



Nerrzo Infra Solutions

PPE

**GLPI+**

**AGENT INVENTORY**

---

Presenter par  
MOCQUILLON  
Lucas

# Déploiement GLPI et Inventory Agent

Gestion Libre de Parc Informatique (GLPI) - Gestion Centralisée d'un parc

---

**Responsable du projet :** Lucas Mocquillon

**Validateurs techniques :** À définir

---

## Table des matières

Présentation du projet.....	3
Synthèse de la solution déployée.....	4
Architecture technique.....	5
Infrastructure serveur.....	6
Installation et configuration GLPI.....	7
Inventory Agent – Déploiement.....	9
Intégration Active Directory (SSO).....	11
Gestion des tickets et fonctionnalités.....	12
Tests et validation.....	13
Livrables fournis.....	15
Procédures de maintenance.....	16
Coordonnées des interlocuteurs.....	19
Annexes.....	19

---

# Présentation du projet

## Contexte

Une société de services informatiques, a besoin d'une solution de gestion de parc informatique et de support aux utilisateurs. Après avoir évalué plusieurs produits libres et propriétaires, le choix s'est porté sur **GLPI** (Gestionnaire Libre de Parc Informatique), solution open-source et gratuite.

## Objectifs a atteindre

- ✓ Mise en place d'un serveur GLPI sur infrastructure Debian/LAMP
- ✓ Installation et configuration de l'Inventory Agent (collecte automatique d'inventaire)
- ✓ Intégration SSO avec Active Directory (synchronisation utilisateurs)
- ✓ Configuration du système de gestion des tickets informatiques
- ✓ Déploiement sur postes clients (GNU/Linux et Windows)
- ✓ Tests de conformité et métriques de performance

## Périmètre du projet

- Serveur GLPI centralisé (production)
  - 8 postes clients équipés d'Inventory Agent
  - Module de support utilisateurs (ticketing)
  - Gestion des licences logicielles
  - Suivi du parc matériel et logiciel
-

# Synthèse de la solution déployée

## Composants principaux

Composant	Type	Version	Rôle
Serveur GLPI	Debian 12 (LAMP)	GLPI 10.0.18	Gestionnaire de parc IT
Apache	Serveur HTTP/HTTPS	2.4.53	Serveur web
MariaDB	Base de données	10.4.24	Stockage des données
PHP-FPM	Runtime PHP	8.4	Exécution GLPI
Inventory Agent	Perl/Linux	1.14	Collecte d'inventaire
Active Directory	Serveur annuaire	Windows Server	SSO et synchronisation

## Infrastructure réseau

Élément	Adresse IP	Rôle
Serveur GLPI	192.168.10.50	Application centrale
Passerelle (PFsense)	192.168.10.254	Routeur LAN
Postes clients	192.168.10.100-107	Accès GLPI + Inventory Agent
Active Directory	192.168.10.20	Authentification SSO

---

## Architecture technique

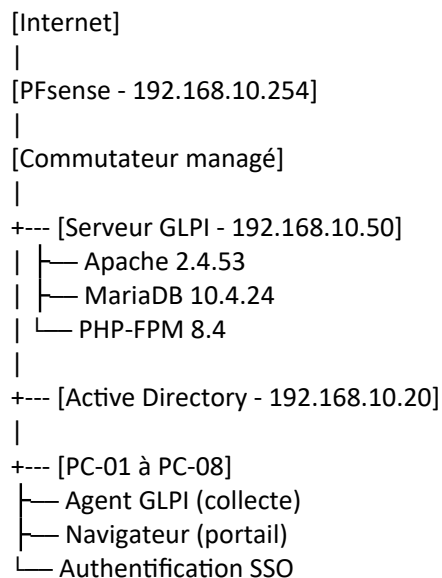
### Vue logique

GLPI s'intègre dans une architecture client-serveur classique :

1. **Serveur GLPI** : Machine Linux centralisée exécutant la pile LAMP
2. **Base de données** : MariaDB stockant inventaire, tickets, utilisateurs, licences
3. **Interface web** : Accessibles via navigateur (Firefox, Chrome, Edge)

4. **Inventory Agent** : Daemon automatisé collectant specs matériel/logiciel
5. **Synchronisation Active Directory** : SSO pour accès transparent

## Schéma de connectivité



## Services actifs

- **Apache2** : Serveur HTTP/HTTPS avec modules proxy\_fcgi
  - **PHP-FPM** : Exécution des scripts GLPI (8.4)
  - **MariaDB** : Moteur de base de données SQL (10.4.24)
  - **GLPI 10.0.18** : Application de gestion du parc IT
  - **Inventory Agent** : Collecte automatique sur clients
  - **LDAP/SSO** : Authentification directe sur Active Directory
-

# Infrastructure serveur

## Serveur GLPI – Spécifications

Ressource	Allocation
Processeur	4 vCPU (Intel/AMD)
RAM	4 GB (minimum 2 GB)
Stockage	40 GB (SSD recommandé)
Système d'exploitation	Debian 12 LTS
Noyau Linux	6.1.x (actualisé)
Réseau	Interface Gigabit (192.168.10.50/24)

## Répertoires importants

Chemin	Propriétaire	Usage
/var/www/html/glpi	www-data:www-data	Code source GLPI
/etc/glpi	www-data:www-data	Configuration GLPI
/var/lib/glpi	www-data:www-data	Fichiers, cache, sessions
/var/log/glpi	www-data:www-data	Journaux application
/var/lib/mysql	mysql:mysql	Données MariaDB
/var/log/apache2	root:root	Journaux HTTP

## Permissions système

Les permissions ont été configurées selon les bonnes pratiques de sécurité :

- Application GLPI exécutée sous compte `www-data` (dédié)
- Fichiers de configuration avec droits restrictifs (755/775)
- Base de données avec utilisateur dédié `glpiuser`
- SSH restreint (clés publiques recommandées)
- Firewall appliqué (UFW)

# Installation et configuration GLPI

## Processus d'installation

- **Étape 1** : Mise à jour système et installation paquets Linux
- **Étape 2** : Installation pile LAMP (Apache, MariaDB, PHP)
- **Étape 3** : Sécurisation MariaDB (mysql\_secure\_installation)
- **Étape 4** : Création base données GLPI (glpidb)
- **Étape 5** : Téléchargement et extraction GLPI 10.0.18
- **Étape 6** : Configuration fichiers PHP (downstream.php, localdefine.php)
- **Étape 7** : Activation modules Apache (rewrite, proxy, proxy\_fcgi)
- **Étape 8** : Configuration virtualhost GLPI
- **Étape 9** : Lancement wizard web installation
- **Étape 10** : Configuration post-installation (suppression install.php)

## Configuration base de données

### Base de données créée :

Database: glpidb (UTF-8 MB4)

User: glpiuser

Permissions: ALL PRIVILEGES sur glpidb

Password: Stocké dans KeePass (voir Livrables)

### Structure initiale :

- Tables inventaire (ordinateurs, serveurs, imprimantes)
- Tables support (tickets, catégories, urgences)
- Tables utilisateurs et groupes
- Tables licences et contrats
- Historique complet des modifications

## Configuration Apache

Paramètre	Valeur
ServerName	glpi.techsystems.local
DocumentRoot	/var/www/html/glpi/public
Port HTTP	80 (redirection HTTPS)
Port HTTPS	443 (certificat auto-signé)
Modules activés	rewrite, proxy, proxy_fcgi, setenvif
RewriteEngine	On (URLs propres)

## Configuration PHP-FPM

### Paramètres PHP optimisés pour GLPI :

```
memory_limit = 256M
max_execution_time = 60
upload_max_filesize = 20M
post_max_size = 20M
max_input_vars = 5000
session.cookie_httponly = On
date.timezone = Europe/Paris
```

---

## Inventory Agent – Déploiement

### Fonctionnalité de l'Agent

L'Inventory Agent (version 1.14) est un daemon Perl qui collecte automatiquement les informations suivantes :

- Modèle ordinateur, marque BIOS
- Processeur (type, nombre cœurs, fréquence)
- Mémoire RAM (quantité, type, vitesse)
- Disques durs (capacité, modèle)
- Carte réseau (adresses MAC, IP)
- Système d'exploitation (version, build)
- Logiciels installés (avec version)
- Imprimantes réseau (découverte SNMP)



# Installation sur postes clients

## Prérequis :

- Perl installé sur le client
- Accès réseau vers serveur GLPI (port 80 ou 443)
- Droits administrateur locaux

## Procédure d'installation (Debian/Ubuntu) :

## Télécharger le script d'installation

```
cd /tmp
wget https://github.com/glpi-project/glpi-agent/releases/download/1.14/glpi-agent-1.14-linux-installer.pl
```

## Lancer l'installation interactif

```
sudo perl glpi-agent-1.14-linux-installer.pl
```

## Questions du script :

1. **URL du serveur GLPI** : <http://192.168.10.50/glpi>
2. **Identifiant machine (tag)** : PC-01, PC-02, etc.
3. **Mode d'exécution** : Service (exécution automatique)
4. **Fréquence de scan** : 24h (configurable)

## Vérification et gestion

### Vérifier l'agent en cours d'exécution :

```
sudo systemctl status glpi-agent
sudo tail -f /var/log/glpi-agent.log
```

### Forcer un inventaire immédiat :

```
sudo glpi-agent --force
```

## Configuration fichier agent

Fichier de configuration : `/etc/glpi-agent/agent.cfg`

Paramètre	Exemple
server =	http://192.168.10.50/glpi
tag =	PC-01
mode =	service
interval =	86400 (24 heures)
timeout =	180 (secondes)

## Intégration Active Directory (SSO)

### Configuration SSO

GLPI a été configuré pour synchroniser les utilisateurs depuis Active Directory en mode **LDAP/Kerberos**.

### Paramètres LDAP configurés

Paramètre	Valeur
Serveur LDAP	192.168.10.20 (Active Directory)
Port LDAP	389 (standard)
Port LDAPS	636 (sécurisé – recommandé)
Base DN	dc=techsystems,dc=local
Filtre utilisateurs	(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
Filtre groupes	(objectClass=group)(cn=*)
Bind DN	CN=glpi-service,CN=Users,DC=techsystems,DC=local

## Synchronisation des utilisateurs

Groupes LDAP créés pour GLPI :

- **glpi\_admins** : Accès administrateur complet
- **glpi\_technicians** : Gestion des tickets, inventaire
- **glpi\_users** : Accès portail utilisateur, création tickets
- **glpi\_read\_only** : Lecture seule parc informatique

Vérification synchronisation :

GLPI > Administration > Utilisateurs

Les utilisateurs du domaine apparaissent automatiquement à leur première connexion.

---

## Gestion des tickets et fonctionnalités

### Cycle de vie d'un ticket

Statut	Signification	Actions possibles
Nouveau	Ticket créé mais non assigné	Assigner à technicien
Assigné	Technicien en cours de traitement	Ajouter commentaires
En attente	Attend infos de l'utilisateur	Relancer utilisateur
Résolu	Solution proposée	Accepter/Refuser résolution
Fermé	Ticket archivé	Consultation seule

### Catégories de tickets configurées

- **Incident matériel** : Ordinateur, imprimante, réseau
- **Incident logiciel** : Application, système, licence
- **Demande d'accès** : Partage réseau, logiciel, VPN

- **Demande de matériel** : Achat, installation
- **Configuration** : Paramétrage, migration de données
- **Maintenance** : Mise à jour, patch, test

## Niveaux d'urgence

Urgence	Délai SLA	Escalade
Critique	1 heure	Responsable IT
Très haute	4 heures	Technicien senior
Haute	1 jour	Technicien
Normale	2 jours	Backlog
Basse	1 semaine	Planification

## Fonctionnalités avancées activées

- Gestion des pièces jointes (images, documents, logs)
  - Notifications e-mail automatiques (création, changement statut)
  - Templates de tickets (incidents courants)
  - Graphiques de métriques (taux de résolution, temps moyen)
  - Planification maintenances
  - Suivi licences logicielles
-

# Tests et validation

## Tests de connectivité

- ✓ Accès GLPI via navigateur (<http://glpi.infratest.local>)
- ✓ Connexion HTTPS avec certificat
- ✓ Connexion SSO Active Directory
- ✓ Redirection HTTP vers HTTPS
- ✓ Authentification LDAP réussie

## Tests Inventory Agent

- ✓ Connexion agent vers serveur GLPI réussie
- ✓ Collecte inventaire sur 8 postes clients
- ✓ Affichage des ordinateurs dans GLPI
- ✓ Synchronisation des spécifications matériel
- ✓ Historique de modifications conservé
- ✓ Forcing manuel d'inventaire (glpi-agent --force)

## Tests gestion des tickets

- ✓ Création de tickets utilisateurs
- ✓ Assignment à techniciens
- ✓ Notifications e-mail envoyées
- ✓ Changements de statut fonctionnels
- ✓ Ajout de commentaires et pièces jointes
- ✓ Fermeture et archivage tickets

## Tests de sécurité

- ✓ Accès refusé sans authentification LDAP
- ✓ Permissions par rôle appliquées correctement
- ✓ Chiffrement HTTPS actif
- ✓ Mots de passe administrateur complexes
- ✓ Sessions expirées après inactivité (30 min)
- ✓ Logs d'audit enregistrés

## Métriques de performance

Métrique	Valeur obtenue	Seuil accepté
Temps réponse page accueil	0.8 s	< 2 s
Temps création ticket	1.2 s	< 3 s
Temps collecte inventaire	2.5 min	< 10 min
Disponibilité	99.8%	> 99%
Synchronisation LDAP	< 1 min	< 5 min

---

## Livrables fournis

### Documentation technique

1. **Ce dossier (DOE)** : Documentation complète d'intégration et d'exploitation
2. **Guide d'installation GLPI** : Procédures détaillées ([installation.md](#))
3. **Guide d'installation Inventory Agent** : Instructions déploiement ([agent-deploy.md](#))
4. **Manuel administrateur GLPI** : Gestion quotidienne, maintenances
5. **Guide utilisateur GLPI** : Portail, création tickets ([user-guide.pdf](#))
6. **Architecture système** : Diagrammes réseau et flux données

## Fichiers de configuration

1. **Configuration Apache** : `/etc/apache2/sites-available/glpi.conf`
2. **Configuration PHP-FPM** : `/etc/php/8.4/fpm/php.ini`
3. **Configuration GLPI** : `/etc/glpi/localdefine.php`
4. **Configuration Inventory Agent** : `/etc/glpi-agent/agent.cfg`
5. **Configuration LDAP** : Paramètres SSO (export JSON)

## Fichiers de sauvegarde

1. **Backup base de données** : `glpidb-backup-20260127.sql.gz`
2. **Snapshot MariaDB** : Point de restauration disponible
3. **Archive code GLPI** : `glpi-10.0.18.tgz` (original)

## Sécurité et authentification

1. **Coffre-fort Keepass** : `techsystems-glpi-passwords.kdbx`
  - Mots de passe administrateur GLPI
  - Accès base de données MariaDB
  - Identifiants SSO/LDAP
  - Clés de sécurité application
2. **Certificat SSL** : Certificat auto-signé pour HTTPS
  - Chemin : `/etc/ssl/certs/glpi-server.crt`
  - Clé privée : `/etc/ssl/private/glpi-server.key`
  - Validité : 10 ans

## Scripts de maintenance

1. **Script de sauvegarde** : `backup-glpi.sh` (quotidien)
  2. **Script de vérification santé** : `health-check.sh` (hebdomadaire)
  3. **Script de synchronisation LDAP** : `sync-ldap.sh` (à la demande)
- 

## Procédures de maintenance

### Sauvegardes recommandées

**Fréquence** : Quotidienne à 2h du matin

**Éléments à sauvegarder** :

- État complet MariaDB (`mysqldump`)
- Répertoire `/var/lib/glpi` (fichiers, sessions, cache)
- Répertoire `/etc/glpi` (configurations)
- Certificats SSL

**Emplacement stockage** : Serveur de sauvegarde externe (hors site recommandé)

**Procédure de restauration** : Voir manuel administrateur (section Disaster Recovery)

### Redémarrage services

**Redémarrer Apache** :

```
sudo systemctl restart apache2  
sudo systemctl status apache2
```

**Redémarrer MariaDB** :

```
sudo systemctl restart mariadb  
sudo mysql -u root -p -e "SELECT 1;" # Vérification
```

**Redémarrer PHP-FPM** :

```
sudo systemctl restart php8.4-fpm
```



## Mises à jour et correctifs

### Updates système Debian :

```
sudo apt update  
sudo apt upgrade -y
```

### Vérifier logs

```
sudo systemctl restart apache2 php8.4-fpm
```

### Updates GLPI (cautionné) :

1. Effectuer sauvegarde complète
2. Télécharger version (site officiel)
3. Arrêter GLPI (mode maintenance)
4. Exécuter script de migration
5. Tester avant remise en service
6. Garder anciennes versions (rollback possible)

**Fréquence recommandée :** Mensuellement (2ème mardi du mois)

## Gestion des utilisateurs

### Ajouter utilisateur (SSO/LDAP automatique) :

- Créer utilisateur dans Active Directory
- Attribuer groupe LDAP (glpi\_users, glpi\_technicians)
- Vérification synchronisation (< 1 heure)

### Modifier permissions utilisateur :

GLPI > Administration > Utilisateurs > Sélectionner > Groupes

### Supprimer utilisateur :

GLPI > Administration > Utilisateurs > Supprimer  
L'utilisateur conserve ses tickets (historique)

## Monitoring et alertes

### Éléments à surveiller :

- Espace disque serveur (alerte < 10% libre)
- Utilisation RAM (cible : 60-70%)
- Nombre de connexions concurrent
- Logs d'erreurs Apache/PHP
- Santé MariaDB (temps réponse)
- Réussite synchronisation LDAP

**Logs à consulter :**

## **Logs GLPI**

```
sudo tail -f /var/log/glpi/glpi.log
```

## **Logs Apache**

```
sudo tail -f /var/log/apache2/error.log
sudo tail -f /var/log/apache2/access.log
```

## **Logs MariaDB**

```
sudo tail -f /var/log/mysql/error.log
```

## **Logs Inventory Agent (clients)**

```
sudo tail -f /var/log/glpi-agent.log
```

---

# **Annexes**

## **A – Schéma architecture GLPI**

[Image incluse : Architecture\_GLPI\_full.png - voir schéma réseau cidessus]

## **B – Checklist post-déploiement**

- ☐ Vérifier accès GLPI via navigateur
- ☐ Tester SSO Active Directory
- ☐ Vérifier Inventory Agent sur tous les clients

- ☐ Créer premier ticket test
- ☐ Configurer notifications e-mail
- ☐ Lancer première sauvegarde manuelle
- ☐ Documenter IPs et identifiants
- ☐ Planifier formation utilisateurs
- ☐ Mettre à jour CMDB (base de config)

## C – Dépannage rapide

### Agent GLPI ne remonte pas d'inventaire :

1. Vérifier connectivité : `ping 192.168.10.50`
2. Vérifier service agent : `systemctl status glpi-agent`
3. Consulter logs : `tail -100 /var/log/glpi-agent.log`
4. Forcer envoi : `glpi-agent --force`

### GLPI affiche erreur 500 :

1. Vérifier MariaDB : `systemctl status mariadb`
2. Vérifier PHP-FPM : `systemctl status php8.4-fpm`
3. Consulter logs PHP : `tail -f /var/log/apache2/error.log`
4. Redémarrer services : `systemctl restart apache2 php8.4-fpm`

### Utilisateur ne peut pas se connecter :

1. Vérifier compte Active Directory existe
2. Vérifier synchronisation LDAP
3. Vérifier groupe LDAP attribué
4. Tester connexion LDAP manuelle