Logwatch

Généralités

Logwatch est un outil de reporting par mail de ce qui se passe sur le serveur. Il est modulable en fonction des éléments qu'on souhaite voir remonter dans les messages.

Documentation

Le fichier de doc explique l'architecture de dossier qui permet de surcharger la configuration par défaut.

```
/usr/share/doc/logwatch/HOWTO-Customize-LogWatch.gz
```

Installation

```
yum install logwatch
apt install logwatch
```

Configuration

Plusieurs répertoires sont présent par défaut.

```
/usr/share/logwatch/default.conf/ : pour la configuration générique
/usr/share/logwatch/dist.conf/ : pour la configuration spécifique à Ubuntu
/etc/logwatch/ : pour la machine en elle-même, c'est la que vous ferez votre propre configuration
```

Créer le fichier de configuration suivant qui contiendra uniquement les éléments à surcharger par rapport au fichier de configuration par défaut `/usr/share/logwatch/default.conf/logwatch.conf`.

```
vi /etc/logwatch/conf/logwatch.conf
```

Ajouter les informations à surcharger par rapport à la configuration par défaut.

```
MailFrom = <source_mail_fqdn>
MailTo = "<destination_mail_fqdn>"
Range = yesterday
Detail = High
mailer = "/usr/sbin/sendmail -t"
```

Voici le script à exécuter pour recevoir le logwatch dans la boite mail.

```
/usr/sbin/logwatch --output mail
/usr/sbin/logwatch --mailto <adressemail>@<domaine>
```

En fonction de la configuration mail, les mails logwatchs iront à root ou une boîte mail dédiée. Ces mails permettront de connaître les modifications intervenues sur le système, les espaces disques, les paquets installés, les comptes ajoutées,...

Pour information, le fichier de configuration sur RHEL 4 utilise mail à la place de sendmail et est positionné à l'endroit suivant.

```
vi /etc/log.d/conf/logwatch.conf
```

Le script exécuté sous RHEL 4 est `/etc/log.d/scripts/logwatch.pl`. Dans la version de logwatch installé sur les RHEL 4, il n'y a pas la possibilité d'envoyer les mails “en tant que” car l'option `MailFrom` n'existe pas. Les mails sont donc affichés en provenance de root. Cela n'a pas de conséquence importante, il faut juste le savoir.