# Présentation




# Qu'est ce que Fail2Ban ?

Fail2Ban est un outil de protection qui analyse les logs des services exposés (SSH, applications web, reverse proxy, etc.) et bannit automatiquement les adresses IP qui présentent un comportement suspect : tentatives de connexion échouées répétées, scan d'endpoints, brute-force, etc.

Concrètement, Fail2Ban fonctionne en trois briques :

| Brique | Rôle |
|---|---|
| Filter | Une expression régulière qui repère une ligne de log correspondant à une tentative échouée |
| Jail | La configuration qui associe un filter à un service, une durée de ban, un nombre d'essais max, et une action |
| Action | Ce qui se passe quand le seuil est dépassé (le plus souvent : bannir l'IP via le pare-feu) |

Le flux est donc : **log → filter (regex) → jail (seuils) → action (ban pare-feu).**

Sur une infra exposée sur Internet (Rakouns), chaque service accessible publiquement (Vaultwarden, Emby, Matrix, NPM, etc.) est une cible potentielle de scan automatisé et de brute-force. Sans fail2ban :

- Les logs d'authentification se remplissent de tentatives parasites.
- Les services restent exposés à du brute-force lent et discret (peu de requêtes par minute, sous le radar d'un rate-limiting applicatif).
- Aucune réponse automatique n'existe en cas d'attaque ciblée.

# Spécificités de l'infra Rakouns

Sur l'infra Rakouns, la quasi-totalité des services tournent en conteneurs Docker derrière NPM (Nginx Proxy Manager) comme reverse proxy. Cela introduit deux contraintes particulières :

1. **Le ban classique d'iptables ne suffit pas avec Docker.** Docker manipule ses propres règles iptables et les insère avant les règles fail2ban standards (chaîne INPUT). Il faut donc cibler explicitement la chaîne DOCKER-USER, via une action personnalisée (iptables-docker), pour qu'un ban soit réellement effectif sur le trafic redirigé vers les conteneurs.
2. Le format des logs Docker (json-file**) nécessite le backend polling** dans la configuration jail, car le backend par défaut (auto/systemd) ne lit pas correctement ce format.

Sur le host AlmaLinux (Comms / OVH VPS), une bascule vers iptables-legacy a également été nécessaire pour la compatibilité avec les actions fail2ban, et un contexte SELinux dédié (var_log_t) a dû être appliqué aux chemins de logs Docker pour autoriser leur lecture.

# Convention de nommage Rakouns

Toutes les jails créées sur l'infra Rakouns sont préfixées rakouns- (ex : rakouns-vaultwarden, rakouns-emby, rakouns-npm) afin de les distinguer clairement des jails par défaut fournies avec le paquet (sshd, recidive, etc.).

---

Revision #2
Created 2026-06-20 11:28:41 UTC by clement-derouet
Updated 2026-06-20 11:41:34 UTC by clement-derouet