

# **PROCEDURE D'INSTALLATION: GLPI – AUTHENTIFICATION LDAP**



# Introduction

- **Objectif** : L'objectif principal de la **liaison LDAP dans GLPI** (Gestionnaire Libre de Parc Informatique) est de **centraliser et automatiser la gestion des utilisateurs** en s'appuyant sur un annuaire existant (comme Active Directory, OpenLDAP, etc.)

## Prérequis

- **Système d'exploitation**
  - **Serveur GLPI fonctionnelle**
  - **Serveur AD avec protocole LDAP config**
- **Ressources matérielles (minimum recommandé)**
  - **CPU: 1 vCPU**
  - **RAM: 1 Go**
  - **Disque: 8 Go**

## Configuration cible

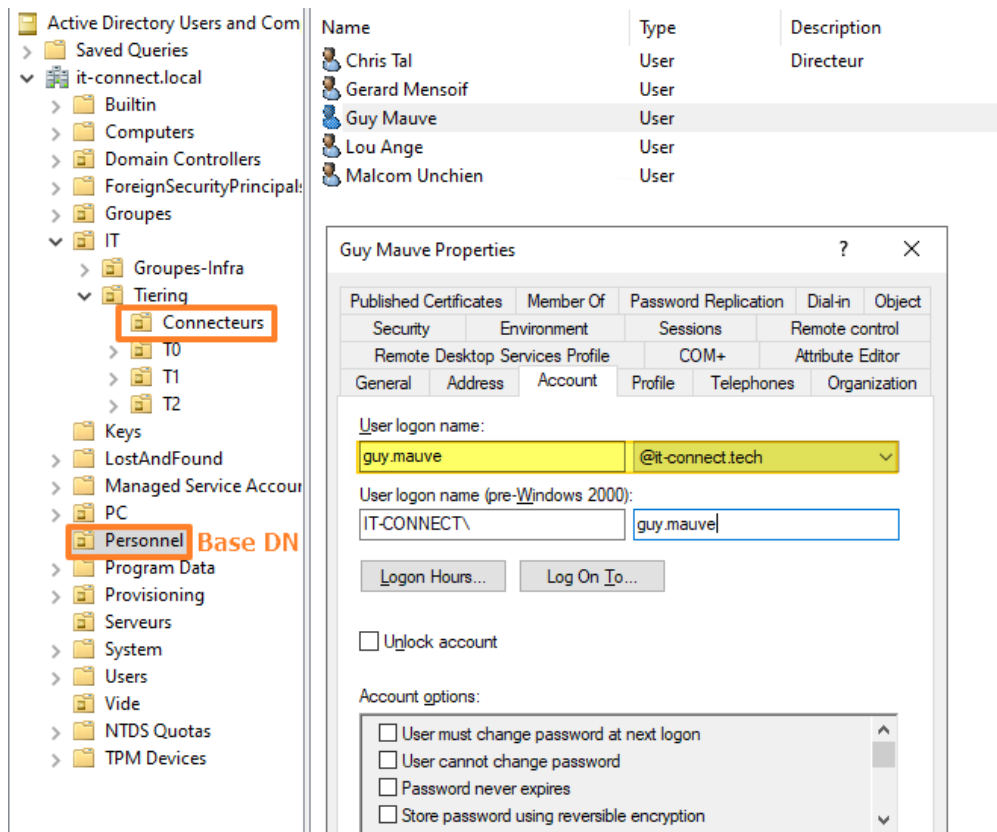
**Avant de passer à la configuration, voici quelques informations sur l'environnement utilisé.**

Pour cette démonstration, le domaine Active Directory "**it-connect.local**" sera utilisé et le contrôleur de domaine **SRV-ADDS-02** sera utilisé. Ce serveur dispose de l'adresse IP "**10.10.100.11**" et la connexion sera effectuée en LDAP, sur le port par défaut (389).

- Le compte utilisateur qui sera utilisé comme "**connecteur**" pour permettre à GLPI de se connecter à l'Active Directory se nomme "**Sync\_GLPI**". Il est stocké dans l'unité d'organisation "**Connecteurs**" de l'annuaire (voir image ci-dessous). Il s'agit d'un compte utilisateur standard, sans aucun droit particulier sur l'annuaire Active Directory. **Faites-moi plaisir : n'utilisez pas de compte Administrateur.**

- Tous les utilisateurs qui doivent pouvoir se connecter à GLPI à l'aide de leur compte Active Directory sont stockés dans l'unité d'organisation "**Personnel**" visible ci-dessous. Elle correspond à ce que l'on appelle la "**Base DN**" vis-à-vis du connecteur LDAP de GLPI. **Les autres utilisateurs ne pourront pas se connecter.** En fait, ce n'est pas utile de mettre la racine du domaine comme base DN : essayez de restreindre autant que possible pour limiter la découverte de l'annuaire Active Directory au strict nécessaire.

- Les utilisateurs de l'Active Directory pourront **se connecter à GLPI à l'aide de leur identifiant correspondant à l'attribut "UserPrincipalName"** (mis en évidence, en jaune, sur l'image ci-dessous). Cet identifiant, sous la forme "identifiant + nom de domaine", leur permettra se connecter à GLPI avec un identifiant qui correspond à leur e-mail. L'alternative consisterait à utiliser l'attribut "**SamAccountName**" (soit l'identifiant sous la forme "DOMAINE\identifiant").



## Installer l'extension LDAP de PHP

L'**extension LDAP de PHP** doit être installée sur votre serveur pour que GLPI soit capable de communiquer avec votre serveur contrôleur de domaine Active Directory (ou tout autre annuaire LDAP).

Connectez-vous à votre serveur GLPI et exécutez les deux commandes suivantes pour mettre à jour le cache des paquets et procéder à l'installation de l'extension.

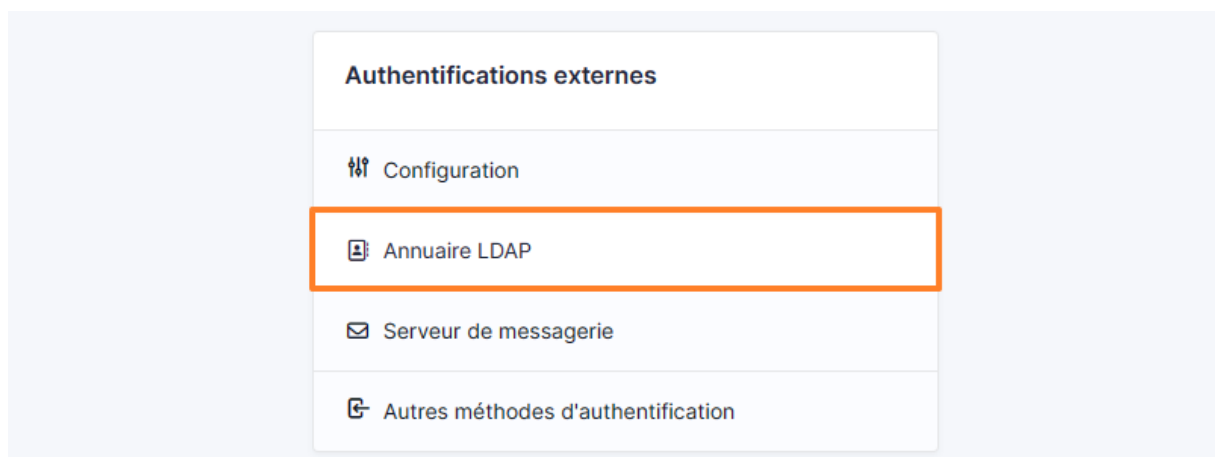
```
# apt-get install php-ldap
```

## Ajouter un annuaire LDAP dans GLPI

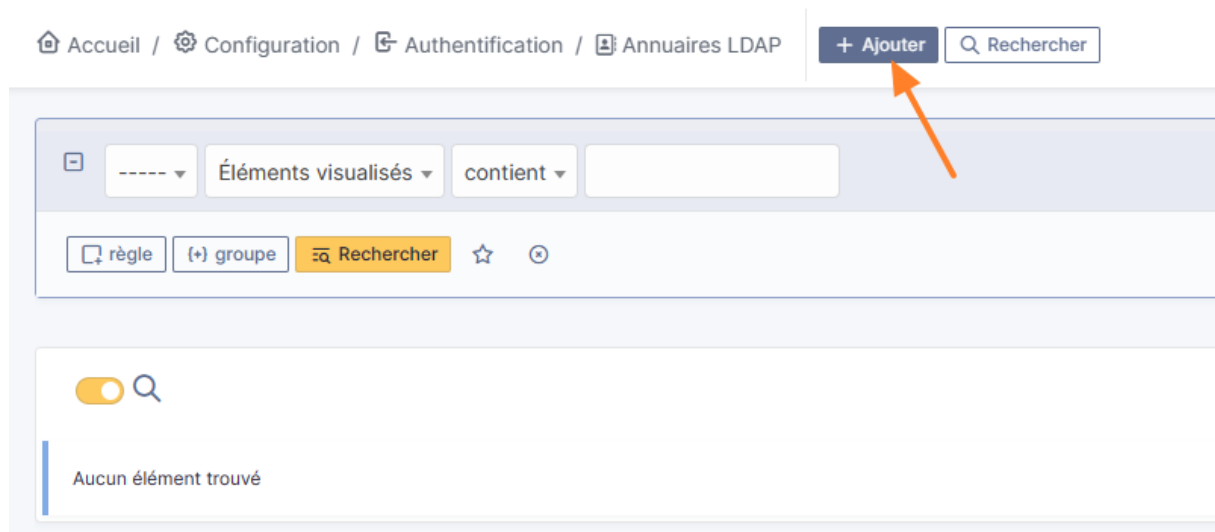
Désormais, nous allons ajouter notre annuaire Active Directory à GLPI. Connectez-vous à GLPI avec un compte administrateur, puis dans le menu "**Configuration**", cliquez sur "**Authentification**".



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




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



Un formulaire s'affiche à l'écran. Comment le renseigner ? À quoi correspondent tous ces champs ? C'est que nous allons voir ensemble.

- **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** : faut-il s'appuyer sur ce serveur par défaut pour l'authentification LDAP ? Il ne peut y avoir qu'un seul serveur LDAP défini par défaut.
- **Actif** : nous allons indiquer "Oui", sinon ce sera déclaré, mais non utilisé.
- **Serveur** : adresse IP du contrôleur de domaine à interroger. Avec le nom DNS, cela ne semble pas fonctionner (malheureusement).
- **Port** : 389, qui est le port par défaut du protocole LDAP. Si vous utilisez TLS, il faudra le préciser à posteriori, dans l'onglet "**Informations avancées**", du nouveau serveur LDAP.
- **Filtre de connexion** : requête LDAP pour rechercher les objets dans l'annuaire Active Directory. Généralement, nous faisons en sorte de récupérer les objets utilisateurs ("objectClass=user") en prenant uniquement les utilisateurs actifs (via un filtre sur l'attribut [UserAccountControl](#)).

- **BaseDN** : où faut-il se positionner dans l'annuaire pour rechercher les utilisateurs ? Ce n'est pas nécessaire la racine du domaine, tout dépend comment est organisé votre annuaire et où se situent les utilisateurs qui doivent pouvoir se connecter. Il faut indiquer le DistinguishedName de l'OU.
- **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. En principe, vous ne pouvez pas utiliser de connexion anonyme ! Ici, il ne faut pas indiquer uniquement le nom du compte, mais la valeur de son attribut [DistinguishedName](#).
- **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).


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 <sup>i</sup>

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 <sup>i</sup>

+ Ajouter

Ci-dessous, la configuration utilisée pour cette démonstration et qui correspond à la "configuration cible" évoquée précédemment.

- **Nom** : Active Directory - it-connect.local
- **Serveur par défaut** : Oui
- **Actif** : Oui
- **Serveur** : 10.10.100.11
- **Port** : 389
- **Filtre de connexion** :  
((&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2))))
- **BaseDN** : OU=Personnel,DC=it-connect,DC=local
- **Utiliser bind** : Oui
- **DN du compte** :  
CN=Sync\_GLPI,OU=Connecteurs,OU=Tiering,OU=IT,DC=it-connect,DC=local
- **Mot de passe du compte** : Mot de passe du compte "Sync\_GLPI"
- **Champ de l'identifiant** : userprincipalname
- **Champ de synchronisation** : objectguid

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

Nouvel élément - Annuaire LDAP

Préconfiguration

Active Directory / OpenLDAP / Valeurs par défaut

Nom: Active Directory - it-connect.local

Serveur par défaut: Oui

Actif: Oui

Serveur: 10.10.100.11

Port (par défaut 389): 389

Filtre de connexion: (&(objectClass=user)(objectCategory=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

BaseDN: OU=Personnel,DC=it-connect,DC=local

Utiliser bind: Oui

DN du compte (pour les connexions non anonymes): CN=Sync\_GLPI,OU=Connecteurs,OU=Tiering,OU=IT,DC=it-connect,DC=local

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

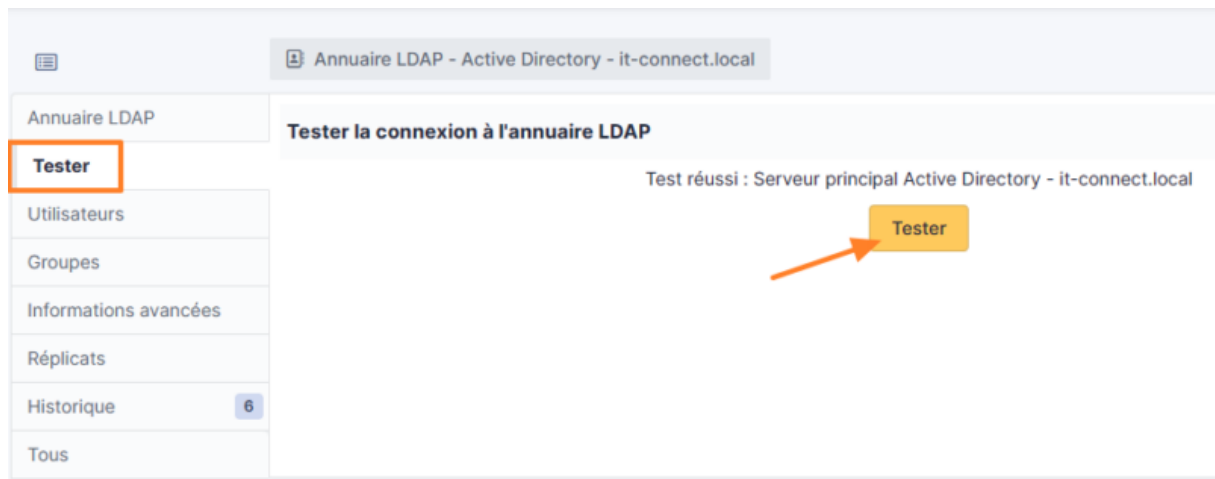
Champ de l'identifiant: UserPrincipalName

Champ de synchronisation: objectguid

+ 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.



Par ailleurs, **vous pouvez explorer les différents onglets : Utilisateurs, Groupes, Réplicats, etc...** Pour affiner la configuration. L'onglet "**Utilisateurs**" est intéressant pour configurer le mappage entre les champs d'une fiche utilisateur dans GLPI et les attributs d'un compte dans l'Active Directory. Quant à l'onglet "**Réplicats**", vous pouvez l'utiliser pour **déclarer un ou plusieurs contrôleurs de domaine "de secours"** à contacter si le serveur principal n'est plus joignable.



## 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 "**guy.mauve@it-connect.tech**" puisque je m'appuie sur l'attribut UserPrincipalName. Pour le mot de passe, je dois indiquer celui de son compte Active Directory.

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



### Login to your account

Login

Password

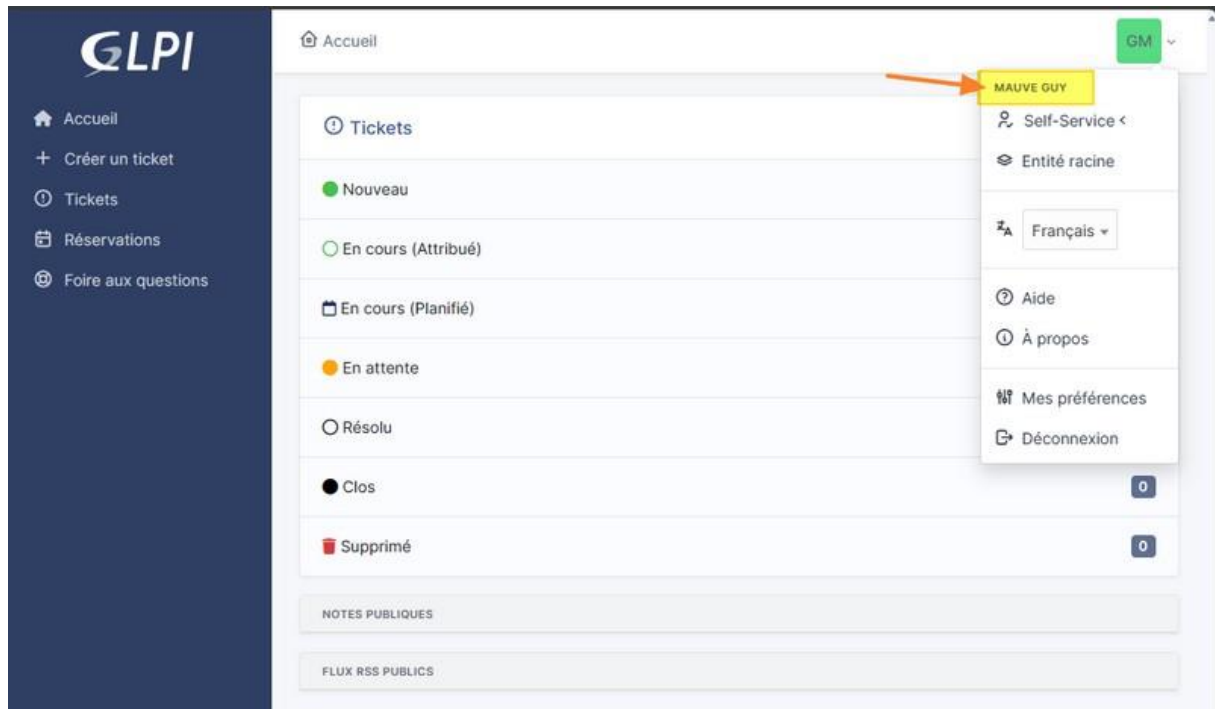
Login source

Active Directory - it-connect.local

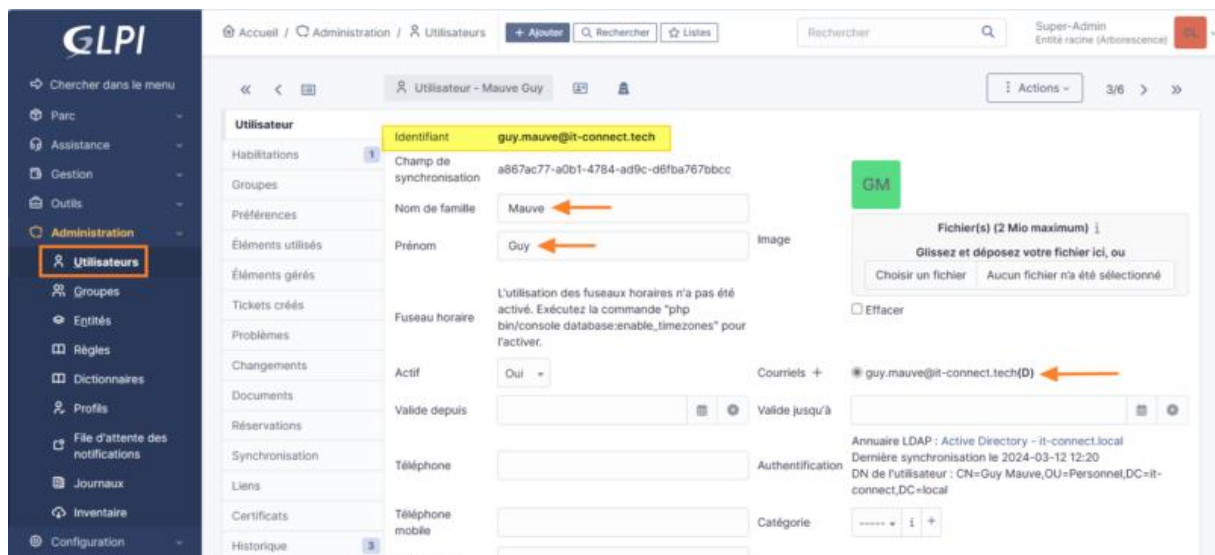
☒ Remember me

Sign in

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 **"guy.mauve@it-connect.tech"** ! GLPI a également récupéré le nom, le prénom et l'adresse e-mail à partir de différents attributs de l'objet LDAP.



En complément, à partir de la section "**Configuration**" puis "**Générale**", vous pouvez décocher l'option "**Afficher la liste des sources d'authentification sur la page de login**" pour que **la page de connexion à GLPI n'affiche pas la liste de vos sources**. Ceci évite d'indiquer publiquement que votre GLPI est synchronisé avec l'Active Directory. Lorsqu'un utilisateur va chercher à s'authentifier, **GLPI va sélectionner la bonne source d'authentification** (Merci à [@Patrice Vaillant](#) pour l'astuce).

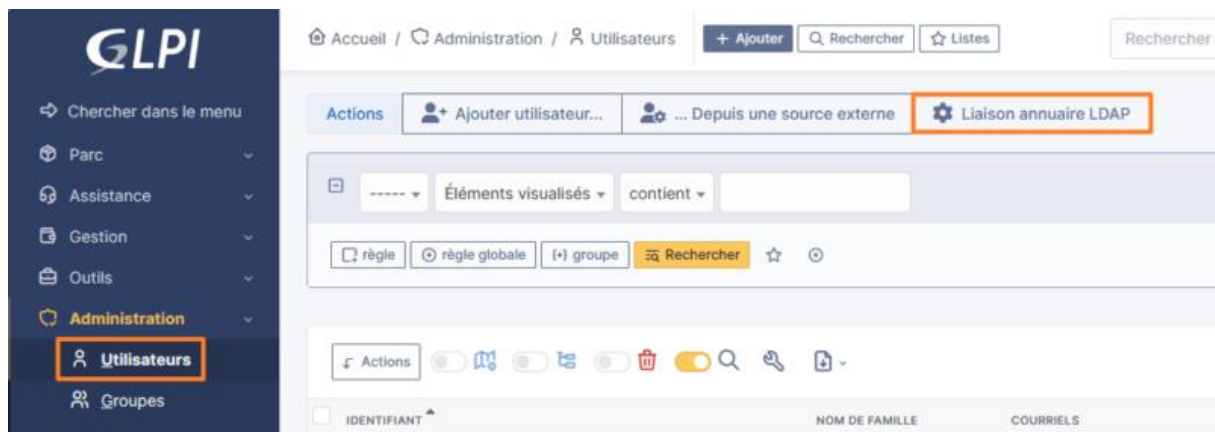
The screenshot shows the GLPI Configuration interface. On the left, a dark blue sidebar contains the 'Configuration' menu with a dropdown arrow, and several sub-items: 'Intitulés', 'Composants', 'Notifications', 'Niveaux de services', 'Général' (highlighted with an orange arrow), 'Unicité des champs', 'Actions automatiques', 'Authentification', 'Collecteurs', 'Liens externes', and 'Plugins'. The main content area is titled 'Général' and contains several settings. At the top right, there is a 'Tous' filter set to 'Non'. Below this are three input fields: 'Nombre maximum de résultats de recherche (par page)' set to 50, 'Taille limite par défaut (zones de texte de résumés)' set to 250, and 'Longueur maximale par défaut pour les URL' set to 30. Further down, there is a section for 'Activer les verrous' with a checkbox, a 'Profil à utiliser pour verrouiller les objets' dropdown set to 'Read-Only', and a 'Types d'objets à verrouiller' input field. Below that is a 'Temps de rétention "se souvenir de moi"' dropdown set to '7 jours'. At the bottom, there is a checkbox for 'État par défaut de la case à cocher' which is checked. The checkbox 'Afficher la liste des sources d'authentification sur la page de login' is highlighted with an orange box and is currently unchecked.

Configuration	Value
Tous	Non
Nombre maximum de résultats de recherche (par page)	50
Taille limite par défaut (zones de texte de résumés)	250
Longueur maximale par défaut pour les URL	30
Activer les verrous	<input type="checkbox"/>
Profil à utiliser pour verrouiller les objets	Read-Only
Types d'objets à verrouiller	
Temps de rétention "se souvenir de moi"	7 jours
État par défaut de la case à cocher	<input checked="" type="checkbox"/>
Afficher la liste des sources d'authentification sur la page de login	<input type="checkbox"/>

## Forcer une synchronisation Active Directory

A partir de GLPI, vous pouvez **forcer une synchronisation LDAP** de façon à mettre à jour les comptes dans GLPI "liés" à des comptes Active Directory, mais aussi pour **importer en masse tous les comptes des utilisateurs Active Directory**. Ceci vous évite d'attendre la première connexion et vous permet de préparer le compte : attribution du bon rôle, etc.

Cliquez sur "**Administration**" dans le menu, puis "**Utilisateurs**". Ici, vous avez accès au bouton "**Liaison annuaire LDAP**".



Vous avez ensuite le choix entre deux actions différentes, selon vos besoins.



Si vous cliquez sur "**Importation de nouveaux utilisateurs**", vous pourrez importer en masse les comptes dans l'Active Directory. Il vous suffit de lancer une recherche, de sélectionner les comptes à importer et de lancer l'import grâce au bouton "**Actions**".

Critère de recherche pour les utilisateurs

Identifiant

Champ de synchronisation (objectguid)

Courriel

Nom de famille

Prénom

Téléphone

Rechercher

Affichage (nombre d'éléments) 20

De 1 à 3 sur 3

Actions

CHAMP DE SYNCHRONISATION	UTILISATEURS	DERNIÈRE MISE À JOUR DANS L'ANNUAIRE LDAP
<input checked="" type="checkbox"/> 6bb7cbf4-23de-42cb-b088-2d4799773802	malcom.unchien@it-connect.tech	2024-03-12 10:59
<input checked="" type="checkbox"/> ae4a243a-08fb-4a8c-821d-eb3fd90c5210	lou.ange@it-connect.local	2024-03-12 10:59
<input checked="" type="checkbox"/> 00005f85-8c7f-4fd4-a391-d417d49501fc	chris.tal@it-connect.local	2024-03-12 10:59
<input checked="" type="checkbox"/> Champ de synchronisation	Utilisateurs	Dernière mise à jour dans l'annuaire LDAP

Actions

Affichage (nombre d'éléments) 20

De 1 à 3 sur 3