Journalisation

ASR ING 2 2021

SERVICE SYSLOG

- syslog est un service (ou daemon) qui journalise les événements du système
- L'enregistrement des événements est géré par les programmes : klogd et syslogd rsyslog
- Fichier de configuration /etc/syslog.conf /etc/rsyslog.conf

Service syslog

Principes de fonctionnement

Les évènements envoyés au démon syslog sont identifiés par 3 éléments :

- Le sous-système (facility) : l'origine du message
- Le niveau (level/priority) : la priorité du message
- L'action à réaliser : correspond à la destination du message

SERVICE SYSLOG

- Facilité

Code	Mot clé	Description
0	Kern	Noyau système
1	User	Utilisateurs
2	Mail	Mécanisme du courrier
3	Daemon	Démons systèmes
4	Auth	L'authentification
5	Syslog	messages internes générés par syslogd
6	Lpr	Processus d'impression
7	News	Serveur de news
8	Uucp	Programmes fondés sur UUCP
9	*	Tous les niveaux (équivalent à debug)
16	Local[0-7]	Réservé pour des usages propres

SERVICE SYSLOG

- Gravité

Code	Gravité	Mot clé	Description
0	Emergency	emerg (panic)	Système inutilisable.
1	Alert	Alert	Une intervention immédiate est nécessaire.
2	Critical	Crit	Erreur critique pour le système.
3	Error	err (error)	Erreur de fonctionnement.
4	Warning	Warning (warn)	Avertissement (une erreur peut intervenir si aucune action n'est prise).
5	Notice	Notice	Événement normal méritant d'être signalé.
6	Informational	Info	Pour information.
7	Debug	Debug	Message de mise au point.

Service syslog

- Action

Peut être :

- un fichier : /var/log/meslogs
- le service syslogd d'une autre machine : @192.168.1.89
- la console : /dev/console
- Le joker * remplace toute facility, level ou action.

Service syslog

- Fichier de configuration syslog.conf

```
#  /etc/syslog.conf     Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.

#
# First some standard logfiles.  Log by facility.
#

auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
uucp.*                          /var/log/uucp.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

# Logging for INN news system
#
news.crit                       /var/log/news/news.crit
news.err                        /var/log/news/news.err
news.notice                     -/var/log/news/news.notice
```

SERVICE SYSLOG

- Fichier de configuration syslog.conf

Chaque entrée dans le fichier /etc/syslog.conf est de la forme

Sous-système.niveau action

Par exemple, l'entrée :

local2.info /var/log/syslog.local2

Service syslog

- Commande logger

Pour tester la configuration du fichier syslog.conf

logger -p facilité.niveau message

- Par exemple :

logger -p local2.info « Message dans le fichier syslog.local2 »

Le message apparaît alors dans le fichier /var/log/syslog.local2, si la configuration est correcte.

SYSLOG-NG VERSUS RSYSLOG

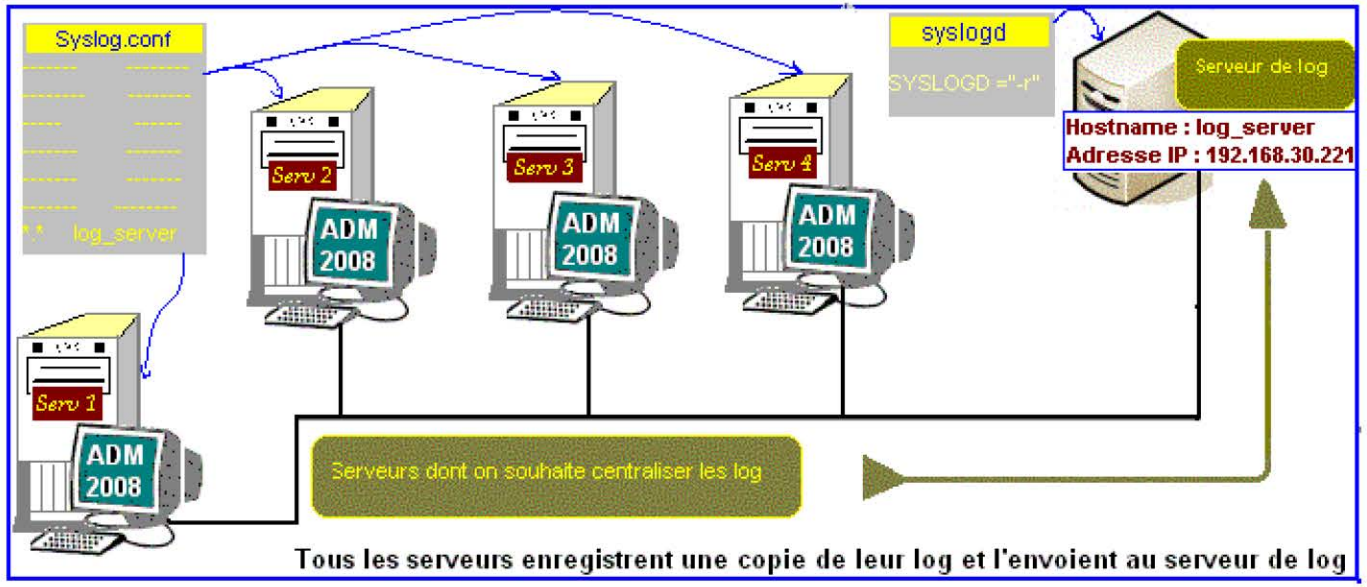
Syslog-ng

- Une configuration puissante
- Un tri des messages par leur contenu
- Une meilleure redirection des messages sur le réseau
- UDP et TCP utilisés pour le transport des journaux
- Chiffrer et authentifier le trafic réseau
- Compresser les journaux

rsyslog

- Gère les relais : possibilité de connaître le chemin parcourus par les messages
- transport sur TCP
- Stockage dans les bases des données
- support du nouveau syslog IETF

CENTRALISATION DES LOGS



Rotation des logs

ROTATION DES LOGS

- Fichier de configuration logrotate.conf

```
# 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
minsize 1M
create 0664 root utmp
rotate 1
}
```

ROTATION DES LOGS

- Exemple : service postfix

```
/var/log/maillog {
daily
missingok
rotate 52
compress
delaycompress
notifempty
create 640 root
sharedscripts
postrotate
if [ -f /var/run/postfix.pid ]; then
/etc/init.d/postfix reload > /dev/null
fi
endscript
}
```

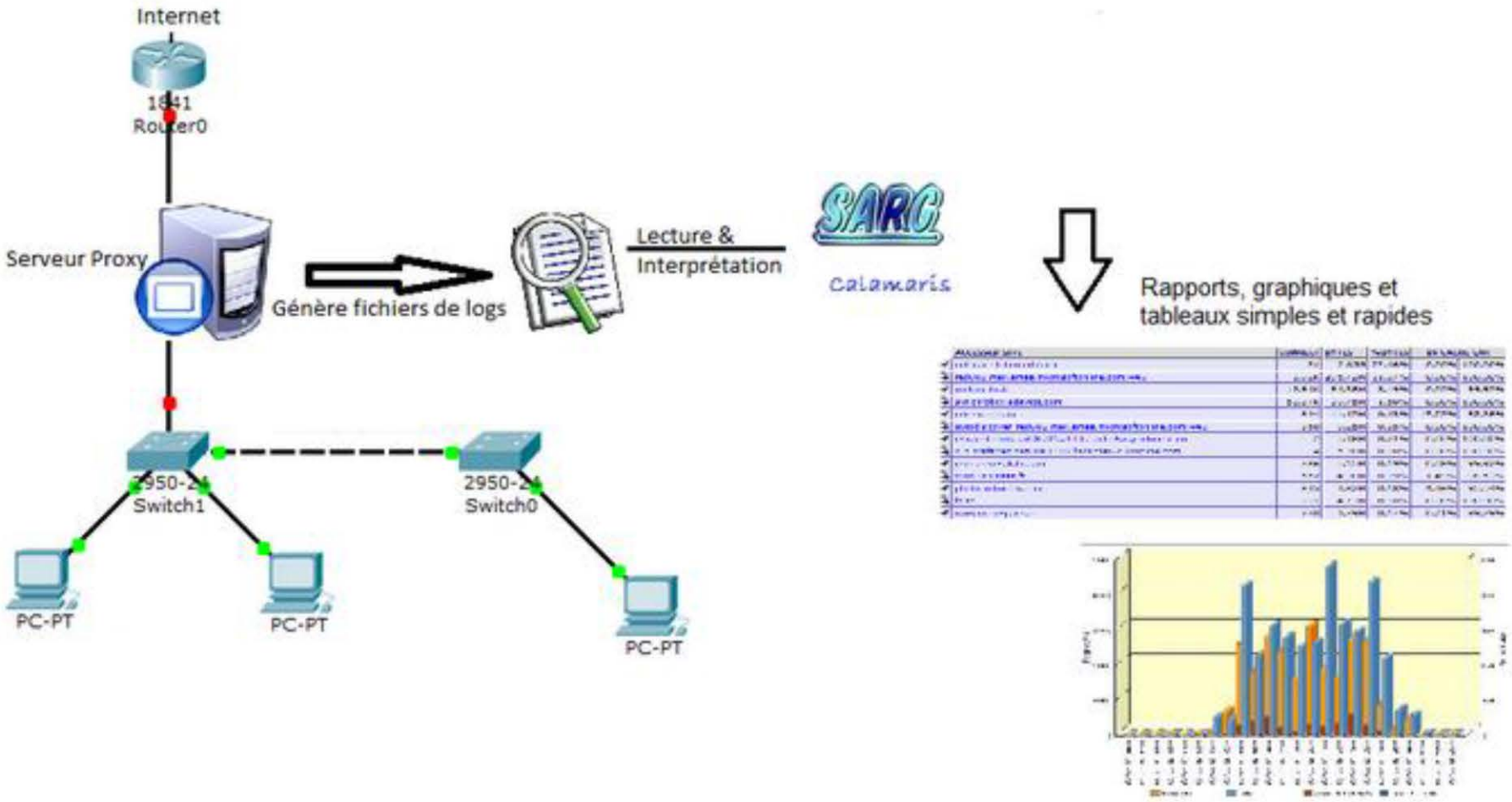
Rotation des logs

- Exécution :

  logrotate -f /etc/logrotate.conf
- Pour débugger :

  logrotate -d /etc/logrotate.conf

Analyse des logs



Analyse des logs

- Exemples d'analyseurs des logs:
- Analog
- Awstats
- W3Perl

Fournissent plusieurs informations utiles telles que:

- les visites
- visiteurs uniques
- pages
- heures de pointes
- moteurs de recherche
- mot clés
- liens invalides et des fonctions inédites