# Commandes Fail2Ban

## Liste des commandes utiles pour Fail2Ban

### Logs Fail2Ban

Pour savoir si fail2ban fonctionne on peut allez voir le fichier de logs :

```
sudo nano /var/log/fail2ban.log
```

### Lister les prisons

```
sudo fail2ban-client status
```

### Lister les bannis d'une prison

```
sudo fail2ban-client status <JAILNAME>
```

Mettre la sortie de la commande dans un fichier :

```
sudo fail2ban-client status <JAILNAME> > <FILENAME>

# Exemple
sudo fail2ban-client status sshd > ipban.txt
```

Filtrer les ip dans un fichier :

```
grep -n -w --color "<KEYWORD>" <FILENAME>

# Exemple
grep -n -w --color "192" ipban.list
```

Il est aussi possible de faire les 2 manipulations précédentes en une seule fois :

```
sudo fail2ban-client status <JAILNAME> | grep -n -w --color "<KEYWORD>"

# Exemple rechercher une chaine de caractère commençant par "192"
sudo fail2ban-client status sshd | grep -n -w --color "192"
```

Avec grep il est possible de faire des recherches avancés que ça soit dans le traitement d'une sortie de commande ou dans un fichier :

```
# Recherche REGEX avec grep
# Il est important de rajouter l'option -E pour signaler que c'est une recherche regex

# Exemple rechercher une chaine de caractère au format IPV4 -> "XX.XX.XX.XX"
grep -n -w --color -E "([0-9]{1,3}[\.]){3}[0-9]{1,3}" <FILENAME>

# Exemple rechercher une chaine de caractère au format IPV4 commençant par 192 ->
"192.XX.XX.XX"
sudo fail2ban-client status sshd | grep -n -w --color -E "192([\.][0-9]{1,3}[0-9]){3}"
```

# Dé bannir une IP

```
sudo fail2ban-client set <JAILNAME> unbanip <IPBAN>
```

---

Revision #7
Created 11 July 2022 09:24:44 by gpatruno
Updated 9 February 2023 12:21:26 by gpatruno