

Fail2ban et Apache - Bannir les scans d'url d'administration (antibot)



Testé sur Debian 8

Si on analyse les logs apache, on remarque beaucoup de bots qui scannent les URL potentiellement associées à des outils d'administration.

Faire l'analyse des 404 dans vos logs apache avec un outil comme [GoAccess](#) permettra de voir la liste des URL que vous devriez bannir avec fail2ban.

Installer fail2ban

Commencer par installer le package fail2ban

```
apt install fail2ban
```

Configuration

Créer le fichier `/etc/fail2ban/jail.local` avec ce contenu :

```
[apache-antibot]
enabled = true
filter = apache-antibot
port = http,https
#Fichier ou dossier de logs à surveiller
logpath = /home/www-data/logs/apache2/*.log
# Nombre de match dans les logs avant de bannir
maxretry = 2
# Période max surveillée
findtime = 432000
# Ban de 10 jours
bantime = 864000
#Décommenter pour envoyer un email en cas de ban
#mta = mail
#destemail = user@email.com
#action = %(action_mw)s
```

Adapter la ligne `logpath` à vos fichiers de logs.

Je recommande de passer `bantime` à 60 (secondes) pour vos tests. `maxretry` est le nombre de correspondances avant de déclencher le ban. `findtime` est la période à analyser dans les fichiers de

log.

Créer le fichier `/etc/fail2ban/filter.d/apache-antibot.conf` avec ce contenu :

```
#Modifier 'badurls' selon votre besoin
[Definition]
badurls =
phpmyadmin|myadmin|mysql|phpadmin|sql|msd|mysqldumper|sqlite|sqlitemanager|w
ebdb|soapCaller|manager|setup\.php|pma|status|jmx-console|HNAP1

failregex = ^(?i)<HOST> .* "(GET|POST|HEAD) .*(%(badurls)s).* HTTP.*"
(403|404) .*$
            ^(?i)<HOST> .* "(GET|POST|HEAD) / HTTP.*" (403|404) .*$

ignoreregex =
```

Adapter la ligne `badurls` pour les chemins sur lesquels vous voulez provoquer un ban par iptables.

Activation de votre jail

Activation

```
fail2ban-client start apache-antibot
```

Vérification des jails actives

```
fail2ban-client status
```

Vous pouvez aussi ajouter une IP aux exceptions (utile pour vos tests)

```
fail2ban-client set apache-antibot addignoreip <IP>
```

Pour l'enlever :

```
fail2ban-client set apache-antibot delignoreip <IP>
```

Redémarrage de fail2ban au besoin :

```
service fail2ban restart
```

En cas de ban intempestif de votre IP, vous pouvez vous débannir :

```
fail2ban-client set YOURJAILNAMEHERE unbanip IPADDRESSHERE
```

Pour voir les ip en ban actuellement :

```
iptables -L
```

Rapport dans un fichier

Le script suivant permet de créer un fichier listant les IP bannies et le pays associé.

```
#!/bin/bash

fail2ban-client status apache-antibot | grep 'IP list' | sed -n
's/\([0-9]\{1,3\}\.\)\{3\}[0-9]\{1,3\}/\nip&\n/gp' | grep ip | sed 's/ip//' |
sort | uniq > /dev/shm/f2b.txt
fail2ban-client status apache-antibot | grep 'IP list' | sed -n
's/\([0-9]\{1,3\}\.\)\{3\}[0-9]\{1,3\}/\nip&\n/gp' | grep ip | sed 's/ip//' |
sort | uniq | xargs -n 1 geoiplookup { } | sed -e 's/GeoIP Country Edition:
//g' > /dev/shm/f2bgeo.txt
paste /dev/shm/f2b.txt /dev/shm/f2bgeo.txt > /home/www-data/domain.info/f2b-
bans.html
sed -i 's$/<br \>\n/g' /home/www-data/domain.info/f2b-bans.html
```

Remarques



Attention si les fichiers de logs analysés sont affectés par logrotate. Ne pas ajouter compress et delay compress. fail2ban ne sais pas lire les fichier compressés par défaut.

[Source 1](#) - [Source 2](#)

From:

<https://wiki.dureuil.info/> - **GD-WIKI**

Permanent link:

<https://wiki.dureuil.info/doku.php/linux:fail2ban-apache-antibot?rev=1465590948>

Last update: **2020/07/24 22:03**

