Les outils de journalisation

Journald

Journald est un service (deamon) de gestion des journaux système (il fait partie du projet systemd) qui remplace les fichiers texte traditionnels comme **/var/log/syslog**. Il stocke les journaux dans une **base de données binaire indexée**, ce qui permet une recherche et un filtrage plus rapides et efficaces des entrées de journal.

Syslog

Syslog est une solution **historique** sur Linux/UNIX, il récupère des informations **noyau** (via **klogd**), celles envoyées sur le socket **/dev/log**, et possiblement via le réseau (**protocole syslog, UDP port 514**) et les écrit (par défaut) dans des fichiers textes dans **/var/log/...**

Les logs sont classé par 2 codes :

1. Les **“facility”** de 0 à 26, ils aident à déterminer les types de message journalisé.
2. Les **“Severity Level”** de 0 à 7, 0 étant le plus critique (emergency) et le 7 du debug.

Voir ici le tableau en entier

Logrotate

Logrotate est un utilitaire qui permet de gérer la **rotation**, l'**archivage** et la **compression** des fichiers journaux (logs) sur les systèmes Unix/Linux. Il est généralement utilisé pour éviter que les fichiers journaux ne deviennent trop **volumineux** et n'occupent trop d'**espace disque**.

Pour installé **logrotate** ou vérifier si il est installé :

```
sudo apt install logrotate
```

Les configurations et les options par défaut de l'utilitaire **Logrotate** sont disponibles dans le fichier **/etc/logrotate.conf**

Mais les informations spécifiques à la journalisation de certaines applications (surchargeant les paramètres par défaut) sont conservées dans le répertoire **/etc/logrotate.d/.** .

Voici un **exemple** de configuration d'un logrotate d'unserveur web stocké dans **/etc/logrotate.d/httpd.conf**

```
/var/log/httpd/access.log
/var/log/httpd/error.log
/var/log/httpd/monsite/*.log
{
  rotate 5
  mail mail@example.org
  size 100k
  shadescripts
  postrotate
    /usr/bin/killall -HUP httpd
  endscript
}
```

- concerne les logs d'un **serveur web**
- les fichiers sont « rotatés » **5 fois** ; la rotation intervenant à chaque fois que le fichier de log **atteint 100 Ko** (puis supprimés)
- un **mail** est envoyé à chaque rotation
- une **action est réalisée** après chaque rotation

Pour s'assurer qu'un fichier de logs effectue correctement ses rotations ou, pour vérifier la date et l'heure de sa dernière rotation, consulter le fichier **/var/lib/logrotate/status** ou **logrotate.status**.

```
sudo cat /var/lib/logrotate/logrotate.status
```

S'il y a besoin de **forcer** la rotation, voici la commande.

```
sudo logrotate -f /etc/logrotate.conf
```

Documentation d'Ubuntu France pour d'autres exemples
