



TP GLPI - authentication LDAP via l'Active Directory

I. Présentation et configuration cible

Dans ce TP, nous allons avoir comment configurer l'authentification **LDAP** de **GLPI** pour pouvoir se connecter à l'application **GLPI** à partir des comptes utilisateurs présents dans un annuaire **Active Directory**.

Ainsi, un utilisateur pourra accéder à GLPI à l'aide de son nom d'utilisateur et son mot de passe habituel (puisque ce seront les informations de son compte dans l'Active Directory).

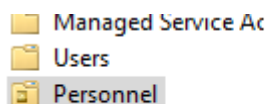
- Domaine AD : `formation.lan`
- Contrôleur de domaine : `SRV01.formation.lan`
- Adresse IP du DC : `192.168.1.101`
- Compte de liaison LDAP : `Syncglpi` dans `OU=Users,DC=formation,DC=lan`
- Base DN des utilisateurs : `OU=Personnel,DC=formation,DC=lan`

II. Prérequis : installer l'extension LDAP de PHP

Sur votre serveur GLPI (Ubuntu/Debian), installez et activez le module LDAP (si vous n'utilisez pas installer GLPI avec mon script sur : <https://github.com/sbeteta42/glpi>)

```
sudo apt-get install php-ldap  
sudo systemctl restart apache2
```

- Tous les utilisateurs qui doivent pouvoir se connecter à GLPI à l'aide de leur compte ActiveDirectory 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.

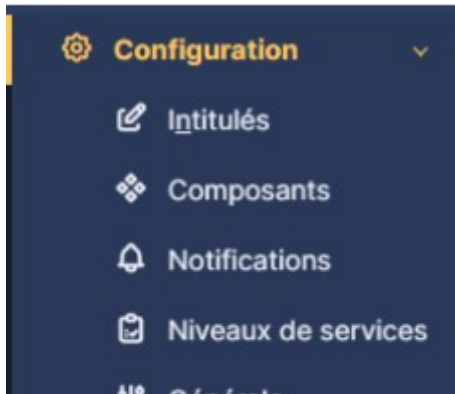
En fait, ce n'est pas utile de mettre la racine du domaine comme base DN : essayez de restreindre autant que possible pour limiter la découverte de l'annuaire Active Directory au strict nécessaire.

- Les utilisateurs de l'Active Directory pourront **se connecter à GLPI à l'aide de leur identifiant correspondant à l'attribut "UserPrincipalName"**.

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").

III. Ajouter l'annuaire LDAP dans GLPI

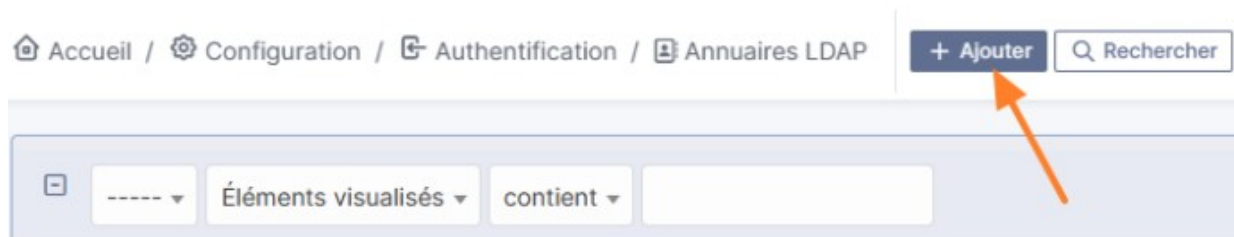
1. **Connexion** : ouvrez GLPI avec un compte admin ou glpi/glpi
2. **Menu Configuration** → Authentification (onglet central)



3. Cliquez sur **"Annuaire LDAP"**,



puis **"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).

Paramètres du formulaire

- **Nom** : formation.lan
- **Serveur par défaut** : Oui
- **Actif** : Oui
- **Serveur** : 192.168.1.101
- **Port** : 389
- **Filtre de connexion** :
(&(objectClass=user)(objectCategory=person)
(! (userAccountControl:1.2.840.113556.1.4.803:=2)))
- **Base DN** : OU=Personnel, DC=formation, DC=lan
- **Utiliser bind** : Oui
- **DN du compte** :

CN=SyncGLPI, CN=Users, DC=formation, DC=lan

- **Mot de passe du compte** : le mot de passe de SyncGLPI
- **Champ de l'identifiant** : userPrincipalName
- **Champ de synchronisation** : objectGuid

Ajoutez et sauvegardez. Vous verrez alors le test automatique de connexion...

V. Forcer la synchronisation LDAP

Depuis GLPI :


1. Administration → Utilisateurs




2. Bouton “Liaison annuaire LDAP”

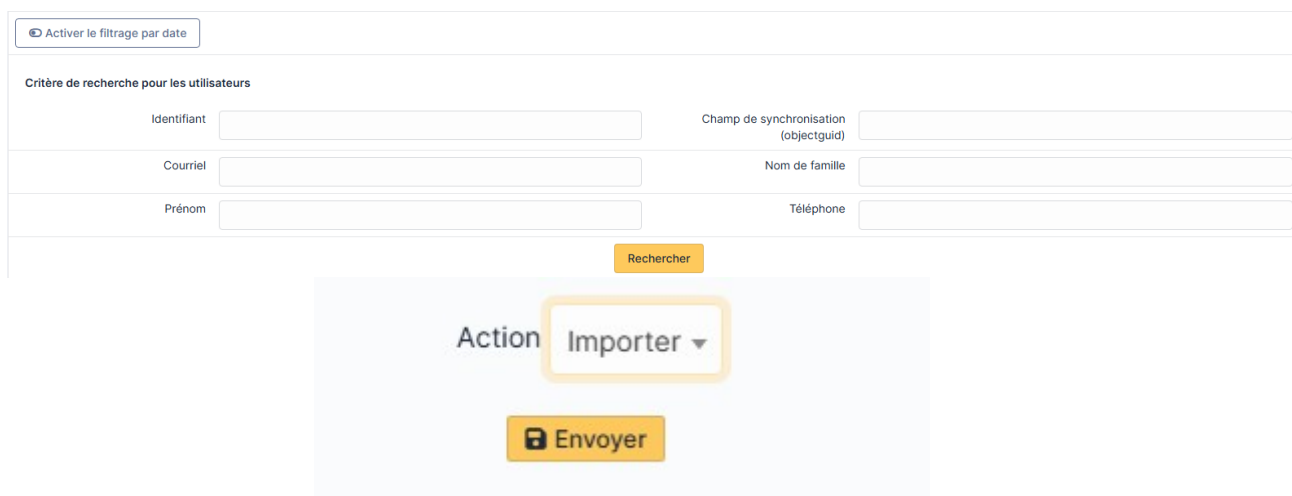
3. Choisissez “Importation de nouveaux utilisateurs” pour pré-charger tous les comptes AD

Import en masse d'utilisateurs depuis un annuaire LDAP

 Synchronisation des utilisateurs déjà importés

 Importation de nouveaux utilisateurs

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**".





↩ Actions

<input type="checkbox"/> CHAMP DE SYNCHRONISATION	UTILISATEURS
<input checked="" type="checkbox"/> 636a8c13-daf0-41a1-a31a-2c6929421a01	gbeteta@esicad.lan

- On clique sur envoyer pour importer le ou les comptes sélectionnés
- Un message de réussite apparaît.

Information ×

Élément ajouté : **BETETA Gabriel**
Opération réalisée avec succès

V. Tester la connexion et l'authentification

- Si le test LDAP échoue, revenez modifier le formulaire (souvent l'IP vs DNS)
- Une fois "Test OK", déconnectez-vous, et sur la page de login de GLPI, sélectionnez la source "Active Directory".
- Connectez-vous avec un utilisateur de l'OU Personnel, par exemple gbeteta@formation.lan.
- Si la connexion fonctionne, GLPI crée automatiquement le compte et importe nom, prénom, e-mail



Connexion à votre compte

Identifiant

Mot de passe



Source de connexion

☒ Se souvenir de moi

Se connecter

GLPI

Accueil

Créer un ticket

Tickets

Réervations

Foire aux questions

Accueil

Créer un ticket

Tickets

Réervations

Foire aux questions

Notes publiques

Self-Service
Entité racine

GB

Tickets

+ Créer un ticket

Nouveau

0

En cours (Planifié)

0

En attente

0

Résolu

0

Clos

0

Supprimé

0

FLUX RSS PUBLICS

Self-Service
Entité racine

GB

BETETA GABRIEL

Self-Service <

Entité racine

Français

Aide

À propos

Mes préférences

Déconnexion