Installation de Fail2ban

MELNOTTE Hugo
BTS SIO

Installation de fail2ban

Tout d'abord il faut installer fail2ban
Puis le lancer
systemctl start fail2ban

Et enfin contrôler la bonne installation

systemctl enable fail2ban

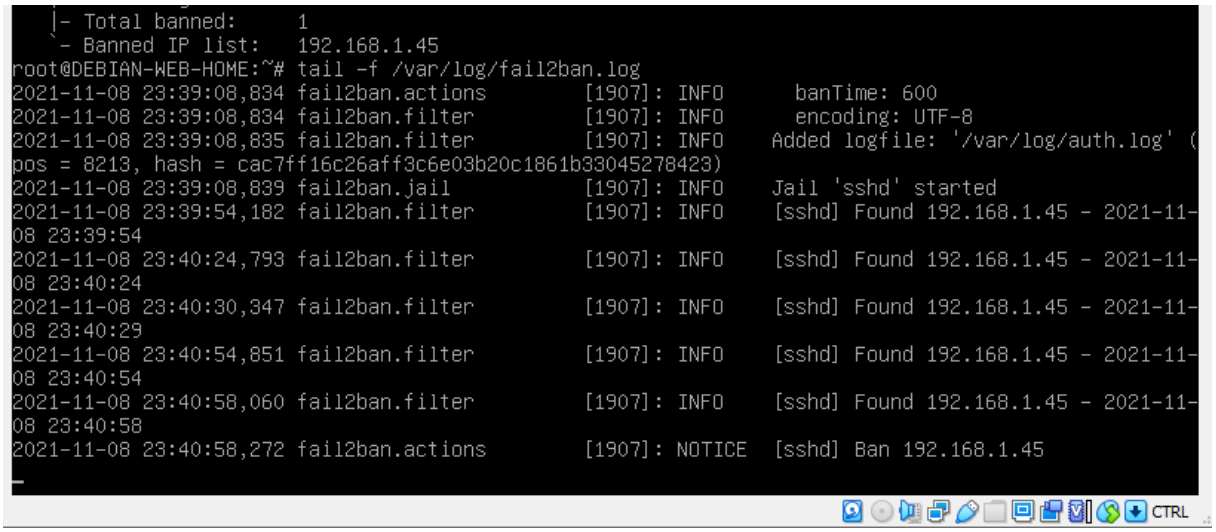
```
root@DEBIAN-WEB-HOME:~# systemctl start fail2ban
root@DEBIAN-WEB-HOME:~# systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd
/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
root@DEBIAN-WEB-HOME:~# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset>
     Active: active (running) since Mon 2021-11-08 23:18:46 CET; 8min ago
       Docs: man:fail2ban(1)
   Main PID: 462 (fail2ban-server)
      Tasks: 5 (limit: 1133)
     Memory: 24.4M
        CPU: 979ms
     CGroup: /system.slice/fail2ban.service
             └─462 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

nov. 08 23:18:46 DEBIAN-WEB-HOME systemd[1]: Starting Fail2Ban Service...
nov. 08 23:18:46 DEBIAN-WEB-HOME systemd[1]: Started Fail2Ban Service.
nov. 08 23:18:50 DEBIAN-WEB-HOME fail2ban-server[462]: Server ready
lines 1-14/14 (END)
```

Si la réponse comporte du vert et les mots "active (running)" sur la ligne commençant par "Active :",
le service est actif.
Nous pouvons voir les tentatives de connexion avec
sudo fail2ban-client status sshd

```
root@DEBIAN-WEB-HOME:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     5
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.45
root@DEBIAN-WEB-HOME:~# _
```

Nous pouvons également voir les logs avec
tail -f /var/log/fail2ban.log



On peut modifier les options dans le répertoire /etc/fail2ban/jail.conf

nano /etc/fail2ban/jail.conf

```
[DEFAULT]
bantime = 0,008h

[sshd]
enabled = true

See jail.conf(5) man page for more information
```

J'ai réglé le ban sur environ 30 secondes pour l'exemple.

Source

https://doc.ubuntu-fr.org/fail2ban