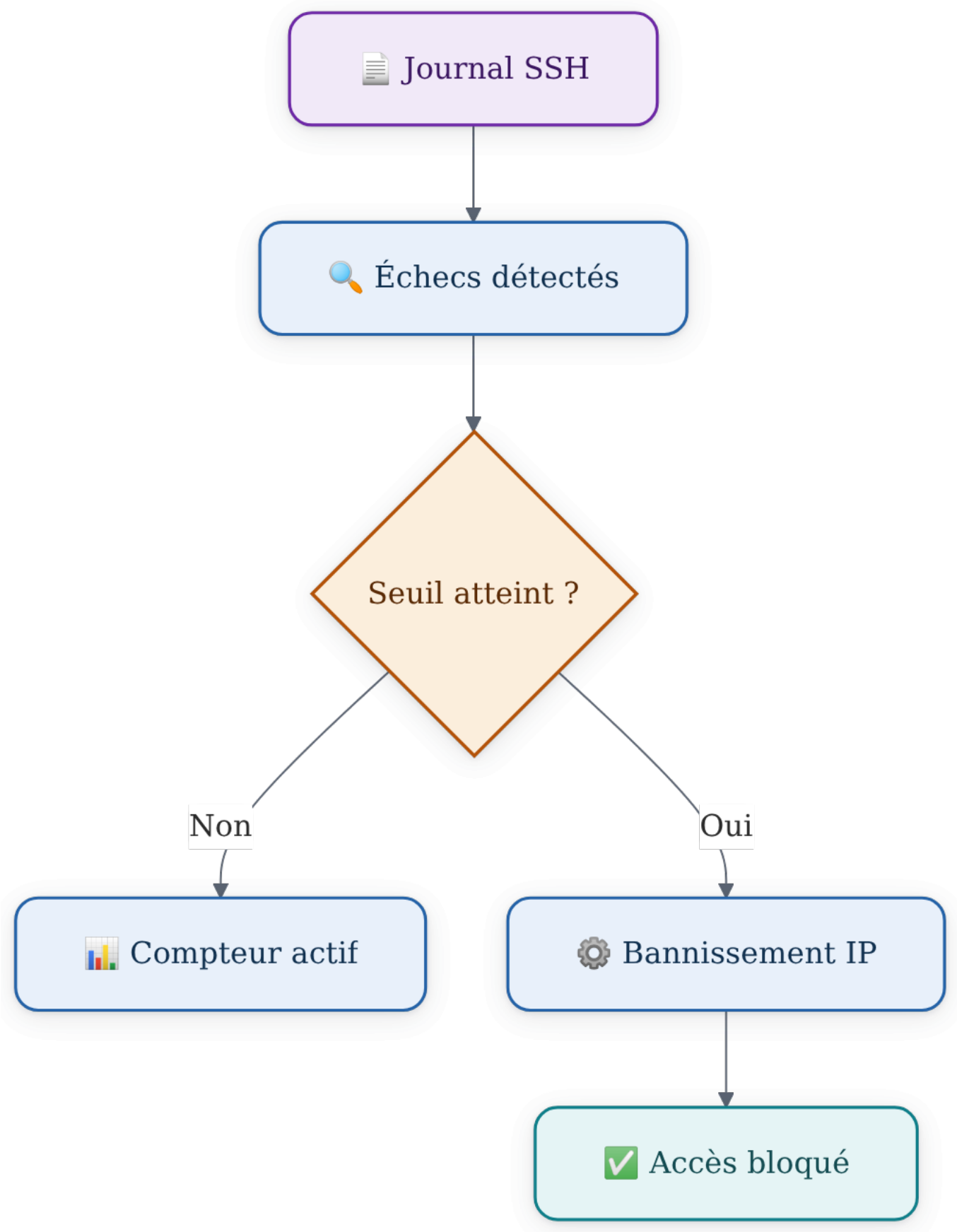
Fail2ban + SSH sur Ubuntu : votre plan de mise en protection

Suivez cette fiche pour installer Fail2ban, activer la prison SSH et contrôler que votre serveur réagit aux tentatives d'authentification répétées. Gardez-la à portée de main pendant la configuration.

Au sommaire

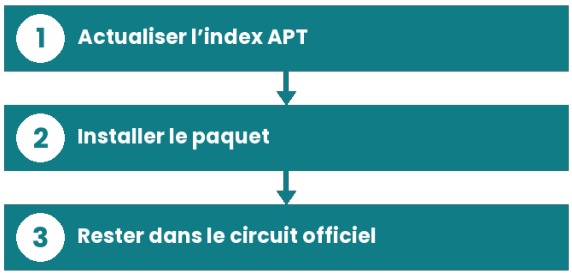
Avant de commencer

- [ ] **Vérifier que SSH fonctionne déjà sur le serveur.**
  Conservez une seconde session SSH ouverte durant toute la configuration.
- [ ] **Utiliser un compte non-root disposant de droits sudo.**
- [ ] **Vérifier l'accès réseau aux dépôts Ubuntu.**
  Commande : sudo -v puis ping -c 3 archive.ubuntu.com
- [ ] **Prévoir un accès de secours.**
  Une console fournie par l'hébergeur ou un accès hors bande aide en cas de bannissement accidentel.
- [ ] **Identifier le port réellement utilisé par SSH.**
  Si UFW est utilisé et que SSH écoute sur le port standard : sudo ufw status | grep 22



INFOGRAPHIE *Schéma Fail2ban Ubuntu montrant la détection des échecs SSH et le bannissement d'adresse IP*

1. Installer Fail2ban depuis Ubuntu

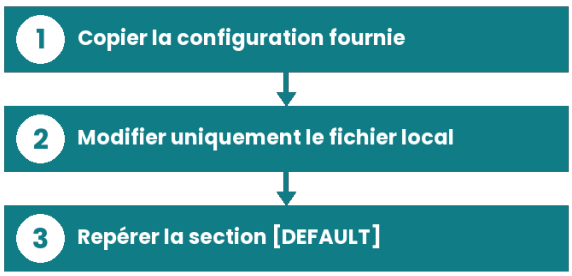


1 **Actualiser l'index APT**
Exécutez sudo apt update et corrigez toute erreur d'accès aux dépôts avant de poursuivre.

2 **Installer le paquet**
Exécutez sudo apt install fail2ban. Les fichiers de configuration sont installés dans /etc/fail2ban.

3 **Rester dans le circuit officiel**
Utilisez le paquet des dépôts Ubuntu plutôt que d'ajouter un dépôt inutile ou de mélanger des configurations prévues pour une autre distribution.

2. Créer une configuration locale durable



1 **Copier la configuration fournie**
Créez votre fichier local avec : sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

2 **Modifier uniquement le fichier local**
Ouvrez-le avec sudo nano /etc/fail2ban/jail.local. Ne modifiez pas jail.conf : ce fichier d'origine peut être remplacé lors d'une mise à jour.

3 **Repérer la section [DEFAULT]**
C'est là que se définissent les réglages généraux de durée, de fenêtre d'observation, de seuil d'échecs et d'exceptions.

Les réglages à comprendre avant de les appliquer

Paramètre	Rôle	Point de vigilance
bantime	Définit la durée du bannissement temporaire.	Choisissez une durée cohérente avec votre contexte d'administration.
findtime	Définit la période pendant laquelle les échecs sont comptés.	Elle fonctionne avec maxretry pour déclencher le bannissement.
maxretry	Définit le nombre maximal d'échecs tolérés.	Un seuil trop bas peut gêner des utilisateurs légitimes.
ignoreip	Exempte certaines adresses IP du bannissement.	N'ajoutez qu'une IP d'administration stable et maîtrisée ; une plage trop large réduit la protection.

Exemple de base pour [DEFAULT]

Dans /etc/fail2ban/jail.local, l'exemple présenté utilise : bantime = 3600m, findtime = 10m, maxretry = 5 et ignoreip = 127.0.0.1/8 ::1 <votre_IP_administration_stable>. Remplacez uniquement le marqueur d'IP par une adresse stable que vous contrôlez, si cette exception est réellement nécessaire.

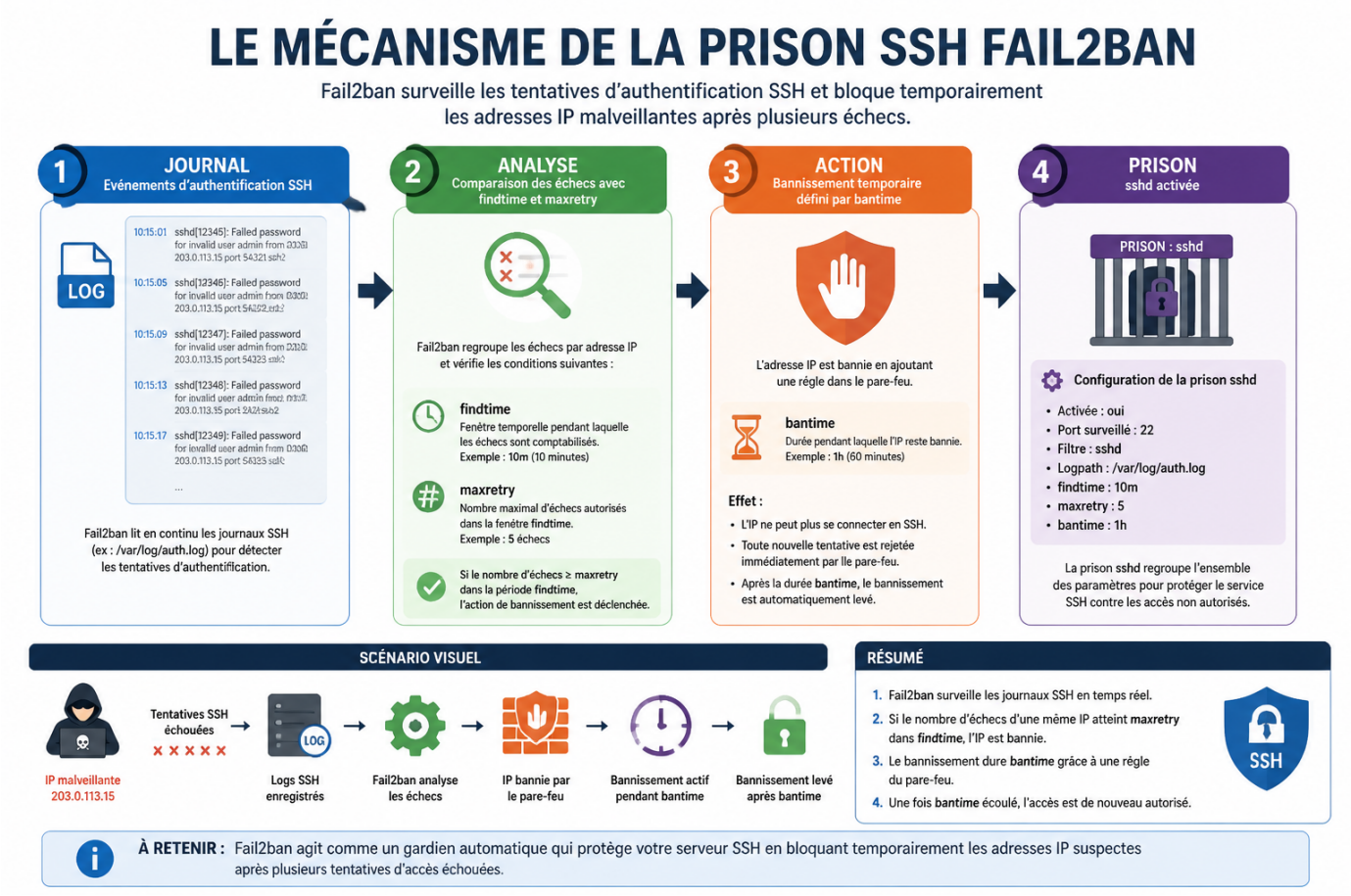


SCHÉMA *La prison sshd surveille les échecs SSH et applique un bannissement temporaire selon les seuils configurés.*

3. Activer et contrôler la protection SSH

- [ ] **Activer la prison sshd dans votre configuration locale.**
  N'activez que les prisons correspondant à des services réellement installés et journalisés.
- [ ] **Adapter le paramètre de port si votre SSH n'utilise pas le port standard.**
  La valeur port = ssh doit correspondre à la configuration réelle du service SSH.

Contrôler l'état de la prison.
Commande : fail2ban-client status sshd

Conserver les autres mesures de sécurité SSH.
Fail2ban limite les tentatives répétées, mais ne remplace ni les mises à jour, ni les clés SSH, ni une politique d'accès rigoureuse.

> ! **Évitez de vous bannir vous-même**
> Ne fermez pas votre session SSH de secours avant d'avoir vérifié votre configuration. L'exception ignoreip est utile pour une adresse stable, mais elle ne doit pas devenir une exemption trop large.

Fail2ban est une couche de protection complémentaire : il réagit aux échecs visibles dans les journaux, sans constituer un pare-feu complet ni une protection absolue.