Monitorer ses Logs avec Logwatch

Installation de Logwatch

Les rapports créés par Logwatch sont classés selon les services (Applications) exécutés sur votre système. Les applications peuvent être définies dans le fichier de configuration de logwatch. De plus, Logwatch permet la création de scripts d'analyse personnalisés pour des besoins spécifiques

Installation du paquet:

```
apt install logwatch
```

S'il n’existe pas déjà créez le dossier `/var/cache/logwatch` nécessaire au bon fonctionnement de logwatch :

```
mkdir /var/cache/logwatch
```

Configuration de Logwatch

On va modifier le fichier de configuration se trouvant à l'adresse `/usr/share/logwatch/default.conf/logwatch.conf`, ouvrons le avec l'éditeur de notre choix.

Pour cela on va créer une copie du fichier de configuration par défaut

```
cp /usr/share/logwatch/default.conf/logwatch.conf /etc/logwatch/conf/logwatch.conf
```

Puis on l'édite:

```
nano /etc/logwatch/conf/logwatch.conf
```

On observera une longue liste de variables que l'application utilise lors de son éxécution.
Nous modifierons ou ajusterons les valeurs suivantes:

```
# Le type d'output ici on veut recevoir nos logs par mail
Output = mail
```

```
# Pour recevoir les mails au format html, c'est plus agréable à lire
Format = html
# Adresse sur laquelle vous allez recevoir les mails
MailTo = root # <= Correspondra a l'adresse précédemment définis pour root dans le setup du service mail
# Niveau de détail des logs Low | Med | High
Detail = Med

# Pour les services vous pouvez gardez la ligne Service = All mais si vous souhaitez
# recevoir seulement des rapports spécifiques vous pouvez lister chaque service comme ci dessous
# (en retirant le #). Nous garderons All dans notre cas

# Service = sendmail
# Service = http
# Service = identd
# Service = sshd2
# Service = sudo
```

Ajoutons un rapport de log pour Nginx (Si vous utilisez Nginx of course)

Pour commencer on va créer une configuration spécifique:

```
nano /etc/logwatch/conf/logfiles/nginx.conf
```

Puis nous allons copier dedans la configuration ci dessous:

```
#########################################################
# Define log file group for nginx
#########################################################

# What actual file? Defaults to LogPath if not absolute path….
LogFile = nginx/*access.log
LogFile = nginx/*access.log.1
LogFile = nginx/*error.log
LogFile = nginx/*error.log.1

# If the archives are searched, here is one or more line
# (optionally containing wildcards) that tell where they are…
#If you use a “-” in naming add that as well -mgt
Archive = nginx/*access.log*
```

```
Archive = nginx/*error.log*

# Expand the repeats (actually just removes them now)
*ExpandRepeats

# Keep only the lines in the proper date range…
*ApplyhttpDate

# vi: shiftwidth=3 tabstop=3
```

On crée ensuite le second fichier essentiel pour faire correspondre notre service *(en se basant sur la conf http existante)*:

```
cp /usr/share/logwatch/default.conf/services/http.conf /etc/logwatch/conf/services/nginx.conf
```

On l'ouvre ensuite avec notre éditeur préféré:

```
nano /etc/logwatch/conf/services/nginx.conf
```

Puis on modifie le début du fichier:

```
Title = “nginx”
LogFile = nginx
```

Et pour finir on copie le fichier du script:

```
cp /usr/share/logwatch/scripts/services/http /etc/logwatch/scripts/services/nginx
```

Puis on relance logwatch vous devriez recevoir un mail récapitulatif et par la suite un mail journalier:

```
logwatch restart
```

Et voilà logwatch vous permettra de garder une trace de ce qu'il se passe sur votre serveur quotidiennement !
Pour modifier un service reprenez l'exemple ci dessus et modifiez `http` et `nginx` par le service correspondant à votre besoin.

Revision #4
Created 2021-01-29 09:30:27 UTC by Faces
Updated 2022-06-10 17:49:11 UTC by Faces