GLPI 11

Liaison avec Active Directory

Import et authentification des utilisateurs

Domaine AD : mvgroup.local
Contrôleur de domaine : 10.0.200.2
Serveur GLPI : 10.0.0.50 (glpi.mvgroup.local)
Protocole : LDAP (port 389)

Rédigé par : Samuel — Avril 2026

1. Introduction et prérequis

Ce document décrit la procédure complète pour lier GLPI 11 à un annuaire Active Directory afin de permettre l'import et l'authentification des utilisateurs via le protocole LDAP.

1.1 Environnement

Composant	Valeur
Domaine Active Directory	mvgroup.local
Contrôleur de domaine	10.0.200.2
Serveur GLPI	10.0.0.50 — glpi.mvgroup.local
Version GLPI	11.0.4
Protocole LDAP	LDAP — Port 389
Compte de service	CN=Service GLPI,OU=Comptes de service,OU=MV GROUP,DC=mvgroup,DC=local

1.2 Prérequis

- GLPI 11 installé et fonctionnel
- Extension PHP php8.4-ldap installée sur le serveur GLPI
- Accès administrateur au contrôleur de domaine Windows
- Port 389 (LDAP) ouvert entre le serveur GLPI et le contrôleur de domaine
- Compte de service créé dans l'Active Directory

⚠ *Si le port 389 est bloqué par le pare-feu Windows du DC, la connexion LDAP échouera. Vérifiez les règles de pare-feu.*

2. Création du compte de service dans l'AD

Pour chaque application nécessitant une liaison LDAP, il est recommandé de créer un compte dédié avec des droits minimaux (lecture seule). Ce compte ne doit jamais avoir de droits administrateur.

2.1 Créer l'OU Comptes de service

Dans Utilisateurs et ordinateurs Active Directory :

- Clic droit sur l'OU MV GROUP
- Nouveau → Unité d'organisation
- Nom : Comptes de service
- Laisser coché : Protéger contre la suppression accidentelle
- Cliquer OK

2.2 Créer le compte svc-glpi

Clic droit sur l'OU Comptes de service → Nouveau → Utilisateur, remplissez :

Champ	Valeur
Prénom	Service
Nom	GLPI
Nom d'ouverture de session	svc-glpi
Mot de passe	Mot de passe fort (ex: Azerty123)
Le mot de passe n'expire jamais	Coché
L'utilisateur ne peut pas changer le mot de passe	Coché
L'utilisateur doit changer le mot de passe	Décoché

> ⚠ *Ce compte peut ouvrir des sessions sur les machines du domaine. Il est fortement recommandé de créer une GPO pour interdire l'ouverture de session interactive de ce compte.*

2.3 Récupérer le DN exact du compte

Dans l'AD, activez Affichage → Fonctionnalités avancées, puis :

- Clic droit sur Service GLPI → Propriétés
- Onglet Editeur d'attributs
- Copier la valeur de l'attribut distinguishedName

Le DN du compte de service dans notre environnement est :

```
CN=Service GLPI,OU=Comptes de service,OU=MV GROUP,DC=mvgroup,DC=local
```

3. Vérifier l'extension PHP LDAP

Avant de configurer GLPI, vérifiez que l'extension php8.4-ldap est bien installée sur le serveur GLPI :

```
php -m | grep ldap
# Doit retourner : ldap
```

Si elle n'est pas installée :

```
sudo apt install -y php8.4-ldap
sudo systemctl restart php8.4-fpm.service
sudo systemctl restart apache2
```

3.1 Tester la connexion LDAP depuis le serveur

Avant de configurer GLPI, testez la connexion LDAP directement depuis le terminal du serveur GLPI :

```
# Installer ldap-utils si nécessaire
sudo apt-get install -y ldap-utils

# Tester la connexion
ldapsearch -x -H ldap://10.0.200.2 \
  -D "CN=Service GLPI,OU=Comptes de service,OU=MV
GROUP,DC=mvgroup,DC=local" \
  -w "Azerty123" \
  -b "DC=mvgroup,DC=local" \
  "(sAMAccountName=svc-glpi)"
```

✅ Si la commande retourne des informations sur l'utilisateur, la connexion LDAP fonctionne.

⚠️ *Si vous obtenez Invalid credentials (49), vérifiez le DN et le mot de passe du compte de service.*

4. Configuration de la liaison LDAP dans GLPI

Connectez-vous à GLPI avec le compte Super-Admin (glpi), puis accédez à :

```
Configuration → Authentification → Annuaires LDAP → + Ajouter
```

4.1 Utiliser la préconfiguration Active Directory

Sur la page d'ajout, GLPI propose des préconfigurations. Cliquez sur Active Directory pour pré-remplir automatiquement :

- Le filtre de connexion
- Le champ de l'identifiant (sAMAccountName)
- Le champ de synchronisation (objectGUID)

ℹ️ *Cette étape évite les erreurs de saisie manuelle pour les paramètres techniques AD.*

4.2 Remplir les paramètres de connexion

Champ GLPI	Valeur à saisir
Nom	mvgroup.local
Serveur par défaut	Oui
Activé	Oui
Serveur	10.0.200.2
Port	389
BaseDN	DC=mvgroup,DC=local
Utiliser bind	Oui
DN du compte	CN=Service GLPI,OU=Comptes de service,OU=MV GROUP,DC=mvgroup,DC=local
Mot de passe du compte	Azerty123
Champ de l'identifiant	sAMAccountName
Champ de synchronisation	objectGUID

⚠️ *Le BaseDN DC=mvgroup,DC=local est la racine de recherche. Pour limiter la recherche à une OU spécifique, utilisez par exemple : OU=Utilisateurs,OU=MV GROUP,DC=mvgroup,DC=local*

Cliquez sur + Ajouter. GLPI effectue un test automatique lors de l'ajout.

4.3 Configuration des groupes

Dans la fiche de l'annuaire, onglet Groupes, configurez :

Champ	Valeur
Type de recherche	Dans les utilisateurs & groupes
Filtre pour la recherche dans les groupes	(objectClass=group)
Attribut des groupes contenant les utilisateurs	member
Utiliser le DN pour la recherche	Oui

4.4 Configuration des attributs utilisateurs

Dans l'onglet Utilisateurs, vérifiez ou complétez les correspondances entre les champs GLPI et les attributs AD :

Champ GLPI	Attribut AD
Nom de famille	sn
Prénom	givenname
E-mail	mail
Téléphone	telephonenumber
Téléphone mobile	mobile
Titre	title
Lieu	physicalDeliveryOfficeName

4.5 Informations avancées

Dans l'onglet Informations avancées, renseignez :

Champ	Valeur
Nom de domaine pour l'outil d'inventaire	mvgroup.local
Utiliser TLS	Non (LDAP simple)
Timeout	10

Le champ Nom de domaine pour l'outil d'inventaire permet de lier automatiquement les machines remontées par l'agent GLPI aux utilisateurs AD.

5. Tester la liaison LDAP

Dans la fiche de l'annuaire, cliquez sur l'onglet Tester. GLPI effectue plusieurs vérifications :

Test	Résultat attendu
Connexion au serveur LDAP	Succès
Authentification avec le compte de service	Succès
Recherche dans le BaseDN	Succès
Test global	Test réussi

6. Import des utilisateurs depuis l'AD

L'import des utilisateurs se fait manuellement depuis l'interface GLPI ou via une tâche planifiée (cron).

6.1 Import manuel via l'interface

Accédez à :

```
Administration → Utilisateurs → Liaison annuaire LDAP → Importation de nouveaux utilisateurs
```

Puis :

- Cliquer sur Rechercher pour lister les utilisateurs disponibles dans l'AD
- Sélectionner les utilisateurs à importer (ou cocher tout)
- Cliquer sur Actions → Importer → Envoyer

✅ Les utilisateurs importés apparaissent dans Administration → Utilisateurs avec la source d'authentification mvgroup.local.

6.2 Synchronisation des utilisateurs existants

Pour mettre à jour les utilisateurs déjà importés (changement de nom, email, groupe...) :

```
Administration → Utilisateurs → Liaison annuaire LDAP → Synchronisation d'utilisateurs existants
```

6.3 Automatiser l'import avec une tâche cron

Pour automatiser l'import et la synchronisation, utilisez les commandes en ligne de GLPI :

```
# Import des nouveaux utilisateurs
php /var/www/glpi/bin/console glpi:ldap:synchronize_users --action=import

# Synchronisation des utilisateurs existants
php /var/www/glpi/bin/console glpi:ldap:synchronize_users --action=sync
```

Ajoutez une entrée cron pour automatiser l'import toutes les nuits :

```
sudo crontab -e

# Ajouter cette ligne (import toutes les nuits à 2h00) :
0 2 * * * php /var/www/glpi/bin/console glpi:ldap:synchronize_users --
action=import --no-interaction
```

7. Connexion avec un compte Active Directory

Une fois les utilisateurs importés, ils peuvent se connecter à GLPI avec leurs identifiants AD.

7.1 Procédure de connexion

Sur la page de connexion GLPI (http://glpi.mvgroup.local) :

Champ	Valeur
Identifiant	Le sAMAccountName de l'utilisateur AD (ex: user2)
Mot de passe	Le mot de passe AD de l'utilisateur
Login source	mvgroup.local (sélectionner dans la liste)

ℹ️ *Par défaut, les utilisateurs importés depuis l'AD ont le profil Self-Service qui donne accès au portail de déclaration de tickets uniquement.*

7.2 Modifier le profil d'un utilisateur

Pour donner des droits supplémentaires à un utilisateur AD :

- Administration → Utilisateurs → cliquer sur l'utilisateur
- Onglet Habilitations → Ajouter une habilitation
- Sélectionner le profil souhaité (Technicien, Admin, etc.) et l'entité

Profil GLPI	Droits
Self-Service	Portail utilisateur, création de tickets uniquement
Observateur	Lecture seule sur les tickets et le parc
Technicien	Gestion des tickets, accès au parc
Superviseur	Gestion des équipes et des statistiques
Admin	Administration complète sauf configuration globale
Super-Admin	Accès complet à toutes les fonctionnalités

8. Récapitulatif des étapes

Étape	Action	Statut
1	Créer l'OU Comptes de service dans l'AD	
2	Créer le compte svc-glpi (Service GLPI)	
3	Vérifier l'extension php8.4-ldap	
4	Tester la connexion LDAP avec ldapsearch	
5	Configurer l'annuaire LDAP dans GLPI	
6	Configurer les groupes et attributs utilisateurs	
7	Tester la liaison depuis l'onglet Tester	
8	Importer les utilisateurs AD dans GLPI	
9	Vérifier la connexion avec un compte AD	

Ressources utiles

- Documentation officielle GLPI : https://glpi-install.readthedocs.io/
- Tutoriel de référence : https://rdr-it.com/glpi-11-liaison-avec-active-directory-pour-authentifier-les-utilisateurs/
- Commandes GLPI CLI LDAP : https://glpi-install.readthedocs.io/en/latest/command-line.html#ldap-synchonization