Installation

Installation générique (Debian/Ubuntu)

```
sudo apt update
sudo apt install fail2ban -y
```

Vérifier que le service est actif :

```
sudo systemctl status fail2ban
sudo systemctl enable --now fail2ban
```

Installation sur AlmaLinux/RHEL

```
sudo dnf install epel-release -y
sudo dnf install fail2ban fail2ban-systemd -y
```

```
sudo systemctl enable --now fail2ban
```

Bascule iptables-legacy (requis sur AlmaLinux)

Sur AlmaLinux, le mode `nftables` par défaut pose des soucis de compatibilité avec certaines actions fail2ban orientées iptables. Bascule en mode legacy :

```
sudo dnf install iptables-services -y
sudo alternatives --set iptables /usr/sbin/iptables-legacy
sudo alternatives --set ip6tables /usr/sbin/ip6tables-legacy
sudo systemctl enable --now iptables
sudo systemctl restart fail2ban
```

Vérifier la bascule :

```
sudo alternatives --display iptables
```

Arborescence de configuration

Fail2ban utilise deux types de fichiers, à ne **jamais** modifier dans `/etc/fail2ban/jail.conf` ou `/etc/fail2ban/filter.d/*.conf` (écrasés lors des mises à jour). Toujours passer par les fichiers `.local` :

```
/etc/fail2ban/
├── jail.conf          # NE PAS MODIFIER (fichier par défaut)
├── jail.local          # Config globale perso (créé manuellement)
├── jail.d/
│   └── rakouns-*.conf  # Une jail par service, convention Rakouns
├── filter.d/
│   ├── *.conf          # Filtres fournis par défaut
│   └── rakouns-*.conf  # Filtres personnalisés
└── action.d/
    ├── *.conf
    └── iptables-docker.conf  # Action custom pour cibler DOCKER-USER
```

Créer la config globale de base si elle n'existe pas :

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

Exemple de socle dans `jail.local` (valeurs par défaut appliquées à toutes les jails, sauf surcharge) :

```
[DEFAULT]
bantime  = 1h
findtime = 10m
maxretry = 5
backend  = auto
ignoreip = 127.0.0.1/8 192.168.1.0/24
```

> **Note —** ignoreip doit inclure ton réseau local pour éviter de te bannir toi-même pendant les tests.

Cas Docker : l'action iptables-docker

Comme évoqué en page 1, le ban standard via la chaîne `INPUT` n'a aucun effet sur le trafic redirigé vers des conteneurs Docker, car Docker insère ses propres règles dans la chaîne `DOCKER-USER` avant que la chaîne `INPUT` ne soit évaluée.

Créer `/etc/fail2ban/action.d/iptables-docker.conf` :

```
[Definition]
actionstart = iptables -N f2b-<name>
              iptables -A f2b-<name> -j RETURN
              iptables -I DOCKER-USER -j f2b-<name>

actionstop = iptables -D DOCKER-USER -j f2b-<name>
             iptables -F f2b-<name>
             iptables -X f2b-<name>

actioncheck = iptables -n -L DOCKER-USER | grep -q 'f2b-<name>[ \t]'

actionban = iptables -I f2b-<name> 1 -s <ip> -j DROP

actionunban = iptables -D f2b-<name> -s <ip> -j DROP
```

```
[Init]
name = default
```

Cette action sera référencée dans chaque jail concernée (voir Page 4).

Vérification rapide de l'installation

```
sudo fail2ban-client status
sudo fail2ban-client version
```

Revision #1
Created 2026-06-20 11:41:55 UTC by clement-derouet
Updated 2026-06-20 11:47:28 UTC by clement-derouet