Ports ouverts Linux : la vérification en 3 contrôles

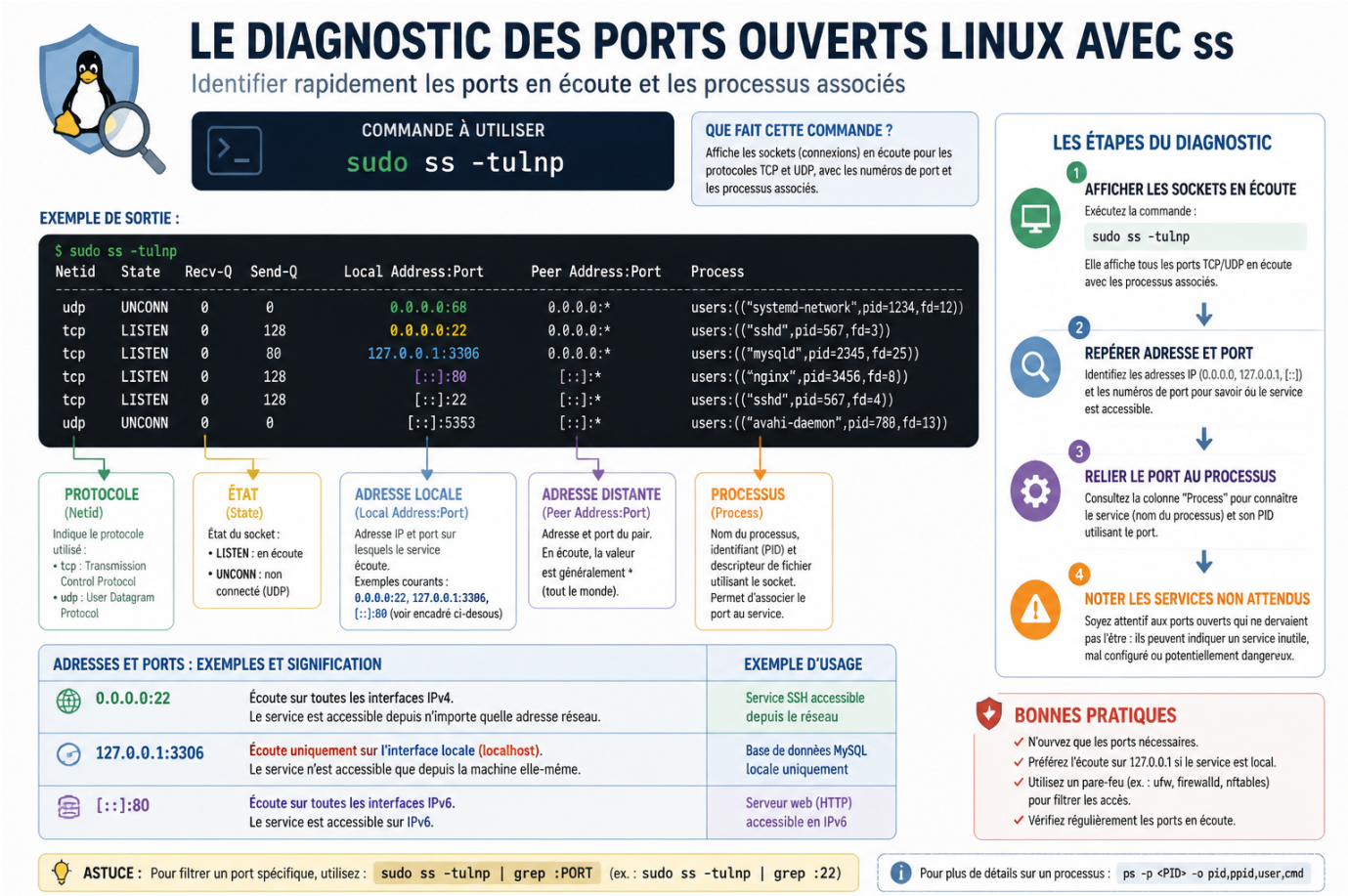
Faites l'inventaire des services en écoute, identifiez leur processus et vérifiez leur exposition réelle. Cette fiche vous aide à distinguer un service attendu d'un port à examiner.

Au sommaire

1. Le bon réflexe : ne pas conclure trop vite
2. Diagnostic express en 3 contrôles
3. Lire une adresse d'écoute
4. Checklist d'analyse de chaque port
5. Commandes à garder sous la main

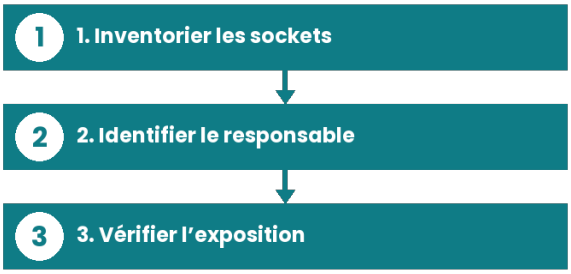
Le bon réflexe : ne pas conclure trop vite

Un port affiché sur la machine indique qu'un service écoute localement. Cela ne prouve pas qu'il est joignable depuis le réseau ou Internet : l'adresse d'écoute, le pare-feu et les règles réseau doivent aussi être contrôlés.



INFOGRAPHIE *Schéma de diagnostic des sockets Linux avec la commande ss -tulnp.*

Diagnostic express en 3 contrôles



1 **1. Inventorier les sockets**
Exécutez sudo ss -tulnp pour afficher les sockets TCP et UDP en écoute, les adresses locales et, si les droits le permettent, les processus associés.

2 **2. Identifier le responsable**
Repérez le nom du programme et son PID dans la sortie. Pour une vérification TCP complémentaire, utilisez sudo lsof -nP -iTCP -sTCP:LISTEN.

3 **3. Vérifier l'exposition**
Lisez d'abord l'adresse d'écoute, puis testez l'accès depuis une machine autorisée sur le réseau concerné. Contrôlez enfin les règles de pare-feu applicables.

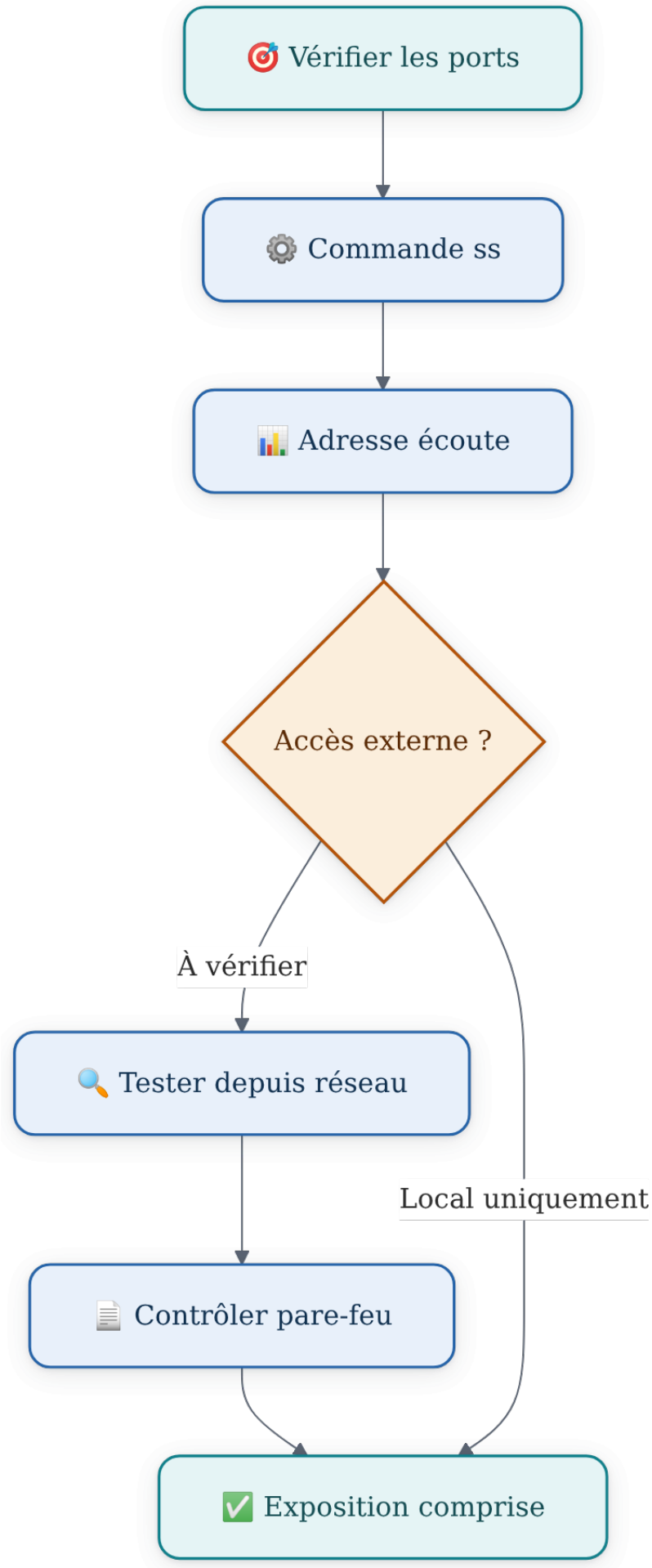

🎯 Vérifier les ports
⚙️ Commande ss
📊 Adresse écoute
Accès externe ?
À vérifier
Local uniquement
🔍 Tester depuis réseau
📄 Contrôler pare-feu
✅ Exposition comprise

SCHÉMA *Le parcours de vérification : socket, processus, adresse d'écoute et pare-feu.*

Lire une adresse d'écoute

Adresse observée	Interprétation pratique	Contrôle à faire
127.0.0.1:8080	Service limité à la machine locale	Vérifier qu'une exposition locale est bien souhaitée
0.0.0.0:8080	Service lié aux interfaces IPv4 disponibles	Contrôler le pare-feu et l'accès réseau
[::]:80	Écoute sur une adresse IPv6 générique	Vérifier les règles réseau et le filtrage IPv6

Checklist d'analyse de chaque port

- [ ] **Noter le protocole : TCP ou UDP**
  L'état LISTEN concerne surtout TCP ; UDP se lit différemment.
- [ ] **Noter l'adresse locale et le numéro de port**
  L'adresse compte autant que le numéro pour évaluer l'exposition.
- [ ] **Associer le port à un programme et à un PID**
  Utiliser la colonne processus de ss ou lsof.
- [ ] **Confirmer que le service est attendu**
  Le rapprocher des applications, agents ou services réellement nécessaires.
- [ ] **Examiner la configuration du service avant toute modification**
  Ne pas arrêter un processus inconnu sans identification.
- [ ] **Vérifier les règles de filtrage et l'accès depuis le réseau visé**
  Une écoute locale n'implique pas un accès extérieur.

Commandes à garder sous la main

`sudo ss -tulnp` : point de départ pour afficher les sockets TCP et UDP en écoute, leurs adresses et les processus accessibles.

`sudo lsof -nP -iTCP -sTCP:LISTEN` : vue orientée programme pour les sockets TCP en écoute.

`sudo lsof -nP -iTCP:8080 -sTCP:LISTEN` : recherche ciblée du programme qui écoute sur le port 8080.

`ss` sert à inventorier localement ; `lsof` aide à relier un port à un programme ; un test réseau reste nécessaire pour confirmer l'accessibilité.

> ! **Un port inattendu n'est pas automatiquement une compromission**
> Un serveur de développement, une base de données ou un agent de supervision peuvent être légitimes. Le critère utile est simple : chaque service exposé doit avoir une raison connue et une règle de filtrage claire.

Les résultats dépendent des permissions utilisées : employez sudo lorsque vous devez voir les processus appartenant à d'autres comptes système.