Mise en place & configuration de Fail2Ban

Installation

```
sudo apt-get install fail2ban
```

Configuration

Le fichier `/etc/fail2ban/jail.conf` contient l'ensemble des plugins que vous pouvez activer pour protéger les services de votre serveur. Pour chaque plugin les actions possibles sont commentées dans le fichier.

Mais vous ne devez pas modifier ce fichier directement. Car lors des mises à jour de votre serveur Debian, le fichier peut être remplacé à tout moment avec une version plus récente.

En fait, Fail2ban charge les configurations dans cet ordre :

- /etc/fail2ban/jail.conf
- puis /etc/fail2ban/jail.d/defaults-debian.conf
- et enfin /etc/fail2ban/jail.local **(le notre)**

On crée donc notre fichier de config perso :

```
sudo nano /etc/fail2ban/jail.local
```

Voici un exemple de configuration standard :

```
[DEFAULT]
# 1 jour de bannissement pour tous les plugins
bantime = 86400

# A host is banned if it has generated "maxretry" during the last "findtime" in seconds.
```

```
findtime  = 600
ignoreip = 127.0.0.1/8 123.456.789.123

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

[sshd]
enabled = true
# 3 mots de passe erronés consécutifs et c'est le bannissement direct en SSH
maxretry = 3
```

Activation du service

```
sudo service fail2ban start
```

Pour vérifier le bon fonctionnement du service :

```
sudo service fail2ban status
```

Il est possible que sous certaine distribution fail2ban ne démarre pas avec cette configuration. Il faudra rajouter la ligne suivante dans le fichier `jail.local` dans la partie `[DEFAULT]` :

```
sshd_backend = systemd
```

puis redémarrer fail2ban.

Revision #2
Created 2022-06-30 11:26:52 UTC by gpatruno
Updated 2025-06-27 13:49:29 UTC by gpatruno