

# DOC TECHNIQUE GLPI

## [I. Informations nécessaires](#)

### [II. Installation sous Debian 12](#)

- [A. Prérequis pour l'installation](#)
- [B. Création de la base de donnée MySQL](#)
- [C. Téléchargement de GLPI](#)
- [D. Connexion à l'interface GLPI](#)

### [III. Sécurisation HTTP/HTTPS](#)

### [IV. Paramétrage des notifications par mail](#)

- [A. Mise en place des suivis par mail](#)
- [B. Exemple](#)
- [C. Liaison LDAP](#)
- [D. Tester la connexion Active Directory](#)

### [V. Inventaire Automatique](#)

#### [Inventaire sous Windows](#)

#### [Inventaire sous Linux](#)

### [VI. Création des gabarits de tickets](#)

- [A. Champs obligatoires :](#)
- [B. Champs masqués:](#)

## [I. Informations nécessaires](#)

Adresse IP du serveur : 172.16.12.110/24

Passerelle : 172.16.12.250

Ma base de données ne se trouve pas sur le srv-glpi mais est déportée vers un autre serveur qui est (srv-BDD). Son adresse IP est : 172.16.12.200

Adresse mail de l'administrateur : glpi@tom.local

## [II. Installation sous Debian 12](#)

### [A. Prérequis pour l'installation](#)

**Pour information, toutes les commandes ont été tapées avec l'utilisateur root donc pas besoin de faire de sudo devant la commande !**

Pour commencer, nous allons ouvrir le logiciel PuTTY et nous connecter en SSH sur la machine, puis, avant d'installer le paquet, nous allons voir si la machine est à jour, puis les faire si besoin.

```
sudo apt update  
sudo apt upgrade -y
```

Nous allons installer MariaDB et MySQL pour stocker notre base de données (pendant l'installation, il faudra répondre aux questions que va vous poser MariaDB pour son installation).

```
sudo apt install mariadb-server mysql_secure_installation
```

Ensuite, nous allons installer les extensions PHP nécessaires pour le fonctionnement de GLPI.

```
sudo apt install php8.2-curl php8.2-gd php8.2-mbstring php8.2-zip php8.2-xm  
php8.2-intl php8.2-mysql php8.2-dom php8.2-simplexml php json php8.2-ph  
php8.2-bz2
```

## **B. Création de la base de donnée MySQL**

Pour se connecter à la base de données, nous allons taper la commande suivante et entrer le mot de passe root de la base de données :

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

Puis, nous allons créer notre base de données avec la commande suivante :

```
CREATE DATABASE db23_glpi ;
```

Nous allons lui créer un utilisateur local et un mot de passe :

```
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'admin' ;
```

Ensuite, nous allons à attribuer des droits d'accès à l'utilisateur glpiuser sur la base de données db23\_glpi.

```
GRANT ALL PRIVILEGES ON db23_glpi* TO 'glpiuser'@'localhost' ;
```

Pour finir, on va recharger les privilèges, sans redémarrer la base de données avec la commande, puis on quitte MariaDB.

```
FLUSH PRIVILEGES ;  
quit;
```

## C. Téléchargement de GLPI

Nous allons télécharger l'outil GLPI, pour cela, il faut se rendre sur le site de Git Hub, copier le lien de téléchargement pour ensuite le coller à la suite de cette commande :

```
sudo wget https://github.com/glpi-project/glpi/releases/download/10.0.16/glpi
```

Ensuite, nous allons décompresser l'archive de GLPI grâce à la commande "tar" :

```
sudo tar -xvf glpi-10.0.16.tgz glpi/
```

Nous allons déplacer le dossier qui s'appelle "glpi" pour le mettre dans le bon dossier :

```
sudo mv glpi /var/www/html
```

Puis nous allons changer le propriétaire et le groupe du répertoire /var/www/html/glpi :

```
sudo chown -R www-data:www-data /var/www/html/glpi
```

Nous allons changer les permissions du dossier grâce à la commande :

```
sudo chmod -R 755 /var/www/html/glpi
```

Puis, pour finir, nous allons redémarrer Apache2 :

```
sudo systemctl reload apache2.service
```

## D. Connexion à l'interface GLPI

Une fois que vous avez bien suivi la procédure ci-dessous, vous devriez pouvoir accéder à l'interface web de GLPI en tapant dans la barre d'adresse : <http://adresseipdelamachine/glpi>. Moi, j'ai directement modifié cela en ajoutant à mon DNS l'adresse IP de la machine GLPI, donc ça me donne " <http://glpi.tom.local> " et vous devriez avoir cette interface :



Nous allons choisir la langue que l'on souhaite, puis, on installe GLPI :



Si vous aviez bien téléchargé tous les paquets PHP, il ne devrait pas y avoir d'erreur à part des avertissements. Sinon, c'est qu'il vous manque des extensions PHP.

## Étape 0

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

TESTS EFFECTUÉS	RÉSULTATS
<b>Requis</b> Parser PHP	✓
<b>Requis</b> Configuration des sessions	✓
<b>Requis</b> Mémoire allouée	✓
<b>Requis</b> mysqli extension	✓
<b>Requis</b> Extensions du noyau de PHP	✓
<b>Requis</b> curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
<b>Requis</b> gd extension <i>Requis pour le traitement des images.</i>	✓
<b>Requis</b> intl extension <i>Requis pour l'internationalisation.</i>	✓
<b>Requis</b> zlib extension <i>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</i>	✓
<b>Requis</b> Libsodium ChaCha20-Poly1305 constante de taille <i>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</i>	✓
<b>Requis</b> Permissions pour les fichiers de log	✓
<b>Requis</b> Permissions pour les dossiers de données	✓
<b>Sécurité</b> Version de PHP maintenue <i>Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.</i>	✓
<b>Sécurité</b> Configuration sécurisée du dossier racine du serveur web <i>La configuration du dossier racine du serveur web devrait être "/var/www/html/glpi/public" pour s'assurer que les fichiers non publics ne peuvent être accessibles. La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.</i>	⚠
<b>Sécurité</b> Emplacement sécurisé pour les dossiers de données <i>Les dossiers de données de GLPI devraient être placés en dehors du dossier racine web. Ceci peut être effectué en redéfinissant les constantes correspondantes. Référez-vous à la documentation d'installation pour plus de détails. Les dossiers suivants devraient être placés en dehors de "/var/www/html/glpi": - "/var/www/html/glpi/files" ("GLPI_VAR_DIR") Vous pouvez ignorer cette suggestion si le dossier racine de votre serveur web est "/var/www/html/glpi/public".</i>	⚠
<b>Sécurité</b> Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée. La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.</i>	⚠
<b>Suggéré</b> Taille d'entier maximal de PHP <i>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau).</i>	✓

<p><b>Sécurité</b> <b>Emplacement sécurisé pour les dossiers de données</b> <span style="float: right;">▲</span></p> <p>Les dossiers de données de GLPI devraient être placés en dehors du dossier racine web. Ceci peut être effectué en redéfinissant les constantes correspondantes. Référez-vous à la documentation d'installation pour plus de détails.</p> <p>Les dossiers suivants devraient être placés en dehors de "/var/www/html/glpi":</p> <ul style="list-style-type: none"> <li>- "/var/www/html/glpi/files" ("GLPL_VAR_DIR")</li> </ul> <p>Vous pouvez ignorer cette suggestion si le dossier racine de votre serveur web est "/var/www/html/glpi/public".</p>	
<p><b>Sécurité</b> <b>Configuration de sécurité pour les sessions</b> <span style="float: right;">▲</span></p> <p>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée.</p> <p>La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.</p>	
<p><b>Suggéré</b> <b>Taille d'entier maximal de PHP</b> <span style="float: right;">✓</span></p> <p>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).</p>	
<p><b>Suggéré</b> <b>exif extension</b> <span style="float: right;">✓</span></p> <p>Renforcer la sécurité de la validation des images.</p>	
<p><b>Suggéré</b> <b>ldap extension</b> <span style="float: right;">✓</span></p> <p>Active l'utilisation de l'authentification à un serveur LDAP distant.</p>	
<p><b>Suggéré</b> <b>openssl extension</b> <span style="float: right;">✓</span></p> <p>Active l'envoi de courriel en utilisant SSL/TLS.</p>	
<p><b>Suggéré</b> <b>Extensions PHP pour le marketplace</b> <span style="float: right;">✓</span></p> <p>Permet le support des formats de paquets les plus communs dans le marketplace.</p>	
<p><b>Suggéré</b> <b>Zend OPcache extension</b> <span style="float: right;">✓</span></p> <p>Améliorer les performances du moteur PHP.</p>	
<p><b>Suggéré</b> <b>Extensions émulées de PHP</b> <span style="float: right;">✓</span></p> <p>Améliorer légèrement les performances.</p>	
<p><b>Suggéré</b> <b>Permissions pour le répertoire du marketplace</b> <span style="float: right;">✓</span></p> <p>Active l'installation des plugins à partir du Marketplace.</p>	

**Voulez-vous continuer ?**

Continuer >
Réessayer ↺

Pour se connecter à la base de données, il suffit de reprendre les informations que l'on a renseignées dans MariaDB un peu plus haut, et ça donne :

- Serveur SQL : IP de votre serveur GLPI (nous = 172.16.12.110)
- Utilisateur SQL : glpiuser
- Mot de passe SQL : admin

**GLPI** **GLPI SETUP**

Étape 1

Configuration de la connexion à la base de données

Serveur SQL (MariaDB ou MySQL)

Utilisateur SQL

Mot de passe SQL

Continuer >

Après avoir cliqué sur "Continuer", nous devons choisir la base de données "db23\_glpi" créée précédemment :

**GLPI** **GLPI SETUP**

Étape 2

Test de connexion à la base de données

✓ Connexion à la base de données réussie

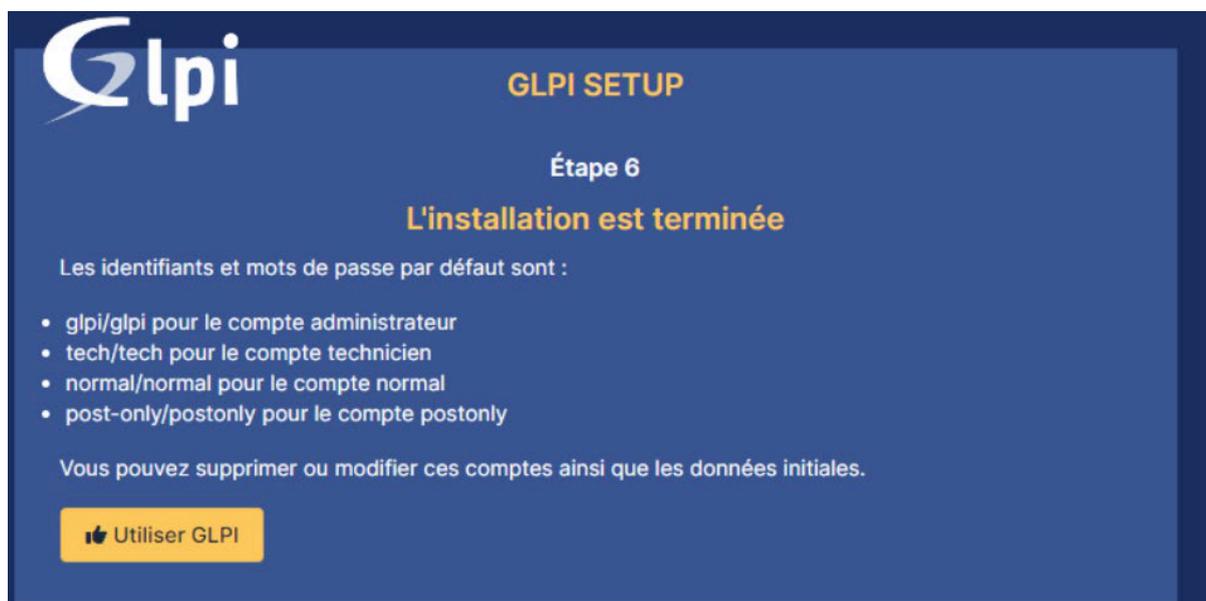
Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

db23\_glpi

Continuer >

Ensuite, vous suivez les dernières étapes, puis vous devriez atterrir sur une page avec des noms d'utilisateurs et des mots de passe :



Nous allons enfin accéder à l'interface de GLPI, pour cela, vous devez vous connecter avec le compte administrateur qui est glpi et son mot de passe qui est aussi glpi. Il faudra impérativement changer le mot de passe administrateur et en mettre un plus robuste. Vous devrez aussi désinstaller le fichier de configuration "install.php" pour des raisons de sécurité. S'il n'est pas désinstallé, il se peut qu'il relance une installation de GLPI...



### Connexion à votre compte

Identifiant

Mot de passe

Source de connexion

Se souvenir de moi

Se connecter

GLPI Copyright (C) 2015-2024 Teclib' and contributors

Accueil

Rechercher

Super-Admin  
Entrée racine (Arborescence)

Tableau de bord

Vue personnelle | Vue groupe | Vue globale | Flux RSS | Tous

Central

Logiciel 0

Ordinateur 0

Matériel réseau 0

Téléphone 0

Licence 0

Moniteur 0

Base 0

Imprimante 0

Statuts des tickets par mois

Ticket 0

Tickets en retard 0

Problème 0

Changement 0

4 Utilisateurs

0 Groupe

0 Fournisseur

0 Document

## III. Sécurisation HTTP/HTTPS

Nous avons mis en place une autorité de certification en interne avec Windows Server et son serveur IIS et AD CS, afin de sécuriser notre serveur GLPI. Nous

souhaitions que lorsque nous entrerons son nom d'url sur internet, le serveur GLPI soit en <https://glpi.tom.local> (nom de domaine chez nous).

Pour cela, nous avons créé un dossier où nous allons stocker les certificats de notre serveur GLPI :

```
sudo mkdir /etc/ssl/glpi.tom.local
```

nous allons générer une clé de chiffrement pour créer, par la suite, notre certificat :

```
cd /etc/ssl/glpi.comwork.blog  
openssl genrsa -out glpi.tom.local.key 2048
```

Ensuite, nous allons créer un fichier sur lequel, nous allons nous baser pour créer le certificat :

```
cd /etc/ssl/glpi.tom.local  
vim fic.txt  
  
# à L'intérieur de ce fichier #  
  
[ req ]  
default_bits = 2048  
distinguished_name = dn  
prompt = no  
default_md = sha256  
req_extensions = req_ext  
  
[ dn ]  
C=FR  
L=Angers  
O=Study  
CN=glpi.tom.local  
  
[ req_ext ]  
subjectAltName = @alt_names
```

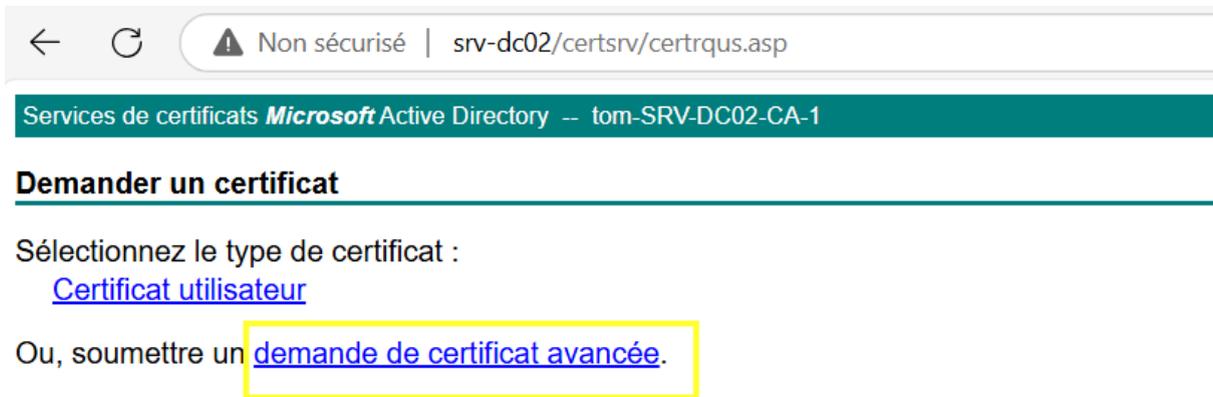
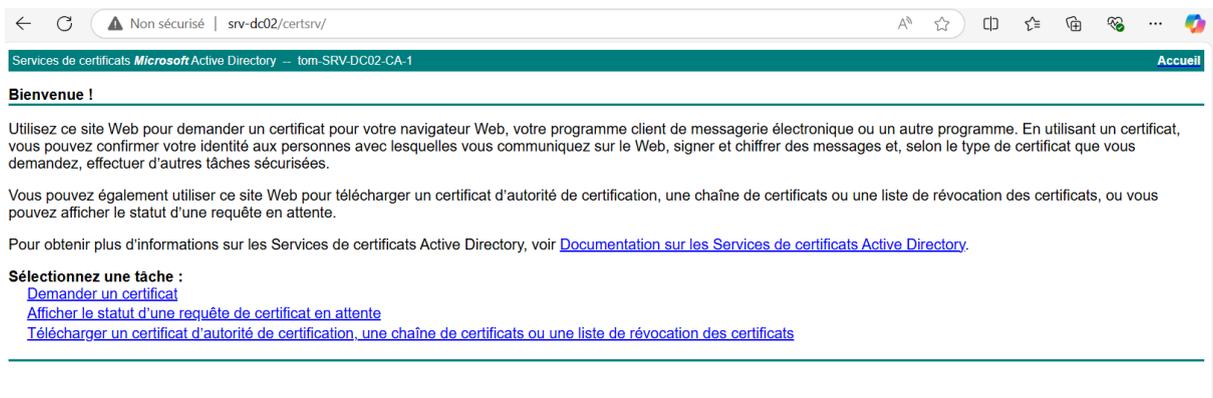
```
[ alt_names ]
```

```
DNS.1 = glpi.tom.local
```

Puis, nous allons créer notre nouvelle clé de certificat pour notre serveur GLPI :

```
openssl req -new -key glpi.tom.local.key -out glpi.tom.local.pem -config fic.tx
```

Maintenant, nous allons copier ce qu'il y a dans notre fichier "glpi.tom.local.pem" grâce à la commande cat, puis le coller dans notre autorité de certifications de Windows Server pour qu'elle me génère le certificat :



On colle notre certificat :

Non sécurisé | srv-dc02/certsrv/certrqxt.asp

Services de certificats **Microsoft** Active Directory -- tom-SRV-DC02-CA-1 Accueil

### Soumettre une demande de certificat ou de renouvellement

Afin de soumettre une demande enregistrée à l'autorité de certification, collez une demande de certificat CMC ou PKCS #10 codé en base 64 ou une demande de renouvellement PKCS #7 générée par une source externe (telle qu'un serveur Web) dans la zone Demande enregistrée.

**Demande enregistrée :**

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1jCCAXICAQAwGTEXMBUGA1UEAwQ2ZxwaS50b20ubG9jYmwwggEj
S1b3DQEBQUAAIIBDwAggEKAOIIBAQCuiZ+CO2+JD11TDUc8BghH9k
L4cm5sv7Yn2Y9ABUpR0HzL/ME6o7yr/UB1aZHSOXbQgk5Khb3WkL1p
kpCpAFDsy7XNtdL3hcxmrxm514mCez7u4ryhxA4A181PKCb6dFRU+HNk
z6A2rDLNkozZ5UTzgm2mbY0ud2BazZdsLqTEVRPNkqCORBm3pVnsNDc
ayQJcNMc4er/HBgupYyZx84DnJ9Arr66vazfsRn1EdDsznya7VesI4z
EK+qr/yBaBmiSkO6AEFDB81ax72M154H24T1871HXi0VCRxvmYVRAgME
BgkqhkiG9w0BQCQ4xHTAbMBkGA1UdEQSMBCCDmDscGkudG9TLmxxvY2Fs
S1b3DQEBQUAAIIBAQcPBHs4rKx0FoCmgT9XwME1q1pTk0463dIKDBB
tal+Xsg++03hYThfQ5zXYPmRudrb6nYh6KBHswQY+pQTbt8ebMq1vQ3F
++q37/th/evaYVdASBk7nTufGvNkcnARBmBFRSf7BDCGlex7mM?T9aKca
-----
```

Base-64-encoded  
Requête de certificat  
(CMC ou  
PKCS #10 ou  
PKCS #7):

Modèle de certificat :

Attributs supplémentaires :

Attributs :

Non sécurisé | srv-dc02/certsrv/certfnsh.asp

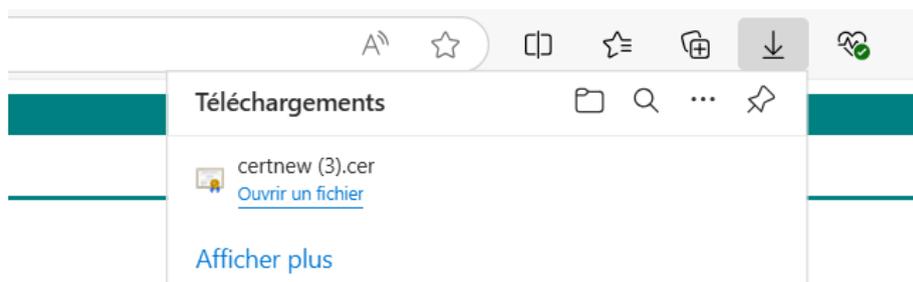
Services de certificats **Microsoft** Active Directory -- tom-SRV-DC02-CA-1

## Certificat émis

Le certificat que vous avez demandé a été émis.

Codé DER ou  Codé en base 64

 [Télécharger le certificat](#)  
[Télécharger la chaîne de certificats](#)



Ensuite, on le renomme, puis nous allons transférer ce certificat à notre serveur GLPI :

```
scp C:\Users\Administrateur\Downloads\glpi.tom.local tom@adresseserveur:
```

Une fois le transfert effectué, vous devriez le retrouver dans le dossier "tmp" :

```
cd /tmp  
ls
```

Nous allons le déplacer dans notre dossier de certificats de notre serveur GLPI :

```
cp glpi.tom.local.cer /etc/ssl/glpi.tom.local/
```

Pour finir, nous allons modifier le fichier de configuration de GLPI dans Apache 2 pour qu'il prenne en compte le certificat :

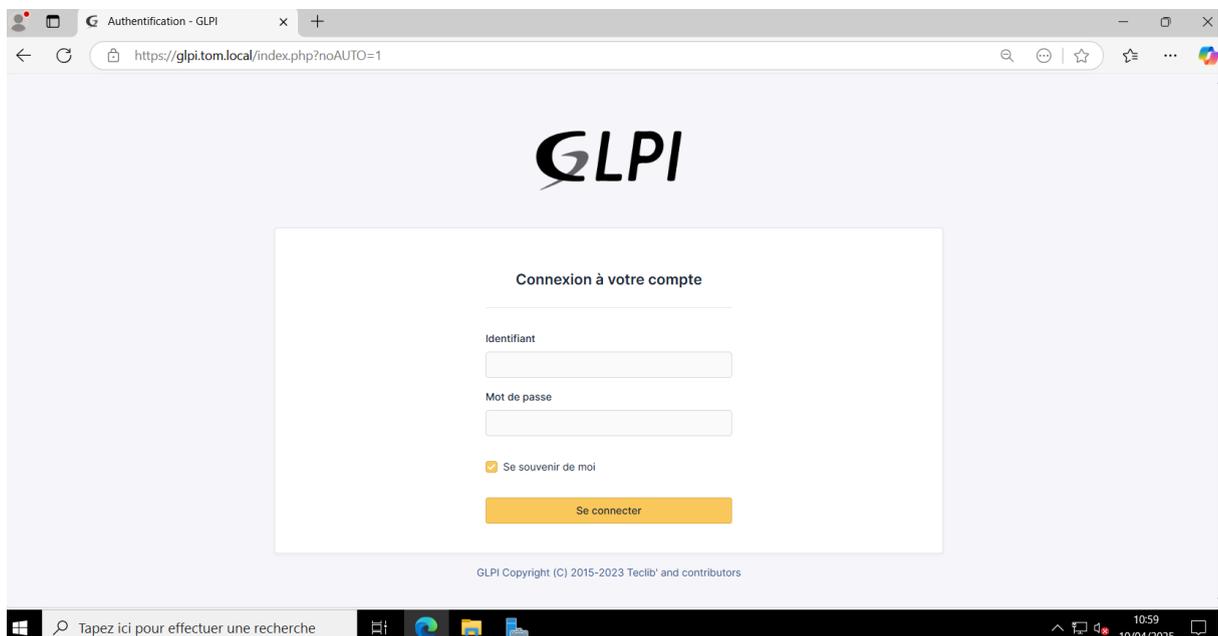
```
vim /etc/apache2/sites-available/glpi.tom.local  
  
# Le fichier devrait ressembler à cela #  
  
<Virtualhost *:443>  
  
    ServerName glpi.tom.local  
    ServerAdmin webmaster@localhost  
    DocumentRoot /var/www/html/glpi  
  
    <Directory "/var/www/html/glpi">  
        Options FollowSymLinks  
        AllowOverride None  
        Require all granted  
    </Directory>  
  
    SSLEngine On  
    SSLCertificateFile /etc/ssl/glpi.tom.local/glpi.tom.local.cer  
    SSLCertificateKeyFile /etc/ssl/glpi.tom.local/glpi.tom.local.key  
    SSLProtocol all -SSLv3  
  
    ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Ensuite, nous allons dépublier le site <http://glpi.tom.local>, puis le republier :

```
a2dissite glpi.tom.local
a2ensite glpi.tom.local
a2enmod ssl

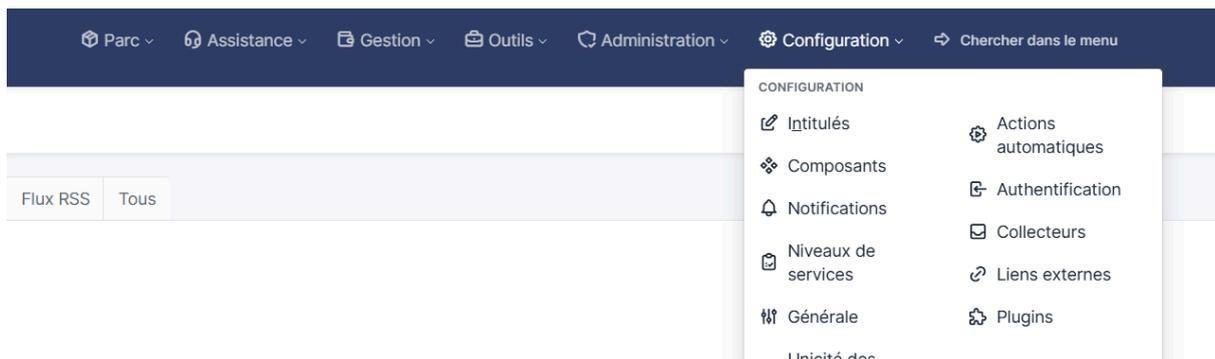
systemctl reload apache2.service
```



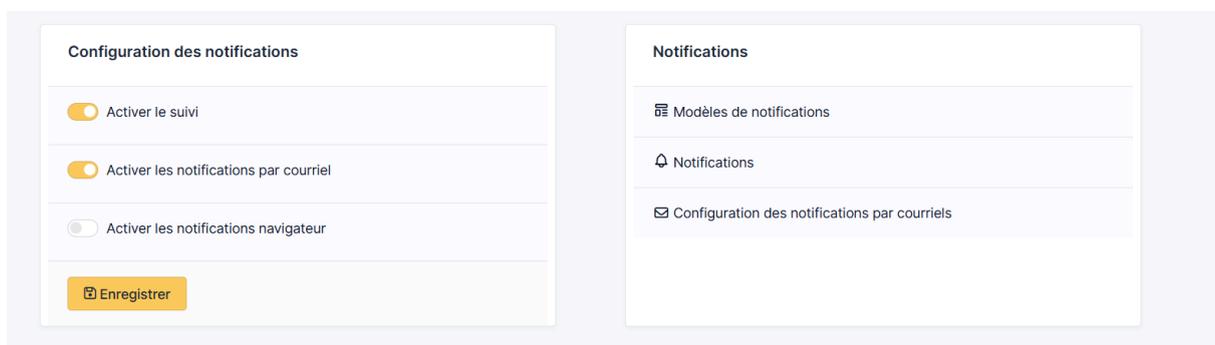
## IV. Paramétrage des notifications par mail

### A. Mise en place des suivis par mail

Après chaque nouveau ticket qui sera créé, nous souhaitons avoir un retour par mail de l'ouverture, clôture, résolution d'un nouveau ticket. Pour cela, nous allons nous rendre dans l'onglet Configuration > Notifications :



Vous devrez "activer le suivi des notifications" ainsi que les " notifications par courriel".



Vous irez dans la « Configuration des notifications par courriels » et vous rentrerez vos informations suivantes :

- ⇒ Courriel de l'administrateur
- ⇒ Nom de l'administrateur
- ⇒ Courriel de l'expéditeur
- ⇒ Nom de l'expéditeur du message
- ⇒ Signature du courriel → si vous souhaitez ajouter un message en fin de mail, c'est ici qu'il faudra le faire.
- ⇒ Ainsi que le mode d'envoi des courriels

**Notifications courriel**

Courriel de l'administrateur	<input type="text"/>	Nom de l'administrateur	<input type="text"/>
Courriel de l'expéditeur <small>i</small>	<input type="text"/>	Nom de l'expéditeur du message <small>i</small>	<input type="text"/>
Adresse de réponse <small>i</small>	<input type="text"/>	Nom de réponse <small>i</small>	<input type="text"/>
Adresse de non réponse <small>i</small>	<input type="text"/>	Nom de non réponse <small>i</small>	<input type="text"/>
Ajouter des documents dans les notifications de ticket	Non <small>v</small>		
Signature des courriels	<input type="text"/>		
Mode d'envoi des courriels	SMTP+SSL <small>v</small>	Tentatives d'envoi max.	5 <small>v</small>
Tenter d'envoyer de nouveau dans (minutes)	3 <small>v</small>		

Le service informatique reviendra vers vous dans les plus brefs délais. Merci de votre compréhension.

Suivant le mode d'envoi que vous aurez choisi, il faudra configurer le serveur de messagerie avec vos informations du serveur de messagerie.

The screenshot shows the 'Serveur de messagerie' configuration form. It includes the following fields:

- Vérifier le certificat:** A dropdown menu set to 'Non'.
- Hôte SMTP:** A text input field.
- Port:** A dropdown menu set to '465'.
- Identifiant SMTP (optionnel):** A text input field.
- Mot de passe SMTP (optionnel):** A password input field.
- Expéditeur du message:** A text input field.
- Effacer:** A checkbox.

Enfin, pour vérifier que vos informations sont correctes. Vous pouvez " Envoyer un courriel de test à l'administrateur", puis vous sauvegarder et quitter.

The screenshot shows the GLPI configuration page for email notifications. The browser address bar is <https://glpi.tom.local/front/notificationmailingsetting.form.php>. The page title is 'Notifications courriel'. The form includes the following sections:

- Notifications courriel:**
  - Courriel de l'administrateur:** glpi@tom.local
  - Nom de l'administrateur:** Admin
  - Courriel de l'expéditeur:** [Empty field]
  - Nom de l'expéditeur du message:** [Empty field]
  - Adresse de réponse:** [Empty field]
  - Nom de réponse:** [Empty field]
  - Adresse de non réponse:** [Empty field]
  - Nom de non réponse:** [Empty field]
  - Ajouter des documents dans les notifications de ticket:** Non
  - Signature des courriels:** Madame, Monsieur, Le service informatique vient de recevoir votre demande, nous allons la traiter dans les plus brefs délais. Merci à vous !
  - Mode d'envoi des courriels:** SMTP+SSL
  - Tentatives d'envoi max.:** 5
  - Temps d'envoyer de nouveau dans (minutes):** 5
- Serveur de messagerie:**
  - Vérifier le certificat:** Non
  - Hôte SMTP:** mail.tom.local
  - Port:** 465
  - Identifiant SMTP (optionnel):** glpi@tom.local
  - Mot de passe SMTP (optionnel):** [Empty field]
  - Expéditeur du message:** [Empty field]
  - Effacer:** [Empty checkbox]

Ensuite dans l'onglet Configuration > Notifications > Notifications, vous pourrez choisir les notifications qui seront envoyées par mail. Pas la peine, de toutes les activées. Activez juste celle qui vous paraissent le plus importantes pour vous.

Accueil / Configuration / Notifications / Notifications

+ Ajouter Rechercher Listes

Rechercher

Éléments visualisés - contient -

régle règle globale (1) groupe Rechercher

Actions

NOM	ACTIF	TYPE	ÉVÈNEMENTS	MODÈLES DE NOTIFICATIONS	ENTITÉ	SOUS-ENTITÉS	MODE DE NOTIFICATION	COMMENTAIRES
Add Followup	Oui	Ticket	Nouveau suivi	Tickets	Entité racine	Oui	Courriel	
Add Task	Non	Ticket	Nouvelle tâche	Tickets	Entité racine	Oui	Courriel	
Add Task	Non	Problème	Nouvelle tâche	Problems	Entité racine	Oui	Courriel	
Add Task	Non	Changement	Nouvelle tâche	Changes	Entité racine	Oui	Courriel	
Alert domains close expiries	Non	Domaine	Domaines en cours d'expiration	Alert domains	Entité racine	Oui	Courriel	
Alert expired domains	Non	Domaine	Domaines expirés	Alert domains	Entité racine	Oui	Courriel	
Alert Reservation	Non	Réservation	Expiration d'une réservation	Alert Reservation	Entité racine	Oui	Courriel	
Alert Tickets not closed	Non	Ticket	Tickets non résolus	Alert Tickets not closed	Entité racine	Oui	Courriel	
Cartridges	Non	Modèle de cartouche	Alerte cartouches	Cartridges	Entité racine	Oui	Courriel	
Certificates	Non	Certificat	Alerte sur l'expiration d'un certificat	Certificates	Entité racine	Oui	Courriel	
Check plugin updates	Non	Marketplace	Vérifier les mises à jour de tous les plugins	Plugin updates	Entité racine	Oui	Courriel	
Close Change	Non	Changement	Clôture d'un changement	Changes	Entité racine	Oui	Courriel	
Close Problem	Non	Problème	Clôture d'un problème	Problems	Entité racine	Oui	Courriel	

50 lignes / page De 1 à 50 sur 73 lignes

## B. Exemple

Prenons l'exemple pour la notification « New Ticket ». Dans l'onglet New Ticket « Notifications » vous avez le nom de la notification ainsi que d'autres éléments :

⇒ Actif : Oui si vous voulez qu'elle soit active

⇒ Permettre d'y répondre : Oui si on veut pouvoir répondre depuis nos mails

⇒ Type : Ticket

⇒ Évènements : Nouveau Ticket

Notification

Gabarits 1 Nom New Ticket

Destinataires 4 Actif Oui

Historique 2 Permettre de répondre Oui

Tous Type Ticket

Évènements Nouveau ticket

Commentaires

Supprimer définitivement Sauvegarder

Dans « Destinataires », veuillez indiquer à qui sera envoyé le mail.

Vous faites la même chose pour les notifications que vous souhaitez activer.

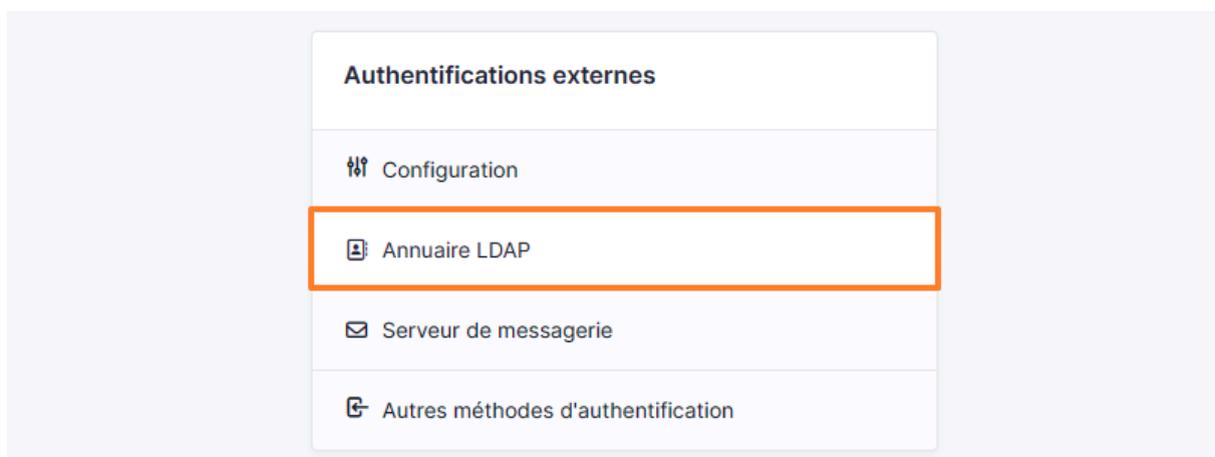
## C. Liaison LDAP

Désormais, nous allons ajouter notre annuaire Active Directory à GLPI.

Connectez-vous à GLPI avec le compte administrateur, puis dans le menu "**Configuration**", cliquez sur "**Authentification**".



Au centre de l'écran, cliquez sur "**Annuaire LDAP**".



Puis, cliquez sur le bouton "**Ajouter**".

----- Éléments visualisés ▼ contient ▼

règle (+) groupe Rechercher ☆

Aucun élément trouvé

Nous allons configurer notre liaison LDAP :

Nouvel élément - Annuaire LDAP

Préconfiguration Active Directory / OpenLDAP / Valeurs par défaut

Nom

Serveur par défaut Non ▼ Actif Non ▼

Serveur Port (par défaut 389) 389

Filtre de connexion

BaseDN

Utiliser bind i Oui ▼

DN du compte (pour les connexions non anonymes)

Mot de passe du compte (pour les connexions non anonymes)

Champ de l'identifiant uid Commentaires

Champ de synchronisation i

+ Ajouter

- **Nom** : le nom de cet annuaire LDAP, vous pouvez utiliser un nom convivial, ce n'est pas obligatoirement le nom du domaine, ni le nom du serveur.
- **Serveur par défaut** : Il ne peut y avoir qu'un seul serveur LDAP défini par défaut.
- **Actif** : nous allons indiquer "Oui"
- **Serveur** : adresse IP du contrôleur de domaine à interroger, pour nous (172.16.12.100)
- **Port** : 389, qui est le port par défaut du protocole LDAP.

- **Filtre de connexion** : requête LDAP pour rechercher les objets dans l'annuaire Active Directory.
- **BaseDN** : l'OU dans laquelle cette trouve les utilisateurs (OU=Tom\_Company,DC=tom,DC=local)
- **Utiliser bind** : à positionner sur "Oui" pour du LDAP classique (sans TLS)
- **DN du compte** : le nom du compte à utiliser pour se connecter à l'Active Directory.
- **Mot de passe du compte** : le mot de passe du compte renseigné ci-dessus
- **Champ de l'identifiant** : dans l'Active Directory, quel attribut doit être utilisé comme identifiant de connexion pour le futur compte GLPI ? Généralement, UserPrincipalName ou SamAccountName, selon vos besoins.
- **Champ de synchronisation** : GLPI a besoin d'un champ sur lequel s'appuyer pour synchroniser les objets. Ici, nous allons utiliser l'**objectGuid** de façon à avoir une valeur unique pour chaque utilisateur. Ainsi, si un utilisateur est modifié dans l'Active Directory, GLPI pourra se repérer grâce à cet attribut qui lui n'évoluera pas (sauf si le compte est supprimé puis recréé dans l'AD).

The screenshot shows the GLPI web interface for configuring an LDAP directory. The page title is 'Annuaire LDAP - tom.local'. The configuration fields are as follows:

Nom	tom.local	Dernière modification	2025-04-07 07:29
Tester			
Utilisateurs	Serveur par défaut	Oui	Actif
Groupes	Serveur	172.16.12.100	Port (par défaut 389)
Informations avancées			389
Réplicats	Filtre de connexion	(&(objectClass=user)(objectCategory=person)((userAccountControl:1.2.840.113556.1.4.803:=2))	
Historique	BaseDN	OU=TOM_Company,DC=tom,DC=local	
Tous	Utilisez un compte (pour les connexions non anonymes)	Oui	
	DN du compte (pour les connexions non anonymes)	CN=administrateur,CN=Users,DC=tom,DC=local	
	Mot de passe du compte (pour les connexions non anonymes)	<input type="text"/>	
	Champ de l'identifiant	userprincipalname	Commentaires
	Champ de synchronisation	objectguid	

Ci-dessus, la configuration utilisée pour mon infrastrucutre

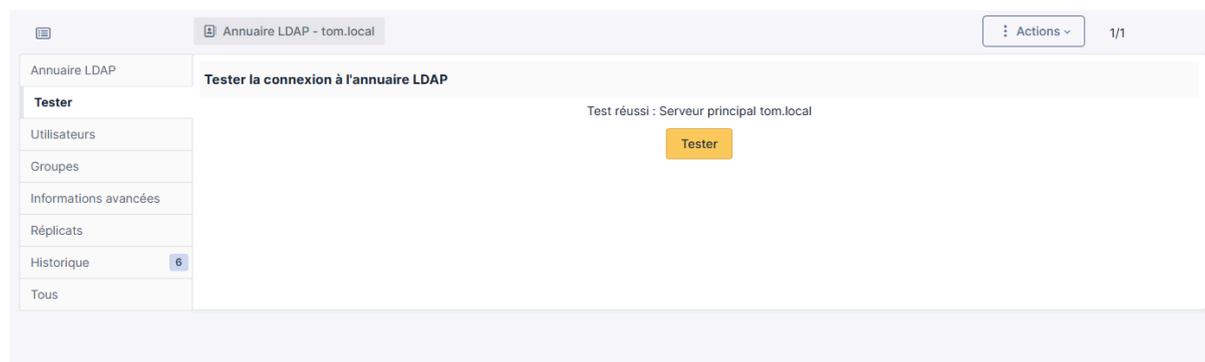
- **Nom** : tom.local
- **Serveur par défaut** : Oui
- **Actif** : Oui

- **Serveur** : 172.16.12.100
- **Port** : 389
- **Filtre de connexion** : (&(objectClass=user)(objectCategory=person)(!userAccountControl:1.2.840.113556.1.4.803:=2)))
- **BaseDN** : OU=TOM\_Company,DC=tom,DC=local
- **Utiliser bind** : Oui
- **DN du compte** : CN=administrateur,CN=Users,DC=tom,DC=local
- **Mot de passe du compte** : Mot de passe du compte "administrateur"
- **Champ de l'identifiant** : userprincipalname
- **Champ de synchronisation** : objectguid

Quand votre configuration est prête, cliquez sur "**Ajouter**".

Dans la foulée, **GLPI va effectuer un test de connexion LDAP et vous indiquer s'il est parvenu, ou non, à se connecter à votre annuaire.**

Si ce n'est pas le cas (comme moi, la première fois), cliquez sur le nom de votre annuaire, vérifiez la configuration, puis retournez dans "**Tester**" sur la gauche afin de lancer un nouveau test. Pour ma part, le problème venait du champ "Serveur" : j'avais mis le nom DNS du serveur à la place de l'adresse IP, mais cela ne fonctionnait pas. Pourtant, mon serveur GLPI parvient bien à résoudre le nom DNS.

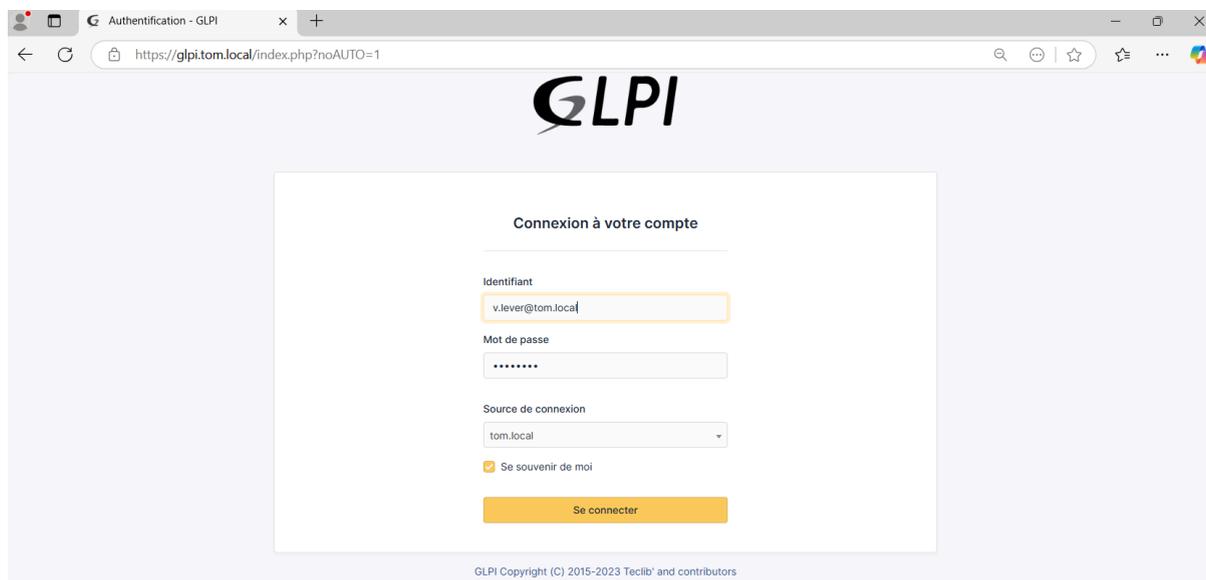


## D. Tester la connexion Active Directory

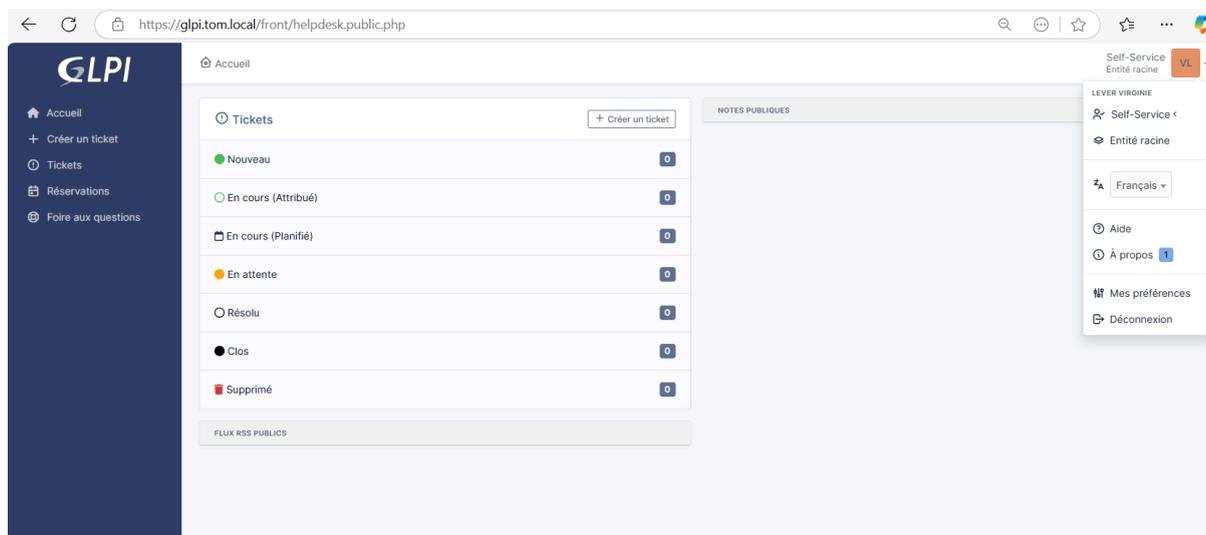
Si GLPI valide la connexion à votre annuaire Active Directory, vous pouvez tenter de vous authentifier à l'application avec un compte utilisateur. Pour ma part, c'est l'utilisateur Guy Mauve qui va servir de cobaye. Son login GLPI sera donc "

**v.lever@tom.local**". Pour le mot de passe, je dois indiquer celui de son compte Active Directory.

**Remarque** : la source d'authentification doit être l'Active Directory.



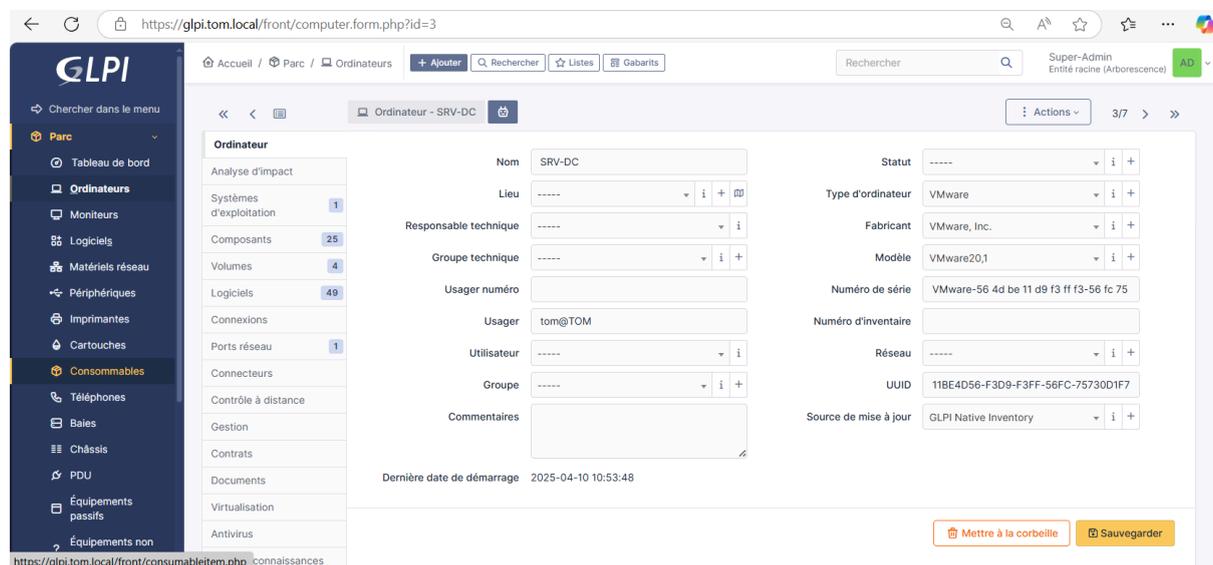
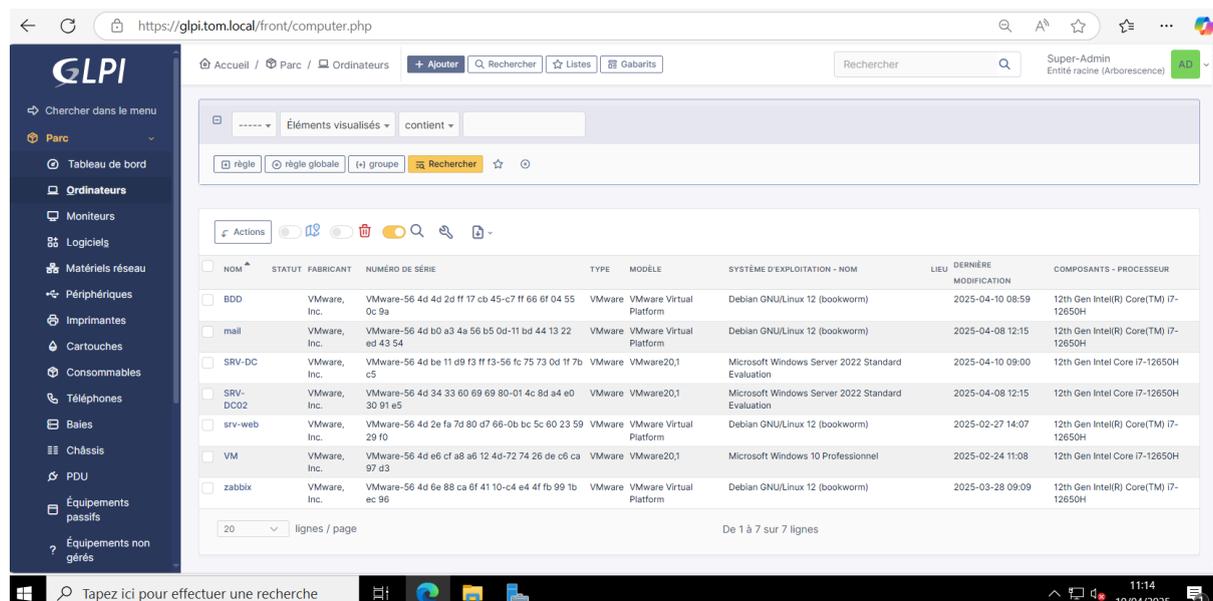
Voilà, l'authentification fonctionne ! L'utilisateur a pu se connecter avec son compte Active Directory et il hérite du rôle "**Self-service**".



Dans le même temps, à partir du compte admin de GLPI, je peux remarquer la présence d'un nouveau compte utilisateur dont l'identifiant est "**v.lever@tom.local**" ! GLPI a également récupéré le nom, le prénom et l'adresse e-mail à partir de différents attributs de l'objet LDAP.

# V. Inventaire Automatique

Afin d'automatiser mon inventaire, j'ai décidé d'installer sur chaque serveur et client le logiciel (GPI Inventory) qui permet de faire une remontée d'inventaire automatique. Cela donne des informations très complètes sur mon serveur ou mon client.

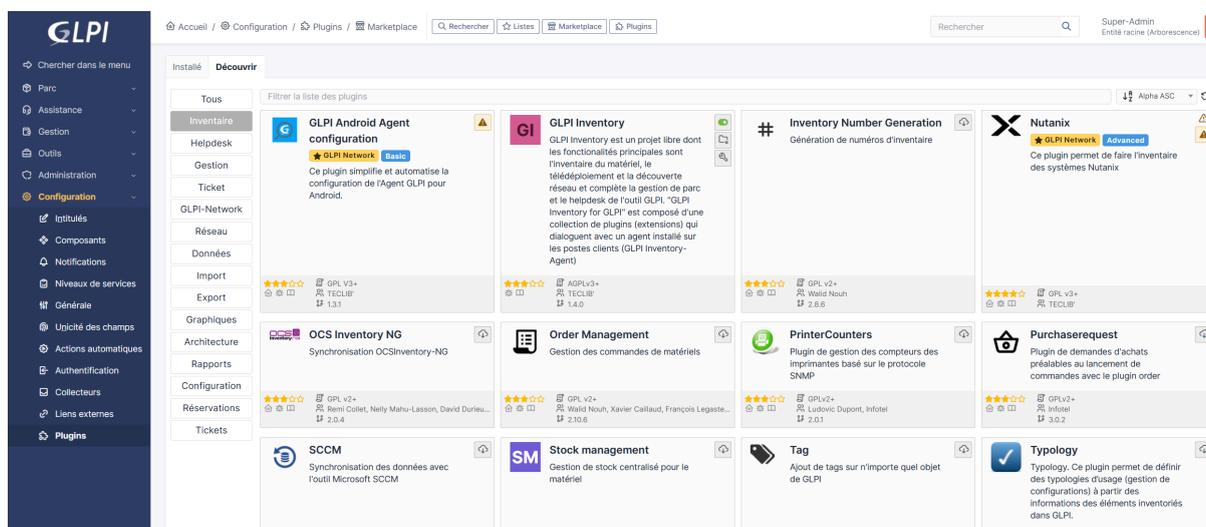


## Inventaire sous Windows

Pour commencer, nous aurons besoin d'installer le plugin Agent-GLPI, sur notre serveur GLPI. Pour cela, nous allons nous rendre dans l'arborescence suivante :

- Configuration > Plugins > Marketplace > Découvrir

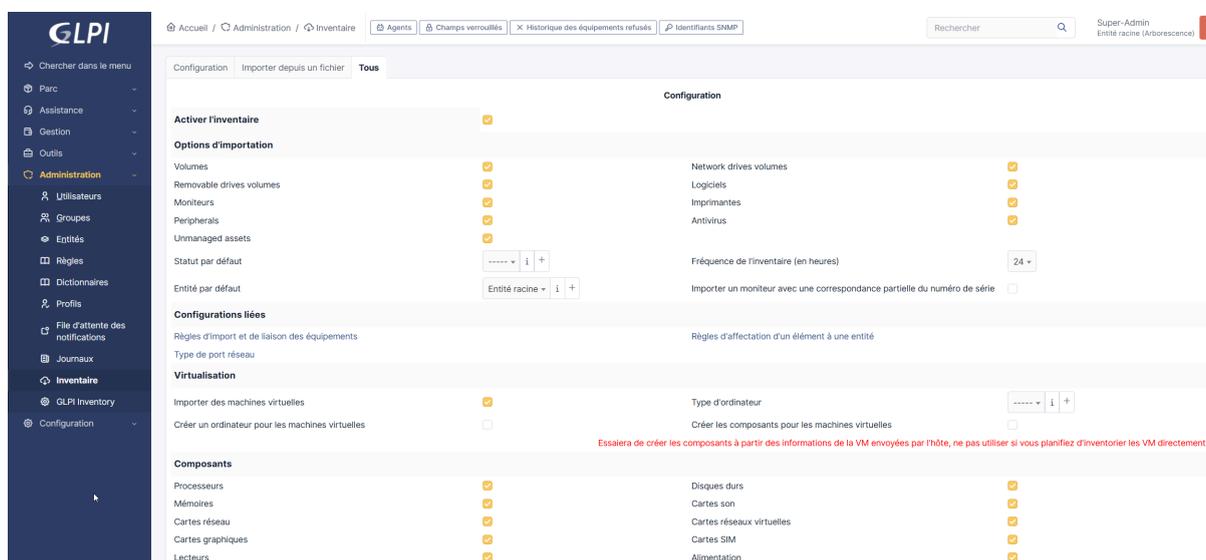
Dans le champ « Inventaire », vous allez rechercher le plugin « GLPI Inventory » et l'installer !



Ensuite, veuillez activer le plugin. Puis, vous vous rendez dans l'onglet :

- **Administration > Inventaire**

Il faudra impérativement « activer » l'inventaire si vous souhaitez que vos machines remontent sur votre GLPI. N'oubliez pas de sauvegarder !



Veuillez télécharger l'agent GLPI sur le site de GITHUB.

# GLPI Agent v1.11 Latest

Here you can download GLPI-Agent v1.11 packages.

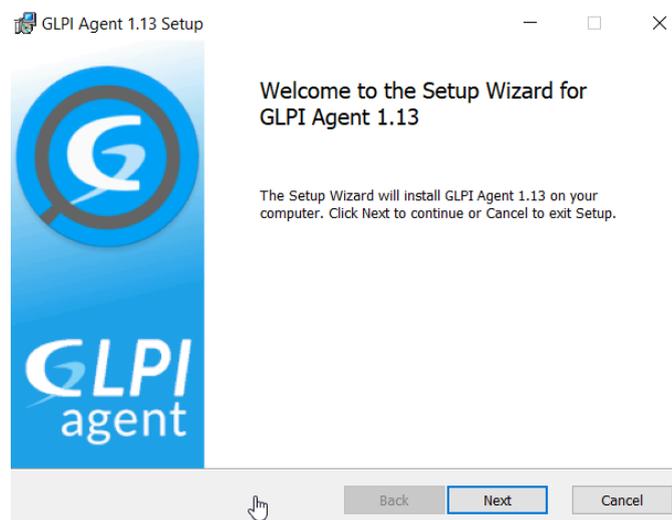
Don't forget to follow our [installation documentation](#).

Release notes are available here: <https://glpi-project.org/glpi-agent-v1-11-released/>

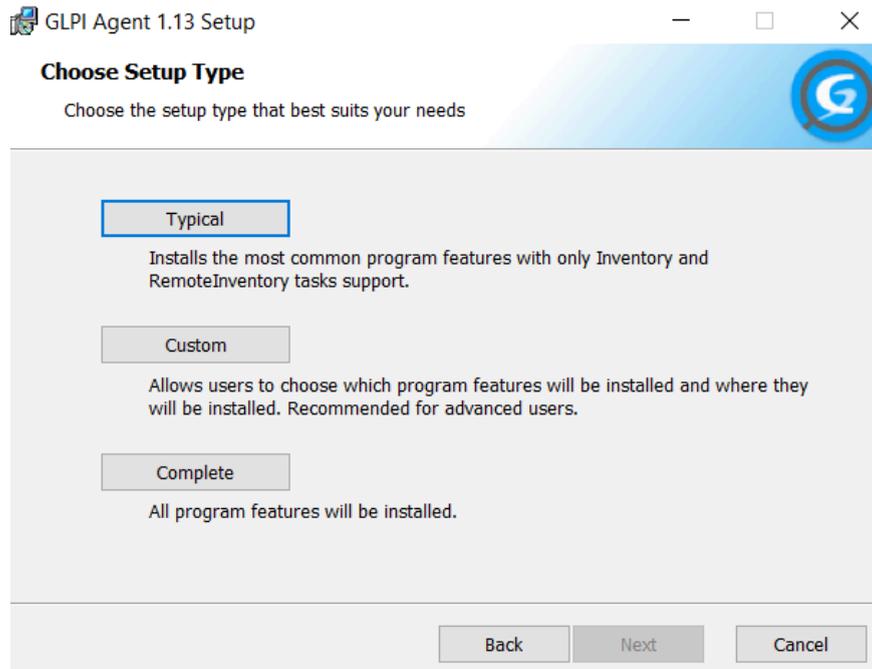
## Windows

Arch	Windows installer	Windows portable archive
64 bits	<a href="#">GLPI-Agent-1.11-x64.msi</a>	<a href="#">GLPI-Agent-1.11-x64.zip</a>

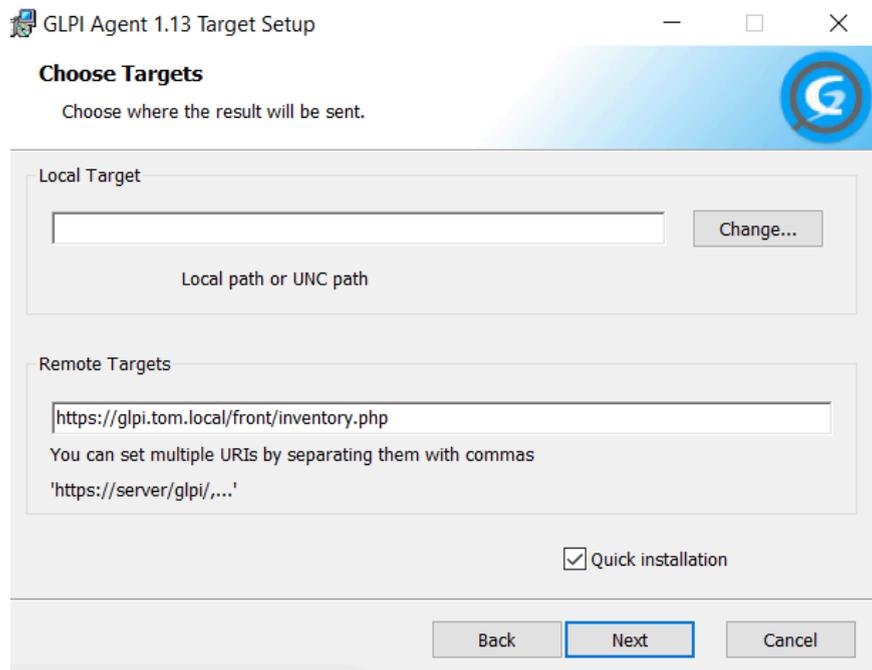
Exécutez-le depuis votre explorateur de fichiers :



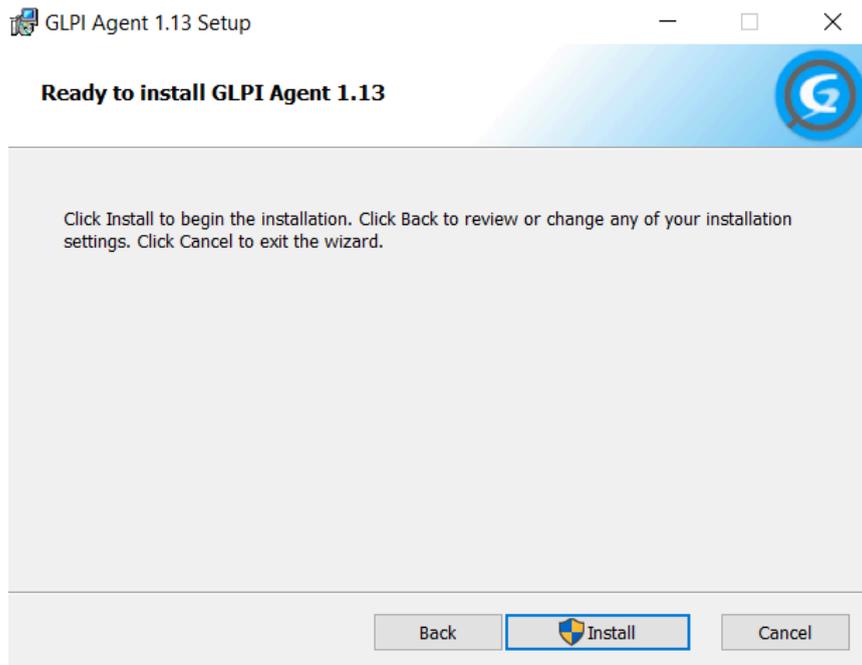
Choisissez "Typical" :



Dans la partie "Remote Targets", il faut que vous ajoutiez <https://glpi.tom.local/front/inventory.php>



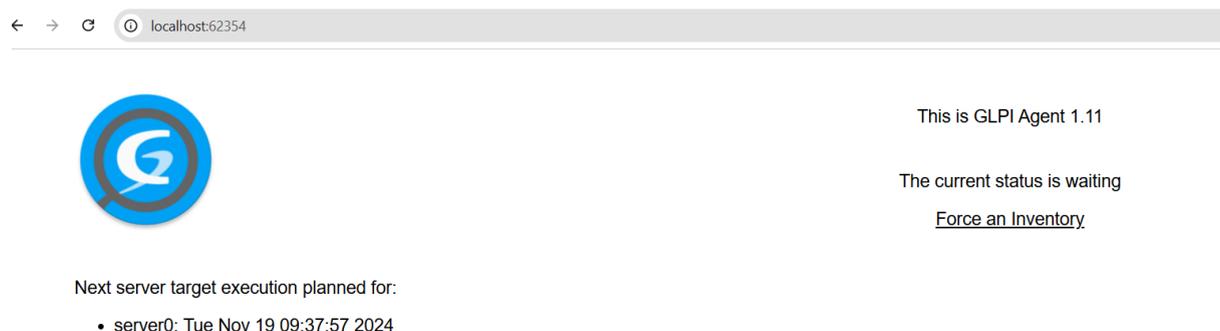
Et ensuite, vous l'installez :



Pour faire une remontée d'inventaire automatique en accéléré, vous pourrez le faire grâce à l'URL suivante que vous entrerez dans une barre d'adresse d'un navigateur web :

- **<http://localhost:62354/>**

Il vous suffira de cliquer sur le lien « Force an Inventory » et la remontée d'inventaire se fera automatiquement.

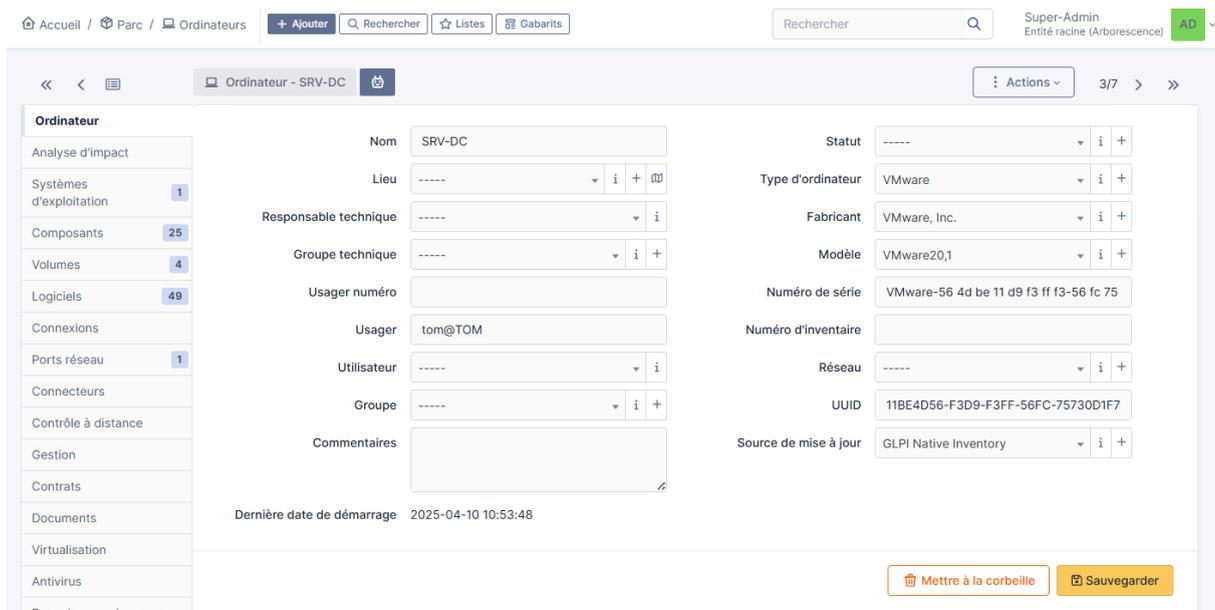
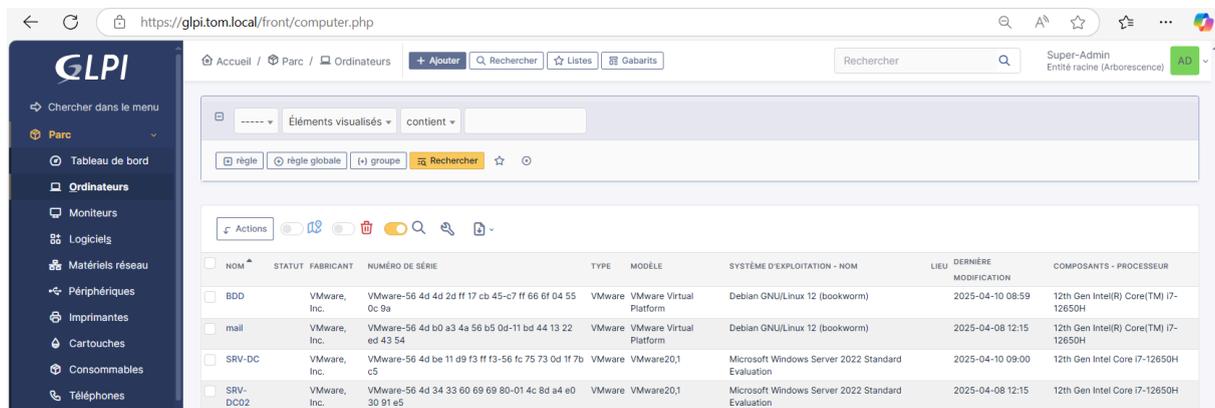


Sinon, il suffit d'attendre 10 à 20 min avant que le premier inventaire se fasse.

Une fois que l'inventaire sera fait, vous pourrez donc vous rendre sur l'interface de GLPI, puis dans l'onglet :

- **Parc > Ordinateurs**

Vous verrez donc votre PC avec le nom d'ordinateur que vous lui avez donné.



## Inventaire sous Linux

Tout d'abord, commençons par installer perl si ce n'est pas fait

```
apt install perl
```

Nous allons exécuter le script d'installation fourni par GLPI. Pensez à récupérer le script d'installation le plus récent : <https://github.com/gipi-project/gipi-agent/releases>

```
wgethttps://github.com/glpi-project/glpi-agent/releases/download/1.13/glpi-agent-1.13-linux-installer.pl
```

Grâce à cette commande, vous pourrez afficher l'aide et adapter votre commande avec les valeurs souhaitées :

```
perl glpi-agent-1.13-linux-intaller.pl --help
```

Pour mon besoin, j'ai personnalisé ma commande de cette façon :

```
perl glpi-agent-1.13-linux-installer.pl -s https://glpi.tom.local/front/inventor  
y.php --runnow --install
```

On peut vérifier la bonne installation avec la commande :

```
systemctl status glpi-agent
```

```
stom@BDD:~$ systemctl status glpi-agent.service
● glpi-agent.service - GLPI agent
   Loaded: loaded (/lib/systemd/system/glpi-agent.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-04-10 10:57:05 CEST; 49min ago
     Docs: man:glpi-agent
   Main PID: 609 (glpi-agent: wai)
    Tasks: 1 (limit: 2273)
   Memory: 117.4M
      CPU: 26.621s
   CGroup: /system.slice/glpi-agent.service
           └─609 "glpi-agent: waiting"

Warning: some journal files were not opened due to insufficient permissions.
```

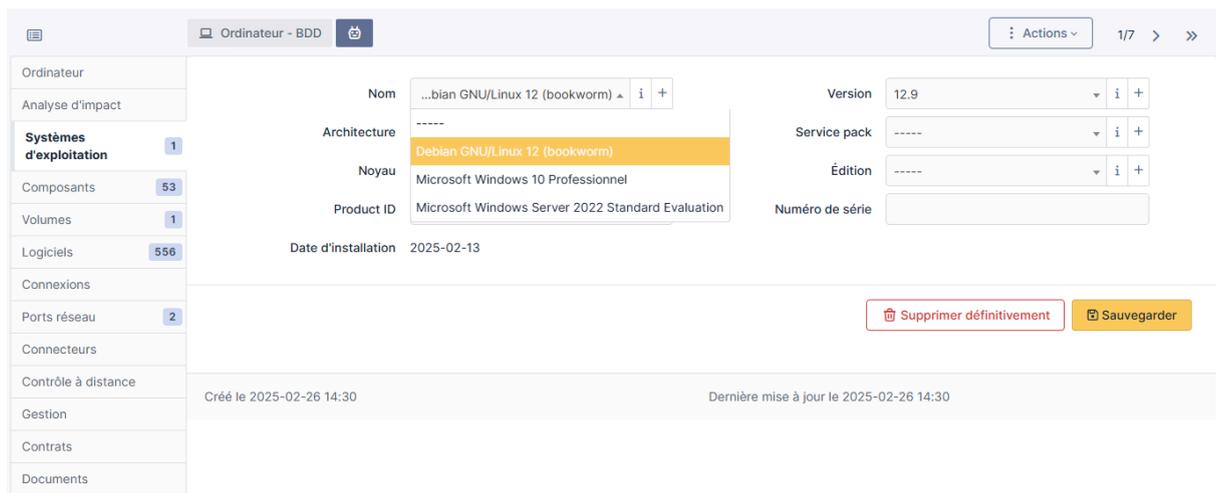
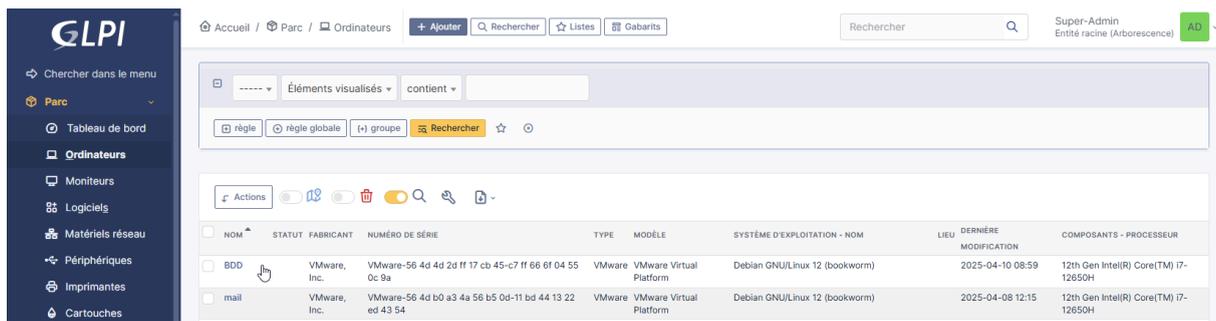
Si on a besoin d'effectuer des modifications, les différents fichier de configuration se situe dans :

```
/etc/glpi-agent/
```

On peut activer le service qui gère l'agent au démarrage de la machine via cette commande :

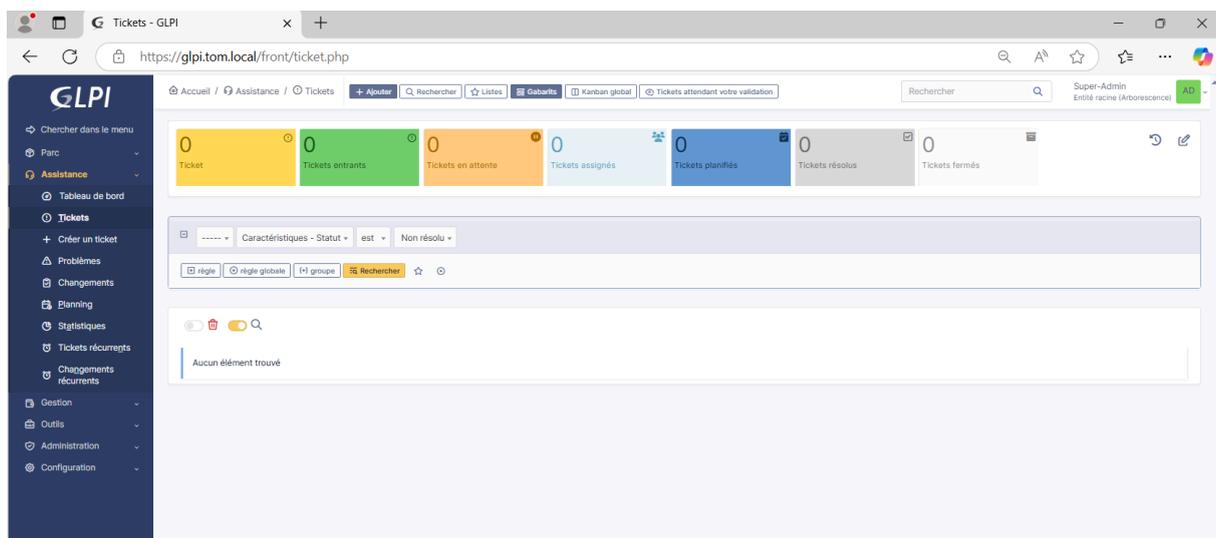
```
systemctl enable glpi-agent
```

Dans l'interface web de GLPI, notre serveur Linux remonte correctement !



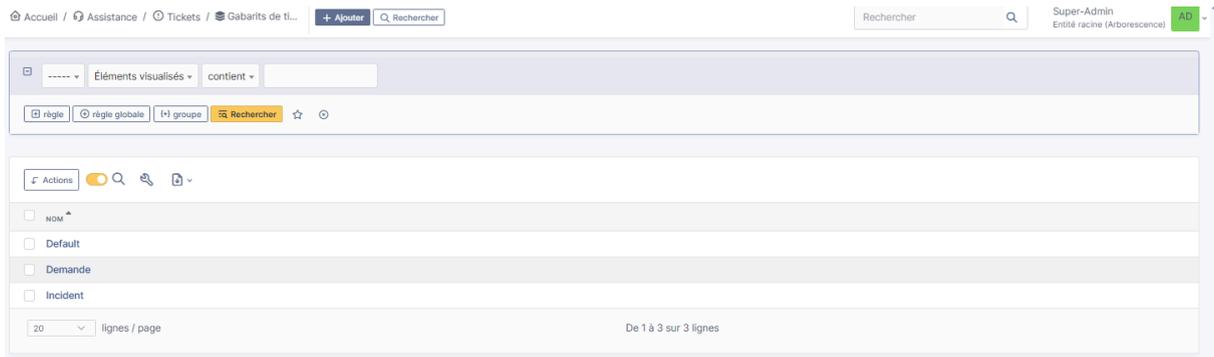
## VI. Création des gabarits de tickets

Se rendre dans Assistance > Ticket > Gabarits :



On va créer deux gabarits qui sont créer exactement de la même façon :

- Incident
- Demande

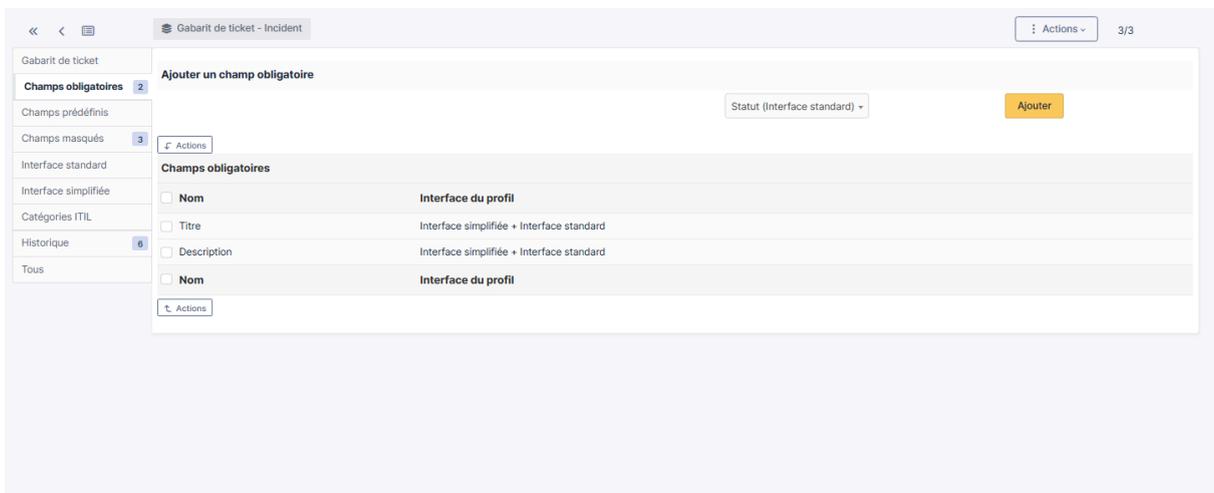


A l'intérieur de chaque gabarit, on va ajouter des "Champs Obligatoires" et des "Champs Masqués".

- Champs obligatoires = obligé de renseigner lors de la création du ticket.
- Champs masqués = champs qui seront masqués lors de la création du ticket.

## A. Champs obligatoires :

Dans les champs obligatoires, j'aurais le titre et la description :



## B. Champs masqués:

Dans les champs masqués, j'aurais la priorité, l'urgence et l'impact :

« < » **Gabarit de ticket - Incident** Actions 3/3

Gabarit de ticket

Champs obligatoires **2**

Champs prédéfinis

**Champs masqués** **3** Actions

Interface standard

Interface simplifiée

Catégories ITIL

Historique **6**

Tous

### Ajouter un champ caché

Titre  Ajouter

#### Champs masqués

- Nom
- Priorité
- Urgence
- Impact
- Nom

Actions