Procédure d'installation et de préparation de GLPI 11

Sommaire

1. Présentation

1.1 Objectifs

Installer GLPI 11 sur Debian 13 dans un environnement de test conforme aux exigences du DAT :

- gestion de parc
- helpdesk
- intégration LDAP
- sécurité
- sauvegardes et PRA

2. Prérequis

2.1 Matériel

- VM Proxmox
- 2 vCPU
- 4 Go RAM

- 50 Go SSD

Partitionnement recommandé :

- `/` : 15 Go
- `/var` : 10 Go
- `/var/log` : 5 Go
- `/var/lib/mysql` : 15 Go
- `/home` : 5 Go

2.2 Logiciel

- Debian 13
- Apache2
- MariaDB ≥ 10.11
- PHP 8.4 (version plus récente et compatible GLPI 11)
- Extensions PHP requises :
  - mysqli, curl, gd, intl, ldap, zip, mbstring, xml, bz2

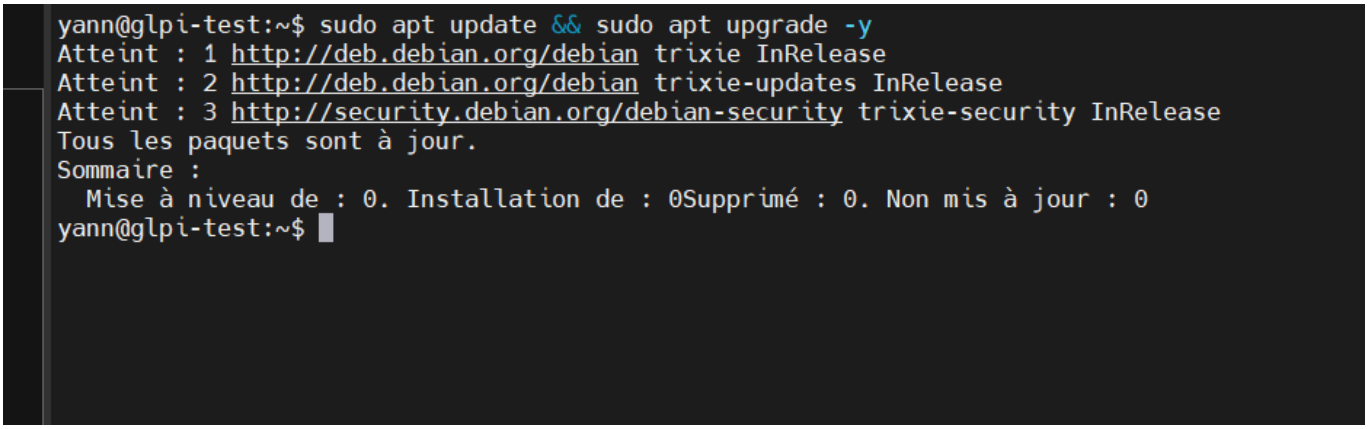
2.3 Réseau et flux

- IP fixe
- DNS fonctionnel
- Ports :
  - 22 (SSH)
  - 443 (HTTPS)
  - 636 (LDAPS)
  - 587 (SMTP)
  - 161 (SNMP)

3. Préparation du serveur Debian 13

3.1 Mise à jour

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



4. Installation de la stack LAMP

4.1 Installation Apache, PHP-FPM et MariaDB

```
sudo apt install apache2 php8.4-fpm mariadb-server
```

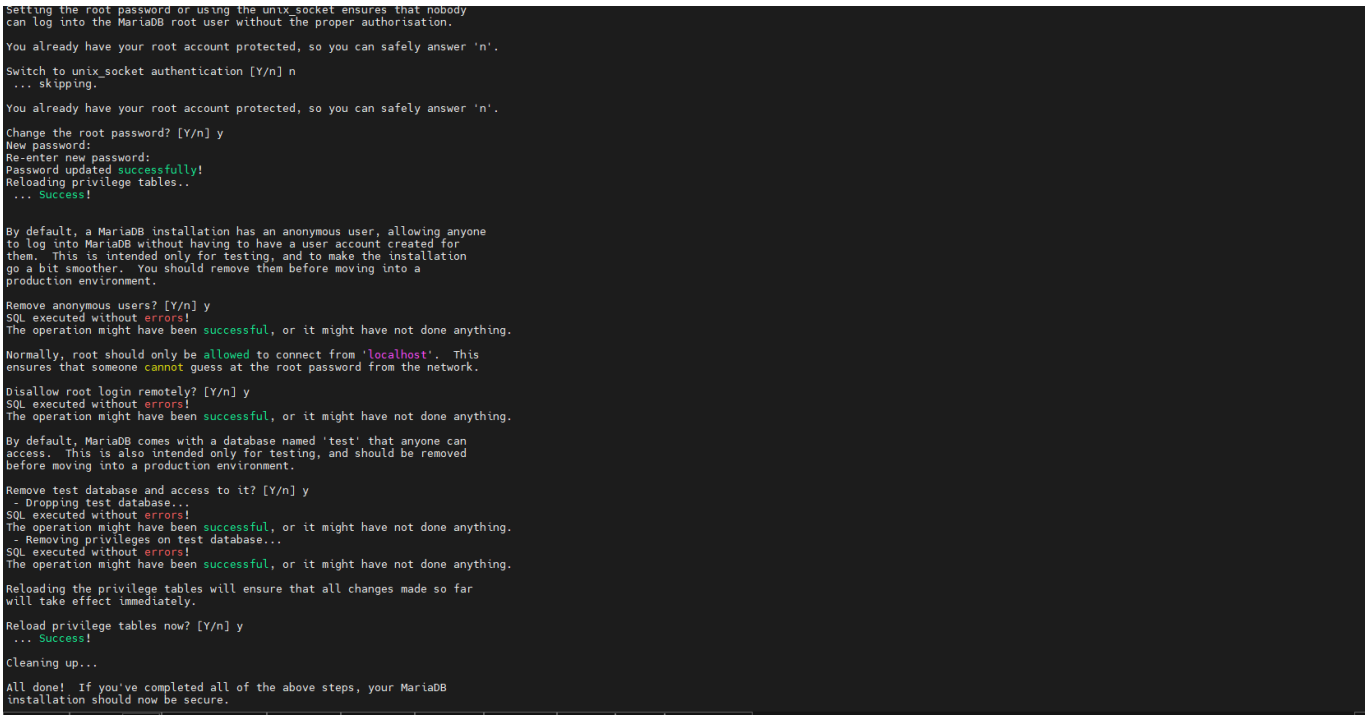
4.2 Installation des extensions PHP

```
sudo apt install php8.4-{curl,gd,intl,mysql,zip,bcmath,mbstring,xml,bz2,ldap}
```

5. Préparation de MariaDB

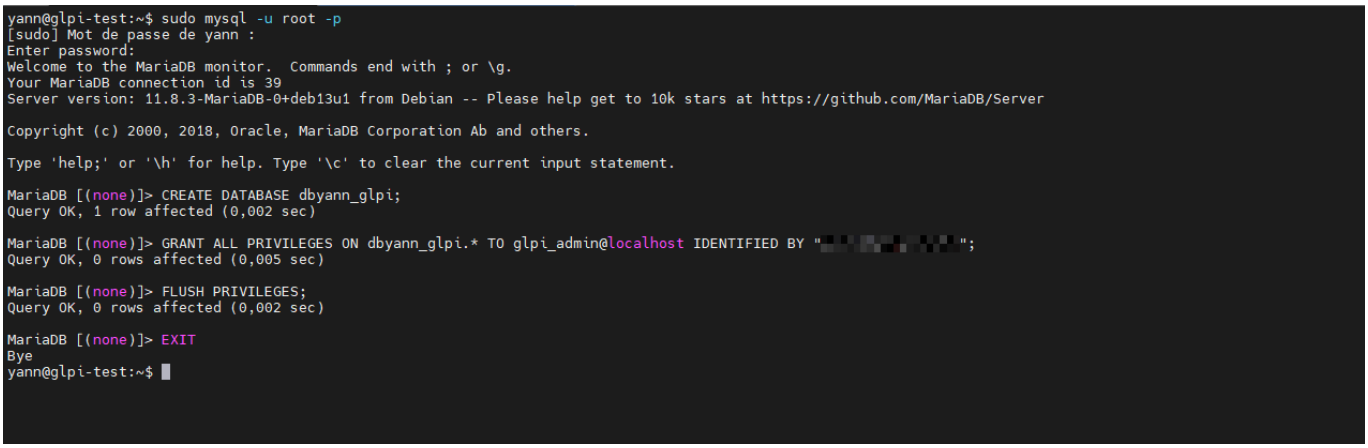
5.1 Sécurisation

```
sudo mariadb-secure-installation
```



5.2 Création de la base GLPI

```
CREATE DATABASE dbyann_glpi;
GRANT ALL PRIVILEGES ON dbyann_glpi.* TO glpi_admin@localhost IDENTIFIED BY
'Monmotdepasse';
FLUSH PRIVILEGES;
EXIT;
```



6. Téléchargement et préparation de GLPI

6.1 Téléchargement

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/11.0.4/glpi-11.0.4.tgz
sudo tar -xzvf glpi-11.0.4.tgz -C /var/www/
```

6.2 Préparation des répertoires et permissions

```
# 1. Création des répertoires
sudo mkdir -p /etc/glpi /var/lib/glpi /var/log/glpi

# 2. Déplacement AVANT permissions
sudo mv /var/www/glpi/config /etc/glpi/
sudo mv /var/www/glpi/files /var/lib/glpi/

# 3. Créer fichiers de configuration :
sudo nano /var/www/glpi/inc/downstream.php
```

```
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
    require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```

```
sudo nano /etc/glpi/local_define.php
```

```
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
```

```
define('GLPI_LOG_DIR', '/var/log/glpi');
```

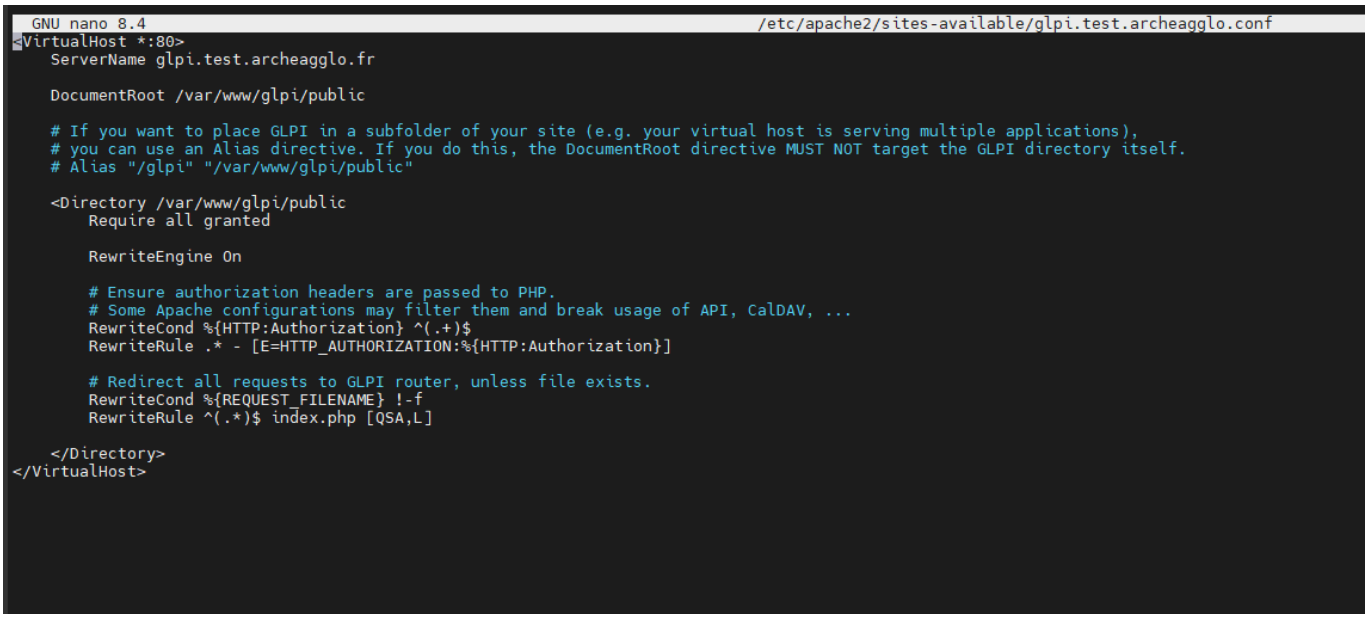
```
# 4. Permissions finales (récursives)
sudo chown -R www-data:www-data \
  /var/www/glpi \
  /etc/glpi \
  /var/lib/glpi \
  /var/log/glpi

sudo chmod -R 750 \
  /var/www/glpi \
  /etc/glpi \
  /var/lib/glpi \
  /var/log/glpi
```

7. Configuration Apache pour GLPI

7.1 VirtualHost complet

```
sudo nano /etc/apache2/sites-available/glpi_test.archeagglo.fr.conf
```

```
<VirtualHost *:80>
    ServerName glpi_test.archeagglo.fr

    DocumentRoot /var/www/glpi/public

    # Alias optionnel
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
```



7.2 Activation et redémarrage

```
sudo a2ensite glpi_test.archeagglo.fr.conf
sudo a2dissite 000-default.conf
sudo a2enmod rewrite proxy_fcgi setenvif
sudo systemctl restart apache2
```

8. Configuration PHP-FPM

L'utilisation de PHP-FPM permet une meilleure gestion des processus PHP, améliore les performances et renforce la sécurité en séparant l'exécution PHP du serveur Apache

8.1 Configuration PHP-FPM

Éditer le fichier de configuration PHP :

```
sudo nano /etc/php/8.4/fpm/php.ini
```

Paramètres de sécurité recommandés :

```
session.cookie_httponly = on
session.cookie_samesite = Lax
```

Ces paramètres permettent :

- de protéger les cookies de session contre les accès JavaScript,
- de limiter les attaques de type CSRF,
- de renforcer la sécurité des sessions utilisateurs.

Redémarrer le service PHP-FPM afin d'appliquer les modifications :

```
; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; https://php.net/session.cookie-httponly
session.cookie_httponly = on

; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF/XSRF)
; Current valid values are "Strict", "Lax" or "None". When using "None",
; make sure to include the quotes, as `none` is interpreted like `false` in ini files.
; https://tools.ietf.org/html/draft-west-first-party-cookies-07
session.cookie_samesite = Lax
```

Redémarrage PHP-FPM :

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

8.2 Liaison Apache ↔ PHP-FPM

Afin qu'Apache transmette l'exécution des fichiers PHP à PHP-FPM, il est nécessaire de configurer le VirtualHost GLPI.

Éditer le fichier du VirtualHost :

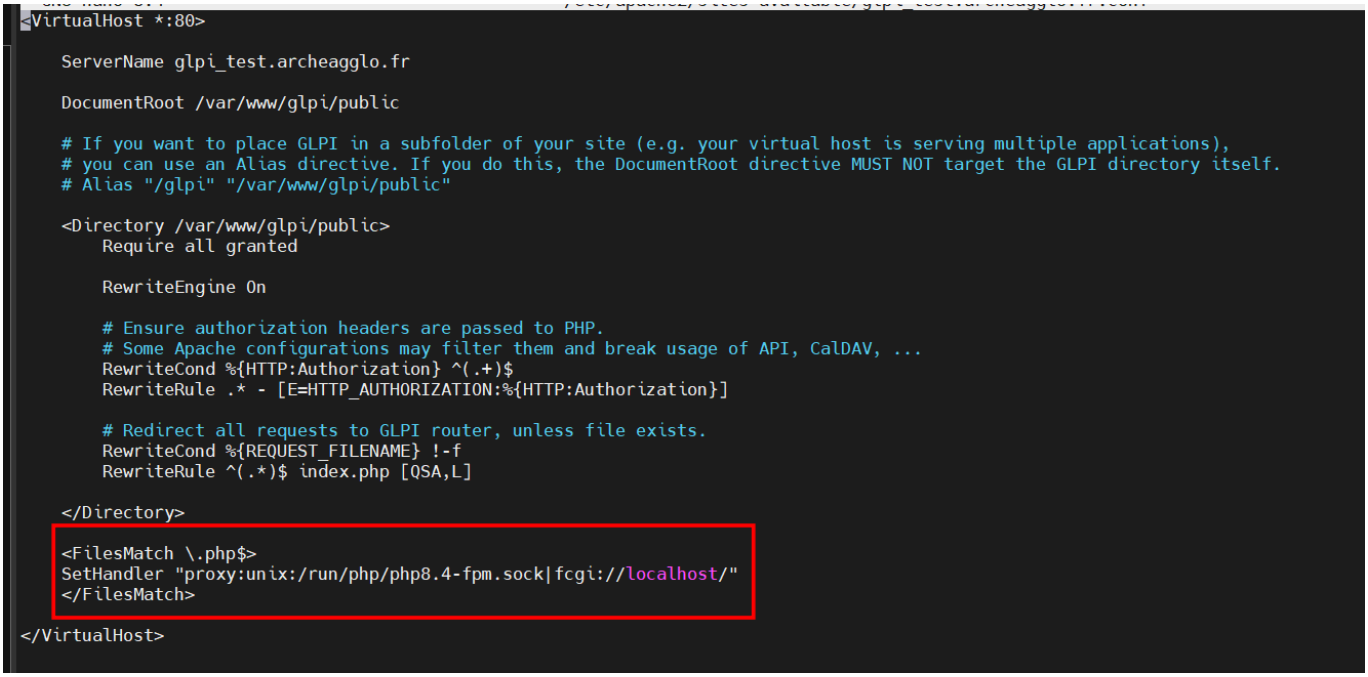
```
sudo nano /etc/apache2/sites-available/glpi_test.archeagglo.fr.conf
```

Ajouter la directive suivante à l'intérieur du VirtualHost :

```
<FilesMatch \.php$>
    SetHandler "proxy:unix:/run/php/php8.4-fpm.sock|fcgi://localhost/"
</FilesMatch>
```

Cette configuration indique à Apache :

- d'utiliser le socket PHP-FPM dédié,
- de déléguer l'exécution des scripts PHP à PHP-FPM



```
<VirtualHost *:80>

    ServerName glpi_test.archeagglo.fr

    DocumentRoot /var/www/glpi/public

    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple applications),
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the GLPI directory itself.
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        # Ensure authorization headers are passed to PHP.
        # Some Apache configurations may filter them and break usage of API, CalDAV, ...
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

        # Redirect all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]

    </Directory>

    <FilesMatch \.php$>
    SetHandler "proxy:unix:/run/php/php8.4-fpm.sock|fcgi://localhost/"
    </FilesMatch>

</VirtualHost>
```

Activer les modules nécessaires si ce n'est pas déjà fait :

```
sudo a2enmod proxy_fcgi setenvif
```

(Si ce n'est pas déjà fait à l'étape précédente)

Le module setenvif est requis pour la gestion correcte des variables d'environnement HTTP, notamment pour l'authentification et certaines fonctionnalités applicatives de GLPI

Redémarrer Apache pour appliquer la configuration :

```
sudo systemctl restart apache2
```

8.3 Validation du fonctionnement PHP-FPM

Le bon fonctionnement de PHP-FPM est validé par :

- l'accès fonctionnel à l'interface GLPI,
- l'absence d'erreurs PHP dans les journaux Apache et PHP-FPM,
- l'exécution correcte des pages dynamiques.

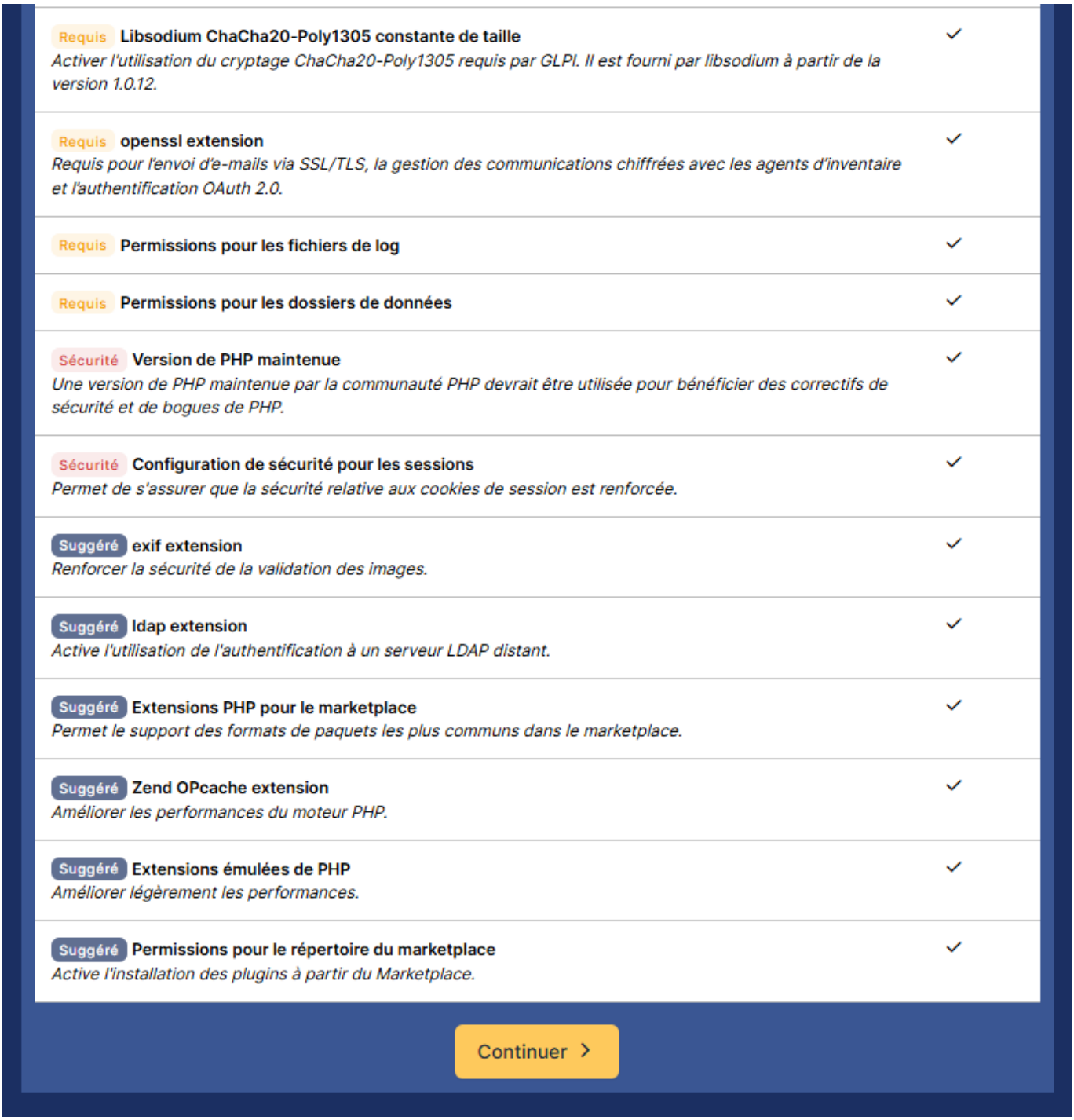
Cette configuration garantit une exécution PHP performante, sécurisée et conforme aux bonnes pratiques pour un environnement GLPI.

9. Installation via l'interface web

- Vérifier prérequis
- Configurer BDD `dbyann_glpi` / utilisateur `glpi_admin`
- Créer compte administrateur
- Supprimer `/install`

```
sudo rm /var/www/glpi/install/install.php
```


GLPI Installation
Étape 0
Vérification de la compatibilité de votre environnement avec l'exécution de GLPI
TESTS EFFECTUÉS
RÉSULTATS
Requis Parser PHP
Requis Taille d'entier maximal de PHP
Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).
Requis Configuration des sessions
Requis Mémoire allouée
Requis Extensions du noyau de PHP
Requis mysqli extension
Requis pour l'accès à la base de données.
Requis curl extension
Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).
Requis gd extension
Requis pour le traitement des images.
Requis intl extension
Requis pour l'internationalisation.
Requis mbstring extension
Requis pour la prise en charge des caractères multioctets et la conversion de jeu de caractères.
Requis zlib extension
Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.
Requis bcmath extension
Requis pour la prise en charge des QR codes.


Requis Libsodium ChaCha20-Poly1305 constante de taille
Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.
Requis openssl extension
Requis pour l'envoi d'e-mails via SSL/TLS, la gestion des communications chiffrées avec les agents d'inventaire et l'authentification OAuth 2.0.
Requis Permissions pour les fichiers de log
Requis Permissions pour les dossiers de données
Sécurité Version de PHP maintenue
Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.
Sécurité Configuration de sécurité pour les sessions
Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.
Suggéré exif extension
Renforcer la sécurité de la validation des images.
Suggéré ldap extension
Active l'utilisation de l'authentification à un serveur LDAP distant.
Suggéré Extensions PHP pour le marketplace
Permet le support des formats de paquets les plus communs dans le marketplace.
Suggéré Zend OPcache extension
Améliorer les performances du moteur PHP.
Suggéré Extensions émulées de PHP
Améliorer légèrement les performances.
Suggéré Permissions pour le répertoire du marketplace
Active l'installation des plugins à partir du Marketplace.
Continuer


GLPI Installation
Étape 1
Configuration de la connexion à la base de données
Serveur SQL (MariaDB ou MySQL)
Utilisateur SQL
Mot de passe SQL
Continuer

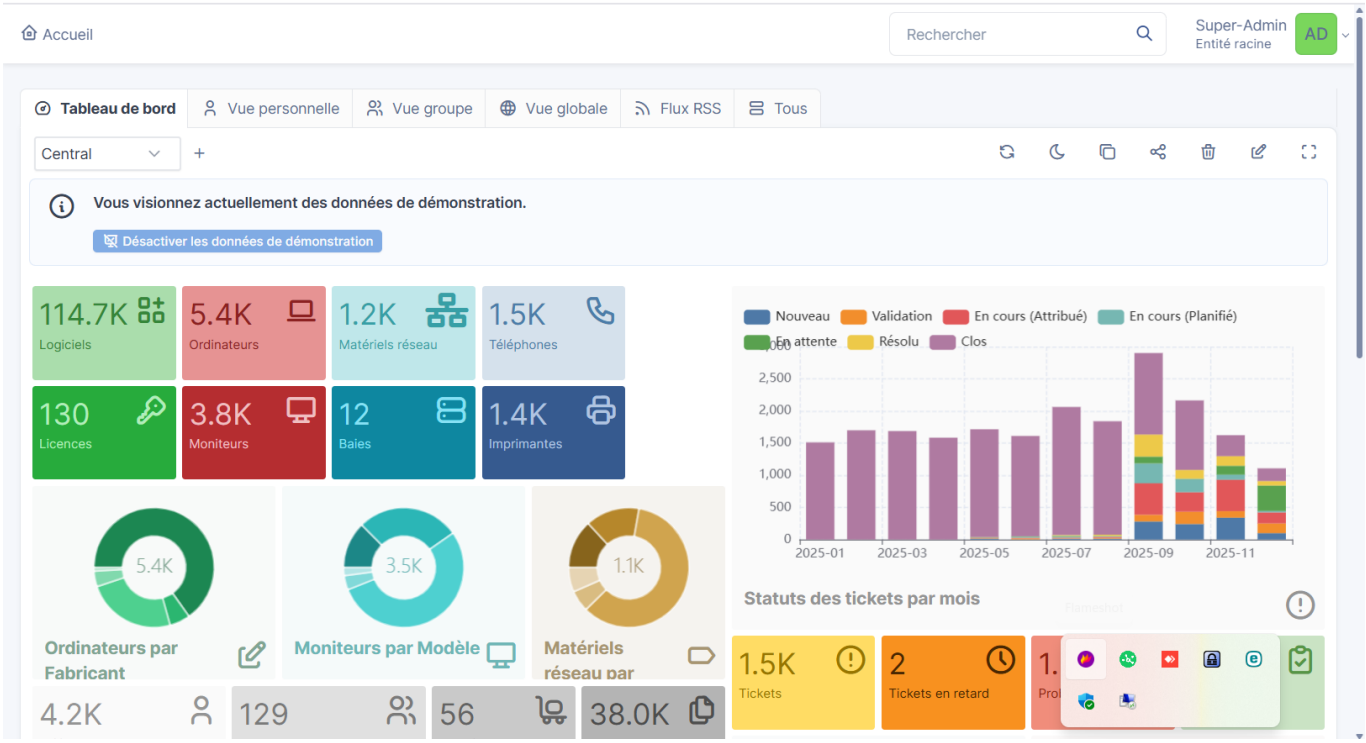

GLPI Installation
Étape 1
Configuration de la connexion à la base de données
Serveur SQL (MariaDB ou MySQL)
localhost
Utilisateur SQL
glpi_admin
Mot de passe SQL
Continuer


GLPI Installation
Étape 2
Test de connexion à la base de données
Connexion à la base de données réussie
Veuillez sélectionner une base de données :
CRÉER UNE NOUVELLE BASE DE DONNÉES :
OU UTILISER UNE BASE EXISTANTE :
dbyann_glpi
Continuer


GLPI Installation
Étape 3
Initialisation de la base de données.
Initialisation des tables de la base de données avec ses données par défaut...
100 %
Structure de la base de données créée.
Données par défaut importées.
Formulaires par défaut créés.
Règles par défaut initialisées.
Clefs de sécurités générées.
Paramètres par défaut définis.
Installation terminée.
Continuer


GLPI Installation
Étape 4
Récolter des données
Envoyer "statistiques d'usage"
Nous avons besoin de vous pour améliorer GLPI et son écosystème de plugins !
Depuis GLPI 9.2, nous avons introduit une nouvelle fonctionnalité de statistiques appelée "Télémétrie", qui envoie anonymement, avec votre permission, des données à notre site de télémétrie.
Une fois envoyées, les statistiques d'usage sont agrégées et rendues disponibles à une large audience de développeurs GLPI.
Dites-nous comment vous utilisez GLPI pour que nous améliorons GLPI et ses plugins !
Voir ce qui serait envoyé...
Référencez votre GLPI
Par ailleurs, si vous appréciez GLPI et sa communauté, prenez une minute pour référencer votre organisation en remplissant le formulaire suivant
Le formulaire d'inscription
Continuer >


GLPI Installation
Étape 5
Une dernière chose avant de démarrer
Vous souhaitez obtenir de l'aide pour intégrer GLPI dans votre SI, faire corriger un bug ou bénéficier de règles ou dictionnaires pré-configurés ?
Nous mettons à votre disposition l'espace https://services.glpi-network.com.
GLPI-Network est un service commercial qui comprend une souscription au support niveau 3, garantissant la correction des bugs rencontrés avec un engagement de délai.
Sur ce même espace, vous pourrez contacter un partenaire officiel pour vous aider dans votre intégration de GLPI.
Continuer >



10. Sécurisation post-installation

- HTTPS (Let's Encrypt en production) Pour ce test, un certificat SSL auto-signé a été utilisé afin de sécuriser l'accès en HTTPS à GLPI. Ce type de certificat n'est pas reconnu par défaut par les navigateurs. Il est donc adapté pour un environnement de test.

Pour un usage en production, il est recommandé d'utiliser un certificat signé par une autorité de certification reconnue afin d'éviter les alertes de sécurité dans les navigateurs

```
  GNU nano 8.4                                                    /etc/apache2/sites-available/gl
# VirtualHost HTTP → Redirection HTTPS

<VirtualHost *:80>
    ServerName glpi_test.archeagglo.fr

    # Redirection forcée vers HTTPS
    Redirect permanent / https://glpi_test.archeagglo.fr/
</VirtualHost>



# VirtualHost HTTPS

<VirtualHost *:443>
    ServerName glpi_test.archeagglo.fr
    DocumentRoot /var/www/glpi/public

    # SSL auto-signé (environnement de test)
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/glpi.crt
    SSLCertificateKeyFile /etc/ssl/private/glpi.key

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        # Transmission des headers Authorization (API, LDAP, etc.)
        RewriteCond %{HTTP:Authorization} ^(.+)$
        RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

        # Redirection vers le routeur GLPI si le fichier n'existe pas
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

    # PHP-FPM via socket
    <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.4-fpm.sock|fcgi://localhost/"
    </FilesMatch>

    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

- SSH restreint / clé
- Fail2ban
- Mises à jour régulières

11. Sauvegardes et PRA

- Dump quotidien MariaDB
- Backup répertoires `/etc/glpi` et `/var/lib/glpi`
- Snapshots VM Proxmox
- Rétention 30 jours
- Stratégie 3-2-1 (3 Sauvegardes, 2 supports différents dont 1 hors site)

12. Tests et validation

Cette section décrit les tests réalisés afin de valider le bon fonctionnement de la plateforme GLPI déployée dans l'environnement de test

12.1 Vérifier accès HTTPS

Objectif :

S'assurer que l'application GLPI est accessible de manière sécurisée via HTTPS.

Actions réalisées :

- Mise en place d'un certificat SSL auto-signé
- Configuration Apache avec redirection HTTPS
- Test d'accès via navigateur et commande `curl`

Résultat :

- Accès HTTPS fonctionnel
- Certificat fonctionnel (auto-signé, accepté dans le cadre de l'environnement de test)
- Communication chiffrée confirmée

Statut : validé

12.2 Authentification LDAP

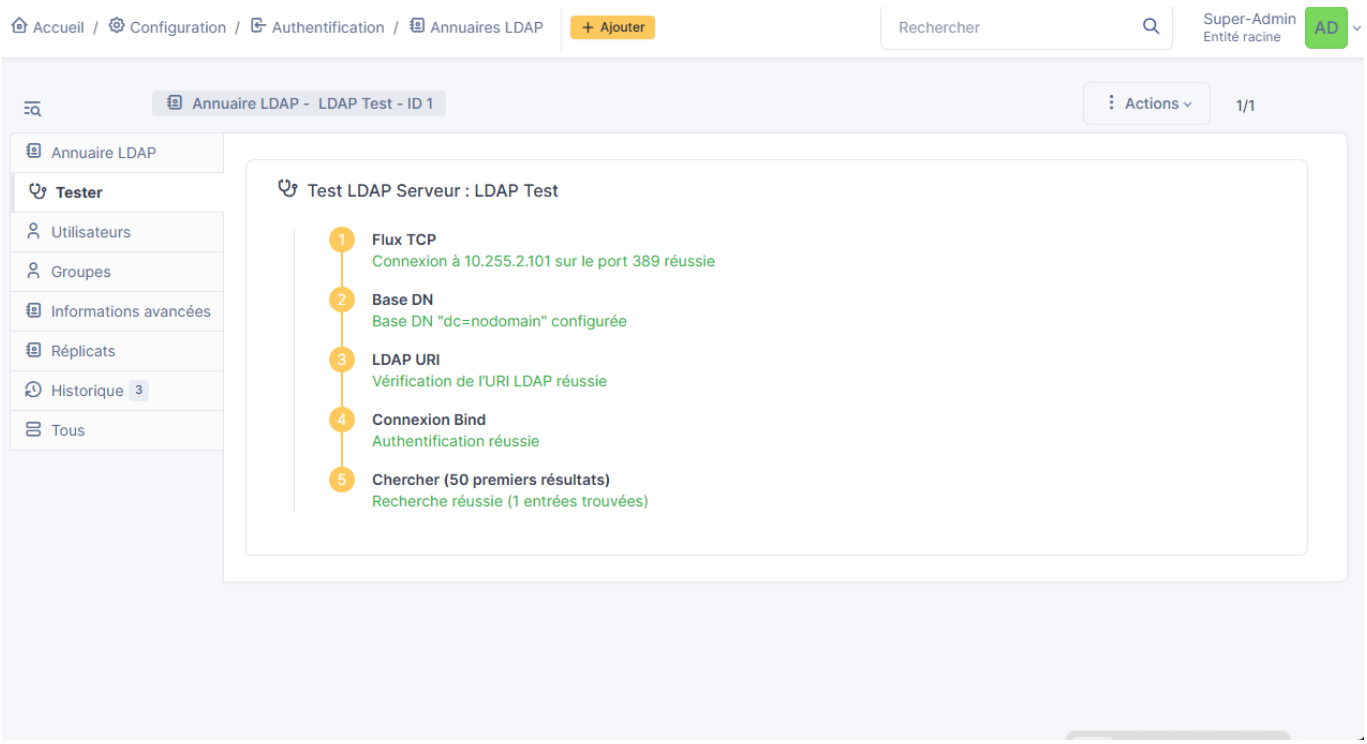
Objectif :
Valider l'authentification des utilisateurs via un annuaire LDAP.

Actions réalisées :

- Configuration du serveur LDAP dans GLPI
- Création d'un utilisateur LDAP de test
- Test d'authentification depuis l'interface GLPI

Résultat :

- Connexion LDAP réussie
- Synchronisation correcte des comptes utilisateurs



Statut : validé

12.3 Envoi notifications SMTP

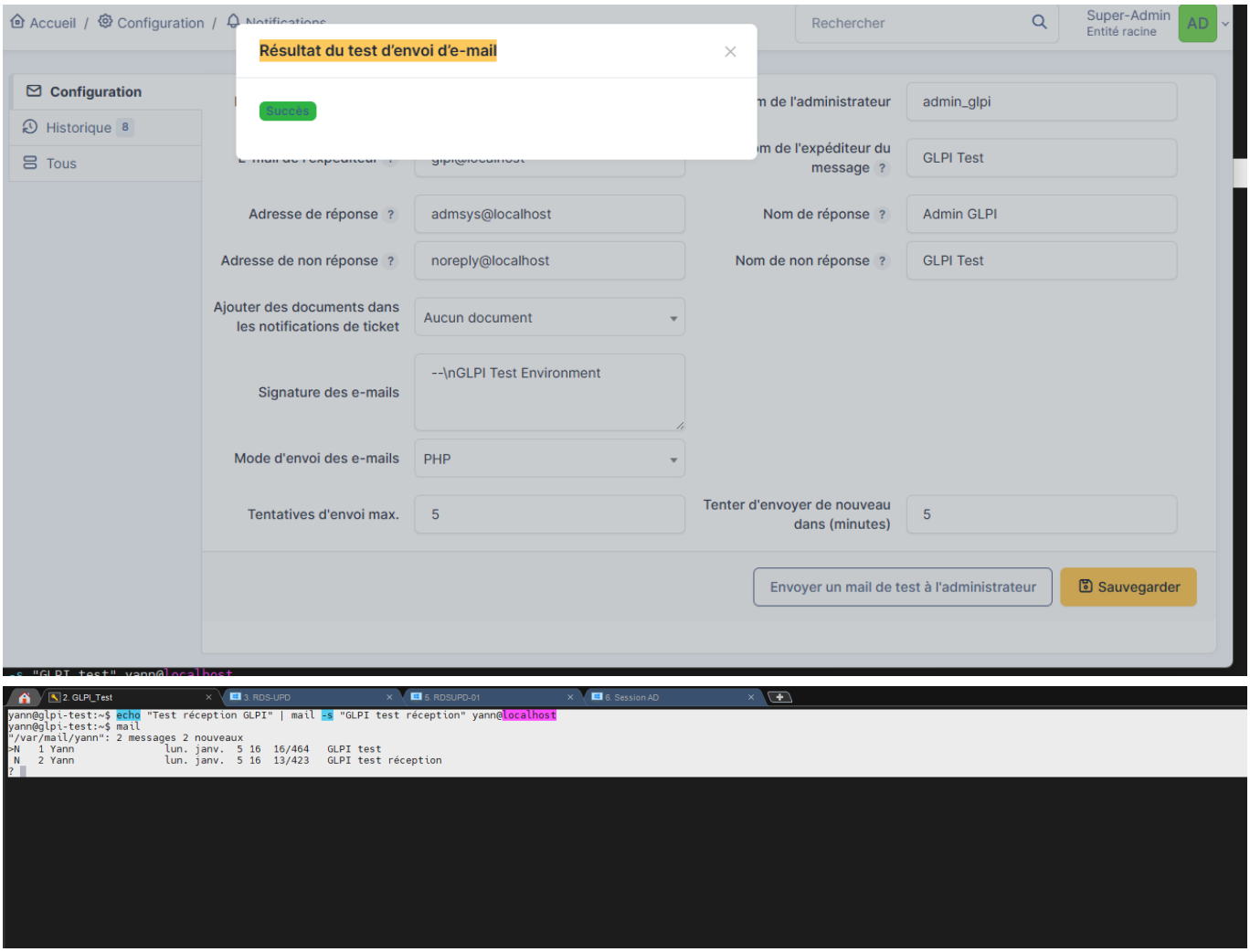
Objectif :
Vérifier l'envoi et la réception des notifications par e-mail depuis GLPI.

Actions réalisées :

- Configuration du service de messagerie local
- Paramétrage des notifications GLPI
- Test d'envoi depuis l'interface GLPI
- Test de réception via la commande `mail`

Résultat :

- Envoi d'e-mails fonctionnel
- Réception des messages confirmée



Statut : validé

12.4 Création et gestion tickets

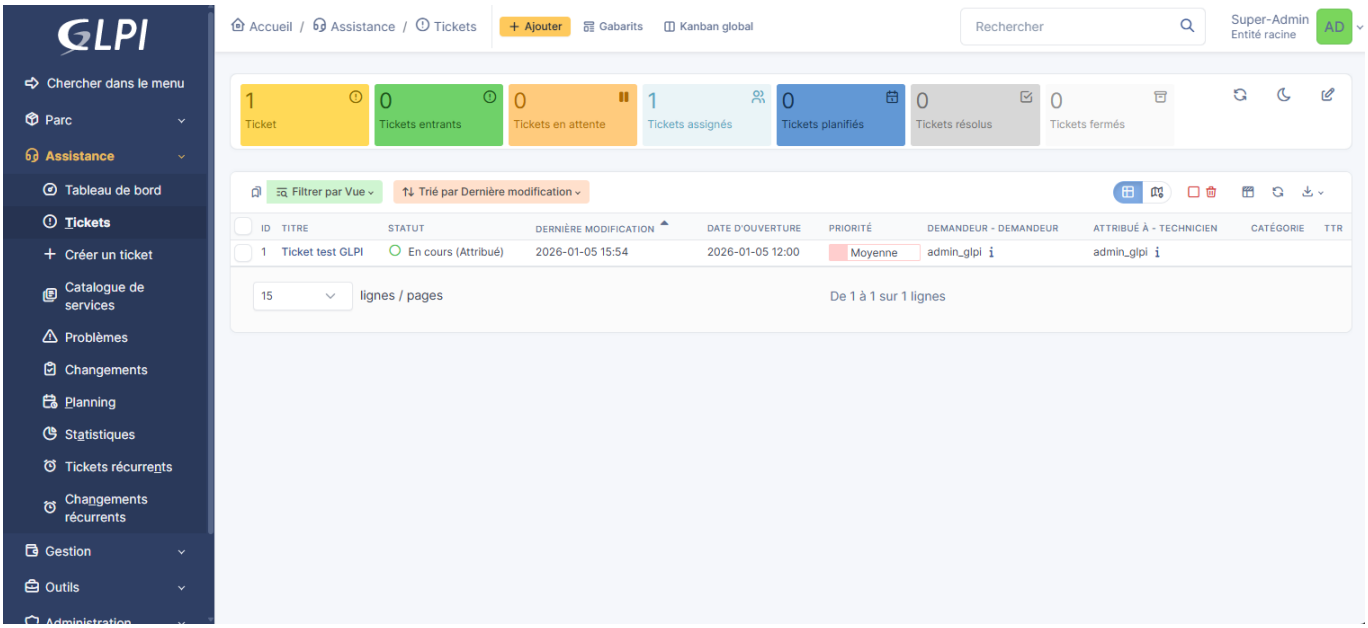
Objectif :
Valider le fonctionnement du module helpdesk

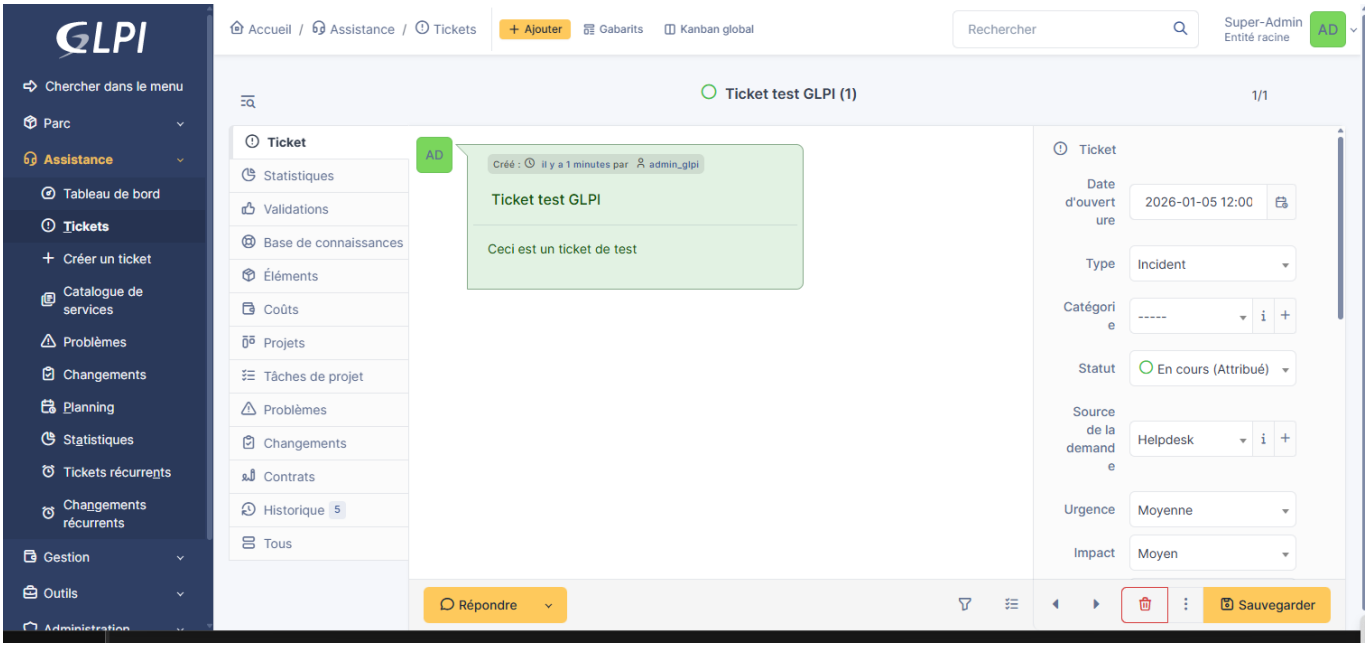
Actions réalisées :

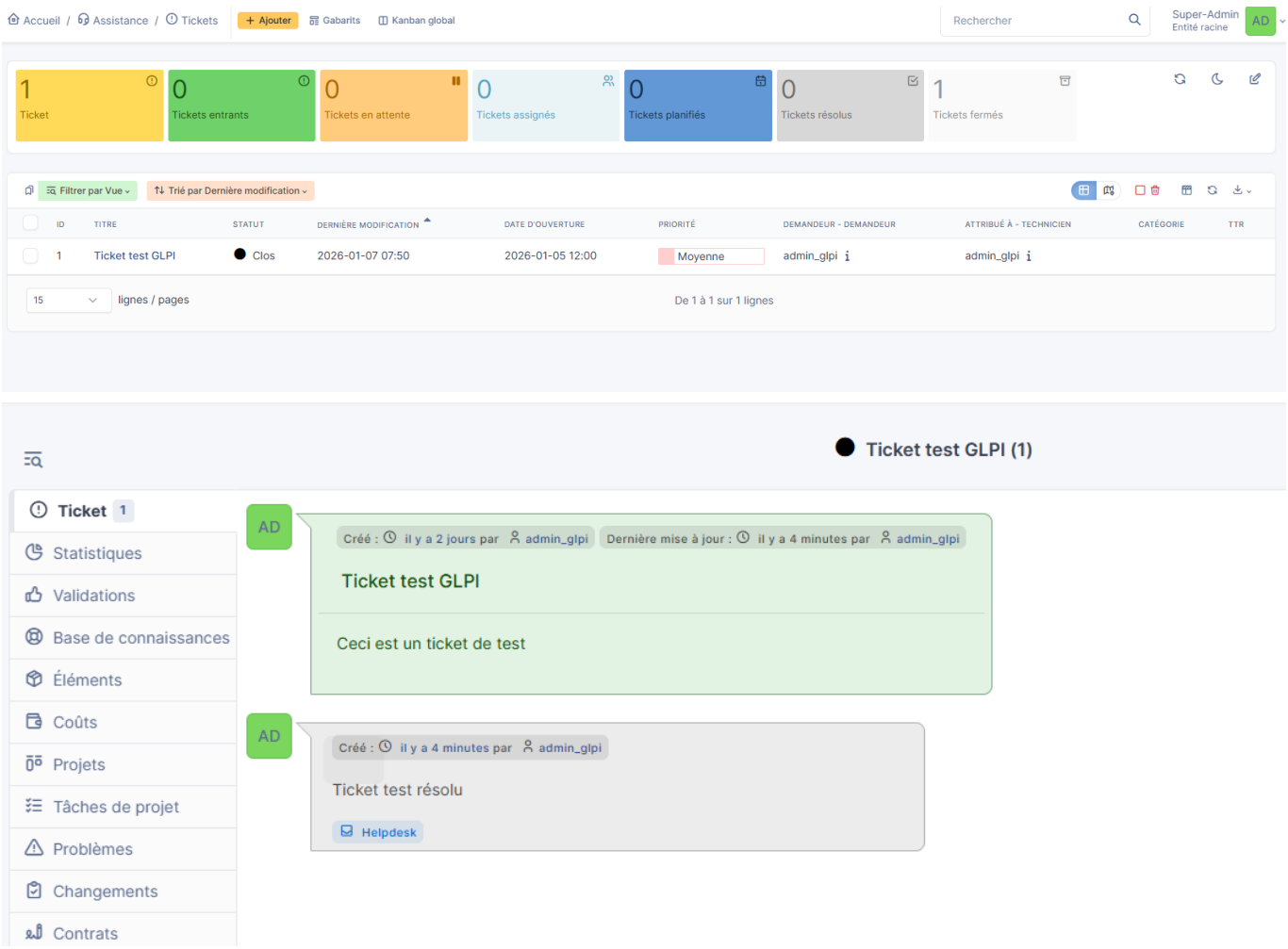
- Création de tickets depuis un compte utilisateur
- Attribution à un technicien
- Changement de statut
- Ajout de commentaires

Résultat :

- Cycle de vie des tickets fonctionnel
- Notifications associées envoyées correctement


GLPI
Chercher dans le menu
Parc
Assistance
Tableau de bord
Tickets
Créer un ticket
Catalogue de services
Problèmes
Changements
Planning
Statistiques
Tickets récurrents
Changements récurrents
Gestion
Outils
Accueil / Assistance / Tickets
+ Ajouter
Gabarits
Kanban global
Rechercher
Super-Admin
Entité racine
AD
1 Ticket
0 Tickets entrants
0 Tickets en attente
1 Tickets assignés
0 Tickets planifiés
0 Tickets résolus
0 Tickets fermés
Filtrer par Vue
Trié par Dernière modification
ID TITRE STATUT DERNIÈRE MODIFICATION DATE D'OUVERTURE PRIORITÉ DEMANDEUR - DEMANDEUR ATTRIBUÉ À - TECHNICIEN CATÉGORIE TTR
1 Ticket test GLPI En cours (Attribué) 2026-01-05 15:54 2026-01-05 12:00 Moyenne admin_glpi admin_glpi
15 lignes / pages
De 1 à 1 sur 1 lignes


GLPI
Chercher dans le menu
Parc
Assistance
Tableau de bord
Tickets
Créer un ticket
Catalogue de services
Problèmes
Changements
Planning
Statistiques
Tickets récurrents
Changements récurrents
Gestion
Outils
Accueil / Assistance / Tickets
+ Ajouter
Gabarits
Kanban global
Rechercher
Super-Admin
Entité racine
AD
Ticket test GLPI (1)
1/1
Ticket
Statistiques
Validations
Base de connaissances
Éléments
Coûts
Projets
Tâches de projet
Problèmes
Changements
Contrats
Historique 5
Tous
Créé : il y a 1 minutes par admin_glpi
Ticket test GLPI
Ceci est un ticket de test
Ticket
Date d'ouverture 2026-01-05 12:00
Type Incident
Catégorie -----
Statut En cours (Attribué)
Source de la demande Helpdesk
Urgence Moyenne
Impact Moyen
Répondre
Sauvegarder



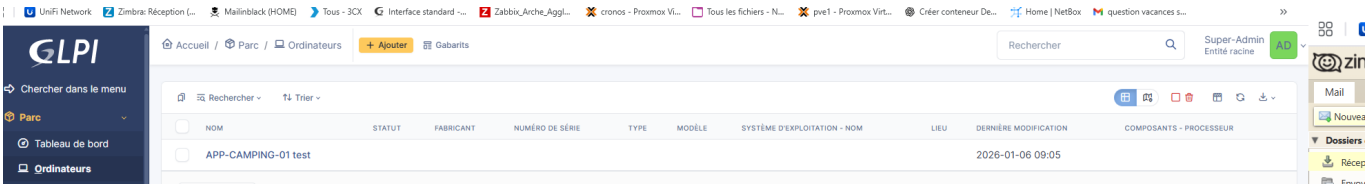
Statut : validé

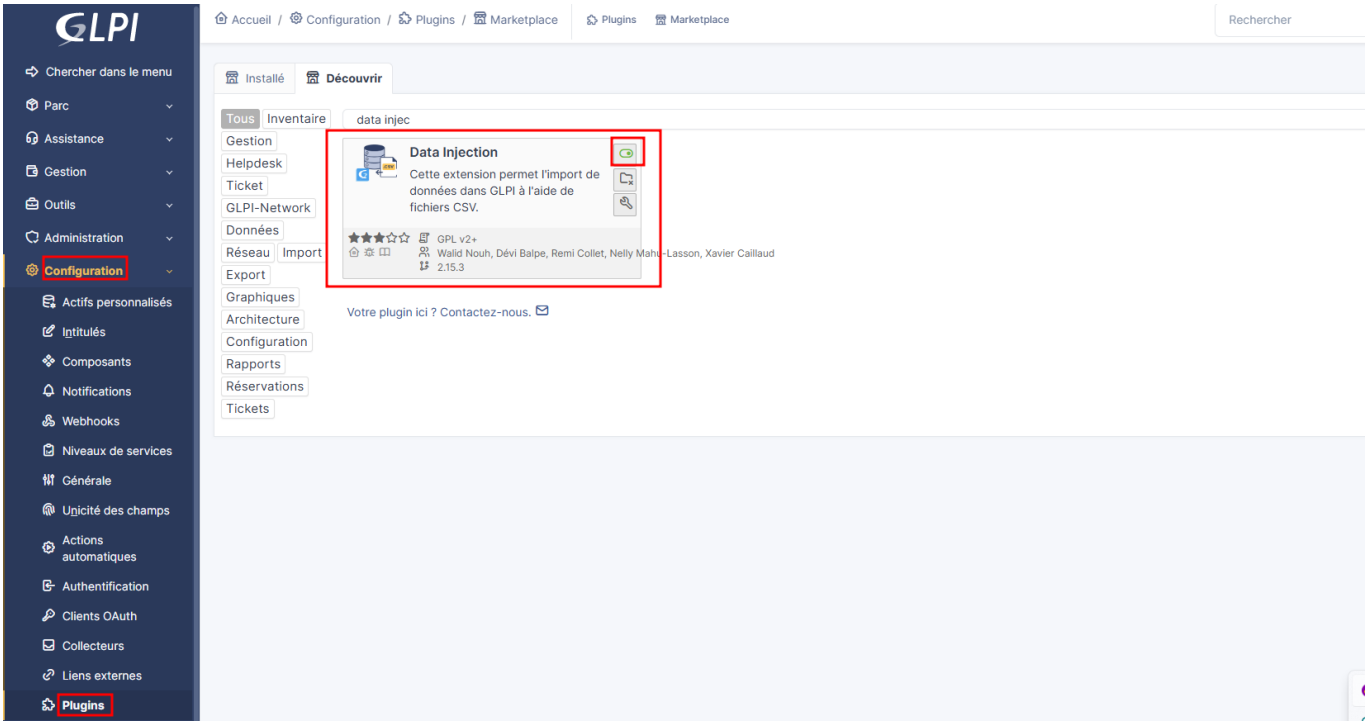
12.5 Ajout d'équipements et gestion des utilisateurs

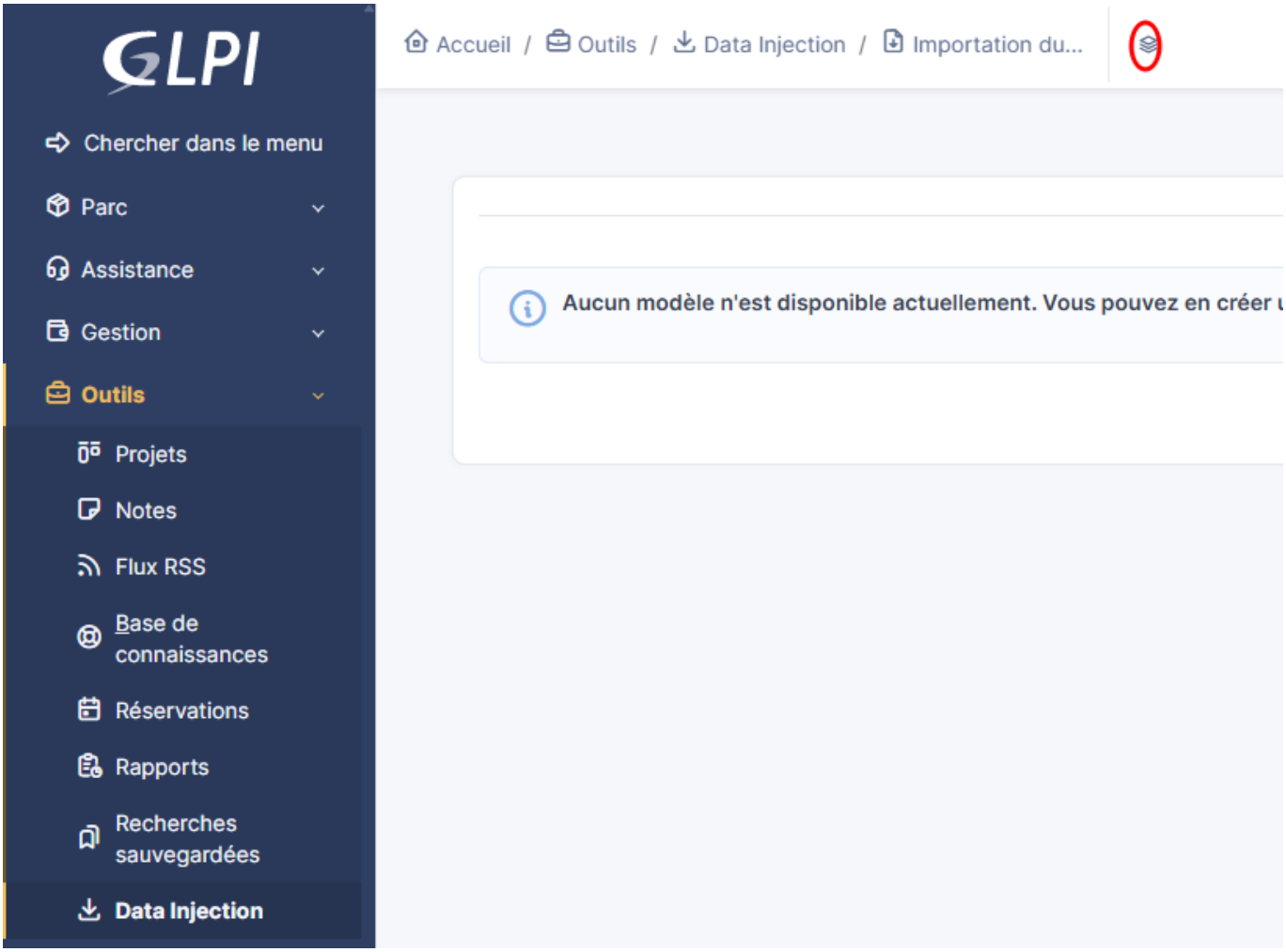
La fonctionnalité de gestion du parc a été testée par l'ajout manuel d'un équipement depuis l'interface GLPI. L'équipement créé est correctement enregistré et visible dans l'inventaire, confirmant le bon fonctionnement du module de gestion des matériels.

La gestion des utilisateurs a également été validée par un import au format CSV. Cet import permet la création en masse de comptes utilisateurs. Le test s'est déroulé avec succès et les utilisateurs importés sont correctement accessibles et exploitables dans l'application.

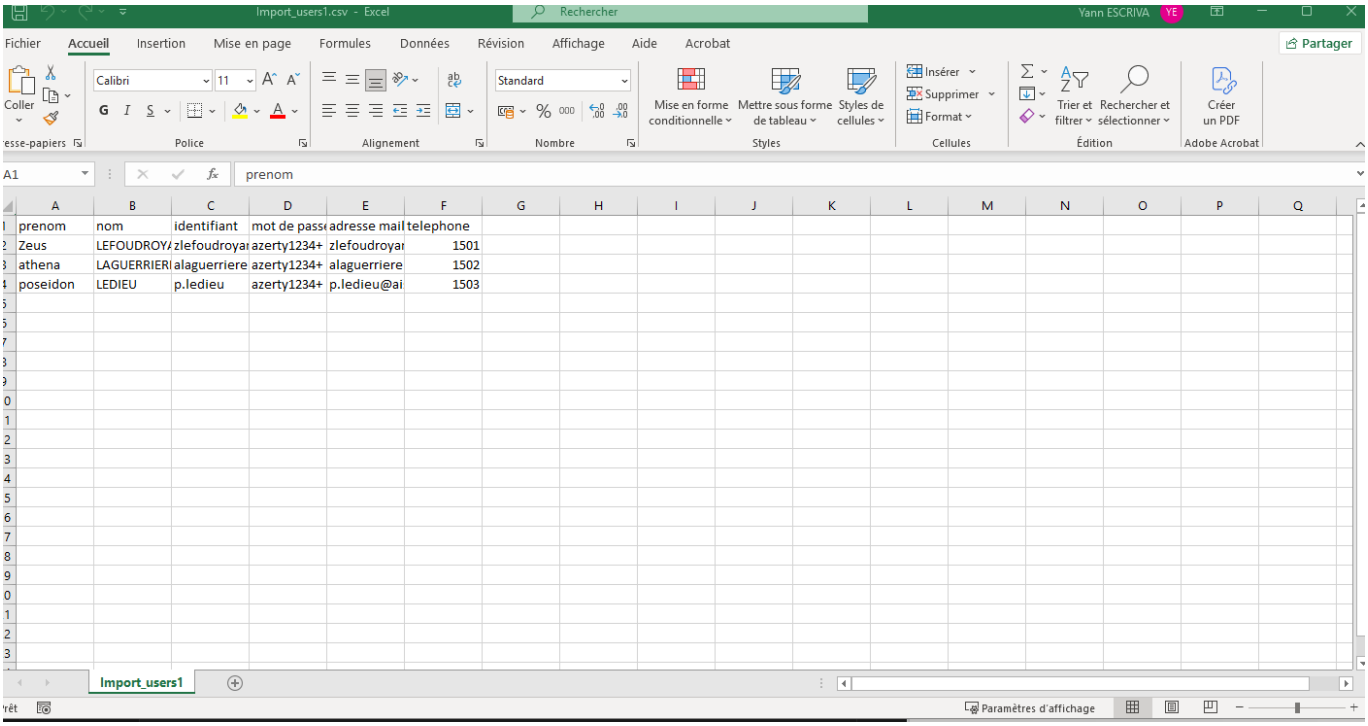
Ces tests confirment la capacité de la solution à gérer un parc informatique et des comptes utilisateurs, aussi bien en création unitaire qu'en import groupé.

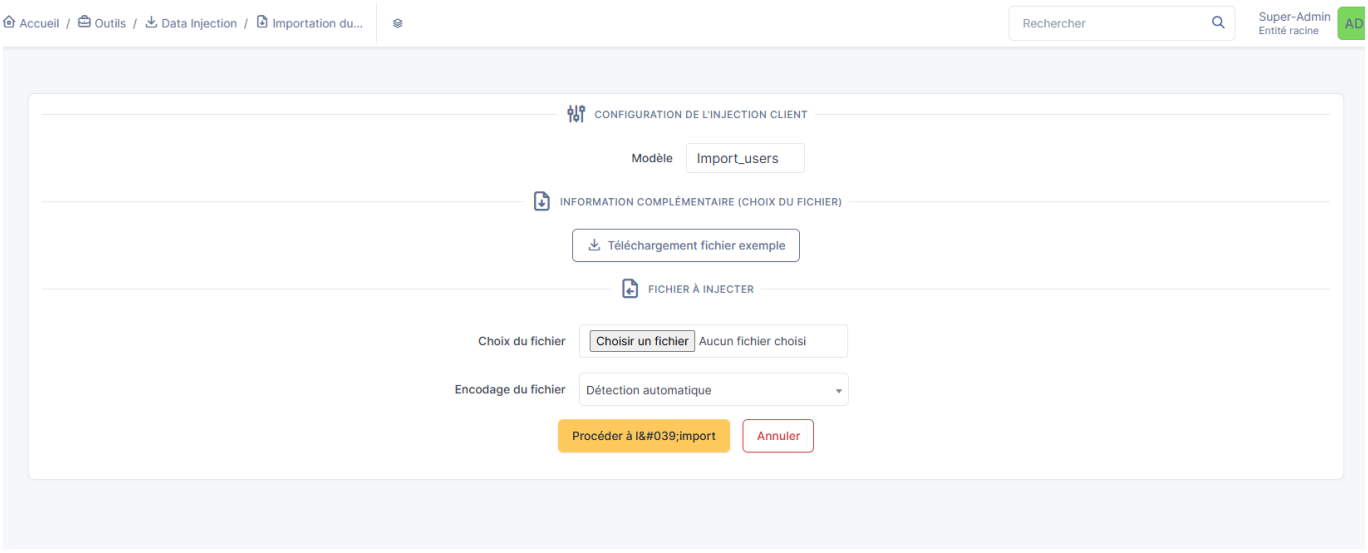


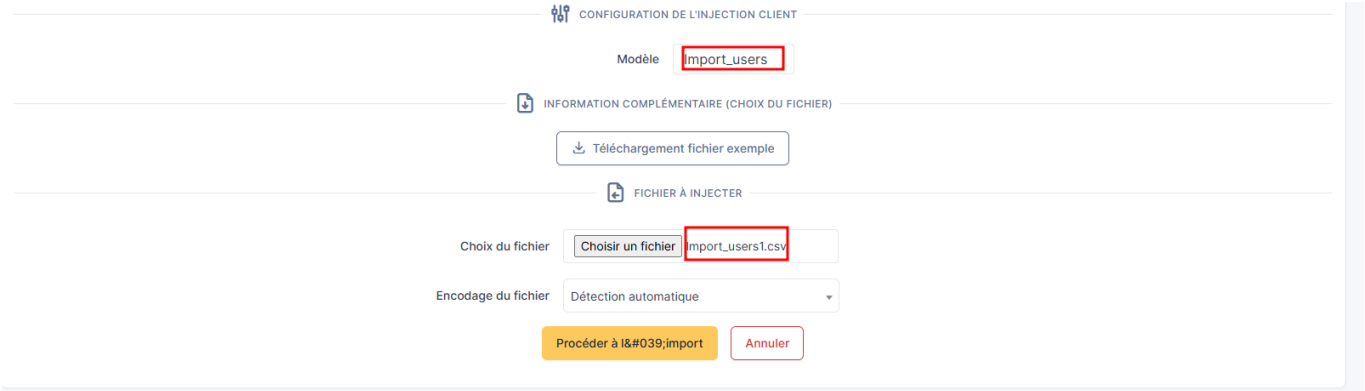


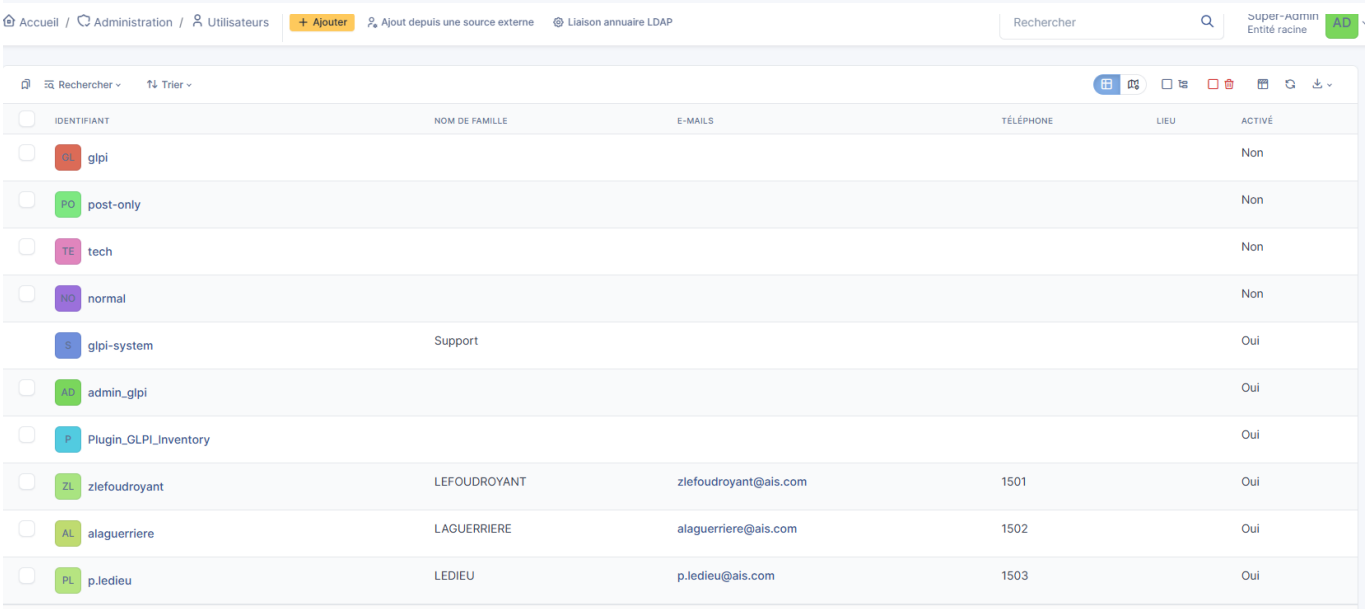


alt text alt text alt text alt text


Import_users1.csv - Excel
Rechercher
Yann ESCRIVA
Fichier
Accueil
Insertion
Mise en page
Formules
Données
Révision
Affichage
Aide
Acrobat
Partager
Coller
Calibri
11
Standard
Mise en forme conditionnelle
Mettre sous forme de tableau
Styles de cellules
Insérer
Supprimer
Format
Trier et filtrer
Rechercher et sélectionner
Créer un PDF
Police
Alignement
Nombre
Styles
Cellules
Édition
Adobe Acrobat
A1
prenom
nom
identifiant
mot de passe
adresse mail
telephone
Zeus
LEFOUDROYA
zlefoudroyar
azerty1234+
zlefoudroyar
1501
athena
LAGUERRIER
alaguerriere
azerty1234+
alaguerriere
1502
poseidon
LEDIEU
p.ledieu
azerty1234+
p.ledieu@ai
1503
Import_users1
Paramètres d'affichage


Accueil / Outils / Data Injection / Importation du...
Rechercher
Super-Admin
Entité racine
CONFIGURATION DE L'INJECTION CLIENT
Modèle
Import_users
INFORMATION COMPLÉMENTAIRE (CHOIX DU FICHIER)
Téléchargement fichier exemple
FICHIER À INJECTER
Choix du fichier
Choisir un fichier
Aucun fichier choisi
Encodage du fichier
Détection automatique
Procéder à l'import
Annuler





Statut : validé

12.6 Sauvegardes restaurables

Objectif :
S'assurer que les données GLPI peuvent être sauvegardées et restaurées.

Actions réalisées :

J'ai effectué une sauvegarde de test : alt text

J'ai vérifié la présence de la sauvegarde ainsi que la cohérence de sa taille :

```
yann@glpi-test:~$ ls -lh glpi-backup-test.tgz
-rw-r--r-- 1 root root 784K  6 janv. 16:28 glpi-backup-test.tgz
yann@glpi-test:~$
```

Enfin, j'ai effectué un test de restauration de cette sauvegarde dans un dossier temporaire.

```
yann@glpi-test:~$ sudo mkdir -p /tmp/glpi_restore
[sudo] Mot de passe de yann :
yann@glpi-test:~$ sudo tar xzvf glpi-backup-test.tgz -C /tmp/glpi_restore
var/lib/glpi/
var/lib/glpi/files/
var/lib/glpi/files/_lock/
var/lib/glpi/files/_cache/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/5/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/5/SO7ot6cI19N8UBSmuxmw
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/+/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/+/VI75U-eFBrijFtyBET5Q
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/Z/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/Z/q59wNam+YeN1I9+Kgx4g
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/G/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/G/0E2gIJ+1NynFnzXWH+CA
tar: var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/G/0E2gIJ+1NynFnzXWH+CA : l'horodatage 2027-01-06 16:46:11 est situé 31479455.081274164 secondes dans le
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/M/
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/M/GwvsHGyg6O5xEELNqfoA
```

```
yann@glpi-test:~$ ls /tmp/glpi_restore
etc  var
yann@glpi-test:~$
```

Statut : validé

Ces tests valident la capacité de restauration des données GLPI en cas d'incident, conformément aux exigences du PRA

12.7 SSO : non implémenté (évolution prévue)

Objectif : Étudier la faisabilité d'une authentification centralisée.

État actuel :

Non implémenté

Justification : Cette évolution n'a pas été intégrée afin de préserver la stabilité et la simplicité de l'architecture

12.8 Conclusion des tests

L'ensemble des fonctionnalités essentielles de GLPI ont été testées et validées avec succès dans l'environnement de test.

La plateforme est :

- Fonctionnelle
- Sécurisée
- Conforme aux objectifs définis dans le DAT

13. Durcissement post-validation (FINAL)

Le durcissement de la plateforme est appliqué **après validation complète du bon fonctionnement de GLPI** (tests fonctionnels, accès HTTPS, LDAP, SMTP, sauvegardes).

Cette approche permet d'éviter tout blocage pendant les phases d'installation et de tests.

13.1 Durcissement du système Debian

Désactivation de la connexion SSH root

```
sudo nano /etc/ssh/sshd_config
```

```
PermitRootLogin no
PasswordAuthentication no
```

```
sudo systemctl restart ssh
```

Objectifs :

- empêcher les connexions directes avec le compte root
- réduire les risques de compromission par force brute
- imposer l'utilisation de comptes nominaux

Mise en place du pare-feu UFW

```
sudo apt install ufw -y
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

```
sudo ufw allow 22/tcp
sudo ufw allow 443/tcp
sudo ufw allow 636/tcp
sudo ufw allow 587/tcp
sudo ufw allow 161/udp
```

```
sudo ufw enable
```

Objectifs :

- limiter les flux réseau aux seuls services nécessaires
- réduire la surface d'attaque du serveur

Protection contre les attaques par force brute (Fail2ban)

```
sudo apt install fail2ban -y
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

Objectifs :

- bloquer automatiquement les tentatives de connexion abusives

- protéger les services SSH et Apache

13.2 Durcissement du serveur Apache

Masquage des informations serveur

```
sudo nano /etc/apache2/conf-available/security.conf
```

```
ServerTokens Prod
ServerSignature Off
```

```
sudo systemctl restart apache2
```

Objectifs :

- ne pas exposer la version d'Apache
- limiter les informations fournies aux clients et attaquants potentiels

13.3 Durcissement PHP / PHP-FPM

Masquage de la version PHP exposée aux clients

```
sudo nano /etc/php/8.4/fpm/php.ini
```

```
expose_php = Off
```

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

Objectif :

- Empêcher l'exposition de la version PHP dans les en-têtes HTTP
- Sécurisation des cookies de session

```
session.cookie_httponly = On
session.cookie_samesite = Lax
```

(rappel et durcissement final des paramètres PHP-FPM validés précédemment)

Objectifs :

- Empêcher l'accès aux cookies via JavaScript
- Limiter les attaques XSS et CSRF

13.4 Sécurisation spécifique à GLPI

Suppression du script d'installation

```
sudo rm -f /var/www/glpi/install/install.php
```

(rappel de sécurité post-validation)

Objectif :

- empêcher toute réinstallation ou détournement de l'application
- Renforcement des permissions sur les fichiers GLPI

```
sudo chown -R www-data:www-data /var/www/glpi /etc/glpi /var/lib/glpi
/var/log/glpi
sudo chmod -R 750 /var/www/glpi /etc/glpi /var/lib/glpi /var/log/glpi
```

Objectifs :

- limiter l'accès aux fichiers sensibles
- empêcher toute modification non autorisée

Forcer l'utilisation du HTTPS

Dans l'interface GLPI :

- Configuration > Générale > Sécurité
- Activation de l'obligation HTTPS
- Activation des cookies sécurisés

Objectif :

- garantir le chiffrement des sessions utilisateurs

13.5 Sécurisation de la base de données

- Utilisation d'un compte MariaDB dédié à GLPI
- Mot de passe fort
- Accès limité à localhost
- Aucun accès distant au compte root
- Sauvegardes régulières de la base de données

13.6 Journalisation et supervision

Les journaux suivants sont surveillés :

- Apache : /var/log/apache2/
- PHP-FPM : /var/log/php8.4-fpm.log
- GLPI : /var/log/glpi/

Objectifs :

- détection rapide des erreurs
- analyse des incidents et tentatives d'attaque

13.7 Politique de mises à jour

```
sudo apt install unattended-upgrades -y
sudo dpkg-reconfigure unattended-upgrades
```

Objectif :

- Appliquer automatiquement les correctifs de sécurité du système

13.8 Conclusion du durcissement

Le durcissement mis en place :

- Renforce significativement la sécurité du serveur et de GLPI
- Respecte les bonnes pratiques système et applicatives
- N'altère pas le fonctionnement validé de la plateforme
- Prépare l'environnement à une mise en production future

14. Table de correspondance DAT ↔ Procédure

Exigence DAT	**Description DAT**	**Section(s) Procédure**
Gestion de parc	Inventaire matériel et logiciel	Sections 6, 12
Helpdesk	Gestion des tickets et notifications	Sections 9, 12
Authentification LDAP/AD	Centralisation des comptes utilisateurs	Section 12
Sécurité HTTPS	Accès sécurisé à l'application	Section 10
Sécurité système	Sécurisation du système et des services	Section 13
Durcissement	Renforcement post-validation de la sécurité	Section 13
Sauvegardes	Sauvegarde de la base de données et des fichiers applicatifs	Sections 11, 12
PRA	Reprise d'activité après incident	Section 11

Exigence DAT	Description DAT	Section(s) Procédure
Supervision	Disponibilité et surveillance du service	Sections 7, 12

15. Conclusion

Procédure complète, conforme aux besoins du DAT, sécurisée et prête pour mise en production.

Auteur : ESCRIVA Yann

Projet : Décembre 2025