BTS SIO 2ème année

Du 6 Janvier au 21 Février 2025

KOUCHA AHMED
BTS SIO 2ème année

RÉGION Nouvelle-Aquitaine

RAPPORT DE STAGE

Sommaire

I. Introduction II. Déroulement III. Bilan IV. Conclusion V. Documentations

Tuteur : Lambert Guillaume

Fonction : Chef du service "Infrastructure systèmes et réseaux des lycées"

Professeur : Monsieur Sautour F.

Introduction

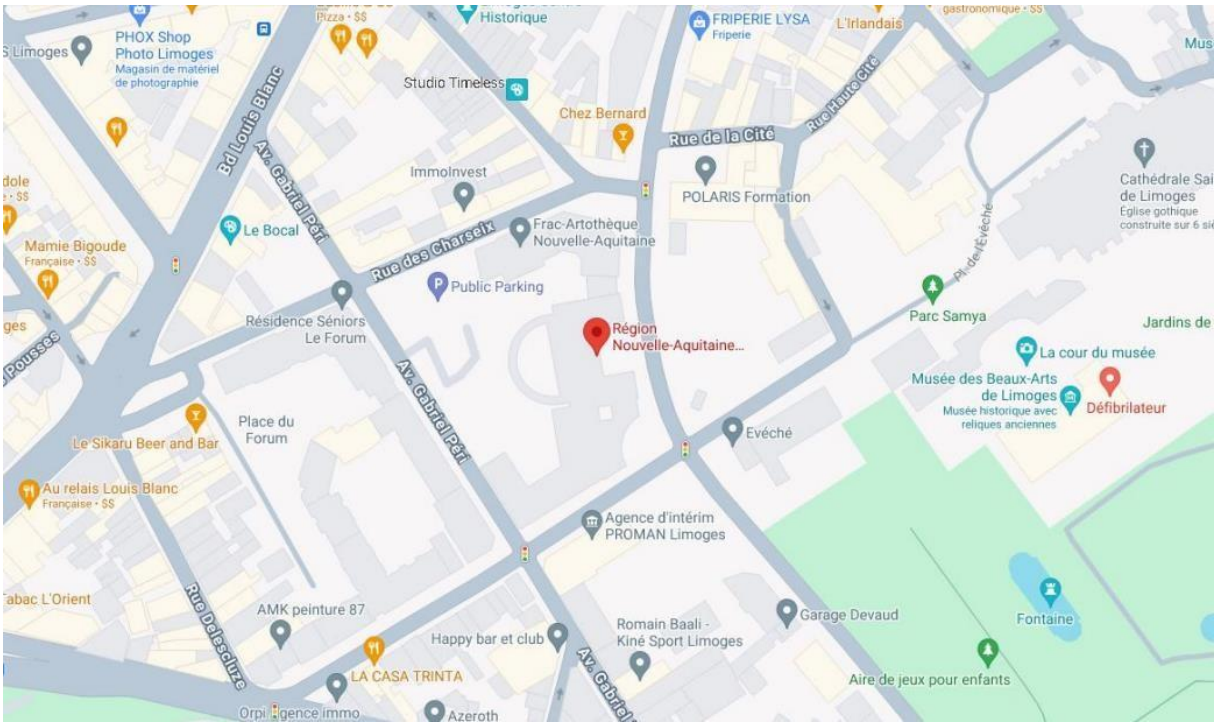
Pendant cette deuxième année de BTS SIO en option SISR, j'ai effectué un stage dans le service Infrastructure systèmes et réseaux des lycées à la région de la Nouvelle-Aquitaine à limoges du 6 Janvier au 21 Février 2025.

Je remercie Mr Lambert de m'avoir permis de re effectuer mon stage, ainsi que les personnes du service.

Le service dédié à l'infrastructure des systèmes et réseaux des lycées de la région Nouvelle-Aquitaine, sous l'égide de la région, a été mis en place progressivement à partir de la création de la région NouvelleAquitaine le 1er janvier 2016.

Ce service s'est développé pour répondre aux besoins spécifiques des lycées en matière de numérique et de technologie après cette date.

CS 3116 cedex, 27 Bd de la Corderie 1, 87000 Limoges, **Lien vers le site**



III) Déroulement

Présentation Générale du Travail Effectué

1. Mise en place d'une Infrastructure de Gestion des Logs

Cette mission visait à déployer une infrastructure complète permettant de collecter, stocker, analyser et exploiter les logs de manière intelligente. **Filebeat** est utilisé pour récupérer automatiquement les logs des machines clientes et les envoyer vers **Elasticsearch**, qui assure leur indexation et leur recherche rapide.

Afin d'aller plus loin dans l'analyse, **Qdrant** stocke ces logs sous forme de vecteurs, permettant d'identifier des similarités et de faciliter la recherche sémantique. **Ollama** joue un rôle clé en générant des embeddings, transformant les logs en représentations numériques exploitables par Qdrant pour une analyse avancée. Enfin, **N8N** orchestre le tout en automatisant les processus et en déclenchant des alertes en cas d'anomalie. Cette architecture optimise la supervision et permet une meilleure réactivité face aux incidents.

2. Une Infrastructure de Surveillance des Services avec Uptime Kuma

L'objectif de cette mission était de **surveiller en temps réel l'état des services** et de **détecter rapidement les pannes**. Pour cela, **Uptime Kuma** a été intégré sous **Docker** pour suivre **Keycloak**, qui gère l'authentification de **Nextcloud**.

Comme **Nextcloud dépend de Keycloak**, une panne de ce dernier empêcherait les connexions. Grâce à **Uptime Kuma**, la disponibilité des deux services est surveillée en continu, avec des **alertes instantanées** en cas de problème, assurant une **réactivité optimale**.

Contexte

Le **service Infrastructure Systèmes et Réseaux des lycées** ,de la **région Nouvelle-Aquitaine** joue un rôle essentiel dans le maintien et l'évolution des infrastructures numériques des établissements scolaires. Son objectif principal est d'assurer la disponibilité, la sécurité et l'optimisation des services informatiques, tout en s'adaptant aux évolutions technologiques et aux besoins des utilisateurs.

Durant mon stage, j'ai été amené à travailler sur des projets visant à améliorer la gestion et la supervision des infrastructures IT. Les enjeux étaient multiples :

- Automatiser la collecte et l'analyse des logs pour une meilleure détection des anomalies et une réponse rapide aux incidents.
- Mettre en place une solution de surveillance en temps réel des services critiques afin d'assurer leur disponibilité et d'optimiser la réactivité en cas de dysfonctionnement.

Mission 1 : FileBeat, Elasticsearch, qdrant, ollama, n8n

L'objectif de cette mission était de concevoir une infrastructure permettant la collecte, le stockage et l'analyse intelligente des logs en temps réel. Pour cela, plusieurs outils ont été intégrés afin d'assurer une gestion efficace des logs provenant de machines clientes.

L’architecture repose sur une combinaison de **Filebeat**, **Elasticsearch**, **Qdrant**, **Ollama** et **N8N**, chacun ayant un rôle spécifique pour garantir un traitement optimal des données.

Filebeat a été utilisé comme agent de collecte des logs, installé directement sur les machines clientes, notamment celles hébergeant un serveur Apache2. Son rôle est de surveiller en continu les fichiers de logs situés dans ‘/var/log/apache2/*.log’ et d’envoyer ces événements vers Elasticsearch. L’utilisation de Filebeat permet une transmission efficace et allégée des logs sans impacter les performances des serveurs sources.

Une fois les logs collectés, Elasticsearch prend en charge leur stockage et leur indexation. Ce moteur de recherche avancé permet d’organiser les logs sous forme d’index structurés, facilitant ainsi l’exécution de requêtes précises pour retrouver rapidement des informations spécifiques.

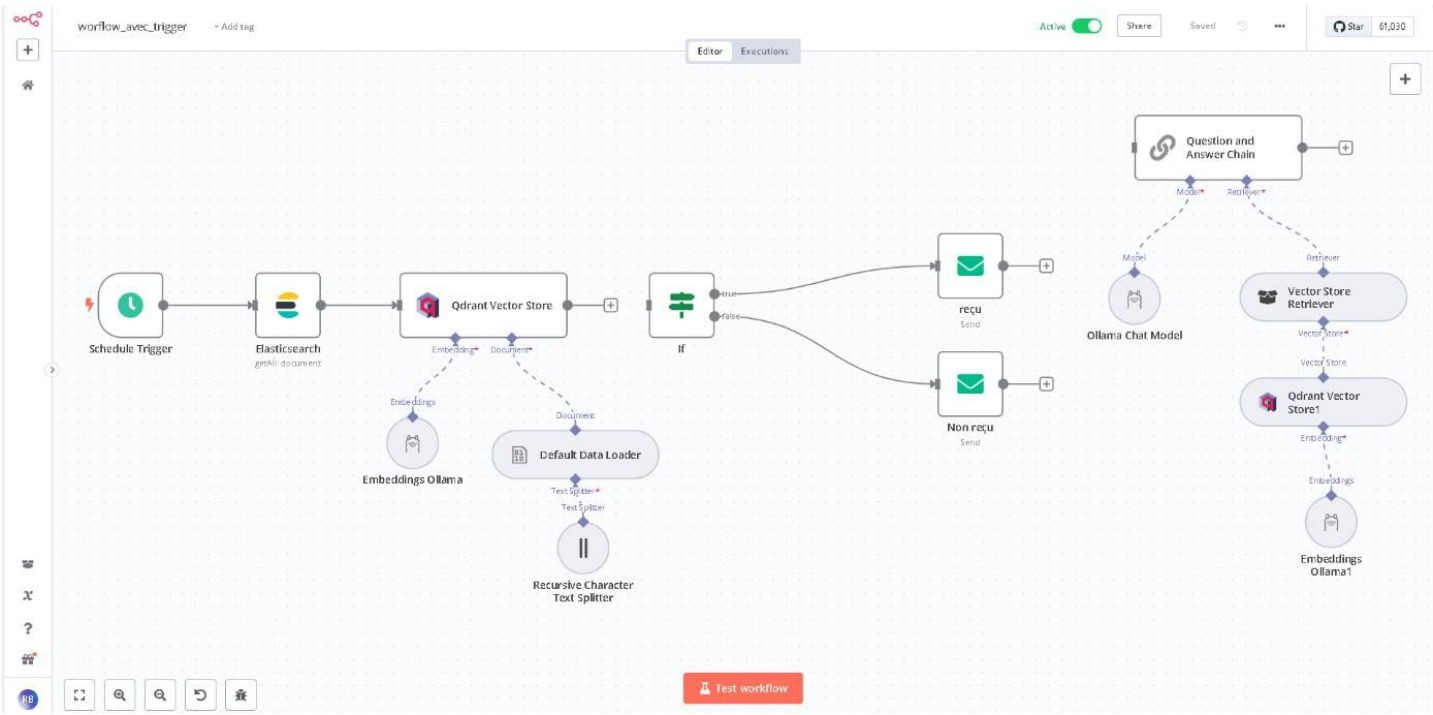
Grâce à ses fonctionnalités analytiques, Elasticsearch permet également de détecter des tendances et d’identifier des anomalies dans les logs, renforçant ainsi la surveillance des systèmes.


```
    },
    "event" : {
      "ingested" : "2025-01-23T10:38:36.485124245Z",
      "original" : "127.0.0.1 - - [22/Jan/2025:15:40:23 +0000] \"GET /nonexistentpage HTTP/1.1\" 404 231",
      "kind" : "event",
      "created" : "2025-01-23T10:36:30.253Z",
      "module" : "apache",
      "category" : "web",
      "dataset" : "apache.access",
      "outcome" : "failure"
    },
    "user" : {
      "name" : "-"
    }
  }
},
{
  "_index" : "filebeat-7.17.27-2025.01.23-000001",
  "_id" : "zR--kpQB07aCxvg6DUHW",
  "_score" : 1.0,
  "_source" : {
    "importance_level" : "high",
    "log" : {
      "file" : {
        "path" : "/var/log/apache2/access.log"
      }
    },
    "source" : {
      "address" : "127.0.0.1",
      "ip" : "127.0.0.1"
    },
    "error" : {
      "message" : "Failed to rename fields in processor: could not fetch value for key: http.request.method, Error: key not found"
```


Cependant, pour aller au-delà des recherches textuelles classiques et introduire une analyse sémantique plus poussée, Qdrant a été intégré à l’infrastructure. Contrairement à Elasticsearch, qui fonctionne avec des index traditionnels, Qdrant est une base de données vectorielle spécialisée dans le stockage et la recherche de similarités à l’aide d’embeddings. Ces représentations numériques permettent d’identifier des événements similaires même si leurs termes exacts diffèrent. Cette approche est particulièrement utile pour regrouper des logs connexes ou repérer des comportements récurrents dans les erreurs système.

L’une des étapes clés de cette architecture repose sur **Ollama**, un moteur d’intelligence artificielle permettant de générer ces embeddings. Ollama convertit les logs en vecteurs numériques exploitables par Qdrant, offrant ainsi une analyse avancée des relations entre les événements. Grâce à cette IA, il devient possible d’extraire des insights plus profonds et d’améliorer la capacité de détection des anomalies, en identifiant des motifs qui échapperaient à une simple analyse textuelle. Ollama joue ainsi un rôle central dans l’enrichissement des logs et l’optimisation de la recherche sémantique.

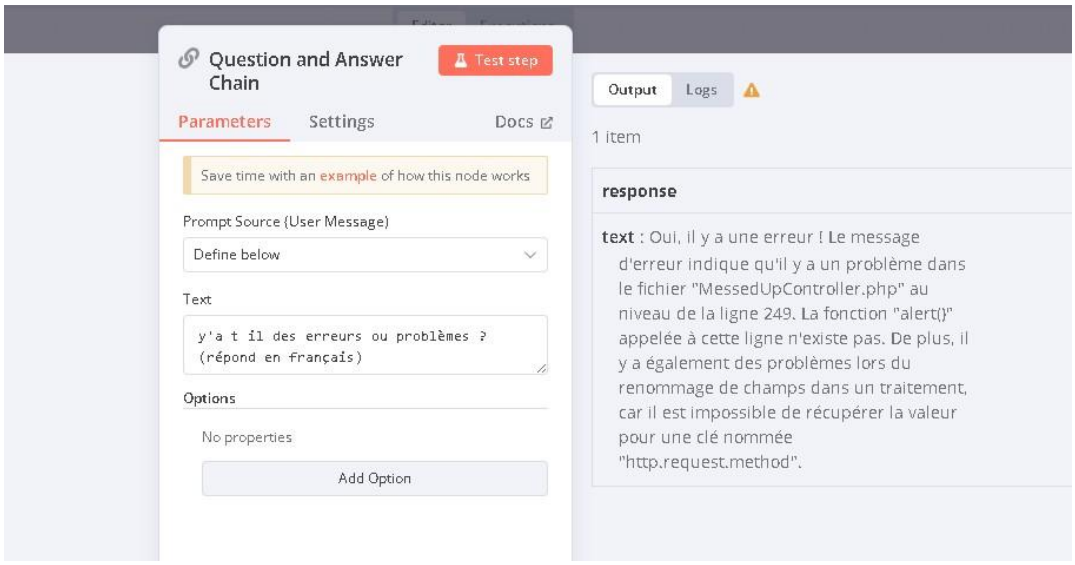
Enfin, N8N vient gérer l’ensemble de ces outils en automatisant le pipeline de traitement des logs. Cet outil permet d’enchaîner les différentes étapes du flux de données, de déclencher des actions spécifiques lorsqu’un log est détecté et d’envoyer des alertes en cas d’anomalie. Par exemple, dès qu’un log critique est enregistré dans Elasticsearch, N8N peut automatiquement le transmettre à Qdrant et Ollama pour analyse et générer une notification ou un rapport d’incident.



L'intégration de ces technologies permet de concevoir une infrastructure robuste et évolutive, capable de traiter un volume important de logs en temps réel tout en exploitant les capacités de l'intelligence artificielle. Grâce à Elasticsearch et Qdrant, l'architecture combine recherche textuelle et analyse vectorielle, offrant ainsi un système de surveillance performant et intelligent.

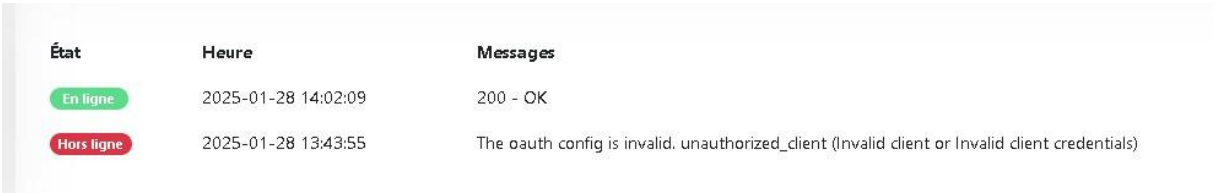
Ollama ajoute une couche supplémentaire d'interprétation et d'automatisation des données, tandis que N8N simplifie l'ensemble du processus en orchestrant les interactions entre les différents composants.

Cette infrastructure assure ainsi un suivi précis des activités des machines clientes et améliore la capacité de réponse aux incidents, tout en exploitant la puissance de l'IA pour une analyse plus pertinente et proactive des logs.

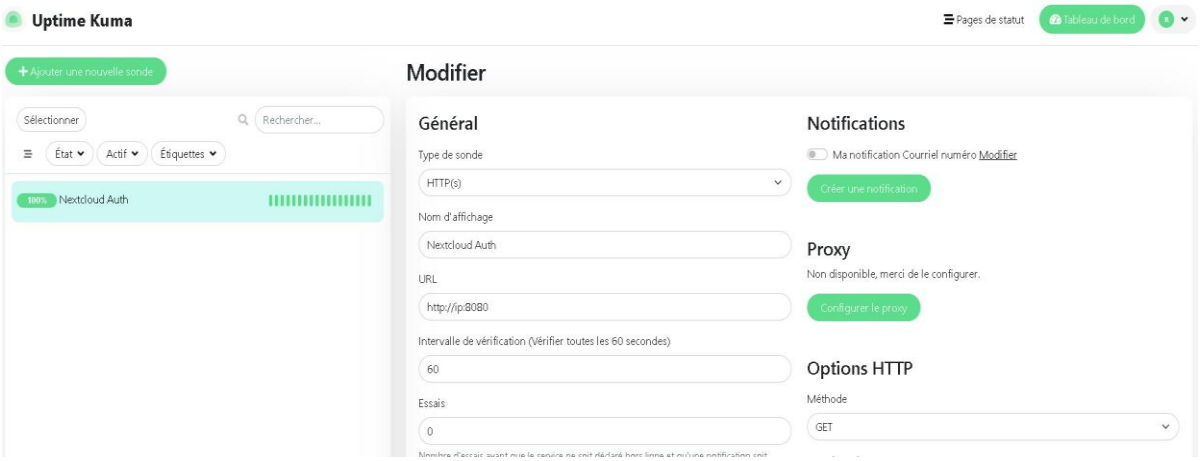


Mission 2 : Uptime Kuma & Keycloak

L'objectif de cette mission était de mettre en place une solution de monitoring permettant de surveiller en temps réel l'état de Keycloak et de détecter rapidement toute panne. Keycloak a été intégré à Nextcloud en tant que **plugin d'authentification**, permettant aux utilisateurs de se connecter via un système de gestion centralisée des identités. Dans ce contexte, assurer la disponibilité de Keycloak est primordial, car une panne empêcherait l'accès à Nextcloud et à toute autre application utilisant cette authentification unique. Pour cela, Uptime Kuma a été mis en place afin de superviser en continu le bon fonctionnement de Keycloak et d'envoyer des alertes en cas de dysfonctionnement.

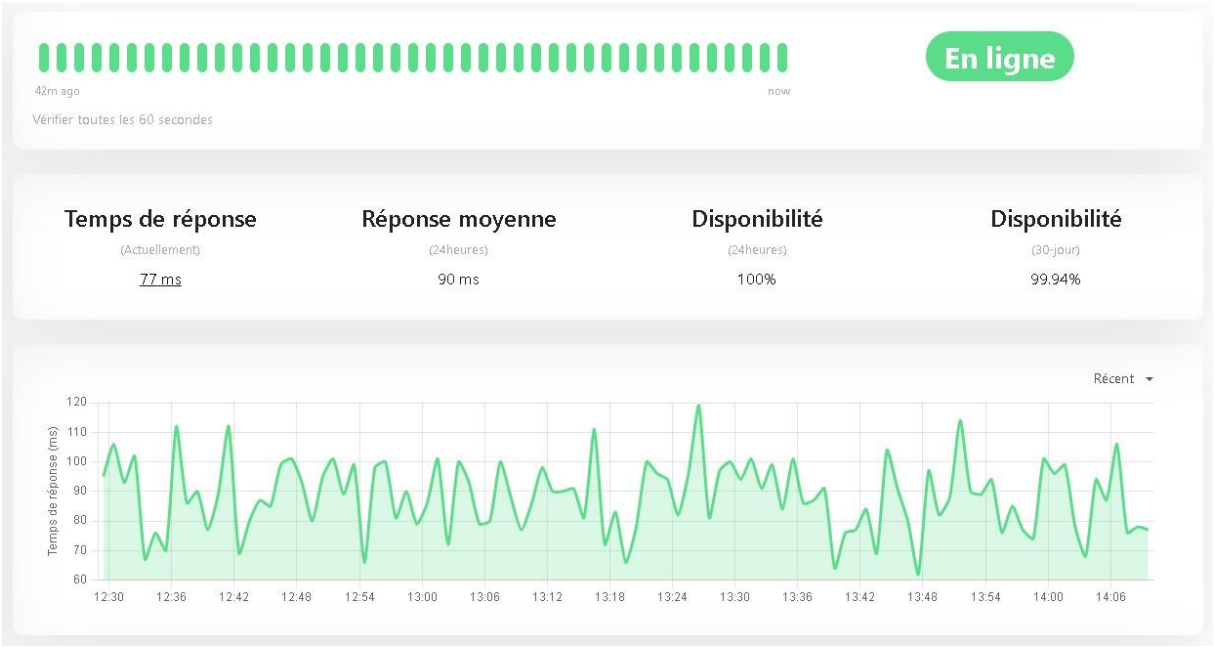


L’architecture repose sur Uptime Kuma comme outil principal de surveillance, chargé de vérifier l’accessibilité de Keycloak. Nextcloud, bien que présent, n’est pas directement surveillé, mais a été utilisé comme support concret pour tester l’intégration de Keycloak et illustrer un cas d’usage réel. Uptime Kuma effectue des vérifications régulières sur Keycloak via des requêtes HTTP afin de s’assurer que le service répond correctement et que l’interface d’authentification est accessible. En cas d’indisponibilité ou de réponse anormalement lente, Uptime Kuma génère automatiquement une alerte et notifie les administrateurs via email, Discord, Telegram ou un webhook personnalisé.



Grâce à Uptime Kuma, il est désormais possible de détecter immédiatement toute interruption de Keycloak et d’intervenir rapidement avant que l’incident ne perturbe l’accès des utilisateurs. Cette infrastructure permet d’anticiper les défaillances, de réduire les temps d’arrêt et d’assurer une continuité de service optimale.

La mise en place de cette solution garantit une supervision efficace et continue de Keycloak, assurant ainsi la stabilité de l’authentification sur Nextcloud. Cette infrastructure apporte un suivi en temps réel des performances et une intervention rapide en cas d’anomalie, rendant l’environnement plus fiable et sécurisé.



III) Bilan

Les deux infrastructures mises en place dans le cadre de ces missions ont chacune répondu à des besoins spécifiques tout en exploitant des technologies modernes pour optimiser la gestion des logs et la supervision des services critiques.

La première a permis de collecter, stocker et analyser les logs en temps réel en combinant des techniques de recherche classique et d'analyse sémantique avancée. L'automatisation a été intégrée pour gérer le traitement et déclencher des alertes en cas d'anomalie. L'ajout de capacités d'intelligence artificielle a également permis d'améliorer la détection des tendances et des comportements inhabituels dans les événements système.

La seconde avait pour objectif de surveiller l'accessibilité et le bon fonctionnement d'un service d'authentification centralisé. Une solution de monitoring a été mise en place pour effectuer des vérifications régulières et alerter immédiatement en cas de panne. Grâce à ce dispositif, les interruptions sont détectées rapidement, garantissant ainsi la continuité des accès aux différentes applications.

Bien que distinctes, ces deux architectures partagent un objectif commun :

renforcer la fiabilité et la réactivité des systèmes informatiques. L'une optimise la gestion des journaux d'événements grâce à des analyses avancées, tandis que l'autre assure une supervision efficace pour éviter toute interruption de service.

IV) Conclusion

En conclusion, ces missions m'ont permis d'acquérir de nouvelles compétences en découvrant des outils et technologies que je n'avais pas encore abordés en cours. Ce stage a été une réelle opportunité d'apprentissage, m'apportant une meilleure compréhension des architectures modernes et des solutions de traitement et de surveillance des systèmes. Il m'a également permis de mettre en pratique mes connaissances théoriques dans un contexte réel, en appliquant les notions vues en formation pour résoudre des problématiques concrètes. Cette expérience a renforcé ma capacité d'adaptation et m'a apporté une vision plus approfondie du fonctionnement des infrastructures en entreprise.

V) Documentations

- Documentation Infrastructure mission 1
- Documentation Infrastructure mission 2
    - Présentation Docker