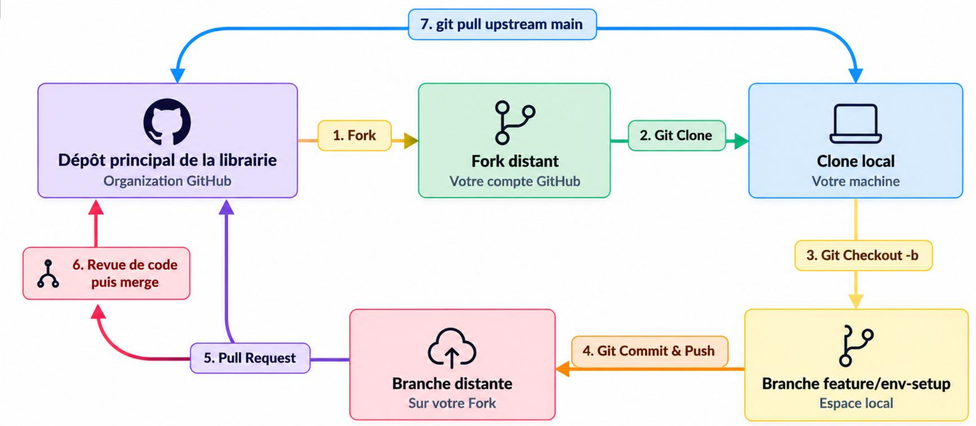
Fiche récap : Configurez votre environnement de développement

Développement

1. Récupérer le projet depuis GitHub et créer une branche de travail dédiée.
2. Installer les dépendances Node.js et auditer leurs vulnérabil avec npm.
3. Déployer PostgreSQL avec Docker Compose, assurer la persistance des données et préremplir la base avec init.sql.
4. Configurer VS Code, démarrer l'application et valider son fonctionnement local.
5. Diagnostiquer les dysfonctionnements à partir des logs et tester des correctifs ciblés.



Définitions

Git
Système de gestion de versions distribué qui conserve l'historique des modifications.

Fork
Copie personnelle d'un dépôt GitHub sur laquelle le développeur dispose de droits d' écriture.

Upstream
Dépôt officiel du projet, déclaré comme second dépôt distant pour récupérer le travail de l'équipe.

Pull Request
Proposition de modifications soumise à l'équipe pour revue avant intégration.

Image Docker
Modèle immuable contenant les éléments nécessaires à l'exécution d'une application.

Conteneur Docker
Instance isolée en cours d'exécution créée à partir d'une image.

Volume Docker
Espace de stockage persistant géré par Docker indépendamment du conteneur.

Docker Compose
Outil qui décrit et démarre les services du projet à partir du fichier déclaratif docker-compose.yml.

Bonnes pratiques

- ❏ Créer une branche dédiée pour chaque nouvelle fonctionnalité.
- ❏ Vérifier les fichiers modifiés avec git status avant chaque commit.
- ❏ Commiter package-lock.json pour garantir des dépendances identiques.
- ❏ Ajouter .env et node_modules/ au fichier .gitignore, et commiter .env.example.
- ❏ Analyser les vulnérabilités des dépendances avec npm audit.
- ❏ Utiliser un volume Docker nommé pour préserver les données PostgreSQL.
- ❏ Légender et dater chaque capture du dossier de recette technique.
- ❏ Tester une seule hypothèse à la fois lors du diagnostic d'une panne.

Erreurs classiques

- ➢ Travailler directement sur le dépôt source sans créer de fork.
- ➢ Utiliser git add . au risque de commiter un fichier sensible.
- ➢ Commiter le dossier node_modules dans le dépôt Git.
- ➢ Utiliser npm audit fix --force au risque de casser l'application.
- ➢ Publier le fichier .env contenant des secrets sur GitHub.
- ➢ Exécuter docker compose down -v lorsque les données doivent être conservées.
- ➢ Exécuter des commandes destructrices sans identifier la cause de la panne.
- ➢ Copier aveuglément une commande proposée par l'IA sans l'analyser.