Born 2 be Root

PARTIE 1 : GENERAL INSTRUCTION

graphical interface `ls /usr/bin/*session`

1- Vérification de la signature.txt - Qu'est qu'un .vdi, ou est le .vdi ? Comparer avec "diff"

- Un .vdi (Virtual Disk Image) est un format de disque dur virtuel utilisé par Oracle VirtualBox. Ce type de fichier permet de simuler un disque dur pour des machines virtuelles. Voici ce que cela signifie et comment il est utilisé : shasum

Qu'est-ce qu'un .vdi ?

1. **Virtual Disk Image (VDI)** :
   - Il s'agit d'un conteneur qui imite le comportement d'un disque dur physique.
   - Il stocke le système d'exploitation, les applications, et les fichiers de la machine virtuelle.
2. **Utilisation dans VirtualBox** :
   - Les machines virtuelles créées dans VirtualBox utilisent des fichiers .vdi pour simuler des disques durs.
   - Vous pouvez allouer un espace disque fixe ou dynamique lors de la configuration.

Types de fichiers VDI

- **Taille fixe** : Le fichier réserve immédiatement tout l'espace disque assigné, ce qui peut être plus rapide en termes de performance.
- **Taille dynamique** : Le fichier s'agrandit au fur et à mesure de l'utilisation, ce qui économise l'espace disque.

Caractéristiques du .vdi

- **Portabilité** : Un fichier .vdi peut être copié d'une machine à une autre pour déplacer une VM.
- **Snapshots** : VirtualBox permet de créer des snapshots (points de sauvegarde) directement sur le fichier .vdi.
- **Compatibilité** : Bien que natif à VirtualBox, les fichiers .vdi peuvent être convertis dans d'autres formats de disques virtuels (comme .vmdk pour VMware ou .qcow2 pour QEMU).

Applications pratiques

- Tester des systèmes d'exploitation.
- Simuler des environnements réseau ou serveurs.
- Développement et tests sans affecter le système hôte.

2- Dupliquer la vm initiale + Start le clone

PARTIE 2 : PROJECT OVERVIEW

1- Comment fonctionne une machine virtuelle ?

Il s'agit d'une ressource qui utilise un logiciel au lieu d'un ordinateur physique pour exécuter des programmes ou des applications. Chaque machine virtuelle possède son propre système d'exploitation et fonctionne séparément, vous pouvez donc avoir plusieurs machines virtuelles par machine. Peut être utilisé pour tester des applications dans un environnement sécurisé et séparé. Fonctionne en utilisant un logiciel pour simuler du matériel virtuel et s'exécuter sur une machine hôte.

2- Mon choix pour l'opérateur système - Un **opérateur système** est responsable de :

1. **Surveillance des systèmes** :
   - Veiller au bon fonctionnement des serveurs et des infrastructures réseau.
   - Utiliser des outils comme Nagios, Zabbix, ou Prometheus pour surveiller les performances et la disponibilité.
2. **Administration système** :
   - Gérer les utilisateurs et les permissions (notamment avec des commandes comme usermod, passwd, ou chown).
   - Configurer les services essentiels (Apache, Nginx, SSH, etc.).
   - Automatiser les tâches avec des scripts (bash, Python, etc.).
3. **Gestion des systèmes d'exploitation** :
   - Installer, mettre à jour et configurer des systèmes Linux/Unix (exemple : Ubuntu, Debian, CentOS, etc.).
   - Résoudre les problèmes de démarrage (grub, fstab, initrd).
4. **Sécurité** :
   - Implémenter des règles de pare-feu avec iptables ou ufw.
   - Gérer les droits root avec des outils comme sudo ou su.
   - Maintenir les systèmes à jour pour éviter les vulnérabilités.
5. **Gestion des disques et partitions** :
   - Gérer le stockage (création et manipulation de partitions avec fdisk, lsblk ou parted).
   - Configurer des systèmes RAID ou LVM pour une meilleure flexibilité et redondance.
6. **Virtualisation et conteneurs** :
   - Utiliser des technologies comme VirtualBox, VMware, KVM, ou des conteneurs comme Docker pour déployer des environnements virtualisés.
7. **Récupération en cas de panne** :
   - Sauvegarder et restaurer les systèmes avec des outils comme rsync, Bacula, ou des snapshots de systèmes de fichiers (ex. : ZFS, Btrfs).

3- Différence entre CentOS et Debian ?

Debian est beaucoup plus facile à mettre à jour que CentOS lorsqu'une nouvelle version est publiée. Debian est plus convivial et prend en charge de nombreuses bibliothèques, systèmes de fichiers et architectures. Il offre également davantage d'options de personnalisation. Si vous êtes une grande entreprise, CentOS offre davantage de fonctionnalités d'entreprise et un excellent support pour les logiciels d'entreprise.

4- Le but d'une machine virtuelle

Une machine virtuelle (VM) est une technologie qui permet d'exécuter un système d'exploitation ou une application dans un environnement simulé, séparé du matériel physique. Le but d'une machine virtuelle peut varier selon les besoins, mais voici les principaux objectifs et avantages :

- Permet de tester des systèmes d'exploitation ou des applications sans affecter le système hôte.
- Une machine virtuelle (par exemple, un fichier .vdi dans VirtualBox) peut être transférée d'un ordinateur à un autre sans perte de configuration, tant que le logiciel de virtualisation est compatible.
- Permet d'exécuter plusieurs systèmes d'exploitation ou applications sur un seul matériel physique, réduisant ainsi le besoin de plusieurs serveurs physiques.
- La VM isole les activités d'un système ou d'une application, limitant ainsi l'impact des failles de sécurité sur le système hôte.

5- Pourquoi j'ai choisi Debian

Plus facile à installer et à configurer, donc meilleur pour les serveurs personnels et pour les débutants.

6- DIfférence entre aptitude et apt

- Aptitude est un gestionnaire de paquets de haut niveau tandis que APT est un gestionnaire de paquets de niveau inférieur qui peut être utilisé par d'autres gestionnaires de paquets de niveau supérieur.
- Aptitude est plus intelligent et supprimera automatiquement les packages inutiles ou suggérera l'installation de packages dépendants.
- Apt ne fera explicitement que ce qui lui est demandé dans la ligne de commande.

7- Qu'est-ce que APPArmor

Système de sécurité Linux qui fournit une sécurité de contrôle d'accès obligatoire (MAC). Permet à l'administrateur système de restreindre les actions que les processus peuvent effectuer. Il est inclus par défaut avec Debian. Exécutez aa-status pour vérifier s'il est en cours d'exécution.

8- Expliquer qu'un script doit apparaître toutes les 5 minutes

PARTIE 3 : SIMPLE SETUP

1- Un mot de passe sera demandé avant de se connecter à la machine.

Connectes-toi avec un user avec l'aide de l'étudiant.

L'utilisateur ne doit pas être un root.

Il faut faire attention au mot de passe, il doit respecter les règles du sujet.

`sudo chage -l mlaussel`

`passwd nom_utilisateur` —> pour changer le mot de passe s'il faut

`cat /etc/passwd` —> voir tous les utilisateurs

2- Vérifier que le UFW service est lancé

`sudo systemctl status ufw`

3- Vérifier que la ssh service est lancé

`sudo systemctl status ssh`

4- Vérifier que l'operating system est Debian

`sudo apt install lsb-release` (si pas installé)

`lsb_release -a || cat /etc/os-release` (dernière partie pas obligatoire)

check Distributor id : Debian

PARTIE 4 : USER

1- Le sujet demande que l'utilisateur avec le login de celui qui est évalué soit présent sur la VM. Vérifier le et qu'il est suivi de "sudo" et "user42" groupes.

- `whoami` : affiche que mlaussel
- Pour afficher les groupes auxquels appartient un utilisateur : `groups mlaussel`
- Pour afficher que le groupe : `getent group sudo ; getent group user42`

2- Vérifions maintenant que les règles du mot de passe soient mises en places avec ces différentes étapes

A) En premier, crée un nouvel user. Attribue-lui le mot de passe de votre choix en respectant les demandes du sujet. Je dois maintenant expliquer comment ils ont pu mettre en place les règles demandées dans le sujet sur leur machine virtuelle. Normalement il devrait y avoir 1 ou 2 fichiers modifiés.

Créer un nouvel utilisateur : `sudo adduser new_username`

Attribuer le mot de passe

Pour les règles de mot de passe, nous utilisons la bibliothèque de vérification de la qualité des mots de passe et il existe deux fichiers : le fichier common-password qui définit les règles telles que les caractères majuscules et minuscules, les caractères en double, etc. et le fichier login.defs qui stocke les règles d'expiration du mot de passe (30 jours, etc.).

- `Sudo nano /etc/login.defs`
- `Sudo nano /etc/pam.d/common-password`

`Pour vérifier que le mot de passe de l'utilisateur respecte la politique de sécurité : sudo chage -l username`

B) Il faut maintenant créer un groupe "evaluating" + attribuer ce groupe au nouvel user + montrer que l'utilisateur est bien assigné au groupe.

```
sudo groupadd groupname
sudo usermod -aG groupname new_username
getent group evaluating
```

`(sudo groupdel evaluating)` —> pour supprimer un groupe

C) Expliquer les avantages et désavantages des règles de ces mots de passes

Avantages des règles de mots de passe

1. **Renforcement de la sécurité** :
   - Des mots de passe complexes et longs sont plus difficiles à deviner ou à pirater via des attaques par force brute ou par dictionnaire.
   - L'obligation d'utiliser des caractères spéciaux, des majuscules, et des chiffres réduit les chances de collisions avec des mots simples.
2. **Protection contre les réutilisations** :
   - Les règles interdisant la réutilisation de mots de passe empêchent qu'un mot de passe ancien, compromis ou divulgué soit utilisé à nouveau.
3. **Mises à jour régulières** :
   - L'expiration périodique des mots de passe réduit les risques en cas de compromission d'un mot de passe.
4. **Conformité réglementaire** :
   - Les organisations peuvent répondre aux exigences des normes de sécurité (comme PCI DSS, GDPR, ISO 27001) en appliquant des politiques strictes sur les mots de passe.
5. **Réduction des attaques internes** :
   - Des règles strictes limitent la possibilité pour un utilisateur malveillant interne ou externe d'exploiter des mots de passe faibles.

Inconvénients des règles de mots de passe

1. **Complexité pour les utilisateurs** :
   - Des mots de passe compliqués sont souvent difficiles à retenir, ce qui peut entraîner des comportements risqués :
     - L'écriture des mots de passe sur papier.
     - Le stockage non sécurisé des mots de passe (ex. : fichiers texte).
2. **Fausses sécurités** :
   - Si les utilisateurs sont contraints de changer fréquemment leur mot de passe, ils peuvent utiliser des schémas prévisibles (ex. : `Password01`, puis `Password02`), rendant ces mots de passe faciles à deviner.
3. **Fatigue des utilisateurs** :
   - Des règles trop strictes peuvent frustrer les utilisateurs et les conduire à adopter des solutions faciles mais risquées (réutiliser un mot de passe entre différents services).
4. **Coût opérationnel** :
   - Les politiques strictes peuvent augmenter les demandes au support technique, comme des réinitialisations de mots de passe fréquents.

5. **Fausse impression de sécurité** :
   - Même avec des mots de passe forts, une attaque ciblée comme l'hameçonnage (phishing) ou une base de données compromise peut toujours les exposer.

PARTIE 5 : HOSTNAME ET PARTITIONS

1- Vérifier que le nom de l'hôte de la machine est correctement formaté de cette façon : login42

```
hostnamectl
```

2- Modifier le nom de l'hôte en le remplaçant avec le login du correcteur + restart la machine (normalement le nom a change)

```
sudo hostnamectl set-hostname new_hostname
sudo reboot
```
(restart la machine)

3- Restaurer la machine avec le nom originel de l'hôte

```
sudo nano /etc/hosts
sudo reboot
```
(restart la machine)

4- Montrer comment voir une partition

```
lsblk
```

5- Comparer avec celle du sujet + donner une explication de comment LVM fonctionne et de quoi il est sujet

Logical Volume Manager – nous permet de manipuler facilement les partitions ou le volume logique sur un périphérique de stockage. C'est comme créer des sous disques durs.

LVM est un excellent choix pour :

- **Faciliter les mises à jour ou modifications du stockage**.
- **Réagir rapidement aux besoins en espace disque**, par exemple, si `/home` nécessite plus d'espace.
- **Séparer les systèmes de fichiers**, une bonne pratique pour la gestion de la sécurité et des sauvegardes.

Dans le cadre du projet **Born2beRoot** de 42, vous devez comprendre les bases du système de fichiers sous Linux, notamment le **LVM** (Logical Volume Manager) et la gestion des partitions. Voici une explication détaillée :

---

1. Qu'est-ce que LVM et comment fonctionne-t-il ?

> **LVM** (Logical Volume Manager) est une méthode flexible pour gérer les espaces de stockage sur un système Linux. Contrairement aux partitions classiques, qui sont statiques et difficiles à modifier, LVM permet une gestion dynamique du stockage.

Principes de fonctionnement de LVM :

1. **Physical Volumes (PVs)** :
   Ce sont les disques physiques ou partitions physiques (ex. : `/dev/sda1`, `/dev/sdb`). Chaque PV est ajouté à un groupe pour former une réserve de stockage.
2. **Volume Groups (VGs)** :
   Les Physical Volumes sont regroupés en Volume Groups. Un VG agit comme un pool de stockage logique (une "réserve").
3. **Logical Volumes (LVs)** :
   À partir d'un Volume Group, on crée des Logical Volumes. Ce sont ces volumes que le système utilise pour les systèmes de fichiers (comme ext4, xfs, etc.).
   Par exemple : le répertoire `/home` ou `/var` peut être situé sur un LV.
4. **Flexibilité du système LVM** :
   - **Redimensionnement** : Les LVs peuvent être redimensionnés (agrandis ou réduits) sans avoir à reformater les disques. Cela simplifie l'ajout de stockage ou la réorganisation des données.
   - **Snapshots** : Vous pouvez créer des instantanés (snapshots) pour sauvegarder l'état d'un système à un moment donné.
   - **Migration** : LVM facilite la migration des données d'un disque à un autre sans interruption.

Avantages de LVM :

- **Dynamisme** : On peut ajouter ou retirer des disques physiques à chaud.
- **Optimisation** : Utilisation plus efficace de l'espace disque.
- **Gestion simplifiée** : Redimensionnement des volumes sans affecter le fonctionnement des systèmes de fichiers.
- **Snapshots** : Utile pour les sauvegardes et les tests.

---

2. Partitionnement classique et avec LVM :

Dans Linux, une **partition** est une division logique d'un disque physique pour organiser les données.

Partitionnement classique :

- Le disque est divisé en **partitions fixes**, définies par une table de partitions (MBR ou GPT).
- Chaque partition est montée sur un répertoire spécifique comme `/`, `/home`, `/var`.
- Problème : La taille des partitions ne peut être modifiée facilement.

Partitionnement avec LVM :

- Un **Physical Volume (PV)** est créé à partir d'une partition ou d'un disque brut.
- Les PVs sont ajoutés à un **Volume Group (VG)**.
- Les **Logical Volumes (LV)** sont ensuite créés dans le VG et montés comme n'importe quelle partition.
  Exemple :
  - `/` (racine) → 1 LV
  - `/home` → 1 LV
  - `/var` → 1 LV

PARTIE 6 : SUDO

1- Vérifier que le program sudo est proprement installé sur le machine virtuel

```
dpkg -l | grep sudo
```

2- Assigner et montrer que le nouvel utilisateur est assigné au group sudo

```
sudo usermod -aG groupname new_username
getent group sudo
```

3- Sudo utilise des règles strictes, expliquer les valeurs et les opérations de sudo avec les exemples de mon choix

sudo (Superuser DO) est une commande puissante utilisée pour exécuter des commandes avec des privilèges administratifs, même lorsque l'utilisateur connecté est un utilisateur standard. Cela repose sur un ensemble de **règles strictes** définies dans le fichier **/etc/sudoers** ou des fichiers complémentaires dans **`/etc/sudoers`**

Pour ouvrir les règles sudo : `sudo visudo`

Ou alors : `cd /etc ; cat sudoers`

4- Montrer une implémentation des règles imposées dans le sujet

Les règles strictes pour `sudo` sont généralement définies dans le fichier `/etc/sudoers`.
Pour l'éditer en toute sécurité, utilisez : `sudo visudo`

Exemple de règles strictes à configurer :

Limiter les tentatives de mot de passe :
Cela empêche les attaques par force brute :

```
Defaults passwd_tries=3
```

Logs des commandes `sudo` :
Activez les journaux pour traquer toutes les commandes passées avec `sudo` :

```
Defaults logfile="/var/log/sudo.log"
```

Un message de votre choix s'affiche en cas d'erreur suite à un mauvais mot de passe lors de l'utilisation de sudo

```
Defaults badpass_message="Password is wrong, please try again!"
```

Autoriser seulement certaines commandes :
Par exemple, limiter un utilisateur `john` à exécuter uniquement des commandes liées au système :

```
john ALL=(ALL) NOPASSWD: /bin/systemctl, /usr/bin/apt
```

Cela empêche `john` de passer des commandes arbitraires.

5- Vérifier que /var/log/sudo existe et a un fichier

```
cd  ..
cd ..
cd /var/log/sudo
ls
```

6- Vérifier le contenu du fichier dans ce dossier. On devrait voir l'historique des commandes utilisées avec sudo.

```
cat sudo.log
```

7- Essayer de lancer une commande via sudo + regarder si le fichier dans /var/log/sudo a ete update

```
sudo ufw status
cat sudo.log
```

PARTIE 7 : UFW

1- Vérifier que le programme UFW est correctement installé sur la VM.

```
sudo ufw status numbered
```

2- Vérifier que ca fonctionne proprement

3- Expliquer simplement qu'est qu'une UFW et l'avantage de l'utiliser.

UFW permet de gérer le trafic réseau entrant et sortant sur une machine en définissant des **règles de pare-feu**. Ces règles permettent ou bloquent les connexions en fonction de critères tels que les adresses IP, les ports ou les protocoles.

- **Trafic entrant** : Par exemple, autoriser les connexions SSH ou HTTP.
- **Trafic sortant** : Par exemple, restreindre les connexions vers des sites spécifiques ou interdire l'accès à Internet pour certains programmes.

Avantages d'UFW :

- **Facilité d'utilisation** : Les commandes sont simples et intuitives.
- **Sécurité renforcée** : Les règles par défaut (bloquer le trafic entrant) protègent la machine dès l'activation.
- **Adapté à Born2beRoot** : Il est exigé de sécuriser votre serveur, et UFW vous aide à contrôler les connexions réseau efficacement.

4- Lister les règles actives dans UFW + montrer qu'une règle existe pour le port 4242.

```
sudo ufw status numbered
```

5- Ajouter une règle ouverte port8080. Vérifier que la regle a ete ajoute a la liste des règles actives

```
sudo ufw allow 8080
sudo ufw status numbered
```

6- Enfin, supprimer cette nouvelle règle

Ensuite, utilisez le numéro de la règle pour la supprimer. Par exemple, si la règle pour le port **8080** est la règle **[2]**, utilisez : `sudo ufw delete 2`

PARTIE 8 : SSH a revoir

1- Vérifier que le service SHH est proprement installé sur la VM.

```
sudo service ssh status
OU
ssh your_user_id@127.0.0.1 -p 4242
```

2- Vérifier que ca fonctionne proprement

3- Expliquer qu'est qu'une SSH et l'intérêt de l'utiliser.

SSH ou Secure Shell est un mécanisme d'authentification entre un client et un hôte. Il utilise des techniques de cryptage pour que toutes les communications entre les clients et les hôtes soient effectuées sous forme cryptée. Les utilisateurs sur Mac ou Linux peuvent utiliser le terminal SSH pour travailler sur leur serveur via SSH.

answer: secure shell, allows 2 computers to securely talk to each other

4- Vérifier que que la SSH utilise seulement le port 4242

```
sudo nano /etc/ssh/sshd_config
sudo ss -tuln | grep 4242
```

Pour voir apparaitre : tcp LISTEN 0 128 0.0.0.0:4242

5- Utiliser la SHH pour log in avec le nouvel utilisateur créé. Pour faire ça, soit on utilise une clé ou alors un mot de passe. Il faut s'assurer qu'on ne peut pas utiliser la SSH avec le root user.

avec un utilisateur : `ssh your_user_id@127.0.0.1 -p 4242`

montrer que ca ne fonctionne pas avec un root : `ssh mlaussel42@127.0.0.1 -p 4242` —> Doit afficher permission denied

PARTIE 9 : SCRIPT MONITORING

1- Expliquer simplement comment le script fonctionne en montrant le code

Script inputted in the monitoring .sh file to display system information

```
cd /usr/local/bin
cat monitoring.sh
```

1- ARC = uname -a : Affiche toutes les informations sur le noyau Linux.

2- PCPU = Cœurs physiques

- **Les cœurs physiques sont les unités réelles de calcul présentes sur le processeur.**
- **Chaque cœur physique peut exécuter des instructions indépendamment des autres.**
- **Exemple :**
  Un processeur quad-core (4 cœurs physiques) possède 4 unités réelles capables de traiter des tâches.

  grep "physical id" : Recherche les identifiants des CPU physiques.
  sort | uniq | wc -l : Compte le nombre de CPU physiques (sans doublon).

3- VCPU = Cœurs virtuels (Threads ou vCPU)

- **Les cœurs virtuels sont créés grâce à des technologies comme Hyper-Threading d'Intel ou SMT (Simultaneous Multi-Threading).**
- **Hyper-Threading permet à chaque cœur physique de se comporter comme deux cœurs logiques (ou virtuels).**
- **En pratique :**
  Un processeur avec 4 cœurs physiques et Hyper-Threading active 8 cœurs virtuels (threads).

Comment ça fonctionne ?

- **Chaque cœur physique peut gérer deux flux d'instructions simultanément.**
- **Cela améliore l'utilisation des ressources du CPU lorsque l'unité est sous-utilisée (par exemple, lors de tâches moins gourmandes).**

grep "^processor" : Compte toutes les entrées "processor" pour obtenir le nombre total de **vCPU** (y compris Hyper-Threading).

4- Utilisation de la mémoire RAM

La mémoire RAM (Random Access Memory, ou mémoire à accès aléatoire) est un type de mémoire volatile utilisée par les ordinateurs pour stocker temporairement des données nécessaires aux programmes en cours d'exécution. Elle perd toutes ses données dès que l'ordinateur est éteint.

FRAM =

free -m : Affiche l'utilisation de la mémoire en Mo.

awk : Filtre pour obtenir la mémoire totale.

URAM = print $3 : Affiche la mémoire utilisée.

PRAM = $3/$2*100 : Calcule le pourcentage d'utilisation de la mémoire.

5- Utilisation du disque

FDISK =

df -BG : Affiche l'espace disque en Go.

grep '^/dev/' : Sélectionne les partitions principales.

ft += $2 : Additionne les tailles des partition

UKDISK =

ut += $3 : Additionne l'espace utilisé (en Mo).

PDISK = ut/ft*100 : Calcule le pourcentage d'utilisation disque.

6- CHARGE CPU

C'est un composant matériel qui exécute les instructions des programmes et effectue les calculs nécessaires au fonctionnement du système.
Exécuter des instructions :

- **Il exécute les commandes des logiciels et du système d'exploitation.**
- **Par exemple : ouvrir un fichier, exécuter un calcul mathématique, charger une page web.**

Effectuer des calculs :

- **Il effectue des opérations arithmétiques (addition, soustraction, etc.) et logiques (comparaisons, conditions).**

Coordonner les opérations :

- **Le CPU gère la communication entre les autres composants (RAM, stockage, carte graphique, etc.).**

Plus il y a de cœurs, plus le CPU peut gérer de tâches simultanément (multitâche).

8- Utilisation de LVM

LVMU =

`lsblk` : Liste les périphériques de stockage.

`grep "lvm"` : Vérifie si LVM est utilisé.

Ternaire Bash : Renvoie yes si LVM est présent, sinon no.

9- CONNEXION TCP

Liste les connexions TCP établies.

Une connexion TCP (Transmission Control Protocol) est une connexion réseau utilisée pour établir une communication fiable entre deux appareils sur un réseau, comme Internet. Elle appartient à la couche transport du modèle OSI (Open Systems Interconnection) et est largement utilisée pour garantir que les données envoyées arrivent correctement et dans l'ordre.

10- Nombres d'utilisateurs connectés

`users` : Liste les utilisateurs actuellement connectés.

`wc -w` : Compte le nombre total.

11- Informations réseau

`hostname -I` : Donne l'adresse IP locale.

12- Nombre de commandes sudo exécutées

`journalctl _COMM=sudo` : Liste les logs des commandes sudo.

`grep COMMAND` : Filtre uniquement les commandes exécutées avec sudo.

`wc -l` : Compte leur nombre.

2- Qu'est ce que cron

Cron ou cron job est un utilitaire de ligne de commande permettant de planifier l'exécution de commandes ou de scripts à des intervalles spécifiques ou à une heure précise chaque jour. Utile si vous souhaitez configurer votre serveur pour qu'il redémarre à une heure précise chaque jour.

- `Cd /usr/local/bin`– pour afficher monitoring.sh
- `Sudo crontab -u root -e`–pour éditer la tâche cron
- `Change script to */1 * * * * sleep 30s && script path`– pour l'exécuter toutes les 30 secondes, supprimez la ligne pour arrêter l'exécution du travail.

3- Comment on fait apparaître le script toutes les 10 minutes quand le serveur commence.

sudo crontab -u root -e (***change 10 value to 1***)

4- Changer l'apparition du script a toutes les 30s.

sudo crontab -u root -e
*/1 * * * * sleep 30s && /usr/local/bin/monitoring.sh

5- On peut varier les valeurs

6- Faire stopper le script quand le serveur start mais sans modifier le script lui-même. Pour vérifier ce point, il faudra restart la machine. Au start, il faudra vérifier que le script existe toujours et au même endroit, sans être modifié tout comme les droits.

L'étudiant évalué doit faire en sorte que le script s'arrête lorsque le serveur a démarré, sans modifier le script lui-même. Pour vérifier cela, redémarrez la machine virtuelle (VM).

```
Pour arrêter le service cron, tu peux utiliser :
sudo systemctl stop cron
Pour arrêter le service cron, meme apres un reboot :
sudo systemctl disable cron

Pour redémarrer le service cron :
sudo systemctl start cron
Pour redémarrer le service cron, meme apres un reboot :
sudo systemctl enable cron
```

```
Pour vérifier si cron fonctionne :
sudo systemctl status cron
```

Au démarrage, vérifiez que le script est toujours au même emplacement, que les droits sont restés inchangés et qu'il n'a pas été modifié.

```
sudo reboot
sudo crontab -u root -e
```