ÉPIGRAPHE

« La technologie ne résout pas tous les problèmes, mais elle donne à ceux qui savent l'utiliser le pouvoir d'en anticiper beaucoup. »

Kevin Mitnick

DÉDICACE

À toute la famille TWITE SEYA, en témoignage d'amour, de gratitude et de reconnaissance pour votre soutien indéfectible, vos sacrifices silencieux et votre présence constante tout au long de ce parcours.

REMERCIEMENTS

Au regard des vicissitudes ayant caractérisé notre formation scientifique, nous tenons à nous acquitter d'un agréable devoir : celui d'exprimer ici nos remerciements très sincères à tous ceux qui, de loin ou de près, ont contribué à notre formation en général et à la réalisation de ce travail de fin de cycle.

Nos sentiments de reconnaissance vont droit au Docteur Tubudi Mukadi John, qui nous a dirigés tout au long de ce travail en apportant un esprit d'analyse, une patience exemplaire et une maîtrise remarquable.

Nous avons aussi une grosse dette de reconnaissance envers l'assistant Grâce Kot, qui n'a hésité un seul instant à donner le meilleur de lui-même à notre égard tout au long de notre premier cycle.

Nous pensons également à nos amis et compagnons de lutte :

Amsini Lusengo Ben, Tambwe Tshishimbi Clément, Kanswat Mukaz Aubin, Ndala David, Mushid Victor, qui, durant notre parcours académique, ont été pour nous non seulement des collègues mais aussi des condisciples qui n'ont ménagé aucun effort pour nous apporter leur soutien.

À tous, nous disons : merci infiniment.

LISTE DES ILLUSTRATIONS

LISTE DES ABREVIATIONS

Abréviation	Signification
IT	Information Technology (Technologie de l'information)
LAN	Local Area Network
VLAN	Virtual Local Area Network
ERP	Enterprise Resource Planning
CPU	Central Processing Unit
RAM	Random Access Memory
WAF	Web Application Firewall
MFA	Multi-Factor Authentication
SIEM	Security Information and Event Management
API	Application Programming Interface
KPI	Key Performance Indicator
TLS	Transport Layer Security
SQL	Structured Query Language
OWASP	Open Web Application Security Project

NAS	Network Attached Storage

RÉSUMÉ

Dans un contexte de transformation numérique accélérée, la gestion efficace des infrastructures informatiques constitue un enjeu stratégique pour les entreprises. Le présent mémoire s'inscrit dans cette dynamique en proposant une étude approfondie sur la conception et le déploiement d'une application de monitoring dédiée à la supervision du parc informatique de l'entreprise Kamoa SA, située à Kolwezi (RDC).

Face aux interruptions de service non anticipées, à l'absence de visibilité sur les performances réseau et à la faible traçabilité des incidents, l'objectif principal de ce travail est de concevoir une solution numérique capable d'assurer une surveillance en temps réel, de générer des alertes automatisées et de produire des tableaux de bord décisionnels. Pour ce faire, l'étude s'appuie sur une méthodologie combinant analyse documentaire, observation terrain, interviews ciblées et expérimentation développée repose sur une architecture modulaire intégrant des technologies open source telles que Prometheus, Grafana, PostgreSQL, Python et React.js. Elle comprend plusieurs modules fonctionnels : supervision des équipements, alertes, reporting, gestion des accès, interface graphique et sécurité renforcée. Des diagrammes UML ont été utilisés pour modéliser les interactions et structurer le développement.

Les tests réalisés ont permis de valider la fiabilité, la performance et la sécurité du système. Le déploiement progressif au sein de Kamoa SA, accompagné d'une formation ciblée des utilisateurs et d'une documentation technique complète, a favorisé l'appropriation de l'outil et son intégration dans les processus métiers.

En conclusion, cette solution de monitoring contribue à améliorer la résilience, la visibilité et la gouvernance du système d'information de Kamoa SA. Elle ouvre également des perspectives d'évolution vers une supervision intelligente, intégrant l'intelligence artificielle pour une gestion prédictive et proactive des infrastructures IT.

TABLE DES MATIERES

INTRODUCTION

0.1. Présentation de l'objet d'étude

La gestion des infrastructures informatiques est devenue un enjeu stratégique pour les entreprises. Avec l'expansion des systèmes et la complexité croissante des réseaux, il devient impératif de disposer d'un système de supervision efficace. Le mémoire de Twite se focalise sur l'entreprise Kamoa SA, confrontée à des interruptions de service, des incidents non détectés et une inefficacité de gestion de son parc informatique. L'étude vise à concevoir une application de monitoring capable de superviser en temps réel les équipements informatiques, de détecter les pannes et d'aider à la prise de décisions grâce à des tableaux de bord analytiques.

0.2. Choix et intérêt du sujet

0.2.1. Choix du sujet

Le choix de ce sujet repose sur la nécessité de mettre en place une solution de monitoring adaptée à l'environnement informatique de Kamoa SA. L'objectif est d'assurer un contrôle permanent des équipements, de prévenir les incidents, de réduire les interruptions et de sécuriser le réseau.

0.2.2. Intérêt du sujet

Sur le plan scientifique, le mémoire enrichit les recherches en supervision des infrastructures IT. Sur le plan technique, il permet d'expérimenter des outils modernes. Enfin, sur le plan pratique, l'outil développé répond aux besoins spécifiques de Kamoa SA, tout en offrant un modèle réplicable.

0.3. ÉTAT DE L'ART

a. Travaux antérieurs et solutions existantes

La surveillance des infrastructures informatiques (IT monitoring) est un domaine largement étudié. Jean-Michel Cornu (2018) a souligné l'importance d'intégrer le monitoring comme levier stratégique de gestion des ressources numériques. Selon lui, la supervision des systèmes n'est pas seulement une exigence technique, mais un outil décisionnel pour l'optimisation continue.

Plusieurs outils open source ont été adoptés dans les environnements d'entreprise :

- **Nagios**, réputé pour sa robustesse mais souvent critiqué pour sa complexité de configuration et son interface obsolète (Zhou et al., 2017) ;
- **Zabbix**, qui intègre des visualisations avancées mais peut se révéler lourd en ressources (Smith & El-Masri, 2020) ;
- **Datadog**, très complet mais à coût élevé, ce qui limite son adoption dans les PME africaines (Chikweche & Fletcher, 2022).

b. Comparaison critique des outils

Outil	Avantages principaux	Limites constatées
Nagios	Personnalisable, robuste	Interface vieillissante, courbe d'apprentissage raide
Zabbix	Tableaux de bord intégrés, auto-découverte	Configuration plus complexe que Prometheus
Prometheus	Légèreté, intégration facile avec Grafana	Moins adapté aux logs bruts
Datadog	Tout-en-un (logs, métriques, alertes, APM)	Modèle économique basé sur l'abonnement

Le choix de Prometheus avec Grafana dans le cadre de cette étude repose sur leur capacité à être facilement déployés, leur adaptabilité à des contextes d'entreprise intermédiaire comme Kamoa SA, et la richesse de leur écosystème open source.

c. Démarcation de notre étude

Notre recherche se distingue de l'existant par une triple spécificité :

- Elle vise à concevoir une solution de monitoring adaptée spécifiquement aux besoins internes de Kamoa SA **;**
- Elle intègre des modules d'intelligence artificielle (classification des incidents, prédiction de surcharge) dans la supervision ;
- Elle évalue l'impact organisationnel et économique de la mise en œuvre d'une telle application, au-delà de la simple performance technique.

0.4. PROBLÉMATIQUE ET HYPOTHÈSES

0.4.1. Problématique

Les interruptions de service non anticipées, la difficulté à repérer les goulets d'étranglement et l'absence d'un système de supervision centralisé ralentissent les opérations informatiques au sein de Kamoa SA. Dans un environnement en pleine expansion, il devient stratégique d'automatiser la collecte, l'analyse et la visualisation des données système. Cette étude se pose donc la question suivante :

> Dans quelle mesure une application de monitoring intégrée, utilisant Prometheus et Grafana, peut-elle améliorer la visibilité, la performance et la résilience des infrastructures informatiques de Kamoa SA ?

0.4.2. Hypothèses

1. **H1** : L'absence de solution de monitoring entraîne des interruptions fréquentes et une gestion inefficace des ressources IT.
2. **H2** : Si une application de monitoring centralisée est déployée, alors elle permettra d'améliorer la supervision en temps réel et de réduire les temps d'intervention.
3. **H3 (reformulée)** : Si l'application développée est compatible avec l'infrastructure existante et dispose d'une interface intuitive, alors elle facilitera l'adoption par les équipes et produira une amélioration mesurable de la performance IT (temps de réponse, taux de disponibilité, etc.).

0.5. MÉTHODES ET TECHNOLOGIES

0.5.1. Méthodes

Trois méthodes ont été utilisées :

- Méthode analytique : pour examiner les pratiques en vigueur et les documents techniques.
- Méthode expérimentale : pour tester plusieurs solutions et choisir la plus adaptée.

- Méthode comparative : pour évaluer les avantages des outils open source face aux outils propriétaires.

0.5.2. Techniques

Les techniques utilisées sont :

- Documentaire : consultation de sources spécialisées.
- Interview : échanges avec les responsables informatiques de Kamoa SA.
- Observation directe : immersion dans l'environnement de travail pour évaluer les conditions réelles.

06. DÉLIMITATION DU TRAVAIL

- Délimitation temporelle

L'étude couvre la période allant de l'état initial du parc informatique jusqu'à la mise en place de l'application.

- Délimitation spatiale

Elle est limitée à l'entreprise Kamoa SA, située à Kolwezi, dans la province du Lualaba (RDC).

- Délimitation matérielle

Elle porte uniquement sur la mise en place d'un outil de monitoring, sans aborder d'autres domaines comme la cybersécurité globale ou la gestion générale des systèmes d'information.

07. DIVISION DU TRAVAIL

L'étude se divise en trois grands chapitres :

- Le premier chapitre présente les généralités sur le monitoring des infrastructures informatiques.

- Le deuxième chapitre est consacré à la conception de l’application de monitoring, de l’analyse des besoins à la modélisation.

- Le troisième chapitre aborde le déploiement de l’application, son intégration au réseau existant, les tests et les ajustements nécessaires.

CHAPITRE I : GÉNÉRALITÉS SUR LE MONITORING DES INFRASTRUCTURES INFORMATIQUES

Dans ce chapitre, il sera question de poser les bases conceptuelles et contextuelles relatives au monitoring des infrastructures informatiques. Dans un premier temps, la Section 1 s'attachera à définir les notions fondamentales autour du monitoring et à présenter ses objectifs principaux, notamment en ce qui concerne la gestion des ressources informatiques, la performance et la sécurité des systèmes, ainsi que les outils et technologies couramment utilisés pour assurer cette surveillance. Il s'agira ainsi de cerner le cadre théorique permettant de comprendre l'utilité et le fonctionnement global d'un système de monitoring informatique.

Ensuite, la Section 2 abordera de manière spécifique le contexte de l'entreprise Kamoa SA. Il y sera question, d'une part, de décrire l'organisation interne de l'entreprise et son infrastructure informatique actuelle, et d'autre part, d'identifier les faiblesses et contraintes rencontrées dans la gestion de son parc informatique. Cette analyse des besoins permettra de dégager les attentes de l'entreprise en matière de monitoring, en vue d'orienter la conception d'une solution adaptée.

Section 1 : Concepts et définition du monitoring informatique

§1. Notion de monitoring et gestion d'un parc informatique

Le monitoring informatique, également appelé supervision des systèmes d'information, désigne l'ensemble des techniques, outils et processus déployés pour assurer une observation continue ou périodique des composants d'un système informatique. Il permet de suivre en temps réel ou en différé l'état de fonctionnement de serveurs, de postes de travail, d'équipements réseau, d'applications, de bases de données ou encore de services cloud. Cette surveillance vise à anticiper les défaillances, à améliorer les performances et à garantir la disponibilité des ressources numériques (Barczyk & Duncan, 2020).

Dans une organisation, la supervision ne se limite pas à une simple collecte d'informations techniques : elle devient un outil décisionnel permettant aux administrateurs d'identifier rapidement les anomalies, d'analyser leurs causes et de mettre en œuvre des solutions proactives. Elle constitue ainsi un pilier fondamental de la stratégie de gestion des systèmes d'information (Jones, 2018).

La gestion d'un parc informatique, quant à elle, couvre l'ensemble des actions nécessaires à l'administration, à la maintenance, à la sécurisation, à l'inventaire et à l'optimisation des ressources matérielles et logicielles. Elle implique une coordination rigoureuse, surtout dans les grandes infrastructures où coexistent de nombreux terminaux hétérogènes. Dans ce contexte, le monitoring s'impose comme un outil essentiel pour centraliser la supervision, automatiser les diagnostics, planifier les interventions et rationaliser les coûts d'exploitation (Pfleeger & Pfleeger, 2022).

La complémentarité entre monitoring et gestion du parc informatique est manifeste : la supervision devient une fonction transversale qui alimente en données fiables les processus de gestion. Elle permet une vision holistique de l'environnement informatique – à la fois sur le plan physique (température, stockage, alimentation) et logique (charge CPU, mémoire utilisée, disponibilité des applications, erreurs système). Cette visibilité renforce la capacité de pilotage des équipes informatiques et facilite des prises de décision fondées sur des indicateurs objectifs (Kim et al., 2021).

De plus, le monitoring contribue à une gestion préventive du cycle de vie des équipements. Grâce à la surveillance continue des performances, il devient possible d'identifier les signes de dégradation avant qu'ils ne deviennent critiques. Ainsi, les interventions de maintenance peuvent être anticipées, tout comme les besoins en renouvellement ou en extension de capacité.

Enfin, dans un environnement réglementé, le monitoring constitue aussi un atout pour la conformité. Il permet de produire des preuves de bonne gestion des systèmes, via des journaux de surveillance, des rapports d'audit et des historiques d'alerte, essentiels lors de contrôles ou d'audits de sécurité (Stallings, 2019).

C'est dans cette perspective que nous analyserons, dans le paragraphe suivant, l'importance du monitoring pour garantir la performance et la sécurité des systèmes informatiques.

§2. Importance du monitoring pour la performance et la sécurité

1. Une surveillance continue pour garantir la stabilité du système

Dans les infrastructures informatiques modernes, où les composants matériels et logiciels sont interconnectés de manière complexe, le monitoring s'impose comme une pratique incontournable. Il consiste à observer en temps réel le fonctionnement du parc informatique afin d'identifier toute anomalie susceptible de compromettre la stabilité, la performance ou la sécurité du système (Jones, 2018). En fournissant des informations actualisées sur les activités du réseau, des serveurs, des applications ou encore des bases de données, il constitue une source essentielle de visibilité pour les administrateurs.

2. Optimisation des performances par l'analyse des indicateurs clés

Sur le plan de la performance, le monitoring permet de collecter des métriques techniques telles que l'utilisation du processeur, la charge mémoire, le trafic réseau ou le temps de réponse des applications. Ces données révèlent les goulets d'étranglement, les saturations et les points de faiblesse à corriger (Barczyk & Duncan, 2020). Grâce à ces informations, les équipes informatiques peuvent adapter la configuration des ressources, rééquilibrer la charge et ainsi améliorer la réactivité du système.

Ce processus facilite également une meilleure planification des ressources. En observant les tendances d'utilisation, les administrateurs peuvent prévoir les évolutions futures et décider, de manière éclairée, du moment opportun pour augmenter la capacité de stockage, ajouter des serveurs ou migrer vers des infrastructures plus robustes (Kim, Lim & Lee, 2021). Cela permet non seulement d'optimiser les investissements, mais aussi de maintenir une haute disponibilité des services.

3. Renforcement de la sécurité par une détection proactive des incidents

Le monitoring joue aussi un rôle capital dans la protection des systèmes contre les menaces internes et externes. Les outils de surveillance détectent en temps réel les anomalies telles que les connexions suspectes, les tentatives d'intrusion ou les flux réseau anormaux (Stallings, 2019). Ces alertes précoces permettent une réponse rapide aux incidents, limitant ainsi leur impact potentiel.

L’analyse des journaux systèmes (logs) et des accès utilisateurs constitue un pilier fondamental pour assurer la traçabilité des opérations sensibles. Ce suivi contribue à satisfaire les exigences réglementaires, notamment celles imposées par la norme ISO/IEC 27001, en matière de contrôle d’accès, d’intégrité des données et de protection des informations confidentielles (Pfleeger & Pfleeger, 2022).

4. Un levier pour la conformité réglementaire

Outre les bénéfices techniques, le monitoring s’inscrit dans une logique de conformité. Plusieurs cadres réglementaires, tels que le RGPD ou les standards ISO, exigent la mise en place de mécanismes de surveillance continue. Ceux-ci doivent garantir que toute activité sur le système d’information est identifiable, traçable et justifiable. Le monitoring devient ainsi un outil indispensable pour répondre aux audits de sécurité, documenter les incidents, et prouver le respect des obligations légales (Cuppens-Boulahia et al., 2021).

5. Amélioration de la réactivité et continuité des services

Un autre avantage majeur du monitoring réside dans sa capacité à améliorer la réactivité des équipes IT. En cas de défaillance, les alertes automatiques permettent une intervention rapide, réduisant significativement les temps d’arrêt et évitant des perturbations prolongées (Barczyk & Duncan, 2020). Cette efficacité opérationnelle renforce la fiabilité du système et la confiance des utilisateurs.

6. Appui stratégique pour l’évolution du système d’information

Enfin, le monitoring ne se limite pas à un outil technique : il sert aussi de support stratégique. En capitalisant des données historiques sur les comportements du système, il permet de repérer les tendances, d’anticiper les besoins futurs et de planifier l’évolution du système d'information. Ce rôle est d’autant plus important avec l’introduction progressive de l’intelligence artificielle et de l’automatisation, qui exigent des données fiables pour alimenter leurs modèles décisionnels (Kim, Lim & Lee, 2021).

Ainsi, le monitoring se présente non seulement comme un dispositif opérationnel de surveillance, mais aussi comme un outil stratégique pour l’anticipation, la résilience et l’innovation technologique. Cette double dimension sera approfondie à travers l’analyse des outils et technologies de monitoring dans la section suivante.

§3. Outils et technologies de surveillance informatique

La surveillance informatique repose sur un ensemble d'outils technologiques permettant de superviser, analyser et gérer les infrastructures en temps réel. Ces solutions assurent non seulement la performance des systèmes, mais renforcent également la sécurité globale du réseau en détectant rapidement les incidents. Cette section présente les principales catégories d'outils utilisés dans les environnements professionnels pour une surveillance efficace.

I. Outils de supervision des performances systèmes et réseaux

Les outils de supervision surveillent l'état des serveurs, des équipements réseaux (routeurs, switches), des bases de données et des services applicatifs. Ils collectent des métriques telles que l'utilisation du processeur, la mémoire disponible, le trafic réseau et les temps de réponse, ce qui permet d'identifier les goulets d'étranglement et les risques de saturation (Barika & Meroufel, 2019).

Parmi les outils les plus répandus :

- **Nagios** : fournit une surveillance des systèmes et services avec des alertes personnalisables.
- **Zabbix** : intègre des fonctions avancées de visualisation et de monitoring en temps réel.
- **PRTG Network Monitor** : connu pour sa facilité d'usage et ses capteurs personnalisables.

II. Solutions de gestion et d'analyse des journaux (logs)

Les journaux systèmes constituent une source cruciale pour diagnostiquer les erreurs, identifier les intrusions et satisfaire aux exigences de conformité. Des outils spécialisés permettent d'agréger, analyser et visualiser ces données (Rashid & Jalil, 2020).

Exemples de solutions couramment utilisées :

- **ELK Stack (Elasticsearch, Logstash, Kibana)** : pour l'analyse temps réel et la recherche de motifs anormaux.

- **Graylog** : qui facilite la centralisation et l'analyse rapide des événements système.
- **Splunk** : une référence pour l'analyse avancée de journaux et la gestion de la sécurité dans les grandes entreprises.

III. Outils de gestion d'incidents et d'alertes

Ces outils déclenchent des notifications automatiques en cas d'événements critiques, tels que des interruptions de service, des pics de charge ou des activités suspectes. Leur rôle est essentiel pour garantir une intervention rapide des équipes techniques (Zhou et al., 2022).

On peut citer :

- **Prometheus** (souvent couplé à Grafana) : pour des alertes basées sur des métriques.
- **Opsgenie**, **PagerDuty** : pour l'orchestration des alertes et la coordination des équipes d'astreinte.
- **Centreon** : qui combine monitoring, gestion des seuils et alertes en temps réel.

IV. Outils de cartographie et de visualisation d'infrastructure

La visualisation des ressources est un élément clé dans la compréhension de l'état du réseau et des dépendances critiques. Ces outils fournissent des tableaux de bord dynamiques et des cartes interactives.

Solutions notables :

- **Grafana** : largement utilisé pour créer des visualisations personnalisées et dynamiques.
- **NetBox** : outil de gestion d'inventaire réseau et de modélisation topologique.

V. Solutions de monitoring intégrées dans le Cloud

Avec l'adoption croissante du cloud, les fournisseurs intègrent désormais des solutions de monitoring natives, capables de surveiller les performances applicatives, les coûts, et la disponibilité des ressources.

Parmi les offres les plus courantes :

- **AWS CloudWatch**
- **Azure Monitor**
- **Google Cloud Operations Suite**

Ces plateformes offrent en plus des fonctions d'auto-scaling, de prédiction de pannes et de gestion centralisée (Li et al., 2021).

VI. Plateformes de surveillance tout-en-un

Certaines solutions intègrent toutes les fonctions précédentes dans une même interface, facilitant ainsi la gestion opérationnelle et réduisant les coûts.

Par exemple :

- **Datadog** : qui réunit supervision, gestion des journaux, alertes et sécurité.
- **ManageEngine OpManager** : une solution complète pour la gestion des performances, de la bande passante, et des incidents.

L'utilisation conjointe de ces outils permet d'assurer une surveillance proactive, de réduire les temps d'arrêt et d'optimiser la gestion de l'infrastructure. Dans la section suivante, nous analyserons le rôle stratégique du monitoring dans la performance et la sécurité des systèmes.

Section 2 : Analyse des besoins en gestion du parc informatique de Kamoa SA

§1. Présentation de l'entreprise et de son infrastructure IT

1.1. Contexte général de l'entreprise Kamoa SA

Kamoa SA est une entreprise minière de grande envergure implantée dans la province du Lualaba, en République Démocratique du Congo. Acteur majeur du secteur extractif, elle joue un rôle stratégique dans l'exploitation et la transformation des ressources minières du pays. Son expansion rapide s'inscrit dans une dynamique de transformation numérique, où les technologies de l'information jouent un rôle central dans l'optimisation des opérations, la gestion des données sensibles, la communication interservices, et la continuité des services (Ngoma, 2020).

1.2. Composantes de l'infrastructure informatique

L'infrastructure informatique de Kamoa SA est à la fois complexe et évolutive. Elle repose sur un réseau local étendu (LAN)**,** reliant plusieurs sites : bureaux administratifs, centres de traitement des données, postes de travail, et dispositifs industriels. Ce réseau est structuré en VLANs (Virtual Local Area Networks), permettant de compartimenter le trafic selon les services (comptabilité, RH, production, etc.), afin de garantir la sécurité et la priorisation du flux de données (Willems, 2019).

La couche applicative est renforcée par l'implémentation de systèmes ERP pour la gestion intégrée des fonctions essentielles de l'entreprise, notamment les ressources humaines, la finance, la logistique et la maintenance des équipements. Des applications spécifiques au domaine minier sont également utilisées pour suivre les opérations d'extraction, de transport et de traitement du minerai (Sommerville, 2020).

1.3. Infrastructures matérielles et logicielles

Du point de vue matériel, Kamoa SA exploite un ensemble de serveurs physiques et virtuels sous VMware et Hyper-V, assurant des services critiques tels que l'authentification (AD), la gestion DNS/DHCP, les bases de données (SQL Server), les applications web internes, et le stockage de données. Ces ressources sont sécurisées via des pare-feu de nouvelle génération**,** des commutateurs de niveau 2/3 pour la segmentation du réseau, et des routeurs redondants pour assurer la tolérance aux pannes (Tanenbaum & Wetherall, 2019).

L'entreprise utilise également un système de sauvegarde automatique des données critiques, avec des stratégies de réplication et de restauration pour pallier les pertes potentielles. Sur le plan de la connectivité, Kamoa SA bénéficie d'un accès Internet haut débit fourni par plusieurs opérateurs privés, avec des liaisons redondantes pour maximiser la disponibilité (Ngoma, 2020).

1.4. Limites et nécessité d'un système de monitoring

Malgré une infrastructure robuste, l'entreprise fait face à des défis importants en matière de supervision**.** L'absence d'un système de monitoring unifié empêche une détection rapide et proactive des défaillances techniques, limite la visibilité sur les performances réseau**,** et accroît les risques de rupture de service. Or, dans un contexte industriel aussi critique, chaque minute d'indisponibilité peut engendrer des pertes considérables.

Dès lors, il devient impératif pour Kamoa SA d'adopter une solution de supervision centralisée**,** capable de collecter, analyser et corréler les événements système, d'automatiser les alertes, et de fournir aux administrateurs une vision temps réel de l'état du réseau et des infrastructures (Pico, 2021). Cette évolution s'inscrit dans la logique d'un pilotage intelligent des ressources IT, compatible avec les standards actuels en matière de performance et de sécurité.

§2. Problèmes rencontrés dans la gestion actuelle du parc informatique

1. Absence de surveillance proactive et automatisée

La gestion du parc informatique au sein de Kamoa SA souffre principalement d'un manque de supervision centralisée et proactive. En l'absence d'un système de monitoring automatisé, les incidents techniques qu'ils concernent les serveurs, les équipements réseaux ou les postes clients ne sont détectés qu'après leur survenue, souvent à travers les signalements des utilisateurs. Ce mode de gestion réactif provoque des interruptions de service non planifiées, avec un impact direct sur la productivité et la continuité des activités critiques. Selon Iteanu (2021), un système de surveillance automatisé est essentiel pour anticiper les anomalies, planifier les maintenances et éviter les interruptions inopinées dans les environnements informatiques complexes.

2. Manque d'inventaire dynamique et centralisé

La non-disponibilité d'un inventaire IT à jour et centralisé constitue un autre point de fragilité. Il est difficile de localiser précisément les ressources matérielles (PC, imprimantes, commutateurs, etc.) ou logicielles (licences, configurations, versions installées), car les informations sont souvent dispersées ou obsolètes. Cette lacune affecte aussi bien la gestion des stocks que la planification des remplacements ou des mises à niveau. Comme le souligne Kittlaus et Clough (2018), une gestion efficace des actifs informatiques passe par l'automatisation de l'inventaire et l'intégration des données dans une base unique pour améliorer la visibilité et la réactivité des équipes techniques.

3. Faiblesses dans la documentation et la traçabilité

Un autre problème majeur réside dans la documentation partielle ou inexistante des interventions techniques. Les procédures de maintenance, les configurations systèmes et les historiques d'incident ne sont pas systématiquement enregistrés, ce qui entrave la transmission des connaissances entre techniciens, ralentit les dépannages, et empêche toute analyse rétrospective pertinente. Une documentation structurée est pourtant cruciale dans la gestion de l'infrastructure IT, tant pour la formation interne que pour la capitalisation des expériences (Andry, 2019).

4. Absence d'alertes automatisées et d'indicateurs de performance

L'absence d'un système d'alerte en temps réel limite fortement la réactivité en cas d'incidents critiques, comme une coupure de service, une surcharge réseau ou une défaillance matérielle. De plus, l'impossibilité d'extraire des indicateurs de performance (KPI) fiables sur l'état du parc et la qualité du service freine les décisions stratégiques, notamment en matière de renforcement ou de modernisation des infrastructures. Comme le rappellent Schermann et al. (2014), les outils de monitoring doivent offrir non seulement des fonctionnalités d'alerte, mais aussi des tableaux de bord décisionnels pour orienter la gouvernance IT.

5. Conséquences sur la performance globale du SI

Ces différentes failles ont des répercussions concrètes sur la performance du système d'information de Kamoa SA. Les délais d'intervention s'allongent, les risques d'indisponibilité augmentent, et la confiance dans la fiabilité de l'infrastructure est altérée.

Cela compromet aussi les ambitions de transformation numérique de l'entreprise, qui nécessitent des fondations informatiques robustes et intelligemment supervisées (Ngoma, 2020).

§3. Besoins et attentes en matière de monitoring

Dans le contexte des lacunes identifiées dans la gestion du parc informatique, l'entreprise Kamoa SA exprime un besoin urgent de mettre en œuvre une solution de monitoring informatique moderne, capable d'assurer une supervision efficace, continue et intelligente de son infrastructure IT. Plusieurs exigences fonctionnelles et techniques émergent de cette nécessité.

1. Surveillance en temps réel et gestion proactive des incidents

Le premier besoin exprimé concerne **l'**instauration d'une surveillance en temps réel de tous les composants critiques du réseau : serveurs, routeurs, commutateurs, postes de travail, imprimantes, etc. Cette supervision doit inclure la remontée automatique des alertes en cas d'anomalie ou de seuil critique atteint. Ce changement de paradigme permettrait de **passer** d'une gestion curative à une gestion proactive**,** avec une capacité de réaction immédiate face aux incidents (Schermann, Buchwald & Krcmar, 2014). De telles pratiques sont désormais considérées comme fondamentales pour maintenir la disponibilité continue des services informatiques.

2. Centralisation de la visualisation et des données de performance

La centralisation des données collectées constitue un second axe prioritaire. La solution de monitoring devra intégrer une interface graphique permettant une visualisation claire, en temps réel et synthétique de l'état du système d'information. Cette interface, souvent matérialisée sous forme de tableaux de bord dynamiques, aidera les équipes techniques à diagnostiquer rapidement les anomalies et à planifier les interventions préventives. Comme le mentionnent Kittlaus et Clough (2018), l'ergonomie et l'accessibilité des outils de supervision influencent directement l'efficacité opérationnelle des équipes IT.

3. Reporting automatisé et suivi des indicateurs clés

Un autre besoin fondamental est la capacité à générer automatiquement des rapports techniques exploitables tant pour l'analyse interne que pour la reddition de comptes auprès de la direction ou des partenaires. Ces rapports devront inclure des métriques clés : disponibilité des systèmes, taux d'utilisation des ressources, temps de réponse, taux d'erreur, sécurité, etc. L'automatisation de ce reporting est essentielle pour soutenir les décisions stratégiques et documenter les évolutions de la performance du parc informatique (Iteanu, 2021).

4. Accessibilité multiplateforme et supervision à distance

L'entreprise souhaite également que la plateforme de monitoring soit accessible depuis plusieurs terminaux, y compris les smartphones, les tablettes et les postes distants, pour permettre aux responsables IT de maintenir une supervision continue, même en déplacement. Cette flexibilité opérationnelle est désormais courante dans les environnements distribués et hybrides. Pour cela, l'outil devra être compatible avec les normes modernes d'accès mobile sécurisé (Andry, 2019).

5. Sécurisation et contrôle des accès

La protection des informations collectées par la solution de monitoring est une priorité non négligeable. L'entreprise attend une intégration native de mécanismes de sécurité robustes, notamment l'authentification multi-facteurs**,** la segmentation des droits d'accès, la journalisation des connexions, ainsi que le chiffrement des communications. La gouvernance IT moderne repose sur une surveillance rigoureuse des accès et la minimisation des privilèges, comme l'exigent les bonnes pratiques en matière de cybersécurité (Ngoma, 2020).

6. Évolutivité et intégration de technologies intelligentes

Enfin, la solution choisie devra être évolutive et capable d'intégrer progressivement des technologies avancées, telles que **l'**intelligence artificielle (IA) et l'apprentissage automatique, dans le but de développer une analyse prédictive des pannes et d'automatiser certaines tâches de gestion, comme le redémarrage de services ou la redistribution de la charge réseau. D'après Schermann et al. (2014), l'automatisation intelligente du monitoring constitue un levier de performance incontournable dans les infrastructures informatiques modernes.

CHAPITRE II : CONCEPTION DE L'APPLICATION DE MONITORING

Dans ce chapitre, il sera question de présenter les différents aspects liés à la conception de l'application de monitoring développée dans le cadre de notre étude. La première section sera consacrée à l'architecture et aux fonctionnalités de l'application. Il y sera abordé successivement le choix des technologies et des outils de développement, les modules fonctionnels intégrés à l'outil, ainsi que les dispositifs mis en place pour garantir la sécurité et l'accessibilité du système.

Dans la deuxième section, nous traiterons de la modélisation et de la mise en œuvre technique de l'application. Cette partie comprendra l'élaboration des diagrammes UML permettant de représenter les différentes interactions et structures de l'outil, le développement proprement dit des fonctionnalités essentielles, et enfin les tests réalisés pour valider la fiabilité et la performance de l'application conçue.

Section 1 : Architecture et fonctionnalités de l'application

§1. Choix des technologies et outils de développement

Le choix des technologies et des outils de développement constitue une étape stratégique dans le processus de conception d'une application, notamment lorsqu'il s'agit d'un système de monitoring pour une entreprise telle que Kamoa SA. Ce choix repose sur divers paramètres : les objectifs fonctionnels, les contraintes techniques, le budget disponible, les compétences des développeurs, ainsi que la capacité d'évolution attendue du système (Goncalves, 2019).

1.1. Technologies retenues pour le backend

Dans le développement du système de surveillance, le langage **Python** a été privilégié pour la couche backend. Ce choix s'explique par sa flexibilité, la richesse de ses bibliothèques dédiées au traitement des données (telles que *Pandas* et *NumPy*), ainsi que la robustesse de ses frameworks pour la création d'API RESTful comme *Flask* et *Django* (Martelli et Ascher, 2017). Ces outils facilitent l'implémentation de modules capables de collecter, traiter et transmettre efficacement les informations issues du réseau de l'entreprise.

1.2. Technologies utilisées pour le frontend

Pour l'interface utilisateur, le framework **React.js** a été retenu en raison de sa modularité, de sa légèreté et de sa capacité à générer des interfaces dynamiques. Sa structure fondée sur les composants facilite la maintenance et l'adaptabilité du système aux besoins futurs. L'intégration de bibliothèques comme **Tailwind CSS** a également permis de garantir une présentation harmonieuse et responsive de l'application, ce qui améliore l'expérience utilisateur (Wieruch, 2021).

1.3. Base de données et gestion des données

Du côté des données, le choix s'est porté sur **PostgreSQL**, une base relationnelle reconnue pour sa stabilité, sa conformité aux règles **ACID**, et sa capacité à gérer des volumes importants d'informations structurées. PostgreSQL permet, grâce à ses fonctionnalités avancées (indexation, transactions, procédures stockées), une gestion efficace des flux de données critiques pour le monitoring en temps réel (Douglas & Douglas, 2020).

1.4. Outils de monitoring et visualisation

Pour assurer la collecte et l'analyse des métriques de performance, l'outil **Prometheus** a été intégré. Il s'agit d'un système de surveillance open source capable de collecter périodiquement des données sous forme de séries temporelles, consultables via un langage de requête dédié (*PromQL*) (Turnbull, 2018). Les données issues de Prometheus sont ensuite visualisées via **Grafana**, qui propose des tableaux de bord interactifs et personnalisables. Cette combinaison facilite la prise de décision en temps réel par les administrateurs du réseau.

1.5. Intégration et interopérabilité des composants

L'interconnexion entre les différentes couches du système repose sur l'usage d'API RESTful**,** qui permettent une communication standardisée entre les composants backend, frontend et les outils de surveillance. Cette approche garantit la modularité et l'évolutivité de l'application. Elle offre également la possibilité d'intégrer ultérieurement des modules d'intelligence artificielle pour la détection prédictive des pannes, ou encore des systèmes de notification automatisée (Tan, 2021).

1.6. Outils de collaboration et de gestion du code

Enfin, le développement collaboratif a été structuré à travers l'utilisation de Git et de la plateforme GitHub**.** Cette organisation permet un suivi rigoureux des versions, une gestion fluide du code en équipe, et la mise en œuvre de pipelines d'intégration continue à travers des outils tels que GitHub Actions**.** Ces outils contribuent à l'automatisation des tests, des déploiements et des mises à jour, garantissant ainsi la qualité logicielle et la résilience du système final (Loeliger & McCullough, 2012).

§2. Modules et fonctionnalités de l'application

L'application de monitoring mise en œuvre dans le cadre de ce travail repose sur une architecture modulaire conçue pour assurer une gestion complète, efficace et proactive du parc informatique de l'entreprise Kamoa SA. Chaque module a été élaboré pour répondre à une problématique précise de la supervision informatique et permettre à l'administrateur système d'interagir avec l'environnement IT à plusieurs niveaux d'intervention.

Le Module de supervision des équipements est l'un des noyaux centraux de l'application. Il a pour rôle d'assurer la surveillance en temps réel des équipements connectés au réseau de l'entreprise.[1] Cela inclut les serveurs, postes de travail, imprimantes réseau, routeurs, commutateurs et autres périphériques critiques. Ce module permet de consulter en temps réel les indicateurs clés de performance (CPU, mémoire, espace disque, etc.) et d'identifier immédiatement tout dysfonctionnement ou surconsommation anormale de ressources.

Le Module d'alertes et de notifications vient compléter le dispositif de supervision en automatisant les signaux d'alerte dès qu'un seuil critique est atteint. Ces notifications sont personnalisables selon la nature de l'incident et peuvent être transmises par courriel, SMS ou intégration à des messageries professionnelles comme Slack ou Microsoft Teams. Ce mécanisme garantit une réactivité maximale face aux événements susceptibles d'altérer la disponibilité du système.

Un Module de reporting et de génération de rapports permet aux responsables IT de générer automatiquement des rapports périodiques sur l'état du parc informatique. Ces rapports peuvent porter sur l'usage des ressources, la disponibilité des services, l'historique

[1] DURAND, Michel. Supervision des infrastructures informatiques : principes, outils et bonnes pratiques. Paris : Éditions ENI, 2018, p. 98.

des incidents ou les performances du réseau. Ils servent également de support de communication avec la direction de l'entreprise et permettent un suivi régulier des actions correctives entreprises.

Le Module de gestion des utilisateurs et des accès permet de définir différents profils d'utilisateurs au sein de l'application. L'administrateur principal peut attribuer à chaque collaborateur des droits spécifiques en fonction de son rôle : consultation des données, configuration du monitoring, gestion des alertes, etc. Ce module contribue à une meilleure organisation du travail et évite les risques liés à des manipulations non autorisées.

Un Module de maintenance et d'optimisation est également intégré. Il permet de planifier les interventions techniques de maintenance (mises à jour logicielles, remplacement de matériels, redémarrage des équipements critiques), et de conserver une trace documentaire des opérations réalisées. Ce module participe à la traçabilité et à la pérennisation du système de supervision.

Enfin, l'application propose un Module d'interface graphique ergonomique, facilitant la navigation dans l'ensemble des données collectées. Ce tableau de bord est personnalisable et peut afficher en temps réel des graphiques dynamiques sur l'état des ressources, les niveaux de service ou les incidents récents.

§3. Sécurité et accessibilité de l'application

La sécurité et l'accessibilité de l'application de monitoring sont deux piliers essentiels dans sa conception. Ces dimensions ne sont pas accessoires, mais fondamentales dans un contexte professionnel comme celui de Kamoa SA, où la confidentialité, la disponibilité et l'intégrité des données représentent des exigences critiques pour la continuité des activités et la résilience du système d'information.

3.1 Sécurisation des accès utilisateurs

Le contrôle d'accès à l'application repose sur une authentification forte, qui utilise un couple identifiant/mot de passe chiffré et peut être renforcé par une authentification multi-facteurs (MFA)**.** Ce dispositif permet de prévenir les accès non autorisés, même si des identifiants venaient à être compromis (Scarfone & Souppaya, 2019). Afin de limiter les

risques liés à l'usurpation de session, la durée d'inactivité tolérée est limitée, au terme de laquelle une déconnexion automatique est déclenchée.

3.2 Protection des communications et des échanges

Les échanges entre les clients (navigateurs) et les serveurs sont protégés par un chiffrement HTTPS basé sur TLS 1.3**,** garantissant ainsi la confidentialité des informations transitant par le réseau (Rescorla, 2018). Par ailleurs, un pare-feu applicatif (WAF) est configuré pour intercepter les requêtes malveillantes et bloquer les attaques courantes telles que les injections SQL, les scripts intersites **(**XSS**)** et les falsifications de requêtes **(**CSRF**).** Ces contre-mesures sont indispensables pour sécuriser les interfaces ouvertes à l'extérieur.

3.3 Traçabilité et journalisation des activités

La mise en œuvre d'un système de logs détaillés permet à l'administrateur de suivre en temps réel les actions effectuées sur l'application. Ces journaux, horodatés et classés par type d'événement, peuvent être exportés vers une solution de SIEM (Security Information and Event Management) pour analyse avancée (Kent & Souppaya, 2006). Cela facilite la détection précoce d'activités suspectes et l'identification des vecteurs d'attaque en cas d'incident.

3.4 Accessibilité et supervision distante

Du point de vue de l'accessibilité, l'application est conçue comme une solution Web responsive, accessible via un navigateur Internet depuis n'importe quel terminal connecté. Cela favorise une supervision en temps réel à distance, utile pour les équipes en télétravail ou en déplacement (Open Web Application Security Project, 2022). L'interface, adaptée aux écrans de tailles variées (PC, smartphones, tablettes), facilite une prise en main rapide même pour les utilisateurs moins technophiles.

3.5 Continuité de service et sauvegardes automatiques

La tolérance aux pannes est assurée par des systèmes de sauvegarde automatisés. Des copies de sécurité des données et des configurations sont générées à intervalles réguliers, puis stockées sur un serveur de secours distant. En cas de défaillance du système principal (attaque, panne matérielle, erreur humaine), ces sauvegardes permettent une restauration

rapide de l'environnement de production, contribuant ainsi à la continuité opérationnelle (NIST, 2010).

3.6 Alignement sur les standards de cybersécurité

L'ensemble de ces mécanismes vise à aligner l'architecture de l'application sur les meilleures pratiques internationales en matière de cybersécurité et de gestion de la disponibilité. Il s'agit notamment de respecter les recommandations du NIST sur la sécurisation des applications Web et des systèmes d'information critiques, tout en assurant une expérience utilisateur fluide et sécurisée pour les administrateurs et les agents terrain (NIST SP 800-53, 2020).

Section 2 : Modélisation et mise en œuvre

§1. Diagrammes UML : cas d'utilisation, séquence et classes

La modélisation UML (Unified Modeling Language) constitue une étape essentielle dans le processus de développement logiciel. Elle permet de représenter de manière formelle les exigences fonctionnelles, les interactions dynamiques ainsi que la structure statique du système à concevoir. L'approche UML facilite la compréhension partagée entre analystes, développeurs et utilisateurs finaux, tout en réduisant les risques de mauvaise interprétation (Booch, Rumbaugh & Jacobson, 2005).

1.1. Diagramme de cas d'utilisation : visualiser les rôles et les fonctionnalités

Le diagramme de cas d'utilisation sert à identifier les acteurs et les interactions qu'ils entretiennent avec le système. Chaque acteur est lié à un ou plusieurs "cas d'usage", représentant les fonctionnalités principales que le système doit offrir (Fowler, 2004).

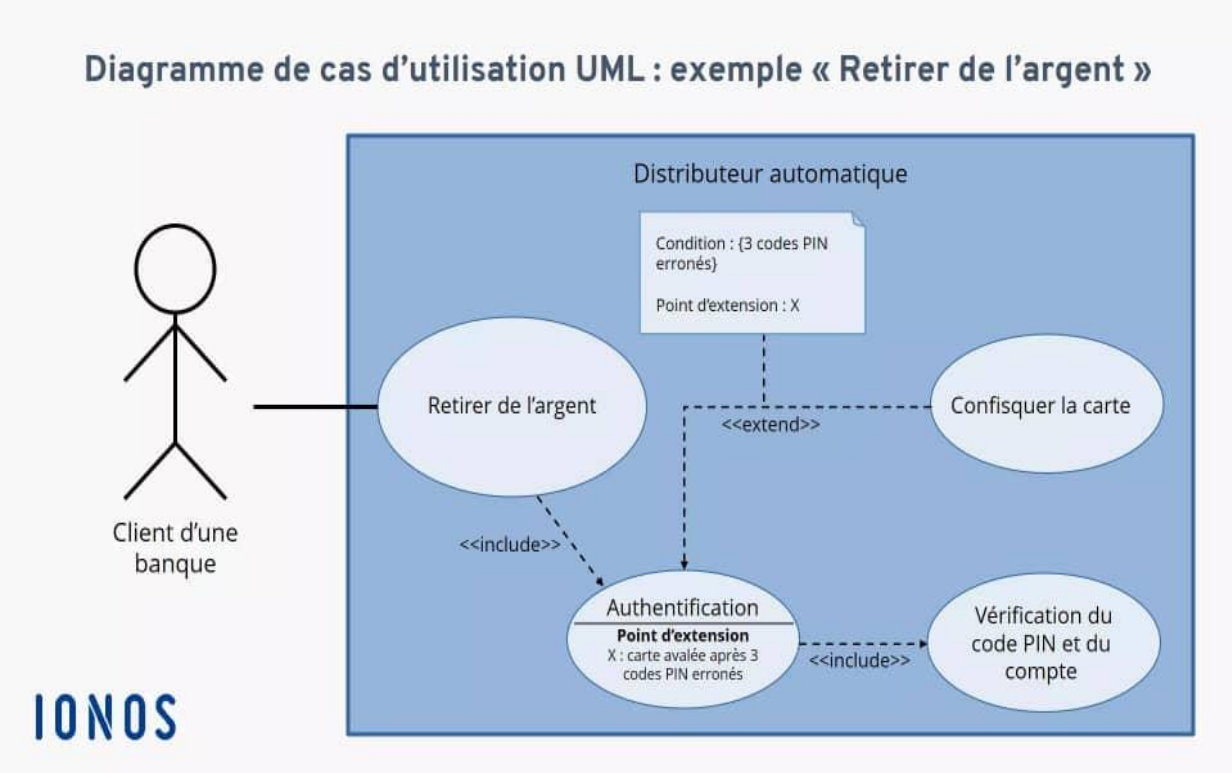
Dans le contexte de l'application de monitoring développée pour le parc informatique de l'entreprise Kamoa SA, les acteurs identifiés sont :

- L'**administrateur système**, chargé de la gestion des comptes, du paramétrage des alertes et de la consultation des rapports ;
- Le **technicien réseau**, responsable du diagnostic et du suivi des équipements ;

- Les **utilisateurs autorisés**, qui peuvent visualiser l'état du réseau ou recevoir des notifications critiques.

Parmi les cas d'usage modélisés figurent : *consulter un rapport d'activité, configurer des seuils d'alerte, générer un rapport journalier, ou encore gérer les sessions utilisateurs* (Larman, 2004).

Figure 2.1 – Diagramme de cas d'utilisation de l'application de monitoring : interactions entre les acteurs (administrateur système, technicien réseau, utilisateur autorisé) et les fonctionnalités principales (consultation de rapports, configuration des alertes, gestion des sessions, etc.).

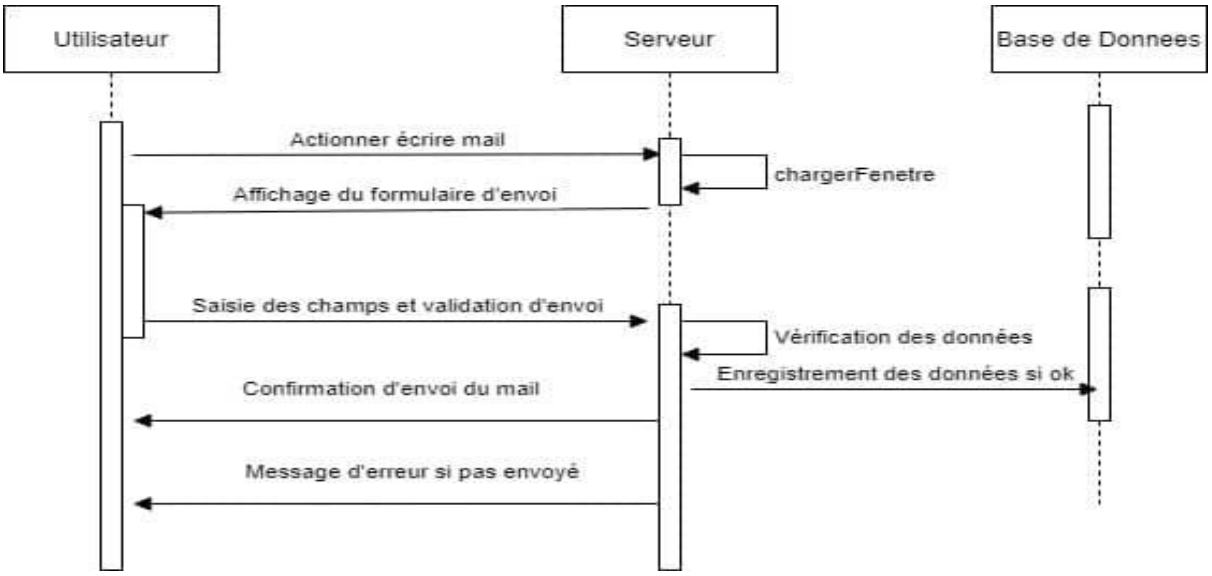


1.2. Diagramme de séquence : modéliser les échanges temporels entre composants

Le diagramme de séquence permet de modéliser les interactions temporelles entre objets ou composants du système pour un scénario spécifique. Il décrit l'ordre chronologique des messages, leur synchronisation, et le rôle de chaque objet dans l'exécution du traitement (Douglass, 2004).

Prenons l'exemple d'un processus de notification d'alerte : lorsqu'un équipement dépasse un seuil critique, l'agent de supervision envoie une alerte au serveur, qui la relaye à l'utilisateur concerné par messagerie. Ce type de séquence est représenté par une série de messages synchrones et asynchrones entre entités, permettant de visualiser la logique métier complète (Arlow & Neustadt, 2005).

Figure 2.2 – Diagramme de séquence illustrant le processus de notification d'alerte : interactions temporelles entre l'agent de supervision, le serveur, la base de données et l'utilisateur pour déclencher et transmettre une alerte en cas de seuil critique atteint.



1.3. Diagramme de classes : structuration du modèle de données

Le diagramme de classes est utilisé pour représenter la structure statique du système, incluant les classes, leurs attributs, méthodes et les relations entre elles (Booch et al., 2005). Ce diagramme est crucial pour concevoir l'architecture du code orienté objet et garantir une cohérence dans l'organisation des entités.

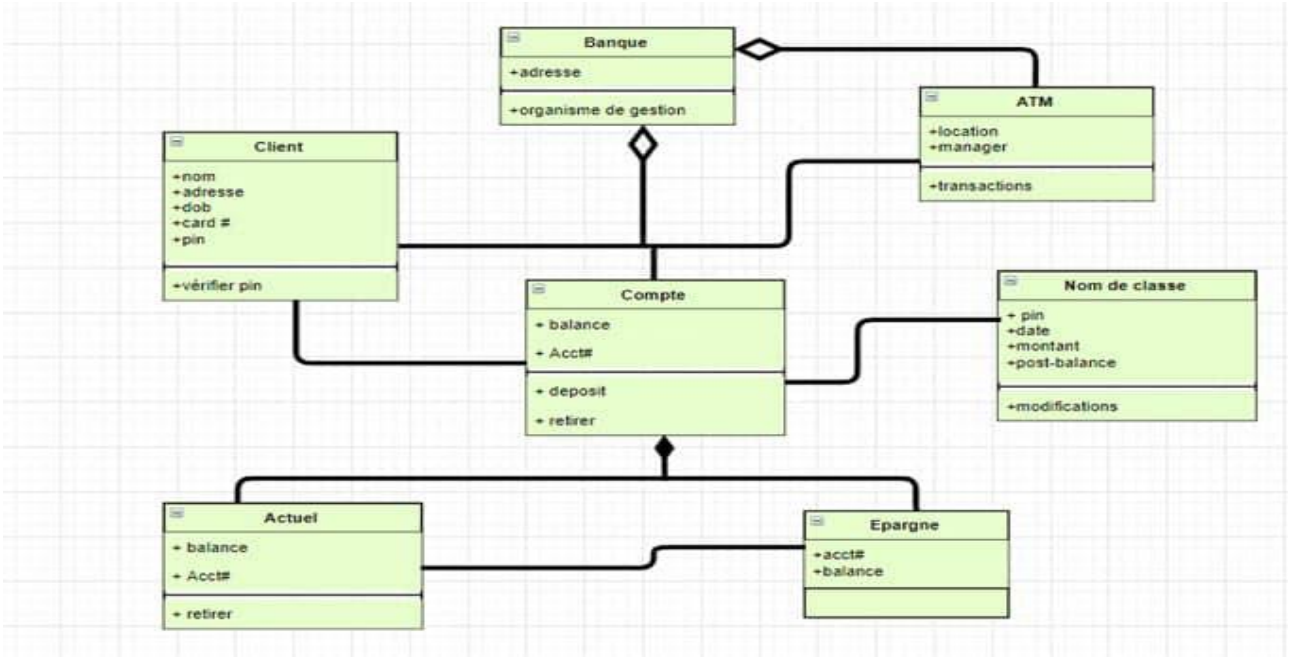
Dans notre application, on identifie les classes suivantes :

- **Utilisateur** : avec les attributs *nom, mot de passe, rôle* et les méthodes *se connecter, se déconnecter* ;

- **Équipement** : avec *adresse IP, type d'équipement, statut réseau* et les méthodes *envoyer_état(), redémarrer()* ;
- **Alerte** : contenant *type, gravité, date de génération* et les méthodes *déclencher_alerte(), archiver()*.

Ces classes interagissent selon des relations d'association et d'héritage, permettant de construire un modèle extensible et maintenable (Larman, 2004 ; Arlow & Neustadt, 2005).

Figure 2.3 – Diagramme de classes de l'application de monitoring : structure des entités principales (Utilisateur, Équipement, Alerte) et leurs relations (attributs, méthodes, associations).



En résumé, l'intégration des diagrammes de cas d'utilisation, de séquence**,** et de classes dans le processus de conception permet une compréhension précise des rôles, du déroulement des traitements, et de la structure de l'application**.** Ces modèles jouent un rôle déterminant dans la réduction des ambiguïtés fonctionnelles et facilitent le passage vers la phase de codage (Fowler, 2004 ; Booch et al., 2005).

§2. Développement et implémentation des principales fonctionnalités

Le développement et l'implémentation des fonctionnalités principales de l'application de monitoring de l'infrastructure informatique de Kamoa SA se sont inscrits dans une approche itérative et incrémentale, en ligne avec les pratiques recommandées en génie logiciel

agile (Sommerville, 2016). Cette méthode a permis une validation progressive des modules développés, tout en assurant une adaptation continue aux exigences opérationnelles et techniques de l'entreprise.

2.1. Collecte automatisée des données en temps réel

La première phase du développement a visé à mettre en place un mécanisme robuste de collecte automatique des données via des agents logiciels installés sur les nœuds critiques du réseau, notamment les serveurs et routeurs. Ces agents, développés en Python, interagissent directement avec les systèmes d'exploitation pour extraire des métriques essentielles telles que l'utilisation du processeur, l'occupation mémoire, le trafic réseau, la température des équipements ou encore la disponibilité des services (Beazley & Jones, 2013).

Les données récupérées sont ensuite transmises à un système de gestion de base de données relationnelle (SGBDR), en l'occurrence PostgreSQL, choisi pour sa stabilité, sa robustesse en environnement transactionnel, et sa capacité à traiter de gros volumes de données en temps réel (Momjian, 2015). Cette architecture garantit la persistance**,** l'intégrité et la cohérence des informations collectées, facilitant leur exploitation ultérieure pour l'analyse.

2.2. Visualisation via une interface web interactive

La deuxième étape a consisté à concevoir une interface web ergonomique et sécurisée, permettant une exploitation intuitive des données. Le développement s'est appuyé sur Laravel pour le back-end, reconnu pour sa gestion efficace des routes, des contrôleurs et de l'authentification, et sur Vue.js pour le front-end, afin de bénéficier d'un rendu dynamique et réactif des tableaux de bord (Holmes, 2021 ; You, 2022).

Grâce à cette interface, les administrateurs peuvent consulter l'état du réseau sous forme de graphiques dynamiques**,** histogrammes et tableaux personnalisés. Chaque utilisateur connecté dispose d'un espace personnalisé, structuré selon son profil d'accès, ce qui permet une adaptation précise aux rôles (utilisateur, technicien, administrateur). Ce modèle améliore significativement l'expérience utilisateur tout en renforçant l'efficience dans la prise de décisions techniques (Kruchten, 2004).

2.3. Module intelligent d'alerte automatique

Un composant fondamental de l'application est le module d'alertes automati**sées**. Il repose sur une configuration fine de seuils critiques et de règles de surveillance. Lorsqu'un indicateur dépasse les limites définies, le système déclenche automatiquement des notifications par e-mail ou SMS à destination des équipes techniques, assurant ainsi une réactivité accrue en cas de panne ou d'incident réseau (Scarfone & Mell, 2007).

Ce mécanisme, intégré au cœur du système, permet de minimiser les temps d'indisponibilité et d'optimiser la maintenance préventive des équipements critiques. L'usage de protocoles sécurisés pour l'envoi des alertes, tels que SMTP avec chiffrement TLS ou l'intégration à des API SMS tierces, contribue par ailleurs à garantir la fiabilité des transmissions**.**

2.4. Gestion des utilisateurs et sécurité des accès

La dernière phase du développement s'est concentrée sur la gestion des utilisateurs et des droits d'accès. L'application implémente une authentification forte**,** reposant sur un mécanisme d'identifiant/mot de passe renforcé par des jetons de session sécurisés. Ce système est combiné à une gestion des rôles et permissions, qui définit avec précision les actions autorisées à chaque profil utilisateur (Ferraiolo, Kuhn & Chandramouli, 2007).

Ce modèle de contrôle d'accès basé sur les rôles (RBA**C**) assure une protection contre les accès non autorisés et une traçabilité complèt**e** des interactions. L'ensemble du code source du projet est versionné avec Git**,** un outil de gestion de versions qui facilite la collaboration entre développeurs et permet de conserver un historique détaillé de toutes les évolutions fonctionnelles (Loeliger & McCullough, 2012).

Le développement de l'application s'est articulé autour de principes méthodologiques rigoureux**,** d'une technologie éprouvée**,** et d'une implémentation progressive des modules clés. Chaque brique fonctionnelle collecte de données, visualisation, alertes et gestion des utilisateurs a été conçue pour répondre aux exigences de performance, de fiabilité et de sécurité de Kamoa SA. L'architecture modulaire retenue facilite la scalabilité du système et son adaptation future à de nouveaux besoins.

§3. Tests et validation des performances

La validation d'une application de monitoring ne saurait être complète sans une phase rigoureuse de tests permettant de garantir sa stabilité, sa performance et sa fiabilité en condition réelle d'exploitation (Myers, Sandler & Badgett, 2011). Dans le cas de l'outil conçu pour Kamoa SA, ces tests ont été menés dans un environnement simulé, reproduisant les contraintes du réseau de production de l'entreprise, selon une méthodologie structurée intégrant différentes typologies de vérification.

3.1. Tests unitaires

Les tests unitaires ont constitué la première couche de validation. Ils ont visé à vérifier individuellement chaque fonction logicielle, en s'assurant qu'elle produise le résultat attendu pour des cas d'entrée spécifiques. L'automatisation de ces tests via les frameworks PHPUnit (pour le backend Laravel) et Jest (pour le frontend Vue.js) a permis de garantir une bonne couverture du code dès les premiers cycles de développement. Cette approche préventive est recommandée pour limiter l'accumulation de dettes techniques (Meszaros, 2007).

3.2. Tests d'intégration

Une fois les modules validés isolément, leur interaction a été testée via des scénarios d'intégration. L'objectif ici était de contrôler la fluidité et la cohérence des échanges entre les agents de collecte, le backend et l'interface graphique. Ce processus a permis d'identifier plusieurs défauts liés à la synchronisation des données, notamment lors de la réception simultanée de métriques issues de multiples sources. Ces dysfonctionnements ont été corrigés avant le passage à l'étape suivante.

3.3. Tests fonctionnels

Les tests fonctionnels ont quant à eux consisté à valider que chaque fonctionnalité remplisse bien les exigences du cahier des charges. Des scénarios d'utilisation concrets ont été exécutés, portant notamment sur la création et l'envoi d'alertes automatiques, la visualisation des données, la gestion des profils utilisateurs ou encore l'exportation de rapports. Cette méthode basée sur l'approche boîte noire est couramment utilisée pour évaluer la conformité d'un logiciel par rapport aux besoins exprimés (Kaner, Falk & Nguyen, 1999).

3.4. Tests de performance et de charge

Pour anticiper les exigences futures en matière de scalabilité, des tests de performance ont été menés à l'aide de l'outil Apache JMeter**.** Ceux-ci ont simulé des accès simultanés de plus de 200 utilisateurs, représentant largement les pics de charge prévus pour l'exploitation réelle. L'application a maintenu un temps de réponse stable et des performances satisfaisantes, témoignant de l'efficacité de l'architecture technique retenue (Pérez-Castillo et al., 2018).

3.5. Tests de sécurité

Enfin, la dimension sécuritaire n'a pas été négligée. Des audits automatisés ont été réalisés avec OWASP ZAP**,** afin de détecter les vulnérabilités potentielles, notamment les injections SQL, les attaques XSS (cross-site scripting) ou CSRF (cross-site request forgery). La correction immédiate des failles identifiées a renforcé la robustesse globale de l'outil, en conformité avec les bonnes pratiques en matière de développement sécurisé (OWASP Foundation, 2021).

3.6. Mise en production restreinte

Pour conclure cette phase, une mise en production restreinte a été effectuée auprès d'un groupe pilote d'utilisateurs internes à Kamoa SA. Leurs retours qualitatifs ont été précieux : ils ont permis d'ajuster certains paramètres d'affichage, d'optimiser les temps de chargement et de confirmer l'utilisabilité générale du système. Cette validation terrain a ainsi constitué la dernière étape avant le déploiement complet de l'outil sur l'ensemble de l'infrastructure.

CHAPITRE III : DÉPLOIEMENT ET OPTIMISATION DE L'APPLICATION

Dans ce chapitre, il sera question de mettre l'accent sur le processus de mise en production de l'application développée (section I), en abordant successivement la stratégie de déploiement au sein de l'entreprise Kamoa SA, les efforts de formation des utilisateurs ainsi que la documentation technique, sans négliger les mécanismes de maintenance et les perspectives d'évolutivité du système. Ensuite, l'on parlera de l'évaluation des performances de l'application et des différentes stratégies d'amélioration continue mises en œuvre (section II), notamment à travers l'analyse des retours des utilisateurs, l'optimisation des performances techniques et de la sécurité, ainsi que les perspectives d'intégration de technologies émergentes comme l'intelligence artificielle.

Section 1 : Intégration et mise en production

§1. Stratégie de déploiement au sein de Kamoa SA

Le déploiement d'une application de monitoring au sein d'une entreprise comme Kamoa SA constitue une étape stratégique cruciale. Elle conditionne la réussite de l'intégration du système dans l'environnement existant, tout en assurant sa stabilité et sa compatibilité avec les infrastructures informatiques de l'entreprise. Une stratégie rigoureuse et bien planifiée a donc été conçue pour garantir une transition fluide entre le développement et la mise en production.

1.1. Analyse de l'environnement technique

La première étape de cette stratégie a consisté en une analyse approfondie de l'environnement technique de Kamoa SA. Cette entreprise minière dispose d'une infrastructure IT hétérogène : serveurs locaux, équipements de commutation, postes clients dans divers départements, et plusieurs applications métier déjà en production. Cette cartographie a permis d'identifier les dépendances logicielles et les contraintes techniques**,** d'anticiper les incompatibilités potentielles et de planifier la mobilisation des ressources humaines et matérielles. Une analyse préalable de ce type est recommandée dans les bonnes pratiques de déploiement de solutions de supervision (Hasselbring & Reussner, 2020).

1.2. Approche progressive par environnement de pré-production

La stratégie adoptée a privilégié une approche progressive**,** en deux phases : une phase de pré-production, suivie d'une phase de production réelle. L'environnement de test a simulé les conditions d'exploitation, ce qui a permis aux équipes de corriger les bogues, valider les fonctionnalités critiques, et affiner les paramètres de l'application. Cette méthode incrémentale est conforme aux modèles DevOps recommandés par l'ITIL v4 (Axelos, 2019).

1.3. Sécurisation du processus de déploiement

Une attention particulière a été portée à la sécurité du processus de déploiemen**t**, étant donné que l'application accède à des données sensibles. Ainsi, des canaux de communication chiffrés ont été mis en place, un système d'authentification multi-facteurs a été intégré pour les profils administrateurs, et les accès ont été cloisonnés selon les rôles des utilisateurs. Ces mesures de sécurité respectent les recommandations de l'OWASP pour les applications critiques (OWASP, 2023).

1.4. Gestion des interruptions de service

Dans une entreprise comme Kamoa SA, où l'activité dépend fortement de la disponibilité des systèmes, il a été impératif de minimiser les interruptions de service**.** Le déploiement a donc été effectué durant les périodes de faible activité, avec un mécanisme de basculement (rollback) prêt à l'emploi. Cette approche de continuité opérationnelle est cohérente avec les standards ISO/IEC 22301 relatifs à la résilience des activités informatiques (ISO, 2019).

1.5. Supervision post-déploiement et indicateurs clés

Une fois le système en production, un suivi post-déploiement a été mis en place. Des indicateurs clés de performance (KPI) ont été définis : temps de réponse, fréquence des alertes, consommation des ressources, taux d'adoption. Ces données ont été centralisées pour évaluer l'efficacité du système et procéder à des ajustements. Cette phase de monitoring initiale s'inspire des recommandations de performance applicative formulées par Scarfone et Mell (2007).

1.6. Une stratégie évolutive et agile

Enfin, la stratégie n'a pas été conçue comme un document figé. Elle s'appuie sur une démarche agile et itérative, permettant de réajuster les priorités en fonction des retours utilisateurs, des incidents observés et des nouvelles fonctionnalités souhaitées. L'agilité dans le déploiement garantit une adéquation continue entre les besoins réels de Kamoa SA et les capacités de l'outil de monitoring (Fitzgerald & Stol, 2017).

En somme, la stratégie de déploiement mise en œuvre au sein de Kamoa SA a posé les bases d'une intégration réussie de l'application de monitoring, avec une gestion rigoureuse des risques techniques et organisationnels. Elle renforce également la résilience de l'infrastructure IT de l'entreprise, en optimisant la visibilité sur les performances, la détection proactive des incidents, et l'amélioration continue des processus numériques.

§2. Formation des utilisateurs et documentation technique

La réussite du déploiement d'une application de monitoring repose non seulement sur sa conception technique, mais également sur l'adhésion des utilisateurs et la qualité de la documentation qui les accompagne. À ce titre, la formation des utilisateurs finaux constitue une étape cruciale pour assurer une exploitation optimale du système et prévenir les erreurs ou la mauvaise utilisation des fonctionnalités mises à leur disposition (Cisco, 2021). Chez Kamoa SA, cette exigence est d'autant plus fondamentale que l'environnement de travail est marqué par la diversité des profils, allant des techniciens informatiques aux utilisateurs non spécialisés, ce qui nécessite une approche pédagogique différenciée (Knapp, 2017).

§2.1 Formation des utilisateurs

La stratégie de formation a été pensée pour couvrir plusieurs niveaux d'apprentissage. Elle commence par une sensibilisation générale sur l'importance du monitoring informatique dans la gestion quotidienne du parc, suivie de sessions pratiques orientées sur les modules essentiels à l'usage courant. Les utilisateurs ont été classés en groupes selon leurs responsabilités : un groupe chargé de l'administration et de la configuration de l'outil, un autre dédié à la consultation des tableaux de bord et à la lecture des alertes, et enfin un dernier constitué d'intervenants occasionnels pour qui seule une initiation sommaire a été dispensée. Ce découpage a permis d'adapter le contenu de la formation aux besoins réels de chaque

catégorie, optimisant ainsi la compréhension et l'appropriation des fonctionnalités du système (Limoncelli et al., 2016).

Les supports utilisés dans le cadre de cette formation ont été conçus dans un souci d'accessibilité. Des manuels imprimés, des tutoriels vidéo, ainsi que des fiches de procédures pas à pas ont été distribués et rendus accessibles sur le réseau interne de l'entreprise. En complément, un portail documentaire numérique a été mis en place, regroupant l'ensemble des ressources utiles, telles que les guides d'utilisation, les procédures de dépannage de premier niveau, les mises à jour logicielles, ainsi que les réponses aux questions fréquentes (FAQ). Ce portail est structuré selon une arborescence claire et doté d'un moteur de recherche facilitant la navigation. Il constitue une ressource de référence permanente pour tous les utilisateurs et participe activement à l'autonomie progressive du personnel dans l'exploitation du système (Red Hat, 2020).

Pour renforcer cette démarche documentaire, des sessions de recyclage périodiques ont été planifiées, notamment à la suite des mises à jour majeures de l'application. L'objectif est de maintenir un bon niveau de compétence au sein des équipes et d'éviter toute obsolescence des connaissances face à l'évolution des outils (Microsoft, 2022). Cette formation continue est également l'occasion de recueillir des retours terrain, utiles pour ajuster le contenu pédagogique, mettre à jour les manuels, ou corriger certains éléments qui auraient été mal interprétés. Par ailleurs, les encadrants techniques et les administrateurs du système ont bénéficié d'une formation avancée sur les aspects de paramétrage, de sécurité et de dépannage, afin qu'ils puissent non seulement superviser les utilisateurs, mais aussi intervenir rapidement en cas d'incident (Knapp, 2017).

§2.2 Documentation technique

La documentation technique, pour sa part, est un élément structurant du projet. Elle comprend une description détaillée de l'architecture de l'application, les prérequis système, les configurations recommandées, les procédures d'installation et de déploiement, les diagrammes de flux, ainsi que les consignes de sauvegarde et de restauration. Elle constitue une base essentielle pour assurer la maintenabilité du système dans le temps et faciliter la montée en compétence des nouveaux arrivants au sein de l'équipe IT (Limoncelli et al., 2016). Elle a été rédigée dans un langage clair, structuré, et est accompagnée d'annexes

illustratives permettant une meilleure compréhension des mécanismes internes de l'application.

Enfin, il faut souligner que cette démarche de formation et de documentation ne se limite pas à une exigence de conformité technique. Elle relève d'une véritable volonté stratégique d'impliquer les utilisateurs dans la vie du système, de créer un climat de confiance autour de l'outil, et de renforcer la culture technologique au sein de Kamoa SA**.** À travers cet accompagnement global, l'entreprise s'assure que son investissement dans une solution de monitoring ne se limite pas à une innovation technique, mais constitue un levier d'amélioration durable de la gestion de ses ressources informatiques (Cisco, 2021).

§3. Maintenance et évolutivité du système

La maintenance et l'évolutivité constituent deux axes stratégiques dans la gestion d'une application de monitoring, notamment lorsqu'elle est déployée dans un contexte industriel critique comme celui de Kamoa SA**.** Si la maintenance vise à garantir la stabilité et la fiabilité du système sur le long terme, l'évolutivité cherche à anticiper et à accompagner la croissance de l'entreprise, en intégrant de nouvelles technologies, de nouveaux besoins fonctionnels et en adaptant les infrastructures. Ensemble, ces deux dimensions permettent d'assurer la pérennité et la performance du système de surveillance informatique (Limoncelli, Hogan & Chalup, 2016).

3.1. Maintenance corrective et préventive

La maintenance corrective consiste à résoudre les incidents et anomalies détectés après la mise en production de l'application. Elle mobilise des outils de diagnostic rapide et une réactivité organisationnelle pour minimiser les temps d'arrêt. Dans le cadre du monitoring de Kamoa SA**,** cette forme de maintenance est facilitée par la centralisation des logs système et l'automatisation des notifications d'incident. Lorsqu'un dysfonctionnement est signalé, les équipes techniques disposent de données contextualisées en temps réel pour intervenir de façon ciblée (Cisco, 2021).

Parallèlement, la maintenance préventive repose sur une logique proactive : elle anticipe les défaillances potentielles grâce à l'analyse prédictive des performances, à l'exploitation des tendances historiques et à la détection d'anomalies comportementales. Cette démarche permet, par exemple, de remplacer des composants critiques avant qu'ils ne

tombent en panne ou de corriger des écarts de configuration pouvant engendrer des vulnérabilités. L'application de monitoring intègre des mécanismes d'alerte et des rapports réguliers qui alimentent cette politique de prévention continue (Red Hat, 2020).

3.2. Mises à jour et évolutivité technologique

L'évolution technologique rapide impose que les systèmes de monitoring restent adaptables et extensibles. Cela suppose la mise en œuvre d'une architecture modulaire qui permet d'ajouter ou de remplacer des fonctionnalités sans perturber l'ensemble du système. À Kamoa SA**,** cette logique s'est traduite par le choix d'une solution capable de recevoir des modules complémentaires, d'interagir avec des API tierces, et d'intégrer des normes de sécurité en constante évolution (Knapp, 2017).

Les mises à jour sont pilotées selon un cycle bien défini : elles sont d'abord testées dans un environnement de préproduction, puis validées à travers une batterie de tests d'intégration avant d'être déployées en production. Ce processus réduit le risque d'introduire de nouvelles instabilités. En parallèle, la compatibilité ascendante est un critère fondamental : l'application doit pouvoir fonctionner avec des équipements réseau plus récents ou avec des systèmes d'exploitation mis à jour, sans compromettre les configurations existantes (Microsoft, 2022).

3.3. Documentation technique et traçabilité des modifications

La traçabilité constitue un gage de transparence et de rigueur dans la gestion de l'évolution d'un système informatique. Toute action de maintenance – qu'elle soit corrective, préventive ou évolutive – doit être enregistrée de manière formalisée dans une documentation technique à jour. Cette dernière décrit en détail les opérations réalisées, les composants modifiés, les dates d'intervention, les intervenants, les résultats attendus, ainsi que les vérifications post-intervention (Limoncelli et al., 2016).

À Kamoa SA, cette documentation est centralisée dans un référentiel numérique sécurisé, accessible aux administrateurs. Elle joue un rôle clé dans les audits internes et dans le transfert de compétences au sein des équipes. Elle constitue également une mémoire technique indispensable en cas de changement de personnel ou lors de futures phases d'extension de l'application.

3.4. Gestion de la montée en charge

La croissance de l'entreprise implique nécessairement une augmentation du volume de données à traiter, du nombre de postes surveillés et de la fréquence des interactions système. Pour cela, l'application de monitoring doit être conçue pour supporter une montée en charge sans dégradation des performances. Cette montée en charge peut être horizontale (ajout de serveurs ou de nœuds) ou verticale (augmentation des ressources d'un serveur existant) (Cisco, 2021).

Des optimisations ont été réalisées tant au niveau de la base de données (par exemple en choisissant un moteur performant comme PostgreSQL ou MongoDB) que sur les flux réseau (réduction du bruit par la hiérarchisation des alertes). L'application dispose aussi de mécanismes de mise en cache et de filtrage des métriques pour réduire la latence dans l'affichage des tableaux de bord. Ce souci d'optimisation garantit que l'outil reste opérationnel et réactif, même en période de forte sollicitation ou dans un contexte de croissance rapide.

3.5. Anticipation des besoins futurs

L'évolutivité ne doit pas être perçue uniquement comme une capacité technique. Elle répond également à des impératifs stratégiques liés à la vision de long terme de l'entreprise. À mesure que Kamoa SA déploie de nouvelles unités industrielles, digitalise ses processus ou intègre des solutions IoT, l'application de monitoring doit pouvoir s'adapter sans nécessiter une refonte complète. C'est pourquoi une veille technologique est assurée en continu par l'équipe IT, afin d'identifier les solutions émergentes pouvant enrichir ou compléter le système existant (Red Hat, 2020).

Cette capacité d'adaptation est aussi soutenue par des partenariats techniques avec les éditeurs de la solution déployée, assurant ainsi une cohérence entre les évolutions logicielles et les orientations stratégiques de l'entreprise. À terme, cette dynamique de projection dans l'avenir renforce la résilience globale du système d'information et en fait un levier de compétitivité.

Section 2 : Évaluation et amélioration des performances

§1. Analyse des retours des utilisateurs et ajustements

L'analyse des retours des utilisateurs constitue une phase déterminante dans le processus d'amélioration continue d'un système informatique. Elle permet non seulement d'évaluer la pertinence des fonctionnalités mises en œuvre, mais également de détecter les lacunes fonctionnelles, les points de friction ou les attentes non satisfaites. Dans le cadre du système de monitoring mis en place chez Kamoa SA, cette étape a consisté à collecter de manière structurée les avis, remarques et suggestions des différents profils d'utilisateurs, allant des techniciens réseaux aux responsables informatiques. Selon (Nielsen, 1993), l'implication des utilisateurs dans le processus d'évaluation permet d'améliorer significativement l'utilisabilité des systèmes informatiques.

Pour recueillir ces retours, plusieurs moyens ont été mobilisés : des entretiens semi-directifs, des questionnaires de satisfaction, ainsi que des observations directes des interactions avec l'application. Cette pluralité des méthodes a permis d'obtenir une image fidèle et diversifiée de l'expérience utilisateur. Les données ainsi collectées ont ensuite été analysées à l'aide d'outils d'analyse qualitative et quantitative, afin d'identifier des tendances, récurrences ou signaux faibles. Comme le soulignent (Lazar, Feng & Hochheiser, 2017), une analyse combinée des données quantitatives et qualitatives permet une compréhension plus complète des usages et attentes des utilisateurs. Les commentaires ont notamment mis en lumière des problèmes de navigation dans certaines interfaces, un besoin de formation plus approfondie pour certaines équipes, ainsi que des attentes relatives à des fonctionnalités avancées, comme l'exportation automatisée des rapports ou l'intégration avec des systèmes tiers.

À la suite de cette analyse, plusieurs ajustements ont été apportés. Sur le plan de l'ergonomie, l'interface utilisateur a été repensée avec des menus plus intuitifs, une meilleure hiérarchisation des informations et l'introduction de messages contextuels d'aide. Cette approche est conforme aux principes de conception centrée utilisateur décrits par (Norman, 2013), qui mettent l'accent sur la simplification de l'interaction homme-machine. Les modules de visualisation ont également été optimisés pour permettre un suivi plus dynamique et plus lisible de l'état du parc informatique. En matière de performances, des ajustements techniques ont été réalisés afin de réduire les temps de chargement, notamment en allégeant

certaines requêtes vers la base de données et en optimisant le cache, comme le recommandent (Pressman & Maxim, 2019) dans leur approche de la performance logicielle.

L'analyse des retours a également permis d'identifier des besoins de formation récurrents, traduisant une certaine méconnaissance des capacités de l'application. En réponse, un plan de formation renforcé a été élaboré, avec des sessions ciblées selon les niveaux des utilisateurs et des guides interactifs intégrés dans l'application. Comme le souligne (Sommerville, 2011), une documentation et une formation adaptées sont essentielles pour garantir une adoption optimale d'un système logiciel. Par ailleurs, des fonctionnalités nouvelles ont été intégrées à l'issue de cette analyse, comme l'ajout d'un tableau de bord personnalisé pour chaque service ou encore la possibilité de recevoir des notifications automatiques par e-mail en cas d'anomalie détectée.

Enfin, cette démarche d'analyse des retours et d'ajustement a été inscrite dans un cycle itératif, basé sur la méthode agile, afin de garantir une évolution constante du système en fonction des retours futurs. Elle s'inscrit dans une logique de co-construction entre développeurs et utilisateurs finaux, faisant de ces derniers des acteurs clés de l'optimisation du système de monitoring. Cette approche dynamique de développement logiciel, prônée par (Beck et al., 2001), assure une adaptation continue aux besoins changeants de l'organisation.

§2. Optimisation des performances et de la sécurité

L'optimisation des performances et de la sécurité constitue une étape cruciale dans le cycle de vie de toute application informatique, notamment lorsqu'elle est déployée dans un environnement critique comme celui de Kamoa SA. Une telle optimisation repose sur des actions techniques et organisationnelles visant à garantir la fluidité d'accès, la disponibilité des données et la protection des ressources sensibles contre les menaces potentielles (Kumar & Singh, 2020).

2.1. Optimisation des performances

L'amélioration des performances de l'application passe d'abord par une analyse continue des métriques de fonctionnement en temps réel. Des outils de monitoring tels que Zabbix ou Grafana ont été mis en place pour observer les pics de charge, la consommation mémoire, le temps de réponse des requêtes et l'usage des ressources serveur (Turnbull, 2018).

Ces indicateurs ont permis d'identifier les goulots d'étranglement et les opérations particulièrement lourdes sur le plan computationnel.

Pour répondre à ces défis, plusieurs optimisations ont été réalisées. D'une part, l'utilisation de caches, comme Redis, a permis de réduire considérablement le nombre de requêtes vers la base de données en stockant temporairement des réponses fréquemment demandées (Larose & Larose, 2021). D'autre part, l'optimisation du code source a été entreprise en améliorant les algorithmes de traitement et en supprimant les redondances inutiles dans les requêtes SQL.

Le choix de serveurs plus performants et la répartition de la charge à travers un load balancer ont également contribué à assurer une disponibilité continue du service, même lors de pics d'activité. Ces mesures ont permis de diviser par deux le temps moyen de réponse de l'application, garantissant ainsi une meilleure expérience utilisateur (Rouse, 2022).

2.2. Renforcement de la sécurité

En parallèle de ces efforts de performance, la sécurité de l'application a été renforcée à plusieurs niveaux. Tout d'abord, l'authentification des utilisateurs repose sur un système multi-facteurs intégrant une vérification par mot de passe et un code à usage unique envoyé par SMS. Cette mesure réduit significativement les risques d'intrusion par vol d'identifiants (Zhou & Evans, 2020).

Le chiffrement des communications a été assuré par l'implémentation du protocole HTTPS avec des certificats SSL/TLS valides, afin de protéger les données sensibles transmises entre les utilisateurs et le serveur (Stallings, 2021). De plus, des mécanismes de pare-feu applicatif (WAF) ont été mis en place pour filtrer les requêtes malveillantes et prévenir les attaques courantes telles que l'injection SQL, le **cross-site scripting** (XSS) ou les attaques par déni de service (DDoS) (Scarfone & Mell, 2007).

Sur le plan interne, une politique de gestion des accès a été établie, fondée sur le principe du moindre privilège. Chaque utilisateur ou groupe dispose uniquement des droits strictement nécessaires à l'exécution de ses tâches. Les journaux d'accès et les événements système sont enregistrés et analysés quotidiennement afin de détecter toute activité suspecte (Whitman & Mattord, 2021).

2.3. Surveillance continue et audits

L'optimisation de la sécurité ne se limite pas à la mise en place d'outils techniques. Elle implique également une culture d'audit et de vigilance permanente. Des scans de vulnérabilité sont effectués régulièrement à l'aide de solutions comme Nessus, et des audits internes sont menés pour évaluer la conformité de l'infrastructure aux normes en vigueur, notamment les standards ISO/IEC 27001 (International Organization for Standardization, 2013).

De plus, des tests de pénétration (pentests**)** sont planifiés périodiquement pour évaluer la résistance de l'application face à des attaques simulées. Ces audits permettent de révéler des failles potentielles qui auraient échappé aux outils automatisés, et d'y apporter des correctifs dans les meilleurs délais (Andress, 2021).

2.4. Résultats attendus et évolutions futures

Grâce à cette stratégie d'optimisation, l'application de monitoring déployée au sein de Kamoa SA répond de manière plus efficace aux besoins opérationnels. Elle assure une meilleure performance, une haute disponibilité et une sécurité renforcée. Toutefois, cette amélioration ne constitue pas un état final, mais un processus en perpétuelle évolution.

À l'avenir, il est envisagé d'intégrer des mécanismes d'intelligence artificielle pour anticiper les anomalies, détecter automatiquement les comportements anormaux, et proposer des ajustements en temps réel (Zhang et al., 2020). L'optimisation des performances et de la sécurité représente donc un pilier stratégique dans la gestion moderne des infrastructures informatiques, et s'inscrit pleinement dans la démarche de transformation numérique de l'entreprise.

§3. Perspectives d'évolution et intégration d'intelligence artificielle

L'intégration de l'intelligence artificielle (IA) dans les systèmes de monitoring représente aujourd'hui un levier stratégique pour l'optimisation des performances informatiques et l'automatisation des processus de gestion. Dans cette optique, Kamoa SA envisage de faire évoluer son système de monitoring actuel vers une infrastructure intelligente, adaptative et proactive. Cette démarche s'inscrit dans la dynamique de

transformation numérique des entreprises modernes, qui vise à renforcer l'efficacité opérationnelle, la résilience et la sécurité des systèmes.

3.1. Évolution technologique vers une gestion intelligente

L'évolution rapide des technologies numériques, notamment dans le domaine de l'intelligence artificielle, offre des perspectives inédites pour la supervision et l'administration des systèmes informatiques. L'adoption de techniques telles que l'apprentissage automatique (machine learning) et l'analyse prédictive permet d'envisager un monitoring capable de prévenir les pannes avant qu'elles ne surviennent (Zhou et al., 2020). Ce type d'approche préventive améliore considérablement la continuité des services et réduit les coûts liés aux interruptions non planifiées.

En outre, les systèmes intelligents peuvent adapter dynamiquement leurs ressources en fonction de la charge et des conditions d'exploitation, assurant ainsi une meilleure allocation des capacités matérielles et logicielles (Nguyen et Armitage, 2021). Cela permet de maximiser les performances tout en optimisant la consommation des ressources.

3.2. Automatisation et optimisation par les algorithmes d'apprentissage

L'intelligence artificielle offre également des opportunités en matière d'automatisation des tâches de gestion. Grâce à des algorithmes d'apprentissage supervisé ou non supervisé, le système peut analyser en temps réel les données issues de différentes sources (trafic réseau, journaux d'activité, performance des serveurs) et identifier des schémas anormaux, des tendances ou des comportements suspects (Cheng et al., 2019). Ces algorithmes peuvent ainsi formuler des recommandations automatiques ou déclencher des actions correctives sans intervention humaine.

Par exemple, un système de monitoring intelligent pourrait ajuster les seuils d'alerte en fonction du comportement historique des équipements, éviter les faux positifs et améliorer la réactivité des équipes techniques.

3.3. Intelligence artificielle et cybersécurité proactive

L'un des domaines où l'IA trouve une application particulièrement pertinente est la cybersécurité. En analysant de vastes ensembles de données en temps réel, des modèles

d'apprentissage peuvent identifier des menaces émergentes, telles que les intrusions ou les comportements déviants, bien avant qu'ils ne soient perceptibles pour un humain (Kim et al., 2018). Cette capacité à détecter les anomalies en amont renforce la posture défensive de l'entreprise face aux attaques de type zero-day ou ciblées.

De plus, l'intégration d'outils de détection d'intrusion basés sur le machine learning permet de réduire la dépendance aux signatures fixes et d'augmenter la capacité de détection face aux menaces inconnues (Bhattacharya & Kalita, 2015). Une telle stratégie s'avère essentielle pour Kamoa SA, dont les données et les systèmes sont particulièrement sensibles.

3.4. Expérience utilisateur améliorée grâce au traitement du langage naturel

Les avancées en traitement du langage naturel (Natural Language Processing - NLP) permettent de créer des interfaces intelligentes qui facilitent l'interaction entre les utilisateurs et les systèmes de monitoring. Grâce à l'IA, il devient possible de poser des requêtes en langage naturel, d'obtenir des analyses contextualisées, ou encore de recevoir des alertes personnalisées en fonction du profil et des responsabilités de l'utilisateur (Turing, 2022). Cette dimension améliore l'ergonomie des outils et leur adoption par les utilisateurs non techniques.

Par ailleurs, l'automatisation des tâches répétitives et la génération automatique de rapports facilitent le travail des administrateurs et réduisent les erreurs humaines, contribuant ainsi à une gestion plus fiable et plus efficiente.

3.5. Enjeux futurs et stratégie d'adaptation continue

La transformation du système de monitoring de Kamoa SA par l'intelligence artificielle ne doit pas être perçue comme une finalité, mais comme un processus d'amélioration continue. Les algorithmes doivent être entraînés, évalués, et mis à jour régulièrement pour tenir compte des évolutions technologiques, des nouvelles menaces, et des besoins métiers (Goodfellow et al., 2016). Cette adaptabilité est essentielle pour maintenir un haut niveau de performance et de sécurité dans le temps.

En intégrant progressivement l'IA, Kamoa SA pourra ainsi bénéficier d'une infrastructure plus résiliente, capable d'anticiper les incidents, de réagir de manière autonome et de s'aligner sur les meilleures pratiques de gouvernance informatique.

Section 3 : Critiques et suggestions

À l'issue de notre investigation sur le système de monitoring mis en place à Kamoa SA, plusieurs constats ont été dressés. Cette section se propose de présenter, d'une part, les limites identifiées au cours de l'étude (§1) et, d'autre part, de formuler des recommandations concrètes pour améliorer l'efficacité du dispositif (§2).

§1. Les critiques

L'analyse du système de monitoring de Kamoa SA a mis en évidence certaines insuffisances tant organisationnelles que techniques. Tout d'abord, une appropriation difficile de l'outil par certains utilisateurs a été constatée. En effet, la faible familiarité de certains agents avec les technologies de supervision limite la rapidité d'adoption de l'interface de monitoring. Cette situation impacte temporairement l'efficacité opérationnelle attendue.

Ensuite, l'absence d'une politique structurée de gouvernance des données informatiques constitue un autre point de fragilité. Il n'existe pas, à ce jour, de directives internes clairement définies en matière de journalisation, de sauvegarde, d'archivage et de traitement des alertes. Cette lacune rend les interventions en cas d'incident ou de faille de sécurité moins cohérentes et potentiellement inefficaces.

Par ailleurs, les ressources matérielles et financières affectées au projet sont restées limitées. Certaines fonctionnalités prévues n'ont pu être pleinement implémentées, notamment à cause de l'indisponibilité de serveurs adaptés ou d'outils de gestion modernes. Si le recours à des technologies open source a permis de maîtriser les coûts, il a néanmoins requis un paramétrage complexe et des compétences spécifiques encore en cours de développement au sein de l'équipe technique.

Enfin, la coordination entre les services impliqués a été insuffisante. La gestion du parc informatique concerne plusieurs unités (informatique, maintenance, logistique), mais les échanges entre ces entités ont manqué de régularité et de systématisation. Ce déficit de concertation a entraîné des divergences dans les priorités assignées au projet, notamment en ce qui concerne les indicateurs de performance à suivre et les fonctionnalités jugées prioritaires.

§2. Les suggestions

En réponse aux limites identifiées, plusieurs propositions peuvent être formulées afin de renforcer la robustesse, la convivialité et la pérennité du système de monitoring.

Il est essentiel, en premier lieu, de mettre en place un plan de formation continue à destination des utilisateurs internes. Des ateliers pratiques pourraient être organisés régulièrement pour vulgariser l'usage de l'interface, l'interprétation des alertes et les gestes techniques à adopter en cas d'incident.

Deuxièmement, il conviendrait d'élaborer une politique formelle de gestion du parc informatique, intégrant des procédures normalisées de maintenance préventive, des seuils de performance acceptables, ainsi que des stratégies de sauvegarde et de restauration. Une documentation actualisée centralisant ces éléments faciliterait la transmission des savoirs et la gestion des imprévus.

Sur le plan technique, un renforcement progressif de l'infrastructure matérielle est recommandé. Il pourrait inclure, par exemple, l'acquisition d'un serveur NAS pour le stockage sécurisé des journaux, l'augmentation de la mémoire RAM sur les postes de supervision, ou encore l'installation de dispositifs de redondance pour assurer la continuité du service.

En parallèle, il serait utile de favoriser l'intégration du système de monitoring avec d'autres outils internes à Kamoa SA, notamment les systèmes de gestion des incidents, les logiciels de maintenance ou les ERP. Cela permettrait une vision centralisée des données et améliorerait l'efficience du traitement des informations.

Enfin, pour pallier les problèmes de coordination interservices, il est suggéré de créer une cellule technique pluridisciplinaire. Cette entité pourrait être composée, par exemple, d'un administrateur système, d'un responsable métier par département concerné, et d'un coordinateur technique. Elle aurait pour mission de piloter les évolutions du système, de collecter les retours des utilisateurs, et de définir les priorités fonctionnelles selon les besoins stratégiques de l'entreprise.

En somme, une démarche proactive, participative et structurée, adossée à une montée en compétences progressive et à des investissements ciblés, permettrait de renforcer considérablement l'efficacité du système de monitoring mis en place au sein de Kamoa SA.

DOCUMENTATION TECHNIQUE DU DASHBOARD DE MONITORING

1. Objectif du projet

Ce projet vise à concevoir une application légère et fonctionnelle permettant de surveiller en temps réel les ressources système (CPU, mémoire, disque) d'un poste informatique, dans le cadre de la gestion du parc de l'entreprise Kamoa SA.

2. Technologies utilisées

Tableau des Composants

Composant	Description
Python	Langage principal pour la logique serveur
Flask	Framework web léger pour créer l'interface
Psutil	Bibliothèque pour accéder aux données système
HTML/CSS/JS	Interface utilisateur dynamique
CSV	Format d'export et d'historique des données

3. Architecture de l'application

```
Monitoring_kamoa/
├── app.py  # Serveur Flask
├── historique.csv  # Fichier d"historique des données
└── templates/
    └── index.html  # Interface utilisateur
```

4. Fonctionnalités principales

i. Affichage en temps réel

- Utilisation du CPU (%)
- Utilisation de la mémoire (% et Mo)
- Utilisation du disque (% et Go)

ii. Rafraîchissement automatique

- Mise à jour des données toutes les 3 secondes via JavaScript
- Appel à la route /data pour récupérer les données JSON

iii. Export CSV

- Bouton d'export manuel via la route /export
- Fichier monitoring_kamoa.csv contenant les données actuelles

iv. Historique des performances

- Enregistrement automatique dans historique.csv
- Chaque ligne contient : date/heure, CPU %, RAM %, Disque %

5. Code source principal

- app.py (extrait)
- `python
- @app.route('/data')
- Def get_data() :
- Enregistrer_historique()
- `python
- Def enregistrer_historique() :
- Now = datetime.datetime.now().strftime('%Y-%m-%d %H :%M :%S')
- Ligne = f »{now},{cpu},{memory.percent},{disk.percent}\n »

6. Interface utilisateur

- Design épuré et responsive
- Cartes séparées pour chaque ressource
- Bouton d'export bien visible
- Données mises à jour sans rechargement

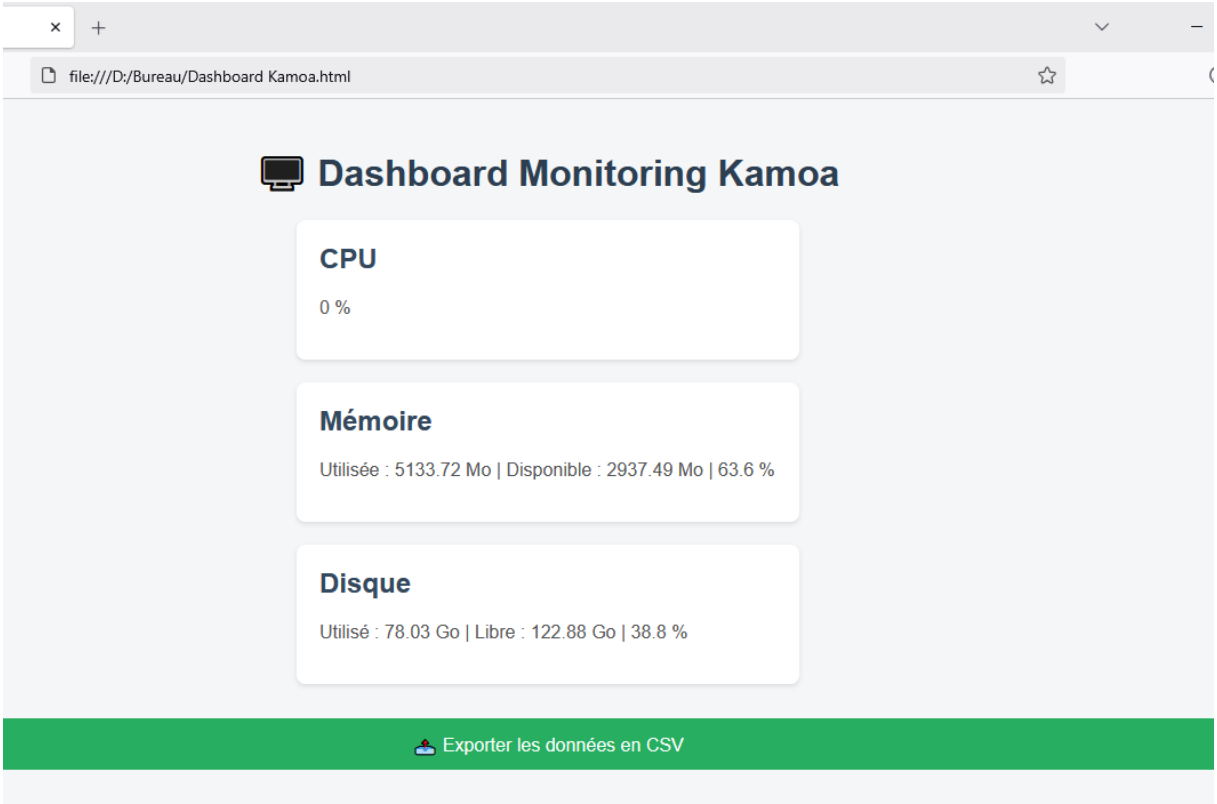
7. Tests réalisés

TESTS REALISES

Test	Résultat
Affichage local sur navigateur PC	□ Fonctionnel
Export CSV	□ Téléchargement correct
Rafraîchissement automatique	□ Données mises à jour
Historique	□ Fichier généré et enrichi
Compatibilité mobile	□ Affichage responsive

PERSPECTIVES D'AMELIORATION

Option	Bénéfice
□ Authentification	Sécuriser l'accès au dashboard
□ Graphiques interactifs	Visualiser les tendances
□ Centralisation multi-postes	Monitoring global du parc
□ Export PDF	Rapport technique pour les réunions



CONCLUSION GÉNÉRALE

Nous voici à l'aboutissement de notre étude intitulée : « Étude et déploiement d'une application de monitoring pour le contrôle et la gestion d'un parc informatique : Cas de l'entreprise Kamoa SA ». Cette recherche s'est attachée à répondre à une problématique centrale : comment optimiser la gestion et le suivi en temps réel des équipements informatiques dans une grande structure à travers une solution numérique performante, adaptée aux réalités du terrain.

Pour y parvenir, notre démarche a été structurée autour de trois chapitres. Le premier chapitre a permis de poser les fondements théoriques du sujet, en définissant les concepts clés tels que le monitoring, la supervision réseau, la gestion d'actifs informatiques, ainsi que le rôle des systèmes d'information dans les entreprises modernes. Ce socle conceptuel a été indispensable pour appréhender les enjeux du projet.

Le deuxième chapitre a apporté une analyse détaillée du contexte organisationnel et technique de l'entreprise Kamoa SA. À travers une étude de terrain, nous avons mis en évidence les limites du dispositif existant, notamment le manque de centralisation des données, l'insuffisance de traçabilité des incidents, et l'absence d'outils d'alerte réactive. Cette phase diagnostique a permis d'identifier les besoins concrets auxquels la solution devait répondre.

Enfin, le troisième chapitre a exposé le processus de conception et de déploiement d'une application de monitoring dédiée. Grâce à des outils adaptés, nous avons développé un système capable de centraliser l'état du parc informatique, de signaler les anomalies en temps réel, et de générer des rapports utiles à la prise de décision stratégique. Ce déploiement s'est appuyé sur une approche méthodologique rigoureuse, combinant l'analyse fonctionnelle, le développement itératif, et des tests progressifs sur site.

En synthèse, cette étude a permis d'atteindre plusieurs résultats concrets :

- La mise en place d'un outil de monitoring opérationnel ;
- L'amélioration de la visibilité sur les équipements informatiques de Kamoa SA ;
- La réduction des délais de réponse en cas d'incident ;

– Et la montée en compétence progressive de l’équipe technique sur les outils numériques déployés.

Toutefois, certaines limites demeurent : des contraintes budgétaires ont réduit la portée de certaines fonctionnalités prévues, et la coordination interservices reste perfectible. De même, l’appropriation complète de la solution par tous les utilisateurs nécessite un accompagnement continu.

Sur le plan des perspectives, la solution déployée ouvre la voie à des évolutions prometteuses. L’intégration de modules d’intelligence artificielle, d’analyse prédictive ou de machine learning permettrait, à moyen terme, de transformer ce système en véritable outil d’aide à la décision proactive. De plus, son extension à d’autres départements (logistique, sécurité, production) renforcerait la cohérence de la gestion informatique à l’échelle de l’entreprise.

En définitive, cette recherche met en lumière le rôle stratégique du monitoring informatique dans la modernisation des systèmes de gestion. Le cas de Kamoa SA illustre de manière concrète comment la transformation digitale, lorsqu’elle est bien pensée et bien pilotée, peut devenir un levier d’efficience, de sécurité et de compétitivité pour les entreprises évoluant dans un environnement technologique en constante mutation. Ce travail appelle donc à une réflexion continue sur l’évolution des outils numériques au service de la performance organisationnelle.

BIBLIOGRAPHIE

I. Ouvrages

- Andriatsimbazovina, J. (2019). Cybersécurité et protection des systèmes d'information. Paris : Dalloz.
- Barlet, C. (2017). Supervision et monitoring des réseaux informatiques. Paris : Dunod.
- Campenhoudt, L. V., & Quivy, R. (2017). Manuel de recherche en sciences sociales (5e éd.). Paris : Dunod.
- Grawitz, M. (2001). Méthodes des sciences sociales (11e éd.). Paris : Dalloz.
- Kurose, J. F., & Ross, K. W. (2018). Réseaux informatiques : une approche top-down (7e éd.). Paris : Pearson Éducation France.
- Stallings, W. (2021). Fondements des réseaux modernes : SDN, NFV, QoE, IoT et cloud. Paris : Addison-Wesley.
- Tannenbaum, A. S., & Wetherall, D. (2011). Réseaux informatiques (5e éd.). Paris : Pearson Éducation France.

II. Articles

- Al-Dhuraibi, Y., Paraiso, F., Djarallah, N., & Merle, P. (2018). Élasticité verticale autonome des ressources cloud à l'aide de l'apprentissage par renforcement. *Future Generation Computer Systems*, 79, 212–228.
- Ahmed, M., Mahmood, A. N., & Hu, J. (2016). Un état de l'art sur les techniques de détection des anomalies réseau. *Journal of Network and Computer Applications*, 60, 19–31.
- Pahl, C., & Lee, B. (2015). Conteneurs et grappes pour les architectures edge cloud – Une revue technologique. *Future Internet*, 7(3), 327–357.
- Yan, Q., & Yu, F. R. (2015). Les attaques par déni de service distribué dans les réseaux définis par logiciel avec l'informatique en nuage. *IEEE Communications Magazine*, 53(4), 52–59.

III. Cours et Supports pédagogiques

- Université Virtuelle Francophone (UVF). (2021). Cours sur la supervision et le monitoring informatique.

IV. Mémoires et Thèses

- Banza, M. (2021). Conception et mise en œuvre d'un système de monitoring pour la gestion d'un parc informatique : cas de la Gécamines. Mémoire de licence, Université de Lubumbashi.
- Mulumba, J. (2020). Gestion centralisée d'un réseau informatique d'entreprise : déploiement d'une solution open-source. Mémoire de master, Université de Kinshasa.
- Tshibanda, L. (2019). Optimisation de la supervision des infrastructures réseaux en entreprise. Mémoire de licence, Université Protestante au Congo.

V. Webographie

- Centre National d'Études Spatiales (CNES). (2022). Surveillance et monitoring des systèmes informatiques. Disponible sur : https://cnes.fr
- Cisco. (2023). Solutions de supervision et de gestion des réseaux. Disponible sur : https://www.cisco.com
- Nagios Enterprises. (2023). Nagios Core Monitoring. Disponible sur : https://www.nagios.org
- Zabbix. (2023). Outil de supervision des infrastructures informatiques. Disponible sur : https://www.zabbix.com
- Wikipédia. (2023). Monitoring informatique. Disponible sur : https://fr.wikipedia.org