HEH.be
Sciences
et technologies

Avenue V. Maistriau 8a
B-7000 Mons
+32 (0)65 33 81 54
scitech-mons@heh.be

WWW.HEH.BE

Projet Interdisciplinaire

Configuration Linux

Cahier de bord – Configuration Linux

Année Académique 2024-2025

Groupe n°4

Bruyère Maximilien, Denis Cyril, Dubois Théo, Duchesne Guillaume, Mauroit Antoine

WALLONIE-BRUXELLES ENSEIGNEMENT
pôle hainuyer

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 local. Ce serveur a pour but de détenir la base de données locale ainsi que le site web tout en ajoutant certaines sécurités. Ce document vous présentera toutes les manipulations effectuées pour sa configuration.

2. Serveur Linux Local

a. Choix de distribution

Nous avons décidé d'utiliser la distribution Fedora. Cette distribution offre déjà une configuration optimale pour les serveurs (installation préconfigurée). Cette installation possède aussi quelques bibliothèques pour l'installation de certains services (php, fail2ban, clamav, …) ainsi il n'est pas obligatoire d'aller rechercher un dépôt distant pour installer ces services.

b. Plan de partitionnements

Données	Type de périphérique	Système de fichiers	Stockage	Chiffré	Options de montage
/backup	**LVM [Fedora]**	**xfs**	10Go	non	defaults,noexec,nosuid,nodev,relatime
/home	**RAID 1**	**ext4**	2Go x 2	oui	defaults,noexec,nosuid,nodev,relatime
/web	**RAID 1**	**ext4**	3Go x 2	oui	defaults,noexec,nosuid,nodev,relatime

Système	Type de périphérique	Système de fichiers	Stockage	Chiffré	Options de montage
/	**RAID 1**	**xfs**	8Go x 2	oui	defaults,nodev
/boot	**Partition Standard**	**ext4**	1024Mo	non	defaults,ro,nodev,nosuid,noexec
/tmp	**LVM [Fedora]**	**ext4**	1024Mo	non	defaults,noexec,nosuid,nodev
/var	**RAID 1**	**ext4**	3Go x 2	oui	defaults,noexec,nosuid,nodev
/boot/efi	**Partition standard**	**EFI System partition**	1024 Mo	non	/
swap	**LVM [Fedora]**	**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
Nous n'avons pas pensé à faire une partition /database pour stocker les fichiers de la base de données. On l'aurait mise à sauvegarder si on y avait pensé.

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

Pour éviter de mettre plus de 20 pages de codes, nous vous proposons notre lien github qui redirige vers notre script ainsi que du fichier de configuration :

Projet_interdisciplinaire/linux at linux · Zafirr-cyber/Projet_interdisciplinaire

e. Caractéristiques des principaux services

Changement du port SSH & SFTP : 6624

Création de 6 utilisateurs pour le serveur :

- bruyere.maximilien : bruyereG4Linux
- denis.cyril : denisG4Linux
- dubois.theo : duboisG4Linux
- duchesne.guillaume : duchesneG4Linux
- mauroit.antoine : mauroitG4Linux
- ftp-user : ftpG4Linux

Remarque :

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

Mise en place du HTTPS : accès au site via https://www.rehabilitation.hopital.lan

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

Changement du dossier web par défaut : /web/site

Utilisation de firewall-d : autorisation (uniquement) des services nécessaires. (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.
- **FTP** : Configuration de SFTP avec chroot pour les utilisateurs.
- **HTTPD** : Installation et configuration d'Apache HTTP Server avec SSL.
- **MariaDB** : Installation et configuration de MariaDB.
- **PHPMyAdmin** : Installation et configuration de PHPMyAdmin.
- **Cockpit** : Web UI pour la configuration du serveur linux.
- **SELINUX** : Sécurisation des services.