DOSSIER DE SPÉCIFICATIONS GÉNÉRALES ET TECHNIQUES

PROJET : INTRANET CORPORATE V1 (Déploiement, Centralisation & Sécurisation)

Date : 26 Décembre 2025

Version : 1.2 (Version Étendue)

Auteur : Expertise Technique & Développement

Destinataires : Direction Générale / DSI / Responsables de Service

1. CONTEXTE ET ENJEUX STRATÉGIQUES

L'entreprise opère actuellement avec des outils de gestion fragmentés, reposant sur un prototype autonome qui, bien que fonctionnel, atteint ses limites en termes de scalabilité et de sécurité. Ce projet vise à refondre l'écosystème numérique interne pour passer d'une logique d'outil isolé à une véritable plateforme ERP/ITSM d'entreprise.

1.1 Objectifs Détaillés

Centralisation et Décloisonnement ("Single Pane of Glass")

L'existant : Les demandes sont éparpillées (mails, téléphone, fichiers Excel, outil prototype).

La cible : Un portail unique fédérant l'ensemble des services supports (Informatique, DAF, Services Généraux, Technique, RH). Cela permet une traçabilité transverse : un manager doit pouvoir visualiser en un coup d'œil une demande d'achat (DAF) et une demande de PC (Info) pour un même collaborateur.

Sécurité et Gouvernance des Identités (IAM)

Suppression des comptes locaux propres à l'application.

Alignement sur la politique de sécurité : Authentification unifiée via l'Active Directory (AD). L'accès à l'intranet devient dépendant du statut du collaborateur dans l'entreprise (un départ = coupure d'accès immédiate).

Hiérarchisation et Workflows de Validation

Introduction d'une couche de contrôle managérial systémique. Aucune demande engageant des coûts ou des ressources matérielles ne doit parvenir aux services supports sans l'approbation explicite ("Visa") du responsable hiérarchique (N+1).

Expérience Utilisateur (UX) et Adoption

Réduire la friction d'utilisation grâce au SSO (Single Sign-On).

Notifications proactives pour éviter la relance téléphonique ("Où en est mon ticket ?").

Traitement ludique des erreurs (Page "Catdance") pour maintenir une image positive de la DSI même en cas de refus d'accès.

2. ARCHITECTURE TECHNIQUE CIBLE

Pour garantir la pérennité de la solution et sa capacité à encaisser la charge de l'ensemble des collaborateurs, l'infrastructure est mise à niveau vers des standards industriels.

2.1 Infrastructure Système & Réseau

- **Serveur Hôte :** Déploiement sur une Machine Virtuelle (VM) dédiée sous Debian 12 (Bookworm - Stable).
  - Justification : Stabilité éprouvée, cycle de vie long (LTS), et faible empreinte ressources.
- **Intégration Réseau :**
  - Le serveur disposera d'une IP fixe dans le VLAN serveur.
  - Enregistrement DNS interne (ex: intranet.corp.local) pour faciliter l'accès utilisateur.
  - Configuration du Pare-feu (UFW/IPTables) pour n'autoriser que les flux HTTP/HTTPS et SSH (Admin).

2.2 Socle Applicatif et Base de Données

- **Migration SGBD :** SQLite vers PostgreSQL.
  - Problématique SQLite : Basé sur un fichier unique, il ne gère pas efficacement les écritures simultanées (verrous bloquants) et manque de typage fort.
  - Avantage PostgreSQL : Supporte une forte concurrence (ACID compliant), gestion native des types complexes (JSONB pour les formulaires dynamiques futurs), et robustesse pour les données financières (DAF).
- **Pile Web :**
  - Nginx (Reverse Proxy) : Gère la terminaison SSL (HTTPS), sert les fichiers statiques (images, CSS, JS) avec haute performance, et protège le serveur applicatif.
  - Gunicorn : Serveur WSGI de production pour exécuter le code Python/Flask en multi-workers.

2.3 Protocole d'Authentification

- **LDAP (Lightweight Directory Access Protocol) :**
  - L'application agira comme un client LDAP vis-à-vis du Contrôleur de Domaine.
  - Mécanisme : "Bind" (vérification) des identifiants saisis par l'utilisateur contre l'AD. Aucune donnée de mot de passe ne transite ou n'est stockée dans la base de données de l'intranet.

3. GESTION DES DROITS (RBAC via ACTIVE DIRECTORY)

La gestion des droits est externalisée dans l'Active Directory. L'application ne fait que "lire" les appartenances aux groupes pour débloquer les fonctionnalités.

3.1 Groupes "Utilisateurs et Hiérarchie"

Nom du Groupe AD	Nom Fonctionnel	Description Détaillée et Implications
GRP_INTRA_ACCESS	"Utilisateur Standard"	Le Sésame. C'est le niveau zéro de l'accès. Tout collaborateur (CDI, CDD, Stagiaire) doit avoir ce groupe pour voir la page d'accueil. Sans ce groupe, l'utilisateur est redirigé vers la page de rejet.
GRP_INTRA_MANAGER	"Responsable / N+1"	Le Valideur. Ce groupe débloque le menu "Validation". Il permet à un responsable de voir les demandes émanant de son périmètre. Note : Un manager est aussi un utilisateur standard pour ses propres demandes.
GRP_INTRA_ADMIN	"Super-Admin"	La Tour de Contrôle. Accès aux logs techniques, à la configuration des workflows, et aux statistiques globales (KPIs). Ce groupe est restreint à l'équipe DSI Core.

3.2 Groupes "Résolution" (Back-Office Services)

Ces groupes définissent qui a le droit de traiter les tickets.

Nom du Groupe AD	Service	Périmètre Fonctionnel
GRP_SVC_INFO	DSI / Support	Gestion du parc, créations de comptes, maintenance préventive/curative.
GRP_SVC_DAF	DAF / Compta	Traitement des demandes d'achat, notes de frais, validation budgétaire.
GRP_SVC_TECH	Services Techniques	Maintenance bâtimentaire (CVC, Plomberie, Élec). Gestion des accès physiques.
GRP_SVC_GEN	Services Généraux	Approvisionnement consommables, logistique salles de réunion, flotte automobile.
GRP_SVC_ENLEV	Logistique Lourde	Gestion des bennes, enlèvements volumineux, réorganisation d'espaces.

4. MATRICE DE ROUTAGE ET FORMULAIRES INTELLIGENTS

L'objectif est de structurer la demande à la source. Fini les mails vagues "Ça ne marche pas". Chaque service dispose de formulaires dédiés.

A. Service Informatique (GRP_SVC_INFO)

- **Nouvel Utilisateur (Onboarding) :**
  - Champs critiques : Date d'arrivée (déclenche SLA), Profil métier (détermine les logiciels), Besoin matériel.
  - Automatisation visée : Génération automatique d'une checklist pour les techniciens.
- **Incident / Bug :**
  - Intelligence : Tentative de récupération automatique du Hostname de la machine via résolution DNS inverse.
  - Champs : Capture d'écran (Upload), Code erreur, Impact (Bloquant/Gênant).

B. Service DAF (GRP_SVC_DAF)

- **Demande d'Investissement (CAPEX) :**
  - Champs : Montant HT, Fournisseur, Centre de Coûts (Analytique), Devis PDF (Obligatoire).
  - Contrainte : Impossible de soumettre sans pièce jointe.

C. Service Technique (GRP_SVC_TECH)

- **Intervention Bâtiment :**
  - Champs : Localisation précise (Liste déroulante Bâtiment > Étage > Bureau), Type d'incident.
  - Priorisation : Champ "Urgence" (Sécurité des personnes vs Confort).

D. Services Généraux & Enlèvement (GRP_SVC_GEN / GRP_SVC_ENLEV)

- **Logistique :**
  - Champs : Volume (m3), Type de déchets (DIB, DEEE, Confidentiel), Contraintes horaires d'enlèvement.

5. WORKFLOW ET CYCLE DE VIE (STATE MACHINE)

La robustesse du processus repose sur un cycle de vie inaltérable des tickets.

01

Étape 1 : Initialisation & Routage Conditionnel

- L'utilisateur soumet le formulaire.
- Condition A (Utilisateur Lambda) : Le système détecte que l'utilisateur n'est pas dans le groupe Manager.
  - État : EN_VALIDATION.
  - Action : Notification email envoyée au N+1. Le ticket reste invisible pour le service support.
- Condition B (Manager) : Le demandeur est autonome.
  - État : EN_ATTENTE_PRISE_EN_CHARGE.
  - Action : Le ticket apparaît directement dans le backlog du service concerné.

02

Étape 2 : Le Sas de Validation (Manager)

Le Manager accède à son tableau de bord "À Valider".

- Option "Valider" : Appose un "Visa numérique". Le ticket est libéré vers le service compétent.
- Option "Refuser" : Le Manager doit saisir un motif de refus (obligatoire).
  - État : REFUSÉ.
  - Action : Notification au demandeur. Ticket archivé.

03

Étape 3 : Traitement Opérationnel (Service)

- Prise en compte ("Ack") : Un technicien s'assigne le ticket.
  - État : EN_COURS.
  - Action : Le demandeur voit qui traite sa demande ("Votre ticket est géré par Salim").
- Interaction : Utilisation du Chat contextuel. Chaque message déclenche une notification. L'historique est scellé (non modifiable) pour audit.
- Escalade/Transfert : Possibilité de transférer un ticket mal aiguillé (ex: DAF vers Info) sans perdre l'historique.

04

Étape 4 : Résolution & Clôture

- État : TERMINÉ.
- Le système enregistre la date de fin pour calcul des KPIs (Temps de résolution).

6. SPÉCIFICATIONS FONCTIONNELLES & UX (EXPERIENCE UTILISATEUR)

L'adoption de l'outil dépendra de sa facilité d'utilisation et de son aspect visuel.

6.1 Gestion des Accès Refusés (Feature "Catdance")

C'est une fonctionnalité clé pour la gestion du changement et la psychologie utilisateur.

- Scénario : Un utilisateur se connecte mais l'AD répond qu'il n'a pas le groupe GRP_INTRA_ACCESS.
- Réponse Système : HTTP 403 interceptée.
- Affichage : Redirection vers une page "Full-Page" épurée.
- Contenu : GIF animé humoristique (type "Catdance") pour dédramatiser.
- Call-to-Action : Message clair expliquant la démarche : "Oups ! Vous n'avez pas encore les droits. Merci de contacter votre manager pour demander l'accès via le groupe GRP_INTRA_ACCESS."

6. SPÉCIFICATIONS FONCTIONNELLES & UX (EXPERIENCE UTILISATEUR) (suite)

6.2 Identifiant Unique Incrémental (Ticket ID)

Format standardisé pour faciliter la communication orale ("Regarde le ticket 107").

- Format : YYYYMMDD-SEQ (ex: 20250524-107).
- Logique :
  - YYYYMMDD : Date du jour.
  - SEQ : Séquence réinitialisée à 001 chaque jour à minuit.
  - Cela permet de trier chronologiquement les dossiers, même en dehors de l'application (Excel exports).

6.3 Centre de Notifications

Pour éviter le "Polling" (rafraîchissement constant de la page par l'utilisateur), l'interface intègre un centre de notifs.

- Visuel : Cloche dans la Navbar avec badge numéroté (Rouge).
- Contenu : Liste déroulante des 5 dernières interactions.
- Triggers :
  - Validation d'un ticket par le manager.
  - Nouveau message du support.
  - Clôture du ticket.

7. LIVRABLES ET JALONS (PHASE 1)

Le projet sera considéré comme "Livré" une fois les éléments suivants validés :

Socle Infrastructure

Serveur Debian opérationnel, sécurisé, avec PostgreSQL et Nginx configurés.

Modèle de Données

Schéma relationnel (ERD) implémenté supportant les Users, Tickets, Messages, et Historiques de validation.

Application V1

- Module d'authentification LDAP fonctionnel.
- Routage dynamique des tickets selon les groupes AD.
- Interfaces distinctes : Demandeur, Manager, Solveur.

Documentation

- Procédure d'installation serveur (pour DRP).
- Guide utilisateur (PDF) pour l'onboarding.

8. ANNEXE : RAPPORT D'EXPERTISE & AUDIT DE L'EXISTANT (V0)

Cette section reprend l'analyse technique réalisée sur le prototype initial, justifiant les choix de la V1.

8.1 Analyse Architecturale & Backend

Le backend actuel (Flask/SQLAlchemy) est une excellente base. Cependant, pour passer à l'échelle :

- **Sécurité des Secrets :** La SECRET_KEY hardcodée est une vulnérabilité critique. Elle sera externalisée dans des variables d'environnement (.env) non versionnées.
- **Chat par Polling :** Le système actuel "bombarde" le serveur toutes les 5 secondes. Pour la V1, nous optimiserons les requêtes, mais une migration vers WebSockets (Socket.IO) est prévue en V2 pour le temps réel.
- **Migrations BDD :** L'absence d'outil de migration (Alembic) rend les mises à jour périlleuses. La V1 intégrera Flask-Migrate pour permettre d'ajouter des colonnes sans perte de données.

8.2 Analyse Frontend & UX

Le design (Tailwind CSS) est le point fort à conserver absolument.

- **Autonomie (Offline Mode) :** Actuellement dépendant de CDNs externes (unpkg.com), le front-end cassera en cas de coupure internet. La V1 internalisera toutes les librairies JS/CSS dans le dossier /static/.
- **Performance :** La recherche full-JS côté client sera remplacée par une recherche SQL côté serveur pour supporter des milliers de tickets sans ralentissement du navigateur.

8.3 Intégrité des Données

- **Soft Delete :** La suppression physique des données (DELETE SQL) est proscrite pour des raisons légales et d'audit. La V1 implémentera un système d'archivage logique (is_deleted = True), rendant les données invisibles mais récupérables.