Logs linux

Table of Contents

1. Important

Les logs sont générés par le service 'rsyslogd'

Où c'est stocké?:

> vi /etc/rsyslog.conf ls /etc/rsyslog.d/

2. Repertoire

> Les logs dans linux sont placés généralement dans le repertoire /var/log et ces sous-repertoires. Ces repertoires sont générés par défaut par les applications installées au file du temps. Les commandes pour afficher les logs sont: .'less' commande .'more' commande .'cat' commande .'grep' commande .'tail' commande .'zcat' commande .'zgrep' commande .'zmore' commande

3. Comment on y accède

Ouvrir le terminale. Accèder a /var/log en tant que 'root' en utilisant la commande:

```
cd /var/log
```

lister les fichiers

```
ls
```

> less /var/log/messages more -f /var/log/messages cat /var/log/messages tail -f /var/log/messages grep -i error /var/log/messages

4. Ce qu’il faut retenir

Les fichiers standard logs et son rôle:

'/var/log/messages' : Les messages générale par le système et le reste '/var/log/auth.log' : Journaux d’authenication '/var/log/kern.log ': Journaux du Kernel '/var/log/cron.log ': Journaux Crond (cron job) '/var/log/maillog' : Journaux du serveur mail '/var/log/qmail/ ': Repertoire des journaux de Qmail, un repertoire (more files inside this directory) '/var/log/httpd/' : Repertoire des journaux des accès et erreur Apache '/var/log/lighttpd/' : Journaux des accès et des erreurs Lighttpd '/var/log/boot.log ': Journaux du System boot '/var/log/mysqld.log' : Journaux de la base de données MySQL serveur '/var/log/secure' or '/var/log/auth.log' : Journaux des authentications '/var/log/utmp' or '/var/log/wtmp' : Journaux des accès Logins '/var/log/yum.log' : Journaux de la commande Yum.

5. Astuces avec AWK sur les LOGs

` cat log | awk'{gsub("\[ | :.* ","", $4) tab[$4" - "$1]++} END {for(i in tab) print i" nb de fois: " tab[i]}' `

` cat log | awk'{gsub("\[","", $4) tab[$4" - "$1]++} END {for(i in tab) print i" nb de fois: " tab[i]}' `