Liste des fonctionnalités principales

Les utilisateurs

Dans ce document, on considère que les utilisateurs sont des personnes ayant un compte. Chaque compte à un rôle qui lui est attribué, à savoir :
- Employé : est le rôle donné de base à la création du compte
- Manager : est le rôle donné uniquement par le global manager à un employé
- Global manager : Il n'en n'existe qu'un, c'est un compte administrateur. Ce rôle est aussi reconnu comme manager.

Créer un compte employé

Une personne doit pouvoir créer un compte utilisateur à partir d'un « pseudonyme », d'un « e-mail » et d'un « mot de passe ».

API :
- Doit vérifier que les informations entrés soient valide
- Doit vérifier que le pseudonyme et l'e-mail ne sont pas déjà utilisé
- Doit enregistrer le nouveau compte avec le rôle employé

Frontend
- Doit afficher un lien vers la création de compte quand l'utilisateur n'est pas authentifié.

Promouvoir un employé en manager

Seul le « global manager » peut promouvoir un employeur en manager. Les autres rôles n'ont pas d'accès à cette fonctionnalité.

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur ait le rôle « global manager »
- Doit vérifier que l'utilisateur à rétrograder existe.

Frontend
- Doit afficher cette fonctionnalité uniquement aux global manager

Rétrogradé au rôle d'employé un manager

Seul le « global manager » peut rétrogradé un manager au rôle d'employé. Les autres rôles n'ont pas d'accès à cette fonctionnalité. Lorsqu'un manager est rétrogradé il quittent alors toutes les teams dont il fait parti.

API :

- Doit vérifier que l’utilisateur ait un token valide
- Doit vérifier que l’utilisateur ait le rôle « global manager »
- Doit vérifier que l’utilisateur à rétrograder existe.
- Doit retirer le manager de toutes les équipes dont il est membre.
- Doit changer le rôle du manager par « employé »

Frontend :
- Doit afficher cette fonctionnalité uniquement aux global manager

Les utilisateurs peuvent se « connecter » à leurs compte pour récupérer un JWT

Chaque utilisateurs peut se connecter à son grâce à son e-mail ou son pseudonyme avec le mot de passe correspondant.

API :
- Doit récupérer l’utilisateur s’il existe et vérifié que le hash du mot de passe est le même, que celui de l’utilisateur récupérer.
- Générer et Renvoyer un JWT à partir de l’email et le rôle de l’utilisateur.

Front :
- Doit afficher un formulaire de login si l’utilisateur n’est pas authentifié (donc quand il n’a pas de token).
- Envoyer la requête quand le formulaire est validé
- Récupérer le token si l’utilisateur est authentifié, sinon afficher une erreur.

Les utilisateurs peuvent changer leurs informations de compte

Chaque utilisateur peut vérifier et modifier les informations de son compte utilisateur en accédant à sa page de profil.

Les informations modifiable en même temps sont :
- le pseudonyme
- l’e-mail

API :
- Doit vérifier que l’utilisateur ait un token valide
- Doit vérifié que les informations de l’utilisateur à modifié soit celles de l’utilisateur courant.
- Doit vérifié la validité des données fourni par la requête. Le pseudonyme et l’e-mail doivent être unique. L’e-mail reçu doit avoir la forme d’une e-mail, ...
- Doit procédé à la sauvegarde des nouvelles informations.

Front :
- Doit afficher le formulaire de modification sur la page de profil, uniquement si l’utilisateur est authentifié et elle lui appartient.

Les utilisateur peuvent modifier leurs mot de passe

Chaque utilisateur peut modifier sont mot de passe depuis sa page de profil.

Pour modifier le mot de passe, il faut fournir :
- le mot de passe actuel
- le nouveau mot de passe

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifié que le mot de passe à modifié soit celui de l'utilisateur courant

Frontend :
- Avant d'appeler l'API, le Frontend doit vérifié que l'utilisateur tape deux fois le même nouveau mot de passe. Pour s'assurer que l'utilisateur se souviendra de son mot de passe et donc éviter qu'il utilise directement le lien associé à la fonctionnalité « mot de passe oublié »

Le Global Manager ou l'utilisateur courant peuvent supprimer un compte utilisateur

Le Global Manager peut supprimer le compte de n'importe quel utilisateur depuis sa page de profil ou depuis le dashboard du global manager qui liste tous les employés.
Chaque utilisateur peut supprimer son propre compte depuis sa page de profil.

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur ait le rôle « global manager » ou alors que le compte soit celui de l'utilisateur courant.
- Doit supprimer le compte, et les temps de travail associés.

Front :
- Doit afficher un moyen de supprimer un compte dans la page utilisateur, à l'utilisateur courant ou le global manager uniquement.
- Doit permettre de supprimer les utilisateurs depuis le dashboard du global manager.

Les utilisateurs peuvent déclarer leurs temps de travail

Les utilisateurs peuvent déclarer leurs temps de travail en fournissant une date et une heure de début et de fin.

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur pour qui crée le temps de travail est l'utilisateur courant.
- Doit vérifier que la date et l'heure de début soit antérieur à la date et l'heure de fin.

- Doit persister le temps de travail

Front :
- Doit implémenter un formulaire parementant l'ajout de temps de travail.
- Pour plus de simplicité au chargement du formulaire, on remplira la date avec celle du jour.

Les utilisateurs peuvent modifier leurs temps de travail déclarer

Les utilisateurs peuvent modifier leurs temps de travail déclarer en fournissant une nouvelle date et une nouvelle heure de début et de fin.

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur pour qui modifie le temps de travail est l'utilisateur courant.
- Doit vérifier que la date et l'heure de début soit antérieur à la date et l'heure de fin.
- Doit persister le temps de travail modifié.

Front :
- Doit implémenter un formulaire parementant l'ajout de temps de travail.
- Pour plus de simplicité au chargement du formulaire, on remplira la date avec celle du jour.

Les utilisateurs peuvent utiliser l'horloge pour déclarer automatiquement leurs temps de travail

Les utilisateurs doivent pouvoir utiliser un bouton activable et désactivable pour déclarer leurs temps de travail automatiquement sans entré de dates et d'heures.

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur pour qui active ou désactive l'horloge est l'utilisateur courant.
- Doit persister la date et l'heure de l'activation si l'horloge est activer, sinon doit persister un nouveau temps de travail avec comme début, la date et l'heure de l'activation, et comme fin, la date et l'heure de la désactivation. La date et l'heure est récupérer par le serveur.

Front :
- Doit implémenter un bouton activable et désactivable pour permettre d'activer ou désactiver l'horloge. Dans le cas où l'API ne répond pas ou renvoi une erreur, l'état du bouton reste le même.

Les utilisateurs peuvent voir leur dashboard (Front)

Les utilisateurs peuvent voir leur dashboard. Le dashboard de chaque utilisateur permet de :
- Voir son temps de travail sur le jour, la semaine, ou sur une période de temps donné.
- Voir un tableau de leurs temps de travail déclarés qui permet aussi de les modifier et les supprimer.

- Voir un bouton activable ou désactivable pour déclarer automatiquement les temps de travail.

Les managers et le global manager ont des sections supplémentaires dans le dashboard qui leurs permettent de voir un tableau pour gérer les équipes (ajouter, modifier, supprimer). En cliquant sur une équipe, on accède aussi à la gestion de l'équipe où les managers et le global manager peuvent :
- Voir un tableau avec les membres d'une équipes. Ce qui leur permet d'ajouter ou de supprimer des employés de l'équipe, ou simple d'ouvrir le dashboard d'un utilisateur.
- Un graphique pour voir le temps de travail moyen sur le jour, la semaine, ou sur une période de temps donné de tous les employés de l'équipe.

Le global manager à une section bien à lui, qui lui permet de voir un tableau avec tous les employés. Comme le tableau des membre d'une équipe, il permet de les ajouter ou les supprimer d'une équipe, de voir leur dashboard. Seuls changement, les fonctionnalités de promotions ou de rétrogradation sont disponible.

Les managers peuvent créer une équipes

Les managers peuvent créer plusieurs équipes. Dès qu'il créer une équipe, il en sont automatiquement membre.

Les champs modifiables sont :
- le nom
- la description

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur ait le rôle manager ou global managers
- Doit vérifier les informations donné en requête
- Doit persister l'équipe créer
- Doit ajouter le manager en tant que membre.

Front :
- Doit implémenter le formulaire de création d'une équipe.
- Doit rediriger sur la page d'administration de l'équipe

Les managers peuvent modifier une équipes

Les managers peuvent modifier une équipe.

Les champs modifiable sont :
- le nom
- la description

API :
- Doit vérifier que l'utilisateur ait un token valide
- Doit vérifier que l'utilisateur ait le rôle manager ou global managers

- Doit vérifier que l’utilisateur soit membre de l’équipe qu’il souhaite modifier.
- Doit vérifier les informations donné en requête
- Doit persister l’équipe modifié

Front :
- Doit implémenter le formulaire de modification d’une équipe.
- Doit rediriger sur la page d’administration de l’équipe

Les managers peuvent ajouter des employés à une équipes

Les managers peuvent ajouter des employés à leurs équipes par leur nom ou leur adresse. Si un employé est déjà dans une équipe alors il n’est pas éligible.

API :
- Doit vérifier que l’utilisateur ait un token valide
- Doit vérifier que l’utilisateur ait le rôle « manager » ou « global manager »
- Doit vérifier que l’utilisateur à ajouter existe et ait le rôle « employé »
- Doit vérifier que l’utilisateur n’est pas déjà dans une autre équipe
- Doit ajouter l’utilisateur dans l’équipe.

Front :
- Doit implémenter un moyen d’ajouter un utilisateur dans une team.
- Proposition : Implémenter une barre de recherche d’utilisateur par pseudonyme ou e-mail.

Les managers peuvent supprimer des employés d’une équipe

Les managers peuvent supprimer des employés de leurs équipes.

API :
- Doit vérifier que l’utilisateur ait un token valide
- Doit vérifier que l’utilisateur ait le rôle « manager » ou « global manager »
- Doit vérifier que l’utilisateur à supprimer existe et ait le rôle « employé »
- Doit supprimer l’utilisateur de l’équipe

Front :
- Doit implémenter un moyen de supprimer un membre d’une équipe.

Un global manager peut supprimer des employés ou des managers d’une équipe

Le global manager peut supprimer des managers de leurs équipes.

API :
- Doit vérifier que l’utilisateur ait un token valide

- Doit vérifier que l’utilisateur ait le rôle « global manager »
- Doit vérifier que l’utilisateur à supprimer existe et ait le rôle « employé » ou « manager »
- Doit supprimer l’utilisateur de l’équipe

Front :
- Doit implémenter un moyen de supprimer un membre d’une équipe.

Liste des fonctionnalités secondaires

Limiter la création de compte aux managers ou au global manager

Actuellement accessible à n'importe qui nous prévoyons dans le futur de limiter cette fonctionnalité aux managers ou au global manager en sécurisant la route et en mettant en place un système d'activation de compte.

La création d'un compte par un manager ou un global manager nécessite seulement une adresse e-mail. Le rôle attribué de base est le rôle « employé », cependant le global manager peut prédéfinir le rôle du futur utilisateur.

Une fois la création du compte validé, un code sera généré et envoyé à une personne via un e-mail, en lui demandant d'activer son compte avec l'aide du code.

Activation d'un compte utilisateur

Lors de l'activation d'un compte, l'utilisateur doit complété son profil avec un pseudonyme et un mot de passe. Un fois fait, l'utilisateur pourra désormais se connecter.

Gestion de rôles et de permissions

La gestion des rôles et des permissions sont actuellement statique. Ici nous envisageons de permettre aux entreprises de créer elles mêmes leurs propres hiérarchie avec les nom de rôles souhaiter, ainsi que les permissions.

API Key

Nous envisageons aussi dans le futur d'ajouter une gestion d'accès à l'API via une API Key qui permettrait aux organisation de développé leur propre code fonctionnalité par dessus les nôtres.