DOSSIER TECHNIQUE E6 - PROJET 2

Déploiement GLPI
et Intégration Active Directory

Présenté par : **Allan Brennus**
BTS SIO (Option SISR)
Session 2026

TABLE DES MATIÈRES

1. Présentation du Contexte et Enjeux (SARL Fantôme).....3

2. Architecture et Sécurisation du Serveur Debian 12.....4

3. Déploiement de la pile LAMP (Linux, Apache, MariaDB, PHP).....5

4. Sécurisation et Isolation de la Base de Données.....6

5. Configuration des Hôtes Virtuels (VirtualHost) et Droits.....7

6. Intégration de l'Annuaire Active Directory (LDAP).....8

7. Troubleshooting : Résolution des Habilitations Utilisateurs.....9

8. Configuration ITIL : Profils et Centre de Services.....10

9. Bilan, Apports Professionnels et Conclusion.....11

1. Présentation du Contexte et Enjeux

Ce second projet s'inscrit dans la continuité de la sécurisation et de l'exploitation de l'infrastructure Vénus de la SARL Fantôme (déployée lors du Projet 1). L'entreprise ayant connu une croissance rapide, le support informatique aux utilisateurs (gestion des pannes, demandes de matériel) ne pouvait plus être géré de manière artisanale (par email ou téléphone).

L'objectif de ce projet est donc de déployer une solution professionnelle d'ITSM (Information Technology Service Management) open-source : GLPI (Gestionnaire Libre de Parc Informatique).

Les enjeux principaux sont :
• Centraliser l'ensemble des tickets d'incidents (Helpdesk) selon le référentiel ITIL.
• Sécuriser l'authentification en liant GLPI au domaine Active Directory de l'entreprise (fantome.local).
• Assurer un haut niveau de sécurité du serveur Linux hébergeant l'application (Droits restreints, VirtualHosts).

2. Architecture et Sécurisation du Serveur Debian 12

2.1 Déploiement de la Machine Virtuelle

GLPI a été déployé sous forme de machine virtuelle sur le cluster Proxmox de l'infrastructure Vénus. Pour des raisons de sécurité, ce serveur est placé dans le VLAN 99 (Management).

Le choix du système d'exploitation s'est porté sur Debian 12 (Bookworm), reconnu mondialement pour sa stabilité exceptionnelle en environnement serveur de production.

• Adresse IP statique : 192.168.99.3
• Ressources : 2 vCPU, 4 Go de RAM, 40 Go de stockage
• Passerelle (FortiGate) : 192.168.99.254
• Serveur DNS (Active Directory) : 192.168.99.1

2.2 Sécurisation de l'accès SSH

Dès l'installation du système, l'accès distant via SSH a été sécurisé en interdisant la connexion directe avec le compte Root, obligeant l'utilisation d'un compte utilisateur standard avant toute élévation de privilèges.

```
apt install ssh -y
nano /etc/ssh/sshd_config
# Modification de la ligne :
PermitRootLogin no
```

```
systemctl restart ssh
```

3. Déploiement de la pile LAMP

GLPI nécessite un serveur Web, un langage d'exécution et une base de données. L'installation des paquets a été réalisée de manière granulaire sur Debian 12.

3.1 Installation du serveur Web et de la Base de Données

```
apt update && apt upgrade -y
apt install apache2 mariadb-server -y
```

3.2 Installation des extensions PHP requises

L'application GLPI dépend d'un grand nombre de bibliothèques PHP pour fonctionner correctement (notamment `php-ldap` pour se connecter à l'Active Directory de la SARL Fantôme, et `php-xml` pour la génération de rapports).

```
apt install php php-ldap php-imap php-apcu php-xmlrpc \
php-cas php-mysqli php-mbstring php-curl php-gd \
php-simplexml php-xml php-intl php-zip php-bz2 -y

systemctl reload apache2
```

3.3 Configuration de la Timezone (Fuseau Horaire)

Il est crucial pour un système de Helpdesk (qui mesure les SLA et le temps de réponse) d'avoir une horloge parfaitement calibrée au niveau du système et de la base de données :

```
timedatectl set-timezone "Europe/Paris"
mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -p -u root mysql
```

4. Sécurisation et Isolation de la Base de Données

La sécurité des bases de données est souvent le maillon faible des infrastructures. L'installation native de MariaDB a donc été durcie avec l'outil `mysql_secure_installation` (suppression des accès anonymes, désactivation du login Root distant).

4.1 Création d'un compte de service MySQL isolé

Plutôt que d'utiliser l'utilisateur système 'Root' pour connecter l'application GLPI à la base de données, un utilisateur dédié (`glpi_admin`) a été créé. Le principe de "Moindre Privilège" a été appliqué : ce compte n'a de droits que sur la base `glpidb`.

```
mysql -u root -p

CREATE DATABASE glpidb;
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpi_admin'@'localhost' IDENTIFIED BY
'MotDePasseComplexe2025!';
FLUSH PRIVILEGES;
EXIT;
```

5. Installation de GLPI et Configuration Apache

5.1 Extraction et sécurisation des répertoires

L'archive compressée (.tgz) de la dernière version de GLPI a été téléchargée via `wget` et extraite dans le répertoire d'Apache. Les droits de propriété ont été strictement restreints au groupe système `www-data` pour éviter toute exécution de code malveillant externe.

```
cd /tmp/
wget
https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz
tar xzf glpi-10.0.10.tgz -C /var/www/html/

chown -R www-data:www-data /var/www/html/glpi
chmod -R 775 /var/www/html/glpi
```

5.2 Bonnes pratiques : Déplacement des fichiers sensibles

Pour éviter que des fichiers de configuration ou des documents joints aux tickets ne soient accessibles directement par une requête web (faille LFI/RFI), les répertoires de configuration et de logs ont été sortis du dossier public `/var/www/` pour être déplacés dans l'arborescence racine de Linux (`/etc` et `/var/log`).

```
mkdir /etc/glpi
```

```
chown www-data /etc/glpi/
mv /var/www/html/glpi/config /etc/glpi

mkdir /var/log/glpi
chown www-data /var/log/glpi

# Suppression du script d'installation après réussite
rm /var/www/html/glpi/install/install.php
```

L'installation s'est finalisée sur l'interface web (http://192.168.99.3/glpi), confirmant la connexion à la base de données et validant les prérequis PHP.

6. Intégration de l'Annuaire Active Directory (LDAP)

Pour s'inscrire dans une logique d'entreprise (SSO/Authentification unifiée), il était indispensable que les employés n'aient pas de nouveau mot de passe à retenir. GLPI a été couplé avec le contrôleur de domaine Windows Server (déployé lors du Projet 1).

6.1 Matrice de configuration LDAP

Dans le menu 'Configuration > Authentification > Annuaires LDAP', les paramètres suivants ont été injectés pour pointer vers le serveur AD `192.168.99.1` de la SARL Fantôme :

Paramètre GLPI	Valeur technique injectée
Nom	Active Directory Fantôme
Serveur	ldap://192.168.99.1
Port	389
Basedn (Racine de recherche)	DC=fantome,DC=local
Rootdn (Compte de service)	CN=GLPI_Bind,OU=Service IT,DC=fantome,DC=local
Champ de login (Identifiant)	samaccountname

L'importation de masse a ensuite été exécutée. GLPI a interrogé l'Active Directory et a rapatrié automatiquement tous les utilisateurs (Noms, Prénoms, Emails) dans sa propre base, prouvant le bon fonctionnement de la liaison inter-VLAN (VLAN 99) autorisée par le pare-feu FortiGate.

7. Troubleshooting : Résolution des Habilitations LDAP

Le déploiement d'une infrastructure complexe génère inévitablement des obstacles techniques qu'il faut savoir analyser et résoudre.

7.1 Identification du problème (Symptômes)

Lorsqu'un utilisateur du domaine tentait de se connecter pour la première fois à GLPI, ses identifiants Windows étaient acceptés par l'Active Directory, mais l'interface GLPI renvoyait une erreur critique : "Vous n'avez pas les droits pour vous connecter à cette application".

7.2 Méthodologie de diagnostic et Résolution

En analysant le comportement logiciel, j'ai compris que l'authentification était valide (Phase 1), mais que l'autorisation (Phase 2) échouait. GLPI ne savait tout simplement pas quel niveau de droits (Profil) attribuer à cet utilisateur nouvellement importé.

J'ai résolu cette anomalie en configurant le moteur de règles de GLPI (Administration > Règles > Règles d'affectation d'habilitations à un utilisateur).

J'ai créé une règle conditionnelle :

• Si : L'utilisateur provient de l'annuaire LDAP 'Active Directory Fantôme'.

• Action : Alors, lui assigner automatiquement le profil 'Client' et l'entité 'Root entity'.

Dès l'activation de cette règle, les utilisateurs ont pu accéder au portail instantanément.

8. Configuration ITIL : Profils et Centre de Services

Conformément au référentiel ITIL (Information Technology Infrastructure Library), le helpdesk a été paramétré pour distinguer clairement les "Incidents" (Pannes) des "Demandes" (Ex: Besoin d'une nouvelle souris).

8.1 Sécurisation et UX du Profil "Client"

Les employés de la SARL Fantôme utilisent le profil "Client". Pour éviter de les submerger d'options techniques, l'interface a été épurée :

- • Interface utilisateur : Forcée en mode "Simplifiée".
- • Visibilité : L'option "Voir mes tickets" est activée, mais l'accès aux tickets globaux de l'entreprise est strictement interdit (Isolement des données).

• Interaction matérielle : L'option "Lier avec des éléments matériels" est cochée. Lorsqu'un utilisateur crée un ticket, il peut sélectionner son propre ordinateur dans une liste déroulante, ce qui fournit instantanément l'adresse IP et l'adresse MAC de la machine au technicien.

8.2 Le profil Technicien et Cycle de vie des tickets

Les membres de l'équipe IT (dont je fais partie) disposent du profil "Technicien" ou "Super-Admin". Nous gérons les tickets selon un Workflow strict : Nouveau ➔ En cours (Attribué) ➔ En attente (Si besoin d'informations du client) ➔ Résolu ➔ Clos.

9. Bilan, Apports Professionnels et Conclusion

Ce second projet a permis de concrétiser la couche logicielle (ITSM) par-dessus l'infrastructure réseau complexe (Vénus) déployée en première phase.

D'un point de vue technique, le déploiement d'un service sur Debian 12 en ligne de commande m'a conforté dans ma maîtrise de l'écosystème Linux (Gestion des paquets, durcissement de MariaDB, gestion fine des permissions avec chown/chmod, et configuration de serveurs virtuels Apache).

D'un point de vue fonctionnel, l'intégration de GLPI avec le serveur Active Directory démontre la capacité à décloisonner les services (Linux d'un côté, Windows Server de l'autre) grâce au protocole LDAP. La résolution de l'incident d'habilitation a prouvé la nécessité d'une démarche d'analyse logique (Symptôme ➔ Cause ➔ Remédiation).

Aujourd'hui, la SARL Fantôme dispose d'un réseau cloisonné et sécurisé, couplé à un centre de services IT professionnel, robuste et prêt à l'emploi.