Jail



Principe

La jail relie un filter à :

- une source de log (logpath ou backend pour Docker),
- des seuils (maxretry, findtime, bantime),
- une action (action, par défaut iptables classique, ou iptables-docker pour les conteneurs).

Convention Rakouns : un fichier par jail dans /etc/fail2ban/jail.d/, nommé rakouns-<service>.conf.

Structure générale d'une jail

```
[rakouns-<service>]
enabled  = true
filter   = rakouns-<service>
logpath  = <chemin ou source du log>
backend  = polling          ; obligatoire pour les logs Docker json-file
maxretry = 5
findtime = 10m
bantime  = 1h
```

```
action   = iptables-docker[name=<service>]
```

> **Note —** backend = polling est requis pour tout service conteneurisé dont les logs sont au format json-file : le backend auto/systemd ne détecte pas les nouvelles lignes correctement dans ce format.

Exemple générique : jail SSH

```
[sshd]
enabled  = true
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 5
findtime = 10m
bantime  = 1h
```

C'est le cas le plus simple : pas de Docker, pas d'action custom, le ban standard sur la chaîne INPUT suffit.

Fil rouge : jail Vaultwarden

Créer /etc/fail2ban/jail.d/rakouns-vaultwarden.conf :

```
[rakouns-vaultwarden]
enabled  = true
filter   = rakouns-vaultwarden
logpath  = /var/lib/docker/containers/<container_id>/<container_id>-json.log
backend  = polling
maxretry = 5
findtime = 10m
bantime  = 24h
action   = iptables-docker[name=vaultwarden]
```

Points clés :

- backend = polling → indispensable, sinon la jail reste en 0 currently failed même en cas d'attaque réelle.
- action = iptables-docker[name=vaultwarden] → utilise l'action custom créée en Page 2, qui cible DOCKER-USER avec une chaîne dédiée f2b-vaultwarden.
- bantime = 24h plus long que la valeur par défaut, car Vaultwarden contient des coffres de mots de passe : la tolérance au brute-force doit être minimale.

> **Note —** Le container_id change si le conteneur est recréé (mise à jour d'image, docker compose up -d --force-recreate). Un script de détection automatique du chemin de log peut éviter d'avoir à mettre à jour la jail manuellement à chaque recréation.

Jail recidive

Recommandé en complément de toutes les jails de service : bannit plus longtemps une IP déjà bannie plusieurs fois.

```
[recidive]
enabled  = true
filter   = recidive
logpath  = /var/log/fail2ban.log
banaction = iptables-allports
bantime  = 1w
findtime = 1d
maxretry = 3
```

Recharger et activer une jail

```
sudo fail2ban-client reload
# ou, pour recharger une jail spécifique sans tout relancer :
sudo fail2ban-client reload rakouns-vaultwarden
```

Vérifier qu'elle est bien prise en compte :

```
sudo fail2ban-client status
Status

|- Number of jail:      3
```

```
`- Jail list:   sshd, recidive, rakouns-vaultwarden
```

Puis le détail d'une jail précise :

```
sudo fail2ban-client status rakouns-vaultwarden
Status for the jail: rakouns-vaultwarden
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/lib/docker/containers/.../....log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

Revision #1
Created 2026-06-20 11:59:26 UTC by clement-derouet
Updated 2026-06-20 12:14:46 UTC by clement-derouet