaque évènement (1 évènement par ligne) enregistré dans un journal contient
  - Date et heure
  - Nom machine à l'origine du message
  - Service ou utilisateur qui génère le message
  - Texte du message

Feb 1 22:09:02 localhost rsyslogd: [origin software="rsyslogd" swVersion="2.0.2" x-pid="2206" x-info="http://www.rsyslog.com"][x-configInfo udpReception="No" udpPort="514" tcpReception="No" tcpPort="0"] restart
Feb 1 22:45:50 localhost gconfd (franck-3194): Sortie
Feb 1 22:45:50 localhost shutdown[9195]: shutting down for system halt
Feb 1 22:45:50 localhost NetworkManager: <info> Deactivating device eth1.
Feb 1 22:45:50 localhost NetworkManager: <info> eth1: canceled DHCP transaction, dhclient pid 3456
Feb 1 22:45:51 localhost kernel: ipw2200: Failed to send ASSOCIATE: Already sending a command.

108.2 Gestion des journaux

- Commandes utiles pour examiner les journaux
  - `less`
  - `tail`
  - `head`
  - `more`
  - `tail -f` : affichage dynamique des nouvelles lignes qui apparaissent dans le journal.
    Pratique pour suivre l'évolution « en ligne » d'un journal
    Crtl + C pour quitter
  - `grep`
    - `-i` : pour inclure minuscules et majuscules

```
[root@localhost ~]# grep -i usb /var/log/messages | wc -l
504
[root@localhost ~]# grep usb /var/log/messages | wc -l
299
```

108.2 Gestion des journaux

- Configuration de syslogd : `/etc/syslog.conf`
- Chaque ligne contient une directive de type :
  facility.level action
- facility : représente un groupe de messages ou l'origine du message
  - auth et authpriv : authentification
  - cron : utilitaire cron
  - kern : messages du noyau
  - mail : message du système de courrier
  - user : processus utilisateurs
  - * : toutes les facility

108.2 Gestion des journaux

- facility local0 à local7 utilisable par utilisateurs
- Configuration dans le fichier de conf du service. Une directive permet de définir que la gestion des logs pour ce service sera assurée par syslogd + définition du facility (local4 par exemple)
- Le couple facility.level est souvent appelé sélecteur
- Attention : sur certains systèmes remplacement de syslogd par syslogd-ng ou rsyslogd donc fichier de conf différent

108.2 Gestion des journaux

- Commande `logger` : interface avec le service syslogd
  `logger [-isd] [-f file] [-p pri] [-t tag] [-u socket] [message ...]`
  - Permet de générer manuellement des messages vers syslogd
- Options
  - -f fichier : envoie le contenu d'un fichier à syslogd
  - -p priorité : définit une priorité particulière
  - -t tag : ajout d'un tag identifiant l'origine du message

```
<...>
# special franck pour test
local4.*                                        /var/log/lpi.log
```

```
[root@localhost ~]# logger -p local4.info "Tous reçus à l'examen LPI"
```

```
[root@localhost ~]# cat /var/log/lpi.log
Feb  8 13:34:55 localhost franck: Tous reçus à l'examen LPI
```

- priority (priorité du message ou niveau de détail) : par ordre croissant
  - emerg, panic
  - alert
  - crit
  - err, error
  - warning, warn
  - notice
  - Info
  - debug
  - * : toutes les priorités
  - none : désactive la facility

- action : en fait correspond à la destination du message
  - Cela peut être un fichier : /var/log/meslogs
  - Cela peut être également le service syslogd d'une autre machine : @192.168.1.89
    Utile pour centraliser les journaux sur une machine de référence (exigences de sécurité)
  - Cela peut être la console : /dev/console
- Le joker * remplace toute facility, level ou action (cf. Exemple)

- Plusieurs facility séparés par des « , » :
  - uucp,news.crit /var/log/spooler
  - Tous les messages de niveau supérieur ou égal à crit pour les facility uucp et news vont dans /var/log/spooler
- Exemple 2 :
  - news.=crit /var/log/news/news.err
  - Tous les messages de niveau égal à crit pour la facility news vont dans /var/log/news/news.err
- Exemple 3 :
  - mail.!err /var/log/monmail.log
  - Tous les messages de niveau inférieur à err pour la facility mail vont dans /var/log/monmail.log

- Possibilité de spécifier plusieurs sélecteurs séparés par “;” pour une même action
  - mail.!warn;cron.!warn /var/log/notice.log
  - Tous les messages de inférieurs à warn pour les facility mail et cron vont dans /var/log/notice.log

```
#kern.*                                         /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.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
# Everybody gets emergency messages
*.emerg                                         *
# Save news errors of level crit and higher in a special file.
uucp,news.crit                                  /var/log/spooler
# Save boot messages also to boot.log
local7.*                                        /var/log/boot.log
```

108.2 Gestion des journaux

- Rotation des journaux : `logrotate`
- Fichiers de configuration
  - `/etc/logrotate.conf`
  - Fichiers spécifiques dans `/etc/logrotate.d`
- Copie régulière du journal dans un autre fichier avec extension .0 puis à la prochaine .0 devient .1 etc..
- Compression
- Lancé quotidiennement par cron
- Man logrotate

```
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# create new (empty) log files after rotating old ones
create
# use date as a suffix of the rotated file
dateext
# uncomment this if you want your log files compressed
#compress
# RPM packages drop log rotation information into this directory
include /etc/logrotate.d
# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}
```

```
[root@localhost ~]# cat /etc/logrotate.d/rsyslog
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log
/var/log/cron {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/rsyslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

```
[root@localhost ~]# cat /etc/cron.daily/logrotate
#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf
EXITVALUE=$?
if [ $EXITVALUE != 0 ]; then
    /usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"
fi
exit 0
```

- Daemon de journalisation des évènements du noyau : klogd
- Alternative à syslogd : syslog-ng, rsyslogd

Quelques conseils LPI...

- Etudier le fonctionnement de syslogd. Connaître la syntaxe de /etc/syslog.conf et entraînez vous à rediriger des messages
- Redirection vers un serveur de log centralisé
- Exclure tout message : level à none
- Il faut comprendre le principe de fonctionnement de logrotate et regarder man logrotate
- Connaître le nom exact des fichiers de config de syslogd et logrotate
- Que fait la commande logger ?