

MIASA

Niharison Dyco

L3 MIT/MISA

Cahier des charges fonctionnel

1. Présentation du projet

Élément	Description
Nom du projet	Système de Gestion de Réseau d'Entreprise
Objectif principal	Offrir une solution intuitive et efficace pour surveiller et gérer les infrastructures réseau
Périmètre du projet	Surveillance en temps réel, gestion des équipements, journalisation des incidents, optimisation des performances

2. Modules et unités fonctionnelles

2.1. Module 1 : Supervision du Réseau

UF1	Surveillance en temps réel des équipements et du trafic
Description	Surveillance en temps réel des équipements et du trafic
MP	Permet la configuration des seuils d'alerte et des métriques surveillées
État d'entrée	Données collectées des équipements réseau (SNMP, ICMP)

État de sortie	Alertes et tableaux de bord actualisés
Contraintes	Doit supporter au moins 250 équipements connectés
Utilisateur	Administrateurs réseau

UF2	Analyse des performances réseau
Description	Évaluation des performances du réseau à l'aide de métriques spécifiques
MP	Génération automatique de statistiques sur l'usage de la bande passante
État d'entrée	Logs de trafic et données de performance
État de sortie	Graphiques et rapports d'analyse
Contraintes	Doit inclure des seuils paramétrables pour chaque équipement
Utilisateur	Administrateurs et ingénieurs réseau

UF3	Gestion des alertes et notifications
Description	Configuration et envoi d'alertes en cas d'anomalies
MP	Personnalisation des types d'alertes et des destinataires
État d'entrée	Événements déclenchés par des anomalies détectées

État de sortie	Notifications via email, SMS ou interface web
Contraintes	Doit fonctionner en temps réel et avec un historique des alertes
Utilisateur	Administrateurs réseau

2.2. Module 2 : Gestion des Configurations

UF1	Gestion centralisée des configurations réseau
Description	Interface permettant la modification des configurations des équipements
MP	Synchronisation automatique des paramètres entre les équipements
État d'entrée	Paramètres réseau modifiés
État de sortie	Configuration appliquée sur les équipements
Contraintes	Compatible avec plusieurs types d'équipements
Utilisateur	Administrateurs réseau

2.3. Module 3 : Journalisation et Rapports

UF1	Stockage et analyse des logs du réseau
Description	Collecte et archivage des événements réseau
MP	Filtrage et tri des logs selon différents critères
État d'entrée	Logs générés par les équipements
État de sortie	Base de données centralisée des logs

Contraintes	Doit supporter une rétention d'au moins 2 à 3 ans
Utilisateur	Administrateurs et analystes réseau

UF2	Génération automatique de rapports sur incidents
Description	Création de rapports détaillés sur les incidents détectés
MP	Programmation automatique des rapports
État d'entrée	Données des incidents collectés
État de sortie	Rapports PDF, Excel ou HTML
Contraintes	Exportation et envoi automatisé des rapports
Utilisateur	Administrateurs et responsables IT

2.4. Module 4 : Sécurité et Authentification

UF1	Gestion des accès et surveillance des comportements suspects
Description	Gestion des accès et surveillance des comportements suspects
MP	Authentification multi-facteurs et journalisation des accès
État d'entrée	Tentatives de connexion et logs d'accès

État de sortie	Alertes en cas de comportement suspect
Contraintes	Doit être conforme aux normes de sécurité IT
Utilisateur	Administrateurs de sécurité

UF2	Implémentation de l'authentification OAuth2 et gestion des rôles
Description	Gestion avancée des droits d'accès
MP	Supporte l'authentification LDAP et OAuth2
État d'entrée	Données d'authentification des utilisateurs
État de sortie	Accès accordé ou refusé selon les rôles
Contraintes	Sécurisation des mots de passe et protocoles HTTPS
Utilisateur	Administrateurs et utilisateurs réseau