

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.



LE DIAGNOSTIC DES PORTS OUVERTS LINUX AVEC ss

Identifier rapidement les ports en écoute et les processus associés

COMMANDE À UTILISER

sudo ss -tulnp

QUE FAIT CETTE COMMANDE ?

Affiche les sockets (connexions) en écoute pour les protocoles TCP et UDP, avec les numéros de port et les processus associés.

EXEMPLE DE SORTIE :

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
udp	UNCONN	0	0	0.0.0.0:68	0.0.0.0:*	users:(("systemd-network",pid=1234,fd=12))
tcp	LISTEN	0	128	0.0.0.0:22	0.0.0.0:*	users:(("sshd",pid=567,fd=3))
tcp	LISTEN	0	80	127.0.0.1:3306	0.0.0.0:*	users:(("mysqld",pid=2345,fd=25))
tcp	LISTEN	0	128	:::80	:::*	users:(("nginx",pid=3456,fd=8))
tcp	LISTEN	0	128	:::22	:::*	users:(("sshd",pid=567,fd=4))
udp	UNCONN	0	0	:::5353	:::*	users:(("avahi-daemon",pid=788,fd=13))

PROTOCOLE (Netid)

Indique le protocole utilisé :

- tcp : Transmission Control Protocol
- udp : User Datagram Protocol

ÉTAT (State)

État du socket :

- LISTEN : en écoute
- UNCONN : non connecté (UDP)

ADRESSE LOCALE (Local Address:Port)

Adresse IP et port sur lesquels le service écoute.

Exemples courants : 0.0.0.0:22, 127.0.0.1:3306, :::80 (voir encadré ci-dessous)

ADRESSE DISTANTE (Peer Address:Port)

Adresse et port du pair.

En écoute, la valeur est généralement * (tout le monde).

PROCESSUS (Process)

Nom du processus, identifiant (PID) et descripteur de fichier utilisant le socket.

Permet d'associer le port au service.

LES ÉTAPES DU DIAGNOSTIC

- 1 AFFICHER LES SOCKETS EN ÉCOUTE**
Exécutez la commande :
`sudo ss -tulnp`
Elle affiche tous les ports TCP/UDP en écoute avec les processus associés.
- 2 REPÉRER ADRESSE ET PORT**
Identifiez les adresses IP (0.0.0.0, 127.0.0.1, :::1) et les numéros de port pour savoir où le service est accessible.
- 3 RELIER LE PORT AU PROCESSUS**
Consultez la colonne "Process" pour connaître le service (nom du processus) et son PID utilisant le port.
- 4 NOTER LES SERVICES NON ATTENDUS**
Soyez attentif aux ports ouverts qui ne devraient pas l'être : ils peuvent indiquer un service inutile, mal configuré ou potentiellement dangereux.

ADRESSES ET PORTS : EXEMPLES ET SIGNIFICATION

0.0.0.0:22	Écoute sur toutes les interfaces IPv4. Le service est accessible depuis n'importe quelle adresse réseau.
127.0.0.1:3306	Écoute uniquement sur l'interface locale (localhost). Le service n'est accessible que depuis la machine elle-même.
:::80	Écoute sur toutes les interfaces IPv6. Le service est accessible sur IPv6.

EXEMPLE D'USAGE

Service SSH accessible depuis le réseau
Base de données MySQL locale uniquement
Serveur web (HTTP) accessible en IPv6

BONNES PRATIQUES

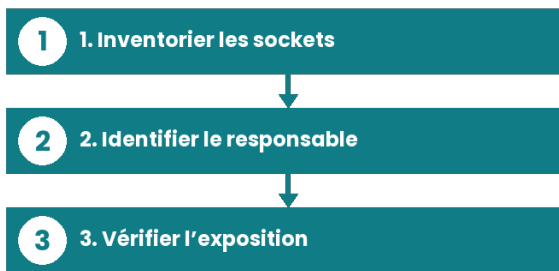
- ✓ N'ouvrez que les ports nécessaires.
- ✓ Préférez l'écoute sur 127.0.0.1 si le service est local.
- ✓ Utilisez un pare-feu (ex. : ufw, firewalld, nftables) pour filtrer les accès.
- ✓ Vérifiez régulièrement les ports en écoute.

ASTUCE : Pour filtrer un port spécifique, utilisez : `sudo ss -tulnp | grep :PORT` (ex. : `sudo ss -tulnp | grep :22`)

Pour plus de détails sur un processus : `ps -p <PID> -o pid,ppid,user,cmd`

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

Diagnostic express en 3 contrôles



1. Inventorier les sockets

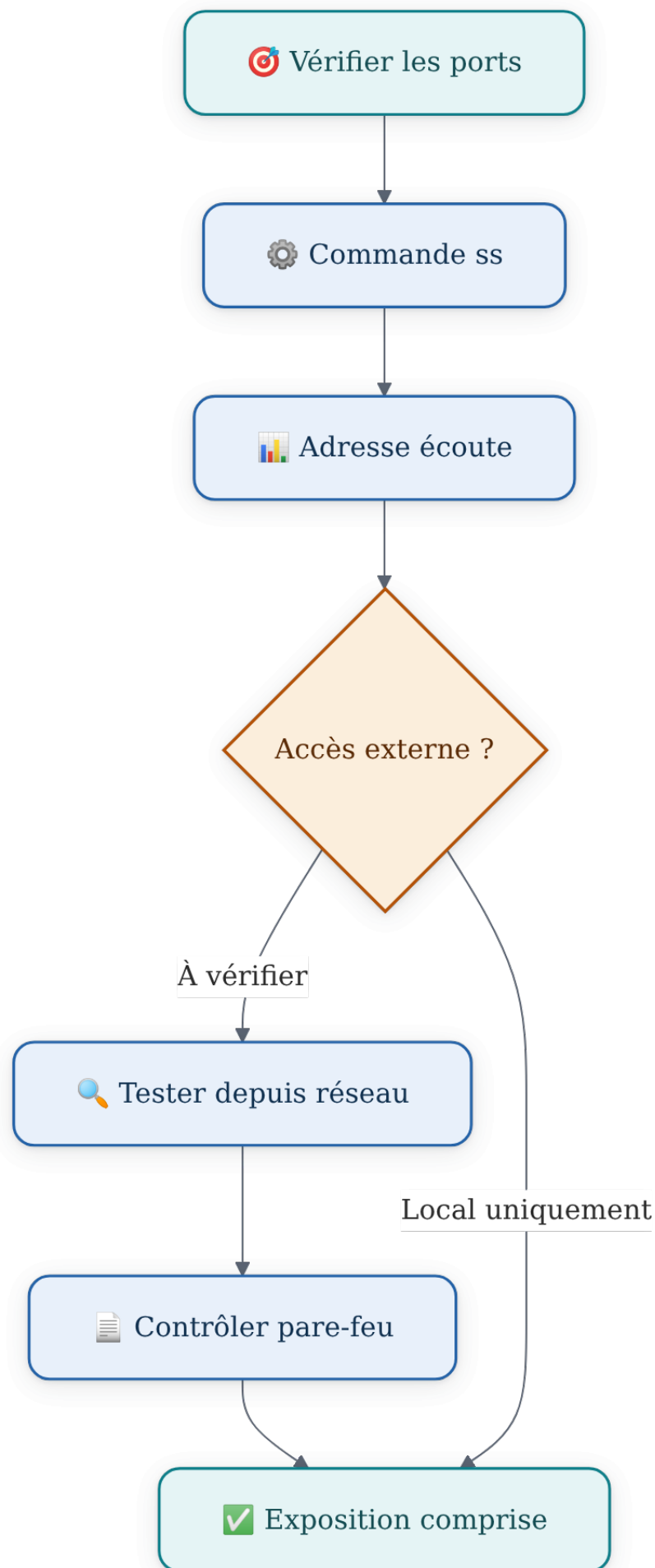
Exécutez `sudo ss -tulnp` pour afficher les sockets TCP et UDP en écoute, les adresses locales et, si les droits le permettent, les processus associés.

2. 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. 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.



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.