

Inotify , surveillance des fichiers

upper limit on inotify watches reached! KESAKO?

- ↪ [upper limit on inotify watches reached!](#)
- ↪ [Résolution](#)
- ↪ [Verification](#)
- ↪ [Test](#)
- ↪ [Logs](#)

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'exécute 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 défaut 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 sysctl -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

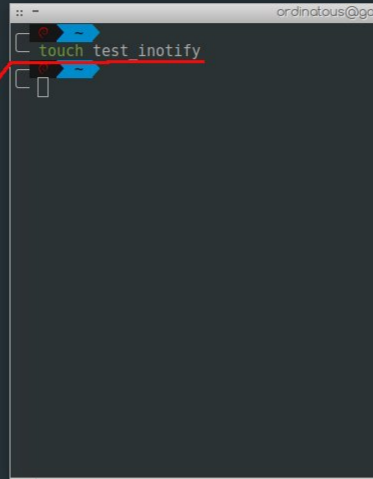
Je vérifie à nouveau le fichier de logs , mais cette fois avec `lnav` qui est un outil vraiment génial.

`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`.

```
Introduction - Inav 0... /usr/local/maldetect/lo... ordinatous@gally-rebo... 2018-07-21-inotify.md ... /usr/local/maldetect/logs/inotify_log /us
dim. juil .. 35:42 CEST
/home/ordinatous/.thunderbird/2es3ur2j.default/ImapMail/imap.gmail.com/Montagne.sbd/MontagneCool.msf MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/ImapMail/imap.gmail.com/Corbeille.msf MODIFY 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp CREATE 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp MODIFY 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp MOVED FROM 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp MOVED TO 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/cert8.db MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/key3.db MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/SecurityPreloadState.txt MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/sessionCheckpoints.json.tmp CREATE 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/sessionCheckpoints.json.tmp MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/sessionCheckpoints.json.tmp MOVED FROM 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/sessionCheckpoints.json.tmp MOVED TO 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/SiteSecurityServiceState.txt MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/SiteSecurityServiceState.txt MODIFY 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/cache2/index.log CREATE 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/cache2/index.log MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/cache2/index MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js CREATE 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs-1.js MOVED FROM 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/prefs.js MOVED TO 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp CREATE 22 Jul 12:34:38
/home/ordinatous/.cache/thunderbird/2es3ur2j.default/ShutdownDuration.json.tmp MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/Telemetry.ShutdownTime.txt.tmp CREATE 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/Telemetry.ShutdownTime.txt.tmp MODIFY 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/Telemetry.ShutdownTime.txt.tmp MOVED FROM 22 Jul 12:34:38
/home/ordinatous/.thunderbird/2es3ur2j.default/Telemetry.ShutdownTime.txt.tmp MOVED TO 22 Jul 12:34:38
/home/ordinatous/.oh-my-zsh/log/update.lock CREATE, ISDIR 22 Jul 12:35:05
/home/ordinatous/.zsh_history.LOCK CREATE 22 Jul 12:35:06
/home/ordinatous/.zsh_history.LOCK CREATE 22 Jul 12:35:23
/home/ordinatous/.zsh_history MODIFY 22 Jul 12:35:23
/home/ordinatous/test_inotify CREATE 22 Jul 12:35:23
/home/ordinatous/.mozilla/firefox/61nvvkq2.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-wal CREATE 22 Jul 12:35:32
/home/ordinatous/.mozilla/firefox/61nvvkq2.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-shm CREATE 22 Jul 12:35:32
/home/ordinatous/.mozilla/firefox/61nvvkq2.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-shm MODIFY 22 Jul 12:35:32
/home/ordinatous/.mozilla/firefox/61nvvkq2.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-shm MODIFY 22 Jul 12:35:32
/home/ordinatous/.mozilla/firefox/61nvvkq2.default/storage/permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite-wal MODIFY 22 Jul 12:35:34

L2 809 100% 0 hits
```



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