

Tuteur interne : Paul Fush
Maîtres de stage : Théo Delgutte
Rémy Dufrenoy



16 août 2023

SHAW Eliot
Institut Mines Télécom Nord Europe
Fise 2025

Administration système et Intégration continue

Rapport de stage



IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille



merci amiral

Table des matières

Introduction	6
1.1 Introduction	7
1.2 Amiral Technologies, une startup prometteuse	7
1.2.1 Description de l'entreprise	7
1.2.2 Une entreprise dans un marché exigeant	7
1.2.3 Organisation interne	8
Travaux réalisés	10
2.0.1 La Culture de la Collaboration et de la Flexibilité	11
2.1 Administration système	11
2.1.1 Objectifs initiaux	11
2.1.2 Missions effectuées	12
2.1.3 Retour et critiques sur le projet	13
2.1.4 Modification des objectifs	14
2.1.5 Enseignements appris	15
2.2 Intégration continue	16
2.2.1 Technologies utilisées	16
2.2.2 Environnement de développement	17
2.2.3 Missions effectuées et problèmes rencontrés	17
Impressions personnelles	19
3.1 Ressenti lors du stage	20
3.1.1 Changement de maître de stage	20
3.1.2 Environnement et relations humaines	20
3.2 Zukunft	20
3.2.1 Environnement de travail visé	20
3.2.2 Orientation professionnelle	20
Conclusion	21
4.1 conclu mais mettre un titre genre : mon stage dans amiral technologies	22
Annexes et Bibliographie	23

abstract
mots cle

Introduction



1.1 Introduction

Au sein de l'entreprise Amiral Technologies, j'ai effectué mon stage d'une durée de 14 semaines au département de l'Administration Système Informatique. Cette startup française se spécialise dans la prédiction de pannes et se positionne comme un dérivé du CNRS. Fondée en 2018 par le Dr Mazen Alamir, directeur de recherche au CNRS, et le Dr Katia Hilal, directrice des opérations de l'entreprise, Amiral Technologies s'appuie sur plus de dix années de recherche académique en théorie du contrôle, automatique et en apprentissage automatique pour développer son logiciel phare, DiagFit.

jolie intro qui dit pk je suis entré à amiral et pk il y avait besoin du refacto

1.2 Amiral Technologies, une startup prometteuse

1.2.1 Description de l'entreprise

Amiral Technologies est une startup spécialisée dans le développement et la vente du logiciel de prédiction de pannes, Diagfit. Elle se dit être une dérivée (spin-off) du CNRS et participe activement à la recherche dans le domaine de la science des données (datascience)

Fondée en 2018, elle compte actuellement 22 employés et cible principalement trois secteurs d'activité : les transports (entreprises ferroviaires et aéronautiques), l'industrie manufacturière (dans le cadre de l'industrie 4.0) et le secteur de l'énergie et du nucléaire.

1.2.2 Une entreprise dans un marché exigeant

Les entreprises clientes

Reconnu pour la qualité du logiciel Diagfit, plusieurs clients de renom ont fait appel à l'expertise d'Amiral Technologies afin d'améliorer leur programme de maintenance de leurs équipements.

La startup s'oriente vers trois secteurs précis pour canaliser leur méthode de communication : le secteur des transports avec les entreprises ferroviaires et aéronautiques, le secteur manufacturier en aidant le développement d'une industrie 4.0 et le secteur de l'énergie et du nucléaire.

Todo ➤ mettre le nom des entreprises images ◀

Le logiciel Diagfit

Il permet aux équipements industriels de fonctionner sans défaut et sans pannes en anticipant les problèmes potentiels grâce à l'analyse de données de capteurs.

DiagFit utilise des modèles d'apprentissage automatique qui le rendent exploitable par une personne sans connaissance de la réalité physique des capteurs et sans connaissance dans la datascience. L'un des atouts majeurs de DiagFit est sa capacité à traiter une multitude d'équipements différents de manière polyvalente, ce qui le rend adaptable à diverses industries. Enfin, le logiciel utilise une méthode d'apprentissage est efficace avec seulement 3h de données de capteurs dans un mode de fonctionnement saint. Les pannes en industrie étant très coûteuses, ne pas avoir à en produire pour l'outil est essentiel pour vendre l'utilisation de Diagfit.

La détection de pannes permet d'entreprendre des maintenances prédictives en fonction des données spécifiques à l'appareil en question et non à une moyenne de la classe de ces appareils. Cette technologie permet alors de réduire les coûts de maintenance en les consacrant uniquement lorsqu'elles sont nécessaires.

1.2.3 Organisation interne

Une organisation en synergie pour l'innovation

L'entreprise est basée en Isère dans la ville de Grenoble et fait remarquer sa présence dans les salons spécialisés de Lyon et Paris.

Voici un aperçu des membres clés de l'administration :

- **Katia Hilal** : Présidente et co-fondatrice de l'entreprise, Katia apporte une expertise essentielle dans la vision stratégique de l'entreprise.
- **Mazen Alamir** : Co-fondateur d'Amiral Technologies et directeur de recherche au CNRS, Mazen est le créateur de l'algorithme derrière DiagFit.
- **Simon Gazikian** : Directeur général, Simon joue un rôle crucial dans le développement des partenariats et dans l'orientation globale d'Amiral Technologies.
- **Sebastien Le Gall** : En tant que directeur technique, Sebastien est responsable de la supervision et du développement de l'aspect technique du logiciel DiagFit et assure également une gestion efficace des opérations quotidiennes de l'entreprise.

Amiral Technologies est composé de différentes équipes en synergie pour pouvoir imaginer un algorithme, le développer en un logiciel et le vendre à de nombreux clients.

Description des groupes qui composent Amiral Technologies :

- **L'équipe commerciale** : Responsable de l'identification et de l'établissement de partenariats avec les entreprises clientes pour promouvoir et vendre DiagFit.
- **Les data-scientists** : Experts en analyse de données, ils utilisent DiagFit pour interpréter les informations collectées par les capteurs et améliorer les prédictions de pannes.
- **Les développeurs fonctionnel-utilisateurs (front-end)** Todo ➤ *renommer* ◀ : Chargés de concevoir et de développer l'interface utilisateur intuitive et conviviale de DiagFit.
- **Les développeurs techniques (back-end)** Todo ➤ *renommer* ◀ : Responsables de la conception et du développement des fonctionnalités principales de DiagFit, en garantissant une performance optimale et une intégration harmonieuse des données.
- **Les administrateurs système** : Gèrent les infrastructures et s'assurent que le logiciel DiagFit fonctionne de manière sécurisée et fiable.

Engagement envers la Responsabilité Sociétale des Entreprises

Amiral Technologies s'engage dans la Responsabilité Sociétale des Entreprises (RSE) en mettant en place des initiatives pour réduire son impact environnemental. Cependant, certains choix peuvent

être critiqués, notamment en ce qui concerne l'utilisation d'outils numériques de signature électronique qui génèrent une surcharge de stockage, ou l'investigation de l'empreinte carbone de l'entreprise sans exploitation des résultats. Malgré cela, l'entreprise continue de rechercher des solutions durables pour améliorer sa contribution à la RSE.

La RSE est devenue un sujet crucial dans le monde des affaires, reflétant l'intérêt croissant des entreprises à contribuer positivement à la société et à l'environnement. Dans la plupart des entreprises, les initiatives mises en œuvre pour répondre aux attentes en matière de RSE ont un fort accent sur le pilier écologique. Cependant, une approche globale de la RSE nécessite également de considérer les autres piliers du développement durable, à savoir le pilier social et économique. Des efforts peuvent être renforcés pour promouvoir le bien-être des employés, favoriser l'inclusion et l'équité dans le lieu de travail, ainsi que pour soutenir l'économie locale.

En tant que futur professionnel, il est essentiel d'être conscient de l'importance de la RSE et des trois piliers du développement durable. C'est en contribuant d'une manière volontaire et naturelle que les entreprises pourront jouer un rôle réel dans la société.

Travaux réalisés



2.0.1 La Culture de la Collaboration et de la Flexibilité

Méthode de Travail

Amiral Technologies opère selon une approche agile, organisée en cycles de travail appelés sprints, d'une durée de 4 à 6 semaines.

Chaque sprint est composé de plusieurs épics (grandes fonctionnalités) rassemblant des tâches liées à un même thème. À la clôture d'un sprint, une réunion de rétrospective est organisée pour obtenir des retours sur la période écoulée et évaluer les progrès des projets. De plus, une activité ludique ou un jeu de société est souvent intégré à la réunion, favorisant ainsi la détente et le renforcement de l'esprit d'équipe au sein du département de développement.

Des réunions trihebdomadaires sont également programmées pour créer des opportunités d'échanger sur les avancées immédiates et de discuter des éventuels obstacles rencontrés par les développeurs. Ces réunions régulières offrent un contexte propice à la résolution collaborative des problèmes et à la génération d'idées.

Environnement de Travail

Les locaux d'Amiral Technologies sont aménagés en un vaste open space comportant une vingtaine de bureaux, ainsi que deux salles de réunion.

Les heures de travail varient en fonction des préférences individuelles, avec un consensus autour d'une arrivée vers 9h30 et d'un départ entre 17h00 et 18h00.

Deux jours de télétravail sont accordés chaque semaine aux employés qui le souhaitent. Pour ma part, j'optais généralement pour le travail au bureau en effectif réduit.

2.1 Administration système

Le pôle administration système joue un rôle essentiel dans le maintien en condition opérationnelle des systèmes informatiques de l'entreprise. Il est responsable de la gestion des sauvegardes et de la récupération des données, assurant ainsi la disponibilité et l'intégrité des informations cruciales. De plus, il effectue également l'inventaire des équipements et des logiciels, ce qui permet de maintenir une visibilité précise sur les ressources technologiques de l'entreprise. Grâce à ces responsabilités, le pôle administration système contribue à assurer la continuité des activités, la sécurité des données et la performance des systèmes, ce qui est essentiel pour la productivité et la réussite globale de l'organisation.

Le pôle d'administrateurs système est composé d'une seule personne, Delgutte Théo. J'ai eu l'occasion de l'assister dans sa mission continue de maintien en condition opérationnelle de la partie informatique de l'entreprise.

2.1.1 Objectifs initiaux

Réduction des risques

L'objectif de mon stage était d'atténuer les divers risques potentiels liés à la cyberattaque et à la perte de données.

Ci-dessous une liste des risques identifiés en amont de mon stage :

- **Vulnérabilités Systèmes**
- **Attaques par Hameçonnage**
- **Perte de Données**
- **Accès Non Autorisés**
- **Malwares et Logiciels Malveillants**
- **Défaillance Matérielle**
- **Fuites d'Informations**

Attraction des clients

De plus, certains clients travaillant avec des données sensibles et des secrets industriels ont manifesté leur intérêt pour l'utilisation du logiciel DiagFit. Toutefois, ils ont émis une condition spécifique : l'obtention de la certification ISO 27001. Cette exigence aurait pu constituer un élément différenciateur et potentiellement plus vendeur pour le logiciel, renforçant ainsi son attrait auprès de clients soucieux de la sécurité de leurs données.

2.1.2 Missions effectuées

Dans le cadre de mon rôle au sein d'Amiral Technologies, j'ai entrepris diverses missions visant à améliorer la fonctionnalité, la stabilité et la gestion globale de notre environnement informatique.

Gestion de l'infrastructure et de l'inventaire

J'ai contribué à l'amélioration de notre infrastructure informatique en mettant en place des actions ciblées pour optimiser son fonctionnement. Cela incluait notamment la résolution d'un problème lié à notre serveur web qui restreignait les modifications par les collaborateurs. Pour résoudre ce problème, j'ai configuré un serveur de développement dédié, permettant de tester les changements avant leur application sur le site en production. J'ai également migré les URL en adaptant la base de données du site via des requêtes SQL.

En parallèle, j'ai supervisé l'inventaire matériel et utilisateurs pour une meilleure gestion des ressources et des droits d'accès. J'ai veillé à ce que les droits d'accès des utilisateurs soient en conformité avec les politiques de sécurité et proposé la conception d'une base de données d'inventaire pour centraliser et suivre les attributions aux utilisateurs.

Enfin, j'ai travaillé sur l'optimisation du schéma réseau en identifiant et en documentant minutieusement les adresses IP associées à chaque machine et service de l'entreprise.

Approche de la Cybersécurité au Quotidien

La sécurité informatique étant une priorité chez Amiral Technologies, j'ai contribué à mettre en place une approche pratique pour garantir la protection de nos systèmes et données. Pour cela, nous avons initié plusieurs axes d'action.

En premier lieu, j'ai participé à la collecte et à la synthèse de documents clés en lien avec la norme ISO27001, ce qui nous a permis d'acquérir une solide compréhension des meilleures pratiques en matière de sécurité.

J'ai également eu l'opportunité de participer à une conférence de la Direction du Renseignement et de la Sécurité de la Défense (DRSD), qui m'a apporté des perspectives concrètes sur les enjeux de cybersécurité et d'espionnage industriel international.

Un aspect clé de notre approche a été l'intégration de l'outil Sophos Zero Trust Network Access (ZTNA), qui répond à nos besoins croissants de protection des données et systèmes. J'ai ensuite organisé une présentation approfondie de l'outil Sophos ZTNA pour assurer sa compréhension et son utilisation par tous les collaborateurs.

Parallèlement, nous avons renforcé notre surveillance en mettant en place Wazuh. Cette solution nous a permis d'améliorer la détection des menaces en centralisant la surveillance via un serveur Wazuh Manager et un Wazuh Indexer. L'installation automatisée des agents Wazuh sur les ordinateurs a assuré une surveillance constante et réactive.

Enfin, pour faciliter la gestion et le partage de connaissances, nous avons créé une documentation interne à l'aide de Docusaurus. Cette plateforme, hébergée sur un PC réhabilité sous Ubuntu, a été organisée en deux parties : une pour les employés et une pour les administrateurs système, couvrant divers scénarios et procédures liées à notre environnement informatique.

Cette approche holistique de la cybersécurité a permis de renforcer notre positionnement tout en garantissant la stabilité et la performance de notre environnement informatique.

2.1.3 Retour et critiques sur le projet

Après environ un mois et demi de mise en place du projet, nous avons organisé une réunion rétrospective pour évaluer son utilité et son impact. Il est apparu que malgré nos efforts, le projet a entraîné certaines difficultés pour de nombreux collègues lors de sa mise en œuvre.

Effets contradictoires sur la sécurité

Les mesures mises en place n'ont pas toujours contribué de manière significative à la réduction des risques, et dans certains cas, elles ont même posé de nouvelles contraintes aux collaborateurs. Par exemple, l'utilisation d'outils complexes a parfois créé une dépendance envers une seule personne, en l'occurrence l'administrateur système Théo Delgutte. Cette situation est devenue problématique lors de ses périodes de congés, entraînant des retards et des perturbations dans les opérations.

Perte de stabilité

Un autre défi que nous avons rencontré concerne la stabilité des outils utilisés par les collaborateurs de l'entreprise. Les modifications apportées en cours de route par le sysadmin ont souvent impacté les ressources et les services, générant ainsi une instabilité préjudiciable au bon fonctionnement quotidien. Cette instabilité a été particulièrement préoccupante pour les employés travaillant à distance, car elle a rendu difficile voire impossible le travail en télétravail sans préavis.

Perte de l'autonomie

La décision de limiter les accès aux ressources a également eu des répercussions négatives sur le fonctionnement général de l'entreprise. Étant donné que le développement de différentes parties du projet est interconnecté et que la documentation d'une partie peut être utile à un autre groupe de personnes, la limitation des accès a entravé la fluidité de la collaboration. De plus, en tant qu'entreprise de petite taille, les contraintes imposées par cette limitation d'accès semblaient disproportionnées par rapport à d'autres risques potentiellement plus importants.

2.1.4 Modification des objectifs

Cette section aborde les ajustements apportés aux objectifs initiaux, visant à résoudre les problèmes identifiés et à reprendre les points bloquants du projet en main.

Éducation à la cybersécurité

Au cœur de la cybersécurité réside une composante essentielle : l'éducation des employés pour réduire les risques potentiels. Dans cette optique, j'ai joué un rôle clé en sensibilisant l'entreprise à l'importance de la cybersécurité grâce à des présentations hebdomadaires. Ces sessions ont couvert une variété de sujets visant à renforcer la vigilance et les bonnes pratiques parmi les collaborateurs.

Parmi les thèmes abordés, nous avons offert un guide complet sur l'hygiène de la cybersécurité. Cela comprenait des conseils pratiques pour naviguer en toute sécurité en ligne, en mettant l'accent sur la prudence face au public, la reconnaissance des extensions de fichiers, la détection d'URL malveillantes et l'utilisation de bloqueurs de traqueurs pour contrôler les publicités et les cookies.

Une attention particulière a été portée sur l'utilisation de gestionnaires de mots de passe pour renforcer la sécurité des comptes en ligne. Nous avons également abordé les risques liés aux emails malveillants, aux spams et au phishing, en fournissant des méthodes pour les identifier et les éviter.

Un volet notable de mon travail a consisté à explorer et utiliser l'outil Gophish pour la création d'une campagne de sensibilisation interne sur le phishing. J'ai récupéré le code source de sites officiels de microsoft et Gitlab ainsi que d'emails officiels des mêmes groupes dans le but de montrer comment des attaquants pourraient collecter des informations sensibles. Par la suite, j'ai conçu un message contenant un lien malicieux pour simuler une campagne de phishing. Une présentation détaillée a ensuite été faite, mettant en lumière des exemples de personnes ayant été trompées par de telles attaques.

Mise en place d'une infrastructure alternative

Les outils trop complexes à maintenir en condition opérationnel pour leur coût humain ont été retirés : les agents Wazuh et Sophos ZTNA ont donc été désinstallés pour cette raison.

Un membre de l'entreprise - Rémy Dufrenoy - a également pris de son temps de travail pour créer sur une nouvelle infrastructure, plus simple pour pouvoir bénéficier d'environnements de travail stables sur lesquels lui et ses collègues pourront travailler.

Modification des droits et autorisations

Les employés d'Amiral Technologies ont également bénéficié de plus de droits d'accès aux ressources générées par leurs collègues permettant une efficacité de travail plus grande.

En parallèle, un groupe de responsables de l'administration du système fut mis en place pour limiter la création d'un point unique de dépendances. Une base de données sécurisée de mot de passe contenant les identifiants administrateur pour les ressources fut également créé et partagé entre les responsables.

2.1.5 Enseignements appris

Dans la section qui suit, je partagerai les enseignements que j'ai acquis au cours de cette expérience.

Prise de Décisions Éclairées

Lors de la genèse du projet visant à renforcer la sécurité de l'entreprise, les décisions initiales ont été influencées par des parties prenantes qui manquaient de connaissances approfondies concernant les complexités liées à la réalisation des objectifs. Ces choix ont été largement motivés par la pression des clients, avec la présidente de l'entreprise prenant la décision finale. Un constat majeur qui émerge est l'importance de consulter des représentants de l'entreprise possédant une perspective éclairée et une compréhension approfondie des enjeux. Une telle approche permettrait de mieux évaluer la faisabilité et la pertinence des tâches envisagées.

Une composante essentielle de ce processus est la capacité à identifier les risques majeurs inhérents à chaque décision. Cette identification proactive est cruciale pour hiérarchiser et mettre en œuvre des mesures ayant un impact significatif sur la réduction des risques et la réussite globale du projet.

Communication Essentielle

Lorsque des problèmes ont conduit à des retours en arrière, l'absence de communication adéquate a souvent été à l'origine de ces situations. Par exemple, lors de la mise en place de nouvelles restrictions d'accès, les utilisateurs n'ont pas été prévenus des changements à venir. Cela a provoqué des frustrations et des interruptions dans leur travail quotidien.

Convaincre plutôt qu'imposer est essentiel pour éviter de mécontenter les utilisateurs des services concernés. Par exemple, au lieu d'imposer des nouvelles politiques de sécurité, il serait préférable de présenter les raisons derrière ces changements et d'offrir des solutions alternatives pour minimiser les perturbations.

L'importance de l'aspect humain, même dans le domaine de l'administration système, est devenue évidente. Par exemple, lorsque le système d'exploitation d'un ordinateur ne fonctionnait plus en raison d'un problème matériel, expliquer aux utilisateurs la nature du problème et les étapes prises pour le résoudre.

L'isopérimétrie dans le monde de l'entreprise

Dans le contexte professionnel actuel, équilibrer l'efficacité au travail et la cybersécurité est crucial. Les entreprises font face à des menaces de cybersécurité de plus en plus sophistiquées, nécessitant une

protection robuste. Les attaques informatiques évoluent constamment, rendant difficile la prévention de chaque menace potentielle.

Les administrateurs système jouent un rôle central dans cet équilibre. Responsables de la sécurité et de la performance des systèmes, ils doivent concevoir des environnements sûrs tout en facilitant la productivité. Le défi réside dans la recherche du bon équilibre entre des mesures de sécurité strictes et des opérations fluides.

Cela exige des solutions astucieuses de la part des administrateurs système. L'objectif ultime étant de créer un environnement où la sécurité est maximisée tout préservant la capacité à livrer de la valeur.

2.2 Intégration continue

2.2.1 Technologies utilisées

Intégration Continue (CI) avec GitLab

L'intégration continue (CI) est une pratique de développement logiciel visant à automatiser et à faciliter le processus de construction et de test d'une application.

La construction et le test de Diagfit se fait sur la plate-forme de gestion de développement GitLab avec une série de tâches automatisées, appelées "jobs", qui sont exécutées séquentiellement en réponse aux changements du code source.

Docker

Docker est une plate-forme de conteneurisation légère qui permet de créer, gérer et exécuter des applications dans des conteneurs. Les conteneurs Docker encapsulent le code, les bibliothèques et les dépendances d'une application, garantissant une exécution cohérente et prévisible quel que soit l'environnement. Contrairement aux machines virtuelles traditionnelles, les conteneurs partagent le noyau du système hôte, ce qui les rend plus efficaces en termes de ressources.

L'un des avantages clés de Docker est la portabilité, un seul fichier descriptif appelé dockerfile est responsable pour la création du conteneur. Grâce à Docker, vous pouvez emballer votre application et toutes ses dépendances dans un conteneur unique, puis le déplacer sans effort entre différents environnements, qu'il s'agisse d'un ordinateur portable de développement, d'un serveur de production ou d'un cloud public.

Docker utilise des images pour définir le contenu et la configuration d'un conteneur. Les images Docker sont des modèles immuables qui contiennent tout ce dont un conteneur a besoin pour s'exécuter. Quand un fichier décrivant une image est modifié, seule la partie modifiée et ce qui suit est reconstruit, en réutilisant ce qui avait été précédemment construit.

Docker Compose

Docker Compose représente un outil simplifiant la gestion d'applications composées de plusieurs conteneurs. Plutôt que de nécessiter une gestion manuelle de chaque conteneur et de ses paramètres

respectifs, Docker Compose offre la possibilité de définir l'ensemble de la configuration d'une application au sein d'un fichier `docker-compose.yml`.

Dans ce fichier, les services sont spécifiés, lesquels constituent les divers composants de l'application, incluant leurs images Docker, les ports exposés, les variables d'environnement et d'autres options de configuration. Par la suite, en utilisant la commande `docker-compose up`, il est possible de lancer simultanément tous les conteneurs, instaurant un environnement cohérent pour l'application.

De plus, Docker Compose simplifie la communication entre les conteneurs d'une application en mettant en place un réseau virtuel par défaut. Ceci permet aux services de se faire référence mutuellement par leur nom de service.

2.2.2 Environnement de développement

Architecture globale de Diagfit

Les développeurs travaillaient sur la dernière version en production : Diagfit 2.5.

Todo ➤ *mettre drawio archi globale 2.5* ◀

Ci-dessus, l'architecture globale de l'application Diagfit avec tous leur services. Suite à une refactorisation de l'application, le système s'est grandement simplifié.

Todo ➤ *mettre drawio archi globale 2.6* ◀

Utilisation de Docker et Docker compose

L'image docker qui était utilisée pour Diagfit lors de la CI demandait une certaine quantité de commandes pour définir l'environnement de l'application. Reproduire le même environnement pour effectuer des tests était fastidieux et causait des différences entre l'environnement de test en local et celui produit lors de la CI par GitLab.

Mission confiée

La mission qui m'a été confiée fut d'optimiser le dockerfile et le fichier Docker Compose utilisés pour le logiciel Diagfit.

J'ai aussi eu l'occasion de créer une image Docker et un fichier Docker Compose pour créer un environnement contrôlé utilisable pour la création du logiciel et également pour les tests des développeurs.

2.2.3 Missions effectuées et problèmes rencontrés

Optimisation du dockerfile ci et docker compose

La construction d'une image Docker à partir d'un dockerfile se fait ligne par ligne - étape par étape. Lors de la reconstruction de l'image, Docker est capable de reprendre la construction au niveau de la première modification dans ce fichier.

L'initialisation de l'environnement de l'image Docker est le téléchargement des packages utilisés pour le logiciel étant long et peu changeant, il était judicieux de les placer avant la récupération du code en développement.

La réduction des services utilisés nous a également permis de les retirer u fichier docker compose et donc d'accélérer le temps de lancement de l'application.

Création de multiples Dockerfiles

La création d'un environnement identique entre la ci de Gitlab et l'ordinateur des développeurs backend était un point important dans la mission qui m'a été proposée.

J'ai pu créer une image spécifique pour le rendu de l'application et une autre pour le développement et les tests unitaires à partir des fichiers existants.

Modification de l'environnement Gitlab

Sur la CI de Gitlab, on inclut le fichier dockerfile mais pas l'image construite de l'application. Il nous a donc fallu lancer une image docker générique pour build l'image docker de développement et de test d'une manière automatisée.

Une des difficultés rencontrées lors de la modification de l'environnement Gitlab fut lors de l'implémentation du nouveau job dans la Ci de gitlab : certaines variables fixées au sein du dockerfile ne prenaient pas effet dans le job

variables gitlab

- des variables ont été set dans l'environnement GitLab en variables globales contenant des informations sensibles

- > on les a enlevées et on a pu utiliser des variables personnalisées pour le programme

Impacts bénéfiques

refacto du gitlab-ci

- une image à récupérer pour faire les tests, plus besoin de la faire en local
- amélioration de la rapidité d'exécution 12'30" to 11'15" sur le job de test
- Robustesse du docker et de la CI!!!!

Impressions personnelles



3.1 Ressenti lors du stage

3.1.1 Changement de maître de stage

Space, pas aimé

vspace : j'ai pas aimé

Perte de la continuité des missions

pas de continuité dans ma mission : cumul de plusieurs missions dcp

3.1.2 Environnement et relations humaines

Effet PME agréable

apprécie les stage dans les petites entreprises, relations humaines
pas de recherche d'optimisation de l'infini, tant mieux

Openspace et télétravail

Fuck les openspaces mais pas trop
fuck le télétravail et ça beaucoup

Experience des autres stagiaires amis

les potos qui vivent mal leur stage : nofun, suis content de m'en sortir mais SRX ?

3.2 Zukunft

3.2.1 Environnement de travail visé

PME

petite entreprise ? ptet pas, mon stage de M1 peut etre un essai pour me faire ma propre idée

Projets longs

3.2.2 Orientation professionnelle

Hésitation entre Dev et DevOps

matière : j'hésite encore fort fort entre dev et sysadmin mon sage de sys s'est trnasformé en stage de dev sans faire expres...

Conclusion



4.1 conclu mais mettre un titre genre : mon stage dans amiral technologies

j'ai travaillé dans entreprise : description

j'ai travaillé pdt 14 semaines

j'ai travaillé sur ça

J'ai beaucoup apporté à l'entreprise pour les 3 mois et demi passé lors de ce stage : :D

j'ai bien aimé, j'ai pas aimé

je me vois bien là dans le ZUKUNFT

Annexes et Bibliographie



annexes et bib