PROJET – Simulation d’un Centre de Services IT

Infrastructure AD sécurisée & implémentation ITSM avec SLA automatisés

Objectif du projet

Dans le cadre de ma montée en compétences en administration systèmes et gestion des services IT, j’ai conçu et simulé un centre de services IT complet basé sur les bonnes pratiques de AXELOS via le référentiel ITIL 4.

L’objectif était de reproduire le fonctionnement réaliste d’une PME de 20 à 50 utilisateurs, en structurant :

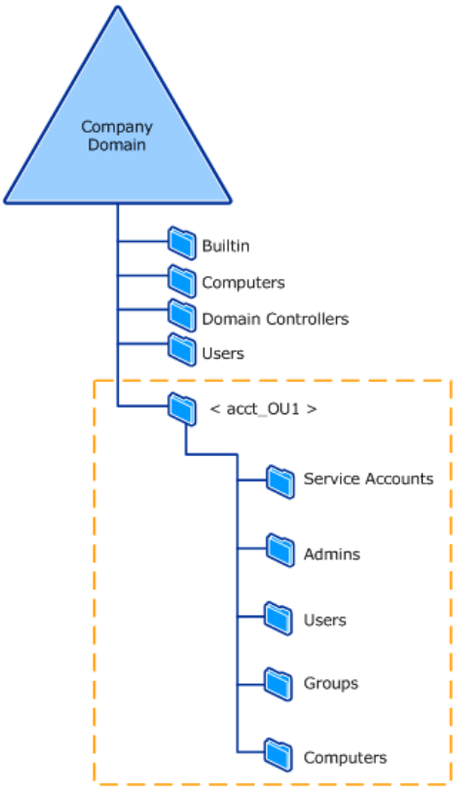
- Une infrastructure Active Directory sécurisée
- Un outil ITSM basé sur GLPI
- Une authentification centralisée via LDAP
- Des SLA automatisés
- Une base de connaissances
- Un workflow Support N1 / N2 structuré

J’ai volontairement reproduit le cycle complet de gestion des incidents :

Création → Qualification → Affectation → Traitement → Escalade → Résolution → Clôture

Architecture mise en place

Infrastructure Active Directory



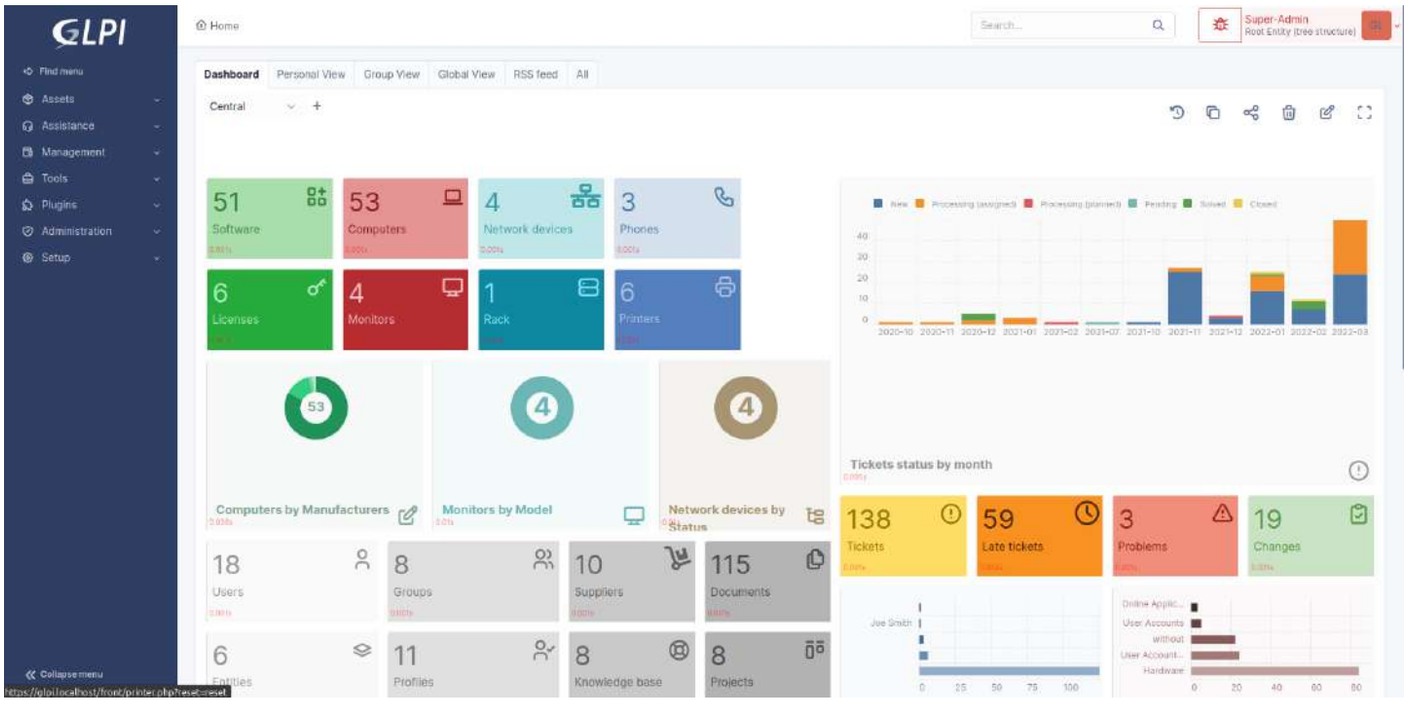
Mise en œuvre :

- Déploiement sous Windows Server 2022
- Structuration en OU (Utilisateurs, Postes, Serveurs, IT)
- Groupes de sécurité par rôle
- Comptes techniques dédiés
- Logique de séparation des privilèges

Ce que cela démontre :

Gestion des identités
Structuration logique
Maîtrise des droits
Organisation sécurisée

Plateforme ITSM – GLPI



Configuration complète :

- Intégration LDAP avec AD
- Création de profils N1 / N2
- Catégorisation des incidents
- Règles métiers automatisées
- SLA avec calcul automatique des délais
- Gestion du parc informatique

Ce que cela démontre :

Vision ITSM
Organisation du support
Automatisation des priorités
Structuration des processus

Application concrète des bonnes pratiques ITIL

Ce projet s'appuie sur :

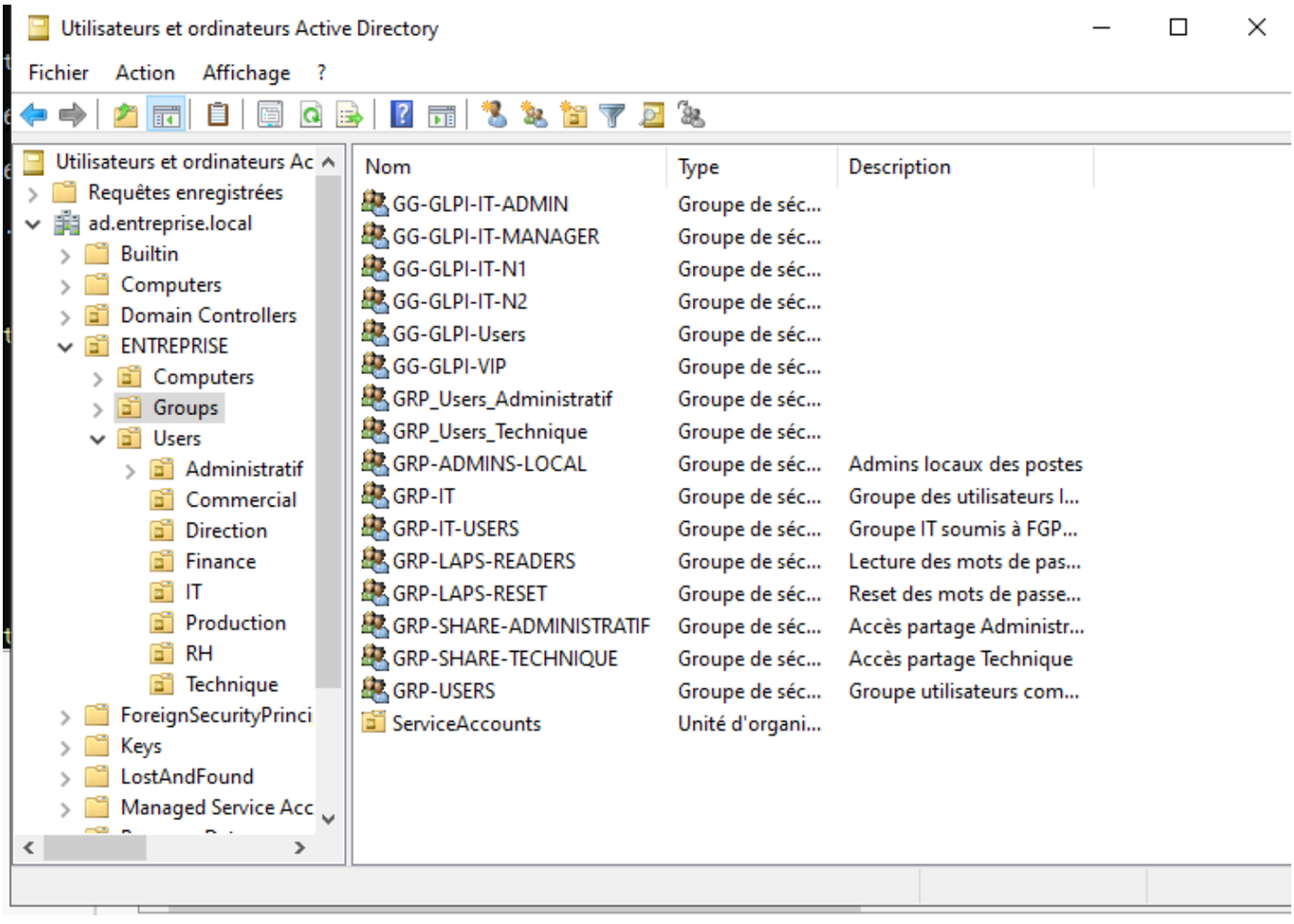
- Gestion des incidents
- Gestion des problèmes
- Gestion des niveaux de service
- Amélioration continue (logique PDCA)

Je ne me suis pas contenté de créer des tickets :
j'ai structuré un véritable processus opérationnel.

Livrables produits

- Infrastructure AD complète et organisée
- GLPI entièrement paramétré
- SLA opérationnels
- Parc informatique structuré
- Base de connaissances interne
- Dossier de preuves avec captures d'écran
- Simulation de tickets N1 → N2 jusqu'à clôture

Capture à insérer :



Architecture Active Directory du domaine ad.entreprise.local : organisation des OU par services, groupes de sécurité et comptes techniques.

Mise en place Active Directory (sécurité + organisation)

Structuration de l'Active Directory

Dans un premier temps, j'ai déployé un contrôleur de domaine sous Windows Server 2022, puis j'ai structuré l'annuaire Active Directory afin de reproduire l'organisation d'une PME réelle.

Organisation des OU

J'ai créé une OU principale ENTREPRISE, que j'ai subdivisée pour séparer logiquement :

- Les utilisateurs
- Les groupes
- Les ordinateurs
- Les comptes de service

J'ai structuré les comptes utilisateurs par service :

- Administratif
- Commercial

- Direction
- Finance
- IT
- Production
- RH
- Technique

Cette organisation me permet :

D’appliquer des stratégies ciblées
De faciliter la gestion des droits
De séparer les responsabilités
De préparer l’intégration LDAP avec GLPI

Création des groupes

Afin d’appliquer une gestion des droits propre et évolutive, j’ai créé plusieurs groupes de sécurité.

Groupes liés à GLPI

- GG-GLPI-IT-ADMIN
- GG-GLPI-IT-MANAGER
- GG-GLPI-IT-N1
- GG-GLPI-IT-N2
- GG-GLPI-Users
- GG-GLPI-VIP

Ces groupes sont utilisés pour l’intégration LDAP et l’attribution automatique des profils dans GLPI.

Groupes métiers

- GRP_IT
- GRP_USERS
- GRP_SHARE-ADMINISTRATIF
- GRP_SHARE-TECHNIQUE
- GRP-LAPS-READERS
- GRP-LAPS-RESET

Cette séparation respecte le principe de moindre privilège.

Création des comptes

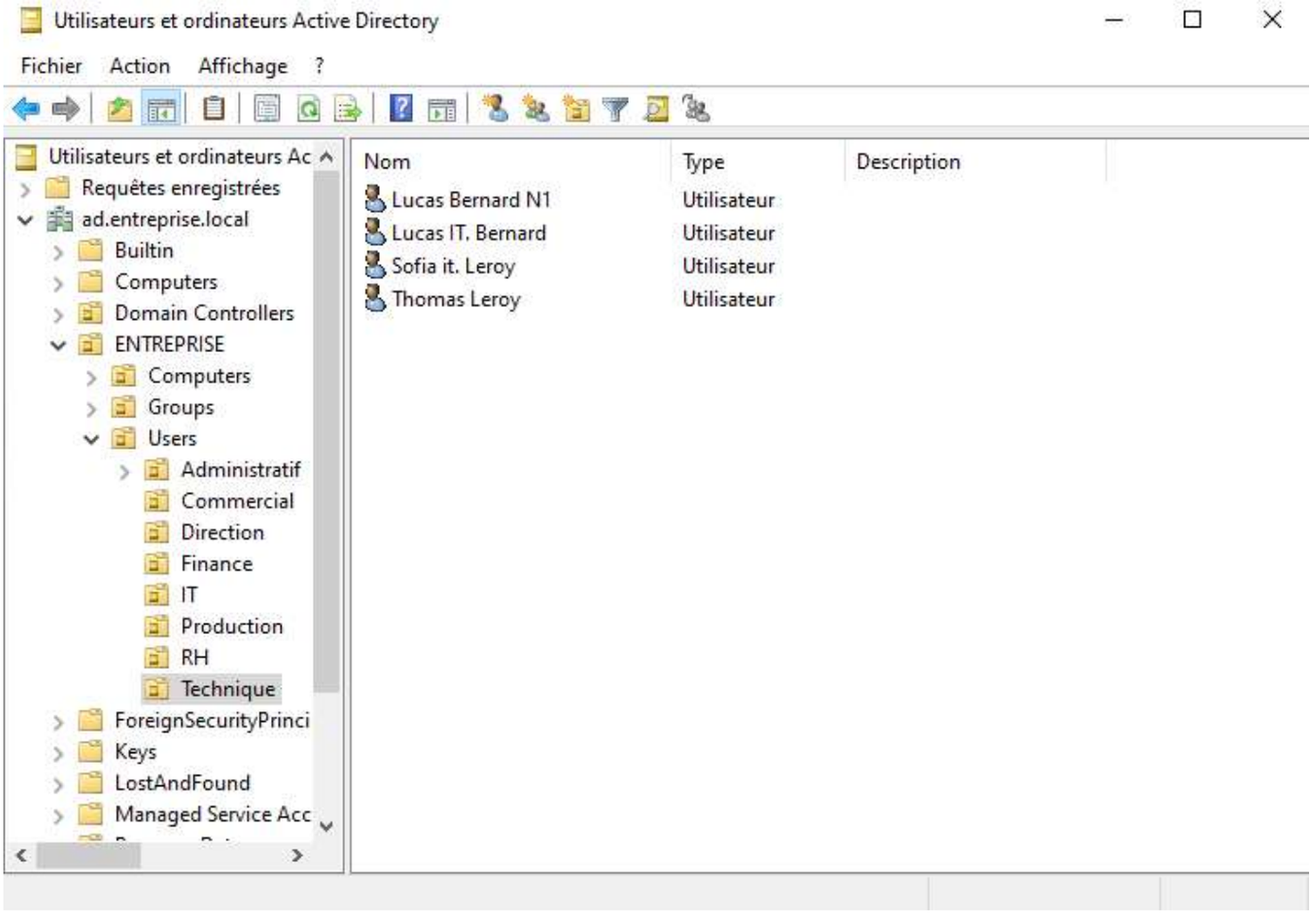
J'ai créé :

- Des comptes utilisateurs standards
- Des comptes techniques pour le support :
    - N1 Tech
    - N2 Tech
- Un compte de service dédié à l'intégration LDAP :
    - svc_glpi_ldap

Le compte LDAP est configuré avec des droits minimums de lecture sur l'annuaire.

Captures insérées :

Architecture Active Directory : structure des OU et groupes de sécurité



Groupes de sécurité créés dans Active Directory(Si tu as une capture PowerShell type Get-ADGroup, on peut la valoriser ici aussi.)

```
PS C:\Users\Administrateur> Get-ADGroup -Filter "Name -like '*GLPI*'" | Select Name

Name
----
GG-GLPI-Users
GG-GLPI-VIP
GG-GLPI-IT-N1
GG-GLPI-IT-N2
GG-GLPI-IT-ADMIN
GG-GLPI-IT-MANAGER
```

Politique de mot de passe (Sécurisation du domaine)

Dans une logique de sécurisation de l'infrastructure, j'ai configuré une politique de mot de passe conforme aux bonnes pratiques.

Paramètres appliqués :

- Complexité activée
- Longueur minimale définie
- Durée de validité configurée
- Historique des mots de passe activé
- Verrouillage du compte après plusieurs tentatives échouées

J'ai vérifié la configuration via PowerShell :

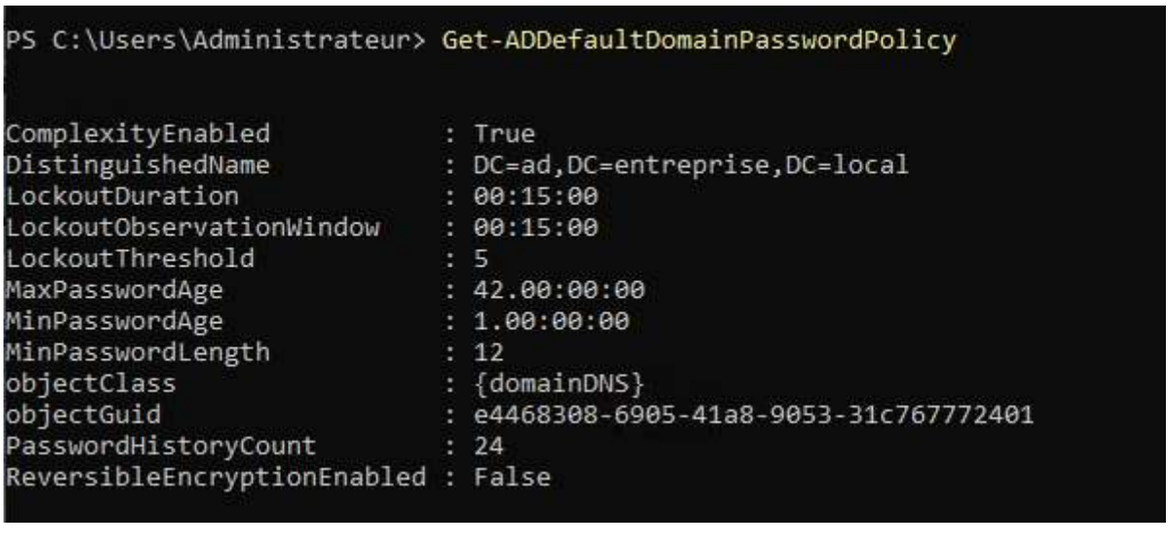
Get-ADDefaultDomainPasswordPolicy

Cette commande m'a permis de contrôler :

- MinPasswordLength
- PasswordHistoryCount
- LockoutThreshold
- MaxPasswordAge
- ComplexityEnabled

Capture insérée :

Vérification de la politique de mot de passe via PowerShell (Get-ADDefaultDomainPasswordPolicy)



Installation et configuration de GLPI

Initialisation de GLPI

Après l'installation de GLPI sur mon serveur, j'ai commencé par me connecter avec le compte Super-Admin afin d'effectuer la configuration initiale de la plateforme.

Lors de cette première connexion, j'ai vérifié plusieurs éléments essentiels :

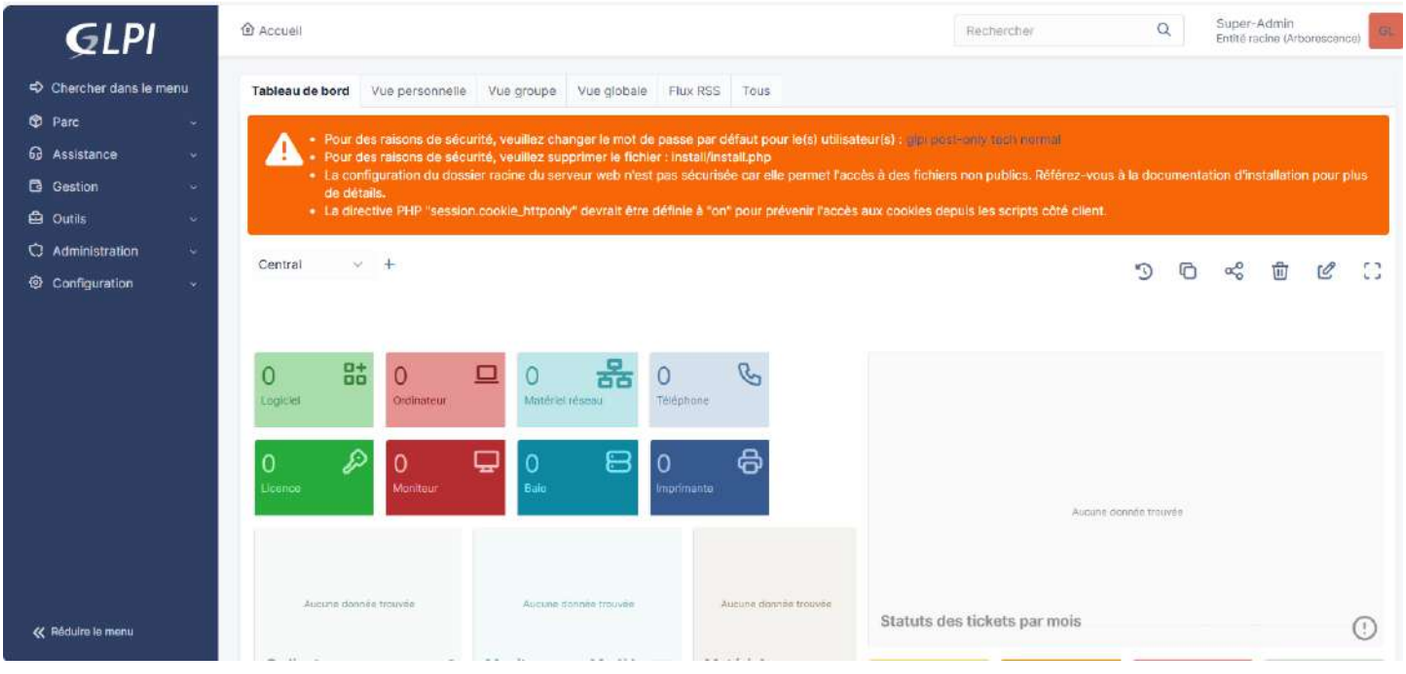
- L'entité racine active
- Les menus principaux :
    - Administration
    - Configuration
    - Assistance
    - Parc

Cette vérification m'a permis de m'assurer que l'environnement était fonctionnel et que je disposais des droits complets pour configurer le centre de services.

J'ai également contrôlé :

- Le bon fonctionnement des profils
- La présence des modules standards
- La structure globale avant toute personnalisation

Capture facultative à insérer : Écran d'accueil en profil Super-Admin



Création des lieux (organisation physique)

Afin de structurer le parc informatique de manière réaliste et cohérente, j'ai configuré une organisation physique représentant une PME.

Depuis Configuration → Lieux, j'ai créé l'arborescence suivante :

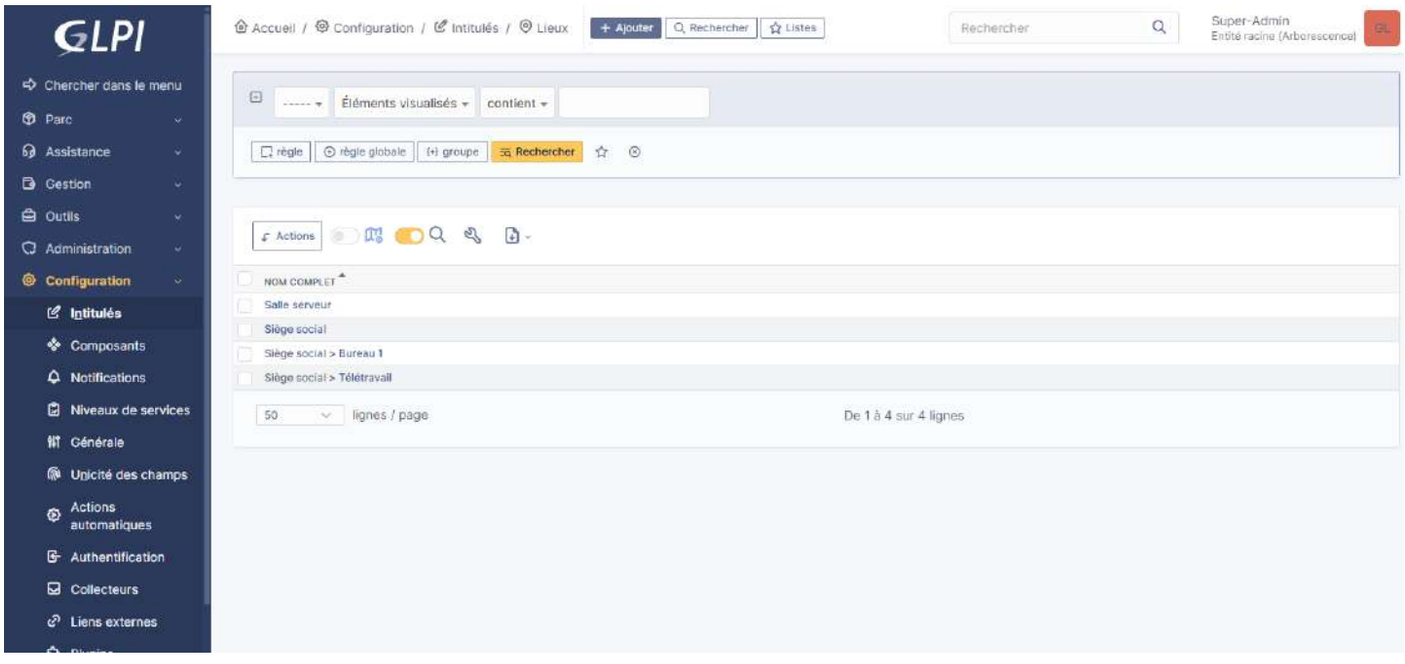
- Salle serveur
- Siège social
    - Siège social > Bureau 1
    - Siège social > Télétravail

Cette organisation me permet :

- D'affecter précisément les postes et serveurs
- De simuler une gestion multi-emplacements
- D'améliorer la traçabilité des équipements
- De faciliter les statistiques et le reporting

La structuration des lieux est une étape importante dans une démarche ITIL, car elle permet de relier les incidents à un contexte physique précis.

Capture à insérer :
Configuration → Lieux (avec l'arborescence visible)



Intégration LDAP (GLPI ↔ Active Directory)

Déclaration de l'annuaire LDAP

Après avoir structuré mon Active Directory, j'ai procédé à l'intégration entre GLPI et AD afin de centraliser l'authentification et la gestion des utilisateurs.

Depuis Configuration → Authentification → Annuaire LDAP, j'ai ajouté un nouvel annuaire en renseignant :

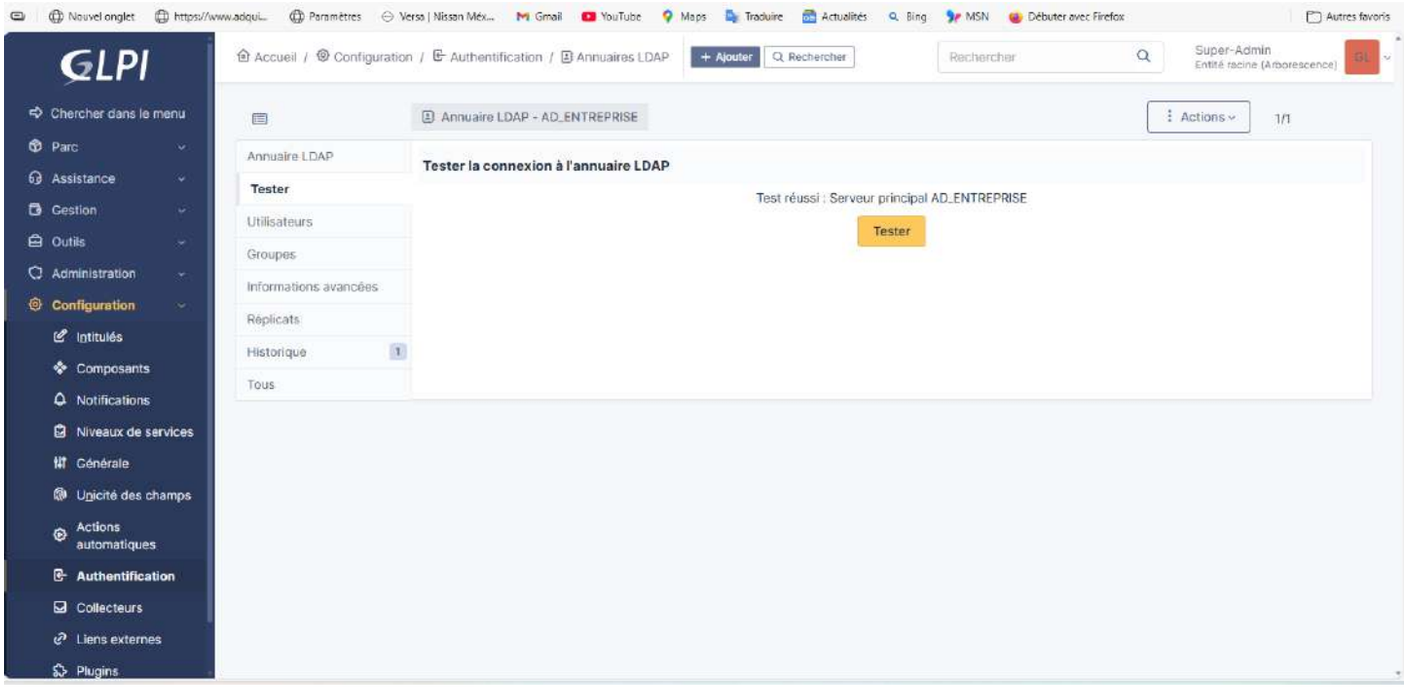
- Le type : Active Directory
- L'adresse du contrôleur de domaine
- Le port LDAP
- Le DN de base (Base DN)
- Le compte de service : svc_glpi_ldap
- Le mot de passe associé
- Le filtre de recherche utilisateurs
- Les attributs (login, nom, email…)

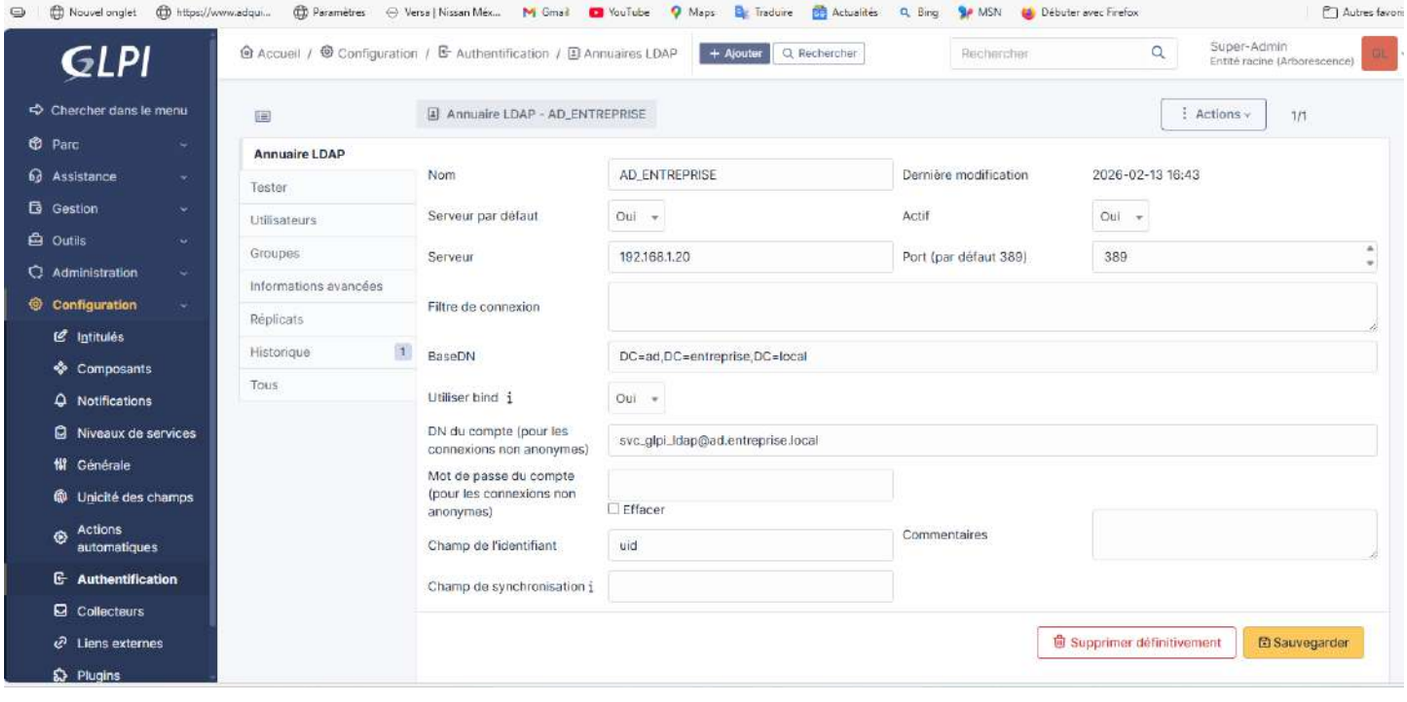
Une fois la configuration effectuée, j'ai réalisé un test de connexion LDAP afin de vérifier :

- L'accessibilité du contrôleur AD
- La validité des identifiants du compte de service
- La bonne lecture des objets AD

Le test étant concluant, l'intégration LDAP était opérationnelle.

Capture à insérer :
Annuaire LDAP configuré dans GLPI (écran configuration + test réussi)





Synchronisation des utilisateurs et des groupes

Une fois l'annuaire configuré, j'ai procédé à la synchronisation des comptes.

J'ai importé un utilisateur test : cmartin depuis Active Directory vers GLPI.

Après l'import :

- L'utilisateur est visible dans Administration → Utilisateurs
- L'authentification est désormais centralisée via AD
- Les informations (nom, prénom, email) sont récupérées automatiquement

J’ai ensuite vérifié l’appartenance aux groupes côté Active Directory afin de confirmer la cohérence de la synchronisation.

En PowerShell, j’ai utilisé :

Get-ADUser cmartin -Properties MemberOf

Cela m’a permis de confirmer que l’utilisateur était bien membre du groupe :

- GG-GLPI-IT-N1 (ou autre groupe métier selon ton test)

J’ai également effectué un test d’ajout au groupe :

Add-ADGroupMember -Identity "GG-GLPI-IT-N1" -Members cmartin

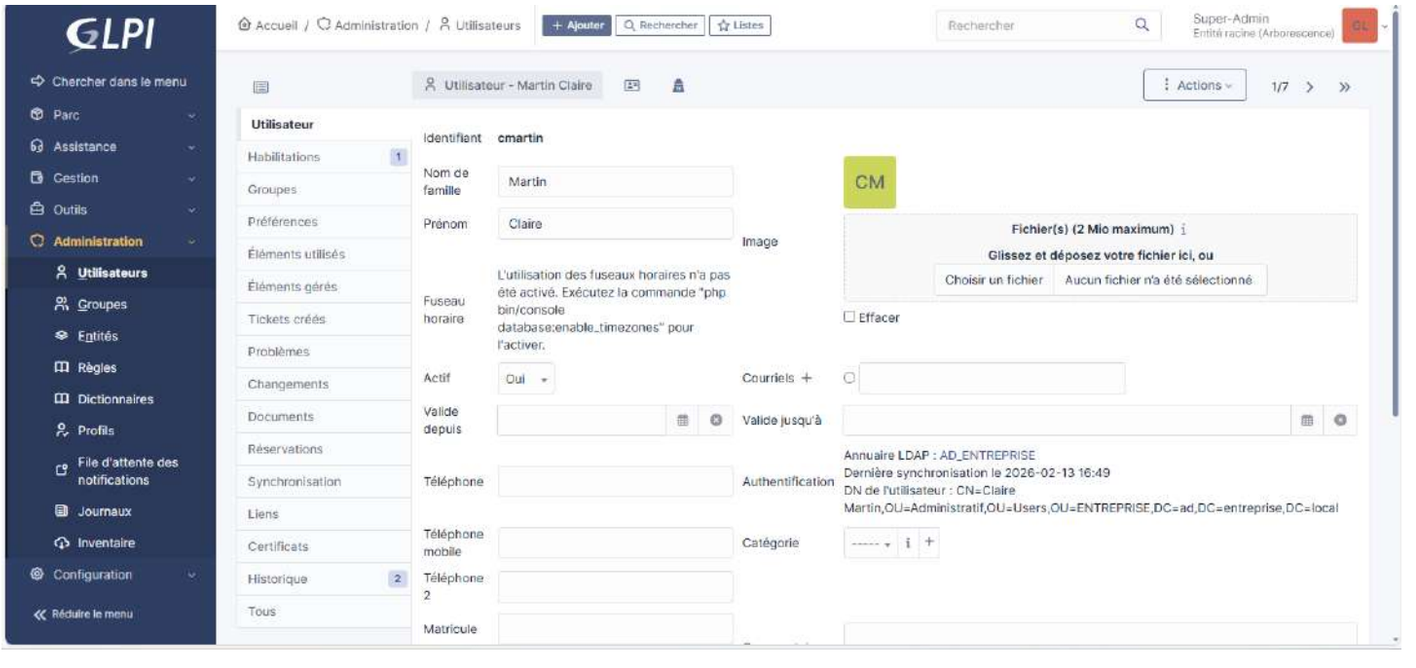
Puis vérification immédiate via MemberOf.

Cette étape démontre :

- La cohérence entre AD et GLPI
- Le bon fonctionnement de l’intégration LDAP
- La capacité à gérer les droits via groupes AD

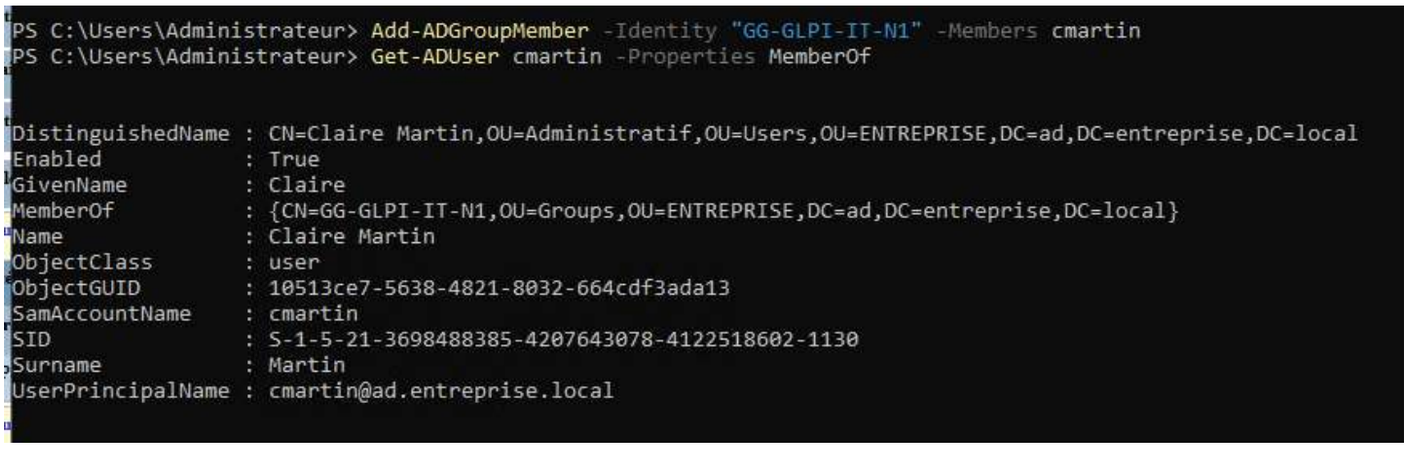
Captures à insérer :

Utilisateur cmartin visible dans GLPI



Capture PowerShell montrant :

Add-ADGroupMember



Structuration du Service Desk (ITIL)

Profils et rôles (N1 / N2 / Self-Service / Admin)

Après avoir intégré l'Active Directory à GLPI, j'ai structuré le centre de services afin de reproduire une organisation conforme aux bonnes pratiques ITIL.

J'ai configuré différents profils correspondant aux rôles d'un service informatique interne :

Self-Service

Ce profil est destiné aux utilisateurs finaux.
Il leur permet de :

- Créer un ticket
- Suivre l'évolution de leur demande
- Ajouter des commentaires
- Consulter la base de connaissances

Cela simule le portail utilisateur d'une PME.

Technicien N1

J'ai configuré un compte dédié au support de niveau 1 (tech_n1).

Le rôle N1 comprend :

- La prise en charge des tickets
- Le diagnostic de premier niveau
- La qualification des incidents
- L'escalade vers le niveau 2 si nécessaire

Ce profil reflète un support standard en centre de services.

Technicien N2

J’ai configuré un compte tech_n2 représentant le support de niveau 2.

Le rôle N2 comprend :

- L’analyse approfondie
- L’intervention sur serveurs et services applicatifs
- La résolution des incidents complexes
- La validation technique avant clôture

Ce niveau intervient principalement lors d’escalades.

Super-Admin

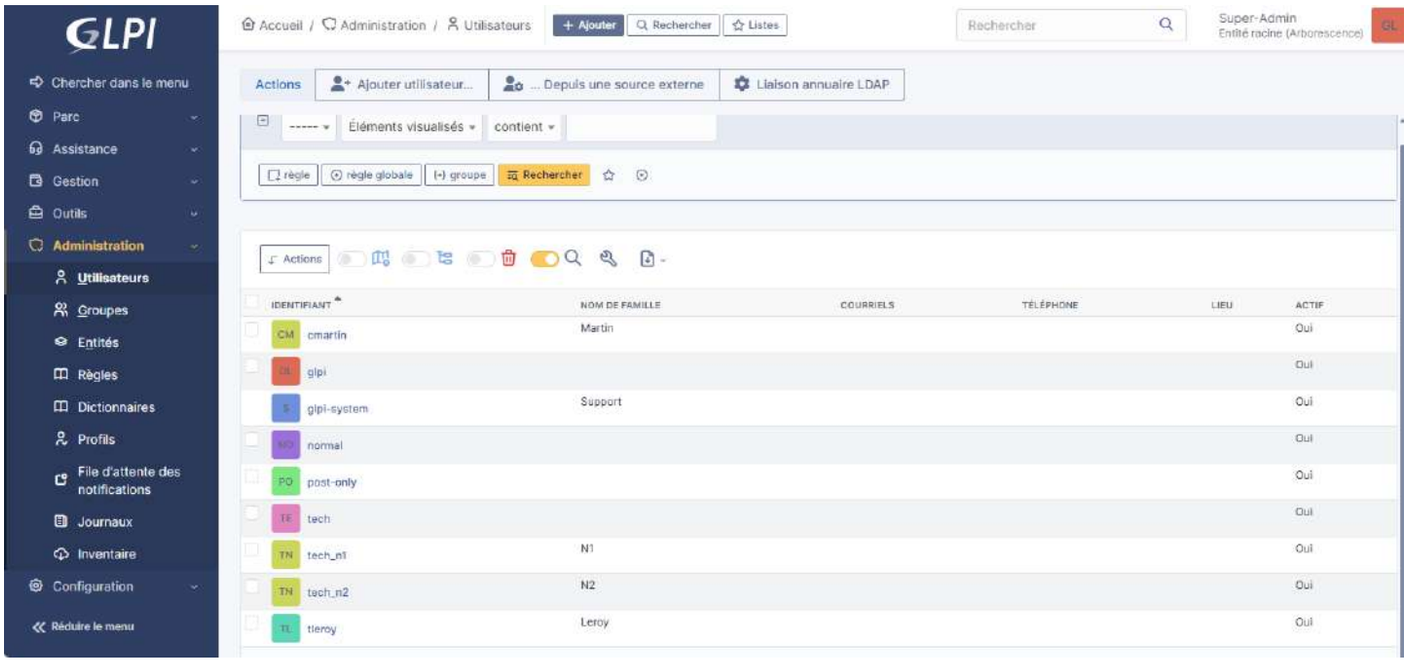
Le profil Super-Admin me permet :

- De configurer les règles métier
- De paramétrer les SLA
- De gérer les profils
- De modifier les paramètres globaux

Cette séparation des rôles permet de :

Respecter le principe de séparation des responsabilités
Simuler une organisation réaliste
Structurer un workflow N1 → N2
Contrôler les accès selon le rôle

Capture à insérer :
Liste des profils GLPI et comptes tech_n1 / tech_n2 visibles dans l'interface.



Catégories ITIL (Classification des incidents)

Afin d'organiser efficacement les tickets, j'ai structuré les catégories selon une logique ITIL.

Depuis Configuration → Intitulés → Catégories ITIL, j'ai créé une arborescence adaptée aux besoins d'une PME.

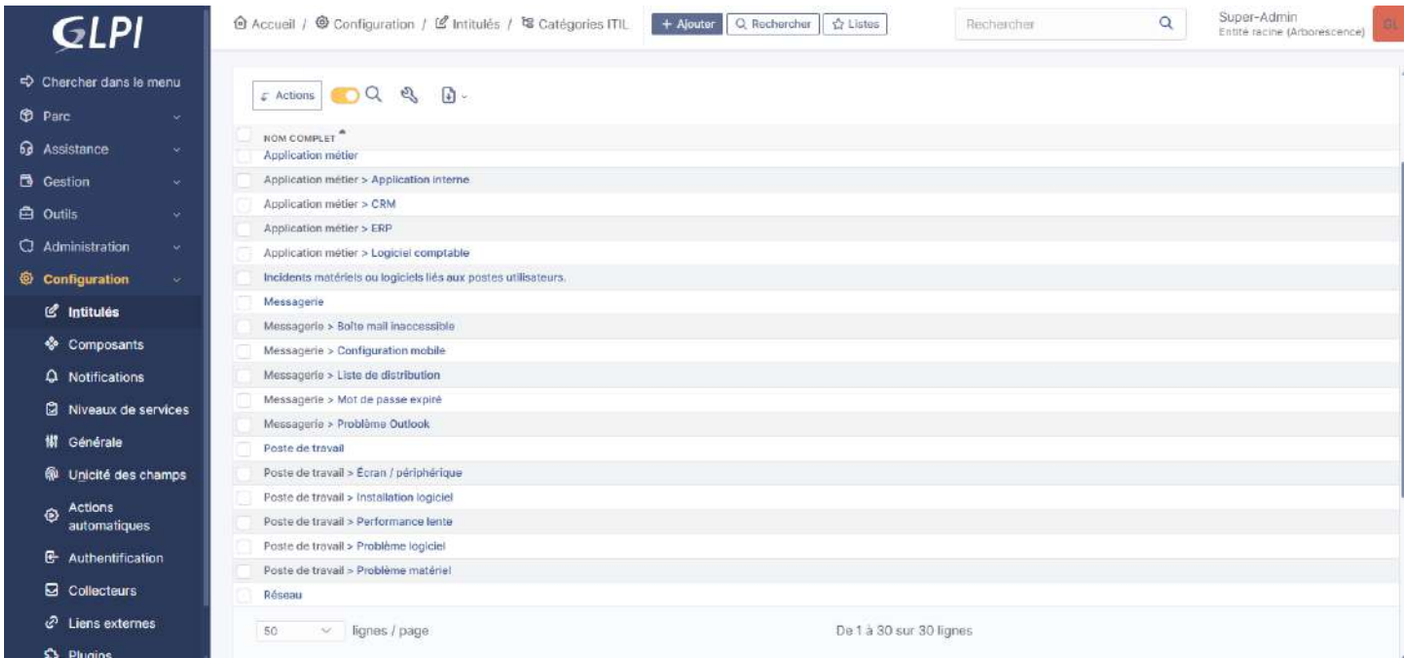
Catégories mises en place :

- Application métier
  - ERP
  - CRM
- Messagerie
  - Outlook
  - Boîte inaccessible
- Poste de travail
  - Installation logiciel
  - Performance lente
- Réseau
  - Perte de connexion
  - VPN
- Serveur
  - Service arrêté
  - Problème base de données

Cette classification permet :

- Une meilleure priorisation
- Une analyse statistique plus précise
- Une gestion des SLA adaptée au type d'incident
- Une meilleure traçabilité

Capture à insérer :
Liste des catégories ITIL avec sous-catégories visibles.



Compétences démontrées dans cette partie :

- Organisation d'un Service Desk
- Séparation des rôles ITIL
- Structuration des incidents
- Gestion des responsabilités
- Préparation à l'analyse statistique

Gestion du parc informatique (Inventaire / CMDB)

Dans le cadre de ce projet, j'ai configuré le module Parc de GLPI afin de simuler une gestion réaliste du matériel informatique d'une PME.

L'objectif était de mettre en place une mini-CMDB (Configuration Management Database) permettant de :

- Suivre les équipements
- Associer chaque matériel à un lieu
- Gérer le cycle de vie
- Faciliter l'analyse des incidents

Normalisation du nommage

Afin d'assurer une cohérence et une lisibilité du parc, j'ai défini une convention de nommage standardisée.

Postes utilisateurs

Format utilisé :

PC-NOM-01

Exemples :

- PC-CMARTIN-01
- PC-JPETIT-01

Cette convention permet d'identifier immédiatement :

- Le type d'équipement
- Le propriétaire
- Le numéro du poste

Serveurs

Format utilisé :

SRV-ROLE-01

Exemples :

- SRV-AD-01
- SRV-FIC-01
- SRV-BACKUP-01

Ce format permet d'identifier rapidement la fonction du serveur dans l'infrastructure.

Cette normalisation facilite :

La gestion des incidents
La documentation
L'analyse des impacts
La communication entre équipes

Données de gestion associées

Pour chaque équipement, j'ai renseigné des informations essentielles :

- Numéro d'inventaire
- Numéro de série
- Lieu d'affectation
- Système d'exploitation
- Commentaires techniques
- Statut dans le cycle de vie

Gestion du cycle de vie

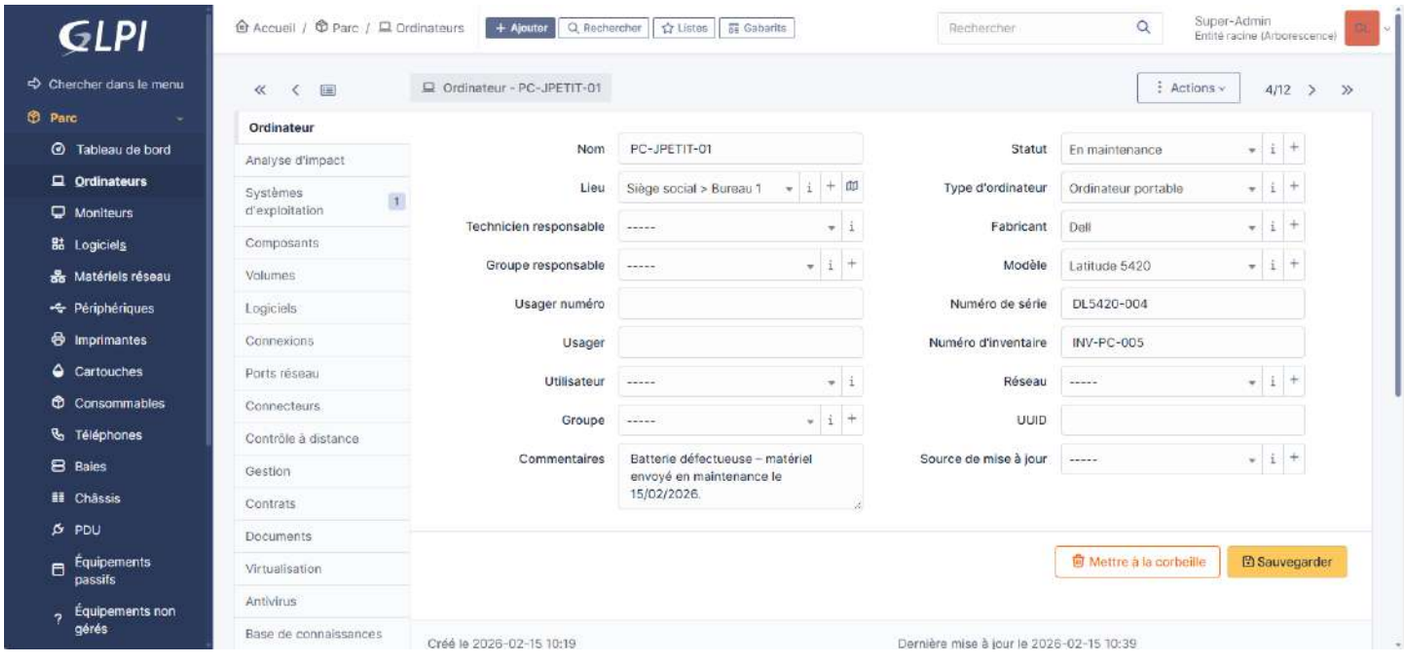
J’ai configuré différents statuts afin de simuler la gestion réelle du matériel :

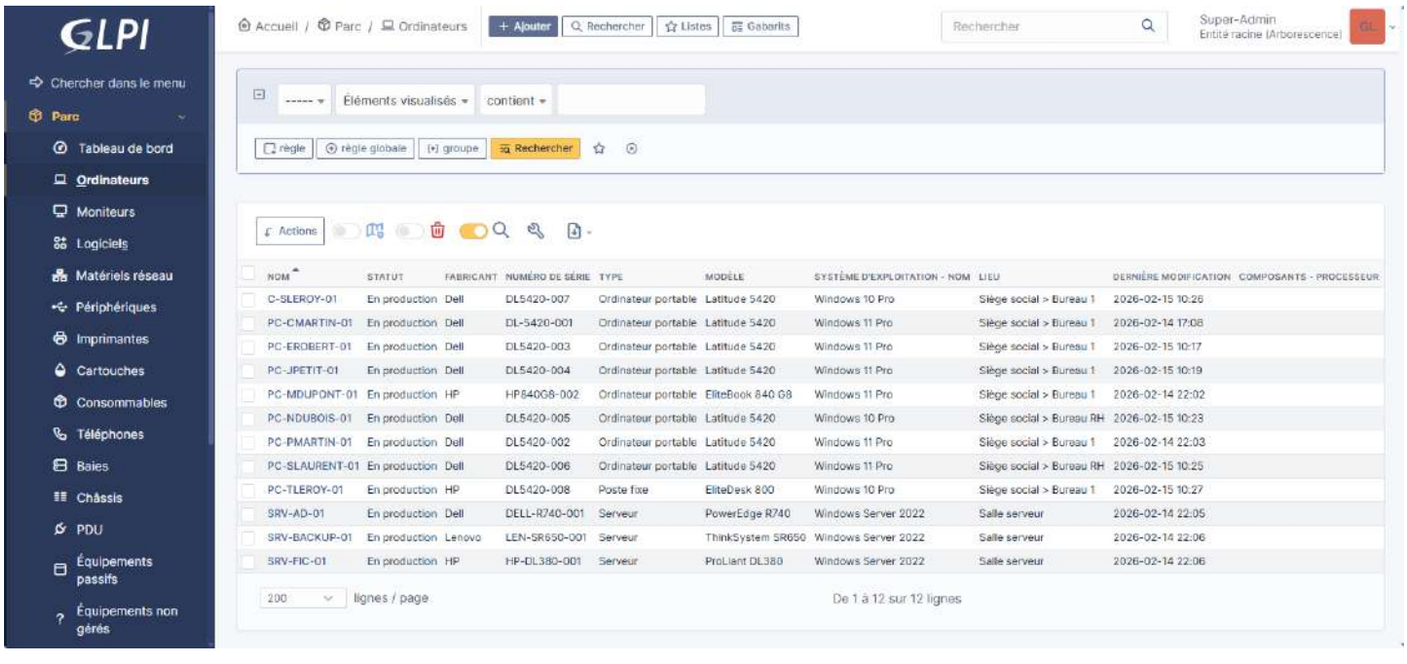
- En production
- En maintenance
- Hors service
- Réformé

Cette gestion permet :

- D’identifier les équipements indisponibles
- De suivre les interventions
- De préparer les renouvellements
- D’avoir une vision claire du parc actif

Captures à insérer **:**





Compétences démontrées dans cette partie :

- Gestion de parc informatique
- Mise en place d'une CMDB simplifiée
- Normalisation du nommage
- Suivi du cycle de vie matériel
- Structuration orientée ITIL

SLA et automatisation (ITIL)

Dans le cadre de la mise en œuvre des bonnes pratiques ITIL, j'ai configuré des SLA (Service Level Agreements) afin de définir des délais de résolution adaptés à la criticité des incidents.

L'objectif était de simuler un environnement professionnel où les engagements de service sont mesurés et suivis automatiquement.

Niveaux de service (SLA)

J'ai créé plusieurs niveaux de service correspondant aux priorités définies dans le système :

- Critique → 2 heures
- Haute → 4 heures
- Normale → 8 heures
- Basse → 24 heures

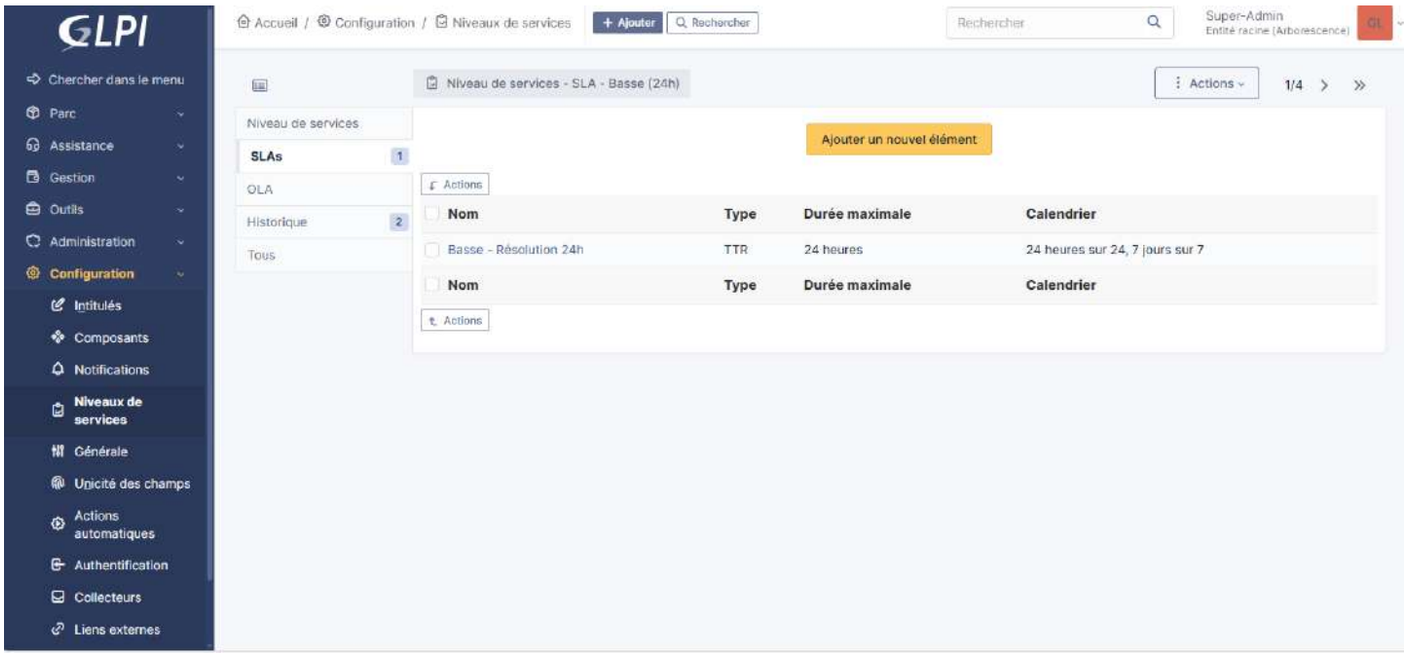
Chaque SLA a été configuré avec :

- Un temps de résolution (TTR – Time To Resolve)
- Un calendrier applicable
- Une activation automatique

Cette configuration permet :

De prioriser les incidents critiques
De garantir un temps d'intervention cohérent
De mesurer la performance du service
De simuler un engagement contractuel

Capture à insérer :
Liste des SLA configurés dans GLPI



Règles métier automatiques

Afin d'automatiser l'attribution des SLA, j'ai configuré des règles métier dans GLPI.

Ces règles permettent d'appliquer automatiquement un SLA en fonction de la priorité du ticket.

Exemple de logique mise en place :

- Si priorité = Critique → SLA Critique (2h)
- Si priorité = Haute → SLA Haute (4h)
- Si priorité = Normale → SLA Normale (8h)
- Si priorité = Basse → SLA Basse (24h)

Ces règles s'appliquent :

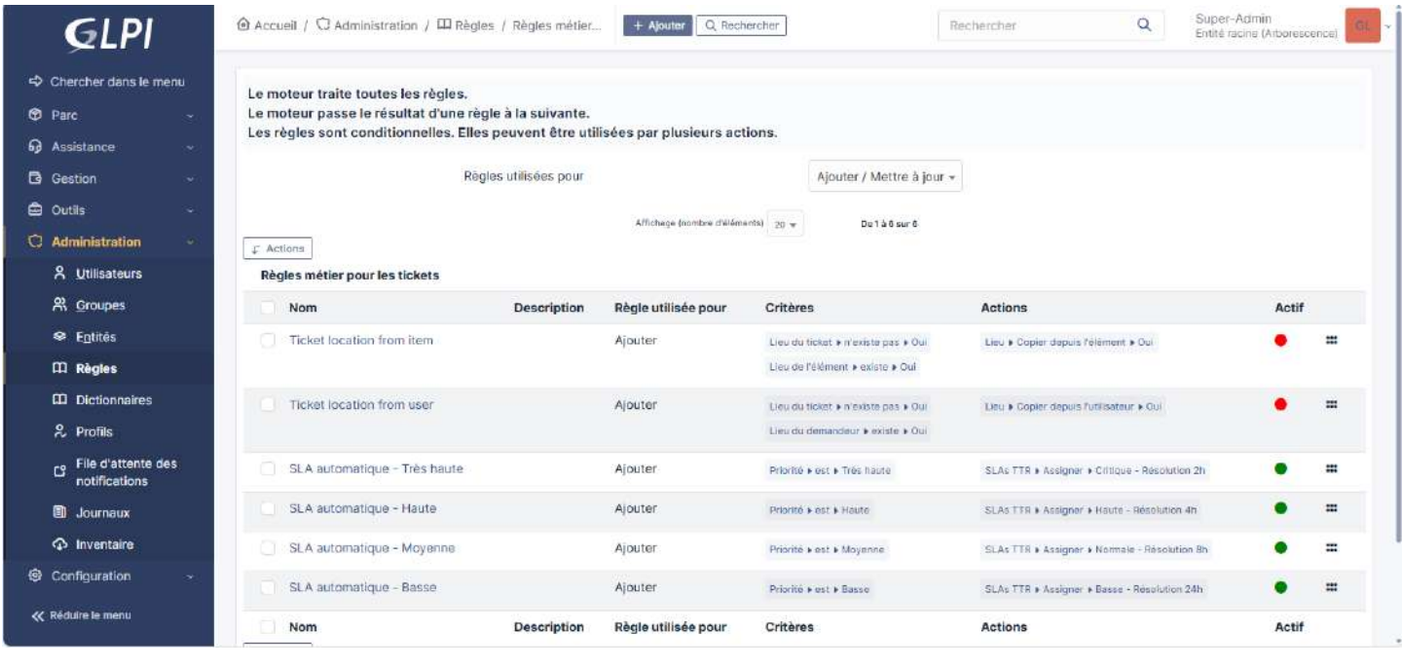
- À la création du ticket
- Lors de la modification de la priorité

Cette automatisation permet :

D'éviter les erreurs humaines
D'assurer une cohérence des délais
De respecter les engagements de service
De simuler un fonctionnement professionnel réel

Captures à insérer :

Liste des règles métier automatiques



(Optionnel) Vue détaillée d'une règle SLA automatique

Compétences démontrées dans cette partie :

- Mise en œuvre des principes ITIL
- Gestion des priorités
- Automatisation via moteur de règles
- Suivi des délais de résolution
- Structuration orientée performance

Base de connaissances

Dans le cadre de la structuration du centre de services IT, j'ai mis en place une base de connaissances afin de capitaliser les solutions techniques et améliorer la qualité du support.

L'objectif était de :

- Réduire le temps de résolution
- Standardiser les procédures
- Permettre l'auto-assistance des utilisateurs
- Faciliter le travail du support N1

Cette approche s'inscrit pleinement dans les bonnes pratiques ITIL, notamment dans la gestion des connaissances.

Création d'articles techniques

J’ai rédigé plusieurs articles couvrant des incidents courants rencontrés en entreprise :

- Réinitialisation mot de passe Active Directory
- Outlook ne se synchronise plus
- Installation imprimante réseau
- Problème de connexion VPN
- Accès au partage réseau \SRV-FIC-01\DATA

Chaque article contient :

- La description du problème
- Les causes possibles
- Les étapes de diagnostic
- La procédure de résolution
- Les vérifications finales

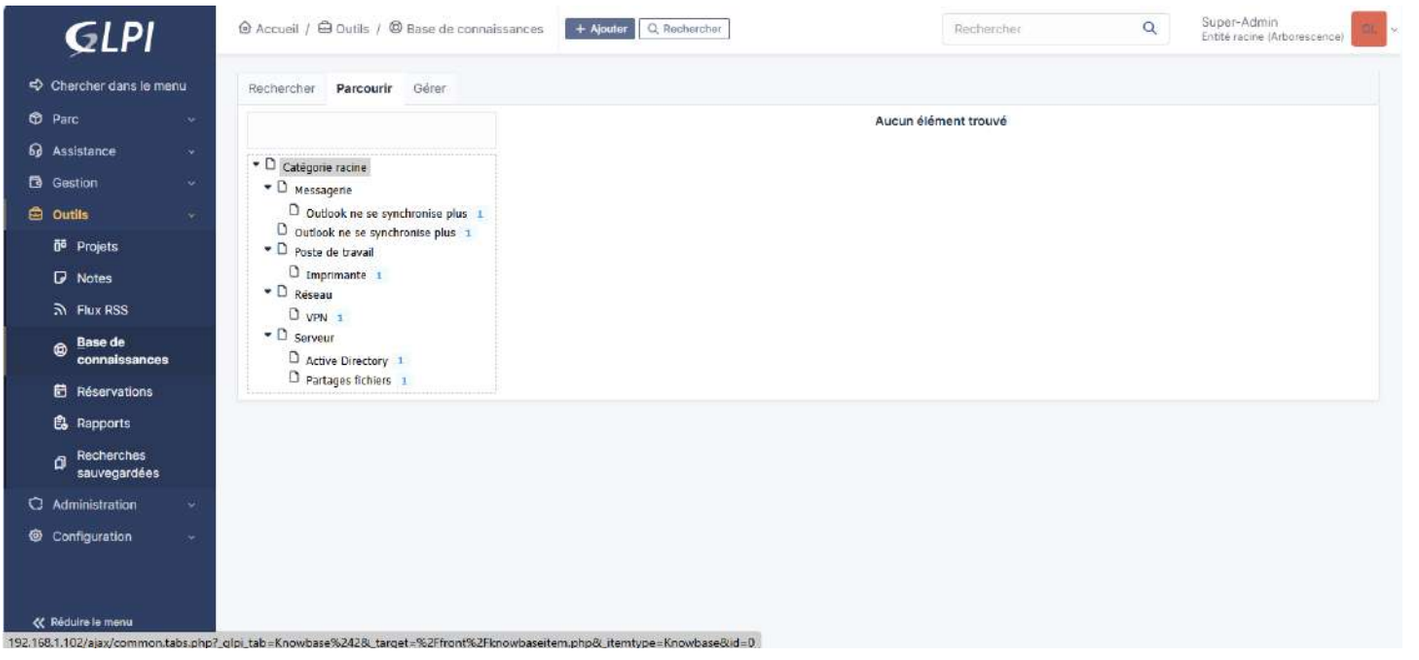
Objectif de la base de connaissances

Cette base me permet de :

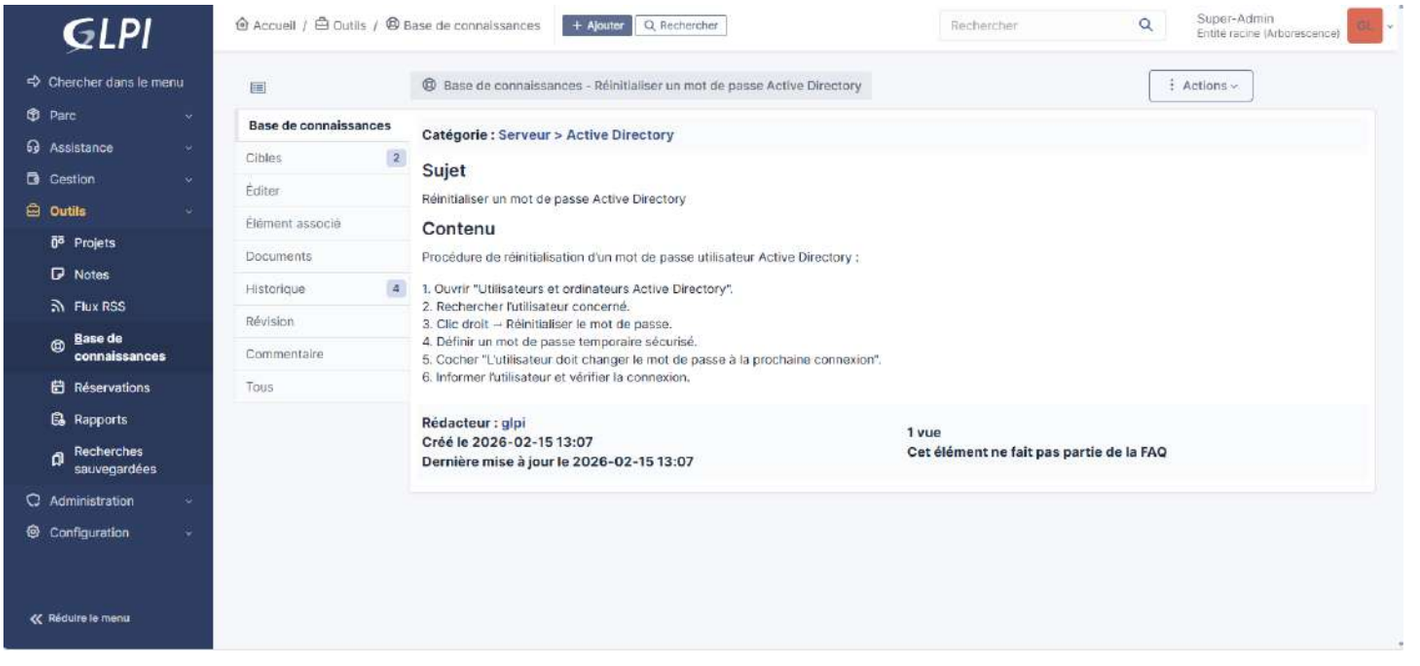
Structurer les réponses du support
Assurer une cohérence des interventions
Faciliter la formation des techniciens N1
Améliorer la réactivité
Préparer un environnement orienté amélioration continue

Captures à insérer :

Liste des articles de la base de connaissances



Exemple d'article détaillé (procédure technique)



Compétences démontrées dans cette partie :

- Documentation technique
- Structuration des procédures
- Amélioration continue
- Capitalisation des connaissances
- Application des bonnes pratiques ITIL

Simulation de tickets (Workflow complet)

Afin de valider le bon fonctionnement du centre de services IT, j'ai simulé plusieurs scénarios d'incidents représentatifs d'un environnement PME.

Ces simulations m'ont permis de tester :

- La création des tickets
- L'application automatique des SLA
- La gestion des priorités
- L'escalade N1 → N2
- La clôture documentée

Ticket N1 standard – Incident messagerie (Outlook)

Dans ce premier scénario, j'ai simulé un incident courant :

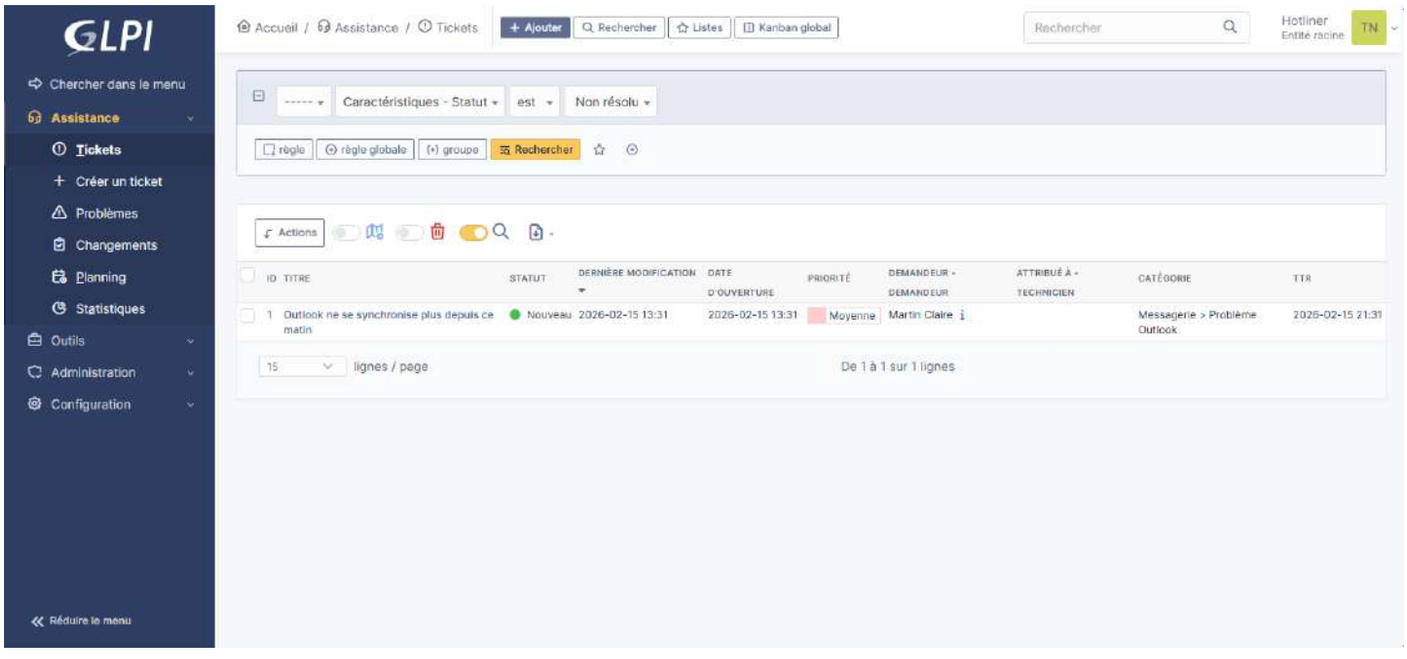
Problème : Outlook ne se synchronise plus.

Étapes réalisées :

1. Connexion avec un profil Self-Service
2. Création d'un ticket avec :
    - Catégorie : Messagerie → Outlook
    - Priorité : Normale
3. Affectation automatique au support N1
4. Diagnostic de premier niveau :
    - Vérification connectivité
    - Test redémarrage Outlook
    - Contrôle profil utilisateur
5. Résolution du problème
6. Clôture du ticket avec compte rendu détaillé

Cette simulation démontre le fonctionnement normal du support N1.

Capture à insérer :
Figure – Ticket N1 standard (historique complet visible)



Escalade N1 → N2 (Incident applicatif ERP)

Dans ce second scénario, j'ai simulé un incident plus complexe :

Problème : ERP inaccessible – erreur base de données.

Étapes réalisées :

1. Création du ticket par l'utilisateur
2. Prise en charge par le support N1
3. Tentative de reproduction
4. Identification d'un problème côté service applicatif
5. Commentaire N1 : "Escalade vers niveau 2"
6. Réassignation au technicien N2
7. Intervention N2 :
    - Vérification du serveur
    - Redémarrage du service concerné
    - Validation de l'accès utilisateur
8. Clôture avec rapport technique

Cette simulation démontre :

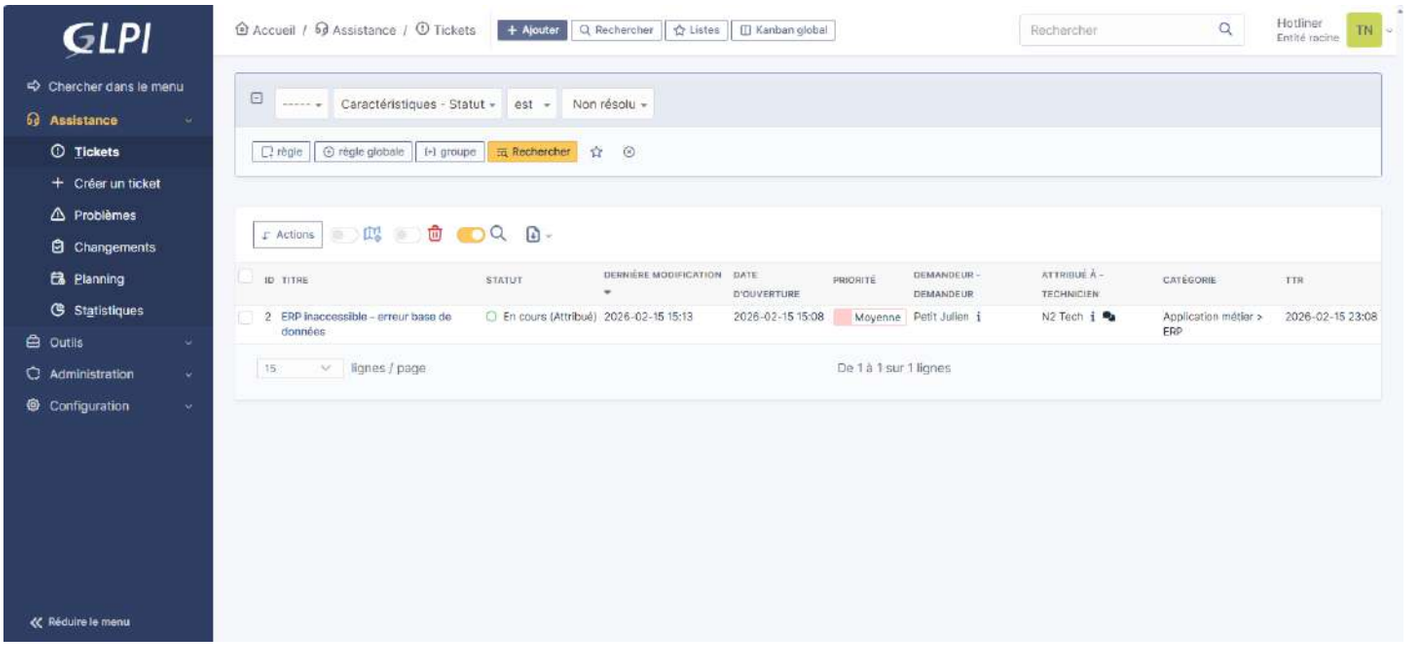
La séparation des rôles
Le processus d'escalade hiérarchique

La traçabilité complète des actions

Captures à insérer :

Ticket avec commentaire N1 “Escalade”

Intervention N2 + mention “Incident résolu”



Vue liste des tickets avec statut “Clos”

Ticket VIP – Priorité Haute

Dans ce troisième scénario, j’ai simulé un incident impactant un utilisateur prioritaire.

Problème : Outlook bloqué avant une réunion urgente.

Étapes réalisées :

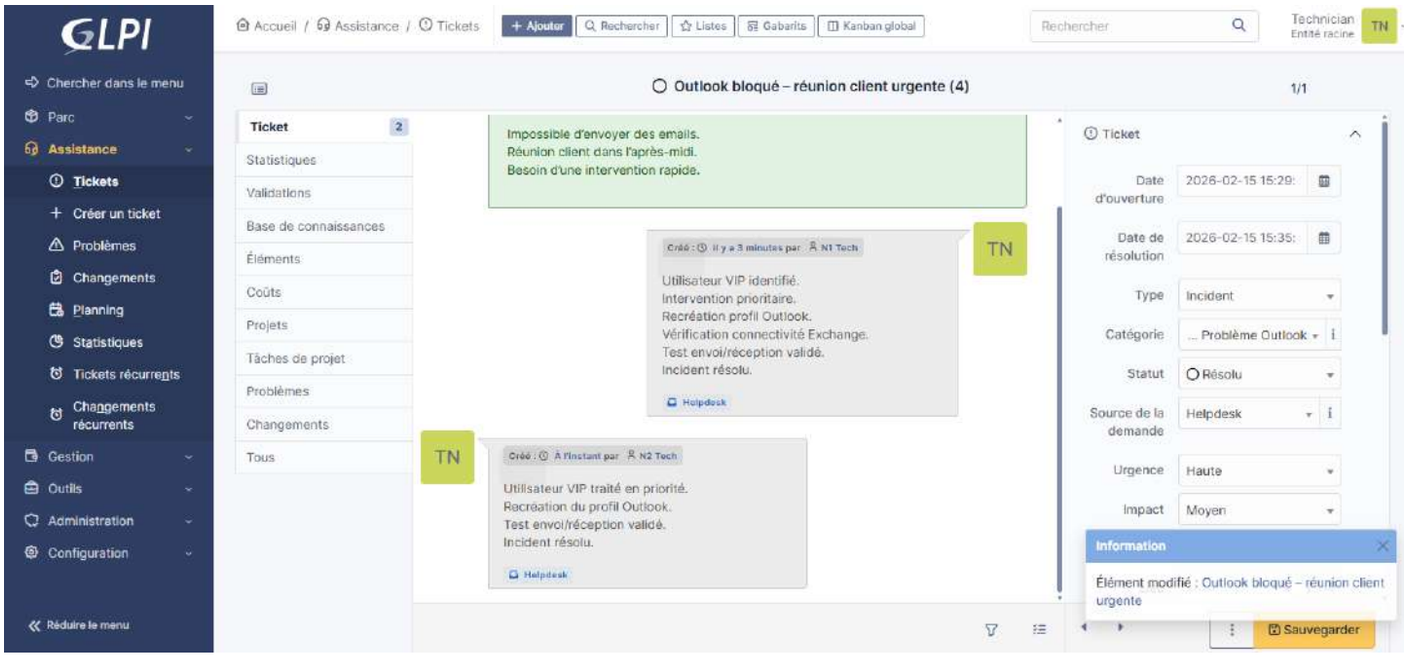
1. Création du ticket avec priorité Haute

2. Application automatique du SLA correspondant (4h)
3. Intervention prioritaire du support
4. Diagnostic :
    - Vérification profil Outlook
    - Test connectivité Exchange
    - Réparation du profil
5. Validation avec l'utilisateur
6. Clôture documentée

Cette simulation démontre :

La gestion des priorités
L'application automatique des SLA
La capacité à traiter un incident critique rapidement

Capture à insérer :
Figure – Ticket VIP résolu



Conclusion finale

À travers ce projet, j'ai conçu et simulé un centre de services IT complet, structuré selon les bonnes pratiques ITIL et basé sur une infrastructure Active Directory sécurisée intégrée à GLPI via LDAP.

J'ai reproduit un environnement PME réaliste incluant :

- Une gestion centralisée des identités
- Une organisation structurée N1 / N2
- Une automatisation des SLA
- Une classification ITIL des incidents

- Une gestion du cycle de vie du parc informatique
- Une base de connaissances technique documentée

Ce projet m'a permis de mettre en pratique :

- La sécurisation d'un domaine Active Directory
- L'intégration LDAP entre annuaire et outil ITSM
- La structuration d'un service desk professionnel
- L'automatisation via règles métier
- La gestion d'un workflow complet d'incident

Au-delà des aspects techniques, j'ai développé une approche orientée :

- Processus
- Traçabilité
- Performance
- Amélioration continue

Ce projet constitue une mise en situation concrète de mes compétences en administration systèmes et gestion des services IT, avec une vision globale et structurée du système d'information.

Glossaire technique

Active Directory (AD)

Service d'annuaire de Microsoft permettant de gérer les utilisateurs, groupes, ordinateurs et stratégies de sécurité au sein d'un domaine.

GLPI

Outil ITSM (IT Service Management) open source permettant la gestion des incidents, du parc informatique, des SLA et de la base de connaissances.

LDAP (Lightweight Directory Access Protocol)

Protocole permettant l'accès et l'interrogation d'un annuaire (comme Active Directory) pour l'authentification et la synchronisation des utilisateurs.

OU (Organizational Unit)

Unité d'organisation dans Active Directory permettant de structurer les objets (utilisateurs, groupes, ordinateurs).

GPO (Group Policy Object)

Stratégie de groupe permettant d'appliquer des règles de sécurité et de configuration aux utilisateurs et ordinateurs.

SLA (Service Level Agreement)

Engagement définissant un délai de résolution ou d'intervention pour un incident donné.

TTR (Time To Resolve)

Temps maximal autorisé pour résoudre un ticket selon le SLA appliqué.

Incident

Événement perturbant le fonctionnement normal d'un service informatique.

N1 (Support Niveau 1)

Premier niveau de support chargé du diagnostic initial et de la résolution des incidents courants.

N2 (Support Niveau 2)

Support technique avancé intervenant sur les incidents complexes ou nécessitant des actions serveur/applicatives.

Base de connaissances (Knowledge Base)

Référentiel documentaire regroupant des procédures et solutions techniques afin de standardiser les interventions.

CMDB (Configuration Management Database)

Base de données recensant les éléments du système d'information (serveurs, postes, équipements).

Escalade

Transfert d'un incident vers un niveau de support supérieur.

Compte de service

Compte technique utilisé par une application (ex : GLPI) pour interroger un annuaire ou un service.

Politique de mot de passe

Règles définissant la complexité, la durée et le verrouillage des mots de passe dans Active Directory.

VPN (Virtual Private Network)

Connexion sécurisée permettant l'accès distant au réseau de l'entreprise.