

# Maintenance des systèmes

# Introduction à la maintenance système

La maintenance informatique regroupe l'ensemble des actions permettant de :

- garantir le bon fonctionnement d'un système
- prévenir les pannes
- optimiser les performances
- assurer la sécurité des données

On distingue :

- **Maintenance préventive** : mises à jour, nettoyage, surveillance
- **Maintenance corrective** : réparation après incident
- **Maintenance évolutive** : ajout de fonctionnalités, optimisation

# Surveillance du système

- **Windows :**
- Gestionnaire des tâches : taskmgr
- Moniteur de ressources: resmon
- Observateur d'événements: eventvwr

Outil	Commande	Exemple d'utilisation
Gestionnaire des tâches	taskmgr	Trouver un programme qui consomme trop
Moniteur de ressources	resmon	Voir quel processus utilise le disque
Observateur d'événements	eventvwr	Trouver la cause d'un plantage

# Surveillance du système

- **Linux :**
- top, htop
- df -h, du -sh
- journalctl -xe

Commande	Syntaxe	Rôle	Exemple
top	top	Surveiller CPU/RAM	Trouver un processus gourmand
htop	htop	Version améliorée de top	Tuer un processus avec F9
df -h	df -h	Voir espace disque	Vérifier disque plein
du -sh	du -sh /chemin	Taille d'un dossier	Trouver dossier volumineux
journalctl -xe	journalctl -xe	Voir logs système	Diagnostiquer une erreur

# Commande : top

- **La commande top** affiche en temps réel :
- l'utilisation CPU
- la mémoire
- les processus en cours
- la charge système
- **Syntaxe** : top
- **→** Permet de repérer un processus qui consomme trop de CPU.
- **k**, puis entrer un PID → tuer un processus
- **M** → trier par mémoire
- **P** → trier par CPU

# Commande : htop

- Htop est une version améliorée de top :
  - interface colorée
  - navigation avec les flèches
  - affichage CPU par cœur
  - plus lisible
- **Syntaxe** :htop
- → Permet de visualiser facilement les processus gourmands et de les tuer.

# Commandes df -h et du -sh

**Commande : df -h** Affiche l'espace disque utilisé et disponible sur chaque partition. L'option **-h** = human readable (Go, Mo).

- **Syntaxe** :df -h

**Commande : du -sh**

- Affiche la taille d'un dossier.
- **Syntaxe** :du -sh chemin
- Options :
  - **-s** : résumé (summary)
  - **-h** : format lisible (Go, Mo)
- **Exemple** :du -sh /var/log
- Donne en sortie : 1.2G /var/log
- → Le dossier /var/log occupe 1,2 Go

# Commande : journalctl -xe

Affiche les logs système récents avec :

- détails
  - erreurs
  - messages critiques
  - contexte supplémentaire
- Permet de diagnostiquer :
- un service qui ne démarre pas
  - une erreur réseau
  - un crash système



# Commande : journalctl -xe

Affiche les logs système récents avec :

- détails
- erreurs
- messages critiques
- contexte supplémentaire

**Syntaxe** : journalctl -xe

- L'option **-x** ajoute des explications, L'option **-e** va à la fin du journal (logs les plus récents).

**Exemple :**

- Si un service échoue : `systemctl start apache2`

→ Erreur

- On tape : `journalctl -xe`

→ Affiche le message exact expliquant pourquoi Apache ne démarre pas.

# Mise à jour du système

- **Sous Linux :**

- mettre à jour régulièrement
- vérifier les services après mise à jour
- lire les notes de version pour les mises à jour majeures

## **Syntaxe :**

- `sudo apt update`
- `sudo apt upgrade -y`
- `sudo apt autoremove`



# Nettoyage du système

- **Windows :**
  - cleanmgr
  - suppression des fichiers temporaires
  - désinstallation des logiciels inutiles
  - nettoyage du démarrage (Task Manager → Démarrage)
- **Linux :**
  - sudo apt autoremove
  - sudo apt clean
  - suppression des logs trop volumineux



# Les sauvegardes (Backup)

La sauvegarde est l'élément **le plus important** de la maintenance. Elle permet de restaurer les données en cas de :

- panne matérielle
- attaque (ransomware)
- erreur humaine
- corruption du système



# Outils de sauvegarde

- **Sous Windows :**
  - Historique des fichiers
  - Sauvegarde système(image système)
  - OneDrive
  - Outils tiers (Acronis, Macrium Reflect...)
- **Sous Linux :**
  - rsync
  - tar
  - Timeshift (snapshots système)
  - Solutions réseau (NFS, Samba, BorgBackup...)



# Sauvegardes sous windows

## **Sauvegarde des fichiers (Historique des fichiers)**

- Sauvegarde automatique des documents, images, vidéos, bureau, etc.
- Vers un disque externe ou un partage réseau.
- **Ouvrir l'outil** :control /name Microsoft.FileHistory

## **Sauvegarde système (Image système)**

- Crée une **image complète** du système (Windows + programmes + fichiers).
- Permet une restauration totale après panne.
- **Ouvrir la sauvegarde système** :sdclt

# Sauvegardes sous windows

## Sauvegarde via OneDrive (Cloud)

- Sauvegarde automatique des dossiers : Bureau, Documents, Images.
- Accessible depuis n'importe quel appareil.
- **Lancer OneDrive** :onedrive

## Sauvegarde en ligne de commande (robocopy)

- **Commande** :robocopy source destination /MIR /R:1 /W:1
- **Exemple** :robocopy C:\Users\Ali\Documents E:\Backup\Documents /MIR
- → Copie exacte du dossier Documents vers un disque externe.

## Sauvegarde avec PowerShell

- **Copier un dossier** :(Powershell) Copy-Item -Path "C:\Data" -Destination "D:\Backup" -Recurse

# Sauvegarde sous linux

- **Sauvegarde avec rsync**

**Syntaxe** : `rsync -avh source destination`

**Exemple** : `rsync -avh /home/user/ /media/backup/home/`

- → Sauvegarde du dossier personnel vers un disque externe.





# Sauvegarde sous linux



- **Timeshift (snapshots système)**
- **Installer** :`sudo apt install timeshift`
- **Lancer** :`sudo timeshift --create --comments "Sauvegarde système"`
- → Sauvegarde du système (comme Windows Restore).
- **Sauvegarde automatique avec cron**

**Exemple de script rsync** :`rsync -avh /home/user/ /media/backup/home/`

**Planifier la sauvegarde quotidienne** :`crontab -e`

- Ajouter :`0 2 * * * rsync -avh /home/user/ /media/backup/home/`
- → Sauvegarde tous les jours à 2h du matin.

# Restauration windows

- **Restauration du système (System Restore)** permet de revenir à un point de restauration créé automatiquement ou manuellement. Cela restaure :
  - les fichiers système
  - les pilotes
  - les paramètres
  - → Sans toucher aux fichiers personnels.
- **Ouvrir la restauration en lançant:** rstrui.exe
- Choisir un point de restauration
- Redémarrer
- → Permet de réparer un problème après une mise à jour ou un pilote défectueux.
- **Restauration à partir d'une image système:** Restaure tout le système (Windows + programmes + fichiers). C'est une restauration complète.
- **Ouvrir l'outil :** sdclt.exe
- **Exemple :**
- Restaurer une image système stockée sur un disque externe après une panne grave.

# Restauration sous linux

- **Restauration du système avec Timeshift** : Equivalent de la restauration système Windows. Restaure :
  - fichiers système
  - configuration
  - → Sans toucher aux fichiers personnels.

## **Exemple :**

- Restaurer un snapshot après une mise à jour qui casse le système.

**Syntaxe :** `sudo timeshift --restore`

- **Restauration de fichiers avec rsync**

**Syntaxe :** `rsync -avh /backup/home/ /home/user/`

## **Exemple :**

- Restaurer un dossier supprimé ou modifié.

# Maintenance de réparation

- **Sous Windows**
- Réparer les fichiers système : `sfc /scannow`
- Vérifier et corriger les erreurs disque : `chkdsk C: /f`
- Désinstaller une mise à jour problématique
- Supprimer un virus avec Microsoft Defender
- Restaurer le système à un point antérieur
- Réinstaller un pilote défectueux

# Maintenance de réparation

- **Sous Linux**
- Réparer un paquet cassé : `sudo apt --fix-broken install`
- Vérifier un système de fichiers : `sudo fsck /dev/sda1`
- Redémarrer un service en panne : `sudo systemctl restart apache2`
- Analyser les logs pour trouver l'erreur : `journalctl -xe`
- Restaurer un snapshot (Timeshift)
- Réinstaller un service ou un paquet

# TP1: taskmgr

- **Trouver un programme qui ralentit le PC**
- Ouvre taskmgr
- Onglet **Processus**
- Clique sur **CPU** pour trier →identifies le programme qui consomme le plus.
- **Forcer l'arrêt d'un programme bloqué**
- Ouvre taskmgr
- Clique sur le programme bloqué
- Bouton **Fin de tâche** →Permet de débloquent le PC sans redémarrer.
- **Accélérer le démarrage**
- Onglet **Démarrage**
- Désactive les programmes inutiles →Windows démarre plus vite.

# TP1: resmon

- **Identifier un processus qui utilise trop le disque**
- Ouvre resmon
- Onglet **Disque**
- Regarde la colonne **Activité disque** → □ Tu vois quel programme fait “ramer” le disque.
- **Voir les connexions réseau actives**
- Onglet **Réseau**
- Regarde les processus qui envoient/reçoivent des données → □ Utile pour repérer un logiciel suspect.
- **Vérifier l'utilisation de la RAM**
- Onglet **Mémoire**
- Regarde la colonne **Durs actifs** → □ Permet de détecter une fuite mémoire.

# TP1: eventvwr

- **Exemple 1 : Trouver la cause d'un plantage**
- Ouvre eventvwr
- Journaux Windows → **Système**
- Filtre → **Erreur** → Tu identifies un pilote ou service défaillant.
- **◆ Exemple 2 : Vérifier les échecs de connexion**
- Journaux Windows → **Sécurité**
- Cherche l'ID **4625** → Indique une tentative de connexion échouée.
- **◆ Exemple 3 : Diagnostiquer un problème réseau**
- Journaux Windows → **Système**
- Cherche les erreurs **DNS, DHCP, TCP/IP** → Permet de comprendre pourquoi Internet ne fonctionne pas.



# TP2: Antivirus sous linux

- installer un antivirus open-source (ClamAV), analyser le système et mettre à jour les signatures.

**1. Mettre à jour le système** `sudo apt update && sudo apt upgrade -y`

**2. Installer ClamAV** `sudo apt install clamav clamav-daemon -y`

**3. Mettre à jour la base de signatures** `sudo freshclam`

**4. Lancer une analyse antivirus**

- **◆ Analyse d'un dossier** : `clamscan -r /home`
- **◆ Analyse complète du système** : `sudo clamscan -r --bell -i /`
  - `-r` : récursif
  - `--bell` : bip si virus trouvé
  - `-i` : afficher uniquement les fichiers infectés

**5. Analyse avec suppression automatique** `sudo clamscan -r --remove /home`

- ⚠ À utiliser avec prudence (supprime les fichiers infectés).

**6. Vérifier le service ClamAV** `systemctl status clamav-daemon`

# TP3 Créer un snapshot sous linux (point de sauvegarde) et restaurer avec Timeshift

- **1. Installer Timeshift** `sudo apt update` `sudo apt install timeshift -y`
- **2. Créer un point de sauvegarde**
  - `sudo timeshift --create --comments "Snapshot avant mise à jour"`
  - -> Un snapshot apparaît dans la liste des sauvegardes.
- **3. Vérifier les snapshots existants** `sudo timeshift --list`
  - -> Le snapshot créé doit apparaître avec la date et le commentaire.
- **4. Faire une modification volontaire**
  - Exemple : installer un paquet `sl`.
  - `sudo apt install sl -y`
- **5. Restaurer le système** `sudo timeshift --restore`
  - Choisir le snapshot créé
  - Confirmer
  - Redémarrer
  - -> Que remarquez vous?