



Projet : Mise en place d'un outil ITSM (GLPI) intégré à Active Directory

Contexte

Ce projet a été réalisé de manière autonome dans un **laboratoire personnel**, avec pour objectif de simuler un **environnement de support informatique en conditions proches de la production**.

L'enjeu était de **reproduire le fonctionnement réel d'un service support N1/N2**, incluant :

- Authentification centralisée des utilisateurs,
- Gestion des incidents et des demandes,
- Priorisation via SLA,
- Documentation des procédures pour les techniciens,
- Diagnostic structuré des incidents (approche OSI).

Le projet s'inscrit dans une démarche de **montée en compétences en support informatique et administration systèmes/réseaux**, en s'appuyant exclusivement sur des **solutions open source**.

Objectif du projet

Les objectifs fonctionnels étaient les suivants :

- Déployer une solutions ITSM open source (GLPI)
- Intégrer GLPI à un **Active Directory existant** pour l'authentification centralisée
- Simuler un **flux réel de tickets utilisateurs**
- Mettre en place des **SLA et règles métier**
- Produire une **documentation opérationnelle N1**
- Comprendre et maîtriser les **flux réseau sous-jacents**

Les objectifs techniques incluaient :

- Intégration LDAP/AD,
- Sécurisation des accès (HTTPS),
- Diagnostic des incidents applicatifs et réseau,
- Exploitation quotidienne de l'outil (pas uniquement l'installation).



Architecture mise en place

Infrastructure existante

- **pfSense** pour le routage et gestion DHCP
- **Windows Server 2022**
 - Active Directory Domain Services
 - DNS avec forwarders (8.8.8.8, 1.1.1.1)
 - **Domaine** : homelab.local
- **Debian GNU/Linux**
 - Serveur Web (Apache avec HTTPS, certificat auto-signé)

Composants du projet

- MariaDB 11.8/PHP 8.2
- GLPI version 10.0.16

L'architecture respecte une séparation claire entre :

- Authentification (Active Directory / LDAP)
- Données applicatives (MariaDB)
- Interface utilisateur (HTTPS)

GLPI s'authentifie auprès d'Active Directory via LDAP pour centraliser la gestion des utilisateurs et des accès.

Intégration Active Directory

L'intégration AD constitue un **point central du projet**.

Fonctionnalités mises en œuvre :

- Authentification des utilisateurs GLPI via LDAP
- Import automatique des comptes Active Directory
- Attribution des profils selon les rôles
- Utilisation d'un **compte de service dédié**



Points clés maîtrisés :

- Structure LDAP et BaseDN
- Attributs AD (sAMAccountName)
- Différence entre authentification et autorisation
- Dépendance critique au DNS

Cette partie a nécessité un **diagnostic approfondi** et a permis de consolider la compréhension des mécanismes AD/LDAP.

Principe de fonctionnement

Le fonctionnement de la solution repose sur une chaîne de dépendances clairement identifiée :

1. Résolution DNS

La résolution correcte du domaine Active Directory est indispensable pour permettre l'authentification LDAP et la communication entre les services.

2. Authentification via Active Directory (LDAP)

GLPI délègue l'authentification des utilisateurs à Active Directory à l'aide d'un compte de service dédié.

Les informations d'identité sont récupérées depuis l'annuaire.

3. Autorisation applicative dans GLPI

Les utilisateurs authentifiés sont associés à des profils GLPI (Technicien, Self-Service) déterminant leurs droits dans l'outil.

4. Exploitation ITSM

Les utilisateurs peuvent créer des tickets, qui sont ensuite qualifiés, traités et clôturés par les techniciens selon les règles ITIL définies (catégories, priorités, SLA).

Tout dysfonctionnement sur une étape amont (DNS, LDAP) empêche le fonctionnement des étapes suivantes, ce qui renforce l'importance d'un diagnostic structuré.

Flux réseau et raisonnement OSI

Les flux nécessaires au fonctionnement de GLPI ont été identifiés afin de faciliter le diagnostic des incidents :

- **DNS** : résolution du domaine Active Directory (pré-requis critique)
- **LDAP** : authentification et import des comptes utilisateurs



- **HTTPS** : accès sécurisé à l'interface GLPI
- **MySQL** : accès à la base de données applicative locale

Le diagnostic réseau est abordé de manière structurée, en s'appuyant sur le modèle OSI :

- Couche réseau / transport (connectivité, ports, latence)
- Couche application (LDAP, HTTPS)

Cette approche permet une identification rapide de la couche défaillante et facilite la résolution des incidents en contexte de support N1/N2.

Exploitation opérationnelle

Gestion des tickets

- Création et traitement de **20 tickets réalistes**
- Incidents couvrant :
 - Accès et comptes
 - Problèmes réseau
 - Incidents matériels
 - Incidents logiciels
 - Demandes d'accès

Chaque ticket suit un cycle complet :

1. Création par l'utilisateur
2. Qualification
3. Diagnostic
4. Résolution
5. Documentation
6. Résolution et clôture

SLA et règles métier

- SLA définis selon la priorité
- Application automatique via les règles pour un ticket
- Respect des délais dans 100% des cas (laboratoire)



Problème rencontrés (principaux)

- **Capacité disque insuffisante sur le Serveur GLPI** : espace initialement sous-dimensionné pour l'exploitation applicative
 - extension du disque virtuel et réorganisation du stockage système, incluant la gestion correcte de l'espace swap
- **Compatibilité applicative (GLPI/PHP)** : version de PHP non supportée par GLPI 10.X
 - adaptation de l'environnement applicatif avec une version PHP compatible
- **Récupération des sources GLPI** : échec du téléchargement depuis le dépôt officiel
 - récupération alternative des sources et validation de l'intégrité avant déploiement
- **Permissions applicatives insuffisantes** : droits d'écriture bloquant la phase d'installations et de configuration
 - ajustement temporaire des permissions suivi d'un durcissement post-installation
- **Import LDAP sans utilisateurs visibles** : connexion LDAP fonctionnelle mais résultats d'import vides
 - utilisation de l'attribut standard sAMAccountName

Ces incidents ont permis de mettre en évidence :

- l'importance de l'anticipation des **besoins en stockage**,
- la gestion des **dépendances applicatives**,
- la distinction entre **connectivité LDAP** et **exploitation des données d'annuaire**,
- la nécessité d'un **équilibre entre accessibilité et sécurité** lors des phases d'installation

Validation fonctionnelle

Les tests suivants ont été réalisés afin de valider le bon fonctionnement de la solution dans un contexte proche de la production :

- Authentification d'un utilisateur Active Directory sur l'interface GLPI
- Import et synchronisation des comptes Active Directory via LDAP
- Attribution automatique des profils utilisateurs selon les rôles définis
- Création de tickets par des utilisateurs non-techniciens
- Prise en charge et traitement des tickets par un technicien



- Application automatique des SLA selon la priorité du ticket
- Consultation et utilisation de la base de connaissances
- Résolution et clôture des tickets avec traçabilité complète

L'ensemble des tests a été concluant, confirmant la stabilité et l'exploitabilité de la solution.

Documentation et support N1

Une base de connaissances a été constituée avec **4 procédures N1**, incluant :

- Réinitialisation de mot de passe AD
- Diagnostic réseau selon le modèle OSI
- Incidents DNS
- Procédure d'escalade N1 → N2.

Chaque procédure comprend :

- Symptômes
- Méthode de diagnostic
- Actions à réalisées
- Critères d'escalade

Résultat final

- Serveur GLPI fonctionnel et sécurisé
- Intégration AD opérationnelle
- Gestion complète du cycle de tickets
- SLA appliqués automatiquement
- Documentation N1 exploitable
- Environnement stable et reproductible



Compétences mises en avant

- Administration Linux (Debian)
- Active Directory / LDAP
- GLPI et ITSM
- Diagnostic réseau (DNS, LDAP, HTTPS)
- Sécurisation des services
- Documentation technique
- Support utilisateurs N1/N2

Topologie Réseau

