

PROJET HOMELAB

Infrastructure personnelle Proxmox & TrueNAS

Architecture du projet

Création d'un **réseau privé isolé** au sein du réseau familial existant. Infrastructure complète avec serveur de virtualisation Proxmox VE et serveur de stockage TrueNAS SCALE, interconnectés via un switch managé TP-Link avec **segmentation VLAN 802.1Q**. Le homelab fonctionne sur des sous-réseaux dédiés (192.168.10-30.x), totalement séparés du WiFi principal de la maison, garantissant un accès restreint et un contrôle total.

Composant	Spécifications	Rôle
Dell Latitude	8 Go RAM 256 Go SSD Proxmox VE 8	Hyperviseur Containers LXC
Acer	16 Go RAM 2x 256 Go + 500 Go SSD 2x USB 32 Go (système) TrueNAS SCALE	Serveur NAS Stockage centralisé Partages SMB
TP-Link TL-SG605E	5 ports Gigabit 802.1Q VLAN	Switch managé Segmentation réseau

Services hébergés

- **AdGuard Home** – Filtrage DNS au niveau réseau, blocage publicités
- **Bitwarden** – Gestionnaire de mots de passe auto-hébergé
- **Jellyfin** – Serveur multimédia personnel (films, séries, musique)
- **Kiwix** – Encyclopédie hors ligne (Wikipedia, Stack Overflow, etc.)
- **WireGuard VPN** – Accès sécurisé au homelab depuis n'importe où

Mise en œuvre technique

1. Infrastructure et virtualisation

Installation et configuration de **Proxmox VE 8** comme hyperviseur principal sur le Dell Latitude. Création d'un container LXC Ubuntu pour héberger les services via Docker et Docker Compose. Configuration réseau avec bridge vmbr0 et attribution d'IPs fixes pour une gestion optimale.

2. Stockage centralisé avec TrueNAS

Déploiement de **TrueNAS SCALE** sur 2 clés USB 32 Go en miroir RAID 1 pour le système d'exploitation. Création d'un pool de stockage **RAIDZ1** avec les 3 SSDs (2x 256 Go + 500 Go) offrant ~756 Go utilisables avec redondance contre la perte d'un disque. Configuration de datasets dédiés (jellyfin, kiwix, bitwarden, backups) et mise en place de partages SMB/NFS pour l'accès réseau.

3. Réseau privé isolé & segmentation VLAN

Le projet consiste à créer un **réseau privé au sein du réseau WiFi familial**. Interconnexion des équipements via le switch **TP-Link TL-SG605E** (Easy Smart, 5 ports Gigabit, 802.1Q). Mise en place de **3 VLANs distincts** sur des sous-réseaux dédiés (192.168.10-30.x), complètement **isolés du réseau WiFi principal** de la maison (192.168.1.x). Seul l'administrateur (moi) a accès à ces sous-réseaux, créant ainsi une infrastructure personnelle sécurisée et indépendante. Les règles de pare-feu bloquent tout accès depuis le WiFi familial vers le homelab.

Réseau	Sous-réseau	Accès	Usage
WiFi familial	192.168.1.0/24	Famille, invités	Navigation web, streaming, usage quotidien
Homelab privé (VLANs 10-30)	192.168.10-30.0/24	Admin uniquement	Serveurs, stockage, services auto-hébergés

VLAN	Zone	Sous-réseau	Équipements
VLAN 10	Bleue – NAS	192.168.10.0/24	TrueNAS (Acer) – 192.168.10.10
VLAN 20	Rose – Services	192.168.20.0/24	Proxmox – 192.168.20.20 Container LXC – 192.168.20.30
VLAN 30	Verte – Admin	192.168.30.0/24	Accès administrateur uniquement

■ Isolation et contrôle d'accès

- **Réseau privé dans le réseau** : le homelab est invisible depuis le WiFi familial
- **Accès restreint** : seul l'administrateur peut accéder aux sous-réseaux 192.168.10-30.x
- **Pare-feu strict** : règles bloquant tout trafic entrant depuis le réseau principal
- **Isolation multi-niveaux** : séparation NAS / Services / Admin au sein même du homelab
- **Indépendance** : l'infrastructure fonctionne de manière autonome et sécurisée

4. Déploiement des services

Containerisation des services via **Docker & Docker Compose** dans le container LXC. Montage des partages SMB de TrueNAS dans le container pour accès aux données. Configuration de chaque service avec persistance des données et automatisation du démarrage au boot.

Service	Port	Description technique
AdGuard Home	53, 3000	DNS filtering, blocage publicités au niveau réseau
Bitwarden	8080	Gestionnaire mots de passe, chiffrement AES-256
Jellyfin	8096	Media server, transcodage H.264/H.265
Kiwix	8181	Encyclopédie offline (fichiers ZIM), Wikipedia FR ~10-90 Go
WireGuard	51820/UDP	VPN moderne, accès distant sécurisé depuis Internet

Compétences développées

Virtualisation & conteneurisation

- Installation et administration Proxmox VE
- Gestion de containers LXC
- Docker & Docker Compose
- Optimisation des ressources (RAM, CPU, stockage)

Systèmes & stockage

- Déploiement TrueNAS SCALE
- Configuration RAID (miroir, RAIDZ1)
- Gestion des pools ZFS et datasets
- Partages réseau SMB/NFS
- Linux (Ubuntu, configuration système)

Réseau & sécurité

- Création d'un réseau privé isolé dans un réseau existant
- Configuration VLANs 802.1Q (3 zones isolées)
- Switch managé TP-Link (Tagged/Untagged ports)
- Plan d'adressage IP multi-sous-réseaux
- Contrôle d'accès strict et règles de pare-feu
- Isolation complète du trafic réseau
- DNS filtering (AdGuard Home)

DevOps & automatisation

- Infrastructure as Code (docker-compose.yml)
- Automatisation des déploiements
- Configuration VPN WireGuard pour accès distant
- Gestion des volumes et montages
- Redirection de ports (NAT/PAT)
- Monitoring et maintenance
- Documentation technique complète

Technologies maîtrisées

Systèmes : Proxmox VE, TrueNAS SCALE, Ubuntu Server, ZFS

Conteneurisation : Docker, Docker Compose, LXC

Réseau : VLANs 802.1Q (segmentation 3 zones), SMB/NFS, DNS, DHCP, routage inter-VLAN

Sécurité : Firewall, isolation réseau multi-tiers, chiffrement, règles ACL

Services : AdGuard Home, Bitwarden, Jellyfin, Kiwix, WireGuard VPN

Perspectives d'évolution

L'infrastructure actuelle avec segmentation VLAN offre une base solide pour de nombreuses évolutions : ajout de nouveaux services (Nextcloud, Home Assistant, Pi-hole), affinage des règles de pare-feu inter-VLAN, mise en place de backups automatisés vers le cloud, monitoring avec Grafana/Prometheus, ou encore déploiement d'un VPN (WireGuard/Tailscale) pour accès distant sécurisé.

Infrastructure privée et autonome – Ce projet démontre la capacité à créer un **réseau privé complet au sein d'un réseau familial existant**, avec isolation totale via VLANs 802.1Q et contrôle d'accès strict. Maîtrise complète de la stack : virtualisation (Proxmox), stockage redondant (TrueNAS RAIDZ1), conteneurisation (Docker), et architecture réseau multi-tiers. Projet entièrement documenté dans un guide technique détaillé de 20+ pages.