Projet : Document d'Architecture Technique de déploiement de GLPI

Contexte :

Mise en place d'une solution GLPI destinée à la gestion de parc informatique et au support utilisateurs, dans un premier temps en environnement de test, avec une mise en production ultérieure.

L'infrastructure repose sur une Machine Virtuelle hébergée sur un hyperviseur Proxmox et un système d'exploitation Debian 13.

1. Analyse des Besoins Clients

Avant tout déploiement technique, il est nécessaire de valider le périmètre avec le client :

1.1 Périmètre fonctionnel

- Gestion de parc informatique :
    - Inventaire matériel et logiciel
    - Suivi du cycle de vie des équipements
    - Historique des modifications
- Helpdesk :
    - Gestion des tickets (Incidents, demandes)
    - Affectation aux agents (support informatique, administrateurs, prestataires)
    - Notification par mail

- Gestion des utilisateurs :
    - Authentification centralisée via Active Directory (LDAPS)
    - Gestion des rôles et profils utilisateurs

1.2 Volumétrie

- Nombre d'utilisateurs finaux : à valider
- Nombre d'agents techniques : à valider
- Nombre estimé d'équipements inventoriés : à valider

1.3 Environnement existant

- Présence d'un Active Directory
- Infrastructure virtualisée sous Proxmox
- Serveur de messagerie existant
- Outil de supervision existant :
    - Présence d'un outil de supervision (Zabbix, Centreon, Nagios) : à valider
    - Méthode de supervision attendue (SNMP, agent, HTTP(S)) : à valider
- Solution de sauvegarde existante :
    - Présence d'un outil de sauvegarde (Veeam, Proxmox Backup, Cobian Backup, etc.) : à valider
    - Version de la solution de sauvegarde : à valider
    - Périmètre couvert par la sauvegarde (VM, fichiers, bases de données) : à valider
    - Politique de rétention existante : à valider
- Stockage externe / Cloud pour la sauvegarde :
    - Existe-t-il un stockage distant / cloud disponible pour externaliser les sauvegardes: à valider
    - Fournisseur / modalités d'accès : à valider

2. Analyse des Risques

(Voir la matrice des risques détaillée ci-dessous)

Risque	Impact	Probabilité	Mesures de réduction
Indisponibilité du service GLPI	Moyen	Faible	Sauvegardes régulières, snapshot VM
Mauvaise configuration LDAP	Moyen	Moyen	Tests en environnement de test
Saturation du stockage	Moyen	Faible	Supervision et alertes
Faille de sécurité applicative	Élevé	Faible	Mises à jour régulières, HTTPS

3. Prérequis Infrastructure (Hardware)

Le déploiement s'effectuera sur une **Machine Virtuelle (VM)** hébergée sur un hyperviseur **Proxmox**.

OS Cible : Debian 13 .

Ressource	Recommandation	Justification
vCPU	**2 vCPU**	Suffisant pour le traitement PHP/Web standard.

Ressource	Recommandation	Justification
RAM	**4 Go**	Minimum recommandé (Passer à 8 Go si >500 utilisateurs).
Stockage	**50 Go (SSD)**	OS + Base de données MariaDB + Stockage des pièces jointes/Documents.
Partitionnement	**LVM Standard**	Découpage recommandé pour isoler les composants critiques :
	`/`	15 Go – Système Debian 13 + LAMP + GLPI
	`/var`	10 Go – Données applicatives légères et cache GLPI
	`/var/log`	5 Go – Journaux système et applicatifs
	`/var/lib/mysql`	15 Go – Base de données MariaDB pour GLPI
	`/home`	5 Go – Comptes administrateurs

4. Prérequis Logiciels

4.1 Système

- OS : Debian 13

4.2 Stack applicative (LAMP)

- Serveur Web : Apache2
- Base de données : MariaDB 10.11 minimum (ou MySQL 8.0)
- Langage : PHP 8.2 minimum

4.3 Extensions PHP requises

- php-mysqli
- php-curl
- php-gd
- php-intl
- php-ldap
- php-zip
- php-mbstring
- php-xml

5. Prérequis Réseau et Flux

5.1 Configuration IP

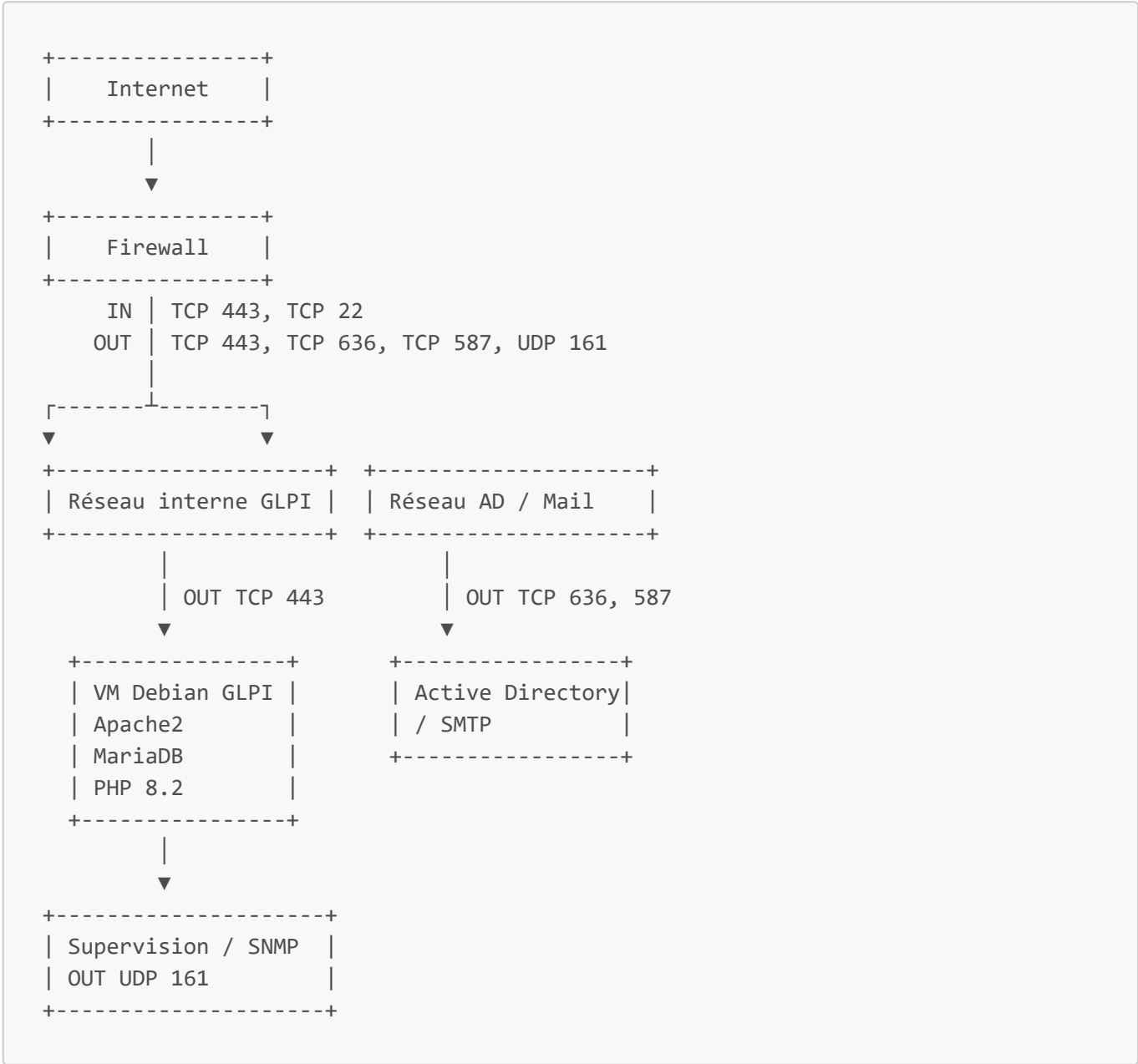
- Adresse IPv4 fixe
- Enregistrement DNS de type A pointant vers la VM GLPI

5.2 Matrice de Flux (Firewall)

Sens	Protocole	Port	Service	Description
IN	TCP	443	HTTPS	Accès sécurisé utilisateurs et agents

Sens	Protocole	Port	Service	Description
IN	TCP	22	SSH	Administration (restreint IP admins)
OUT	TCP	443	HTTPS	Accès Internet sécurisé (mises à jour, plugins)
OUT	TCP	636	LDAPS	Liaison sécurisée Active Directory
OUT	TCP	587	SMTP	Relais messagerie
OUT	UDP	161	SNMP	Supervision

5.3 Schéma réseau – Déploiement GLPI



6. Stratégie de Sécurité

6.1 Sécurisation des accès

- Mise en place obligatoire du HTTPS

6.2 Durcissement du système

- Désactivation de l'accès SSH root
- Authentification SSH par clé
- Pare-feu (UFW)
- Fail2ban (SSH / Apache)
- Mises à jour de sécurité régulièrement

6.3 Sauvegardes et PRA

Stratégie de sauvegarde

La plateforme GLPI est protégée par une stratégie de sauvegarde professionnelle respectant la règle **3-2-1** :

- **3 copies** des données
- **2 supports différents** (local + NAS)
- **1 copie hors site** (Cloud)

En l'absence de site secondaire, l'externalisation des sauvegardes est assurée via un stockage distant accessible par Internet (Cloud).
L'objectif est de garantir la **disponibilité et l'intégrité** des données GLPI en cas d'incident majeur.

Périmètre de sauvegarde

La sauvegarde couvre l'ensemble de la machine virtuelle GLPI :

- Système d'exploitation Debian 13
- Application GLPI
- **Base de données MariaDB** (dump quotidien et compressé)
- Fichiers applicatifs (`/var/www/glpi`)

Plan de sauvegarde

- **Fréquence :** quotidienne
- **Automatisation :** via Veeam Backup pour éviter toute erreur humaine
- **Compression :** réduite pour optimiser l'espace de stockage
- **Stockage sur plusieurs supports :**
  - Local : infrastructure Proxmox
  - Externe : NAS interne
  - Distant : Cloud sécurisé

Notes :

- Les dumps de la base MariaDB permettent une restauration rapide en cas de corruption ou suppression accidentelle des données.
- Les sauvegardes complètes de la VM assurent une restauration rapide de l'ensemble de la plateforme si nécessaire.

Politique de rétention

- Rétention : **30 jours**

- Conservation des sauvegardes sur les 30 derniers jours
- Suppression automatique des sauvegardes expirées

PRA (Plan de Reprise d'Activité)

- Restauration complète de la VM GLPI possible depuis les sauvegardes
- Restauration des données applicatives et de la base de données
- Tests de restauration réalisés périodiquement sur un environnement de test
- Objectif : remise en service rapide du service GLPI en cas de sinistre

6.4 Évolution : intégration SSO (Single Sign-On)

L'authentification actuelle repose sur LDAP, solution fiable pour l'environnement de test.

Pour un futur SSO, deux options existent :

- SAML 2.0
- OpenID Connect.

Recommandation :

OpenID Connect : plus simple à intégrer, compatible web et mobile, basé sur des standards modernes (JSON/REST), idéal pour les applications actuelles.

SAML 2.0 : robuste pour les applications web traditionnelles, mais plus complexe à mettre en place et moins adapté aux apps modernes et mobiles.

Conclusion : OpenID Connect est privilégié pour un SSO moderne, sécurisé et évolutif.

Bénéfices du SSO :

- Authentification unique
- Meilleure expérience utilisateur
- Centralisation IAM
- Traçabilité renforcée

Cette évolution n'a pas été implémentée volontairement afin de garantir la stabilité et la lisibilité de l'architecture actuelle.

7. Supervision et exploitation

- Surveillance des ressources : CPU, RAM, disque
- Supervision de la disponibilité HTTP(S)
- Centralisation et consultation des logs
- Outils possibles : Zabbix, Centreon, Nagios

8. Planning prévisionnel

- Installation de Debian 13
- Installation et configuration de la stack LAMP
- Déploiement de GLPI

- Suppression du dossier /install
- Configuration LDAP (LDAPS) et SMTP
- Tests fonctionnels
- durcissement système
- Validation avant mise en production

Auteur : ESCRIVA Yann

Projet : Décembre 2025