

Projet Interdisciplinaire

Configuration Linux

Cahier de bord – Configuration Linux Global

Année Académique 2024-2025

Classe 2/10E

1. INTRODUCTION.....	3
2. SERVEUR LINUX GLOBAL	3
A. CHOIX DE DISTRIBUTION	3
B. PLAN DE PARTITIONNEMENTS	3
C. PLAN DE SAUVEGARDES	4
D. SCRIPT	5
E. CARACTERISTIQUES DES PRINCIPAUX SERVICES	5

1. Introduction

Lors de ce projet, nous avons dû configurer deux serveurs Linux (le local mais aussi le global). Ici, nous allons nous intéresser au serveur Linux Global. Ce serveur a pour but de détenir la base de données globale ainsi que l'application en Django.

2. Serveur Linux Global

a. Choix de distribution

Le choix du serveur global s'est porté sur AlmaLinux. Étant la distribution utilisée lors du cours de Linux en plus de pouvoir être utilisée pour les serveurs, la prise en main était donc facilitée.

b. Plan de partitionnements

Par manque de stockage sur le pc, nous n'avons pas pu utiliser de RAID pour les partitions avec un disque dur virtuel. Nous avons donc préalablement choisi du LVM à la place.

Données	Type de périphérique	Système de fichiers	Stockage	Chiffré	Options de montage
/backup	LVM [AlmaLinux]	xfs	5Go	non	defaults,noexec,nosuid,nodev,relatime
/home	LVM [AlmaLinux]	ext4	2Go	oui	defaults,noexec,nosuid,nodev,relatime
/web	LVM [AlmaLinux]	xfs	3Go	oui	defaults,noexec,nosuid,nodev,relatime
/database	LVM [AlmaLinux]	xfs	2Go	oui	defaults,noexec,nosuid,nodev,relatime

Système	Type de périphérique	Système de fichiers	Stockage	Chiffré	Options de montage
/	LVM [AlmaLinux]	xfs	5Go	oui	defaults,nodev
/boot	Partition Standard	ext4	1024Mo	non	defaults,ro,nodev,nosuid,noexec
/tmp	LVM [AlmaLinux]	ext4	1024Mo	non	defaults,noexec,nosuid,nodev
/var	LVM [AlmaLinux]	ext4	3Go	oui	defaults,noexec,nosuid,nodev
biosboot	Partition standard	Bios Boot	2 Mo	non	/
swap	LVM [AlmaLinux]	swap	4Go	non	defaults

- ❖ **noexec** : Empêche l'exécution de fichiers binaires sur cette partition. Utile pour éviter l'exécution de scripts malveillants.
- ❖ **nosuid** : Empêche l'escalade de privilèges via les fichiers setuid.
- ❖ **nodev** : Empêche la création de périphériques spéciaux sur cette partition.
- ❖ **relatime** : Met à jour les timestamps d'accès aux fichiers de manière relative, ce qui peut améliorer les performances sans compromettre la sécurité.
- ❖ **ro (read-only)** : Monte la partition en lecture seule pour éviter toute modification accidentelle ou malveillante.

c. Plan de sauvegardes

1. Que faut-il sauvegarder ?

/etc,/web,/var,/home,/root, /database

2. Avec quelle fréquence ?

Chaque jour à 12h pendant la pause.

3. Combien de temps conservera-t-on les sauvegardes, en combien d'exemplaires ?

Les sauvegardes seront effacées après 1 semaine.

4. A quel endroit seront stockées les sauvegardes et l'historique des sauvegardes ?

Les sauvegardes seront stockées dans une partition à part : /backup

5. Quels sont les besoins, en capacité, du support de sauvegarde ?

On a pensé à utiliser un /backup de 10Go pour ce projet.

6. Combien de temps, au plus, doit durer la sauvegarde ?

Elles doivent **au maximum** durer 5-10 minutes.

7. Combien de temps prévoit-on pour restaurer un fichier, un système de fichiers, est-ce raisonnable ?

La restauration devra prendre **au maximum** 20 minutes.

8. La sauvegarde doit-elle être automatique ou manuelle ?

Les sauvegardes seront automatisées chaque jour à 12h pendant le repas. Il sera possible de les faire manuellement grâce à la commande dailybackup.

9. Quelle est la méthode de sauvegarde la plus appropriée ?

La méthode de sauvegarde la plus appropriée est la sauvegarde incrémentielle car elle met à jour seulement les fichiers modifiés grâce à la commande rsync. Elle est appropriée pour réduire le temps de sauvegarde et l'espace de stockage nécessaire.

10. Quel est le support le plus approprié ?

Il aurait été approprié de prendre un serveur de backup à part mais dans le cadre de ce projet, il est préférable de n'utiliser qu'une simple partition dans le but de stocker les données.

d. Script

La configuration de ce serveur est sensiblement la même que pour le serveur local du groupe 4 car nous avons utilisé le même script et donc, pour éviter de mettre plus de 20 pages de codes, nous vous proposons un lien github qui redirige vers le script ainsi que des fichiers de configuration :

[Projet_interdisciplinaire/linux at linux · Zafirr-cyber/Projet_interdisciplinaire](#)

e. Caractéristiques des principaux services

Mot de passe du chiffrement des partitions : HopitalPassword!2024

Changement du port SSH & SFTP : 6624

Création de 1 utilisateur pour le serveur :

- administrateur : GlobalHopital

Remarque :

Les utilisateurs n'ont accès au SSH que si et seulement s'ils ont la clef SSH dans leur dossier .ssh (sur windows).

Mise en place d'un mot de passe sur le GRUB :

administrateur : grubG4Linux

Mise en place des options de montage (cf. plan de partition)

Mise en place des backups ainsi que des restaurations de backup (cf. plan de sauvegardes)

Utilisation de SELINUX

Utilisation de firewall-d : (cf. photo ci-dessous)

Services installés et configurés

- **SSH key** : Utilisation de clés ssh pour une connexion sécurisée.
- **Audit** : Configuration de l'audit pour surveiller les changements dans les fichiers critiques.
- **Rootkit** : Installation et configuration de `rkhunter` et `chkrootkit` pour la détection des rootkits.
- **Tests de sécurité** : Installation et exécution de `lynis` pour les audits de sécurité.
- **ClamAV** : Installation et configuration de l'antivirus ClamAV.
- **Fail2Ban** : Installation et configuration de Fail2Ban pour la protection contre les attaques par force brute.
- **Nmap** : Installation et configuration de Nmap pour l'analyse des ports.
- **GRUB** : Configuration de GRUB avec un utilisateur et un mot de passe.
- **Fstab** : Configuration des options de montage pour les partitions.
- **MariaDB** : Installation et configuration de MariaDB.
- **Django** : Utilisation de python pour le web.
- **Cockpit** : Web UI pour la configuration du serveur linux.
- **SELINUX** : Sécurisation des services.