Commandes pertinentes

Réseau bloqué → `ping`, `traceroute`, `ip a`, `ip r`, `tcpdump`
Bridging/NAT → `brctl show`, `sysctl -p`, `iptables -t nat -L -n -v`
Pare-feu → `iptables -L -n -v`, `ufw status verbose`
Logs → `journalctl -xe`, `dmesg`, `cat /var/log/syslog`

Commandes essentielles pour les logs en live

1. **Afficher les logs en direct d'un fichier spécifique**
   ```
   tail -f /var/log/syslog
   ```

2. **Suivre uniquement les logs liés au kernel**
   ```
   tail -f /var/log/kern.log
   ```

3. **Suivre les logs de l'authentification (ex: SSH, sudo, etc.)**
   ```
   tail -f /var/log/auth.log
   ```

4. **Surveiller un fichier de log spécifique (ex: Apache, rsyslog, etc.)**
   ```
   tail -f /var/log/apache2/access.log
   tail -f /var/log/nginx/access.log
   tail -f /var/log/rsyslog.log
   ```

5. **Filtrer les logs avec `grep` (ex: voir uniquement les erreurs dans syslog)**
   ```
   tail -f /var/log/syslog | grep -i "error"
   ```

Alternative plus avancée avec **journalctl** (si systemd est utilisé)

1. **Voir les logs système en temps réel**
   ```
   journalctl -f
   ```

2. **Voir uniquement les logs d'un service spécifique**
   ```
   journalctl -f -u ssh
   journalctl -f -u apache2
   journalctl -f -u networkd
   ```

3. **Voir les logs du démarrage précédent**
   ```
   journalctl --boot -1
   ```

Commandes `lsof` pertinentes pour le réseau

1. **Lister toutes les connexions réseau actives (TCP & UDP)**
   ```
   lsof -i
   ```

2. **Voir les connexions ouvertes sur un port spécifique** (ex: SSH sur le port 22)
   ```
   lsof -i :22
   ```

3. **Lister uniquement les connexions TCP ou UDP**
   ```
   lsof -i tcp
   lsof -i udp
   ```

4. **Trouver quel processus utilise une IP spécifique**
   ```
   lsof -i @192.168.1.10
   ```

5. **Lister tous les processus utilisant des connexions réseau et leurs ports**
   ```
   lsof -i -P -n
   ```

   (**`-P`** : affiche les ports en numéros au lieu de les résoudre en noms)
   (**`-n`** : évite la résolution DNS pour aller plus vite)

6. **Lister les connexions réseau ouvertes par un utilisateur spécifique**
   ```
   lsof -i -u <nom_utilisateur>
   ```

   Exemple :
   ```
   lsof -i -u wingarmac
   ```

7. **Trouver quel processus utilise un port particulier (ex: 443 pour HTTPS)**
   ```
   lsof -i :443
   ```

8. **Trouver quel processus empêche l'arrêt d'une interface réseau**
   ```
   lsof -i | grep eth0
   ```

   (Pour un redémarrage d'une interface qui à eu lieu et voir ce qui l'utilise.)

9. **Lister les connexions réseau par programme (ex: voir ce que `apache2` utilise)**
   ```
   lsof -i | grep apache2
   ```