DOCUMENTATION TECHNIQUE

Déploiement d'une solution centralisée de gestion des identités et du support informatique avec Active Directory et GLPI

Intégration LDAP • Habilitations • Gestion des incidents

Emmanuel Kadina
BTS SIO option SISR
Projet réalisé du 12 au 17 novembre 2026
Environnement de laboratoire

Sommaire

1. Présentation générale **3**

1.1 Contexte et problématique . . . 3

1.2 Objectifs . . . 3

1.3 Organisation du projet . . . 3

1.4 Anonymisation . . . 3

2. Architecture et environnement technique **3**

2.1 Architecture logique . . . 3

2.2 Environnement . . . 3

2.3 Prérequis . . . 4

2.4 Outils . . . 4

3. Étape 1 - Intégration d'Active Directory à GLPI via LDAP **5**

3.1 Préparation de l'annuaire . . . 5

3.2 Création du compte de service . . . 5

3.3 Relevé du nom distinctif (DN) . . . 5

3.4 Configuration de l'annuaire LDAP dans GLPI . . . 6

3.5 Choix technique : LDAP en clair sur le port 389 . . . 6

3.6 Test de la connexion et importation . . . 7

4. Étape 2 - Centralisation des utilisateurs et habilitations **8**

4.1 Ajout et importation de comptes . . . 8

4.2 Profils et habilitations . . . 9

4.3 Vérification par connexion de chaque compte . . . 9

5. Étape 3 - Gestion des incidents **12**

5.1 Scénario . . . 12

5.2 Déroulement . . . 12

5.3 Résolution et clôture . . . 14

6. Tests réalisés et résultats **16**

7. Difficultés rencontrées et solutions **16**

8. Bilan technique et compétences acquises **16**

9. Pistes d'amélioration **16**

1. Présentation générale

1.1 Contexte et problématique

Une organisation fictive souhaite que ses utilisateurs accèdent à l'outil de gestion de parc et de support GLPI avec leurs identifiants Active Directory, sans second annuaire à maintenir. Elle veut aussi que chacun dispose de droits adaptés à son rôle et que chaque demande d'assistance soit tracée de sa création à sa clôture.

Problématique : comment relier l'annuaire et l'outil de support, limiter les droits de chaque profil et formaliser le traitement des incidents ?

1.2 Objectifs

- Relier GLPI à l'annuaire Active Directory par le protocole LDAP.
- Importer les comptes de l'annuaire et leur attribuer un profil selon leurs responsabilités.
- Traiter un incident de bout en bout, du signalement à la clôture, en tenant successivement les rôles d'utilisateur, de technicien et d'administrateur.

1.3 Organisation du projet

Le projet est conduit en trois étapes successives, chacune s'appuyant sur la précédente :

Étape	Intitulé	Résultat attendu
1	Intégration d'Active Directory à GLPI via LDAP	Annuaire configuré, testé, premiers comptes importés
2	Centralisation des utilisateurs et gestion des habilitations	Quatre comptes importés, profils Super-Admin, Technicien, Self-Service
3	Mise en œuvre du processus de gestion des incidents	Un ticket traité et clos selon le cycle complet

1.4 Anonymisation

> Les captures ont été anonymisées : le nom de domaine interne et les adresses IP sont masqués par des aplats noirs ou gris. Dans ce document, ils sont désignés par « <domaine> » et « <IP> ». Les comptes de test (user1 à user4) et le compte de service (glpisync) sont des identifiants génériques de laboratoire.

2. Architecture et environnement technique

2.1 Architecture logique

Les utilisateurs se connectent à GLPI avec leur identifiant de domaine. GLPI interroge Active Directory en LDAP avec un compte de service dédié, **glpisync**, qui lit les comptes de l'unité d'organisation **glpi-users**.



Schéma 1 - Architecture logique de la solution

2.2 Environnement

Élément	Description
Annuaire	Windows Server avec Active Directory Domain Services (contrôleur de domaine), domaine <domaine>
Outil de support	GLPI sur serveur Linux, accessible depuis un navigateur web

Élément	Description
Protocole d'annuaire	LDAP, port 389 (non chiffré)
Outils d'administration	Console « Utilisateurs et ordinateurs Active Directory », PowerShell
Comptes	glpisync (compte de service, OU synch) ; user1 à user4 (OU glpi-users)

2.3 Prérequis

- Un contrôleur de domaine Active Directory opérationnel.
- Une instance GLPI accessible, avec un compte Super-Admin.
- Une communication réseau entre le serveur GLPI et le contrôleur de domaine sur le port 389.

2.4 Outils

Outil	Rôle dans le projet
Active Directory	Annuaire central : stockage des comptes et de leur organisation en OU
LDAP	Protocole d'interrogation de l'annuaire par GLPI
GLPI	Gestion des utilisateurs, des profils et des tickets (ITSM)
PowerShell	Relevé du nom distinctif (DN) du compte de service

3. Étape 1 - Intégration d'Active Directory à GLPI via LDAP

3.1 Préparation de l'annuaire

Deux unités d'organisation (OU) sont créées pour séparer les rôles : **synch** accueille le compte de service, **glpi-users** accueille les comptes des utilisateurs. Cette séparation permet de limiter la recherche de GLPI aux seuls comptes utilisateurs.

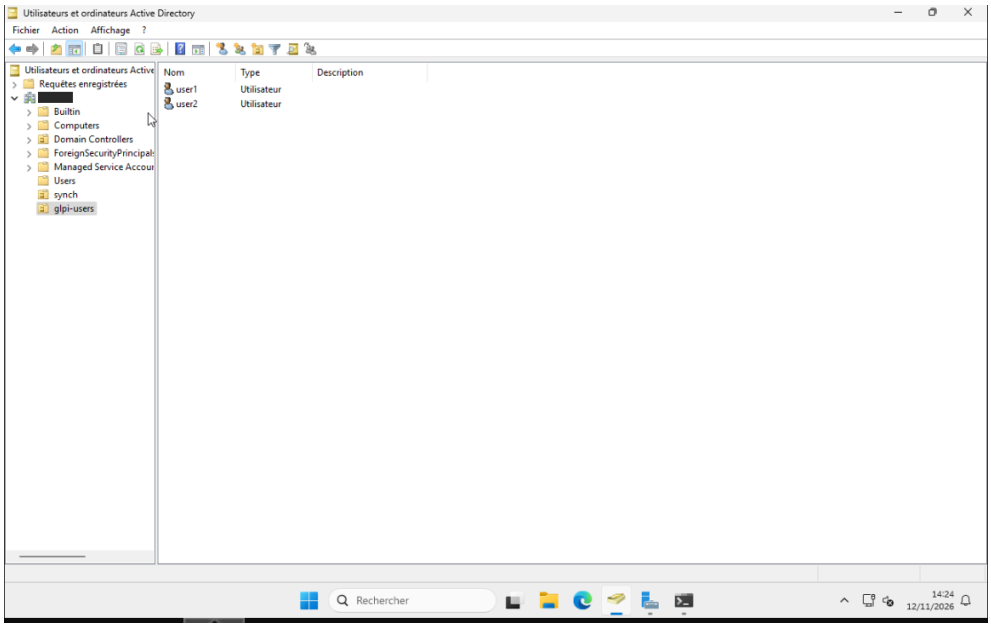


Figure 1 *- Active Directory : OU glpi-users contenant user1 et user2.*

3.2 Création du compte de service

Le compte **glpisync** est créé dans l'OU synch. Il sert uniquement à la liaison (bind) entre GLPI et l'annuaire ; l'utiliser plutôt qu'un compte d'administration limite l'exposition en cas de compromission.

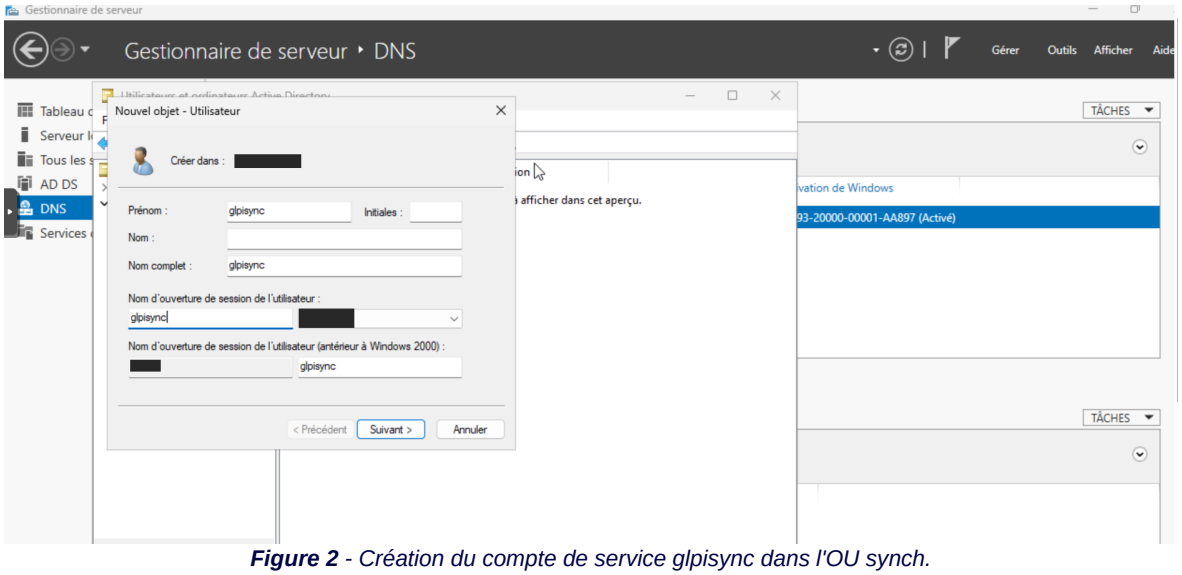


Figure 2 *- Création du compte de service glpisync dans l'OU synch.*

3.3 Relevé du nom distinctif (DN)

GLPI attend le DN complet du compte de liaison. Il est relevé avec PowerShell au moyen de la commande `Get-ADUser`, visible sur la capture.

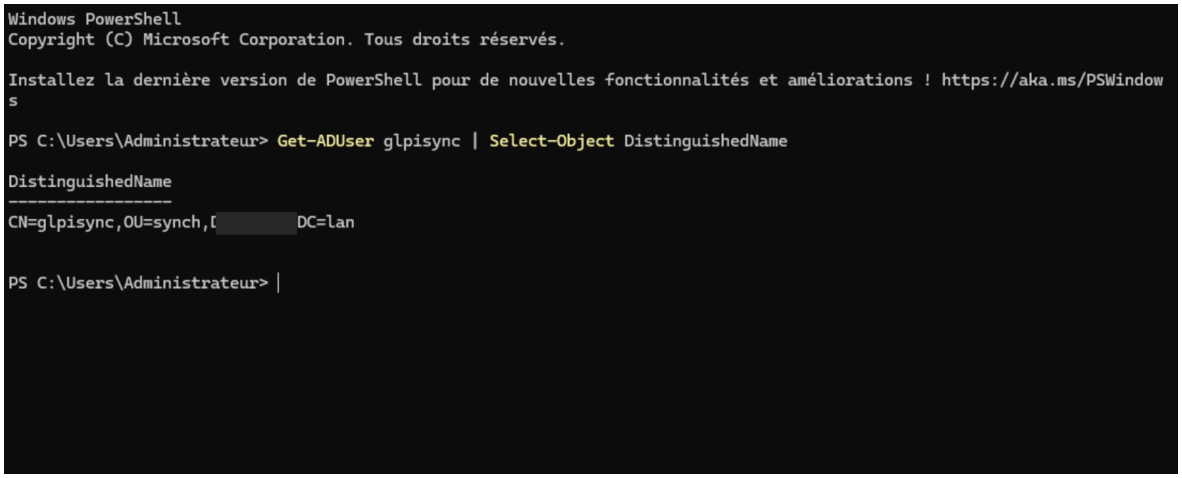


Figure 3 *- Relevé du DN du compte glpisync avec PowerShell.*

3.4 Configuration de l'annuaire LDAP dans GLPI

Dans Configuration > Authentification > Annuaires LDAP, l'annuaire est renseigné avec les paramètres suivants :

Paramètre	Valeur	Justification
Serveur	<IP> du contrôleur de domaine	Hôte interrogé par GLPI
Port	389	Port LDAP standard
BaseDN	OU glpi-users du domaine <domaine>	Restreint la recherche aux comptes utilisateurs
Utiliser bind	Oui	Les connexions anonymes ne sont pas utilisées
DN du compte	DN de glpisync	Compte de liaison dédié
Mot de passe	Mot de passe de glpisync	Masqué dans l'interface

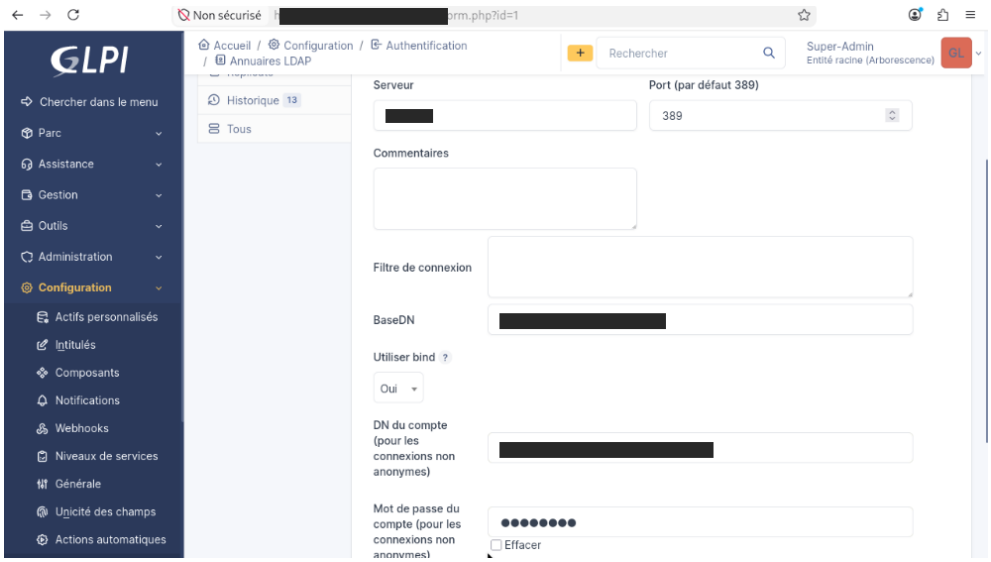


Figure 4 *- Configuration de l'annuaire LDAP dans GLPI (serveur, BaseDN et DN masqués).*

3.5 Choix technique : LDAP en clair sur le port 389

Choix et limite. Le LDAP sur le port 389 transmet les échanges, dont le mot de passe du compte de liaison, sans chiffrement. Ce choix est acceptable dans un laboratoire isolé, car il simplifie la mise en place et le diagnostic. **En production, LDAPS (port 636) ou LDAP avec StartTLS serait à privilégier**, avec un certificat sur le contrôleur de domaine, afin de protéger les identifiants en transit.

3.6 Test de la connexion et importation

Le test intégré à GLPI valide successivement la connexion au serveur, le port, la base de recherche, l'URI LDAP et l'authentification du compte, puis effectue une recherche : 50 entrées sont trouvées. user1 et user2 sont ensuite importés.

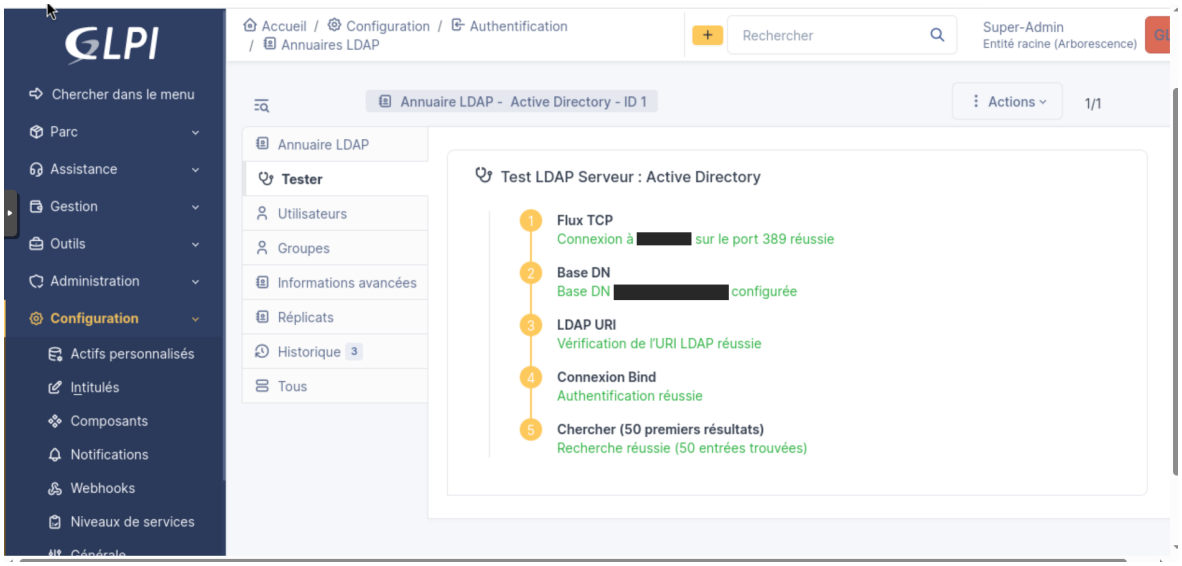


Figure 5 *- Test LDAP réussi : 5 étapes validées, 50 entrées trouvées.*

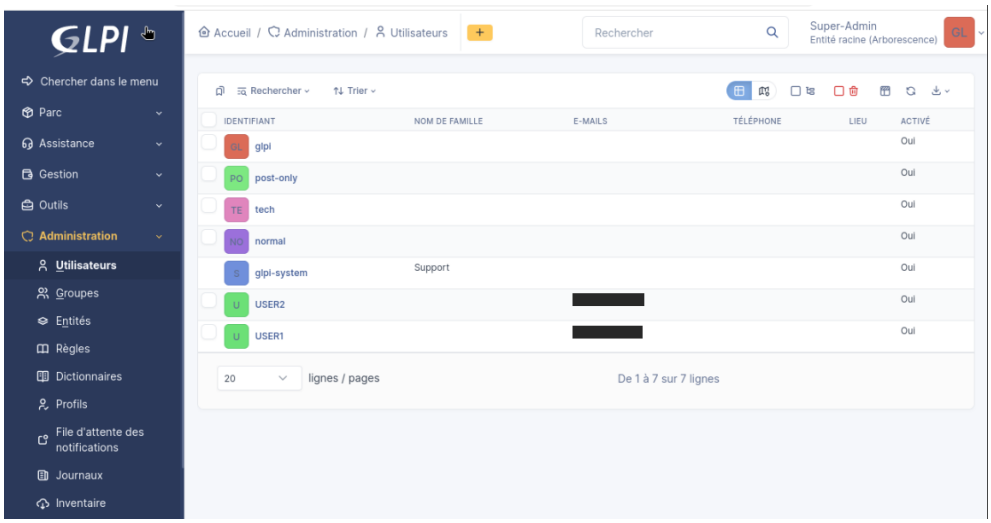


Figure 6 *- user1 et user2 importés dans la liste des utilisateurs GLPI.*

4. Étape 2 - Centralisation des utilisateurs et habilitations

4.1 Ajout et importation de comptes

Deux comptes supplémentaires, user3 et user4, sont créés dans l'OU glpi-users puis importés dans GLPI par LDAP le 12/11/2026. Les quatre comptes sont désormais gérés depuis l'annuaire, qui reste la source unique d'identité.

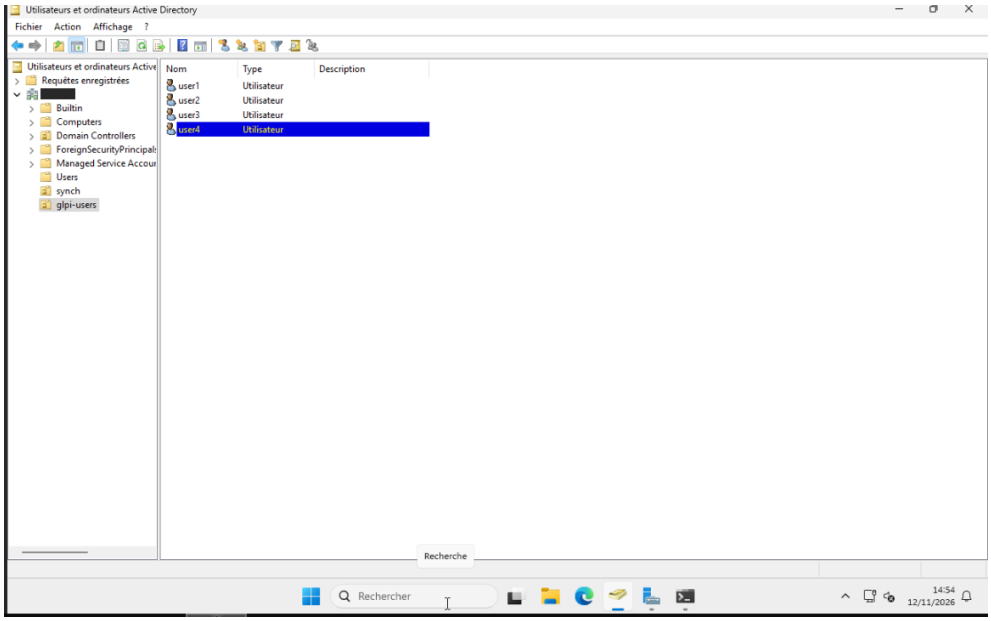


Figure 7 *- Les quatre utilisateurs de l'OU glpi-users dans Active Directory.*

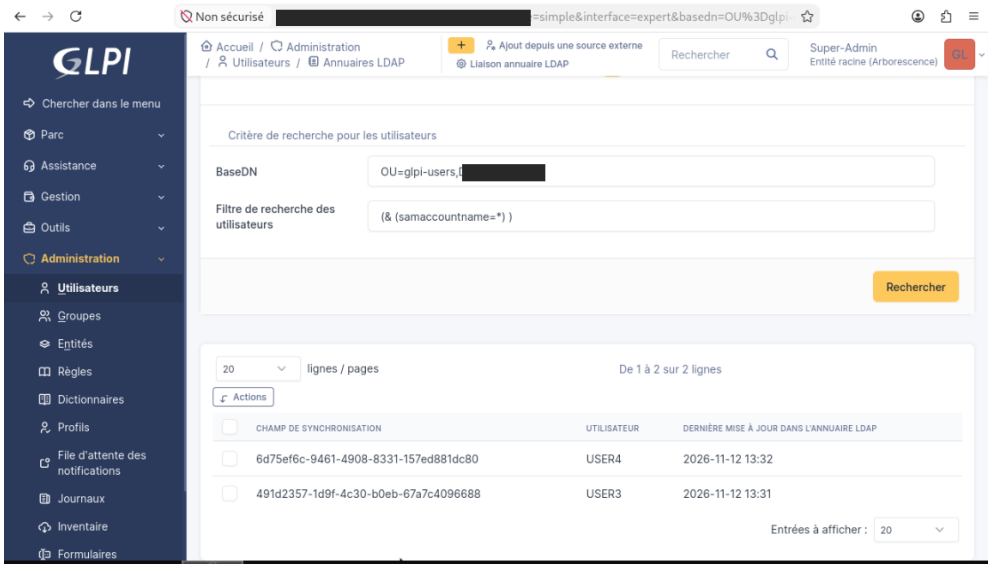


Figure 8 *- Importation LDAP de user3 et user4 dans GLPI.*

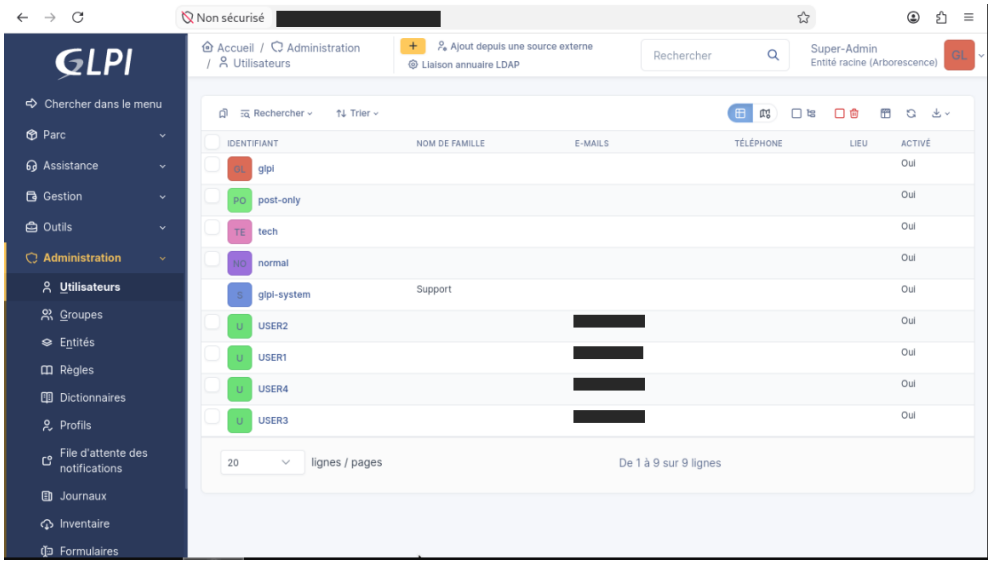


Figure 9 *- Les quatre comptes présents dans GLPI.*

4.2 Profils et habilitations

Un profil est attribué à chaque compte selon sa responsabilité :

Compte	Profil	Rôle dans le projet
user1	Super-Admin	Administration, affectation des tickets
user2	Technicien	Traitement des incidents
user3	Self-Service	Demandeur
user4	Self-Service	Demandeur

> La capture de l'onglet Habilitations de user2 présente le formulaire d'attribution ; l'application effective des profils est démontrée par les connexions de chaque compte (4.3).

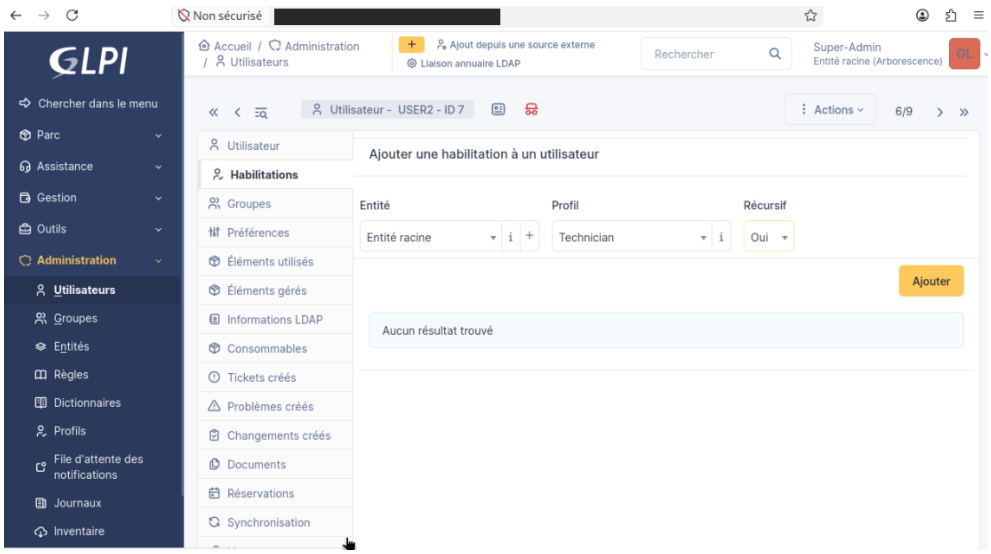


Figure 10 *- Onglet Habilitations de user2 dans GLPI.*

4.3 Vérification par connexion de chaque compte

Chaque utilisateur se connecte à GLPI avec son identifiant de domaine. Le profil actif, affiché en en-tête, et le menu proposé correspondent au rôle attendu : interface complète pour le Super-Admin, interface de traitement pour le Technicien, interface simplifiée pour les profils Self-Service.

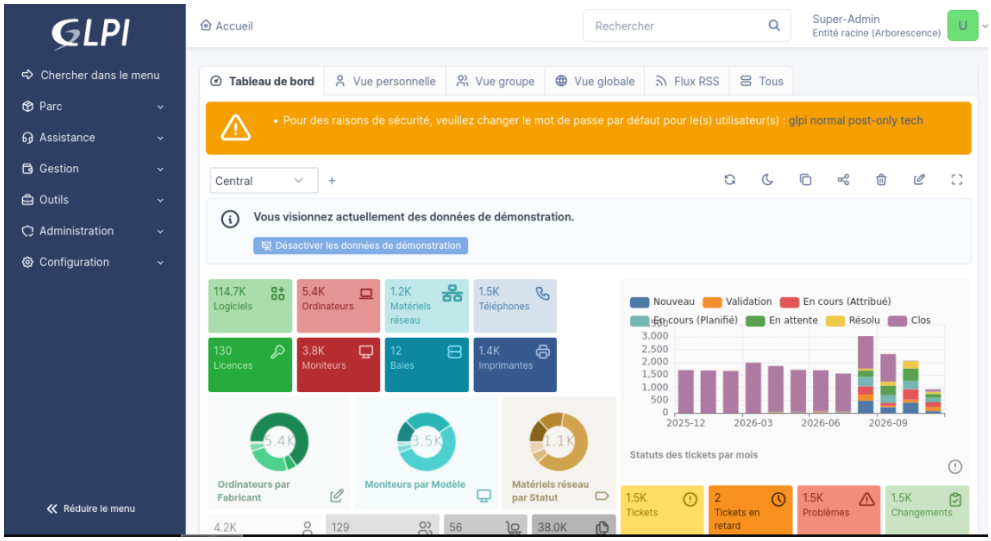


Figure 11 *- Connexion de user1 : profil Super-Admin.*

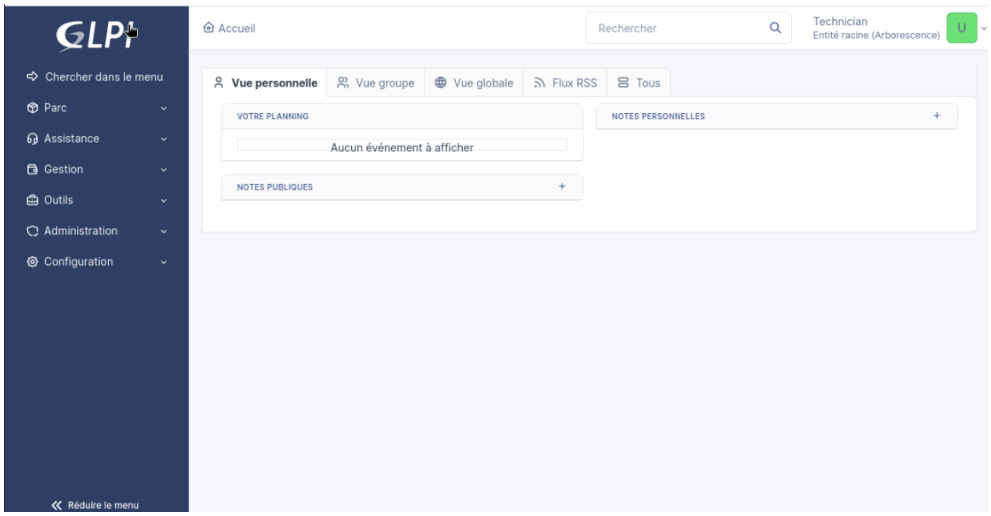


Figure 12 *- Connexion de user2 : profil Technicien.*

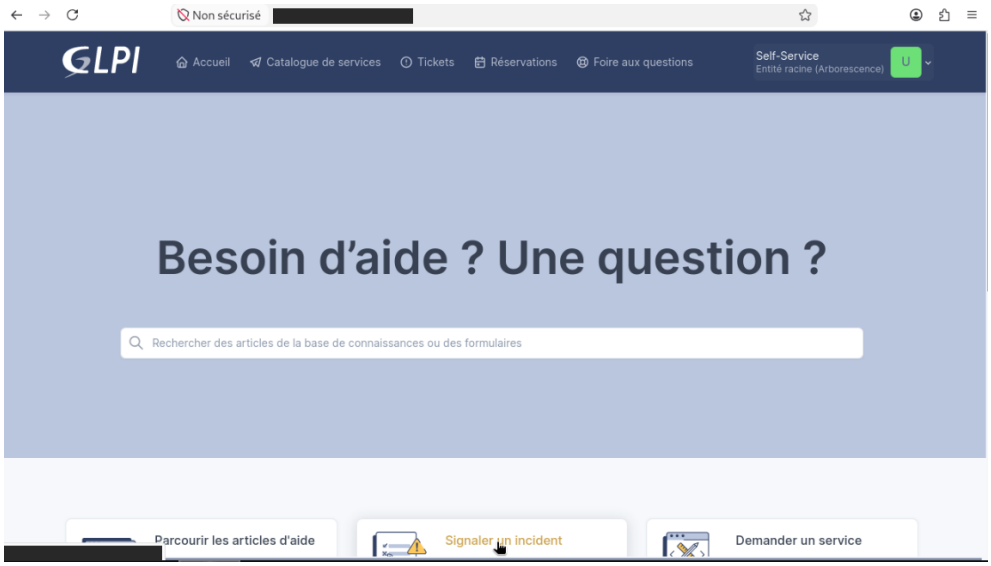


Figure 13 *- Connexion de user3 : profil Self-Service.*

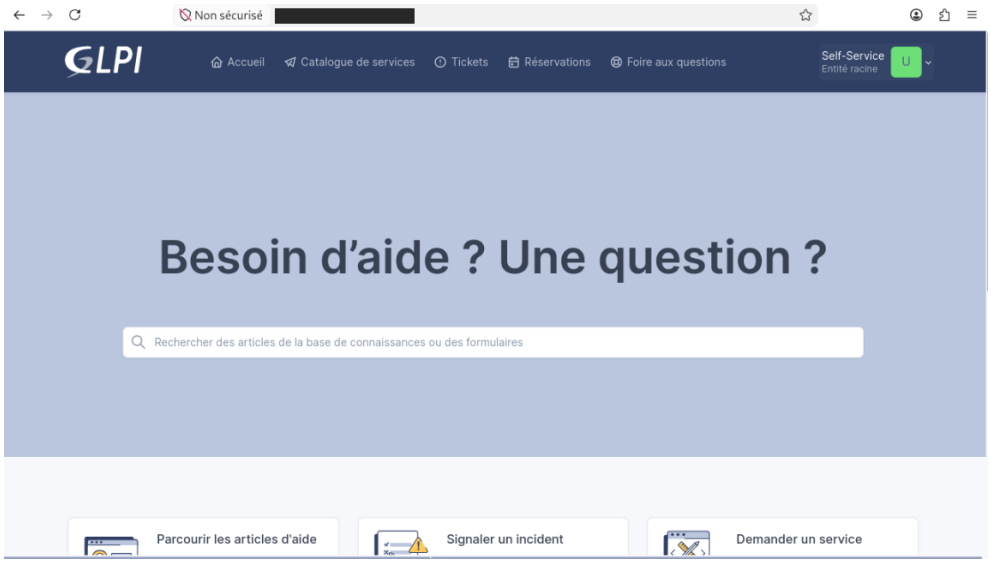


Figure 14 *- Connexion de user4 : profil Self-Service.*

5. Étape 3 - Gestion des incidents

5.1 Scénario

L'incident traité est : **« Impossible d'accéder au dossier partagé de l'entreprise »**, catégorie Réseau / Partage de fichiers, priorité moyenne. Le demandeur est user3 ; le ticket est affecté à user2 par user1.

Phase du cycle	Acteur	Capture
Ticket de user3, attribué à user2	user3 / user1	Fig. 15
Prise en charge, réponse au demandeur	user2	Fig. 16
Diagnostic (suivi privé)	user2	Fig. 17
Tâche technique et suivis d'intervention	user2	Fig. 18 à 20
Solution proposée (statut Résolu)	user2	Fig. 21
Solution approuvée le 17/11/2026 à 15:04	user3	Fig. 22
Ticket clos	Super-Admin	Fig. 23

5.2 Déroulement

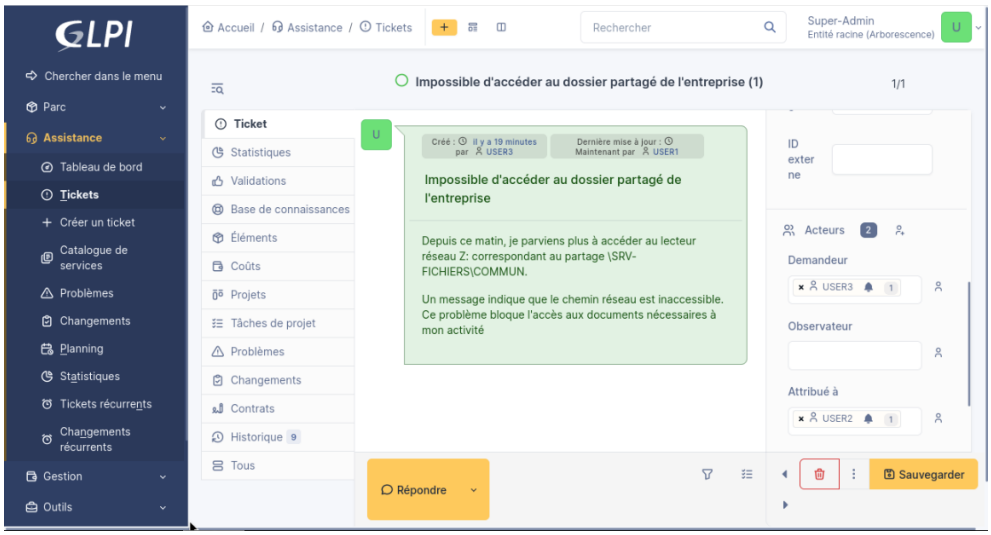


Figure 15 *- Ticket créé par user3 et attribué à user2.*

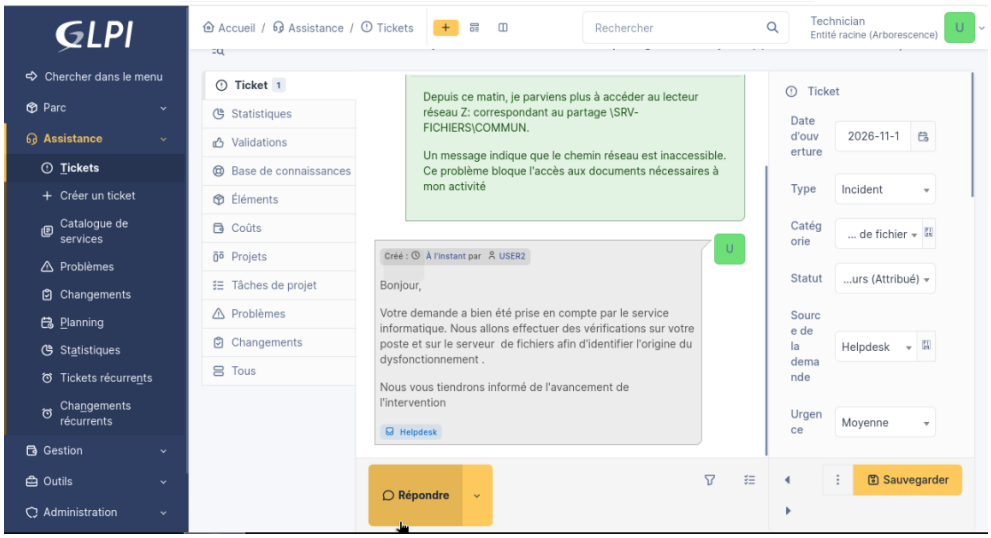


Figure 16 *- Réponse de prise en charge par user2.*

Le diagnostic est consigné dans un **suivi privé**, visible des seuls techniciens : le demandeur ne voit que les informations utiles à sa demande.

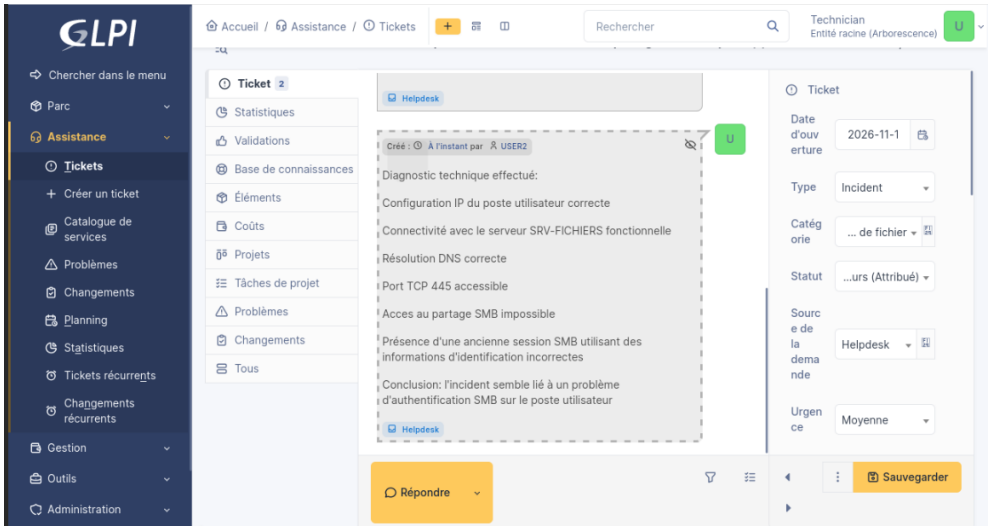


Figure 17 *- Suivi privé de diagnostic technique.*

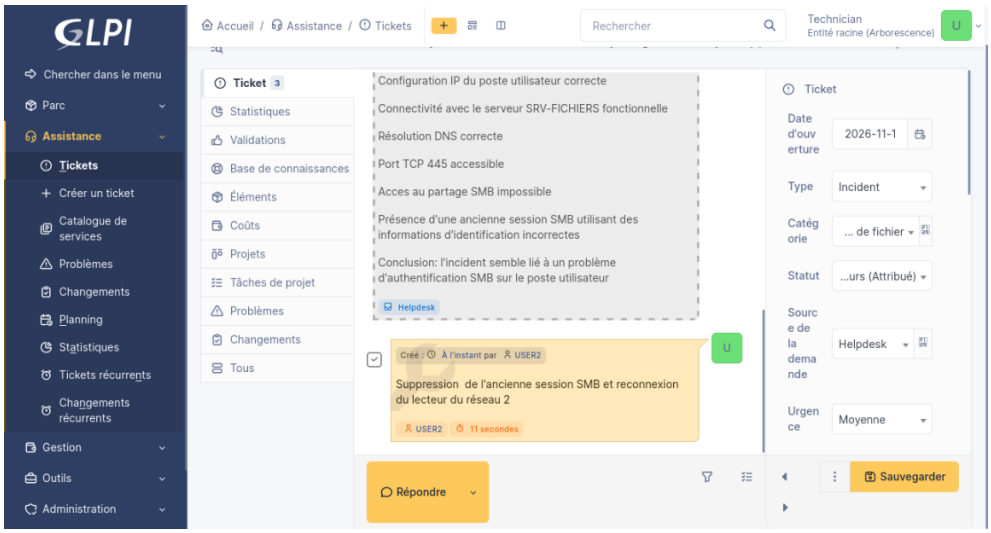


Figure 18 *- Tâche technique créée dans le ticket.*

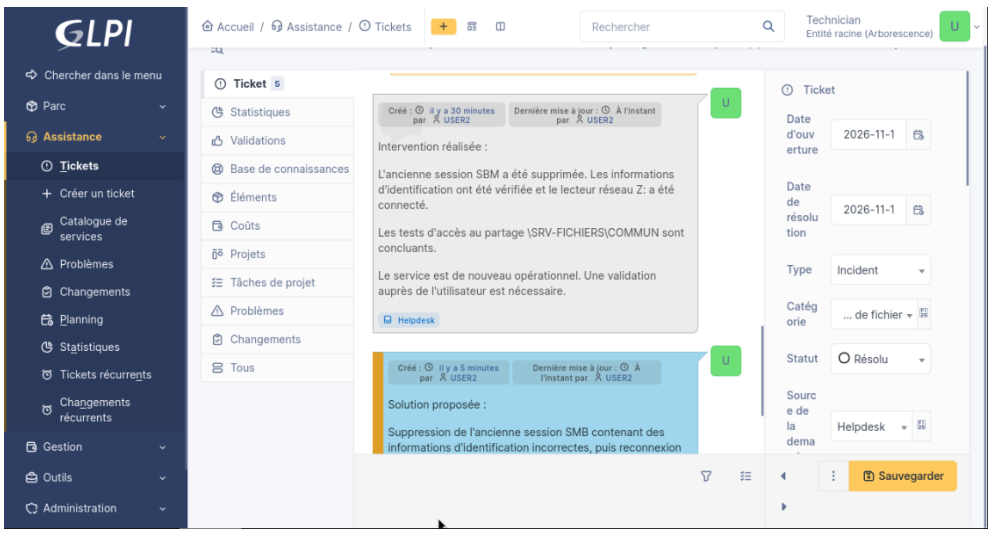


Figure 19 *- Suivi d'intervention du technicien.*

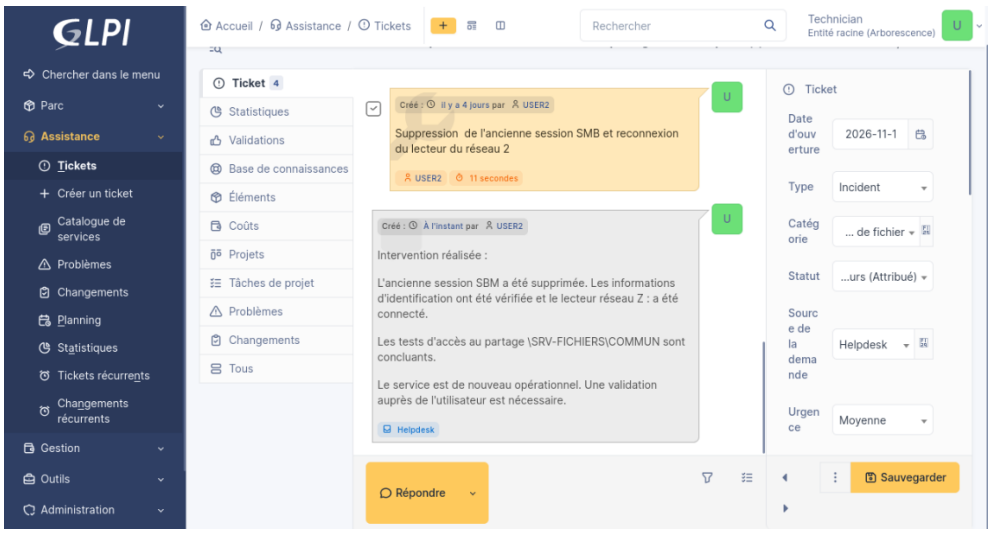


Figure 20 *- Compte rendu d'intervention de user2.*

5.3 Résolution et clôture

user2 propose une solution, qui place le ticket au statut Résolu. user3, demandeur, l'approuve ; le ticket passe alors à l'état Clos, ce que confirme la liste des tickets.

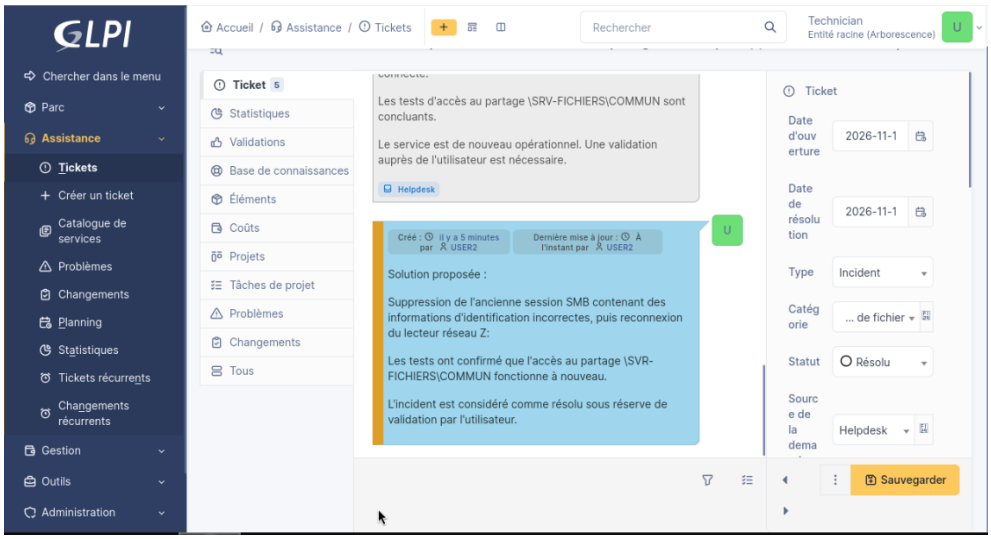


Figure 21 *- Solution proposée, ticket au statut Résolu.*

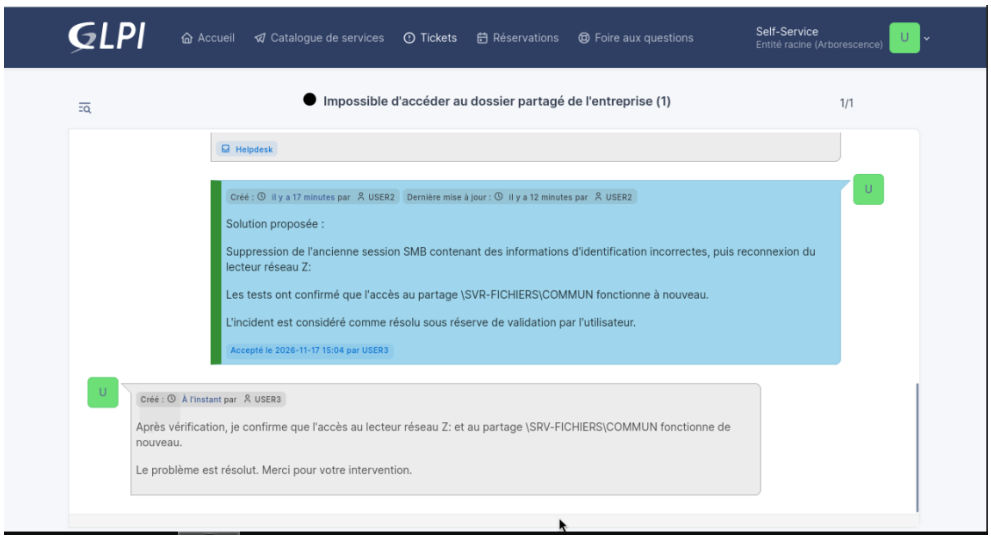


Figure 22 *- Solution approuvée par user3.*

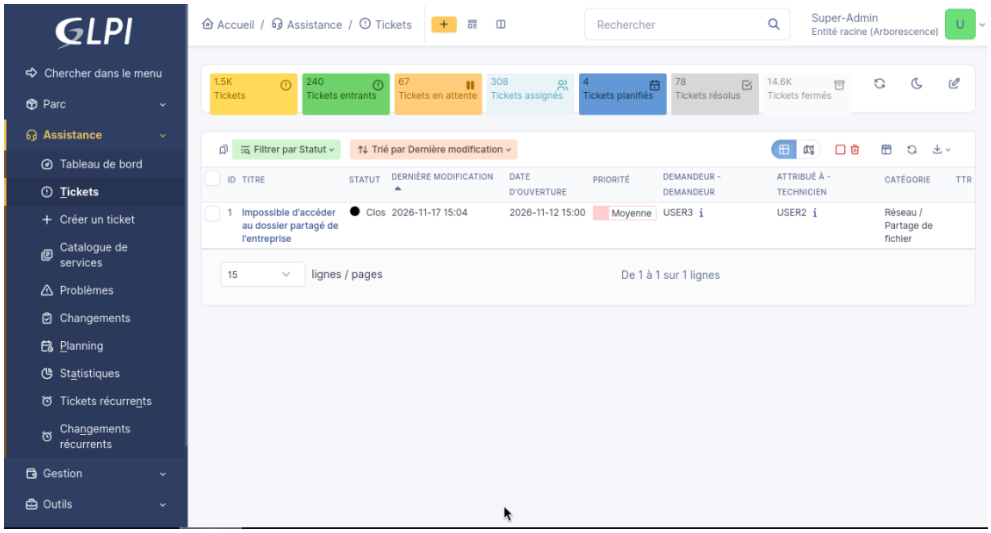


Figure 23 *- Ticket clos dans la liste des tickets.*

6. Tests réalisés et résultats

Test	Résultat	Preuve
Test de connexion LDAP depuis GLPI (connexion, port, base, URI, authentification, recherche)	Réussi, 50 entrées trouvées	Fig. 5
Importation de user1 et user2, puis de user3 et user4	Quatre comptes présents dans GLPI	Fig. 6, 8, 9
Connexion de user1, user2, user3 et user4	Profil attendu pour chacun	Fig. 11 à 14
Traitement complet d'un ticket (affectation, diagnostic, tâche, solution, approbation, clôture)	Ticket clos	Fig. 15 à 23

Périmètre. Aucune capture ne documente la synchronisation d'une modification d'attribut de l'annuaire vers GLPI, ni un test exhaustif des restrictions de droits. Ces vérifications n'étant pas démontrées, elles ne sont pas présentées comme réalisées. De même, le formulaire de création du ticket n'est pas capturé : l'auteur user3 ressort du champ « Créé par » du ticket.

7. Difficultés rencontrées et solutions

Difficulté	Solution
Renseigner le compte de liaison avec son DN complet	Relevé du DN avec PowerShell (Get-ADUser)
N'importer que les comptes utilisateurs	BaseDN positionné sur l'OU glpi-users
Respecter les rôles du processus	Chaque étape du ticket est réalisée avec le profil concerné

8. Bilan technique et compétences acquises

Le projet montre qu'un compte unique dans Active Directory suffit à ouvrir l'accès à GLPI, et que le profil détermine ensuite ce que chacun peut faire. Il a aussi nécessité de tracer chaque étape (configuration, test, capture) pour pouvoir la justifier.

Compétence (BTS SIO SISR)	Mobilisation	Justification
B1.2 Répondre aux incidents et demandes d'assistance	Principale	Cycle complet d'un ticket
B1.1 Gérer le patrimoine informatique	Principale	Profils Super-Admin, Technicien, Self-Service vérifiés par connexion
B1.5 Mettre à disposition un service informatique	Principale	Tests LDAP et de connexion ; acceptation par le demandeur
B2.2 Installer, tester et déployer une solution d'infrastructure réseau	Complémentaire	Liaison GLPI / Active Directory configurée et testée
B3.3 Sécuriser les équipements et les usages	Complémentaire	Compte de service dédié ; droits selon les rôles
B1.4 Travailler en mode projet	Complémentaire	Trois étapes successives

9. Pistes d'amélioration

- **Chiffrer les échanges :** passer à LDAPS ou StartTLS avec un certificat sur le contrôleur de domaine.
- **Limiter les droits du compte de service :** lecture seule sur l'OU glpi-users.

- **Automatiser la synchronisation :** planifier les actions automatiques LDAP de GLPI et tester la propagation des modifications d'attributs.
- **Gérer les profils par groupes :** affecter les profils selon l'appartenance à des groupes de l'annuaire.
- **Compléter les preuves :** capturer le formulaire de création du ticket et tester les restrictions de droits du profil Self-Service.