MIASA

Niharison Dyco

L3 MIT/MISA

Analyse des existants et des besoins

1. Introduction

La gestion des infrastructures réseau est un enjeu crucial pour les entreprises modernes, nécessitant des solutions performantes et adaptées aux besoins spécifiques des organisations. L'objectif de cette analyse est de comprendre les outils existants, leurs atouts et leurs limites, afin d'identifier les besoins qui guideront le développement d'une solution optimisée.

Dans cette étude, nous utilisons une approche méthodologique basée sur :

- Une analyse des **solutions existantes** via un benchmarking des outils couramment utilisés.
- Une évaluation des **performances et limites** de ces solutions pour identifier les améliorations possibles.
- Une identification des **contraintes et besoins** fonctionnels et techniques nécessaires à la mise en place du projet.

L'objectif final est de proposer une solution innovante et efficace, répondant aux exigences des entreprises en matière de gestion de réseau.

2. Analyse de l'existant

2.1. Présentation des solutions actuelles

Actuellement, plusieurs solutions de gestion de réseau sont disponibles sur le marché, allant des logiciels open-source aux solutions propriétaires. Parmi les outils les plus couramment utilisés, nous retrouvons :

- **Nagios** : Solution open-source populaire permettant la supervision des infrastructures réseau et serveurs. Elle est extensible mais requiert une configuration avancée.
- **Zabbix** : Plateforme de surveillance réseau avancée, offrant des analyses en temps réel et une interface intuitive. Toutefois, elle demande des ressources système importantes.
- **PRTG Network Monitor** : Outil commercial offrant une interface conviviale et des fonctionnalités puissantes, mais dont le coût des licences peut être un frein pour certaines entreprises.
- **SolarWinds Network Performance Monitor** : Solution robuste pour la supervision réseau, mais qui peut être complexe à configurer et nécessite un budget conséquent.

2.2. Fonctionnalités disponibles et leurs limites

Les principales fonctionnalités offertes par ces outils incluent :

- ✔ Surveillance en temps réel des équipements réseau.
- ✔ Gestion des alertes et notifications en cas d'incident.
- ✔ Collecte et analyse des logs pour le diagnostic des problèmes.
- ✔ Visualisation graphique des performances réseau.
- ✔ Gestion des configurations et supervision des mises à jour.

Cependant, malgré ces fonctionnalités avancées, plusieurs **limitations** sont relevées :

- ✗ Interfaces utilisateur parfois complexes, nécessitant une formation approfondie.
- ✗ Coût élevé des licences pour les solutions propriétaires.
- ✗ Intégration limitée avec d'autres outils de gestion informatique.
- ✗ Manque de flexibilité pour personnaliser les fonctionnalités selon les besoins spécifiques des entreprises.

2.3. Évaluation des performances et adoption des solutions existantes

L'adoption des solutions existantes varie selon les entreprises et leurs besoins spécifiques. Les grandes entreprises privilégient souvent des solutions propriétaires offrant des garanties en matière de support et de maintenance. En revanche, les PME optent davantage pour des outils open-source pour des raisons budgétaires.

L'évaluation des performances des solutions actuelles montre que :

- Les outils open-source sont économiques mais nécessitent une expertise technique pour leur mise en place et leur maintenance.
- Les solutions propriétaires offrent une meilleure expérience utilisateur, mais leur coût peut être prohibitif.
- Aucune solution ne propose une approche **totalement intégrée**, combinant flexibilité, facilité d'utilisation et faible coût.

2.4. Contraintes techniques et organisationnelles

Les entreprises rencontrent plusieurs défis liés à la gestion de leur réseau :

Contraintes techniques :

- Besoin d'une infrastructure robuste pour supporter l'outil de surveillance.
- Compatibilité avec divers équipements réseau (switches, routeurs, serveurs).
- Exigence de haute disponibilité et de tolérance aux pannes.

Contraintes organisationnelles :

- Nécessité de former les équipes IT à l'utilisation des outils.
- Intégration avec les politiques de cybersécurité en place.
- Gestion des droits d'accès et des rôles au sein des équipes.

---

3. Identification des besoins

Suite à cette analyse, plusieurs besoins clés ont été identifiés pour concevoir une solution adaptée et performante.

3.1. Besoins fonctionnels

- **Surveillance en temps réel** : Affichage instantané de l'état du réseau, des équipements et des flux de données.
- **Gestion proactive des alertes** : Notifications intelligentes en cas de panne ou d'anomalie détectée.
- **Rapports et analyses détaillées** : Génération automatique de statistiques et tableaux de bord interactifs.
- **Gestion centralisée des configurations** : Uniformisation des paramètres réseau et automatisation des mises à jour.

3.2. Besoins non fonctionnels

- **Interface utilisateur intuitive** : Simplification de l'expérience utilisateur pour une prise en main rapide.
- **Performance et scalabilité** : Capacité à gérer un grand volume de données sans impact sur les performances.
- **Interopérabilité** : Compatibilité avec d'autres outils de gestion IT et cybersécurité.

3.3. Besoins techniques

- **Infrastructure cloud ou hybride** : Hébergement flexible permettant une accessibilité à distance.
- **Sécurisation avancée** : Mise en place d'authentification forte (OAuth2, 2FA).
- **Automatisation et intelligence artificielle** : Détection proactive des anomalies et recommandations d'optimisation.

---

4. Contraintes et risques

Tout projet de gestion de réseau comporte des défis et risques qu'il convient d'anticiper.

4.1. Contraintes légales

- Respect des réglementations.
- Conformité aux normes ISO 27001.
- Gestion des journaux d'audit et traçabilité des actions réseau.

4.2. Contraintes budgétaires

- Investissement initial pour l'acquisition et l'installation du logiciel.
- Coûts de maintenance et mises à jour.
- Budget alloué à la formation des équipes IT.

4.3. Contraintes techniques

❍ Adaptabilité du système aux infrastructures existantes.
❍ Capacité à gérer des environnements réseau complexes et multi-sites.
❍ Protection contre les cyberattaques et vulnérabilités.

4.4. Risques du projet

❍ **Complexité de mise en œuvre** : Risque de retard dans le déploiement.
❍ **Acceptation par les utilisateurs** : Résistance au changement des équipes IT.
❍ **Évolutivité** : Adaptation du système aux besoins futurs et croissance des infrastructures.

5. Conclusion

L'analyse des solutions existantes et des besoins démontre qu'il est essentiel de développer une solution de gestion de réseau **moderne, intuitive et hautement sécurisée**.

Les principales recommandations sont :

✔ Développer une **interface simplifiée** pour améliorer l'expérience utilisateur.

✔ Intégrer des **fonctionnalités avancées de surveillance** et d'alerte intelligente.

✔ Garantir une **interopérabilité maximale** avec les autres outils de gestion IT.

✔ Mettre en place une **sécurisation renforcée** pour prévenir les cybermenaces.

En prenant en compte ces éléments, le projet vise à offrir une plateforme de gestion de réseau **fiable, évolutive et adaptée aux défis des entreprises modernes**