

GPLI & Authentication LDAP

ESICAD – SIO1

CUENCA Teva

INTRODUCTION :

Ce rapport présente la procédure d'authentification des utilisateurs Active Directory (AD) sur GLPI (Gestionnaire Libre de Parc Informatique) via le protocole LDAP. L'objectif de ce projet est de centraliser et simplifier la gestion des accès des utilisateurs en intégrant AD avec GLPI.

Active Directory, couramment utilisé pour administrer les droits et les identités des utilisateurs dans un réseau, permet de sécuriser les informations d'identification. L'utilisation du protocole LDAP (Lightweight Directory Access Protocol) pour cette intégration assure une communication standardisée et efficace entre AD et GLPI.

CAHIER DES CHARGES :

Le but de cette réalisation, est de mettre en place GLPI et mettre en place une authentification des utilisateurs AD sur GLPI.

Cette réalisation passe par plusieurs étapes dont la mise en place et configuration d'un serveur GLPI qui sera lié à un serveur Windows avec les services Active Directory avec différents utilisateurs qui auront différents droits :

- 1 utilisateur standard qui n'aura pas de droits spécifiques
- 1 utilisateur qui lui aura des droits

Les utilisateurs autorisés à se connecter à GLPI avec leurs identifiants Active Directory seront regroupés dans une OU "Personnel". Seuls les utilisateurs appartenant à cette OU pourront accéder à GLPI. La mise en place de LDAP est nécessaire pour faire communiquer GLPI et notre serveur AD. Depuis GLPI, nous pourrons déclencher une synchronisation LDAP afin de mettre à jour les comptes dans GLPI.

SOMMAIRE

□ Introduction

- Objectif du projet
- Présentation générale de l'authentification AD via LDAP

□ Installation du serveur Active Directory (AD)

- Préparation de l'environnement
- Installation de Windows Server
- Configuration du rôle Active Directory Domain Services (AD DS)
- Création et gestion des utilisateurs dans AD

□ Installation du serveur Debian 11 et des composantes pour GLPI

- Préparation de l'environnement Debian
- Installation de Debian 11
- Mise à jour et configuration initiale de Debian
- Installation du serveur web (Apache/Nginx)
- Installation de la base de données (MySQL/MariaDB)
- Installation de PHP et des extensions requises
- Téléchargement et installation de GLPI
- Configuration de GLPI pour l'accès LDAP
 - Configuration des paramètres LDAP dans GLPI
 - Mappage des attributs utilisateur

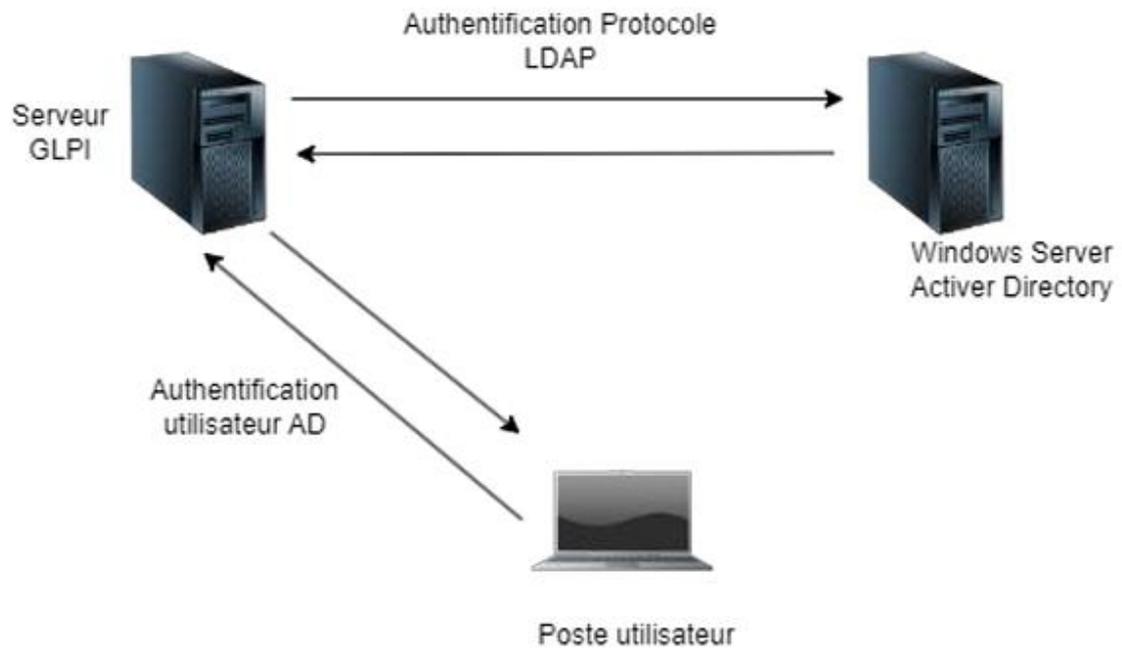
□ Tests d'accès des utilisateurs sur le poste client

- Préparation des postes clients
- Configuration du client pour accéder à GLPI
- Tests d'authentification des utilisateurs
 - Création de comptes de test dans AD
 - Connexion à GLPI avec les comptes AD
- Validation des résultats
- Dépannage et ajustements si nécessaires

□ Conclusion

- Résumé des étapes réalisées

ARCHITECTURE RESEAU :



CONFIGURATION AD :

Notre serveur AD sera configuré avec l'ip Suivante :

- 192.168.1.254

Voici les paramètres IP du serveur :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) ×

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 1 . 254

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : . . .

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

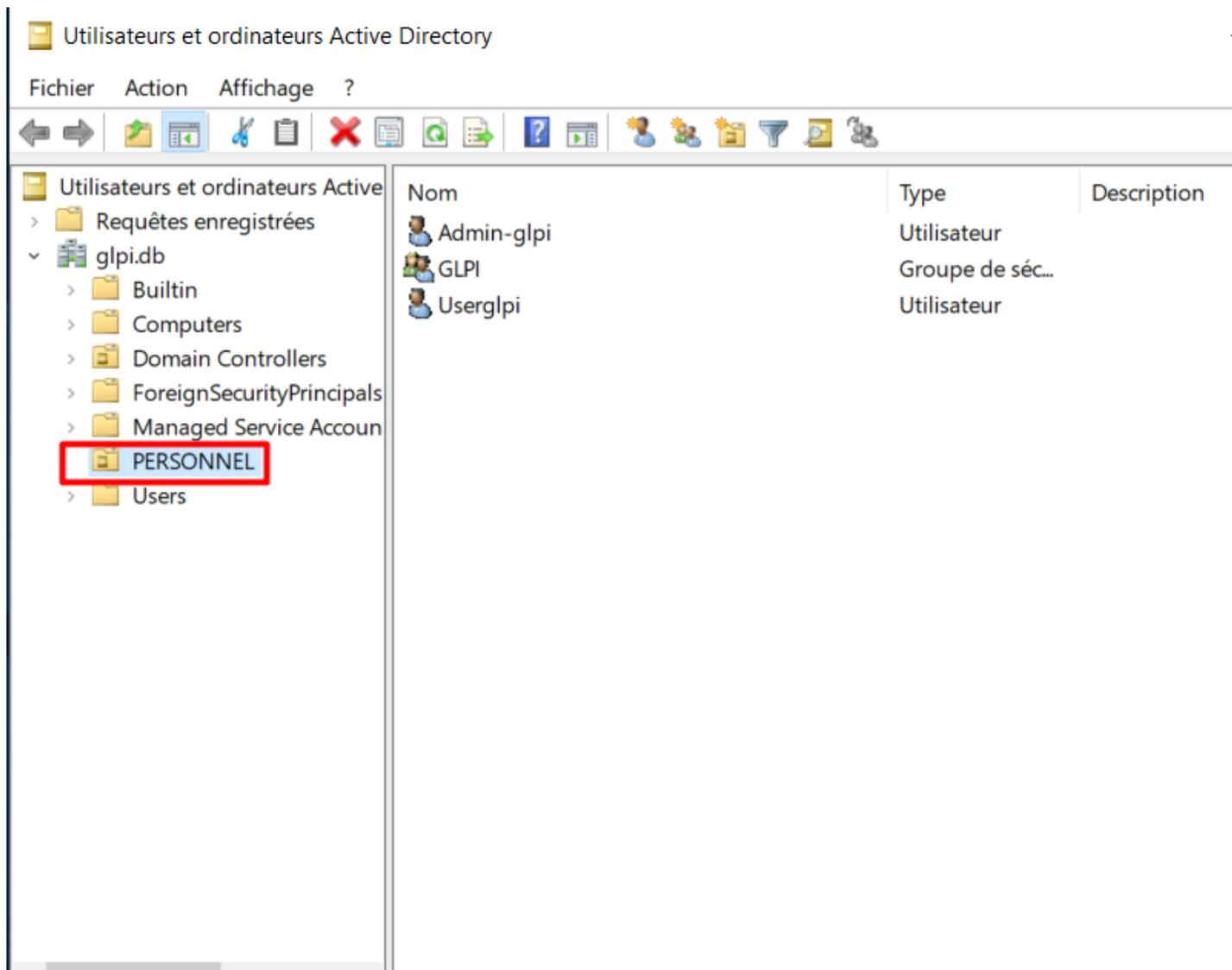
Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

OK Annuler

Nous allons ensuite créer une OU PERSONNEL où nous allons créer différents utilisateurs pour notre GLPI :



Notre AD est opérationnel pour effectuer la liaison avec notre serveur Debian qui lui servira de serveur GLPI .

MISE EN PLACE SERVEUR DEBIAN 11 :

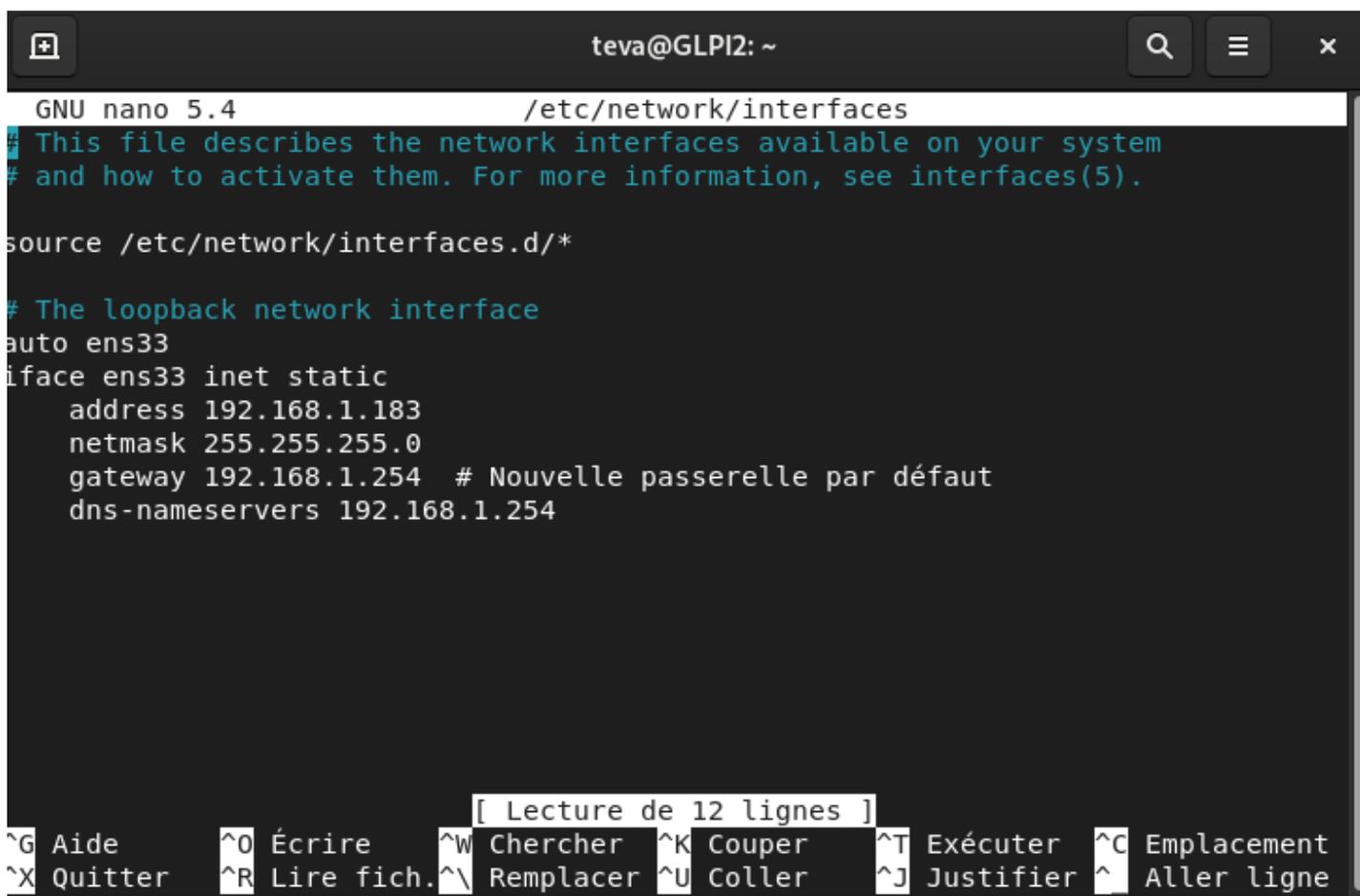
Afin de faire fonctionner notre serveur GLPI, j'ai choisi de le configurer sur Debian 11.

Tout d'abord il faut faire communiquer le serveur debian avec le serveur AD :

Pour cela effectuer les commandes suivantes :

- Su root (renseigner le mot de passe super admin)
- sudo nano /etc/network/interfaces

Ensuite il faut renseigner les informations suivantes afin de faire communiquer les serveurs :



```
teva@GLPI2: ~
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

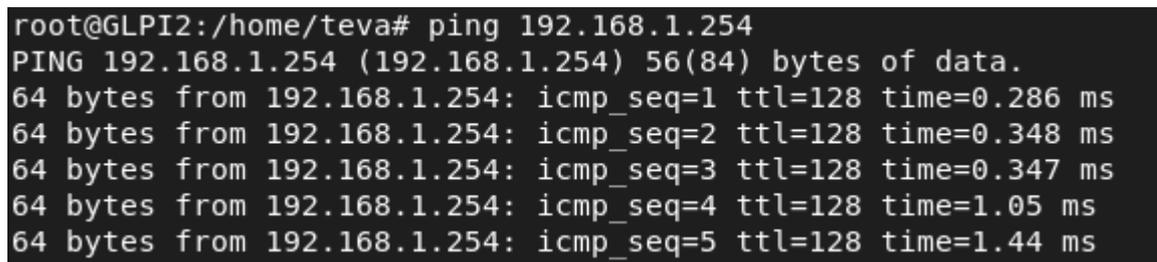
# The loopback network interface
auto ens33
iface ens33 inet static
    address 192.168.1.183
    netmask 255.255.255.0
    gateway 192.168.1.254 # Nouvelle passerelle par défaut
    dns-nameservers 192.168.1.254

[ Lecture de 12 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne
```

Puis il faut ensuite enregistrer cette configuration et relancer les services via la commande :

- systemctl restart networking

Une fois que tout cela a été effectué il faut effectuer un test de ping avec notre serveur AD :



```
root@GLPI2:/home/teva# ping 192.168.1.254
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=128 time=0.286 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=128 time=0.348 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=128 time=0.347 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=128 time=1.05 ms
64 bytes from 192.168.1.254: icmp_seq=5 ttl=128 time=1.44 ms
```

C'est donc bon, nos serveurs communiquent bien entre eux.

MISE EN PLACE GLPI :

Afin de mettre en place notre GLPI, plusieurs prérequis sont à prendre en compte :

1. Mettre à jour le système

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

2. Installer les prérequis

Ces prérequis nous permettront de configurer notre GLPI en l'hébergeant via un serveur web apache 2 en ligne et à configurer sa base de donnée.

```
sudo apt install -y apache2 mariadb-server php php-mysql php-curl php-gd php-intl php-xml php-mbstring php-ldap php-apcu php-zip
```

3. Télécharger et extraire GLPI

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.0/glpi-10.0.0.tgz
tar -xvzf glpi-10.0.0.tgz
sudo mv glpi /var/www/html/
```

4. Configurer les permissions

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

5. Configurer la base de données

Se connecter à MariaDB :

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

Créer une base de données et un utilisateur pour GLPI (exécuter ces commandes dans le terminal MySQL) :

```
CREATE DATABASE glpi;
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'yourpassword';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpiuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

6. Configurer Apache pour GLPI

Créer un fichier de configuration pour GLPI :

```
sudo nano /etc/apache2/sites-available/glpi.conf
```

Ajouter le contenu suivant dans le fichier glpi.conf :

```
<VirtualHost *:80>
  ServerAdmin admin@example.com
  DocumentRoot /var/www/html/glpi
  ServerName example.com

  <Directory /var/www/html/glpi>
    Options FollowSymlinks
    AllowOverride All
    Require all granted
  </Directory>

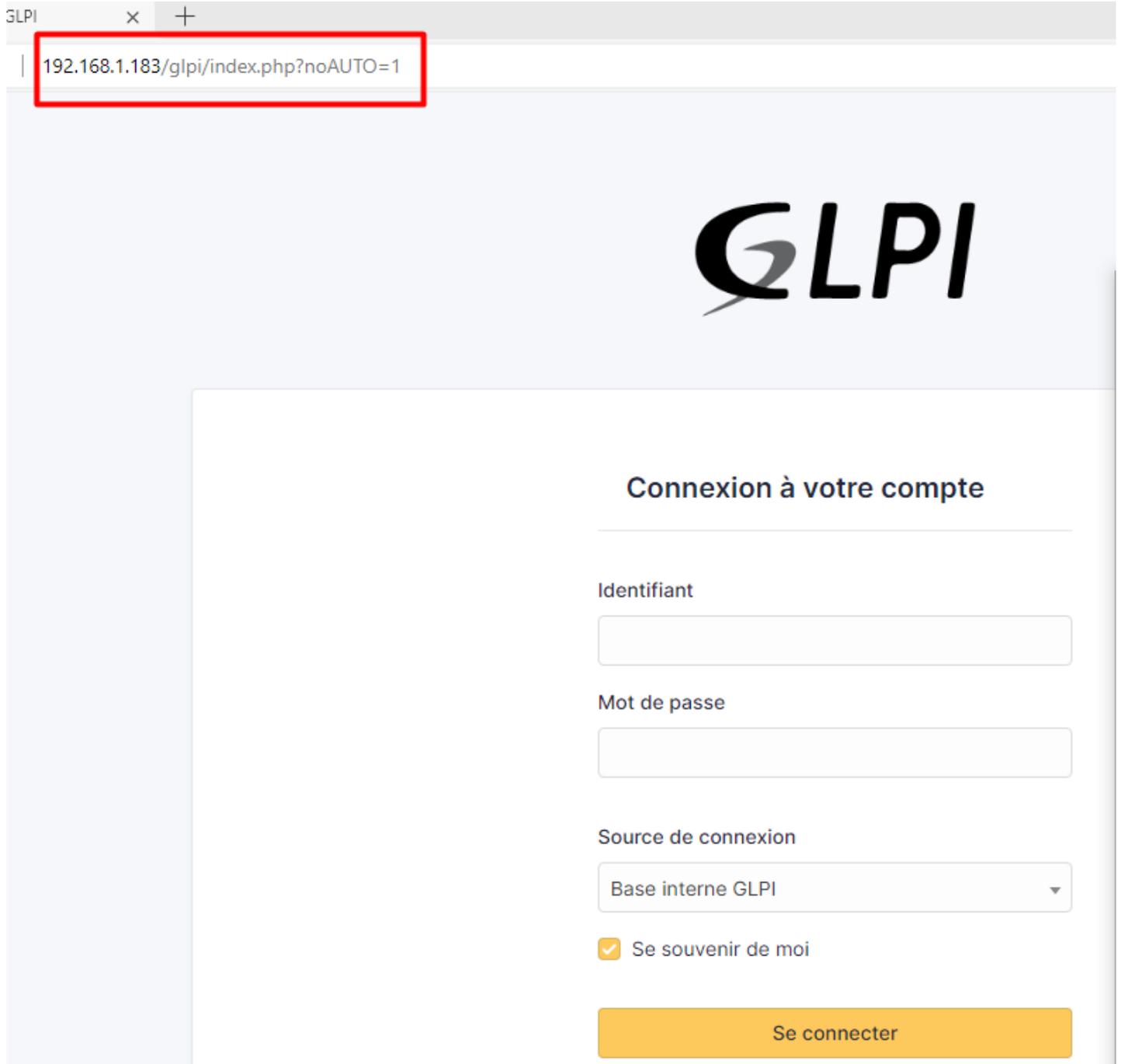
  ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
  CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

Activer le site GLPI et le module rewrite :

```
sudo a2ensite glpi.conf
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Une fois ces étapes terminées, nous devrions avoir accès à notre GLPI via navigateur en tapant l'ip assigné au serveur :

Test d'accès à GLPI depuis notre VM utilisateur Windows 10 :



GLPI est correctement installé, maintenant il nous faut faire remonter les utilisateurs AD dedans.

MISE EN PLACE D'UNE LIAISON LDAP ENTRE GLPI et l'AD

Il nous faut donc configurer LDAP :

Suivre notre VM Linux nous allons installer l'extension LDAP :

Les commandes sont les suivantes :

INSTALLATION DE LDAP et des outils Associés :

```
sudo apt update  
sudo apt install slapd ldap-utils -y
```

CONFIGURATION de OPENLDAP

Pendant l'installation, nous serons invité à définir un mot de passe pour l'administrateur LDAP. Si vous n'êtes pas invité, vous pouvez reconfigurer slapd en utilisant la commande suivante :

```
sudo dpkg-reconfigure slapd
```

3. Vérifier l'installation

Une fois l'installation terminée, vous pouvez vérifier que le service OpenLDAP fonctionne correctement :

```
sudo systemctl status slapd  
sudo systemctl restart apache2
```

Notre Serveur Debian est correctement configuré pour faire la liaison LDAP avec l'AD :

CONFIGURATION LIAISON LDAP :

Il nous faut maintenant nous connecter à notre interface GLPI :

The image shows the GLPI login interface. At the top, there is a large logo for 'GLPI' in a bold, black, sans-serif font. Below the logo, the heading 'Connexion à votre compte' is centered. Underneath, there are three input fields: 'Identifiant' with the value 'glpi', 'Mot de passe' with four dots, and 'Source de connexion' with a dropdown menu showing 'Base interne GLPI'. A checked checkbox labeled 'Se souvenir de moi' is located below the dropdown. At the bottom of the form is a large orange button labeled 'Se connecter'.

En utilisant les identifiants suivants de base :

ID : glpi

Psw : glpi

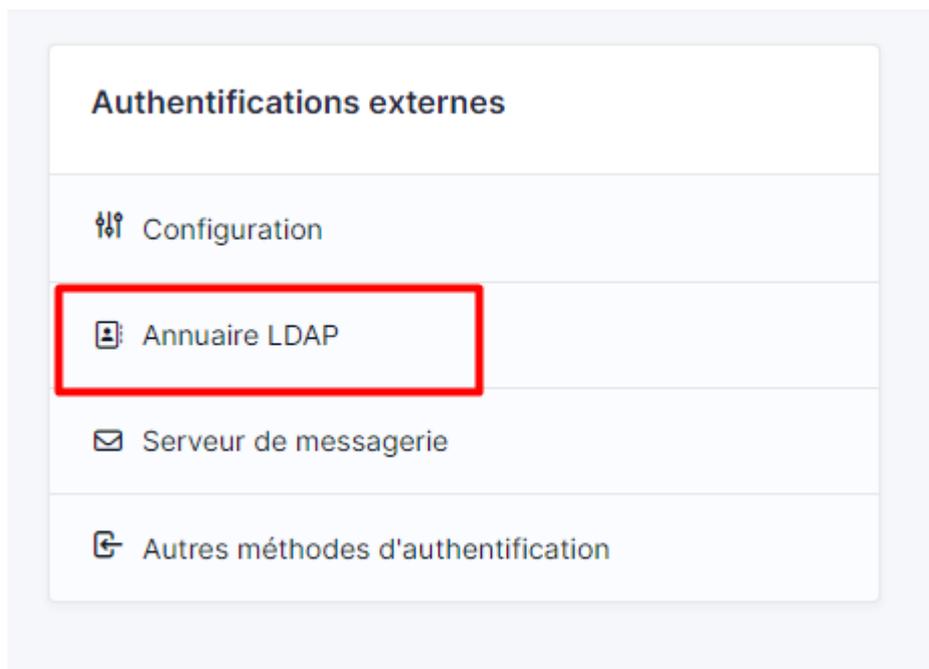
Nous arrivons donc sur l'interface de GLPI :

The screenshot shows the GLPI dashboard. On the left is a dark blue sidebar with the GLPI logo and a search bar. Below the search bar are menu items: Parc, Assistance, Gestion, Outils, Administration, and Configuration. At the bottom of the sidebar is a 'Réduire le menu' button. The main content area is titled 'Accueil' and features a 'Tableau de bord' section with tabs for 'Vue personnelle', 'Vue groupe', 'Vue globale', 'Flux RSS', and 'Tous'. A prominent orange warning banner at the top right contains a warning icon and two security-related messages in French. Below the banner is a 'Central' dropdown menu. The dashboard displays eight colored tiles representing different asset categories, each with a '0' count: Logiciel (green), Ordinateur (red), Matériel réseau (light blue), Téléphone (light blue), Licence (green), Moniteur (red), Baie (teal), and Imprimante (dark blue). At the bottom, there are three larger tiles for 'Ordinateurs par Fabricant', 'Moniteurs par Modèle', and 'Matériels réseau par', all showing 'Aucune donnée trouvée'. A bottom navigation bar shows icons for '6' (users), '2' (groups), '0' (shopping cart), and '0' (documents).

Ensuite il faut se rendre dans la Rubrique Configuration > Authentification :

This screenshot shows the 'Configuration' menu in GLPI. The menu is dark blue with white text and icons. The 'Authentification' option is highlighted with a red rectangular box. Other options in the menu include: Intitulés, Composants, Notifications, Niveaux de services, Générale, Unicité des champs, Actions automatiques, Collecteurs, Liens externes, and Plugins.

Il faut ensuite sélectionner :



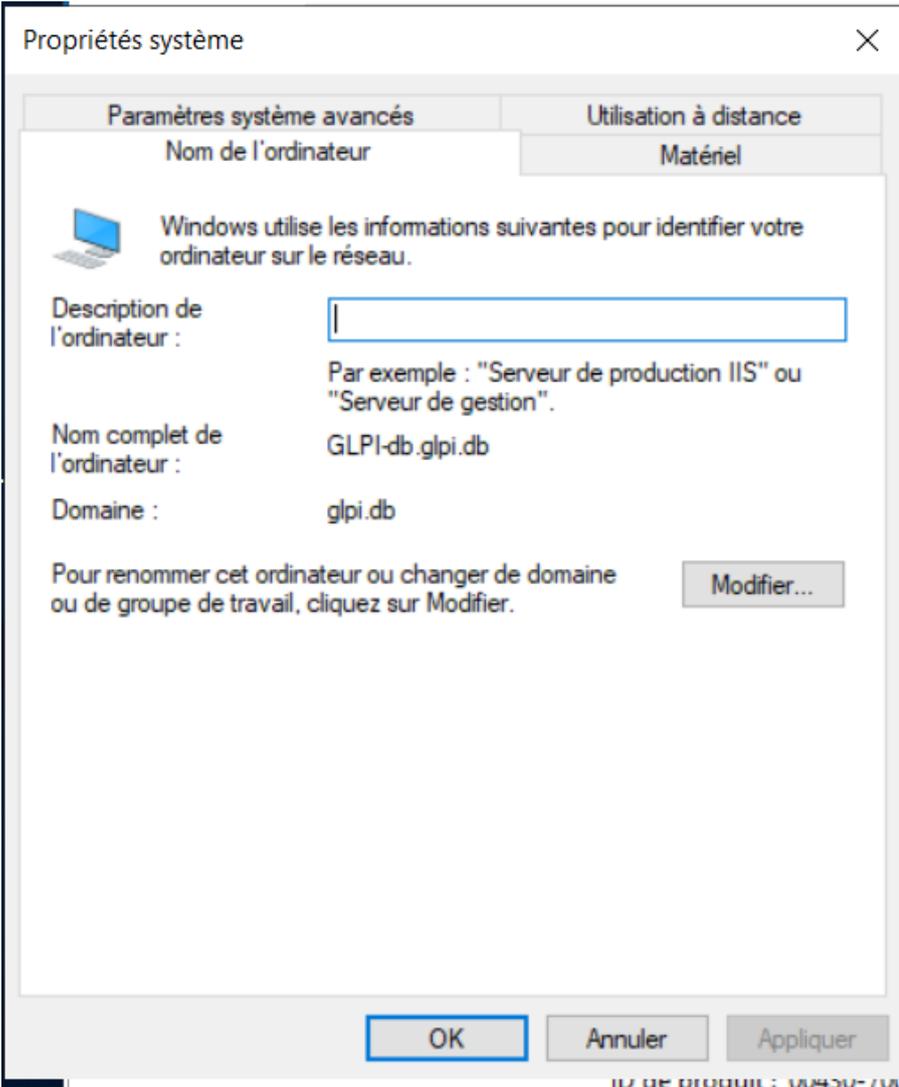
Nous serons ensuite amené à rentrer diverses informations pour que tout fonctionne correctement :

Annuaire LDAP - GLPI-db.glp.db Actions

Nom	GLPI-db.glp.db	Dernière modification	2024-06-18 22:00
Serveur par défaut	Oui	Actif	Oui
Serveur	192.168.1.254	Port (par défaut 389)	389 Saisir le port 389
Filtre de connexion	(&(objectClass=user)(objectCategory=person)!((userAccountControl:1.2.840.113556.1.4.803:=2)))		
BaseDN	OU=PERSONNEL,DC=glpi,DC=db Préciser à GLPI où il doit aller chercher les utilisateurs		
Utilisez un compte (pour les connexions non anonymes)	Oui		
DN du compte (pour les connexions non anonymes)	userglpi@glpi.db Renseigner le compte glpi disponible dans L'AD		
Mot de passe du compte (pour les connexions non anonymes)	<input type="text"/>		
Champ de l'identifiant	samaccountname	Commentaires	<input type="text"/>
Champ de synchronisation	objectguid		

Toutes ces informations sont disponibles ici :

Nom complet du serveur : (très important de saisir le nom complet sinon cela ne fonctionnera pas)



Propriétés système

Paramètres système avancés Utilisation à distance

Nom de l'ordinateur Matériel

Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.

Description de l'ordinateur :

Par exemple : "Serveur de production IIS" ou "Serveur de gestion".

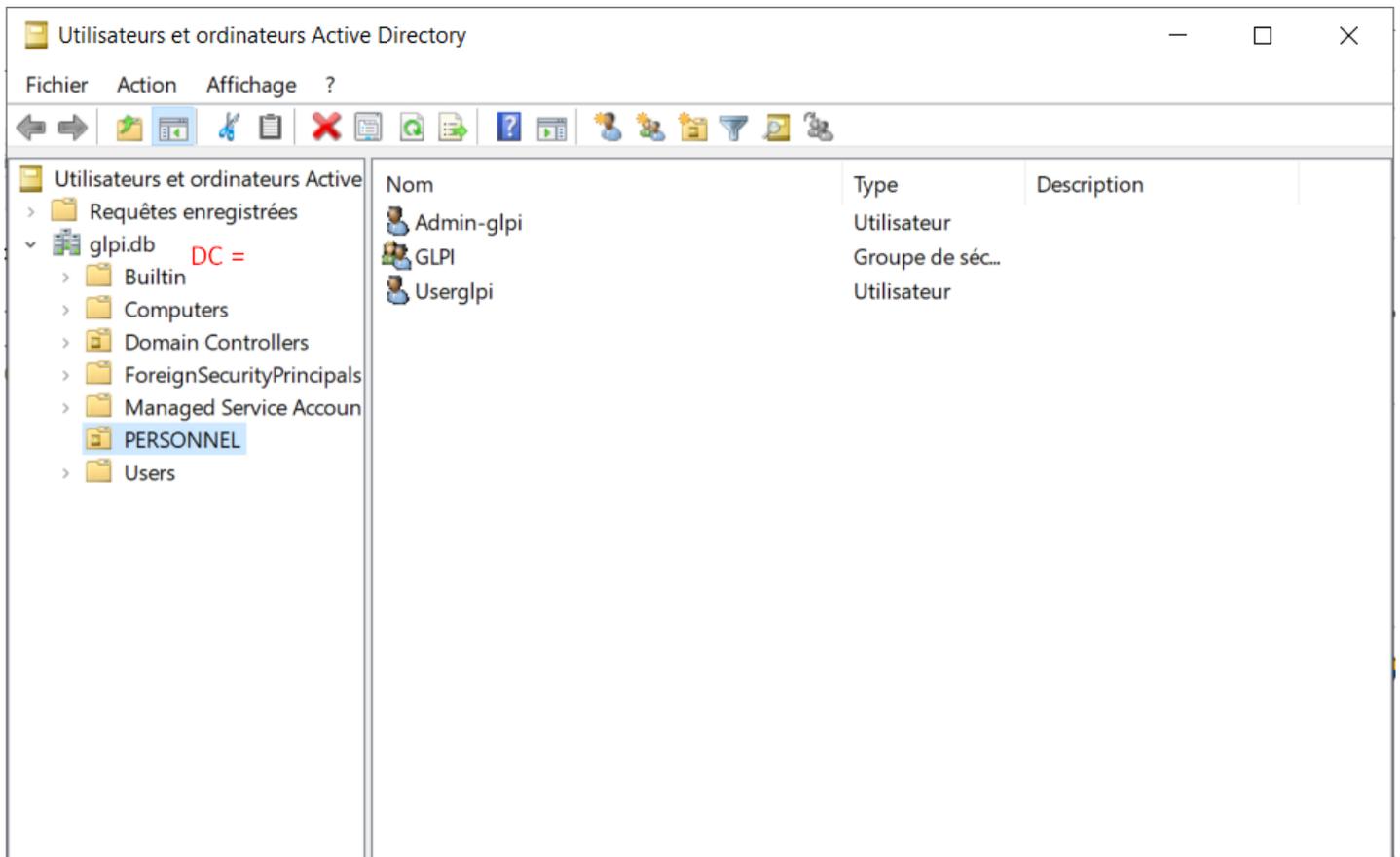
Nom complet de l'ordinateur : GLPI-db.glpi.db

Domaine : glpi.db

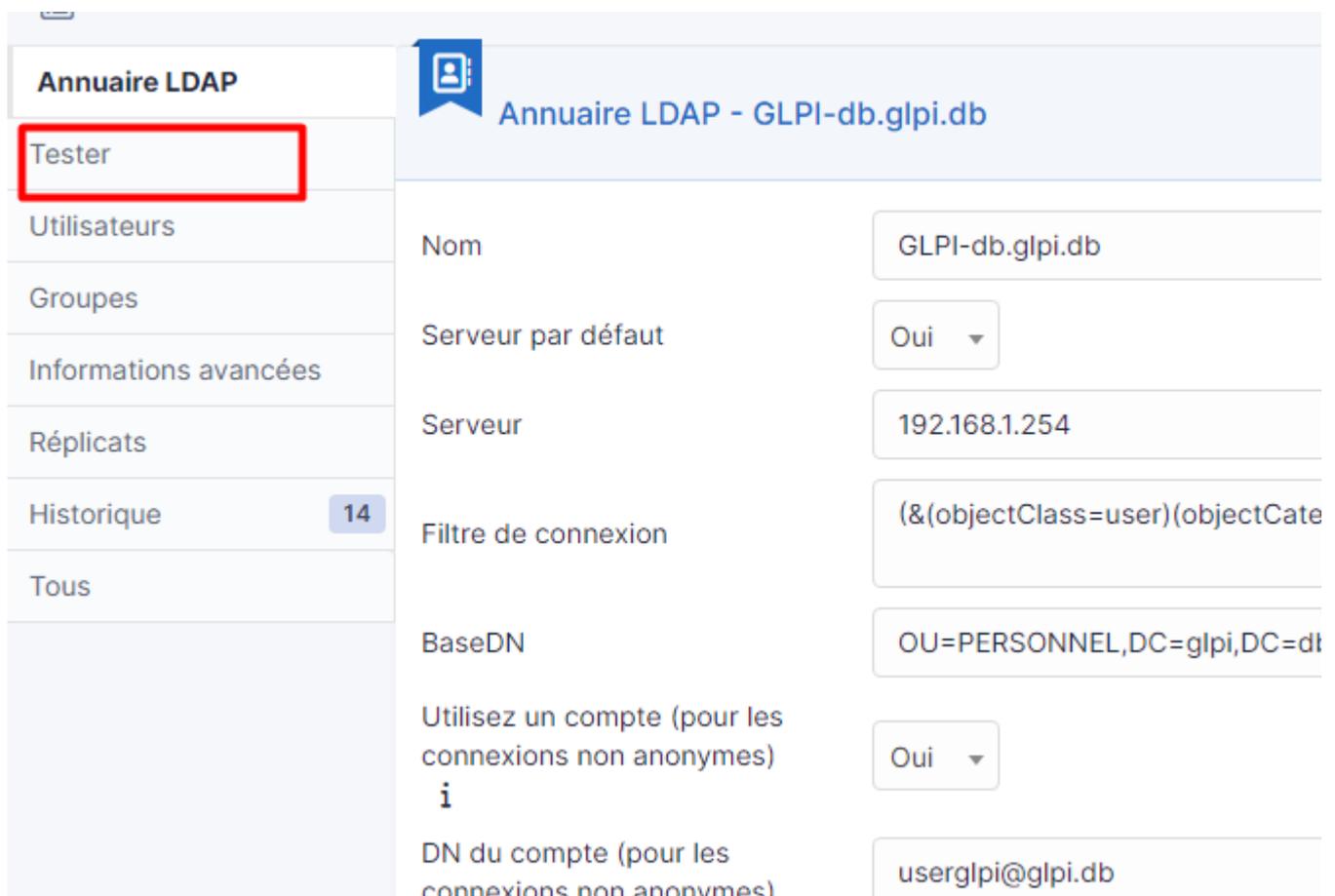
Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier...

ID de produit : 00430-70000-00001-AA701

Idem pour le chemin :



Ensuite nous pouvons enregistrer notre configuration, et procéder à un test de verification de jonction :

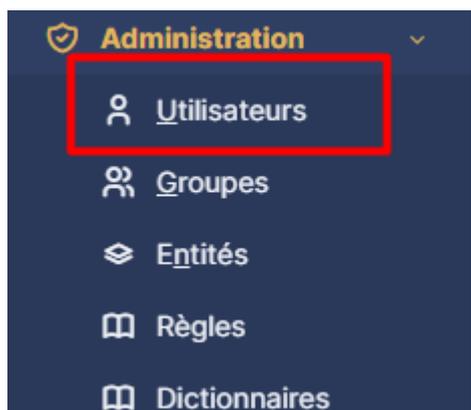


Si vous avez suivi toutes les étapes, normalement vous devriez avoir ce message :



Cela signifie que notre GLPI a bien réussi à avoir accès à l'OU PERSONNEL de notre serveur AD qui est réservé à GLPI :

Il faut ensuite aller importer nos utilisateurs via l'annuaire LDAP :



Ensuite :



Import en masse d'utilisateurs depuis un annuaire LDAP

 Synchronisation des utilisateurs déjà importés

 Importation de nouveaux utilisateurs

Ensuite sélectionnez mode expert :

Importation de nouveaux utilisateurs Mode expert

Activer le filtrage par date

Critère de recherche pour les utilisateurs

Identifiant	<input type="text"/>	Champ de synchronisation (objectguid)	<input type="text"/>
Adresse de messagerie	<input type="text"/>	Nom de famille	<input type="text"/>

Il faut maintenant bien vérifier le chemin :

Importation de nouveaux utilisateurs Mode simplifié

BaseDN

Filtre de recherche des utilisateurs

Et faites rechercher, le résultat devrait trouver tous les utilisateurs présents dans L'OU PERSONNEL de glpi :

Actions

<input type="checkbox"/>	IDENTIFIANT	NOM DE FAMILLE	EMAILS	TÉLÉPHONE
<input type="checkbox"/>	 adminglpi			
<input type="checkbox"/>	 glpi			
<input type="checkbox"/>	 glpi-system	Support		
<input type="checkbox"/>	 normal			
<input type="checkbox"/>	 post-only			
<input type="checkbox"/>	 tech			
<input type="checkbox"/>	 userglpi			

Il faut ensuite configurer les droits :

- 1 utilisateur doit être admin et peut donc voir les tickets créés par les utilisateurs lambda
- 1 utilisateur quant à lui peut seulement faire des tickets

L'administrateur sera donc le compte AD : adminglpi

L'utilisateur sera le compte AD : userglpi

Ajout des permission administrateur au compte admin.

Afin de réaliser la répartition des droits, il nous faut donc repasser sur le compte super ADMIN de GLP donc faire déconnexion puis :



The image shows a login form for GLPI. It has three main input fields: 'Identifiant' (username) with 'glpi' entered, 'Mot de passe' (password) with four dots, and 'Source de connexion' (connection source) with a dropdown menu showing 'Base interne GLPI'. A red rectangular box highlights the 'Source de connexion' dropdown. Below the dropdown is a checked checkbox labeled 'Se souvenir de moi'. At the bottom is a yellow button labeled 'Se connecter'. The text 'choisir base interne' is written in red below the dropdown menu.

Il faut ensuite aller vérifier nos différents groupes ainsi que leurs droits, ici nous voulons donner les droits admin au compte admin :

GLPI Administration / Utilisateurs

+ Ajouter Rechercher Listes

Utilisateur - adminglpi

Habilitations	2
Groupes	2
Préférences	
Éléments utilisés	
Éléments gérés	
Tickets créés	
Problèmes	
Changements	
Documents	
Réservations	
Synchronisation	
Liens	
Certificats	
Historique	7
Tous	

Identifiant: **adminglpi**

Champ de synchronisation: 5fd75d1c-5758-44bf-8632-763b1fc58b7c

Nom de famille:

Prénom: Admin-glpi Image

Fuseau horaire: L'utilisation des fuseaux horaires n'a pas été activé. Exécutez la commande "php bin/console glpi:database:enable_timezones" pour l'activer.

Actif: Oui Emails

Valide depuis: Valide

Téléphone: Auther

Téléphone mobile: Catégr

Téléphone 2:

Il faut ensuite lui ajouter le bon profil correspondant :

Actions

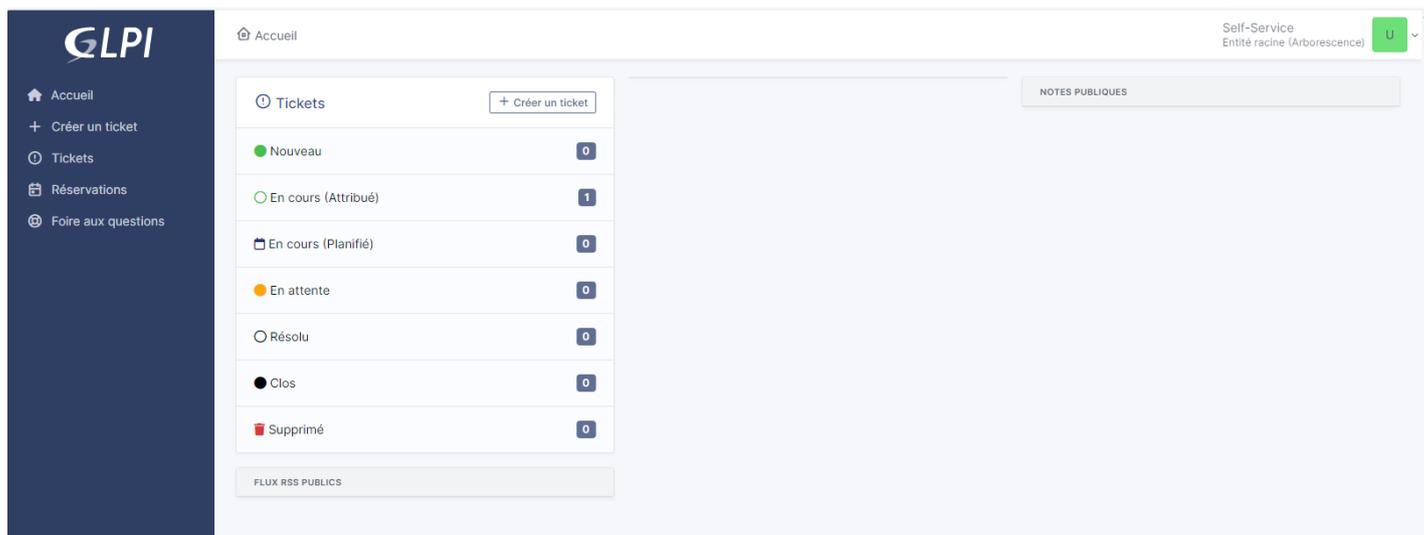
Entités	Profils (D=Dynamique, R=Récuratif)
<input type="checkbox"/> Entité racine	Admin
<input type="checkbox"/> Entité racine	Self-Service (D)

Actions

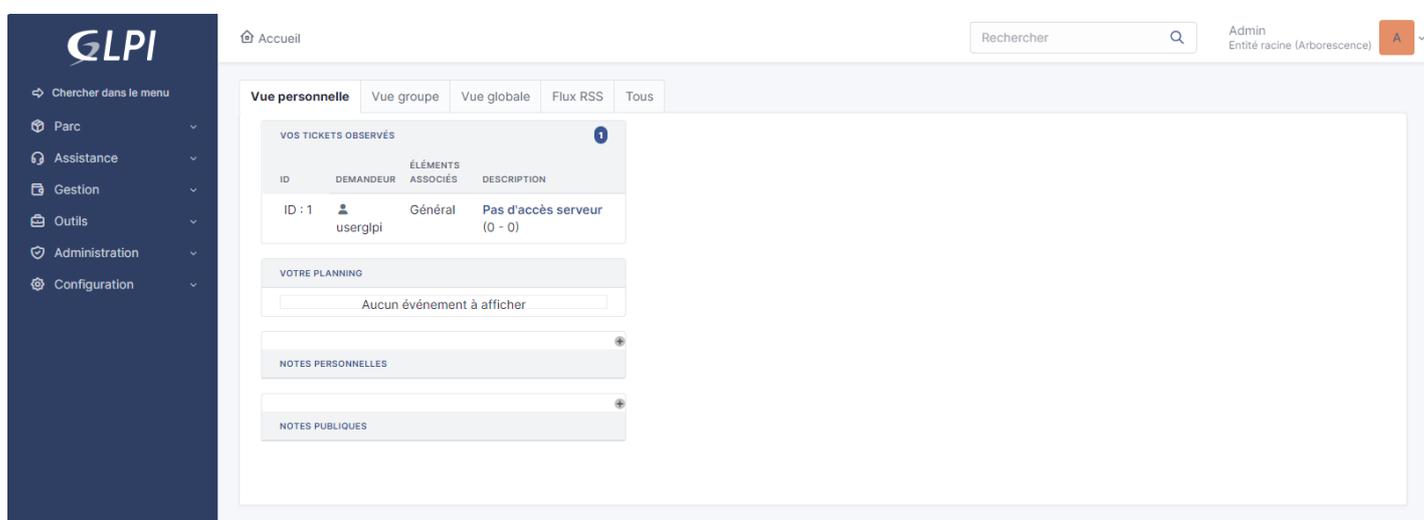
Nous allons donc procéder à des test en nous connectant au compte :

Userglpi :

Son interface est basique et se limite à la création de tickets.



Maintenant nous allons donc voir si l'admin GLPI à quant à lui tous les droits nécessaires.



On observe qu'il a bien la bonne interface correspondant à son profil ce qui permet de différencier l'utilisation classique des utilisateurs à celle des admin ou des technicien qui vont répondre à leurs demandes.

On observe donc que l'admin est le seul à pouvoir voir le ticket créé par l'utilisateur.