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

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 Allo


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 All


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
                                trafic LDAP distant. [TCP389]
DisplayGroup                  : Active Directory Domain Services
Group                         : @FirewallAPI.dll,-37601
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)
```

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"`

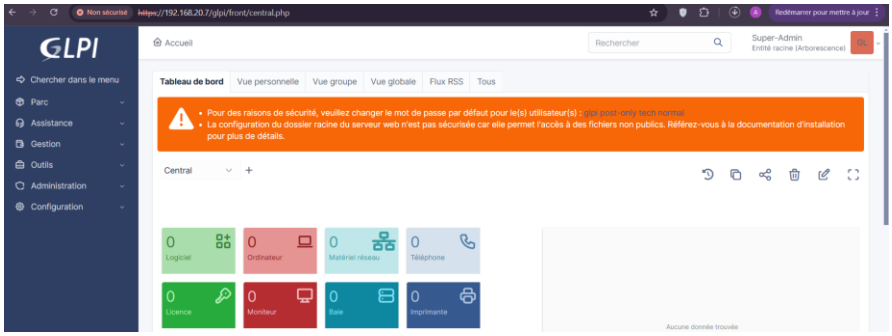
```
root@srv-web:~# ldapsearch -x -h 192.168.20.10 "administrateur@formation.lan" -W -b "dc=formation,dc=lan"
ldapsearch: unrecognized option -
usage: ldapsearch [options] [filter [attributes...]]
where:
  filter        RFC 4515 compliant LDAP search filter
  attributes    whitespace-separated list of 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.

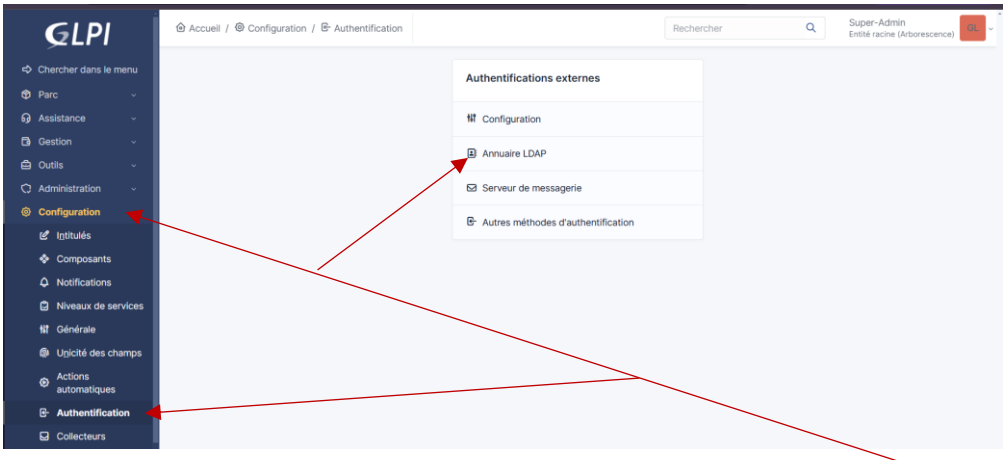
---

6. Configuration LDAP dans GLPI
Accès aux paramètres LDAP

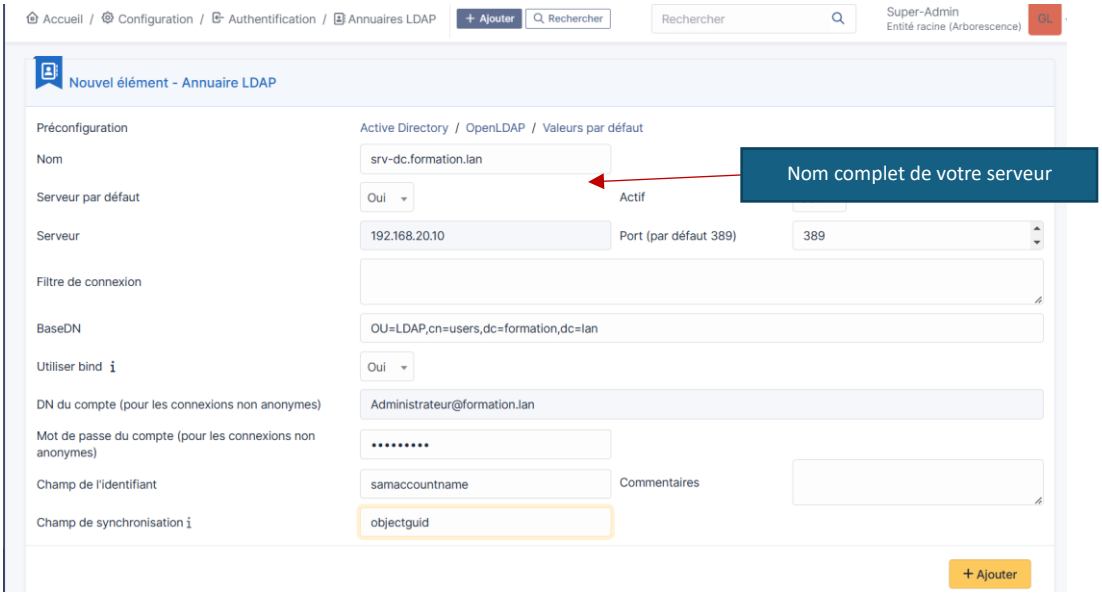
1. GLPI en tant qu'administrateur.



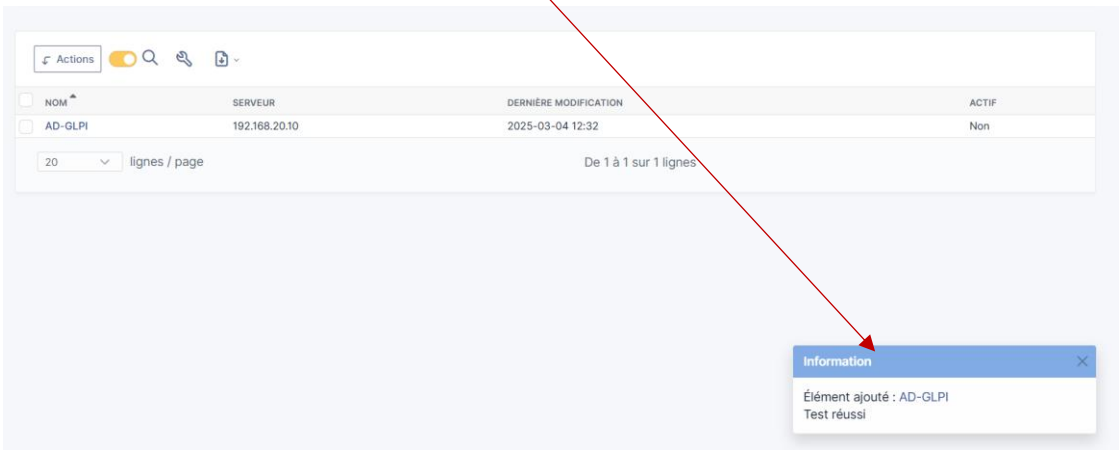
2. Allez dans **Configuration → Authentification → Annuaire LDAP**.



3. Ajoutez un serveur LDAP avec les paramètres suivants :

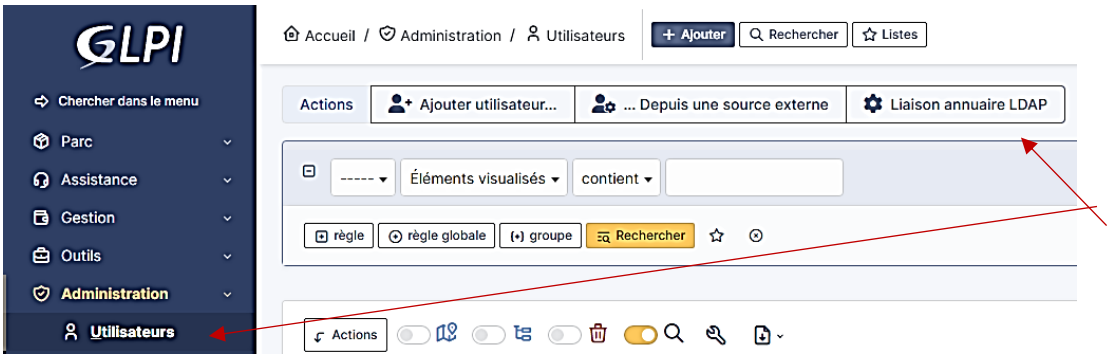


4. Testez la connexion et enregistrez.



7. Activer la synchronisation des utilisateurs

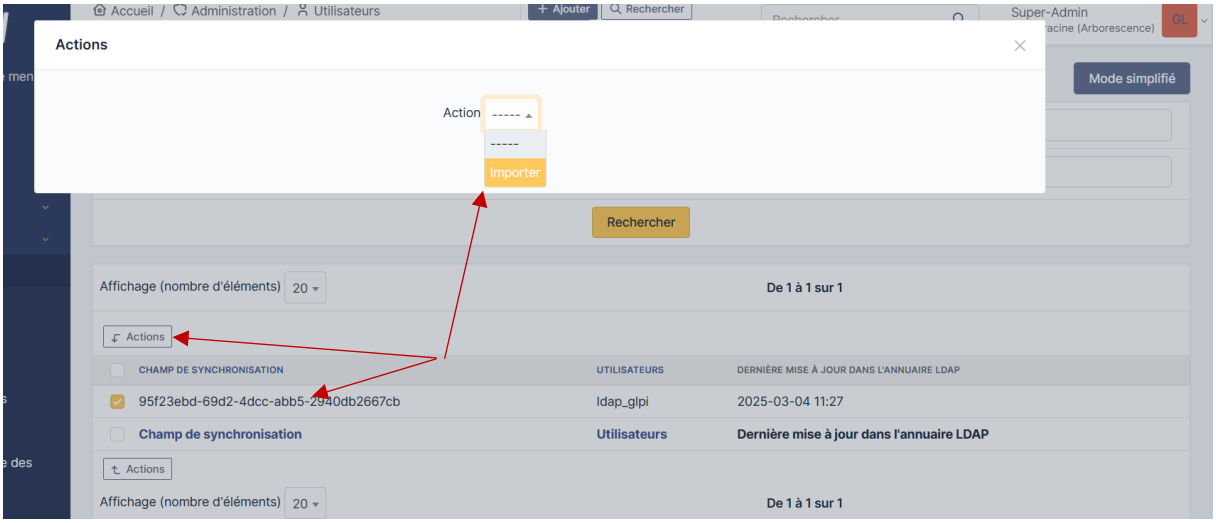
1. **Administration → Utilisateurs**.

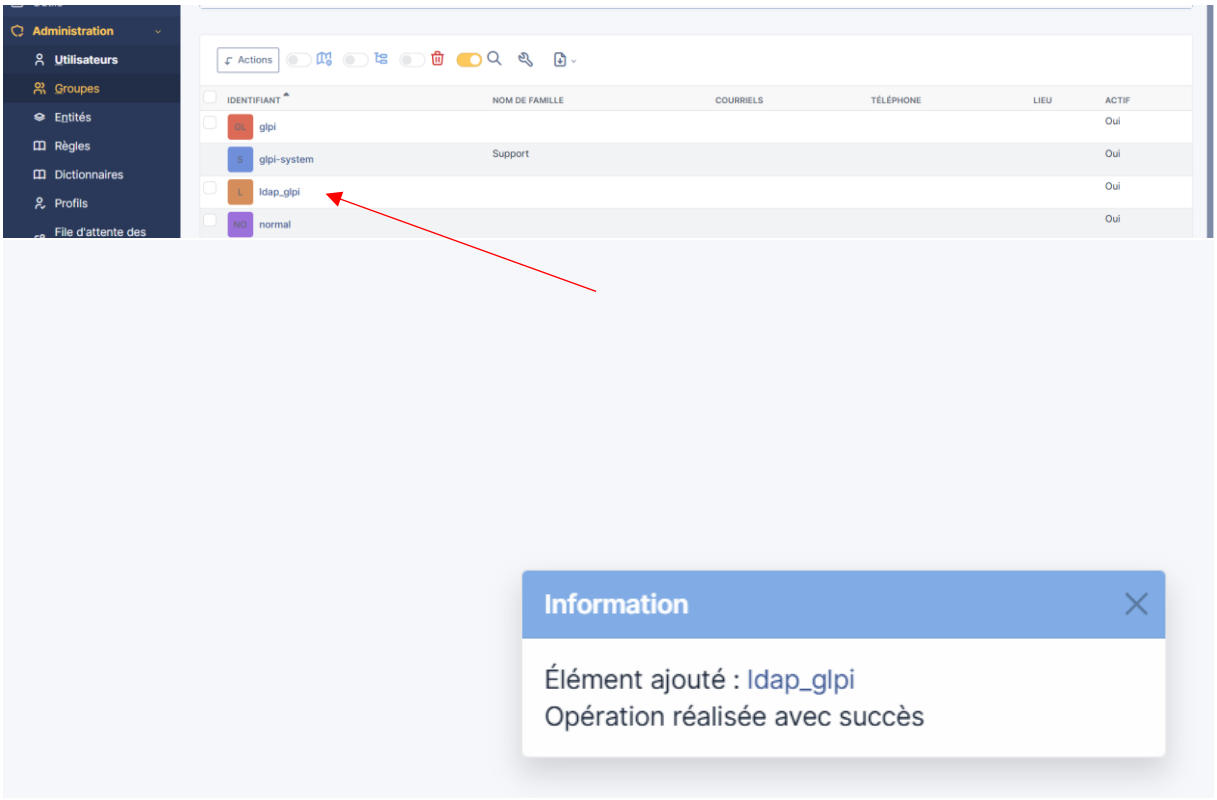


- Cliquez sur « Importation de nouveaux utilisateurs »
- Cliquez sur « Mode expert » (en haut à droite de la fenêtre) et sur « Rechercher » :

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

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





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.