Internet

tellserv.fr
(Domaine public)

Clients Externes
(Internet, hors réseau local)

Réseau Local (192.168.1.0/24)

Clients Locaux
(Ordinateurs, téléphones)
Réseau 192.168.1.0/24

Serveur Ubuntu 24.04 LTS (192.168.1.2)

dnsmasq
(*.local.tellserv.fr)
(image: system)
Port: 53

Pare-feu UFW
(image: system)
Ports: 80, 443, 9090

Réseau Docker
(traefik_network)

Traefik Public
(image: traefik)
192.168.1.2:80, 443

Pile Sécurité

CrowdSec
(image: crowdsecurity/crowdsec)
Détection d'intrusions

CrowdSec Bouncer
(image: fbonalair/traefik-crowdsec-bouncer)
Blocage automatique

TinyAuth
(image: ghcr.io/steveiliop56/tinyauth)
OAuth via GitHub

Traefik Private
(image: traefik)
192.168.1.3:80, 443

Plex
(image: plexinc/pms-docker)

AudiobookShelf
(image: ghcr.io/advplyr/audiobookshelf)

Kavita
(image: jvmilazz0/kavita)

PhotoPrism
(image: photoprism/photoprism)

Paperless
(image: ghcr.io/paperless-ngx/paperless-ngx)

Vikunja
(image: vikunja/vikunja)

FreshRSS
(image: freshrss/freshrss)

Stirling PDF
(image: stirlingpdf/stirling-pdf)

Kopia
(image: kopia/kopia)

Gotify
(image: gotify/server)

Blog
(image: ghost)

Mobilizon
(image: framasoft/mobilizon)

Larabouillere
(image: custom)

Feedropolis
(image: custom)

Yamtrack
(image: custom)

Loggifly
(image: custom)

Pingvin
(image: stonith404/pingvin-share)

EteSync
(image: etesync/server)

Bin
(image: privatebin/privatebin)

ClipCascade
(image: custom)

qBittorrent
(image: linuxserver/qbittorrent)

JOAL
(image: anthonyraymond/joal)

Cockpit
(image: cockpit/ws)

Dockge
(image: louislam/dockge)

Beszel
(image: henrygd/beszel)

Uptime Kuma
(image: louislam/uptime-kuma)

Glance
(image: glanceapp/glance)

Watchtower
(Monitoring des mises à jour)
(image: containrrr/watchtower)

Autoheal
(image: willfarrell/autoheal)

Headscale
(image: headscale/headscale)

Vaultwarden
(Gestionnaire de mots de passe)
(image: vaultwarden/server)

⚙️ ORCHESTRATION ANSIBLE

Playbook principal : playbook.yml

4 rôles exécutés en séquence :

📦 **common** - Paquets de base, dnsmasq, firewall UFW

🖥️ **cockpit** - Interface web de gestion serveur (port 9090)

🐳 **docker** - Installation Docker CE, création du réseau traefik_network

📌 **services** - Templates .env depuis Vault, synchronisation stacks/, déploiement via docker compose

Commande de déploiement :
ansible-playbook -i inventory/hosts.yml playbook.yml --ask-vault-pass

🌐 CONFIGURATION RÉSEAU

Architecture réseau :

- Réseau local : 192.168.1.0/24
- Serveur principal : 192.168.1.2
- DNS local : dnsmasq (*.local.tellserv.fr → 192.168.1.2)
- Traefik Public : 192.168.1.2:80, 443 (Services publics via tellserv.fr)
- Traefik Private : 192.168.1.3:80, 443 (Services locaux via *.local.tellserv.fr)
- Réseau Docker : traefik_network (bridge externe)
- Pare-feu : UFW (ports 80, 443, 9090)
- Cockpit : Port 9090 (gestion système)

📖 LÉGENDE

═══ FLUX DE TRAFIC ═══

——— Bleu épais
Trafic Internet public
(clients externes → services publics)

——— Violet épais
Trafic réseau local
(clients internes → services privés)

— — Rouge pointillé
Flux sécurité
(vers pile CrowdSec/TinyAuth)

↔ Orange bidirectionnel
Communication CrowdSec ↔ Traefik
(détection/blocage)

——— Vert
Routing vers services applicatifs

— — Violet pointillé
Déploiement Ansible (IaC)

══ CODE COULEURS COMPOSANTS ══

Bleu
Reverse Proxies
(Traefik Public/Private)

Rouge
Pile Sécurité
(CrowdSec, Bouncer, TinyAuth)

Vert
Services applicatifs Docker
(30+ conteneurs)

Violet
Orchestration Ansible,
clients locaux

Jaune
Infrastructure réseau
(DNS, firewall)

Gris
Frontières réseau
(conteneurs logiques)

ARCHITECTURE HOMELAB - NOTES TECHNIQUES

- Double Traefik pour séparation stricte public/privé
- Pile sécurité centralisée repositionnée entre les deux Traefik (optimisation des flux)
- DNS local automatique via dnsmasq (résolution *.local.tellserv.fr)
- Tous les services connectés au réseau Docker partagé (traefik_network)
- Secrets managés via Ansible Vault (chiffrement AES256)
- Déploiement Infrastructure-as-Code (IaC) reproductible et versionné
- Surveillance et monitoring intégrés (Uptime Kuma, Beszel, Glance)
- Sécurité multi-couches : CrowdSec (IDS), TinyAuth (OAuth), Vaultwarden (gestion secrets)