Logwatch : Outil d'analyse de journaux système

I – Présentation

Logwatch est un analyseur de journaux système (appelés logs) pour Unix. Ce dernier est entièrement personnalisable à partir du fichier de configuration. Il permet de recevoir quotidiennement un mail récapitulatif de l'utilisation d'un serveur en analysant les logs situés dans /var/log (paquets installés, désinstallés, ou mis à jour ; mails envoyés ; utilisation des disques durs ; attaques potentielles reçues par le serveur ; etc.).

II – Installation

Note : Pour pouvoir utiliser Logwatch, une messagerie est nécessaire. J'ai utilisé Postfix (voir le TD correspondant pour la configuration).
Attention : Si vous utilisez deux machines identiques sous VMware, il faut changer le nom d'hôte de l'une des deux sous peine de non réception du mail de la part de Logwatch. Faites *Gedit /etc/hostname* ; indiquer le *nouveau_nom_hote* puis redémarrer la machine.

Afin de pouvoir procéder à l'installation de cet outil dans la salle C107, nous devons définir la variable d'environnement http_proxy. Ouvrez un terminal et tapez la commande suivante :

```
export http_proxy=http://192.168.196.246:3128
```

Sur la majorité des distributions, la commande suivante fonctionne et permet d'installer « Logwatch » directement à partir d'Internet :

```
apt-get install logwatch
```

Note : Sur Debian, cela fonctionne très bien. Si vous obtenez des difficultés avec Ubuntu, vous pouvez télécharger le package « Logwatch » à partir de cette adresse : http://packages.ubuntu.com/

III – Configuration

Maintenant que l'installation est terminé, nous pouvons passé à sa configuration. Le nom du fichier permettant ceci se nomme « logwatch.conf » :

```
gedit /usr/share/logwatch/default.conf/logwatch.conf
```

Dans ce fichier, nous allons modifier les champs suivants :

Ligne n°34 : Nous indiquons l'adresse mail vers laquelle nous souhaitons recevoir les rapports de logs : *remplacer* **`MailTo = root`** *par* **`MailTo = mon@adresse.com`**

Ligne n°65 : Indication du niveau de détail (Low, Medium, High ou un chiffre entre 1 et 10 du moins détaillé au plus détaillé) : **`Detail = High`**

Ligne n° 79 : Indication des services que l'on souhaite voir dans le rapport : nous laissons **`Service = All`** pour tout autoriser, puis, s'il y a des services que vous ne désirez pas voir apparaître dans votre future analyse de logs, il suffit de les soustraire de cette manière :

```
Service = "-zz-network"
Service = "-zz-eximstats"
Service = "-iptables"
```

Notes : En procédant ainsi, les journaux systèmes seront plus simple à analyser ; dû à une meileure clarté. La liste des services surveillés par Logwatch se situent dans le répertoire suivant : /usr/share/logwatch/default.conf/services

Ligne n° 109 : Indication du type de messagerie utilisé. Par défaut, Logwatch utilise Sendmail. En utilisant Postfix, nous pouvons laisser la ligne telle quelle : **`mailer = "sendmail -t"`**

Ligne n° 48 : Nous désirons recevoir les informations uniquement par mail et non sur le terminal. Pour cela, nous allons changer la valeur suivante au champ Print : **`Print = No`**

Nous devons également ajouter une ligne au fichier de configuration de Postfix :

```
gedit /etc/postfix/main.cf
```

Ajouter l'origine sous la forme suivante : **`myorigin=logwatch.fr`**

IV – Utilisation

La configuration étant effectuée, nous pouvons taper la commande suivante pour vérifier le bon fonctionnement :

```
logwatch --range=Today --print
```

Normalement, l'analyse des journaux systèmes devrait s'afficher sur le terminal. Nous pouvons maintenant utiliser la commande suivante afin de recevoir un mail :

```
logwatch --range=Today
```

Vous devriez avoir reçu un mail.

Le script de lancement (00logwatch) est dans `/etc/cron.daily`

Désormais, vous recevrez chaque jour ce type de mail. Logwatch est un outil très pratique pour les administrateurs réseaux et systèmes car il procure un gain de temps relativement important.

V – Liens utiles

http://www.logwatch.org
http://www.tryxy.net/index.php/Logwatch