

Fail2ban SSH : installez, configurez et vérifiez votre protection

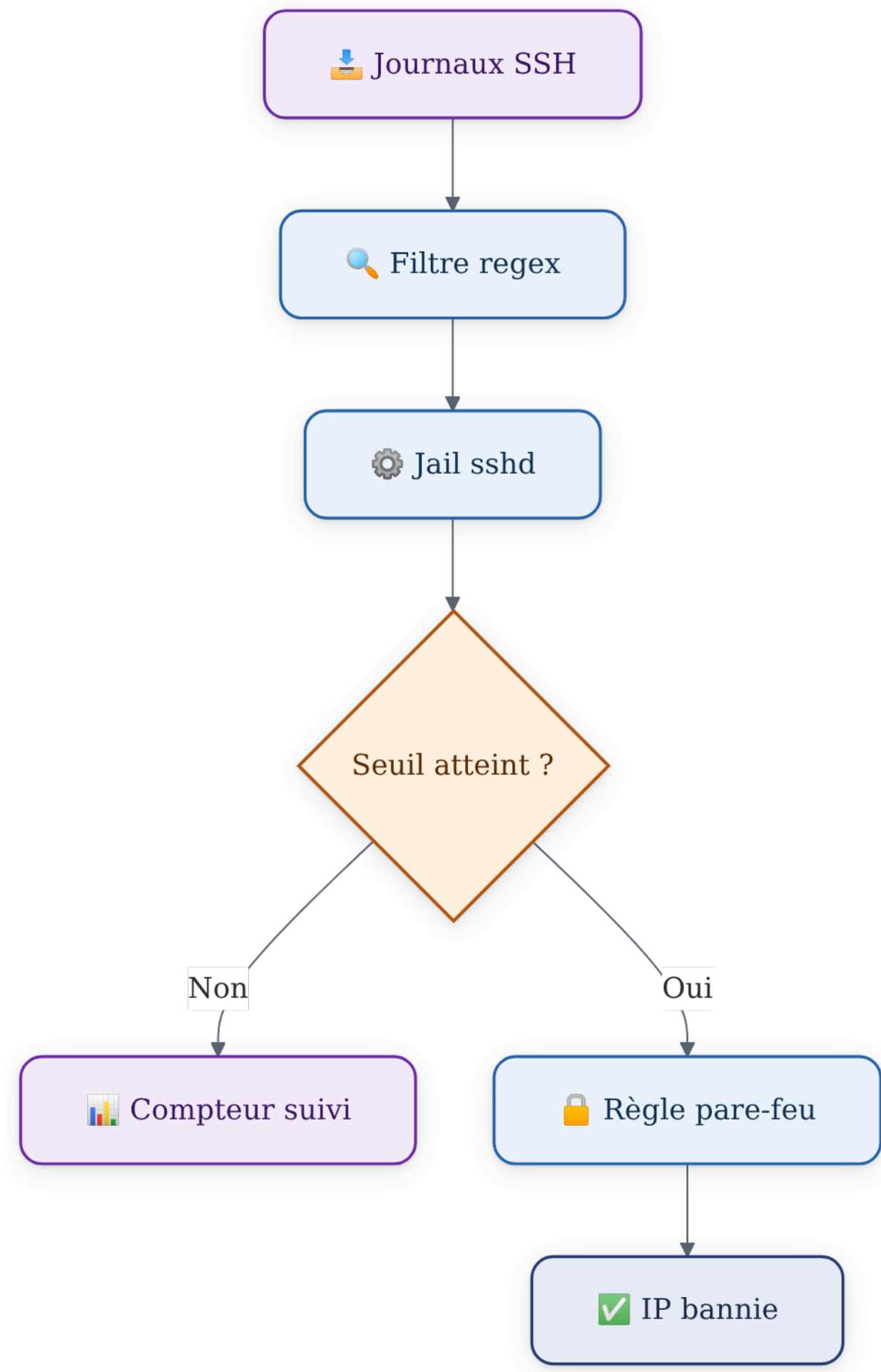
Suivez cette marche à suivre pour déployer Fail2ban sans modifier les fichiers fournis par le paquet ni risquer de bloquer votre propre accès SSH. Gardez ce guide à portée de main lors de votre première configuration.

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.**



 Vérifier Fail2ban

 Service actif

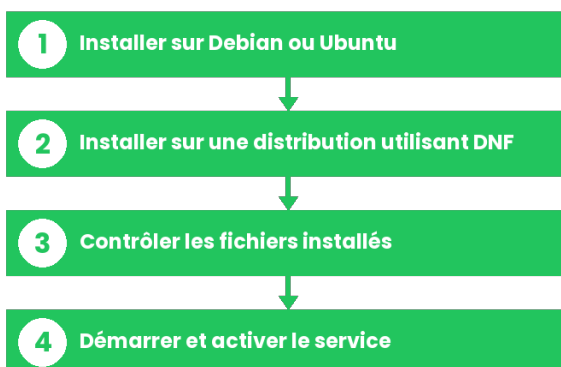
 Jail sshd

 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.



CONFIGURATION D'UNE JAIL SSH FAIL2BAN

Protéger votre serveur contre les tentatives de connexion SSH non autorisées



FICHIER DE CONFIGURATION

`/etc/fail2ban/jail.local`

```
# Fichier de configuration personnalisé pour Fail2ban
# Les paramètres définis ici écrasent ceux par défaut
[DEFAULT]
# ... autres paramètres globaux ...

[sshd]
enabled = true           # Jail SSH activée
port = ssh               # Surveille le service SSH
filter = sshd            # Utilise le filtre SSH intégré
logpath = /var/log/auth.log # Fichier de logs à analyser
backend = systemd        # Méthode de lecture des logs

ignoreip = 127.0.0.1/8, ::1, VOTRE_ADRESSE_ADMINISTRATION
findtime = 10m
maxretry = 5
bantime = 1h
```

Ce fichier se trouve dans `/etc/fail2ban/jail.local`
Après toute modification, redémarrez Fail2ban : `systemctl restart fail2ban`

EXPLICATION DES PARAMÈTRES

	JAIL SSH ACTIVÉE enabled = true	Active la jail SSH. Fail2ban surveillera les tentatives de connexion SSH et appliquera les règles définies.
	SURVEILLANCE SSH port, filter, logpath, backend	Surveille le service SSH (port 22 par défaut), utilise le filtre SSHD pour détecter les échecs dans <code>/var/log/auth.log</code> via <code>systemd</code> .
	IGNORER CERTAINES ADRESSES ignoreip	Les adresses listées ne seront jamais bannies : 127.0.0.1/8 (localhost IPv4) ::1 (localhost IPv6) - VOTRE_ADRESSE_ADMINISTRATION (votre IP publique d'administration)
	FENÊTRE DE DÉTECTION findtime = 10m	Période pendant laquelle Fail2ban compte les tentatives échouées. Ici : 10 minutes.
	NOMBRE MAXIMUM D'ÉCHECS maxretry = 5	Si 5 tentatives de connexion échouées sont détectées dans la fenêtre de 10 minutes, l'IP sera bannie.
	DURÉE DU BAN bantime = 1h	L'adresse IP sera bannie pendant 1 heure. Passé ce délai, elle pourra réessayer.

COMMENT FAIL2BAN PROTÈGE VOTRE SERVEUR

1 Analyse des logs
Fail2ban surveille en continu `/var/log/auth.log` à la recherche de tentatives de connexion SSH échouées.

2 Détection des échecs
Si une même adresse IP échoue plus de 5 fois en 10 minutes (`maxretry = 5`, `findtime = 10m`), elle est considérée comme malveillante.

3 Bannissement
Fail2ban ajoute automatiquement une règle dans le pare-feu (iptables ou nftables) pour bloquer l'IP pendant 1 heure (`bantime = 1h`).

4 Fin du bannissement
Après 1 heure, la règle est supprimée et l'IP peut de nouveau tenter de se connecter.

Résultat : réduction des tentatives de brute force, protection contre les accès non autorisés et sécurisation de votre serveur SSH.

RÉSUMÉ DE VOTRE CONFIGURATION

- ✓ Jail SSH activée : `enabled = true`
- ✓ Adresses ignorées : 127.0.0.1/8, ::1 et votre IP d'administration
- ✓ Fenêtre de détection : 10 minutes
- ✓ Nombre maximum d'échecs : 5
- ✓ Durée du bannissement : 1 heure

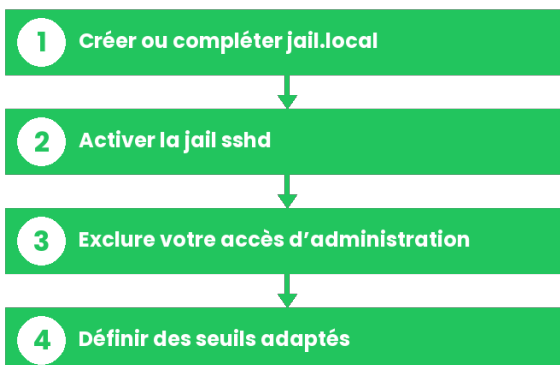
BONNES PRATIQUES

- Utilisez des clés SSH**
L'authentification par clé SSH reste la meilleure protection.
- Maintenez votre système à jour**
Appliquez régulièrement les mises à jour de sécurité.
- Surveillez les logs**
Consultez régulièrement `/var/log/auth.log` et les actions de Fail2ban.

Fail2ban est un outil puissant et léger pour renforcer la sécurité de vos services. Adaptez ces paramètres selon vos besoins et le niveau de menace.

SCHEMA 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.

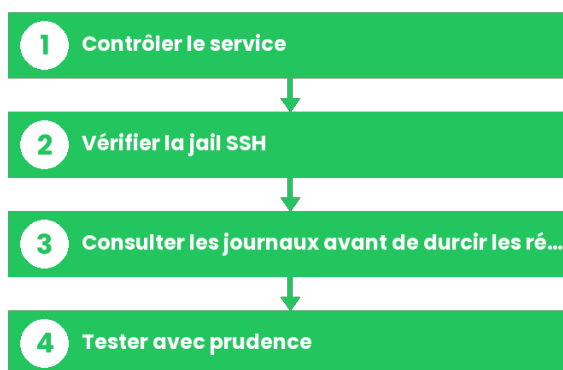
4 Définir des seuils adaptés

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
<code>jail.local</code>	Contient vos réglages locaux personnalisés.
<code>sshd</code>	Jail dédiée à la surveillance des échecs d'authentification SSH.
<code>ignoreip</code>	Adresses ou réseaux d'administration à ne jamais bannir.
<code>maxretry</code>	Nombre d'échecs tolérés avant déclenchement.
<code>findtime</code>	Période pendant laquelle les échecs sont comptabilisés.
<code>bantime</code>	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.