

Documentation : Liaison LDAP entre Debian (GLPI) et Windows Server 2022 (Active Directory)

GLPI 10

Configurer une remontée LDAP



SOMMAIRE

LDAP

1. QU'EST-CE QUE « LDAP » ?
2. CONFIGURER LDAP SUR GLPI 10
3. IMPORTATION DES UTILISATEURS DE L'AD DANS GLPI
4. CONNEXION A GLPI 10 AVEC UN UTILISATEUR DE L'AD

1. Introduction

Cette documentation décrit en détail la procédure pour configurer une liaison LDAP entre un serveur Debian hébergeant GLPI et un serveur Windows Server 2022 contenant un Active Directory (AD). L'objectif est de permettre l'authentification des utilisateurs GLPI via AD.

2. Définition des termes

- **LDAP (Lightweight Directory Access Protocol)** : Protocole permettant d'interroger et de modifier les services d'annuaire, utilisé pour l'authentification et la gestion des utilisateurs.
- **Active Directory (AD)** : Service d'annuaire développé par Microsoft permettant de centraliser l'authentification et la gestion des ressources réseau.
- **GLPI (Gestion Libre de Parc Informatique)** : Application de gestion de parc informatique incluant des fonctionnalités de helpdesk et d'inventaire.
- **Base DN (Distinguished Name)** : Référence hiérarchique des objets dans un annuaire LDAP.
- **LDAPS (LDAP Secure)** : Version sécurisée de LDAP utilisant SSL/TLS pour chiffrer les communications.

3. Prérequis

Avant de commencer, assurez-vous que :

- GLPI est installé et fonctionnel sur votre serveur Debian.
- Un Active Directory est configuré et fonctionnel sur Windows Server 2022.
- Un utilisateur dédié à l'authentification LDAP est créé dans l'AD.
- Les ports **389** (LDAP) ou **636** (LDAPS) sont ouverts sur le serveur AD.

Installation des paquets nécessaires sur Debian

- `sudo apt update`
- `sudo apt install php-ldap ldap-utils`

4. Ouverture des ports LDAP sur Windows Server 2022

Par défaut, **LDAP (389)** et **LDAPS (636)** peuvent être bloqués par le pare-feu Windows.

1. Ouvrir les ports sur le pare-feu Windows

1. Ouvrir **PowerShell en administrateur** et exécuter :

- `New-NetFirewallRule -DisplayName "Open LDAP 389" -Direction Inbound -Protocol TCP -LocalPort 389 -Action Allow`

```
PS C:\Users\Administrateur> New-NetFirewallRule -DisplayName "Open LDAP 389" -Direction Inbound -Protocol TCP -LocalPort 389 -Action Allow

Name                : {763e8740-c7cf-4cc0-8c11-4db8b157686b}
DisplayName          : Open LDAP 389
Description          :
DisplayGroup        :
Group               :
Enabled             : True
Profile            : Any
Platform           : {}
Direction          : Inbound
Action             : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner              :
PrimaryStatus       : OK
Status              : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus   : NotApplicable
PolicyStoreSource   : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId        :
```

- `New-NetFirewallRule -DisplayName "Open LDAPS 636" -Direction Inbound -Protocol TCP -LocalPort 636 -Action Allow`

```
PS C:\Users\Administrateur> New-NetFirewallRule -DisplayName "Open LDAPS 636" -Direction Inbound -Protocol TCP -LocalPort 636 -Action Allow

Name                : {c6b58756-3659-472b-a40b-500baa4f52c9}
DisplayName          : Open LDAPS 636
Description          :
DisplayGroup        :
Group               :
Enabled             : True
Profile            : Any
Platform           : {}
Direction          : Inbound
Action             : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner              :
PrimaryStatus       : OK
Status              : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus   : NotApplicable
PolicyStoreSource   : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId        :
```

2. Vérifier si les règles sont bien appliquées :

- `Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*LDAP*" }`

```
PS C:\Users\Administrateur> Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*LDAP*" }

Name                : ADDS-LDAP-TCP-In
DisplayName          : Contrôleur de domaine Active Directory - LDAP (TCP-entrant)
Description          : Règle de trafic entrant pour le service de contrôleur de domaine Active Directory autorisant le
DisplayGroup        : trafic LDAP distant. [TCP389]
Group               : Active Directory Domain Services
Enabled             : True
Profile            : @FirewallAPI.dll,-37601
Platform           : {}
Direction          : Inbound
Action             : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping  : False
LocalOnlyMapping    : False
Owner              :
PrimaryStatus       : OK
Status              : La règle a été analysée à partir de la banque. (65536)
```

2. Vérifier si LDAP répond

Depuis votre serveur Debian, lancez cette commande pour tester si les ports sont ouverts :

- `telnet 192.168.20.10 389`

```
root@srv-web:~# telnet 192.168.20.10 389
Trying 192.168.20.10...
Connected to 192.168.20.10.
```

5. Test de la connexion LDAP

Avant de configurer GLPI, testez la connexion LDAP entre Debian et Windows Server 2022 :

- `ldapsearch -x -h AD_IP -D "Administrateur@Domaine.local" -W -b "dc=Domaine,dc=local"`

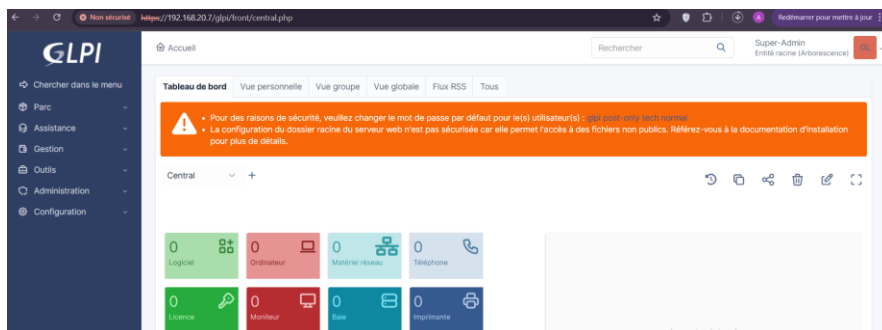
```
root@srv-web:~# ldapsearch -x -h 192.168.20.10 "administrateur@formation.lan" -W -b "dc=formation,dc=lan"
ldapsearch: unrecognized option -
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter          RFC 4515 compliant LDAP search filter
  attributes       whitespace-separated list of attribute descriptions
                   which may include:
                   1.1 no attributes
                   *   all user attributes
                   +   all operational attributes
Search options:
-a deref          one of never (default), always, search, or find
-A               retrieve attribute names only (no values)
-b basedn         base dn for search
-c               continuous operation mode (do not stop on errors)
-E [!]<ext>[=<extparam>] search extensions (! indicates criticality)
                  [!]accountUsability      (NetScape Account usability)
                  [!]domainScope           (domain scope)
                  [!]dontUseCopy           (Don't Use Copy)
                  [!]mv=<filter>           (RFC 3876 matched values filter)
                  [!]pr=<size>[/prompt|noprompt] (RFC 2696 paged results/prompt)
```

- une liste d'objets provenant de l'AD.

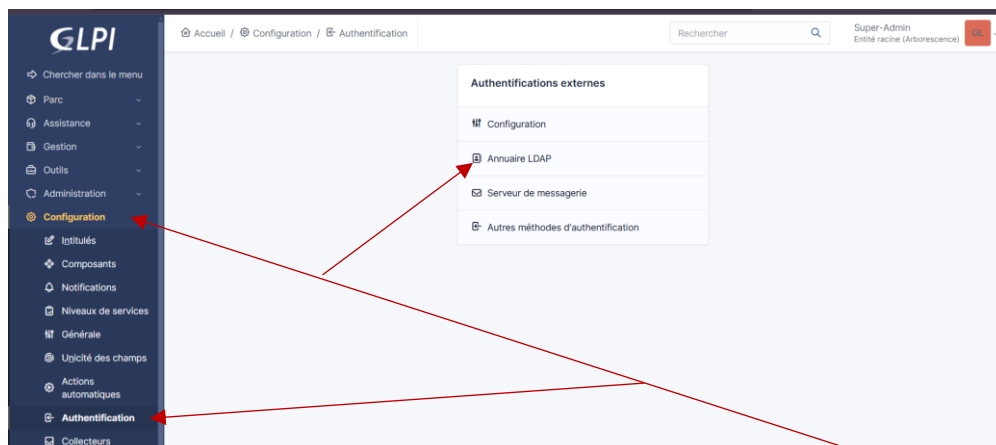
6. Configuration LDAP dans GLPI

Accès aux paramètres LDAP

1. GLPI en tant qu'administrateur.



2. Allez dans **Configuration** → **Authentification** → **Annuaire LDAP**.



3. Ajoutez un serveur LDAP avec les paramètres suivants :

Accueil / Configuration / Authentification / Annuaire LDAP + Ajouter Rechercher Rechercher Super-Admin Entité racine (Arborescence)

Nouvel élément - Annuaire LDAP

Préconfiguration Active Directory / OpenLDAP / Valeurs par défaut

Nom **Nom complet de votre serveur**

Serveur par défaut Actif

Serveur Port (par défaut 389)

Filtre de connexion

BaseDN

Utiliser bind

DN du compte (pour les connexions non anonymes)

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

Champ de l'identifiant Commentaires

Champ de synchronisation

+ Ajouter

4. Testez la connexion et enregistrez.

Actions

NOM	SERVEUR	DERNIÈRE MODIFICATION	ACTIF
<input type="checkbox"/> AD-GLPI	192.168.20.10	2025-03-04 12:32	Non

20 lignes / page De 1 à 1 sur 1 lignes

Information
Élément ajouté : AD-GLPI
Test réussi

7. Activer la synchronisation des utilisateurs

1. Administration → Utilisateurs.

GLPI

Chercher dans le menu

- Parc
- Assistance
- Gestion
- Outils
- Administration
- Utilisateurs**

Accueil / Administration / Utilisateurs + Ajouter Rechercher Listes

Actions + Ajouter utilisateur... ... Depuis une source externe Liaison annuaire LDAP

Éléments visualisés contient

régle règle globale groupe Rechercher

Actions

- Cliquez sur « Importation de nouveaux utilisateurs »
- Cliquez sur « Mode expert » (en haut à droite de la fenêtre) et sur « Rechercher » :

Importation de nouveaux utilisateurs Mode expert

☐ Activer le filtrage par date

Critère de recherche pour les utilisateurs

Identifiant Champ de synchronisation (objectguid)

Importation de nouveaux utilisateurs Mode simplifié

BaseDN

Filtre de recherche des utilisateurs

Rechercher

2. Les utilisateurs de l'AD s'affichent, sélectionnez-les :

Affichage (nombre d'éléments) 20 ▼ De 1 à 1 sur 1

Actions

<input type="checkbox"/> CHAMP DE SYNCHRONISATION	UTILISATEURS	DERNIÈRE MISE À JOUR DANS L'ANNUAIRE LDAP
<input checked="" type="checkbox"/> 95f23ebd-69d2-4dcc-abb5-2940db2667cb	ldap_glpi	2025-03-04 11:27
<input type="checkbox"/> Champ de synchronisation	Utilisateurs	Dernière mise à jour dans l'annuaire LDAP

Actions

Affichage (nombre d'éléments) 20 ▼ De 1 à 1 sur 1

3. Cliquez le bouton « Actions », sélectionnez « Importer » et cliquez « Envoyer » :

Accueil / Administration / Utilisateurs

Actions

Action

Rechercher

Affichage (nombre d'éléments) 20 ▼ De 1 à 1 sur 1

Actions

<input type="checkbox"/> CHAMP DE SYNCHRONISATION	UTILISATEURS	DERNIÈRE MISE À JOUR DANS L'ANNUAIRE LDAP
<input checked="" type="checkbox"/> 95f23ebd-69d2-4dcc-abb5-2940db2667cb	ldap_glpi	2025-03-04 11:27
<input type="checkbox"/> Champ de synchronisation	Utilisateurs	Dernière mise à jour dans l'annuaire LDAP

Actions

Affichage (nombre d'éléments) 20 ▼ De 1 à 1 sur 1

The screenshot shows the GLPI Administration interface. On the left is a sidebar with navigation links: Administration, Utilisateurs, Groupes, Entités, Règles, Dictionnaires, Profils, and File d'attente des. The main area displays a table of 'Identifiants' (Identifiers) with columns: IDENTIFIANT, NOM DE FAMILLE, COURRIELS, TÉLÉPHONE, LIEU, and ACTIF. The table contains four entries: 'glpi', 'glpi-system', 'ldap_glpi' (highlighted with a red arrow), and 'normal'. Below the table, an 'Information' message box indicates that the element 'ldap_glpi' has been successfully added.

IDENTIFIANT	NOM DE FAMILLE	COURRIELS	TÉLÉPHONE	LIEU	ACTIF
glpi					Oui
glpi-system	Support				Oui
ldap_glpi					Oui
normal					Oui

Information ✕
Élément ajouté : ldap_glpi
Opération réalisée avec succès

8. Conclusion

Une fois la liaison LDAP configurée, les utilisateurs de l'Active Directory pourront se connecter à GLPI avec leurs identifiants AD, simplifiant ainsi la gestion des accès.