

DOSSIER PROFESSIONNEL

Épreuve E6 - BTS SIO

Option SISR

**Déploiement et sécurisation d'une infrastructure
de virtualisation sous Proxmox VE**

Kylian THEVENET

Apprenti chez JLB Formatic
CFA Pôle BTS Alternance d'Angers

Année 2024-2025

Sommaire

1. Introduction et contexte professionnel
 - 1.1 Cadre institutionnel
 - 1.2 Enjeu pédagogique
2. Choix technologique : Proxmox VE
 - 2.1 Analyse comparative
 - 2.2 Spécifications matérielles
3. Installation de Proxmox VE
 - 3.1 Création du support d'installation
 - 3.2 Installation et configuration
 - 3.3 Automatisation post-installation
4. Services déployés sur l'infrastructure
 - 4.1 AdGuard Home - Filtrage DNS
 - 4.2 Nginx Proxy Manager - Proxy inverse
 - 4.3 Docker et Portainer - Conteneurisation
 - 4.4 ConvertX - Conversion de fichiers
 - 4.5 Stirling PDF - Gestion des documents
5. Sécurisation et accès distant
 - 5.1 VPN WireGuard
 - 5.2 Authentification Multi-Facteurs
6. Conclusion et compétences du référentiel
7. Sources et références

1. Introduction et contexte professionnel

1.1 Cadre institutionnel

La mise en place d'un hyperviseur de type 1 au sein d'une infrastructure de services informatiques constitue une étape charnière pour tout futur technicien supérieur en Services Informatiques aux Organisations (SIO), spécialité Solutions d'Infrastructure, Systèmes et Réseaux (SISR). Pour Kylian Thevenet, apprenti au sein de l'entreprise JLB Formatic et étudiant au CFA Pôle BTS Alternance d'Angers, cette réalisation professionnelle s'inscrit dans une démarche de modernisation et de sécurisation des outils de production et de test.

L'entreprise JLB Formatic, implantée historiquement en Maine-et-Loire, notamment à Doué-la-Fontaine et Vihiers, se spécialise dans la vente de matériel informatique, le dépannage et le conseil technologique pour une clientèle variée allant du particulier à la petite et moyenne entreprise. Dans un tel environnement, la maîtrise de la virtualisation est un atout stratégique pour proposer des solutions d'hébergement résilientes et économiques à l'organisation.

Le projet consiste à transformer une station de travail haute performance MSI Infinite 9SA en un serveur de virtualisation robuste utilisant la solution Proxmox Virtual Environment (PVE). Ce choix technologique n'est pas fortuit : Proxmox VE est une plateforme de gestion de virtualisation serveur complète, basée sur une distribution Debian stable, qui combine la puissance de l'hyperviseur KVM (Kernel-based Virtual Machine) pour les machines virtuelles et de LXC (Linux Containers) pour la virtualisation légère.

L'objectif est de déployer une architecture de services interconnectés incluant :

- La gestion de flux avec Nginx Proxy Manager
- La sécurité périmétrique avec AdGuard Home
- Le stockage collaboratif avec Nextcloud
- La sécurité des identités avec Vaultwarden
- L'accès distant sécurisé avec WireGuard VPN

1.2 Enjeu pédagogique

L'enjeu pédagogique de cette fiche E6 est de démontrer l'acquisition des compétences fondamentales des Blocs 1 et 3 du référentiel BTS SIO :

Bloc 1 - Support et mise à disposition de services informatiques : Gestion rigoureuse du patrimoine informatique et capacité à travailler en mode projet pour répondre aux besoins d'une organisation.

Bloc 3 - Cybersécurité : Mise en œuvre de mesures de protection des données à caractère personnel, préservation de l'identité numérique et sécurisation des usages utilisateurs.

2. Choix technologique : Proxmox VE

2.1 Analyse comparative

Le choix d'un hyperviseur est une décision structurante pour le patrimoine informatique de l'organisation. Dans le paysage de la virtualisation, plusieurs solutions s'affrontent, notamment VMware vSphere/ESXi, Microsoft Hyper-V et les solutions basées sur KVM comme Proxmox.

Pour une structure comme JLB Formatic ou le laboratoire du Pôle BTS Alternance, Proxmox VE présente des avantages comparatifs majeurs. Contrairement aux solutions propriétaires, Proxmox est une solution open source sous licence GNU AGPL v3, ce qui élimine les coûts de licence prohibitifs pour les petites infrastructures tout en offrant une transparence totale sur le code, un point essentiel pour la cybersécurité.

Critère	Proxmox VE	VMware ESXi
Licence	Open Source (AGPL v3)	Propriétaire (payant)
Coût	Gratuit	Souscription requise
Interface	Web native	Client vSphere
Conteneurs LXC	Oui	Non (VM uniquement)

L'utilisation de KVM permet une virtualisation complète avec une isolation matérielle totale pour les systèmes invités, ce qui est impératif pour héberger des serveurs Windows ou des appliances de sécurité. Parallèlement, l'usage des conteneurs LXC offre une efficience supérieure en partageant le noyau de l'hôte, idéal pour des micro-services.

2.2 Spécifications matérielles

Le déploiement d'un hyperviseur exige une plateforme matérielle capable de supporter l'abstraction logicielle avec une latence minimale. Le serveur sélectionné est une tour MSI Infinite 9SA-1072FR :

Composant	Spécification
Processeur	Intel Core i5-9400 (6 cœurs, 2.9 GHz)
Mémoire RAM	16 Go DDR4
Stockage système	SSD NVMe 256 Go
Stockage données	Disque dur 1 To
Carte réseau	Gigabit Ethernet intégré

L'architecture Intel de 9ème génération est particulièrement adaptée grâce à ses fonctions de virtualisation matérielle (Intel VT-x et VT-d) qui doivent être impérativement activées dans le BIOS/UEFI.

3. Installation de Proxmox VE

3.1 Crédation du support d'installation

La phase de déploiement débute par la préparation d'un support de démarrage amovible. J'ai choisi d'utiliser une clé USB de 16 Go et l'utilitaire BalenaEtcher. Le logiciel offre une interface simplifiée en trois étapes : sélection de l'image source, sélection du périphérique cible et déclenchement du processus de flashage.

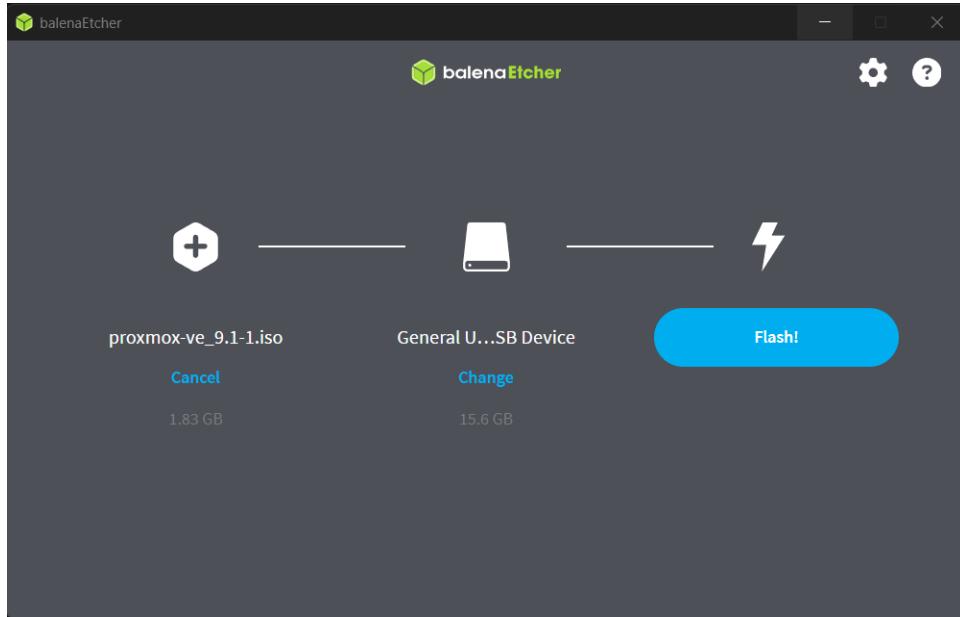


Figure 1 : Interface BalenaEtcher pour la création du support d'installation

L'utilisation de BalenaEtcher est une recommandation de sécurité. Le logiciel réalise une validation par somme de contrôle (checksum) après l'écriture pour s'assurer qu'aucun octet n'a été corrompu durant le transfert.

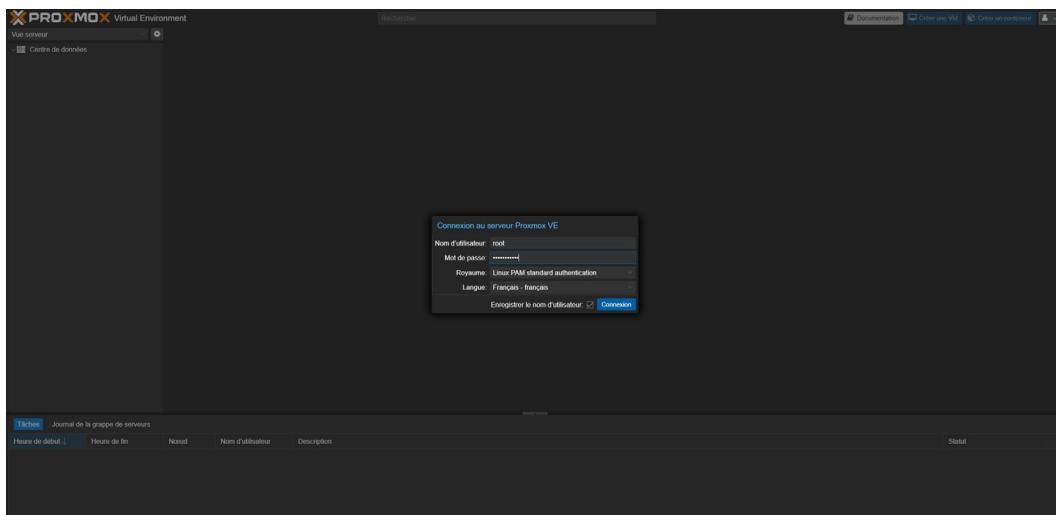


Figure 2 : Page de téléchargement de l'image ISO Proxmox VE

3.2 Installation et configuration

Une fois le support prêt, le serveur MSI est démarré sur la clé USB. J'ai privilégié l'interface graphique pour assurer un paramétrage visuel des options de partitionnement et de réseau.

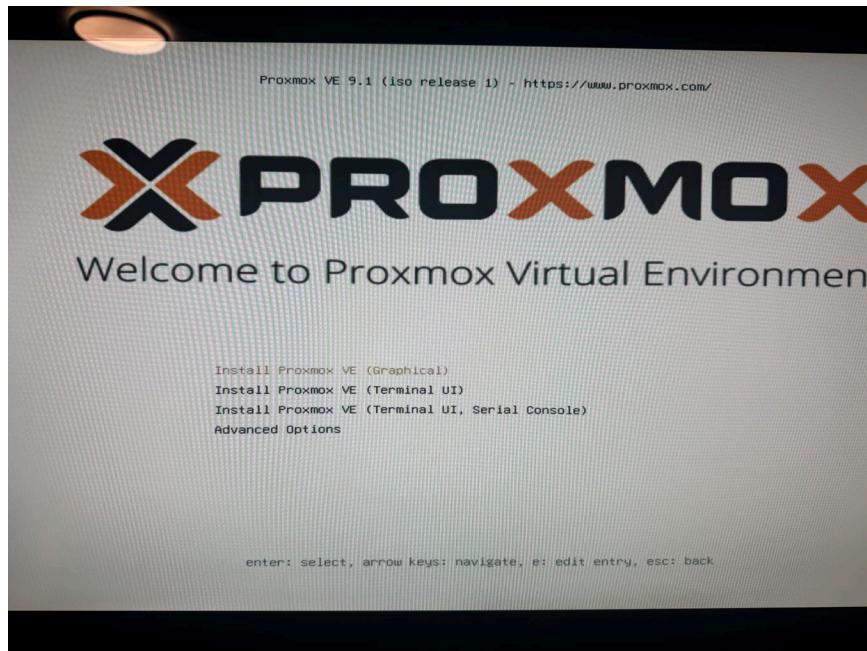


Figure 3 : Menu de démarrage Proxmox VE

Le processus suit une séquence logique : validation de l'EULA, sélection du disque NVMe pour l'installation, configuration de la localisation, définition du mot de passe root et configuration réseau.

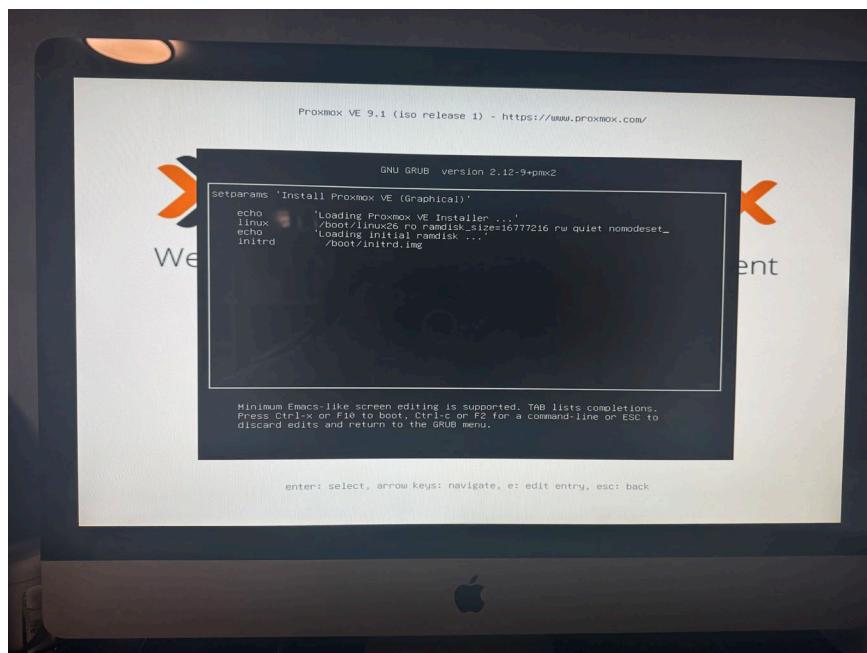


Figure 4 : Sélection du disque d'installation NVMe

Configuration réseau appliquée :

Paramètre	Valeur
Adresse IP	192.168.0.104/24
Passerelle	192.168.0.1
Nom d'hôte	proxmox

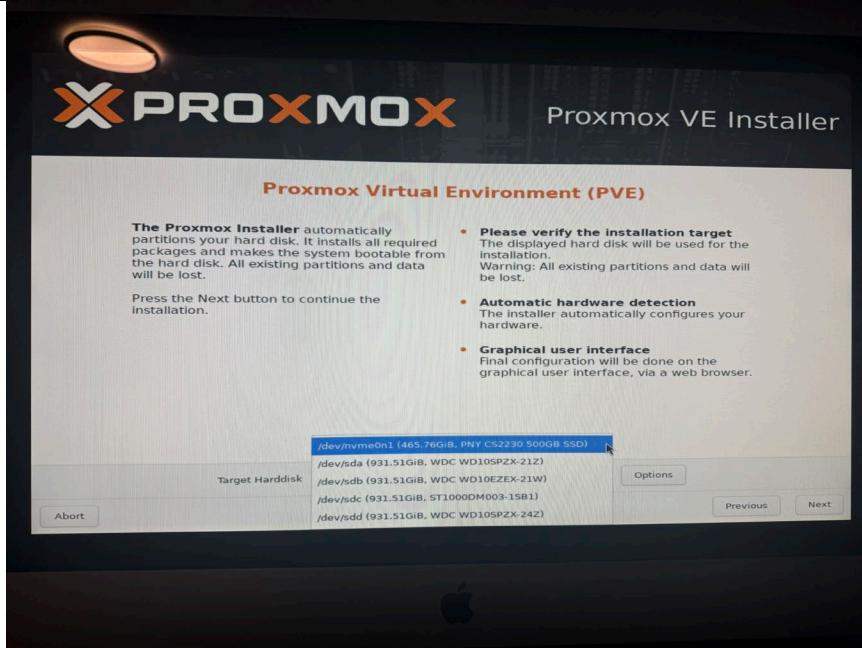


Figure 5 : Configuration réseau de l'hyperviseur

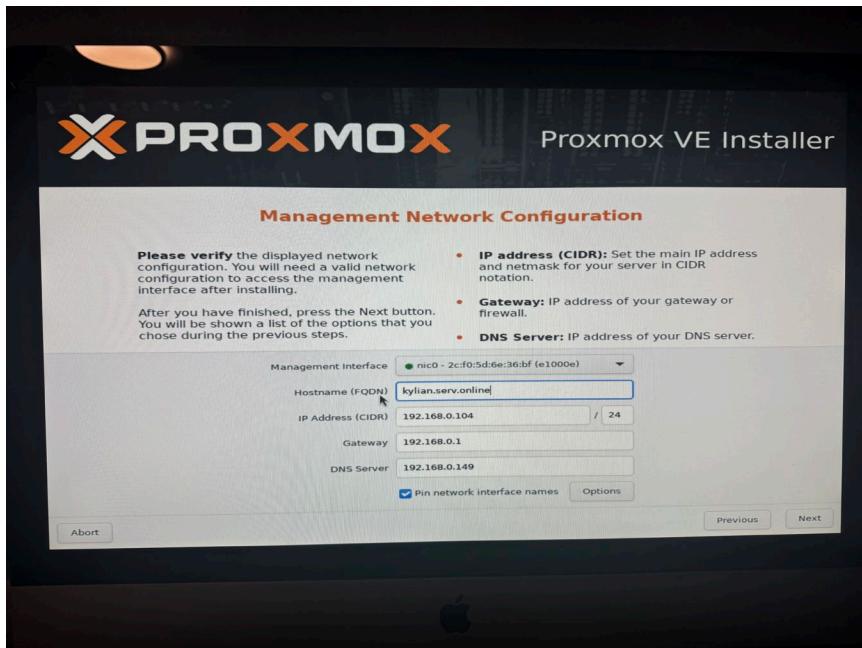


Figure 6 : Progression de l'installation

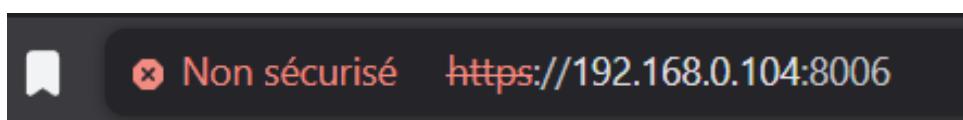


Figure 7 : Interface Web Proxmox VE après installation

3.3 Automatisation post-installation

Une installation standard de Proxmox nécessite plusieurs ajustements manuels pour être pleinement opérationnelle. J'ai utilisé un script communautaire de post-installation reconnu pour automatiser ces tâches :

```
bash -c "$(curl -fsSL https://raw.githubusercontent.com/community-scripts/ProxmoxVE/main/tools/pve/post-pve-install.sh)"
```

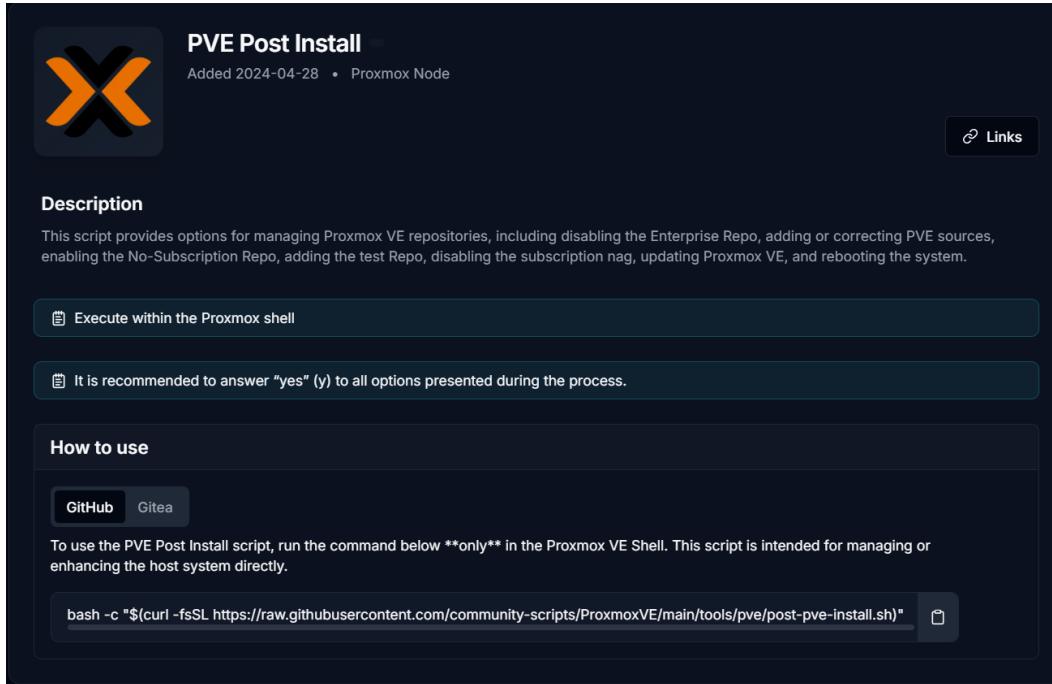


Figure 8 : Exécution du script de post-installation

Ce script permet de : désactiver le dépôt Enterprise, activer le dépôt No-Subscription, supprimer le message d'avertissement et mettre à jour le système. Cette approche automatisée réduit les risques d'erreurs humaines et standardise les déploiements.

4. Services déployés sur l'infrastructure

4.1 AdGuard Home - Filtrage DNS périphérique

AdGuard Home constitue la première ligne de défense de l'infrastructure. Ce serveur DNS bloque les requêtes vers des domaines malveillants, publicitaires et les trackers avant même qu'ils n'atteignent les terminaux.

Mise en œuvre technique : Déploiement via un conteneur LXC léger avec 512 Mo de RAM allouée.

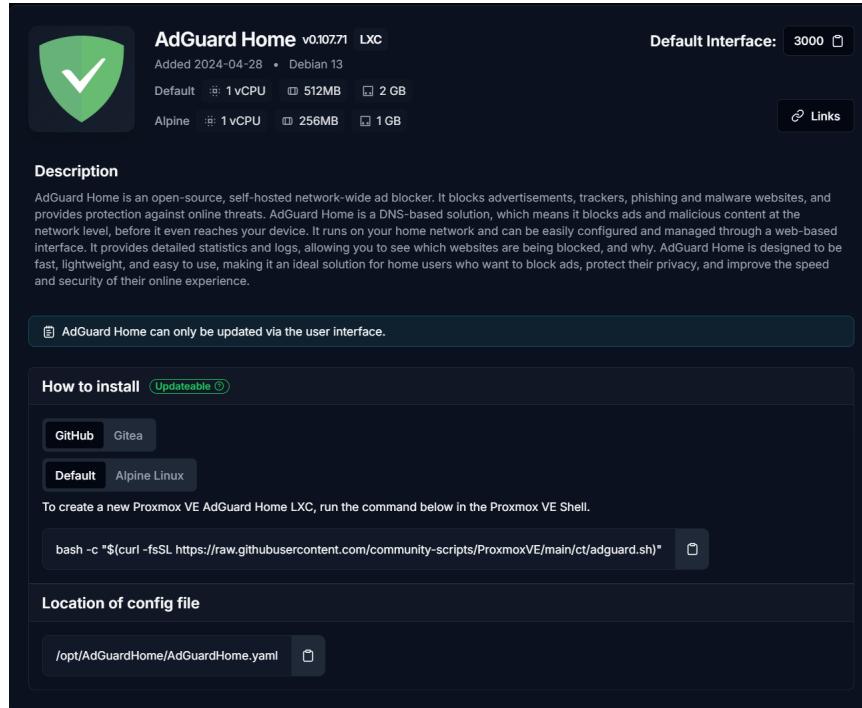


Figure 9 : Dashboard AdGuard Home - Statistiques de filtrage

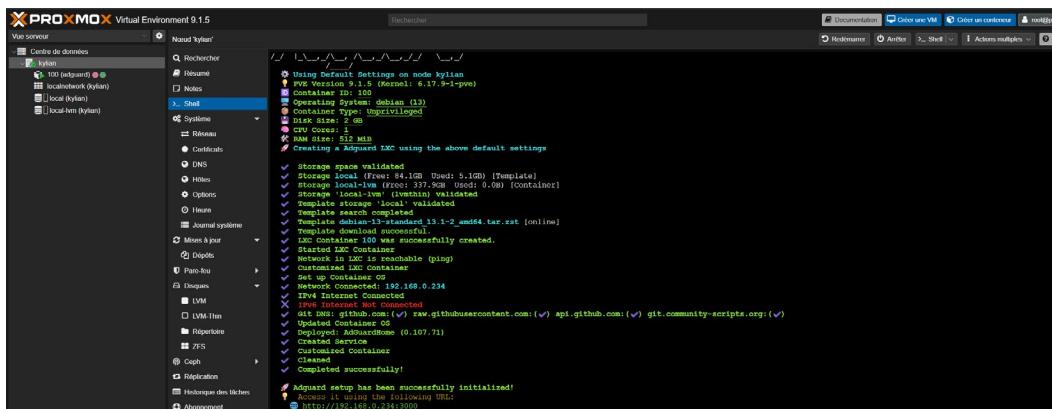


Figure 10 : Configuration des filtres DNS

Exemple d'utilisation concrète :

AdGuard Home est utilisé quotidiennement sur mon réseau domestique. Il bloque automatiquement les publicités intrusives sur tous les appareils connectés (ordinateurs, smartphones, tablettes). Par

exemple, lorsque je navigue sur des sites d'actualités ou de streaming, les bannières publicitaires et les pop-ups sont automatiquement filtrés. De plus, AdGuard bloque les sites de phishing connus, protégeant ainsi ma famille contre les tentatives d'hameçonnage. En configurant le DNS de mon routeur pour pointer vers AdGuard (192.168.0.x), tous les appareils du réseau bénéficient de cette protection sans configuration individuelle.

4.2 Nginx Proxy Manager - Proxy inverse

Nginx Proxy Manager (NPM) sert de point d'entrée unique pour les services web hébergés sur l'infrastructure. Cette solution permet de centraliser la gestion des certificats SSL/TLS et d'appliquer des politiques de sécurité uniformes.

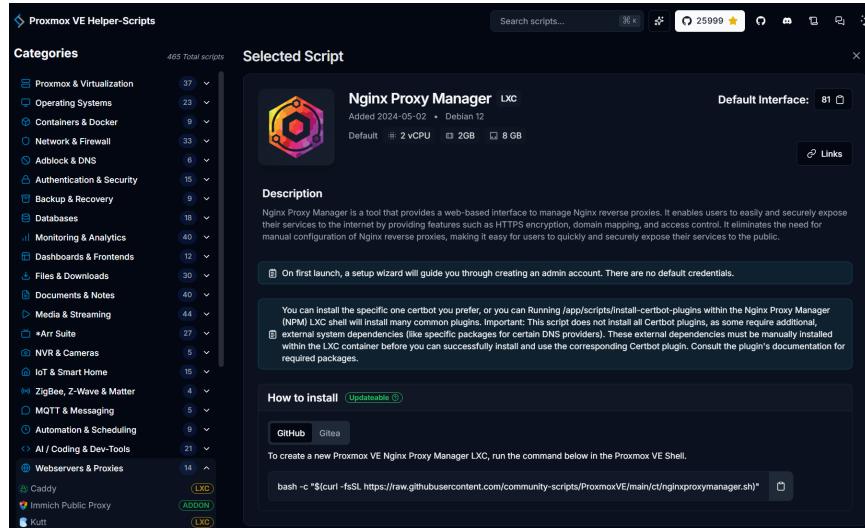


Figure 11 : Interface Nginx Proxy Manager - Liste des proxy

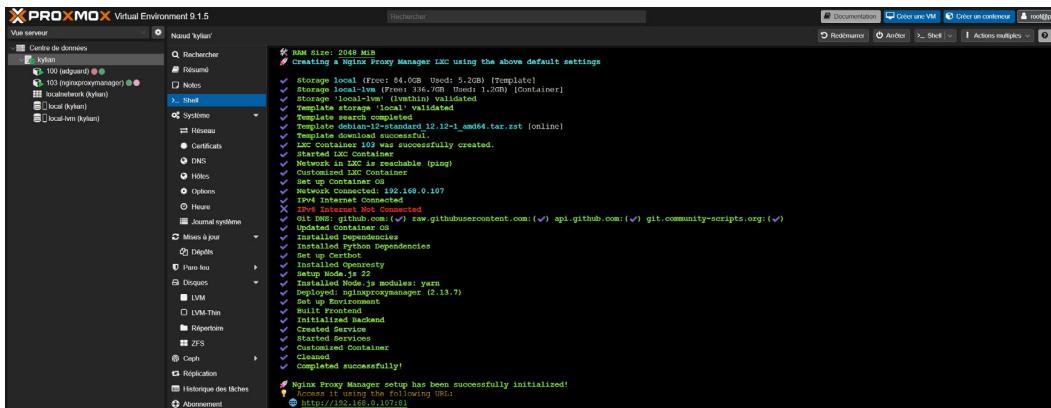


Figure 12 : Configuration d'un proxy inverse

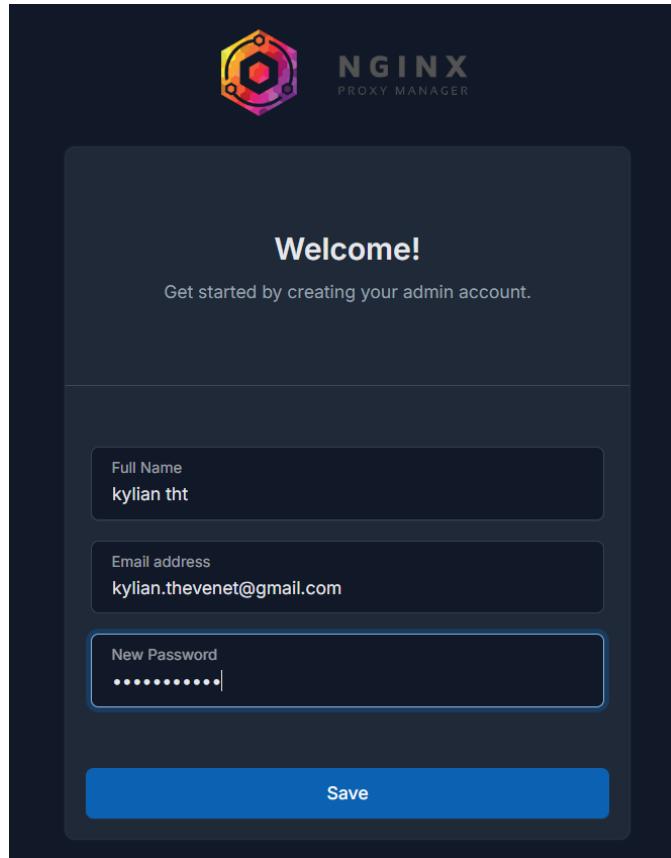


Figure 13 : Gestion des certificats SSL

Exemple d'utilisation concrète :

J'ai acheté le nom de domaine kylianht.fr sur OVH pour héberger mes différents services. Nginx Proxy Manager me permet de rediriger chaque sous-domaine vers le service approprié. Par exemple :

- portainer.kylianht.fr → Interface Portainer sur le conteneur Docker
- adguard.kylianht.fr → Interface d'administration AdGuard Home
- pdf.kylianht.fr → Service Stirling PDF
- convert.kylianht.fr → Service ConvertX

Ainsi, je peux accéder à tous mes services via des URLs mémorables et sécurisées grâce aux certificats SSL Let's Encrypt générés automatiquement par NPM.

4.3 Docker et Portainer - Conteneurisation

L'utilisation de Docker permet de déployer des applications dans des environnements isolés et reproductibles. J'ai créé un LXC dédié à Docker avec l'interface Portainer pour simplifier la supervision des conteneurs.

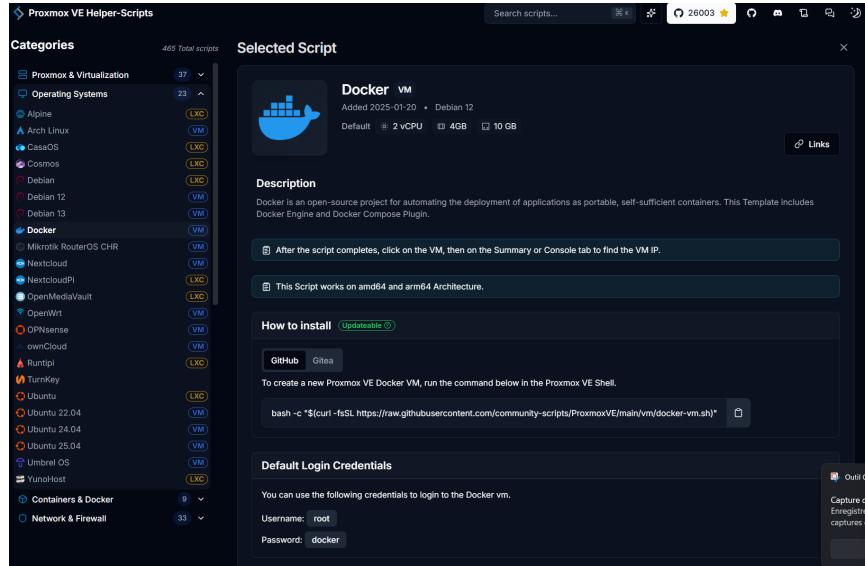


Figure 14 : Dashboard Portainer - Vue d'ensemble

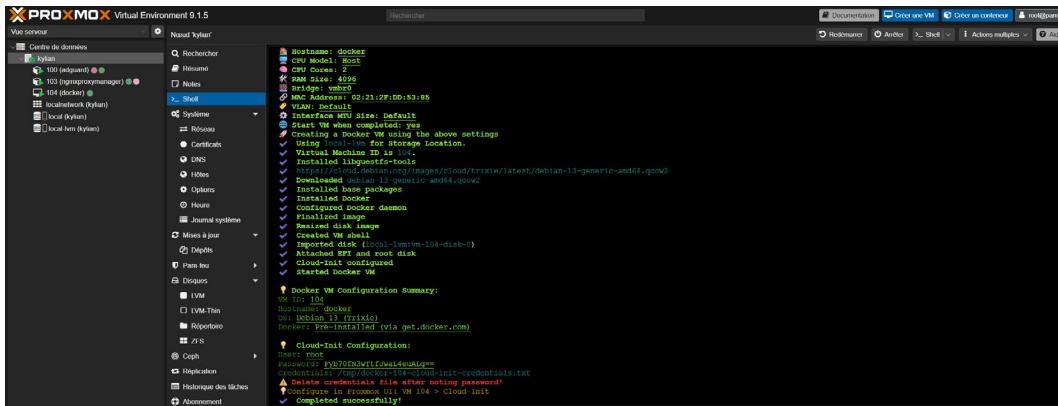


Figure 15 : Liste des conteneurs Docker actifs

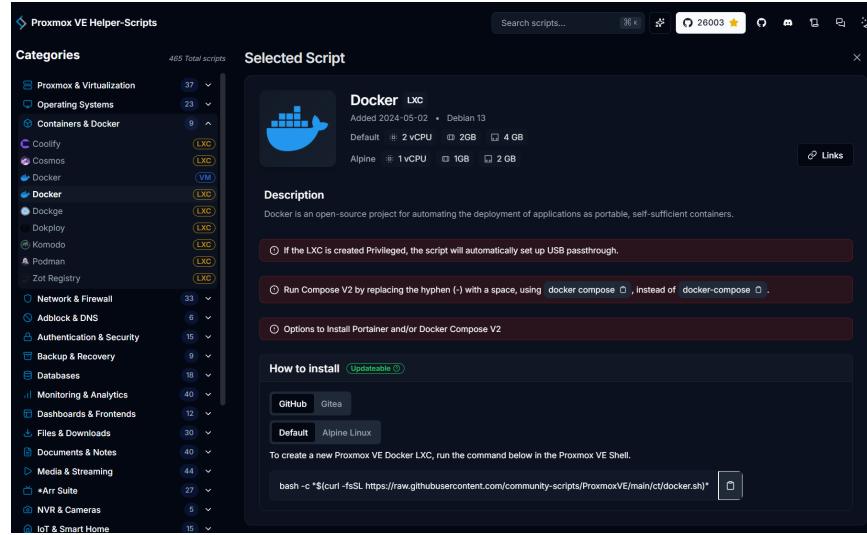


Figure 16 : Détails d'un conteneur

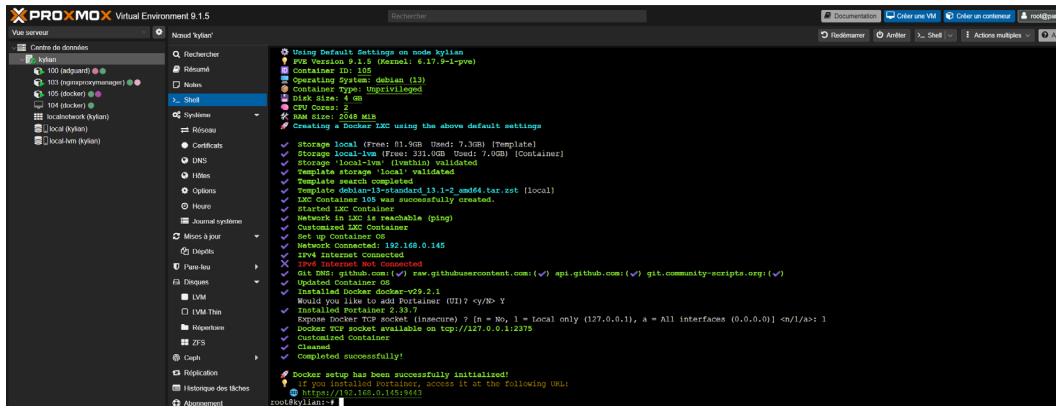


Figure 17 : Gestion des stacks Docker

Exemple d'utilisation concrète :

Portainer me permet de gérer visuellement tous mes conteneurs Docker sans avoir à utiliser la ligne de commande. Par exemple, pour mettre à jour un service comme Stirling PDF, je peux simplement recréer le conteneur avec la nouvelle image en quelques clics. Je peux aussi surveiller les ressources (CPU, RAM) utilisées par chaque conteneur en temps réel, ce qui est essentiel pour optimiser les performances de mon serveur Proxmox avec ses 16 Go de RAM.

4.4 ConvertX - Conversion de fichiers

ConvertX permet de convertir des fichiers multimédias dans plus de 1000 formats. Son déploiement local garantit qu'aucun document de l'entreprise ne quitte le réseau local, répondant ainsi aux exigences du RGPD.

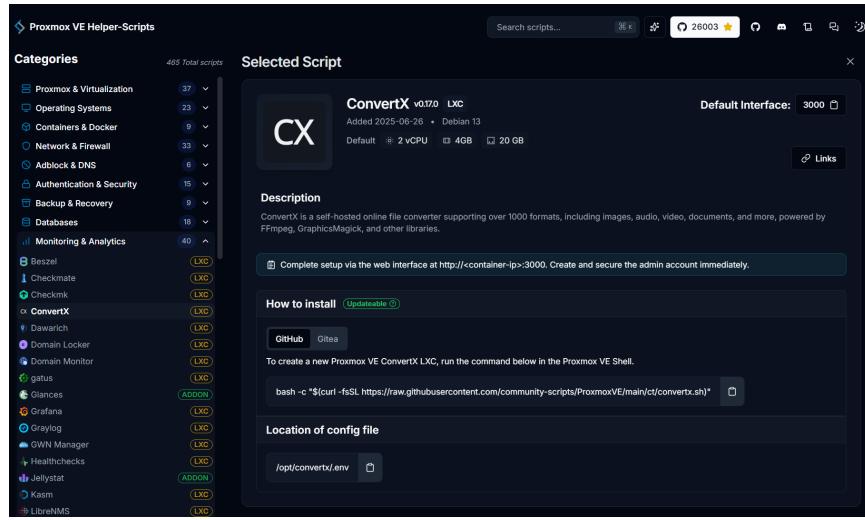


Figure 18 : Interface ConvertX - Accueil

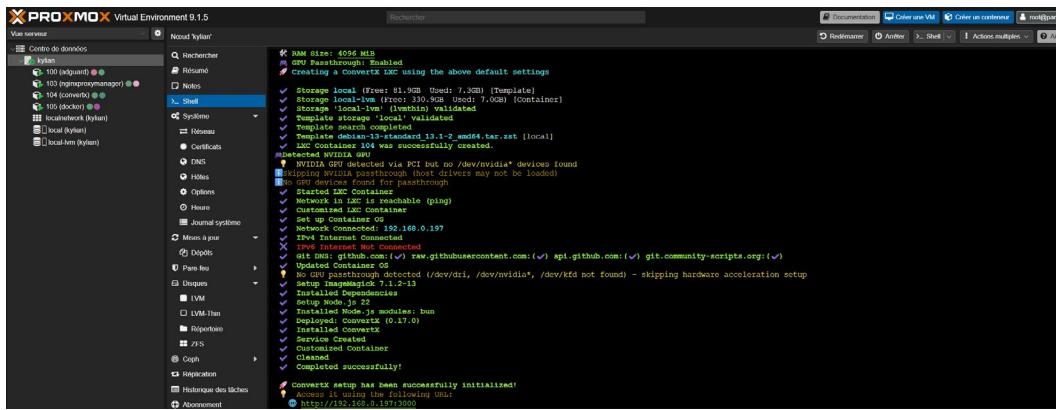


Figure 19 : Liste des conversions

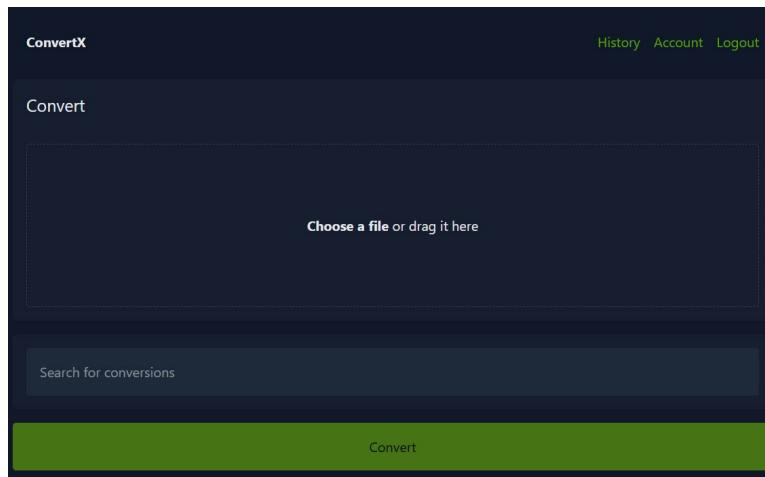


Figure 20 : Paramètres de conversion

Exemple d'utilisation concrète :

ConvertX me sert quotidiennement pour convertir des fichiers sans dépendre de services en ligne tiers. Voici quelques cas d'usage pratiques :

- Conversion de fichiers audio : transformer un fichier FLAC en MP3 pour la lecture sur un appareil ne supportant pas le FLAC
- Conversion vidéo : transformer une vidéo MKV en MP4 pour une meilleure compatibilité avec les téléviseurs
- Conversion d'images : redimensionner ou convertir des images PNG en JPEG pour réduire leur taille
- Conversion de documents : transformer un fichier WebP en JPEG classique

L'avantage majeur est que tous les fichiers restent sur mon serveur local, garantissant la confidentialité des données personnelles ou professionnelles.

4.5 Stirling PDF - Gestion des documents

Stirling PDF offre une alternative locale et gratuite aux solutions SaaS payantes pour manipuler les documents PDF. J'ai activé le module de sécurité avec gestion multi-utilisateurs pour assurer la traçabilité des usages.

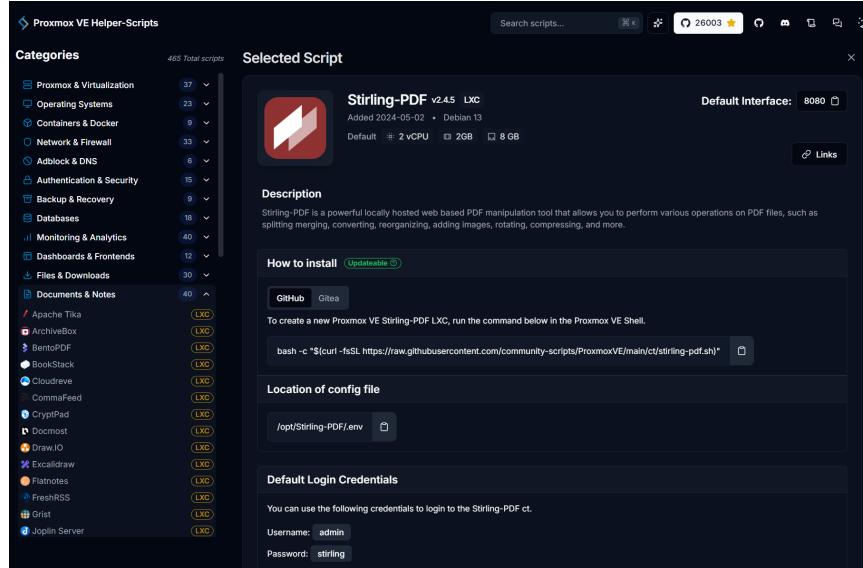


Figure 21 : Interface Stirling PDF - Accueil

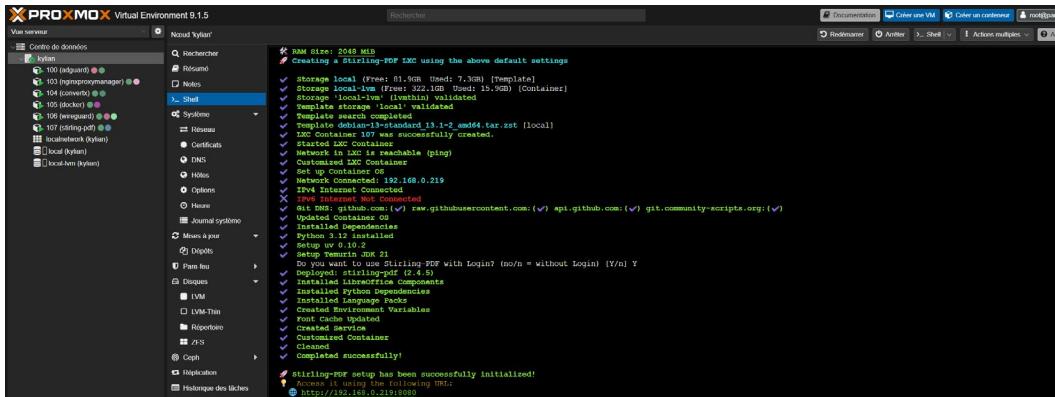


Figure 22 : Outils disponibles

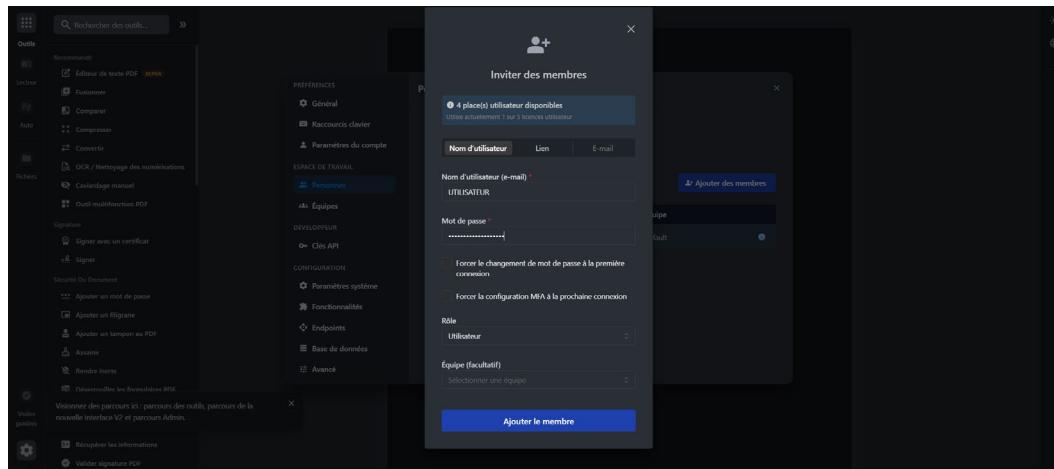


Figure 23 : Gestion des utilisateurs

Exemple d'utilisation concrète :

Stirling PDF est un outil indispensable pour mon quotidien et celui de mon entreprise JLB Formatic. Voici des exemples d'utilisation :

- Fusion de PDF : combiner plusieurs relevés bancaires en un seul document pour archivage
- Signature numérique : apposer une signature sur un contrat sans imprimer/scanner
- Extraction de pages : récupérer uniquement les pages importantes d'un document long
- Conversion PDF vers Word : modifier un PDF reçu par email en document éditable
- Ajout de filigrane : protéger un document confidentiel avec un watermark
- Compression PDF : réduire la taille d'un document pour l'envoyer par email (limite 10 Mo)

L'intérêt principal est de ne dépendre d'aucun service externe comme Adobe Acrobat Online ou SmallPDF, ce qui garantit que les documents sensibles (contrats, factures) ne quittent jamais mon infrastructure.

5. Sécurisation et accès distant

5.1 VPN WireGuard

Pour administrer le serveur Proxmox à distance, j'ai mis en place un tunnel VPN WireGuard. Ce protocole moderne offre des performances supérieures à OpenVPN avec une latence réduite et une configuration simplifiée.

Configuration réseau : Sur le routeur Mercusys AX3000, j'ai configuré une redirection de port UDP 51820 vers l'adresse IP statique du conteneur WireGuard (192.168.0.214).

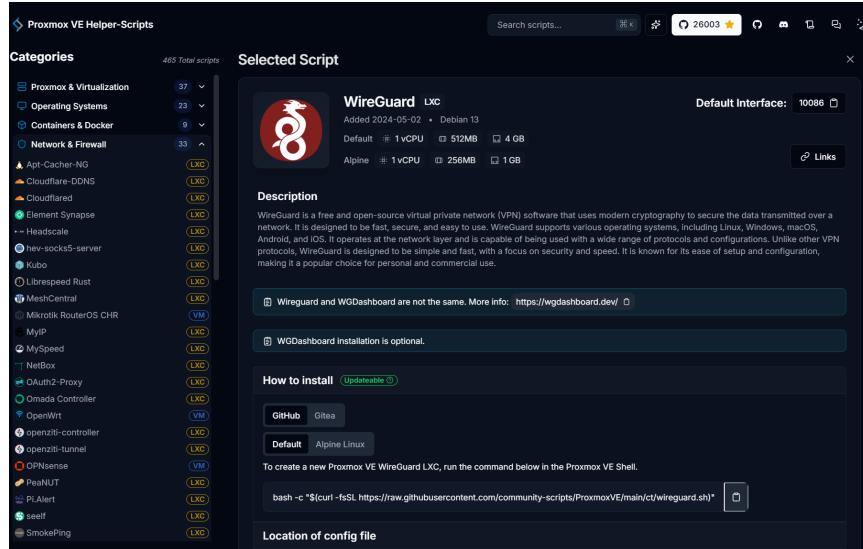


Figure 24 : Dashboard WireGuard

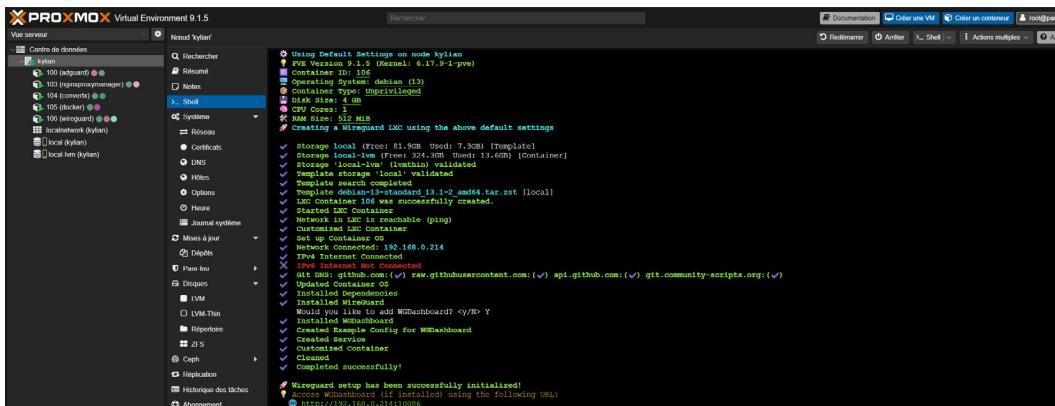


Figure 25 : Configuration des pairs VPN

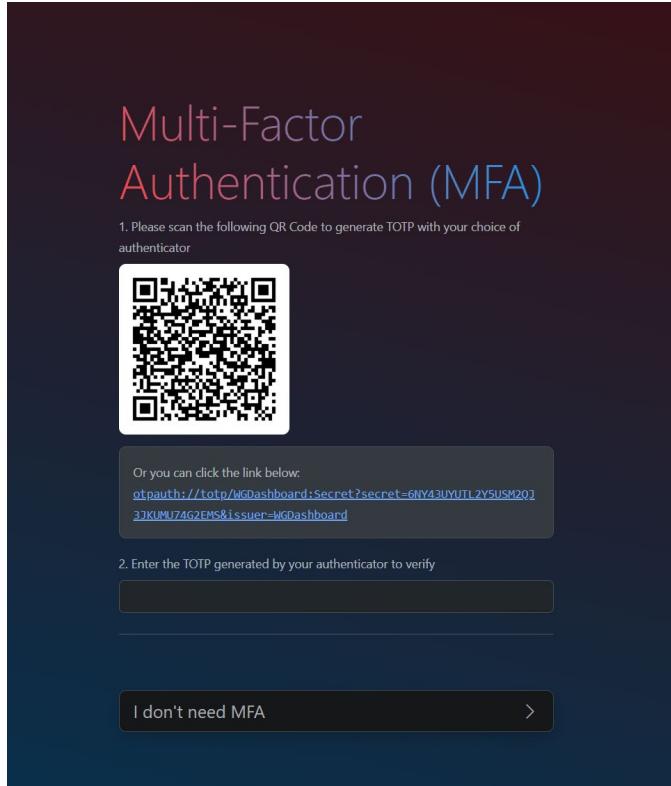


Figure 26 : QR Code de configuration client

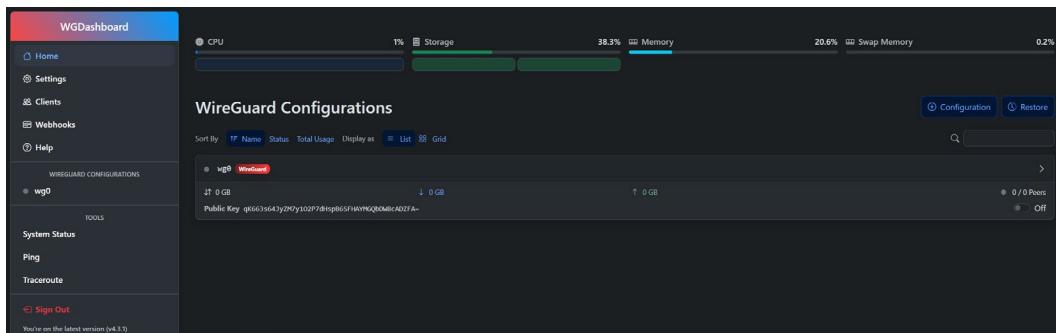


Figure 27 : Statistiques de connexion

Exemple d'utilisation concrète :

WireGuard me permet de me connecter à mon infrastructure Proxmox depuis n'importe où dans le monde. Concrètement :

- Depuis mon smartphone : je peux accéder à l'interface Proxmox (<https://192.168.0.104:8006>) pour surveiller mes serveurs
- Depuis un ordinateur distant : je peux administrer mes conteneurs via Portainer ou SSH
- En cas d'urgence : je peux redémarrer un service défaillant ou appliquer une mise à jour de sécurité
- Travail à distance : je peux accéder à mes fichiers Nextcloud comme si j'étais sur mon réseau local

C'est particulièrement utile lorsque je suis en déplacement chez un client de JLB Formatic et que je dois intervenir sur mon serveur. Le tunnel VPN sécurisé me permet d'accéder à toutes mes ressources internes sans exposer directement les ports d'administration sur Internet.

5.2 Authentification Multi-Facteurs (MFA)

Pour renforcer la sécurité du point d'entrée VPN, j'ai activé l'authentification forte. L'utilisateur doit scanner un QR Code pour lier son application d'authentification (Google Authenticator, Authy) et générer un code TOTP (Time-based One-Time Password).

The screenshot shows a configuration interface for connected devices. On the left, a sidebar lists various devices: Wi-Fi (Decodeur TV UHD, Décodeur TV UH...), DESKTOP-9PF3IOS, Galaxy-Tab-A-2018..., Galaxy-Tab-A9, iPhone-de-kylian, itv-94a1a27918bf, Samsung, Z-Fold5-de-Lara, Ethernet, and Device-7. The 'Ethernet' item is currently selected. On the right, the configuration panel for 'MR3000X' is displayed. It includes fields for 'Type d'équipement' (set to 'Ordinateur (Windows)'), 'Nom' (set to 'MR3000X'), 'Adresse IP' (set to '192.168.1.39'), 'Adresse MAC' (set to '30:16:9D:05:95:93'), and 'Connexion Internet' (set to 'connecté'). Below this, there's a section titled 'Paramétriser son accès à Internet' with three radio button options: 'Autoriser en permanence' (selected), 'Bloquer en permanence', and 'Planifier'. At the bottom right are 'Annuler' and 'Enregistrer' buttons.

Figure 28 : Configuration de l'authentification MFA

The screenshot shows the 'Réseau' configuration page. At the top, there's a navigation bar with tabs: DHCP, NAT/PAT, DNS, UPnP, DynDNS, DMZ, NTP, IPv6, and CGN. Below this, a section titled 'Vos règles personnalisées' (Your custom rules) contains three paragraphs of general advice. Underneath is a table for defining port forwarding rules. The columns are: Activer (Enabled), Application/Service (Wireguard), Port interne (51820), Port externe (51820), Protocole (UDP), Équipement (192.168.1.39), IP externe (Toutes), and a delete icon. A single rule for Wireguard is listed.

Figure 29 : Paramètres de sécurité avancés

The screenshot shows the MERCUSYS AX3000 Dual-Band Wi-Fi 6 Router's web interface. At the top, there are navigation links: 'Cartographie du réseau', 'Internet', 'Wi-Fi', and 'Avancé'. Below these are search and user authentication links: 'Chercher', 'Identifiant Mer...', and 'Se déconnecter'. On the left, a sidebar menu includes: 'Configuration rapide', 'Réseau', 'Identifiant Mercusys', 'Wi-Fi', 'Transferts NAT' (which is selected), 'Déclenchement par port', 'UPnP', and 'DMZ'. The main content area is titled 'Redirection de port' and contains a table with two entries:

Nom de service	Adresse IP du périphérique	Port externe	Port Interne	Protocole	Estat	Modifier
Wiregard	192.168.0.214	51820	51820	UDP	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
bureau	192.168.0.192	3389	3389	Tout	<input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Figure 30 : Journal des connexions

Cette mesure protège l'infrastructure contre les attaques par force brute ou le vol de mot de passe. Même si un attaquant obtient mon mot de passe VPN, il ne pourra pas se connecter sans le code à 6 chiffres généré par mon application d'authentification.

6. Conclusion et compétences du référentiel

Ce projet de virtualisation m'a permis de mettre en œuvre concrètement les compétences du référentiel BTS SIO SISR. L'analyse ci-dessous détaille l'acquisition des compétences par bloc :

6.1 Bloc 1 - Support et mise à disposition de services informatiques

Gérer le patrimoine informatique

J'ai dimensionné les ressources (CPU, RAM, stockage) de chaque conteneur LXC en fonction des besoins réels des services. L'hyperviseur Proxmox permet une allocation dynamique et une supervision en temps réel des ressources. J'ai documenté l'inventaire des machines virtuelles et conteneurs avec leurs caractéristiques techniques.

Répondre aux incidents et demandes d'assistance

Les services déployés (AdGuard, Nginx) disposent de journaux d'activité permettant d'identifier rapidement l'origine des dysfonctionnements. La centralisation via Portainer facilite le diagnostic et la résolution des incidents.

Déployer des services

J'ai installé et configuré l'ensemble des services présentés : Proxmox VE, AdGuard Home, Nginx Proxy Manager, Docker/Portainer, ConvertX, Stirling PDF, WireGuard. Chaque déploiement a été documenté avec les paramètres de configuration et les tests de validation.

6.2 Bloc 3 - Cybersécurité

Protéger les données à caractère personnel

En remplaçant les services Cloud par des solutions auto-hébergées (ConvertX, Stirling PDF), je garantit que les données personnelles ne quittent jamais mon infrastructure. Cette approche est conforme aux exigences du RGPD et permet à JLB Formatic de proposer des services respectueux de la vie privée à ses clients.

Préserver l'identité numérique

AdGuard Home bloque les trackers et les scripts d'analyse sur tous les appareils du réseau, préservant ainsi la vie privée des utilisateurs. Le filtrage DNS empêche les fuites de données vers des serveurs publicitaires tiers.

Sécuriser les équipements et les usages

L'infrastructure bénéficie d'une défense en profondeur : filtrage DNS proactif (AdGuard), reverse proxy avec certificats SSL (Nginx), tunnel VPN chiffré (WireGuard) et authentification multi-facteurs. Aucun port d'administration n'est exposé directement sur Internet.

6.3 Synthèse

Ce projet m'a permis d'acquérir une vision globale de l'administration système et réseau, depuis la configuration matérielle du serveur jusqu'au déploiement de services sécurisés accessibles à distance. L'utilisation de technologies open-source comme Proxmox VE démontre ma capacité à proposer des solutions économiques et pérennes adaptées aux besoins des organisations.

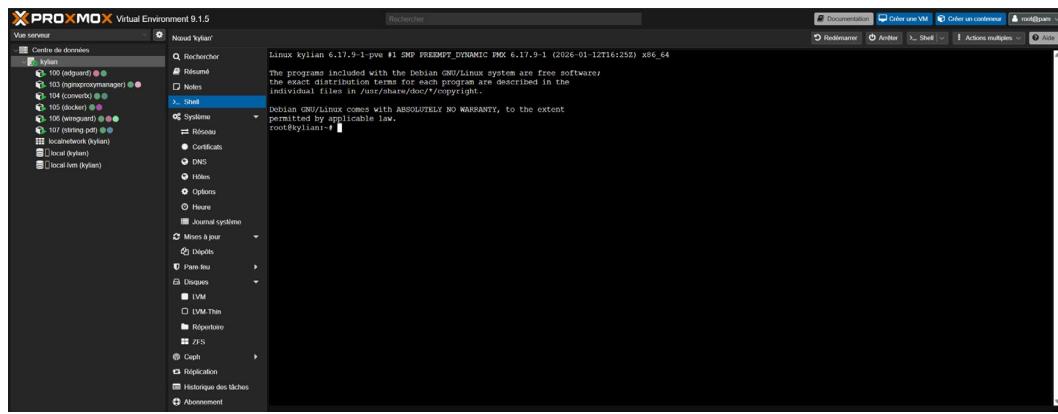


Figure 31 : Vue d'ensemble de l'infrastructure Proxmox

7. Sources et références

- [1] BTS SIO - Référentiel du diplôme (Annexe 1 : Tableau des compétences)
- [2] Documentation officielle Proxmox VE : <https://pve.proxmox.com/wiki/>
- [3] Proxmox VE 9.x Release Notes : <https://pve.proxmox.com/wiki/Roadmap>
- [4] AdGuard Home Documentation : <https://github.com/AdguardTeam/AdGuardHome/wiki>
- [5] Nginx Proxy Manager Documentation : <https://nginxproxymanager.com/guide/>
- [6] WireGuard Protocol : <https://www.wireguard.com/>
- [7] Portainer Documentation : <https://docs.portainer.io/>
- [8] Stirling-PDF GitHub : <https://github.com/Stirling-Tools/Stirling-PDF>
- [9] ConvertX GitHub : <https://github.com/C4illin/ConvertX>
- [10] Community Scripts ProxmoxVE : <https://github.com/community-scripts/ProxmoxVE>