



Assurmer

DE CARVALHO

LOPES

Bruno

LE CLAINCHE

Killian

DRIF

Wassim





| Auteur | Date de création | Version | Valideur | Destinataire | Diffusion | Nombre de pages |
|--|------------------|---------|----------|---------------|--------------------|-----------------|
| Bruno DE CARVALHO Killian LE CLAINCHE | 29/04/2024 | 1.0 | En cours | Technicien IT | Teams Equipe IT | 18 |

| | |
|--|-----------|
| I. Préparation de la machine Debian 12..... | 3 |
| 1. Mise à jour des paquets Debian | 3 |
| 2. Installation du serveur LAMP (Linux Apache MariaDB PHP) | 3 |
| a) Installation d'Apache : | 3 |
| b) Installation PHP : | 4 |
| c) Installation de MariaDB : | 4 |
| 3. Création de la base de données « GLPI » | 6 |
| II. Installation et décompression de GLPI | 7 |
| 1. Installation de GLPI..... | 7 |
| 2. Décompression de GLPI..... | 7 |
| III. Sécurisation de GLPI | 8 |
| 1. Création des répertoires..... | 8 |
| a. Création du répertoire (/etc/glpi) | 8 |
| b. Création du répertoire (/var/lib/glpi) | 8 |
| c. Création du répertoire (/var/log/glpi) | 8 |
| 2. Créer les fichiers de configuration | 9 |
| 3. Activation de la sécurisation des cookies de GLPI | 10 |
| 4. Configuration de Apache2 | 11 |
| IV. Lancement de l'installation de GLPI | 12 |

I. Préparation de la machine Debian 12

Dans ce guide, nous allons installer et configurer un helpdesk de type « GLPI » (version stable 10.0.10) sur une machine virtuelle Debian 12.

Prérequis :

- Une machine Debian 12 fonctionnelle
- La machine a accès à Internet

1. Mise à jour des paquets Debian

On commence par mettre à jour les paquets présents :

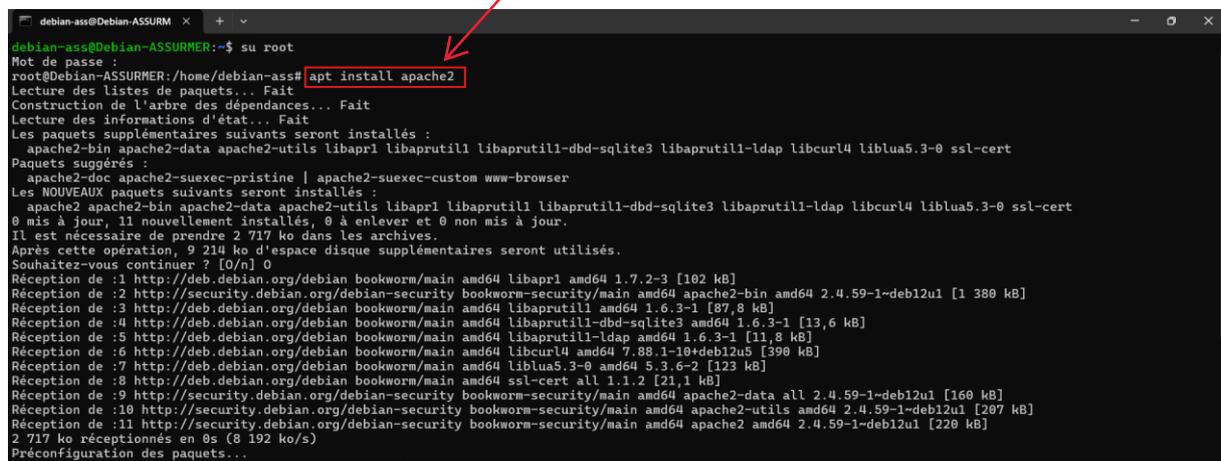
- apt update
- apt upgrade -y

2. Installation du serveur LAMP (Linux Apache MariaDB PHP)

Remarque : cette étape n'est pas nécessaire si un serveur LAMP a déjà été installé

a) Installation d'Apache :

Etape 1 : faite la commande « apt install apache2 »

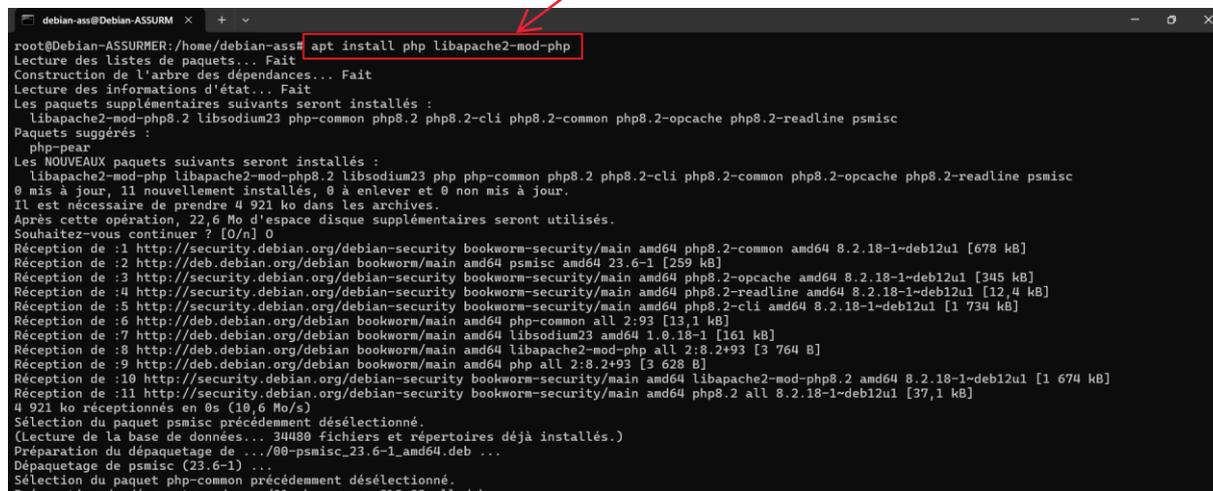


```
debian-ass@Debian-ASSURM x +
debian-ass@Debian-ASSURMER:~$ su root
Mot de passe :
root@Debian-ASSURMER:/home/debian-ass# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libcurl4 liblua5.3-0 ssl-cert
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libcurl4 liblua5.3-0 ssl-cert
0 mis à jour, 11 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 2 717 ko dans les archives.
Après cette opération, 9 214 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] 0
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libapr1 amd64 1.7.2-3 [102 kB]
Réception de :2 http://security.debian.org/debian-security bookworm-security/main amd64 apache2-bin amd64 2.4.59-1-deb12u1 [1 380 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 libaprutil1 amd64 1.6.3-1 [87,8 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1 [13,6 kB]
Réception de :5 http://deb.debian.org/debian bookworm/main amd64 libaprutil1-ldap amd64 1.6.3-1 [11,8 kB]
Réception de :6 http://deb.debian.org/debian bookworm/main amd64 libcurl4 amd64 7.88.1-10+deb12u5 [390 kB]
Réception de :7 http://deb.debian.org/debian bookworm/main amd64 liblua5.3-0 amd64 5.3.6-2 [123 kB]
Réception de :8 http://deb.debian.org/debian bookworm/main amd64 ssl-cert all 1.1.2 [21,1 kB]
Réception de :9 http://security.debian.org/debian-security bookworm-security/main amd64 apache2-data all 2.4.59-1-deb12u1 [160 kB]
Réception de :10 http://security.debian.org/debian-security bookworm-security/main amd64 apache2-utils amd64 2.4.59-1-deb12u1 [207 kB]
Réception de :11 http://security.debian.org/debian-security bookworm-security/main amd64 apache2 amd64 2.4.59-1-deb12u1 [220 kB]
2 717 ko réceptionnés en 0s (8 192 ko/s)
Préconfiguration des paquets...
```

b) Installation PHP :

Pour installer PHP en tant que module Apache, vous devez procéder ainsi (Debian 12 possède les paquets PHP par défaut) :

Etape 1 : faite la commande « **apt install php libapache2-mod-php** »



```
root@Debian-ASSURMER: /home/debian-ass# apt install php libapache2-mod-php
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libapache2-mod-php8.2 libsodium23 php-common php8.2 php8.2-cli php8.2-common php8.2-openssl php8.2-readline psmisc
Paquets suggérés :
  php-pear
Les NOUVEAUX paquets suivants seront installés :
  libapache2-mod-php libapache2-mod-php8.2 libsodium23 php php-common php8.2 php8.2-cli php8.2-common php8.2-openssl php8.2-readline psmisc
0 mis à jour, 11 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 4 921 ko dans les archives.
Après cette opération, 22,6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://security.debian.org/debian-security bookworm-security/main amd64 php8.2-common amd64 8.2.18-1-deb12u1 [678 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 psmisc amd64 23.6-1 [259 kB]
Réception de :3 http://security.debian.org/debian-security bookworm-security/main amd64 php8.2-openssl amd64 8.2.18-1-deb12u1 [345 kB]
Réception de :4 http://security.debian.org/debian-security bookworm-security/main amd64 php8.2-readline amd64 8.2.18-1-deb12u1 [12,4 kB]
Réception de :5 http://security.debian.org/debian-security bookworm-security/main amd64 php8.2-cli amd64 8.2.18-1-deb12u1 [1 734 kB]
Réception de :6 http://deb.debian.org/debian bookworm/main amd64 php-common all 2:8.2+93 [13,1 kB]
Réception de :7 http://deb.debian.org/debian bookworm/main amd64 libsodium23 amd64 1.0.18-1 [161 kB]
Réception de :8 http://deb.debian.org/debian bookworm/main amd64 libapache2-mod-php all 2:8.2+93 [3 764 B]
Réception de :9 http://deb.debian.org/debian bookworm/main amd64 php all 2:8.2+93 [3 628 B]
Réception de :10 http://security.debian.org/debian-security bookworm-security/main amd64 libapache2-mod-php8.2 amd64 8.2.18-1-deb12u1 [1 674 kB]
Réception de :11 http://security.debian.org/debian-security bookworm-security/main amd64 php8.2 all 8.2.18-1-deb12u1 [37,1 kB]
4 921 ko réceptionnés en 0s (10,6 Mo/s)
Sélection du paquet psmisc précédemment désélectionné.
(Lecture de la base de données... 34480 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../00-psmisc_23.6-1_amd64.deb ...
Dépaquetage de psmisc (23.6-1) ...
Sélection du paquet php-common précédemment désélectionné.
Dépaquetage de php-common (2:8.2+93) ...
```

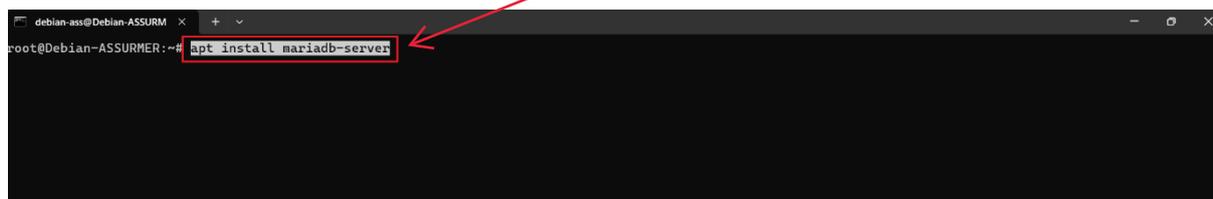
Etape 2 : faite la commande « **systemctl restart apache2** »



```
root@Debian-ASSURMER: /home/debian-ass# sudo systemctl restart apache2
```

c) Installation de MariaDB :

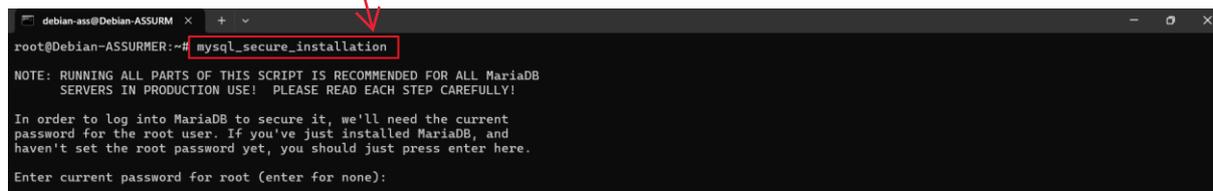
Etape 1 : faite la commande « **apt install mariadb-server** »



```
root@Debian-ASSURMER:~# apt install mariadb-server
```

Etape 2 : Une fois l'installation de MariaDB effectuée, nous allons lancer l'utilitaire de configuration du mot de passe root en saisissant la commande suivante :

« **mysql_secure_installation** »



```
root@Debian-ASSURMER:~# 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):
```

Installation de GLPI

Etape 3 : cliquez sur « **entrer** » (car le mot de passe actuelle est inexistant) puis écrivez « **Y** »

```
debian-ess@Debian-ASSURM x +
root@Debian-ASSURMER:~# 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] Y
```

Etape 4 : Ecrivez « **Y** » puis tapez votre nouveau mot de passe.

```
You already have your root account protected, so you can safely answer 'n'.
Change the root password? [Y/n] Y
```

Etape 5 : Ecrivez « **Y** »

```
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
```

Etape 6 : Ecrivez « **Y** »

```
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
```

Etape 7 : Ecrivez « **Y** »

```
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
```

Etape 8 : Ecrivez « **Y** »

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

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

La sécurisation de MariaDB est finie.

3. Création de la base de données « GLPI »

Pour commencer nous allons nous connecter à MariaDB afin de créer une base de données : La commande est : « **mysql -u root -p** » (saisir le mot de passe du root que vous avez défini lors de l'installation)

Ensuite nous allons créer une base de données nommée « glpi », créer un utilisateur « glpi », lui donner un mot de passe robuste et lui accorder tous les droits de lecture/écriture. Pour cela, nous saisissons les commandes :

Etape 1 : Pour créer la base de données faite la commande « **create database glpi;** »

Etape 2 : Afin de créer l'utilisateur et de lui accorder les droits, faites la commande « **grant all privileges on glpi.* to NomUtilisateur@localhost IDENTIFIED BY "MotDePasseRobuste";** »

Etape 3 : Pour mettre à jour les modifications faite la commande « **flush privileges;** »

```
root@Debian-Assurmer:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.11.6-MariaDB-0+deb12u1 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 glpi;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on glpi.* to glpi@localhost IDENTIFIED BY "Assurmer@glpi.";
Query OK, 0 rows affected (0,015 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> |
```

Etape 4 : Faite « **quit** (ou **exit**) » pour sortir de la base de données

II. Installation et décompression de GLPI

1. Installation de GLPI

Pour installer GLPI, il est nécessaire de connaître le lien de téléchargement du logiciel. En parcourant le web, on trouve l'adresse exacte de téléchargement de la dernière version stable.

Etape 1 : Faites la commande (Lien de téléchargement de la version de GLPI 10.0.15)

« **wget https://github.com/glpi-project/glpi/releases/download/10.0.15/glpi-10.0.15.tgz** »

```

root@Debian-ASSURMER:~# wget https://github.com/glpi-project/glpi/releases/download/10.0.15/glpi-10.0.15.tgz
--2024-04-29 14:51:26-- https://github.com/glpi-project/glpi/releases/download/10.0.15/glpi-10.0.15.tgz
Résolution de github.com [github.com]: 140.82.121.3
Connexion à github.com [github.com]:140.82.121.3:443... connecté.
requête HTTP transmise, en attente de la réponse_ 302 Found
Emplacement : https://objects.githubusercontent.com/github-production-release-asset-2665be/39182755/522ff5e8-464a-4ea3-85f2-65c5089274b3?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA3PQW4ZA%2F20240429%2Fus-east-1%2F%3Faws4_request&X-Amz-Date=20240429T125126Z&X-Amz-Expires=300&X-Amz-Signature=f6382a74c97c04fb8e9dd1b3f1eafe951d8fc215e57d1cbdf740116a998b576X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=39182755&response-content-disposition=attachment%3B%2Ffilename%3Dglpi-10.0.15.tgz&response-content-type=application%2Foctet-stream [suivant]
--2024-04-29 14:51:26-- https://objects.githubusercontent.com/github-production-release-asset-2665be/39182755/522ff5e8-464a-4ea3-85f2-65c5089274b3?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVCODYLSA3PQW4ZA%2F20240429%2Fus-east-1%2F%3Faws4_request&X-Amz-Date=20240429T125126Z&X-Amz-Expires=300&X-Amz-Signature=f6382a74c97c04fb8e9dd1b3f1eafe951d8fc215e57d1cbdf740116a998b576X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=39182755&response-content-disposition=attachment%3B%2Ffilename%3Dglpi-10.0.15.tgz&response-content-type=application%2Foctet-stream
Résolution de objects.githubusercontent.com [objects.githubusercontent.com]: 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connexion à objects.githubusercontent.com [objects.githubusercontent.com]:185.199.110.133:443... connecté.
requête HTTP transmise, en attente de la réponse_ 200 OK
Taille : 59757265 (57M) [application/octet-stream]
Sauvegarde en : « glpi-10.0.15.tgz »

glpi-10.0.15.tgz 100%[=====] 56,99M 5,42MB/s ds 9,7s
2024-04-29 14:51:36 (5,86 MB/s) - « glpi-10.0.15.tgz » sauvegardé [59757265/59757265]
    
```

2. Décompression de GLPI

Etape 1 : Une fois l'archive téléchargée, il faut la décompresser en saisissant :

« **tar xvf glpi-10.0.15.tgz** »

Un dossier « glpi » est créé (et contient tous les fichiers nécessaires à l'installation de GLPI) :

```

root@Debian-ASSURMER:~# ls
glpi  glpi-10.0.15.tgz
root@Debian-ASSURMER:~#
    
```

On va maintenant déplacer ce dossier décompressé nommé « glpi » dans l'arborescence d'Apache et à l'endroit suivant : **/var/www/**

Etape 2 : faite la commande « **mv glpi /var/www/glpi** »

```

root@Debian-Assurmer:~# cd /var/www/
root@Debian-Assurmer:/var/www# ls
glpi  html
root@Debian-Assurmer:/var/www#
    
```

III. Sécurisation de GLPI

1. Création des répertoires

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.

a. Création du répertoire (`/etc/glpi`)

Etape 1 : Faites les commandes « `mkdir /etc/glpi` » et « `chown www-data /etc/glpi/` »

```

root@Debian-Assurmer:~# mkdir /etc/glpi
root@Debian-Assurmer:~# chown www-data /etc/glpi/
root@Debian-Assurmer:~#
    
```

Etape 2 : Nous allons déplacer le répertoire "config" de GLPI vers ce nouveau dossier. Faites la commande « `mv /var/www/glpi/config /etc/glpi` »

```

root@Debian-Assurmer:~# mv /var/www/glpi/config /etc/glpi
root@Debian-Assurmer:~#
    
```

b. Création du répertoire (`/var/lib/glpi`)

Etape 1 : Faites les commandes « `mkdir /var/lib/glpi` » et « `chown www-data /var/lib/glpi` »

```

root@Debian-Assurmer:~# mkdir /var/lib/glpi
root@Debian-Assurmer:~# chown www-data /var/lib/glpi
root@Debian-Assurmer:~#
    
```

Etape 2 : Nous allons déplacer le répertoire "files" de GLPI vers ce nouveau dossier. Faites la commande « `mv /var/www/glpi/files /var/lib/glpi` »

```

root@Debian-Assurmer:~# mv /var/www/glpi/files /var/lib/glpi
root@Debian-Assurmer:~#
    
```

c. Création du répertoire (`/var/log/glpi`)

Etape 1 : Faites les commandes « `mkdir /var/log/glpi` » et « `chown www-data /var/log/glpi` »

```

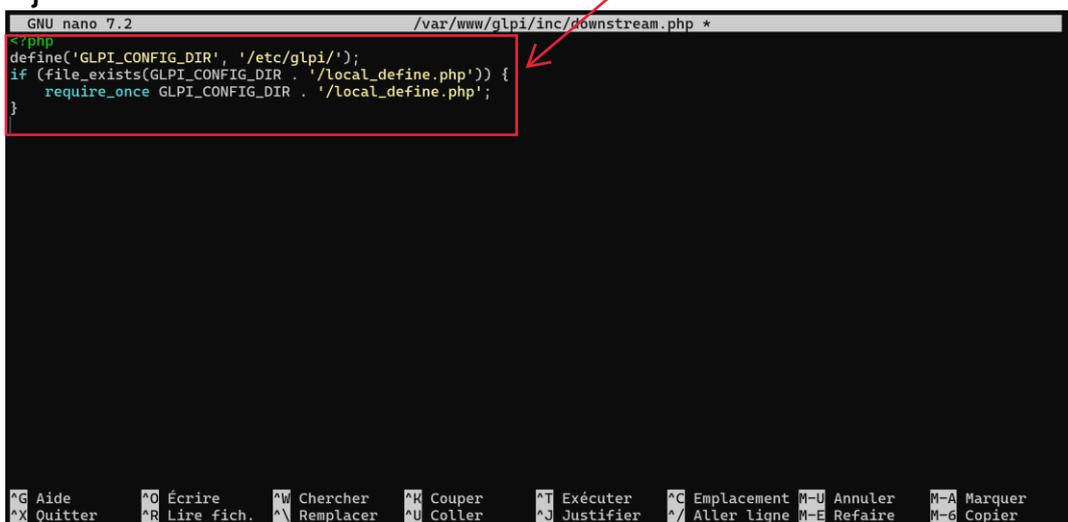
root@Debian-Assurmer:~# mkdir /var/log/glpi
root@Debian-Assurmer:~# chown www-data /var/log/glpi
root@Debian-Assurmer:~#
    
```

2. 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 fraîchement créés.

Etape 1 : Création de ce premier fichier « `nano /var/www/glpi/inc/downstream.php` » et y ajouter ceci :

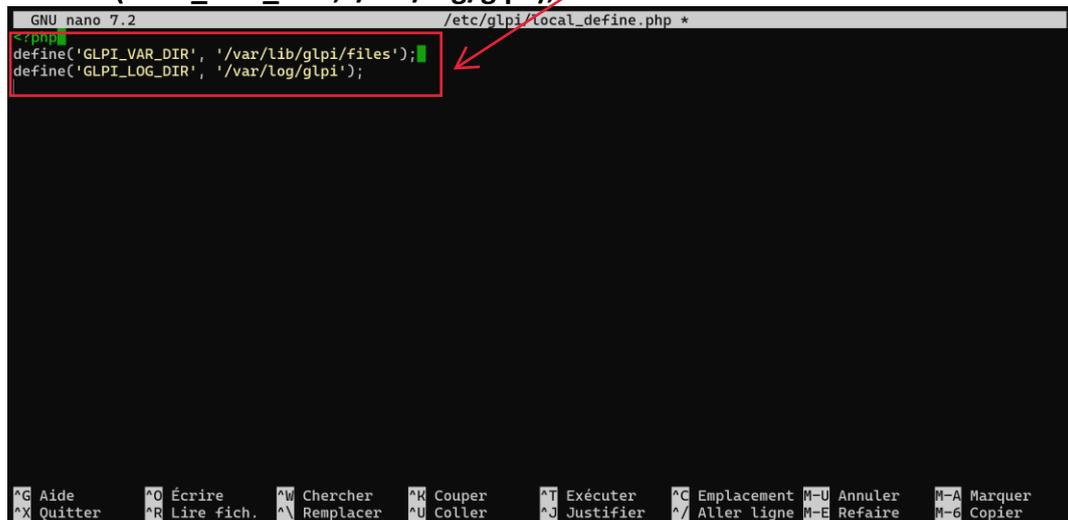
```
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
    require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```



Puis sauvegarder avec « CTRL+X », ensuite « O » et enfin « Entrer »

Etape 2 : Création du second fichier « `nano /etc/glpi/local_define.php` » et y ajouter ceci :

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



Puis sauvegarder avec « CTRL+X », ensuite « O » et enfin « Entrer »

3. Activation de la sécurisation des cookies de GLPI

Etape 1 : Faites la commande « `nano /etc/php/8.2/phpdbg/php.ini` » et recherchez avec « `CTRL+W` » l'option « `session.cookie_httponly` »

```
GNU nano 7.2 /etc/php/8.2/phpdbg/php.ini
[PHP]
;;;;;;;;;;;;;;;;;;;;;;;;;
; About php.ini ;
;;;;;;;;;;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations.
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or the
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file

; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.

Recherche: session.cookie_httponly
^G Aide          M-C Resp.casse  M-B ->Arrière   ^P Plus ancien   ^T Aller ligne
^C Annuler       M-R Exp.ration.  ^R Remplacer     ^N Plus récent
```

Etape 2 : Une fois que vous avez trouvé l'option, indiquez la valeur « `1` » pour l'activer.

```
GNU nano 7.2 /etc/php/8.2/phpdbg/php.ini
session.cookie_lifetime = 0

; The path for which the cookie is valid.
; https://php.net/session.cookie-path
session.cookie_path = /

; The domain for which the cookie is valid.
; https://php.net/session.cookie-domain
session.cookie_domain =

; Whether or not to add the httpOnly flag to the cookie, which makes it
; inaccessible to browser scripting languages such as JavaScript.
; https://php.net/session.cookie-httponly
session.cookie_httponly = 1

; Add SameSite attribute to cookie to help mitigate Cross-Site Request Forgery (CSRF/XSRF)
; Current valid values are "Strict", "Lax" or "None". When using "None",
; make sure to include the quotes, as `none` is interpreted like `false` in ini files.
; https://tools.ietf.org/html/draft-west-first-party-cookies-07
session.cookie_samesite =

; Handler used to serialize data. php is the standard serializer of PHP.
; https://php.net/session.serialize-handler
session.serialize_handler = php

; Defines the probability that the 'garbage collection' process is started on every
```

Nous allons répéter ces formules :

Etape 3 : Faites la commande « `nano /etc/php/8.2/apache2/php.ini` » et recherchez avec « `CTRL+W` » l'option « `session.cookie_httponly` »

Etape 4 : Une fois que vous avez trouvé l'option, indiquez la valeur « `1` » pour l'activer.

Etape 5 : Faites la commande « `systemctl restart apache2` »

4. Configuration de Apache2

Passons à la configuration du serveur web Apache2. Nous allons créer un nouveau fichier de configuration qui va permettre de configurer le VirtualHost dédié à GLPI. Dans mon cas, le fichier s'appelle « assurmer.support.it.conf » en référence au nom de domaine choisi pour accéder à GLPI : assurmer.support.it. 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.

Etape 1 : Faites la commande `nano /etc/apache2/sites-available/assurmer.support.it.conf`

Etape 2 : Ajouter ceci :

```
<VirtualHost *:80>
  ServerName assurmer.support.it

  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 its> # 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>
```

```
GNU nano 7.2 /etc/apache2/sites-available/assurmer.support.it.conf *
~VirtualHost *:80~
ServerName assurmer.support.it
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 its>
# 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>
```

Puis sauvegarder avec « CTRL+X », ensuite « O » et enfin « Entrer »

Etape 3 : Faites la commande « `a2enmod rewrite` » puis « `systemctl restart apache2` »

Etape 4 : Activez le site avec la commande « `a2ensite assurmer.support.it.conf` »

```
root@Debian-Assurmer:~# a2ensite assurmer.support.it.conf
Site assurmer.support.it already enabled
root@Debian-Assurmer:~#
```

IV. Lancement de l'installation de GLPI

Avant de lancer l'installation de GLPI, vous devez ajouter les modules PHP suivants qui sont nécessaires à GLPI.

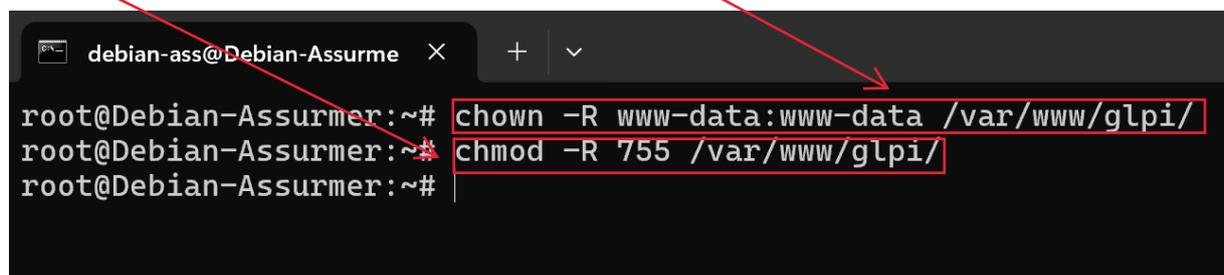
Etape 1 : Entrez la commande si dessous dans la machine Debian :

```
« apt install php8.2-curl php8.2-gd php8.2-mbstring php8.2-zip php8.2-xml php8.2-ldap  
php8.2-intl php8.2-mysql php8.2-dom php8.2-simplexml php8.2-json php8.2-phpdbg php8.2-  
cgi »
```

```
root@Debian-ASSURMER:~# apt install php8.2-curl php8.2-gd php8.2-mbstring php8.2-zip php8.2-xml php8.2-ldap php8.2-intl php8.2-mysql php8.2-dom php8.2-simplexml php8.2-json php8.2-phpdbg php8.2-cgi
```

Etape 2 : Il faut donner la propriété du dossier GLPI à l'administrateur Apache « www-data ». Tapez les commandes suivantes :

```
chown -R www-data:www-data /var/www/glpi/  
chmod -R 755 /var/www/glpi/
```

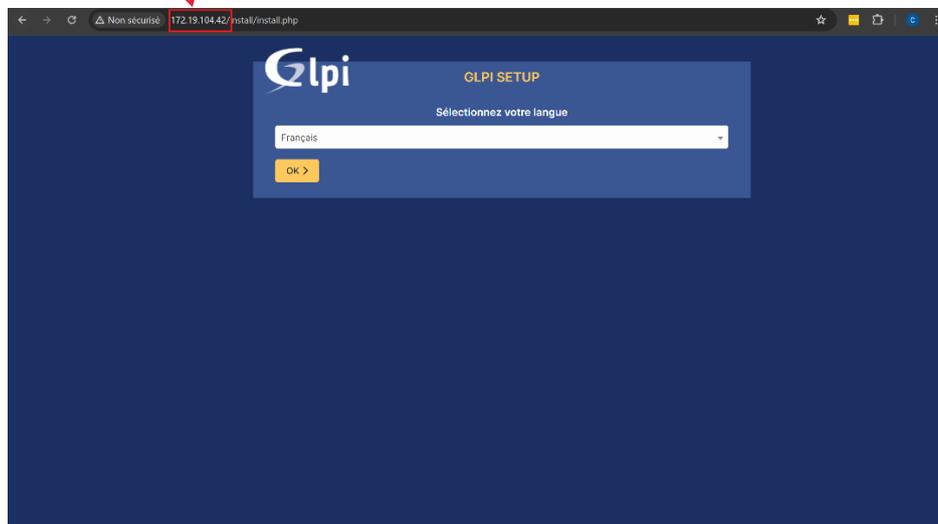


```
root@Debian-Assurmer:~# chown -R www-data:www-data /var/www/glpi/  
root@Debian-Assurmer:~# chmod -R 755 /var/www/glpi/  
root@Debian-Assurmer:~#
```

Etape 3 : Il faut redémarrer le serveur Apache : « **systemctl restart apache2** »

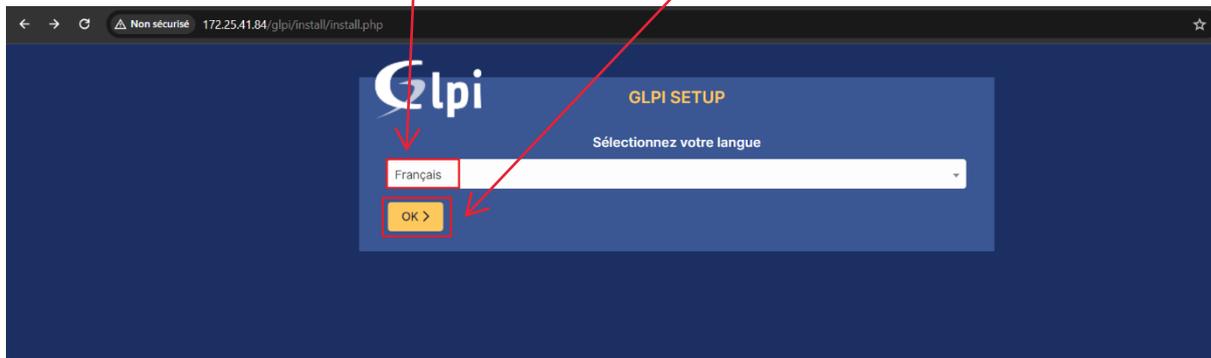
Pour terminer l'installation de l'helpdesk GLPI, il suffit d'ouvrir le navigateur et de saisir, dans la barre d'adresse, l'IP de votre serveur web Apache.

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



Installation de GLPI

Etape 1 : Sélectionnez votre langue et cliquez sur « OK »



Etape 2 : Cliquez sur « Continuer »

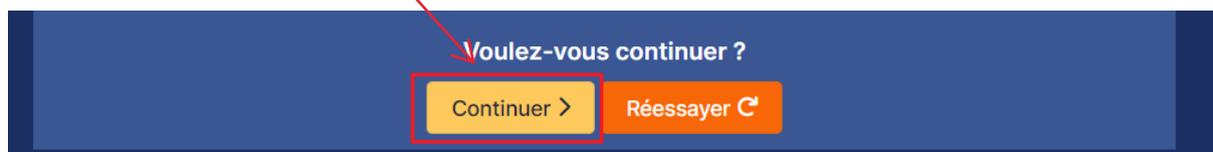


Installation de GLPI

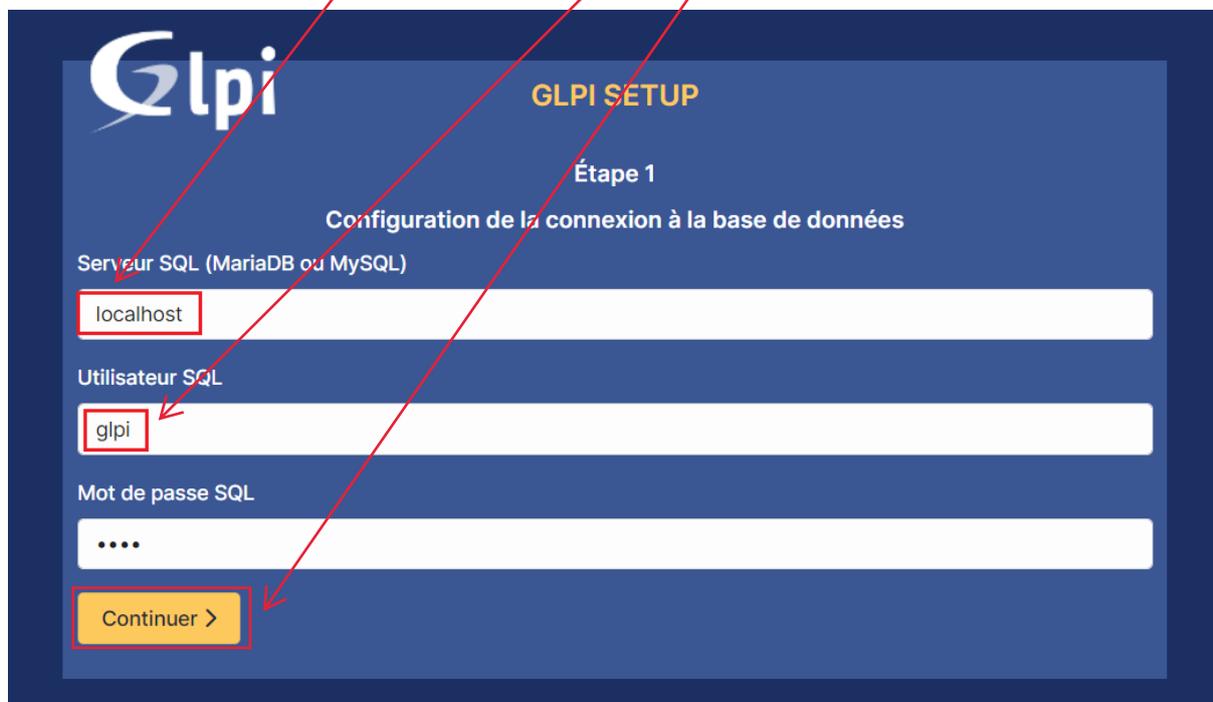
Etape 3 : Cliquez sur « Installer »



Etape 4 : Cliquez sur « Continuer »



Etape 5 : On indique « localhost » et l'utilisateur « glpi » précédemment configuré (avec son mot de passe !) et on clique sur le bouton « Continuer »



Etape 6 : Sélectionnez la base « **GLPI** » précédemment créée, puis cliquez sur « **Continuez** »



GLPI

GLPI SETUP

Étape 2
Test de connexion à la base de données

✓ Connexion à la base de données réussie

Veillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

glpi

Continuer >

Etape 7 : Il faut **attendre l'initialisation** de la base de données (attention cette phase peut prendre du temps ; soyez patient !). Si tout se passe bien au niveau de l'initialisation de la base, une fenêtre s'affiche ; cliquez le bouton « **Continuez** » :



GLPI

GLPI SETUP

Étape 3
Initialisation de la base de données.

OK - La base a bien été initialisée

Continuer >

Etape 8 : Cliquez sur « **Continuez** »

GLPI

GLPI SETUP

Étape 4
Récolter des données

Envoyer "statistiques d'usage"

Nous avons besoin de vous pour améliorer GLPI et son écosystème de plugins !

Depuis GLPI 9.2, nous avons introduit une nouvelle fonctionnalité de statistiques appelée "Télémetrie", qui envoie anonymement, avec votre permission, des données à notre site de télémétrie. Une fois envoyées, les statistiques d'usage sont agrégées et rendues disponibles à une large audience de développeurs GLPI.

Dites-nous comment vous utilisez GLPI pour que nous améliorions GLPI et ses plugins !

[Voir ce qui serait envoyé...](#)

Référez votre GLPI

Par ailleurs, si vous appréciez GLPI et sa communauté, prenez une minute pour référencer votre organisation en remplissant le formulaire suivant [Le formulaire d'inscription](#)

Continuer >

Etape 9 : Cliquez sur « **Continuez** »

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 pré-configurés ?

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.

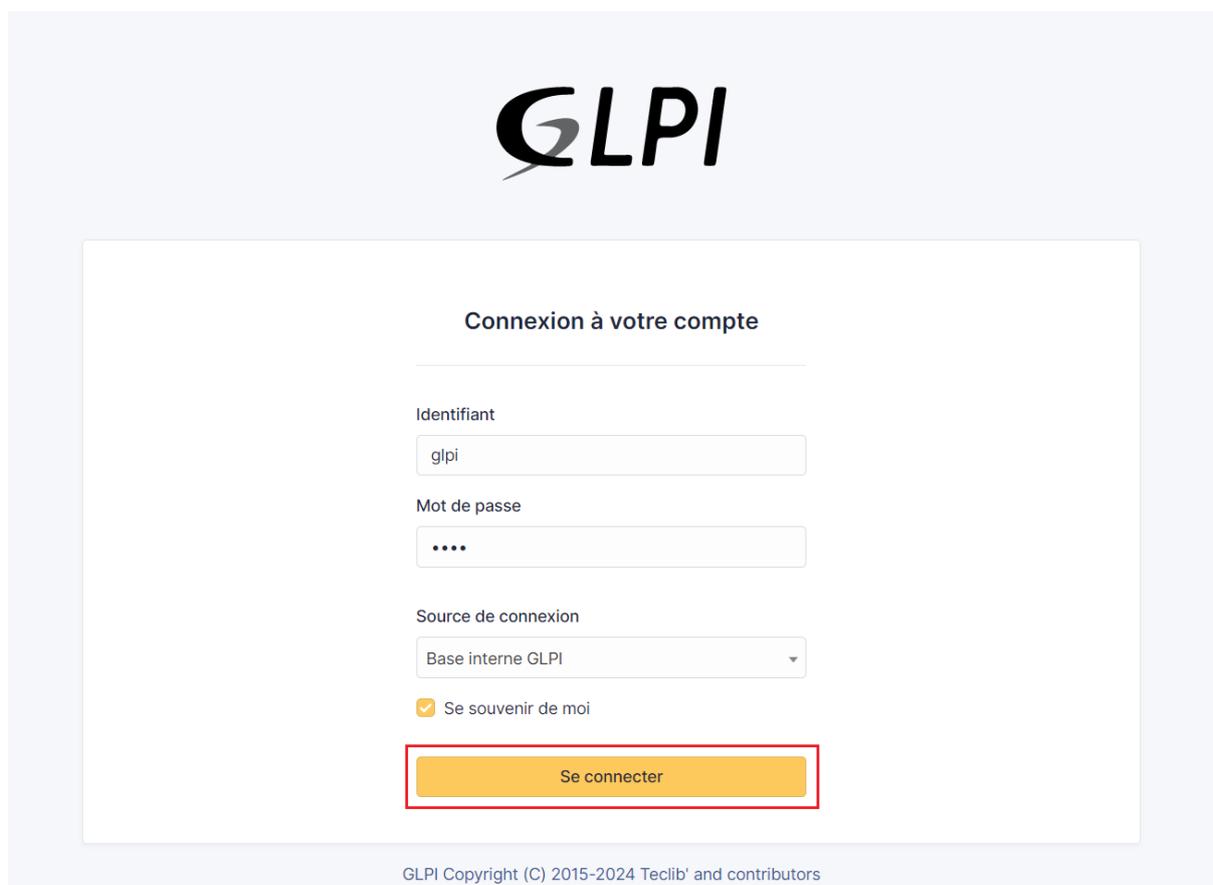
Sur ce même espace, vous pourrez contacter un partenaire officiel pour vous aider dans votre intégration de GLPI.

Continuer >

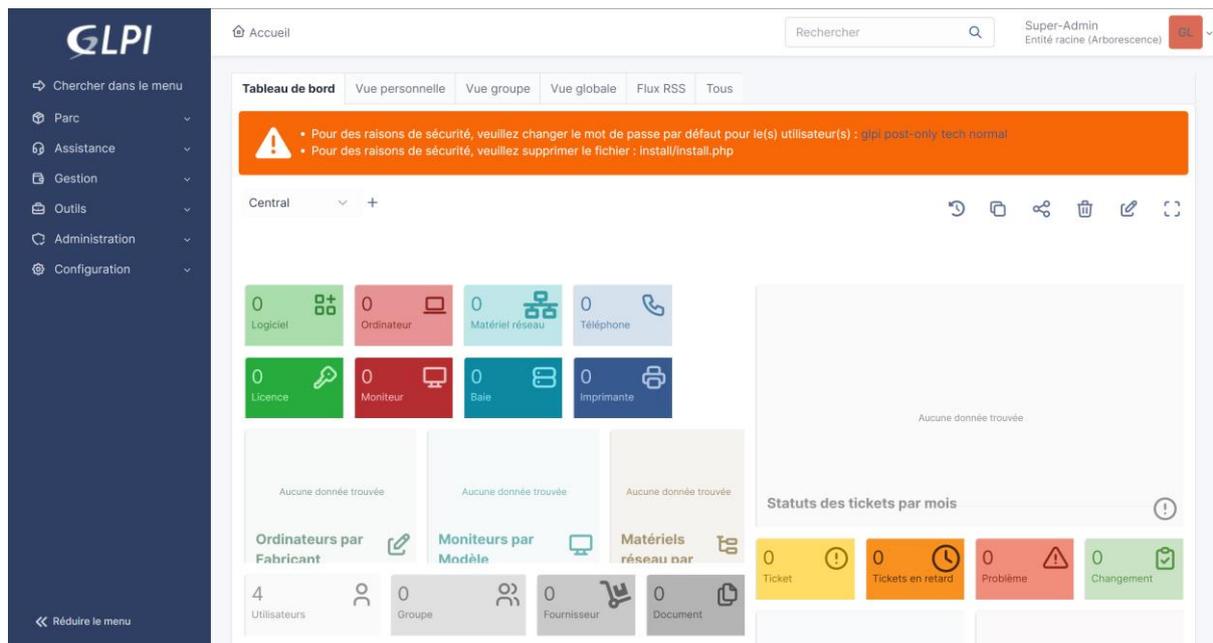
Etape 10 : Vous pouvez remarquer les **comptes** par défaut de **GLPI**. Cliquez sur « **Utiliser GLPI** »



Etape 11 : Vous pouvez maintenant utiliser GLPI en utilisant les comptes par défaut.



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)

Etape 1 : Faites la commande « **rm /var/www/glpi/install/install.php** »

```
root@Debian-Assurmer:~# rm /var/www/glpi/install/install.php
root@Debian-Assurmer:~#
```

Voilà, c'est fait. Désormais, votre GLPI est prêt à être utilisé et configuré (création d'utilisateurs, de catégories, de tickets, etc...).



| Auteur | Date de création | Version | Valideur | Destinataire | Diffusion | Nombre de pages |
|-------------------------|------------------|---------|----------|---------------|--------------------|-----------------|
| Bruno De Carvalho Lopes | 24/04/2024 | 1.0 | En cours | Technicien IT | Teams Equipe IT | 10 |

- I. Qu'est-ce que LDAP ? 3**
 - 1. Prérequis : 3
 - 2. LDAP, c'est quoi ?..... 3
- II. Configuration LDAP sur GLPI 10 3**
 - 1. Mise en place du lien entre GLPI et l'AD..... 3
 - 2. Test de la liaison LDAP 7
- III. Importation des utilisateurs de l'Active Directory dans GLPI..... 8**

I. Qu'est-ce que LDAP ?

Dans cette fiche guide, nous allons configurer une liaison « **LDAP** » entre un Active Directory et GLPI 10.

1. Prérequis :

- Un serveur Windows fonctionnel avec le rôle AD/DS installé
- GLPI 10 installé et fonctionnel

2. LDAP, c'est quoi ?

LDAP (Lightweight Directory Access Protocol) est un protocole standard permettant de gérer des annuaires, c'est à dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.

II. Configuration LDAP sur GLPI 10

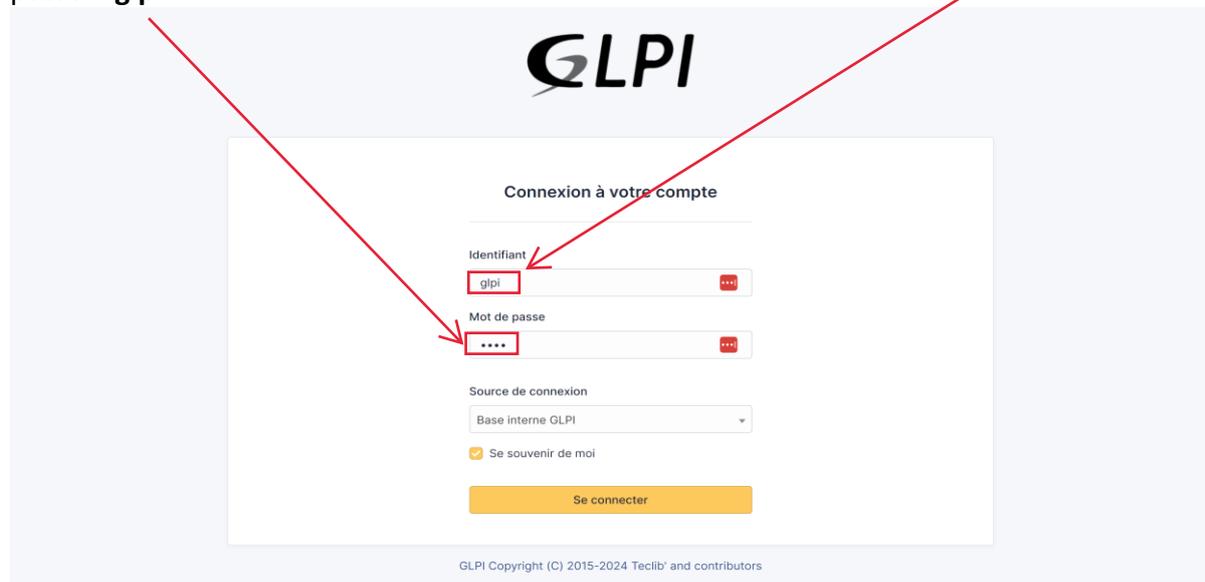
Dans cette partie, nous allons expliquer comment mettre en place une liaison LDAP entre un Active Directory et l'helpdesk GLPI 10.

L'objectif est d'importer l'ensemble des utilisateurs de l'AD vers GLPI de manière à ne pas avoir à créer des utilisateurs dans GLPI.

De plus, les utilisateurs du domaine conserveront leurs identifiants et mots de passe de domaine ce qui facilitera et simplifiera la connexion à l'helpdesk.

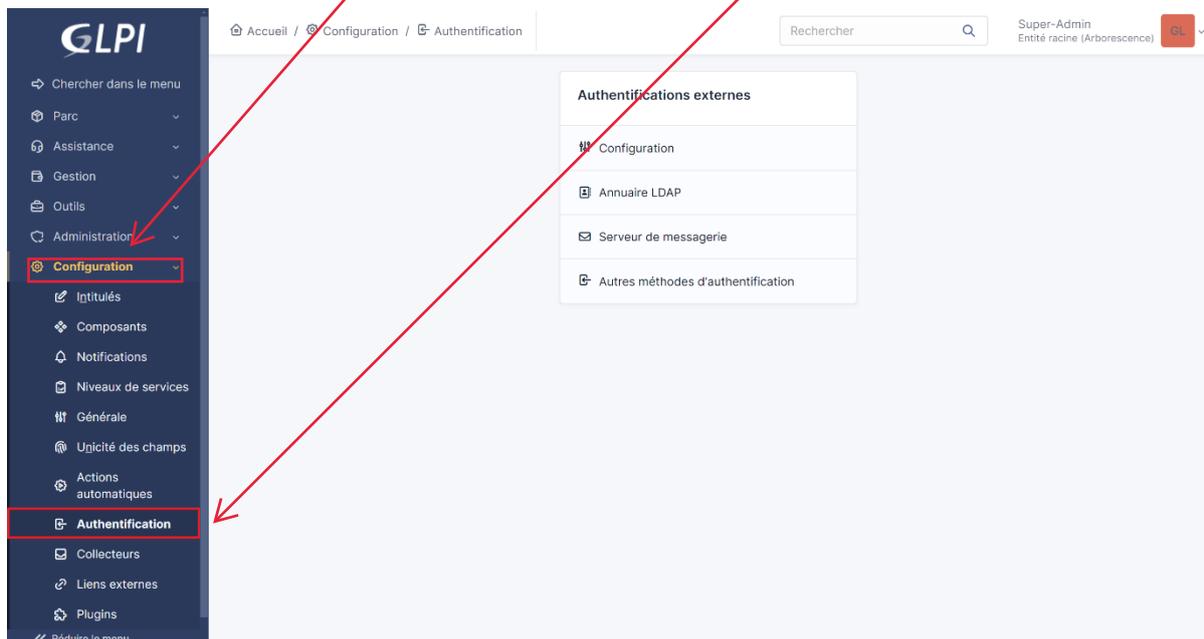
1. Mise en place du lien entre GLPI et l'AD

Etape 1 : Se connecter à GLPI avec le compte administrateur par défaut : « **gipi** » et mot de passe « **gipi** »

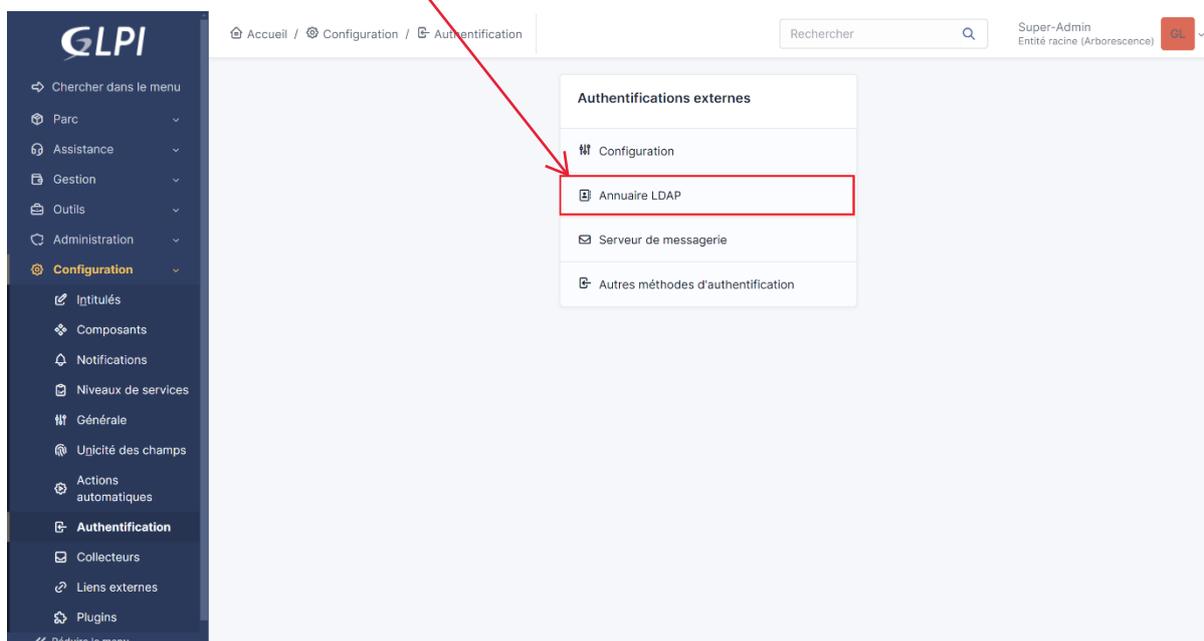


The screenshot shows the GLPI login interface. At the top, the GLPI logo is displayed. Below it, the heading "Connexion à votre compte" is centered. There are two input fields: "Identifiant" (Username) containing "gipi" and "Mot de passe" (Password) containing four dots. Both fields are highlighted with red boxes and have red arrows pointing to them from the text above. Below the password field is a dropdown menu for "Source de connexion" set to "Base interne GLPI". There is a checked checkbox for "Se souvenir de moi" and a yellow "Se connecter" button at the bottom. The footer text reads "GLPI Copyright (C) 2015-2024 Teclib' and contributors".

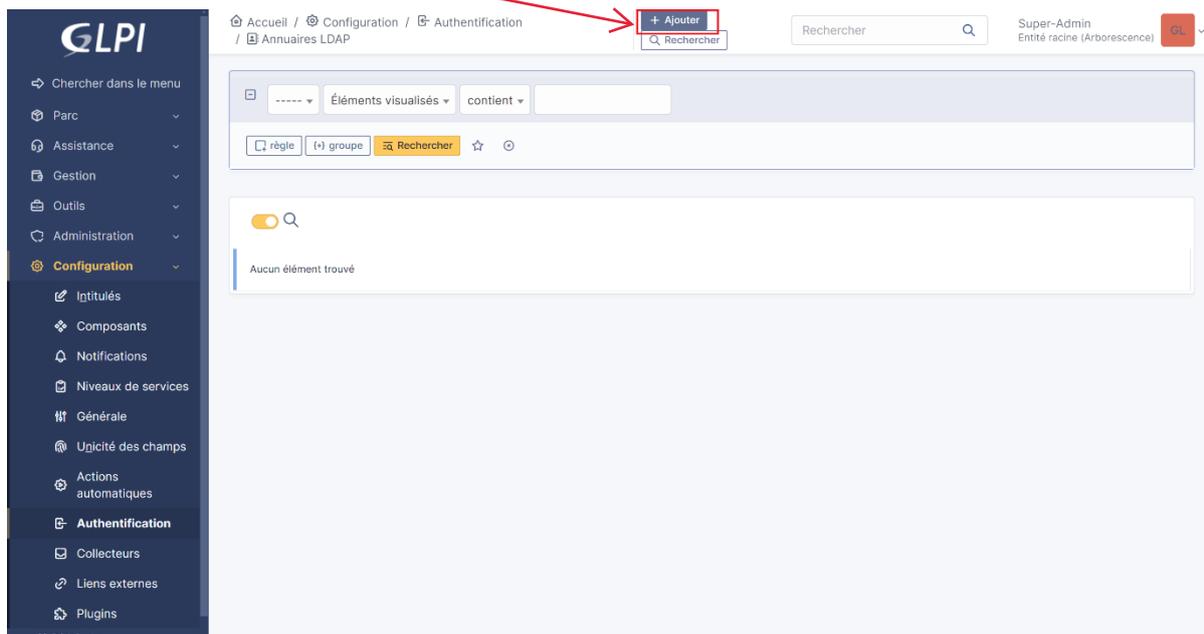
Etape 2 : Dans le menu « **Configuration** », cliquez sur « **Authentification** » pour obtenir la fenêtre suivante :



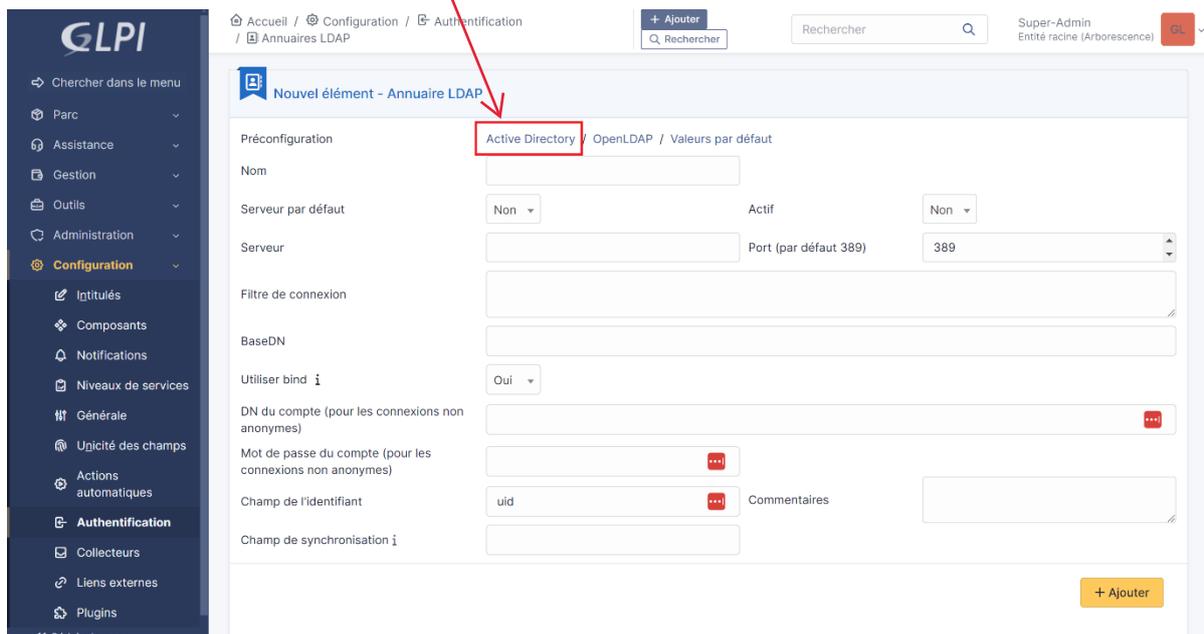
Etape 3 : Cliquez sur « **Annuaire LDAP** »



Etape 4 : Cliquez sur « Ajouter »

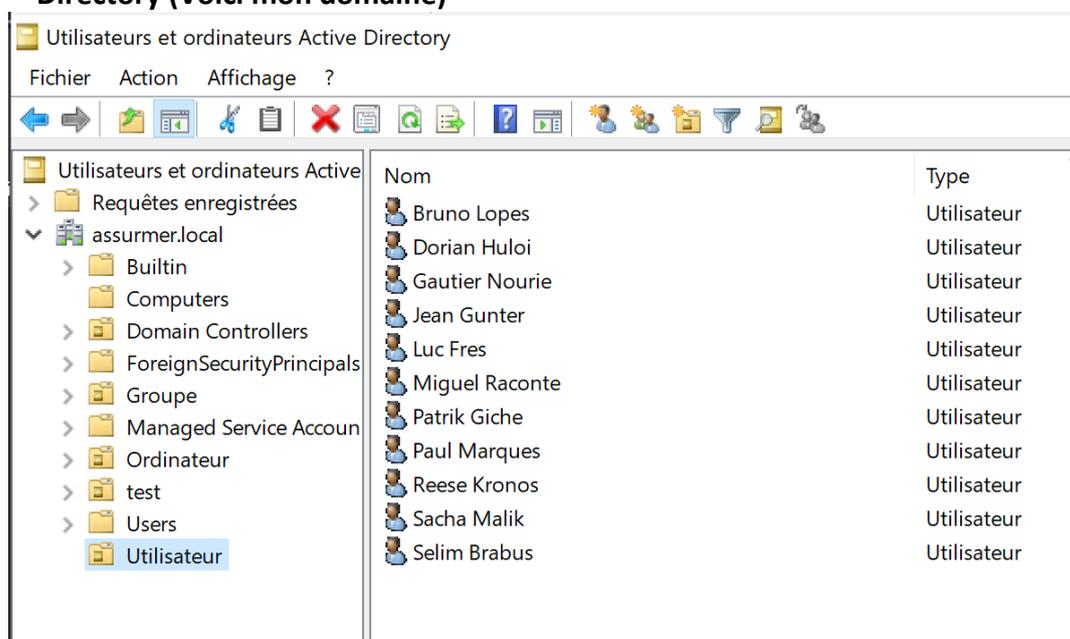


Etape 5 : Cliquez sur « Active Directory » dans la partie pré-configuration.



Etape 6 : Il faut maintenant configurer la liaison LDAP en fonction des caractéristiques de votre Active Directory et cliquer le bouton « **Ajouter** » quand tout est indiqué (voir fenêtre ci-dessous) :

- 1- **Nom du nouvel élément**
- 2- **Adresse IP de votre serveur Active Directory**
- 3- **On complète ici, l'arborescence qui correspond à vos utilisateurs dans l'Active Directory (Voici mon domaine)**



- 4- **Saisir l'identifiant d'un compte avec des droits dans l'Active Directory**
- 5- **Saisir le mot de passe du compte**

2. Test de la liaison LDAP

Une fois les paramètres de votre Active Directory renseignés et sauvegardés, il faut tester la connexion entre GLPI et l'AD de votre serveur AD/DS :

Etape 1 : Cliquez sur le serveur AD que vous venez de configurer

The screenshot shows the GLPI interface with the 'Configuration' menu on the left. The main content area displays a table of LDAP servers. The entry 'SRV ASSURMER AD' is highlighted with a red box. A red arrow points from the text 'Etape 1' to this entry.

| NOM | SERVEUR | DERNIERE MODIFICATION | ACTIF |
|-----------------|--------------|-----------------------|-------|
| SRV ASSURMER AD | 192.168.1.50 | 2024-04-24 14:35 | Oui |

Etape 2 : Cliquez, dans le menu de gauche, sur « Tester » et cliquez le bouton jaune « Tester » :

The screenshot shows the GLPI interface with the 'Annuaire LDAP - SRV ASSURMER AD' page. The 'Tester' button in the left sidebar is highlighted with a red box, and a red arrow points to it. The 'Tester' button in the dialog box is also highlighted with a red box, and a red arrow points to it.

Si tout est correctement paramétré, le message « Test réussi » s’affiche. Vous pouvez maintenant préparer l’importation des utilisateurs de votre Active Directory !

Test réussi : Serveur principal SRV ASSURMER AD

Tester

III. Importation des utilisateurs de l’Active Directory dans GLPI

Nous allons ici importer des utilisateurs qui figurent dans l’annuaire de notre serveur Windows (nous avons créé préalablement des utilisateurs dans l’Active Directory).

On retourne sur l’interface de GLPI pour effectuer l’importation des utilisateurs de l’AD :

Etape 1 : Cliquez sur « Administration » - « Utilisateurs » - « Liaison annuaire LDAP »

The screenshot shows the GLPI interface. On the left, the 'Administration' menu is expanded to 'Utilisateurs'. In the top right, the 'Liaison annuaire LDAP' option is highlighted. Below, a table lists users with columns for ID, identifier, family name, emails, phone, location, and active status.

| IDENTIFIANT | NOM DE FAMILLE | COURRIELS | TÉLÉPHONE | LIEU | ACTIF |
|-------------|----------------|-----------|-----------|------|-------|
| BL | bruno.lopes | Lopes | | | Oui |
| DH | dorian.huloi | Huloi | | | Oui |
| SN | gautier.nourie | Nourie | | | Oui |
| GL | glpi | | | | Oui |
| S | glpi-system | Support | | | Oui |
| JG | jean.gunter | Gunter | | | Oui |
| LF | luc.fres | Fres | | | Oui |
| MR | miguel.raconte | Raconte | | | Oui |
| NG | normal | | | | Oui |

Etape 2 : Cliquez sur « Importation de nouveaux utilisateurs »

The screenshot shows the 'Importation en masse d'utilisateurs depuis un annuaire LDAP' configuration page. The 'Importation de nouveaux utilisateurs' option is highlighted with a red box.

Etape 3 : Cliquez sur « Mode expert »

The screenshot shows the 'Importation de nouveaux utilisateurs' page in GLPI. The left sidebar contains the navigation menu with 'Utilisateurs' selected. The top navigation bar shows 'Administration / Utilisateurs / Annuaire LDAP'. The main content area is titled 'Importation de nouveaux utilisateurs' and features a 'Mode expert' button in the top right corner, which is highlighted with a red box. A red arrow points from this button to another 'Mode expert' button located in the top right of the main content area. Below this, there is a section for search criteria with fields for 'Identifiant', 'Courriel', 'Prénom', 'Titre', 'Champ de synchronisation (objectguid)', 'Nom de famille', 'Téléphone', and 'Téléphone mobile'. A 'Rechercher' button is at the bottom of this section.

Etape 4 : Cliquez sur « Rechercher »

The screenshot shows the 'Importation de nouveaux utilisateurs' page in GLPI, now in 'Mode simplifié' view. The left sidebar and top navigation bar are the same. The main content area is titled 'Importation de nouveaux utilisateurs' and features a 'Mode simplifié' button in the top right corner. Below this, there are two input fields: 'BaseDN' with the value 'OU=Utilisateur,DC=assurmer,DC=local' and 'Filtre de recherche des utilisateurs' with the value '(& (samaccountname=*) (& (objectClass=user)(objectCategory=person)! (userAccountControl:1.2.840.113556.1.4.803:=2)))'. A 'Rechercher' button is at the bottom of this section, highlighted with a red box. A red arrow points from this button to another 'Rechercher' button located in the top right of the main content area.

Etape 5 : Sélectionnez les utilisateurs et cliquez sur « Actions »

The screenshot shows the 'Importation de nouveaux utilisateurs' interface. The left sidebar is expanded to 'Administration' > 'Utilisateurs'. The main area shows a search filter and a table of users. The 'Actions' button in the table is highlighted with a red box, and a red arrow points to it from the step title.

| CHAMP DE SYNCHRONISATION | UTILISATEURS | DERNIERE MISE À JOUR DANS L'ANNUAIRE LDAP |
|-------------------------------------|--------------------------------------|---|
| <input checked="" type="checkbox"/> | e2b32d68-1227-419d-960e-508a189d6c31 | sacha.malik |
| <input checked="" type="checkbox"/> | 80216b5e-ae90-4b28-bf0f-5ba3a9b3f796 | reese.kronos |
| <input checked="" type="checkbox"/> | 167a6705-8275-4273-bb4d-4128b2ee6e8c | paul.marques |
| <input checked="" type="checkbox"/> | 0f77dc81-f7dc-4494-88ec-db355ca23ace | patrik.giche |
| <input checked="" type="checkbox"/> | Champ de synchronisation | Utilisateurs |

Etape 6 : Sélectionnez « Importer » puis, cliquez sur « Envoyer »

The screenshot shows the 'Importation de nouveaux utilisateurs' interface with an 'Actions' modal open. The 'Importer' and 'Envoyer' buttons in the modal are highlighted with red boxes, and red arrows point to them from the step title.

En cliquant, dans le menu de gauche, sur « Administration » et « Utilisateurs », on constate que nos utilisateurs de l'AD ont bien été importés dans GLPI

Enfin, vous pouvez vous connecter avec vos comptes de l'Active Directory en utilisant leurs identifiants.



ASSURMER

| Auteur | Date de création | Version | Valideur | Destinataire | Diffusion | Nombre de pages |
|-------------------------|-------------------------|----------------|-----------------|---------------------|--------------------|------------------------|
| Bruno De Carvalho Lopes | 24/04/2024 | 1.0 | En cours | Technicien IT | Teams Equipe IT | 8 |

| | | |
|------|---|---|
| I. | Qu'est-ce que l'agent GLPI ? | 3 |
| 1. | Présentation : | 3 |
| 2. | Prérequis : | 3 |
| II. | Création d'un dossier pour le logiciel « GLPI agent » | 3 |
| III. | Création d'une GPO pour le déploiement de GLPI Agent | 5 |

I. Qu'est-ce que l'agent GLPI ?

1. Présentation :

GLPI 10.0.0 intègre en natif un inventaire qui peut être réalisé à l'aide d'un agent nommé « GLPI-Agent ».

L'agent GLPI est un programme utilisé pour exécuter l'inventaire automatique. Il prend également en charge l'exécution de quelques autres tâches telles que le déploiement de packages, la collecte d'informations, la découverte et l'inventaire des périphériques réseau, l'inventaire distant ESX. Il prend également en charge l'inventaire sans agent grâce à sa tâche d'inventaire à distance.

Cette procédure vous présente la méthode pour effectuer une remontée d'inventaire des ordinateurs d'un domaine avec une GPO et en utilisant le nouvel agent GLPI.

2. Prérequis :

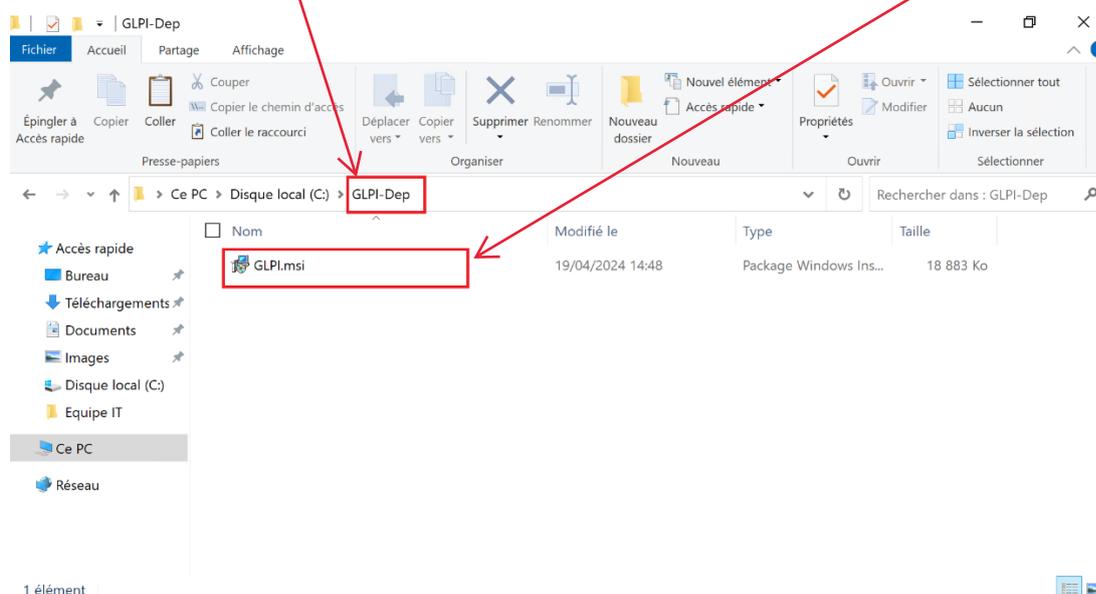
- D'un serveur avec le rôle AD/DS déjà configuré
- D'une liaison LDAP déjà configurée
- D'un serveur LAMP (dans notre cas, nous disposons d'une machine Debian 12)
- D'une version de GLPI fonctionnant avec GLPI 10.0 au minimum

II. Création d'un dossier pour le logiciel « GLPI agent »

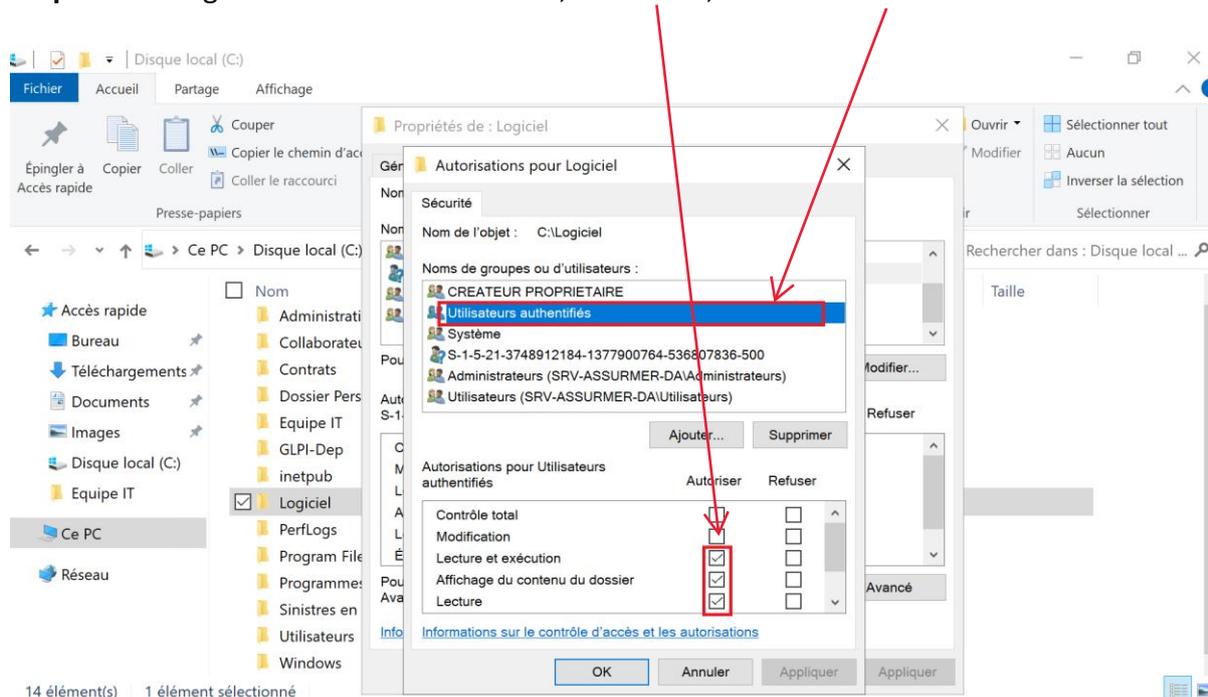
Avant de lancer le déploiement, il est nécessaire de créer un dossier de partage sur notre serveur qui accueillera le logiciel.

Etape 1 : Téléchargez l'agent GLPI à cette adresse, on utilisera la version au format « msi » <https://github.com/glpi-project/glpi-agent/releases/download/1.4/GLPI-Agent-1.4-x64.msi>

Etape 2 : Créez un dossier sur votre serveur et ajoutez dedans le package « msi » de l'agent GLPI téléchargé.



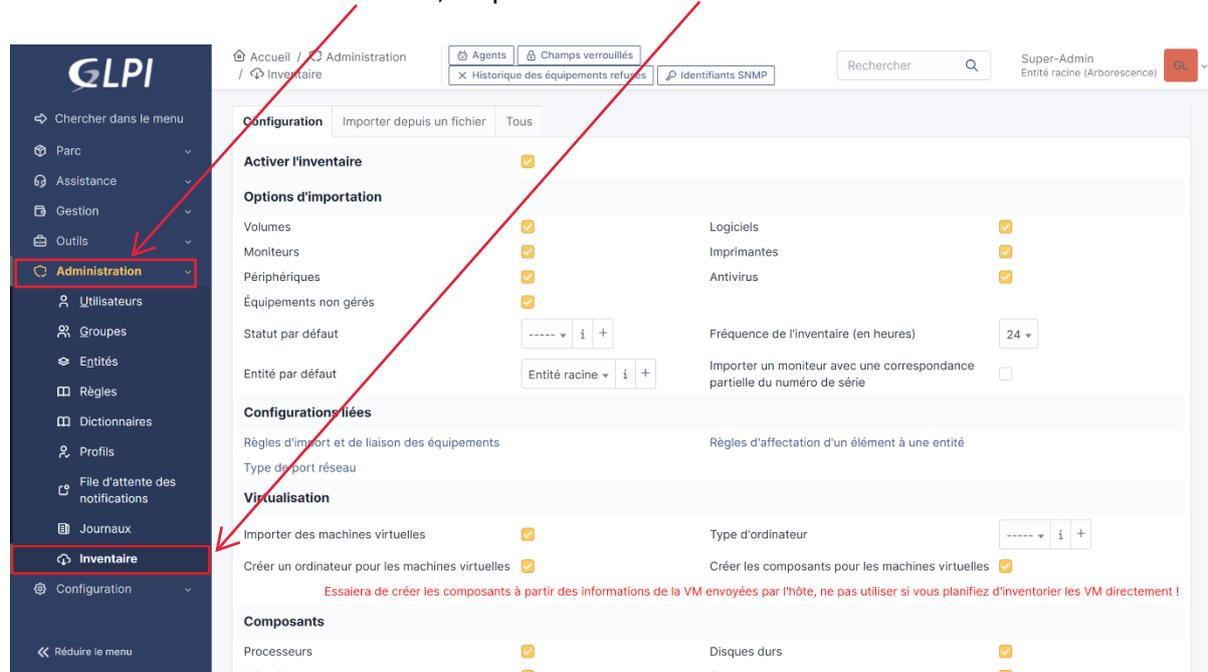
Etape 3 : Partagez le dossier en autorisant, en lecture, les utilisateurs authentifiés



Si vous installez la dernière version de GLPI en date (à ce jour la version 10.0.6), il est à noter que le module natif « inventaire » n'est pas activé par défaut !

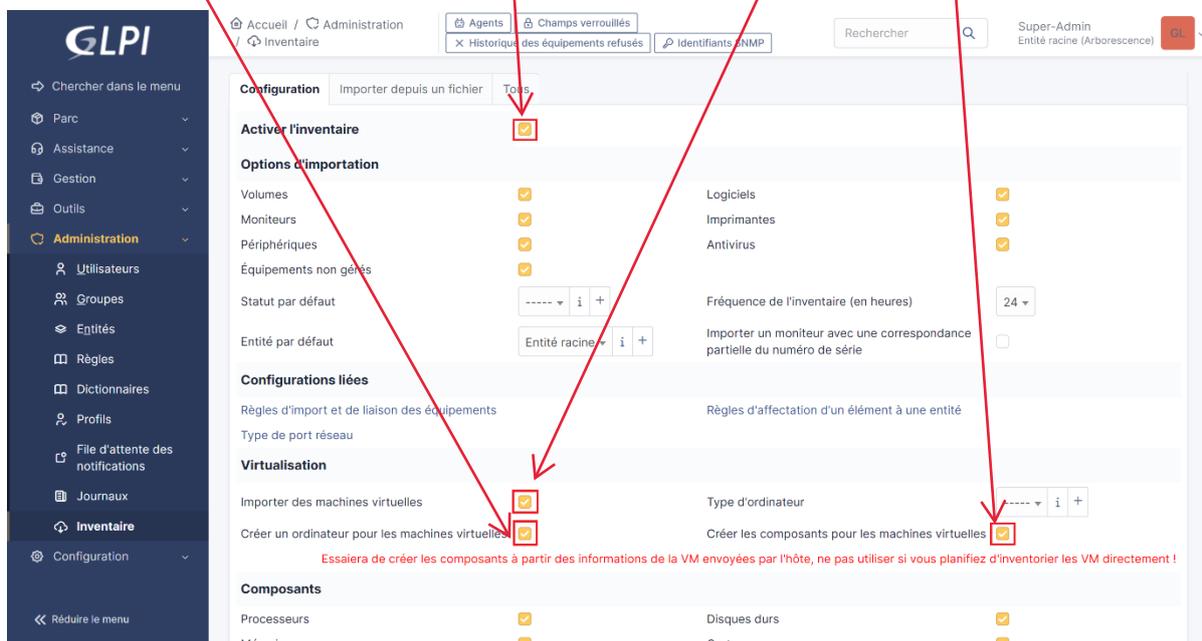
Si vous souhaitez déployer l'agent GLPI sur les postes de votre réseau et faire en sorte que la remontée d'inventaire se réalise, il faut obligatoirement activer l'inventaire !

Etape 4 : Connectez-vous à l'interface GLPI en tant qu'administrateur de la base interne. Dans le menu « Administration », cliquez sur « inventaire »



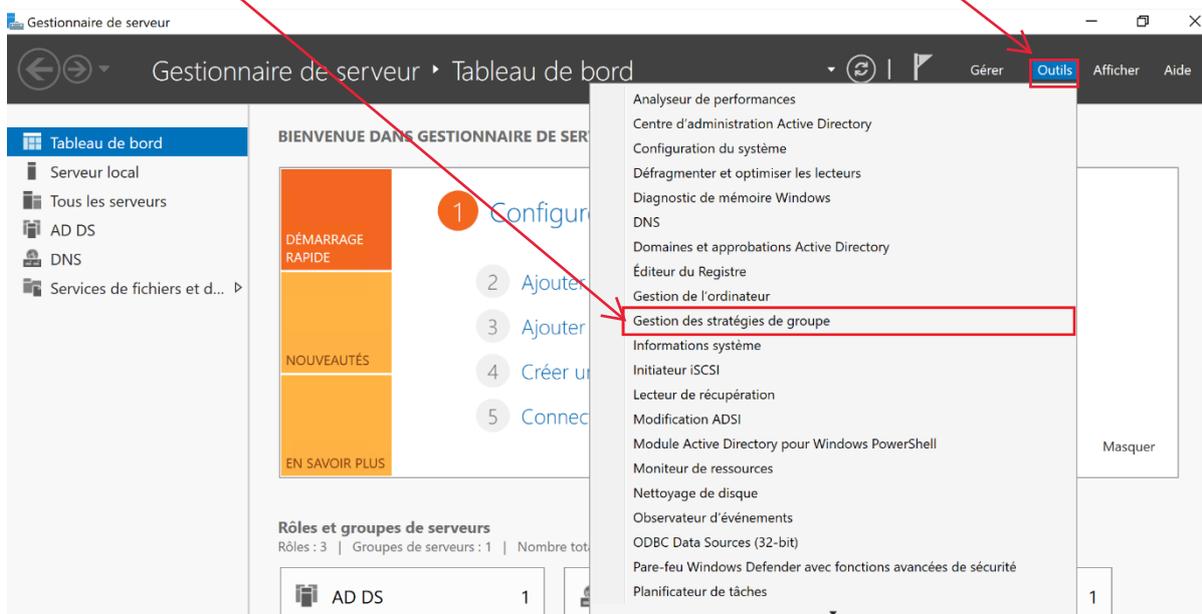
DEPLOYER L'AGENT GLPI AVEC UNE GPO

Etape 5 : Cochez les cases « Activer l'inventaire », « importer des machines virtuelles », « Créer un ordinateur pour les machines virtuelles » et « Créer les composants pour les machines virtuelles », puis sauvegarder.



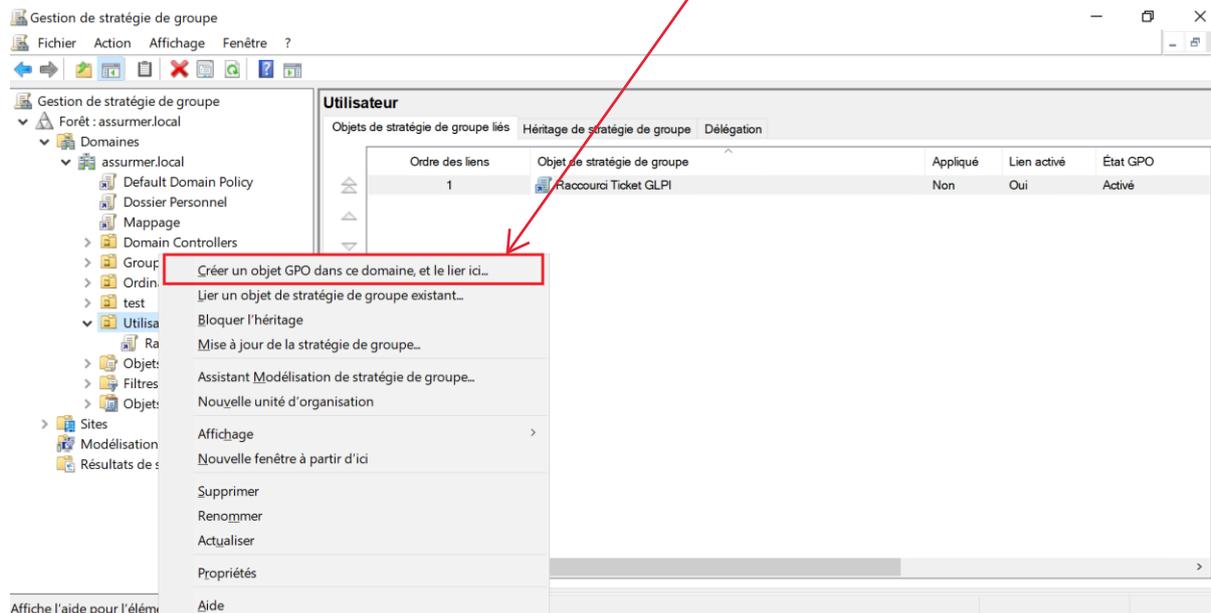
III. Création d'une GPO pour le déploiement de GLPI Agent

Etape 1 : Ouvrez le gestionnaire de serveur et cliquez le menu « Outils » et « Gestion des stratégies de groupe »



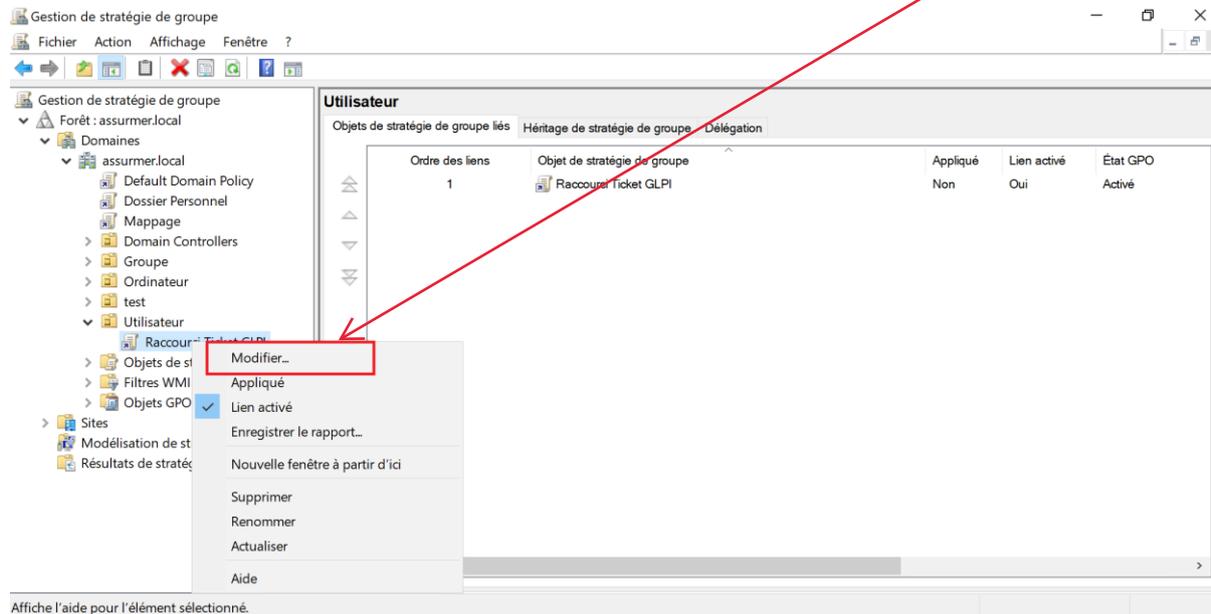
DEPLOYER L'AGENT GLPI AVEC UNE GPO

Etape 2 : Faites un clic droit sur l'unité d'organisation sur laquelle vous souhaitez déployer l'agent (ici « Utilisateurs ») et cliquez « Créer un objet GPO dans ce domaine et le lier ici... »

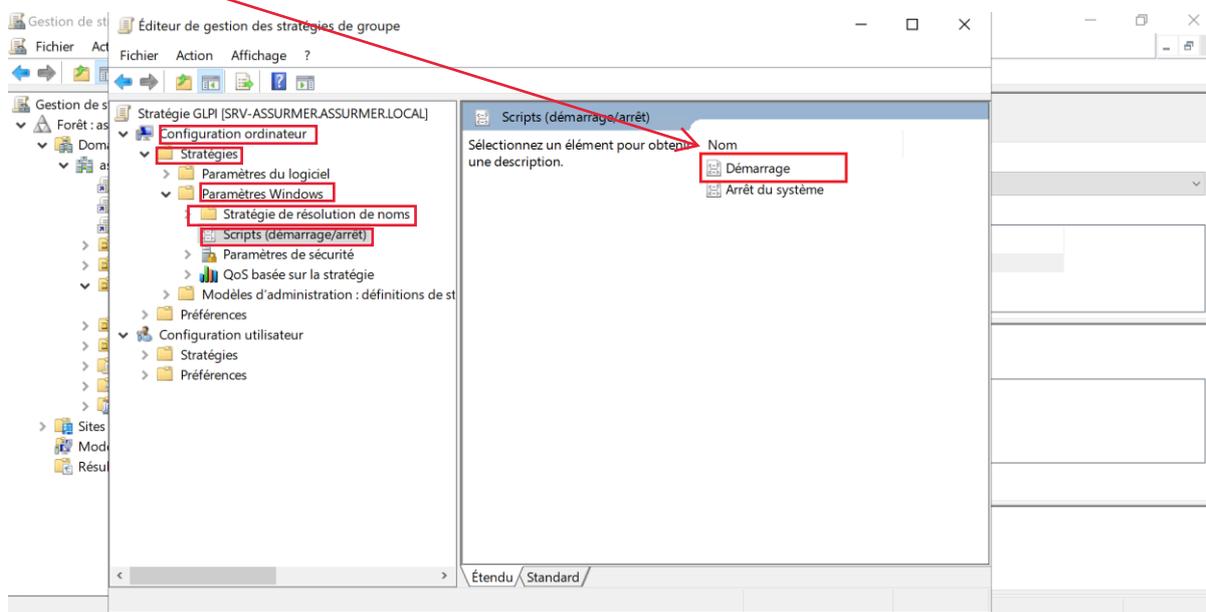


Donnez un nom à votre objet GPO et cliquez « Ok »

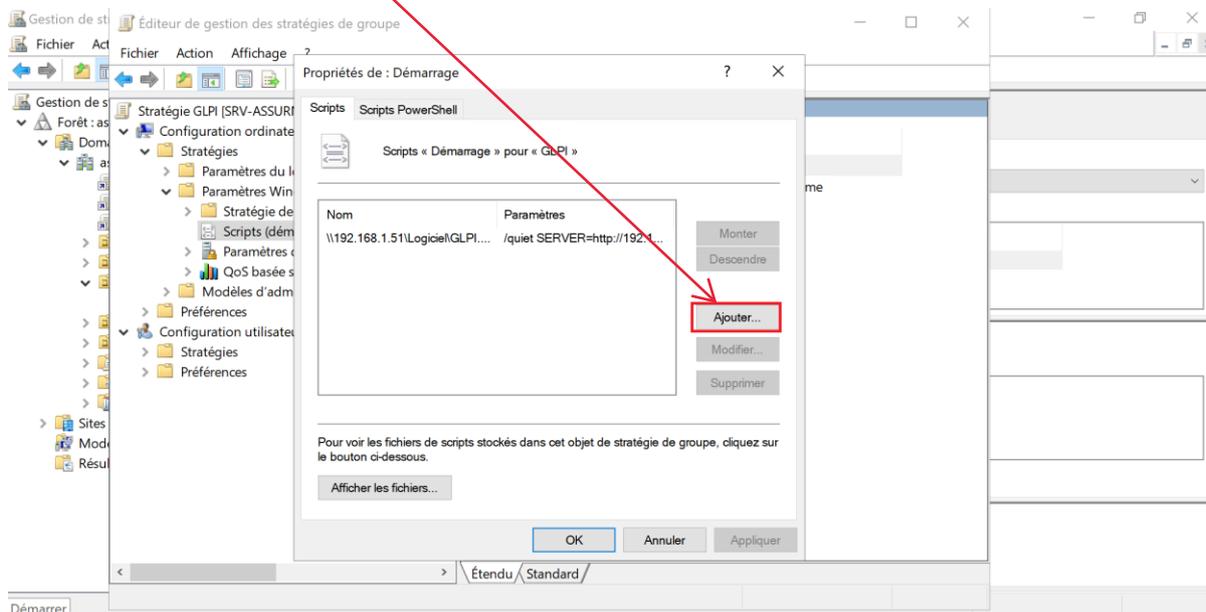
Etape 3 : Une fois l'objet GPO créé, faites un clic droit dessus et cliquez « Modifier »



Etape 4 : Déployez, dans la partie « Configuration ordinateur », la catégorie « Stratégies » - « Paramètres Windows » - « Stratégie de résolution de noms » - « Scripts » et cliquez sur « Démarrage »

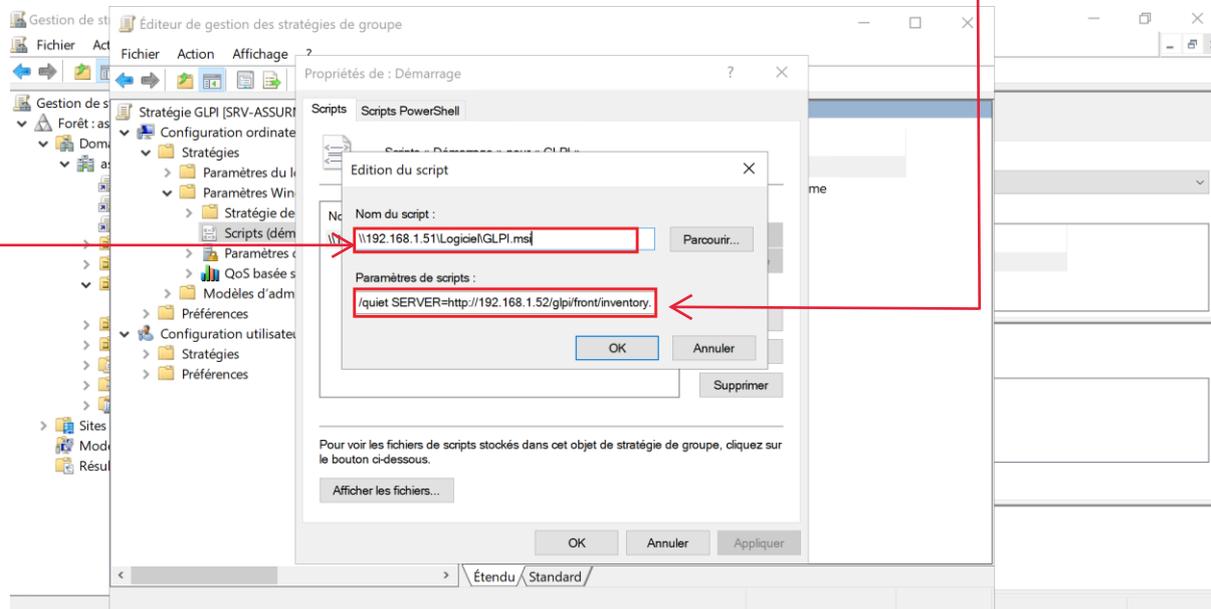


Etape 5 : Cliquez sur « Ajouter »



Etape 6 : Dans le nom du script, remplissez avec le chemin jusqu'au logiciel GLPI Agent (ici « \\AdresseIP du Serveur\LeDossierCréé\GLPI Agent.msi »)

Dans les paramètres de scripts, remplissez avec cette commande sans oublier de modifier le chemin vers GLPI « /quiet SERVER=http://192.168.1.52/gpi/front/inventory.php »



Lancez une machine cliente du domaine et authentifiez-vous en tant qu'utilisateur de la « OU » sur laquelle la stratégie doit s'appliquer.

L'ordinateur s'ajoutera automatiquement dans l'inventaire au bout de quelques minutes. L'inventaire GLPI est maintenant installé et configuré.