log

- Objet : Tableau des différents messages log
- Niveau requis :
  avisé
- Suivi :
  à-compléter, à-placer
- Commentaires : *Tableau des différents messages distribués par le système.*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !.
- Commentaires sur le forum : C'est ici[1)]

Introduction

Le répertoire `/var/log/` est l'endroit où sont centralisés tous les fichiers de **log**.

C'est donc simple de se souvenir qu'il faut aller voir dans ce répertoire au moindre problème.

L'un des fichiers de ce répertoire que l'on regarde à chaque problème est le fichier `/var/log/messages`.
Ce fichier contient toutes les erreurs dites "générales".
Dans ce fichier, vous y trouverez les messages relatifs au réseau, aux médias, etc...

Pour administrer votre machine, vous pouvez toujours utiliser une application telle que **logwatch** qui va générer des rapports basés sur les fichiers du répertoire `/var/log/`.

Tableau

18/07/2011

Le tableau ci-dessous représente les fichiers présents dans le répertoire `/var/log` avec un petit descriptif de ces fichiers.

LIEN	***PARTICULARITÉ***	***COMMENTAIRE***
/var/log/aptitude	Journal de l'utilisation de aptitude	Utile pour situer une version particulière modifiée par une mise à jour
/log/auth.log	Journal des activités demandant une permission	Surveiller l'activité d'un crontab par exemple...
/var/mail	Ce sont des messages datés du système	Visite des différents fichiers mail disponibles conseillés.
/var/log/syslog	Démarrages du système	Le journal du fonctionnement du système depuis son démarrage.

Exemple pratique

À propos du sinistre sur une copie rsync malencontreuse faite dans un disque externe.

Si on veut les logs du noyau, on prend les fichiers kern.log* et pas les syslog* et autres messages* pour ne pas être pollué par les messages d'autres sources que le noyau.
Chaque ligne de log est horodatée, donc il faut avoir au moins la date et l'heure approximatives.

Par exemple si ça s'est produit le 17 avril vers 7 ou 8 heures du matin la commande :

```
zgrep "Apr 17 0[78]" /var/log/kern.log*
```

(*zgrep c'est pour lire les logs qui ont été compressés*)

De raleur sur le forum, là :

- https://debian-facile.org//viewtopic.php?pid=329880#p329880

Merci.

1)
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !