



Spécifications techniques - Workflow

Objet du document
Spécifications techniques

Niveau de confidentialité du document			
0 – Public	1 – Interne	2 – Restreint	3 – Confidentiel
		X	

Fiche de révision			
Version	Date	Auteur	Nature
V0	13/09/2024	MJB, TCA, LSA, MAC	Définition des spécifications techniques

L'incrémentation de la version s'effectue :

- En version (0.x) pour les versions de travail, non diffusées à l'extérieur,
- En version majeure (1.0) pour les modifications fonctionnelles,
- En version mineure (x.1) pour les modifications de forme.

Sommaire :

Préambule	4
Dépendances	4
Exigences	4
Choix technologiques.....	4
Domaines/Hébergement	4
Environnement/Architecture	4
Exigences de programmation.....	5
1. Une matrice de droits :	5
2. Une console d'administration :	6
3. Un processus de validation :	6
4. Un rôle d'Administration globale du Workflow :	8
5. L'interface de l'application contiendra les éléments suivants, définis par le client :	8
Accessibilité.....	9
Sécurité	9
Maintenance/Évolutions	10
Références.....	10
Glossaire	10

Préambule

Le but premier de ce document est de préciser au plus détaillé possible l'ensemble des fonctionnalités à faire exister. La liste de ces fonctionnalités est tirée des documents de spécifications du besoin et fonctionnelles.

Dépendances

Ce projet nécessitant certaines fonctionnalités, des dépendances seront utilisées, telles que :

- Nous utiliserons Breeze pour gérer l'authentification sur le Framework Laravel.
 - Nous avons pu étudier cet outil et confirmer qu'il ne comporte aucun risque
 - Nous modifierons tant que besoin cette fonctionnalité afin de la faire parfaitement correspondre avec le projet.

Exigences

Choix technologiques

Nous utiliserons Laravel v8.83.27 avec PHP v8.2.24 pour propulser le serveur. Il sera hébergé sur une machine virtuelle sous Debian 12 (Linux), située sur un serveur ProxMox à l'Aigle.

Domaines/Hébergement

L'application web Workflow sécurisé sera hébergée par la société MTB111 sur un serveur PROXMOX dédié à notre application.

Environnement/Architecture

L'application web Workflow sécurisé doit être utilisable depuis n'importe quel appareil informatique ayant la possibilité d'utiliser un navigateur web.

A préciser que pour des questions logiques d'utilisation, seuls les utilisateurs préalablement autorisés par l'administration pourront créer un compte sur l'application (autorisation depuis la console d'administration et via l'adresse email à autoriser).

Concernant l'architecture choisie pour le projet, se référer au document de « Règles de code » (cf. Annexe)

Exigences de programmation

Afin de répondre à l'objectif fixé ainsi qu'aux exigences du client, l'application doit comprendre :

- Une matrice de droits
- Une console d'administration
- Un processus de validation
- Un rôle d'administration globale du Workflow
- Les exigences du client

1. Une matrice de droits :

- Comprenant une base générique.
 - Rôle « Collaborateur »
 - Peut créer des demandes
 - Peut créer des notes de frais
 - Peut créer des charges mensuelles
 - Peut consulter ses demandes
 - Peut créer une demande liée à un type de workflow customisé
 - Rôle « Direction »
 - Peut créer des équipes pour chaque workflow existant
 - Peut créer des projets pour chaque équipe
 - Peut générer les différents récapitulatifs (demande de congés, note de frais, etc...)
 - Rôle « SysAdmin »
 - Peut réaliser les mêmes actions qu'un membre « Direction »
 - Peut créer des rôles
 - Peut instancier un nouveau type de workflow

- Peut attribuer les rôles
- Modifiable à souhait par les utilisateurs administrateurs définis.
- Par défaut, dans le workflow de gestion des congés, tous les utilisateurs auront le rôle de «Collaborateur».
 - La modification de ce rôle se fera lors de la définition d'une équipe.
- Intégrant la possibilité de modifier la base générique :
 - Permettant d'adapter à sa guise la matrice de droits générique en fonction du workflow (gestion des congés, gestion des notes de frais, etc.).

2. Une console d'administration :

- Une console permettant d'administrer tous les workflows, cette console sera gérée par l'administration MTB111.
 - Cette console sera accessible si et seulement si l'utilisateur possède le rôle « SysAdmin ». Cette page sera sous forme de cases à cocher en fonction des permissions à attribuer aux rôles existants. Pour la création de rôle le principe sera le même avec une attribution supplémentaire concernant le nom du rôle. D'un point de vue plus technique, toutes les informations concernant les rôles seront stockées dans une table de la base de données. Pour les accès aux fonctionnalités nécessitant certaines permissions, le traitement sera directement fait dans le code.

3. Un processus de validation :

- Une base générique commune à toutes les fonctionnalités : demande de congé, note de frais, charges mensuelles.
- Quatre stades de validation :
 - 1. Collaborateur
 - 2. Chef de projet
 - 3. Directeur de projet
 - 4. Direction
- Selon le rôle de l'utilisateur défini dans une équipe, il sera intégré dans le processus de validation.
- Un processus de validation spécifique pour chaque équipe.
 - Les informations de ce processus pourront être modifiées par les utilisateurs définis. Les informations spécifiques à une équipe seront stockées en bdd et traitée visuellement dans le code.

- Des contrôles dans la validation :
 - Comparaison des jours de congés demandés avec les jours de congés acquis.
 - Comparaison réalisée via les informations stockées en base de données
 - Avertissement à l'utilisateur concernant le caractère légal de la demande (congés sans solde, congés anticipés, etc.).
 - Ce type de message sera affiché par la comparaison entre le nombre de congés acquis et demandés.
- Un processus de validation adaptable en fonction :
 - Du projet sélectionné.
 - Des disponibilités de chaque valideur.
 - Mise en place d'une solution permettant la continuité du processus si un valideur est temporairement indisponible.
 - Si un valideur est indisponible pour des vacances par exemple, sa validation est passée automatiquement.
- Champs du formulaire de demande obligatoires ou facultatifs selon le rôle de l'utilisateur.
 - Numéro de téléphone
 - Contexte client ou contrat (impact sur le projet dû à l'absence du personnel)
- Possibilité de retours sur une demande :
 - Via un champ spécifique aux personnels ayant été autorisés comme valideurs au sein de leur équipe :
 - Possibilité de compléter une demande d'informations en fonction du rôle.
 - Possibilité de questionner le demandeur ou le valideur précédent.
 - Possibilité de joindre une pièce jointe annexe lors du retour.
- Le processus doit être complet pour éviter au maximum les retours en arrière.
 - La validation peut se faire avec ou sans réserve par la direction.
 - La validation doit générer un récapitulatif.
 - A la fin du processus de traitement, un récapitulatif sera automatiquement envoyé au demandeur et à la direction par mail (sur l'adresse fournie dans l'application).

4. Un rôle d'Administration globale du Workflow :

- Un rôle « SysAdmin » permettant d'administrer l'ensemble du workflow.
- Création d'une console d'administration spécifique.
 - Création d'une console d'administration permettant aux utilisateurs « SysAdmin » d'administrer l'application, la création / l'attribution de rôles. L'autorisation de création de compte par adresse email.
- La création d'un nouveau type de workflow et son paramétrage.

5. L'interface de l'application contiendra les éléments suivants, définis par le client :

- L'application doit être responsive.
 - Pour ceci, appliquer un css permettant de rendre l'application utilisable sur n'importe quel support tout en respectant la charte graphique définie.
- Un écran dédié à chaque rôle.
 - En fonction du rôle de l'utilisateur, des fonctionnalités seront ou non visibles. Le traitement de ceci se fera via les rôles et permissions stockés en base de données et dans le backend.
- Une notion de statut pour le traitement de chaque demande :
 - Cette notion sera affichée sur la page d'accueil de l'application. Les informations visibles seront différentes en fonction des permissions de l'utilisateur au sein de son équipe.
 - Pour les demandes émises par l'utilisateur.
 - Pour les demandes à traiter (en fonction du rôle).
 - Pour le statut de la demande en cours :
 - Numéro d'identification de la demande.
 - Étape de validation (déposée / en cours de validation / acceptée ou refusée).
 - Les demandes, les annulations.
 - Nombre de jours de congés restants à l'utilisateur.
 - Petite synthèse sur les jours acquis, jours utilisés, jours demandés.
- Possibilité pour chaque utilisateur de revenir sur sa saisie (mode brouillon).
- Possibilité de saisir une prévision de congé à destination du chef de projet ou du directeur de projet (à titre purement informatif), sans que cela n'implique une validation. Ils peuvent alors reprendre et valider cette prévision pour une demande officielle.

- L'enregistrement en mode brouillon/informatif sera possible via un bouton présent au sein de la page de demande.

Accessibilité

Le système doit garantir une disponibilité continue, permettant aux utilisateurs d'accéder et de valider les congés à tout moment, en particulier pendant des périodes critiques comme la fin d'année ou les vacances d'été.

- Accès en continu à la plateforme, avec une disponibilité de 99,9%.
- Serveurs de production et environnements de préproduction répondants pour garantir la continuité du service.
- Notifications en cas d'indisponibilité ou de maintenance programmée pour informer les utilisateurs de tout problème ou mise à jour.
- Tous les employés y compris les handicapés visuels et moteurs doivent pouvoir utiliser l'application.

Sécurité

La sécurité est primordiale pour protéger les données sensibles des employés et éviter toute fuite ou tout accès non autorisé.

- Contrôles d'accès stricts basés sur les rôles et la matrice des droits, avec une authentification forte pour chaque utilisateur.
 - Mise en place de règles de vérification de mots de passe respectant les normes en vigueur.
- Audit des actions réalisées dans le système, notamment pour le processus de validation (historique des modifications et validations).
 - Ceci permettra d'identifier les potentiels risques et potentiels attaques réalisables.
- Protection contre les intrusions et surveillance active des activités suspectes dans le système.

- Ceci sera mis en place via les logs et des protections actives de cybersécurité. Ce processus sera dans le but notamment de minimiser les risques identifiés par l'audit.
- Conformité légale avec la réglementation en vigueur, comme le RGPD, pour la gestion des données personnelles.
- Pour des questions évidentes de suivi des activités d'un point de vue sécuritaire, des « logs » seront générés pour les actions effectuées par les utilisateurs.

Maintenance/Évolutions

L'application web **Workflow Sécurisé** doit respecter les différentes règles définies pour le projet. En suivant ces règles, nous aurons une application facile à faire évoluer et à maintenir. Une transparence totale sur le code produit, sa portée et son utilité permettra à un nouvel arrivant de comprendre et d'assimiler rapidement et facilement le projet ainsi que son développement.

Les demandes d'évolution reçues à ce stade sont reprises en annexe n°1 et feront l'objet de spécifications ultérieurement.

Références

Supports de spécifications :

Spécifications du besoin : Spécifications_besoins_Workflow_V0.1

Spécifications fonctionnelles : Specifications_fonctionnelles_Workflow_v1.0

Supports liés au projet :

Plan projet : Plan Projet WorkFlow

Organisation complète du projet : Organisation projet Workflow

Les règles de codes : Règle de code Workflow sécurisé

Tous ces documents vous sont fournis avec les documents livrables.

Glossaire

Workflow : C'est un processus qui se déroule en plusieurs étapes dans le but d'obtenir un résultat final, en fonction des valeurs d'entrée.

Matrice de droits : C'est un tableau ou un schéma qui définit et organise les droits d'accès des utilisateurs aux différentes fonctionnalités ou ressources du système. Elle permet de spécifier qui (utilisateurs, rôles, groupes) peut effectuer quelles actions (permissions) sur quels objets (ressources, modules).

Proxmox Virtual Environment (PVE): C'est une solution de virtualisation libre et Open Source (licence AGPLv3) qui permet le déploiement de système virtualisés avec Linux KVM ou sur des containers Linux LXC, le stockage défini par logiciel et des capacités de mise en réseau de mise en réseau, sur une seule plateforme.