Fail2ban SSH : installez, configurez et vérifiez votre protection

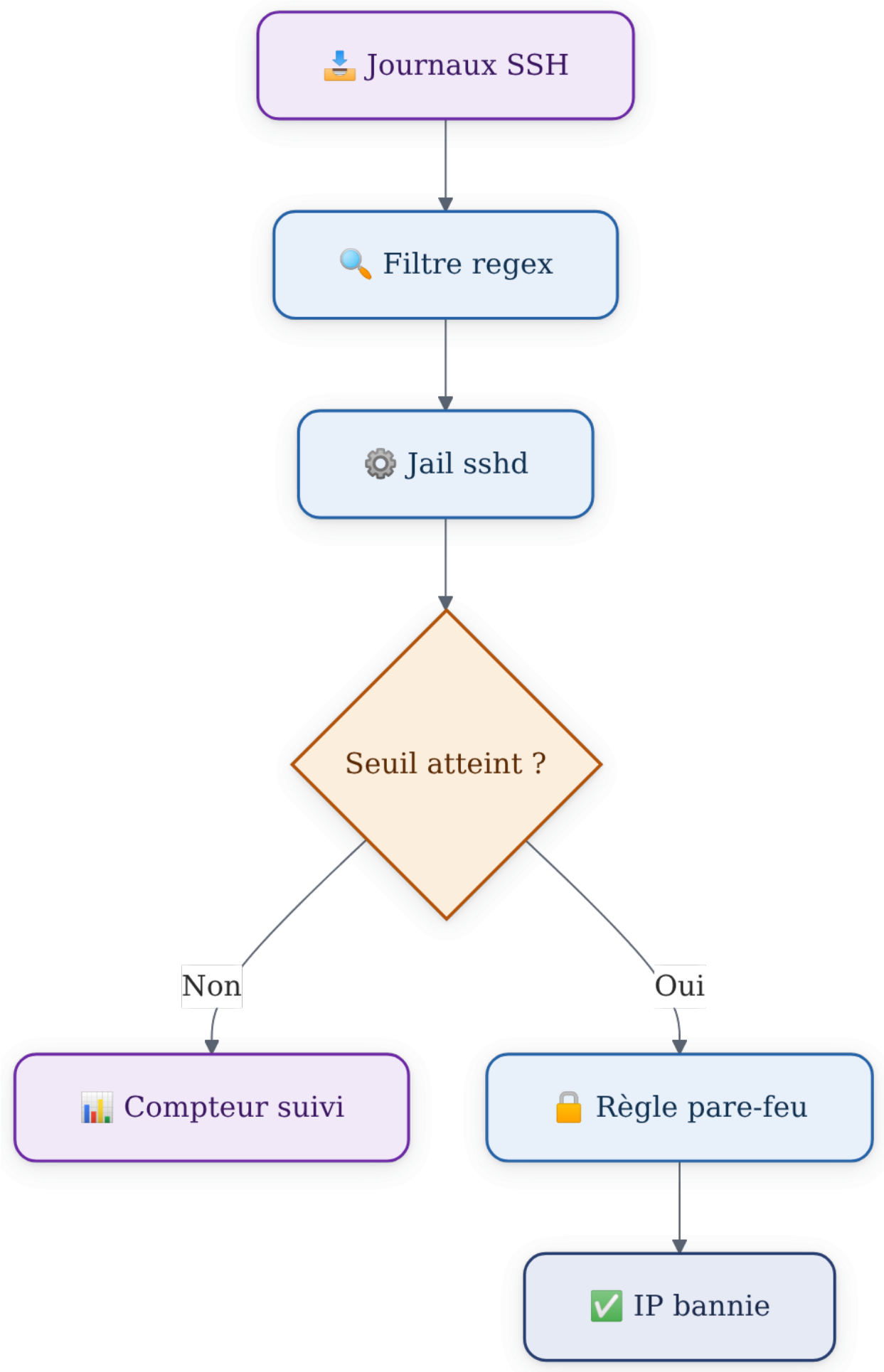
Suivez cette marche à suivre pour déployer Fail2ban sans modifier les fichiers fournis par le paquet ni risquer de bloquer votre propre accès SSH. Gardez ce guide à portée de main lors de votre première configuration.

Au sommaire

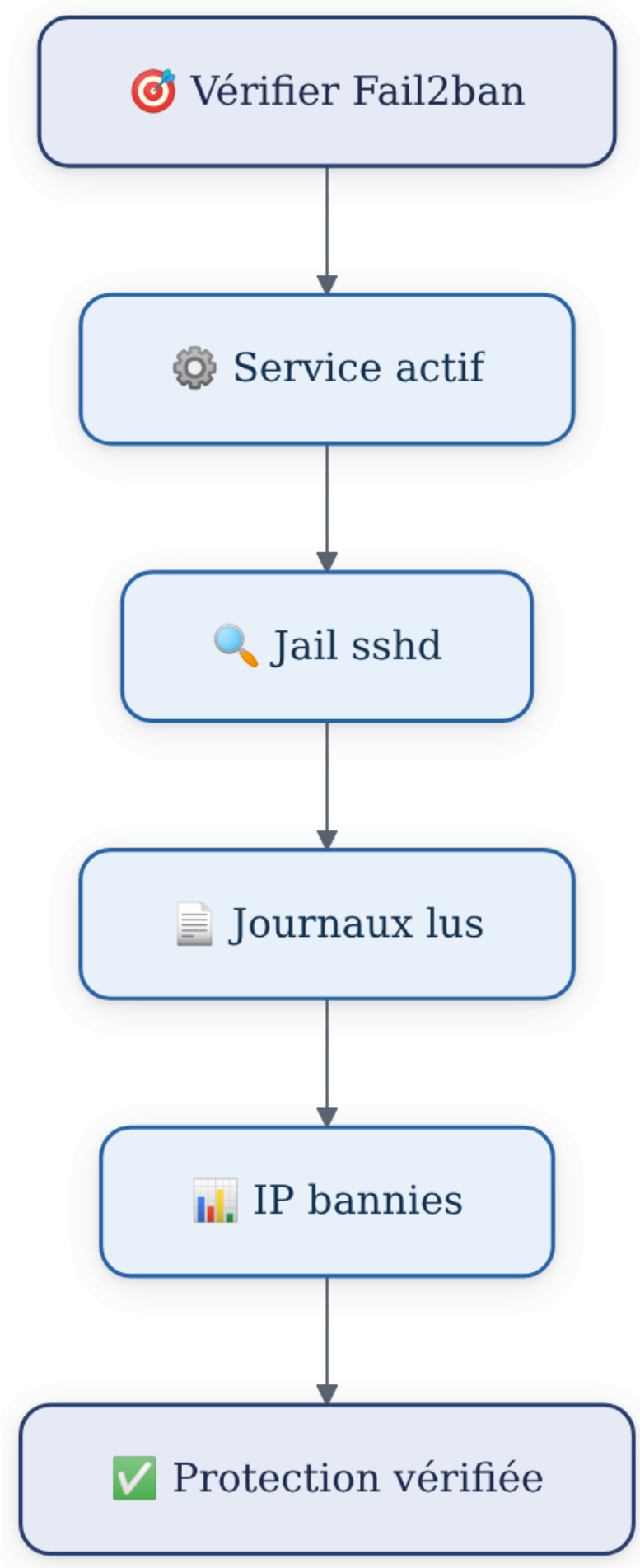
1 Avant de commencer : sécurisez votre accès
2 1. Installer et démarrer Fail2ban
3 2. Créer une jail SSH locale
4 Repères pour relire votre configuration
5 3. Vérifier le service, la jail et les bannissements
6 À retenir : Fail2ban complète votre sécurité SSH

Avant de commencer : sécurisez votre accès

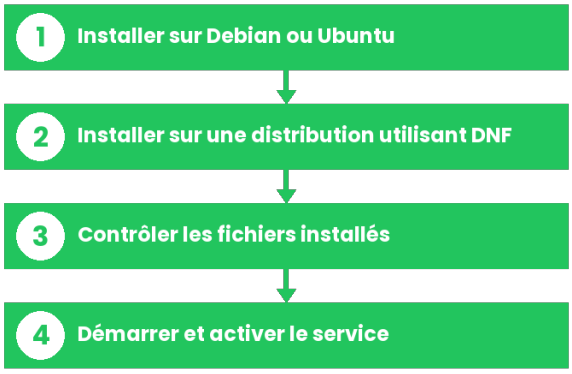
- [ ] **Vérifier que votre connexion SSH d'administration fonctionne.**
- [ ] **Ouvrir une seconde session SSH avant toute modification.**
  Elle permet de corriger rapidement une erreur de configuration.
- [ ] **Identifier votre adresse IP publique ou votre sous-réseau d'administration.**
- [ ] **Prévoir un accès de secours.**
  Par exemple, une console fournie par l'hébergeur.
- [ ] **Vérifier que le service SSH enregistre les échecs d'authentification dans les journaux.**
- [ ] **Confirmer la présence d'un pare-feu compatible avec l'action de bannissement choisie.**


📥 Journaux SSH
🔍 Filtre regex
⚙️ Jail sshd
Seuil atteint ?
Non
Oui
📊 Compteur suivi
🔒 Règle pare-feu
✅ IP bannie

INFOGRAPHIE *Schéma de configuration Fail2ban SSH avec journaux, filtre, jail et bannissement d'adresse IP*


🎯 Vérifier Fail2ban
⚙️ Service actif
🔍 Jail sshd
📄 Journaux lus
📊 IP bannies
✅ Protection vérifiée

1. Installer et démarrer Fail2ban



1 **Installer sur Debian ou Ubuntu**
Mettez à jour l'index des paquets, puis installez Fail2ban : sudo apt-get update puis sudo apt-get install fail2ban.

2 **Installer sur une distribution utilisant DNF**
Installez le paquet avec : sudo dnf install fail2ban.

3 **Contrôler les fichiers installés**
Vérifiez le répertoire de configuration avec : sudo ls -la /etc/fail2ban.

4 **Démarrer et activer le service**
Exécutez : sudo systemctl start fail2ban, puis sudo systemctl enable fail2ban. Contrôlez enfin son état avec : sudo systemctl status fail2ban.

! **Ne modifiez pas jail.conf**
Conservez jail.conf comme fichier de référence fourni par le paquet. Placez vos réglages personnalisés dans /etc/fail2ban/jail.local afin qu'ils restent distincts des fichiers distribués et plus simples à maintenir lors des mises à jour.

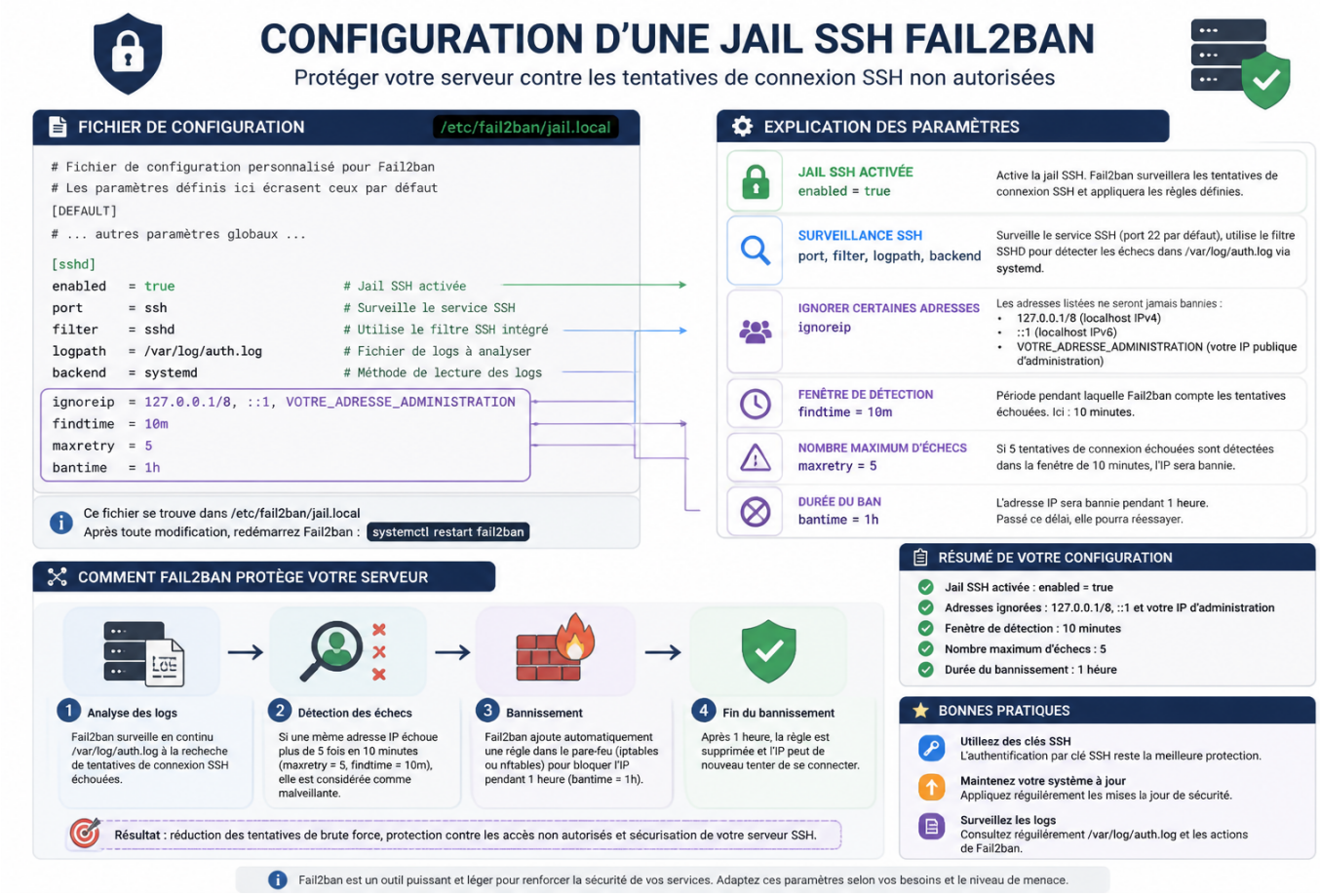
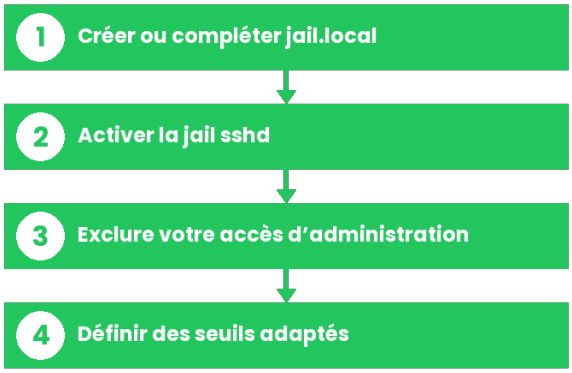


SCHÉMA *Les paramètres essentiels d'une jail SSH locale : ignoreip, maxretry et bantime.*

2. Créer une jail SSH locale



1 **Créer ou compléter jail.local**
Configurez la protection SSH dans /etc/fail2ban/jail.local plutôt que dans le fichier de configuration fourni par le paquet.

2 **Activer la jail sshd**
La jail sshd surveille les échecs de connexion SSH et associe cette surveillance à une action de bannissement via le pare-feu.

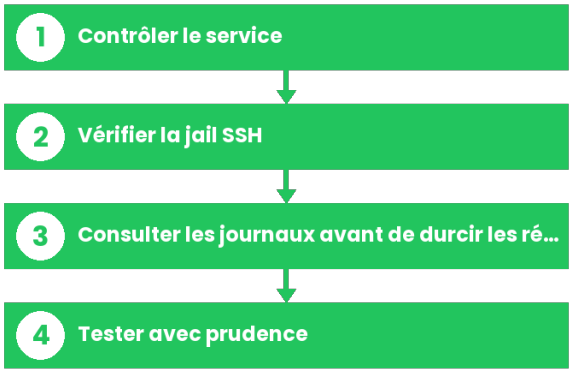
3 **Exclure votre accès d'administration**
Ajoutez uniquement votre adresse IP publique ou un réseau réellement maîtrisé dans ignoreip, avant d'appliquer des seuils stricts.

4 **Définir des seuils adaptés**
Réglez maxretry pour le nombre d'échecs admis, findtime pour la fenêtre d'observation et bantime pour la durée du bannissement. Ajustez-les selon votre mode réel d'administration.

Repères pour relire votre configuration

Élément	Rôle à contrôler
jail.local	Contient vos réglages locaux personnalisés.
sshd	Jail dédiée à la surveillance des échecs d'authentification SSH.
ignoreip	Adresses ou réseaux d'administration à ne jamais bannir.
maxretry	Nombre d'échecs tolérés avant déclenchement.
findtime	Période pendant laquelle les échecs sont comptabilisés.
bantime	Durée du blocage temporaire appliqué à l'adresse IP.

3. Vérifier le service, la jail et les bannissements



1 **Contrôler le service**
Utilisez systemctl status fail2ban pour confirmer que le service est actif.

2 **Vérifier la jail SSH**
Exécutez fail2ban-client status sshd pour contrôler le statut de la jail et les informations de bannissement associées.

3 **Consulter les journaux avant de durcir les réglages**
En cas de comportement inattendu ou d'échec de démarrage, examinez les journaux plutôt que de modifier les paramètres au hasard.

4 **Tester avec prudence**
Gardez votre seconde session ouverte et validez que votre accès légitime reste possible avant de réduire les seuils.

À retenir : Fail2ban complète votre sécurité SSH

- Fail2ban détecte les échecs répétitifs visibles dans les journaux et applique des blocages temporaires via le pare-feu.
- Les clés publiques SSH pour les comptes d'administration restent une mesure essentielle.
- N'excluez pas de larges plages publiques, de VPN partagé ou de réseau non maîtrisé dans ignoreip.
- Il ralentit les tentatives automatisées, mais ne corrige pas une configuration SSH faible ni une vulnérabilité.
- Maintenez le système et les services exposés à jour, et limitez les ports et services accessibles avec le pare-feu.

Fail2ban est une couche de protection complémentaire : conservez un accès de secours et vérifiez vos journaux avant de rendre les règles de bannissement plus strictes.