PROCÉDURE TECHNIQUE

Sécurisation de la liaison annuaire (LDAPS)
entre GLPI et Active Directory

Migration LDAP port 389 → LDAPS port 636 avec certificat AD CS

Auteur : CHADHOULI EL-Anrif — BTS SIO SISR 2026 — MEWO Metz

Élément	Valeur
Serveur AD	SRV-AD-01 — Windows Server — 10.11.3.18
Serveur GLPI	SRV-GLPI — Ubuntu — 10.11.3.22
Domaine	sio.local
Port actuel	TCP 389 (LDAP non chiffré)
Port cible	TCP 636 (LDAPS chiffré SSL/TLS)
Prérequis	Rôle AD CS installé sur SRV-AD-01

1. CONTEXTE ET ENJEUX DE SÉCURITÉ

Pourquoi abandonner le port 389 ?

Actuellement, la liaison entre GLPI et Active Directory utilise LDAP sur le port 389. Ce protocole transmet toutes les données en clair sur le réseau, ce qui expose l'infrastructure à des risques critiques :

- Transmission en clair : les identifiants du compte de service GLPI (login + mot de passe) circulent sans aucun chiffrement sur le LAN.
- Attaque Man-in-the-Middle (MitM) : un attaquant positionné sur le réseau peut capturer ces credentials en quelques secondes avec Wireshark ou tcpdump.
- Compromission de l'annuaire : avec ces credentials, l'attaquant peut interroger l'AD, lister les utilisateurs et élever ses privilèges.

La solution : LDAPS sur le port 636

Le protocole LDAPS (LDAP over SSL/TLS) encapsule les échanges dans un tunnel chiffré via un certificat SSL émis par notre Autorité de Certification interne (AD CS). Cette migration garantit trois propriétés fondamentales :

- Confidentialité : toutes les données échangées sont chiffrées (AES).
- Authentification : GLPI vérifie l'identité du serveur AD via le certificat.
- Intégrité : aucune modification des données n'est possible en transit.

Durcissement Microsoft

Depuis la mise à jour de sécurité ADV190023 (Mars 2020), Microsoft exige par défaut la signature LDAP et prépare l'obligation du channel binding. L'utilisation de LDAP non chiffré sur le port 389 sera progressivement bloquée par les mises à jour Windows. Migrer vers LDAPS est une démarche proactive, obligatoire à terme et conforme aux bonnes pratiques CIS Benchmark.

SECURITE — En LDAP port 389, une simple capture Wireshark suffit à récupérer le mot de passe du compte de service GLPI en quelques secondes. Risque critique en cas d'attaquant interne.

---

2. PRÉREQUIS

- Le rôle Services de certificats Active Directory (AD CS) est installé sur SRV-AD-01.
- Le service Autorité de Certification (CertSvc) est démarré.
- SRV-GLPI a accès réseau à SRV-AD-01 sur les ports 389, 636 et 443.
- Un compte Administrateur est disponible sur SRV-AD-01.
- Un accès SSH ou console est disponible sur SRV-GLPI.
- Les snapshots VMware sont disponibles avant manipulation.

Vérification	Commande / Emplacement	Résultat attendu
AD CS installé	Gestionnaire de serveur → Rôles	Services de certificats AD présent
CA démarrée	services.msc → CertSvc	En cours d'exécution
Port 636 (avant)	netstat -an | findstr 636	Aucun résultat (normal avant reboot)
Connectivité	ping 10.11.3.18 depuis SRV-GLPI	Réponse OK

ÉTAPE 1 — SAUVEGARDE (SNAPSHOTS)

Avant toute manipulation de certificats, créer des snapshots des deux VMs. En cas d'erreur, ces snapshots permettent un retour arrière immédiat.

1.1 Snapshot de SRV-AD-01

- Ouvrir VMware (ESXi ou Workstation)
- Clic droit sur SRV-AD-01 → Snapshot → Prendre un snapshot
- Nom : AVANT-LDAPS-AD-01
- Description : Avant migration LDAP 389 vers LDAPS 636
- Cliquer sur OK

1.2 Snapshot de SRV-GLPI

- Clic droit sur SRV-GLPI → Snapshot → Prendre un snapshot
- Nom : AVANT-LDAPS-GLPI
- Cliquer sur OK

ÉTAPE 2 — CRÉATION DU CERTIFICAT LDAPS VIA AD CS

Le rôle AD CS est installé. Nous allons demander un nouveau certificat basé sur le modèle "Domain Controller Authentication". Ce modèle inclut l'usage "Server Authentication" requis par LDAPS.

2.1 Demande de certificat sur SRV-AD-01

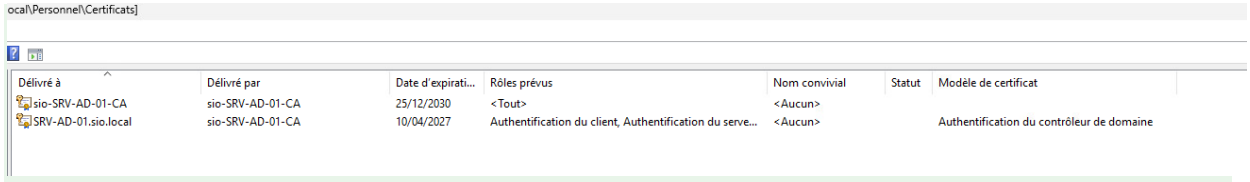
- Sur SRV-AD-01, ouvrir une invite de commande en tant qu'Administrateur
- Lancer la console MMC des certificats ordinateur :

```
certlm.msc
```

- Naviguer vers : Certificats (Ordinateur local) → Personnel → Certificats
- Clic droit dans le volet → Toutes les tâches → Demander un nouveau certificat
- Cliquer sur Suivant → Suivant
- Sélectionner le modèle : Domain Controller Authentication
- Cliquer sur Inscrire puis Terminer

2.2 Vérification du certificat

- Double-cliquer sur le nouveau certificat
- Onglet Général : vérifier que le nom du sujet = SRV-AD-01.sio.local
- Onglet Détails → Utilisation de clé améliorée : "Authentification du serveur" présent



ÉTAPE 3 — VÉRIFICATION DE L'ÉCOUTE SUR LE PORT 636

Après attribution du certificat, redémarrer le serveur AD pour que le service d'annuaire (NTDS) détecte le nouveau certificat et active l'écoute sur le port 636.

3.1 Redémarrage de SRV-AD-01

- Sur SRV-AD-01, ouvrir une invite de commande Administrateur
- Exécuter le redémarrage :

```
shutdown /r /t 0
```

SECURITE — Prévenir les utilisateurs avant le redémarrage. Sur un DC en production, planifier cette opération hors des heures de bureau.

3.2 Vérification via netstat

- Après redémarrage, ouvrir une invite de commande Administrateur
- Exécuter :

```
netstat -an | findstr ":636"
```

Résultat attendu :

```
TCP    0.0.0.0:636    0.0.0.0:0    LISTENING
```

```
C:\Users\Administrateur>netstat -an | findstr ":636"
  TCP    0.0.0.0:636            0.0.0.0:0              LISTENING
  TCP    [::]:636               [::]:0                 LISTENING
```

3.3 Vérification via ldp.exe (recommandée)

- Ouvrir ldp.exe : Démarrer → Exécuter → ldp
- Cliquer sur Connexion → Connecter
- Renseigner les paramètres :

Champ	Valeur
Serveur	SRV-AD-01.sio.local
Port	636
SSL	Coché

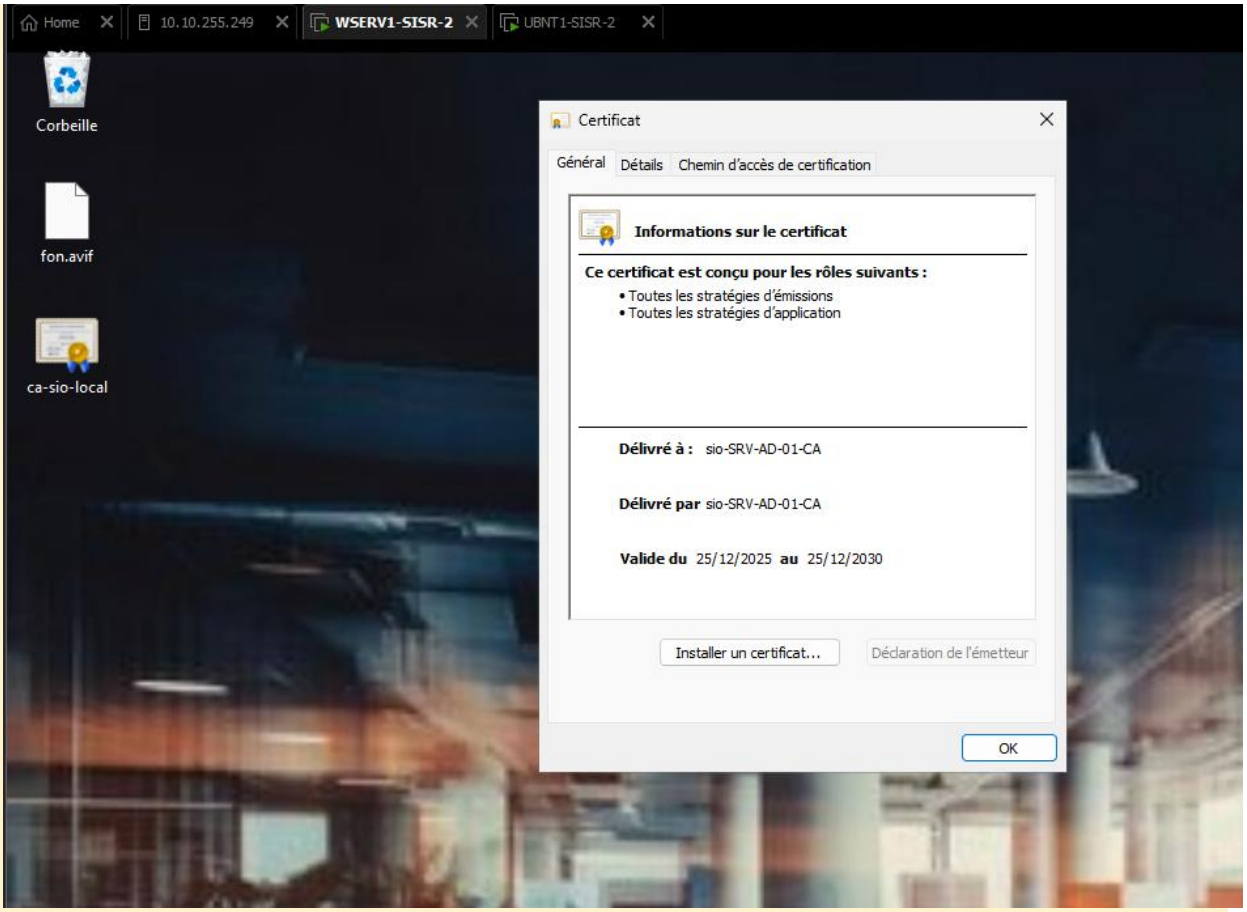
- Cliquer sur OK
- Le volet droit doit afficher : dn: DC=sio,DC=local — connexion réussie

ÉTAPE 4 — EXPORTATION DU CERTIFICAT RACINE (CA)

Pour que SRV-GLPI (Ubuntu) accepte la connexion LDAPS, il doit faire confiance à notre CA interne. Il faut exporter le certificat racine et le transférer sur Ubuntu.

4.1 Export depuis la console Autorité de Certification

- Sur SRV-AD-01 : Outils d'administration → Autorité de Certification
- Dans l'arborescence, clic droit sur le nom de la CA
- Sélectionner : Propriétés → onglet Général
- Cliquer sur Afficher le certificat
- Aller dans l'onglet Détails → Copier dans un fichier
- Choisir le format : X.509 encodé en base 64 (.CER)
- Nommer le fichier : ca-sio-local.cer
- Sauvegarder sur le Bureau de SRV-AD-01



SECURITE — Exporter uniquement le certificat PUBLIC (.cer), jamais la clé privée (.pfx). Exporter la clé privée compromettrait l'intégralité de l'infrastructure PKI.

4.2 Transfert du certificat vers SRV-GLPI

Depuis SRV-GLPI (Ubuntu), rapatrier le certificat via SCP :

```
# Depuis SRV-GLPI, rapatrier le .cer depuis l'AD
scp Administrateur@10.11.3.18:"/C:/Users/Administrateur/Desktop/ca-sio-local.cer"
/tmp/
```

```
C:\Users\Administrateur>scp C:\Users\Administrateur\Desktop\ca-sio-local.cer admin-local@10.11.3.22:/tmp/
admin-local@10.11.3.22's password:
ca-sio-local.cer                                              100% 1266    29.4KB/s   00:00
```

ÉTAPE 5 — IMPORTATION DU CERTIFICAT SUR UBUNTU (SRV-GLPI)

Ubuntu doit intégrer le certificat CA dans son magasin de confiance système pour que PHP (et donc GLPI) valide la connexion LDAPS sans erreur SSL.

5.1 Copie et importation

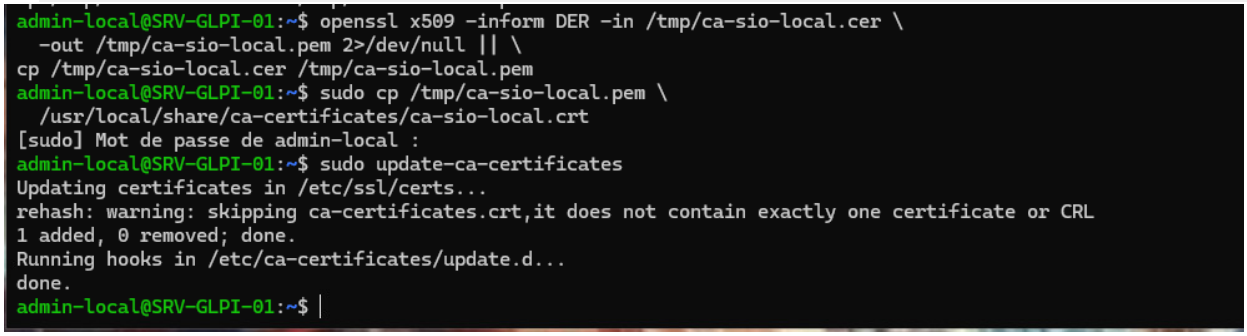
- Se connecter en SSH ou console sur SRV-GLPI

- Exécuter les commandes suivantes en tant que root :

```
# Convertir le certificat en PEM si nécessaire
openssl x509 -inform DER -in /tmp/ca-sio-local.cer \
  -out /tmp/ca-sio-local.pem 2>/dev/null || \
cp /tmp/ca-sio-local.cer /tmp/ca-sio-local.pem

# Copier dans le répertoire des CA de confiance
sudo cp /tmp/ca-sio-local.pem \
  /usr/local/share/ca-certificates/ca-sio-local.crt

# Mettre à jour le magasin de certificats Ubuntu
sudo update-ca-certificates
```

Résultat attendu :

```
1 added, 0 removed; done.
```

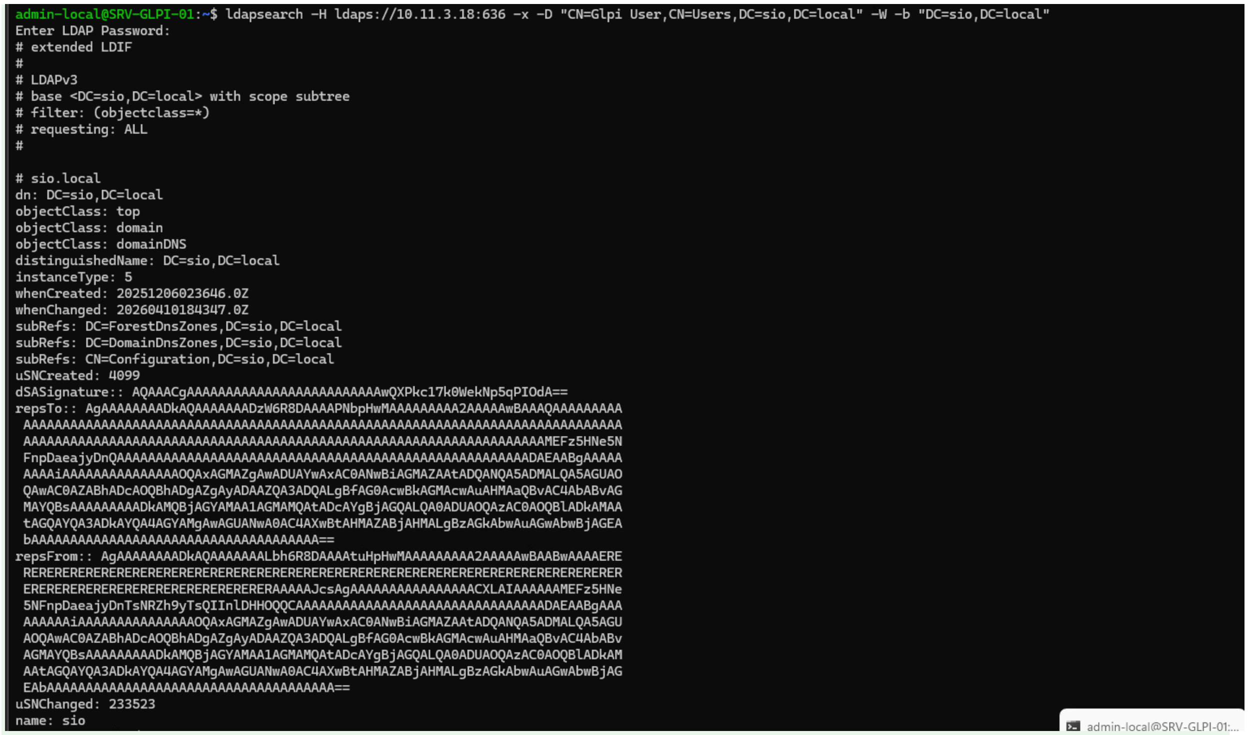


5.2 Vérification LDAPS depuis Ubuntu

Tester la connexion LDAPS depuis Ubuntu avant de modifier GLPI :

```
ldapsearch -H ldaps://SRV-AD-01.sio.local:636 \
  -b "DC=sio,DC=local" \
  -D "CN=Glpi User,CN=Users,DC=sio,DC=local" \
  -W "(objectClass=user)" cn
```

Résultat attendu : liste des utilisateurs AD retournée sans erreur SSL.



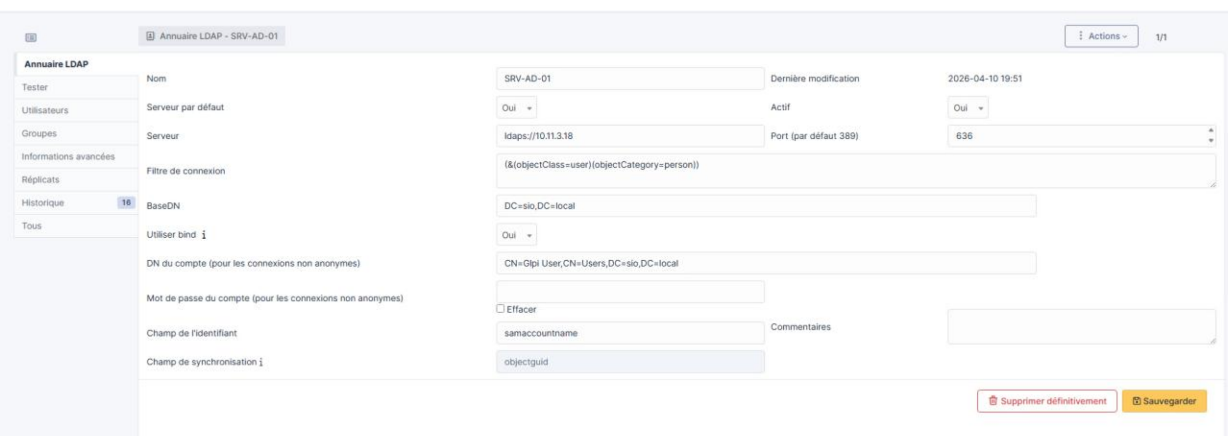
```
admin-local@SRV-GLPI-01:~$ ldapsearch -H ldaps://10.11.3.18:636 -x -D "CN=Glpi User,CN=Users,DC=sio,DC=local" -W -b "DC=sio,DC=local"
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <DC=sio,DC=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# sio.local
dn: DC=sio,DC=local
objectClass: top
objectClass: domain
objectClass: domainDNS
distinguishedName: DC=sio,DC=local
instanceType: 5
whenCreated: 20251206023646.0Z
whenChanged: 20260410184347.0Z
subRefs: DC=ForestDnsZones,DC=sio,DC=local
subRefs: DC=DomainDnsZones,DC=sio,DC=local
subRefs: CN=Configuration,DC=sio,DC=local
uSNCreated: 4099
dSASignature:: AQAAACgAAAAAAAAAAAAAAAAAAAAAAAAAwQXPkc17k0WekNp5qPIOdA==
repsTo:: AgAAAAAAAADkAQAAAAAAADzW6R8DAAAAPNbpHwMAAAAAAAA2AAAAAwBAAAQAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMEFz5HNe5N
 FnpDaeajyDnQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADAEAABgAAAAA
 AAAAiAAAAAAAAAAAAAAAAOQAxAGMAZgAwADUAYwAxAC0ANwBiAGMAZAAtADQANQA5ADMALQA5AGUAO
 QAwAC0AZABhADcAOQBhADgAZgAyADAAZQA3ADQALgBfAG0AcwBkAGMAcwAuAHMAaQBvAC4AbABvAG
 MAYQBsAAAAAAAAADkAMQBjAGYAMAA1AGMAMQAtADcAYgBjAGQALQA0ADUAOQAzAC0AOQBlADkAMAA
 tAGQAYQA3ADkAYQA4AGYAMgAwAGUANwA0AC4AXwBtAHMAZABjAHMALgBzAGkAbwAuAGwAbwBjAGEA
 bAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==
repsFrom:: AgAAAAAAAADkAQAAAAAAALbh6R8DAAAAtuHpHwMAAAAAAAA2AAAAAwBAABwAAAAERE
 RERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERERER
 ERERERERERERERERERERERERERERERERAAAAAJcsAgAAAAAAAAAAAAAAAACXLAIAAAAAAAMEFz5HNe
 5NFnpDaeajyDnTsNRZh9yTsQIInlDHHOQQCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAADAEAABgAAA
 AAAAAAiAAAAAAAAAAAAAAAAOQAxAGMAZgAwADUAYwAxAC0ANwBiAGMAZAAtADQANQA5ADMALQA5AGU
 AOQAwAC0AZABhADcAOQBhADgAZgAyADAAZQA3ADQALgBfAG0AcwBkAGMAcwAuAHMAaQBvAC4AbABv
 AGMAYQBsAAAAAAAAADkAMQBjAGYAMAA1AGMAMQAtADcAYgBjAGQALQA0ADUAOQAzAC0AOQBlADkAM
 AAtAGQAYQA3ADkAYQA4AGYAMgAwAGUANwA0AC4AXwBtAHMAZABjAHMALgBzAGkAbwAuAGwAbwBjAG
 EAbAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==
uSNChanged: 233523
name: sio
```


ÉTAPE 6 — RECONFIGURATION DE GLPI

L'interface GLPI doit être mise à jour pour utiliser LDAPS sur le port 636 à la place de LDAP sur le port 389.

6.1 Accès à la configuration LDAP

- Se connecter à GLPI avec un compte Administrateur
- Aller dans : Configuration → Authentification → Annuaires LDAP
- Cliquer sur l'annuaire existant (sio.local) pour le modifier



6.2 Modification des paramètres

Paramètre	Ancienne valeur	Nouvelle valeur
Serveur	ldap://10.11.3.18	ldaps://10.11.3.18

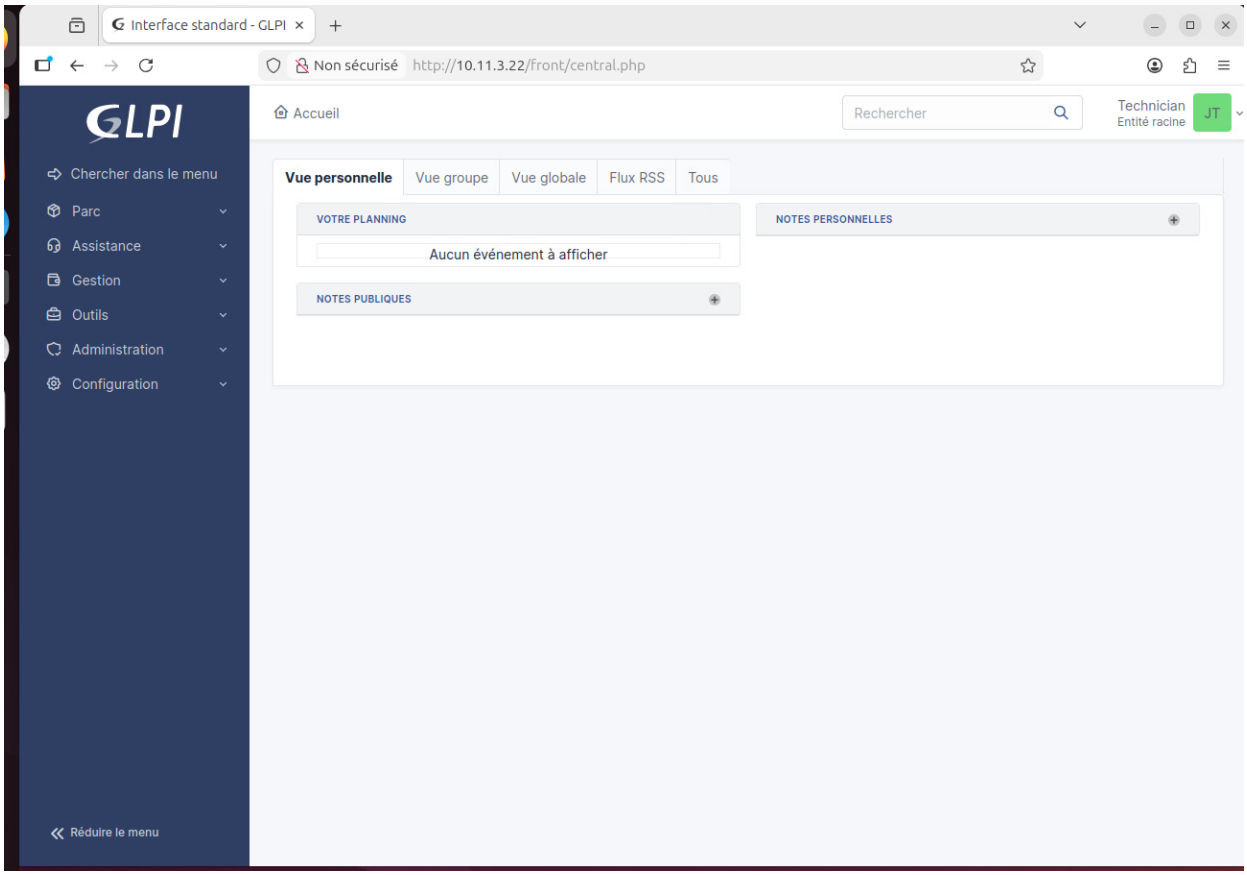
Port	389	636
Utiliser TLS	Non	Oui (strict)
Certificat	Aucun	Géré par le système Ubuntu

6.3 Test et sauvegarde

- Cliquer sur le bouton Tester la connexion
- Résultat attendu : bandeau vert "Connexion au LDAP réussie"
- Sauvegarder la configuration

6.4 Test d'authentification utilisateur

- Dans GLPI : Administration → Utilisateurs
- Tenter de se connecter avec un compte AD (ex : julien)
- L'utilisateur doit être reconnu et authentifié via LDAPS

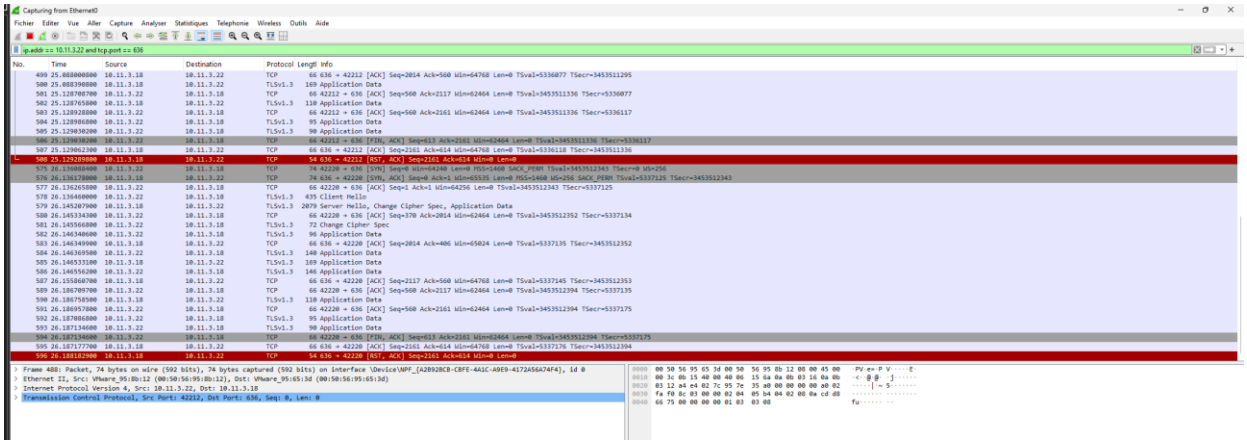


VÉRIFICATION FINALE — PREUVE DU CHIFFREMENT

Pour prouver que le chiffrement est effectif, réaliser une capture réseau montrant la différence entre LDAP (clair) et LDAPS (chiffré).

Vérification via Wireshark

- Lancer Wireshark sur SRV-GLPI ou un poste du LAN
- Appliquer le filtre : tcp.port == 636
- Déclencher une authentification GLPI
- Les paquets doivent afficher : TLS Application Data (chiffré)



Conclusion

La mise en œuvre de cette procédure a permis d'élever significativement le niveau de sécurité de l'infrastructure. En migrant l'authentification de l'annuaire du protocole standard LDAP (port 389) vers LDAPS (port 636), la vulnérabilité critique liée à l'interception des identifiants en clair a été définitivement corrigée. Le déploiement d'une Autorité de Certification (AD CS) et l'intégration du certificat racine au sein du conteneur GLPI ont permis d'établir un tunnel chiffré de bout en bout. Enfin, la validation technique par analyse de trames réseau a confirmé l'utilisation d'une session TLSv1.3 robuste. Cette démarche proactive garantit une infrastructure de production conforme aux exigences actuelles de cybersécurité et aux standards de durcissement des systèmes d'information.