Contexte TiersLieux

Compte rendu – Projet TiersLieux

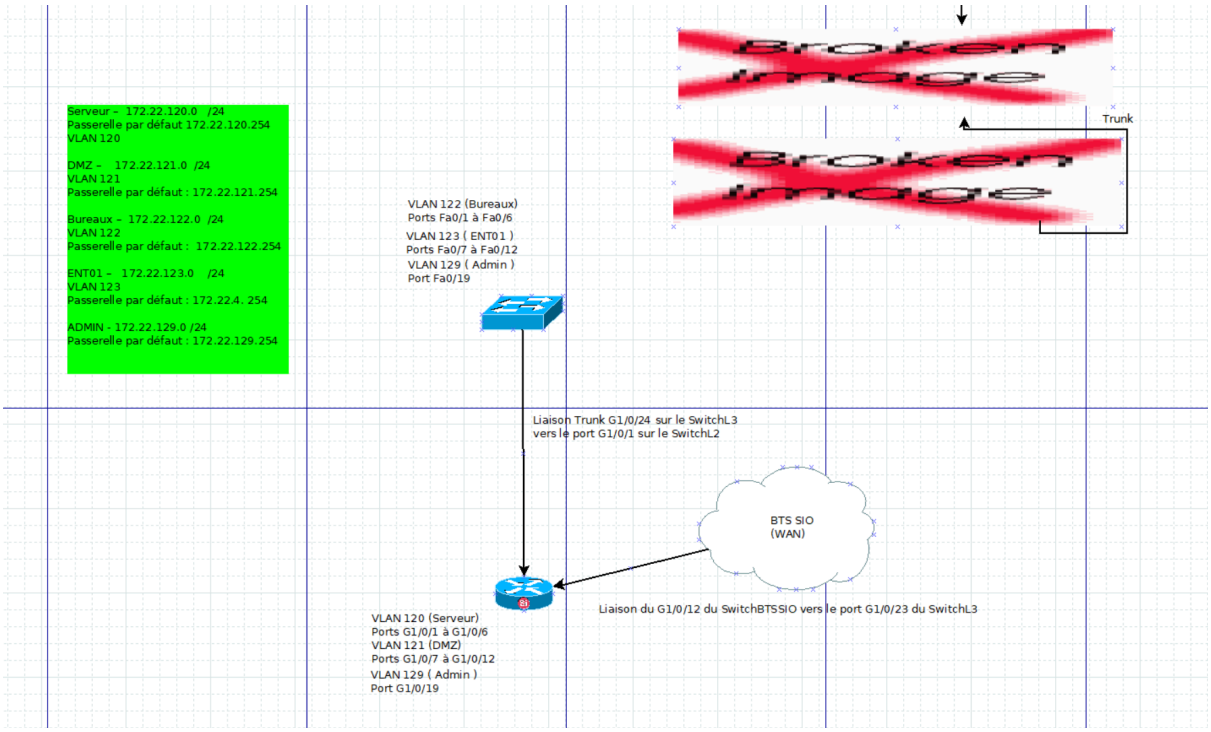
Liens importants :
Contexte :
https://delenne.org/wp-content/uploads/2026/03/Contexte-TiersLieux.pdf
Documentation Technique:
https://delenne.org/wp-content/uploads/2026/03/Documentation-Technique-_-Grafana-Prometheus.pdf

Bloc	Activités réalisées
1.1 Gérer le patrimoine informatique	Gestion Active Directory (utilisateurs/groupes), configuration VLAN, DNS, NAT/PAT, supervision avec Prometheus et Grafana, sauvegarde des configurations
1.2 Répondre aux incidents	Mise en place de GLPI, suivi des tickets, détection et traitement des incidents via supervision
1.4 Travailler en mode projet	Analyse des besoins, organisation en phases (InfraSYS, InfraRES, VPN, supervision), suivi des performances
1.5 Mettre à disposition un service	Déploiement AD, GLPI, VPN, tests de connectivité, mise en place d'un accès sécurisé pour les utilisateurs

1. Contexte général

TiersLieux est une association régionale qui gère des Espaces de Travail Partagés (ETP) pour les indépendants, télétravailleurs, TPE et jeunes entreprises. Chaque ETP est conçu pour offrir un environnement de travail flexible, convivial et sécurisé, avec des bureaux modulables, des salles de réunion, des espaces libres-service et des équipements numériques modernes.

Les résidents ont accès à des services tels que le Wi-Fi haut débit, des imprimantes et photocopieurs, ainsi que des réservations en ligne via un portail sécurisé. L'accès aux locaux est disponible 24/7 grâce à un pass numérique. Les entreprises bénéficient également d'un réseau sécurisé avec des VLAN dédiés et d'un accès contrôlé aux serveurs mutualisés.



Phase 1 – InfraSYS : Infrastructure système

Objectifs

- ☑ ~~Installer et configurer l'**Active Directory** pour gérer les utilisateurs et les groupes.~~
- ☑ ~~Déployer le serveur **GLPI** pour la gestion des incidents.~~
- ☑ ~~Assurer l'accès distant aux serveurs et postes clients.~~

Opérations principales

Active Directory

- [x] ~~Installer **2 contrôleurs de domaine** (Infra1 + DNS et Infra2 en réplication).~~
- [x] ~~Créer les **utilisateurs et groupes** : IT, Bureau, Compta.~~
- [x] ~~Configurer les **répertoires personnels mappés** sur H: pour chaque utilisateur.~~

DNS

- [x] ~~Configurer la **zone inverse** pour le réseau TiersLieux.~~
- [x] ~~Définir un **redirecteur DNS** vers 1.1.1.1 pour les requêtes externes.~~

GLPI

- [x] ~~Installer et intégrer GLPI au domaine.~~
- [x] ~~Créer un utilisateur IT avec profil Technicien et un utilisateur Bureau avec droits limités (création tickets).~~

Phase 1.1 – InfraRES : Infrastructure réseau

Objectifs

- [x] ~~Configurer les **VLANs et le routage inter-VLAN** selon le schéma TiersLieux.~~
- [x] ~~Assurer la **gestion distante** des équipements et serveurs via SSH et bureau à distance.~~
- [x] ~~Garantir la **connectivité Internet et la sécurité** via le pare-feu Stormshield.~~
- [x] ~~Mettre en place la **supervision SNMP** pour tous les équipements réseau.~~

Opérations principales

Réseau

- [x] ~~Définir et configurer les VLANs pour serveurs, bureaux et administration.~~
- [x] ~~Activer le **Rapid Spanning Tree** sur les commutateurs.~~
- [x] ~~Configurer le **routage inter-VLAN** pour permettre la communication entre sous-réseaux.~~
- [x] ~~Assurer l'accès Internet via NAT/PAT sur le pare-feu.~~

Administration

- [x] ~~Activer l'accès **SSH** aux serveurs Linux et équipements réseau depuis le VLAN d'administration.~~
- [x] ~~Sauvegarder les configurations des équipements sur le NAS via FTP.~~
- [x] ~~Configurer SNMP pour la supervision (communauté publique en RO, privée en RW).~~

Phase 2. Mission Supervision

Dans le cadre du projet, ma première mission consistait à mettre en place une solution de supervision pour évaluer les performances et la disponibilité des serveurs et équipements réseau des ETP. L'objectif principal était de choisir un outil efficace, peu coûteux, capable de surveiller à la fois l'infrastructure technique et les services applicatifs.

Objectifs de supervision

- [x] ~~Surveiller les serveurs Windows et Linux : CPU, mémoire, espace disque, processus et I/O.~~
- [x] ~~Contrôler l'état des équipements réseau (routeurs, commutateurs).~~
- [ ] Vérifier les services réseau et applicatifs essentiels : DNS, DHCP, HTTP, SMTP, FTP, Active Directory, bases de données, etc.
- [ ] Analyser le trafic réseau : bande passante, paquets perdus, trames broadcast/multicast.
- [ ] Détecter les anomalies et envoyer des notifications (mail ou SMS) en cas de problème.

- [ ] Générer des rapports mensuels et des graphiques pour faciliter le suivi par la direction.

Solution choisie

J’ai utilisé Prometheus pour collecter les métriques et Grafana pour visualiser les données via des tableaux de bord clairs et interactifs. Les alertes ont été configurées selon différents seuils pour anticiper les problèmes avant qu’ils n’impactent les utilisateurs.

Résultats

Grâce à cette supervision, nous pouvons désormais suivre en temps réel la santé des serveurs, des équipements réseau et des services applicatifs. Les tableaux de bord permettent aux techniciens et à la direction de détecter rapidement tout dysfonctionnement et d’intervenir de manière préventive.

Phase 3. Mission VPN – Accès sécurisé

La deuxième mission portait sur la mise en place d’un accès VPN sécurisé afin de connecter les agences distantes au siège et de permettre aux utilisateurs nomades d’accéder aux ressources de TiersLieux.

Objectifs

- [ ] Permettre aux utilisateurs nomades d’accéder aux serveurs de fichiers et aux applications depuis n’importe quel endroit via un VPN SSL.
- [ ] Connecter les agences distantes au siège via un VPN IPSec site-à-site pour partager les ressources internes.
- [ ] Garantir un accès Internet sécurisé et filtré pour chaque VLAN, tout en respectant la sécurité des données.

Opérations réalisées

Configuration de la NAT pour permettre l’accès Internet depuis tous les VLAN.

Mise en place du VPN site-à-site et du VPN nomade avec Stormshield, avec authentification via Active Directory.

Tests de connectivité et validation de l’accès aux fichiers et applications depuis différents points distants.

En option, mise en place d’un portail captif pour authentifier les utilisateurs avant de leur donner l’accès à Internet, y compris les visiteurs.

Résultats

Les utilisateurs peuvent désormais accéder aux ressources TiersLieux de manière sécurisée, que ce soit depuis leur agence ou en mobilité. Le VPN et le portail captif garantissent un accès contrôlé et sécurisé, tout en permettant de centraliser la gestion des connexions.