Création serveur GLPI

Table des matières

I) Présentation de GLPI

Qu'est-ce que GLPI ?

Il s'agit d'un gestionnaire de parc informatique et de suivi de demandes. Il permet donc dans un premier temps de recenser et de gérer plusieurs éléments informatiques comme des ordinateurs ; d'imprimantes, de périphériques en tout genre, etc…

Ensuite, il permet de suivre les tickets de demande ou d'incidents des utilisateurs de l'entreprise.

GLPI est clairement un incontournable dans un système d'informations, sans lui, nous n'avons pas de quoi inventorier les appareils informatiques, ni les demandes utilisateurs.

II) Installation des paquets de base

2.1 Installation de PHP

Nous allons installer PHP et les dépendances avec les commandes suivantes :

```
dnf install php -y
```

```
dnf install 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 -y
```

2.2 Installation de HTTPD

Sur Rocky Linux, Apache s'appelle httpd donc in utilise la commande :

```
dnf install httpd -y
```

2.3 Installation de MariaDB

L'installation de MariaDB est essentielle afin de créer un GLPI, pour la simple et bonne raison que sans base de données, Ni le parc informatique et ni les utilisateurs n'y seront stockés.

Pour installer MariaDB donc, utiliser la commande suivante :

```
dnf install mariadb-server -y
```

2.4 Configuration de MariaDB

Une fois MariaDB installé, nous pouvons le configurer avec la commande suivante :

```
mysql_secure_installation
```

Un long prompt sera alors lancé

```
[root@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):
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] n
 ... skipping.

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

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

Répondre aux questions suivantes :

- `Switch to unix_socket authentication ? No`
- `Change root password ? Yes`
- `Remove anonymous users ? Yes`
- `Disallow root login remotely ? Yes`
- `Remove test database and acces to it ? Yes`
- `Reload privilege tables now ? Yes`

Une fois cela fait, la configuration est terminée. Pour se connecter à la console MariaDB, vous pouvez utiliser la commande suivante :

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

III) Création du GLPI

Avant de réellement installer GLPI, il faut d'abord créer la base de données

3.1 Création de la BDD

Dans la console MariaDB, lancer les commandes suivantes :

```
CREATE DATABASE DB_GLPI;

GRANT ALL PRIVILEGES ON DB_GLPI.* TO AdminGLPI@localhost
IDENTIFIED BY "Azerty12*";

FLUSH PRIVILEGES;
```

Une fois ces commandes tapées, la BDD sera créée.

3.2 Installation de GLPI

Pour installer GLPI sur la machine, nous utiliserons la commande suivante.

`cd /tmp` ← cette commande sert à se positionner dans le fichier /tmp

`wget https://github.com/glpi-project/glpi/releases/download/11.0.6/glpi-11.0.6.tgz`

Décompresser ensuite le fichier .tgz

`tar -xzvf glpi-10.0.18.tgz -C /var/www/`

3.3 Configuration de Apache

Il faut d'abord créer un fichier conf avec la commande :

```
nano /etc/httpd/conf.d/glpi.conf
```

Un fichier vierge se lancera. Il ne reste plus qu'à copier les informations suivantes :

```
<VirtualHost *:80>
    ServerName glpi.sisr.local

    DocumentRoot /var/www/glpi/public

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

        RewriteEngine On

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

Puis valider la fermeture avec Ctrl + X

3.4 Paramétrage de GLPI

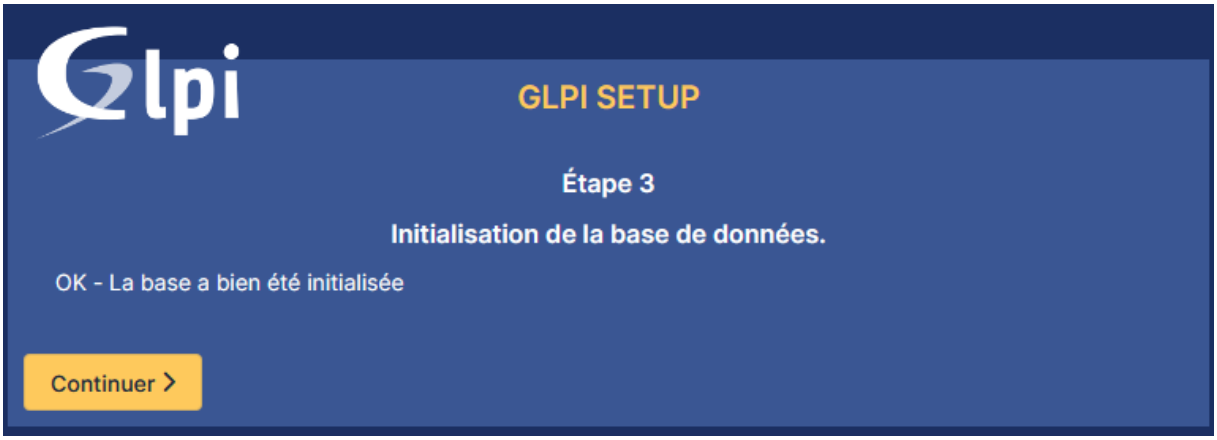
Comme le GLPI est installé sur une VM, il faut donc y accéder depuis le navigateur WEB de notre ordinateur. Il faut donc renseigner l'IP de la machine dans la barre de recherche à la place de l'url que nous avions mis précédemment.

Nous arrivons sur cette page

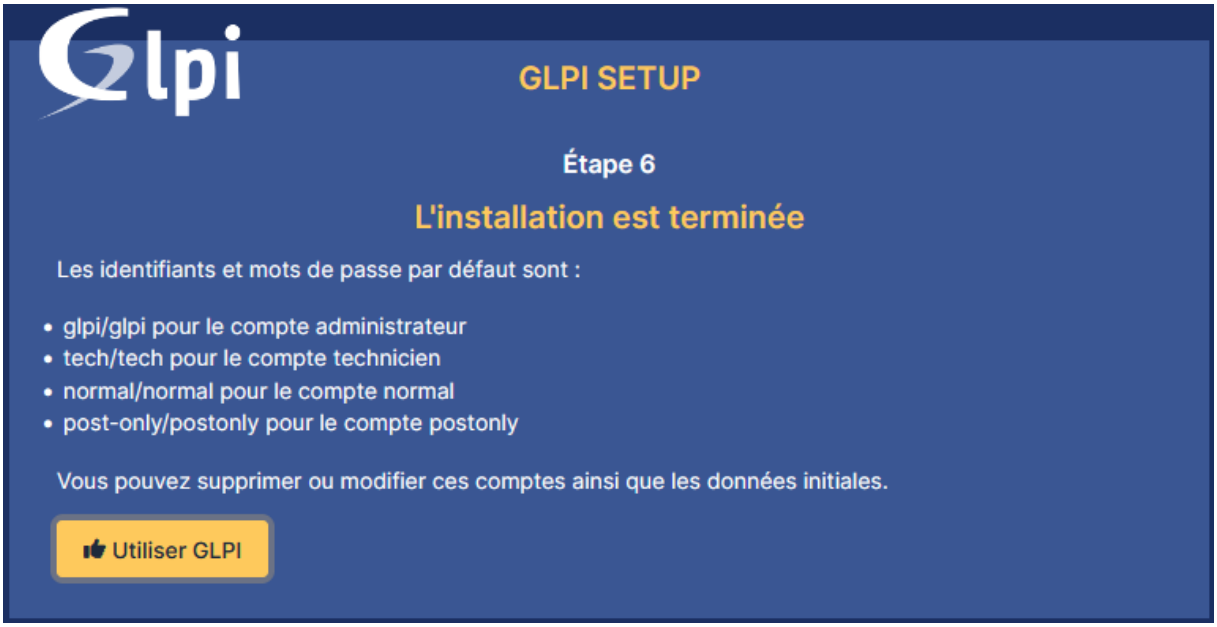
Après avoir validé la langue, GLPI va nous proposer de mettre à jour ou d'installer ce dernier. Evidemment, comme rien n'a été fait, il faut l'installer.

Ici, c'est la page de connexion à la base de données. Comme elle est directement installé sur la VM avec MariaDB, nous avons juste à mettre « localhost » dans l'option « serveur SQL »

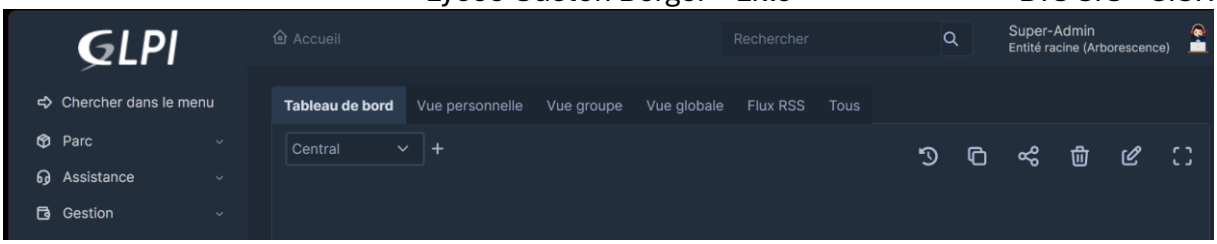
La connexion a bien été initialisée :)



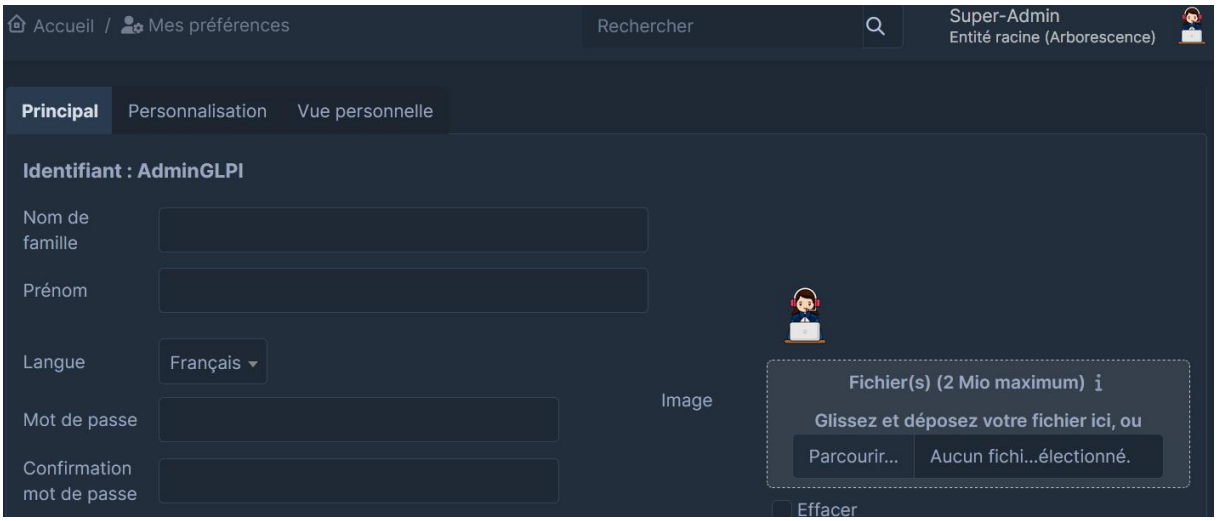
Après avoir ignoré l'étape 4 et 5 (récolte de données et don à l'équipe GLPI), nous arrivons à l'étape 6 qui est celle de la vérification finale de GLPI



Et si nous nous connectons :



Nous sommes bien connecté avec le compte AdminGLPI



Le GLPI est maintenant prêt à être utilisé !

IV) Mise en place du SLA

Une SLA (Service Level Agreement) est un accord documenté entre un fournisseur de services informatiques et un client, définissant les services requis et le niveau de service attendu. Dans GLPI, il est possible de saisir ces SLA afin que le niveau de service attendu par un client soit conforme au contrat signé entre les 2 parties.

La configuration se fait en plusieurs étapes :

1. Définir les temps d'intervention via le calendrier (heures ouvrables, astreinte, etc. plusieurs calendriers possibles).
2. Définition des SLA (Service Level Agreements)
    - Temps maximum de prise en charge (TTO)
    - Temps maximum de résolution (TTR - Time To Resolve)
3. Définition des OLA (Operational Level Agreement)
    - Temps maximum de prise en charge (TTO)
    - Temps maximum de résolution (TTR - Time To Resolve)
4. Mise en œuvre des règles d'affectation SLA (niveau d'escalade)

4.1 Exemple de SLA

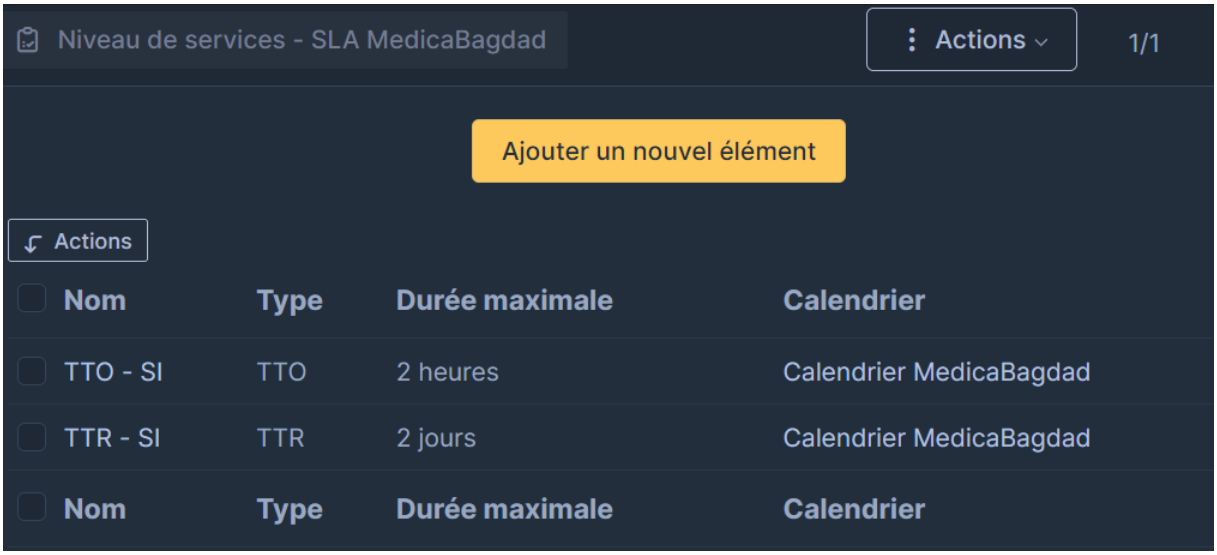
TTO (Temps Maximum de Prise en Charge) :

Si le ticket n'est pas attribué au bout de 3 heures, le SLA sera alors automatiquement rappelé aux utilisateurs.

TTR (Temps Maximum de Résolution) :

Si au bout de 5 jours le ticket n'est pas résolu ou clos, il sera automatiquement escaladé en très haute urgence et en très haute priorité.

4.2 Exemple de OLA



TTO :

Si le ticket n'est pas pris en charge au bout de 2h, il sera automatiquement attribué aux techniciens.

TTR :

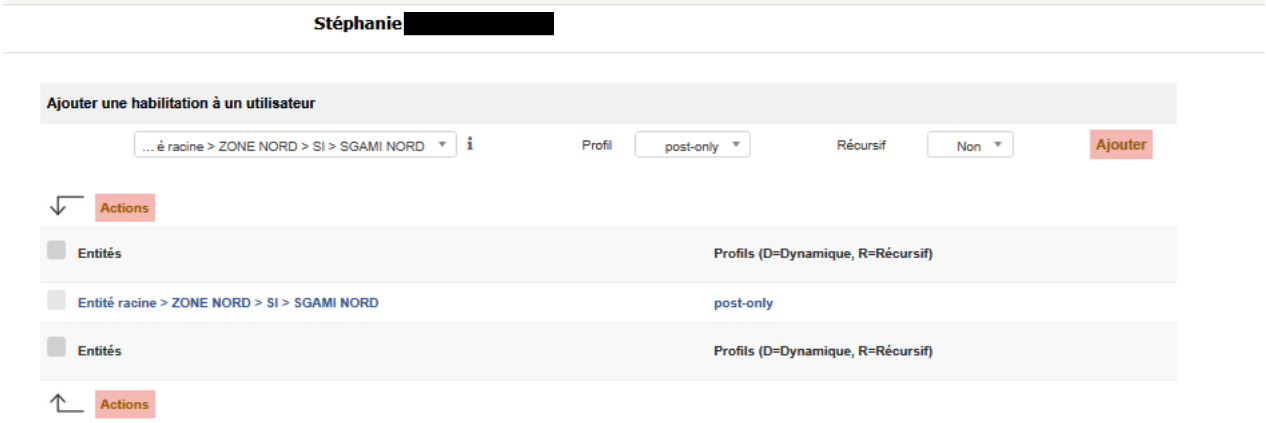
Si le ticket n'est pas résolu ou clos au bout de 2 jours, il sera mis en haute urgence.

V) Présentation des différents types d'utilisateurs

Les exemples ici seront ceux des agents travaillants au sein de mon entreprise (le SGAMI-Nord). Il y aura donc certaines parties masquées pour raison de secret professionnel.

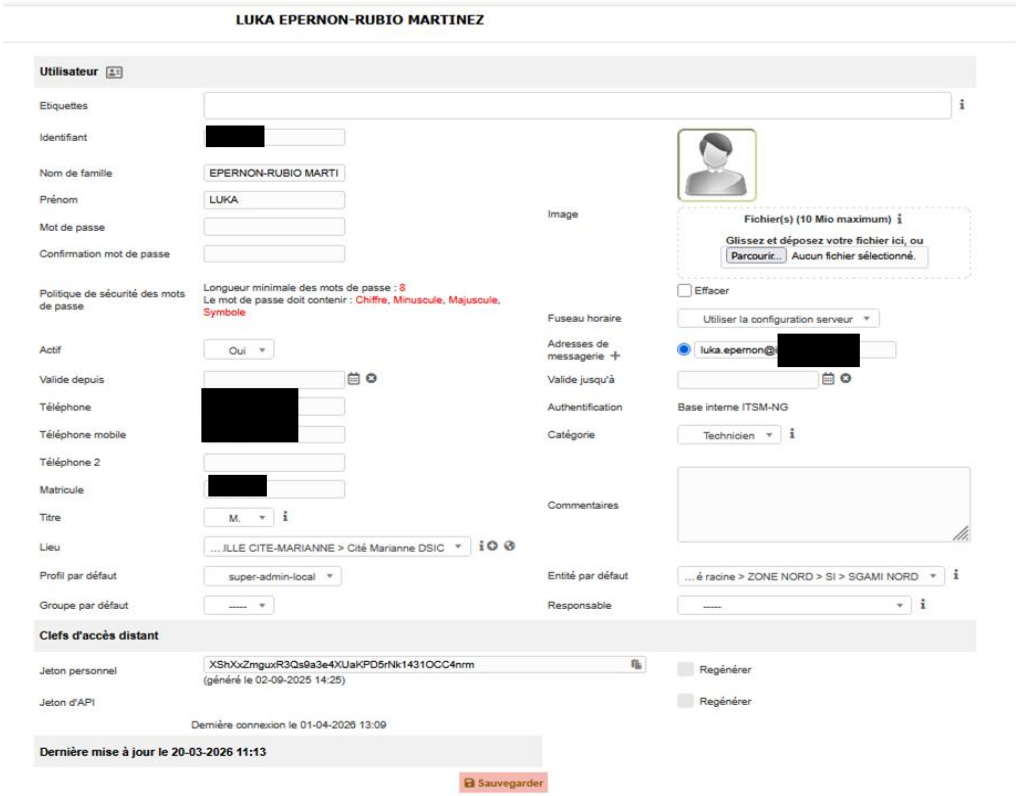
5.1 Utilisateur basique

Voici un exemple d'utilisateur basique :



5.2 Technicien

Voici un exemple de technicien :



5.3 Administrateur zonal