

Table des matières :

Présentation	1
Prérequis	2
Installation de GLPI	4
Intégration des utilisateurs AD via LDAPS	11

Présentation

GLPI (*Gestionnaire Libre de Parc Informatique*) est une solution open-source de gestion des services informatiques (ITSM). Il permet aux entreprises et administrations de gérer leur parc informatique, leurs interventions et leur helpdesk de manière centralisée.

Principales fonctionnalités :

- **Gestion des actifs** : Inventaire des matériels, logiciels et périphériques.
- **Helpdesk** : Système de ticketing pour le support technique.
- **Gestion financière** : Suivi des contrats, licences et garanties.
- **Gestion des utilisateurs** : Intégration avec Active Directory et gestion des droits d'accès.
- **Tableaux de bord et reporting** : Analyse des données pour optimiser la gestion IT.

GLPI est largement utilisé par les DSI et les administrateurs systèmes pour améliorer la gestion et la maintenance du SI tout en automatisant de nombreuses tâches.

Prérequis

Avoir une machine Debian 12 fonctionnelle et à jour, avec apache2 de préinstallé.

```
apt install apache2
```

Installation de php non disponible par défaut sous Debian :

```
apt install ca-certificates apt-transport-https software-properties-common wget curl lsb-release -y
```

```
curl -sSL https://packages.sury.org/php/README.txt | bash -x
```

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

```
apt install php8.2 libapache2-mod-php8.2
```

```
systemctl restart apache2
```

Installation de mariaDB :

```
apt install mariadb-server
```

```
mysql_secure_installation
```

Une série de questions va être posé pour la configuration de la base de donnée, puis une fois l'installation terminée un message apparait :

```
All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.
```

```
Thanks for using MariaDB!
```

Créons la base de données pour GLPI :

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

```
root@srv-glpi:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

```
create database glpi;
```

```
MariaDB [(none)]> create database glpi ;
Query OK, 1 row affected (0,001 sec)
```

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

```
MariaDB [(none)]> create user 'glpi'@'localhost' identified by 'glpi';
Query OK, 0 rows affected (0,002 sec)
```

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

```
MariaDB [(none)]> grant all privileges on glpi.* to 'glpi'@'localhost' with grant option;
Query OK, 0 rows affected (0,001 sec)
```

```
flush privileges;
```

```
quit
```

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> quit
Bye
```

La base de données de glpi a bien été configurée.

Installation de GLPI

Téléchargeons GLPI :

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz
tar xvf glpi-10.0.18.tgz
```

```
root@srv-glpi:~# ls
glpi-10.0.18.tgz
root@srv-glpi:~# tar xvf glpi-10.0.18.tgz
```

Déplaçons le dossier « glpi » dans notre dossier html, et changeons les autorisations :

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

```
root@srv-glpi:~# ls
glpi glpi-10.0.18.tgz
root@srv-glpi:~# mv glpi /var/www/html/glpi
root@srv-glpi:~# chown -R www-data:www-data /var/www/html/glpi/
root@srv-glpi:~# chmod -R 755 /var/www/html/glpi/
```

Ajouter les modules PHP suivants qui sont nécessaires à GLPI :

```
apt install php8.2-curl php8.2-gd php8.2-mbstring php8.2-zip php8.2-xml php8.2-ldap php8.2-intl php8.2-mysql php8.2-dom php8.2-simplexml php-json php8.2-phpdbg php8.2-cgi
```

Enfin redémarrons apache :

```
systemctl restart apache2
```

Nous pouvons maintenant nous connecter sur l'interface web de GLPI pour lancer l'installation à l'adresse http://ip_serveur_glpi/glpi :



Vérifions que tout les packages sont bien installés :

GLPI SETUP
Étape 0
Vérification de la compatibilité de votre environnement avec l'exécution de GLPI

TESTS EFFECTUÉS	RESULTATS
Requis Parser PHP	✓
Requis Configuration des sessions	✓
Requis Mémoire allouée	✓
Requis mysql extension	✓
Requis Extensions du noyau de PHP	✓
Requis curl extension <i>Requis pour l'accès à distance aux ressources (requêtes des agents d'inventaire, Marketplace, flux RSS, ...).</i>	✓
Requis gd extension <i>Requis pour le traitement des images.</i>	✓
Requis intl extension <i>Requis pour l'internationalisation.</i>	✓
Requis zlib extension <i>Requis pour la gestion de la communication compressée avec les agents d'inventaire, l'installation de paquets gzip à partir du Marketplace et la génération de PDF.</i>	✓
Requis Libsodium ChaCha20-Poly1305 constante de taille <i>Activer l'utilisation du cryptage ChaCha20-Poly1305 requis par GLPI. Il est fourni par libsodium à partir de la version 1.0.12.</i>	✓
Requis Permissions pour les fichiers de log	✓
Requis Permissions pour les dossiers de données	✓
Sécurité Version de PHP maintenue <i>Une version de PHP maintenue par la communauté PHP devrait être utilisée pour bénéficier des correctifs de sécurité et de bogues de PHP.</i>	✓
Sécurité Configuration sécurisée du dossier racine du serveur web <i>La configuration du dossier racine du serveur web devrait être "/var/www/html/glpi/public" pour s'assurer que les fichiers non publics ne peuvent être accessibles. La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.</i>	▲
Sécurité Emplacement sécurisé pour les dossiers de données <i>Les dossiers de données de GLPI devraient être placés en dehors du dossier racine web. Ceci peut être effectué en redéfinissant les constantes correspondantes. Référez-vous à la documentation d'installation pour plus de détails. Les dossiers suivants devraient être placés en dehors de "/var/www/html/glpi": - "/var/www/html/glpi/files" ("GLPL_VAR_DIR") Vous pouvez ignorer cette suggestion si le dossier racine de votre serveur web est "/var/www/html/glpi/public".</i>	▲
Sécurité Configuration de sécurité pour les sessions <i>Permet de s'assurer que la sécurité relative aux cookies de session est renforcée. La directive PHP "session.cookie_httponly" devrait être définie à "on" pour prévenir l'accès aux cookies depuis les scripts côté client.</i>	▲
Suggéré Taille d'entier maximal de PHP <i>Le support des entiers 64 bits est nécessaire pour les opérations relatives aux adresses IP (inventaire réseau, filtrage des clients API, ...).</i>	✓
Suggéré exif extension <i>Renforcer la sécurité de la validation des images.</i>	✓
Suggéré ldap extension <i>Active l'utilisation de l'authentification à un serveur LDAP distant.</i>	✓
Suggéré openssl extension <i>Active l'envoi de courriel en utilisant SSL/TLS.</i>	✓
Suggéré Extensions PHP pour le marketplace <i>Permet le support des formats de paquets les plus communs dans le marketplace. Les extensions suivantes sont installées : Phar, zip. Les extensions suivantes ne sont pas présentes : bz2.</i>	▲
Suggéré Zend OPcache extension <i>Améliorer les performances du moteur PHP.</i>	✓
Suggéré Extensions émulées de PHP <i>Améliorer légèrement les performances.</i>	✓
Suggéré Permissions pour le répertoire du marketplace <i>Active l'installation des plugins à partir du Marketplace.</i>	✓

Voulez-vous continuer ?

Continuer > Réessayer

Rentrer les informations de l'utilisateur glpi configuré plus tôt :



The screenshot shows the 'GLPI SETUP' interface at 'Étape 1'. The title is 'Configuration de la connexion à la base de données'. It contains three input fields: 'Serveur SQL (MariaDB ou MySQL)' with the value 'localhost', 'Utilisateur SQL' with the value 'glpi', and 'Mot de passe SQL' with masked characters '****'. A yellow 'Continuer >' button is at the bottom.

Puis sélectionner la base de données « glpi » :



The screenshot shows the 'GLPI SETUP' interface at 'Étape 2'. The title is 'Test de connexion à la base de données'. A green checkmark and the text 'Connexion à la base de données réussie' are displayed. Below, it asks 'Veillez sélectionner une base de données :'. There are two radio buttons: 'Créer une nouvelle base ou utiliser une base existante :' (unselected) and 'glpi' (selected). A yellow 'Continuer >' button is at the bottom.

Attendre la fin de l'installation de la BDD :



The screenshot shows the 'GLPI SETUP' interface at 'Étape 3'. The title is 'Initialisation de la base de données.'. The text 'OK - La base a bien été initialisée' is displayed. A yellow 'Continuer >' button is at the bottom.

Une fois terminé, nous pouvons accéder à l'interface web via l'utilisateur glpi :

Voici l'interface web de GLPI, (ne pas oublier de changer le mot de passe par défaut) :

Pour accéder à toutes les fonctionnalités de GLPI, il faut s'enregistrer sur le site : <https://services.glpi-network.com/registration> et récupérer la clé d'enregistrement :

Puis la coller dans notre serveur GLPI, sous Configuration > Générale > GLPI Network :

Nous avons maintenant accès à toutes les fonctionnalités et plugins :

The screenshot displays the GLPI Plugins Marketplace interface. On the left is a dark blue navigation sidebar with categories like 'Parc', 'Assistance', 'Gestion', 'Outils', 'Administration', 'Configuration', 'Intitulés', 'Composants', 'Notifications', 'Niveaux de services', 'Générale', 'Utilité des champs', 'Actions automatiques', 'Authentification', 'Collecteurs', 'Liens externes', and 'Plugins'. The main content area is titled 'Découvrir' and shows a grid of 14 plugins. Each plugin card includes an icon, a title, a brief description, a star rating, and version information. The plugins shown are: Accounts inventory, Activity, ActualTime, Additional Alerts, Advanced GLPI dashboards, advancedplanning, Airwatch connector, anonymize, Appliances Dashboard, Appliances Inventory, ApprovalByMail, and Apps structure inventory. At the bottom of the grid, there is a pagination bar showing '1 2 ... 8 9 >' and the text 'Plugins 104'.

Intégration des utilisateurs AD via LDAPS

Pour intégrer nos utilisateurs AD à GLPI en utilisant une connexion sécurisée LDAPS, il faut préalablement créer une autorité de certifications sur notre serveur AD, puis créer le certificat LDAPS. Enfin un compte AD en lecture seule est nécessaire pour récupérer les informations des utilisateurs.

Dans notre cas nous avons créé l'utilisateur « vmail » pour intégrer nos utilisateurs AD à notre serveur mail, nous allons donc utiliser cet utilisateur.

Une fois le certificat créé, nous l'envoyons sur notre serveur GLPI, via la commande scp sur notre invite de commande de notre serveur AD :

```
scp C:/ldaps.cer thomas@172.10.11.243:/tmp/
```

```
C:\Users\administrateur>scp C:/ldaps.cer thomas@172.10.11.243:/tmp/
thomas@172.10.11.243's password:
ldaps.cer                               100% 1715    1.7KB/s   00:00
```

Sur notre serveur GLPI, il faut convertir notre fichier de certificat en .crt grâce à openssl :

```
cd /tmp/
openssl x509 -inform der -in ldaps.cer -out ldaps.crt
```

Puis copier le certificat dans le dossier ca-certificates :

```
cp ldaps.crt /usr/local/share/ca-certificates
```

Enfin mettons à jour les certificats :

```
update-ca-certificates
```

Installons le package ldap pour tester la liaison :

```
apt-get install ldap-utils
```

Testons avec la commande ldapsearch, ici j'utilise l'utilisateur « vmail » et je fais une recherche dans l'ou où sont stocké mes utilisateurs AD :

```
ldapsearch -x -H ldaps://srv-dc1.algara.at:636 -D 'vmail' -W -b 'ou=_algara,dc=algara,dc=at'
```

La commande doit renvoyer les informations des utilisateurs :

```
# Anne Bouchard, Direction, _algara, algara.at
dn: CN=Anne Bouchard,OU=Direction,OU=_algara,DC=algara,DC=at
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Anne Bouchard
sn: Bouchard
description: Directeur1
givenName: Anne
distinguishedName: CN=Anne Bouchard,OU=Direction,OU=_algara,DC=algara,DC=at
```

Rendons-nous sur l'interface web de notre GLPI. Accéder à la configuration d'un annuaire LDAP dans la section « Authentification » présente dans le menu « Configuration » afin d'ajouter un nouvel annuaire ou de modifier un annuaire déjà déclaré, dans le cas où vous souhaitez faire évoluer une configuration existante.

The screenshot shows the configuration page for an LDAP directory in GLPI. The page title is 'Annuaire LDAP - AD algara.at'. On the left, there is a sidebar menu with options: Tester, Utilisateurs, Groupes, Informations avancées, Réplicats, Historique (selected, showing 10 items), and Tous. The main content area contains the following fields:

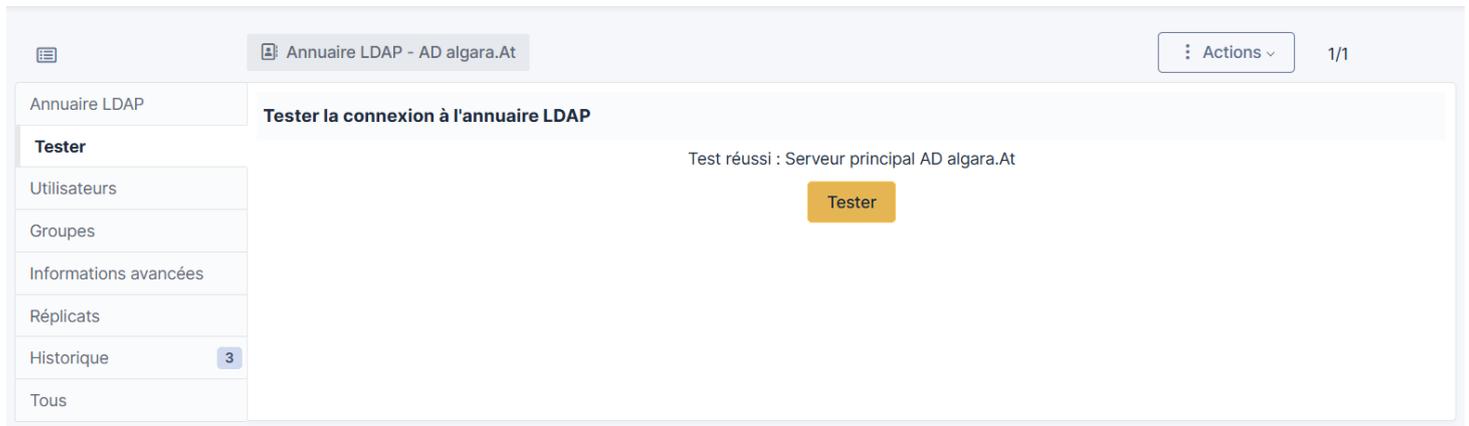
- Nom: AD algara.at
- Dernière modification: 2025-02-28 10:55
- Serveur par défaut: Oui
- Actif: Oui
- Serveur: ldaps://srv-dc1.algara.at
- Port (par défaut 389): 636
- Filtre de connexion: (&(objectClass=user)(objectCategory=person)!((userAccountControl:1.2.840.113556.1.4.803:=2)))
- BaseDN: OU=_algara,DC=algara,DC=at
- Utiliser bind: Oui
- DN du compte (pour les connexions non anonymes): CN=vmail,DC=algara,DC=at
- Mot de passe du compte (pour les connexions non anonymes): Effacer
- Champ de l'identifiant: samaccountname
- Champ de synchronisation: (empty)

At the bottom right, there are two buttons: 'Supprimer définitivement' (red) and 'Sauvegarder' (yellow).

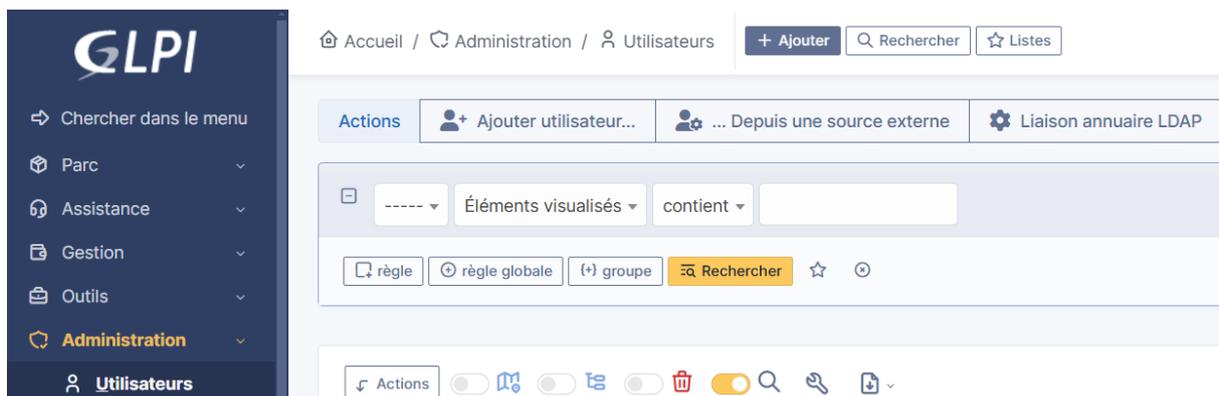
Voici le filtre de connexion utilisé :

```
(&(objectClass=user)(objectCategory=person)!((userAccountControl:1.2.840.113556.1.4.803:=2)))
```

Dans l'onglet « Tester » vérifions que la connexion fonctionne :



Dans le menu, « Administration » > « Utilisateurs » cliquer sur « Liaison annuaire LDAP »



Cliquer sur importation de nouveaux utilisateurs :



Cliquer sur rechercher, les utilisateurs de l'AD doivent apparaitre :

Rechercher

Affichage (nombre d'éléments) 10000 De 1 à 19 sur 19

Actions

<input type="checkbox"/> UTILISATEURS	DERNIÈRE MISE À JOUR DANS L'ANNUAIRE LDAP
<input type="checkbox"/> tthivierge	2025-02-27 09:14
<input type="checkbox"/> tbergeron	2025-02-27 09:14
<input type="checkbox"/> rlachapelle	2025-02-27 09:15
<input type="checkbox"/> ravare	2025-02-27 09:13
<input type="checkbox"/> psabourin	2025-02-27 09:16
<input type="checkbox"/> prod-poste3	2025-02-22 10:54
<input type="checkbox"/> olouineaux	2025-02-27 09:12
<input type="checkbox"/> mverreau	2025-02-27 09:10
<input type="checkbox"/> llebrun	2025-02-27 09:15
<input type="checkbox"/> llabelle	2025-02-27 09:10
<input type="checkbox"/> glangelier	2025-02-27 09:12
<input type="checkbox"/> fferland	2025-02-26 13:10
<input type="checkbox"/> fchauvin	2025-02-27 09:15

Enfin sélectionné tous les utilisateurs, cliquer sur « action » puis « importer » :

Actions

Action **Importer** ▼

Envoyer

Un message d'information doit apparaître :



Les utilisateurs peuvent maintenant s'authentifier sur avec leurs identifiants Windows.