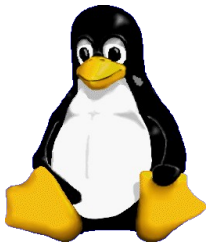

Le système GNU/Linux

By ShareVB

Syslog

Table des matières

I. Introduction

Syslog permet de centraliser les différents messages de sécurité et d'information des services du système. Ces différents messages peuvent être redirigés dans un fichier, ce qui permettra à l'administrateur de savoir par exemple pourquoi un service ne fonctionne pas correctement, quelles sont les dernières connexions qui ont échouées…Syslog permet par exemple de regrouper les logs par niveau de criticité (erreur, warning, info, debug...) mais aussi par service.

II. Fichier de configuration

Le fichier de configuration de syslogd est `/etc/syslog.conf`. Lorsque ce fichier est modifié, il faut envoyer le signal SIGHUP au démon syslogd pour le forcer à relire ce fichier.

Les fichiers de log sont en général dans `/var/log`

2. Syntaxe générale

Une ligne de `/etc/syslog.conf` se compose comme suit :

facility.level <tabs> destination

- *facility* peut prendre les valeurs suivantes :
  - auth, authpriv, security (same as auth)
  - cron, daemon,
  - kern, lpr, mail, mark, news, syslog,
  - user, uucp et local0 à local7.

- *level* peut prendre les valeurs suivantes :
  - debug,
  - info, notice, warning, warn (same as warning),
  - err, error (same as err),
  - crit, alert,
  - emerg, panic (same as emerg).

- *destination* peut prendre les valeurs suivantes :
  - *<nom de fichier absolu>* : un fichier de log
  - *<nom de fichier fifo>* : un programme « filtre » de logs
  - *<nom de console ou de tty>* : un terminal ou une console
  - *<nom d'utilisateur(s)>* : toutes les consoles d'un utilisateur
  - *@nom_de_machine* : une machine serveur de log
  - * : toute personne loguée

- On peut combiner plusieurs facility pour un même level avec la syntaxe : facility1,facility2,...,facilityn.level
- On peut mettre plusieurs facility.level pour une même destination en les separant par ;
- facility et level peuvent être remplacé par * pour dire toutes les valeurs possibles de level ou de facility
- level peut être none pour indiquer que l'on ne veut pas de logs de la facility qui précède. (par ex : *.crit;kern.none : tous les crit sauf ceux du kernel)

- le signe « . » peut être :
  - . signifie tous les niveaux supérieurs ou égaux à level
  - .= signifie seulement le niveau level
  - .! signifie tous les niveaux sauf level et les niveaux supérieurs à level
  - .!= signifie tous les niveaux sauf level

Par exemple, pour que tous les messages d'erreur s'affichent sur le terminal 12 (console virtuelle 12), on peut inscrire :

```
*.err                /dev/tty12
```

3. Redirection de logs par le réseau

Pour rediriger des logs vers une autre machines qui sert de serveur de logs, il suffit de mettre dans destination « *@IP_ou_nom_DNS_serveur_logs* ». Par exemple, « *.* @172.20.12.3 » redirige tous les logs à la machine 172.20.12.3. Ensuite, il faut lancer syslogd avec l'option -r.

Toutefois, le serveur de logs 172.20.12.3 ne peut pas, à son tour, renvoyer les logs vers un autre serveur de logs par le réseau à moins qu'il est été lancé avec l'option -f et qu'il soit configuré avec une ligne « @ » dans son fichier /etc/syslog.conf. **Attention toutefois à ne pas faire de boucle : un serveur de logs envoie à un autre qui, à son tour, renvoie ce qu'il a reçu. Il y a risque de remplir un disque entier en très peu de temps avec un seul message.**

Il est à noter que pour autoriser des logs à parvenir à un serveur de logs faisant tourner syslog, il faut autoriser le trafic UDP sur le port 514. Cela peut donner les règles iptables suivantes :

```
iptables -A INPUT -p udp --dport 514 -s <ip machine loggante> -j ACCEPT
```

Il peut être plus sûr de spécifier de quelles machines peuvent venir les logs afin de ne pas risquer une attaque par flooding.

III. Consultation des logs

Par défaut, les messages de sécurités sont dans `/var/log/secure` et les messages de généraux sont dans `/var/log/messages`. De plus, la commande `dmesg` permet de consulter les messages de log du noyau de dernier démarrage.

Enfin, la commande `last` sert à connaitre les dernière personnes qui se sont connectées sur la machine.

IV. La rotation des logs : logrotate

En rapport avec syslogd mais utilisant surtout cron, on remarquera que dans tous les répertoires de logs, il y a des fichiers .0, .1...qui contiennent les logs anciens. Ces fichiers sont générés par `logrotate` dans le but d'alléger les logs des programmes et de supprimer les logs les plus anciens. Sa configuration se fait dans `/etc/logrotate.conf`.

Si l'on inclus la directive `include /etc/logrotate.d`, tous les fichiers contenu dans ce dossier sont inclus dans le traitement.

Pour chaque fichier de log, on ajoute soit dans `/etc/logrotate.conf` ou dans un fichier de `/etc/logrotate.d` :

```
<chemin et nom du fichier> {
    <directives>
}
```

<chemin et nom du fichier> peut être soit un fichier ou un nom extensible (`*`).

<directives> est un ensemble de plusieurs directives, une par ligne :

- `daily` : rotation journalière
- `weekly` : rotation hebdomadaire
- `monthly` : rotation mensuelle
- `rotation` *<number> :* période de rotation. Nombre de rotation avant suppression du fichier de log le plus ancien (par ex: si `weekly` et `rotation 4`, supression des log de plus d'un mois)
- `mail` *<email>* : envoyer le fichier de log par email quand il sort de la période de rotation
- `missingok` : pas d'erreur si le fichier n'existe pas
- `postrotate/endscript` : script à exécuter après la rotation
- `sharedscripts` : n'exécuter le script qu'une fois en cas de nom de log extensible (*)
- `notifempty` : ne pas traiter les fichiers vides

Par exemple :

```
            /var/log/httpd/*log {
                  # pas d'erreur si pas de logs
                missingok
                  # passer les fichiers vides
                notifempty
                  # ne recharger syslog qu'une fois
                sharedscripts
                postrotate
                  /bin/kill -HUP $(cat /var/run/httpd.pid 2>/dev/null) 2>
/dev/null || true
                endscript
            }
```

V. Bibliographie

Syslog - Wikipédia

Logging via **Syslog**

Syslog