



Installation de GLPI sur debian 12

GLPI



Sommaire :

- 1- Prérequis
- 2- MAJ des paquets
- 3- Installation de GLPI via apt-get
- 4- Mise en pratique
- 5- Consulter les alertes GLPI

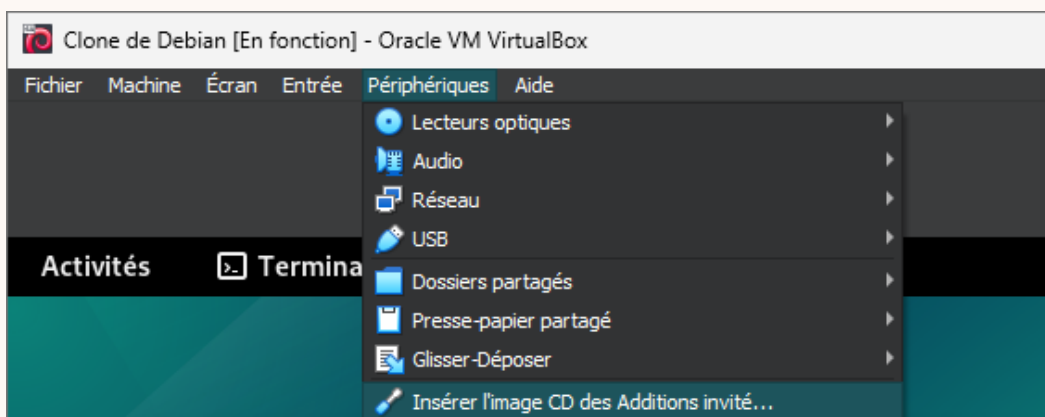
Configuration serveur GLPI

1- Prérequis

GLPI est un système de détection d'intrusion (IDS) open source qui analyse le trafic réseau en temps réel pour identifier des comportements malveillants ou suspects. Il utilise des règles pour détecter des attaques, des intrusions ou des activités non autorisées sur le réseau. GLPI peut aussi être configuré en mode préventif (IPS), où il bloque activement les menaces détectées.

2- Préparation :

Dans notre cas GLPI sera installer sur une VM pour faciliter le copier coller sans SSH il est conseillé d'installer les ADDONS :



Configuration serveur GLPI

monter la partition :

```
sacha@debian:~$ su root
Mot de passe :
root@debian:/home/sacha# mount /dev/cdrom /mnt
mount: /mnt: ATTENTION: source protégée en écriture,
root@debian:/home/sacha# cd /mnt
```

Exécutez le script :

```
root@debian:/mnt# ./VBoxLinuxAdditions.run
Verifying archive integrity... 100% MD5 checksums are OK.
Uncompressing VirtualBox 7.0.10 Guest Additions for Linux 1
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
```

1- Installation des dépendances :

GLPI fonctionne avec la base LAMP (Linux, Apache, MySQL, PHP) pour cela il faut impérativement tout installer avant de lancer l'installation de GLPI

```
root@debian:/home/sacha# sudo apt-get install apache2 php mariadb-server
```

apt-get install apache2 php mariadb-server

Configuration serveur GLPI

apt-get install

php-{mysql,mbstring,curl,gd,xml,intl,ldap,apcu,xmldr,zip,bz2,imap}

```
root@debian:/home/sacha# sudo apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apcu
```

apt-get install php-ldap

```
root@debian:/home/sacha# sudo apt-get install php-ldap
```

1- Configurer le serveur SQL :

Sécurisation de la BDD :

mysql_secure_installation

```
root@debian:/home/sacha# sudo mysql_secure_installation
```

Entrez le mdp root :

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.
```

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...
```

```
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] |
```

Configuration serveur GLPI

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

```
Switch to unix_socket authentication [Y/n]
```

```
Enabled successfully!
```

```
Reloading privilege tables..
```

```
... Success!
```

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

```
Change the root password? [Y/n]
```

```
Remove anonymous users? [Y/n]
```

```
... Success!
```

```
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]
```

```
... Success!
```

```
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]
```

```
- Dropping test database...
```

```
... Success!
```

```
- Removing privileges on test database...
```

```
... Success!
```

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

```
Reload privilege tables now? [Y/n]
```

```
... Success!
```

```
Cleaning up...
```

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

Configuration serveur GLPI

Création de la Base et des droits :

create database *NOMBDD*; grant all privileges on *NOMBDD*.* to *USER*@localhost identified by "*MDP*";

```
MariaDB [(none)]> CREATE DATABASE db23_glpi; GRANT ALL PRIVILEGES ON db23_glpi.*  
TO glpi_adm@localhost IDENTIFIED BY "R00tR00t"; FLUSH PRIVILEGES; EXIT
```



Dans notre cas nous autorisons la connexion uniquement en localhost (127.0.0.1) à adapter avec l'ip du GLPI si la BDD n'est pas sur le même serveur que le GLPI.

Il faut maintenant récupérer le dernier fichier de glpi sur le [site](#) :

```
root@debian:/tmp# wget https://github.com/glpi-project/glpi/releases/download/10  
.0.10/glpi-10.0.10.tgz
```

Ensuite nous décompressons l'archive et nous la déplaçons dans /var/www/html :

sudo tar -xzf *GLPIVERSION* -C /var/www/html

```
root@debian:/tmp# sudo tar -xzf glpi-10.0.10.tgz -C /var/www/
```

Configuration serveur GLPI

Affectation des droits :

`chown -R www-data /var/www/html`

`root@debian:/tmp# sudo chown www-data /var/www/glpi/ -R`

1- Configurer le GLPI :

se connecter avec un navigateur sur l'ip du GLPI :



The screenshot shows the GLPI SETUP interface. At the top, the GLPI logo is on the left, and 'GLPI SETUP' is on the right. Below the logo, there's a section 'Sélectionnez votre langue' with a dropdown menu set to 'Français' and an 'OK >' button. To the right of the language selection, there's a table of requirements and security warnings.

Type	Message	Status
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	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 sécurisée du dossier racine du serveur web La configuration du dossier racine du serveur web devrait être '/var/www/html/glpi/public' pour s'assurer que les fichiers non publics ne peuvent être accessibles. La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.	⚠
Sécurité	Emplacement sécurisé pour les dossiers de données Les dossiers de données de GLPI devraient être placés en dehors du dossier racine web. Ceci peut être effectué en redéfinissant les constantes correspondantes. Référez-vous à la documentation d'installation pour plus de détails. Les dossiers suivants devraient être placés en dehors de '/var/www/html/glpi': - '/var/www/html/glpi/files' ('GLPI_VAR_DIR') Vous pouvez ignorer cette suggestion si le dossier racine de votre serveur web est '/var/www/html/glpi/public'.	⚠
Sécurité	Configuration de sécurité pour les sessions Permet de s'assurer que la sécurité relative aux cookies de session est renforcée. La directive PHP 'session.cookie_httponly' devrait être définie à 'on' pour prévenir l'accès aux cookies depuis les scripts côté client.	⚠
Suggéré	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, ...).	✓
Suggéré	exif extension Renforcer la sécurité de la validation des images.	✓
Suggéré	Idap extension	✓

Configuration serveur GLPI



GLPI SETUP

Étape 1
Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

127.0.0.1

Utilisateur SQL

glpi_adm

Mot de passe SQL

.....

Continuer >



GLPI SETUP

Étape 2
Test de connexion à la base de données

✓ Connexion à la base de données réussie

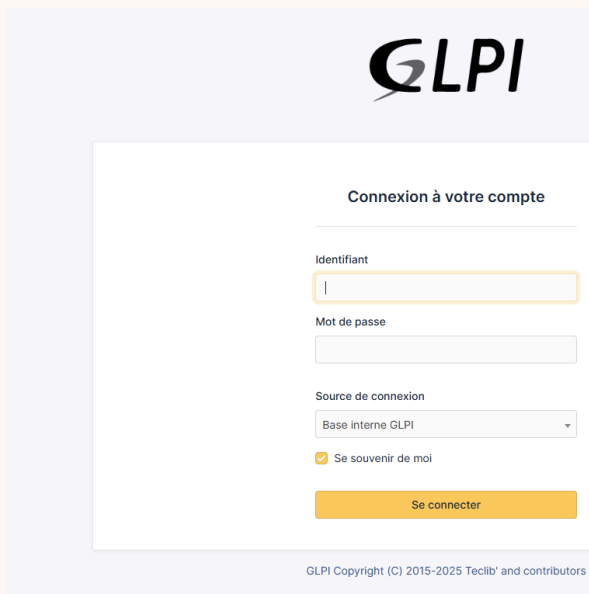
Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

☐

☒ db23_glpi

Continuer >



GLPI

Connexion à votre compte

Identifiant

Mot de passe

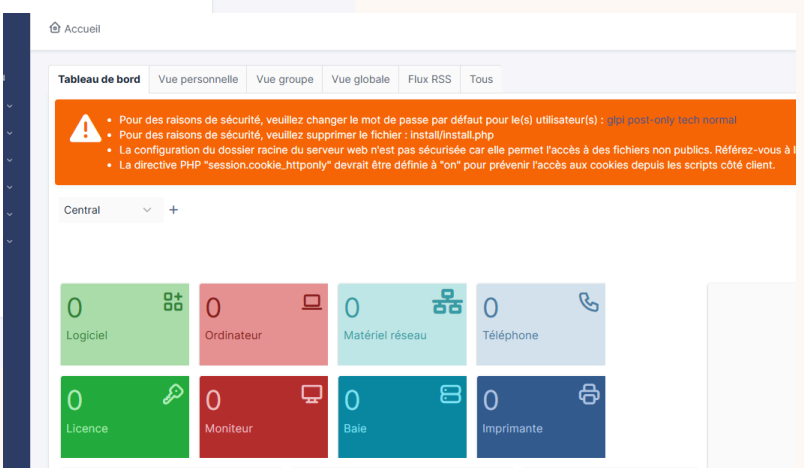
Source de connexion

Base interne GLPI

☒ Se souvenir de moi

Se connecter

GLPI Copyright (C) 2015-2025 Teclib' and contributors



Accueil

Tableau de bord | Vue personnelle | Vue groupe | Vue globale | Flux RSS | Tous

⚠ Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal

⚠ Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php

⚠ La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à l'installation

⚠ La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.

Central

Logiciel

Ordinateur

Matériel réseau

Téléphone

Licence

Moniteur

Baie

Imprimante