

Una utilidad que como sysadmins nos será de muchísima ayuda, es logwatch. Ésta herramienta nos envía un informe todos los días indicando los cambios o acciones más significativas sobre el sistema.

Vamos a describir unos sencillos pasos de instalación y configuración

1) instalar logwatch: Dependiendo de la versión de Linux bien **yum install logwatch** o **apt-get install logwatch**

2) configurar logwatch: /usr/share/logwatch/default.conf/logwatch.conf

un ejemplo de lo que debería tener el archivo conf sería

```
Output = mail
Format = html (también podemos comentarlo con # si lo queremos "plano")
MailTo = myemail@mydomain.com
MailFrom = logwatch@mydomain.com
```

3) editamos el cron para que se ejecute diariamente

```
# m h dom mon dow  command
0 1 * * *    /usr/sbin/logwatch
```

Si trasteamos un poco más con el archivo de configuración veremos que de igual manera podemos elegir los logs a evaluar, el rango de días, el detalle...