GUIDE D'INSTALLATION

Homelab Proxmox + TrueNAS

Serveur NAS	Serveur Containers
Acer Truenass TrueNAS SCALE 16 Go RAM 2×256 Go + 500 Go SSD	**Dell Latitude** Proxmox VE 8 8 Go RAM 256 Go SSD

Services hébergés : AdGuard Home • Bitwarden • Jellyfin • Kiwix • Anki Sync • WireGuard VPN

Table des matières

1. Vue d'ensemble & architecture

Ce homelab crée un réseau privé isolé au sein du réseau familial existant. L'objectif : avoir une infrastructure personnelle complètement séparée du WiFi principal de la maison, où seul l'administrateur (vous) a accès. Deux machines connectées via un switch managé TP-Link avec segmentation VLAN :

Objectif du projet

Créer un « réseau dans le réseau » : votre homelab fonctionne sur des sous-réseaux dédiés (192.168.10-30.x), complètement isolés du WiFi familial (192.168.1.x).
Accès restreint : personne d'autre sur le réseau de la maison ne peut accéder à vos serveurs ou services.
Infrastructure privée : stockage, services, et administration totalement indépendants.
Accès distant via VPN WireGuard : connexion sécurisée depuis l'extérieur (4G, autre WiFi).

Ce homelab est composé de deux machines :

Rôles des machines

Dell Latitude (Proxmox) : hyperviseur principal. Il héberge les containers (LXC) qui font tourner les services quotidiens : AdGuard Home (DNS filtrant), Bitwarden (gestionnaire de mots de passe) et Jellyfin (serveur média).
Acer (TrueNAS) : serveur de stockage centralisé. Il expose les données via des partages SMB/NFS que Proxmox (et les autres machines du réseau) pourront monter.
Switch TP-Link : coeur du réseau local. Tous les appareils sont reliés par câble RJ45 pour une connexion fiable et rapide.

1.1 Schéma logique du réseau

Appareil	Rôle	IP suggérée
Routeur / FAI	Gateway + DHCP	192.168.1.1
Switch TP-Link	Commutateur réseau	192.168.1.2
Acer – TrueNAS	NAS / Stockage	192.168.10.10 (VLAN 10)
Dell – Proxmox	Hyperviseur + Containers	192.168.20.20 (VLAN 20)
LXC Container	Services	192.168.20.30 (VLAN 20)
PC Perso / Autre	Client réseau	DHCP automatique

⚡ Conseils réseau

Utilisez des IPs fixes pour le NAS, Proxmox et le container principal. Le reste peut rester en DHCP.
Les IPs ci-dessus sont des suggestions. Adaptez-les selon votre réseau existant.
Le sous-réseau 192.168.1.0/24 est utilisé comme exemple. Si votre routeur utilise un autre sous-réseau (ex: 10.0.0.x), ajustez en conséquence.

2. Préparation du matériel

2.1 Ce qu'il vous faut

Matériel	Détails
Dell Latitude	8 Go RAM, 256 Go SSD – sera utilisé pour Proxmox
Acer (avec les SSDs)	16 Go RAM, 2× 256 Go SSD + 1× 500 Go SSD – tous les SSDs restent libres pour le pool de données
2 clés USB 32 Go	Stockage système TrueNAS – TrueNAS sera installé dessus en miroir (RAID 1). Elles restent branchées en permanence sur l'Acer.
Clé USB Ventoy (existante)	Utilisée pour booster les ISO Proxmox et TrueNAS SCALE afin de démarrer les installations
Switch TP-Link TL-SG605E	Easy Smart Switch, 5 ports Gigabit, gérable via interface web
Câbles RJ45	Un par machine connectée au switch
Écran + clavier/souris	Pour l'installation initiale des deux machines
PC avec accès Internet	Pour télécharger les ISO

2.2 Téléchargement des ISO

1. **Proxmox VE :** rendez-vous sur **https://www.proxmox.com/en/downloads** → téléchargez la dernière version de Proxmox VE (ISO).
2. **TrueNAS SCALE :** rendez-vous sur **https://www.truenas.com/truenas-scale/** → téléchargez la dernière version de TrueNAS SCALE (ISO).

2.3 Ajout des ISO à votre clé Ventoy

Vous avez déjà une clé USB Ventoy. Il suffit de copier les ISO dedans :

3. Branchez votre clé Ventoy sur votre PC.
4. Copiez l'ISO Proxmox VE dans le dossier racine de la partition « Ventoy » de la clé.
5. Copiez l'ISO TrueNAS SCALE dans le même dossier.
6. À l'installation, Ventoy vous proposera un menu pour choisir quelle ISO démarrer.

Conseils Ventoy

Ventoy gère automatiquement le multiboot – pas besoin de reflasher la clé à chaque fois.
Assurez-vous que votre clé Ventoy a assez d'espace libre pour les 2 ISO (environ 2-3 Go au total).

3. Configuration du switch TP-Link TL-SG605E

Le TL-SG605E est un « Easy Smart Switch » de 5 ports Gigabit. Il est gérable via une interface web et supporte nativement les VLANs 802.1Q – ce qui sera très utile plus tard pour sécuriser votre réseau (les « zones de couleurs » de votre schéma).

3.1 Connexion physique

- Port 1 du switch → câble vers votre routeur / FAI (uplink vers Internet)
- Port 2 du switch → câble vers l'Acer (TrueNAS)
- Port 3 du switch → câble vers le Dell Latitude (Proxmox)
- Port 4 du switch → câble vers votre PC personnel (si nécessaire)
- Port 5 → libre pour un appareil supplémentaire à l'avenir

3.2 Accès à l'interface web du switch

Le TL-SG605E reçoit automatiquement une IP via DHCP de votre routeur. Pour y accéder :

7. Reliez votre PC au switch avec un câble RJ45.
8. Le switch obtient une IP DHCP de votre routeur. Pour la trouver, vous pouvez regarder dans l'interface de votre routeur (liste des clients DHCP) ou utiliser un outil comme « Advanced IP Scanner » sur votre PC.
9. Ouvrez votre navigateur et tapez cette IP (ex: http://192.168.1.XXX).
10. **Identifiez-vous avec :** admin / admin (identifiants par défaut du TL-SG605E).
11. Vous êtes dans l'interface de gestion du switch !

3.3 Assigner une IP fixe au switch

12. Dans l'interface, allez dans : System → System Information (ou Device Information).
13. Changez le mode IP de « DHCP » à « Static ».
14. Renseignez :

```
IP :           192.168.1.2
Masque :       255.255.255.0
Passerelle :   192.168.1.1  (IP de votre Livebox Orange)
```

15. Cliquez « Apply » puis « Save ».
16. Reconnectez-vous à l'interface via http://192.168.1.2

3.4 Vérifier les ports

17. Dans l'interface, allez dans : Switching → Port → Port Overview (ou Port Status).
18. Vérifiez que tous les ports utilisés sont en « Up » et en « 1000 Mbps » (Gigabit).
19. Si un port montre « 100 Mbps », vérifiez votre câble RJ45 – il faut un câble Cat5e minimum pour du Gigabit.

Conseils TL-SG605E

Le switch est « plug and play » – même sans configuration, il fait passer le trafic correctement.
L'IP fixe et la vérification des ports sont des bonnes pratiques, pas strictement obligatoires pour démarrer.
Ce switch supporte 802.1Q VLAN nativement – nous allons les configurer maintenant pour isoler votre homelab.

3.5 Configuration des VLANs pour isoler votre homelab

Voici la partie clé : créer votre réseau privé isolé du WiFi familial. Vous allez configurer 3 VLANs sur le switch :

VLAN ID	Zone	Sous-réseau
VLAN 10	Bleue – NAS	192.168.10.0/24
VLAN 20	Rose – Services	192.168.20.0/24
VLAN 30	Verte – Admin	192.168.30.0/24

Concept d'isolation

Le WiFi Orange de votre maison reste sur 192.168.1.0/24 (toute la famille y a accès).
Votre homelab fonctionne sur 192.168.10-30.0/24 (vous seul y avez accès).
Les VLANs créent une barrière : personne depuis le WiFi ne peut voir vos serveurs.

3.6 Étapes de configuration VLAN sur le TL-SG605E

1. Dans l'interface du switch (http://192.168.1.2), allez dans : VLAN → 802.1Q VLAN.
2. Activez « 802.1Q VLAN » dans Global Config → Apply.
3. **Créer VLAN 10 (NAS) :** entrez « 10 » dans VLAN ID. Configurez les ports comme suit :

```
Port 2 (Acer/TrueNAS) : Untagged, PVID 10
Port 3 (Dell/Proxmox) : Tagged (il verra tous les VLANs)
```

1. **Créer VLAN 20 (Services) :** entrez « 20 ». Configurez :

```
Port 3 (Dell/Proxmox) : Tagged
Port 4 (votre PC admin si branché) : Untagged, PVID 20
```

1. **Créer VLAN 30 (Admin) :** entrez « 30 ». Configurez :

```
Port 3 (Dell/Proxmox) : Tagged
Port 5 (libre pour admin) : Untagged, PVID 30
```

1. Allez dans VLAN → 802.1Q PVID Setting. Assignez les PVID :

```
Port 1 (Livebox Orange) : PVID 1 (réseau familial)
Port 2 (Acer/TrueNAS) : PVID 10
Port 3 (Dell/Proxmox) : PVID 20
Port 4 (PC admin) : PVID 20 ou 30
```

1. Cliquez Apply puis Save Configuration.

Important

Une fois les VLANs activés, le switch lui-même reste accessible sur 192.168.1.2 (vous pouvez le gérer depuis le WiFi).
Vos machines TrueNAS et Proxmox seront sur leurs VLANs respectifs et ne seront plus accessibles depuis 192.168.1.x.
Assurez-vous de bien noter les IPs que vous allez utiliser dans chaque VLAN !

4. Installation de TrueNAS SCALE (Acer)

Cette section détaille l'installation de TrueNAS SCALE sur l'Acer. TrueNAS va s'installer sur vos 2 clés USB 32 Go en mode miroir (RAID 1) : c'est le disque système. Les 3 SSDs du laptop restent entièrement libres pour le pool de données.

Disposition des disques sur l'Acer

2× clés USB 32 Go → Disque système TrueNAS en miroir (RAID 1). Elles restent branchées en permanence. Si l'une lâche, l'autre prend le relais.
2× SSD 256 Go + 1× SSD 500 Go → Tous libres pour le pool de données (films, sauvegardes, etc.).
La clé USB Ventoy est utilisée uniquement pour le démarrage de l'installation – elle est retirée après.

4.1 Préparation : brancher les clés USB

20. Branchons les 2 clés USB 32 Go sur l'Acer (sur des ports USB différents).
21. Branchons aussi la clé Ventoy.
22. Reliez l'Acer au switch avec un câble RJ45.

4.2 Boot depuis la clé Ventoy

23. Allumez l'Acer et accédez au BIOS/UEFI (en général F2, F12, Esc ou Del pendant le démarrage – regardez l'écran au boot).
24. Dans le BIOS, changez l'ordre de démarrage pour mettre la clé USB Ventoy en première priorité.
25. Sauvegardez et quittez le BIOS (en général F10).
26. Le menu Ventoy apparaît : sélectionnez l'ISO TrueNAS SCALE.
27. L'Acer démarre sur l'installeur TrueNAS.

4.3 Installation de TrueNAS sur les 2 clés USB

28. À l'écran de démarrage TrueNAS, sélectionnez « Install TrueNAS ».
29. **Choisissez la destination :** sélectionnez vos 2 clés USB 32 Go comme destination d'installation.
30. TrueNAS va automatiquement les configurer en miroir (RAID 1) – vous n'avez rien à faire de plus.
31. **Créez un mot de passe root** fort et notez-le soigneusement. C'est le mot de passe de l'interface web.
32. Confirmez l'installation.
33. Quand c'est terminé, choisissez « Boot from disk ».
34. **Retirez la clé Ventoy** avant de redémarrer. Les 2 clés USB 32 Go restent branchées.
35. L'Acer redémarre sur TrueNAS installé.

Attention

Ne retirez JAMAIS les 2 clés USB 32 Go après l'installation – c'est le système d'exploitation de TrueNAS.
Si vous retirez une clé USB, le miroir se dégrade mais TrueNAS continue de fonctionner. Remplacez-la rapidement.
Les 3 SSDs du laptop ne sont PAS touchés pendant l'installation.

4.4 Première connexion à l'interface web

36. Attendez que TrueNAS affiche une adresse IP sur l'écran. Vous devriez voir http://192.168.10.10 (si le VLAN est correctement configuré).
37. Sur votre PC, ouvrez un navigateur et tapez cette adresse IP.
38. **Connectez-vous avec :** username = root, mot de passe = celui que vous avez créé.
39. Vous êtes dans le tableau de bord TrueNAS !

Attention – IP fixe TrueNAS

À ce stade, TrueNAS a probablement une IP DHCP automatique. Vous allez l'y fixer dans la section suivante pour avoir une adresse stable (192.168.10.10 sur VLAN 10).

5. Configuration des pools & datasets TrueNAS

5.1 Assigner une IP fixe à TrueNAS

4. Dans l'interface TrueNAS, allez en haut à gauche dans le menu.
5. Allez dans : Network → Interfaces.
6. Cliquez sur votre interface réseau (en général « em0 » ou « eth0 »).
7. Décochez « DHCP » et entrez manuellement :

```
Adresse IP :   192.168.10.10   (VLAN 10 - Zone NAS)
Masque :       255.255.255.0   (ou /24)
Passerelle :   192.168.10.1    (interface VLAN Proxmox, à créer plus tard)
```

2. Cliquez « Save » puis « Apply ».
3. Reconnectez-vous à l'interface via http://192.168.10.10

5.2 Création du pool de données

Le pool est l'espace de stockage organisé. Vous allez utiliser vos 3 SSDs (2× 256 Go + 1× 500 Go) pour créer un pool. Avec 3 disques, vous avez une option intéressante : RAIDZ1.

Options de pool – Quoi choisir ?

Stripe (JBOD) : vous utilisez les 3 SSDs comme un seul grand disque (256 + 256 + 500 = 1 012 Go totaux). Espace maximum, mais aucune redondance – si un SSD lâche, vous perdez tout.

RAIDZ1 (recommandé) : équivalent à un RAID 5. Vous perdez l'espace d'un disque pour la redondance, soit environ 256 Go perdus. Vous gardez ~756 Go utilisables. Si un SSD lâche, TrueNAS peut se relever automatiquement.

Mirror : non recommandé ici car les disques sont de tailles différentes.

Recommandation : utilisez RAIDZ1 si vous voulez protéger vos données. Utilisez Stripe si vous avez besoin de l'espace maximum et que vous acceptez le risque.

2. Dans l'interface TrueNAS, allez dans Storage → Pools.
3. Cliquez « Create Pool ».
4. Donnez un nom à votre pool (ex: « datapool »).
5. Ajoutez vos 3 SSDs (2× 256 Go + 500 Go) au pool.
6. Choisissez le layout « RAIDZ1 » (ou « Stripe » si vous préférez max d'espace).
7. Confirmez la création.

5.3 Création des datasets

Les datasets sont comme des dossiers de niveau supérieur dans votre pool. Créez-en un pour chaque service :

Dataset	Utilisation
jellyfin	Stockage des films, séries et musique pour Jellyfin
kiwix	Fichiers ZIM pour Kiwix (encyclopédies hors ligne)
bitwarden	Données de Bitwarden (sauvegardées depuis Proxmox)
backups	Dossier de sauvegarde général

2. Dans Storage → Pools → Cliquez sur votre pool « datapool ».

3. Cliquez « Add Dataset ».
4. Nom : jellyfin → Créer.
5. Répétez pour « kiwix », « bitwarden » et « backups ».

5.4 Configuration des partages SMB

SMB permet de rendre ces datasets accessibles depuis votre réseau local (Proxmox, PC, etc.).

2. Allez dans Sharing → SMB.
3. Cliquez « Add ».
4. Sélectionnez le chemin vers votre dataset (ex: /pool/jellyfin).
5. Nom du partage : « jellyfin ».
6. Cliquez « Save ».
7. Répétez pour chaque dataset que vous voulez partager.

Conseils SMB

Créez un utilisateur dédié pour accéder aux partages SMB : allez dans Accounts → Users → Add User.
Assignez cet utilisateur aux datasets via les permissions du partage.
Notez le nom d'utilisateur et le mot de passe – vous en aurez besoin plus tard pour monter les dossiers dans Proxmox.

6. Installation de Proxmox VE (Dell Latitude)

Proxmox sera votre hyperviseur principal sur le Dell Latitude. Il hébergera les containers LXC pour vos services.

6.1 Boot depuis la clé USB

40. Insérez la clé USB contenant l'ISO Proxmox VE dans le Dell Latitude.
41. Allumez le Dell et accédez au BIOS (en général F2 sur un Dell).
42. Changez l'ordre de démarrage : clé USB en premier.
43. Sauvegardez (F10) et redémarrez.

6.2 Installation de Proxmox

44. À l'écran d'installation Proxmox, sélectionnez « Install Proxmox VE ».
45. Acceptez la licence.
46. **Configuration du disque :** Proxmox va s'installer sur votre SSD 256 Go. Laissez les paramètres par défaut.
47. **Configuration réseau :** Assurez-vous que le câble RJ45 est connecté au switch.

Paramètres réseau à renseigner :

```
Interface :     eno1 (ou celle détectée automatiquement)
Nom d'hôte :    proxmox
Domaine :       local
IP :            192.168.20.20  (VLAN 20 - Zone Services)
Masque :        255.255.255.0
Passerelle :    192.168.20.1  (sera configuré dans Section 7)
DNS :           192.168.1.1  (votre routeur)
```

1. Créez un mot de passe root fort.
2. Vérifiez le résumé et confirmez l'installation.
3. Proxmox redémarrera automatiquement. Retirez la clé USB.

6.3 Première connexion à l'interface Proxmox

48. Sur votre PC, ouvrez un navigateur et allez à : https://192.168.20.20:8006
49. **Identifiez-vous :** utilisateur = root, mot de passe = celui que vous avez choisi.
50. Vous êtes dans le tableau de bord Proxmox VE !

Certificat SSL

Le navigateur va peut-être afficher un avertissement de sécurité « certificat non reconnu ». C'est normal pour un serveur local. Cliquez « Accepter / Continuer ».

7. Configuration réseau Proxmox

Proxmox utilise un système de « bridges » réseau pour connecter les containers et VMs au réseau local.

7.1 Vérifier le bridge réseau

51. Dans l'interface Proxmox, allez dans : Datacenter (à gauche) → votre noeud « proxmox ».
52. Puis : Network.
53. Vous devriez voir un bridge « vmbr0 » déjà créé automatiquement pendant l'installation.
54. Ce bridge est lié à votre carte réseau physique et permet aux containers/VMs de communiquer sur le réseau local.

7.2 Configurer une IP fixe pour le bridge (si nécessaire)

En général, Proxmox a déjà configuré vmbr0 avec l'IP 192.168.20.20 pendant l'installation. Vérifiez :

55. Cliquez sur « vmbr0 ».
56. Vérifiez que l'IP est bien « 192.168.20.20/24 ».
57. La passerelle doit être « 192.168.1.1 ».
58. Si tout est correct, rien à changer.

7.2 Création des interfaces VLAN

Maintenant que le switch a des VLANs configurés, vous devez créer les interfaces VLAN correspondantes dans Proxmox :

59. Dans Proxmox, allez dans : votre noeud « proxmox » → Network.
60. Cliquez « Create » → « Linux VLAN ».
61. **Créer vmbr0.10 (accès au NAS) :**

```
Name :          vmbr0.10
VLAN raw device : vmbr0
VLAN Tag :      10
IPv4/CIDR :     192.168.10.1/24
Gateway :       (laisser vide)
Autostart :     ✓
```

62. **Créer vmbr0.20 (zone services) :**

```
Name :          vmbr0.20
VLAN raw device : vmbr0
VLAN Tag :      20
IPv4/CIDR :     192.168.20.1/24
Gateway :       (laisser vide)
Autostart :     ✓
```

63. **Créer vmbr0.30 (zone admin) :**

```
Name :          vmbr0.30
VLAN raw device : vmbr0
VLAN Tag :      30
IPv4/CIDR :     192.168.30.1/24
Gateway :       (laisser vide)
Autostart :     ✓
```

64. Cliquez « Apply Configuration » pour activer les interfaces.
65. Redémarrez Proxmox pour que tout soit pris en compte :

```
reboot
```

✅Vérification

Après le redémarrage, reconnectez-vous à Proxmox via https://192.168.20.20:8006
Allez dans Network → vous devriez voir vmbr0, vmbr0.10, vmbr0.20, et vmbr0.30 tous actifs.
Proxmox peut maintenant router le trafic entre les VLANs et agit comme passerelle pour TrueNAS et le container.

8. Création du container LXC & déploiement des services

Vous allez créer un container LXC sur Proxmox pour héberger vos services. Un seul container suffit pour démarrer – vous pourrez toujours en créer d'autres plus tard.

8.1 Téléchargement d'un template LXC

66. Dans Proxmox, allez dans : Storage → local → CT Templates.
67. Cliquez « Download from Template Library ».
68. Cherchez « ubuntu » et téléchargez la dernière version (ex: ubuntu-24.04-cloud).

8.2 Création du container

69. Cliquez « Créer CT » (en haut à droite, ou clic droit sur votre noeud → Create → LXC Container).
70. Paramètres de base :

```
Nom :          homelab-services
Mot de passe : [choisissez un mot de passe fort]
Template :     ubuntu-24.04
```

71. Disque dur : laissez 8 Go (amplement suffisant pour ces services).
72. Processeur : 2 cœurs.
73. Mémoire : 2048 Mo (2 Go). Vous avez 8 Go sur le Dell, gardez du côté libre pour Proxmox.
74. **Réseau :** Bridge = vmbr0.20 (VLAN 20). Assignez l'IP fixe 192.168.20.30/24.
75. Confirmez et créez le container.
76. Démarrez le container.

8.3 Connexion au container

77. Dans Proxmox, sélectionnez votre container « homelab-services ».
78. Cliquez « Console » (en haut à droite).
79. Identifiez-vous avec « root » et le mot de passe que vous avez choisi.
80. Vous êtes maintenant dans un terminal Ubuntu !

8.4 Installation de Docker dans le container

Les services AdGuard, Bitwarden et Jellyfin vont être déployés via Docker Compose.

81. Dans la console du container, exécutez ces commandes une par une :

```
curl -fsSL https://get.docker.com | sh
```

```
systemctl enable docker && systemctl start docker
```

```
apt update && apt install -y docker-compose-plugin
```

✓ Vérification

Tapez « docker --version » et « docker compose version ». Si vous voyez des numéros de version, Docker est bien installé.

9. Configuration de AdGuard Home

AdGuard Home est un serveur DNS filtrant. Il bloque les pubs et trackers pour tout votre réseau local.

9.1 Création du fichier Docker Compose

82. Dans la console du container, créez un dossier :

```
mkdir -p /opt/homelab/adguard && cd /opt/homelab/adguard
```

83. Créez le fichier docker-compose.yml :

```
nano docker-compose.yml
```

Collez le contenu suivant :

```
version: '3'
```

```
services:
  adguard:
    image: adguard/adguard-home
    container_name: adguard
    restart: unless-stopped
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "3000:3000/tcp"
    volumes:
      - ./config:/opt/adguard-home/data
      - ./work:/opt/adguard-home/work
```

84. Sauvegardez avec Ctrl+S puis quittez avec Ctrl+X.
85. Lancez le service :

```
docker compose up -d
```

9.2 Configuration initiale d'AdGuard

86. Sur votre PC, ouvrez votre navigateur et allez à : http://192.168.20.30:3000
87. Suivez l'assistant de configuration AdGuard Home.
88. Choisissez un nom d'utilisateur et un mot de passe.
89. AdGuard Home est prêt !

9.3 Activer AdGuard comme DNS sur votre réseau

Pour que AdGuard filtre les requêtes DNS de toutes les machines de votre réseau, vous devez changer le DNS configuré sur votre routeur :

90. Ouvrez l'interface de votre routeur/FAI.
91. Dans les paramètres réseau ou DHCP, changez le serveur DNS vers : 192.168.20.30
92. Sauvegardez. Les appareils du réseau utiliseront désormais AdGuard comme DNS.

10. Configuration de Bitwarden

Bitwarden est un gestionnaire de mots de passe open-source. Vous allez héberger votre propre instance.

10.1 Création du fichier Docker Compose

93. Dans la console du container :

```
mkdir -p /opt/homelab/bitwarden && cd /opt/homelab/bitwarden
nano docker-compose.yml
```

```
version: '3'
services:
  bitwarden:
```

```
    image: bitwarden/core:latest
    container_name: bitwarden
    restart: unless-stopped
    ports:
      - "8080:80"
    volumes:
      - ./data:/data
    environment:
      - ROCKET_DISABLE_USER_REGISTRATION=true
```

94. Sauvegardez et quittez.
95. Lancez le service :

```
docker compose up -d
```

10.2 Première connexion

96. Sur votre PC, ouvrez : http://192.168.20.30:8080
97. Créez un compte (vous êtes le seul utilisateur par défaut).
98. Bitwarden est prêt !

Conseils Bitwarden

Pour la production, vous pouvez utiliser l'image officielle « bitwarden/bitwarden » à la place de « core ». Elle inclut toutes les fonctionnalités.

Si vous voulez activer l'inscription pour plusieurs utilisateurs, retirez la ligne ROCKET_DISABLE_USER_REGISTRATION.

Les données Bitwarden sont stockées dans le dossier ./data – sauvegardez ce dossier régulièrement vers votre TrueNAS.

11. Configuration de Jellyfin

Jellyfin est votre serveur média personnel. Il permet de streamer films, séries et musique depuis votre réseau local.

11.1 Création du fichier Docker Compose

Jellyfin a besoin de monter un dossier média. Ce dossier sera le partage SMB de votre TrueNAS (vous le monterez dans la section 12).

99. Dans la console du container :

```
mkdir -p /opt/homelab/jellyfin && cd /opt/homelab/jellyfin
mkdir -p /mnt/media
nano docker-compose.yml
```

```
version: '3'
services:
```

```
  jellyfin:
    image: jellyfin/jellyfin
    container_name: jellyfin
    restart: unless-stopped
    network_mode: host
    volumes:
      - ./config:/config
      - ./cache:/cache
      - /mnt/media:/mnt/media:ro
```

100. Sauvegardez et quittez.
101. Lancez :

```
docker compose up -d
```

11.2 Configuration initiale de Jellyfin

102. Sur votre PC, ouvrez : http://192.168.20.30:8096
103. Suivez l'assistant de configuration.
104. Créez un compte administrateur.
105. Ajoutez vos bibliothèques de médias (vous pointerez vers /mnt/media/films, /mnt/media/series, etc. – ces dossiers seront disponibles après la section 12).
106. Jellyfin est prêt !

12. Configuration de Kiwix

Kiwix vous permet d'héberger une encyclopédie complète hors ligne (Wikipedia, Stack Overflow, etc.). C'est votre propre bibliothèque de connaissances accessible sur votre réseau local, même sans Internet.

12.1 Qu'est-ce que Kiwix ?

Kiwix est un serveur qui héberge des fichiers ZIM – des archives compressées de sites web entiers. Par exemple :

- Wikipedia (français, anglais, etc.) – plusieurs dizaines de Go
- Stack Overflow, Khan Academy, Project Gutenberg, OpenStreetMap
- Documentation technique, livres, tutoriels

Téléchargement des fichiers ZIM

Les fichiers ZIM se téléchargent depuis : https://library.kiwix.org/
Exemple : Wikipedia FR (sans images) = ~10 Go, Wikipedia FR (avec images) = ~90 Go.
Téléchargez les ZIM que vous voulez sur votre PC, puis copiez-les vers votre TrueNAS (via SMB) dans un dataset dédié.

12.2 Création du dataset Kiwix sur TrueNAS

107. Dans l'interface TrueNAS, allez dans Storage → Pools → votre pool « datapool ».
108. Cliquez « Add Dataset ».

109. Nom : kiwix → Créer.
110. Allez dans Sharing → SMB → Add.
111. Partagez le dataset /pool/kiwix comme partage SMB « kiwix ».
112. Depuis votre PC, copiez vos fichiers ZIM téléchargés vers ce partage SMB.

12.3 Création du fichier Docker Compose

113. Dans la console du container :

```
mkdir -p /opt/homelab/kiwix && cd /opt/homelab/kiwix
mkdir -p /mnt/kiwix
nano docker-compose.yml
```

```
version: '3'
services:
  kiwix:
    image: kiwix/kiwix-serve
    container_name: kiwix
    restart: unless-stopped
    ports:
      - "8181:80"
    volumes:
      - /mnt/kiwix:/data
    command: "*.zim"
```

114. Sauvegardez et quittez.
115. Avant de démarrer Kiwix, vous devez monter le partage SMB kiwix (comme pour Jellyfin) :

```
mount -t cifs //192.168.10.10/kiwix /mnt/kiwix -o
username=VOTRE_USER,password=VOTRE_MDP
```

116. Ajoutez cette ligne dans /etc/fstab pour un montage permanent (comme expliqué en Section 13).
117. Lancez le service :

```
docker compose up -d
```

12.4 Accès à votre encyclopédie

118. Sur votre PC, ouvrez : http://192.168.20.30:8181
119. Vous verrez la liste de tous vos fichiers ZIM disponibles.
120. Cliquez sur l'un d'eux (ex: Wikipedia FR) pour commencer à naviguer.
121. Kiwix offre une recherche intégrée et une navigation identique au site d'origine.

Conseils Kiwix

Les fichiers ZIM sont en lecture seule – vous ne pouvez pas les modifier.
Pour mettre à jour Wikipedia, téléchargez la dernière version ZIM et remplacez l'ancien fichier.
Kiwix est très léger en ressources – il consomme très peu de RAM même avec de gros fichiers ZIM.
Vous pouvez héberger plusieurs ZIM en même temps (Wikipedia + Stack Overflow + Khan Academy, etc.).

13. Configuration d'Anki Sync Server

Anki Sync Server vous permet d'héberger votre propre serveur de synchronisation pour Anki. Vos cartes de révision (vocabulaire norvégien, etc.) seront stockées sur votre homelab au lieu des serveurs AnkiWeb publics. Vous gardez vos apps Anki habituelles (PC, Android, iOS), seule la synchronisation change.

13.1 Pourquoi héberger son propre serveur Anki ?

- Confidentialité : vos données d'apprentissage restent chez vous
- Contrôle total : pas de limite de stockage ou de synchronisation
- Disponibilité : sync même si les serveurs AnkiWeb sont down
- Vitesse : synchronisation ultra-rapide en local quand vous êtes chez vous

13.2 Création du fichier Docker Compose

122. Dans la console du container :

```
mkdir -p /opt/homelab/anki && cd /opt/homelab/anki
nano docker-compose.yml
```

```
version: '3'
services:
  anki-sync:
    image: kuklinistvan/anki-sync-server:latest
    container_name: anki-sync
    restart: unless-stopped
    ports:
      - "27701:27701"
    volumes:
      - ./data:/app/data
    environment:
      - SYNC_USER1=VOTRE_USERNAME:VOTRE_MOT_DE_PASSE
      - MAX_SYNC_PAYLOAD_MEGS=500
```

Configuration

SYNC_USER1 : remplacez par votre nom d'utilisateur et mot de passe (format username:password).
Vous pouvez ajouter plusieurs utilisateurs : SYNC_USER2, SYNC_USER3, etc.
MAX_SYNC_PAYLOAD_MEGS : taille max des médias (images, audio) - 500 Mo devrait suffire.

123. Sauvegardez et quittez.
124. Lancez le service :

```
docker compose up -d
```

13.3 Configuration de l'app Anki Desktop (PC/Mac)

Sur votre ordinateur avec Anki installé :

125. Ouvrez Anki.

126. Allez dans : Outils → Préférences → Synchronisation.
127. Décochez « Utiliser AnkiWeb » (si coché).
128. **Configurez le serveur personnalisé :**

```
Serveur de sync : http://192.168.20.30:27701/
Serveur média :   http://192.168.20.30:27701/
```

129. Entrez votre nom d'utilisateur et mot de passe (ceux définis dans SYNC_USER1).
130. Cliquez « Synchroniser » dans Anki.
131. Vos decks sont maintenant synchronisés sur votre homelab !

13.4 Configuration sur smartphone (AnkiDroid / AnkiMobile)

Sur Android (AnkiDroid) :

- Ouvrez AnkiDroid → Menu (☰) → Paramètres → Avancé → Serveur de synchronisation personnalisé.
- Activez « Utiliser un serveur de synchronisation personnalisé ».
- Renseignez :

```
Adresse du serveur sync : http://192.168.20.30:27701/
Adresse du serveur média : http://192.168.20.30:27701/
```

- Retournez à l'écran principal → Synchroniser.
- Entrez vos identifiants.
- C'est bon !

Sur iOS (AnkiMobile) :

AnkiMobile supporte les serveurs personnalisés depuis la version 2.0.90+ :

- Ouvrez AnkiMobile → Paramètres → Synchronisation.
- Tapez sur « AnkiWeb Account ».
- En bas, activez « Custom sync server ».
- Entrez l'URL : http://192.168.20.30:27701/
- Entrez vos identifiants.
- Synchronisez.

⚠ Attention - Accès depuis l'extérieur

En local (WiFi chez vous), utilisez http://192.168.20.30:27701
Depuis l'extérieur (4G, autre WiFi), vous devrez passer par le VPN WireGuard d'abord.
Une fois connecté au VPN, l'URL reste la même : http://192.168.20.30:27701

13.5 Migration depuis AnkiWeb

Si vous avez déjà des decks sur AnkiWeb que vous voulez migrer :

132. Sur Anki Desktop, synchronisez une dernière fois avec AnkiWeb pour tout récupérer.
133. Changez la config pour pointer vers votre serveur (Section 13.3).
134. Faites « Upload vers le serveur » lors de la première sync.
135. Vos decks sont maintenant sur votre homelab.
136. Sur smartphone, faites « Download depuis le serveur » pour tout récupérer.

✓ Conseils Anki

Sauvegardez régulièrement le dossier /opt/homelab/anki/data – ce sont toutes vos cartes !
Vous pouvez ajouter ce dossier au dataset TrueNAS pour des backups automatiques.
L'app Anki fonctionne parfaitement offline – la sync n'est nécessaire que pour partager entre appareils.
Bon courage pour le norvégien ! □□

14. Configuration de WireGuard VPN (accès distant)

WireGuard est un VPN moderne et ultra-rapide qui vous permet d'accéder à votre homelab depuis n'importe où dans le monde de manière sécurisée. Vous pourrez vous connecter depuis votre smartphone en 4G, un autre WiFi, ou même depuis un réseau public.

13.1 Pourquoi WireGuard ?

- Accès sécurisé depuis l'extérieur : connexion chiffrée à votre homelab depuis n'importe où
- Ultra-rapide : beaucoup plus performant qu'OpenVPN
- Simple à configurer : quelques commandes suffisent
- Intégré au noyau Linux : stable et léger
- Multi-plateforme : apps officielles pour Android, iOS, Windows, macOS, Linux

□ Sécurité

WireGuard crée un tunnel chiffré entre votre appareil et votre homelab.
Personne ne peut intercepter vos données, même sur un WiFi public.
Votre trafic passe par votre homelab comme si vous étiez chez vous.

13.2 Création du fichier Docker Compose

137. Dans la console du container :

```
mkdir -p /opt/homelab/wireguard && cd /opt/homelab/wireguard
nano docker-compose.yml
```

```
version: '3'
services:
  wireguard:
    image: linuxserver/wireguard
    container_name: wireguard
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=Europe/Paris
      - SERVERURL=VOTRE_IP_PUBLIQUE_OU_DOMAINE
      - SERVERPORT=51820
      - PEERS=smartphone,laptop
      - PEERDNS=192.168.20.30
      - INTERNAL_SUBNET=10.13.13.0
```

```
    volumes:
      - ./config:/config
      - /lib/modules:/lib/modules
    ports:
      - 51820:51820/udp
    sysctls:
      - net.ipv4.conf.all.src_valid_mark=1
    restart: unless-stopped
```

⚠ Configuration importante

SERVERURL : mettez votre IP publique (trouvable sur https://whatismyip.com) ou votre nom de domaine si vous en avez un.
PEERS : liste des appareils qui pourront se connecter (smartphone, laptop, tablet, etc.). Séparez-les par des virgules.
PEERDNS : l'IP de votre container (192.168.20.30) pour utiliser AdGuard Home via le VPN.

138. Sauvegardez et quittez.
139. Lancez le service :

```
docker compose up -d
```

13.3 Récupération des configurations clients

WireGuard génère automatiquement des QR codes pour chaque appareil. Pour les voir :

```
docker logs wireguard
```

Vous verrez des QR codes s'afficher dans les logs. Chaque QR code correspond à un appareil (smartphone, laptop, etc.).

13.4 Configuration sur smartphone (Android/iOS)

140. Téléchargez l'app WireGuard officielle depuis Google Play Store ou App Store.
141. Ouvrez l'app → Cliquez sur le → Scan QR code.
142. Scannez le QR code correspondant à « smartphone » affiché dans les logs.
143. Donnez un nom à la connexion (ex: « Homelab »).
144. Activez le VPN avec le bouton toggle.
145. Vous êtes connecté à votre homelab !

13.5 Configuration sur ordinateur

Pour un laptop/PC, vous devez récupérer le fichier de configuration :

146. Les fichiers de config sont dans : /opt/homelab/wireguard/config/peer_laptop/
147. Copiez le fichier peer_laptop.conf sur votre PC.
148. Téléchargez WireGuard pour votre OS : https://www.wireguard.com/install/
149. Importez le fichier .conf dans l'app WireGuard.
150. Activez la connexion.

13.6 Redirection de port sur votre box Internet

Pour que WireGuard soit accessible depuis l'extérieur, vous devez ouvrir le port 51820/UDP sur votre box :

151. Ouvrez l'interface de votre box (en général http://192.168.1.1).
152. Allez dans les paramètres « NAT / PAT » ou « Redirection de ports ».
153. Créez une règle :

```
Port externe :  51820 (UDP)
Port interne :  51820 (UDP)
IP locale :     192.168.20.30  (votre container)
```

154. Sauvegardez la règle.
155. Testez la connexion WireGuard depuis votre smartphone en 4G (WiFi désactivé).

Conseils WireGuard

Si votre IP publique change souvent (IP dynamique), utilisez un service comme DuckDNS ou No-IP pour avoir un nom de domaine stable.
WireGuard ne consomme presque pas de batterie sur smartphone.
Vous pouvez configurer le VPN pour se connecter automatiquement hors de chez vous.
Le trafic DNS passe par AdGuard Home → blocage des pubs même en déplacement !

15. Liaison Proxmox ↔ TrueNAS (dossiers partagés)

Cette section explique comment monter les partages SMB de TrueNAS dans votre container Proxmox, pour que Jellyfin (et les autres services) puissent accéder à vos données.

12.1 Monter le partage SMB dans le container

156. Dans la console du container « homelab-services » :

```
apt update && apt install -y cifs-utils
```

157. Créez le point de montage :

```
mkdir -p /mnt/media
```

158. Montez le partage SMB (remplacez « jellyfin » par le nom de votre partage, et utilisez les credentials SMB créés dans TrueNAS) :

```
mount -t cifs //192.168.10.10/jellyfin /mnt/media -o
username=VOTRE USER,password=VOTRE MDP
```

12.2 Rendre le montage permanent

Pour que le dossier soit monté automatiquement à chaque démarrage, ajoutez une ligne dans /etc/fstab :

```
nano /etc/fstab
```

Ajoutez cette ligne à la fin du fichier :

```
//192.168.10.10/jellyfin  /mnt/media  cifs
username=VOTRE_USER,password=VOTRE_MDP,uid=1000,gid=1000  0  0
```

159. Sauvegardez et quittez.
160. Testez avec :

```
mount -a
ls /mnt/media/
```

Si vous voyez les dossiers de votre partage TrueNAS, tout est connecté !

Conseils de sécurité

Ne laissez pas le mot de passe en clair dans fstab. À la place, créez un fichier séparé avec les credentials :
Créez /root/.smbcredentials avec : username=VOTRE_USER et password=VOTRE_MDP
Puis dans fstab utilisez : ...,credentials=/root/.smbcredentials,...
Et faites : chmod 600 /root/.smbcredentials

16. Isolation réseau & architecture VLANs

Cette section explique comment votre homelab est isolé du réseau familial grâce aux VLANs. Votre switch TL-SG605E supporte déjà 802.1Q nativement.

13.1 Architecture actuelle (simple)

Votre homelab est maintenant complètement isolé du réseau familial (192.168.1.0/24). Toutes vos machines fonctionnent sur les VLANs 10-30, créant une infrastructure privée et sécurisée.

13.2 Plan des sous-réseaux (VLANs)

Voici la correspondance entre les zones de couleurs de votre schéma et les VLANs à configurer :

Zone (couleur)	VLAN ID	Sous-réseau
Bleue – NAS	VLAN 10	192.168.10.0/24
Rose – Services	VLAN 20	192.168.20.0/24
Verte – Clients	VLAN 30	192.168.30.0/24

13.3 Configuration des VLANs sur le TL-SG605E

Voici les étapes pour configurer les VLANs directement sur votre switch via son interface web :

161. Ouvrez l'interface du switch : http://192.168.1.2
162. Allez dans le menu : VLAN → 802.1Q VLAN.
163. Dans « Global Config », activez « 802.1Q VLAN » et cliquez « Apply ».
164. **Créez VLAN 10 (NAS) :** entrez « 10 » dans le champ VLAN ID. Ajoutez le port où est branché l'Acer (TrueNAS) comme port « Untagged ». Le port vers Proxmox doit être « Tagged » (il transporte plusieurs VLANs). Cliquez Apply.

165. **Créez VLAN 20 (Services) :** entrez « 20 ». Ajoutez le port Proxmox comme « Untagged ». Le port vers le routeur comme « Tagged ». Cliquez Apply.
166. **Créez VLAN 30 (Clients) :** entrez « 30 ». Ajoutez le port de votre PC comme « Untagged ». Le port vers le routeur comme « Tagged ». Cliquez Apply.
167. Allez dans VLAN → 802.1Q PVID Setting. Assignez les PVID : port Acer = 10, port Proxmox = 20, port PC = 30.
168. Sauvegardez la configuration du switch.

13.4 Configuration des VLANs côté Proxmox

Proxmox doit aussi créer des interfaces réseau pour chaque VLAN :

169. Dans Proxmox, allez dans votre noeud → Network.
170. Créez une nouvelle interface de type « VLAN » :

```
Interface VLAN 10 :  vmbr0.10  →  IP 192.168.10.1/24  (pour communiquer avec le NAS)
Interface VLAN 20 :  vmbr0.20  →  IP 192.168.20.1/24  (pour les services/containers)
```

171. Assignez ces interfaces VLAN à votre container LXC selon besoin.
172. Activez le pare-feu Proxmox pour contrôler les flux entre les VLANs.

Conseils VLANs

Cette configuration VLAN est une évolution optionnelle. Votre homelab fonctionne parfaitement sans elle.
Faites-la uniquement une fois votre homelab de base stable et fonctionnel.
Le port « Tagged » sur le switch = un port qui transporte plusieurs VLANs en même temps (vers le routeur ou vers Proxmox).
Le port « Untagged » = un port qui n'appartient qu'à un seul VLAN (vers une machine spécifique).

13.5 Bonnes pratiques de sécurité de base

- Utilisez des mots de passe forts et différents pour chaque service.
- Ne jamais exposer vos services directement à Internet sans VPN (comme WireGuard ou Tailscale).
- Faites des sauvegardes régulières de vos données sur TrueNAS.
- Gardez Proxmox et TrueNAS à jour.
- Activez le pare-feu intégré à Proxmox pour limiter l'accès aux services.

17. Vérifications finales & maintenance

14.1 Checklist de vérification

✓	TrueNAS est accessible sur http://192.168.10.10
✓	Proxmox est accessible sur https://192.168.20.20:8006
✓	AdGuard Home fonctionne sur http://192.168.20.30:3000
✓	Bitwarden fonctionne sur http://192.168.20.30:8080
✓	Jellyfin fonctionne sur http://192.168.20.30:8096
✓	Kiwix fonctionne sur http://192.168.20.30:8181

✓	Anki Sync fonctionne (testez la sync depuis l'app)
✓	WireGuard VPN est actif (testez depuis 4G)
✓	Les partages SMB TrueNAS sont montés dans le container
✓	Jellyfin peut lire les fichiers médias depuis TrueNAS
✓	AdGuard filtre les requêtes DNS (testez dans un navigateur)

14.2 Maintenance régulière

- Mises à jour : Vérifiez les mises à jour de Proxmox (dans Settings) et de TrueNAS régulièrement (tous les mois).
- Sauvegardes : Utilisez la fonction de snapshot de Proxmox pour sauvegarder vos containers. Exportez aussi régulièrement les données vers un disque externe.
- Surveillance : Installez un outil de monitoring comme Netdata ou Grafana dans un container pour surveiller la santé de vos serveurs.
- Logs : En cas de problème, consultez les logs dans Proxmox (sur chaque container) et dans les interfaces de TrueNAS.

14.3 Ports utilisés – résumé

Port	Service
53 (TCP/UDP)	AdGuard Home – DNS
3000 (TCP)	AdGuard Home – Interface web
8080 (TCP)	Bitwarden – Interface web
8096 (TCP)	Jellyfin – Interface web
8181 (TCP)	Kiwix – Encyclopédie
27701 (TCP)	Anki Sync Server
51820 (UDP)	WireGuard – VPN accès distant
445 (TCP)	SMB – Partages TrueNAS
8006 (TCP)	Proxmox – Interface d'admin

Félicitations !

Votre homelab est opérationnel ! Vous avez maintenant un NAS TrueNAS, un hyperviseur Proxmox avec des containers pour AdGuard Home, Bitwarden, Jellyfin et Kiwix (votre encyclopédie personnelle), tout relié sur votre réseau local via le switch TP-Link.
N'hésitez pas à explorer d'autres services : Nextcloud, Home Assistant, Pi-hole, Portainer… Les possibilités sont illimitées.