INTÉGRATION SÉCURISÉE DE GLPI À L'ACTIVE DIRECTORY

Auteur :
MVOUAMA AMOUR NADREL

1. Introduction Générale

Ce projet a pour objectif principal le déploiement de l'application GLPI (Gestion Libre de Parc Informatique) sur un serveur Ubuntu, tout en assurant une intégration sécurisée avec un annuaire Active Directory Windows Server via le protocole LDAPS (LDAP sécurisé via TLS). L'objectif clé est de centraliser l'authentification des utilisateurs GLPI en s'appuyant sur l'infrastructure Active Directory existante.

Les composantes techniques couvertes incluent l'installation de la pile LAMP (Linux, Apache, MySQL, PHP), le déploiement de GLPI, la configuration réseau avec une résolution DNS appropriée, la mise en place d'une connexion LDAPS sécurisée sur le port 636, et la vérification complète de la chaîne de confiance des certificats.

Ce document servira de référence technique détaillée, documentant les étapes réalisées, les configurations mises en place, les tests effectués, et les outils utilisés pour garantir une intégration fiable et sécurisée. Il vise à fournir un guide reproductible pour toute personne souhaitant mettre en œuvre une solution similaire.

2. Concepts Fondamentaux

2.1. Qu'est-ce que GLPI ?

GLPI (Gestion Libre de Parc Informatique) est une application web open source essentiellement conçue pour la gestion des services informatiques (ITSM) et la gestion des actifs informatiques (ITAM). Elle offre un ensemble complet de fonctionnalités, incluant :

- Gestion des utilisateurs
- Gestion du matériel (ordinateurs, imprimantes, licences, etc.)
- Suivi des incidents et des demandes (helpdesk)
- Inventaire automatisé via des agents comme FusionInventory
- Création de rapports et de statistiques

2.2. Qu'est-ce qu'un annuaire Active Directory (AD)

Active Directory (AD) est un service d'annuaire développé par Microsoft, jouant un rôle central dans les environnements Windows Server. Il permet de centraliser la gestion des utilisateurs, des

groupes, des ordinateurs et des permissions au sein d'un domaine. AD utilise le protocole LDAP (Lightweight Directory Access Protocol) pour gérer les connexions et les authentifications.

2.3. Pourquoi connecter GLPI à Active Directory ?

La connexion de GLPI à Active Directory offre plusieurs avantages significatifs :

- Centralisation de l'authentification : Les utilisateurs GLPI peuvent utiliser leurs identifiants Windows/AD pour se connecter, évitant ainsi la nécessité de créer des comptes séparés dans GLPI.
- Importation automatique : Les comptes utilisateurs et les groupes AD peuvent être automatiquement importés dans GLPI, simplifiant ainsi l'administration des utilisateurs.

2.4. Architecture du Projet

Dans l'architecture cible, un utilisateur interagit avec GLPI via un navigateur web. GLPI est déployé sur un serveur web (sous Linux ou Windows) équipé de PHP, MySQL/MariaDB et Apache/Nginx. Pour l'authentification et l'importation des comptes, GLPI communique avec l'annuaire AD via le protocole LDAP.

3. Prérequis Techniques

La mise en œuvre de ce projet nécessite un environnement technique spécifique. Le tableau ci-dessous détaille les éléments indispensables, assurant ainsi une base solide pour le déploiement et l'intégration de GLPI avec Active Directory.

Élément Requis	Détail
Serveur avec GLPI	Pile LAMP (Apache, PHP, MariaDB) installée et configurée.
Serveur Active Directory	Windows Server avec AD DS installé, configuré et accessible.
Réseau	Communication bidirectionnelle entre les serveurs GLPI et Active Directory (LAN ou VPN).
Ports Ouverts	LDAP (389) ou LDAPS (636) ouverts et accessibles entre les serveurs.
Compte Utilisateur	Compte pour tester la connexion LDAP et l'authentification.

Élément Requis	Détail
AD	
Compte Admin GLPI	Accès administrateur pour configurer la connexion à Active Directory.

4. Mise en Place du Contrôleur de Domaine Active Directory

Cette section détaille la configuration d'un contrôleur de domaine Active Directory (AD DS) sur une machine Windows Server virtuelle, permettant au serveur Ubuntu de s'y connecter via LDAP.

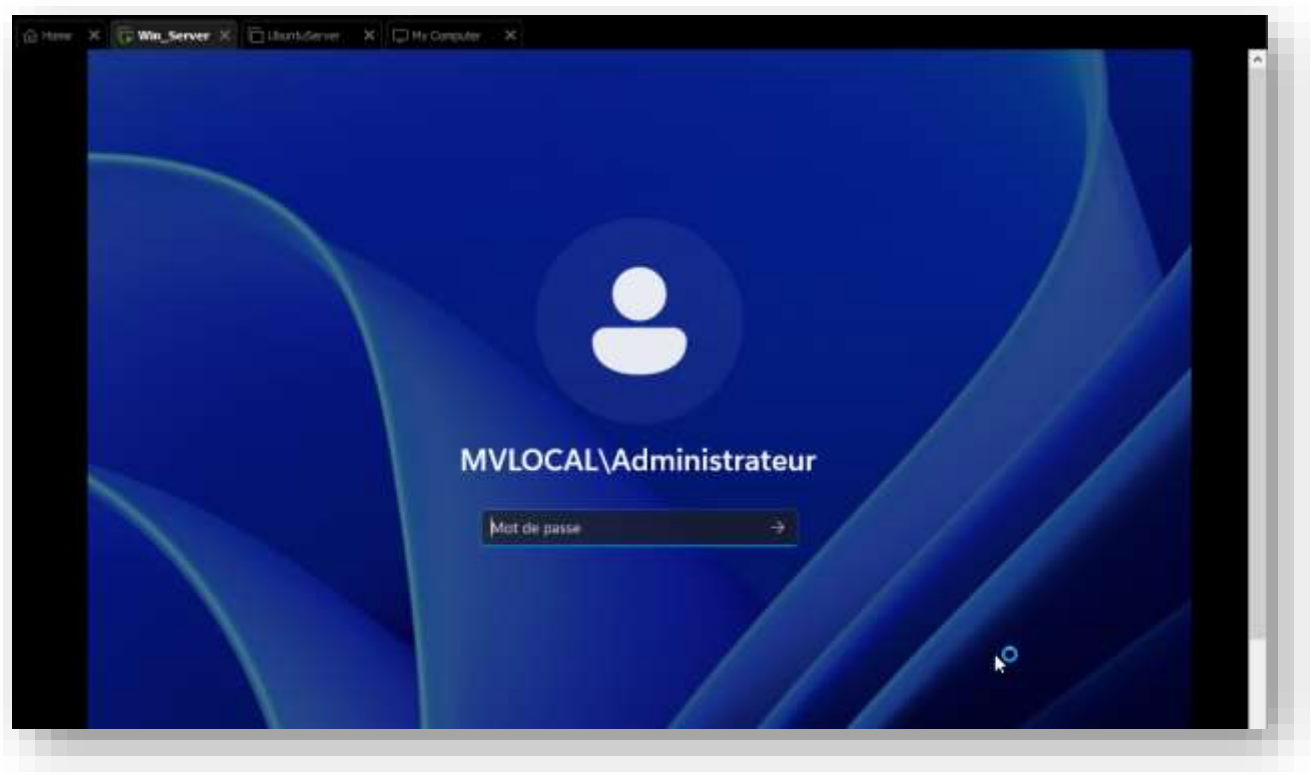
4.1. Installation des Rôles Nécessaires sur Windows Server

Pour installer les rôles 'Services de domaine Active Directory (AD DS)' et 'Serveur DNS', utilisez le Server Manager ('Ajouter des rôles et fonctionnalités'). AD DS est le cœur du domaine, et DNS assure la résolution des noms de domaine complets (FQDN).

4.2. Promotion du Serveur en Contrôleur de Domaine

La promotion du serveur inclut l'ajout d'une nouvelle forêt, la définition du nom de domaine racine (ex: `mvlocal.lan`), et la configuration du mot de passe de restauration DSRM (option par défaut pour DNS). La VM redémarrera après cette configuration.

4.3. Vérification Post-Redémarrage et Configuration DNS



Après le redémarrage, vérifiez l'accès à l'interface. Créez une Unité d'Organisation (OU) et un compte utilisateur de test (ex: `svc_glpi`) via 'Outils' > 'Utilisateurs et ordinateurs Active Directory'. Configurez le DNS pour Ubuntu : assurez-vous que le serveur Windows a une IP fixe (ex: `192.168.24.150`) et que son DNS pointe vers lui-même. Testez le ping du FQDN depuis Ubuntu.

4.4. Résumé de la Configuration AD

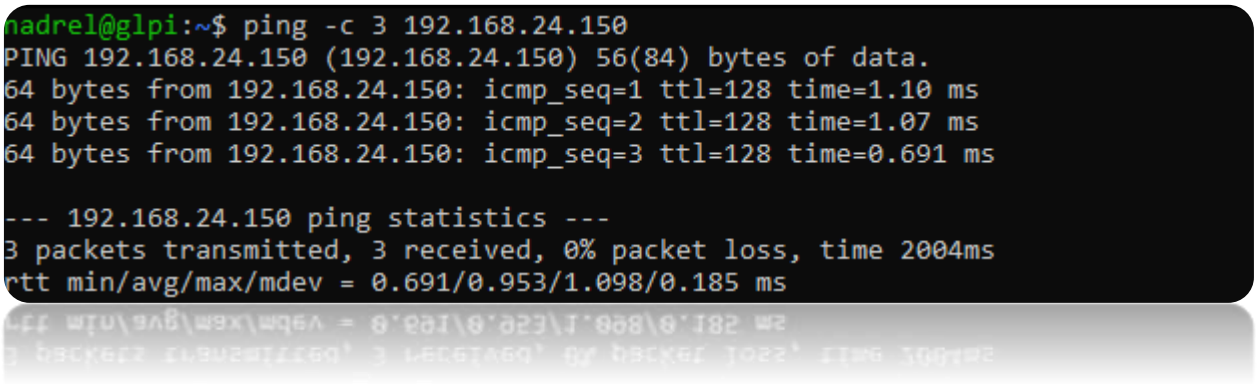
Paramètre	Valeur (Exemple)
Nom du domaine AD	`mvlocal.lan`
IP du DC Windows Server	`192.168.24.150`
Nom NetBIOS	`MVLOCAL`
Utilisateur test	`svc_glpi`
DNS activé	`Oui`

Paramètre	Valeur (Exemple)
Suffixe DNS complet	`dc.mvlocal.lan`

5. Préparation de l'Environnement Réseau pour GLPI et AD

5.1. Configuration Réseau de Base et Matériel Utilisé

L'objectif est d'assurer une connectivité réseau fiable entre le serveur Ubuntu hébergeant GLPI et le contrôleur de domaine Windows Server. Les deux machines sont des VMs situées sur le même réseau local virtuel `192.168.24.0/24`.



Machine	Rôle	Adresse IP	Nom
Ubuntu Server 22.04	Hôte GLPI	`192.168.24.144`	`glpi`
Windows Server	Contrôleur de domaine (AD + DNS)	`192.168.24.150`	`dc.mvlocal.lan`

5.2. Configuration et Vérification DNS sur Ubuntu Server

Par défaut, Ubuntu utilise un DNS externe, ce qui empêche la résolution du nom de domaine local `dc.mvlocal.lan`. Pour résoudre ce problème, nous avons modifié le fichier `/etc/resolv.conf` en utilisant les commandes suivantes :

Sudo rm /etc/resolv.conf

echo "nameserver 192.168.24.150" | sudo tee /etc/resolv.conf

sudo chattr +i /etc/resolv.conf

La commande `chattr +i` verrouille le fichier pour empêcher sa réécriture par `systemd-resolved`.

```
nadrel@glpi: ~
nadrel@glpi:~$ cat /etc/resolv.conf
nameserver 192.168.24.150
nadrel@glpi:~$
```

5.3. Vérification de la Résolution DNS

Pour vérifier la résolution DNS, nous avons utilisé les commandes **`dig dc.mvlocal.lan @192.168.24.150`** et **`ping dc.mvlocal.lan`.** Le succès du ping confirme la résolution DNS fonctionnelle et une connectivité stable entre Ubuntu et le contrôleur de domaine.

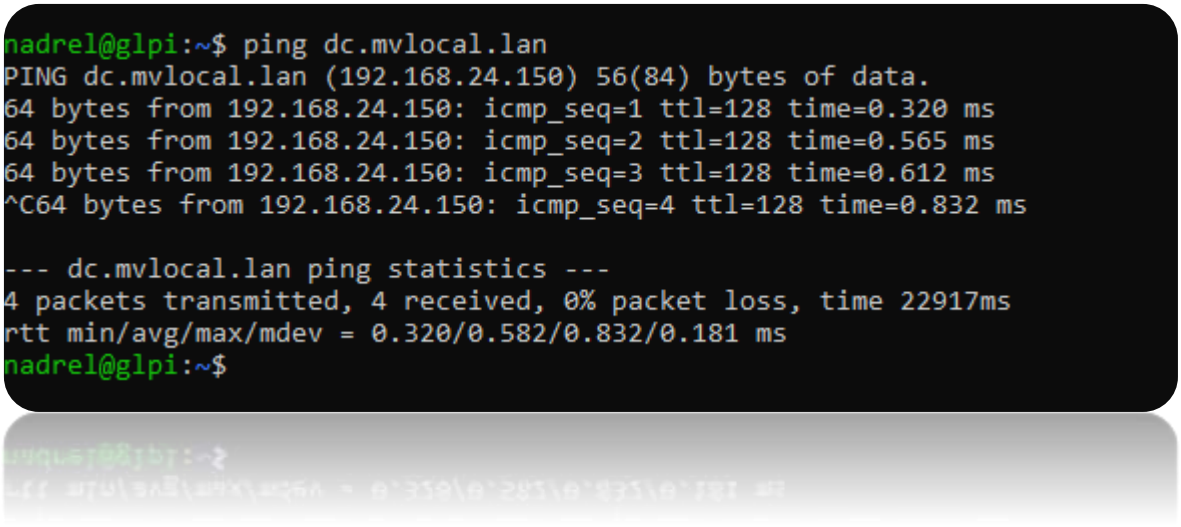
```
nadrel@glpi:~$ dig dc.mvlocal.lan @192.168.24.150

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> dc.mvlocal.lan @192.168.24.150
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13857
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;dc.mvlocal.lan.                        IN      A

;; ANSWER SECTION:
dc.mvlocal.lan.         3600    IN      A       192.168.24.150

;; Query time: 4 msec
;; SERVER: 192.168.24.150#53(192.168.24.150) (UDP)
;; WHEN: Mon Jul 21 06:50:09 UTC 2025
;; MSG SIZE  rcvd: 59
```



5.4. Justification Technique et Importance

L'utilisation du DNS Windows local est cruciale pour que GLPI puisse résoudre le FQDN du contrôleur de domaine. Le forçage de `/etc/resolv.conf` garantit que cette résolution est utilisée de manière cohérente. Cette préparation est essentielle car GLPI nécessite un accès réseau fonctionnel sur les ports 389 (non sécurisé) ou 636 (sécurisé) avec un temps de réponse rapide pour les échanges LDAP, sans quoi les requêtes LDAP échoueraient.

6. Installation de la Pile LAMP

Cette section détaille le déploiement de la pile LAMP (Linux, Apache, MariaDB, PHP) sur le serveur Ubuntu, fournissant une base solide pour l'installation et le fonctionnement de GLPI.

6.1. Justification des Composants LAMP

Chaque composant de la pile LAMP joue un rôle crucial dans le fonctionnement de GLPI. Voici un aperçu :

Composant	Rôle dans GLPI	Justification
Apache	Serveur Web	Stable, compatible PHP, supporté nativement par GLPI.
MariaDB	Base de données SQL	Plus léger que MySQL, 100% compatible GLPI, stocke tous les objets de GLPI (tickets, utilisateurs, logs...).

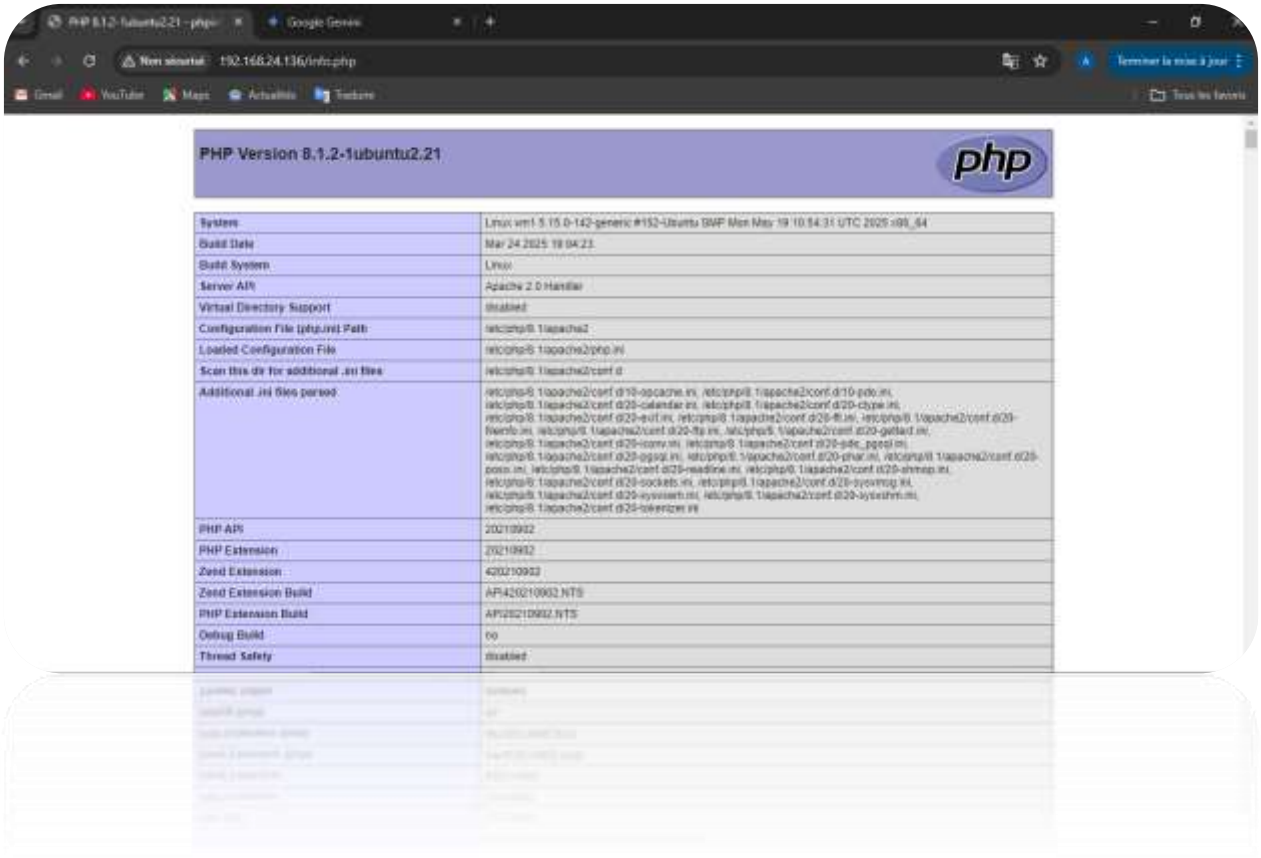
Composant	Rôle dans GLPI	Justification
PHP	Moteur applicatif	GLPI est écrit en PHP; Apache charge les pages via PHP.

6.2. Procédure d'Installation et de Configuration

Suivez ces étapes pour installer et configurer la pile LAMP :

1. Mise à jour du système : **sudo apt update && sudo apt upgrade -y**
2. Installation d'Apache : **sudo apt install apache2 -y**. Testez avec http://<IP_Ubuntu>.

3. Installation de MariaDB : **sudo apt install mariadb-server mariadb-client -y.**
4. Sécurisation de MariaDB : **sudo mysql_secure_installation.** Définissez un mot de passe root, supprimez les utilisateurs anonymes, désactivez l'accès root distant, supprimez la base de test.
5. Installation de PHP et extensions : **sudo apt install php php-mysql php-cli php-curl php-gd php-intl php-mbstring php-xml php-ldap php-zip -y**



6. Redémarrage d'Apache : **sudo systemctl restart apache2.**
7. Tests de validation PHP : Créez un fichier info.php (**echo "<?php phpinfo(); ?>" | sudo tee /var/www/html/info.php**) et naviguez vers http://<IP_Ubuntu>/info.php pour vérifier l'installation de PHP et de ses extensions.

7. Installation et Configuration Initiale de GLPI

Cette section décrit l'installation de GLPI sur le serveur Apache, son intégration à MariaDB, et la validation via l'interface web.

7.1. Déploiement des Fichiers GLPI

Les fichiers GLPI seront installés dans /var/www/html/glpi :

- Téléchargez la dernière version stable dans /tmp: **cd /tmp && wget https://github.com/glpi-project/glpi/releases/download/10.0.16/glpi-10.0.16.tgz.**

- Extrayez l'archive et déplacez les fichiers : **tar -xvzf glpi-10.0.14.tgz && sudo mkdir -p /var/www/html/glpi && sudo mv glpi/* /var/www/html/glpi/.**
- Modifiez les permissions : **sudo chown -R www-data:www-data /var/www/html/glpi && sudo chmod -R 755 /var/www/html/glpi.**

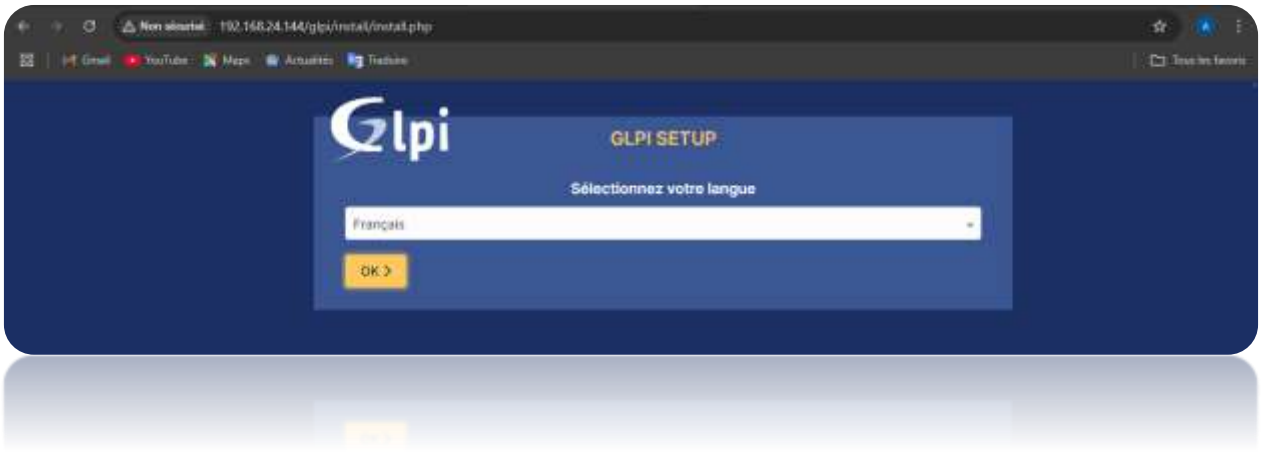
7.2. Configuration de MariaDB pour GLPI

Créez une base de données spécifique pour GLPI :

- Accédez à **MariaDB** : **sudo mysql -u root -p**
- Créez la **base glpidb** : **CREATE DATABASE glpidb CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;**
- **Créez l'utilisateur glpiuser** : **CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'MotDePasseFort123';**
- **Accordez les privilèges** : **GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'localhost';**
- **Rechargez les privilèges et quittez** : **FLUSH PRIVILEGES; EXIT;**

7.3. Accès Web et Finalisation de l'Installation

Accédez à l'interface via http://192.168.24.144/glpi et suivez les étapes : langue, licence, 'Installer', connexion à la base de données (Hôte: localhost, Base: glpidb, Utilisateur: glpiuser, Mot de passe: défini précédemment). GLPI créera les tables automatiquement. Cliquez sur 'Continuer'.



7.4. Connexion Initiale et Nettoyage

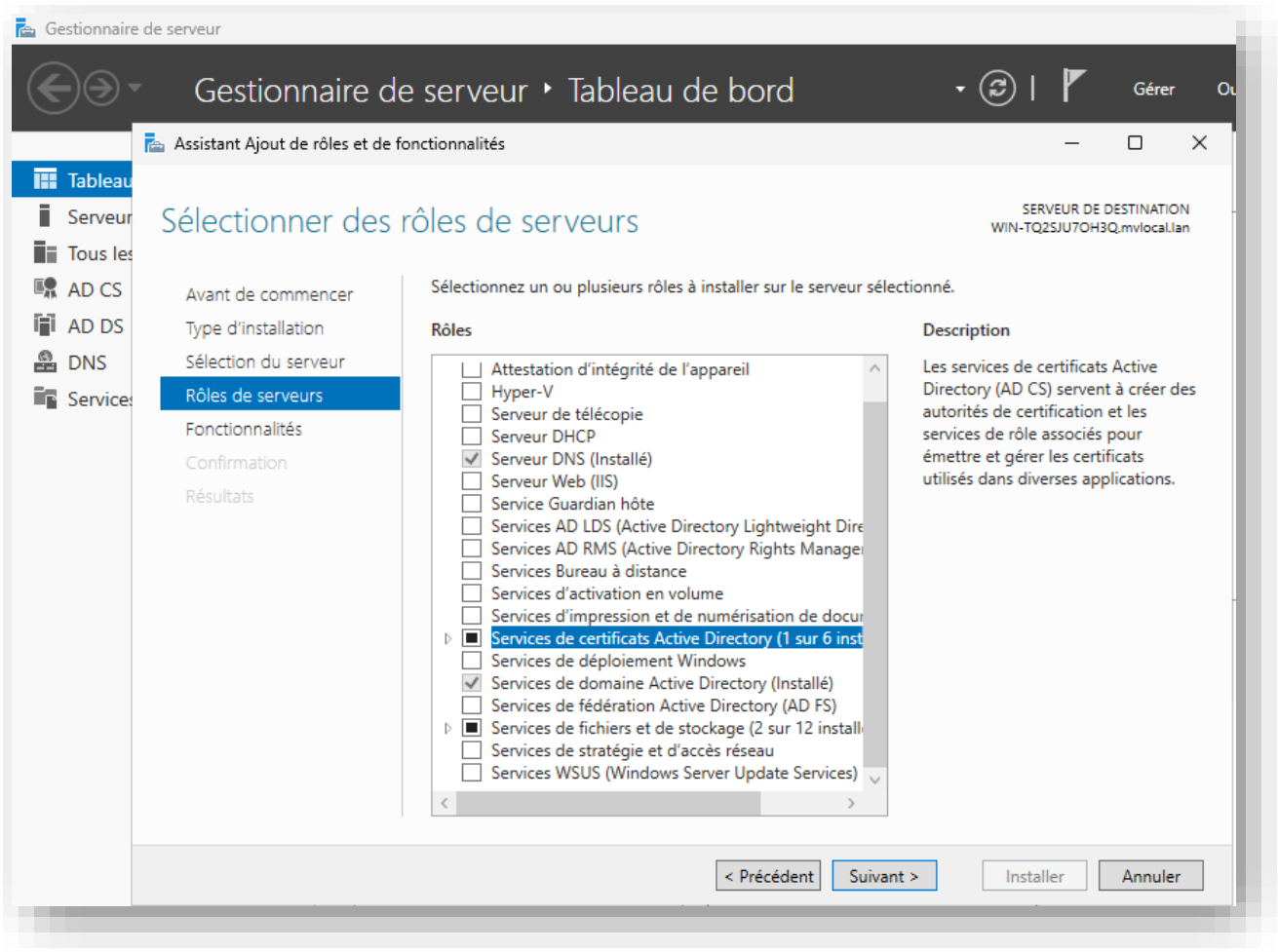
Utilisez les comptes initiaux (Super Admin, Technicien, Normal, Post-only) et modifiez les mots de passe. Supprimez le répertoire d'installation : **sudo rm -rf /var/www/html/glpi/install**.

8. Configuration des Services de Certificats Active Directory (AD CS)

Cette section détaille la configuration des Services de Certificats Active Directory (AD CS) pour permettre au contrôleur de domaine de répondre aux requêtes LDAPS (port 636) via un certificat SSL valide, émis par une Autorité de Certification d'entreprise (CA interne).

8.1. Installation et Configuration d'AD CS

Installez les services de certificats AD via le Gestionnaire de serveur (Ajouter des rôles et fonctionnalités) en sélectionnant le rôle 'Services de certificats Active Directory'. Configurez en choisissant le compte administrateur de domaine, le rôle 'Autorité de certification (CA)', le type d'AC (Autorité de certification d'entreprise, Racine), et créez une nouvelle clé privée (2048 bits, SHA256). Indiquez le nom commun de l'AC, la durée de validité (5 ans par défaut), puis finalisez.

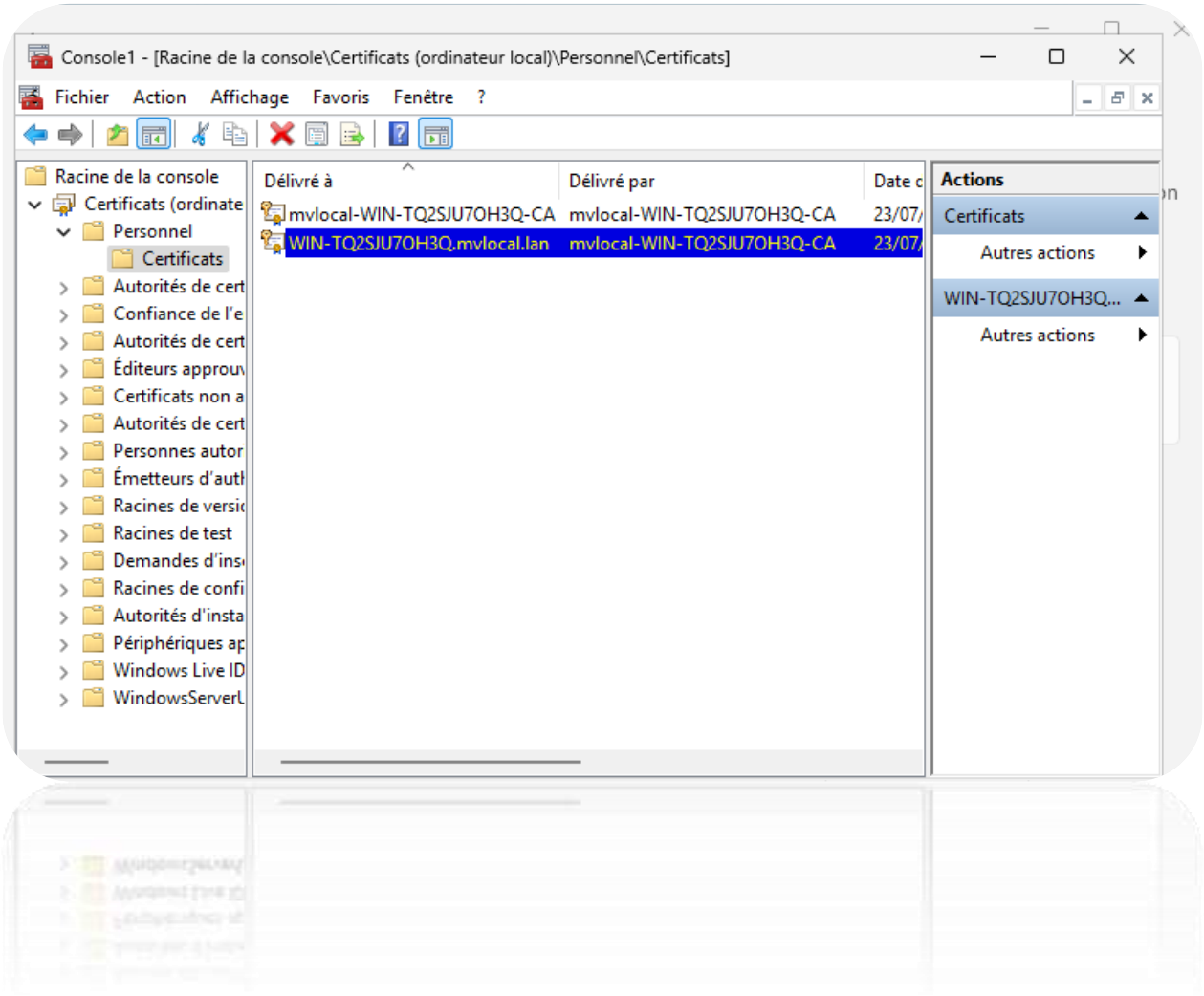


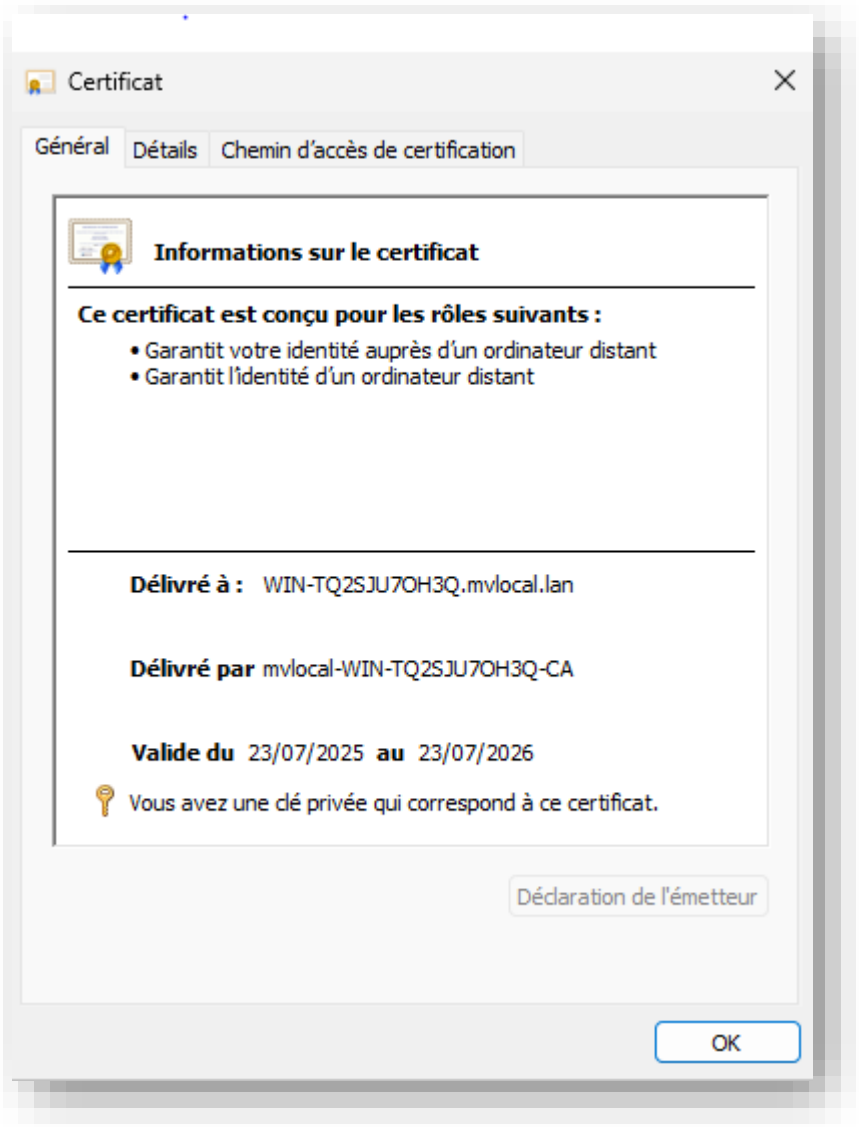
8.2. Redémarrage et Vérification du Certificat

Redémarrez le contrôleur de domaine après l'installation. Active Directory doit automatiquement demander et recevoir un certificat SSL via Autoenrollment.

8.3. Vérification du Certificat Généré Automatiquement

Vérifiez la génération du certificat : Ouvrez la console MMC (`Win + R` puis `mmc`), ajoutez le composant logiciel enfichable 'Certificats' pour le 'Compte ordinateur', naviguez vers 'Certificats (ordinateur local) > Personnel > Certificats'. Vérifiez la présence et les détails du certificat délivré par l'AC interne, conçu pour garantir l'identité du serveur distant avec une clé privée correspondante. Le certificat doit être valide.


Console1 - [Racine de la console\Certificats (ordinateur local)\Personnel\Certificats]
Fichier
Action
Affichage
Favoris
Fenêtre
?
Racine de la console
Certificats (ordinate
Personnel
Certificats
Autorités de cert
Confiance de l'e
Autorités de cert
Éditeurs approuv
Certificats non a
Autorités de cert
Personnes autor
Émetteurs d'autl
Racines de versic
Racines de test
Demandes d'ins
Racines de confi
Autorités d'insta
Périphériques ap
Windows Live ID
WindowsServerU
Délivré à
Délivré par
Date c
mvlocal-WIN-TQ2SJU7OH3Q-CA
mvlocal-WIN-TQ2SJU7OH3Q-CA
23/07/
WIN-TQ2SJU7OH3Q.mvlocal.lan
mvlocal-WIN-TQ2SJU7OH3Q-CA
23/07/
Actions
Certificats
Autres actions
WIN-TQ2SJU7OH3Q...
Autres actions



8.4. Exportation du Certificat CA pour Linux

Exportez le certificat de l'Autorité de Certification pour l'installer sur le serveur Linux GLPI : Ouvrez la console de l'Autorité de Certification **(`certsrv.msc`),** accédez aux propriétés du nom de la CA, allez dans l'onglet '**Affichage du certificat**' ou '**Général**', puis cliquez sur '**Afficher le certificat...**' et 'Détails'. Cliquez sur '**Copier dans un fichier**...' pour lancer l'Assistant Exportation de certificat. Choisissez le format '**Base-64 encodé X.509 (.CER)**', et définissez un chemin et un nom de fichier (ex: `C:\Users\Administrateur\Desktop\ca_mvlocal.crt`).

8.5. Transfert et Installation du Certificat sur Linux (GLPI)

Transférez le certificat vers le serveur GLPI via SCP depuis PowerShell sur Windows (ex: **`scp C:\Users\Administrateur\Desktop\ca_mvlocal.crt nadrel@192.168.24.168:/tmp/`**). Sur le serveur Linux GLPI, connectez-vous en SSH, déplacez le fichier **(`sudo cp /tmp/ca_mvlocal.crt /usr/local/share/ca-certificates/`**), et mettez à jour la liste des certificats (`sudo update-ca-certificates`). Le message attendu est **'1 added, 0 removed; done'.**

9. Intégration et Test de la Connexion LDAPS entre GLPI et Active Directory

9.1. Principes de l'Authentification LDAP et Paramètres Clés

GLPI agit comme un client LDAP, sollicitant le serveur Active Directory pour authentifier et gérer les utilisateurs et les groupes. Pour ce faire, GLPI doit connaître l'adresse IP ou le nom du serveur AD, le port de connexion LDAP (389 ou 636 pour LDAPS), le DN de base (Base DN) pour la recherche, ainsi qu'un compte de service LDAP (Bind DN) et son mot de passe.

Les paramètres LDAP essentiels sont:

- **Hôte:** Adresse IP ou nom d'hôte du serveur Active Directory.
- **Port:** Port de connexion LDAP (389 ou 636).
- **Base DN:** Point de départ pour la recherche dans l'annuaire.
- **Bind DN:** Compte de service utilisé pour se connecter à l'annuaire.
- **Mot de passe Bind:** Mot de passe du compte de service.
- **Filtre de recherche:** Filtre LDAP utilisé pour rechercher des utilisateurs.

Le processus d'authentification logique est le suivant: l'utilisateur interagit avec l'interface GLPI, GLPI envoie une requête LDAP au serveur AD en utilisant le Base DN et un filtre, et AD confirme ou infirme l'authentification.

9.2. Avantages de l'Utilisation de LDAP pour l'Authentification GLPI

L'authentification LDAP offre des avantages significatifs : gain de temps grâce aux comptes utilisateurs déjà existants dans l'AD, centralisation de la gestion (mots de passe, suspensions, droits) côté AD, et sécurité renforcée avec une seule identité par utilisateur.

9.3. Création des Comptes Utilisateurs et Groupes de Test dans Active Directory

Il est recommandé de créer une Unité d'Organisation (OU), un groupe (ex: 'GLPI_Utilisateurs'), un utilisateur de test (ex: 'anadrel') et un compte de service pour GLPI (ex: 'svc_glpi', avec droits de lecture seule) dans Active Directory pour effectuer des tests d'intégration.

9.4. Configuration LDAP dans GLPI

La configuration LDAP se fait dans l'interface web de GLPI, sous `Configuration > Authentification > Annuaire LDAP`. Il faut renseigner le nom (ex: 'Active Directory MVLOCAL'), le serveur (`WIN-TQ2SJU7OH3Q.mvlocal.lan`), le port (`636`), le BaseDN (`DC=mvlocal,DC=lan`), le DN du compte (Bind DN, ex: `CN=svc_glpi,CN=Users,DC=mvlocal,DC=lan`), et le mot de passe du compte. Le filtre de connexion (`(&(objectClass=user)(objectCategory=person))`) est également important.

9.5. Importation et Connexion des Utilisateurs AD

Pour importer des utilisateurs depuis l'AD, naviguez vers `Administration > Utilisateurs > Liaison Annuaires LDAP`, puis 'Importation de nouveaux Utilisateurs'. Utilisez le 'Mode Expert' et cliquez sur 'Rechercher' pour voir les utilisateurs AD. Après l'importation, déconnectez-vous du compte GLPI par défaut et connectez-vous avec un utilisateur importé de l'Active Directory (ex: `svc_glpi`) pour valider l'intégration.

9.6. Test Avancé du Service LDAPS

Des tests techniques peuvent être effectués depuis le serveur Linux GLPI :

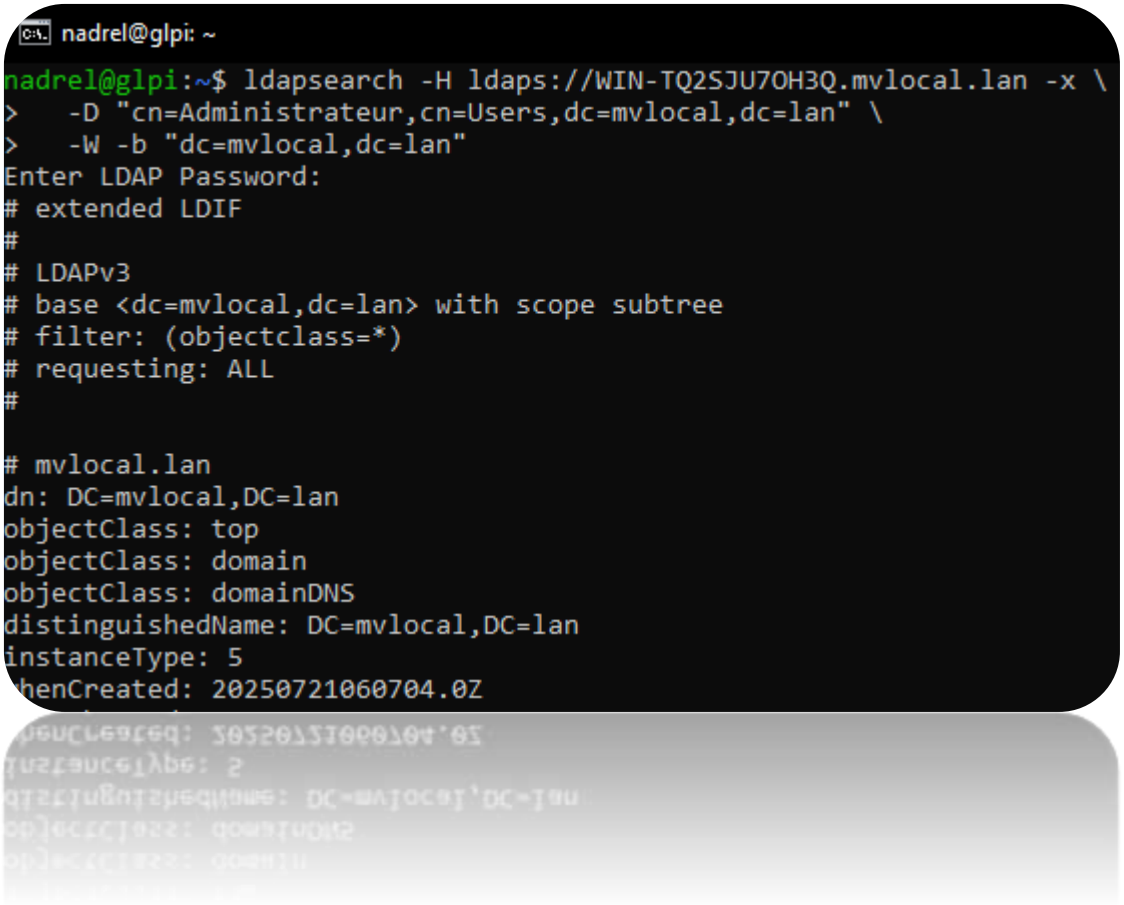
- **openssl s_client -connect 192.168.24.150:636 -showcerts**: Vérifie la connexion SSL et la validité du certificat (`**verify return:0 (ok)**`).

```
nadrel@glpi: ~
nadrel@glpi:~$ openssl s_client -connect win-tq2sju7oh3q.mvlocal:636 -showcerts
CONNECTED(00000003)

depth=1 DC = lan, DC = mvlocal, CN = mvlocal-WIN-TQ2SJU7OH3Q-CA
verify return:1
depth=0 CN = WIN-TQ2SJU7OH3Q.mvlocal.lan
verify return:1
---
Certificate chain
 0 s:CN = WIN-TQ2SJU7OH3Q.mvlocal.lan
   i:DC = lan, DC = mvlocal, CN = mvlocal-WIN-TQ2SJU7OH3Q-CA
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jul 23 12:15:07 2025 GMT; NotAfter: Jul 23 12:15:07 2026 GMT
-----BEGIN CERTIFICATE-----
MIIGcjCCBVqgAwIBAgITIAAAAAMZJsf7U2GkvAAAAAAAAzANBgkqhkiG9w0BAQsF
ADBTMRMwEQYKCZImiZPyLGQBGRYDbGFuMRcwFQYKCZImiZPyLGQBGRYHbXZsb2Nh
```

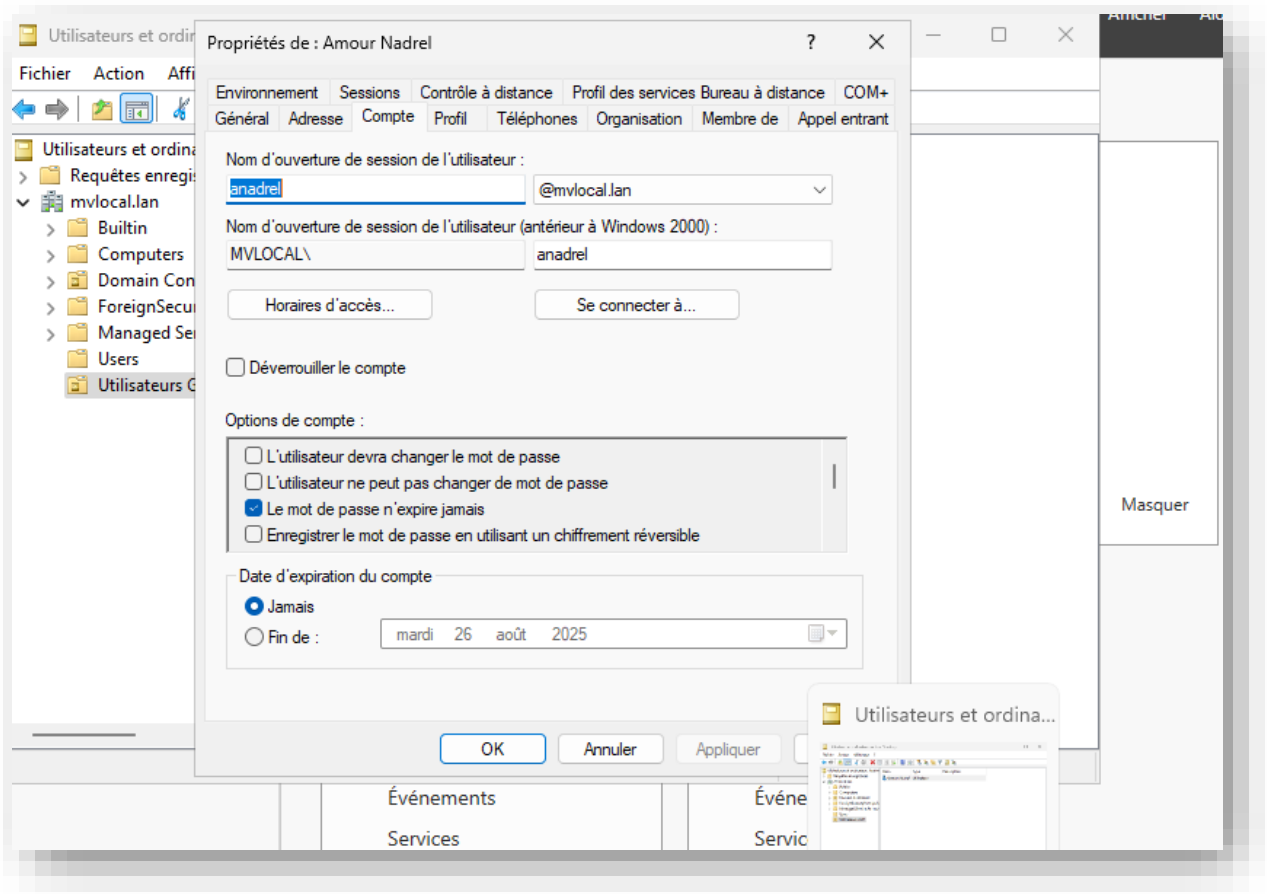
```
    Start Time: 1753601332
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

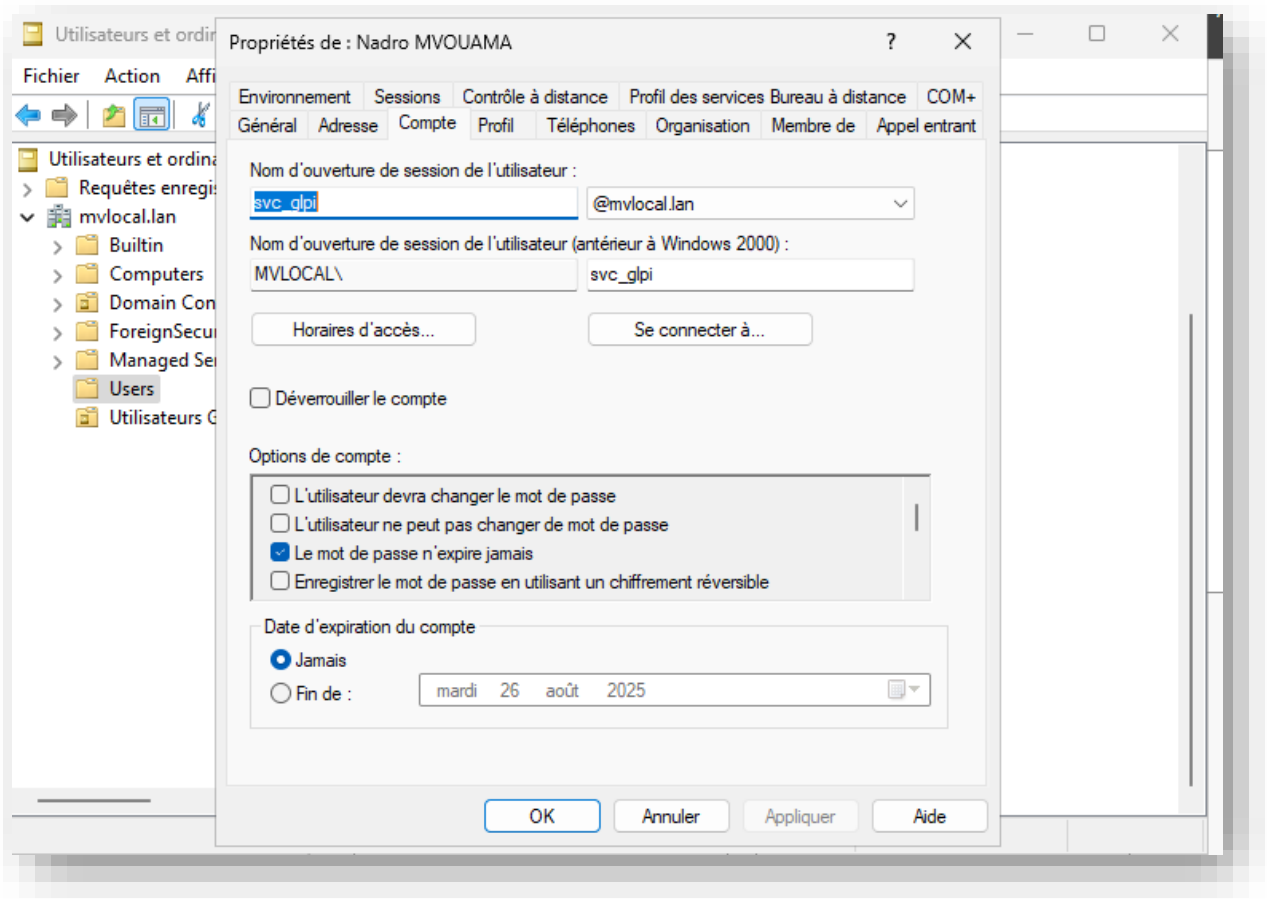
- **ldapsearch -H ldaps://WIN-TQ2SJU7OH3Q.mvlocal.lan -x -D "cn=Administrateur,cn=Users,dc=mvlocal,dc=lan" -W -b "dc=mvlocal,dc=lan"**: Effectue une recherche LDAP sécurisée, en utilisant les options suivantes : `-H` (URL LDAP), `-x` (mode simple), `-D` (DN de l'utilisateur), `-W` (mot de passe), `-b` (base de recherche).



Création d'un utilisateur et d'un groupe de Test dans Active Directory

Pour les tests avec GLPI, nous aurons besoin d'un utilisateur et d'un groupe, d'où j'ai créé une Unité d'Organisation, puis un groupe 'GLPI_Utilisateurs' auquel j'ai ajouté un utilisateur 'anadrel' (Nom d'ouverture de session). Ensuite j'ai créé un compte de service pour GLPI (Lecture Seule), Nom d'ouverture de session utilisateur : 'svc_glpi'.


Utilisateurs et ordi
Propriétés de : Amour Nadrel
Fichier
Action
Affi
Environnement
Sessions
Contrôle à distance
Profil des services Bureau à distance
COM+
Général
Adresse
Compte
Profil
Téléphones
Organisation
Membre de
Appel entrant
Nom d'ouverture de session de l'utilisateur :
anadrel
@mvlocal.lan
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
MVLOCAL\
anadrel
Horaires d'accès...
Se connecter à...
Déverrouiller le compte
Options de compte :
L'utilisateur devra changer le mot de passe
L'utilisateur ne peut pas changer de mot de passe
Le mot de passe n'expire jamais
Enregistrer le mot de passe en utilisant un chiffrement réversible
Date d'expiration du compte
Jamais
Fin de :
mardi 26 août 2025
OK
Annuler
Appliquer
Utilisateurs et ordina...
Utilisateurs et ordin
Requêtes enregis
mvlocal.lan
Builtin
Computers
Domain Con
ForeignSecu
Managed Se
Users
Utilisateurs G
Masquer
Événements
Services
Événe
Servic



Je me connecte avec les identifiants par défaut de GLPI pour avoir accès au tableau de bord, puis modifier les mots de passe ainsi donc je pourrai importer les utilisateurs de mon Active Directory.

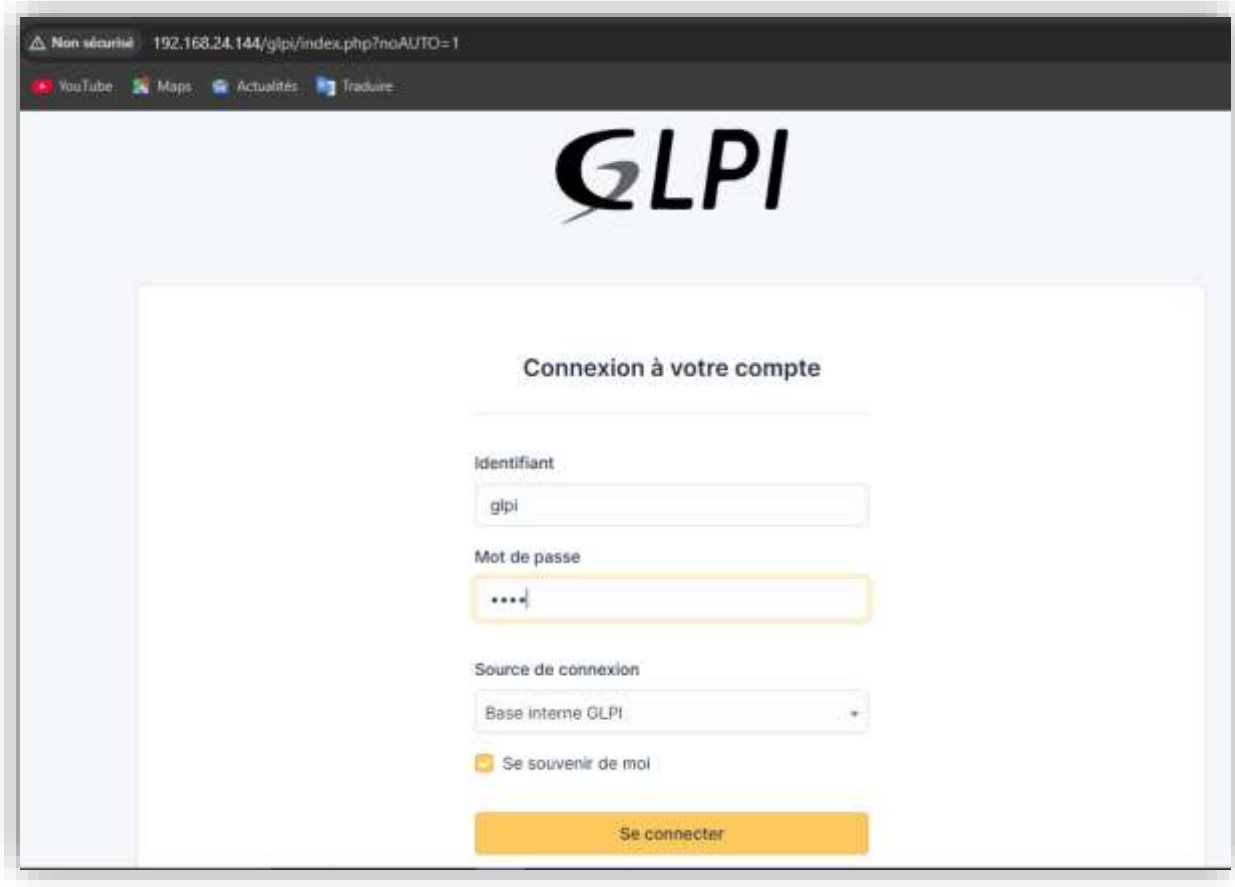
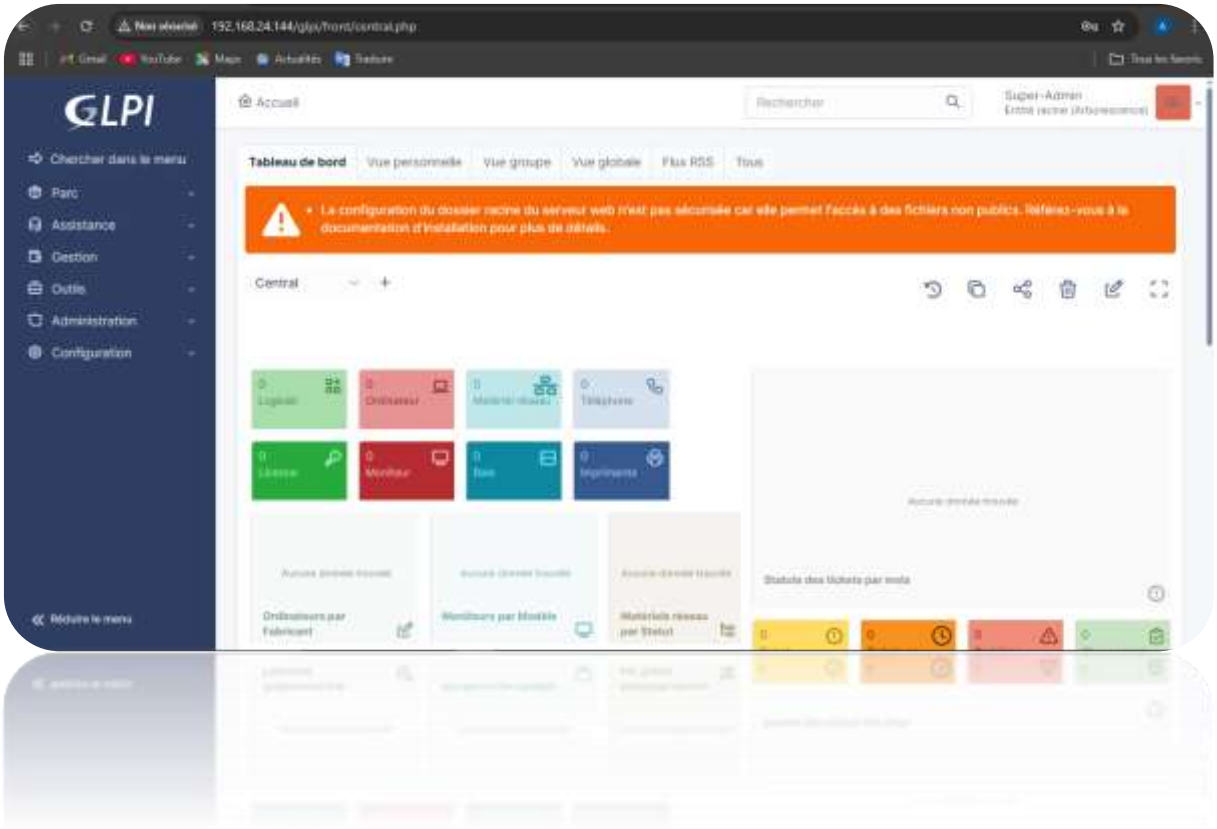
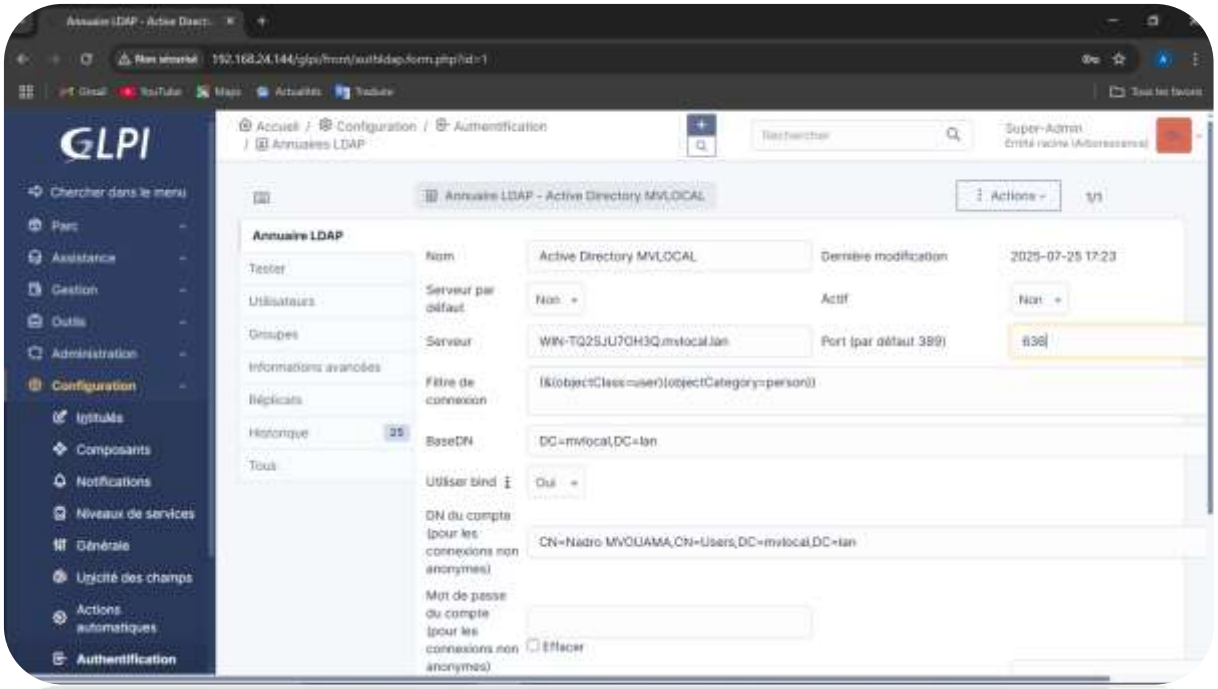
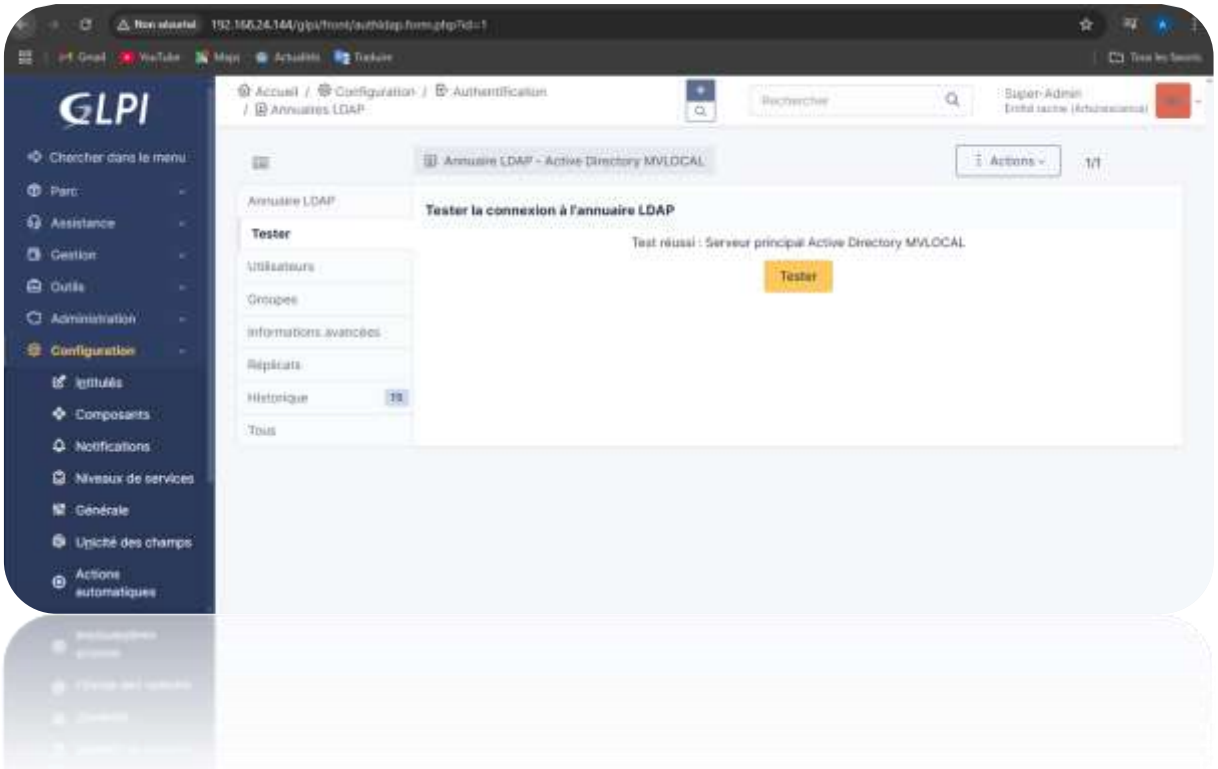


Tableau de Bord

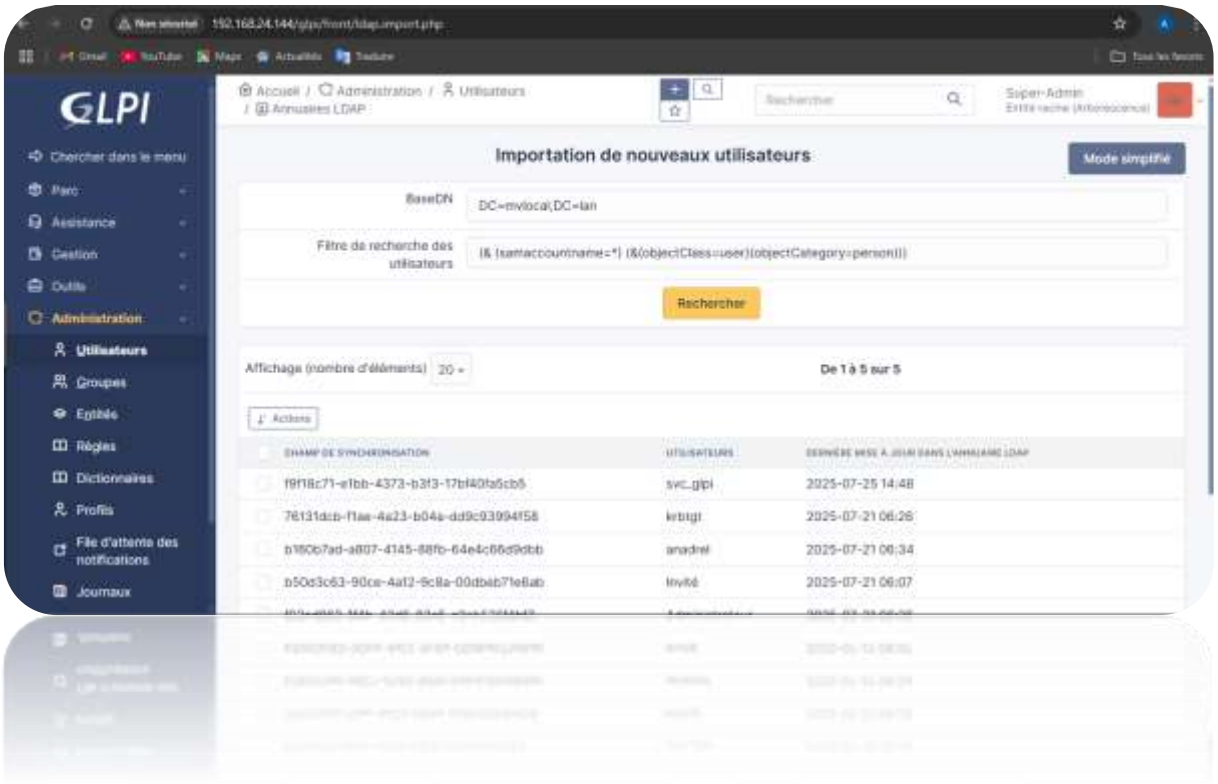


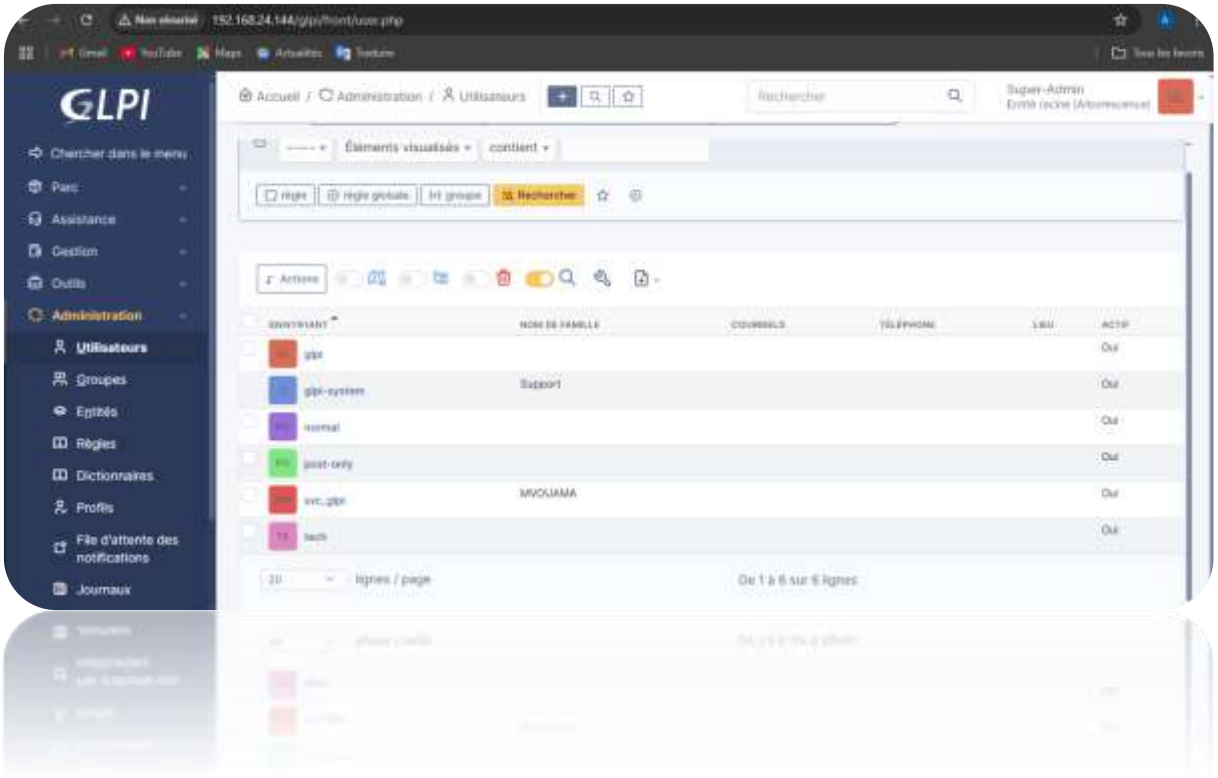
Naviguer Vers **Configuration > Authentification > Annuaire LDAP**, puis remplir les champs (voir l'image ci-dessous)


GLPI
Accueil / Configuration / Authentification
/ Annuaires LDAP
Annuaire LDAP - Active Directory MVLOCAL
Actions
1/1
Annuaire LDAP
Tester
Utilisateurs
Groupes
Informations avancées
Réplicats
Historique 25
Tous
Nom
Active Directory MVLOCAL
Dernière modification
2025-07-25 17:23
Serveur par défaut
Non
Actif
Non
Serveur
WIN-TQ2SJU7OH3Q.mvlocal.lan
Port (par défaut 389)
636
Filtre de connexion
(&(objectClass=user)(objectCategory=person))
BaseDN
DC=mvlocal,DC=lan
Utiliser bind
Oui
DN du compte (pour les connexions non anonymes)
CN=Nadro MVOUAMA,CN=Users,DC=mvlocal,DC=lan
Mot de passe du compte (pour les connexions non anonymes)
Effacer
Chercher dans le menu
Parc
Assistance
Gestion
Outils
Administration
Configuration
Intitulés
Composants
Notifications
Niveaux de services
Générale
Unicité des champs
Actions automatiques
Authentification

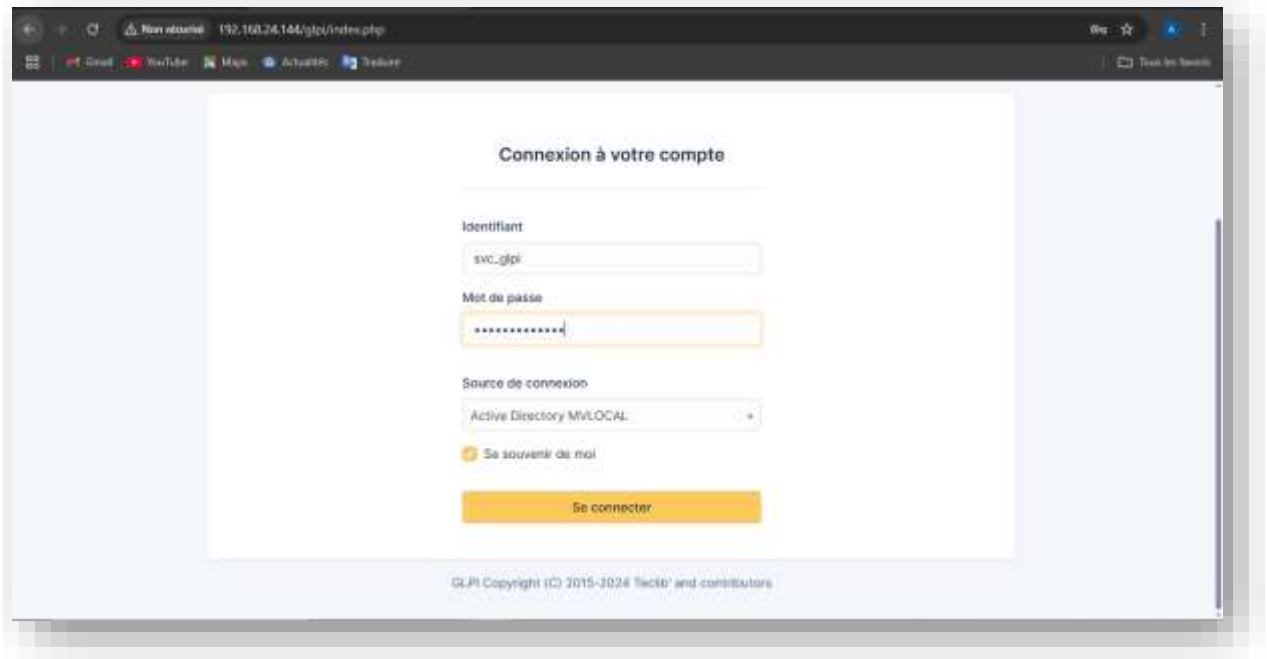

GLPI
Accueil / Configuration / Authentification
/ Annuaires LDAP
Annuaire LDAP - Active Directory MVLOCAL
Actions
1/1
Annuaire LDAP
Tester
Utilisateurs
Groupes
Informations avancées
Réplicats
Historique 19
Tous
Tester la connexion à l'annuaire LDAP
Test réussi : Serveur principal Active Directory MVLOCAL
Tester
Chercher dans le menu
Parc
Assistance
Gestion
Outils
Administration
Configuration
Intitulés
Composants
Notifications
Niveaux de services
Générale
Unicité des champs
Actions automatiques

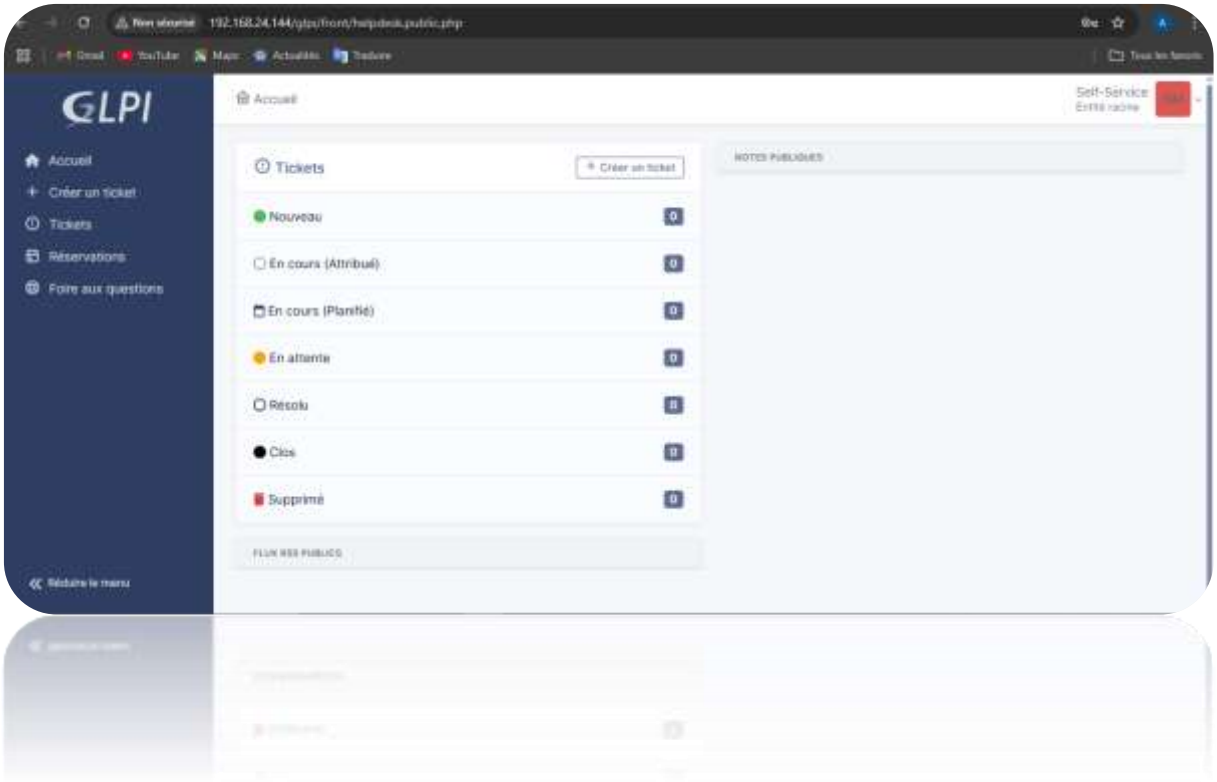
Naviguer vers **Administration > Utilisateurs > Liaison Annuaires LDAP > Importation de nouveaux Utilisateurs** puis cliquer sur **Mode Expert** Ensuite **Rechercher**





Je vais à présent me déconnecter de ce compte par défaut de GLPI, puis me connecter avec l'utilisateur **'svc_glpi'** dont j'ai importer de mon Active Directory.





10. Difficultés Rencontrées et Leçons Apprises

10.1. Résolution DNS et Communication avec l'Active Directory

La résolution DNS du domaine Active Directory (`mvlocal.lan`) a posé problème initialement. Sans configuration correcte du fichier `/etc/resolv.conf`, les outils LDAP et les commandes comme `ping` et `dig` ne pouvaient localiser le contrôleur de domaine. Plusieurs tests croisés ont été nécessaires pour assurer la cohérence entre les adresses IP, les noms d'hôtes et le serveur DNS.

10.2. Mise en Place de la Connexion LDAPS (Port 636)

La sécurisation de la communication LDAP avec LDAPS a été une étape complexe. La génération d'un certificat personnalisé via les services de certificats Windows Server nécessitait une configuration correcte et la publication d'un modèle de certificat approprié. Le certificat attribué au contrôleur de domaine devait contenir les bons usages étendus pour être accepté par le client Linux. L'ajustement de la chaîne de confiance était crucial, notamment en ajoutant

manuellement le certificat racine de l'autorité de certification au magasin de certificats systèmes sur le serveur Ubuntu. Des erreurs courantes comme 'unable to verify the first certificate' ont été rencontrées jusqu'à la validation complète avec `openssl s_client`.

10.3. Intégration GLPI ↔ Active Directory

Bien que l'intégration GLPI avec LDAP soit documentée, plusieurs ajustements ont été nécessaires, notamment l'utilisation du bon format de DN (Distinguished Name) dans la configuration du serveur LDAP dans GLPI, ainsi que la résolution des problèmes de synchronisation dus aux différences entre les attributs attendus par GLPI et ceux fournis par le serveur AD.

10.4. Configuration Apache et Droits sur GLPI

Des problèmes de permissions ont été rencontrés lors du déploiement initial de GLPI dans `/var/www/html/`. Il a fallu attribuer correctement les droits au groupe `www-data` et s'assurer que les modules Apache nécessaires (PHP, rewrite, etc.) étaient bien activés.

10.5. Documentation Continue et Résilience Face aux Obstacles

La documentation continue et rigoureuse (captures, commandes, commentaires) a renforcé la qualité et la traçabilité du travail, tout en offrant des opportunités pour approfondir la compréhension des environnements hybrides (Linux/Windows), du protocole LDAP/LDAPS, de la gestion des certificats SSL, et des bonnes pratiques de déploiement sécurisé.

CONCLUSION

Ce projet a permis de mettre en œuvre une solution professionnelle de gestion de parc informatique avec GLPI sur Ubuntu, entièrement intégrée à un annuaire Active Directory via LDAPS. Les objectifs clés suivants ont été atteints :

- Mise en place de la pile LAMP.
- Installation et configuration initiale de GLPI.
- Configuration du réseau et résolution correcte du domaine AD.
- Intégration sécurisée à l'Active Directory via LDAPS (port 636).
- Validation complète de la communication LDAP sécurisée à l'aide de certificats.

Au-delà des aspects techniques, ce projet a permis de renforcer les compétences en administration système, sécurité réseau, gestion d'annuaire LDAP et documentation technique. Il constitue une base solide pour de futurs projets plus complexes (automatisation, supervision, intégration de modules supplémentaires).

Ce projet a démontré l'importance de la sécurisation des communications réseau, de la maîtrise des environnements hybrides et de la rigueur dans la documentation des procédures techniques.

Table des matières