# Dédicaces

Je dédie le fruit de mes efforts à ma famille et toutes les personnes chères à mon cœur, qui par leur soutien, amour et encouragement ont contribué à l’aboutissement de ce travail.

À MES CHERS PARENTS MOHAMED ET SAMIA

Que ce travail soit l’expression de ma reconnaissance pour vos sacrifices consentis, votre Soutien moral et matériel que vous n’avez cessé de prodiguer. Vous avez tout fait pour Mon bonheur et ma réussite. Que Dieu vous préserve en bonne santé et vous protéger pour moi et mes fréres

Merci pour tout, Que Dieu vous préserve en bonne santé et vous accorde une longue vie

À MES PROFESSEURS ET MES ENSEIGNANTS

Qui m’ont formé durant ma carrière scolaire et universitaire, je vous remercie pour le bon encadrement que j’ai eu tout au long de ce projet.

Vous étiez toujours présents pour m’aider et m’encourager. Sachez que vous êtes toujours dans mon cœur.

À TOUS MES AMIS...

À tous mes amis qui n’ont cessé de m’encourager et de me soutenir À tous ceux que j’aime Et à tous ceux qui m’aiment

# Remerciements

Au terme de ce rapport, je tiens à exprimer mes profonds respects et gratitudes à l’École Polytechnique de Sousse qui m’a offert l’occasion d’effectuer ce stage au sein de la société " PEAK Technologies ", aussi bien, pour enrichir mes connaissances dans la vie professionnelle et de découvrir l’environnement de la société.

Je tiens à exprimer mes remerciements avec un grand plaisir et un grand respect à mon encadrant académique Mr. Rouatbi Adnen pour tous les conseils et les informations qu’il ma dispensés afin que ce stage se passe dans les meilleures conditions, pour son soutient, son sérieux, sa gentillesse et surtout pour son aide précieuse tout au long de l’élaboration de ce travail. .Je présente mes sincères remerciements et mes profondes gratitudes à mon encadrant professionnel Mr. Hasni Mehdi

son assistance, son soutien, sa disponibilité et ses précieux conseils durant la période de ce stage.

J’adresse aussi ma plus vive reconnaissance à tous mes enseignants de l’École Polytechnique de Sousse pour la formation qu’ils mont donnée ainsi qu’aux membres du jury qui ont accepté de juger ce travail.

Finalement, je remercie tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

TABLE DES MATIÈRES

**Introduction générale 1**

1. **Cadre général du projet 3**
   1. **Introduction** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
   2. Étude Préalable : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
      1. Problématique : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
      2. Étude de l’existant : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
      3. Critique de l’existant : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
      4. Solution proposé : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
   3. Présentation de l’organisme d’accueil : . . . . . . . . . . . . . . . . . . . . . . . . 6
      1. Présentation de l’entreprise . . . . . . . . . . . . . . . . . . . . . . . . . . 6
      2. Spécialisations de «L2T» . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7
      3. Fiche Technique de «L2T» : . . . . . . . . . . . . . . . . . . . . . . . . . . 7
      4. Logo de L2T . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
   4. **Conclusion** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
2. **Analyse et Spécification des besoins 9**
   1. **Introduction** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
   2. Spécification des besoins . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
      1. Identification des acteurs . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
      2. Les besoins fonctionnels . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
      3. Besoins non fonctionnels . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11
   3. Étude de méthodologie de développement . . . . . . . . . . . . . . . . . . . . . . 11
      1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 12
      2. Choix de la méthodologie . . . . . . . . . . . . . . . . . . . . . . . . . . . 12
      3. Méthodologie choisie (En v) . . . . . . . . . . . . . . . . . . . . . . . . . . 14
      4. Les principales caractéristiques de la méthode cycle en V . . . . . . . . . . . 14
   4. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15
3. **Etude Conceptuelle 16**
   1. **Introduction** . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16
   2. Définition UML . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 16
   3. Conception . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17
      1. Diagramme des cas d’utilisation . . . . . . . . . . . . . . . . . . . . . . . . 17
      2. Diagramme de classes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23
      3. Diagramme de séquence . . . . . . . . . . . . . . . . . . . . . . . . . . . . 25
      4. diagramme de déploiement . . . . . . . . . . . . . . . . . . . . . . . . . . . 32
   4. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33
4. **Réalisation 34**
   1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
   2. Architecture de la solution . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
      1. Modèle MVC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
   3. Environnement du projet . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
      1. Environnement matériel . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
      2. Environnement logiciel . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
   4. Présentation de la solution . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
      1. Interface d’accueil . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
      2. Interface registre . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
      3. Interface login . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
      4. Dashboard admin . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
      5. Liste annonces prestataire admin . . . . . . . . . . . . . . . . . . . . . . . . 44
      6. Liste profiles demandeur admin . . . . . . . . . . . . . . . . . . . . . . . . 44
      7. Choix type annonce prestataire . . . . . . . . . . . . . . . . . . . . . . . . . 45
      8. Créer annonce prestataire baby-sitter . . . . . . . . . . . . . . . . . . . . . . 46
      9. Créer annonce prestataire auxiliaire de vie . . . . . . . . . . . . . . . . . . . 47
      10. Créer annonce prestataire garde animaux . . . . . . . . . . . . . . . . . . . 48
      11. Liste annonces prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . 49
      12. Détails annonce prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . 49
      13. Chat . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50
      14. Profil prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50
      15. Choix type annonce demandeur . . . . . . . . . . . . . . . . . . . . . . . . 51
      16. Créer annonce demandeur baby-sitter . . . . . . . . . . . . . . . . . . . . . 52
      17. Créer annonce demandeur auxiliaire de vie . . . . . . . . . . . . . . . . . . 53
      18. Créer annonce demandeur garde animaux . . . . . . . . . . . . . . . . . . . 54
      19. Edit annonce prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55
      20. Supprimer annonce Demandeur . . . . . . . . . . . . . . . . . . . . . . . . 56
   5. Conclusion . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 56

**Conclusion Générale 57**

**Bibliographie 58**

TABLE DES FIGURES

* 1. Logo officiel de Bambinosit . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
  2. Etude de l’application Yoopies . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5
  3. Logo officiel de L2T . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

2.1 Le cycle en v . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

* 1. UML . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17
  2. Diagramme des cas d’utilisation globale . . . . . . . . . . . . . . . . . . . . . . . . 18
  3. Diagramme des cas d’utilisation «Valider utilisateur» . . . . . . . . . . . . . . . . . 19
  4. Diagramme des cas d’utilisation «Valider annonce» . . . . . . . . . . . . . . . . . . 20
  5. Diagramme des cas d’utilisation «Valider commentaire» . . . . . . . . . . . . . . . 21
  6. Diagramme des cas d’utilisation «gérer annonce» . . . . . . . . . . . . . . . . . . . 22
  7. Diagramme des cas d’utilisation «gérer profilr» . . . . . . . . . . . . . . . . . . . . 22
  8. Diagramme des cas d’utilisation «consulter annonce demandeur» . . . . . . . . . . . 23
  9. Diagramme des cas d’utilisation «consulter annonce prestataire» . . . . . . . . . . . 23
  10. Diagramme de classes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
  11. Diagramme de séquence «s’inscrire» . . . . . . . . . . . . . . . . . . . . . . . . . . 25
  12. Diagramme de séquence«s’authentifier» . . . . . . . . . . . . . . . . . . . . . . . . 26
  13. Diagramme de séquence«valider compte uilisateur» . . . . . . . . . . . . . . . . . . 26
  14. Diagramme de séquence«créer annonce» . . . . . . . . . . . . . . . . . . . . . . . . 27
  15. Diagramme de séquence «modifier annonce» . . . . . . . . . . . . . . . . . . . . . 28
  16. Diagramme de séquence «supprimer annonce» . . . . . . . . . . . . . . . . . . . . 29
  17. Diagramme de séquence «détail annonce» . . . . . . . . . . . . . . . . . . . . . . . 29
  18. Diagramme de séquence «ecrire commentaire» . . . . . . . . . . . . . . . . . . . . 30
  19. Diagramme de séquence «gérer message» . . . . . . . . . . . . . . . . . . . . . . . 31
  20. Diagramme de séquence «consulter notification» . . . . . . . . . . . . . . . . . . . 32
  21. Diagramme de séquence «diagramme de déploiement» . . . . . . . . . . . . . . . . 33
  22. Modèlé MVC . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35
  23. Interface d’accueil 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41
  24. Choix du Type d’Utilisateur . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42
  25. Formulaire d’Inscription . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 42
  26. Interface login . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
  27. Dashboard admin . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
  28. Liste annonces prestataire admin . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44
  29. Liste profiles demandeur admin . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
  30. Choix type annonce prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 45
  31. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 46
  32. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 46
  33. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
  34. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
  35. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 48
  36. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 48
  37. Liste annonces prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49
  38. Détails annonce . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 49
  39. Chat . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50
  40. Profil prestataire . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 50
  41. Choix type annonce demandeur . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 51
  42. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52
  43. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 52
  44. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53
  45. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 53
  46. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 54
  47. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 54
  48. Step 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55
  49. Step 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55
  50. Supprimer annonce Demandeur . . . . . . . . . . . . . . . . . . . . . . . . . . . . 56

LISTE DES TABLEAUX

1.2 Etude de l’application Bambinosit . . . . . . . . . . . . . . . . . . . . . . . . . . . 5 1.3 Etude de l’application Yoopies . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

1.4 Fiche signalétique de la société L2T . . . . . . . . . . . . . . . . . . . . . . . . . . 7

2.1 Comparaison des méthodes de développement . . . . . . . . . . . . . . . . . . . . 14

* 1. Environnement matériel . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
  2. Technologies et languages utilisées . . . . . . . . . . . . . . . . . . . . . . . . . . . 40

***Introduction générale***

Dans un contexte économique et réglementaire de plus en plus contraignant, la maîtrise des risques et la conformité aux normes constituent des enjeux majeurs pour les organisations. La digitalisation croissante des processus expose en effet les entreprises à de nouveaux risques – opérationnels, financiers, juridiques ou liés à la sécurité des données – qu’il convient d’identifier, d’évaluer puis de piloter de façon continue. C’est dans cette optique que s’inscrit notre Projet de Fin d’Études (PFE), dont l’objectif est de concevoir et de réaliser une plateforme logicielle innovante, baptisée **SentinelRisk**, dédiée à la gestion intégrée des risques et à la conformité réglementaire.

Le projet a été mené au sein de **PEAK Consulting GmbH – PEAK Technologies SARL**, cabinet de conseil spécialisé en Identity & Access Management (IAM) et en sécurité des systèmes d’information, implanté à Mannheim (Allemagne) et à Sousse (Tunisie). Fondée en 2016, PEAK-CS accompagne de grandes organisations dans la mise en place de solutions IAM, le développement d’applications sur mesure et la prévention de la fraude, s’appuyant sur une expertise attestée par un effectif de 11 – 50 collaborateurs et un portefeuille de références internationales.

Le sujet de notre PFE porte sur le développement complet de SentinelRisk :

* **Étude et spécification des besoins** (identification des acteurs, besoins fonctionnels et non fonctionnels),
* **Conception conceptuelle** (modélisation UML des cas d’utilisation, des classes et des séquences),
* **Implémentation technique** (backend Spring Boot, frontend Angular, base PostgreSQL, authentification Keycloak),
* **Déploiement** (Docker Compose, Kubernetes).

Les principaux objectifs sont de proposer une solution robuste et évolutive permettant :

1. d’agréger et de catégoriser les risques (opérationnels, financiers, sécurité des données…),
2. de calculer automatiquement un score de risque et de piloter des plans de mitigation,
3. d’assurer le suivi de la conformité réglementaire via des cadres (ISO 27001, NIST, GDPR, SOC 2),
4. de gérer les profils utilisateurs et les droits d’accès grâce à une intégration transparente avec Keycloak.

Pour guider la rédaction de ce rapport, la structure retenue est la suivante :

* **Chapitre 1 : Cadre général du projet**

Resitue le contexte métier, présente l’organisme d’accueil, expose la problématique, justifie le choix de la méthodologie en cycle en V et illustre la planification par un diagramme de Gantt.

* **Chapitre 2 : État de l’art**

Dresse une revue des solutions et normes existantes, en abordant notamment le protocole SNMP, la gouvernance et les cadres réglementaires (ISO 27001, NIST, GDPR, SOC 2).

* **Chapitre 3 : Analyse et spécification des besoins et architecture**

Identifie les acteurs et leurs cas d’usage, détaille les exigences fonctionnelles et non-fonctionnelles, puis décrit l’architecture technique retenue.

* **Chapitre 4 : Étude conceptuelle**

Modélise le système à l’aide de diagrammes UML (cas d’utilisation, classes, séquences et déploiement).

* **Chapitre 5 : Réalisation**

présente l’environnement de développement et détaille l’application à travers ses interfaces et ses flux métiers.

* **Conclusion générale et perspectives**

Bilan des objectifs atteints, apports personnels et pistes d’évolution

Cette trame nous permettra de présenter de manière claire et méthodique l’ensemble des travaux réalisés dans le cadre de notre PFE, de l’analyse initiale à la mise en œuvre concrète de la plateforme SentinelRisk.

CHAPITRE 1

CADRE GÉNÉRAL DU PROJET

**1.1 Introduction**

L’étude du cadre de projet est une phase primordiale au démarrage de tout projet. Elle permet une compréhension précise du contexte pour fixer les objectifs à atteindre. Dans ce chapitre nous mettons notre travail dans son contexte général. Tout d’abord, nous parlons sur l’environnement de la société à travers une présentation de l’organisme d’accueil et ses activités. Ensuite, nous détaillons la problématique traitée et la spécification des besoins, puis, nous décrivons les diagrammes des cas d’utilisation généraux ainsi que la méthodologie du travail adoptée.

**1.2 Étude Préalable :**

L’analyse de l’existant appartient à la phase d’analyse de projet. Cette étape est primordiale à toute mise en route de tout projet informatique. Elle permet de définir le cadre général du travail, d’éviter les redites, d’aiguiser l’esprit critique et de favoriser la créativité.

**1.3 Présentation de l’organisme d’accueil :**

**1.3.1 Présentation de l’entreprise**

PEAK Consulting GmbH (Allemagne) et sa filiale PEAK Technologies SARL (Tunisie) constituent un cabinet de conseil fondé en 2016, spécialisé dans l’Identity & Access Management (IAM) et le développement de solutions sur mesure. Depuis sa création, PEAK-CS a mené de nombreux projets pour des clients internationaux de premier plan, bénéficiant d’un fort taux de satisfaction et d’un positionnement reconnu sur le marché de la sécurité des systèmes d’information

**1.3.2 Spécialisations de «PEAK Technologies SARL»**

• IAM Consulting : intégration et exploitation de solutions IAM adaptées aux besoins métiers.

• Développement : réalisation de solutions logicielles web et mobiles, incluant des applications IAM, .NET, Android, iOS…

• Graphic Design : création d’identités visuelles, brochures et supports de communication.

• Services pour startups : recrutement de talents, umbrella services (portage salarial) et outsourcing de développement

**1.3.3 Fiche Technique de «PEAK Technologies SARL» :**

|  |  |
| --- | --- |
| **Nom de**  **l’entreprise :** | PEAK Technologies SARL |
| **Nom du gérant :** | Mr Finch John |
| **Site web :** | https ://www.l2t.io/ |
| **Adresse :** | Imm. Espace Sousse, Rue de Khartoum, Sousse 4000. |
| **Téléphone :** | +(216) 22 419 820 |
| **Émail :** | info@peak-cs.com |

Table 1.4 – Fiche signalétique de la société PEAK Technologies SARL

**1.3.4 Logo de PEAK Technologies SARL**

A blue text on a black background

AI-generated content may be incorrect.

Figure 1.3 – Logo officiel de PEAK Technologies SARL

**1.4 Problématique :**

Dans le contexte actuel, les organisations sont exposées à une multitude de risques – opérationnels, financiers, juridiques, technologiques et liés à la sécurité des données – dont la nature et l’impact évoluent constamment. La multiplication des référentiels normatifs (ISO 27001, NIST, GDPR, SOC 2, etc.) et l’hétérogénéité des outils de gestion (tableurs, solutions ponctuelles de reporting, ERP, solutions IAM isolées) conduisent souvent à une vision fragmentée et peu dynamique du pilotage des risques et de la conformité.

Les principaux points de blocage identifiés sont :

* **Dispersion des données et des processus** : absence d’un référentiel unique pour consolider les incidents, les évaluations et les plans d’action, ce qui engendre des redondances et des écarts d’information.
* **Calcul de risque manuel ou semi-automatique** : les méthodes artisanales (feuilles Excel, scripts isolés) ne garantissent ni la traçabilité ni la fiabilité des scores, et sont difficiles à maintenir face à un contexte réglementaire évolutif.
* **Manque d’intégration IAM & gouvernance** : la gestion des droits d’accès et des profils utilisateurs, cruciale pour la conformité, n’est pas toujours reliée aux workflows de mitigation des risques.
* **Faible capacité d’analyse transverse** : difficulté à obtenir des indicateurs consolidés et des tableaux de bord dynamiques qui permettent de prioriser rapidement les actions selon le niveau de criticité.
* **Absence de surveillance automatisée des infrastructures** : les ressources réseau (serveurs, routeurs, équipements IoT, postes de travail) ne sont pas suffisamment supervisées en continu, ce qui retarde la détection des vulnérabilités et des anomalies opérationnelles.

Ainsi, la **problématique** centrale de ce projet consiste à **concevoir et implémenter une plateforme intégrée** qui :

1. **Centralise** toutes les informations relatives aux risques et à la conformité,
2. **Automatise** le calcul des scores de risque et la génération de plans de mitigation,
3. **Intègre** la gestion des identités et des accès via Keycloak pour assurer un contrôle granulaire des droits,
4. **Superviser en continu** l’état des actifs réseau grâce au protocole SNMP (collecte d’OID, détection d’anomalies, remontée automatique de risques),
5. **Fournit** des tableaux de bord interactifs et des indicateurs clés pour un pilotage en temps réel.

Répondre à cette problématique permettra de doter les entreprises d’un outil unique, évolutif et sécurisé, capable de répondre aux exigences réglementaires tout en facilitant la prise de décision et la réactivité face aux nouveaux risques.

* + 1. **Étude de l’existant :**

La conception et la réalisation de tout projet doivent être précédées par une étude de l’existant qui détermine les points faibles et les points forts des systèmes actuels, tenant compte des objectifs à atteindre. La recherche que nous avons menée sur les solutions de Gouvernance et de Monitoring existantes dans le marché tunisien et dans le marché international, nous a permis d’exposer dans la suite quelques applications qui s’y intéressent de près :

* + - 1. **Étude de l’application SimpleRisk**

**SimpleRisk,** vise à centraliser la gestion des risques au sein des entreprises, en proposant une plateforme intuitive, complète et adaptée aux exigences de gouvernance et de conformité des organisations modernes . *D’une part*, cette plateforme va permettre aux entreprises d’identifier, d’évaluer, de suivre et d’atténuer l’ensemble de leurs risques sur une interface unique , leur offrant une vue globale pour prioriser les actions, anticiper les problèmes et assurer la conformité réglementaire. *D’autre part*, elle permettra aux équipes chargées des risques et de la conformité de collaborer plus facilement grâce à des workflows clairs et automatisés, d’accélérer leurs processus de suivi et de validation, et de se concentrer sur la résolution des problèmes plutôt que sur des tâches administratives lourdes. Nous mettons à la disposition des entreprises un registre centralisé des risques, des workflows intégrés pour la gestion et le suivi des actions, un reporting clair et complet, des outils pour assurer la conformité réglementaire, etc., afin que chaque utilisateur – du dirigeant au collaborateur – puisse bénéficier d’un pilotage des risques simplifié et efficace.



Figure 1.1 – Logo officiel de SimpleRisk

|  |  |
| --- | --- |
| **Avantages :** | **inconvénients :** |
| - Open-source  -Facilité d’Utilisation  - Personnalisation par développeurs  - Communauté active  - Extensibilité | - Fonctionnalités limitées  - Interface utilisateur vieillissante  - Absence de module de conformité avancée  - Manque de tableaux de bord dynamiques  - Gestion des accès et audit peu robuste |

Table 1.2 – Étude ade l’application SimpleRisk

* + - 1. **Étude de l’application Eramba**

**Eramba,** est une plateforme open-source de **Gouvernance, Risque & Comformité (GRC)** destinée à offrir aux organisations un outil unique pour organiser, surveiller et documenter l’ensemble de leurs processus de gouvernance, de gestion des risques et de conformité. *D’une part*, elle permet de définir et de maintenir un référentiel normatif (ISO 27001, SOC 2, PCI-DSS…) tout en traçant incidents, évaluations, plans d’action et audits dans un registre centralisé. *D’autre part*, elle fournit des workflows automatisés pour la gestion des politiques de sécurité, la collecte d’évidences, la planification des revues et la génération de rapports, facilitant la collaboration entre les équipes de sécurité, de conformité et d’audit. Avec ses tableaux de bord prêts à l’emploi, son moteur de reporting et sa modularité via plugins, Eramba s’adresse aussi bien aux petits organismes qu’aux grandes entreprises souhaitant piloter efficacement leurs enjeux GRC.[2]

A green logo with a white background

AI-generated content may be incorrect.

Figure 1.1 – Logo officiel de Eramba

|  |  |
| --- | --- |
| **Avantages :** | **inconvénients :** |
| - Open-source et sans licence  - Référentiels normatifs intégrés  - Workflows GRC complets  - Extensible via plugins et API  - Reporting et tableaux de bord prêts à l’emploi | - Automatisation limitée  - Absence de supervision réseau  - Intégration IAM basique  - Analyse transverse limitée |

Table 1.2 – Etude de l’application Eramba

**1.2.3 Critique de l’existant :**

Cette partie consiste à comprendre et analyser les solutions existantes et à déterminer leurs points

Faibles et leurs points forts pour pouvoir dégager les besoins du projet, et de les prendre en considération

|  |  |
| --- | --- |
| **Avantages :** | **inconvénients :** |
| - Plateformes open-source, sans coûts de licence  - Référentiels normatifs (ISO 27001, NIST, SOC 2, GDPR…) intégrés  - Workflows GRC complets (risque, contrôle, conformité, plans d’action)  - Extensible via plugins et API  - Communauté active et documentation pour pilotes (configurations, guides, retours d’expérience) | - Automatisation limitée (calculs semi-manuels, pas de supervision réseau)  - Supervision SNMP / collecte d’actifs absente  - IAM & gouvernance basiques (intégration Keycloak/accès peu granulaires)  - Tableaux de bord statiques ou vieillissants (manque d’indicateurs temps réel et de filtres avancés)  -UX/UI perfectible (ergonomie, responsivité, cohérence graphique) |

Table 1.2 – Etude de l’application Eramba

**1.2.4 Solution proposée :**

Notre solution, SentinelRisk, se présente comme une plateforme web modulaire et centralisée, conçue pour couvrir l’ensemble du cycle de vie de la gestion des risques et de la conformité réglementaire. Elle repose sur une architecture à trois niveaux : un backend robuste développé en Spring Boot, exposant des API REST sécurisées par Keycloak ,un frontend moderne en Angular Material garantissant une expérience utilisateur fluide et responsive et une base de données PostgreSQL, assurant performance et fiabilité du stockage des données. SentinelRisk intègre nativement la gestion des identités et des accès (IAM) via Keycloak pour relier automatiquement les profils utilisateurs aux workflows de mitigation et aux processus d’audit. Les principaux modules – catégories de risque, identification et évaluation des risques, contrôle et plan de mitigation, évaluations périodiques et mapping vers les cadres ISO 27001, NIST, GDPR, SOC 2 – communiquent entre eux afin d’offrir un référentiel unique et cohérent. L’automatisation du calcul des scores de risque, la génération dynamique de tableaux de bord et d’alertes, ainsi que le déploiement simplifié en conteneurs Docker garantissent une solution évolutive, facile à maintenir et adaptée aux besoins des PME comme des grands groupes.

## **Étude de méthodologie de développement**

* + 1. **Introduction**

Une méthodologie de développement est un cadre utilisé pour structurer, planifier et contrôler le développement d’une application. C’est la manière particulière avec laquelle les tâches dans ce projet sont organisées. Une méthodologie de développement permet : de produire un produit de meilleur qualité (mieux documenté, acceptable par l’utilisateur, facile à maintenir, plus homogène), aide à assurer que les spécifications des utilisateurs sont suivies, aide le manager du projet à contrôler le projet, réduit les coûts de développement, encourage la communication entre les personnes.

* + 1. **Choix de la méthodologie**

Devant le nombre de méthodes disponibles, le choix parmi elles devient difficile. Nous étudions à ce propos quelques méthodes de développement objet. Suite à cette étude nous choisissons la méthodologie la plus correspondante.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Description** | **Points Forts** | **Point Faibles** |
|  | - Le développement |  |  |
|  | reprend les différentes |  |  |
|  | étapes du cycle en V. |  | -Adapté qu’aux projets |
|  | Par l’implémentation | - Très adaptatif : si | suffisamment gros. Ce |
|  | de versions | chaque prototype | type de cycle |
|  | successives, le cycle | apporte des | dedéveloppement est |
|  | recommence en | fonctionnalités | complexe, entre les |
|  | proposant un produit | indépendantes, il est | étapes prévues en |
|  | de plus en plus complet | possible de changer | théorie et celles mises |
| Spirale | et robuste c’est la | l’ordre de livraison des | en pratique il y a une |
|  | notion de prototype. | versions. | grande différence. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | - Rarement utilisé tel |
|  |  |  | quel. - le V est bien |
|  |  | - Validations | souvent déséquilibré, |
|  |  | intermédiaires. - Facile | tantôt côté analyse, |
|  | - Ce modèle se | de prévoir les tests à | tantôt côté recette et la |
|  | découpe en 9 phases | réaliser au moment où | marge d’erreur est bien |
|  | qui se répondent 2 à 2 : | l’on conçoit une | souvent |
|  | à chaque étape de | fonctionnalité ou une | proportionnelle à la |
|  | conception correspond | interface, le travail | marge de liberté prise |
|  | une phase de test ou de | s’enchaîne donc de | par rapport au modèle |
| En v | validation. | façon assez naturelle. | théorique. . |
|  |  | -Itératif. -Spécifie le |  |
|  | - -Promu par Rational | dialogue entre les |  |
|  | -Le RUP est à la fois | différents intervenants |  |
|  | une méthodologie et un | du projet : les livrables, |  |
|  | outil prêt à l’emploi | les plannings, les | -Coûteux à |
|  | (documents types | prototypes. . . -Propose | personnaliser. -Très axé |
| RUP | partagés dans un | des modèles de | processus, au détriment |
| (Rational | référentiel web). -Cible | documents, et des | du développement : |
| Unified | des projets de plus de | canevas pour des | peu de place pour le |
| Process) | 10 personnes. | projets types. | code et la technologie. |
|  |  |  | - Ne couvre pas les |
|  |  | -Itératif. -Simple à | phases en amont et en |
|  |  | mettre en œuvre. -Fait | aval au |
|  |  | une large place aux | développement : |
| XP | -Ensemble de « Bests | aspects techniques : | capture des besoins, |
| (Extreme | Practices » de | prototypes, règles de | support, maintenance, |
| Program- | développement (travail | développement, | tests d’intégration. . . |
| ming) | en équipes, transfert de | tests. . . -Innovant : | -Élude la phase |
| (Two | compétences. . .). | programmation en duo, | d’analyse, si bien qu’on |
| Tracks) | -Cible des projets de | kick-off matinal | dépenser son énergie à |
|  | moins de 10 personnes. | debout. | faire et défaire. |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | -Plutôt superficiel sur |
|  |  |  | les phases situées en |
|  |  | Itératif. -Fait une large | amont et aval du |
|  |  | place à la technologie | développement : |
| 2TUP | -S’articule autour de | et à la gestion du | capture des besoins, |
| (Two | l’architecture. -Cible | risque. -Définit les | support, |
| Tracks | des projets de toutes | profils des | maintenance,gestion du |
| Unified | les tailles. -Propose un | intervenants, les | changement. -Ne |
| Process) | cycle de | livrables, les plannings, | propose pas de |
|  | développement en Y. | les prototypes | documents types. |

Table 2.1 – Comparaison des méthodes de développement

* + 1. **Méthodologie choisie (En v)**

Le cycle en V est une méthode de gestion de projet linéaire utilisée principalement pour le développement de logiciels. Chaque phase de conception est accompagnée d’une phase de test. Bien que ce modèle soit déjà un peu ancien, il s’agit d’une méthode idéale pour les projets simples et de petite taille.

A diagram of a v

AI-generated content may be incorrect.

Figure 2.1 – Le cycle en v

* + 1. **Les principales caractéristiques de la méthode cycle en V**

La méthode du cycle en V implique toutes les étapes du cycle de mise en œuvre d’un produit ou d’un logiciel. Elle permet de définir le processus d’un projet en neuf étapes regroupées en trois phases : la conception, la réalisation et la validation.

* + - * **La conception :**

Dans un premier temps, la phase de conception permet de recueillir les besoins et spécifications

nécessaires pour programmer de manière exacte l’ensemble du projet. Il s’agit également de compiler à l’avance les éléments indispensables au développement du projet. La conception d’un logiciel selon la méthode du cycle en V implique quatre étapes : l’analyse des besoins, les spécifications, la conception générale et la conception détaillée.

* + - * **La réalisation :**

Après la conception vient l’étape de réalisation qui permet de créer et d’assembler tous les com- posants nécessaires pour arriver au produit final. Il peut s’agir de la fabrication d’un équipement ou du codage d’un logiciel. Dans ce dernier cas, l’équipe choisit le langage de programmation en fonction des attentes fonctionnelles et architecturales établies lors de la phase de conception. L’étape de réalisation doit ensuite suivre les directives et normes de codage en vigueur.

* + - * **La validation :**

conception du produit. Ces mesures d’assurance qualité prennent la forme de tests unitaires, de tests d’intégration, de tests de validation et d’une recette fonctionnelle. Les tests unitaires correspondent à l’étape de conception détaillée. Réalisés au niveau du code par le développeur, ils permettent de détecter et de corriger d’éventuelles erreurs. L’équipe contrôle ainsi le bon fonctionnement de chaque brique logicielle.[3]

* + 1. **Planification du projet**

Le diagramme de Gantt ci-dessous présente la planification de notre projet répartie sur cinq mois. Chaque barre correspond à une phase majeure du cycle en V, positionnée sur l’axe temporel mensuel :

A graph with different colored rectangles

AI-generated content may be incorrect.

Figure 2.1 – Diagramme de Gantt

* + Analyse des besoins : 10 février – 10 mars
  + Spécifications système : 10 février – 10 avril
  + Conception détaillée : 10 mars – 10 avril
  + Implémentation / Développement : 10 avril – 10 juin
  + Tests unitaires : 10 mai – 31 mai
  + Tests d’intégration : 1 juin – 7 juin
  + Tests de validation (recette) : 8 juin – 10 juin

**1.4 Conclusion**

Ce premier chapitre a plongé dans le contexte métier de la gestion des risques en présentant l’organisme d’accueil et ses enjeux, exposé la problématique d’une vision fragmentée et manuelle des workflows GRC, justifié le recours à une méthodologie en cycle en V pour garantir rigueur et traçabilité tout au long du projet, et illustré notre calendrier de travail à travers un diagramme de Gantt. Ces éléments servent de préambule à l’état de l’art présenté au chapitre suivant.

CHAPITRE 2

État de le art

1. **Introduction**

Au sein de l’environnement sans cesse renouvelé des infrastructures informatiques, la supervision réseau est aujourd’hui un pilier indispensable pour garantir performance, fiabilité et sécurité. Confrontés à l’expansion et à la complexité croissantes des architectures, les outils de monitoring doivent évoluer pour fournir des données à la fois précises et en temps réel, tout en offrant simplicité d’usage, capacité de montée en charge et intégration fluide. Le chapitre « État de l’art » propose une étude approfondie des solutions de surveillance réseau les plus répandues, examinant leurs fonctionnalités, architectures et limites. En comparant ces outils selon leur ergonomie, leur évolutivité, leurs performances et leur coût, nous mettons en lumière les lacunes persistantes. Cette analyse révèle tant les atouts que les faiblesses de plateformes établies comme Nagios, Zabbix ou PRTG, et justifie la nécessité d’une solution plus moderne et adaptable. Comprendre l’état actuel du domaine est une étape essentielle pour concevoir un système à la fois innovant et en phase avec les besoins opérationnels du secteur.

1. **Aperçu sur SNMP**

Le protocole SNMP (Simple Network Management Protocol) est couramment employé pour administrer les équipements sur les réseaux IP. Il permet de superviser et de contrôler des matériels tels que routeurs, commutateurs, serveurs ou imprimantes. SNMP repose sur une architecture client-serveur : le gestionnaire SNMP (client) échange avec les agents SNMP (serveurs) installés sur les dispositifs. Cette communication donne aux administrateurs la possibilité de recueillir des indicateurs clés de performance, de configurer les équipements et de recevoir des notifications en cas d’événements réseau.

SNMP a connu plusieurs évolutions : SNMPv1 a vu le jour à la fin des années 1980, suivi de SNMPv2 au début des années 1990, puis de SNMPv3 à la fin des années 1990, cette dernière version apportant des renforcements significatifs en matière de sécurité et de gestion des données. Grâce à ces avancées successives, SNMP demeure un outil fiable et complet pour la gestion des infrastructures réseau.[1]

1. **Importance de la gestion réseau**

Une gestion efficace du réseau est essentielle au maintien de la santé et des performances des infrastructures numériques modernes. Face à la complexité croissante des réseaux et au nombre croissant d'appareils connectés, les entreprises sont confrontées à des défis majeurs pour garantir la fiabilité des communications et des transferts de données. Une gestion réseau efficace contribue à :

* **Surveillance des Performance** : Suivi Continue de réseau performance métrique permet d'identifier en temps opportun les goulots d'étranglement et les opportunités d'optimisation.
* **Gestion des pannes** : SNMP permet une détection rapide des défaillances, ce qui permet aux administrateurs de réagir rapidement pour minimiser les temps d’arrêt.
* **Gestion de la configuration** : Les changements de configuration automatisés peuvent être mis en œuvre à l’aide du SNMP, ce qui améliore l’efficacité opérationnelle et la cohérence entre les appareils.
* **Planification de la capacité**: En analysant les tendances d’utilisation, les organisations peuvent mieux planifier la croissance future et l’affectation des ressources.

L’utilisation efficace du SNMP contribue à l’efficacité organisationnelle globale, réduisant les coûts opérationnels et améliorant la prestation des services.

1. **Historique**

Depuis le début des années 1990, la surveillance du réseau est passée de simples scripts ping à des plateformes sophistiquées en temps réel alimentées par l’automatisation et les analyses.

* 1. **Origines de SNMP**

Le protocole SNMP (Simple Network Management Protocol) voit le jour à la fin des années 1980, alors que l’expansion rapide des réseaux informatiques rendait indispensable un outil de supervision unifié. À mesure que les organisations multipliaient les systèmes interconnectés, le besoin d’un standard pour surveiller et gérer ces infrastructures devint évident. C’est l’Internet Engineering Task Force (IETF) qui élabora SNMP pour répondre à cette exigence.

Conçu pour offrir une méthode simple et efficace de collecte d’informations sur les équipements réseau, SNMP permet aux administrateurs de suivre les performances, diagnostiquer les incidents et administrer les configurations. La première version, SNMPv1, fut formalisée en 1988 via la RFC 1157, jetant les bases d’une gestion de réseau amenée à évoluer au fil des décennies.

* 1. **Évolution des versions SNMP**

L’évolution du protocole SNMP (Simple Network Management Protocol) se décline en trois versions majeures : SNMPv1, SNMPv2 et SNMPv3, chacune apportant des améliorations et corrigeant les limites de la précédente.

Publiée en 1990, SNMPv1 a constitué le socle de la gestion réseau. Elle proposait des mécanismes de requête pour extraire des données et des pièges (« traps ») pour signaler les événements. Cependant, cette première version présentait d’importantes failles de sécurité, reposant uniquement sur des chaînes de communauté pour l’authentification, aisément interceptables.

Présenté au milieu des années 1990, SNMPv2 renforçait SNMPv1 en introduisant la récupération de données en masse et la possibilité de lancer des requêtes d’information fiables pour optimiser les échanges. Malgré des performances accrues et une interface plus conviviale, les lacunes en matière de sécurité restaient importantes, freinant son adoption généralisée. Déployé en 1998, SNMPv3 a comblé ces failles grâce à l’User-based Security Model (USM) robuste et au View-based Access Control Model (VACM). Ces améliorations ont offert une authentification solide, le chiffrement des messages et des contrôles d’accès granulaires, faisant de SNMPv3 la solution de référence pour une gestion réseau sécurisée dans les infrastructures modernes.

1. **Les normes actuel SNMP**

Cette section fournit un aperçu des normes actuel SNMP, y compris leur statut de conformité et de mise en œuvre dans l’ensemble du secteur.

* 1. **Aperçu des normes actuel (IETF RFC)**

Le Internet Ingénierie Tâche Forcer (IETF) a établi plusieurs clé Demande Documents de consultation publique (RFC) définissant les normes SNMP. Les plus importants sont :

* + - **RFC 1157** : définit SNMPv1, établissant le cadre de base et les opérations de gestion du réseau.
    - **RFC 1901-1908** : présente SNMPv2, détaillant les améliorations telles que les performances améliorées et les nouvelles capacités de gestion des données.
    - **RFC 2570-2576** : Spécifie SNMPv3, en se concentrant sur les améliorations de sécurité et l'introduction du modèle de sécurité basé sur l'utilisateur (USM) et de l'accès basé sur la vue Modèle de contrôle (VACM).

Ces RFC fournir des lignes directrices pour exécution SNMP à travers divers appareils et plateformes, garantissant l’interopérabilité et la cohérence des pratiques de gestion du réseau.

* 1. **État de la conformité et de la mise en œuvre dans l’industrie**

SNMPv3 est largement considéré comme la norme pour la gestion de réseau en raison de ses fonctionnalités de sécurité robustes. De nombreux réseaux gestion outils et prise en charge des appareils SNMPv3, réfléchissant un fort industrie changement vers sécurisé gestion pratiques. Conformité avec SNMP les normes varient selon l'organisation, les grandes entreprises et les fournisseurs de services adoptant généralement SNMPv3 pour la gestion des infrastructures critiques.

Bien que SNMPv1 et SNMPv2 soient toujours utilisés, notamment sur les systèmes existants, on observe une nette tendance à leur abandon progressif au profit de SNMPv3. De nombreuses organisations explorent également des protocoles et des stratégies de gestion alternatifs pour compléter SNMP, notamment dans les environnements où le cloud computing et les objets connectés sont prédominants.

1. **Architecture SNMP**

L’architecture Simple Network Management Protocol (SNMP) est conçue pour permettre une surveillance et une gestion efficaces des périphériques réseau. Il fonctionne sur un modèle client-serveur, composé de deux composants principaux : les gestionnaires SNMP et les agents SNMP. Cette architecture permet aux administrateurs réseau de recueillir des informations, de configurer les périphériques et de répondre efficacement aux événements sur divers éléments du réseau.

Le SNMP architecture comprend :

* **SNMP Directeur** : Centralisé logiciel que supervise le fonctionnement du réseau.
* **SNMP Agent** : Logiciel en cours d'exécution sur réseau appareils, collectionner et stockage des données de gestion.
* **Base d'informations de gestion (MIB)** : Base de données définissant la structure et les types de données disponibles pour la gestion.
  1. **Gestion Information Base (MIB)**

Le La base d'informations de gestion (MIB) est une composant crucial de SNMP Architecture. Il s'agit d'un référentiel structuré décrivant les objets gérés au sein d'un périphérique réseau. Les MIB sont organisées hiérarchiquement et utilisent des identifiants d'objet (OID) pour identifier chaque objet de manière unique.

Clé caractéristiques de Les MIB incluent :

* + - **Structure hiérarchique** : les objets sont organisés sous forme d'arborescence, facilitant ainsi la navigation et l'accès.
    - **Standard et Coutume Objets** : Contient standard objets défini par IETF comme Bien en tant qu'objets spécifiques au fournisseur qui fournissent des fonctionnalités supplémentaires.
    - **Types de données** : définit différents types de données pour les objets, tels qu'un entier, une chaîne ou une jauge, permettant une représentation précise des données.
  1. **SNMP agents**

SNMP agents sont logiciel applications installé sur réseau appareils que collecter et gérer l'information. Leurs principales responsabilités comprennent :

* + - **Données Collection** : Surveillance appareil paramètres comme processeur usage, mémoire, trafic réseau, etc. Ces données sont stockées dans la base de données MIB.
    - **Réponse aux demandes** : lorsqu'un gestionnaire SNMP envoie une demande, l'agent récupère les données pertinentes du MIB et répond en conséquence.
    - **Envoi de notifications** : les agents peuvent générer des messages non sollicités appelés interruptions pour alerter le gestionnaire SNMP des événements importants, tels que des pannes ou des dépassements de seuil.
  1. **SNMP gestionnaires et leur rôles**

Les gestionnaires SNMP, souvent intégrés aux systèmes de gestion de réseau (NMS), jouent un rôle essentiel dans la gestion des opérations réseau. Leurs principales fonctions incluent :

* + - **Information Récupération** : Envoi demandes à SNMP agents à collecter données depuis le MIB, permettant la surveillance en temps réel des périphériques réseau.
    - **Configuration Gestion** : Faciliter changements à appareil configurations en envoyant des commandes aux agents, garantissant ainsi des performances optimales de l'appareil.
    - **Surveillance des événements** : analyse continue des données des agents et réponse aux pièges pour résoudre les problèmes rapidement.
    - **Rapports et Analyse** : Agrégation données sur temps pour s'orienter analyse, rapports et planification des capacités, aidant les administrateurs à prendre des décisions éclairées
  1. **Communication Modèle (Protocole Données Unités)**

La communication dans SNMP est principalement réalisé en utilisant Unités de données de protocole (PDU). PDU sont le format pour messages échangés entre SNMP gestionnaires et agents. Le Les principaux types de PDU dans SNMP incluent :

* + - **GET** : Utilisé par le gestionnaire SNMP pour demander des informations à un agent. L'agent répond avec les données demandées.
    - **ENSEMBLE** : Permet le SNMP gestionnaire de modifier le valeurs de spécifique objets dans un MIB de l'agent. Utilisé pour les modifications de configuration.
    - **GETNEXT** : Facilite la récupération de l'objet suivant dans la hiérarchie MIB, permettant au gestionnaire de parcourir la structure MIB.
    - **PIÈGE** : Un non sollicité message envoyé par le agent à le directeur, alerte il à événements importants ou changements de statut.
    - **INFORMER** : Similaire à PIÈGE, mais nécessite reconnaissance depuis le gestionnaire, assurant une communication fiable.

Ces PDU activer robuste et efficace communication dans le SNMP cadre permettant une gestion efficace du réseau.[2]

* 1. **Flux de travail de SNMP opérations**

Le flux de travail des opérations SNMP implique plusieurs étapes clés, en particulier pour les opérations GET, SET et TRAP :

* **OBTENIR Opération :**

1. Le gestionnaire SNMP envoie une requête GET PDU à l'agent SNMP, spécifiant l'OID des données souhaitées.
2. Le agent processus le demande, récupère le données depuis le MIB, et renvoie une réponse PDU contenant les informations demandées.

* **Opération SET** :

1. Le gestionnaire SNMP envoie une requête SET PDU à l'agent, incluant l'OID et la nouvelle valeur à définir.
2. Le agent mises à jour le correspondant objet dans le MIB et répond avec confirmation indiquant le succès ou l'échec de l'opération.

* **PIÈGE Opération** :

1. Lorsqu'un événement important se produit (par exemple, une panne de périphérique ou un dépassement de seuil), l'agent SNMP génère un PDU TRAP.
2. Le agent envoie le PIÈGE à le SNMP directeur, lequel journaux le événement et peut déclencher des alertes ou des réponses automatisées.

Ce flux de travail structuré facilite une communication efficace entre les gestionnaires et les agents, permettant des réponses rapides aux conditions du réseau.

1. **Applications de SNMP**

Ce chapitre examine les applications de SNMP dans divers secteurs, mettant en valeur son rôle essentiel dans la gestion du réseau et la surveillance des performances.

* 1. **Utiliser cas dans divers industries**

Le protocole SNMP (Simple Network Management Protocol) est largement utilisé dans de nombreux secteurs en raison de son efficacité pour la surveillance et la gestion des réseaux. Parmi les principaux cas d'utilisation, on peut citer :

* **Télécommunications** : SNMP est essentiel à la surveillance de l'infrastructure réseau, notamment des routeurs, des commutateurs et des stations de base. Il permet aux fournisseurs de garantir la qualité de service, de gérer la bande passante et de réagir rapidement aux pannes ou aux problèmes de performances.
* **Technologies de l'information (TI)** : Dans les environnements informatiques, SNMP est utilisé pour gérer les serveurs, les postes de travail et les périphériques réseau. Il permet aux administrateurs de surveiller l'état du système, de suivre l'utilisation des ressources et d'appliquer des modifications de configuration à distance.
* **Internet des objets (IoT)** : Face à la prolifération des objets connectés, SNMP joue un rôle essentiel dans leur surveillance et leur gestion. Il permet une gestion centralisée de divers objets connectés, garantissant leur fonctionnement efficace et sécurisé.
  1. **Utilisé réseau surveillance outil**

Nombreux applications et outils effet de levier SNMP pour efficace réseau gestion.

Notable exemples inclure

Dans notre cas, nous utilisons Zabbix, une solution de surveillance réseau open source robuste qui fournit des informations détaillées sur les performances et la santé des infrastructures informatiques. Conçue pour surveiller divers composants, notamment les serveurs, les périphériques réseau, les applications et les ressources cloud, elle offre une grande polyvalence pour différents environnements. Voici les principales fonctionnalités de Zabbix [3].

* **Surveillance en temps réel** : Zabbix offre des fonctionnalités de surveillance en direct, permettant aux administrateurs de suivre les performances du réseau et l'état des appareils en temps réel, ce qui est crucial pour la détection immédiate des problèmes.
* **Méthodes de collecte des données** : il prend en charge plusieurs méthodes de collecte de données, notamment SNMP, IPMI, JMX et la surveillance basée sur des agents, offrant une flexibilité dans la manière dont les données sont collectées.
* **Tableaux de bord personnalisables** : les utilisateurs peuvent créer des tableaux de bord personnalisés adaptés à leurs besoins de surveillance spécifiques, affichant des indicateurs clés et des tendances pour une analyse rapide.
* **Alerte et Notifications** : Zabbix dispose d'un puissant système d'alerte qui peut informer les utilisateurs de problèmes potentiels par e-mail, SMS ou autres méthodes de communication, garantissant des réponses rapides aux événements critiques.
* **Évolutivité** : Il est conçu pour évoluer des petits réseaux aux grands environnements d'entreprise, capable de surveiller des milliers d'appareils sans compromettre les performances.
* **Données historiques et rapports** : Zabbix conserve les données historiques, permettant l'analyse des tendances et les rapports de performances, ce qui facilite la planification des capacités et la gestion des ressources.

1. **Progrès et innovations récents**

Cette section explore les derniers développements en matière de gestion de réseau qui améliorent et complètent les fonctionnalités SNMP traditionnelles .

* 1. **Nouveau Protocoles et Cadres complétant SNMP**

Les avancées récentes en matière de gestion de réseau ont introduit de nouveaux protocoles et infrastructures qui améliorent les capacités de SNMP. Des protocoles tels que NETCONF et RESTCONF offrent des moyens plus flexibles et plus efficaces de gérer les périphériques réseau, permettant la configuration et la surveillance via des services web modernes .

* 1. **Intégration avec moderne technologies**

L'intégration de SNMP aux technologies modernes, telles que le cloud computing et l'intelligence artificielle (IA), transforme la gestion des réseaux. Les solutions de surveillance cloud permettent une gestion centralisée des réseaux distribués, tandis que les algorithmes d'IA analysent les modèles de données pour prédire les problèmes réseau et optimiser les performances, améliorant ainsi la fiabilité globale des infrastructures réseau.

* 1. **Développement d’alternatives SNMP**

Face à l'évolution des besoins en gestion réseau, plusieurs alternatives au protocole SNMP sont développées. Les API RESTful, par exemple, offrent une approche plus simple et plus flexible de la gestion réseau, facilitant ainsi l'intégration aux applications et services web. Ces alternatives fournissent aux développeurs les outils nécessaires pour créer des systèmes de gestion réseau plus dynamiques et réactifs.