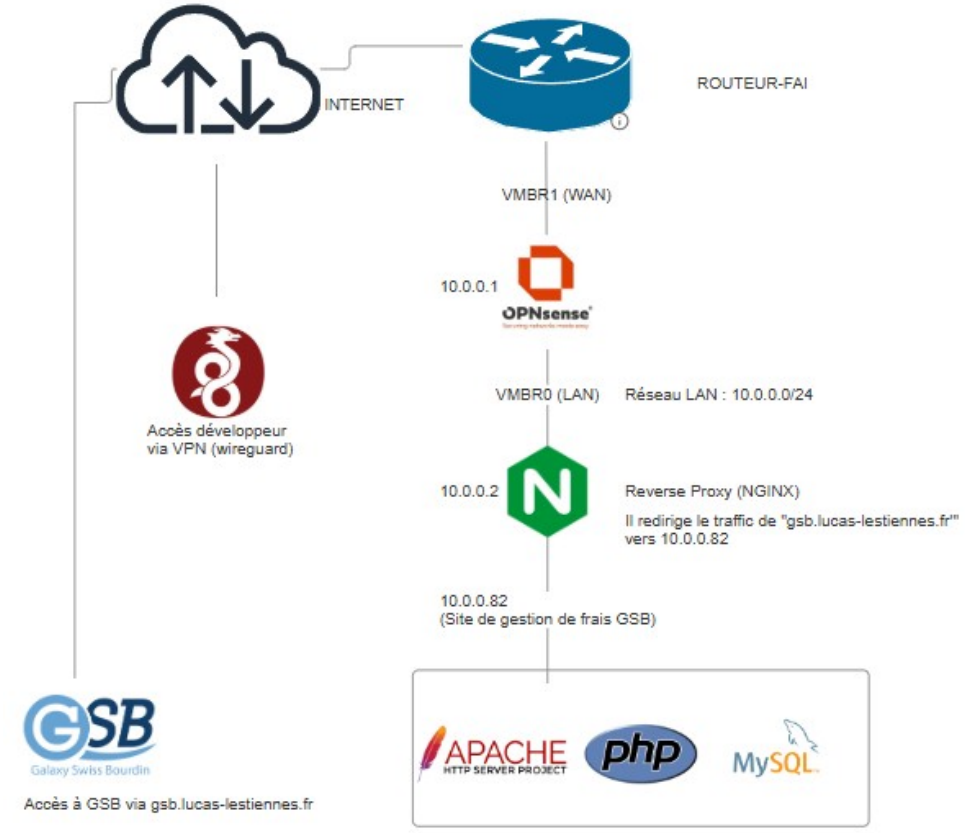
Documentation GSB 1

Documentation Technique pour la Gestion des Frais chez GSB

Sommaire

1. Présentation du réseau & contexte



1. Infrastructure réseau

Le réseau est structuré de la façon suivante :

- **Accès Internet** via un **routeur FAI**.
- **Pare-feu OPNsense** relié à deux interfaces :
  - **VMBr1 (WAN)** : connecté au routeur FAI.
  - **VMBr0 (LAN)** : réseau local interne (plage 10.0.0.0/24).
- Un **serveur NGINX** (reverse proxy) sur l'adresse **10.0.0.2**.
- Une **VM applicative** hébergeant le site de gestion des frais sur **10.0.0.82**, avec Apache2, PHP et MySQL.
- Un **accès VPN WireGuard** permet aux développeurs de se connecter à gsb-gestion-frais depuis l'extérieur et de le configurer via SSH.

2. Détail des composants

OPNsense (10.0.0.1)

- Fait office de pare-feu entre Internet et le réseau local.
- Configure les règles de NAT/pare-feu pour autoriser les connexions entrantes vers NGINX.
- Intègre un serveur VPN WireGuard permettant aux développeurs d'accéder au réseau local en toute sécurité.

NGINX (10.0.0.2)

- Utilisé comme reverse proxy.
- Reçoit les requêtes sur le domaine gsb.lucas-lestiennes.fr (DNS configuré chez OVH).
- Redirige ces requêtes vers l'IP 10.0.0.82 où est hébergé le site.

Site de gestion des frais (10.0.0.82)

- Serveur Apache2 avec PHP et base de données MySQL.
- Application web de GSB installée et accessible en HTTP via le reverse proxy.
- Le site est uniquement accessible via le reverse proxy, donc pas exposé directement à Internet.

3. Étapes de mise en place

1. **Installation des VM** :
    - Déploiement de 3 VMs : OPNsense, NGINX, site GSB.
    - Affectation des IP statiques dans la plage 10.0.0.0/24.
2. **Configuration OPNsense** :
    - Interfaces WAN (VMBr1) et LAN (VMBr0) configurées.
    - Règles de pare-feu : autoriser port 80/443 vers NGINX, port VPN (51820) pour WireGuard.
    - Configuration du serveur WireGuard avec une clé publique/privée et autorisation des IP clientes.
3. **Configuration DNS OVH** :
    - Ajout d'un enregistrement A pointant **gsb.lucas-lestiennes.fr** vers l'IP publique du routeur FAI.
4. **Reverse proxy NGINX** :
    - Configuration du fichier de site pour rediriger le trafic vers 10.0.0.82.
5. **Installation de l'application GSB** :
    - Installation de **Apache2**, **PHP** et **MySQL**.
    - Déploiement du site GSB sur **/var/www/html/gsb**.
    - Configuration de la base de données et des accès.
6. **Connexion VPN** :
    - Création du fichier de configuration client WireGuard.
    - Test de connexion : le développeur peut accéder à 10.0.0.82

Résultat

Grâce à cette architecture, l’accès à l’application de gestion des frais est :

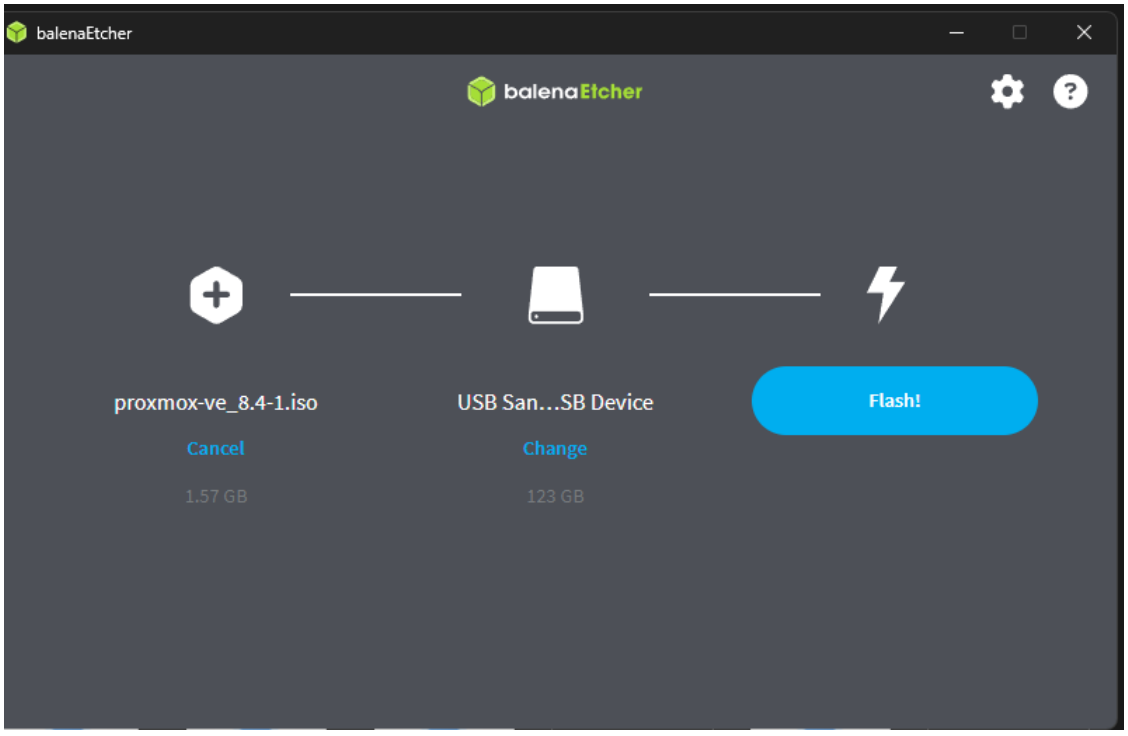
- Sécurisé (VPN + pare-feu).
- Accès via un **reverse proxy**.
- Scalable et maintenable (le reverse proxy peut gérer plusieurs services et sites à l’avenir).

2. Installation et Configuration de Proxmox

Étapes d'Installation

1. **Téléchargement de l'ISO Proxmox VE** :
    - Allez sur le site officiel de proxmox : https://www.proxmox.com/en/downloads et téléchargez la dernière version de l'ISO Proxmox VE.

2. **Création d'un support bootable** :
    - Utilisez un outil comme Balena Etcher (https://etcher.balena.io/#download-etcher) pour créer une clé USB bootable avec l'ISO téléchargée.

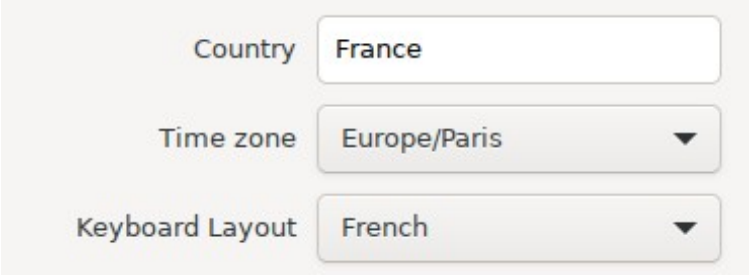


1- Sélectionner l'iso de proxmox
2 - Sélectionner la clé USB sur laquelle sera installé proxmox
3 - Appuyer sur "Flash!" et attendre.

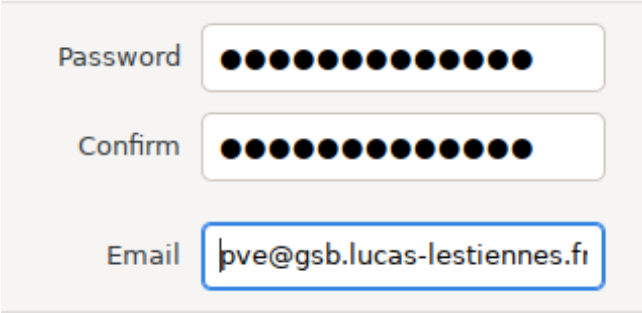
2. **Installation de Proxmox VE**:
    - Démarrer le serveur depuis la clé USB

- Sélectionner "Install Proxmox VE (Graphical)"

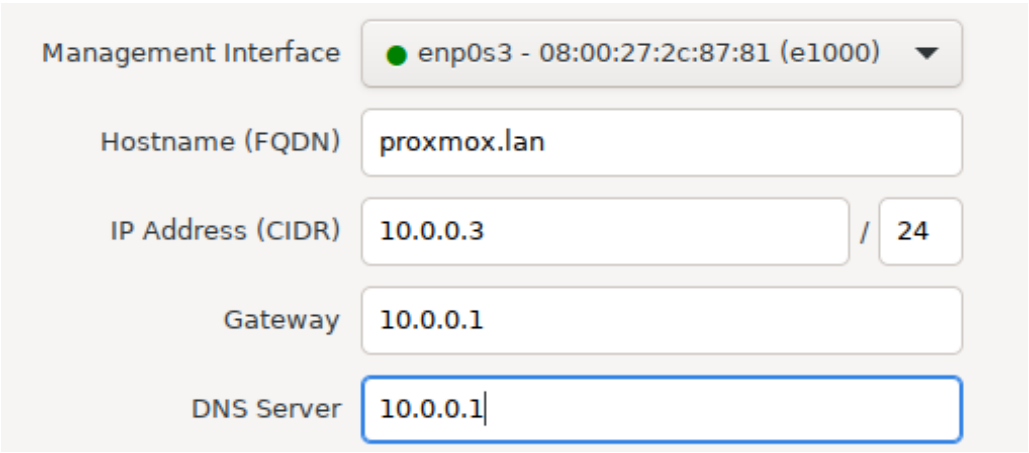
Choisir le disque par défaut pour l'installation de Proxmox



Choisir ces paramètres pour le pays le fuseau horaire & le layout du clavier.



Choisir le mots de passe de proxmox, **il doit être d'au moins 12 charactères, lettre majuscules et minuscule chiffre et charactères spéciaux !** exemple : "EewK!298bzaue.="



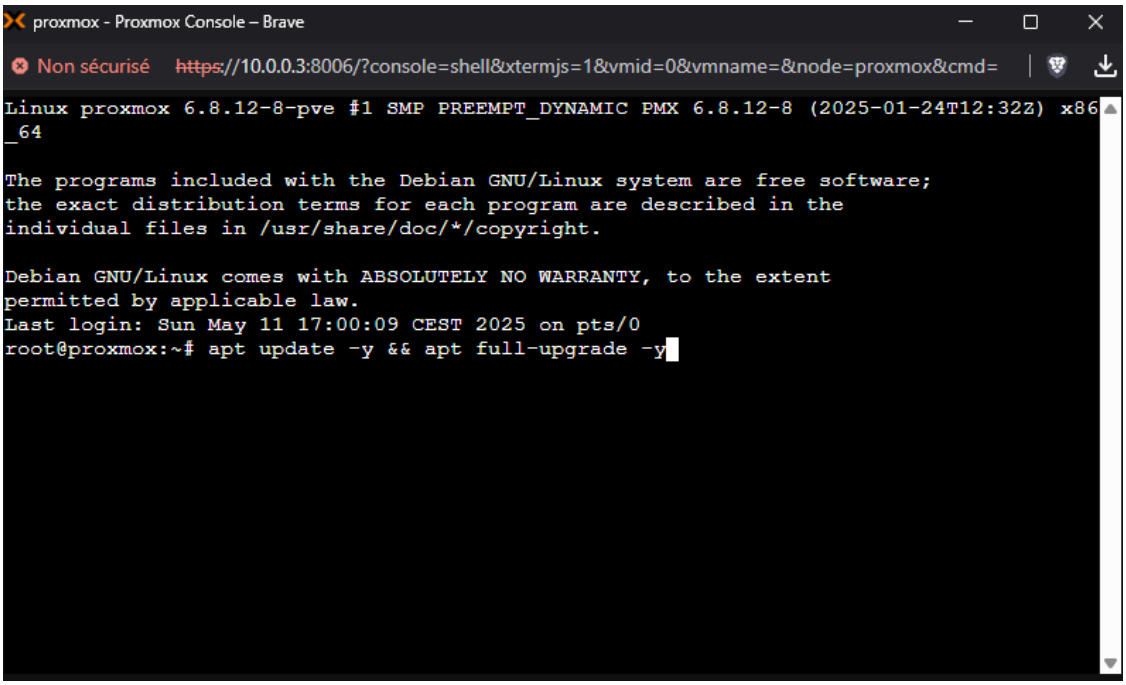
Définir les paramètres d'adressage IP :
l'adresse IP du pour déterminer l'appareil dans le réseau
Gateway pour donner le chemin vers ou aller pour accéder à internet
DNS Serveur pour avoir accès au nom de domaine (exemple : Google.fr)

Valider les paramètres et appuyer sur install.

Configuration Initiale

1. **Accéder à l'interface web** :
    - Après l'installation, accédez à `https://10.0.0.3:8006` pour la configuration initiale.
    - Connectez-vous avec les identifiants par défaut (root/password).
2. **Mise à jour des paquets**:

    ```
    apt update && apt full-upgrade -y
    ```



3. **Configurer le dépôt de mise à jour** :
    - Éditez `/etc/apt/sources.list` et ajoutez les lignes suivantes pour activer le dépôt `no-subscription` :

        ```
        deb http://download.proxmox.com/debian/pve buster pve-no-subscription
        ```

    - Ensuite, mettre à jour la liste des paquets:

        ```
        apt update && apt dist-upgrade -y
        ```

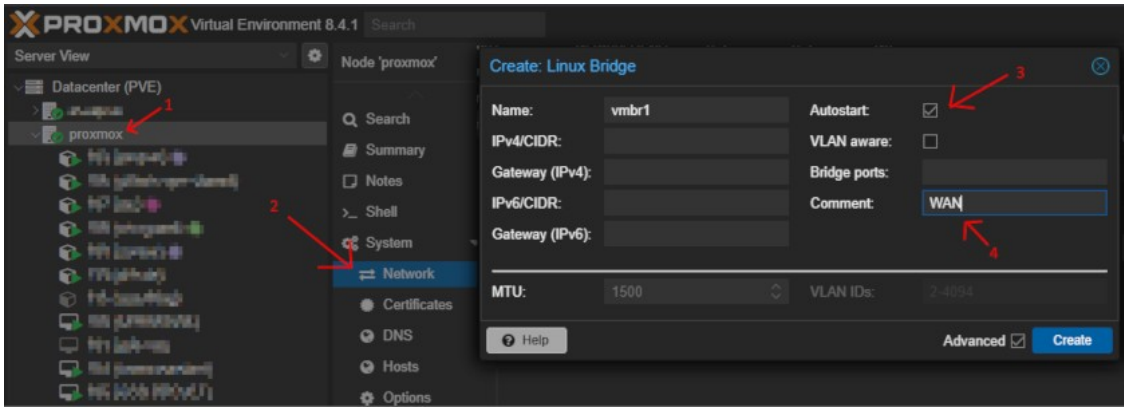
3. Configuration d'OPNsense comme Routeur/Pare-Feu

Prérequis – Création du bridge vmbr1 pour le WAN sur Proxmox

Avant de configurer OPNsense en tant que routeur/pare-feu, il est nécessaire de créer une interface réseau dédiée pour le **WAN**, nommée ici **vmbr1**. Ce bridge permettra de connecter l'interface WAN d'OPNsense à Internet.

Étapes à suivre sur Proxmox :

1. Dans l'interface web de Proxmox, aller dans la section **"Datacenter > proxmox"**, puis cliquer sur **"Network"** (voir étape 1 et 2 sur l'image).
2. Cliquer sur **"Create"** puis **"Linux Bridge"**.
3. Renseigner les champs suivants :
    - **Name** : `vmbr1`
    - **Autostart** : coché ✅ pour activer le bridge au démarrage.
    - **Comment** : `WAN` pour faciliter l'identification.
4. Laisser les autres champs vides (IPv4/IPv6/CIDR, Gateway), car l'adresse IP sera gérée par OPNsense.
5. Cliquer sur **"Create"** pour finaliser la création du bridge.



Installation d'OPNsense

1. **Télécharger l'ISO OPNsense** :
    - Téléchargez la dernière version de l'ISO OPNsense.
2. **Créer une VM sur Proxmox VE**:
    - Allez dans `Proxmox VE` -> `Create VM`.
    - Suivez les étapes pour créer la machine virtuelle en utilisant l'ISO téléchargée.
3. **Installer OPNsense** :
    - Démarrez la VM et suivez les instructions d'installation guidées par le programme d'installation.
4. **Accéder à l'interface web** :
    - Après l'installation, accédez à `https://<votre_ip_opnsense>` pour la configuration initiale.

les logins par défaut sont :
utilisateur : **root**
mots de passe : **opnsense**

Configuration Initiales

1. **Configurer le réseau**:
    - Allez dans `Interfaces` -> `Assignments` et configurez les interfaces LAN/WAN.

vtnet correspond au bridge **vmbr** sur proxmox.

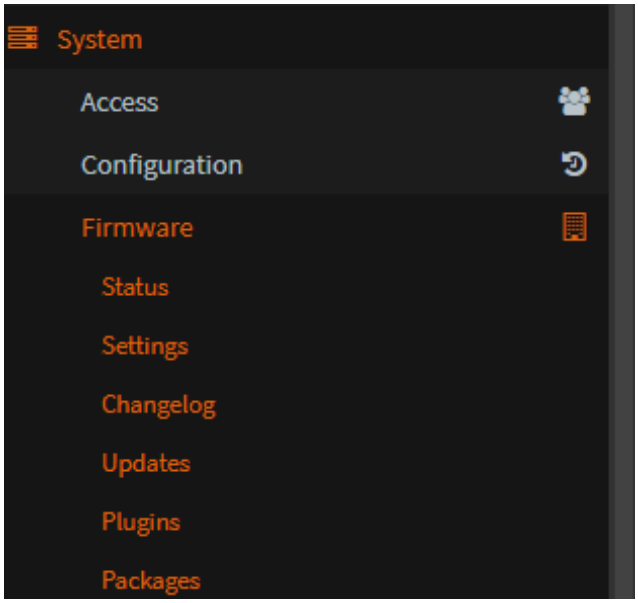
1. **Configurer les adresses IP** :
    - Dans `Interfaces`, configurez l'adresse IP pour l'interface LAN.

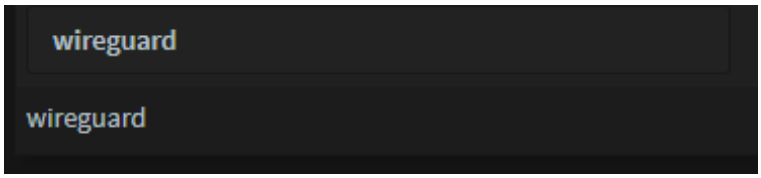
Passerelle en 10.0.0.1 (IP du opnsense)
et le réseau en 10.0.0.0 / 24 (255.255.255.0)

    - L'activation du DHCP n'est pas obligatoire, car de ce cas il s'agit que d'appareil avec des adressage IP statique

Installation et Configuration de WireGuard

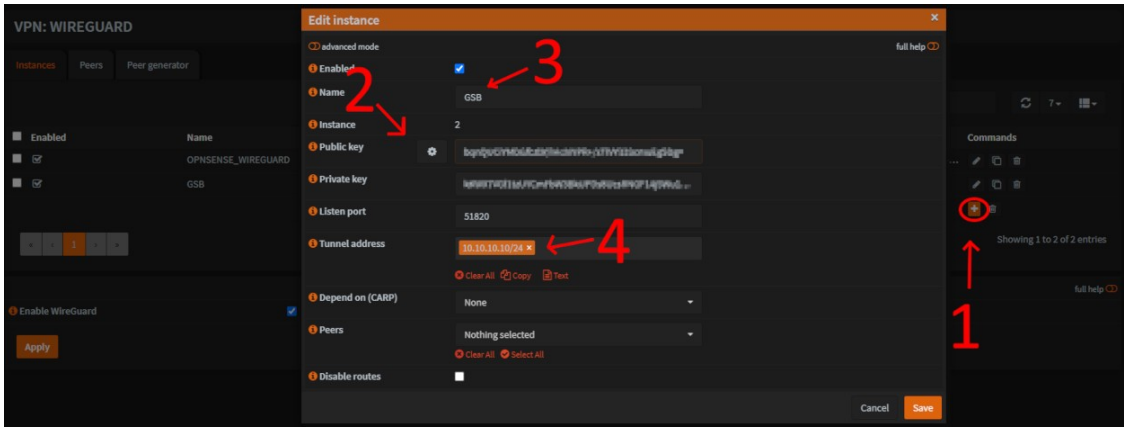
1. **Installer WireGuard**:
    - Allez dans le gestionnaire de paquets (`System` -> `Packages`) et installez WireGuard.





2. **Configurer WireGuard** :

   - Créer une instance avec les étapes suivante



   a. Cliquer sur + pour crée l'instance

   b. Appuyer sur l'engrenage pour générer la clé publique & privée

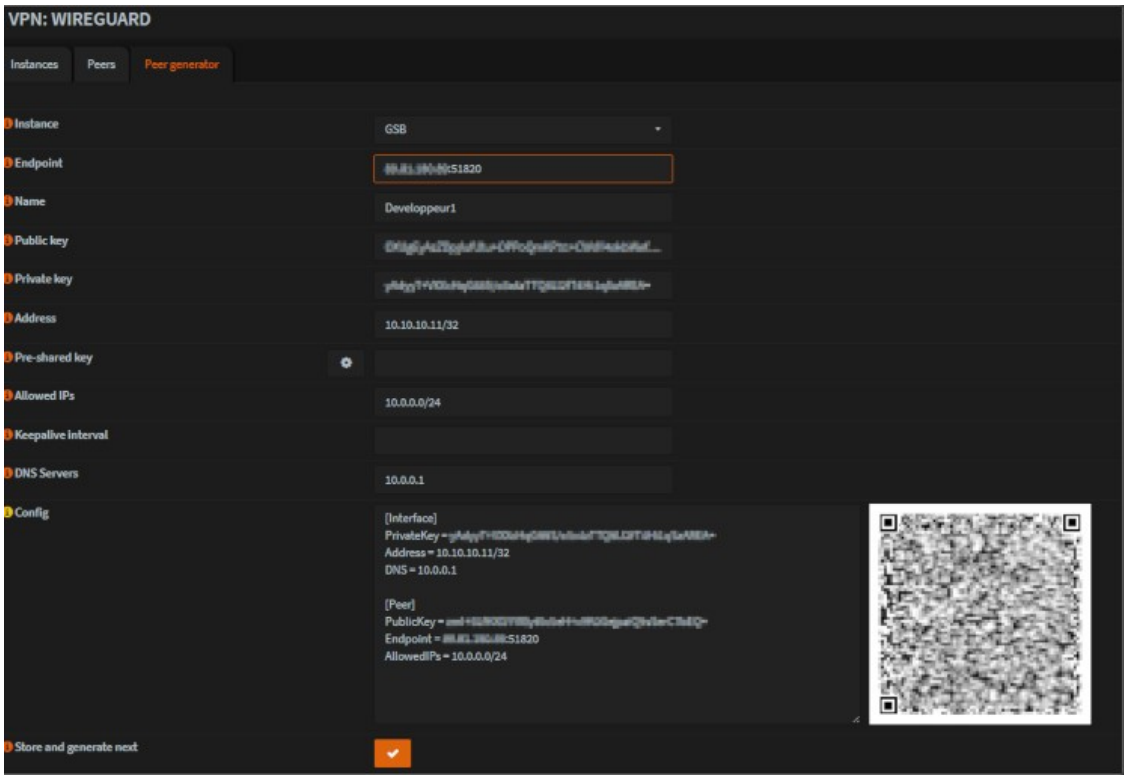
   c. Nommer l'instance (GSB)

   d. Dans *"tunnel adress"* choisir 10.10.10.10/24 il s'agira du réseau dans lequel sera les connection au VPN Wireguard.

Ajout de peers (Utilisateurs du VPN)

Configuration VPN – Ajout d'un peer via le **Peer Generator** (WireGuard)

Pour permettre un accès sécurisé à l'infrastructure de GSB à distance, nous avons mis en place un **VPN WireGuard** sur OPNsense. Le **Peer Generator** simplifie la création d'un utilisateur distant (ici, pour un développeur).



Exemple de configuration d’un peer (Développeur1)

L'image ci-dessus montre l'interface de génération d’un peer WireGuard sur OPNsense.

Voici les champs essentiels :

- **Instance** : nom du serveur WireGuard (ici `GSB`).
- **Endpoint** : l’adresse IP publique (ou nom de domaine) du serveur suivie du port utilisé (par défaut, `51820`).
- **Name** : identifiant du client (ex. : `Developpeur1`).
- **Public/Private Key** : paires de clés générées automatiquement.
- **Address** : IP du client dans le tunnel (ex. `10.10.10.11/32`).
- **Allowed IPs** : plages autorisées à passer par le VPN (ici `10.0.0.0/24`, correspondant au LAN interne).
- **DNS Servers** : ici `10.0.0.1` (OPNsense), utilisé pour résoudre les noms internes.
- **Config** : fichier de configuration automatiquement généré, copiable ou scannable via QR code.

  Utilisation :
  L’utilisateur peut scanner le **QR code** avec une application WireGuard (mobile ou desktop) pour importer automatiquement la configuration et se connecter au réseau GSB via VPN.

Configuration du NAT et des Règles de Pare-Feu sur OPNsense

Une fois OPNsense configurer avec WireGuard, on peut appliquer les règles de pare-feu nécessaire pour wireguard et pour le reverse proxy.

1. Une règle de **NAT (Port Forwarding)** pour rediriger le trafic entrant vers le reverse proxy NGINX.
2. Des **règles de pare-feu** pour autoriser uniquement le trafic nécessaire (web et VPN notamment).

1. Règle NAT – Redirection du port 80/443 vers le reverse proxy

Objectif : rediriger les connexions HTTP/HTTPS (ports 80/443) arrivant sur l'IP publique vers le reverse proxy NGINX (`10.0.0.2`).

Étapes :

- Aller dans **Firewall > NAT > Port Forward**.
- Cliquer sur **Add** (+).
- **Interface** : `WAN`
- **Protocol** : `TCP`
- **Destination port range** : `80 - 443`
- **Redirect target IP** : `10.0.0.2`
- **Redirect target port** : `80 - 443`
- **Description** : `Redirection web vers Reverse Proxy`

Cocher "NAT reflection" si besoin d'accès local via IP publique.

2. Règles de Pare-Feu – Autoriser le trafic nécessaire

Objectif : sécuriser l'accès à l'infrastructure en ouvrant uniquement les ports utiles sur l'interface WAN.

Aller dans **Firewall > Rules > WAN**, puis ajouter les règles suivantes :

Action	Interface	Protocol	Port	Source	Destination	Description
Pass	WAN	TCP	80	any	WAN address	Autoriser HTTP vers Reverse Proxy
Pass	WAN	TCP	443	any	WAN address	Autoriser HTTPS vers Reverse Proxy
Pass	WAN	UDP	51820	any	WAN address	Autoriser VPN WireGuard

Ensuite, dans **Firewall > Rules > LAN**, ajouter une règle pour autoriser tout le trafic sortant depuis le réseau LAN (`10.0.0.0/24`) :

Action	Interface	Protocol	Source	Destination	Description
Pass	LAN	any	LAN network	any	Autoriser le trafic LAN

Tester l'accès externe via `https://gsb.lucas-lestiennes.fr`.

Vérifier les logs dans **Firewall > Log Files > Live View** pour diagnostiquer en cas de problème

GeoIP et Filtrage IP (Protection réseau)

L'objectif de cette section est de restreindre l'accès à l'infrastructure uniquement aux pays autorisés (ici : **France**) et de bloquer automatiquement les IP malveillantes détectées par **Maltrail**.

Installation du plugin GeoIP

Étapes :

Aller dans **System > Firmware > Plugins**.
Rechercher le plugin : `os-maxmindgeoip`.
Cliquer sur **+ Install** à droite.
Une fois installé, redémarrer le service **Firewall / Aliases** si nécessaire.

Ce plugin permet d'utiliser les bases de données MaxMind pour filtrer le trafic réseau selon le pays d'origine des IP.

Téléchargement de la base GeoIP

- Aller dans **Firewall > Aliases > GeoIP settings**.
- Renseigner une adresse e-mail valide (obligatoire pour accepter la licence MaxMind).
- Cliquer sur **Download GEOIP Data** pour récupérer la dernière base.
- Vérifier que le statut passe à **Last update successful**.

Création d'un alias GeoIP (autoriser uniquement la France)

Étapes :

- Aller dans **Firewall > Aliases**.

- Cliquer sur **+ Add**.
  - **Name** : `GeoIP-France`

  - **Type** : `GeoIP`

  - **Countries** : cocher uniquement **France**

  - **Description** : `Alias IPs France`

  Enregistrer et appliquer.

3. Création d'une règle pare-feu WAN : ***Bloquer tout le traffic qui n'est pas français***

- Aller dans **Firewall > Rules > WAN**.
- Ajouter une règle **en haut de la liste** :
  - **Action** : `Block`
  - **Interface** : `WAN`
  - **Source** : `! GeoIP-France` (le `!` signifie « tout sauf la France »)
  - **Destination** : `any`
  - **Description** : `Blocage IPs hors France`
- Enregistrer et appliquer.

Résultat : Seuls les utilisateurs avec une IP géolocalisée en France pourront accéder au services GSB.

Intégration de l’alias Maltrail pour bloquer les IPs malveillantes

Maltrail (surveille les logs et détecte les comportements suspects) et génèrer un alias d’IP à bloquer.

Donc à partir de l'alias générer automatiquement, on peut créer une règle de pare-feu qui va filtrer et empêcher l'accès aux adresses IP qui ont été détecter comme malveillante.

- Aller dans **Firewall > Rules > WAN**
- Ajouter une nouvelle règle :
  - **Action** : `Block`
  - **Interface** : `WAN`
  - **Source** : l’alias généré BlocklistMaltrail
  - **Destination** : `any`
  - **Description** : `Blocage IPs malveillantes détectées`

Cette règle doit être **placée avant** toute autre règle "Pass" pour qu'elle s’applique en priorité.

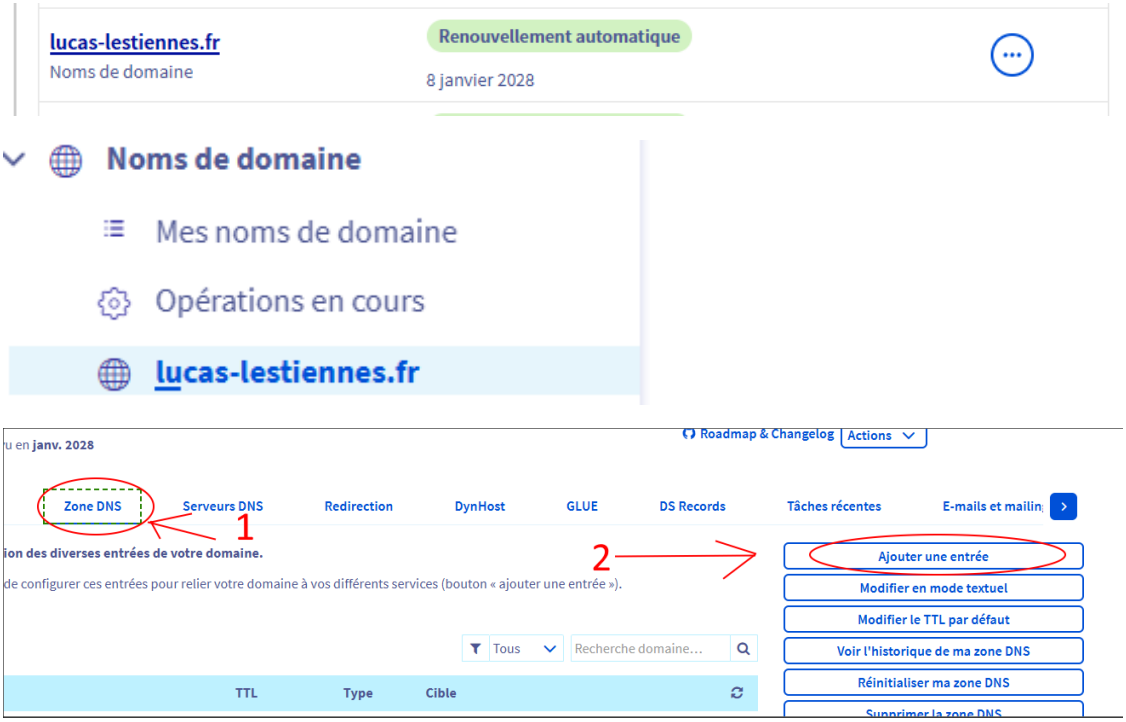
Conclusion :
Grâce à GeoIP et Maltral :

- On autorises uniquement les connexions françaises.
- On bloques en temps réel les IPs malveillantes automatiquement repérées.

5. Configuration DNS sur OVH

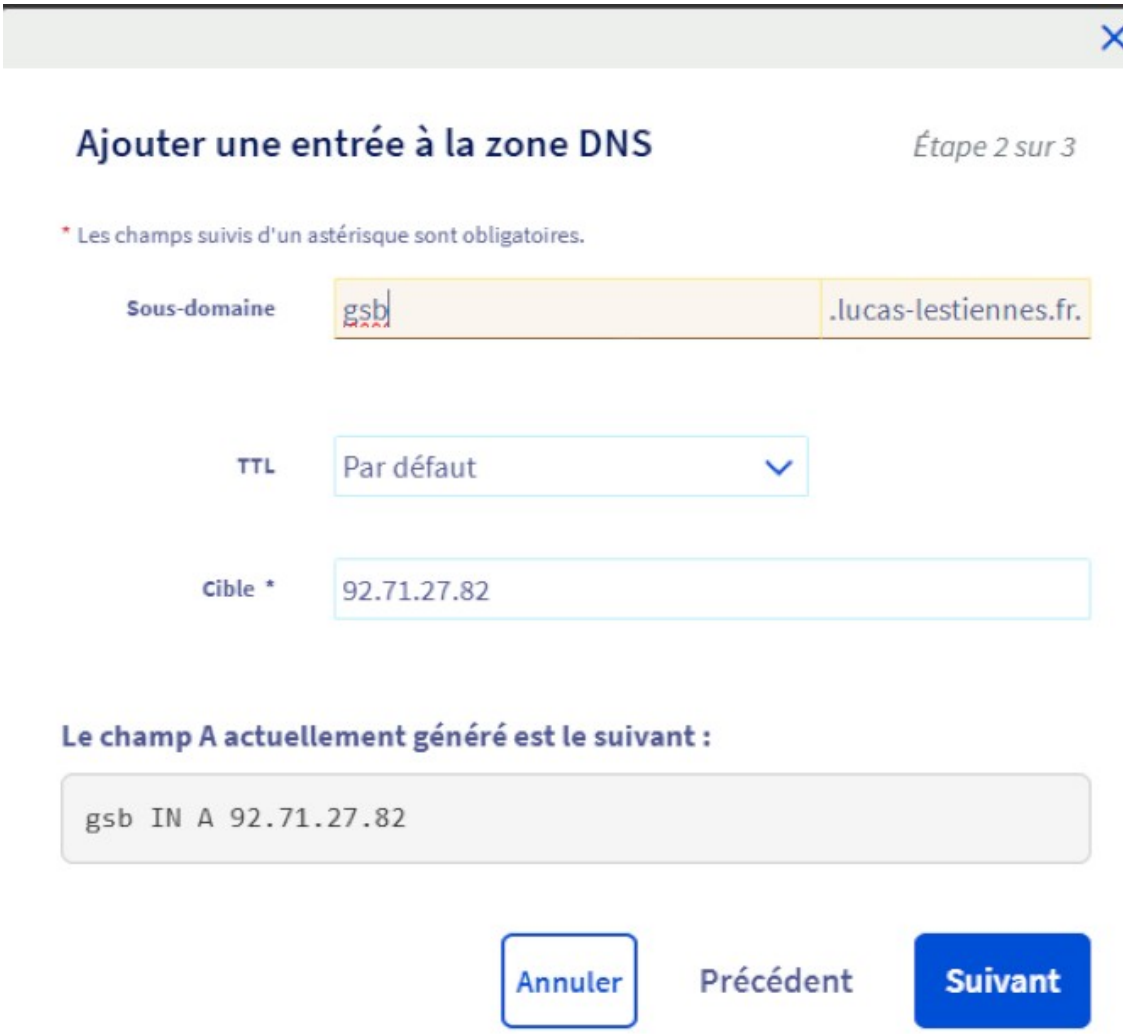
Ajouter un domaine

1. **Accéder à OVH**:
    - Connectez-vous à votre compte OVH et allez dans gestion de nom de domaine.



2. Ajouter le domaine :

- Ajoutez un enregistrement de type A avec comme information : **gsb** et en destination l'adresse IP public du routeur.
  Exemple : gsb.lucas-lestiennes pointe vers ---> l'ip publique



Puis attendre que le changement de domaine s'appliquer sur tout les serveurs DNS racines, généralement le délai est de moins de 10mn.

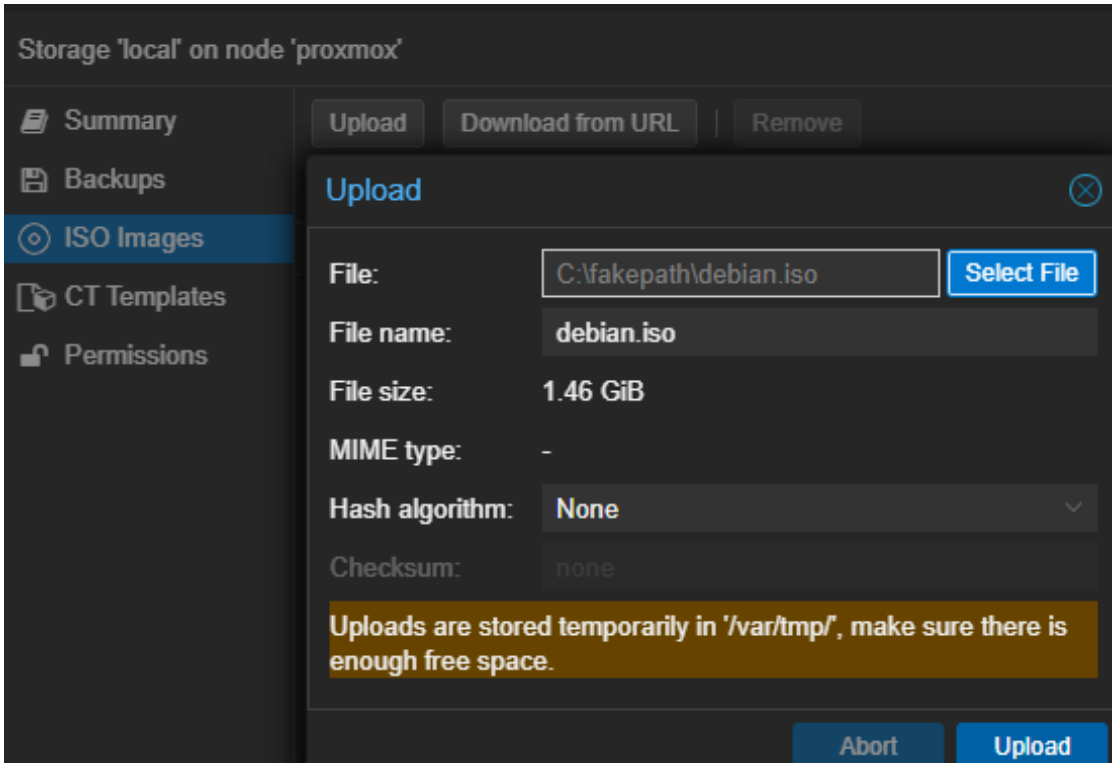
6. Création VM debian-reverse-proxy et configuration de NGINX Reverse Proxy avec Docker Compose

Installation de la VM debian-reverse-proxy de Docker et Docker Compose

0.Téléchargement de l'iso de debian sur proxmox

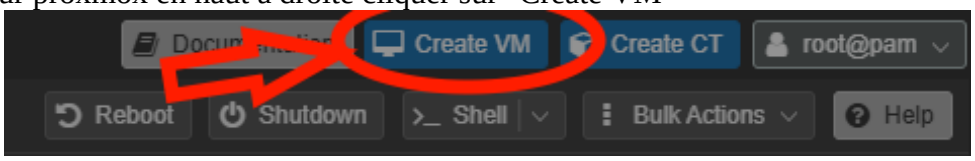
Télécharger l'image "netinst" pour amd64 : `debian-12.x.x-amd64-netinst.iso`

Puis uploader le fichier iso dans Datacenter / Proxmox / Stockage (**Local**)

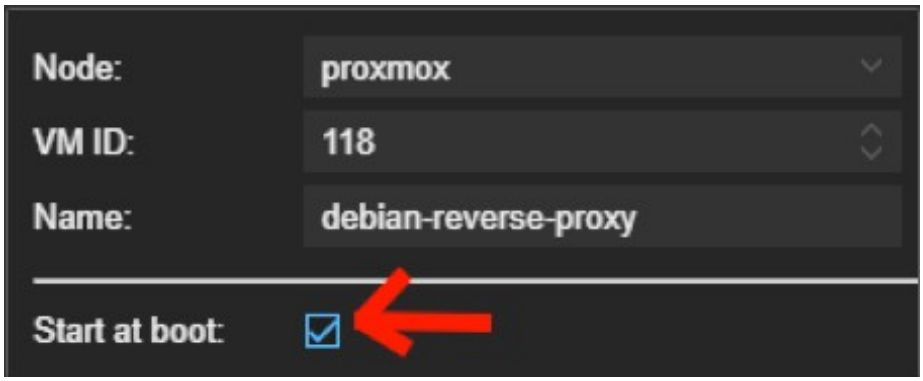


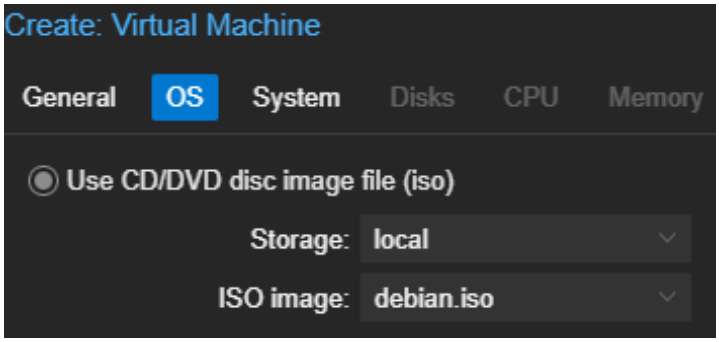
Dans select file choisir sur son ordinateur le fichier ISO de debian télécharger précedemment.

1. Création de la VM debian-reverse-proxy
   Sur proxmox en haut à droite cliquer sur "Create VM"



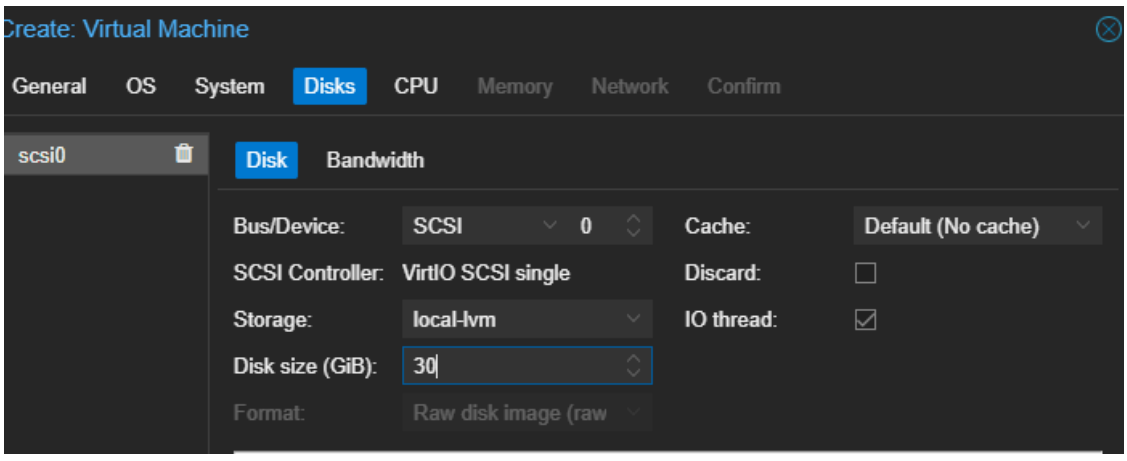
Ensuite entrer le nom de la machine virtuelle, dans ce cas il s'agit de **debian-reverse-proxy**
Ne surtout pas oublier de cocher "***Start at boot***" cela permet de faire automatiquement démarrer la machine virtuelle quand le serveur se rallume par exemple.





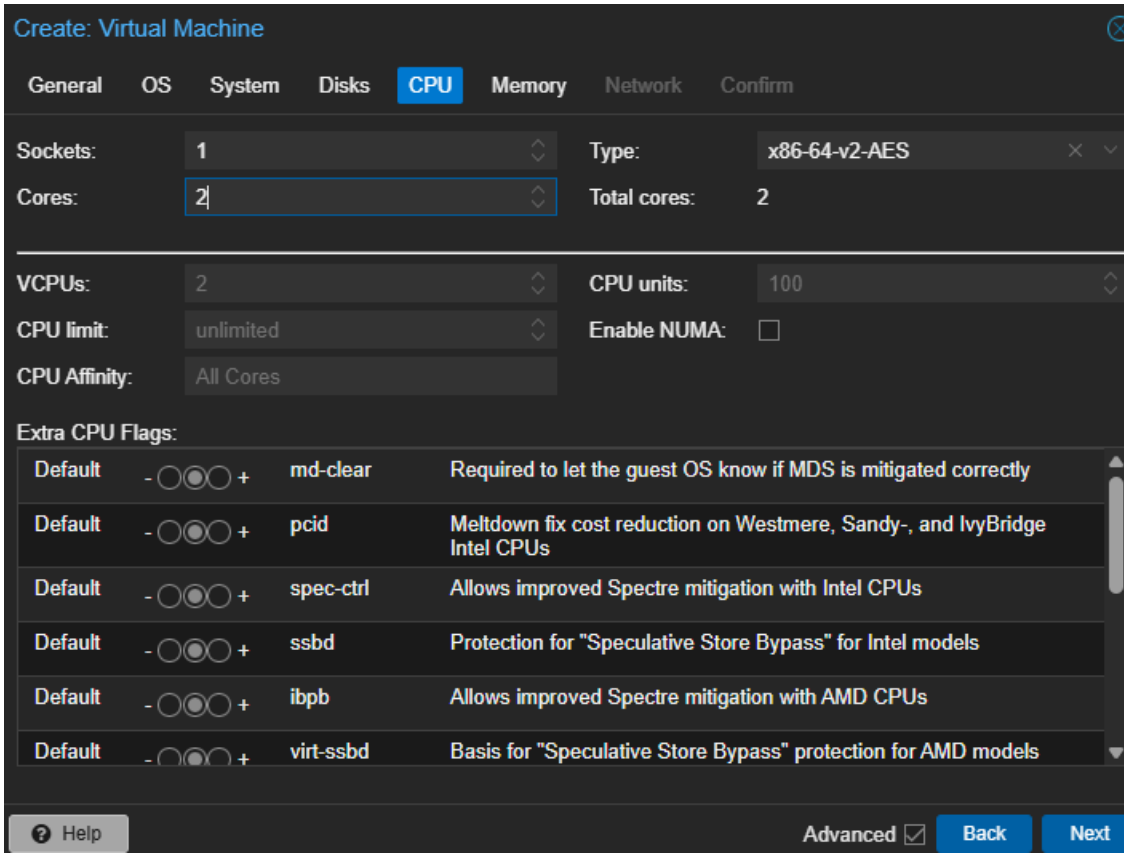
Sélectionner dans "Storage" '**local**' et comme iso prendre debian celui qui as été importer précédemment.

- Laisser l'onglet **System** telle quel

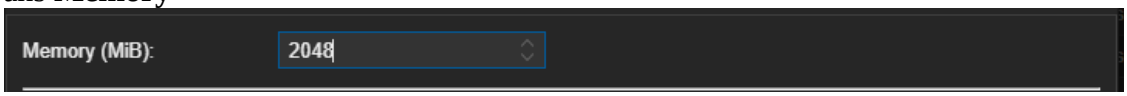


- Dans l'onglet "*disks*" choisir une taille de disque de 30GiB

- Dans CPU choisir deux cœurs dans l'onglet core, pas besoin de toucher à d'autres paramètres.

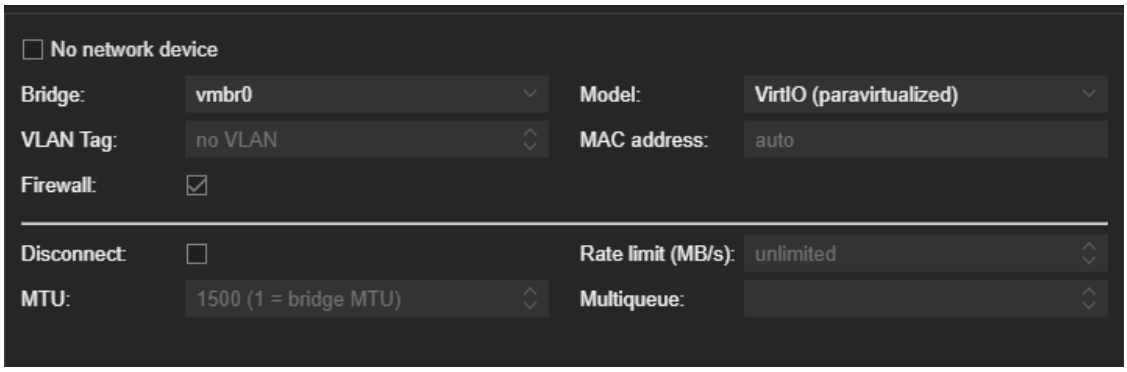


- Dans **Memory**

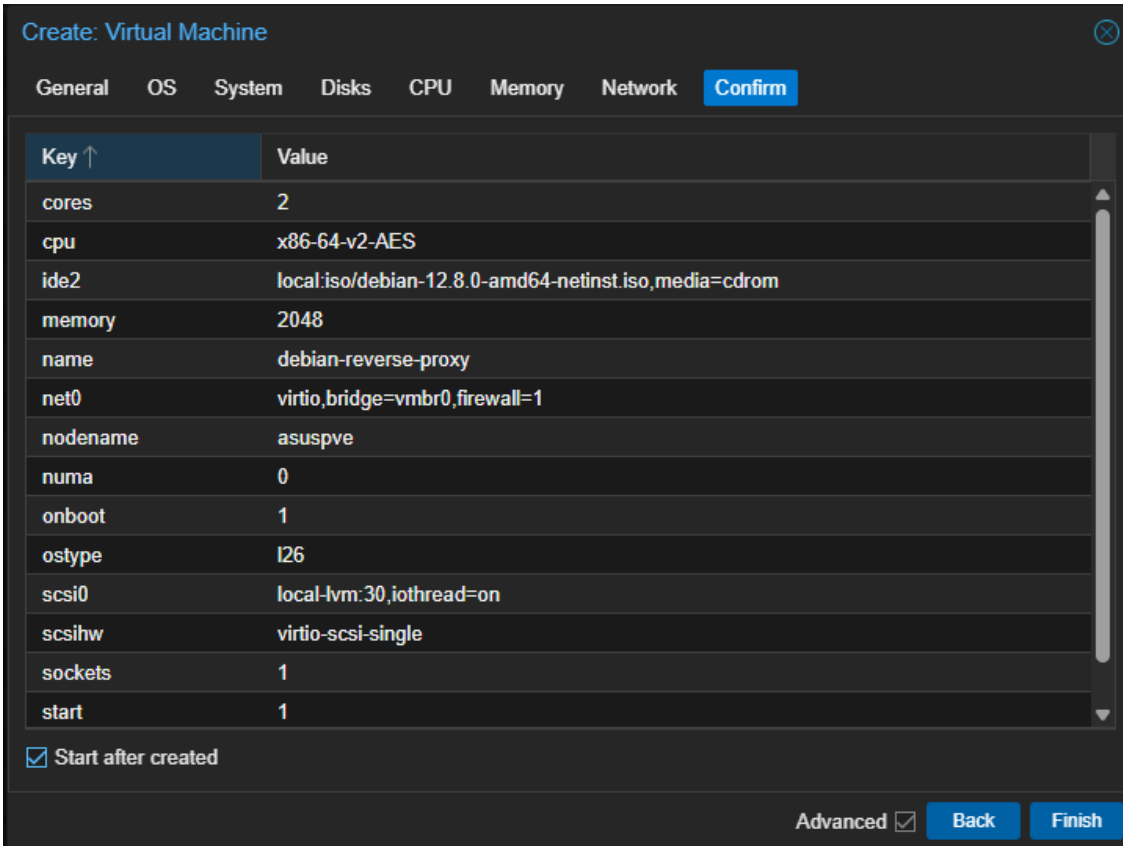


Choisir 2048, la VM à juste comme rôle de reverse proxy donc pas besoin d'énormément de ressources.

- Dans **Network**



Laisser tel quel nous utiliserons le bridge par défaut.



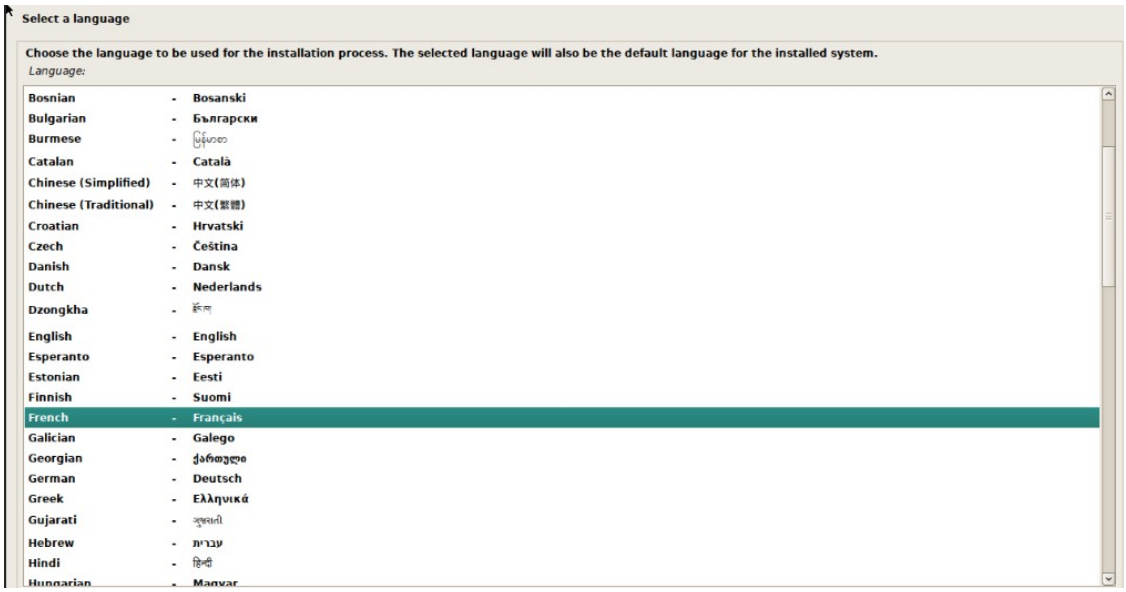
Valider et cocher **Start after created**

Pour accéder à la console de la VM, sélectionner la VM en cliquant dessus puis en appuyant sur console on as un retour, comme si la machine était connectée à un écran

Installation de debian

1. Choix de la langue

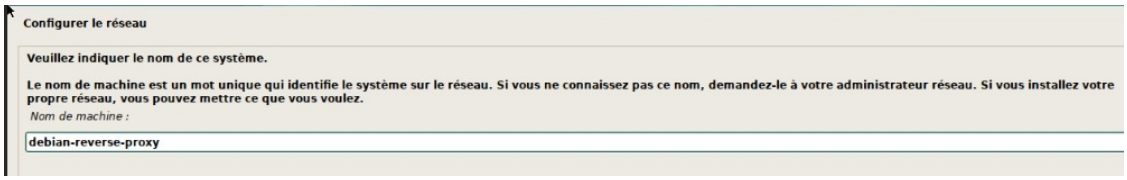
Sélectionner : **Français**



2. Configuration réseau

- Mode : **Manuel**

- Adresse IP : `10.0.0.2`
- Masque : `255.255.255.0` (ou `/24`)
- Passerelle : `10.0.0.1`
- DNS : `10.0.0.1`
- Nom d’hôte : `debian-reverse-proxy`



Domaine : laisser vide

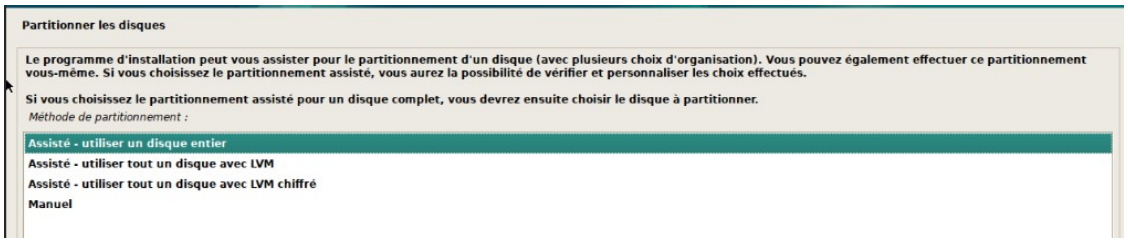
3. Configuration des utilisateurs

Définir un mot de passe root sécurisé.

Créer un utilisateur normal (ex. : `admin`) avec un mot de passe sécurisé. **il doit être d'au moins 12 charactères, lettre majuscules et minuscule chiffre et charactères spéciaux !** exemple : "EewK!298bzaue.="

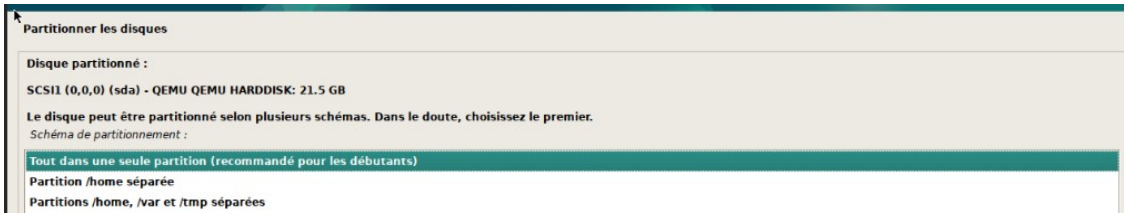
4. Partitionnement des disques

- Sélectionner : **Assisté – utiliser un disque entier**



- Choisir le disque disponible

- Type de partitionnement : **tout sur une seule partition**



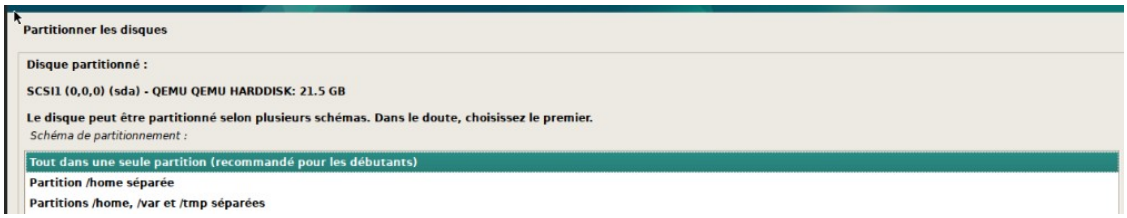
- Valider les modifications et écrire les changements sur le disque.

5. Sélection des logiciels

Il serait conseillé de ne cocher que :

✅ Utilitaires usuels du système et Serveur SSH

Décocher les autres (Environnement de bureau, serveur web, etc.)



6. Finalisation de l'installation

Laisser l’installation se terminer.

Une fois terminé, retirer l’ISO dans l’onglet "Hardware" de Proxmox si ce n’est pas automatique.

Redémarrer la VM.

Créer compte administrateur de secours :

```
sudo adduser administrateur
sudo usermod -aG sudo administrateur
groups administrateur
```

Installer Docker :

- Installez Docker en suivant les instructions suivante, ces commandes peuvent être mise dans un .sh (script bash) pour automatiser les commandes

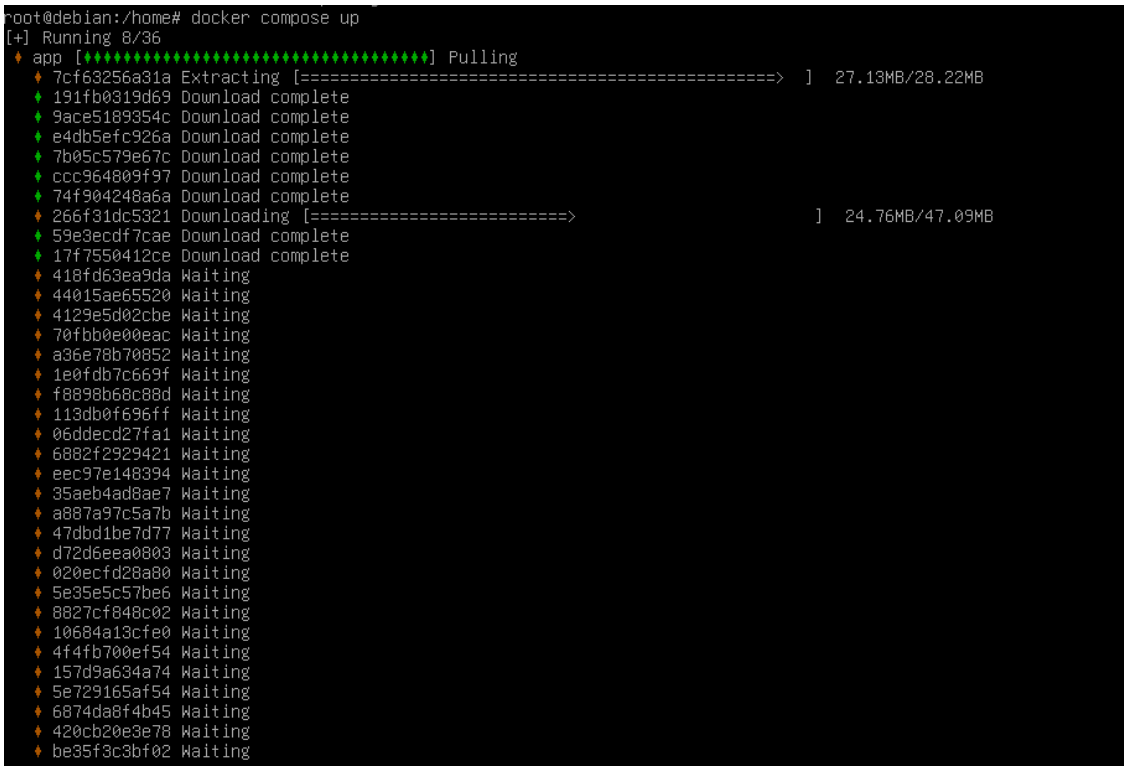
```
sudo curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --
dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io
sudo systemctl enable docker
```

1. **Créer un fichier `docker-compose.yml`** avec le contenu suivant à l'intérieur :

```
services:
app:
image: 'docker.io/jc21/nginx-proxy-manager:latest'
restart: unless-stopped
ports:
- '80:80'
- '81:81'
- '443:443'
volumes:
- ./data:/data
- ./letsencrypt:/etc/letsencrypt
```

2. **Démarrer les services** :
    - Démarrez NGINX avec Docker Compose:

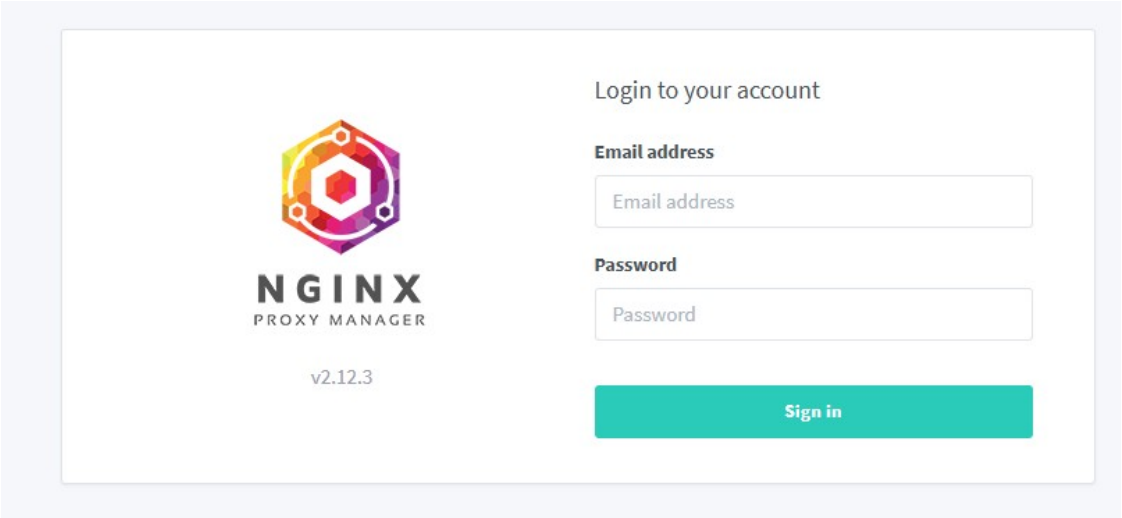
```
docker-compose up
```



si l'installation s'est bien déroulée, on peut faire CTRL + C pour éteindre le container et le redémarrer avec la commande " docker-compose up **-d**" pour le mettre en arrière plan.

7. Configuration de Certificats HTTPS avec Nginx Reverse Proxy

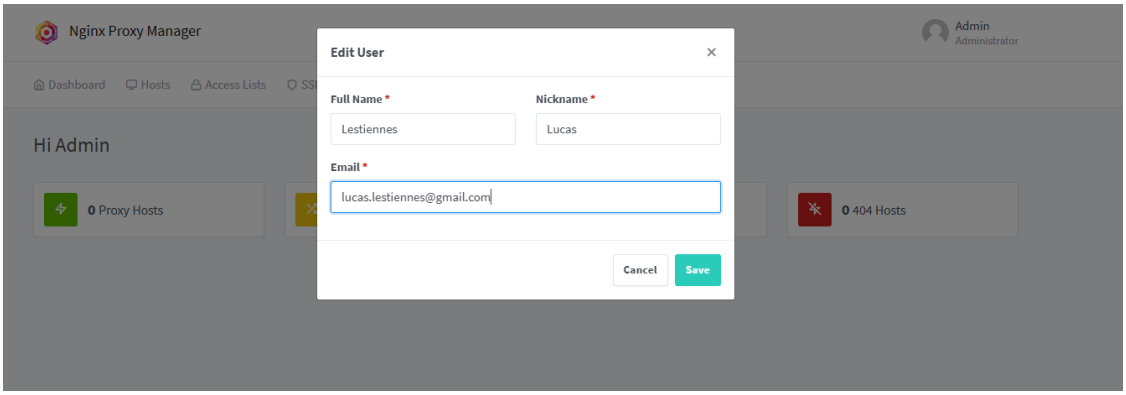
a. Se connecter à l'interface face de nginx proxy : 10.0.0.2:81



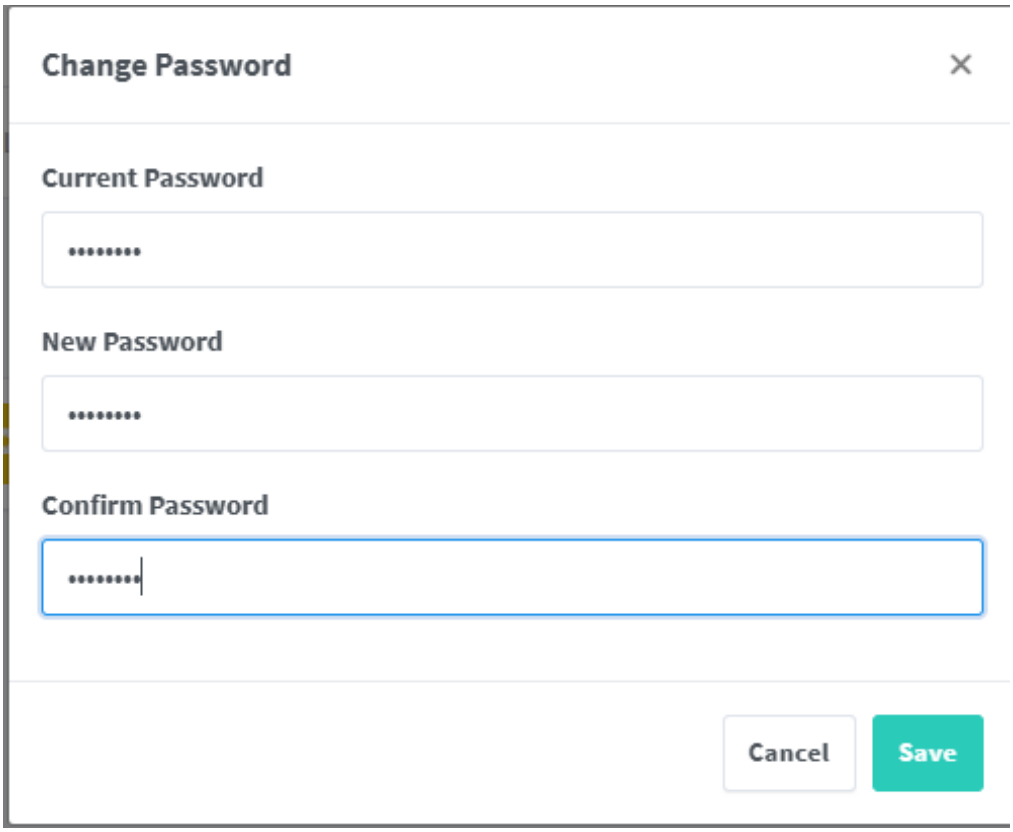
les identifiants par défaut sont les suivants :

```
Email:    admin@example.com
Password: changeme
```

3. **Configurer la redirection HTTPS** :
    - Modifiez votre fichier de configuration Nginx pour rediriger le trafic HTTP vers HTTPS.



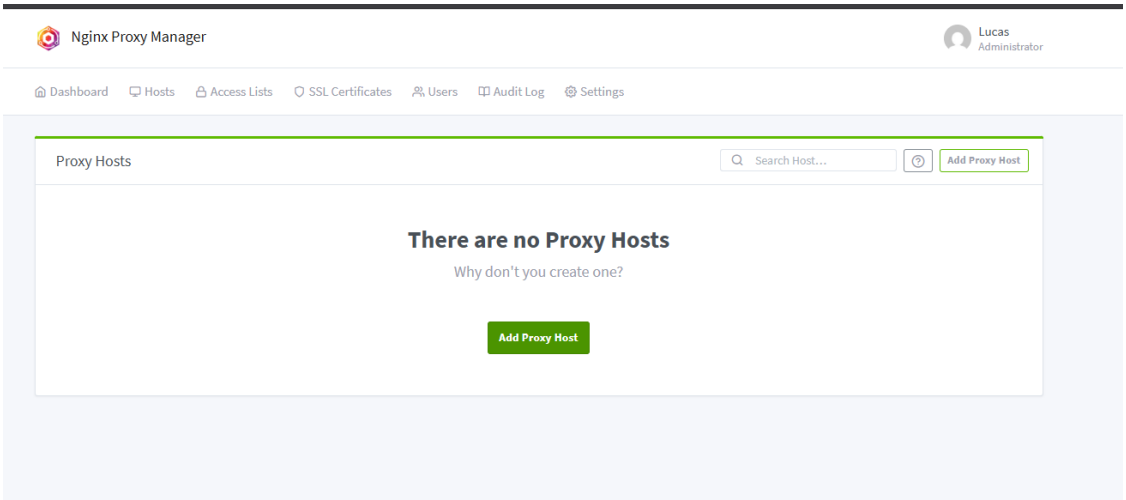
Au démarrage, il sera nécessaire de mettre à jour les informations sur l'administrateur du service nginx



Il sera aussi nécessaire de change le mots de passe par défaut.

Allez dans l’onglet "Proxy Hosts".

Cliquez sur "Add Proxy Host".



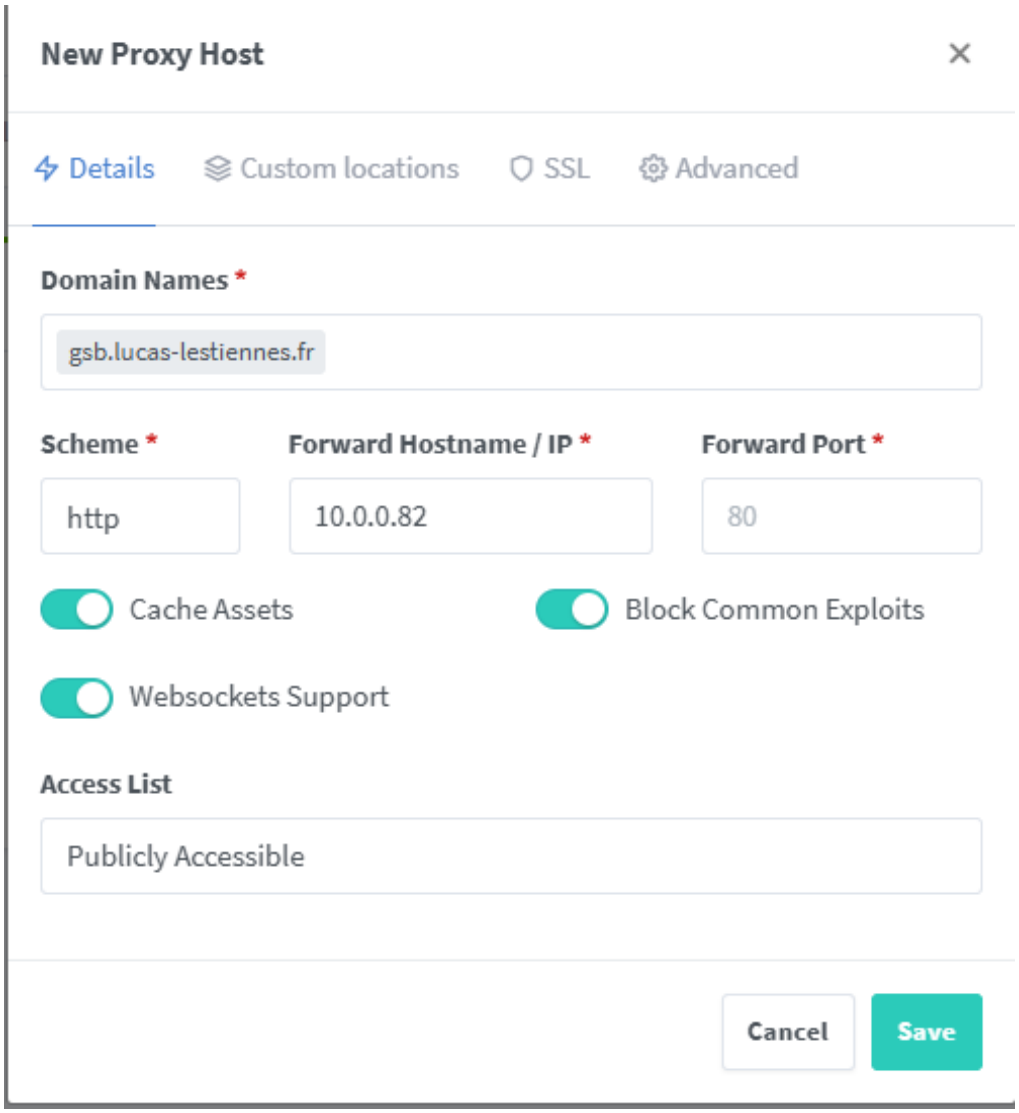
Remplir les informations :

Domain Names : gsb.lucas-lestiennes.fr

Forward Hostname / IP : 10.0.0.82

Forward Port : 80

Block Common Exploits : cochez.



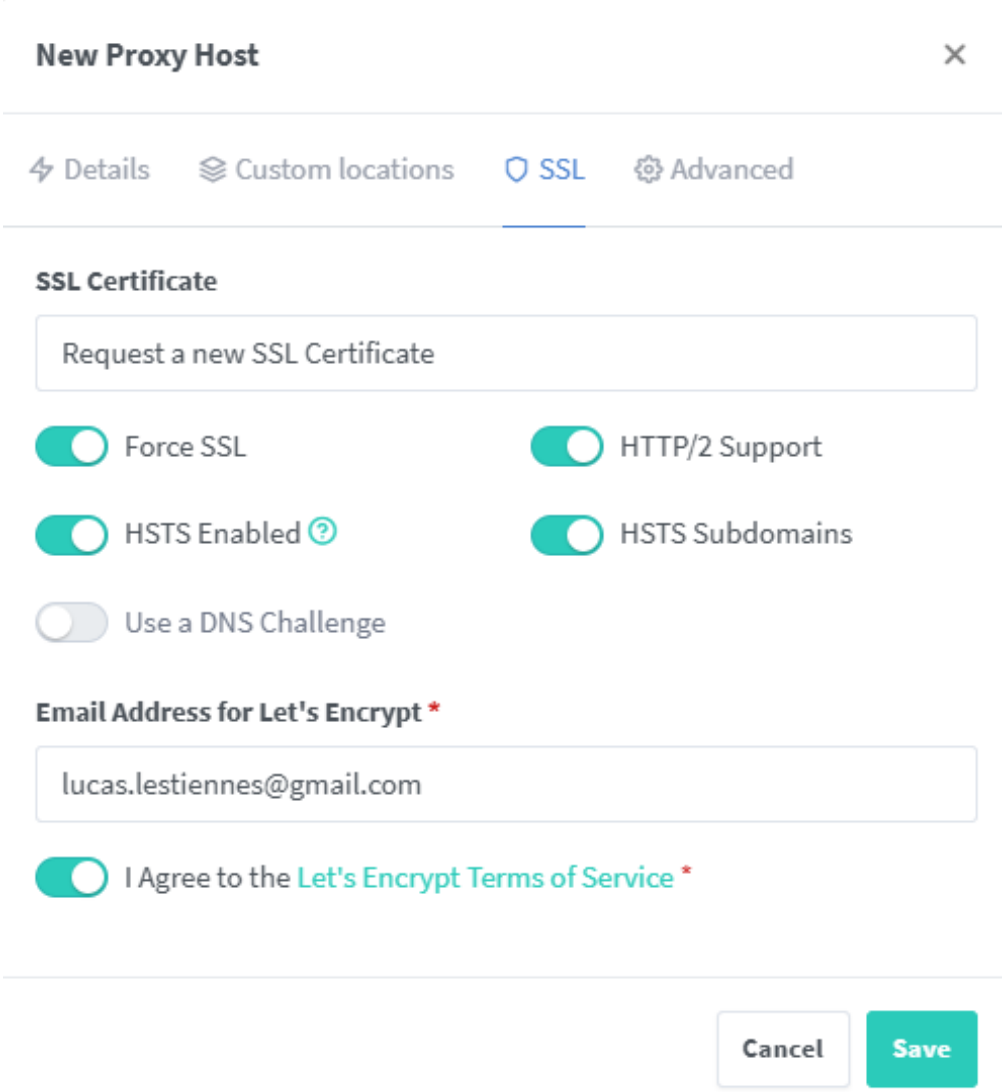
Allez dans l’onglet SSL.

Cochez :

Block HTTP

Force SSL

Certificat SSL (pour obtenir le HTTPS).



Sélectionnez "Request a new SSL Certificate"

Entrez votre adresse mail

Acceptez les termes de Let's Encrypt

Enregistrer

Cliquez sur "Save"

nginx va automatiquement demander, générer et configurer le certificat HTTPS Let’s Encrypt et par défaut il effectuera une redirection vers le HTTPS

8. Synchronisation du site avec Git (pull + cron)

Configuration de Git

1. **Configurer Git**
   Il est nécessaire définir un nom d'utilisateur et une adresse e-mail pour pouvoir récupérer les le repo du site GSB.
   `git config --global user.name "nom-du-compte" git config --global user.email "adresse@email.com"`

2. **Cloner le dépôt Git**
   Le dépôt Git peut être cloné dans le répertoire `/var/www/gsb` à l'aide de la commande suivante :

   ```
   git clone https://github.com/lugamecooper/gsb.git /var/www/gsb
   ```

3. **Vérifier les permissions**
   Il est important de s'assurer que l'utilisateur qui exécutera les futures commandes `git pull` (notamment via cron) dispose des droits suffisants en lecture/écriture sur le dossier `/var/www/gsb`.

4. **Créer un script de pull `pull.sh`**:

   - Créez un fichier `/var/www/pull.sh` avec le contenu suivant:

   - ```
     git pull origin main
     ```

   - Rendez le script exécutable:

     ```
     chmod +x /var/www/pull.sh
     ```

Configuration de Cron

Cron permet d'automatiser des tâches en définissant un délai, dans notre cas on veut automatiquement pull le repo github du site GSB.

1. **Ajouter une tâche cron** :
   - Éditez la crontab avec `crontab -e` et ajoutez la ligne suivante pour exécuter le script toutes les 3 heures:

     ```
     0 */3 * * * /var/www/pull.sh
     ```
     ```

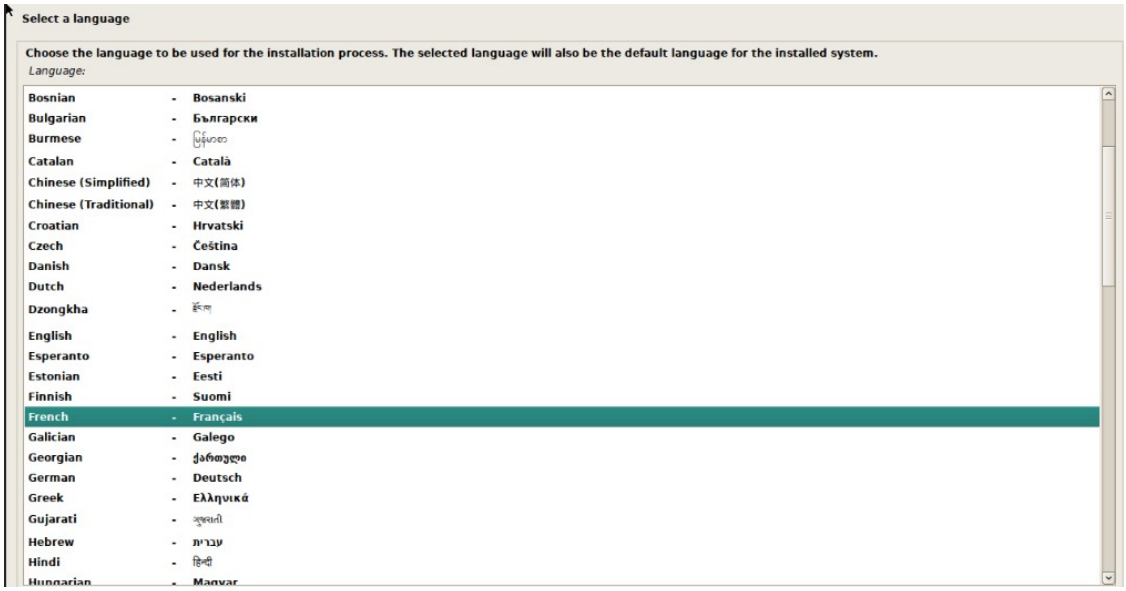
9. Installation et Configuration de Debian 12 serveur gsb-gestion-frais

Création d'une VM Debian 12 serveur gsb-gestion-frais

Installation de debian 12

1. Choix de la langue

- Sélectionner : **Français**



2. Configuration réseau

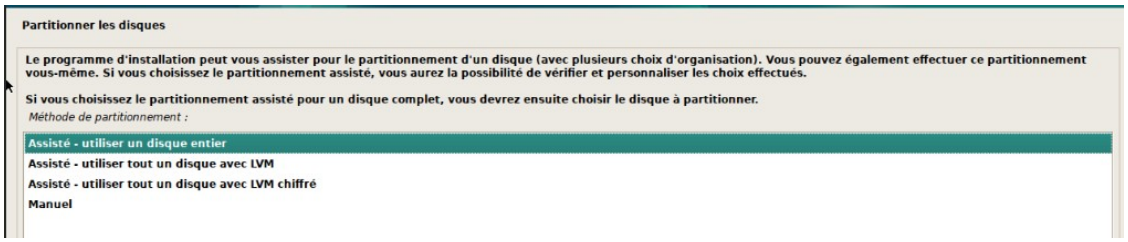
- Mode : **Manuel**
- Adresse IP : `10.0.0.82`
- Masque : `255.255.255.0` (ou `/24`)
- Passerelle : `10.0.0.1`
- DNS : `10.0.0.1`
- Nom d’hôte : `gsb-gestion-frais
- Domaine : laisser vide

3. Configuration des utilisateurs

- Définir un mot de passe root sécurisé.
- Créer un utilisateur normal (ex. : `admin`) avec un mot de passe sécurisé. **il doit être d'au moins 12 charactères, lettre majuscules et minuscule chiffre et charactères spéciaux !** exemple : "EewK!298bzaue.="

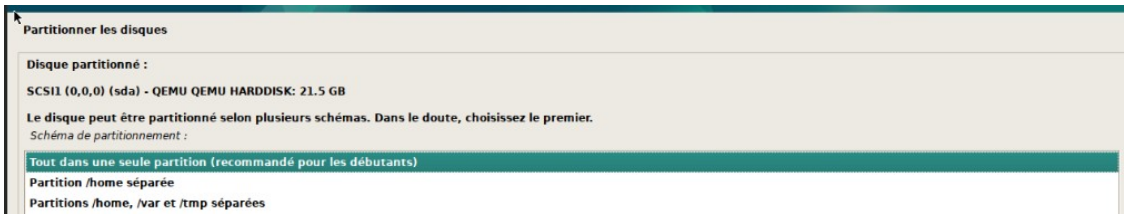
4. Partitionnement des disques

Sélectionner : **Assisté – utiliser un disque entier**



Choisir le disque disponible

Type de partitionnement : **tout sur une seule partition**



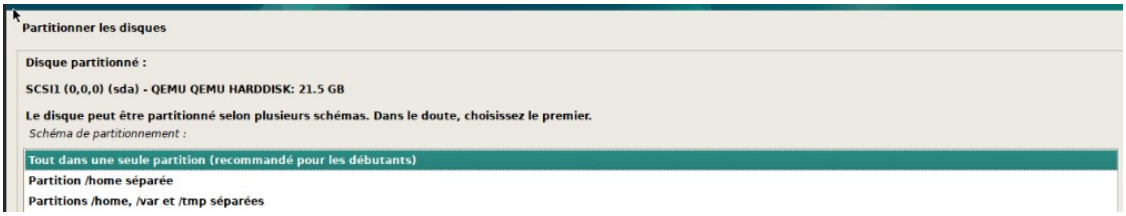
Valider les modifications

5. Sélection des logiciels

Il serait conseillé de ne cocher que :

- ✅ Utilitaires usuels du système et Serveur SSH

Décocher les autres (Environnement de bureau, serveur web, etc.)



6. Finalisation de l'installation

- Laisser l’installation se terminer.
- Une fois terminé, retirer l’ISO dans l’onglet "Hardware" de Proxmox si ce n’est pas automatique.
- Redémarrer la VM.

Configuration Initiale

1. **Mettre à jour les paquets** :

   ```
   sudo apt update && sudo apt full-upgrade -y
   ```

Créer compte administrateur de secours :

sudo adduser administrateur
sudo usermod -aG sudo administrateur
groups administrateur

10. Installation et Configuration de MySQL, Apache2

Installation des services

9. **Installer Apache2** :

```
sudo apt install apache2 -y
```

10. **Installer MySQL** :

```
sudo apt install mysql-server -y
```

Configuration de Apache2

11. **Créer le dossier pour le site** :

```
sudo mkdir /var/www/gsb
```

12. **Créer un fichier de configuration pour le site** :

```
sudo nano /etc/apache2/sites-available/gsb.conf
```

Contenu du fichier :

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName gsb.lucas-lestiennes.fr
    DocumentRoot /var/www/gsb
    <Directory /var/www/gsb>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
    ErrorLog ${APACHE_LOG_DIR}/gsb_error.log
    CustomLog ${APACHE_LOG_DIR}/gsb_access.log combined
</VirtualHost>
```

13. **Activer le site** :

```
sudo a2ensite gsb.conf
sudo systemctl reload apache2
```

11: Installation et Configuration de Maltrail (IDS)

Installation

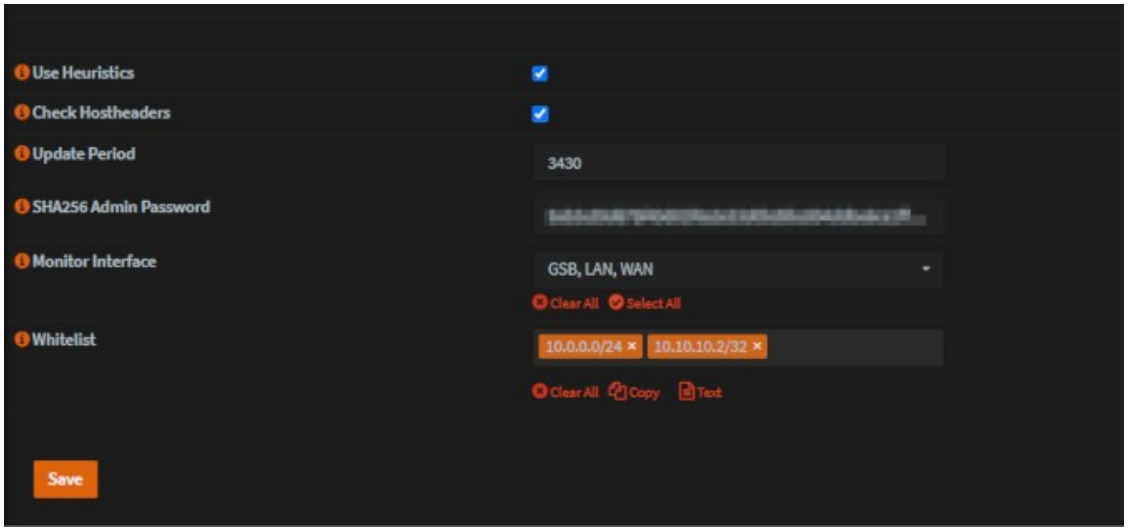
Dans le menu de opnsense, se rendre dans **System > Firmware > Plugins**.

Recherchez `os-maltrail` dans la liste des plugins disponibles.

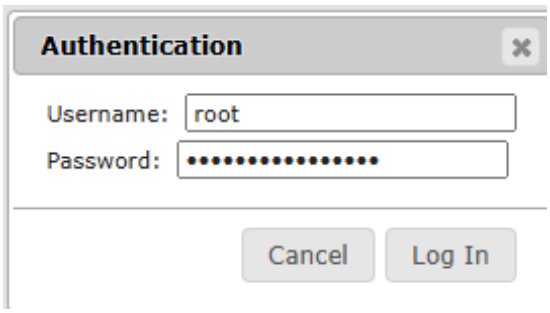
Cliquez sur le bouton + pour installer le plugin.

Une fois l'installation terminée, le plugin sera disponible dans le menu sous **Services > Maltrail**.

1. Changement du mot de passe par défaut & connexion à l'interface web
   Se rendre dans les paramètres de maltrail et changer le hash du mot de passe par défaut le hash correspond à "**changeme**"
   Il faut donc fournir un hash sha256 de mot de passe que l'on souhaite



Pour se connecter il suffit de se rendre à l'adresse IP du opnsense avec le bon port et un accès a l'interface avec les évènements récent apparaît l'utilisateur est "**admin”**



Une fois connectée nous avons un accès à l'interface et pouvons voir les alertes ainsi que d'autres informations sur ces dernières.