



# Procédure d'installation et de préparation de GLPI 11

---

## Sommaire

- Procédure d'installation et de préparation de GLPI 11
  - Sommaire
  - 1. Présentation
    - 1.1 Objectifs
  - 2. Prérequis
    - 2.1 Matériel
    - 2.2 Logiciel
    - 2.3 Réseau et flux
  - 3. Préparation du serveur Debian 13
    - 3.1 Mise à jour
  - 4. Installation de la stack LAMP
    - 4.1 Installation Apache, PHP-FPM et MariaDB
    - 4.2 Installation des extensions PHP
  - 5. Préparation de MariaDB
    - 5.1 Sécurisation
    - 5.2 Création de la base GLPI
  - 6. Téléchargement et préparation de GLPI
    - 6.1 Téléchargement
    - 6.2 Préparation des répertoires et permissions
  - 7. Configuration Apache pour GLPI
    - 7.1 VirtualHost complet
    - 7.2 Activation et redémarrage

- 8. Configuration PHP-FPM
  - 8.1 Configuration PHP-FPM
  - 8.2 Liaison Apache ↔ PHP-FPM
  - 8.3 Validation du fonctionnement PHP-FPM
- 9. Installation via l'interface web
- 10. Sécurisation post-installation
- 11. Sauvegardes et PRA
- 12. Tests et validation
  - 12.1 Vérifier accès HTTPS
  - 12.2 Authentification LDAP
  - 12.3 Envoi notifications SMTP
  - 12.4 Création et gestion tickets
  - 12.5 Ajout d'équipements et gestion des utilisateurs
  - 12.6 Sauvegardes restaurables
  - 12.7 SSO : non implémenté (évolution prévue)
  - 12.8 Conclusion des tests
- 13. Durcissement post-validation (FINAL)
  - 13.1 Durcissement du système Debian
    - Désactivation de la connexion SSH root
  - 13.2 Durcissement du serveur Apache
  - 13.3 Durcissement PHP / PHP-FPM
  - 13.4 Sécurisation spécifique à GLPI
  - 13.5 Sécurisation de la base de données
  - 13.6 Journalisation et supervision
  - 13.7 Politique de mises à jour
  - 13.8 Conclusion du durcissement
  - 14. Table de correspondance DAT ↔ Procédure
- 15. Conclusion

## 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
```

```
yann@glpi-test:~$ sudo apt update && sudo apt upgrade -y
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Atteint : 2 http://deb.debian.org/debian trixie-updates InRelease
Atteint : 3 http://security.debian.org/debian-security trixie-security InRelease
Tous les paquets sont à jour.
Sommaire :
  Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 0
yann@glpi-test:~$ █
```

## 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
```

```
Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.
You already have your root account protected, so you can safely answer 'n'.
Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
SQL executed without errors!
The operation might have been successful, or it might have not done anything.

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
SQL executed without errors!
The operation might have been successful, or it might have not done anything.

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
SQL executed without errors!
The operation might have been successful, or it might have not done anything.
  Removing privileges on test database...
SQL executed without errors!
The operation might have been successful, or it might have not done anything.

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
... Success!

Cleaning up...

All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.
```

### 5.2 Crédit de la base GLPI

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

```
yann@glpi-test:~$ sudo mysql -u root -p
[sudo] Mot de passe de yann :
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 11.8.3-MariaDB-0+deb13u1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]> CREATE DATABASE dbyann_glpi;
Query OK, 1 row affected (0,002 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dbyann_glpi.* TO glpi_admin@localhost IDENTIFIED BY "██████████";
Query OK, 0 rows affected (0,005 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> EXIT
Bye
yann@glpi-test:~$ █
```

## 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>
```

```

GNU nano 8.4
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>
</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
```

The screenshot shows the GLPI Installation process. The main title is "GLPI Installation". Below it, a message states: "La base de données de GLPI doit être installée et configurée." A button labeled "Aller à la page d'installation" is present. A note in a box says: "Si vous voyez cette page alors que l'installation est terminée, cela signifie que la configuration de la base de données de GLPI est soit supprimée, soit corrompue."

The screenshot shows the "Sélectionnez votre langue" (Select your language) step. It displays a dropdown menu set to "Français" and a yellow "OK >" button.

The screenshot shows the "Licence" (License) step. It displays the GNU General Public License (Version 3, 29 June 2007). A note at the bottom says: "Des traductions non officielles sont également disponibles". A yellow "Continuer >" button is at the bottom right.

The screenshot shows the "Début de l'installation" (Installation start) step. It has a radio button selected for "Installation ou mise à jour de GLPI". A note says: "Choisissez 'Installation' pour une nouvelle installation de GLPI. Choisissez 'Mise à jour' pour lancer la mise à jour de votre version de GLPI à partir d'une version antérieure." Two buttons are at the bottom: "Installer" (with a red arrow pointing to it) and "Mettre à jour".

The screenshot shows a compatibility check page for the GLPI installation. The header features the GLPI logo and the text "GLPI Installation". Below this, the title "Étape 0" is displayed, followed by the subtitle "Vérification de la compatibilité de votre environnement avec l'exécution de GLPI". A table titled "TESTS EFFECTUÉS" lists various PHP extensions required for GLPI's functionality. The table has two columns: "TESTS EFFECTUÉS" and "RÉSULTATS". Each row contains a requirement, its description, and a green checkmark indicating success.

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.	✓

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

Continuer >



The screenshot shows the first step of the GLPI installation process, titled "GLPI Installation" and "Étape 1". The title "GLPI Installation" is at the top center in yellow. Below it, "Étape 1" is centered. The main heading "Configuration de la connexion à la base de données" is in bold black text. There are three input fields: "Serveur SQL (MariaDB ou MySQL)" with a placeholder box, "Utilisateur SQL" with a placeholder box, and "Mot de passe SQL" with a placeholder box. At the bottom is a yellow "Continuer >" button.

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 >



The screenshot shows the fourth step of the GLPI installation wizard. The title is "GLPI Installation" and the sub-section is "Étape 4". The heading "Récolter des données" is displayed. A checked checkbox labeled "Envoyer 'statistiques d'usage'" is present. A note below it says "Nous avons besoin de vous pour améliorer GLPI et son écosystème de plugins !". It explains that since GLPI 9.2, a new "Télémétrie" feature has been introduced to send usage statistics anonymously with permission. Below this, a text input field asks "Dites-nous comment vous utilisez GLPI pour que nous améliorons GLPI et ses plugins !" with a "Voir ce qui sera envoyé..." button. A "Continuer >" button is located at the bottom.



The screenshot shows the fifth step of the GLPI installation wizard. The title is "GLPI Installation" and the sub-section is "Étape 5". The heading "Une dernière chose avant de démarrer" is displayed. It asks if the user wants help integrating GLPI into their SI, fixing bugs, or getting pre-configured rules/dictionaries. It introduces the GLPI-Network service, which provides support level 3 and guarantees bug fixes within a specified time frame. It also mentions that users can contact official partners for integration assistance. A "Continuer >" button is located at the bottom.



The dashboard includes the following data:

- Hardware Count:**
  - Logiciels: 114.7K
  - Ordinateurs: 5.4K
  - Matiéris réseau: 1.2K
  - Téléphones: 1.5K
  - Licences: 130
  - Moniteurs: 3.8K
  - Baies: 12
  - Imprimantes: 1.4K
- Manufacturers:**
  - Ordinateurs par Fabricant: 4.2K
  - Moniteurs par Modèle: 129
  - Matiéris réseau par: 56
- Inventory:**
  - 4.2K
  - 129
  - 56
  - 38.0K
- Ticket Status by Month:**

Mois	Nouveau	Validation	En cours (Attribué)	En cours (Planifié)	En attente	Résolu	Clos
2025-01	~100	~100	~100	~100	~100	~100	~100
2025-03	~100	~100	~100	~100	~100	~100	~100
2025-05	~100	~100	~100	~100	~100	~100	~100
2025-07	~100	~100	~100	~100	~100	~100	~100
2025-09	~100	~100	~100	~100	~100	~100	~100
2025-11	~100	~100	~100	~100	~100	~100	~100
- Tickets Summary:**
  - 1.5K Tickets
  - 2 Tickets en retard
  - 1. Profil

## 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
# VirtualHost HTTP → Redirection HTTPS
# /etc/apache2/sites-available/glpi.conf

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

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

# VirtualHost HTTPS
# /etc/apache2/sites-available/glpi-ssl.conf

<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

```
yann@glpi-test:~$ curl -vk https://glpi_test.archeaggle.fr
* Host glpi_test.archeaggle.fr:443 was resolved.
* IPv6: (none)
* IPv4: 10.255.2.101
* Trying 10.255.2.101:443...
* ALPN, offering h2,http/1.1
* TLSv1.3 (OUT) TLS handshake, Client hello (1):
*   TLSv1.3 (IN), TLS handshake, Server hello (2):
*     TLSv1.3 (IN), TLS change cipher, Change cipher spec (1):
*     TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
*     TLSv1.3 (IN), TLS handshake, Certificate (11):
*       TLSv1.3 (IN), TLS handshake, CERT verify (15):
*         TLSv1.3 (IN), TLS handshake, Finished (20):
*   SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / RSASSA-PSS
* ALPN: server accepted http/1.1
* Server certificate:
*   subject: C=FR; ST=Mauves; L=Mauves; O=Arche Agglo; OU=SI; CN=glpi_test.archeaggle.fr; emailAddress=y.escriva@archeaggle.fr
*   start date: Jan 5 08:55:18 2026 GMT
*   expire date: Jan 5 08:55:18 2027 GMT
*   issuer: C=FR; ST=Mauves; L=Mauves; O=Arche Agglo; OU=SI; CN=glpi_test.archeaggle.fr; emailAddress=y.escriva@archeaggle.fr
*   SSL certificate verify result: self-signed certificate (18), continuing anyway.
*   Certificate level 0: Public key type RSA (2048/112 Bits/secBits), signed using sha256WithRSAEncryption
*   Connected to glpi_test.archeaggle.fr (10.255.2.101) port 443
* using HTTP/1.x
> GET / HTTP/1.1
> Host: glpi_test.archeaggle.fr
> User-Agent: curl/8.14.1
> Accept: */*
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Mon, 19 Nov 2024 10:39:02 GMT
< Server: Apache/2.4.65 (Debian)
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, no-cache, private
< Pragma: no-cache
< Set-Cookie: glpi_05a38ef3f66bb4c5f37e130763859d7b17981e767dc8632fd481a58765d632c8800303ca90038f5fc7e7c2ebc4521aea409670dc5501f27ddec763be3bded79=b79e1f1e4a737acb4269dc9fe
[REDACTED]
```

## 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

The screenshot shows the GLPI interface for managing LDAP configurations. The top navigation bar includes links for Accueil, Configuration, Authentification, Annuaires LDAP, and a button to Add a new configuration. A search bar and a user dropdown are also present. The main content area displays a test result for 'Annuaire LDAP - LDAP Test - ID 1'. The test summary is titled 'Test LDAP Serveur : LDAP Test' and lists five steps: 1. Flux TCP (Connection to 10.255.2.101 on port 389 successful), 2. Base DN (Base DN "dc=nodomain" configured), 3. LDAP URI (URI LDAP verification successful), 4. Connexion Bind (Authentication successful), and 5. Chercher (50 first results found) (Search successful (1 entries found)). On the left, a sidebar menu lists options like Annuaire LDAP, Tester, Utilisateurs, Groupes, Informations avancées, Réplicats, Historique, and Tous.

**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

"GLPI test" yann@localhost

```
yann@glpi-test:~$ echo "Test réception GLPI" | mail -s "GLPI test réception" yann@localhost
yann@glpi-test:~$ mail
"/var/mail/yann": 2 messages 2 nouveaux
>N 1 Yann           lun. janv. 5 16 16/464  GLPI test
N 2 Yann           lun. janv. 5 16 13/423  GLPI test réception
?
```

**Statut :** validé

## 12.4 Crédation et gestion tickets

### Objectif :

Valider le fonctionnement du module helpdesk

### Actions réalisées :

- Crédation 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

The screenshot displays two views of the GLPI application. The top view shows a Kanban board with ticket counts: 1 Ticket (yellow), 0 Tickets entrants (green), 0 Tickets en attente (orange), 1 Tickets assignés (light blue), 0 Tickets planifiés (blue), 0 Tickets résolus (grey), and 0 Tickets fermés (white). Below the board is a table with one ticket entry:

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 i	admin_glpi i		

The bottom view shows a detailed ticket edit screen for "Ticket test GLPI (1)". The ticket details include:

- Créé :** il y a 1 minutes par admin\_glpi
- Titre :** Ticket test GLPI
- Contenu :** Ceci est un ticket de test
- Date d'ouverture :** 2026-01-05 12:00
- Type :** Incident
- Catégorie :** -----
- Statut :** En cours (Attribué)
- Source de la demande :** Helpdesk
- Urgence :** Moyenne
- Impact :** Moyen

Buttons at the bottom include "Répondre", "Sauvegarder", and navigation controls.

The screenshot shows the GLPI ticket management interface. At the top, there are six summary boxes: 1 Ticket (yellow), 0 Tickets entrants (green), 0 Tickets en attente (orange), 0 Tickets assignés (light blue), 0 Tickets planifiés (blue), and 1 Tickets résolus (grey). Below this is a search bar and a navigation menu with 'Super-Admin' and 'Entité racine' options.

The main area displays a table of tickets. A single ticket is listed:

ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
1	Ticket test GLPI	Clos	2026-01-07 07:50	2026-01-05 12:00	Moyenne	admin_glpi i	admin_glpi i		

Below the table, it says "15 lignes / pages" and "De 1 à 1 sur 1 lignes".

A modal window titled "Ticket test GLPI (1)" is open, showing the details of the ticket. The ticket title is "Ticket test GLPI" and the description is "Ceci est un ticket de test". The ticket status is "résolu".

The left sidebar lists various modules: Statistiques, Validations, Base de connaissances, Éléments, Coûts, Projets, Tâches de projet, Problèmes, Changements, and Contrats. Each item has an "AD" badge next to it.

**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.

The screenshot shows the GLPI interface with the following details:

- Top Navigation Bar:** Shows various system status icons like UniFi Network, Zimbra Reception, Mailinblack, etc.
- Left Sidebar:** Includes links for Accueil, Parc, Configuration, Plugins (highlighted with a red box), and other system management options.
- Plugins Marketplace:** Shows a list of available plugins. One plugin, "data inject" by Walid Nouh, is highlighted with a red box. It is described as allowing CSV import into GLPI.
- Bottom Left Sidebar:** Shows a navigation menu with "Outils" selected, followed by "Projets", "Notes", "Flux RSS", "Base de connaissances", "Réservations", "Rapports", "Recherches sauvegardées", and "Data Injection".
- Bottom Right Content Area:** Displays a message stating "Aucun modèle n'est disponible actuellement. Vous pouvez en créer un." (No model is currently available. You can create one.)

Alt text Alt text Alt text Alt text Alt text

Import_user1.csv - Excel																
Fichier	Accueil	Insertion	Mise en page	Formules	Données	Révision	Affichage	Aide	Acrobat	Rechercher	Yann ESCRIVA	Partager				
Collier	Calibri	11	A <sup>°</sup> A <sup>®</sup>													
Coller																
esse-papiers																
										<img						

Accueil / Administration / Utilisateurs + Ajouter Ajout depuis une source externe Liaison annuaire LDAP Rechercher Super-admin Entité racine AD

IDENTIFIANT	NOM DE FAMILLE	E-MAILS	TÉLÉPHONE	LIEU	ACTIVÉ
glpi					Non
post-only					Non
tech					Non
normal					Non
glpi-system	Support				Oui
admin_glpi					Oui
Plugin_GLPI_Inventory					Oui
zlefoudroyant	LEFOUDROYANT	zlefoudroyant@ais.com	1501		Oui
alaguerriere	LAGUERRIERE	alaguerriere@ais.com	1502		Oui
p.ledieu	LEDIEU	p.ledieu@ais.com	1503		Oui

**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 :

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/S07ot6cI19N8UBSmuxmw
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/+
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/+/V75U-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/GwvsH6yg605xEELNqfoA
var/lib/glpi/files/_cache/11.0.4-1d4fbe9a-production/core/D/M/GwvsH6yg605xEELNqfoA

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

<b>Exigence DAT</b>	<b>Description DAT</b>	<b>Section(s) Procédure</b>
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

<b>Exigence DAT</b>	<b>Description DAT</b>	<b>Section(s) Procédure</b>
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