

Date de publication Dimanche 30 janvier 2011 à 12:01:15 par Cyril
Catégorie Administration Linux

Comment stopper les plantages de Fail2ban sur un serveur multicores (plus de 8 coeurs)

J'ai du ce matin intervenir sur une machine (sur sollicitation) sous Debian dotée de deux processeurs et 16 coeurs parce que ce foutu Fail2ban refusait de se lancer normalement, ou ne chargeait que quelques jails mais pas tous ...

Analyse du problème.

Lors du lancement de Fail2ban, et ce de manière aléatoire je me prend dans la face un joli failed.

Type de truc qui me plait bien, ni une ni deux je fonce dans les logs, pour me retrouver avec une floppée de messages de ce type sur les jails non lancés

```
[linux]2011-01-30 10:58:13,010 fail2ban.actions.action: ERROR iptables -N fail2ban-ProFTPD  
iptables -A fail2ban-ProFTPD -j RETURN  
iptables -I INPUT -p tcp --dport ftp -j fail2ban-ProFTPD returned 200[/linux]
```

Voici une solution toute simple pour palier au fait que le multi cores carbure à l'hélium :)

Dans un premier temps, j'ai incriminé Fail2ban qui n'était pas dans sa dernière mouture publique, mais en 0.8.3.

Me voilà donc avec un joli

```
[linux]aptitude remove --purge fail2ban [/linux]
```

Par acquis de conscience je vais toujours vérifier si tout à bien dégagé, et comme souvent ce n'est pas le cas, donc un petit delete du folder /etc/fail2ban/ s'impose !

On est OK, me voilà installer Fail2ban 0.8.4 direct à partir des sources me disant, tu vas voir ...

Je relance ce foutu Fail2ban pour me reprendre dans la face le même type de message lol (alors qu'il est précisé sur le site officiel que la version corrige ceci , mais que neni :().

OK, marcel tu me cherches, tu vas me trouver car une machine sans Fail2ban c'est comme une maison sans verrous ...

Solution clef en main pour Debian multi core (au moins 8 coeurs et un processeur)

Le problème ne s'est jamais rencontré sur des machines 4 coeurs monio processeur, ou double processeurs quatre coeurs (du moins pas avec moi ni ceux pour qui je suis intervenu), c'est cette foutue machine double processeurs 2 * 8 coeurs qui semble générer ceci, très probablement que le

16 coeurs carbure de trop pour fail2ban :)

Pour faire simple, j'ouvre le fichier /etc/fail2ban/action.d/iptables.conf

et j'ajoute la ligne suivante `time sleep ${RANDOM:0:1}` comme suit

```
[linux]# Option: actionstart
# Notes.: command executed once at the start of Fail2Ban.
# Values: CMD
#
actionstart = time sleep ${RANDOM:0:1}
iptables -N fail2ban-
iptables -A fail2ban- -j RETURN
iptables -I INPUT -p --dport -j fail2ban-

# Option: actionstop
# Notes.: command executed once at the end of Fail2Ban
# Values: CMD
#
actionstop = time sleep ${RANDOM:0:1}
iptables -D INPUT -p --dport -j fail2ban-
iptables -F fail2ban-
iptables -X fail2ban-[/linux]
```

Vous remarquerez que j'ai donc ajouter cette fameuse ligne dans `actionstart` et `actionstop`

J'ai pu trouver plusieurs types de solutions en googlant mais aucune ne fonctionnait réellement sous Debian, avec celle ci no problem !

Fail2bban relancé, plus de messages d'erreur , un petit test simpose de lui même en tentant un accès ftp avec un compte inexsitant et paf dégagé, un second pour le fun sur un accès ssh avec un mauvais mot de passe, et paf dans la face ...

Bref fail2ban semble ne pas aimer les machines trop puissantes :(, mais avec ce petit sleep (et non petit slip), il repart comme en 40 ... et il est ainsi possible de lancer autant de jails que désiré

Billet issu du site internet Cyril Levert, my blog:

<http://www.cyril-levert.info>

URL du billet

http://www.cyril-levert.info/blog_comment_stopper_les_plantages_de_fail2ban_sur_un_serveur_multicores_plus_de_8_coeurs-101.html