Boumrah Samy

GLPI - Chapitre 1 : Installer l'helpdesk GLPI sur notre machine debian 13

GLPI (Gestion Libre de Parc Informatique) est une solution open source de gestion des services informatiques (**ITSM – IT Service Management**) et de gestion d'actifs IT.
Développé en **PHP** et reposant sur une base de données **MySQL/MariaDB**, GLPI permet d'administrer l'ensemble de l'infrastructure informatique depuis une interface web centralisée.

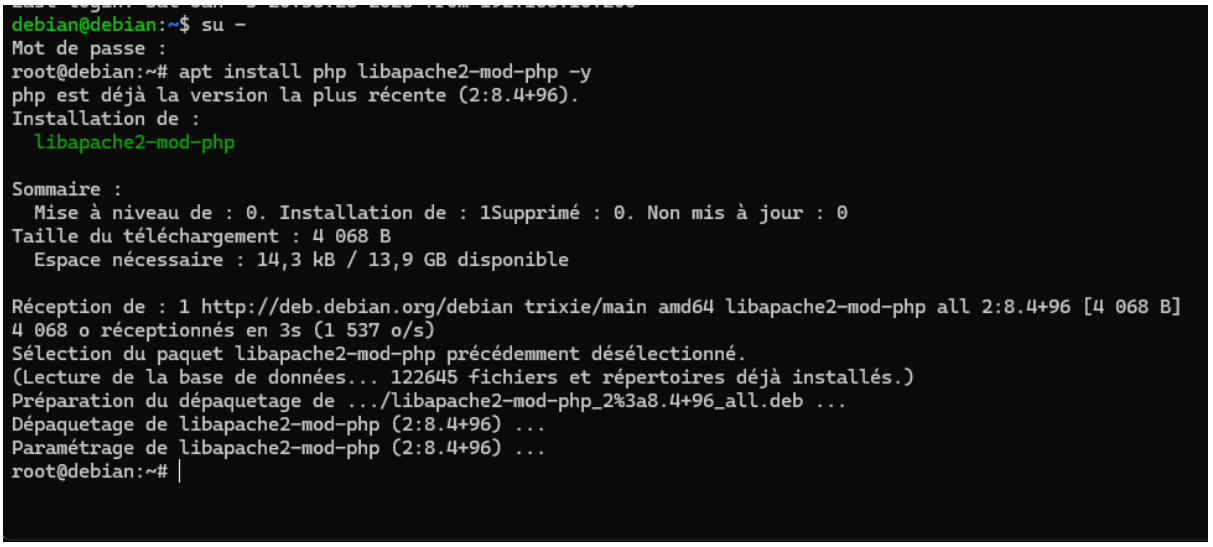
Fonctionnalités principales

- **Gestion d'inventaire** : Suivi du matériel informatique (postes de travail, serveurs, périphériques, licences logicielles, etc.).
- **Helpdesk / Ticketing** : Système de gestion des incidents et des demandes utilisateurs, avec suivi, priorisation et éventuels SLA.
- **Gestion des actifs** : Suivi du cycle de vie complet du parc (acquisition, déploiement, maintenance, retrait).
- **Base de connaissances** : Mise à disposition d'une documentation centralisée et de FAQ à destination des utilisateurs et techniciens.
- **Réservations** : Gestion des prêts et réservations de matériel.
- **Gestion financière** : Suivi des coûts, contrats, budgets et amortissements associés aux actifs informatiques.

Préparation de l'environnement LAMP pour GLPI

Pour déployer GLPI dans notre environnement **LAMP** (Linux, Apache, MariaDB, PHP), il est nécessaire de compléter la configuration d'Apache avec les modules PHP adaptés.
Les opérations d'installation et de configuration suivantes seront réalisées directement sur la machine **Debian 13**.

Pour la suite de ce chapitre, les commandes sont exécutées en session SSH avec le compte **superutilisateur root** afin de simplifier la saisie.
Il est également possible de rester connecté avec un utilisateur standard et de préfixer chaque commande avec `sudo`.



"Figure 1 : Connexion à la machine Debian en SSH en tant que superutilisateur pour l'installation et la configuration de GLPI."

Après l'installation des composants nécessaires, il est important de redémarrer le service Apache afin de prendre en compte les éventuelles modifications liées à PHP ou à la configuration du serveur web.

```bash
systemctl restart apache2
```

Connexion au serveur MariaDB

Une fois Apache relancé, la prochaine étape consiste à préparer la base de données qui sera utilisée par GLPI.
Connectez-vous au serveur **MariaDB** avec le compte `root` :

```bash
mysql -u root
```

(Le mot de passe pourra être demandé si configuré lors de `mariadb-secure-installation`.)

Création de la base de données GLPI

Une fois connecté au shell MariaDB, commencez par créer la base de données dédiée à GLPI :

```
bash
create database glpi;
```

NB : Ne pas oublier le **point-virgule** à la fin de la commande, indispensable pour son exécution.

Création de l'utilisateur GLPI

Créez ensuite un utilisateur spécifique `glpi` et associez-lui un mot de passe (ici glpi) pour la connexion depuis `localhost` :

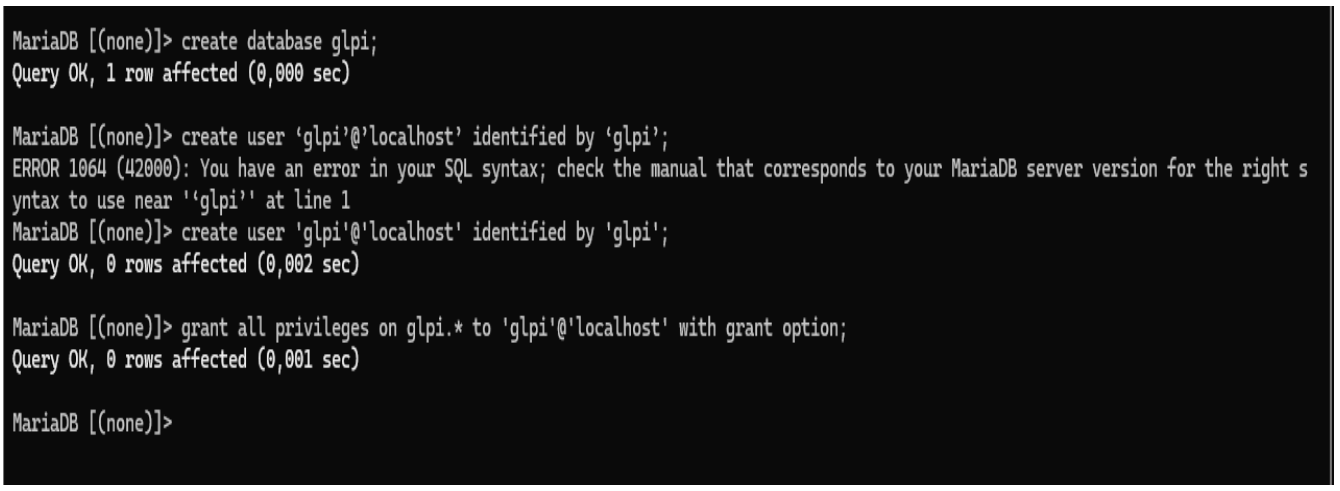
```
bash
create user 'glpi'@'localhost' identified by 'glpi';
```

Attribution des privilèges

Enfin, accordez à cet utilisateur tous les privilèges nécessaires sur la base `glpi`, avec la possibilité de les déléguer :

```
bash
grant all privileges on glpi.* to 'glpi'@'localhost' with
grant option;
```

Cette étape permet à l'utilisateur glpi de gérer entièrement la base de données GLPI (création de tables, modification de schéma, insertions, etc.), ce qui est requis lors de l'installation de l'application.



"Figure 2 : Création de la base de données GLPI et de l’utilisateur dédié dans MariaDB."

Pour terminer la configuration de l’utilisateur `glpi`, il est nécessaire de recharger les privilèges dans MariaDB afin de prendre en compte les modifications effectuées.

```
bash
flush privileges;
```

Une fois cette commande exécutée, vous pouvez quitter le shell MariaDB :

```
bash
exit;
```

On ne va pas l’installer directement, sinon ce dernier se retrouverait sur notre machine locale ce qui nous serait inutile pour notre lab. On va donc faire un clique droit sur le fichier et copier le lien de ce dernier.

À ce stade, la base de données **`glpi`** et l’utilisateur **`glpi`** sont correctement créés et prêts à être utilisés par l’application GLPI.

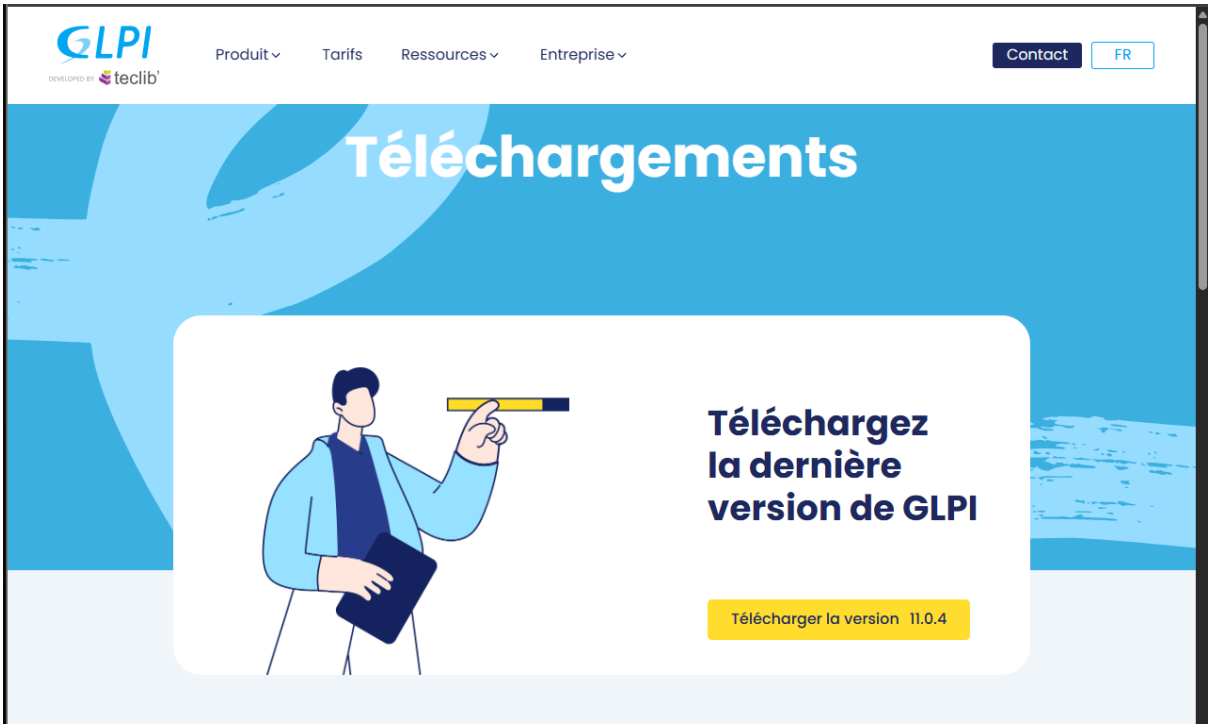
Récupération du fichier d’installation GLPI

La prochaine étape consiste à récupérer l’archive d’installation de **GLPI** depuis le site officiel du projet.
L’objectif est de télécharger le fichier directement sur le serveur Debian, via un lien vers l’archive, plutôt que de l’installer sur la machine locale.

Depuis un navigateur web (sur votre poste), accédez au site officiel de GLPI, puis :

1. Localisez la page de **téléchargement** de la version souhaitée de GLPI.
2. Sur le lien vers l'archive (fichier `.tgz` ou `.tar.gz`), effectuez un **clic droit**.
3. Sélectionnez **Copier l'adresse du lien** (ou équivalent selon le navigateur).

Ce lien sera ensuite utilisé sur la machine Debian (par exemple avec `wget` ou `curl`) pour télécharger directement l'archive dans l'environnement serveur, adapté à votre lab.



"Figure 3 : Récupération du lien de téléchargement de l'archive GLPI depuis le site officiel."

Une fois l'URL de l'archive GLPI copiée depuis le site officiel, le téléchargement se fait directement depuis la machine Debian.

Depuis votre session sur Debian, exécutez :

```
bash
wget
https://github.com/glpi-project/glpi/releases/download/11.0.
4/glpi-11.0.4.tgz
```

La commande `wget` télécharge le fichier `glpi-11.0.4.tgz` dans le répertoire courant en utilisant le lien précédemment copié.

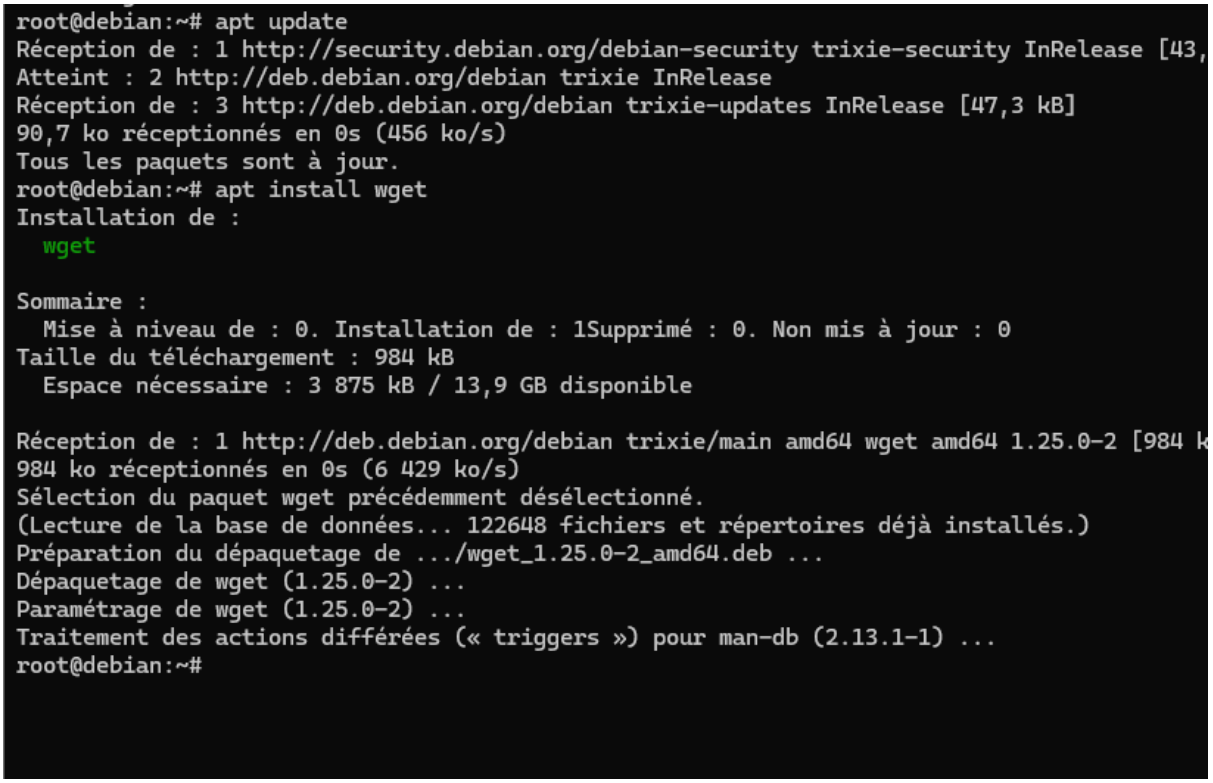
Installation de wget si nécessaire

Si Debian renvoie un message du type `wget : commande introuvable`, cela signifie que l'outil **wget** n'est pas encore installé sur la machine.
Vous pouvez l'installer en deux étapes :

```
bash
apt update
apt install wget
```

- `apt update` met à jour la liste des paquets disponibles.
- `apt install wget` installe l'outil de téléchargement en ligne de commande.

Une fois `wget` installé, vous pouvez relancer la commande de téléchargement de l'archive GLPI.



"Figure 4 : Téléchargement de l'archive GLPI depuis GitHub avec la commande wget sur Debian."

Nous pouvons ensuite lancé le téléchargement de glpi 👍



Une fois le téléchargement terminé, l'archive GLPI peut être décompressée afin d'extraire l'arborescence de l'application.

Décompression de l'archive GLPI

Depuis le répertoire où a été téléchargé le fichier `glpi-11.0.4.tgz`, exécutez :

```
bash
tar xvf glpi-11.0.4.tgz
```

Remarque : adaptez le nom du fichier (`glpi-11.0.4.tgz`) à la version exacte que vous avez téléchargée.

Pour vérifier le nom exact du fichier ou du répertoire créé, vous pouvez lister le contenu du répertoire courant :

```
bash
ls -la
```

Vous devriez voir un répertoire nommé `glpi` correspondant aux fichiers extraits de l'archive.

Déplacement du répertoire GLPI vers le serveur web

Par défaut, après l'extraction, le dossier `glpi` se trouve dans le répertoire personnel de l'utilisateur (ici, le `home` de `root` si vous travaillez en tant que superutilisateur). Il doit être déplacé dans le répertoire racine du serveur web Apache.

Utilisez la commande suivante :

```
bash
mv glpi /var/www/html/glpi
```

Cette commande place l'application GLPI dans le répertoire `/var/www/html/glpi`, qui sera utilisé par Apache pour servir l'interface web de GLPI.

Vous pouvez vérifier que le dossier est désormais au bon emplacement avec :

```
bash
ls -la /var/www/html
```

Vous devez y voir apparaître le répertoire `glpi`

```
root@debian:~# cd /var/www/html
root@debian:/var/www/html# ls -la
total 24
drwxr-xr-x  3 root   root    4096  4 janv. 18:24 .
drwxr-xr-x  3 root   root    4096  2 janv. 23:54 ..
drwxr-xr-x 22 debian debian  4096  4 déc.  10:19 glpi
-rw-r--r--  1 root   root   10703  2 janv. 23:54 index.html
root@debian:/var/www/html#
```

"Figure 5 : Répertoire GLPI déplacé dans /var/www/html et vérification de sa présence via la commande ls."

Pour fonctionner correctement, GLPI nécessite un ensemble de modules PHP supplémentaires (base de données, LDAP, extensions graphiques, internationalisation, etc.).

Installation des modules PHP nécessaires à GLPI

Placez-vous d'abord dans le répertoire du serveur web :

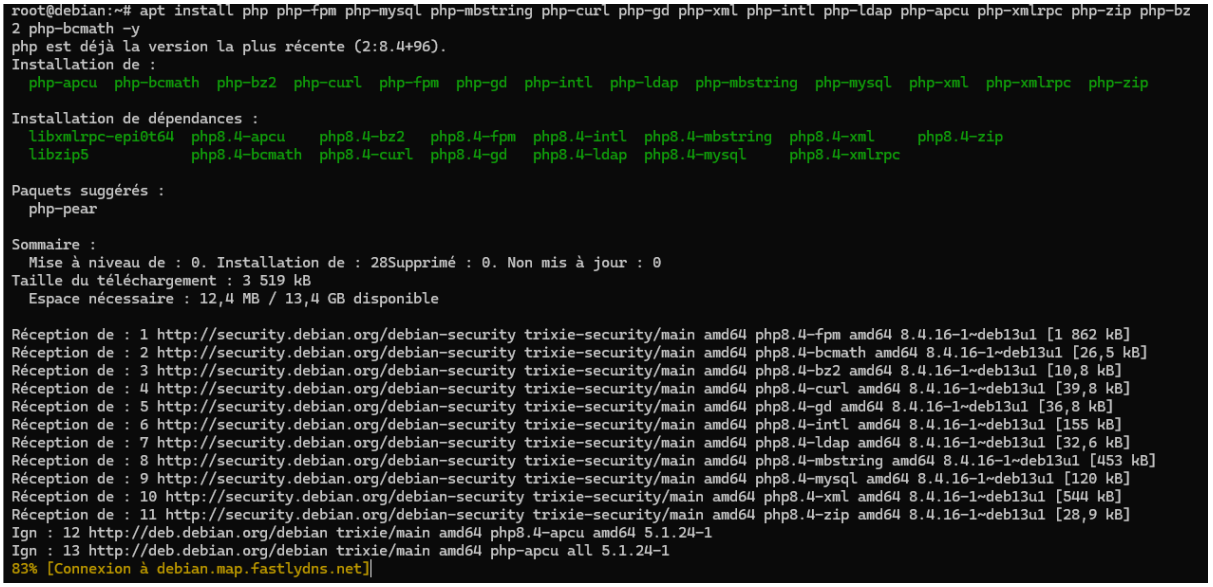
```
bash
cd /var/www/html
```

Puis installez l'ensemble des modules PHP requis pour GLPI avec la commande suivante :

```
bash
apt install php php-fpm php-mysql php-mbstring php-curl
php-gd php-xml php-intl php-ldap php-apcu php-xmlrpc php-zip
php-bz2 php-bcmath -y
```

Cette commande installe notamment :

- le support base de données (`php-mysql`),
- les extensions de chaînes et encodage (`php-mbstring`, `php-intl`),
- les fonctionnalités réseau et API (`php-curl`),
- le rendu graphique (`php-gd`),
- LDAP (`php-ldap`) pour l'authentification d'annuaires,
- le cache APCu (`php-apcu`),
- ainsi que d'autres extensions nécessaires au bon fonctionnement de GLPI.



"Figure 6 : Installation des modules PHP requis pour GLPI depuis le répertoire /var/www/html."

Pour que GLPI puisse fonctionner correctement avec Apache, il est nécessaire d'ajuster le propriétaire du répertoire de l'application de façon à ce qu'il soit géré par l'utilisateur du serveur web.

Attribution de la propriété du dossier GLPI à Apache

Sur Debian, le serveur web Apache s'exécute généralement sous l'utilisateur et le groupe **`www-data`**.
L'objectif est donc de donner la propriété du dossier `glpi` à cet utilisateur, afin qu'Apache puisse lire et écrire dans les répertoires nécessaires (logs, fichiers, configuration, etc.).

Placez-vous d'abord dans le répertoire racine du serveur web :

```
bash
chown -R www-data:www-data glpi
```

- `chown` : change le propriétaire des fichiers.
- `-R` : applique le changement de façon récursive à tout le contenu du dossier `glpi`.
- `www-data:www-data` : définit l'utilisateur et le groupe propriétaires.

Puis exécutez la commande de changement de propriétaire sur le dossier GLPI

```
bash
ls -la
```

On voit que ça passe de DEBIAN à www-data

```
root@debian:/var/www/html# ls -la
total 24
drwxr-xr-x  3 root   root    4096  4 janv. 18:24 .
drwxr-xr-x  3 root   root    4096  2 janv. 23:54 ..
drwxr-xr-x 22 debian debian  4096  4 déc.  10:19 glpi
-rw-r--r--  1 root   root   10703  2 janv. 23:54 index.html
root@debian:/var/www/html# cd
```

```
root@debian:/var/www/html# chown -R www-data:www-data /var/www/html/glpi/
root@debian:/var/www/html# ls -la
total 24
drwxr-xr-x  3 root     root      4096  4 janv. 18:24 .
drwxr-xr-x  3 root     root      4096  2 janv. 23:54 ..
drwxr-xr-x 22 www-data www-data  4096  4 déc.  10:19 glpi
-rw-r--r--  1 root     root     10703  2 janv. 23:54 index.html
root@debian:/var/www/html#
```

"Figure 7 : Attribution récursive de la propriété du dossier GLPI à l'utilisateur et au groupe www-data pour permettre à Apache de gérer les fichiers de l'application."

Pour compléter la configuration des permissions, il est nécessaire d'ajuster les **droits d'accès** sur le répertoire `glpi` et l'ensemble de ses sous-répertoires.

Configuration des droits en 755 sur le répertoire GLPI

L'objectif est de définir des permissions permettant à l'utilisateur du serveur web (`www-data`) d'avoir un contrôle complet sur le répertoire, tout en limitant les droits des autres utilisateurs. Depuis le répertoire contenant `glpi` (par exemple `/var/www/html`), exécutez :

```
bash

chmod -R 755 glpi
```

Cette commande applique les droits suivants sur le dossier `glpi` et tout son contenu (`-R` pour récursif) :

- **Propriétaire (www-data)** : droits `7` → lecture, écriture et exécution (`rwx`).
- **Groupe** : droits `5` → lecture et exécution (`r-x`).
- **Autres utilisateurs** : droits `5` → lecture et exécution (`r-x`).

Ce modèle de permissions (`755`, soit `drwxr-xr-x`) est courant pour les répertoires web : le propriétaire peut modifier les fichiers, tandis que les autres peuvent les lire et y accéder, sans pouvoir les altérer.

Enfin, nous sommes prêts à finaliser l'installation de GLPI. Nous allons redémarrer Apache.

```
bash

systemctl restart apache2
```

Pour terminer l'installation de GLPI, la dernière étape se fait via l'interface web. Avant cela, il est nécessaire d'adapter la configuration d'Apache pour pointer vers le bon répertoire de l'application.

Configuration d'Apache pour GLPI 11

Modification du DocumentRoot

Pour **GLPI 11**, le serveur web doit pointer vers le sous-répertoire `/public` de GLPI. Modifiez le fichier de configuration du site par défaut d'Apache :

- Fichier à éditer : `/etc/apache2/sites-enabled/000-default.conf`

Appliquez la configuration suivante :

```
text
<Directory /var/www/html/glpi/public>

    Require all granted

    AllowOverride All

    RewriteEngine On

    RewriteCond %{REQUEST_FILENAME} !-f

    RewriteRule ^(.*)$ index.php [QSA,L]

</Directory>
```

Cette configuration :

- définit `/var/www/html/glpi/public` comme **racine web** du site,
- autorise l'accès à ce répertoire (`Require all granted`),
- permet l'utilisation de `.htaccess` (`AllowOverride All`),
- active la réécriture d'URL pour rediriger les requêtes vers index.php lorsqu'aucun fichier physique ne correspond.

Activation de mod_rewrite et redémarrage d'Apache

Activez ensuite le module de réécriture d'URL d'Apache, puis redémarrez le service pour prendre en compte les modifications :

```
bash
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Le module `rewrite` est indispensable pour la gestion correcte des URL par GLPI.

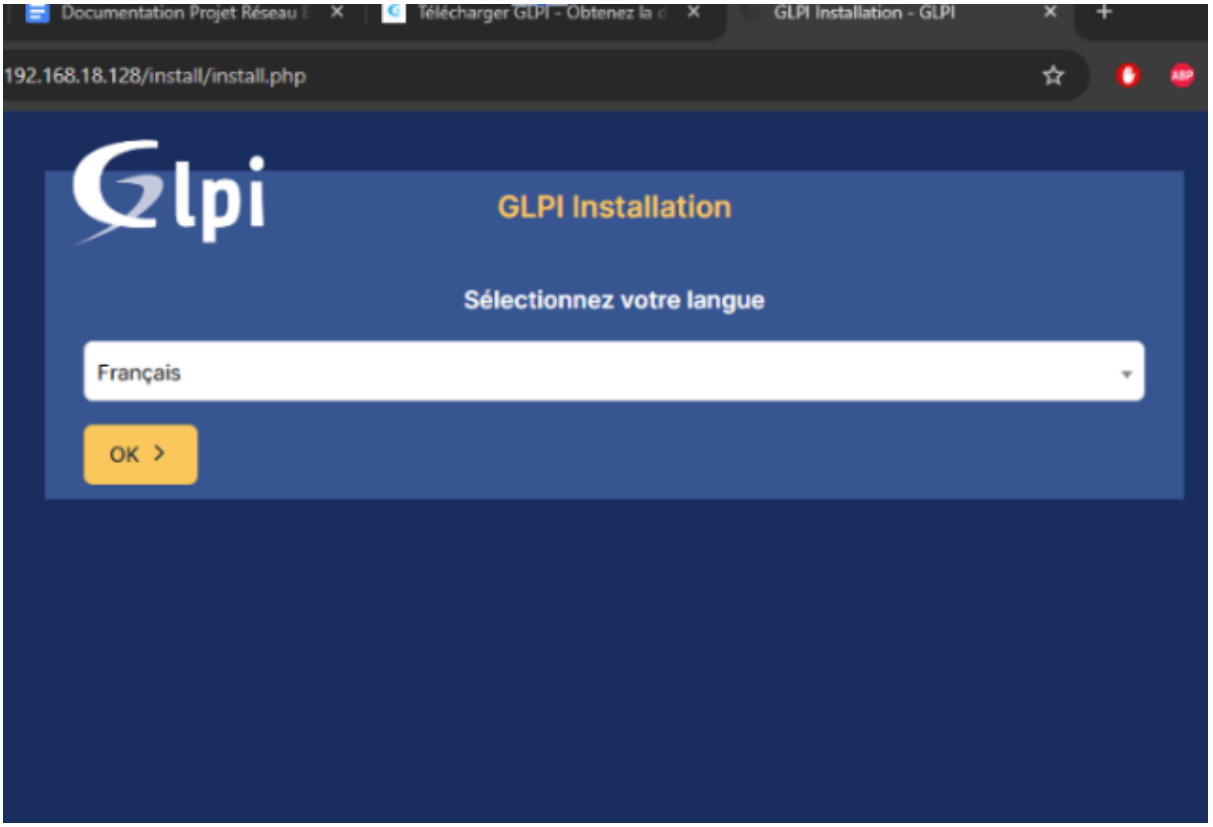
Accès à l'interface web d'installation de GLPI

Depuis un poste client, ouvrez un navigateur web puis saisissez l'adresse suivante :

http://IP-wan

- Remplacez `IP-wan` par l'adresse IP WAN de votre pare-feu pfSense (sur laquelle le port HTTP est redirigé vers votre serveur Apache/GLPI, comme vu dans le chapitre précédent).

Si la configuration Apache et la redirection sont correctes, la page d'accueil de l'**installeur web GLPI** doit s'afficher, vous permettant de poursuivre l'installation via l'interface graphique (choix de la langue, vérification des prérequis, configuration de la base de données, etc.) qu'on va faire tout de suite..



"Figure 8 : Accès à l'interface web d'installation de GLPI via l'IP WAN, après configuration d'Apache pour pointer vers /var/www/html/glpi/public."

La page suivante vous propose deux choix :

- **Installation**
- **Mise à jour**

Dans le cadre de ce lab sur une nouvelle instance, choisissez l'option **Installer** afin de procéder à une **nouvelle installation de GLPI**.



"Figure 9 : Étapes initiales de l'assistant web GLPI – choix de la langue, acceptation de la licence puis sélection du mode Installation."

Vérification des prérequis PHP par GLPI

À l'étape suivante, GLPI affiche une page récapitulant l'ensemble des **prérequis techniques**, notamment les **extensions PHP** nécessaires au bon fonctionnement de l'application.

Sur cet écran :

- GLPI liste les modules PHP détectés (ceux que vous avez installés précédemment via `apt install php ...`).
- Si un module ou une extension obligatoire est **manquant**, GLPI le signale clairement, généralement avec un indicateur d'erreur ou d'avertissement.

En cas de module manquant, il suffit de :

1. Revenir sur la machine Debian (en SSH).
2. Installer le module PHP concerné avec `apt install nom_du_module`.
3. Redémarrer Apache (`systemctl restart apache2`).
4. Rafraîchir la page de l'assistant GLPI dans le navigateur.

Cette étape permet de s'assurer que l'environnement PHP répond bien à toutes les exigences de GLPI avant de poursuivre la configuration de la base de données.



Lors des étapes suivantes de l'assistant web, GLPI vous demande de configurer la connexion à la base de données.

Configuration de la base de données dans l'assistant GLPI

Sur l'écran de configuration SQL, renseignez les paramètres de connexion à la base de données **MariaDB** que vous avez préparée auparavant sur Debian.

- **Serveur SQL** : la machine locale (dans la plupart des cas `localhost` ou `127.0.0.1`, puisque MariaDB est installé sur le même serveur que GLPI).

- **Login** : l'utilisateur que vous avez créé précédemment pour GLPI : `glpi`
- **Mot de passe** : le mot de passe associé à cet utilisateur (défini lors de la création de l'utilisateur MariaDB) : `glpi`



GLPI utilise ensuite ces informations pour se connecter au serveur MariaDB, détecter la base `glpi` existante et y créer automatiquement la structure nécessaire (tables, index, données initiales) lors des étapes suivantes de l'installation.



Nous allons sélectionner la base de données GLPI que nous avons administrée précédemment.

Nous poursuivons une fois l'installation correctement terminée.



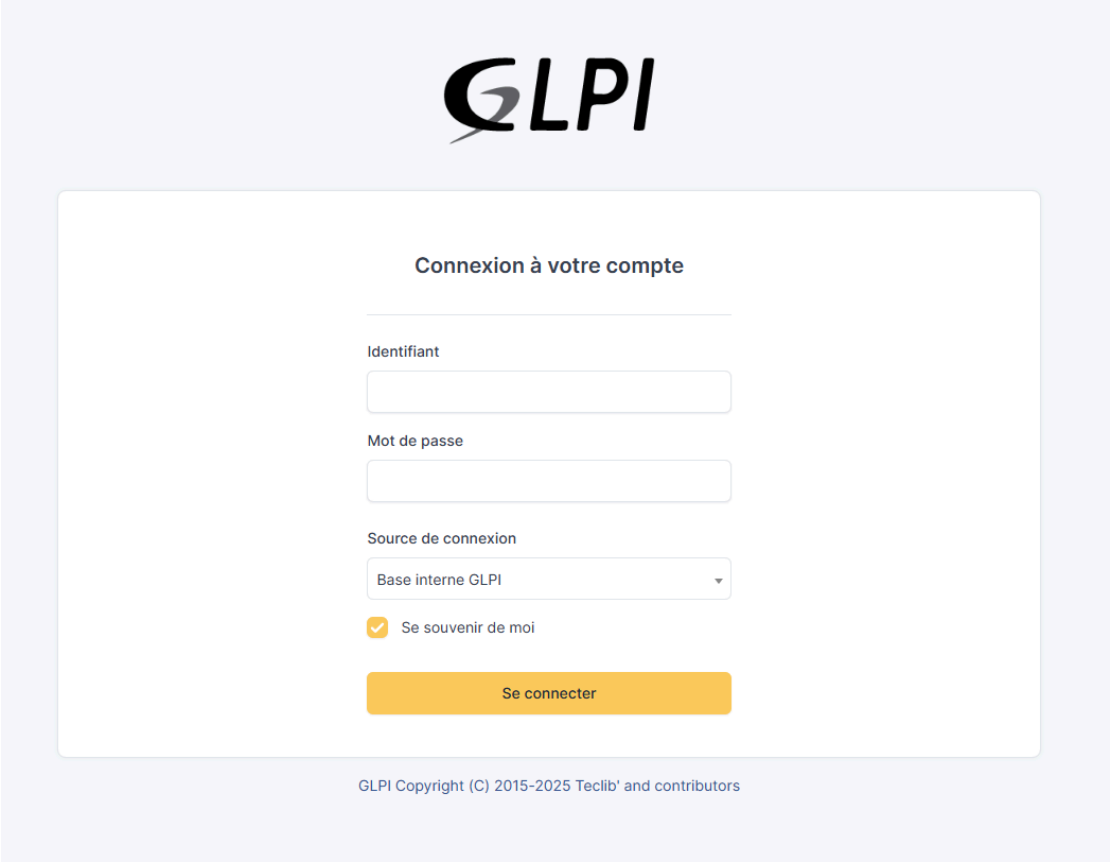
Nous pouvons ensuite décocher la case « Envoyer des statistiques d'usage », dont nous n'avons pas besoin.

L'installation est désormais terminée. Sur la dernière page, on remarque que GLPI a créé des comptes utilisateurs par défaut avec un mot de passe.

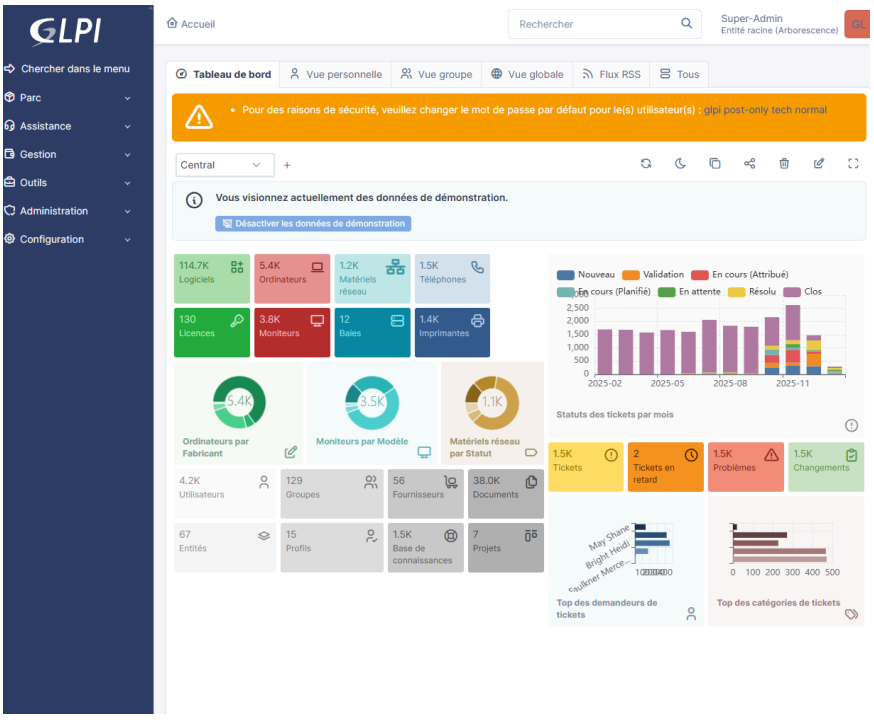


Le compte « glpi » permet notamment l'administration. Les identifiants sont présentés sous la forme login/mot de passe.

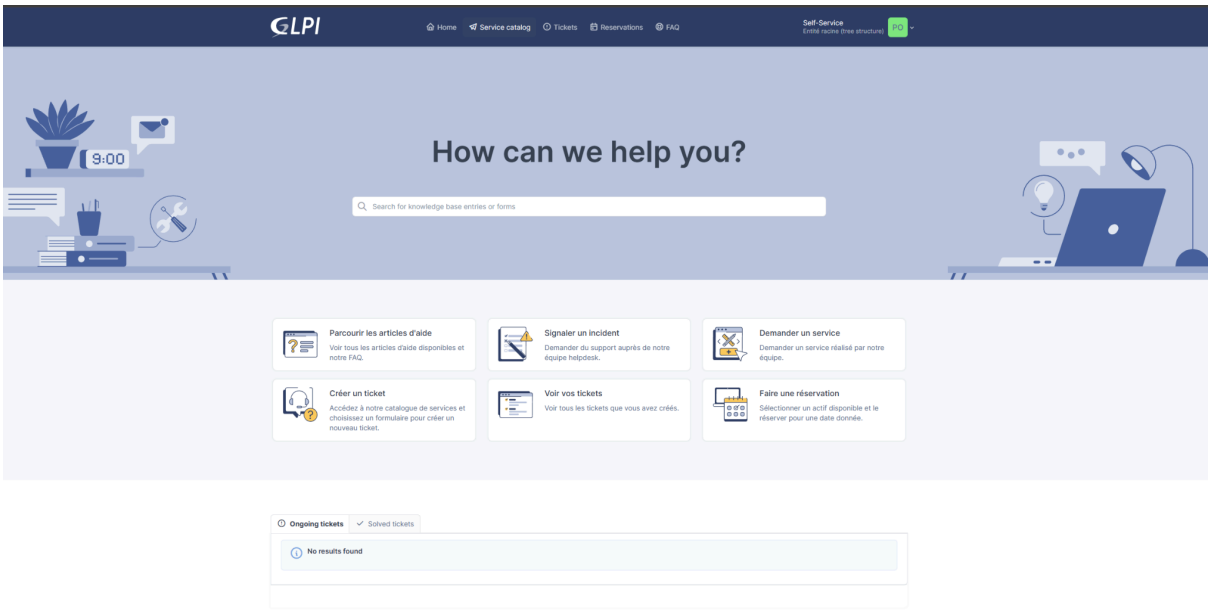
En cliquant sur « Suivant », nous accédons désormais directement à la console d'accueil : GLPI est bien installé.



Nous pouvons nous y connecter en tant qu'administrateur et commencer à découvrir GLPI.



Voici l'interface destinée à un utilisateur standard de GLPI (connecté en mode « post-only ») :



Conlcusion du chapitre :

Cette première phase d'installation de GLPI a permis de déployer une instance fonctionnelle et proprement intégrée à ton environnement LAMP Debian 13.

Les points essentiels réalisés dans ce chapitre sont :

- Préparation de l'infrastructure : création de la base glpi, de l'utilisateur SQL dédié glpi avec les droits adaptés, puis sécurisation des privilèges.
- Téléchargement, extraction et déploiement du code GLPI dans /var/www/html/glpi, avec mise en place des **propriétés** (chown www-data:www-data) et **permissions** (chmod 755) conformes aux besoins d'Apache.
- Installation des **modules PHP requis** (MySQL, intl, mbstring, gd, curl, LDAP, APCu, etc.) puis configuration d'Apache pour pointer vers /var/www/html/glpi/public, avec activation de mod_rewrite.
- Lancement de l'**assistant web GLPI**, validation des prérequis, configuration de la base de données, puis finalisation de l'installation via la création du compte administrateur et les premiers accès (admin et post-only).

Nous disposos désormais d'une base GLPI opérationnelle, installée proprement sur Debian 13, prête à être intégrée à ton lab (agents, inventaire, helpdesk, règles, annuaire LDAP, etc.), ce qui constituera la matière des chapitres suivants.

Fin du chapitre 1.

Boumrah Samy

GLPI - Chapitre 2 : Intégrer les utilisateurs AD dans GLPI avec LDAP

Contexte et objectifs

L'authentification centralisée est un élément essentiel de la gestion des systèmes d'information en entreprise.
L'intégration d'**Active Directory (AD)** avec **GLPI** permet d'éviter la double gestion des comptes utilisateurs et de simplifier l'administration du parc informatique.

Dans une infrastructure IT moderne, les utilisateurs sont généralement gérés via un annuaire Active Directory qui centralise l'authentification pour l'ensemble des services de l'entreprise.
GLPI propose nativement une connexion **LDAP / Active Directory** permettant d'importer automatiquement les utilisateurs et de synchroniser leurs informations.

Cette intégration répond à plusieurs besoins essentiels :

- **Authentification unique (SSO)** : les utilisateurs se connectent à GLPI avec leurs identifiants Active Directory.
- **Synchronisation automatique** : les modifications dans l'AD, comme un changement de service ou un départ, se répercutent dans GLPI.
- **Simplification administrative** : il n'est plus nécessaire de créer manuellement chaque compte utilisateur dans GLPI.
- **Sécurité renforcée** : la politique de mots de passe et les accès sont centralisés dans l'annuaire.

Prérequis techniques

Pour réaliser cette intégration, l'infrastructure doit disposer des éléments suivants :

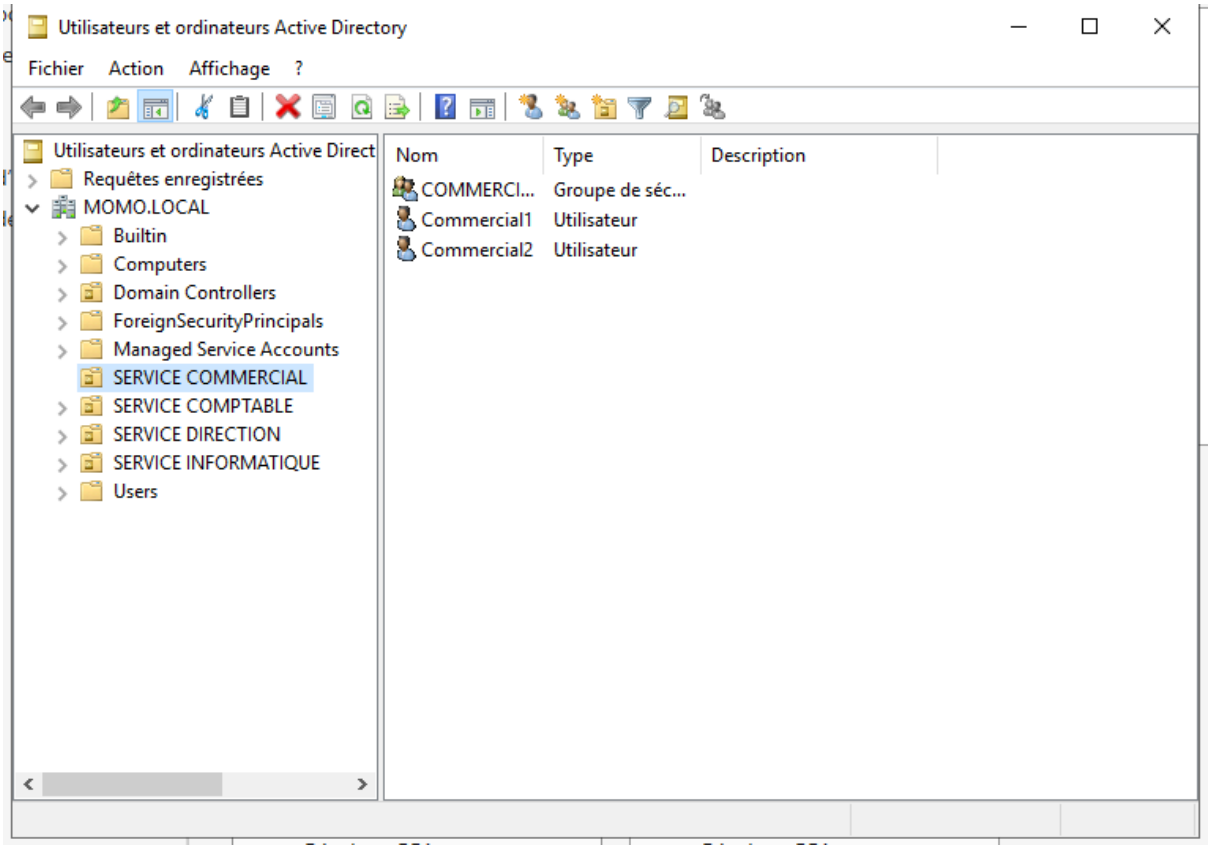
- Un serveur **Active Directory** fonctionnel avec un contrôleur de domaine accessible.
- **GLPI 11** correctement installé avec l'extension PHP **LDAP** (`php-ldap`).
- Une connectivité réseau entre le serveur GLPI et le contrôleur de domaine AD.
- Un compte de service AD avec des droits de lecture sur l'annuaire.

Cette configuration permettra aux techniciens et aux utilisateurs finaux de s'authentifier directement via leurs comptes Active Directory tout en bénéficiant des fonctionnalités complètes de GLPI.

Objectif du module

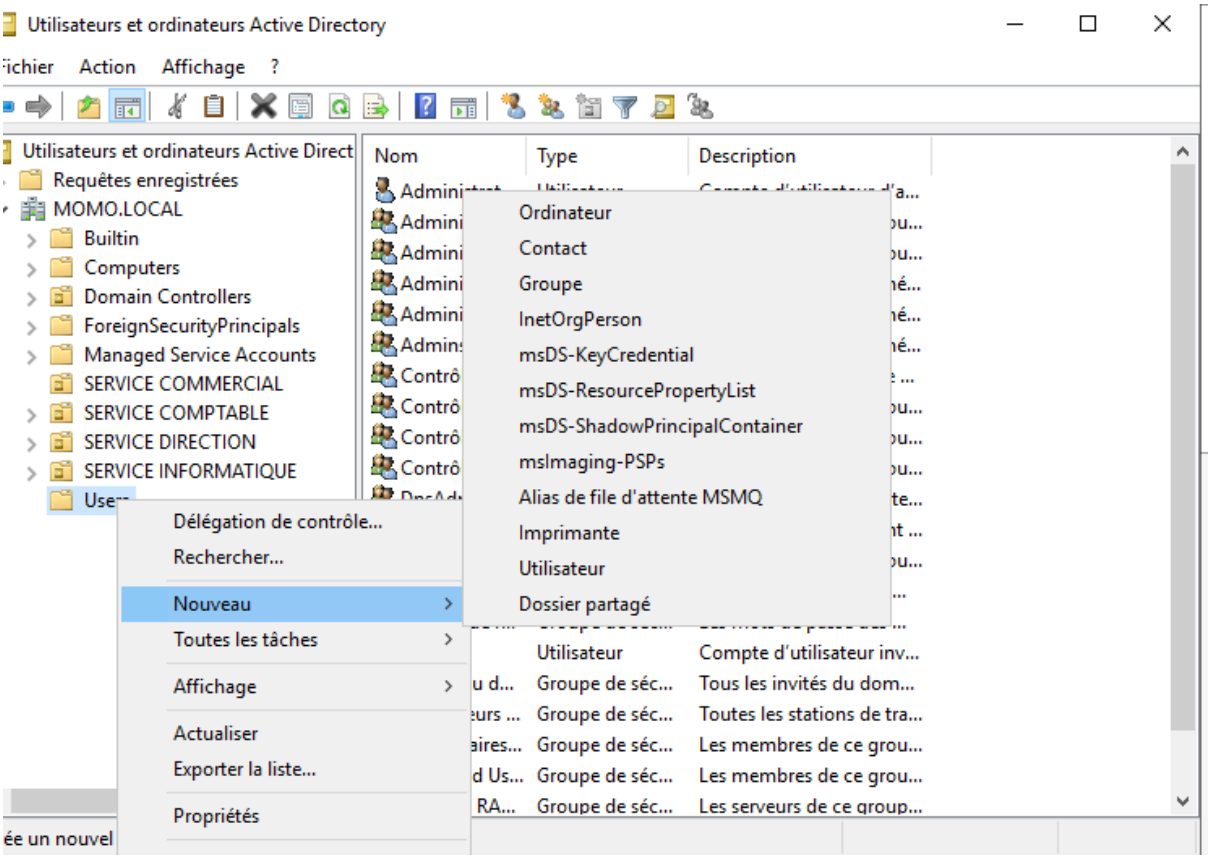
L'objectif de ce module est de spécifier les comptes ayant accès à notre GLPI à partir des utilisateurs de notre Active Directory, afin d'obtenir une traçabilité plus détaillée.

La première étape consiste à créer un nouvel utilisateur dans l'AD. Pour cela, on se connecte au **Windows Server**, puis dans le **Gestionnaire de serveur**, on accède à : **Outils > Utilisateurs et ordinateurs Active Directory**.



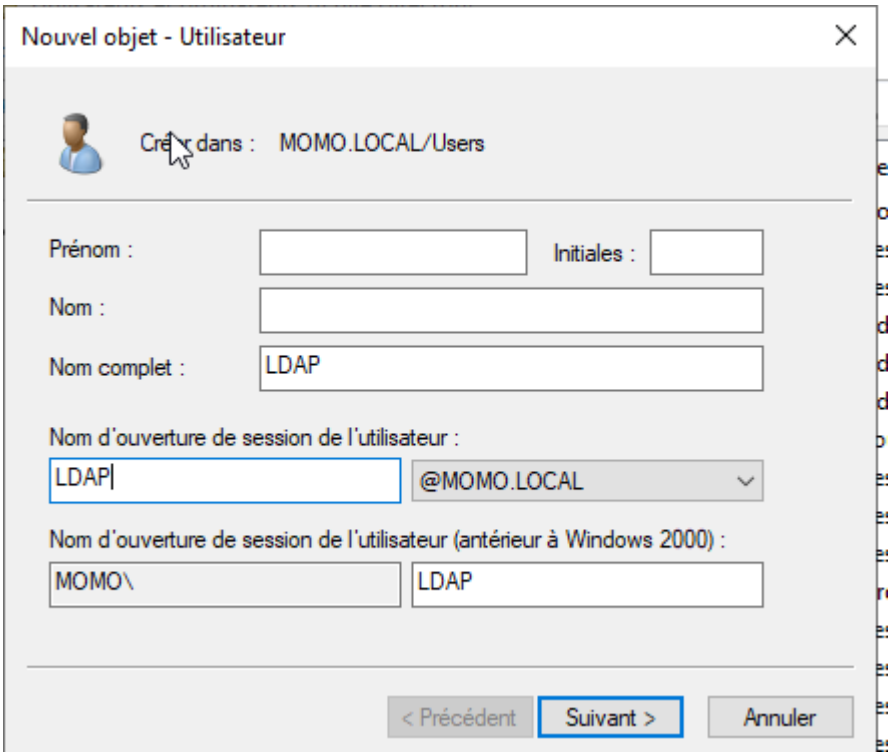
"Figure 1 : Accès à l'outil Utilisateurs et ordinateurs Active Directory depuis le Gestionnaire de serveur Windows."

La création du compte se fait depuis l'outil **Utilisateurs et ordinateurs Active Directory**. Pour cela, effectuez un clic droit sur **Users**, puis sélectionnez **Nouveau > Utilisateur**.



"Figure 2 : Création d'un nouvel utilisateur dans Active Directory via le menu contextuel de l'unité Users."

Ensuite, on crée notre utilisateur LDAP, puis on choisit son mot de passe et les paramètres associés.

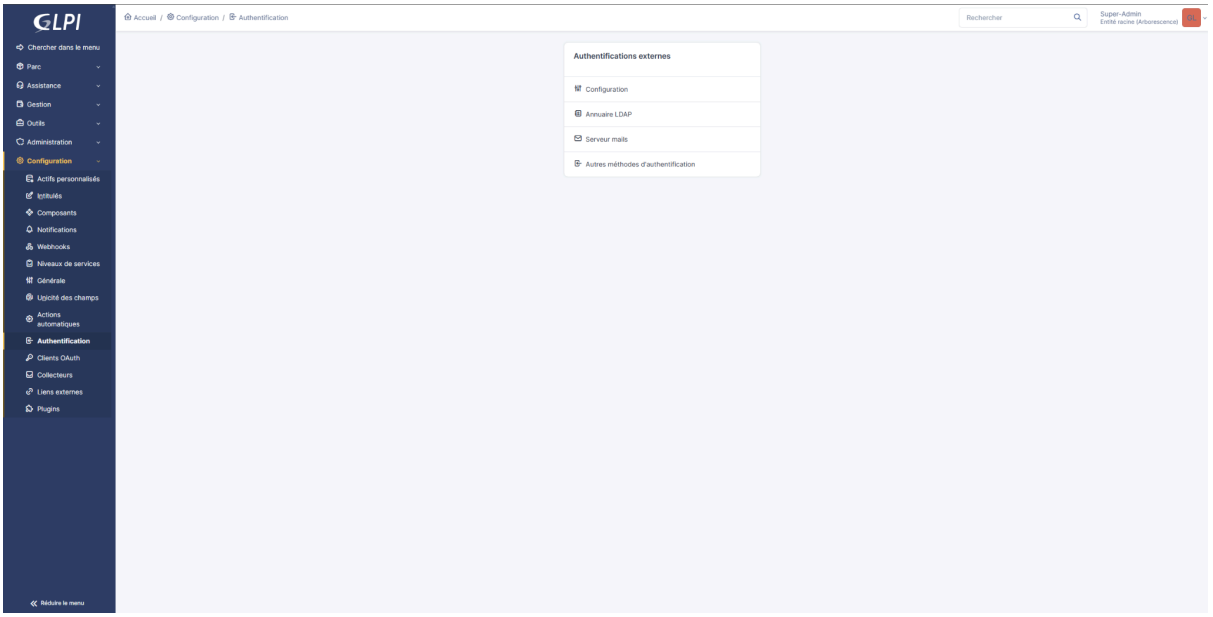


Ce sera via cet utilisateurs que GLPI se connectera sur notre AD et qu'il pourra importer nos utilisateurs présents dans nos Unité d'Organisation.

"Figure 3 : Création de l'utilisateur LDAP dans Active Directory avec définition du mot de passe."

Pour l'étape suivante, nous pouvons retourner sur notre GLPI en nous connectant en **super-admin** avec le compte par défaut glpi/glpi.

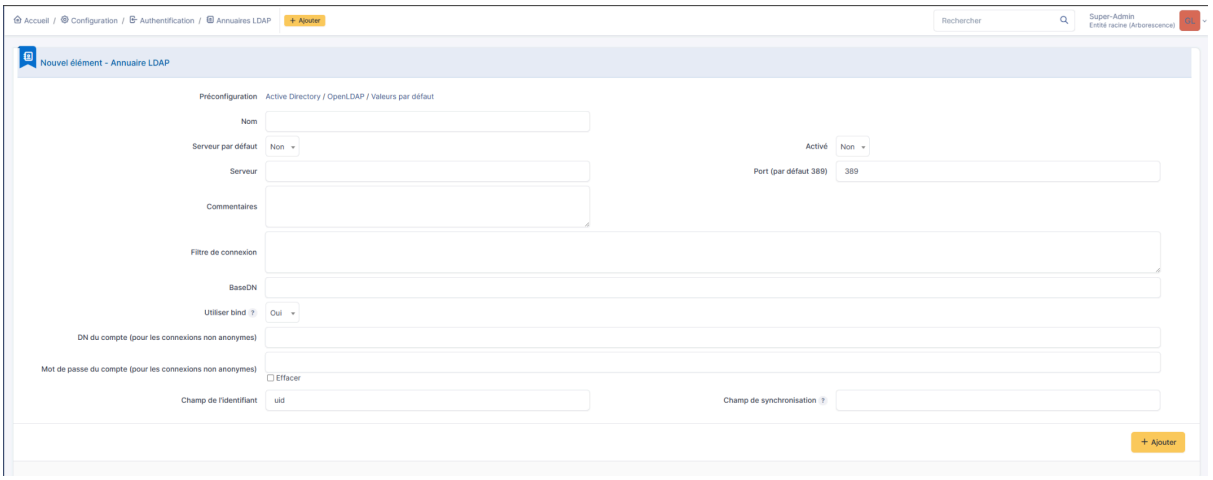
Ensuite, rendez-vous dans le menu **Configuration > Authentification**.



"Figure 4 : Accès au menu Configuration > Authentification depuis l'interface GLPI en super-admin."

Pour l'étape suivante, on retourne sur GLPI en se connectant avec le compte **super-admin** : `glpi/glpi`.

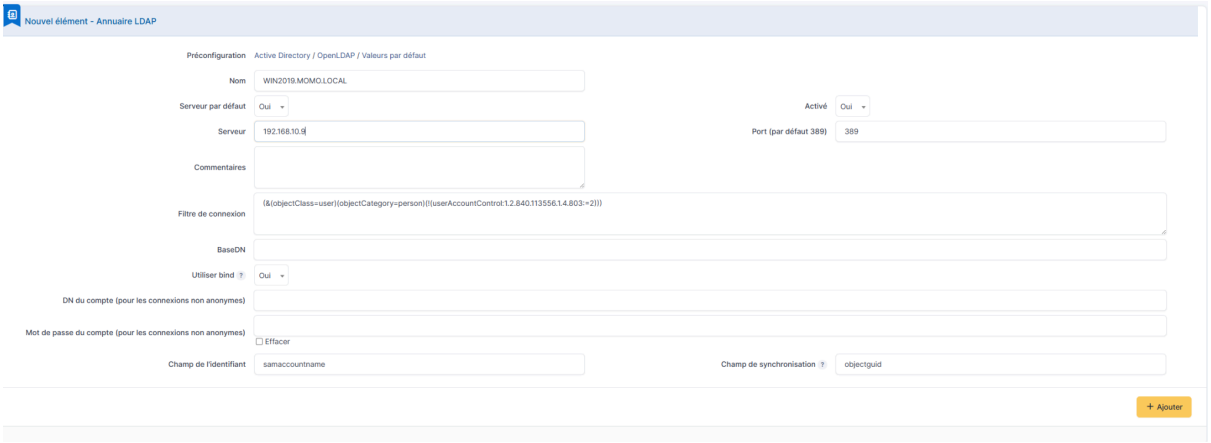
Ensuite, on se rend dans **Configuration > Authentification**, on clique sur + Ajouter et on va pouvoir identifier notre Annuaire AD



"Figure 4 : Accès au menu Configuration > Authentification dans l'interface GLPI en super-admin."

On peut alors cliquer sur **Active Directory** en bleu dans la case de préconfiguration. Cette option permet de pré-remplir les paramètres de base pour une liaison avec un annuaire AD.
Ensuite, on renseigne les premières informations du serveur hébergeant notre Active Directory :

- **Nom** : nom du serveur suivi du nom du domaine AD.
- **Serveur par défaut** : `Oui`.
- **Actif** : `Oui`.
- **Serveur** : adresse IP du serveur Windows.
- **Port** : `389` par défaut, correspondant au port LDAP standard.



"Figure 5 : Ajout d'un annuaire LDAP dans GLPI avec préconfiguration Active Directory et saisie des premiers paramètres de connexion."

Le BaseDN (Base Distinguished Name) doit correspondre au chemin complet et unique qui identifie l'emplacement exact du compte de service dans l'arborescence Active Directory, sous la forme :

- DC = Domain Component (composant du nom de domaine)
- OU = Organizational Unit (unité d'organisation)
- CN = Common Name (conteneur par défaut des utilisateurs)

Pour le domaine **`momo.local`**, chaque partie du nom de domaine devient un **`DC=`** :

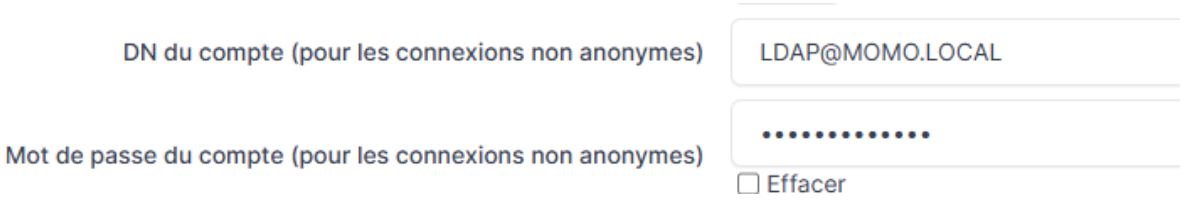
- **`momo`** → **`DC=momo`**
- **`local`** → **`DC=local`**

De ce fait, pour notre service direction la syntaxe de la BaseDN sera pour ma part :

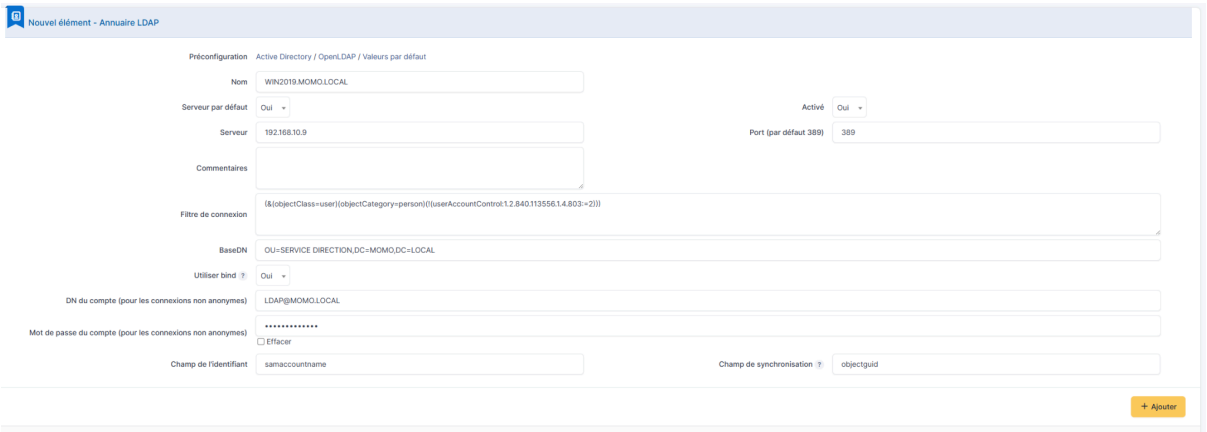


Le **DN du compte** correspond à l'identifiant complet du compte de service Active Directory utilisé par GLPI pour interroger l'annuaire LDAP.

Dans notre cas, ce rôle est attribué à l'utilisateur LDAP créé précédemment dans l'Active Directory.

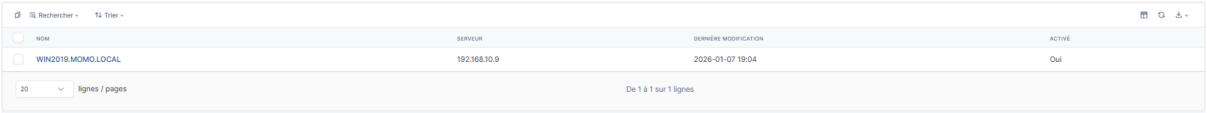


Une fois l'annuaire LDAP complété, on clique sur **Ajouter**. Voici à quoi ressemble le formulaire une fois renseigné :



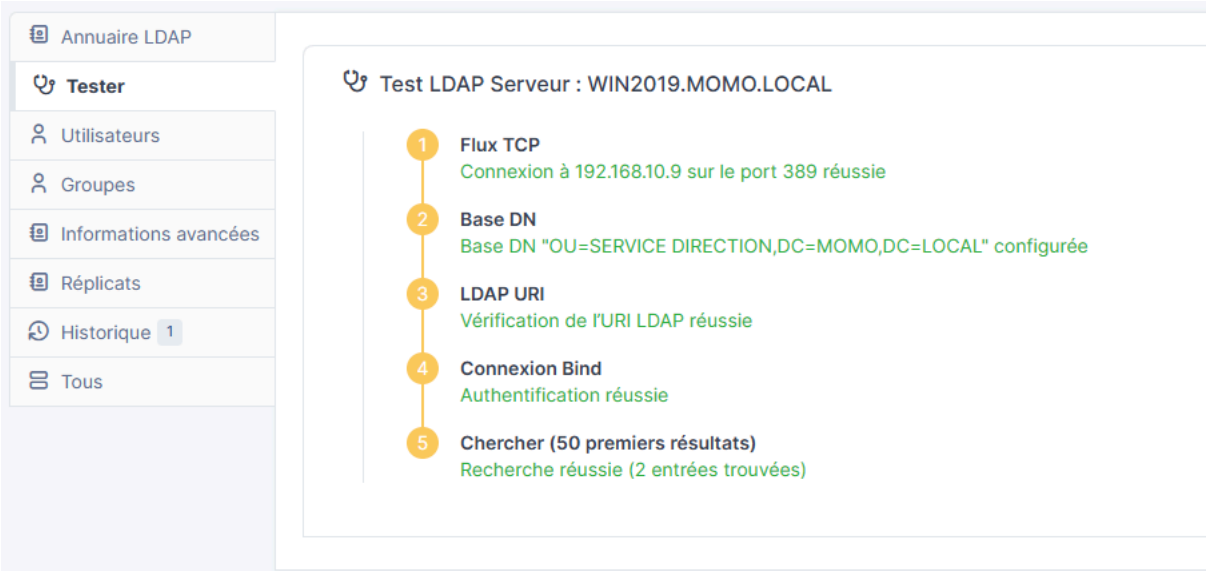
"Figure 6 : Configuration complète de l'annuaire LDAP dans GLPI avant ajout."

Si la configuration est correcte, on revient ensuite sur la page récapitulative qui confirme que l'annuaire LDAP a bien été ajouté :



"Figure 7 : Annuaires LDAP ajoutés avec succès dans GLPI."

Pour vérifier la connectivité avec le **Windows Server** et l'Active Directory, on peut cliquer sur l'annuaire puis sur **Tester**.
Si le message **Connexion réussie** s'affiche, cela confirme que le lien entre le serveur GLPI et l'Active Directory fonctionne correctement.



"Figure 8 : Test de connexion LDAP entre GLPI et l'Active Directory avec succès."

Si la connexion échoue, il faut vérifier qu'il n'y a pas d'erreur dans la configuration de l'annuaire LDAP.

Maintenant que le lien fonctionne, nous allons effectuer une première importation. Pour cela, il faut se rendre dans **Administration > Utilisateurs** dans le panneau de gauche.

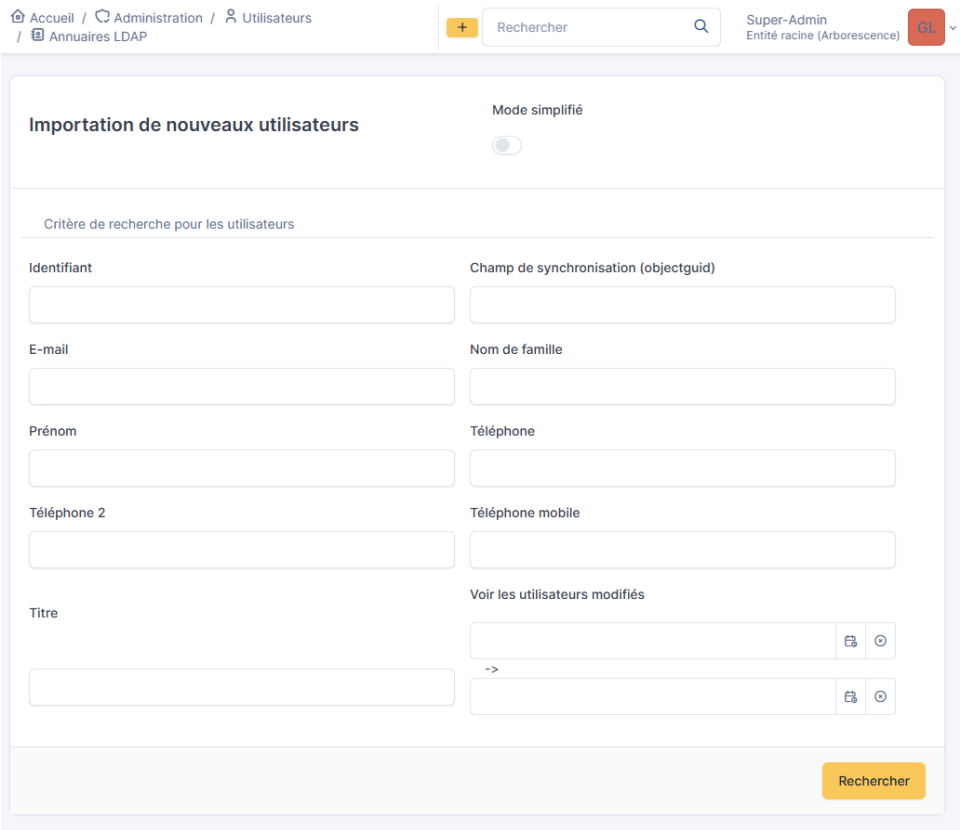


"Figure 9 : Accès au menu Administration > Utilisateurs dans GLPI."

Normalement, un bouton **Liaison annuaire LDAP** doit apparaître dans la zone **Actions**.
S'il est visible, il suffit de cliquer dessus. Sinon, il faut ajouter `/ldap.import.php` à l'URL, ce qui donnera :

```
text
http://[ton-ip-glpi]/front/ldap.import.php
```

Cela vous amène à la page d'**importation de nouveaux utilisateurs** depuis l'annuaire LDAP.

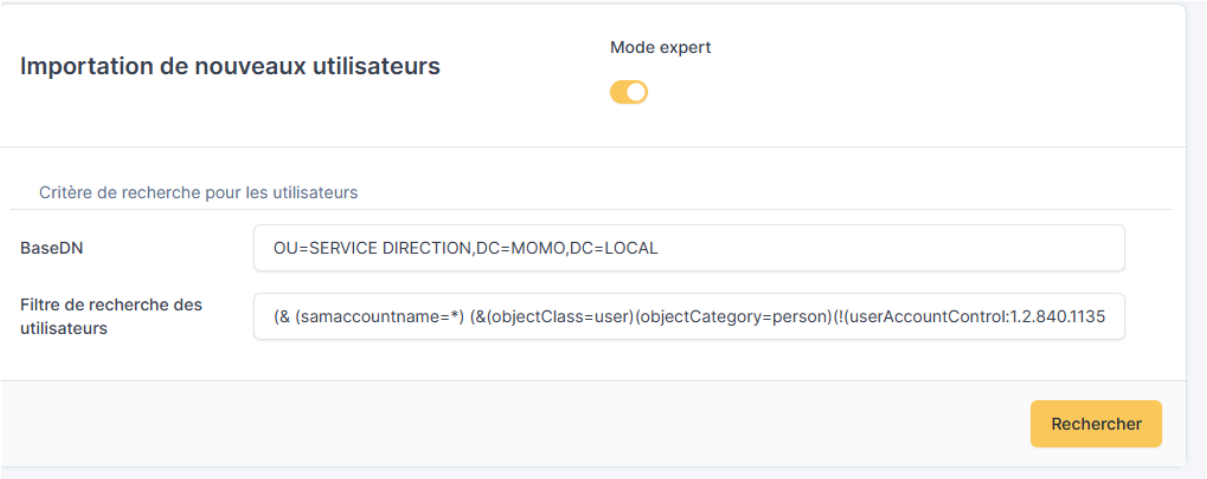


"Figure 10 : Page d'importation des nouveaux utilisateurs LDAP dans GLPI."

Vous pouvez cliquer sur **Mode simplifié** pour passer en **mode expert**, puisque toute la configuration nécessaire a déjà été réalisée.

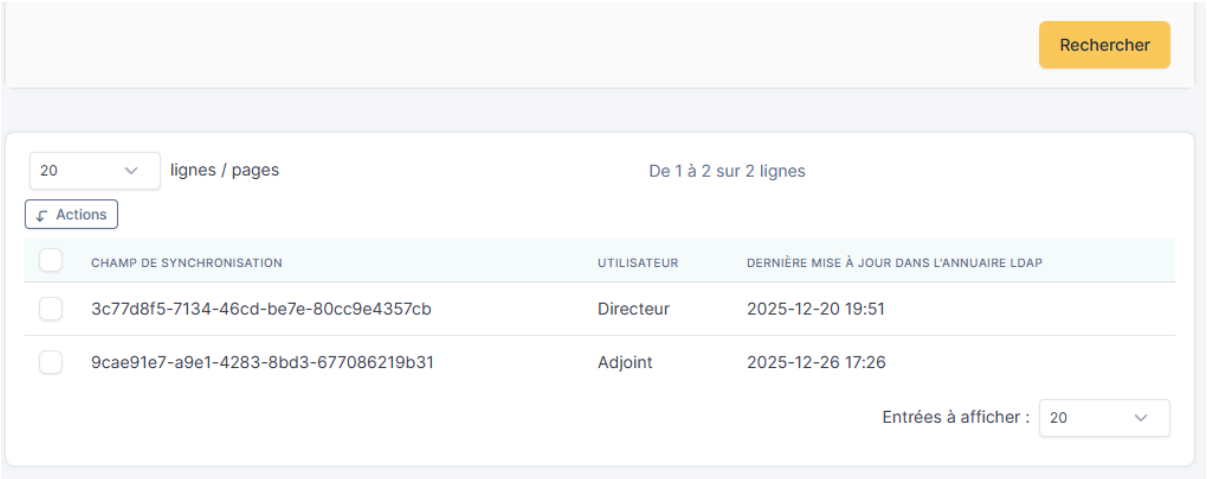
Dans ce mode, GLPI affiche notamment :

- le **BaseDN** utilisé pour la recherche ;
- le **filtre de recherche** des utilisateurs LDAP.



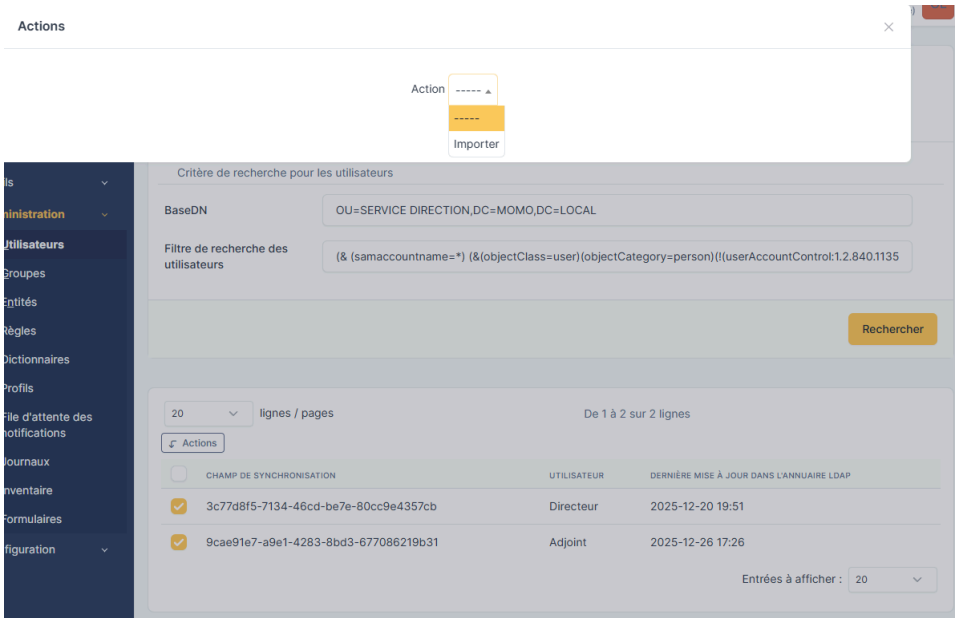
"Figure 11 : Passage en mode expert avec affichage du BaseDN et du filtre LDAP."

En cliquant sur **Rechercher**, GLPI retrouve bien les deux utilisateurs présents dans l'unité d'organisation **Service Direction** :



"Figure 12 : Résultat de la recherche LDAP affichant les utilisateurs Directeur et Adjoint."

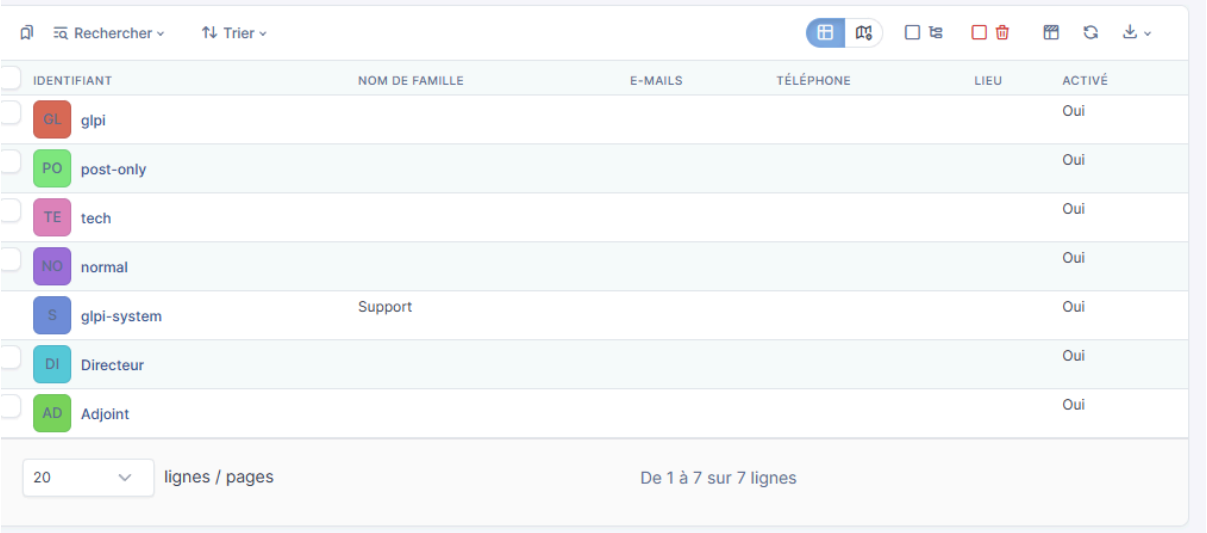
Il suffit ensuite de cocher les deux utilisateurs, puis d'ouvrir le menu **Action** et de choisir **Importer**.
Après avoir cliqué sur **Envoyer**, un message de confirmation apparaît en bas à droite pour indiquer que l'opération s'est déroulée avec succès.





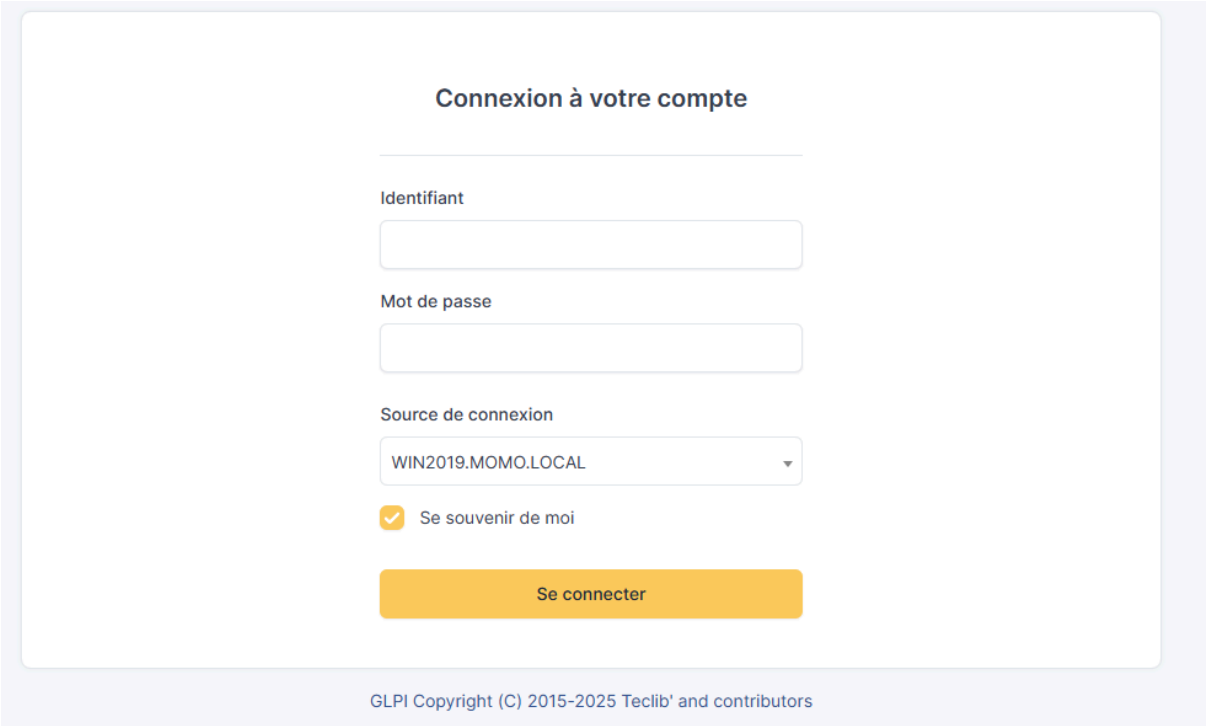
"Figure 13 : Importation des utilisateurs LDAP Directeur et Adjoint dans GLPI."

Les utilisateurs **Directeur** et **Adjoint** sont maintenant présents dans la liste des utilisateurs GLPI.



"Figure 14 : Utilisateurs LDAP importés et visibles dans la liste des comptes GLPI."

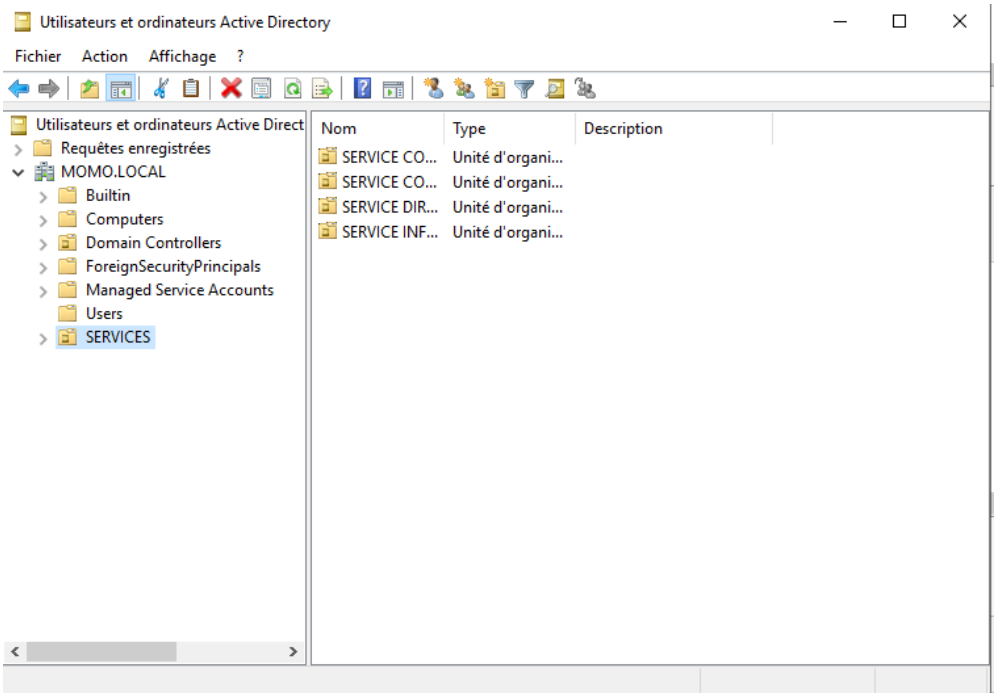
Après la déconnexion du compte **Super-Admin**, l'écran de connexion GLPI affiche désormais une nouvelle source d'authentification : le **Windows Server** ajouté précédemment.



"Figure 15 : Écran de connexion GLPI avec sélection de la source LDAP Active Directory."

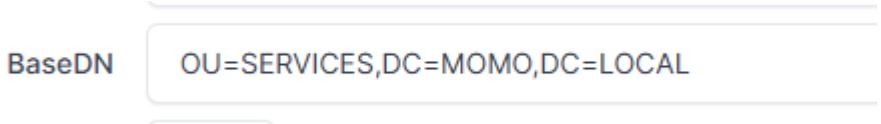
Grâce à cette source de connexion, il est possible de s'authentifier avec les comptes **Directeur** et **Adjoint** issus de l'Active Directory.

Pour éviter de devoir importer les utilisateurs une par une, il est possible de créer une unité d'organisation plus globale dans le contrôleur de domaine Windows, afin de regrouper plusieurs services au même endroit.



"Figure 16 : Création d'une unité d'organisation globale dans Active Directory pour regrouper plusieurs services."

Ensuite, il faut retourner dans GLPI en tant que **super-admin** pour modifier le **BaseDN** et le faire pointer vers cette nouvelle unité d'organisation qui regroupe l'ensemble des services.



"Figure 17 : Modification du BaseDN dans GLPI pour pointer vers l'unité d'organisation globale."



L'import d'une de nos unités d'organisation Active Directory dans GLPI est désormais opérationnelle. Les comptes utilisateurs ont bien été créés et peuvent maintenant se connecter à GLPI avec leurs identifiants AD, ce qui centralise l'authentification et simplifie la gestion des accès.

Conclusion du Chapitre

Ce chapitre a permis d'intégrer l'Active Directory au sein de GLPI pour centraliser l'authentification des utilisateurs et éviter la gestion manuelle des comptes.
La configuration de l'annuaire LDAP, la définition du **BaseDN** et du **DN du compte**, puis les tests de connexion ont validé la liaison entre GLPI et le contrôleur de domaine.

L'import des utilisateurs issus de l'unité d'organisation choisie s'est déroulé avec succès, ce qui permet désormais aux comptes AD de se connecter à GLPI avec leurs identifiants de domaine.
La mise en place d'une unité d'organisation plus globale améliore ensuite la gestion et facilite les imports futurs dans l'annuaire.

Cette intégration constitue une base solide pour la suite du projet, notamment pour la gestion des droits, des groupes et des prochaines étapes de l'administration GLPI.

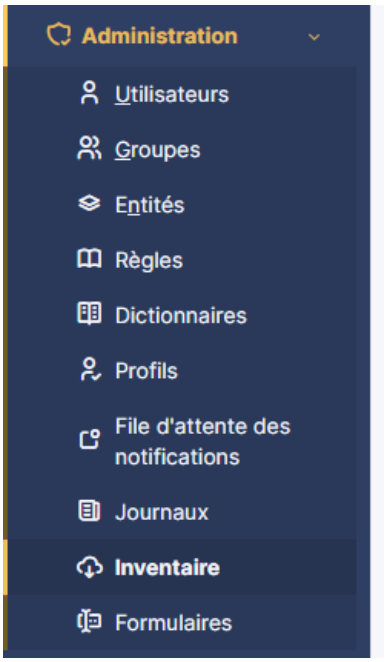
Fin du Chapitre 2.

Boumrah Samy

GLPI - Chapitre 3 :Remonter l'inventaire du Parc Info dans GLPI avec l'agent GLPI

Ce nouveau module a pour objectif de mettre en place une stratégie structurée d'inventaire du parc informatique en s'appuyant sur l'agent GLPI. L'enjeu est de disposer d'une vision centralisée, fiable et à jour de l'ensemble des postes, serveurs et périphériques, afin de mieux gérer les équipements, anticiper les besoins et sécuriser l'infrastructure.

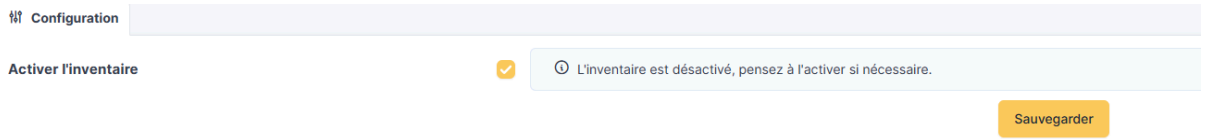
À travers la configuration de l'agent GLPI et la définition de règles claires de recensement, ce module permettra d'automatiser la remontée des informations techniques, de standardiser le suivi du matériel et de poser les bases d'une gestion professionnelle du parc.



Avant toute chose, il faut se rendre sur GLPI, se connecter en **super-admin**, puis aller dans **Administration > Inventaire**.

"Figure 1 : Accès au menu Administration > Inventaire depuis l'interface GLPI en super-admin."

Pour cocher la case **« Activer l'inventaire »**, qui n'est pas cochée par défaut, il faut se rendre dans le menu **Administration > Inventaire**.



"Figure 2 : Activation de l'inventaire dans GLPI depuis le menu Administration > Inventaire."

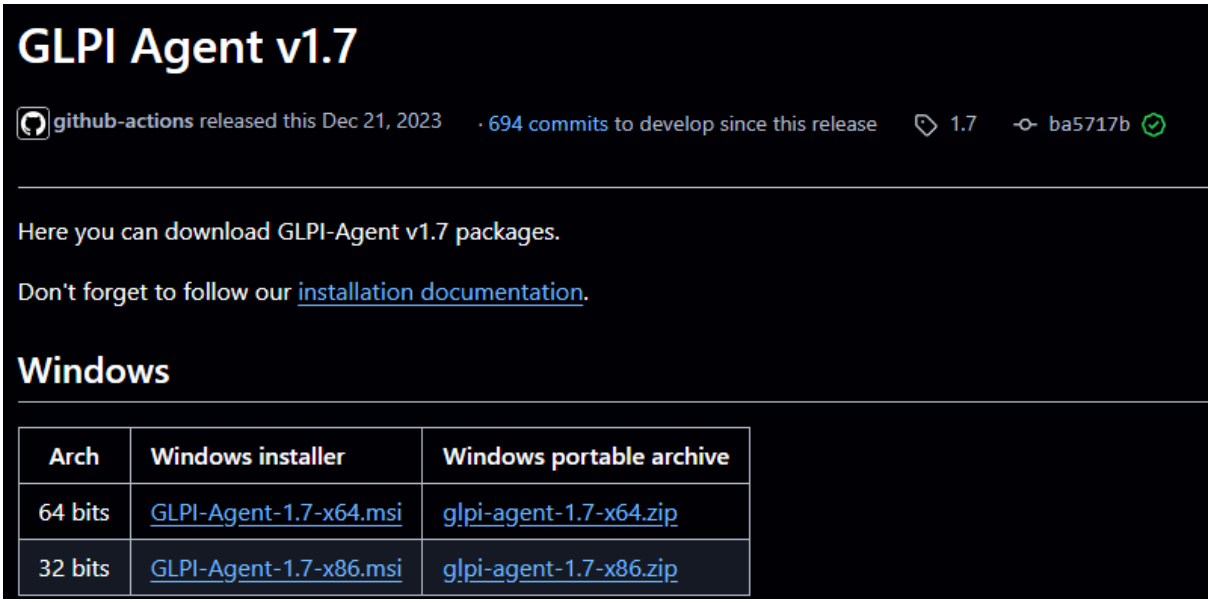
Pour déployer l'agent GLPI, il faut d'abord le télécharger sur le **Windows Server**.

Dans l'explorateur, on recherche **GLPI Agent**, puis on accède au lien GitHub correspondant afin de récupérer l'installateur.

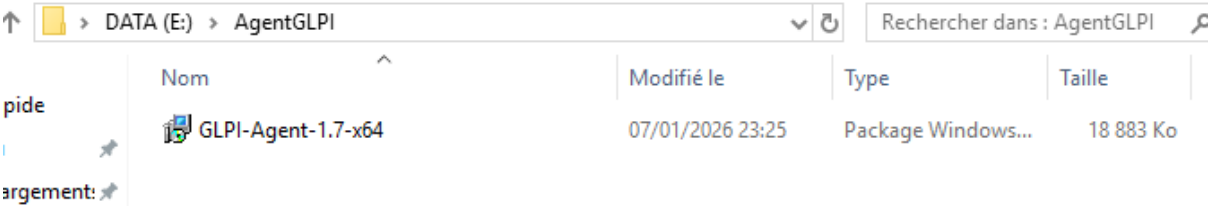


"Figure 3 : Téléchargement de l'agent GLPI depuis la page GitHub officielle."

On installe la version **MSI Installer 64 bits**.

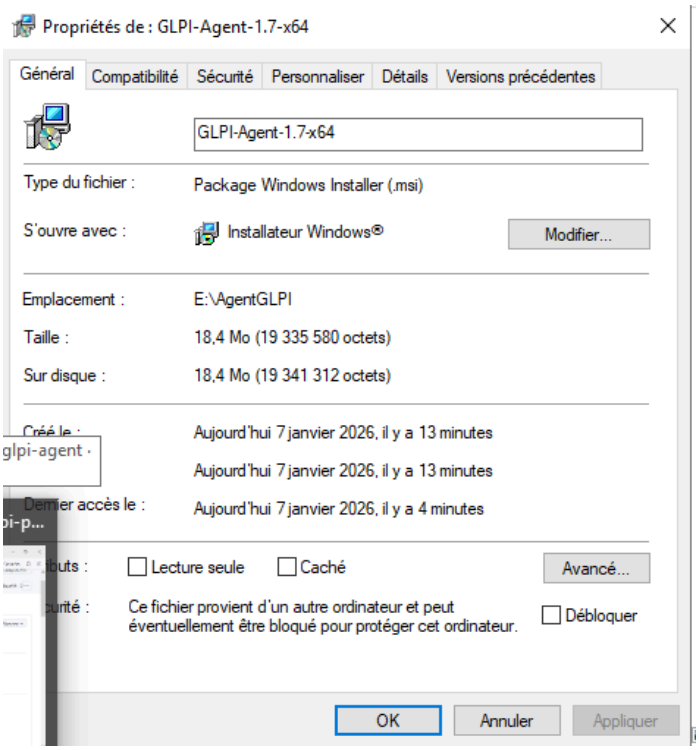


Ensuite, on déplace l'installateur dans un dossier créé à cet effet, nommé **AgentGLPI**, sur le disque **DATA (E:)**.



"Figure 4 : Déplacement de l'installateur GLPI Agent dans le dossier AgentGLPI du disque DATA (E:)."

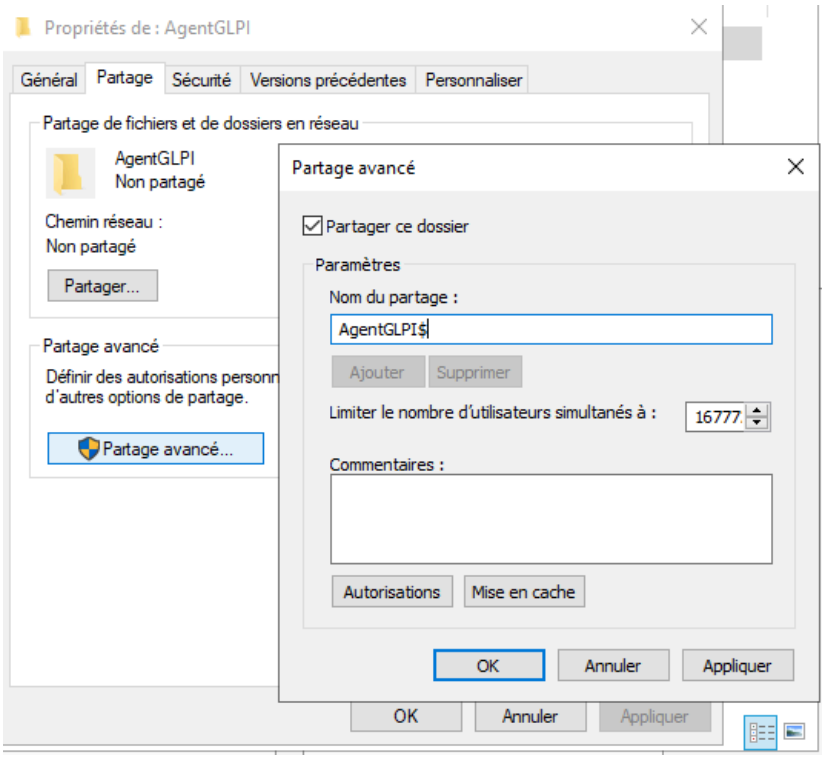
Il est ensuite important de vérifier que l'installation pourra se faire correctement et silencieusement sur les machines cibles.



Pour cela, on fait un clic droit sur le fichier **GLPI-Agent-1.7-x64**, puis on ouvre les **Propriétés** afin de cocher la case permettant de **débloquer le fichier**, située en bas à droite.

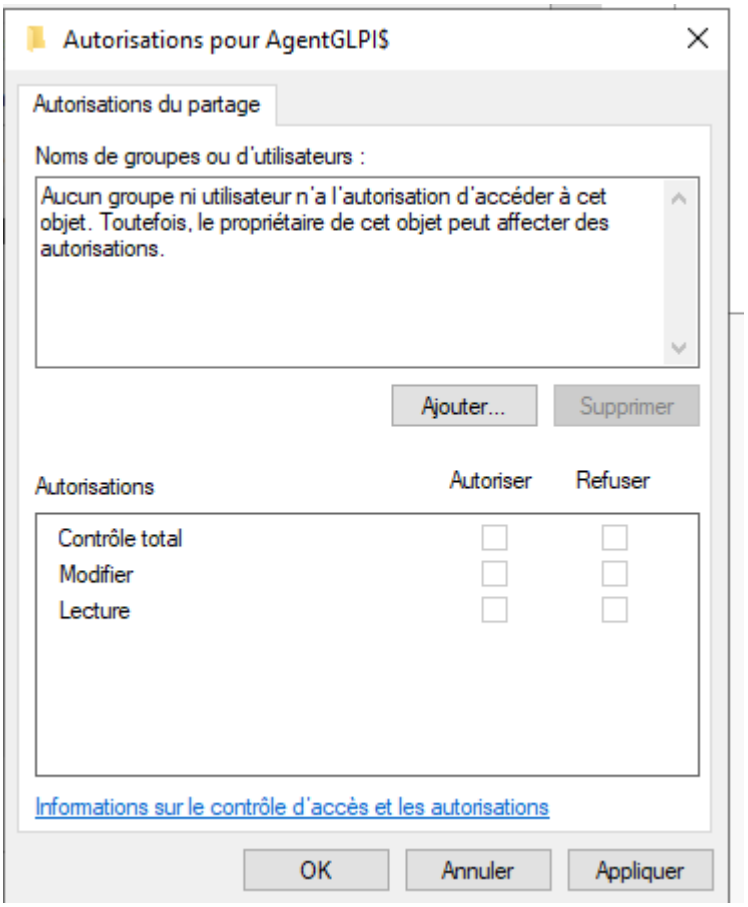
Une fois le fichier débloqué, on clique sur **Appliquer** puis sur **OK**.

Ensuite, on retourne dans le dossier **AgentGLPI** et on active le partage du répertoire.
Pour cela, on fait un clic droit sur le dossier, puis on suit le chemin : **Propriétés > Partage > Partage avancé**.
On coche ensuite la case **Partager ce dossier** et on donne un nom au partage.



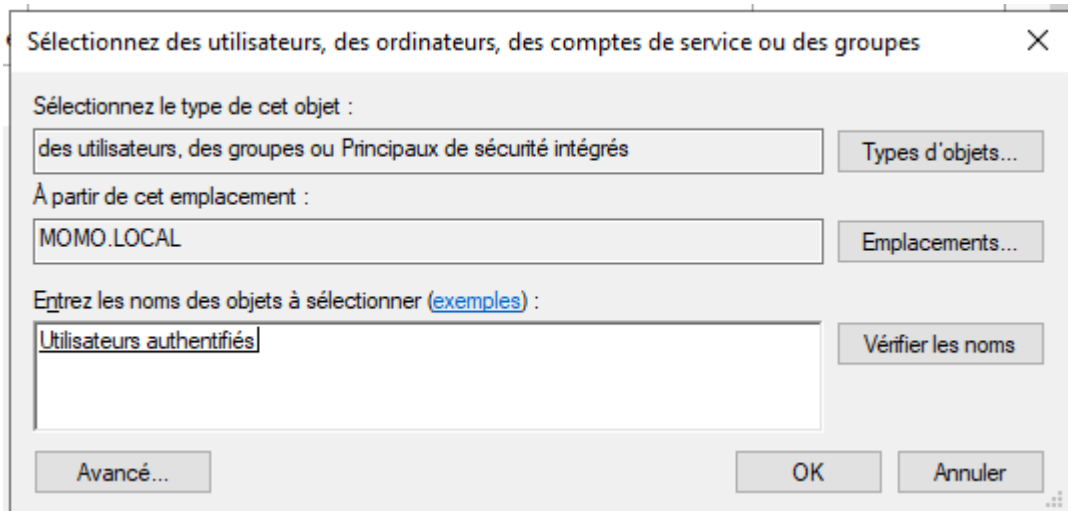
"Figure 5 : Activation du partage avancé du dossier AgentGLPI et définition du nom de partage."

Ensuite, on se rend dans **Autorisations**. Dans la liste située sous la fenêtre de commentaire, on supprime les groupes déjà présents, puis on clique sur **Ajouter**.



"Figure 6 : Gestion des autorisations du partage du dossier AgentGLPI."

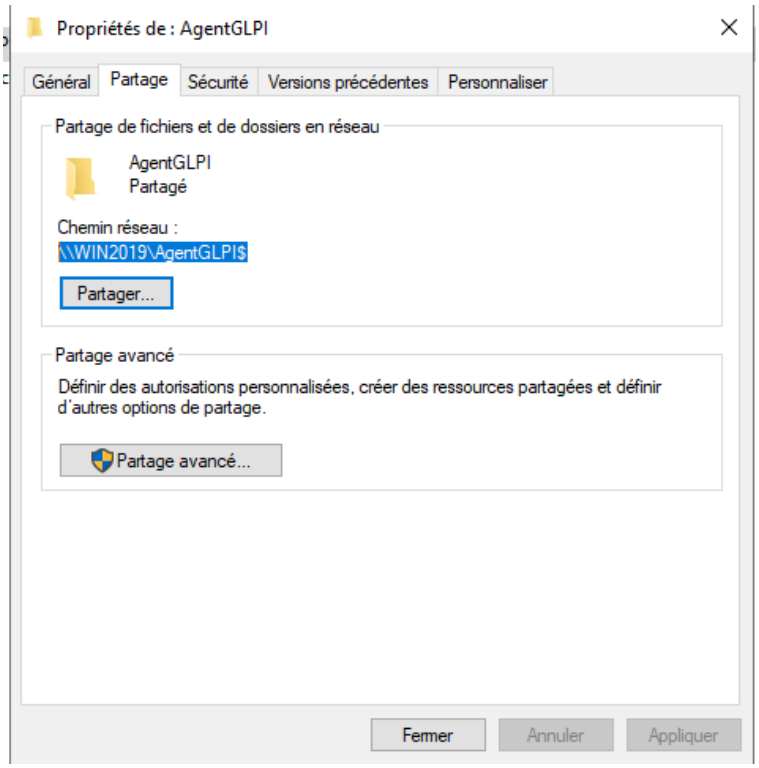
On renseigne ensuite le groupe **Utilisateurs authentifiés**.



"Figure 7 : Ajout du groupe Utilisateurs authentifiés dans les permissions du partage."

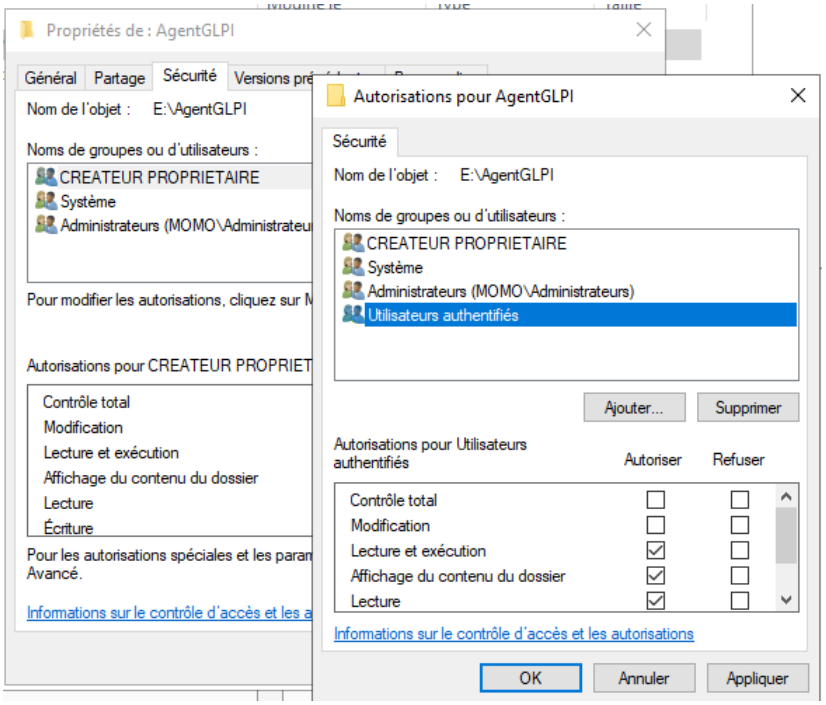
Une fois le groupe ajouté, il suffit de cliquer sur **OK**.
Le droit de lecture étant suffisant, on peut ensuite appliquer la configuration puis valider avec **OK**.

On peut garder en mémoire le chemin réseau qui nous servira plus tard.



"Figure 8 : Chemin réseau du dossier AgentGLPI à conserver pour la suite de la configuration."

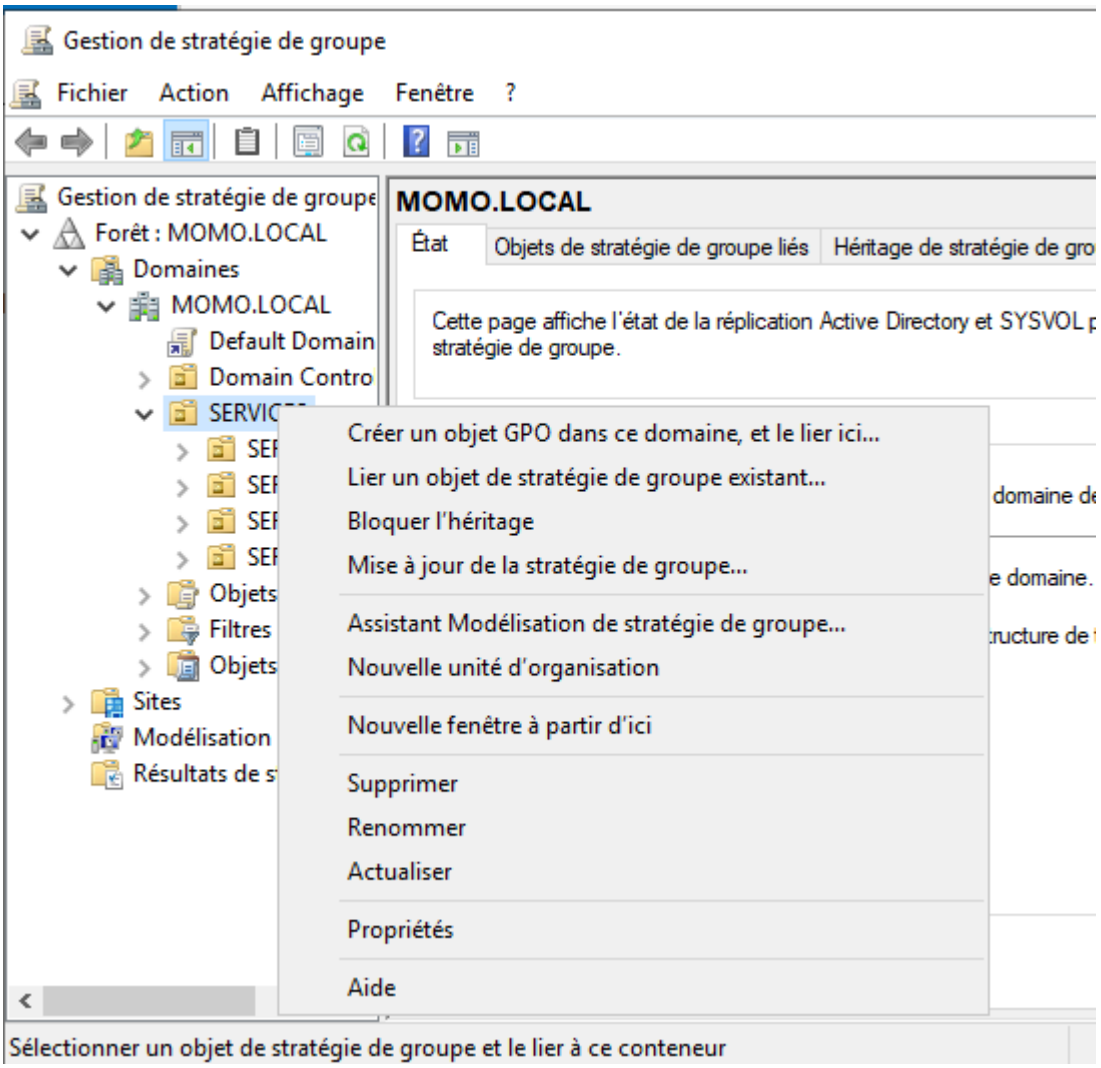
Ensuite, on se rend dans l'onglet **Sécurité**.
On y ajoute également le groupe **Utilisateurs authentifiés**. Il n'est pas nécessaire de modifier ses droits : on peut simplement appliquer la configuration puis valider avec **OK**.



"Figure 9 : Ajout du groupe Utilisateurs authentifiés dans les permissions de sécurité du dossier AgentGLPI."

Désormais, le dossier de partage est prêt.
On peut donc passer à la suite de la configuration et se rendre dans la gestion des stratégies de groupe du gestionnaire de serveur.

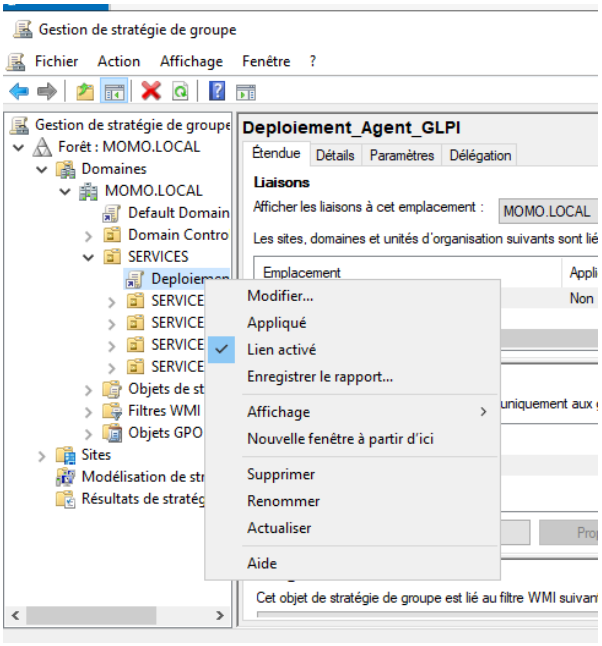
Ensuite, on fait un clic droit sur l'**Unité d'organisation** visée, ici **SERVICES**, afin d'y regrouper les autres services.



"Figure 10 : Création d'un nouvel objet GPO lié à l'unité d'organisation SERVICES."

On choisit alors **Créer un objet GPO dans ce domaine et le lier ici**, puis on donne un nom à l'objet.
Une fois le GPO créé, on fait un clic droit dessus et on sélectionne **Modifier**.

On peut ensuite ouvrir le GPO **Deploiement_Agent_GLPI** dans l'éditeur pour préparer la configuration.



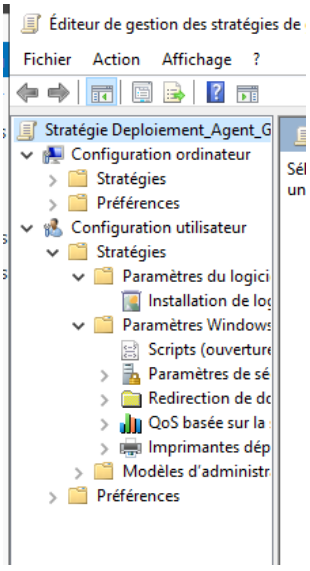
"Figure 11 : Accès au GPO Deploiement_Agent_GLPI depuis la console de gestion des stratégies de groupe."

Dans l'éditeur, on repère les deux volets à déployer dans la configuration utilisateur :

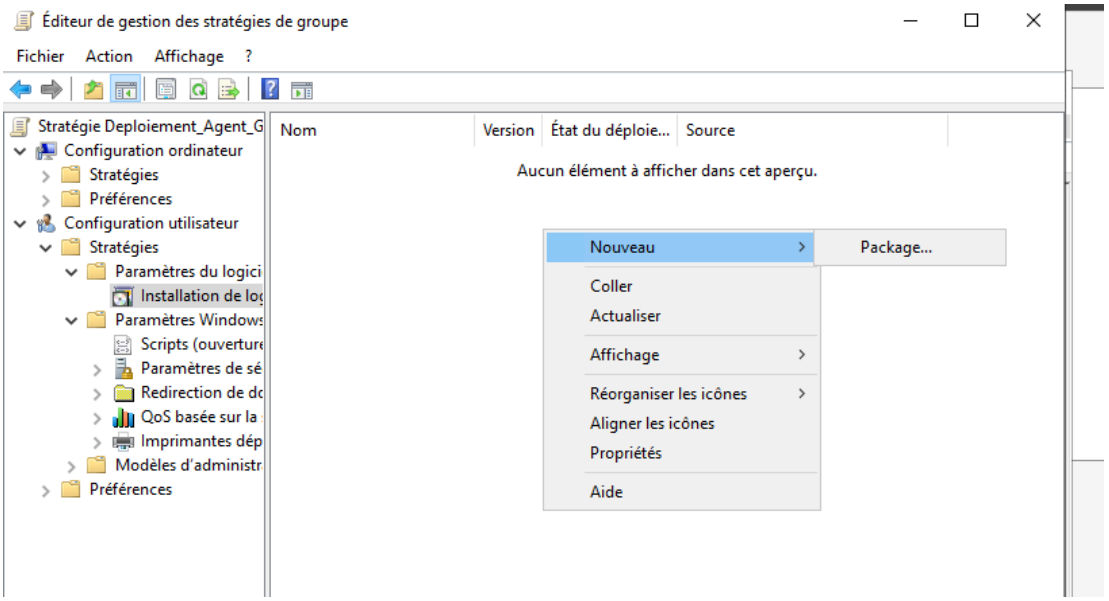
- **Paramètres du logiciel**.
- **Paramètres Windows**.

Ces deux sections serviront ensuite à définir la stratégie de déploiement du package.

On va se rendre sur Installation du Logiciel dans le volet "Paramètres du logiciel" puis clique droit dans la zone blanche => Nouveau => Package



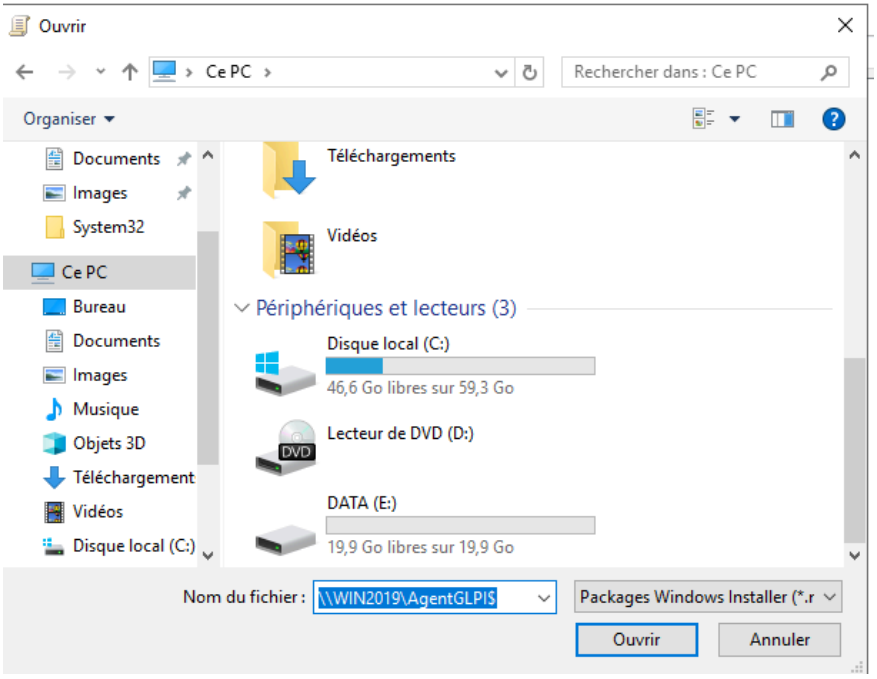
Il faut ensuite créer un nouveau package dans **Paramètres du logiciel > Installation de logiciels**.



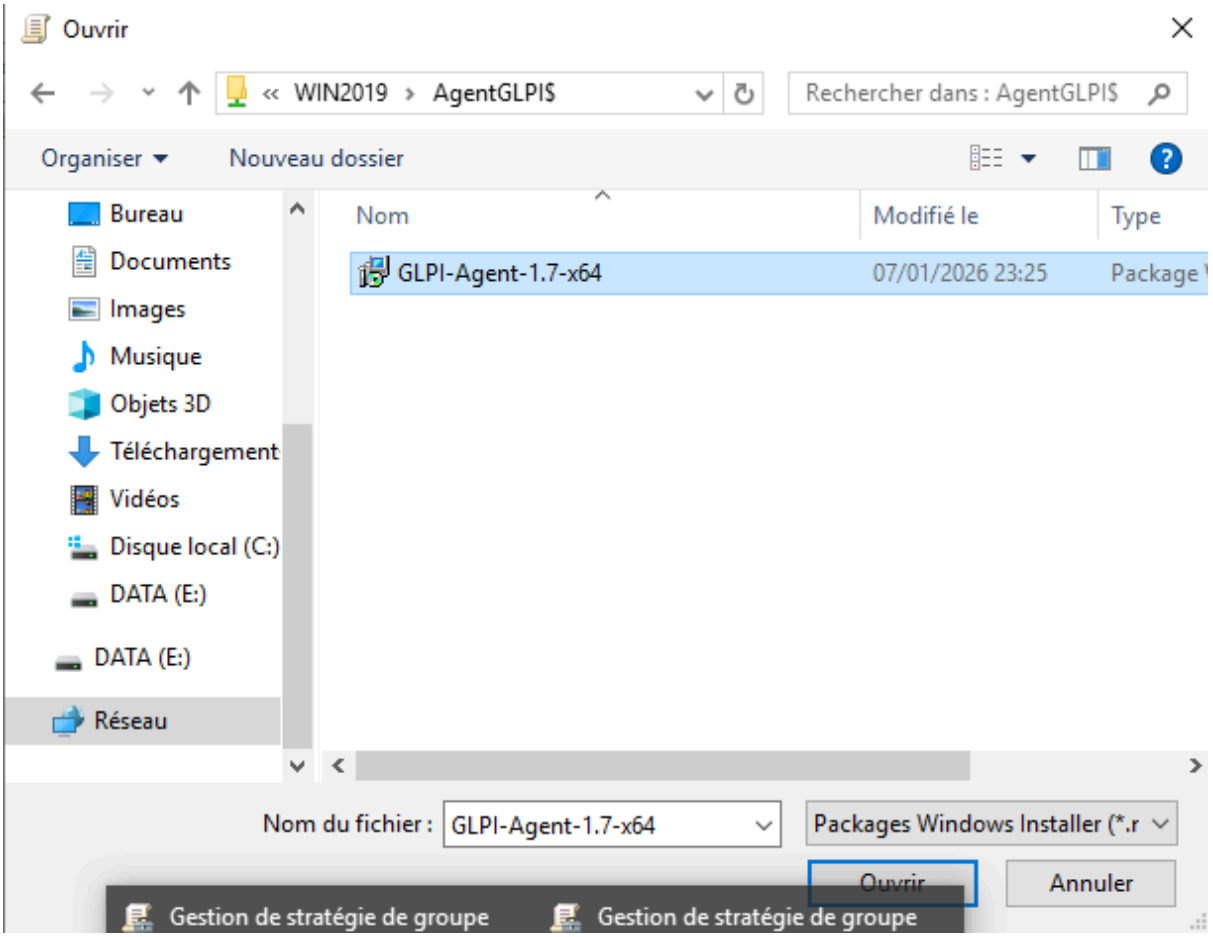
"Figure 12 : Création d'un nouveau package MSI dans les paramètres du logiciel du GPO."

Point important : on ne doit pas chercher l'agent via un chemin absolu dans l'explorateur de fichiers.
On utilise plutôt le **chemin réseau** défini précédemment, celui qu'on a gardé en mémoire pendant le partage du dossier.

Dans la fenêtre d'ouverture du fichier, il suffit donc de saisir le chemin réseau du dossier **AgentGLPI** et de sélectionner le package MSI correspondant.



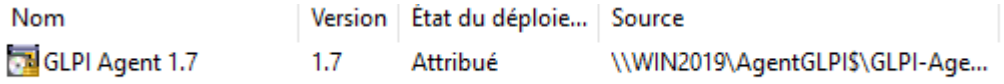
Après avoir collé le **chemin réseau**, on ouvre le dossier puis on sélectionne le package **GLPI-Agent-1.7-x64** et on clique sur **Ouvrir**.



"Figure 13 : Sélection du package MSI GLPI-Agent-1.7-x64 depuis le partage réseau."

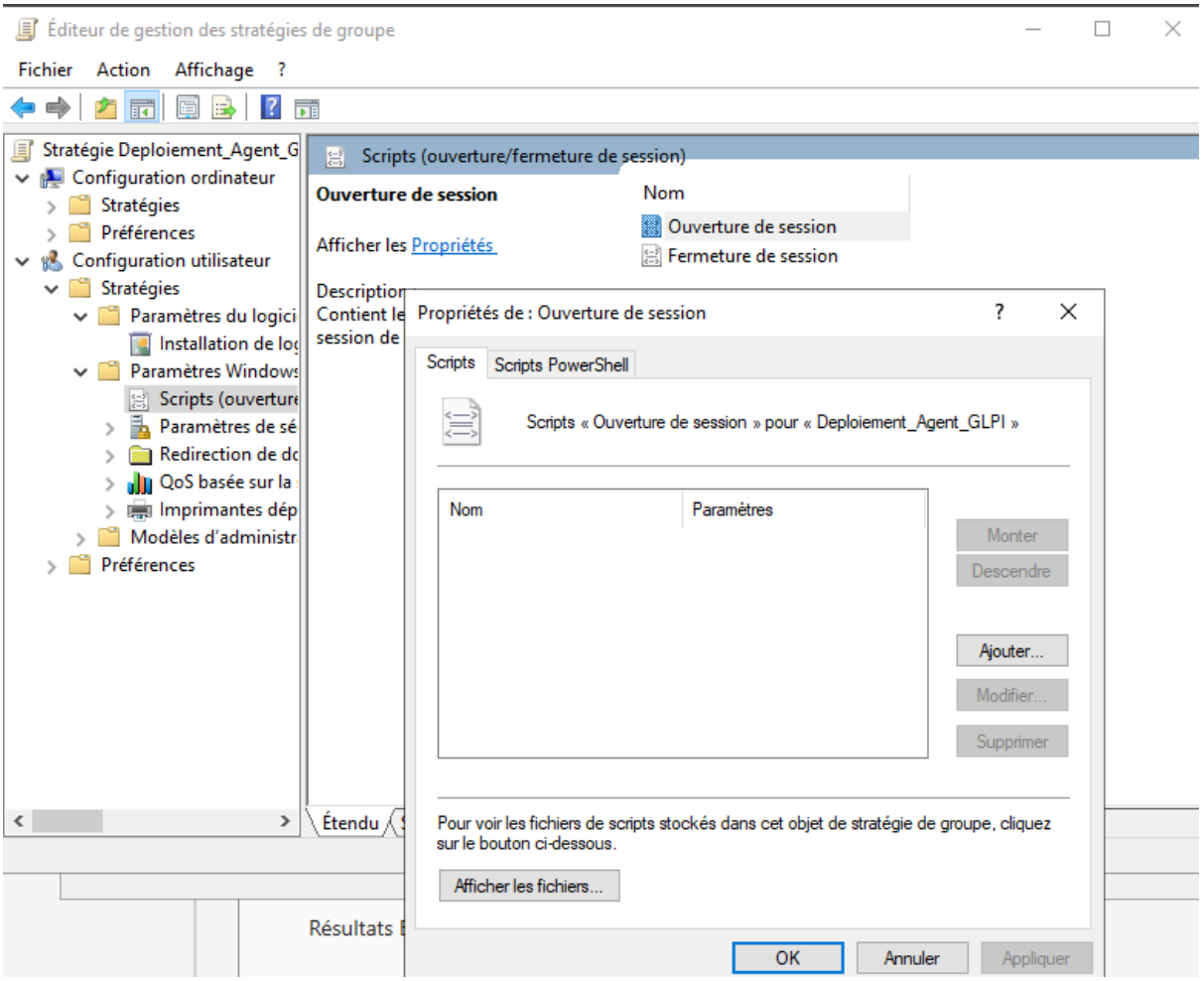
À l'étape suivante, on choisit le mode de déploiement du package.
Il faut cocher **Attribué**, ce qui permet un déploiement automatique sans validation de l'utilisateur, puis valider avec **OK**.

Le package apparaît alors dans la liste des installations de logiciels.
Il faut vérifier que la source correspond bien au **chemin réseau** récupéré dans les propriétés de partage.



Ensuite, on met en place un **script d'ouverture de session** pour que le package soit lancé à la connexion au domaine.

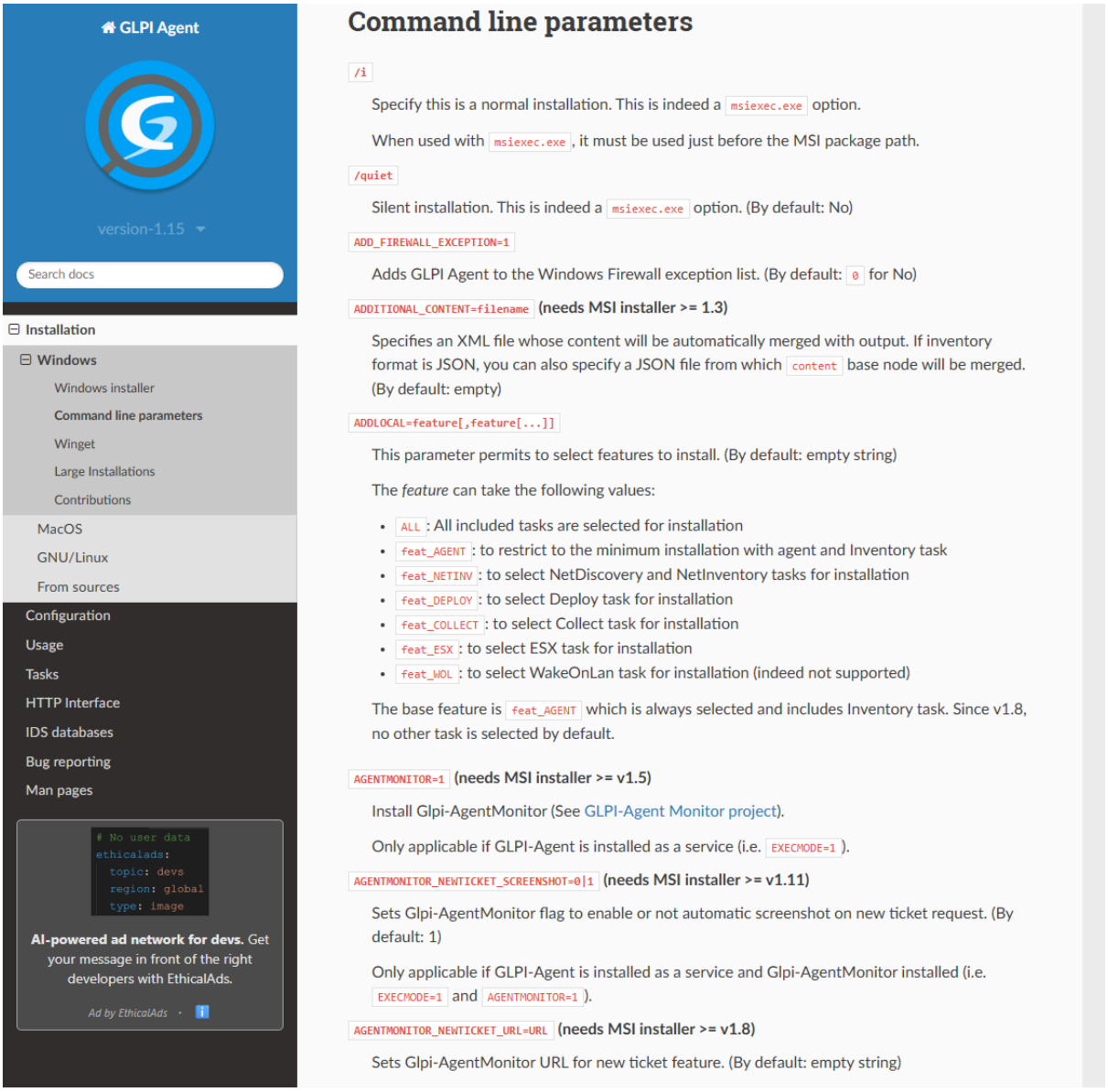
On se rend ensuite dans **Scripts > Ouverture de session** pour ajouter le script de lancement.



"Figure 14 : Configuration du script d'ouverture de session dans le GPO Déploiement_Agent_GLPI."

On clique sur **Ajouter** et on renseigne le nom**msiexec.exe**.
Ce nom est obligatoire : c'est l'exécutable qui permettra de lancer l'installation du package défini dans **Installation de logiciels**.

Ensuite, on complète les paramètres du script afin d'appeler correctement le package au démarrage de session.
Les paramètres peuvent ensuite être récupérés depuis la page web de l'agent GLPI.



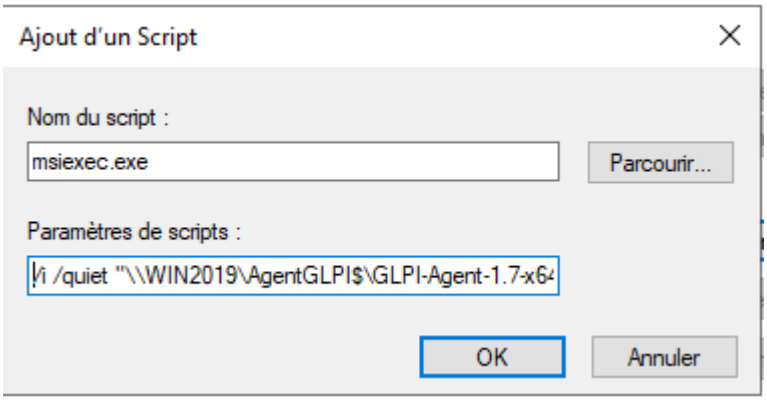
"Figure 15 : Paramètres de ligne de commande pour l'installation silencieuse de GLPI Agent."

Les paramètres à utiliser sont donc :

- **/i**.
- **/quiet**.

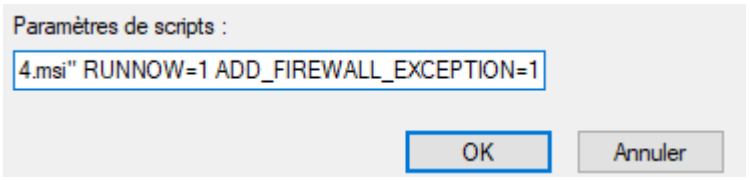
Il faut ensuite ajouter le chemin réseau entre guillemets, suivi du nom du package : **GLPI-Agent-1.7-x64.msi**.

La commande complète doit donc lancer une installation silencieuse du MSI depuis le partage réseau, ce qui permet au déploiement de se faire automatiquement à la connexion.



On ajoute alors les paramètres complémentaires à la commande.

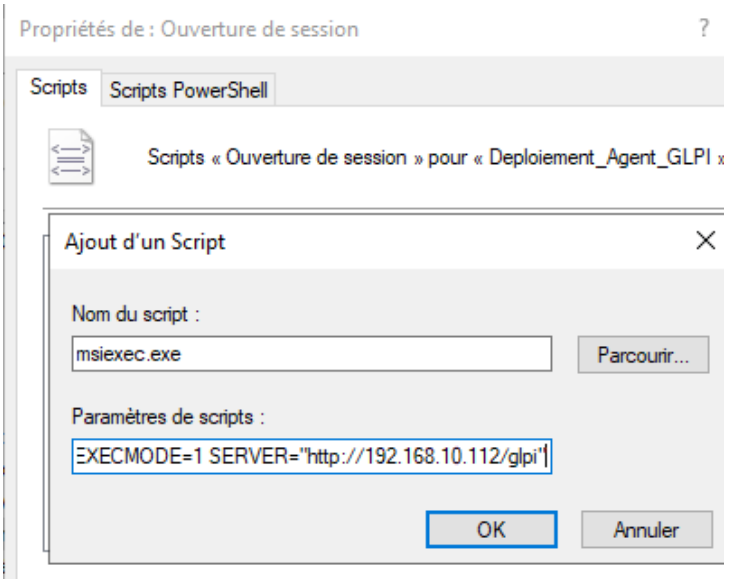
Puis espace RUNNOW=1 qui signifie que l'agent GLPI sera directement lancé après son installation espace une autre règle qui fera office d'omission du firewall pendant l'exécution de GLPI, autorisant une sorte d'ouverture au niveau du parefeu



"Figure 16 : Ajout des paramètres Runnow, Add Firewall Exception et ExecMode dans le script de déploiement."

Les paramètres sont les suivants :

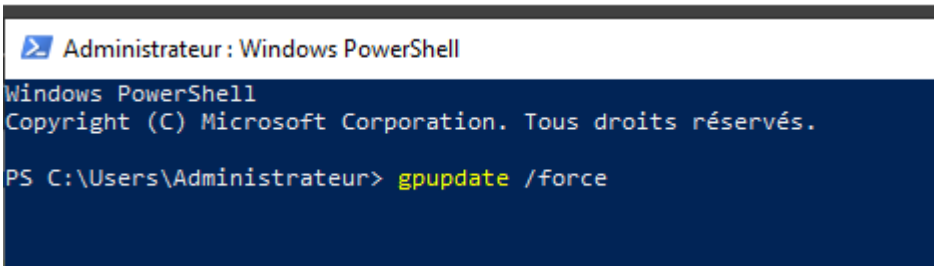
- **RUNNOW=1**, pour lancer immédiatement l'agent GLPI après son installation.
- **ADD_FIREWALL_EXCEPTION=1**, pour créer une exception de pare-feu pendant l'exécution.
- **EXECMODE=1**, pour exécuter l'agent sur la machine cliente en tant que service.
- **SERVER=http://192.168.10.112/glpi**, pour envoyer les données vers le serveur GLPI.



La commande finale combine donc le lancement du MSI avec ces options, ce qui automatise l'installation, l'exécution du service et la remontée des informations vers le serveur.

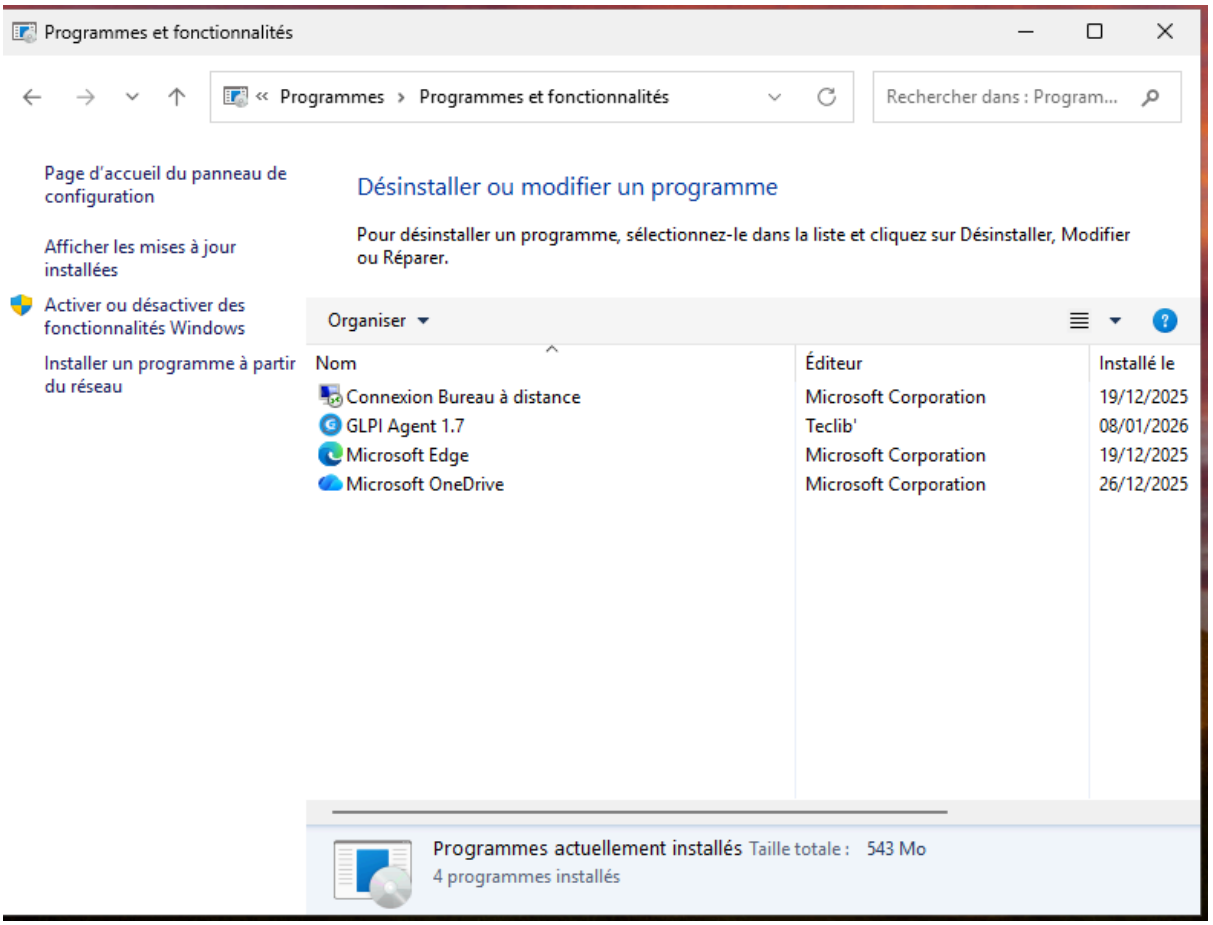
Une fois les paramètres validés, on clique sur **OK**.

Tout est alors configuré, et il ne reste plus qu'à ouvrir **PowerShell** pour lancer la commande **gpupdate /force** afin d'appliquer immédiatement la stratégie de groupe.



Ensuite, on peut se connecter sur la machine Windows 11 avec un compte utilisateur pour vérifier que le déploiement s'exécute correctement.

Dans **Programmes et fonctionnalités**, on doit voir apparaître **GLPI Agent 1.7** installé, ce qui confirme que la stratégie de déploiement fonctionne.



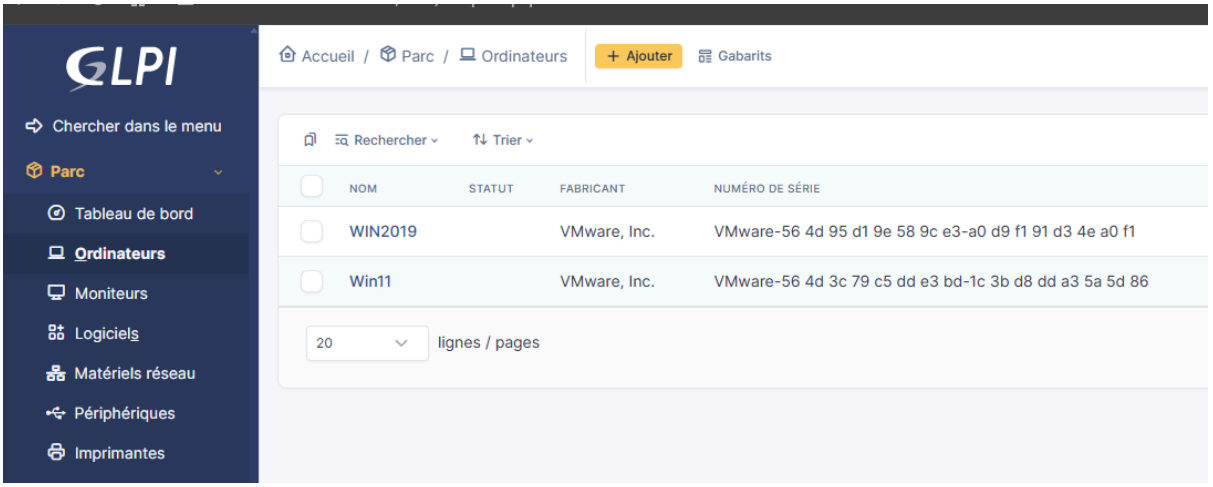
Si l'installation silencieuse ne s'est pas faite automatiquement, il faut vérifier les paramètres du GPO ainsi que les autorisations de partage du dossier.

On peut aussi contrôler que l'inventaire remonte bien dans **GLPI** en se connectant en **super-admin** pour administrer le parc informatique.



Sur le tableau de bord, on voit que les logiciels et les ordinateurs ont bien été répertoriés dans le parc.

Dans l'onglet **Ordinateurs**, les machines du domaine apparaissent, ce qui confirme que la remontée fonctionne correctement.



Conclusion du chapitre

Ce chapitre a permis de mettre en place le déploiement automatique de l'agent GLPI via une stratégie de groupe. Après le partage du dossier, la création du GPO et la configuration du script de connexion, l'installation a pu être automatisée sur les postes du domaine.

La vérification finale dans GLPI confirme que les ordinateurs et les logiciels remontent correctement dans l'inventaire. Le parc informatique est donc bien centralisé et administrable depuis la console GLPI, ce qui valide le bon fonctionnement de la solution..

Fin du chapitre 3.