Réalisation professionnelle n°1

Installation de Proxmox via RUFUS et mise en place d'un Fail2Ban

Période	Localisation	Contexte	Situation	Acteurs et partenaires
Ponctuel	☐ Organisation ☒ Centre de formation ☐ Mixte ☐ Autre	☐ Etude ou analyse ☐ Production ☐ Relation/support	☒ Vécue ☐ Observée ☐ Simulée ☐ Mixte	Aucun

1 - Introduction :

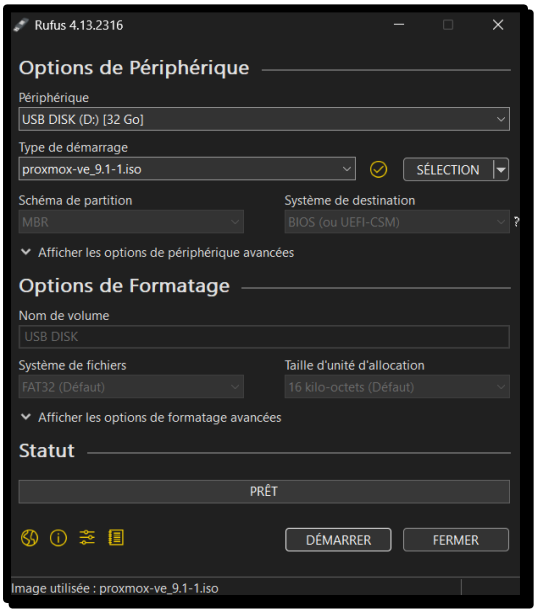
Dans le cadre de ma formation, j'ai dû faire l'installation de Proxmox sur plusieurs postes. Proxmox permet de créer et gérer des machines virtuelles et des conteneurs. Cela permet de centraliser plusieurs serveurs sur un seul système physique.

2 – Prérequis :

- Une clé USB
- Le logiciel Rufus
- L'ISO Proxmox

3 – Mettre l'ISO Proxmox sur la clé USB grâce à Rufus :

Une fois sur le logiciel Rufus et la clé USB insérée dans l'ordinateur :



Mise en place de l'ISO sur la clé

- Dans la partie « périphérique », sélectionné la clé USB
- En cliquant sur sélection, il faut mettre l'ISO de proxmox

Après cela en cliquant sur démarrer, le téléchargement va se lancer et à la fin la clé sera prête à l'emplois afin de lancer Proxmox sur un poste.

4 – Installer Proxmox sur le serveur

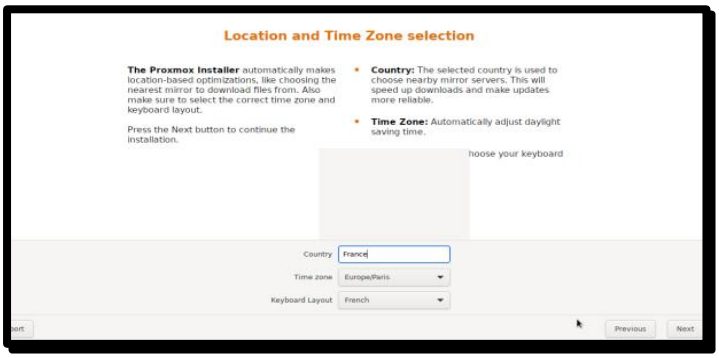
Après avoir branché la clé USB sur le serveur, allumer le serveur et accéder au menu boot en appuyant sur la touche de boot, j'ai sélectionné la version Graphical de Proxmox.

Choix de la version

Il faut ensuite accepter la licence utilisateur et choisir sur quel disque installer Proxmox en fonction de ces besoins.

Ensuite aller dans les options et choisir le système de fichier qui est généralement ext4

Vous pouvez ensuite choisir votre pays, la zone horaire et la langue de saisie du clavier

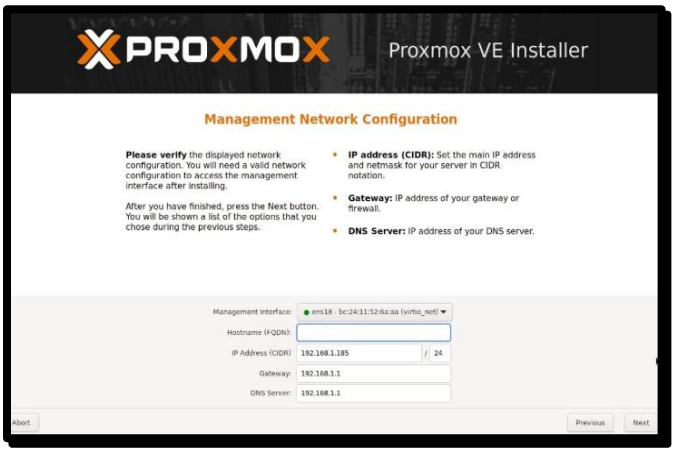


Choix du pays

Ensuite, il faut choisir son mot de passe qui servira par la suite pour se connecter et son mail

Choix du mot de passe

Enfin il faut paramétrer la partie réseau en choisissant son adresse IP, sa passerelle et son DNS



Configuration réseau

Après cela, il est possible de lancer l'installation la configuration de Proxmox.

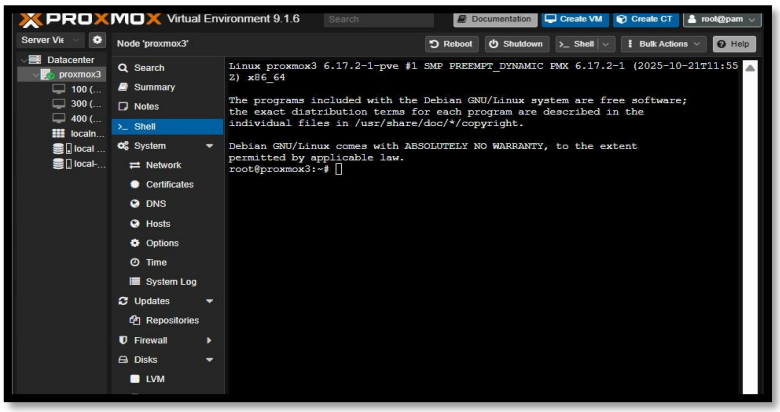
A la fin, pour tester la configuration, je me connecte aux serveurs sur un navigateur web en saisissant https://IP_DU_SRV:8006 et si tout est ok, cela me redirige sur l'interface web de mon serveur après avoir rentré les identifiants.

5 – Mise en place du Fail2Ban :

Une fois sur l'interface web connecté en administrateur, aller dans le shell de l'hôte Proxmox, lancer ces 2 commandes pour mettre à jour les paquets et ensuite pour installer Fail2Ban :

> apt update

> apt install fail2ban



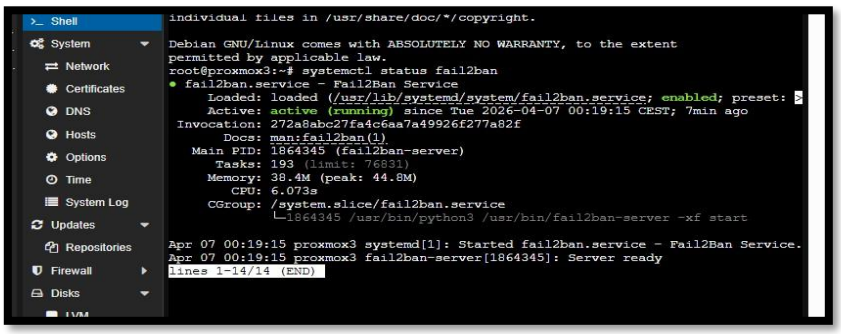
Emplacement du shell de l'interface web Proxmox

Une fois Fail2Ban installé, il va falloir le démarrer, pour cela faire ces 2 commandes afin de le lancer :

>systemctl start fail2ban

>systemctl enable fail2ban

Après cela il est possible de vérifier qu'il est bien lancé avec la commande : >systemctl status fail2ban



Statut du Fail2Ban

Pour la suite, il va falloir configurer la prison, qui sert à configurer les filtres pour indiquer une mauvaise connexion mais aussi les actions qui servent à définir les actions effectuées après des mauvaises connexions.

Pour cette étape il est recommandé de faire une copie du fichier de configuration car celui-ci pourrait être écrasé par des mises à jour, il est donc important de faire une copie pour garder les sécurités appliquées.

Pour ceci faire la commande :

>cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Une fois à cette étape il va falloir modifier 2 sections :

Dans la section [DEFAULT] :

- bantime = (choisir la durée du bannissement)
- findtime = (choisir la durée dans laquelle le nombre de tentative est possible)
- maxretry = (choisir le nombre d'essais avant bannissement
- backend = systemd (afin de lire les logs du journal)
- enabled = true

Dans la section [SSHD] :

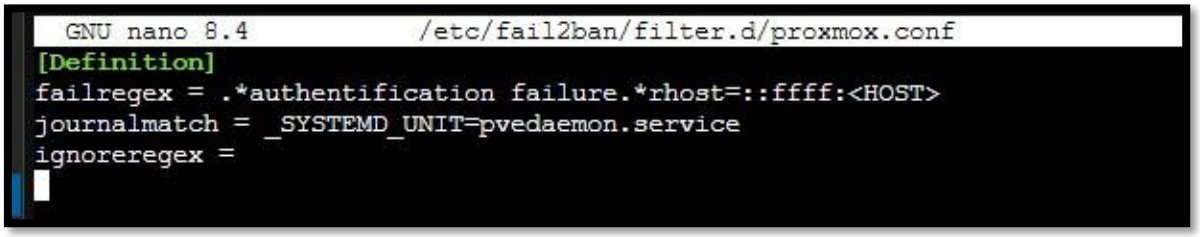
Configuration de la section SSHD

Enfin il va falloir configurer le filtre afin que le système reconnaisse les tentatives de connexions échouées dans les logs. Pour cela faire la commande pour créer un fichier :

>touch /etc/fail2ban/filter.d/proxmox.conf

Et ensuite rentrer les valeurs suivante dedans en le modifiant :

>nano /etc/fail2ban/filter.d/proxmox.conf



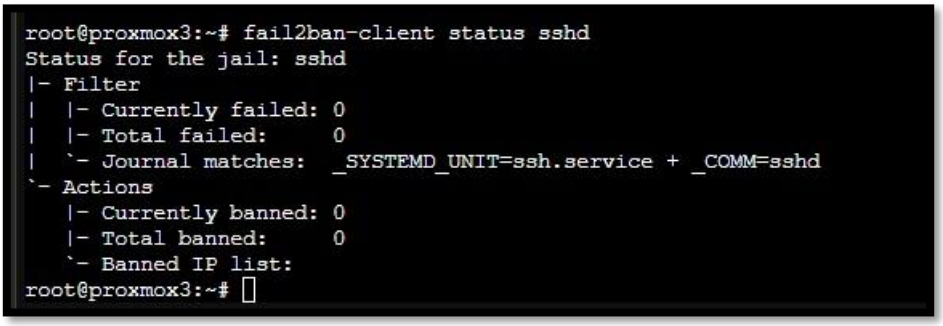
Configuration du filtre

Le fail2ban est alors mis en place, il suffit de relancer le service et de le tester.

>systemctl restart fail2ban

Il est possible de voir la liste du nombre de loupé, de banni et la liste des IP bannis avec la commande :

>fail2ban-client status [type de connexion ex : sshd]



Affichage des alertes pour la connexion SSH

6 – Compétences acquises :

Gérer le patrimoine informatique :

- Recenser les équipements informatiques
- Suivre les versions et configurations
- Suivre les évolutions de l'infrastructure

Mettre à disposition des utilisateurs un service informatique :

- Installer un serveur
- Déployer un service réseau