Fail2ban

fail2ban est une application qui analyse les logs de divers services (SSH, Apache, FTP…) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs.

1. Installation

Installation des paquets nécessaires au fonctionnement de Fail2ban :

```
# apt install fail2ban iptables -y
```

2. Configuration

Configuration de fail2ban :

/etc/fail2ban/jail.conf

```
# Réseau qui ne sera pas pris en compte par Fail2ban
ignoreip = <Réseau1> <Réseau2>

# Temps pendant lequel l'hôte sera banni
bantime = <TempsEnSecondes>
findtime = <TempsEnSecondes>

# Tentatives maximales
maxretry = <1-9999>

# Activation de Fail2ban pour SSH
[sshd]
enabled = true
```

3. Commandes utile

Lister toutes les commandes du Client

```
fail2ban-client -h
```

Afficher l'état du serveur

```
fail2ban-client status
```

Vérification du statut de SSHD

```
fail2ban-client status sshd
```

Bannir une IP

```
fail2ban-client set sshd banip <IP>
```

Débannir une IP

```
fail2ban-client set sshd unbanip <IP>
```

Visualisation des logs

```
tail -f /var/log/syslog
tail -f /var/log/fail2ban.log
```

Redémarrer le service Fail2ban

```
systemctl restart fail2ban.service
```