

1. BONUS : Contrôle à distance de la machine Debian en SSH

Avant de démarrer la réalisation de ce tuto, **je vous conseille plus que vivement d'installer OpenSSH Server** sur la VM Debian, cela est plus pratique pour administrer un serveur Linux distant, Voici la commande :

```
apt install openssh-server -y
```

A partir de ce point, vous pouvez directement vous connectez à distance à la machine en utilisant un **terminal** ou via un émulateur de terminal tel que [Putty](#).

Récupérez au préalable l'IP de la machine GLPI avec la commande « **ip a** » :

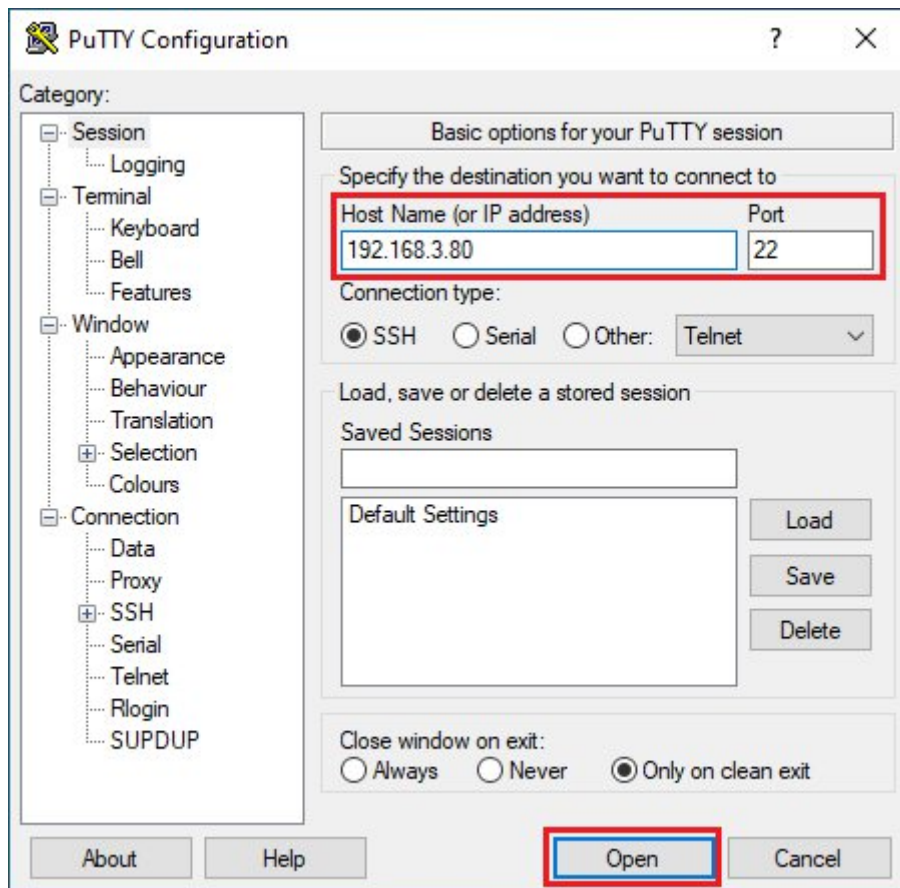
```
root@vm-glpi:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNK
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq
    link/ether 08:00:27:ab:2f:ca brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.80/24 brd 192.168.3.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feab:2fca/64 scope link
        valid_lft forever preferred_lft forever
```

Si vous utilisez un terminal classique type **invite de commande** chez Windows, tapez la commande suivante pour vous connecter :

```
ssh nom-user@IP-ou-nom-serveurGLPI
```

```
C:\Users\Administrateur>ssh tech@192.168.3.80
The authenticity of host '192.168.3.80 (192.168.3.80)' can't be established.
ECDSA key fingerprint is SHA256:hyWigr/1TPAh9NB5MZZfg/4creBTMGJEHB7C6veq9u0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.3.80' (ECDSA) to the list of known hosts.
tech@192.168.3.80's password: _
```

Si vous utilisez putty, saisissez simplement l'adresse IP ou le nom du serveur GLPI en veillant bien à ce que le port soit le 22 (port par défaut du protocole SSH et cliquez sur Open



S'il s'agit de la 1^{ère} connexion distance au serveur depuis votre machine, vous verrez un message d'avertissement (*que vous passiez par putty ou non*), **cliquez simplement sur OUI ou saisissez YES pour continuer.**

Vous pouvez ensuite vous connecter avec un **compte utilisateur** (*une fois encore pas le compte root mais un user qui a les droits sudo de préférence sinon vous serez vite bridé...*).

```
login as: tech
tech@192.168.3.80's password: █
```

Vous pouvez ensuite **passer en super utilisateur root** si vous le souhaitez avec la **commande « su - »**. Il ne vous restera qu'à saisir le mot de passe du compte root.

```
tech@vm-glpi:~$ su -
Mot de passe :
root@vm-glpi:~# █
```

C'est tout pour cette étape « bonus », passons maintenant au sujet

2. Installation des packages nécessaires sur le serveur

Alors comme d'habitude, on commence comme par **mettre à jour la machine** avec la commande suivante :

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

On va **installer les applications nécessaires** pour transformer notre serveur en **LAMP**.

```
apt install apache2 php mariadb-server -y
```

Ensuite, nous allons installer toutes les **dépendances** donc **pourrait avoir besoin GLPI**

```
apt install php-  
{mysql,mbstring,curl,gd,xml,intl,ldap,apcu,xmllrpc,zip,bz2,imap} -y
```

3. Configuration du service de bases de données

Nous allons maintenant **sécuriser l'accès au service de base de données**. Lancez la commande suivante :

```
mysql_secure_installation
```

Le mot de passe de l'utilisateur root est demandé. Il ne s'agit pas ici du mot de passe de l'utilisateur root sur la machine elle-même mais de l'utilisateur SQL (base de données). A ce stade, aucun mot de passe ne lui a été configuré, c'est donc ce que nous allons faire. **Appuyez simplement sur Entrée**.

```
root@vm-glpi:~# mysql_secure_installation  
  
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): █
```

Aux questions posées, **appuyez sur Entrée pour répondre « yes »** directement.

```
Switch to unix socket authentication [Y/n]
Enabled successfully!
Reloading privilege tables..
... Success!

You already have your root account protected

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

L'une des questions vous demande justement si vous voulez attribuer un mot de passe au **compte root pour accéder au service de base de données**. Appuyez sur **Entrée** pour dire Oui.

Saisissez 2 fois le mot de passe que vous voulez donner au compte SQL root pour. **Attention, aucun symbole ne va s'afficher pendant la saisie, soyez vigilant à votre frappe !**

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

Vous pourrez par la suite répondre **Yes à toutes les autres questions** posées.

```
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.

Thanks for using MariaDB!
root@vm-glp1:~#
```

Maintenant que l'accès aux bases de données est sécurisé, nous allons pouvoir nous y **connecter avec le compte root** et le mot de passe que nous venons de lui définir :

```
mysql -u root -p
```

Commençons par **créer la base de données** qui sera utilisée par GLPI. Dans nom cas, je vais nommer cette base de données « **db_glpi** » mais vous pouvez la nommer selon vos désirs, il faut juste vous en souvenir pour la suite. Utilisez la commande suivante :

```
create database db_glpi;
```

Nous allons ensuite créer un **utilisateur de base de données** et lui **donner des droits** sur cette base de données. La commande suivante va **créer un utilisateur ici nommé « admindb_glpi »**, lui **attribuer le mot de passe « votre-MDP »** et lui **donner tous les privilèges**

```
grant all privileges on db_glpi.* to admindb_glpi@localhost identified by "votre-MDP";
```

C'est terminé pour cette partie, vous pouvez quitter mysql ou mariadb avec la commande suivante :

```
exit
```

La base de données est prête, passons maintenant au téléchargement de GLPI sur notre serveur !

4. Téléchargement de GLPI

Placez vous dans le répertoire de votre choix

```
cd /tmp
wget https://github.com/glpi-project/glpi/releases/download/10.0.17/glpi-10.0.17.tgz
```

Décompressez l'archive de GLPI directement dans le **répertoire par défaut du service web** qui est /var/www/html :

```
tar -xvzf glpi-10.0.17.tgz -C /var/www/html
```


Rendez l'utilisateur des services web (nommé `www-data`) propriétaire de ces nouveaux fichiers :

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


Vous pouvez vérifier que tout est OK en listant le contenu du répertoire avec la commande « `ls -l /var/www/html` ». Vous pourrez alors constater la présence du répertoire `glpi` et que le propriétaire est bien l'utilisateur nommé « `www-data` ».


```
root@vm-glpi:/tmp# chown -R www-data /var/www/html
root@vm-glpi:/tmp# ls -l /var/www/html/
total 16
drwxr-xr-x 24 www-data tech 4096 11 juil. 09:08 glpi
-rw-r--r-- 1 www-data root 10701 30 juil. 14:59 index.html
```

GLPI est en place !

A partir de ce point, GLPI est presque déjà fonctionnel. Cependant, afin de respecter les prérequis et les recommandations de l'éditeur et de sécuriser un peu tout cela, ils restent encore quelques étapes importantes.

Ce premier screen montre les warnings émis par GLPI lors de l'installation de ce dernier via son interface web. Ce n'est pas bloquant, vous aurez juste à descendre en bas de la page d'installation de GLPI et cliquer sur Continuer.

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.

Ce second screen est issu du **tableau de bord de GLPI** après la première connexion. Les deux dernières alertes concernent la configuration du service web qui n'est pas conforme avec les recommandations de l'éditeur. Une fois encore, ce n'est pas bloquant, vous pouvez simplement ignorer la présence de ces messages.



- 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 la documentation d'installation pour plus de détails.
- La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.

5. Configuration des emplacements des dossiers et fichiers de GLPI

Nous allons suivre une partie de recommandations de GLPI présentent dans la [documentation](#). Nous allons séparer une partie des fichiers de GLPI afin de sécuriser le tout un minimum.

Créez un dossier nommé « **glpi** » dans **/etc** :

```
mkdir /etc/glpi
```

Dans ce nouveau dossier, **créez un fichier nommé « local_define.php »** :

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

Y insérer le contenu suivant (*bien respecter la syntaxe*) :

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

```
tech@vm-glpi: ~
GNU nano 7.2 /etc/glpi/local_define.php
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Quittez le fichier en appuyant sur les touches **Ctrl + X**, puis ensuite sur **O** pour valider l'enregistrement des modifications puis sur la touche **Entrée** pour conserver le nom du fichier.

Déplacez le dossier « config » situé actuellement dans /var/www/html/glpi dans /etc/glpi :

```
mv /var/www/html/glpi/config /etc/glpi
```

Rendez **www-data** propriétaire de /etc/glpi et de son contenu :

```
chown -R www-data /etc/glpi/
```

N'oubliez pas vous pouvez **vérifier le contenu d'un dossier et le propriétaire** de ce contenu grâce à la commande « ls -l /etc/glpi » :

```
root@vm-glpi:/tmp# ls -l /etc/glpi/
total 8
drwxr-xr-x 2 www-data tech 4096 11 juil. 09:05 config
-rw-r--r-- 1 www-data root   88 30 juil. 16:04 local_define.php
```

Poursuivons en **déplaçant le dossier « files »** de glpi dans /var/lib/glpi :

```
mv /var/www/html/glpi/files /var/lib/glpi
```

Ensuite nous allons **préparer le dossier de logs de GLPI** et rendre, une fois encore, l'utilisateur **www-data** propriétaire avec les 2 commandes suivantes :

```
mkdir /var/log/glpi
chown www-data /var/log/glpi
```

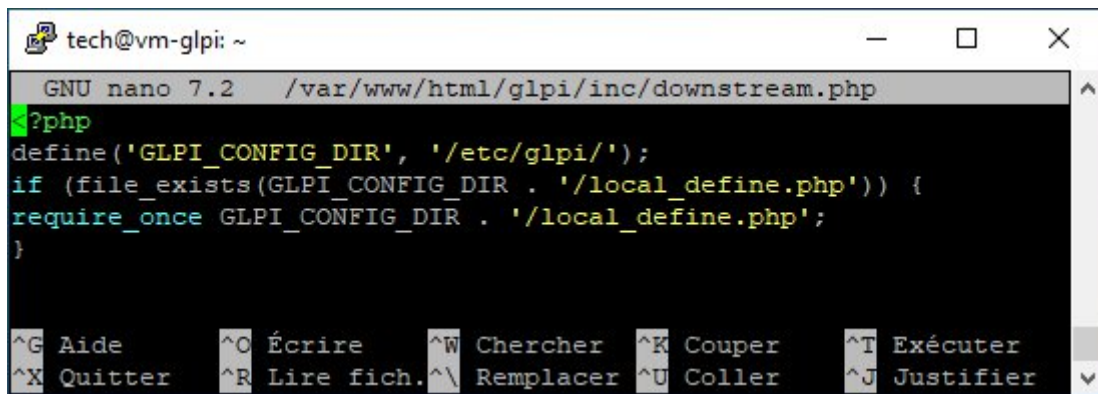
Il va maintenant falloir **faire comprendre à GLPI où il va devoir chercher les fichiers et ses configs**. Cela est en fait décrit dans le fichier « local_define.php » que l'on a créé précédemment mais il faut tout de même dire à GLPI d'aller **checker cela dans /etc/glpi**

Pour cela, **créez un fichier nommé « downstream.php »** dans /var/www/html/glpi/inc :

```
nano /var/www/html/glpi/inc/downstream.php
```

Y insérer le contenu suivant (*bien respecter la syntaxe*) :

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

```
tech@vm-glpi: ~
GNU nano 7.2 /var/www/html/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';
}

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier
```

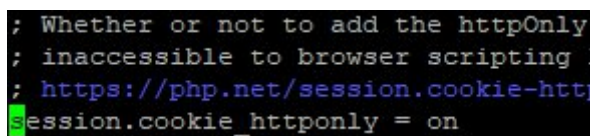
Voilà pour les emplacements recommandés. Passons ensuite à l'étape suivante : la configuration d'Apache, le service web.

6. Configuration du service web

Nous allons **modifier le fichier php.ini** situé dans `/etc/php/votre-version-de-php/apache2` (pour moi php version 8.2) :

```
nano /etc/php/8.2/apache2/php.ini
```

Dans ce fichier, sans rien toucher d'autres, **recherchez la ligne « `session.cookie_httponly =` » et ajoutez « `on` » après le égal.** Vous pouvez ensuite quitter le fichier en enregistrant les modifications et sans le renommer. Cette manipulation aura pour but de refuser l'accès à un cookie issu d'un langage de navigateur type javascript, car ils peuvent être corrompus et donc infecter le système.



```
; Whether or not to add the httpOnly
; inaccessible to browser scripting :
; https://php.net/session.cookie-htt
session.cookie_httponly = on
```

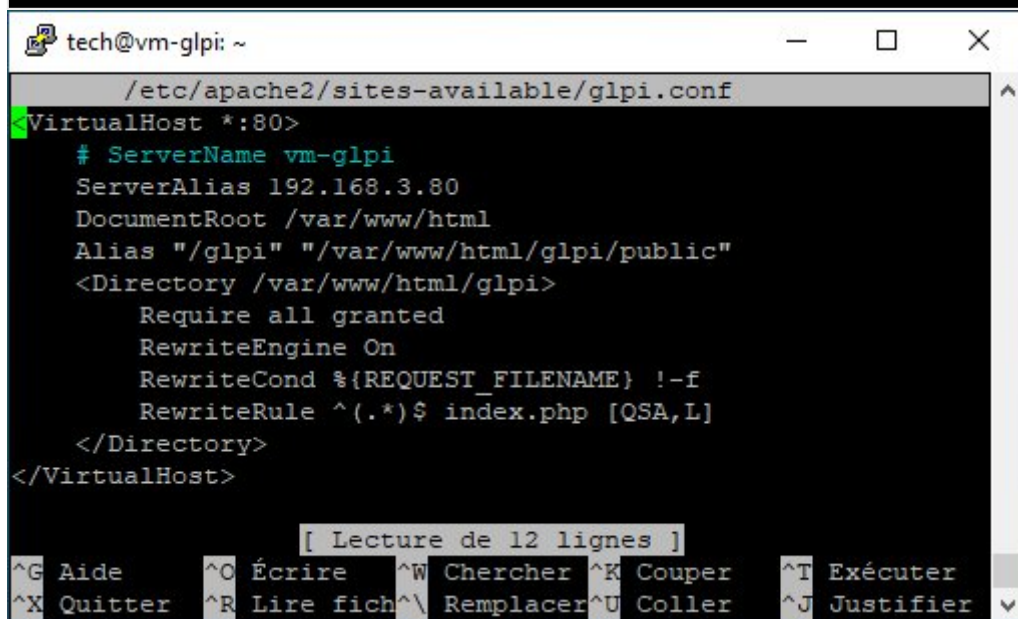
Ensuite pour terminer sur la grosse partie configuration, il faut **créer un virtualhost dans le service web spécialement dédié au site web de notre GLPI.** Un virtualhost est un fichier configuré sur apache permettant de faire cohabiter plusieurs sites web différents sur la même machine. Chaque virtualhost est configuré pour l'un des sites web hébergé sur le serveur.

Créez dans le dossier d'apache2 un **fichier nommé « `glpi.conf` »** :

```
nano /etc/apache2/sites-available/glpi.conf
```

Y insérer le contenu suivant basé sur la doc GLPI, une fois encore en adaptant à votre environnement (*bien respecter la syntaxe*) :

```
<VirtualHost *:80>
# ServerName vm-glpi
ServerAlias 192.168.3.80
DocumentRoot /var/www/html
Alias "/glpi" "/var/www/html/glpi/public"
<Directory /var/www/html/glpi>
Require all granted
RewriteEngine On
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>
```



```
tech@vm-glpi: ~
/etc/apache2/sites-available/glpi.conf
VirtualHost *:80>
# ServerName vm-glpi
ServerAlias 192.168.3.80
DocumentRoot /var/www/html
Alias "/glpi" "/var/www/html/glpi/public"
<Directory /var/www/html/glpi>
    Require all granted
    RewriteEngine On
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteRule ^(.*)$ index.php [QSA,L]
</Directory>
</VirtualHost>
[ Lecture de 12 lignes ]
^G Aide    ^O Écrire  ^W Chercher ^K Couper  ^T Exécuter
^X Quitter ^R Lire fich ^\ Remplacer ^U Coller  ^J Justifier
```

Une fois ceci fait, **activez un module apache** qui permet de faire de la redirection d'URL :

```
a2enmod rewrite
```

Désactivez la config par défaut d'Apache avec la commande suivante :

```
a2disssite 000-default.conf
```

Et enfin, **activez le fichier de configuration web spécialement créé précédemment pour glpi** :

```
a2ensite glpi.conf
```

Il ne reste plus qu'à **redémarrer le service apache2** pour appliquer toutes les modifications apportées :

```
systemctl restart apache2
```

C'est tout pour cette partie, **le serveur est prêt**, maintenant dernière ligne droite !

7. Configuration finale de GLPI via interface web

Les fichiers pour GLPI sont prêts, l'installation va se poursuivre directement via une interface web.

Accédez à la machine depuis n'importe quel PC sur le même réseau en vous rendant sur à l'URL suivante :

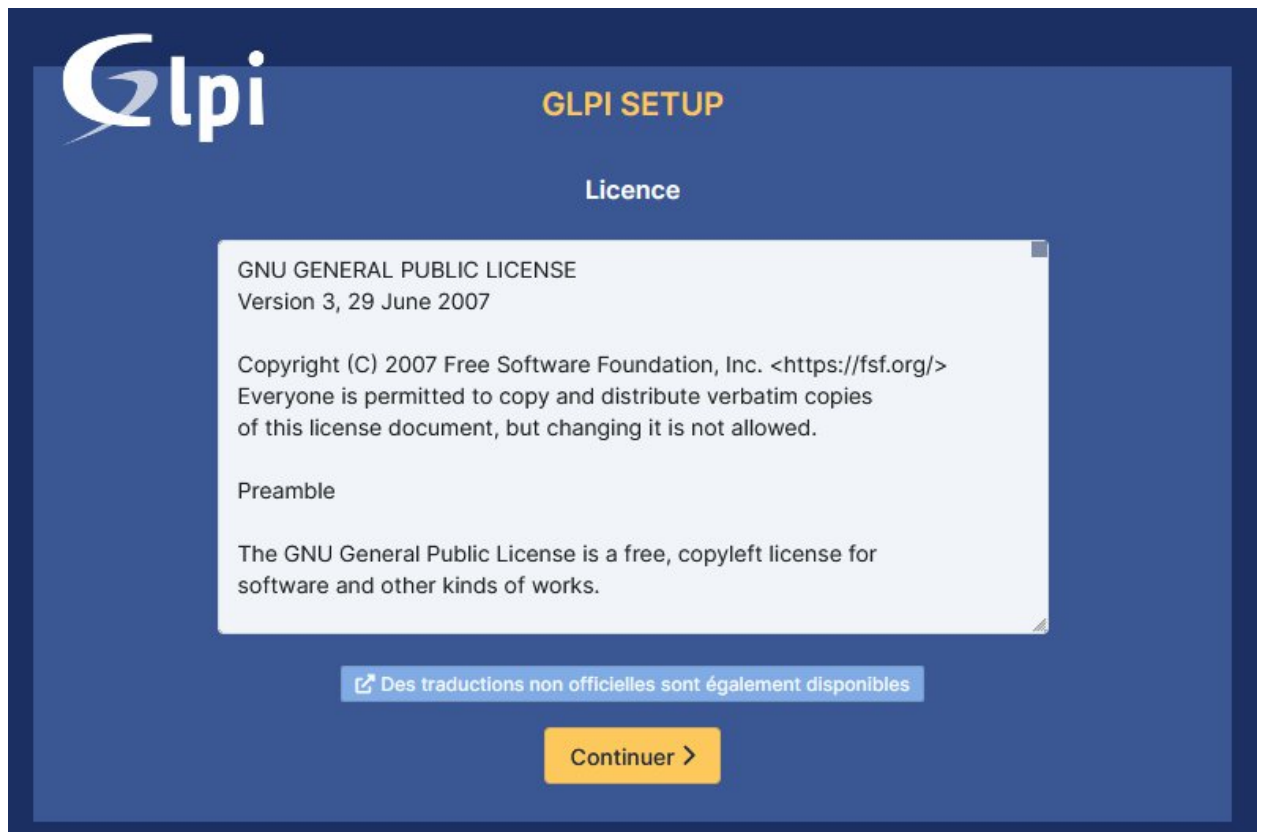
http://ip_ou_nom_de_votre_machine_glpi/glpi



Vous arrivez sur la page du **setup de GLPI**. Sélectionnez le Français dans la liste déroulante et cliquez sur OK.



Acceptez les conditions d'utilisation pour poursuivre.



Cliquez sur le bouton **Installer** pour lancer le setup.



Une série de test sera lancée par le setup pour s'assurer que tous **les prérequis nécessaires au bon fonctionnement de GLPI sont remplis**. Si vous avez correctement suivi ce tuto, il ne devrait y avoir que des coches vertes, si ce n'est pas le cas, corrigez d'abord les erreurs présentes qui peuvent être bloquantes. . Cliquez sur **Continuer**.



GLPI SETUP

Étape 0

Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

TESTS EFFECTUÉS	RÉSULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysqli extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis zlib extension <i>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.</i>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <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>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Sécurité Version de PHP maintenue <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>	✓
Sécurité Configuration sécurisée du dossier racine du serveur web <i>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.</i>	✓
Sécurité Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</i>	✓
Suggéré Taille d'entier maximal de PHP <i>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).</i>	✓
Suggéré exif extension <i>Renforcer la sécurité de la validation des images.</i>	✓
Suggéré ldap extension <i>Active l'utilisation de l'authentification à un serveur LDAP distant.</i>	✓
Suggéré openssl extension <i>Active l'envoi de courriel en utilisant SSL/TLS.</i>	✓
Suggéré Extensions PHP pour le marketplace <i>Permet le support des formats de paquets les plus communs dans le marketplace.</i>	✓
Suggéré Zend OPcache extension <i>Améliorer les performances du moteur PHP.</i>	✓
Suggéré Extensions émulées de PHP <i>Améliorer légèrement les performances.</i>	✓
Suggéré Permissions pour le répertoire du marketplace <i>Active l'installation des plugins à partir du Marketplace.</i>	✓

Continuer >

Il reste à saisir les **informations sur la base de données destinées à GLPI** que nous avons précédemment créée. Saisissez **localhost** pour spécifier que la machine actuelle héberge à la fois le site web de GLPI et la base de données (*si la base de données est stockée sur une autre machine, saisissez son adresse IP ou son nom*). Rentrez ensuite le nom de l'utilisateur qui a tous les privilèges sur cette base de données et son mot de passe.



The screenshot shows the 'GLPI SETUP' interface for 'Étape 1'. The title is 'Configuration de la connexion à la base de données'. It contains three input fields: 'Serveur SQL (MariaDB ou MySQL)' with the value 'localhost', 'Utilisateur SQL' with the value 'admindb_glpi', and 'Mot de passe SQL' which is masked with dots. A yellow 'Continuer >' button is at the bottom.

Sélectionnez ensuite la **base de données créée spécialement pour GLPI**, il n'y a qu'à cocher le cercle devant le nom de la base de données que vous aurez créée avant de cliquer sur Continuer.



The screenshot shows the 'GLPI SETUP' interface for 'Étape 2'. The title is 'Test de connexion à la base de données'. A green success message '✓ Connexion à la base de données réussie' is displayed. Below, under the heading 'Veuillez sélectionner une base de données :', there is a section 'Créer une nouvelle base ou utiliser une base existante :'. It features a radio button for creating a new database and a list of existing databases, with 'db_glpi' selected and highlighted. A yellow 'Continuer >' button is at the bottom.

Le setup va contacter la base de données pour s'assurer que tout est OK. Patientez quelques secondes avant de pouvoir continuer.



Choisissez d'envoyer ou pas des statistiques sur votre utilisation de GLPI à l'équipe qui gère le projet et poursuivez.



On vous informe ensuite qu'il existe une version commerciale de GLPI avec un service support dédié. Vous pouvez également si vous le souhaitez faire un don. Cliquez sur Continuer.



The screenshot shows the GLPI Setup interface. At the top left is the GLPI logo. To its right, the text 'GLPI SETUP' is displayed in orange. Below this, 'Étape 5' is centered. The main heading is 'Une dernière chose avant de démarrer' in orange. The text below explains that users can get help, report bugs, or benefit from preconfigured rules/dictionaries. It mentions the service 'https://services.glpi-network.com' and states it is a commercial service with level 3 support. A button labeled 'Continuer >' is at the bottom left.

GLPI

GLPI SETUP

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 préconfigurés ?

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 >

L'installation est désormais terminée. Notez bien les identifiants par défaut qui permettront de rentrer dans l'interface web de GLPI. Ils seront à changer par la suite. Cliquez sur Utiliser GLPI.



The screenshot shows the GLPI Setup interface for Step 6. At the top left is the GLPI logo. To its right, the text 'GLPI SETUP' is displayed in orange. Below this, 'Étape 6' is centered. The main heading is 'L'installation est terminée' in orange. The text below states that default identifiers and passwords are provided. A list of default accounts is shown: glpi/glpi for administrator, tech/tech for technician, normal/normal for normal user, and post-only/postonly for postonly user. It also mentions that these accounts can be deleted or modified. A button labeled 'Utiliser GLPI' with a thumbs-up icon is at the bottom left.

GLPI

GLPI SETUP

Étape 6

L'installation est terminée

Les identifiants et mots de passe par défaut sont :

- glpi/glpi pour le compte administrateur
- tech/tech pour le compte technicien
- normal/normal pour le compte normal
- post-only/postonly pour le compte postonly

Vous pouvez supprimer ou modifier ces comptes ainsi que les données initiales.

Utiliser GLPI

Connectez vous avec les **identifiants par défaut** du compte GLPI qui est le super-administrateur.

GLPI

Connexion à votre compte

Identifiant

Mot de passe

Source de connexion

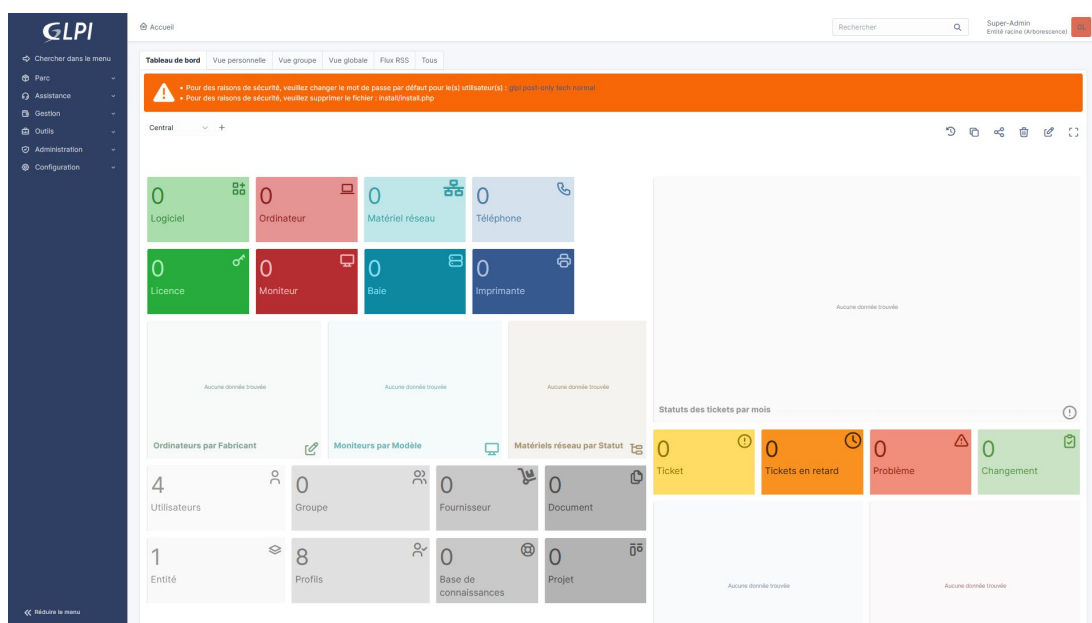
Base interne GLPI

☒ Se souvenir de moi

Se connecter

GLPI Copyright (C) 2015-2023 Teclib' and contributors

Vous voilà maintenant connecté au **tableau de bord** de votre outil GLPI !



Un **message d'avertissement** vous informe que par sécurité il faudra **changer les mots de passe par défaut des 4 utilisateurs** créés automatiquement et **supprimer le fichier « install.php »**.



- 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

Si vous cliquez sur le nom de l'un des utilisateurs, vous arriverez directement **dans ses configurations**. Vous pourrez alors lui **attribuer un nouveau mot de passe**.

The screenshot shows the GLPI user configuration interface for a user named 'tech'. The left sidebar contains a menu with options like 'Habilitations', 'Groupes', 'Préférences', etc. The main area is titled 'Utilisateur - tech' and contains various input fields for user details. A red rectangle highlights the 'Mot de passe' (Password) and 'Confirmation mot de passe' (Confirm password) fields, which are currently masked with dots. Other fields include 'Identifiant' (Username), 'Nom de famille', 'Prénom', 'Image', 'Fuseau horaire' (Timezone), 'Actif' (Active), 'Courriels' (Emails), 'Valide depuis' (Valid from), 'Valide jusqu'à' (Valid until), 'Téléphone', 'Téléphone mobile', 'Authentification' (Authentication), and 'Catégorie' (Category). A file upload section on the right allows for uploading a file (up to 2 Mio) with a 'Parcourir...' button and a note that no file is currently selected. A note at the bottom states: 'L'utilisation des fuseaux horaires n'a pas été activé. Exécutez la commande "php bin/console glpi:database:enable_timezones" pour l'activer.'

Pour **supprimer le fichier install.php**, la commande est la suivante :

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

En actualisant la page d'accueil de GLPI, **les avertissements auront disparu**.

Votre GLPI est désormais prêt à fonctionner !

Les différents **menus latéraux** vous permettront par exemples de gérer votre parc, vos tickets d'incidents, de centraliser vos contrats, fournisseurs ou autres, de gérer les projets du SI et d'administrer GLPI.

