DOCUMENTATION GLPI

Sommaire :

- Installation et configuration de Debian
- Installation du socle LAMP
- Installation et configuration de GLPI
- Installation et configuration du plugin OCSNG
- Synchronisation entre OCS et GLPI
- Collecteur Oauth IMAP
- LDAP

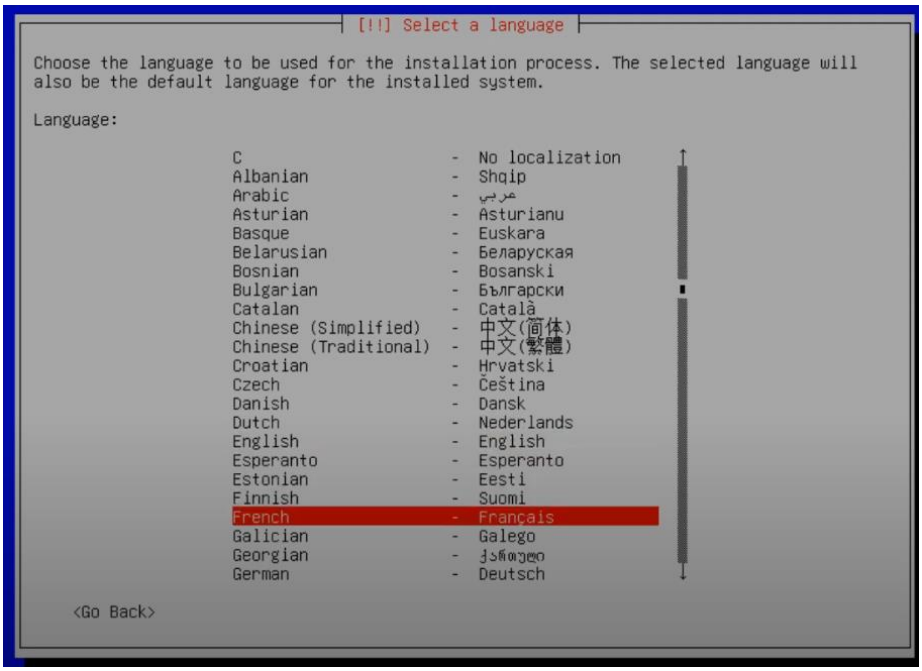
Tous ce qui se trouve en ROUGE sont des chants que vous pouvez modifier celons vos besoins

Conseille : prendre des instantané/snapshot après chaque étape

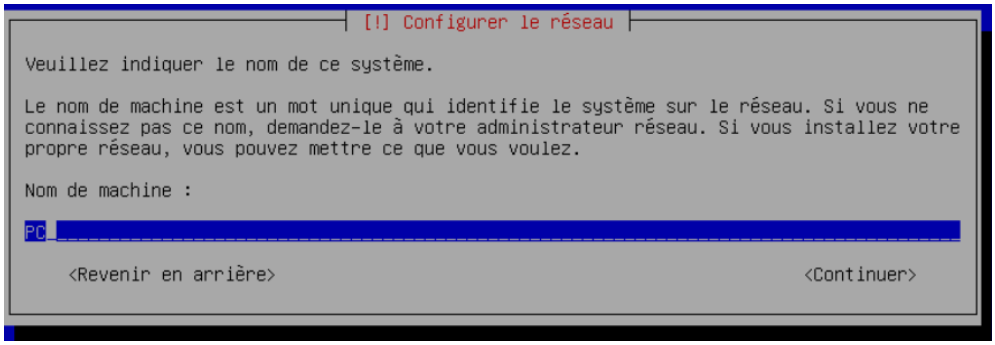
Installation et Configuration de DEBIAN.

Recherchez la version la plus récente de Debian. Dans mon cas, il s'agissait de **Debian 12.10.0**.

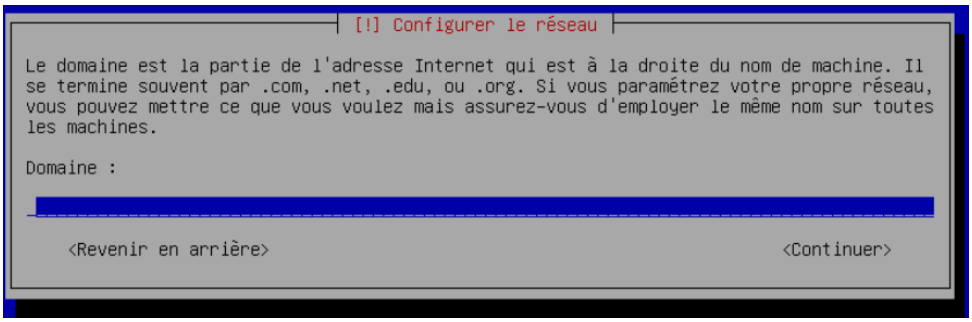
1. J'ai personnellement choisi l'installation sans interface graphique de DEBIAN en sélectionnant dans le premier menu "Install"



On vous demandera de choisir un nom pour votre machine :



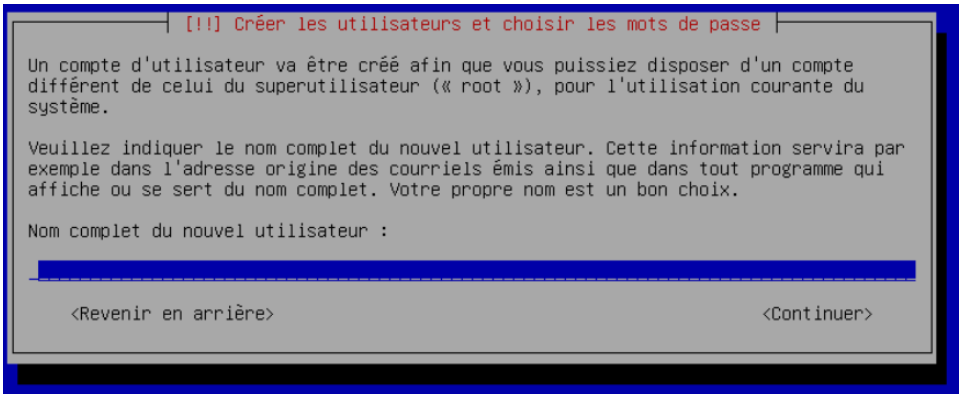
Dans le menu suivant, on vous demandera un nom de domaine, Si votre installation n'est pas à disposition d'une entreprise, cette étape est optionnelle pour vous. Laissez le champ vide et appuyez sur entrée :



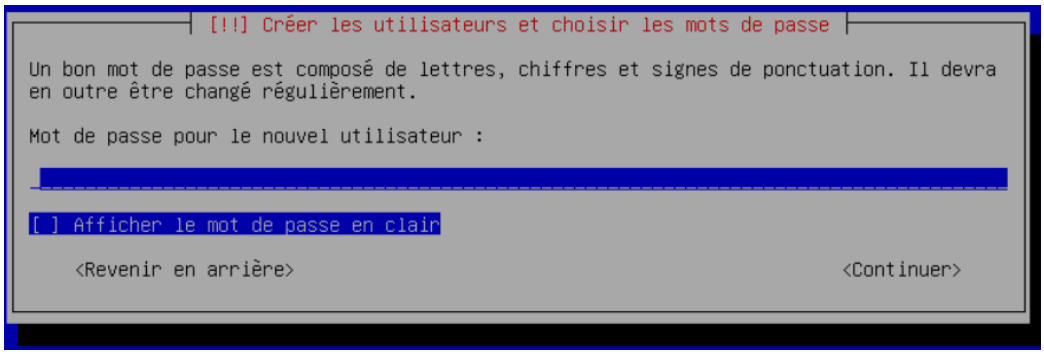
On vous demandera ensuite un mot de passe Root :

Une confirmation du mot de passe vous sera ensuite demandée.

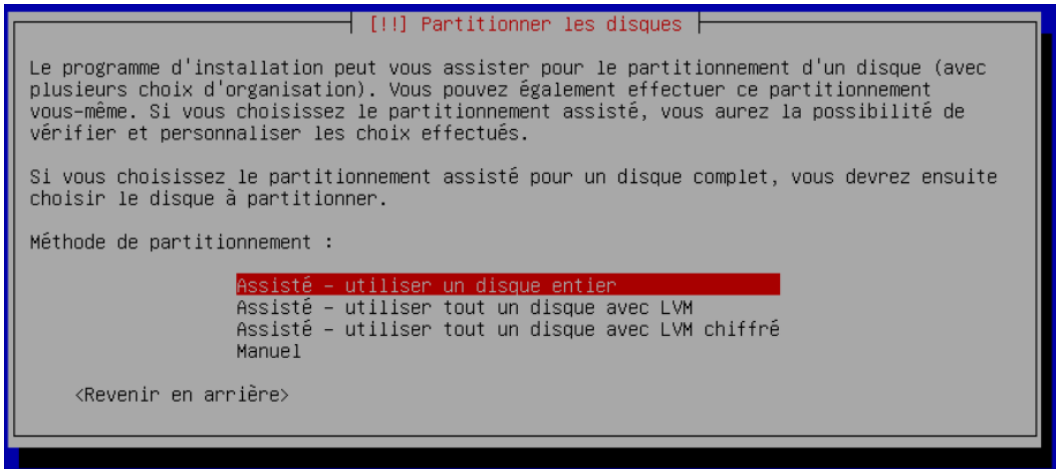
On vous demandera ensuite de créer votre utilisateur :



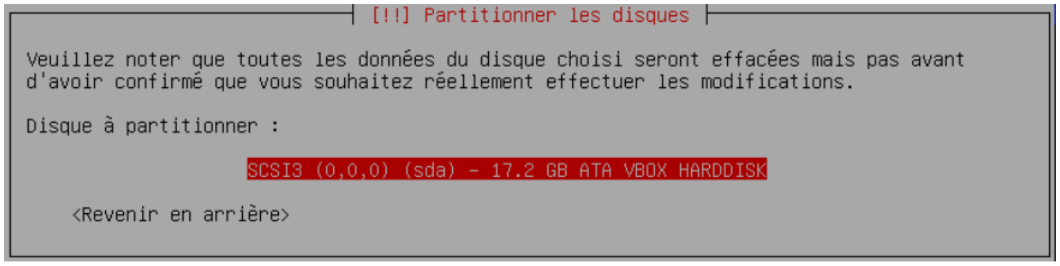
Indiquez un nom, une confirmation vous sera demandée pour valider que votre login sera le même. Par la suite un mot de passe vous sera demandé ainsi que la confirmation de celui-ci



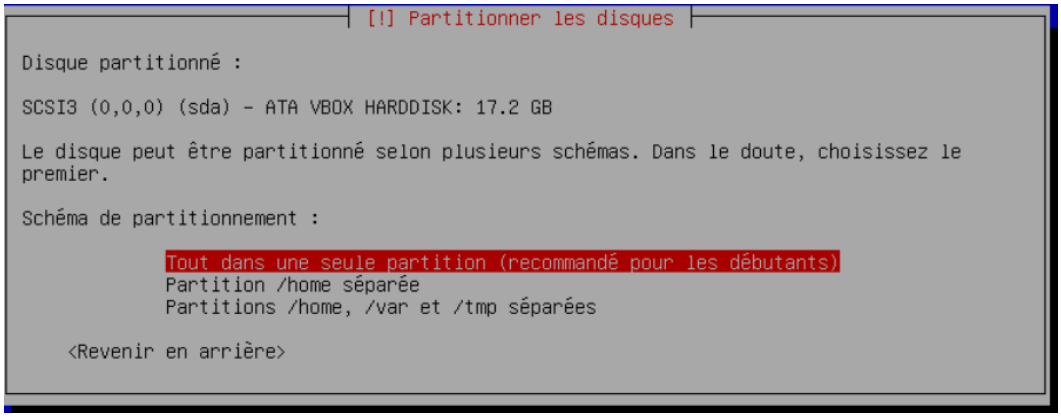
Ensuite vient le tour de la configuration des disques :



Sur l'écran suivant, on vous demandera sur quel disque vous voulez installer le système d'exploitation, en général vous n'en aurez qu'un ou deux. Choisissez donc celui par défaut et cliquez sur entrée.



Choisissez ensuite la méthode de partitionnement par défaut si vous n'avez pas de besoins spécifiques :



Validez ensuite les changements sur les disques :

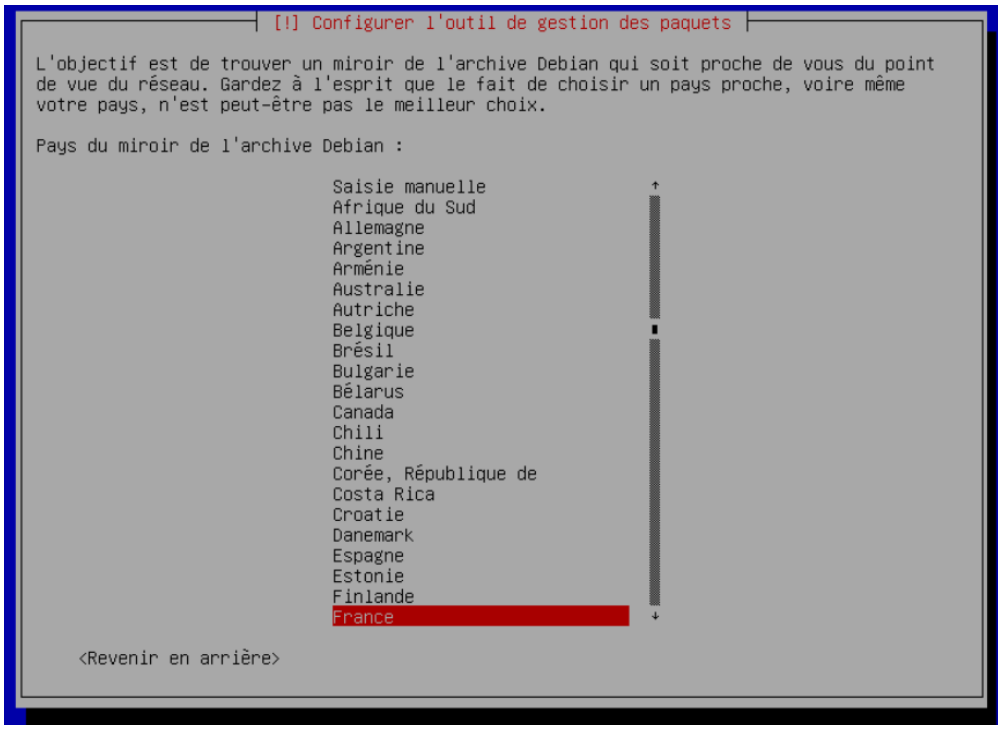
```
[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous
pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point
de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

                Partitionnement assisté
                Configurer le RAID avec gestion logicielle
                Configurer le gestionnaire de volumes logiques (LVM)
                Configurer les volumes chiffrés
                Configurer les volumes iSCSI

                SCSI3 (0,0,0) (sda) - 17.2 GB ATA VBOX HARDDISK
                     n° 1  primaire  12.9 GB    f  ext4    /
                     n° 5  logique    4.3 GB    f  swap    swap

                Annuler les modifications des partitions
                Terminer le partitionnement et appliquer les changements

    <Revenir en arrière>
```

```
[!!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le
cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
   SCSI3 (0,0,0) (sda)

Les partitions suivantes seront formatées :
   partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
   partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

    <Oui>                                                    <Non>
```

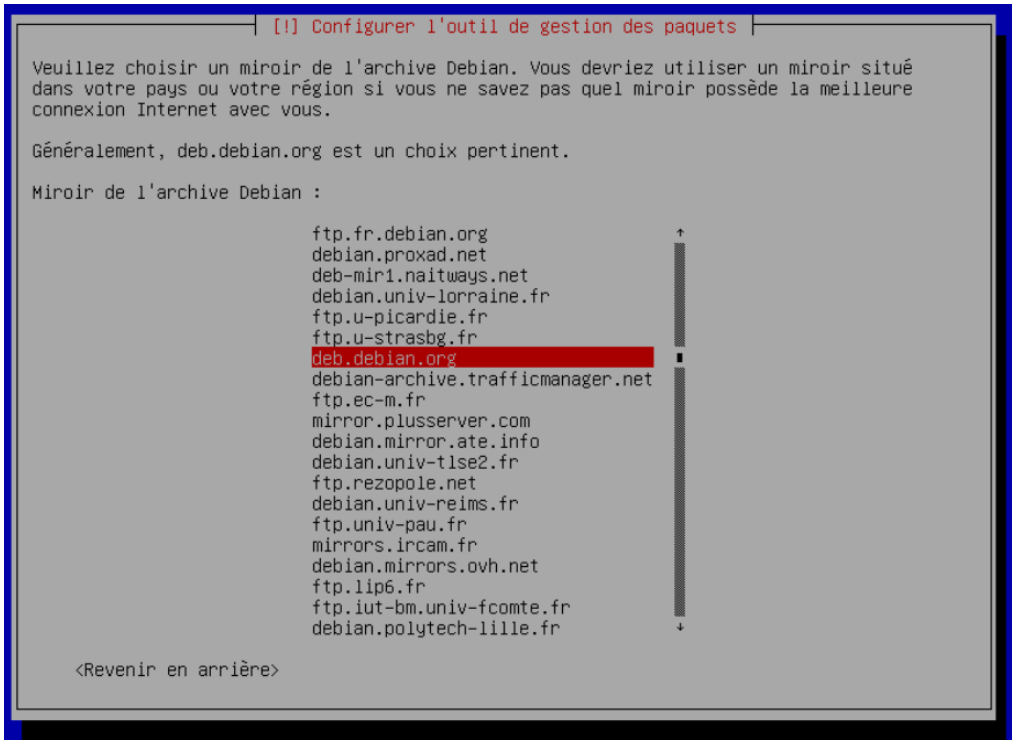
L'installation du système va alors se dérouler. A la fin de celle-ci, on vous demandera si vous avez un autre CD d'installation. Choisissez non et poursuivez :

```
[!] Configurer l'outil de gestion des paquets

Le support d'installation (CD ou DVD) a été analysé. Son étiquette est :

Debian GNU/Linux 10.6.0 _Buster_ - Official amd64 NETINST 20200926-10:16

Vous pouvez maintenant analyser des CD ou DVD supplémentaires qui seront utilisés par
l'outil de gestion des paquets (APT). En principe, ils devraient appartenir au même
ensemble de supports que le CD ou le DVD d'installation. Si vous n'avez pas d'autres CD
ou DVD disponibles, vous pouvez passer cette étape.

Si vous souhaitez analyser un autre CD ou DVD, veuillez le mettre en place maintenant.

Faut-il analyser un autre CD ou DVD ?

    <Revenir en arrière>                                <Oui>    <Non>
```

On vous demandera ensuite de choisir un dépôt des mises à jour. Choisissez votre pays :



Choisissez ensuite le dépôt vers lequel vous souhaitez récupérer vos mises à jour. Choisissez celui par défaut si vous n'avez pas de besoins spécifiques :



L'utilitaire vous demandera ensuite si vous disposez d'un proxy sur votre réseau. Cette étape n'est en général pas utile dans un environnement privé. Cliquez simplement sur entrée :

```
┤ [!] Configurer l'outil de gestion des paquets ├

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder
au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée
« http://[[utilisateur][:mot-de-passe]@]hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

    <Revenir en arrière>                                    <Continuer>
```

L'utilitaire va ensuite télécharger des paquets de mises à jour. Il vous demandera ensuite si vous souhaitez participer à l'étude sur l'utilisation des paquets. Ceci n'est pas obligatoire, vous pouvez choisir non.

```
┤ [!] Configuration de popularity-contest ├

Le système peut envoyer anonymement aux responsables de la distribution des statistiques
sur les paquets que vous utilisez le plus souvent. Ces informations influencent le choix
des paquets qui sont placés sur le premier CD de la distribution.

Si vous choisissez de participer, un script enverra automatiquement chaque semaine les
statistiques aux responsables. Elles peuvent être consultées sur
https://popcon.debian.org/.

Vous pourrez à tout moment modifier votre choix en exécutant « dpkg-reconfigure
popularity-contest ».

Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?

    <Revenir en arrière>                            <Oui>    <Non>
```

Pour la suite l'utilitaire vous demandera quels sont les logiciels dont vous avez besoin dans notre cas serveur web uniquement (pour sélectionner et désélectionner appuyer sur la touche espace) :

```
┤ [!] Sélection des logiciels ├

Actuellement, seul le système de base est installé. Pour adapter l'installation à vos
besoins, vous pouvez choisir d'installer un ou plusieurs ensembles prédéfinis de
logiciels.

Logiciels à installer :

[ ] environnement de bureau Debian
[ ] ... GNOME
[ ] ... Xfce
[ ] ... KDE Plasma
[ ] ... Cinnamon
[ ] ... MATE
[ ] ... LXDE
[ ] ... LXQt
[ ] serveur web
[ ] serveur d'impression
[ ] serveur SSH
[*] utilitaires usuels du système

                    <Continuer>
```

Installez ensuite l'amorceur de démarrage GRUB, choisissez oui :

```
[!] Installer le programme de démarrage GRUB sur un disque dur

Il semble que cette nouvelle installation soit le seul système d'exploitation existant
sur cet ordinateur. Si c'est bien le cas, il est possible d'installer le programme de
démarrage GRUB sur le secteur d'amorçage du premier disque dur.

Attention : si le programme d'installation ne détecte pas un système d'exploitation
installé sur l'ordinateur, la modification du secteur principal d'amorçage empêchera
temporairement ce système de démarrer. Toutefois, le programme de démarrage GRUB pourra
être manuellement reconfiguré plus tard pour permettre ce démarrage.

Installer le programme de démarrage GRUB sur le secteur d'amorçage ?

    <Revenir en arrière>                                    <Oui>    <Non>
```

Choisissez ensuite votre disque pour l'installer dessus :

```
[!] Installer le programme de démarrage GRUB sur un disque dur

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à
installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode
habituelle pour cela est de l'installer sur le secteur d'amorçage principal du premier
disque dur. Vous pouvez, si vous le souhaitez, l'installer ailleurs sur le disque, sur un
autre disque ou même sur une disquette.

Périphérique où sera installé le programme de démarrage :

                    Choix manuel du périphérique
                    /dev/sda  (ata-VBOX_HARDDISK_VBf8125ed9-5d0ad990)

    <Revenir en arrière>
```

L'installation est désormais terminée :

```
[!!] Terminer l'installation

                    Installation terminée
L'installation est terminée et vous allez pouvoir maintenant démarrer le nouveau système.
Veuillez vérifier que le support d'installation est bien retiré afin que le nouveau
système puisse démarrer et éviter de relancer la procédure d'installation.

    <Revenir en arrière>                                    <Continuer>
```

INSTALATION DU SOCLE LAMP

Commençons par installer ces trois paquets :

apt-get update && apt-get upgrade

apt-get install apache2 php mariadb-server

Puis, nous allons installer toutes les extensions nécessaires au bon fonctionnement de GLPI :

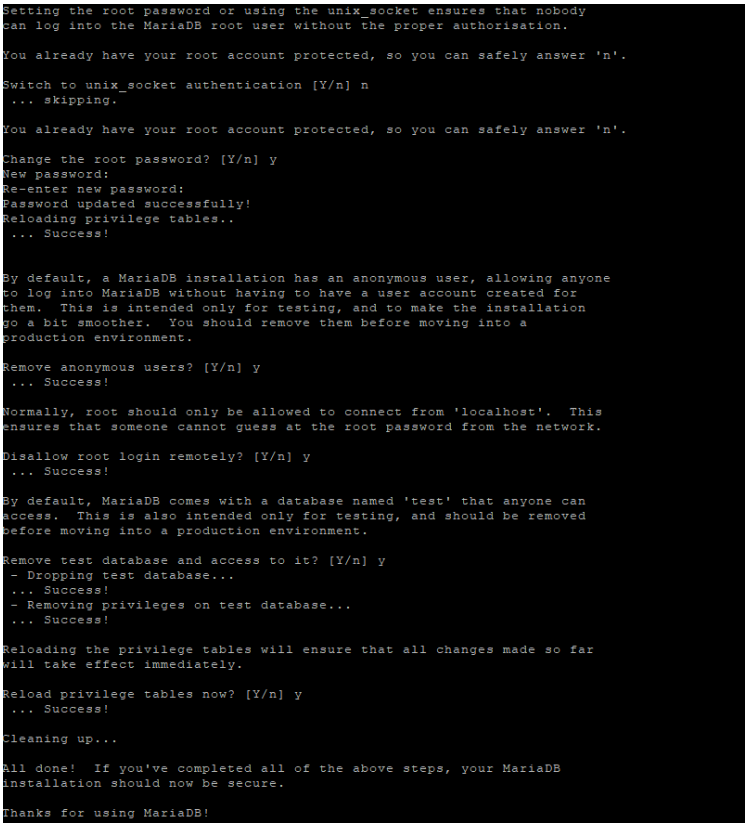
#apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apcu php-ldap

Préparer une base de données pour GLPI

Nous allons préparer MariaDB pour qu'il puisse héberger la base de données de GLPI.
La première action à effectuer, c'est d'exécuter la commande ci-dessous pour **effectuer le minimum syndical en matière de sécurisation de MariaDB** :

#mysql_secure_installation

(zoomer l'image pour savoir se qu'il faut entrer)



```
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
 ... 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] y
 ... 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] y
 - 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] y
 ... 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!
```

Ensuite, nous allons créer **une base de données dédiée pour GLPI** et celle-ci sera accessible par **un utilisateur dédié**. Hors de question d'utiliser le compte root de MariaDB : une base de données = un utilisateur.

Connectez-vous à votre instance MariaDB :

#mysql -u root -p

Puis, nous allons exécuter les **requêtes SQL** ci-dessous pour **créer la base de données ainsi que l'utilisateur** avec **le mot de passe** (que vous changez, bien sûr). Cet utilisateur aura tous les droits sur cette base de données (et uniquement sur celle-ci) :

CREATE DATABASE dbglpi;
CREATE USER "glpi_admin"@"localhost " IDENTIFIED BY " MotDePasseRobuste ";
GRANT ALL PRIVILEGES ON dbglpi.* TO " glpi_adm" @" localhost" ;
FLUSH PRIVILEGES;
EXIT ;

Exemple :

```
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.11.3-MariaDB-1 Debian 12

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 db23_glpi;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON db23_glpi.* TO glpi_adm@localhost IDENTIFIED BY
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> EXIT
Bye
glpi_adm@SRV-GLPI:~$
```

Télécharger GLPI et préparer son installation

La prochaine étape consiste à télécharger l'archive ".tgz" qui contient les sources d'installation de GLPI. A partir du GitHub de GLPI, récupérez le lien vers la dernière version. Ici, c'est la version GLPI 10.0.10 qui est installée. Attention : veiller à prendre la version la plus récente de glpi ici nous somme en 10.0.18 pour cela vous allez sur le site officiel de glpi https://glpi-project.org/fr/telecharger-glpi/ clic droit sur Téléchargement copier l'adresse du lien.

Ensuite vous faite :

#apt install wget

#cd /tmp

#wget https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz

Puis, nous allons exécuter la commande ci-dessous pour **décompresser l'archive .tgz dans le répertoire "/var/www/"**, ce qui donnera le chemin d'accès "**/var/www/glpi**" pour GLPI :

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

Nous allons définir l'utilisateur "**www-data**" correspondant à **Apache2**, en tant que **propriétaire** sur les fichiers GLPI.

#chown www-data /var/www/glpi/ -R

Ensuite, nous allons devoir **créer plusieurs dossiers** et sortir des données de la racine Web (/var/www/glpi) de manière à les stocker dans les nouveaux dossiers que nous allons créer. Ceci va permettre de faire une **installation sécurisée de GLPI, qui suit les recommandations de l'éditeur**.

- **Le répertoire /etc/glpi**

Commencez par **créer le répertoire "/etc/glpi"** qui va recevoir les fichiers de configuration de GLPI. Nous donnons des autorisations à www-data sur ce répertoire car il a besoin de pouvoir y accéder :

#mkdir /etc/glpi

#chown www-data /etc/glpi/

Puis, nous allons déplacer le répertoire "config" de GLPI vers ce nouveau dossier :

#mv /var/www/glpi/config /etc/glpi

- **Le répertoire /var/lib/glpi**

Répétons la même opération avec la création du répertoire "/var/lib/glpi" :

#mkdir /var/lib/glpi

#chown www-data /var/lib/glpi/

Dans lequel nous déplaçons également le dossier "**files**" qui contient la majorité des fichiers de GLPI : CSS, plugins, etc.

#mv /var/www/glpi/files /var/lib/glpi

- **Le répertoire /var/log/glpi**

Terminons par la création du répertoire "**/var/log/glpi**" destiné à stocker les journaux de GLPI. Toujours sur le même principe :

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

- **Créer les fichiers de configuration**

Nous devons configurer GLPI pour qu'il sache où aller chercher les données. Autrement dit, nous allons déclarer les nouveaux répertoires fraichement créés.

Nous allons créer ce premier fichier :

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

Afin d'ajouter le contenu ci-dessous qui indique le chemin vers le **répertoire de configuration** :

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

Ensuite, nous allons créer ce second fichier :

#nano /etc/glpi/local_define.php

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

Préparer la configuration Apache2

Nous allons créer un nouveau fichier de configuration qui va permettre de configurer le VirtualHost dédié à GLPI par exemple le **« nomduserveur** ».conf. L'idéal étant d'avoir un nom de domaine (même interne) pour accéder à GLPI afin de pouvoir positionner un certificat SSL par la suite.

#nano /etc/apache2/sites-available/ « nom du serveur » .conf

Ce qui donne la configuration suivante (selon le modèle officiel de la documentation) :

```
<VirtualHost *:80>
ServerName nom du serveur

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

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

Quand la configuration est prête, enregistrez le fichier.

Puis, nous allons **activer ce nouveau site dans Apache2** :

#a2ensite « nom su serveur ».conf

#a2dissite 000-default.conf

#a2enmod rewrite

#systemctl restart apache2

Utilisation de PHP8.2-FPM avec Apache2

l est recommandé d'utiliser PHP-FPM car il est plus performant et se présente comme un service indépendant. Dans l'autre mode, chaque processus Apache2 exécute son propre moteur de scripts PHP.
Si vous souhaitez utiliser PHP-FPM, suivez les étapes ci-dessous. Sinon, passez à la suite mais veillez à configurer l'option "session.cookie_httponly" évoquée ci-dessous

Nous allons commencer par **installer PHP8.2-FPM** avec la commande suivante :

#apt-get install php8.2-fpm

Puis, nous allons activer deux modules dans Apache et la configuration de PHP-FPM, avant de recharger Apache2 :

#a2enmod proxy_fcgi setenvif
#a2enconf php8.2-fpm
#systemctl reload apache2

Pour **configurer PHP-FPM pour Apache2**, nous n'allons pas éditer le fichier "**/etc/php/8.2/apache2/php.ini**" mais **plutôt** ce fichier :

#nano /etc/php/8.2/fpm/php.ini

Dans ce fichier, recherchez l'option "**session.cookie_httponly**" et indiquez la valeur "on" pour l'activer, afin de protéger les cookies de GLPI.

session.cookie_httponly = on

Enregistrez le fichier quand c'est fait. Pour appliquer les modifications, nous devons redémarrer PHP-FPM :

#systemctl restart php8.2-fpm.service

Pour finir, nous devons **modifier notre VirtualHost** pour préciser à Apache2 que PHP-FPM doit être utilisé pour les fichiers PHP :

#nano /etc/apache2/sites-available/ « nom du serveur » .conf

On y ajoute :

```
<FilesMatch \.php$>
SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
</FilesMatch>
```

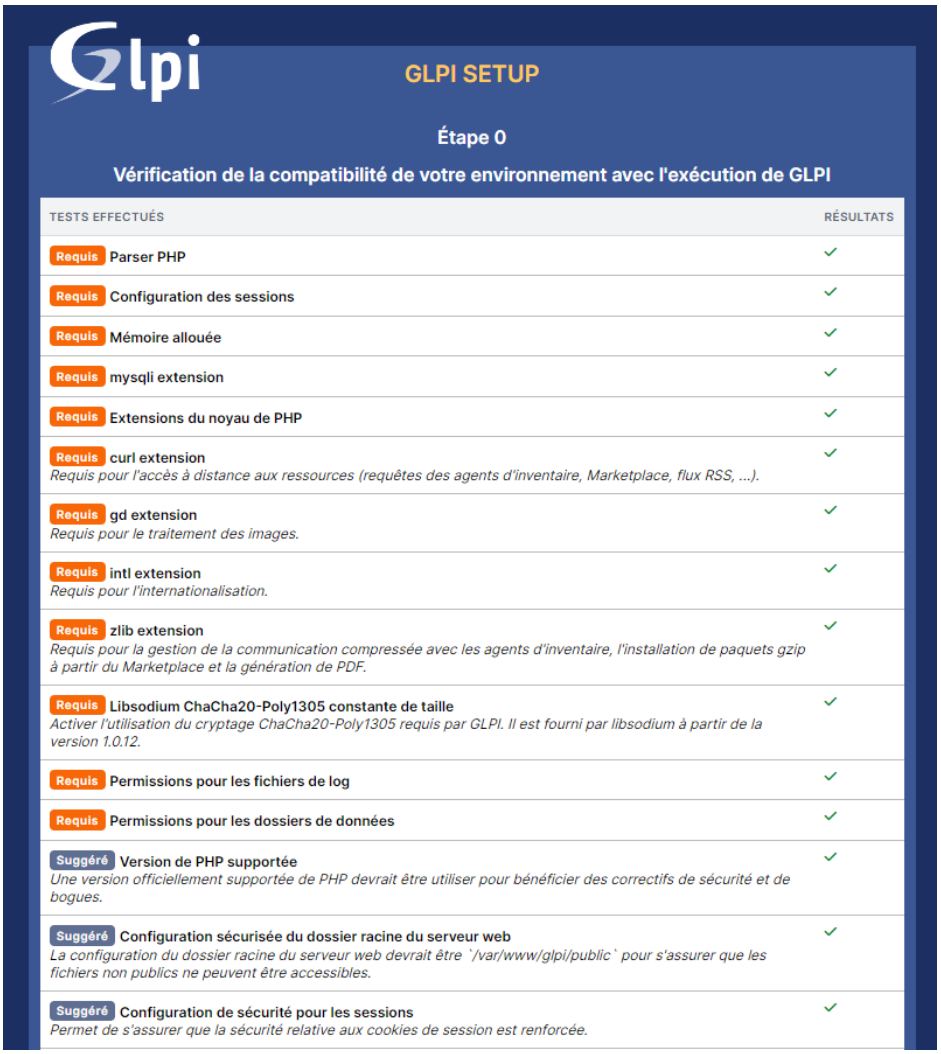
Quand c'est fait, relancer Apache2 :
#systemctl restart apache2

Installation de GLPI

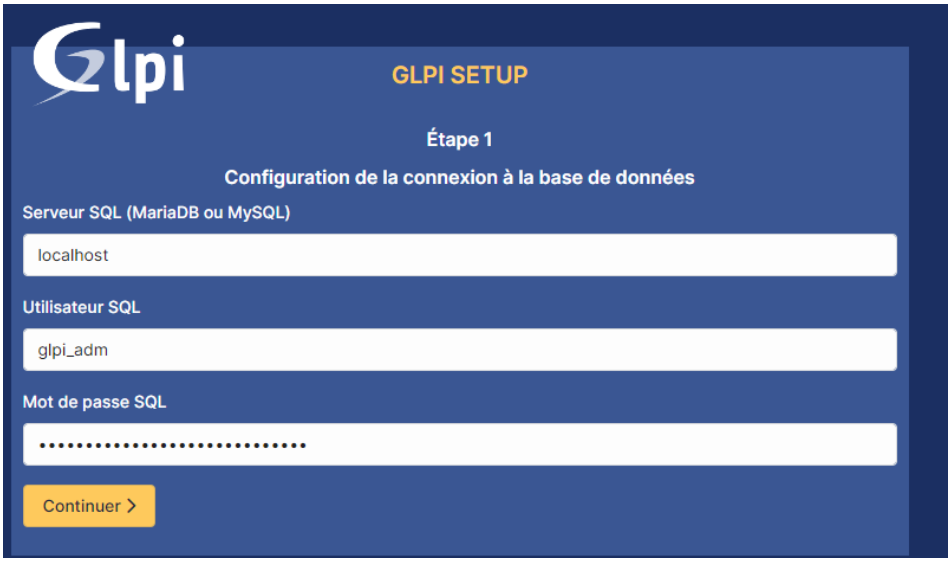
Si vous avez suivi toutes les étapes correctement, vous devriez arriver sur cette page.
Nous allons commencer par choisir la langue.

Puisqu'il s'agit d'une nouvelle installation, nous cliquons sur "**Installer**".

Etape importante : **GLPI vérifie la configuration de notre serveur** pour déterminer si tous les prérequis sont respectés. Tout est bon, donc nous pouvons continuer.

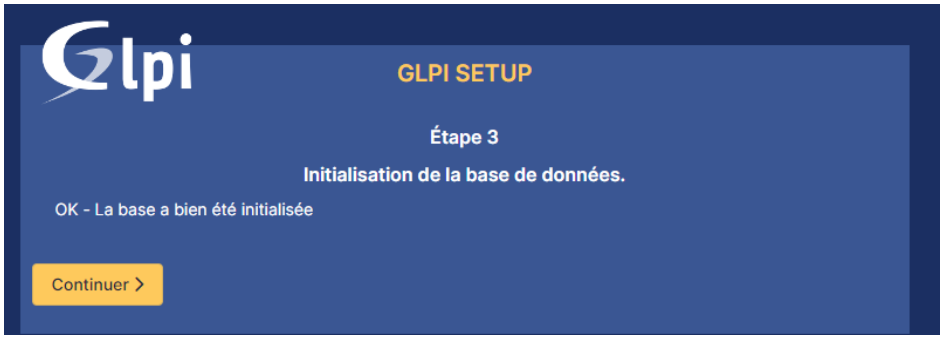


Ensuite on indique "**localhost**" en tant que serveur SQL puisque MariaDB ,puis entrer votre utilisateur et votre mot de passe associe (cela correspond a vos information de Base de donnés)

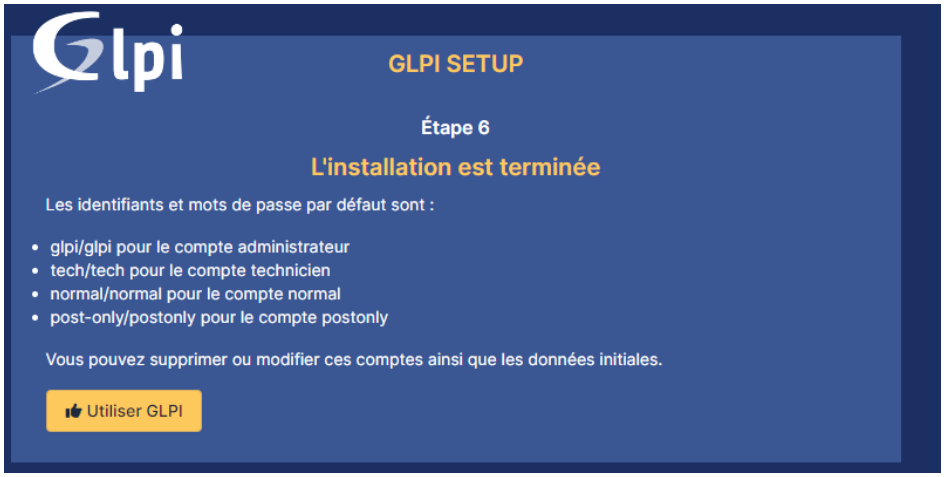


Après avoir cliqué sur "**Continuer**", nous devons choisir la base de données créée précédemment exemple ici :"**db23_glpi**".

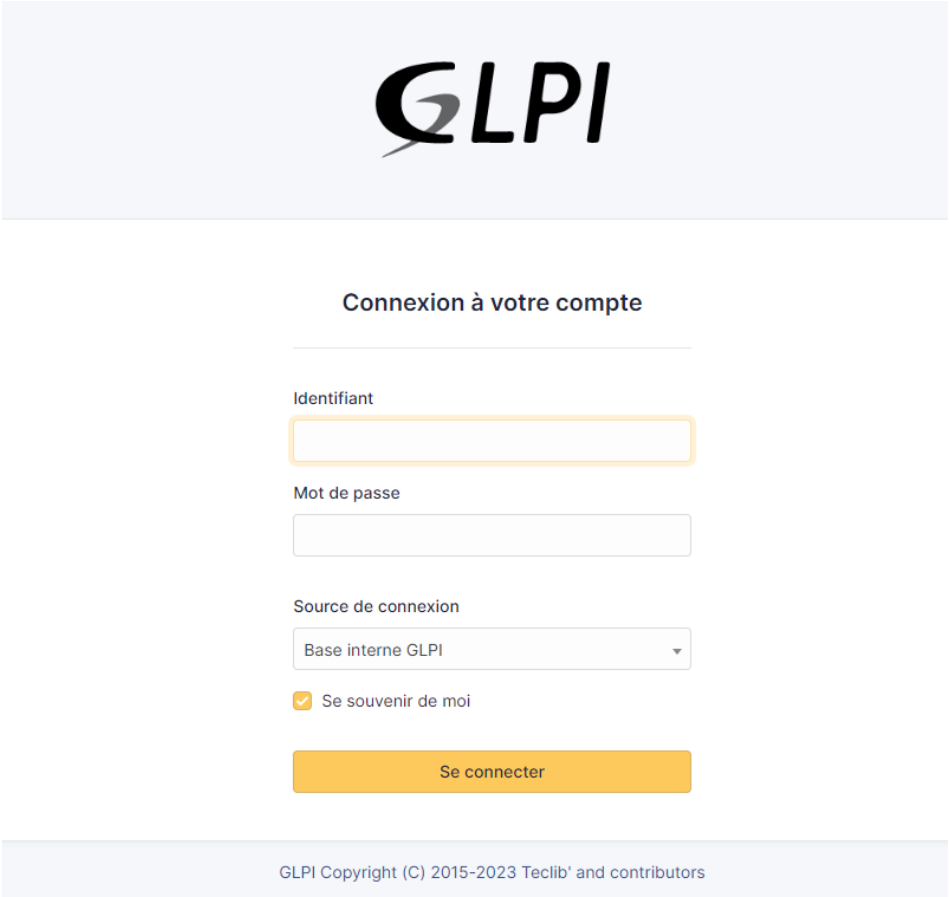
- Il est possible qu'il est une page erreur accès refusé si le chargement est trop long ils suffit juste de cliquer sur retourner à la page précédente et vous tomberez sur la page de connexion de l'interface GLPI .



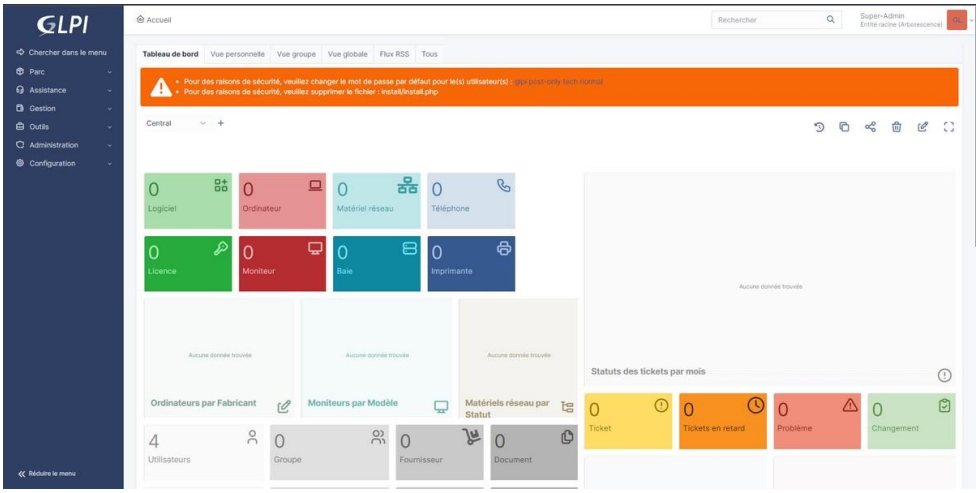
Faite continuer



Nous allons donc nous connecter avec le compte "glpi" et le mot de passe "glpi" pour la première connexion



Bienvenue sur votre nouveau serveur GLPI !



Même si l'installation est terminée, nous avons encore quelques actions à réaliser pour la finaliser :

- Changer le mot de passe de tous les comptes par défaut (cliquez sur les liens situés dans l'encadré orange)

- Supprimer le fichier "install.php" puisqu'il n'est plus nécessaire et représente un risque (relancer l'installation)

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

PLUGINS OCSNG

Nous allons maintenant voir l'installation du plugins OCS pour lier OCS INVENTORY NG qui est une application permettant de réaliser un inventaire sur la configuration matérielle des machines du réseau, sur les logiciels qui y sont installés et de visualiser ces informations grâce à une interface web. (vous pourrez possiblement adapter cette partie avec un plugin qui correspond à votre inventaire).

Nous nous rendons dans le dossier des plugins de GLPI suivant l'emplacement de votre fichier

#cd /var/www555NAN/22/glpi/plugins

Ou

#cd /var/www/html/glpi/plugins

Puis nous téléchargeons le plugin qui sert à lier OCS à GLPI. Attention : prendre la version du plugin la plus récente ici c'est glpi-ocsinventoryng-2.0.4.tar.bz2 :

Dans le cas où le plugin est en bz2 on fait

#apt install bzip2

#wget https://github.com/pluginsGLPI/ocsinventoryng/releases/download/2.0.4/glpi-ocsinventoryng-2.0.4.tar.bz2

#tar -tvjf glpi-ocsinventoryng-2.0.4.tar.bz2

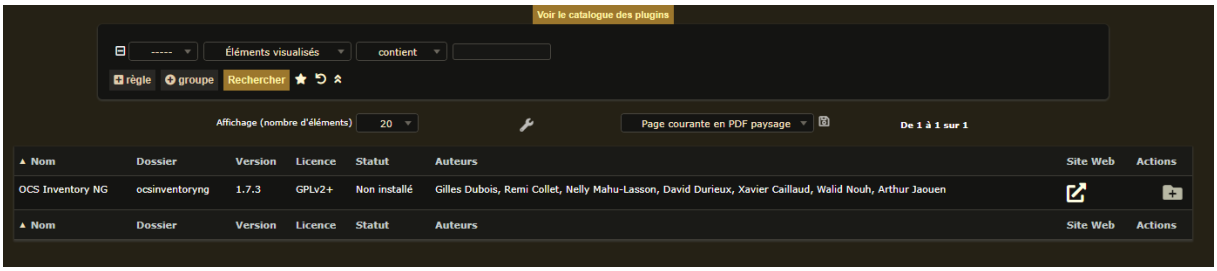
#tar -jxvf glpi-ocsinventoryng-2.0.4.tar.bz2

Sinon si le fichier est en tgz (exemple avec une ancienne version) on fait :

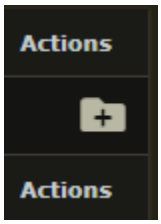
#wget https://github.com/pluginsGLPI/ocsinventoryng/releases/download/1.7.3/glpi-ocsinventoryng-1.7.3.tar.gz

#tar -xf glpi-ocsinventoryng-1.7.3.tar.gz

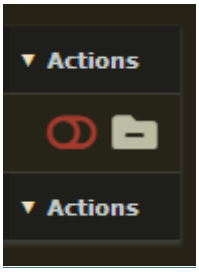
Maintenant nous pouvons actualiser GLPI ; Nous constatons que le plugin apparait dans la liste.



Cependant, le statut du plugin est défini comme "Non installé". Nous allons donc cliquer sur le bouton ci-dessous pour installer le plugin.

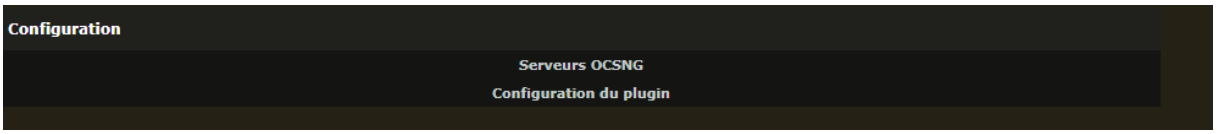


Une fois le chargement terminé, nous allons pouvoir activer le plugin en cliquant sur le bouton ci-dessous :

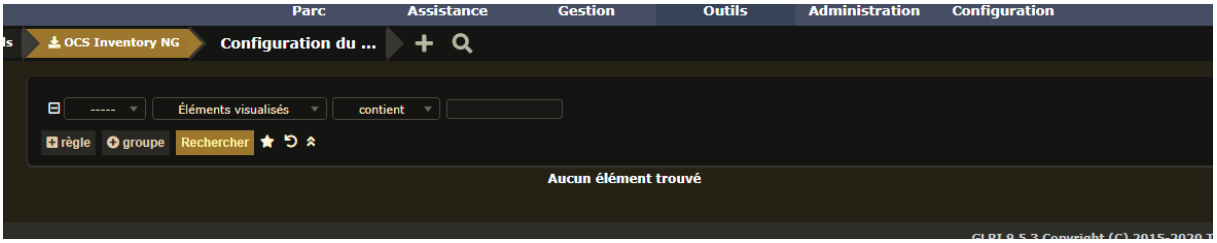


Cela a pour conséquences d'activer le plugin comme ci-dessous :

Soit dans la colonne « action » soit en passent par Outils > OSC Inventory NG nous allons cliquer sur "Serveur OCSNG".

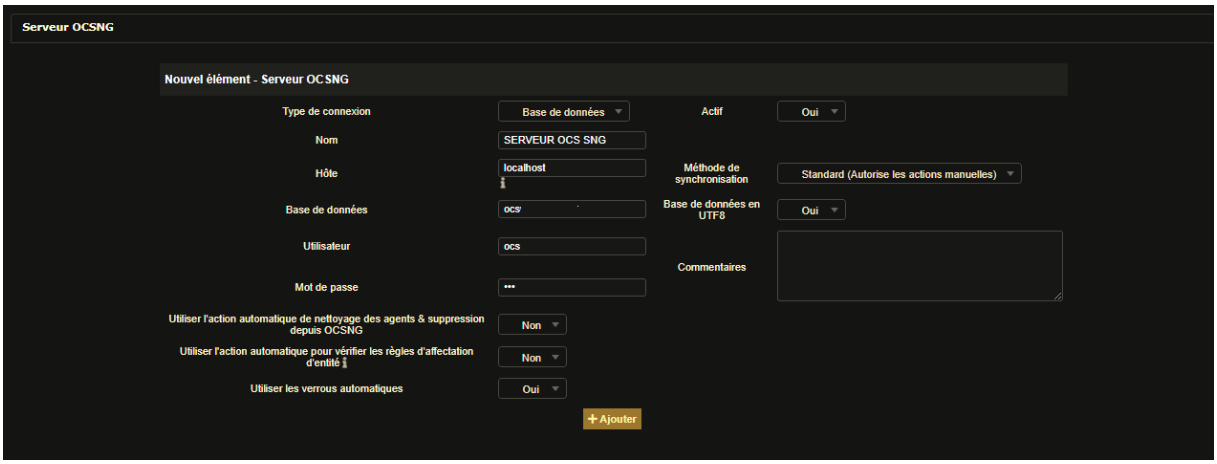


Puis nous allons cliquer sur le "+" (à gauche de la loupe).

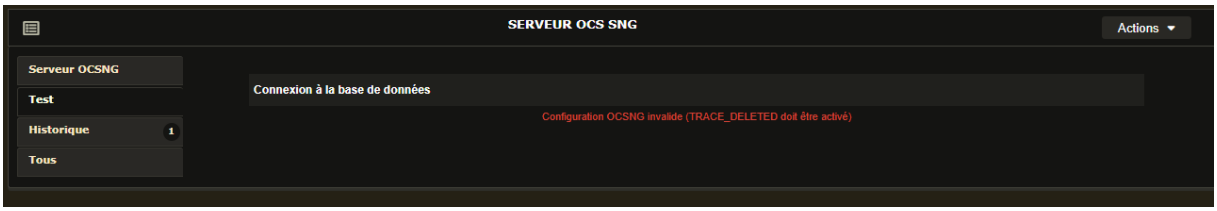


Ensuite, nous allons remplir le formulaire comme ci-dessous (puis cliquez sur "+ Ajouter") Remarque : le formulaire est basé sur les informations de votre base de donné de ocs.

On peut retrouver ces infos dans : nano /usr/share/ocsinventory-reports/ocsreports/dbconfig.inc.php



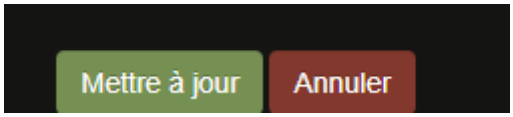
Puis aller sur « Tester ».



Pour corriger cette erreur, nous allons aller sur l'interface web d'OCS. Dans le menu "Configuration" nous allons cliquer sur "Configuration Générale" :

Puis nous allons cliquer sur "ON" dans la catégorie "TRACE_DELETED" :

Puis, tout en bas de la page, nous allons cliquer sur "Mettre à jour" :



Nous pouvons retourner sur GLPI et actualiser la page de test. En voici le résultat :

Si malgré tout cela ne marche pas faite les étapes suivantes sinon passer à la suite :

Dans glpi et ocs

#nano /etc/myslq/mariadb.conf.d/50-server.cnf

Remplacer

Bind- adresse = 127.0.0.1 par Bind- adresse = 0.0.0.0

```
#bind-address            = 127.0.0.1
bind-address             = 0.0.0.0
```

#systmctl restart mariadb

Dans ocs :

Mysql -p

Le mot de passe de base de données sinon faite Entrer puis :

GRANT ALL PRIVILEGES ON nom de la base de donne d'ocs .* TO utilisateur_ocs @ IP de votre Glpi IDENTIFIED BY "MotDePasseRobuste";

(Facultatif) ouvrir le port 3306 :

#apt install ufw
Où
#apt-get install ufw
#ufw allow 3306zc

Dans le Glpi vous faite :

#mysql -u utilisateur_ocs -p -h Ip_OCS nom de la base de donne_ocs

Entre le mot de passe de la base de données

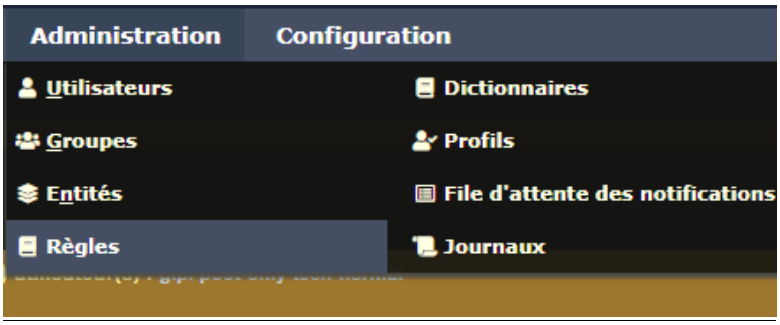
Maintenant on peut retourner sur le formulaire de l'interface de glpi dans par Outils > OSC Inventory NG

On remplit les cases avec les infos de la basse de donne de ocs sauf qu'on remplace localhost par l'IP d'ocs dans la case hôte

Retester la connexion

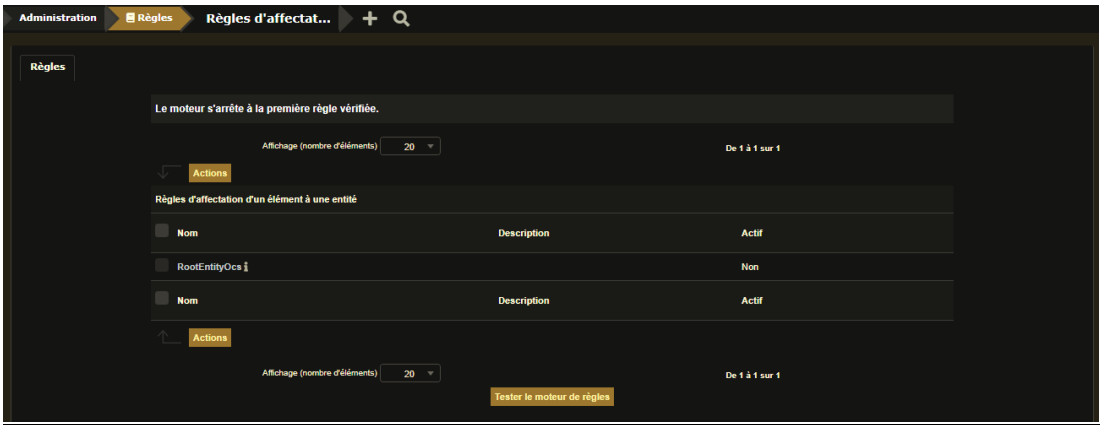
Créations des règles de filtrage de GLPI

Pour que l'étape suivante fonctionne, nous devons au préalable créer des règles de filtrage GLPI. Pour cela nous allons aller dans "Administration" puis "Règles".

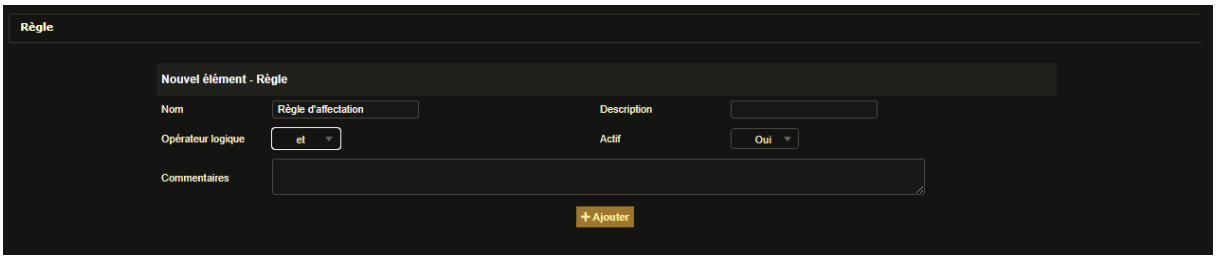


Nous allons premièrement cliquer sur "Règles d'affectation d'un élément à une entité".

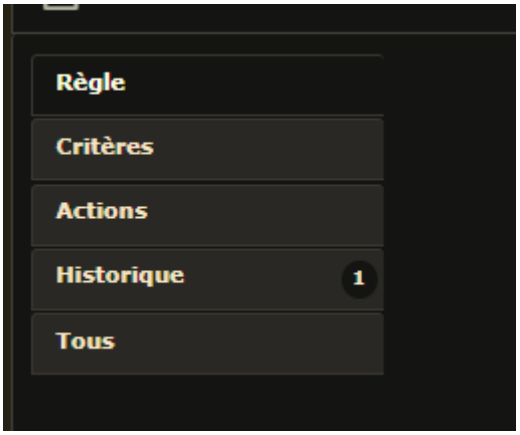
Puis, nous allons cliquer sur le + en haut de l'écran :



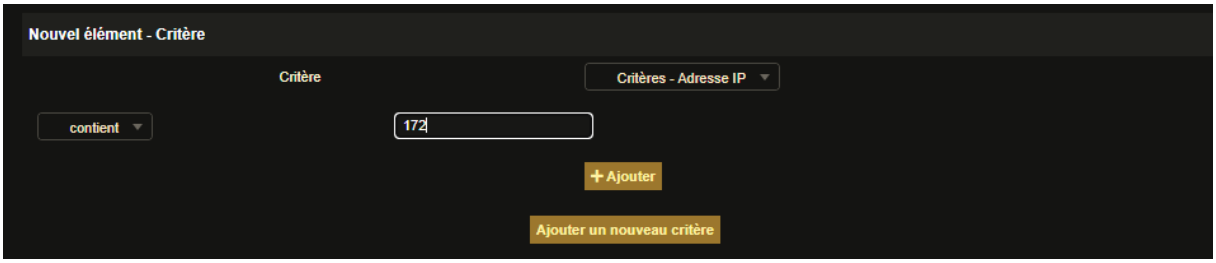
Nous allons créer la règle suivante :



Puis nous allons cliquer sur "Critères" et nous allons cliquer sur "Ajouter un nouveau critère" :

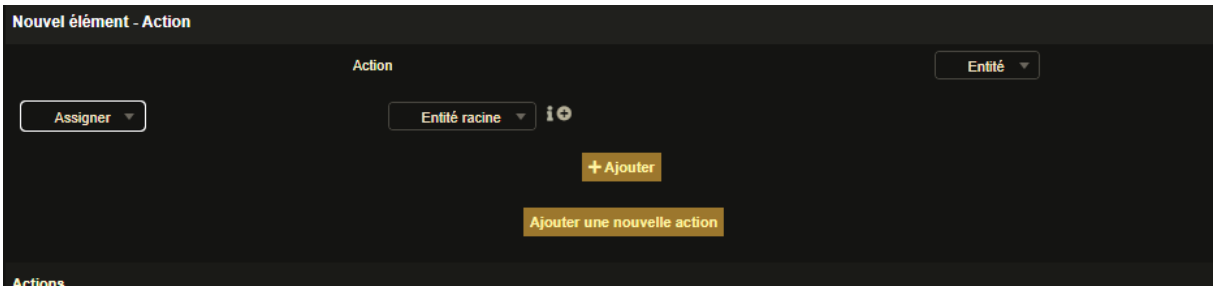


Définition du critère :

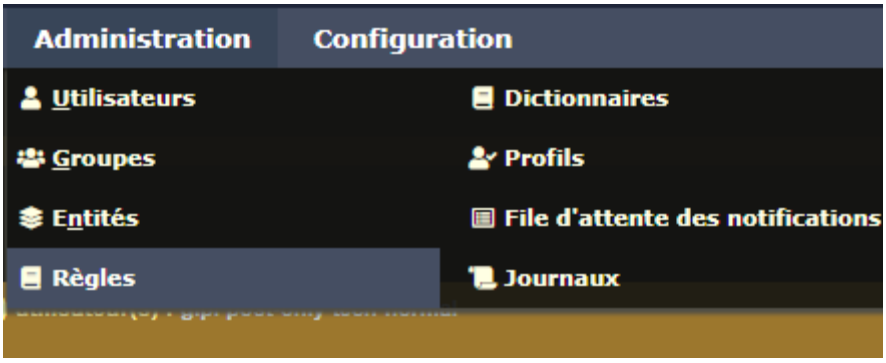


Ici, j'ai choisi d'accepter les adresses IP commençant par 172. Vous pouvez choisir d'autre critères.

Puis nous allons cliquer sur "Actions" et créer l'action ci-dessous :

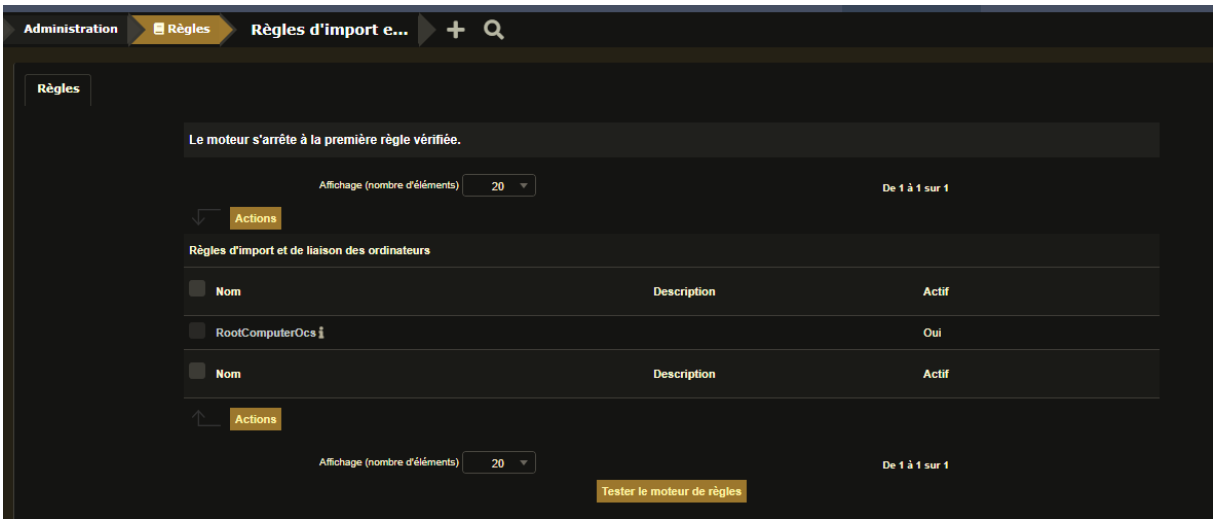


Ensuite, nous allons aller dans "Administration" puis "Règles".

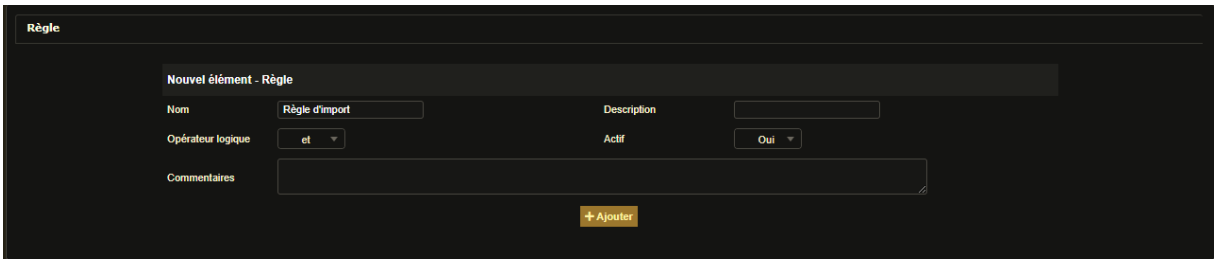


Nous allons cliquer sur "Règles d'import et de liaison des ordinateurs" ou alors sur "Règles d'import et de liaison des équipements" enfoncions de votre version.

Puis, nous allons cliquer sur le + en haut de l'écran :

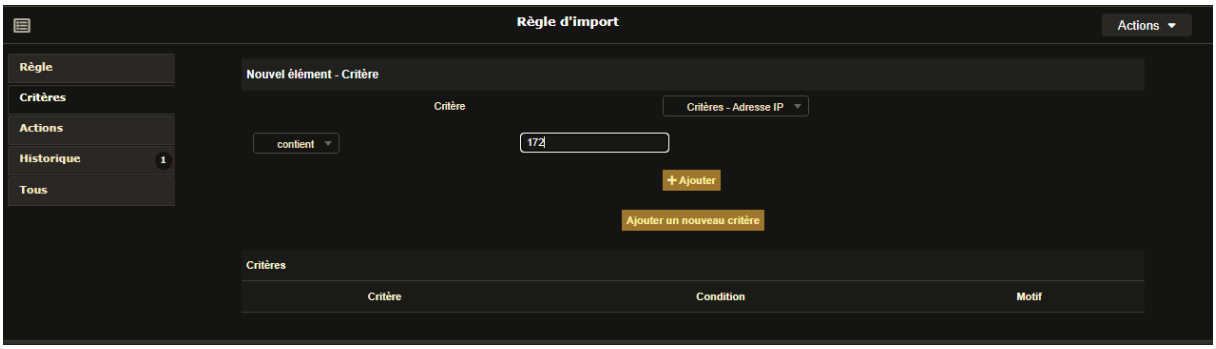


Nous allons créer la règle suivante :

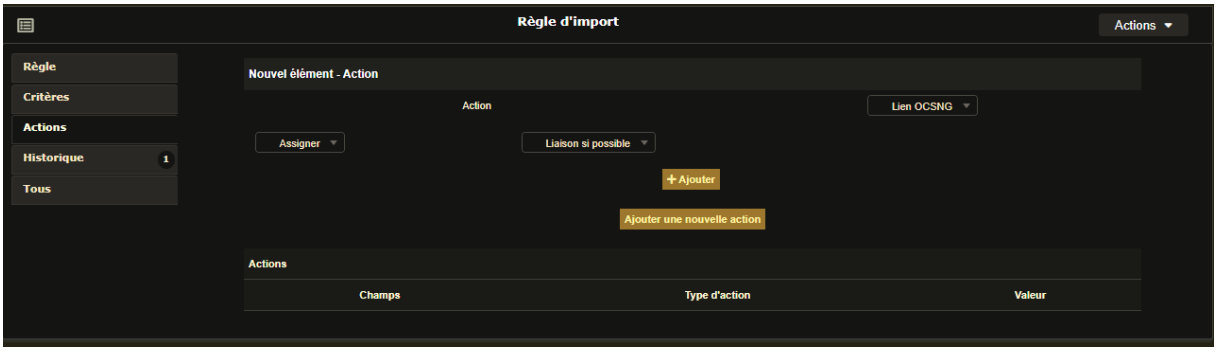


Puis nous allons cliquer sur "Critères" et nous allons cliquer sur "Ajouter un nouveau critère" :

Et nous allons créer le critère suivant sur les version cela peut être nommé Parc > Port réseau > IP)



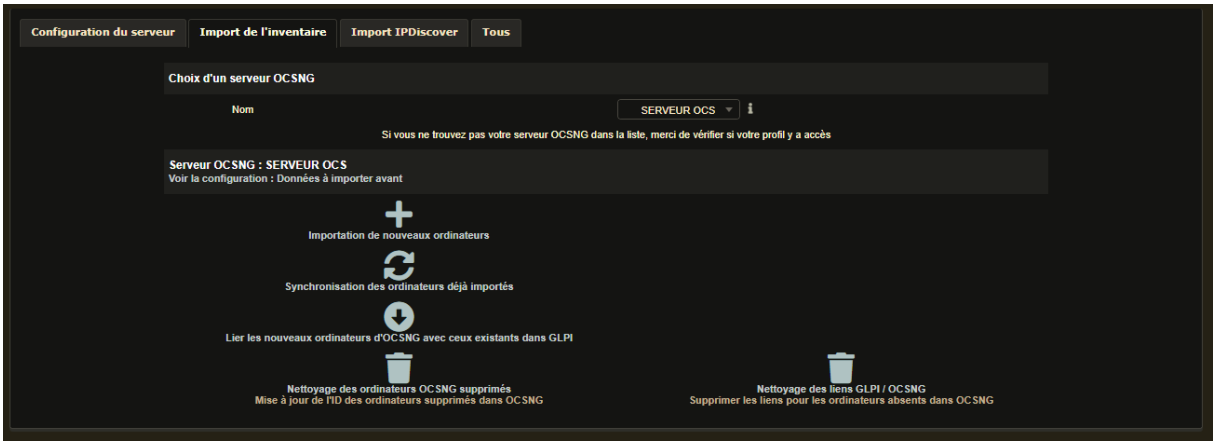
Enfin, nous allons cliquer sur "Actions" puis "Ajouter une nouvelle action" et nous allons remplir l'action comme ci-dessous :



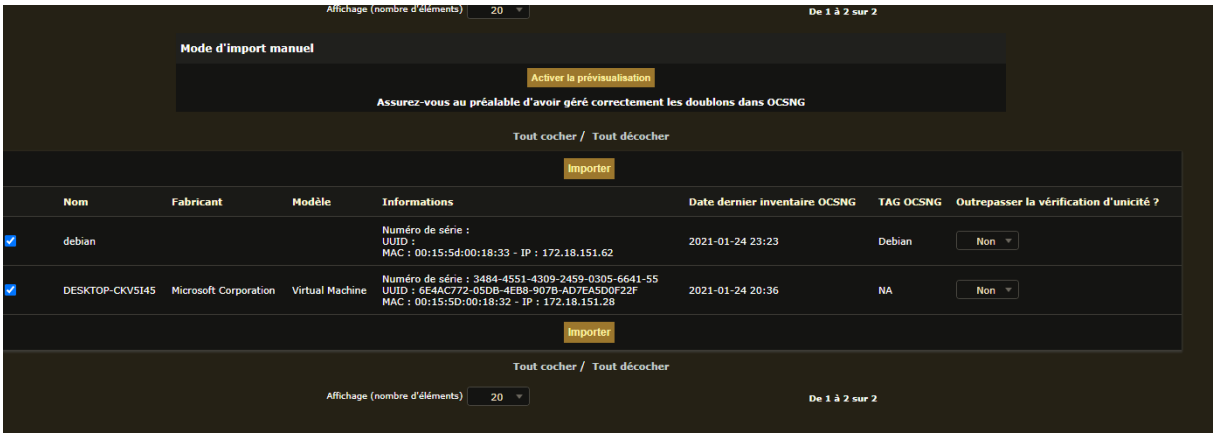
Import des informations d'OCS vers GLPI :

Pour importer les ordinateurs présents dans OCS. Nous allons nous rendre sur l'interface Web de GLPI et nous allons aller dans "Outils" puis "OCS Inventory NG".

Ensuite nous allons cliquer sur "Importation de nouveaux ordinateurs" cela peut aussi se nommer « Importer ou lier des ordinateurs » :



Nous pouvons maintenant importer les ordinateurs en cliquant sur "Importer" :



Aller voir dans l'accueil si les ordinateurs ont bien été remonter.

Synchronisation permanente entre OCS et GLPI.

Pour synchroniser automatiquement OCS et GLPI, nous allons ajouter le plugin "massocaimport" à GLPI.

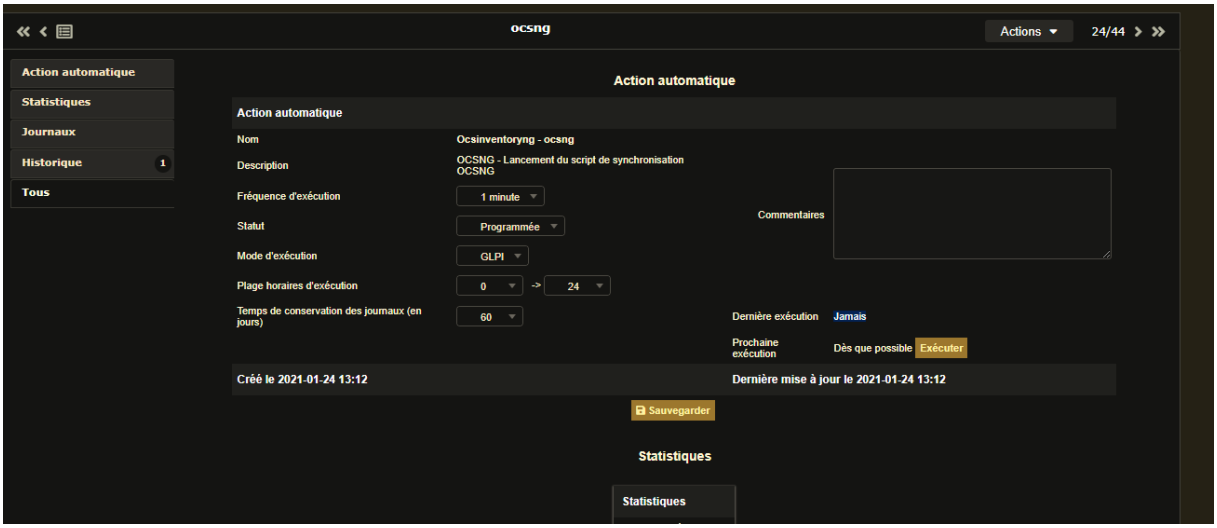
cd /var/www/html/glpi/plugins/ocsinventoryng/scripts/

chmod 755 ocsng_fullsync.sh

Le fichier de synchronisation est maintenant opérationnel. Nous allons donc modifier l'action automatique de GLPI :

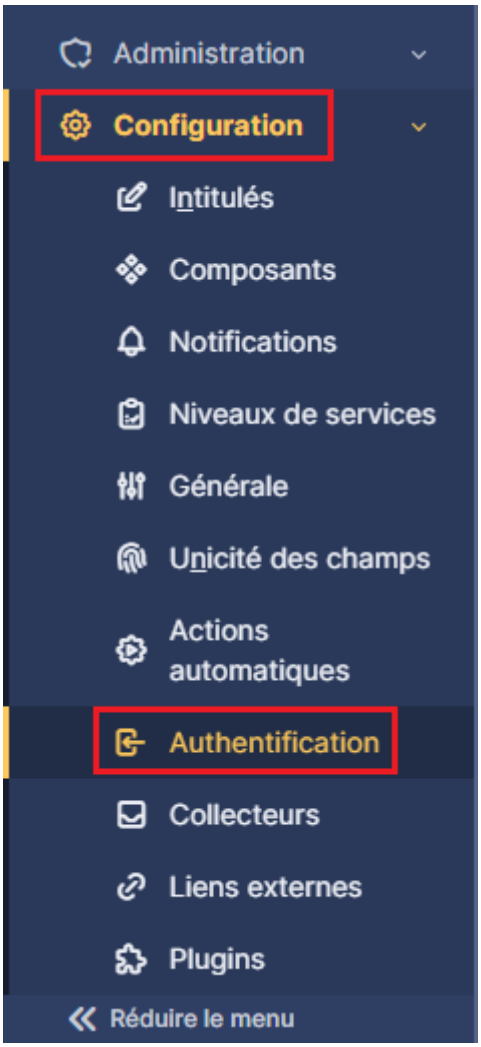
Nous allons chercher dans la liste le nom "ocs". (Petit conseil, augmentez le nombre de résultat par page pour le trouver)

Et nous modifions la tache comme ceci :

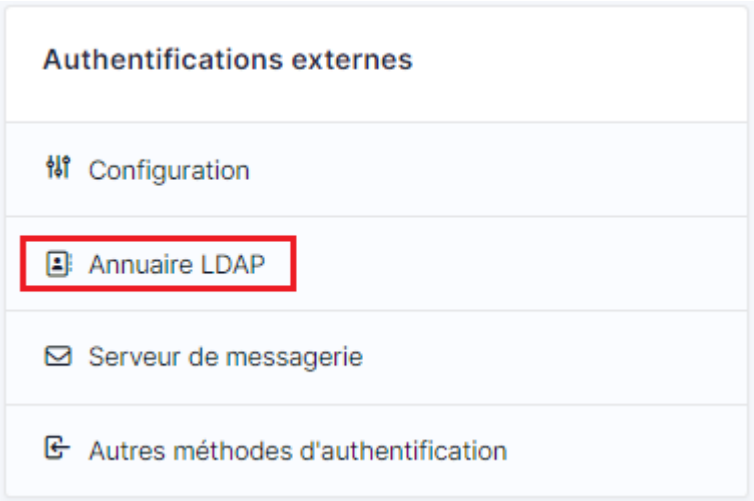


Connexion ldap GLPI ET AD

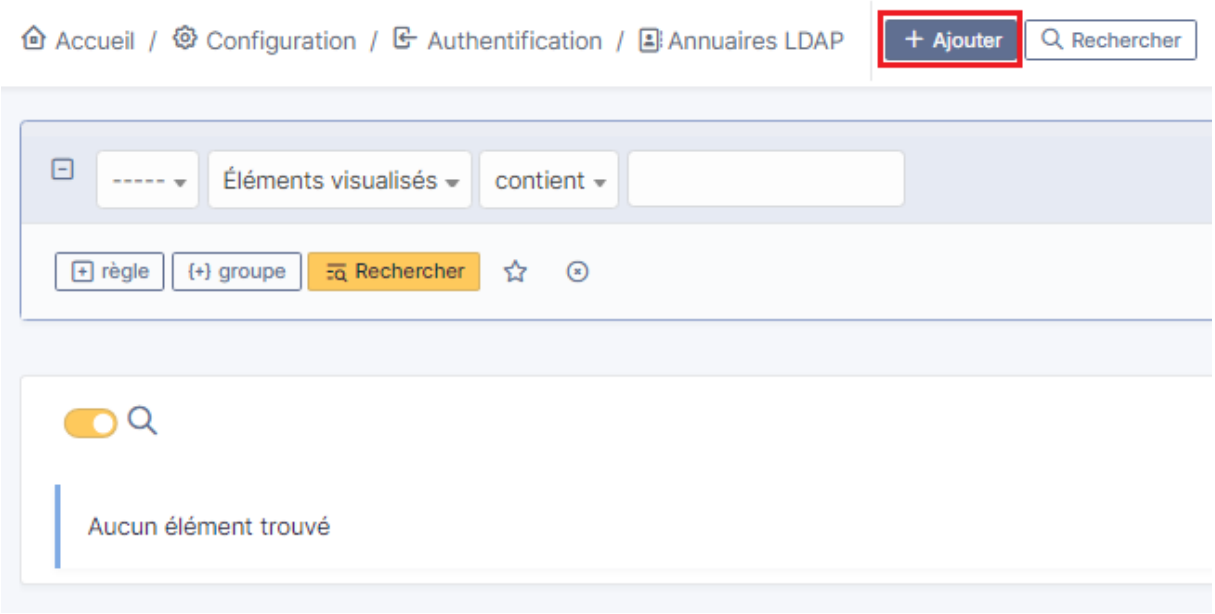
Connectez vous en tant que super-admin *(compte glpi par défaut)* sur l'interface web de GLPI. Rendez-vous dans le menu Configuration puis dans Authentification.



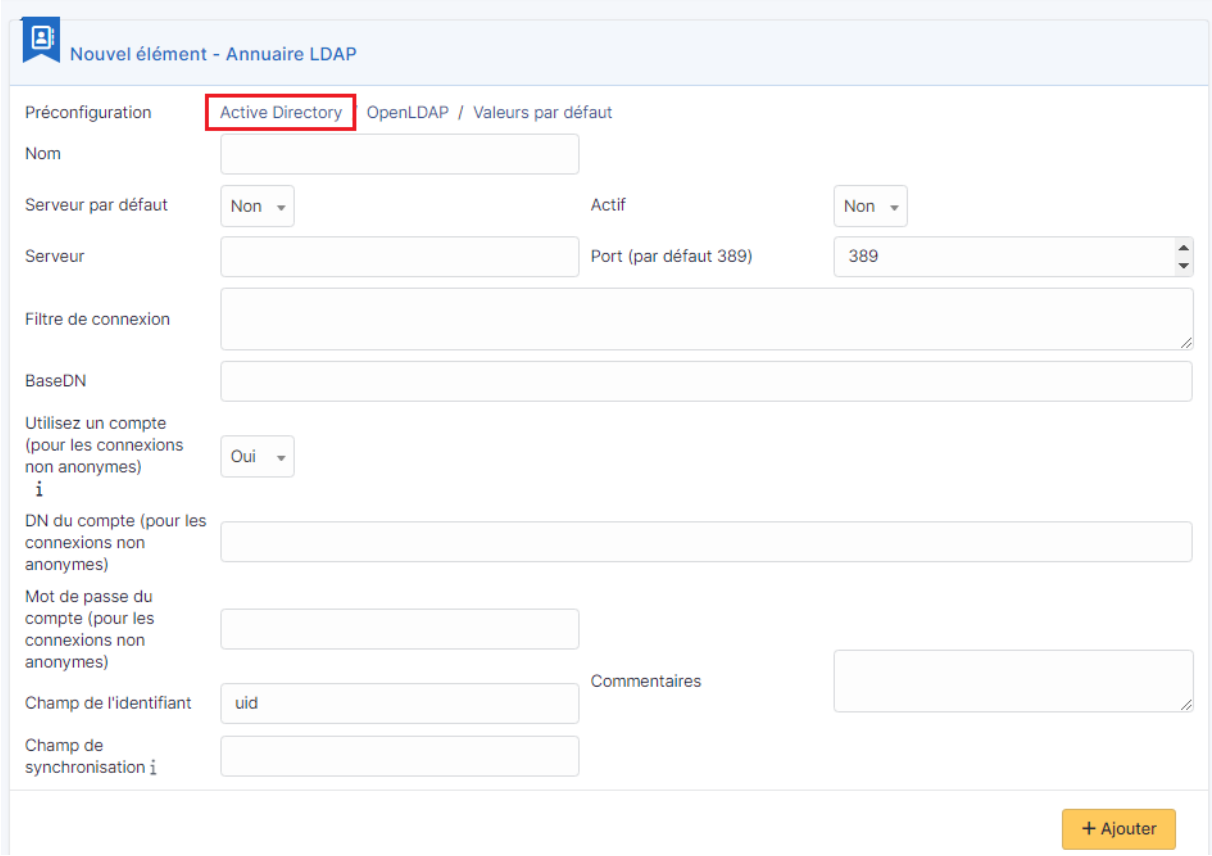
Cliquez sur Annuaires LDAP.



Il faut ajouter un annuaire pour créer la liaison. Pour cela, cliquez sur le bouton « + » ou « Ajouter » situé dans la barre du haut.

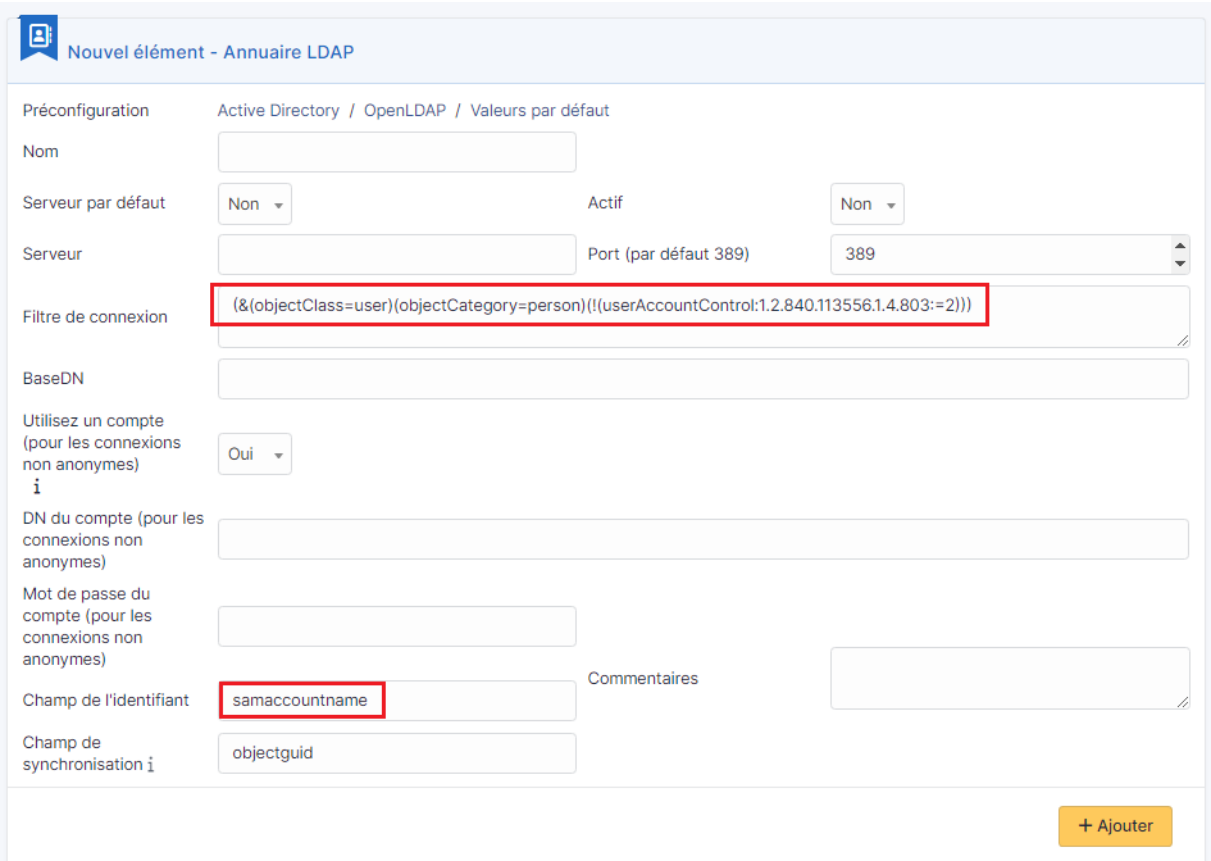


Il faut maintenant remplir différentes informations qui vont permettre à GLPI de communiquer avec le contrôleur de domaine. GLPI propose de remplir certains champs automatiquement, dont le champ Filtre de connexion, ce qui est assez pratique ! Pour cela, cliquez sur « Active Directory » dans la ligne Préconfiguration.



Les zones Filtre de connexion, champ de l'identifiant et champ de synchronisation ont été remplies. Ces 3 zones permettent de définir comment seront recherchés les

utilisateurs dans la base de données AD et quels seront les attributs d'un objet utilisateur utilisés pour se connecter.



Complétez le formulaire avec les informations de votre domaine comme ceci :

- Nom : donnez un nom à ce nouvel élément *(de préférence le nom du domaine pour bien identifier la connexion par la suite)*

- Serveur par défaut : mettre Oui *(sauf si vous avez l'intention de créer plusieurs liaisons AD différentes, dans ce cas, à vous de choisir quel serveur sera celui par défaut)*

- Actif : mettre Oui pour activer la liaison entre le serveur et GLPI

- Serveur : renseignez l'adresse IP du serveur Active Directory ou son nom complet avec le nom du domaine *(au format serveur.domaine.com)*

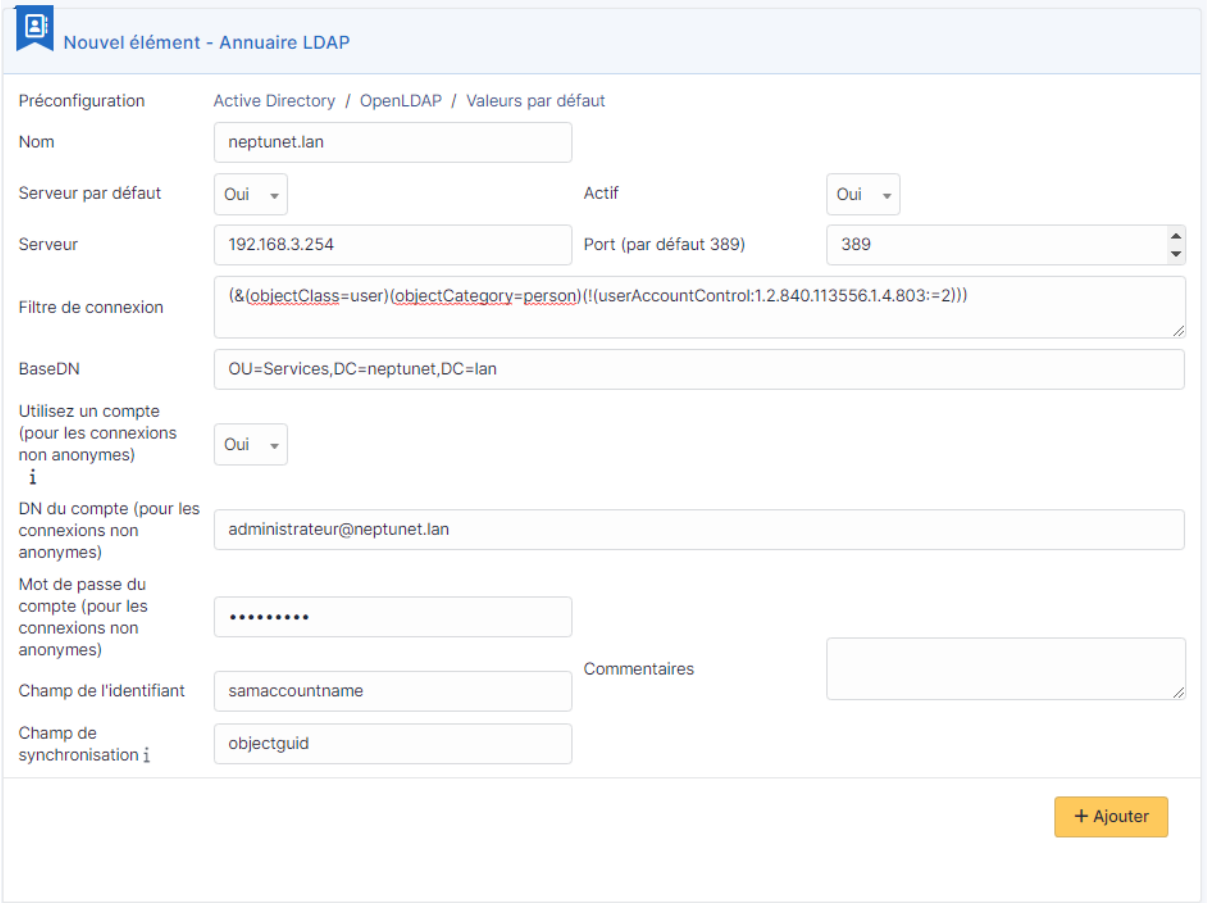
- Port : par défaut en non sécurisé, le protocole LDAP utilise le port 389. Si vous n'avez pas modifié ce port dans votre infrastructure, laissez par défaut.

- BaseDN : renseignez le Distinguished Name de l'Unité d'Organisation dont vous voulez importer les utilisateurs ou le Distinguished Name du domaine entier si vous souhaitez tout importer *(au format « OU=monOU,DC=domaine,DC=com » ou simplement « DC=domaine,DC=com » pour le domaine entier)*

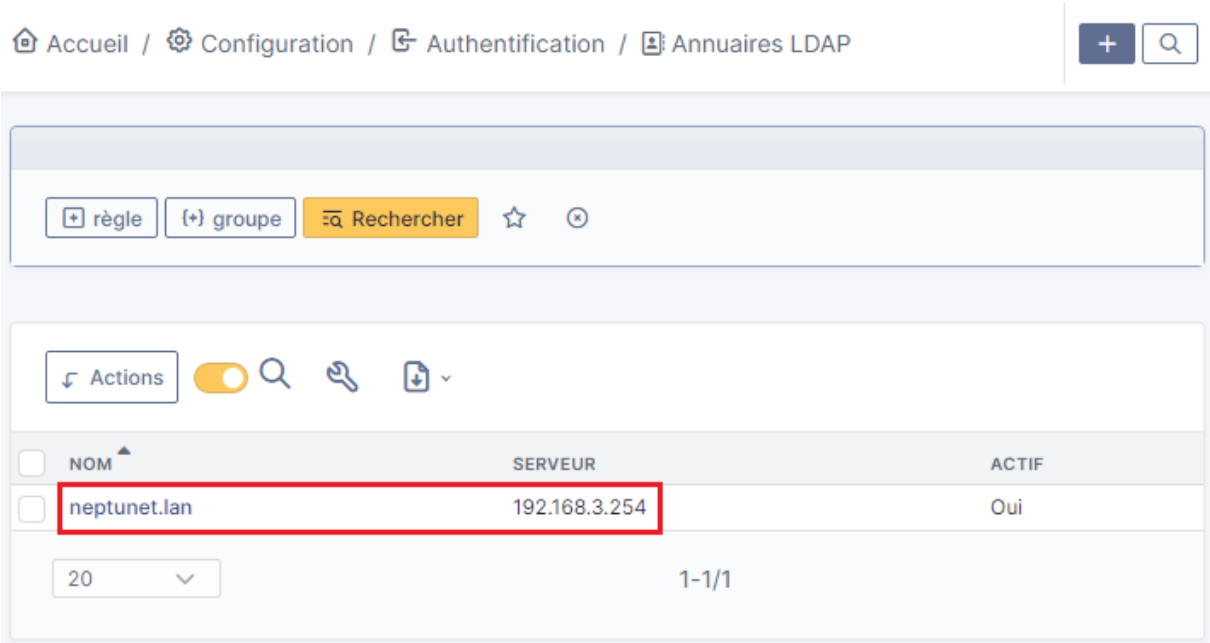
- DN du compte : renseignez ici l'identifiant complet d'un utilisateur ayant les droits d'accès sur le domaine *(comme l'administrateur par exemple, au format administrateur@domaine.com)*

- Mot de passe du compte : ajoutez le mot de passe de l'utilisateur déclaré dans le champ précédent

Cela devrait vous donner une configuration de ce genre :

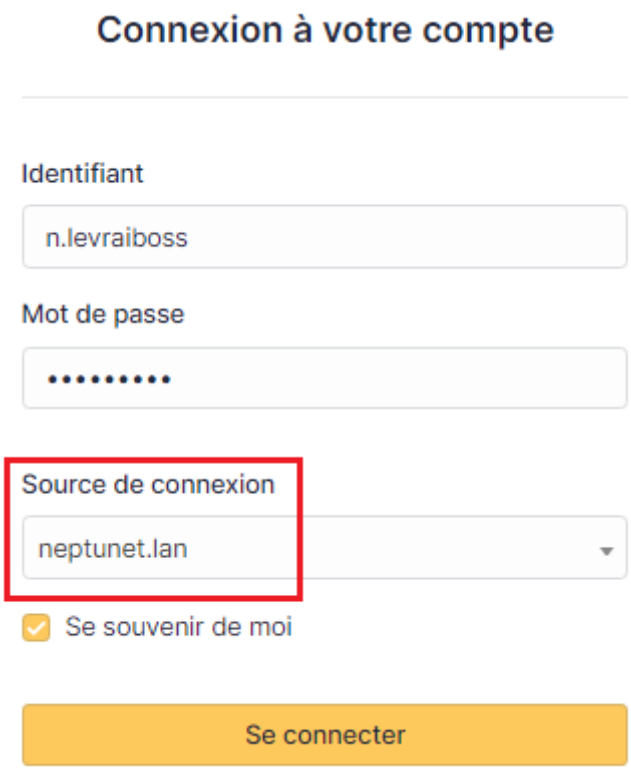


Quand vous avez terminé de remplir les différents champs, cliquez sur le bouton Ajouter. L'annuaire LDAP que vous venez de configurer sera ajouté à la liste. Après cet ajout, un test de connexion à l'AD est automatiquement effectué. Une infobulle en bas à droite de la fenêtre de GLPI vous avertira en cas de problème.

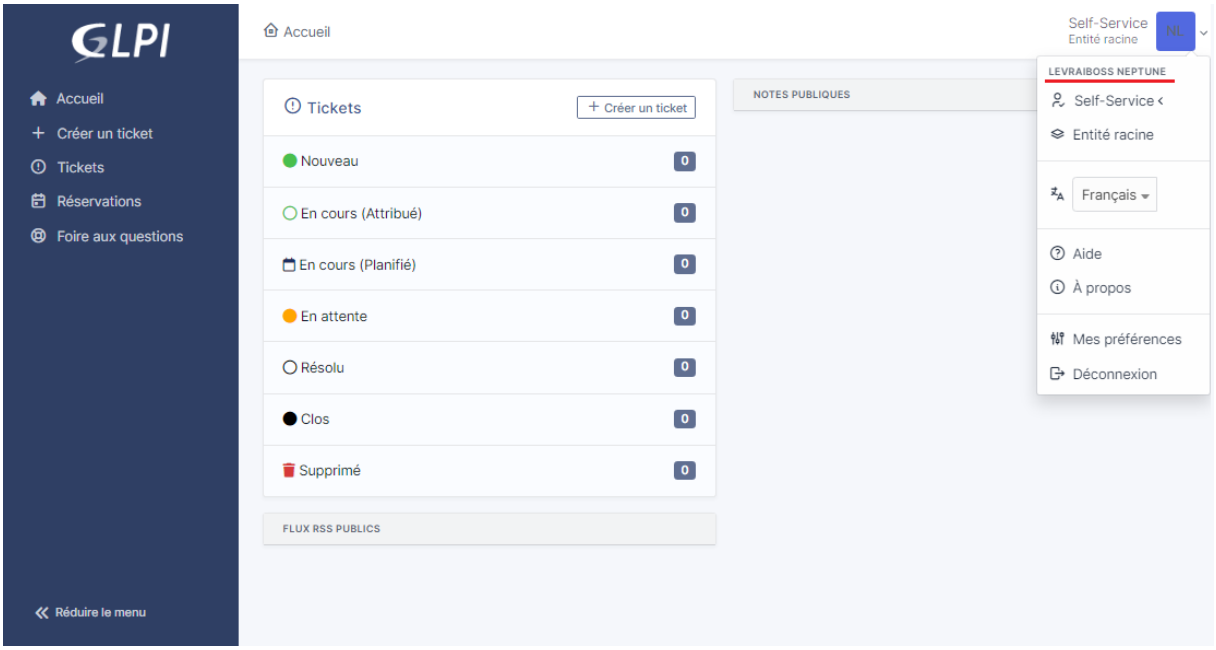


A partir de ce point, la configuration du serveur est terminée. Les utilisateurs du domaine pourront s'identifier directement. Leurs informations seront ajoutées automatiquement à GLPI.

Faisons un test de connexion avec l'un de nos utilisateurs présents dans AD. On voit tout de suite que la page de connexion à GLPI à changer et permet de se connecter sur le domaine en plus de la base de données interne de GLPI.

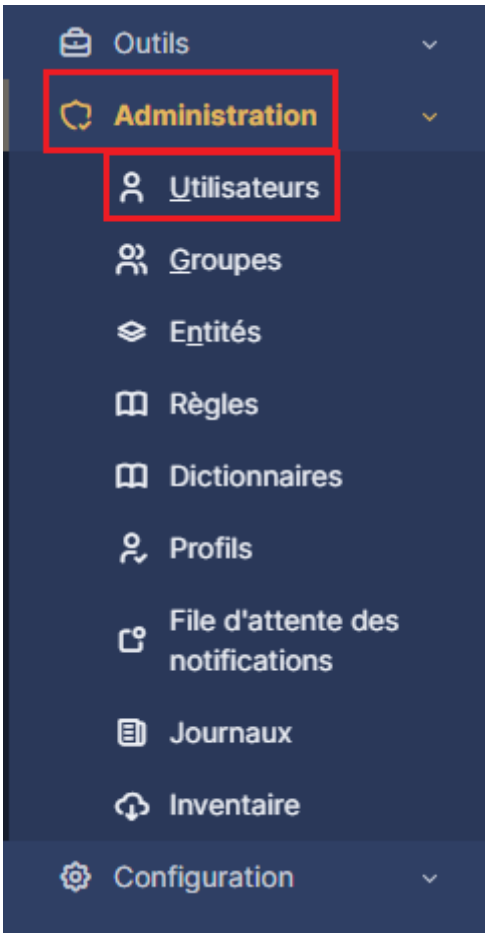


Après avoir saisi l'identifiant de mon utilisateur AD et son mot de passe, il aura bien accès à GLPI avec par défaut un profil « Self-Service » dans lequel il ne pourra que créer et suivre l'état de ses propres tickets et accéder à la base de connaissance de GLPI en mode FAQ si celle ci est utilisée.

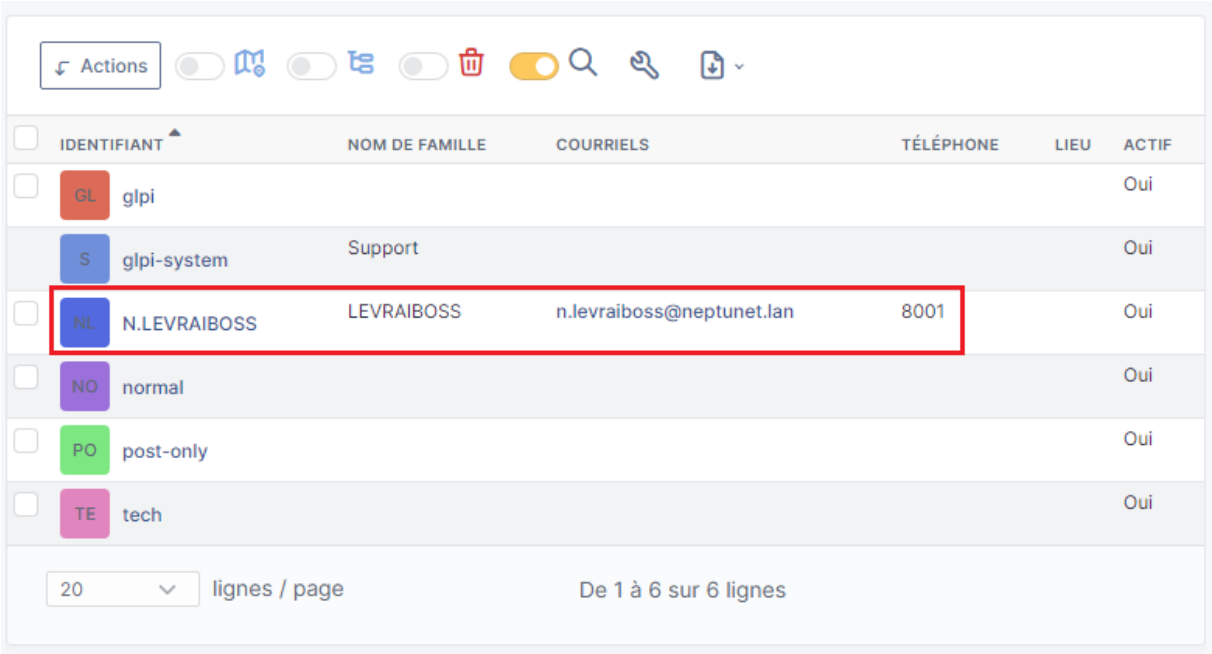


Retournez sur le compte du super-admin, en pensant bien à sélectionner cette fois ci « Base interne GLPI » et non pas le nom du domaine.

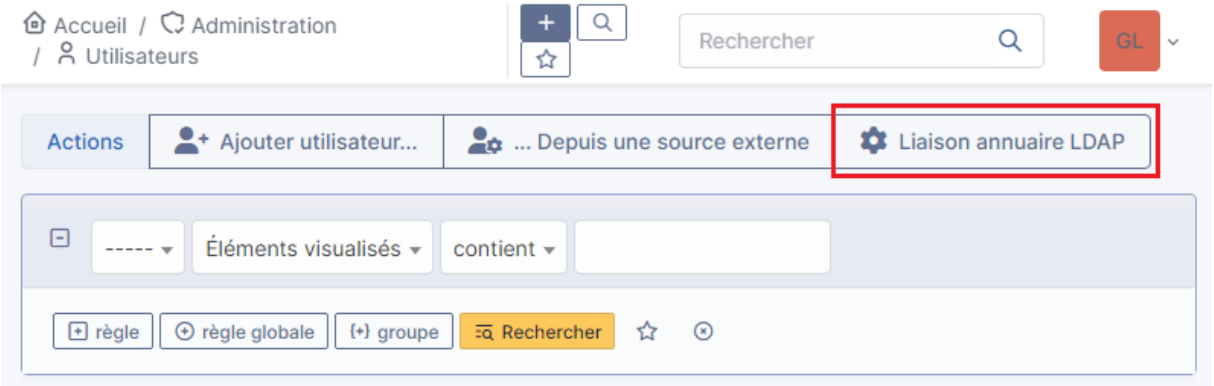
Allez dans le menu Administration puis dans Utilisateurs.



Dans la liste des utilisateurs, vous allez retrouver votre utilisateur que vous avez connecté précédemment. Vous n'avez donc plus aucune manipulation à faire.

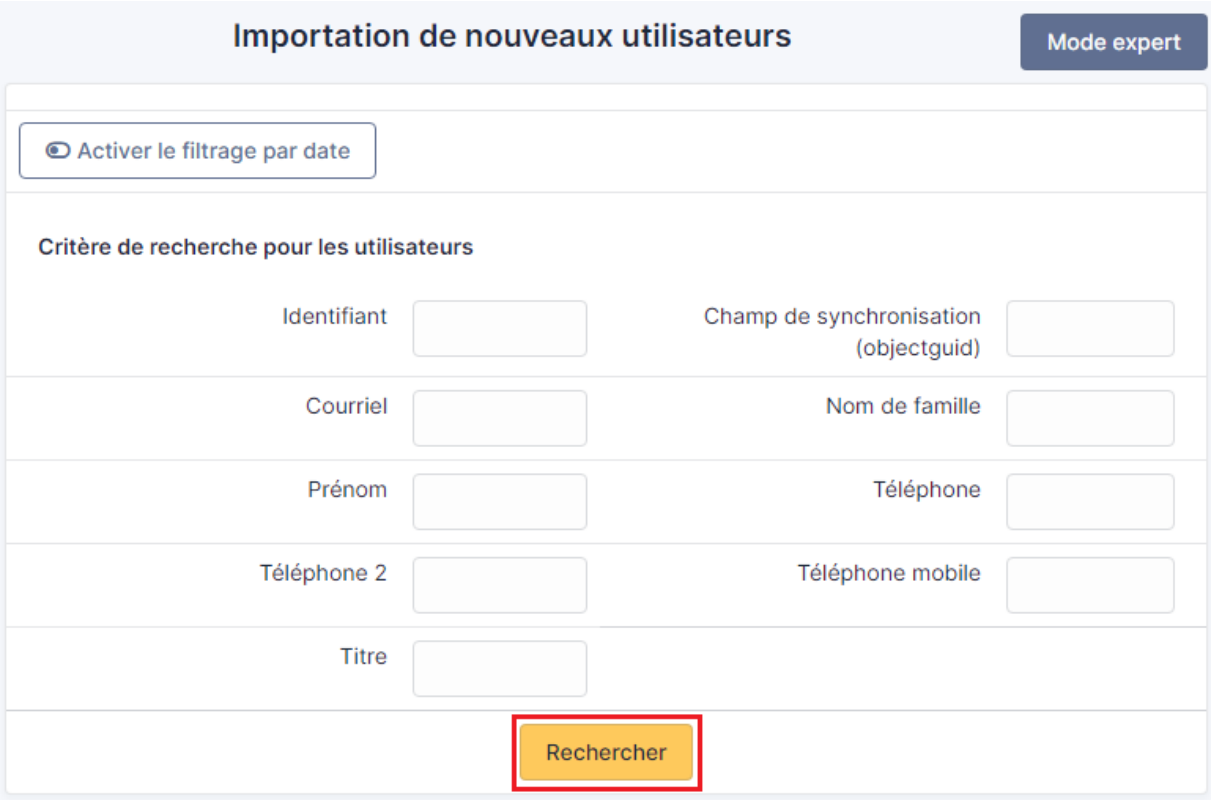


Vous pouvez si vous le souhaitez importer en masse tous les utilisateurs qui sont dans la « BaseDN » que vous avez déclaré lors de la configuration afin qu'ils soient synchronisés avec votre GLPI avant même leur 1ère connexion. Pour cela, toujours dans le sous-menu Utilisateurs, cliquez sur le bouton Liaison annuaire LDAP.



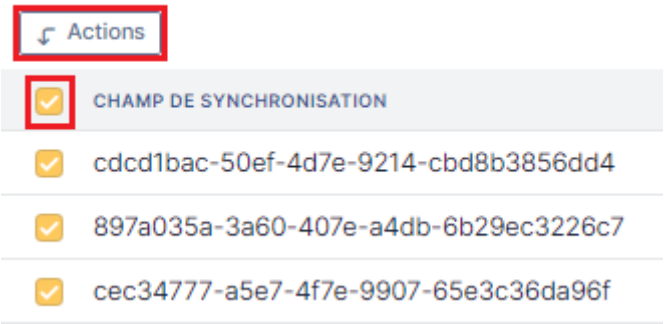
Cliquez sur Importation de nouveaux utilisateurs.

Sauf si vous souhaitez importer un utilisateur bien précis, cliquez simplement sur le bouton Rechercher sans définir de critère.

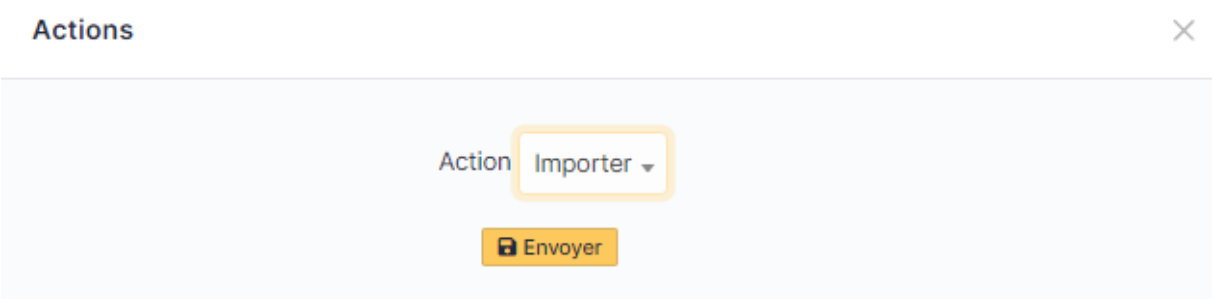


Vous verrez apparaître en bas de la page, tous les utilisateurs qui sont dans la BaseDN déclarée *(soit ceux d'une OU, soit tous les utilisateurs du domaine selon votre configuration)*.

Pour les importer dans GLPI, cochez les cases sur la gauche pour les sélectionner, cliquez sur le bouton Actions.

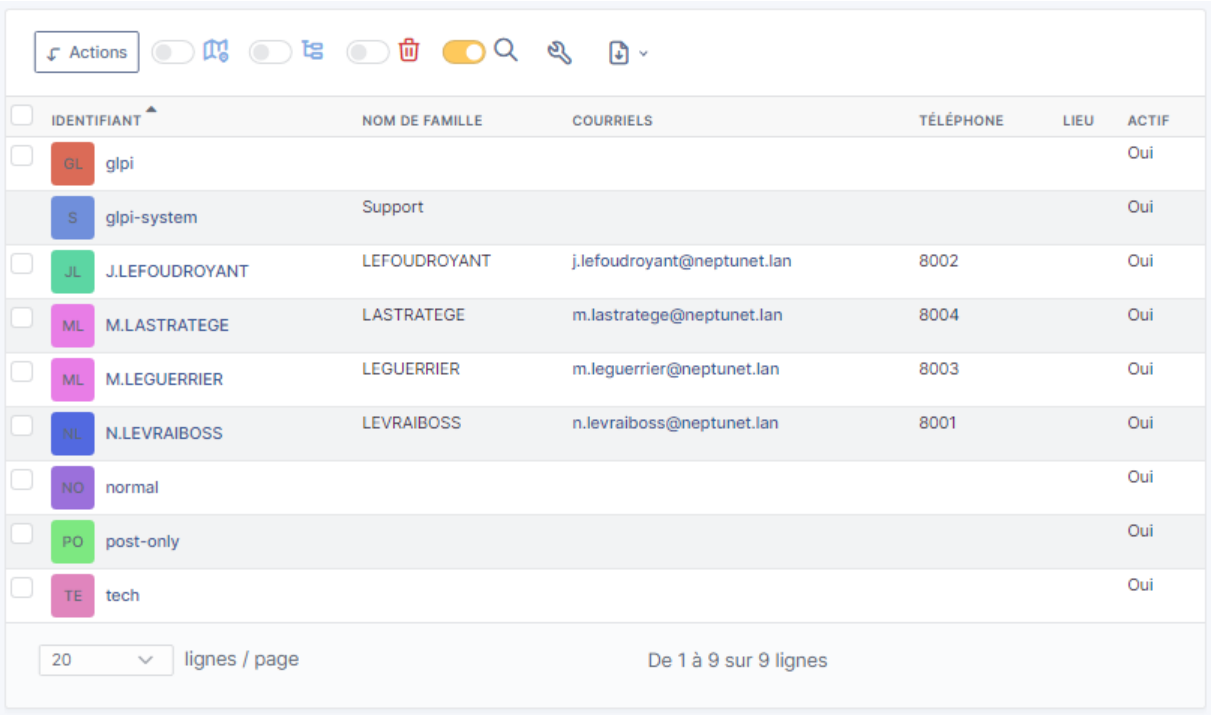


Sélectionnez Importer puis cliquez sur Envoyer.



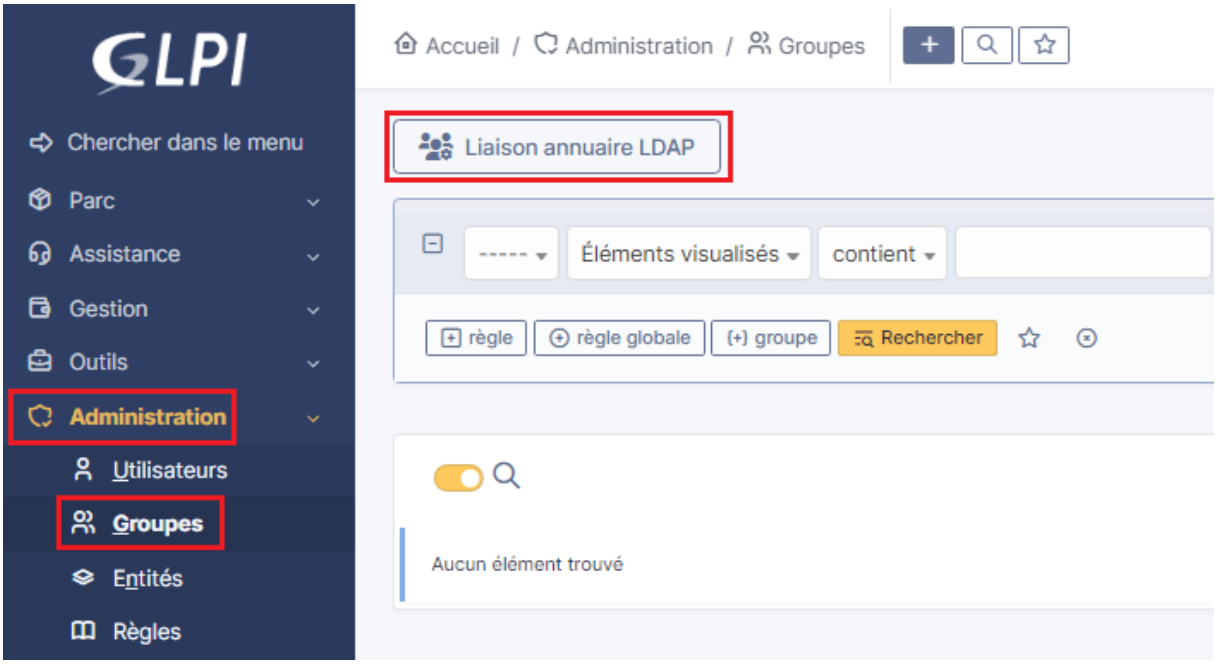
Une infobulle vous informera du déroulement de l'import.

Si vous allez vérifier vos utilisateurs, ils apparaitront bien dans GLPI. Je retrouve bien mes 4 utilisateurs AD.



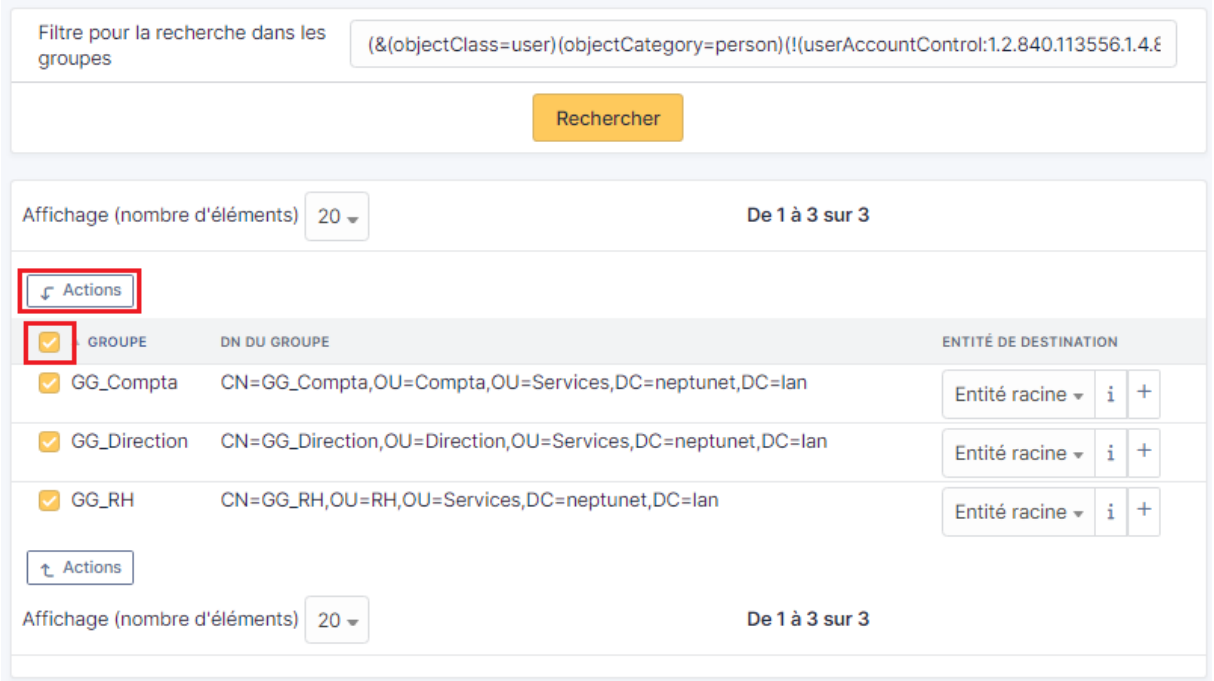
Vous pouvez également importer des groupes AD, les manipulations restent les mêmes.

Allez dans le menu Administration puis dans Groupes cette fois-ci. Cliquez sur le bouton de liaison LDAP.

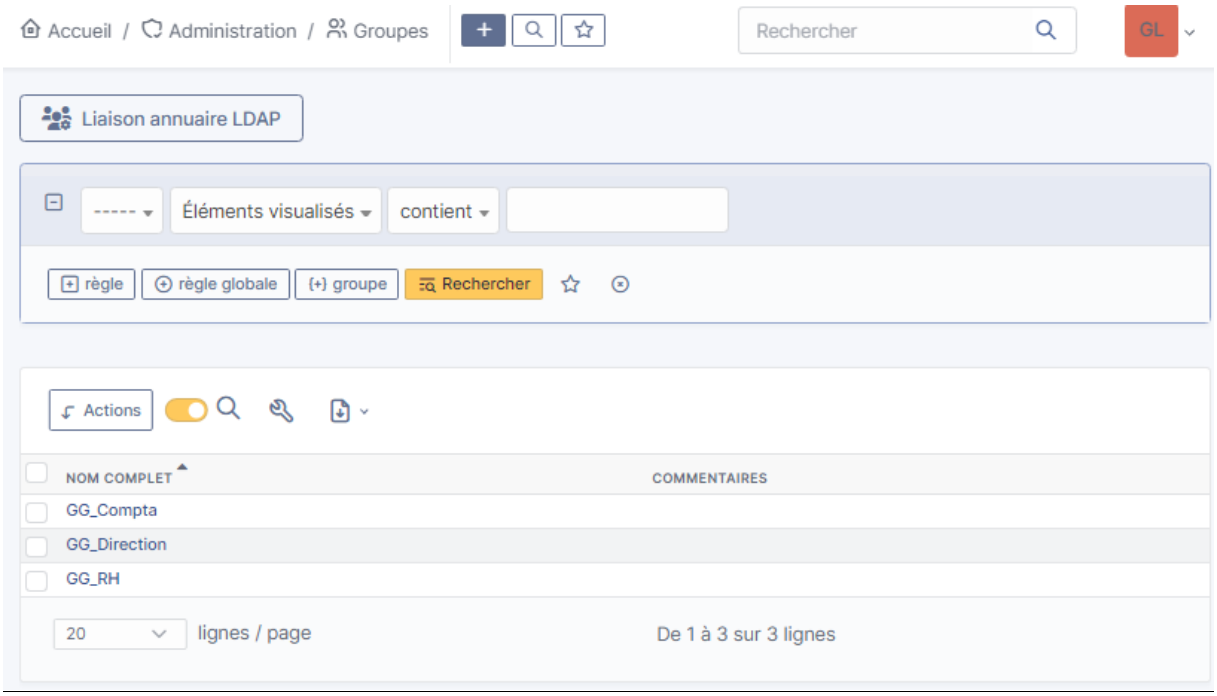


Cliquez sur « Importation de nouveaux groupes ».

GLPI vous proposera en bas de page tous les groupes disponibles dans le BaseDN renseigné précédemment. Il ne vous reste qu'à cocher les cases des groupes que vous voulez importer, menu Actions puis Importer.



Les groupes importés depuis l'AD seront disponibles dans GLPI.

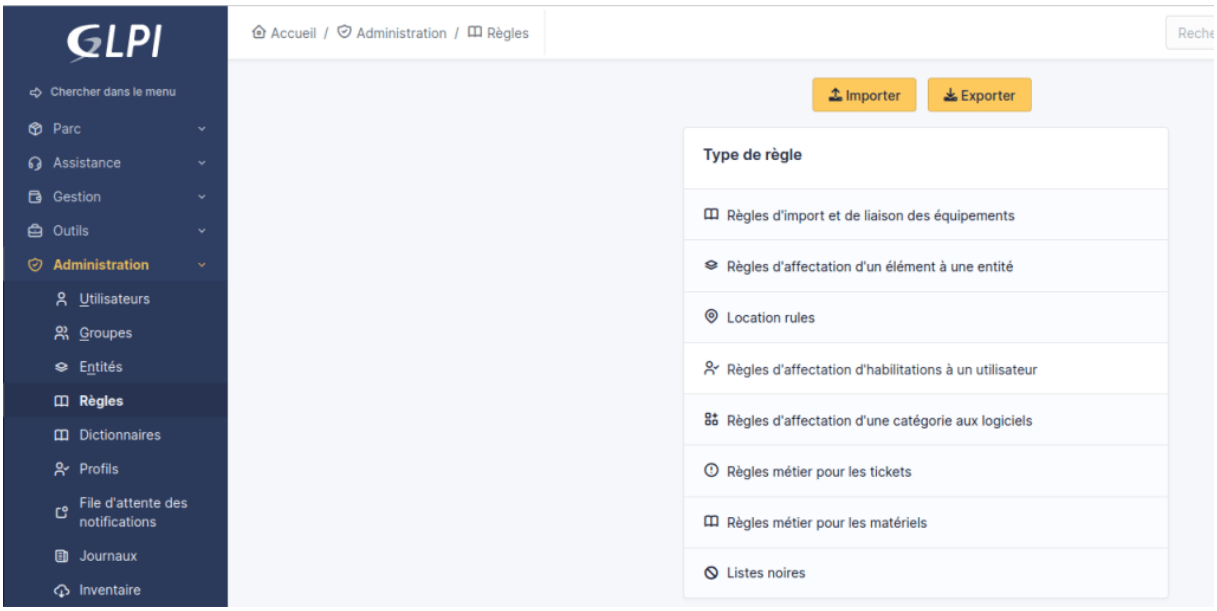


Règles d'attribution

Il est possible dans GLPI, d'attribuer un profil en fonction de l'OU ou est placé l'utilisateur Active Directory.
Par exemple un utilisateur présent dans l'OU « DSI » aura automatiquement le profil « *Technicien* » attribué par défaut.
Nous pourrons ainsi créer les profils correspondants au particularités que nous souhaitons attribuer à chaque utilisateur.

Dans le cas ou rien n'est précisé c'est le profil « self-service » qui sera attribué.

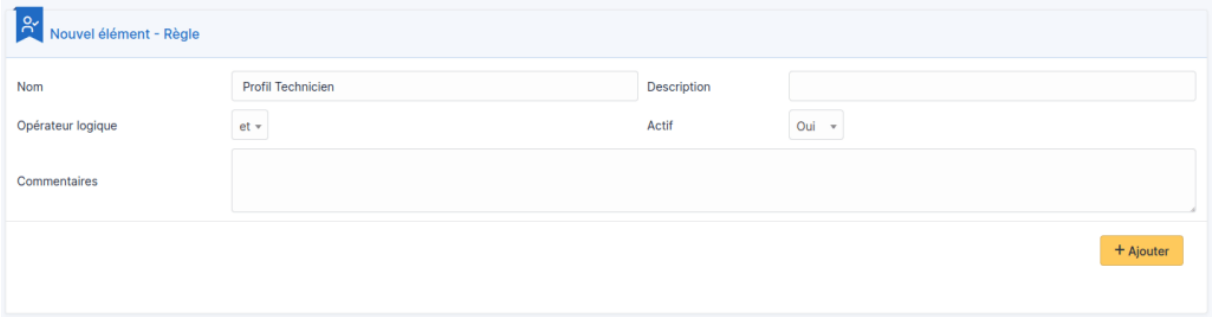
Pour commencer nous irons dans « *Administration* », « *Règles* », et « *Règles d'affectation d'habilitation à un utilisateur* ».



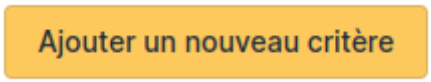
Puis nous cliquerons sur le bouton « *Ajouter* »

.

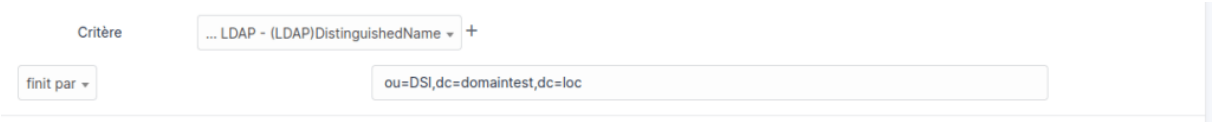
Nous donnerons un nom à notre règle : « *Profil Technicien* » et nous l'activerons en sélectionnant « *Oui* » sur la ligne « *Actif* » :



Nous rentrerons dans la règle pour la paramétrer.
Nous commencerons par définir les critères d'application de la règle en cliquant sur « *Ajouter un nouveau critère* ».



Nous sélectionnerons alors le paramètre « *(LDAP)DistinguishedName* » puis « *finit par* » « *ou=DSI,dc=domaintest,dc=loc* » indiquant ainsi les utilisateurs de l'OU DSI.

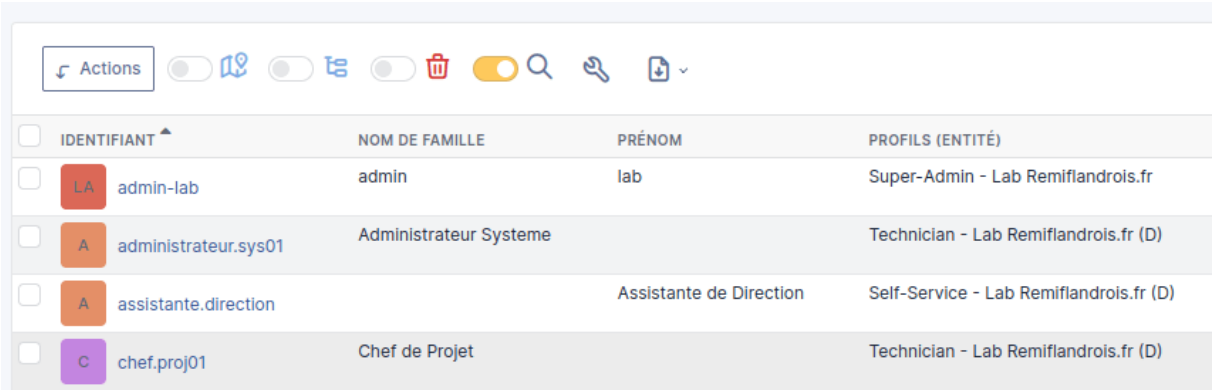


Puis dans le menu « *Actions* », nous cliquerons sur le bouton « *Ajouter une nouvelle action* » Ajouter une nouvelle action .

Nous définirons l'action « *d'Assigner* » un « *Profil* » de « *Technician* ». Nous validerons en cliquant sur le bouton « *Ajouter* »:

Les utilisateurs ayant déjà été importés auront besoin d'être resynchronisés avec la commande:

sudo /usr/bin/php8.1 /var/www/glpi.domaintest.loc/bin/console glpi:ldap:synchronize_users -d 3



Collecteur Oauth IMAP

Installer#

Information

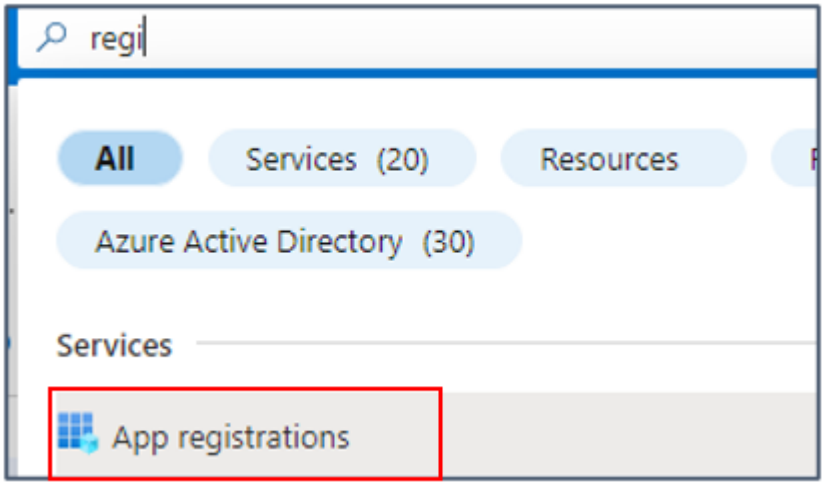
Ce plugin est communautaire et ne nécessite pas de licence particulière. Il est également disponbile en Cloud.

- Rendez-vous dans la marketplace. Téléchargez et installez le plugin "**OAuth IMAP**"

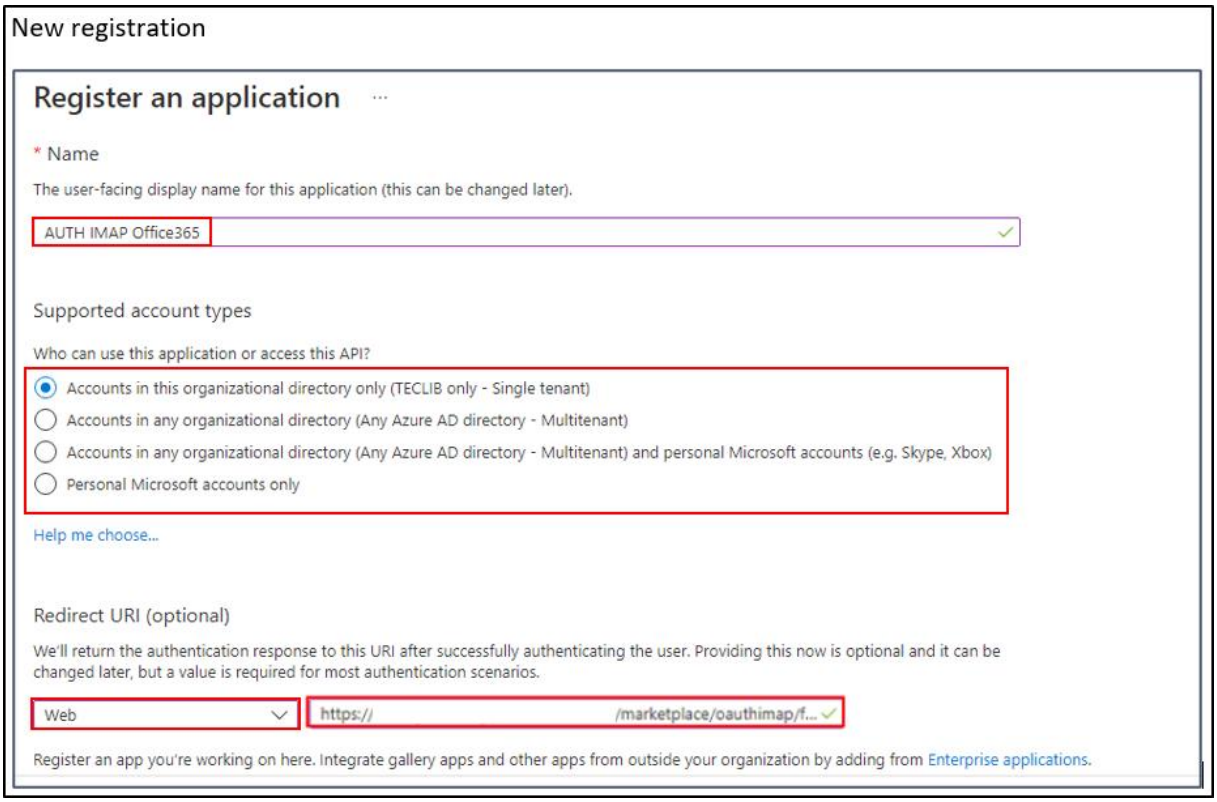
Inscription Application Entra#

Création de l'application Entra#

- RdV maintenant sur votre tenant Azure
- Dans la zone de recherche tapez **inscription** puis sélectionnez **inscriptions d'applications**

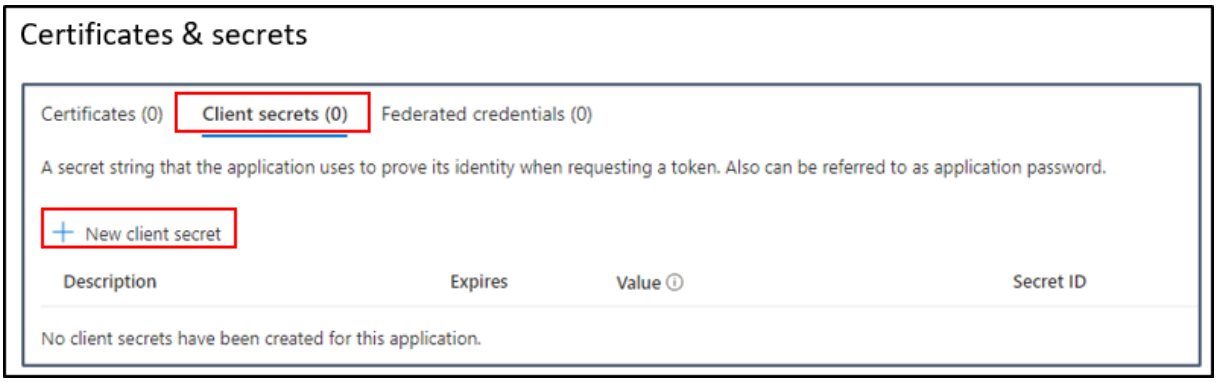


- Cliquez sur **nouvelle inscription**
- Indiquez le nom souhaité,
- Sélectionnez le type de compte pris en charge puis indiquez l'**URL de redirection** (présente dans la configuration du plugin depuis votre interface GLPI : https://XXXXXXXXXXXXXX/marketplace/oauthimap/front/authorization.callback.php) en précisant l'option **Web**
- Puis cliquez sur **s'inscrire**

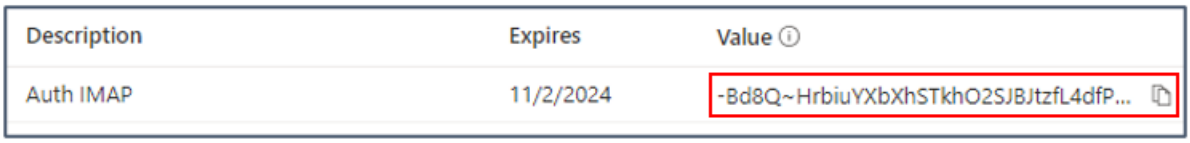


Ajout d'un secret#

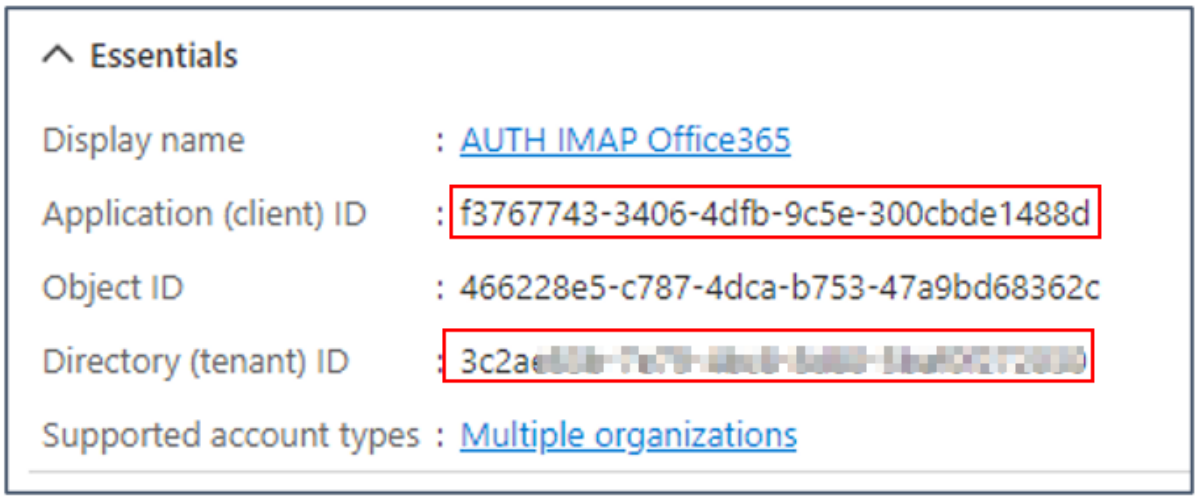
- Dans l'onglet **Certificats et secrets**, cliquez sur **Secrets client** puis **Nouveau secret client**



- Entrez une description puis une date d'expiration
- Une **valeur** de secret est alors généré. Conservez bien cette valeur car une fois que vous aurez quitté cette page, celui-ci ne sera plus récupérable.

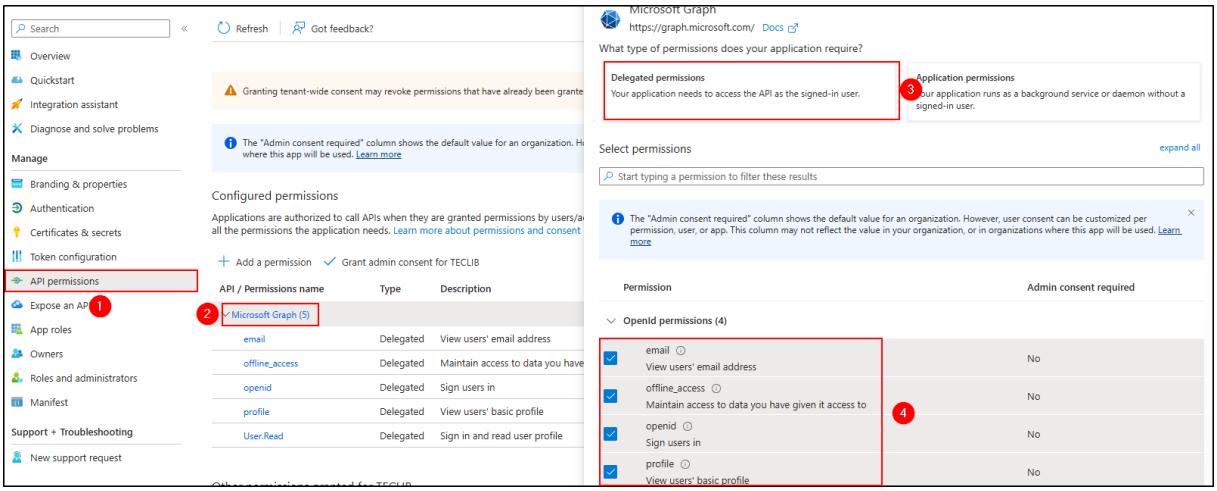


- Retournez dans l'onglet **"Vue d'ensemble"** et copiez les valeurs suivantes et le secret vu un peu plus haut



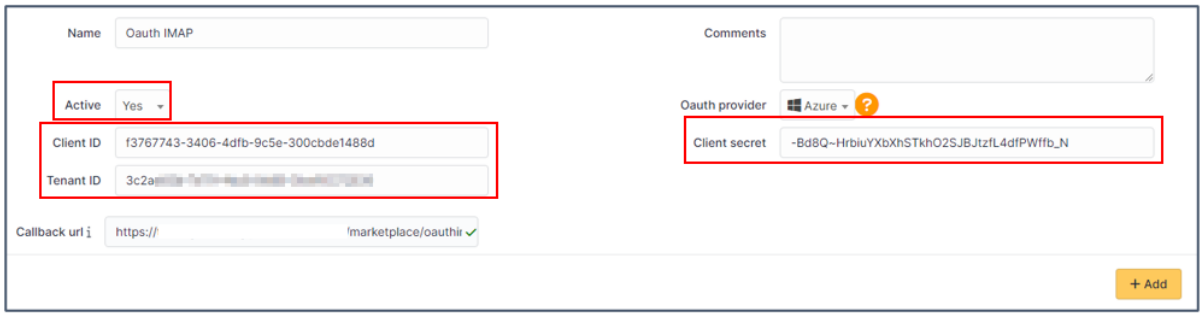
Ajouter des autorisations API¶

- Dans l' onglet **Autorisations API**
- Cliquez sur **votre API** (Microsoft Graph dans ce cas)
- Sélectionnez ensuite **l'autorisation déléguée**
- Sélectionner :
  - e-mail
  - accès hors ligne
  - openid
  - profil

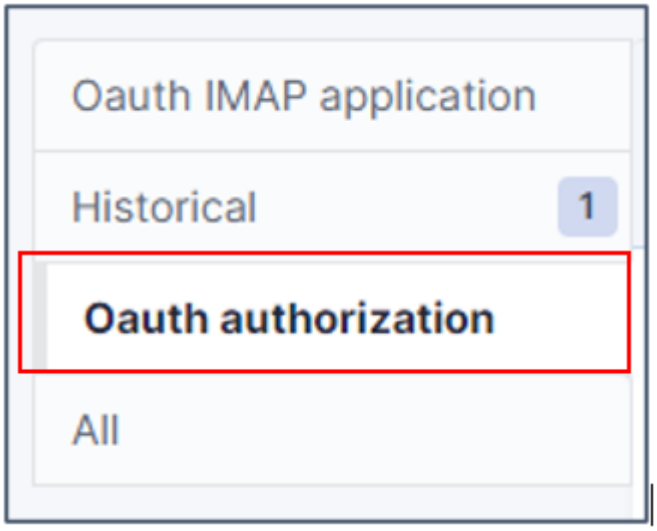


Paramétrer GLPI#

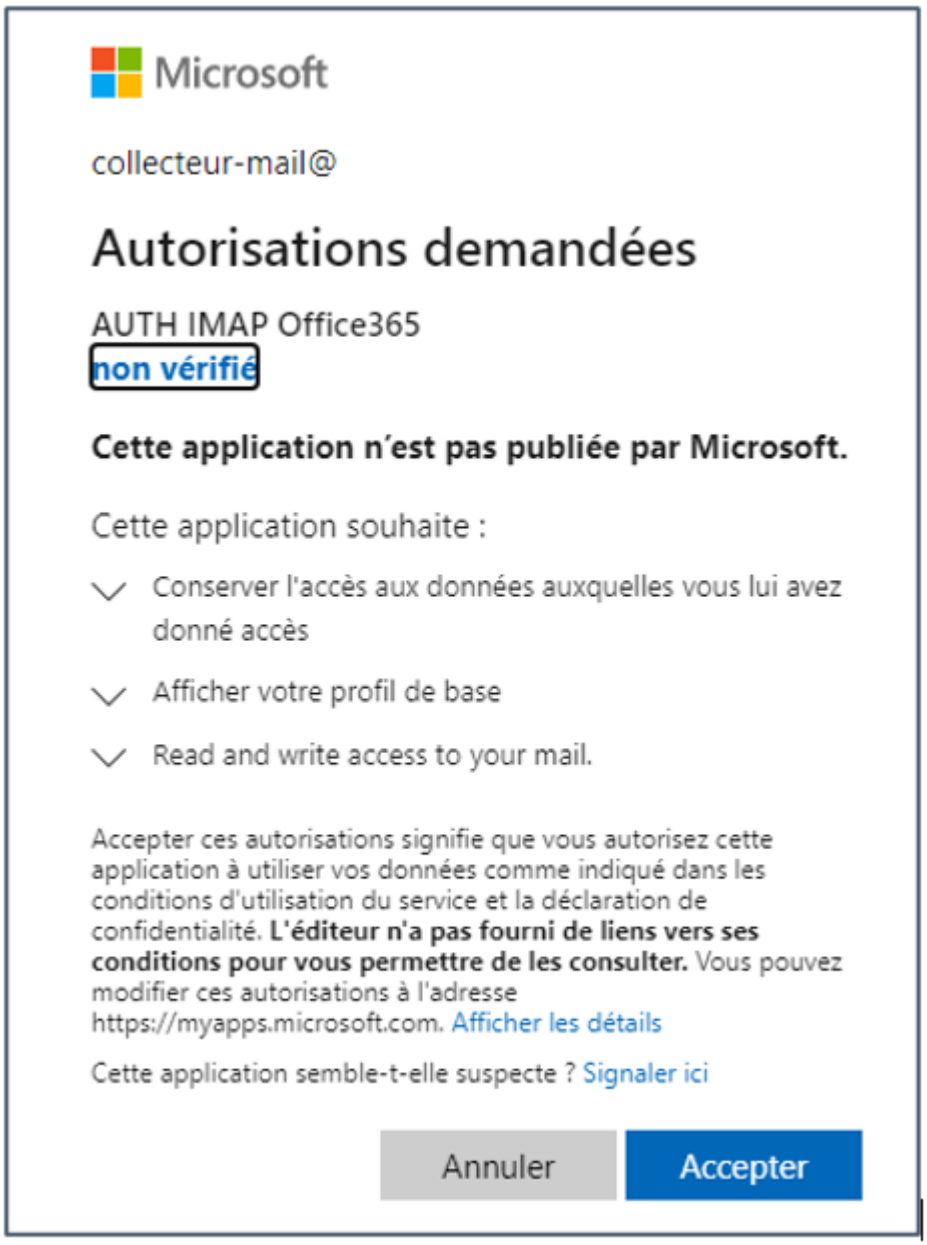
- Retournez maintenant dans votre interface GLPI **configuration** > **Application OAuth IMAP**
- Cliquez sur **ajouter** et indiquez les informations récoltées précédemment



- Cliquez sur **ajouter**
- Maintenant, dans l'onglet **autorisation Oauth**, nous allons **créer une autorisation**

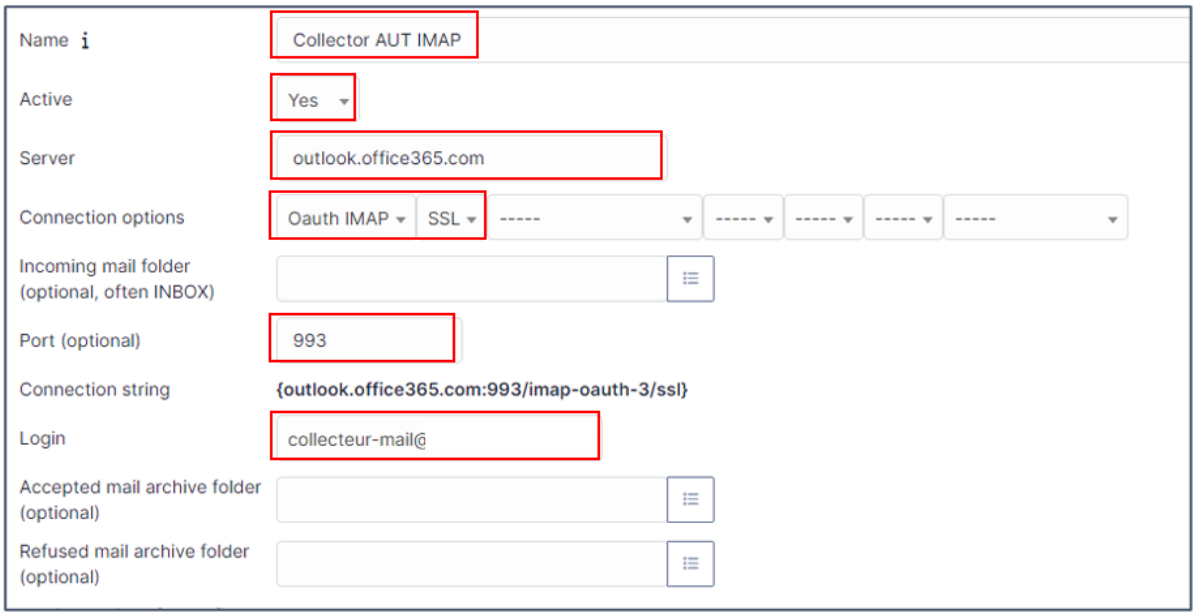


- Lorsque vous cliquerez sur ajouter **créer une autorisation**, vous serez redirigé vers la page de connexion aux services Microsoft.
- Entrez l'adresse mail et le mot de passe du compte qui sera utilisé pour le collecteur. Il vous faudra également accepter les autorisations nécessaires liées au plugin.



- RdV maintenant dans **configuration** > **collecteur** afin de le paramétrer :

Paramétrer le collecteur



CONNEXION LDAP à GLPI