Born 2 be root

Administration systeme

Virtualisation

Creer une machine virtuelle (VM) (installer un système d'exploitation) (serveur virtuel)

But : installer et configurer un serveur

VirtualBox : logiciel de virtualisation open source

Permet de faire tourner un système Linux sur un PC avec un autre système principal

Permet d'isoler des environnements spécifiques (serveurs ou environnements de développement)

Host : OS qui execute VirtualBox

Guest : OS qui tourne dans la VM

Disque virtuel : fichier agissant comme un disque dur pour la VM (les donnees et l'OS y sont stockes)

Snapshot : instantane de l'etat de la VM, permet de restaurer la VM a cet etat en cas de probleme (possibilite de revenir en arrière en cas de fausse manip par exemple, ou pour reprendre une installation en cours)

Version utilisee : Oracle VirtualBox (7.0.14 pour Ubuntu 22.0.4, 7.1.4 pour Windows)

Le système d'exploitation sera un serveur

VirtualBox propose plusieurs offres de reseau :

- NAT (par defaut) : permet une connexion internet en toute sécurité, avec peu de configuration. Utilise l'adresse IP de l'hote pout accéder a internet, passe par une translation d'adresse (NAT) pour accéder au reseau externe : le reseau externe voit alors l'adresse IP de l'hote, et non celle de la VM. La VM a alors acces a internet VM, mais n'est pas accessible depuis le reseau externe (local ou internet), par d'autres machines
- Pont : connecte directement la VM au reseau local, la rendant accessible aux autres appareils du reseau (comme si la VM était un appareil a part entière). Usage ideal si l'on veut que la VM agisse comme un serveur accessible aux autres appareils du reseau local (serveur zeb, base de donnees, etc)
- Reseau interne : permet une communication entre les VM sur le même hote (sans passer par le reseau externe). Les VM connectes au reseau interne ne peuvent pas accéder au reseau interne ou a internet, ni atteintes par l'hote ou

d’autres appareils du reseau. Pour les tests en environnement isole, ou pour un cluster de serveurs ou un reseau restreint

UTM : similaire a VirtualBox, mais pour les Mac sous ARM

Virtualisation (pour les OS conçus pour la même architecture que celle du Mac hote), ou emulation (simule une autre architecture materielle)

Debian 12.8.0 (amd64) (https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/ (debian-12.8.0-amd64-netinst.iso)

Debian : OS open source, base sur le noyau Linux (très populaire dans le monde des serveurs et développeurs car très stable et securise)

Debian est a la base d’Ubuntu par exemple

Utilise APT (Advanced Package Tool) pour installer, mettre a jour et gérer les logiciels

possède un grand depot de logiciels de tout genre

Grosse communauté et support a long terme

Securise, mises a jour rapide, failles potentielles corrigees rapidement

Très polyvalent sur de larges gammes d’architecture

Trois branches : stable (version testee et fiable), testing (version en cours de tests, pour les développeurs et les testeurs), et unstable (potentiellement instable, pour les tests et contributeurs)

Rocky Linux : distribution Linux open source, gratuite et stable

Depuis que CentOS a change son modele de mise a jour (alternative a CentOS)

Stable et compatible avec Red Hat Entreprise Linux (RHEL)

Rocky est un clone de REHL, qui est payant, mais n’inclus pas le support direct de Red Hat, ni Red Hat Satellite (qui simplifie la gestion des systèmes a grande échelle a partir d’une interface centralisee)

Support a plus long terme (10 ans)

Utilise DNF comme gestionnaire de paquets

Projet ouvert et aligne avec les besoins des utilisateurs

Migration facile depuis CentOS

Plutôt utilise pour les serveurs en production dans les entreprises

Debian est gere par une communauté mondiale de bénévoles, n'est pas affiliee a une entreprise commerciale : liberté logicielle et transparence totale, alors que Rocky est gere par RESH (Red Hat), et plus oriente vers la compatilite avec RHEL (payant)

Debian est très flexible, peut être facilement adapte pour divers usages (OS, système de bureau, etc). Enorme bibliotheque de logiciels, versions adaptees a différentes architectures matérielles, alors que Rocky est plus centre sur les environnements de type entreprise (stable et compatible avec RHEL). Offre moins de personnalisation dans sa configuration initiale (vise plutôt les environnements serveurs professionnels)

Debian utilise le gestionnaire de paquets APT, bien documente et simple a utilliser, et est déjà livre avec un vaste dépôt de logiciels, ce qui facilite l'installation et la mise a jour des applications, alors que Rocky utilise DNF et les dépôts RPM (bibliotheque plus limitee dans ses dépôts officiels)

Debian propose trois branches de mises a jour, ce qui permet de choisir la version correspondant a ses besoins. La version stable de Debian est solide. Rocky suit le modele de RHEL, avec des mises a jour moins frequentes et davantages orientees entreprise

Debian a une grosse communauté d'utilisateurs et de contributeurs : forums, documentation : support et resolution de problèmes plus simple, alors que Rocky est plutôt nouveau, plus faible communauté, peu de support communautaire

Debian est extrêmement polyvalent, comme OS bureau ou comme OS serveur,avec une interface utilisateur plus riche et son support de paquet, alors que Rocky est concu pour les serveurs d'entreprise

VirtualBox stocke le contenu du disque virtuel de la VM dans le fichier .vdi (Virtual Disk Image)

Il contient le systeme d'exploitation, les donnees et toutes les applications installees dans la VM

Il simule un disque dur classique et est utilise par VirtualBox pour lire et écrire les donnees de la VM, comme s'il s'agissait d'un vrai disque dur

Stockage dynamique : le fichier .vdi ne prend initialement que peu de place sur le disque dur de l'hote, et grossit en fonction de la quantite de donnees que l'on y ajoute, jusqu'à atteindre une taille maximale (définie lors de sa creation)

Stockage fixe : taille définie des le depart, prend immediatement tout l'espace defini sur le disque physique de l'hote (mem si la VM n'utilise pas tout cet espace)

Le fichier .vdi peut être facilement deplace d'une machine a une autre : on peut copier le fichier .vdi sur un autre ordinateur et lancer la VM en le chargant dans VirtualBox : toutes les donnees seront intactes

Il est possible de prendre des snapshots (instantanes) de la VM, ce qui sauvegarde l'etat actuel du système et permet de revenir a cet etat plus tard (un fichier .vdi supplementaire est alors cree, qui enregistre uniquement les modifications apportees depuis le dernier snaphot

Il est possible de le convertir en VMDK (utilise par VMware) par exemple, ou même VHD (Hyper-V)

La signature SHA-1 (Secure Hash Algorithm 1) d'un fichier est un code unique généré par une fonction de hachage cryptographique : elle transforme le contenu du fichier en une chaine de caractères fixe (40 caracteres hexadecimaux)

Chaque bit du fichier effectue des calculs mathématiques pour générer le hash
Le resultat sera toujours le même tant que le contenu du fichier ne changere pas

Si le contenu du fichier est modifie, même d'un seul bit, le hash SHA-1 genere a partir de celui-ci sera completement different

Cela permet de confirmer que le fichier est authentique et n'a subi aucune modification

Installer le minimum de services et pas d'interface graphique :

Permet de reduire l'utilisation des ressources : les interfaces graphiques et les services supplémentaires consomment de la mémoire, du CPU et de l'espace disque

Les ressources sont ainsi libérees pour les taches essentielles du serveur

Meilleures performances pour les applications critiques (on maximise l'effacite et la rapidité en allouant toutes les ressources au serveur)

Amelioration de la sécurité : en limitant les services, on réduit la surface d'attaque du serveur (moins de points potentiels de vulnerabilite) : ainsi, le serveur est plus difficile a compromettre

Moins de mises a jour a effectuer, moins de risque d'introduire de nouvelles vulnerabilites

Gestion plus facile, maintenance réduite : configuration plus simple, moins sujette aux conflits ou aux erreurs

Moins de logs a surveiller, moins de dependances a gérer, moins de risque de defaillance d'un service secondaire qui pourrait affecter le serveur principal

Mises a jour plus rapides, plus faciles a planifier

Deploiement plus rapide et leger, démarrage et sauvegardes rapides, taille de l'image système reduite

Moins de dependances lors des migrations

Les systèmes Linux sont conçus pour fonctionner de manière modulaire, en installant seulement les services nécessaires pour une tache specifique (système dedie et fiable)

Maitrise complete en ligne de commande : encourage l'utilisation de la ligne de commande, plus puissante et flexible pour l'administration a distance : automatisation et gestion des serveurs plus efficace, avec des scripts et des outils de gestion de configuration

X.org est donc interdit (utilise pour gérer l'interface graphique GUI des systèmes Linux)

Fournit la base graphique pour utiliser une interface graphique sur les systèmes Linux (éléments visuels, fenêtres, menus, etc)

KDump est un mecanisme de capture de pannes de noyau (kernel crash dump) pour les systèmes Linux

Il est utilise pour collecter des informations de diagnostic et de debogage lorsaue le noyau de l'OS rencontre une panne critique (kernel panic)

Les informations (dumps ou crash dumps) sont essentielles pour les admins système, pour comprendre la cause de la panne et apporter des correctifs

KDump est preconfigure par defaut pour Rocky, et peut y être installe et active facilement

SELinux (Security-Enhanced Linux) est un module de securite pour Linux

Il fournit un mecanisme de contrôle d'acces obligatoire (MAC – Mandatory Access Control)

Il est concu pour renforcer la sécurité su système en appliquant des politiques de sécurité strictes (contrôle comment les processus et les utilisateurs peuvent interagir avec les fichiers, les repertories, les périphériques et les autre ressources du systeme

Contexte de sécurité : Chaque fichier, processus et ressource dans un système SELinux est associe a un contrôle de sécurité

Cela inclus des attributs comme l'utilisateur SELinux, le rôle, le type, et le niveau de securite

Par exemple, un fichier de configuration de serveur pourrait avoir un contexte specifique qui limite son acces aux seuls processus qui en ont besoin

La politique SELinux est un ensemble de règles predefinies, qui contrôlent les acces

Exemple : Certains processus peuvent lire les fichiers de configuration, mais ne peuvent pas modifier les fichiers systemes critiques

3 modes pour SELinux existent :

Enforcing : applique toutes les règles de la politique de sécurité (les actions non autorisees sont bloquees

Permissive : SELinux est en mode d'observation et n'applique pas réellement les règles, mais enregistre dans les logs toutes les actions qui auraient été bloquees

Disabled : SELinux est desactive (aucon controle d'acces supplementaire n'est applique)

Renforce la sécurité : couche de sécurité qui limite les actions des processus et des utilisateurs, même en cas de compromission (si un attaquant réussit a exploiter une vulnerabilite dans une application, SELinux peut empêcher l'application d'acceder a d'autres parties critiques du systeme

Protection contre les escalades de privileges : limite les privileges des applications et des utilisateurs : empeche un processus compromis d'acceder a des fichiers ou processus auxquels il ne devrait pas avoir acces

Contrôle précis des acces : offre un contrôle très granulaire, permet de définir des règles d'acces spécifiques pour chaque fichier, processus et utilisateur, ce qui est particulièrement utile pour les serveurs, ou la sécurité et l'isolation des services sont essentielles

Mais :

Difficile a configurer et a comprendre, gestion des contextes de sécurité et des politiques complexe, un mauvais reglage peut bloquer l'acces a des ressources essentielles

Certaines applications ne fonctionnent pas correctement avec SELinux active (ne sont pas conçues pour respecter les politiques de sécurités strictes

Maintenance accrue : la gestion des règles et des politiques de SELinux necessite une surveillance continue (surtout dans les systèmes evolutifs, ou des services et applications sont fréquemment ajoutes ou modifies)

Utilise donc pour limiter l'acces au serveur aux seuls répertoires et fichiers nécessaires (pour éviter que des vulnerabilites compromettent tout le système)

Active par defaut pour Rocky, car souvent utilise un environnement d'entreprise nécessitant de controles de sécurité eleves

Desactive par defaut pour Debian (utiliser plutôt AppArmor, similaire mais plus simple a configurer)

AppArmor est un module de sécurité pour Linux qui fournit un contrôle d'acces base sur des profils, pour restreindre les actions des applications

Il permet aux administrateurs système de définir précisément quelles ressources chaque application peut utiliser (quels fichiers, répertoires et fonctionnalités reseau)

AppArmor est concu pour ajouter une couche de sécurité, sans nécessiter de configurations complexes : il offre une alternative pus simple a SELinux

Des profils sont utilises pour définir les permissions d'acces des applications

Ces profils peuvent être en mode strict (limite les acces de l'application), ou complaisant (genere des logs sans restreindre l'application, pour tester le profils)

Les profils décrivent les fichiers, répertoires, sockets et autres ressources qu'une application peut lire, écrire ou executer

AppArmor fonctionne de façon similaire a un pare-feu

Mais au lieu de contrôler le trafic reseau, il contrôle les acces des applications aux ressources du systeme

Les profils peuvent être très précis ou génériques (par exemple, limiter l'acces aux fichiers de configurations et aux répertoires publics, bloque completement l'acces aux fichiers système sensibles)

AppArmor est plus simple a configurer que SELinux : les profils sont bases sur des chemins de ifchier, l'ecriture des règles est ainsi plus simple et intuitive (même pour les administrateurs ayant peu d'experience avec les modules de sécurité)

Contrôle granulaire : restreint les actions des applications de manière fine (par exemple, une application peut être autorisee a lire un fichier specifique, mais pas a le modifier)

Prêt a l'emploi : Debian est installe avec des profils AppArmor predefinis pour les applications courantes (serveur par exemple), ce quie simplifie encore plus la sécurité de base

Basé sur les chemins : se base sur les chemins des fichiers pour appliquer les règles « pose des problèmes de sécurité si les chemins sont modifies ou si des liens symboliques sont utilises. AppArmor n'est donc pas aussi flexible que SELinux dans des environnements ou les fichiers peuvent changer de place ou si des liens sont utilises

Couverture limitee pour des environnements multi-utilisateurs complexes ou pour des serveurs nécessitant des politiques de sécurité avancees

Support limite sur Rocky par exemple

AppArmor est donc plus simple a configurer et a utiliser que SELinux, est utilise pour des serveurs simples ou une sécurité de base est nécessaire, et est supporte par Debian (mais moins pour Rocky, utiliser SELinux a la place dans ce cas)

Un domaine est une structure qui organise et gere un ensemble de ressources (ordinateurs, utilisateurs, imprimantes, etc) sous une identite commune

Ils sont souvent utilisés dans le cadre d'un réseau d'entreprise ou d'une organisation

Cela implique la mise en place d'un controleur de domaine avec des configurations spécifiques pour la gestion des utilisateurs, des groupes et des permissions

Un domaine pour un serveur installe pour un usage specifique n'est généralement pas nécessaire (cela est plis adapte pour les serveurs gérant de nombreux utilisateurs et ressources

Cela requiert aussi une maintenance supplementaire, pour l'authentification des utilisateurs notamment

Un compte utilisateur sera aussi créé. Il sera utilisé pour les activités non administratives

Creer au minimum 2 partitions chiffrees en utilisant LVM (Logical Volume Manager)

LVM permet de gérer l'espace disque de manière flexible et dynamique : redimensionner, ajouter ou supprimer des partitions (volumes logiques) sans avoir a redémarrer le système ou a reconfigurer manuellement les partitions, ce qui simplifie la gestion du stockage

Trois concepts de base :

PV (Physical Volumes) : disques physiques, partition de disque sur lesquels LVM est configure. Un disque dur ou une partition peut être converti en Physical Volume

VG (Volume Groups) : regroupement de plusieurs Physical Volumes : unité principale de stockage dans LVM, permet de combiner plusieurs disques physiques en un seul espace de stockage logique

LV (Logical Volumes) : partitions créées a l'interieur des VG (Volumes Groups). Ces volumes logiques peuvent être facilement redimensionnes, ajoutes ou supprimes

Partie obligatoire :

Partition disks :

Pour des soucis de gestion, d'organisation des données et de sécurité, nous allons partitionner le disque en plusieurs parties

Cela permettra d'isoler le système d'exploitation sur une partition, pour pouvoir mettre a jour ou réinstaller le système d'exploitation sans affecter les donnes

D'organiser le disque par type de donnees (système, utilisateur, sauvegardes, etc), ce qui facilite la gestion et la recherche de fichiers spécifiques

D'isoler les fichiers système des fichiers utilisateurs (si le système d'exploitation est compromis ou corrompu, les donnes de l'utilisateur resteront intactes sur une autre partition (simplifie la recuperation des fichiers)

De pouvoir chiffrer des partitions spécifiques, contenant des donnees sensibles de l'utilisateur par exemple, sans affecter l'ensemble du disque. Cela ameliore la sécurité tout en limitant l'impact sur les performances

D'optimiser les performances :

Sur les systèmes Linux, une partition swap peut être cree pour gérer la mémoire virtuelle : cette partition sert de prolongement a la mémoire RAM, en stockant temporairement des donnees en cas de besoin

Système de fichiers optimises : On peut choisir différents systèmes de fichiers en fonction des types de donnees (un système de fichiers rapides pour une partition utilisee comme base de donnees, un système de fichier plus robuste pour les sauvegardes

Gestion des ressources et facilite de maintenance :

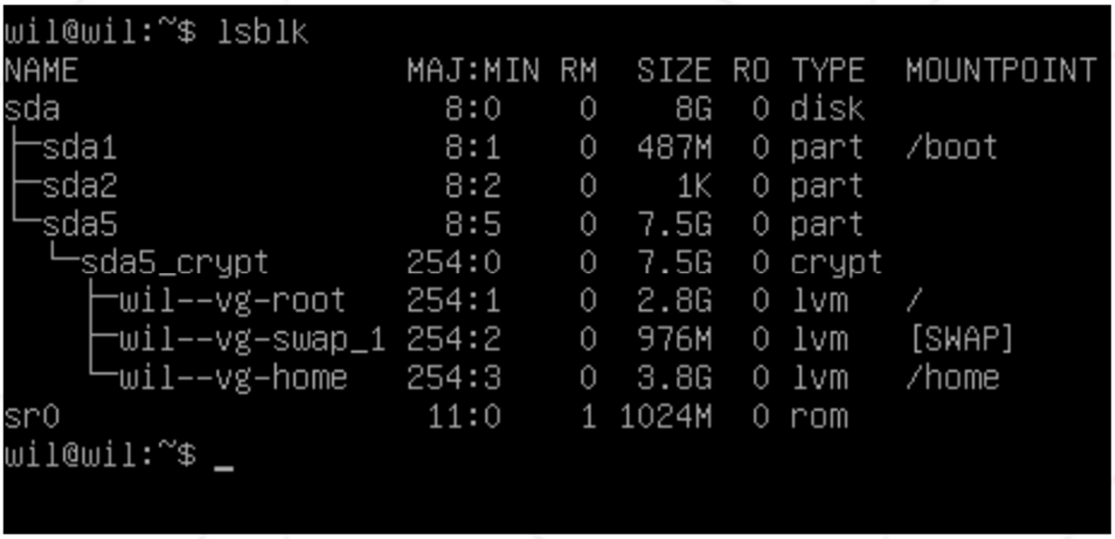
Contrôle de l'espace disque : on peut allouer une quantite specifique d'espace disque pour différentes utilisations (limiter l'espace pour la partition racine pour éviter que les fichiers système ne prennent pas trop de place et affecte les autres donnees par exemple)

Facilite les sauvegardes et les snapshots pour certaines parties du système, sans avoir a sauvegarder l'ensemble du disque

Isole les pannes (si une partition est corrompue ou presente des erreurs, les autres partitions ne peuvent pas être affectees). Cela minimise les risques d'endommagement de l'ensemble du disque et facilite le diagnostic et la reparation

Réduit les pertes de donnees : en cas de corruption des fichiers systemes, les donnees utilisateur peuvent être protegees sur une partition separee, ce qui limite l'etendue des pertes de donnees

Pour la partie obligatoire, voici la partition attendue pour la VM :



PV, VG et LV sont les éléments de base du système LVM (Logical Volume Manager) dans Linux

Ils permettent de gérer l'espace disque de manière flexible, en creant une couche d'abstraction entre le materiel et le système de fichiers

PV (Physical Volume) : disque physique ou partition de disque, configure pour être utilise par LVM

C'est la base du stockage dans LVM : les disques physiques (ou partitions) sont d'abord convertis en Physical Volumes, pour permettre à LVM de les gérer

Le disque physique sda (techniquement, c'est un disque virtuel géré par VirtualBox, mais il est présenté comme un disque physique à Debian) est un PV (Physical Volume)

sda1, sda2 et sda5 sont des partitions de sda

Tous sont donc des PV, mais sda est un disk (disque entier, physique ou virtuel), et sda1, sda2 et sda5 sont des part (partitions) du disque sda

sda5_crypt est aussi un PV, mais de type crypt (voir plus bas)

VG : Volume Group : regroupement de plusieurs Physical Volumes (PV), qui est l'unité de stockage logique principale dans LVM

Ils permettent de combiner plusieurs PV pour créer un espace de stockage commun et unifie

Une fois un PV ajoute a un VG, l'espace du PV est disponible pour créer des LV

Remarque : il est aussi possible de combiner 2 PV en un seul VG, ce qui utilisera alors l'espace total disponible sur ces deux disques (cela n'est pas le cas ici)

Les VG permettent d'agreger l'espace de plusieurs disques physique, ce qui facilite l'expamsion de l'espace de stockage

Ainsi, si on ajoute un nouveau disque, on peut alors simplement l'ajouter au VG pour augmenter l'espace disponible

Les VG sont creees a partir d'un (ou de plusieurs) PV

Ici, le VG wil-vg a été cree a partir du PV sda5_crypt

LV (Logical Volume) : c'est une unite de stockage logique créée a partir de l'espace disponible dans un VG

Un LV est l'equivalent d'une partition traditionnelle, mais avec beaucoup plus de flexibilité : un LV est cree a partir de l'espace disponible dans un VG, et peut être redimensione facilement (tout comme le VG dont il dépend)

Les LV correspondent aux volumes que l'on monte ou que l'on utilise comme des partitions normales (PV), mais il est possible, contrairement aux PV, de les redimensionner, des les supprimer et d'en créer de nouveaux sans affecter les disques physiques (PV) sous-jacents

Ici, les LV sont root, swap_1 et home (le type lvm signifie : LV créé avec LVM)

Ils font tous partie du VG wil-vg

Remarque : sr0 est de type **rom**, ce qui indique un lecteur optique (un lecteur de CD/DVD). Ce n'est ni pas un PV (il ne fait pas partie du système de stockage de LVM)

C'est le peripherique attribue par Linux pour le premier lecteur de disque optique (CD, DVD ou Blu-ray) connecte au système

Les périphériques sont representes par Linux par des fichiers spéciaux dans le repertoire /dev

/dev/sr0 est le fichier de peripherique pour accéder au premier lecteur optique

sr signifie SCSI ROM, et 0 indique que c'est le premier lecteur optique detecte par le systeme

La taille correspond a la taille du media insere : ici, 1 Go est insere dans le lecteur (ou une estimation fournie par le système si aucun disque n'a été insere, comme une valeur par defaut

Le type rom signifie que ce peripherique est de type Read Only Memory (ROM), mémoire en lecture seule

Remarque : meme si des disques reinscriptibles existent, le perihperique de lecture reste typiquement identifie comme de type rom (sa fonction principale est la lecture de donnees)

Cela aide a différencier les périphériques optiques de lecture des disques ou partitions classiques (disk ou part)

C'est un périphérique amovible (RM : 1) (voir plus bas)

R0 est à 0, ce qui indique que ce peripherique n'est pas en lecture seule : il est capable d'ecrire sur le CD-ROM ou DVD-ROM si le media le permet

Ici, la commande lsblk a été executee pour afficher les informations detaillees sur les peripheriques de stockage de type bloc (les disques durs, les partitions et les volumes logiques)

Cette commande montre comment les disques, partitions, les volumes LVM et les partitions chiffrees sont organises entre eux, en utilisant une hierarchie

Elle donne des informations comme le nom, la taille, le type, et le point de montage de chaque peripherique

Elle indique également si le peripherique est en lecture seule, amovible, ou chiffre

Les points de montage (voir plus bas) sont aussi indiques : cela indique ou chaque partition ou volume est monte dans le système de fichiers

sda represente le disque dur (ou SSD) entier : il s'agit du premier disque detecte par le système

sd signifie SCSI Disk (ce terme est utilise pour tous les types de disques modernes, même les disques SATA ou NVMe)

Small Computer System Interface (SCSI) est un dispositif de transmission de données qui sert à relier par câble deux ordinateurs entre eux ou un ordinateur avec un périphérique externe

a signifie qu'il s'agit du premier disque detecte (le deuxième disque serait sdb par exemple)

sda1 est la premiere partition du disque sda

C'est une partition principale

Un disque formate avec un schema de partitionnement MBR (Master Boot Record), comme sda, peut contenir jusqu'à 4 partitions principales maximum : elles sont utilisees pour installer des systèmes d'exploitation ou stocker des donnees

MBR est un système de partition et de démarrage utilise pour organiser les disques et démarrer le système d'exploitation

On sait que sda1 est une partition principale (la premiere de sda) car sda1, sda2, sda3 et sda4 sont des partitions principales

sda2 est la deuxième partition du disque sda

C'est aussi une partition principale

Elle est creee automatiquement par les outils de partitionnement lorsqu'une partition logique est cree sur un disque utilisant le schema MBR

En effet, pour créer une partition logique, une partition principale doit être creee et transformee en partition étendue

Elle agit comme un conteneur pour les partitions logiques

Elle ne contient pas de donnees en elles-memes, elle sert uniquement de structure pour organiser les partitions logiques qu'elle contient (c'est pourquoi elle est souvent affichee avec une taille de 1K, ce qui correspond a un espace minimal reserve pour marquer le début de la partition étendue)

Elle est cree automatiquement, et est notee sda2 si sda1 existe déjà

sda5 est la cinquieme partition du disque sda

C'est une partition logique

La difference avec une partition principale est que, contrairement a cette dernière, qui est reservee pour les systèmes d'exploitation ou les partitions de démarrage, la partition logique est destinee aux donnees supplémentaires, ou pour des partitions ne nécessitant pas d'etre demarrees directement. De plus, il n'y a pas de limitations pour la creation de partitions logiques (alors que seulement 4 partitions principales (3 si des partitions logiques sont aussi creees) peuvent être creees au max)

Un point de montage est un repertoire dans le système de fichiers ou un peripherique (une partition de disque par exemple) est accessible et integre dans la hiérarchie du système de fichiers

C'est donc l'endroit ou le contenu de la partition est rendu visibleet utilisable par le système d'exploitation et l'utilisateur

Contrairement a Windows, il n'y a pas de lettre de lecteur comme C : ou D :

Le système est structure comme un arbre unique avec la racine / au sommer

Chaque peripherique ou partition supplementaire est monte dans cette arbre, dans un repertoire specifique appele point de montage

Le contenu de ce perihperique apparait dans le repertoire du point de montage : si on demonte le perihperique, le repertoire devient vide

Exemples :

/ est le point de montage racine, ou le système de fichiers principal est monte : toutes les autres partitions ou perihperiques montes apparaissent comme des sous-repertoires de /

/home est utilise pour monter une partition dediee aux fichiers des utilisateurs, pour que leurs donnees personnelles soient separees du systemee principal

/boot est monte sur une partition separee contenant les fichiers nécessaires au démarrage du système, comme le noyau

Les points de montages sont utilises pour structurer le système de fichiers, pour séparer le système, les donnees utilisateur et les sauvegardes. Cela facilite la gestion, les sauvegardes et les restaurations

Il est facile de monter et démonter des perihperiques dans différents répertoires, pour ajouter ou retirer de l'espace de stockage selon les besoins, sans affecter le reste du système de fichiers

Il est aussi possible de définir des permissions et des configurations spécifiques pour chaque repertoire monte : un système peut donc restreindre l'acces en ecriture a certains points de montage par exemple, pour des raisons de securite

Cela permet aussi de gérer les ressources de dtockage de manière plus efficace, de redimensionner ou de remplacer certaines partitions sans impacter les autres

Dans la commande lsblk, les colonnes MAJ:MIN représentent les numéros majeurs et mineurs associes aux périphériques de stockage

Ces numéros sont utilises par le noyau Linux pour identifier et gérer les périphériques de manière unique

MAJ : numero majeur

Tous les disques durs SATA ou SCSI sont généralement associes au numero majeur 8

MIN : numero mineur

Le numero mineur identifie chaque instance d'un type de perihperique

Si plusieurs disques durs (ou partitions) sont connectes, chacun aura un numero mineur different

sda 8:0 signifie que sda est un disque SCSI/SATA, et c'est le premier disque de ce type

sda1 8:1 signifie que sda1 est un disque SCSI/SATA, et c'est la premiere partition de sda

sda5 8:5 signifie que sda5 est un disque SCSI/SATA, et c'est la premiere partition logique de sda (car les partitions logiques commencent par 5)

sda1 est la premiere partition de sda, de taille 487 Mo, avec comme point de montage /boot

C'est une pratique courante dans les systèmes Linux, pour plusieurs raisons liees a la gestion, la sécurité et la compatibilite du demarrage

La partition /boot stocke les fichiers essentiels au démarrage du système, comme le noyau Linux, l'image disque initiale et le chargeur d'amorcage (GRUB)

En isolant ces fichiers critiques dans une partition dediee, on réduit le risque de corruption accidentelle causee par d'autres operations sur le systeme

Si le système de fichiers principal est endommage ou inaccessible, la partition /boot separee reste intacte, ce qui peut faciliter la recuperation et le depannage du système

Il est aussi courant de laisse la partition /boot non chifree, même si le reste du système est chiffre (comme cela sera le cas pour le serveur)

Cela permet au chargeur d'amorcage GRUB (charge le kernel en mémoire pour démarrer le système d'exploitation) d'acceder aux fichiers de démarrage nécessaires avant de dechiffrer et de monter le reste du systeme

Une partition de 500 Mo est suffisante pour plusieurs noyaux et chargeurs d'amorcage sans encombrer les système de fichiers principal

La colonne RM indique si le perihperique est amovible (comme une cle usb ou un disque dur externe) : 0 signifie que le peripherique n'est pas amovible (fixe), 1 signifie que le peripherique est amovible

La colonne RO (Read Only) indique si le perihperique est en lecture seule : 0 signifie qu'il est en lecture / ecriture (il est possible de lire et d'ecrire dessus), 1 signifie que le peripherique est en lecture seule (on peut lire les donnees, mais pas écrire)

MAJ:MIN : 11:0

11 (MAJ) est associe aux peripheriques de type rom (lecteurs optiques) (sr0)

0 indique que c'est le premier lecteur optique detecte par le système

Crypter la partition sda5 est une mesure de sécurité visant a protéger les donnees sensibles sur cette partition

Si l'ordinateur ou le disque dur est volé, les donnees non chiffrees peuvent être facilement accessibles en connectant le disque a un autre ordinateur

En chiffrant sda5, les donnees ne peuvent être lues qu'avec la cle de chiffrement, ce qui rend l'acces beaucoup plus difficile pour une personne non autorisee

Cela permet de sécuriser les informations sensobles

Les donnees utilisateurs motamment (fichiers personnels et de configurations) sont souvent stockes sur une partition dediee (comme /home), qui peut être situee sur sda5 (comme c'est le cas ici)

En chiffrant cette partition, on protege tous les fichiers utilisateurs de manière centralisee

Meme si quelqu'un tente d'acceder au disque en dehors du système, le chiffrement garantit que le contenu reste chiffré et protégé. Même des attques de recuperation de donnees (par clonage ou manipulation de disque) seraient bloquees par le chiffrement)

Les snapshots ou sauvegardes de cette partition restent aussi protegees et chifrees : les sauvegardes seront inutilisables sans la clé de déchiffrement, les copies resteront ainsi sécurisées, même stockées sur un emplacement externe

Tous les volumes logiques LVM créés à l'intérieur de sda5_crypt seront chifrées : cette configuration est courante dans les systèmes Linux

Toutes les donnees des volumes logiques (root /, swap et home) sont chifreees en une seule operation, ce qui simplifie la gestion du chiffrement

Les fichiers système sensible et les donnees utilisateur bénéficient ainsi due chiffrement

sda5_crypt est une partition cryptee de sda5

Elle utilise sda5 comme conteneur : sda5 est ainsi une partition logique sur le disque

C'est un volume chiffré créé a l'intereur de sda5 en utilisant un logiciel de chiffrement

La partition sda5 est tout d'abord formatee pour le chiffrement, puis un conteneur chiffre est cree sur sda5, ce qui cree une couche de sécurité sur la partition

Une fois deverouille, sda5_crypt peut être utilise comme un volume non chiffre pour le système, permettant la creation de LV dans un VG

254:0 sont des périphériques mappes par le peripherique (Device-mapper)

Le numero majeur 254 est souvent utilise pour les volumes logiques (LV) ou chiffres

Ainsi, le 1er peripherique chiffre est sda5_crypt, et les suivants sont les LV de ce peripherique

La partition root (/) contient le système d'exploitation en lui-meme, y compris tous les fichiers système, les applications installees et les bibliothèques nécessaires au fonctionnement du système

Créer une partition dediee pour la racine permet d'isoler les fichiers systèmes des donnees de l'utilisateur, pour éviter que les fichiers personnels ou les erreurs de l'utilisateur n'affectent directement les fichiers système critiques, de protéger les fichiers systèmes en cas de corruption ou probleme dans une autre partition (comme /home), et de faciliter la maintenance et les mises a jour

La partition swap est utilisee quant à elle conne mémoire virtuelle pour compléter la RAM (mémoire vive) lorsqu'elle est saturée

Le swap est utile pour les operations nécessitant beaucoup de mémoire ou pour éviter les plantages en cas de surcharge de la RAM

Les donnees sont stockees temporairement dans la partition swap lorsque la RAM est epuisee, pour éviter les erreurs de mémoire insuffisante

Elle peut aussi être utilisee pour l'hibernation : le contenu de la RAM peut être enregistre dans le swap pour pouvoir être restaure au demarrage

La partition /home contient les fichiers personnels de chaque utilisateur du système, y compris les documents, les configurations personnelles, et les paramètres des applications

La separation de la partie /home et de la partie /root permet de faciliter la gestion des donnees personnelles et réduit le risque de pertes de donnees lors de la modification du système, facilite la sauvegarde et la restauration, indépendamment du reste de système (protection des donnees utilisateur)

De plus, lors de la réinstallation ou de la mise a niveau du système d'exploitation, la partition /home peut être conservee sans être formatee, ce qui permet aux utilisateurs de retrouver leurs donnees et configurations après la réinstallation

Enfin, la partition /home permet de gérer l’espace disque de chacun des utilisateurs de manière flexible et de contrôler plus facilement les quotas ou les sauvegardes

Isolation des données : En isolant le système, les fichiers personnels, et la mémoire virtuelle, chaque partie du système est protégée en cas de problème sur une autre partition.

Facilité de gestion des ressources : La partition swap offre un espace de mémoire virtuel dédié, tandis que root et home ont leurs propres espaces réservés pour leurs besoins spécifiques.

Sécurité et stabilité : En cas de corruption de la partition root, les données utilisateurs restent intactes dans /home, et inversement.

Flexibilité lors de l’allocation d’espace : Vous pouvez redimensionner, formater ou migrer chaque partition séparément, ce qui rend la gestion du disque plus flexible.

Optimisation des performances : Les partitions séparées permettent de configurer chaque partition avec des options optimales (par exemple, la partition swap peut être positionnée pour un accès rapide, et le système de fichiers de /home peut être ajusté pour des performances adaptées aux fichiers personnels).

Gestion des quotas d'utilisateur : Dans un environnement multi-utilisateurs, la partition /home séparée permet de gérer plus facilement l'espace disque attribué à chaque utilisateur, notamment avec l'usage de quotas.

Partitionner en **root (/)**, **swap**, et **home (/home)** permet de structurer le système de manière efficace et sécurisée :

- **Root** (/) : Pour le système et les fichiers critiques.
- **Swap** : Pour la mémoire virtuelle et l'hibernation.
- **Home** (/home) : Pour les données personnelles des utilisateurs.

Cette approche améliore la sécurité, la gestion des données, la flexibilité de maintenance, et la récupération en cas de panne, tout en optimisant les performances et la stabilité du système.

Un volume iSCI est un type de stockage reseau qui utilise le protocole iSCI (Internet Small Computer Systems Interface) pour permettre aux ordinateurs de se connecter à des périphériques de stockage distants via un reseau, comme s’ils étaient connectes directement au niveau materiel

SCSI2 (0,0,0) (sda) – 21.5 GB ATA VBOX HARDDISK

SCSI2 indique que le disque est présenté via une interface SCSI virtuelle, émulée par l'hyperviseur (VirtualBox dans ce cas)

(0,0,0) représente l'identifiant SCSI du disque dans la machine virtuelle (controleur, bus, unite)

Chaque nombre represente un composant de l'adresse du peripherique virtuel

(sda) est le nom du perihperique attribue par l'OS invite (l'OS a l'interieur de la VM, Debian donc) : sda est le premier disque detecte

21.5 GB : la taille totale du disque (définie lors de la configuration de la VM)

ATA : type d'interface de disque presente dans la VM (Advanced Technology Attachment) : une interface commune pour les disques durs

VBOX HARDDISK : le disque virtuel est géré par VirtualBox (nom par defaut donne par VirtualBox aux disques virtuels)

pri/log 21.5 GB FREE SPACE

pri/log : partition principale (primary) / partition logique (logical)

Indique que l'espace libre peut être utilise pour creeer des partitions principales et des partitions logiques

21.5 GB : 21.5 GB sont disponibles sur le disque

FREE SPACE : cet espace n'est pas actuellement utilisé ou alloué à une parition

L'acces aux donnees situees au début du disque peuvent offrir des vitesses d'acces légèrement plus rapides

Ainsi, les premiers secteurs peuvent être reserves aux partitions nécessitant un acces rapide, comme les partitions systèmes (/ ou /boot)

La fin peut être reservee aux donnees moins dritiques (/home par exemple)

Ext4 journaling file system est un système de fichiers populaire sous Linux, souvent choisi pour son journaling et ses améliorations en matière de performance, de stabilité et de gestion de grandes partitions et fichiers

Le journaling ajoute une couche de protection contre la corruption des données : lorsqu'une opération de modification des fichiers est sur le point d'etre executee (ecriture, suppression ou deplacement d'un fichier), le système enregistre d'abord l'operation dans un journal avant de la réaliser

Ainsi, en cas de panne, on peut se référer au journal pour revenir a un etat coherent

La performance est aussi ameloiree car Ext4 conserve les donnees temporairement en mémoire, pour les écrire plus efficacement par la suite : reduction de la fragmentation

Plusieurs blocs sont regroupes dans un seul segment logique, ce qui ameliore l'acces aux fichiers volumineux

Les partitions peuvent aller jusqu'à 1 EiB, et les fichiers individuels jusqu'à 16 TiB

dm-crypt est une infrastructure intégrée au noyau Linux qui fournir une couche de chiffrement bas niveau pour des volumes de stockage

Elle est utilisée en conjonction avec LUKS (Linux Unified Key Setup) pour créer des volumes chiffrés, et déchiffre les données à la volée (lorsqu'elles sont lues ou écrites)

AES est un algoruthme de chiffrement largement utilisé, connu pour être rapide et efficace. C'est le standard de chiffrement par défaut adopté par de nombreux systèmes, y compris Linux, en raison de ses performances elevees et de son niveau de sécurité connu

Key size est la longueur de la cle de chiffrement utilisee par l'algorithme AES. Les tailles courantes sont 128, 192 et 236 bits

Plus la cle est longue, plus le chiffrement est securise

IV (Initialization Vector) est une methode qui permet de varier le chiffrement en ajoutant un vecteur initial unique pour chaque bloc de données, empêchant la creation de motifs identiques dans les donnees chiffrées

Même si le même bloc de donnees est chiffre plusieurs fois, le resultat chiffre sera different a chaque fois

Pour dm-crypt, le mode e chiffrement utilise pour IV est souvent xt, bien securise et bien adapte au chiffrement de disque

La passphrase est une phrase secrete ou un mot de passse utilise pour accéder au volume chiffre. Elle est souvent convertie en une cle cryptographique (en utilisant un processus de derivation de cle) pour deverouiller le volume chiffre

Attention : si la passphrase est perdue, les donnees deviennent inaccessibles

Pour une partition chiffree, le marquage bootable flag doit être indiquer pour que le système de démarrage (GRUB par exemple) puisse accéder a cette partition chiffree

Le point de montage /var (Variable Data) stocke les données variables qui changent fréquemment ou qui sont générées dynamiquement par le système

Cette séparation permet de préserver les données dynamiques en cas de crash du système, tout en isolant les données variables pour éviter qu'elles n'encombrent la partition principale

Le point de montage /srv contient les données spécifiques aux services fournis par le serveur. Cela inclus les fichiers utilisés par les services zeb, FTP ou autres

Organiser les données des services réseau permet de faciliter la gestion, la sauvegarde et la restauration

Le point de montage /tmp permet de stocker els fichiers temporaires créés par le système ou les applications (par les programmes ou les scripts, les sessions de navigation, les fichiers de travail intermédiaires...)

Son contenu est souvent effacé automatiquement lors du redémarrage système, ou périodiquement par le système

Tout utilisateur peut lire et écrire dans /tmp, mais les permissions protègent les fichiers des autres utilisateurs

Cette séparation permet d'éviter que les fichiers temporaires encombrent la partition principale ou persistent inutilement après leur utilisation

Le point de montage /var/log est dédié au stockage des logs (journaux système et applicatifs). C'est un sous-répertoire de /var

Exemple de contenu :

- les logs systèmes : fichiers comme syslog (messages systèmes généraux) ou dmesg (messages du kernel, du noyau)
- les logs des services : les journaux des serveurs web, des bases de données, etc
- Les logs d'authentification : historique de connexions et des tentatives d'accès au système

Cette séparation facilite la gestion et la surveillance des logs

Ces fichiers sont cruciaux pour le diagnostic et la sécurité : leur isolement permet de mieux les protéger et les organiser

Configure the package manager

Scanning your installation media finds the label:

Debian GNU/Linux 12.8.0 _Bookworm_ - Official amd64 NETINST with firmware 20241109-11:04

You now have the option of scanning additional media for use by the package manager (apt)

Normally, these should be from the same set as the one you booted from

If you do not have additional media, this step can just be skipped

If you wish to scam more media, please insert another one mow

Scan extra installation media ?

Ce message apparait pendant l'installation de Debian, et concerne la configuration du gestionnaire de paquets (apt) pour installer des logiciels et des mises à jour

L'installation est basée sur une image d'installation (l'iso), qui contient un certain nombre de paquets

Ce message demande si l'on veut scanner d'autres supports d'installation (CX/DVD/USB) pour élargir les sources de logiciels disponibles pendant l'installation

L’image NETINST mentionnée est une version minimale de Debian

Elle contient uniquement les fichiers nécessaires pour démarrer et installer un système de base

On peut donc ignorer cette étape, car on veut une installation minimale

De plus, nous pourrons toujours utiliser les dépôts en ligne une fois l’installation terminée

Package manager :

Le package manager APT (Advanced Package Tool) est un gestionnaire de paquets utilisé sur les systèmes basés sur Debian (Debian et Ubuntu par exemple)

Il facilite la gestion des logiciels installés sur un système Linux en automatisant les taches liées aux paquets (leur installation, leur mise à jour, leur suppression et la gestion des dépendances)

Il installe les logiciels en téléchargeant les paquets nécessaires depuis des dépôts en ligne ou des supports locaux (CD ou DVD)

Il peut aussi mettre à jour un logiciel spécifique ou l’ensemble du système en vérifiant les nouvelles versions des paquets dans les dépôts

Il peut aussi supprimer un logiciel, tout en gérant ses dépendances non utilisées

Il gère automatiquement les dépendances des logiciels : si un paquet nécessite d’autres paquets pour fonctionner, APT les télécharge et les installe automatiquement

Les paquets gérés par APT proviennent de dépôts qui sont des serveurs contenant des logiciels compatibles avec la distribution (Debian par exemple)

Il est aussi possible de télécharger un paquet sans l’installer grâce à APT

APT est donc automatisé, sécurisé (sources vérifiées), commode, et fiable

Aptitude est aussi un gestionnaire de paquets, et possède des fonctions similaires à APT, mais a des différences notables en termes de fonctionnalités, d'utilisation et de présentation

Aptitude est une surcouche à APT, qui fournit une interface plus conviviale, avec des fonctionnalités avancées pour la gestion des paquets

Il peut être utilisé à la fois en mode ligne de commande et avec une interface semi-graphique dans le terminal

Il permet de gérer plus finement les dépendances, avec la possibilité de résoudre automatiquement les conflits

Il possède aussi un historique des actions : il est donc plus facile de voir quelles actions ont été entreprises sur les paquets

Il suggère aussi des solutions alternatives en cas de conflits entre paquets

Il offre donc plus de contrôle et de détails qu'APT, mais il peut être plus difficile à utiliser pour des utilisateurs non expérimentés

APT doit être utilisé pour des taches simples, pour installer et mettre à jour des paquets rapidement

Un miroir est un serveur qui héberge une copie exacte des fichiers d'un autre serveur

Ces fichiers, ici, sont les ressources pour installer Debian

Les miroirs permettent de dupliquer les fichiers d'un serveur principal vers plusieurs serveurs, situés à plusieurs endroits

Cela garantit que les utilisateurs peuvent accéder aux fichiers, même si le serveur principal est hors ligne ou surchargé

De plus, en utilisant un miroir géographiquement proche, les utilisateurs peuvent télécharger plus rapidement les fichiers nécessaires (car la latence et les temps de transferts sont réduits)

Les miroirs répartissent, de plus, la charge de trafic réseau entre plusieurs serveurs, ce qui evite de surcharger un seul serveur

Enfin, si le serveur principal rencontre un problème technique, les miroirs garantissent la disponibilité continue des fichiers

Le miroir deb.debian.org est un service de redirection intelligent (powered by Fastly CDN) qui diriige la requête vers un miroir proche et performant

Il utilise un système distribué (CDN) pour fournir des paquets à partir de serveurs situés partout dans le monde

Il est donc automatique (sélectionne automatiquement un miroir rapide et disponible), global (redirection selon la proximité géographique des miroirs disponibles), et fiable (maintenu directement par Debian, via des miroirs officiels vérifiés

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank

The proxy information should be given in the standard form of :
“http://[user][:pass]@]host[:port]/”

HTTP proxy information (leave blank for none) :

Ce message demande si le système a besoin d’utiliser un proxy http pour se connecter à internet pendant l’installation de Debian

Si l’on est dans un environnement ou un proxy est requis (serveur d’entreprise ou protégé derrière un pare-feu), il faut indiquer les détails du proxy dans le format spécifié

Un proxy http agit comme un intermédiaire entre le système et internet, et est souvent utilisé pour surveiller et filtrer le trafic, restreindre ou autoriser l’accès à certains sites, accélérer les requetes repetees en mettant en cache les ressources souvent accédées, et cacher l’IP du client (en faisant apparaitre les requetes comme si elles provenaient du serveur proxy, et non du client)

Si on utilise une connexion internet directe, ou si un proxy n’est pas nécessaire pour accéder à internet, il faut laisser ce champ vide

Participate in the package usage survey ?

Le popularity-contest package, activé avec cette option, collecte des données anonymes à propos des packages installés sur le système et leur fréquence d'utilisation

Cela aide les développeurs Debian à savoir quels packages sont le plus souvent utilisés, pour qu'ils puissent prioriser leur support, leur mise à jour et leur amélioration

Software selection :

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections od software

Choose software to install

Ce message demande si l'on veut installer des collections de logiciels additionnelles, comme un environnement de bureau, des outils de serveur, etc

Pour l'instant, seul le système minimal de base est installé

Il est possible, à cette étape, d'installer des collections de logiciels

ATTENTION : décocher tout ce qui est déjà coché (Debian desktop environment, GNOME et standard system utilities), car on veut installer le minimum de services et pas d'interface graphique

Permet de reduire l'utilisation des ressources : les interfaces graphiques et les services supplémentaires consomment de la mémoire, du CPU et de l'espace disque

Les ressources sont ainsi libérees pour les taches essentielles du serveur

Meilleures performances pour les applications critiques (on maximise l'effacite et la rapidité en allouant toutes les ressources au serveur)

Amelioration de la sécurité : en limitant les services, on réduit la surface d'attaque du serveur (moins de points potentiels de vulnerabilite) : ainsi, le serveur est plus difficile a compromettre

Moins de mises a jour a effectuer, moins de risque d'introduire de nouvelles vulnerabilites

Gestion plus facile, maintenance réduite : configuration plus simple, moins sujette aux conflits ou aux erreurs

Moins de logs a surveiller, moins de dependances a gérer, moins de risque de defaillance d'un service secondaire qui pourrait affecter le serveur principal

Mises a jour plus rapides, plus faciles a planifier

Deploiement plus rapide et leger, démarrage et sauvegardes rapides, taille de l'image système reduite

Moins de dependances lors des migrations

Les systèmes Linux sont conçus pour fonctionner de manière modulaire, en installant seulement les services nécessaires pour une tache specifique (système dedie et fiable)

Maitrise complete en ligne de commande : encourage l'utilisation de la ligne de commande, plus puissante et flexible pour l'administration a distance : automatisation et gestion des serveurs plus efficace, avec des scripts et des outils de gestion de configuration

Debian desktop environment est une option proposée lors de l'installation de Debian pour installer un environnement graphique complet (GUI, Graphical User Interface) sur le système

Cela pernet d'interagir avec le système via une interface visuelle plutôt qu'avec le ligne de commande

Cela inclus aussi Firefox, LibreOffice, Nautilus (gestionnaire de fichiers), etc

Cela est inutile si l'on configure un serveur avec un système minimal sans applications préinstallées

GNOME :

GNOME (GNU Network Object Model Environment) est un des environnements de bureau les plus populaires pour Linux

Il fournit une interface graphique complète et intuitive pour interagir avec les système d'exploitation, sans nécessiter d'utiliser les lignes de commandes

Il est livré avec un gestionnaire de fichiers, un navigateur web, un terminal, un outil de gestion des paramètres système, un gestionnaire d'applications, etc.

Cela est aussi inutile si l'on configure un serveur avec un système minimal sans applications préinstallées

Standard system utilities :

Cette collection regroupe des programmes et outils essentiels pour gérer et maintenir un système Linix

Ils fournissent des fonctionnalités de base pour rendre le système opérationnel pour des taches courantes

Cela inclus des commandes comme ls, cp, mv, rm, cat, more, less, tar, unzip, ping, su, les IDE vim et nano, les commandes adduser, chmod, man, whoami, etc

Cela fournit les outils nécessaires pour surveiller les ressources système, diagnostiquer les problème, gérer les fichiers, les utilisateurs, effectuer des diagnostics réseau, exécuter des scripts shells, effectuer des operations de sauvegarde et de restauration, etc

Cela est aussi inutile si l'on configure un serveur avec un système minimal sans applications préinstallées

Certains de ces utilitaires nous sont inutiles, nous choisirons d'installer uniquement ceux qui nous seront utiles

Nous voulons en effet un système minimaliste entièrement personnalisé

GRUB (GNU Grand Unified Bootloader) est un chargeur d'amorçage open source

Il est essentiel pour les systèmes Linux

Il est responsable du démarrage du système en chargeant le noyau du système d'exploitation en mémoire et en transférant le contrôle à celui-ci

Le BIOS ou l'UEFI initialise le matériel et transfère le contrôle au chargeur d'amorcage (boot loader)GRUB prend le relais, localise le noyau du systeme (le kernel Linux dans ce cas) et le charge en memoire

Si plusieurs OS sont disponibles, GRUB permet à l'utilisateur de choisir celui à démarrer

Une fois chargé par GRUB, le noyau prend le contrôle et demarre le systeme

GRUB prend en charge le multiboot, est flexible (supporte une large gamme de systèmes de fichiers), permet de modifier les options de démarrage en temps réel, est personnalisable, et inclus même un mode de secours pour dépanner le système s'il est défectueux (en démarrant manuellement le noyau ou en réparant une configuration incorrecte)

Configure grub-pc :

It seems that this new installation is the only operating system on this computer

If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record)

Warning : if your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it

Install the GRUB boot loader to your primary drive ?

Ce message demande si l'on veut installer GRUB boot loader sur le disque dur primaire

Si Debian est le seul OS sur le système, GRUB est nécessaire pour le démarrer (boot)

Le disque primaire est typiquement le disque dur principal (/dev/sda)

Ce message indique aussi qu'aucun autre OS n'a été détecté sur la machine.

Cela est le cas si Debian est l'unique OS de cette machine

Si l'on autorise GRUB a être installé sur le disque principal, cela installera GRUB dans le MBR (Mater Boot Record) pour les systèmes BIOS

Le BIOS chargera ainsi le MBR, qui contiendra maintenant le code nécessaire pour charger le boot loader GRUB

En effet, MBR ne suffit pas pour booter Debian : MBR ne sait pa lire les systèmes de fichiers ext4, n'est pas capable de localiser et charger un noyau Linux, ni lui transmettre de paramètres

Cependant, pour des OS comme Windows, MBR seul est nécessaire (car le boot loader de Windows est intégré dans le boot sector, sur la partition système de Windows)

You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device

The usual way to de this is to install GRUB to your primary drive (UEFI partition/boot record)

You may instead install GRUB to a different drive (or partition), or to a removable media

Device for boot loader installation :

/dev/sda (ata-VBOX-HARDDISK-VB02d809df-3fce6ae1))

Cette étape permet de choisir le périphérique sur lequel sera installé GRUB boot loader

GRUB boot loader est nécessaire pour rendre le système bootable

Il permet au système de localiser et de charger l'OS (Debian dans ce cas) une fois le PC (la VM) demarree

L'installer suggere d'installer GRUB sur le disque primaire (/dev/sda), car c'est typiquement ou le système cherchera un peripherique bootable par defaut

Il est aussi possible de l'installer sur un autre peripherique (sdb par exemple) ou sur une partition specifique (sda1 par exemple), mais cela est utile seulement dans le cas d'une installation multi-disque, ou dans le cas de la preparation d'un peripherique removable (

Apres cette etape, GRUB sera installe sur le MBDR, et le BIOS chargera GRUB pour booter le systeme

L'affichage de tty1 apres l'installation de Debian signifie que l'on est connecte au terminal virtuel 1

Cela indique que système Linux a bien demarre et que ;on agit avec une console en mode texte, sans interface graphique

TTY signifie Teletypewriter

Cela designe un terminal virutel qui permet d'interagir avec le système via une interface en ligne de comamnde

C'est le mode console

Sur tty1, on peut se connecter en entrant le nom d’utilisateur et le mot de passe pour accéder a la session

Une fois connecte, on peut exécuter des commandes pour administrer le système, installer des logiciels ou configurer des services

6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

Cette chaine de texte fournit des informations sur le noyau Linux utilise par le système Debian :

6.1.0-27-amd64

6.1.0 : version principale du noyau Linux

La version est 6.1, une version stable du noyau Linux

-27 : Revision ou numero de build specifique a la distribution Debian

Cela indique que cette version du noyau a été modifiée ou empaquetée 27 fois pour Debian.

amd64 : architecture processeur

Cela signifie que le noyau est conçu pour les systèmes 64 bits basés sur l'architecture **x86_64** (compatible avec les processeurs AMD et Intel modernes).

#1 :

- Numéro de build.
- Indique que c'est la première compilation de cette version spécifique du noyau pour Debian.

SMP (Symmetric Multi-Processing) :

- Signifie que ce noyau est configuré pour tirer parti des processeurs multi-cœurs ou multi-threads.
- Cela optimise les performances sur les systèmes modernes avec plusieurs cœurs CPU.

PREEMPT_DYNAMIC :

- Indique que ce noyau prend en charge la préemption dynamique.
- **Préemption** : Capacité du noyau à interrompre des processus pour garantir des performances réactives, par exemple dans des scénarios critiques ou en temps réel.
- **Dynamique** : Le niveau de préemption peut être ajusté en fonction des besoins du système.

Debian 6.1.115-1 (2024-11-01) :

- **Debian** : Indique que ce noyau a été spécialement empaqueté et adapté pour Debian.
- **6.1.115-1** : Révision Debian du noyau.
    - **6.1.115** correspond à une mise à jour spécifique de la version 6.1 du noyau.
    - **-1** est la version du paquet Debian contenant ce noyau.
- **2024-11-01** : Date de compilation ou de publication de cette version du noyau.

x86_64 :

- Architecture matérielle pour laquelle le noyau est conçu.
- Cela signifie qu'il est compatible avec les processeurs 64 bits basés sur l'architecture x86.

Commande cat/etc/os-release

Cette commande affiche le contenu du fichier /etc/os-release, qui contient des informations importantes sur la distribution Linux installee

C'est un fichier standardise pour identifier le système d'exploitation

PRETTY_NAME : nom complet de la distribution, dans un format lisible (Debian GNU/Linux version 12 (nom de code bookworm)

NAME : Debian GNU/Linux

VERSION ID : numero de version de l'OS (12)

VERSION 12 (bookworm) : numero de versión et non de code

VERSION_CODENAME bookworm : nom de code de cette version specifique de Debian

ID debian : identifiant unique de la distribution

HOME_URL : url officielle du site de Debian

SUPPORT_URL : url pour obtenir de l'aide ou du support technique

BUG_REPORT_URL : url pour signaler des bugs ou problèmes lies au système Debian

Pour passer au compte root (administrateur) afin d'obtenir les privileges d'administrateur (et pouvoir ainsi avoir tous les droits sur le système, comme installer des logiciels, modifier des fichiers systèmes, gérer les utilisateurs, etc), il faut taper la commande su root (switch user root)

Cela demande au système de se connecter au compte root

Utiliser la commande whoami pour savoir quel utilisateur est connecte en ce moment

De plus, $ sera indique si un utilisateur est connecté, # si root est connecté

Attention : travailler en root est risqué, car on peut facilement faire des erreurs critiques (effacer des fichiers systèmes, altérer la configuration, etc)

Il faut privilégier alors la commande sudo pour exécuter des commandes ponctuelles avec des privileges eleves

Cela est plus securise que de rester connecte en root

sudo (superuser do) permet d'executer des commandes spécifiques avec des privileges administratifs, tout en restant sur le compte utilisateur

Avec sudo, pas besoin du mot de passe roots

On peut configurer sudo pour autoriser uniquement certains utilisateurs a utiliser cette commande

Aussi, toutes les commandes executees avec sudo sont enregistrees dans des fichiers de log (/var/log/auth.log), ce qui permet de savoir qui a execute quoi et quand

On peut aussi donner des autorisations temporaires ou limitées, sans exposer tout le systeme

Cela facilite aussi l'utilisation, car plus besoin de changer de compte (entre root et l'utilisateur)

Attention, avec sudo, l'acces admin expire après 15 minutes

Pour installer sudo, on utilise apt : la commade apt install sudo permettra d'installer la commande sudo

Cependant, il est important de taper apt update puis apt upgrade avant d'utiliser apt install, pour garantir que l'installation d'un logiciel ou d'un paquet se fasse correctement, avec les versions les plus récentes disponibles

La commande apt update telecharge la liste la plus recente des logiciels et de leurs versions depuis les dépôts configures

Si l'on saute cette etape, le système pourrait tenter d'installer une version obsolete du logiciel, ou même échouer si le paquet n'est plus disponible dans les dépôts actuels

Cela evite aussi de rencontrer des problèmes lors de la resolution de dependances nécessaires pour installer le logiciel

Il est aussi conseille de s'assurer que le système est a jour en exécutant la commande apt upgrade, car sinon il y a un risque d'incompatibilite entre les bibliothèques système et le logiciel installe

Attention : apt update doit être execute avant apt upgrade

Donc, la marche a suivre pour installer sudo est (une fois connecte en root) :

apt update

apt upgrade

apt install sudo

Pour autoriser un utilisateur à utiliser la commande sudo, il faut, une fois connecte en root, lui donner les privileges pour exécuter cette commande

Cela est essentiel pour accorder a un utilisateur un acces contrôle aux taches nécessitant des droits admin

La commande pour cela est :

sudo usermod -aG sudo juduchar

usermod est une commande permettant de modifier les paramètres d'un utilisateur existant

Elle permet d'ajouter un utilisateur a un groupe, changer son nom, son repertoire personnel, etc

L'option -aG ajoute un utilisateur à un groupe, sans supprimer les groupes existants

A signifie append, et G signifie group

Apres cette option, il faut préciser le nom du groupe secondaire auquel on veut ajouter l'utilisateur, puis le nom de l'utilisateur

Attention : si on oublie l'option a, l'utilisateur sera retire de tous les groupes secondaires existants et sera ajoute uniquement aux groupes specifies

Attention : G est utilise pour les groupes secondaires d'un utilisateur (qui permettent de donner a l'utilisateur des permissions supplémentaires), alors que g concerne le groupe principal (donné par defaut a l'utilisateur, utilise lors de la creation de fichiers) : le groupe principal est aussi appele le groupe proprietaire des fichiers crees : cela définit qui est proprietaire de quels fichiers)

Il est important d'indiquer sudo devant la commande pour que l'environnement PATH inclus le repertoire specifique de cette commande (sinon, l'erreur « bash: usermod: command not found » sera affichée

La commande groups juduchar permet de vérifier a quels groupes un utilisateur appartient

Apres cette commande, sudo (entre autres) doit s'afficher

Groupe	Description
cdrom	Permet d'accéder aux lecteurs de CD/DVD.
floppy	Autorise l'accès aux lecteurs de disquettes (obsolete mais encore présent sur certains systèmes).
sudo	Permet d'exécuter des commandes avec des privilèges administratifs via `sudo`.
audio	Permet l'accès aux périphériques audio (cartes son, microphones, etc.).
dip	Autorise la gestion de connexions réseau manuelles, comme les VPN ou les modems.
video	Permet l'accès direct aux périphériques vidéo (GPU, cartes graphiques).
plugdev	Permet de monter et démonter des périphériques de stockage (clés USB, disques externes).
users	Groupe général pour les utilisateurs standards, avec des permissions étendues sur certaines actions.
netdev	Permet de gérer certains aspects des interfaces réseau (connexion/déconnexion Wi-Fi, etc.).
bluetooth	Permet d'utiliser et de gérer les périphériques Bluetooth.

Attention : Les changements de groupe ne prennent effet qu'à la prochaine connexion de l'utilisateur !

Une fois l'utilisateur ajouté au groupe sudo, il faut sortir du mode root, ce qui permet de revenir à l'utilisateur, mais aussi se déconnecter

En effet, les modifications ne seront effectives qu'une fois que la déconnexion et la reconnexion de cet utilisateur sera effectuée

La commande sudo whoami permet d'afficher le nom de l'utilisateur actuellement connecté, mais en exécutant cette commande avec des privileges root

Lorsque l'on combine les deux, la commande affiche root, car elle est executee avec les privileges root

Avec seulement la commande whoami, juduchar sera affiché

Avec sudo whoami, root sera affiché

Cela permet de tester si l'on peut bien exécuter des commandes avec des privilèges root

Attention : il faut vérifier que la date et l'heure du système corresponde bien à la date et l'heure actuelle, sinon la commande apt update ne fonctionnera pas

Les messages :

E: Release file for http://deb.debian.org/debian/dists/bookworm-updates/InRealease is not valid yet (invalid for another 3d 17h 16min 25s). Updates for this repositoty will not be applied

E: Release file for http://security.debian.org/debian-security/dists/bookworm-security/InRealease is not valid yet (invalid for another 3d 17h 16min 25s). Updates for this repository will not be applied

Pour vérifier cela, il faut taper la commande :

timedatectl

Si le Local time ne correspond pas et que le NTP service (Network Time Protocol) est n/a, il faut alors installer un service de synchronisation NTP, puis synchroniser la date et l'heure

Pour cela, taper la commande suivante pour installer timesyncd :

sudo apt install systemd-timesyncd

timesyncd est alors intégré dans systemd (un système d'initialisation et un gestionnaire de services pour Linux, qui sert a démarrer, arrêter et superviser les services ainsi que les processus systèmes

puis activer systemd-timesyncd :

sudo systemctl enable systemd-timesyncd

puis démarrer systemd-timesyncd :

sudo systemctl start systemd-timesyncd

Enfin, forcer timedatectl à utiliser NTP :

Activer NTP avec la commande :

sudo timedatectl set-ntp true

timedatectl est un outil fourni par system pour gerer l'heure, le fuseau horaire et la synchronisation avec les serveurs NTP

En forçant l'utilisation de NTP avec timedatectl, cela garanti que le système reste synchronisé avec un serveur de temps

Verifier si la date est synchronisee avec timedatectl

NTP service : active doit être affiché, et la date et l'heure synchronisée

La commande sudo systemctl start systemd-timesyncd devra etre executee apres avoir demarre Debian

Apres cette synchronisation, lancer à nouveau sudo apt update, sudo apt upgrade, puis sudo apt install sudo

Pour ajouter l'utilisateur au groupe user42, on peut taper la commande

sudo usermod -aG user42 juduchar

Attention : si le groupe user42 n’existe pas encore, le message usermod: group ‘user42’ does not exist est affichèe

Avant cela, il faut donc tout d’abord créer le groupe user42 avec la commande :

sudo groupadd user42

puis retaper la commande

sudo usermod -aG user42 juduchar

On peut vérifier avec la commande groups juduchar

Puis se déconnecter et se reconnecter pour que ce changement soit bien pris en compte

Lorsque un utilisateur utilise la commande sudo, le système vérifie s’il a la permission d’utiliser sudo

Si c’est le cas, le système demande le mot de passe de l’utilisateur

Il est possible de configurer sudo pour limiter le nombre d’essais en cas de mot de passe erroné

Par exemple, si on limite à 3 tentatives de mot de passe incorrect, sudo met fin à la tentative actuelle et affiche un message (qu’il faut définir)

Il faut alors reprendre la commande depuis le début

La tentative actuelle est abandonnée, mais on peut immédiatement réessayer en tapant à nouveau la commande avec sudo

Cet echec n’entraine pas le blocage complet du compte utilisateur (sauf si des restrictions supplémentaires ont été configurées)

Pour éditer en toute sécurité le fichier de configuration sudoers (/etc/sudoers), qui contrôle les permissions et les règles associées à l'utilisation de la commande sudo sur un système Linux, il faut utiliser la commande sudo visudo

Ce fichier est en effet critique pour le fonctionnement de sudo

Une erreur de syntaxe dans ce fichier peut rendre sudo inutilisable, ce qui complique l'administration du système

visudo vérifie automatiquement la syntaxe avant de sauvegarder les modifications : si une erreur est détectée, elle empeche la sauvegarde

Le fichier sudoers est aussi verrouillé temporairement pendant l'édition, ce qui empeche d'autres utilisateurs ou processus de le modifier simultanément

Cette commande ouvre l'éditeur de texte configuré dans la variable d'environnement EDITOR

Une fois les modifications effectuees et sauvegardees, visudo analyse le fichier pour détecter les erreurs de syntaxe : si une erreur est trouvee, elle est signalee, et les changements ne sont pas appliques

Sinon, les modifications sont enregistrees dans le fichier /etc/sudoers

Voici les règles par défaut (déjà présentes) dans le fichier sudoers :

env_reset : réinitialise l'environnement de l'utilisateur lorsqu'il utilise sudo

Les variables d'environnement de l'utilisateur comme PATH, HOME, LANG etc sont remplacees par un ensemble sur et contrôle de variables par defaut

Cela réduit les risques de sécurité (protege des vulnerabilites dues à la modification de ces variables en amont), et garde un environnement coherant est securise pour les commandes executees avec sudo

mail_badpass : envoie un mail a l'admin système si un utilisateur entre un mot de passe incorrect avec sudo

secure_path : definit un PATH securise pour les commandes executees avec sudo (remplace le PATH de l'utilisateur par la liste specifiee ici)

Cela empeche l'execution de commandes non sures (si un attaquant modifie le PATH de l'utilisateur pour y inclure un repertoire contenant des programmes malveillants, ces programmes pourraient être executes avec des privileges root)

Cela garantit que seules les commandes situes dans des emplacements de confiance sont accessibles avec sudo

use_pty : force l'utilisation d'un pseudo-terminal (PTY) pour toutes les commandes executees avec sudo

Cela ameliore la sécurité en permettant de mieux contrôler et surveiller les commandes executees avec sudo, et réduit le risque d'attaques basees sur les detournements de de session ou des redirections non autorisees

Cela facilite aussi la journalisation : l'enregistrement complet des commandes est ainsi garanti

root ALL=(ALL:ALL) ALL

cette ligne donne au compte root un acces complet a toutes les commandes, sur toutes les machines, en tant qu'utilisateur ou groupe

root : le compte ciblé

ALL : le premier signifie que la regle s'applique a toutes les machines (utile pour les configurations mutli-serveurs)

Le second permet à root d'executer les commandes en tant que n'importe quel utilisateur

Le troisième permet a root d'executer les commandes en tant que n'importe quel groupe

Le dernier autorise root a exécuter toutes les commandes

%sudo ALL=(ALL:ALL) ALL

Cette ligne donne à tous les membres du groupe sudo les mêmes permissions que le compte root

% indique qu'il s'agit d'un groupe (et non d'un utilisateur)

Le groupe sudo contient tous les utilisateurs qui ont des privileges admin via sudo

Mêmes règles que pour root

Enfin, @includedir /etc/sudoers.d inclut tous les fichiers supplémentaires situes dans le repertoire /etc/sudoers.d

Ces fichiers permettent de définir des règles sudo supplémentaires de manière modulaire, sans modifier le fichier principal /etc/sudoers

Cela permet de définir des règles spécifiques par utilisateur, groupe ou application, dans des fichiers separes, ce qui rend la gestion plus propre

Par exemple, /etc/sudoers.d/apache pour les permissions liées à Apache

Le fichier /etc/sudoers.d/developers pour les développeurs

Le mot clé Defaults est utilisé pour définir ou modifier des options globales qui affectent le comportement de sudo

Ces options agissent comme des paramètres par défaut pour tous les utilisateurs ou groupes

Pour limiter l'authentification en utilisant sudo à 3 essais en cas de mot de passe erroné, il faut ajouter la ligne :

Defaults passwd_tries=3

Si on tape 3 fois un mauvais mot de passe apres l'execution d'une commande sudo, la commande sera interrompue et «3 incorrect password attempts" sera affiché à l'écran

Pour afficher un message de notre choix ("You have entered a bad password” par exemple) en cas d’erreur d’execution suite à un mauvais mot de passe lors de l’utilisation de sudo, il faut ajouter la ligne :

Defaults badpass_message="You have entered a bad password”

Sinon, “Sorry, try again.” Sera affiché

Pour archiver chaque action executee avec la commande sudo, aussi bien les inputs que les outputs, c’est-à-dire les commandes et leur résultat, il faut ajouter les 2 lignes suivantes :

Pour archiver les inputs :

Defaults log_input

Pour vérifier que les logs d’input soient bien générés :

Par défaut, les fichiers de log sont enregistrés dans le répertoire /var/log/sudo-io

Ce répertoire n’est accessible qu’en tant que root

Il faut tout d’abord taper la commande sudo -i pour ouvrir une session shell avec les privilèges root, tout en chargeant l’environnement du compte root, comme si on était connecté directement en tant que root

Cela nous permettra d’avoir l’autorisation de se déplacer dans le répertoire /var/log/sudo-io, accessible uniquement en tant que root normalement

Puis taper la commande :

sudo whoami

La commande sudoreplay -l affiche les commandes tapées avec sudo

Taper donc la commande sudoreplay -l

Chercher le code TSID correspondant à la dernière commande tapée en sudo (par exemple 000009

Puis taper la commande

sudoreplay 000009

Cela affichera : Replay sudo session : /usr/bin/whoami

Ce qui correspond bien à la commande whoami

Pour archiver les outputs :

Defaults log_output

Pour vérifier que les logs d'output soient bien générés, taper la commande :

sudo whoami

La commande sudoreplay -l affiche les commandes tapées avec sudo

Taper donc la commande sudoreplay -l

Chercher le code TSID correspondant à la dernière commande tapée en sudo (par exemple 00000A)

Puis taper la commande

sudoreplay 00000A

Cela affichera :

Replay sudo session : /usr/bin/whoami

root

Ce qui correspond bien à la commande whoami, et son résultat

Pour modifier le répertoire où sont enregistrés les logs, écrire la ligne suivante :

Defaults iolog_dir=/var/log/sudo

Pour vérifier que les logs soient bien générés dans le nouveau répertoire :

sudo whoami

Se déplacer dans le répertoire correspondant avec la commande :

cd /var/log/sudo

Taper la commande ls

Un répertoire 00 et seq doivent être présents

Naviguer vers 00, puis 00

Un répertoire 01 doit être présent

S'y déplacer, puis faire un cat sur log.json

La valeur pour command doit être /usr/bin/whoami

Attention : pour utiliser à nouveau sudoreplay après avoir modifié le répertoire de log, il faut utiliser l'option -d en précisant le chemin du nouveau répertoire, donc :

sudo sudoreplay -d /var/log/sudo -l

La directive Defaults logfile="/var/log/sudo/sudo.log" configure un fichier de log classique pour enregistrer les commandes exécutées via sudo

Chaque fois qu'un utilisateur utilisera sudo, les informations seront écrites dans ce fichier :

- L'utilisateur qui a exécuté la commande
- La commande exécutée
- L'heure de l'exécution

Le mode TTY (teletypewriter) est une fonctionnalité essentielle dans les systèmes Linux, qui fait référence à une interface interactive permettant de communiquer avec le terminal

Activer l'utilisation d'un TTY pour sudo garantit une sécurité accrue, en liant les commandes sudo à un terminal interactif

Ainsi, les commandes sont exécutées dans un TTY, et liées à une session interactive spécifique, qui permet de savoir qui a exécuté la commande et d'où elle a été lancée

Sans le mode TTY, les commandes peuvent être exécutées en arrière plan, via des scripts ou d'autres processus automatisés, sans interface interactives, ce qui rend plus difficile la traçabilité et le contrôle des commandes

Pour l'activer, taper la ligne :

Defaults requiretty

Dans le fichier sudoers (avec la commande sudo visudo)

Restreindre les paths utilisables par sudo est une mesure de sécurité essentielle pour contrôler et limiter les commandes executees avec des privileges eleves

En specifiant explicitement les chemins dans lesquels sudo peut chercher des executables (commandes executables), on réduit le risque d'executer des programmes malveillants ou non souhaites

Pour cela, éditer la ligne Defaults secure_path comme ceci (pour y ajouter /snap/bin) :

Defaults secure_path=

”/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin”

Ajouter **/snap/bin** au **secure_path** de sudo permet d'exécuter les commandes et applications installées via **Snap**, un gestionnaire de paquets développé par Canonical (les créateurs d'Ubuntu), avec les privilèges appropriés.

Pour tester que les commandes qui ne sont pas dans le secure_path ne fonctionnent pas, taper :

echo «echo Hello World» > /tmp/test-script

puis chmod +x /tmp/test-script

et sudo test-script

“sudo: test-script: command not found” doit etre affiché

Faire de meme avec le repertoire /snap/bin :

A la racine :

mkdir snap

cd snap

mkdir bin

echo «echo Hello World» > /snap/bin/test-script2

puis chmod +x /snap/bin/test-script2

et sudo test-script2

Hello World devra s’afficher

Un service SSH sera obligatoirement actif sur le port 4242 dans votre machine virtuelle

Un service SSH est un service réseau qui permet d’établir des connexions sécurisées à distance entre un client et un serveur, en utilisant le protocole SSH (Secure Shell)

Il est largement utilisé pour l’administration distante des systèmes, notamment pour exécuter des commandes, transférer des fichiers, ou configurer des services

Le serveur SSH ecoute les connexions entrantes sur un port spécifique (par defaut, le port 22)

Un port est un point de communication logique utilise pour identifier un service ou une application specifique sur un reseau : ils focntionnent en conjonction avec une adresse IP pour permettre aux ordinateurs et appareils de se connecter entre eux et d'echanger des donnees

Une adresse IP identifie un appareil sur un reseau (comme une maison dans une rue)

Un port specifie un service ou une application sur cet appareil (comme une piece ou une porte dans une maison)

Les ports permettent donc a un appareil d'executer plusieurs services ou applications sur une même adresse IP !

Chaque port identifie une application ou un service specifique

Le port 22 est utilise par defaut pour l'administration distante

Lorsqu'un appareil communique sur un réseau :

1. **Le client** (exemple : un navigateur) ouvre un **port source dynamique (exemple : 49160)**.
2. **Le serveur** écoute sur un **port spécifique** associé au service demandé (par exemple, 80 pour HTTP).
3. Une connexion est établie, et les données sont échangées via ces ports.

Les données circulent ainsi :

Client : 192.168.1.100:49160 → Serveur : 192.168.1.10:80

Pour une meilleure sécurité, il faut fermer les ports inutilisés (désactiver les services inutiles), configurer un pare-feu, et surveiller les ports (détecter les ports ouverts et vérifier leur légitimité)

Aussi, pour éviter les attaques automatisées, il faut modifier les ports par défaut des services : par exemple, utiliser le port 4242 pour SSH au lieu du port 22

Le serveur authentifie les utilisateurs via des mots de passe, des cles SSH, ou d'autres mecanismes

Une fois authentifie, le serveur établit un tunnel securise entre le client et le serveur

Le client SSH est un logiciel utliise pour se connecter au serveur SSH

Il établit la connexion en utilisant des protocoles securises (cryptes)

Exemple : PuTTY

Cela permet par exemple d'utiliser SCP (Secure Copy Protocol) ou SFTP (Secure File Transfer Protocol) pour copier les fichiers

Les clés SSH permettent une authentification securisee sans mot de passe

Sous Linux, le serveur OpenSSH est le plus couramment utilisé

Nous allons donc configurer le service SSH

Il devra être actif sur le port 4242

Modifier le port par défaut de SSH (port 22) par un port personnalisé (comme 4242) est une mesure de sécurité qui peut réduire les risques liés aux attaques automatisées, et renforcer la protection du serveur

En effet, les attaquants savent que SSH utilise le port 22 par défaut

Ils lancent alors des scans automatisés sur les adresses IP á la recherche de services SSH actifs sur ce port, suivis d'attaque par force brute pour deviner les mots de passe

Même si les tentatives d'acces non autorise echouent, cela genere des entrees inutiles dans les journaux et charge inutilement le serveur

En modifiant ce port par defaut, le service SSH sera caché des bots qui scannent le port 22, cela agit comme une barriere de sécurité supplementaire, et oblige un attaquant a

effectuer un scan complet des ports (prend plus de temps et augmente donc les chances de detection)

Il faut aussi interdire la connexion par SSH avec l'utilisateur root

Cela réduit le risque d'attaques par force brute, car le compte root est une cible privilégiée (il dispose de privilièges illimités)

Les bots effectuent souvent des attaques par force brute en essayent de deviner le mot de passe du compte root

Si cela fonctionne, un accès complet au système est donné à l'attaquant !

De plus, travailler directement en tant que root est déconseillé (exécution accidentelle de commandes destructrice par exemple)

Pour installer SSH, taper les commandes suivantes :

sudo apt update

sudo apt upgrade

sudo apt install openssh-server

Vérifier le statut du serveur SSH :

sudo systemctl status ssh

Resultat attendu :

Loaded : loaded ... enabled .. enabled

Active : active (running)

Le fichier /etc/ssh/sshd_config contient les paramètres de configuration du serveur SSH sur le système

Port définit le port sur lequel le serveur SSH ecoute

Par défaut, ce port est le port 22

AdressFamily détermine les types d'adresse réseau utilisées (inet (pour IPv4), inet6 (pour IPv6) ou any (les deux)

ListenAddress indique les adresses IP sur lesquelles SSH écoute (par défaut, il écoute sur toutes les interfaces)

PermitRootLogin autorise ou interdit la connexion directe en tant qu'utilisateur root

Par défaut, la connexion en root par SSH est autorisée (mais seulement avec une clé SSH)

PasswordAuthentification interdit ou non l'authentification par mot de passe (si désactivé, seule la connexion via clé SSH

Attention : installer et paramétrer UFW avant de modifier les paramètres de SSH

UFW (Uncomplicated Firewall) est un outil simplifié pour gérer les règles de pare-feu sur les systèmes Linux

Il permet de configurer facilement les règles de pare-feu pour sécuriser les systèmes contre les acces non autorises

Il est concu pour rendre la gestion des règles de pare-feu plus accessible, même pour les utilisateurs ayant peu d'experience

Il sert de frontal convivial pour iptables, qui est complexe et peut être sujette a des erreurs

Avec UFW, on peut :

Autoriser ou bloquer l'acces a des services ou ports spécifiques

Définir des règles reseau pour des adresses IP ou sous-reseaux

Mettre rapidement en place un pare-feu fonctionnel, avec des commandes simples

Les connexions entrantes sont bloquées par defaut, et les connexions sortantes sont autorisees

Firewalld est un outil de gestion de pare-feux sous Lunix, principalement utilisé avec Rocky

Il permet de configurer et surveiller un pare-feu via une interface dynamique et flexible

Il peut appliquer des changements au pare-feu sans redémarrer les services réseau ou interrompre les connexions en cours

Il utilise des zones pour simplifier la configuration : chaque zone correspond a un niveau de sécurité spécifique (home, work, public)

On peut associer des interfaces reseau à des zones et configurer des règles spécifiques pour chaque zone

Il permet de basculer rapidement entre des profils de sécurité

On peut aussi ajouter des services autorisés, des ports ouverts, ou des règles personnalisées facilement

Il gère les protocoles modernes et les NAT (translation d'adresse réseau)

Des logs sont générés pour surveiller le trafic autorisé ou bloqué

On peut aussi créer des règles avancées avec des conditions spécifiques

Firewalld est plus puissant et adapté pour des configurations complexes ou dynamiques

Pour installer UFW, taper les commandes suivantes :

sudo apt update

sudo apt upgrade

sudo apt install ufw

Pour activer UFW :

sudo ufw enable

Le message : Firewall is active and enabled on system startup doit s'afficher

Verifier le statut d'UFW :

sudo ufw status verbose

Status : active

Signifie que le pare-feu UFW est actuellement activé et que les règles configurees sont appliquees au trafic reseau

Logging : on (low)

Logging : on : la journalisation est activée : certaines informations sur les connexions reseau sont enregistrees dans les journaux systeme

(low) : le niveau de journalisation est defini sur low (faible)

Seules les connexions bloquees ou certaines connexions autorisees seront enregistrees

Les niveaux de journalisation sont : low, medium, high, full, off

Default: deny (incoming), allow (outgoing), disabled (routed)

Ce sont les paramètres définissant les politiques par defaut du pare-feu :

deny (incoming) : tous les paquets entrants (trafic reseau qui arrive sur la machine) sont bloques par defaut (sauf si on a configure une regle pour les autoriser)

Protege la machine des connexions non autorisees

allow (outgoing) : tous les paquets sortants (trafic réseau provenant de la machine) sont autorises par defaut

cela permet a la machine d'initier des connexions reseau sans restrictions

disabled (routed) : le trafic routé (le trafic passant par la machine comme un routeur) est désactivé

Cela signifie que la machine n'est pas configurée pour agir comme un routeur ou un pont réseau

sudo ufw allow ssh permet de paramétrer ufw pour SSH sur le port 22, avec un profil d'application préconfiguré pour SSH

Les lignes suivantes devraient s'afficher :

Rule added

Rule added (v6)

sudo ufw status devrait maintenant afficher :

22/tcp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)

Ajouter ensuite la règle pour le port 4242 :

sudo ufw allow 4242

sudo ufw status devrait maintenant afficher :

22/tcp	ALLOW	Anywhere
4242	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)
4242 (v6)	ALLOW	Anywhere (v6)

Modifier le port SSH 22 (par défaut) pour le port 4242 :

sudo nano /etc/ssh/sshd_config

Modifier la ligne :

#Port 22

Par :

Port 4242

Interdire la connexion en SSH avec le compte root :

Modifier la ligne :

#PermitRootLogin prohibit-password

Par

PermitRootLogin no

La commande sudo service ssh restart permet de redémarrer le service SSH

La commande sudo ss -tuln permet d'afficher les port ouverts (listening)

Voici le resultat si le port 4242 est ouvert :

LISTEN 0 128 0.0.0.0:4242 0.0.0.0:*

LISTEN 0 128 [::]:4242 [::]:*

Maintenant, supprimer l'accès au port 22 pour UFW :

sudo ufw delete allow ssh

Vérifier les règles actives avec sudo sfw status

sudo ufw status devrait maintenant afficher :

4242	ALLOW	Anywhere
4242 (v6)	ALLOW	Anywhere (v6)

Le port forwarding (redirection de port) est une technique utilisée pour acheminer le trafic reseau entrant ou sortant d'un port specifique d'une machine vers une autre

Cela facilite la communication entre la VM et l'exterieur, notamment l'hote ou d'autres réseaux

En effet, les VM sont souvent configurees avec des adresses IP privees, qui ne sont pas directement accessibles depuis l'exterieur (hote,reseau local ou internet)

Le port forwarding redirige le trafic des ports de l'hote vers la VM, ce qui permet de pouvoir se connecter à la VM en SSH notamment

Pour cela, apres avoir arrêté la VM, aller dans VirtualBox, puis dans Settings, Network, Adapter 1, puis Port Forwarding

Créer une nouvelle règle de redirection

Indiquer 4242 pour Port hote, et 4242 pour Port invité

Relancer la VM

Une demande d'autorisation pour la redirection reseau devrait apparaitre, accepter

Taper :

sudo systemctl restart ssh

sudo service sshd status

Les lignes suivantes devraient apparaitre :

Starting ssh.service

Server listening on 0.0.0.0 port 4242

Server listening on :: port 4242

Started ssh.service

Ouvrir la console en mode admin sur l'hote (avec un terminal 42, ou invite de commande Windows)

ssh juduchar@localhost -p 4242

yes

juduchar@juduchar42 devrait s'afficher

whoami

juduchar devrait s'afficher

Une commande avec sudo (sudo whoami par exemple) devrait s'afficher dans les logs du serveur

Taper exit dans la console pour quitter la connexion ssh

Mettre en place une politique de mot de passe fort :

Mettre en place une politique de **mot de passe fort** pour les utilisateurs est une **mesure de sécurité essentielle** pour protéger un système contre des attaques courantes et garantir la confidentialité des données

- Dans une attaque par force brute, un attaquant tente de deviner un mot de passe en essayant toutes les combinaisons possibles.
- Les mots de passe faibles, simples ou courts sont beaucoup plus faciles à deviner.

Solution avec un mot de passe fort :

- Des mots de passe longs, complexes et aléatoires augmentent le nombre de combinaisons possibles, rendant les attaques par force brute **impraticables** en termes de temps.
- Les attaquants utilisent des listes de mots courants, de noms ou de combinaisons populaires pour deviner un mot de passe (attaques par dictionnaire).
- Des mots de passe simples comme **"123456"**, **"password"** ou des variations comme **"Pa$$w0rd"** figurent souvent dans ces listes.

Solution avec un mot de passe fort :

- Une politique exigeant des caractères spéciaux, des majuscules/minuscules et des chiffres empêche l'utilisation de mots communs ou prévisibles.

- Si un mot de passe est facile à deviner ou à cracker, un attaquant peut obtenir un accès non autorisé à un compte utilisateur ou à des ressources sensibles.

Solution avec un mot de passe fort :

- Un mot de passe fort rend les comptes beaucoup plus difficiles à compromettre, réduisant ainsi les risques de vol de données ou de sabotage.
- Les mots de passe réutilisés sur plusieurs sites/services augmentent les risques. Si un mot de passe est compromis ailleurs, il pourrait être utilisé pour accéder à d'autres comptes (attaque par credential stuffing).

Solution avec une politique forte :

- En exigeant des mots de passe uniques et complexes, on limite l'impact d'une fuite de mot de passe sur d'autres systèmes.
- Dans certains cas, les menaces viennent de l'intérieur (employés malintentionnés, collaborateurs négligents).
- Des mots de passe faibles augmentent le risque d'accès non autorisé à des comptes internes.

Solution :

- Une politique stricte garantit que même à l'intérieur de l'organisation, les utilisateurs adoptent des pratiques sécurisées.

Exemples de politiques pour renforcer les mots de passe

1. **Longueur minimale :**
    - Exiger un minimum de 12 à 16 caractères.
2. **Complexité :**
    - Inclure des majuscules, des minuscules, des chiffres et des caractères spéciaux.
3. **Expiration des mots de passe :**
    - Forcer un renouvellement régulier (par exemple, tous les 90 jours).
4. **Historique des mots de passe :**
    - Empêcher la réutilisation des 5 ou 10 derniers mots de passe.
5. **Bloquer les mots de passe courants :**
    - Comparer les mots de passe aux listes de mots courants compromis.
6. **Limitation des tentatives de connexion :**
    - Verrouiller un compte après un certain nombre de tentatives échouées (par exemple, 3 ou 5).

Règles pour un mot de passe fort :

Expire tous les 30 jours

2 jours minimum avant de pouvoir modifier un mot de passe

Envoyer un avertissement à l'utilisateur 7 jours avant que son mot de passe n'expire

Les règles d'expiration des mots de passe se trouvent dans le fichier /etc/login.defs

Ces paramètres définissent les politiques de cycle de vie des mots de passe, comme leur durée de validité et les avertissements avant expiration :

La durée maximale (en jours) avant qu'un utilisateur soit obligé de modifier son mot de passe : PASS_MAX_DAYS

Le nombre minimum de jours entre deux changements de mot de passe : PASS_MIN_DAYS

Le nombre de jours avant l'expiration d'un mot de passe ou l'utilisateur recevra un avertissement : PASS_WARN_AGE

Pour mettre en place ces règles de sécurité, il faut donc éditer le fichier /etc/login.defs comme ceci :

PASS_MAX_DAYS 30

PASS_MIN_DAYS 2

PASS_WARN_AGE 7

Attention : ces modifications ne seront pas appliquées automatiquement aux utilisateurs existants, mais seulement aux nouveaux !

Pour appliquer ces mêmes règles de sécurité à l'utilisateur déjà existant et au root, il faut utiliser les commandes suivantes (chage signifie Change Age) :

Expire tous les 30 jours :

sudo chage -M 30 juduchar

sudo chage -M 30 root

Vérifier avec :

sudo chage -l juduchar

sudo chage -l root

2 jours minimum avant de pouvoir modifier un mot de passe :

sudo chage -m 2 juduchar

sudo chage -m 2 root

Vérifier avec :

sudo chage -l juduchar

sudo chage -l root

Envoyer un avertissement à l'utilisateur 7 jours avant que son mot de passe n'expire

sudo chage -W 7 juduchar

sudo chage -W 7 root

Vérifier avec :

sudo chage -l juduchar

sudo chage -l root

Pour mettre en place les autres règles de mot de passe, nous allons utiliser pwquality

pwquality est une bibliothèque et un outil en ligne de commande permettant de défini et d'appliquer des politiques de qualité de mot de passe

Son objectif est de garantir que les mots de passe créés ou modifiés respectent certaines règles de complexité et de sécurité

Les critères paramètrables par pwquality sont, entre autres :

La longueur minimale

L'inclusion de caractères spéciaux, de chiffres, de majuscules, etc

L'exclusion de mots simples, ou liés à l'utilisateur

...

C'est un PAM (Pluggable Authentication Module), qui intervient lors de la création ou la modification d'un mot de passe

Il évalue le mot de passe selon les règles définies

Les paramètres de pwquality se trouvent dans el fichier /etc/security/pwquality.conf

Exemple :

Paramètre	Description	Exemple
`minlen`	Définit la longueur minimale d'un mot de passe.	`minlen = 12`
`minclass`	Nombre minimum de classes de caractères différentes (chiffres, majuscules, minuscules, spéciaux).	`minclass = 3`
`maxrepeat`	Nombre maximal de répétitions consécutives d'un même caractère autorisé.	`maxrepeat = 2`
`maxsequence`	Longueur maximale des séquences consécutives de caractères autorisées.	`maxsequence = 3`
`dictcheck`	Vérifie que le mot de passe ne contient pas de mots simples ou communs.	`dictcheck = 1`
`usercheck`	Vérifie que le mot de passe ne contient pas le nom ou l'identifiant de l'utilisateur.	`usercheck = 1`
`retry`	Nombre de tentatives autorisées pour entrer un mot de passe valide.	`retry = 3`

Il faut donc, pour appliquer les règles suivantes, installer pwquality avec la commande suivante :

sudo apt install libpam-pwquality

Puis éditer le fichier /etc/security/pwquality.conf

nano /etc/security/pwquality.conf

Supprimer le # devant la ligne correspondante et modifier la valeur pour indiquer celle voulue

Mot de passe de 10 caractères minimum :

minlen = 10

Avec une majuscule, une minuscule et un chiffre :

Pour forcer l'inclusion d'au moins une majuscule, minuscule et un chiffre, il faut utiliser le système de credit de pwquality

Chaque type de caractere (majuscule, minuscule, chiffre et caractere special) peut être controlé via des credits positifs ou negatifs

dcredit : nombre minimal de chiffres dans le mot de passe

lcredit : nombre minimal de lettres minuscules dans le mot de passe

ucredit : nombre minimal de lettres majuscules dans le mot de passe

Une valeur de -1 représente une exigence stricte : par exemple, lcredit = -1 exige au moins une minuscule

Une valeur positive ou de 0 rend le critère optionnel ou non contraignant

Ainsi, pour imposer une majuscule, une minuscule et un chiffre, voici la configuration nécessaire :

dcredit = -1

lcredit = -1

ucredit = -1

Ne doit pas comporter plus de 3 caractères identiques consécutifs

maxrepeat = 3

Ne pas contenir le nom de l'utilisateur :

usercheck = 1

Doit comporter au moins 7 caractères qui ne doivent pas être présents dans l'ancien mot de passe :

difok = 7

Cette dernière règle ne doit pas concerner l'utilisateur root, mais le mot de passe root doit suivre toutes les autres règles :

Le module pam_pwquality.so applique généralement des règles globales définies dans /etc/security/pwquality.conf à tous les utilisateurs, y compris root

Pour exclure root de la règle difok, il faut utiliser une approche conditionnelle dans les fichiers de configuration PAM

Le fichier /etc/pam.d/common-password est un fichier de configuration pour le système PAM (Pluggable Authentication Module) qui détermine quels modules PAM sont utilisés lors des changements de mot de passe (par exemple, avec la commande passwd)

Si l'utilisateur est root, appliquer les règles de pam_pwquality avec difok désactivé :

password [success=1 default=ignore] pam_succeed_if.so user = root

password requisite pam_pwquality.so retry=3 difok=0

password requisite pam_pwquality.so retry=3 difok=7

password [success=1 default=ignore] pam_succeed_if.so user = root

password : cette directive indique que cette ligne s'applique aux opérations liées aux mots de passe (comme la commande passwd pour changer un mot de passe

[success=1 default=ignore] :

success=1 : si cette règle réussit, PAM va alors appliquer les règles de la ligne suivante (ligne 2)

default=ignore : si cette règle échoue, PAM ignorera la ligne suivante (la ligne 2), et appliquera celles de la ligne qui suit (ligne 3)

pam_succeed_if.so : un module PAM qui permet de conditionner l'application des règles en fonction de certains critères (l'utilisateur, le groupe, etc)

user = root : critère spécifique : cette règle sera un succès uniquement si l'utilisateur courant est root

password requisite pam_pwquality.so retry=3 difok=0

password : idem

requisite : signifie que cette règle est obligatoire : si cette règle échoue (si le mot de passe ne respecte pas les critères suivants, PAM retournera immédiatement une erreur

pam_pwquality.so : ce module PAM applique des règles de qualité aux mots de passe (longueur minimale, majuscules, chiffres, minuscules, différences avec l'ancien mot de passe, etc. Les critères sont définis soit dans cette ligne, soit dans le fichier de configuration global /etc/security/pwquality.conf

retry=3 : l'utilisateur a 3 tentatives pour entrer un mot de passe valide avant que le système ne quitte la commande de modification du mot de passe

difok=0 : désactiver la règle difok=7 (qui concernera alors tous les autres utilisateurs). Ainsi, root pourra choisir un mot de passe similaire ou identique à l'ancien

Cette règle ne s'appliquera qu'à root (grâce à la premiere ligne)

password requisite pam_pwquality.so retry=3 difok=7

Idem, sauf qu'ici, grâce à difok=7, le mot de passe devra avoir au moins 7 caractères différents de l'ancien mot de passe

Cette règle ne s'appliquera qu'aux utilisateurs non root (grâce à la premiere ligne, qui exclut root de cette règle)

Redémarrer la VM pour que ces modifications soient prises en compte

Pour tester, mettre à 0 la limite de nombre de jours avant le changement de mot de passe :

sudo chage -m 0 juduchar

Changer le mot de passe de l'utilisateur avec la commande passwd

Tester avec plusieurs combinaisons de mot de passe (sans majuscule, sans minuscule, sans chiffre, avec moins de 10 caractères, avec plus de 3 caractères identiques consécutifs, et contenant le login de l'utilisateur

Enfin, tester avec moins de 7 caractères différents de l'ancien mot de passe

Tous ces tests devraient échouer

Tester la même chose avec le compte root (se connecter en root pour cela), puis :

sudo chage -m 0 root

Le test avec moins de 7 caractères différents de l'ancien mot de passe ne devrait pas échouer

Changer tous les mots de passe des comptes présents sur la VM, compte root inclus, après la mise en place de la config

Remettre la limite de jours avant le changement de mot de passe à 2 :

sudo chage -m 2 juduchar

sudo chage -m 2 root

Enfin, vous devrez mettre en place un petit script nommé monitoring.sh. Ce dernier sera à développer en bash.

Il faut donc tout d'abord créer le fichier monitoring.sh, que l'on placera dans le dossier /root

Ce script doit être développé en bash, il faut donc indiquer l'entête : #!bin/bash en première ligne de ce fichier

Et lui donner les droits de lecture, d'écriture et d'exécution pour root (mais pas pour les autres utilisateurs ou les autres groupes)

Pour cela, on utilise la commande : chmod 700 monitoring.sh

Votre script devra toujours pouvoir afficher les informations suivantes :

L'architecture de votre système d'exploitation ainsi que sa version de kernel :

Exemple :

#Architecture: Linux juduchar42 6.1.0-27-amd64 #1 SMP Debian 6.1.115-1 (2024-11-101) x86_64 GNU/Linux

La commande uname permet d'afficher les informations de l'architecture (le système d'exploitation et le noyau (kernel) du système Linux

Elle fournit des détails sur le type de système, la version du noyau, l'architecture matérielle, et d'autres caractéristiques importantes

Par défaut, uname retourne simplement le nom du système d'exploitation (Linux)

L'option -a fournit une sortie complète avec plusieurs détails :

- Le nom du noyau du système d'exploitation (Linux)
- Le nom de l'hote du système, l'hostname (juduchar42)
- La version du noyau Linux et architecture (6.1.0-27-amd64)
    - 6.1.0 : version majeure et mineure du noyau Linux
    - -27 : révision ou patch spécifique à cette version du noyau
    - amd64 : indique que le noyau est compilé pour une architecture 64 bits compatible avec AMD ou Intel
- L'identifiant de la construction du noyau (#1)
- Si le noyau a été concu pour prendre en charge plusieurs cœurs ou processeurs (SMP)
- Si le noyau est compilé avec un support dynamique de préemption (le système est plus réactif, car il ajuste dynamiquement la priorité des taches)
- Le nom de la distribution Linux utilisée (Debian)
- La version exacte du paquet noyau Debian (6.1.115-1)
    - 6.1.115 : version précise du noyau utilisé
    - -1 : révision du paquet dans les dépôts Debian
- La date de compilation du noyau (2024-11-01)
- L'architecture matérielle (x86_64)
- Le nom complet du système d'exploitation (GNU/Linux)

Le nombre de processeurs physiques.

Le nombre de processeurs virtuels.

Exemple :

#CPU physical : 1

#vCPU : 1

Le fichier /proc/cpuinfo contient des informations détaillées sur les processeurs (CPU) du système

Ce fichier fait partie du système de fichiers /proc, qui fournit des informations en temps réel sur le matériel et les processus du système

Le nombre de processeurs physiques :

Le champ physical id indique l'identifiant physique du processeur. Si le système a plusieurs processeurs physiques, ce champ les distingue, et il y aura donc une ligne physical id par processeur

Pour compter le nombre de processeurs physiques, il faut donc compter le nombre de lignes commençant par «physical id» (après avoir extrait ces lignes bien sur)

Attention : il faut éliminer les doublons avant de compter le nombre de lignes, car chaque processeur physique peut être mentionne plusieurs fois : une fois pour chaque processeur virtuel qu'il gère

Par exemple, un processeur physique qui gère 4 processeurs virtuels sera affiché comme ceci dans /proc/cpuinfo :

processor : 0

physical id : 0

cpu cores : 2

processor : 1

physical id : 0

cpu cores : 2

processor : 2

physical id : 0

cpu cores : 2

processor : 3

physical id : 0

cpu cores : 2

Pour cela, on utilise la commande sort -u (n'affiche que la première valeur identique rencontrée)

Puis la commande wc - l pour compter le nombre de lignes

Le commande grep "physical id" /proc/cpuinfo servira quand à elle à extraire les lignes du fichier /proc/cpuinfo commençant par physical id

La commande suivante servira donc à compter le nombre de processeurs physiques :

grep "physical id" /proc/cpuinfo | sort -u | wc -l

Le nombre de processeurs virtuels :

Le champ processor indique l'identifiant du processeur virtuel. Si le système a plusieurs processeurs virtuels, ce champ les distingue, et il y aura donc une ligne processor par processeur virtuel

Pour compter le nombre de processeurs virtuels, il faut donc compter le nombre de lignes commençant par «processor» (après avoir extrait ces lignes bien sur)

Il n'est donc pas nécessaire de filtrer le résultat avec sort -u (car il n'y aura pas de doublons)

La commande suivante servira donc à compter le nombre de processeurs virtuels :

grep "processor" /proc/cpuinfo | wc -l

La mémoire vive disponible actuelle sur votre serveur ainsi que son taux d'utilisation

sous forme de pourcentage.

Exemple :

#Memory Usage: 74/987MB (7.50%)

La commande free est utilisée sous Linux pour afficher des informations sur la mémoire vive (RAM) du système

Elle affiche aussi des informations sur la mémoire d'échange (swap) du système

Elle permet de surveiller l'utilisation actuelle de la mémoire, notamment la quantité de mémoire totale, utilisée, libre et mise en cache

Exemple de sortie de la commande free :

	total	used	free	shared	buff/cache	available
Mem:	2014496	218136	1822508	620	98688	1796360
Swap:	2244604	0	2244604			

Les informations sur la mémoire vive (RAM) sont indiquées sur la ligne commençant par « Mem: »

Sans option, free affiche les informations en Ko

Nous voulons afficher la mémoire disponible en MB

L'option -m permet de préciser que les informations doivent être présentées en MB

La mémoire vive utilisée sur le serveur est indiquée sous la colonne used (3eme colonne, en comptant "Mem:")

La commande pour afficher la mémoire vive actuellement utilisée sur le serveur est donc :

free -m | grep "Mem:" | awk '{print $3}'

La mémoire vive totale sur le serveur est indiquée sous la colonne total (2eme colonne, en comptant "Mem:")

Celle pour afficher la mémoire vive totale est donc :

free -m | grep "Mem:" | awk '{print $2}'

Pour afficher le taux d'utilisation de la mémoire sous forme de pourcentage (avec 2 décimales), on divise la mémoire vive utilisée par la mémoire vive totale

On utilisera awk pour faire ce calcul et formater le résultat à exactement 2 chiffres après la virgule

Avec used_memory et total_memory, la mémoire utilisée et totale (respectivement) :

awk "BEGIN {printf \"%.2f\", ($used_memory / $total_memory) * 100}"

BEGIN permet d'exécuter le calcul ($used_memory / $total_memory) * 100) avant le traitement des données (le formatage à 2 décimales)

printf \"%.2f\" permet de formater à 2 décimales (on échappe les doubles guillemets)

($used_memory / $total_memory) * 100 effectue la division entre les deux variables, puis multiplie par 100 pour obtenir le pourcentage

Attention, pour plus de précision, utiliser plutôt free -k pour effectuer ces calculs !

En effet, les informations seront alors affichées en Ko, ce qui est plus précis qu'qvec free -m, ou les résultats sont affichés en Mo (et donc arrondis)

La mémoire disponible actuelle sur votre serveur ainsi que son taux d'utilisation sous forme de pourcentage.

Exemple :

#Disk Usage: 1.3G/28G (5%)

La commande df (Disk Free) affiche des informations sur l'espace disque disponible et utilisé pour les systèmes de fichiers montés

Elle est utile pour surveiller l'utilisation des disques et détecter un éventuel manque d'espace

Elle montre combien d'espace est utilisés sur chaque système de fichiers (partitions, disques locaux et points de montage), et combien d'espace reste disponible

L’option -h signifie human readable (lisible par les humains) et comvertit les tailles affichées par défaut (en blocs de 1 Ko) en unités plus lisibles (en Ko, Mo, Go ou To) (elle choisit automatiquement l’unité la plus adaptée)

L’option --total affiche l’espace disque total, utilisé et disponible, sur l’ensemble des systèmes de fichiers répertoriés

Cela donne une idée rapide de l’utilisation globale de l’espace disque

Ces informations se trouvent sur la ligne "total"

On peut combiner cette option avec l’option -h

La mémoire utilisée sur le serveur est indiquée sous la colonne Used (3eme colonne, en comptant "total")

La commande pour afficher la mémoire actuellement utilisée sur le serveur est donc :

df -h --total | grep "total" | awk ‘{print $3}’

La mémoire totale sur le serveur est indiquée sous la colonne Size (2eme colonne, en comptant "total")

Celle pour afficher la mémoire vive totale est donc :

df -h --total | grep "total" | awk ‘{print $2}’

Le taux d’utilisation de la mémoire sous forme de pourcentage est indiqué sous la colonne Use% (5eme colonne, en comptant "total")

Celle pour afficher la mémoire vive totale est donc :

df -h --total | grep "total" | awk ‘{print $5}’

Le taux d’utilisation actuel de vos processeurs sous forme de pourcentage.

Exemple :

#CPU load: 6.7%

La commande top est un outil interactif sous Linux utilisé pour surveiller en temps réel les processus et les performances du système

Elle affiche des informations essentielles sur l’utilisation des ressources, comme le processeur (CPU), la mémoire (RAM) et les processus actifs

Cette commande est interactive : on peut interagir avec les processus pour changer leurs priorités ou les arrêter

k permet de tuer un processus, r modifier la priorité, P trie par utilisation CPU et M trie par utilisation mémoire

Nous souhaitons seulement le résultat de cette commande, obtenir une sortie unique (en mode batch, non interactif), et l’afficher dans un format lisible pour le script

Pour cela, nous utiliserons l’option -bn1

-b exécute top en mode batch, ce qui désactivera l’interface interactive de top et produira une sortie brute dans la console

-n1 définit le nombre de rafraichissements (d’itérations)

Avec -n1, top exécute une seule itération et s’arrete immédiatement

La ligne %Cpu(s) fournit une vue d'ensemble de l'utilisation des cœurs du CPU par le système. Elle montre comment le temps processeur est réparti entre différents types d'activités

Ces informations sont indiquées en pourcentage (avec une décimale)

Champ	Signification
`us`	**Temps utilisateur** (**user space**) : Temps CPU utilisé par les processus utilisateur (ex. programmes, scripts).
`sy`	**Temps système** (**system space**) : Temps CPU utilisé par le noyau et ses processus.
`ni`	**Temps utilisateur avec priorité modifiée** (**nice**) : Temps CPU pour des processus utilisateur ayant une priorité `nice`.
`id`	**Inactif** (**idle**) : Temps CPU pendant lequel il n'y a aucune tâche à exécuter (CPU au repos).
`wa`	**Attente I/O** (**wait**) : Temps CPU passé à attendre des entrées/sorties (ex. lecture/écriture disque).
`hi`	**Interruptions matérielles** (**hardware interrupts**) : Temps CPU utilisé pour gérer des interruptions matérielles.
`si`	**Interruptions logicielles** (**software interrupts**) : Temps CPU utilisé pour gérer des interruptions logicielles.
`st`	**Temps volé** (**steal time**) : Temps CPU "volé" par un hyperviseur (ex. dans une machine virtuelle).

Les champs concernant les temps CPU actifs sont us (temps utilisateur), sy (temps système), et ni (temps utilisateur avec une priorité modifiée)

Il faut donc additionner les valeurs de ces champs pour obtenir le taux d'utilisation actuel de vos processeurs

Il faut donc tout d'abord extraire les valeurs correspondantes :

Pour us (2eme colonne) :

top -bn1 | grep "%Cpu(s):" | awk '{print $2}'

Pour sy (4eme colonne) :

top -bn1 | grep "%Cpu(s):" | awk '{print $4}'

Pour ni (6eme colonne) :

top -bn1 | grep "%Cpu(s):" | awk '{print $6}'

Puis les additionner :

awk "BEGIN {printf \"%.1f\", $us_load + $sy_load + $ni_load}"

La date et l'heure du dernier redémarrage (reboot)

Exemple :

#Last boot: 2024-11-21 10:59

La commande who sous Linux est utilisée pour afficher des informations sur les utilisateurs actuellement connectés au système

Elle fournit des détails comme leurs noms d'utilisateur, les terminaux qu'ils utilisent, les heures de connexion, et parfois leur adresse IP ou le nom de la machine distante (si applicable)

L'option -a affiche toutes les informations possibles (sessions inactives, processus système, temps de démarrage, etc)

L'option -q affiche le nom et le nombre d'utilisateurs connectés

L'option -b indique la dernière fois que le système a redémarré (c'est ce qui nous intéresse ici

Avec l’option -b, le résultat sera affiché comme ceci :

system boot 2024-11-21 10:59

Pour extraire la date du dernier reboot :

who -b | awk ‘{print $3}’

Pour extraire l’heure du dernier reboot :

who -b | awk ‘{print $4}’

Si LVM est actif ou pas.

LVM peut être désactivé pour un volume logique donné (par exemple tmp)

Le volume ne sera pas supprimé, mais il sera inactif

Pour cela, la commande lvchange -an tmp est utilisée

Il est aussi possible de désactiver un groupe de volumes auquel appartient un volume logique (par exemple le groupe LVMGroup) avec la commande vgchange -an LVMGroup

Tous les volumes logiques du groupe seront alors inaccessibles

Pour réactiver un volume logique, on utilise la commande :

lvchange -ay tmp

pour un groupe de volumes :

vgchange -ay LVMGroup

Pour vérifier l'état des volumes logiques, on utilise la commande lvs

Cela affichera les volumes logiques actifs, aucun résultat sinon

Pour vérifier si des volumes logiques existent, on peut utiliser la commande suivante :

lvs | wc -l

Pour vérifier l'état des groupes de volumes logiques, on utilise la commande vgs

Cela affichera les groupes de volumes logiques actifs, aucun résultat sinon

Pour vérifier si des groupes de volumes logiques existent, on peut utiliser la commande suivante :

vgs | wc -l

LVM peut aussi être totalement désactivé : dans ce cas, les volumes LVM devront être converties en partitions standards

Pour vérifier si des partitions LVM sont montées (par exemple /LVMGroup-home), on utilise la commande df

Les partitions LVM montées seront indiquées sous /dev/mapper (car c'est le chemin sous lequel les volumes logiques créés par LVM sont accessibles)

On peut donc utiliser la commande df est vérifier si des disques (sous Filesystem) commencent par /dev/mapper

Pour vérifier si des partitions LVM existent, on peut utiliser la commande suivante :

df | grep "^/dev/mapper" | wc -l

Ainsi, si le résultat de ces commandes est 0, cela indiquera que LVM n'est pas activé

Sinon, cela indiquera que LVM est actif

Nous allons donc additionner le résultat de ces trois commandes et vérifier si cette somme est égale à 0 : dans ce cas, LVM est inactif ; sinon, il est actif

lvm_active_total=$((lvm_active_logical_volumes + vm_active_volume_groups + lvm_active_mounted_partitions))

Puis

```
if [ $lvm_active_total -eq 0]; then
        lvm_active=”no”
else
        lvm_active=”yes”
fi
```

Le nombre de connexions TCP actives.

Le fichier /proc/net/sockstat contient des statistiques détaillées sur l’utilisation des sockets réseau dans le système

Un socket réseau est une interface logicielle permettant à un programme d’établir une communication entre deux machines (ou entre deux processus sur une même machine)

C’est l’unité fondamentale de la communication en réseau

Cela permet d’envoyer et de recevoir des données via un réseau et d’établir une connexion entre un client et un serveur

Différents protocoles peuvent être utilisés (le TCP ou l’UDP par exemple)

Le protocole TCP (Transmission Control Protocol) garantit une communication fiable entre deux machines

Cela assure que toutes les données envoyées arrivent dans le bon ordre. Si un paquet est perdu, il est retransmis

Une connexion doit être établie entre le client et le serveur avant de pouvoir transmettre des données

Le TCP adapte la vitesse de transmission en fonction de la capacité du destinataire

Il donne des statistiques détaillées sur l’utilisation des sockets réseau ouverts, et leur répartition selon leur protocole (TCP, UDP, etc)

Ce fichier est particulièrement utile pour diagnostiquer des problèmes de réseau et pour surveiller les connexions réseau en temps réel

sockets indique le nombre total de sockets ouverts sur le système (cela inclus toutes les connexions (TCP, UDP, RW, etc))

TCP inuse correspond au nombre de sockets TCP actifs (établis ou en cours de connexion)

TCP orphan indique le nombre de sockets orphelins (sans processus propriétaire, mais toujours actifs) : cela indique des problèmes de gestion réseau

TCP tw indique le nombre de sockets TCP en etat TIME_WAIT (en attente d'etre fermés, pour éviter des collisions dans le trafic réseau)

TCP allow indique le nombre de structures TCP allouées par le noyau

TCP mem indique la quantité de mémoire utilisée par les sockets TCP

La commande ss est plus utile pour lister les connexions TCP actives, car sockets compte aussi le nombre de sockets TCP en cours de connexion, et ne différencie pas les deux !

Cette commande (Sockets Statistics) est un outil puissant pour surveiller et diagnostiquer les connexions réseau et l'utilisation des sockets sur Linux

Elle affiche une liste détaillée de toutes les connexions actives sur le système

L'option -s (summary) affiche un résumé des statistiques des sockets réseau sur le système, qui inclus des informations agrégées sur les connexions TCP, UDP et RAW

Sur la ligne "TCP:", nous pouvons voir le nombre de connexions TCP établies (estab, pour established)

La commande pour extraire le nombre de connexions TCP est donc :

ss -s | grep "TCP:" | awk '{print $4}'

Attention à supprimer la virgule du résultat avec sed 's/,//'

Le nombre d’utilisateurs utilisant le serveur.

La commande who sous Linux est utilisée pour afficher des informations sur les utilisateurs actuellement connectés au système

Elle fournit des détails comme leurs noms d’utilisateur, les terminaux qu’ils utilisent, les heures de connexion, et parfois leur adresse IP ou le nom de la machine distante (si applicable)

L’option -q affiche le nom et le nombre d’utilisateurs connectés

Nous pouvons donc utiliser who avec l’option -q pour afficher le nombre d’utilisateurs connectés

Attention : si un même utilisateur est connecté sur plusieurs terminaux (par exemple tty, console locale, et pts/0, terminal virtuel ou SSH), le système considèrera chaque session comme une connexion séparée

Le nombre d’utilisateurs sera indiqué comme ceci (par exemple avec 2 utilisateurs) :

users=2

La commande sera donc :

who -q | awk -F ‘=’ ‘/# users=/ {print $2}’

L’adresse IPv4 de votre serveur, ainsi que son adresse MAC (Media Access Control)

Exemple :

#Network: IP 10.0.2.15 (08:00:27:51:9b:a5)

L’adresse IPv4 de votre serveur :

L’adresse IPv4 d’un serveur est une adresse numérique unique utilisée pour identifier ce serveur sur un réseau basé sur le protocole IPv4

Elle permet au serveur de communiquer avec d’autres dispositifs (ordinateurs, routeurs, etc) via un réseau local ou internet

Elle est composée de 4 nombres (octets) séparés par des points

Exemple : 192.168.1.1

Chaque nombre est compris entre 0 et 255 (représentant 8 bits, soit 1 octet)

Si le serveur est connecté à un réseau local, il aura une adresse IPv4 privée, comme 192.168.x.x ou 10.x.x.x

Ces adresses sont uniquement accessibles dans le réseau interne

Si le serveur est accessible via internet, il aura une adresse IPv4 publique (par exemple 203.0.113.1)

Cette adresse est unique dans le monde et permet au serveur d’etre atteint depuis n’importe ou

La commande hostname permet de voie ou de modifier le nom de l’hote (hostname) d’une machine

C’est un identifiant lisible par les humains, attribué à un ordinateur sur un réseau

Il est souvent utilisé pour identifier le serveur dans un réseau local ou sur internet

Afficher le nom de l’hote : hostname

Modifier le nom de l’hote (pour la session en cours uniquement) : hostname nouveau_nom

Afficher l’adresse IP associée à l’interface réseau correspondant au nom d’hote :

hostname -i

Afficher les adresses IP de la machine (du serveur) :

hostname -I

C’est cette dernière que nous allons utiliser pour afficher l’adresse IPv4 du serveur

Cette commande affiche en premier l’adresse IPv4 du serveur, puis en deuxième son adresse IPv6

La commande sera donc :

hostname -I | awk ‘{print $1}’

L’adresse MAC (Media Access Control) du serveur :

Une adresse MAC (Media Access Control) est un identifiant unique attribué à chaque interface réseau (par exemple, une carte Ethernet ou Wi-Fi) par le fabricant

Elle est utilisée pour identifier un appareil spécifique sur un réseau local (LAN) (même s’ils partagent une même adresse IP)

Elle est représentée par 6 paires de caractères hexadécimaux, séparés par des deux points ou des tirets

Elle est constituée de 48 bits (6 octets)

Les 3 premiers octets sont appelés OUI (Organizationally Unique Identifier) et identifient le fabricant de la carte réseau

Les 3 derniers octets sont un numéro unique assigné par le fabricant

Les routeurs utilisent les adresses MAC pour transmettre les paquets au bon appareil

Sous Linux, on peut afficher l’adresse MAC avec la commande ip add show

La commande ip est utilisée pour gérer et afficher la configuration réseau sous Linux

Elle affiche la configuration réseau (interfaces, adresses IP, routes, etc), mais permet aussi de supprimer une adresse IP, d’activer ou désactiver une interface, de gérer les routes réseau, les tunnels et VPN, etc

La sous-commande ip addr affiche ou modifie les adresses IP associées aux interfaces réseau

Les adresses MAC de la machine sont affichées sur la ligne commençant par link/ether

Attention, plusieurs lignes peuvent être présentes, car chaque interface réseau physique ou virtuelle a sa propre adresse MAC

Si la machine a plusieurs interfaces réseau (par exemple, une pour Ethernet et une pour Wi-Fi), chaque interface aura sa propre adresse MAC

La commande ip link est cependant plus adaptée pour lister toutes les interfaces réseau disponibles sur la machine, qu'elles soient actives ou non

Elle affiche toutes les interfaces réseau existantes, qu'elles soient câblées (ethernet), sans fil (Wi-Fi), ou virtuelles

Avec ip link show, et en précisant l'identifiant de l'interface, on peut afficher l'adresse MAC de cette interface précise

Pour trouver l'interface réseau utilisée pour les communications principales, on peut utiliser la commande ip route show default, qui identifie l'interface associée à la route par défaut

Exemple de sortie de la commande ip route show :

default via 10.0.2.2 dev emp0s3

L'identifiant de l'interface associée à la route par défaut se trouve toujours après « dev »

Pour obtenir cet identifiant, on peut utiliser la commande suivante :

ip route show default | grep -o "dev [^]*" | awk '{print $2}'

L'option -o de grep force l'affichage (uniquement) de la partie du texte qui correspond au motif, au lieu de la ligne entière

dev [^]*

"dev ": cherche le mot dev suivi d'un espace

[ ] : indique un ensemble de caractères à correspondre

[^] : tous les caractères sauf l'espace

* : 0 ou plusieurs caractères qui remplissent cette règle

Cette commande recherche donc le mot "dev " dans le résultat de la commande ip route show default, puis la chaine de caractères (le mot) qui suit (jusqu'à rencontrer un espace ou la fin de la ligne)

Avec cette commande, dev enp0s3 sera retourné

Il faut alors capturer la 2eme colonne avec awk '{print $2}

Grâce à cet identifiant, nous pourrons alors trouver son adresse MAC avec la commande ip link show :

ip link show enp0s3 | grep 'link/ether' | awk '{print $2}'

Le nombre de commande exécutées avec le programme sudo.

Exemple :

#Sudo : 42 cmd

Les commandes exécutées avec le programme sudo sont enregistrées dans le fichier sudo.log, se trouvant dans /var/log/sudo

Elles se trouvent sur la ligne contenant «COMMAND=»

Il suffit de compter le nombre de lignes de ce fichier contenant «COMMAND=" pour connaitre le nombre de commandes exécutées avec sudo

La commande à executer est donc :

grep "COMMAND=" /var/log/sudo/sudo.log | wc -l

Attention, si plusieurs commandes ont été exécutées dans un même contexte (contexte interactif par exemple), les commandes seront regroupées sur une seule ligne. Car elles partagent un contexte commun

Il faut donc plutôt extraire les différentes commandes comme ceci :

grep -o “COMMAND=[^]*” /var/log/sudo/sudo.log

Puis compter le nombre de lignes

grep -o “COMMAND=[^]*” /var/log/sudo/sudo.log | wc -l

Dès le lancement de votre serveur, le script écrira des informations toutes les 10 minutes sur tous les terminaux (jetez un oeil du côté de wall).

La commande wall (abbreviation de write all) est un outil sous Linux pour envoyer un message à tous les utilisateurs connectés au système

Elle diffuse un message à tous les terminaux actifs (TTYs ou PTSs)

Cela peut être utile pour alerter tous les utilisateurs d’une maintenance système, envoyer des annonces importantes, ou informer d’un redémarrage imminent du serveur

On peut envoyer un message contenu dans un fichier par exemple

Les utilisateurs peuvent recevoir ou bloquer les messages syteme envoyes avec wall en modifiant leurs permissions de terminal avec la commande mesg

On peut aussi automatiser une notification avec un script

Cron est un service Linux utilisé pour automatiser l’execution de taches planifiees

Il permet de lancer des commandes ou des scripts à des moments prédéfinis ou selon un intervalle régulier

Il fonctionne en arrière plan, surveille et execute des taches planifiées définies dans les fichiers de configuration appelés crontab

Le daemon est généralement démarré au démarrage du système, et tourne en permanence

Crontab est un fichier de configuration ou les taches planifiees sont définies

Chaque utilisateur peut avoir son propre fichier crontab, et le système dispose également de taches globales

Une tache planifiee dans crontab suit une syntaxe précise, avec les champs suivants :

* * * * * commande

minute (de 0 à 59) heure (de 0 à 23) jour du mois (de 0 à 31) mois (de 1 à 12) jour de la semaine (0 à 7) (de lundi à dimanche)

Par exemple, pour exécuter la commande tous les jours à 23h, if faut indiquer :

0 23 * * * commande

Crontab permet de planifier des taches à des horaires, jours ou dates précis, mais il est aussi possible de planifier une tâche pour qu'elle s'execute régulièrement (toutes les minutes, tous les jours, toutes les heures, etc

Pour cela, il faut utiliser la syntaxe des intervalles :

Par exemple, pour exécuter une commande toutes les 10 minutes, on écrit :

*/10 * * * * commande

La commande crontab permet de gérer les taches planifiées :

crontab -l liste les taches planifiées

crontab -e permet d'éditer le fichier crontab pour planifier une tache

crontab -r permet de supprimer toutes les taches planifiees

Pour vérifier si le daemon cron est actif : systemctl status cron

Pour activer cron : systemctl enable cron

Pour redémarrer cron : sudo systemctl restart cron

Donc, pour planifier l'exécution de notre script toutes les 10 minutes (par bash) :

crontab -e

*/10 * * * * bash /root/monitoring.sh

Pour diffuser le résultat de la commande à tous les terminaux actifs, on passe simplement celui-ci à la commande wall

*/10 * * * * bash /root/monitoring.sh | wall

Le script monitoring.sh sera alors exécuté toutes les 10 minutes (à 23h, 23h10, 23h20, etc)

Pour faire en sorte qu'il s'execute toutes les 10 minutes à partir du démarrage du système, on peut créer un script sleep.sh qui calculera l'écart entre le moment ou le serveur a démarré et la 10eme minute précédente, et attendra ce délai avant de démarrer le script (toutes les 10 minutes)

Ex : 18:42:57

2 minutes 57 entre 18:42:57 et 18:40:00

A 18:50:00, le script attendra 2 minutes 57 avant de s'executer

La commande uptime récupère l'heure du démarrage du serveur

L'option -s retourne l'heure à laquelle le système a démarré, sous la forme YYYY-MM-DD HH:MM:SS

Pour extraire les minutes et les secondes, on utilise la commande cut pour extraire les caractères correspondant aux minutes (MM) du format :

cut -c 15-16 permet ici d'extraire le 15eme et le 16eme caractère du résultat de la commande uptime -s

On utilise de nouveau la commande cut pour extraire les secondes (SS) du format :

cut -c 18-19 permet ici d'extraire le 18eme et le 19eme caractère du résultat de la commande uptime -s

On extrait l'unité du nombre de minutes extraites, ce qui correspondra au nombre de minutes à attendre avant de lancer le script

min % 10

On multiplie le résultat par 60, pour obtenir un résultat en secondes, puis on y ajoute les secondes extraites

La commande sleep permet de mettre en pause l'exécution du script pendant un certain délai (en secondes)

On exécutera ce script avant l'exécution du script de monitoring

La tache cron sera donc :

*/10 * * * * bash /root/sync_10_min.sh && /root/monitoring.sh

Script appliqué

Maj tuto

Bonus :

Installation de WordPress (sources : https://oleks.ca/2024/09/28/installation-lamp-sur-debian-12/ ; https://oleks.ca/2024/09/30/installer-wordpress-sur-debian-12-avec-lamp/)

Mettre en place un site web WordPress fonctionnel avec, comme services, lighttpd, MariaDB et PHP.

Lighttpd est un serveur web open source concu pour être rapide, sécurisé et peu gourmand en ressources

Il est particulièrement adapté aux environnements à forte charge ou les performances et l'efficacité sont cruciales

Il offre des performances élevées, tout en consommant peu de mémoire et de CPU

Il utilise un modèle évènementiel asynchrone, ce qui le rend capable de gérer des milliers de connexions simultanées

La configuration est claire et facile à gérer, et il est adapté pour les sites web dynamiques

Il est plus léger qu'Apache et plus rapide pour les contenus statiques, et est comparable à Nginx en termes de légèreté et de performances

MariaDB est un système de gestion de bases de données relationnelles (SGBDR) open source

C'est un fork de MySQL, mais avec des améliorations en termes de fonctionnalités et de performances (pour des charges importantes)

PHP est un langage de script open source largement utilisé pour le développement zeb coté serveur : il est utilisé pour créer des pages web dynamiques et interactives

Il permet de communiquer facilement avec des bases de données comme MariaDB et MySQL, est flexible et puissant

Avant d'utiliser apt update, synchroniser la date du serveur :

sudo systemctl restart systemd-timesyncd

Mettre à jour la liste des paquets :

sudo apt update

Mettre à jour les paquets :

sudo apt upgrade

wget (World Wide Web get) est un outil en ligne de commande gratuit et open source pour télécharger des fichiers depuis internet pour Linux

Il permettra de télécharger WordPress

sudo apt install wget

Curl (Client URL) est un outil en ligne de commande open source permettant de transférer des données depuis ou vers un serveur à l'aide d'URL

Il est basé sur la bibliothèque libcurl, permettant des transferts réseau

Il prend en charge de nombreux protocoles (HTTP, HTTPS, FTP, SMTP, etc)

Il prend aussi en charge SSL/TLS pour sécuriser les connexions réseau

Elle doit être installée sur le système pour que l'extension php-curl fonctionne

Cette dernière est une extension PHP qui sert d'interface entre PHP et libcurl (voir plus bas)

sudo apt install curl

sudo apt install php

php-common est un package regroupant des fichiers, extensions et configurations partagées entre plusieurs modules PHP. Il contient des outils et des fichiers de base nécessaires au bon fonctionnement de PHP et de ses extensions (comme php-curl par exemple)

De nombreux modules PHP nécessaires pour WordPress dépendent de php-common

sudo apt install php-common

php-cgi est une version de PHP configurée pour fonctionner avec le protocole CGI (Common Gateway Interface). CGI est un protocole permettant à un serveur web (comme lighttpd) d'exécuter des scripts en lançant un processus PHP pour chaque requête

Il est simple à configurer et peut fonctionner avec presque tous les serveurs web

Il peut être utilisé comme méthode d'exécution de PHP avec Lighttpd, mais il est recommandé de plutôt utiliser PHP-FPM, plus optimisé pour gérer des requêtes simultanées de manière efficace

sudo apt install php-cgi

php-cli (Command Line Interface) est une version PHP conçue pour être utilisée en ligne de commande, plutôt que via un serveur web

Il permet d'exécuter des scripts PHP directement depuis un terminal, sans passer par un navigateur ou un serveur http

Il permet d'exécuter des scripts d'automatisation, des tests rapides de code PHP, des taches cron, gérer la base de données, traiter les fichiers, interagir avec des APIs, etc

Il n'est pas strictement nécessaire pour qu'un site WordPress fonctionne, mais il peut être utile pour mieux gérer WordPress

sudo apt install php-cli

php-mysql est une extension qui permet aux scripts PHP de se connecter et de communiquer avec des bases de données MySQL ou MariaDB

Elle fournit des fonctions pour exécuter des requêtes SQL, récupérer des données, insérer des enregistrements, etc

Sans php-mysql, WordPress ne pourra pas communiquer avec la base de données et exécuter les requêtes nécessaires

sudo apt install php-mysql

php-curl permet à un script PHP de communiquer avec des serveurs distants via des protocoles http, HTTPS, FTP, etc

Elle permet d'envoyer des requetes GET, POST, PUT, DELETE, etc, de télécharger des fichiers à partir d'une URL distante et les enregistrer localement, et gère les appels API

REST (l’envoi des données JSON, XML, etc), et gère aussi les cookies, les redirections automatiques, et prend en charge TLS/SSL pour des connexions sécurisées

sudo apt install php-curl

php-gd est une extension PHP qui fournit des outils pour créer, manipuler et traiter des images. Elle utilise la bibliothèque GD (Graphical Draw) qui gère les JPEG, les PNG, les GIF, etc

WordPress utilise php-gd pour redimensionner et générer automatiquement des miniatures d’images téléchargées (thumbnails)

sudo apt install php-gd

php-zip est une extension PHP permettant de manipuler des fichiers et des archives ZIP

Elle permet de créer, extraire, lire et modifier des fichiers ZIP

Cela est utile pour télécharger des plugins, des thèmes et des mises à jour pour WordPress

sudo apt install php-zip

Nous allons utiliser Lighttpd comme serveur web, nous n’avons donc plus besoin d’Apache2

Vérifier si apache2 est actif :

systemctl status apache2

Désinstaller Apache2 et supprimer ses fichiers de configurations associées (plus complet que sudo apt remove, qui ne fait que désinstaller le paquet) :

sudo apt purge apache2

Supprimer les dépendances inutilisées (après la désinstallation d’Apache 2) :

sudo apt autoremove

Installer Lighttpd :

sudo apt install lighttpd

Vérifier si Lighttpd a bien été installé :

sudo lighttpd -v

Démarrer le serveur web Lighttpd :

sudo systemctl start lighttpd

Permet de lancer automatiquement Lighttpd au démarrage du serveur :

sudo systemctl enable lighttpd

Vérifier si Lighttpd est actif :

sudo systemctl status lighttpd

La commande suivante permet d'activer le module fastcgi pour Lighttpd

FastCGI est un protocole permettant au serveur web de communiquer efficacement avec des applications serveur (comme PHP), en gardant les processus de ces applications en mémoire pour gérer plusieurs requêtes

sudo lighty-enable-mod fastcgi

Redémarrer Lighttpd :

sudo systemctl restart lighttpd

Configure FastCGI spécifiquement pour PHP, pour qu'il cherche une configuration prête à l'emploi pour traiter les scripts PHP

sudo lighty-enable-mod fastcgi-php

Redémarrer Lighttpd :

sudo systemctl restart lighttpd

Recharger la configuration de Lighttpd :

sudo service lighttpd force-reload

Autoriser le port 80 avec UFW pour permettre l'accès au serveur web depuis une machine cliente en utilisant le protocole TCP :

sudo ufw allow 80/tcp

Recharger UFW pour qu'il prenne en compte cette modification :

sudo ufw reload

Voir les ports autorisés ou interdits :

sudo ufw status

Résultat attendu :

```
Status: active

To                         Action      From
--                         ------      ----
4242                       ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
4242 (v6)                  ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
```

Le port forwarding redirige le trafic des ports de l'hote vers la VM, ce qui permet de pouvoir se connecter à la VM en HTTP

Pour cela, apres avoir arrêté la VM, aller dans VirtualBox, puis dans Settings, Network, Adapter 1, puis Port Forwarding

Créer une nouvelle règle de redirection

Indiquer 8080 pour Port hote, et 80 pour Port invité

Redémarrer la VM, et accéder à Apache2 sur le système invité via navigateur avec l'url suivant :

http://localhost:8080

Installer MariaDB Server :

sudo apt install mariadb-server

Démarrer MariaDB :

sudo systemctl start mariadb

Executer un script de sécurité fourni avec MariaDB (et MySQL), pour renforcer la sécurité du serveur de base de données, en désactivant les configurations par défaut potentiellement vulnérables, en appliquant les paramètres de sécurité essentiels :

sudo mysql_secure_installation

Enter current password for root or enter id you've just installed MariaDB :

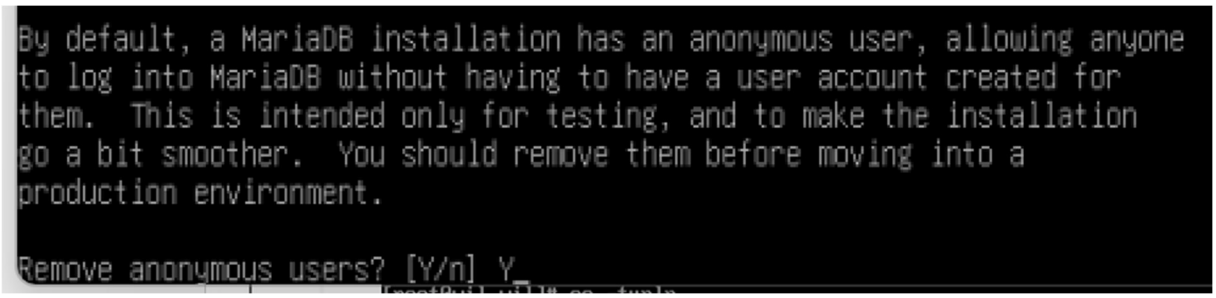
Nous venons juste d'installer MariaDB, donc appuyer sur entrée

Setting the root password (no) or using the unix_socket (ensure that nobody can log into the MariaDB root user without the proper authorization) (yes)

Utiliser unix_socket permet d'activer l'authentification socket, ce qui interdit tout utilisateur non autorisé par le root du serveur à se connecter en tant que root de MariaDB. Confirmer avec Y

Change the root password ?

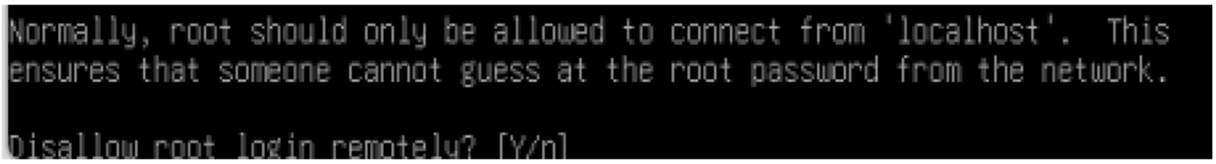
Appuyer sur Y pour définir un mot de passe pour le root de MariaDB



Supprimer les utilisateurs anonymes de MariaDB (qui peuvent se connecter à MariaDB sans compte spécifique) (oui) :

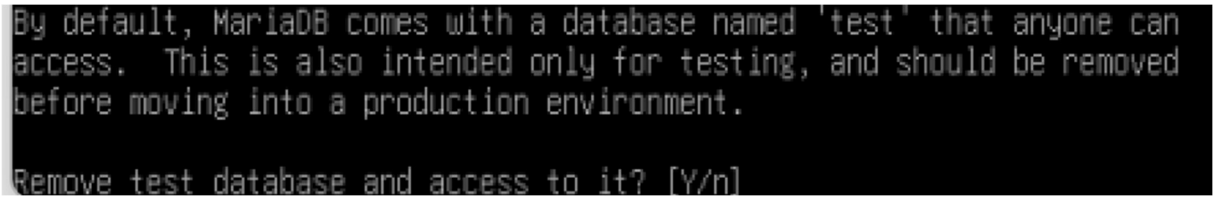
Y

Désactiver l'accès à la connexion root de MariaDB à distance (oui) :



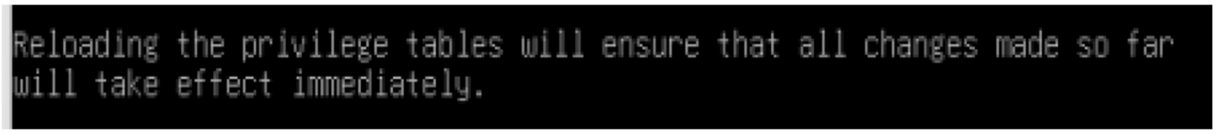
Y

Supprimer la base de données « test » (oui) :



Y

Recharger les tables de privilèges pour appliquer immédiatement ces modifications (oui) :



Y

Se connecter à MariaDB en tant que root (-u root : en tant que l'utilisateur root), en demandant le mot de passe avant d'établir la connexion (-p : password) :

sudo mysql -u root -p

Créer la base de données WordPress (remplacer wordpress par un nom plus sécurisé !) :

CREATE DATABASE wordpress;

Créer l'utilisateur de cette base de données, avec son mot de passe (remplacer wordpress_user et password par un nom et un mot de passe plus sécurisé !) :

CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'password';

Accorder tous les privileges sur cette base de données à l'utilisateur wordpress_user (remplacer par le nom défini plus haut) :

GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpress_user'@'localhost';

Appliquer les modifications :

FLUSH PRIVILEGES;

Quitter MariaDB :

EXIT;

Télécharger et configurer WordPress :

Se déplacer dans le répertoire par défaut de Lighttpd :

cd /var/www/html

Télécharger la dernière version de WordPress depuis le site officiel :

sudo wget https://wordpress.org/latest.tar.gz

Extraire le contenu de l'archive téléchargée (tar : utilitaire pour manipuler des archives au format TAR ; x : extrait les fichiers contenus dans l'archive ; z : indique que l'archive est au format .gz (gzip) ; v : afficher les fichiers extraits (mode verbeux) ; f : spécifier le fichier d'archive à traiter (doit être suivi du nom de l'archive) :

sudo tar -xzvf latest.tar.gz

Déplacer les fichiers de WordPress dans le répertoire racine /var/www/html :

sudo mv wordpress/* /var/www/html/

Supprimer l'archive téléchargée et le dossier WordPress vide :

sudo rm -rf latest.tar.gz wordpress

Accorder les permissions nécessaires pour que Lighttpd puisse accéder aux fichiers (modifie le propriétaire et le groupe de fichiers et dossiers situés dans /var/www/html à l'utilisateur et au groupe www-data, utilisés par Lighttpd ; -R indique que l'opération doit être effectuée de manière récursive, pour tous les fichiers et sous-dossiers dans /var/www/html) :

sudo chown -R www-data:www-data /var/www/html

Accorder toutes les permissions au propriétaire des fichiers, le droit de lecture et d'exécution pour les autres utilisateurs, au contenu (-R) de /var/www/html :

sudo chmod -R 755 /var/www/html

Renommer le fichier de configuration d'exemple pour pouvoir le personnaliser et l'appliquer à WordPress :

sudo mv /var/www/html/wp-config-sample.php /var/www/html/wp-config.php

Editer le fichier de configuration de WordPress :

sudo nano /var/www/html/wp-config.php

// Remplacez 'wordpress' par le nom de votre base de données.

define('DB_NAME', 'wordpress');

// Remplacez 'wordpressuser' par votre nom d'utilisateur MySQL.

define('DB_USER', 'wordpressuser');

// Remplacez 'password_here' par votre mot de passe MySQL.

define('DB_PASSWORD', 'password_here');

Aller sur cet URL depuis le navigateur du client :

http://localhost:8080/

Cliquer sur Install WordPress

Indiquer le nom du site, le nom de l'utilisateur (admin) WordPress, son mot de passe, son email

Cocher la case Discourage search engines from indexing this site

Cliquer sur Install WordPress

Se connecter

Pour obtenir la signature :

%HOMEDRIVE%%HOMEPATH%\VirtualBox VMs\

certUtil -hashfile centos_serv.vdi sha1

signature.txt

The hostname must be your_intra_login42, but the hostname must be changed during the Born2beroot evaluation. The following commands might help:

$ sudo hostnamectl set-hostname <new_hostname>

$ hostnamectl status

There must be a user with your_intra_login as username. During evaluation, you will be asked to create, delete, modify user accounts. The following commands are useful to know:

- useradd : creates a new user.
- usermod : changes the user's parameters: -l for the username, -c for the full name, -g for groups by group ID.
- userdel -r : deletes a user and all associated files.
- id -u : displays user ID.
- users : shows a list of all currently logged in users.

- cat /etc/passwd | cut -d ":" -f 1 : displays a list of all users on the machine.
- cat /etc/passwd | awk -F '{print $1}' : same as above.

The user named your_intra_login must be part of the sudo and user42 groups. You must also be able to manipulate user groups during evaluation with the following commands:

- groupadd : creates a new group.
- gpasswd -a : adds a user to a group.
- gpasswd -d : removes a user from a group.
- groupdel : deletes a group.
- groups : displays the groups of a user.
- id -g : shows a user's main group ID.
- getent group : displays a list of all users in a group.