Inotify , surveillance des fichiers

upper limit on inotify watches reached! KESAKO?

1) upper limit on inotify watches reached!

Les systèmes **Linux** et **Unix-like** disposent d'un système de surveillance , de création des fichiers utilisateur : **inotify**.
En voulant lancer **Malware detector** en mode monitor, que j'ai eu ce message:

```
sudo maldet --monitor /home/ordinatous
Linux Malware Detect v1.6.2
            (C) 2002-2017, R-fx Networks <proj@rfxn.com>
            (C) 2017, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(10359): {mon} added /home/ordinatous to inotify monitoring array
maldet(10359): {mon} starting inotify process on 1 paths, this might take awhile...
maldet(10359): {mon} no inotify process found, check /usr/local/maldetect/logs/inotify_log for errors.
```

Je m'execute et vais voir les logs:

```
sudo tail /usr/local/maldetect/logs/inotify_log
Setting up watches.  Beware: since -r was given, this may take a while!
Failed to watch /home/ordinatous; upper limit on inotify watches reached!
Please increase the amount of inotify watches allowed per user via `/proc/sys/fs/inotify/max_user_watches'.
```

Et le système demande d'augmenter la valeur (le nombre de fichiers) que **inotify** peut surveiller par utilisateurs. Par défault ce doit être 8152 (il me semble)

1.1) Résolution

Il faut donc modifier la valeur pour l'inscrire dans le fichier de configuration système.

```
echo fs.inotify.max_user_watches=524288 | sudo tee -a /etc/sysctl.conf && sudo systctl -p
```

1.2) Verification

```
sudo sysctl -p
[sudo] Mot de passe de ordinatous :
net.ipv4.icmp_echo_ignore_all = 1
fs.inotify.max_user_watches = 524288
```

2) Test

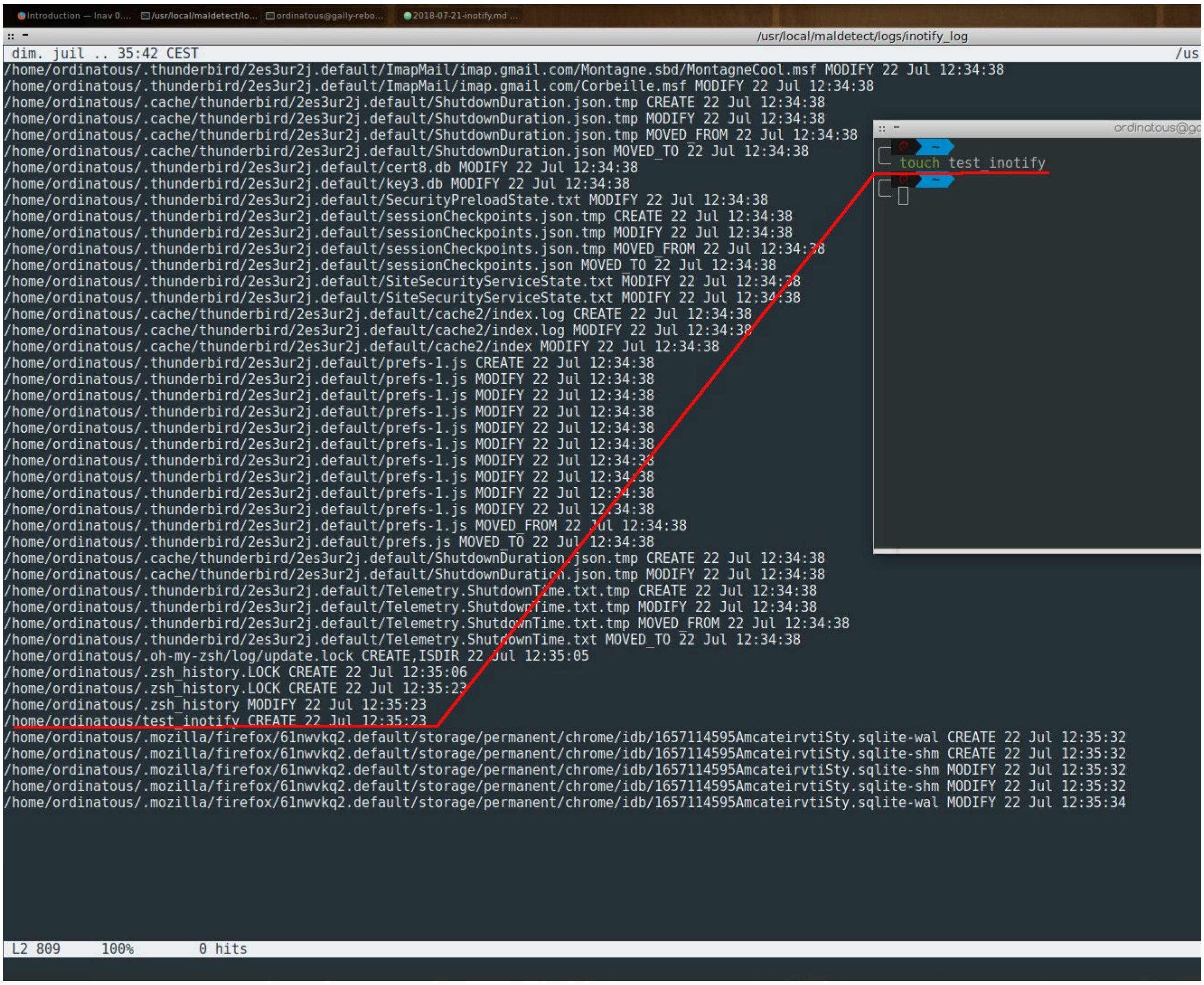
```
sudo maldet -m /home/ordinatous
Linux Malware Detect v1.6.2
            (C) 2002-2017, R-fx Networks <proj@rfxn.com>
            (C) 2017, Ryan MacDonald <ryan@rfxn.com>
This program may be freely redistributed under the terms of the GNU GPL v2

maldet(13645): {mon} added /home/ordinatous to inotify monitoring array
maldet(13645): {mon} starting inotify process on 1 paths, this might take awhile...
maldet(13645): {mon} inotify startup successful (pid: 13755)
maldet(13645): {mon} inotify monitoring log: /usr/local/maldetect/logs/inotify_log
```

On voit que la modification a été prise en compte

2.1) Logs

Je vérifie à nouveau le fichier de `logs` , mais cette fois avec `lnav` qui est un outil vraiment génial.
`lnav` permet de d'avoir un affichage dynamique des `logs` avec une coloration ce qui les rend plus lisible, sauf ici car c'est du text brut.
Je vais un petit test, en créant un fichier `test_inotify`.



Et voilà. Exactement ce qu'il faut, `inotify` m'indique toutes les modifications faites dans mon répertoire personnel.